robustel | Software Manual

RobustOS Pro Software Manual

robustOS Pro

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

About this Document

This document provides web interface information of the RobustOS Pro based gateway products, including gateway configuration and operation.

Related Products

EG5100, EG5101, LG5100, EG5120, EV8100

Trademarks and Permissions

Disclaimer

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	Firmware Version	Document Version	Change Description
August 5, 2022	2.0.0	1.0.0	Initial release.
May 22, 2023	2.1.0	2.1.0	Added support for RobustOS Pro V2.1.0
September 14, 2023	2.1.1 or newer version	2.1.1	Added support for EG5101, EV8100

Contents

Chapter 1 Introduction

This software manual, used for all the RobustOS Pro based gateway products, provides web interface information (configuration and operation).
Please refer to the specific chapter accordingly, as hardware configurations or interfaces may vary from product to product.

Related Product	EG5100	EG5101	LG5100	EG5120	EV8100													
SIM card Slots	2	2	2	2	2													
Ethernet ports	2	1	2	2	2													
Console ports	-	-	-	-	-													
HDMI	-	-	-	-	-													
POE-PD	*	-	*	-	-													
Wi-Fi	*	-	-	*	*													
Bluetooth	*	-	-	*	*													
GNSS	*	-	-	*	-													
DI/DO	4	-	4	4	5													
Relay Output	-	-	-	-	-													
RS232	√	√	√	√	√													
RS485	√	√	√	√	√													
RS422	-	-	-	-	-													
USB	√	√	√	√	√													
CAN	*	-	-	-	√													
Docker	√	-	√	√	√													
FXS	-	-	-	-	√													

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

About RobustOS Pro

RobustOS Pro is developed by Robustel based on Debian 11 (bullseye), a common Linux operating system with enhanced cybersecurity, advanced GUI and docker container supported. It will be more convenient for customers to develop and deploy edge computing applications by themselves according to their needs, supporting programming languages such as C, C++, Python, Java, Node.js etc., and the latest common APPs including VPNs, SMS remote control and more can be downloaded in RCMS to fully meet the needs of fragmented IoT applications.

Chapter 2 Initial Configuration

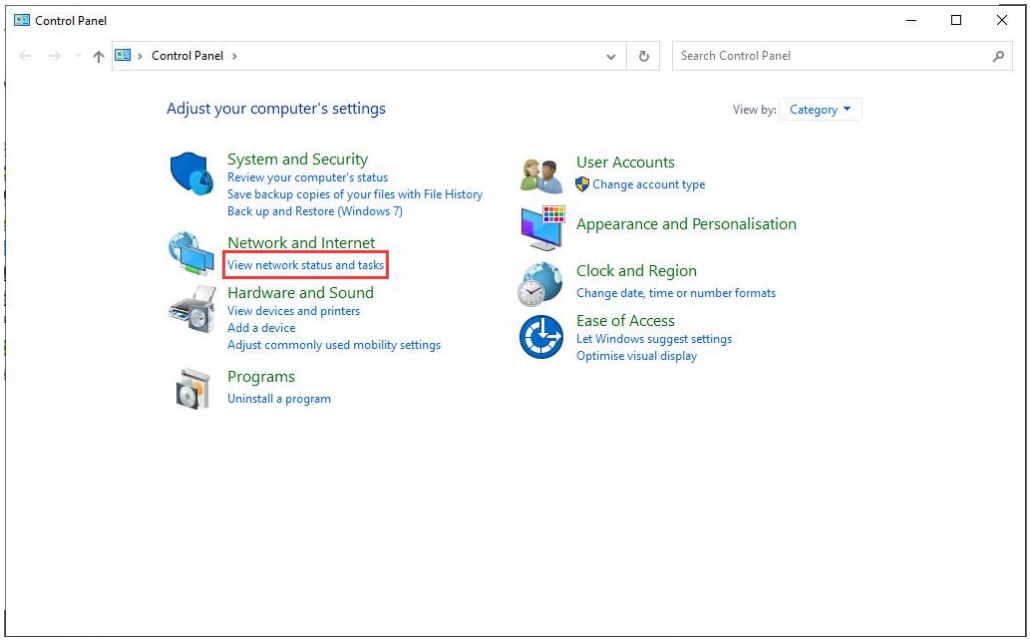
The device can be configured through your web browser that including Microsoft Edge, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows. It provides an easy and user-friendly interface for configuration. There are various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

2.1 PC Configuration

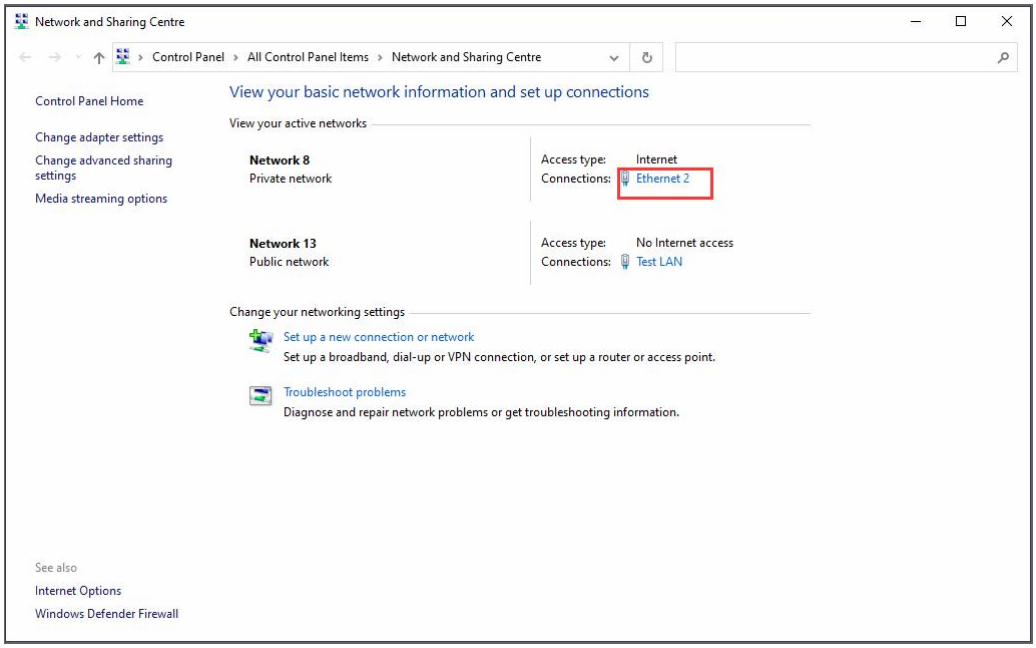
There are two ways to get an IP address for the computer. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configurate a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

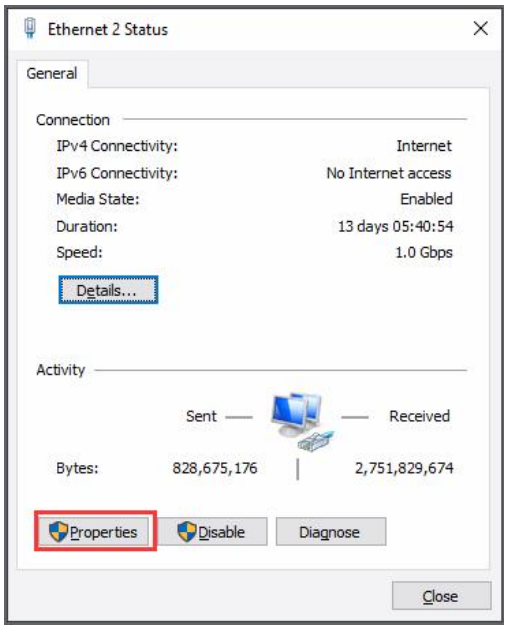
1. Right-click “**Windows LOGO**” on the taskbar, select “**Run**”, and type "**Control**" to launch the Control panel, then Click “**View network status and tasks**”.



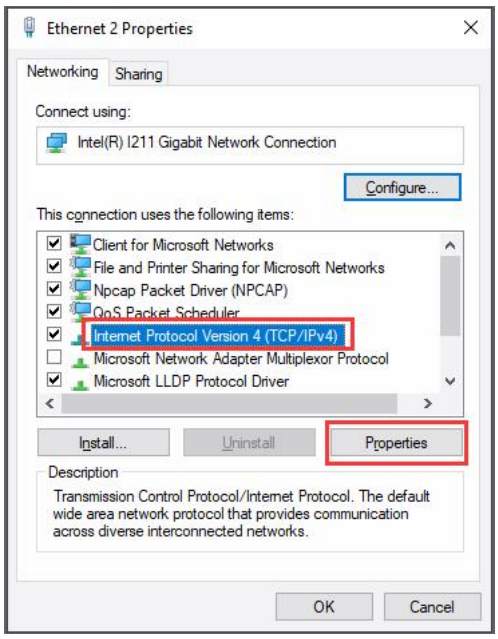
2. After entering **"**Network and Sharing Center", click "**Ethernet**" connections status.



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

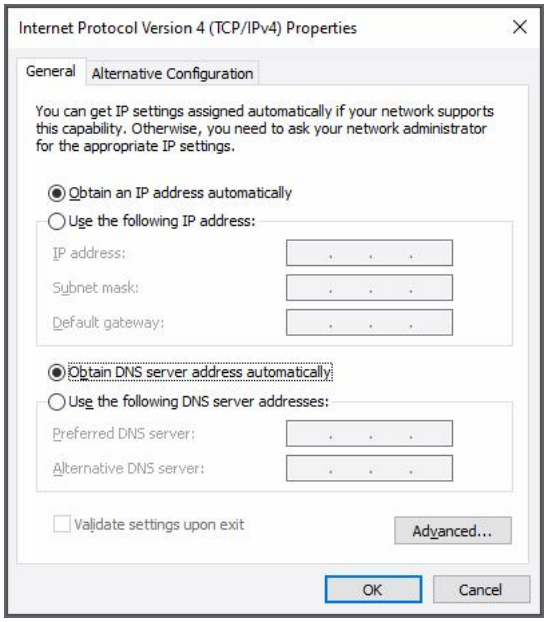


4. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

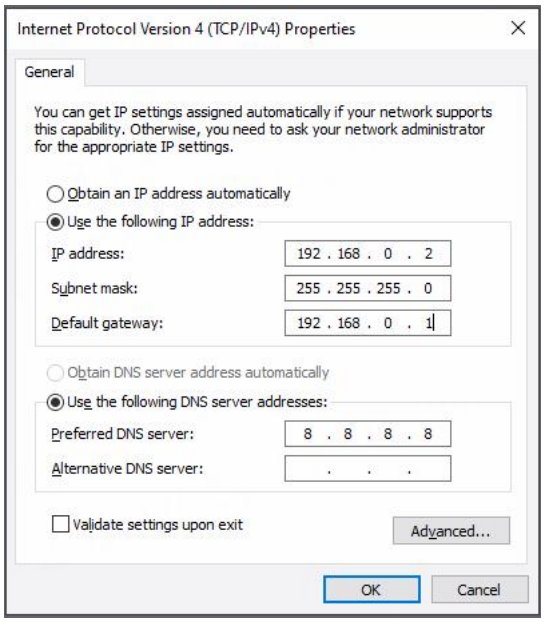


5. Two ways to configurate the IP address of the computer.

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



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



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

2.2 Factory Default Settings

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

Item	Description
Username	admin
Password	See the information from the product label
ETH0	WAN mode or 192.168.0.1/255.255.255.0, LAN mode
ETHn	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

2.3 Factory Reset

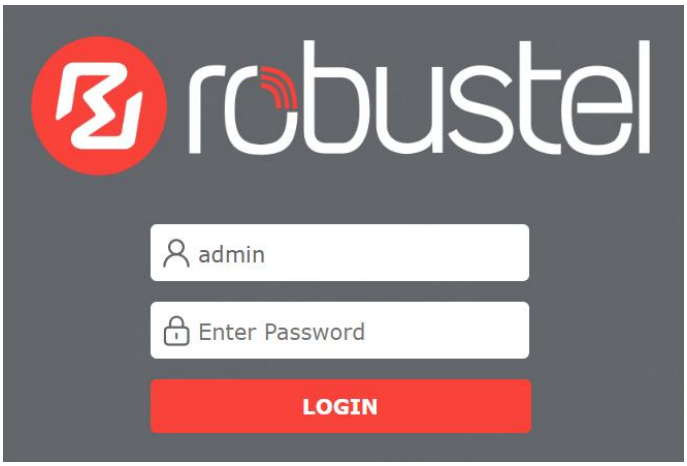
Function	Operation
Reboot	Press and hold the RST button for 2~5 seconds under the operating status.
Restore to default configuration	Press and hold the RST button for 5 ~10 seconds under the operating status. The RUN light flashes quickly, and then release the RST button, and the device will restore 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 the Device

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

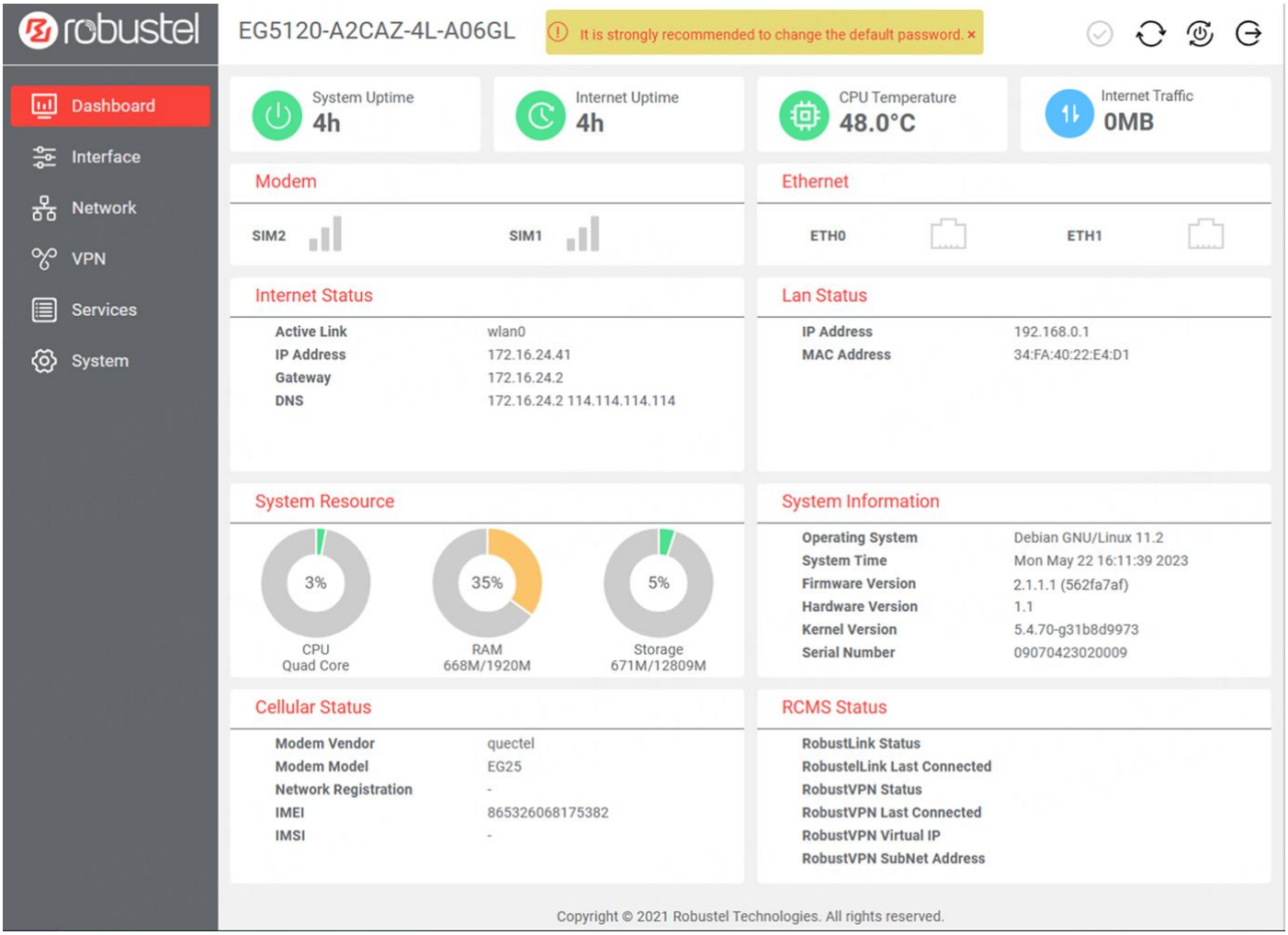
1. On your PC, open a web browser such as Microsoft Edge, Google Chrome or Firefox, etc.
2. From your web browser, type the IP address of the device into the address bar and press enter. The default IP address of the device is http://192.168.0.1/ ,though the actual address may vary.
   Note: If a SIM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

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



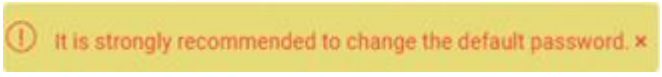
2.5 Control Panel

After logging in, the home page of the web interface is displayed, here take EG5120 for example.



From the homepage, users can find the model information and 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 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 **3.8.9 System > User Management**.

Control Panel		
Item	**Description**	**Icon**
Save & Apply	The icon is in gray by default, and will turn red if any modifications on configuration, then click to save the current configuration into device's flash and apply the modification on every configuration page, to make the	or

	modification taking effect.	
Restart	Click to restart all the RobustOS Pro operating system based applications(applications controlled by ystem are not included), then switch to the login page.	
Reboot	Click to reboot the device, then switch to the login page.	
Logout	Click to log the current user out safely. After logging out, it will switch to login page. Shut down web page directly without logout, the next one can login web on this browser without a password before timeout.	

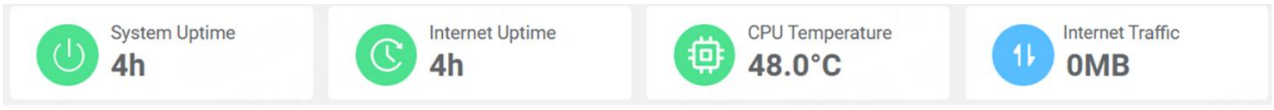
Note: The steps of how to modify configuration are as bellow:

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

Chapter 3 WebUI Descriptions

3.1 Dashboard

3.1.1 Overview



(Normal)

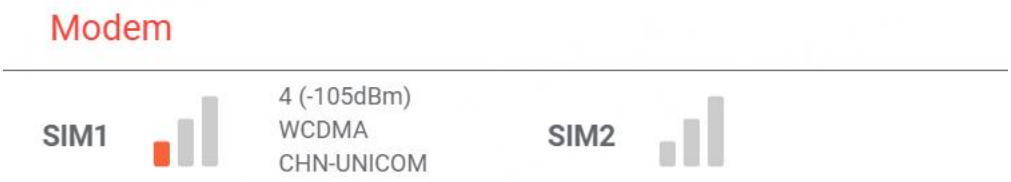
(EV8100)

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

Traffic	Show the amount of WWAN data traffic usage.
Power Source (EV8100 Only)	Show the current power source.
Battery status (EV8100 Only)	Show the current battery status.

3.1.2 Modem

This page shows the status of SIM card.



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

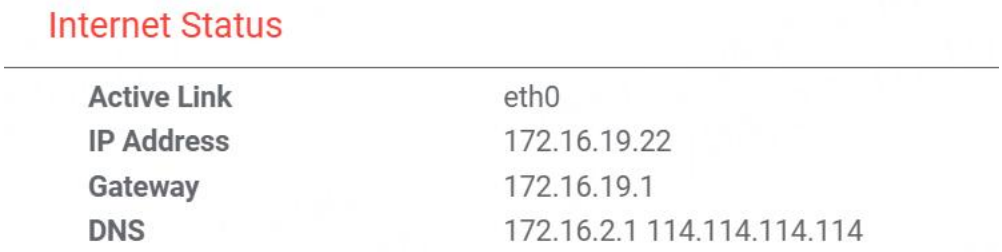
3.1.3 Ethernet

This page shows the device's Ethernet status

Icon	Description
	Port disable or link down.
	Link up.

3.1.4 Internet Status

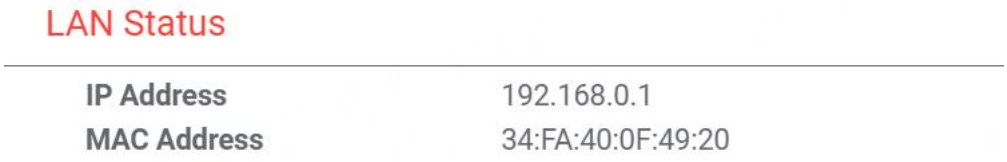
This page shows the device's Internet status information.



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

3.1.5 LAN Status

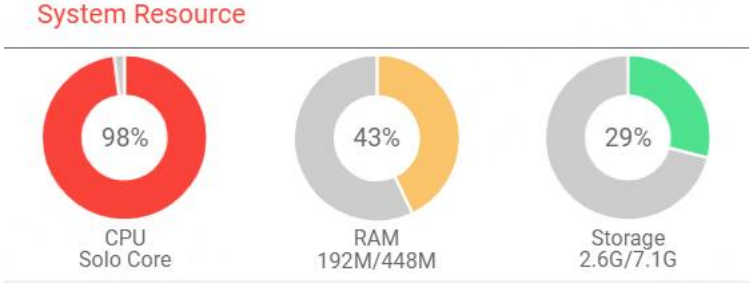
This page shows the device's LAN status



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

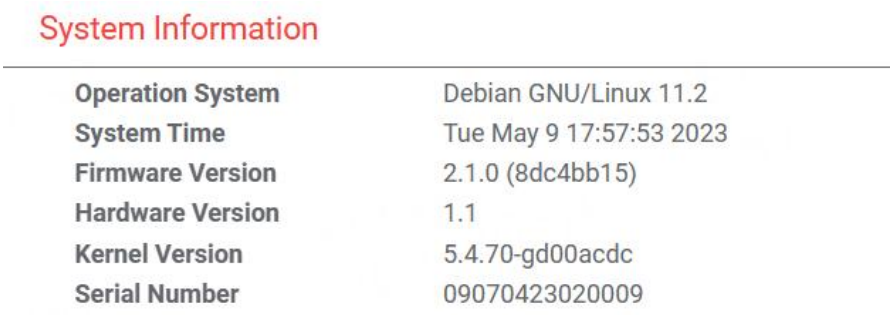
3.1.6 System Resource

This page shows the device's system resources usage information.
When the usage is more than 65%, the icon will be in Red.
When the usage is between 30% and 65%, the icon will be in Yellow.
When the usage is less than 30%， the icon will be in Green.



3.1.7 System Information

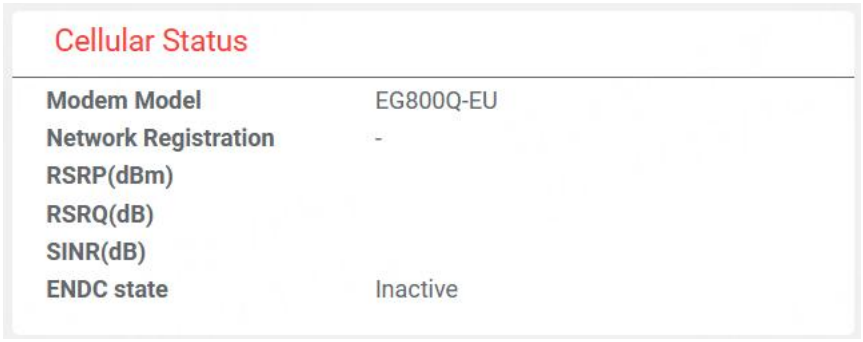
This page shows the device's system information.



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

3.1.8 Cellular Status

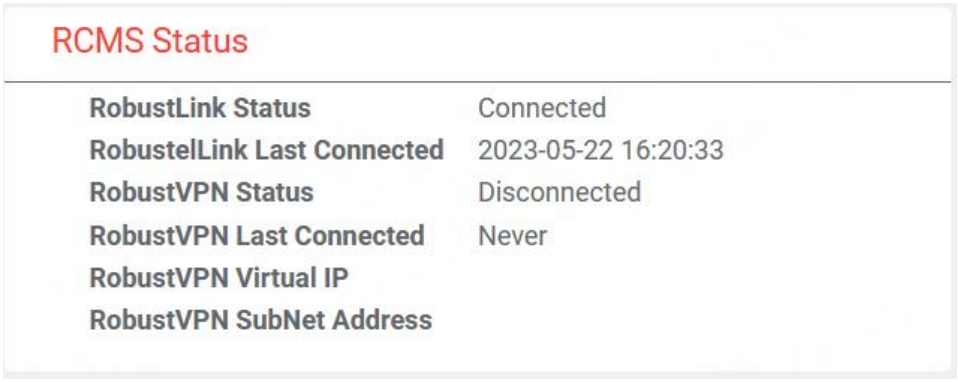
This page shows the device's cellular status.



Item	Description
Modem Vendor	Show the radio module vendor information.
Network Registration	Show the current network registration information.
RSRP(dBm)	Show the current RSRP when you register to the 4G network.
RSRQ(dB)	Show the current RSRQ when you register to the 4G network.
SINR(dB)	Show the current SINR when you register to the 4G/5G network.
ENDC state	Show the ENDC state of 5G network.

3.1.9 RCMS Status

This page shows the device's cellular status.



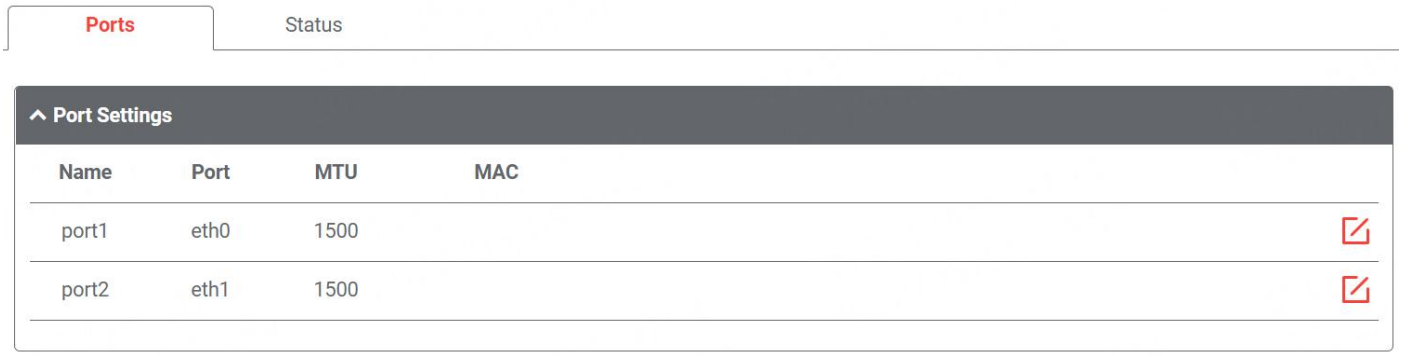
Item	Description
RobustLink Status	Show the status of RobustLink
RobustelLink Last Connected	Show the last connected times of RobustLink
RobustVPN Status	Show the status of RobustVPN
RobustVPN Last Connected	Show the last connected times of RobustVPN
RobustVPN Virtual IP	Show the virtual IP of RobustVPN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

3.2 Interface

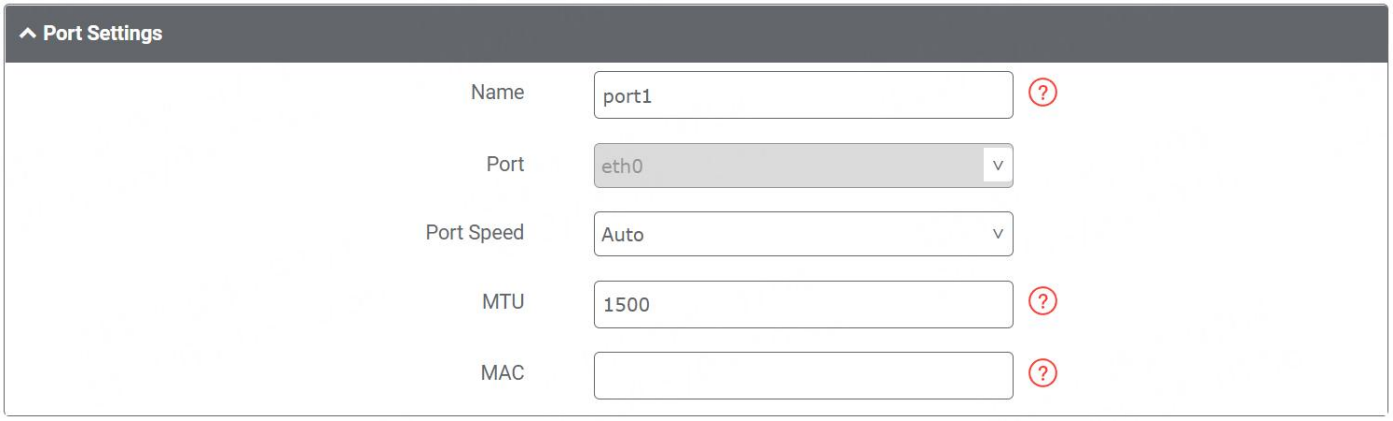
3.2.1 Ethernet

This section allows you to set the related parameters for Ethernet. There may be multiple Ethernet ports in the device. All Ethernet port in the device can be configured as either a WAN port or LAN port. The default settings of all Ethernet ports are lan0 and their default IP are 192.168.0.1/255.255.255.0. PoE could be supported in some devices.

Ports



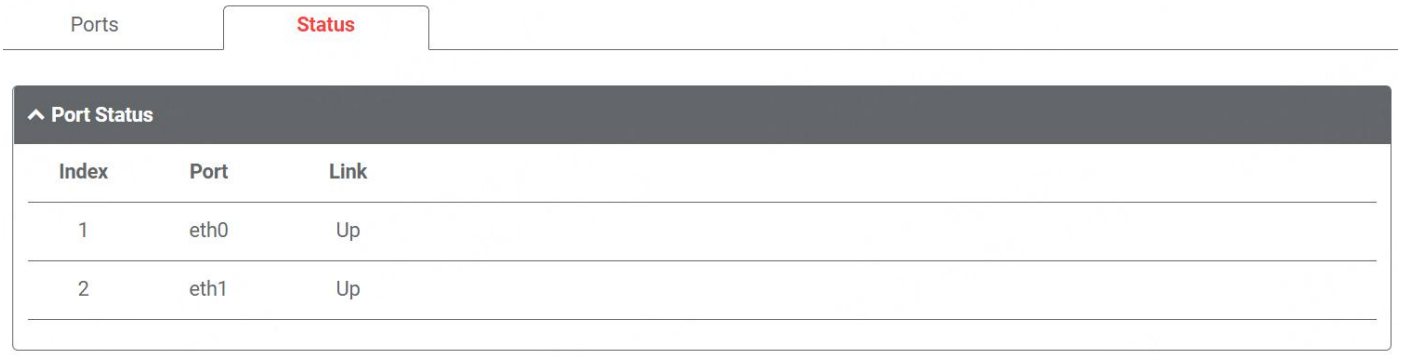
Click to configure its parameters, and modify the port assignment parameters in the pop-up window.



Item	Description	Default
Name	Name of the port.	--
Port	Show the editing port, read only.	--
Port Speed	Select from “Auto”, “10M-half”, “10M-full”,“100M-half”, “100M-full”,“1000M-half”, “1000M-full”.	Auto
MTU	Enter the value of the maximum transmission unit(MTU).	1500
MAC	Specify the MAC address of the port.	--
POE Enable (Optional)	Click the toggle button to enable or disable the POE function. When POE function enabled, it will connect the POE voltage.	ON

Status

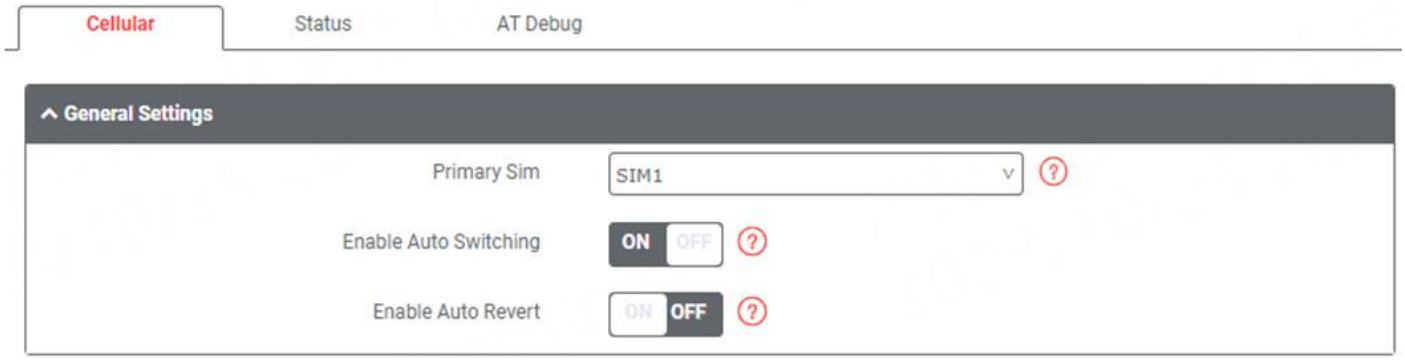
This page allows you to view the status of Ethernet port.



3.2.2 Cellular

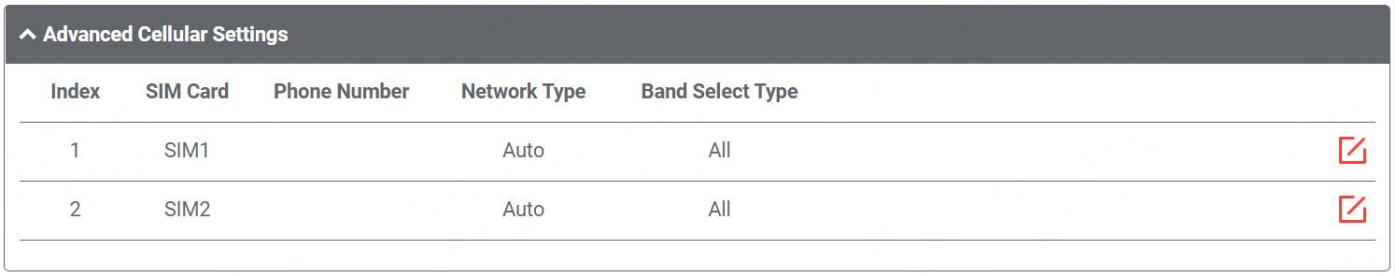
This section allows you to set the related parameters of Cellular. The device supports one cellular modem and two SIM slots, but only one SIM slot is activated at any time.

Cellular

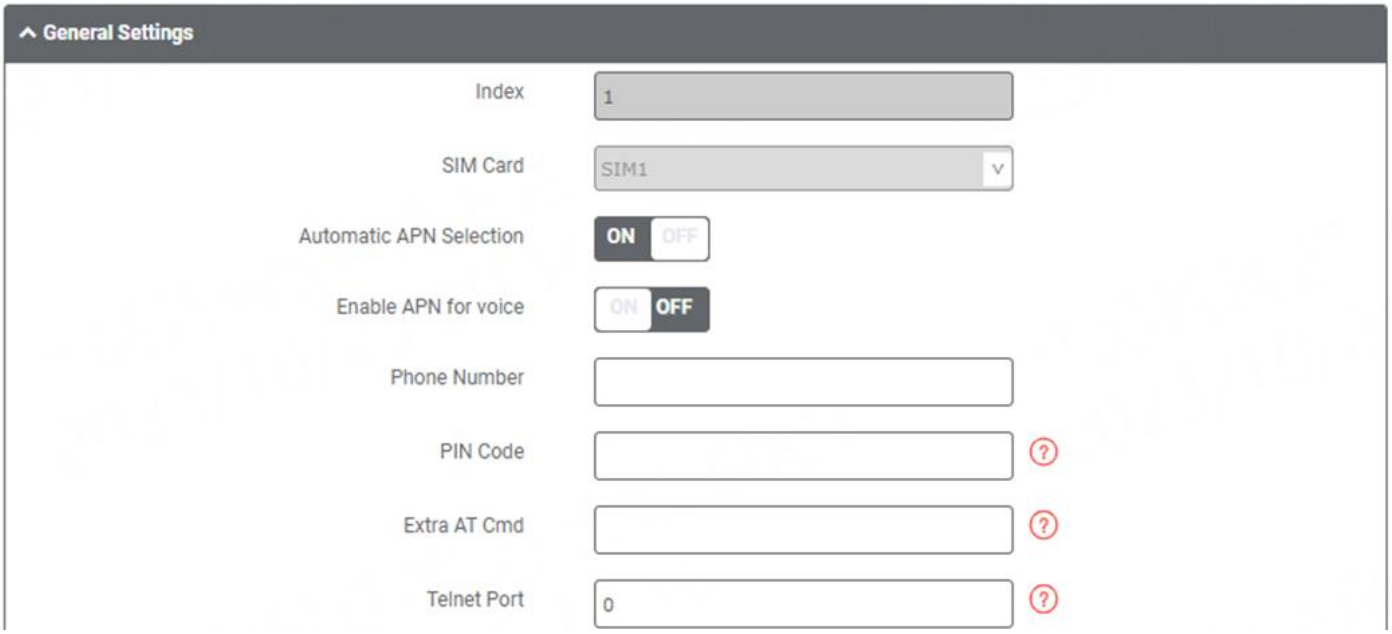


Item	Description	Default
Primary Sim	Select one Sim card as primary Sim card	SIM1
Enable Auto Switching	When auto switching is enabled, the SIM card will be automatically switched to another one when there is SIM card error or connection error or ping fails by default.	ON
Enable Auto Revert	When auto switching is enabled, the backup SIM card will be automatically switched to primary sim card when backup SIM card online time is greater than revert interval time.	OFF

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

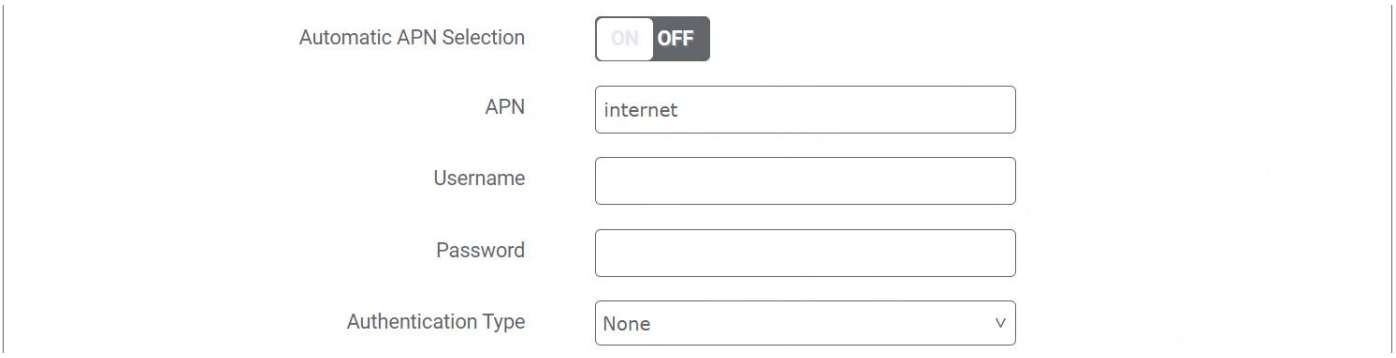


Click to configure its parameters in the pop-up window.



