robustel | User Guide

MG460

Maritime Cyber Security Gateway

robustOS Pro

Guangzhou Robustel Co., Ltd.
www.robustel.com

About This Document

This document provides hardware and software information of the Robustel MG460 Maritime Cyber Security Gateway, including introduction, installation, configuration and operation.

Trademarks and Permissions

Disclaimer

Supplier's Products and Services related to the operation and monitoring of vessels (including but not limited to solutions relating to onboard navigation and remote ship traffic control) are provided only as an aid to decision making. The safe voyage planning, navigation, manoeuvring, operation and monitoring of and instructions and advice given to vessels are dependent on human skill and judgement and are the responsibility of the relevant appropriately qualified personnel responsible for such tasks in accordance with all applicable laws, regulations and best practices. Accordingly, Supplier will not be liable for any accident, damage or delay caused by or to any vessel owned or operated by Customer or any other person whether or not the accident or damage is related to the operation or failure of the Products or Services.

The contents of this document are subject to change without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the inappropriate use of this document.

Technical Support

Tel: 400-987-3791
Email: support@robustel.com
Web: www.robustel.com

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the router is used in a normal manner with a well-constructed network, the router should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Robustel accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the router, or for failure of the router to transmit or receive such data.

Safety Precautions

General

- The router generates radio frequency (RF) power. When using the router, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your router in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Be sure that the router will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the router for proper operation. Only uses approved antenna with the router. Please contact authorized distributor on finding an approved antenna.
- Always keep the antenna with minimum safety distance of 20 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.
- When used, the device needs a suitable environment.
    1. If indoors, it needs to be provided an indoor enclosure.
    2. If outdoors, it needs to be provided a rain proof enclosure.
- RF exposure statements
    1. For mobile devices without co-location (the transmitting antenna is installed or located more than 20cm away from the body of user and nearby person)
- FCC RF Radiation Exposure Statement
    1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
    2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and human body.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Router may be used at this time.

Using the Router in Vehicle

- Check for any regulation or law authorizing the use of cellular devices in vehicle in local country before installing the router.
- The driver or operator of any vehicle should not operate the router while driving.
- Install the router by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the router.
- The router should be connected to the vehicle's supply system by using a fuse-protected terminal in the vehicle's fuse box.
- Be careful when the router is powered by the vehicle's main battery. The battery may be drained after extended period.

Protecting Your Gateway

To ensure error-free usage, please install and operate your router with care. Do remember the following:

- Do not expose the router to extreme conditions such as high humidity / rain, high temperature, direct sunlight, caustic / harsh chemicals, dust, or water.
- Do not try to disassemble or modify the router. There is no user serviceable part inside and the warranty would be void.
- Do not drop, hit or shake the router. Do not use the router under extreme vibrating conditions.
- Do not pull the antenna or power supply cable. Attach/detach by holding the connector.
- Connect the router only according to the instruction manual. Failure to do it will void the warranty.
- In case of problem, please contact authorized distributor.

Regulatory and Type Approval Information

Table 1: Directives

2011/65/EU	The European RoHS2.0 2011/65/EU Directive was issued by the European parliament and the European Council on 1 July 2011 on the restriction of the use of certain Hazardous substances in electrical and electronic equipment.
	On June 4, 2015, the Official Journal of the European Union published the RoHS2.0 Amendment Directive (EU) In 2015/863, four phthalates (DEHP, BBP, DBP, DIBP) were officially included in the list of restricted substances in Appendix II of RoHS 2.0 (2011/65/EU). From July 22, 2019, all electronic and electrical products exported to Europe (except medical and monitoring equipment) must meet this restriction; from July 22, 2021, medical equipment and monitoring equipment will also be included in the scope of control.
2012/19/EU	The European WEEE 2012/19/EU Directive was issued by the European parliament and the European Council on 24 July 2012 on waste electrical and electronic equipment.
2013/56/EU	The European 2013/56/EU Directive is a battery Directive which published in the EU official gazette on 10 December 2013. The button battery used in this product conforms to the standard of 2013/56/EU directive.

Table 2: Toxic or Hazardous Substances or Elements with Defined Concentration Limits

Name of the Part	Hazardous Substances									
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal parts	X	o	o	o	-	-	-	-	-	-
Circuit modules	o	o	o	o	o	o	o	o	o	o
Cables and cable assemblies	o	o	o	o	o	o	o	o	o	o
Plastic and polymeric parts	o	o	o	o	o	o	o	o	o	o

o:
Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in RoHS2.0.
X:
Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in RoHS2.0.
-:
Indicates that it does not contain the toxic or hazardous substance.

Note: Excessive lead can be exempted.
1.Copper alloy containing up to 4 % lead by weight (RoHS Exemption 6(c)).
2.Electrical and electronic components containing lead in a glass or ceramic other than dielectric ceramic in capacitors, e.g. piezoelectronic devices, or in a glass or ceramic matrix compound (ROHS Exemption 7(c)-Ⅰ)

⚠WARNING:

This product can expose you to chemicals including Lead, known to the State of California to cause cancer and birth defects or other reproductive harm. For more information go to www.P65Warnings.ca.gov.

Document History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Date	Firmware Version	Document Version	Change Description
Jan. 25, 2024	2.1.3	V.1.0.0	Initial release
May 6, 2024	2.1.3	V.1.1.0	Added the installation note and optimized the description.

Contents

Chapter 1 Product Overview

1.1 Key Features

Robustel's MG460 is a new generation of industrial maritime gateway which is compliant to IEC61162-460 (Maritime Safety and Security) standards, IEC60945 standards and IEC61162-1&2 standards. The MG460 can be used as a gateway between on-board vessel equipment and external services (Cloud platforms, servers, etc).

1.2 Package Contents

Before installing your MG460 Router, verify the kit contents as following.

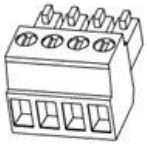
Note:

A) The following pictures are for illustration purposes only, not based on their actual sizes.

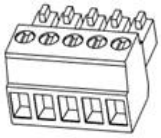
B) It is advisable to use accessories that have the same operating temperature range. However, if the accessories being used do not have the same temperature range, it may be necessary to adjust the operating temperature range accordingly.

- 1 x Robustel MG460 Maritime Cyber Security Gateway

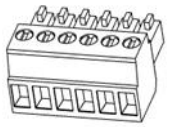
- 1 x 4-pin 3.5 mm male terminal block



- 2 x 5-pin 3.5 mm male terminal block

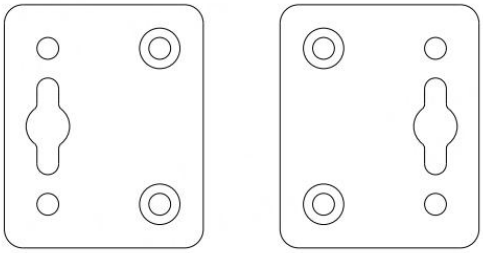


- 1 x 6-pin 3.5 mm male terminal block



- 1 x Wall Mounting Kit or 1 x DIN Rail Mounting Kit (According to actual order requirements)

DIN Rail Mounting Kit



Wall Mounting Kit

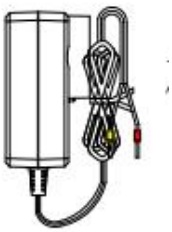
Note: If any of the above items is missing or damaged, please contact your Robustel sales representative.

Optional Accessories (sold separately):

- 4G SMA Cellular Antenna

- RP-SMA WiFi antenna (stubby/magnet optional)

- AC/DC power adapter (24V DC, 2A; EU/US/UK/AU plug optional)



1.3 Specifications

Hardware System

- CPU: Quad core Cortex-A53, 1.6 GHz
- RAM 4 GB DDR4
- Flash: 64 GB eMMC

Cellular Interface

- Number of antennas 4G: 2
- Connector: SMA-K
- SIM: 2 x Mini SIM (2FF)

Ethernet Interface

- Ports: 5 x RJ45, 10/100/1000Mbps, compliance with 1000BASE-T, LAN or WAN Magnet isolation
- Protection: 1 KV

Serial Interface

- Type: 2 x RS232/RS422/RS485 (software configurable)
- Connector: 2 x 6-pin 3.5 mm terminal block ESD protection 8 KV Air, 4 KV Contact Baud rate 300 bps to 115200 bps Signal: RS232: TXD, RXD, GND RS485: Data+ (A), Data- (B), GND RS422: A, B, Y, Z, GND

Console Interface

- Type: 1 x RS232 Connector RJ45 Baud rate 115200 bps
- Signal: TXD, RXD, GND

DI Interface

- Ports: 2 x DI, wet contact Connector 4-pin 3.5 mm terminal block
- Isolation: Bi-directional optocoupler (DI) Absolute maximum VDC + 30V DC Absolute maximum ADC 100 mA
- Signal definition: DI1+, DI1-, DI2+, DI2-

Relay Output Interface

- Ports: 2 x Relay Output Connector 6-pin 3.5 mm terminal block Absolute maximum VDC + 48V DC Absolute maximum ADC 100 mA
- Signal definition: NC1, NO1, COM1, NC2, NO2, COM2

USB Interface

- Ports: 2 x USB 3.0 (host), Type A, 5V 900Ma, 1 x USB 2.0 (OTG), Type C

Others

- SD: 1 x microSD
- HDMI: 1 x HDMI
- Reset button: 1 x RST
- LED indicators: 1 x RUN, 1 x MDM, 2 x USR, 1 x Signal, 1 x VPN
- Watchdog: External

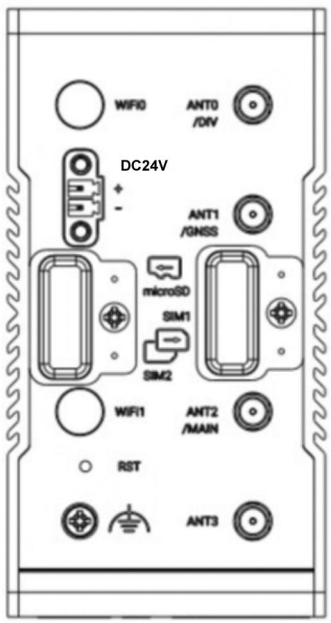
Physical Characteristics

- Ingress protection: IP30
- Housing: Metal
- Dimensions: 58 x 111 x 128 mm
- Installations: Desktop, wall mounting and 35 mm DIN rail mounting
- Operating temperature: -40 ~ +70 °C
- Storage temperature: -40 ~ +85 °C
- Relative humidity: 5 ~ 95% RH

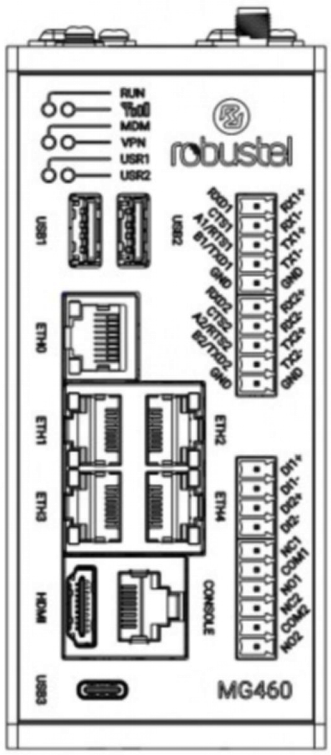
Power Supply

- Connector: 2-pin 3.5 mm terminal block with lock
- Input voltage: 24V DC

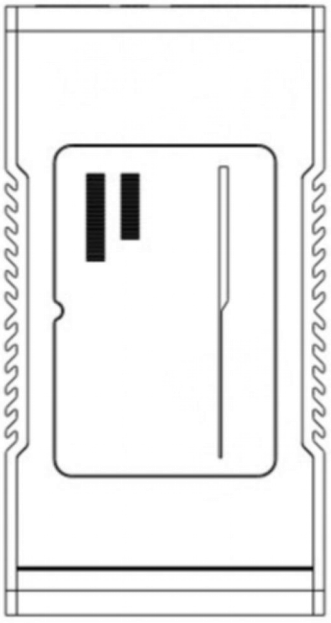
1.4 Dimensions



Top View



Front View



Bottom View

Chapter 2 Hardware Installation

2.1 PIN Assignment

Serial Ports. Two software configurable serial ports, could be configured as RS232 or RS422, or RS485.

Name	RS232 Mode	RS485 Mode	RS422 Mode
RXD1 or RX1+	data receiving		data receiving positive
CTS1 or RX1-	clear to send		data receiving negative
A1/RTS1 or TX1+	request to send	RS485_A1	data sending positive
B1/TXD1 or TX1-	data sending	RS485_B1	data sending negative
GND	Ground	Ground	Ground
RXD2 or RX2+	data receiving		data receiving positive
CTS2 or RX2-	clear to send		data receiving negative
A2/RTS2 or TX2+	request to send	RS485_A2	data sending positive
B2/TXD2 or TX2-	data sending	RS485_B2	data sending negative
GND	Ground	Ground	Ground

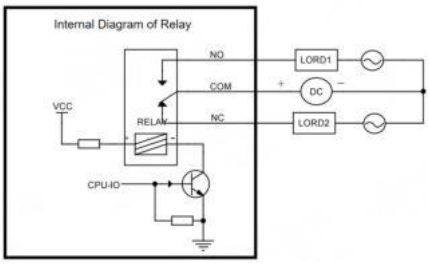
2.2 Ethernet Ports

Ethernet Ports. 5 Ethernet ports, Eth0 is the WAN port, and others are LAN ports.

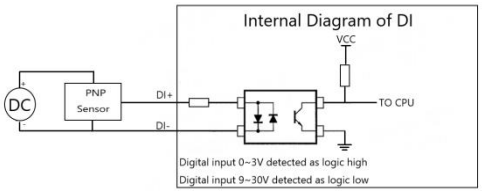
LED		Description
Activity	On, blinking	Transmitting data
	Off	No activity
Link	Off	Link off
	On	Link on

2.3 Digital Input and Relay Output Ports

Two sets of digital inputs and two sets of relay outputs. Some applications for reference are as below:



Note: When the relay is off, NC is connected to COM, and NO is disconnected. The external power supply input voltage range is DC 5-48V, with a maximum load current of 300mA.

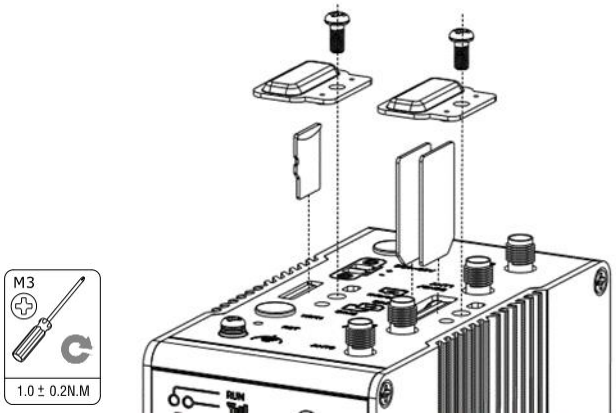


Note: The external power supply DC voltage range is 5V~30V, 0.1A max.

2.4 LED Indicators

LED	Description	
RUN	On, solid	Gateway system is initializing
	On, blinking	Gateway starts operating
	Off	Gateway is powered off
	Note: The RUN LED's color is green	
MDM	Color	2G: Red, 3G: Yellow, 4G: Green
	On, blinking	Link connection is working
	Off	Link connection is not working
	Green	Strong signal
	Yellow	Medium signal
	Red	Weak or no signal
VPN	On, solid	VPN connection is established
	Off	VPN connection is not established

2.5 SIM Card Installation



- **Insert SIM card**

1. Make sure gateway is powered off.
2. To remove slot cover, loosen the screws associated with the cover by using a screwdriver and then find the SIM card slot.
3. To insert SIM card, press the card with finger until you hear a click and then tighten the screws associated with the cover by using a screwdriver.
4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

- **Remove SIM card**

1. Make sure router is powered off.

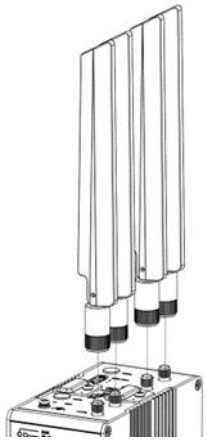
2. To remove slot cover, loosen the screws associated with the cover by using a screwdriver and then find the SIM card slot.
3. To remove SIM card, press the card with finger until it pops out and then take out the card.
4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

Note:

1. Recommended torque for inserting is 0.5 N.m, and the maximum allowed is 0.7 N.m.
2. Use the specific card when the device is working in extreme temperature (temperature exceeding 40 °C), because the regular card for long-time working in harsh environment will be disconnected frequently.
3. Do not forget to twist the cover tightly to avoid being stolen.
4. Do not touch the metal of the card surface in case information in the card will lose or be destroyed.
5. Do not bend or scratch the card.
6. Keep the card away from electricity and magnetism.
7. Make sure router is powered off before inserting or removing the card.

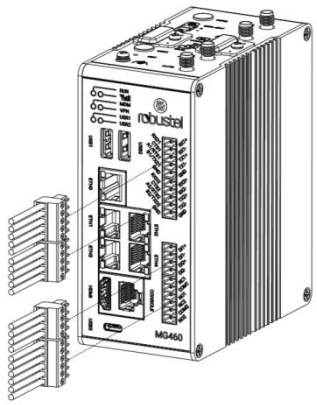
2.6 Attach External Antenna (SMA Type)

Attach an external SMA antenna to the router's antenna connector and twist tightly. Make sure the antenna is within the correct frequency range provided by the ISP.
Note: Recommended torque for tightening is 0.35 N.m.



2.7 Terminal Block Installation

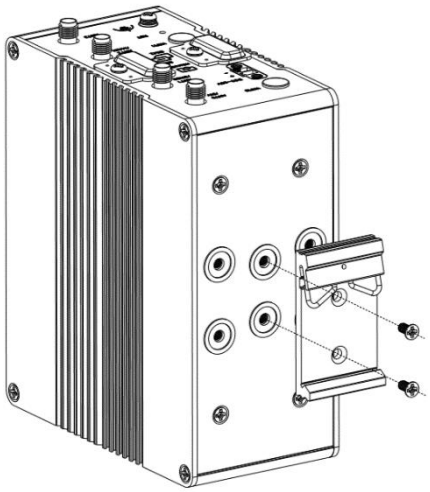
Insert the 4PIN and 5PIN and 6PIN terminal blocks into the interfaces connector, then can connect the devices or sensors to the gateway with wires via corresponding interfaces e.g. RS232/RS485, DIDO...



2.8 Mount the router

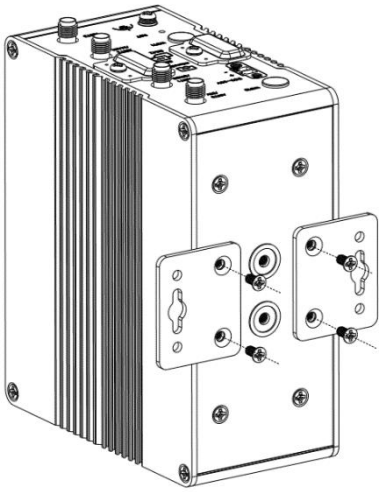
DIN Rail Mounting

Use 2 M3 screws to fix the DIN rail to the device, then hang the DIN rail on the mounting bracket.



Wall Mounting

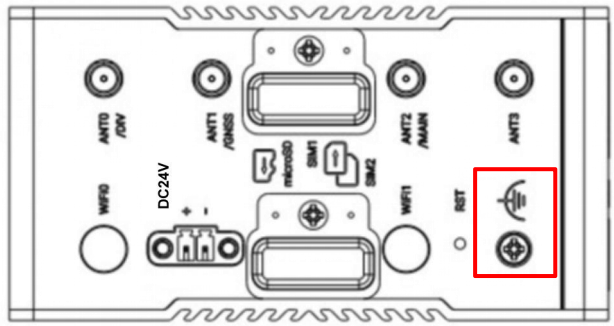
.Use 4 M3 screws to fix the wall mount kit to the device, then hang the wall mount kit on the wall.



2.9Ground the Router

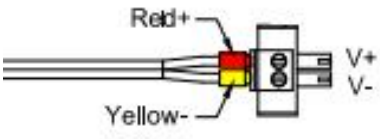
Grounding will help to prevent the noise effect due to electromagnetic interference (EMI). Connect the device to the site ground wire by the grounding screw before powering on.

Note: This product is appropriate to be mounted on a sound grounded device surface, such as a metal panel.



2.10 Power Supply installation

Insert the power supply cord into the corresponding terminal block if needed, then insert the terminal block into the power connector.



MG460 supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way. The last step is to plug the power adapter into your socket.

Note: The typical power voltage is 24V DC.

2.11 Installation notices

Ensure that the MG460 is installed in a secure location with restricted access, requiring authorized personnel to obtain the necessary authority for entry.

Ensure that the MG460 installed with other IEC 61162-460 network components, the MG460 functions as an individual component and does not provide the network monitoring or system management capabilities. These functions are fulfilled by the 460-switch within the IEC 61162-460 network.

Chapter 3 Initial Configuration

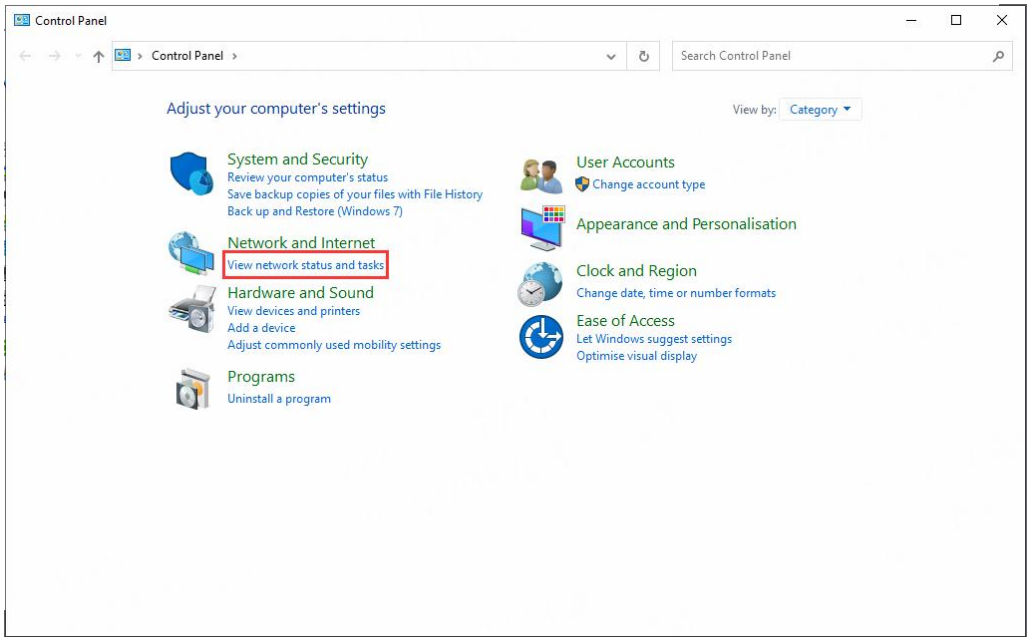
The device can be configured through your web browser that including Microsoft Edge, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows. It provides an easy and user-friendly interface for configuration. There are various ways to connect the device, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC has an Ethernet interface properly installed prior to connecting the device. You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the device. If you encounter any problems accessing the device web interface, it is advisable to uninstall your firewall program on your PC, as this tends to cause problems accessing the IP address of the device.

3.1 PC Configuration

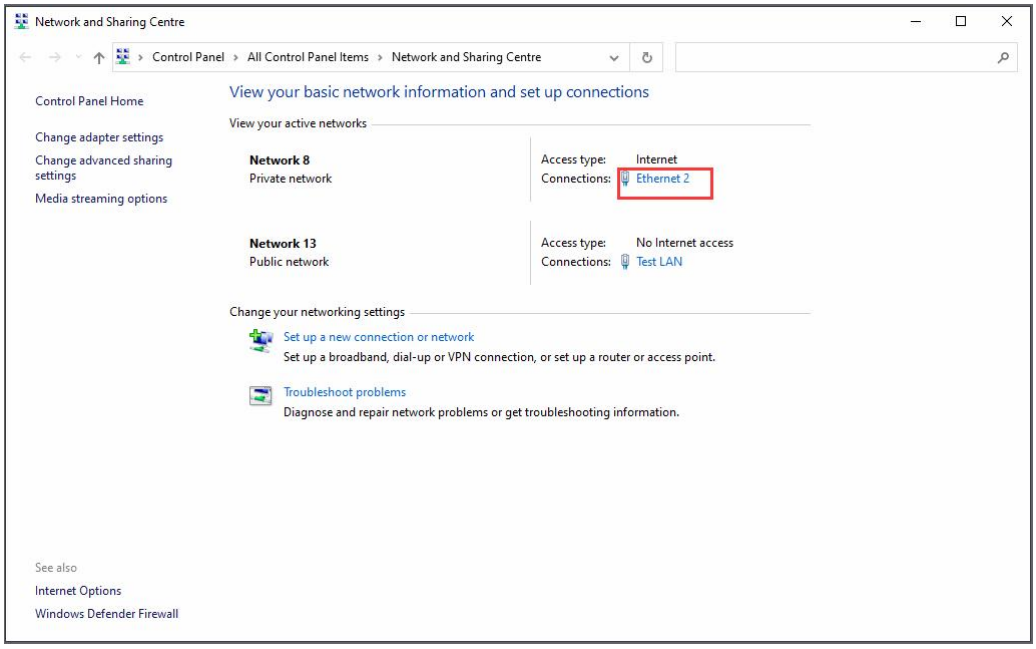
There are two ways to get an IP address for the computer. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configurate a static IP address manually within the same subnet of the router. Please refer to the steps below.

Here take **Windows 10** as an example.The configuration for Windows 7 or newer is similar.

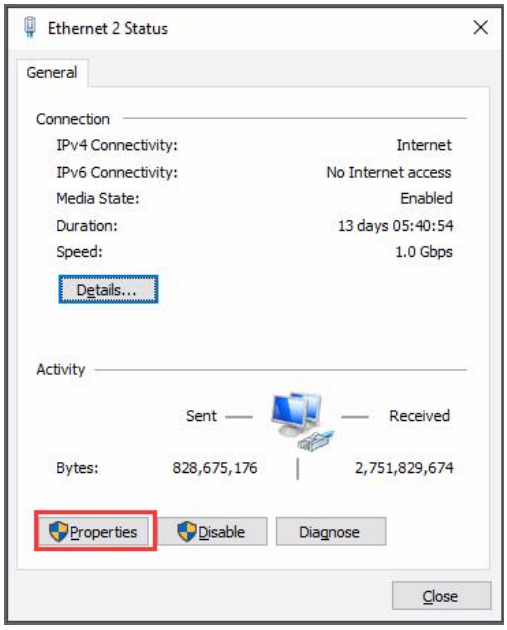
1. Right-click “**Windows LOGO**” on the taskbar, select “**Run**”, and type "**Control**" to launch the Control panel, then Click “**View network status and tasks**”.



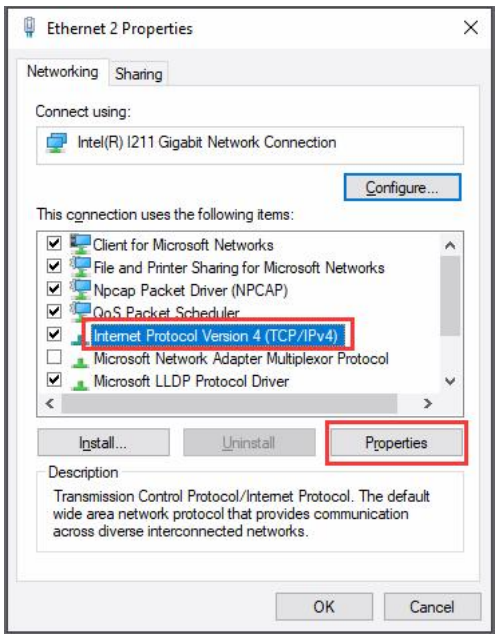
2. After entering “Network and Sharing Center", click "**Ethernet**" connections status.



3. Click **Properties** in the window of **Network Connection status**.

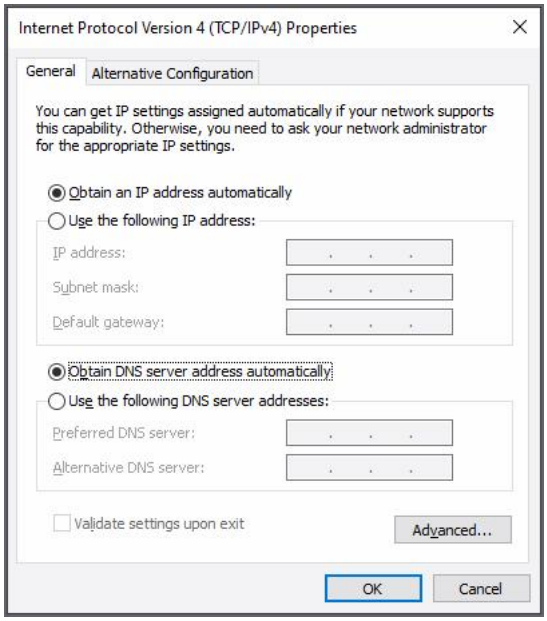


4. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

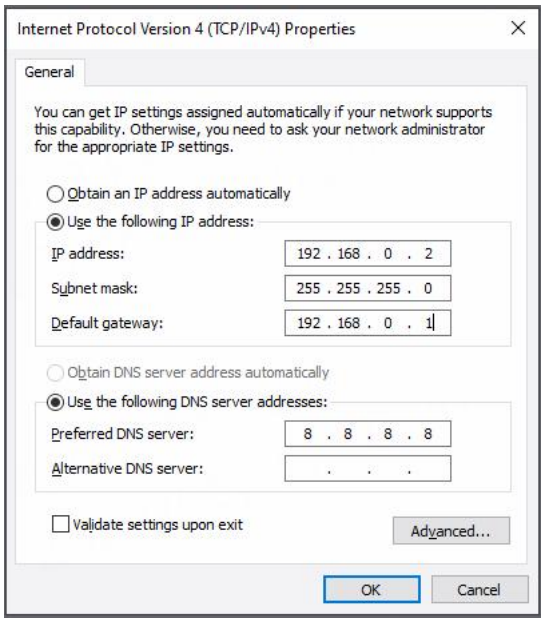


5. Two ways to configurate the IP address of the computer.

(1) Auto obtain from the DHCP server, click "**Obtain an IP address automatically".**



(2) Manually configurate the PC with a static IP address on the same subnet as the device address, click and configurate "**Use the following IP address**";



6. Click **OK** to finish the configuration.

3.2 Factory Default Settings

Before configuring your device, you need to know the following default settings.

Item	Description
Username	admin
Password	See the information from the product label
ETH0	WAN mode
ETHn	192.168.0.1/255.255.0.0, LAN mode
DHCP Server	Enabled

3.3 Factory Reset

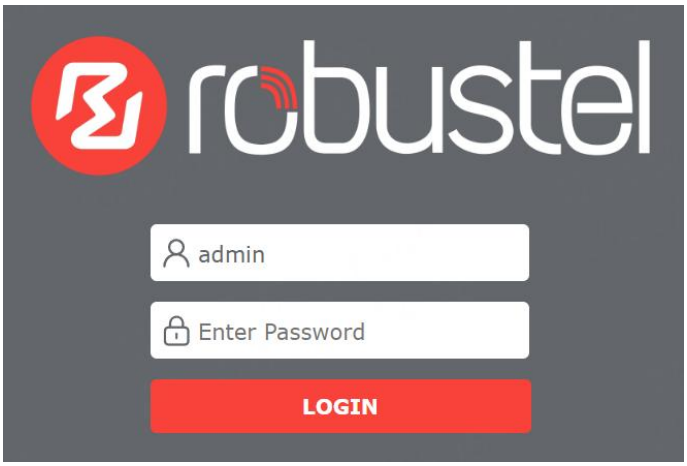
Function	Operation
Reboot	Press and hold the RST button for 2~5 seconds under the operating status.
Restore to default configuration	Press and hold the RST button for 5 ~10 seconds under the operating status. The RUN light flashes quickly, and then release the RST button, and the device will restore to the default configuration.
Restore to factory configuration	Once the operation of restoring the default configuration is performed twice within one minute, the device will restore to the factory default settings.

3.4 Log in the Device

To log in to the management page and view the configuration status of your device, please follow the steps below.

1. On your PC, open a web browser such as Microsoft Edge, Google Chrome or Firefox, etc.
2. From your web browser, type the IP address of the device into the address bar and press enter. The default IP address of the device is https://192.168.0.1/24 ,though the actual address may vary.
   Note: If a SIM card with a public IP address is inserted in the device , enter this corresponding public IP address in the browser's address bar to access the device wirelessly.

3. In the login page, enter the username and password, you can check the login information from the device's stick, and then click **LOGIN**. See the information on the product label for default username and password.
   Note: If enter the wrong password over 6 times, the user account will be locked for 5 minutes.



3.5 Control Panel

After logging in, the home page of the web interface is displayed.

From the homepage, users can find the model information and perform operations such as saving the configuration, restarting the device , and logging out.

Control Panel		
Item	**Description**	**Icon**
Save & Apply	The icon is in gray by default, and will turn red if any modifications on configuration, then click to save the current configuration into device's flash and apply the modification on every configuration page, to make the modification taking effect.	or
Restart	Click to restart all the RobustOS Pro operating system based applications(applications controlled by ystem are not included), then switch to the login page.	
Reboot	Click to reboot the device, then switch to the login page.	
Logout	Click to log the current user out safely. After logging out, it will switch to login page. Shut down web page directly without logout, the next one can login web on this browser without a password before timeout.	

Note: The steps of how to modify configuration are as bellow:

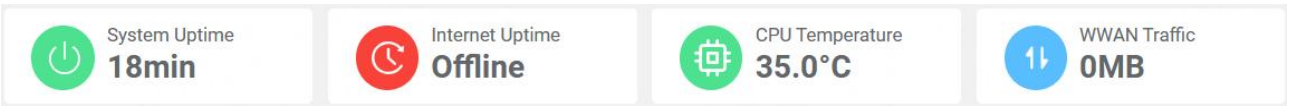
1. Modify in one page;

2. Click Submit under this page;
3. Modify in another page;
4. Click Submit under this page;
5. Complete all modification;
6. Click  for save and apply.

Chapter 4 WebUI Descriptions

4.1 Dashboard

4.1.1 Overview



Item	Description
System Uptime	Show the current amount of time the router has been powered on.
Internet Uptime	Show the current amount of time the router has been connected to internet.
CPU Temperature	Show the CPU temperature.
Traffic	Show the amount of WWAN data traffic usage.

4.1.2 Modem

This page shows the status of SIM card.

Item	Description
	Not connected.
	Weak signal.
	Medium signal.
	Strong signal.

4.1.3 Ethernet

This page shows the device's Ethernet status

Icon	Description
	Port disable or link down.
	Link up.

4.1.4 Internet Status

This page shows the device's Internet status information.

Item	Description
Active Link	Show the currently online link.
IP Address	Show the address of current link.
Gateway	Show the gateway address of the current link.
DNS	Show the current DNS server.

4.1.5 LAN Status

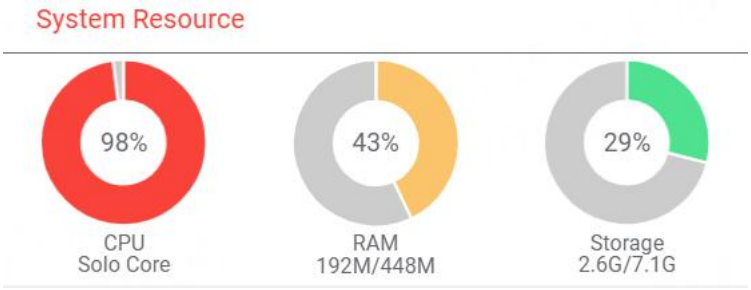
This page shows the device's LAN status

Item	Description
IP Address	Show the IP address of the LAN.
MAC Address	Show the MAC address of the LAN.

4.1.6 System Resource

This page shows the device's system resources usage information.

When the usage is more than 65%, the icon will be in Red.
When the usage is between 30% and 65%, the icon will be in Yellow.
When the usage is less than 30%， the icon will be in Green.



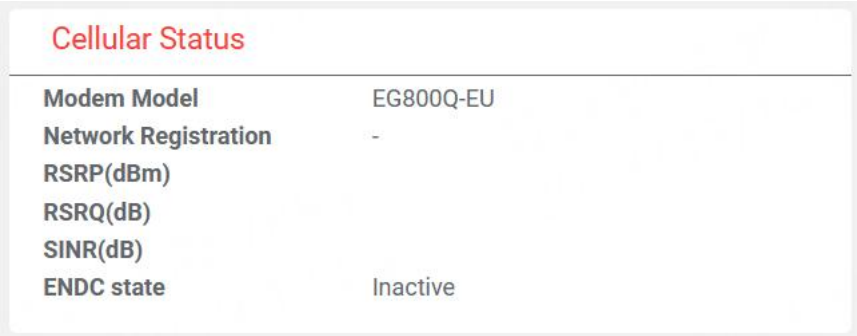
4.1.7 System Information

This page shows the device's system information.

Item	Description
Operating System	Show the operating system information.
System Time	Show the current system time.
Firmware Version	Show the firmware version running on the device.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of your device.

4.1.8 Cellular Status

This page shows the device's cellular status.



Item	Description
Modem Vendor	Show the radio module vendor information.
Modem Model	Show the model of the radio module.
Network Registration	Show the current network registration information.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
IMSI	Show the IMSI (International Mobile Subscriber Identity) number of the current SIM.

4.1.9 RCMS Status

This page shows the device's RCMS status.

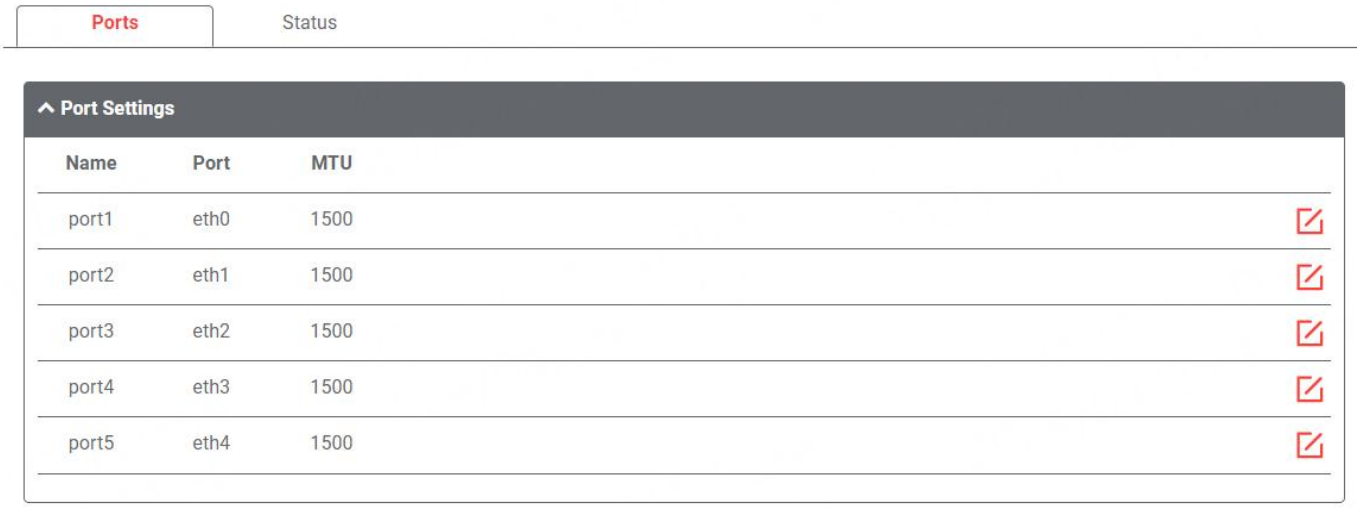
Item	Description
RobustLink Status	Show the status of RobustLink
RobustelLink Last Connected	Show the last connected times of RobustLink
RobustVPN Status	Show the status of RobustVPN
RobustVPN Last Connected	Show the last connected times of RobustVPN
RobustVPN Virtual IP	Show the virtual IP of RobustVPN
RobustVPN SubNet Address	Show the subnet address of RobustVPN

4.2 Interface

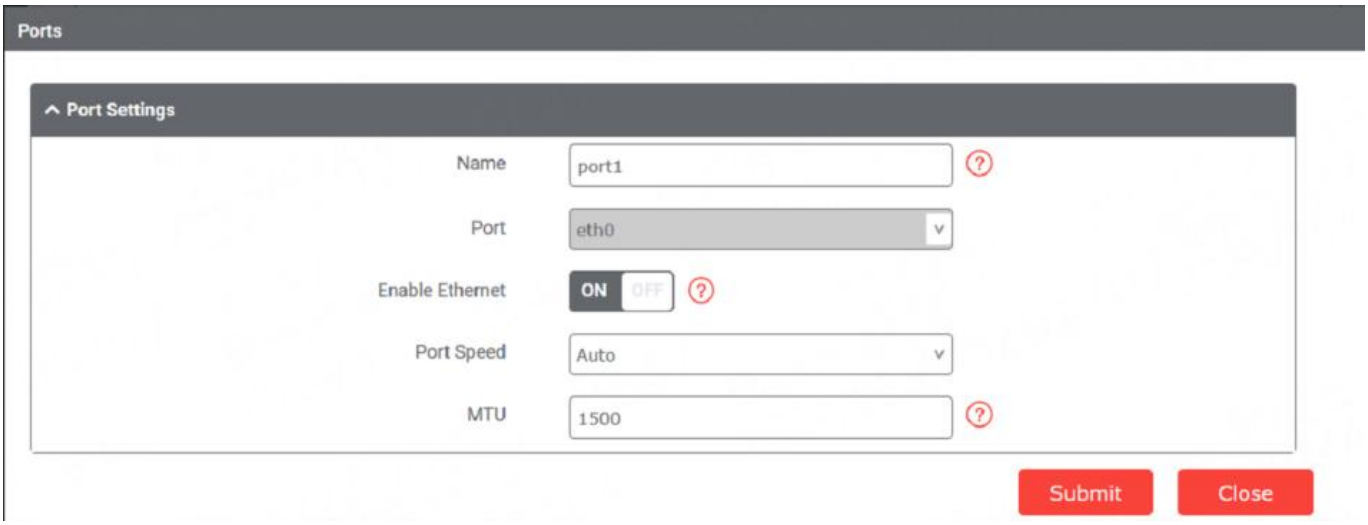
4.2.1 Ethernet

This section allows you to set the related parameters for Ethernet. There are 5 Ethernet ports in the device. The ETH0 is the WAN port, and others are the LAN port.

Ports



Click to configure its parameters, and modify the port assignment parameters in the pop-up window.

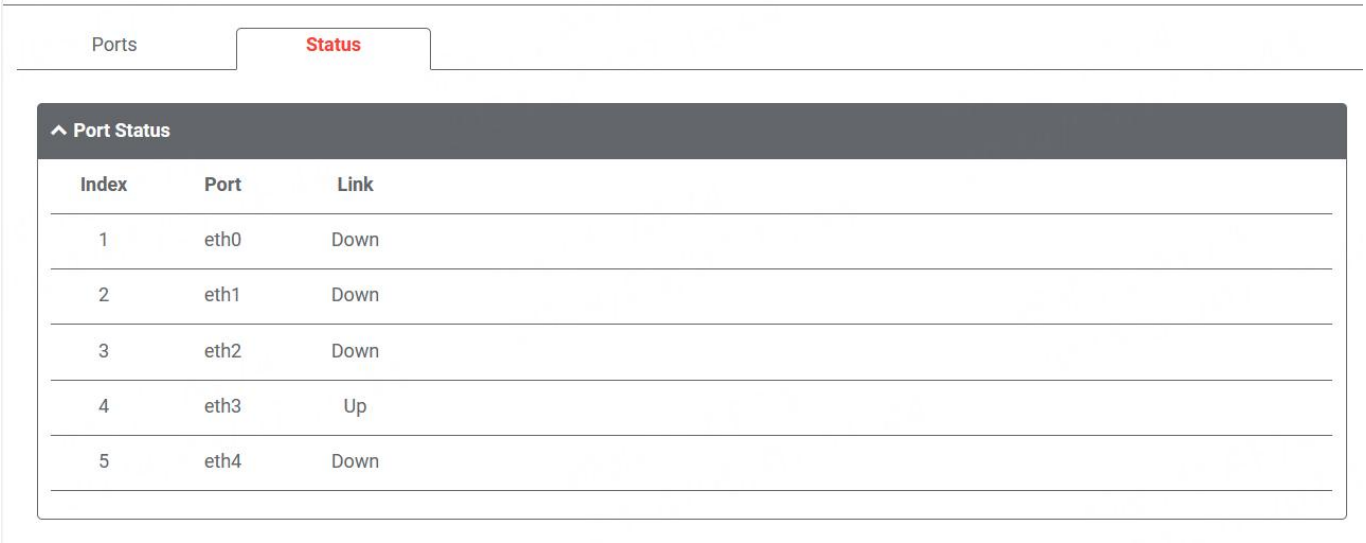


Item	Description	Default
Name	Name of the port.	--
Port	Show the editing port, read only.	--

Enable Ethernet	Click the toggle button to enable/disable the Ethernet port.	ON
Port Speed	Select from “Auto”, “10M-half”, “10M-full”,“100M-half”, “100M-full”,“1000M-half”, “1000M-full”.	Auto
MTU	Enter the value of the maximum transmission unit(MTU).	1500

Status

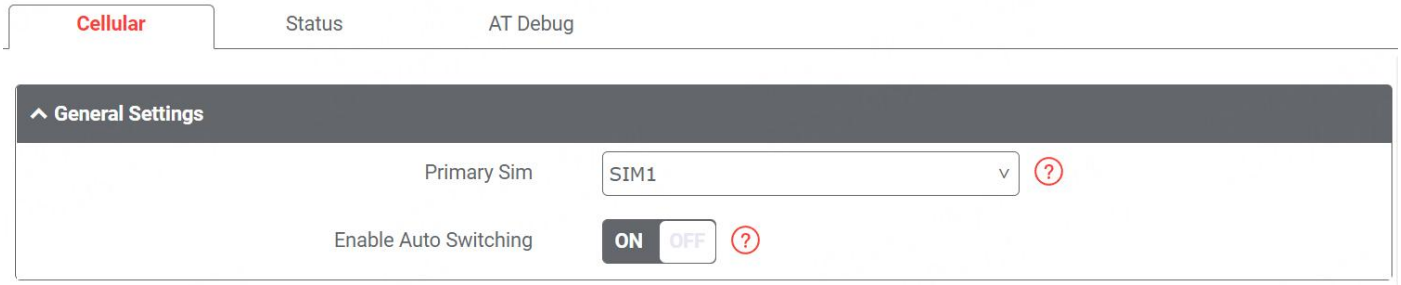
This page allows you to view the status of Ethernet port.



4.2.2 Cellular

This section allows you to set the related parameters of Cellular. The device supports one cellular modem and two SIM slots, but only one SIM slot is activated at any time.

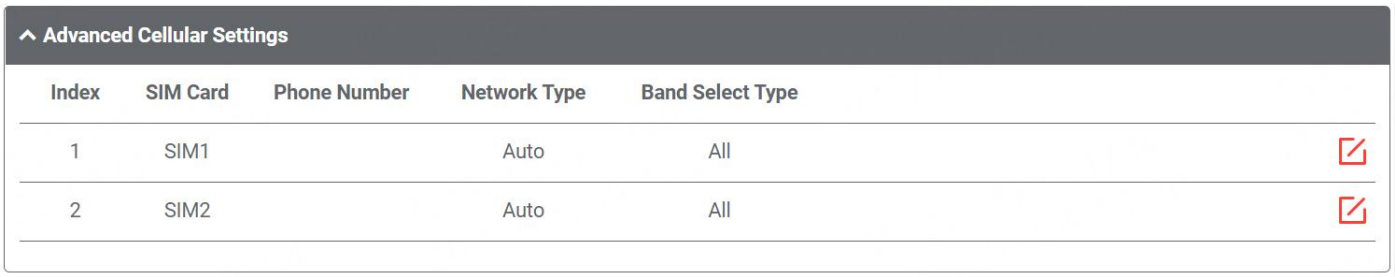
Cellular



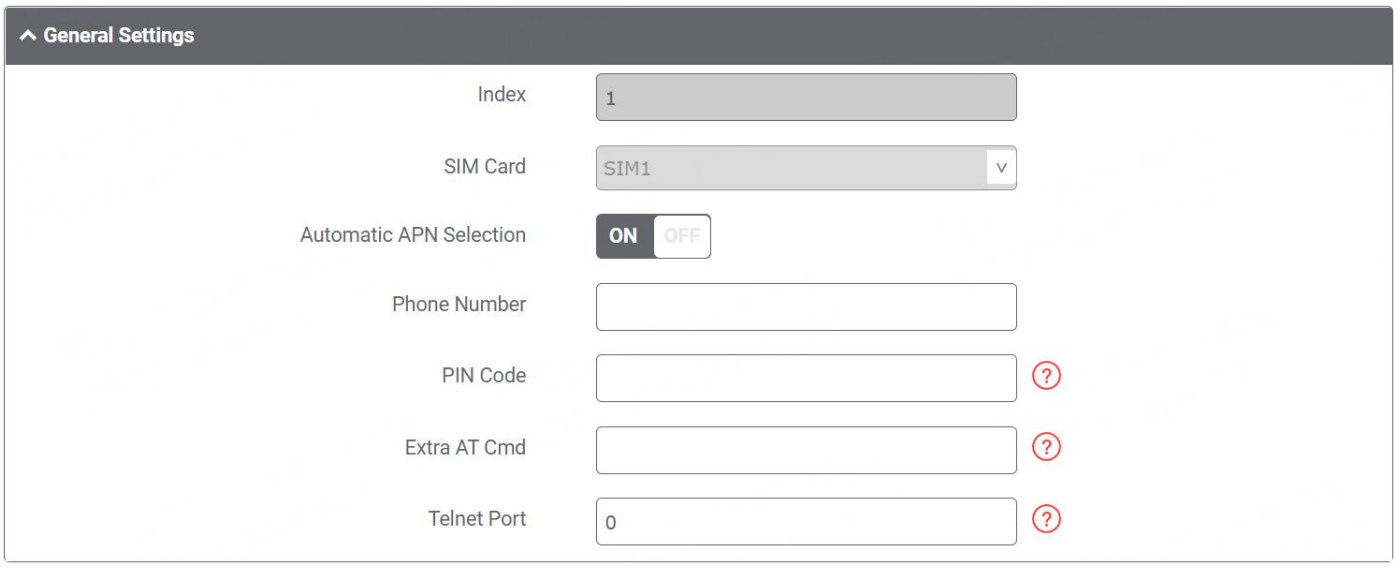
Item	Description	Default
Primary Sim	Select one Sim card as primary Sim card	SIM1

Enable Auto Switching	When auto switching is enabled, the SIM card will be automatically switched to another one when there is SIM card error or connection error or ping fails by default.	ON

Item	Description	Default
Weak Signal	Switch to another SIM card when the signal is poor, only used for dual SIM backup.	ON
While Roaming	Switch to another SIM card while roaming, only used for dual SIM backup.	OFF



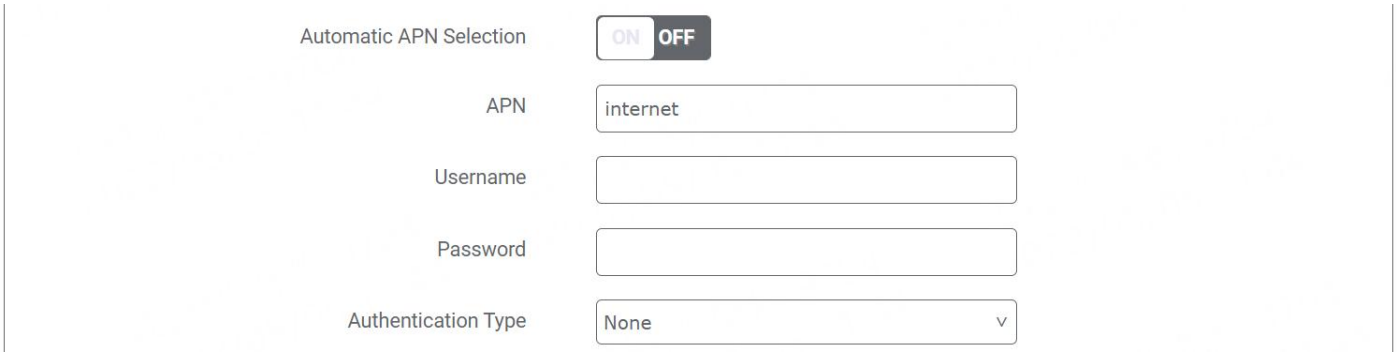
Click to configure its parameters in the pop-up window.



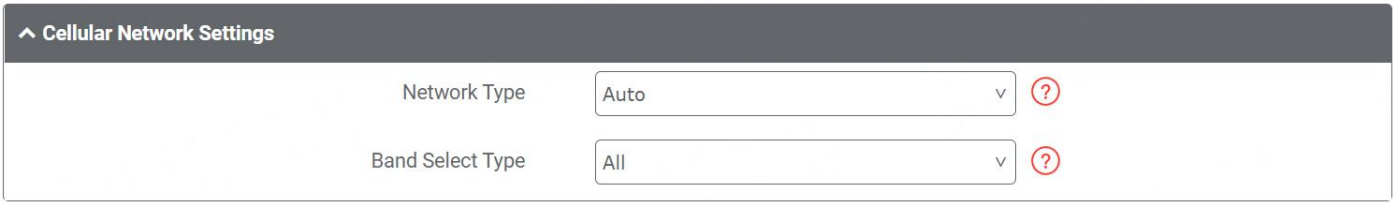
Item	Description	Default
Index	Indicate the ordinal of the list.	--
SIM Card	Show the currently editing SIM card.	--
Automatic APN Selection	Click the toggle button to enable/disable the “Automatic APN Selection” option. After enabling, the device will recognize the access point name automatically. Alternatively, users can disable this option and manually add the access point name.	ON

Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet. 0 means not supported.	0

When the Automatic APN Selection is off, users can specify their own APN setting.



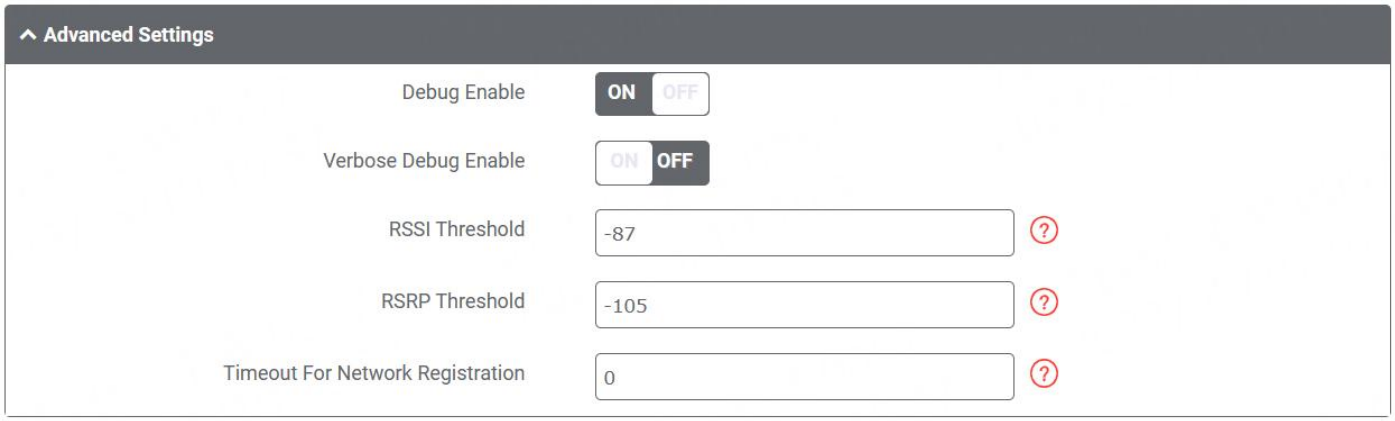
Item	Description	Default
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Authentication Type	Select the authentication type. Select from “None”, “CHAP”, “PAP”. • None: None. • CHAP: Challenge-Handshake Authentication Protocol. • PAP: Password Authentication Protocol.	None



This page allows you to configure cellular network settings. type and network band. You can specify a specific frequency band or network type for device.

Item	Description	Default
Network Type	Select the cellular network type, which is the network access order. Select from “Auto”, “2G Only”, “3G Only”, “4G Only”, “5G Only”. • Auto: Connect to the best signal network automatically • 2G Only: Only the 2G network is connected • 3G Only: Only the 3G network is connected • 4G Only: Only the 4G network is connected • 5G Only: Only the 5G network is connected *Note:*	Auto

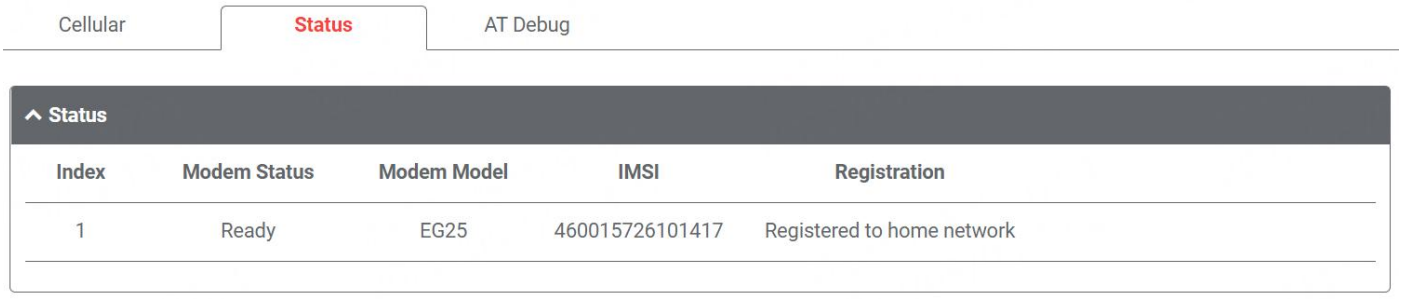
	1) *There may be some different optional network types due to the different cellular module.*	
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify". *Note:* *There may be some differences in Band Setting due to the different cellular module.*	All



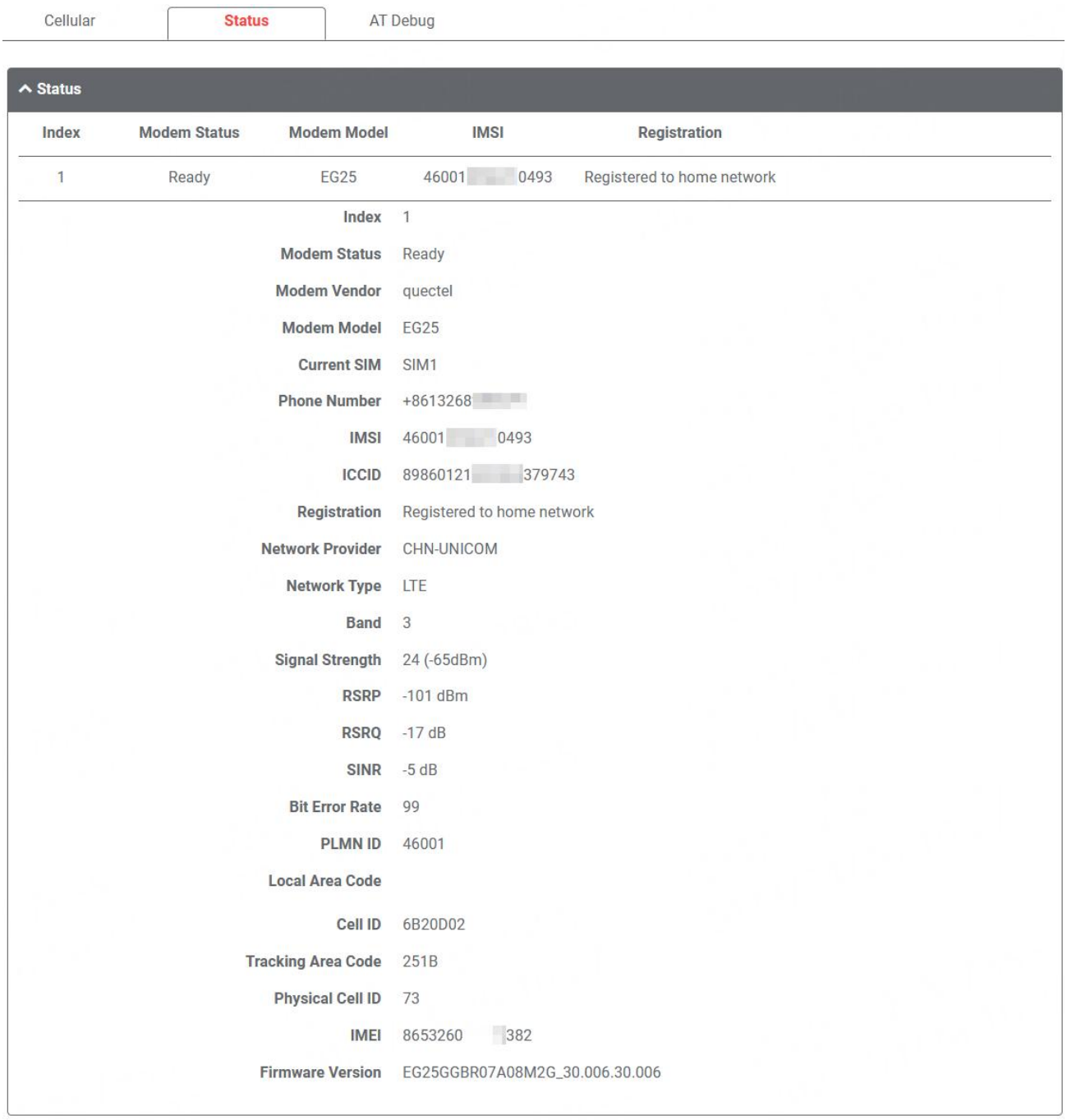
Item	Description	Default
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF
RSSI Threshold	Is used to judge whether the signal is too weak to switch SIM, unit: dbm.	-87
RSRP Threshold	Is used to judge whether the signal is too weak to switch SIM, unit: dbm.	-105
Timeout For Network Registration	The timeout required for the module to register to the network. Unit: seconds. 0 means the default setting is used.	150

Status

This page allows you to view the status of the cellular connection.



Click the row of status, the detailed status information will be displayed under the row.

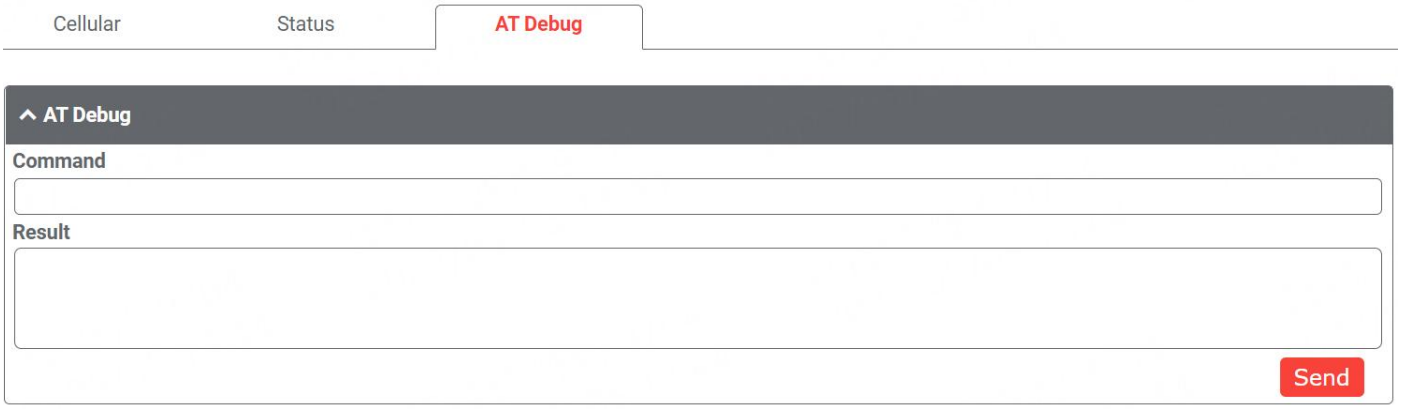


Item	Description
Index	Indicate the ordinal of the list.
Modem Status	Show the status of the radio module.
Modem Vendor	Show the vendor of the radio module.
Modem Model	Show the model of the radio module.
Current SIM	Show the SIM card that your router is using.
Phone Number	Show the phone number of the current SIM.
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.

