robustel | Software Manual

RobustOS Software Manual

robustOS

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

About this Document

This document provides web interface information of the RobustOS-based DTU, Router, and Gateway products, including function introduction and operation configuration.

Related Products

M1200, M1201
R1500, R1510, R1510 Lite, R1511, R1511P, R1520
R2000, R2000 Dual, R2000 Ent, R2010, R2011, R2110
R3000, R3000 Lite, R3000 Quad, R3000 LG, R3010
R5020

Trademarks and Permissions

robustel & robustOS are trademarks of Guangzhou Robustel Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective owners.

Disclaimer

The entire document cannot be reproduced in any form without the written permission of the copyright owner. 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 mistaking use of this document.

Technical Support

Tel: +86-20-82321505
Email: support@robustel.com
Web: www.robustel.com

Document History

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

Date	Document Version	Firmware Version	Change Description
Aug. 1, 2022	V1.0.0	V5.0.0 or newer	1. Initial release.
Oct. 16, 2022	V1.1.0	V5.1.0 or newer	Added support for RobustOS V5.1.0 or newer.

Contents

1. Introduction

This software manual, used for all the RobustOS-based products including the DTU, Router, and Gateway products, provides web interface information (configuration and operation).
Please refer to the specific chapter accordingly, as hardware configurations or interfaces may vary on different models.

Related Product	M1200	M1201	R1510	R1510 Lite	R1511	R1520	R2000	R2000 Dual	R2000 Ent	R2010	R2011	R2110	R3000	R3000 Lite	R3000 Quad	R3000 LG	R3010	R5020
SIM Card	2	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	1	2
Ethernet	-	-	2	1	2	5	2	5	5	2	5	4	2	1	4	2	2	4
PoE PD	-	-	-	-	-	*	*	-	*	*	*	*	-	-	-	-	-	*
PoE PSE	-	-	-	-	-	-	-	√	-	-	-	-	-	-	-	-	-	-
Wi-Fi	-	-	√	-	√	√	*	√	√	√	√	√	*	-	*	-	-	√
BLE	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-
GNSS	-	-	-	-	-	*	-	-	-	-	-	*	*	-	*	*	-	*
DI	2	-	√	-	-	√	-	√	-	√	-	√	2	-	-	2	-	√
DO	√	-	√	-	-	√	-	-	-	√	-	√	2	-	-	-	-	√
AI	-	-	-	-	-	√	-	-	-	-	-	-	-	-	-	-	-	-
RS232	√	*	-	-	*	√	-	-	*	*	-	√	√	√	*	*	√	√
RS485	√	*	-	-	*	√	-	-	*	*	-	√	√	√	*	*	√	√
USB Host	-	-	-	-	-	√	-	-	√	-	-	√	√	√	√	√	√	√
RS422	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CAN	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	√	-
Voice (FXS)	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-	-	√	-
MicroSD	-	-	-	-	-	-	-	-	-	-	-	√	√	-	√	√	-	√

*Note: √ = Supported, - = Unsupported, * = Optional*

About RobustOS

RobustOS is a Robustel self-developed and Linux-based operating system designed for Robustel devices. The RobustOS includes basic networking features and protocols providing customers excellent user experience. Meanwhile, Robustel offers a Software Development Kit (SDK) for partners and customers to allow additional customization by using C and C++. It also provides rich Apps to meet fragmented IoT market demands.

2. Initial Configuration

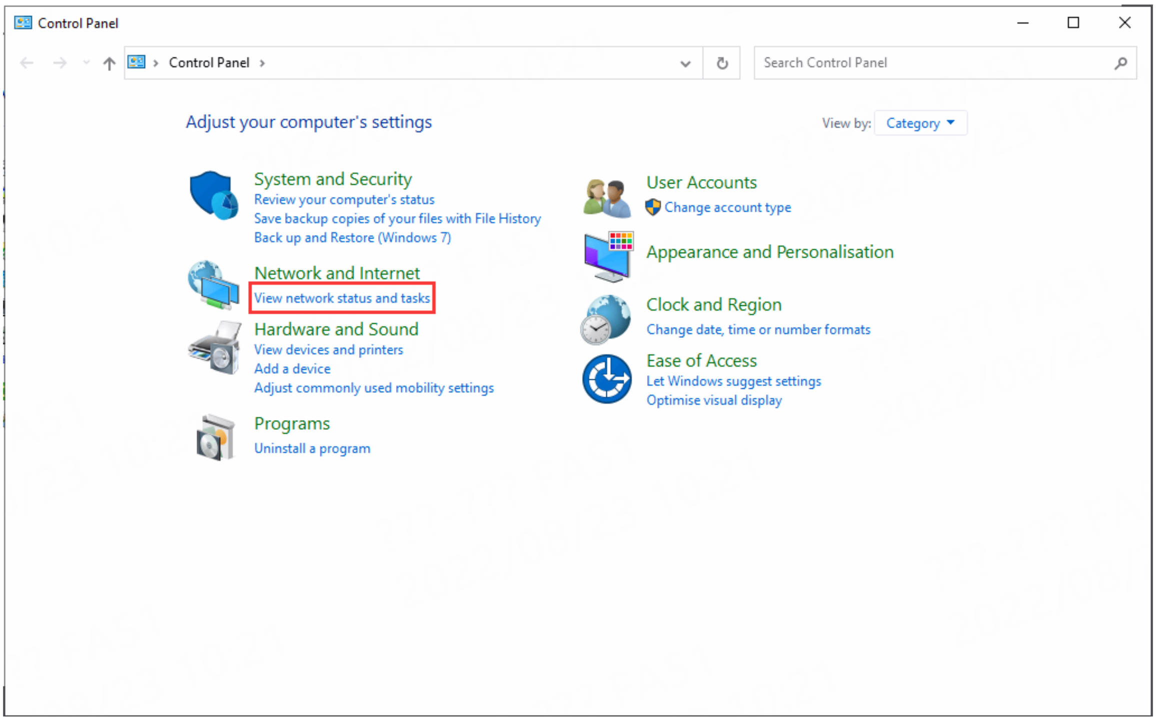
You can configure the device through the web browser, including Microsoft Edge, Google Chrome, Firefox, etc. A web browser is a standard application in the following operating systems: Ubuntu, macOS, Windows7/8/10/11, etc. It provides an easy and user-friendly interface for configuration. There are various ways to connect the device, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC is equipped with an Ethernet port before 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.

2.1 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 configure a static IP address manually within the same subnet of the device. Please refer to the steps below.

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

1. Find the Windows logo key (hereinafter referred to as Win key) of the keyboard, press **Win + R**, type "**Control**" to run **Control Panel**. After opening the Control Panel, left-click on “**View Network Status and Tasks**”.



Control Panel

Control Panel ›

Search Control Panel

Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
Save backup copies of your files with File History
Back up and Restore (Windows 7)

Network and Internet
View network status and tasks

Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings

Programs
Uninstall a program

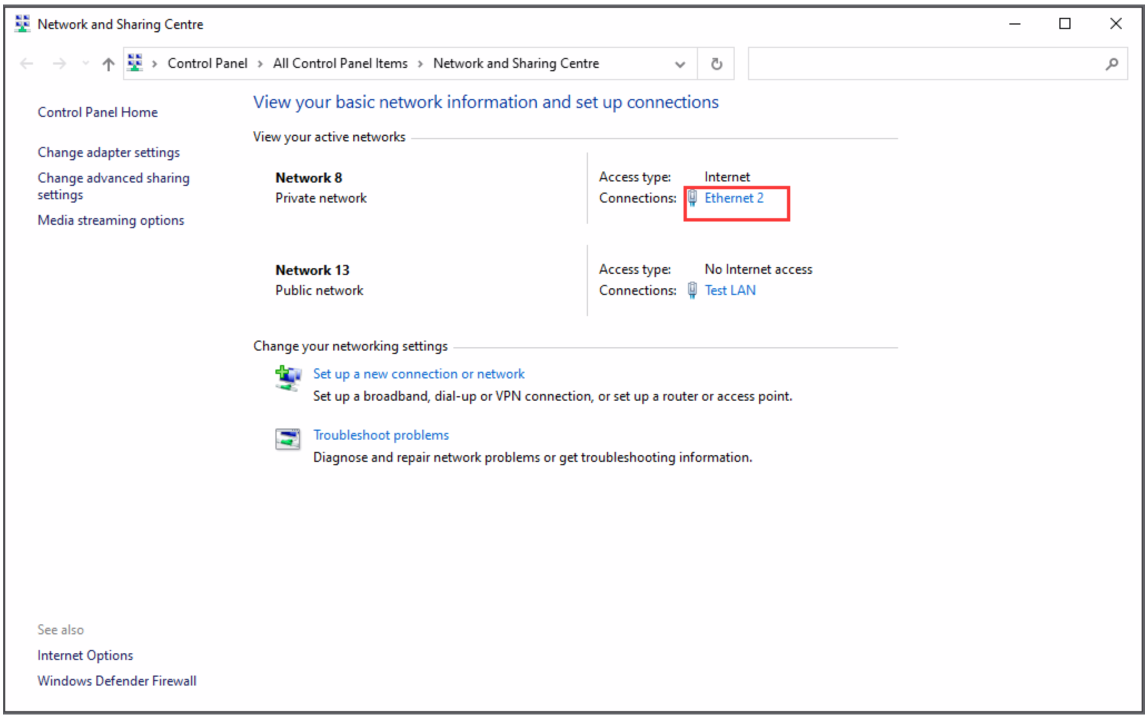
User Accounts
Change account type

Appearance and Personalisation

Clock and Region
Change date, time or number formats

Ease of Access
Let Windows suggest settings
Optimise visual display

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



Network and Sharing Centre
Control Panel > All Control Panel Items > Network and Sharing Centre
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
See also
Internet Options
Windows Defender Firewall

View your basic network information and set up connections

View your active networks

Network 8
Private network
Access type: Internet
Connections: Ethernet 2

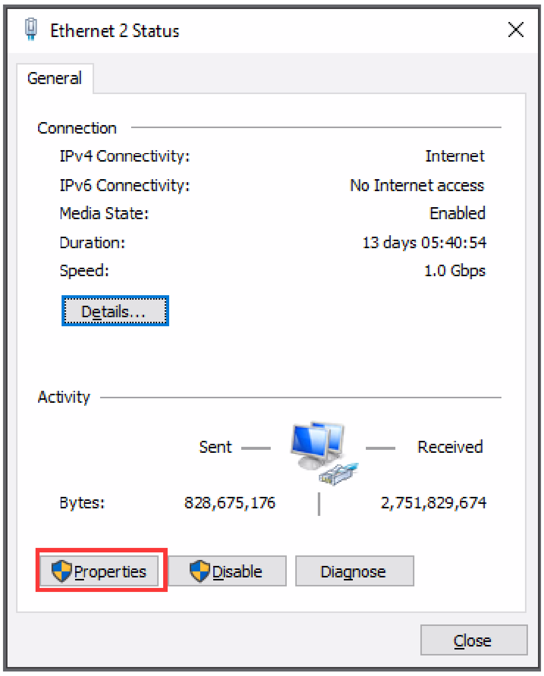
Network 13
Public network
Access type: No Internet access
Connections: Test LAN

Change your networking settings

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

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

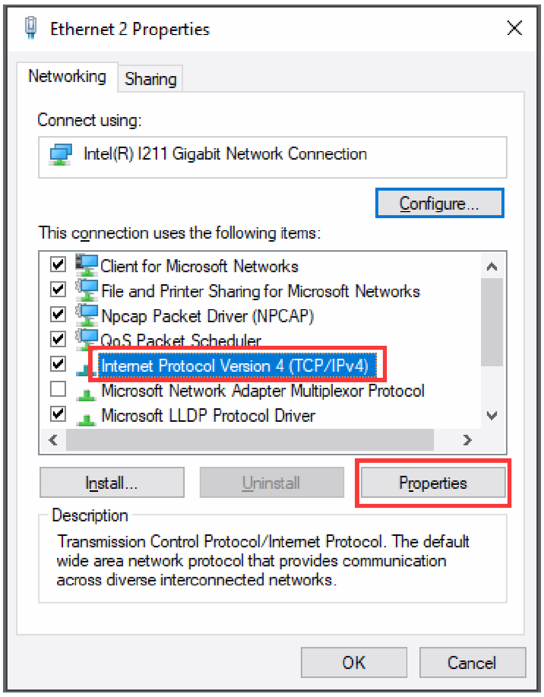
3. Click **Properties** in the window of **Local Area Connection status**.



Connection
IPv4 Connectivity: Internet
IPv6 Connectivity: No Internet access
Media State: Enabled
Duration: 13 days 05:40:54
Speed: 1.0 Gbps

Activity
Sent — Received
Bytes: 828,675,176 | 2,751,829,674

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



Connect using:

Intel(R) I211 Gigabit Network Connection

This connection uses the following items:

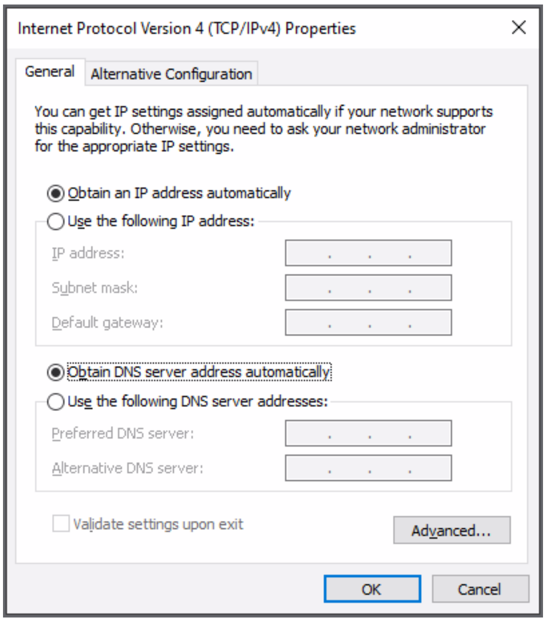
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

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



Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternative Configuration
Advanced...
OK
Cancel

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

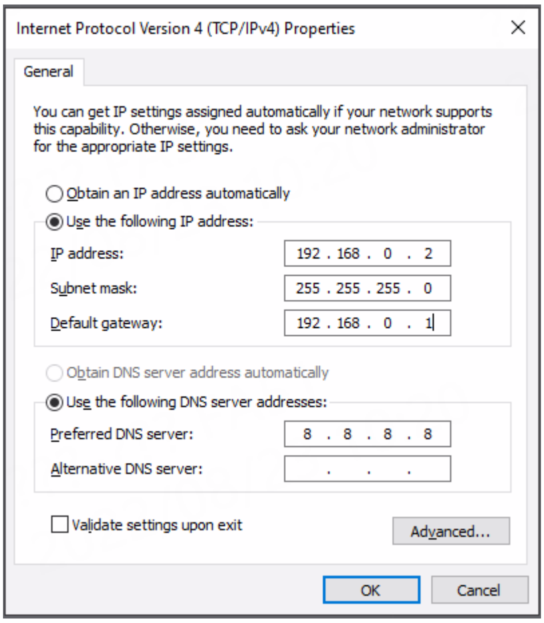
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternative DNS server: . . .

□ Validate settings upon exit

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


Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

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

Preferred DNS server: 8 . 8 . 8 . 8
Alternative DNS server: . . .

□ Validate settings upon exit

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

2.2 Factory Default Settings

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

Item	Description
Username	admin
Password	admin
ETH0	WAN mode or 192.168.0.1/255.255.255.0, LAN mode.
ETH1/2/3/4$^{(*)}$	192.168.0.1/255.255.255.0, LAN mode.
DHCP Server	Enabled

* *There are differences in the number of ETH ports of different devices. For details, please refer to the product specification of the device.*

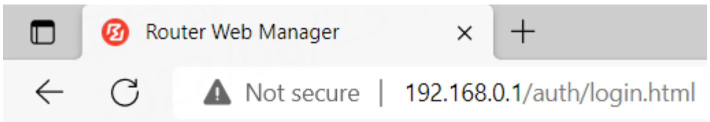
2.3 Factory Reset

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.

2.4 Log in Your Device

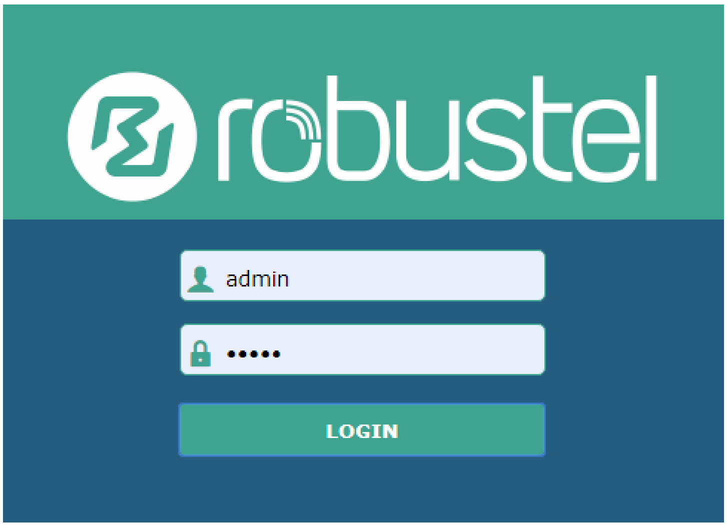
To log in to the management page and view the configuration status of your device, please follow the steps below.

1. On your PC, launch a browser. e.g.: 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 http://192.168.0.1/, though the actual address may vary.
   Note: *If a SIM card with a public IP address is inserted into the device, enter this corresponding public IP address in the browser's address bar to access the device wirelessly.*

   192.168.0.1/auth/login.html

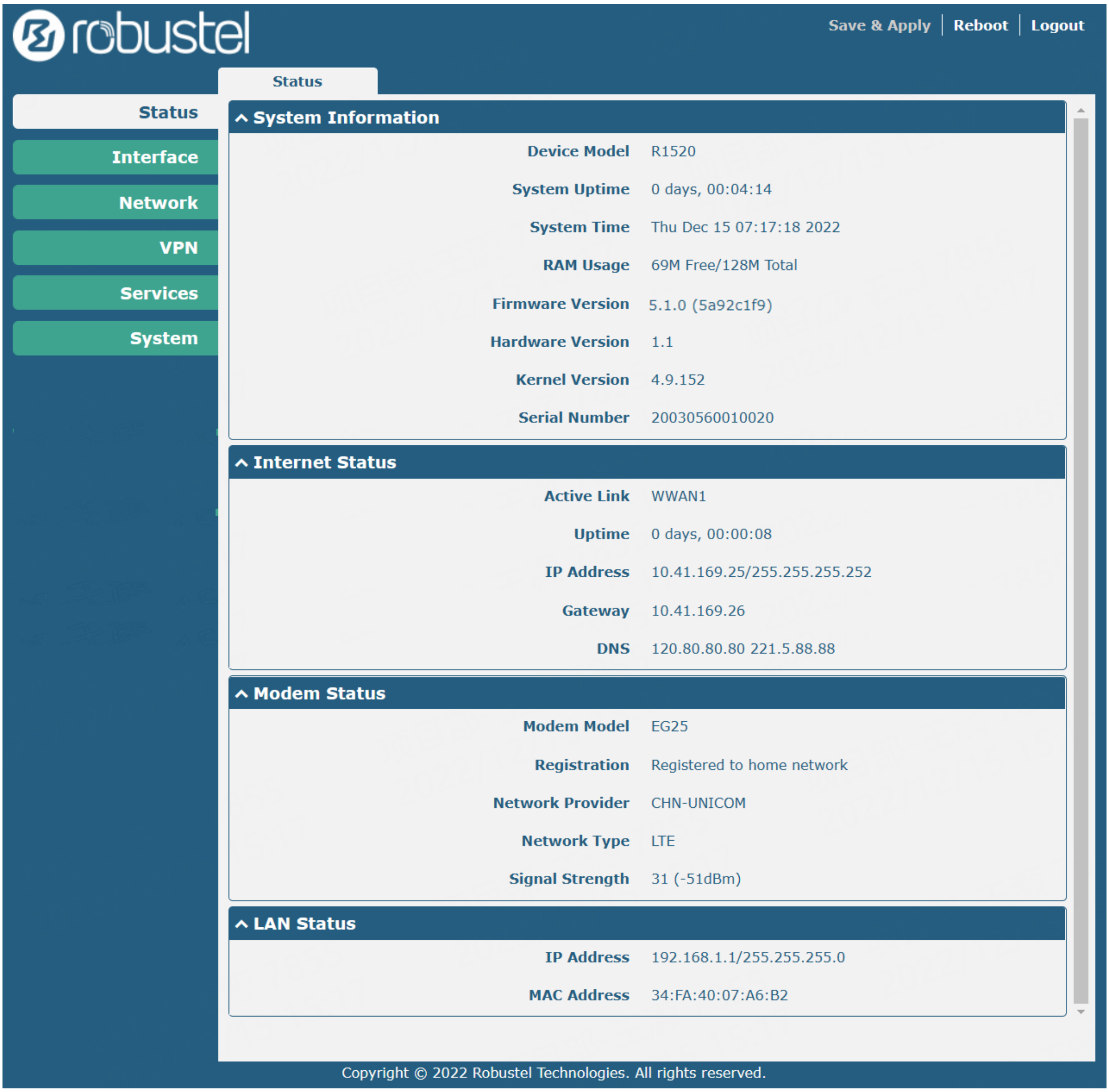
3. On the login page, enter the username and password, choose language and then click **LOGIN**. Please check the information on the product label for the default username and password.
   Note: *If enter the wrong username or password over 6 times, the login web will be locked for 5 minutes.*

   admin
   •••••

2.5 Control Panel

After logging in, the home page of the web interface is displayed. Here take R1520 for example.



^ System Information

Device Model	R1520
System Uptime	0 days, 00:04:14
System Time	Thu Dec 15 07:17:18 2022
RAM Usage	69M Free/128M Total
Firmware Version	5.1.0 (5a92c1f9)
Hardware Version	1.1
Kernel Version	4.9.152
Serial Number	20030560010020

^ Internet Status

Active Link	WWAN1
Uptime	0 days, 00:00:08
IP Address	10.41.169.25/255.255.255.252
Gateway	10.41.169.26
DNS	120.80.80.80 221.5.88.88

^ Modem Status

Modem Model	EG25
Registration	Registered to home network
Network Provider	CHN-UNICOM
Network Type	LTE
Signal Strength	31 (-51dBm)

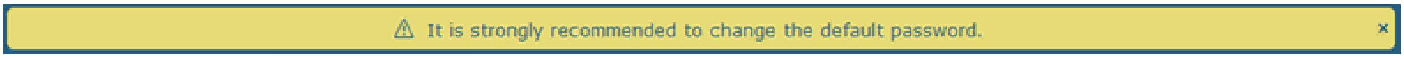
^ LAN Status

IP Address	192.168.1.1/255.255.255.0
MAC Address	34:FA:40:07:A6:B2

Copyright © 2022 Robustel Technologies. All rights reserved.

On the homepage, users can perform operations such as saving the configuration, restarting the device, and logging out.

Using the default username and password to log in to the device, the page will pop up in the following tab



⚠ It is strongly recommended to change the default password. ×

It is strongly recommended for security purposes that you change the default username and/or password. Click the × button to close the notification. To change your username and/or password, see **3.6.6 System > User**

Management.

Control Panel		
Item	**Description**	**Button**
Save & Apply	Click to save the current configuration into the device's flash and apply the modification on every configuration page, to modify taking effect.	Save & Apply
Reboot	Click to reboot the device. If the Reboot button is yellow, it means that some completed configurations will take effect only after the reboot.	Reboot
Logout	Click to log the current user out safely. After logging out, it will switch to the login page. Shut down the web page directly without logout, the next one can log in web on this browser without a password before timeout.	Logout
Submit	Click to save the modification on the current configuration page.	Submit
Cancel	Click to cancel the modification on the current configuration page.	Cancel

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

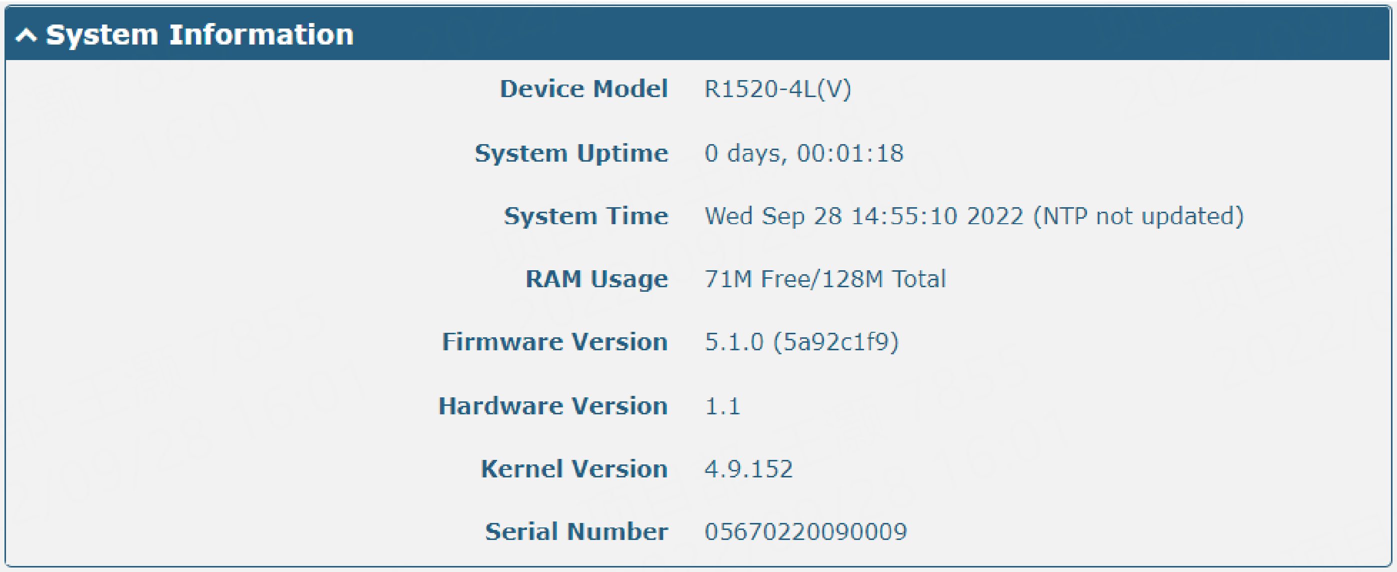
1. Modify in one page;
2. Click Submit under this page;
3. Modify on another page;
4. Click Submit under this page;
5. Complete all modifications;
6. Click Save & Apply.

3. WebUI Descriptions

3.1 Status

3.1.1 System Information

This page allows you to view the System Information, Internet Status, and LAN Status of your device.



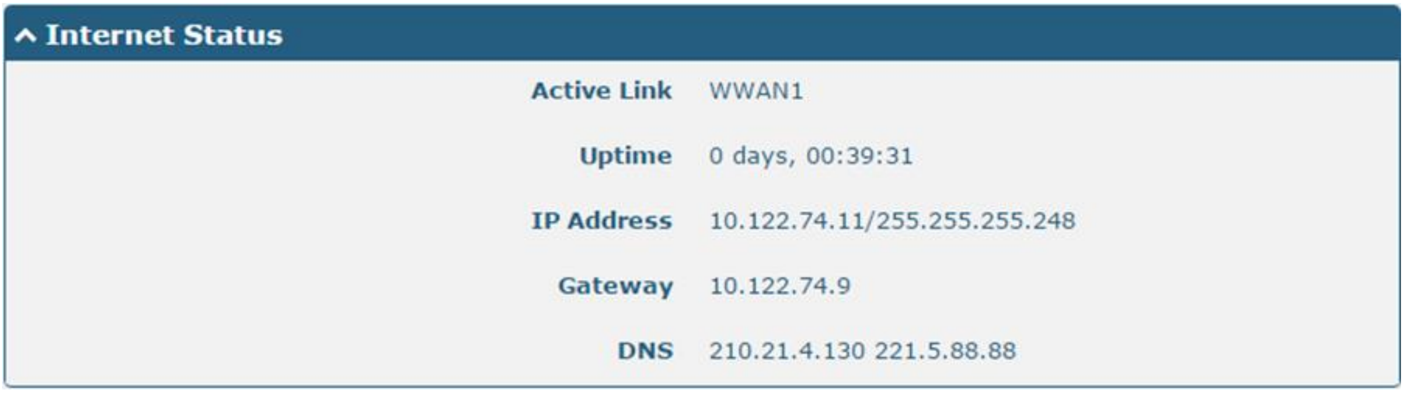
System Information

Device Model	R1520-4L(V)
System Uptime	0 days, 00:01:18
System Time	Wed Sep 28 14:55:10 2022 (NTP not updated)
RAM Usage	71M Free/128M Total
Firmware Version	5.1.0 (5a92c1f9)
Hardware Version	1.1
Kernel Version	4.9.152
Serial Number	05670220090009

System Information	
Item	**Description**
Device Model	Show model name of your device.
System Uptime	Show device uptime.
System Time	Show current system time.
RAM Usage	Show free memory and the total memory.
Firmware Version	Show firmware version running on the device.
Hardware Version	Show current hardware version.
Kernel Version	Show current kernel version.
Serial Number	Show Serial Number of the device.

3.1.2 Internet Status

This page shows the device's Internet status information.



^ Internet Status

Active Link WWAN1

Uptime 0 days, 00:39:31

IP Address 10.122.74.11/255.255.255.248

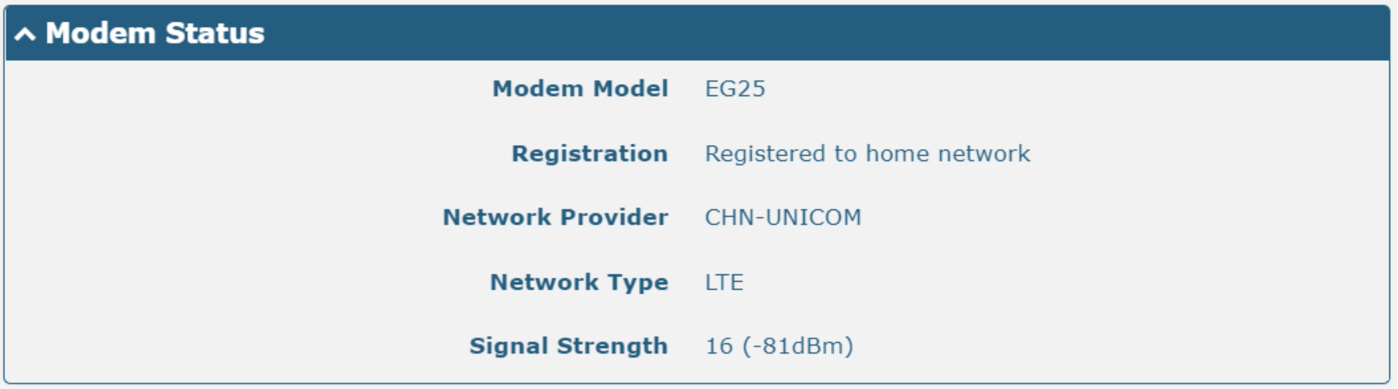
Gateway 10.122.74.9

DNS 210.21.4.130 221.5.88.88

Internet Status	
Item	**Description**
Active Link	Show currently used link: WWAN1, WWAN2, or WAN.
Uptime	Show current amount of time the link has been connected.
IP Address	Show IP address of active link.
Gateway	Show gateway address of active link.
DNS	Show current DNS server address.

3.1.3 Modem Status

This page shows the device's Modem information.



^ Modem Status

Modem Model EG25

Registration Registered to home network

Network Provider CHN-UNICOM

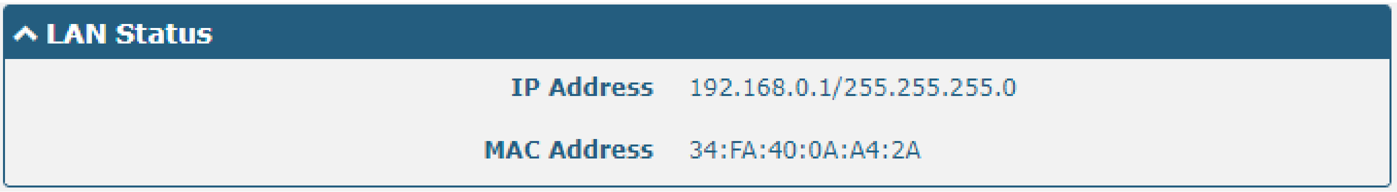
Network Type LTE

Signal Strength 16 (-81dBm)

Modem Status	
Item	**Description**
Modem Model	Show model of cellular module.
Registration	Show current network status.
Network Provider	Show name of network provider.
Network Type	Show current network service type.
Signal Strength	Show the values of signal strength.

3.1.4 LAN Status

This page shows the devices' LAN status



^ LAN Status

IP Address 192.168.0.1/255.255.255.0

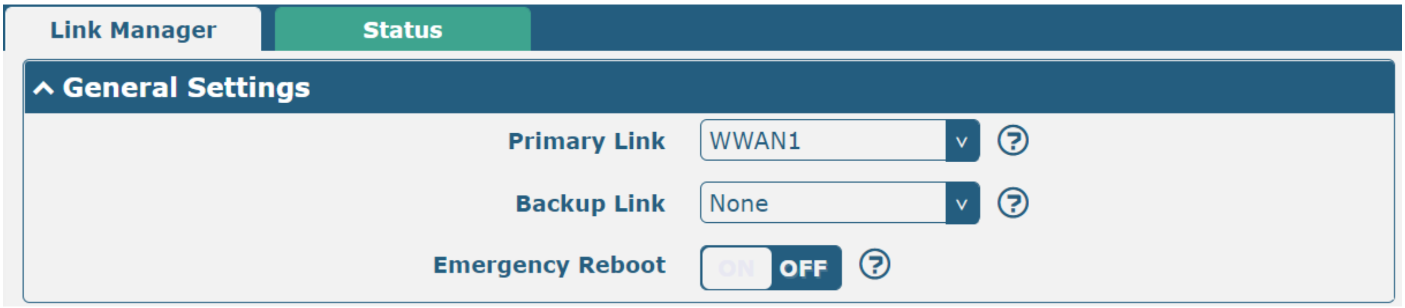
MAC Address 34:FA:40:0A:A4:2A

LAN Status	
Item	**Description**
IP Address	Show IP address and the netmask of the LAN.
MAC Address	Show MAC address of the LAN.

3.2 Interface

3.2.1 Link Manager

This page allows you to manage link connections. The Link management function supports the selection of single/dual links. At the same time, each link supports the configuration of the link detection function to keep the network connection always online.



^ General Settings

Primary Link WWAN1

Backup Link None

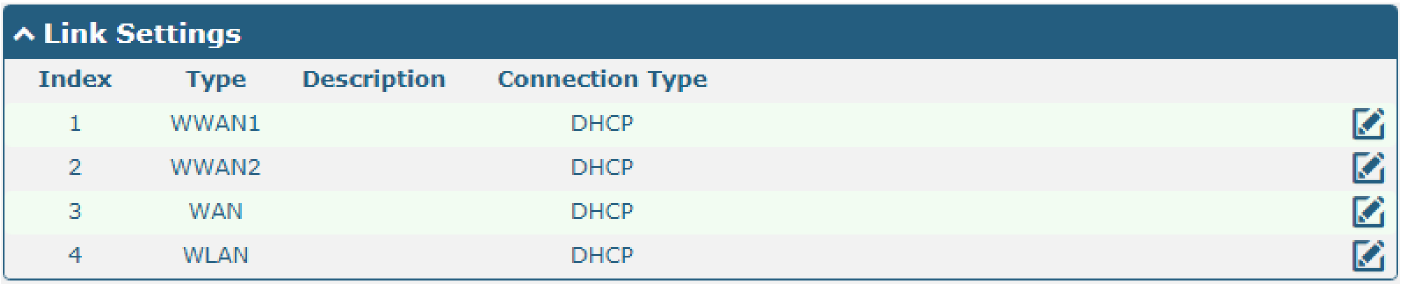
Emergency Reboot ON OFF

General Settings @ Link Manager		
Item	**Description**	**Default**
Primary Link	Select from “WWAN1”, “WWAN2”, “WAN” or “WLAN”. • WWAN1: Select SIM1 as the primary wireless link. • WWAN2: Select SIM2 as the primary wireless link. • WAN: Select WAN Ethernet port as the primary wired link. • WLAN: Select WLAN as the primary wireless link. ***Note:*** *WLAN link is available only if enable Wi-Fi as Client mode, please refer to **3.2.5 Wi-Fi**.*	WWAN1

General Settings @ Link Manager		
Item	**Description**	**Default**
Backup Link	Select from "WWAN1", "WWAN2", "WAN", "WLAN", or "None". • WWAN1: Select SIM1 as the backup wireless link. • WWAN2: Select SIM2 as the backup wireless link. • WAN: Select WAN Ethernet port as the backup wired link. • WLAN: Select WLAN as the backup wireless link. ***Note:*** *WLAN link is available only if enable Wi-Fi as Client mode, please refer to* ***3.2.5 Wi-Fi****.* • None: No backup link.	None
Backup Mode	Select from "Cold Backup", "Warm Backup", or "Load Balancing". • Cold Backup: The inactive link is offline on standby. • Warm Backup: The inactive link is online on standby. • Load Balancing: Use two links simultaneously. ***Note: Backup Mode*** *is available only Backup Link isn't None.*	Cold Backup
Revert Interval	Specify number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking. ***Note:*** *Revert interval is available only under the cold backup mode.*	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links are available.	OFF

Note: *Click ? for help.*

Link Settings allows you to set the parameters of link connection, including WWAN1/WWAN2, WAN, and WLAN. It is recommended to enable Ping detection to keep the device always online. The Ping detection increases reliability and also saves data traffic.

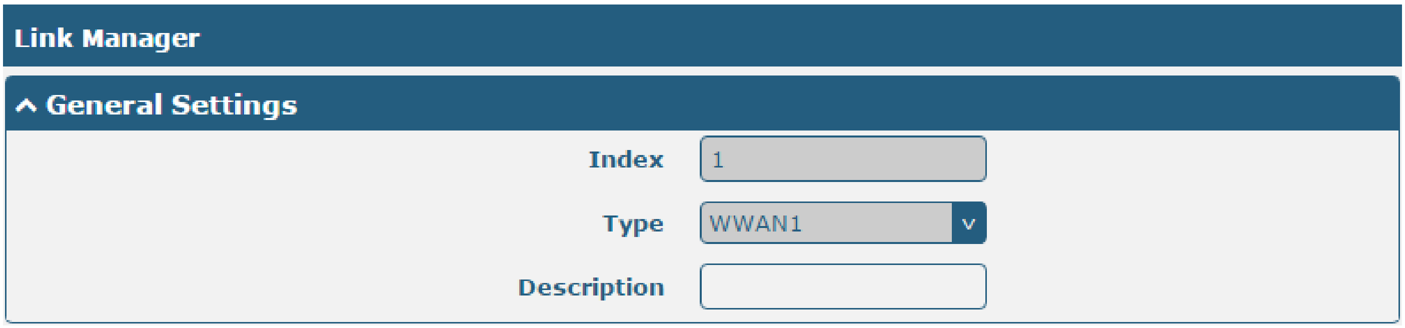


Link Settings

Index	Type	Description	Connection Type
1	WWAN1		DHCP
2	WWAN2		DHCP
3	WAN		DHCP
4	WLAN		DHCP

Click on the right-most of WWAN1/WWAN2 to enter the configuration window.

WWAN1/WWAN2

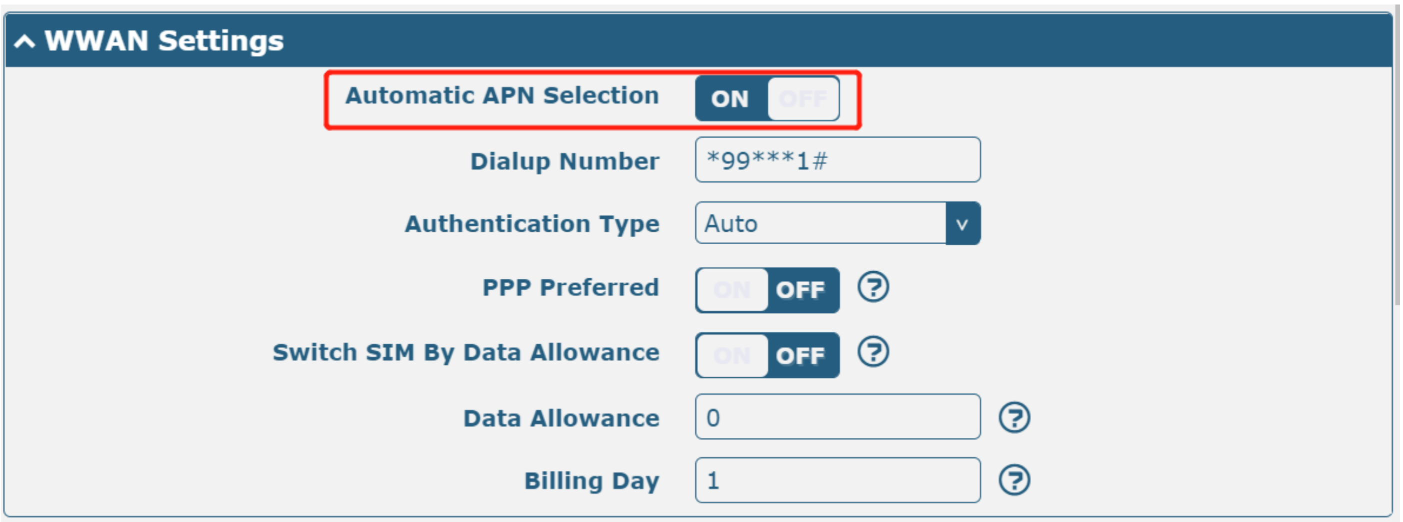


Link Manager

General Settings

Index	1
Type	WWAN1
Description	

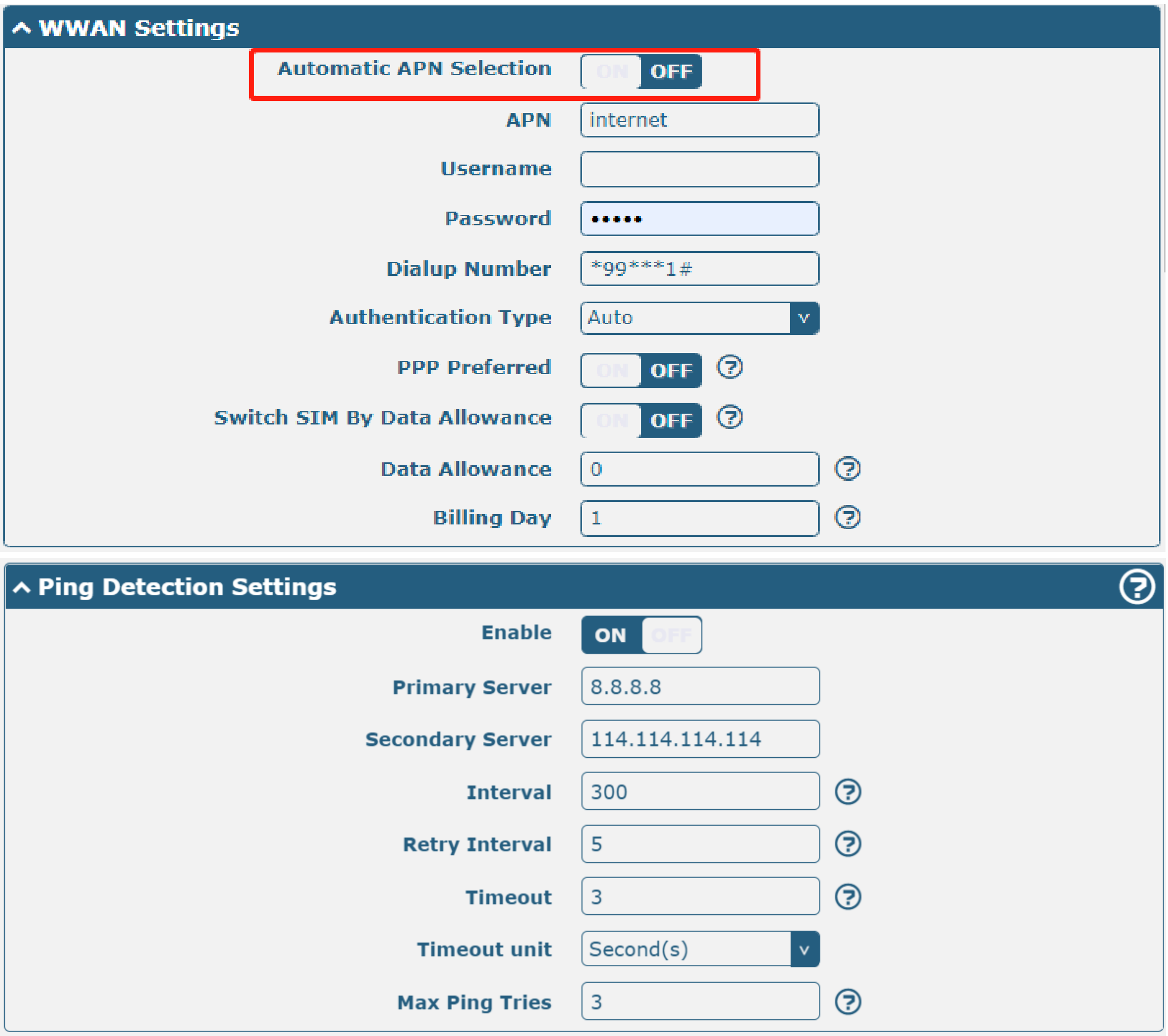
The window is displayed below when enabling the “Automatic APN Selection” option.



WWAN Settings

Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
PPP Preferred	OFF
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

The window is displayed below when disabling the “Automatic APN Selection” option.

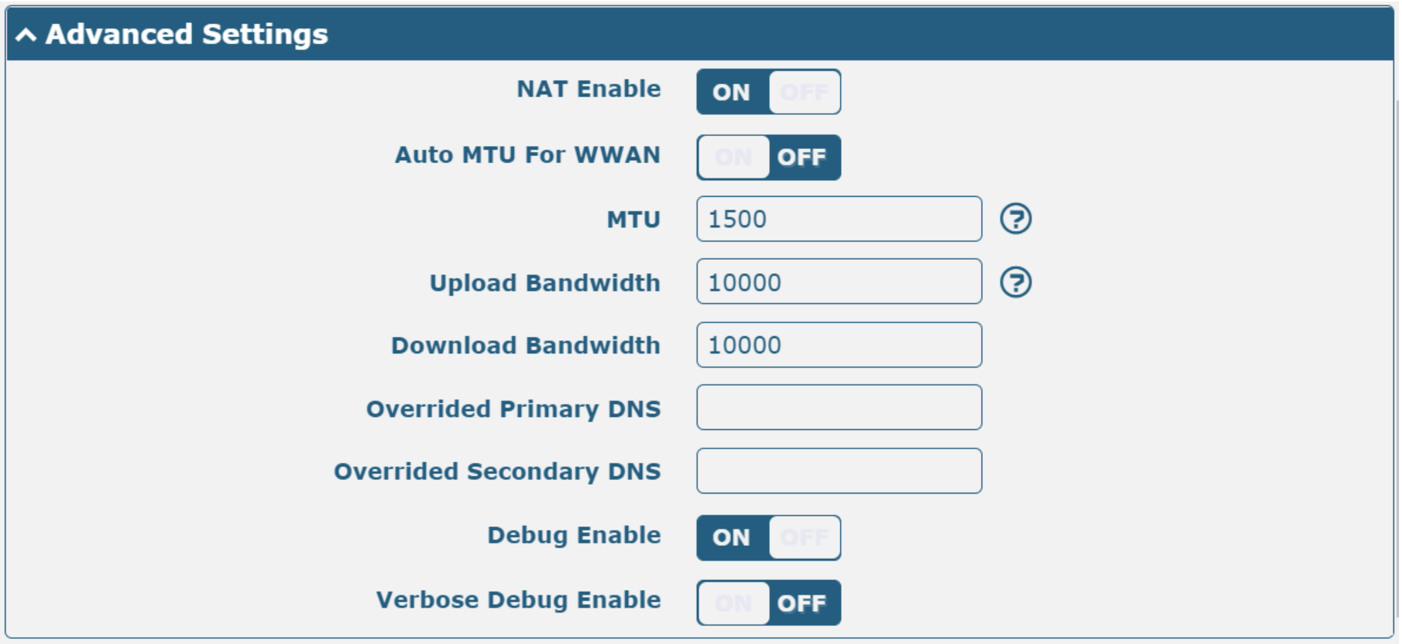


WWAN Settings

Automatic APN Selection	OFF
APN	internet
Username	
Password	•••••
Dialup Number	*99***1#
Authentication Type	Auto
PPP Preferred	OFF
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

Ping Detection Settings

Enable	ON
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Timeout unit	Second(s)
Max Ping Tries	3



^ Advanced Settings

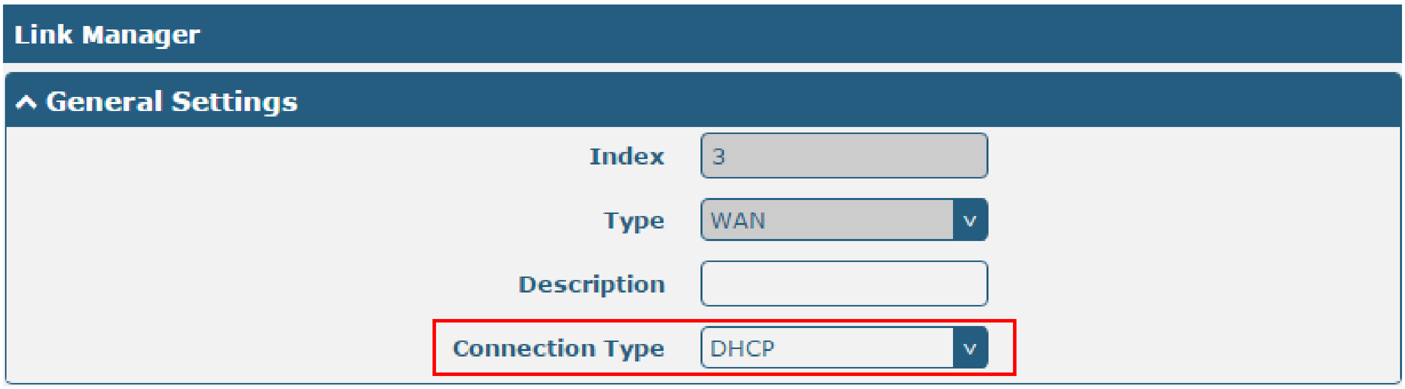
NAT Enable	ON
Auto MTU For WWAN	OFF
MTU	1500
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Debug Enable	ON
Verbose Debug Enable	OFF

Link Settings (WWAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate ordinal of the list.	--
Type	Show type of the link.	WWAN1
Description	Enter a description for this link.	Null
WWAN Settings		
Automatic APN Selection	Click the toggle button to enable/disable the “Automatic APN Selection” option. After enabling, the device will recognize the APN (Access Point Name) automatically. Alternatively, you can disable this option and manually add the APN (Access Point Name).	ON
APN	Enter APN (Access Point Name) for cellular dial-up connection, provided by the local ISP.	Internet
Username	Enter username for cellular dial-up connection, provided by the local ISP.	Null
Password	Enter password for cellular dial-up connection, provided by the local ISP.	Null
Dialup Number	Enter dial-up number for the cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from “Auto”, “PAP” or “CHAP” as the local ISP required.	Auto
PPP Preferred	The PPP dial-up method is preferred.	OFF
Switch SIM By Data Allowance	Click the toggle button to enable/disable this option. After enabling, it will switch to another SIM when the data limit is reached. ***Note****: Only used for dual-SIM backup.*	OFF
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in **Interface > Link Manager > Status > WWAN Data Usage Statistics**. 0 means disable data traffic record.	0
Billing Day	Specify monthly billing day. The data traffic statistics will be recalculated from that day.	1

Link Settings (WWAN)		
Item	**Description**	**Default**
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the device.	ON
Primary Server	The device will ping this primary address/domain name to check if the current IPv4 connectivity is active.	8.8.8.8
Secondary Server	The device will ping this secondary address/domain name to check if the current IPv4 connectivity is active.	114.114.114.114
Interval	Set ping interval.	300
Retry Interval	Set ping retry interval. When ping failed, the device will ping again every retry interval.	5
Timeout	Set ping timeout.	3
Timeout Unit	Set ping timeout unit. Second(s) or Millisecond(ms).	Second
Max Ping Tries	Set max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable Network Address Translation.	ON
Auto MTU For WWAN	Click the toggle button to enable/disable Auto MTU feature for WWAN.	ON
MTU	Set the Maximum Transmission Unit. ***Note:*** *MTU is available only "Auto MTU For WWAN" is OFF.*	1500
Upload Bandwidth	Set upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Set download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Define primary IPv4 DNS server address used by the link.	Null
Specify Secondary DNS	Define secondary IPv4 DNS server address used by the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose debugging information output.	OFF

WAN

The device will obtain IP automatically from DHCP server when apply "DHCP".



Link Manager

General Settings

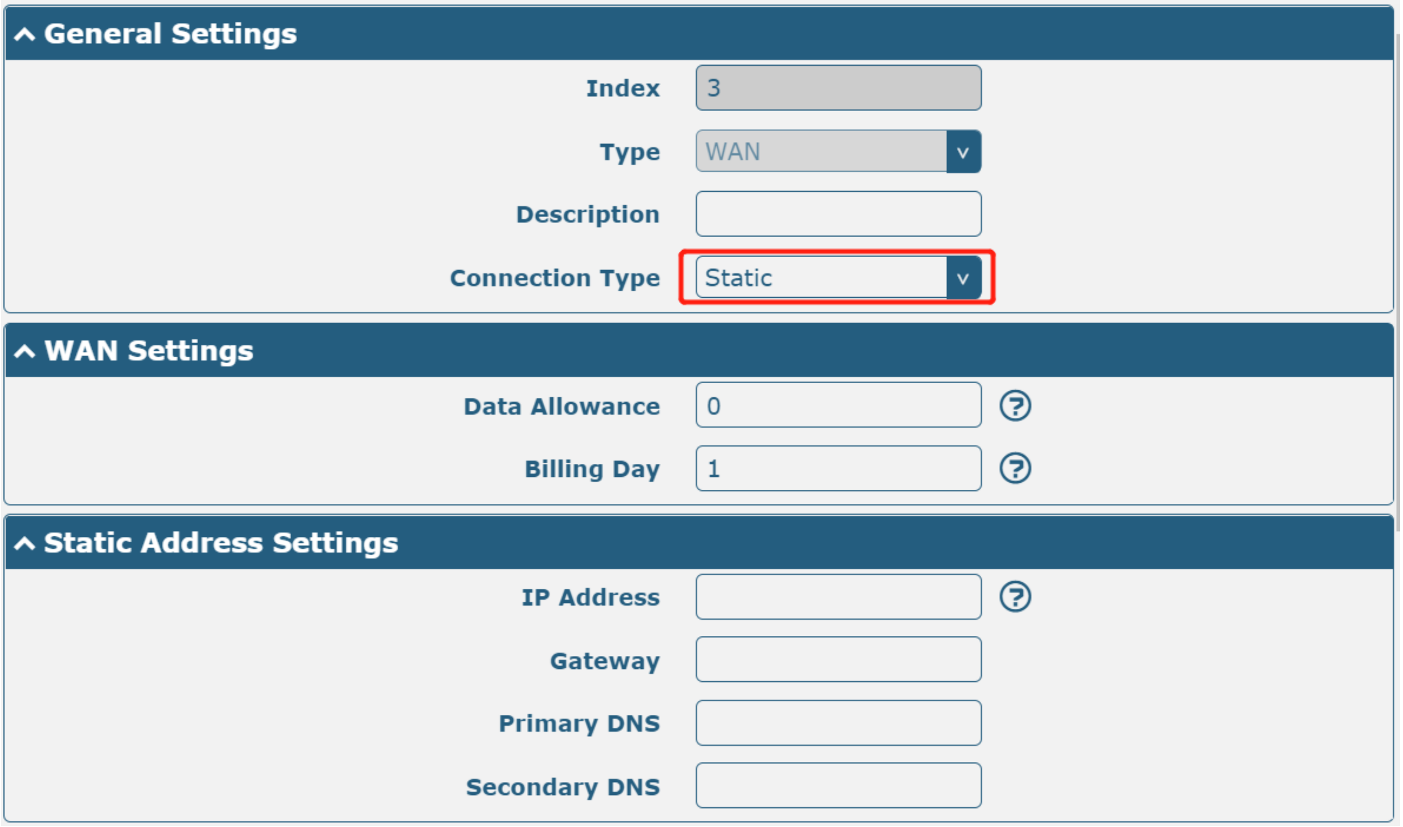
Index: 3

Type: WAN

Description:

Connection Type: DHCP

The window is displayed below when choosing "Static" as connection type.



General Settings

Index	3
Type	WAN
Description	
Connection Type	Static

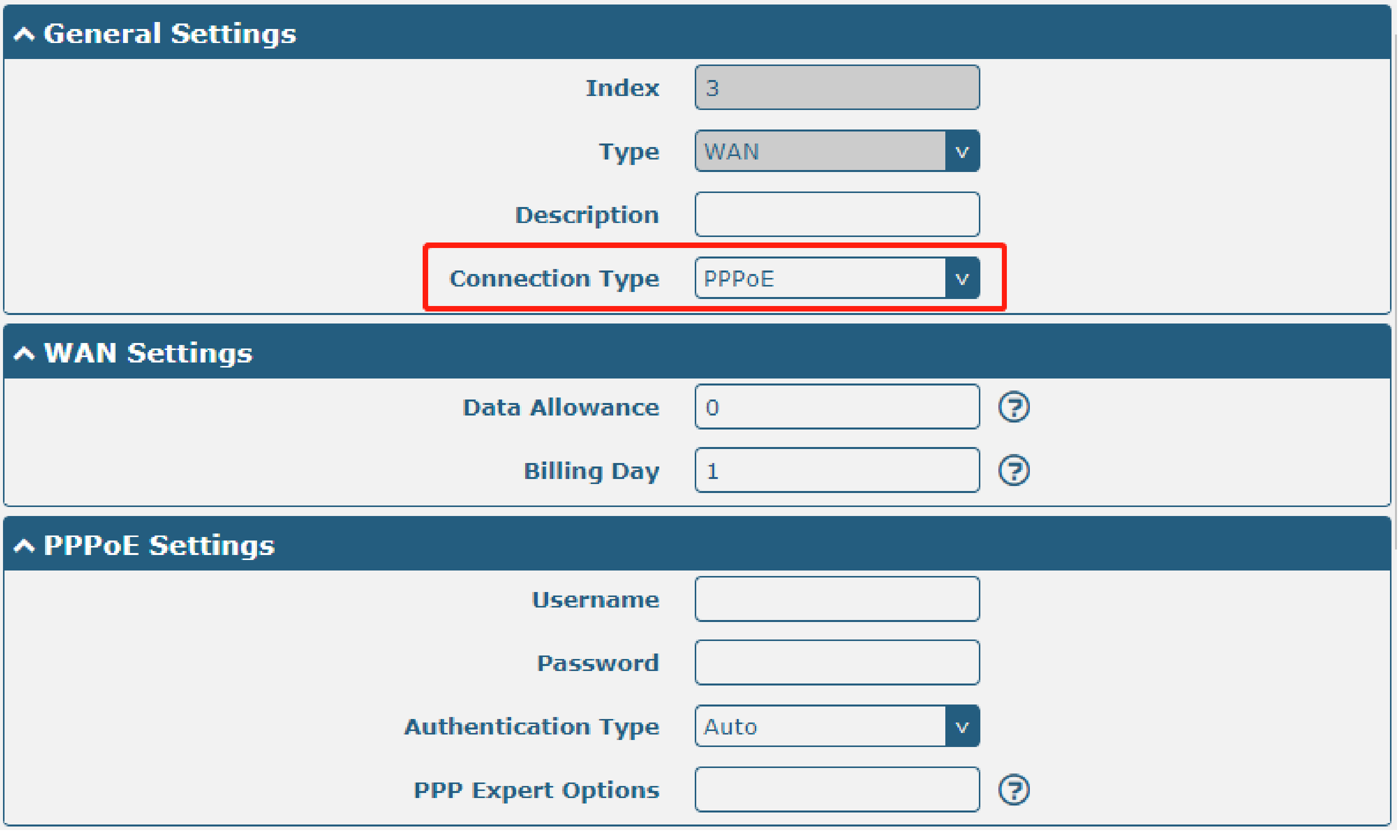
WAN Settings

Data Allowance	0
Billing Day	1

Static Address Settings

IP Address	
Gateway	
Primary DNS	
Secondary DNS	

The window is displayed below when choosing "PPPoE" as connection type.



General Settings

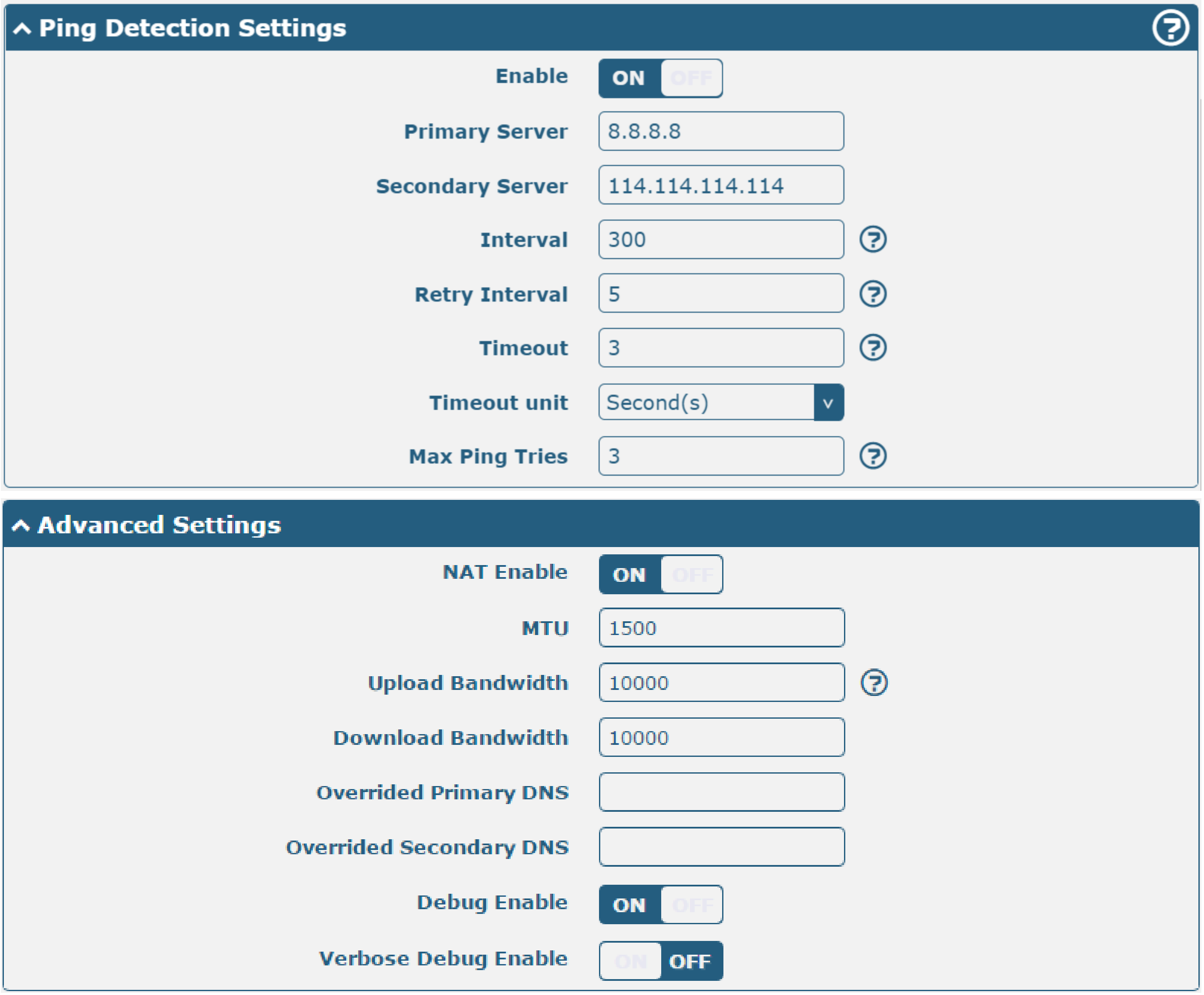
Index	3
Type	WAN
Description	
Connection Type	PPPoE

WAN Settings

Data Allowance	0
Billing Day	1

PPPoE Settings

Username	
Password	
Authentication Type	Auto
PPP Expert Options	



Enable: ON OFF

Primary Server: 8.8.8.8

Secondary Server: 114.114.114.114

Interval: 300

Retry Interval: 5

Timeout: 3

Timeout unit: Second(s)

Max Ping Tries: 3

NAT Enable: ON OFF

MTU: 1500

Upload Bandwidth: 10000

Download Bandwidth: 10000

Overrided Primary DNS:

Overrided Secondary DNS:

Debug Enable: ON OFF

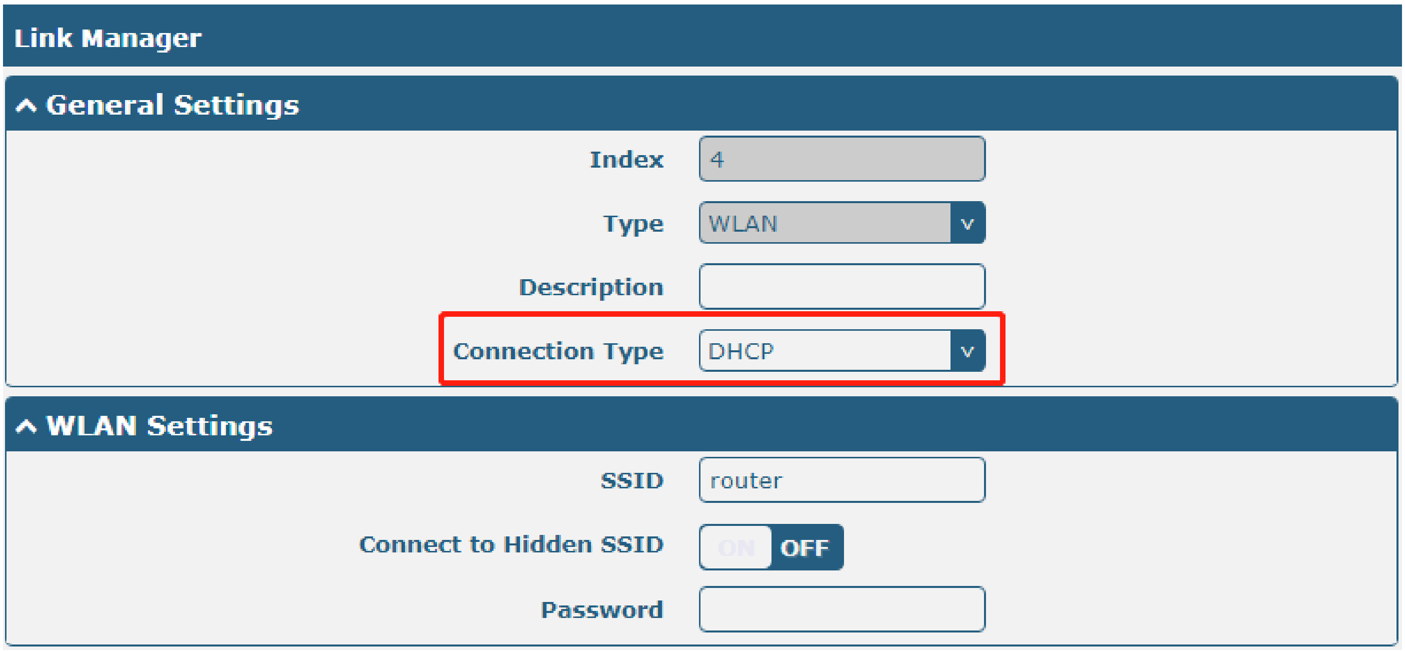
Verbose Debug Enable: ON OFF

Link Settings (WAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate ordinal of the list.	--
Type	Show type of the link.	WAN
Description	Enter a description for this link.	Null
Connection Type	Select from "DHCP", "Static" or "PPPoE".	DHCP
Static Address Settings		
IP Address	Set IP address with Netmask which can access the Internet. IP address with Netmask, e.g., 192.168.1.1/24	Null
Gateway	Set gateway address of the WAN port.	Null
Primary DNS	Set primary DNS address.	Null
Secondary DNS	Set secondary DNS address.	Null
PPPoE Settings		
Username	Enter username provided by your Internet Service Provider.	Null
Password	Enter password provided by your Internet Service Provider.	Null

Authentication Type	Select from "Auto", "PAP" or "CHAP" as the local ISP required.	Auto
PPP Expert Options	Enter PPP Expert options used for PPPoE dialup. You can enter some other PPP dial strings in this field. Each string can be separated by a semicolon.	Null
WAN Settings		
Data Allowance	Set monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MB) is specified. The traffic record will be displayed in **Interface > Link Manager > Status > WAN Data Usage Statistics**. 0 means disable data traffic record.	0
Billing Day	Specify monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the device.	ON
Primary Server	The device will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8
Secondary Server	The device will ping this secondary address/domain name to check if the current connectivity is active.	114.114.114.114
Interval	Set ping interval.	300
Retry Interval	Set ping retry interval. When ping failed, the device will ping again every retry interval.	5
Timeout	Set ping timeout.	3
Timeout Unit	Set ping timeout unit. Second(s) or Millisecond(ms)	Second
Max Ping Tries	Set max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter Maximum Transmission Unit.	1500
Upload Bandwidth	Enter upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Define primary IPv4 DNS server address used by the link.	Null
Specify Secondary DNS	Define secondary IPv4 DNS server address for the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose debugging information output.	OFF

WLAN

The device will obtain IP address automatically from the WLAN AP when applied "DHCP" as the connection type. The specific parameter configuration of SSID is shown below.



Link Manager

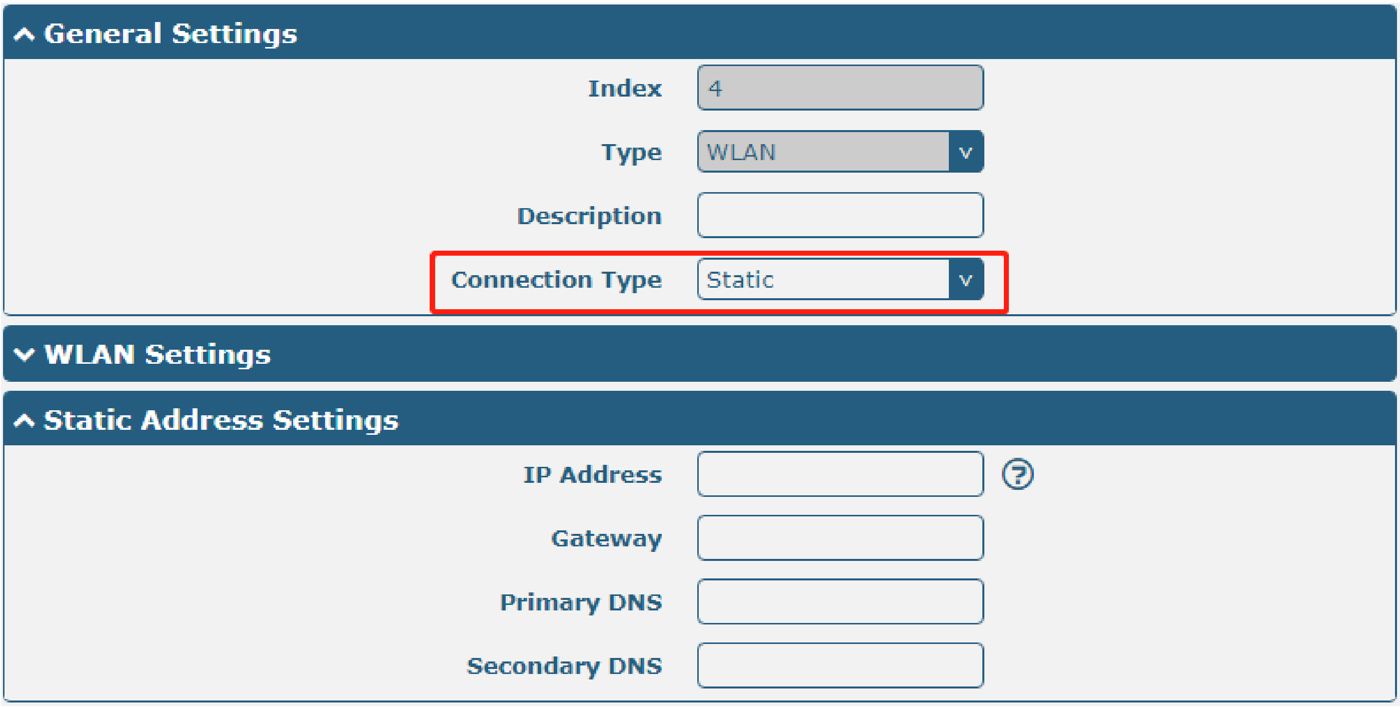
^ General Settings

Index	4
Type	WLAN
Description	
Connection Type	DHCP

^ WLAN Settings

SSID	router
Connect to Hidden SSID	ON OFF
Password	

The window is displayed below when choosing "Static" as connection type.



^ General Settings

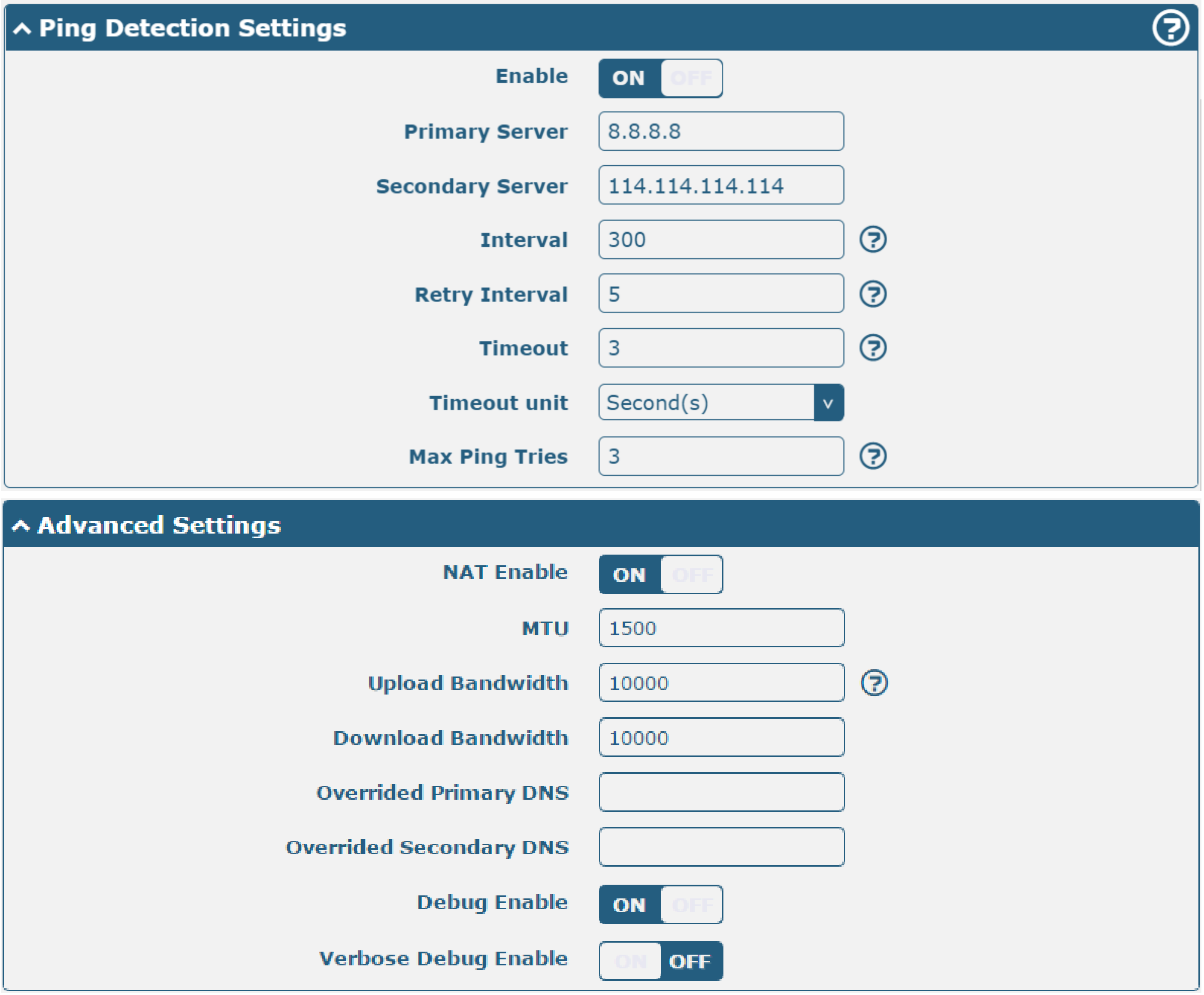
Index	4
Type	WLAN
Description	
Connection Type	Static

v WLAN Settings

^ Static Address Settings

IP Address	
Gateway	
Primary DNS	
Secondary DNS	

Note: WLAN connection type not support ”PPPoE”.



^ Ping Detection Settings

Enable: ON

Primary Server: 8.8.8.8

Secondary Server: 114.114.114.114

Interval: 300

Retry Interval: 5

Timeout: 3

Timeout unit: Second(s)

Max Ping Tries: 3

^ Advanced Settings

NAT Enable: ON

MTU: 1500

Upload Bandwidth: 10000

Download Bandwidth: 10000

Overrided Primary DNS:

Overrided Secondary DNS:

Debug Enable: ON

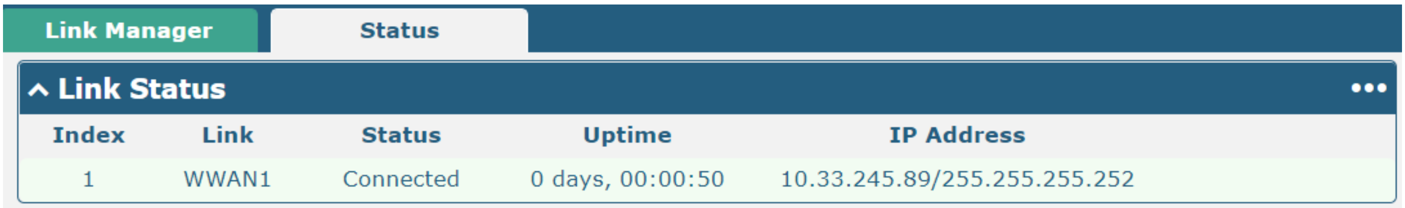
Verbose Debug Enable: OFF

Link Settings (WLAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate ordinal of list.	--
Type	Show type of the link.	WLAN
Description	Enter a description for this link.	Null
Connection Type	Select from “DHCP” or “Static”.	DHCP
WLAN Settings		
SSID	Enter 1-32 characters SSID that your device wants to connect. SSID (Service Set Identifier) is the name of your wireless network.	device
Connect to Hidden SSID	Click the toggle button to enable/disable this option. When the device works in Client mode and needs to connect to any access point which has a hidden SSID, you need to enable this option.	OFF
Password	Enter 8-63 characters password of the access point to which your device wants to connect.	Null
Static Address Settings		

IP Address	Enter IP address with Netmask which can access the Internet, e.g., 192.168.1.1/24.	Null
Gateway	Enter IP address of the Wi-Fi AP.	Null
Primary DNS	Set primary DNS address.	Null
Secondary DNS	Set secondary DNS address.	Null
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the device.	ON
Primary Server	The device will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8
Secondary Server	The device will ping this secondary address/domain name to check if the current connectivity is active.	114.114.114.114
Interval	Set ping interval.	300
Retry Interval	Set ping retry interval. When ping failed, the device will ping again every retry interval.	5
Timeout	Set ping timeout.	3
Timeout Unit	Set ping timeout unit. Second(s) or Millisecond(ms)	Second
Max Ping Tries	Set max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advance Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter Maximum Transmission Unit.	1500
Upload Bandwidth	Enter upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Define a primary DNS server address used by the link.	Null
Specify Secondary DNS	Define a secondary DNS server address for the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose debugging information output.	OFF

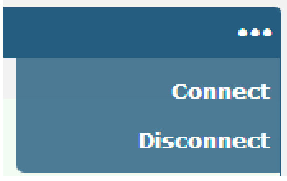
Status

This page allows you to view the status of link connection and clear the monthly data usage statistics.

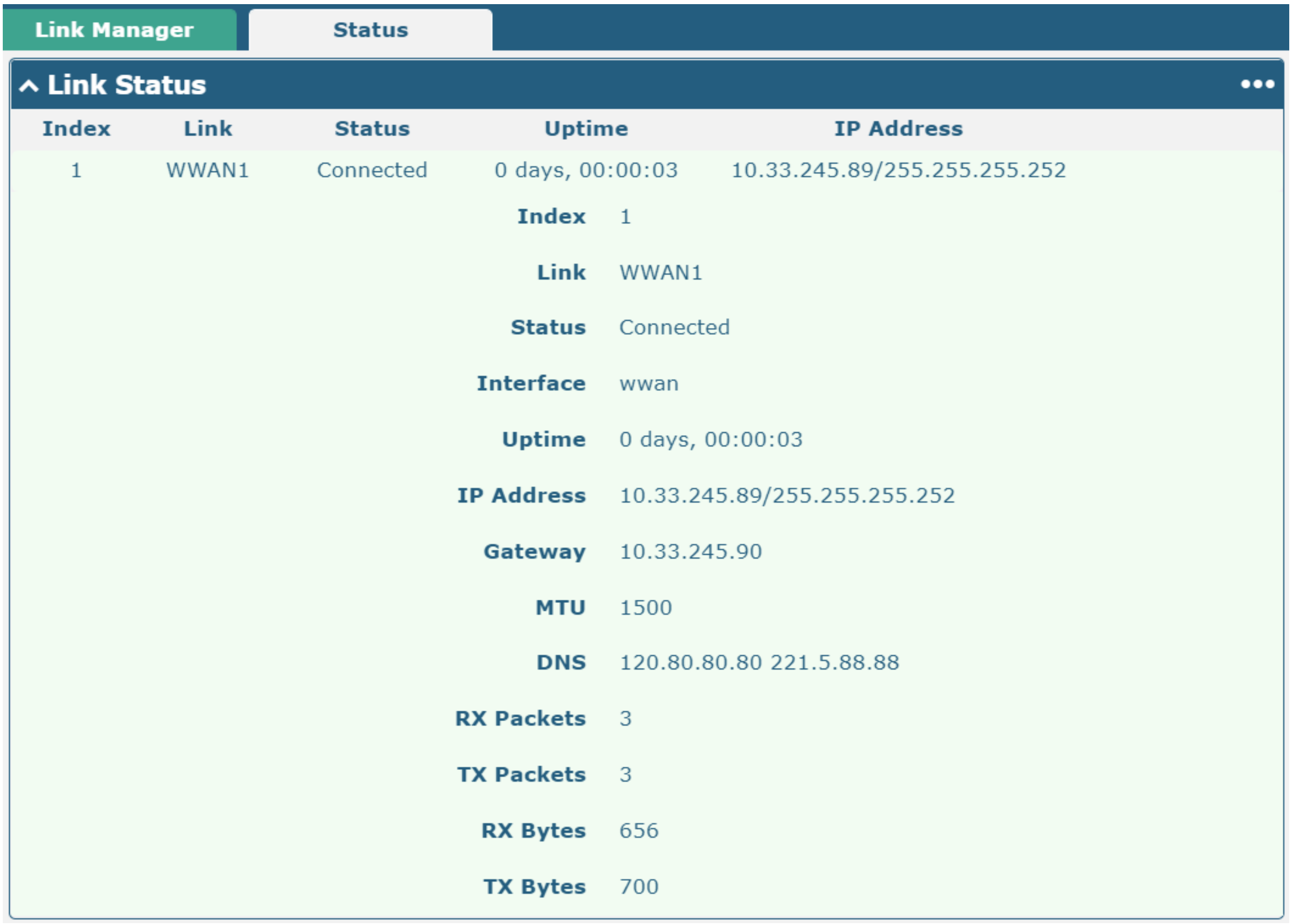


Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:00:50	10.33.245.89/255.255.255.252

Click the right-most button ••• to select the connection status of the current link.

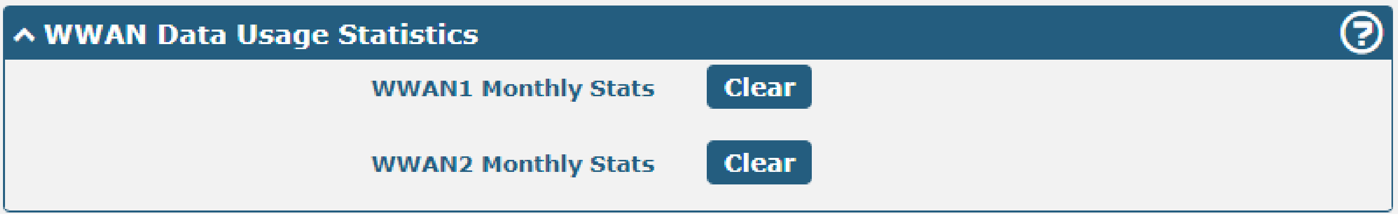


Click the row of the link, and it will show the details information of the current link connection under the row.



Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:00:03	10.33.245.89/255.255.255.252

Index	1
Link	WWAN1
Status	Connected
Interface	wwan
Uptime	0 days, 00:00:03
IP Address	10.33.245.89/255.255.255.252
Gateway	10.33.245.90
MTU	1500
DNS	120.80.80.80 221.5.88.88
RX Packets	3
TX Packets	3
RX Bytes	656
TX Bytes	700

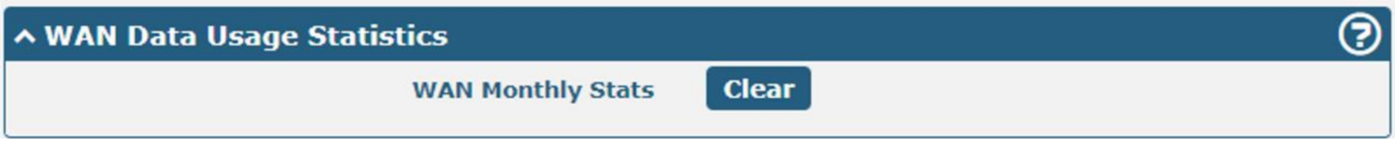


WWAN Data Usage Statistics

WWAN1 Monthly Stats Clear

WWAN2 Monthly Stats Clear

Click Clear button to clean SIM1 or SIM2 monthly data usage statistics. Data statistics will be displayed only if enable the Data Allowance function in **Interface > Link Manager > Link Settings > WWAN Settings > Data Allowance**.



WAN Data Usage Statistics

WAN Monthly Stats Clear

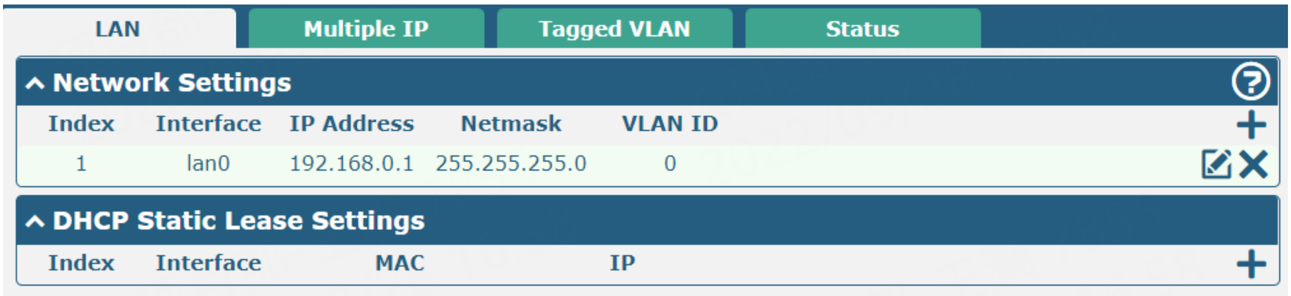
Click the Clear button to clear WAN monthly data traffic usage statistics. Data statistics will be displayed only if enable Data Allowance function in **Interface > Link Manager > Link Settings > WAN Settings > Data Allowance**.