Item	Description	Default
Index	Indicate the ordinal of the list.	--
SIM Card	Show the currently editing SIM card.	--
Automatic APN Selection	Click the toggle button to enable/disable the "Automatic APN Selection" option. After enabling, the device will recognize the access point name automatically. Alternatively, users can disable this option and manually add the access point name.	ON
Enable APN for voice	Click the toggle button to enable/disable the option. (Only EV8100 support)	OFF
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet. 0 means not supported.	0
MTU	1280 - 1500	1500
Traffic Statistics	Click the toggle button to enable/disable the option.	ON
Billing Day	This option specifies the day of month for billing, the data traffic statistics will be recalculated from this day.	1
Enable IPv6	Click the toggle button to enable/disable the option.	OFF

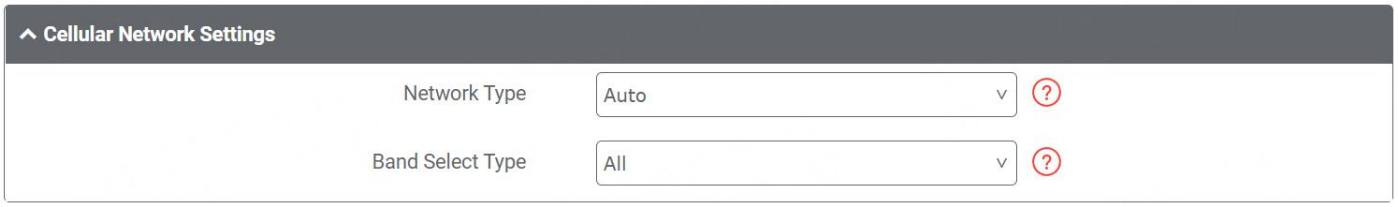
When the Automatic APN Selection is off, users can specify their own APN setting.



Item	Description	Default
Automatic APN Selection	Click the toggle button to enable/disable this option. Enable for AutoAPN feature.	OFF
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null

Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Authentication Type	Select the authentication type. Select from “None”, “CHAP”, “PAP”. • None: None. • CHAP: Challenge-Handshake Authentication Protocol. • PAP: Password Authentication Protocol.	None

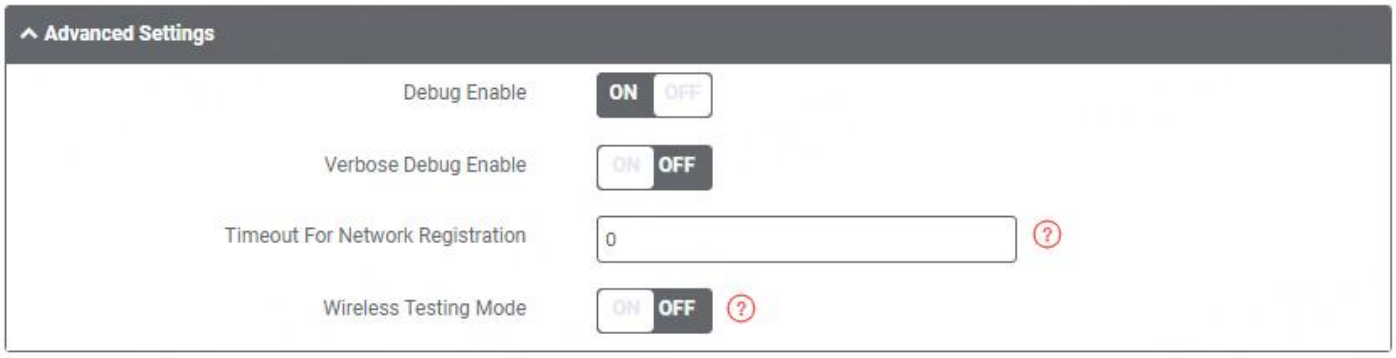
When the APN for voice is on, users can configure their own voice APN in need.



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

Note: EG5120 does not support this feature.

Item	Description	Default
Network Type	Select the cellular network type, which is the network access order. Select from “Auto”, “2G Only”, “3G Only”, “4G Only”, “5G Only”. • Auto: Connect to the best signal network automatically • 2G Only: Only the 2G network is connected • 3G Only: Only the 3G network is connected • 4G Only: Only the 4G network is connected • 5G Only: Only the 5G network is connected *Note:* 1) *There may be some different optional network types due to the different cellular module.*	Auto
Band Select Type	Select from “All” or “Specify”. You may choose certain bands if choosing “Specify”. *Note:* *There may be some differences in Band Setting due to the different cellular module.*	All

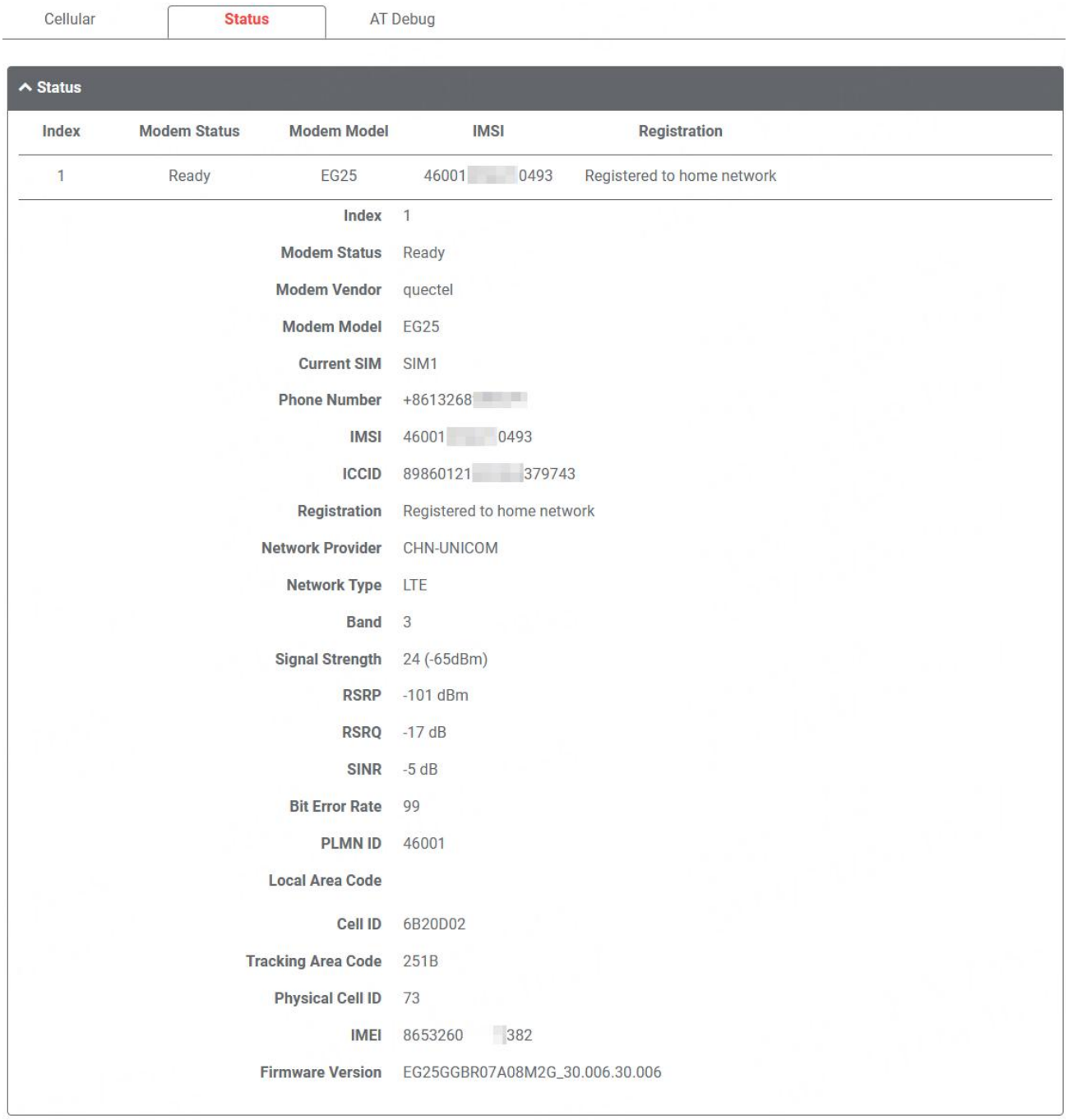


Item	Description	Default
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF
Timeout For Network Registration	The timeout required for the module to register to the network. Unit: seconds. 0 means the default setting is used.	0
Wireless Testing Mode	Can only be turned on during laboratory testing when connected to wireless tester! Must be turned off when connected to real network!	OFF

Status

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

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

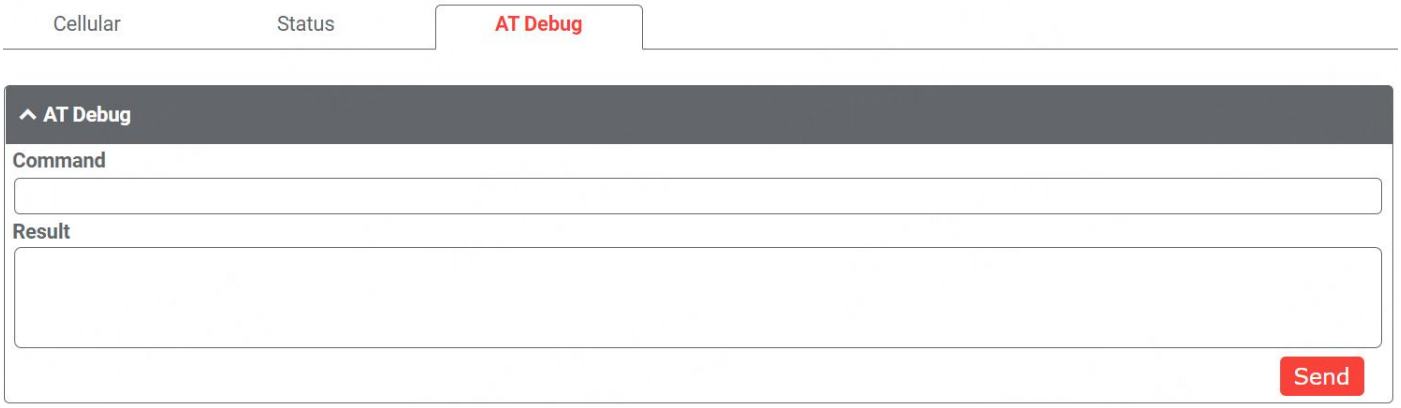


Item	Description
Index	Indicate the ordinal of the list.
Modem Status	Show the status of the radio module.
Modem Vendor	Show the vendor of the radio module.
Modem Model	Show the model of the radio module.
Current SIM	Show the SIM card that your router is using.
Phone Number	Show the phone number of the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

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

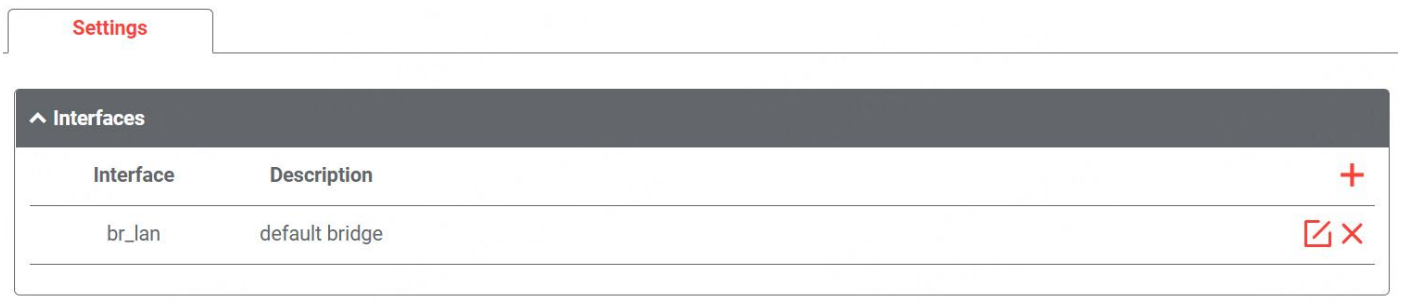
AT Debug

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



3.2.3 Bridge

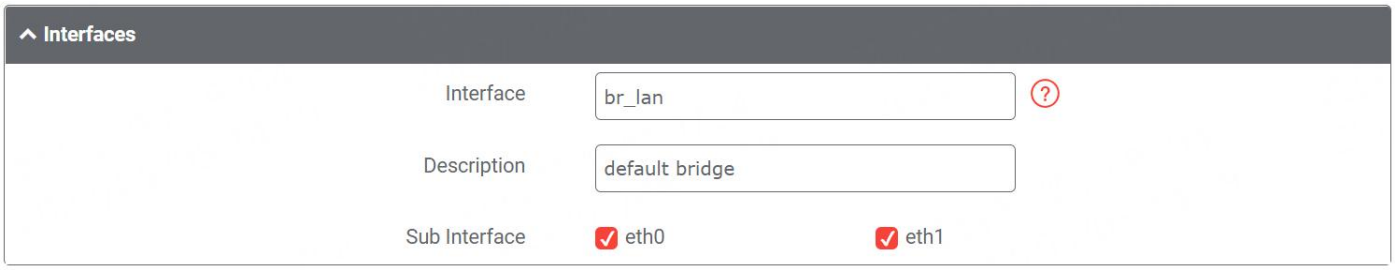
Bridge is used to create a single network consisting of multiple devices. The default bridge(br_lan) interface is always available.



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

Click ✕ to delete the Bridge.

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



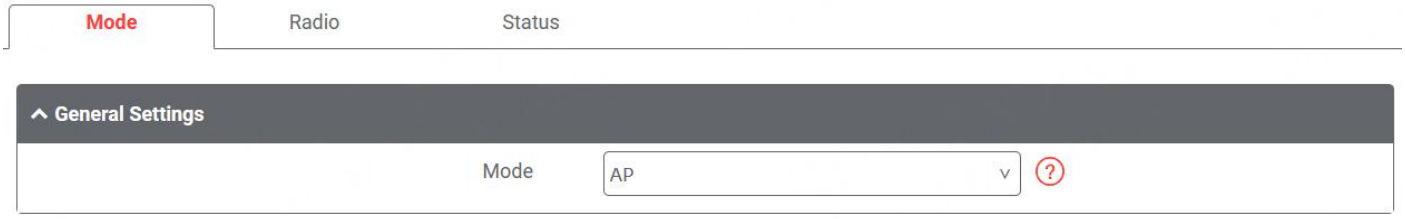
Note: You should uncheck the eth0 of sub interface when set eth0 as WAN.

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

3.2.4 Wi-Fi

This section allows you to configure the parameters of Wi-Fi AP mode. Router supports Wi-Fi AP or Client modes.

Mode



Item	Description
Mode	Select the device's wireless mode, "AP" or "Client". **AP:** Devices act as the center of the network and they provide wireless connectivity to other devices. **Client:** Client devices act as clients and they connect to an already existing Wi-Fi network rather than creating their own network. **Note:** The change of this option would cause wan link to restore default configuration. You need to restart the whole device for changes to take effect.

Radio

Radio Settings

Wi-Fi can work on either 2.4 GHz or 5 GHz, but cannot support both concurrently.

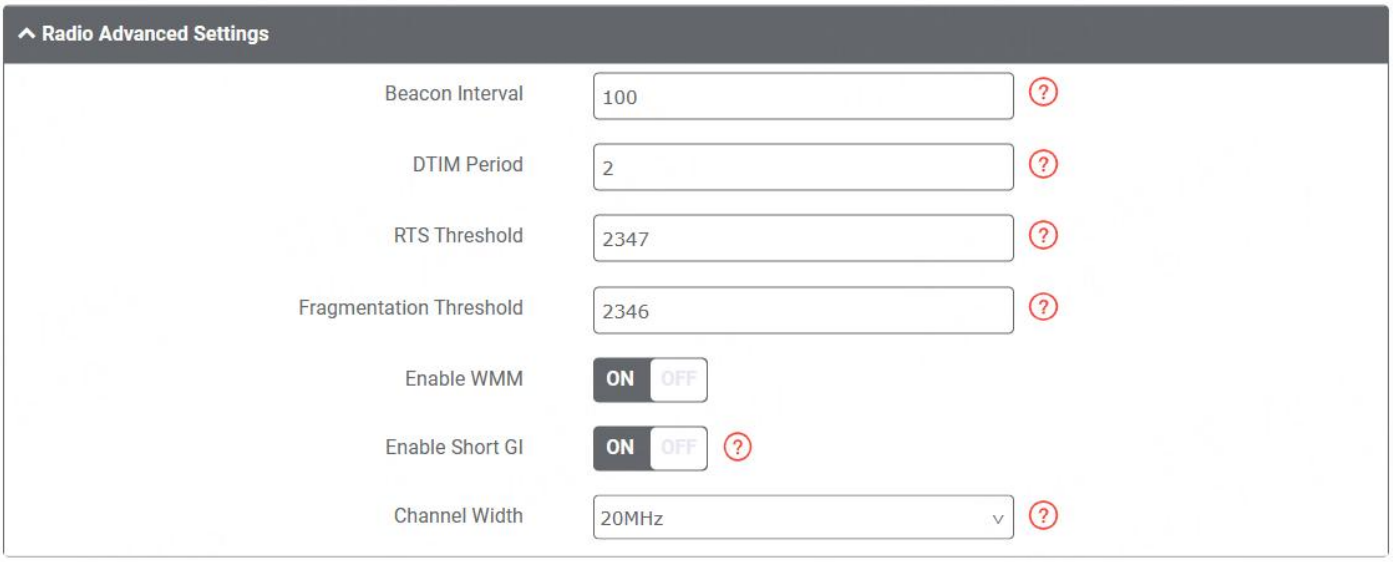
2.4 GHz： 11bgn Mixed & 11b Only & 11g Only & 11n Only

5 GHz： 11an & 11a/an/ac

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”, “11n Only”, “11an” or “11a/ac/an”. • 11bgn Mixed: Mix IEEE 802.11b/g/n three agreements, for backward compatibility. • 11b only: IEEE 802.11b. • 11g only: IEEE 802.11g. • 11n only: IEEE 802.11n. • 11a/an/ac: IEEE 802.11a/an/ac. • 11an: IEEE 802.11an only.	11bgn Mixed
Channel	Select the frequency channel, including “Auto”, “1”, “2”..... “13”, or “36”, “40”, “44”, “48”, “149”, “153”, “157”, “161”, “165”. • Auto: Router will scan all frequency channels until the best one is found. • Others: Router will be fixed to work with this 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.	Auto

Item	Description	Default
	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.	

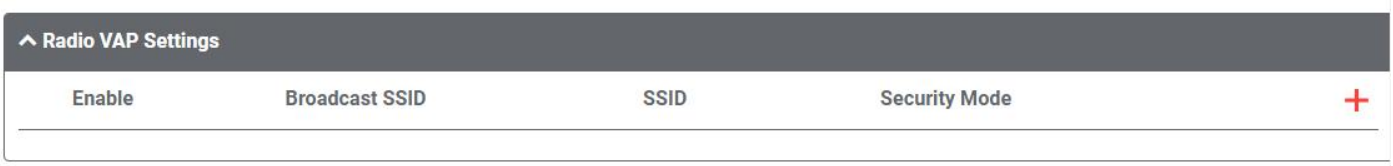
Radio Advanced Settings



Item	Description	Default
Beacon Interval	Set the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.	100
DTIM Period	Set the delivery traffic indication message period and the router AP will multicast the data according to this period.	2
RTS Threshold	Set the “request to send” threshold. When the threshold set as 2347, the router AP will not send detection signal before sending data. And when the threshold set as 0, the router AP will send detection signal before sending data.	2347
Fragmentation Threshold	Set the fragmentation threshold of a Wi-Fi AP. It is recommended that you use the default value 2346.	2346
Enable WMM	Click the toggle button to enable/disable the Wi-Fi MultiMedia 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

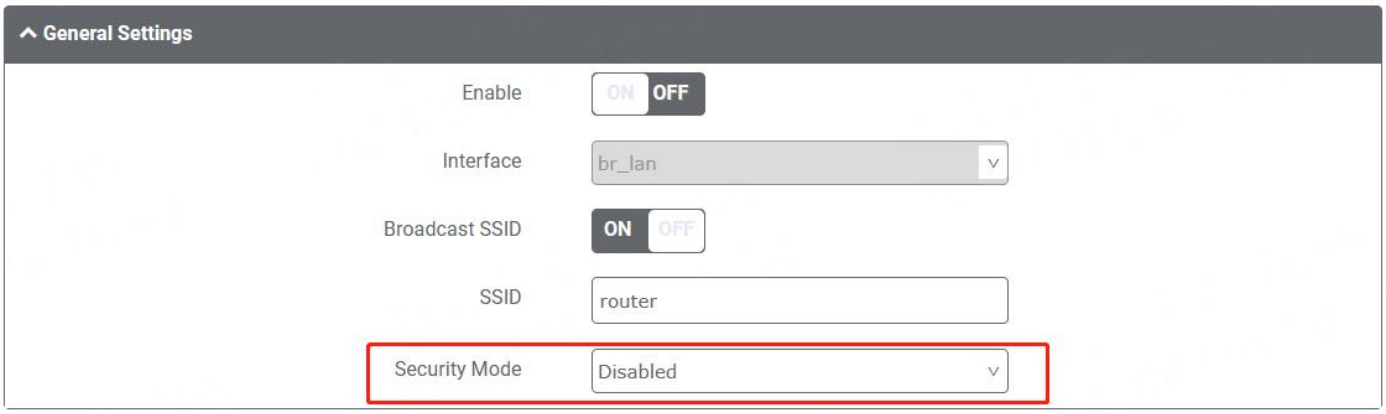
Item	Description	Default
Channel Width (available on 11bgn Mixed/11b/11g/11n/ 11ac)	Select from “20MHz” or “40MHz”. **Note**: 40 MHz channel width provides higher available data rate, twice as many as 20 MHz channel width.	Auto

Radio VAP Settings

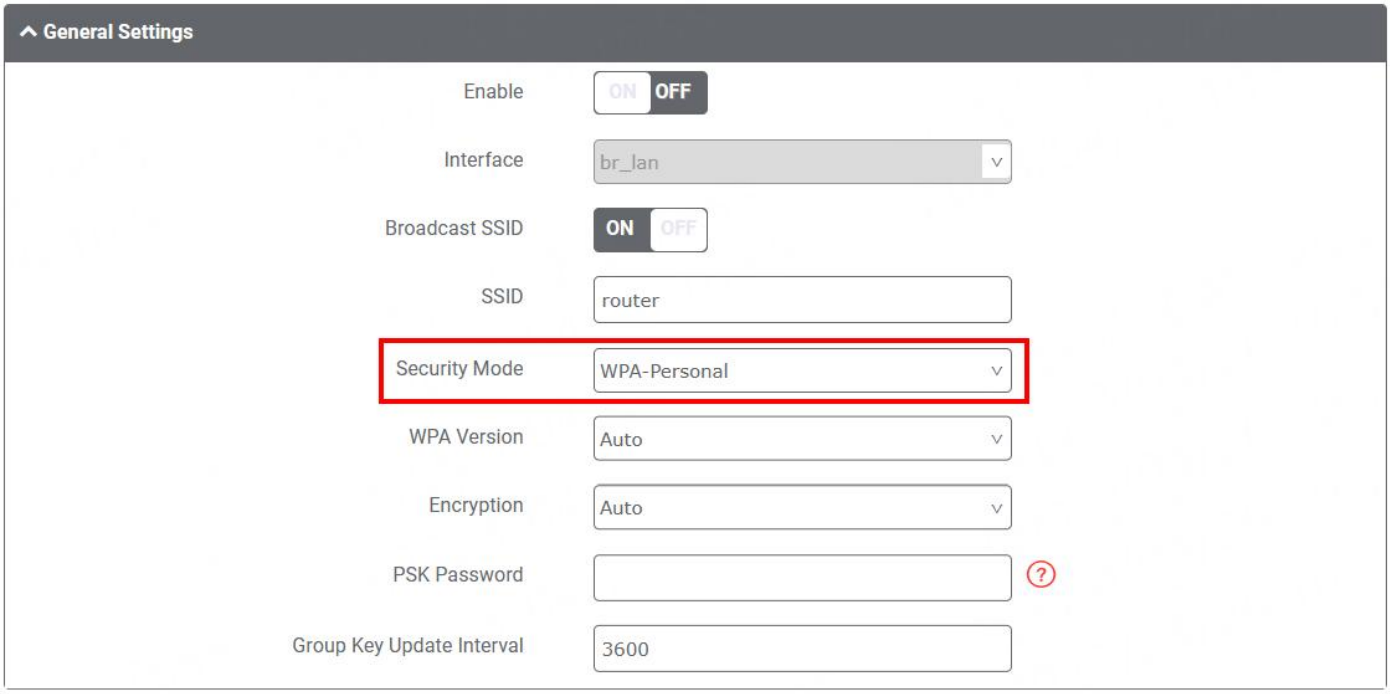


Click + to add an access point. The maximum count is **2.**

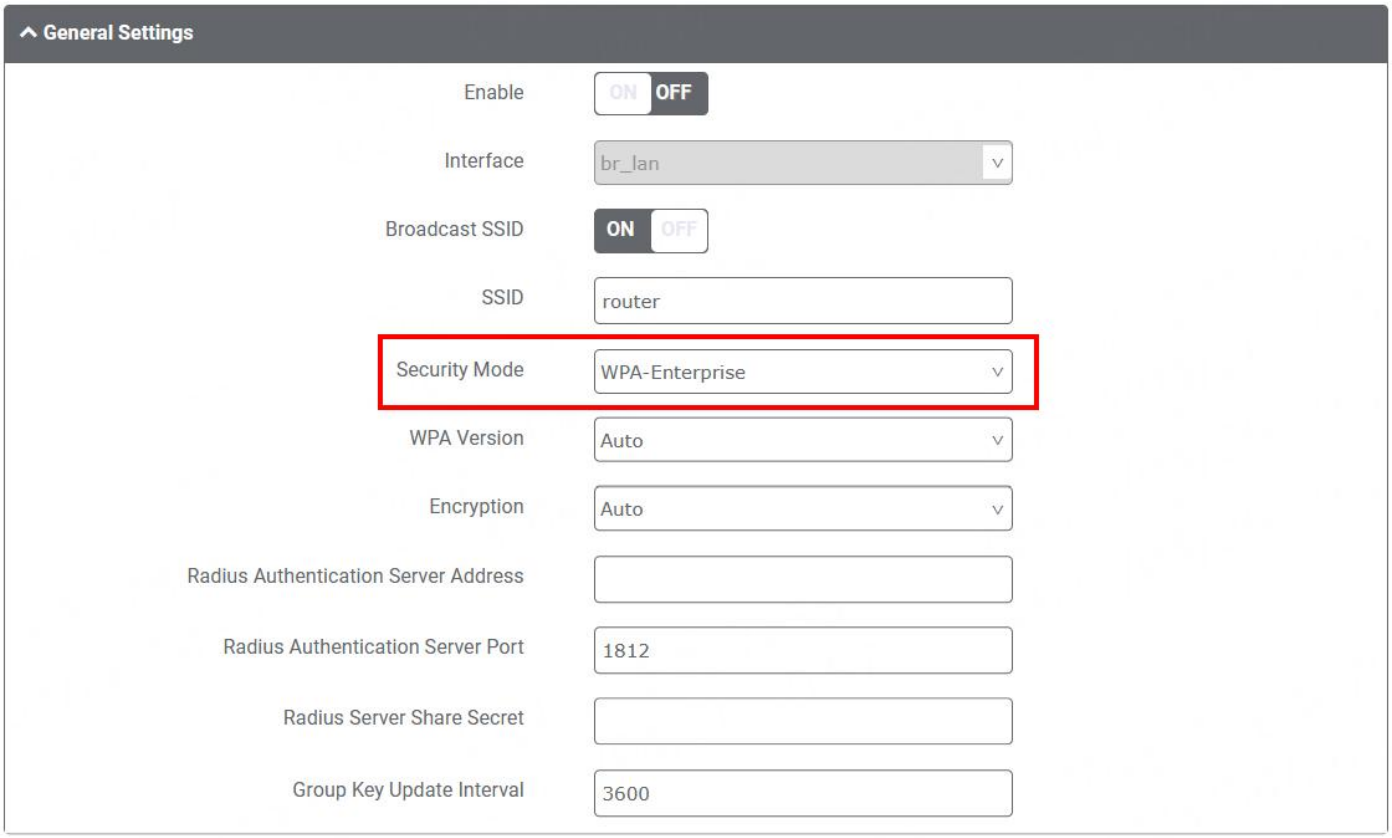
Click to configure an access point, the security mode is set as “Disabled”.



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

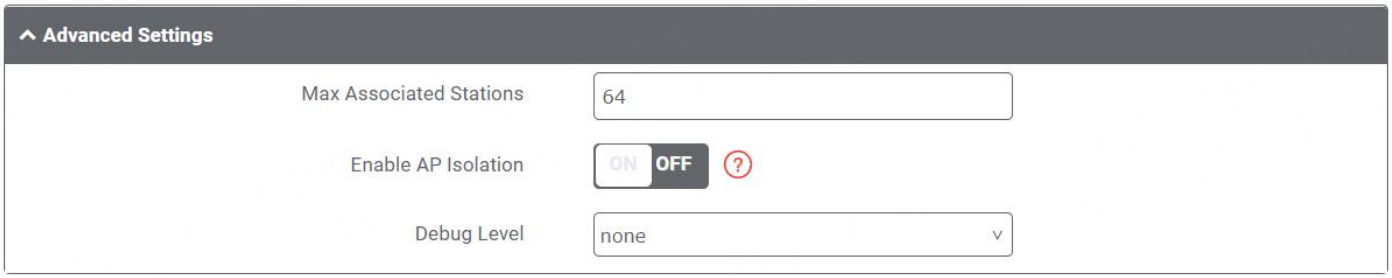

General Settings
Enable
ON
OFF
Interface
br_lan
Broadcast SSID
ON
OFF
SSID
router
Security Mode
WPA-Personal
WPA Version
Auto
Encryption
Auto
PSK Password
Group Key Update Interval
3600

The window is displayed as below when setting “WPA-Enterprise” as the security mode.



Item	Description	Default
Name	Enter the name of the Wi-Fi access point.	--
Enable	Click the toggle button to enable/disable the Wi-Fi access point option.	ON
Interface	Select one interface.	br_lan
SSID	Enter the 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.	--
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 router AP, you need to manually enter the SSID of router AP at Wi-Fi client side.	ON
Security Mode	Select from “Disabled”, “WPA-Personal”, “WPA-Enterprise”. • Disabled: User can access the Wi-Fi without password **Note**: It is strongly recommended for security purposes that you do not choose this kind of mode. • WPA-Personal: Wi-Fi Protected Access only provides one password used for Identity Authentication • WPA-Enterprise: Provides an authentication interface for EAP which can be authenticated via Radius Authentication	Disabled

Item	Description	Default
	Server or other Extended Authentication	
WPA Version	Select from “Auto”, “WPA” or “WPA2”. • Auto: Router will choose automatically the most suitable WPA version • WPA2 is a stronger security feature than WPA	Auto
Encryption	Select from “Auto” or “AES”. • Auto: Router will choose automatically the most suitable encryption • 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	Auto
PSK Password	Enter the Pre share key password. When router works as AP mode, enter Master key to generate keys for encryption. A PSK Password is used as a basis for encryption methods (or cipher types) in a WLAN connection. The PSK Password should be complicated and as long as possible. For security reasons, this PSK Password should only be disclosed to users who need it, and it should be changed regularly. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the interval of group key update.	3600
Radius Authentication Server Address@WPA-Enterprise	Enter the address of radius authentication server.	Null
Radius Authentication Server Port@WPA-Enterprise	Enter the port of radius authentication server.	1812
Radius Server Share Secret@WPA-Enterprise	Enter the shared secret of radius authentication server.	Null



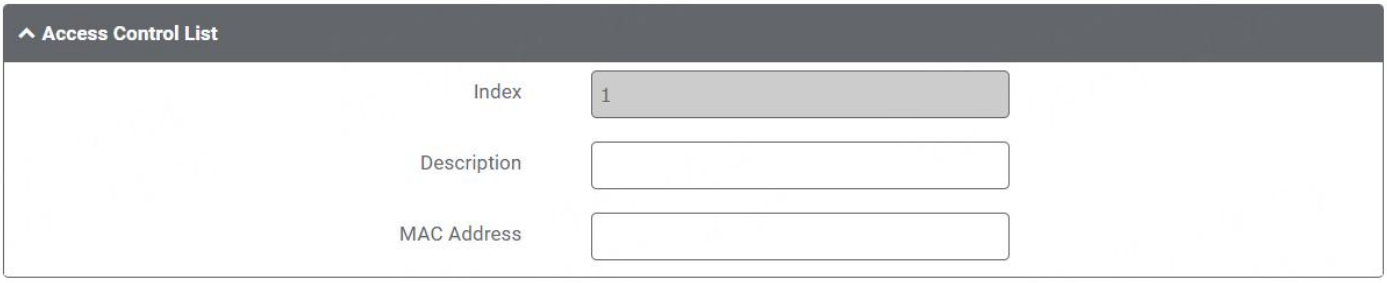
Item	Description	Default
Max Associated Stations	Set the max number of clients allowed to access the router’s AP.	64
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the router will isolate all connected wireless devices.	OFF
Debug Level	Select from “verbose”, “debug”, “info”, “notice”, “warning” or “none”.	none

Radio ACL Settings

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**: Router can only allow or deny devices which are included in “Access Control List” at one time.	Accept

Radio Access Control List

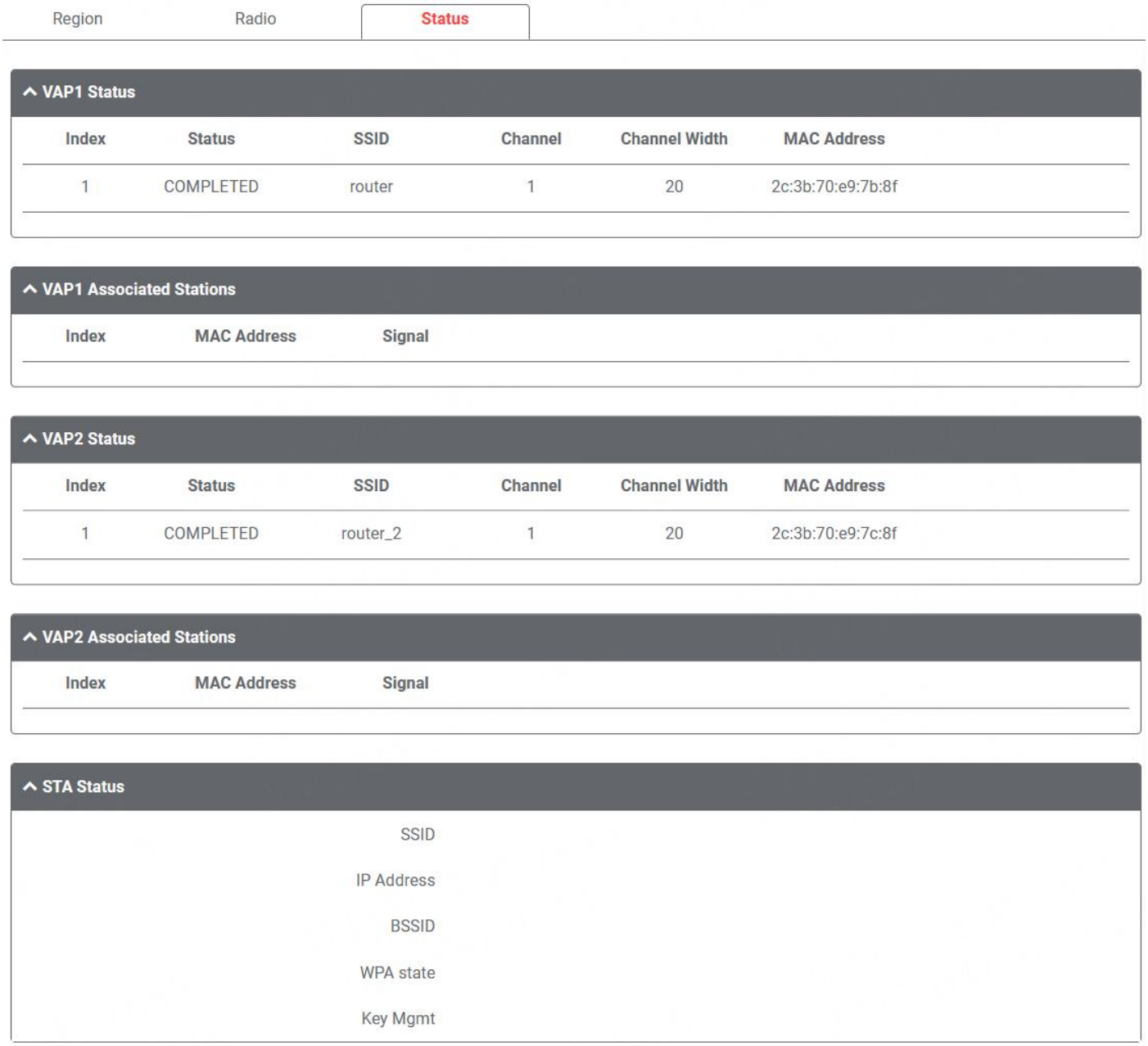
Click + to add an access control point. The maximum count is **64.**



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this access control list.	Null
MAC Address	MAC address of WiFi device	Null

Status

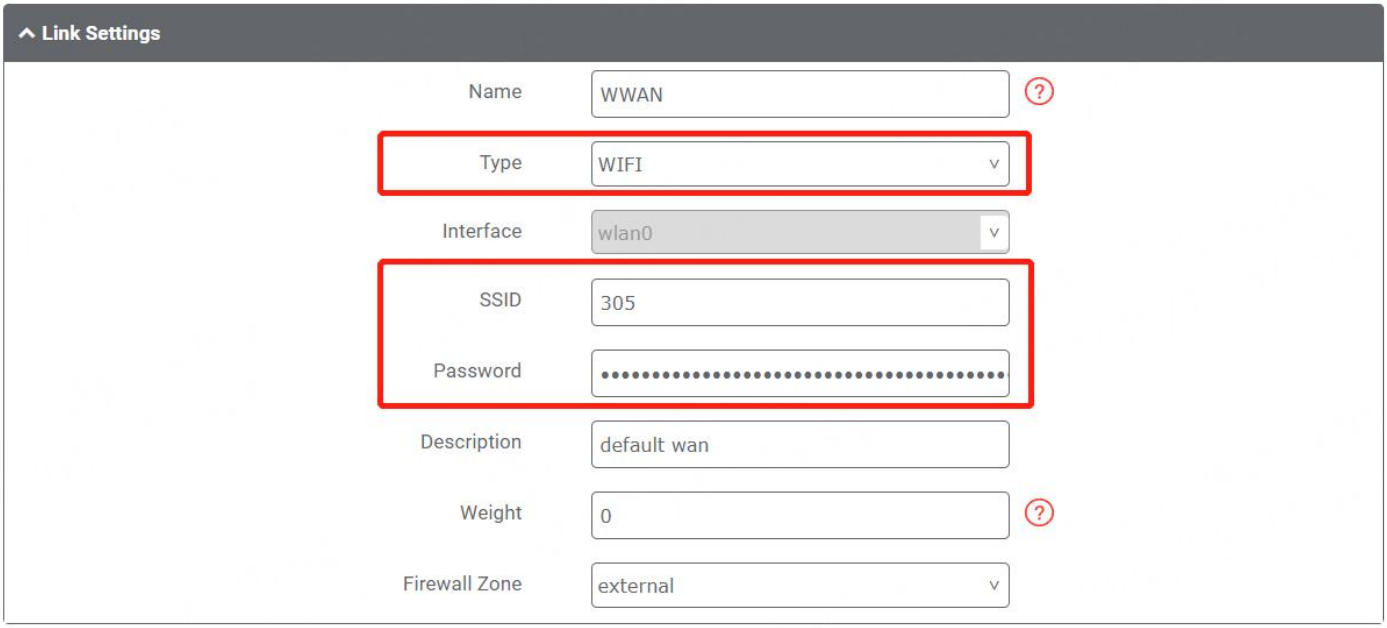
This section allows you to view the status of AP.