Item	Description
Network Type	Show the current network service type, e.g. WCDMA.
Band	Show the band information.
Signal Strength	Show the signal strength detected by the mobile.
RSRP	Show the current RSRP when you register to the 4G network.
RSRQ	Show the current RSRQ when you register to the 4G network.
SINR	Show the current SINR when you register to the 5G network.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the router.
Physical Cell ID	Show the current physical cell ID used for locating the router.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

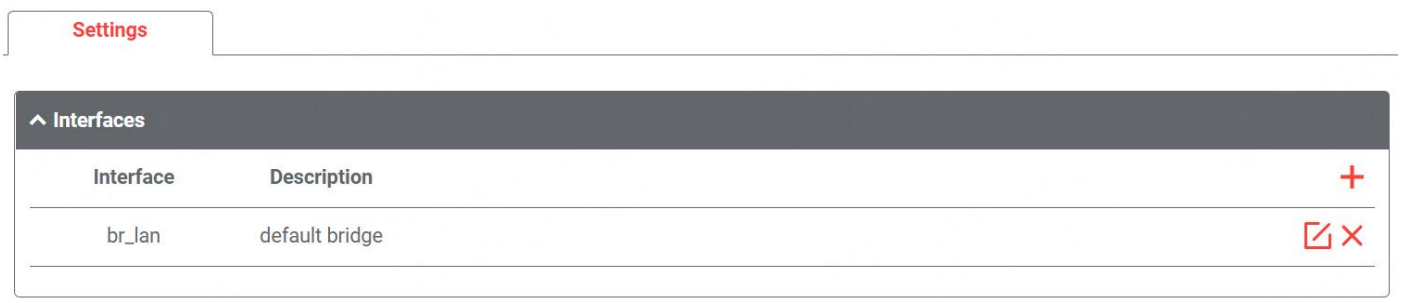
AT Debug

This page allows you to send an AT command for device debugging.



4.2.3 Bridge

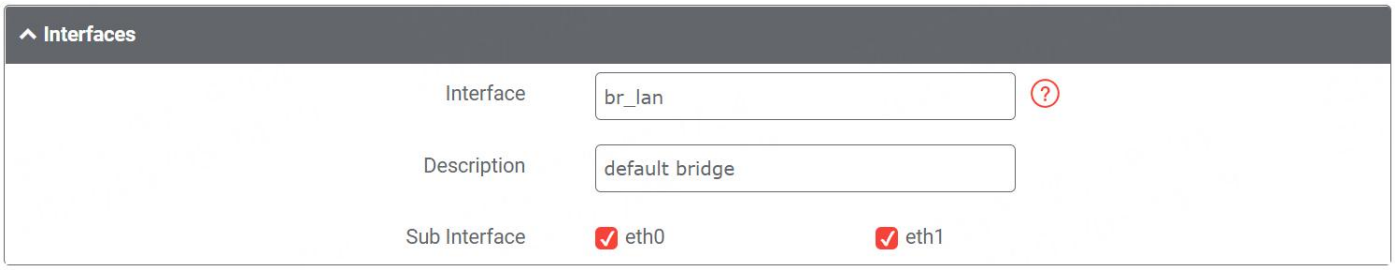
Bridge is used to create a single network consisting of multiple devices. The default bridge(br_lan) interface is always available.



Click + to add a new Bridge. The maximum count is **10.**

Click ✕ to delete the Bridge.

Click to configure the Bridge's parameters in the pop-up window.

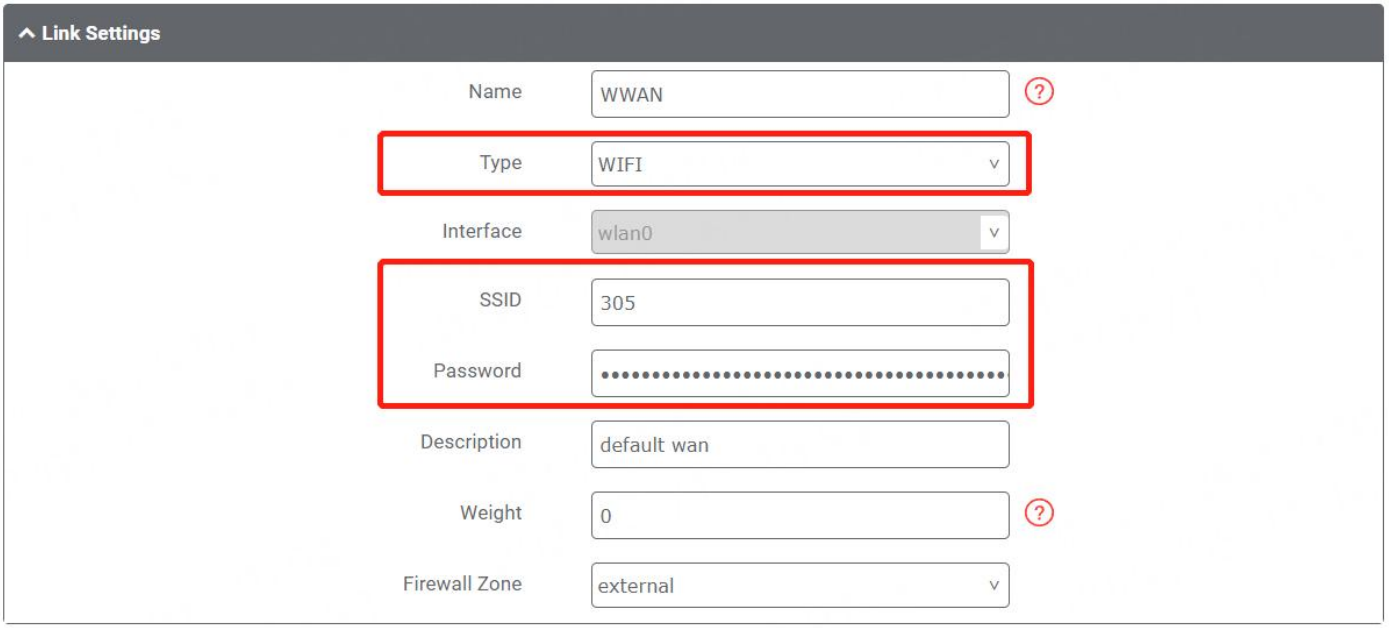


Item	Description
Interface	The interface of Bridge.
Description	The description of the Bridge.
Sub Interface	Select and enable the related Ethernet port.

4.2.4 Wi-Fi

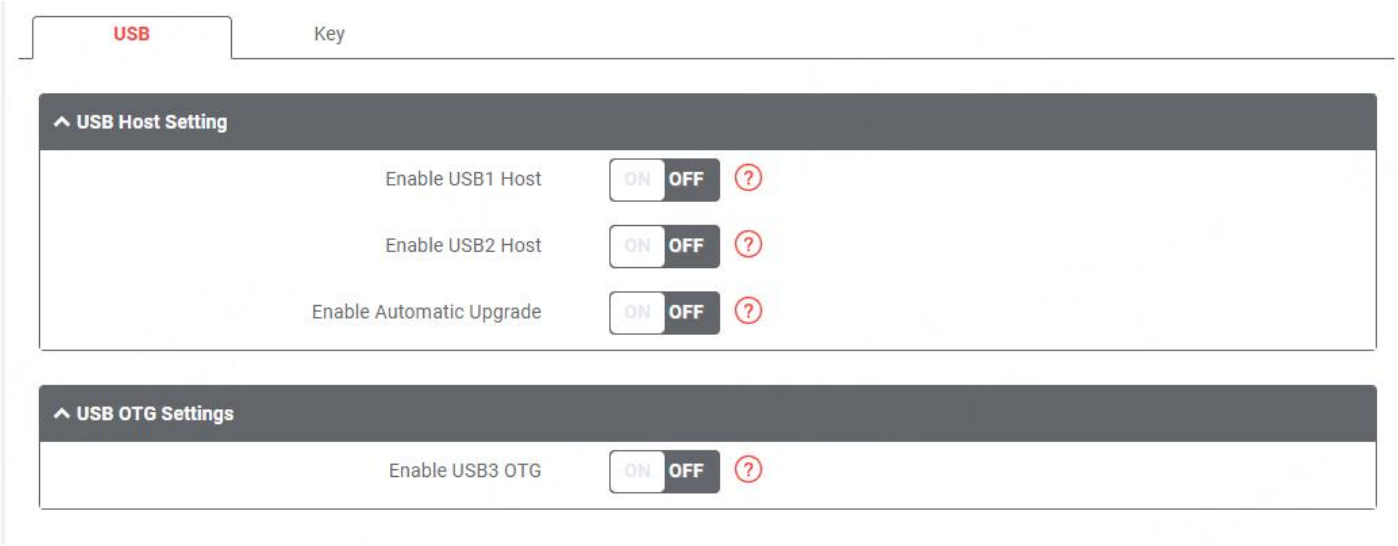
This router cannot support WiFi AP mode, User can configure the device as Wi-Fi client by following steps.

Click **"Network> WAN>Link> Setting"**, click + to add a new WAN link, then configure the related parameters.



4.2.5 USB

This section allows you to configure the USB parameters. The router has two USB Host type A and one USB OTG type C ports available, the router's USB interface can be used to upgrade firmware and upgrade configuration. The users can disable all the USB ports for safety if needed.



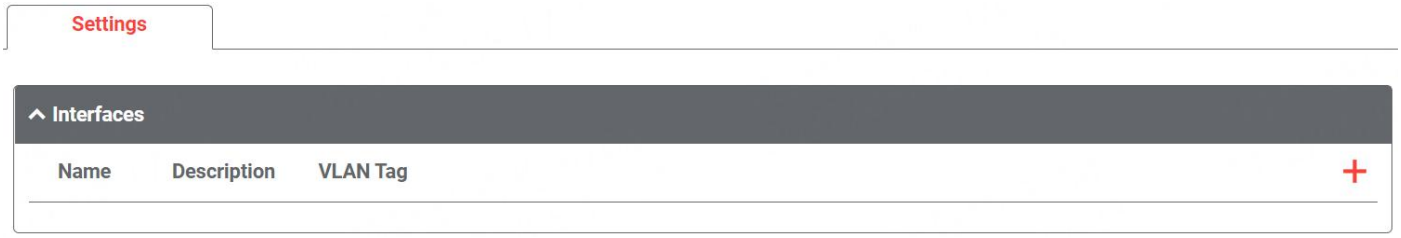
Item	Description	Default
Enable USB1 Host	Click the toggle button to enable/disable the USB1 Host option.	OFF
Enable USB2 Host	Click the toggle button to enable/disable the USB2 Host option.	OFF
Enable Automatic Upgrade	Click the toggle button to enable/disable this option. Enable to automatically update the firmware of the router when inserting a USB storage device with a router firmware.	OFF
Enable USB3 OTG	Click the toggle button to enable/disable the USB3 OTG option, to access to the microSD embedded.	OFF

Item	Description	Default
USB Automatic Upgrade Key	Click Generate to generate and click Download to download the key.	--

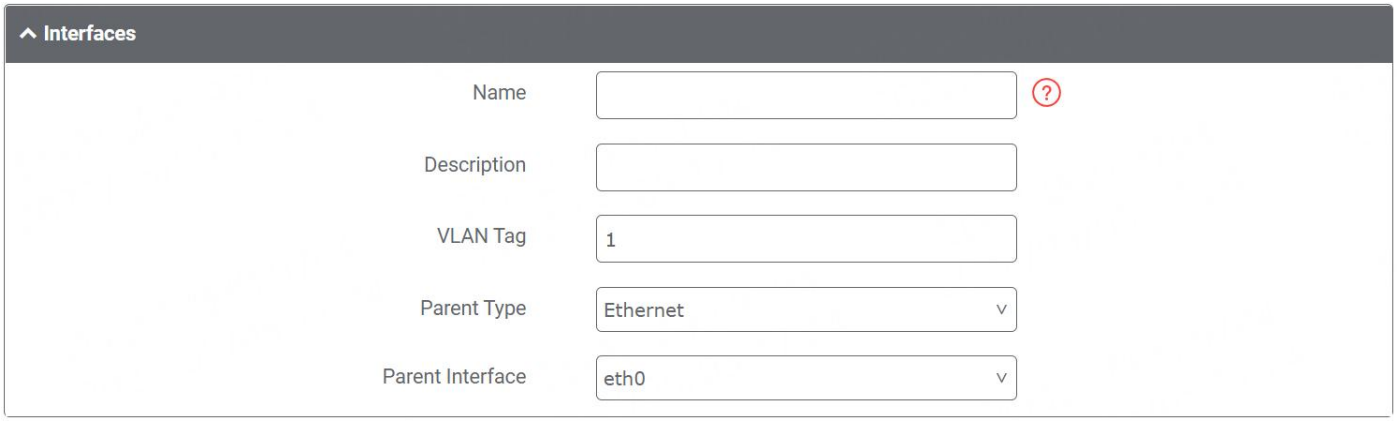
Note: when using the USB automatic upgrade function, the LEDs start blinking one by one, it means that the upgrade is in progress. When LEDs stop blinking one by one, and the USR Indicators is on, it means that the upgrade is completed. After upgrading, the device will not restart automatically. If there is no LEDs start blinking one by one all the time, it means there is an exception, and it does not enter into the automatic upgrade process.

4.2.6 VLAN

VLAN stands for Virtual LAN, allows splitting a single physical LAN into separate Virtual LANs, to reduce broadcast traffic on the LAN.



Click + to add a new Interface. The maximum count is **10.**



Item	Description	Default
Name	The name of VLAN.	Null
Description	Enter a description for this VLAN.	Null
VLAN Tag	Enter a tag for this VLAN.	1
Parent Type	Select from “Ethernet” or “Bridge”.	Ethernet
Parent Interface	Select the related parent interface.	eth0

4.2.7 DI/DO

This section allows you to set the DI/Relay output parameters.

DIDO

DIDO | Status

DIDO Settings

Index	PHY Mode	Enable
1	DI	false
2	DI	false
3	Relay	false
4	Relay	false

Click to configure the parameters in the pop-up window.

DI

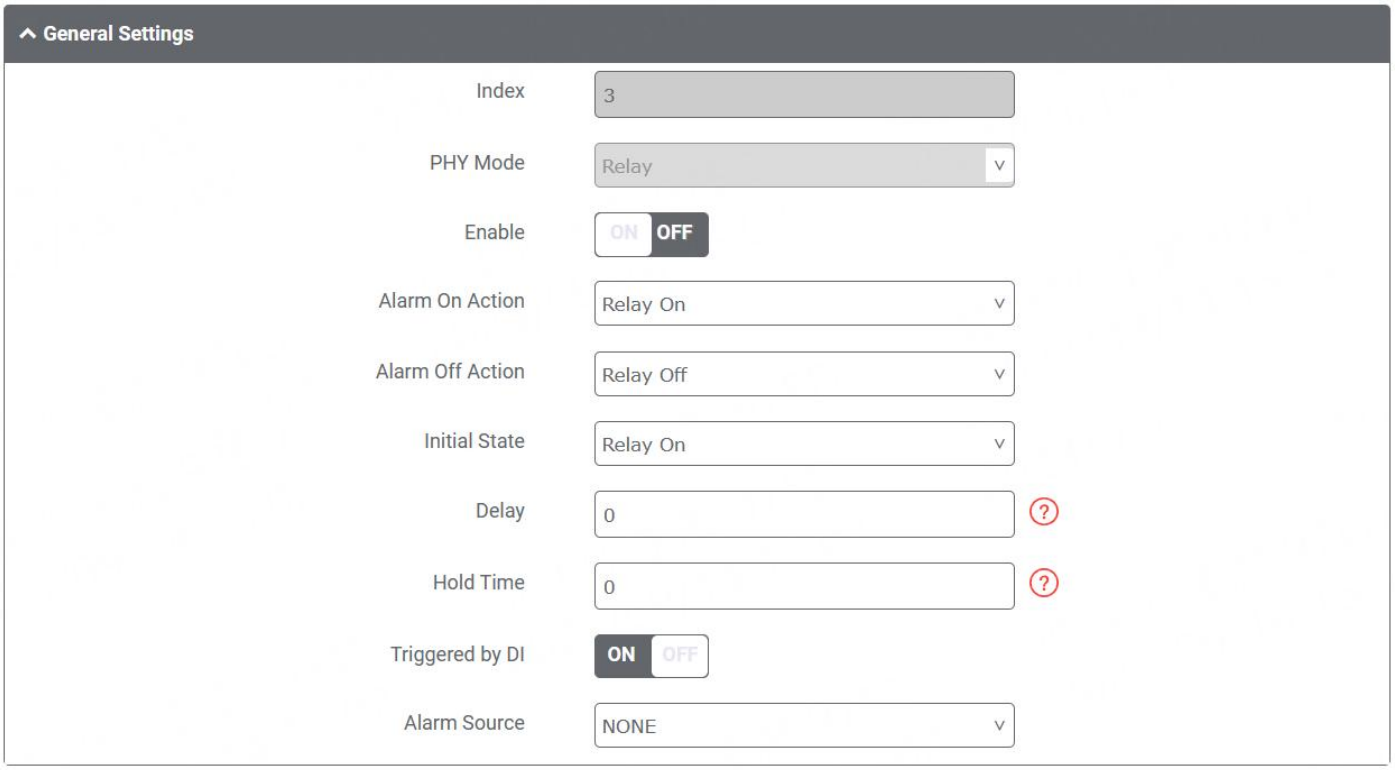
General Settings

Index	1
PHY Mode	DI
Enable	ON / OFF
Mode	Counter
Inversion	ON / OFF
Threshold Value	0
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off

Item	Description	Default
Index	Indicate the ordinal of the list.	--
PHY Mode	DI, fixed, read only.	--
Enable	Click the toggle button to enable/disable the digital input function.	OFF
Mode	Select from “ON-OFF” or “Counter”. • ON-OFF: Alarm mode can be triggered at the DI access ON-OFF. • Counter: Event counter mode	Counter
Inversion	The count is divided into a rising edge count of the level or a falling edge count. If the current rising edge count, the reverse edge is the falling edge count.	OFF
Threshold Value	The threshold value is a unique parameter when the mode is **Count**. Set the threshold value to trigger the DI alarm when the count value reaches the threshold value.	0
Alarm On Content	Show the content when alarm on.	Alarm On
Alarm Off Content	Show the content when alarm off.	Alarm Off

Note: It defaults as high alarm, while turns to low alarm after enabling the “Inversion” button.

Relay Output

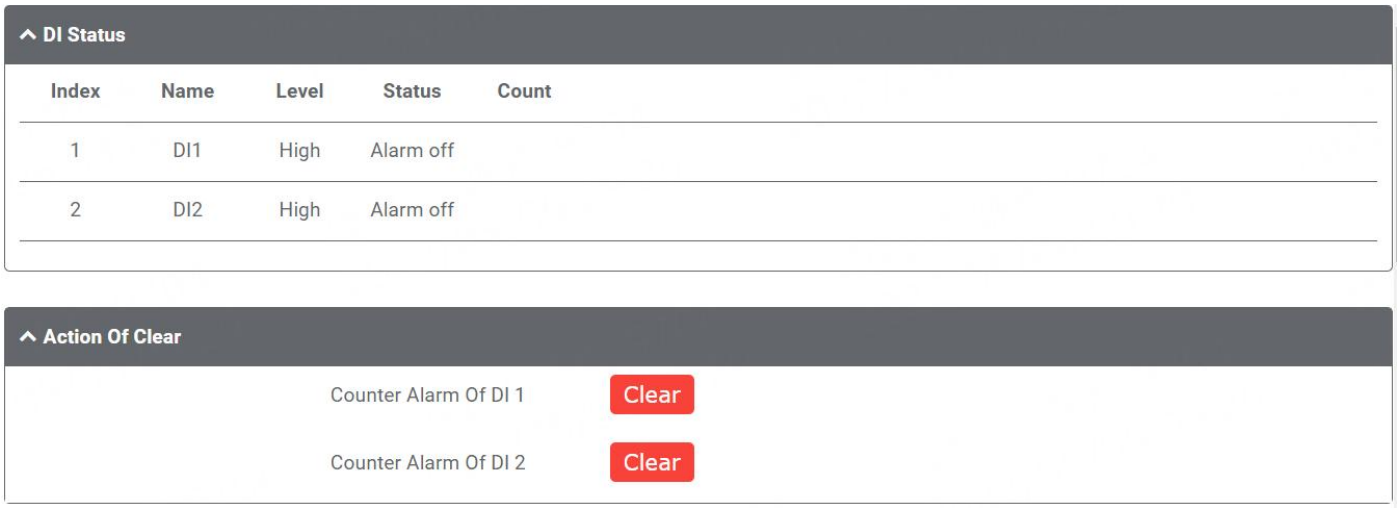


Item	Description	Default
Index	Indicate the ordinal of the list.	--
PHY Mode	Relay only on Relay Output device	Relay
Enable	Click the toggle button to enable/disable this Relay Output.	OFF
Alarm On Action	Relay Output initiates when there is an alarm. Selected from “High”, “Low” or “Pulse”. • Relay On: The relay will connect • Relay Off :The relay will disconnect	Relay On

Item	Description	Default
Alarm Off Action	Relay Output initiates when alarm removed. Selected from “High”, “Low” or “Pulse”. • Relay On: The relay will connect • Relay Off :The relay will disconnect	Relay Off
Initial State	Specify the Relay Output status when powered on. Selected from “Last”, “High” or “Low”. • Relay On: The relay will connect • Relay Off :The relay will disconnect	Relay On
Delay (unit: 100ms)	Set the delay time for DO alarm start-up. The first pulse will be generated after a “Delay”. Enter from 0 to 3000 (0=generate pulse without delay).	0
Hold Time (unit: s)	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reach this specified time, DO will stop the action. Enter from 0 to 3000 seconds. (0=keep on until the next action)	0
Triggered by DI	Click the toggle button to enable/disable the relay output triggered by digital input.	ON
Alarm Source	Digital output activation can be activated by this alarm.	None

Status

This window allows you to view the status of DI/DO interface. It can also clear the counter alarm of DI in here. Click the Clear button to clear DI 1 or DI 2 monthly usage statistics info for counter alarm. Click the Toggle button to switch the electrical level output.



DO Status

Index	Name	Relay Action	Level	Low-level Width	High-level Width
1	Relay1	Off	Low		
2	Relay2	Off	Low		

DO Control

Level Of Relay1	Toggle
Level Of Relay2	Toggle

4.2.8 Serial Port

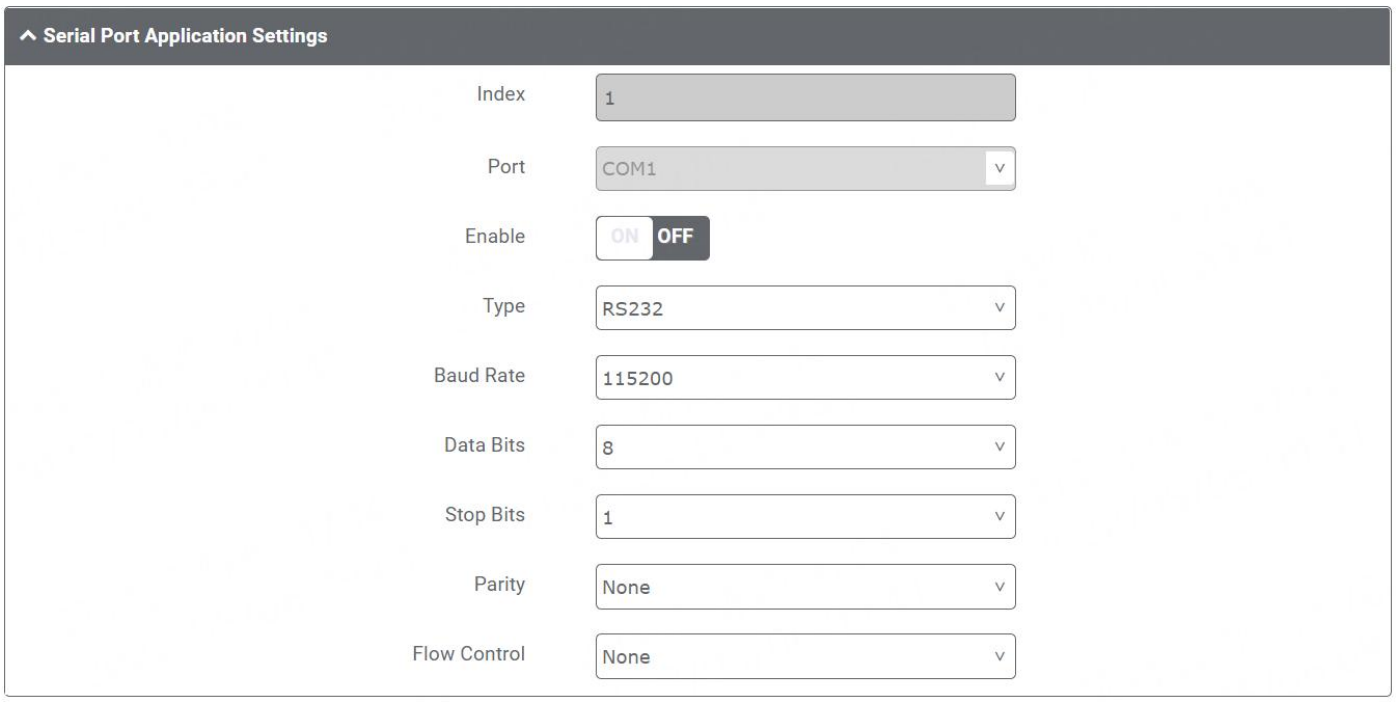
This section allows you to set the serial port parameters. The device supports two serial ports, which might be configured as RS232 or RS422 or RS485 according to requirements . The serial data can be converted into IP data or through IP data into serial data, and then the data can be transmitted through wired or wireless network, so as to realize the function of transparent data transmission.

Serial Port

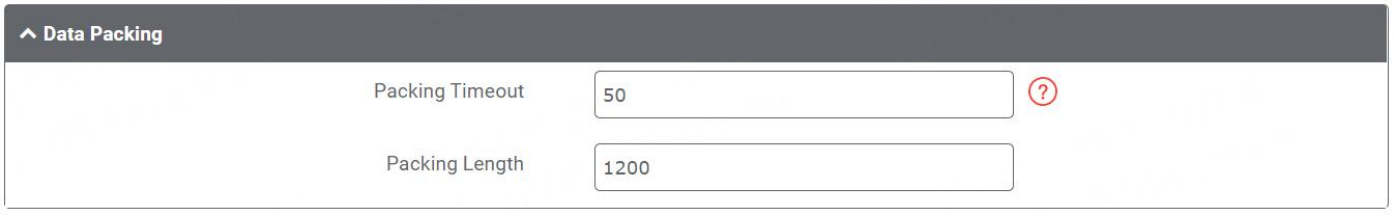
Serial Port Settings

Index	Port	Enable	Type	Baud Rate	Application Mode	
1	COM1	false	RS232	115200	Transparent	
2	COM2	false	RS232	115200	Transparent	

Click to configure the parameters in the pop-up window.



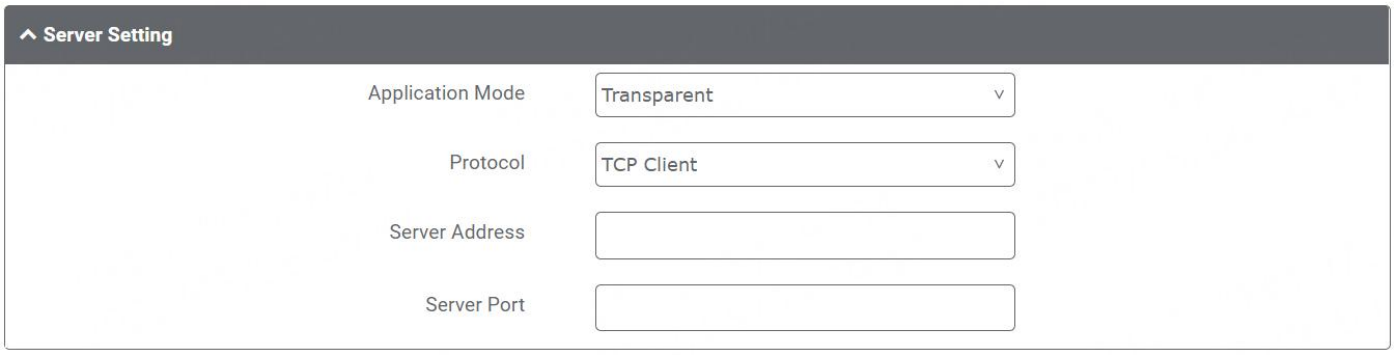
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Port	Show the current serial's name, read only.	COM1
Type	Select from "RS232", "RS422" "RS485".	--
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" or "115200".	115200
Data Bits	Select from "7" or "8".	8
Stop Bits	Select from "1" or "2".	1
Parity	Select from "None", "Odd" or "Even".	None
Flow control	Select from "None", "Software" or "Hardware".	None



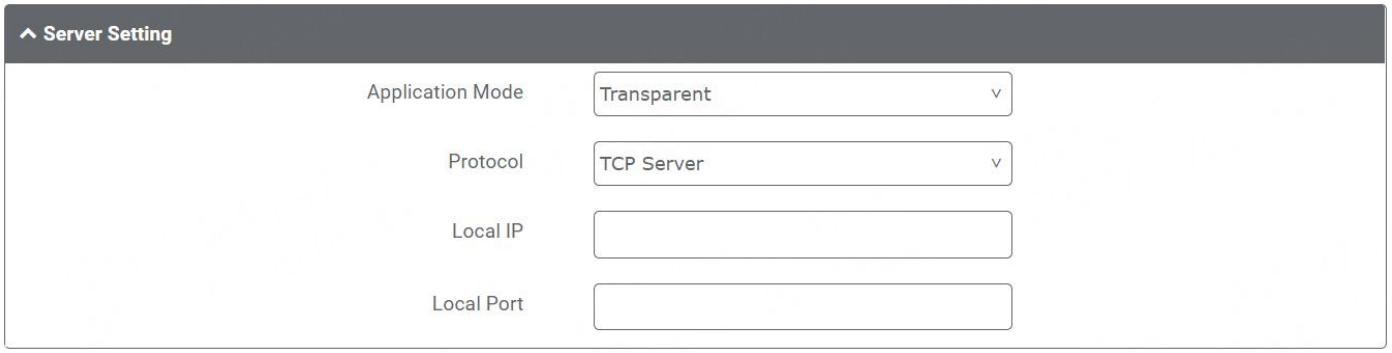
Item	Description	Default
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. The unit is milliseconds. **Note**: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	50
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as	1200

Item	Description	Default
	soon it reaches the specified length.	

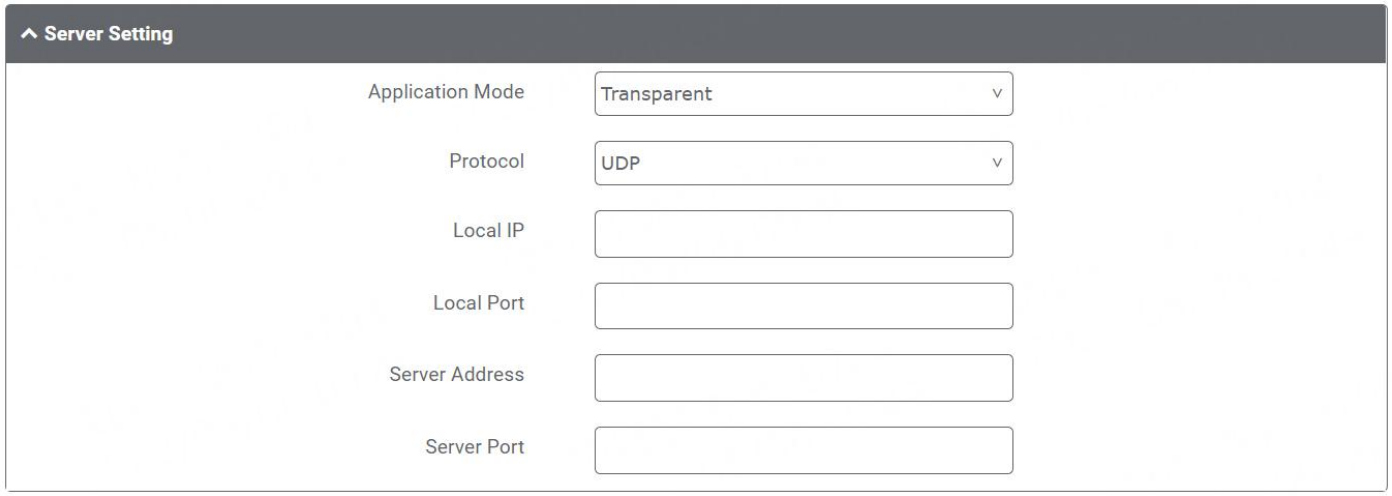
In the "Server Settings" column, when "Transparent" is selected as the application mode and "TCP Client" as the protocol, the window is as follows:



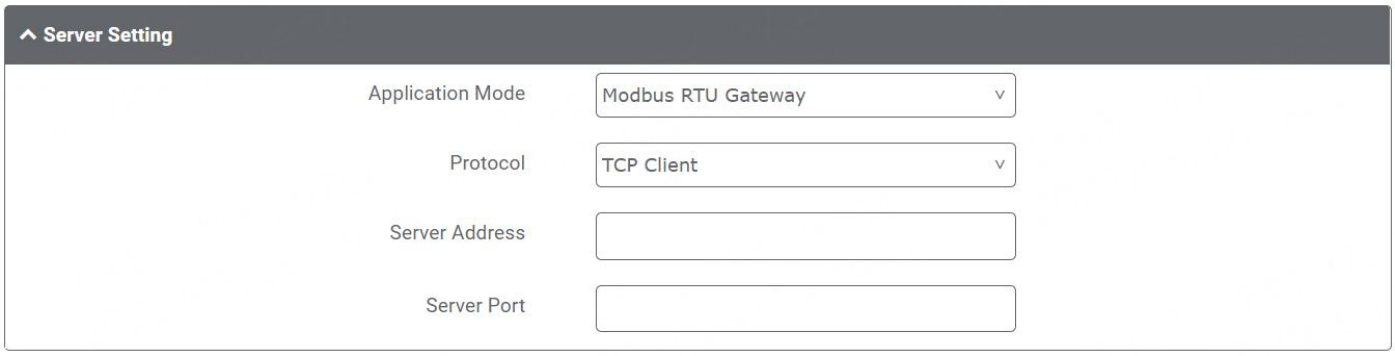
When "Transparent" is selected as the application mode and "TCP Server" as the protocol, the window is as follows:



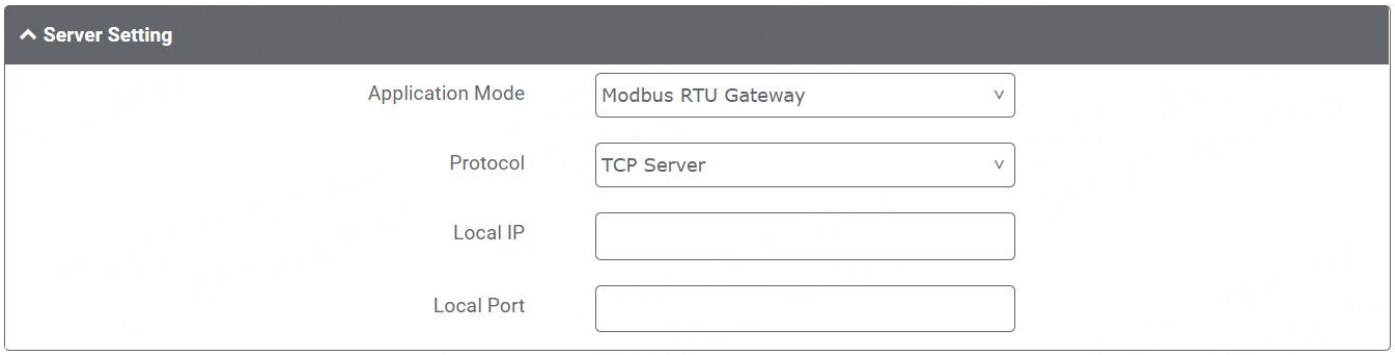
When "Transparent" is selected as the application mode and "UDP" is used as the protocol, the window is as follows:



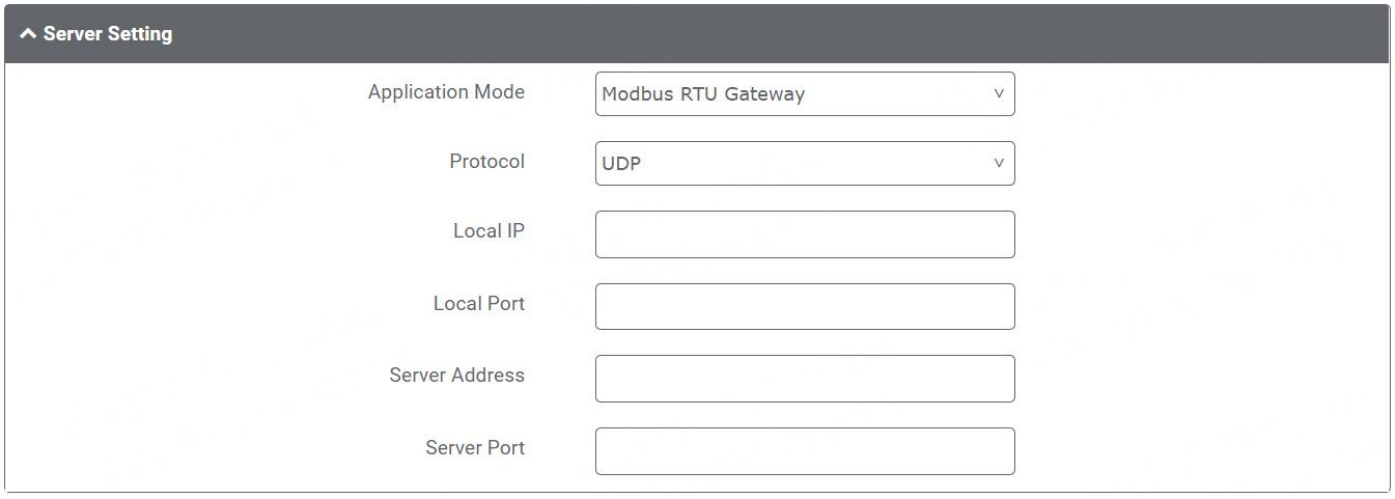
When "Modbus RTU Gateway" is selected as the application mode and "TCP Client" as the protocol, the window is as follows:



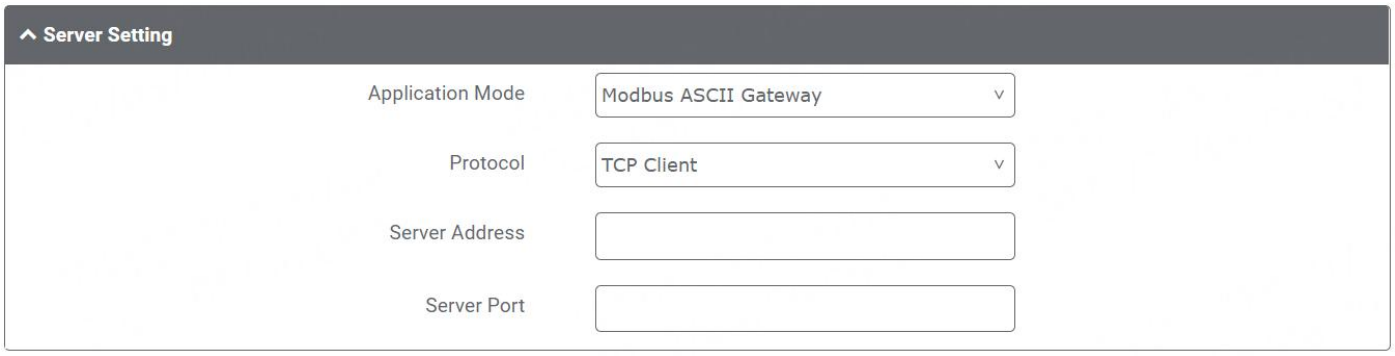
When "Modbus RTU Gateway" is selected as the application mode and "TCP Server" as the protocol, the window is as follows:



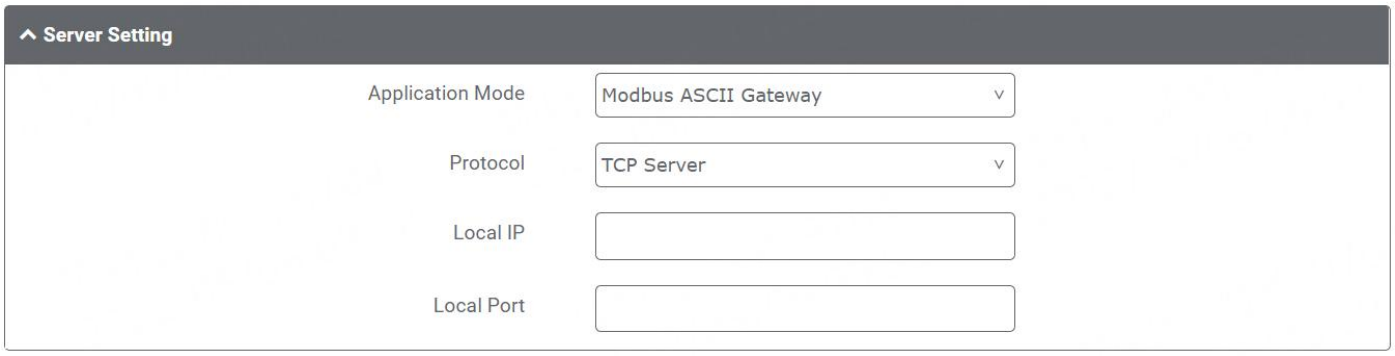
When selecting "Modbus RTU Gateway" as the application mode and "UDP" as the protocol, the window is as follows:



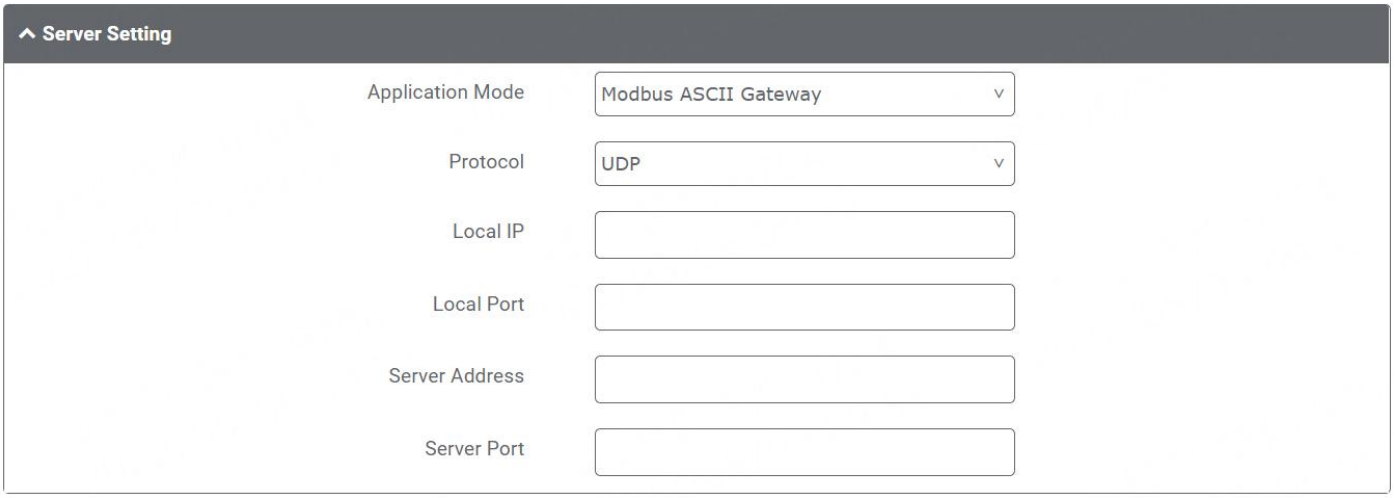
When “Modbus ASCII Gateway” is selected as the application mode and “TCP Client” as the protocol, the window is as follows:


Server Setting
Application Mode
Modbus ASCII Gateway
Protocol
TCP Client
Server Address
Server Port

When selecting "Modbus ASCII Gateway" as the application mode and "TCP Server" as the protocol, the window is as follows:



When selecting "Modbus ASCII Gateway" as the application mode and "UDP" as the protocol, the window is as follows:

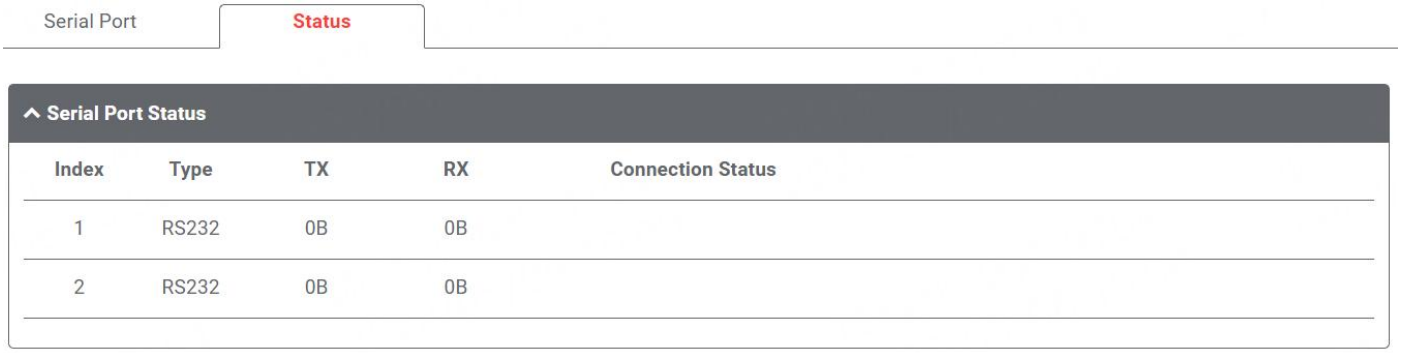


Item	Description	Default
Application Mode	Select from “Transparent”, “Modbus RTU Gateway” or “Modbus ASCII Gateway”. • Transparent: Device will transmit the serial data transparently • Modbus RTU Gateway: Device will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa • Modbus ASCII Gateway: Device will translate the Modbus ASCII data to Modbus TCP data and sent out, and vice versa	Transparent
Protocol	Select from “TCP Client”, “TCP Server”, or “UDP”. • TCP Client: Device works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name • TCP Server: Device works as TCP server, listening for connection request from TCP client • UDP: Device works as UDP client	TCP Client
Server Address	Enter the address of server which will receive the data sent from device’s serial port. IP address or domain name will be available.	Null
Server Port	Enter the specified port of server which is used for receiving the serial data.	Null
Local IP @ Transparent	Enter device’s LAN IP which will forward to the internet port of device.	Null
Local Port @	Enter the port of device’s LAN IP.	Null

Item	Description	Default
Transparent		
Local IP @ Modbus	Enter the local IP of under Modbus mode.	Null
Local Port @ Modbus	Enter the local port of under Modbus mode.	Null

Status

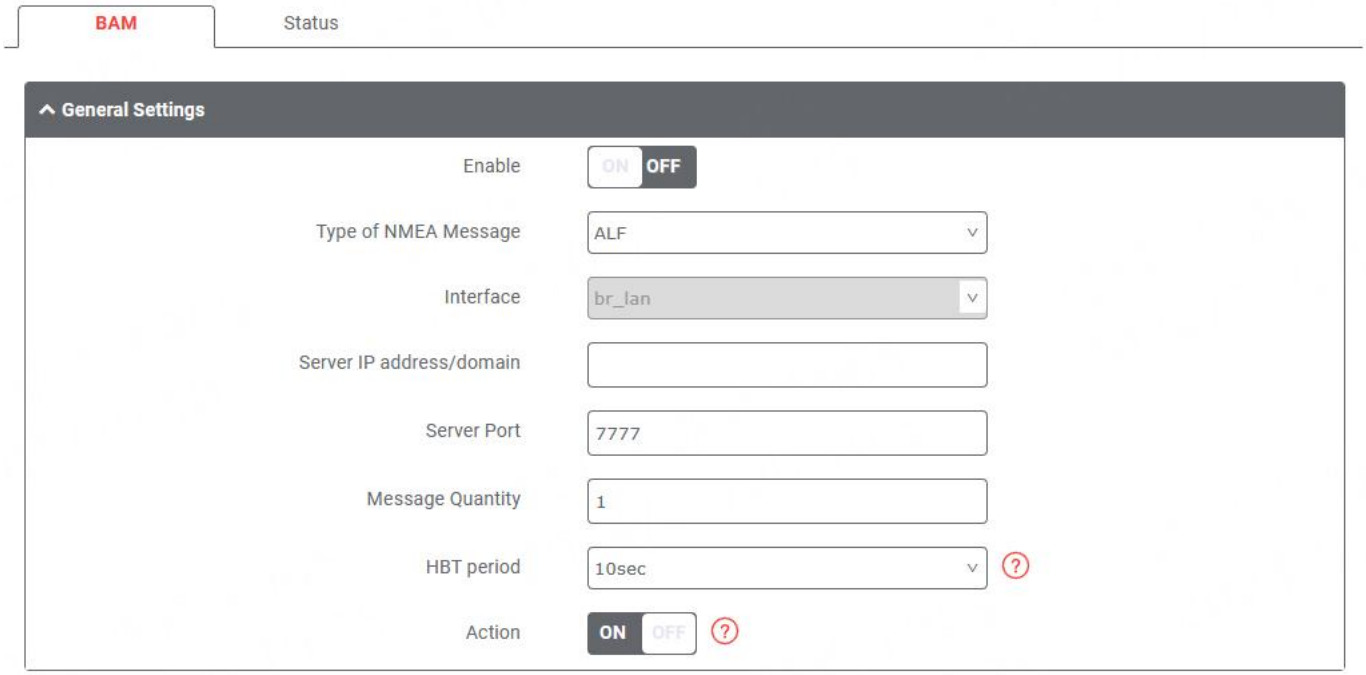
Click the "Status" column to view the current serial port type.



4.2.9 BAM

This section allows you to set the BAM(Bridge Alarm Management) parameters.

BAM



Item	Description	Default
Enable	Click the toggle button to enable or disable the function.	OFF
Type of NMEA Message	Select from “ALF”, “HLT”	Null
Interface	Set the message outgoing interface	br_lan
Server IP address/domain	Set the Server IP address and domain	Null
Server Port	Set the Server port	7777
Message Quantity	Set the message quantity	1
HBT period	Set the heart beat peride	10sec
Action	Click the toggle button to enable or disable the function. ON: Send ALF message when VPN session is connected. OFF: Do not send ALF message.	

Status

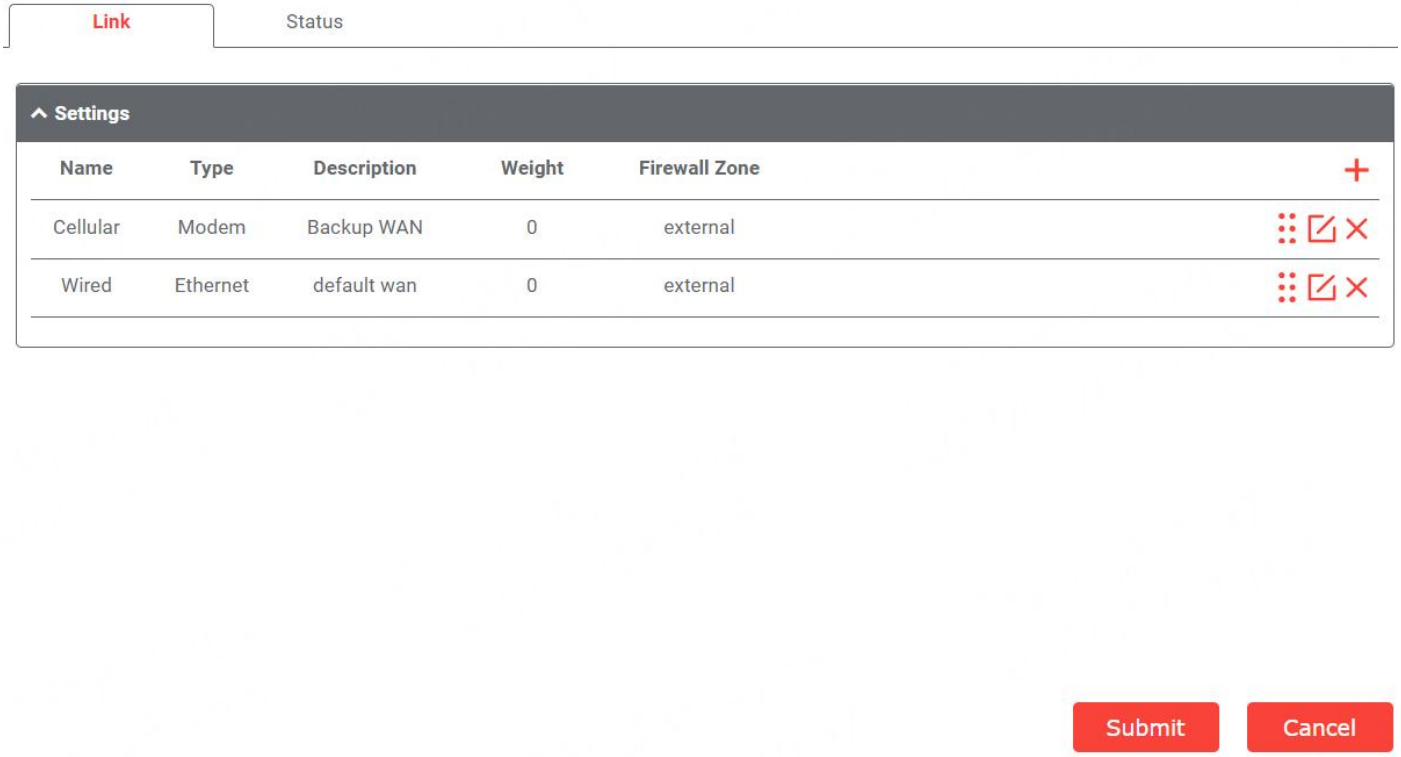
You can view detailed information here.

4.3 Network

4.3.1 WAN

WAN stands for Wide Area Network, provides connectivity to the internet. You can configure WAN based on Ethernet, Cellular modem or Wi-Fi(if supported).

Link



Click + to add a new WAN link.

Click ✕ to delete the link.

Press ⠿ to drag the WAN link into the required order to switch between WAN connections, the topper one has higher priority.

Click ✎ to edit the link.

Users can manage link connections in this section. It provides four types of connectivity interface to internet including Modem, Ethernet, VLAN and Wi-Fi.

Link Settings

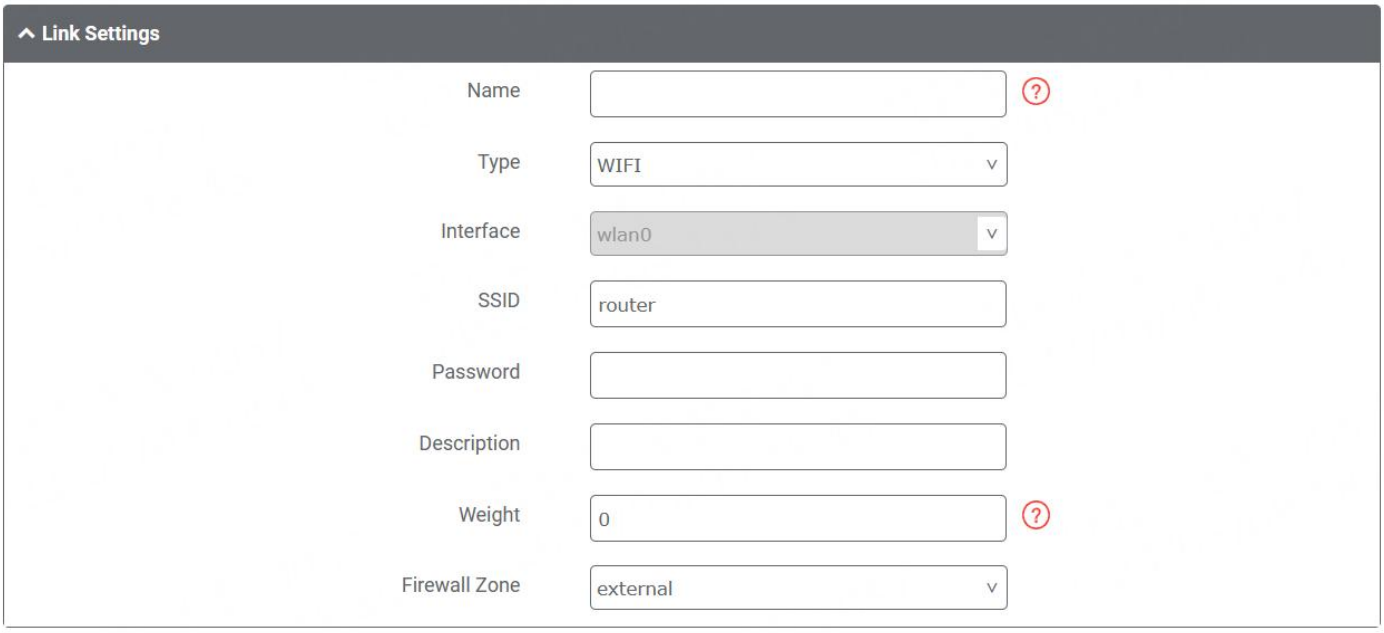
Name	WWAN
Type	Modem
Interface	wwan
Description	default wan
Weight	0
Firewall Zone	external

Link Settings

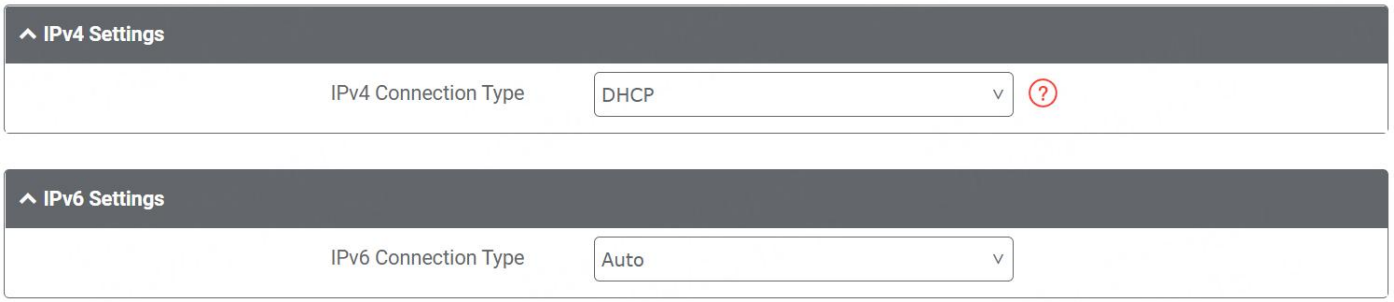
Name	WAN
Type	Ethernet
Interface	eth1
Description	
Weight	0
Firewall Zone	external

Link Settings

Name	
Type	VLAN
Interface	
Description	
Weight	0
Firewall Zone	external

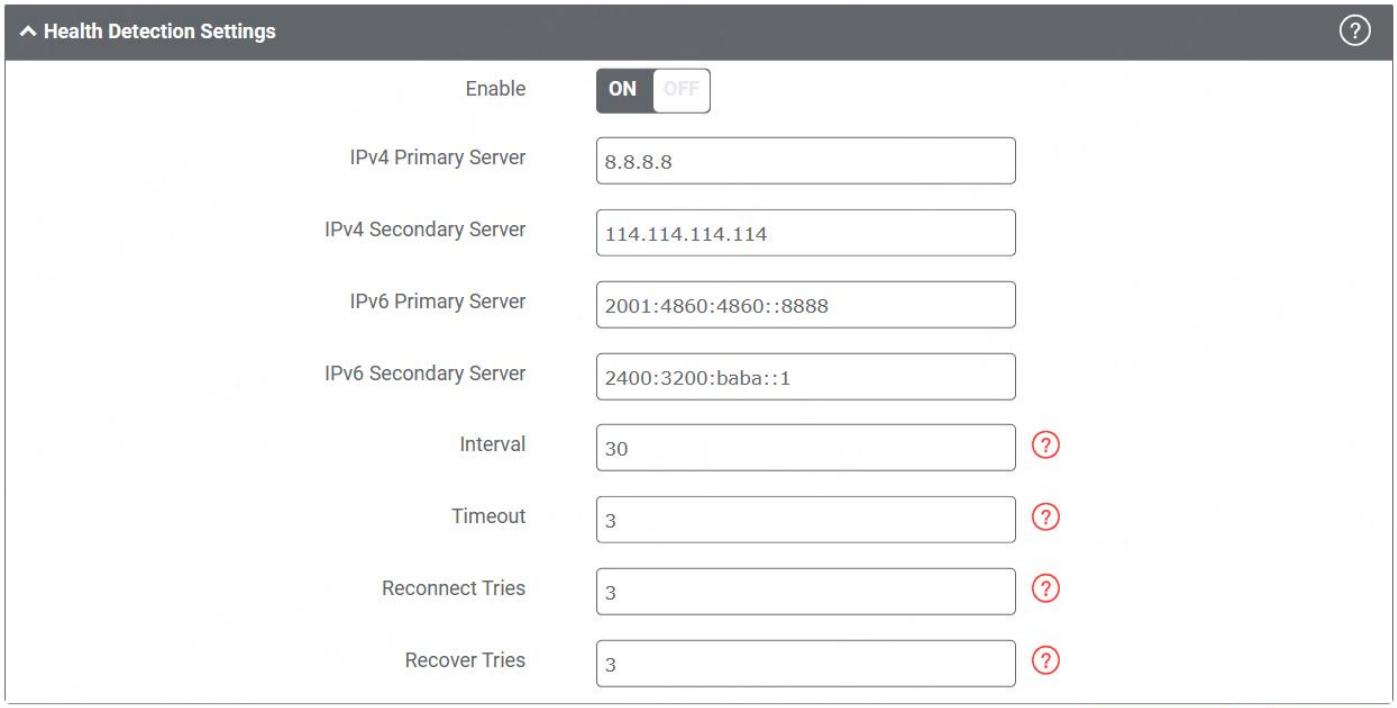


Item	Description	Default
Name	The name of link.	--
Type	The types of connectivity. • Modem: connected by cellular network. • Ethernet: connected by Ethernet wired network. • VLAN: connected by VLAN network. • Wi-Fi: connected by Wi-Fi network.	--
Interface	Set the related interface. If the type is Modem, please see the **4.2.2 Cellular.** If the type is Ethernet, please see the **4.2.1 Ethernet.** If the type is VLAN, please see the 4.2.6 VLAN.	--
Description	The description of the link.	--
SSID	The name of Wi-Fi network.	--
Password	The Password of Wi-Fi network.	--
Weight	The weight of this link among all links. 0 means not involved.	--
Firewall Zone	The chosen set of firewall rules, please see the 4.3.5 Firewall.	--



Item	Description	Default
IPv4 Connection Type	The type of IPv4 connection.	DHCP

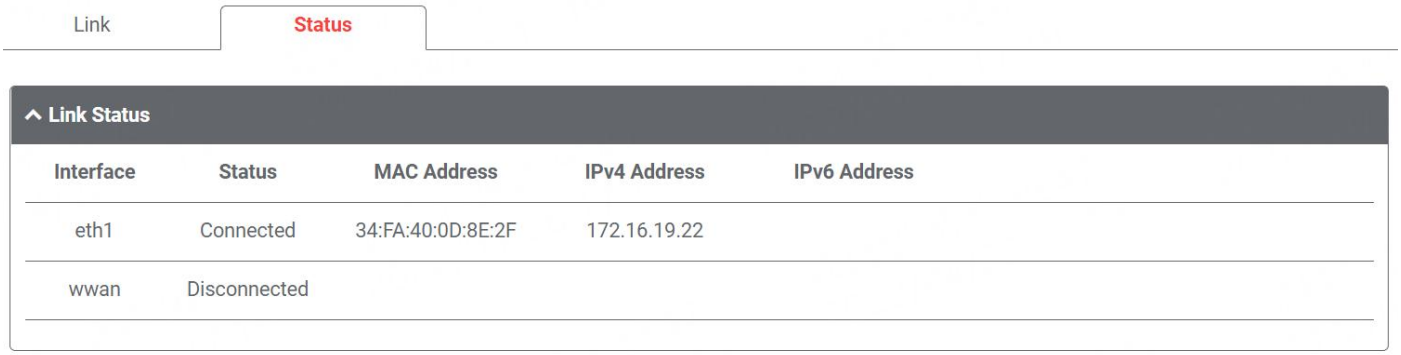
Item	Description	Default
	• DHCP. • PPPoE. • Manual. • Disable. Enter the parameters accordingly. **Note: IPv6 over PPPoE is not supported now, so disabling IPv6 if choosing PPPoE here.*	
IPv6 Connection Type	The type of IPv6 connection. • Auto. • Manual. • Disable. Enter the parameters accordingly.	Auto



Item	Description	Default
Enable	Toggle the button to enable the health detection function	ON
IPv4 Primary Server	IPv4 Primary Server	8.8.8.8
IPv4 Secondary Server	IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	IPv6 Primary Server	2001:4860:4860::8888
IPv6 Secondary Server	IPv6 Secondary Server	2400:3200:baba::1
Interval	Seconds to send next ping	30
Timeout	Seconds to wait for ping response	3
Reconnect Tries	Reconnect this link in case of sequential probes are unsuccessful.	3
Recover Tries	Recovery this link in case of sequential probes are successful.	3

Status

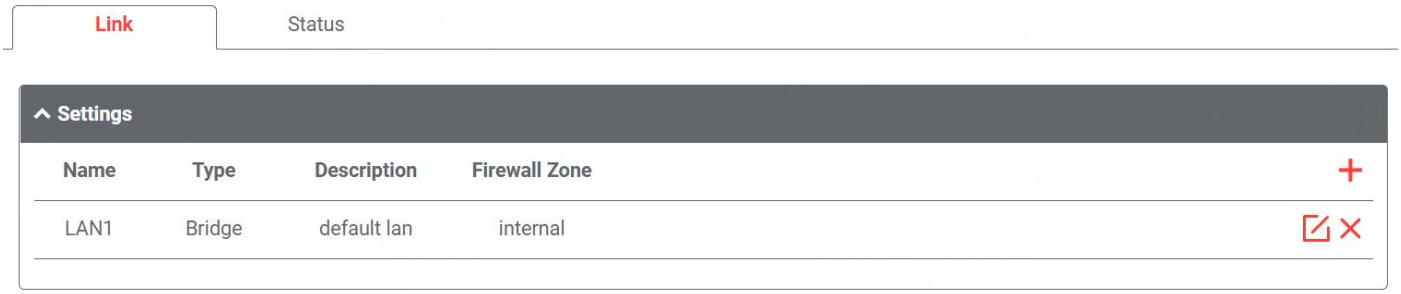
This window allows you to view the link status of device.