3.2.2 LAN

This section allows you to set the related parameters for the LAN port. There may be multiple Ethernet ports in the device, and at least one LAN port must be assigned as lan0 with its or their default IP 192.168.0.1/255.255.255.0.

Note:
1) R3000 Lite has only one Ethernet port which can only be assigned as LAN.
2) R2000 Lite has only one Ethernet port which can only be assigned as LAN.
3) R1510 Lite has only one Ethernet port which can only be assigned as LAN.

LAN



Network Settings

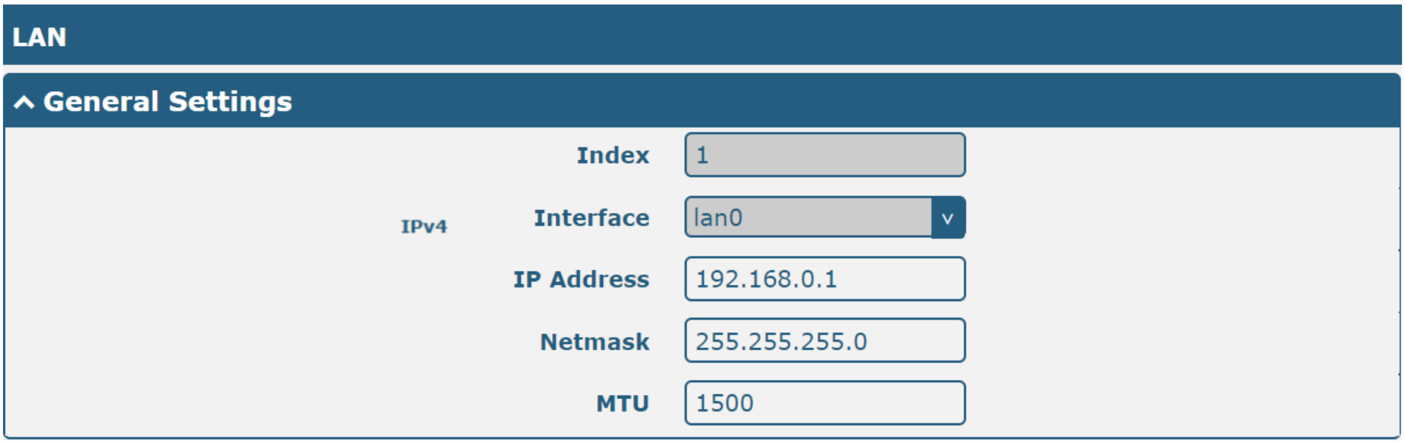
Index	Interface	IP Address	Netmask	VLAN ID
1	lan0	192.168.0.1	255.255.255.0	0

DHCP Static Lease Settings

Index	Interface	MAC	IP

Note: *The lan0 cannot be deleted.*

You may click + to add a new LAN port or click ✕ to delete the current LAN port. Now, click ✎ to edit the configuration of the LAN port.



LAN

General Settings

IPv4

Index: 1

Interface: lan0

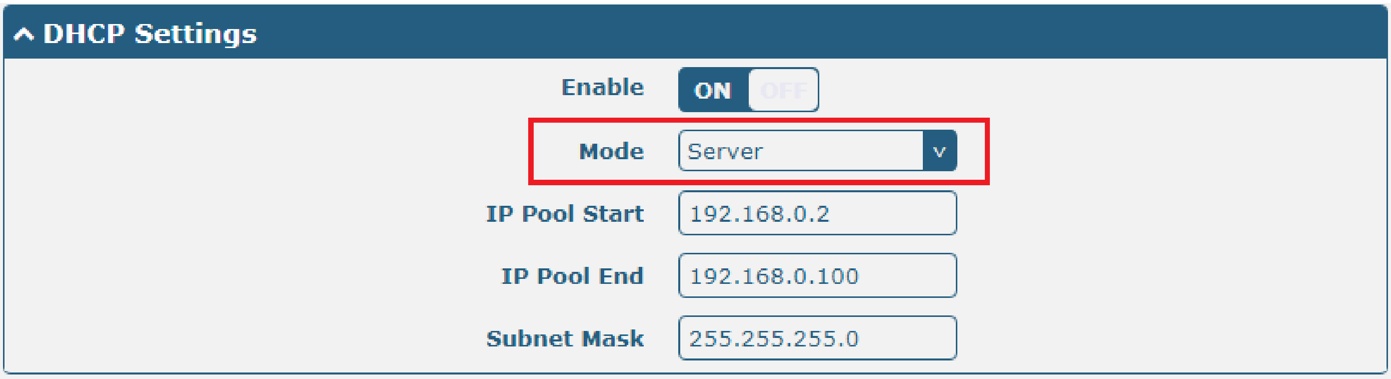
IP Address: 192.168.0.1

Netmask: 255.255.255.0

MTU: 1500

General Settings @ LAN		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Interface	Show editing port. The lan1 is available only if it was selected by one of ETH0~ETHn in **Ethernet > Ports > Port Settings**.	lan0
IPv4 Address	Set IP address of the LAN port.	192.168.0.1
Netmask	Set Netmask of the LAN port.	255.255.255.0
MTU	Enter Maximum Transmission Unit.	1500

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



DHCP Settings

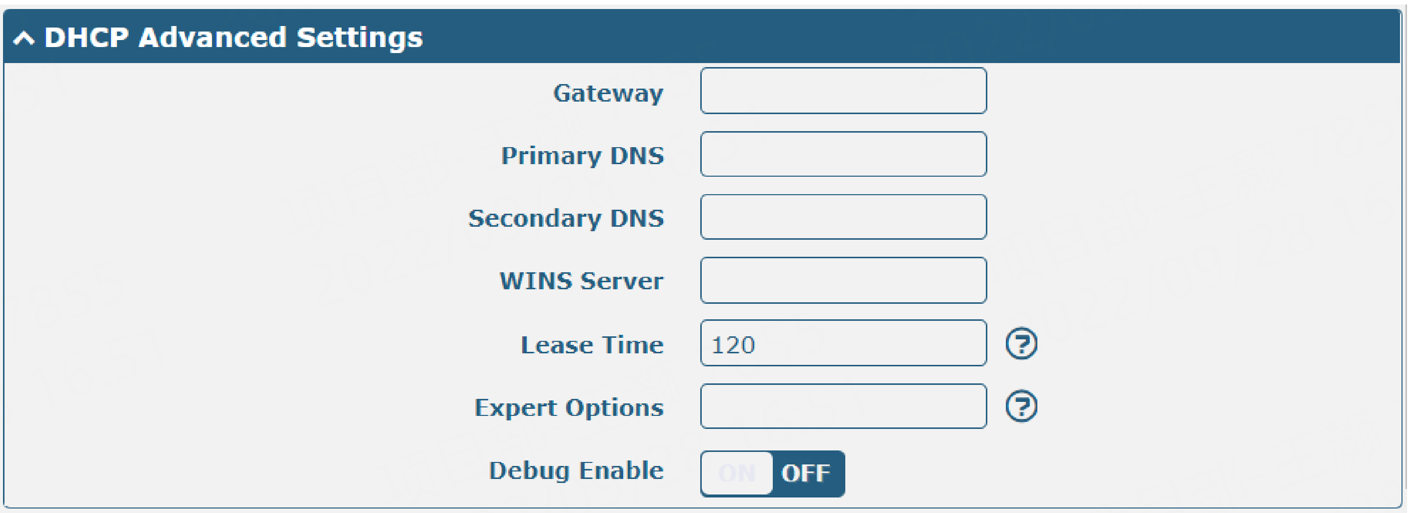
Enable: ON

Mode: Server

IP Pool Start: 192.168.0.2

IP Pool End: 192.168.0.100

Subnet Mask: 255.255.255.0



DHCP Advanced Settings

Gateway:

Primary DNS:

Secondary DNS:

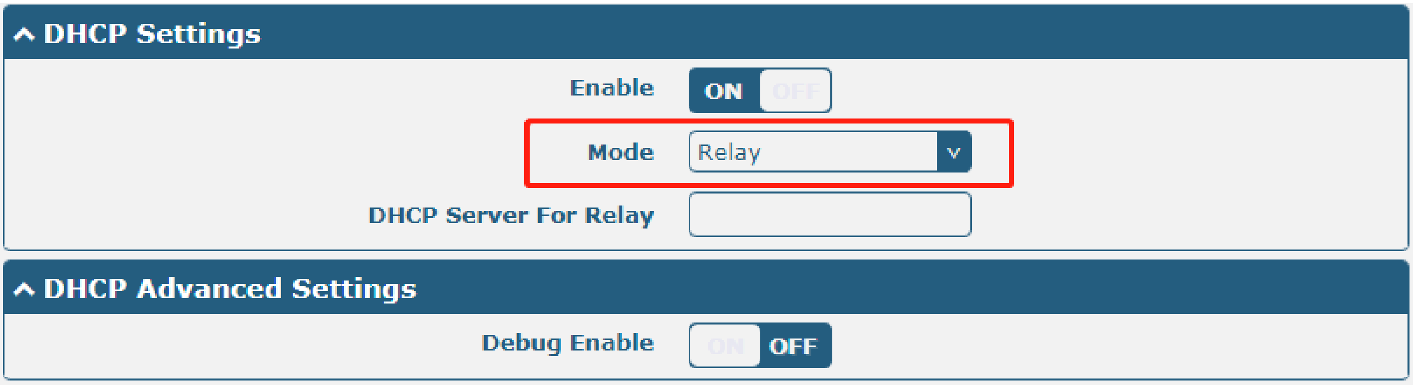
WINS Server:

Lease Time: 120

Expert Options:

Debug Enable: OFF

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

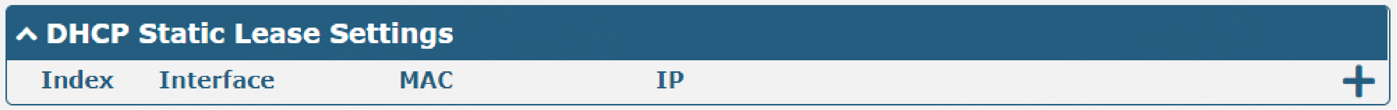


Mode: Relay

DHCP Server For Relay:

Debug Enable: OFF

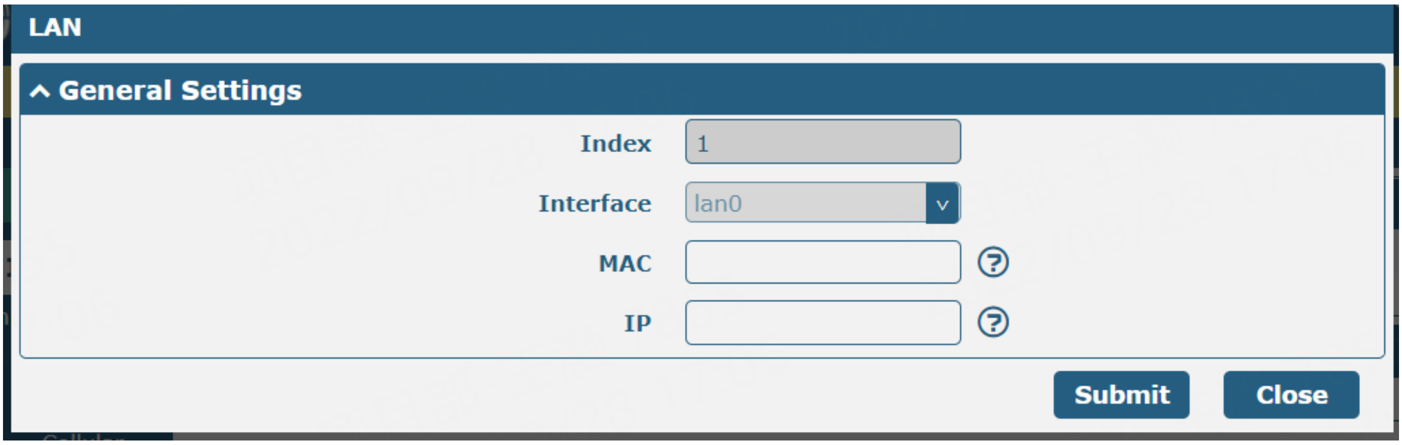
LAN		
Item	**Description**	**Default**
	DHCP Settings	
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select from “Server” or “Relay”. • Server: Lease IP address to DHCP clients which have been connected to LAN port • Relay: The device can be a DHCP Relay, which will provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet	Server
IPv4 Pool Start	Define the beginning of the pool of IP addresses that will be leased to DHCP clients.	192.168.0.2
IPv4 Pool End	Define the end of the pool of IP addresses that will be leased to DHCP clients.	192.168.0.100
Subnet Mask	Define the subnet mask of the IP address obtained by DHCP clients from the DHCP server.	255.255.255.0
DHCP Server for Relay	Enter the IP address of the DHCP relay server.	Null
	DHCP Advanced Settings	
Gateway	Define gateway address assigned by the DHCP server to the clients, which must be on the same network segment as the DHCP address pool.	Null
Primary DNS	Define primary DNS server address assigned by the DHCP server to the clients.	Null
Secondary DNS	Define secondary DNS server address assigned by the DHCP server to the clients.	Null
WINS Server	Define Windows Internet Naming Service obtained by DHCP clients from DHCP sever.	Null
Lease Time	Set lease time in which the client can use the IP address obtained from the DHCP server, measured in seconds.	120
Expert Options	Enter some other options of the DHCP server in this field. format: config-desc;config-desc, e.g. log-DHCP;quiet-DHCP	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable DHCP information output.	OFF



^ DHCP Static Lease Settings

Index	Interface	MAC	IP	+

You can click + to add a new MAC and IP from the pop-up window in DHCP Static Lease Settings.



LAN

^ General Settings

Index: 1

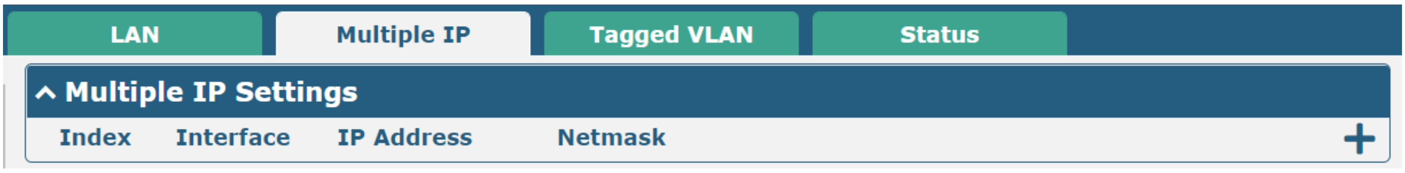
Interface: lan0

MAC:

IP:

LAN		
Item	**Description**	**Default**
Geraral Settings		
MAC	Enter MAC address for static lease.	NULL
IP	Enter IP address for static lease.	NULL

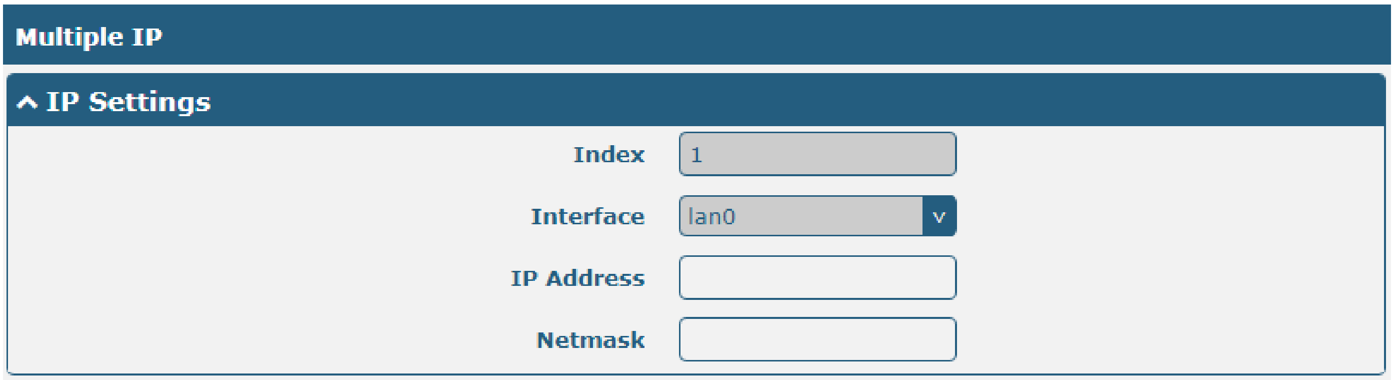
Multiple IP



^ Multiple IP Settings

Index	Interface	IP Address	Netmask	+

You may click + to add a multiple IP to the LAN port or click ✕ to delete the multiple IP of the LAN port. Now, click ✎ to edit the multiple IP of the LAN port.



Multiple IP

^ IP Settings

Index: 1

Interface: lan0

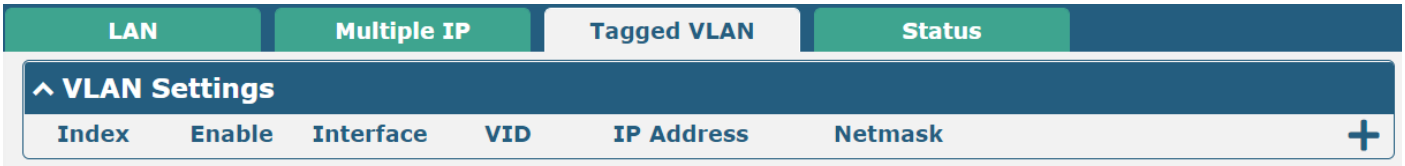
IP Address:

Netmask:

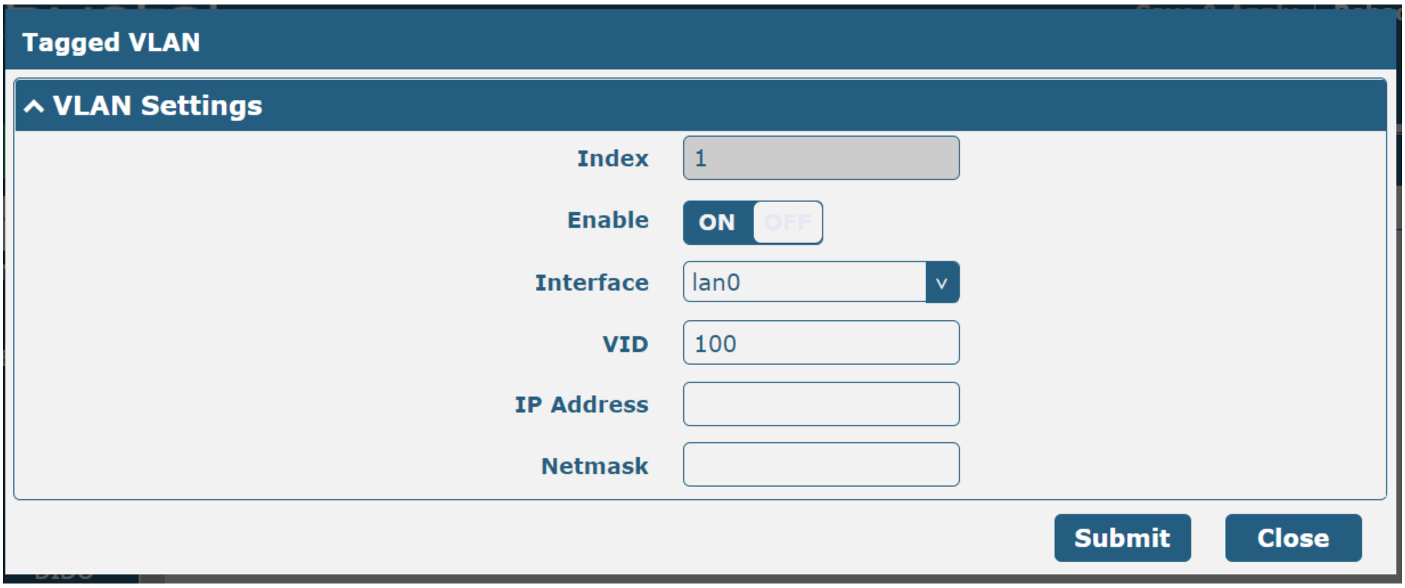
IP Settings		
Item	**Description**	**Default**
Index	Display index list.	--
Interface	Show editing port.	--
IP Address	Set IP addresses of the LAN port.	Null

IP Settings		
Item	**Description**	**Default**
Netmask	Set Netmask of the LAN port.	Null

Tagged VLAN



You may click + to add a VLAN to the LAN port or click ✕ to delete the VLAN of the LAN port. Now, click ✎ to edit the VLAN of the LAN port.



Tagged VLAN

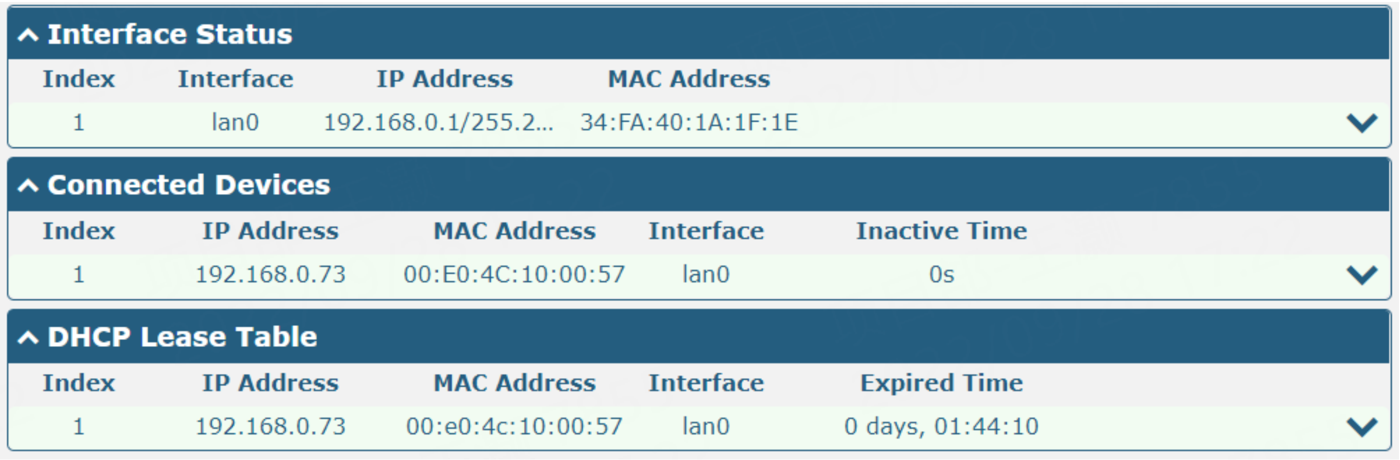
^ VLAN Settings

Index	1
Enable	ON
Interface	lan0
VID	100
IP Address	
Netmask	

VLAN Settings		
Item	**Description**	**Default**
Index	Display index list.	--
Enable	Click the toggle button to enable/disable the Tagged VLAN function.	ON
Interface	Show editing port.	--
VID	Set VLAN ID of the LAN port. Values range from 1 to 4094	100
IP Address	Set IP address of the VLAN.	Null
Netmask	Set Netmask of the VLAN.	Null

Status

This section allows you to view the status of the LAN connection.



Interface Status

Index	Interface	IP Address	MAC Address
1	lan0	192.168.0.1/255.2...	34:FA:40:1A:1F:1E

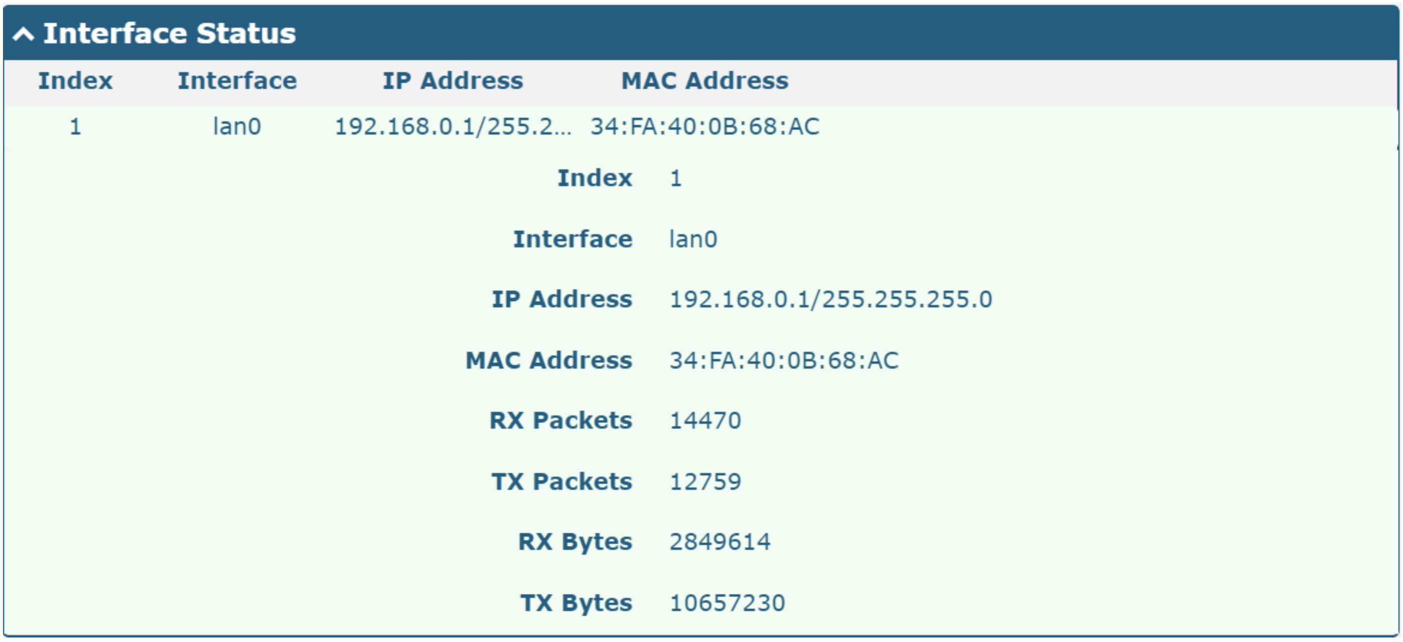
Connected Devices

Index	IP Address	MAC Address	Interface	Inactive Time
1	192.168.0.73	00:E0:4C:10:00:57	lan0	0s

DHCP Lease Table

Index	IP Address	MAC Address	Interface	Expired Time
1	192.168.0.73	00:e0:4c:10:00:57	lan0	0 days, 01:44:10

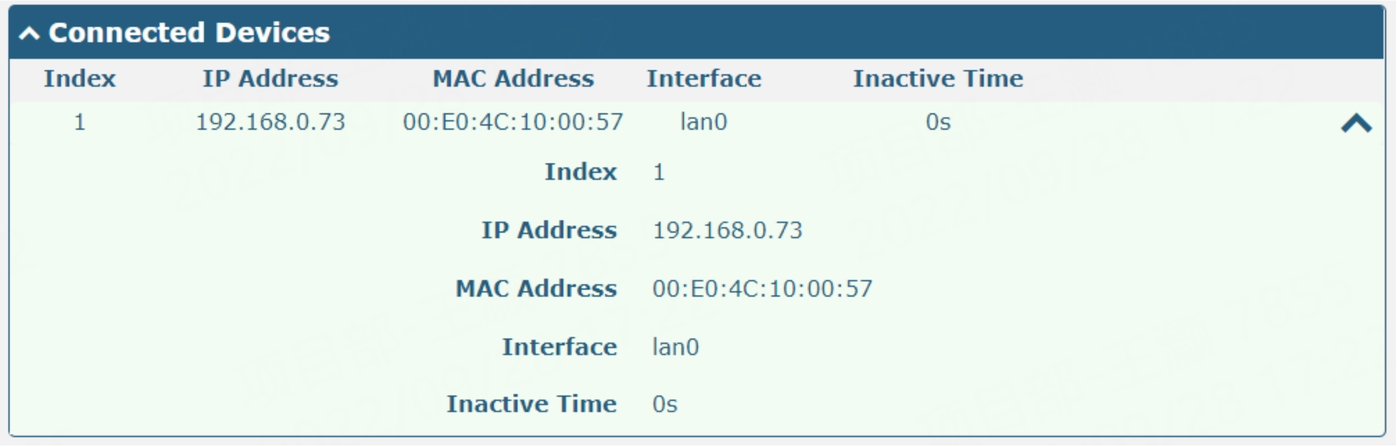
Click the row of status, the details status information will be displayed under the row.



Interface Status

Index	Interface	IP Address	MAC Address
1	lan0	192.168.0.1/255.2...	34:FA:40:0B:68:AC

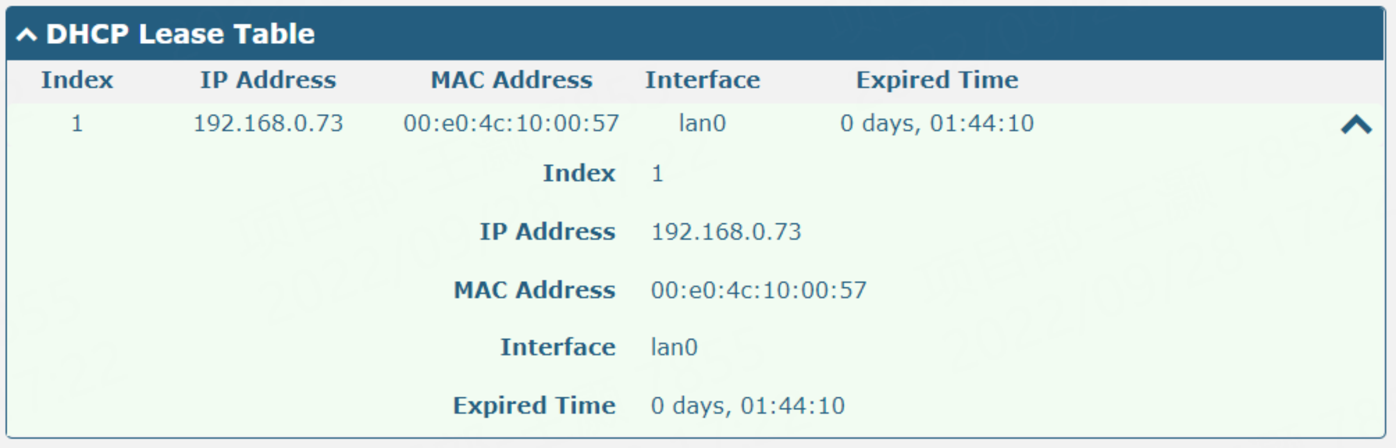
Index	1
Interface	lan0
IP Address	192.168.0.1/255.255.255.0
MAC Address	34:FA:40:0B:68:AC
RX Packets	14470
TX Packets	12759
RX Bytes	2849614
TX Bytes	10657230



Connected Devices

Index	IP Address	MAC Address	Interface	Inactive Time
1	192.168.0.73	00:E0:4C:10:00:57	lan0	0s

Index	1
IP Address	192.168.0.73
MAC Address	00:E0:4C:10:00:57
Interface	lan0
Inactive Time	0s



DHCP Lease Table

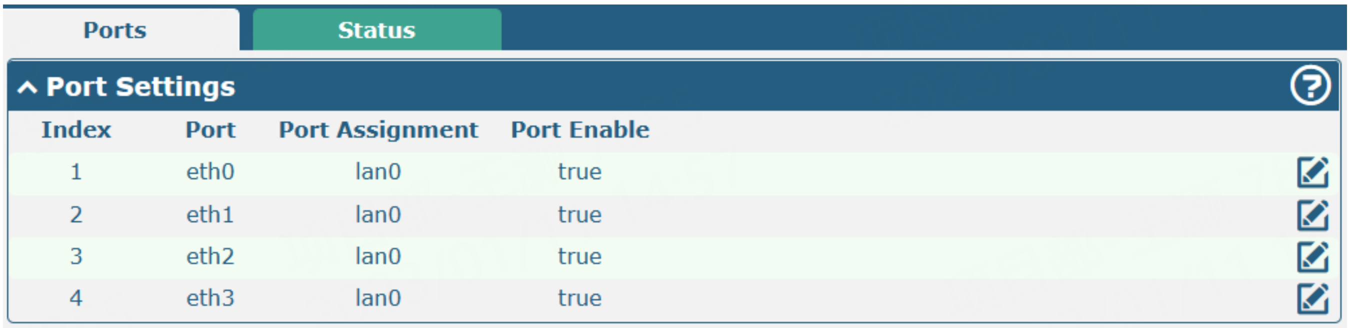
Index	IP Address	MAC Address	Interface	Expired Time
1	192.168.0.73	00:e0:4c:10:00:57	lan0	0 days, 01:44:10

Index	1
IP Address	192.168.0.73
MAC Address	00:e0:4c:10:00:57
Interface	lan0
Expired Time	0 days, 01:44:10

3.2.3 Ethernet

This section allows you to set the related parameters for Ethernet. There may be multi-Ethernet ports in the device. The ETH0 in the device can be configured as either a WAN port or LAN port, while other Ethernet port(s) can only be configured as LAN ports. The default settings of all Ethernet ports are lan0 and their default IP is 192.168.0.1/255.255.255.0.

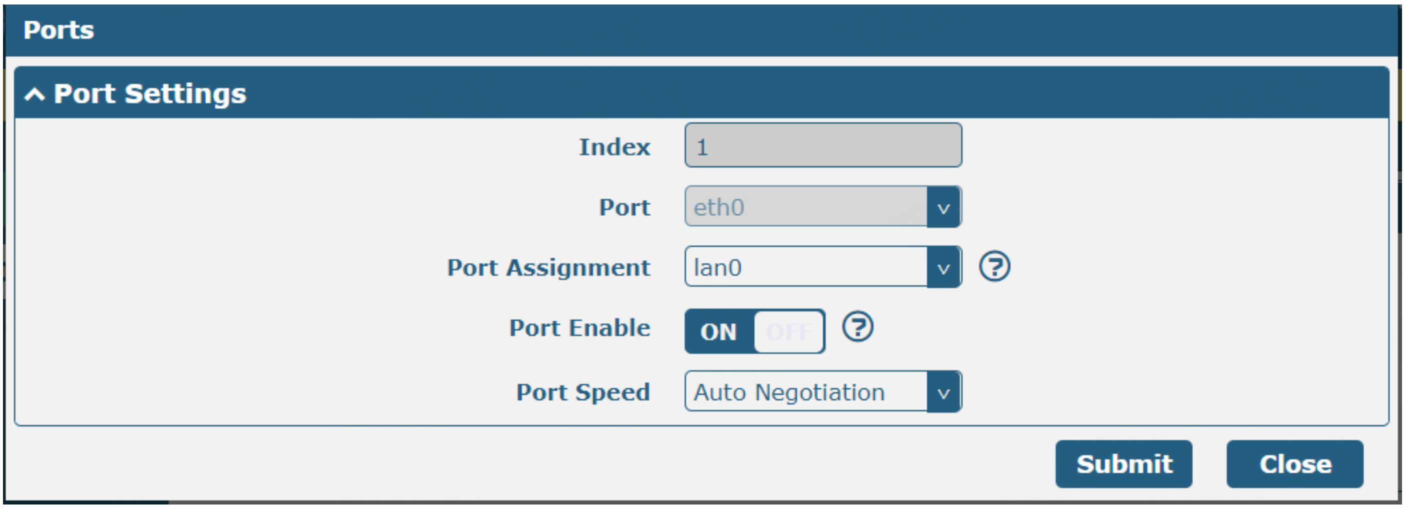
Note:
1) R2000 Dual can supply power to the behind device via ETH1~ETH4(enable the POE in Ports settings).
2) R3000 Lite has only one Ethernet port which can only be configured as LAN.
3) R2000 Lite has only one Ethernet port which can only be configured as LAN.
4) R1510 Lite has only one Ethernet port which can only be configured as LAN.



Port Settings

Index	Port	Port Assignment	Port Enable
1	eth0	lan0	true
2	eth1	lan0	true
3	eth2	lan0	true
4	eth3	lan0	true

Click button of eth0 to configure its parameters, and modify the port assignment parameters of eth0 in the pop-up window.



Ports

Port Settings

Index: 1

Port: eth0

Port Assignment: lan0

Port Enable: ON

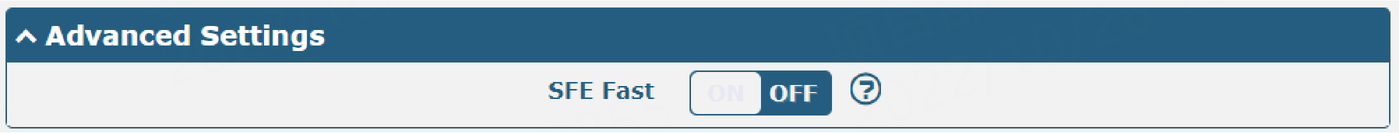
Port Speed: Auto Negotiation

Note:

(1) R2000 Series/R3000 Quad not support "Port Enable".

(2) Only R3000 Series support specify port speed.

Port Settings		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Port	Show editing port, read-only.	--
Port Assignment	Choose Ethernet port type, such as a WAN port or LAN port. When setting the port as a LAN port, you can click the drop-down list to select from “lan0” or “lan1”.	lan0
Port Enable	Enable or disable the port.	ON
Port Speed（Optional）	Specify port speed.	Auto Negotiation
PoE Enable (Optional)	Click to enable or disable the PoE function. When the PoE function is enabled, it will connect the POE voltage.	ON



Advanced Settings

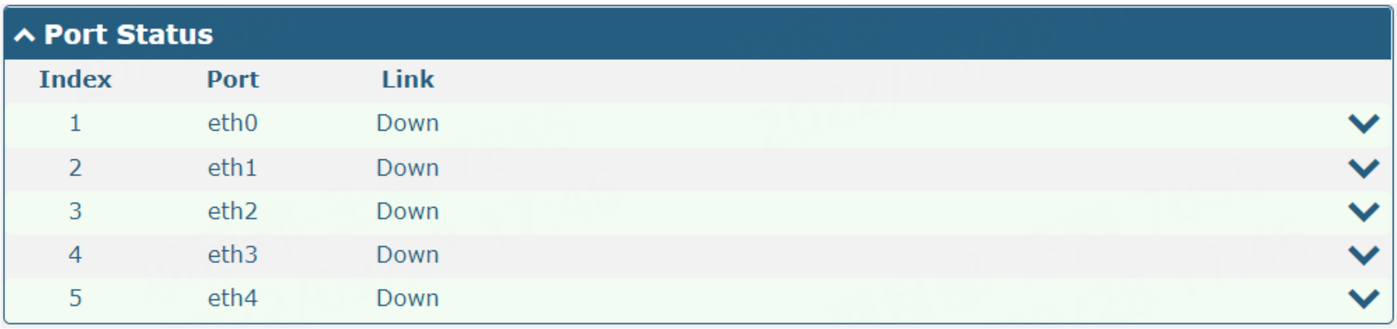
SFE Fast: OFF

Advanced Settings		
Item	**Description**	**Default**
SFE Fast	Click the toggle button to enable/disable this feature. SFE Fast can increase the ethernet port rate, but it affects QoS.	OFF

Note: Only R5020 support "SFE Fast ".

Status

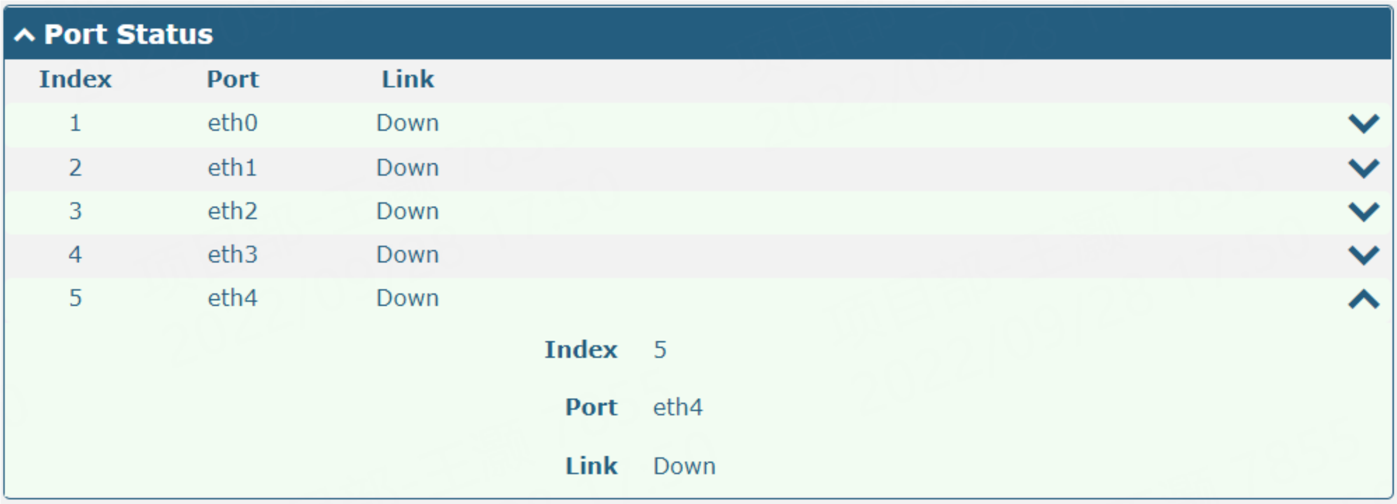
This section allows you to view the status of the Ethernet connection.



Port Status

Index	Port	Link
1	eth0	Down
2	eth1	Down
3	eth2	Down
4	eth3	Down
5	eth4	Down

Click the row of status, the details status information will be displayed under the row. Please refer to the screenshot below.



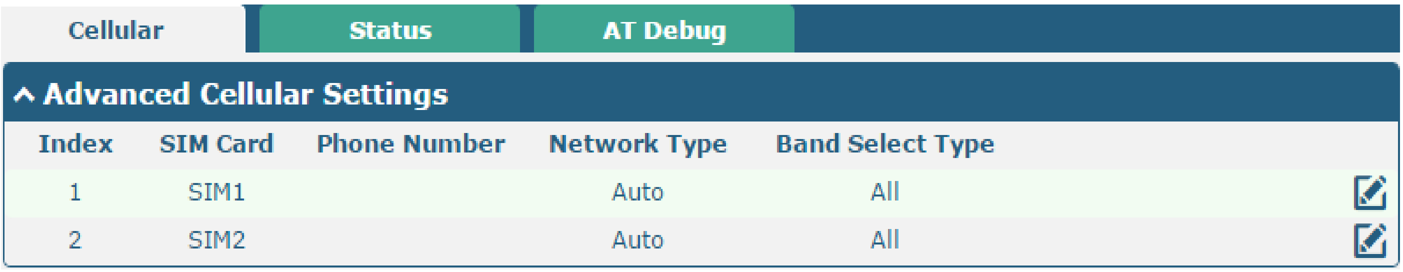
Port Status

Index	Port	Link
1	eth0	Down
2	eth1	Down
3	eth2	Down
4	eth3	Down
5	eth4	Down

Index	5
Port	eth4
Link	Down

3.2.4 Cellular

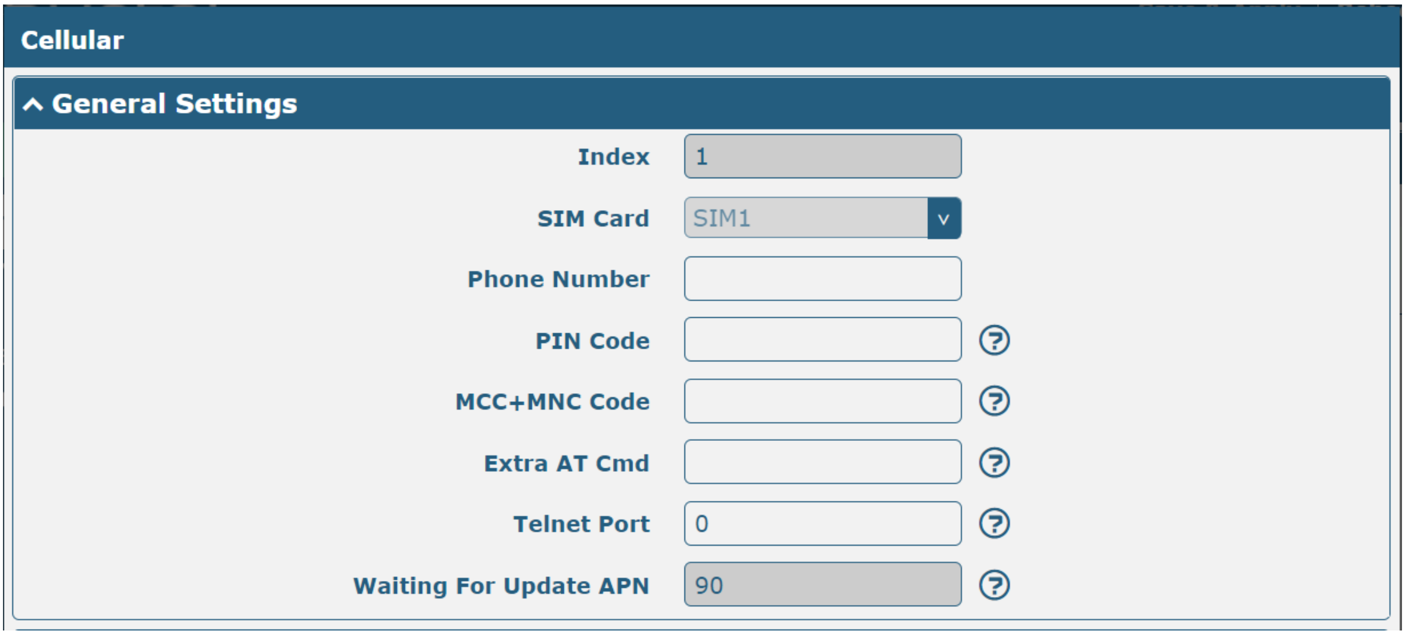
This section allows you to set the related parameters of Cellular. The device has 1 or 2 SIM card slots.



Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type
1	SIM1		Auto	All
2	SIM2		Auto	All

Click ✎ on the right-most of SIM 1 to edit the parameters.

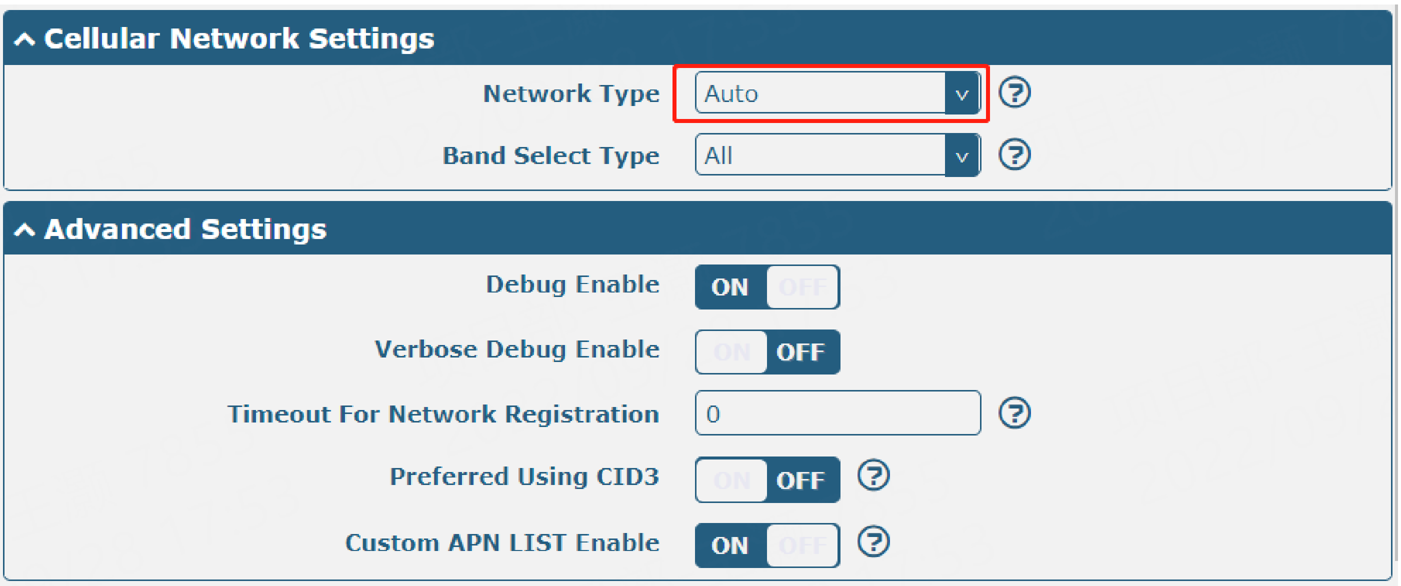


Cellular

^ General Settings

Index	1
SIM Card	SIM1
Phone Number	
PIN Code	
MCC+MNC Code	
Extra AT Cmd	
Telnet Port	0
Waiting For Update APN	90

The window is displayed below when choosing **"Auto"** as the network type.



^ Cellular Network Settings

Network Type	Auto
Band Select Type	All

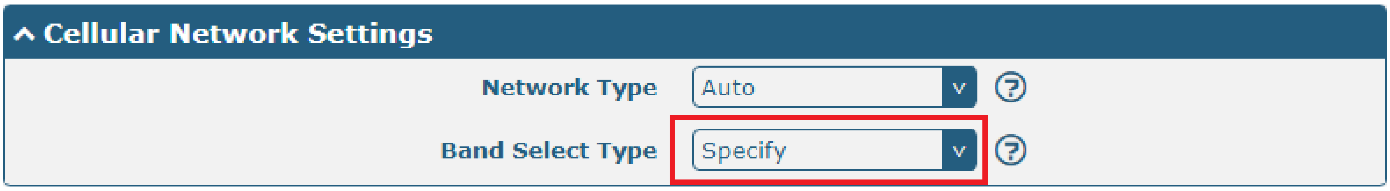
^ Advanced Settings

Debug Enable	ON
Verbose Debug Enable	OFF
Timeout For Network Registration	0
Preferred Using CID3	OFF
Custom APN LIST Enable	ON

The window is displayed below when choosing "**Specify**" as the band select type.

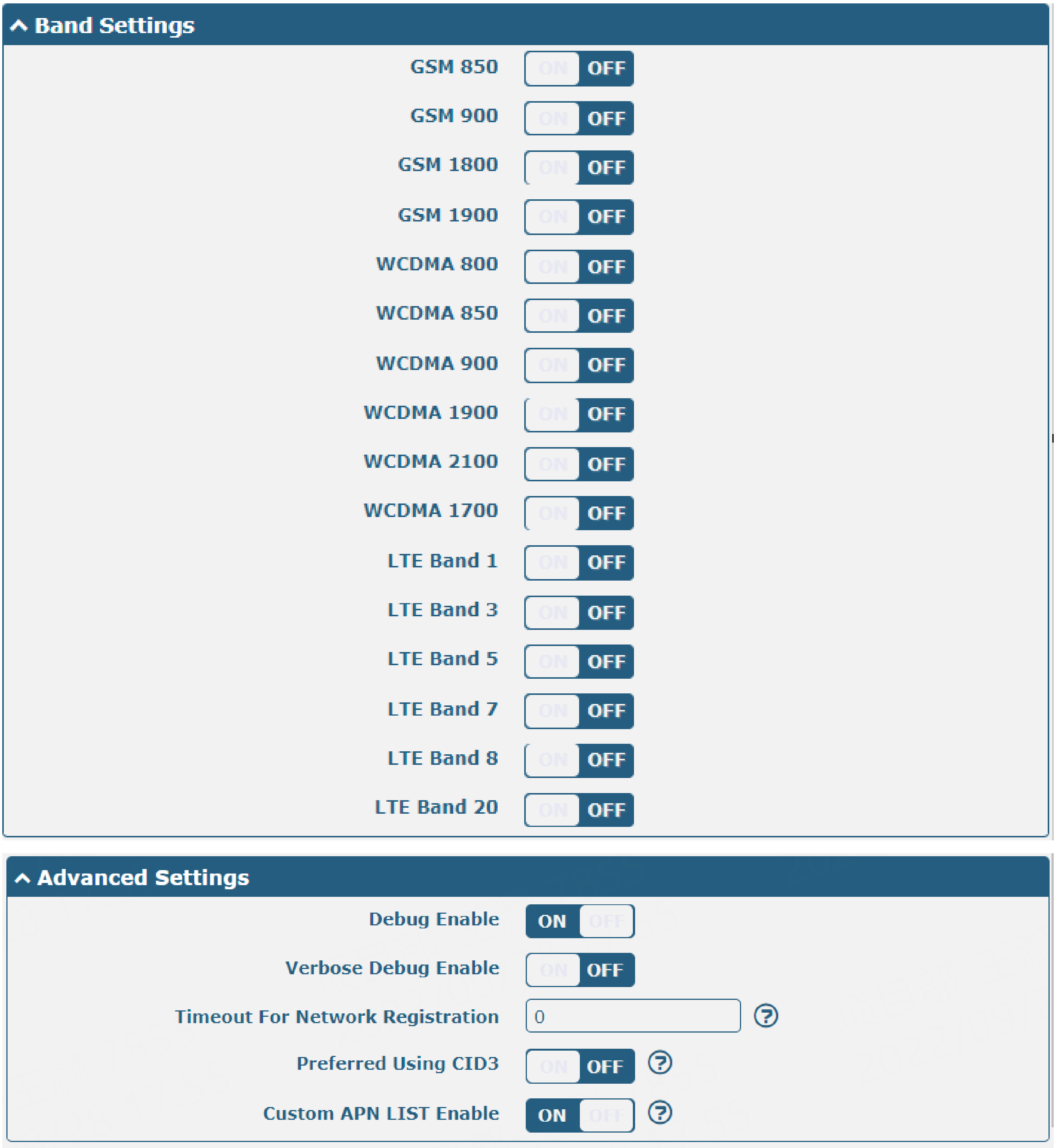
Note:

1) There may be some differences in Band Settings due to the different cellular modules.



^ Cellular Network Settings

Network Type	Auto
Band Select Type	Specify



^ Band Settings

GSM 850 OFF

GSM 900 OFF

GSM 1800 OFF

GSM 1900 OFF

WCDMA 800 OFF

WCDMA 850 OFF

WCDMA 900 OFF

WCDMA 1900 OFF

WCDMA 2100 OFF

WCDMA 1700 OFF

LTE Band 1 OFF

LTE Band 3 OFF

LTE Band 5 OFF

LTE Band 7 OFF

LTE Band 8 OFF

LTE Band 20 OFF

^ Advanced Settings

Debug Enable ON

Verbose Debug Enable OFF

Timeout For Network Registration 0

Preferred Using CID3 OFF

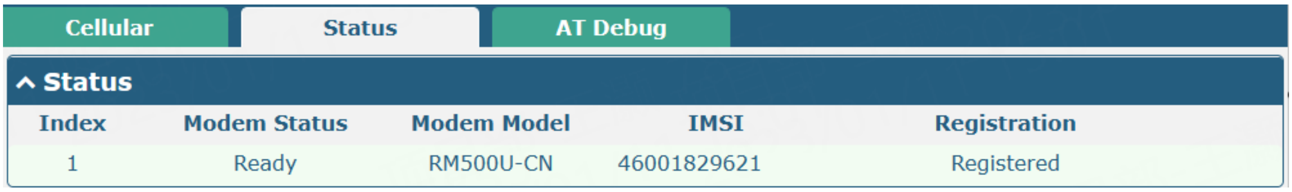
Custom APN LIST Enable ON

Cellular		
Item	**Description**	**Default**
General Settings		
Index	Indicate ordinal of list.	--
SIM Card	Show currently editing SIM card.	SIM1
Phone Number	Enter phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null

Cellular		
Item	**Description**	**Default**
MCC+MNC Code	Enter 5-6 digits and semicolon endings must be used. Used to lock the device can only use the specified carrier SIM card.	Null
Extra AT Cmd	Enter AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Waiting For Update APN	The time interval for automatically updating the APN after connecting to the network. Unit: second The modem needs to support automatic update APN feature. e.g.: HL7618RD	90
Cellular Network Settings		
Network Type	Select the cellular network type, which is the network access order. Select from "Auto", "2G Only", "2G First", "3G Only", "3G First", "4G Only", and "4G First". • Auto: Connect to the best signal network automatically. • 2G Only: Only the 2G network is connected. • 2G First: Connect to the 2G Network preferentially. • 3G Only: Only the 3G network is connected. • 3G First: Connect to the 3G Network preferentially. • 4G Only: Only the 4G network is connected. • 4G First: Connect to the 4G Network preferentially. ***Note:*** *1) There may be some different optional network types due to the different cellular modules.* *2) Click"?" Character in the menu for help to see the details.*	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose debugging information output.	OFF
Timeout For Network Registration	The timeout is required for the module to register to the network. Unit: seconds. 0 means the default setting is used.	0
Preferred Using CID3	Click the toggle button to enable/disable this option. Enable using APN3 to access the Internet. Some operators need to use APN3 to access the Internet normally, just like Verizon and it can be turned on if necessary	OFF
Custom APN LIST Enable	Click the toggle button to enable/disable this option. Enable Custom APN LIST feature	ON

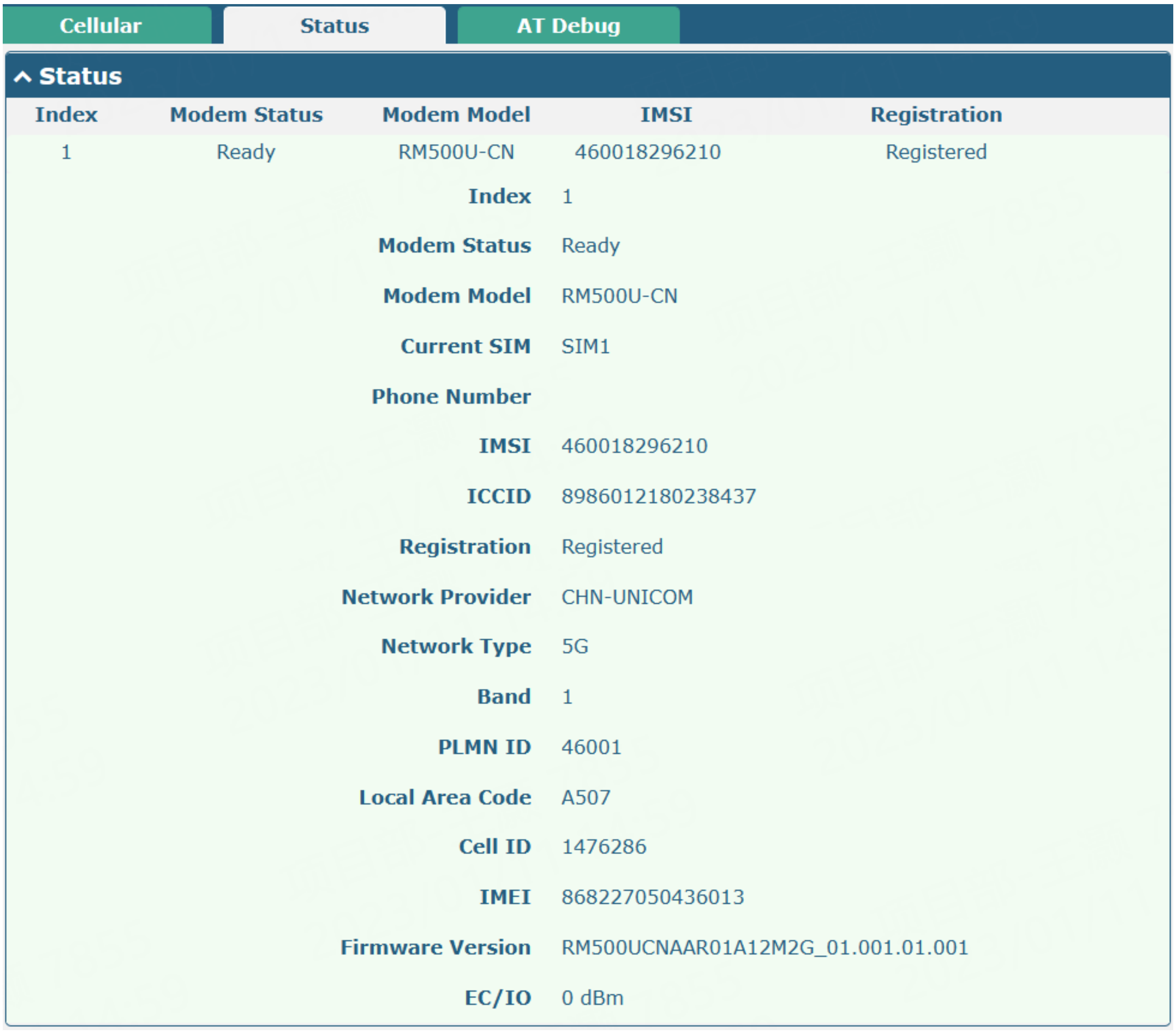
Status

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



Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	RM500U-CN	46001829621	Registered

Click the row of status, detail will be displayed under the row.



Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	RM500U-CN	460018296210	Registered

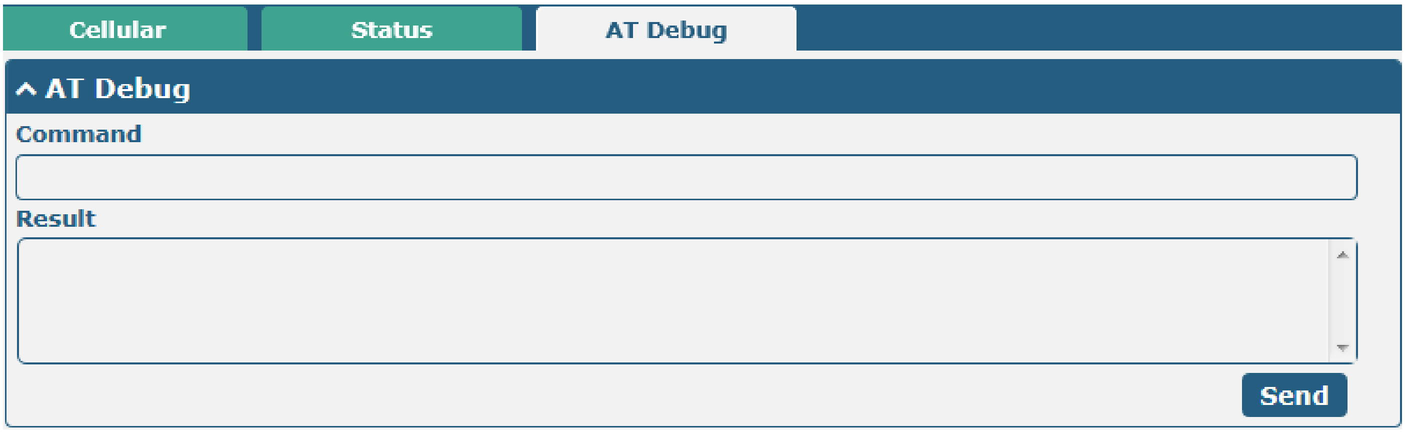
Index	1
Modem Status	Ready
Modem Model	RM500U-CN
Current SIM	SIM1
Phone Number	
IMSI	460018296210
ICCID	8986012180238437
Registration	Registered
Network Provider	CHN-UNICOM
Network Type	5G
Band	1
PLMN ID	46001
Local Area Code	A507
Cell ID	1476286
IMEI	868227050436013
Firmware Version	RM500UCNAAR01A12M2G_01.001.01.001
EC/IO	0 dBm

Status	
Item	**Description**
Index	Indicate ordinal of list.
Modem Status	Show status of radio module.
Modem Model	Show model of radio module.

Status	
Item	**Description**
Current SIM	Show SIM card that your device is using.
Phone Number	Show phone number of current SIM. ***Note:*** *This option will be displayed if entered manually in* ***Cellular >SIM1/ SIM2 > General Settings > Phone Number****.*
IMSI	Show IMSI number of current SIM.
ICCID	Show ICCID number of current SIM.
Registration	Show current network status.
Network Provider	Show name of the Network Provider.
Network Type	Show current network service type, e.g., GPRS.
5G Architecture	Show current 5G type. SA or NSA. This option is only displayed on 5G products.
Band	Show band of the current network.
Signal Strength	Show signal strength. (Only valid for 2/3/4G network, please refer to RSRP for 5G network)
RSRP	Show Reference Signal Received Power value. (Only valid for 4G or 5G networks)
RSRQ	Show Reference Signal Received Quality value. (Only valid for 4G or 5G networks)
PLMN ID	Show current PLMN ID.
Local Area Code	Show current local area code used for identifying the different areas.
Cell ID	Show current cell ID used for locating the device.
IMEI	Show IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show current firmware version of cellular module.
SINR	Show signal to interference plus noise ratio. (Only for 4G network or 5G network)
Physical Cell ID	Show Physical Cell ID.

AT Debug

This section allows you to do the AT Debug.



AT Debug		
Item	**Description**	**Default**

AT Debug		
Item	**Description**	**Default**
Command	Enter AT command that you want to send to the cellular module in this text box.	Null
Result	Show AT command responded by the cellular module in this text box.	Null
Send	Click the button to send AT command.	--

3.2.5 Wi-Fi

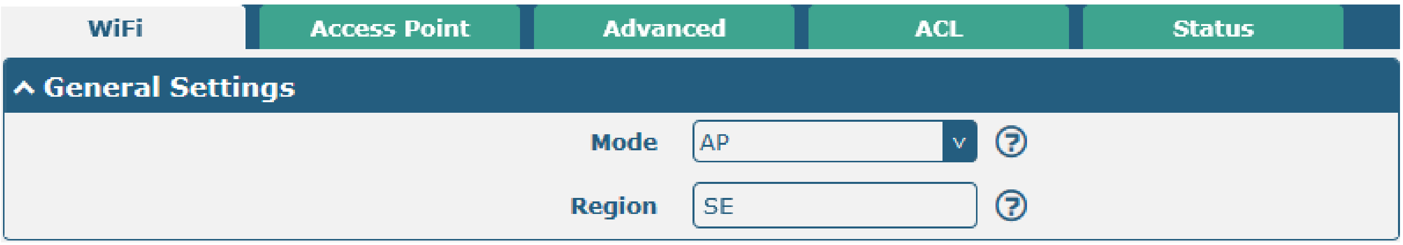
This section allows you to configure the parameters of two Wi-Fi modes. The device supports both Wi-Fi AP or Client modes and defaults as AP.

Wi-Fi AP

Configure Device as Wi-Fi AP

Click **"Interface > Wi-Fi > Wi-Fi"**, select "AP" as the mode and click "Submit".

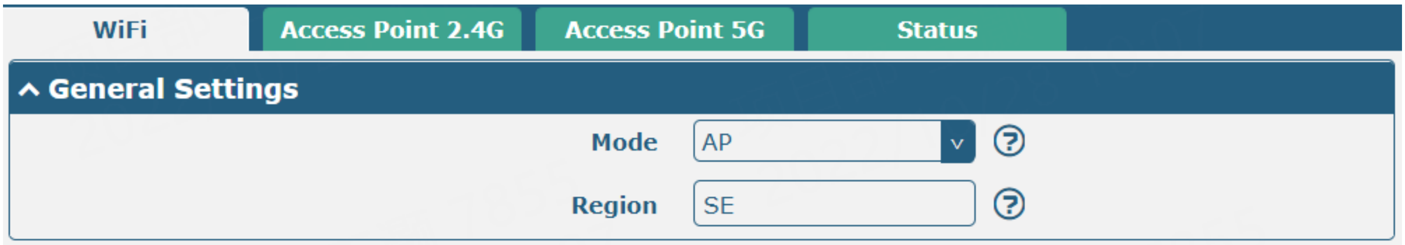
2.4GHz WI-FI Only



Mode AP

Region SE

2.4GHz and 5GHz Wi-Fi



Mode AP

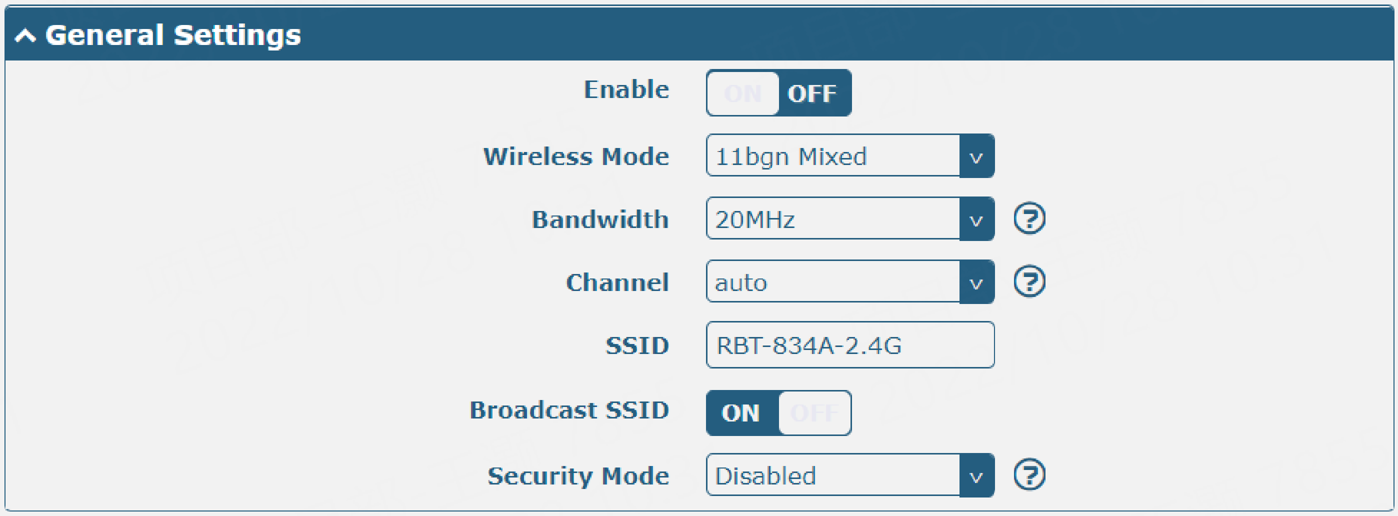
Region SE

Note:

1) Please click **Save & Apply > Reboot** after finishing the configuration, then the change will take effect.
2) Only R2110 and R5020 support 2.4GHz and 5GHz.

Access Point 2.4G

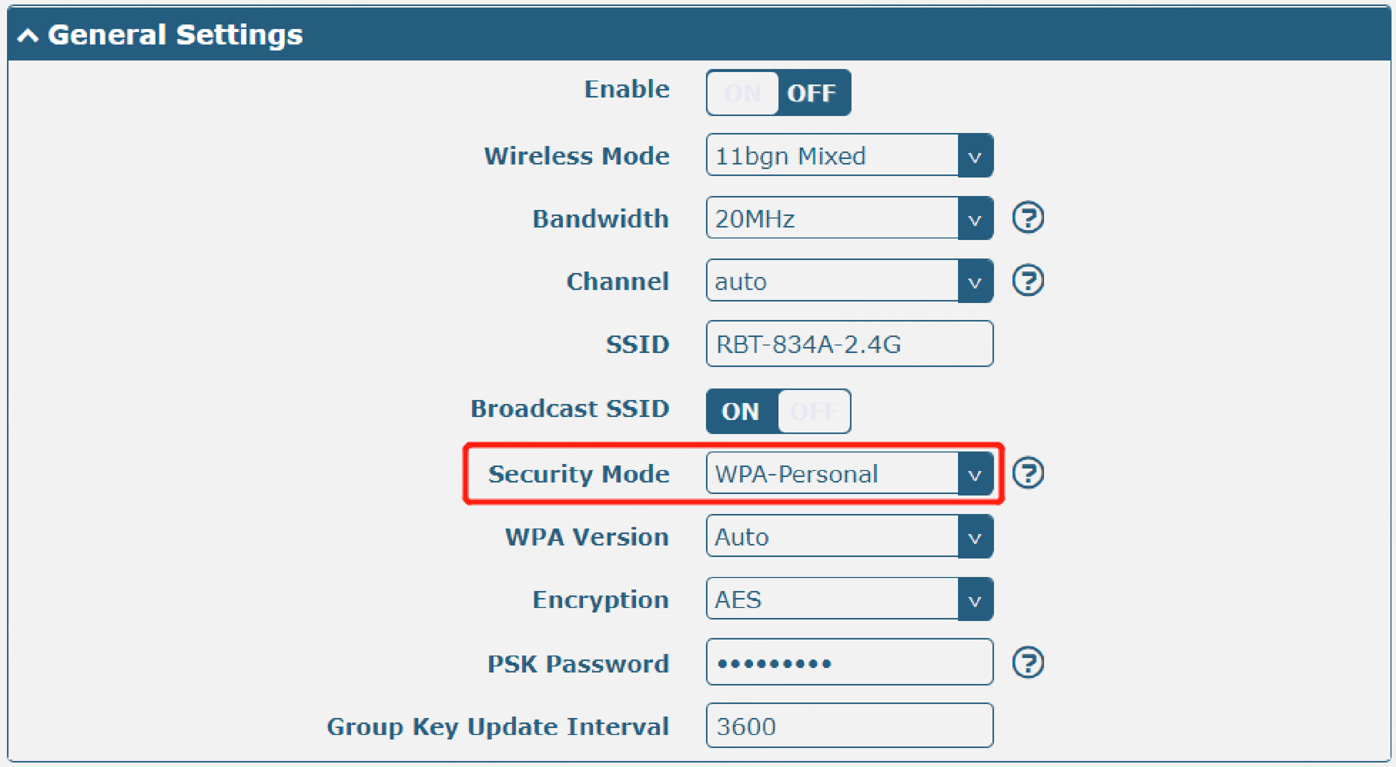
Click the **Access Point 2.4G** column to configure the parameters of Wi-Fi AP. By default, the security mode is set as "Disabled".



^ General Settings

Enable	ON OFF
Wireless Mode	11bgn Mixed
Bandwidth	20MHz
Channel	auto
SSID	RBT-834A-2.4G
Broadcast SSID	ON OFF
Security Mode	Disabled

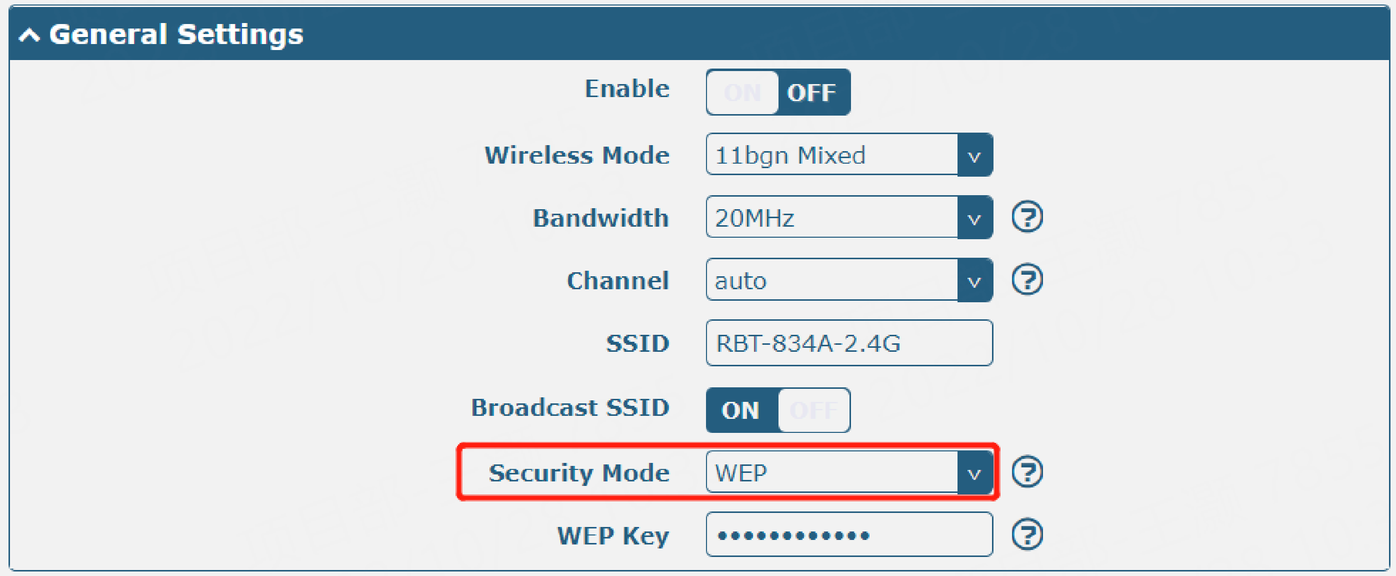
The window is displayed below when setting "WPA-Personal" as the security mode.



^ General Settings

Enable	ON OFF
Wireless Mode	11bgn Mixed
Bandwidth	20MHz
Channel	auto
SSID	RBT-834A-2.4G
Broadcast SSID	ON OFF
Security Mode	WPA-Personal
WPA Version	Auto
Encryption	AES
PSK Password	•••••••••
Group Key Update Interval	3600

The window is displayed below while setting “WEP” as the security mode.



General Settings

Enable: ON OFF

Wireless Mode: 11bgn Mixed

Bandwidth: 20MHz

Channel: auto

SSID: RBT-834A-2.4G

Broadcast SSID: ON OFF

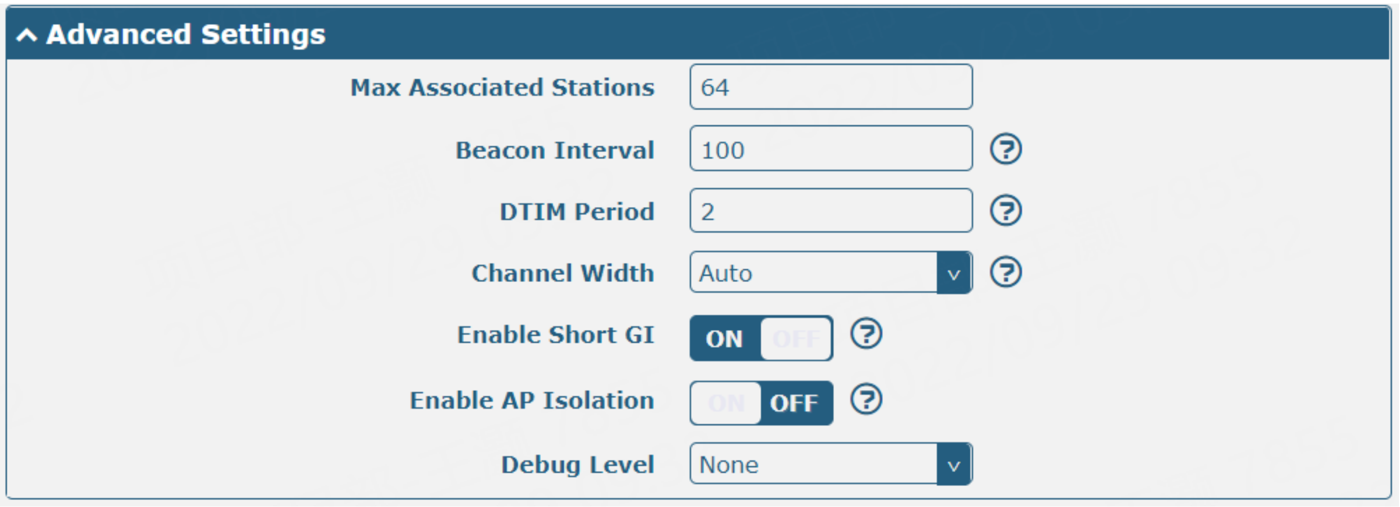
Security Mode: WEP

WEP Key: ••••••••••••

General Settings @ Access Point 2.4G		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Wi-Fi access point option.	OFF
Wireless Mode	Select from “11bgn Mixed”, “11b only”, “11g only”, and “11n only”. • 11bgn Mixed: mix three protocols for backward compatibility • 11b only: IEEE 802.11b, 11 Mbps • 11g only: IEEE 802.11g, 54 Mbps • 11n only: IEEE 802.11n, 450 Mbps	11bgn Mixed
Channel	The channel that different bandwidths can choose is as follows. • Auto: The device will scan all frequency channels until the best one is found. • The frequency of 1~13 channels of 20MHz bandwidth available channel: 1–2412 MHz 2–2417 MHz 3–2422 MHz 4–2427 MHz 5–2432 MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz 10–2457 MHz 11–2462 MHz 12–2467 MHz	Auto

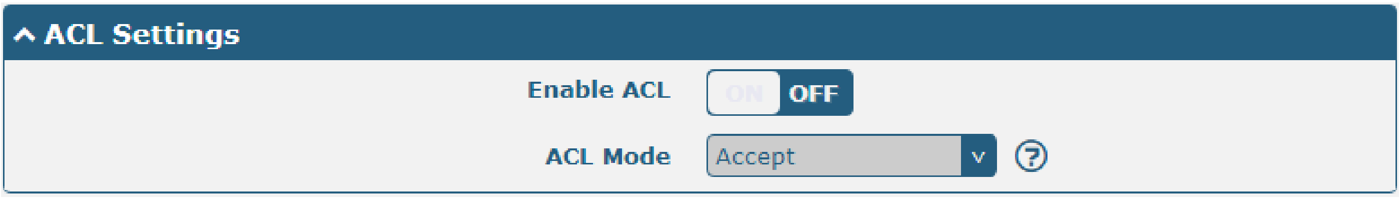
General Settings @ Access Point 2.4G		
Item	**Description**	**Default**
	13–2472 MHz • The frequency of 1~13 channels of 40MHz bandwidth available channel: 1–2412 MHz 2–2417 MHz 3–2422 MHz 4–2427 MHz 5–2432 MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz 10–2457 MHz 11–2462 MHz 12–2467 MHz 13–2472 MHz	
SSID	Enter SSID (Service Set Identifier), the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	RBT-XXXX-2.4G
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the device AP, you need to manually enter the SSID of the device AP on the Wi-Fi client side.	ON
Security Mode	Select “Disabled”, “WPA-Personal” or “WEP”. • Disabled: The user can access the Wi-Fi without a password ***Note**: It is strongly recommended for security purposes that you do not choose this kind of mode.* • WPA-personal: Wi-Fi access protection. Only one password is provided for identity authentication • WEP: Wired Equivalent Privacy provides encryption for wireless device’s data transmission	Disabled
WPA Version	Select from “Auto”, “WPA” or “WPA2” or “WPA3”. • Auto: Device will automatically choose the most suitable WPA version • WPA2 is a stronger security feature than WPA • ***Note**: Only R151x/R201x support WPA3.*	Auto

General Settings @ Access Point 2.4G		
Item	**Description**	**Default**
Encryption	Select from "TKIP" or "AES". • TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication • AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP ***Note:*** *The security mode will affect the wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor the TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode.*	Auto
PSK Password	Enter Pre-share key password. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the time of group key renewal.	3600
WEP Key	Enter WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null



Advanced Settings @ Access Point 2.4G		
Item	**Description**	**Default**
Max Associated Stations	Set the max number of clients allowed to access the device's AP. (Value 0 means without limitation)	0
Beacon Interval	Set the interval of time in which the device AP broadcasts a beacon which is used for wireless network authentication.	100
DTIM Period	Set delivery traffic indication message period, and the device AP will multicast the data according to this period.	2

Advanced Settings @ Access Point 2.4G		
Item	**Description**	**Default**
Channel Width	Select device channel width, “20 MHz” or “40 MHz” ***Note:*** *40 MHz channel width provides twice the data rate available over a single 20 MHz channel; the data transfer rate of 80MHz bandwidth is 4 times greater than that of a single 20Mhz bandwidth.*	Auto
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval option. Short GI is a blank time between two symbols, providing a long buffer time for signal delay. Using the Short GI would increase 11% in data rates, but also result in higher packet error rates.	ON
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the device will isolate all connected wireless devices. The wireless devices can’t access each other.	OFF
Debug Level	Select from “verbose”, “debug”, “info”, “notice”, “warning”, or “none”.	none

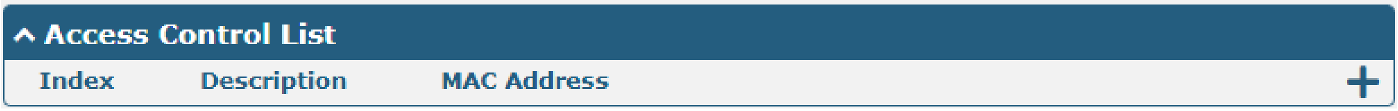


^ ACL Settings

Enable ACL ON OFF

ACL Mode Accept

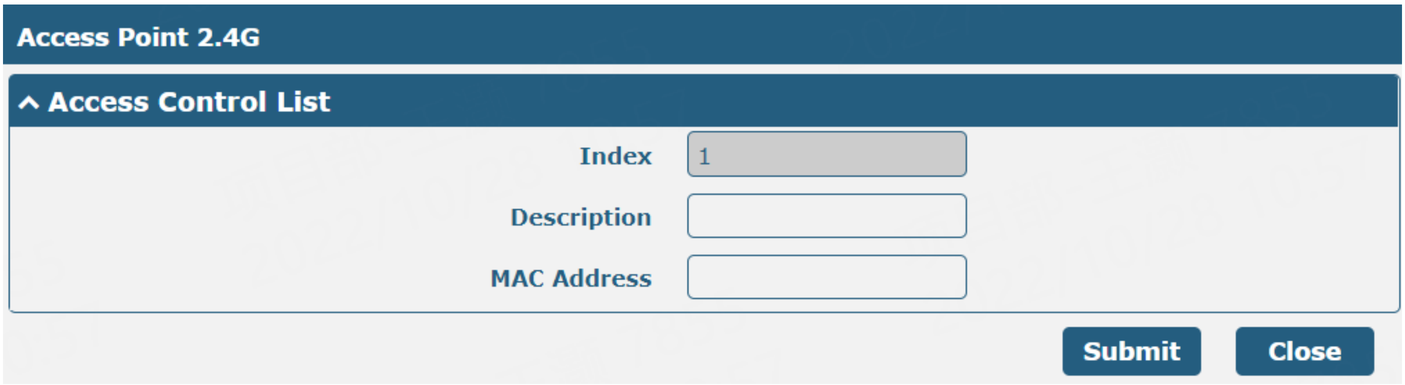
ACL Settings @ Access Point 2.4G		
Item	**Description**	**Default**
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select “Accept” or “Deny”. • Accept: Only the packets fitting the entities of the “Access Control List” can be allowed • Deny: All the packets fitting the entities of the “Access Control List” will be denied ***Note****: The device can only allow or deny devices included in the “Access Control List” at one time.*	Accept



^ Access Control List

Index	Description	MAC Address	+

Click + to add a MAC address to the Access Control List. The maximum count for MAC addresses is **64**.