Wi-Fi Client

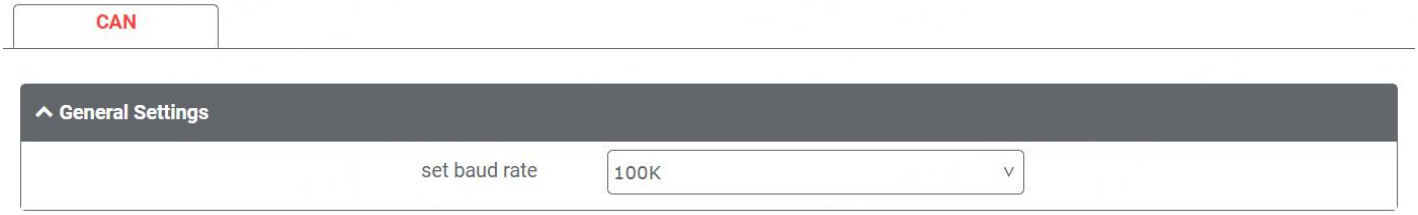
Note: User can configure the device as Wi-Fi client by following steps.
Before setting Wi-Fi Client, you need to switch the Wi-Fi mode to Client first.

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



3.2.5 CAN

This section allows you to configure the parameters of CAN.



Item	Description	Default
set baud rate	Select from “100K”, “250K”,“500K” or “1000K”.	100K

3.2.6 USB

This section allows you to configure the USB parameters. The router's USB interface can be used to upgrade firmware and upgrade configuration.

Item	Description	Default
Enable USB	Click the toggle button to enable/disable the USB option.	ON

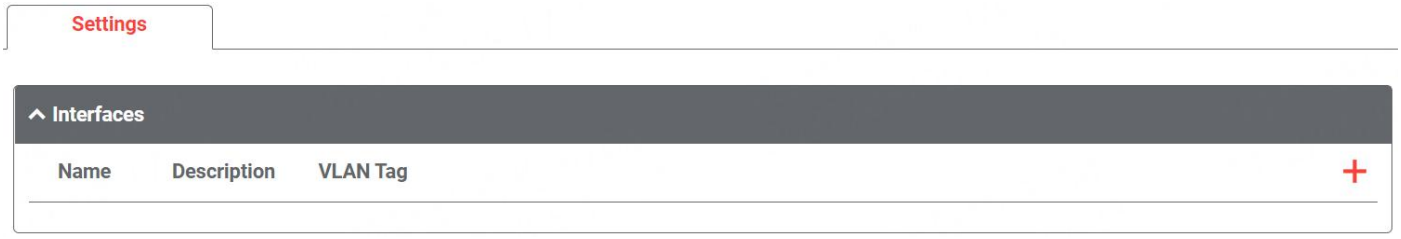
Enable Automatic Upgrade	Click the toggle button to enable/disable this option. Enable to automatically update the firmware of the router when inserting a USB storage device with a router firmware.	OFF

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

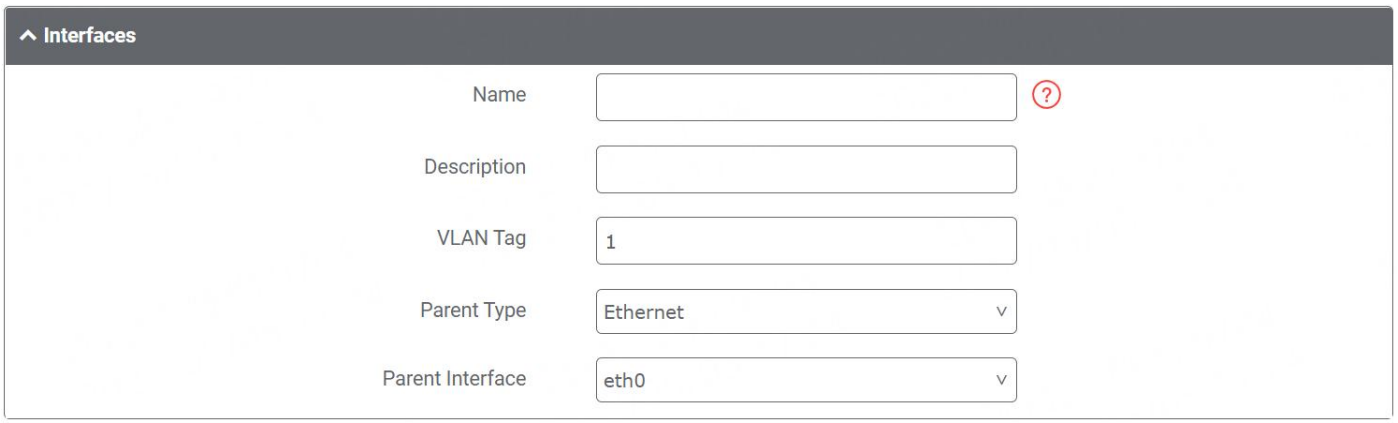
Note: when using the USB automatic upgrade function, the LEDs start blinking one by one, it means that the upgrade is in progress. When LEDs stop blinking one by one, and the USR Indicators is on, it means that the upgrade is completed. After upgrading, the device will not restart automatically. If there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

3.2.7 VLAN

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



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

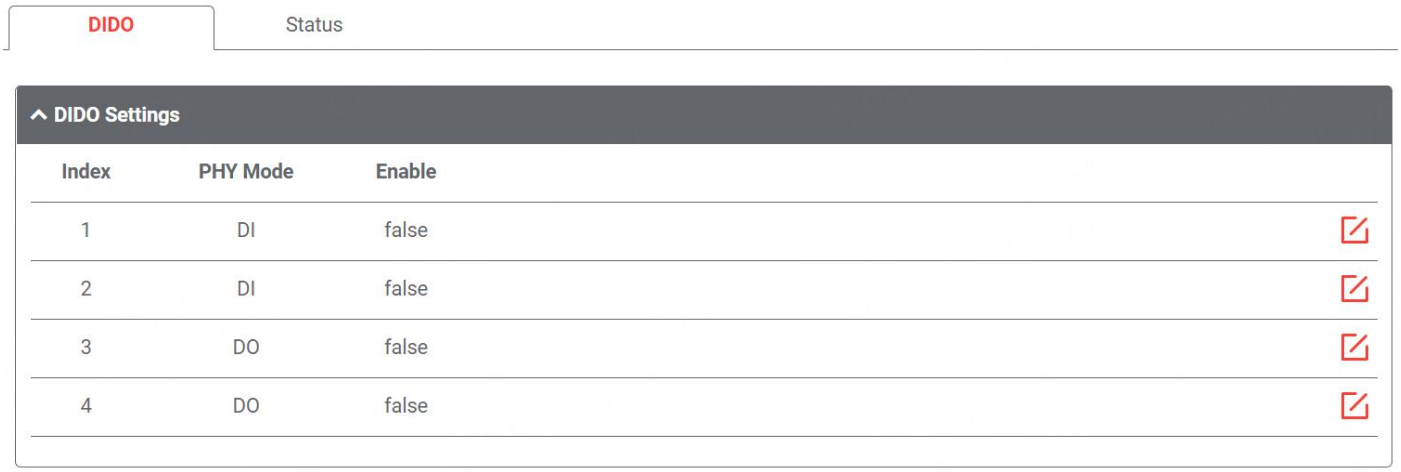


Item	Description	Default
Name	The name of VLAN.	Null
Description	Enter a description for this VLAN.	Null
VLAN Tag	Enter a tag for this VLAN.	1
Parent Type	Select from “Ethernet” or “Bridge”.	Ethernet
Parent Interface	Select the related parent interface.	eth0

3.2.8 DI/DO

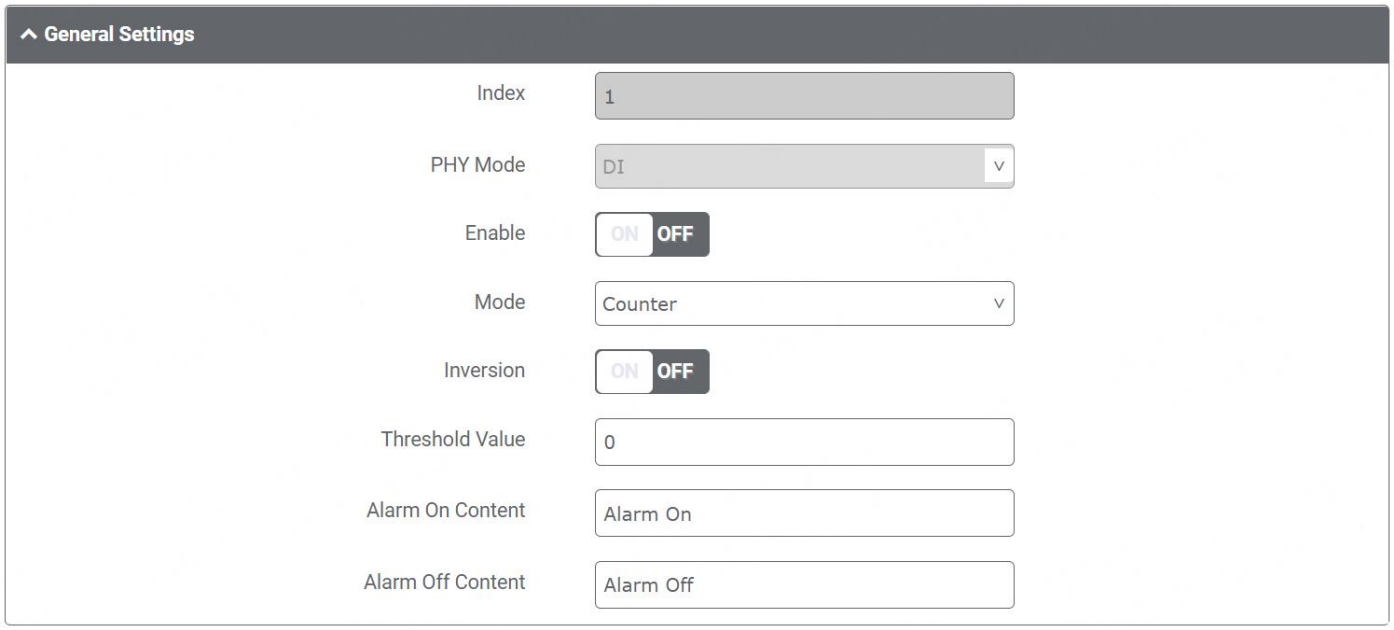
This section allows you to set the DI/DO parameters. The DI interface can be used for triggering alarm, while the DO can be used for controlling the slave device so as to do real-time monitoring. In some devices, users can configure the IO as DI or DO.

DIDO



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

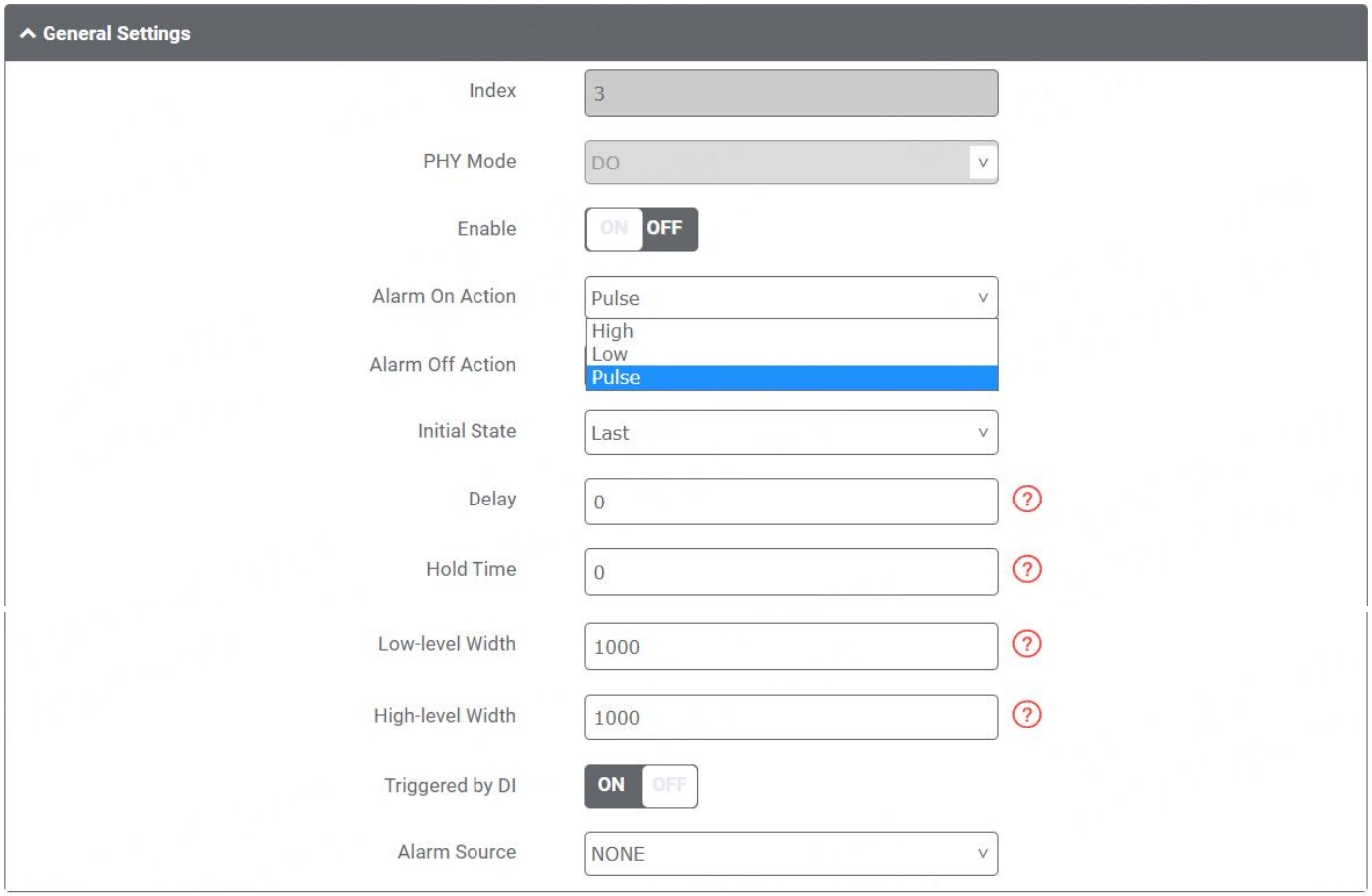
DI


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

Item	Description	Default
Index	Indicate the ordinal of the list.	--
PHY Mode	DI, fixed, read only.	--
Enable	Click the toggle button to enable/disable the digital input function.	OFF
Mode	Select from “ON-OFF” or “Counter”. • ON-OFF: Alarm mode can be triggered at the DI access ON-OFF. • Counter: Event counter mode	Counter EV8100: 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 **Count**. Set the threshold value to trigger the DI alarm when the count value reaches the threshold value.	0
Alarm On Content	Show the content when alarm on.	Alarm On
Alarm Off Content	Show the content when alarm off.	Alarm Off

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

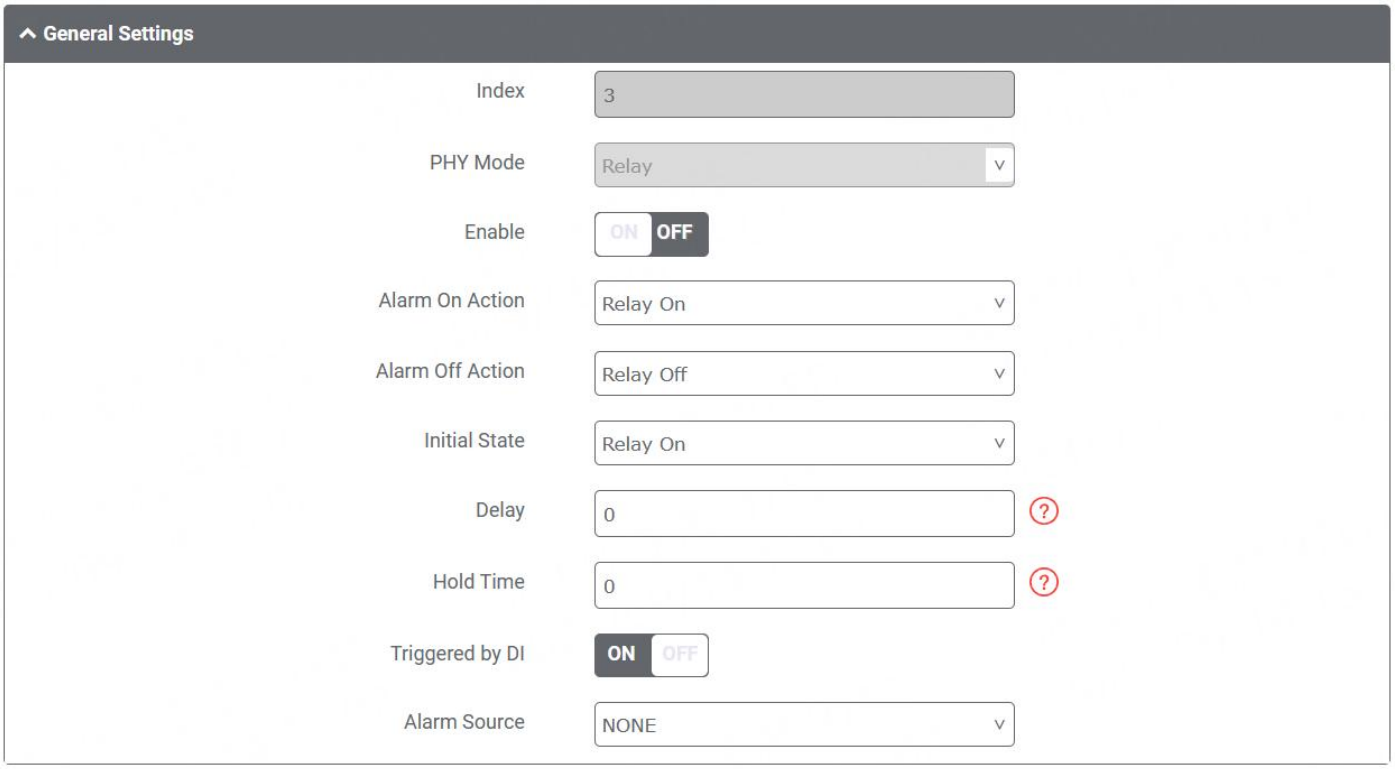
DO



Item	Description	Default
Index	Indicate the ordinal of the list.	--
PHY Mode	DO, fixed, read only.	--

Item	Description	Default
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 alarm 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 with the status of last power off • High: DO interface is in high electrical level • Low: DO interface is in low electrical level	Last
Delay (unit: 100ms)	Set the delay time for DO alarm start-up. The first pulse will be generated after a “Delay”. Enter from 0 to 3000 (0=generate pulse without delay).	0
Hold Time (unit: s)	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reach this specified time, DO will stop the action. Enter from 0 to 3000 seconds. (0=keep on until the next action)	0
Low-level Width (unit: ms)	Set the 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 the 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

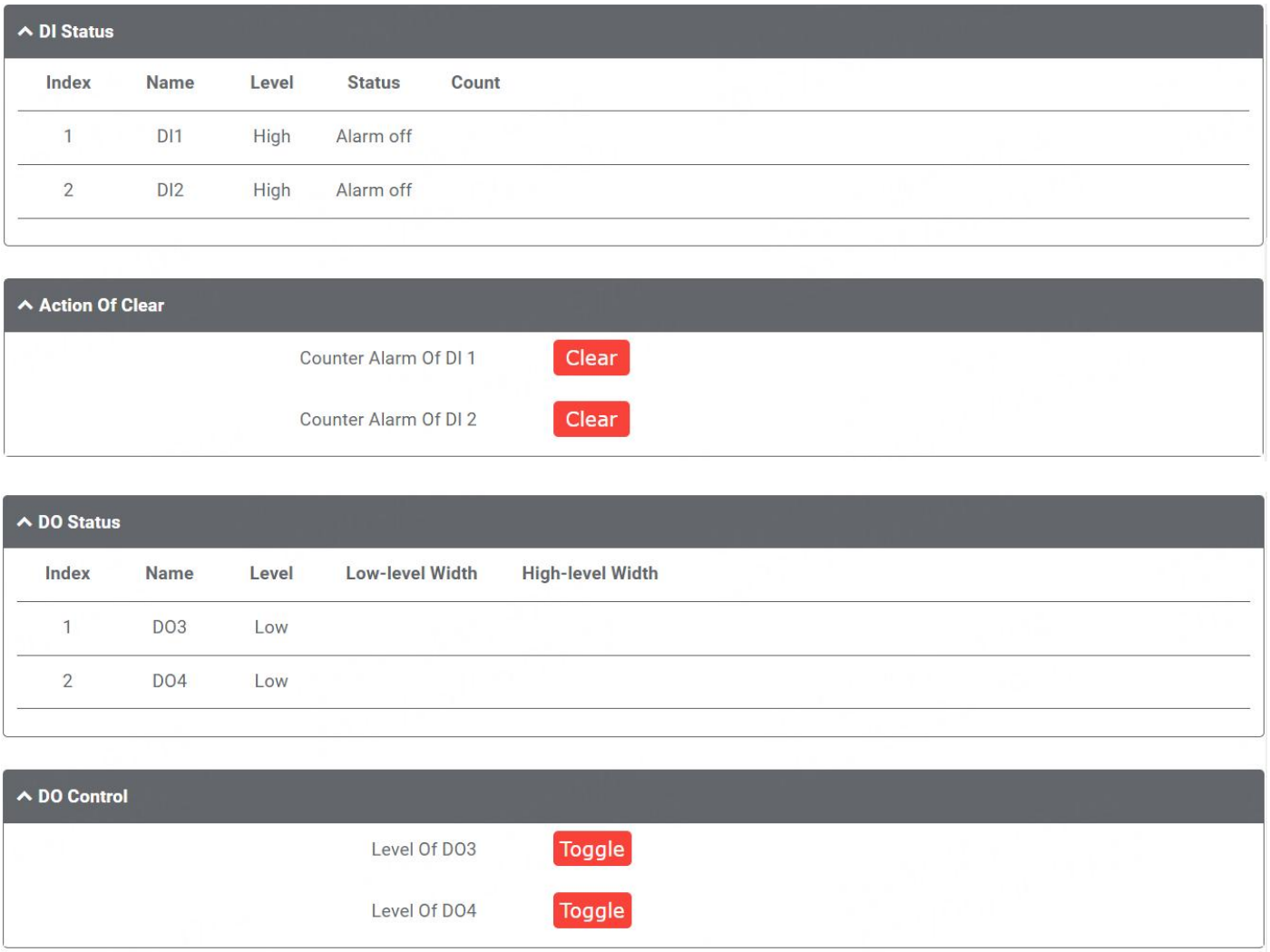
Relay Output



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

Status

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



3.2.9 Serial Port

This section allows you to set the serial port parameters. The device might support two serial ports, which might be configured as RS232or RS485 according to requirements . The serial data can be converted into IP data or through IP data into serial data, and then the data can be transmitted through wired or wireless network, so as to realize the function of transparent data transmission.

Serial Port

Serial Port Settings

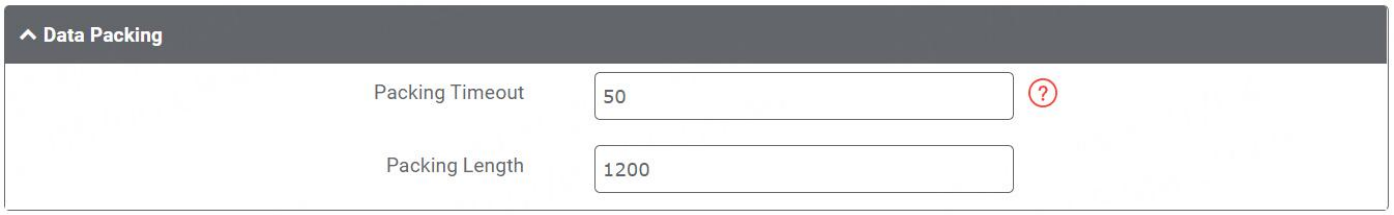
Index	Port	Enable	Type	Baud Rate	Application Mode	
1	COM1	false	RS232	115200	Transparent	
2	COM2	false	RS232	115200	Transparent	

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

Serial Port Application Settings

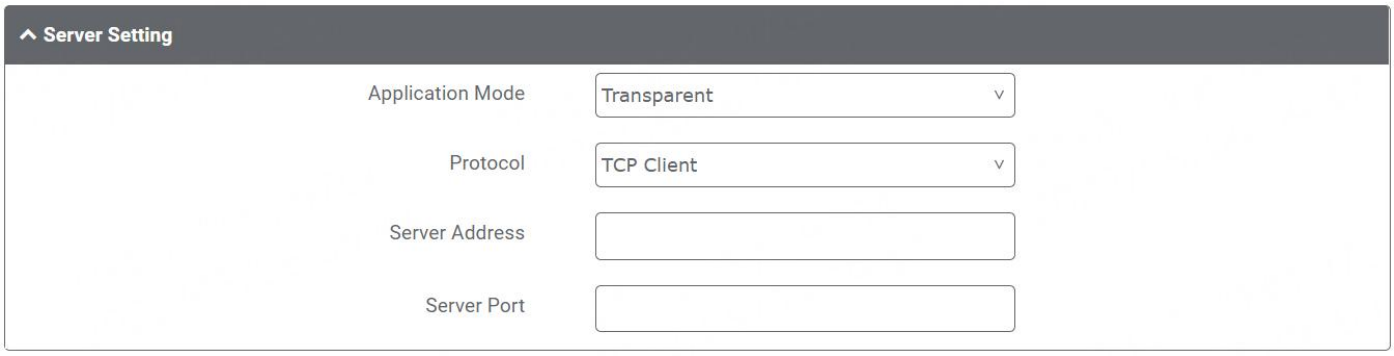
Index	1
Port	COM1
Enable	ON OFF
Type	RS232
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

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

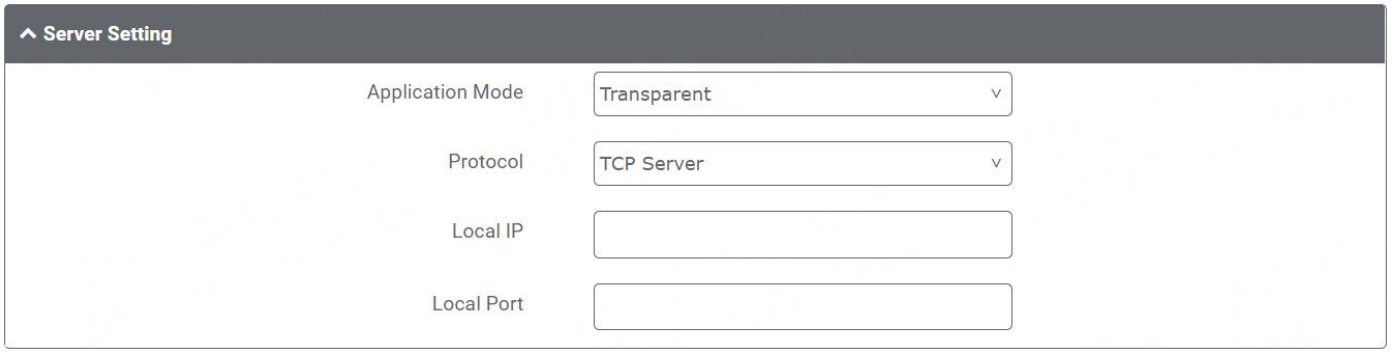


Item	Description	Default
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. The unit is milliseconds. **Note**: Data will also be sent as specified by the packet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

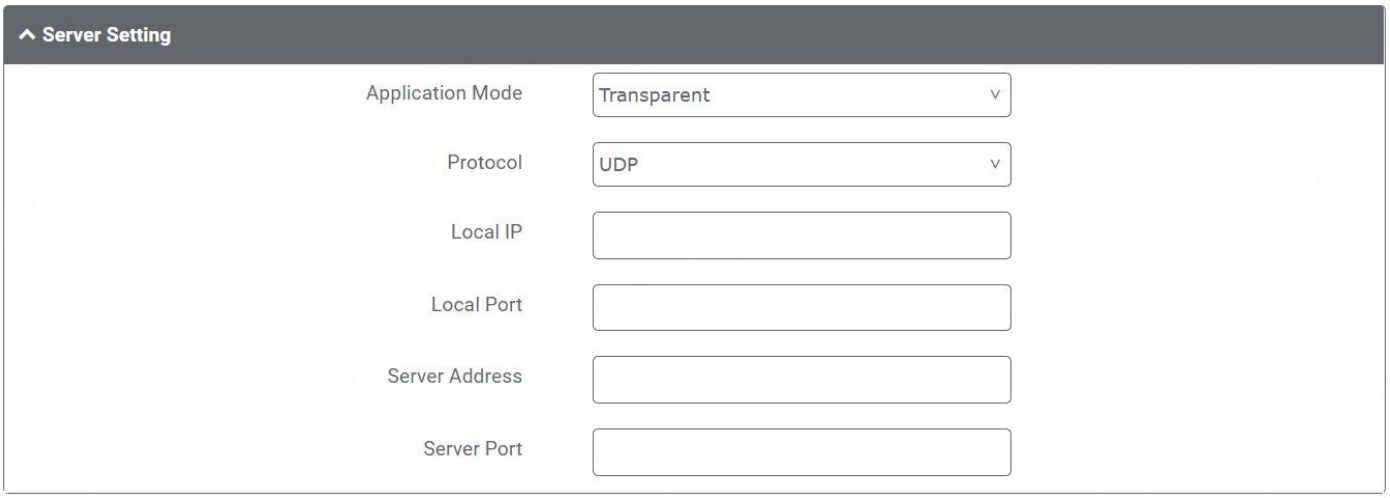
In the "Server Settings" column, when "Transparent" is selected as the application mode and "TCP Client" as the protocol, the window is as follows:



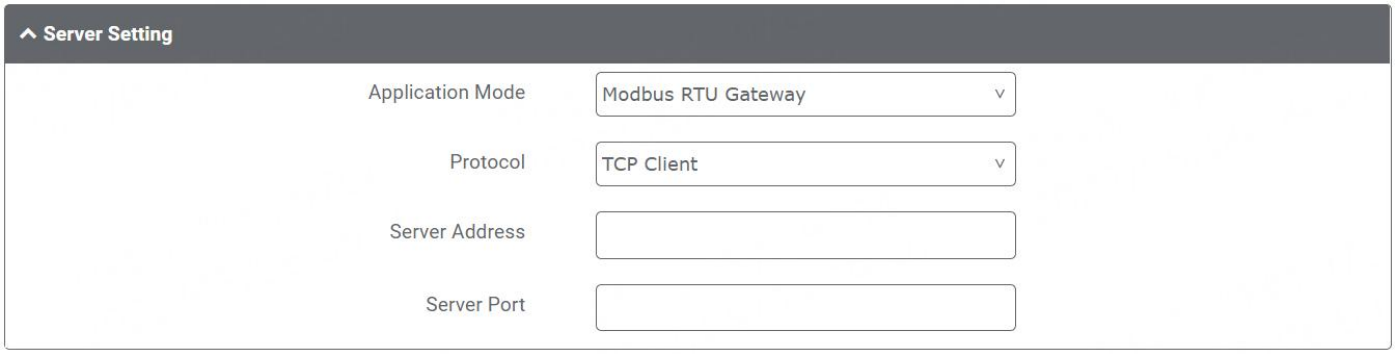
When "Transparent" is selected as the application mode and "TCP Server" as the protocol, the window is as follows:



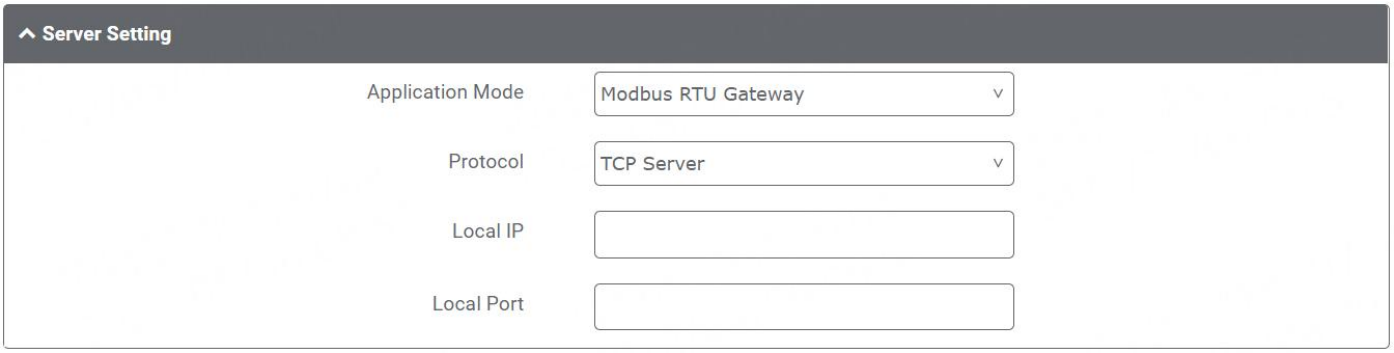
When "Transparent" is selected as the application mode and "UDP" is used as the protocol, the window is as follows:



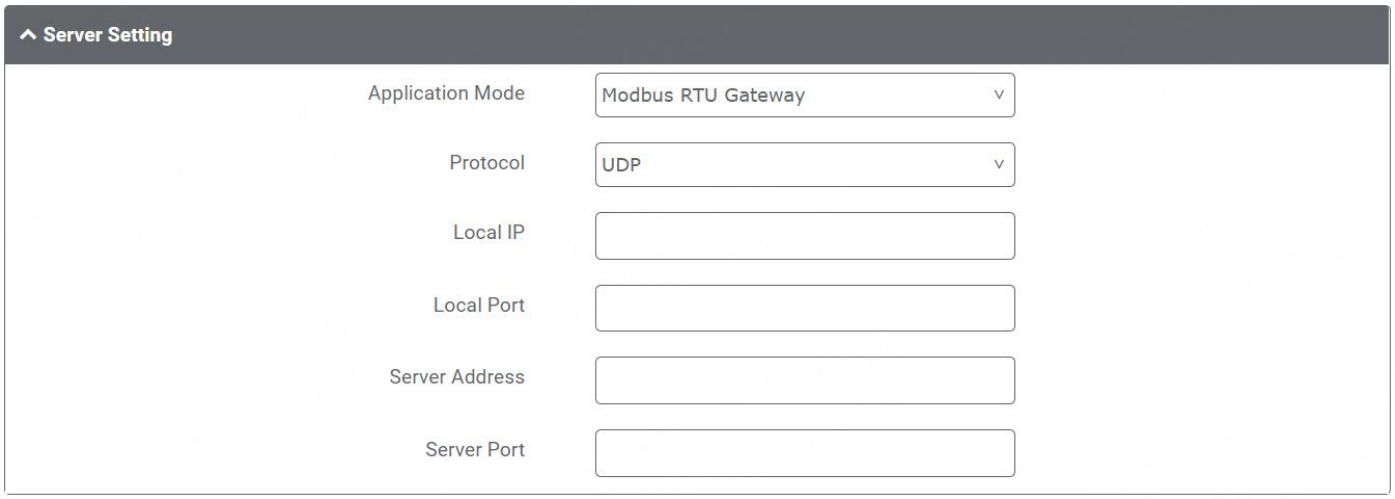
When “Modbus RTU Gateway” is selected as the application mode and “TCP Client” as the protocol, the window is as follows:



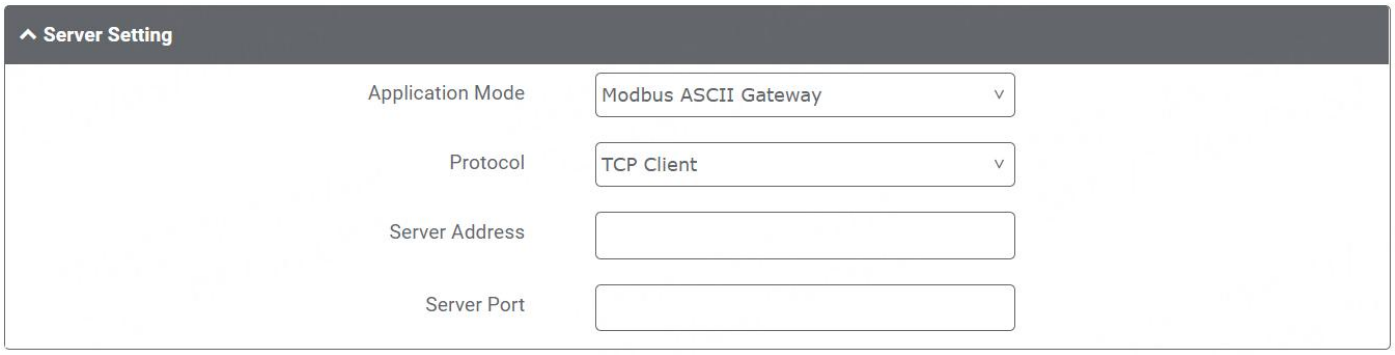
When "Modbus RTU Gateway" is selected as the application mode and "TCP Server" as the protocol, the window is as follows:



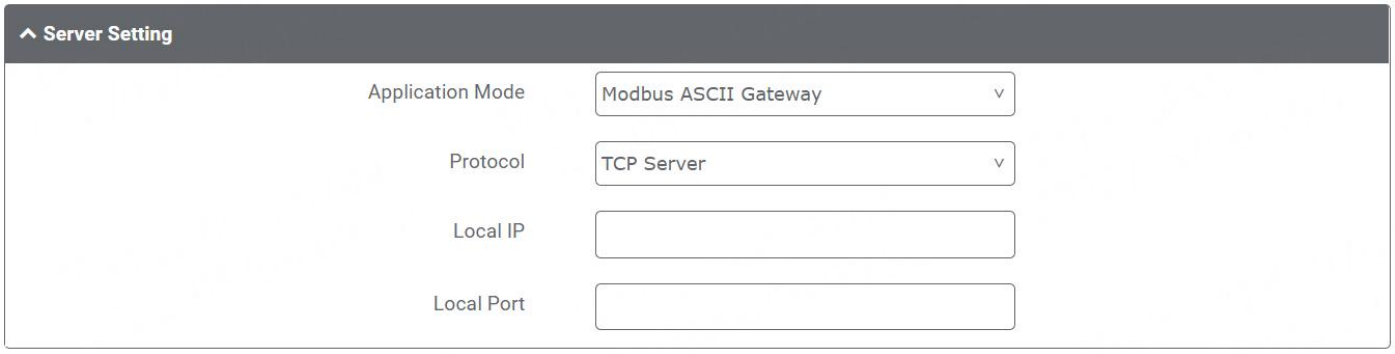
When selecting "Modbus RTU Gateway" as the application mode and "UDP" as the protocol, the window is as follows:



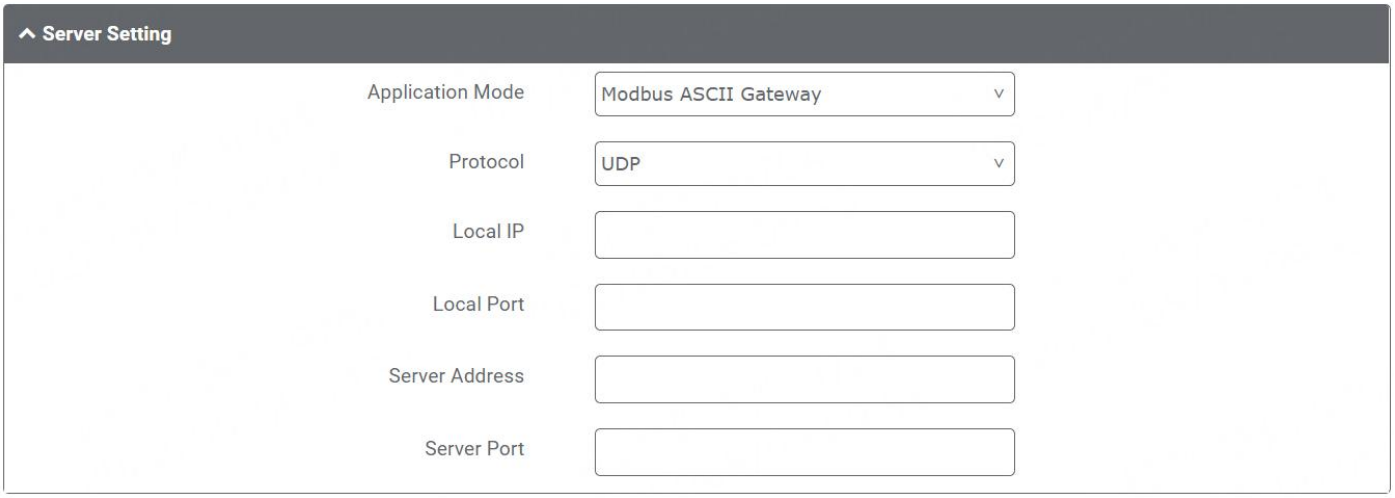
When “Modbus ASCII Gateway” is selected as the application mode and “TCP Client” as the protocol, the window is as follows:



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



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

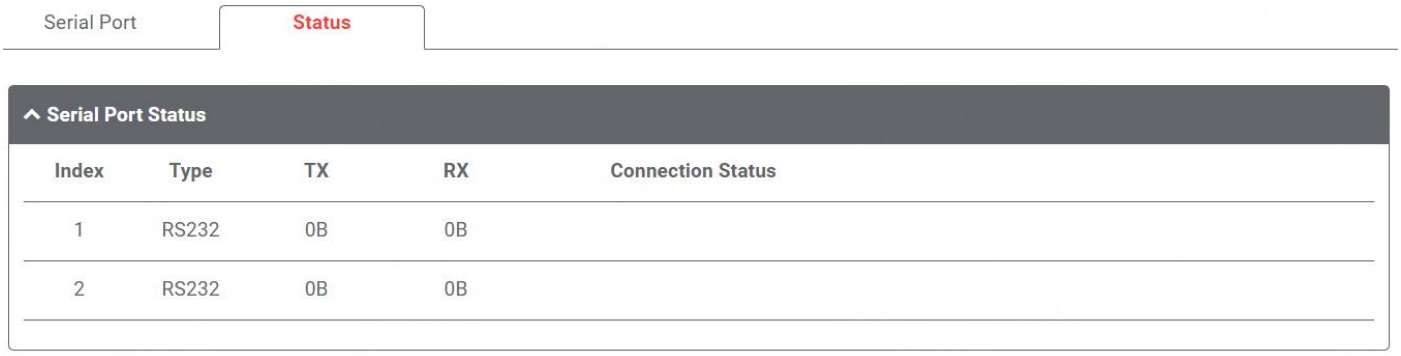


Item	Description	Default
Application Mode	Select from “Transparent”, “Modbus RTU Gateway” or “Modbus ASCII Gateway”. • Transparent: Device will transmit the serial data transparently • Modbus RTU Gateway: Device will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa • Modbus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

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

Status

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



3.2.10 Bluetooth (Optional)

This section allows you to set the Bluetooth parameters. Bluetooth can scan for other nearby Bluetooth devices.

General

Item	Description	Default
Enable	Click the toggle button to enable or disable the function.	OFF
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF
Clear Interval	Enter the interval of Bluetooth scan result clearify. unit:second valid range:5-3600	60

Status

Click Clear to clear scan results

You can view scan results in the scan column.

Scan RawData

Index	MAC	Name	RAW Data	RSSI
1	23D542E5452F	(unknown)	1EFF0600010F20028F5026A2BD63221C6CF...	-99
2	7E2FC52A2621	(unknown)	02010607FFFCE806EEEF3C03020016	-103
3	37A59DE7A336	(unknown)	1EFF0600010F20023ABD0EA095D5361721F...	-82
4	4383A12E809C	(unknown)	1EFF4C000719010E2002F98F0200059BDA3...	-97
5	45DAEF4F92C7	(unknown)	02011A020A080CFF4C001007351F6FD2814...	-91
6	3F746D777121	(unknown)	02011A0DFF4C001608C1003BCF631475D5	-92
7	248FEE485581	(unknown)	1EFF0600010920222DD45D389589F631710...	-97
8	EA95C8FC7BB1	(unknown)	07FF4C0012020001	-92
9	C77877D985B3	(unknown)	07FF4C0012023200	-84

Scan iBeacon

Index	MAC	UUID	Major	Minor	RSSI at 1m	RSSI

Scan Eddystone

Index	MAC	Name	RSSI	Type	Data

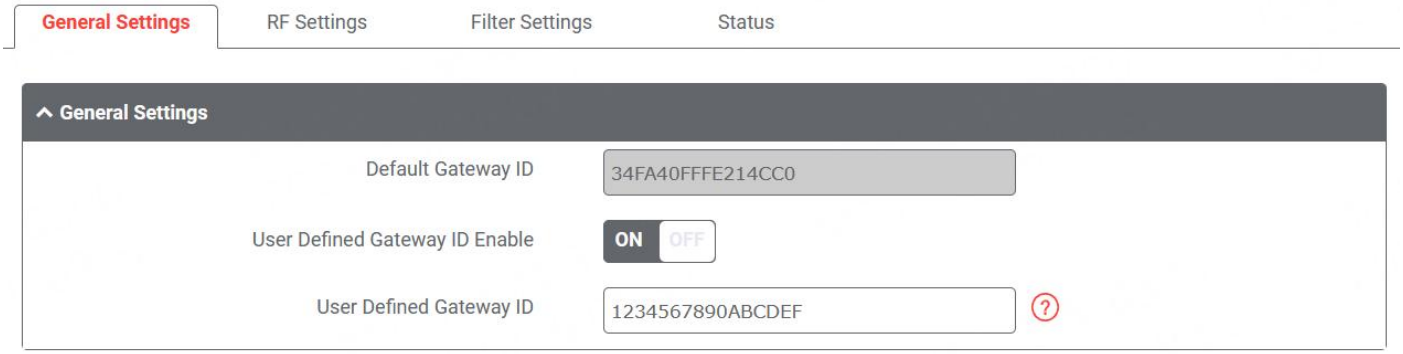
Scan ELA

Index	MAC	Name	RSSI	Type	Data

3.2.11 LoRa (Supported in LG5100)

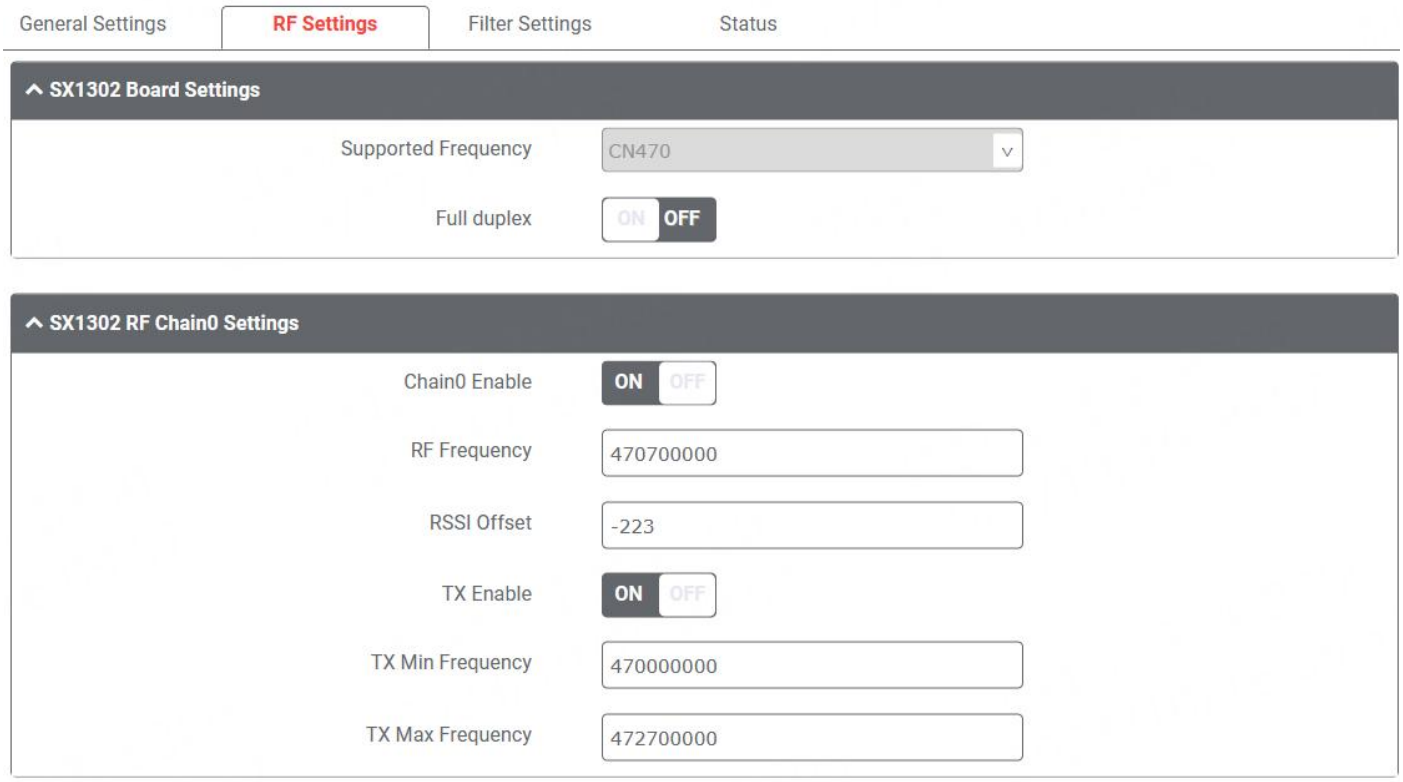
This section allows you to set the LoRaWAN parameters. It is only for the LG5100.

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



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.	1234567890ABCDEF

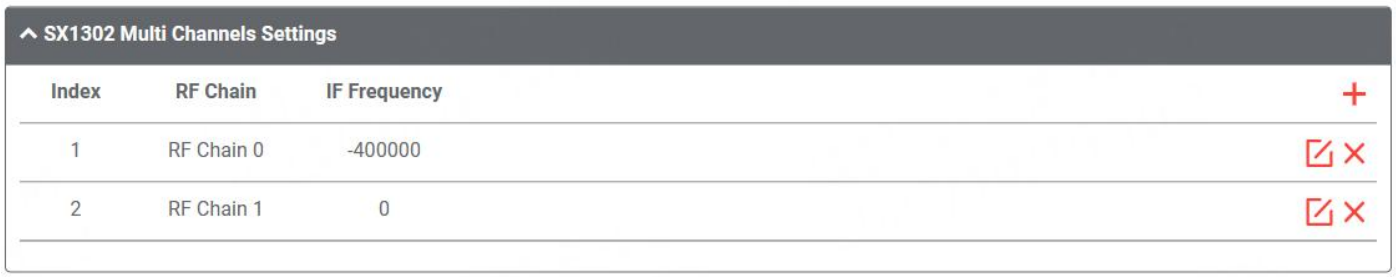
RF Settings



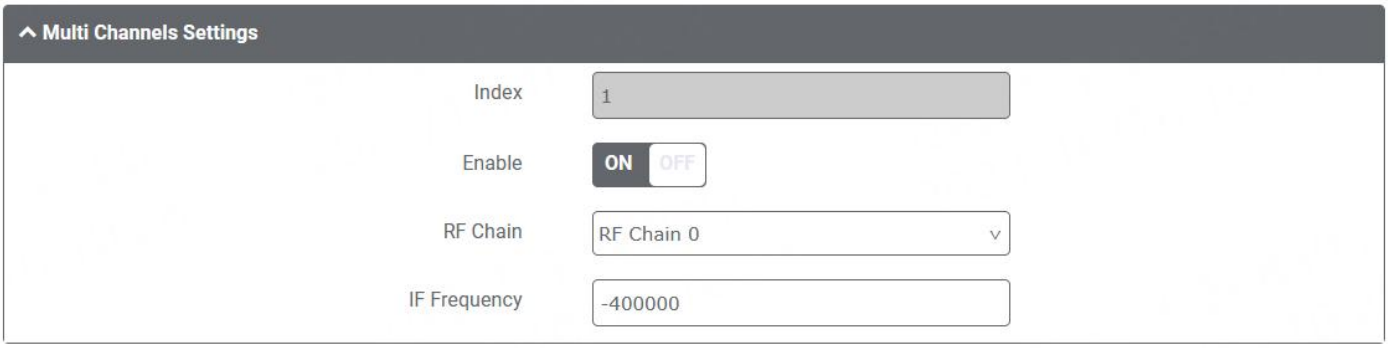
RF Settings		
Item	**Description**	**Default**
SX1302 Board Settings		
Support Frequency	Display support frequency. EU868: 868.1,868.3,868.5,867.1,867.3,867.5,867.7,867.9, STD 868.3 and FSK 868.8; RU868: RF Chain 0:869000000,RF Chain 1:864500000, 868.9,869.1,869.3,864.1,864.3,864.5,864.7,864.9; KZ868: RF Chain 0:865300000,RF Chain 1:867500000, 865.1,865.3,865.5,867.1,867.3,867.5,867.7,867.9. CN470: RF Chain 0:470700000,RF Chain 1: 471500000, 470.5,470.7,470.9,471.1,471.3,471.5,471.7,471.9.	Followed your device's model
Full duplex	Enabled/Diasbled Full duplex mode.	OFF
SX1302 RF Chain 0 Settings		
Chain 0 Enable	Enabled/Diasbled Chain 0.	ON
RF Frequency	Set frequency of RF link 0.	Followed your device's model
RSSI Offset	Set RSSI offset of RF link 0.	-223
TX Enable	Enabled/Disabled TX mode	ON
TX Min Frequency	Set TX Minimum frequency of RF link 0.	Followed your device's model
TX Max Frequency	Set TX Maximum frequency of RF link 0.	Followed your device's model
SX1302 RF Chain 1 Settings		
Chain 0 Enable	Enabled/Diasbled Chain 0.	ON
RF Frequency	Set frequency of RF link 1.	Followed your device's model
RSSI Offset	Set RSSI offset of RF link 0.	-223
TX Enable	Enabled/Disabled TX mode	OFF
TX Min Frequency	Set TX Minimum frequency of RF link 1.	Followed your device's model
TX Max	Set TX Maximum frequency of RF link 1.	Followed your device's

RF Settings		
Item	**Description**	**Default**
SX1302 Board Settings		
Frequency		model

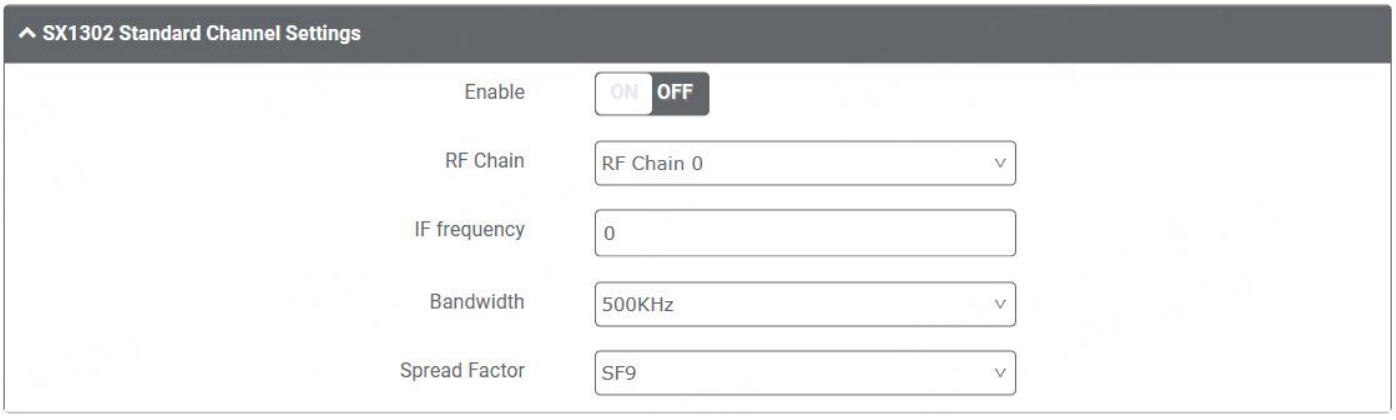
You can enable multi channels on this setting.



Click  to edit the RF Chain settings, here takes RF Chain 0 for example.

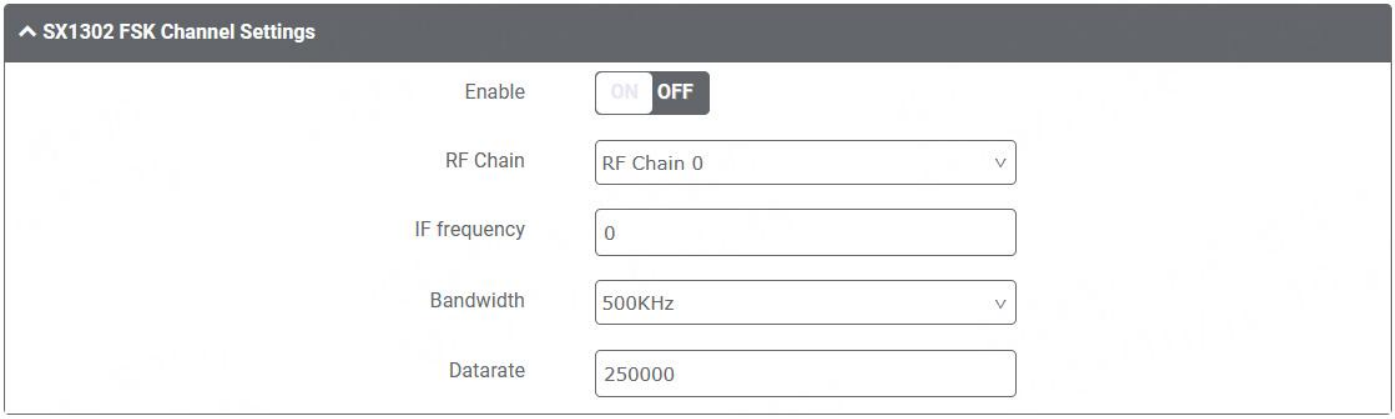


General Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this option.	ON
RF Chain	Select the RF Chain	RF Chain 0
IF frequency	Enter center frequency in the range -500000-500000 in Hz. The offset between the center frequency of a particular channel and the center frequency of RF link 0/1.	0



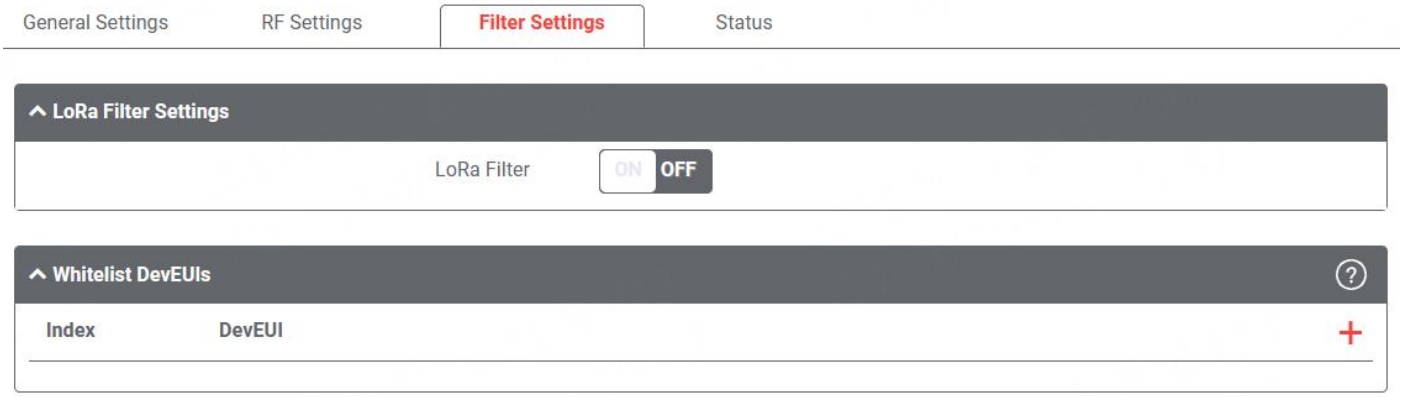
SX1302 Standard Channel Settings		
Item	**Description**	**Default**

SX1302 Standard Channel 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



SX1302 Standard Channel 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
Datarate	Enter the datarate.	250000

Filter Settings



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

Status

Basic

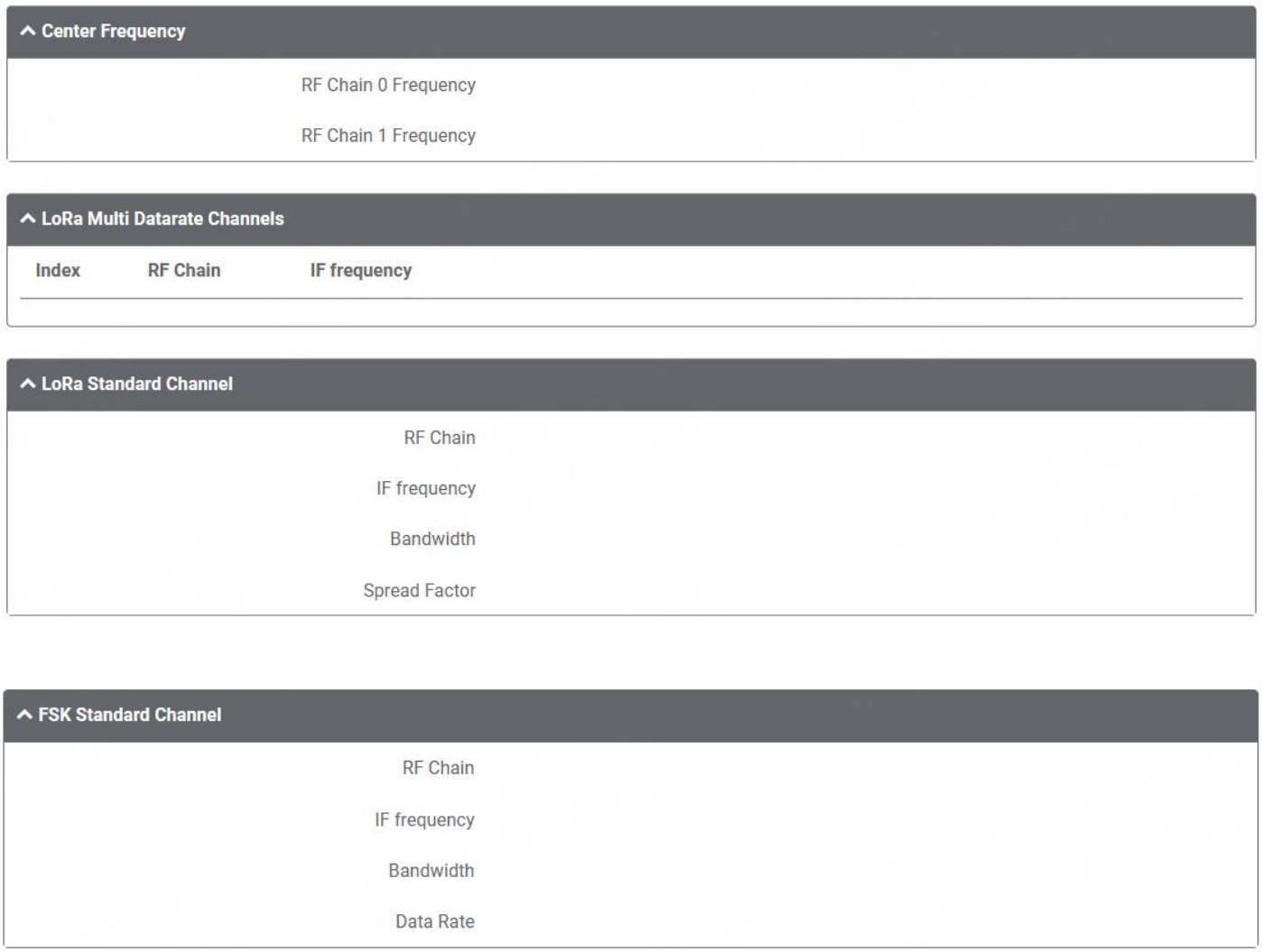
Model	

RF package received

CRC Errors	
Duplicates	
Join Duplicates	
Join Requests	
Total Packets	
RF Packets Received	
RF Packets Received State	
RF Packets Forwarded	

RF package sent

Duplicates Acked	
Packets Acked	
Total Join Responses	
Join Responses Dropped	
Total Packets	
Packets Dropped	
RF Packets Sent to Concentrator	
RF Packets Sent Errors	



Status	
Item	**Description**
Basic	
Model	Show LoRa module model.
RF Package 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
RF Packets Forwarded	Packets that CRC verified are sent from gateway to server.
Packets sent	
Duplicates Acked	Show the value of duplicate RF response packets sent.
Packets Acked	Show the value of RF response packets sent.

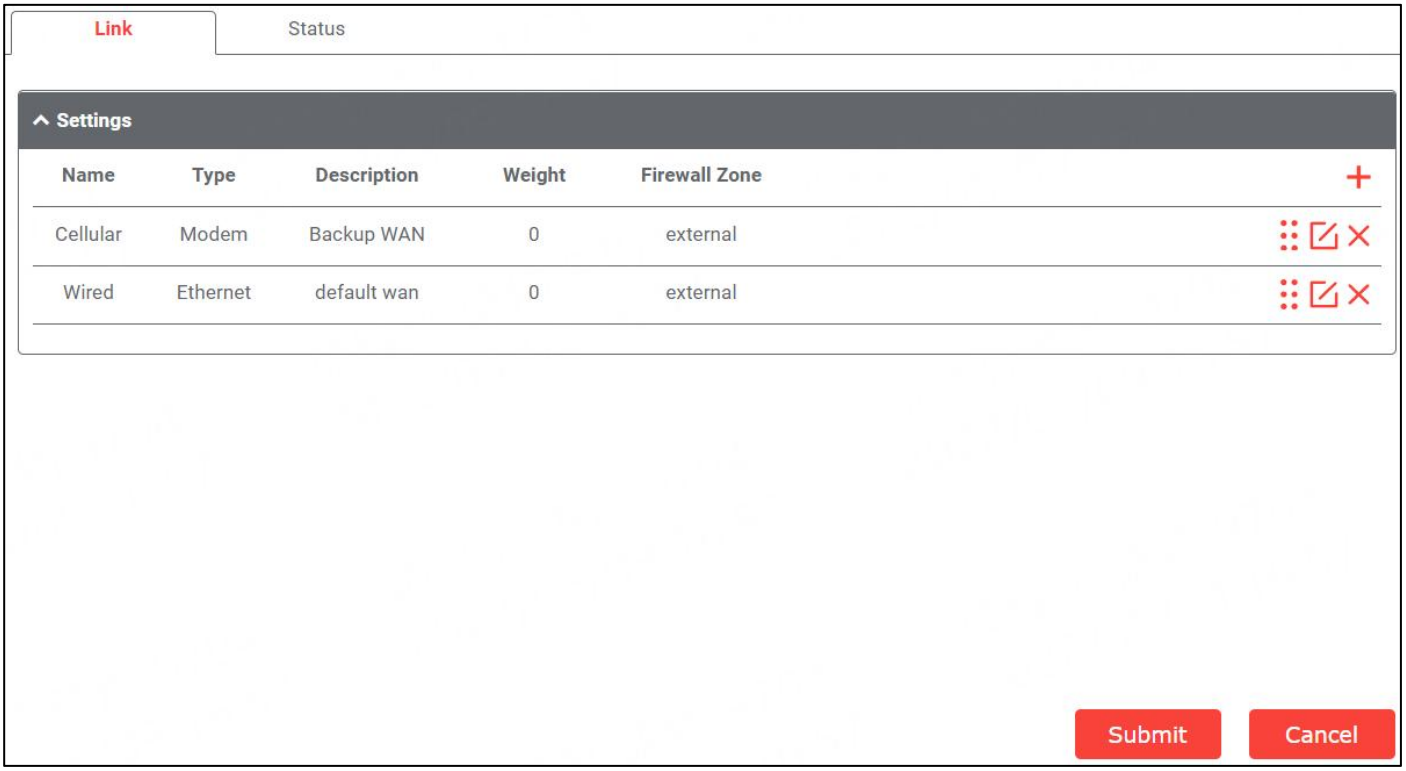
Status	
Item	**Description**
Total Join Responses	Show the value of duplicate RF join response packets sent.
Join Responses Dropped	Show the value of failed RF join response packets.
Total Packets	Show the value of RF packets sent.
Packets Dropped	Show the value of RF dropped packets.
RF Packets Sent to Concentrator	Show the value of RF packets sent to concentrator.
RF Packets Sent Errors	Show the value of RF packets sent error.
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 Network

3.3.1 WAN

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

Link



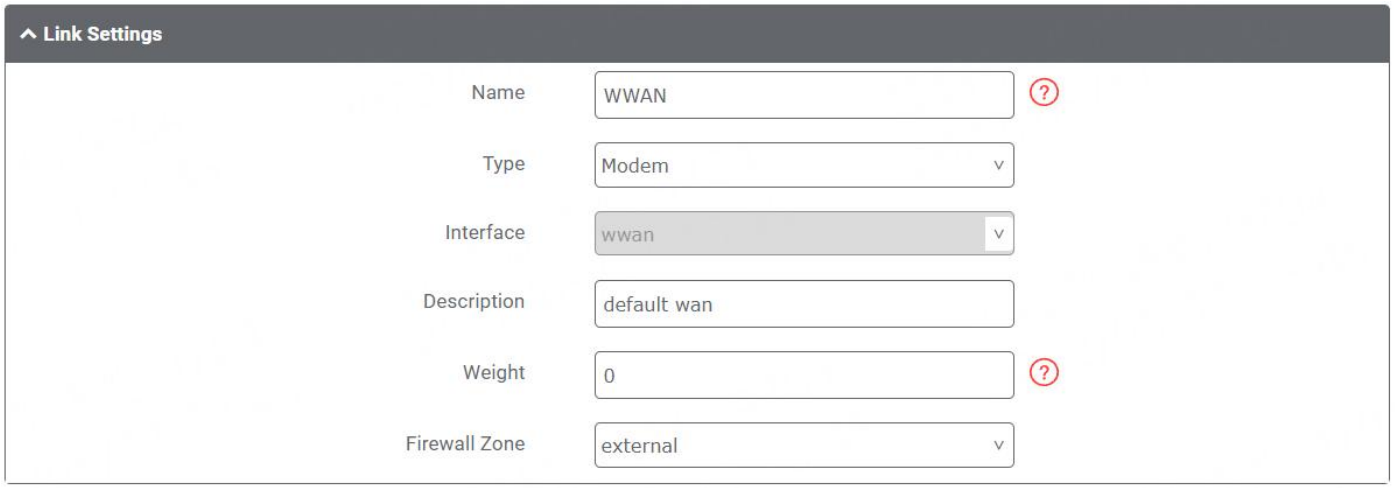
Click + to add a new WAN link.