4.3.2 LAN

A Local Area Network (LAN) connects network devices together, such as Ethernet or Bridge, in a logical Layer-2 network. The default link(br_lan) is always available.

Link

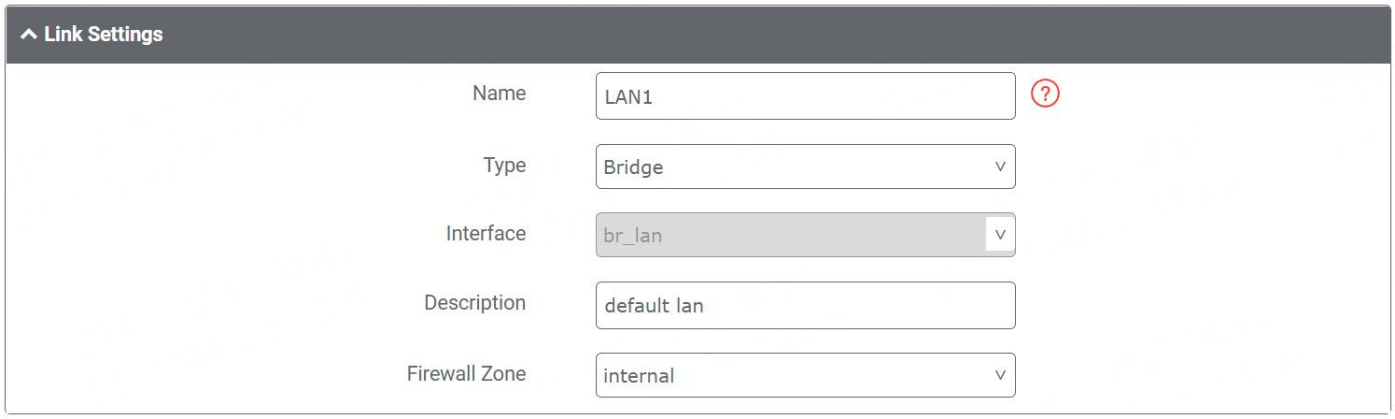


Click + to add a new LAN link.

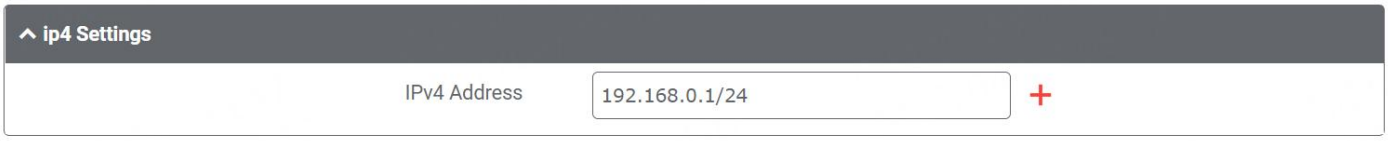
Click ✕ to delete the LAN link.

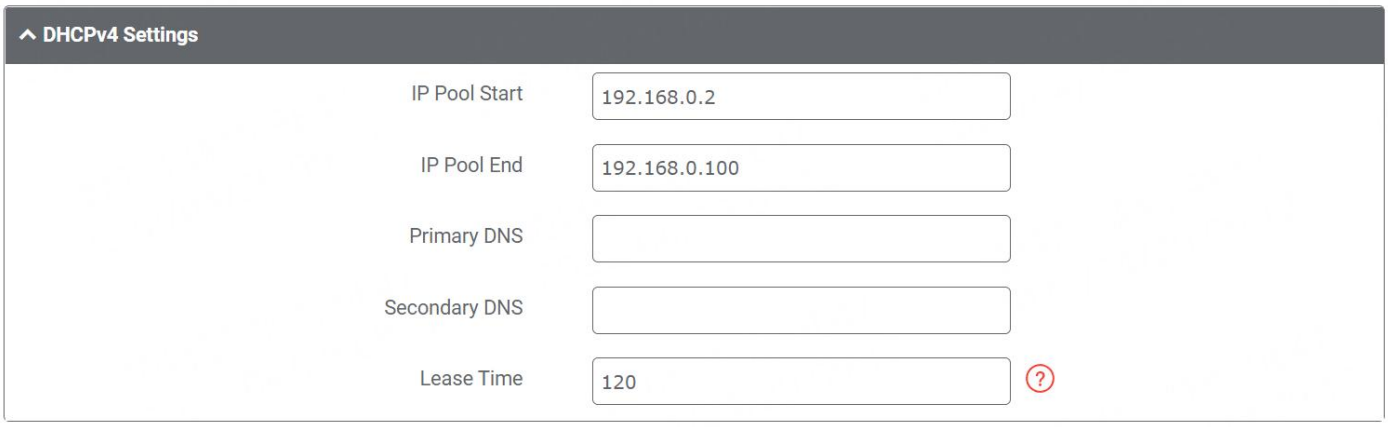
Click to edit the LAN link.

Users can manage link connections in this section. It provides three types of connectivity interface to internet including Bridge, Ethernet and VLAN.



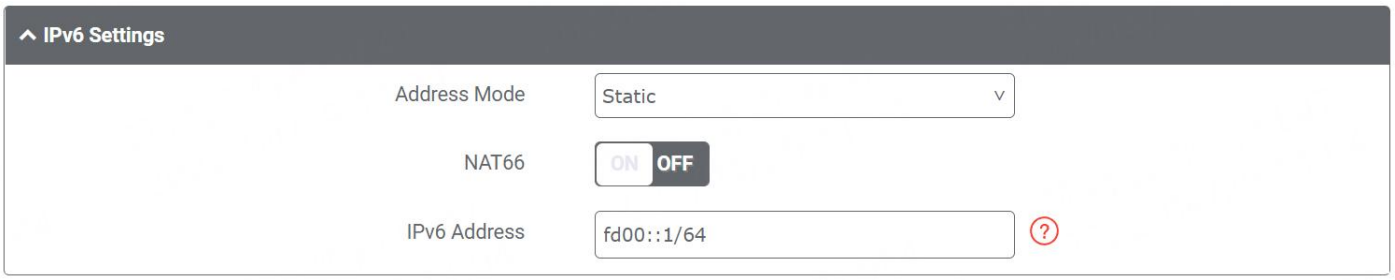
Item	Description	Default
Name	The name of the LAN link.	--
Type	The types of connectivity. Select from “Bridge”, “Ethernet” and “VLAN”. • Bridge: connected by Bridge network. • Ethernet: connected by Ethernet wired network. • VLAN: connected by VLAN network.	Bridge
Interface	Set the related interface. If the type is Bridge, please see the 4.2.3 Bridge. If the type is Ethernet, please see the **4.2.1 Ethernet.** If the type is VLAN, please see the 4.2.6 VLAN.	--
Description	The description of the link.	--
Firewall Zone	The chosen set of firewall rules, please see the 4.3.5 Firewall.	internal





Item	Description	Default
IPv4 Address	Enter the IPv4 address with netmask.	192.168.0.1/24
IP Pool Start	The start IP address in pool.	192.168.0.2
IP Pool End	The end IP address in pool.	192.168.0.100
Primary DNS	Enter the primary DNS.	Null

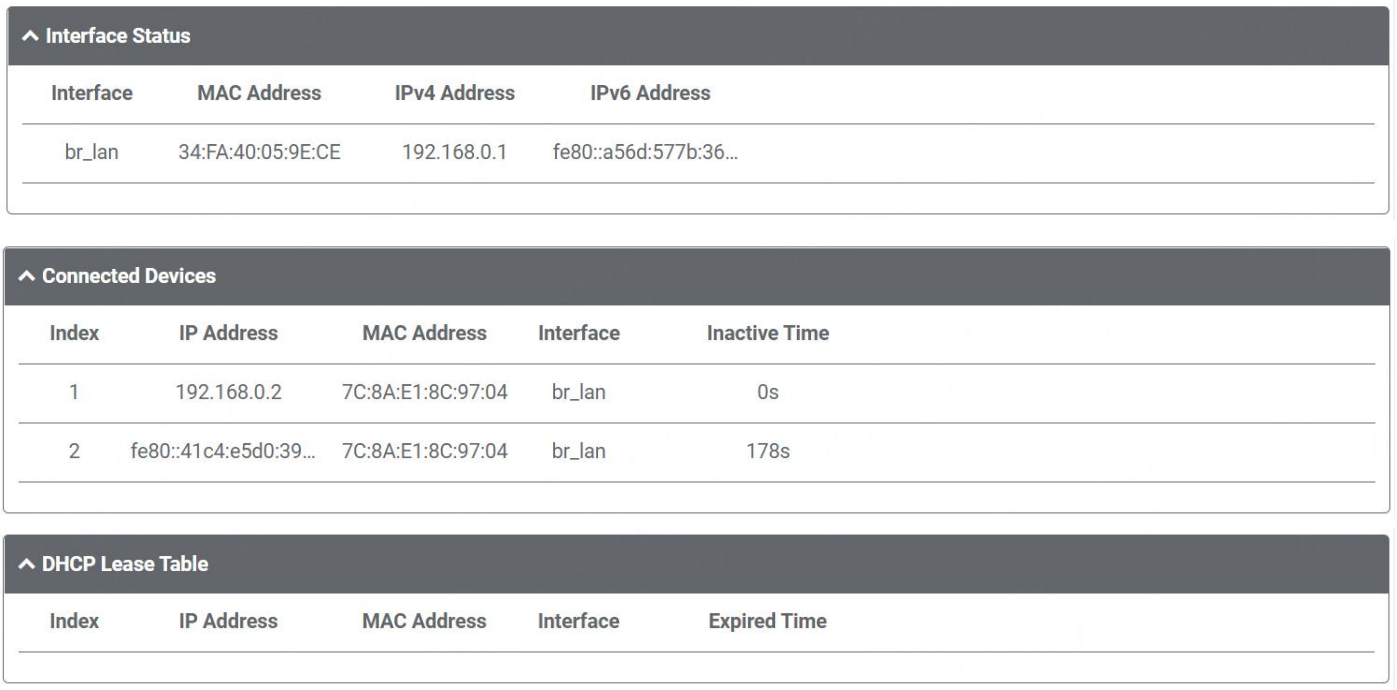
Item	Description	Default
Secondary DNS	Enter the secondary DNS.	Null
Lease Time	The lease time in minute.	120



Item	Description	Default
Address Mode	Delegated or Static.	Delegated
NAT66	IPv6-to-IPv6 Network Address Translation. On or Off in static mode.	OFF
IPv6 Address	Enter the IPv6 address with 64-bit network prefix in static mode.	fd00::1/64

Status

This window allows you to view the status of LAN link.

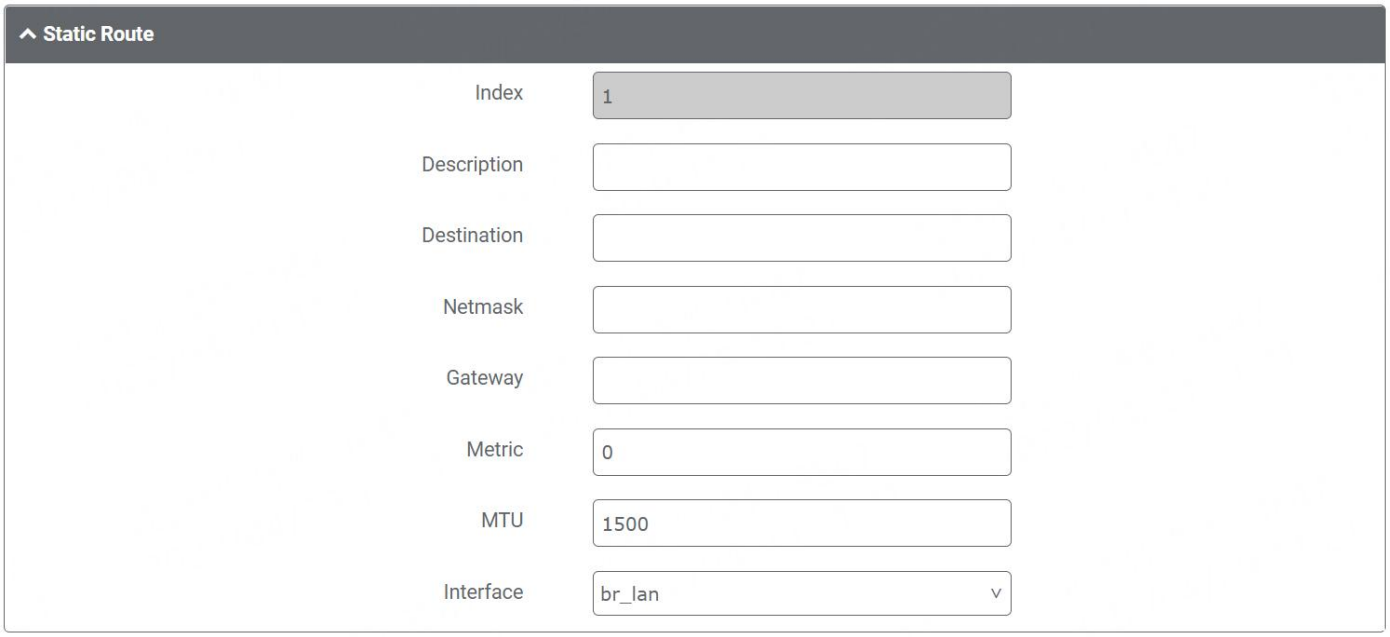


4.3.3 Route

Routes ensure that network traffic finds its path to a destination network. Static routes are fixed routing entries in routing table.

Static Route

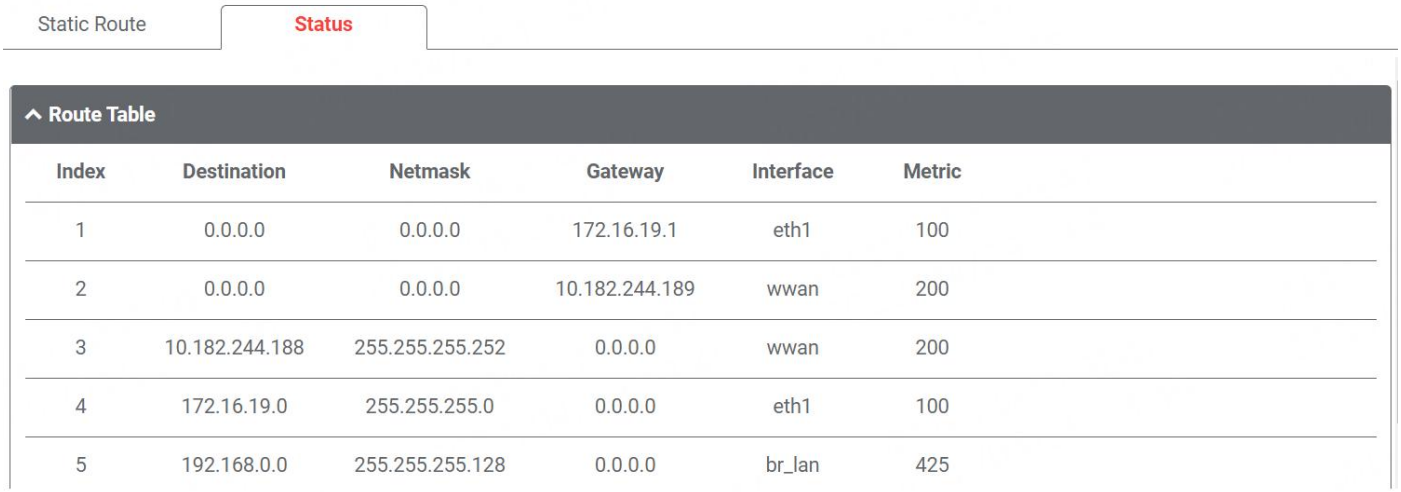
Click + to add static routes. The maximum count is 20.



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this static route.	Null
Destination	Enter the IP address of destination host or destination network.	Null
Netmask	Enter the Netmask of destination host or destination network.	Null
Gateway	Define the gateway of the destination.	Null
Metric	Enter the Metric value. Metrics help the gateway choose the best route among multiple feasible routes to a destination. The route will go in the direction of the gateway with the lowest metric value.	0
MTU	Enter the MTU value, 1280~1500.	1500
Interface	Choose the corresponding port of the link that you want to configure.	br_lan

Status

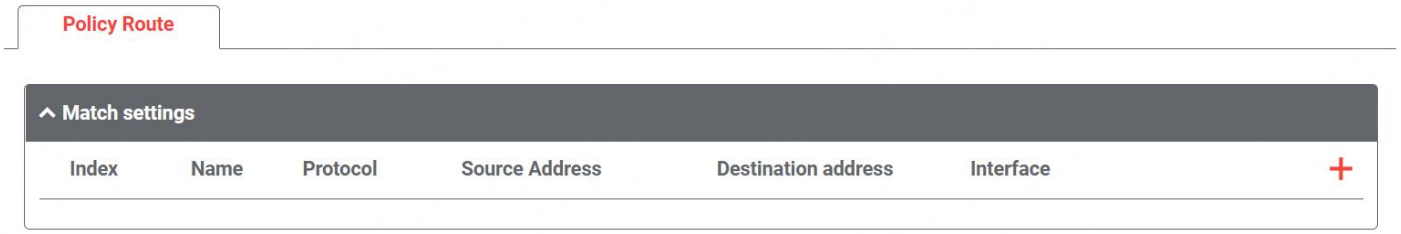
This window allows you to view the status of route.



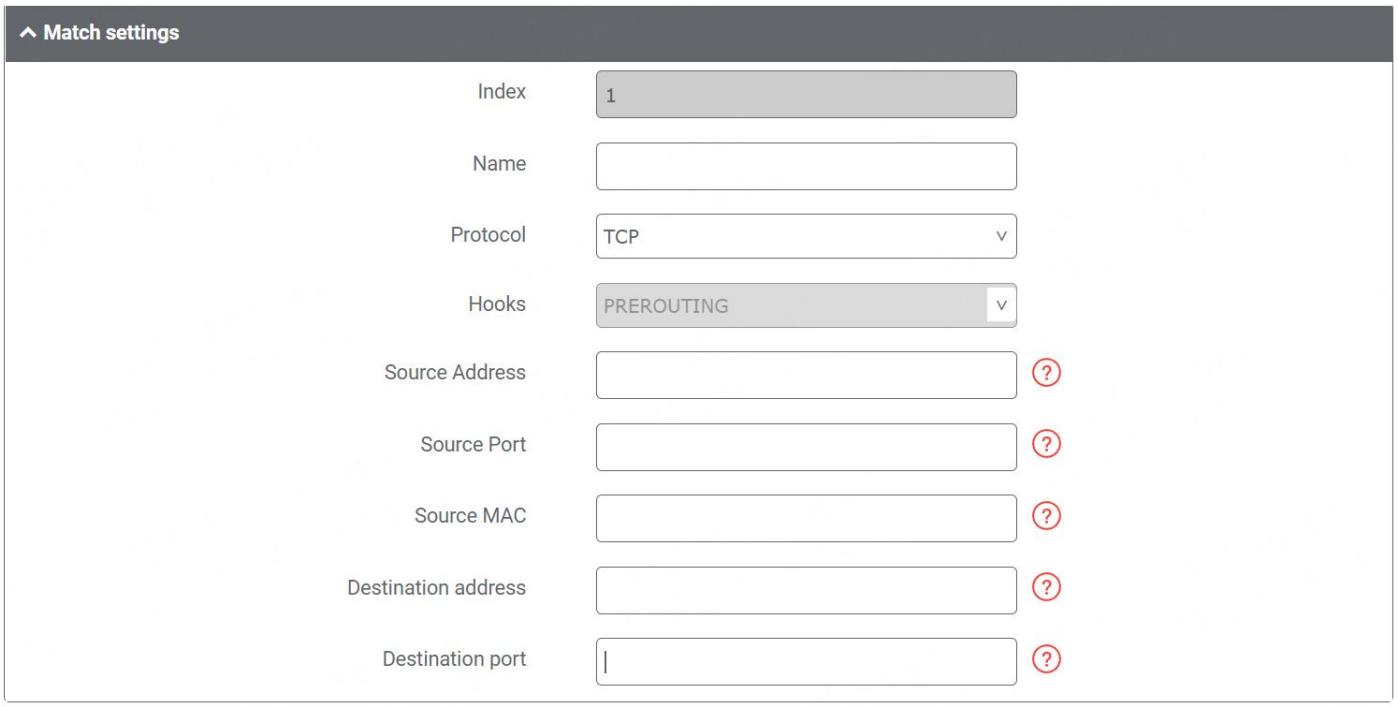
4.3.4 Policy Route

In this window, you can manage the outbound route based on the IP address, port number in the packet.

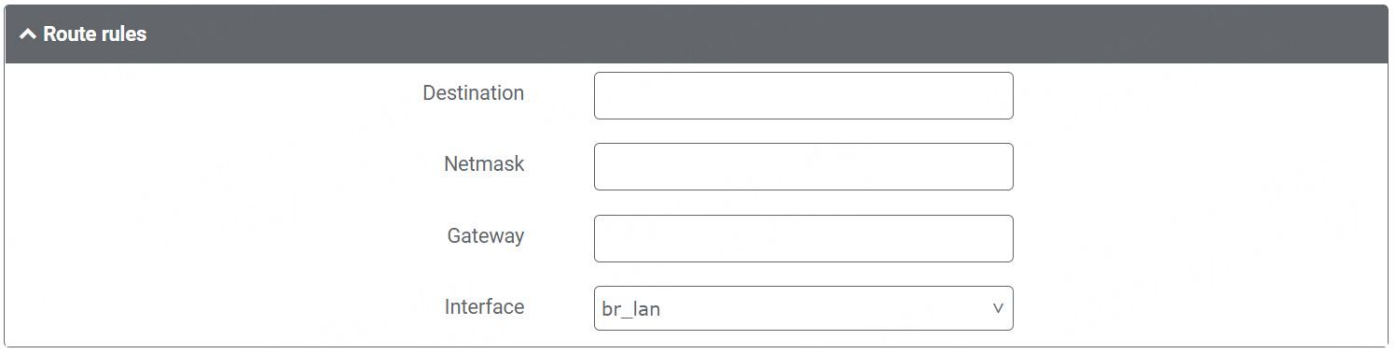
Policy Route



Click + to add a policy route. The maximum count is **20.**



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	Name of Policy Route.	--
Protocol	The type of network protocol. Select from “Any”, “TCP”,”UDP”,”TCP-UDP”,”ICMP” and “IGMP”.	TCP-UDP
Hooks	Fixed setting.	--
Sources Address	Enter the source IP address.	--
Source Port	Enter the source port in TCP/UDP type.	--
Source MAC	Enter the source mac address.	--
Destination Address	Enter the destination IP address.	--
Destination Port	Enter the destination port in TCP/UDP type.	--

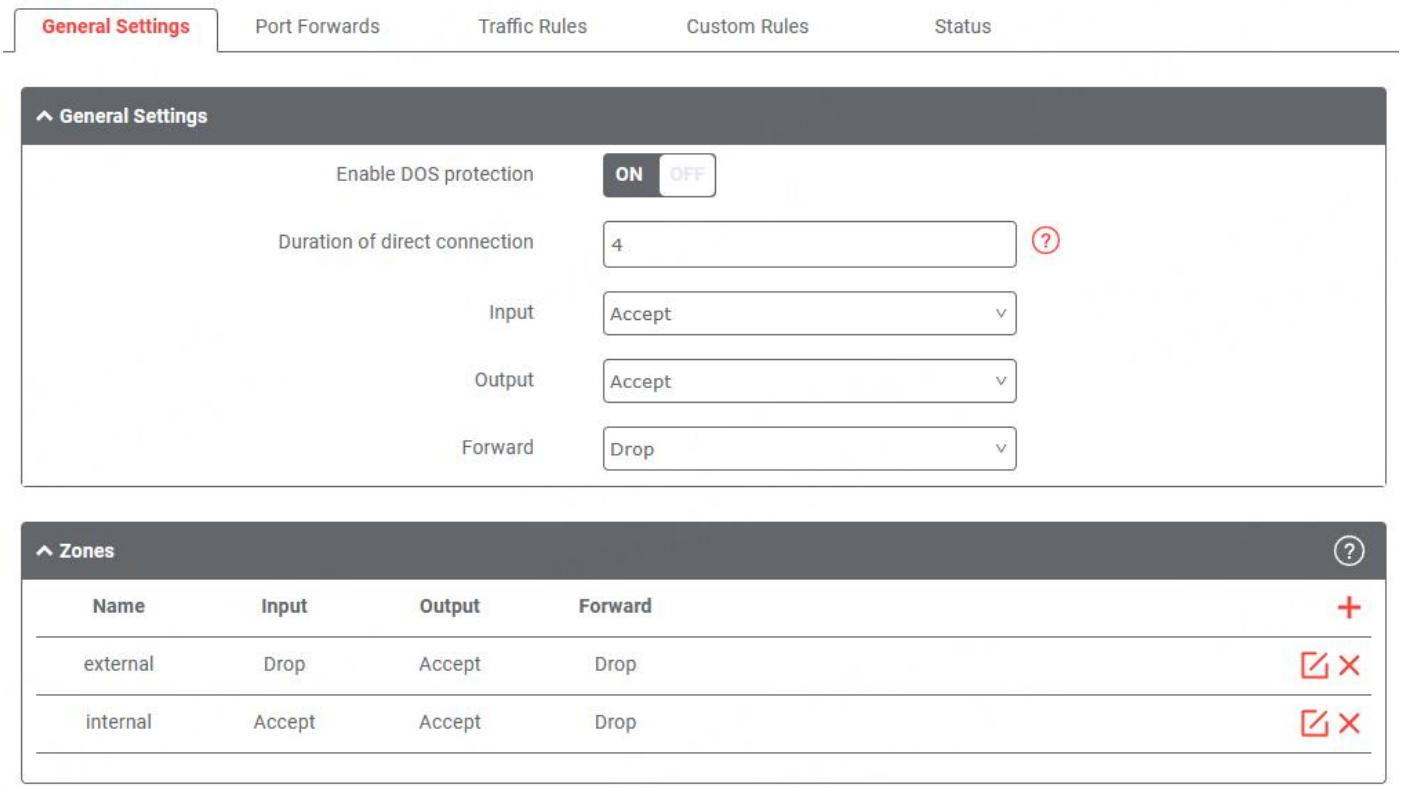


Item	Description	Default
Destination	Enter the IP address of destination host or destination network.	--
Netmask	Enter the Netmask of destination host or destination network.	--
Gateway	Define the gateway of the destination.	--
Interface	Choose the corresponding port of the link that you want to configure.	br_lan

4.3.5 Firewall

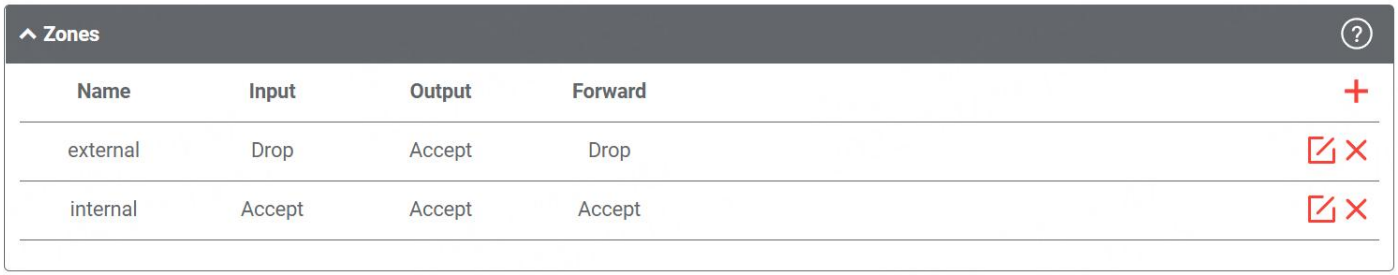
Firewall makes use of Linux iptables to control inbound and outbound traffic, the router has already been configured to meet IEC61162-460 requirements.

General Setting



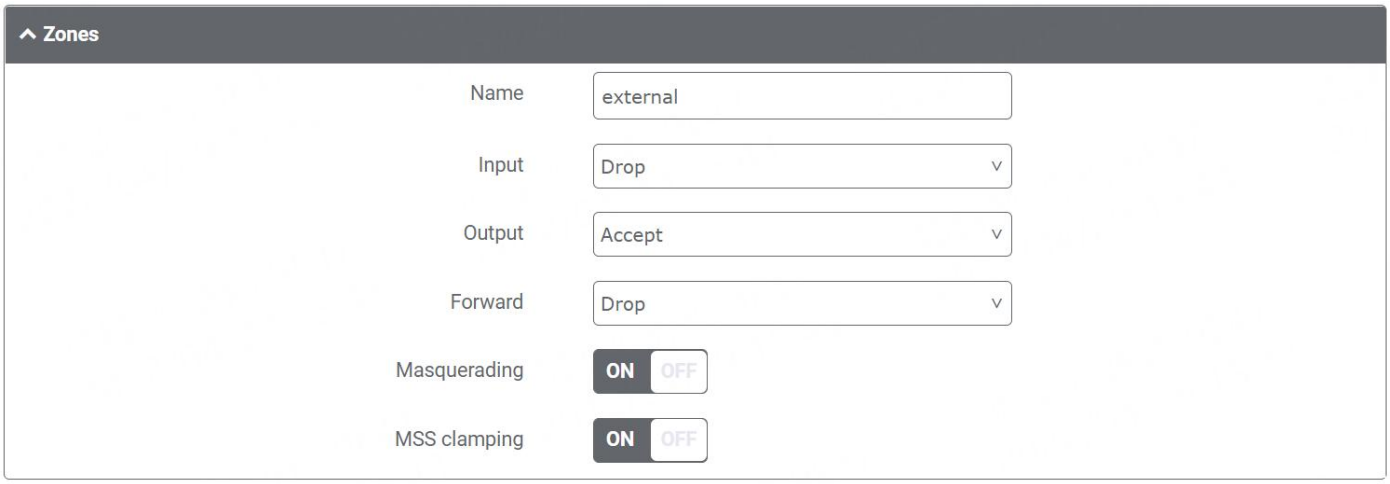
Item	Description	Default
Enable DOS protection	click the toggle button to enable/disable.	ON
Duration of direct connection	• The duration(hour) of direct connection Each rule is valid for four hours	4
Input	Default action of the Input chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Accept
Output	Default action of the Output chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Accept
Forward	Default action of the Forward chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Drop

Note: The general setting is used as a default firewall setting unless specified.



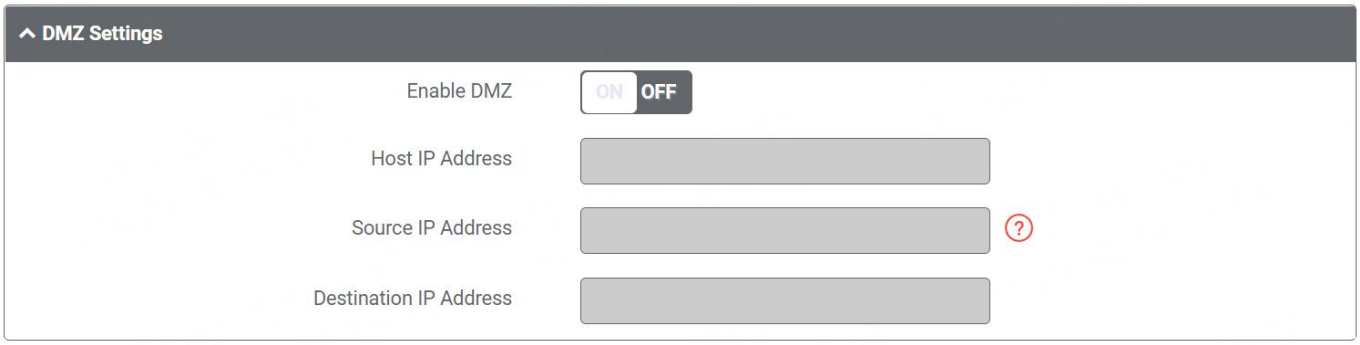
Zone is a set of firewall rules, users can define their own firewall zone.

Click + to add one firewall zone. The maximum count is **50**



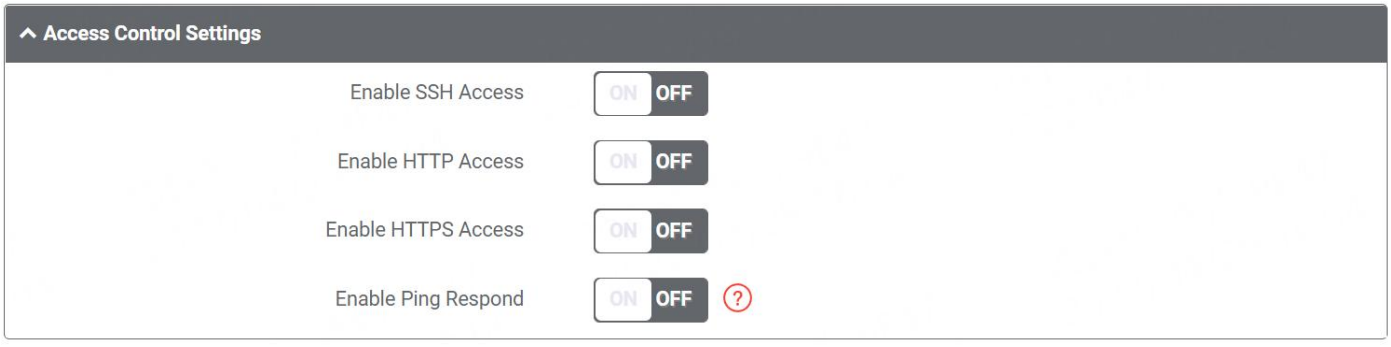
Item	Description	Default
Name	The name of the firewall zone.	--
Input	Default action of the Input chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Drop
Output	Default action of the Output chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Accept
Forward	Default action of the Forward chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Drop
Masquerading	Click the toggle button to enable/disable. MASQUERADE is an iptables target that can be used instead of the SNAT (source NAT) target when the external IP of the network interface is not known at the moment of writing the rule (when the interface gets the external IP dynamically).	ON

MSS clamping	Click the toggle button to enable/disable. MSS clamping is a workaround used to change the maximum segment size (MSS) of all TCP connections passing through links with an MTU lower than the Ethernet default of 1500.	ON



DMZ (Demilitarized Zone), also known as the demilitarized zone. It is a buffer between a non-secure system and a secure system that is set up to solve the problem that users who access the external network cannot access the internal network server after the firewall is installed. A DMZ host is an intranet host where all ports are open to the specified address except the ports that are occupied and forwarded.

Item	Description	Default
Enable DMZ	Click the toggle button to enable/disable DMZ. DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	OFF
Host IP Address	Enter the IP address of the DMZ host on your internal network.	Null
Source IP Address	Set the address which can talk to the DMZ host. Null means for any addresses.	Null
Destination IP Address	Set the address which the DMZ host can talk to . Null means for any addresses.	Null



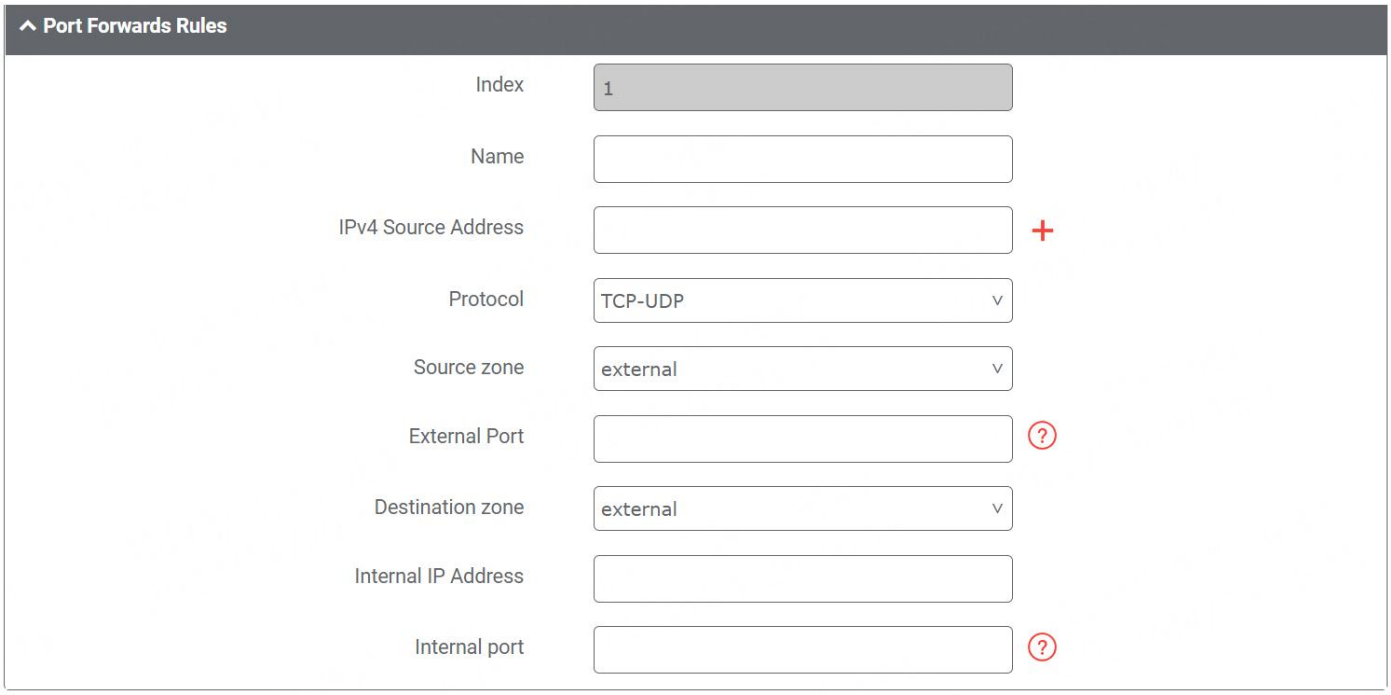
Item	Description	Default
Enable SSH Access	Click the toggle button to enable/disable this option. When enabled, the zone user can access the device via SSH.	OFF
Enable HTTP Access	Click the toggle button to enable/disable this option. When enabled, the zone user can access the device via HTTP.	OFF
Enable HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the zone user can access the device via HTTPS.	OFF

Enable Ping Respond	Click the toggle button to enable/disable this option. When enabled, the device will reply to the Ping requests from other hosts on the zone.	OFF

Port Forwards

This window allows you to view the port forward rules. Port forwarding is a way of redirecting an incoming connection to another IP address, port or the combination of both.

Click + to add one. The maximum count is **50.**



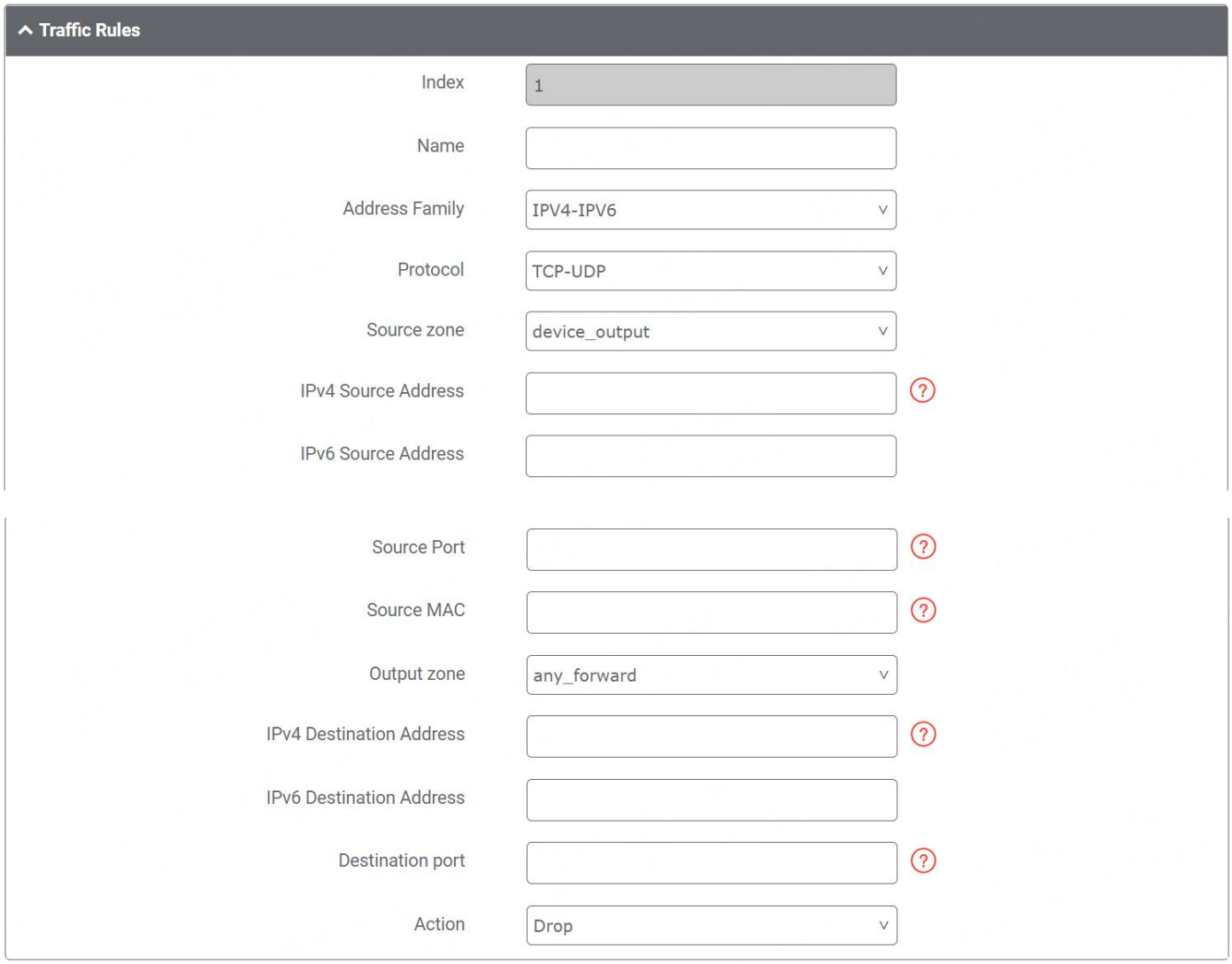
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	Name of the rule.	Null
IPv4 Source Address	IP address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field.	Null
Protocol	Select from “TCP”, “UDP” or “TCP-UDP” as your application required.	TCP-UDP
Source zone	The zone to which the third party will be connecting. Select a configured zone.	external
External Port	Match incoming traffic directed at the given destination port or port range on this host. Select a configured zone.	Null

Item	Description	Default
Destination zone	The zone to which the incoming connection will be redirected.	external
Internal IP Address	The IP address to which the incoming connection will be redirected.	Null
Internal Port	The port number to which the incoming connection will be redirected.	Null

Traffic Rules

This window allows you to view the traffic rules.

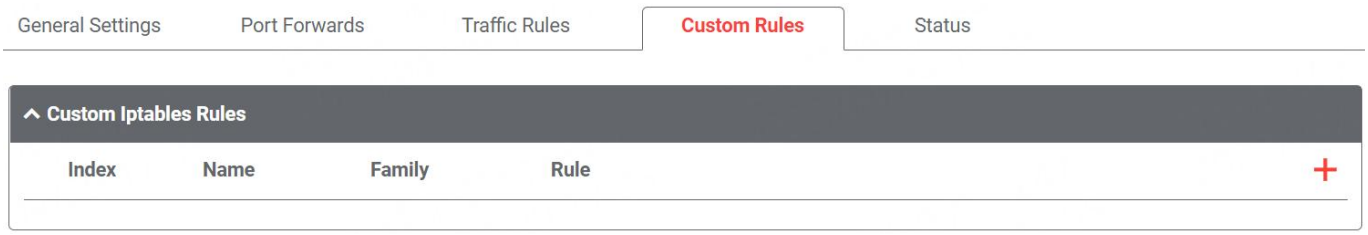
Click + to add one. The maximum count is **50.**



Item	Description	Default
Index	Indicate the ordinal of the list.	--

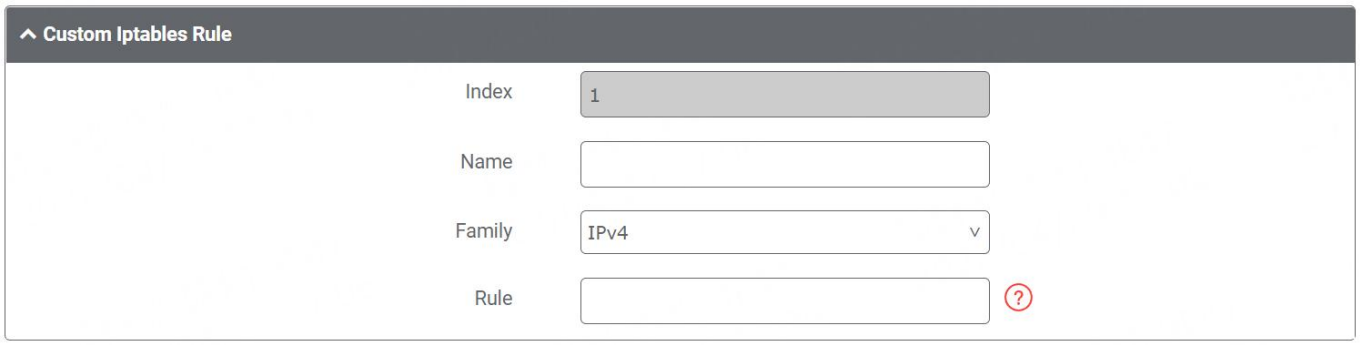
Item	Description	Default
Name	The name of the rule.	Null
Address family	Select from “IPv4”, “IPv6” or “IPv4-IPv6” as your application required.	IPv4-IPv6
Protocol	Select from “TCP”, “UDP” or “TCP-UDP” as your application required.	TCP-UDP
Source zone	The zone to which the third party will be connecting.	device_output
IPv4 Source Address	The IPv4 address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field.	Null
IPv6 Source Address	The IPv6 address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field.	Null
Source Port	Port number(s) used by the connecting host. The rule will match the source port used by the connecting host with the port number(s) specified in this field. Leave empty to make the rule skip source port matching.	Null
Source MAC	MAC address of connecting hosts. The rule will apply only to hosts that match MAC addresses specified in this field. Leave empty to make the rule skip MAC address matching.	Null
Output zone	The zone to which the incoming connection will be redirected.	any_forward
IPv4 Destination Address	The IP address to which the incoming connection will be redirected.	Null
IPv6 Destination Address	The IP address to which the incoming connection will be redirected.	Null
Destination port	The port number to which the incoming connection will be redirected.	Null
Action	Select from “Accept”, or “Drop” as your application required.	Null

Custom Rules



This window allows you to view the custom rules.

Click + to add one. The maximum count is **50.**



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	Enter a description for this.	Null
Family	Select from “IPv4”, “IPv6” or “IPv4-IPv6” as your application required.	IPv4
Rule	Users specify their own iptables rule in required format.	Null

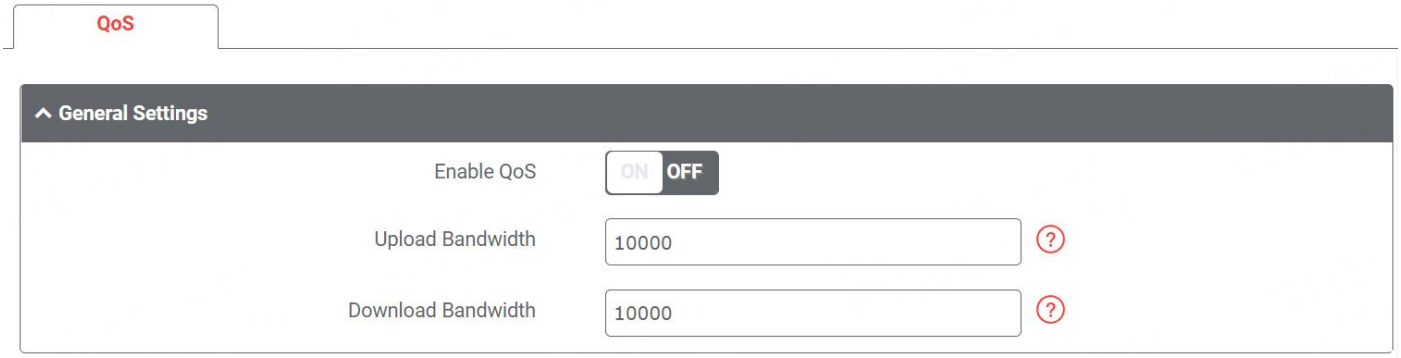
Status

This window allows you to view the status of firewall.

4.3.6 QoS

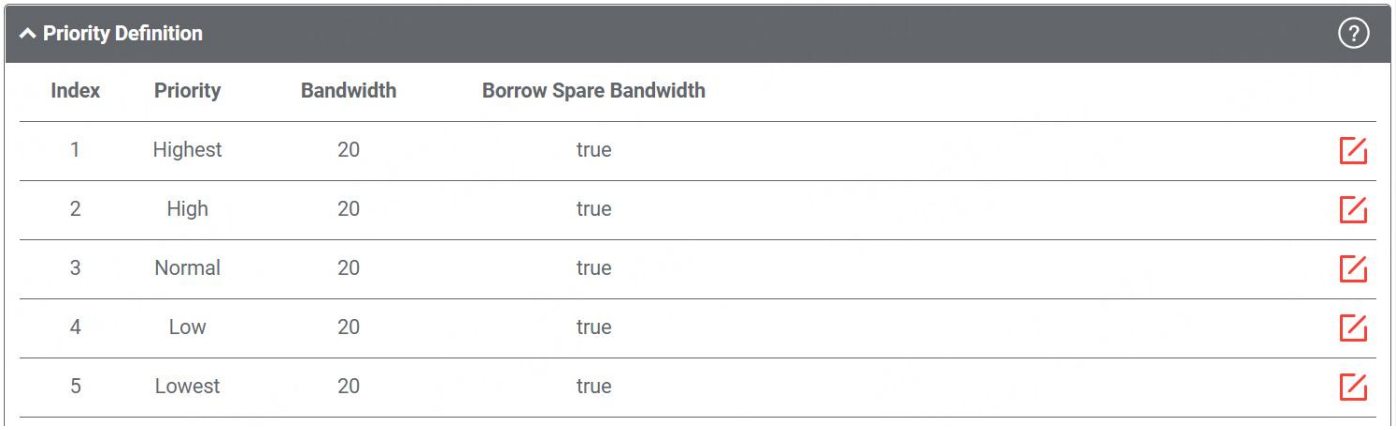
QoS provides the possibility to prioritize network traffic based on hosts, ports or services and limit download or upload speeds on a selected interface.

General Setting

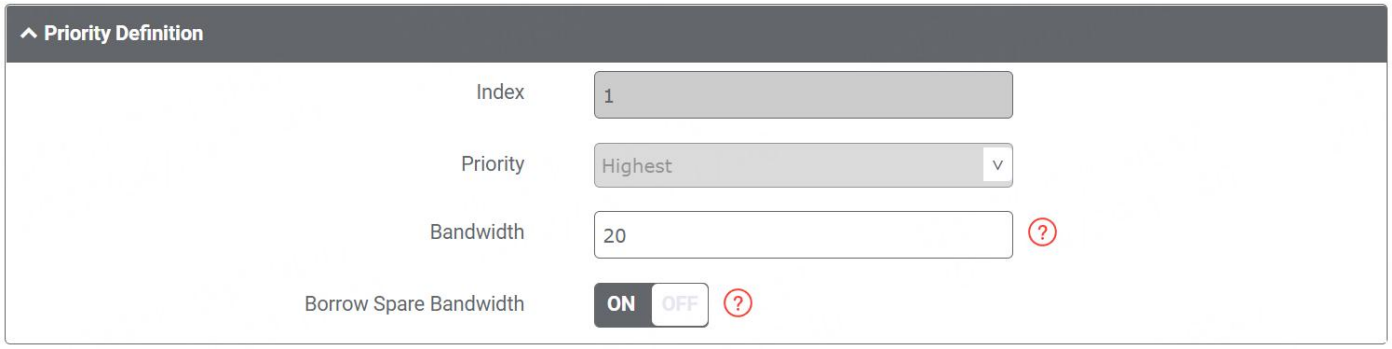


Item	Description	Default
Enable QoS	Click the toggle button to enable or disable.	OFF
Upload Bandwidth	Enter a value for the upload bandwidth, the unit is kbit.	10000
Download Bandwidth	Enter a value for the download bandwidth, the unit is kbit.	10000

Priority Definition



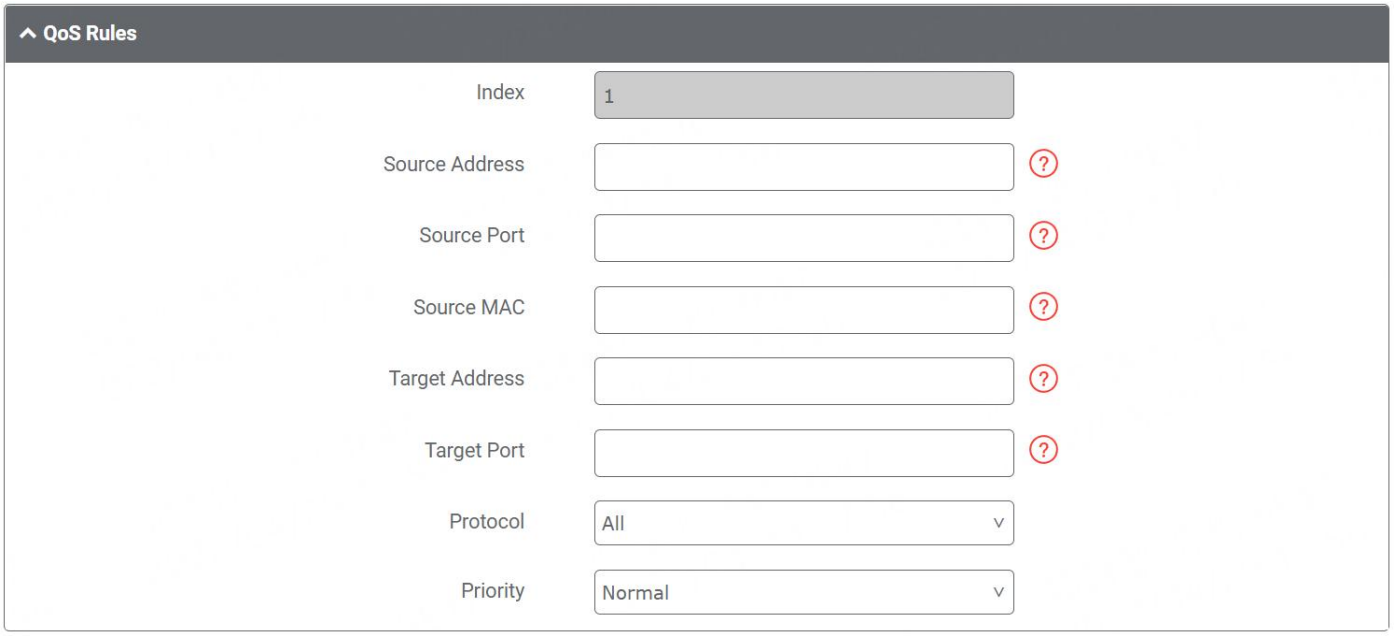
Click to set the priority.



Item	Description	Default
Bandwidth	Percentage of total bandwidth. The sum of bandwidth of all the priorities cannot be greater than 100.	20
Borrow Spare Bandwidth	The traffic associated with this priority will borrow unused bandwidth from other priorities when borrowing is enabled, and will be limited to the specified bandwidth when borrowing is disabled.	ON

IPv4 QoS Rules

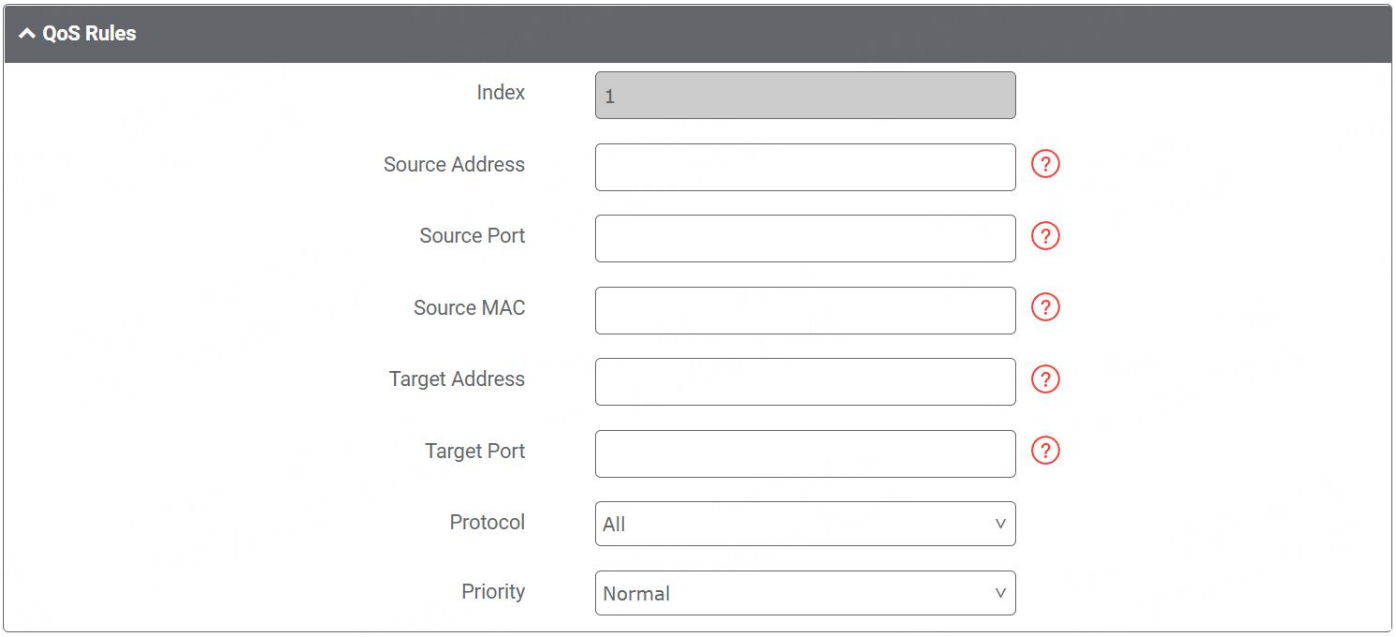
Click + to add one. The maximum count is **10.**



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Source Address	The address of Host(s) from which data will be transmitted.	Null
Source Port	The port of Host(s) from which data will be transmitted.	Null
Source MAC	The MAC address of Host(s) from which data will be transmitted.	Null
Target Address	The address of Host(s) to which data will be transmitted.	Null
Target Port	The port of Host(s) to which data will be transmitted.	Null
Protocol	Select from “All”, “TCP”, “UDP” or “ICMP” as your application required.	All
Priority	Select from “Highest”, “High”, “Normal”, “Low” or “Lowest” as your application required.	Normal

IPv6 QoS Rules

Click + to add one. The maximum count is **10.**



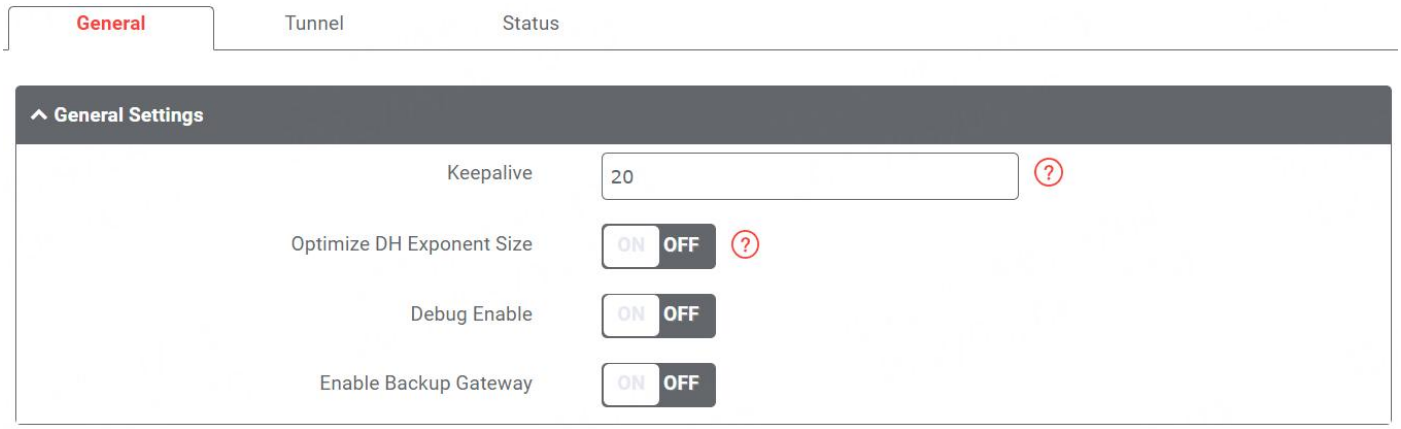
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Source Address	The address of Host(s) from which data will be transmitted.	Null
Source Port	The port of Host(s) from which data will be transmitted.	Null
Source MAC	The MAC address of Host(s) from which data will be transmitted.	Null
Target Address	The address of Host(s) to which data will be transmitted.	Null
Target Port	The port of Host(s) to which data will be transmitted.	Null
Protocol	Select from “All”, “TCP”, “UDP” or “ICMP” as your application required.	All
Priority	Select from “Highest”, “High”, “Normal”, “Low” or “Lowest” as your application required.	Normal

4.4 VPN

4.4.1 IPsec

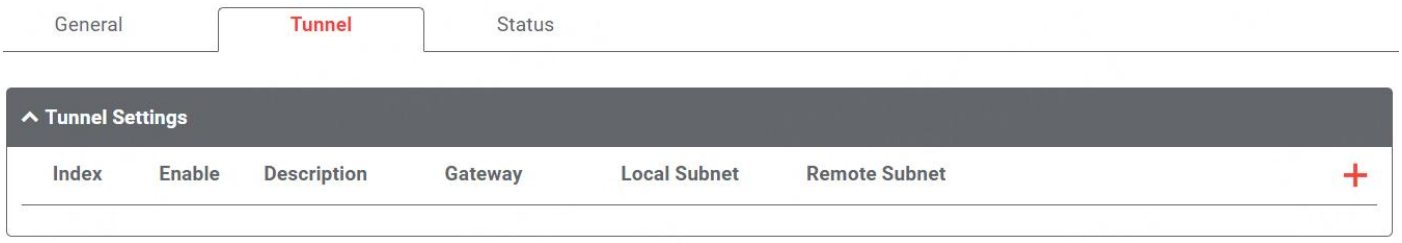
This section allows you to set the IPsec and the related parameters. Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session.