Access Point 2.4G

^ Access Control List

Index: 1

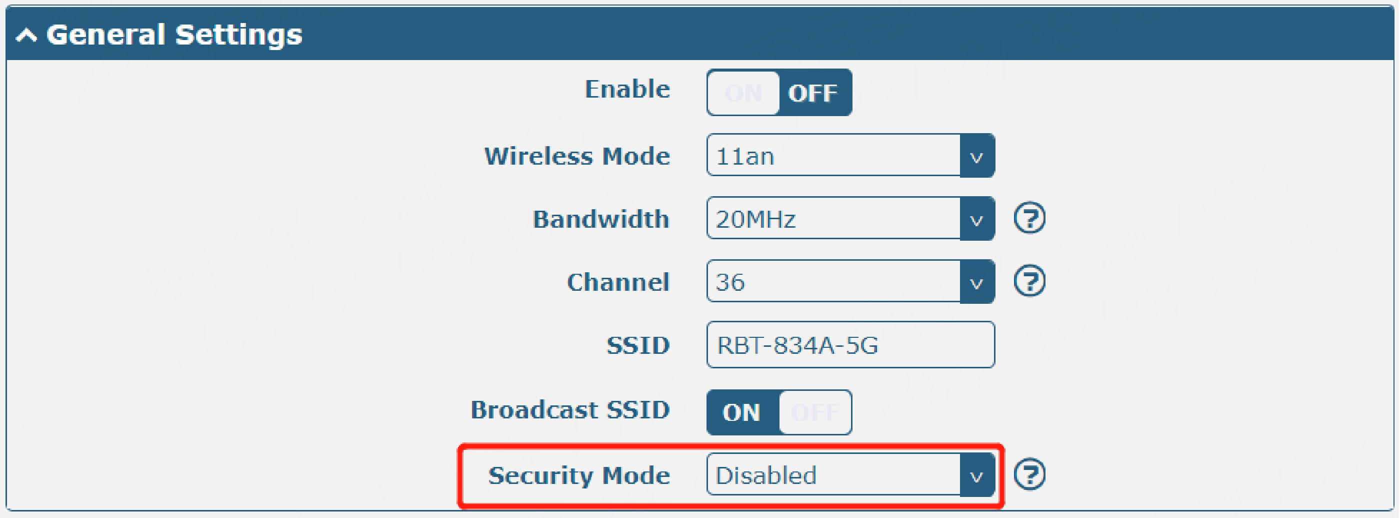
Description:

MAC Address:

Access Control List @ Access Point 2.4G		
Index	Indicate ordinal of list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

Access Point 5G

Click the **Access Point 5G** column to configure the parameters of Wi-Fi AP. By default, the security mode is set as "Disabled".


^ General Settings

Enable: ON OFF

Wireless Mode: 11an

Bandwidth: 20MHz

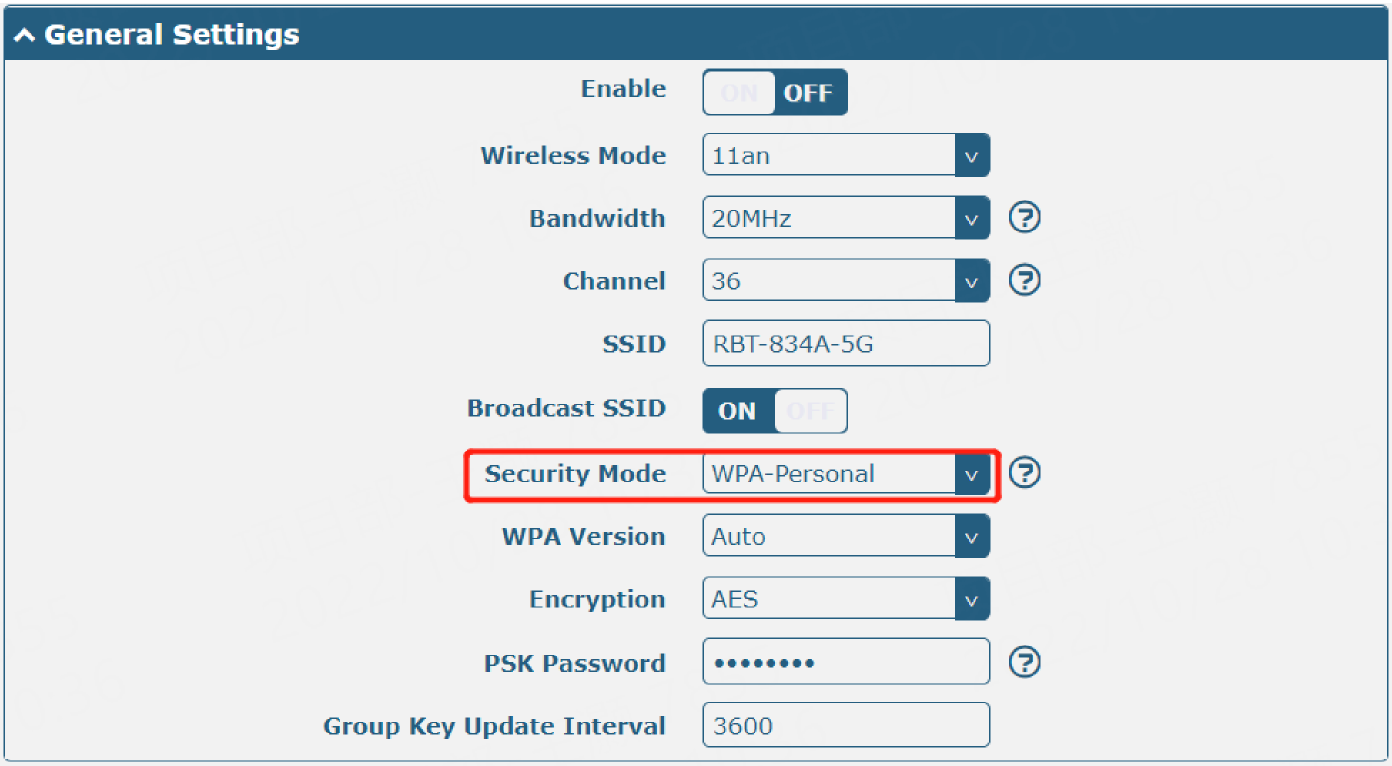
Channel: 36

SSID: RBT-834A-5G

Broadcast SSID: ON OFF

Security Mode: Disabled

The window is displayed below when setting "WPA-Personal" as the security mode.



Enable ON OFF

Wireless Mode 11an

Bandwidth 20MHz

Channel 36

SSID RBT-834A-5G

Broadcast SSID ON OFF

Security Mode WPA-Personal

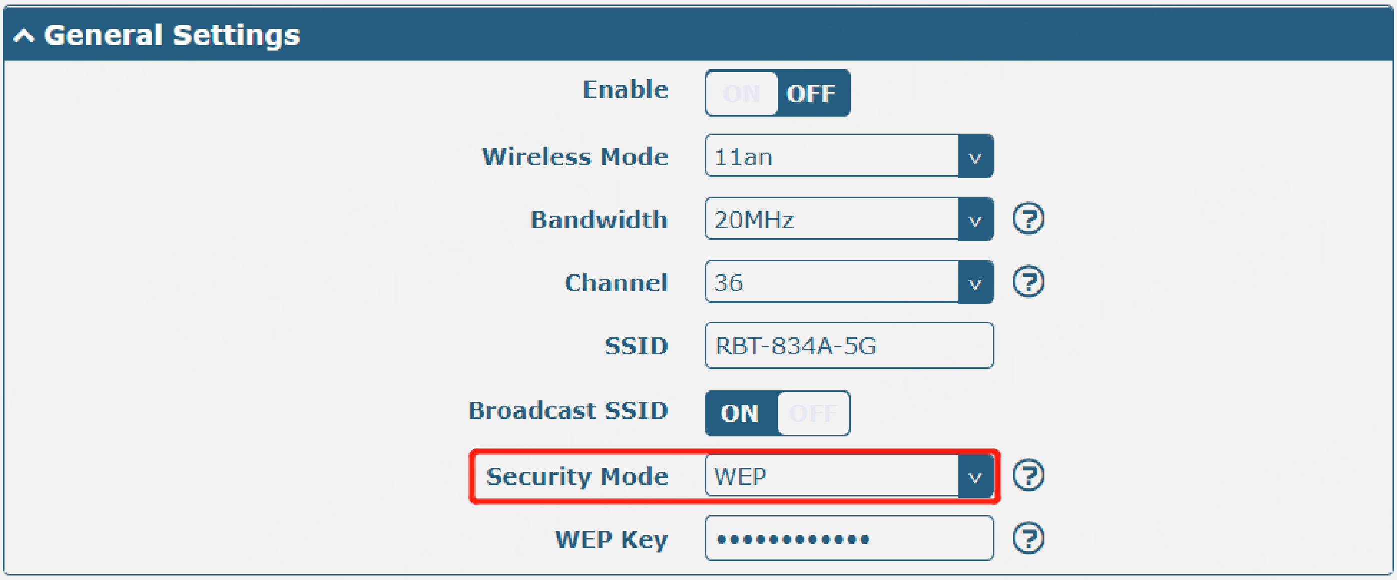
WPA Version Auto

Encryption AES

PSK Password ••••••••

Group Key Update Interval 3600

The window is displayed below when setting “WEP” as the security mode.



Enable ON OFF

Wireless Mode 11an

Bandwidth 20MHz

Channel 36

SSID RBT-834A-5G

Broadcast SSID ON OFF

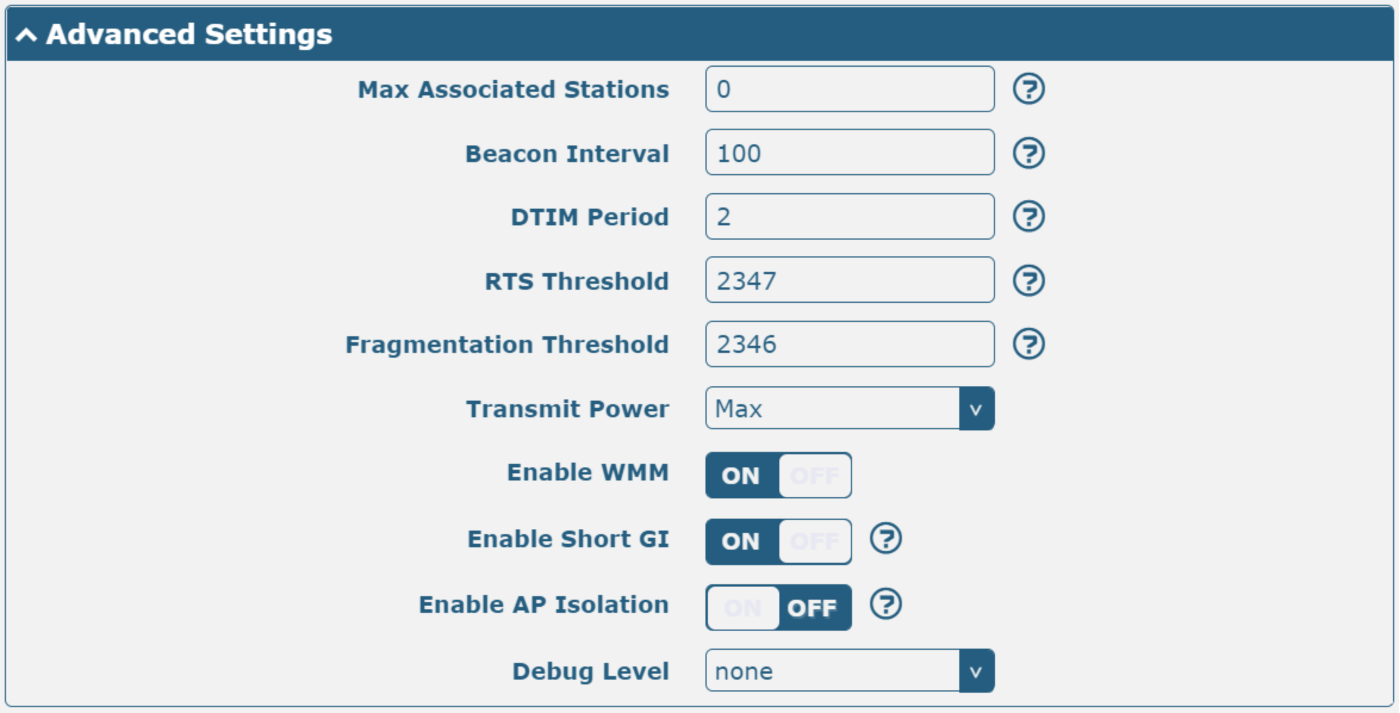
Security Mode WEP

WEP Key ••••••••••••

General Settings @ Access Point 5G		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Wi-Fi access point option.	OFF
Wireless Mode	Select from “11an”, or “11a/an/ac”. • 11an: Compatible IEEE 802.11a, 54 Mbps and IEEE 802.11n, 300Mbps • 11a/an/ac: Compatible IEEE 802.11a, 54 Mbps, IEEE802.11n 300 Mbps and 802.11ac, 867 Mbps	11an

General Settings @ Access Point 5G		
Item	**Description**	**Default**
Bandwidth	Select from “20MHz”, “40MHz” or “80MHz”. ***Note***: *40 MHz channel width provides twice the data rate available over a single 20 MHz channel; the data transfer rate of 80MHz bandwidth is 4 times greater than that of a single 20Mhz bandwidth.*	20MHz
Channel	The optional channels for bandwidths are as below. • The frequency of 36~165 channels of 20MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz • The frequency of 36~165 channels of 40MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz • The frequency of 36~165 channels of 80MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz ***Note:*** *All available channels of 5GHz Wi-Fi on different bandwidths are listed above. Web parameters should be configured due to the different available channels in different countries and areas.*	36

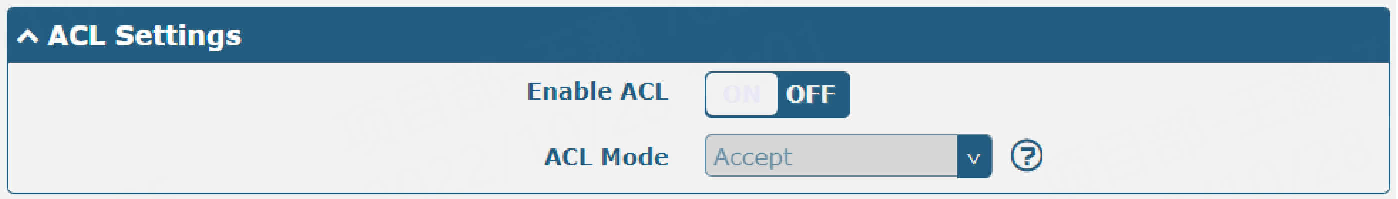
General Settings @ Access Point 5G		
Item	**Description**	**Default**
SSID	Enter SSID (Service Set Identifier), the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	RBT-XXXX-5G
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the device AP, you need to manually enter the SSID of the device AP on the Wi-Fi client side.	ON
Security Mode	Select from "Disabled", "WPA-Personal", or "WEP". • Disabled: The user can access the Wi-Fi without a password ***Note**: It is strongly recommended for security purposes that you do not choose this kind of mode.* • WPA-personal: Wi-Fi access protection, only one password is provided for identity authentication • WEP: Wired Equivalent Privacy provides encryption for wireless device's data transmission	Disabled
WPA Version	Select from "Auto", "WPA" or "WPA2" • Auto: Device will choose automatically the most suitable WPA version • WPA2 is a stronger security feature than WPA	Auto
Encryption	Select from "TKIP" or "AES". • TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication • AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP ***Note:** The security mode will affect the wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor the TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode.*	AES
PSK Password	Enter Pre-share key password. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the time of group key renewal.	3600
WEP Key	Enter WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null



^ Advanced Settings

Max Associated Stations	0
Beacon Interval	100
DTIM Period	2
RTS Threshold	2347
Fragmentation Threshold	2346
Transmit Power	Max
Enable WMM	ON
Enable Short GI	ON
Enable AP Isolation	OFF
Debug Level	none

Advanced Settings @ Access Point 5G		
Item	**Description**	**Default**
Max Associated Stations	Set the max number of clients allowed to access the device's AP. (Value 0 means without limitation)	0
Beacon Interval	Set the interval of time in which the device AP broadcasts a beacon which is used for wireless network authentication.	100
DTIM Period	Set delivery traffic indication message period and the device AP will multicast the data according to this period.	2
RTS Threshold	Set "request to send" threshold. When the threshold is set as 2347, the device AP will not send a detection signal before sending data. And when the threshold is set as 0, the device AP will send a detection signal before sending data.	2347
Fragmentation Threshold	Set fragmentation threshold of a Wi-Fi AP. It is recommended that you use the default value 2346.	2346
Transmit Power	Select from "Max", "High", "Medium" or "Low".	Max
Enable WMM	Click the toggle button to enable/disable the WMM option.	ON
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval option. Short GI is a blank time between two symbols, providing a long buffer time for signal delay. Using the Short GI would increase 11% in data rates, but also result in higher packet error rates.	ON
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the device will isolate all connected wireless devices. The wireless devices cannot access each other.	OFF
Debug Level	Select from "verbose", "debug", "info", "notice", "warning", or "none".	none

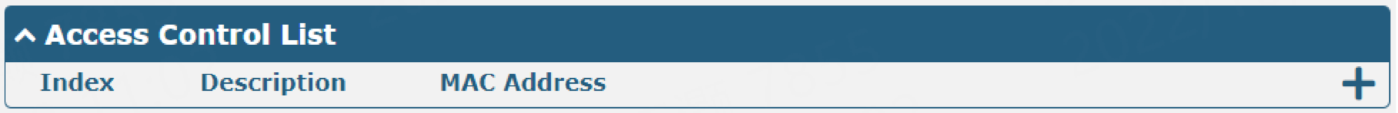


ACL Settings

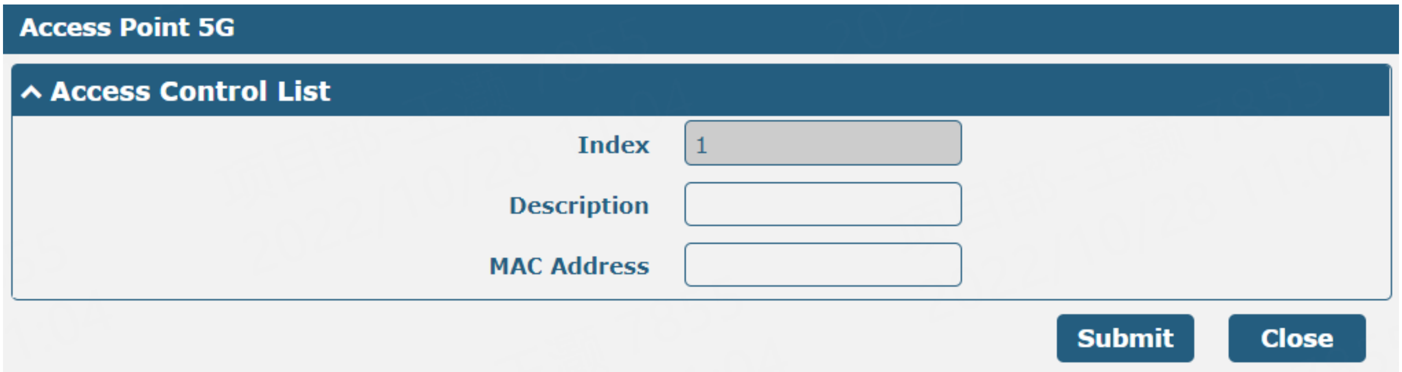
Enable ACL: ON OFF

ACL Mode: Accept

ACL Settings @ Access Point 5G		
Item	**Description**	**Default**
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select from “Accept” or “Deny”. • Accept: Only the packets fitting the entities of the “Access Control List” can be allowed • Deny: All the packets fitting the entities of the “Access Control List” will be denied ***Note**: The device can only allow or deny devices that are included in the “Access Control List” at one time.*	Accept



Click + to add a MAC address to the Access Control List. The maximum count for MAC addresses is **64**.



Access Point 5G

Access Control List

Index: 1

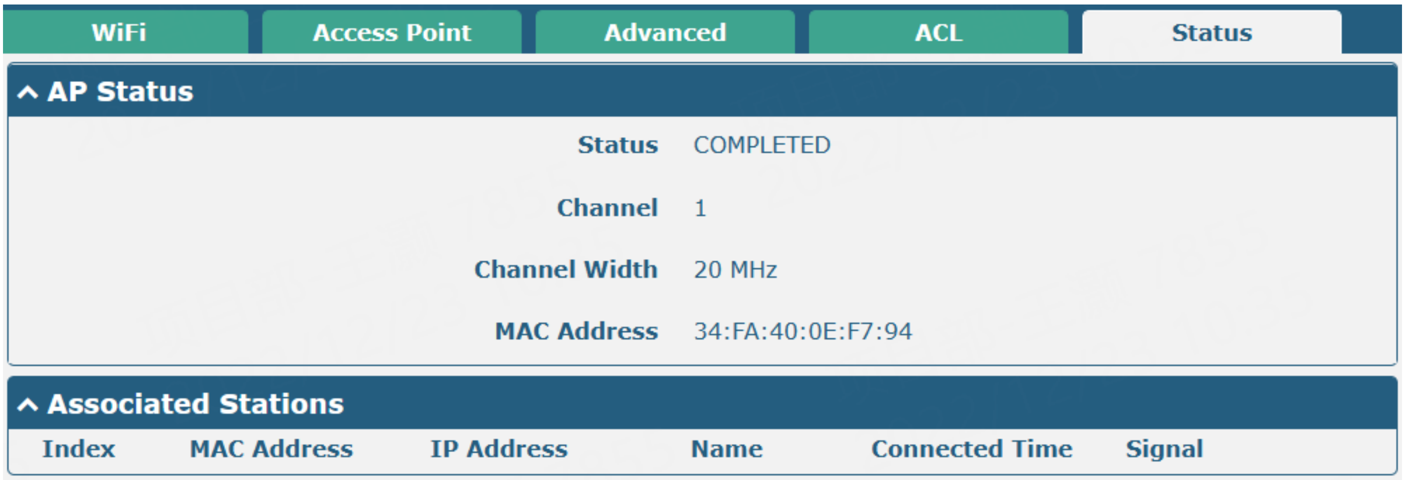
Description:

MAC Address:

Access Control List @ Access Point 5G		
Index	Indicate ordinal of list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

Status

This section allows you to view the status of AP.



AP Status

Status	COMPLETED
Channel	1
Channel Width	20 MHz
MAC Address	34:FA:40:0E:F7:94

Associated Stations

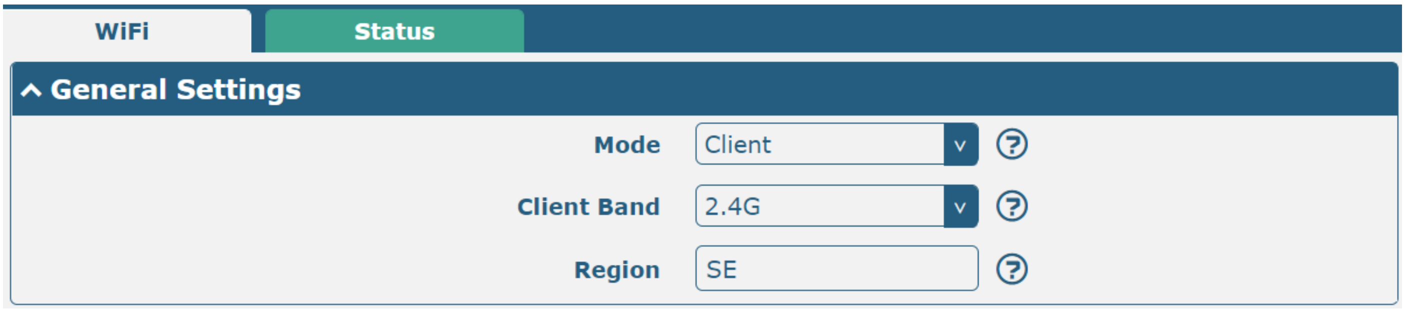
Index	MAC Address	IP Address	Name	Connected Time	Signal

Note: *Wi-Fi is off by default. Follow the steps below to enable it and set the device as Wi-Fi client.*

Wi-Fi Client

Configure Device as Wi-Fi Client

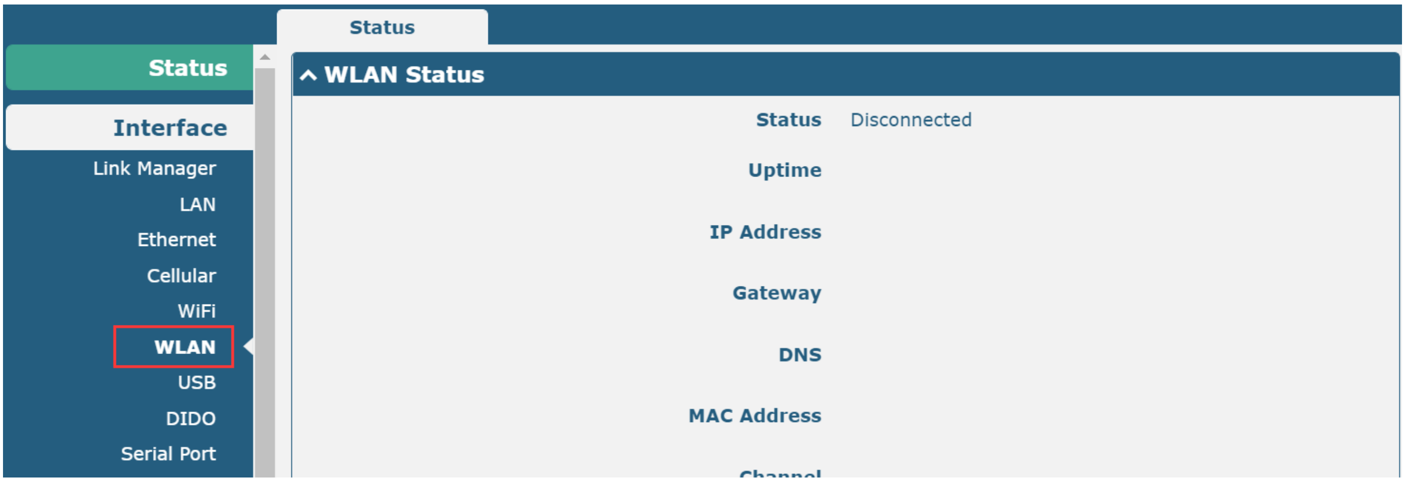
Click **Interface > WiFi > WiFi**, select "Client" as the mode, and regarding the AP type to choose the related Client Band then click "Submit".



General Settings

Mode	Client
Client Band	2.4G
Region	SE

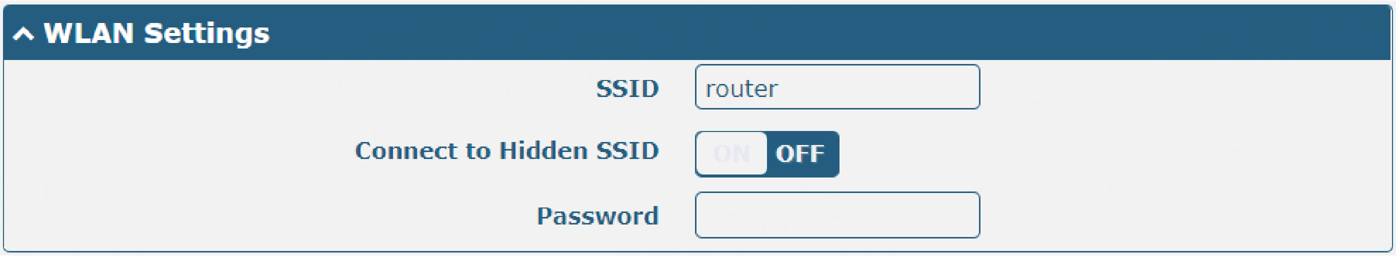
And then a "WLAN" column will appear under the Interface list.



WLAN Status

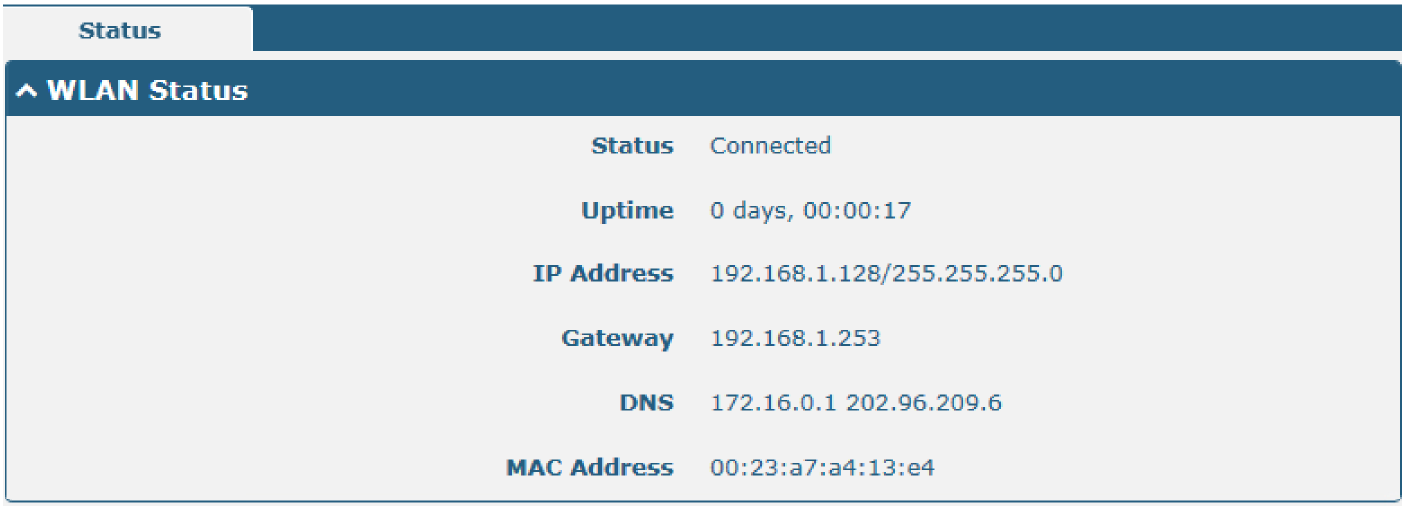
Status	Disconnected
Uptime	
IP Address	
Gateway	
DNS	
MAC Address	
Channel	

Click **Interface > Link Manager > Link Settings**, and click the edit button of WLAN, then configure its related parameters.



SSID	router
Connect to Hidden SSID	ON OFF
Password	

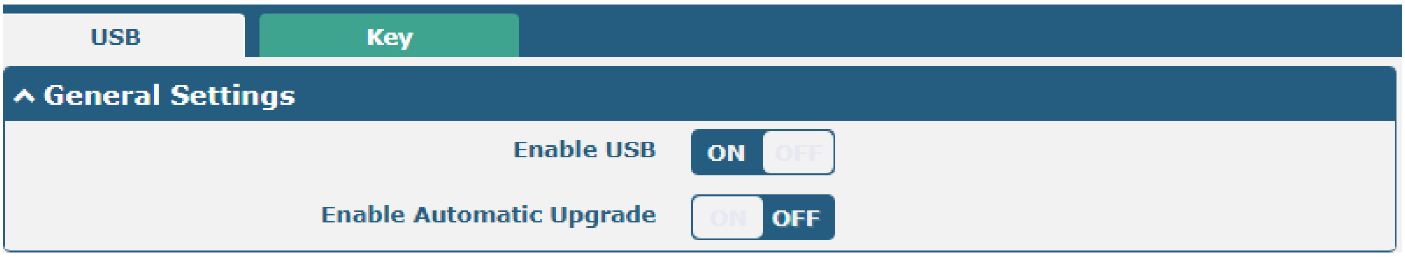
Click **Interface > WLAN** to configure the parameters of Wi-Fi Client after setting the mode as Client. Please remember to click **Save & Apply > Reboot** after finishing the configuration, so that the configuration can take effect.



Status	Connected
Uptime	0 days, 00:00:17
IP Address	192.168.1.128/255.255.255.0
Gateway	192.168.1.253
DNS	172.16.0.1 202.96.209.6
MAC Address	00:23:a7:a4:13:e4

3.2.7 USB

This section allows you to set the USB parameters. The USB interface of the device can be used for firmware upgrades and configuration upgrades.



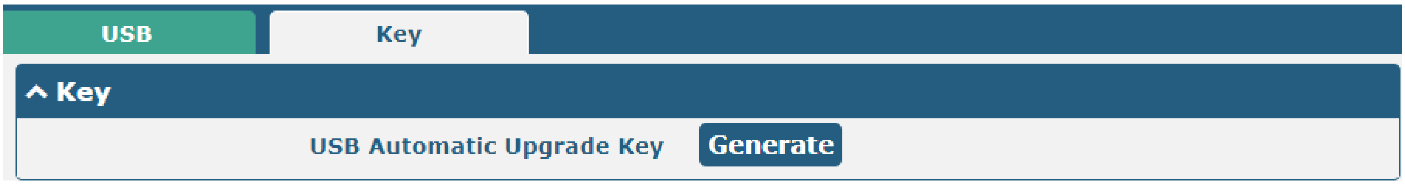
General Settings

Enable USB: ON

Enable Automatic Upgrade: OFF

Key

This section allows you to generate the key for the USB.



Key

USB Automatic Upgrade Key: Generate

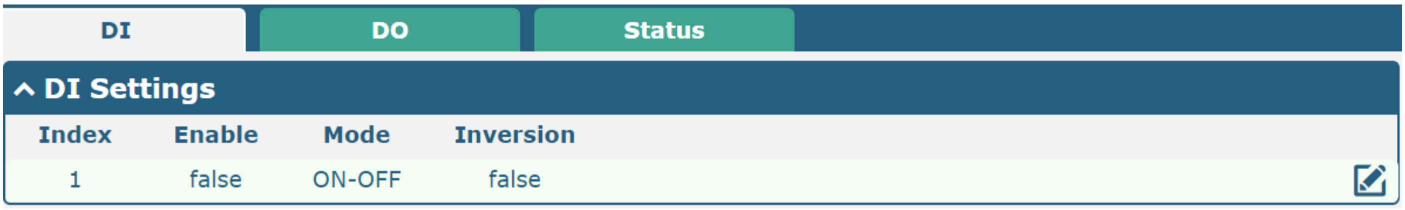
General Settings @ USB		
Item	**Description**	**Default**
Enable USB	Click the toggle button to enable/disable the USB option.	ON
Enable Automatic Upgrade	Click the toggle button to enable/disable this option. Enable to automatically update the firmware of the device when inserting a USB storage device with a device firmware.	OFF
Key		
Item	**Description**	**Default**
USB Automatic Update Key	Click Generate to generate a key, and click Download to download the key.	--

Note: *In the process of USB auto upgrade, when using the USB auto-upgrade function, when the running light appears, it means the upgrade is in progress. When the running light stops and the USR light is on, it means the upgrade is complete. After upgrading, the device will not restart automatically. If there is no running light effect, it means that there is an abnormality, and it does not enter into the automatic upgrade process.*

3.2.8 DI/DO

This section allows you to set the DI/DO parameters. The DI interface can be used for triggering the alarm, while the DO can be used for controlling the slave device to realize real-time monitoring.

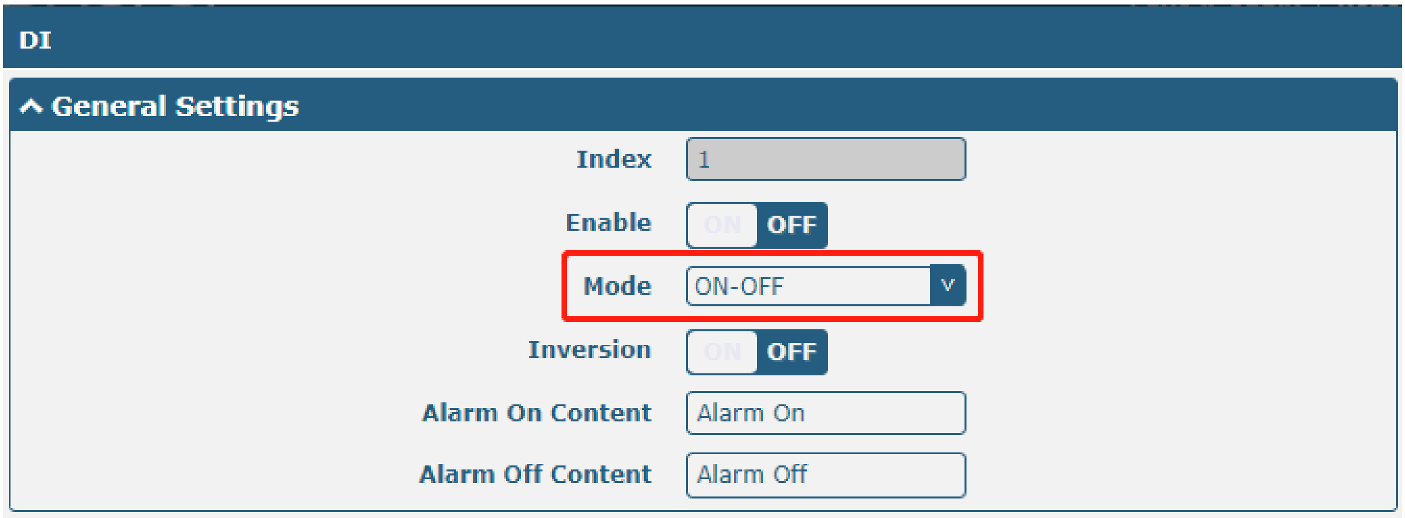
DI



DI Settings

Index	Enable	Mode	Inversion
1	false	ON-OFF	false

Click the right-most ✎ button of DI index 1 as below. The window is displayed below when the default mode is "ON-OFF".

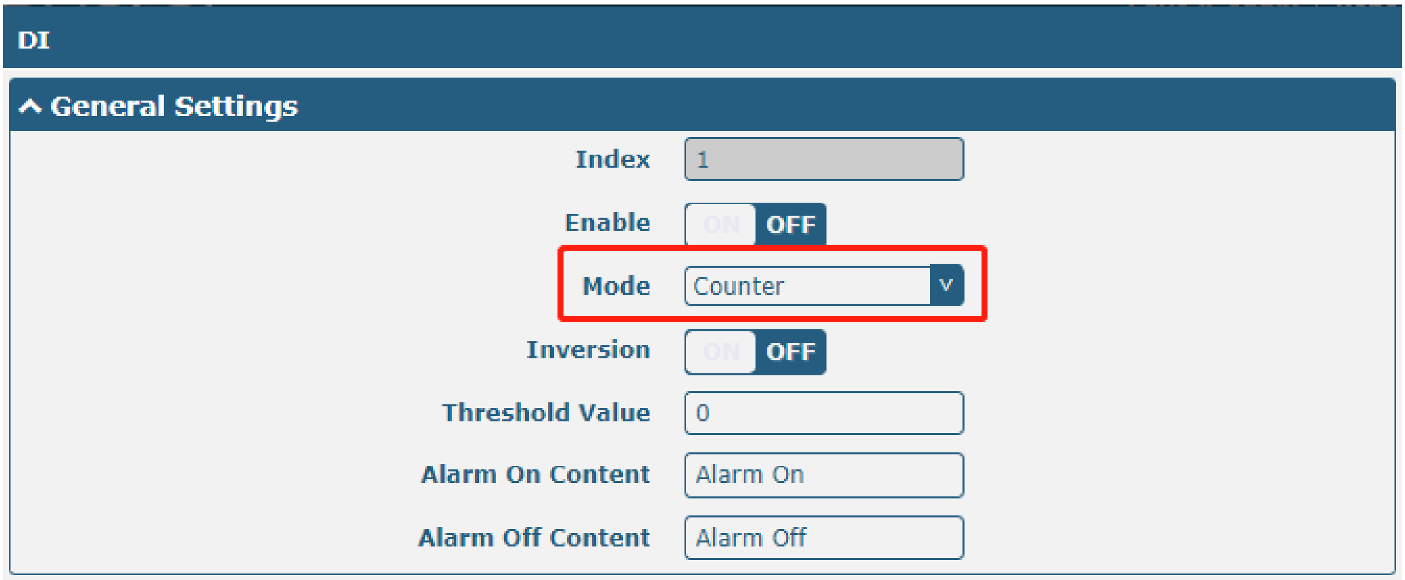


DI

General Settings

Index	1
Enable	ON OFF
Mode	ON-OFF
Inversion	ON OFF
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off

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



DI

General Settings

Index: 1

Enable: ON OFF

Mode: Counter

Inversion: ON OFF

Threshold Value: 0

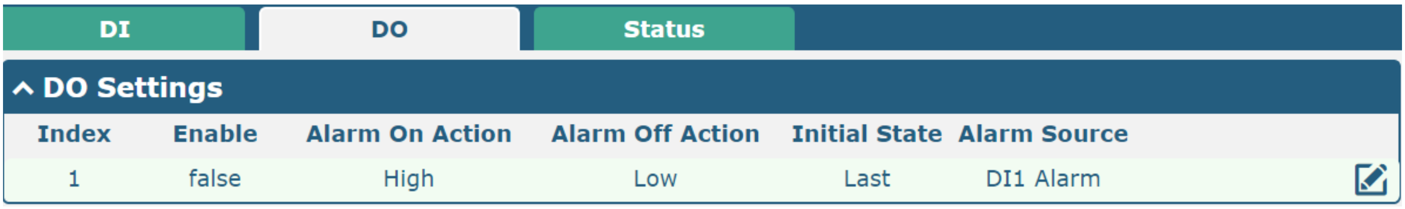
Alarm On Content: Alarm On

Alarm Off Content: Alarm Off

General Settings @ DI		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
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.	ON-OFF
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 counted. Set the threshold value to trigger the DI alarm when the count value reaches the threshold value.	0
Alarm On Content	Show content when the alarm is on.	Alarm On
Alarm Off Content	Show content when the alarm is off.	Alarm Off

Note: *It defaults to a high alarm while turning to a low alarm after enabling the “Inversion” button.*

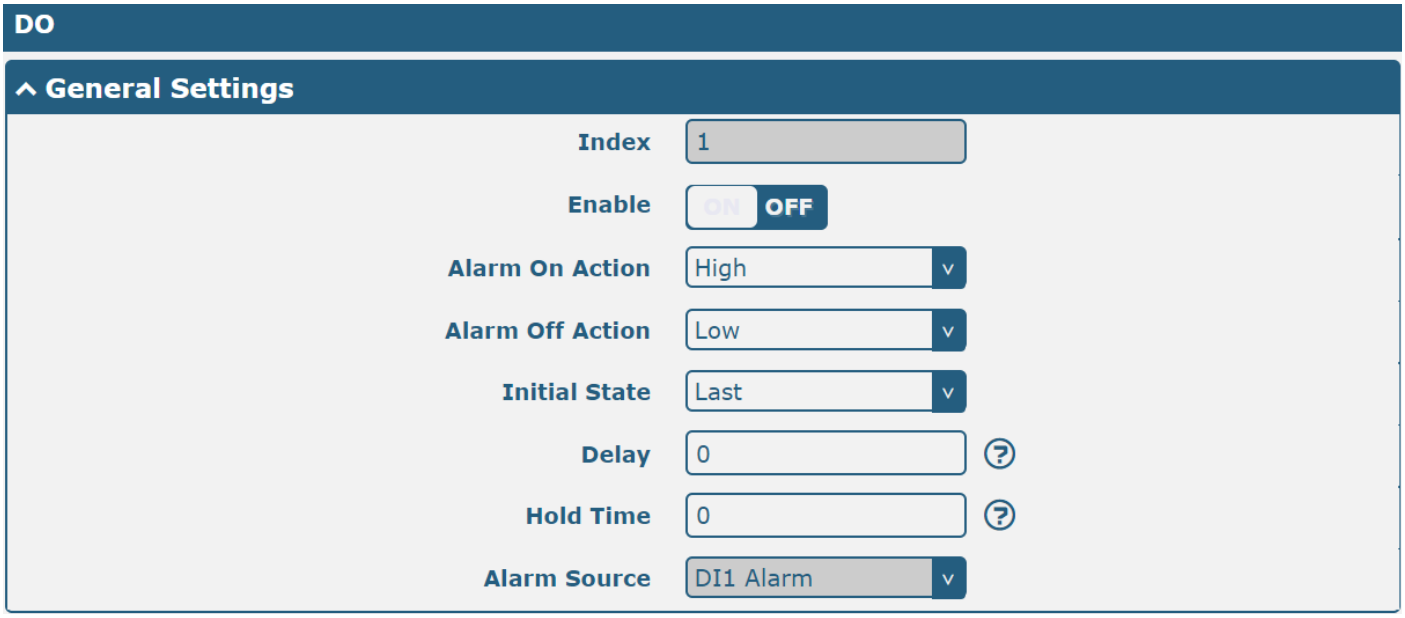
DO



DO Settings

Index	Enable	Alarm On Action	Alarm Off Action	Initial State	Alarm Source
1	false	High	Low	Last	DI1 Alarm

Click to enter the DO index 1, the configuration window is shown below.

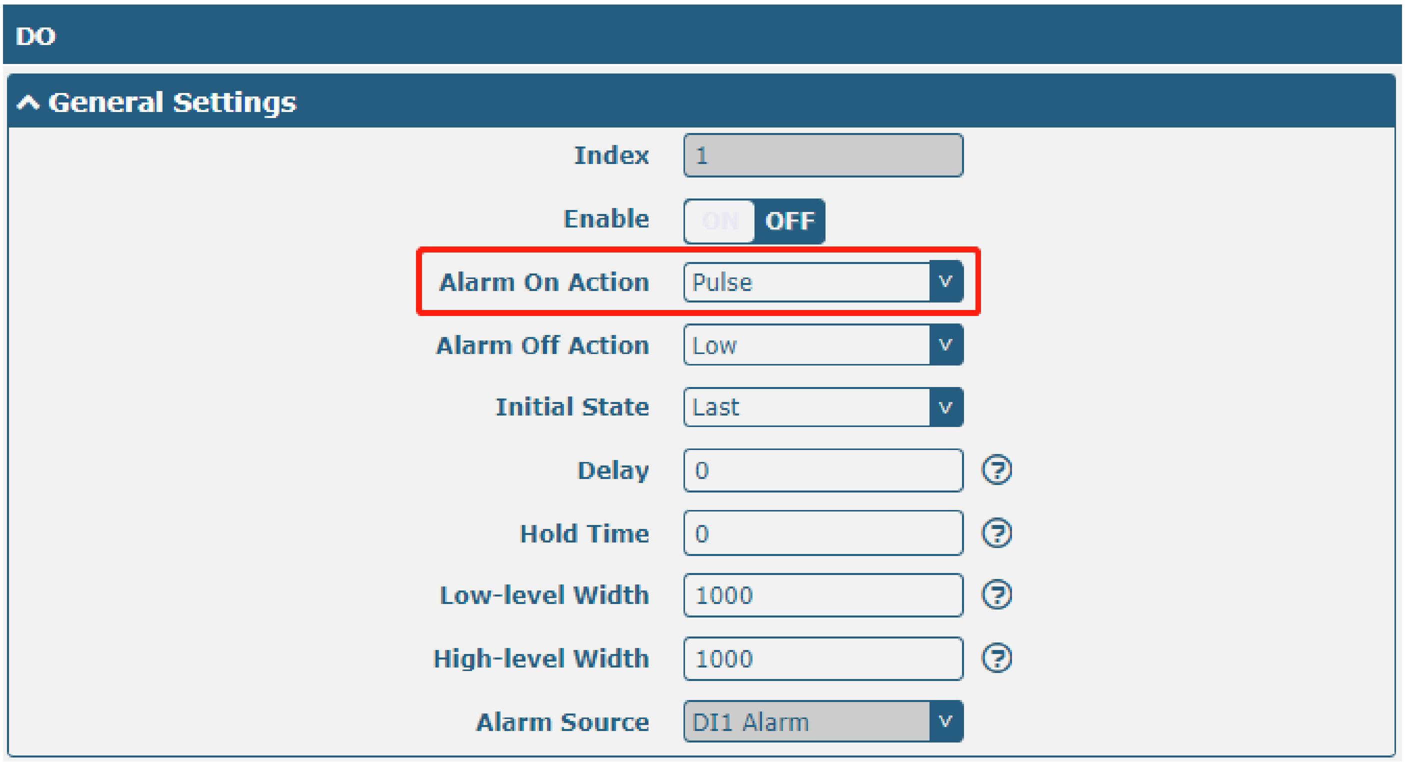


DO

^ General Settings

Index	1
Enable	ON OFF
Alarm On Action	High
Alarm Off Action	Low
Initial State	Last
Delay	0
Hold Time	0
Alarm Source	DI1 Alarm

The window is displayed below when choosing “Pulse” as the alarm on the action.

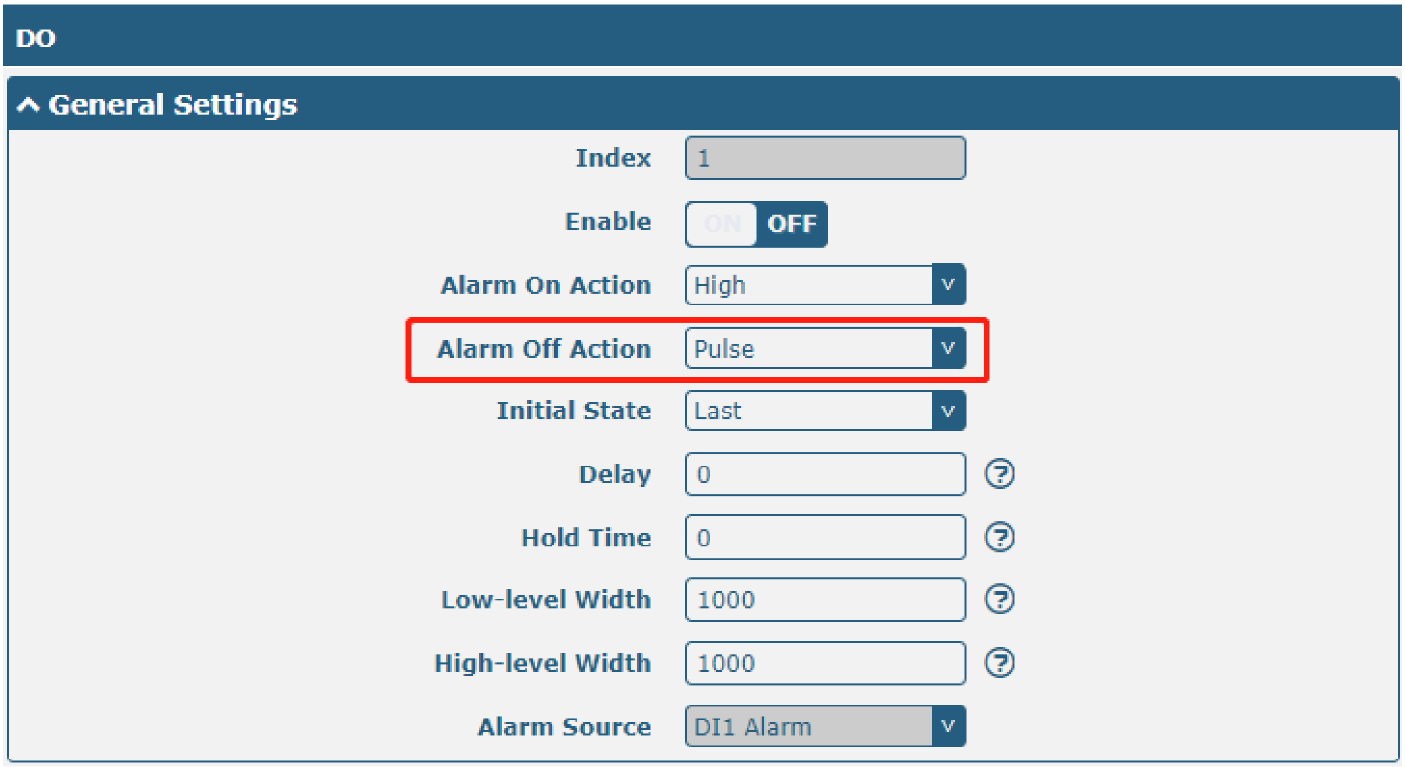


DO

^ General Settings

Index	1
Enable	ON OFF
Alarm On Action	Pulse
Alarm Off Action	Low
Initial State	Last
Delay	0
Hold Time	0
Low-level Width	1000
High-level Width	1000
Alarm Source	DI1 Alarm

The window is displayed below when choosing “Pulse” as the alarm off action.



DO

General Settings

Index: 1

Enable: ON OFF

Alarm On Action: High

Alarm Off Action: Pulse

Initial State: Last

Delay: 0

Hold Time: 0

Low-level Width: 1000

High-level Width: 1000

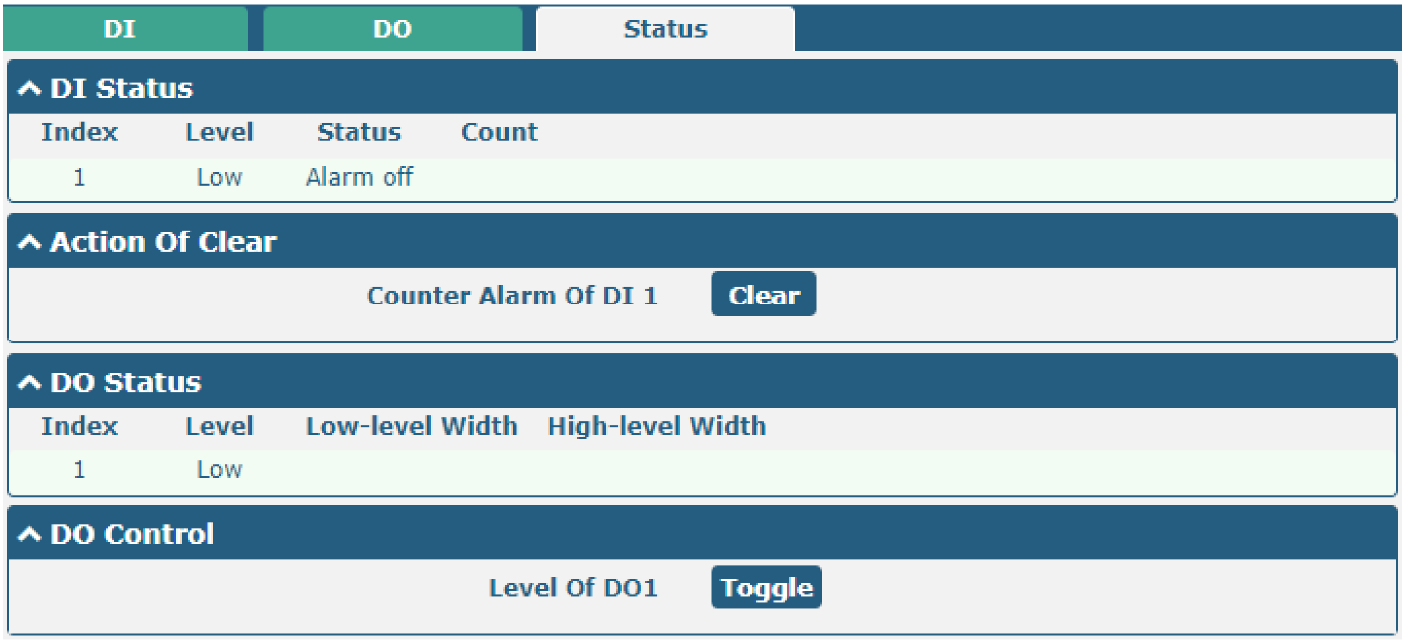
Alarm Source: DI1 Alarm

General Settings @ DO		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Enable	Click the toggle button to enable/disable this DO.	OFF
Alarm On Action	Digital Output initiates when there is an alarm. Selected from “High”, “Low” or “Pulse”. • High: a high electrical level output. • Low: a low electrical level output. • Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.	High
Alarm Off Action	Digital Output initiates when the alarm is removed. Selected from “High”, “Low” or “Pulse”. • High: a high electrical level output. • Low: a low electrical level output. • Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.	Low
Initial State	Specify the Digital Output status when powered on. Selected from “Last”, “High” or “Low”. • Last: DO’s status will consist of the status of the last power off. • High: DO interface is in high electrical level. • Low: DO interface is in low electrical level.	Last
Delay (unit: 100ms)	Set 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 hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reaches this specified time, DO will stop the action. Enter from 0 to 3000 seconds.	0

General Settings @ DO		
Item	**Description**	**Default**
	(0: keep on until the next action)	
Low-level Width (unit: ms)	Set low-level width. It is available when enabling Pulse as "Alarm On Action/Alarm Off Action". In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low-level widths are specified here. Enter from 1000 to 3000.	1000
High-level Width (unit: ms)	Set high-level width. It is available when enabling Pulse as "Alarm On Action/Alarm Off Action". In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high-level widths are specified here. Enter from 1000 to 3000.	1000
Alarm Source	Digital output activation can be activated by this alarm.	None

Status

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



^ DI Status

Index	Level	Status	Count
1	Low	Alarm off	

^ Action Of Clear

^ DO Status

Index	Level	Low-level Width	High-level Width
1	Low		

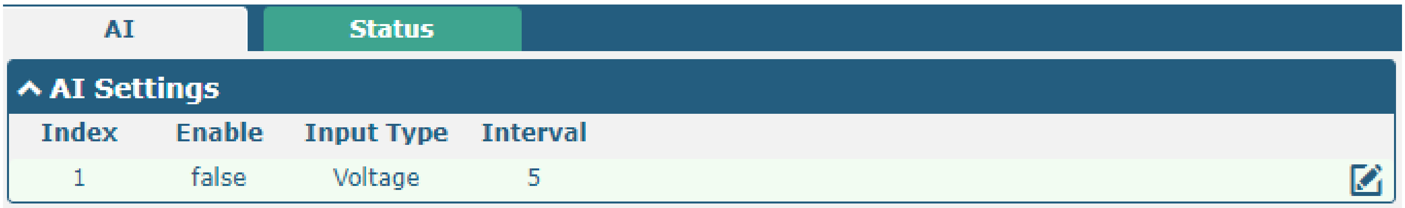
^ DO Control

3.2.9 AI

This section is used to set the parameters of analog input (AI). The analog input is used to collect analog signals within a certain range and is often used to collect continuously changing values such as voltage, current, temperature, and pressure of the sensor. The higher the accuracy of the ADC bits used for analog input, the finer the analog quantization and the more accurate the result.

Note:

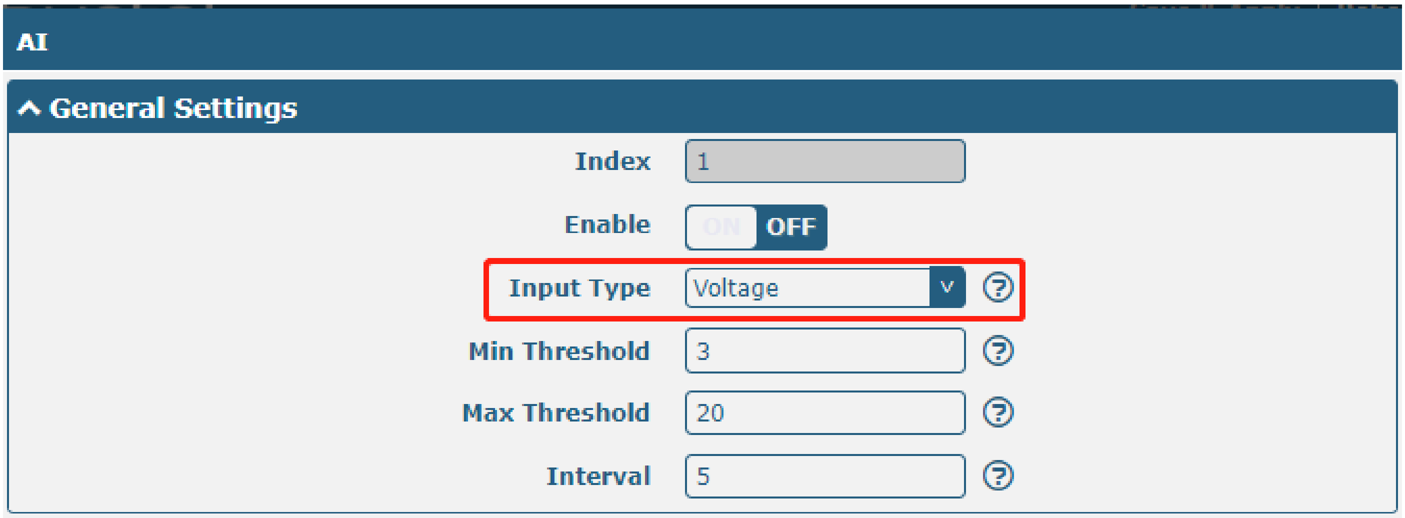
1) R1520 support an AI interface.



AI Settings

Index	Enable	Input Type	Interval
1	false	Voltage	5

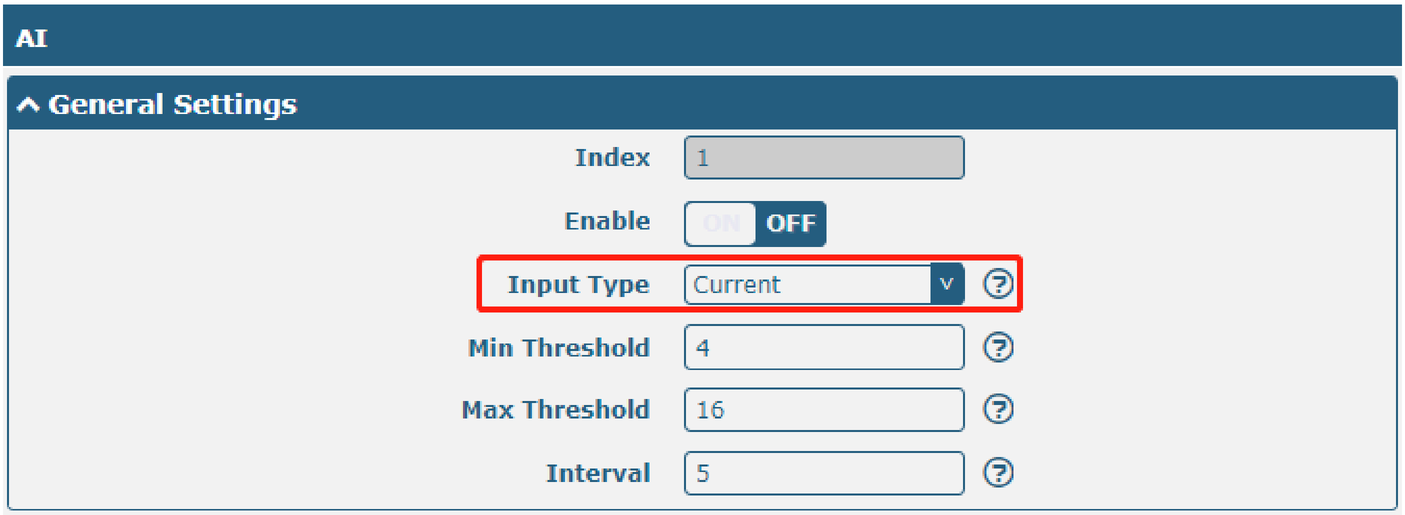
Click the right-most button of DI index 1 as below. The window is displayed as below when the “input type” is “voltage”.



General Settings

Index	1
Enable	ON OFF
Input Type	Voltage
Min Threshold	3
Max Threshold	20
Interval	5

The window is displayed below when the “input type” is “Current”.



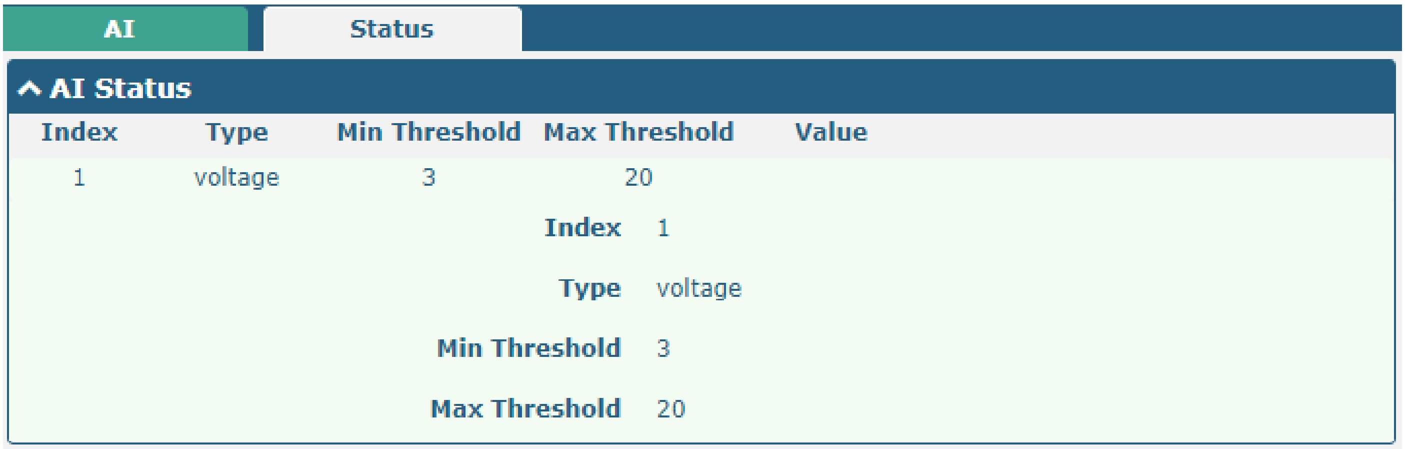
General Settings

Index	1
Enable	ON OFF
Input Type	Current
Min Threshold	4
Max Threshold	16
Interval	5

AI (Analog Input)		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Enable	Click the switch button to "ON" to turn on the analog input function.	OFF
Input type	Select from "Voltage" or "Current". • Voltage: The data collected is voltage. • Current: The data collected is Current.	Voltage
Min Threshold @Voltage	Set minimum voltage threshold. When the voltage collected by the AI interface is less than the minimum voltage threshold, an event notification will be triggered. Unit: V.	3
Max Threshold @Voltage	Set maximum voltage threshold. When the voltage collected by the AI interface is greater than the minimum voltage threshold, an event notification will be triggered. Unit: V.	20
Min Threshold @Current	Set minimum current threshold. When the current collected by the AI interface is less than the minimum voltage threshold, an event notification will be triggered. Unit: mA.	4
Min Threshold @Current	Set maximum current threshold. When the current collected by the AI interface is greater than the minimum voltage threshold, an event notification will be triggered. Unit: mA.	16
Interval	Collect latest data every few seconds.	5

Status

Click the "Status" column to view the status of the AI.



Index	Type	Min Threshold	Max Threshold	Value
1	voltage	3	20	

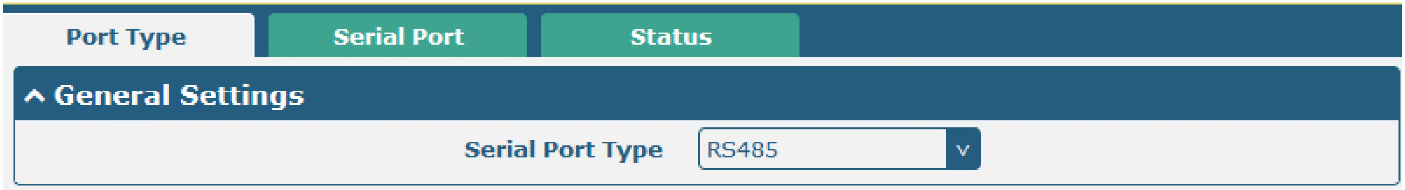
Index	1
Type	voltage
Min Threshold	3
Max Threshold	20

3.2.10Serial Port

This section allows you to set the serial port parameters. The device might support two serial ports, COM1 and COM2, which can be configured as two COM1 or two COM2 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 a wired or wireless network, to realize the function of transparent data transmission.

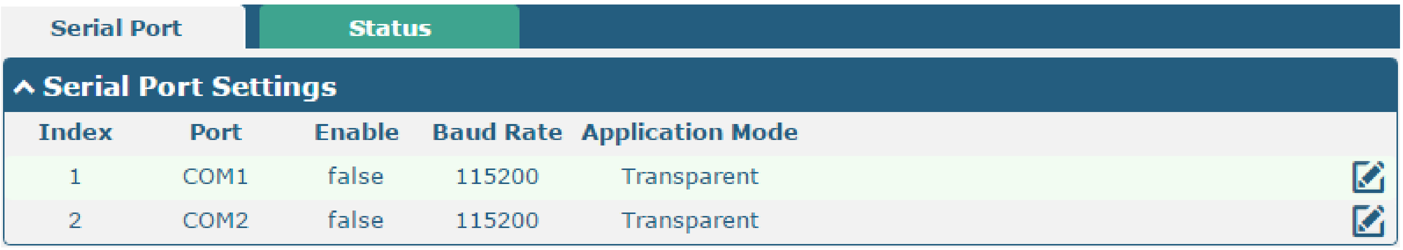
Note:

1) The serial port of R2010 and R3000-Quad can be configured as RS232 or RS485.



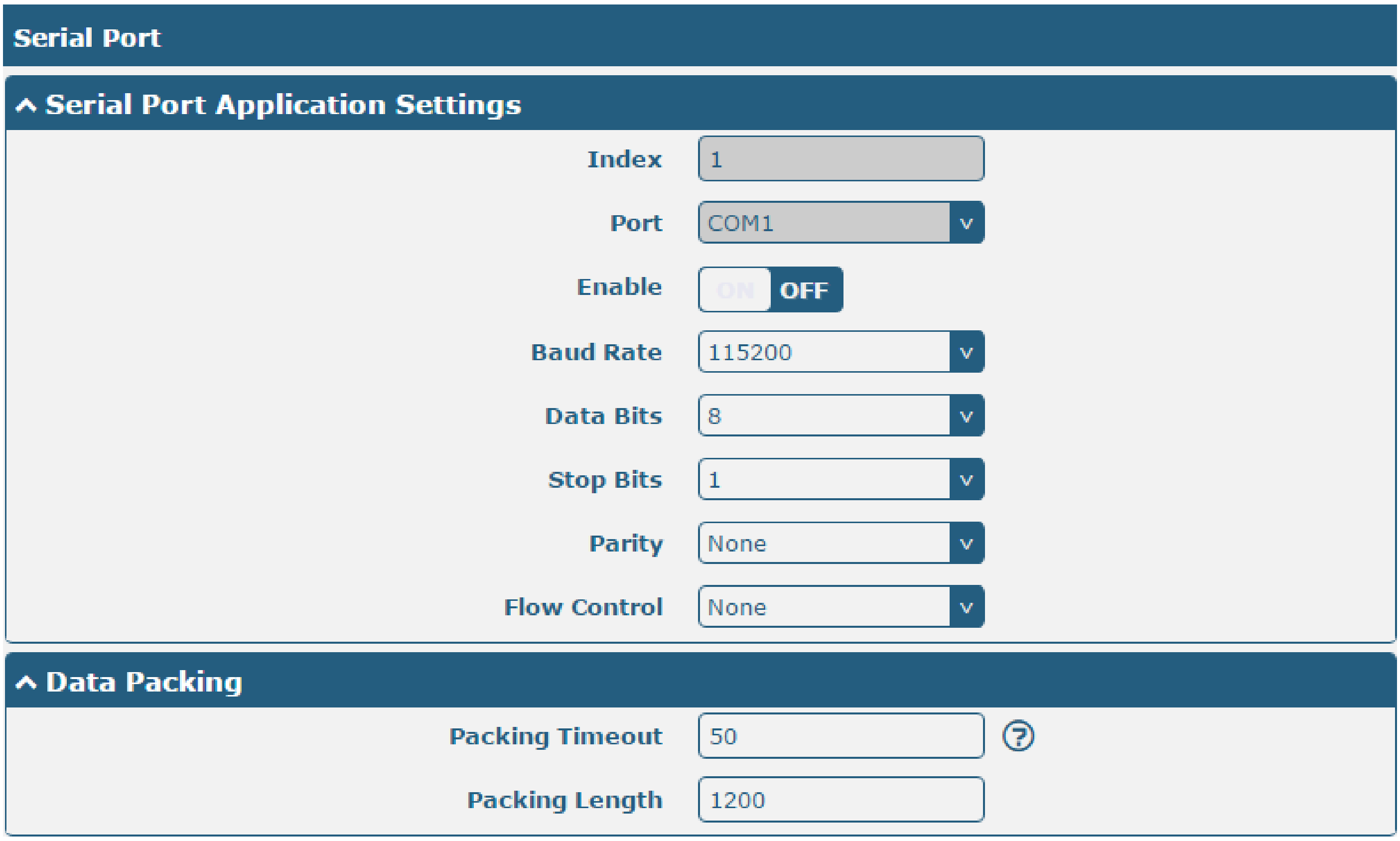
Serial Port Type: RS485

Serial Port		
Item	**Descriptions**	**Default**
Serial Port Type	Support RS485 or RS232	RS485



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

Click the right-most ✎ button of COM1 as below.



Index: 1

Port: COM1

Enable: ON OFF

Baud Rate: 115200

Data Bits: 8

Stop Bits: 1

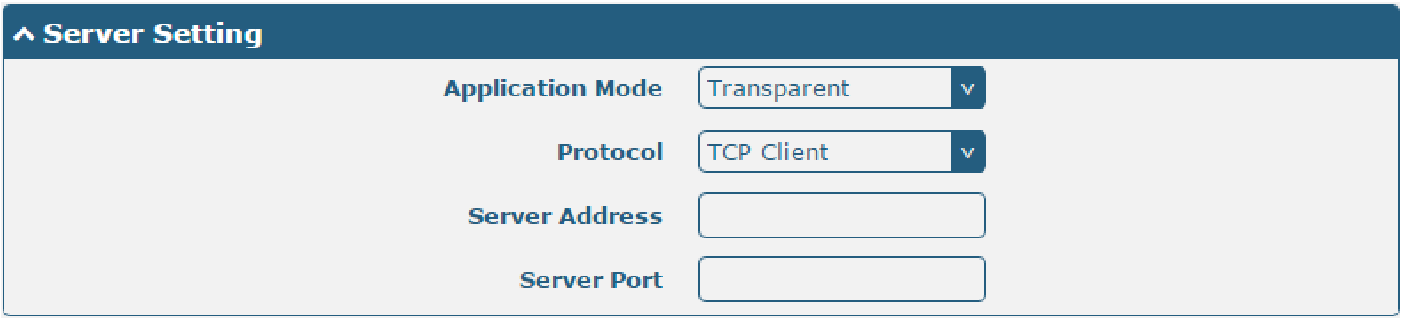
Parity: None

Flow Control: None

Packing Timeout: 50

Packing Length: 1200

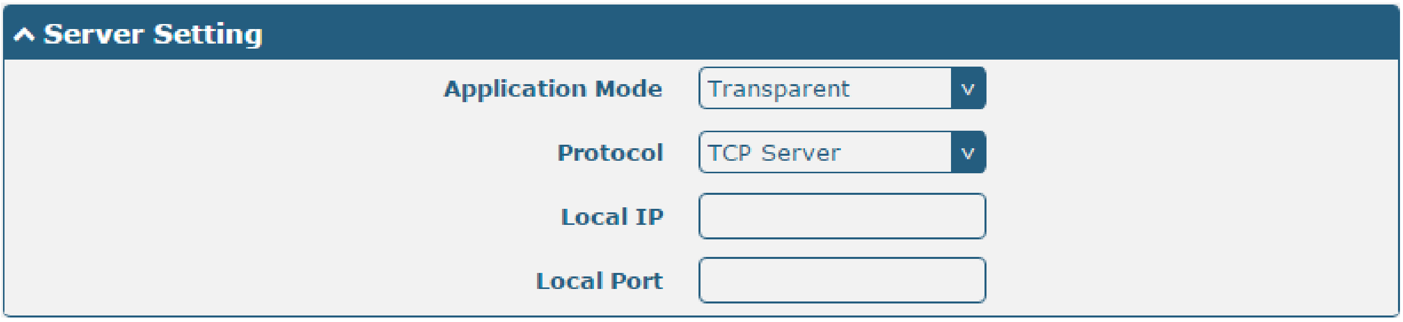
In "Server Setting" column, when "Transparent” is selected as the application mode and "TCP Client" as the protocol, the window is as follows:



^ Server Setting

Application Mode	Transparent
Protocol	TCP Client
Server Address	
Server Port	

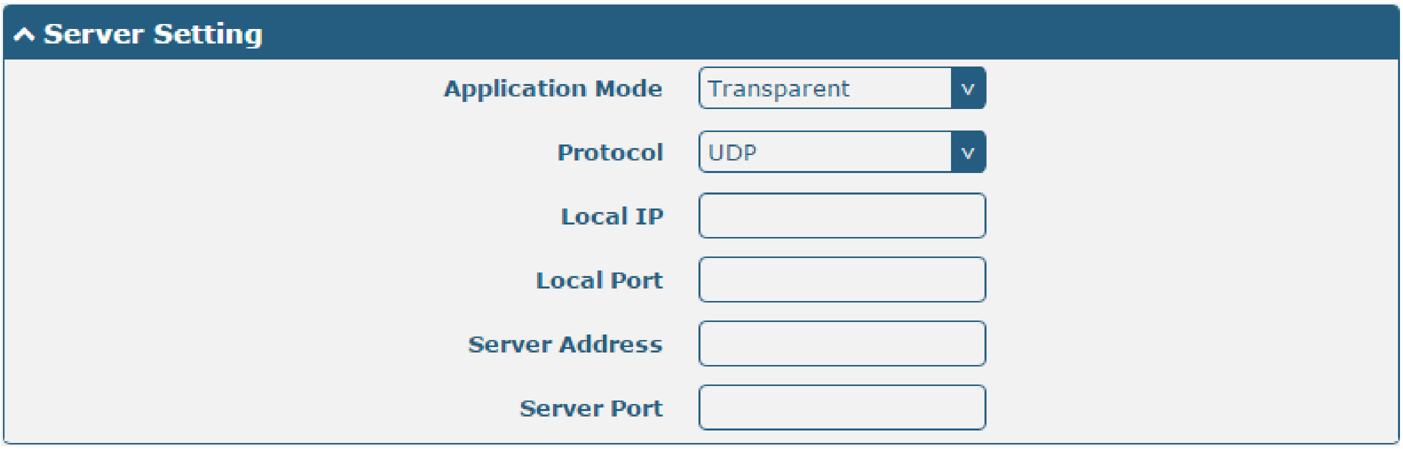
When "Transparent” is selected as the application mode and "TCP Server" as the protocol, the window is as follows:



^ Server Setting

Application Mode	Transparent
Protocol	TCP Server
Local IP	
Local Port	

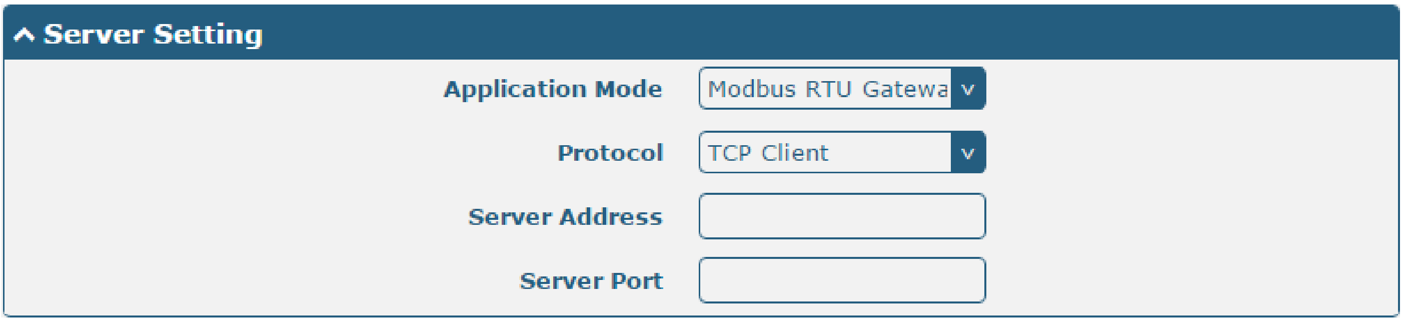
When "Transparent” is selected as the application mode and "UDP" is used as the protocol, the window is as follows:



^ Server Setting

Application Mode	Transparent
Protocol	UDP
Local IP	
Local Port	
Server Address	
Server Port	

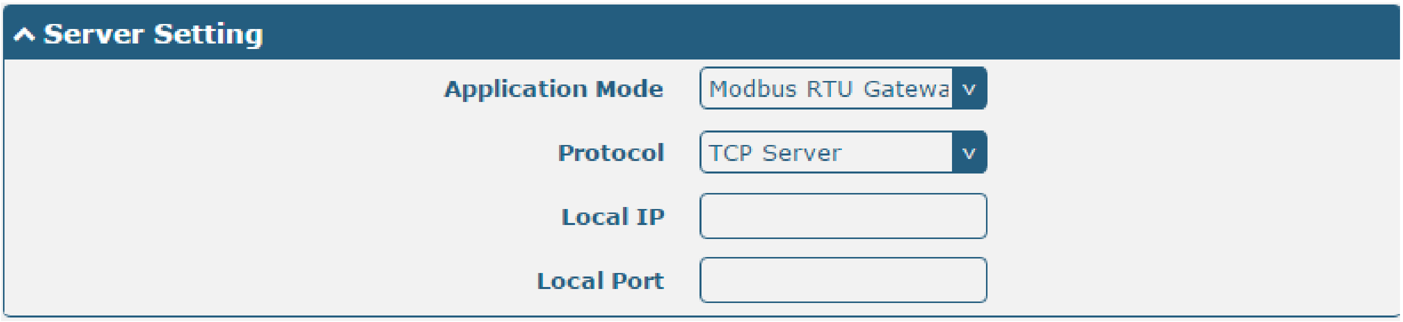
When “Modbus RTU Gateway” is selected as the application mode and “TCP Client” as the protocol, the window is as follows:



^ Server Setting

Application Mode	Modbus RTU Gatewa
Protocol	TCP Client
Server Address	
Server Port	

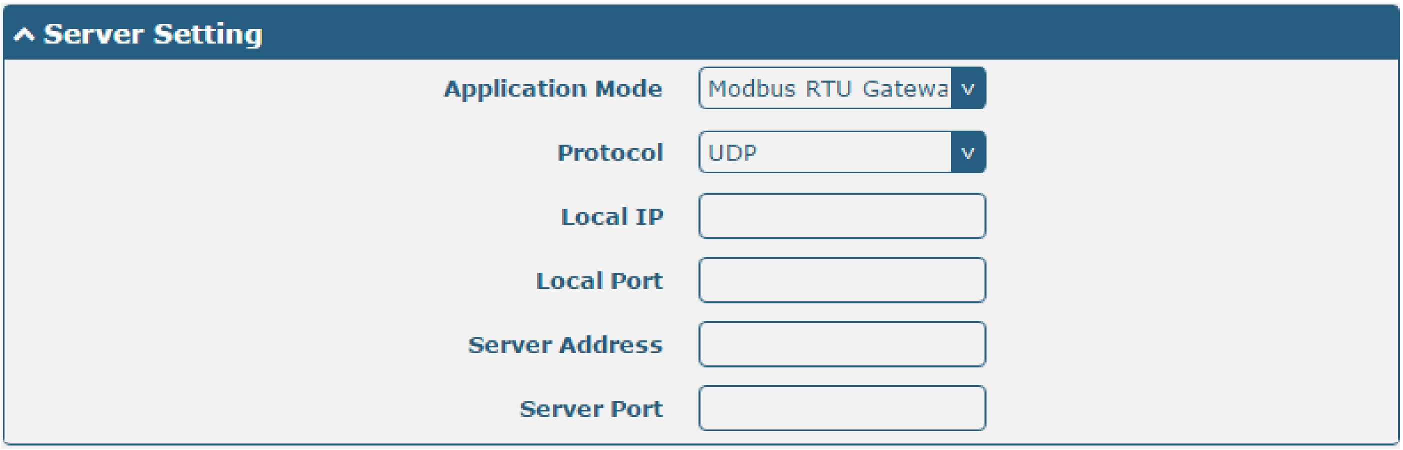
When "Modbus RTU Gateway" is selected as the application mode and "TCP Server" as the protocol, the window is as follows:



^ Server Setting

Application Mode	Modbus RTU Gatewa
Protocol	TCP Server
Local IP	
Local Port	

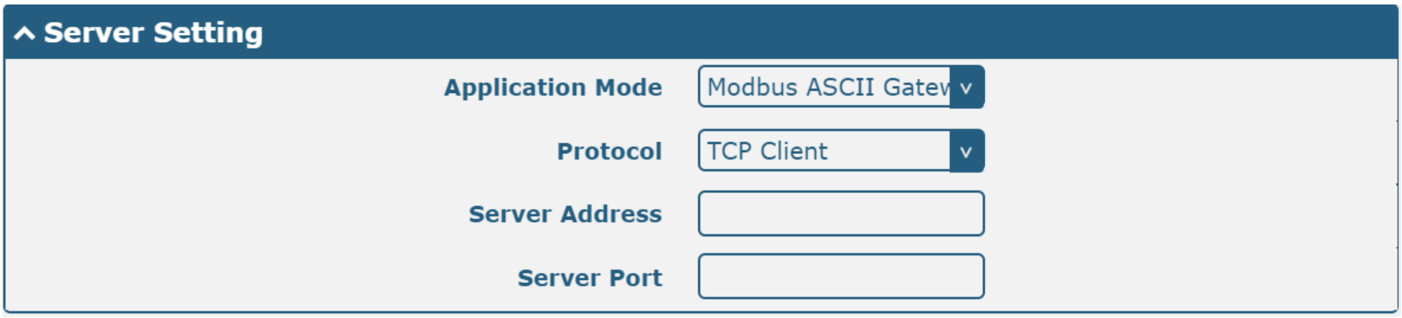
When selecting "Modbus RTU Gateway" as the application mode and "UDP" as the protocol, the window is as follows:



^ Server Setting

Application Mode	Modbus RTU Gatewa
Protocol	UDP
Local IP	
Local Port	
Server Address	
Server Port	

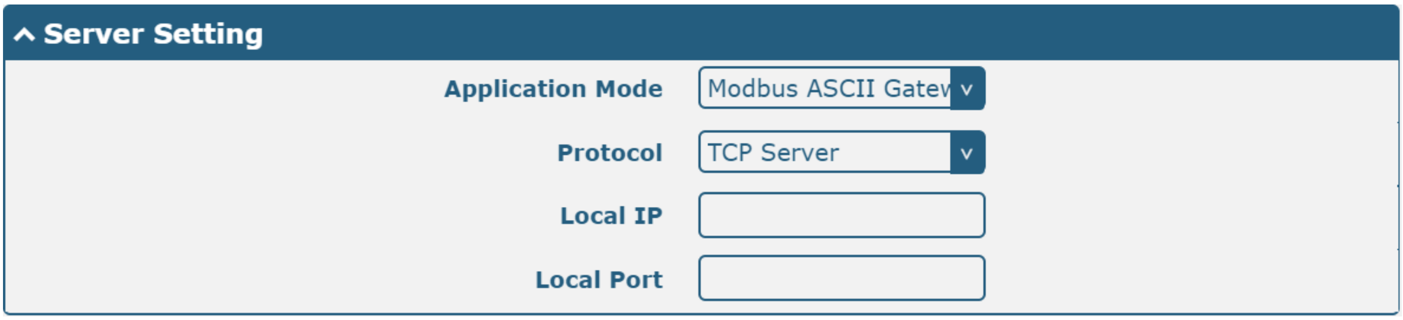
When “Modbus ASCII Gateway” is selected as the application mode and “TCP Client” as the protocol, the window is as follows:



^ Server Setting

Application Mode	Modbus ASCII Gatev
Protocol	TCP Client
Server Address	
Server Port	

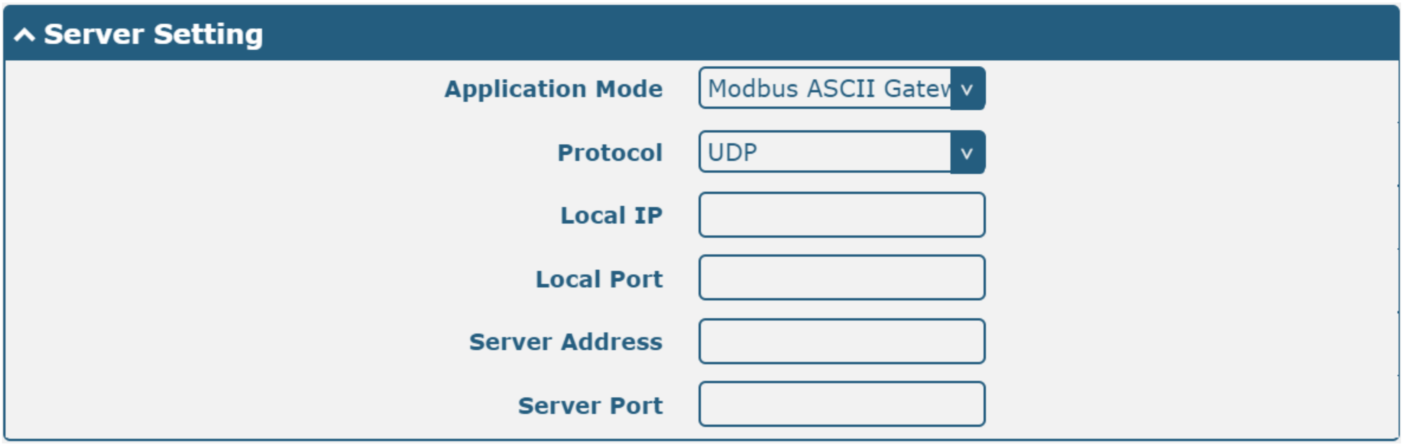
When selecting "Modbus ASCII Gateway" as the application mode and "TCP Server" as the protocol, the window is as follows:



^ Server Setting

Application Mode	Modbus ASCII Gatev
Protocol	TCP Server
Local IP	
Local Port	

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



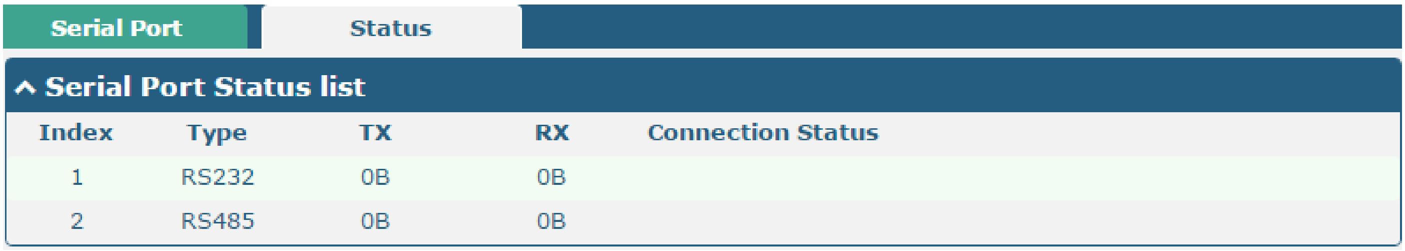
^ Server Setting

Application Mode: Modbus ASCII Gatev v
Protocol: UDP v
Local IP
Local Port
Server Address
Server Port

Serial Port		
Item	**Description**	**Default**
Serial Port Application Settings		
Index	Indicate ordinal of list.	--
Port	Show current serial's name, read-only.	COM1
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
Data Packing		
Packing Timeout	Set packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN/ WLAN 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 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 soon it reaches the specified length.	1200
Server Settings		
Item	**Description**	**Default**
Application Mode	Select from "Transparent", "Modbus RTU Gateway", or "Modbus ASCII Gateway". • Transparent: The device will transmit the serial data transparently. • Modbus RTU Gateway: The device will translate the Modbus RTU data to Modbus TCP data and send it out, and vice versa. • Modbus ASCII Gateway: The device will translate the Modbus ASCII data to Modbus TCP data and send it out, and vice versa.	Transparent

Serial Port		
Item	**Description**	**Default**
Protocol	Select from "TCP Client", "TCP Server", or "UDP". • TCP Client: Device works as TCP client, initiates TCP connection to TCP server. The server address supports both IP and domain name. • TCP Server: Device works as a TCP server, listening for a connection request from a TCP client. • UDP: Device works as UDP client.	TCP Client
Server Address	Enter address of the server which will receive the data sent from the device's serial port. IP address or domain name will be available.	Null
Server Port	Enter a specified port of the 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 the device.	Null
Local Port @ Transparent	Enter port of the device's LAN IP.	Null
Local IP @ Modbus	Enter local IP under Modbus mode.	Null
Local Port @ Modbus	Enter local port under Modbus mode.	Null

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



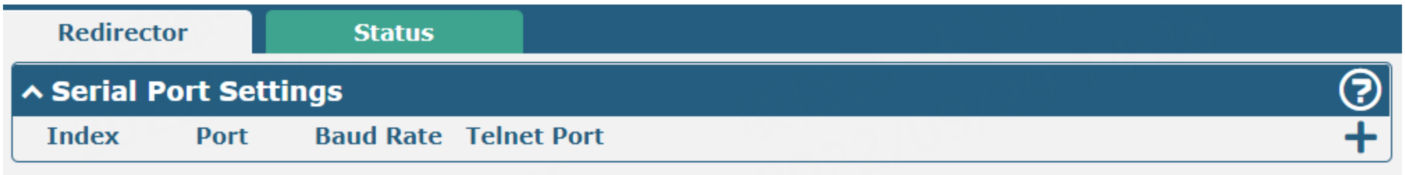
Serial Port Status list

Index	Type	TX	RX	Connection Status
1	RS232	0B	0B	
2	RS485	0B	0B	

Status	
Item	**Descriptions**
TX	Send Data to Serial Port.
RX	Received Data from Serial Port.