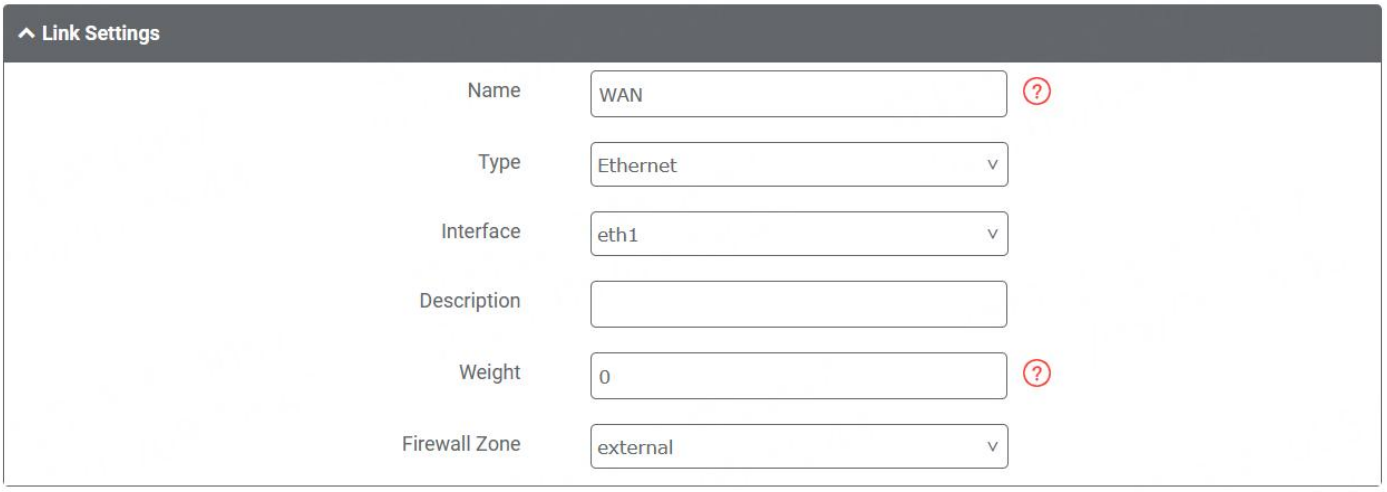
Click ✕ to delete the link.

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

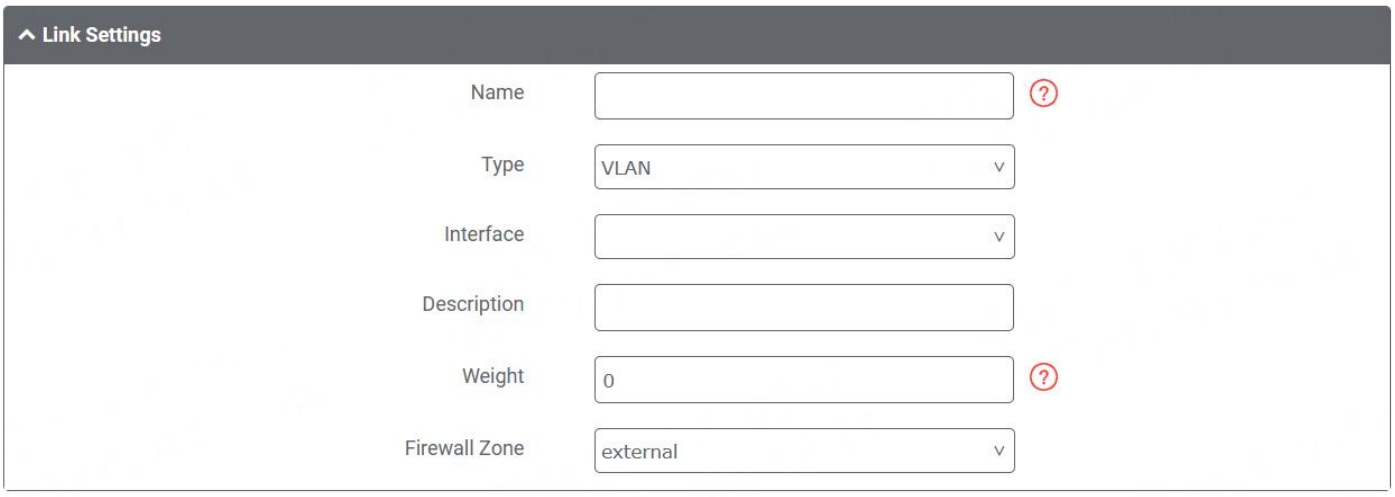
Click ✎ to edit the link.

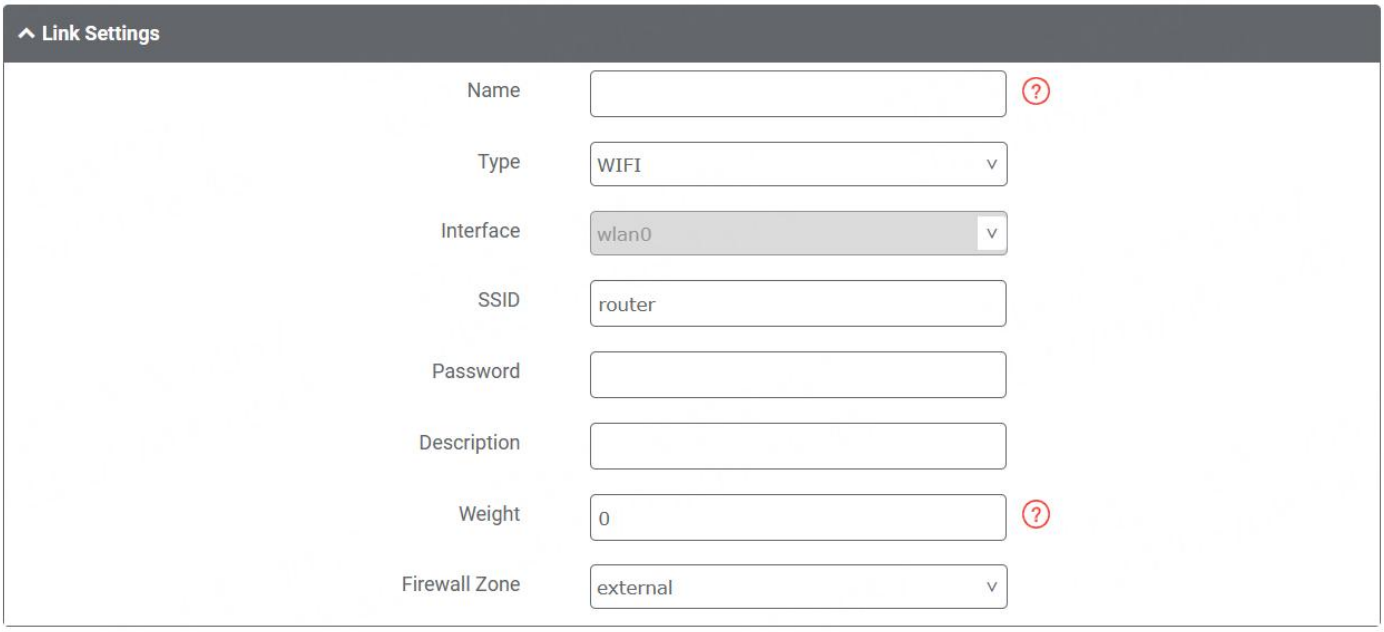
Users can manage link connections in this section. It provides four types of connectivity interface to internet including Modem, Ethernet, VLAN and Wi-Fi.





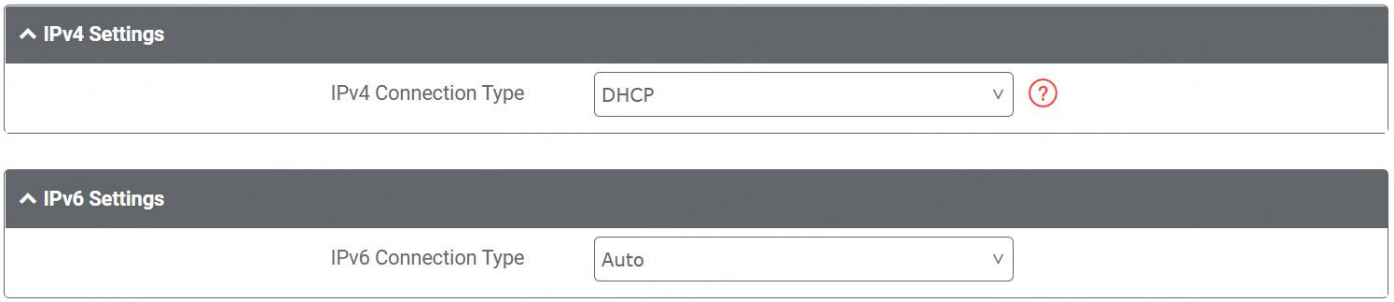
Note: You should uncheck the eth0 of sub interface on **Bridge** section when set eth0 as WAN.





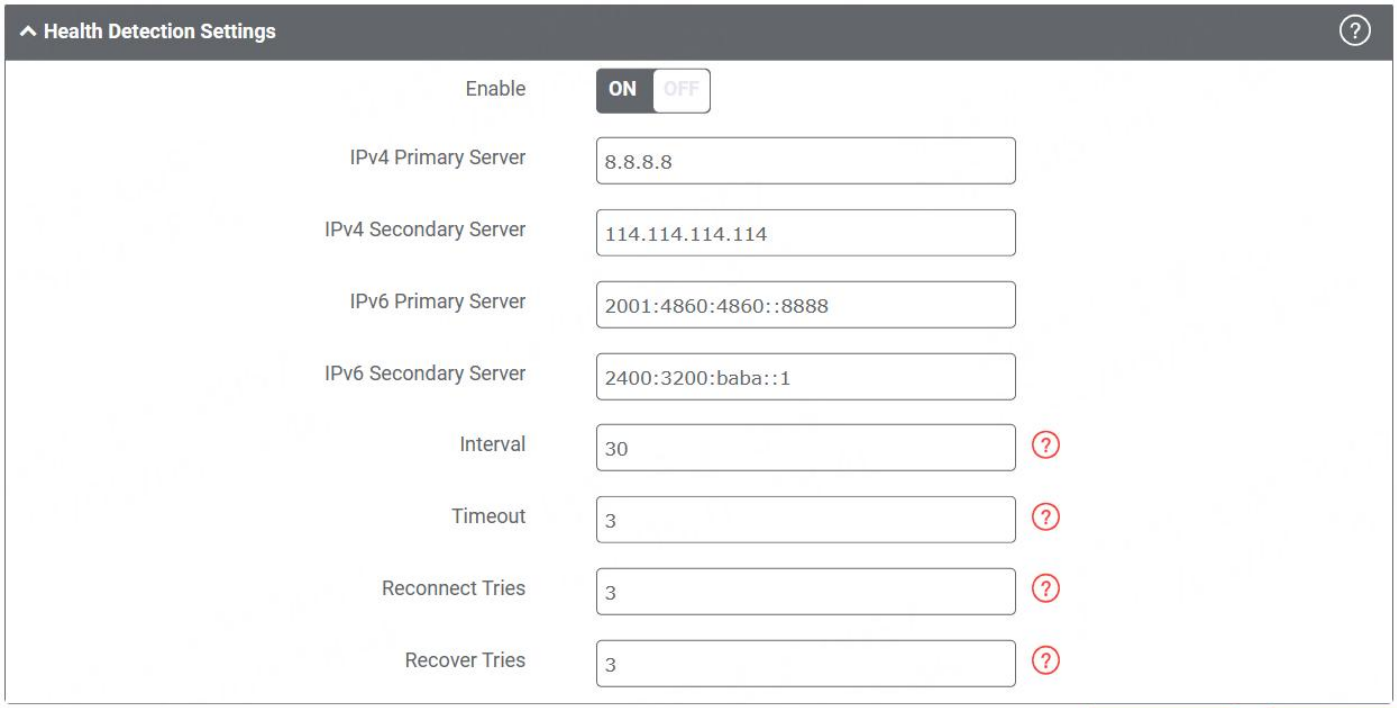
Note: Before setting the WIFI link type, you should config the Wi-Fi to Client mode.

Item	Description	Default
Name	The name of link.	--
Type	The types of connectivity. • Modem: connected by cellular network. • Ethernet: connected by Ethernet wired network. • VLAN: connected by VLAN network. • Wi-Fi: connected by Wi-Fi network.	--
Interface	Set the related interface. If the type is Modem, please see the **3.2.2 Cellular.** If the type is Ethernet, please see the **3.2.1 Ethernet.** If the type is VLAN, please see the **3.2.7 VLAN.**	--
Description	The description of the link.	--
SSID	The name of Wi-Fi network.	--
Password	The Password of Wi-Fi network.	--
Weight	The weight of this link among all links. 0 means not involved.	--
Firewall Zone	The chosen set of firewall rules, please see the **3.3.5 Firewall.**	--



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

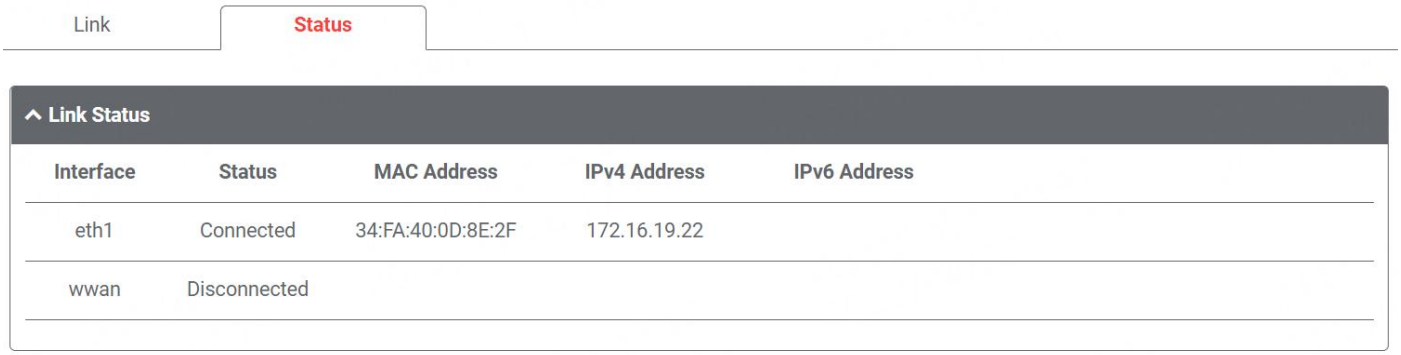
Item	Description	Default
	• DHCP. • PPPoE. • Manual. • Disable. Enter the parameters accordingly. **Note: IPv6 over PPPoE is not supported now, so disabling IPv6 if choosing PPPoE here.*	
IPv6 Connection Type	The type of IPv6 connection. • Auto. • Manual. • Disable. Enter the parameters accordingly.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



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

Status

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



3.3.2 LAN

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

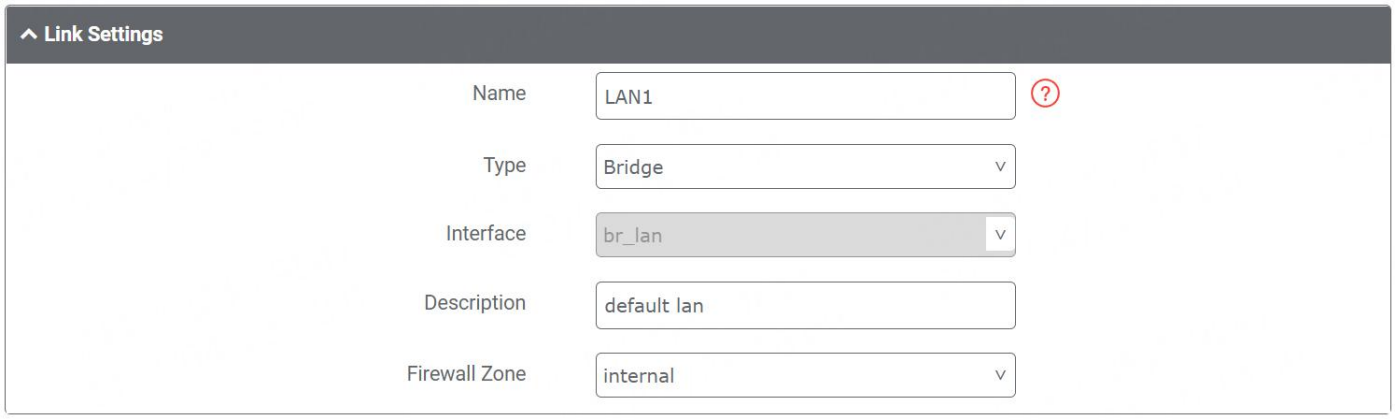
Link

Click + to add a new LAN link.

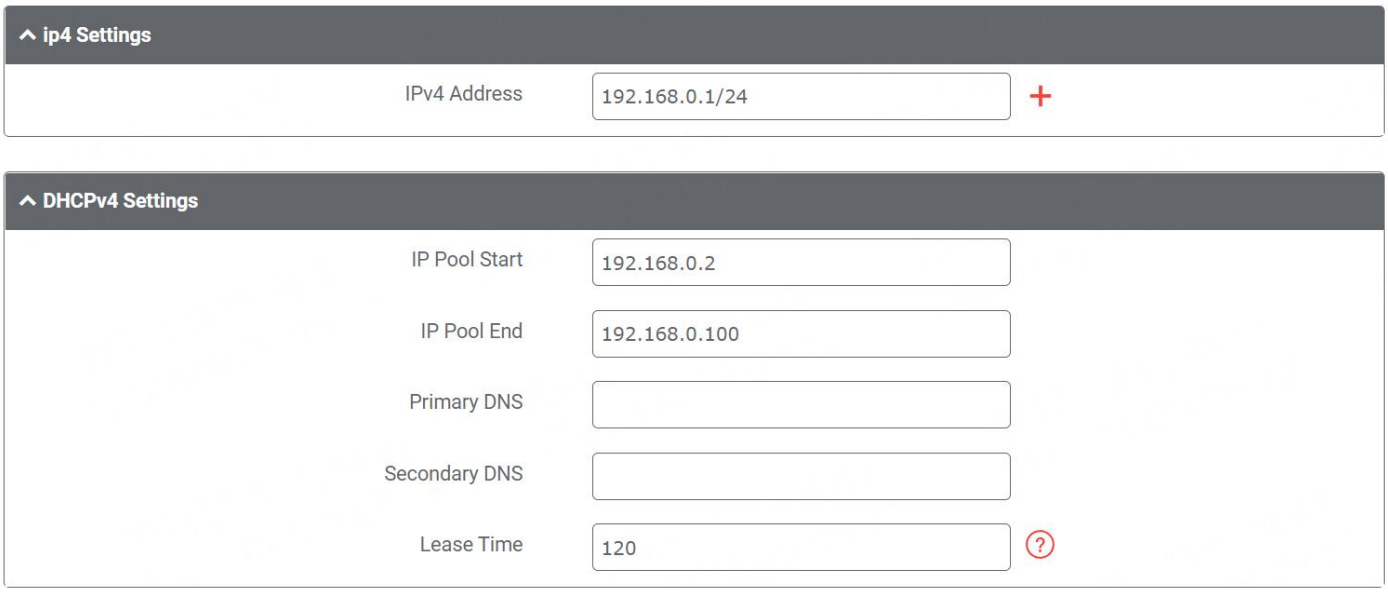
Click ✕ to delete the LAN link.

Click to edit the LAN link.

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

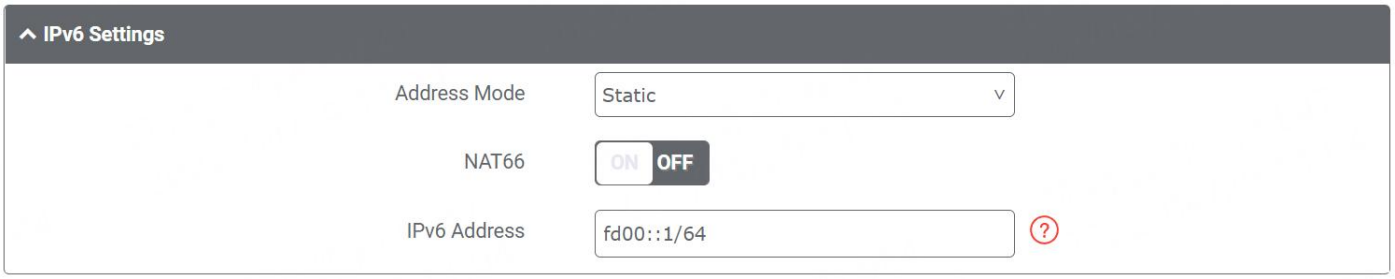


Item	Description	Default
Name	The name of the LAN link.	--
Type	The types of connectivity. Select from “Bridge”, “Ethernet” and “VLAN”. • Bridge: connected by Bridge network. • Ethernet: connected by Ethernet wired network. • VLAN: connected by VLAN network.	Bridge
Interface	Set the related interface. If the type is Bridge, please see the **3.2.3 Bridge.** If the type is Ethernet, please see the **3.2.1 Ethernet.** If the type is VLAN, please see the **3.2.7 VLAN.**	--
Description	The description of the link.	--
Firewall Zone	The chosen set of firewall rules, please see the **3.3.5 Firewall.**	internal



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

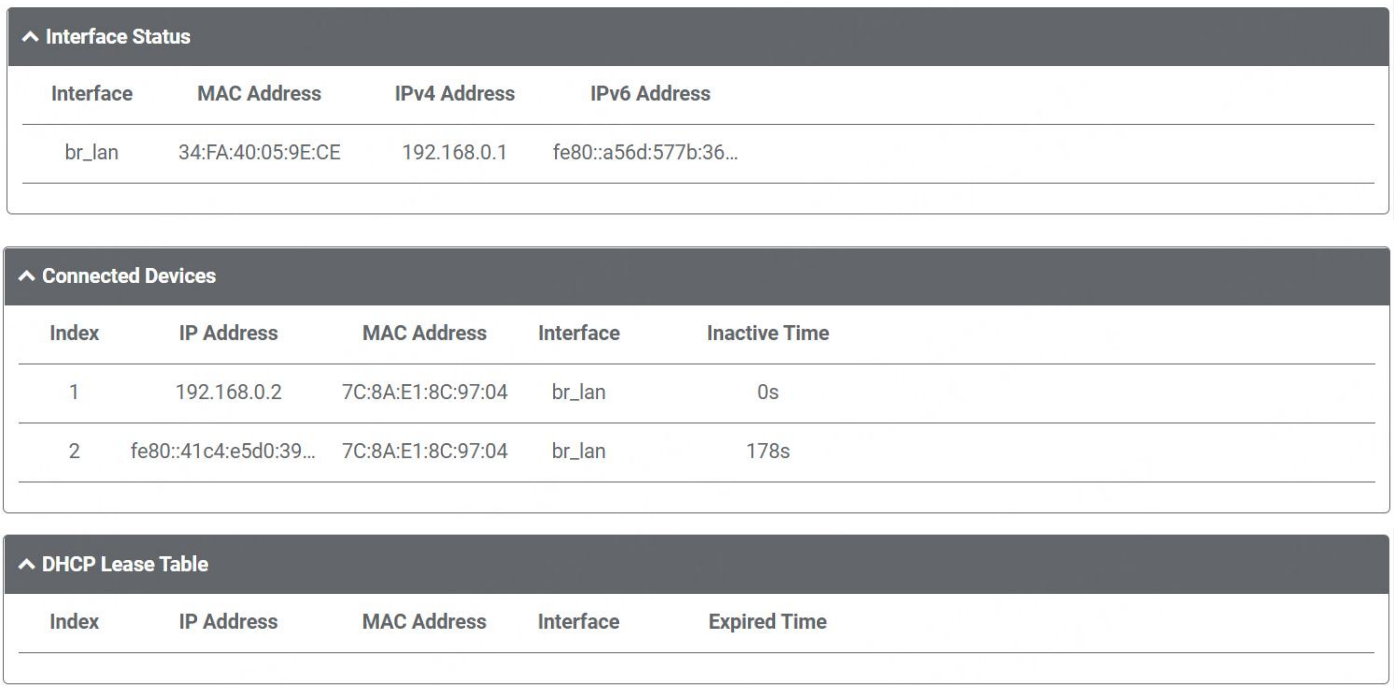
Item	Description	Default
Secondary DNS	Enter the secondary DNS.	Null
Lease Time	The lease time in minute.	120



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

Status

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

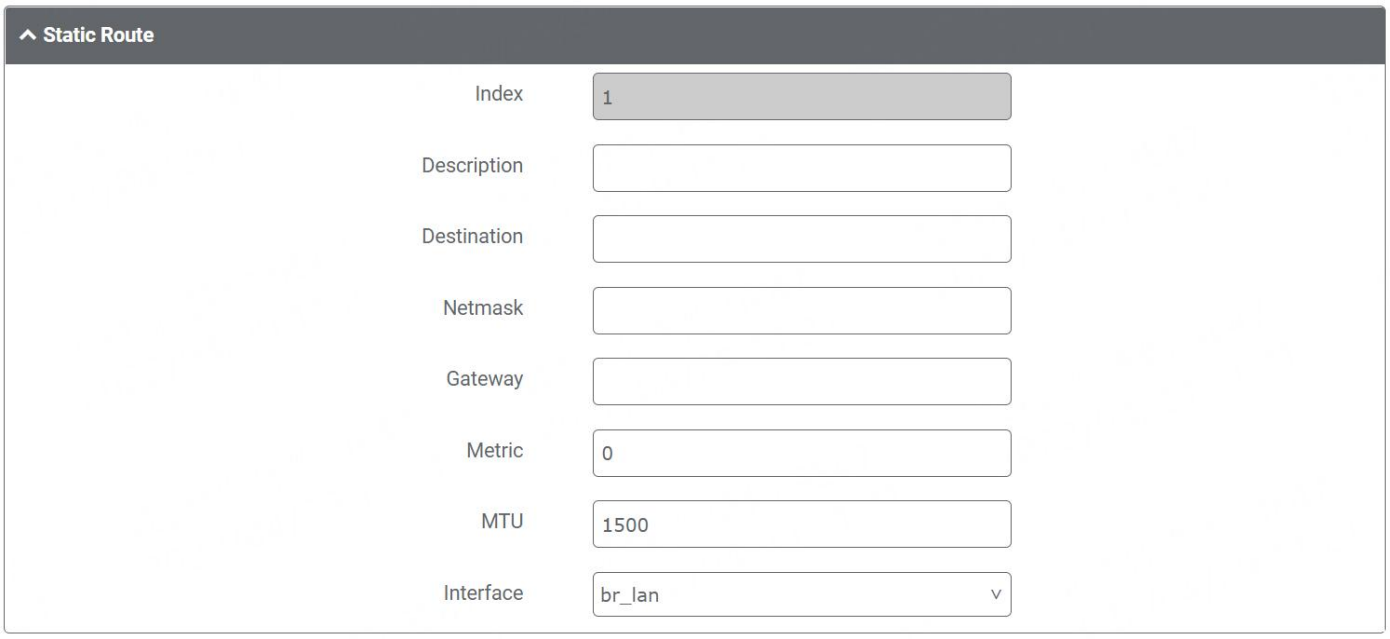


3.3.3 Route

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

Static Route

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

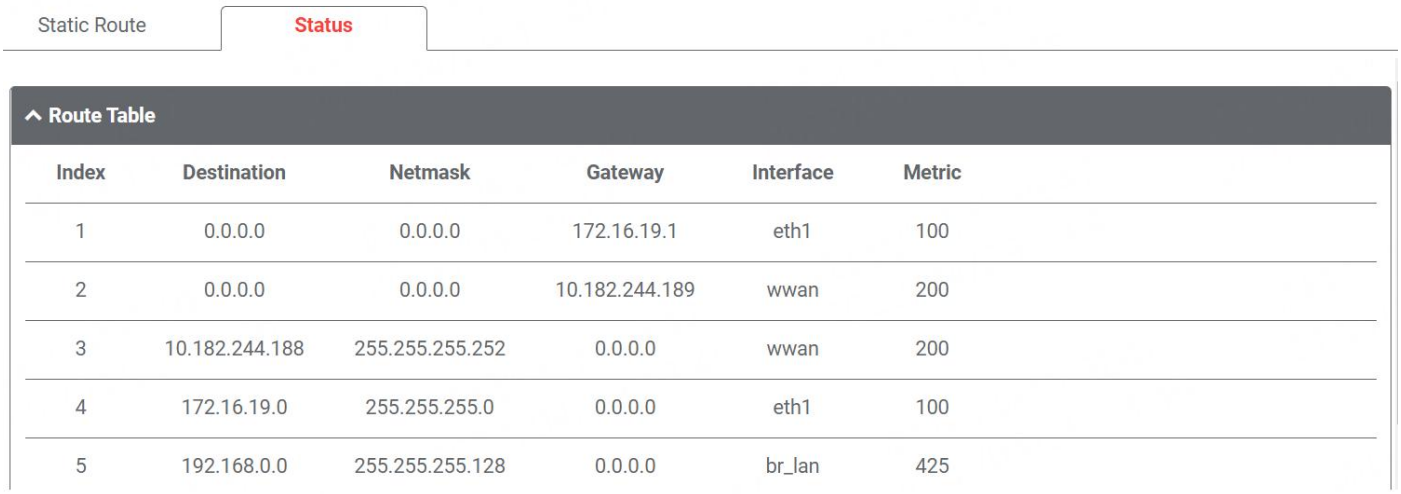


Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this static route.	Null
Destination	Enter the IP address of destination host or destination network.	Null
Netmask	Enter the Netmask of destination host or destination network.	Null
Gateway	Define the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

Item	Description	Default
Interface	Choose the corresponding port of the link that you want to configure.	br_lan

Status

This window allows you to view the status of route.

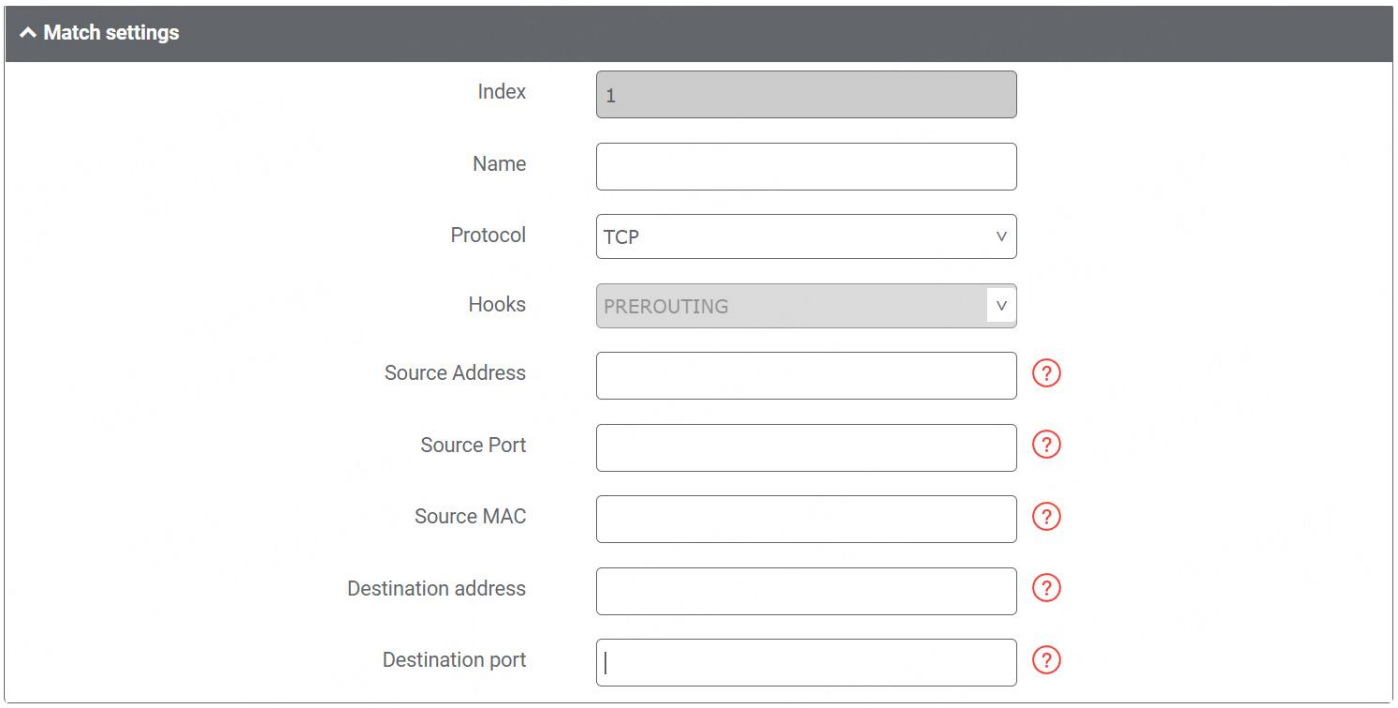


3.3.4 Policy Route

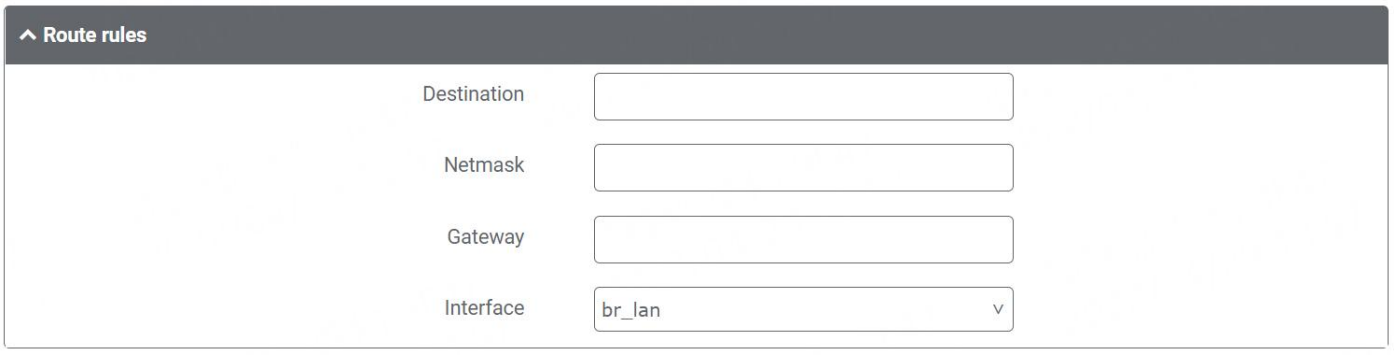
In this window, you can manage the outbound route based on the IP address, port number in the packet.

Policy Route

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



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

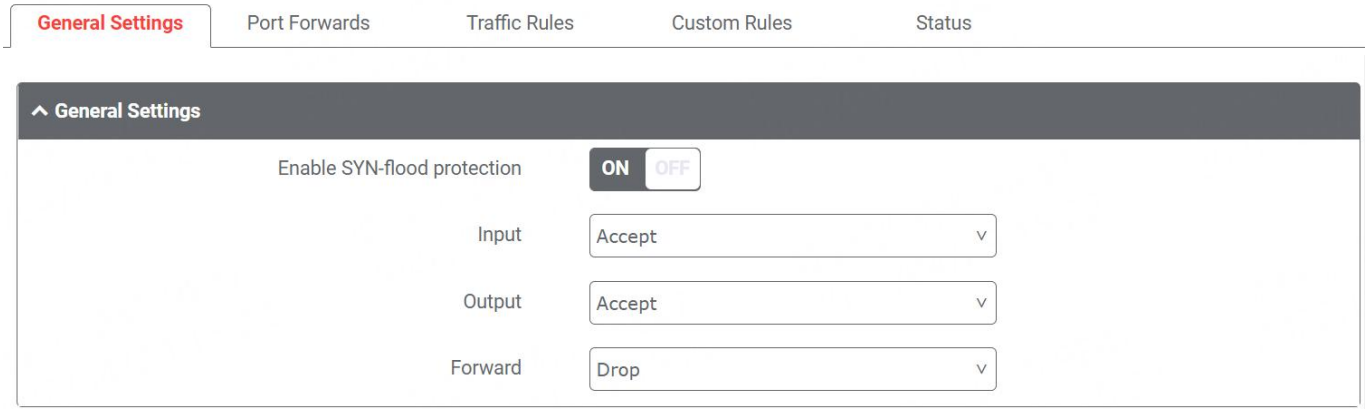


Item	Description	Default
Destination	Enter the IP address of destination host or destination network.	--
Netmask	Enter the Netmask of destination host or destination network.	--
Gateway	Define the gateway of the destination.	--
Interface	Choose the corresponding port of the link that you want to configure.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

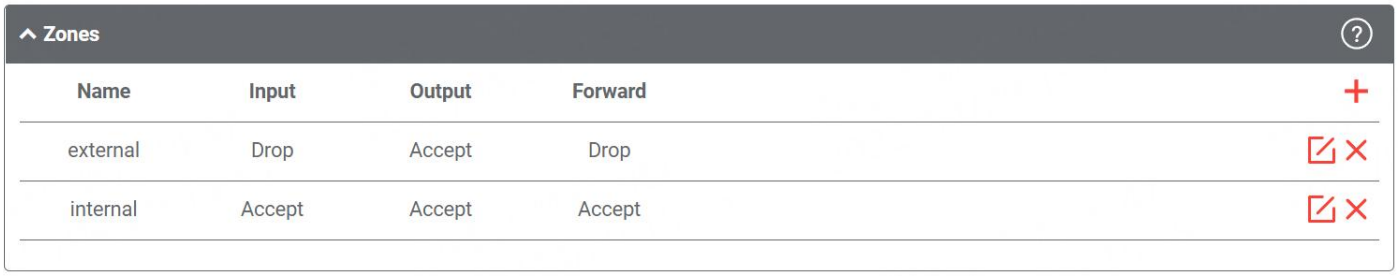
3.3.5 Firewall

Firewall makes use of Linux iptables to control inbound and outbound traffic.