General



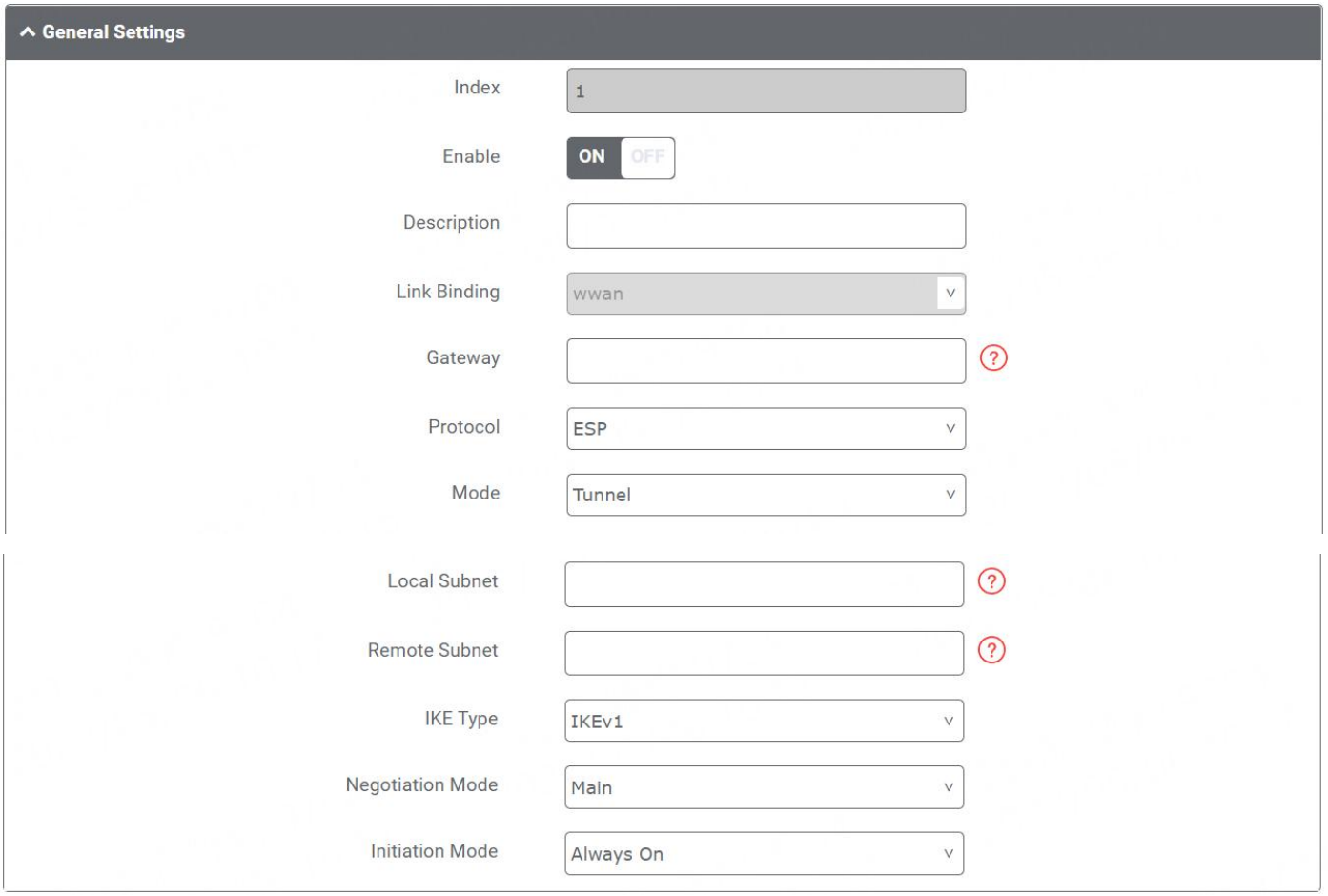
Item	Description	Default
Keepalive	Set the time to live in seconds. The router sends keep-alive packets to the NAT (Network Address Translation) server at regular intervals to prevent the records on the NAT table from disappearing.	20
Optimize DH Size	Click the toggle button to enable/disable this option. When enabled, when using dhgroup17 or dhgroup18, it helps to shorten the time to generate the dh key.	OFF
Debug Enable	Click the toggle button to enable/disable this option. Enable for IPsec VPN information output to the debug port.	OFF
Enable Backup Gateway	Click the toggle button to enable/disable this option.	OFF

Tunnel



Click + to add IPsec tunnel settings. The maximum count is **6**.

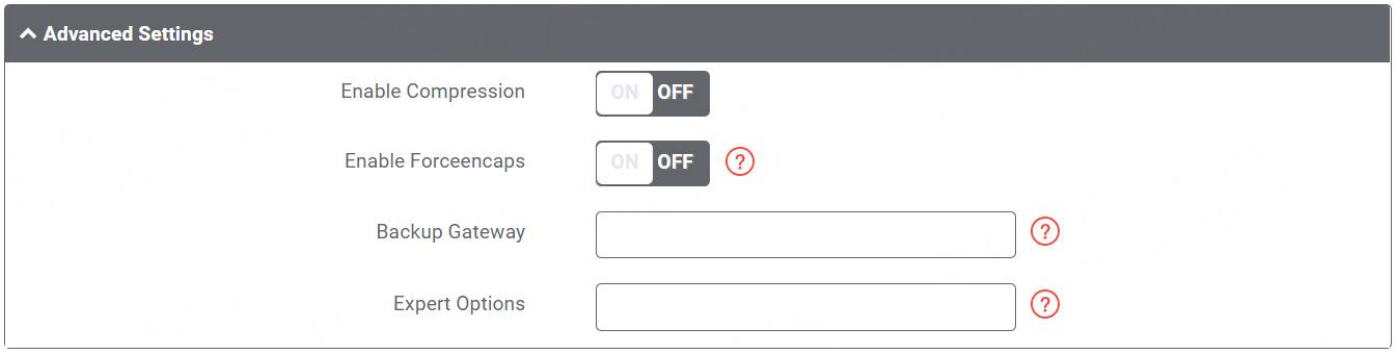
General Setting



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Link binding	Select the link to build IPSec.	Unbound
Gateway	Enter the address of remote side IPsec VPN server. 0.0.0.0 represents for any address.	Null
Mode	Select from “Tunnel” and “Transport”. • Tunnel: Commonly used between routers, or at an end-station to a router, the router acting as a proxy for the hosts behind it • Transport: Used between end-stations or between an end-station and a router, if the router is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination	Tunnel
Protocol	Select the security protocols from “ESP” and “AH”.	ESP

	• ESP: Use the ESP protocol • AH: Use the AH protocol	
Local Subnet	Enter the local subnet's address with mask protected by IPsec, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g. 10.8.0.0/24	Null
IKE Type	Select from "IKEv1" and "IKEv2".	IKEv1
Negotiation Mode	Select from "Main" and "Aggressive" for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Initial Mode	Select from "Always On" and "On Demand".	Always On

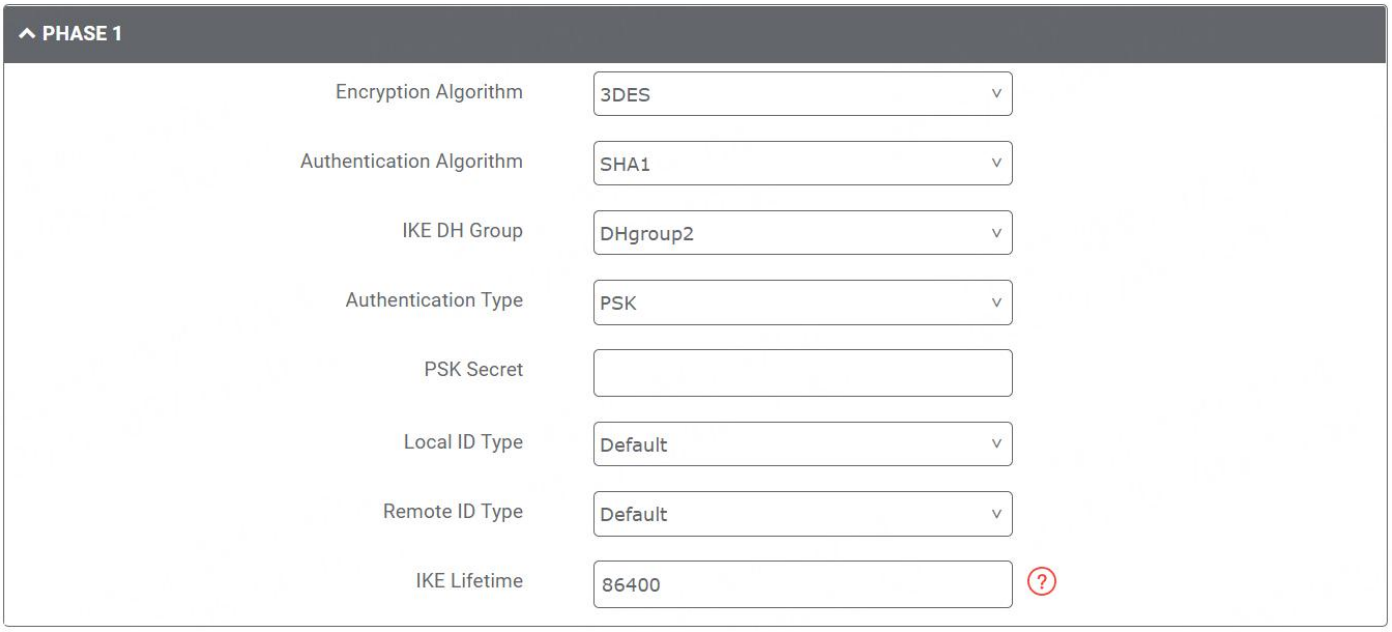
Advanced Setting



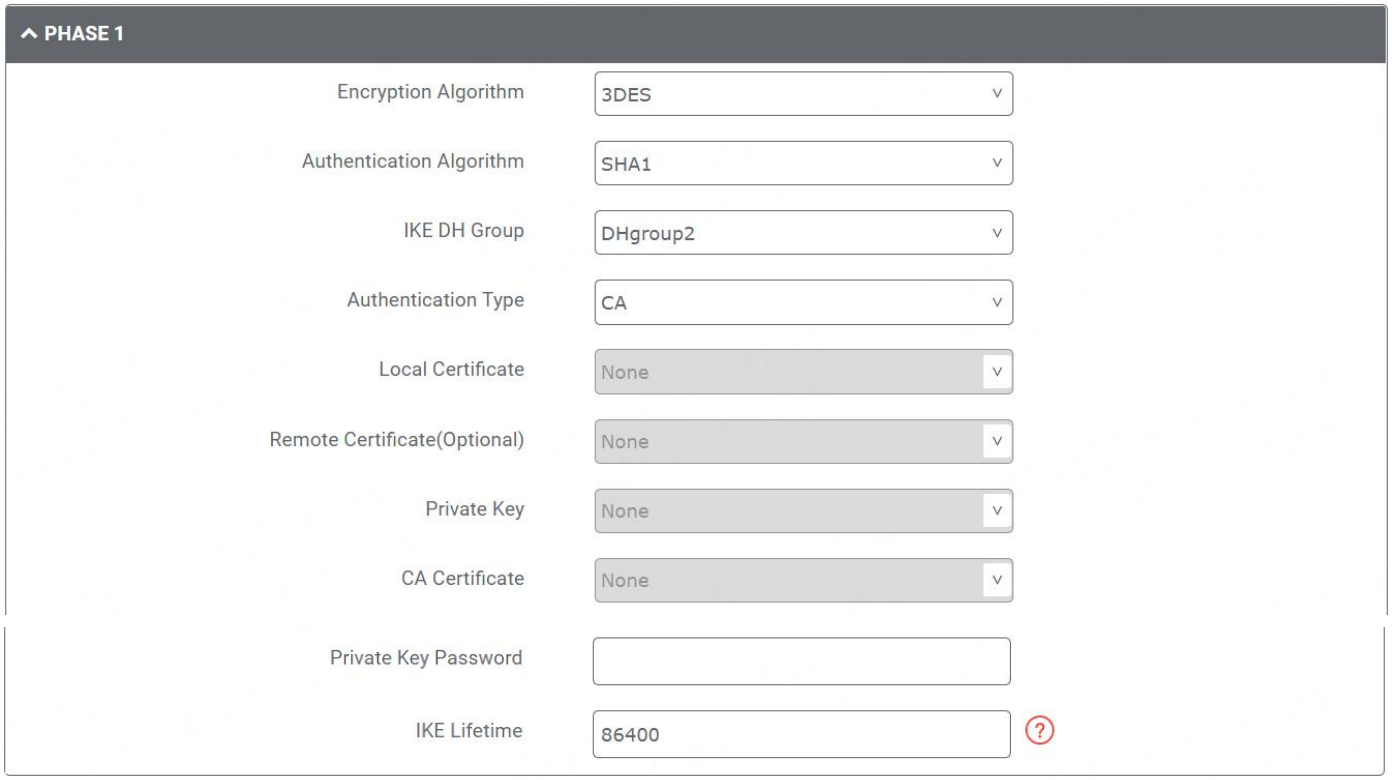
Item	Description	Default
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Enable Forceencaps	Force UDP encapsulation for ESP packets even if no NAT situation is detected.This may help to surmount restrictive firewalls.	OFF
Backup Gateway	Backup Address of remote peer to initiate connection, empty means disable.	Null
Expert Options	Add more PPP configuration options here, format: config-desc; config-desc, e.g. protostack=netkey; plutodebug=none	Null

PHASE 1

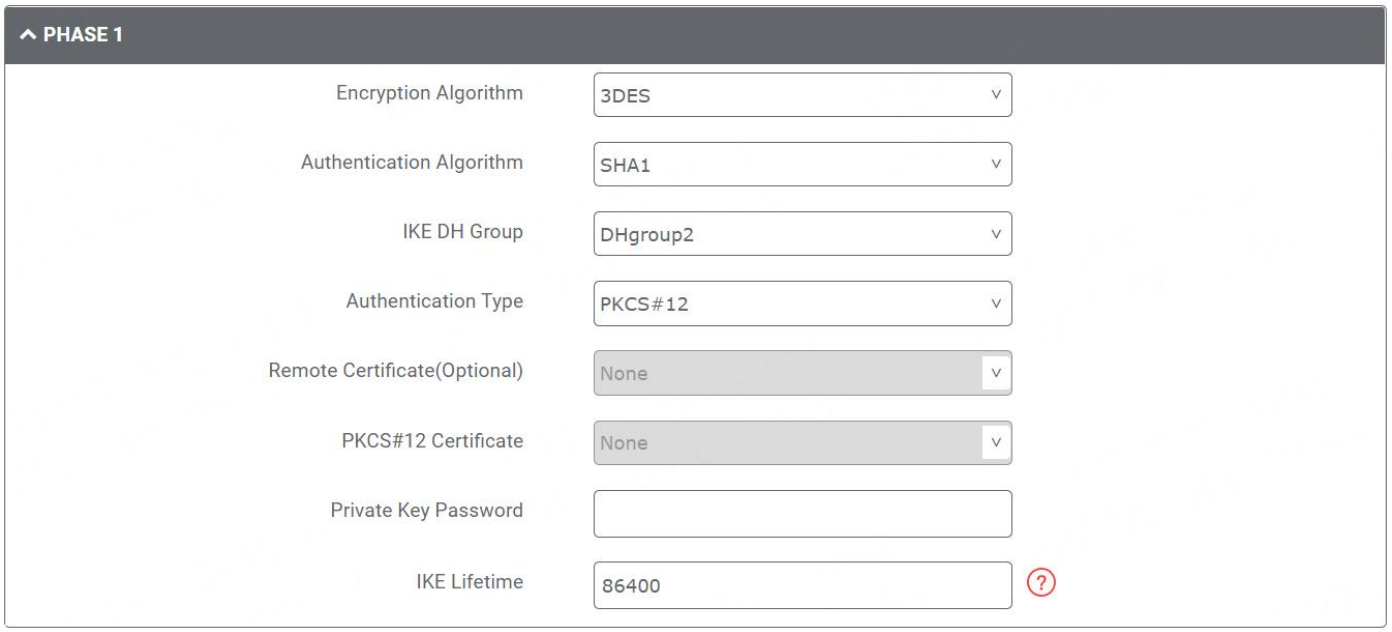
The window is displayed as below when choosing "PSK" as the authentication type.



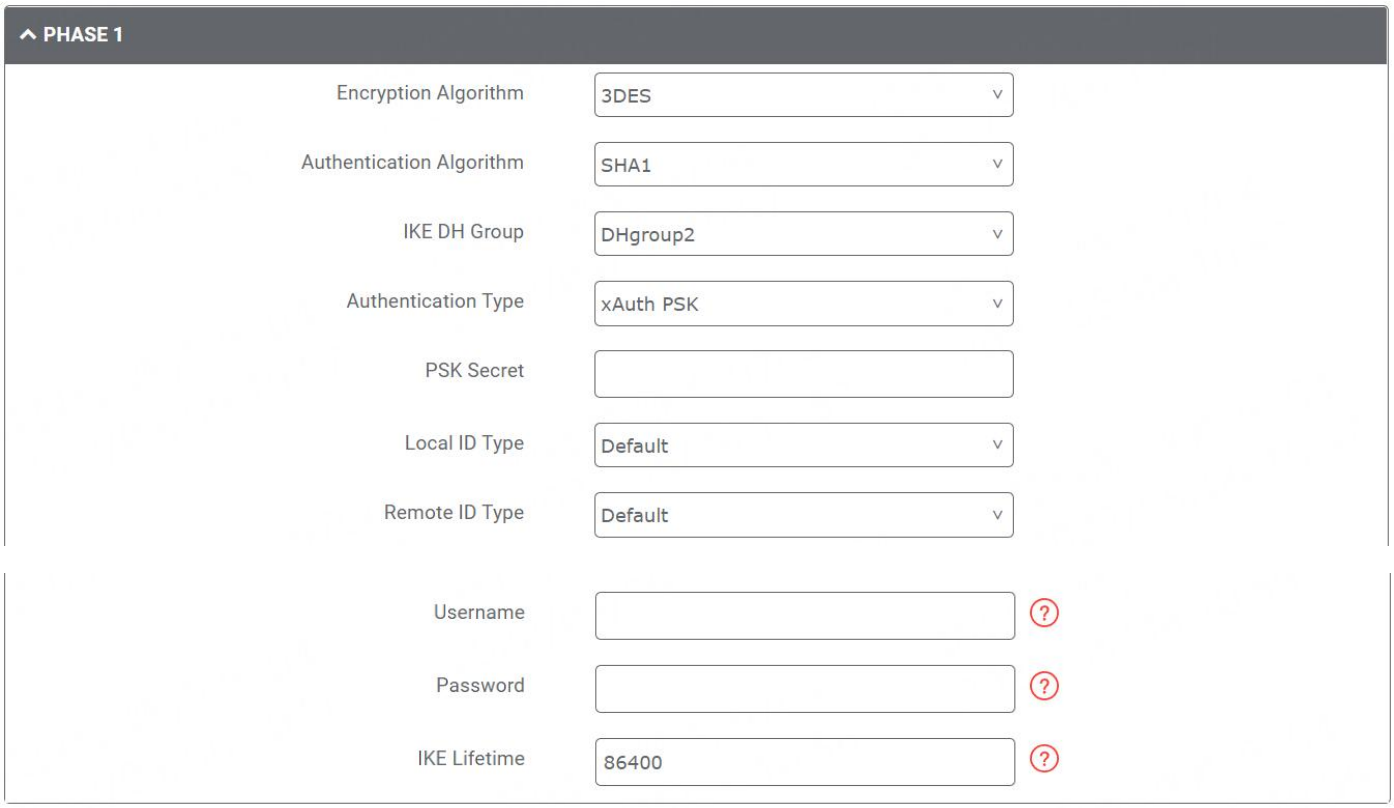
The window is displayed as below when choosing “CA” as the authentication type.



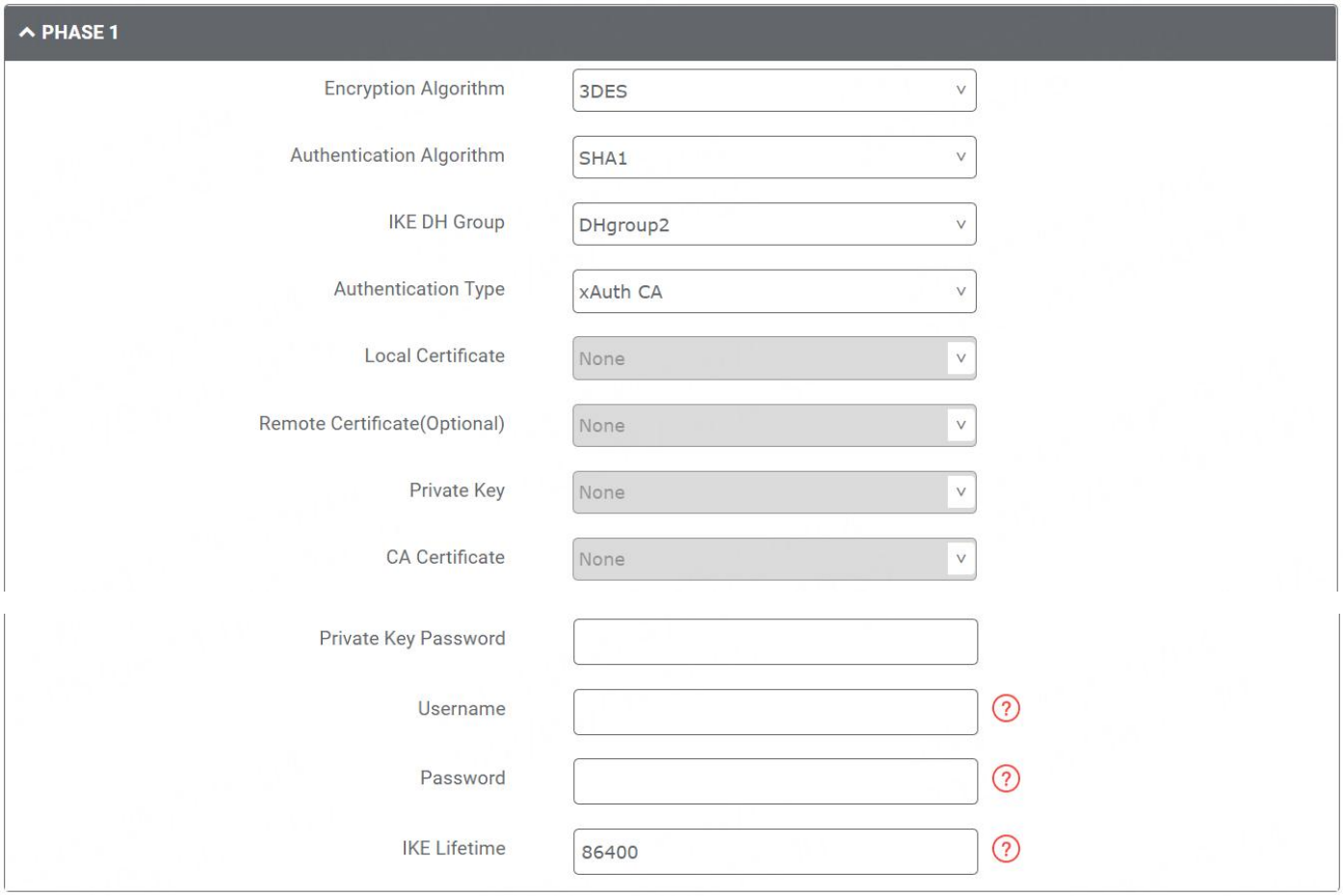
The window is displayed as below when choosing “PKCS#12” as the authentication type.



The window is displayed as below when choosing “xAuth PSK” as the authentication type.



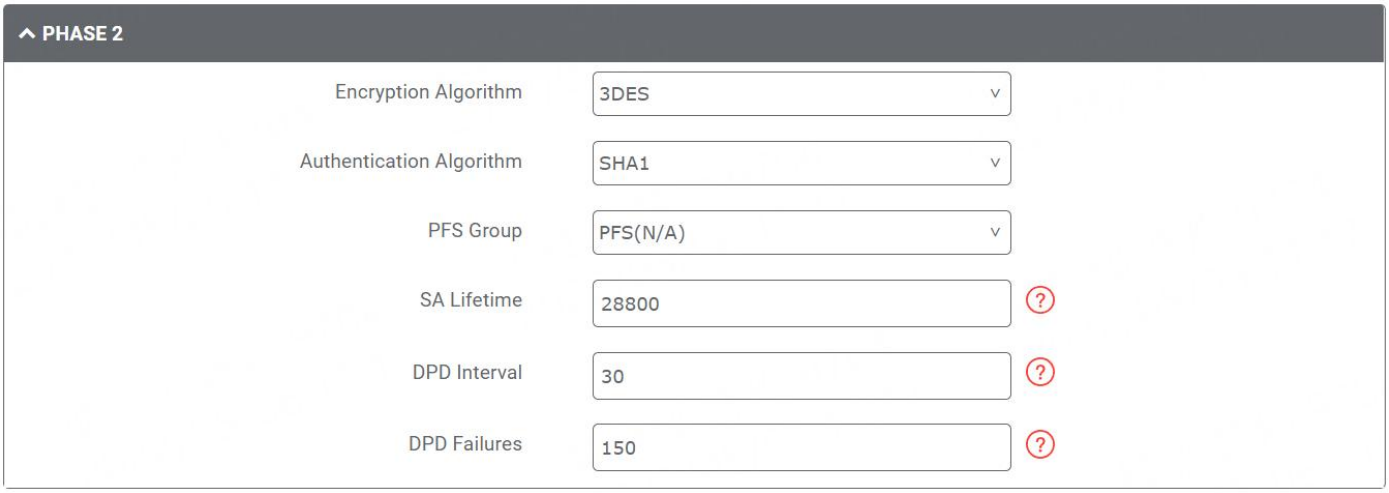
The window is displayed as below when choosing “xAuth CA” as the authentication type.



Item	Description	Default
Encrypt Algorithm	Select from “3DES”, “AES128”, “AES192”and “AES256”. • 3DES: Use 168-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES128: Use 192-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	3DES
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256”,“SHA2 384” or “SHA2 512” .	MD5
IKE DH Group	Select from “DHgroup1”,“DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” .	DHgroup2
Authentication Type	Select from “PSK”, “CA”, “xAuth PSK” ,”PKCS#12”and “xAuth CA” to be used in IKE negotiation. • PSK: Pre-shared Key • CA: Certification Authority • xAuth: Extended Authentication to AAA server • PKCS#12: Exchange digital certificate authentication	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from “Default”, “Address”, “FQDN” and “User FQDN” . • Default: Uses an IP address as the ID in IKE negotiation • FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security router, e.g., test.robustel.com	Default

Item	Description	Default
	• User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security router, e.g., test@robustel.com	
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Uses an IP address as the ID in IKE negotiation • FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security router, e.g., test.robustel.com • User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security router, e.g., test@robustel.com	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key under the "CA" and "xAuth CA" authentication types.	Null
Username	Enter the username used for the "xAuth PSK" and "xAuth CA" authentication types.	Null
Password	Enter the password used for the "xAuth PSK" and "xAuth CA" authentication types.	Null

PHASE 2



Item	Description	Default
Encrypt Algorithm	Select from "3DES", "AES128", "AES192"or "AES256" when you select "ESP" in "Protocol". Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from "MD5", "SHA1", "SHA2 256" or "SHA2 512" to be used in SA negotiation.	MD5
PFS Group	Select from "PFS(N/A)", "DHgroup1","DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18"	DHgroup2

Item	Description	Default
	to be used in SA negotiation.	
SA Lifetime	Set the IPsec SA lifetime. When negotiating to set up IPsec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is a Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	30
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	150

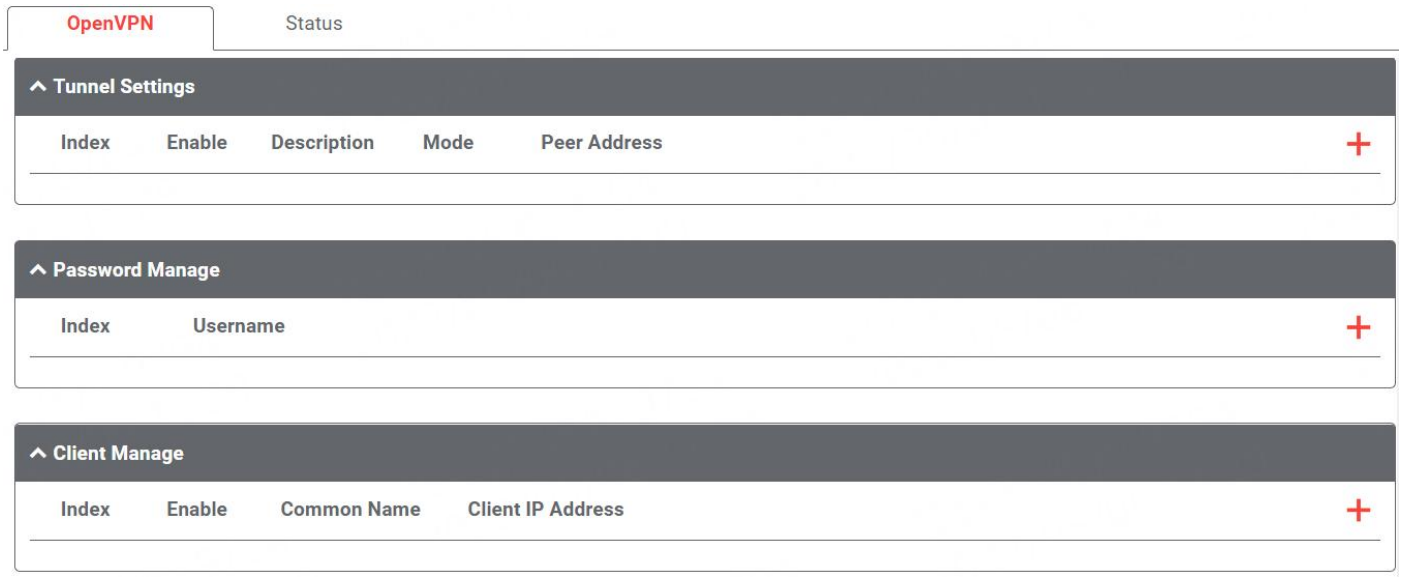
Status

This section allows you to view the status of the IPsec tunnel.

4.4.2 OpenVPN

This section allows you to set the OpenVPN and the related parameters. OpenVPN is an open-source software application that creates secures point-to-point or site-to-site connections.

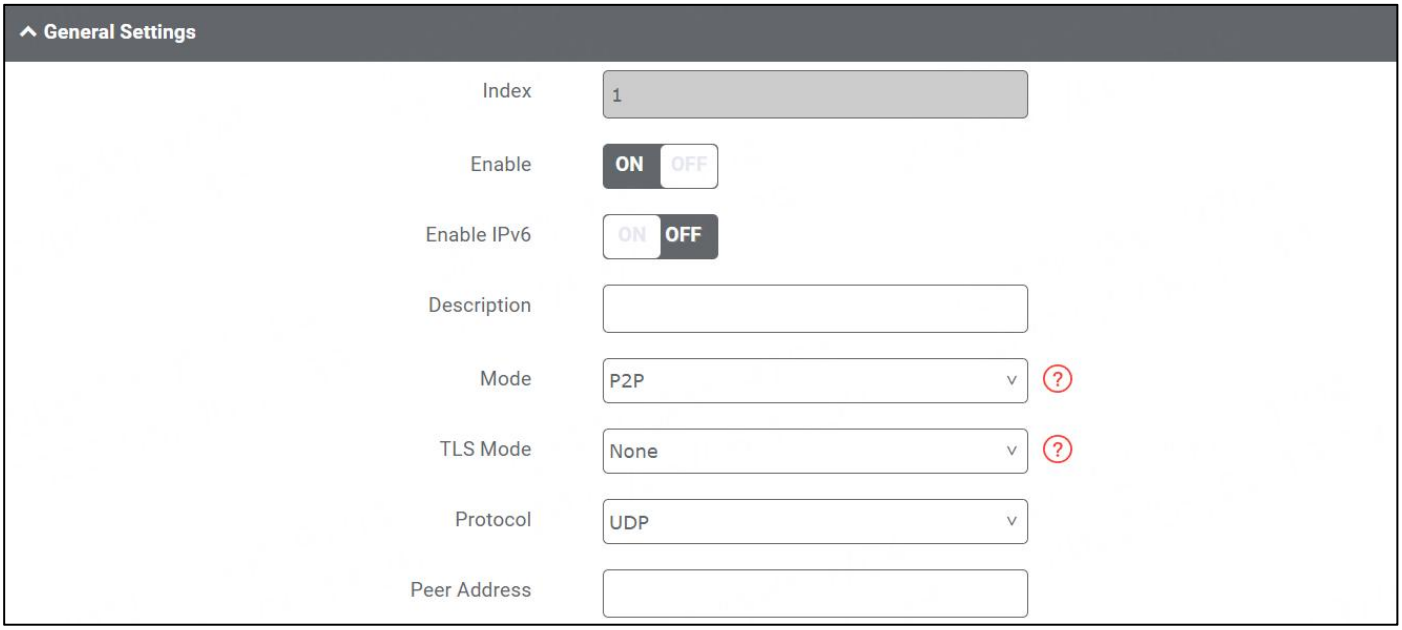
OpenVPN

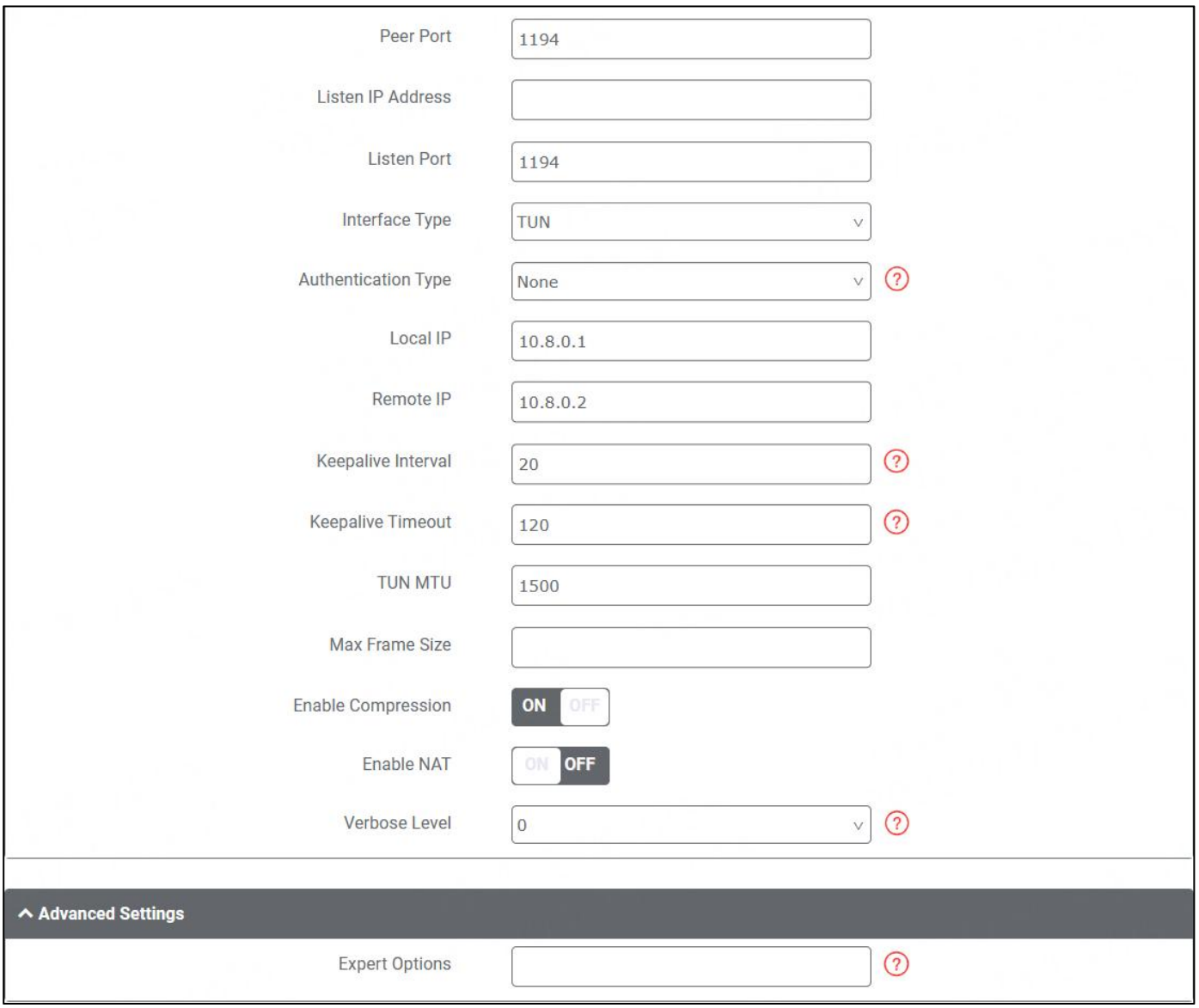


Tunnel Setting

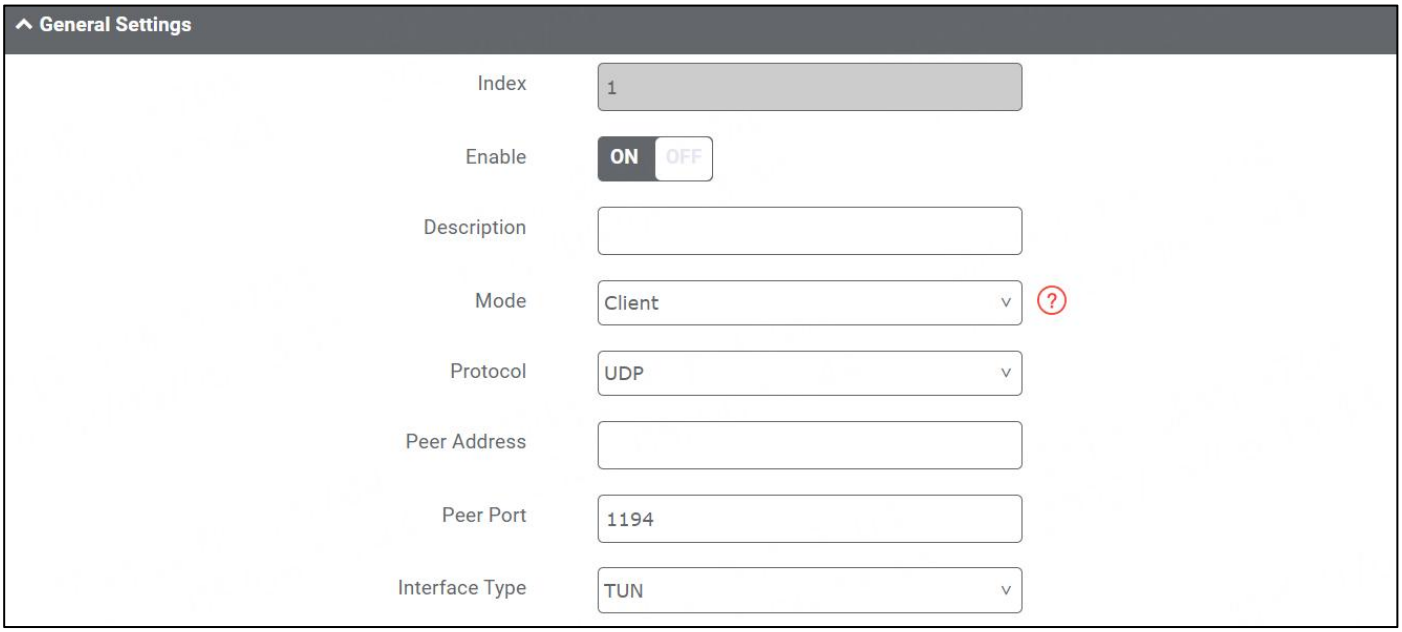
Click + to add an OpenVPN tunnel settings. The maximum count is 5. The configure page might vary when choosing different mode, and the **Authentication Type** might be fixed for using on specific mode.

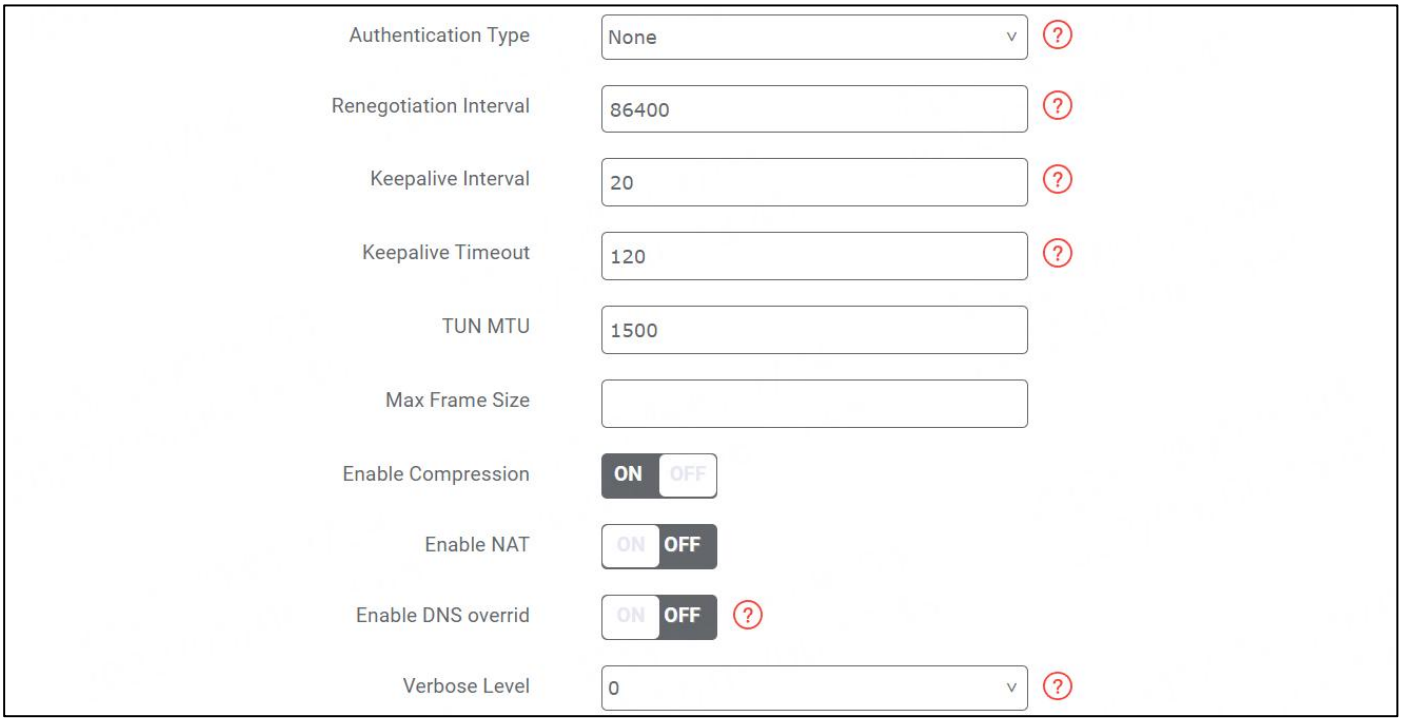
By default, the mode is “P2P”. The window is displayed as below when choosing “P2P” as the mode.



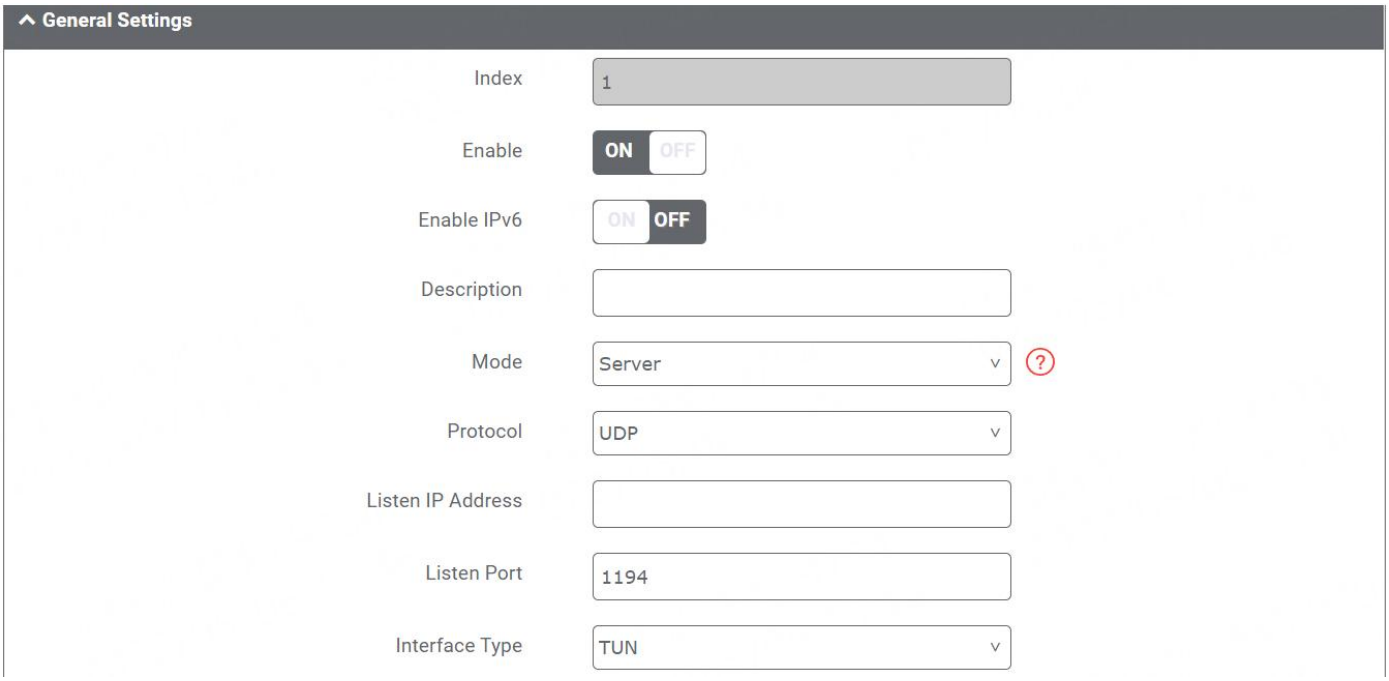


The window is displayed as below when choosing “Client” as the mode.



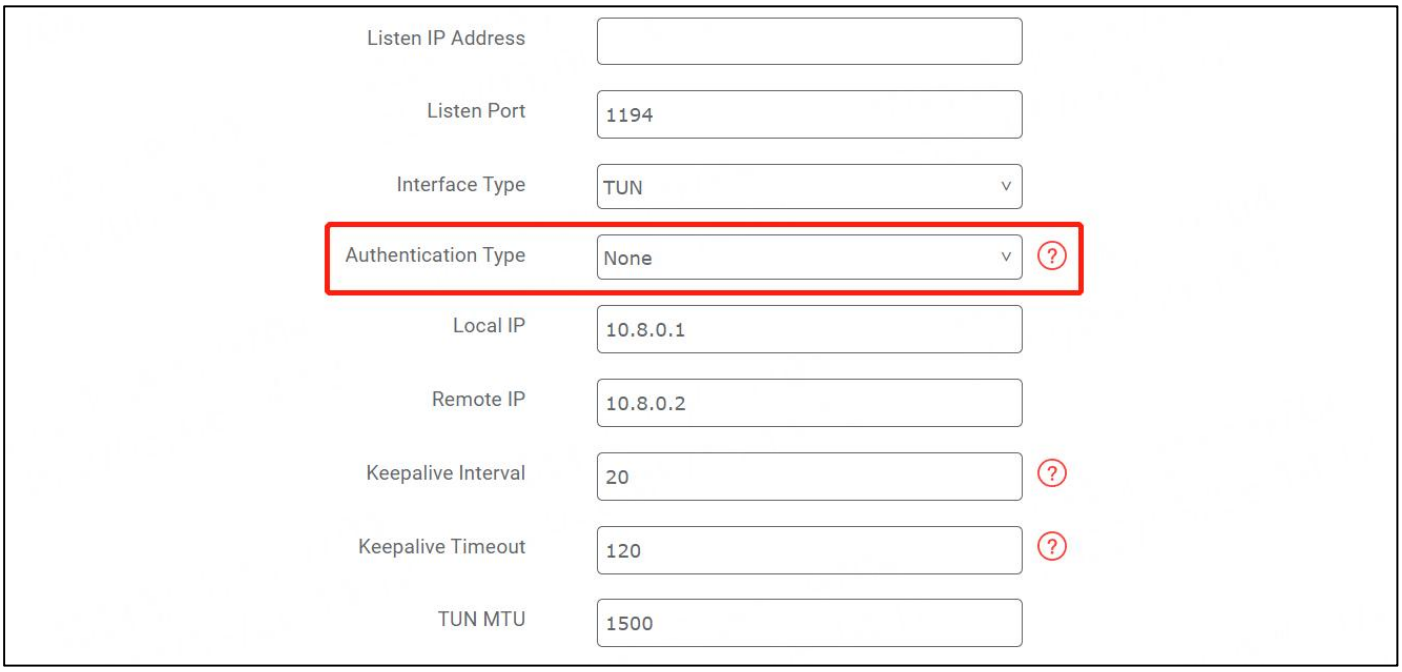


The window is displayed as below when choosing “Server” as the mode.

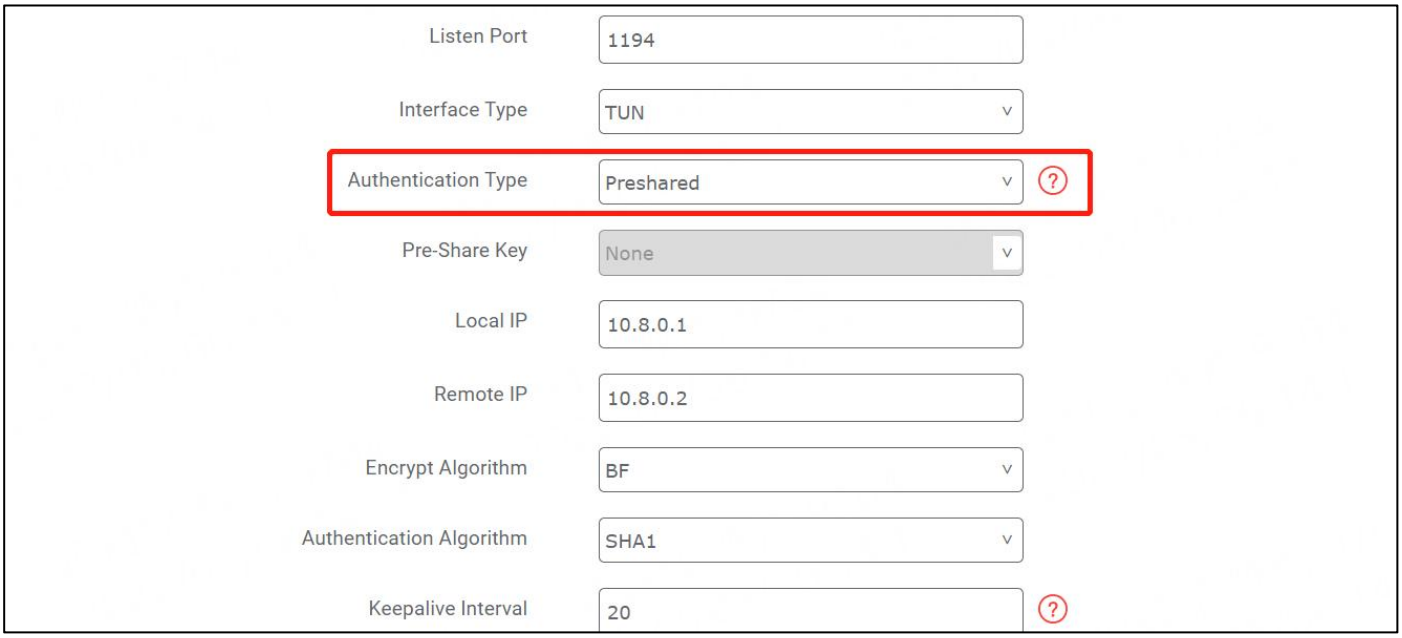


Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Enable IP Pool	OFF
Client Subnet	10.8.0.0
Client Subnet Netmask	255.255.255.0
Renegotiation Interval	86400
Max Clients	10
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable Default Gateway	OFF
Enable NAT	OFF
Verbose Level	0

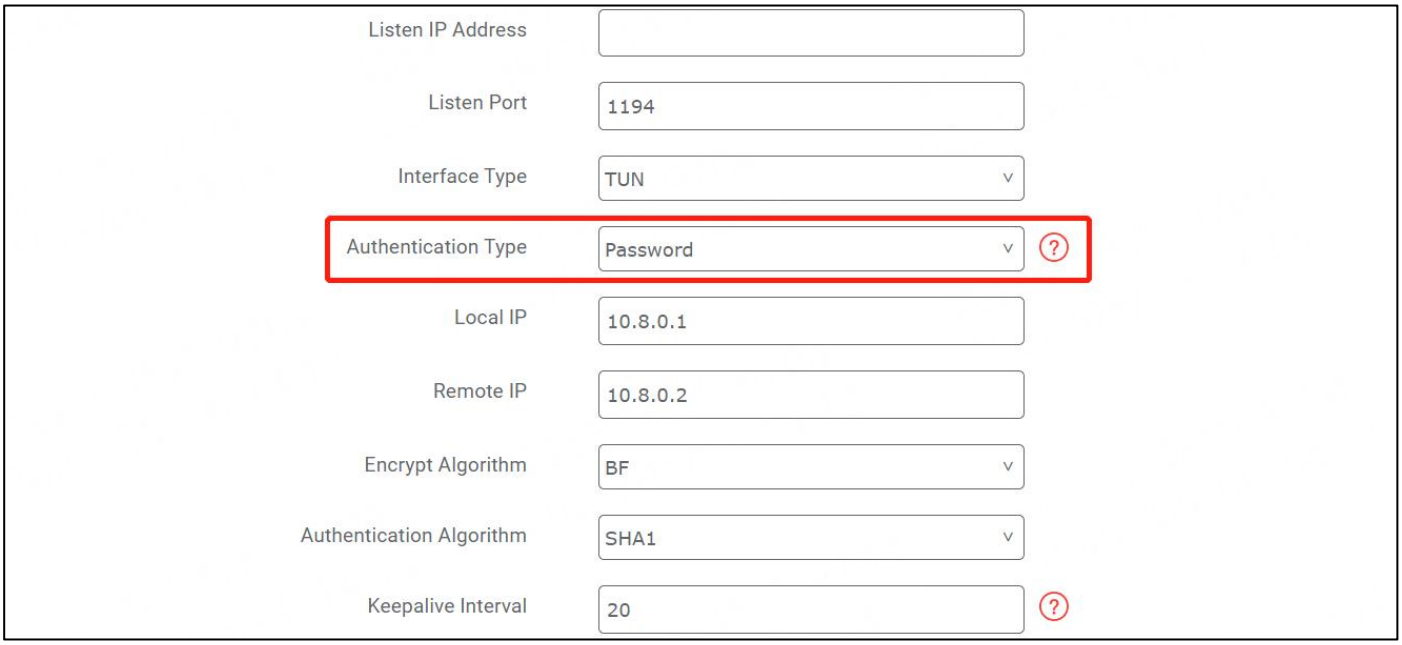
The window is displayed as below when choosing “None” as the authentication type.



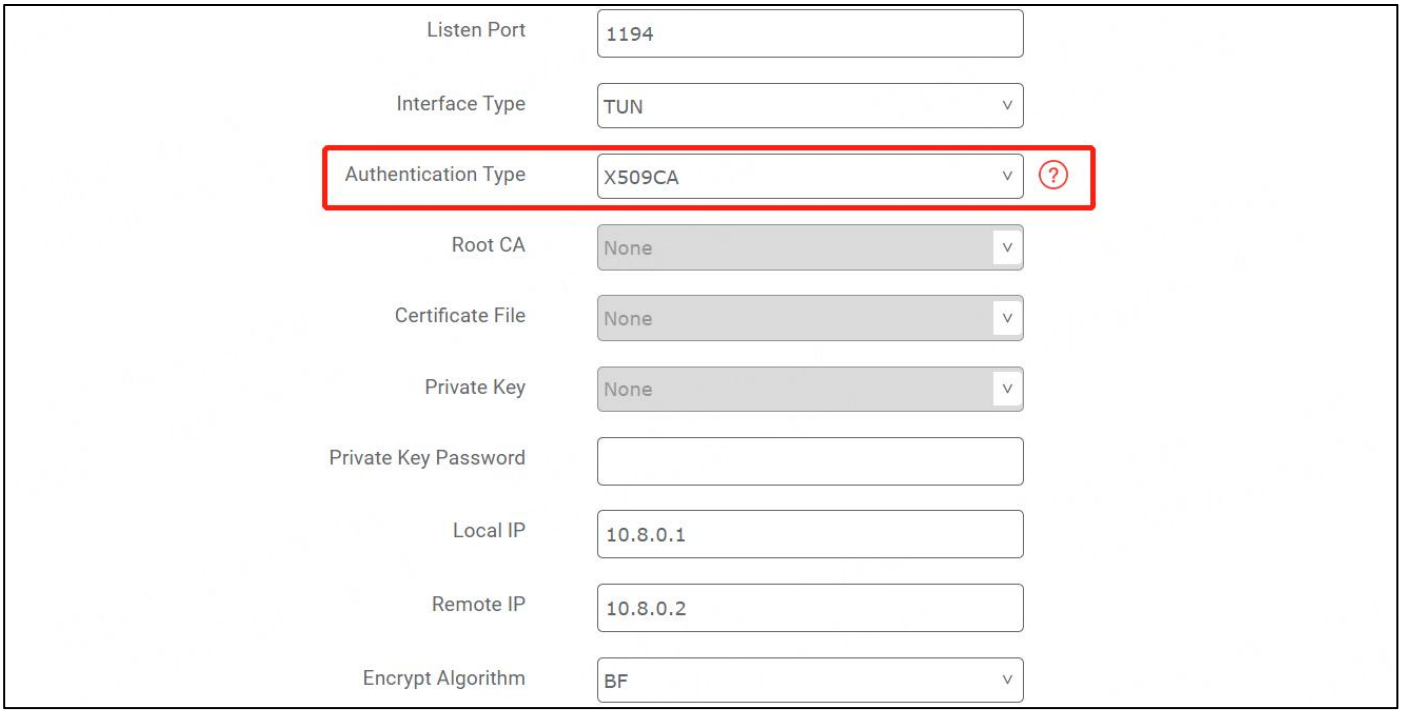
The window is displayed as below when choosing “Preshared” as the authentication type.



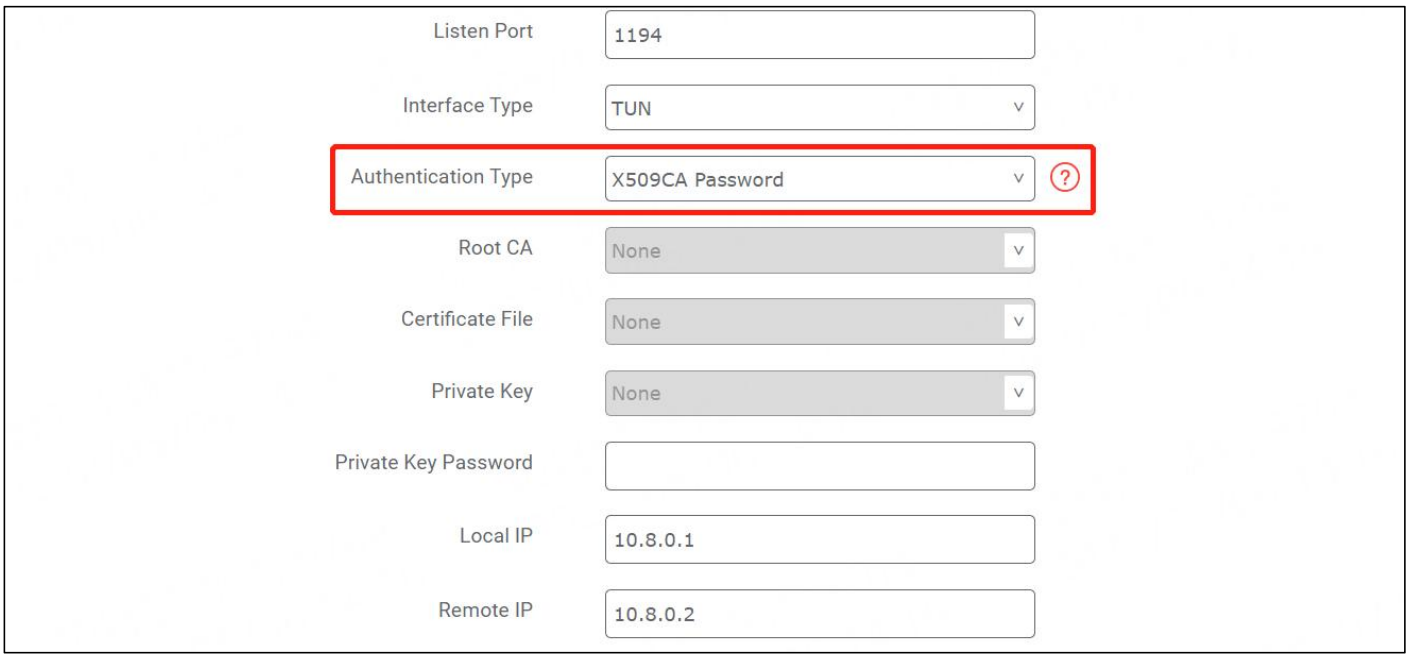
The window is displayed as below when choosing “Password” as the authentication type.



The window is displayed as below when choosing “X509CA” as the authentication type.

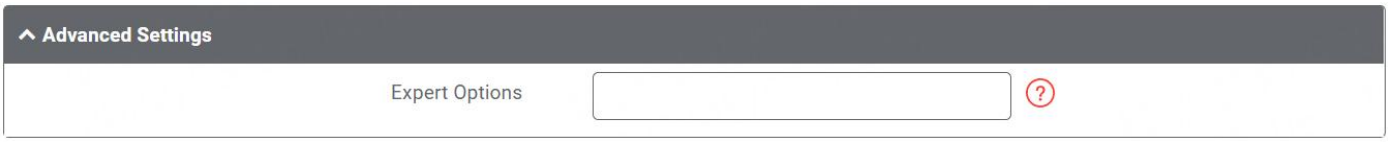


The window is displayed as below when choosing “X509CA Password” as the authentication type.



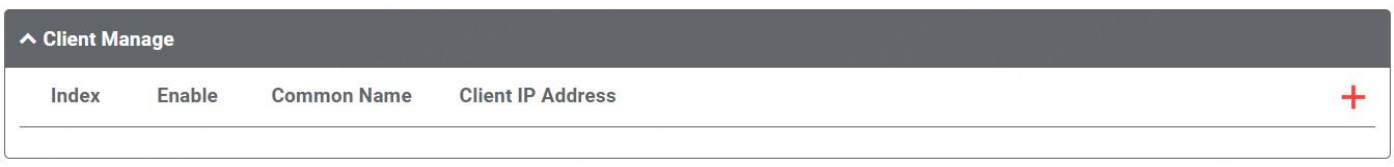
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Enable IPv6	Click the toggle button to enable/disable IPv6.	OFF
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “P2P”, “Client” or “Server”.	P2P
TLS Mode	Select from “None”, “Client” or “Server”.	None
Protocol	Select from “UDP”, “TCP-Client” or “TCP-Server”.	UDP
Peer Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Peer Port	Enter the end-to-end listener port or the listener port of the OpenVPN server.	1194
Listen IP Address	Enter the IP address or domain name.	Null
Listen Port	Enter the listener port at this end.	1194
Interface Type	Select from “TUN”, “TAP” which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA”, “X509CA password”. Note:None and Preshared types only used for P2P mode. It must to add account from the User Management, when using server mode with password authentication.	Null
Private Key Password	Enter the private key password under "X509CA" and "X509CA password" authentication.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2

Item	Description	Default
Encrypt Algorithm	Select from “BF”, “DES”, “DES-EDE3”, “AES-128”, ″AES-192” and “AES-256”. • BF: Use 128-bit BF encryption algorithm in CBC mode • DES: Use 64-bit DES encryption algorithm in CBC mode • DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES192: Use 192-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	BF
Authentication Algorithm	Select from "MD5", "SHA1", "SHA256" or "SHA512".	SHA1
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
TUN MTU	Set the MTU for the tunnel.	1500
Max Frame Size	Sets the shard size of the data to be transmitted through the tunnel.	Null
Enable Compression	Click the switch button to enable/disable this option. When enabled, this feature compresses the header of the IP packet.	ON
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of host behind router will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	Select the level of the output log and values from 0 to 11. • 0: No output except fatal errors • 1~4: Normal usage range • 5: Output R and W characters to the console for each packet read and write • 6~11: Debug info range	0



Item	Description	Default
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ‘;’.	Null

Client Management

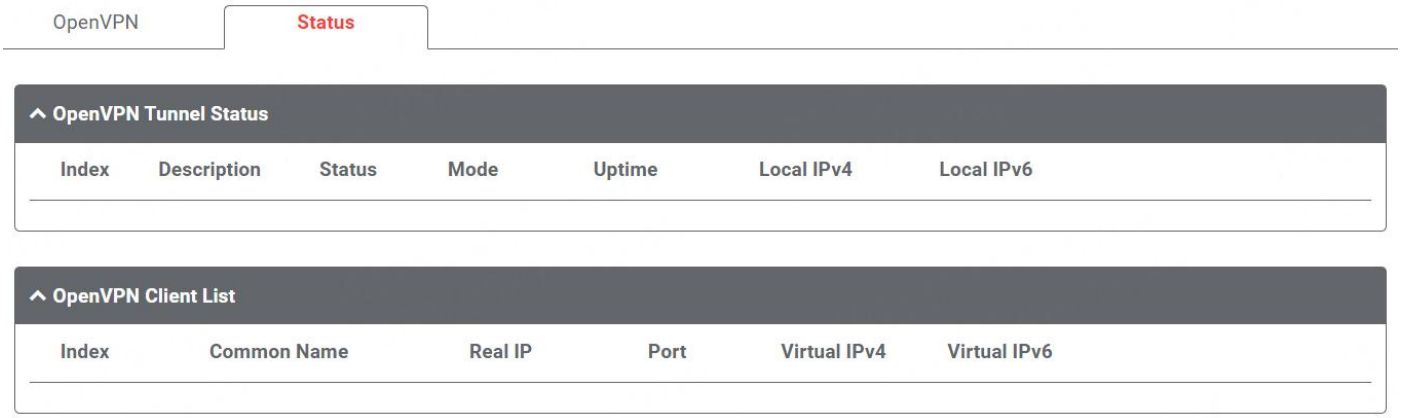


Click + to add client information. The maximum count is **20.**

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the switch button to enable/disable this option.	ON
Common Name	Specify a common name for the client.	Null
Client IP Address	Specify the client's virtual IP address.	Null

Status

This section allows you to view the status of the OpenVPN tunnel.