3.2.11 Serial Redirector

This section allows you to redirect the Serial Port to Telnet. It is only for the R1520.

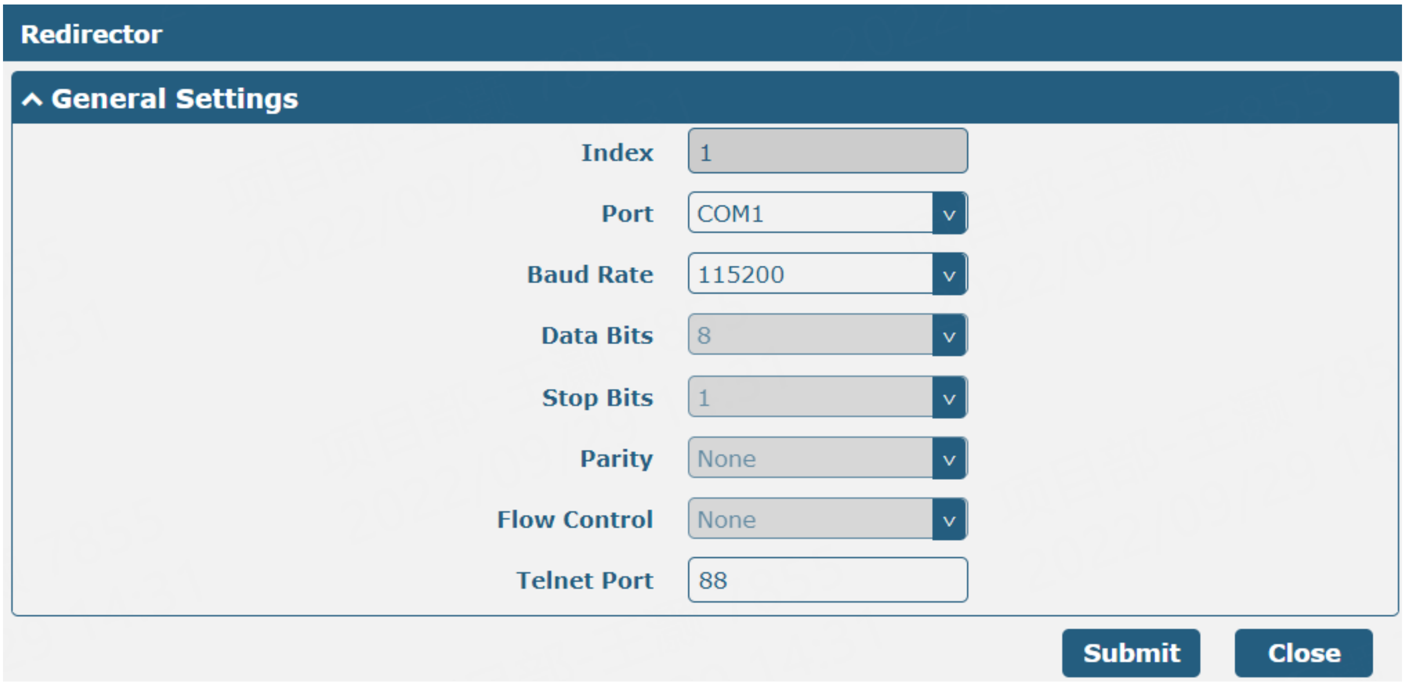


Serial Port Settings

Index	Port	Baud Rate	Telnet Port

Click “Redirector” column to configure the Serial Redirector.

Click + to select serial port and baud rate correspond the device of serial port had connected, then input the correct Telnet port you expect to redirect.

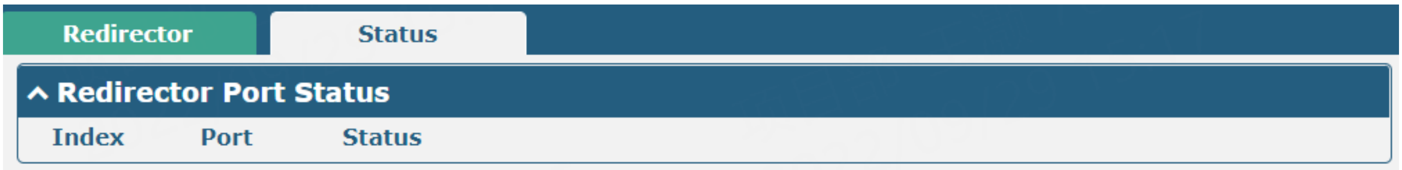


Redirector

General Settings

Index	1
Port	COM1
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Telnet Port	88

Click the "Status" column to view redirection status.



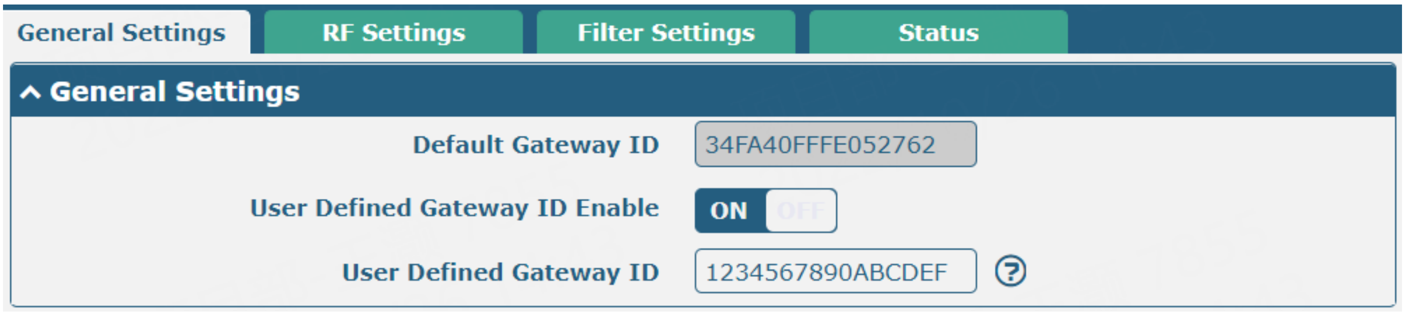
Redirector Port Status

Index	Port	Status

3.2.12 LoRa

This section allows you to set the LoRaWAN parameters. It is only for the R3000-LG.

Click "General Settings" to configure the Gateway ID. Here is an example below.



^ General Settings

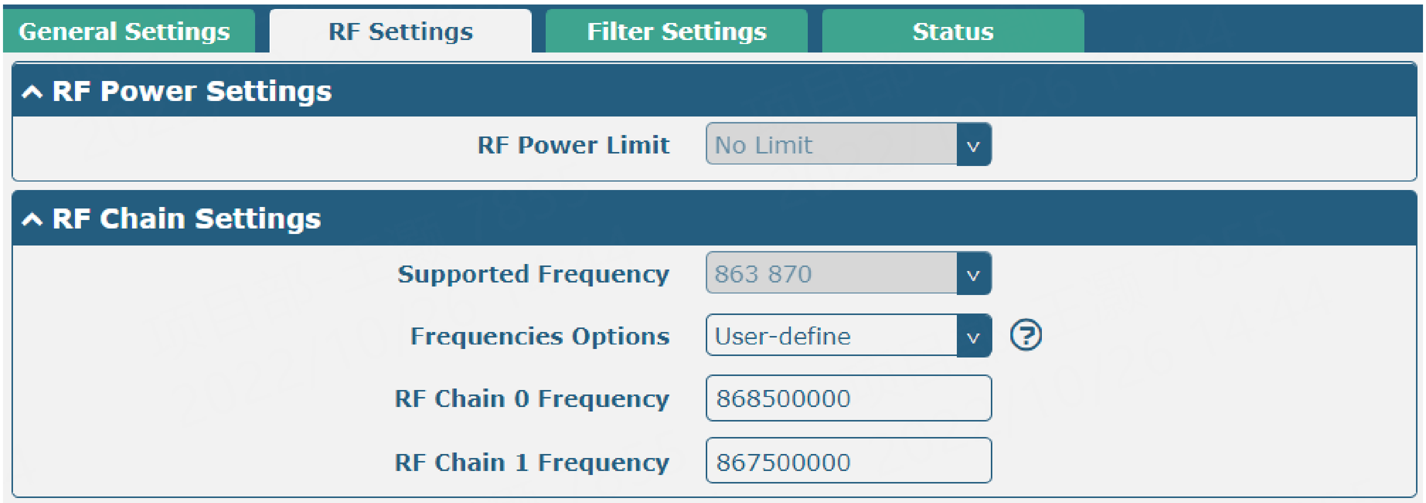
Default Gateway ID: 34FA40FFFE052762

User Defined Gateway ID Enable: ON | OFF

User Defined Gateway ID: 1234567890ABCDEF ?

General Settings		
Item	**Description**	**Default**
Default Gateway ID	Set default gateway ID, or you could define the Gateway ID with a unique 64-bit sequence by yourself.	Null
User Defined Gateway ID Enable	Click the toggle button to enable/disable this option.	OFF
User Defined Gateway ID	Enter Gateway ID.	Null

RF Settings



^ RF Power Settings

RF Power Limit: No Limit

^ RF Chain Settings

Supported Frequency: 863 870

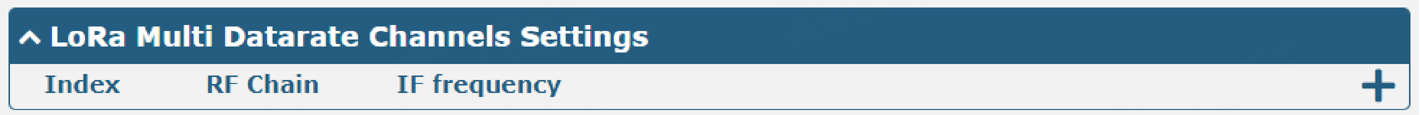
Frequencies Options: User-define ?

RF Chain 0 Frequency: 868500000

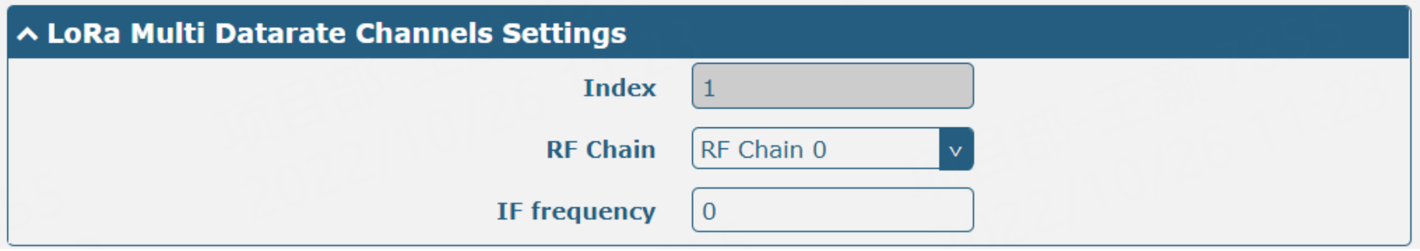
RF Chain 1 Frequency: 867500000

RF Settings		
Item	**Description**	**Default**
RF Power Settings		
RF Power Limit	Display RF power limit.	No Limit

RF Settings		
Item	**Description**	**Default**
RF Power Settings		
RF Chain Settings		
Support Frequency	Display support frequency.	863 870
Frequencies Options	Set link frequency. EU868: 868.1,868.3,868.5,867.1,867.3,867.5,867.7,867.9, STD 868.3 and FSK 868.8; RU868: RF Chain 0:869000000,RF Chain 1:864500000, 868.9,869.1,869.3,864.1,864.3,864.5,864.7,864.9; KZ868: RF Chain 0:865300000,RF Chain 1:867500000, 865.1,865.3,865.5,867.1,867.3,867.5,867.7,867.9.	User-define
RF Chain 0 Frequency	Set frequency of RF link 0.	868500000
RF Chain 1 Frequency	Set frequency of RF link 1.	867500000



Click + to Add LoRa Multi Datarate Channels Settings.

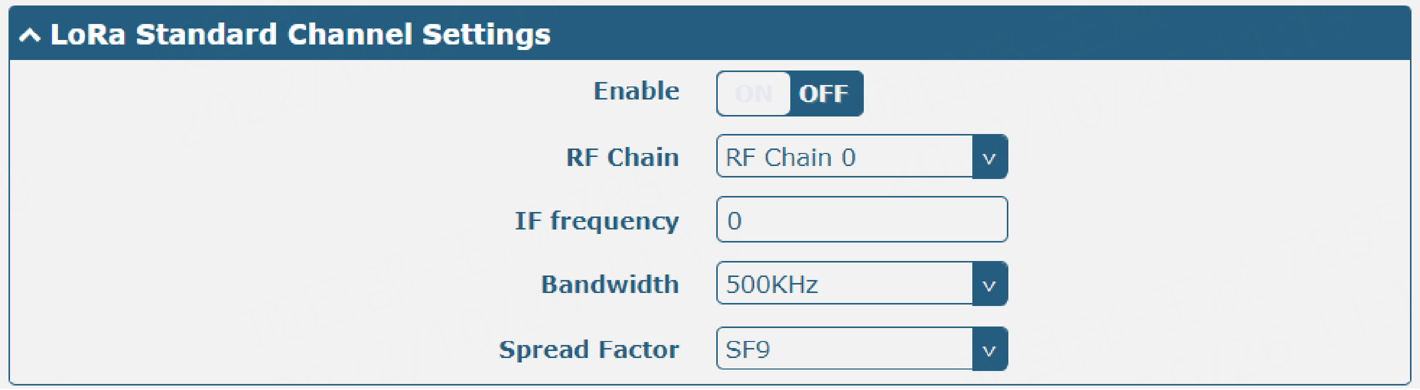

^ LoRa Multi Datarate Channels Settings

Index: 1

RF Chain: RF Chain 0

IF frequency: 0

LoRa Multi Datarate Channels Settings@RF Settings		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	1
RF Chain	Select RF Chain.	RF Chain 0
IF frequency	Enter center frequency in the range -500000-500000 in Hz. The offset between the center frequency of a particular channel and the center frequency of RF link 0/1.	0



^ LoRa Standard Channel Settings

Enable: ON OFF

RF Chain: RF Chain 0

IF frequency: 0

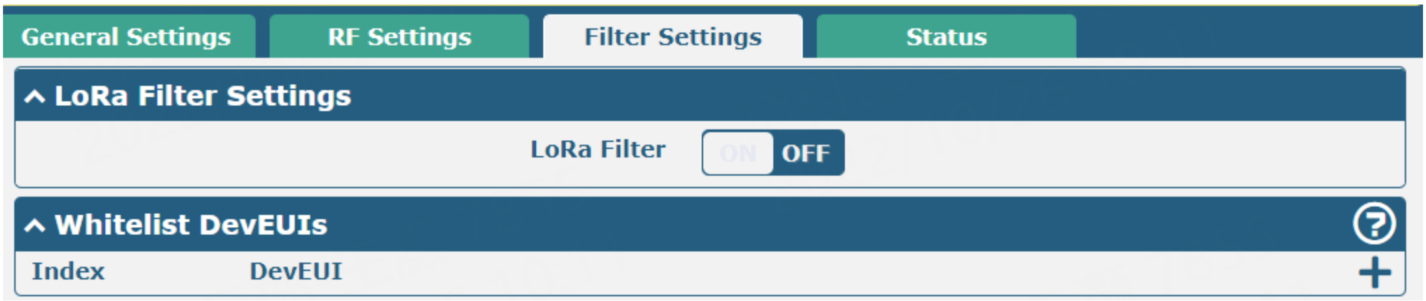
Bandwidth: 500KHz

Spread Factor: SF9

LoRa Standard Channel Settings@RF Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Select RF Chain.	RF Chain 0
IF frequency	Enter center frequency in the range -500000-500000 in Hz. The offset between the center frequency of a particular channel and the center frequency of RF link 0/1.	0
Bandwidth	Select optional bandwidth in KHz.	500KHz
Spread Factor	Enter an optional spreading factor. A high spreading factor corresponds to a low rate, and a low spreading factor corresponds to a high rate.	SF9

Filter Settings

This section is used to modify LoRa filter settings.



^ LoRa Filter Settings

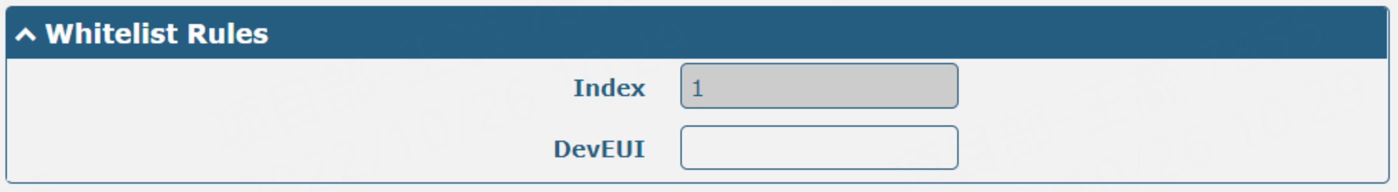
LoRa Filter: ON OFF

^ Whitelist DevEUIs

Index	DevEUI

Filter Settings		
Item	**Description**	**Default**
LoRa Filter	Click the toggle button to enable/disable this option.	OFF

Click + to add a whitelist rule.



^ Whitelist Rules

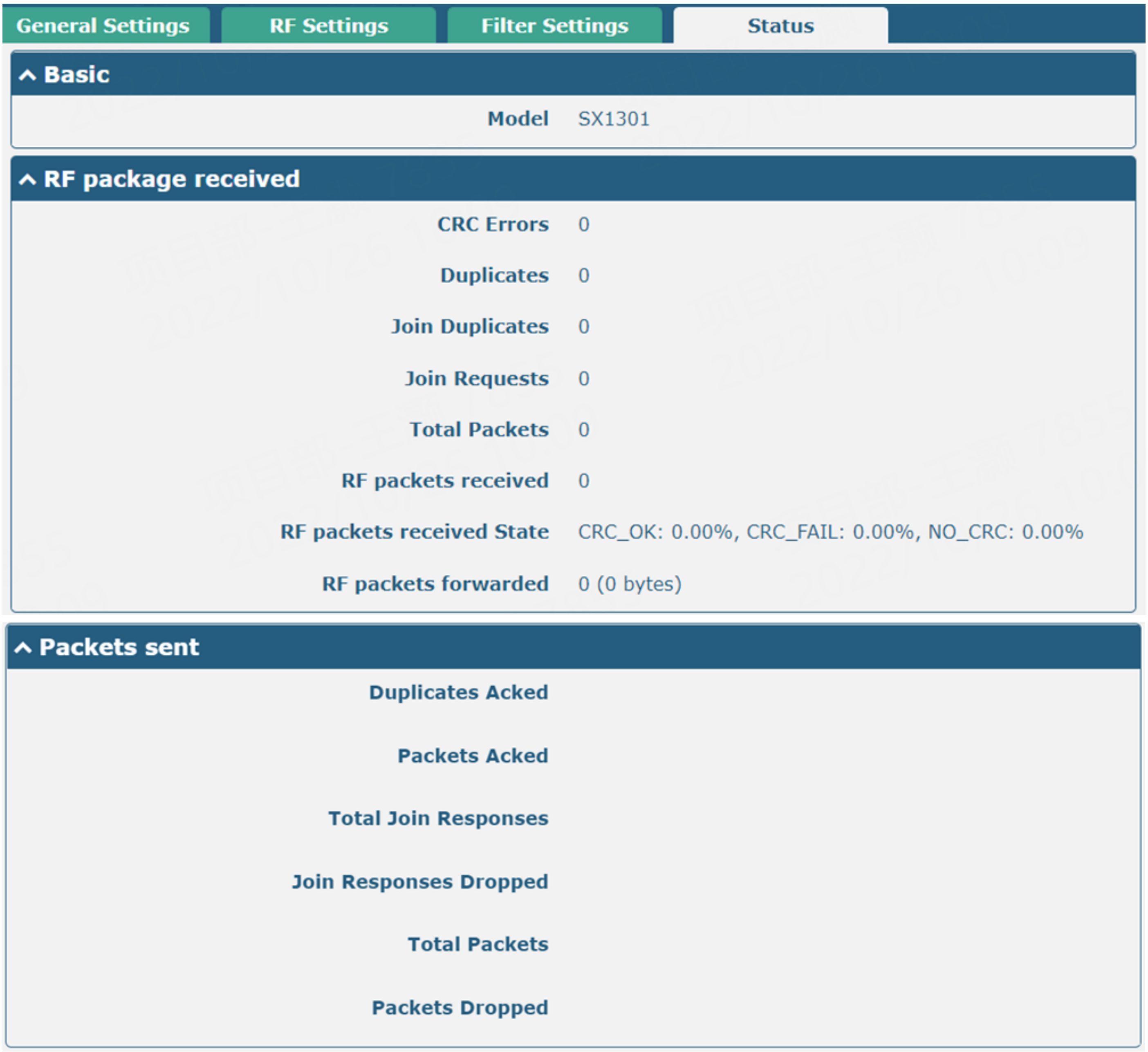
Index: 1

DevEUI:

Whitelist Rules@Filter Settings		
Item	**Description**	**Default**
Index	Display table number.	1
DevEUI	Enter DevEUI for device.	Null

Status

This section allows you to check the status of LoRa interface.



^ Basic

Model SX1301

^ RF package received

CRC Errors 0

Duplicates 0

Join Duplicates 0

Join Requests 0

Total Packets 0

RF packets received 0

RF packets received State CRC_OK: 0.00%, CRC_FAIL: 0.00%, NO_CRC: 0.00%

RF packets forwarded 0 (0 bytes)

^ Packets sent

Duplicates Acked

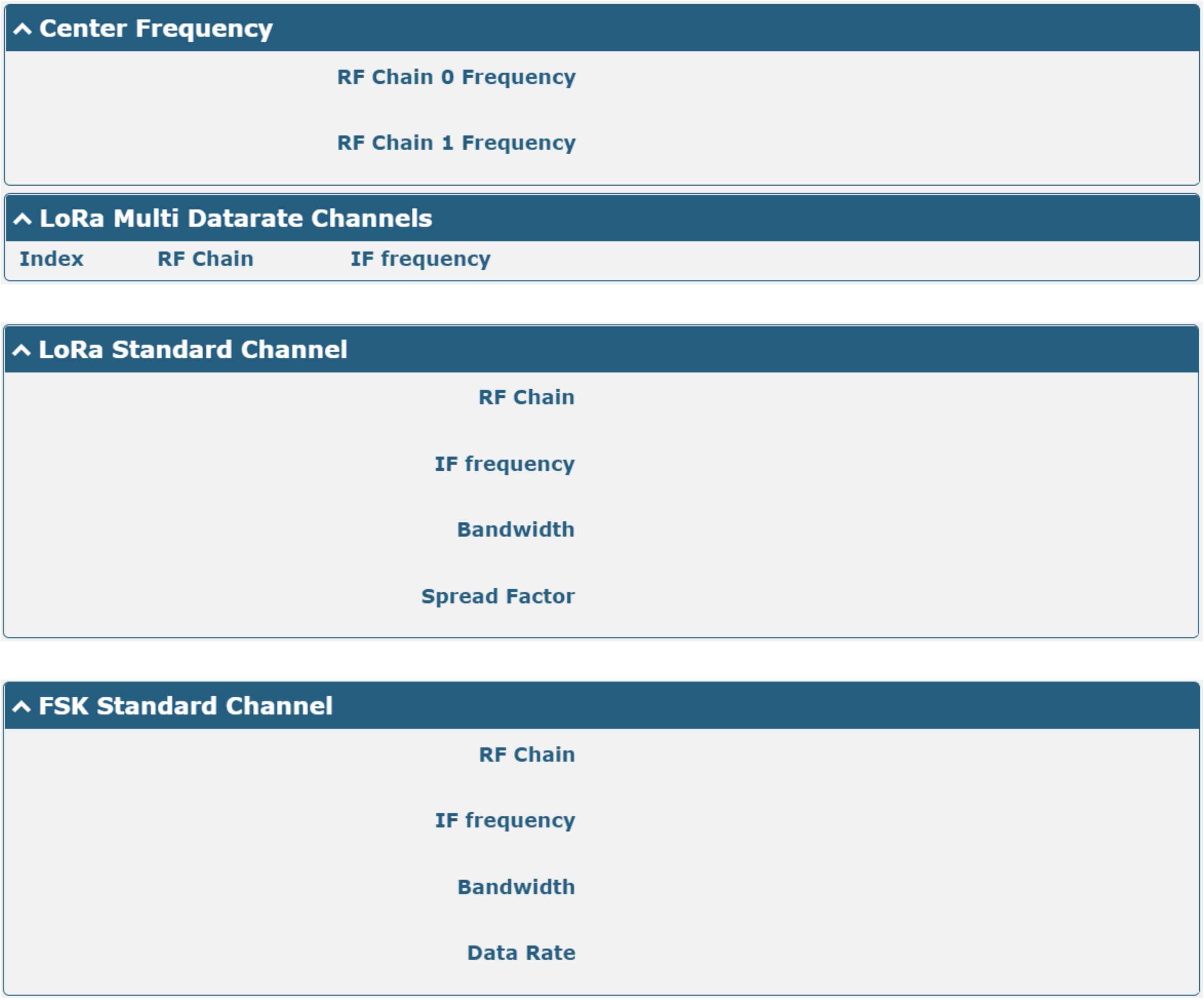
Packets Acked

Total Join Responses

Join Responses Dropped

Total Packets

Packets Dropped



^ Center Frequency

RF Chain 0 Frequency

RF Chain 1 Frequency

^ LoRa Multi Datarate Channels

Index	RF Chain	IF frequency

^ LoRa Standard Channel

RF Chain

IF frequency

Bandwidth

Spread Factor

^ FSK Standard Channel

RF Chain

IF frequency

Bandwidth

Data Rate

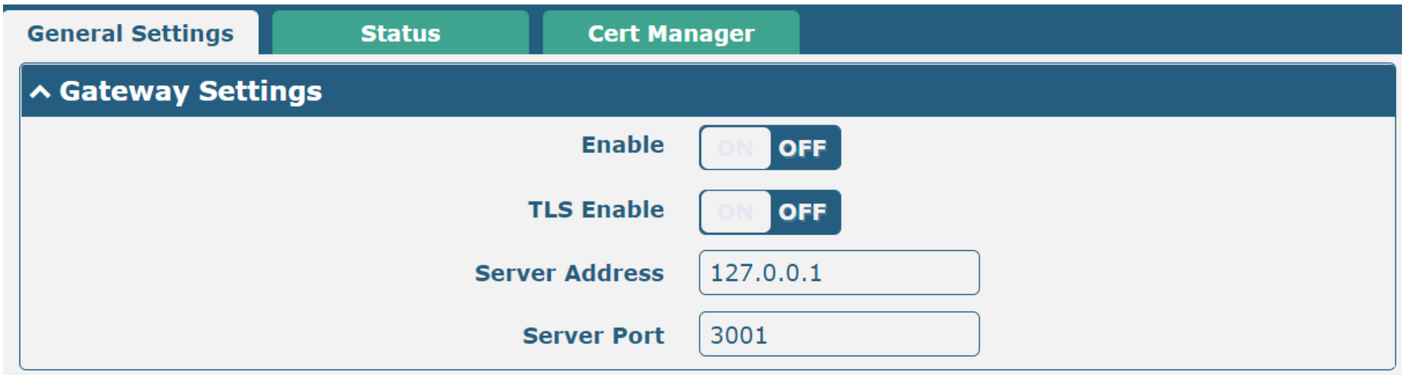
Status	
Item	**Description**
Basic	
Model	Show LoRa module model.
Packets received	
CRC Errors	Show the value of RF packets received in error.
Duplicates	Show the value of duplicate RF packets received.
Join Duplicates	Show the value of duplicate RF join request packets received.
Join Requests	Show the value of RF join request packets received.
Total Packets	Show the value of RF packets received.
RF Packets Received	Show count of data packets from node to gateway.
RF Packets Received State	Show the RF packets receiving state. • CRC_OK: Percentage of CRC verification • CRC_Fail: Percentage of CRC verification failure • NO_CRC: Percentage of abnormal packets without CRC
Packets sent	

Status	
Item	**Description**
Duplicates Asked	Show the value of duplicate RF response packets sent.
Packets Asked	Show the value of RF response packets sent.
Total Join Responses	Show the value of duplicate RF join response packets sent.
Join Responses Dropped	Show the value of failed RF join response packets.
Total Packets	Show the value of RF packets sent.
Packets Dropped	Show the value of RF dropped packets.
Center Frequency	
RF Chain 0 Frequency	Center frequency of LoRa channel 0.
RF Chain 1 Frequency	Center frequency of LoRa channel 1.
LoRa Multi Datarate Channels	
RF Chain	Index of LoRa channel.
IF Frequency	IF frequency of LoRa channel.
LoRa standard Channel	
RF Chain	Index of LoRa standard channel.
IF frequency	IF frequency of LoRa standard channel.
Bandwidth	Bandwidth of LoRa standard channel.
Spread Factor	Spread Factor of LoRa standard channel.
FSK Standard Channel	
RF Chain	Index of FSK Standard Channel.
IF frequency	IF frequency of FSK Standard Channel.
Bandwidth	Bandwidth of FSK Standard Channel.
Data Rate	Data Rate of FSK Standard Channel.

3.3 Packet Forwarders

3.3.1 Basic Station

General Settings



Enable ON OFF

TLS Enable ON OFF

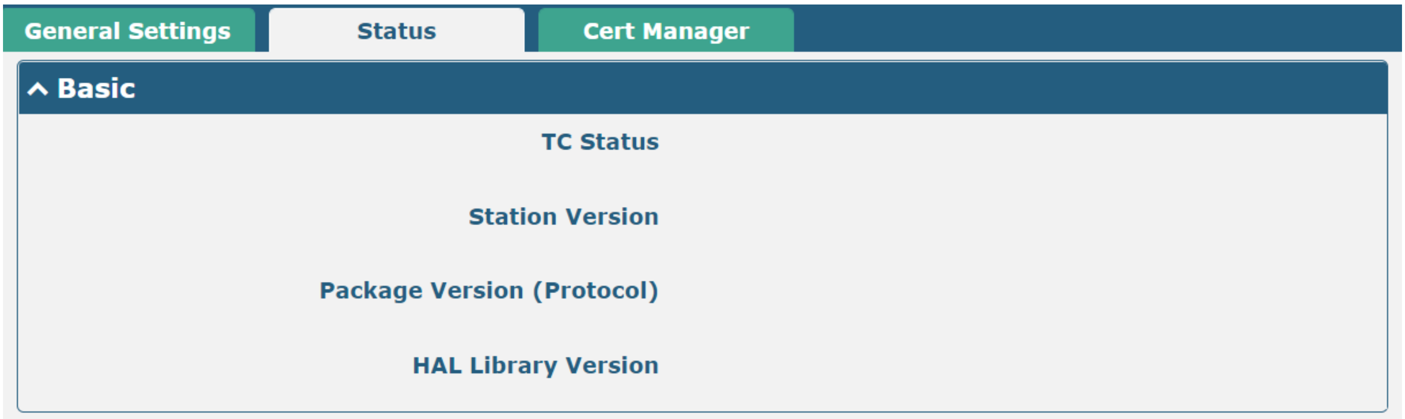
Server Address 127.0.0.1

Server Port 3001

General Settings		
Gateway Settings		
Item	Description	Default
Enable	Enable application.	OFF
TLS Enable	Enable TLS encrypted transmission.	OFF
Server Address	Server address (e.g., 127.0.0.1)	
Server Port	Server port number.	

Status

This section allows you to view the status of the basic station.

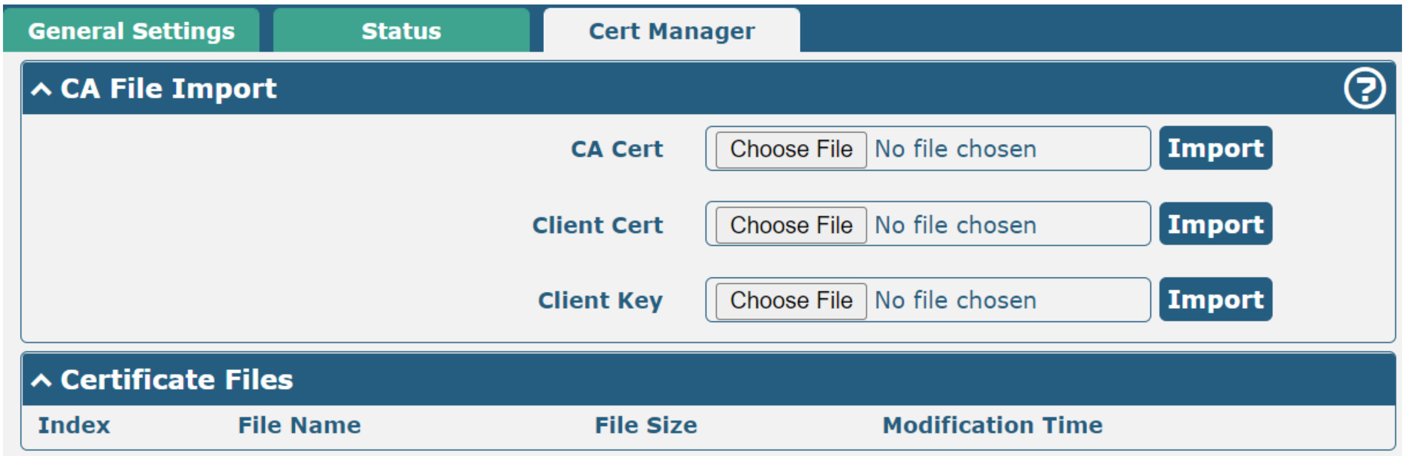


Item	Description
TC Status	Platform connection status.
Station Version	Application version.
Package Version	Application package version.

(Protocol)	
HAL Library Version	LoRaWAN HAL library version.

Cert Manager

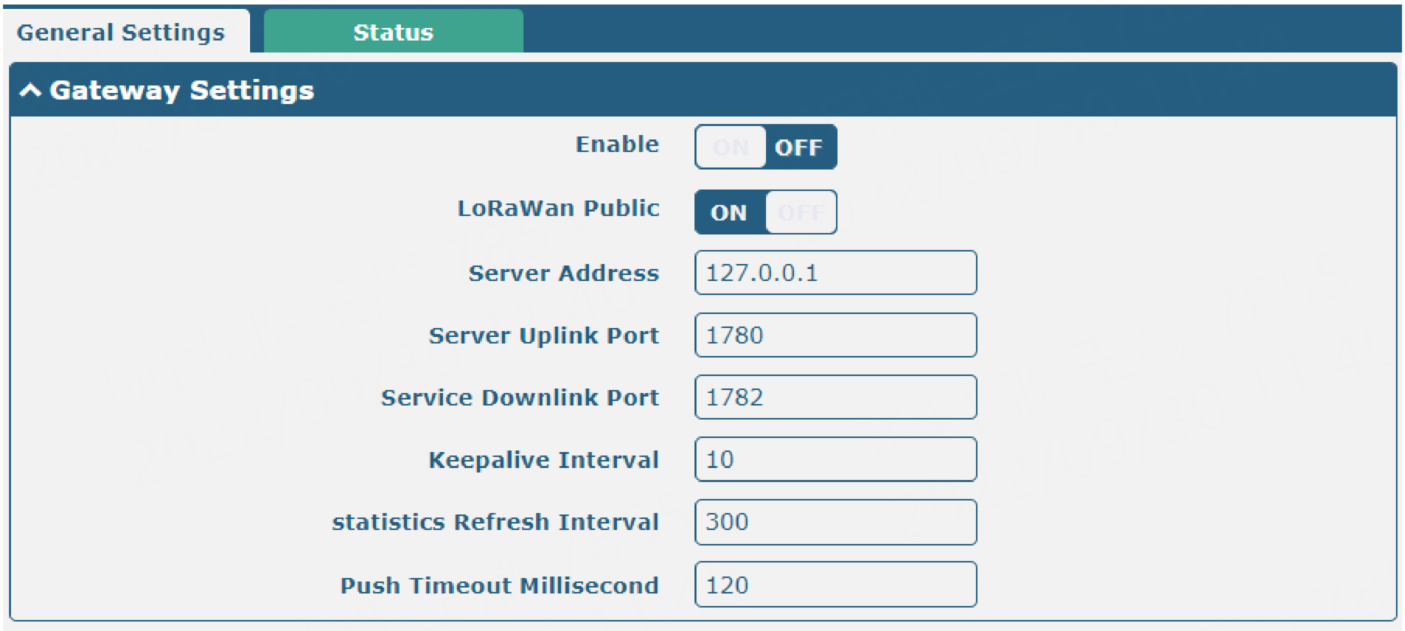
This section allows you to view and import the certification.



Cert Manager		
CA File Import		
Item	Description	Default
CA Cert	Server certificate.	Null
Client Cert	The certificate assigned by the server to the client.	Null
Client Key	The server assigns the private key of the certificate to the client.	Null

3.3.2 Semtech UDP Forwarder

General Settings



Enable: ON OFF

LoRaWan Public: ON OFF

Server Address: 127.0.0.1

Server Uplink Port: 1780

Service Downlink Port: 1782

Keepalive Interval: 10

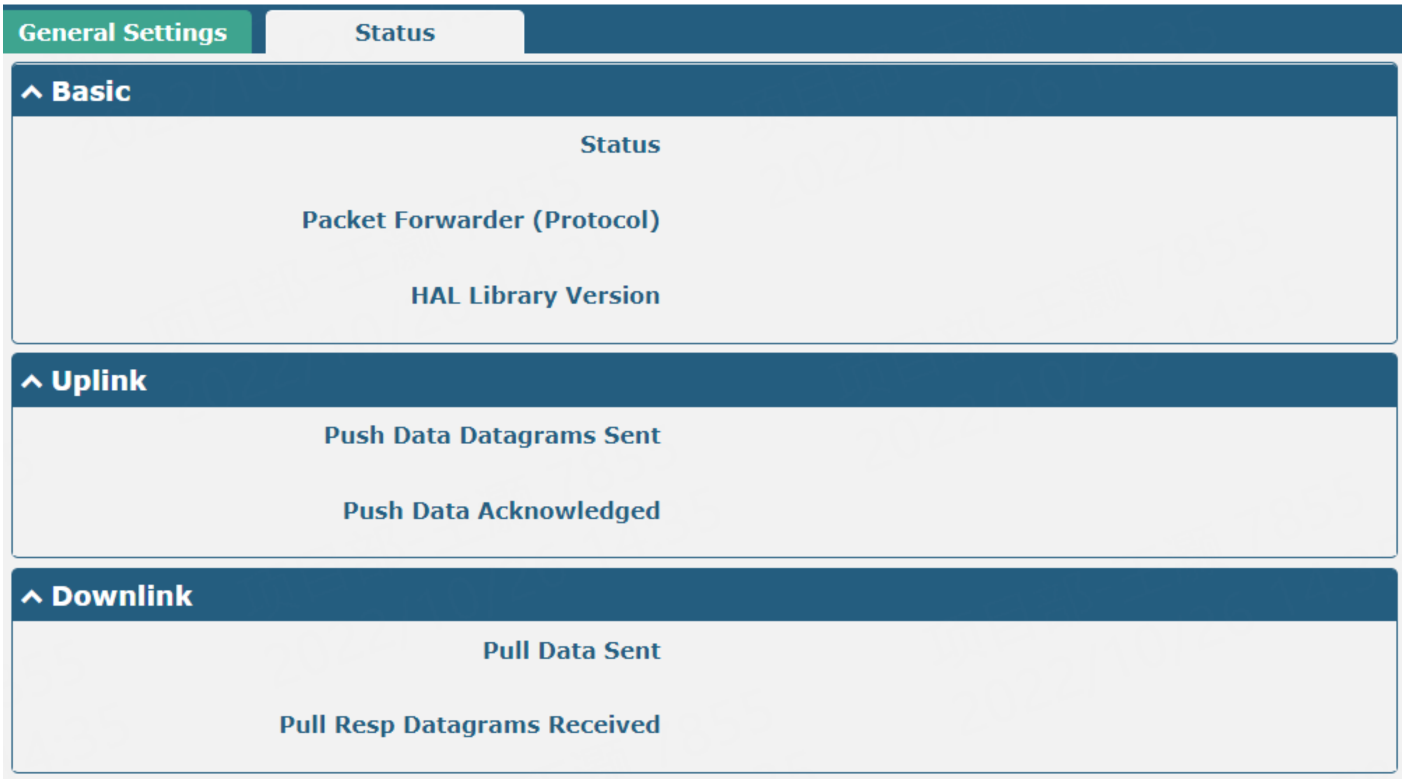
statistics Refresh Interval: 300

Push Timeout Millisecond: 120

General Settings		
Gateway Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable this option.	OFF
LoRaWan Public	Click the toggle button to enable/disable this option.	ON
Server Address	Set the Server address.	127.0.0.1
Server Uplink Port	UDP uplink connection port.	1780
Service Downlink Port	UDP downlink connection port.	1782
Keepalive Interval	Time interval for obtaining downlink data.	10
Statistics Refresh Interval	Statistical interval, USI update interval.	300
Push Timeout Millisecond	Uplink data timeout.	120

Status

This section allows you to view the status of Semtech UDP Forwarder.



^ Basic

Status

Packet Forwarder (Protocol)

HAL Library Version

^ Uplink

Push Data Datagrams Sent

Push Data Acknowledged

^ Downlink

Pull Data Sent

Pull Resp Datagrams Received

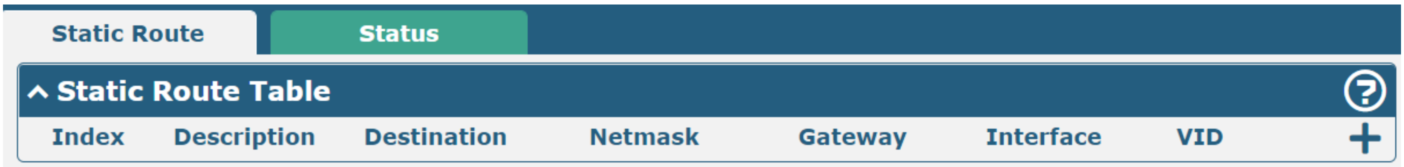
Status	
Item	**Description**
Basic	
Status	Show LoRaWAN status of your gateway.
Packet Forwarder (Protocol)	Show version of Packet forwarder.
HAL Library Version	Show driver version of LoRaWAN chipset inside gateway.
Uplink	
RF packets forwarded	Packets that CRC verified are sent from gateway to server.
Push Data Datagrams Sent	Total quantity of packets sent from gateway to server, including RF packets forwarded and statistics packets.
Push Data Acknowledged	Percentage of acknowledged packets among Push Data Datagrams Sent:
Downlink	
Pull Data Sent	Show the number of keepalive packets sent to the server, and the percentage of acknowledged packets regarding the keepalive packet from the server.
Pull Resp Datagrasms Received	Show packet counts and size that will be sent from server to gateway.

3.4 Network

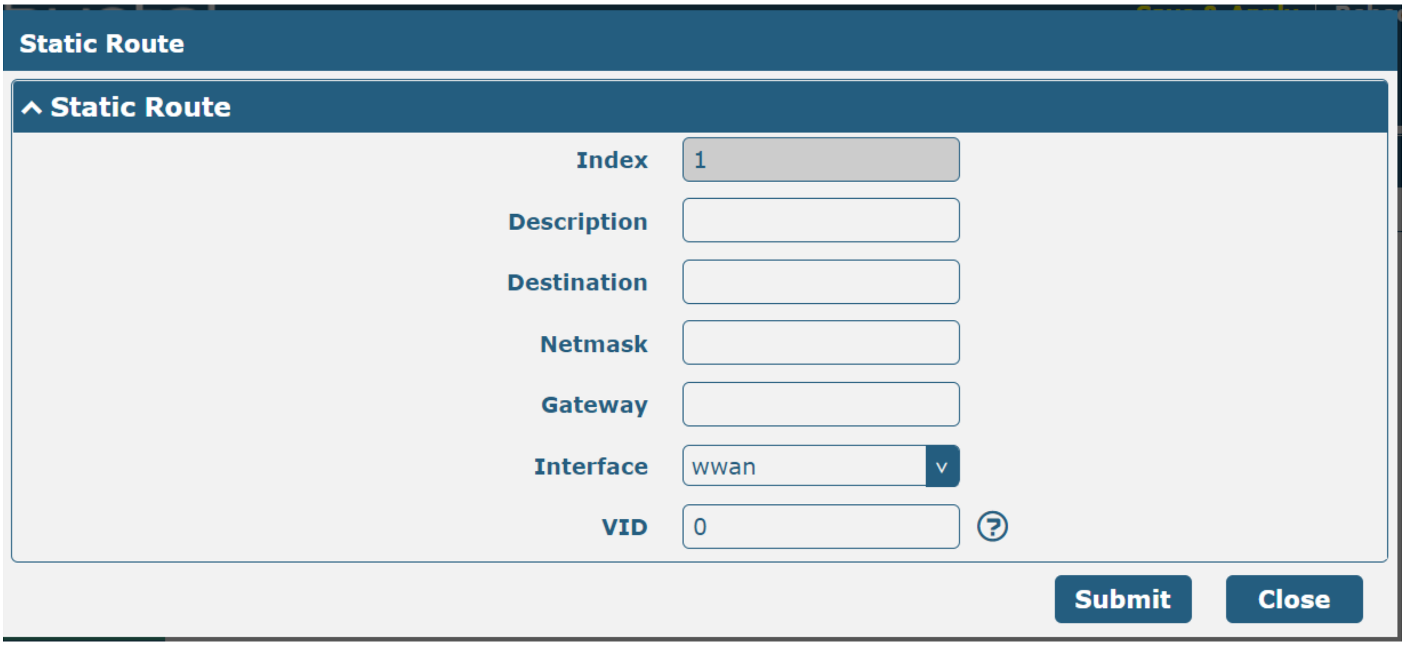
3.4.1 Route

This section allows you to set the static route. A static route is a form of routing that occurs when a device uses a manually-configured routing entry, rather than information from dynamic routing traffic. Route Information Protocol (RIP) is widely used in a small network with a stable use rate. Open Shortest Path First (OSPF) is made device within a single autonomous system and used in a large network.

Static Route



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

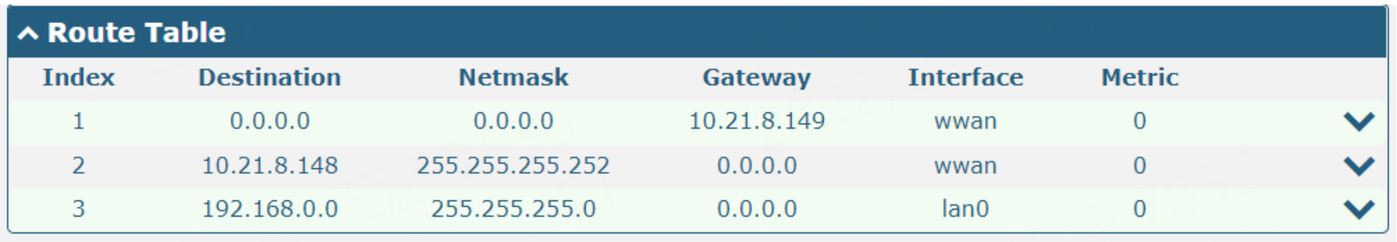


Index	1
Description	
Destination	
Netmask	
Gateway	
Interface	wwan
VID	0

Static Route		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Description	Enter a description for this static route.	Null
Destination	Enter IP address of destination host or destination network.	Null
Netmask/Prefix Length	Enter Netmask of destination host or destination network.	Null
Device	Define device of destination.	Null
Interface	Choose corresponding port of the link that you want to configure.	wwan
VID	Ener VLAN ID. 0 means no VLAN ID.	0

Status

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

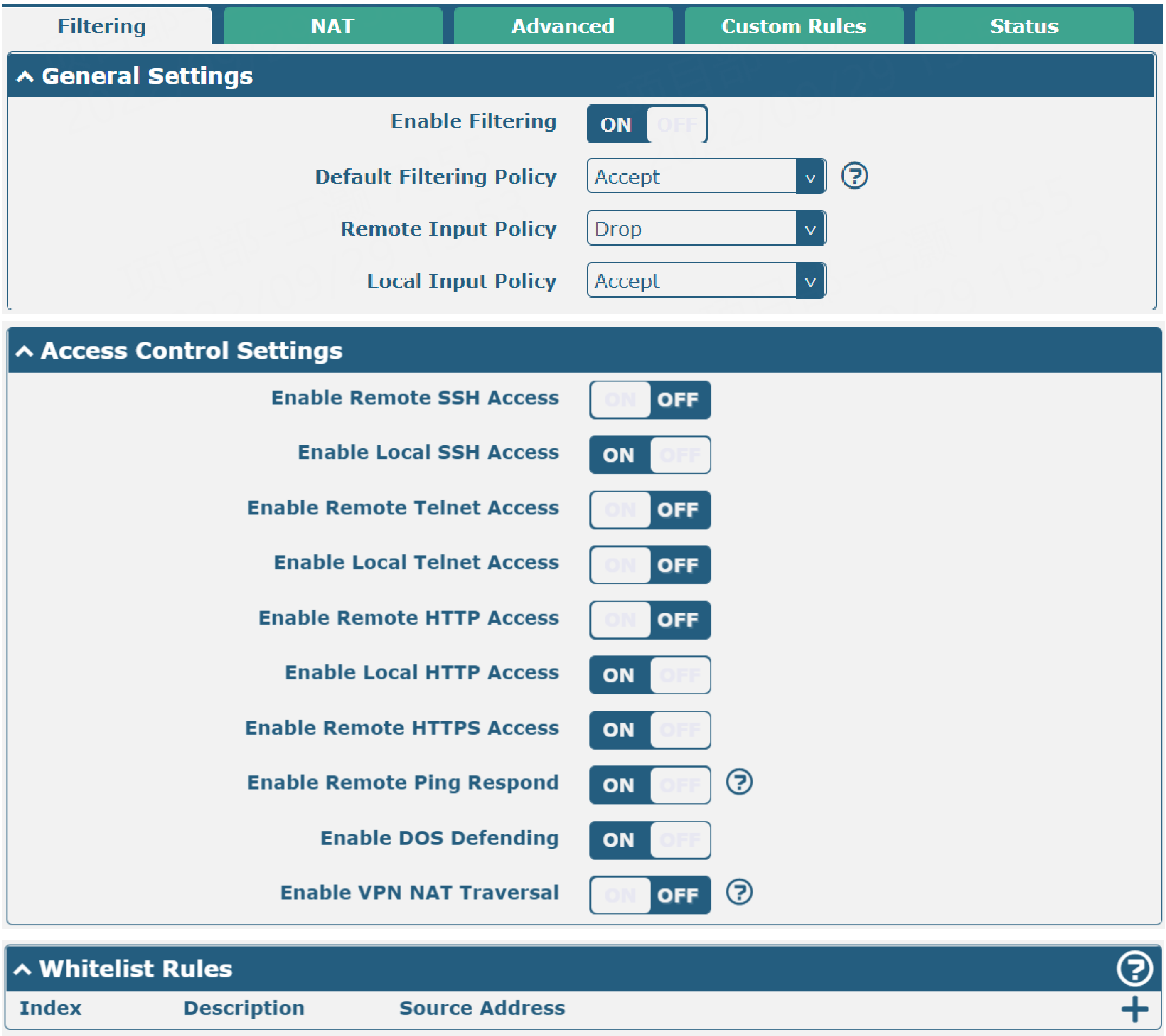


Route Table

Index	Destination	Netmask	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	10.21.8.149	wwan	0
2	10.21.8.148	255.255.255.252	0.0.0.0	wwan	0
3	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0

3.4.2 Firewall

This section allows you to set the firewall and its related parameters, including Filtering, NAT, and IPset. The filtering rules can be used to either accept or block certain users or ports from accessing your device. Click "**Network> Firewall> Filter**". The following information is displayed:



General Settings

Enable Filtering: ON

Default Filtering Policy: Accept

Remote Input Policy: Drop

Local Input Policy: Accept

Access Control Settings

Enable Remote SSH Access: OFF

Enable Local SSH Access: ON

Enable Remote Telnet Access: OFF

Enable Local Telnet Access: OFF

Enable Remote HTTP Access: OFF

Enable Local HTTP Access: ON

Enable Remote HTTPS Access: ON

Enable Remote Ping Respond: ON

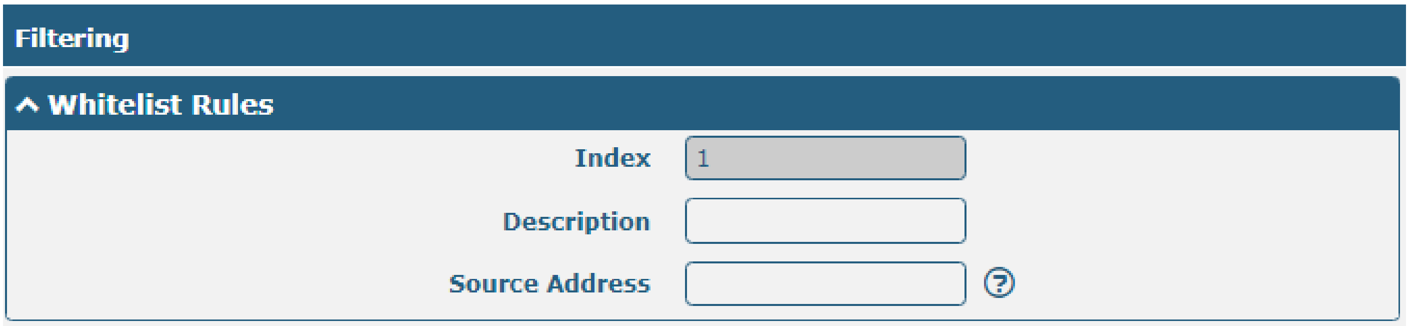
Enable DOS Defending: ON

Enable VPN NAT Traversal: OFF

Whitelist Rules

Index	Description	Source Address

Click + to add the whitelist rules.



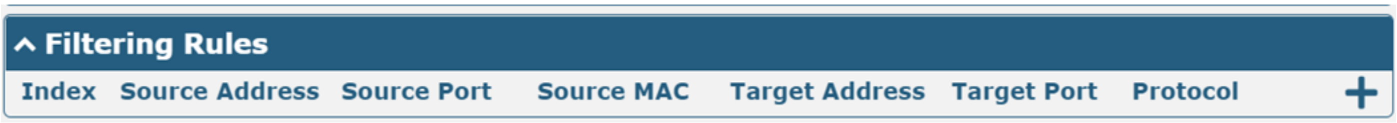
Filtering

Whitelist Rules

Index: 1

Description:

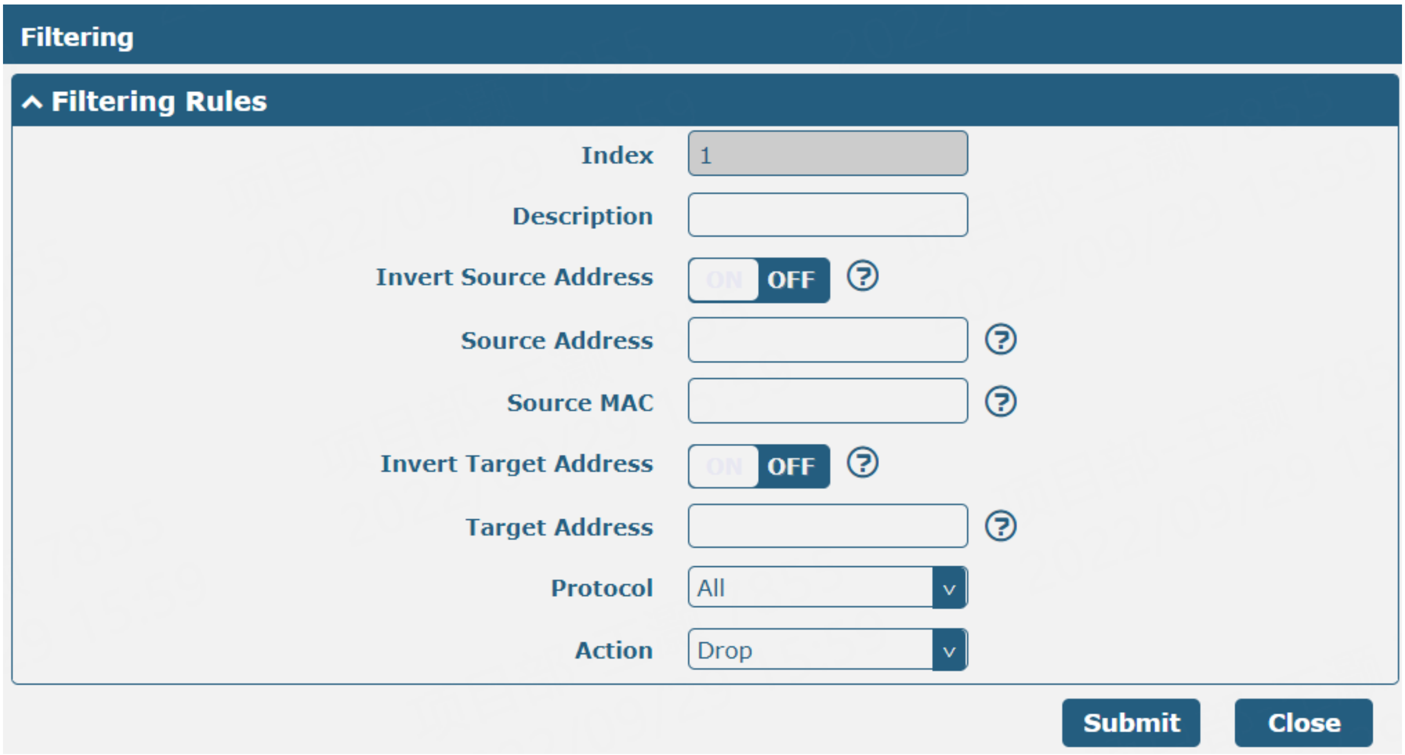
Source Address:



Filtering Rules

Index	Source Address	Source Port	Source MAC	Target Address	Target Port	Protocol

Click + to add a filtering rule. The maximum count is **50**. The window is displayed as below when defaulting "All" or choosing "ICMP" as the protocol. Here take "All" as an example.

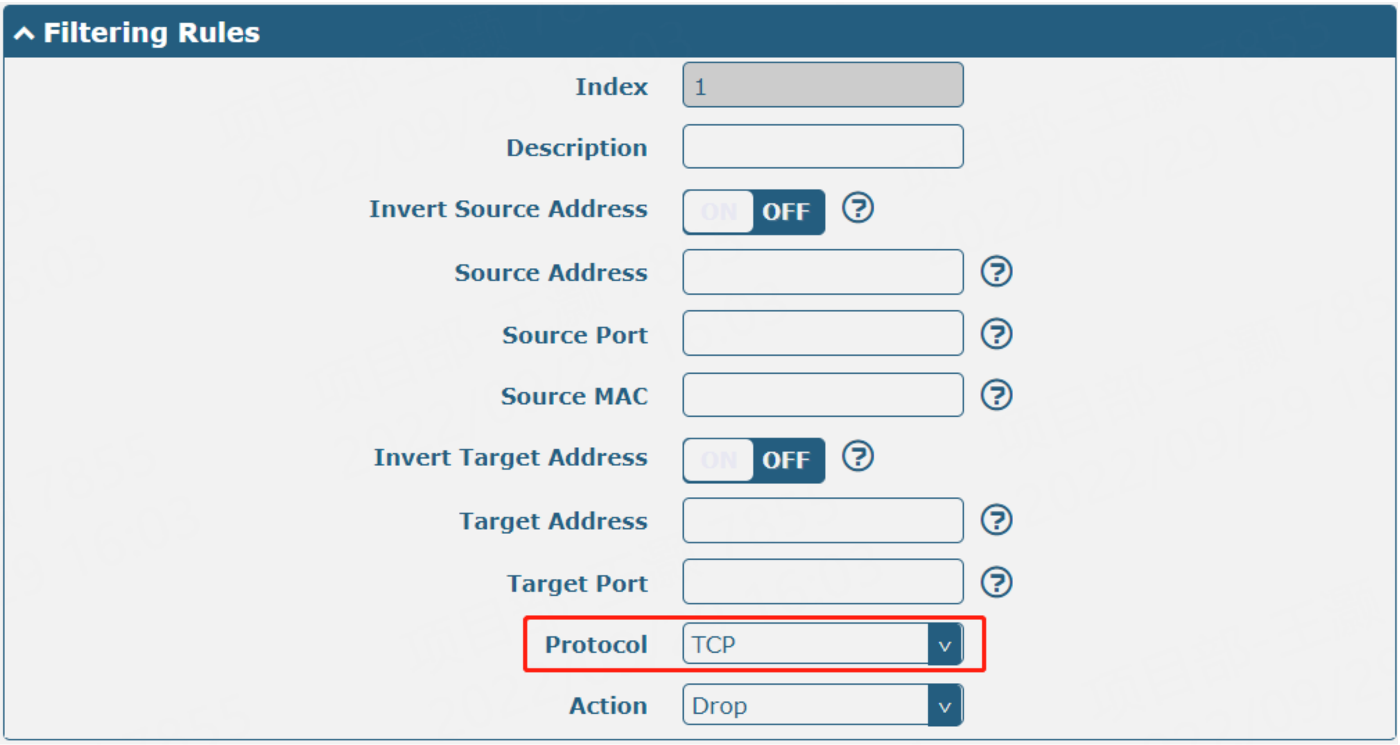


Filtering

Filtering Rules

Index	1
Description	
Invert Source Address	ON OFF
Source Address	
Source MAC	
Invert Target Address	ON OFF
Target Address	
Protocol	All
Action	Drop

The window is displayed below when choosing "TCP", "UDP" or "TCP-UDP" as the protocol. Here takes "TCP" as an example.



Filtering Rules

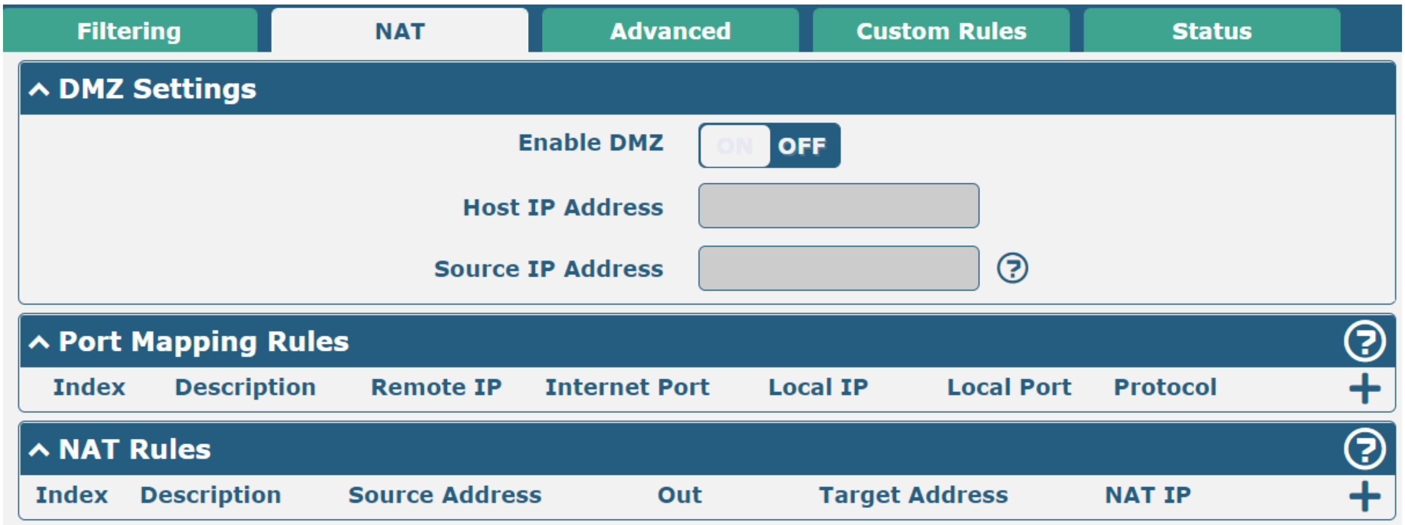
Index	1
Description	
Invert Source Address	ON OFF
Source Address	
Source Port	
Source MAC	
Invert Target Address	ON OFF
Target Address	
Target Port	
Protocol	TCP
Action	Drop

Filtering		
Item	**Description**	**Default**
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON
Default Filtering Policy	Select from “Accept” or “Drop”. • Accept: Device will accept all the connecting requests except the hosts which fit the drop filter list • Drop: Device will drop all the connecting requests except the hosts which fit the accepted filter list	Accept
Remote Input Policy	Select from “Accept” or “Drop”. • Accept: Device will accept all the connecting requests except the hosts which fit the drop filter list • Drop: Device will drop all the connecting requests except the hosts which fit the accepted filter list • Reject: Device will reject all the connecting requests except the hosts which fit the accepted filter list, and a deny (terminate) packet is returned	Drop
Local Input Policy	Select from “Accept” or “Drop”. • Accept: Device will accept all the connecting requests except the hosts which fit the drop filter list • Drop: Device will drop all the connecting requests except the hosts which fit the accepted filter list • Reject: Device will reject all the connecting requests except the hosts which fit the accepted filter list, and a deny (terminate) packet is returned	Accept
Access Control Settings		
Enable Remote SSH Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the device remotely via SSH.	OFF
Enable Local SSH Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the device locally via SSH.	ON
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the device remotely via Telnet.	OFF
Enable Local Telnet Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the device locally via Telnet.	OFF
Enable Remote HTTP Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the device remotely via HTTP.	OFF
Enable Local HTTP Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the device locally via HTTP.	ON
Enable Remote HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the device remotely via HTTPS.	ON
Enable Remote 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 Internet.	ON

Filtering		
Item	**Description**	**Default**
Enable DOS Defending	Click the toggle button to enable/disable this option. When enabled, the device will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON
Enable VPN_NAT traversal	Click the toggle button to enable/disable this option. When enabled, enable NAT traversal for GRE / L2TP / PPTP VPN packets.	OFF
Whitelist Rules		
Index	Indicate ordinal of list.	--
Description	Enter a description for this whitelist rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Filtering Rules		
Index	Indicate ordinal of list.	--
Description	Enter a description for this filtering rule.	Null
Invert Source Address	Enable to invert source address the user input	OFF
Source Address	Specify an access originator and enter its source address.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Specify an access originator and enter its source MAC address.	Null
Invert Target Address	Enable to invert target address the user input	OFF
Target Address	Enter target address which the access originator wants to access.	Null
Target Port	Enter target port that the access originator wants to access.	Null
Protocol	Select from “All”, “TCP”, “UDP”, “ICMP”, “ICMPv6” or “TCP-UDP”. ***Note****: It is recommended that you choose “All” if you don’t know which protocol of your application to use.*	All
Action	Select from “Accept” or “Drop”. • Accept: When Default Filtering Policy is dropped, the device will drop all the connecting requests except the hosts which fit this accepted filtering list. • Drop: When Default Filtering Policy is accepted, the device will accept all the connecting requests except the hosts which fit this drop filtering list.	Drop

NAT

This section allows you to set the NAT related feature, including DMZ, Port Mapping, and NAT.



^ DMZ Settings

Enable DMZ: ON OFF

Host IP Address

Source IP Address

^ Port Mapping Rules

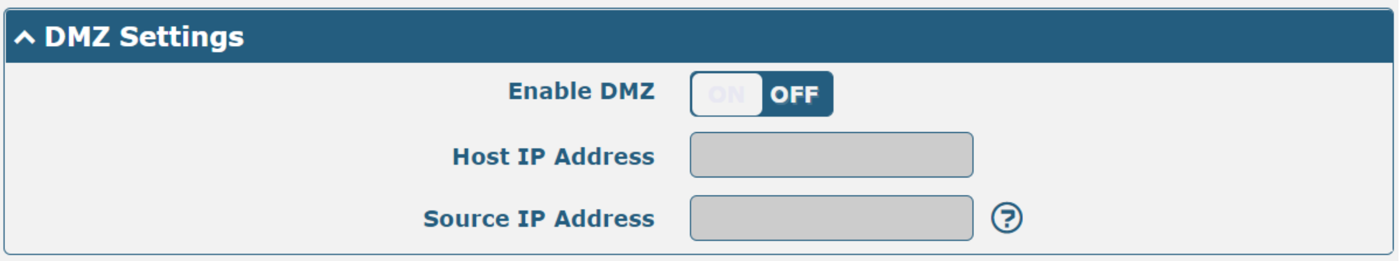
Index	Description	Remote IP	Internet Port	Local IP	Local Port	Protocol

^ NAT Rules

Index	Description	Source Address	Out	Target Address	NAT IP

DMZ (Demilitarized Zone), also known as the demilitarized zone. It is a buffer between a non-secure system and a security 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.

Click "**Network> Firewall> NAT> DMZ"**. The following information is displayed:



^ DMZ Settings

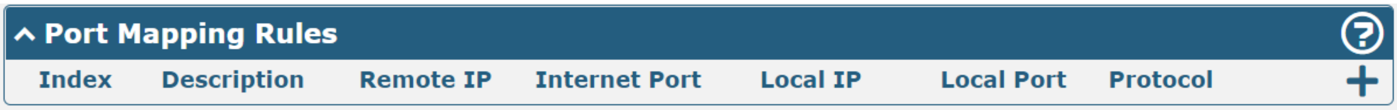
Enable DMZ: ON OFF

Host IP Address

Source IP Address

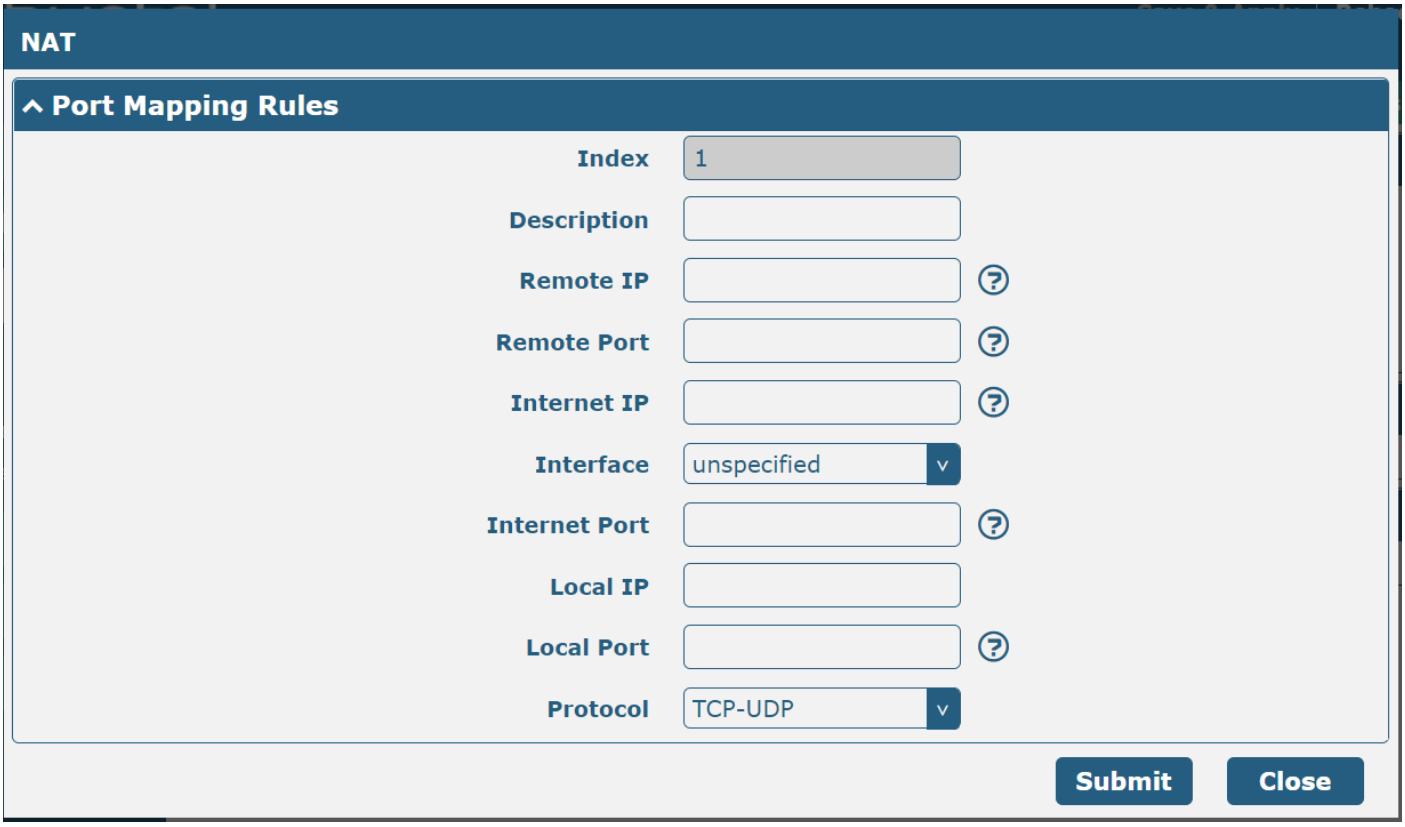
DMZ Settings		
Item	**Description**	**Default**
Enable DMZ	Click the toggle button to enable/disable DMZ. DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	OFF
Host IP Address	Enter IP address of the DMZ host on your internal network.	Null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

Port mapping is defined manually in the device, and all data received from certain ports on the public network is forwarded to a certain port on a certain IP in the internal network. Click "**Network> Firewall> NAT> Port Mapping"** to display the following:



Index	Description	Remote IP	Internet Port	Local IP	Local Port	Protocol

Click + to add port mapping rules. The maximum rule count is **50**.



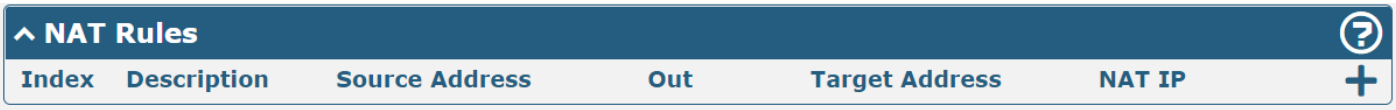
NAT

Port Mapping Rules

Index	1
Description	
Remote IP	
Remote Port	
Internet IP	
Interface	unspecified
Internet Port	
Local IP	
Local Port	
Protocol	TCP-UDP

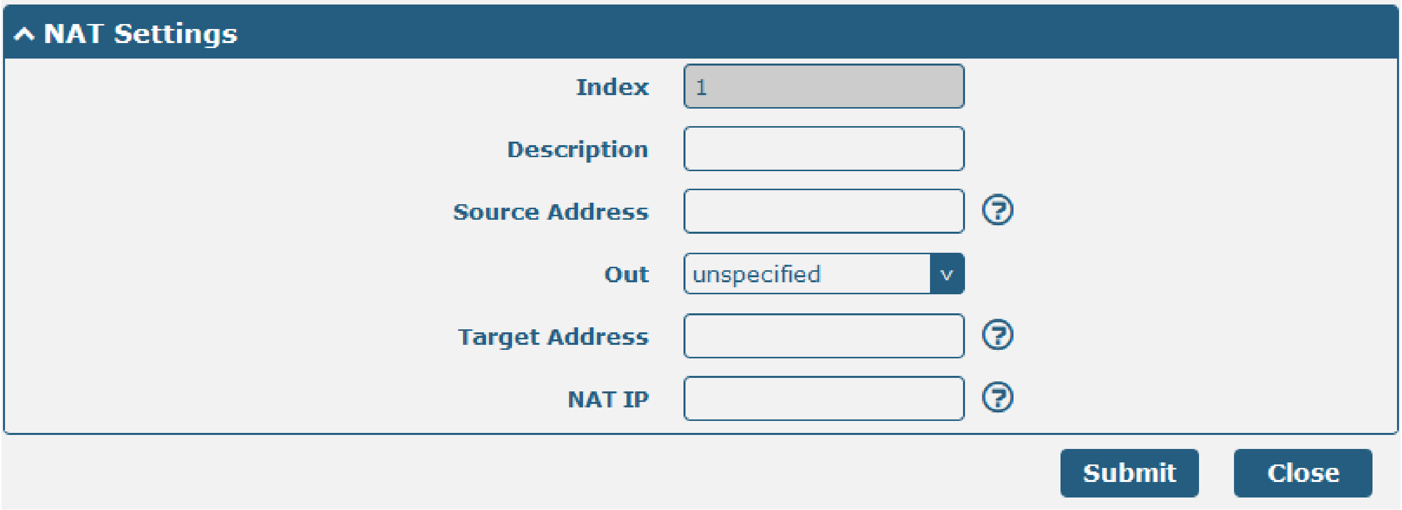
Port Mapping Rules		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Description	Enter a description for this port mapping.	Null
Remote IP	Specify the host or network which can access the local IP address. Empty means unlimited, e.g., 10.10.10.10/255.255.255.255 or 192.168.1.0/24.	Null
Remote Port	Specify the port of the host or network which can access the local IP address. Empty means unlimited.	Null
Internet IP	Enter Internet IP of the device which can be accessed by other hosts from the Internet.	Null
Interface	Choose corresponding port of the link that you want to configure.	Unspecified
Internet Port	Enter Internet port of the device which can be accessed by other hosts from Internet.	Null
Local IP	Enter device’s LAN IP which will forward to the Internet port of device.	Null
Local Port	Enter port of device’s LAN IP.	Null
Protocol	Select from “TCP”, “UDP” or “TCP-UDP” as your application required.	TCP-UDP

NAT setting, custom NAT rules. Click "**Network > Firewall > NAT> NAT Rules**" to display the following.



Index	Description	Source Address	Out	Target Address	NAT IP

Click + to add custom rules.


NAT Settings

Index: 1

Description:

Source Address:

Out: unspecified

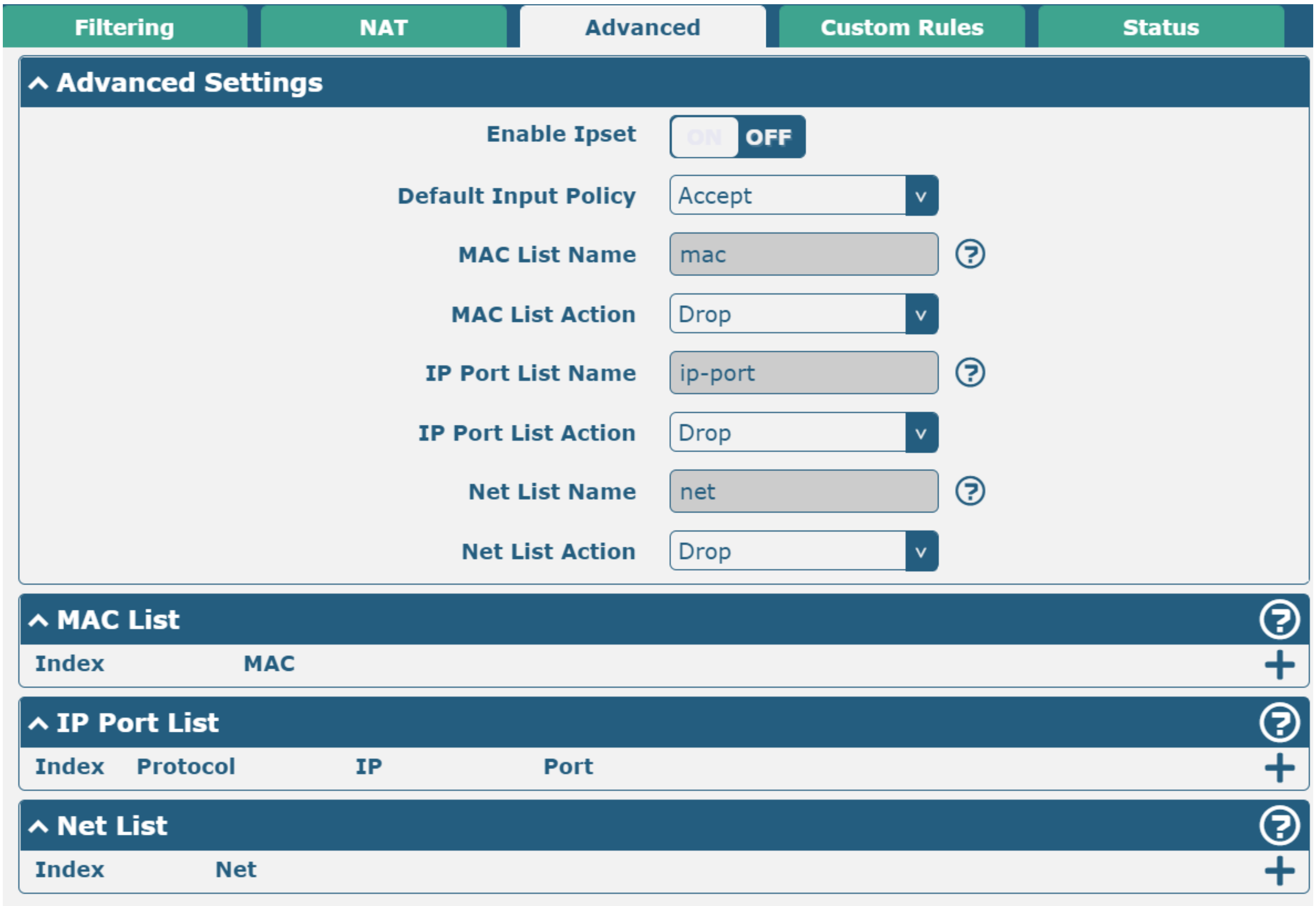
Target Address:

NAT IP:

NAT Settings		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Description	Enter a description of this NAT rule.	Null
Source Address	Enter source address in the format x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x, or null to indicate any address.	Null
Out	Select output interface. Selecting unspecified means any output interface.	unspecified
Target Address	Enter target address in the format x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x.	Null
NAT IP	Enter NAT address in the format x.x.x.x.	Null

Advanced

IP sets are a framework inside the Linux kernel, which can be administered by the Ipset utility. Depending on the type, an IP set may store IP addresses, networks, (TCP/UDP) port numbers, MAC addresses, interface names, or combinations of them in a way, which ensures lightning speed when matching an entry against a set. Click “**Network> Firewall> Advanced”**. The following information is displayed:



Advanced Settings

Enable Ipset	ON OFF
Default Input Policy	Accept
MAC List Name	mac
MAC List Action	Drop
IP Port List Name	ip-port
IP Port List Action	Drop
Net List Name	net
Net List Action	Drop

MAC List

Index	MAC

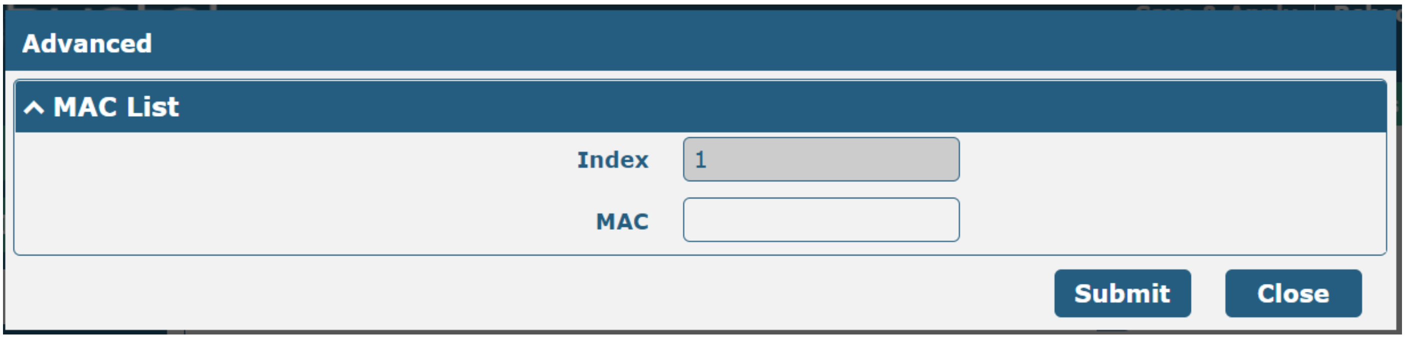
IP Port List

Index	Protocol	IP	Port

Net List

Index	Net

Click + to add a MAC list. The maximum count is **50**.