General Setting

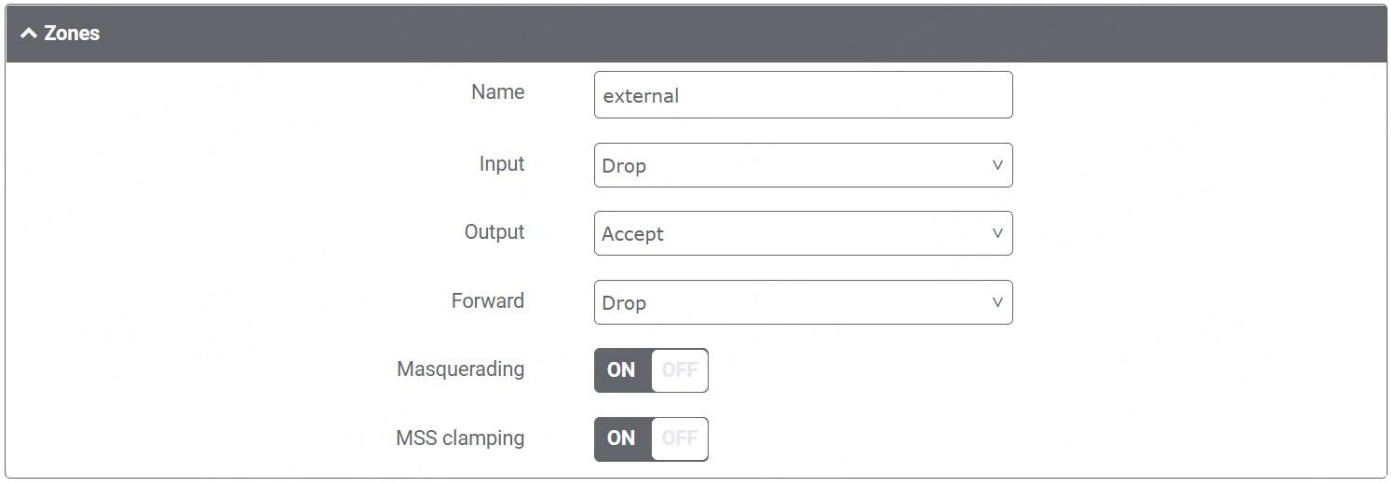


Item	Description	Default
Enable SYN-flood protection	Countermeasures to protect against SYN flood attacks, click the toggle button to enable/disable.	ON
Input	Default action of the Input chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Accept
Output	Default action of the Output chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Accept
Forward	Default action of the Forward chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Drop
Note: The general setting is used as a default firewall setting unless specified.		

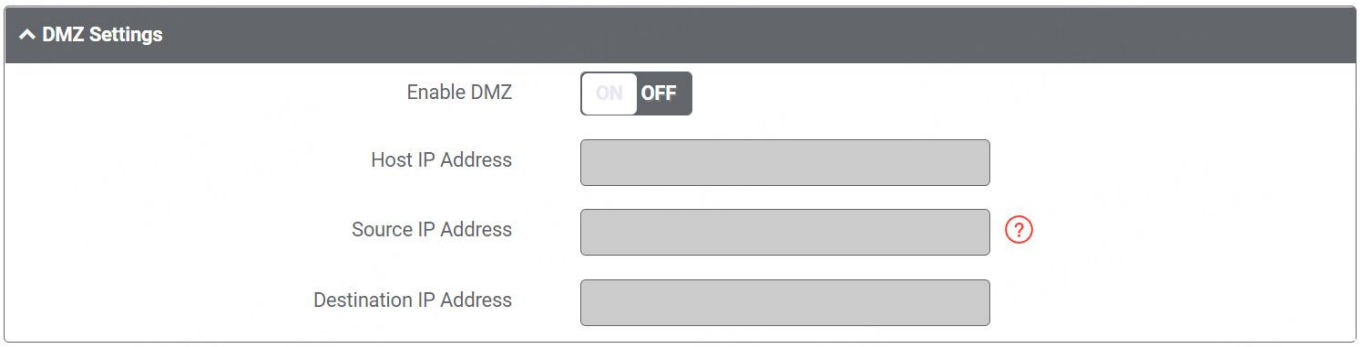


Zone is a set of firewall rules, users can define their own firewall zone.

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

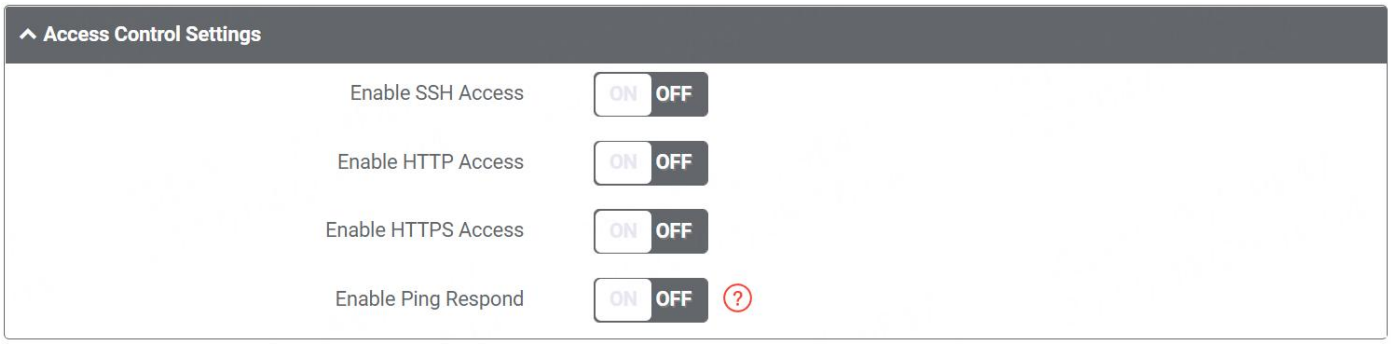


Item	Description	Default
Name	The name of the firewall zone.	--
Input	Default action of the Input chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Drop
Output	Default action of the Output chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Accept
Forward	Default action of the Forward chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • Drop: Packet is stopped and deleted.	Drop
Masquerading	Click the toggle button to enable/disable. MASQUERADE is an iptables target that can be used instead of the SNAT (source NAT) target when the external IP of the network interface is not known at the moment of writing the rule (when the interface gets the external IP dynamically).	ON
MSS clamping	Click the toggle button to enable/disable. MSS clamping is a workaround used to change the maximum segment size (MSS) of all TCP connections passing through links with an MTU lower than the Ethernet default of 1500.	ON



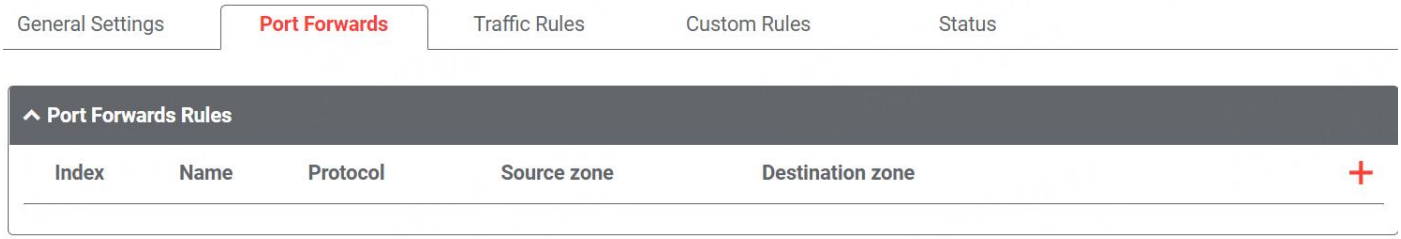
DMZ (Demilitarized Zone), also known as the demilitarized zone. It is a buffer between a non-secure system and a secure system that is set up to solve the problem that users who access the external network cannot access the internal network server after the firewall is installed. A DMZ host is an intranet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

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



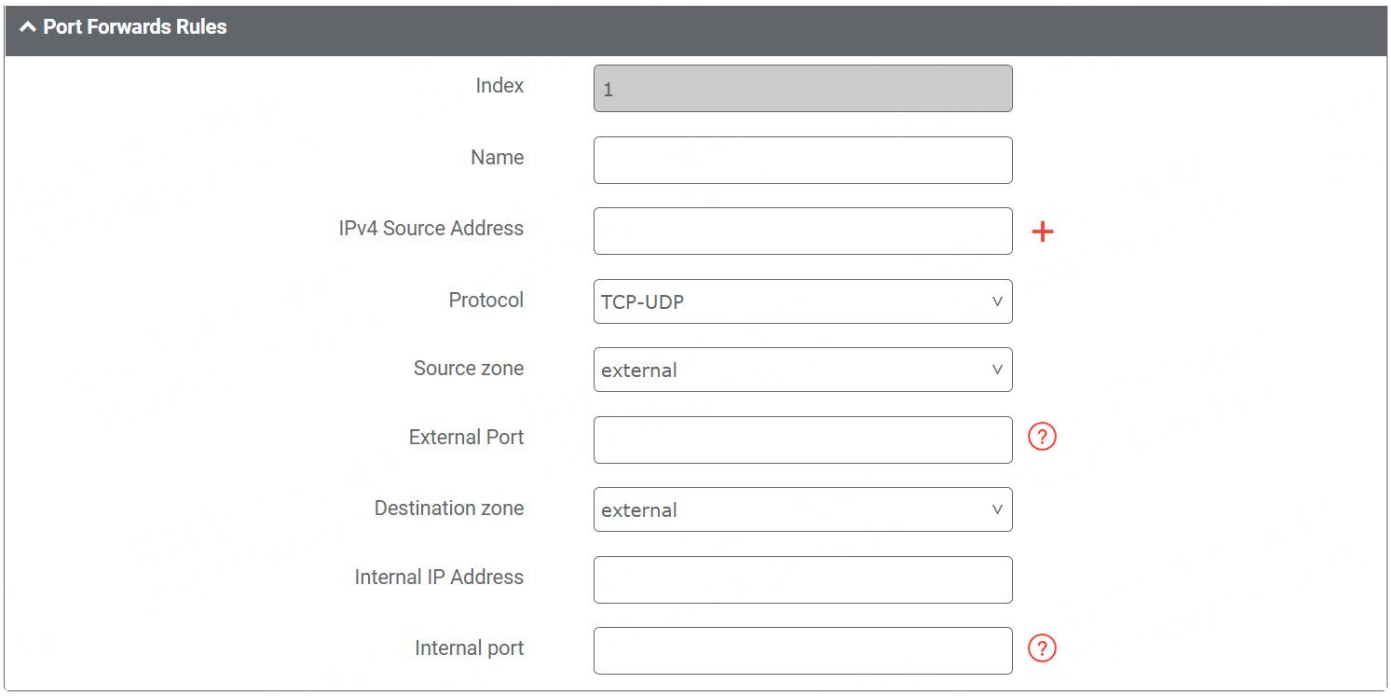
Item	Description	Default
Enable SSH Access	Click the toggle button to enable/disable this option. When enabled, the zone user can access the device via SSH.	OFF
Enable HTTP Access	Click the toggle button to enable/disable this option. When enabled, the zone user can access the device via HTTP.	OFF
Enable HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the zone user can access the device via HTTPS.	OFF
Enable Ping Respond	Click the toggle button to enable/disable this option. When enabled, the device will reply to the Ping requests from other hosts on the zone.	OFF

Port Forwards



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

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

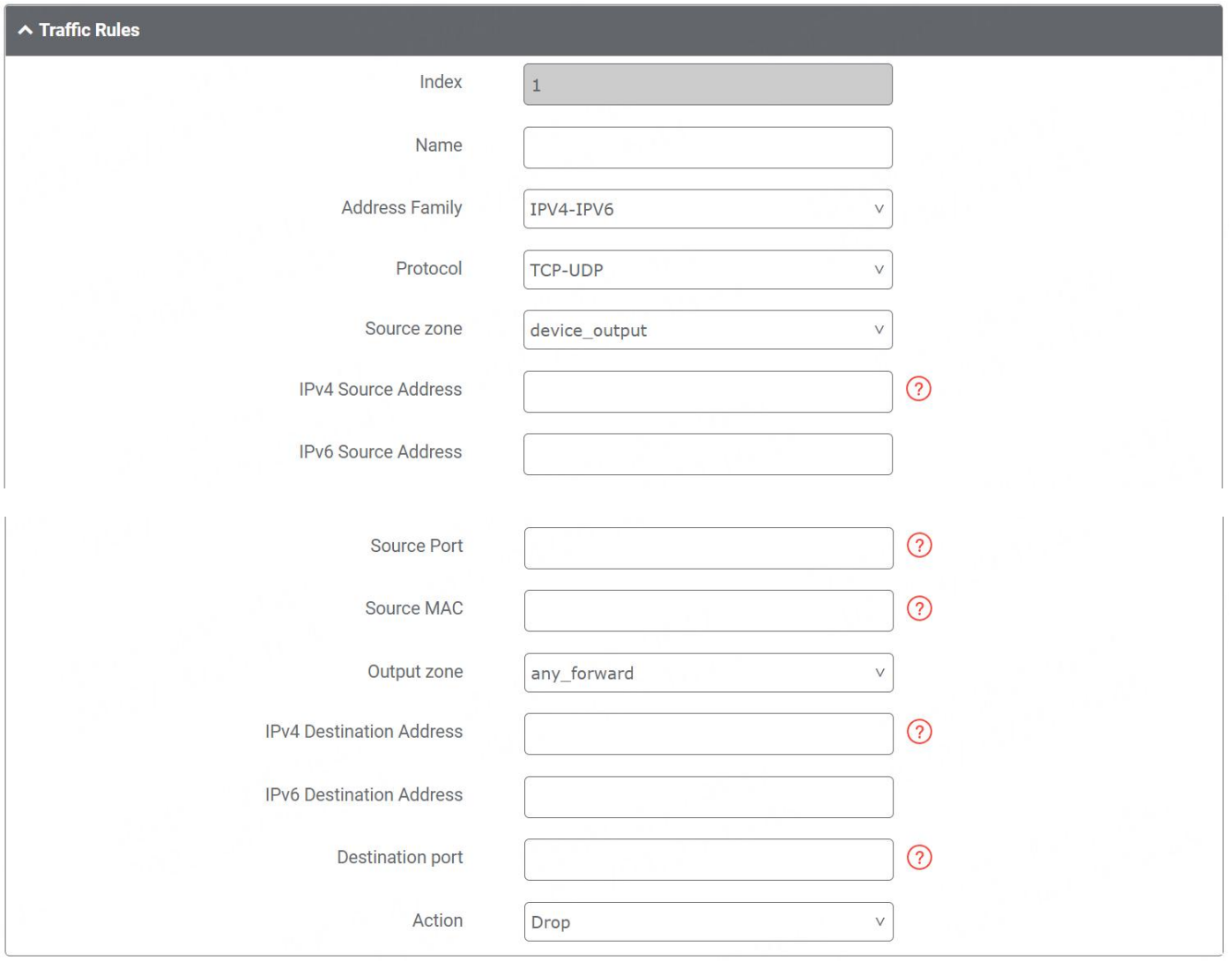


Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	Name of the rule.	Null
IPv4 Source Address	IP address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field.	Null
Protocol	Select from “TCP”, “UDP”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

Traffic Rules

This window allows you to view the traffic rules.

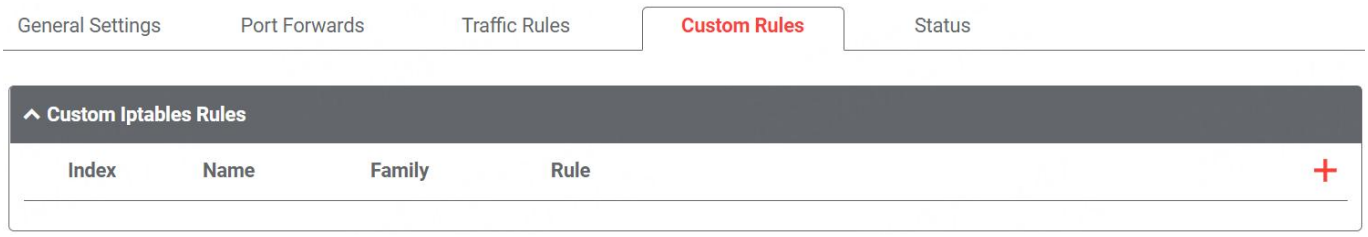
Click + to add one. The maximum count is **50.**



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	The name of the rule.	Null
Address family	Select from “IPv4”, “IPv6” or “IPv4-IPv6” as your application required.	IPv4-IPv6
Protocol	Select from “TCP”, “UDP” or “TCP-UDP” as your application required.	TCP-UDP

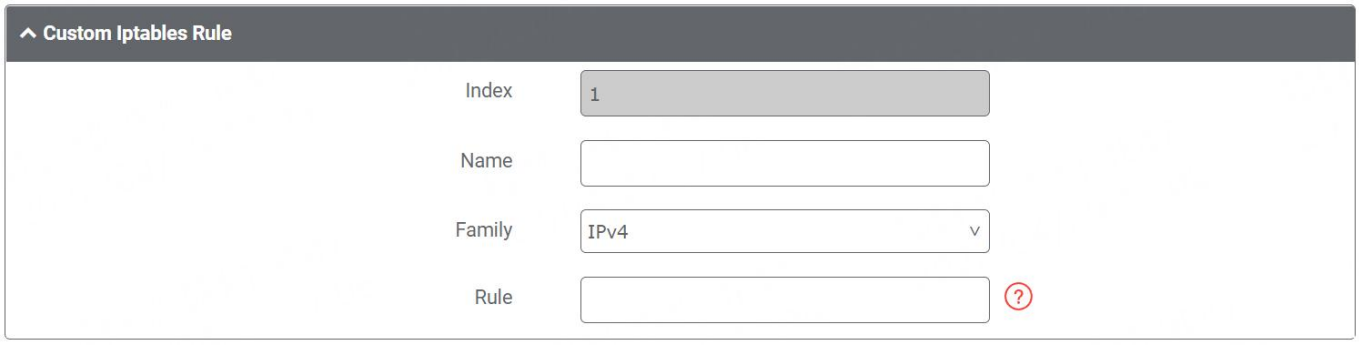
Item	Description	Default
Source zone	The zone to which the third party will be connecting.	device_output
IPv4 Source Address	The IPv4 address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field.	Null
IPv6 Source Address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

Custom Rules



This window allows you to view the custom rules.

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



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

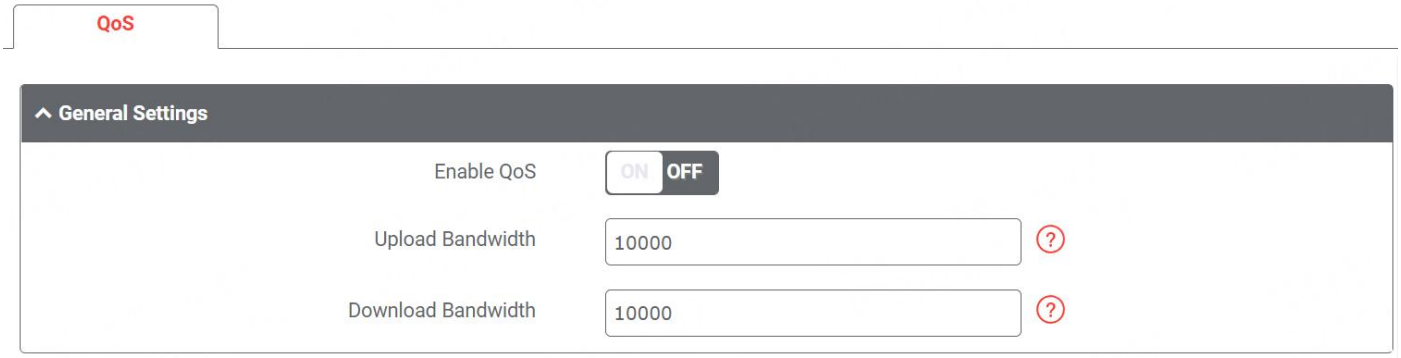
Status

This window allows you to view the status of firewall.

3.3.6 QoS

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

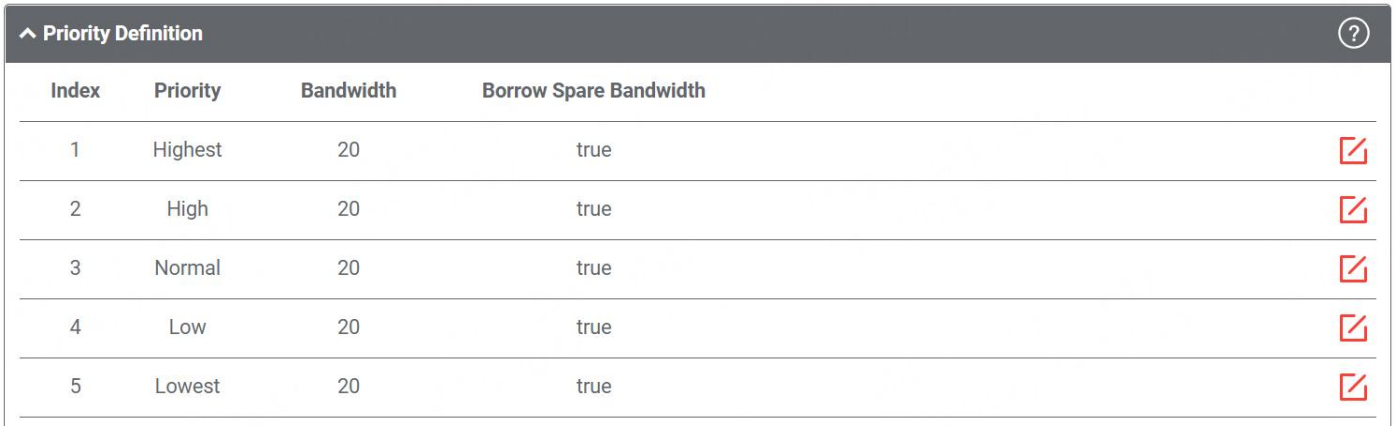
General Setting



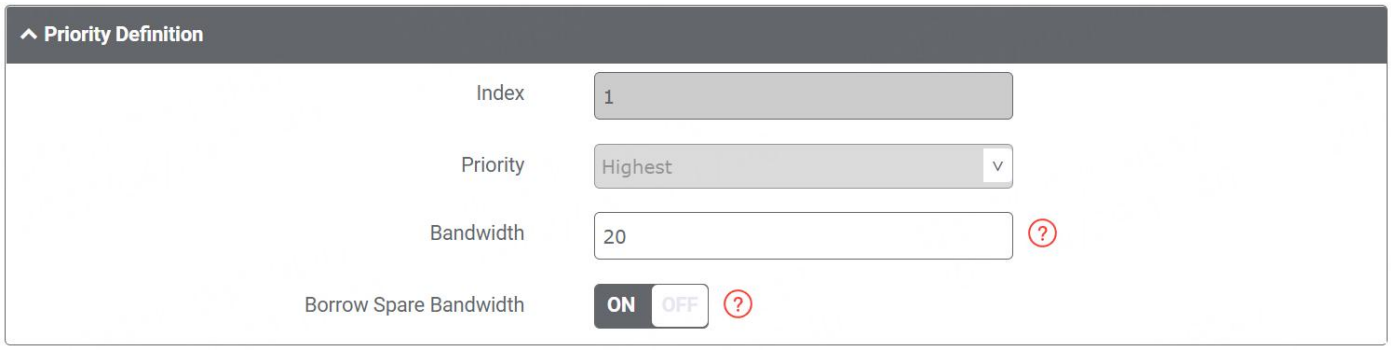
Item	Description	Default
Enable QoS	Click the toggle button to enable or disable.	OFF
Upload Bandwidth	Enter a value for the upload bandwidth, the unit is kbit.	10000

Item	Description	Default
Download Bandwidth	Enter a value for the download bandwidth, the unit is kbit.	10000

Priority Definition



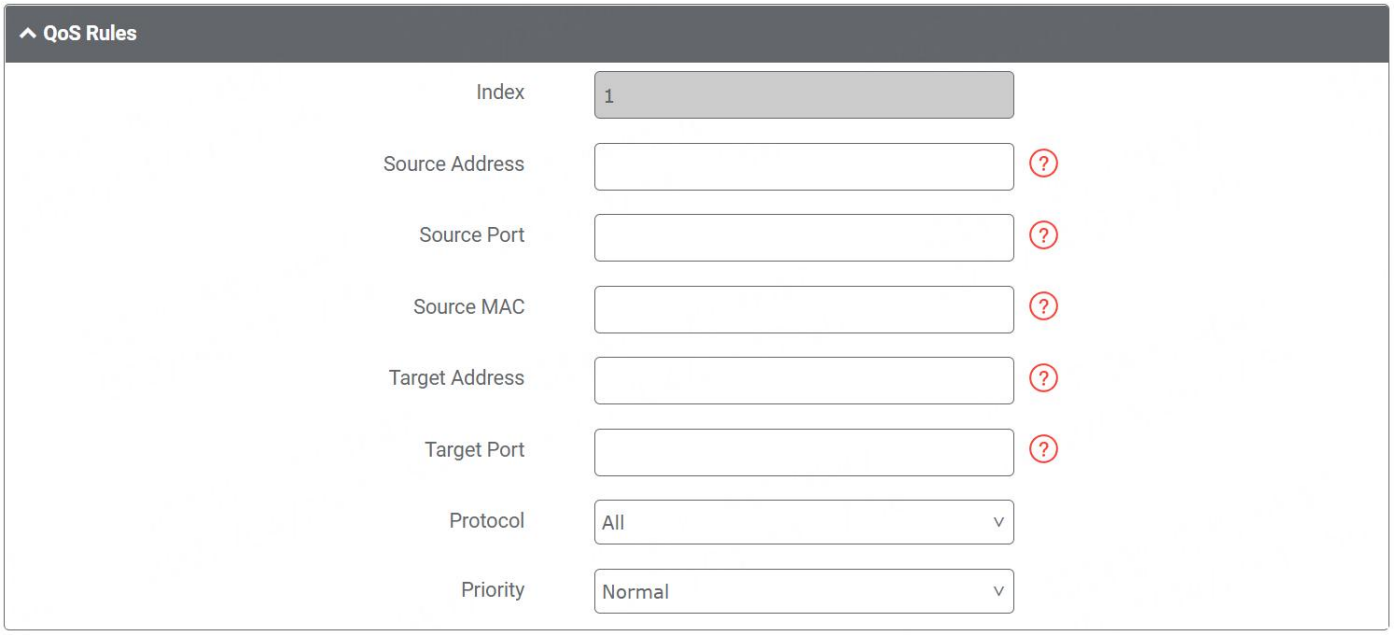
Click to set the priority.



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

IPv4 QoS Rules

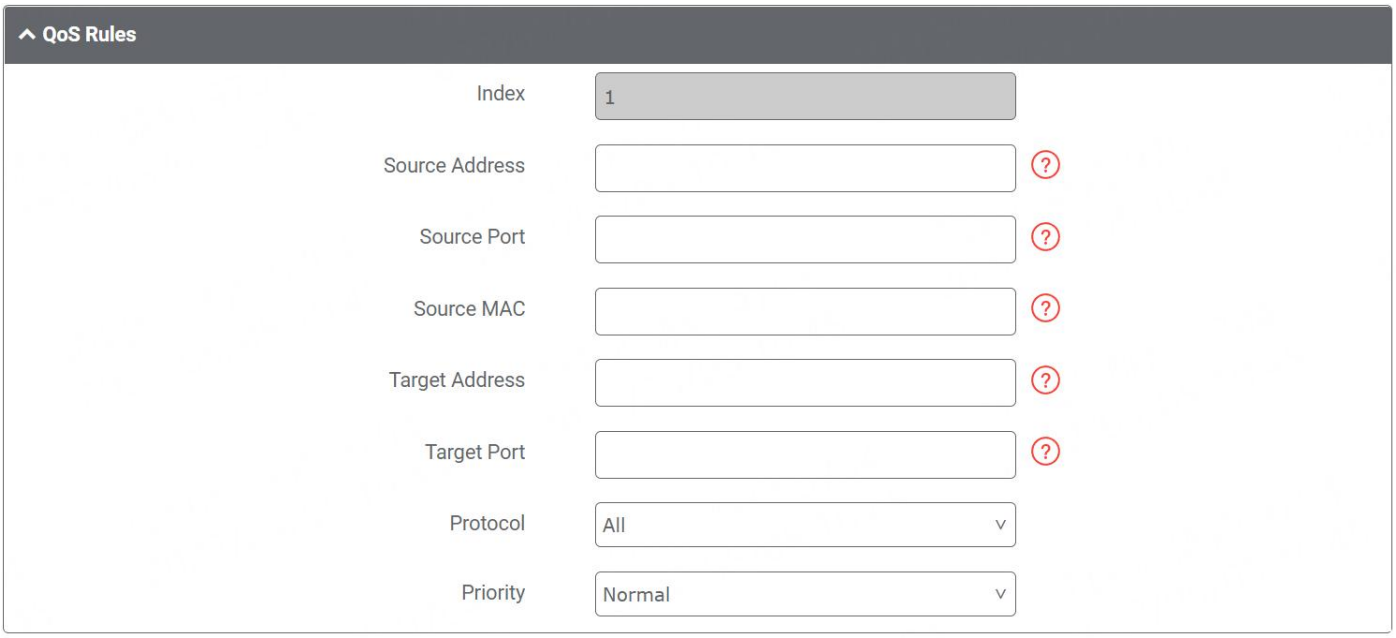
Click + to add one. The maximum count is **10.**



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

IPv6 QoS Rules

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



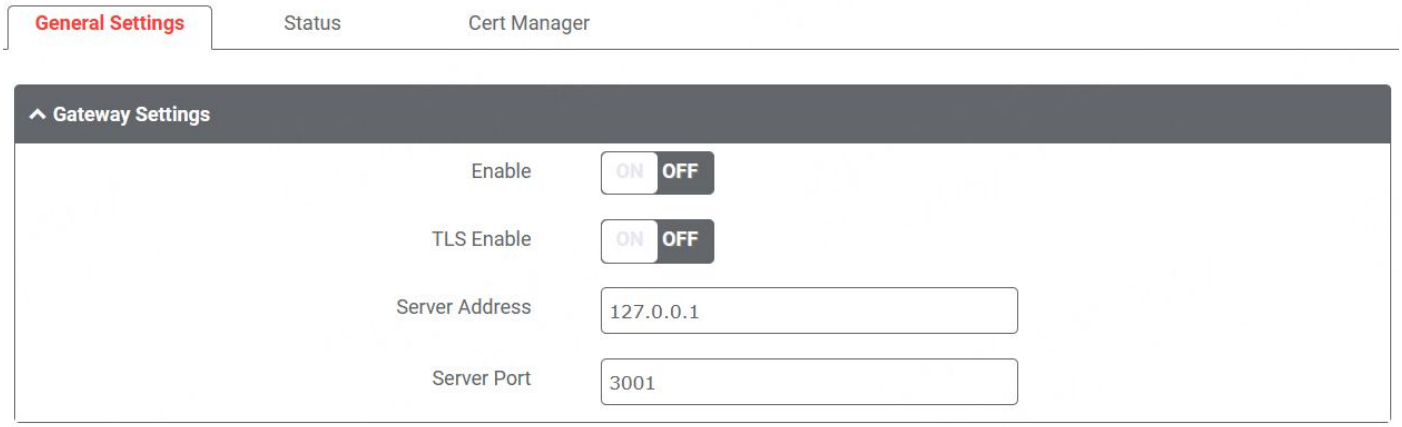
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Source Address	The address of Host(s) from which data will be transmitted.	Null
Source Port	The port of Host(s) from which data will be transmitted.	Null
Source MAC	The MAC address of Host(s) from which data will be transmitted.	Null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

3.4 Packet Forwarders (Supported in LG5100)

3.4.1 Basic Station

A LoRa Basic Station is a LoRaWAN device software implementation which provides this core functionality in terms of handling the packet flow, managing spectrum access and LNS backhaul connectivity, and more.

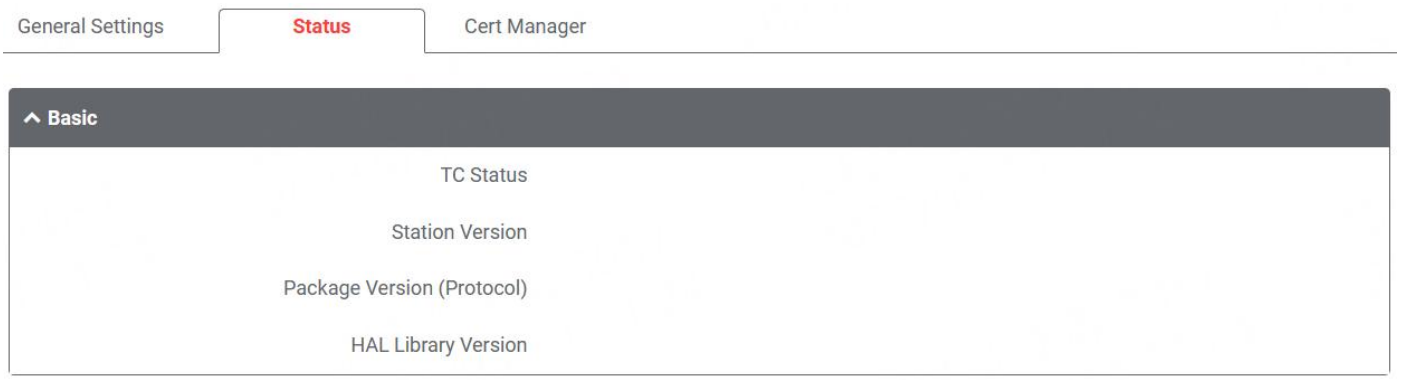
General Setting



Item	Description	Default
Enable	Enable application	OFF
TLS Enable	Enable TLS encrypted transmission	OFF
Server Address	Server address	127.0.0.1
Server Port	Server port	3001

Status

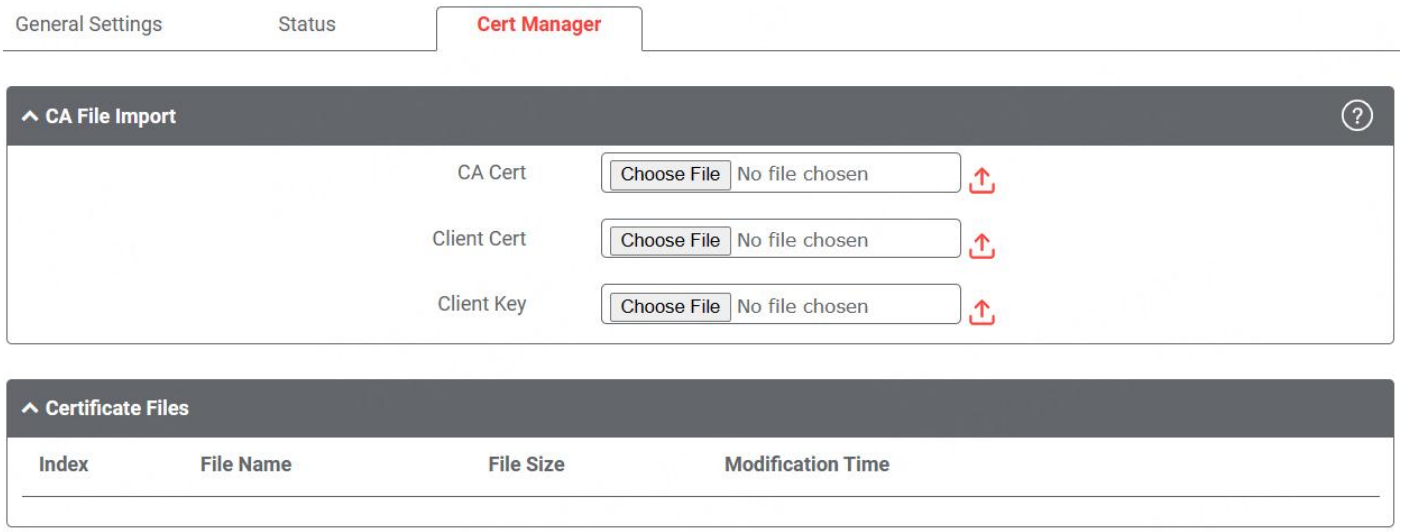
This section allows you to view the status of basic station.



Item	Description
TC Status	Platform connection status

Station Version	Application version
Package Version (Protocol)	Application package version
HAL Library Version	LoRaWAN HAL library version

Cert Manager



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

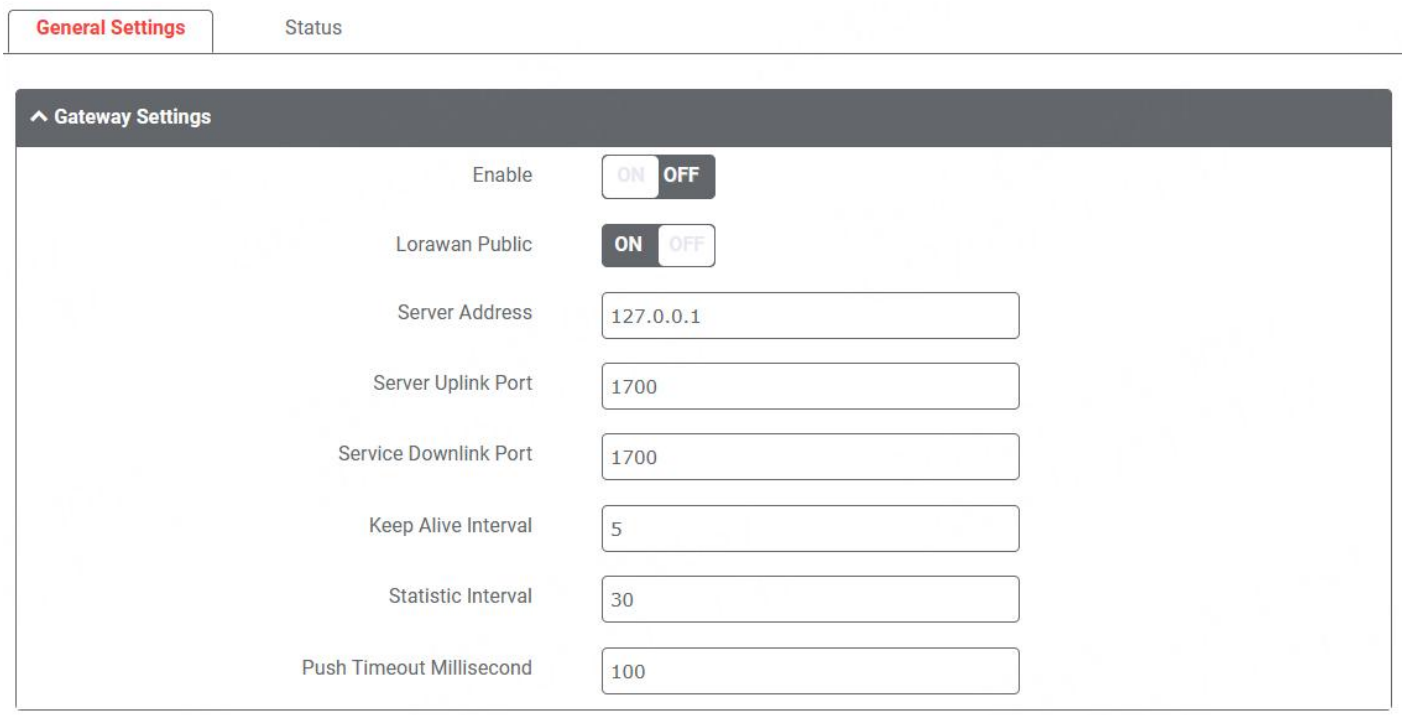
3.4.2 UDP Forwarder

A Packet Forwarder is a program running on a device, that interacts:

(1) With the LoRa chip, to receive and transmits LoRa packets;

(2) With the network, to transmit them for applications.