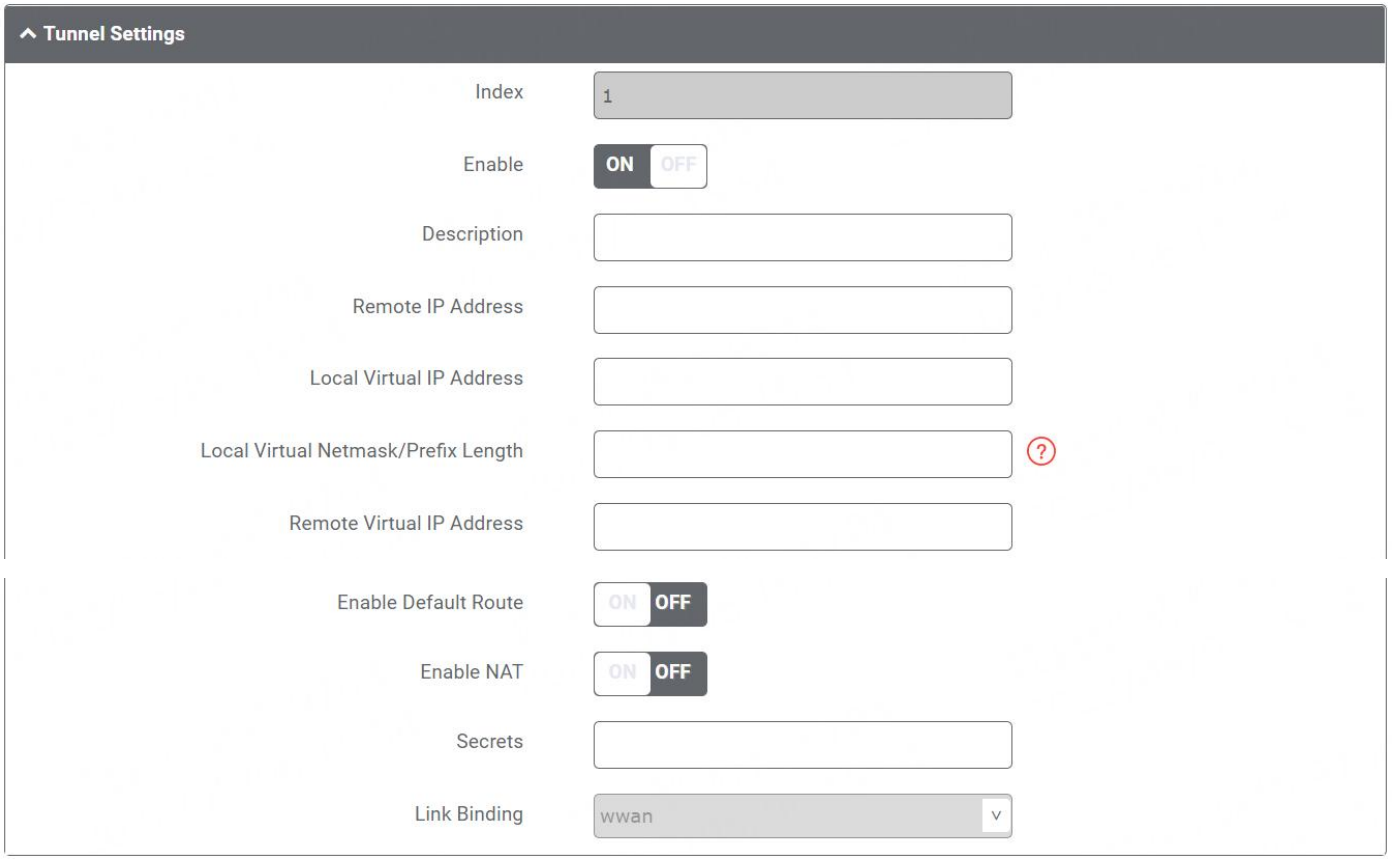


4.4.3 GRE

This section allows you to set the GRE and the related parameters. Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. There are two main uses of GRE protocol: internal protocol encapsulation and private address encapsulation.

GRE

Click + to add tunnel settings. The maximum count is **5**.

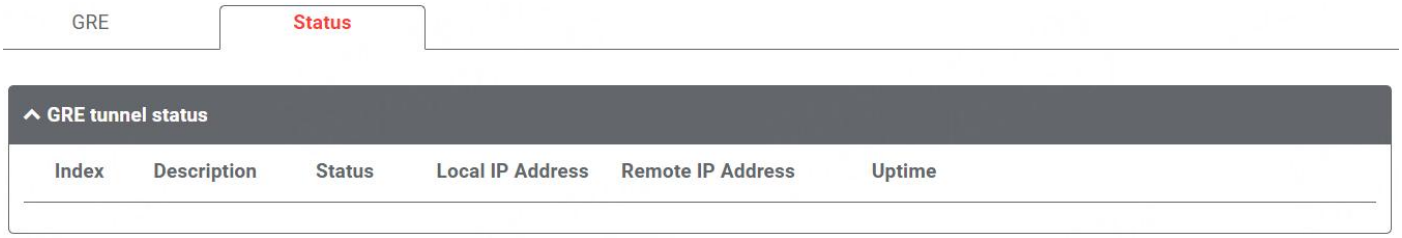


Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel. GRE (Generic Routing Encapsulation) is a protocol that encapsulates data packets so that it can route packets of other protocols in an IP network.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask/Prefix	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set the remote virtual IP Address of the GRE tunnel.	Null
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all the traffics of the router will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable/disable this option. This option must	OFF

	be enabled when router under NAT environment.	
Secrets	Set the key of the GRE tunnel.	Null
Link Binding	Set the specified interface of the GRE Tunnel	wwan

Status

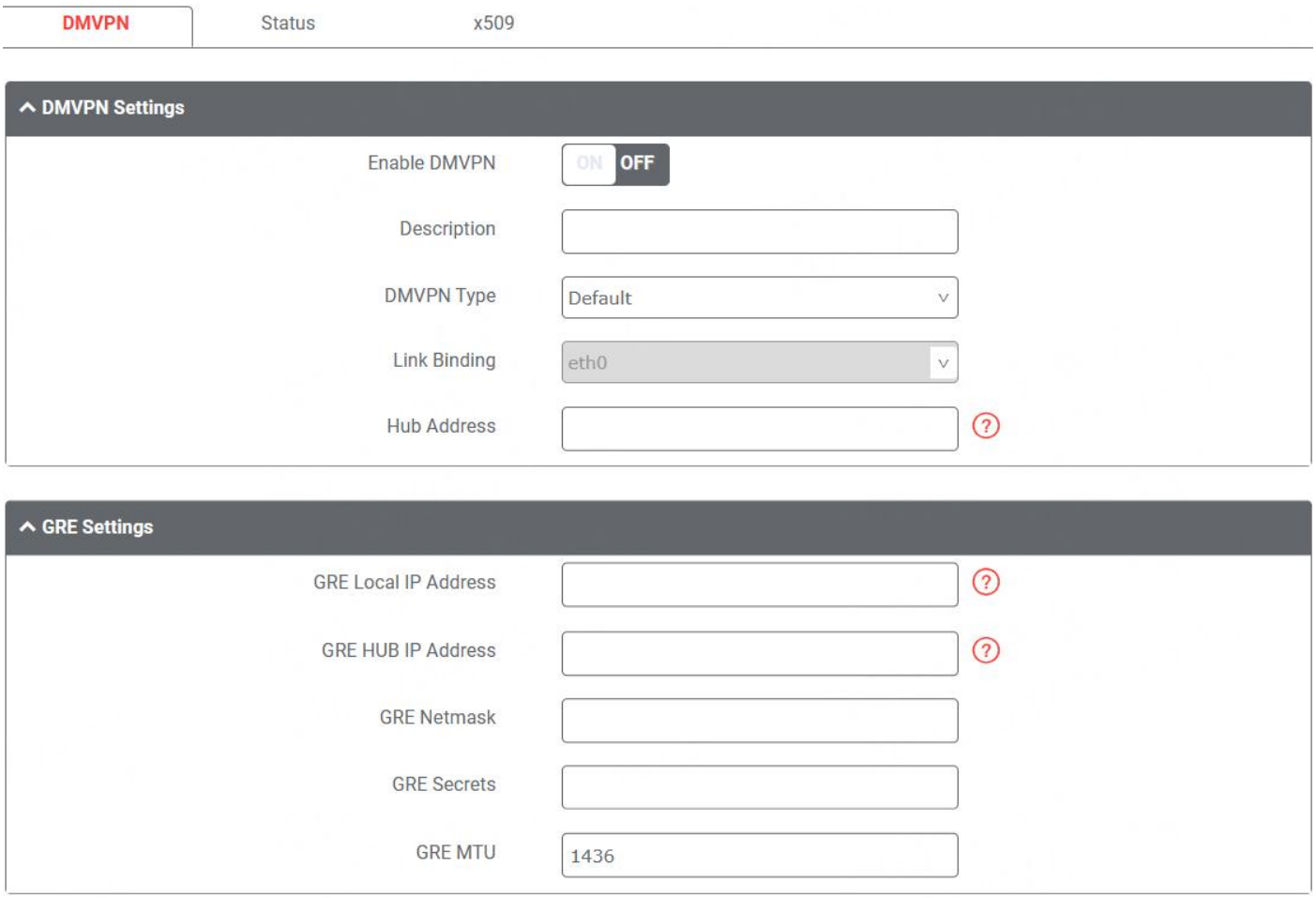
This section allows you to view the GRE tunnel status.



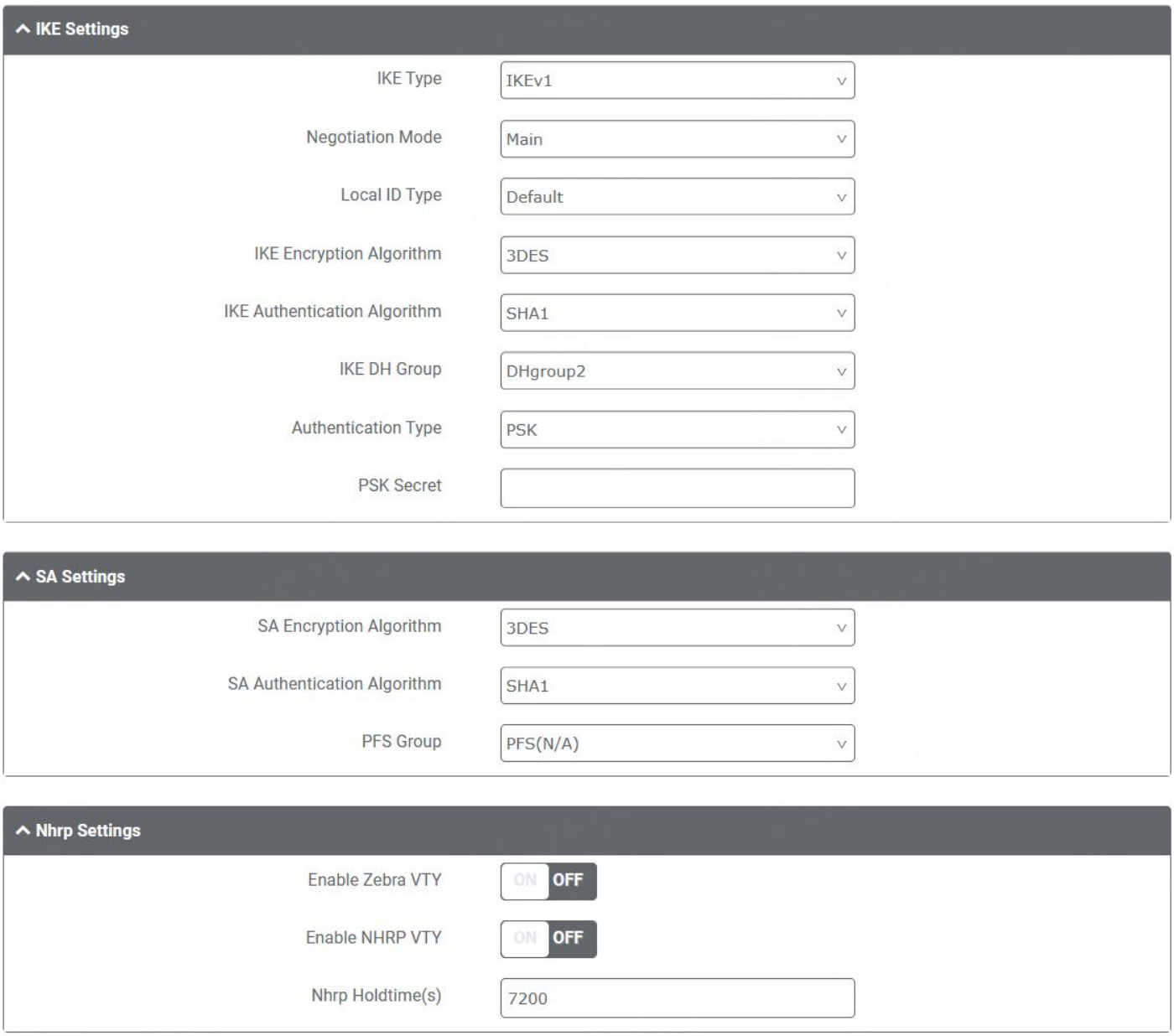
4.4.4 DMVPN

DMVPN is a routing technique we can use to build a VPN network with multiple sites without having to statically configure all devices. It is a hub and spoke network, where the spokes will be able to communicate with each other directly without having to go through the hub.

DMVPN



Item	Description	Default
Enable	Click the toggle button to enable/disable the DMVPN client.	OFF
Description	Enter a description for DMVPN client.	Null
DMVPN Type	Select DMVPN Type Default: Single hub mode Dual-hub: Dual hub mode	Default
Link Binding	Select a link binding with DMVPN	Null
Hub Address	Enter the DMVPN hub address. e.g. 172.16.8.198	Null
GRE Local IP Address	Enter local tunnel address, e.g. 182.16.0.1	Null
GRE HUB IP Address	Enter hub tunnel address, e.g. 182.16.0.100	Null
GRE Netmask	Enter tunnel netmask.	Null
GRE Secrets	Enter GRE tunnel secret key.	Null
GRE MTU	Enter the maximum transmission unit.	1436



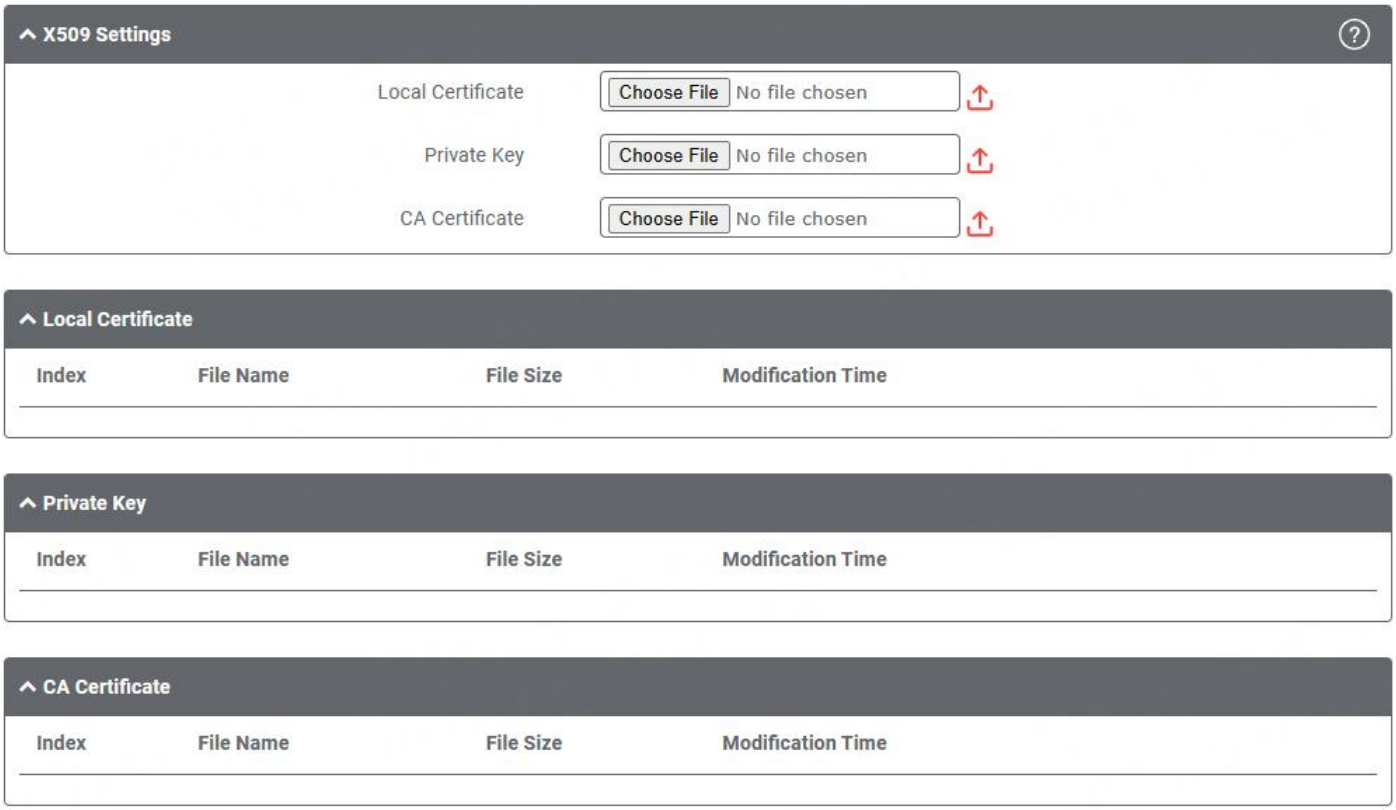
Item	Description	Default
IKE Type	Select IKE Type	IKEv1
Negotiation Mode	Select from “Main” and “aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Local ID Type	Select from “ID”, “FQDN” and “User FQDN” for IKE negotiation. “Default” stands for “Router’s extern IP”. ID: Uses custom string as the ID in IKE negotiation. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with an sign “@” for the local	Default

Item	Description	Default
	security gateway, e.g., test@robustel.com.	
IKE Encryption Algorithm	Select from “DES”, “3DES” and “AES128” to be used in IKE negotiation. DES: Uses the DES algorithm in CBC mode and 56-bit key. 3DES: Uses the 3DES algorithm in CBC mode and 168-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key.	3DES
IKE Authen Algorithm	Select from “MD5” and “SHA1”to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
IKE DH Group	Select from “MODP768_1”, “MODP1024_2” and “MODP1536_5”to be used in key negotiation phase 1. MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	MODP1024_2
Authentication Type	Select Authentication Type	PSK
PSK Secrets	Enter PSK secret key.	Null
SA Encryption Algorithm	Select the SA Encryption Algorithm from “DES”, “3DES”, “AES 128”, “AES 192”, “AES 256”.	3DES
SA Authentication Algorithm	Select the SA Authentication Algorithm from “MD5”, “SHA1”, “SHA2 256”, “SHA2 512”.	SHA1
PFS Group	Select the PFS Group.	PFS(N/A)

Status

The status bar allows to view DMVPN connection status.

X509



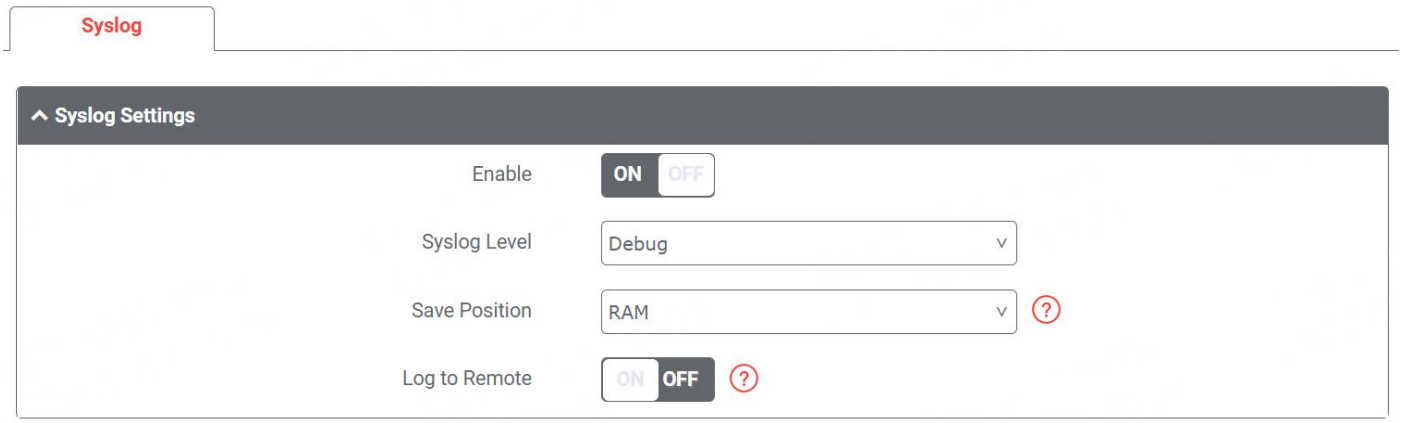
x509		
Item	**Description**	**Default**
X509 Settings		
Root CA	Click “Choose File” to locate Root CA file and then import this file into your device.	--
Certificate File	Click “Choose File” to locate Certificate file, and then import this file into your device.	--
Private Key	Click “Choose File” to locate Private Key file, and then import this file into your device.	--
Certificate Files		
Index	Indicate ordinal of list.	--
Filename	Show imported certificate’s name.	Null
File Size	Show size of certificate file.	Null
Modification Time	Show timestamp of that the last time to modify the certificate file.	Null

4.5 Services

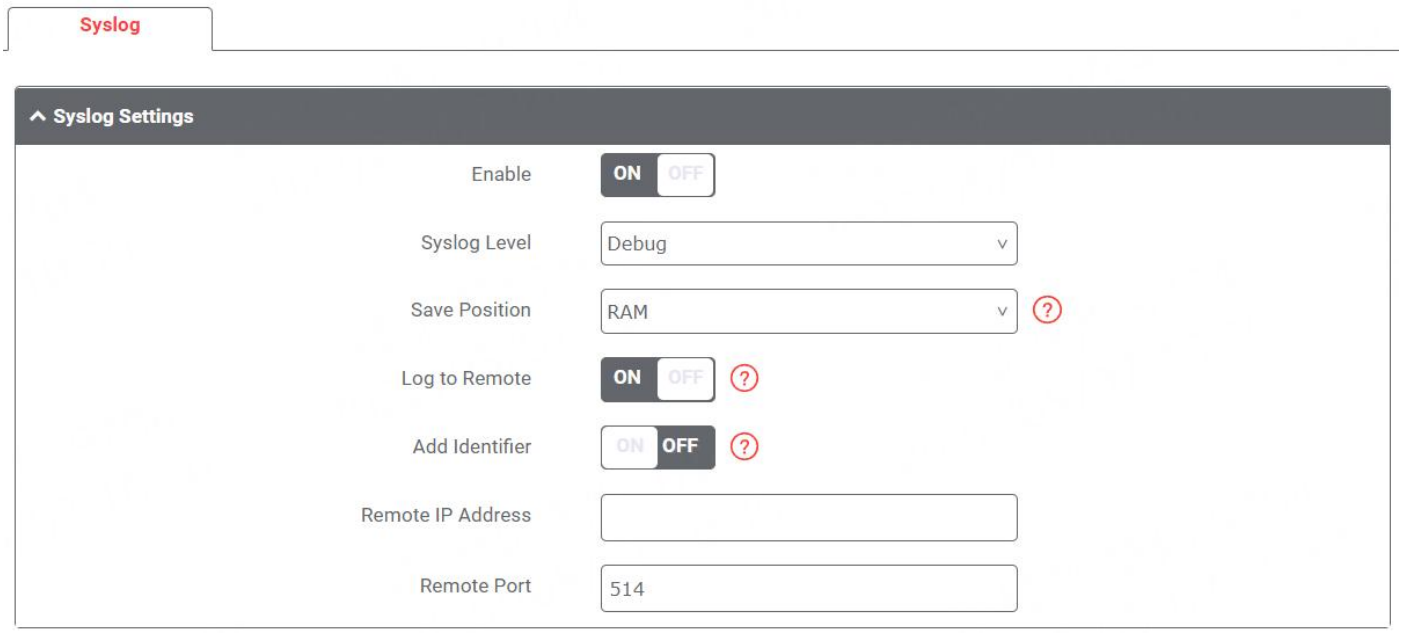
4.5.1 Syslog

This section allows you to set the syslog parameters. The system log of the router can be saved in the local, also

supports to be sent to remote log server and specified application debugging. By default, the “Log to Remote” option is disabled.



The window is displayed as below when enabling the “Log to Remote” option.

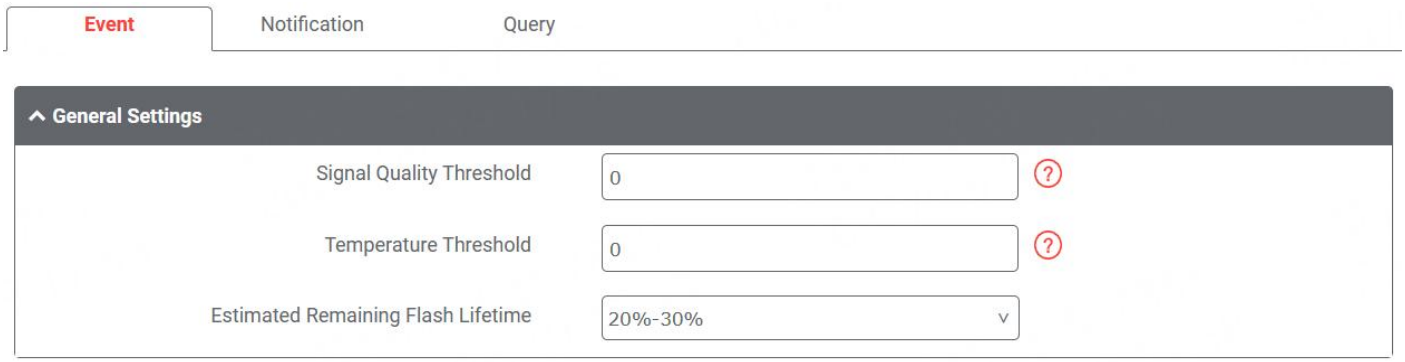


Item	Description	Default
Enable	Click the toggle button to enable/disable the Syslog settings option.	ON
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. The lower level will output more syslog in details.	Debug
Save Position	Select the save position from “RAM”, “NVM” or “Console”. The data will be cleared after reboot when choose “RAM”. **Note**: It's not recommended that you save syslog to NVM (Non-Volatile Memory) for a long time.	NVM
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	ON
Add Identifier	Click the toggle button to enable/disable this option. When enabled, you can add serial number to syslog message which used for loading Syslog to RCMS.	OFF
Remote IP Address	Enter the IP address of syslog server when enabling the “Log to Remote” option.	Null
Remote Port	Enter the port of syslog server when enabling the “Log to Remote” option.	514

4.5.2 Event

This section allows you to set the event parameters. Event feature provides an ability to send alerts by SMS or Email when certain system events occur.

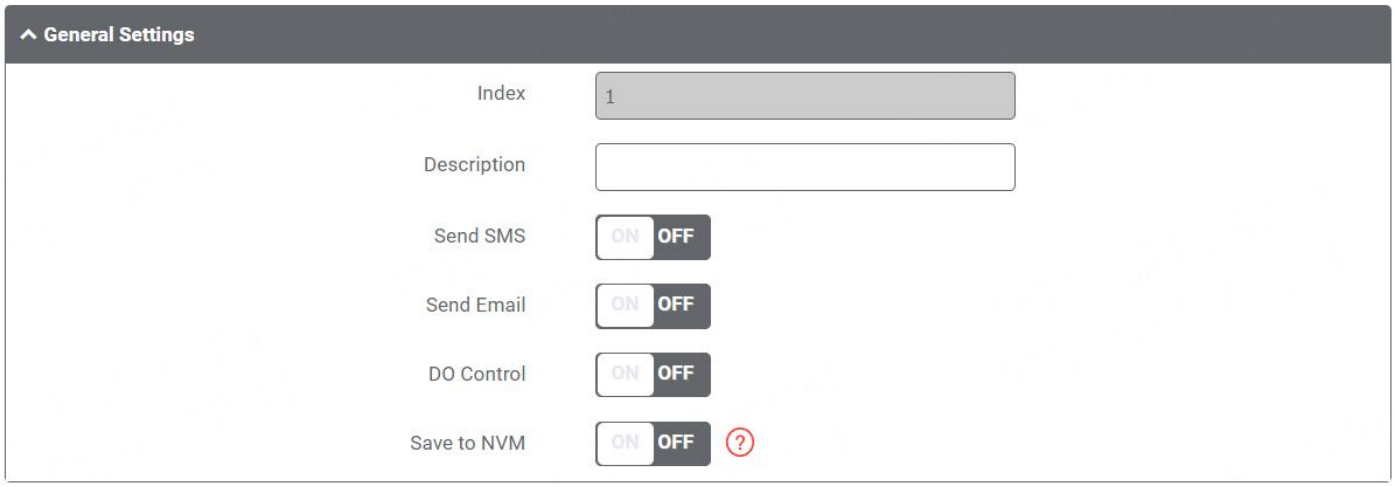
Event



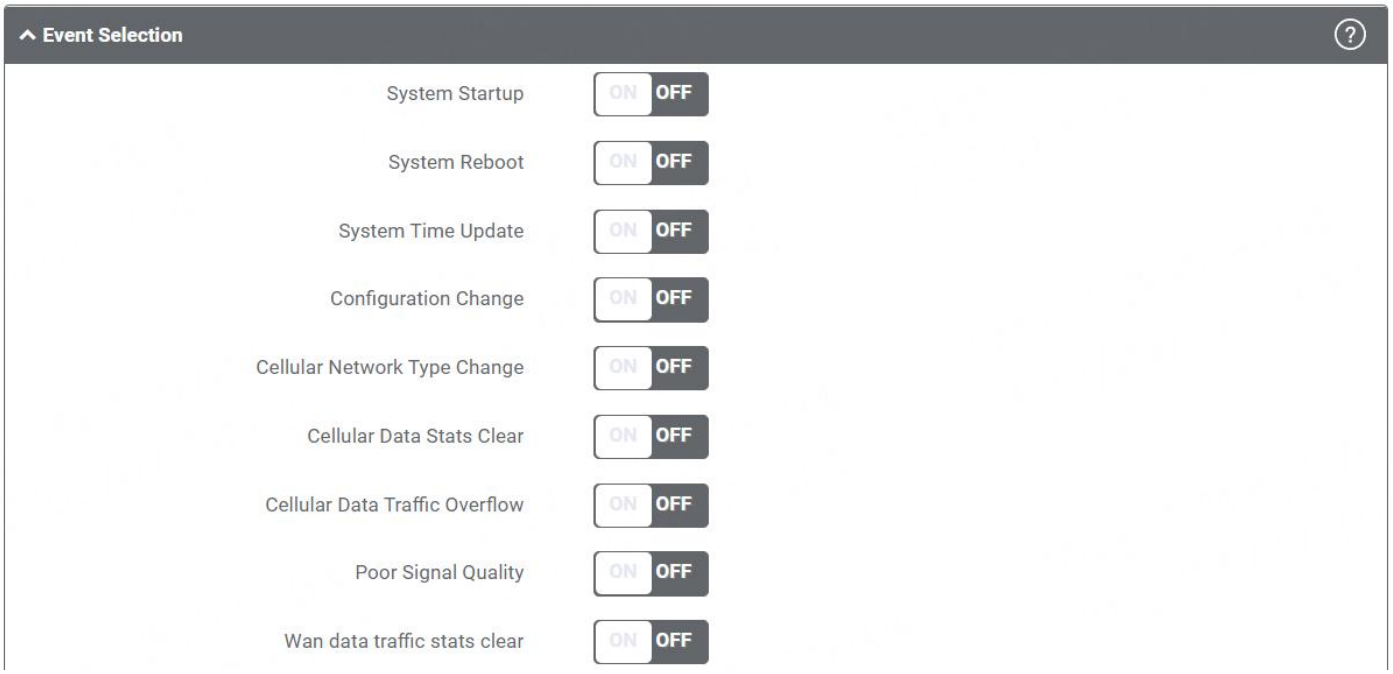
Item	Description	Default
Signal Quality Threshold	Set the threshold for signal quality. Device will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0
Temperature Threshold	Set the threshold for temperature. Device will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0
Estimate Remaining Flash Lifetime	Set the estimate of EMMC life. Device will generate a log event when the actual estimate is in the specified parameter range.	20%-30%

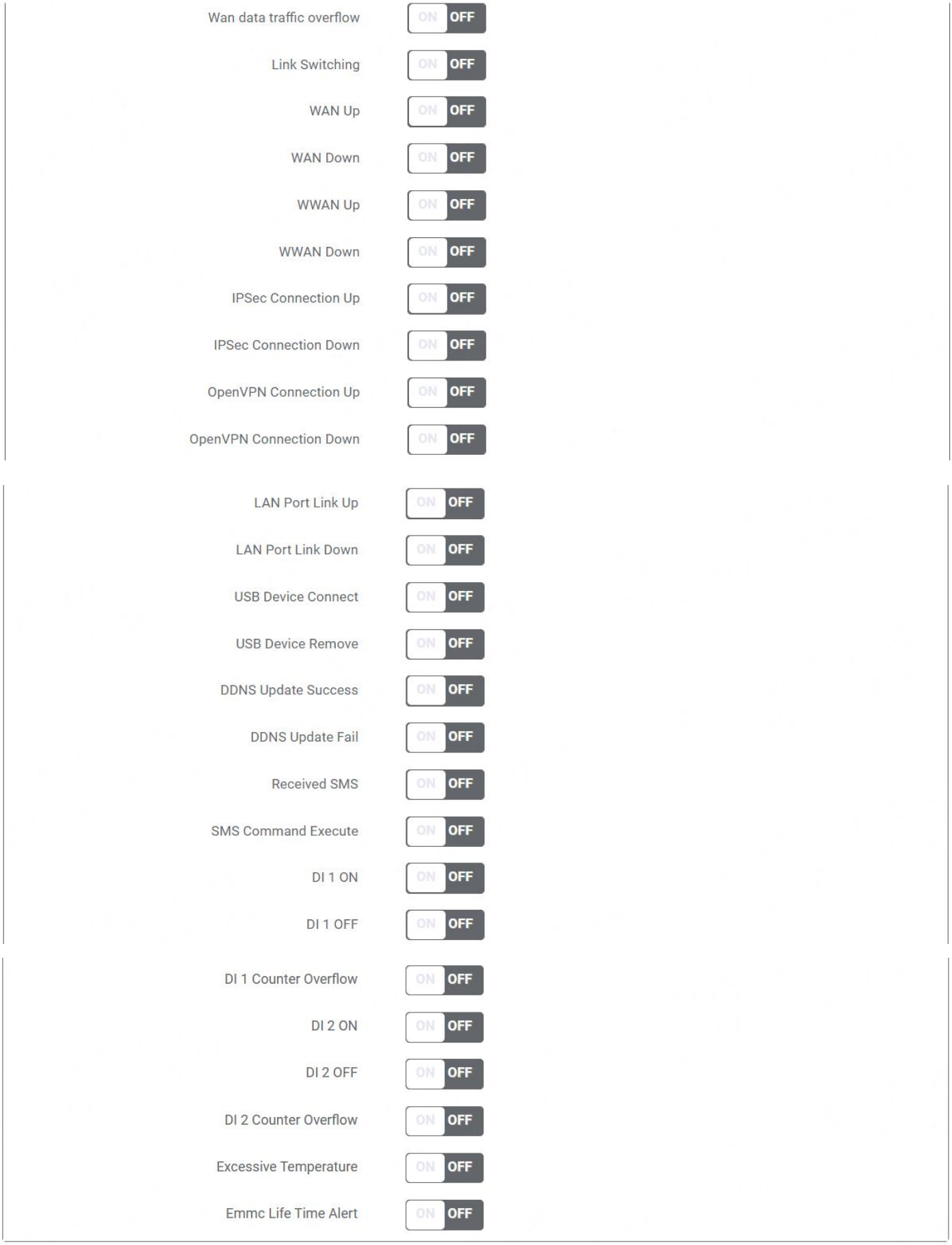
Notification

Click + button to add an Event parameters.



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in “3.21 Services > Email”, and use ‘;’to separate each number.	OFF
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified email box via Email if event occurs. Set the related email address in “3.21 Services > Email”.	OFF
DO Control	Click the toggle button to enable / disable this option. After it is turned on, the event router will send it to the corresponding DO in the form of Low / High level.	OFF
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

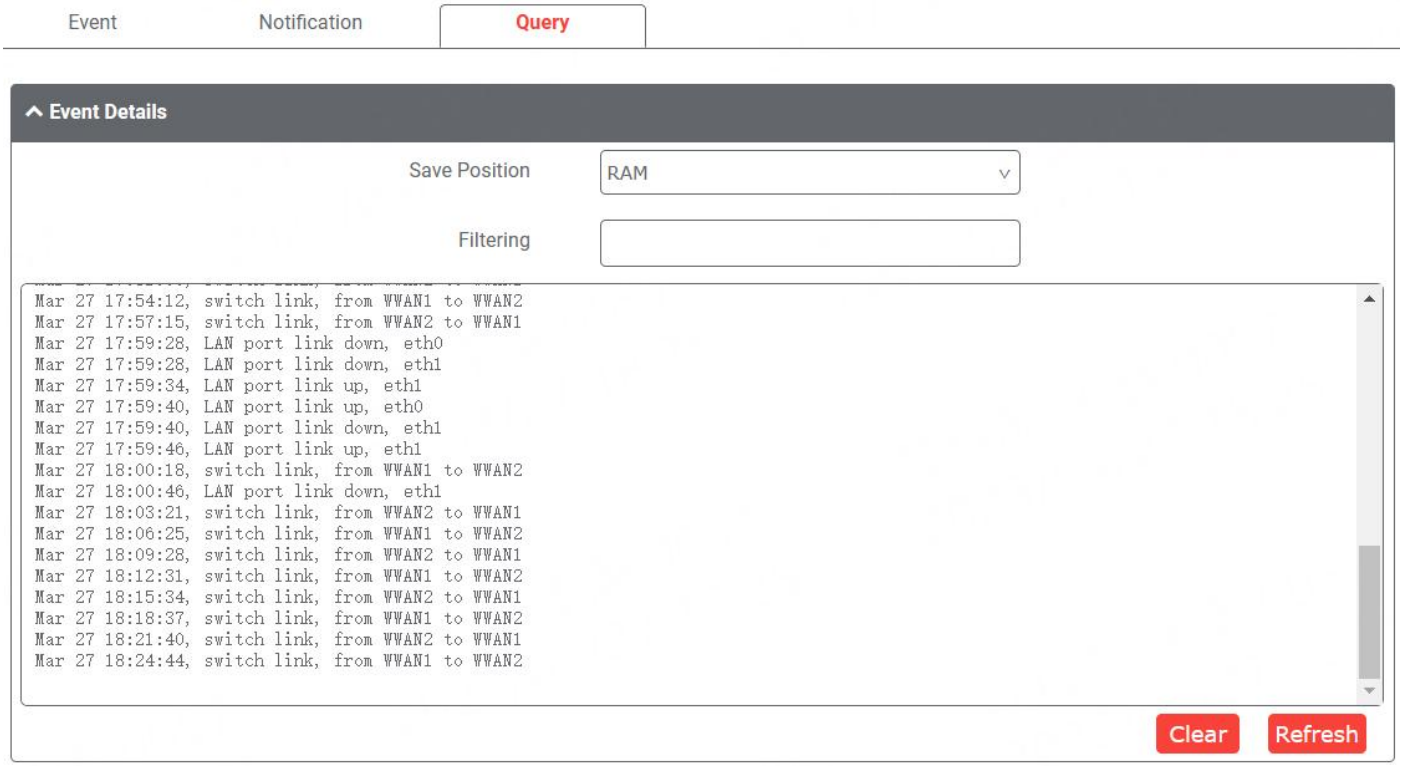



Wan data traffic overflow
Link Switching
WAN Up
WAN Down
WWAN Up
WWAN Down
IPSec Connection Up
IPSec Connection Down
OpenVPN Connection Up
OpenVPN Connection Down
LAN Port Link Up
LAN Port Link Down
USB Device Connect
USB Device Remove
DDNS Update Success
DDNS Update Fail
Received SMS
SMS Command Execute
DI 1 ON
DI 1 OFF
DI 1 Counter Overflow
DI 2 ON
DI 2 OFF
DI 2 Counter Overflow
Excessive Temperature
Emmc Life Time Alert
ON
OFF

Item	Description	Default
Event	Click the toggle button to enable this option to generate a log.	OFF

Query

In the following window you can query various types of events record. Click Refresh to query filtered events while click Clear to clear the event records in the window.

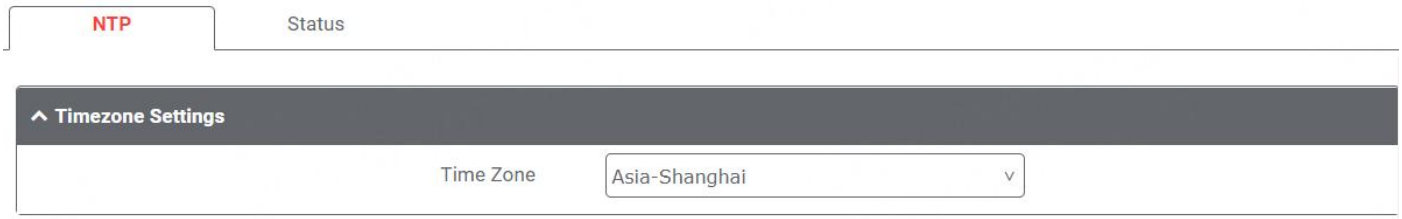


Item	Description	Default
Save Position	Select the events' save position from "RAM" or "NVM". • RAM: Random-access memory • NVM: Non-Volatile Memory	NVM
Filtering	Enter the filtering message based on the keywords set by users. Click the "Refresh" button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1&message2.	Null

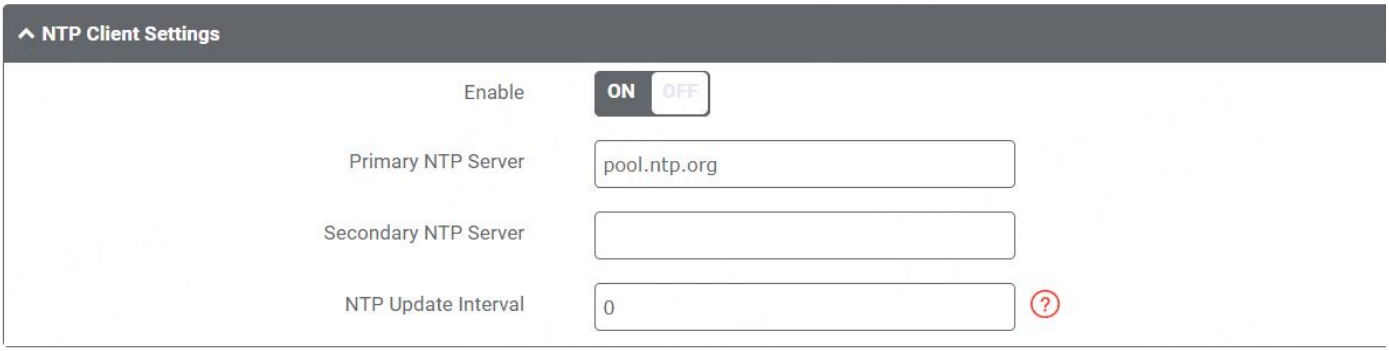
4.5.3 NTP

This section allows you to set the related NTP (Network Time Protocol) parameters.

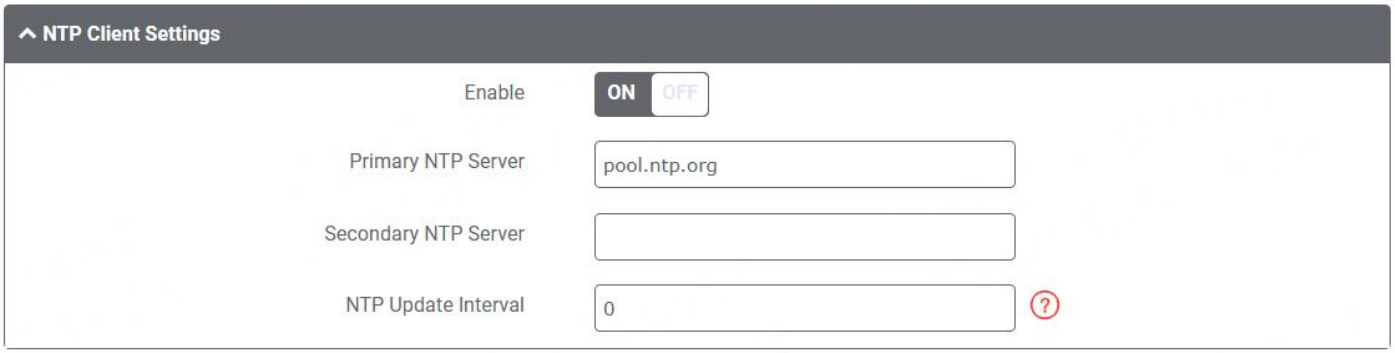
NTP



Item	Description	Default
Time Zone	Click the drop down list to select the time zone you are in.	UTC +08:00



Item	Description	Default
Enable	Click the toggle button to enable/disable this option. Enable to synchronize time with the NTP server.	ON
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null
NTP Update interval	Enter the interval (minutes) synchronizing the NTP client time with the NTP server's. Minutes wait for next update, and 0 means update only once.	0

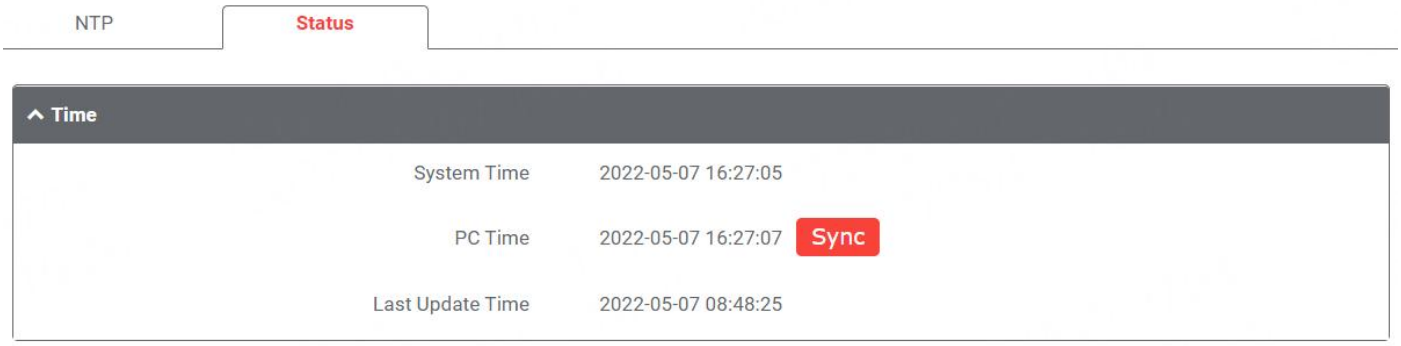


Item	Description	Default
Enable	Click the toggle button to enable/disable the NTP server option.	OFF
Primary NTP Server	Enter the primary NTP server	pool.ntp.org
Secondary NTP Server	Enter the secondary NTP server	Null
NTP Update Interval	Enter the NTP update interval, 0 means update only once.	0

Item	Description	Default
Enable	Click the toggle button to enable/disable the NTP server option.	OFF

Status

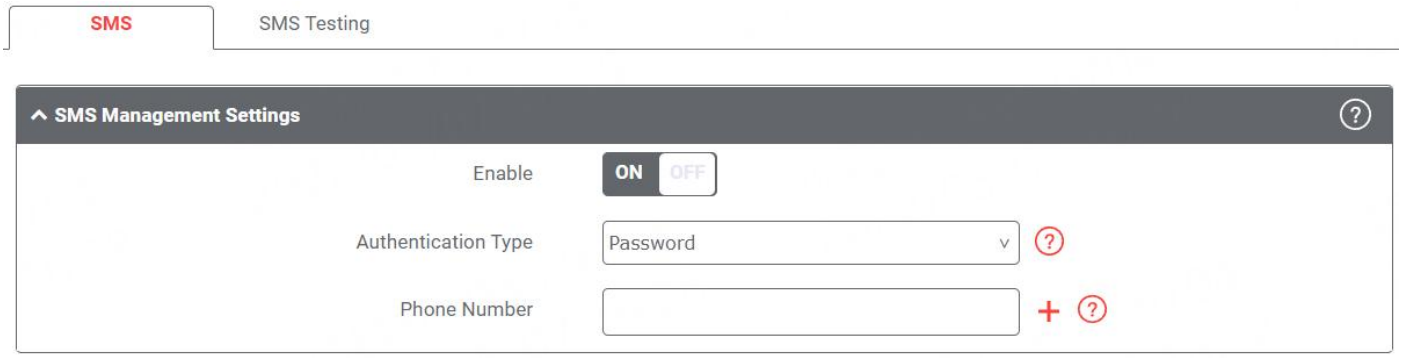
This window allows you to view the current time of router and also synchronize the router time. Click Sync button to synchronize the router time with the PC's time.



4.5.4 SMS

This section allows you to set SMS parameters. Device supports SMS management, and user can control and configure their devices by sending SMS. For more details about SMS control, refer to **4.1.2 SMS Remote Control**.

SMS

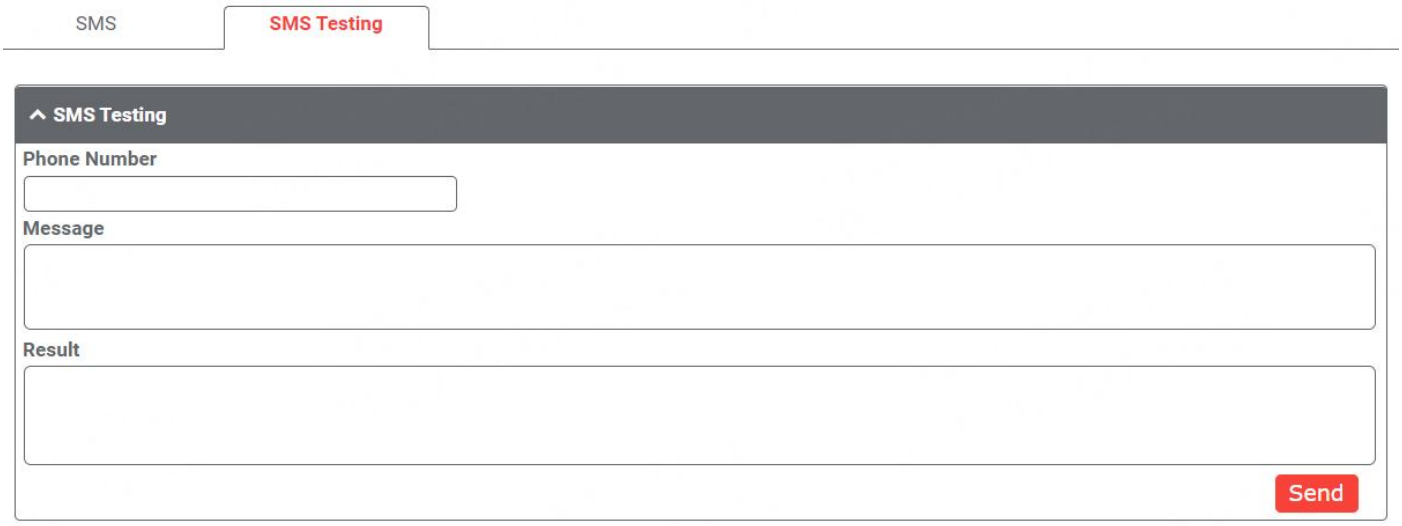


Item	Description	Default
Enable	Click the toggle button to enable/disable the SMS Management option. **Note**: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from "Password", "Phonenum" or "Both".	Password

	Password: Use the same username and password as WEB manager for authentication. For example, the format of the SMS should be "username: password; cmd1; cmd2; …" Note: Set the WEB manager password in System > User Management section. Phonenum: Use the Phone number for authentication, and user should set the Phone Number that is allowed for SMS management. The format of the SMS should be "cmd1; cmd2; …" Both: Use both the "Password" and "Phonenum" for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be "username: password; cmd1; cmd2; …"	
Phone Number	Set the phone number used for SMS management, and click + to add new phone number. ***Note:*** *It can be null when choose "Password" as the authentication type.*	Null

SMS Testing

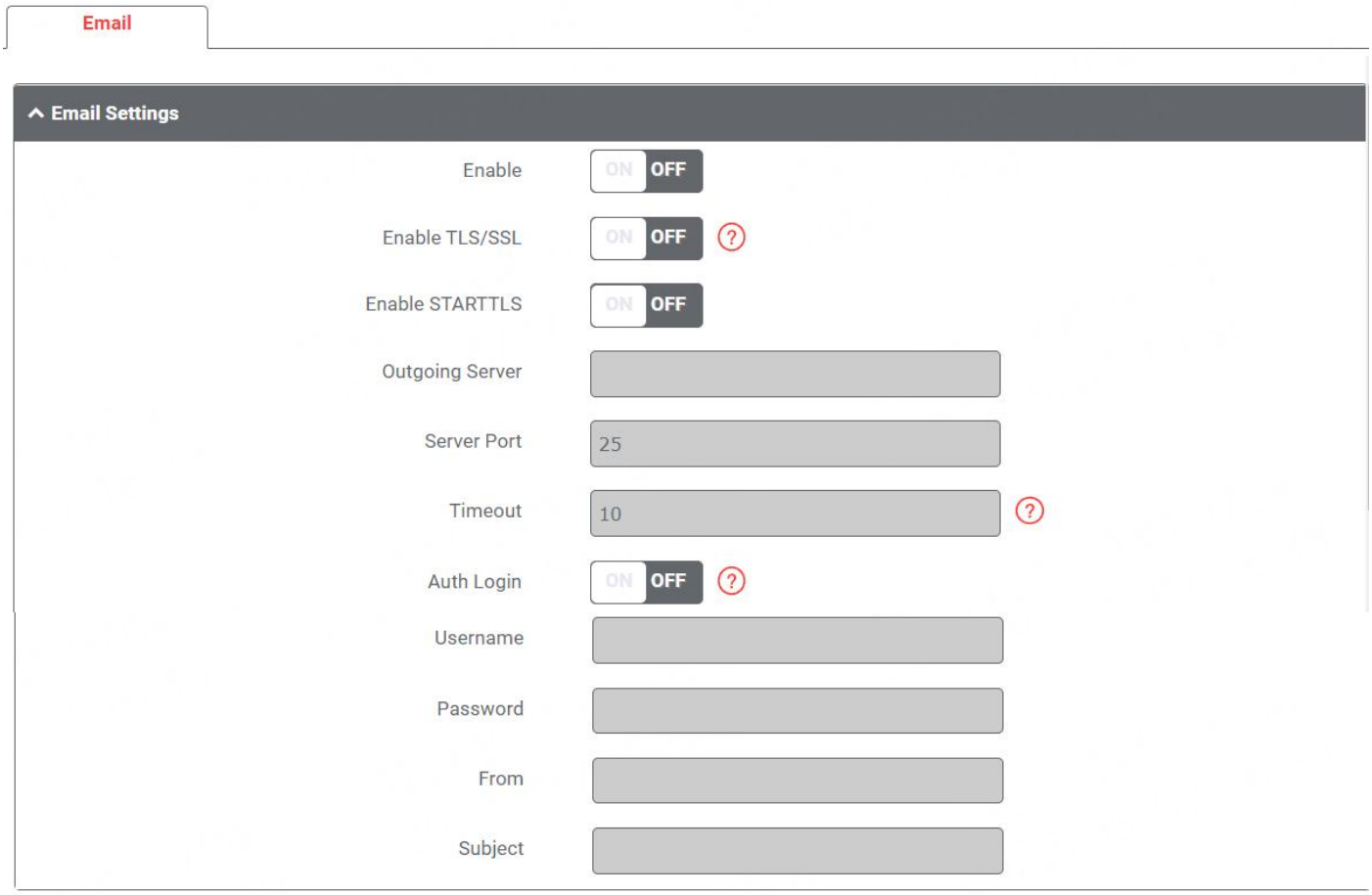
User can test the current SMS service whether it is available in this section.



Item	Description	Default
Phone Number	Enter the specified phone number which can receive the SMS from router.	Null
Message	Enter the message that router will send it to the specified phone number.	Null
Result	The result of the SMS test will be displayed in the result box.	Null
Send	Click the button to send the test message.	--

4.5.5 Email

Email function supports to send the event notifications to the specified recipient by ways of email.



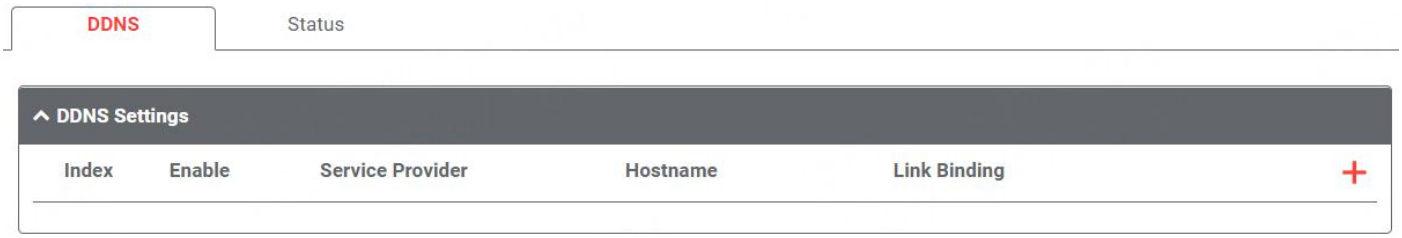
Item	Description	Default
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Enable STARTTLS	Click the toggle button to enable / disable STARTTLS encryption.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
Server port	Enter the SMTP server port.	25
Timeout	Set the max time for sending email to SMTP server. When the server doesn't receive the email over this time, it will try to resend.	10
Auth Login	If the mail server supports AUTH login, you must enable this button and set a username and password.	OFF
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

4.5.6 DDNS

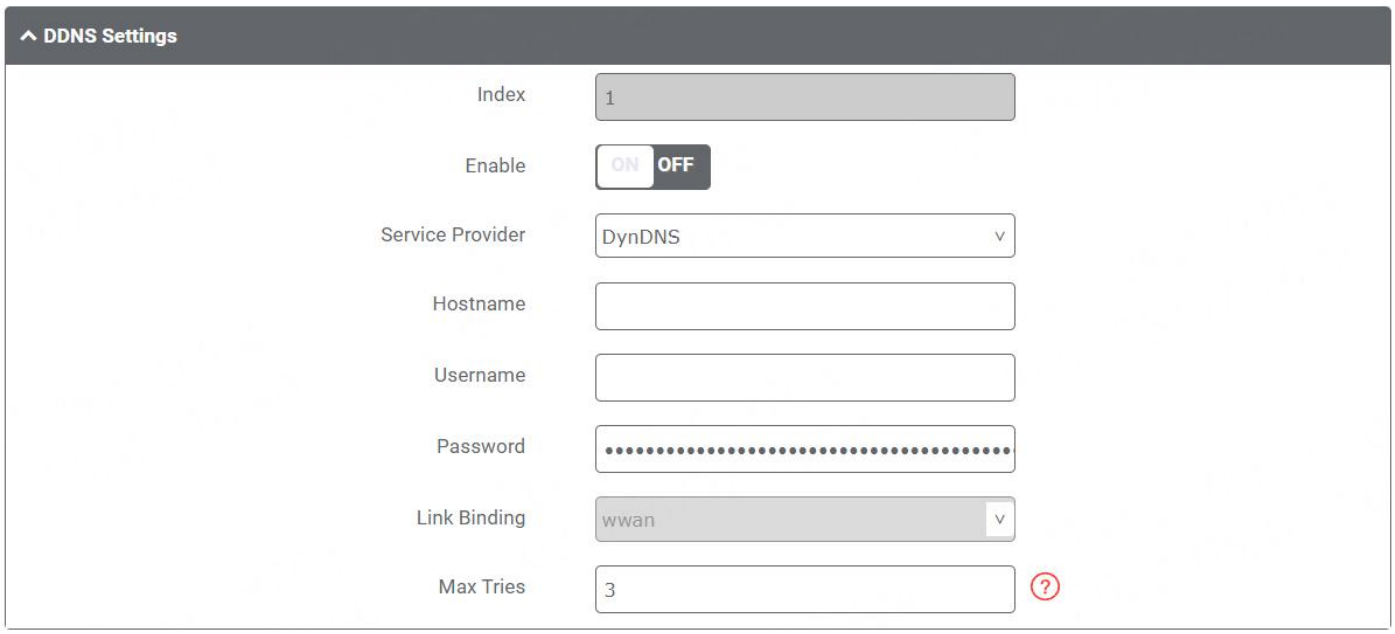
This section allows you to set the DDNS parameters. The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows you whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may

use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP. The service provider defaults to “DynDNS”, as shown below.

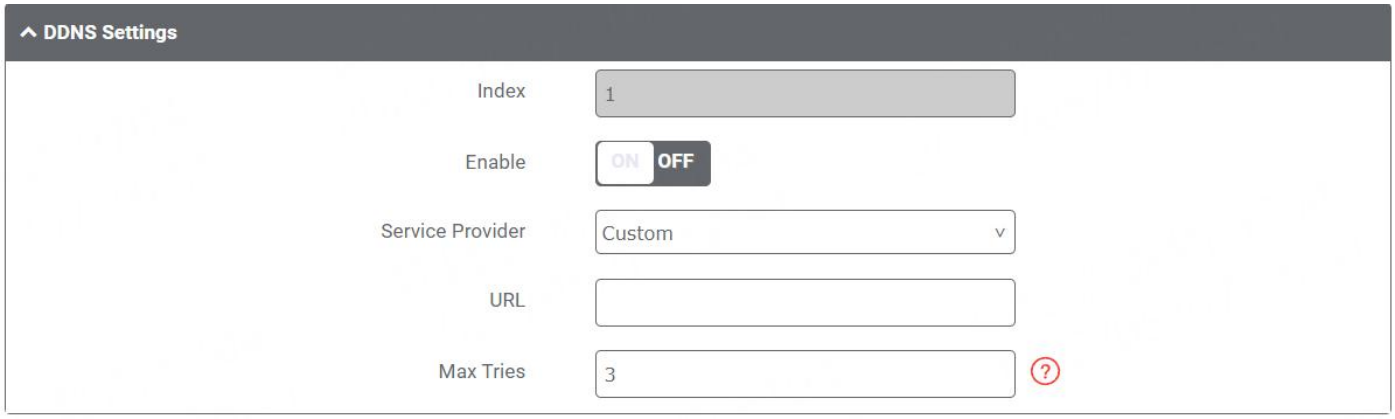
DDNS



Click + to add a new Dynamic Domain Name Server.



When “Custom” service provider chosen, the window is displayed as below.

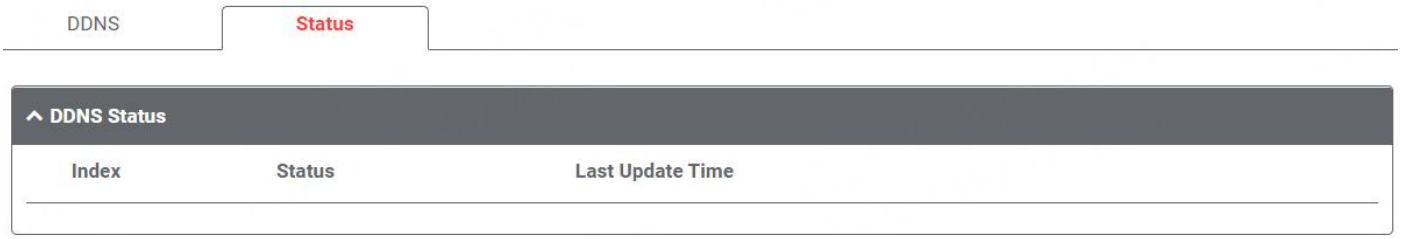


Item	Description	Default
Enable	Click the toggle button to enable/disable the DDNS option.	OFF

Service Provider	Select the DDNS service from “DynDNS”, “NO-IP”, “3322” or “Custom”. **Note:** The DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the hostname provided by the DDNS server.	Null
Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null
Max tries	Enter the maximum tries times	3

Status

The status bar allows to view DDNS connection status.