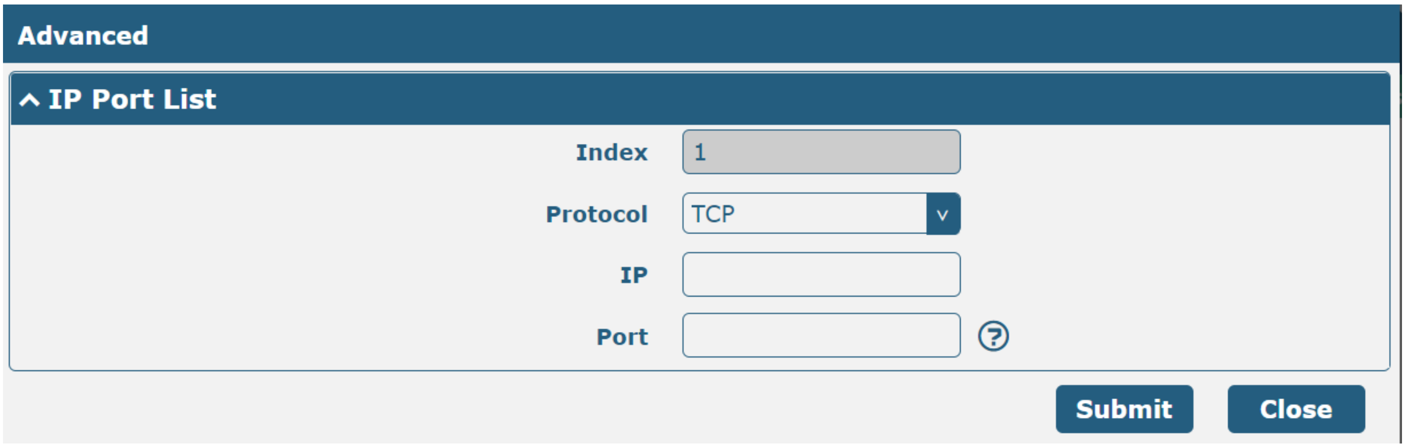


Advanced

MAC List

Index	1
MAC	

Click + to add an IP Port list. The maximum count is **50**.



Advanced

IP Port List

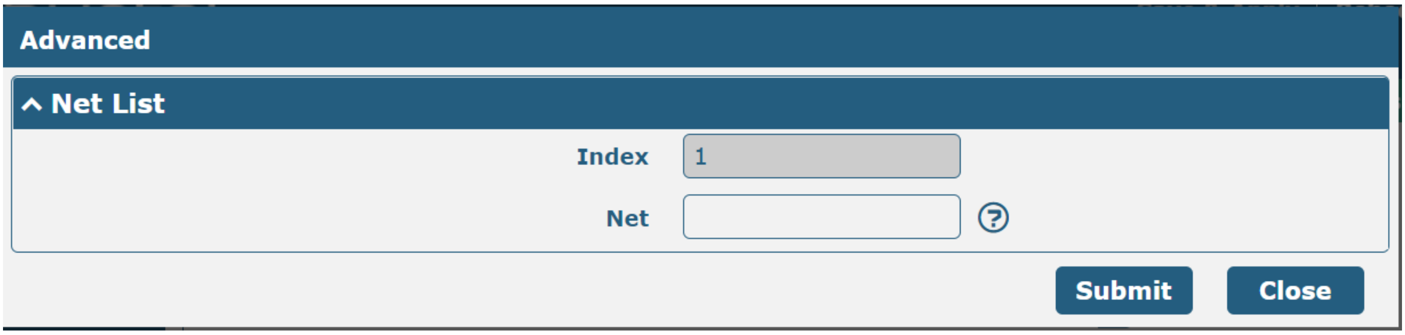
Index: 1

Protocol: TCP

IP:

Port:

Click + to add a Net list. The maximum count is **50**.



Advanced

Net List

Index: 1

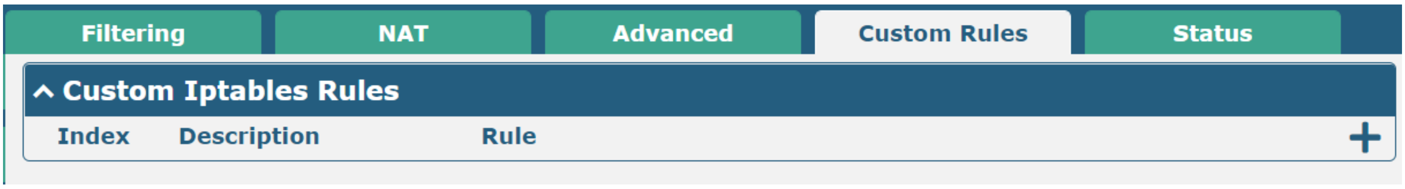
Net:

Advanced		
Item	**Description**	**Default**
General Settings		
Enable Ipset	Click the toggle button to enable/disable the Ipset option.	ON
Default Input Policy	Select from "Accept" or "Drop". • Accept: Device will accept all the input connecting requests except the hosts which fit the drop list of MAC/ IP-Port/ Net. • Drop: Device will drop all the input connecting requests except the hosts which fit the accepted list of MAC/ IP-Port/ Net.	Accept
MAC List Name	Enter the name of the MAC list. It cannot support entering pure numbers.	mac
MAC List Action	Select from "Accept" or "Drop". • Accept: When Default Input Policy is dropped, the device will drop all the connecting requests except the hosts which fit this accepted MAC list. • Drop: When Default Input Policy is accepted, the device will accept all the connecting requests except the hosts which fit this drop MAC list.	Drop
IP Port List Name	Enter name of the MAC list. It cannot support entering pure numbers.	ip-port

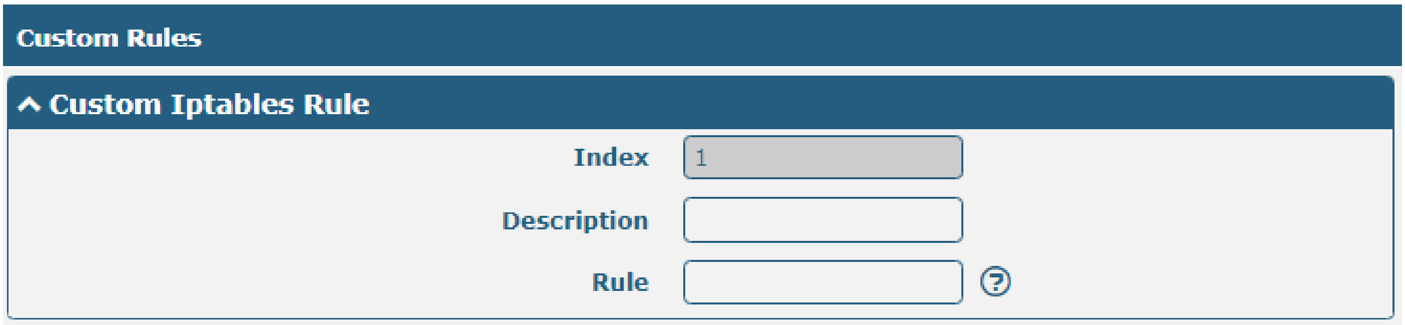
Advanced		
Item	**Description**	**Default**
IP Port List Action	Select from “Accept” or “Drop”. • Accept: When Default Input Policy is dropped, the device will drop all the connecting requests except the hosts which fit this accepted IP Port list. • Drop: When Default Input Policy is accepted, the device will accept all the connecting requests except the hosts which fit this drop IP Port list.	Drop
Net List Name	Enter the name of the MAC list. It cannot support entering pure numbers.	net
Net List Action	Select from “Accept” or “Drop”. • Accept: When Default Input Policy is dropped, the device will drop all the connecting requests except the hosts which fit this accepted Net list. • Drop: When Default Input Policy is accepted, the device will accept all the connecting requests except the hosts which fit this drop Net list.	Drop
MAC List		
Index	Indicate ordinal of the list.	--
MAC address	Enter the MAC address. Format: XX:XX:XX:XX:XX:XX.	Null
IP Port list		
Index	Indicate ordinal of list.	--
Protocol	Select from “TCP”, or “UDP”.	TCP
IP	Enter IP address.	Null
Port	Enter port number.	Null
Net list		
Index	Indicate ordinal of list.	--
Net	Enter domain name/ IP/ IP segment	Null

Custom Rules

This section allows you to add rules that define yourself. Click “**Network> Firewall> Custom Rule”** to display the following:



Click + to add custom rules. The maximum count is **20**.



Custom Rules

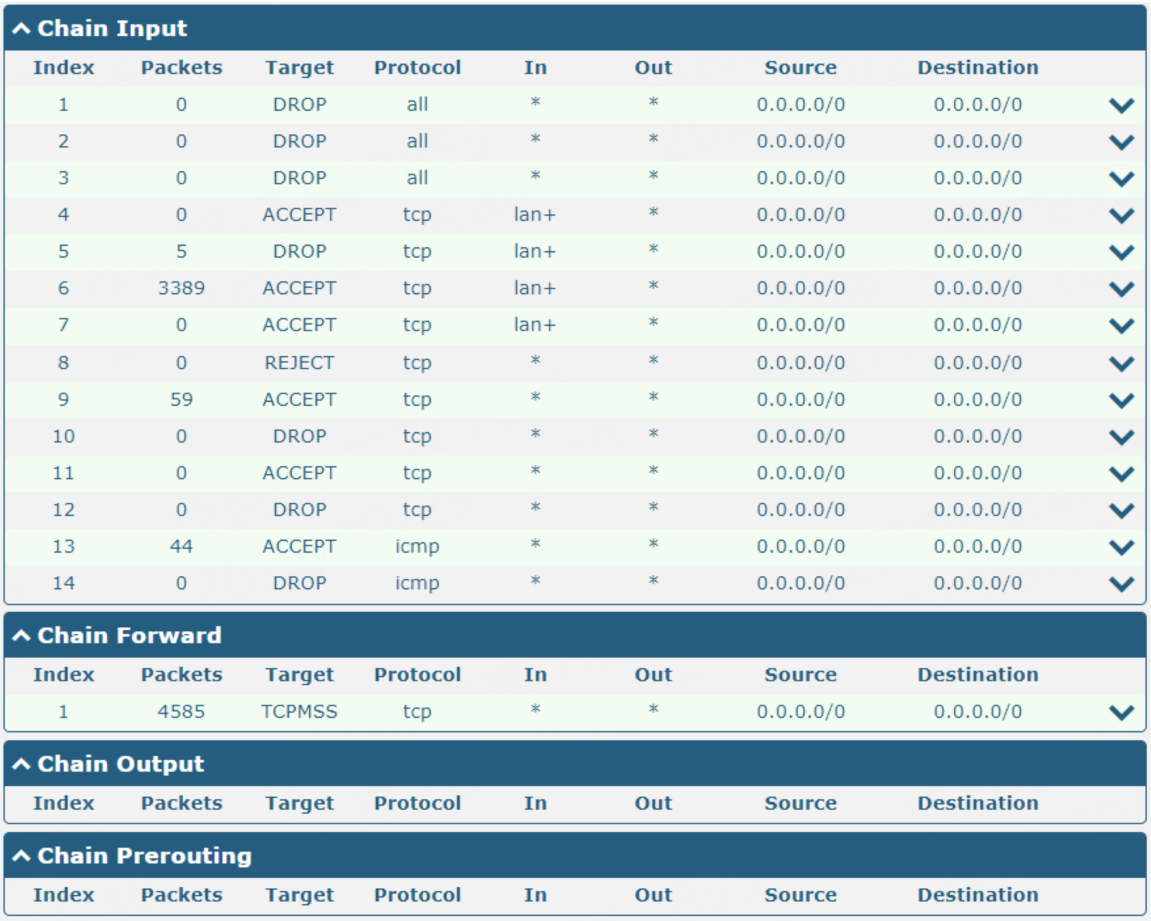
^ Custom Iptables Rule

Index	1
Description	
Rule	

Custom Firewall Rules		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Description	Enter a description for these Custom Firewall Rules.	Null
Rule	Enter custom rules.	Null

Status

This section allows you to view the status of the device's firewall.



^ Chain Input

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0
2	0	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0
4	0	ACCEPT	tcp	lan+	*	0.0.0.0/0	0.0.0.0/0
5	5	DROP	tcp	lan+	*	0.0.0.0/0	0.0.0.0/0
6	3389	ACCEPT	tcp	lan+	*	0.0.0.0/0	0.0.0.0/0
7	0	ACCEPT	tcp	lan+	*	0.0.0.0/0	0.0.0.0/0
8	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	59	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
12	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
13	44	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
14	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0

^ Chain Forward

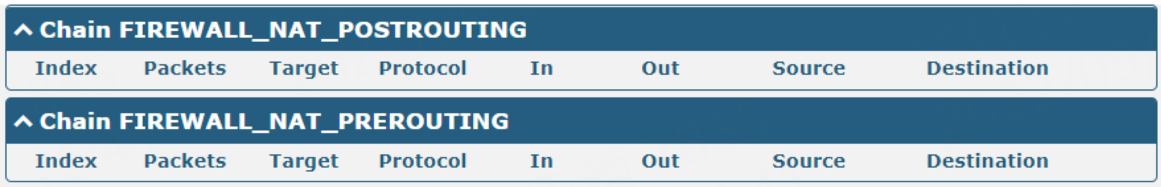
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	4585	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0

^ Chain Output

Index	Packets	Target	Protocol	In	Out	Source	Destination

^ Chain Prerouting

Index	Packets	Target	Protocol	In	Out	Source	Destination



^ Chain FIREWALL_NAT_POSTROUTING

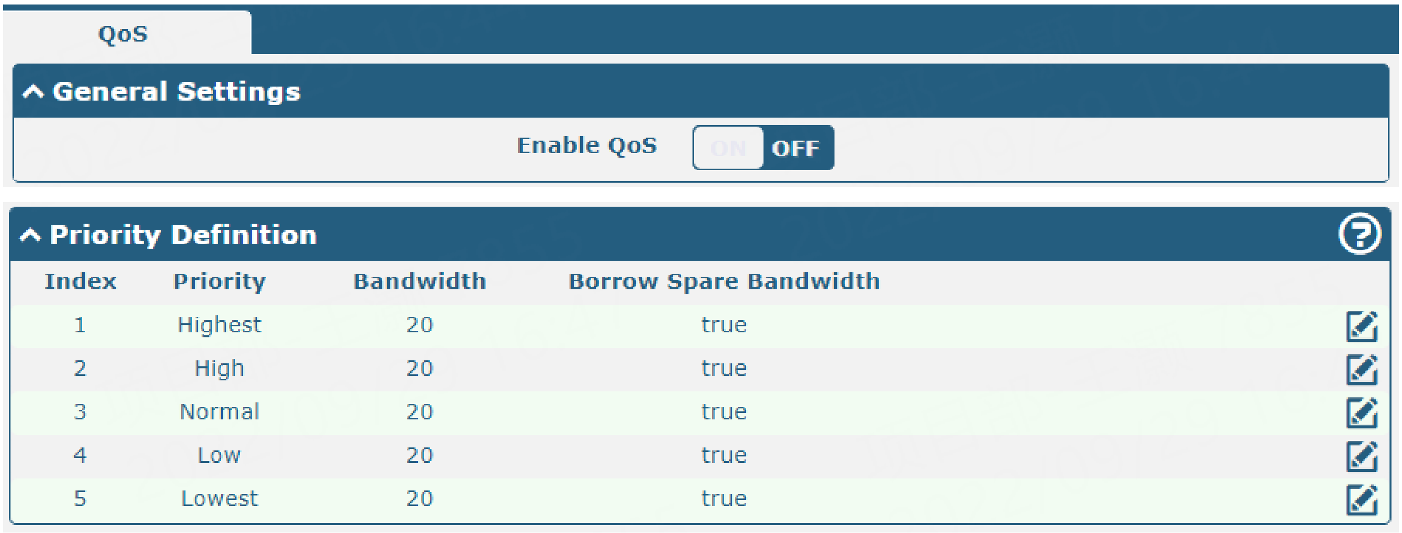
Index	Packets	Target	Protocol	In	Out	Source	Destination

^ Chain FIREWALL_NAT_PREROUTING

Index	Packets	Target	Protocol	In	Out	Source	Destination

3.4.3 QoS

Click "**Network > QoS > Enable QoS"** to enable or disable QoS feature.



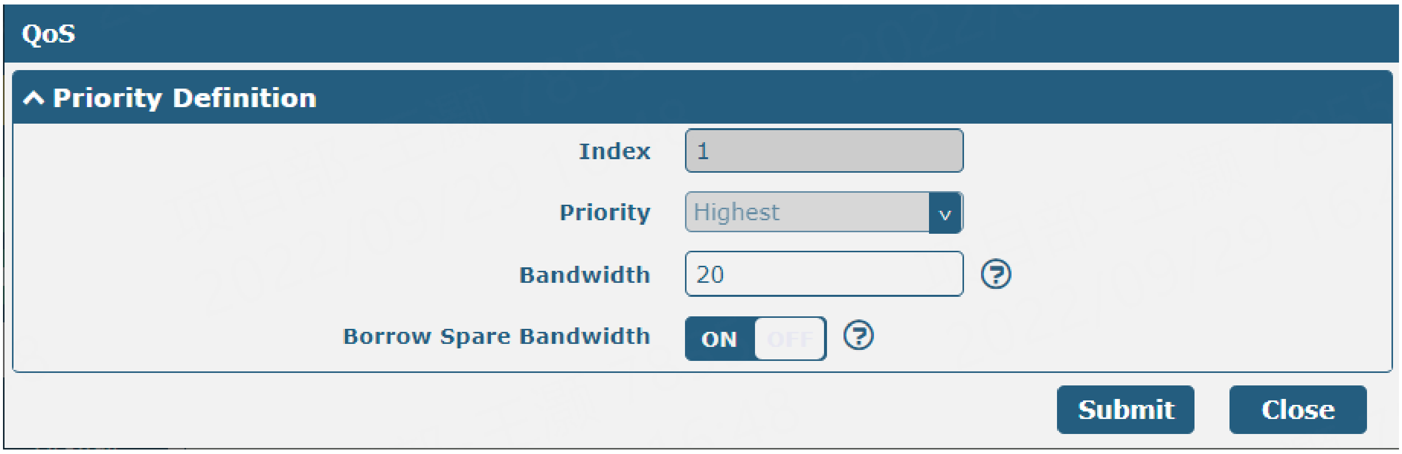
^ General Settings

Enable QoS: ON [✓ OFF]

^ Priority Definition

Index	Priority	Bandwidth	Borrow Spare Bandwidth	
1	Highest	20	true	✎
2	High	20	true	✎
3	Normal	20	true	✎
4	Low	20	true	✎
5	Lowest	20	true	✎

Click the right-most ✎ button to modify QoS Priority. Here take the **Highest** Priority for example, **High, Normal, Low, Lowest** take similar operations.



^ Priority Definition

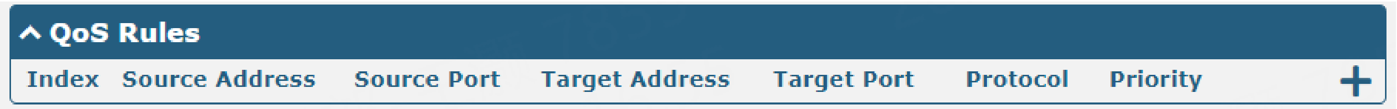
Index: 1

Priority: Highest

Bandwidth: 20

Borrow Spare Bandwidth: [✓ ON] OFF

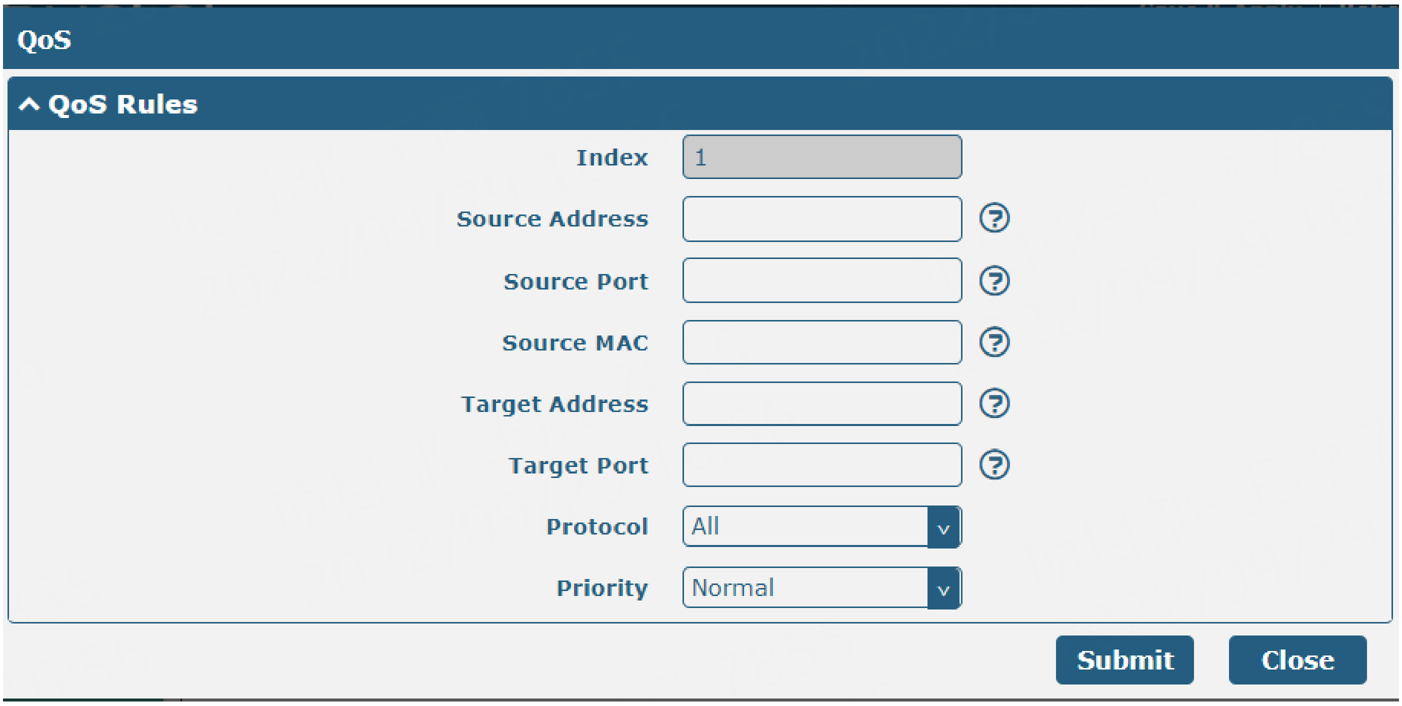
Priority Definition		
Item	**Description**	**Default**
Bandwidth	Enter the percentage of total bandwidth. Full is 100.	20
Borrow Spare Bandwidth	Enable to borrow unused bandwidth from other priorities when the switch is enabled.	ON



^ QoS Rules

Index	Source Address	Source Port	Target Address	Target Port	Protocol	Priority

Click + to add QoS Rule. The maximum count is **20**.



QoS

^ QoS Rules

Index: 1

Source Address:

Source Port:

Source MAC:

Target Address:

Target Port:

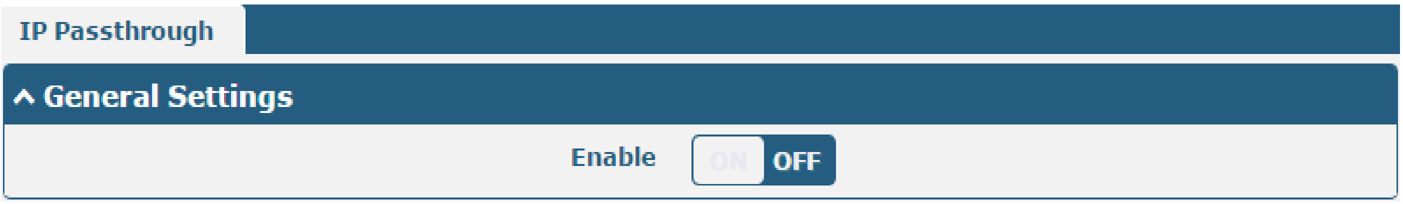
Protocol: All

Priority: Normal

QoS Rules		
Item	**Description**	**Default**
Source Address	Format: x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x, empty means anywhere	NULL
Source Port	Format: port[:port]	ON
Source MAC	Format: XX:XX:XX:XX:XX:XX	NULL
Target Address	Format: x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x, empty means anywhere	NULL
Target Port	Format: port[:port]	NULL
Protocol	Set TCP, UDP, ICMP, TCP-UDP for protocol	All
Priority	Set Priority for QoS	Normal

3.4.4 IP Passthrough

Click “**Network > IP Passthrough > IP Passthrough”** to enable or disable the IP Passthrough option.



IP Passthrough

^ General Settings

Enable: ON OFF

If the device enables the IP Passthrough, the terminal device (such as a PC) will enable the DHCP Client mode and connect to the LAN port of the device, and after the device dial up successfully, the PC will automatically obtain the IP address and DNS server address which assigned by ISP.

Note:

（1） *The IP Passthrough function can only assign one network provider address.*

（2） *To use this function, the main link needs to be set to WWAN, and the backup link needs to be set to None.*

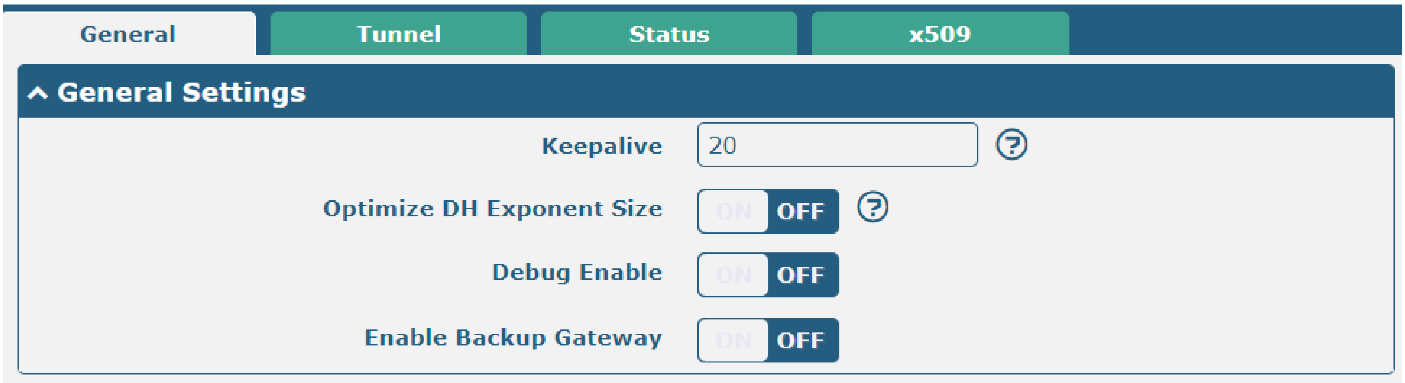
3.5 VPN

3.5.1 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.

Click **VPN > IPsec > General** to set IPsec parameters.

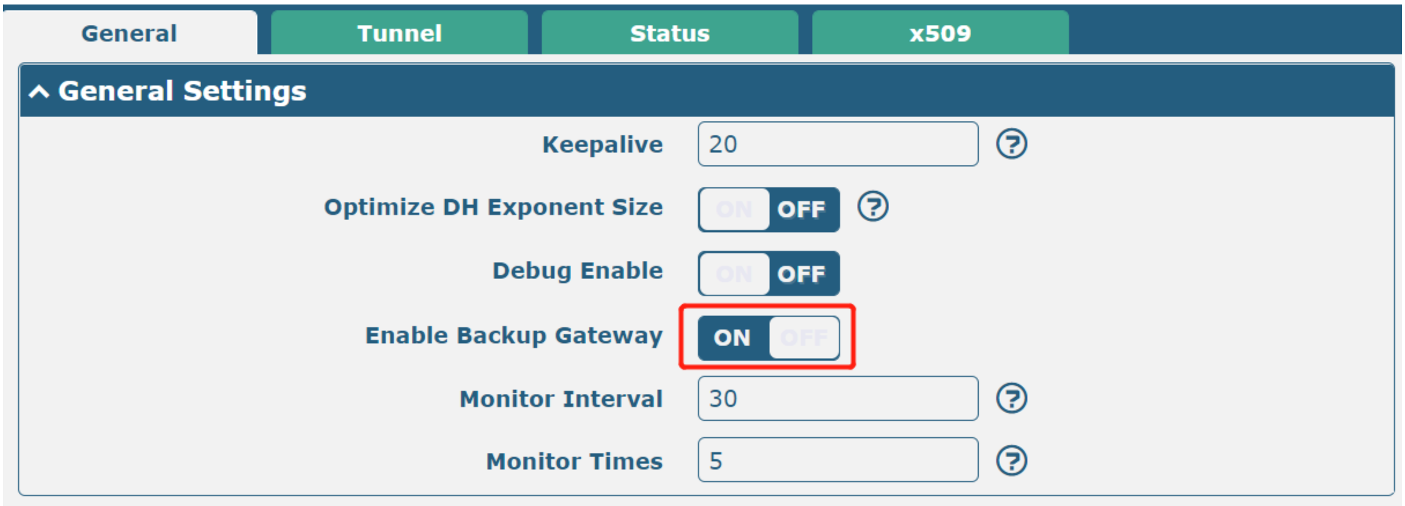
General



General Settings

Keepalive	20
Optimize DH Exponent Size	OFF
Debug Enable	OFF
Enable Backup Gateway	OFF

The window is displayed as below when enabling "Enable Backup Gateway".



Keepalive: 20

Optimize DH Exponent Size: OFF

Debug Enable: OFF

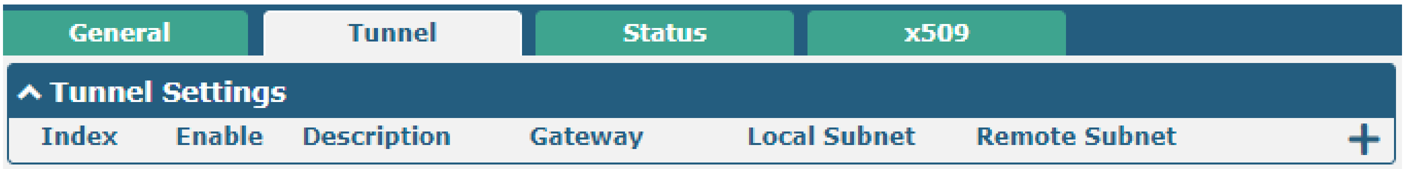
Enable Backup Gateway: ON

Monitor Interval: 30

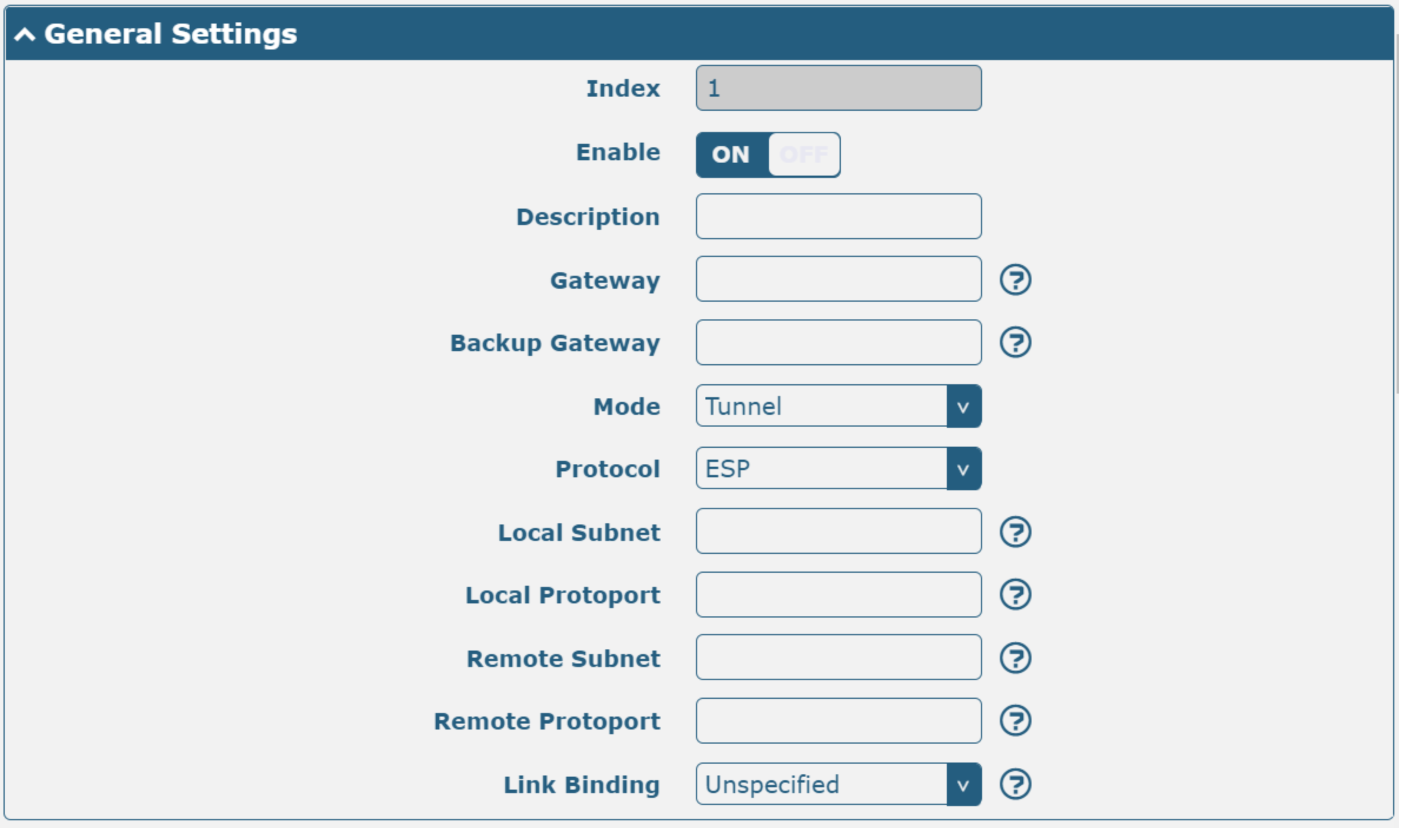
Monitor Times: 5

General Settings @ General		
Item	**Description**	**Default**
Keepalive	Set the time to live in seconds. The device 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 IPsec VPN information output to the debug port.	OFF
Enable Backup Gateway		
Monitor Interval	Enter Monitor Interval. Unit: second.	30
Monitor Times	Enter number maxim of IPsec primary device not answered.	5

Tunnel



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

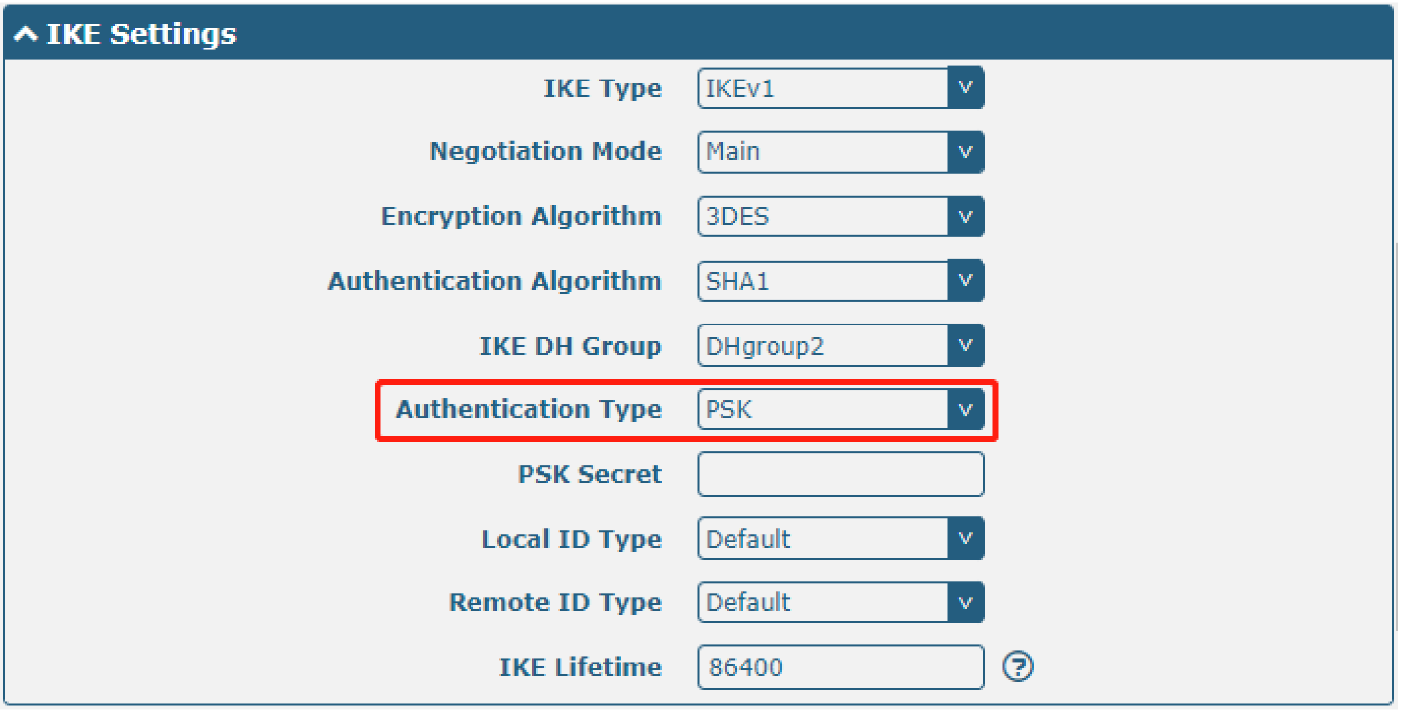


General Settings

Index	1
Enable	ON OFF
Description	
Gateway	
Backup Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Local Protoport	
Remote Subnet	
Remote Protoport	
Link Binding	Unspecified

General Settings @ Tunnel		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Gateway	Enter address of remote side IPsec VPN server. 0.0.0.0 represents any address.	Null
Backup Gateway	Enter backup address of remote side IPsec VPN server. Empty means disable.	Null
Mode	Select from “Tunnel” and “Transport”. • Tunnel: Commonly used between devices, or at an end-station to a device, the device acting as a proxy for the hosts behind it. • Transport: Used between end-stations or between an end-station and a device, if the device is being treated as a host-for example, an encrypted Telnet session from a workstation to a device, in which the device is the actual destination.	Tunnel
Protocol	Select the security protocols from “ESP” and “AH”. • ESP: Use the ESP protocol. • AH: Use the AH protocol.	ESP
Local Subnet	Enter local subnet’s address with a mask protected by IPsec, e.g., 192.168.1.0/24.	Null
Local Protoport	Enter protocol with port, e.g., tcp/443; udp/1701. Local protoport and remote protoport must be the same if both are not empty.	Null
Remote Subnet	Enter remote subnet’s address with a mask protected by IPsec, e.g., 10.8.0.0/24.	Null
Remote Protoport	Enter protocol with port, e.g., tcp/443; udp/1701. Local protoport and remote protoport must be the same if both are not empty.	Null
Link binding	Select link to build IPsec.	Unbound

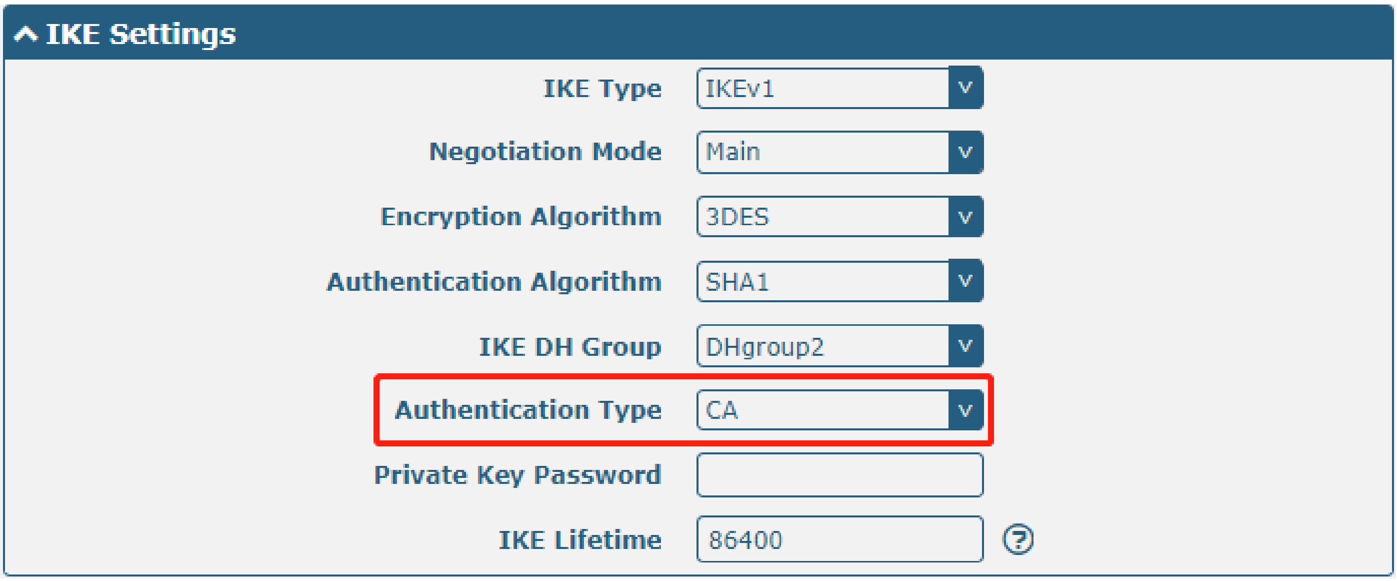
The window is displayed below when choosing “PSK” as the authentication type.



IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

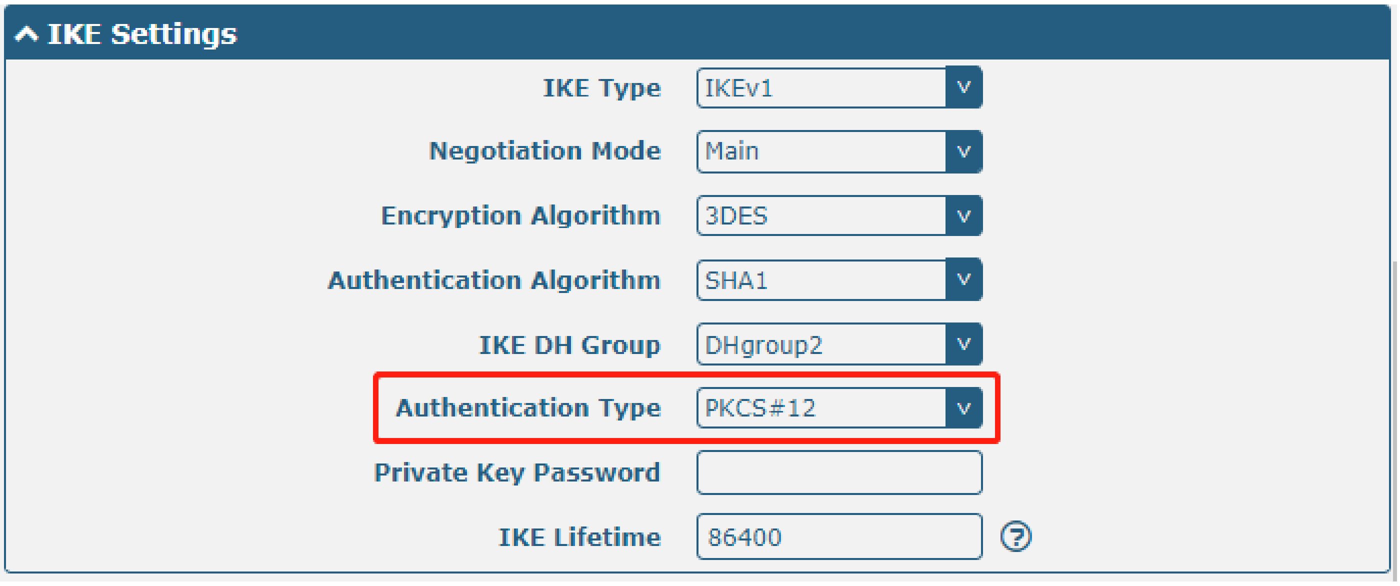
The window is displayed below when choosing “CA” as the authentication type.



IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	CA
Private Key Password	
IKE Lifetime	86400

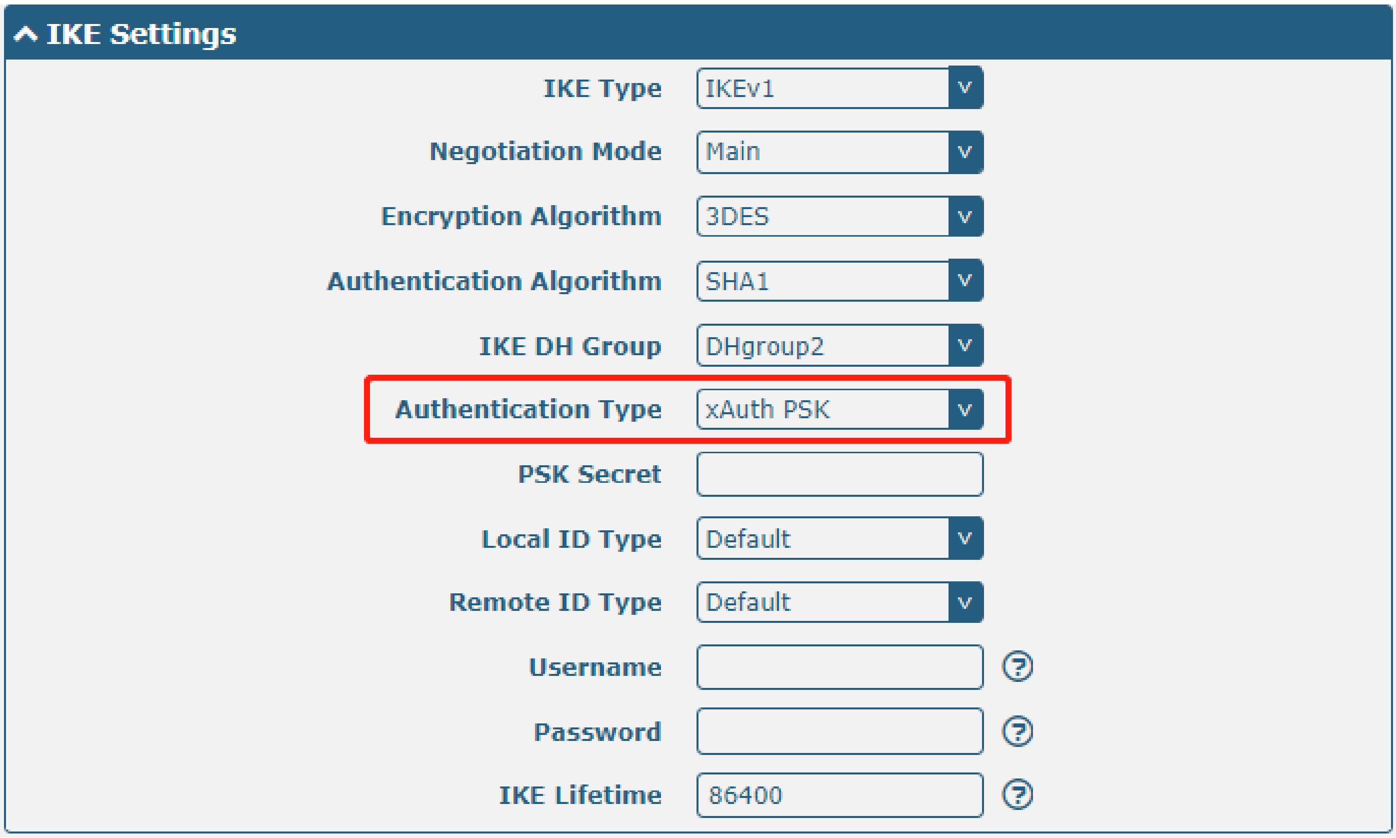
The window is displayed below when choosing "PKCS#12" as the authentication type.



IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PKCS#12
Private Key Password	
IKE Lifetime	86400

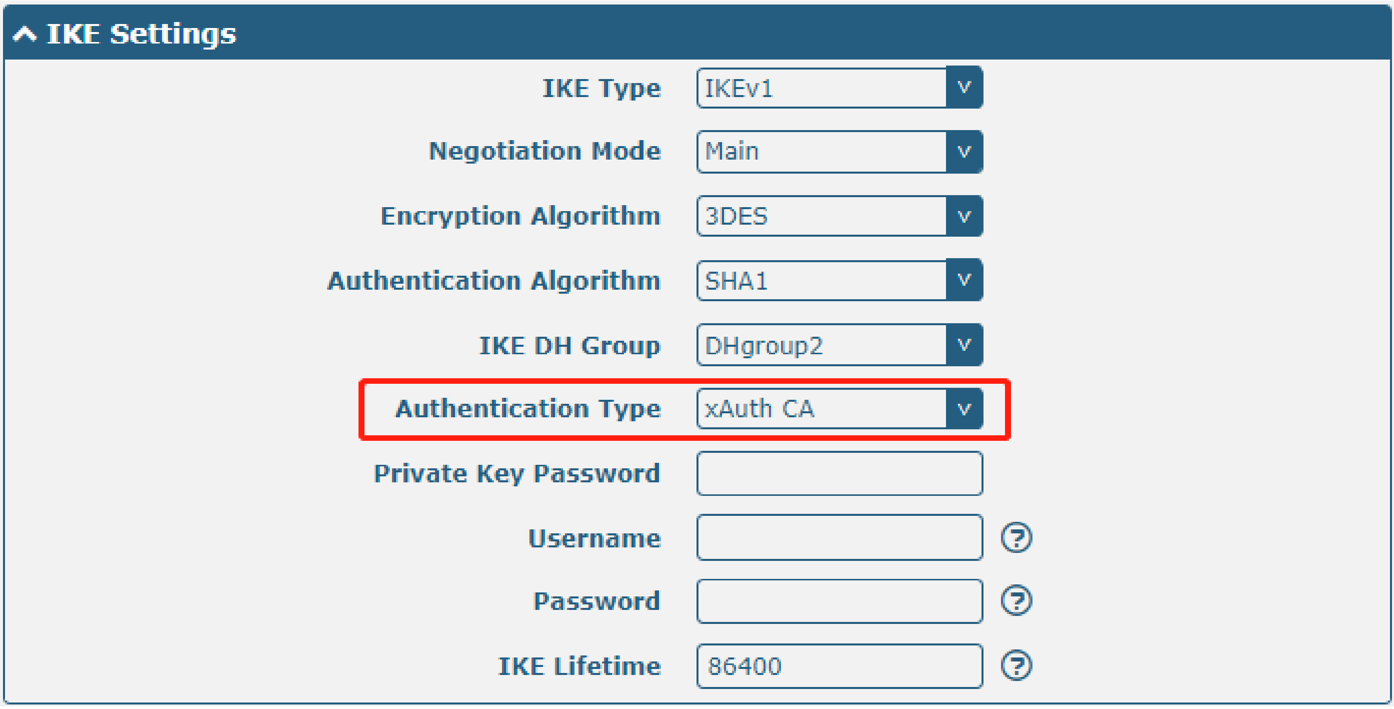
The window is displayed below when choosing "xAuth PSK" as the authentication type.



IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	xAuth PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
Username	
Password	
IKE Lifetime	86400

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



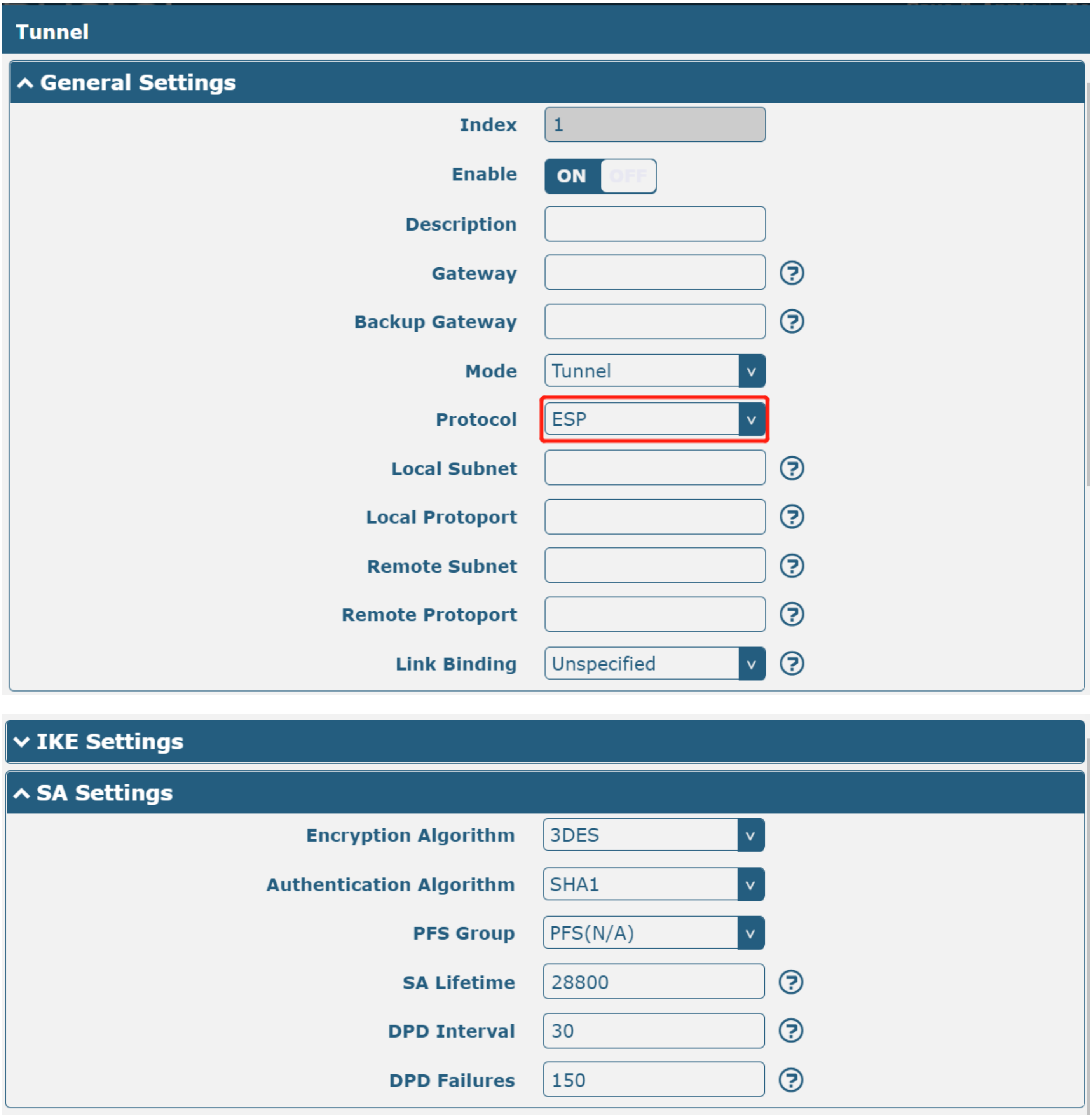
IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	xAuth CA
Private Key Password	
Username	
Password	
IKE Lifetime	86400

IKE Settings		
Item	**Description**	**Default**
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, SA can be established as long as the username and password are correct.	Main
Encrypt Algorithm	Select from "3DES", "AES128", "AES192" and "AES256" to be used in IKE negotiation. • 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", or "SHA2 512" to be used in IKE negotiation.	SHA1
IKE DH Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17", or "DHgroup18" to be used in key negotiation phase 1.	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 pre-shared key.	Null
Local ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Uses an IP address as the ID in IKE negotiation.	Default

IKE Settings		
Item	**Description**	**Default**
	• 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 device, 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 device, 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 device, 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 device, e.g., test@robustel.com.	Default
IKE Lifetime	Set lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as 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 private key under "CA" and "xAuth CA" authentication types.	Null
Username	Enter username used for "xAuth PSK" and "xAuth CA" authentication types.	Null
Password	Enter password used for "xAuth PSK" and "xAuth CA" authentication types.	Null

If click **VPN > IPsec > Tunnel > General Settings**, and choose **ESP** as protocol. The specific parameter configuration is shown below.



Tunnel

General Settings

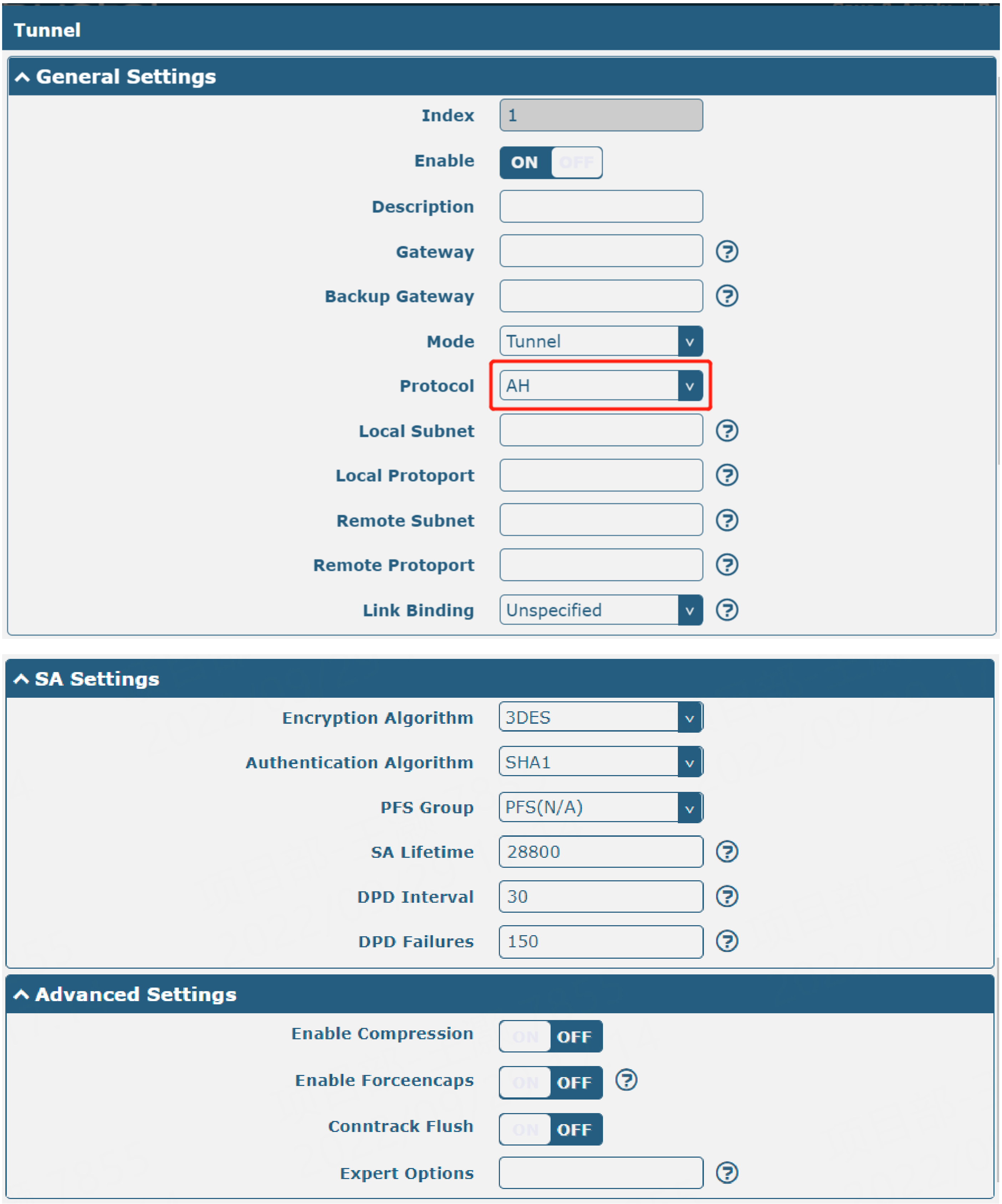
Index	1
Enable	ON OFF
Description	
Gateway	
Backup Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Local Protoport	
Remote Subnet	
Remote Protoport	
Link Binding	Unspecified

IKE Settings

SA Settings

Encryption Algorithm	3DES
Authentication Algorithm	SHA1
PFS Group	PFS(N/A)
SA Lifetime	28800
DPD Interval	30
DPD Failures	150

When protocol in "Virtual Private Network> IPsec> Tunnel> General Settings" selects "**AH**", SA settings are displayed as follows:



Tunnel

^ General Settings

Index	1
Enable	ON
Description	
Gateway	
Backup Gateway	
Mode	Tunnel
Protocol	AH
Local Subnet	
Local Protoport	
Remote Subnet	
Remote Protoport	
Link Binding	Unspecified

^ SA Settings

Encryption Algorithm	3DES
Authentication Algorithm	SHA1
PFS Group	PFS(N/A)
SA Lifetime	28800
DPD Interval	30
DPD Failures	150

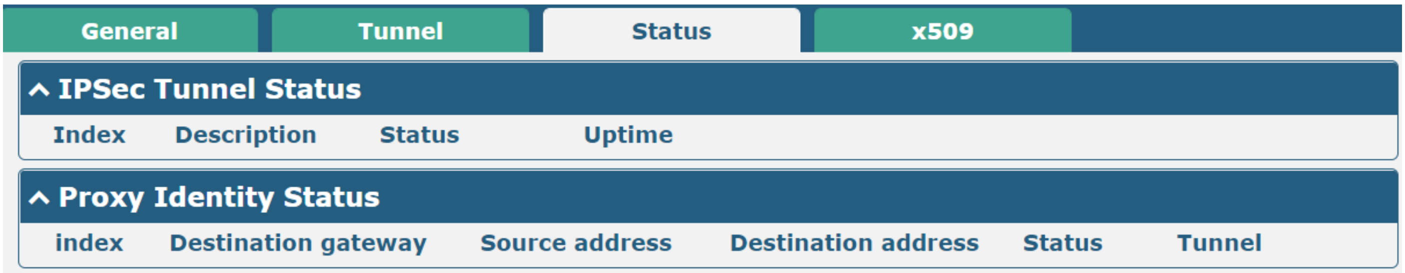
^ Advanced Settings

Enable Compression	OFF
Enable Forceencaps	OFF
Conntrack Flush	OFF
Expert Options	

SA Settings		
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.	SHA1
PFS Group	Select from “PFS(N/A)”, “DHgroup1”, “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in SA negotiation.	PFS(N/A)
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 interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is 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 acknowledgement within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgement 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 timeout of DPD (Dead Peer Detection) packets.	150
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Enable Forceencaps	Click the toggle button to enable/disable this option. After it is enabled, even if no NAT condition is detected, the UDP encapsulation of esp packets is forced. This may help overcome restrictive firewalls.	OFF
Conntrack Flush	Click the toggle button to enable/disable this option. Clear conntrack after establishing IPsec.	OFF
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none.	Null

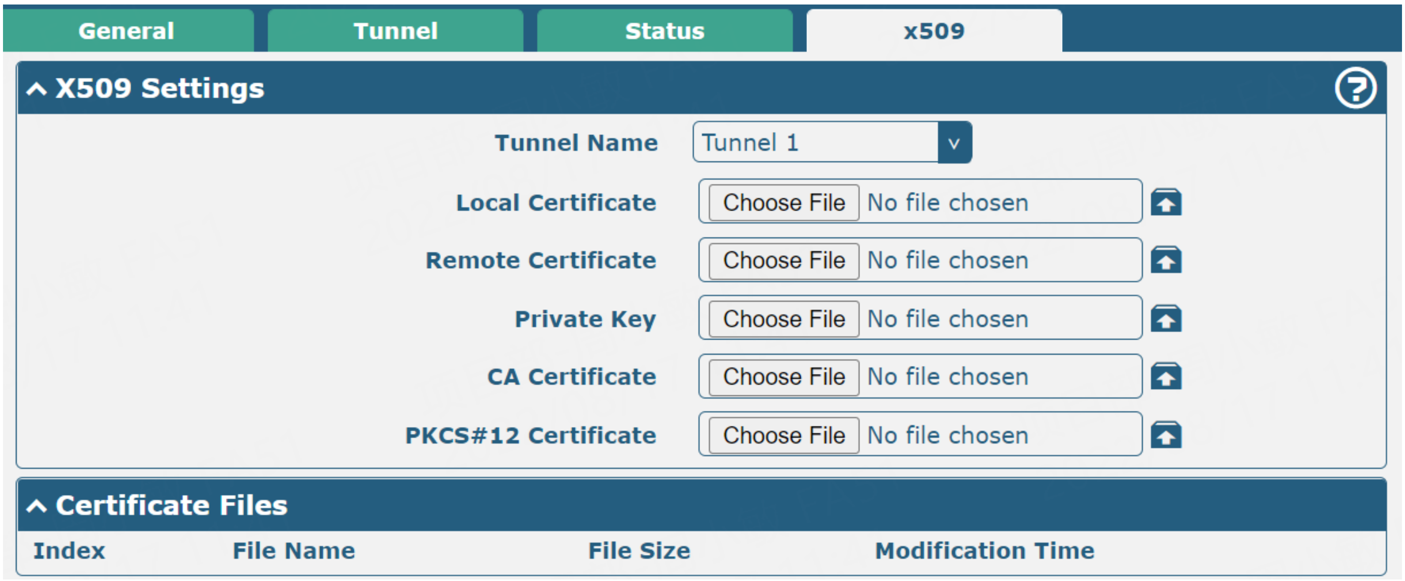
Status

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



x509

Users can upload the certificates for the IPsec tunnel in this section.



Tunnel Name: Tunnel 1

Local Certificate: Choose File No file chosen

Remote Certificate: Choose File No file chosen

Private Key: Choose File No file chosen

CA Certificate: Choose File No file chosen

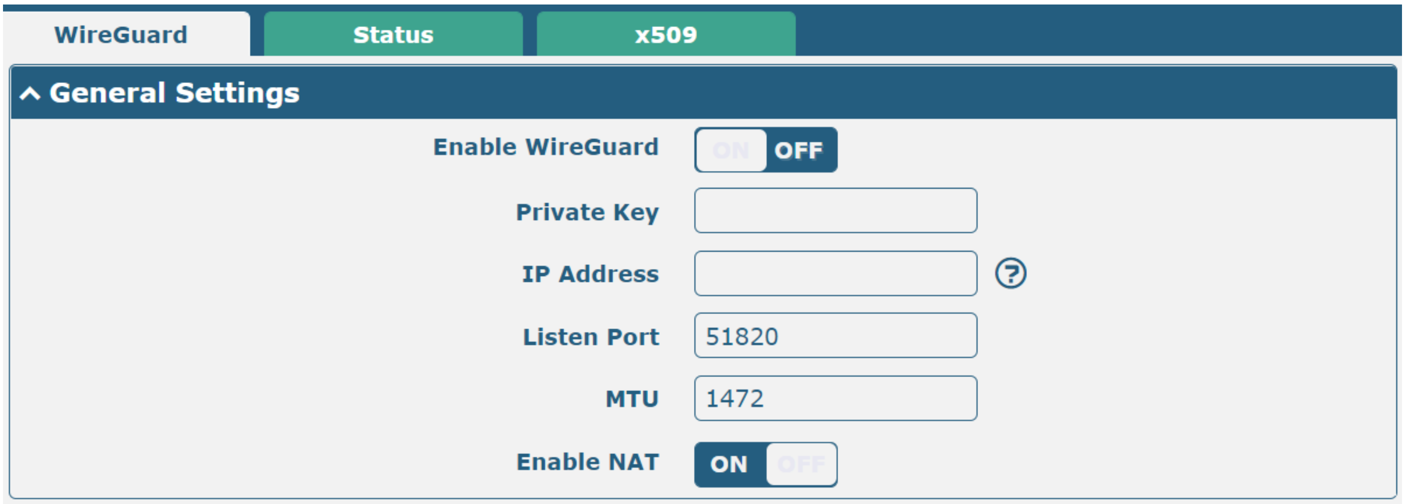
PKCS#12 Certificate: Choose File No file chosen

x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3", "Tunnel 4", "Tunnel 5", or "Tunnel 6".	Tunnel 1
Local Certificate	Click "Choose File" to locate the certificate file from the local computer, and then import this file into your device.	--
Remote Certificate	Click "Choose File" to locate the certificate file from the remote computer, and then import this file into your device.	--
Private Key	Click "Choose File" to locate the private key file.	--
CA Certificate	Click "Choose File" to locate the correct CA certificate file.	--
PKCS#12 Certificate	Click "Choose File" to locate the PKCS # 12 certificate file.	--
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show imported certificate's name.	Null

x509		
Item	**Description**	**Default**
X509 Settings		
File Size	Show size of certificate file.	Null
Last Modification	Show time of that last time to modify the certificate file.	Null

3.5.2 WireGuard

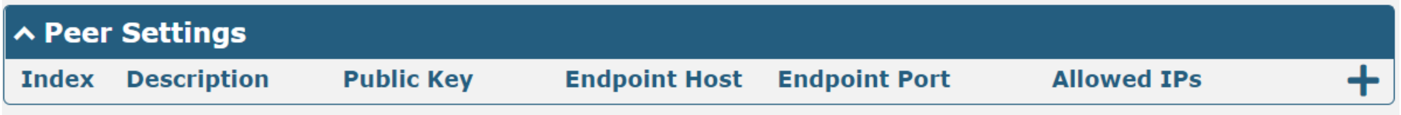
This section is used to set the parameters of WireGuard VPN, an open-source SSL-based VPN system. The device's WireGuard feature can support both point-to-point and point-to-multipoint VPN channels.
Click “**VPN> WireGuard”** to set the WireGuard parameters.



Enable WireGuard: ON OFF
Private Key:
IP Address:
Listen Port: 51820
MTU: 1472
Enable NAT: ON OFF

WireGuard@General Settings		
Item	**Descriptions**	**Default**
Enable WireGuard	Enable or disable WireGuard	OFF
Private Key	Enter local private key. It can be generated automatically or imported manually via X509 settings, but it cannot be empty.	Null
IP Address	Enter IP address of the virtual interface. It cannot be empty.	Null
Listen Port	Enter virtual interface listen port. It cannot be empty.	51820
MTU	Enter virtual interface slice size.	1472
Enable NAT	Enable/disable NAT feature. When enabled, the IP address will be converted to the interface virtual IP address.	ON

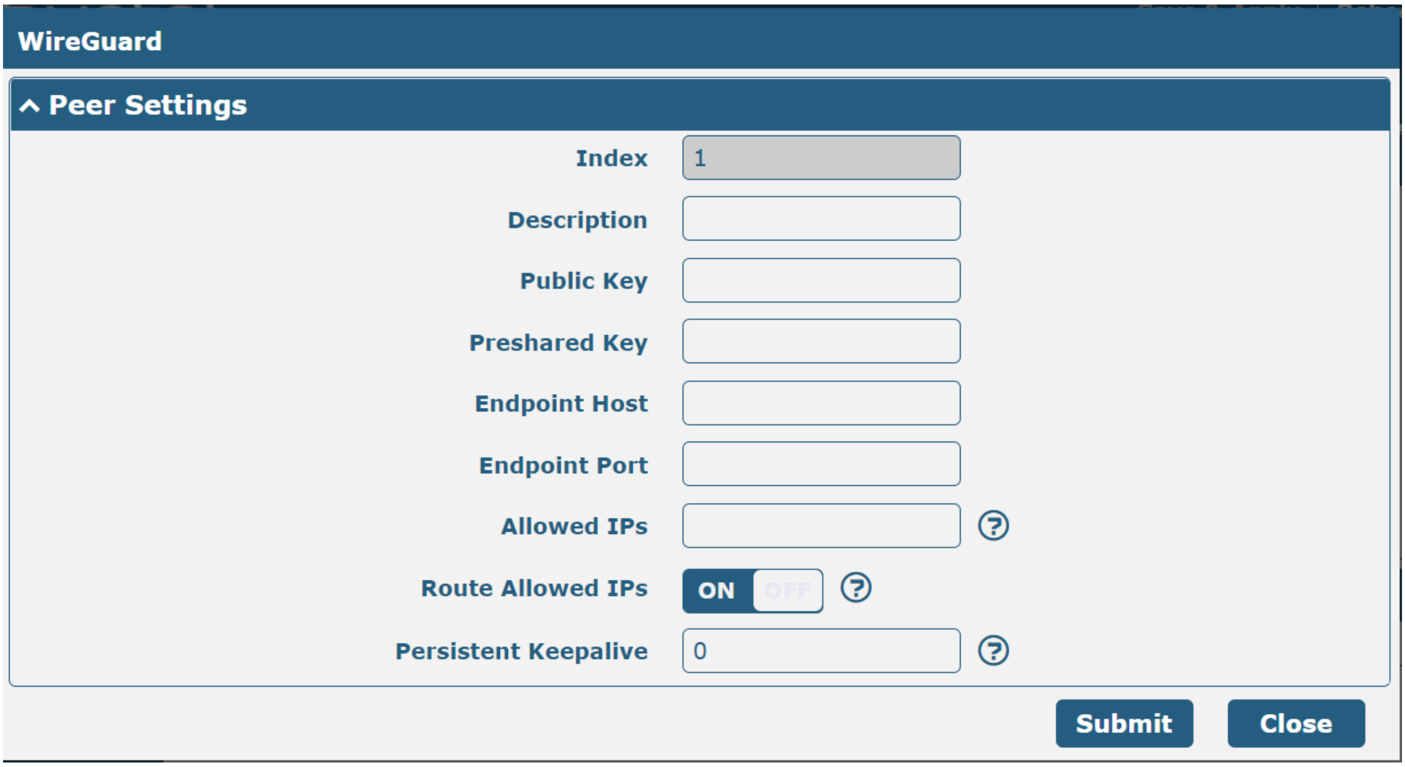
Note: Click ? for help.



^ Peer Settings

Index	Description	Public Key	Endpoint Host	Endpoint Port	Allowed IPs	+

Click + to add peer setting. The maximum count is **20**.



WireGuard

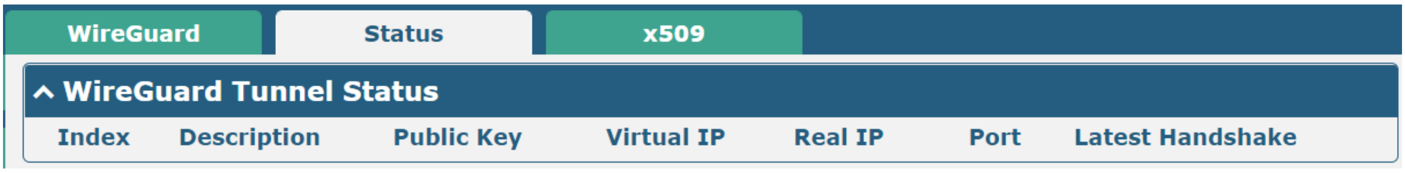
^ Peer Settings

Index	1
Description	
Public Key	
Preshared Key	
Endpoint Host	
Endpoint Port	
Allowed IPs	
Route Allowed IPs	ON
Persistent Keepalive	0

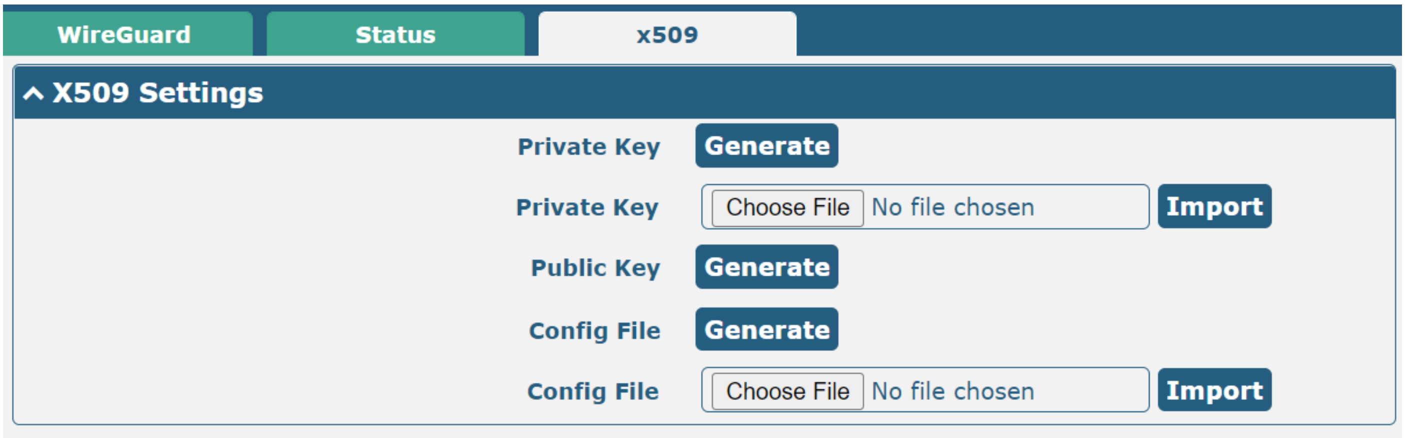
WireGuard@Peer Settings		
Item	**Descriptions**	**Default**
Peer Settings		
Index	Display index.	--
Description	Enter peer descriptions.	Null
Public Key	Enter public key and it cannot be empty.	Null
Preshared Key	Enter pre-share key and it cannot be empty.	Null
Endpoint Host	Enter peer IP address. A null value will not initiate a connection request.	Null
Endpoint Port	Enter peer port. A null value will not initiate a connection request.	Null
Allowed IPs	Enter allowed IP address, which cannot be empty.	Null
Route Allowed IPs	Enable/disable feature. When enabled, routes will be created for the networks allowed for this peer. If the allowed network is 0.0.0.0/0, this peer will be set as the default route.	ON
Persistent Keepalive	Enter interval of sending Persistent Keepalive messages, in seconds. 0 means disabling the feature.	0

Status

The status bar allows you to view WireGuard's connection status. Click on one of the rows and details of its link connection will be displayed below the current row.



This section is used to generate or import private and public keys.



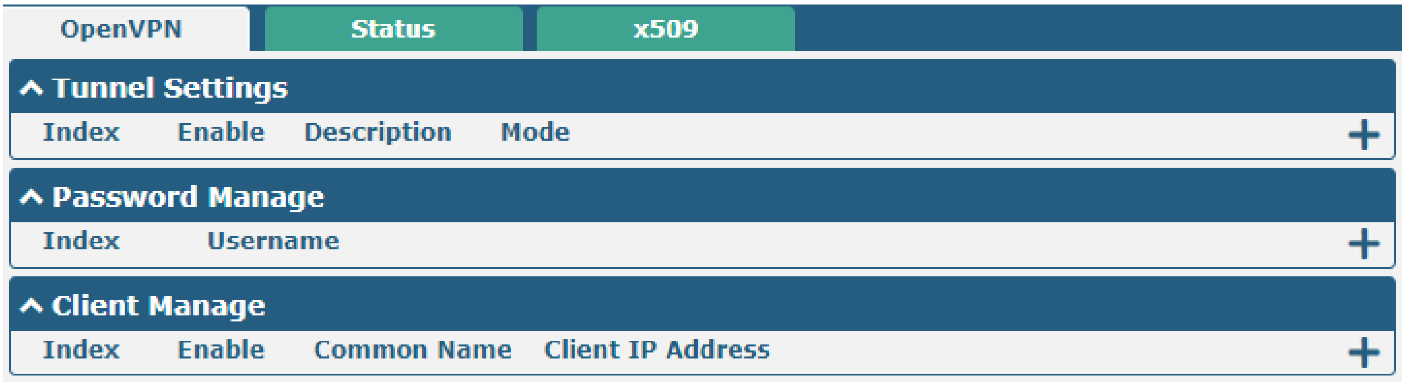
x509		
Item	**Descriptions**	**Default**
X509 Settings		
Private Key	Click Generate button to generate a private key.	--
Private Key	Click Choose File button to locate the private key from your computer, and then click Import button to import the private key.	--
Public Key	Click Generate button to generate a public key.	--
Config File	Click Generate button to generate a config file	--
Config File	Click Choose File button to locate the config file from your computer, and then click Import button to import the config file.	--

3.5.3 OpenVPN

This section allows you to set the OpenVPN and the related parameters. OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. The device supports point-to-point and point-to-point connections.

Click "**VPN > OpenVPN > OpenVPN**" to display as follows:

OpenVPN



Tunnel Settings

Index	Enable	Description	Mode

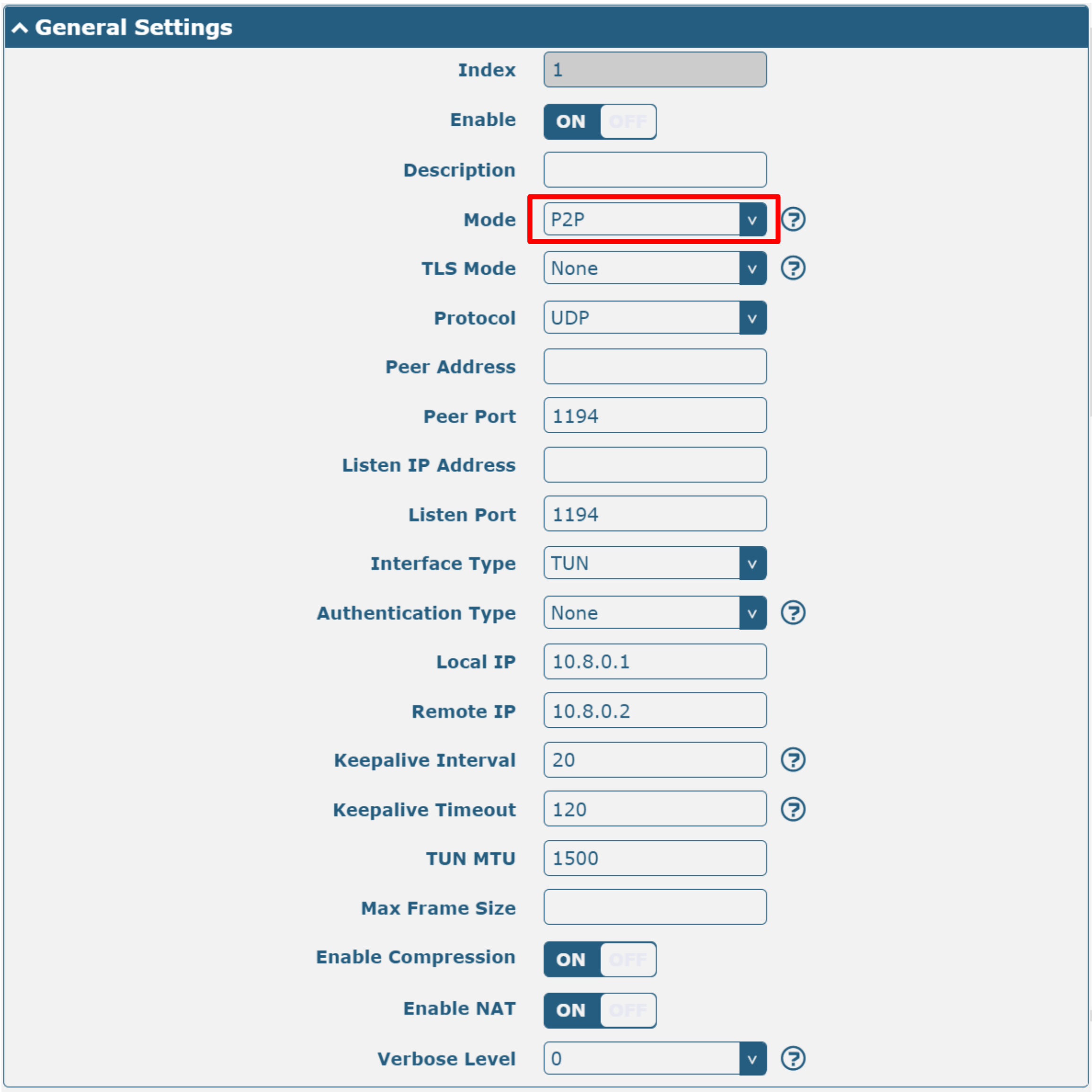
Password Manage

Index	Username

Client Manage

Index	Enable	Common Name	Client IP Address

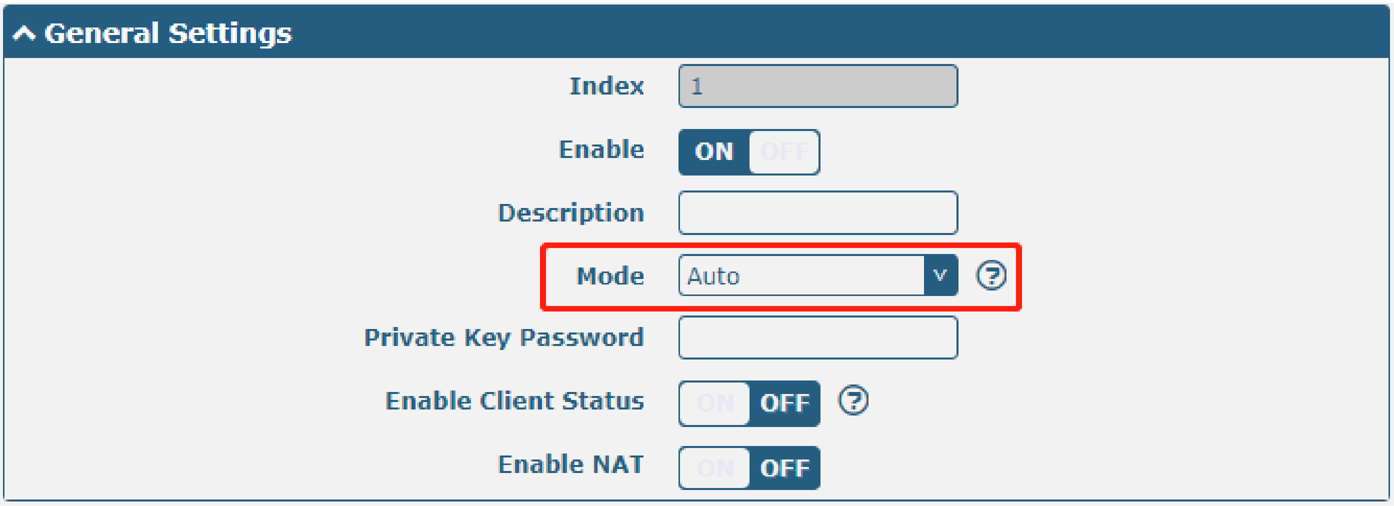
Click + to add OpenVPN tunnel settings. The maximum count is **5**. “Mode” is set “P2P” by default. The window is displayed below when choosing “P2P” as the mode.