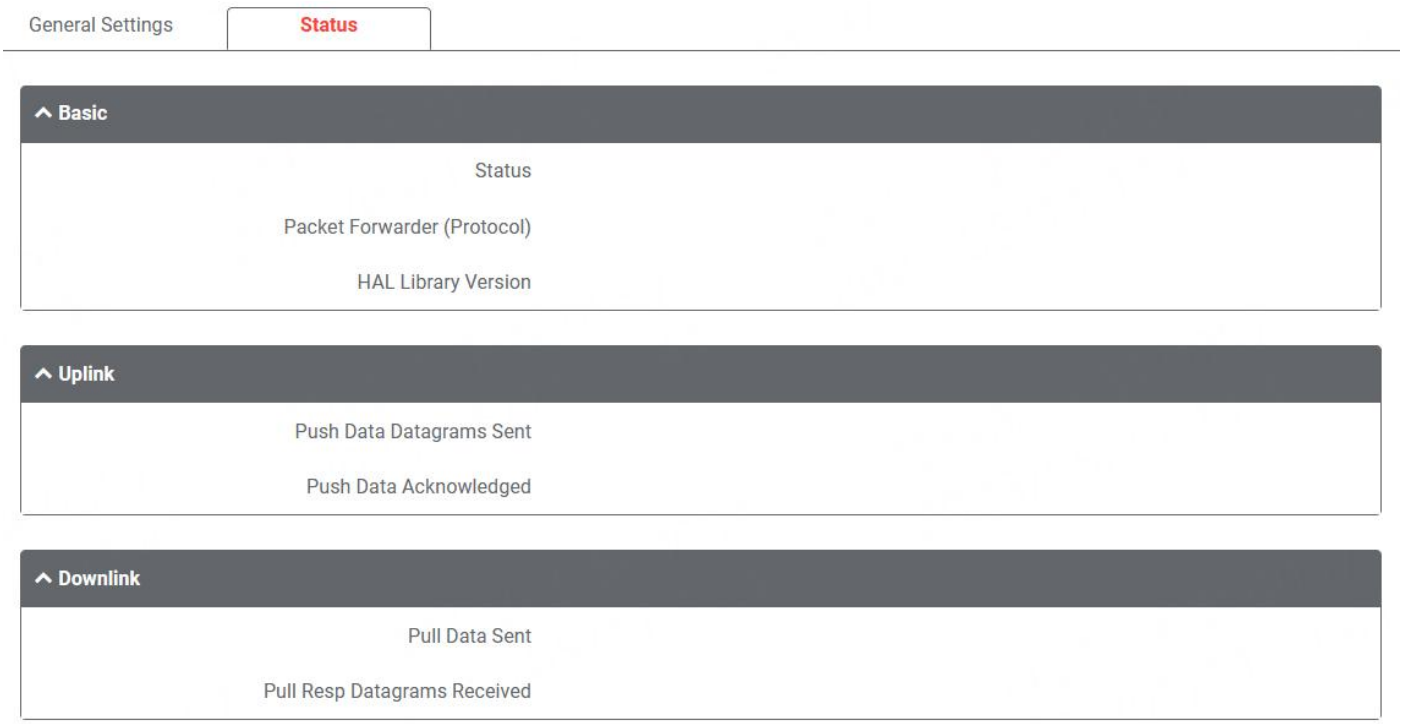
General Setting



Item	Description	Default
Enable	Click the toggle button to enable or disable the function.	OFF
Lorawan Public	Click the toggle button to enable or disable the function.	ON
Server Address	Set the LoRaWAN network server address.	127.0.0.1
Server Uplink Port	Set the uplink port to LoRaWAN network server	1700
Server Downlink Port	Set the downlink port to LoRaWAN network server.	1700
Keep Alive Interval	Time interval for obtaining downlink data.	5
Statistic Interval	Statistical interval, USI update interval.	30
Push Timeout Millisecond	Uplink data timeout.	100

Status

This section allows you to view the status of Packet forwarder.



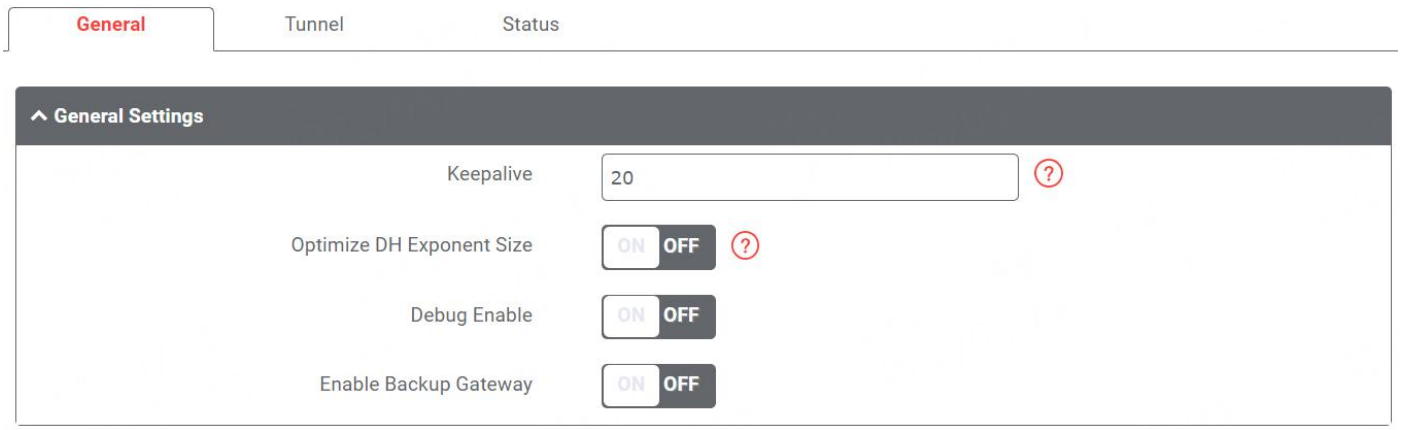
Status	
Item	**Description**
Basic	
Status	Show LoRaWAN status of your gateway.
Packet Forwarder (Protocol)	Show version of Packet forwarder.
HAL Library Version	Show driver version of LoRaWAN chipset inside gateway.
Uplink	
Push Data Datagrams Sent	Total quantity of packets sent from gateway to server, 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.

3.5 VPN

3.5.1 IPsec

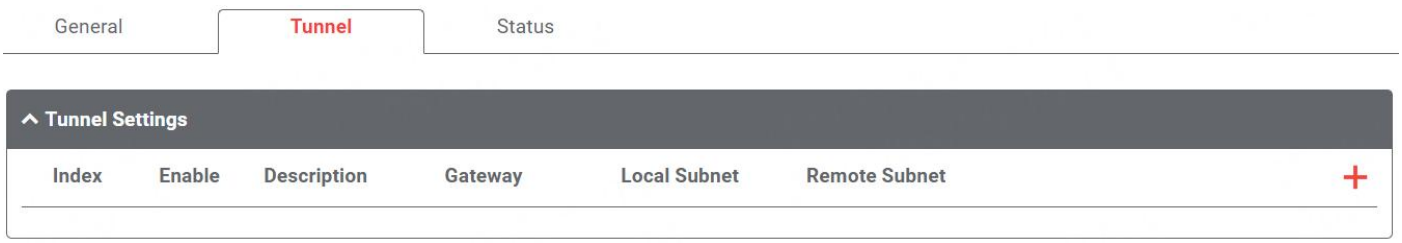
This section allows you to set the IPsec and the related parameters. Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session.

General



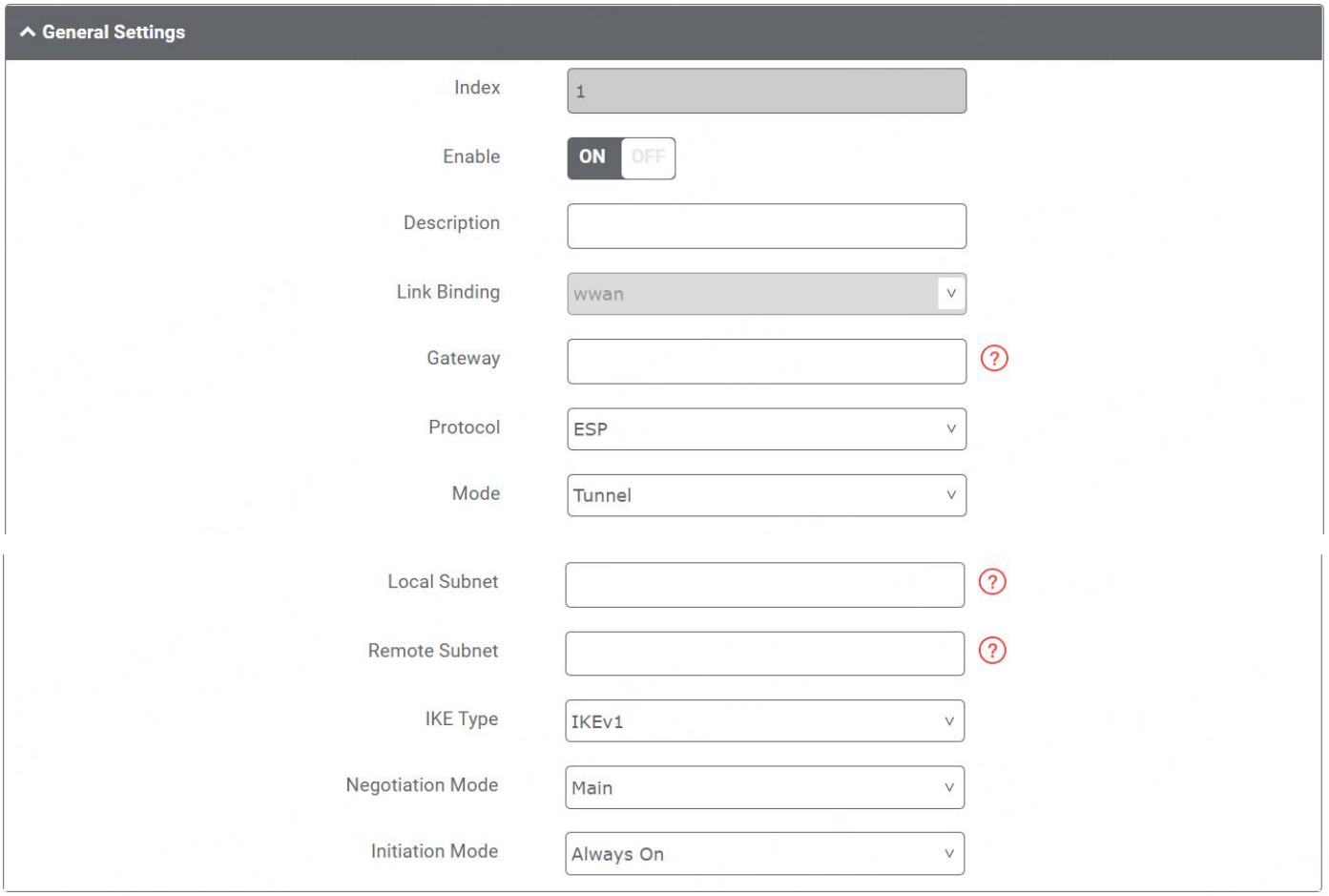
Item	Description	Default
Keepalive	Set the time to live in seconds. The router sends keep-alive packets to the NAT (Network Address Translation) server at regular intervals to prevent the records on the NAT table from disappearing.	20
Optimize DH Size	Click the toggle button to enable/disable this option.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

Tunnel



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

General Setting



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

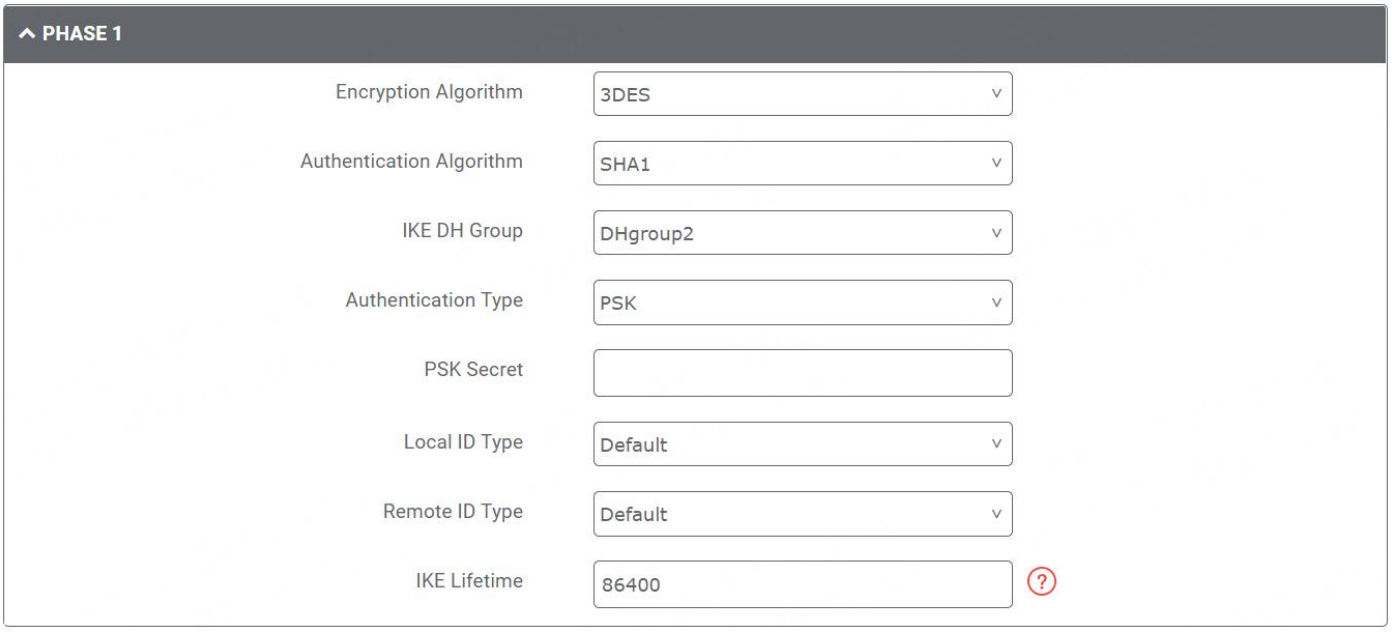
	• ESP: Use the ESP protocol • AH: Use the AH protocol	
Local Subnet	Enter the local subnet's address with mask protected by IPsec, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g. 10.8.0.0/24	Null
IKE Type	Select from "IKEv1" and "IKEv2".	IKEv1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

Advanced Setting

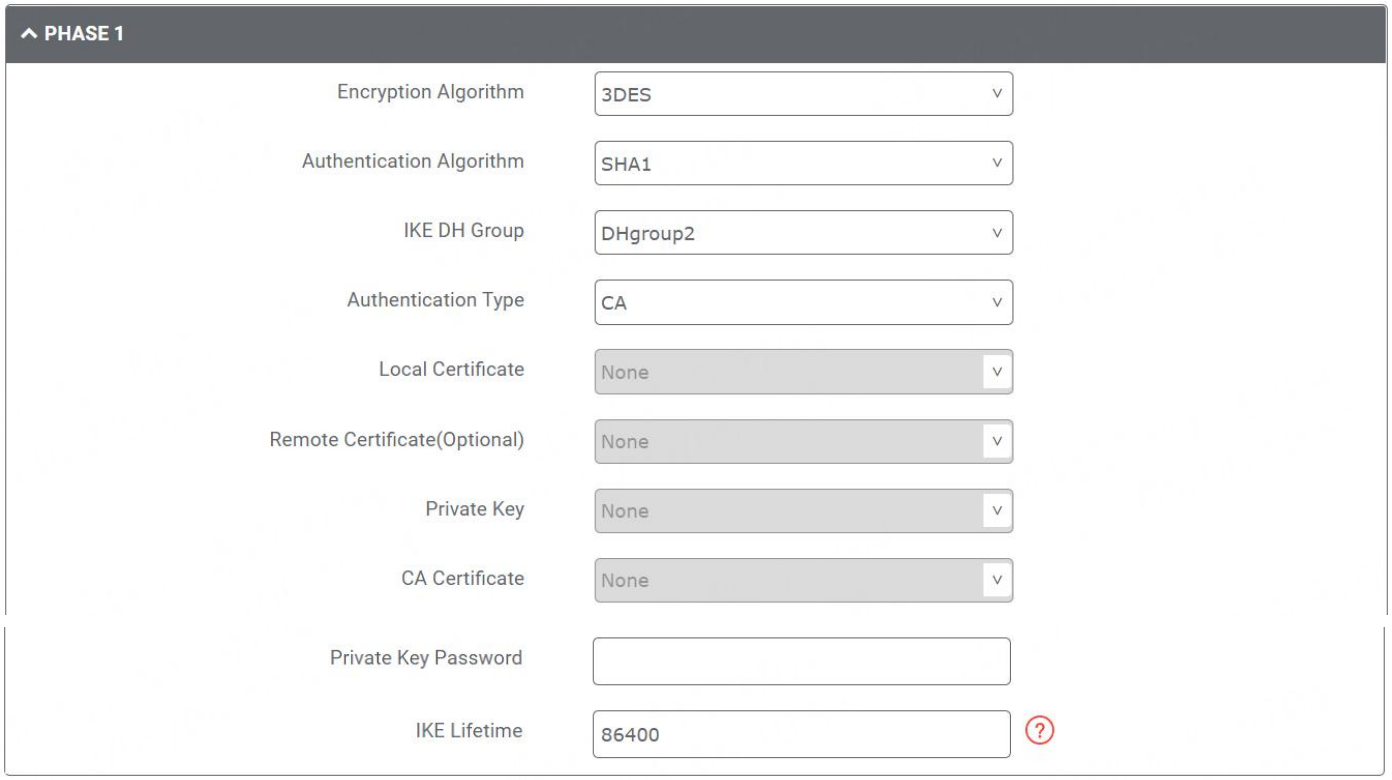
Item	Description	Default
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Enable Forceencaps	Force UDP encapsulation for ESP packets even if no NAT situation is detected.This may help to surmount restrictive firewalls.	OFF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

PHASE 1

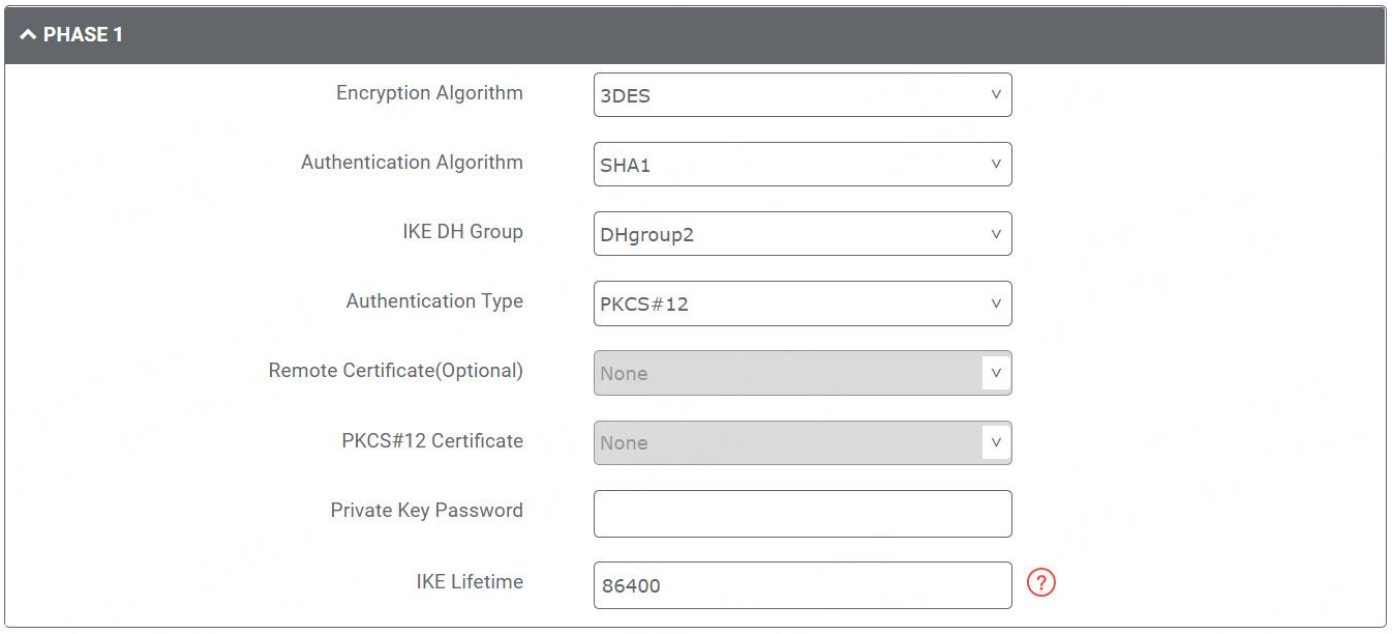
The window is displayed as below when choosing "PSK" as the authentication type.



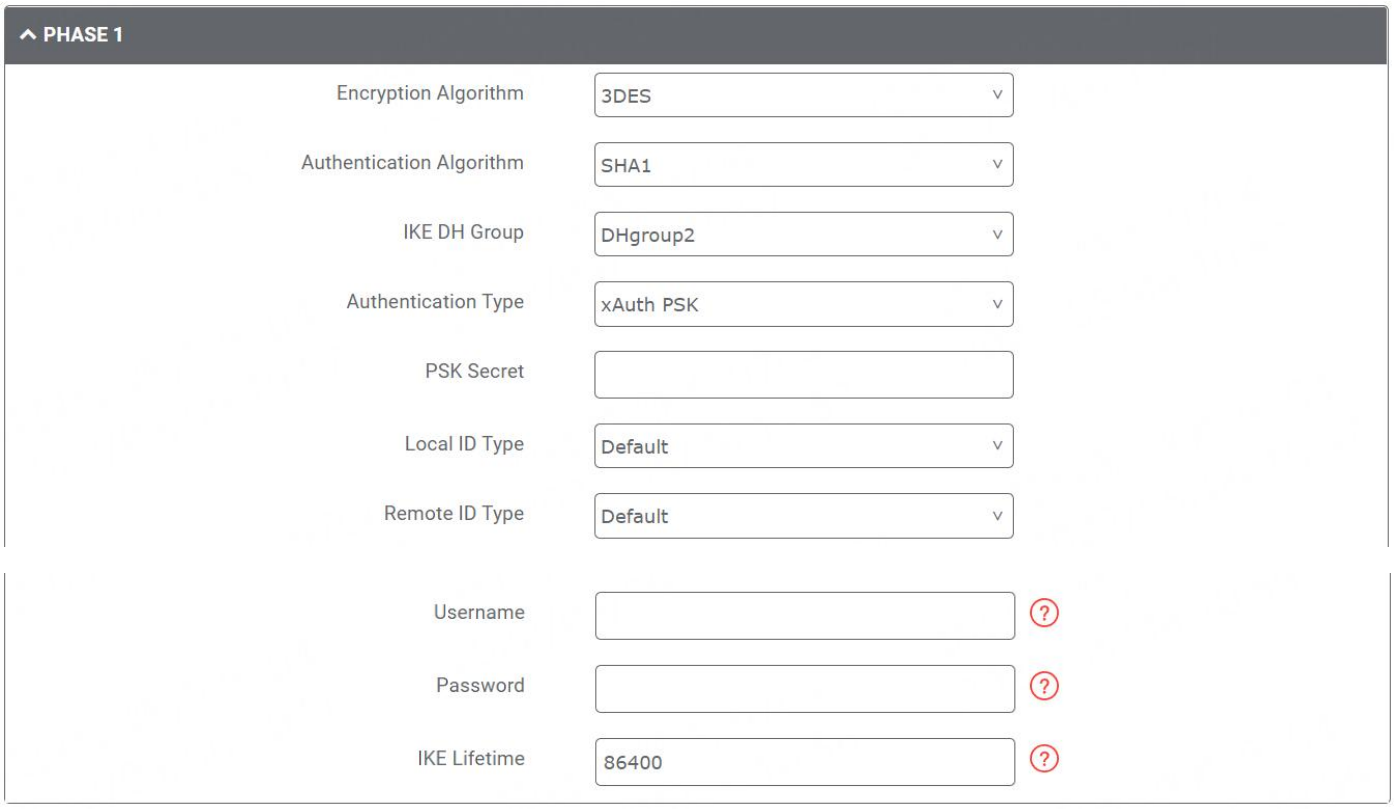
The window is displayed as below when choosing “CA” as the authentication type.



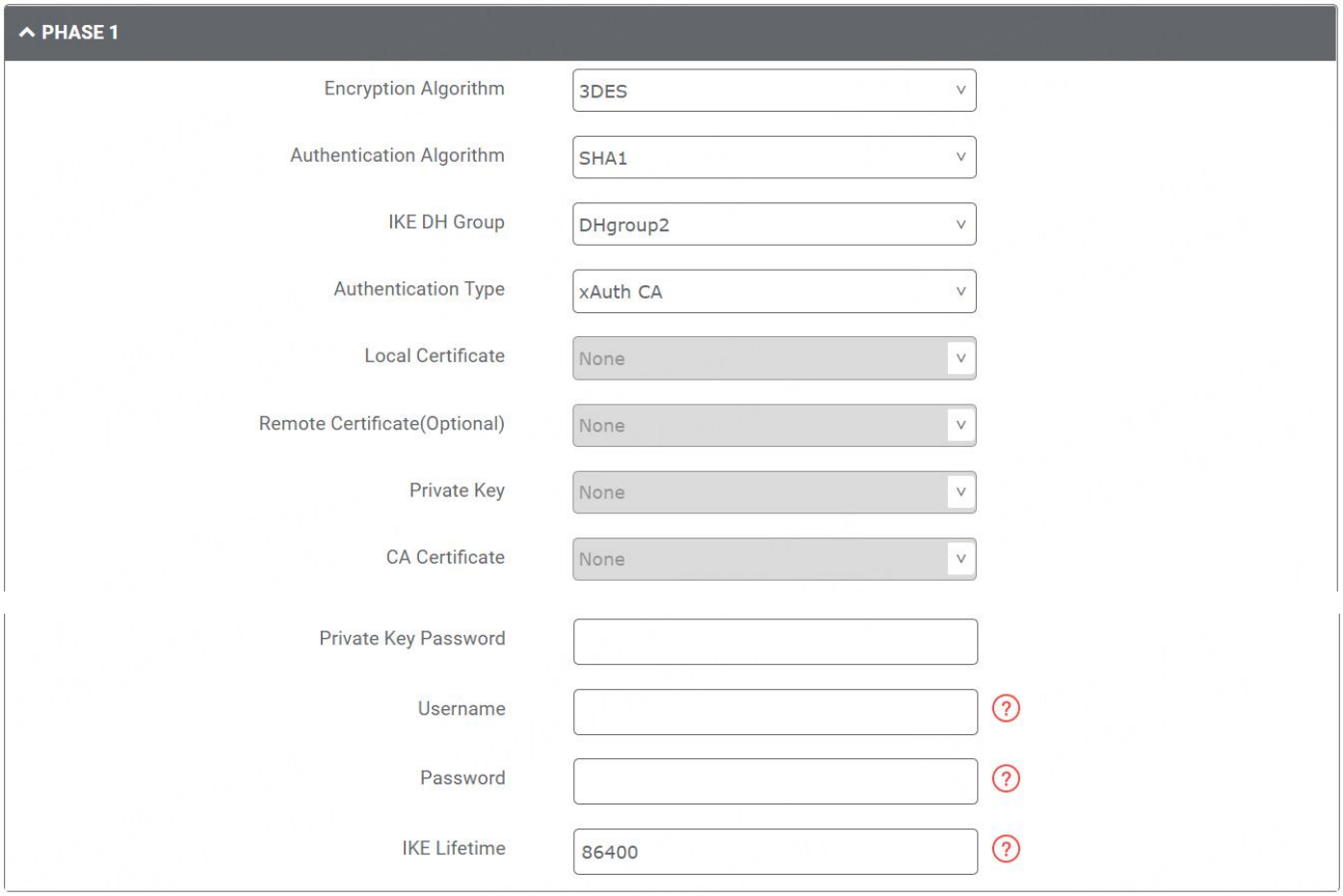
The window is displayed as below when choosing “PKCS#12” as the authentication type.



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



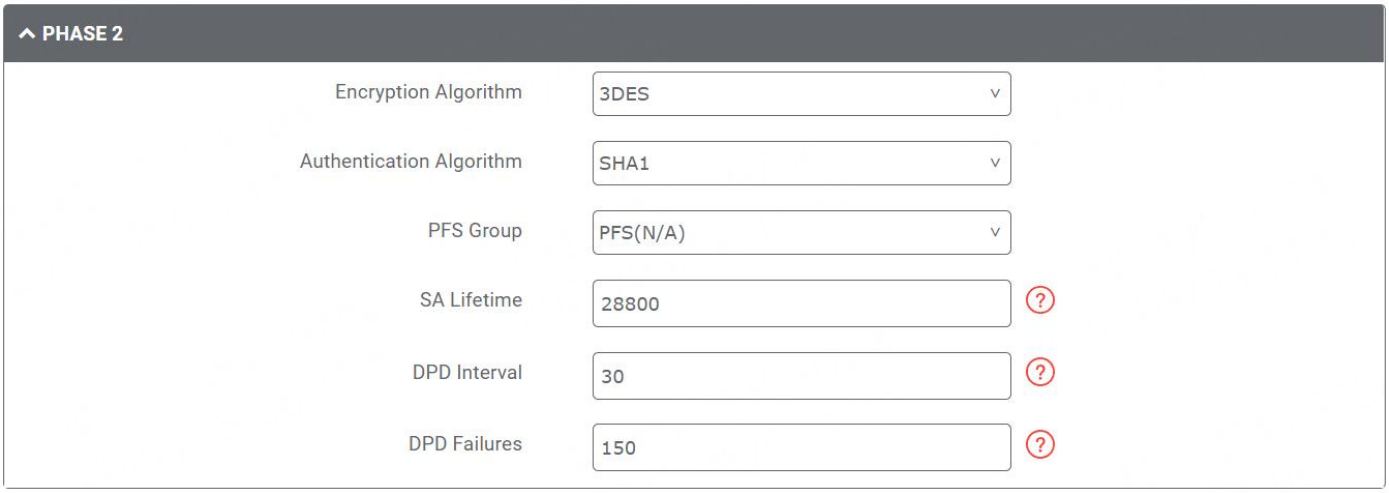
The window is displayed as below when choosing “xAuth CA” as the authentication type.



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

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

PHASE 2



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

Item	Description	Default
	"DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in SA negotiation.	
SA Lifetime	Set the IPsec SA lifetime. When negotiating to set up IPsec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is a Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	30
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	150