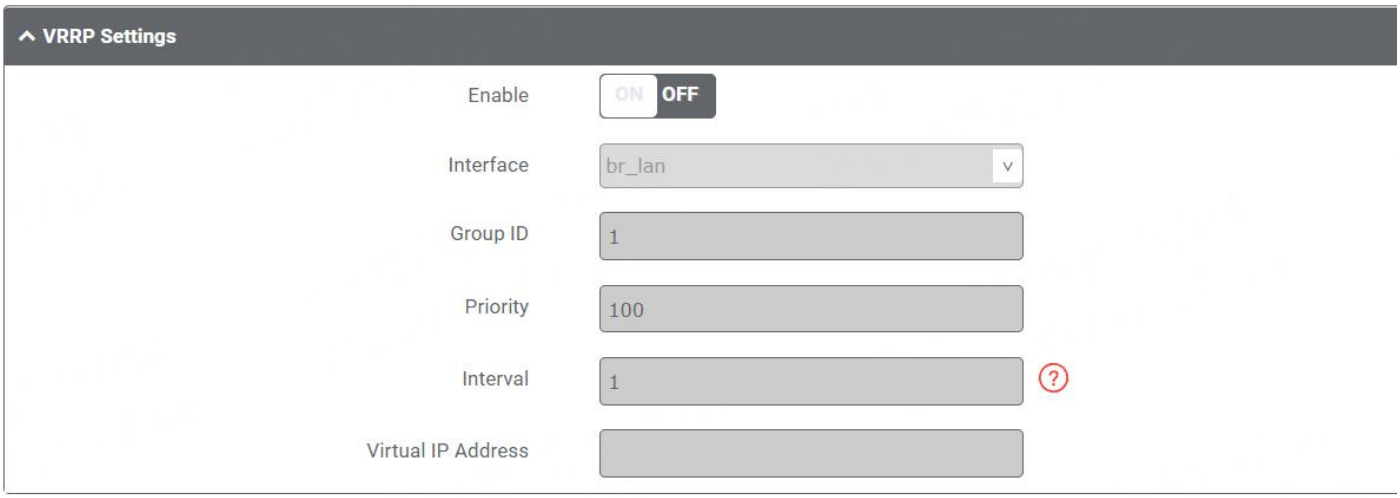


Item	Description
Status	Display the current status of the DDNS.
Last Update Time	Display the date and time for the DDNS was last updated successfully.

4.5.7 VRRP

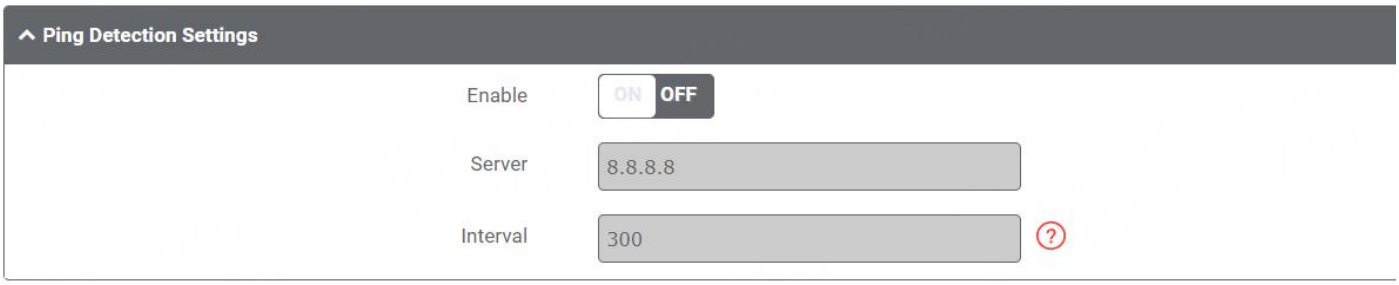
This section allows you to set the VRRP parameters. VRRP stands for Virtual Router Redundancy Protocol, is a standard for device redundancy and failover that creates a virtual router with a floating IP address.

VRRP Settings



Item	Description	Default
Enable	Click the toggle button to enable/disable the VRRP option.	OFF
Interface	Selects which interface VRRP will operate on.	--
Group ID	The Virtual Router Identifier. Routers with identical IDs will be grouped in the same VRRP cluster.	1
Priority	VRRP priority of the virtual router. Higher values equal higher priority.	100
Interval	Interval value in second, must be the same for all routing platforms in the VRRP group.	1
Virtual IP Address	Virtual IP address for the router's VRRP cluster.	Null

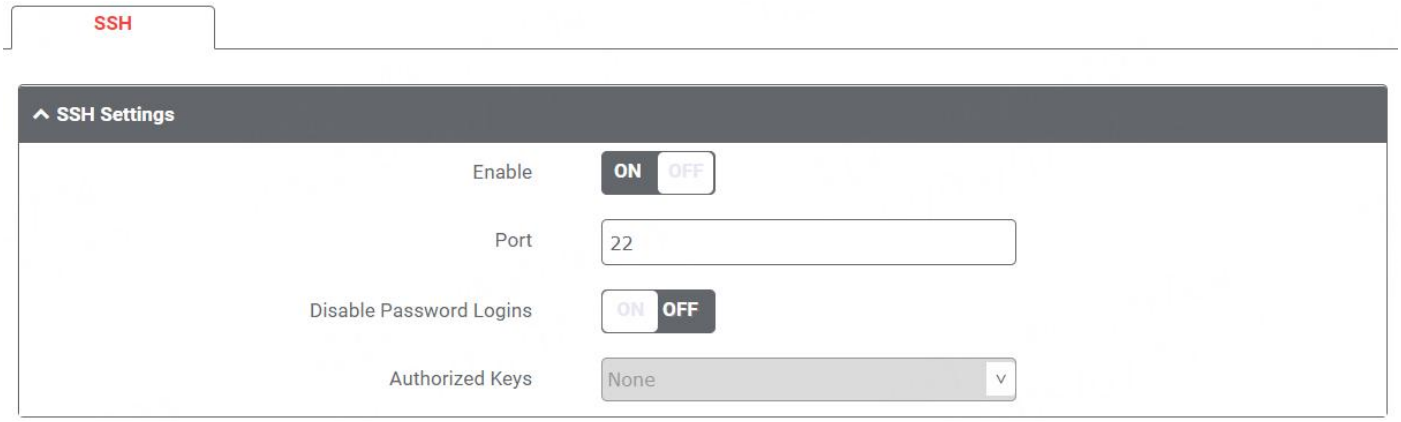
Ping Detection Settings



Item	Description	Default
Enable	Click the toggle button to enable/disable the option.	OFF
Server	The ping detection sever address.	8.8.8.8
Interval	Interval value for ping detection in second.	300

4.5.8 SSH

Device supports SSH password access and secret-key access.

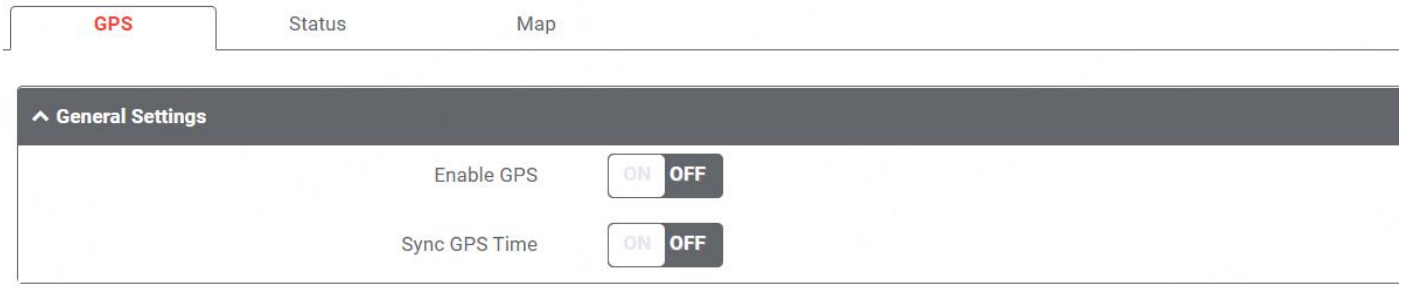


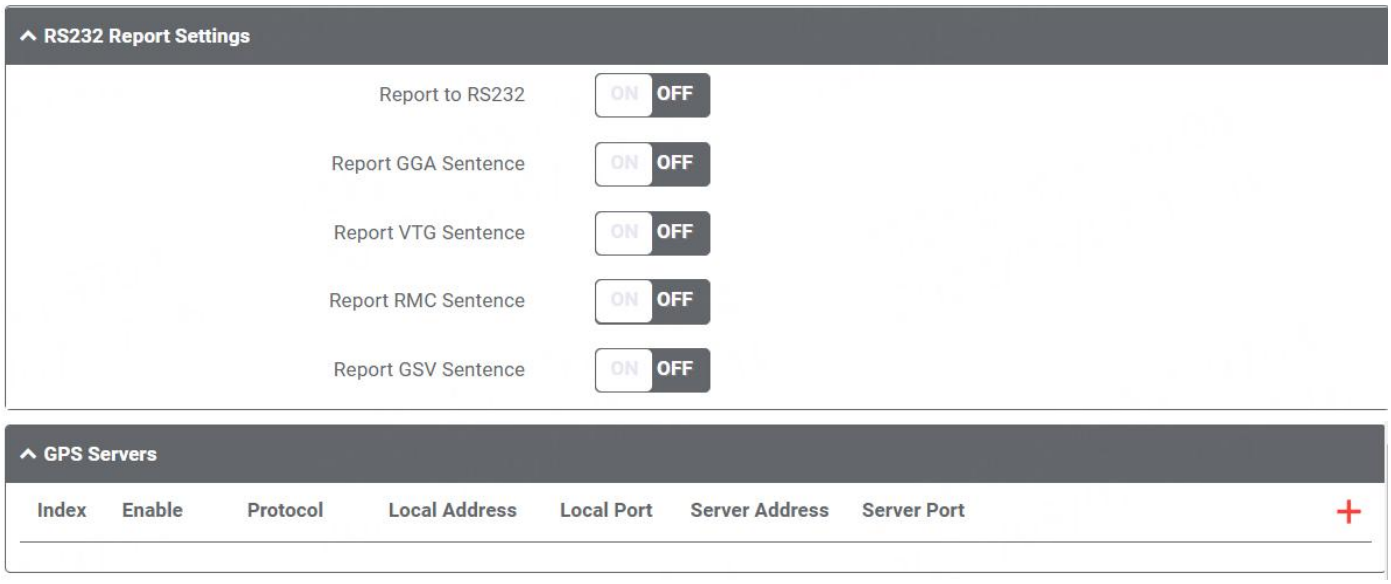
Item	Description	Default
Enable	Click the toggle button to enable/disable this option. When enabled, you can access the router via SSH.	ON
Port	Set the port of the SSH access.	22
Disable Password Logins	Click the toggle button to enable/disable this option. When enabled, you cannot use username and password to access the router via SSH. In this case, only the key can be used for login.	OFF

4.5.9 GPS

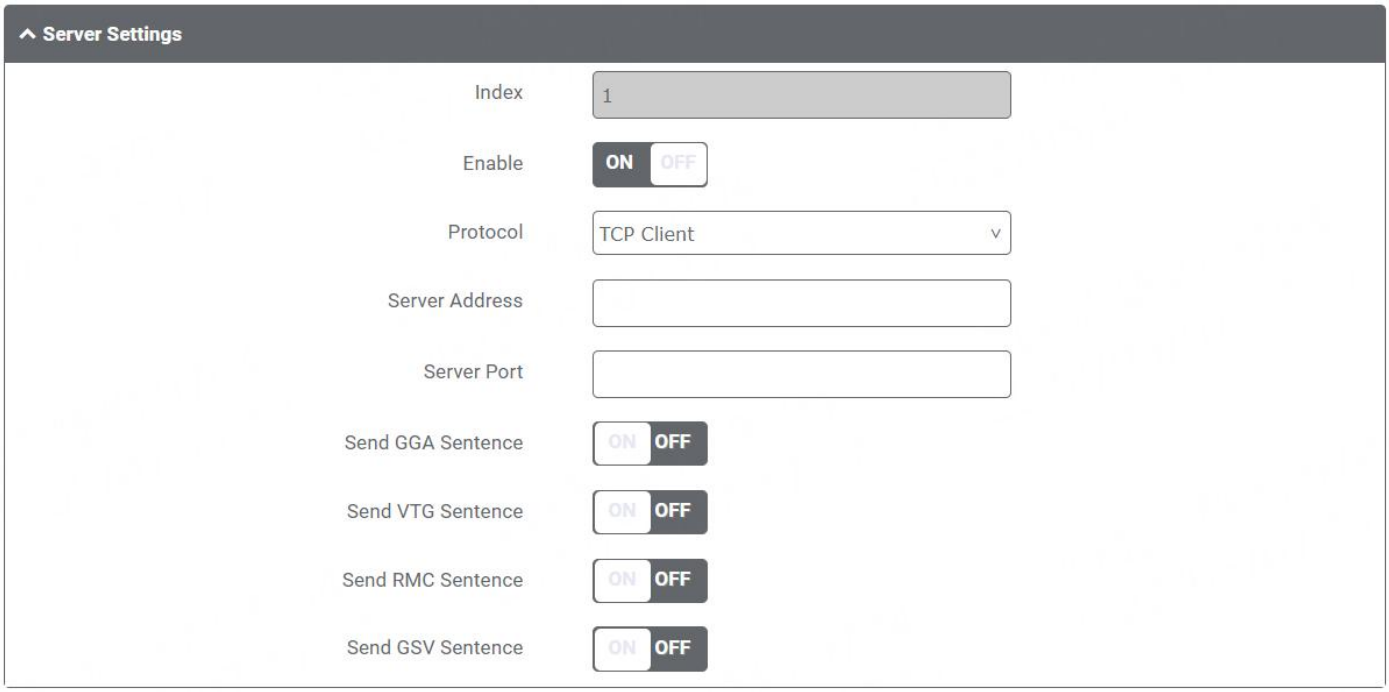
This section is used to configure the parameters of GPS. The GPS function of device can locate and acquire the location information of the device and report it to the designated server.

GPS





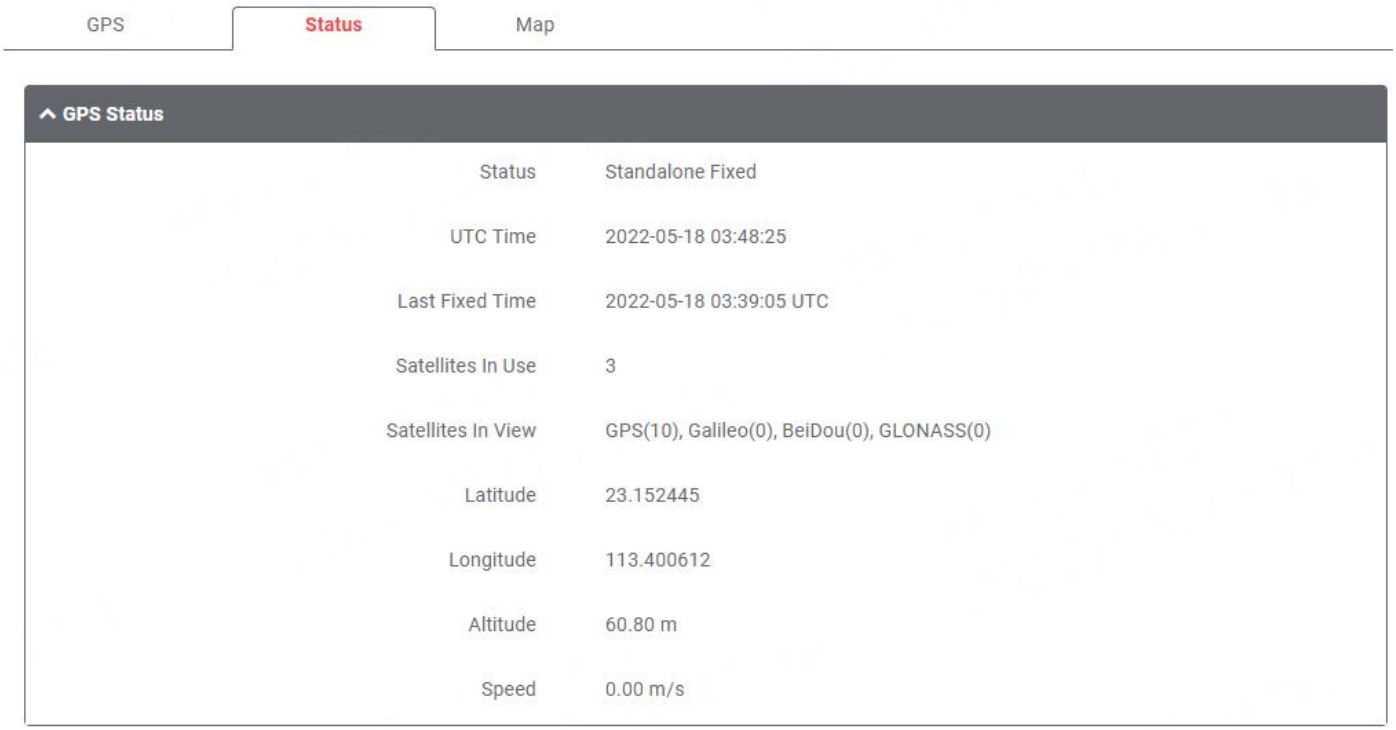
Click + to add a new GPS Server. The maximum count is **5.**



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable the server.	ON
Protocol	Select from “TCP Client”, “TCP Server”, “UDP”.	TCP Client
Server/Local Address	Server or local IP address.	Null
Server/Local Port	Server or local IP port.	Null
Send GGA Sentence	Click the toggle button to enable/disable this option.	OFF
Send VTG Sentence	Click the toggle button to enable/disable this option.	OFF
Send RMC Sentence	Click the toggle button to enable/disable this option.	OFF
Send GSV Sentence	Click the toggle button to enable/disable this option.	OFF

Item	Description	Default
Add SN as GPSID	Click the toggle button to enable/disable this option.	OFF
Self-define GPSID Prefix	Self-define GPSIS Prefix, four upper case.	Null

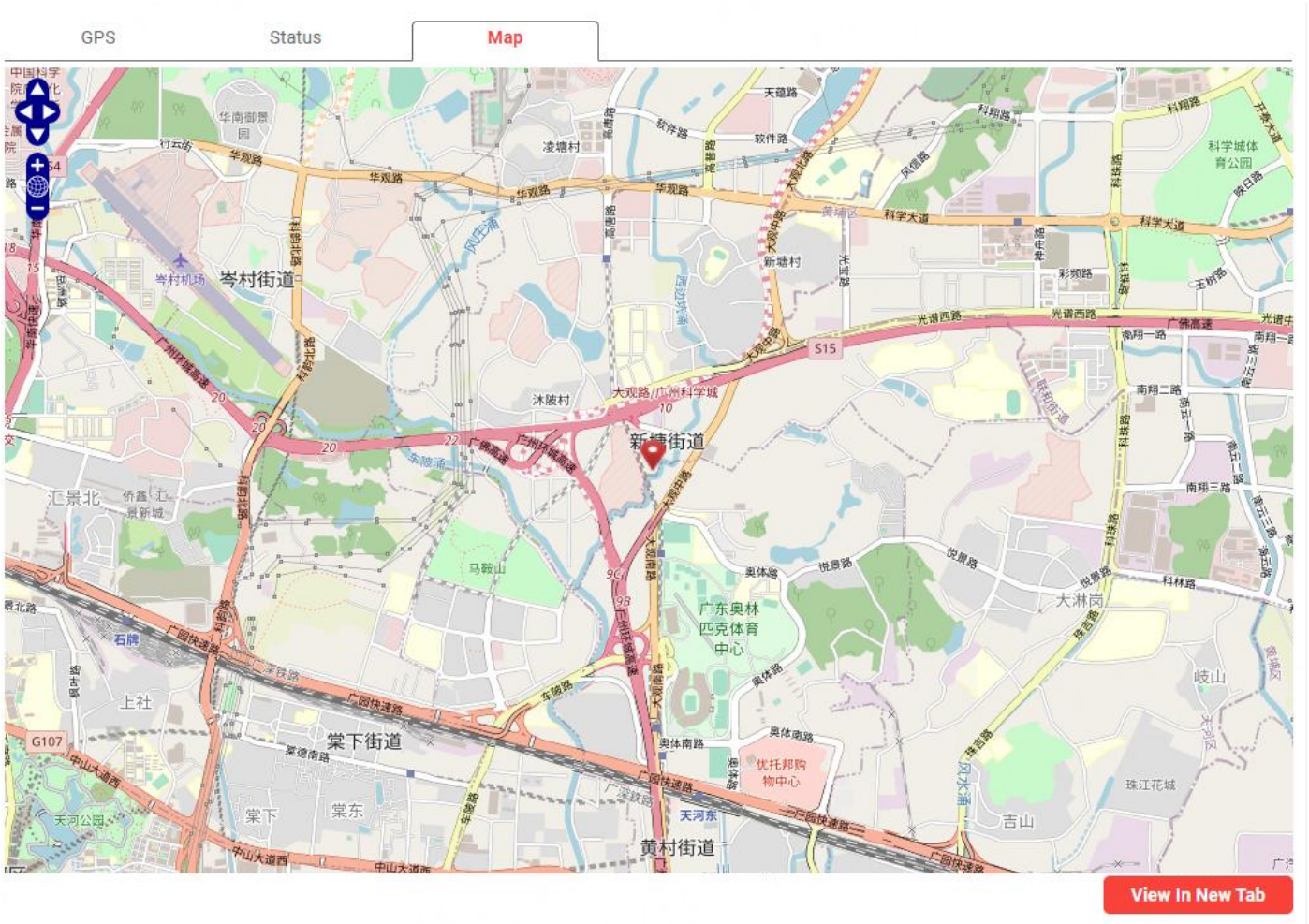
Status



Item	Description
Status	Shows the current GPS status of the router.
UTC Time	Shows the UTC of satellite. ***Note:*** *UTC is the world's unified time, not local time.*
Last Fixed Time	The time of the last successful positioning.
Satellites In Use	Number of satellites used
Satellites In View	Number of visible satellites
Latitude	Shows the Latitude information of the router.
Longitude	Shows the longitude information of the router.
Altitude	Shows the height information of the router.
Speed	Shows the speed information of the router.

Map

The Map page displays the device's current coordinates and position on the map. To see the device's location on the map, make sure to attach the GPS antenna on the device and enable GPS in the GPS page.

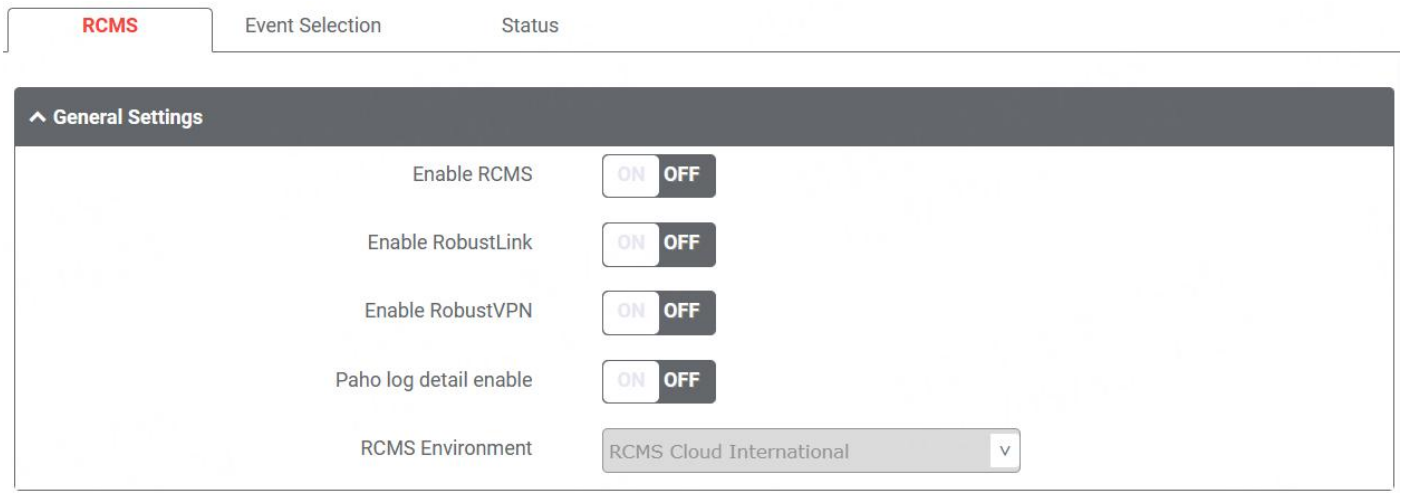


Click the View In New Tab button to view in a new tab.

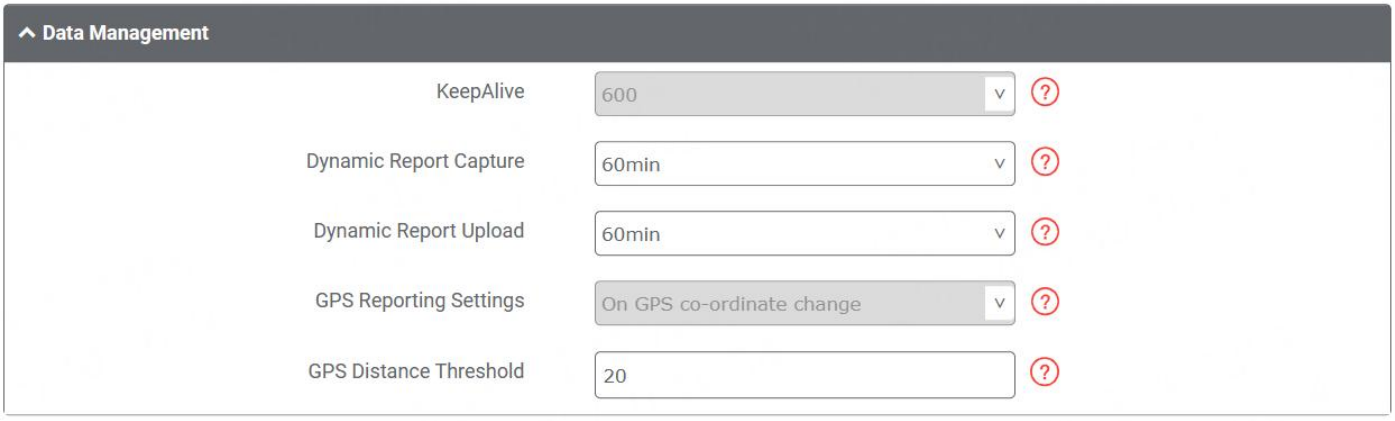
4.5.10 RCMS

This section allows you to set the RCMS parameters. Robustel Cloud Manager Service (RCMS) is a modular IoT cloud software platform compatible with all Robustel products.

RCMS



Item	Description	Default
Enable RCMS	Click the toggle button to enable/disable this option.	OFF
Enable RobustLink	Click the toggle button to enable/disable this option.	OFF
Enable RobustVPN	Click the toggle button to enable/disable this option.	OFF
Paho log detail enable	Click the toggle button to enable/disable this option.	OFF
RCMS Environment	Select RCMS Environment	RCMS Cloud International



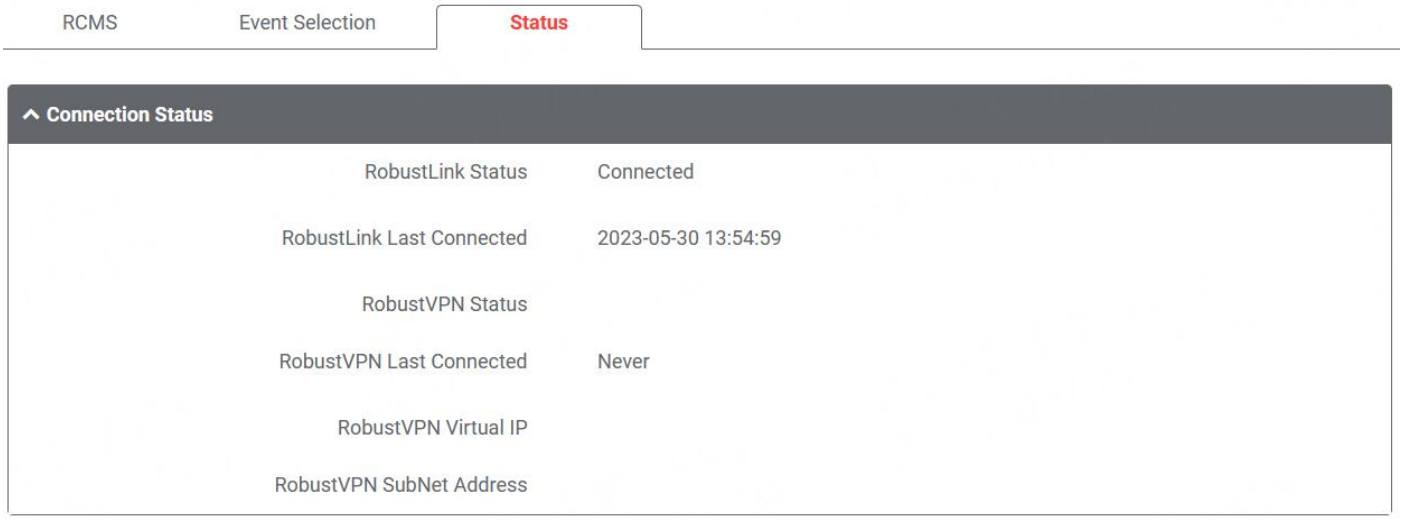
Item	Description	Default
KeepAlive	KeepAlive determines how long your device checks in with RCMS. A shorter KeepAlive will update RCMS more frequently but consume more data.	600

Dynamic Report Capture	Select the capture period of dynamic data is logged in the device	60min
Dynamic Report Upload	Select the upload period of dynamic data is update in the device	60min
GPS Reporting Settings	Select GPS Reporting way: - On GPS co-ordinate change - Report when GPS is updated - Only with Dynamic Report - Collect and report in sync with the Data Collection Interval and Data Reporting Frequency	On GPS co-ordinate change
GPS Distance Threshold	GPS data will be updated when the current position exceeds this value; Unit:meters Valid Range:10-10000	20

Item	Description	Default
Enable Ping	Click the toggle button to enable/disable this option.	OFF
Primary Server	Enter the ping server.	8.8.8.8
Ping Timeout	Enter the time of waiting for a ping response. Unit: seconds	5
Ping Count	Enter the number of pings conducted to calculate average.	3

Event Selection

Status

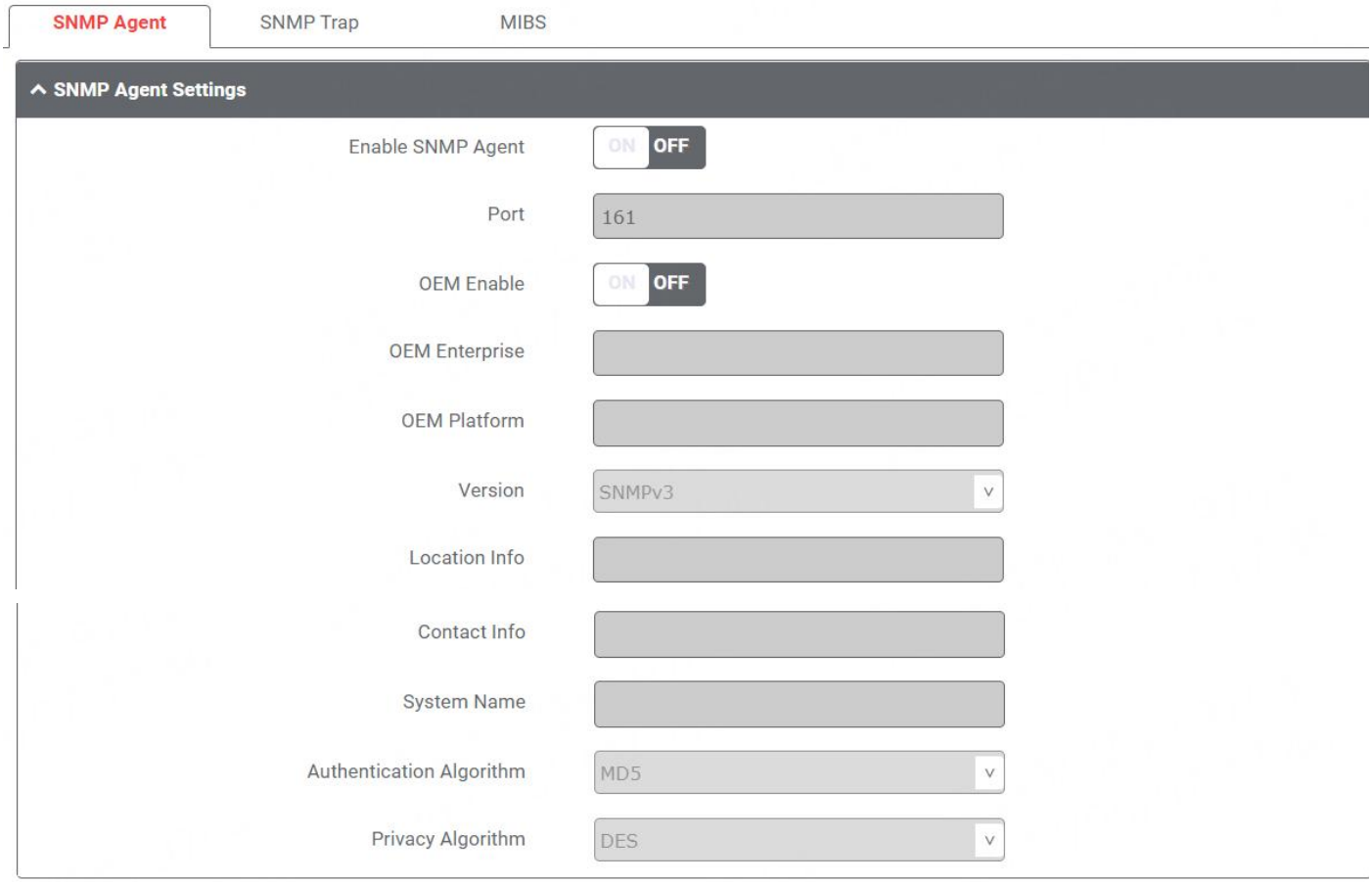


Item	Description
RobustLink Status	Show the status of RobustLink
RobustelLink Last Connected	Show the last connected times of RobustLink
RobustVPN Status	Show the status of RobustVPN
RobustVPN Last Connected	Show the last connected times of RobustVPN
RobustVPN Virtual IP	Show the virtual IP of RobustVPN
RobustVPN SubNet Address	Show the subnet address of RobustVPN

4.5.11 SNMP

This section allows you to set the SNMP parameters. Simple Network Management Protocol is a network management protocol used for collecting information and configuring network devices.

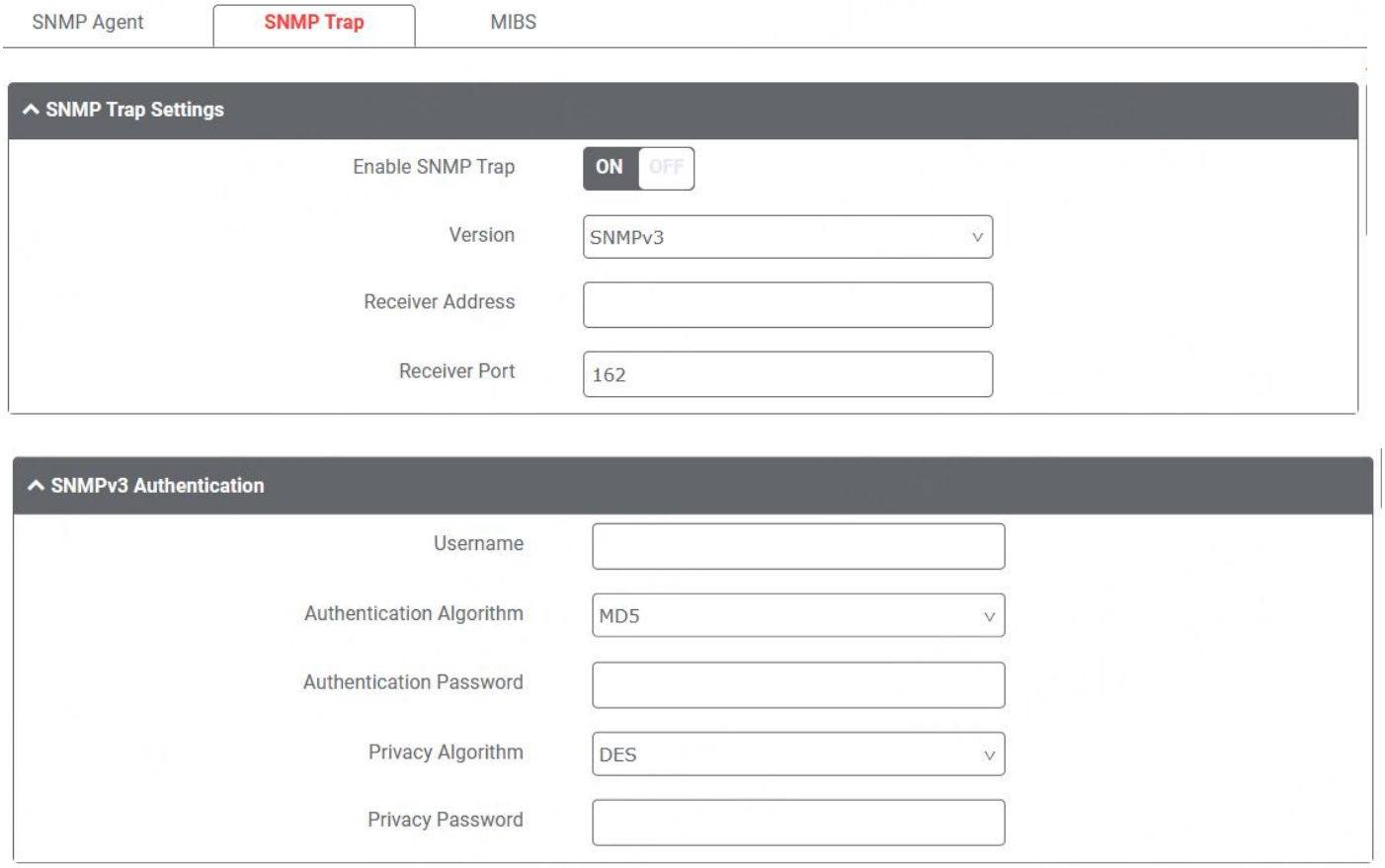
SNMP Agent



Item	Description	Default
Enable SNMP Agent	Click the toggle button to enable/disable this option.	OFF
Port	SNMP service's port.	161
OEM Enable	Click the toggle button to enable/disable this option.	OFF
OEM Enterprise	OEM enterprise information.	Null
OEM Platform	OEM platform information.	Null
Version	The SNMP version, select from “SNMPv3” or “SNMPv1v2v3”.	SNMPv3
Location Info	System location information.	Null
Contact Info	System contact information.	Null
System Name	System name.	Null
Readonly Community Name	Access mode for current community.	Null
Readwrite Community Name	Access mode for current community.	Null
Authentication Algorithm	Select from “MD5”, “SHA”.	MD5
Privacy Algorithm	Select from “DES”, “AES”.	DES

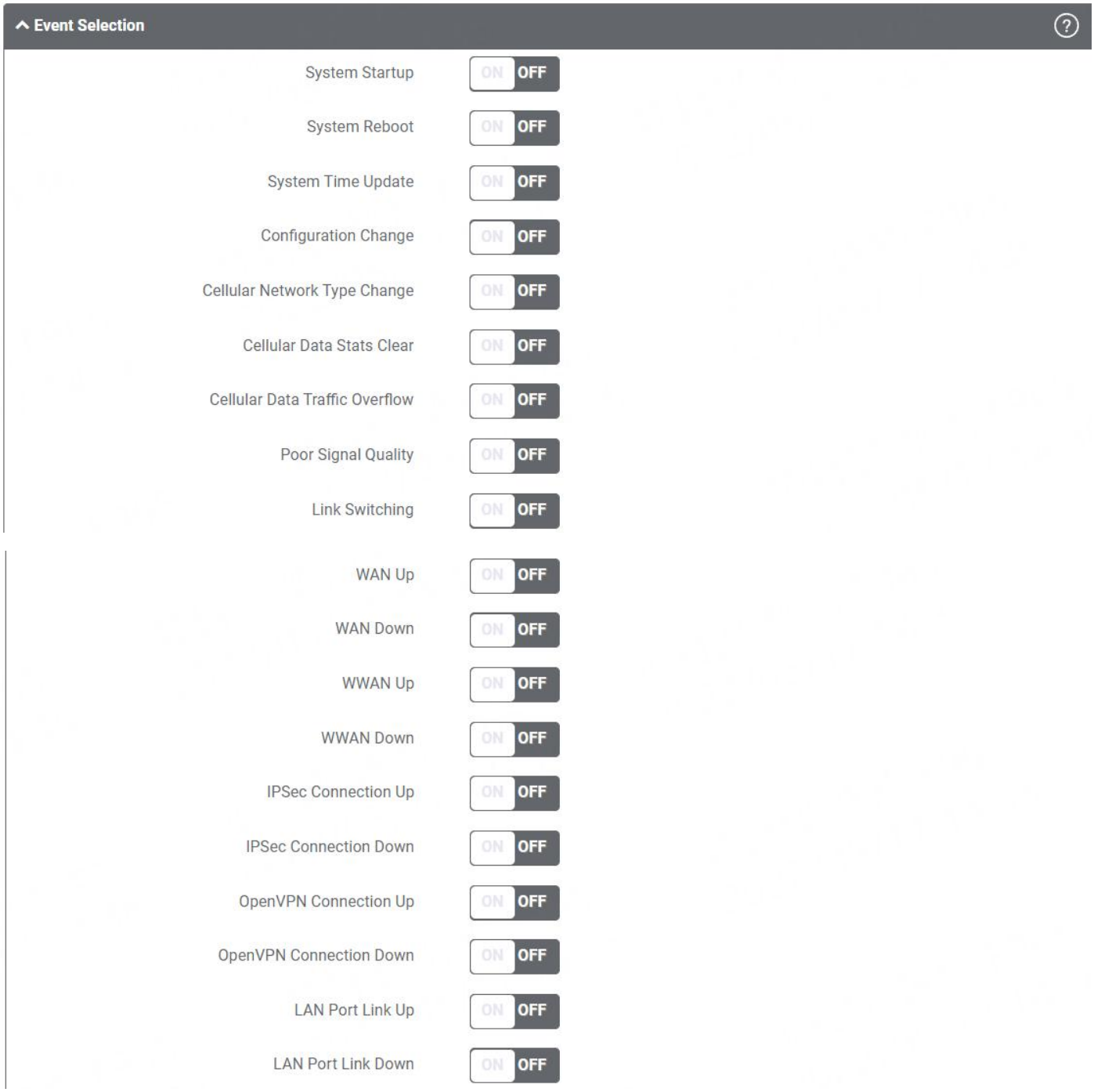
SNMP Trap

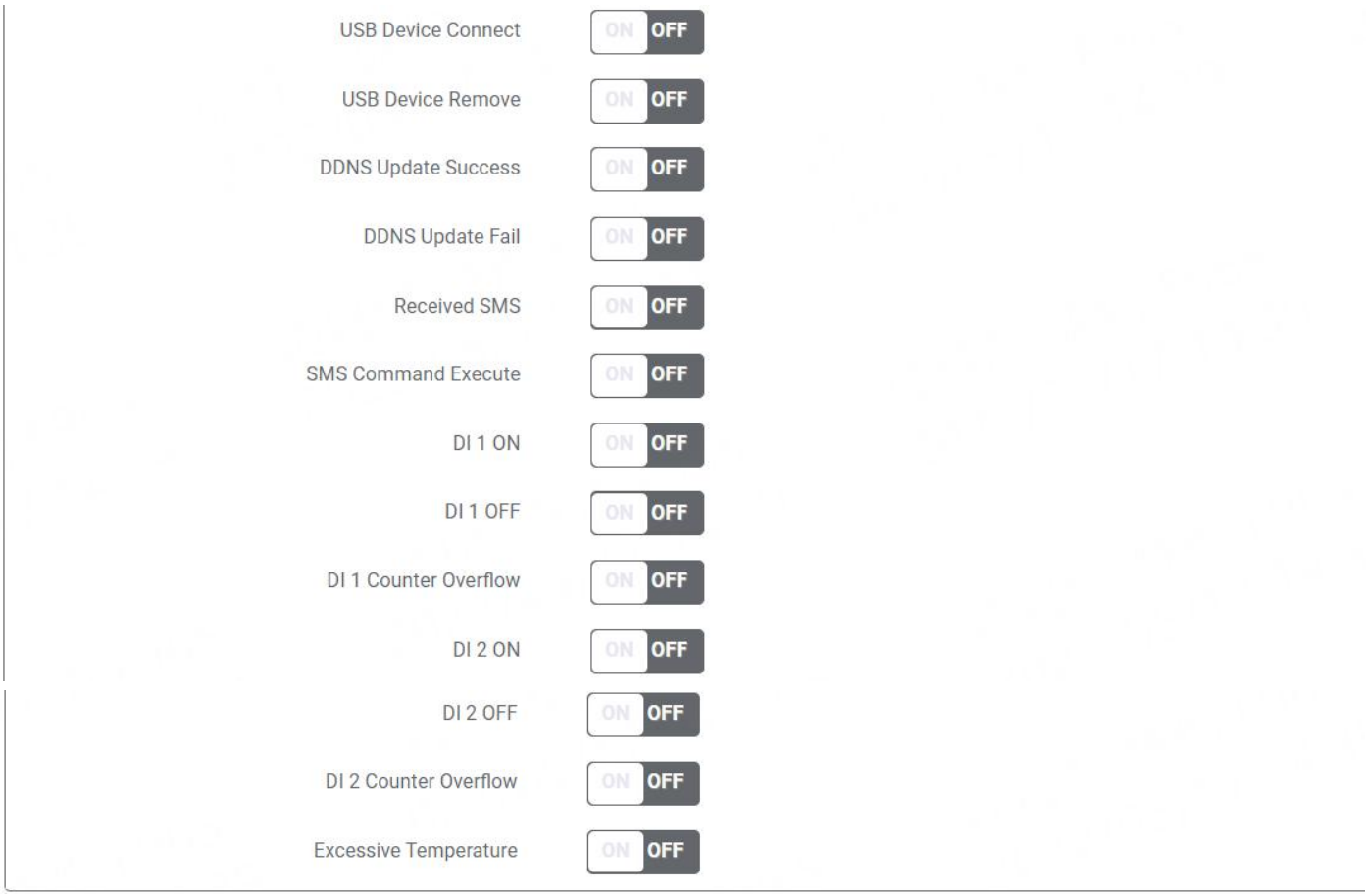
SNMP Trap Rules are alerts that trigger when certain user-specified events occur. When the trigger event happens, the trap will notify known SNMP hosts.



Item	Description	Default
Enable SNMP Agent	Click the toggle button to enable/disable this option.	OFF
Receiver Address	Host name or IP address to transfer SNMP traffic to.	Null
Receiver Port	Trap host's port number.	162
User name	The user name access to SNMP.	Null
Authentication Algorithm	Select from “MD5”, “SHA”.	MD5
Authentication Password	Enter the authentication password.	Null
Privacy Algorithm	Select from “DES”, “AES”.	DES
Privacy Password	Enter the privacy password.	Null

Click the toggle button the enable or disable the related event.


Event Selection
System Startup
System Reboot
System Time Update
Configuration Change
Cellular Network Type Change
Cellular Data Stats Clear
Cellular Data Traffic Overflow
Poor Signal Quality
Link Switching
WAN Up
WAN Down
WWAN Up
WWAN Down
IPSec Connection Up
IPSec Connection Down
OpenVPN Connection Up
OpenVPN Connection Down
LAN Port Link Up
LAN Port Link Down
ON
OFF



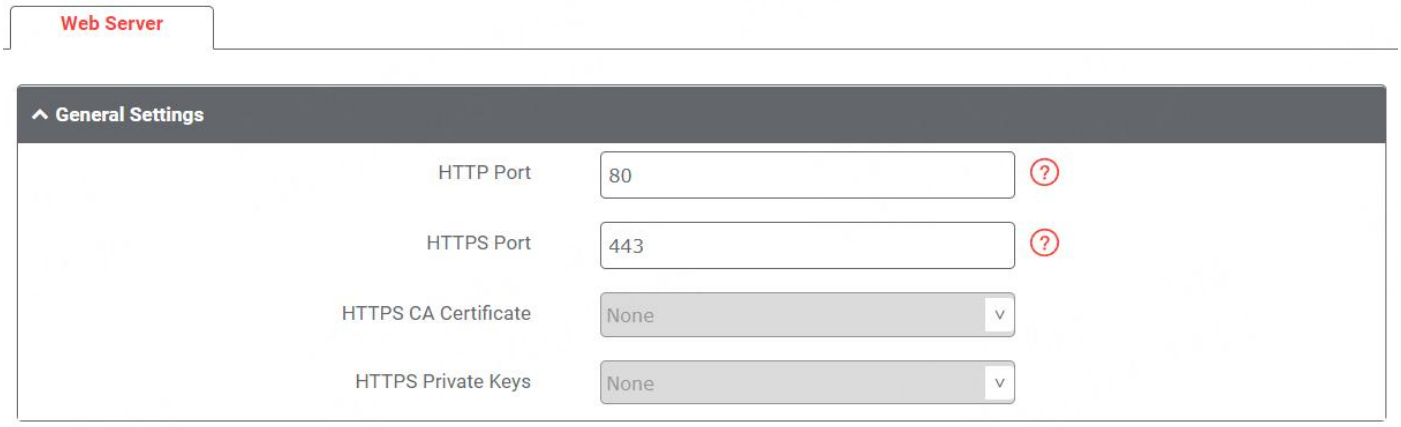
MIBS

MIB stands for Management Information Base, a MIB contains the variables that the managed device maintains and can be queried or set by the agent. The MIB defines the attributes of the managed device, including the name, status, access rights, and data type.

Item	Description	Default
MIBS	Click Generate to generate and click Download to download the device's MIB file.	--

4.5.12 Web Server

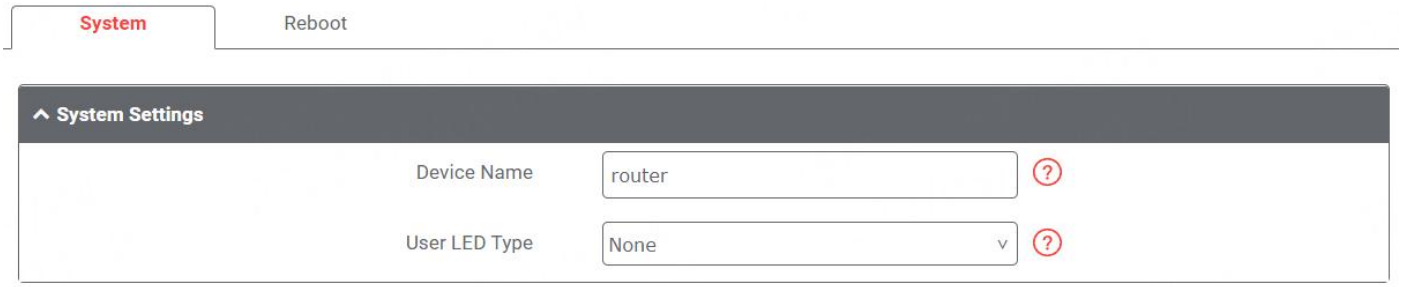
This section allows you to modify the parameters of Web Server.



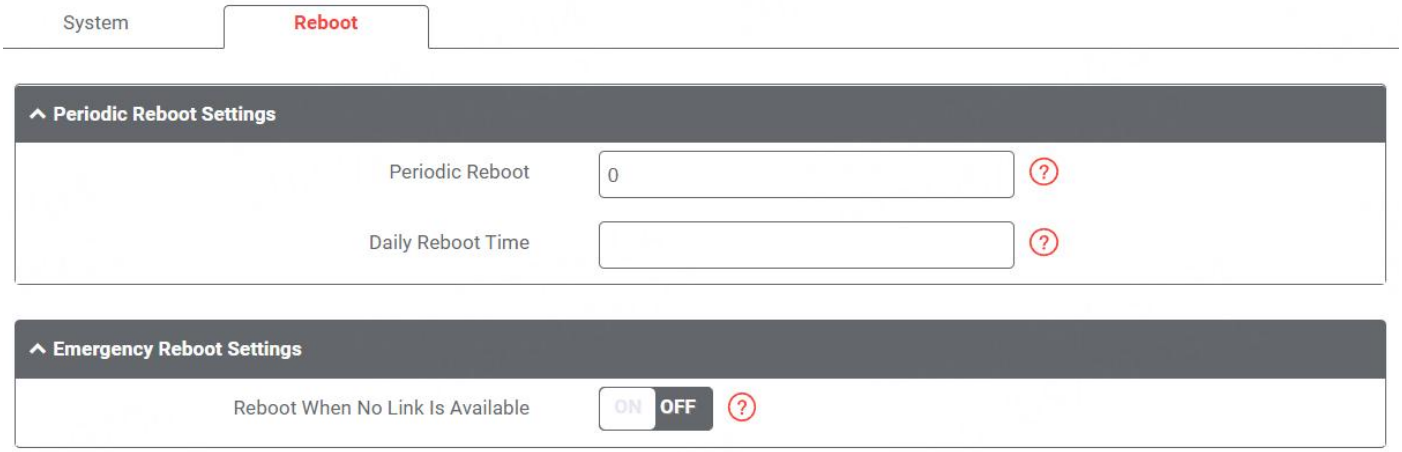
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in router's Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login router's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in router's Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port number except 443, only adding that port number then you can login router's Web Server. **Note**: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.	443
HTTPS CA Certificate	Select one once the certification is imported, see **4.6.2 Certificate Manager**	
HTTPS Private Keys	Select one once the certification is imported, see **4.6.2 Certificate Manager**	

4.5.13 Advanced

This section allows you to set the Advanced and parameters. Advanced router settings include system settings and reboot.



Item	Description	Default
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	router
User LED Type	Specify the display type of your USR LED. Select from “None”, “OpenVPN” or “IPsec”. • None: Meaningless indication, and the LED is off • SIM:show the sim status. • OpenVPN: USR indicator showing the OpenVPN status • IPsec: USR indicator showing the IPsec status	None



Periodic Reboot Settings		
Item	**Description**	**Default**
Periodic Reboot	Set the reboot period of the router. 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the router. You should follow the format as HH: MM, in 24h time frame, otherwise the data will be invalid. Leave it empty means disable.	Null
Reboot When No Link Is Available	Click the toggle button to enable/disable this option.	OFF

4.6 System

4.6.1 Debug

This section allows you to check and download the syslog details. Click “**Service > Syslog > Syslog Settings**” to enable

the syslog.

Syslog

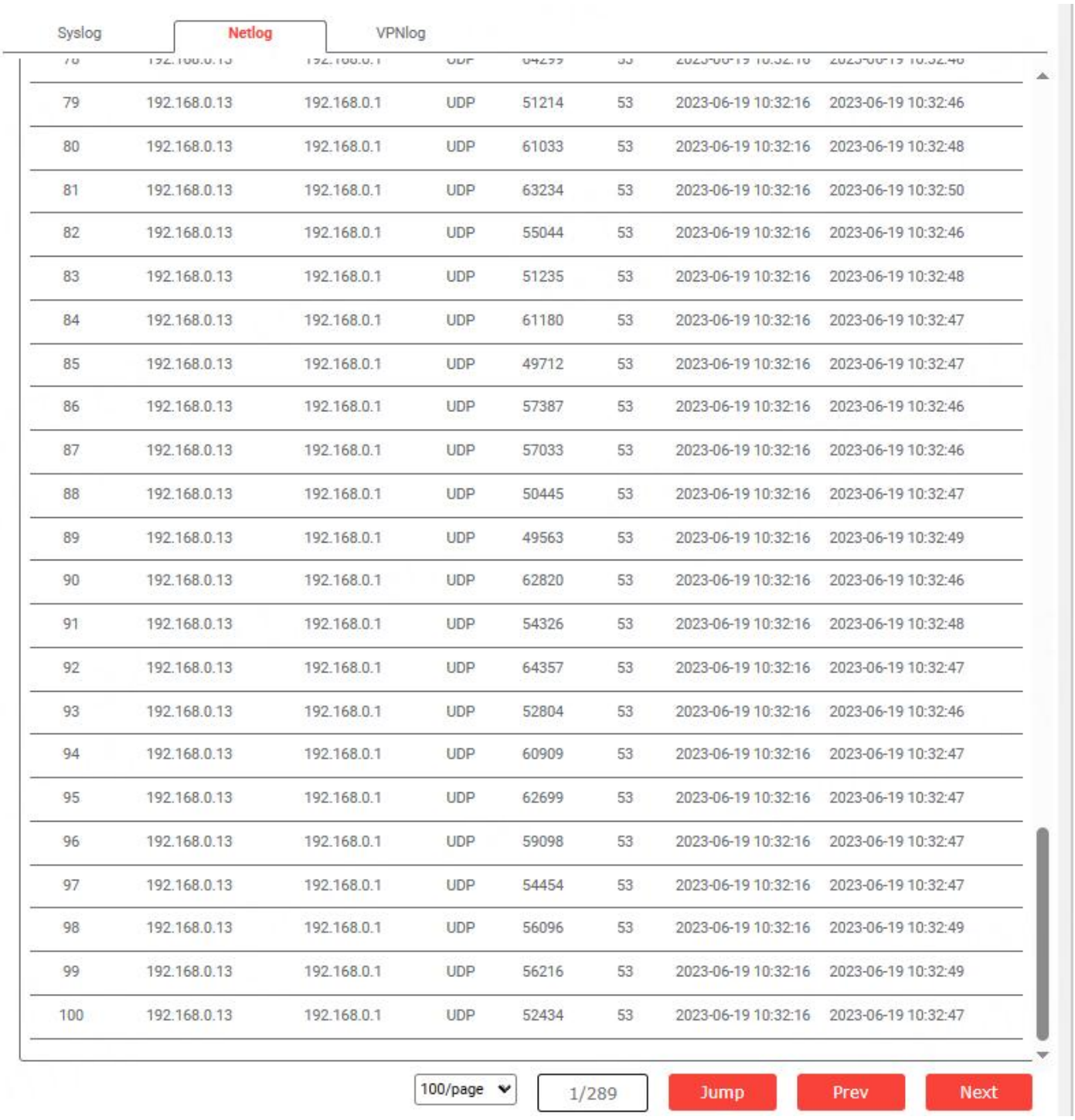
Item	Description	Default
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, “Error” which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Enter the filtering message based on the keywords. Use “&” to separate more than one filter message, such as “keyword1&keyword2”.	Null
Refresh	Select from “Manual Refresh”, “5 Seconds”, “10 Seconds”, “20 Seconds” or “30 Seconds”. You can select these intervals to refresh the log information displayed in the follow box. If selecting “manual refresh”, you should click the refresh	Manual Refresh

	button to refresh the syslog.	
Clear	Click the button to clear the syslog.	--
Refresh	Click the button to refresh the syslog.	--

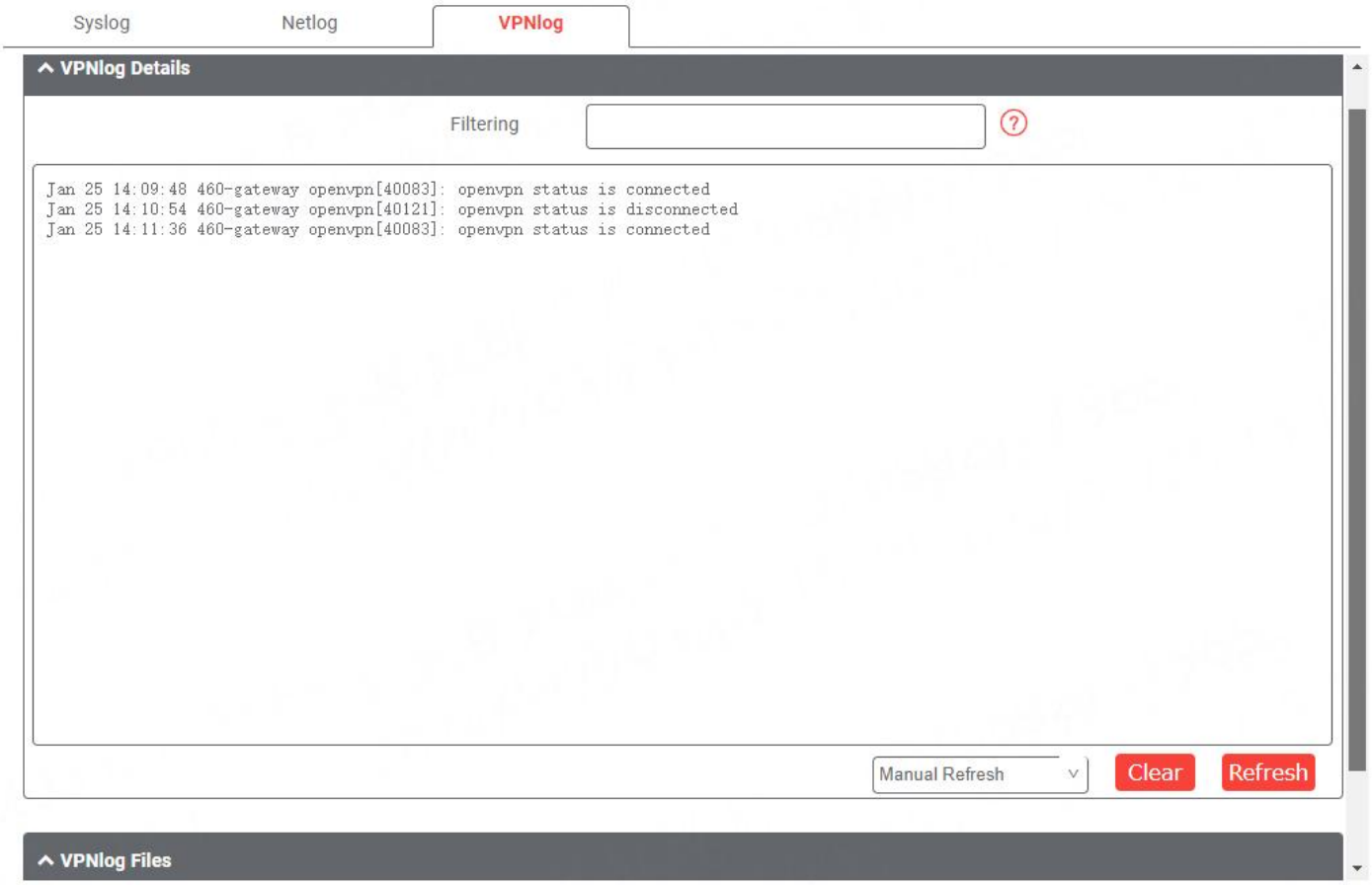
Item	Description	Default
System Journal File	Click Generate to generate and click Download to download the system journal file.	--

Item	Description	Default
System Diagnostic Data	Click Generate to generate and click Download to download the system diagnostic data.	--

Netlog


Syslog
Netlog
VPNlog
79 192.168.0.13 192.168.0.1 UDP 51214 53 2023-06-19 10:32:16 2023-06-19 10:32:46
80 192.168.0.13 192.168.0.1 UDP 61033 53 2023-06-19 10:32:16 2023-06-19 10:32:48
81 192.168.0.13 192.168.0.1 UDP 63234 53 2023-06-19 10:32:16 2023-06-19 10:32:50
82 192.168.0.13 192.168.0.1 UDP 55044 53 2023-06-19 10:32:16 2023-06-19 10:32:46
83 192.168.0.13 192.168.0.1 UDP 51235 53 2023-06-19 10:32:16 2023-06-19 10:32:48
84 192.168.0.13 192.168.0.1 UDP 61180 53 2023-06-19 10:32:16 2023-06-19 10:32:47
85 192.168.0.13 192.168.0.1 UDP 49712 53 2023-06-19 10:32:16 2023-06-19 10:32:47
86 192.168.0.13 192.168.0.1 UDP 57387 53 2023-06-19 10:32:16 2023-06-19 10:32:46
87 192.168.0.13 192.168.0.1 UDP 57033 53 2023-06-19 10:32:16 2023-06-19 10:32:46
88 192.168.0.13 192.168.0.1 UDP 50445 53 2023-06-19 10:32:16 2023-06-19 10:32:47
89 192.168.0.13 192.168.0.1 UDP 49563 53 2023-06-19 10:32:16 2023-06-19 10:32:49
90 192.168.0.13 192.168.0.1 UDP 62820 53 2023-06-19 10:32:16 2023-06-19 10:32:46
91 192.168.0.13 192.168.0.1 UDP 54326 53 2023-06-19 10:32:16 2023-06-19 10:32:48
92 192.168.0.13 192.168.0.1 UDP 64357 53 2023-06-19 10:32:16 2023-06-19 10:32:47
93 192.168.0.13 192.168.0.1 UDP 52804 53 2023-06-19 10:32:16 2023-06-19 10:32:46
94 192.168.0.13 192.168.0.1 UDP 60909 53 2023-06-19 10:32:16 2023-06-19 10:32:47
95 192.168.0.13 192.168.0.1 UDP 62699 53 2023-06-19 10:32:16 2023-06-19 10:32:47
96 192.168.0.13 192.168.0.1 UDP 59098 53 2023-06-19 10:32:16 2023-06-19 10:32:47
97 192.168.0.13 192.168.0.1 UDP 54454 53 2023-06-19 10:32:16 2023-06-19 10:32:47
98 192.168.0.13 192.168.0.1 UDP 56096 53 2023-06-19 10:32:16 2023-06-19 10:32:49
99 192.168.0.13 192.168.0.1 UDP 56216 53 2023-06-19 10:32:16 2023-06-19 10:32:49
100 192.168.0.13 192.168.0.1 UDP 52434 53 2023-06-19 10:32:16 2023-06-19 10:32:47
100/page
1/289
Jump
Prev
Next

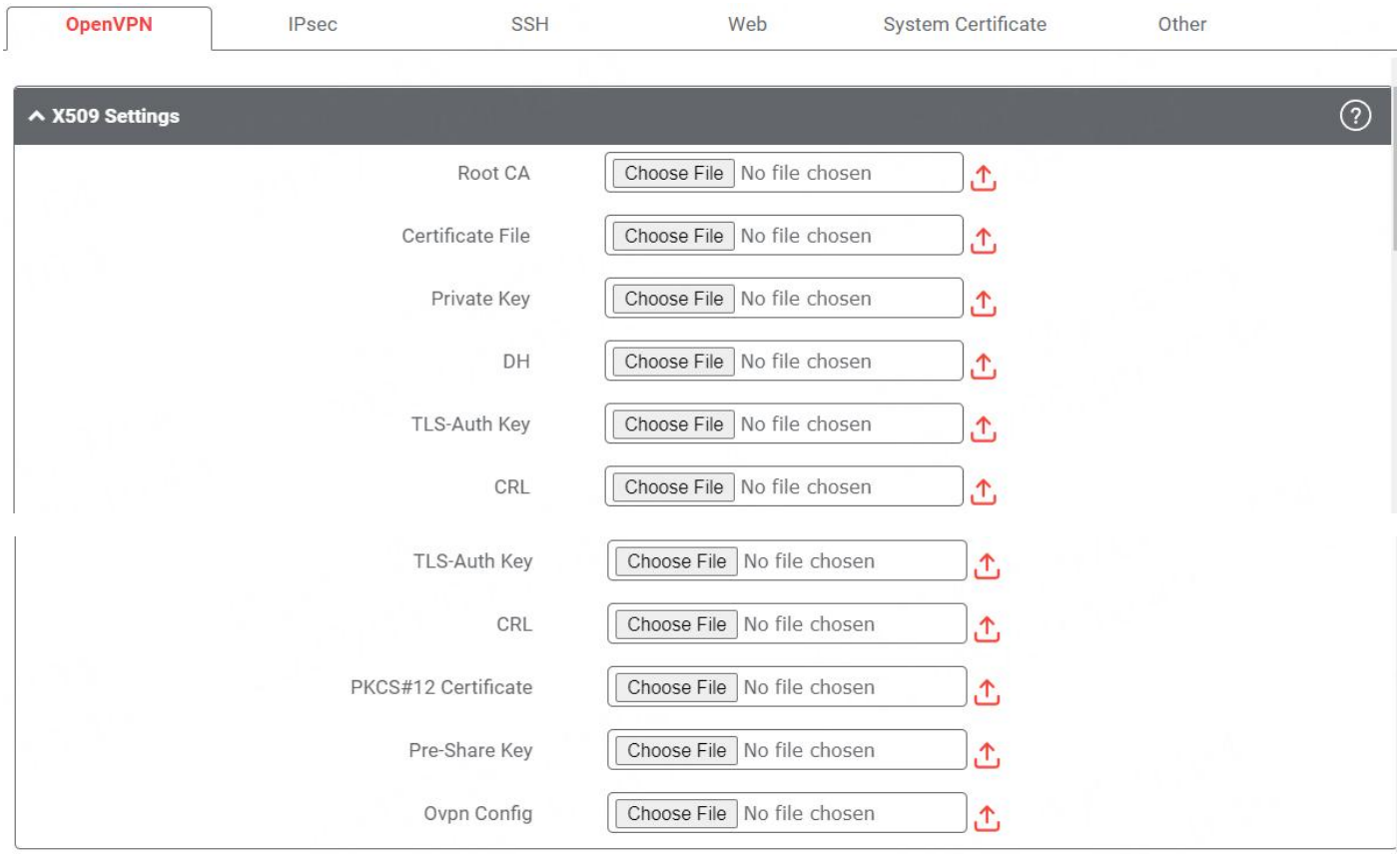
VPNlog



4.6.2 Certificate Manager

This section allows you to mange all of certificates here. If you want to manage a certificate for your custom application, you can manage it through Other tab.