General Settings

Index	1
Enable	ON
Description	
Mode	P2P
TLS Mode	None
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	ON
Verbose Level	0

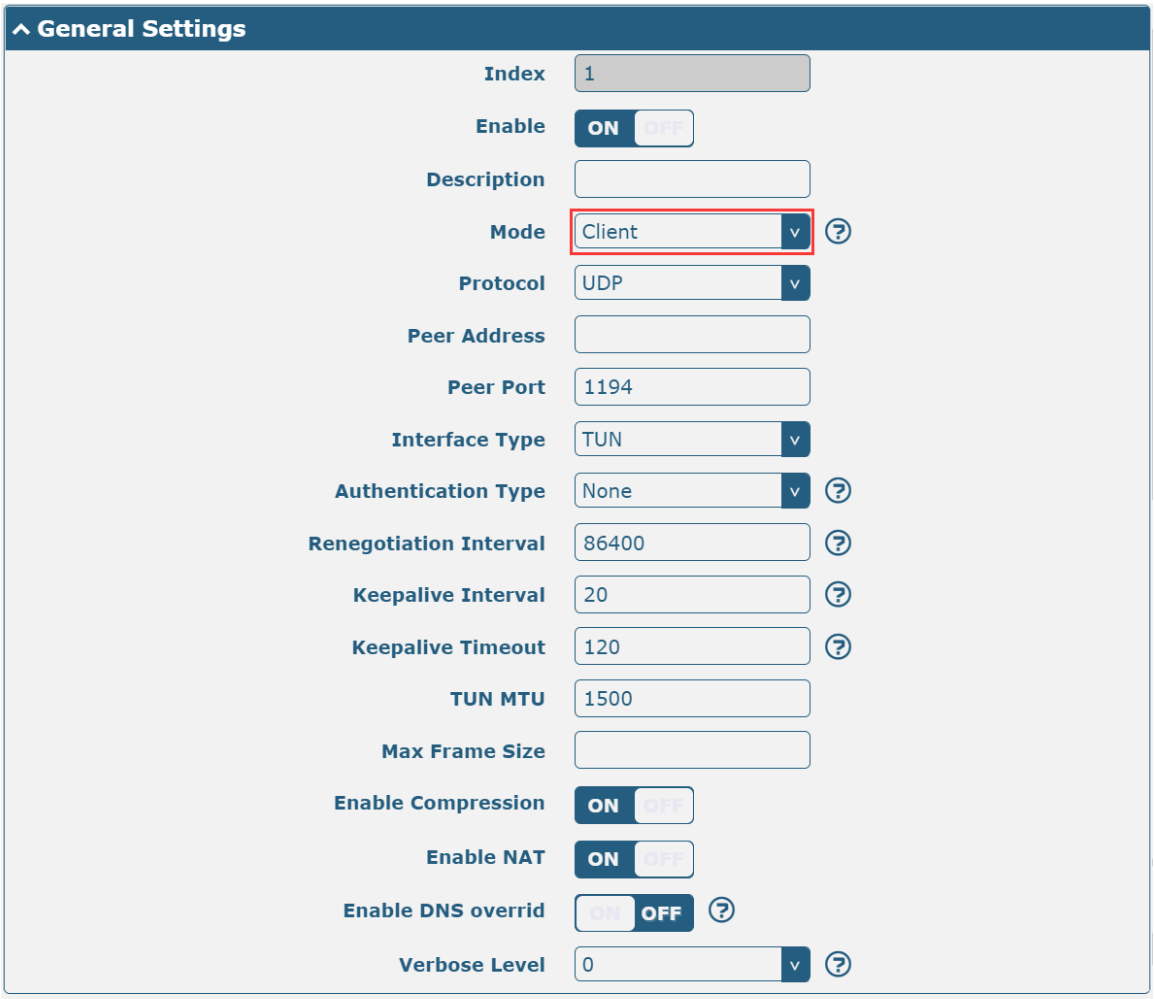
The window is displayed below when choosing “Auto” as the mode.



General Settings

Index	1
Enable	ON
Description	
Mode	Auto
Private Key Password	
Enable Client Status	OFF
Enable NAT	OFF

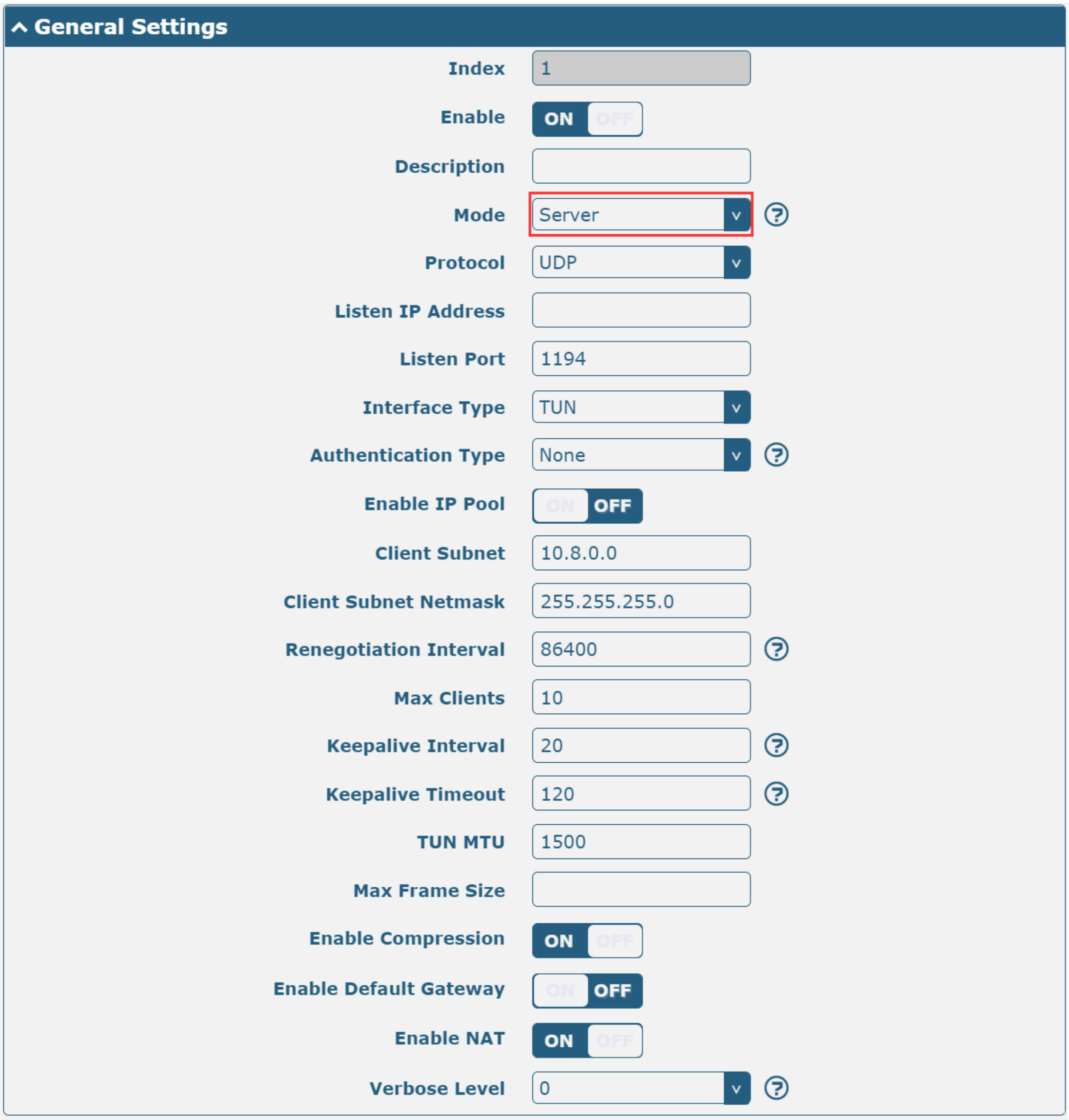
The window is displayed below when choosing “Client” as the mode.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	None
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	ON
Enable DNS overrid	OFF
Verbose Level	0

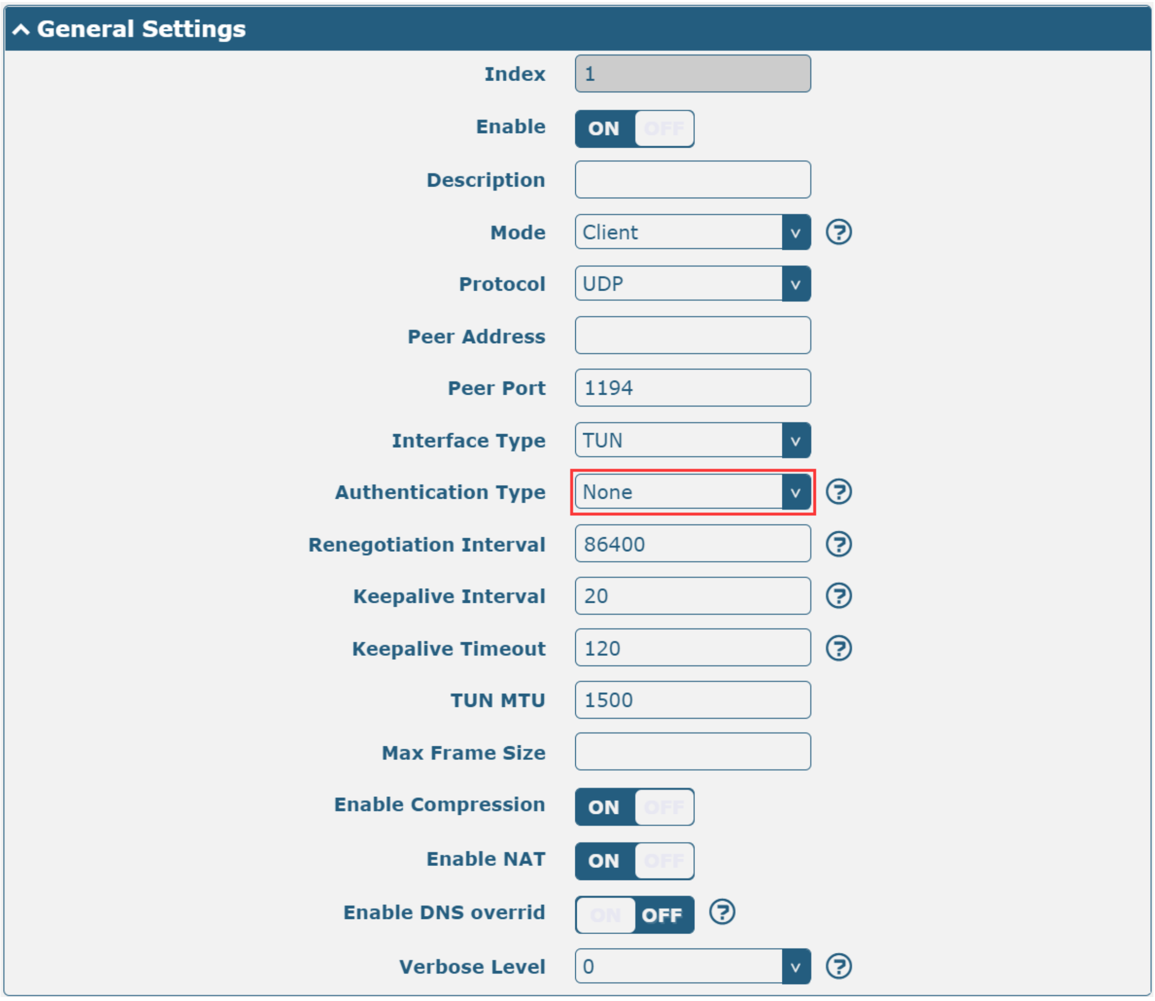
The window is displayed below when choosing "Server" as the mode.



General Settings

Index	1
Enable	ON
Description	
Mode	Server
Protocol	UDP
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	ON
Verbose Level	0

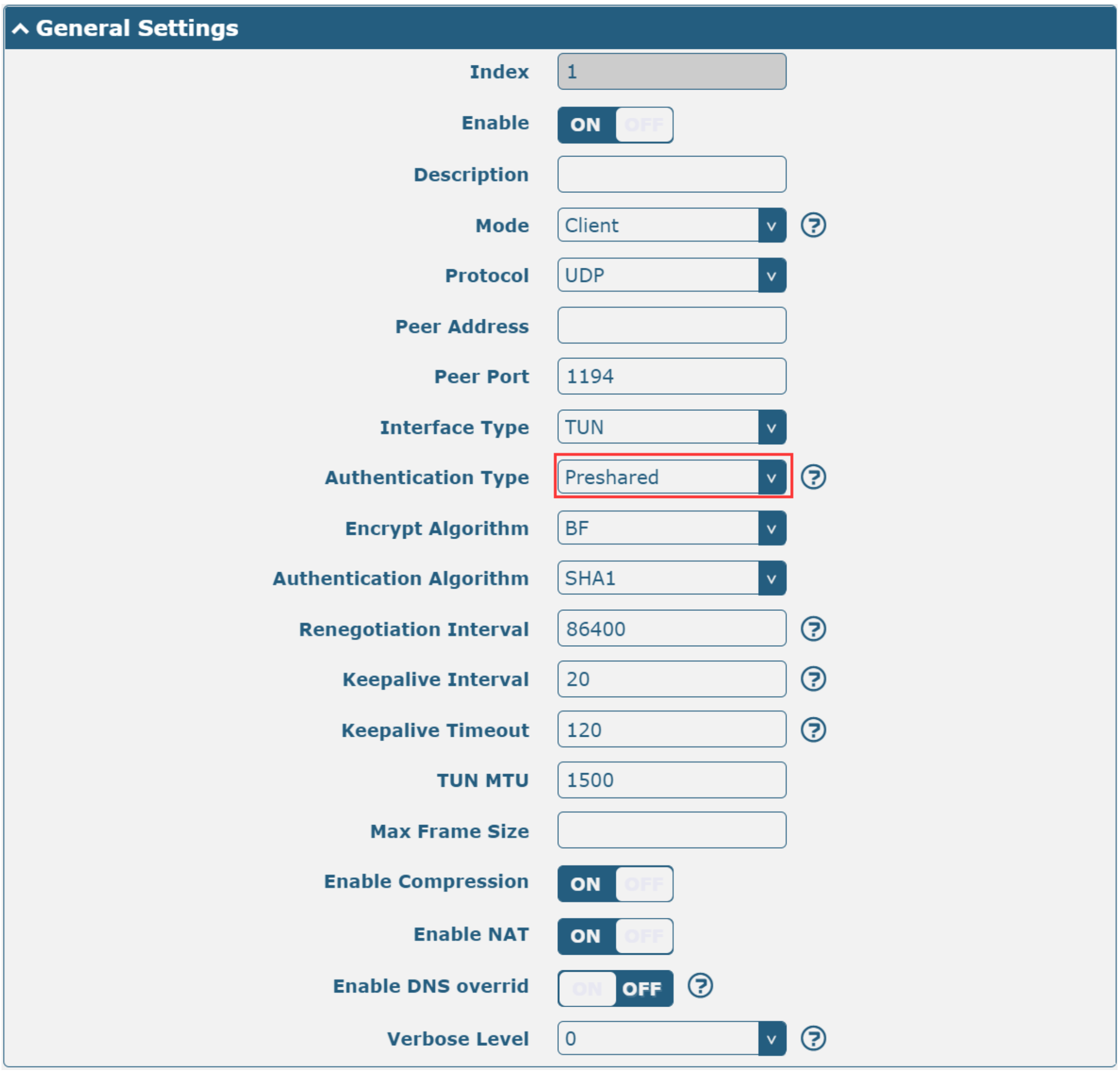
The window is displayed below when choosing "None" as the authentication type.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	None
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	ON
Enable DNS overrid	OFF
Verbose Level	0

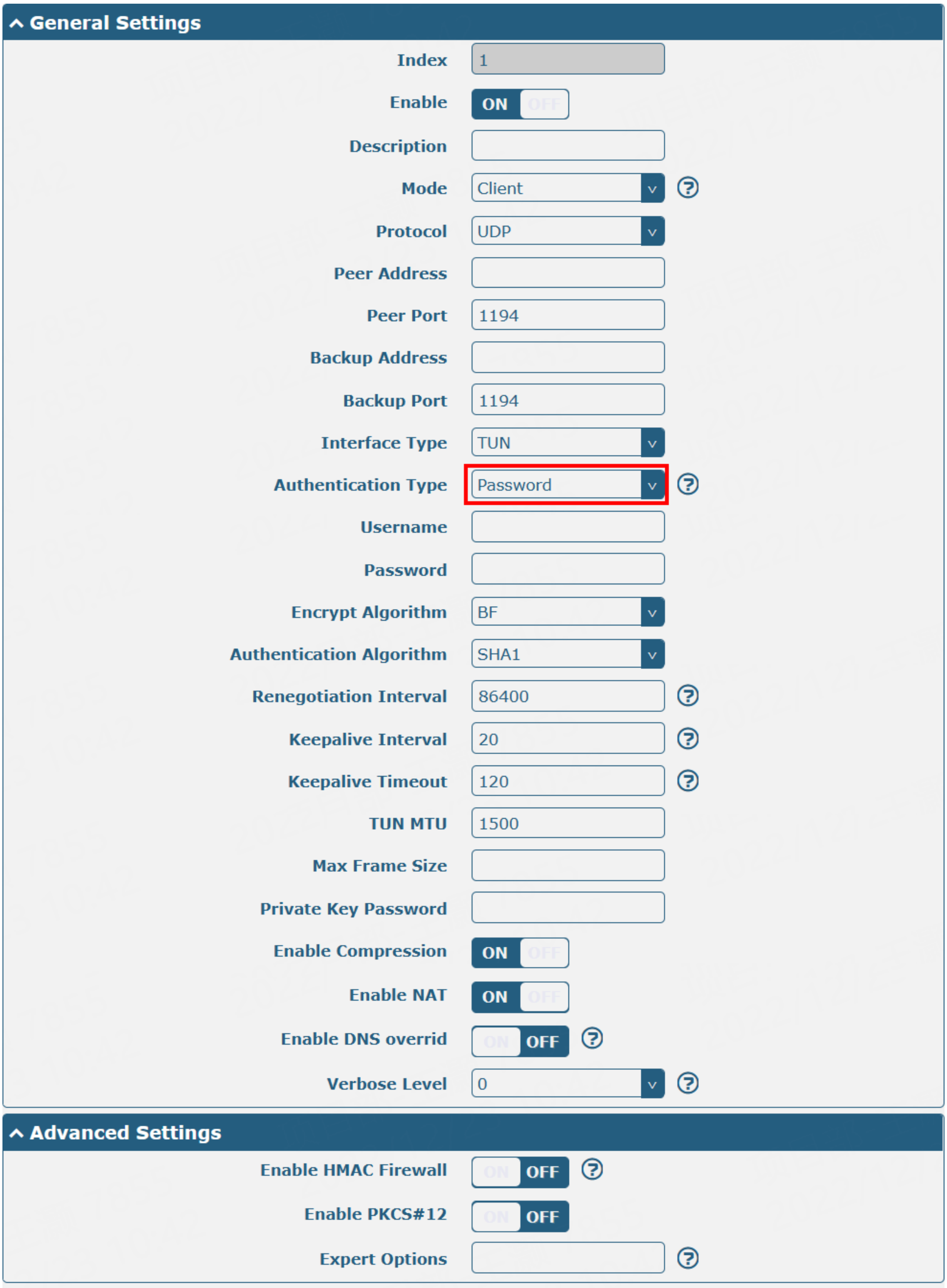
The window is displayed below when choosing “Preshared” as the authentication type.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	Preshared
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	ON
Enable DNS overrid	OFF
Verbose Level	0

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



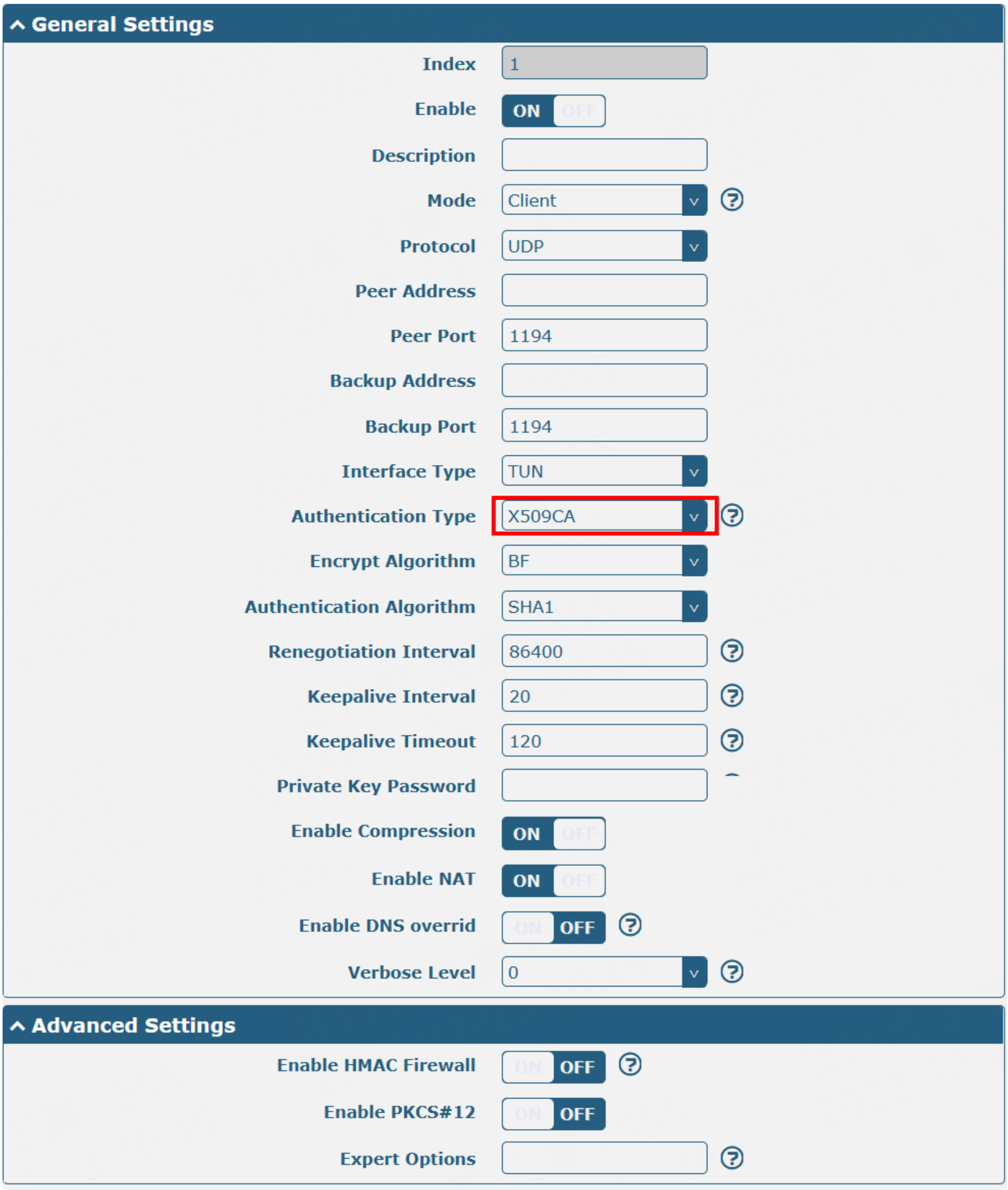
General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Backup Address	
Backup Port	1194
Interface Type	TUN
Authentication Type	Password
Username	
Password	
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	ON
Enable NAT	ON
Enable DNS overrid	OFF
Verbose Level	0

Advanced Settings

Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Expert Options	

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



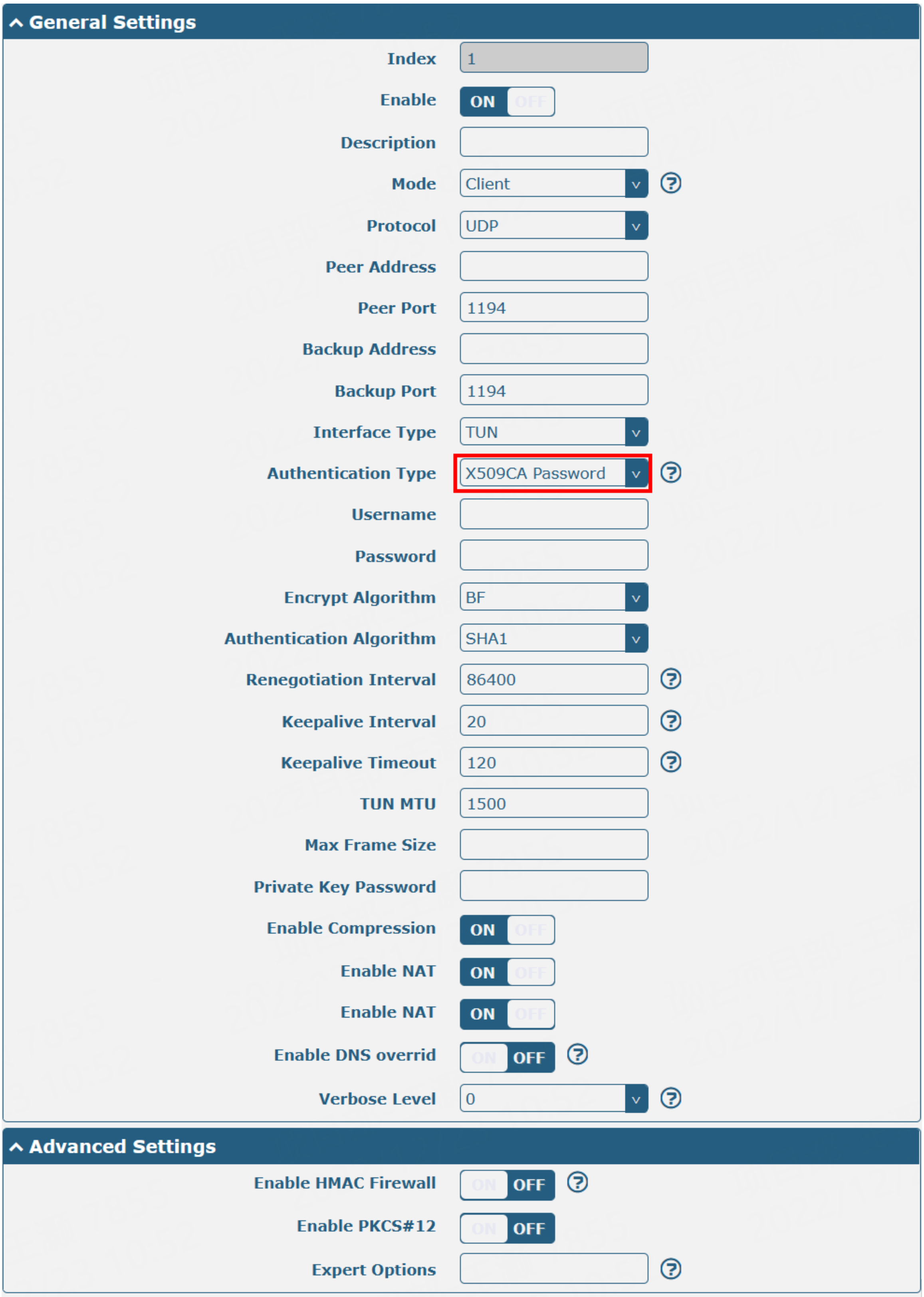
General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Backup Address	
Backup Port	1194
Interface Type	TUN
Authentication Type	X509CA
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Private Key Password	
Enable Compression	ON
Enable NAT	ON
Enable DNS overrid	OFF
Verbose Level	0

Advanced Settings

Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Expert Options	

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



^ General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Peer Address	
Peer Port	1194
Backup Address	
Backup Port	1194
Interface Type	TUN
Authentication Type	X509CA Password
Username	
Password	
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	ON
Enable NAT	ON
Enable NAT	ON
Enable DNS overrid	OFF
Verbose Level	0

^ Advanced Settings

Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Expert Options	

General Settings @ OpenVPN		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON

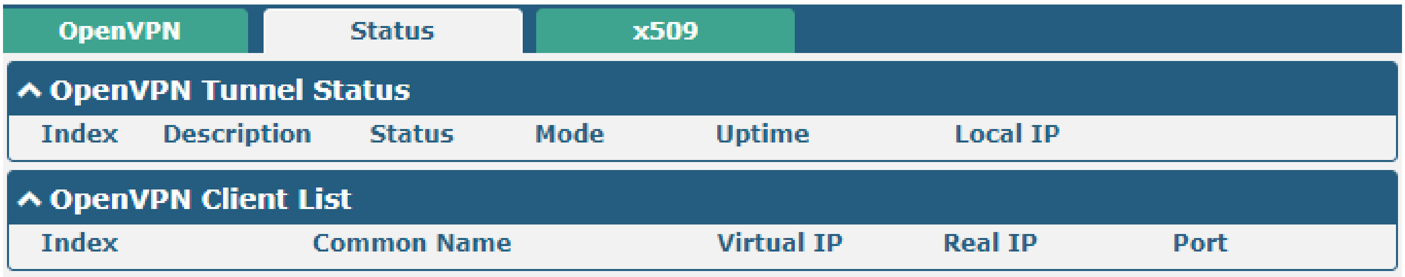
General Settings @ OpenVPN		
Item	**Description**	**Default**
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “Auto”, “P2P”, “Client” or “Server”.	P2P
Protocol	Select from “UDP”, “TCP-Client”, or “TCP-Server”.	UDP
Server Address	Enter end-to-end IP address or domain of remote OpenVPN server.	Null
Server Port	Enter end-to-end listener port or listener port of OpenVPN server.	1194
Listen IP Address	Enter IP address or domain name.	Null
Listen Port	Enter listener port at this end.	1194
Interface Type	Select from “TUN”, and “TAP” which are two different kinds of device interfaces for OpenVPN. The difference between TUN and TAP devices is that a TUN device is a point-to-point virtual device on the network while a TAP device is a virtual device on Ethernet.	TUN
Username	Enter username used for the “Password” or “X509CA Password” authentication type.	Null
Password	Enter password used for the “Password” or “X509CA Password” authentication type.	Null
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA”, and “X509CA Password”. ***Note***: *“None” and “Preshared” authentication types are only working with P2P mode.*	None
Enable IP Pool	Click the toggle button to enable/disable this option. When enabled, the client will obtain a virtual IP from the address pool. ***Note:*** *Enable IP Pool is available only “Mode” is Server.*	OFF
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Client Subnet	Client virtual IP network address.	10.8.0.0
Client Subnet Netmask	Client virtual IP network address mask.	255.255.255.0
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
Max Clients	Set retention timeout. If the connection continues to timeout during this time, the OpenVPN tunnel will be re-established. ***Note:*** *Max Clients is available only “Mode” is Server.*	10
Renegotiation Interval	Set renegotiation interval. If the connection failed, OpenVPN will renegotiate when the renegotiation interval is reached.	86400

General Settings @ OpenVPN		
Item	**Description**	**Default**
Keepalive Interval	Set a keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
TUN MTU	Set MTU for the tunnel.	1500
Max Frame Size	Set shard size of the data to be transmitted through the tunnel.	Null
Private Key Password	Enter private key password under "X509CA" and "X509CA password" authentication.	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 DNS override	Click the switch button to enable/disable this option. When enabled, DNS pushed by the server is received as the local DNS server.	OFF
Enable Bridge With LAN0	Click the toggle button to enable/disable this option. When enabled, the virtual interface can be bridged with Lan0. ***Note:*** *Enable Bridge with LAN0 available only "Mode" is Client.*	ON
Enable Default Gateway	Click the toggle button to enable/disable this option. When enabled, it will receive the gateway pushed by the server as the local gateway.	OFF
Enable Client Status	Click the toggle button to enable/disable this option. After the server is enabled, it can display the connected client status information.	OFF
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of the host behind the device 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

Advanced Settings @ OpenVPN		
Item	**Description**	**Default**
Enable HMAC Firewall	Click the toggle button to enable/disable this option. Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Click the toggle button to enable/disable the PKCS#12 certificate. It is an exchange of digital certificate encryption standards, used to describe personal identity information.	OFF
Enable nsCertType	Click the toggle button to enable/disable nsCertType. Require that the peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.	Null

Status

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



OpenVPN | Status | x509

^ OpenVPN Tunnel Status

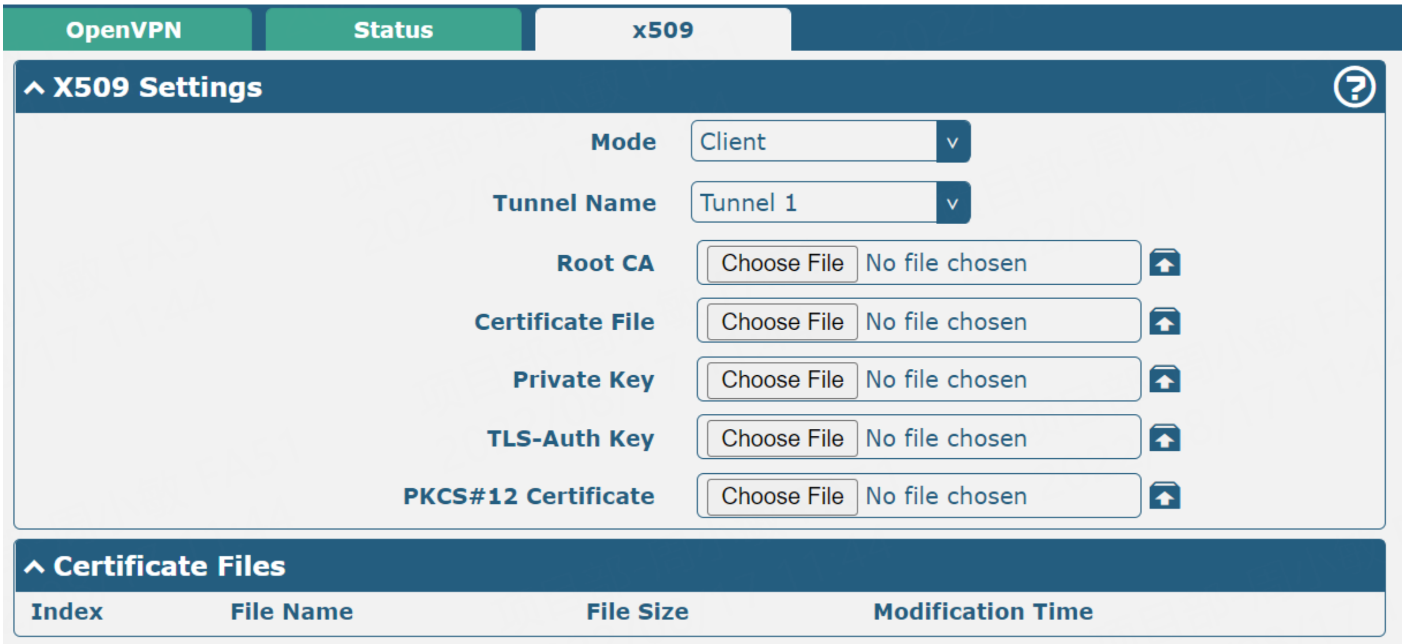
Index	Description	Status	Mode	Uptime	Local IP

^ OpenVPN Client List

Index	Common Name	Virtual IP	Real IP	Port

X509

This section is used to import the certificates such as CA.



OpenVPN | Status | x509

^ X509 Settings

Mode: Client

Tunnel Name: Tunnel 1

Root CA: Choose File No file chosen

Certificate File: Choose File No file chosen

Private Key: Choose File No file chosen

TLS-Auth Key: Choose File No file chosen

PKCS#12 Certificate: Choose File No file chosen

^ Certificate Files

Index	File Name	File Size	Modification Time

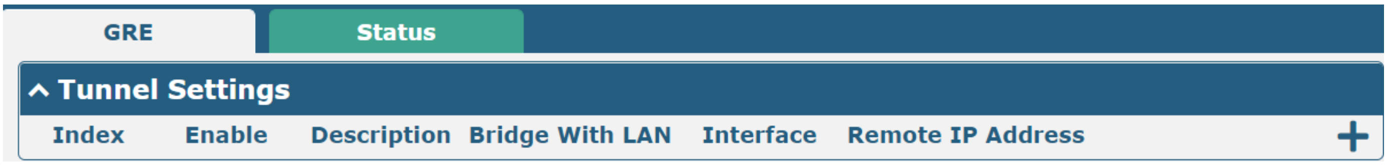
x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3", "Tunnel 4", "Tunnel 5”, or "Tunnel 6".	Tunnel 1
Mode	The mode selected in Tunnel	Client
Root CA	Click “Choose File” to locate Root CA file and then import this file 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.	--
TLS-Auth Key	Click “Choose File” to locate TLS-Auth Key file, and then import this file into	--

x509		
Item	**Description**	**Default**
X509 Settings		
	your device.	
PKCS#12 Certificate	Click "Choose File" to locate the PKCS#12 Certificate 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

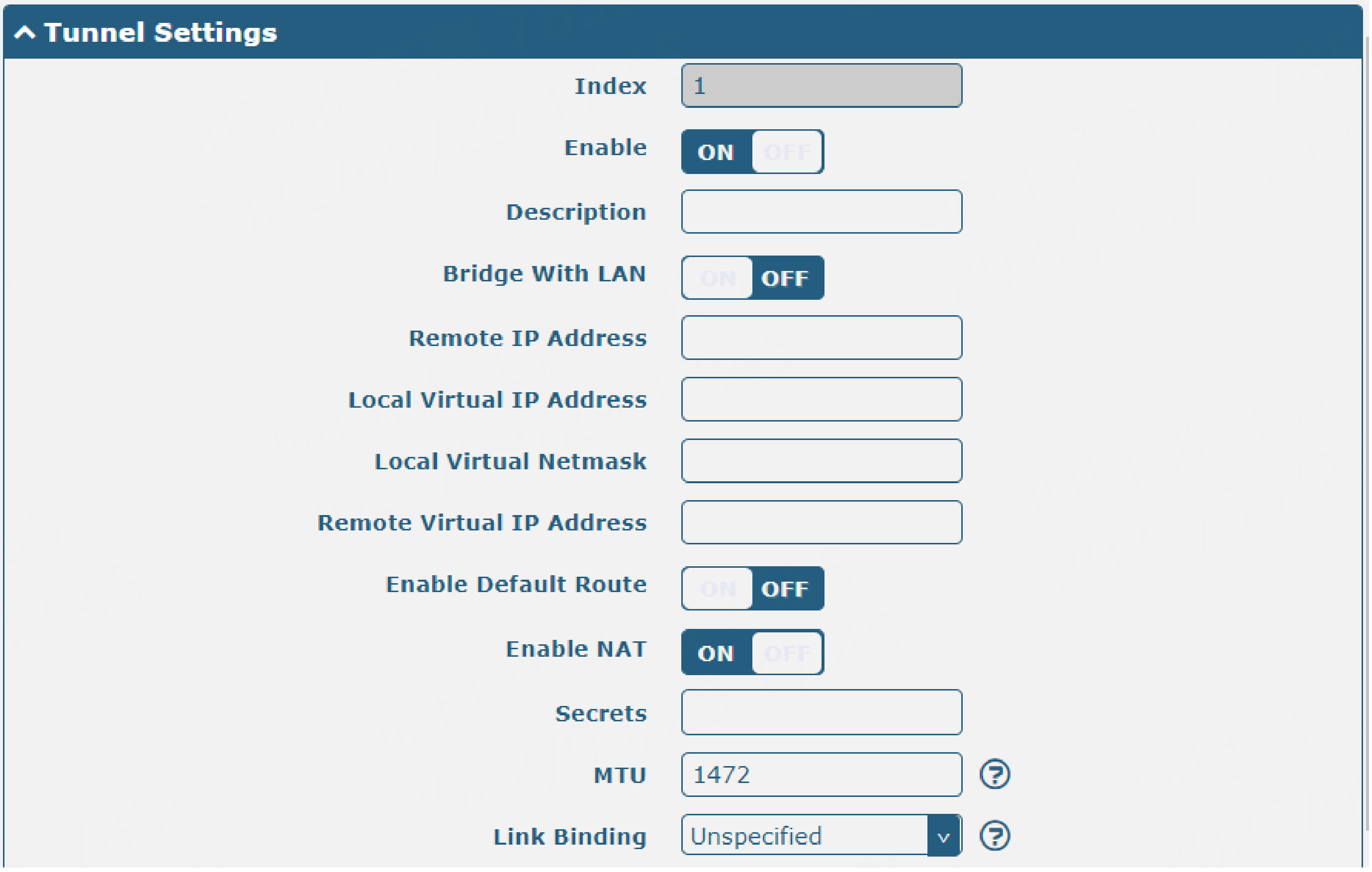
3.5.4 GRE

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**.



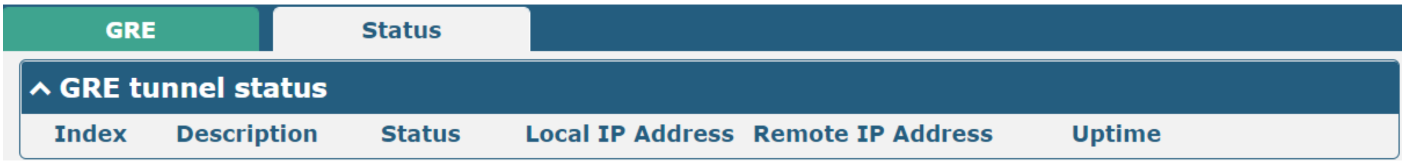
^ Tunnel Settings

Index	1
Enable	ON
Description	
Bridge With LAN	OFF
Remote IP Address	
Local Virtual IP Address	
Local Virtual Netmask	
Remote Virtual IP Address	
Enable Default Route	OFF
Enable NAT	ON
Secrets	
MTU	1472
Link Binding	Unspecified

Tunnel Settings @ GRE		
Item	**Description**	**Default**
Index	Indicate ordinal of 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
Bridge with LAN	Click the toggle button to enable/disable this option. When enabled, the virtual interface can be bridged with lan0.	OFF
Remote IP Address	Set remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask	Set local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set 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 gateway will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when the device is under a NAT environment.	ON
Secrets	Set key to the GRE tunnel.	Null
MTU	Enter Maximum Transmission Unit.	1472
Link Binding	Select link to build GRE.	Unbound

Status

This section allows you to view the GRE tunnel status.



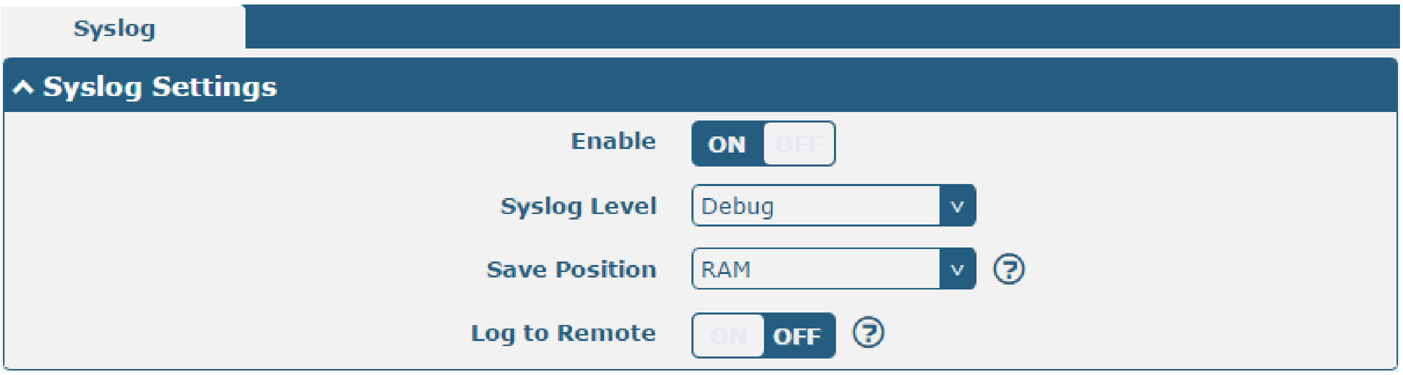
GRE tunnel status

Index	Description	Status	Local IP Address	Remote IP Address	Uptime

3.6 Services

3.6.1 Syslog

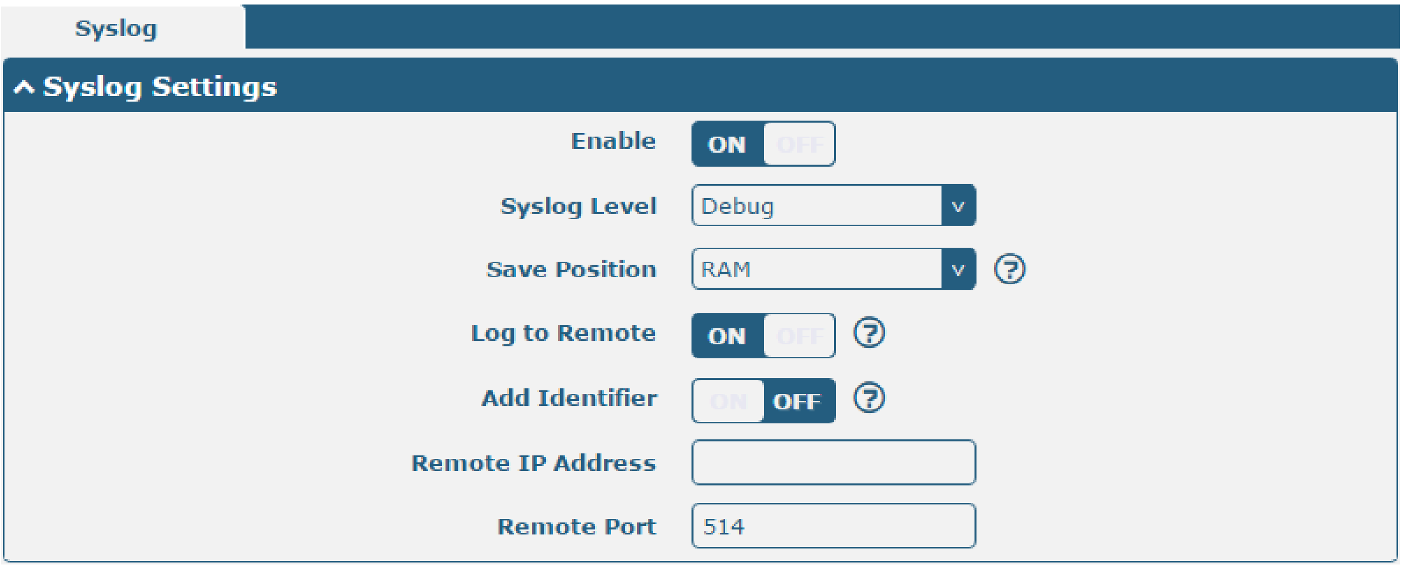
This section allows you to set the Syslog parameters. The system log of the device can be saved in the local, also supports to be sent to remote log server and specified application debugging. By default, the "Log to Remote" option is disabled.



Syslog Settings

Enable	ON
Syslog Level	Debug
Save Position	RAM
Log to Remote	OFF

The window is displayed below when enabling the "Log to Remote" option.



Syslog Settings

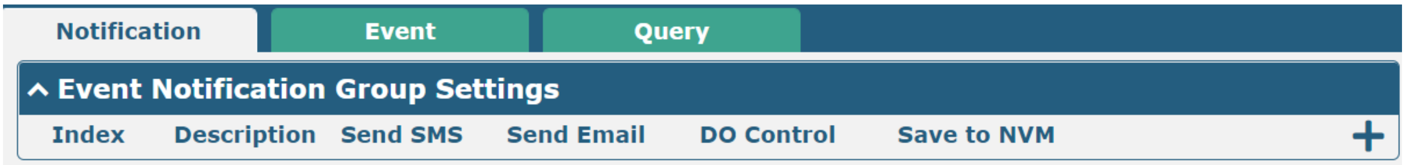
Enable	ON
Syslog Level	Debug
Save Position	RAM
Log to Remote	ON
Add Identifier	OFF
Remote IP Address	
Remote Port	514

Syslog Settings		
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 detail.	Debug
Save Position	Select save position from “RAM”, “NVM” or “Console”. The data will be cleared after reboot when choosing “RAM”. ***Note****: It's not recommended that you save Syslog to NVM (Non-Volatile Memory) for a long time.*	RAM
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow device sending Syslog to the remote Syslog server. You need to enter the IP and Port of the Syslog server.	OFF
Add Identifier	Click the toggle button to enable/disable this option. When enabled, you can add a serial number to the Syslog message which is used for loading Syslog to RobustLink.	OFF
Remote IP Address	Enter IP address of the Syslog server when enabling the “Log to Remote” option.	Null
Remote Port	Enter port of the Syslog server when enabling the “Log to Remote” option.	514

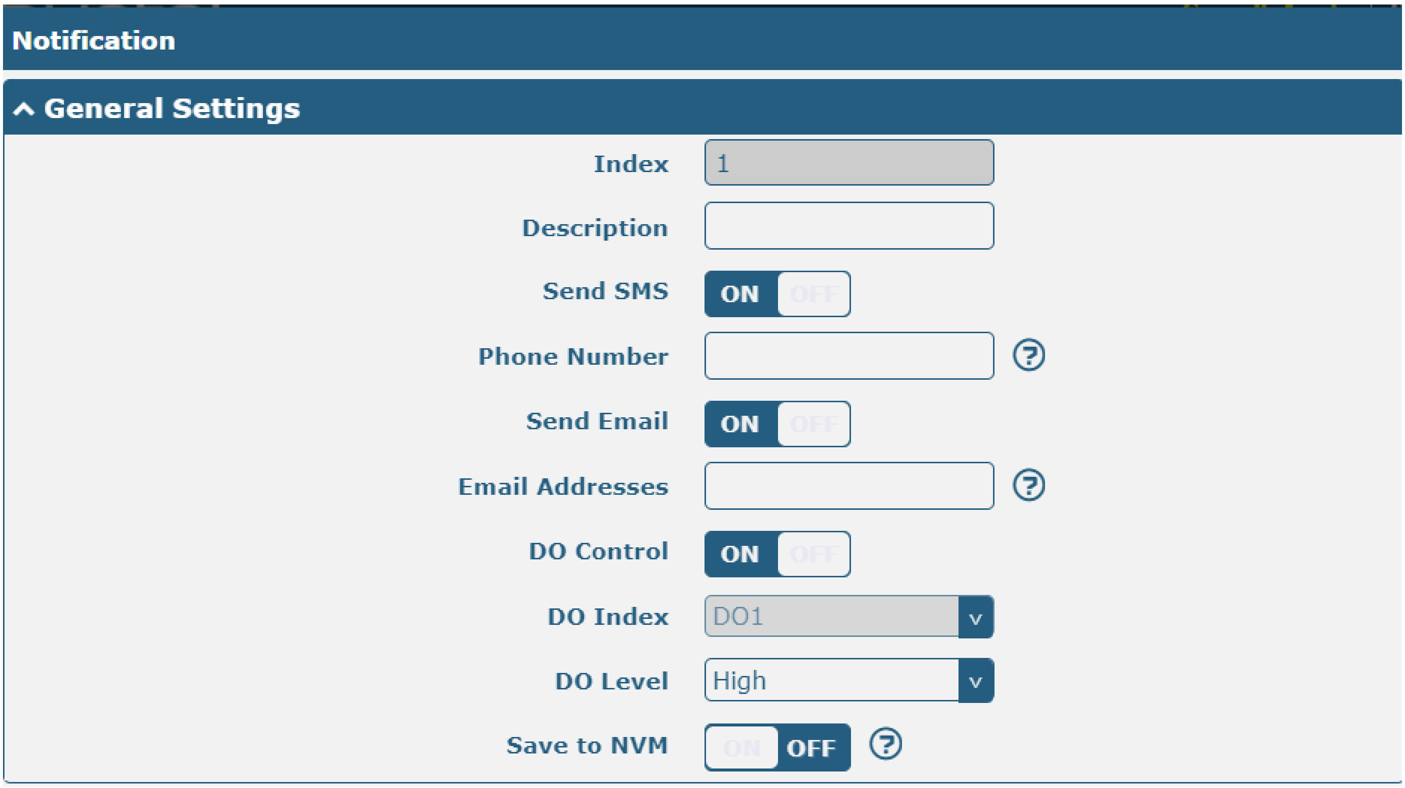
3.6.2 Event

This section allows you to set the event parameters. The event feature is able to send alerts by SMS or Email when certain system events occur.

Notification



Click + button to add an Event parameter.

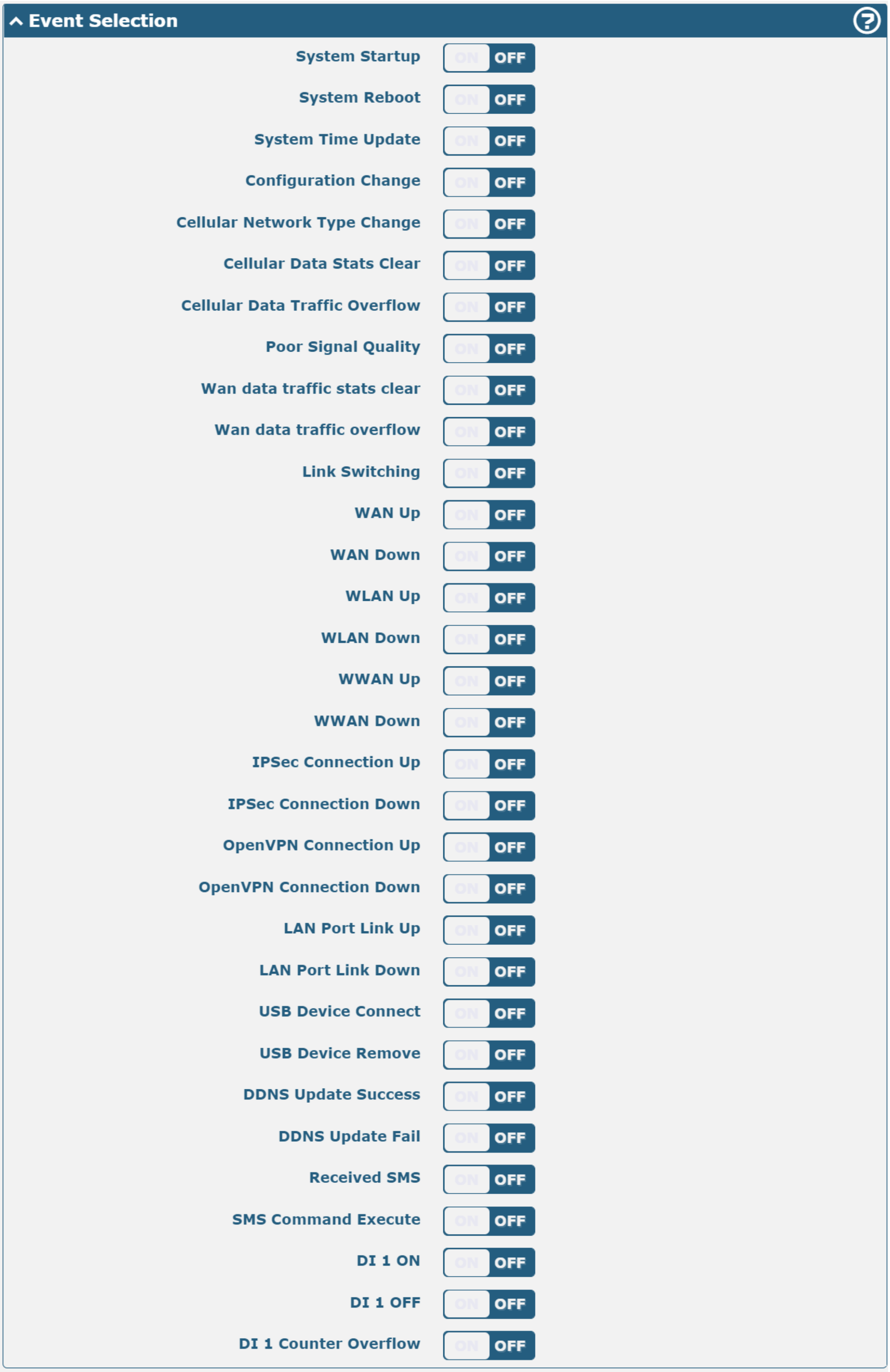


Notification

General Settings

Index	1
Description	
Send SMS	ON
Phone Number	
Send Email	ON
Email Addresses	
DO Control	ON
DO Index	DO1
DO Level	High
Save to NVM	OFF

General Settings @ Notification		
Item	**Description**	**Default**
Index	Indicate ordinal of list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the device will send a notification to the specified phone numbers via SMS if an event occurs. Set the related phone number in "**3.6.5 Services > Email**", and use ';' to separate each number.	OFF
Send Email	Click the toggle button to enable/disable this option. When enabled, the device will send a notification to the specified email box via email if an event occurs. Set the related email address in "**3.6.5 Services > Email**".	OFF
DO Control	Click the toggle button to enable/disable this option. After it is turned on, the event device 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 the event to nonvolatile memory.	OFF

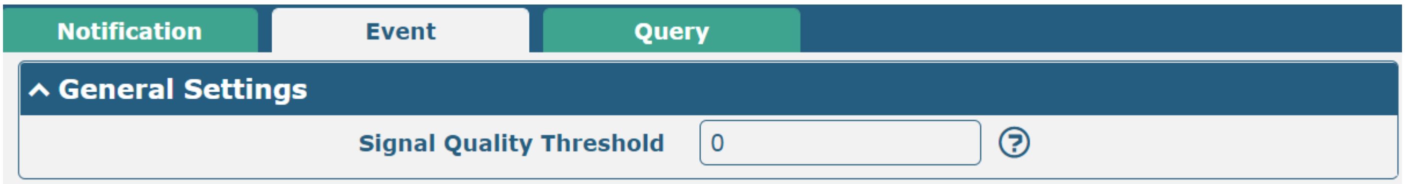


^ Event Selection

System Startup	OFF
System Reboot	OFF
System Time Update	OFF
Configuration Change	OFF
Cellular Network Type Change	OFF
Cellular Data Stats Clear	OFF
Cellular Data Traffic Overflow	OFF
Poor Signal Quality	OFF
Wan data traffic stats clear	OFF
Wan data traffic overflow	OFF
Link Switching	OFF
WAN Up	OFF
WAN Down	OFF
WLAN Up	OFF
WLAN Down	OFF
WWAN Up	OFF
WWAN Down	OFF
IPSec Connection Up	OFF
IPSec Connection Down	OFF
OpenVPN Connection Up	OFF
OpenVPN Connection Down	OFF
LAN Port Link Up	OFF
LAN Port Link Down	OFF
USB Device Connect	OFF
USB Device Remove	OFF
DDNS Update Success	OFF
DDNS Update Fail	OFF
Received SMS	OFF
SMS Command Execute	OFF
DI 1 ON	OFF
DI 1 OFF	OFF
DI 1 Counter Overflow	OFF

Event

This section allows you to set the event.



Signal Quality Threshold: 0

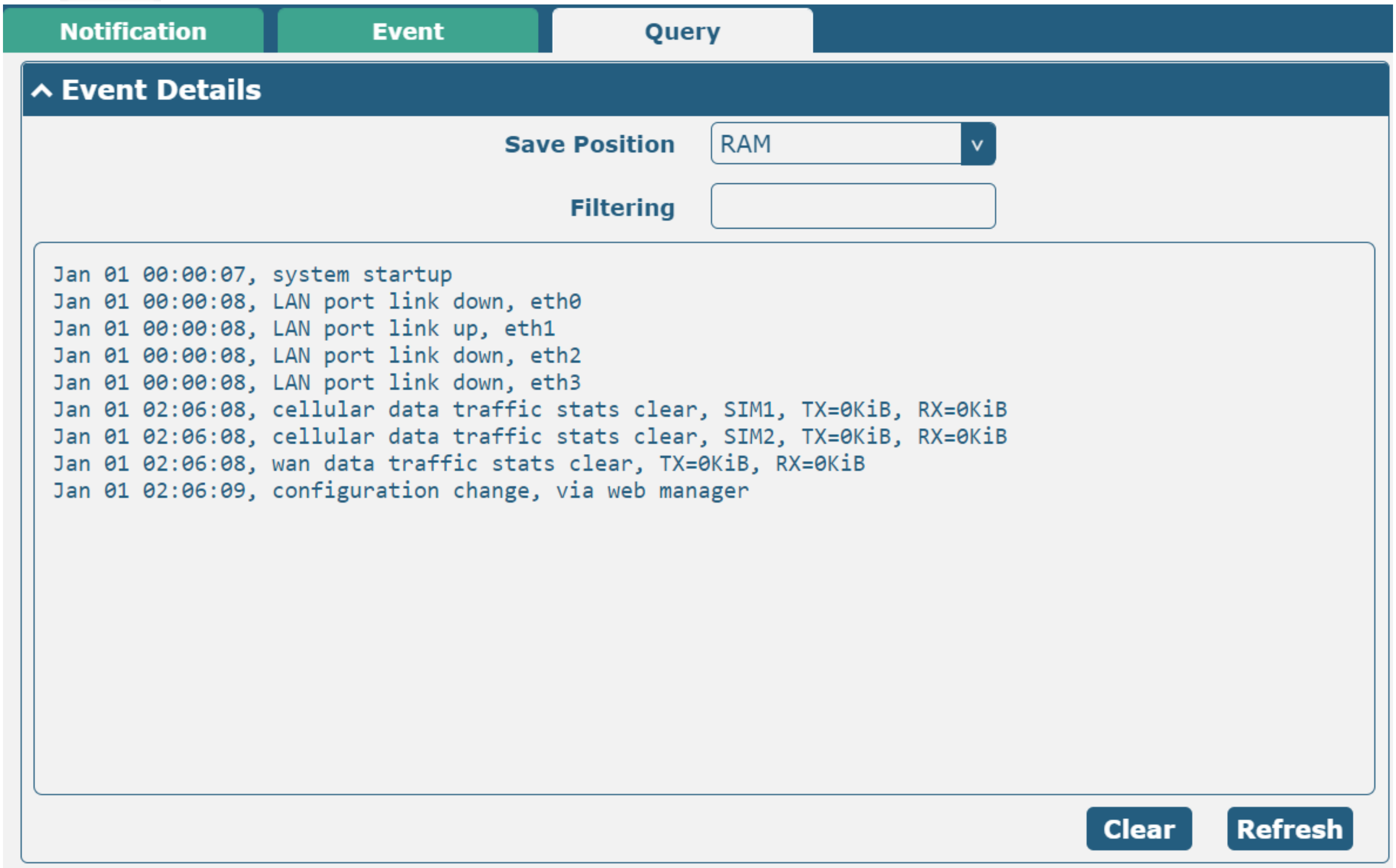
General Settings @ Event		
Item	**Description**	**Default**
Signal Quality Threshold	Set threshold for signal quality. The device will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0

Query

In the following window, you can query various types of event records.

Click Refresh to query filtered events.

Click Clear to clear the event records in the window.



Save Position: RAM

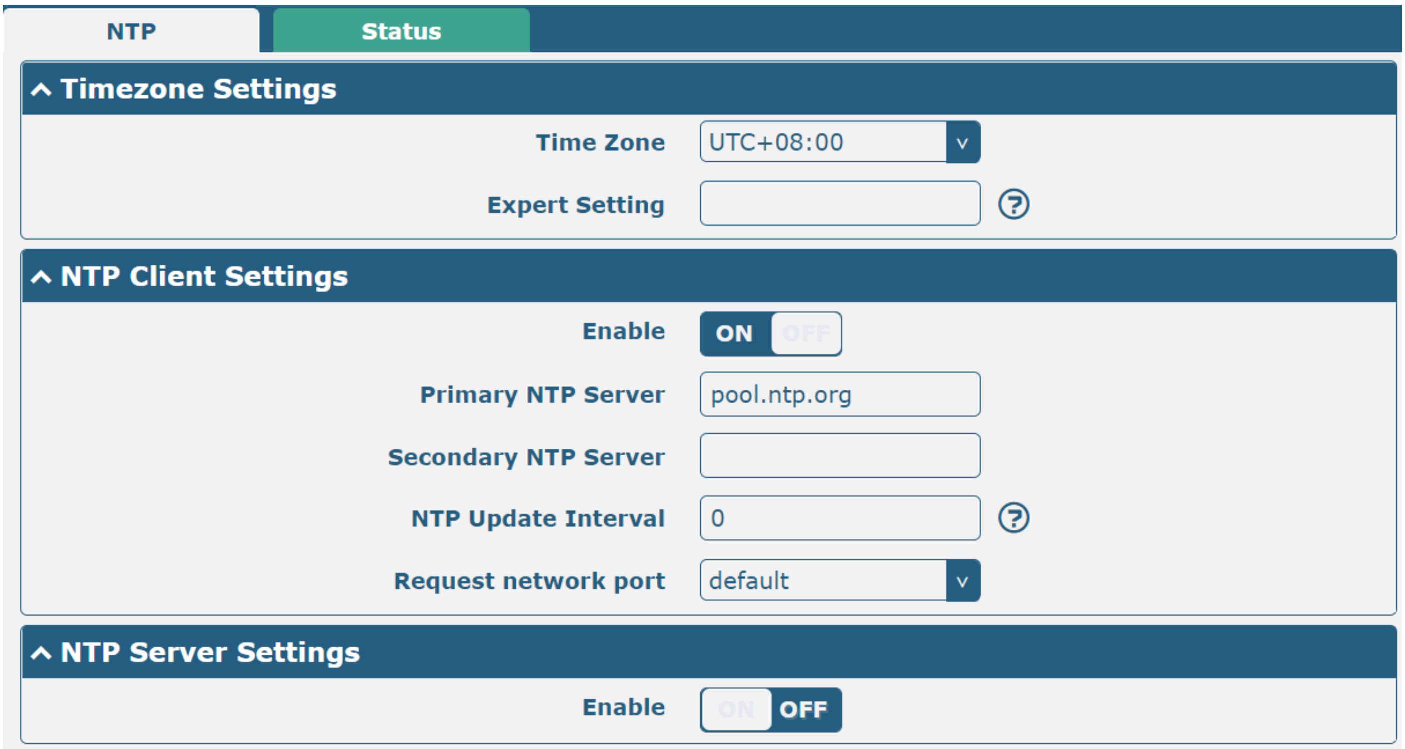
Filtering:

```
Jan 01 00:00:07, system startup
Jan 01 00:00:08, LAN port link down, eth0
Jan 01 00:00:08, LAN port link up, eth1
Jan 01 00:00:08, LAN port link down, eth2
Jan 01 00:00:08, LAN port link down, eth3
Jan 01 02:06:08, cellular data traffic stats clear, SIM1, TX=0KiB, RX=0KiB
Jan 01 02:06:08, cellular data traffic stats clear, SIM2, TX=0KiB, RX=0KiB
Jan 01 02:06:08, wan data traffic stats clear, TX=0KiB, RX=0KiB
Jan 01 02:06:09, configuration change, via web manager
```

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

3.6.3 NTP

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



^ Timezone Settings

Time Zone: UTC+08:00

Expert Setting:

^ NTP Client Settings

Enable: ON

Primary NTP Server: pool.ntp.org

Secondary NTP Server:

NTP Update Interval: 0

Request network port: default

^ NTP Server Settings

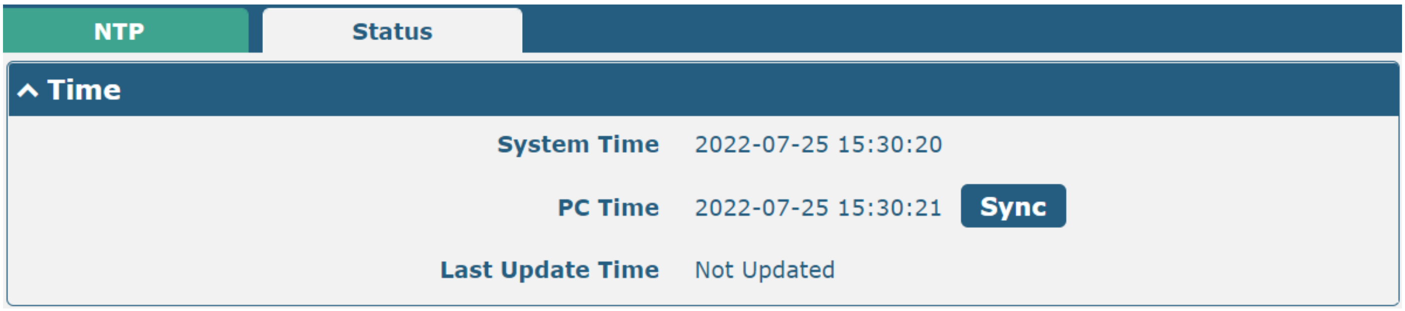
Enable: OFF

NTP		
Item	**Description**	**Default**
Time zone Settings		
Time Zone	Click the drop-down list to select the time zone you are in.	UTC +08:00
Expert Setting	Specify time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
NTP Client Settings		
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 interval (minutes) synchronizing the NTP client time with the NTP servers. Minutes wait for the next update, and 0 means update only once.	0

Request network port	Select Request network port from "default" or "lan".	default
NTP Server Settings		
Enable	Click the toggle button to enable/disable the NTP server option.	OFF

Status

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



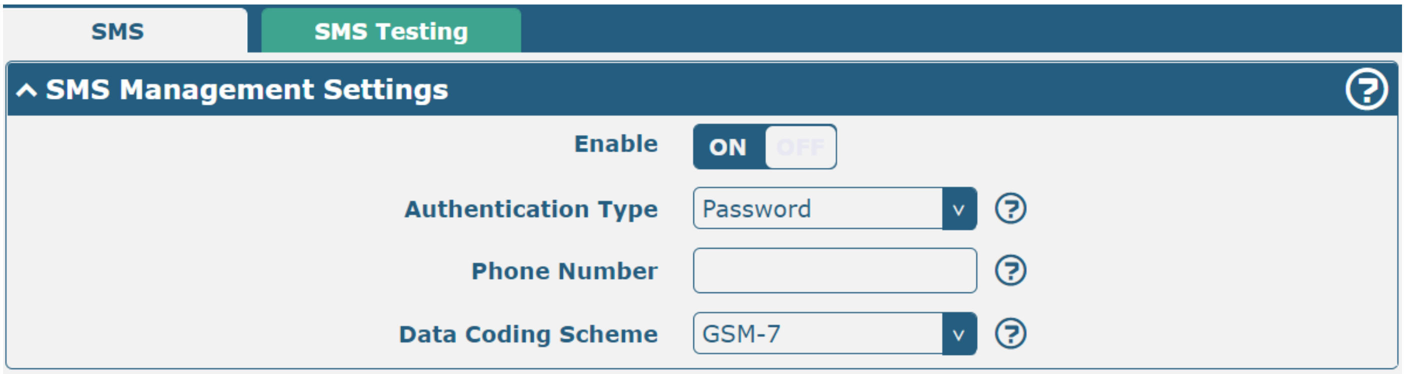
System Time 2022-07-25 15:30:20

PC Time 2022-07-25 15:30:21

Last Update Time Not Updated

3.6.4 SMS

This section allows you to set SMS parameters. The device supports SMS management, and users can control and configure their devices by sending SMS. For more details about SMS control, refer to [4.1.2 SMS Remote Control](#).



Enable: ON

Authentication Type: Password

Phone Number:

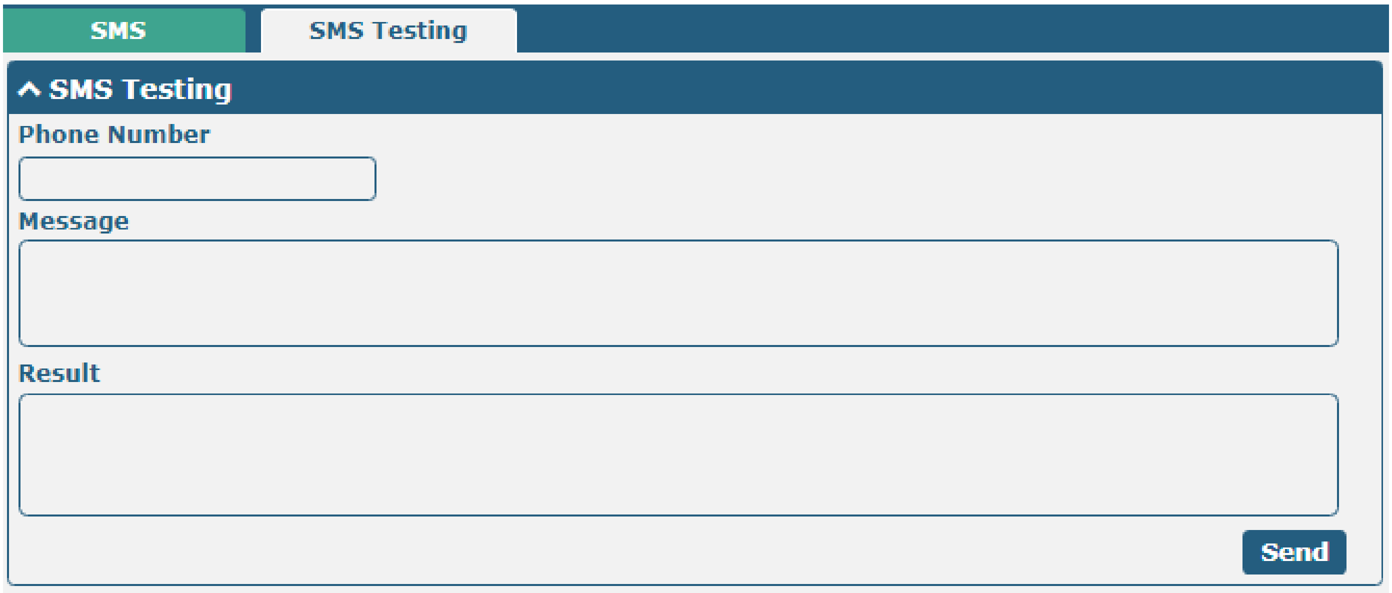
Data Coding Scheme: GSM-7

SMS Management Settings		
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: Use the same username and password as the WEB manager for authentication. For example, the format of the SMS should be "username: password; cmd1; cmd2; …" ***Note:*** *Set WEB manager password in the* ***System > User Management*** *section.* • Phonenum: Use the Phone number for authentication, and the 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. The	Password

	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 phone number used for SMS management, and use '; 'to separate each number. ***Note**: It can be null when choosing "Password" as the authentication type.*	Null
Data Coding Scheme	Select Data Coding Scheme from "GSM-7" or "ucs2".	GSM-7

SMS Testing

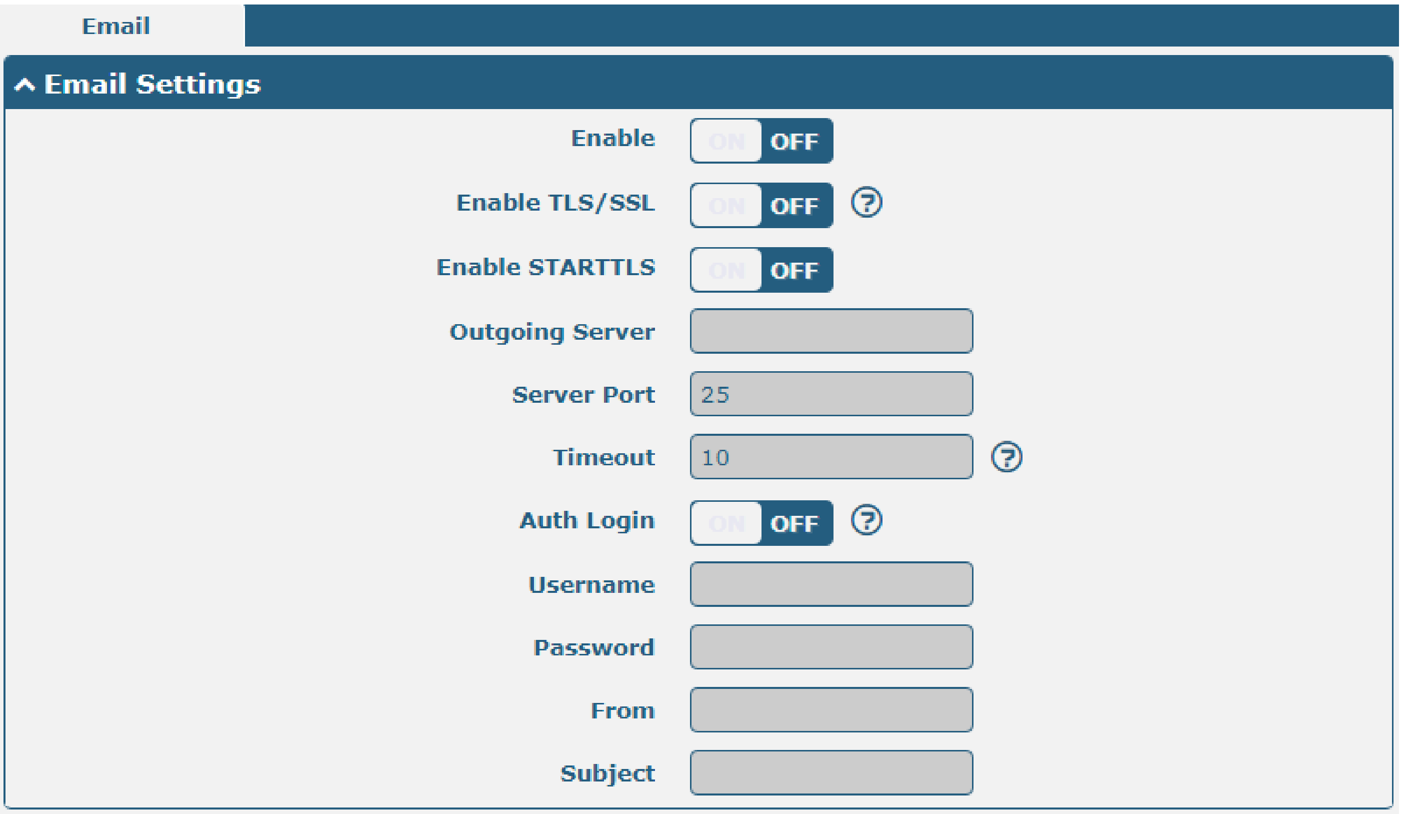
This section allows you to test the current SMS service whether is available.



SMS Testing		
Item	**Description**	**Default**
Phone Number	Enter specified phone number which can receive the SMS from the device.	Null
Message	Enter message that the device will send 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.	--

3.6.5 Email

The email function supports sending the event notifications to the specified recipient by way of an email.



Enable	ON OFF
Enable TLS/SSL	ON OFF
Enable STARTTLS	ON OFF
Outgoing Server	
Server Port	25
Timeout	10
Auth Login	ON OFF
Username	
Password	
From	
Subject	

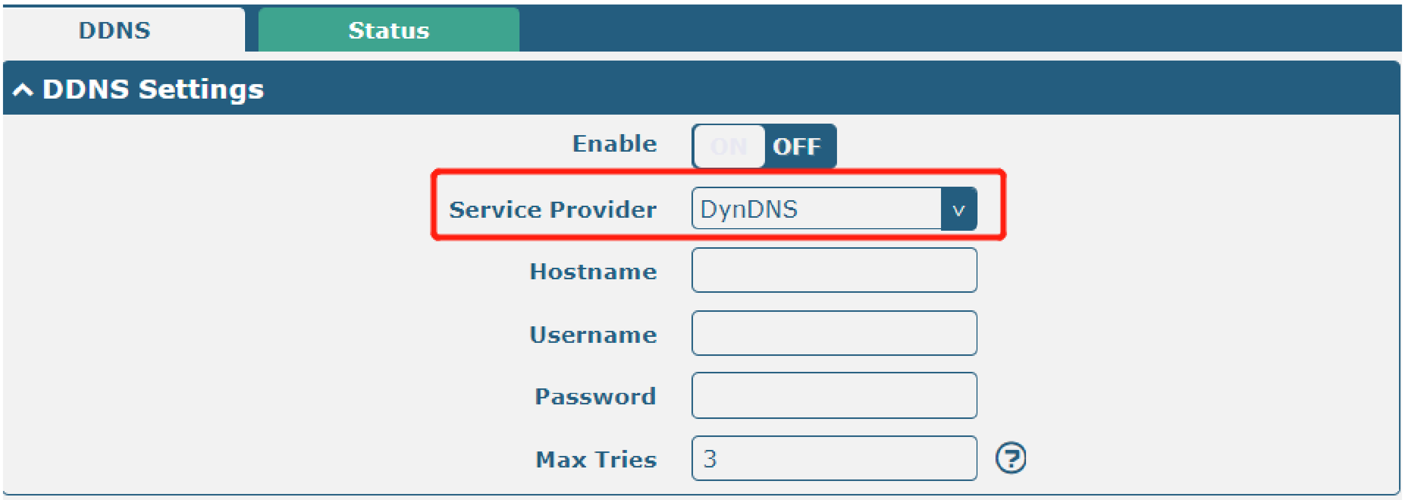
Email Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Enable STARTTLS	Click the toggle button to enable/disable STARTTLS encryption.	OFF
Outgoing server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

3.6.6 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, and 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 device, which is assigned to you by your ISP.

DDNS

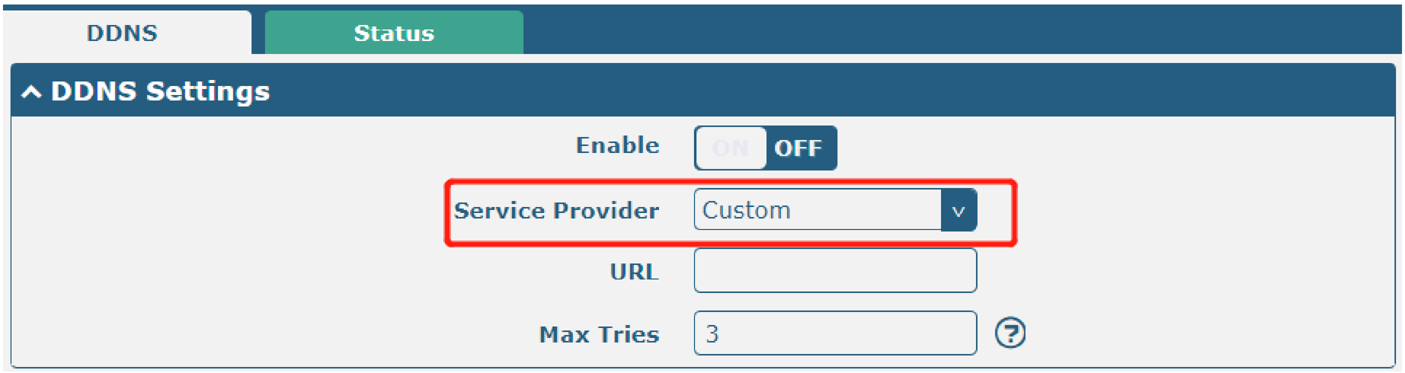
The service provider defaults to “DynDNS”, as shown below.



^ DDNS Settings

Enable	ON OFF
Service Provider	DynDNS
Hostname	
Username	
Password	
Max Tries	3

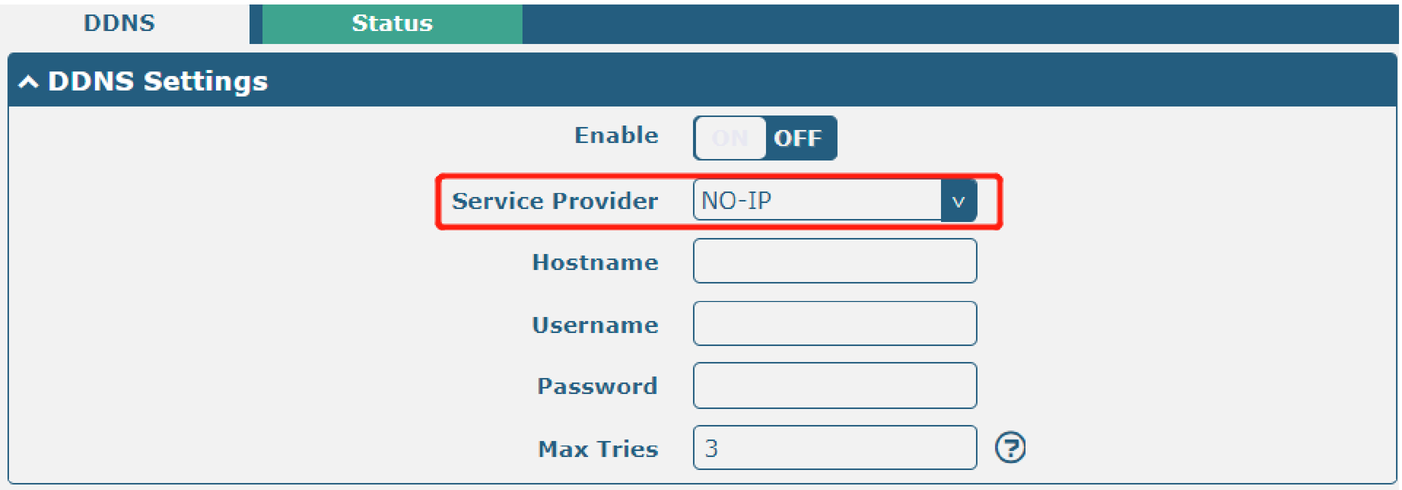
When the “Custom” service provider is chosen, the window is displayed as below.



^ DDNS Settings

Enable	ON OFF
Service Provider	Custom
URL	
Max Tries	3

When the “NO-IP” service provider is chosen, the window is displayed as below.



Enable: ON OFF

Service Provider: NO-IP

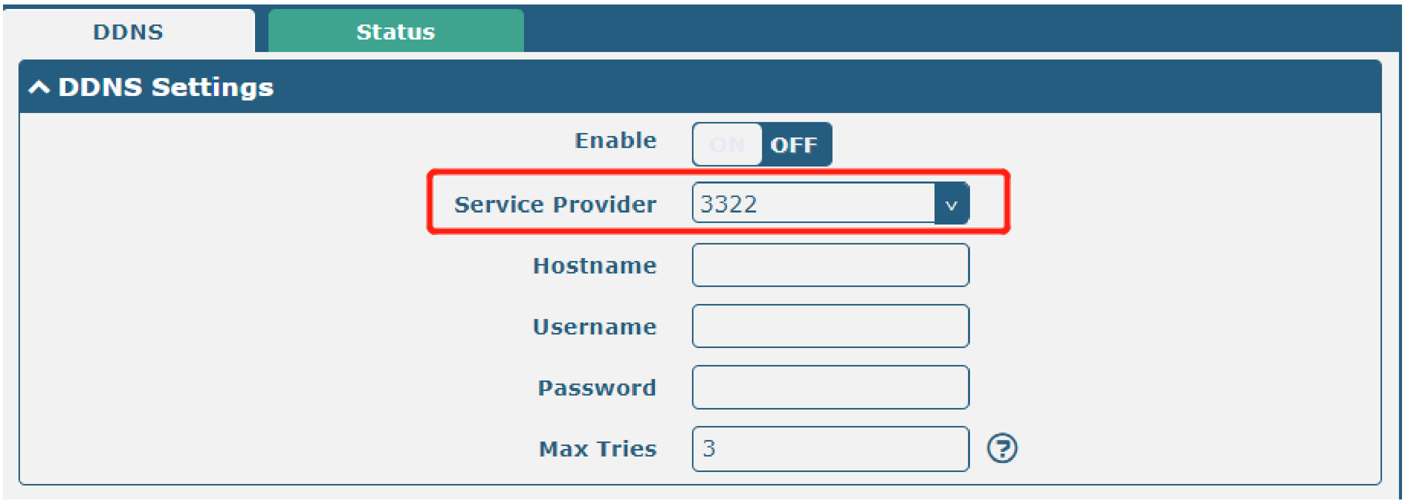
Hostname:

Username:

Password:

Max Tries: 3

When the “3322” service provider is chosen, the window is displayed as below.



Enable: ON OFF

Service Provider: 3322

Hostname:

Username:

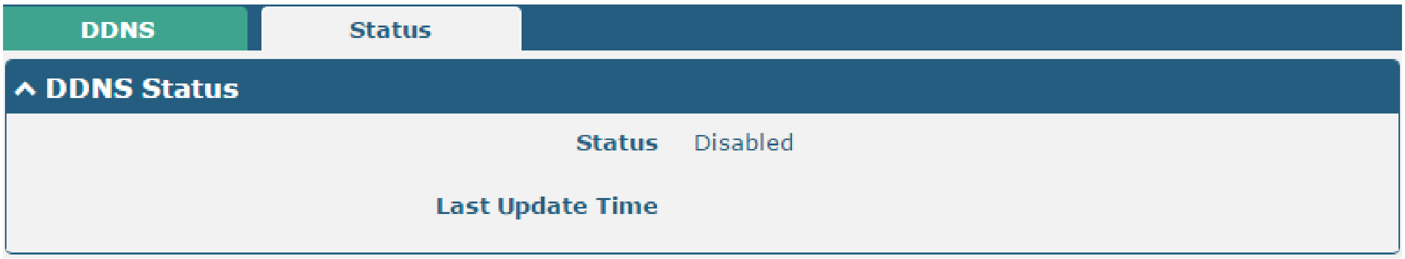
Password:

Max Tries: 3

DDNS Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the DDNS option.	OFF
Service Provider	Select DDNS service from “DynDNS”, “NO-IP”, “3322”, or “Custom”. ***Note:*** *DDNS service only can be used after being registered by the Corresponding service provider.*	DynDNS
Hostname	Enter hostname provided by DDNS server.	Null
Username	Enter username provided by DDNS server.	Null
Password	Enter password provided by DDNS server.	Null
URL	Enter URL customized by the user.	Null
Max tries	Enter maximum tries times.	3

Status

This section allows you to view the status of DDNS.



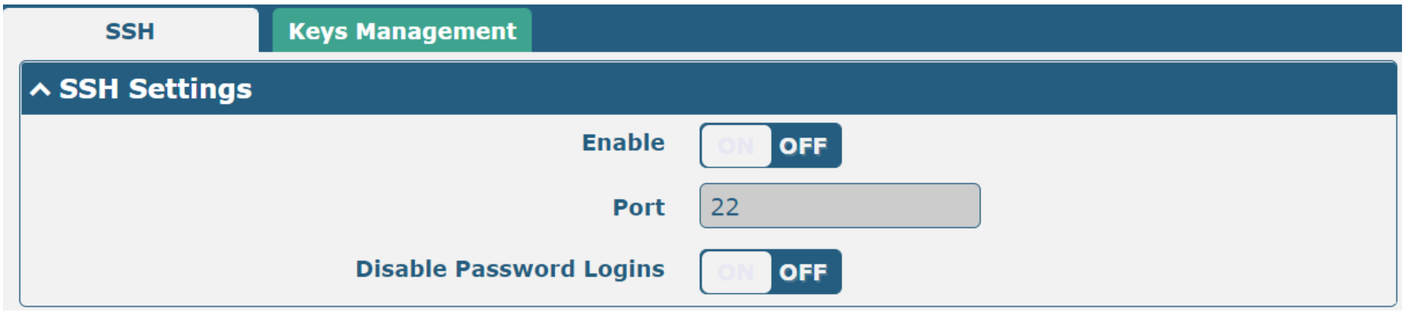
Status Disabled

Last Update Time

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

3.6.7 SSH

The device supports SSH password access and secret-key access.



Enable ON OFF

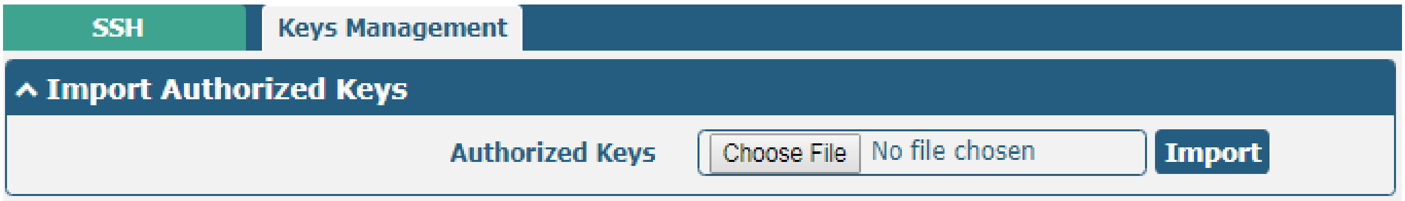
Port 22

Disable Password Logins ON OFF

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

Key Management

This section allows you to import authorized Keys.



Import Authorized Keys	
Item	**Description**
Authorized Keys	Click “Choose File” to locate an authorized key from your PC, and then click “Import” to import this key into your device. ***Note***: *This option is valid when enabling the password logins option.*

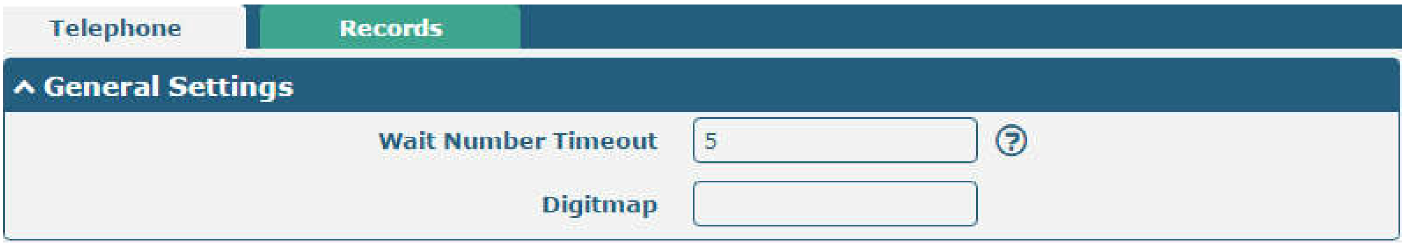
3.6.8 Telephone

This section allows you to set the related parameters of the voice function. If your device has voice input, this page is configurable.

Note:

1) Whether or not voice call and data transmission can be used simultaneously is dependent upon your ISP network.

2) R2000-Ent and R3010 support “Telephone” feature.

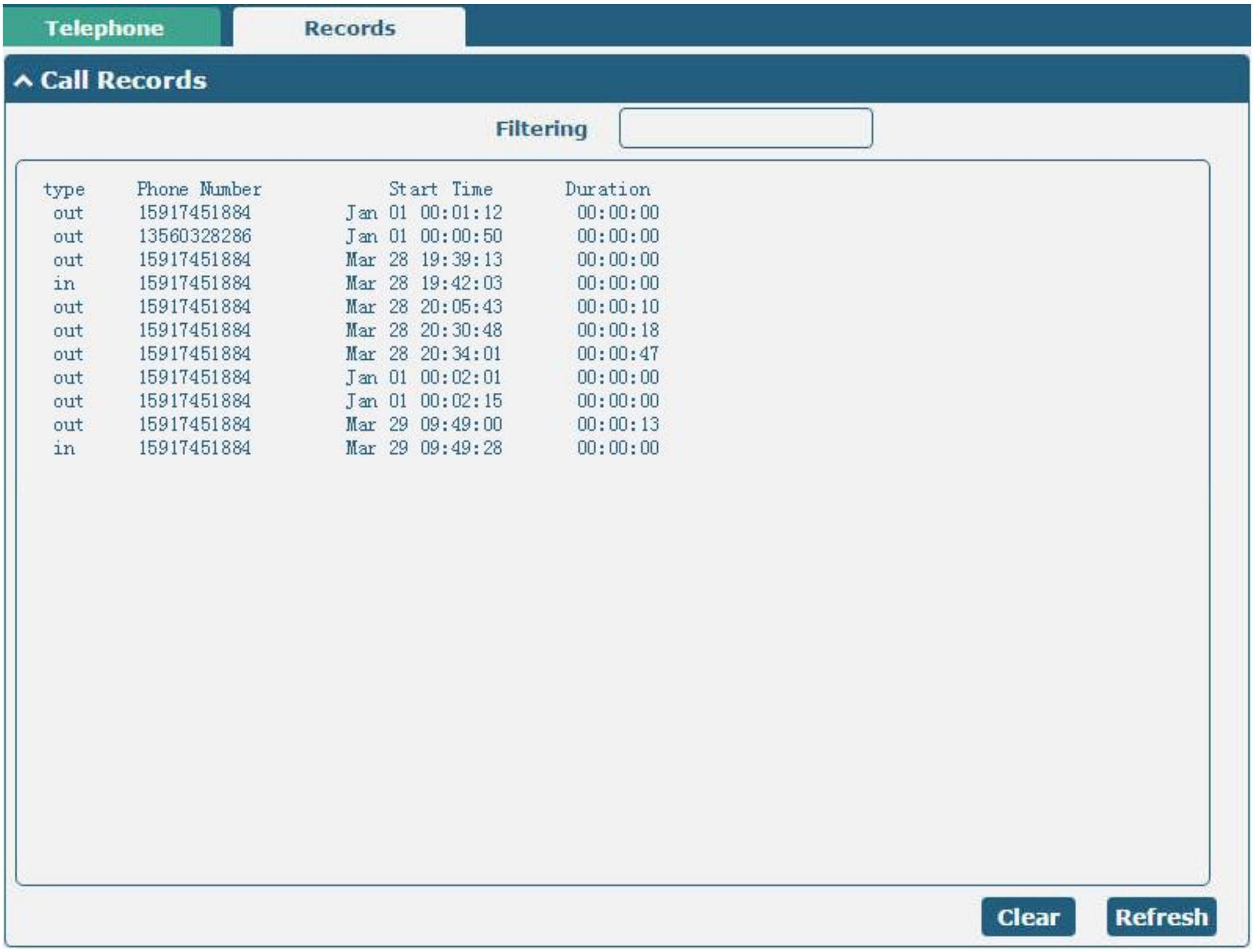


Wait Number Timeout 5

General Settings @ Telephone		
Item	**Description**	**Default**
Wait Number Timeout	Set wait number timeout for the dial plan, measured in seconds.	5
Digitmap	Enter digitmap used for matching the telephone number when making voice calls. When matched, the system will call this number immediately, and you don’t need to wait for the dial-up timeout. This option is used for speed dialing.	Null

Records

This section allows you to view the call records.



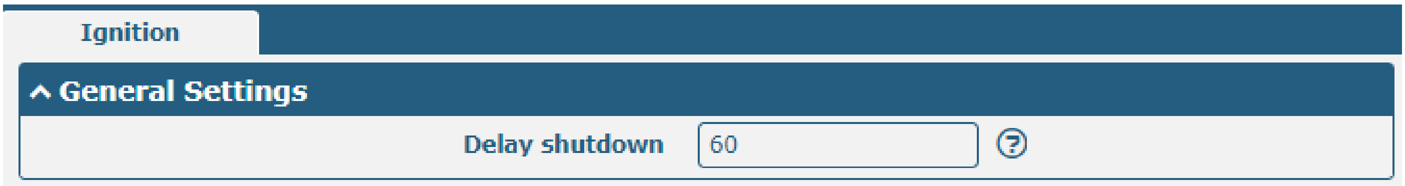
```
type    Phone Number         Start Time        Duration
 out    15917451884       Jan 01 00:01:12      00:00:00
 out    13560328286       Jan 01 00:00:50      00:00:00
 out    15917451884       Mar 28 19:39:13      00:00:00
 in     15917451884       Mar 28 19:42:03      00:00:00
 out    15917451884       Mar 28 20:05:43      00:00:10
 out    15917451884       Mar 28 20:30:48      00:00:18
 out    15917451884       Mar 28 20:34:01      00:00:47
 out    15917451884       Jan 01 00:02:01      00:00:00
 out    15917451884       Jan 01 00:02:15      00:00:00
 out    15917451884       Mar 29 09:49:00      00:00:13
 in     15917451884       Mar 29 09:49:28      00:00:00
```

General Settings		
Item	**Description**	**Default**
Filtering	Set wait number timeout for the dial plan, measured in seconds.	--
Clear	Click the button to clear the call record.	--
Refresh	Click the button to refresh the call record.	--

3.6.9 Ignition

This section is used to configure the parameters of Ignition.

Note: *R5020 and R2110 support the ignition feature.*



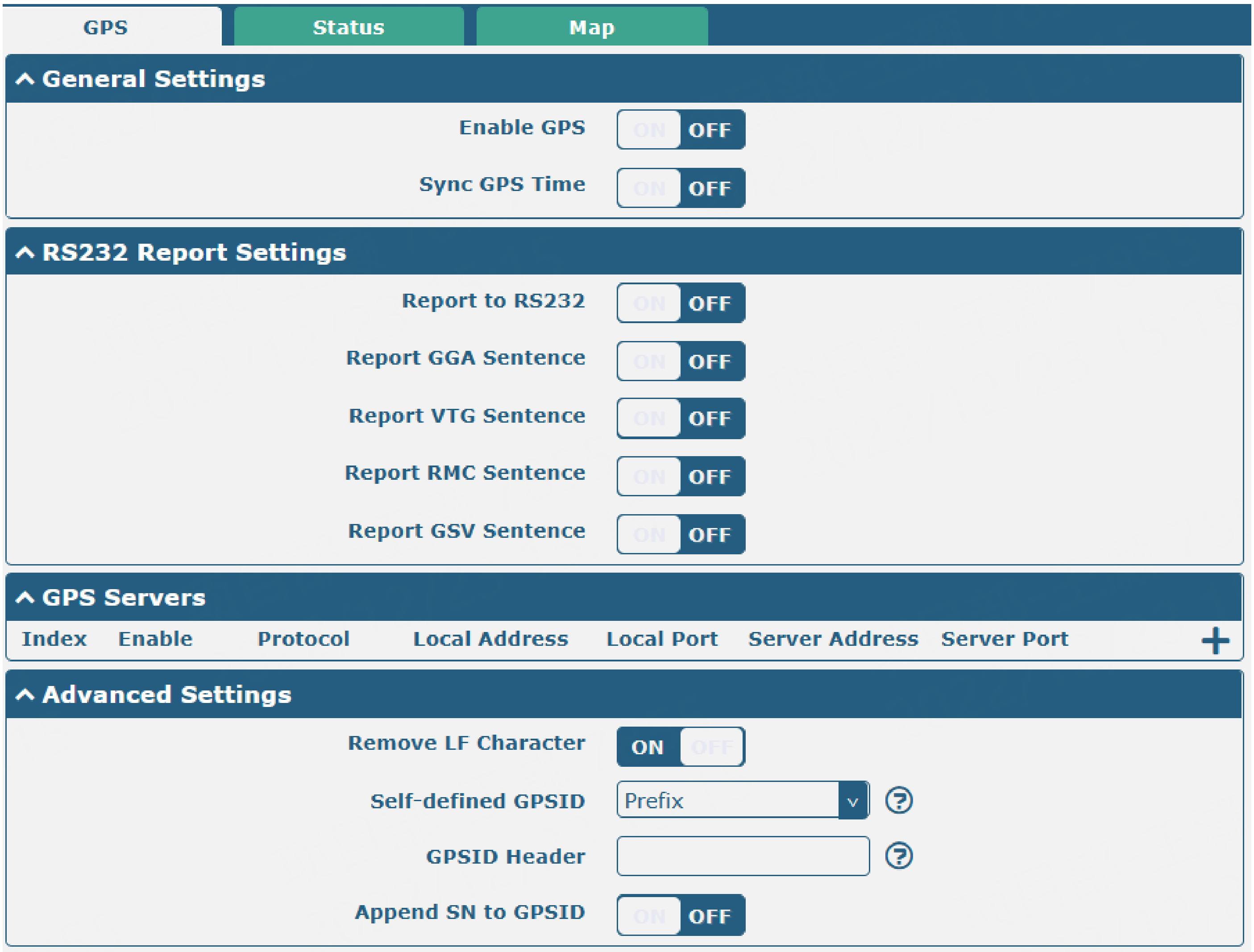
General Settings

Delay shutdown: 60

General Settings		
Item	**Description**	**Default**
Delay shutdown	Enter the time in seconds you want to delay power down. The timeout for delayed power down is 60 seconds to 3600 seconds.	60

3.6.10 GPS

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



General Settings

Enable GPS: OFF

Sync GPS Time: OFF

RS232 Report Settings

Report to RS232: OFF

Report GGA Sentence: OFF

Report VTG Sentence: OFF

Report RMC Sentence: OFF

Report GSV Sentence: OFF

GPS Servers

Index	Enable	Protocol	Local Address	Local Port	Server Address	Server Port

Advanced Settings

Remove LF Character: ON

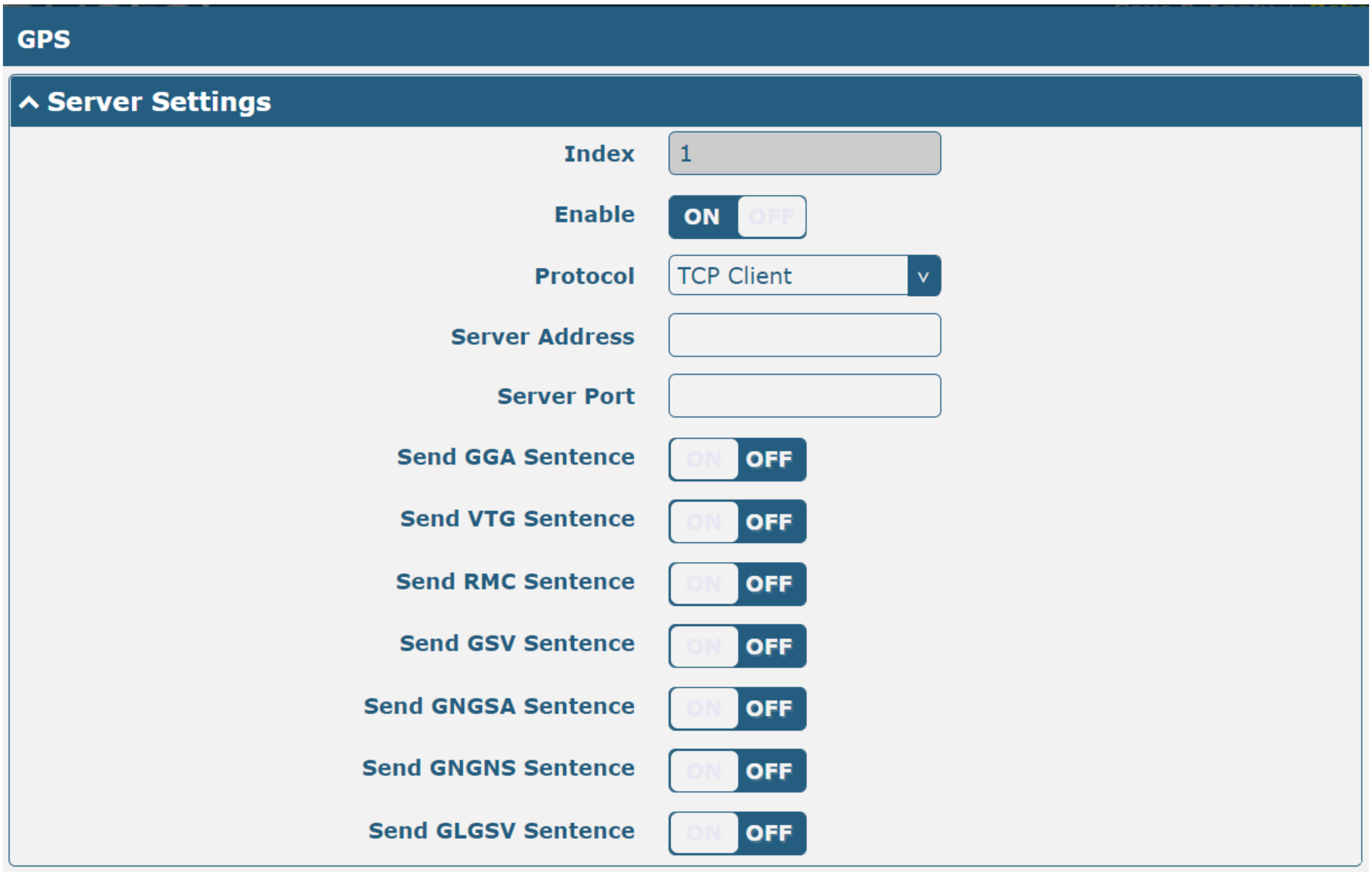
Self-defined GPSID: Prefix

GPSID Header:

Append SN to GPSID: OFF

GPS		
Item	**Description**	**Default**
General Settings		
Enable	Click the toggle button to ON to enable GPS.	OFF
Synchronized GPS Time	Click the toggle button to ON to synchronize GPS time.	OFF
RS232 Report Data Settings		
Reporting data through RS232	Reporting GPS Information by RS232.	OFF
Reporting GGA Sentence	Reporting GGA Sentence Information.	OFF
Reporting VTG Sentence	Reporting VTG Sentence Information.	OFF
Reporting RMC Sentence	Reporting RMC Sentence Information.	OFF
Reporting GSV Sentence	Reporting GSV Sentence Information.	OFF
Advanced Settings		
Remove LF Character	Enable to remove Line Feed character	ON
Self-defined GPSID	The GPSID is appended to the NMEA message before transmit. You can choose "None", "Prefix", and "Suffix".	None
GPSID Header	Added GPSID Header. Usually using 7 upper case.	N/A
Append SN to GPSID	Enable to append SN to GPSID	OFF

Click + to add a new GPS Server.

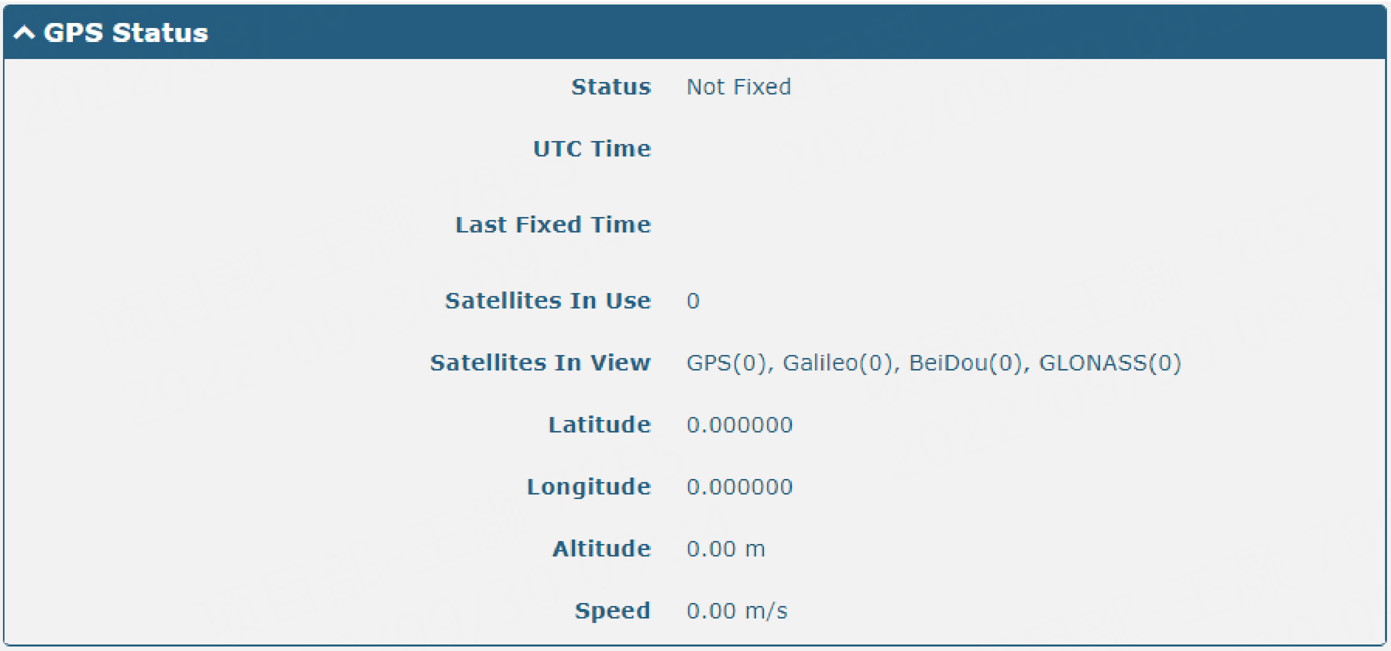


Index: 1
Enable: ON
Protocol: TCP Client
Server Address:
Server Port:
Send GGA Sentence: OFF
Send VTG Sentence: OFF
Send RMC Sentence: OFF
Send GSV Sentence: OFF
Send GNGSA Sentence: OFF
Send GNGNS Sentence: OFF
Send GLGSV Sentence: OFF

Item	Description	Default
Index	Indicate ordinal of 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
Send GNGSA Sentence	Click the toggle button to enable/disable this option.	OFF
Send GNGNS Sentence	Click the toggle button to enable/disable this option.	OFF
Send GLGSV Sentence	Click the toggle button to enable/disable this option.	OFF

Status

This section allows you to view the status of GPS.



GPS Status

Status Not Fixed

UTC Time

Last Fixed Time

Satellites In Use 0

Satellites In View GPS(0), Galileo(0), BeiDou(0), GLONASS(0)

Latitude 0.000000

Longitude 0.000000

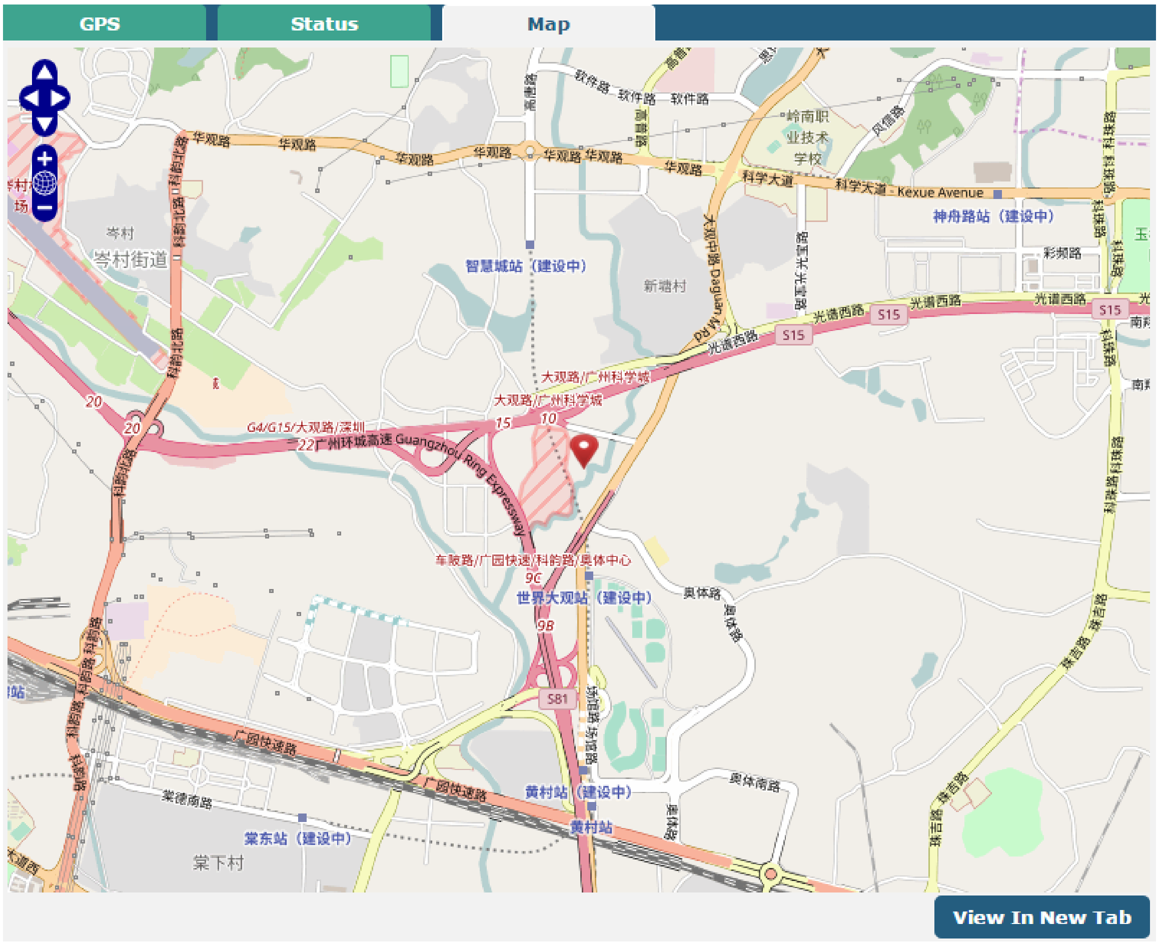
Altitude 0.00 m

Speed 0.00 m/s

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

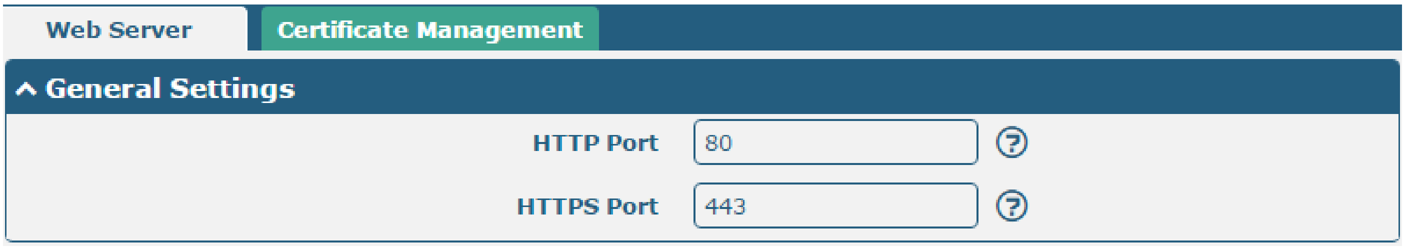
MAP

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 to the device and enable GPS on the GPS page.


GPS
Status
Map
View In New Tab

3.6.11 Web Server

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



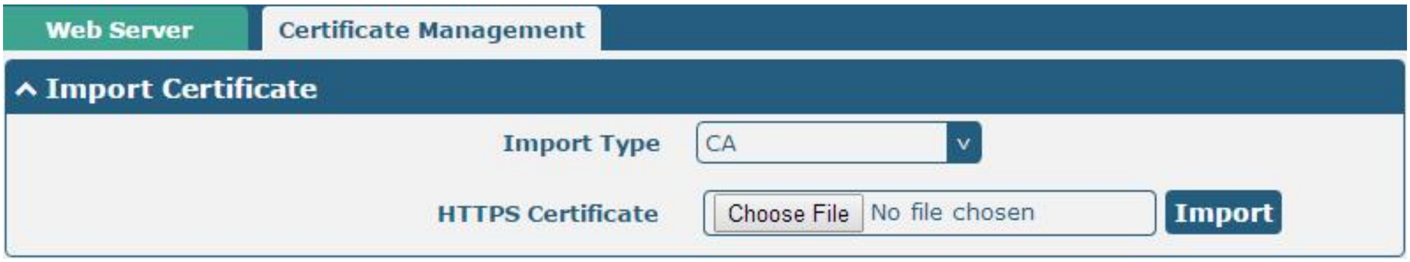
HTTP Port: 80

HTTPS Port: 443

General Settings @ Web Server		
Item	**Description**	**Default**
HTTP Port	Enter HTTP port number you want to change in the device'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 device with other HTTP Port numbers except 80, only adding that port number then you can log in device's Web Server.	80
HTTPS Port	Enter HTTPS port number you want to change in the device'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 device with other HTTPS Port numbers except 443, only adding that port number then you can log in device'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 to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.*	443

Certificate Management

This section allows you to import the certificate file into the device.



Import Type: CA

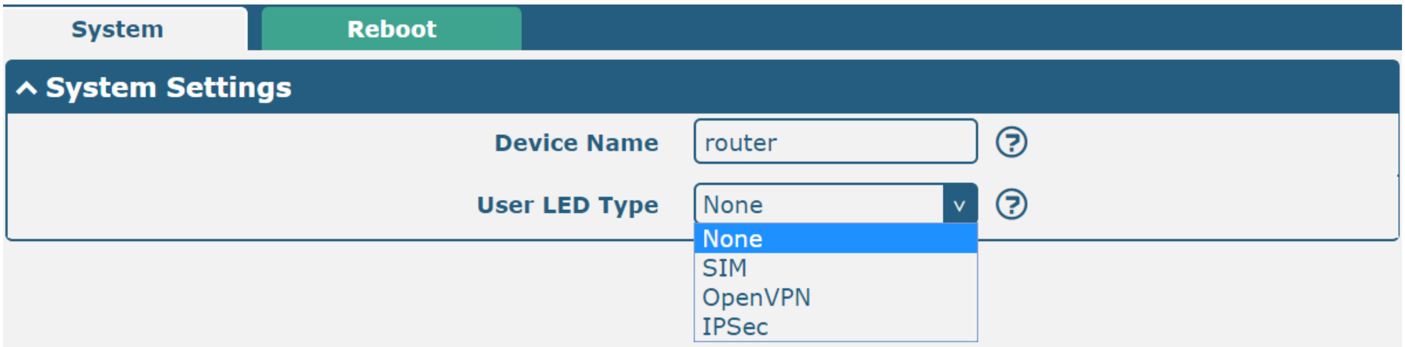
HTTPS Certificate: No file chosen

Import Certificate		
Item	**Description**	**Default**
Import Type	Select from "CA" and "Private Key". • CA: a digital certificate issued by the CA center. • Private Key: a private key file.	CA
HTTPS Certificate	Click "Choose File" to locate the certificate file from your PC, and then	--

Import Certificate		
Item	Description	Default
	click “Import” to import this file into your device.	

3.6.12 Advanced

This section allows you to set the Advanced and parameters. Advanced device settings include system settings and restart.



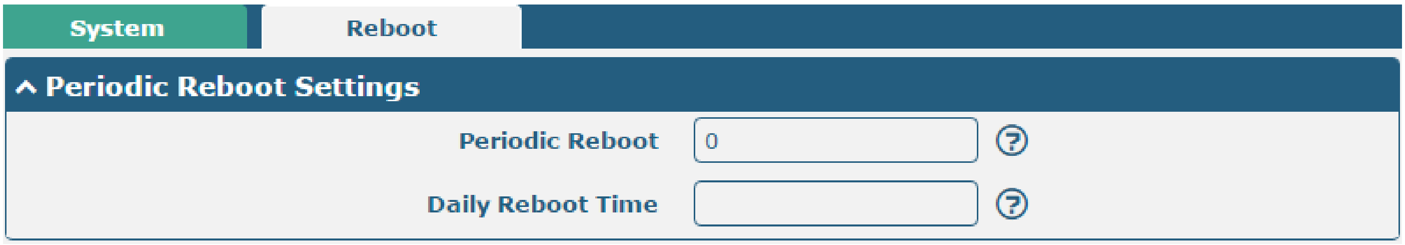
Device Name: router

User LED Type: None

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

Reboot

This section allows you to configure the reboot type.



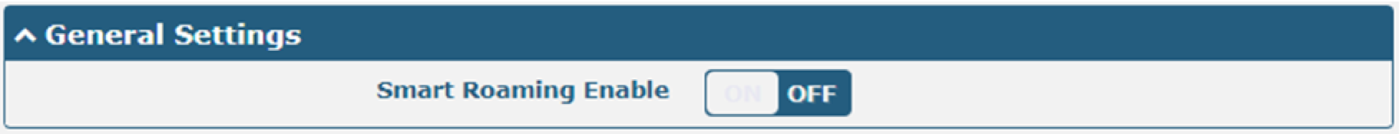
Periodic Reboot: 0

Daily Reboot Time:

Periodic Reboot Settings		
Item	Description	Default
Periodic Reboot	Set reboot period of the device. 0 means disable.	0
Daily Reboot Time	Set daily reboot time of device. You should follow the format as HH: MM, in 24h time frame, otherwise, the data will be invalid. Leave it empty means disable.	Null

3.6.13 Smart Roaming V2

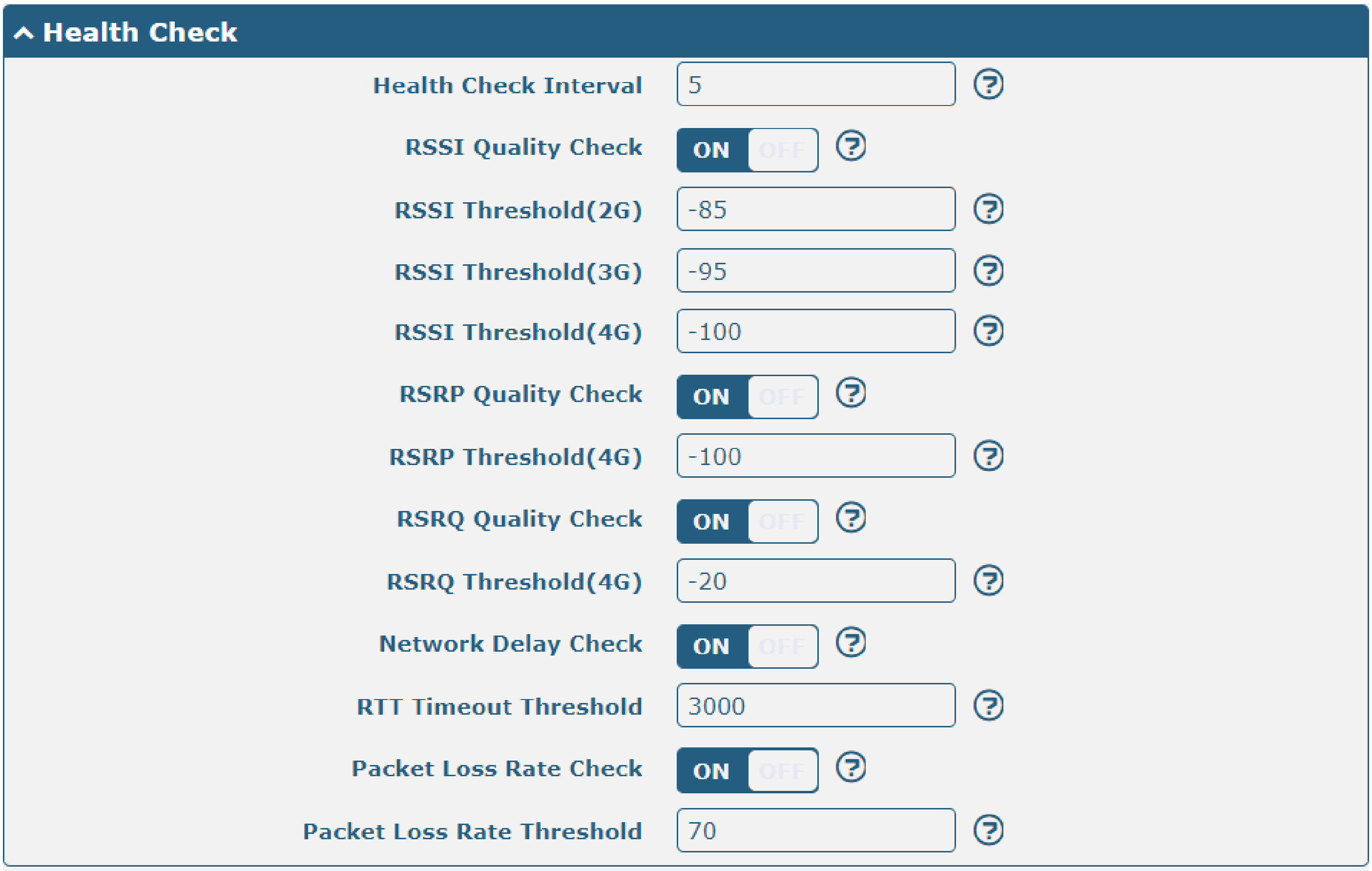
Smarting roaming includes general settings, health checks, PING settings, and advanced settings.



General Settings

Smart Roaming Enable: ON / OFF (OFF)

General Setting		
Item	**Descriptions**	**Default**
Smart Roaming Enable	Enable Smart Roaming feature	OFF



Health Check

Health Check Interval: 5

RSSI Quality Check: ON

RSSI Threshold(2G): -85

RSSI Threshold(3G): -95

RSSI Threshold(4G): -100

RSRP Quality Check: ON

RSRP Threshold(4G): -100

RSRQ Quality Check: ON

RSRQ Threshold(4G): -20

Network Delay Check: ON

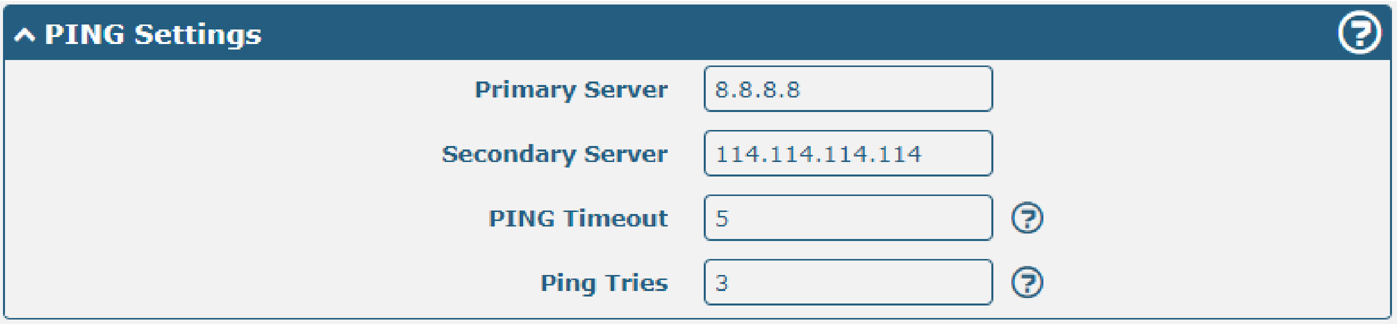
RTT Timeout Threshold: 3000

Packet Loss Rate Check: ON

Packet Loss Rate Threshold: 70

Health Check		
Item	**Descriptions**	**Default**
Health Check Interval	The health check interval for the current connection is in minutes. If the health check fails, Smart Roaming will try to switch to another carrier network. Be careful not to set all check conditions to theoretically unattainable values.	5 Minutes
RSSI Quality Check	To enable/disable "RSSI Quality Check" feature.	ON

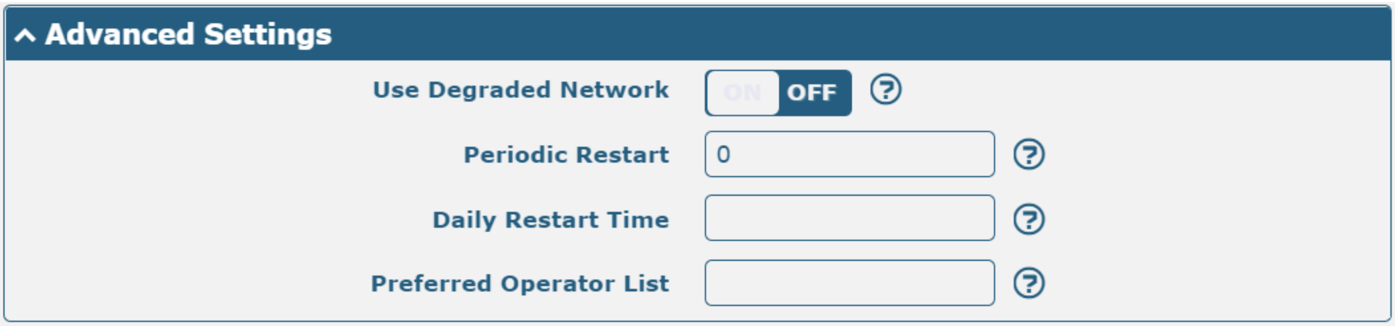
Health Check		
Item	**Descriptions**	**Default**
Health Check Interval	The health check interval for the current connection is in minutes. If the health check fails, Smart Roaming will try to switch to another carrier network. Be careful not to set all check conditions to theoretically unattainable values.	5 Minutes
RSSI Threshold (2G)	Signal strength threshold for 2G networks.	-85 dBm
RSSI Threshold (3G)	Signal strength threshold for 3G networks.	-95 dBm
RSSI Threshold (4G)	Signal strength threshold for 4G networks.	-100 dBm
RSRP Quality Check	To enable/disable "RSRP Quality Check" feature.	OFF
RSRP Threshold (4G)	The reference signal received power threshold for 4G networks.	-100 dBm
RSRQ Quality Check	To enable/disable "RSRQ Quality Check" feature.	OFF
RSRQ Threshold (4G)	The reference signal receiving quality threshold for 4G networks.	-20 dBm
Network Delay Check	To enable/disable “Network Delay Check " feature.	OFF
RTT Timeout Threshold	The reference signal received power threshold for 4G networks.	3000 ms
Packet Loss Rate Check	Enable/disable “Packet Loss Rate Check" feature.	ON
Packet Loss Rate Threshold	Packet loss rate threshold value.	70



Primary Server	8.8.8.8
Secondary Server	114.114.114.114
PING Timeout	5
Ping Tries	3

PING Settings		
Item	**Descriptions**	**Default**
Primary Server	The device pings primary address/domain name to detect if current connection is always alive.	8.8.8.8
Secondary Server	The device pings secondary address/domain name to detect if current connection is always alive.	114.114.114.114
Ping Timeout	Set Ping timeout.	5 seconds
Ping Tries	The number of ping attempts per health check. Each ping attempt sends 3 ping messages by default, so the total number of ping messages sent per	3 times

PING Settings		
Item	**Descriptions**	**Default**
	health check is (3 * number of ping attempts).	



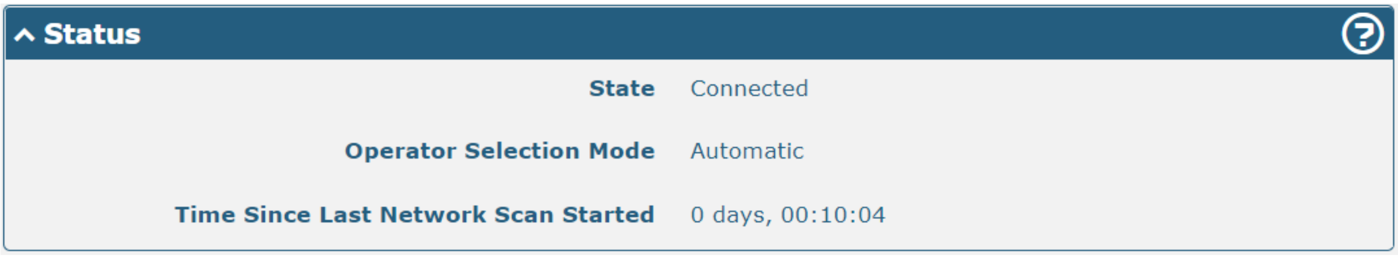
Use Degraded Network: ON OFF

Periodic Restart: 0

Daily Restart Time:

Preferred Operator List:

Advanced Settings		
Item	**Descriptions**	**Default**
Use Degraded Network	To enable/disable "Use Degraded Network" feature. A degraded network is defined as a network that can be connected, but the network quality does not meet the health check thresholds.	OFF
Periodic Restart	Set period of rebooting the "Smart Roaming" function in hours. 0 means no periodic reboot is enabled. Restarting "Smart Roaming" will re-find the available carrier network and reset the current status because it takes a long time to search the available provider network, the reboot may take 3 to 5 minutes.	0
Daily Restart Time	Set time point to restart "Smart Roaming" every day in the format of HH: MM (24-hour system). When this item is empty, it means to disable the timer reboot.	Null
Preferred Operator List	Set list of preferred operators by PLMN. If multiple operators are required, use semicolons to separate, e.g., 46000;46001	Null



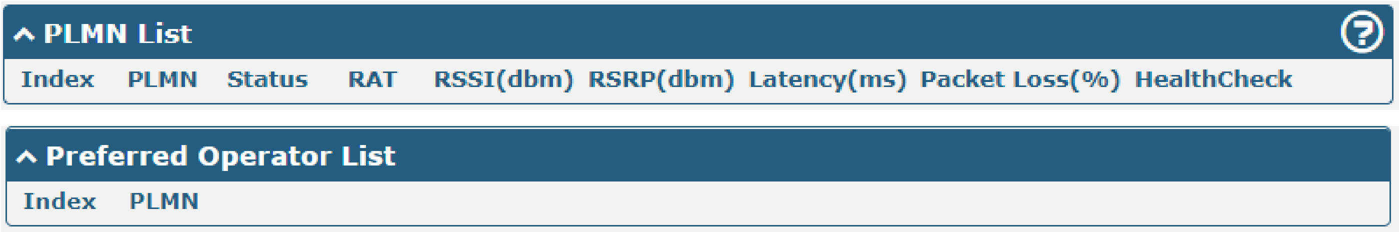
State: Connected

Operator Selection Mode: Automatic

Time Since Last Network Scan Started: 0 days, 00:10:04

Status	
Item	**Descriptions**
Status	Display current status of "Smart Roaming". It includes Scanning, Connecting, Connected, and Inactive status, which indicates that the network is searching for an available network, connecting network, network is connected and the function is not started respectively.

Status	
Item	**Descriptions**
Operator Selection Mode	Display which carrier network is currently selected. These include Automatic and Manual, which refer to automatic selection according to standard specifications and software selection based on network quality, respectively, and the software will cycle through the two methods.
Time Since Last Network Scan	Displays time elapsed since the last search for available networks. A "Smart Roaming" reboot will refresh this time.



^ PLMN List

Index	PLMN	Status	RAT	RSSI(dbm)	RSRP(dbm)	Latency(ms)	Packet Loss(%)	HealthCheck

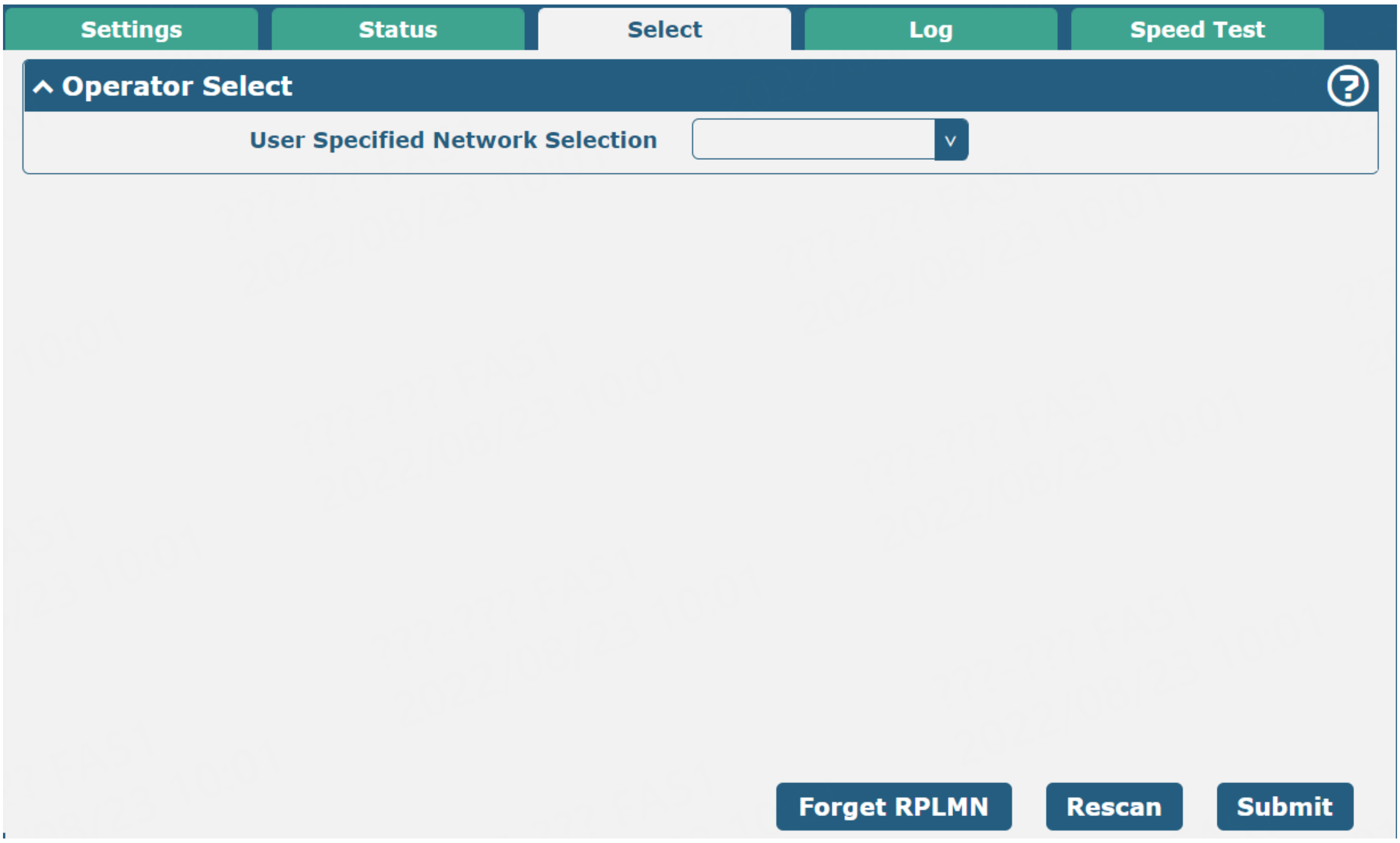
^ Preferred Operator List

Index	PLMN

PLMN List	
Item	**Descriptions**
Index	PLMN list index
PLMN	PLMN = MCC + MNC, which is a combination of mobile country code and mobile network code.
Status	The current network status, including Current, Visible, Forbidden, and Unknown, indicates the current use of this network, the available network, the forbidden network, and the unknown network, respectively.
RAT (dBm)	Current wireless access technologies, including 2G/3G/4G.
RSSI (dBm)	Current signal quality for 3G and 4G networks.
RSRP (dBm)	Current reference signal reception power for 4G networks.
Latency	Current network latency.
Packet Loss (%)	Current network packet loss rate.
Health Check	The current health check status, including Pending, Good, Degraded, and Failed, indicates that the current network has not yet been health checked; the network quality is good; the network is degraded; and the network quality is poor (including disconnected or does not meet the health check threshold), respectively.
Preferred PLMN list	
Index	PLMN list index
PLMN	PLMN = MCC + MNC, which is a combination of mobile country code and mobile network code.

Select

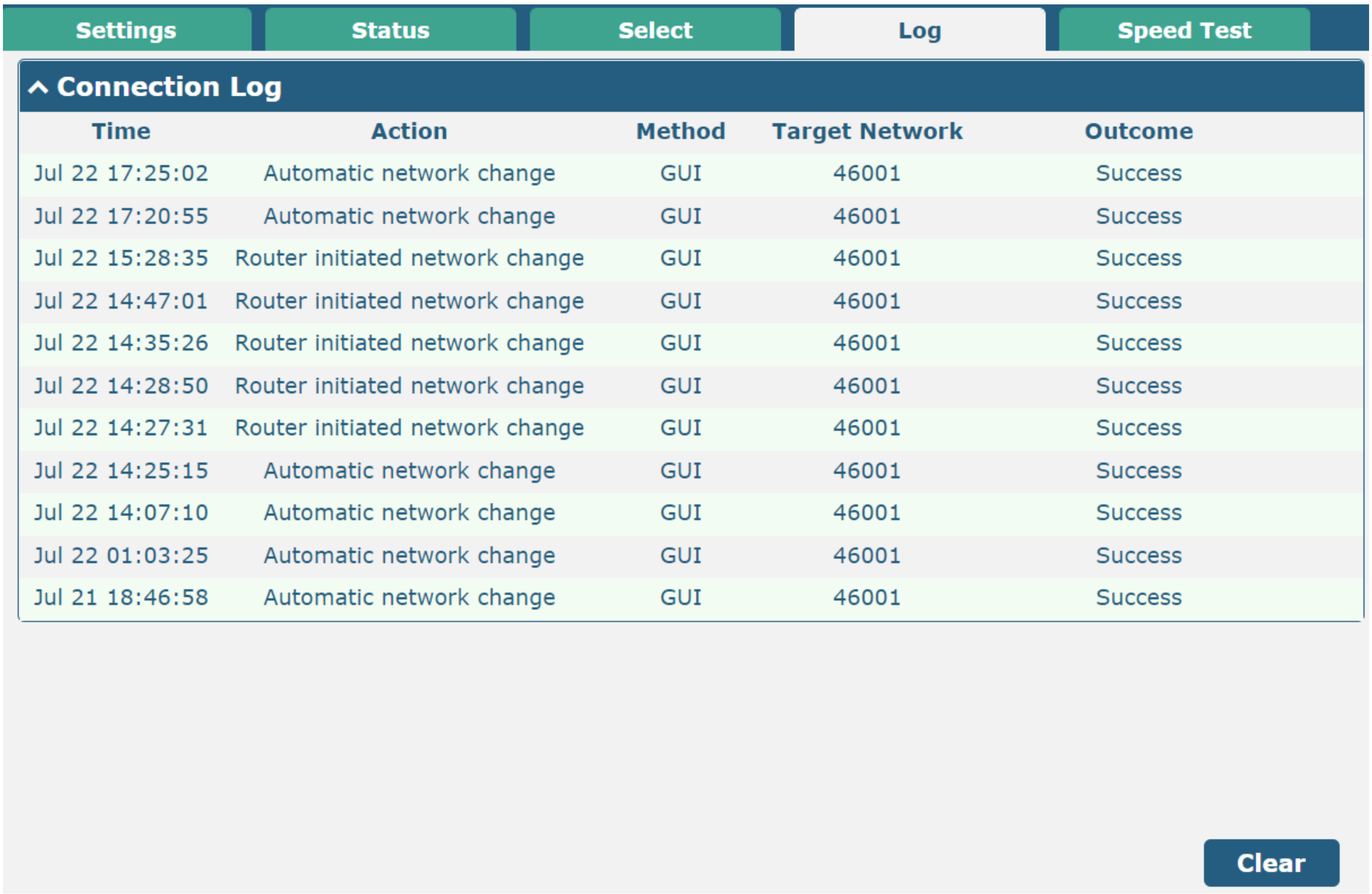
This section allows you to select the network.



Operator Select		
Item	**Descriptions**	**Default**
User Specified Network Selection	Select Specified Network.	--
Forget RPLMN	Forces deletion of all location information from the SIM.	--
Rescan	Rescan operator list and this causes Smart Roaming to start again.	--
Submit	Submit operator selected by the drop-down box.	--

Log

This section allows you to view the connection log.



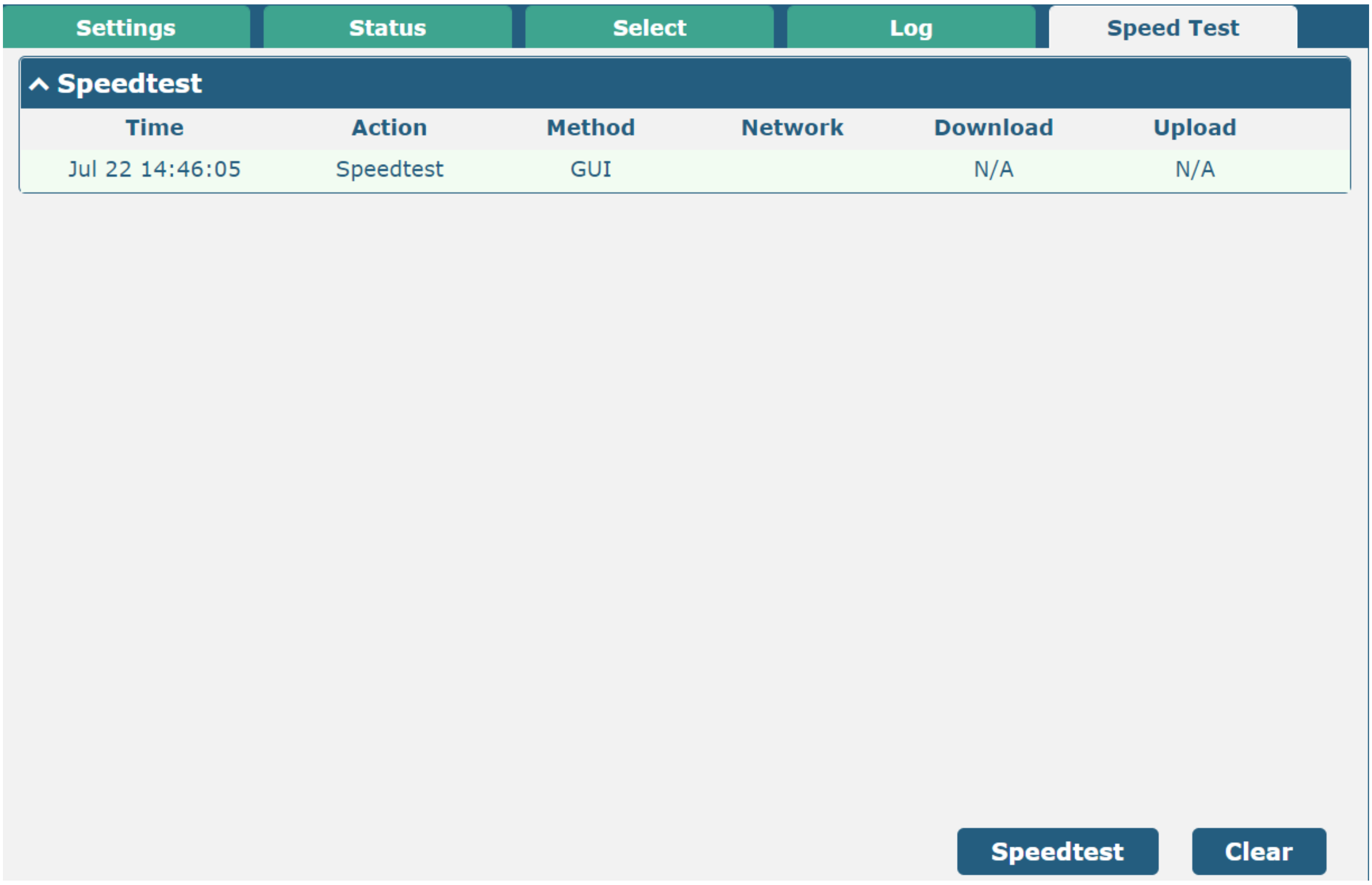
Connection Log

Time	Action	Method	Target Network	Outcome
Jul 22 17:25:02	Automatic network change	GUI	46001	Success
Jul 22 17:20:55	Automatic network change	GUI	46001	Success
Jul 22 15:28:35	Router initiated network change	GUI	46001	Success
Jul 22 14:47:01	Router initiated network change	GUI	46001	Success
Jul 22 14:35:26	Router initiated network change	GUI	46001	Success
Jul 22 14:28:50	Router initiated network change	GUI	46001	Success
Jul 22 14:27:31	Router initiated network change	GUI	46001	Success
Jul 22 14:25:15	Automatic network change	GUI	46001	Success
Jul 22 14:07:10	Automatic network change	GUI	46001	Success
Jul 22 01:03:25	Automatic network change	GUI	46001	Success
Jul 21 18:46:58	Automatic network change	GUI	46001	Success

Connection Log		
Clear	Click the button to clear the connection log.	--

Speed Test

This section allows you to test the network speed.



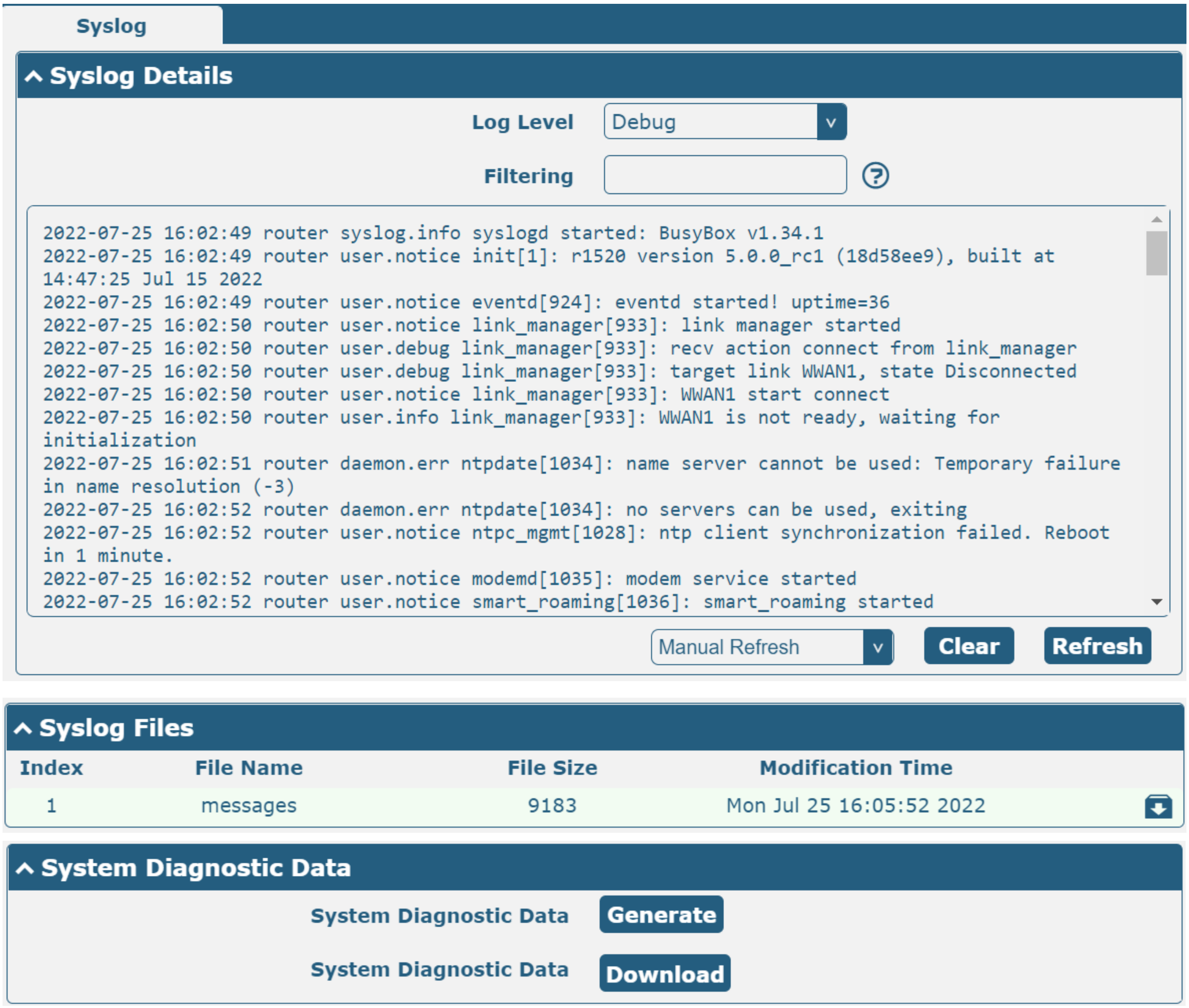
Time	Action	Method	Network	Download	Upload
Jul 22 14:46:05	Speedtest	GUI		N/A	N/A

Speed Test		
Speedtest	Click the button to start the network speed test.	--
Clear	Click the button to clear the speed test log.	--

3.7 System

3.7.1 Debug

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



Log Level: Debug

Filtering:

```
2022-07-25 16:02:49 router syslog.info syslogd started: BusyBox v1.34.1
2022-07-25 16:02:49 router user.notice init[1]: r1520 version 5.0.0_rc1 (18d58ee9), built at
14:47:25 Jul 15 2022
2022-07-25 16:02:49 router user.notice eventd[924]: eventd started! uptime=36
2022-07-25 16:02:50 router user.notice link_manager[933]: link manager started
2022-07-25 16:02:50 router user.debug link_manager[933]: recv action connect from link_manager
2022-07-25 16:02:50 router user.debug link_manager[933]: target link WWAN1, state Disconnected
2022-07-25 16:02:50 router user.notice link_manager[933]: WWAN1 start connect
2022-07-25 16:02:50 router user.info link_manager[933]: WWAN1 is not ready, waiting for
initialization
2022-07-25 16:02:51 router daemon.err ntpdate[1034]: name server cannot be used: Temporary failure
in name resolution (-3)
2022-07-25 16:02:52 router daemon.err ntpdate[1034]: no servers can be used, exiting
2022-07-25 16:02:52 router user.notice ntpc_mgmt[1028]: ntp client synchronization failed. Reboot
in 1 minute.
2022-07-25 16:02:52 router user.notice modemd[1035]: modem service started
2022-07-25 16:02:52 router user.notice smart_roaming[1036]: smart_roaming started
```

Index	File Name	File Size	Modification Time
1	messages	9183	Mon Jul 25 16:05:52 2022

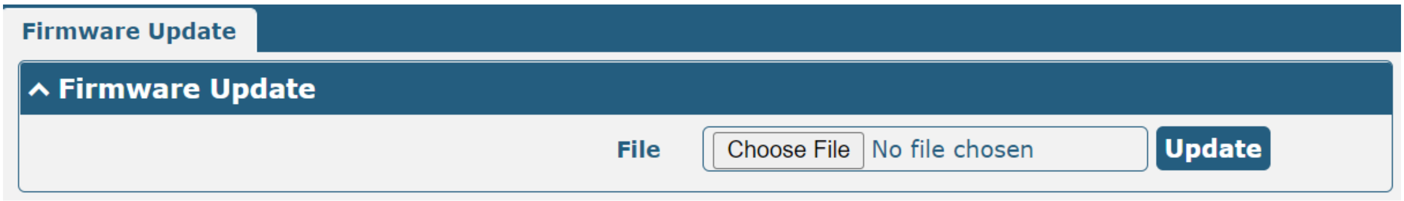
Syslog		
Item	**Description**	**Default**
Syslog Details		
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, and “Error” from low to high. The lower level will output more Syslog in detail.	Debug
Filtering	Enter filtering message based on the keywords. Use “&” to separate more than one filter 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 following box. If selecting “manual refresh”, you should click the refresh button to refresh the Syslog.	Manual Refresh
Clear	Click the button to clear the Syslog.	--
Refresh	Click the button to refresh the Syslog.	--
Syslog Files		
Syslog Files List	It can show at most 5 Syslog files in the list, the files’ name ranges from message0 to message 4. And the newest Syslog file will be placed on the top of the list.	--
System Diagnosing Data		
Generate	Click to generate the Syslog diagnosing file. When there is a problem with the device, system diagnostic data can be generated and sent to a **Robust technical support representative** for assistance.	--

3.7.2 Update

This section allows you to upgrade the device system and implement system updates by importing and updating firmware files. Import a firmware file from the PC to the device, click Update and restart the device as prompted to complete the firmware update.

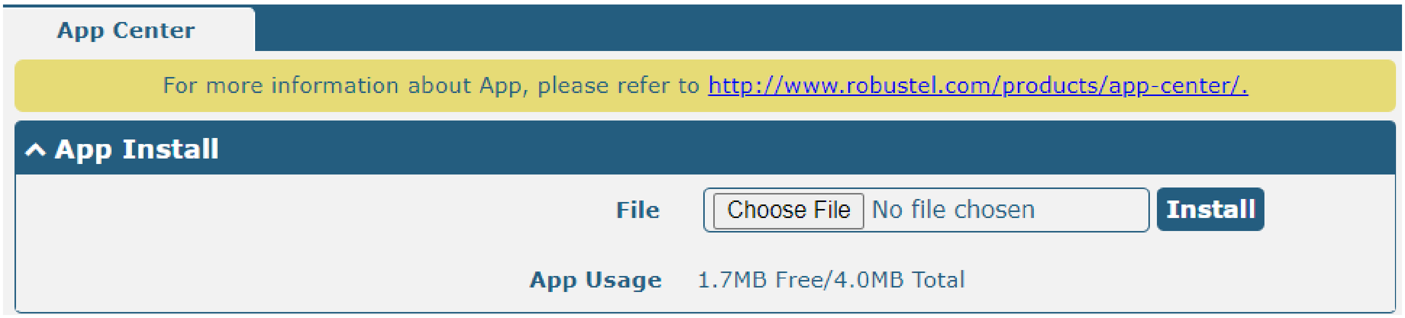
Note: *To access the latest firmware file, please contact your technical support engineer.*



3.7.3 App Center

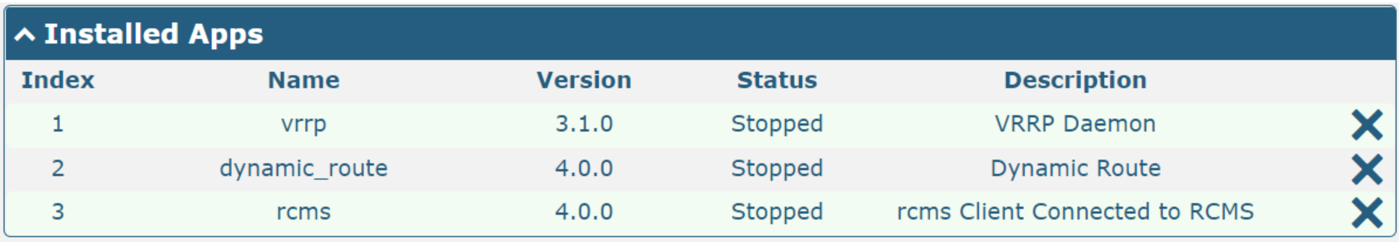
This section allows you to add some required or customized applications to the device. Import and install your applications to the App Center, and reboot the device according to the system prompts. Each installed application will be displayed under the “Services” menu, while other applications related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

Note: *After importing the applications to the device, 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 to the device again.*


For more information about App, please refer to http://www.robustel.com/products/app-center/.

App Usage 1.7MB Free/4.0MB Total

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



^ Installed Apps

Index	Name	Version	Status	Description	
1	vrrp	3.1.0	Stopped	VRRP Daemon	✕
2	dynamic_route	4.0.0	Stopped	Dynamic Route	✕
3	rcms	4.0.0	Stopped	rcms Client Connected to RCMS	✕

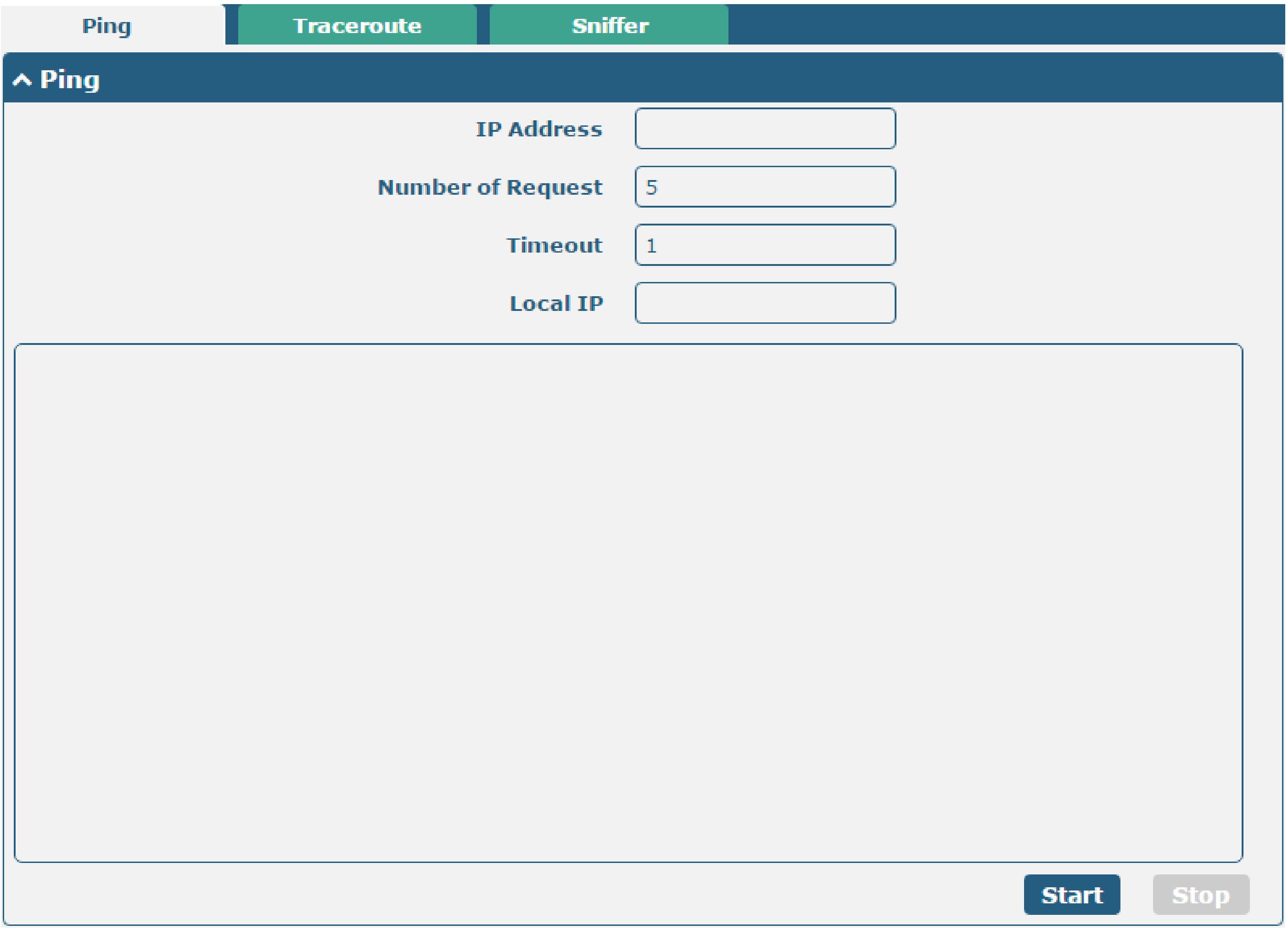
App Center		
Item	**Description**	**Default**
App Install		
File	Click on "Choose File" to locate the App file from your PC, and then click Install to import this file into your device. ***Note****: File format should be xxx.rpk, e.g., r1520-vrrp-5.0.0.rpk.*	--
Installed Apps		
Index	Indicate ordinal of list.	--
Name	Show name of App.	Null
Version	Show version of App.	Null
Status	Show status of App.	Null
Description	Show description for App.	Null

3.7.4 Tools

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

Ping

This section allows you to use the Ping tools.

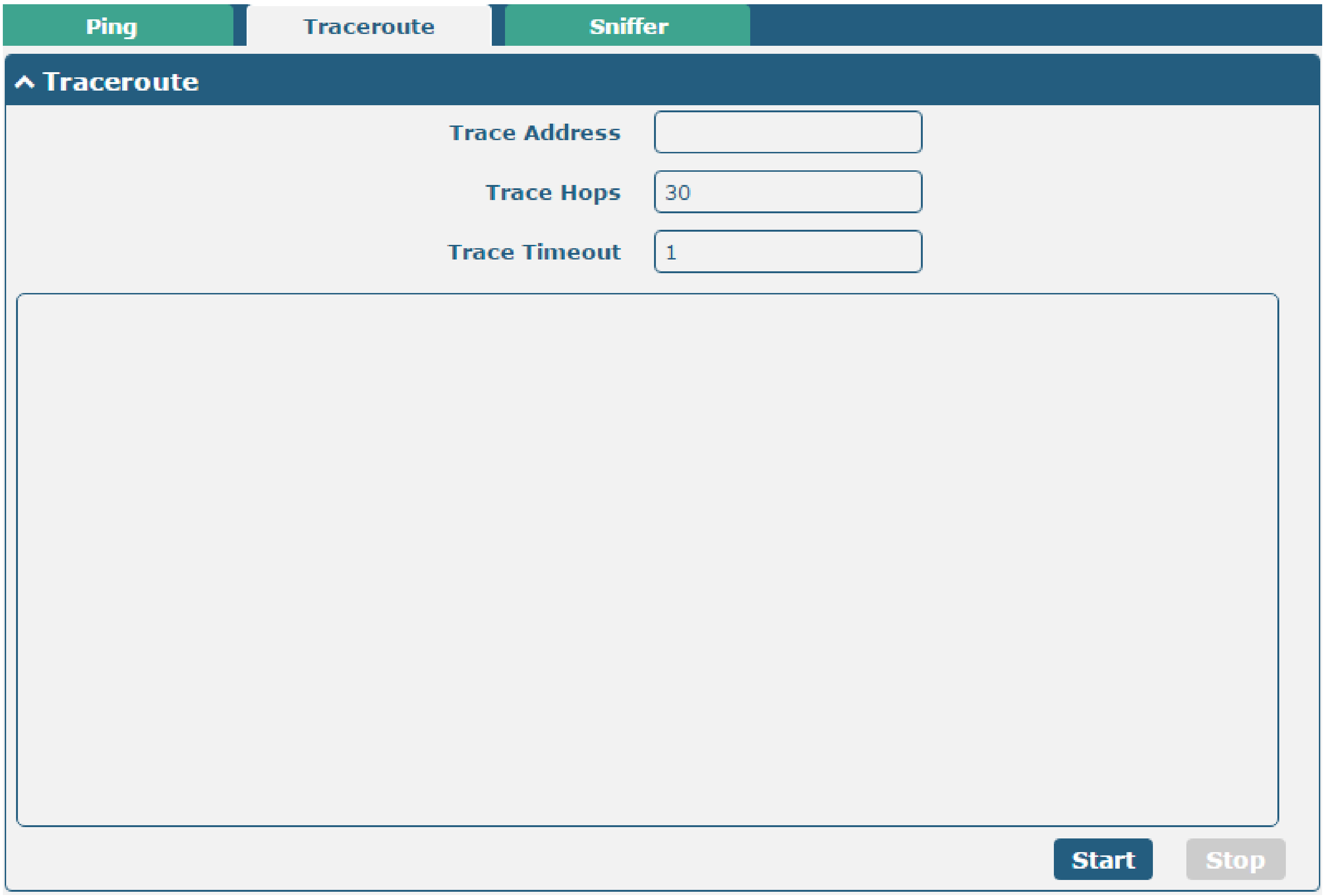


IP Address	
Number of Request	5
Timeout	1
Local IP	

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

Traceroute

This section allows you to use the Traceroute tools.



Trace Address

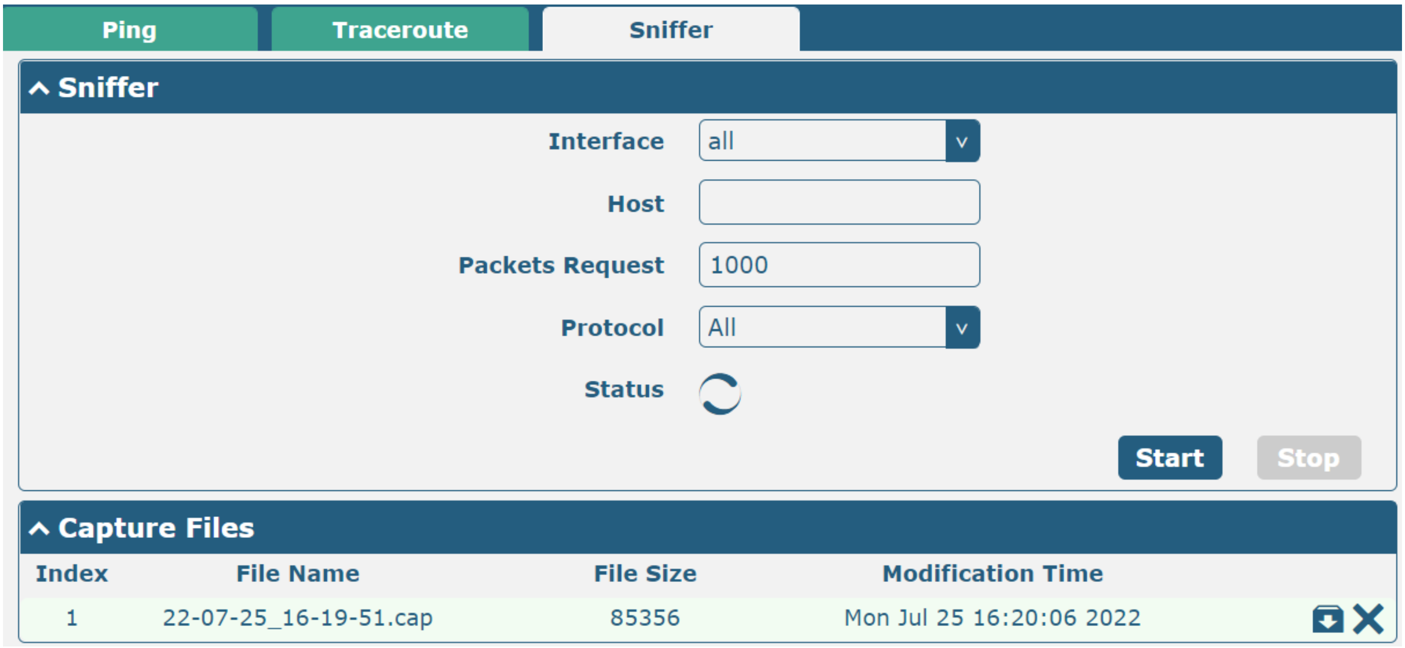
Trace Hops 30

Trace Timeout 1

Traceroute		
Item	**Description**	**Default**
Trace Address	Enter trace’s destination IP address or destination domain.	Null
Trace Hops	Specify max trace hops. The device will stop tracing if the trace hops have met the max value no matter whether destination has been reached or not.	30
Trace Timeout	Specify the timeout of Traceroute request.	1
Start	Click this button to start Traceroute request, and the log will be displayed in the following box.	--
Stop	Click this button to stop Traceroute request.	--

Sniffer

This section allows you to use the Sniffer tools.



Sniffer

Interface: all

Host:

Packets Request: 1000

Protocol: All

Status:

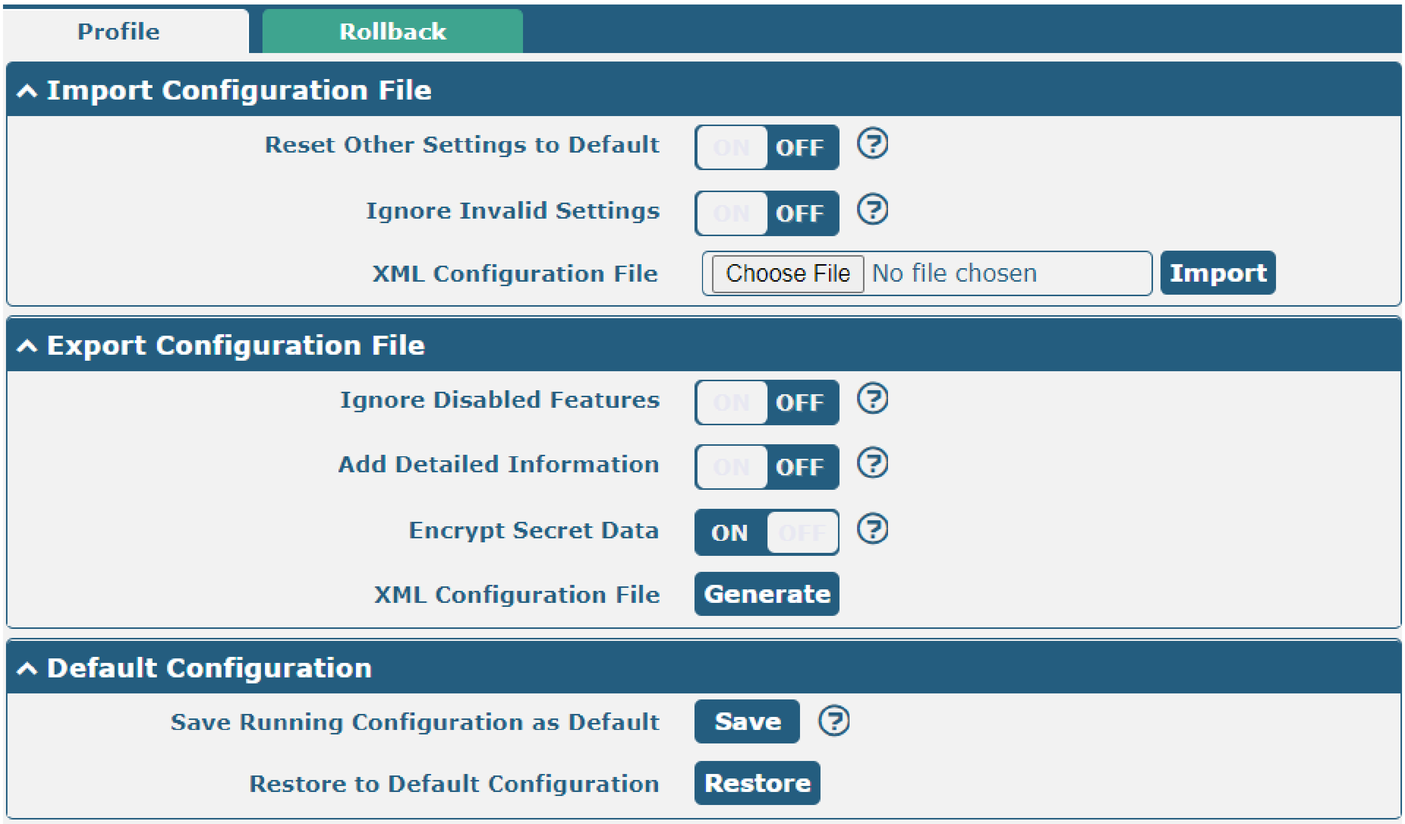
Capture Files

Index	File Name	File Size	Modification Time
1	22-07-25_16-19-51.cap	85356	Mon Jul 25 16:20:06 2022

Sniffer		
Item	**Description**	**Default**
Interface	Choose interface according to your Ethernet configuration.	All
Host	Filter packet that contains the specified IP address.	Null
Packets Request	Set packet number that the device can sniffer at a time.	1000
Protocol	Select from “All”, “IP”, “TCP”, “UDP” and “ARP”.	All
Status	Show current status of sniffer.	--
Start	Click the button to start sniffer.	--
Stop	Click the button to stop the sniffer. Once you click this button, a new log file will be displayed in the following List.	--
Capture Files	Every time of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List click ⬇ to download the log and click ✕ to delete the log file. It can cache a maximum of 5 files.	--

3.7.5 Profile

This section allows you to import or export the configuration file, and restore the device to the factory default setting.