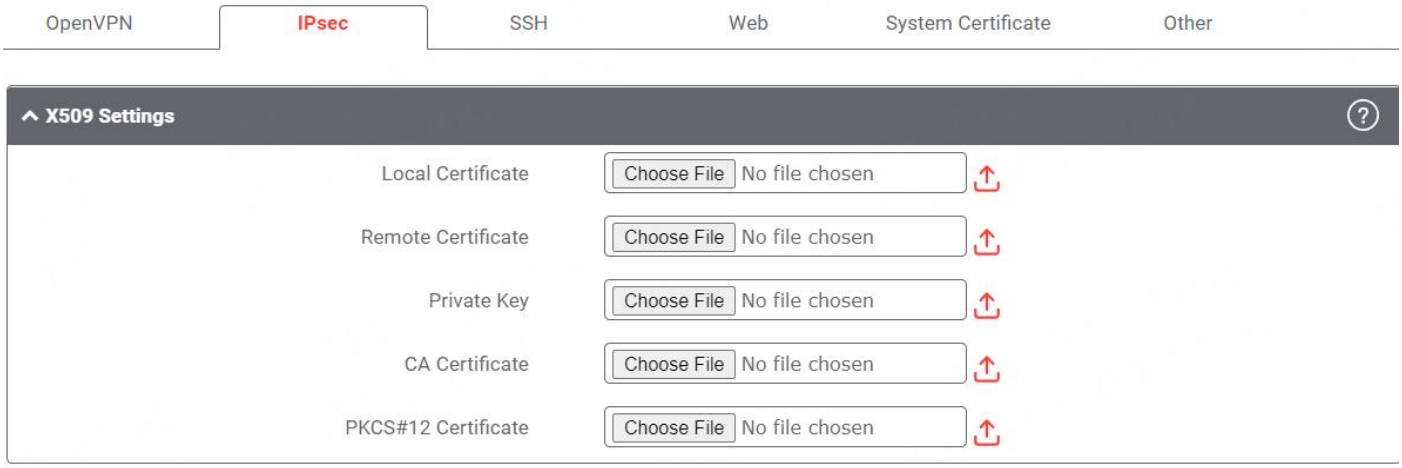
OpenVPN



Item	Description	Default
Root CA	Click on Choose File to locate the root ca file, and then click on to import this file into your device.	--
Certificate File	Click on Choose File to locate the certificate file, and then click on to import this file into your device.	--
Private Key	Click on Choose File to locate the Private Key file, and then click on to import this file into your device.	--
DH	Click on Choose File to locate the DH file, and then click on to import this file into your device.	
TLS-Auth Key	Click on Choose File to locate the TLS-Auth Key file, and then click on to import this file into your device.	--
CRL	Click on Choose File to locate the CRL file, and then click on to import this file into your device.	--
PKCS#12 Certificate	Click on Choose File to locate the PKCS#12 Certificate file, and then click on	--

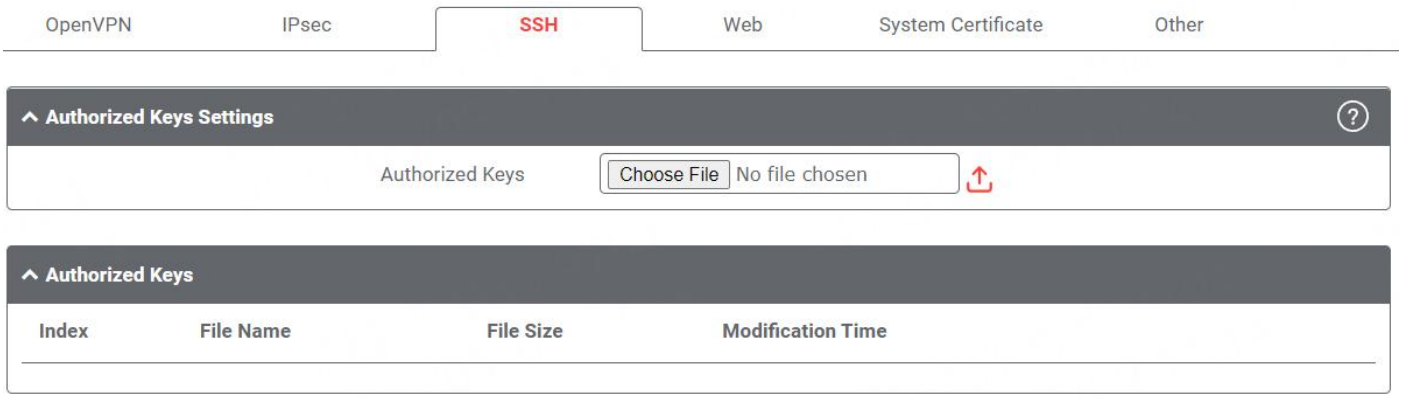
	to import this file into your device.	
Pre-Share Key	Click on Choose File to locate the Pre-Share Key file, and then click on to import this file into your device.	--
Ovpn Config	Click on Choose File to locate the Ovpn Configy file, and then click on to import this file into your device.	--

IPsec



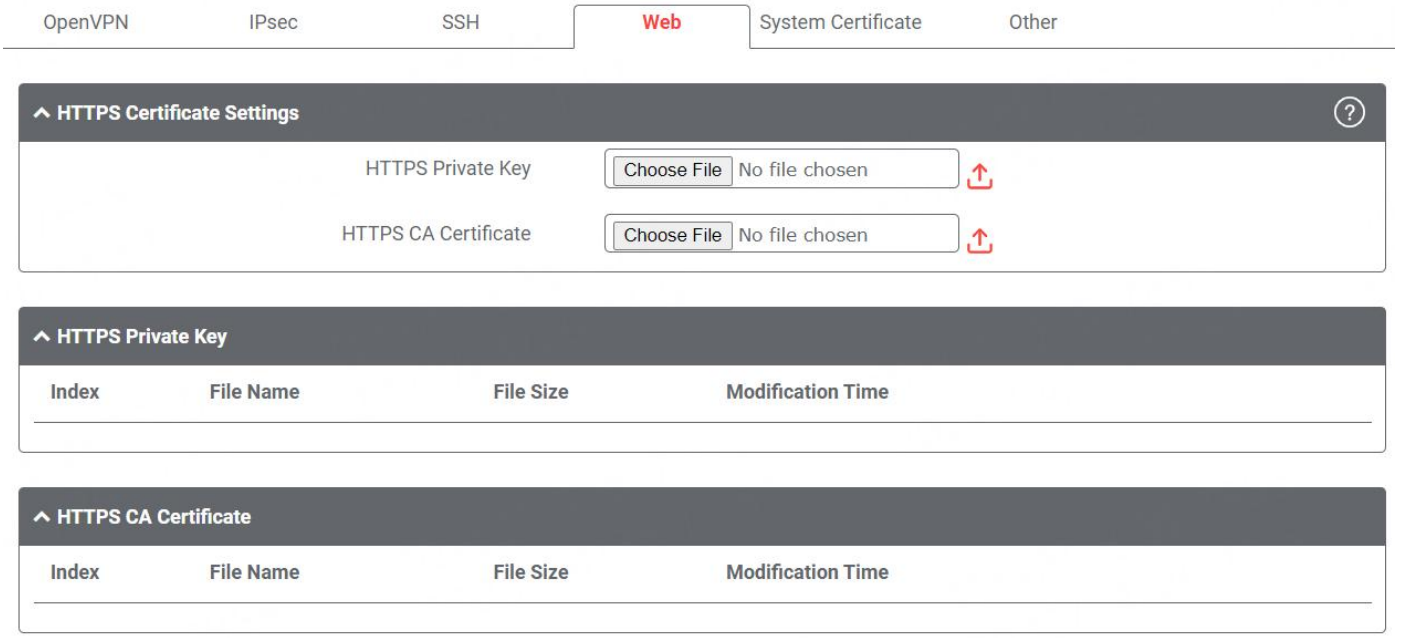
Item	Description	Default
Local Certificate	Click on Choose File to locate the Local Certificate file, and then click on to import this file into your device.	--
Remote Certificate	Click on Choose File to locate the Remote Certificate file, and then click on to import this file into your device.	--
Private Key	Click on Choose File to locate the Private Key file, and then click on to import this file into your device.	--
CA Certificate	Click on Choose File to locate the CA Certificate file, and then click on to import this file into your device.	--
PKCS#12 Certificate	Click on Choose File to locate the PKCS#12 Certificate file, and then click on to import this file into your device.	--

SSH



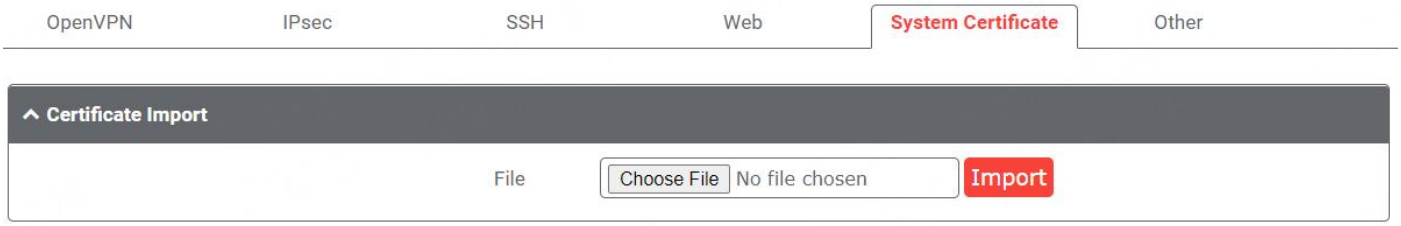
Item	Description	Default
Authorized Keys	Click on Choose File to locate the Authorized Keys file, and then click on to import this file into your device.	--

Web



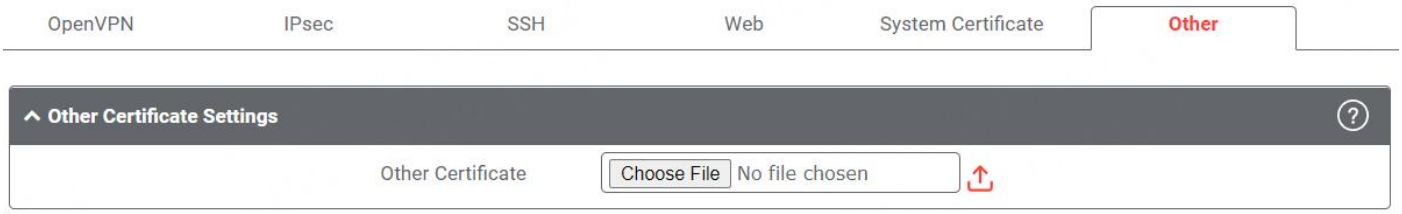
Item	Description	Default
HTTPS Private Key	Click on Choose File to locate the Authorized Keys file, and then click on to import this file into your device.	--
HTTPS CA Certificate	Click on Choose File to locate the Certificate file, and then click on to import this file into your device.	

System Certificate



Item	Description	Default
File	Click on Choose File to locate the System certificate file, and then click on to import this file into your device.	--

Other

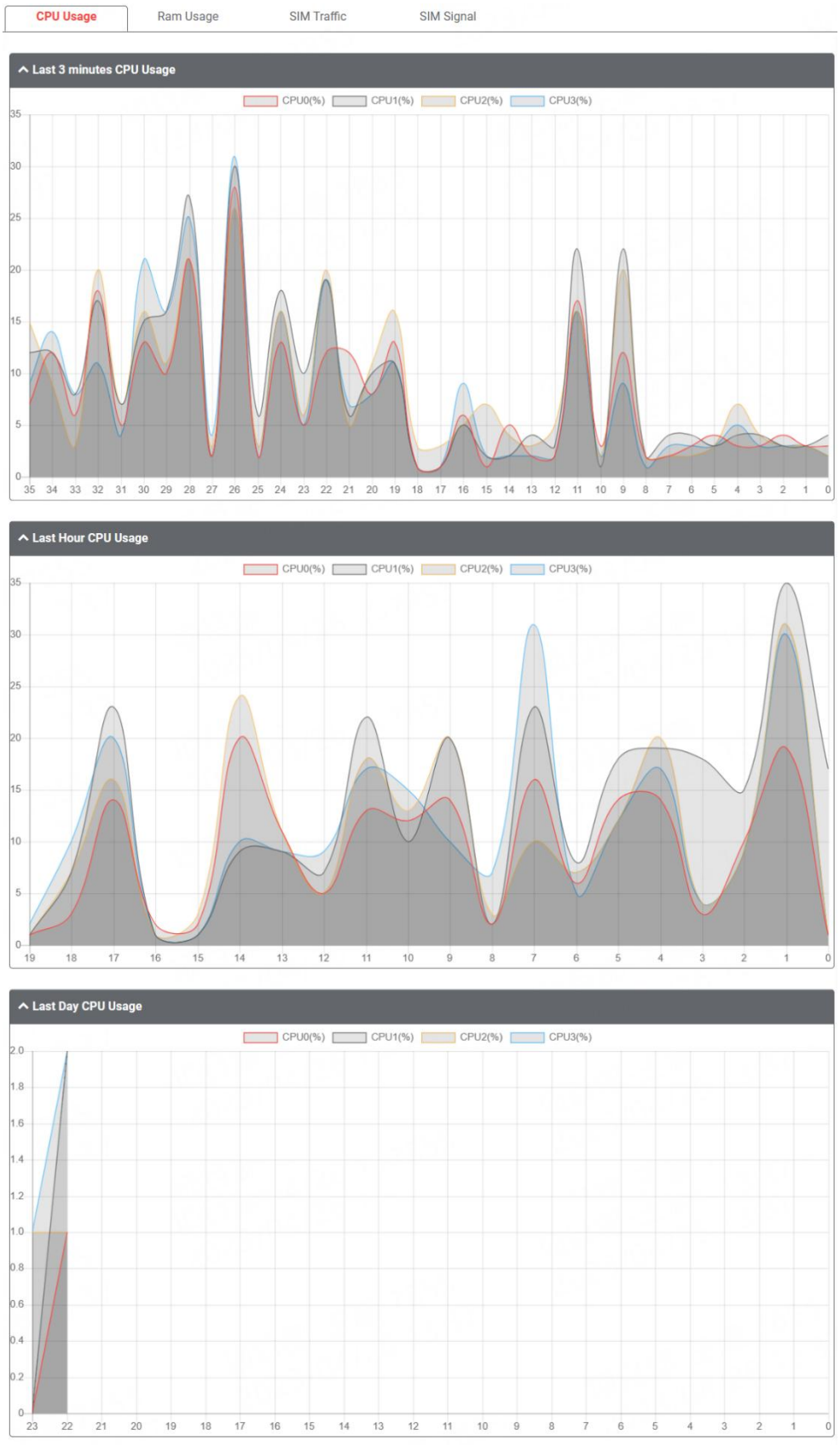


Item	Description	Default
Other Certificate	Click on Choose File to locate the Other Certificate file, and then click on to import this file into your device.	--

4.6.3 Resource Graph

This section allows you to view the system resource such as CPU usage or cellular signal strength in recent 3 minutes, last hour or last day.

CPU Usage


CPU Usage
Ram Usage
SIM Traffic
SIM Signal
Last 3 minutes CPU Usage
CPU0(%)
CPU1(%)
CPU2(%)
CPU3(%)
Last Hour CPU Usage
Last Day CPU Usage

RAM Usage


CPU Usage
Ram Usage
SIM Traffic
SIM Signal
Last 3 minutes RAM Usage
RAM(%)
28.00
27.90
27.80
27.70
27.60
27.50
27.40
27.30
27.20
27.10
27.00
35 34 33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Last Hour RAM Usage
RAM(%)
28.0
27.8
27.6
27.4
27.2
27.0
26.8
26.6
26.4
26.2
26.0
19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Last Day RAM Usage
RAM(%)
27.0
26.5
26.0
25.5
25.0
24.5
24.0
23.5
23.0
22.5
22.0
23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0

SIM Traffic


CPU Usage
Ram Usage
SIM Traffic
SIM Signal
Last 3 minutes SIM Traffic
SIM1(MB)
SIM2(MB)
Last Hour SIM Traffic
SIM1(MB)
SIM2(MB)
Last Day SIM Traffic
SIM1(MB)
SIM2(MB)

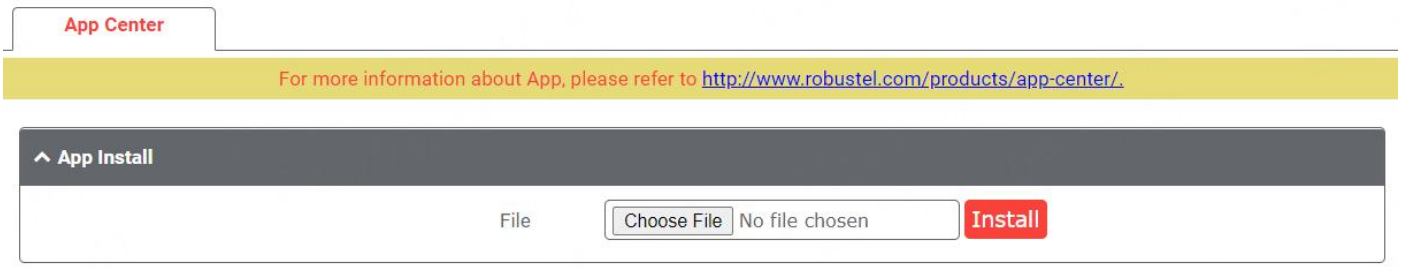
SIM Signal


CPU Usage
Ram Usage
SIM Traffic
SIM Signal
Last 3 minutes SIM Signal
SIM1(dBm)
SIM2(dBm)
-139.0
-139.2
-139.4
-139.6
-139.8
-140.0
-140.2
-140.4
-140.6
-140.8
-141.0
35 34 33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Last Hour SIM Signal
SIM1(dBm)
SIM2(dBm)
-139.0
-139.2
-139.4
-139.6
-139.8
-140.0
-140.2
-140.4
-140.6
-140.8
-141.0
19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Last Day SIM Signal
SIM1(dBm)
SIM2(dBm)
-139.0
-139.2
-139.4
-139.6
-139.8
-140.0
-140.2
-140.4
-140.6
-140.8
-141.0
23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0

4.6.4 App Center

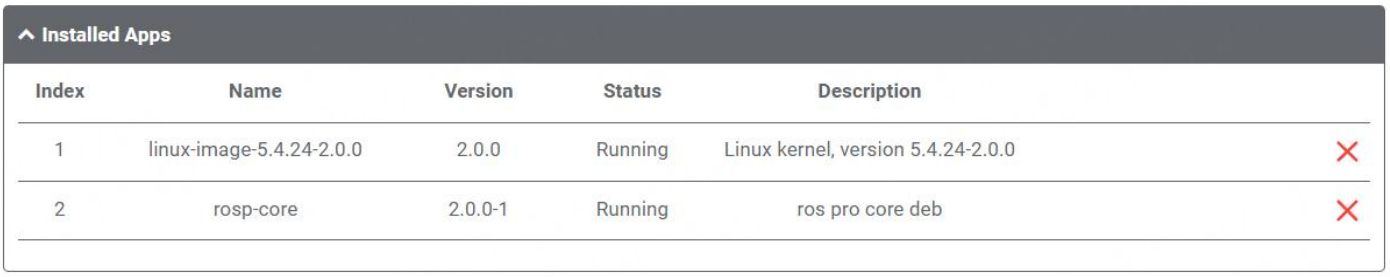
This section allows you to add some required or customized applications to the router. Import and install your applications to the App Center, and reboot the device according to the system prompts. Each installed application will be displayed under the “Services” menu, while other applications related to VPN will be displayed under the “VPN” menu.

Note: After importing the applications to the router, the page display may have a slight delay due to the browser cache. It is recommended that you clear the browser cache first and log in the router again.



Item	Description	Default
File	Click on “Choose File” to locate the App file from your PC, and then click Install to import this file into your device.	--

The successfully installed app will be displayed in the following list. Click ✕ to uninstall the app.

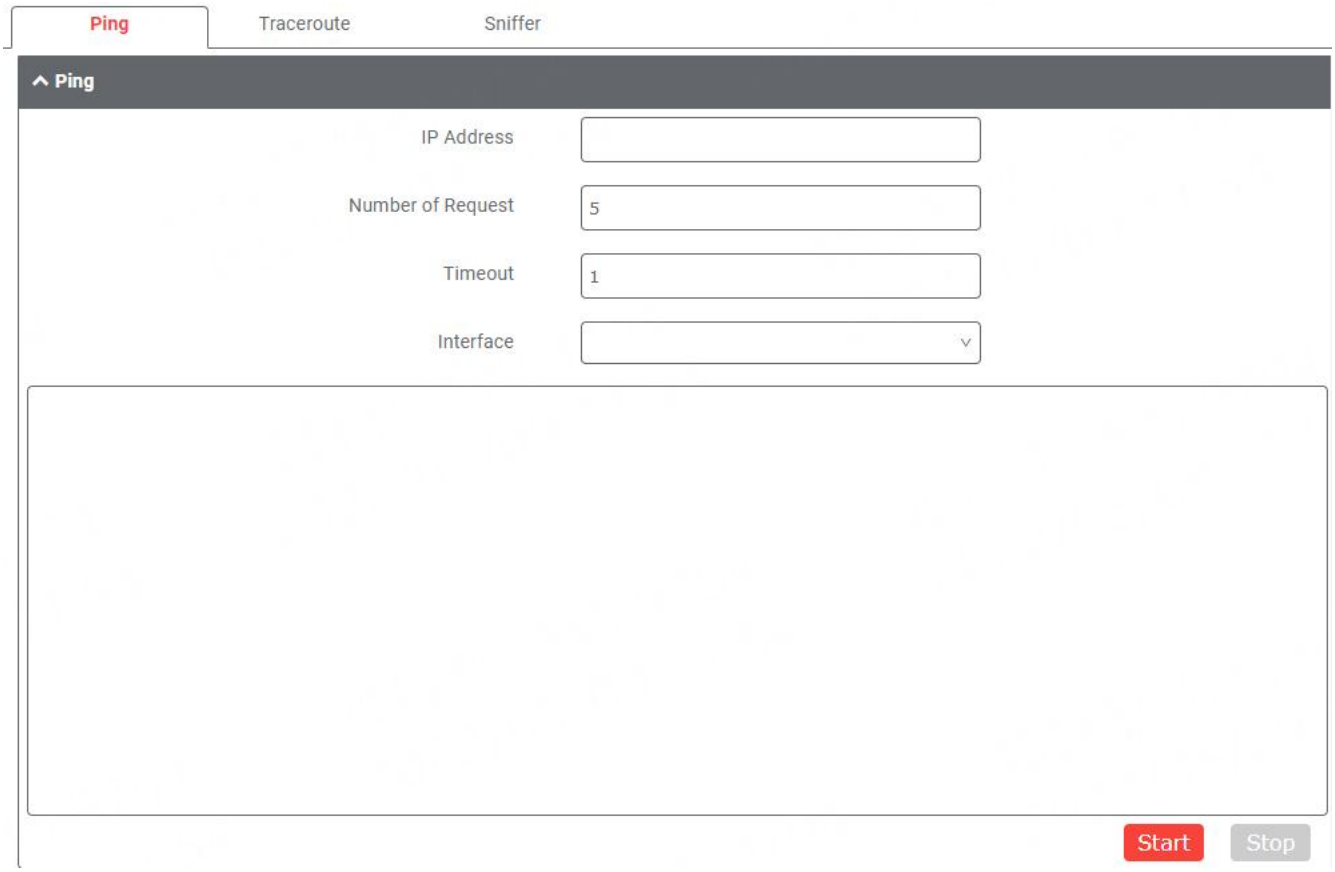


Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

4.6.5 Tools

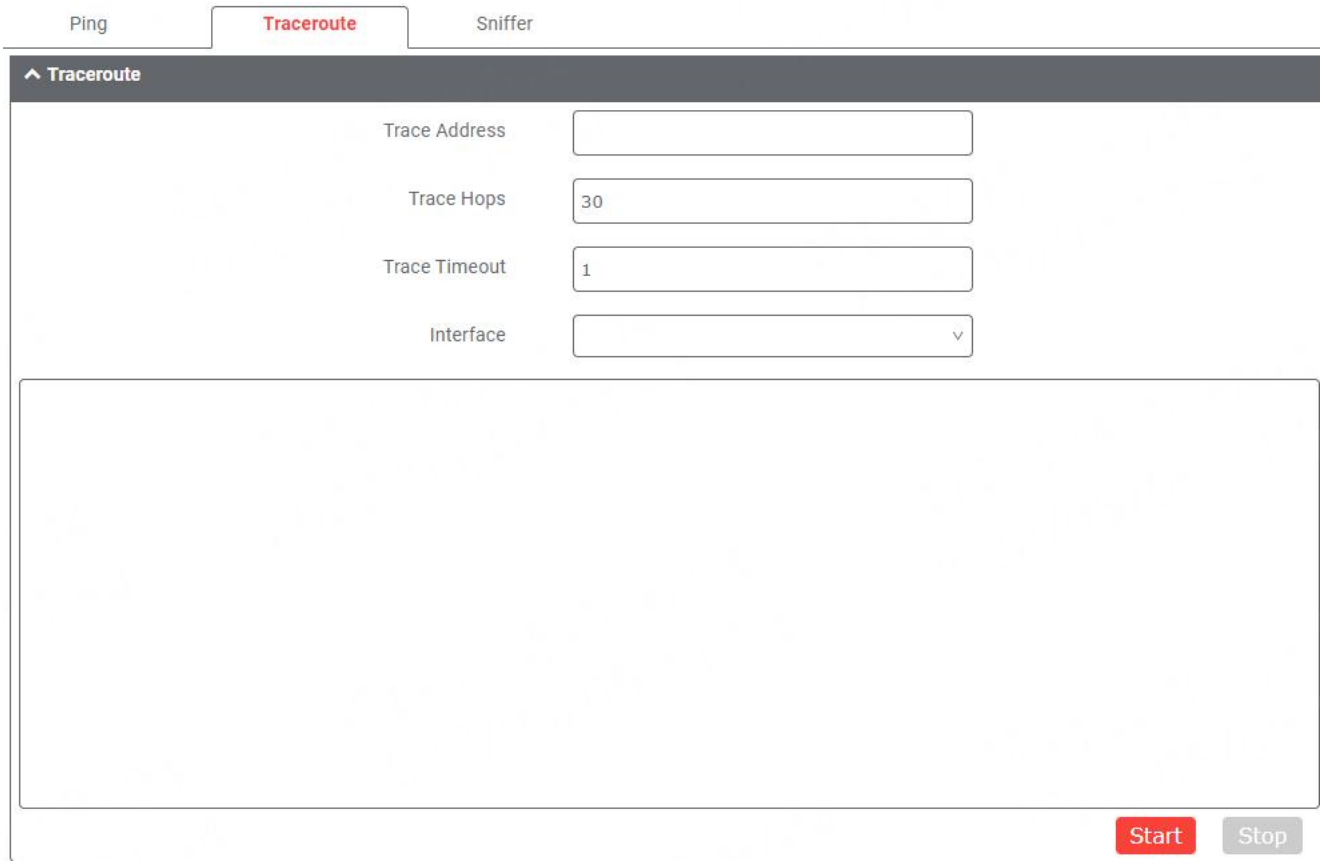
This section provides users three tools: Ping, Traceroute and Sniffer. The Ping is used to check the network connectivity.

Ping



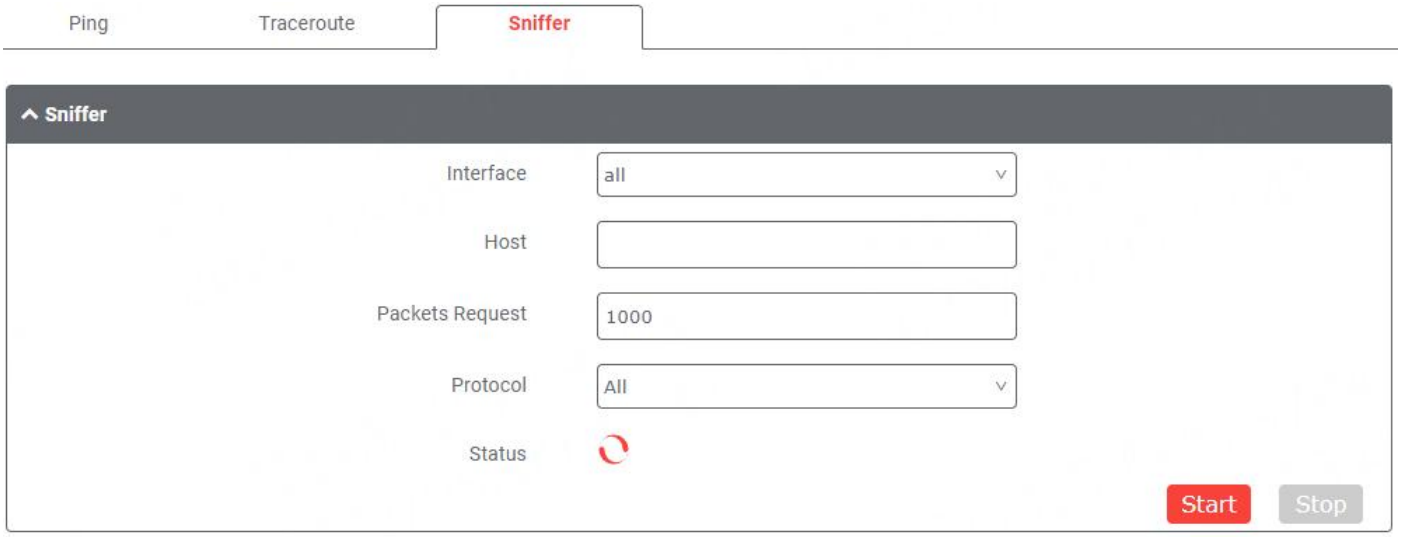
Item	Description	Default
IP address	Enter the ping's destination IP address or destination domain.	Null
Number of Requests	Specify the number of ping requests.	5
Timeout	Specify the timeout of ping requests.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for selecting local IP address from these three automatically.	Null
Start	Click this button to start ping request, and the log will be displayed in the follow box.	--
Stop	Click this button to stop ping request.	--

Traceroute



Item	Description	Default
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify the timeout of Traceroute request.	1
Interface	Select the trace interface.	--
Start	Click this button to start ping request, and the log will be displayed in the follow box.	--
Stop	Click this button to stop ping request.	--

Sniffer



Item	Description	Default
Interface	Choose the interface according to your Ethernet configuration.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from “All”, “IP”, “TCP”, “UDP” and “ARP”.	All
Status	Show the current status of sniffer.	--
Start	Click this button to start the sniffer.	--
Stop	Click this button to stop the sniffer. Once you click this button, a new log file will be displayed in the following List.	--

Item	Description	Default
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List and click to download the log, click to delete the log file. It can cache a maximum of 5 files.	--

4.6.6 Flash Manager

This section allows you to manage the device’s flash memory life, you can easily check the flash status or thoughput and start a period test on this section .

Status

This page shows the flash status and data throughput details.

Status | Flash Memory Tests

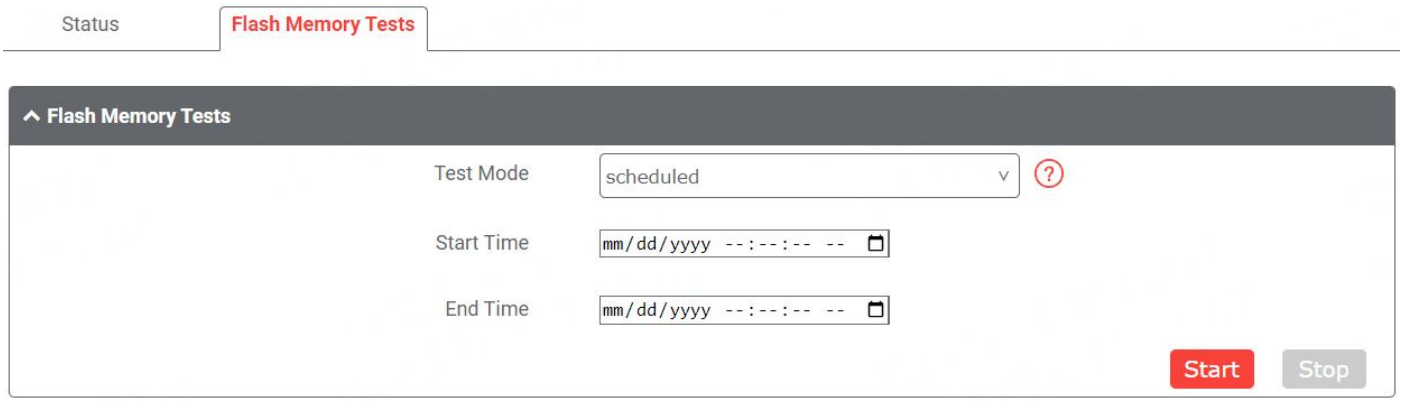
Flash Status

Estimated Remaining Device Lifetime	90% - 100%
Flash Total Erase Amount	303756.75 MB
Total Blocks Erased	12273
Block Size	24.75 MB
Total Number of Blocks	3000
Flash Avg Erase Count	18
Flash Avg Erase Rate	<1%
Flash Bad Block Count	7
Increase Bad Block Count	0
Power On Count	359 Times
Reserved Block Consumption	Normal
Capacity	14930 MB

Data Throughput

Item	Today	Yesterday	Last 7 Days	Total
Data Read(MB)	0	0	0	39040
Data Write(MB)	128	0	128	76928

Flash Memory Tests

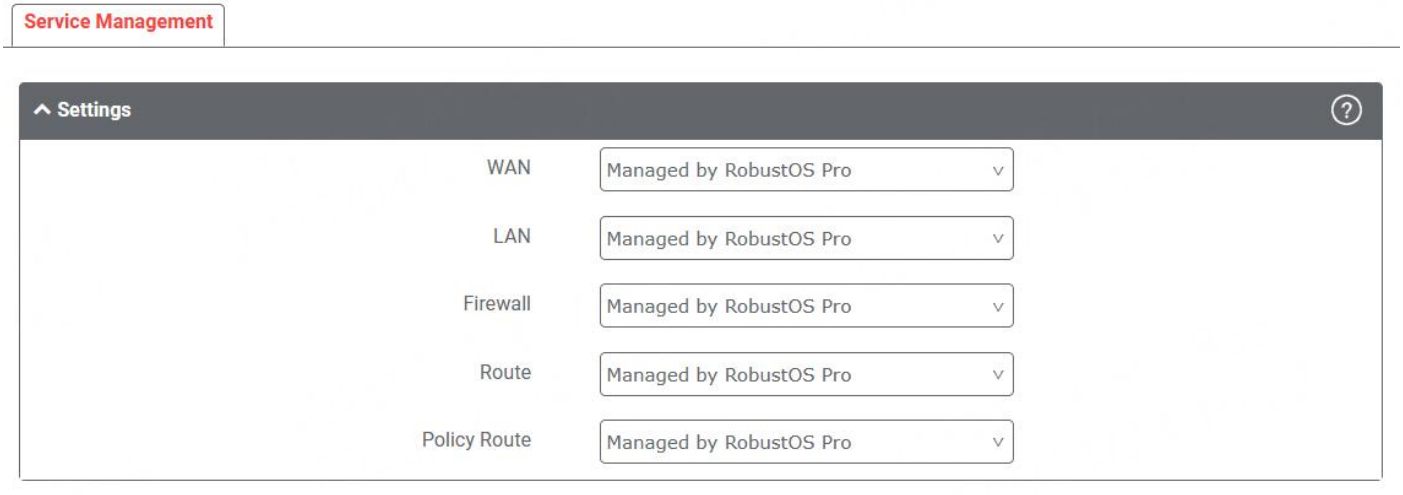


Flash Memory Tests @ Flash Manager	
Item	**Description**
Test Mode	**Manual**: When choosing 'manual', click 'start' to run a test, you can click 'stop' to end the test; **Scheduled**: Input the 'start' and 'end' time for a scheduled test. You can click 'stop' button under whatever mode.
Start Time	Enter start time, format: yyyy/mm/dd, hh/mm/ss. E.g. 2023/04/24, 12:00:00
End Time	Enter end time, format: yyyy/mm/dd, hh/mm/ss. E.g. 2023/04/24, 18:00:00

You can click  to download the test log for viewing more information.

4.6.7 Service Management

This section allows you to modify the network services manage way.



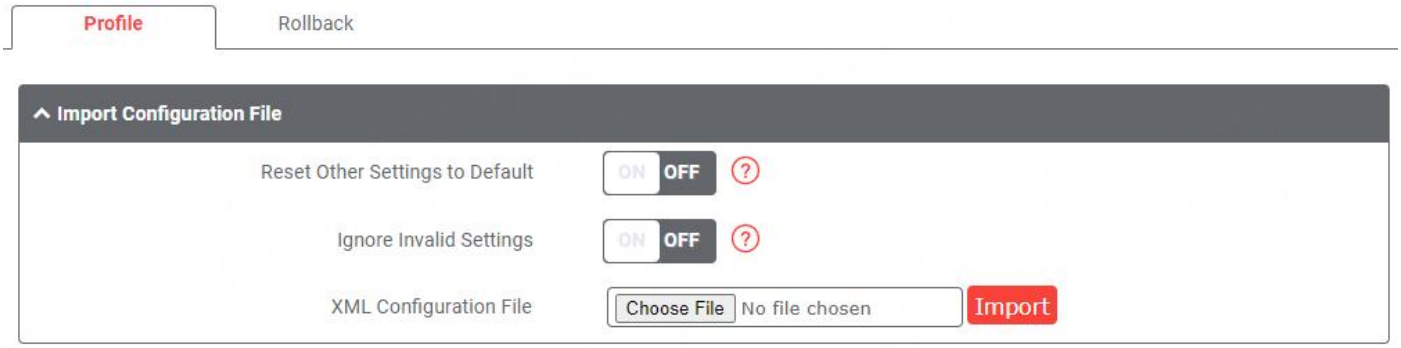
Mode	View Status on RobustOS Pro	Configure via RobustOS Pro	Configure via Linux Shell
Managed By RobustOS Pro	√	√	X

Managed By Third-Party	X	X	√

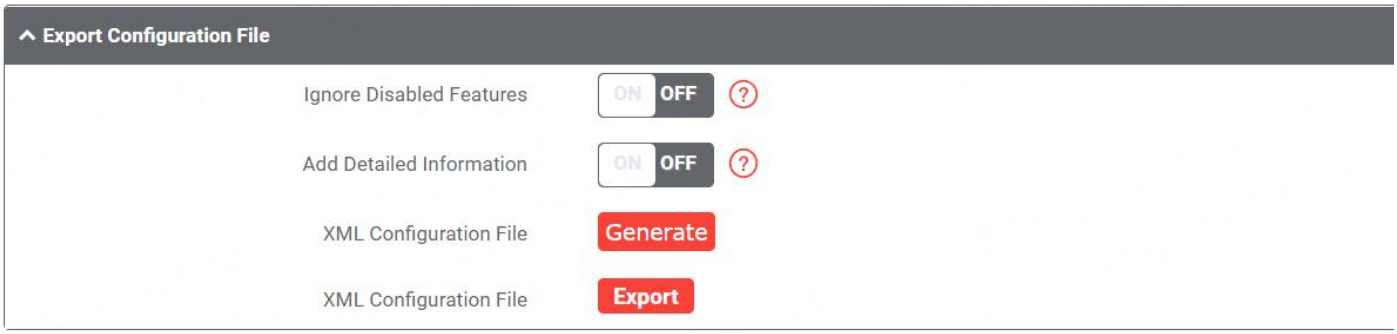
4.6.8 Profile

This section allows you to import or export the configuration file, or rollback the device to a previous configuration.

Profile



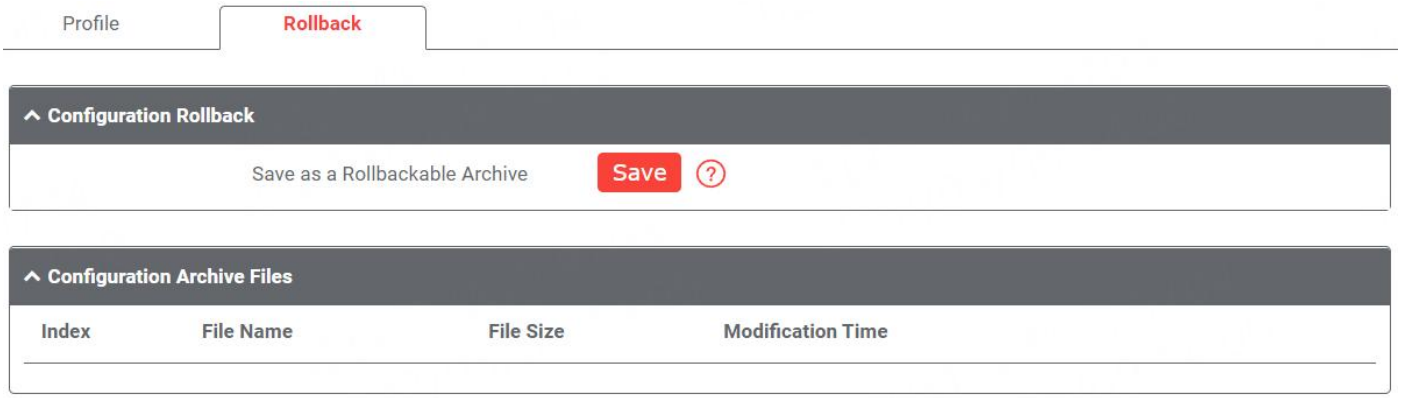
Item	Description	Default
Reset Other Settings to Default	Click the toggle button as “ON” to return other parameters to default settings.	OFF
Ignore Invalid Settings	Click the toggle button as “ON” to ignore invalid settings.	OFF
XML Configuration File	Click on Choose File to locate the XML configuration file from your PC, and then click Import to import this file into your device.	--



Item	Description	Default
Ignore Disabled Features	Click the toggle button as “OFF” to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as “On” to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as “ON” to encrypt the secret data.	ON
XML Configuration File	Click Generate button to generate the XML configuration file, and click Export to export the XML configuration file.	--

Item	Description	Default
Save Running Configuration as Default	Click Save button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click Restore button to restore the defaults configuration.	--
Restore to Factory Default Configuration	Click Restore button to restore the factory defaults configuration. Note: The linux file system will be restored to the initialization state.	--

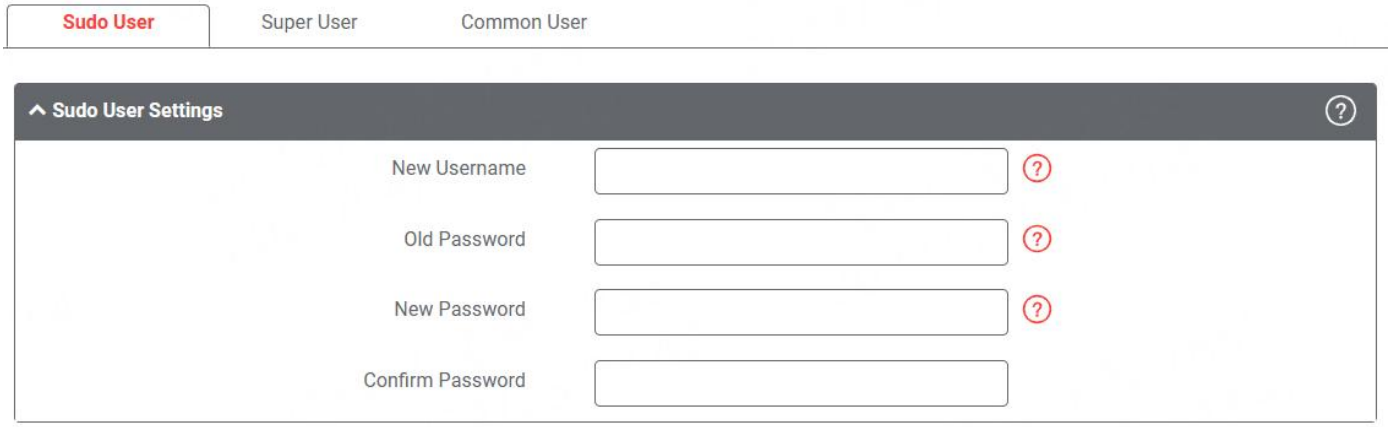
Rollback



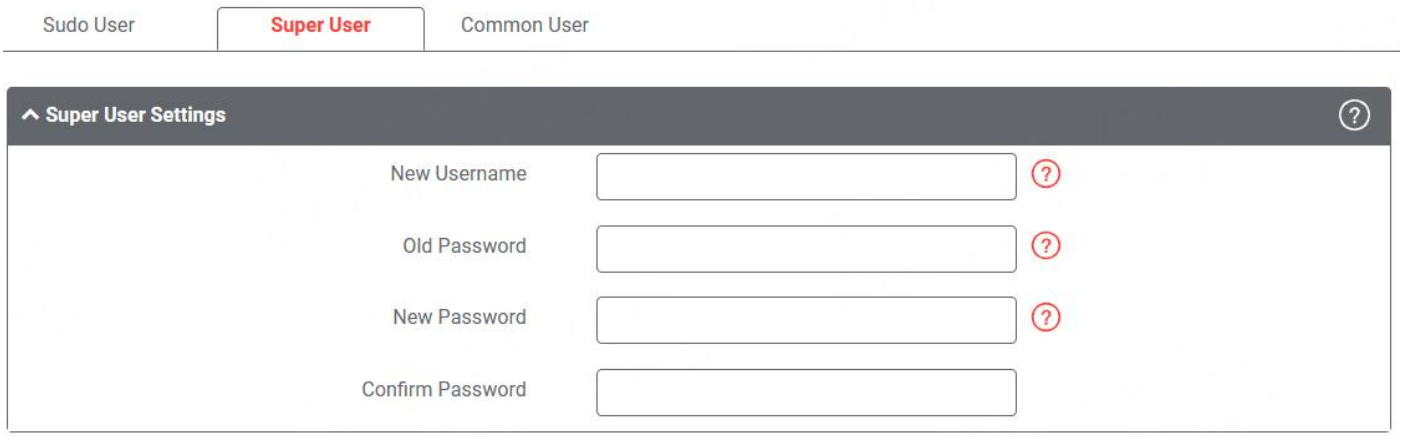
Item	Description	Default
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point every day automatically if configuration changes.	--
Configuration Archive Files	View the related information about configuration archive files, including name, size and modification time.	--

4.6.9 User Management

This section allows you to change your username and password, and create or manage user accounts. One device has only one super user who has the highest authority to modify, add and manage other common users.
The password need to be meet the requirement: 8-32 characters, must consist of at least three types of lowercase, uppercase, digit, and special characters.
Special characters allowed: @, #, $, ., *, !, -

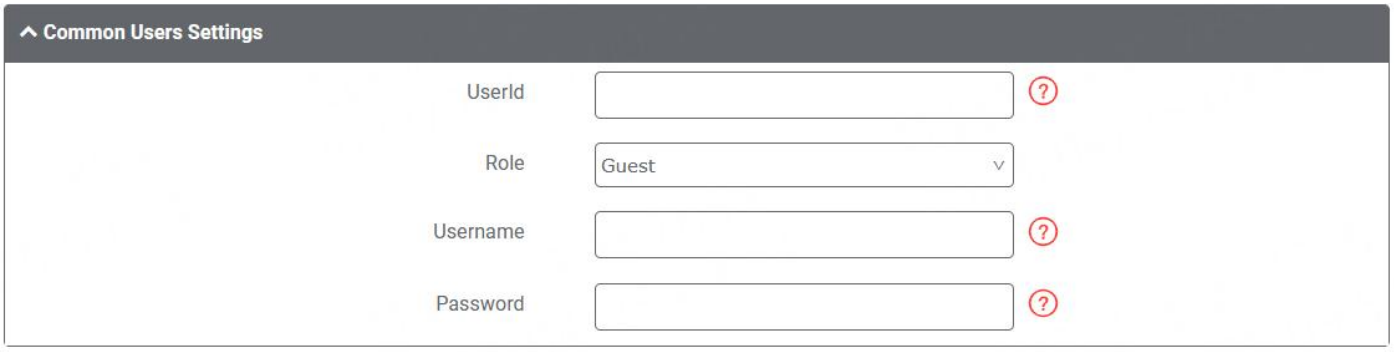

Sudo User
Super User
Common User
Sudo User Settings
New Username
Old Password
New Password
Confirm Password

Item	Description	Default
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Null
Old Password	Enter the old password of your router. The default password please see the product label.	Null
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Null
Confirm Password	Enter the new password again to confirm.	Null



Item	Description	Default
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Null
Old Password	Enter the old password of your router. The default password please see the product label.	Null
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Null
Confirm Password	Enter the new password again to confirm.	Null

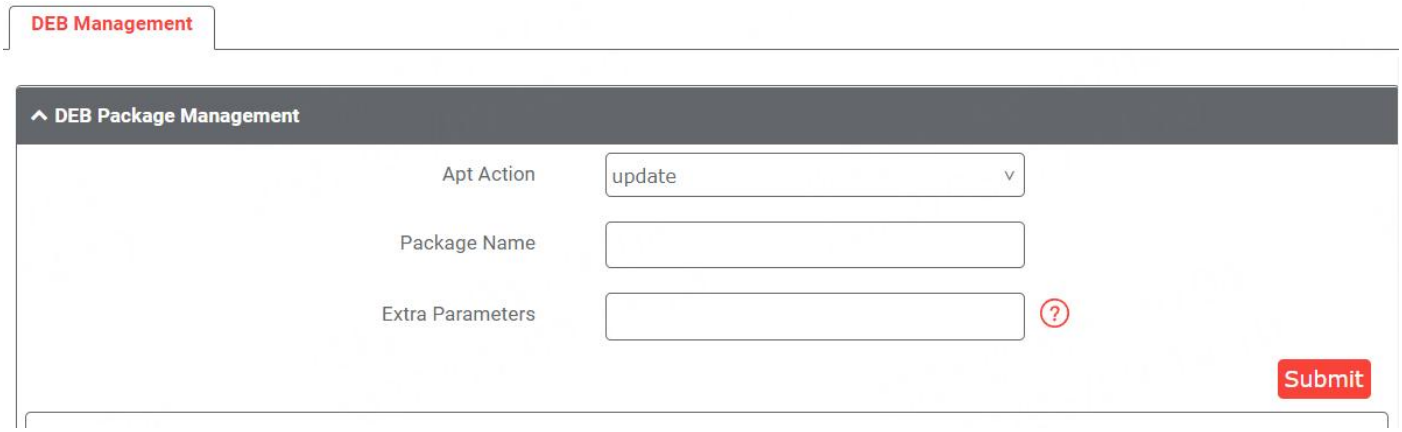
Click + button to add a new common user. The maximum rule count is 5.



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Role	Select from “Guest” and “User”. • Guest: Guest only can view the configuration of router under this level • User: User can view and set the configuration of router under this level	Guest
Username	Set the Username; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Password	Set the password which at least contains 5 characters; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null

4.6.10 DEB Management

This section allows you to manage your own Debian packages.

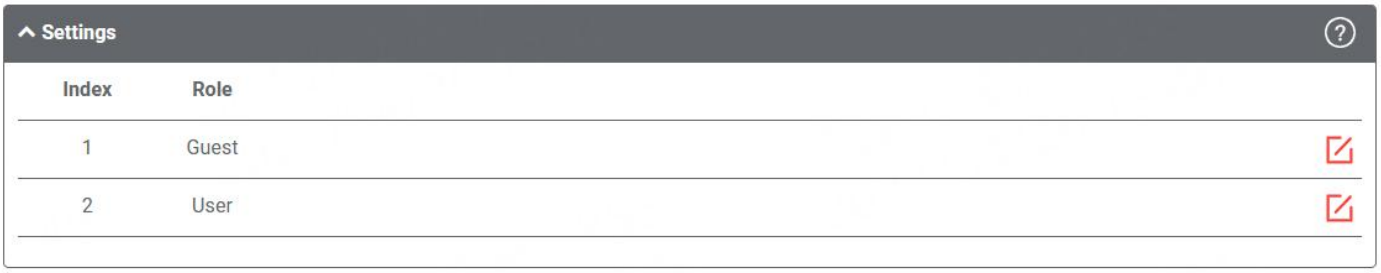


Item	Description	Default
Apt Action	Select from “update”, “install”, “clean”, “remove”, “show”. • update: to update the apt. • Install: to install the apt. • Remove: to remove the apt. • Clean: to clean the apt. • Show: to show the apt list.	--
Package Name	Enter the package name to implement.	--
Extra Parameters	More parameters of 'apt' command, such as '--purge', etc.	Null

4.6.11 Role Management

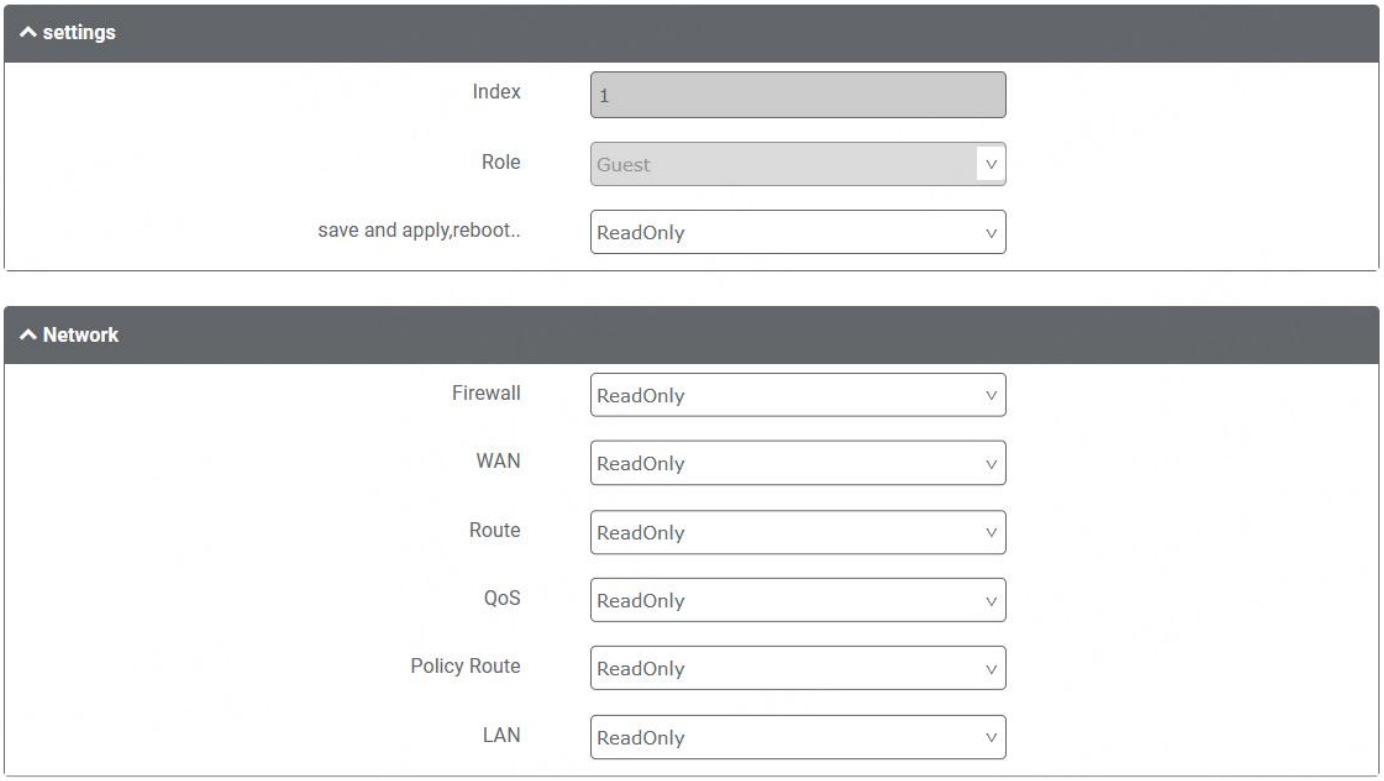
This section is used to manage user roles and manage permissions for users in different roles.

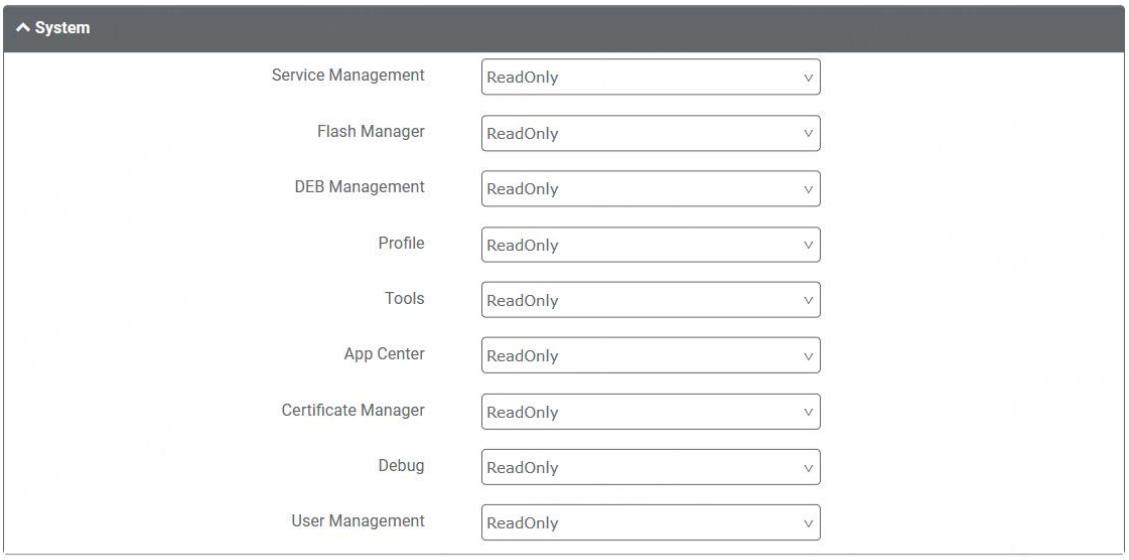
Role Management

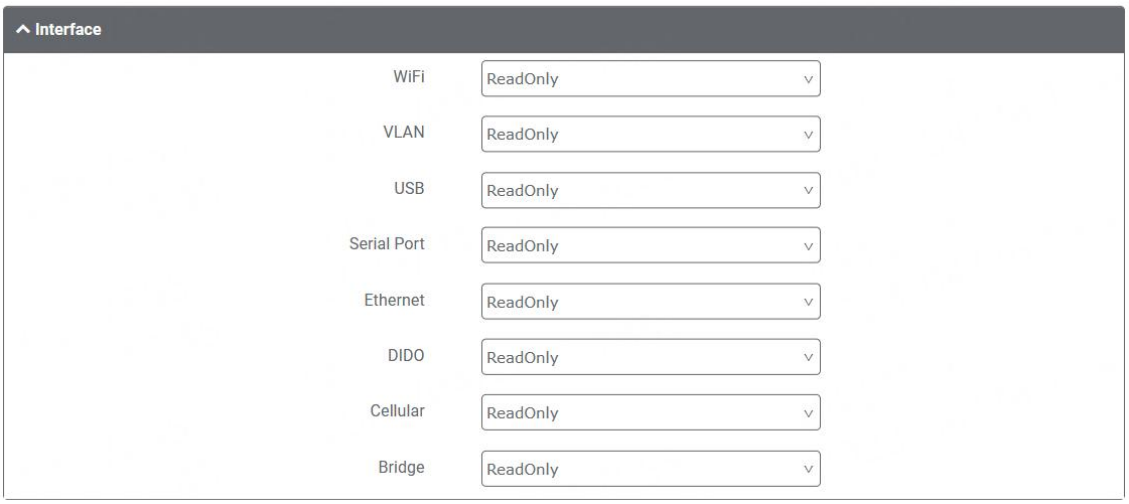


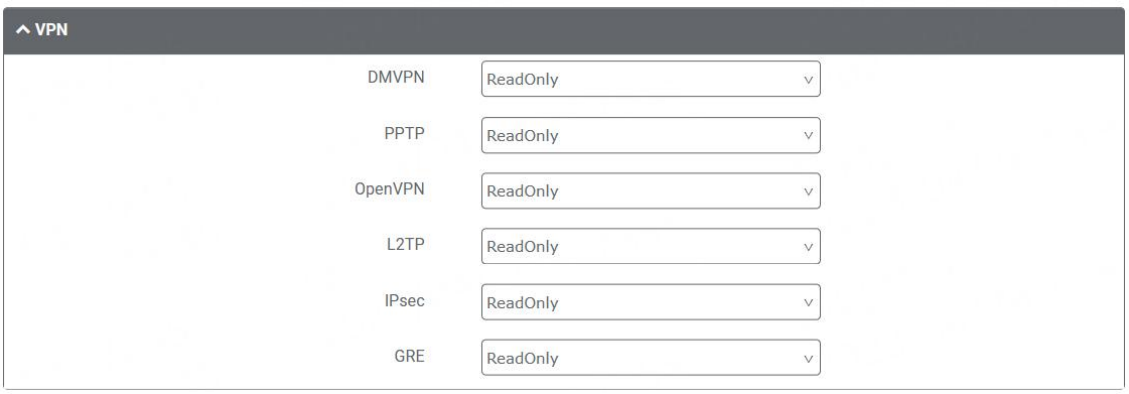
Role Names @ Role Management		
Item	**Description**	**Default**
Guest	Enter a visitor name; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Guest
User	Enter a editor name; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	User

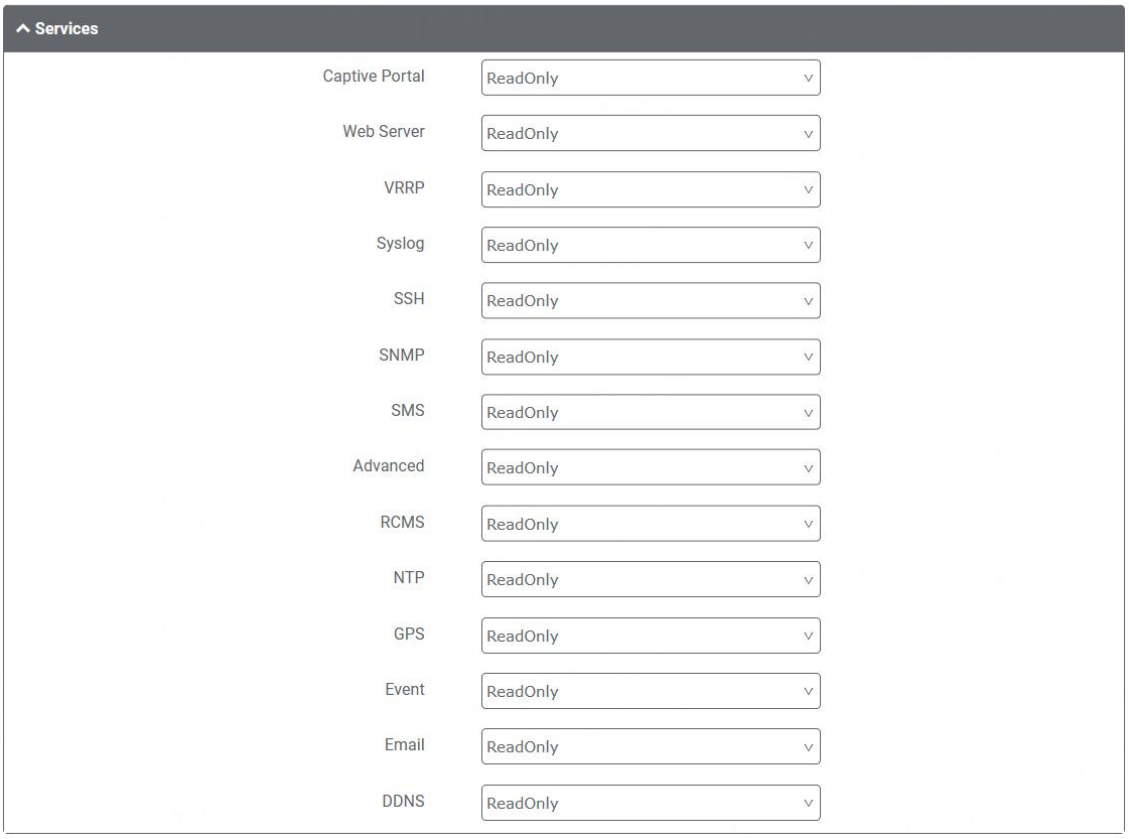
Click to edit Visitor/Editor permission.