Import Configuration File

Reset Other Settings to Default: OFF

Ignore Invalid Settings: OFF

XML Configuration File: Choose File No file chosen Import

Export Configuration File

Ignore Disabled Features: OFF

Add Detailed Information: OFF

Encrypt Secret Data: ON

XML Configuration File: Generate

Default Configuration

Save Running Configuration as Default: Save

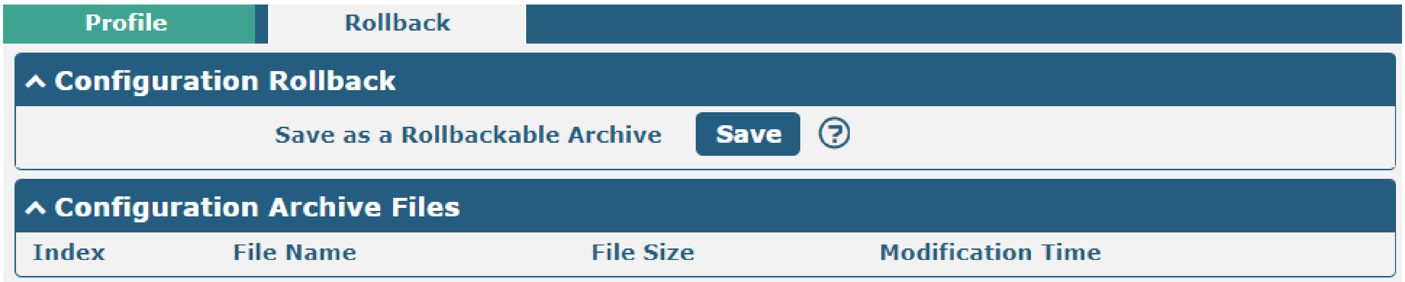
Restore to Default Configuration: Restore

Profile		
Item	**Description**	**Default**
Import Configuration File		
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 “OFF” 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.	--
Export Configuration File		
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.	--

Default Configuration		
Save Running Configuration as Default	Click Save button to save the current running parameters as the default configuration.	--
Restore to Default Configuration	Click the button to restore the factory defaults.	--

Rollback

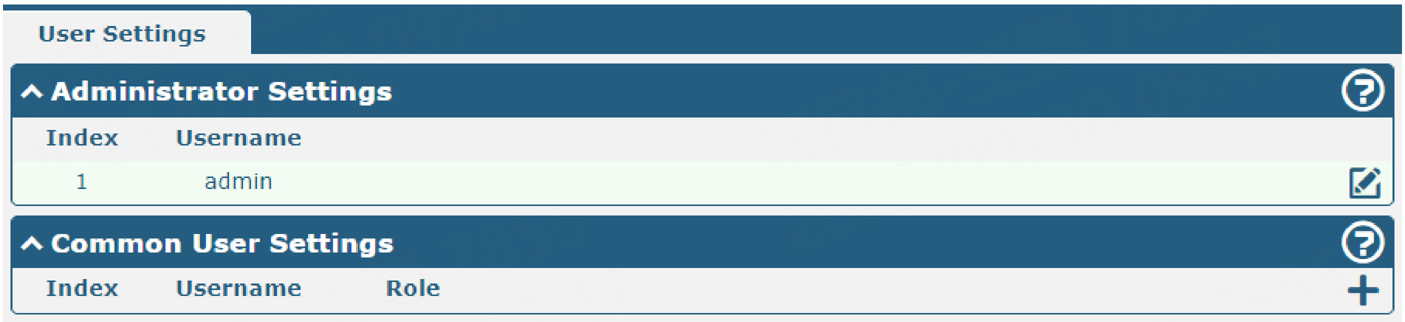
This section allows you to roll back the configuration.



Rollback		
Item	**Description**	**Default**
Configuration Rollback		
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		
Configuration Archive Files	View related information about configuration archive files, including name, size, and modification time.	--

3.7.6 User Management

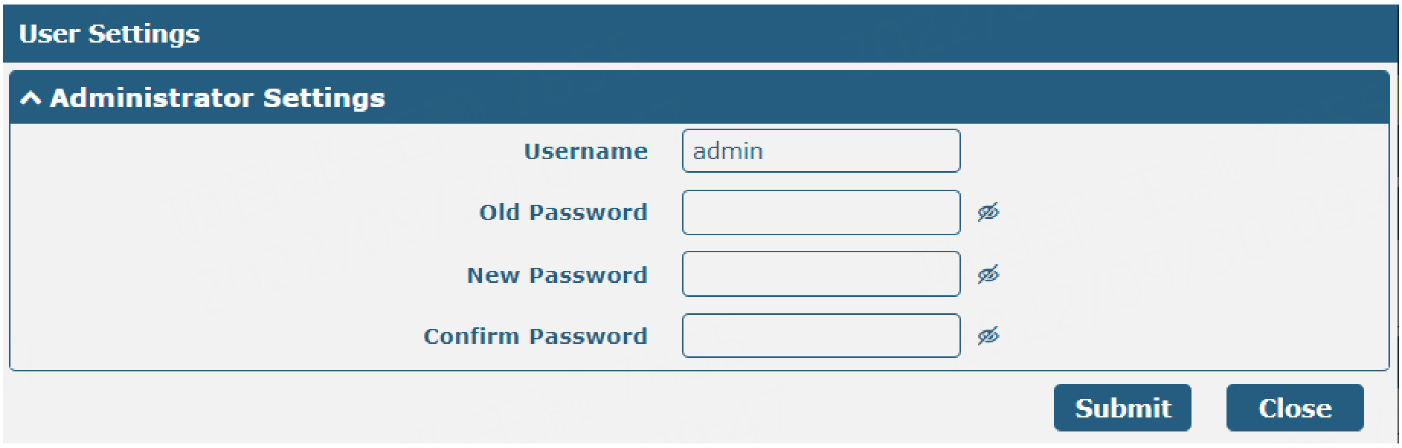
This section allows you to change your username and password, and create or manage user accounts.



Index	Username
1	admin

Index	Username	Role

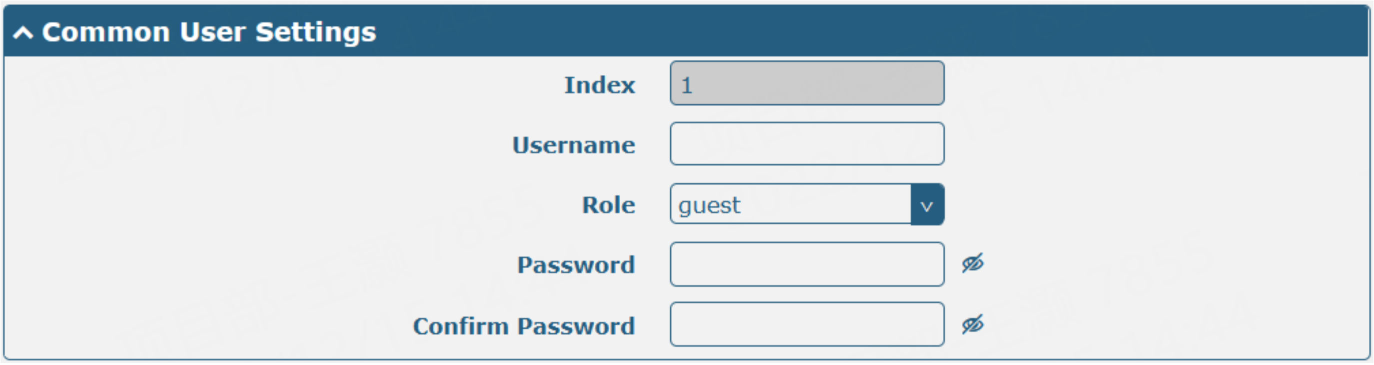
Click ✎ to modify Administrator information.



Username	admin
Old Password	
New Password	
Confirm Password	

Admittatur Settings		
Item	**Description**	**Default**
Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Null
Old Password	Enter old password of your device. The default is “admin”.	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 new password again to confirm.	Null

Click + to Add a Common User.

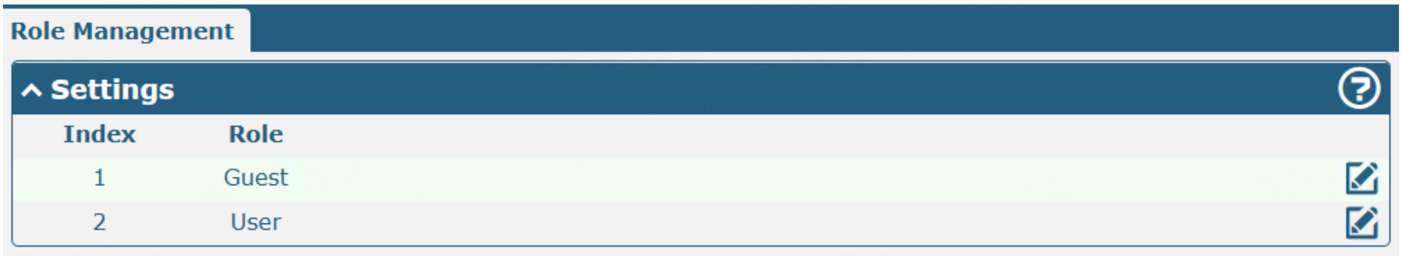


Index	1
Username	
Role	guest
Password	
Confirm Password	

Common User Settings		
Item	**Description**	**Default**
Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Null
Role	Select common user role. Select from User or Guest	Gust
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Null
Confirm Password	Enter new password again to confirm.	Null

3.7.7 Role Management

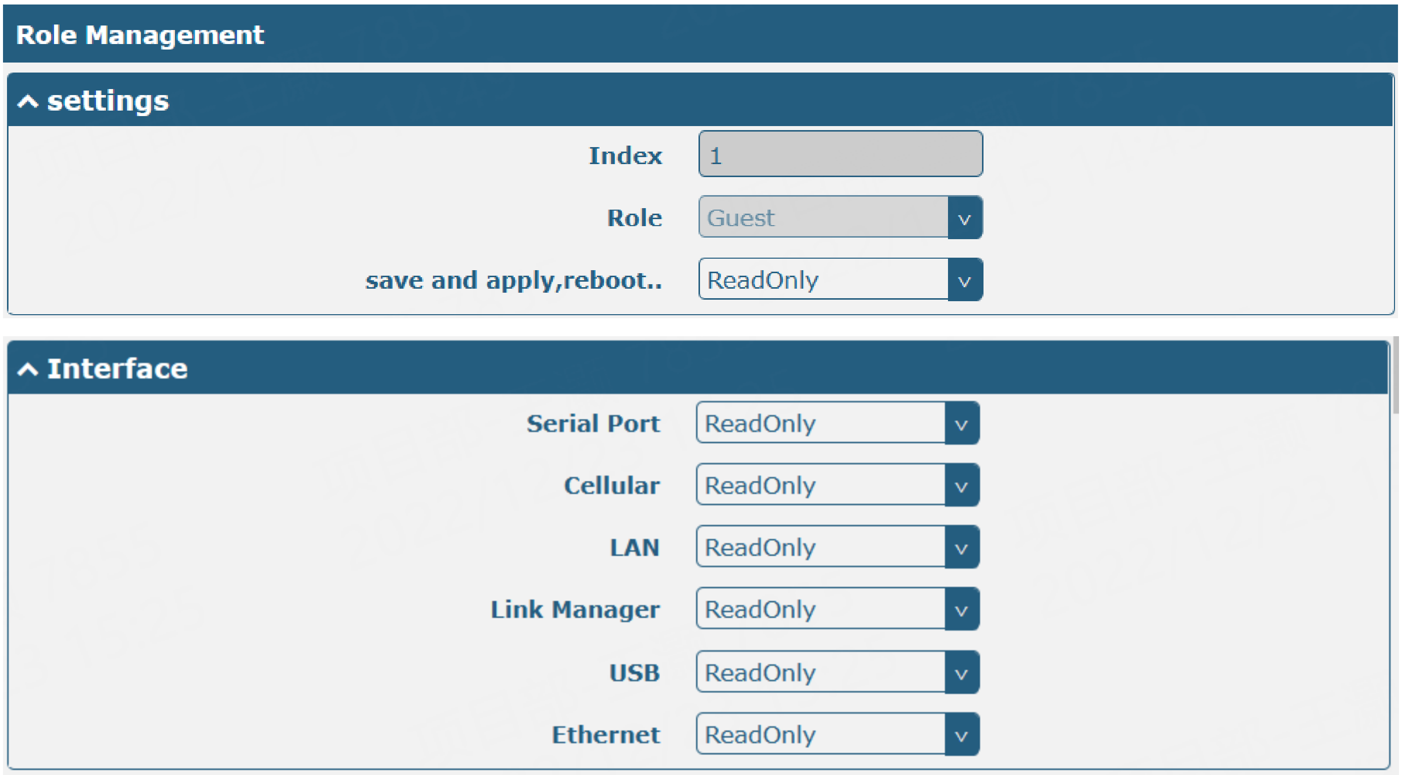
This section is used to manage user roles and manage permissions for users in different roles.



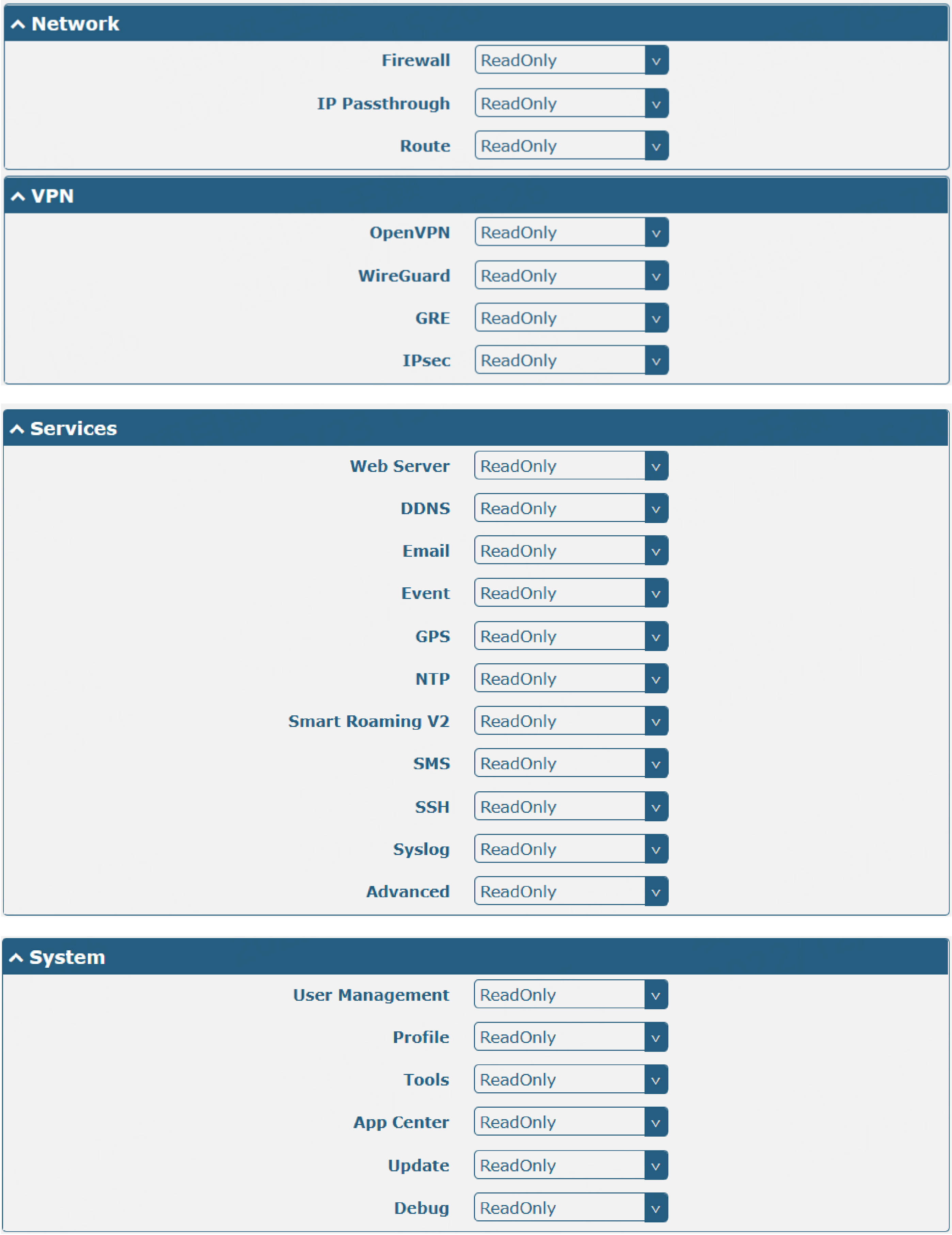
Index	Role
1	Guest
2	User

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

Click ✎ to edit Guest/User permission.



Index	1
Role	Guest
save and apply,reboot..	ReadOnly
Serial Port	ReadOnly
Cellular	ReadOnly
LAN	ReadOnly
Link Manager	ReadOnly
USB	ReadOnly
Ethernet	ReadOnly



^ Network

Firewall	ReadOnly
IP Passthrough	ReadOnly
Route	ReadOnly

^ VPN

OpenVPN	ReadOnly
WireGuard	ReadOnly
GRE	ReadOnly
IPsec	ReadOnly

^ Services

Web Server	ReadOnly
DDNS	ReadOnly
Email	ReadOnly
Event	ReadOnly
GPS	ReadOnly
NTP	ReadOnly
Smart Roaming V2	ReadOnly
SMS	ReadOnly
SSH	ReadOnly
Syslog	ReadOnly
Advanced	ReadOnly

^ System

User Management	ReadOnly
Profile	ReadOnly
Tools	ReadOnly
App Center	ReadOnly
Update	ReadOnly
Debug	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:

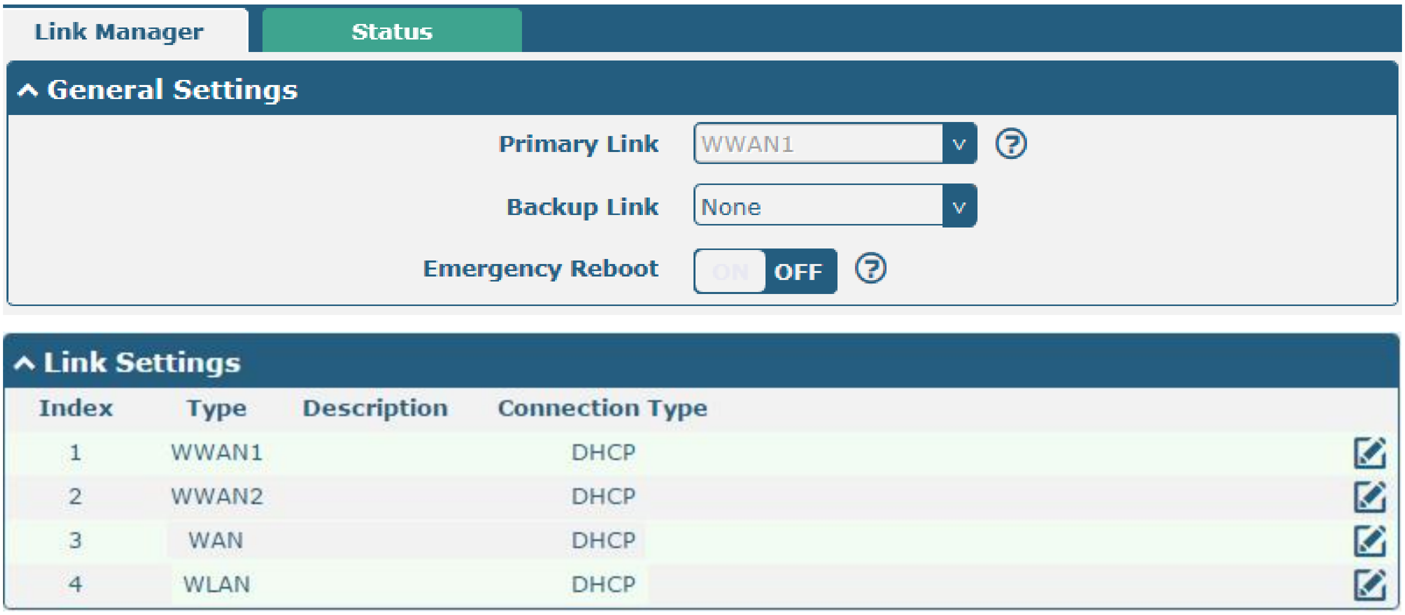
1. When logging in with Guest/User, “Profile” is not available.
2. When Guest “Save and apply, reboot” permission was set to “ReadOnly”. After logging as Guest, “save and apply”, “reboot” buttons will not be displayed.

4. Configuration Examples

4.1 Cellular

4.1.1 Cellular Dial-Up

This section shows you how to configure the primary and backup SIM card for Cellular Dial-up. Connect the device correctly and insert two SIM, then open the configuration page. Under the homepage menu, click "**Interface > Link Manager > Link Manager > General Settings"**, choose "WWAN1" as the primary link and "WWAN2" as the backup link, and set "Cold Backup" as the backup mode, then click "Submit".



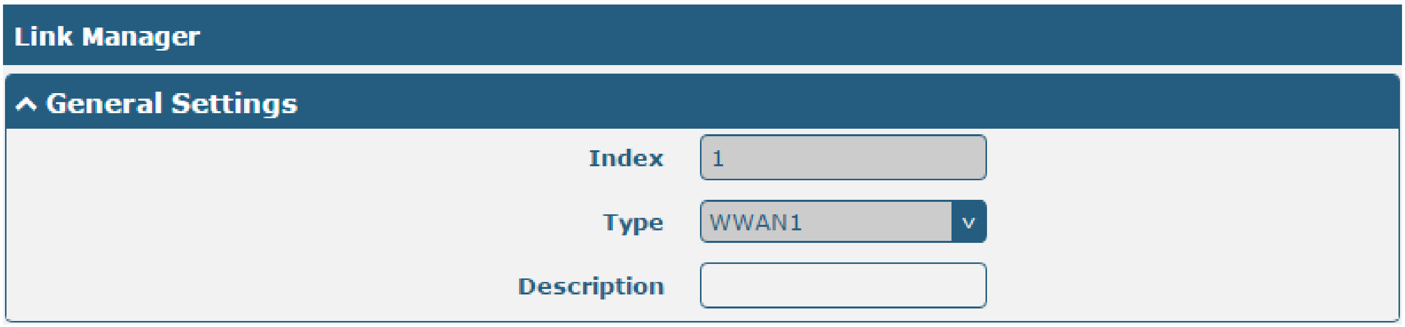
General Settings

Primary Link	WWAN1
Backup Link	None
Emergency Reboot	ON OFF

Link Settings

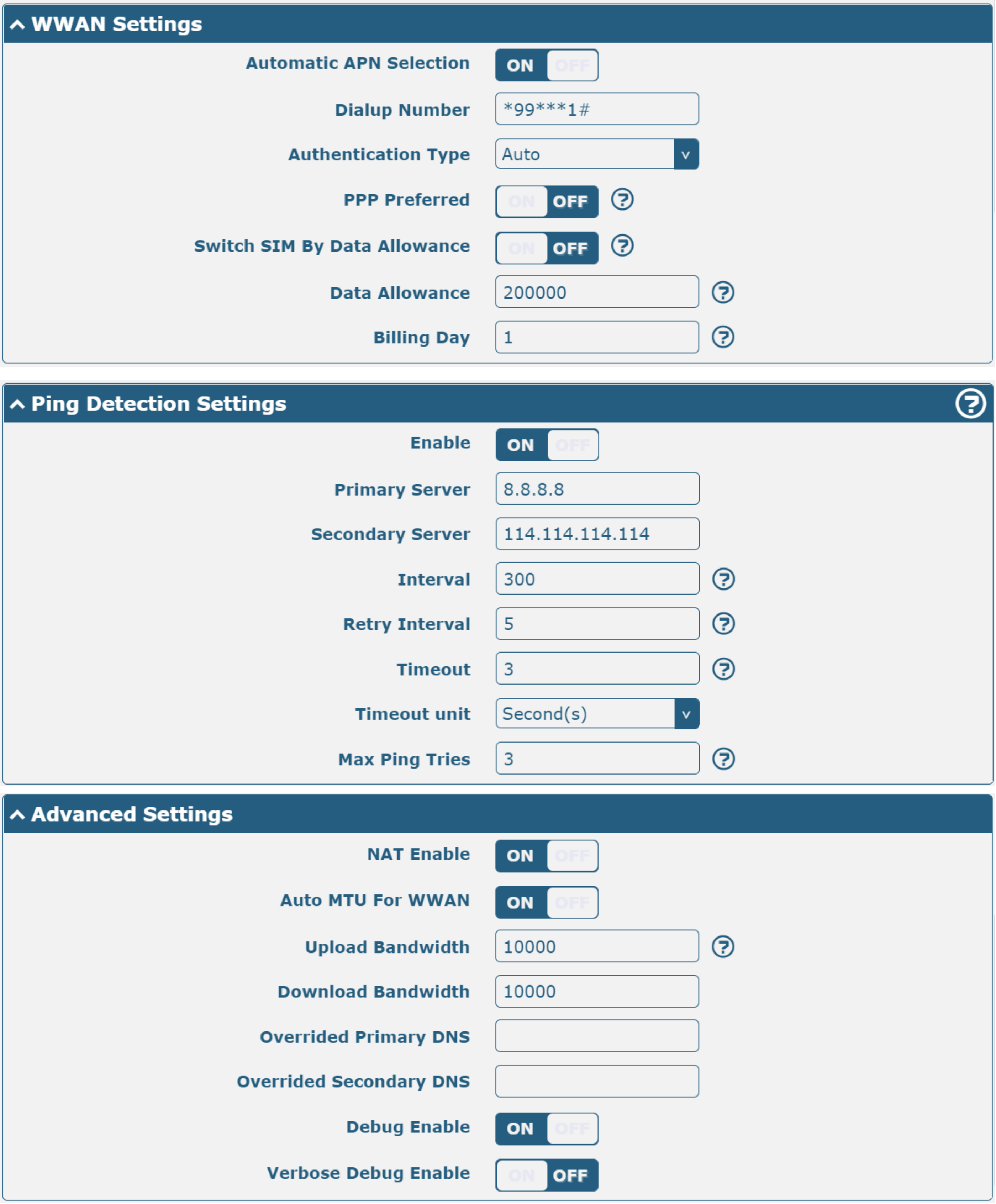
Index	Type	Description	Connection Type
1	WWAN1		DHCP
2	WWAN2		DHCP
3	WAN		DHCP
4	WLAN		DHCP

Click the ✎ button of WWAN1 to set its parameters according to the current ISP.



General Settings

Index	1
Type	WWAN1
Description	



WWAN Settings

Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
PPP Preferred	OFF
Switch SIM By Data Allowance	OFF
Data Allowance	200000
Billing Day	1

Ping Detection Settings

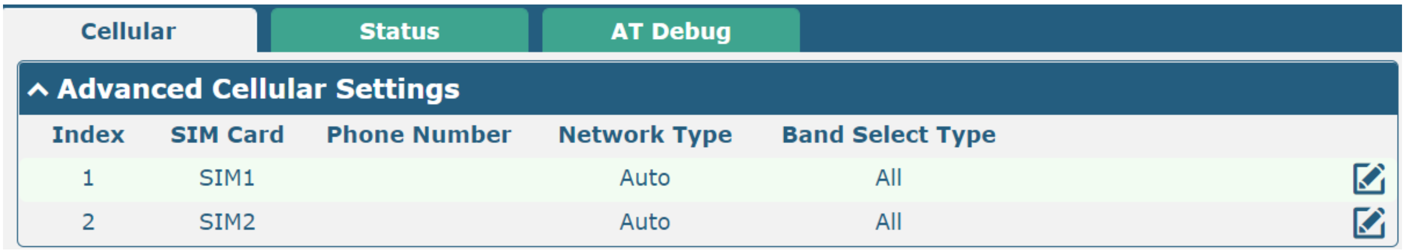
Enable	ON
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Timeout unit	Second(s)
Max Ping Tries	3

Advanced Settings

NAT Enable	ON
Auto MTU For WWAN	ON
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Debug Enable	ON
Verbose Debug Enable	OFF

When finished, click “**Submit > Save & Apply”** for the configuration to take effect.

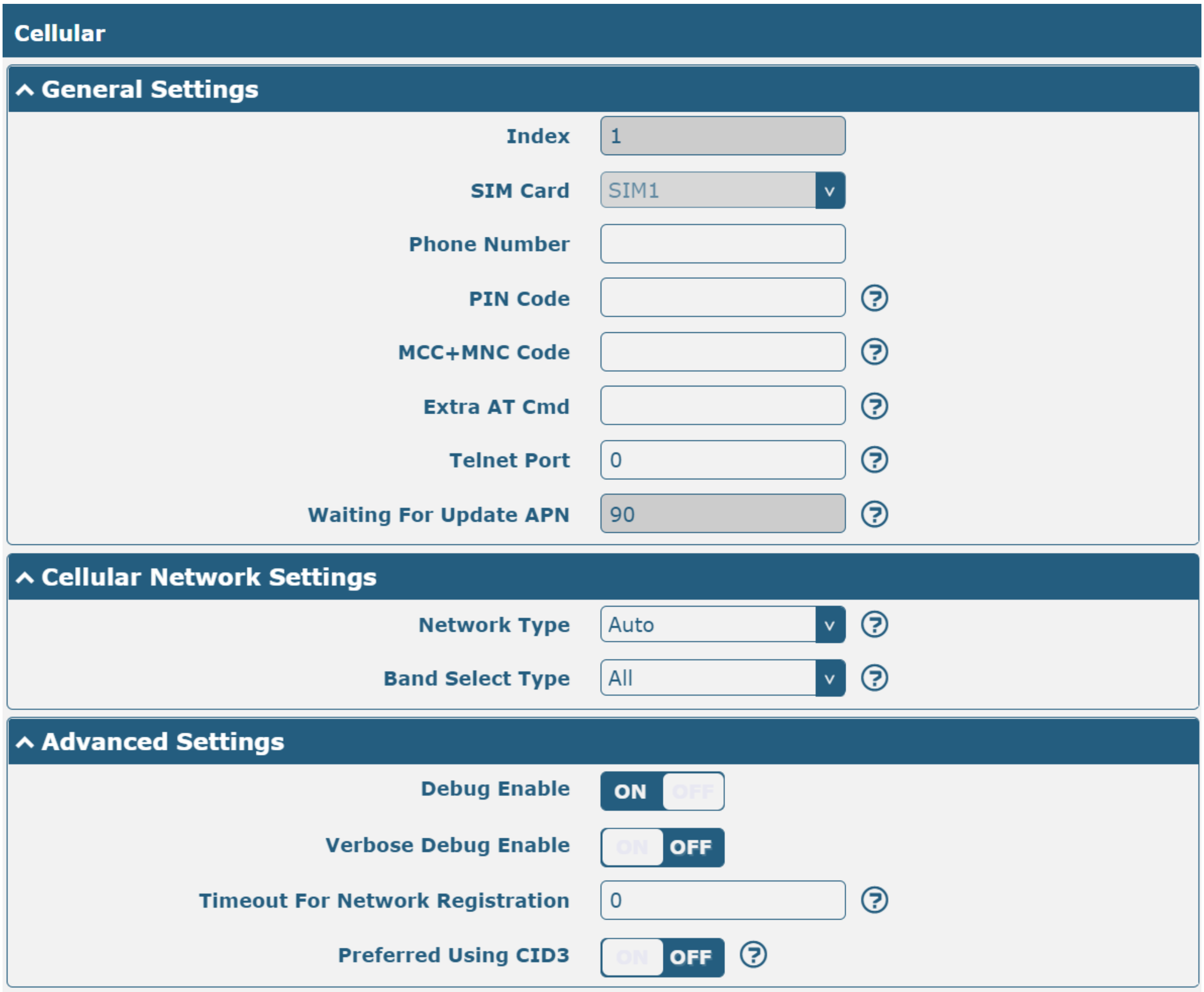
The window is displayed below by clicking “**Interface > Cellular > Advanced Cellular Settings”**.



^ Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type
1	SIM1		Auto	All
2	SIM2		Auto	All

Click edit button of SIM1 to set its parameters according to your application request.



Cellular

^ General Settings

Index	1
SIM Card	SIM1
Phone Number	
PIN Code	
MCC+MNC Code	
Extra AT Cmd	
Telnet Port	0
Waiting For Update APN	90

^ Cellular Network Settings

Network Type	Auto
Band Select Type	All

^ Advanced Settings

Debug Enable	ON
Verbose Debug Enable	OFF
Timeout For Network Registration	0
Preferred Using CID3	OFF

When finished, click “**Submit > Save & Apply”** for the configuration to take effect.

4.1.2 SMS Remote Control

R2011 supports remote control via SMS. You can use the following commands to get the status of the device, and set all the parameters of the device.

SMS commands 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 to the device'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 device's phone group).

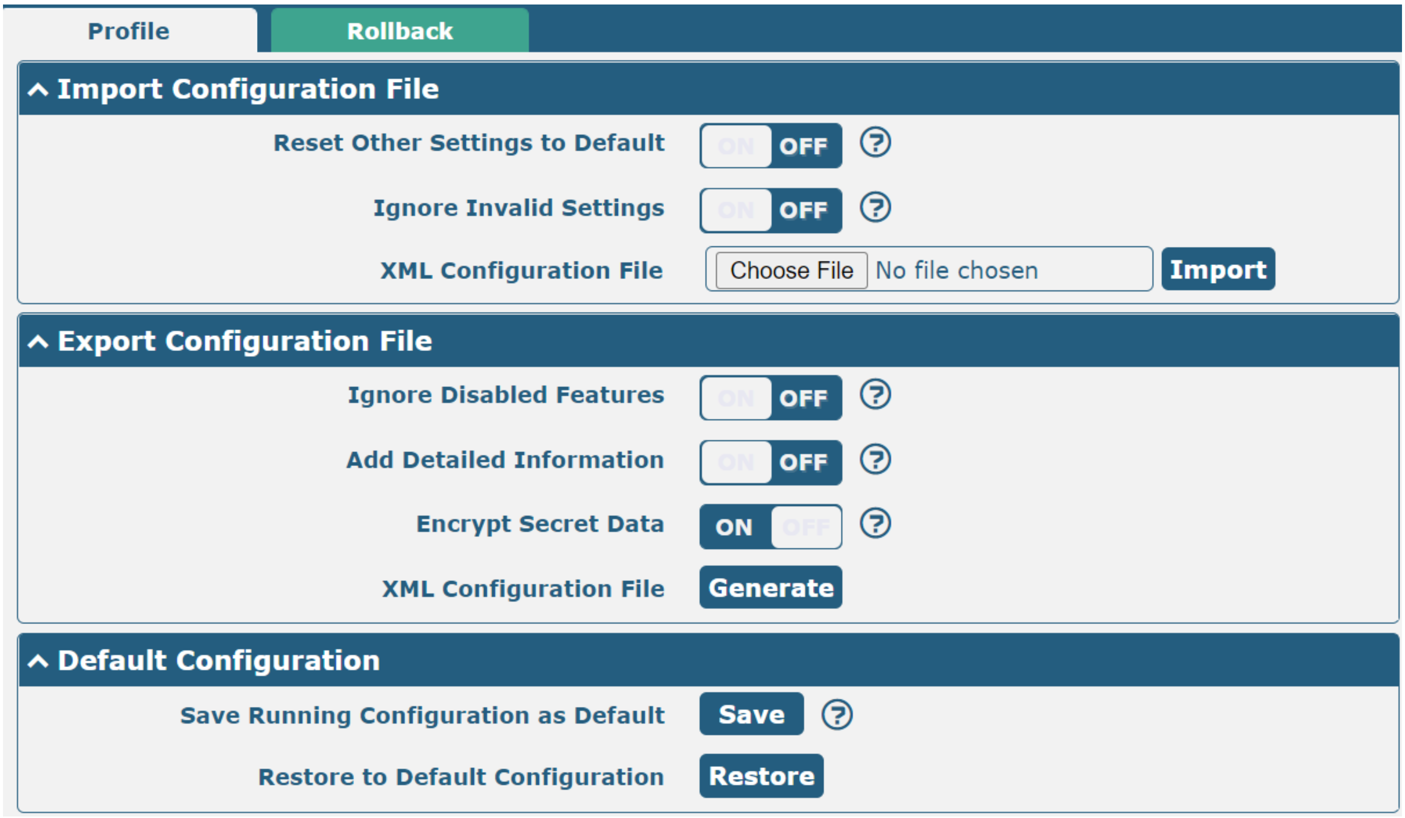
Note: All command symbols must be entered in the half-angle mode of the English input method.

SMS command Explanation:

1. Username and Password: Use the same username and password as the 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 configured XML file from the configured web browser. The format of the 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.



Profile | Rollback

Import Configuration File

Reset Other Settings to Default: OFF

Ignore Invalid Settings: OFF

XML Configuration File: Choose File No file chosen | Import

Export Configuration File

Ignore Disabled Features: OFF

Add Detailed Information: OFF

Encrypt Secret Data: ON

XML Configuration File: Generate

Default Configuration

Save Running Configuration as Default: Save

Restore to Default Configuration: Restore

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 command packed in a single SMS.
4. E.g.

admin:admin;status system

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

SMS received:

```
hardware_version = 1.0
firmware_version = beta210618
firmware_version_full = "beta210618 (Rev 4250)"
kernel_version = 4.9.152
device_model = R2011
serial_number = ""
uptime = "0 days, 01:25:16"
system_time = "Tue Apr 21 17:09:04 2021"
ram_usage = "77M Free/128M Total"
```

admin:admin;reboot

In this command, the username is "admin", the password is "admin", and the command is to reboot the Device.

SMS received:

```
OK
```

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

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

SMS received:

OK

OK

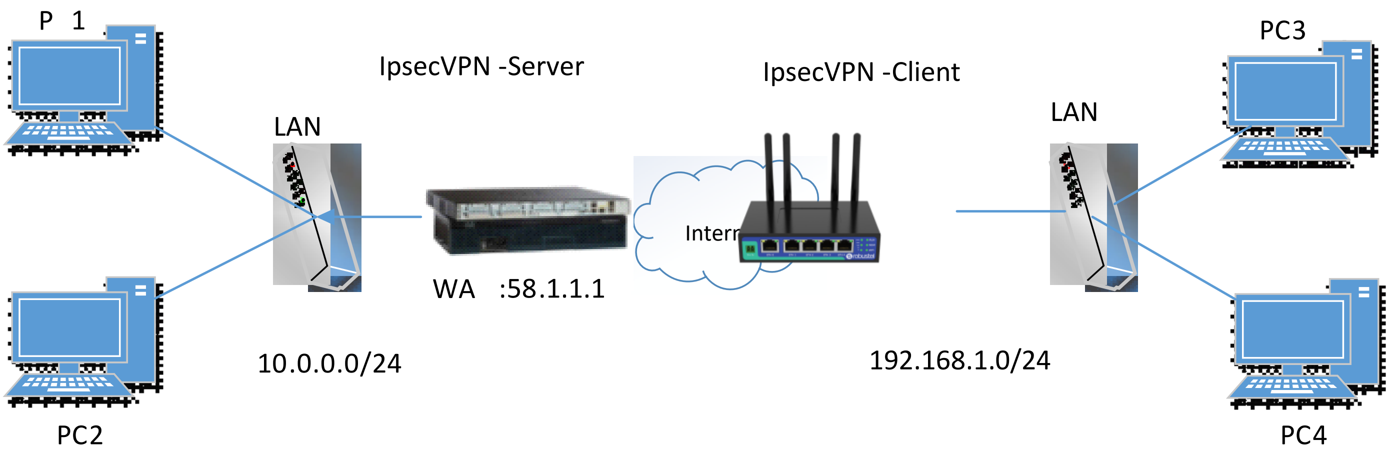
OK

OK

4.2 VPN Configuration Examples

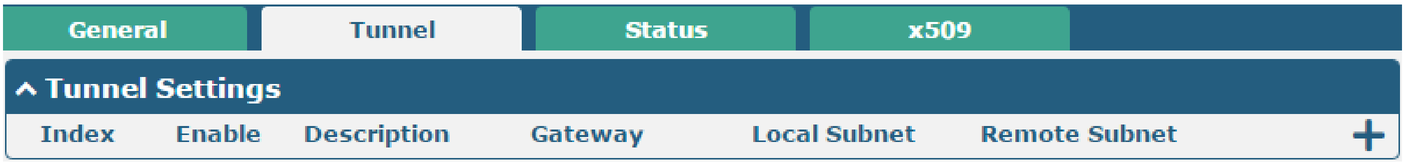
4.2.1 IPsec VPN

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



IPsec VPN_Client:

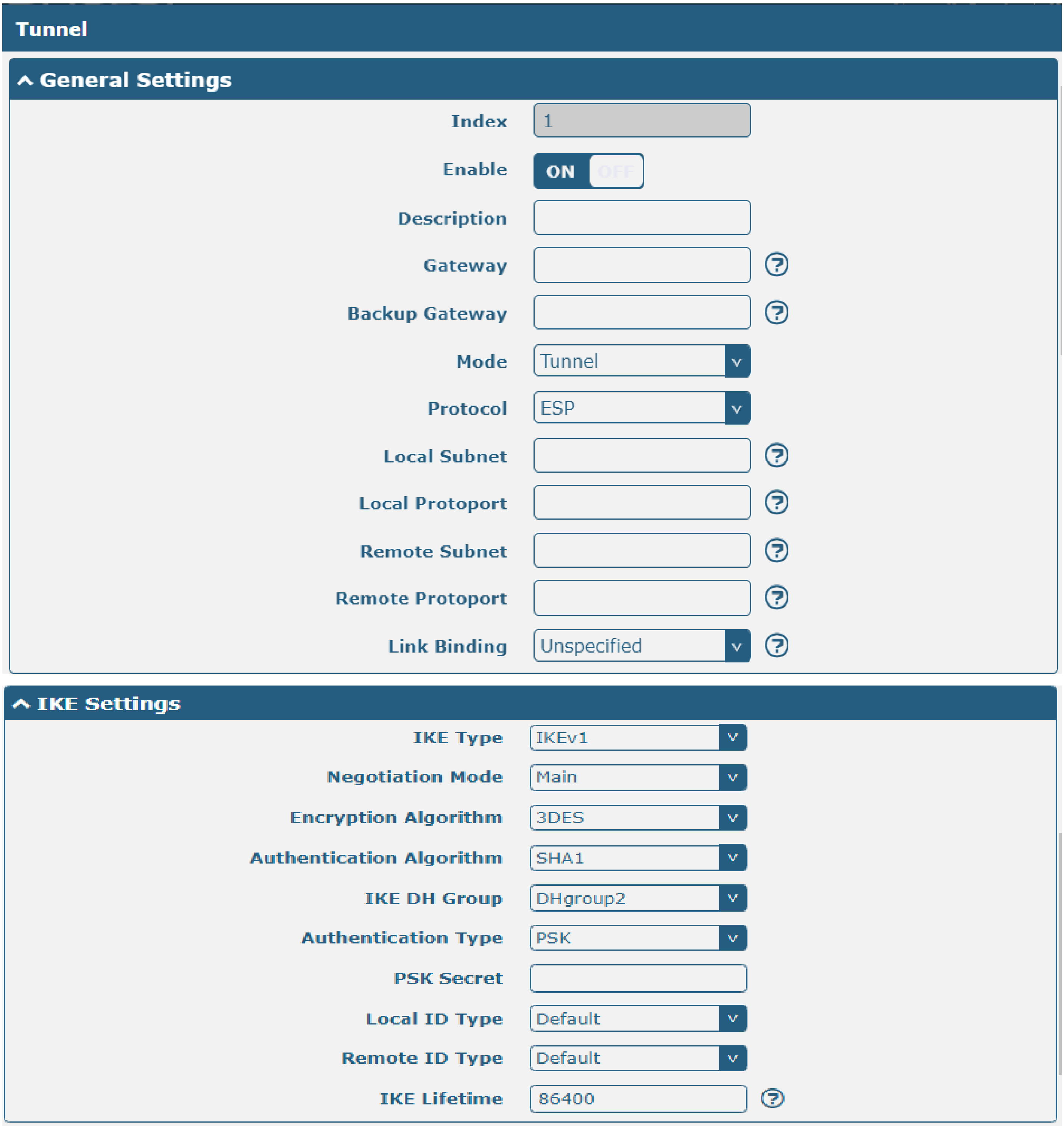
The window is displayed below by clicking “**VPN > IPsec > Tunnel**.”



^ Tunnel Settings

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+

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



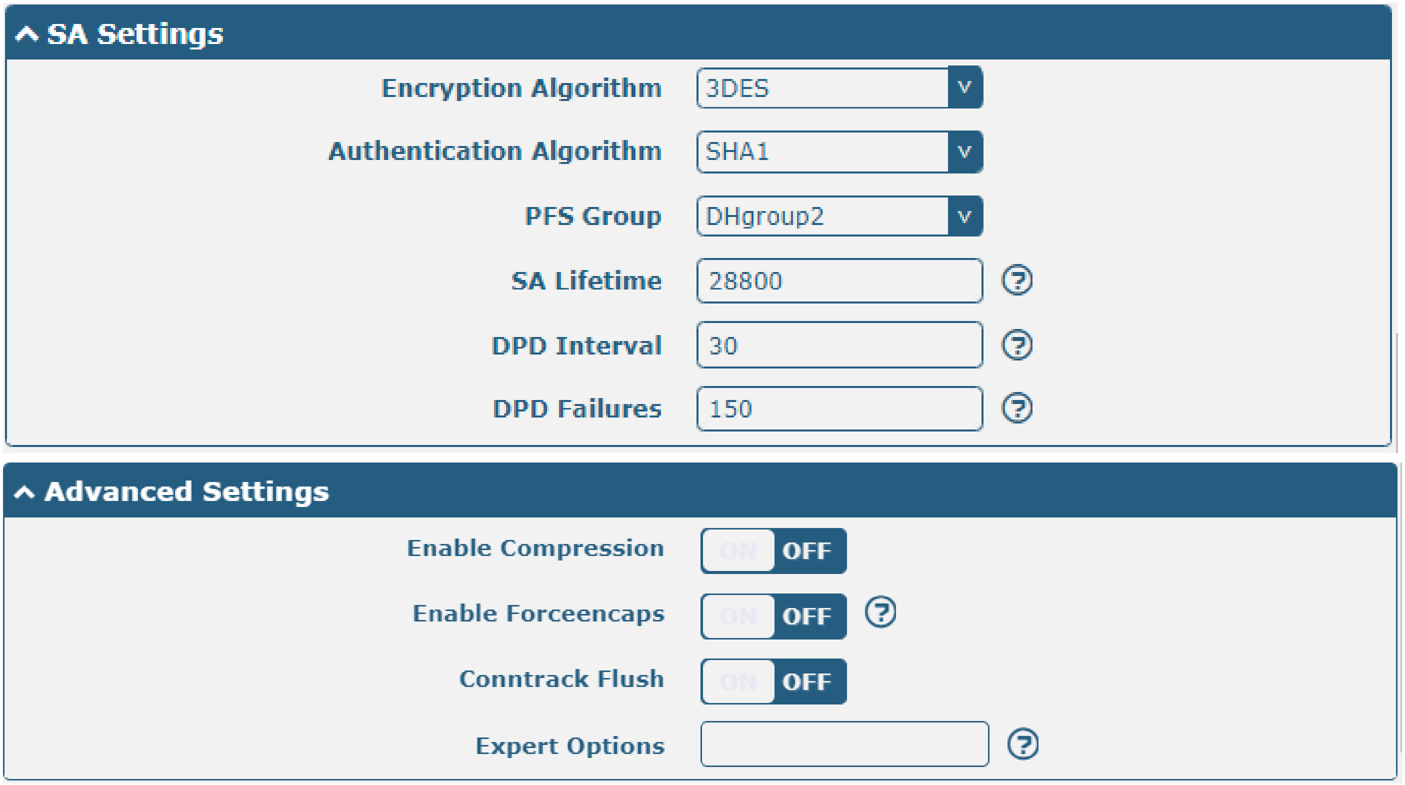
Tunnel

^ General Settings

Index	1
Enable	ON OFF
Description	
Gateway	
Backup Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Local Protoport	
Remote Subnet	
Remote Protoport	
Link Binding	Unspecified

^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400



^ SA Settings

Encryption Algorithm	3DES
Authentication Algorithm	SHA1
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	30
DPD Failures	150

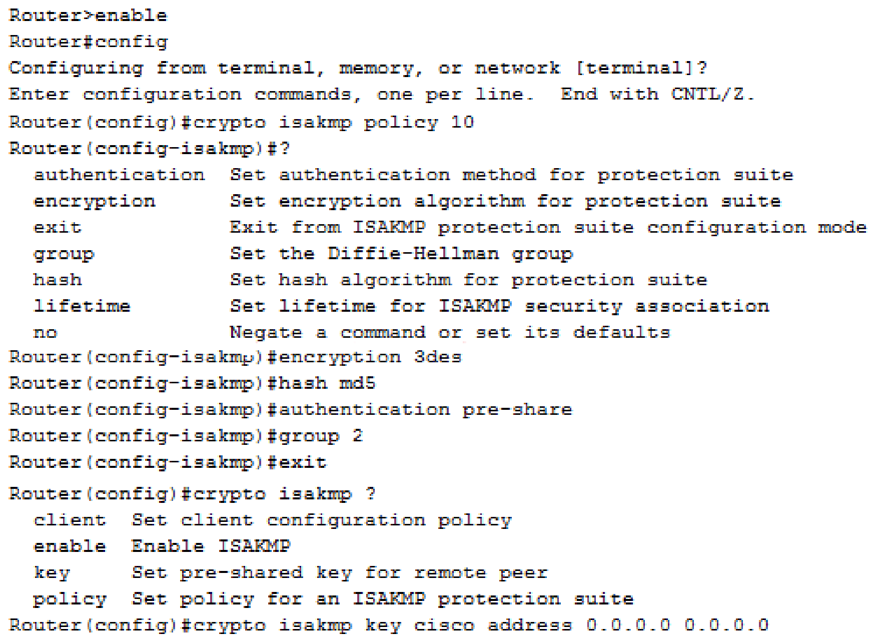
^ Advanced Settings

Enable Compression	ON OFF
Enable Forceencaps	ON OFF
Conntrack Flush	ON OFF
Expert Options	

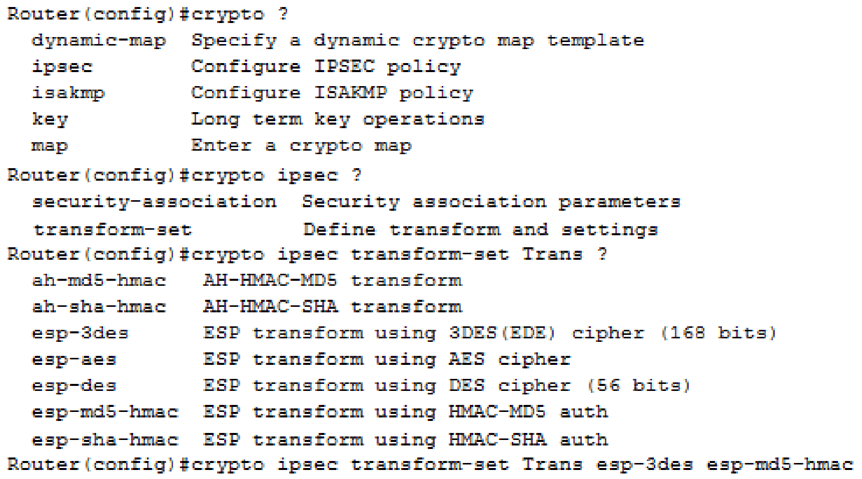
When finished, click “**Submit > Save & Apply”** for the configuration to take effect.

IPsecVPN_Server:

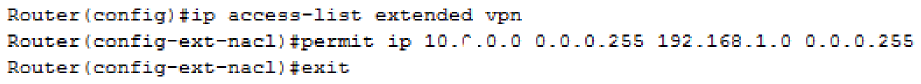
Cisco 2811:



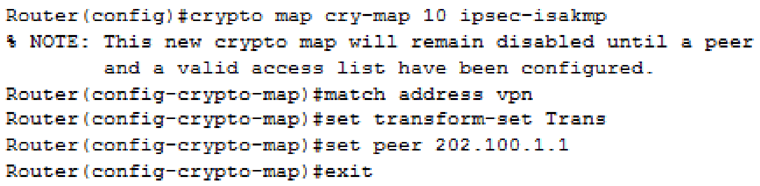
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set 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
```



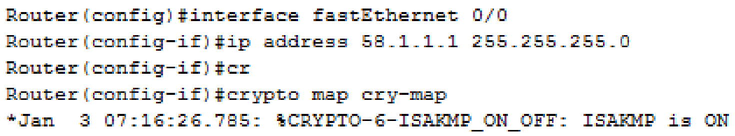
```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association 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
```

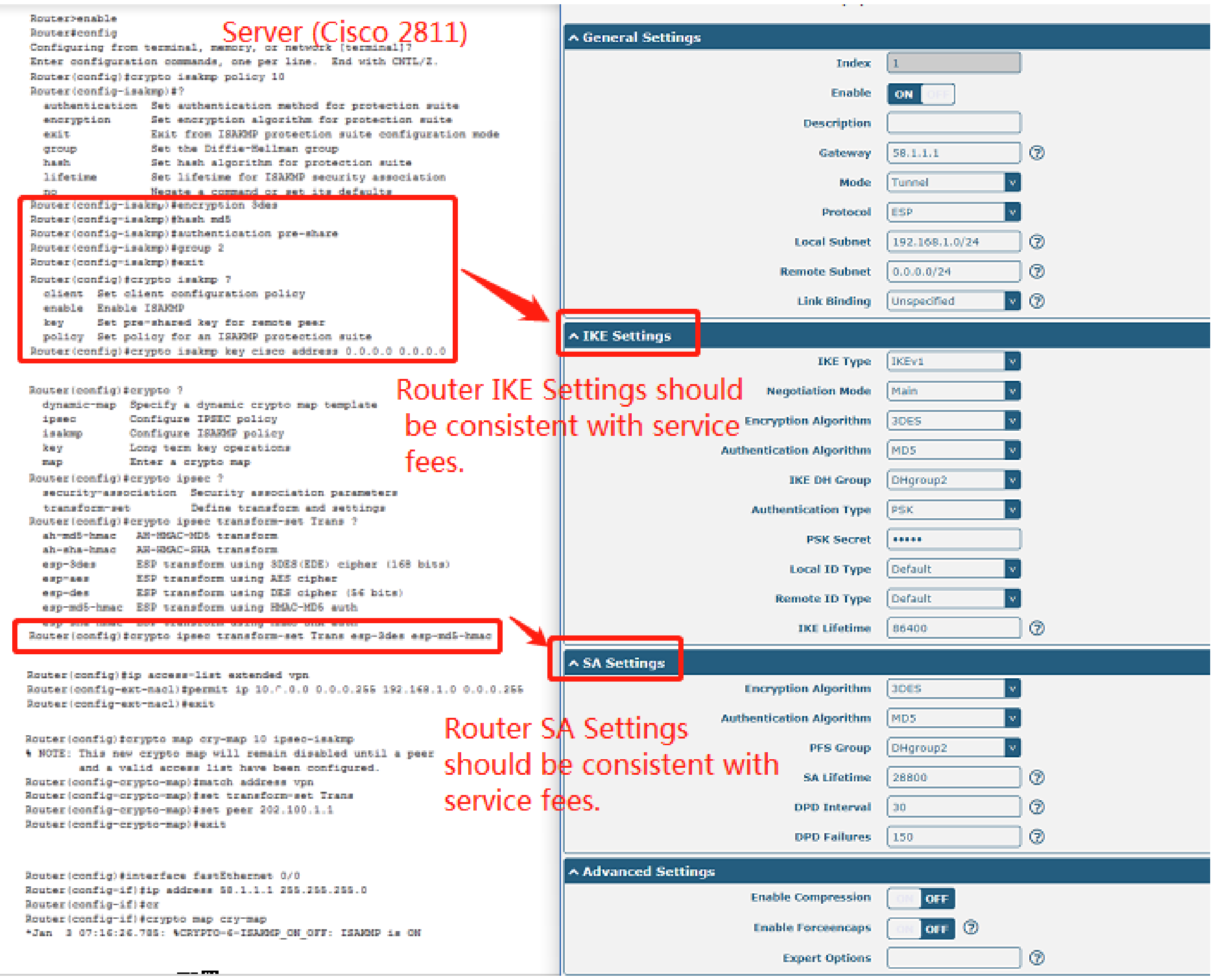


```
Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1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

The comparison between server and client is as below.



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
```

Router IKE Settings should be consistent with service fees.

Router SA Settings should be consistent with service fees.

General Settings

Index	1
Enable	ON
Description	
Gateway	58.1.1.1
Mode	Tunnel
Protocol	ESP
Local Subnet	192.168.1.0/24
Remote Subnet	0.0.0.0/24
Link Binding	Unspecified

IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	MD5
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	•••••
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

SA Settings

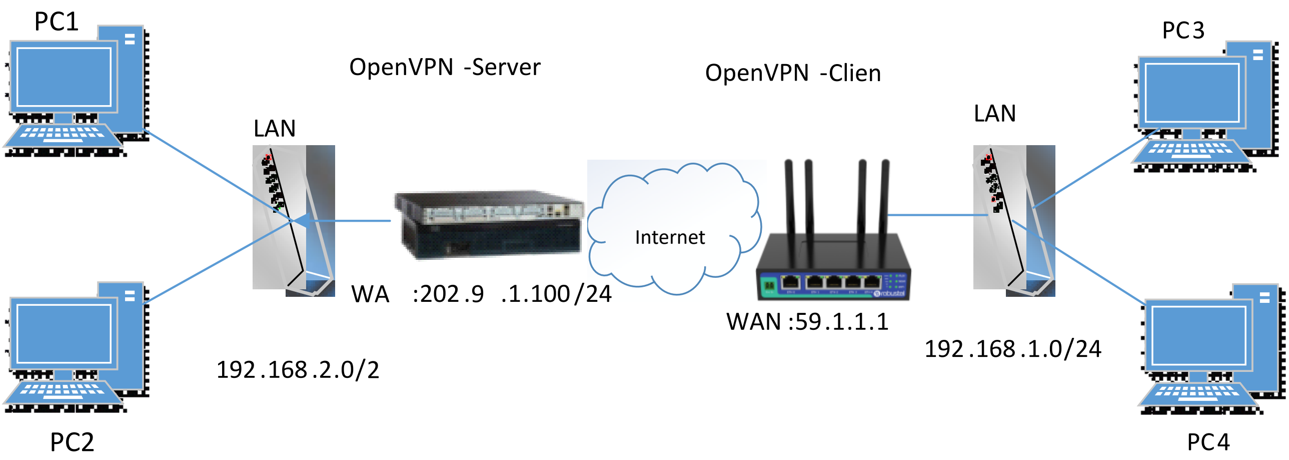
Encryption Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	30
DPD Failures	150

Advanced Settings

Enable Compression	OFF
Enable Forceencaps	OFF
Expert Options	

4.2.2 OpenVPN

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



OpenVPN_Server:

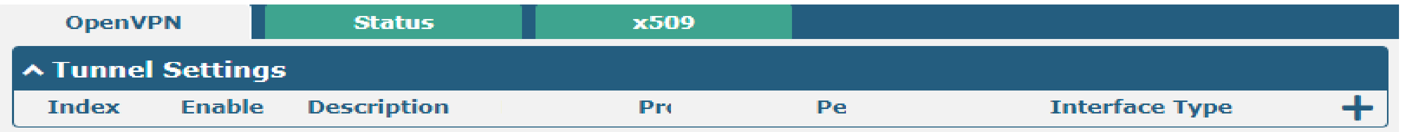
Generate the relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configure the Server:

```
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.

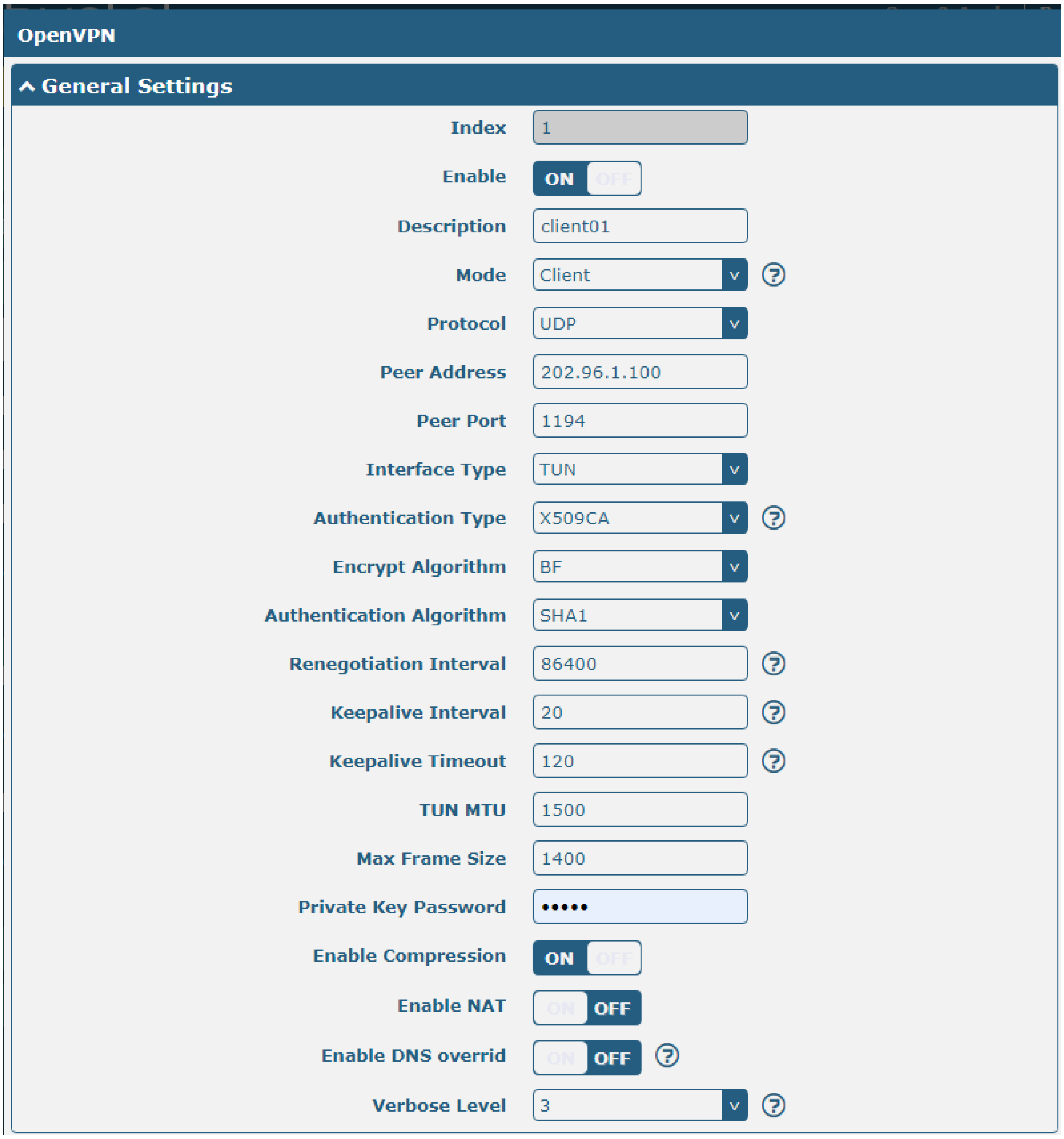
OpenVPN_Client:

Click “**VPN > OpenVPN > OpenVPN**” as below.



Index	Enable	Description	Pr	Pe	Interface Type

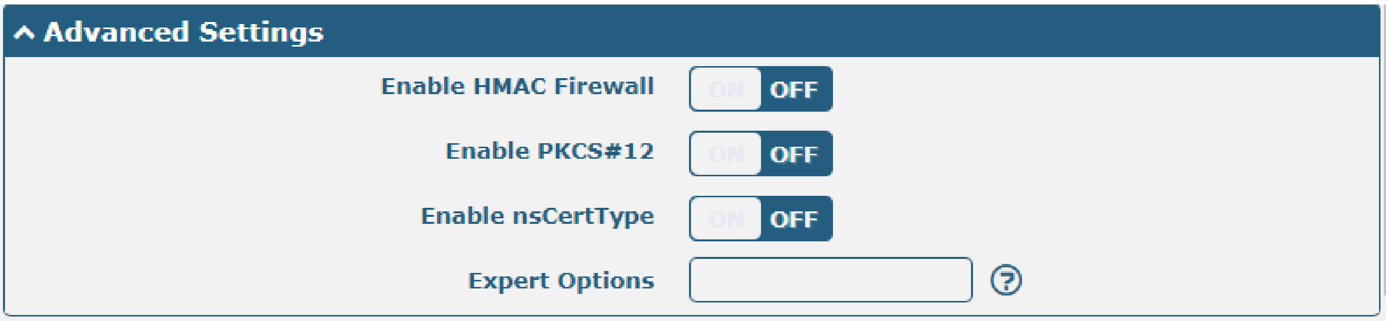
Click + to configure the Client01 as below.



OpenVPN

General Settings

Index	1
Enable	ON
Description	client01
Mode	Client
Protocol	UDP
Peer Address	202.96.1.100
Peer Port	1194
Interface Type	TUN
Authentication Type	X509CA
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	1400
Private Key Password	•••••
Enable Compression	ON
Enable NAT	OFF
Enable DNS overrid	OFF
Verbose Level	3



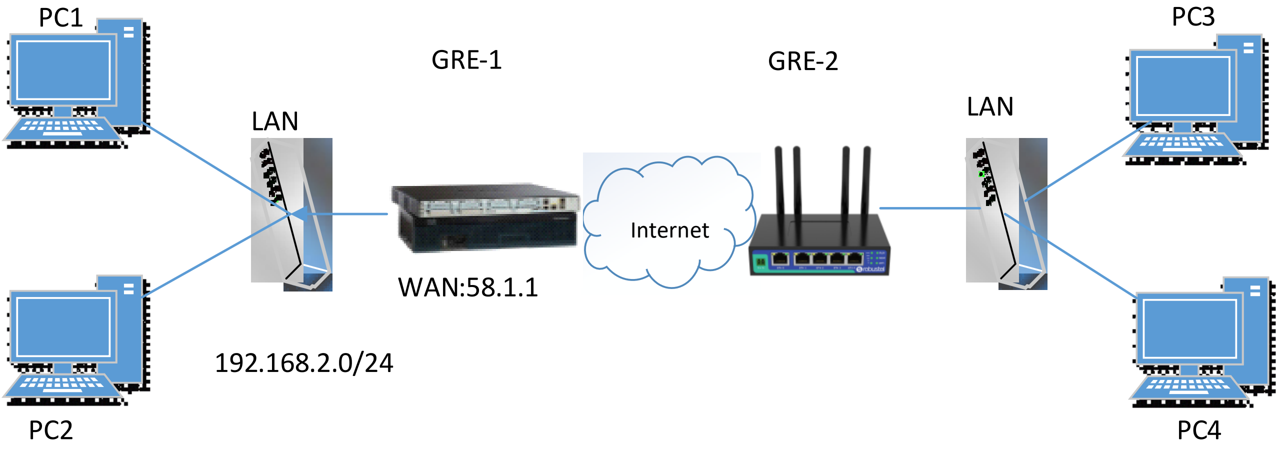
Advanced Settings

Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Enable nsCertType	OFF
Expert Options	

When finished, click “**Submit > Save & Apply”** for the configuration to take effect.

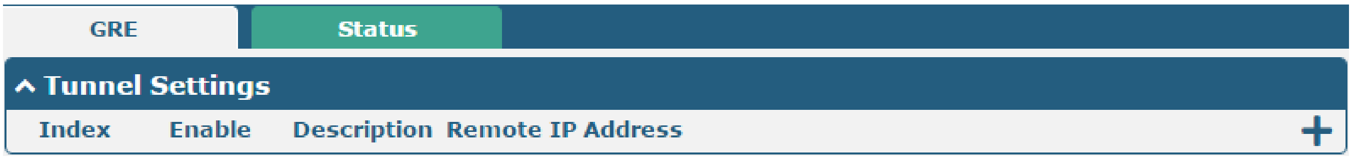
4.2.3 GRE VPN

GRE VPN topology



GRE-1:

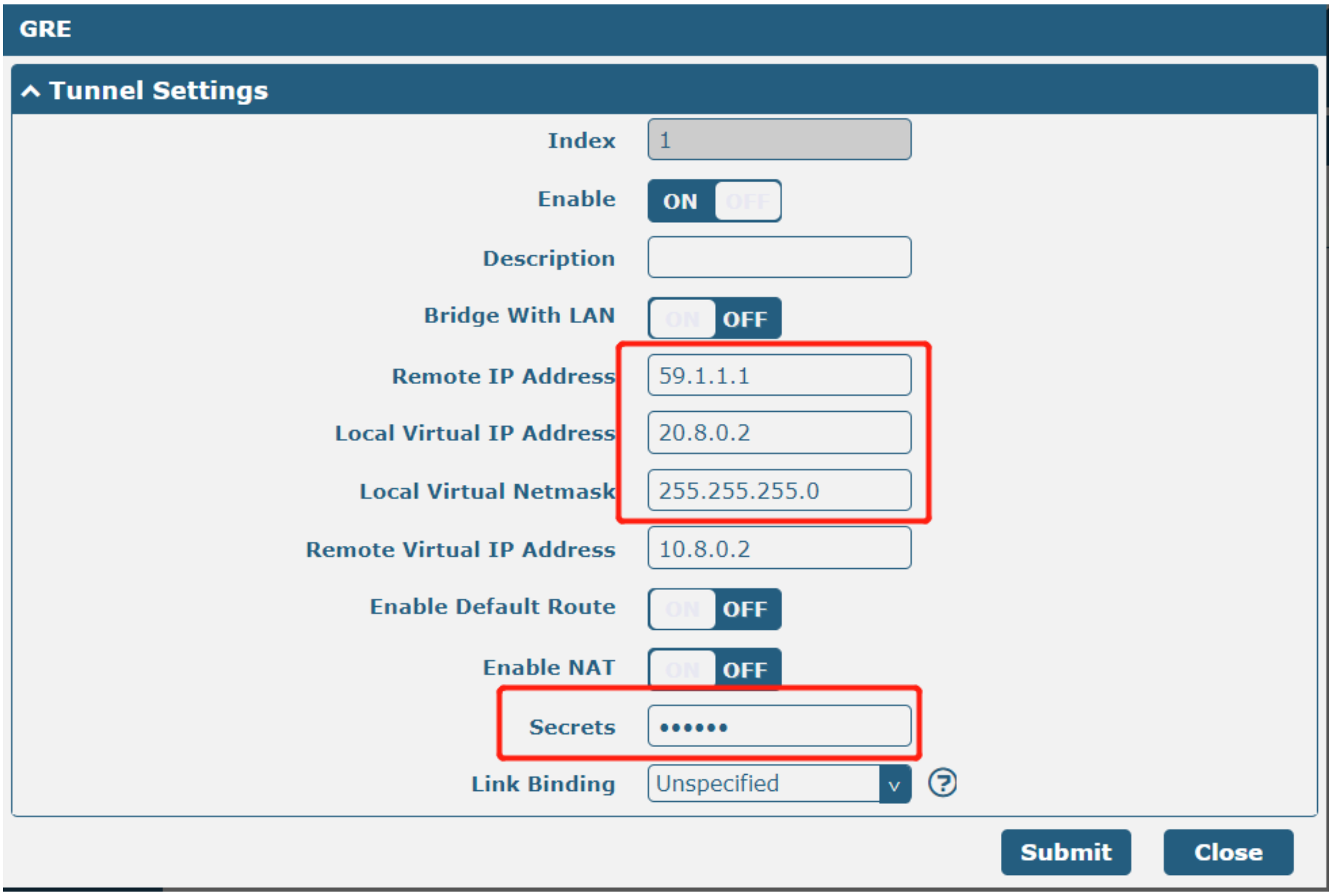
The window is displayed below by clicking “**VPN > GRE > GRE**”.



^ Tunnel Settings

Index	Enable	Description	Remote IP Address	+

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



GRE

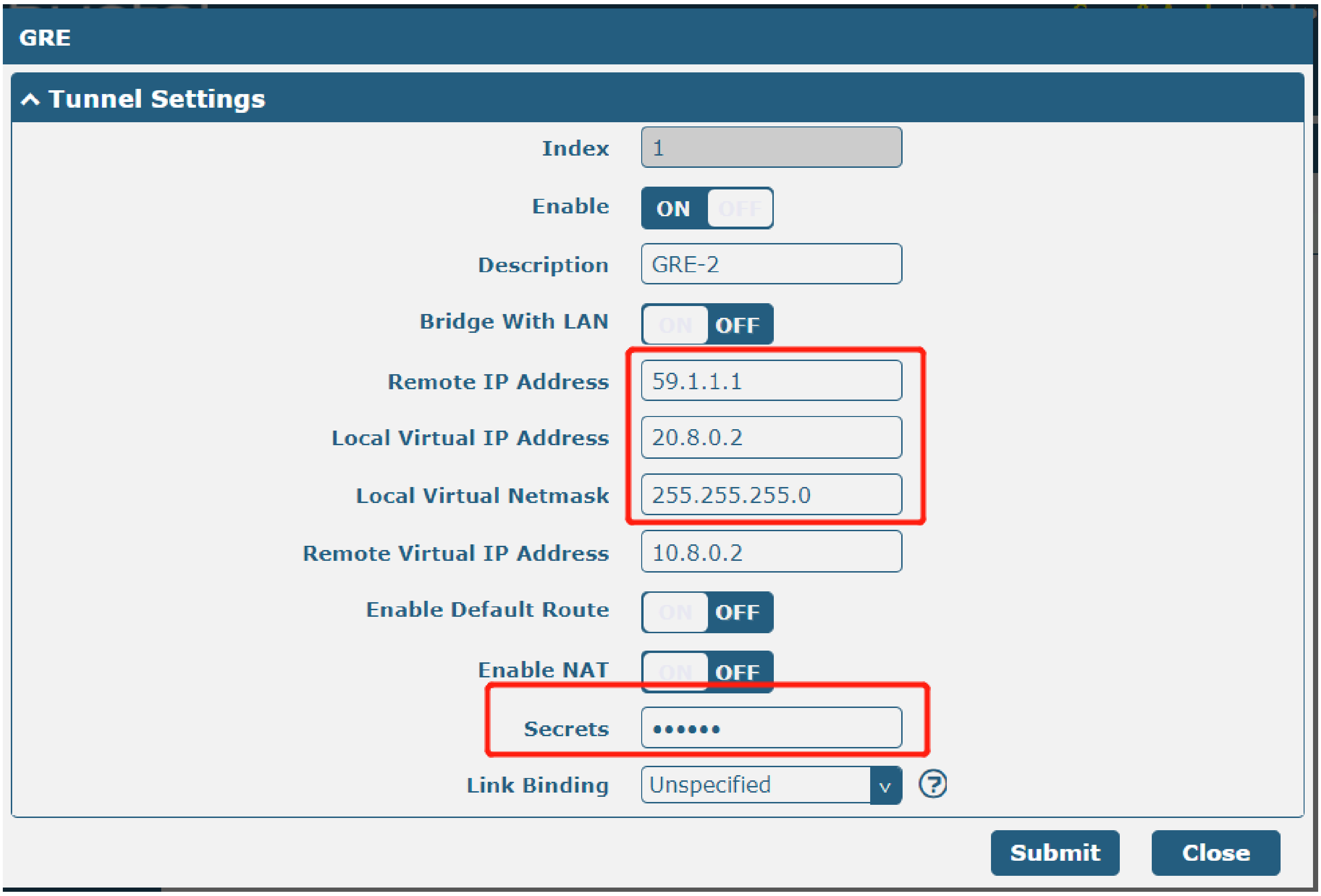
^ Tunnel Settings

Index	1
Enable	ON
Description	
Bridge With LAN	OFF
Remote IP Address	59.1.1.1
Local Virtual IP Address	20.8.0.2
Local Virtual Netmask	255.255.255.0
Remote Virtual IP Address	10.8.0.2
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••
Link Binding	Unspecified

When finished, click “**Submit > Save & Apply**” for the configuration to take effect.

GRE-2:

Click ➕ button and set the parameters of GRE-2 as below.



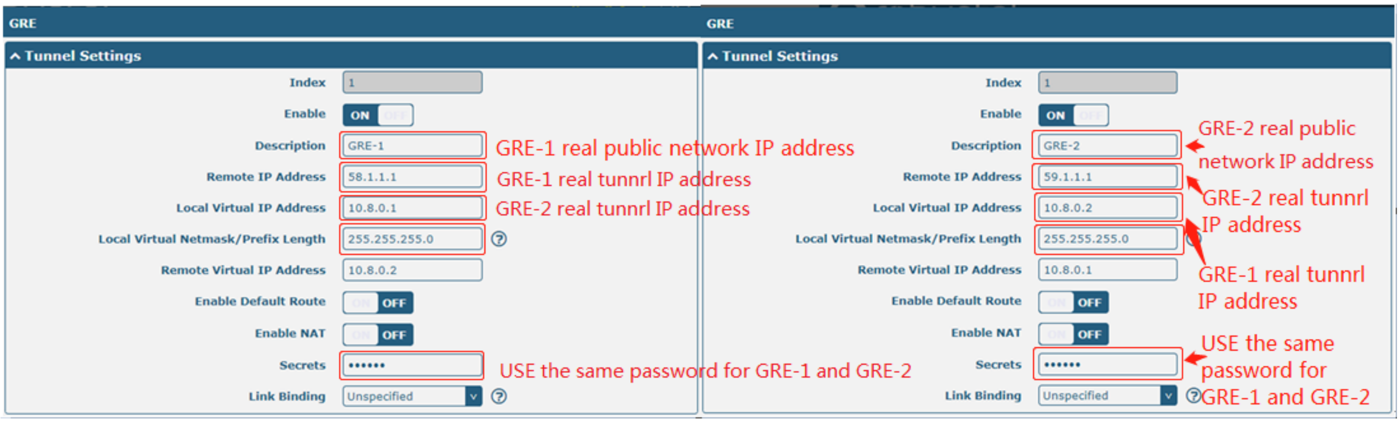
GRE

^ Tunnel Settings

Index	1
Enable	ON
Description	GRE-2
Bridge With LAN	OFF
Remote IP Address	59.1.1.1
Local Virtual IP Address	20.8.0.2
Local Virtual Netmask	255.255.255.0
Remote Virtual IP Address	10.8.0.2
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••
Link Binding	Unspecified

When finished, click “**Submit > Save & Apply”** for the configuration to take effect.

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



GRE

^ Tunnel Settings

Index	1
Enable	ON
Description	GRE-1
Remote IP Address	58.1.1.1
Local Virtual IP Address	10.8.0.1
Local Virtual Netmask/Prefix Length	255.255.255.0
Remote Virtual IP Address	10.8.0.2
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••
Link Binding	Unspecified

GRE-1 real public network IP address

GRE-1 real tunnrl IP address

GRE-2 real tunnrl IP address

USE the same password for GRE-1 and GRE-2

GRE

^ Tunnel Settings

Index	1
Enable	ON
Description	GRE-2
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0
Remote Virtual IP Address	10.8.0.1
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••
Link Binding	Unspecified

GRE-2 real public network IP address

GRE-2 real tunnrl IP address

GRE-1 real tunnrl IP address

USE the same password for GRE-1 and GRE-2

5. Introductions for CLI

5.1 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 device, enter the login account and password (default admin/admin) to enter the configuration mode of the device, as shown below.

Route login:

Device login: admin

Password: admin

#

CLI commands:

```
# ?
   !                 Comments
 add                 Add a list entry of configuration
 add_preferred       smart roaming add preferred plmn list
 clear               Clear statistics
 config              Configuration operation
 debug               Output debug information to the console
 del                 Delete a list entry of configuration
 delete_preferred    smart roaming remove all preferred operators
 do                  Set the level state of the do
 exit                Exit from the CLI
 force_rescan        smart roaming network rescan
 forget_rplmn        smart roaming forget rplmn
 help                Display an overview of the CLI syntax
 ipsec_cert_get      Download IPSec certificate file via http or ftp
 ovpn_cert_get       Download OpenVPN certificate file via http or ftp
 ping                Send messages to network hosts
 reboot              Halt and perform a cold restart
 saveConfig          Save Running Configuration as Default
 select              smart roaming select operator
 set                 Set system configuration
 show                Show system configuration
 show_networks       show networks that scanf
 speedtest           speedtest
```

status	Show running system information
tftp_upload_diagnostic	Generate diagnostic files and upload them using TFTP
tftpupdate	Update firmware or configuration file using tftp
traceroute	Print the route packets trace to network host
trigger	Trigger action
uninstall	Uninstall App
UploadConfig	Upload Current UCI Config to FTP Server
urlupdate	Update firmware via http or ftp
ver	Show version of firmware

5.2 How to Configure the CLI

Following is a table about the description of help and the error that 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 the changed configuration save_and_apply Save the configuration changes and take effect the changed configuration loaddefault Restore Factory Configuration
Ctrl+c	Press these two keys at the same time, except for its “copy” function but also can be used to “break” out of the setting program.
Syntax error: The command is not completed	The command is not completed.
Tick space key+ Tab key	It can help you finish your 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 is finished, you should enter those commands to make your setting take effect on the device. ***Note:*** *Commit and save_and_apply play the same role.*

5.3 Commands Reference

Commands	Syntax	Description
Debug	Debug *parameters*	Turn on or turn off debug function
Show	Show *parameters*	Show the current configuration of each function.
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.*

5.4 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 learning to configure it with some reference examples.

Example 1: Show the current version

```
# status system
hardware_version = 1.0
firmware_version = beta210618
firmware_version_full = "beta210618 (Rev 4250)"
kernel_version = 4.9.152
device_model = R2011
serial_number = ""
uptime = "0 days, 01:25:16"
system_time = "Tue Apr 15 17:09:04 2021"
ram_usage = "77M Free/128M Total"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
  firmware    New firmware
   config      New configuration file
# tftpupdate firmware (space+?)
  filename    New file
# tftpupdate firmware filename R2011-firmware-sysupgrade-unknown.ruf host 192.168.100.99 //enter a new firmware name
Downloading
Download success.
Upgrading
Upgrade success.          //Update succeed
```

```
# reboot                    //Take effect after rebooting
Rebooting...
OK
```

Example 3: Set link-manager

```
# set
# set (space+?)
   cellular                  Cellular
   ddns                      DDNS
   dido                      DIDO
   email                     Email
   ethernet                  Ethernet
   event                     Event Management
   firewall                  Firewall
   gre                       GRE
   ip_passthrough            IP Passthrough
   ipsec                     IPSec
   lan                       Local Area Network
   link_manager              Link Manager
   ntp                       NTP
   openvpn                   OpenVPN
   reboot                    Automatic Reboot
   route                     Route
   serial_port               Serial
   sms                       SMS
   ssh                       SSH
   syslog                    Syslog
   system                    System
   user_management           User Management
   web_server                Web Server

# set link_manager（space+?）
   primary_link              Primary Link
   backup_link               Backup Link
   backup_mode               BackSup Mode
   revert_interval           Revert Interval
   emergency_reboot          Emergency Reboot
   link                      Link Settings
# set link_manager primary_link（space+?）
Enum    Primary Link  （wwan1/wan）
# set link_manager primary_link wwan1            //select “wwan1” as primary_link
OK                                               //setting succeed
#set link_manager link 1（space+?）
   type                            Type
   desc                            Description
```

```
    connection_type            Connection Type
    wwan                        WWAN Settings
    static_addr                  Static Address Settings
    pppoe                        PPPoE Settings
    ping                         Ping Settings
    nat_enable                   NAT Enable
    mtu                          MTU
    weight                        Weight
    upload_bandwidth             Upload Bandwidth
    download_bandwidth          Download Bandwidth
    dns1_overrided               Overrided Primary DNS
    dns2_overrided               Overrided Secondary DNS
    debug_enable                  Debug Enable
    verbose_debug_enable          Verbose Debug Enable
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan（space+?）
    auto_apn                       Automatic APN Selection
    apn                            APN
    username                       Username
    password                       Password
    dialup_number                  Dialup Number
    auth_type                      Authentication Type
    data_allowance                 Data Allowance
    billing_day                    Billing Day
# set link_manager link 1 wwan data_allowance 100              //enable cellular switch_by_data_traffic
OK                                                             //setting succeed
# set link_manager link 1 wwan billing_day 1                   //setting specifies the day of the month for billing
OK                                                            // setting succeed
…
# config save_and_apply
OK                                          // save and apply the current configuration, make your configuration effect
```

Example 4: Set Ethernet

```
# set Ethernet port_setting 2 port_assignment lan0                 //Set Table 2 (eth1) to lan0
OK
# config save_and_apply                                           //setting succeed
OK
```

Example 5: Set LAN IP address

```
# show lan all
```

```
network {
        id = 1
        interface = lan0
        ip = 192.168.0.1
        netmask = 255.255.255.0
        mtu = 1500
        dhcp {
                enable = true
                mode = server
                relay_server = ""
                pool_start = 192.168.0.2
                pool_end = 192.168.0.100
                netmask = 255.255.255.0
                device = ""
                primary_dns = ""
                secondary_dns = ""
                wins_server = ""
                lease_time = 120
                static_lease = ""
                expert_options = ""
                debug_enable = false
        }
        vlan_id = 0
}
#
# set lan（space+?）
    network             Network Settings
    multi_ip       Multiple IP Address Settings
# set lan network 1(space+?)
    interface      Interface
    ip             IP Address
    netmask        Netmask
    mtu            MTU
    dhcp           DHCP Settings
    Vlan_id         VLAN ID
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.24.24                    //set the IP address for lan
OK                                                      //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
…
# config save_and_apply
OK                                          // save and apply the current configuration, make your configuration effect
```

Example 6: CLI for setting Cellular

```
# show cellular all
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
    }
    telit_band_settings {
            gsm_band = 900_and_1800
            wcdma_band = 1900
      }
      debug_enable = true
      verbose_debug_enable = false
}
# set(space+space)
cellular        ddns            dido            email           ethernet
event           firewall        gre             ip_passthrough  ipsec
l2tp            lan             link_manager    ntp             openvpn
pptp            reboot          route           serial_port     sms
ssh             syslog          system          user_management web_server
# 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 the current configuration, make your 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
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

Abbr.	Description
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
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, 63 Yongan Road, Huangpu District,
Guangzhou, China 511350

Email: info@robustel.com

Web: www.robustel.com