System
Service Management
ReadOnly
Flash Manager
ReadOnly
DEB Management
ReadOnly
Profile
ReadOnly
Tools
ReadOnly
App Center
ReadOnly
Certificate Manager
ReadOnly
Debug
ReadOnly
User Management
ReadOnly


Interface
WiFi
ReadOnly
VLAN
ReadOnly
USB
ReadOnly
Serial Port
ReadOnly
Ethernet
ReadOnly
DIDO
ReadOnly
Cellular
ReadOnly
Bridge
ReadOnly


VPN
DMVPN
ReadOnly
PPTP
ReadOnly
OpenVPN
ReadOnly
L2TP
ReadOnly
IPsec
ReadOnly
GRE
ReadOnly



User Permission @ Role Management	
Item	**Description**
None	User have no permission to access or modify this setting.
ReadOnly	User only have permission to read.
Read/Write	User have permission to access or modify this setting.

Note:

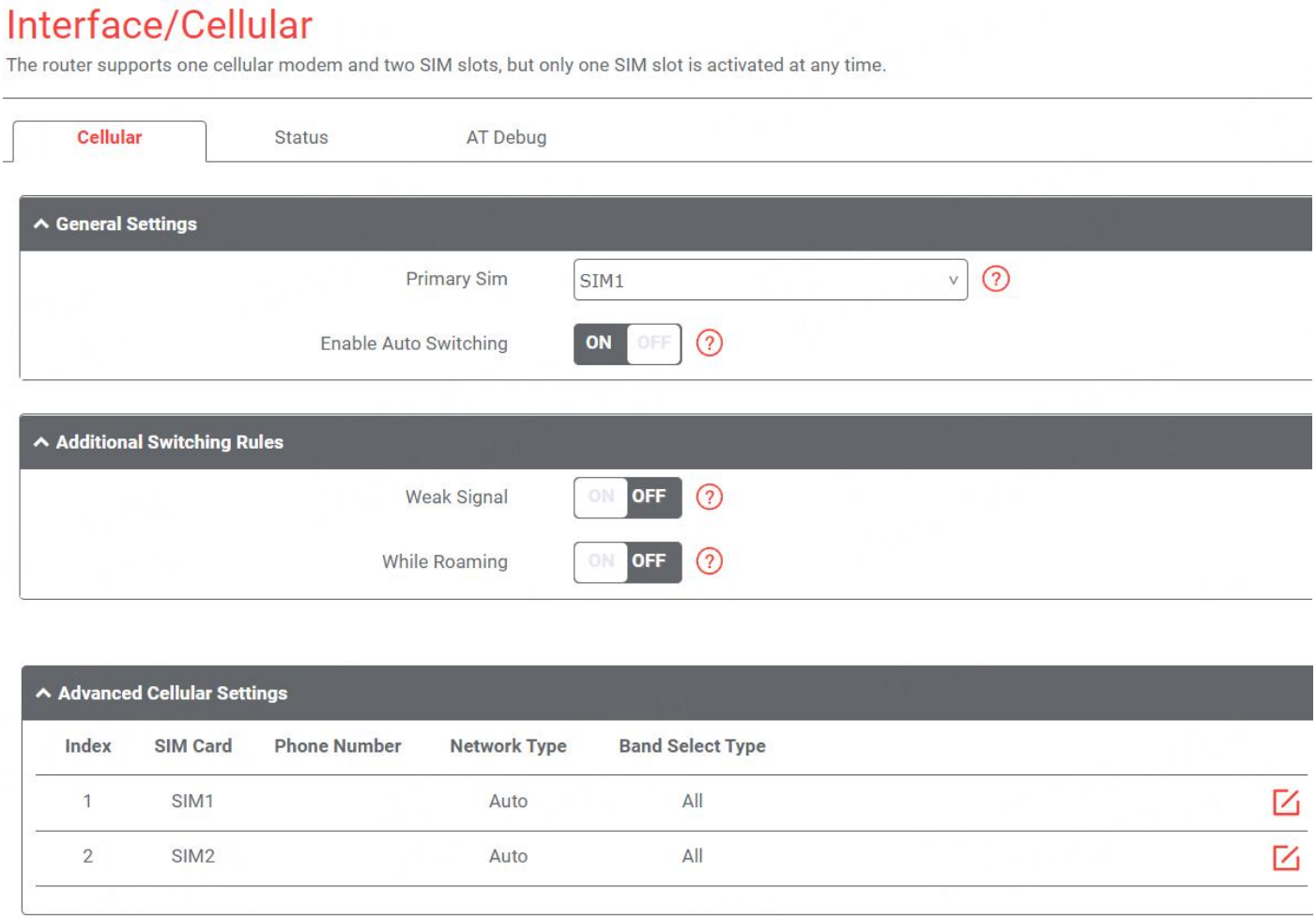
1. When logging in with Guest/User, “Profile” is not available.
2. When Guest “Save and apply, reboot” permission was set to “ReadOnly”. After logging as Guest, “save and apply”, “reboot” buttons will not be displayed.

Chapter 5 Configuration Examples

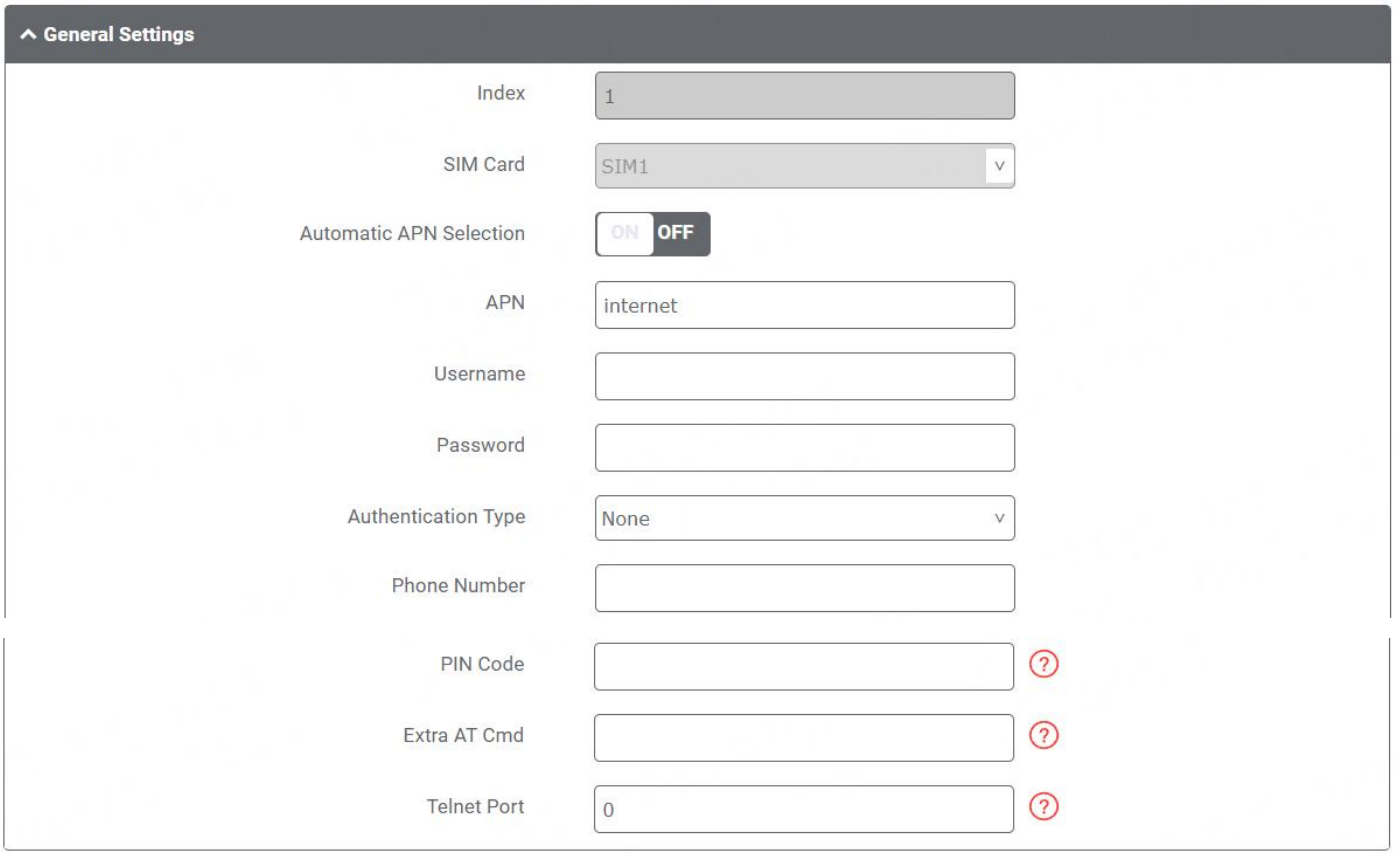
4.1 Cellular

4.1.1 Cellular APN Manual Setting and Cellular Dial-up.

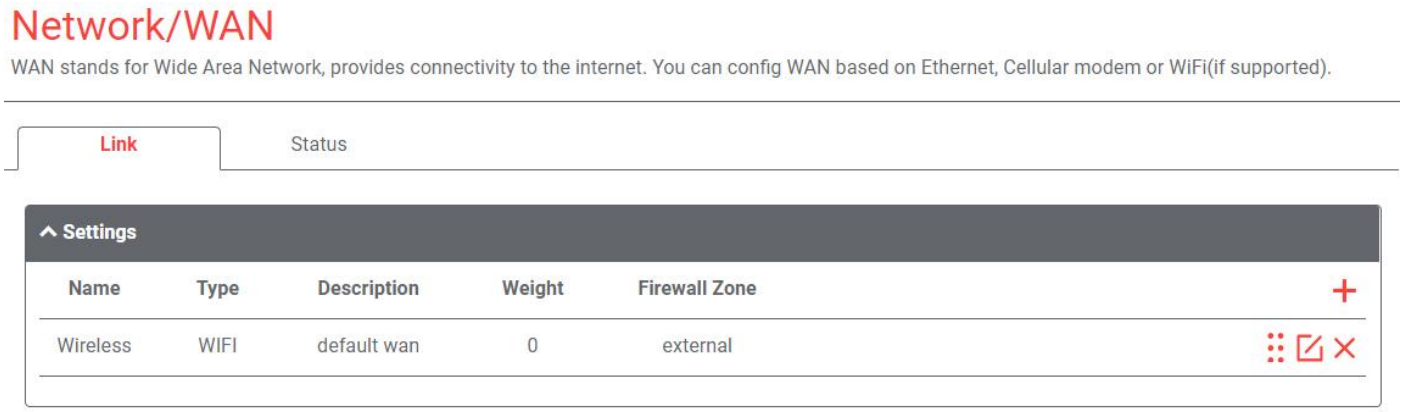
This section shows you how to configure the APN for Cellular Dial-up. Connect the device correctly and insert the SIM card, then open the web configuration page. Under the homepage menu, click "**Interface > Cellular > Cellular "** to go to the cellular configuration page.



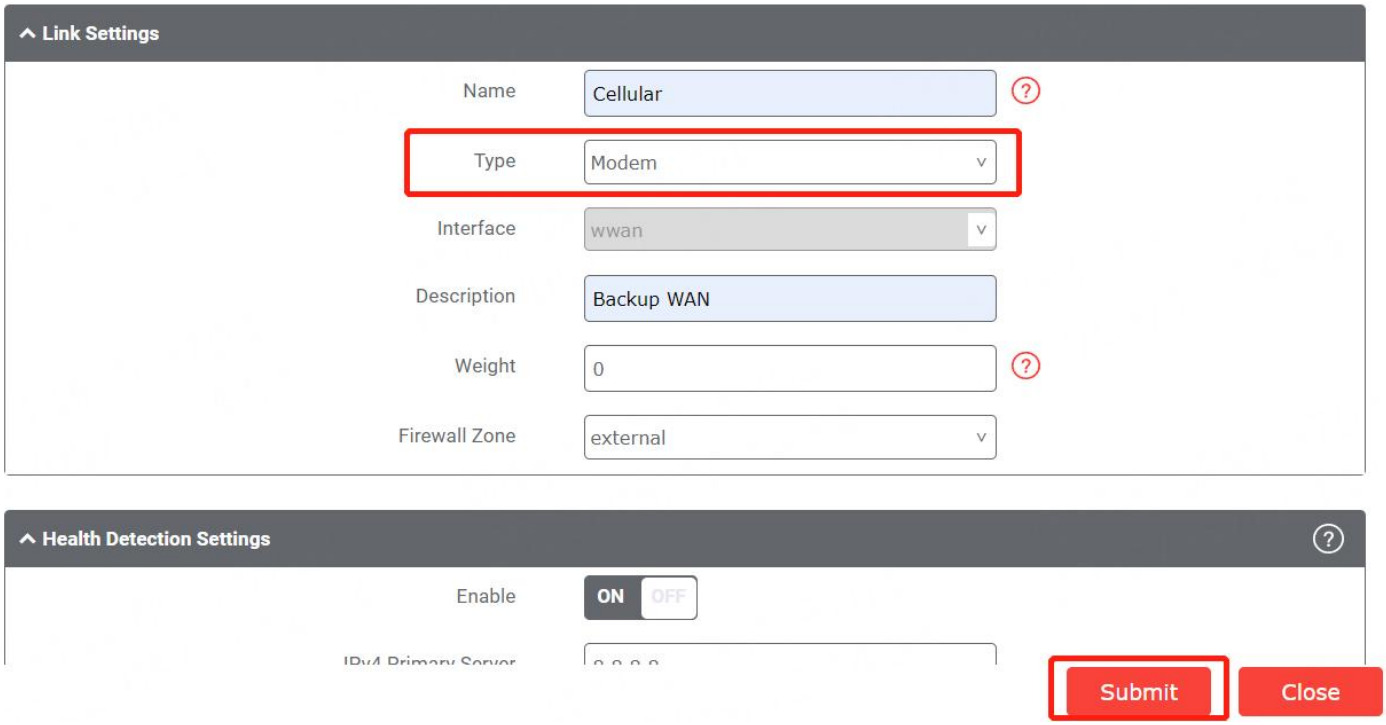
Click  to set its parameters according to the current ISP.



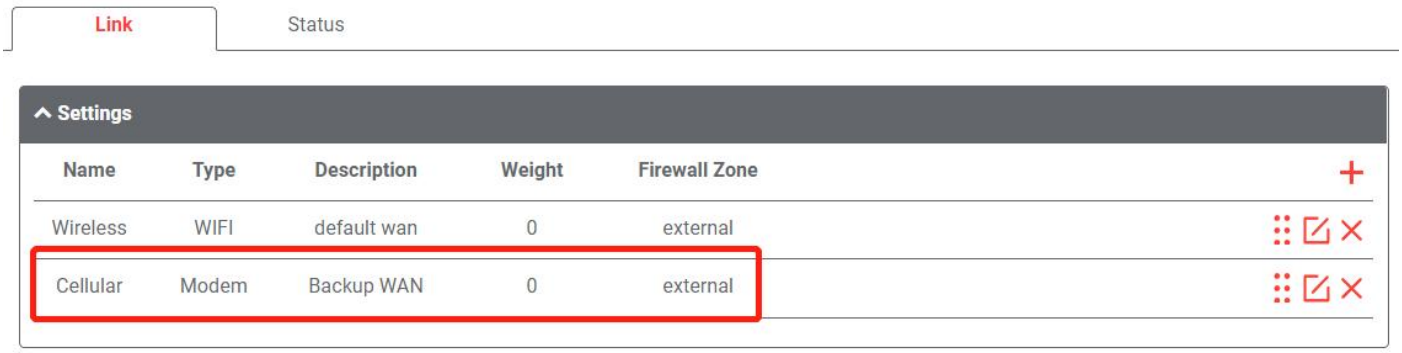
Then Click **"Network> WAN> Link"** go to the WAN configuration page.



Click + to add one link for cellular dial-up, select "Modem" as the link type, then click Submit to submit.



After save and apply, the new cellular WAN link will take effect.



4.1.2 SMS Remote Control

MG460 supports remote control via SMS. You can use following commands to get the status of the router, and set all the parameters of the router.

SMS command have the following structures:

1. Password mode—Username: **Password;cmd1;cmd2;cmd3; …cmdn** (available for every phone number).
2. Phonenum mode-- **Password; cmd1; cmd2; cmd3; … cmdn** (available when the SMS was sent from the phone number which had been added in router's phone group).
3. Both mode-- **Username: Password;cmd1;cmd2;cmd3; …cmdn** (available when the SMS was sent from the phone number which had been added in router's phone group).

Note: All command symbols must be entered in the half-angle mode of the English input method.

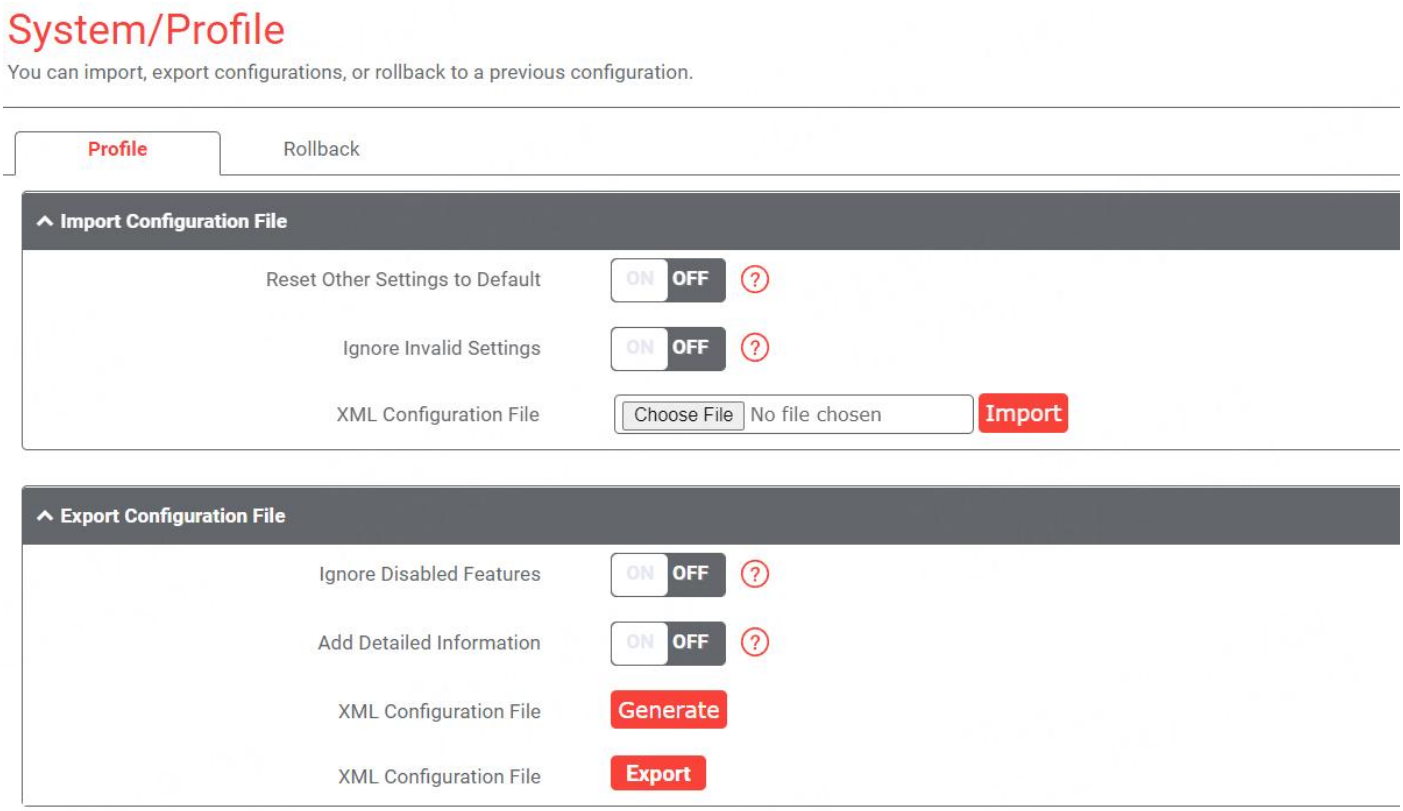
SMS command Explanation:

1. Username and Password: Use the same username and password as WEB manager for authentication.
2. **cmd1, cmd2, cmd3 to cmdn**, the command format is the same as the CLI command, more details about CLI cmd

please refer to **5.1 What Is CLI**.

Note: Download the configure XML file from the configured web browser. The format of SMS control command can refer to the data of the XML file.

Go to "**System > Profile > Export Configuration File**", click Generate to generate the XML file and click Export to export the XML file.



XML command:

```
<lan>
<network max_entry_num="5">
<id>1</id>
<interface>lan0</interface>
<ip>172.16.24.24</ip>
<netmask>255.255.0.0</netmask>
<mtu>1500</mtu>
```

SMS cmd:

set lan network 1 interface lan0
set lan network 1 ip 172.16.24.24
set lan network 1 netmask 255.255.0.0
set lan network 1 mtu 1500

3. The semicolon character (';') is used to separate more than one commands packed in a single SMS.
4. E.g.

admin:admin;status system

In this command, username is "admin", password is "admin", control command is "status system", and the function of the command is to get the system status.

SMS received:

firmware_version = 2.0.0
firmware_version_full = "2.0.0 (60b55c0)"
kernel_version = 5.4.24-2.0.0
hardware_version = 0.0
operation_system = "Debian GNU/Linux 11.3"
device_model = ""
serial_number = 2204190667030003
temperature_interval = 53.0
uptime = "0 days, 00:12:06"
system_time = "Thu May 19 16:52:22 2022"
ram_usage = 392M/448M
cpu_usage = "22569s Idle/71405s Total /1 cpus"
disk_usage = 1.9G/7.1G

admin:admin;reboot

In this command, username is “admin”, password is “admin”, and the command is to reboot the Router.

SMS received:

OK

admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet_access false

In this command, username is “admin”, password is “admin”, and the command is to disable the remote_ssh and remote_telnet access.

SMS received:

OK
OK

admin:admin;set lan network 1 interface lan0;set lan network 1 ip 172.16.24.24;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

In this command, username is “admin”, password is “admin”, and the commands is to configure the LAN parameter.

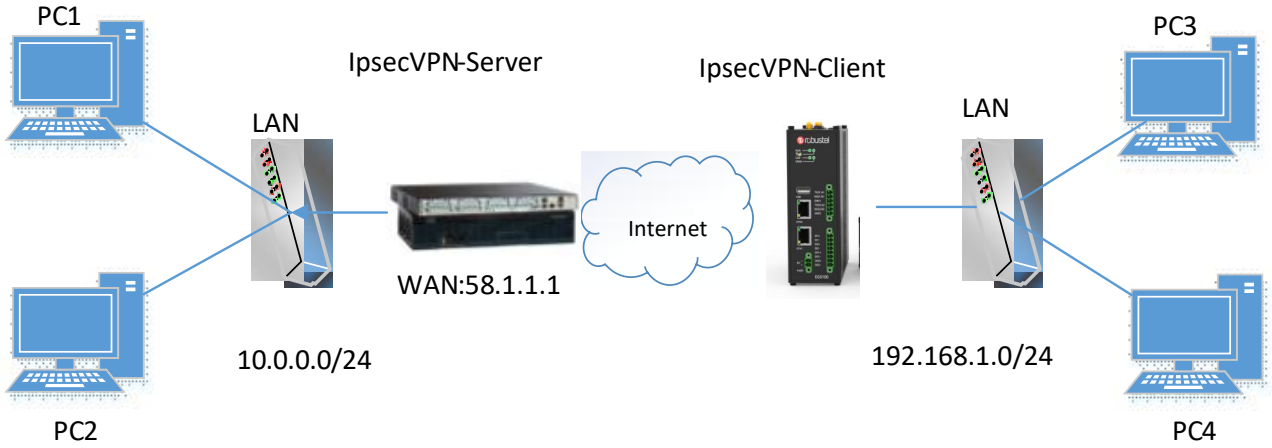
SMS received:

OK
OK
OK
OK

4.2 VPN Configuration Examples

4.2.1 IPsec VPN

IPsec VPN topology (server-side and client-side IKE and SA parameters must be configured the same).



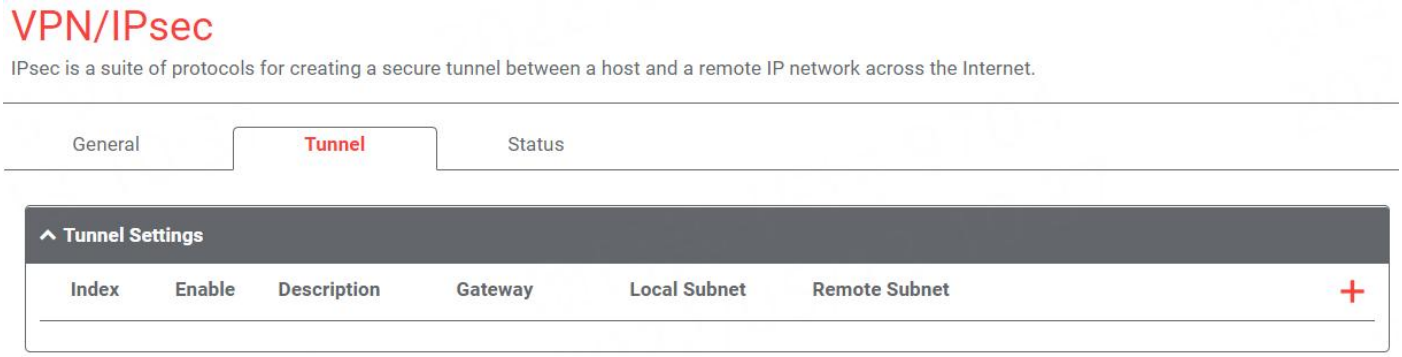
IPsecVPN_Server:

Cisco 2811:

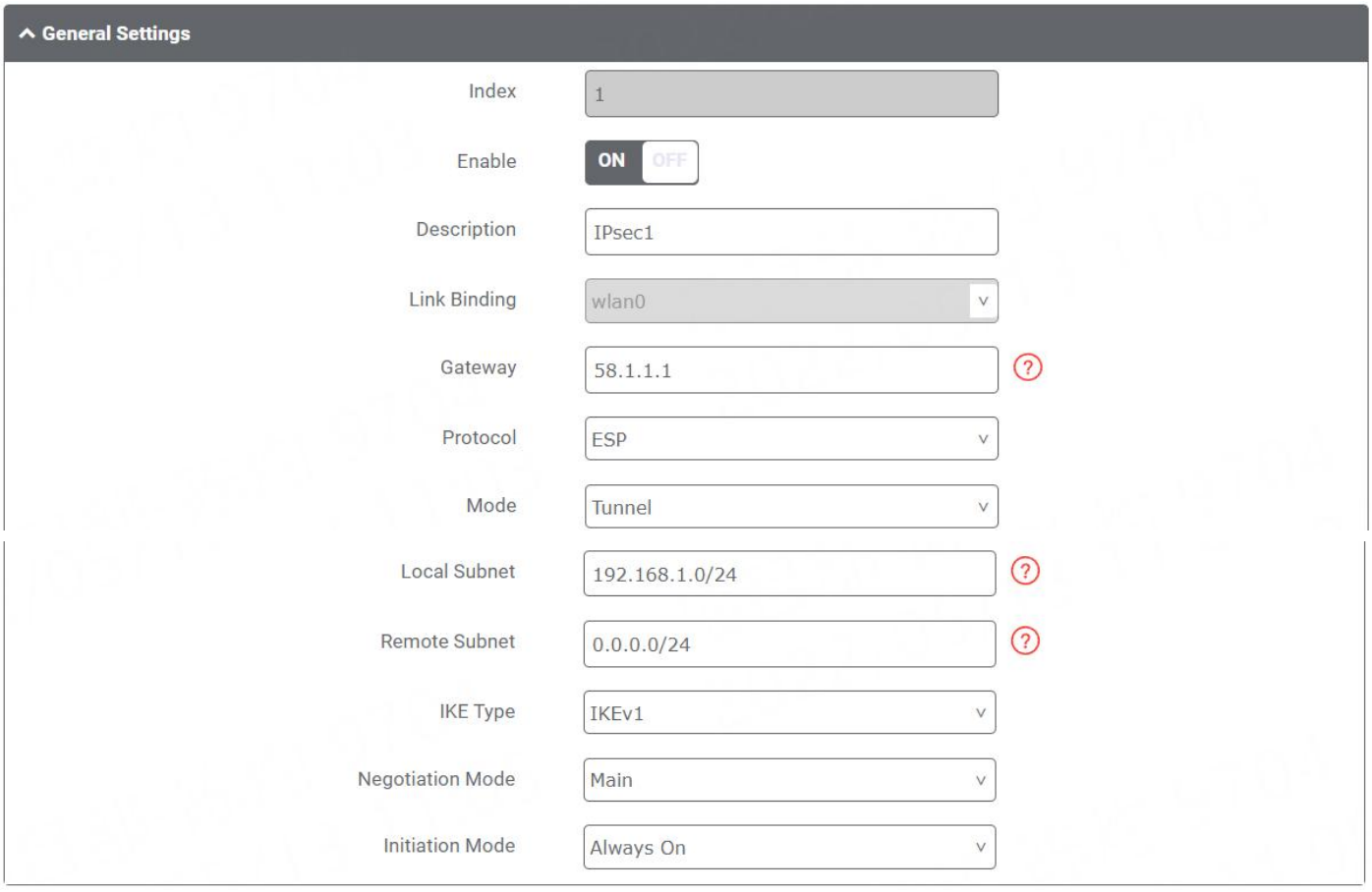
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0


Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac


Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit


Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit



Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

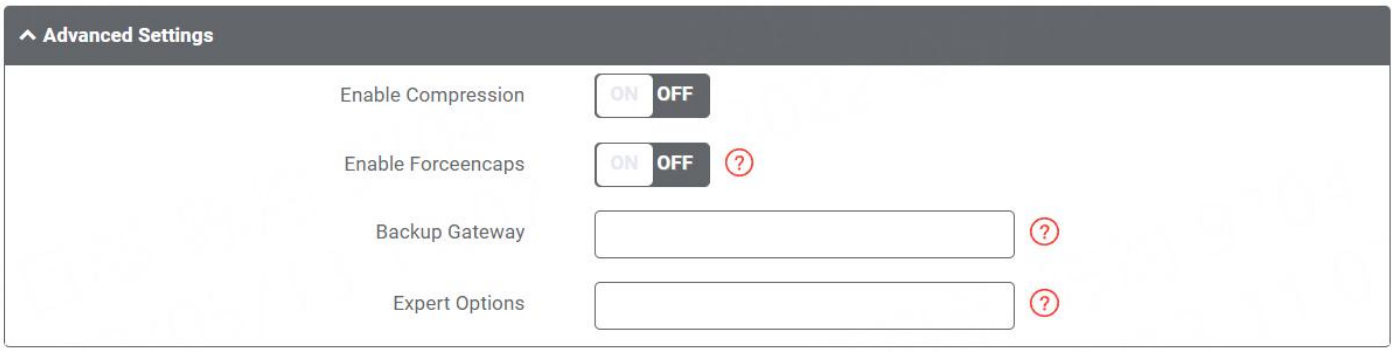
IPsec VPN_Client:

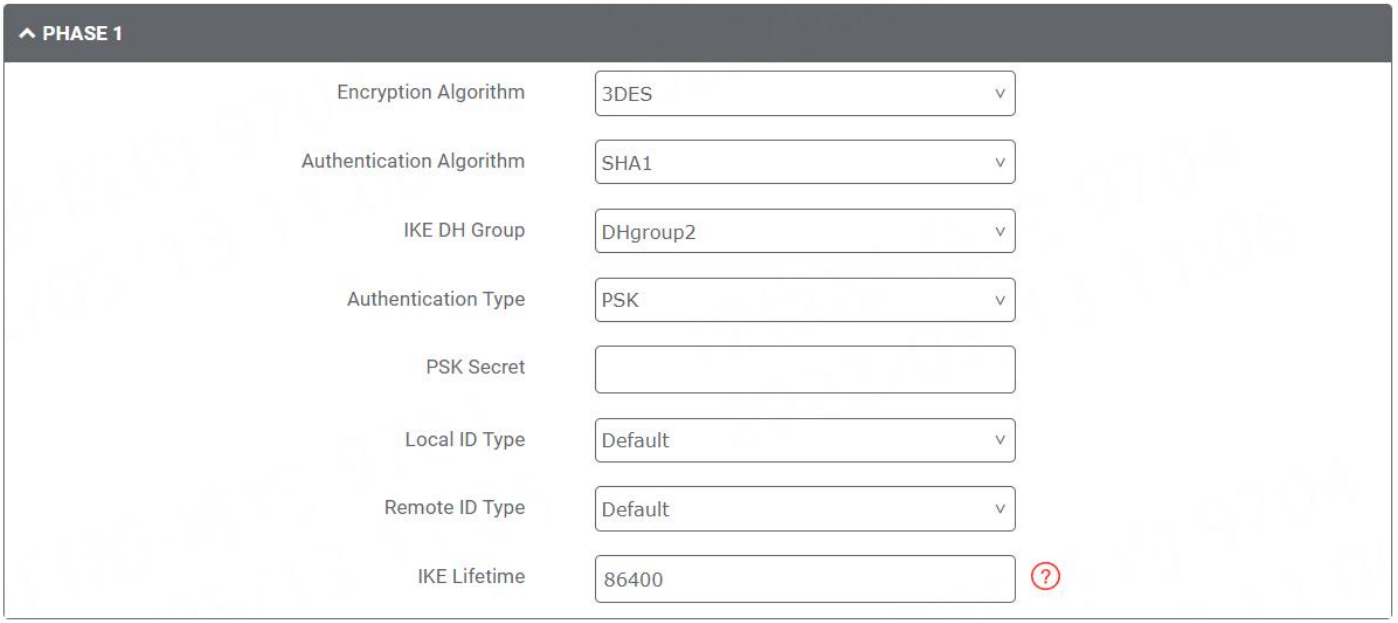
The window is displayed as below by clicking "**VPN > IPsec > Tunnel**."

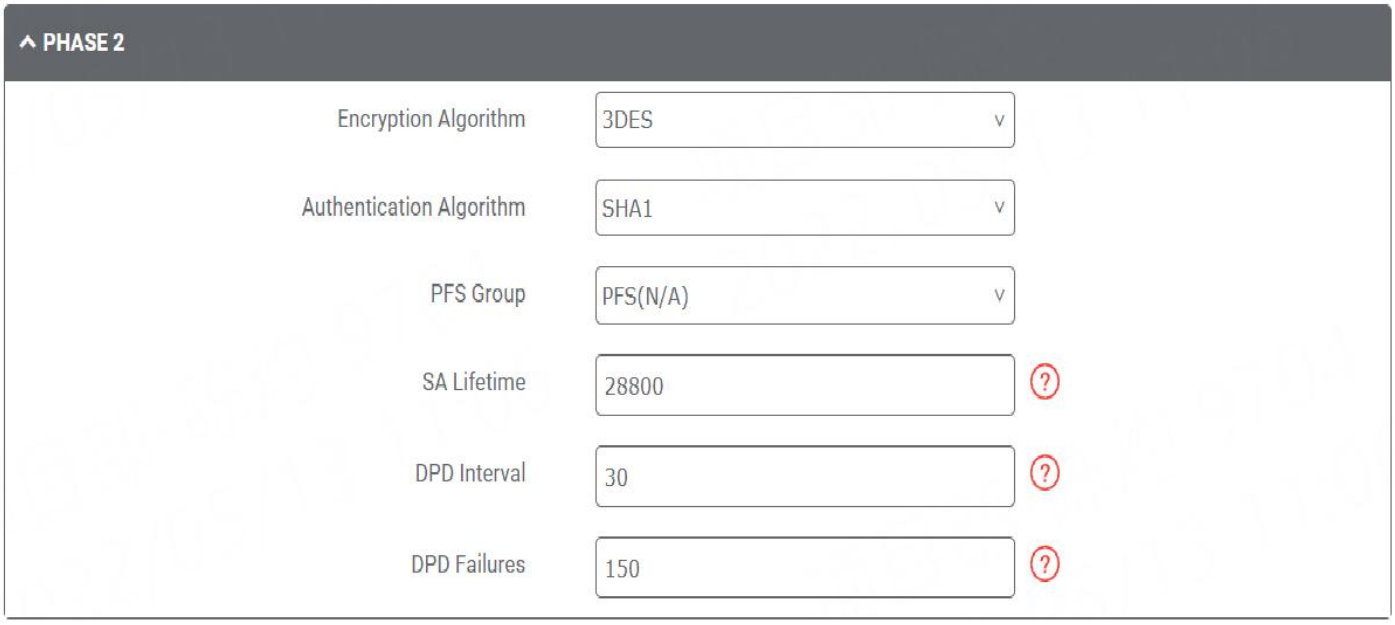


Click + button and set the parameters of IPsec Client as below.





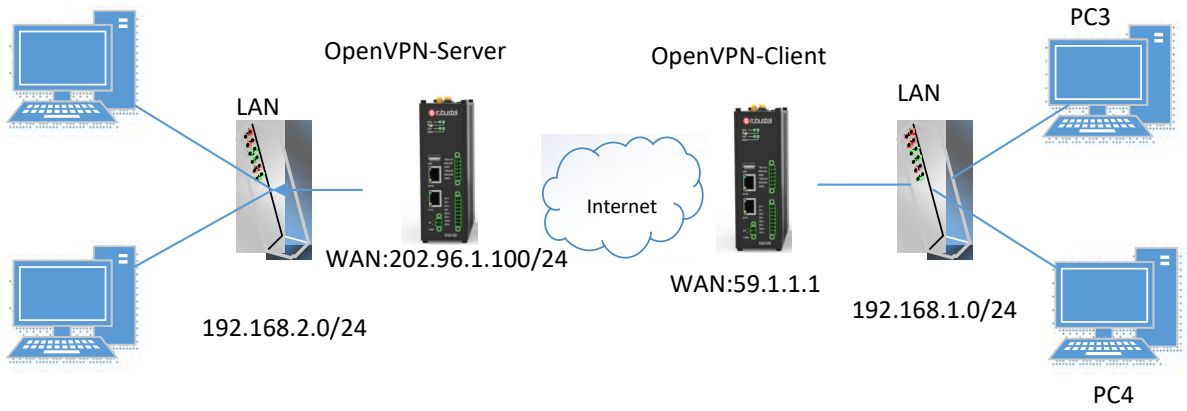




When finished, click Submit to submit and click for the configuration to take effect.

4.2.2 OpenVPN

OpenVPN supports two modes, including Client and P2P. Here takes Client as an example.



OpenVPN_Server:

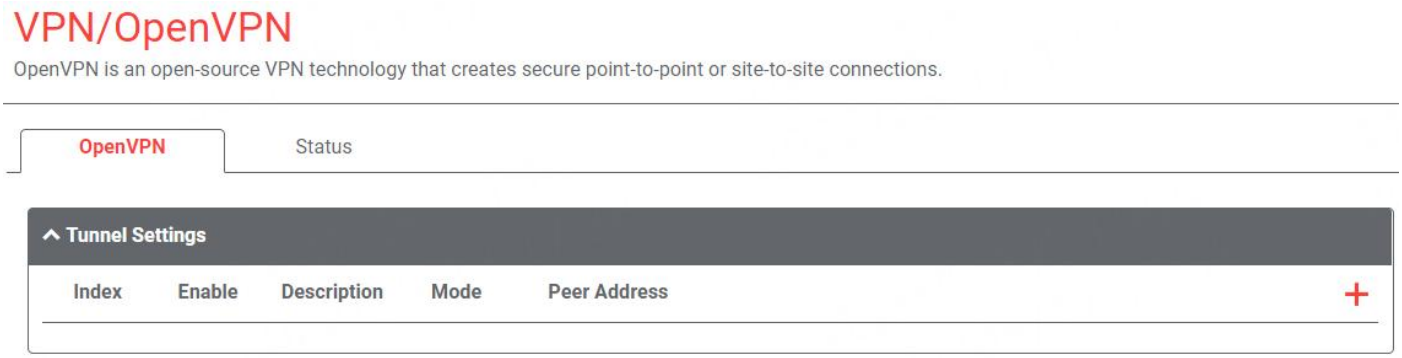
Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server:

local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3

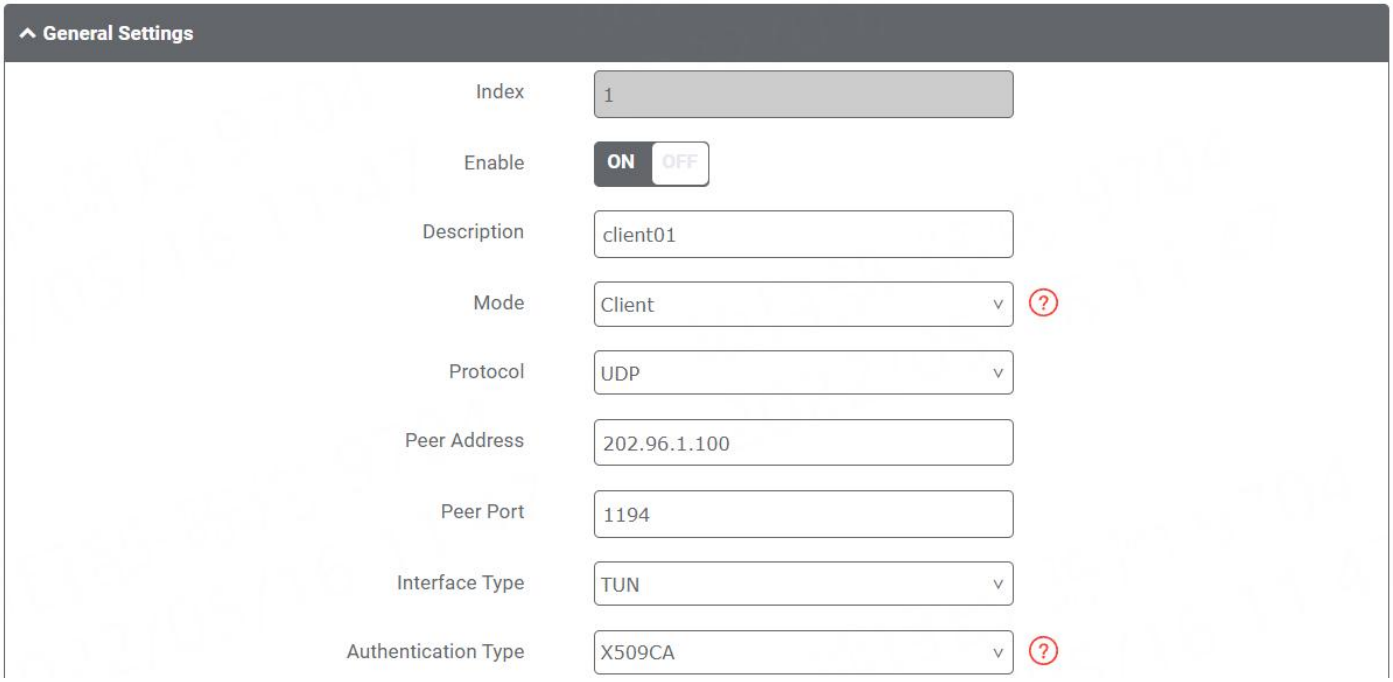
Note: For more configuration details, please contact your technical support engineer.

OpenVPN_Client:

Click "**VPN > OpenVPN > OpenVPN"** as below.



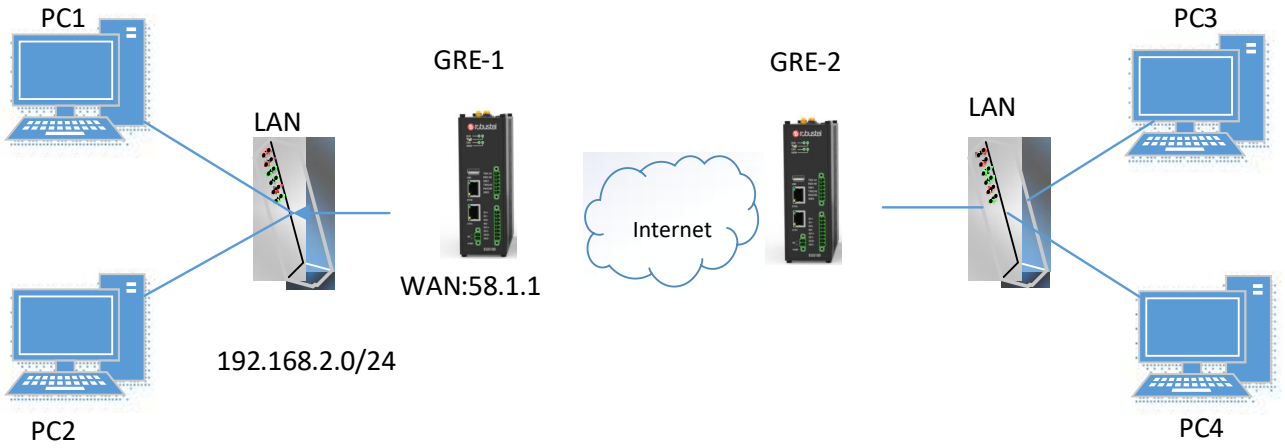
Click + to configure the Client01 as below.



When finished, click Submit to submit and click for the configuration to take effect.

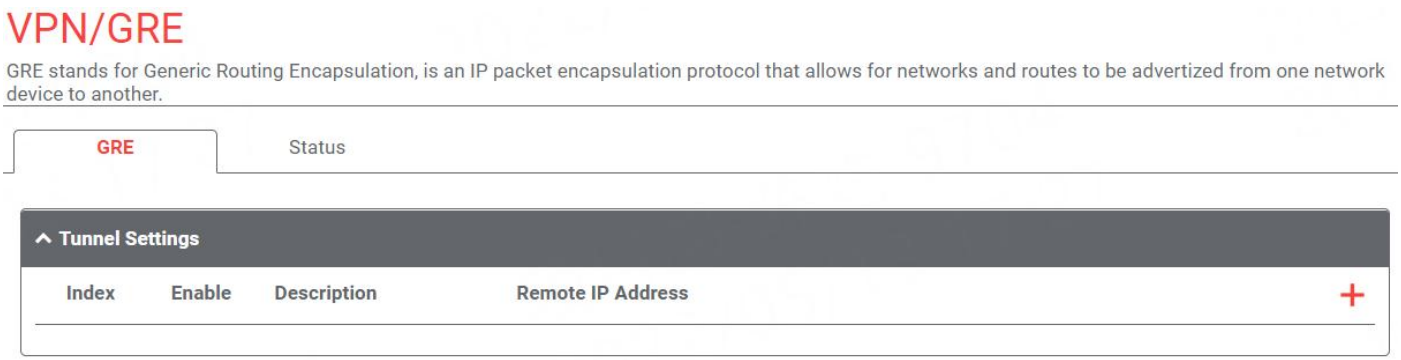
4.2.3 GRE VPN

GRE VPN topology

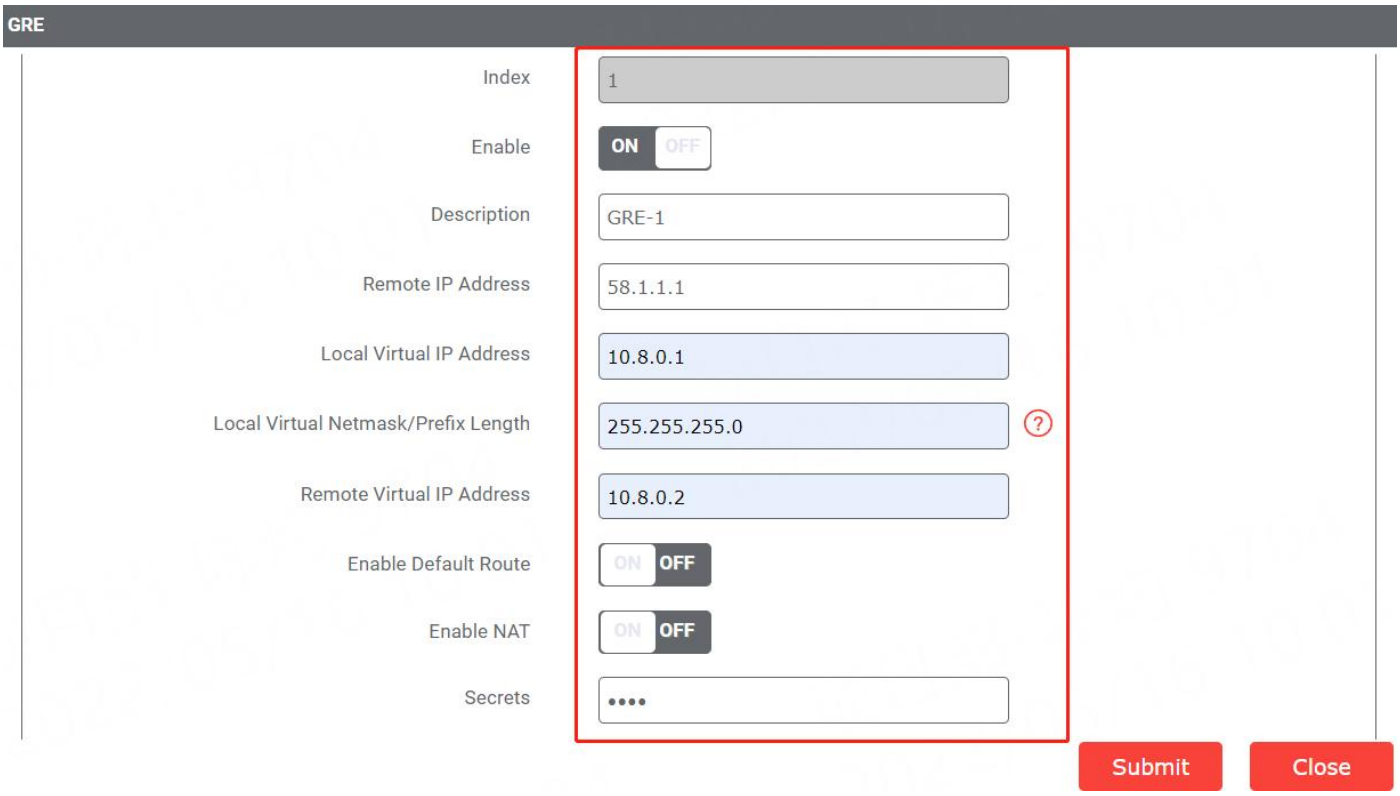


GRE-1：

The window is displayed as below by clicking "**VPN > GRE > GRE"**.



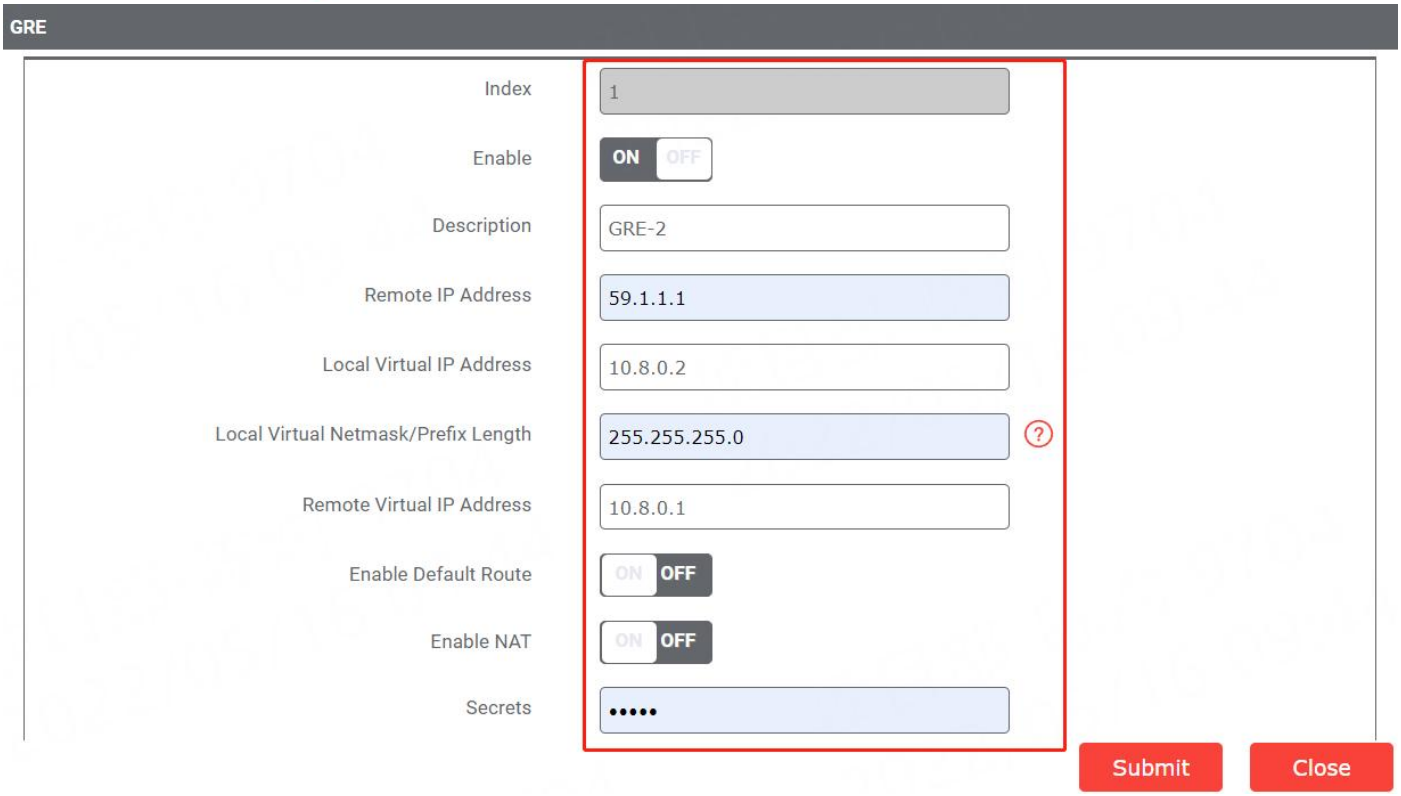
Click + button and set the parameters of GRE-1 as below.



When finished, click Submit to submit and click for the configuration to take effect.

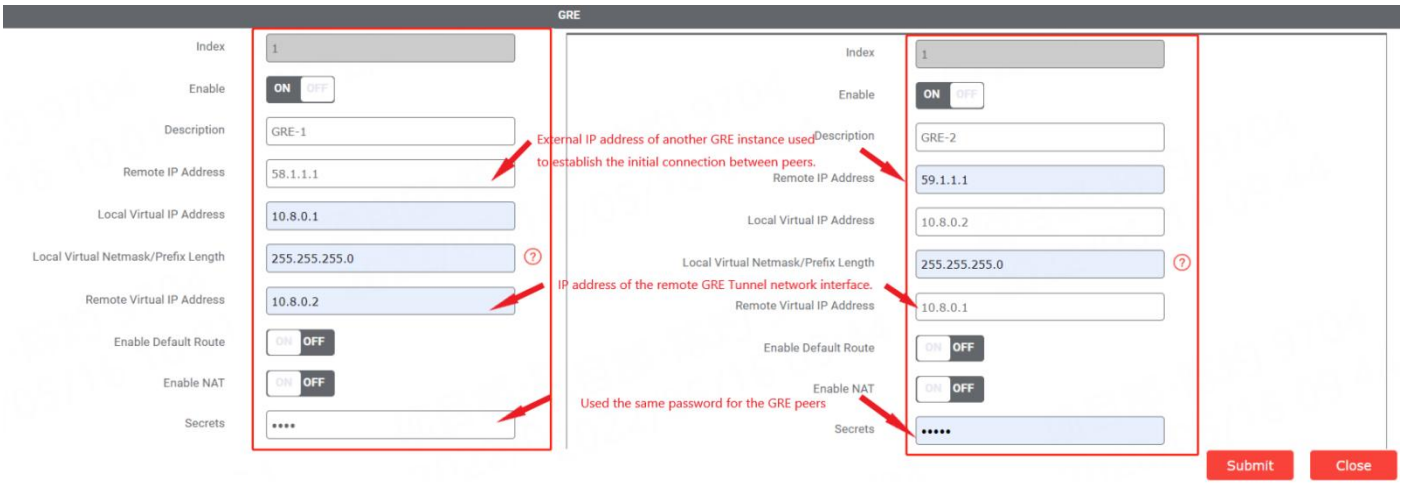
GRE-2:

On the remote side, click + button and set the parameters of GRE-2 as below.



When finished, click Submit to submit and click ✓ for the configuration to take effect.

The comparison between GRE-1 and GRE-2 is as below.



Chapter 6 Introductions for CLI

6.1 What Is CLI

Command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the SSH or through a telnet network connection. After establishing a Telnet or SSH connection with the router, enter the login account and password (here take admin/admin for example) to enter the configuration mode of the router, as shown below.

Route login:

Router login: admin

Password: admin(could be different)

#

CLI commands:

```
# ?
#
  !                 Comments
  add               Add a list entry of configuration
  clear             Clear statistics
  config            Configuration operation
  debug             Output debug information to the console
  del               Delete a list entry of configuration
  do                Set the level state of the do
  exit              Exit from the CLI
  help              Display an overview of the CLI syntax
  ovpn_cert_get     Download OpenVPN certificate file via http or ftp
  ping              Send messages to network hosts
  reboot            Halt and perform a cold restart
  set               Set system configuration
  show              Show system configuration
  status            Show running system information
  tftpupdate        Update firmware or configuration file using tftp
  traceroute        Print the route packets trace to network host
  trigger           Trigger action
  urlupdate         Update firmware via http or ftp
  ver               Show version of firmware
```

6.2 How to Configure the CLI

Following is a table about the description of help and the error should be encountered in the configuring program.

Commands /tips	Description
?	Typing a question mark "?" will show you the help information. eg. # config（Press '?'） config Configuration operation # config（Press spacebar +'?'） commit Save the configuration changes and take effect changed configuration save_and_apply Save the configuration changes and take effect changed configuration loaddefault Restore Factory Configuration
Ctrl+c	Press these two keys at the same time, except its "copy" function but also can be used for "break" out of the setting program.
Syntax error: The command is not completed	Command is not completed.
Tick space key+ Tab key	It can help you finish you command. Example: # config (tick enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply loaddefault
#config commit # config save_and_apply	When your setting finished, you should enter those commands to make your setting take effect on the device. **Note:** Commit and save_and_apply plays the same role.

6.3 Commands Reference

Commands	Syntax	Description
Debug	Debug *parameters*	Turn on or turn off debug function
Show	Show *parameters*	Show current configuration of each function , if we need to see all please using "show running "
Set	Set *parameters*	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add *parameters*	

Note: Download the config.XML file from the configured web browser. The command format can refer to the config.XML file format.

6.4 Quick Start with Configuration Examples

The best and quickest way to master CLI is firstly to view all features from the web page and then read all CLI commands at a time, finally learn to configure it with some reference examples.

Example 1: Show current version

```
# status system
firmware_version = 2.0.0
firmware_version_full = "2.0.0 (60b55c0)"
kernel_version = 5.4.24-2.0.0
hardware_version = 0.0
operation_system = "Debian GNU/Linux 11.3"
device_model = ""
serial_number = 2204190667030003
temperature_interval = 53.0
uptime = "0 days, 00:12:06"
system_time = "Thu May 19 16:52:22 2022"
ram_usage = 392M/448M
cpu_usage = "22569s Idle/71405s Total /1 cpus"
disk_usage = 1.9G/7.1G
#
```

Example 2: CLI for setting Cellular

```
# show cellular all
primary_sim = sim1
auto_switch = false
switch_by_signal = false
rssi_quality = -87
switch_while_roaming = false
sim {
    id = 1
    card = sim1
    phone_number = ""
    pin_code = ""
    extra_at_cmd = ""
    telnet_port = 0
    network_type = auto
    band_select_type = all
    band_settings {
        gsm_850 = false
        gsm_900 = false
        gsm_1800 = false
        gsm_1900 = false
```

```
            wcdma_800 = false
            wcdma_850 = false
            wcdma_900 = false
            wcdma_1900 = false
            wcdma_2100 = false
            wcdma_1700 = false
            wcdma_band19 = false
            lte_band1 = false
            lte_band2 = false
            lte_band3 = false
            lte_band4 = false
            lte_band5 = false
            lte_band7 = false
            lte_band8 = false
            lte_band13 = false
            lte_band17 = false
            lte_band18 = false
            lte_band19 = false
            lte_band20 = false
            lte_band21 = false
            lte_band25 = false
            lte_band28 = false
            lte_band31 = false
            lte_band38 = false
            lte_band39 = false
            lte_band40 = false
            lte_band41 = false
        }
        debug_enable = true
        verbose_debug_enable = false
}
# set(space+space)
ai                  bridge              cellular            ddns                dido
dmvpn               email               ethernet            event               firewall
gps                 gre                 ipsec               l2tp                lan_links
ntp                 openvpn             policy_router       pppoe_bridge        pptp
qos                 rcms                reboot              route               serial_port
sms                 snmp                ssh                 syslog              system
Usb                 syslog              user_management     vlan                vrrp
web_server          wan_links           web_server          wireless

# set cellular(space+?)
  sim    SIM Settings
# set cellular sim(space+?)
  Integer    Index (1..1)
```

```
# set cellular sim 1(space+?)
    card                    SIM Card
    phone_number            Phone Number
    pin_code                PIN Code
    extra_at_cmd            Extra AT Cmd
    telnet_port             Telnet Port
    network_type            Network Type
    band_select_type        Band Select Type
    band_settings           Band Settings
    telit_band_settings     Band Settings
    debug_enable            Debug Enable
    verbose_debug_enable    Verbose Debug Enable
# set cellular sim 1 phone_number 18620435279
OK
…
# config save_and_apply
OK                                  // save and apply current configuration, make you configuration effect
```

Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface for batch scripting
CSD	Circuit Switched Data
CTS	Clear to Send
dB	Decibel
dBi	Decibel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DI	Digital Input
DO	Digital Output
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready

Abbr.	Description
EDGE	Enhanced Data rates for Global Evolution of GSM and IS-136
EMC	Electromagnetic Compatibility
EMI	Electro-Magnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
EVDO	Evolution-Data Optimized
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
ID	identification data
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
kbps	kbits per second
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send

Abbr.	Description
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Guangzhou Robustel Co., Ltd.
Add: 501, Building 2, No. 63, Yong'an Avenue,
Huangpu District, Guangzhou, China 510660
Tel: 400-987-3791
Email: support@robustel.com
Web: www.robustel.com