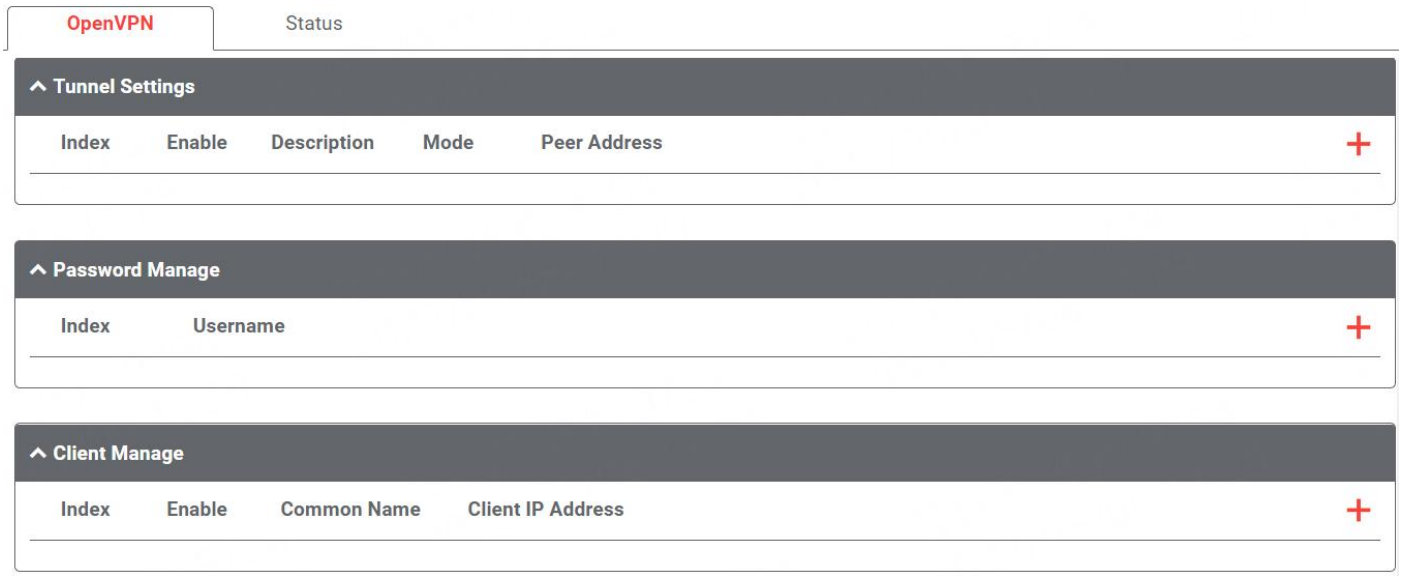
Status

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

3.5.2 OpenVPN

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

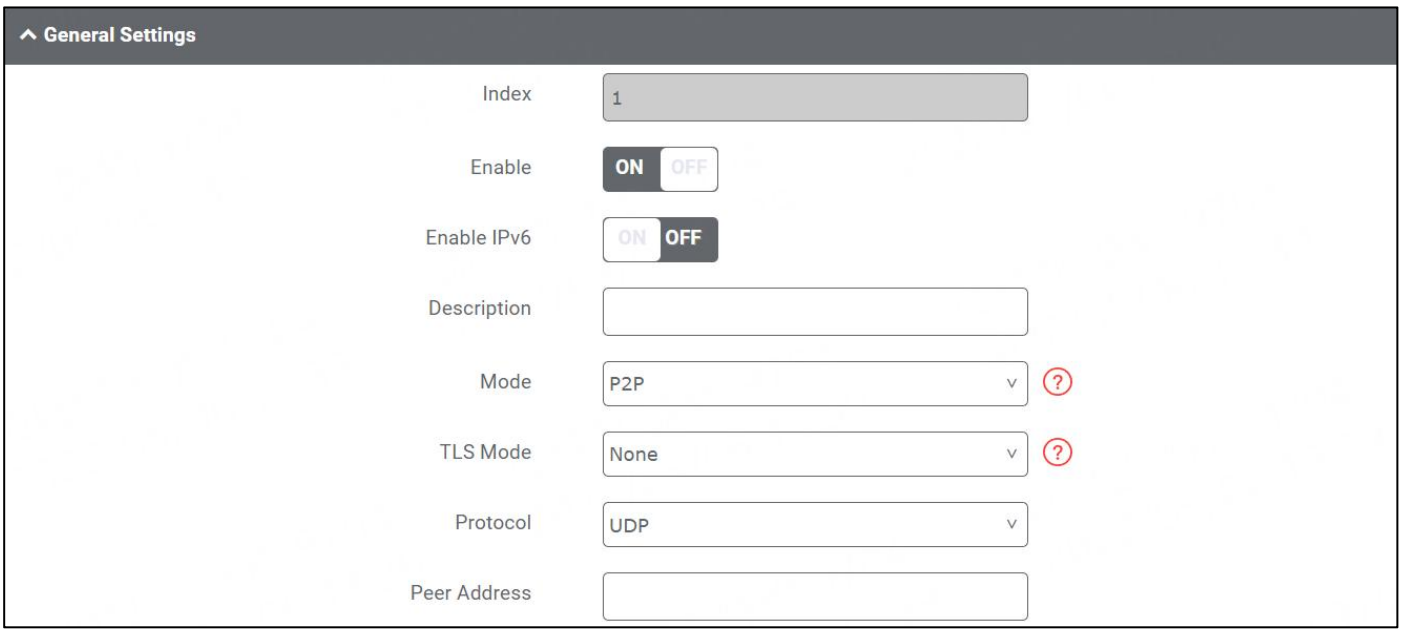
OpenVPN

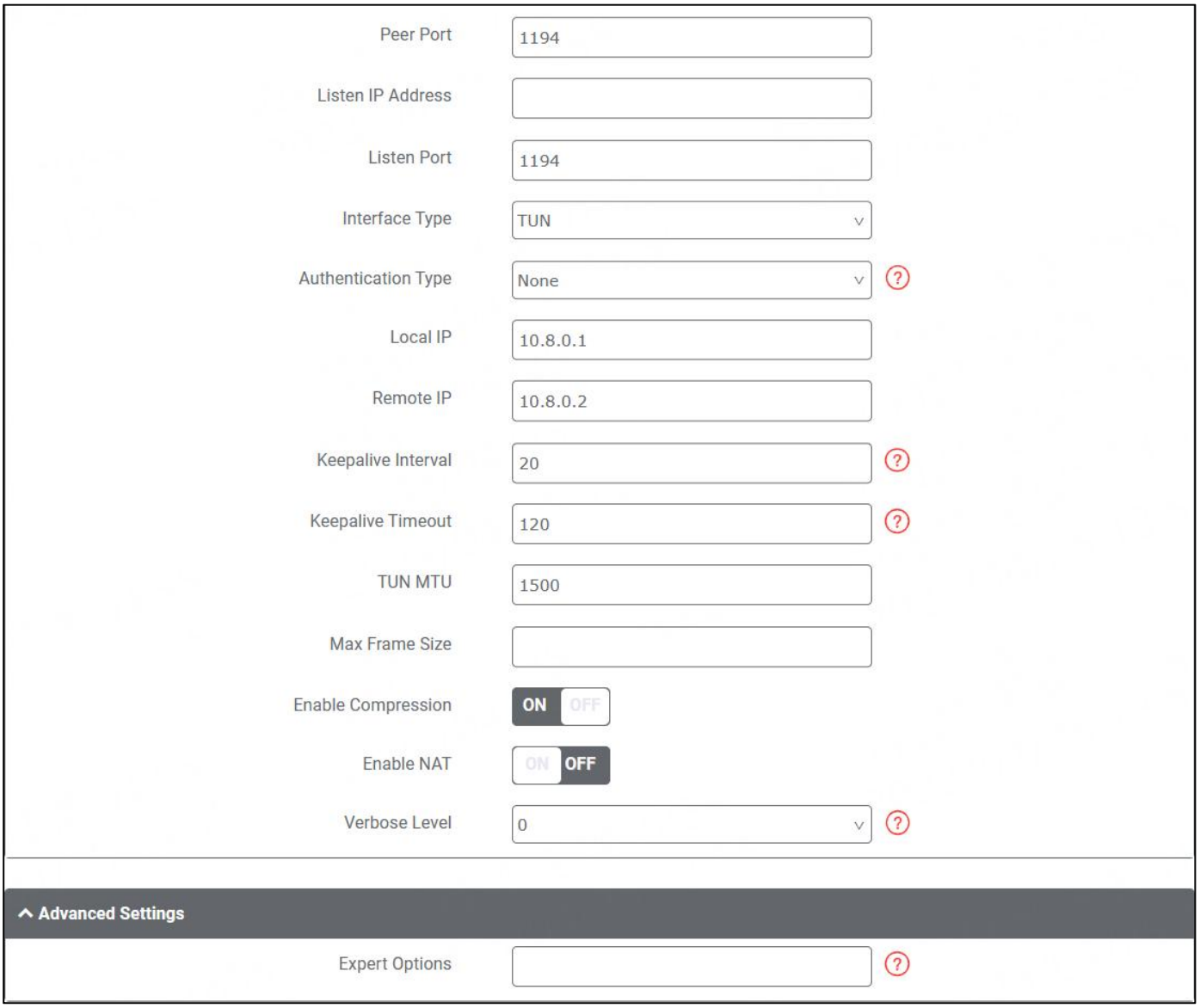


Tunnel Setting

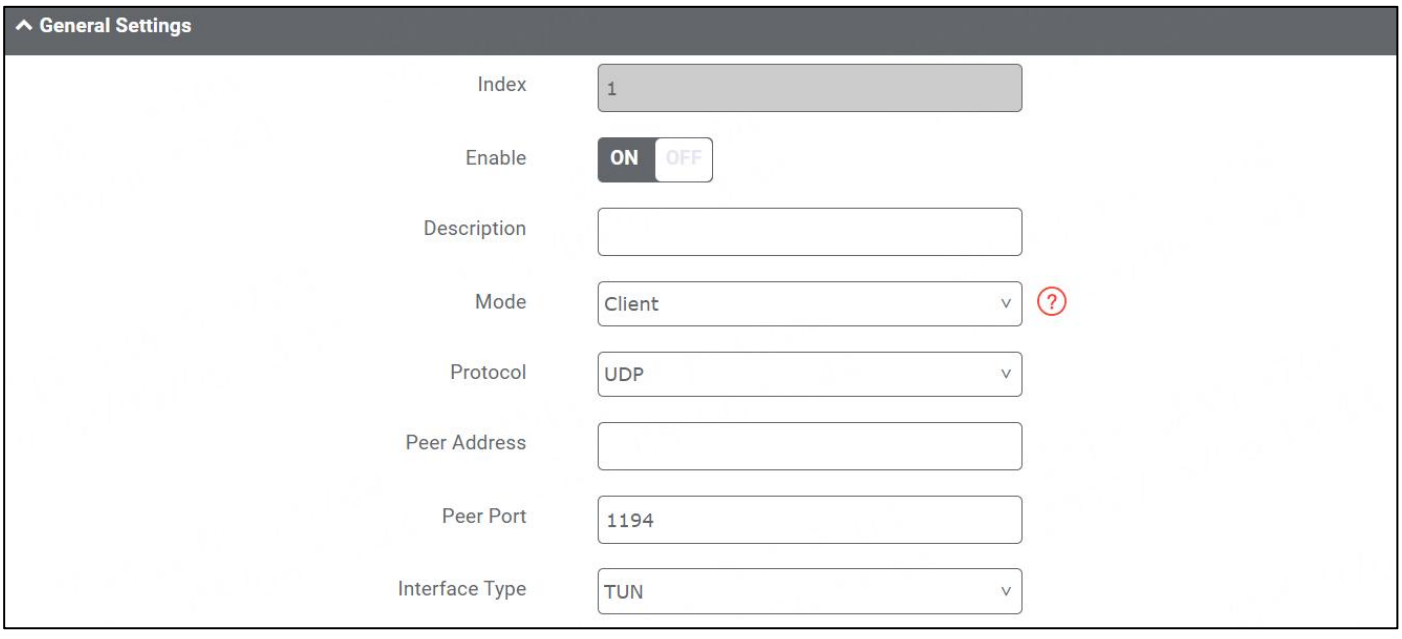
Click + to add an OpenVPN tunnel settings. The maximum count is 5. The configure page might vary when choosing different mode, and the **Authentication Type** might be fixed for using on specific mode.

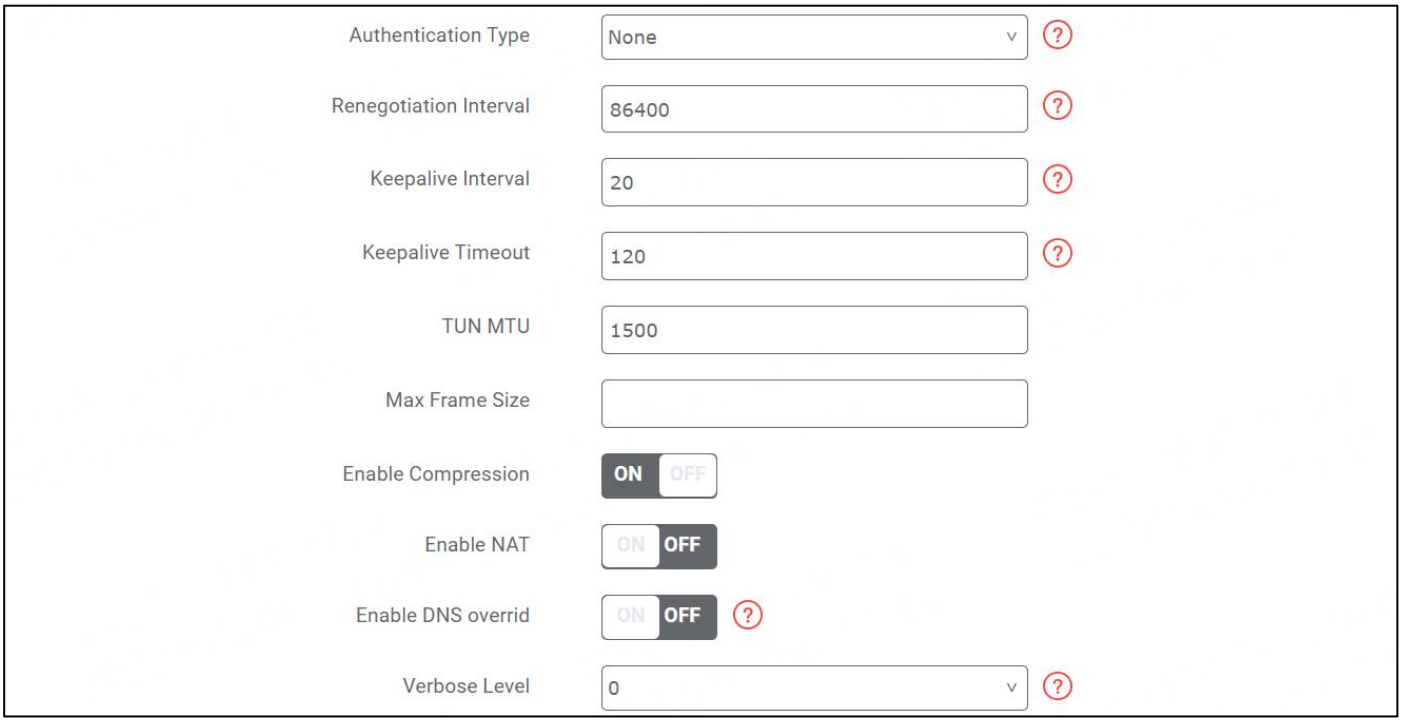
By default, the mode is “P2P”. The window is displayed as below when choosing “P2P” as the mode.



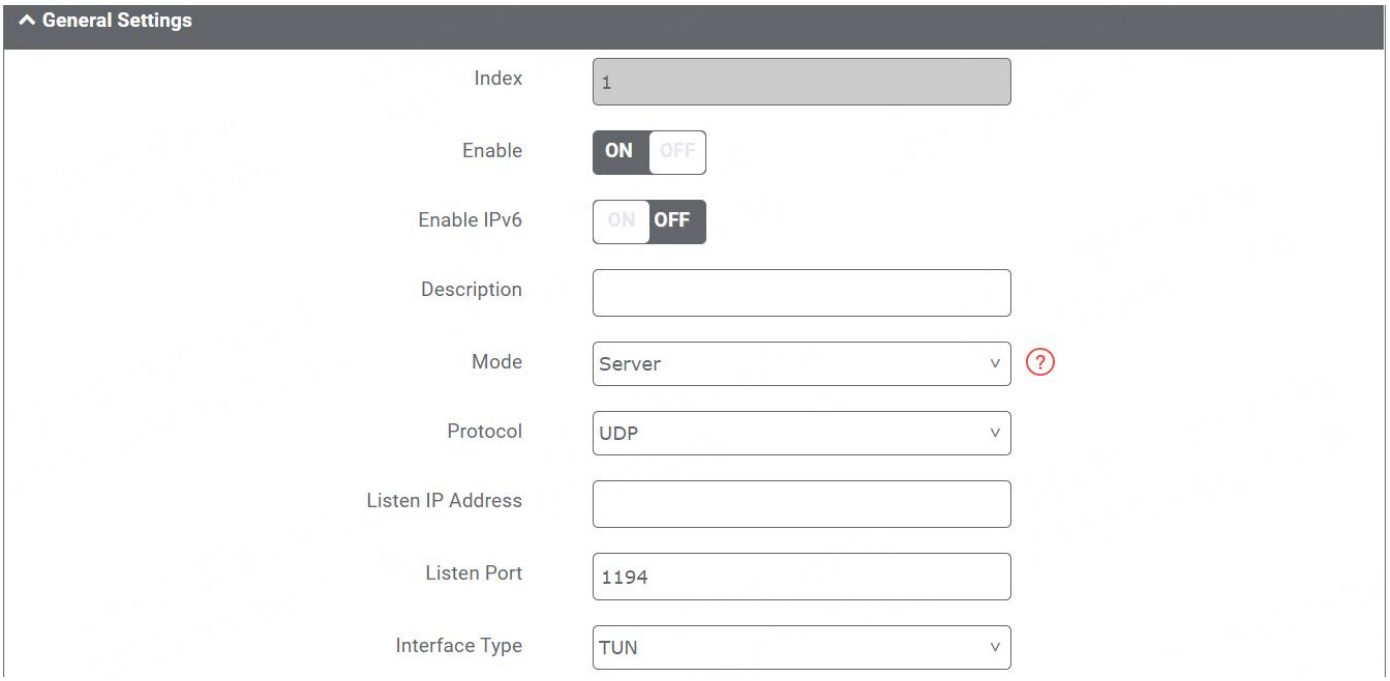


The window is displayed as below when choosing “Client” as the mode.



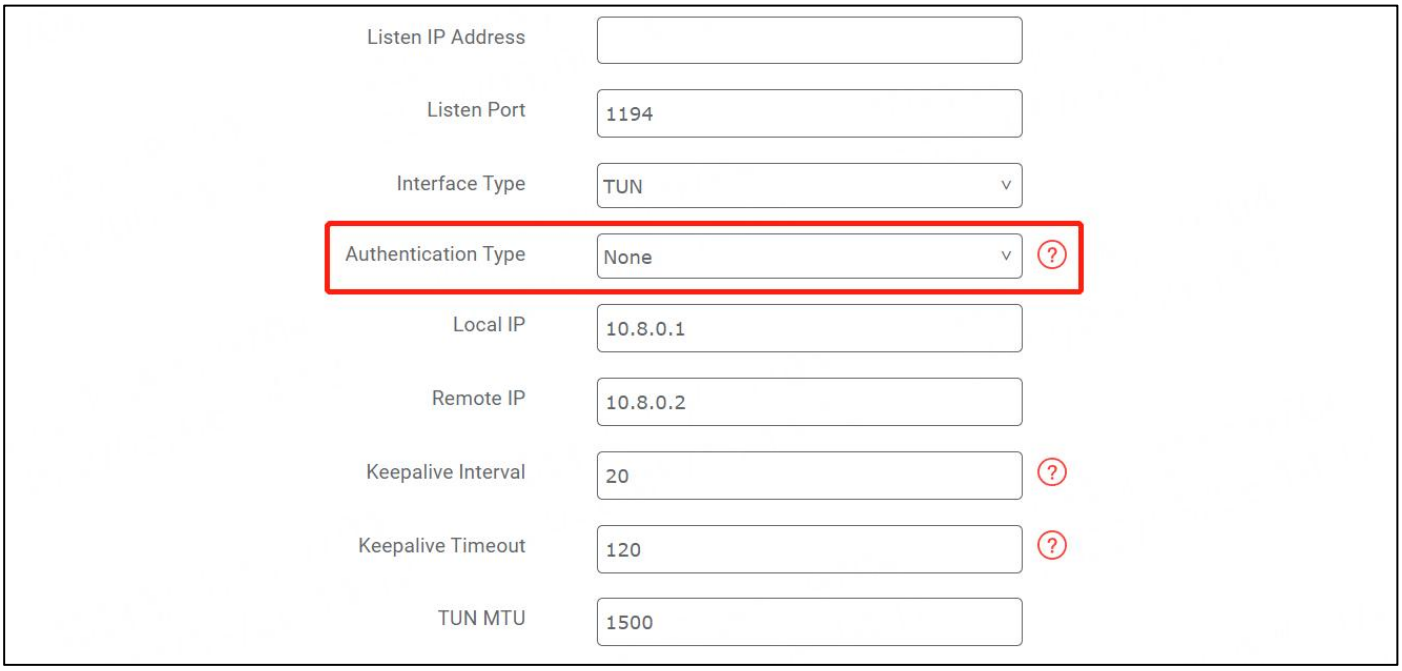


The window is displayed as below when choosing “Server” as the mode.

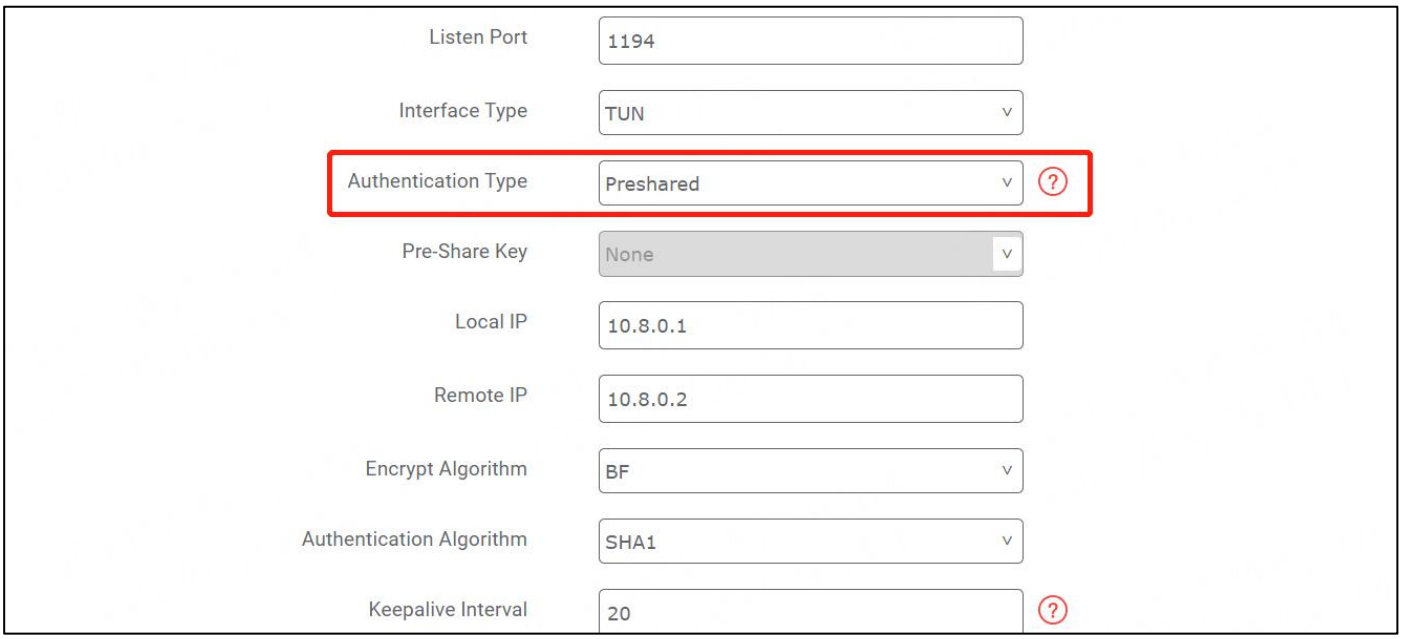


Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Enable IP Pool	OFF
Client Subnet	10.8.0.0
Client Subnet Netmask	255.255.255.0
Renegotiation Interval	86400
Max Clients	10
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable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

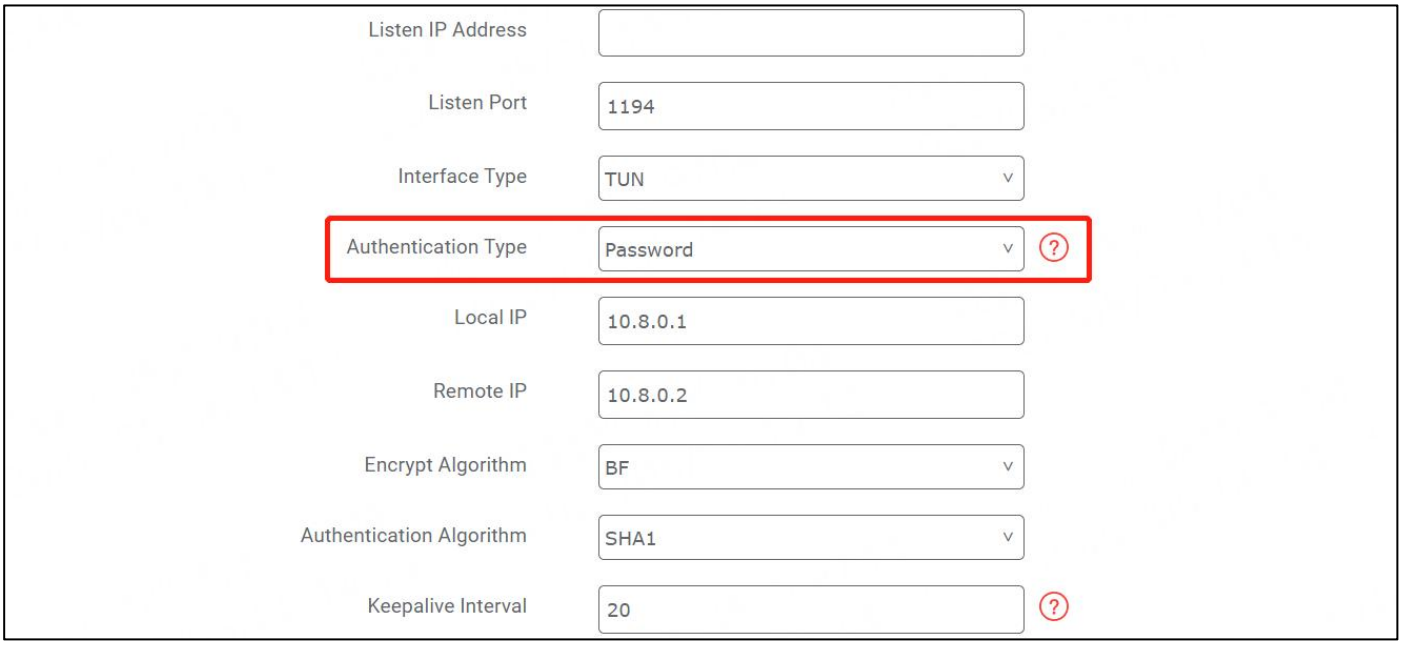
The window is displayed as below when choosing “None” as the authentication type.



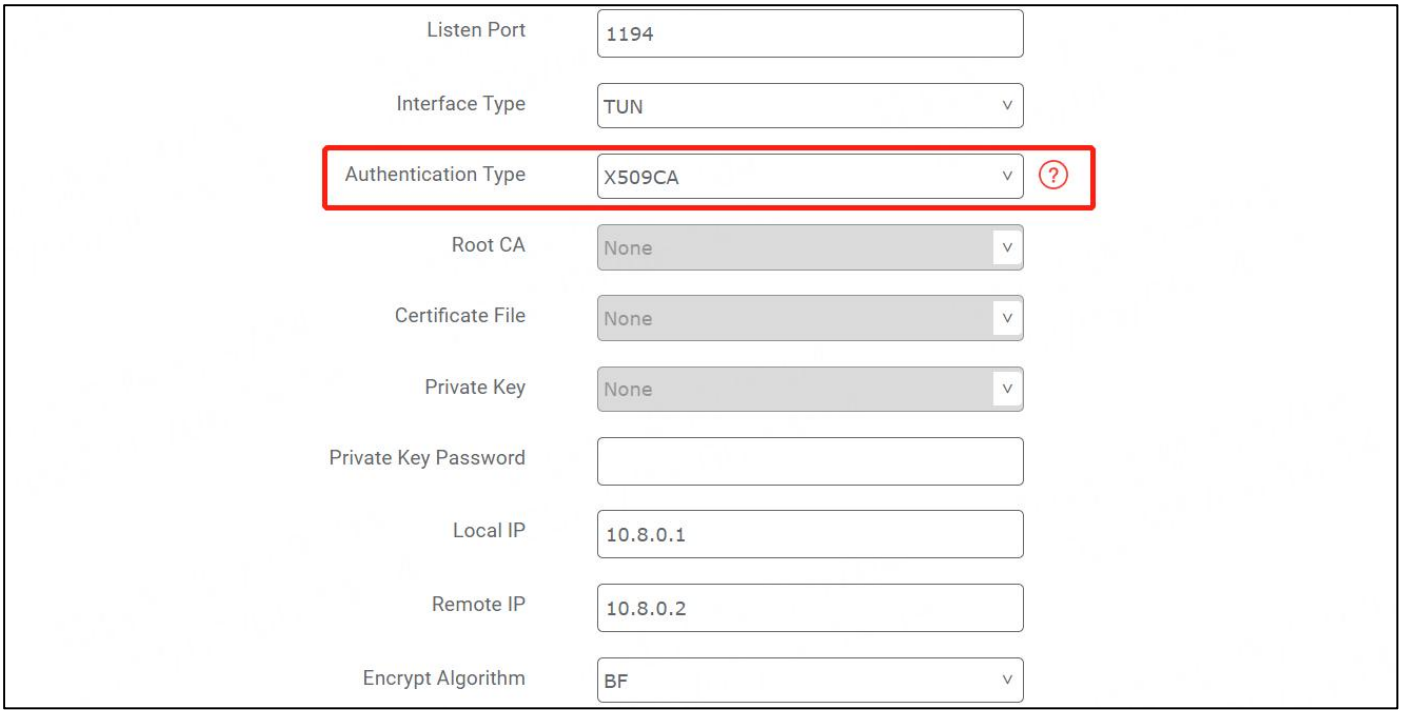
The window is displayed as below when choosing “Preshared” as the authentication type.



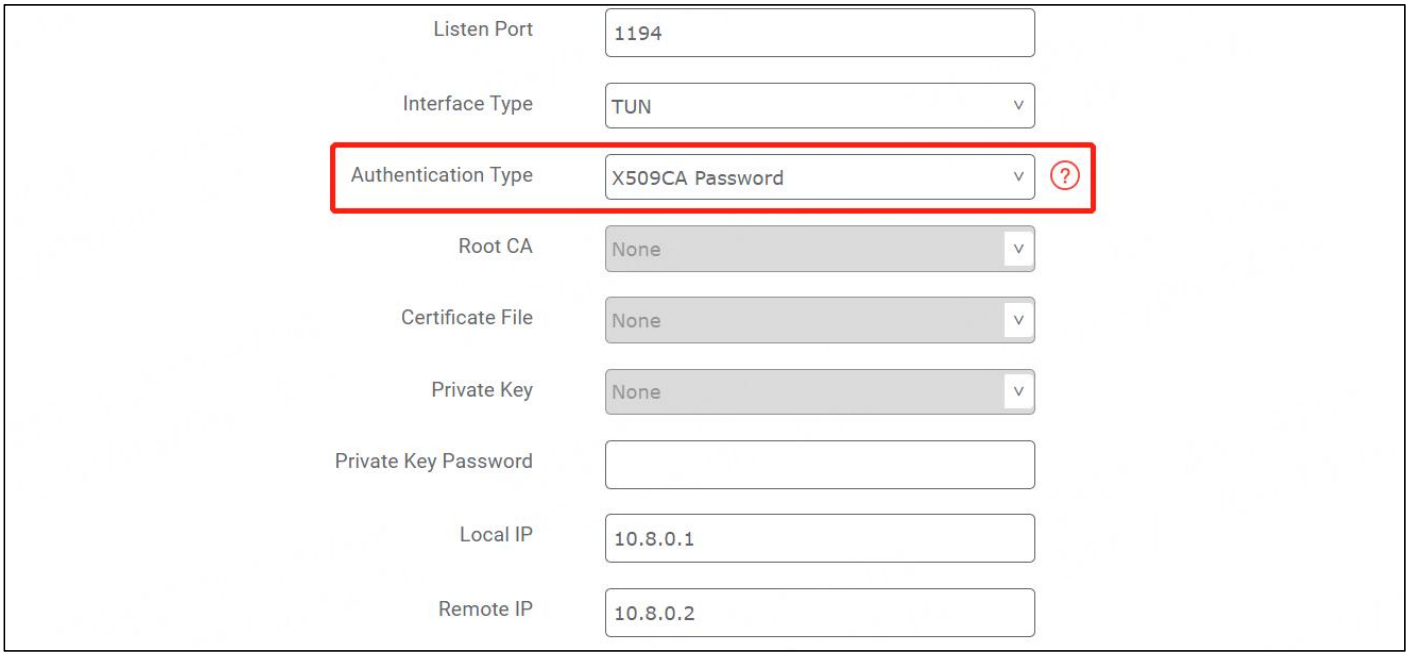
The window is displayed as below when choosing “Password” as the authentication type.



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

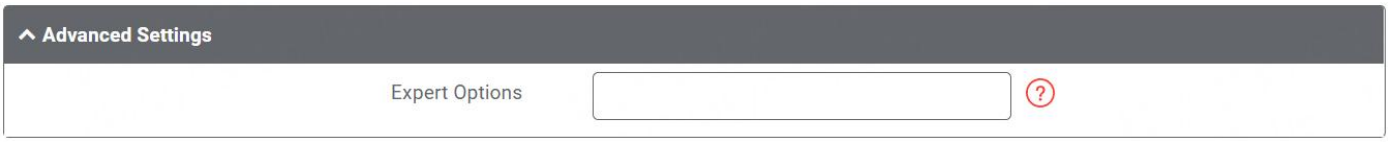


The window is displayed as below when choosing “X509CA Password” as the authentication type.



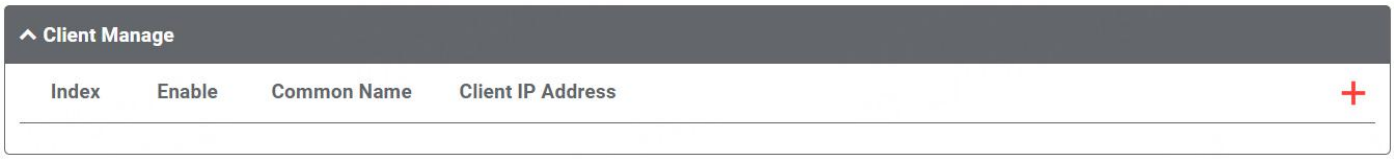
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Enable IPv6	Click the toggle button to enable/disable IPv6.	OFF
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “P2P”, “Client” or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

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



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

Client Management

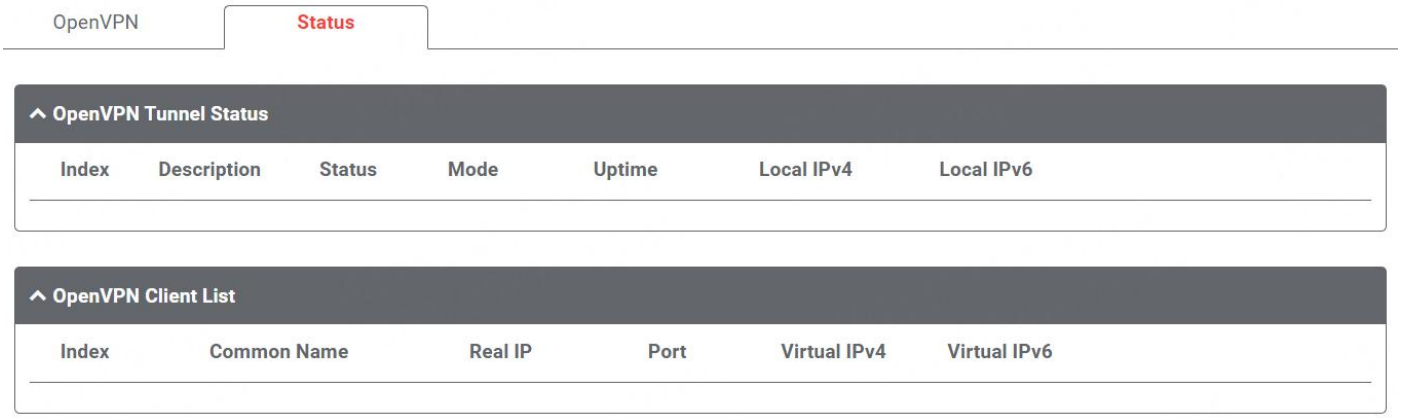


Click + to add client information. The maximum count is **20.**

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

Status

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

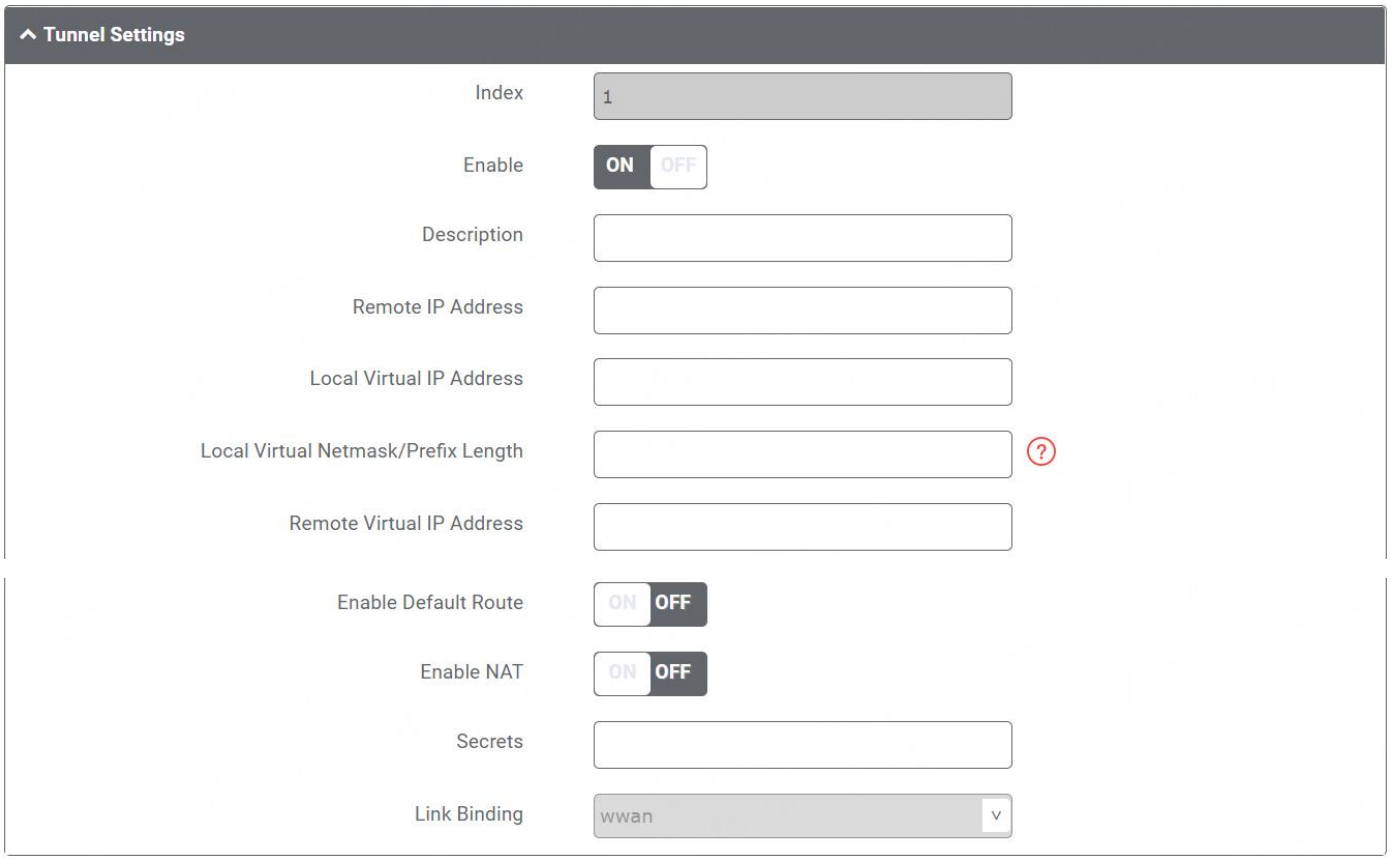


3.5.3 GRE

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

GRE

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

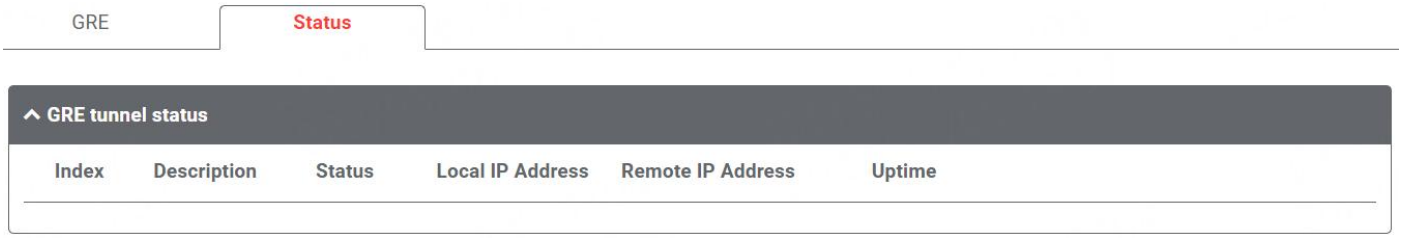


Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel. GRE (Generic Routing Encapsulation) is a protocol that encapsulates data packets so that it can route packets of other protocols in an IP network.	ON
Description	Enter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

Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when router under NAT environment.	OFF
Secrets	Set the key of the GRE tunnel.	Null
Link Binding	Set the specified interface of the GRE Tunnel	wwan

Status

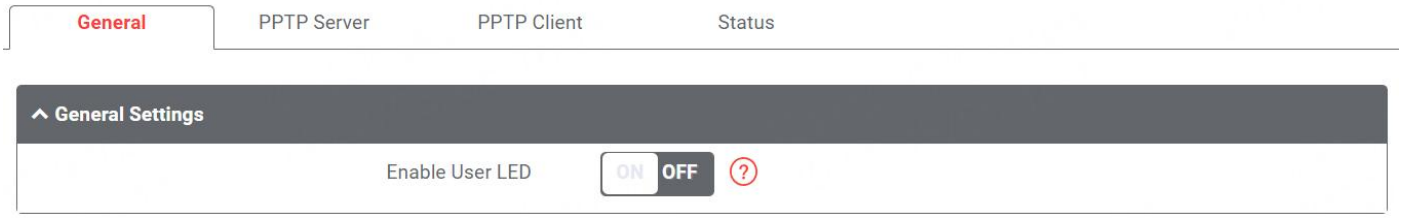
This section allows you to view the GRE tunnel status.



3.5.4 PPTP

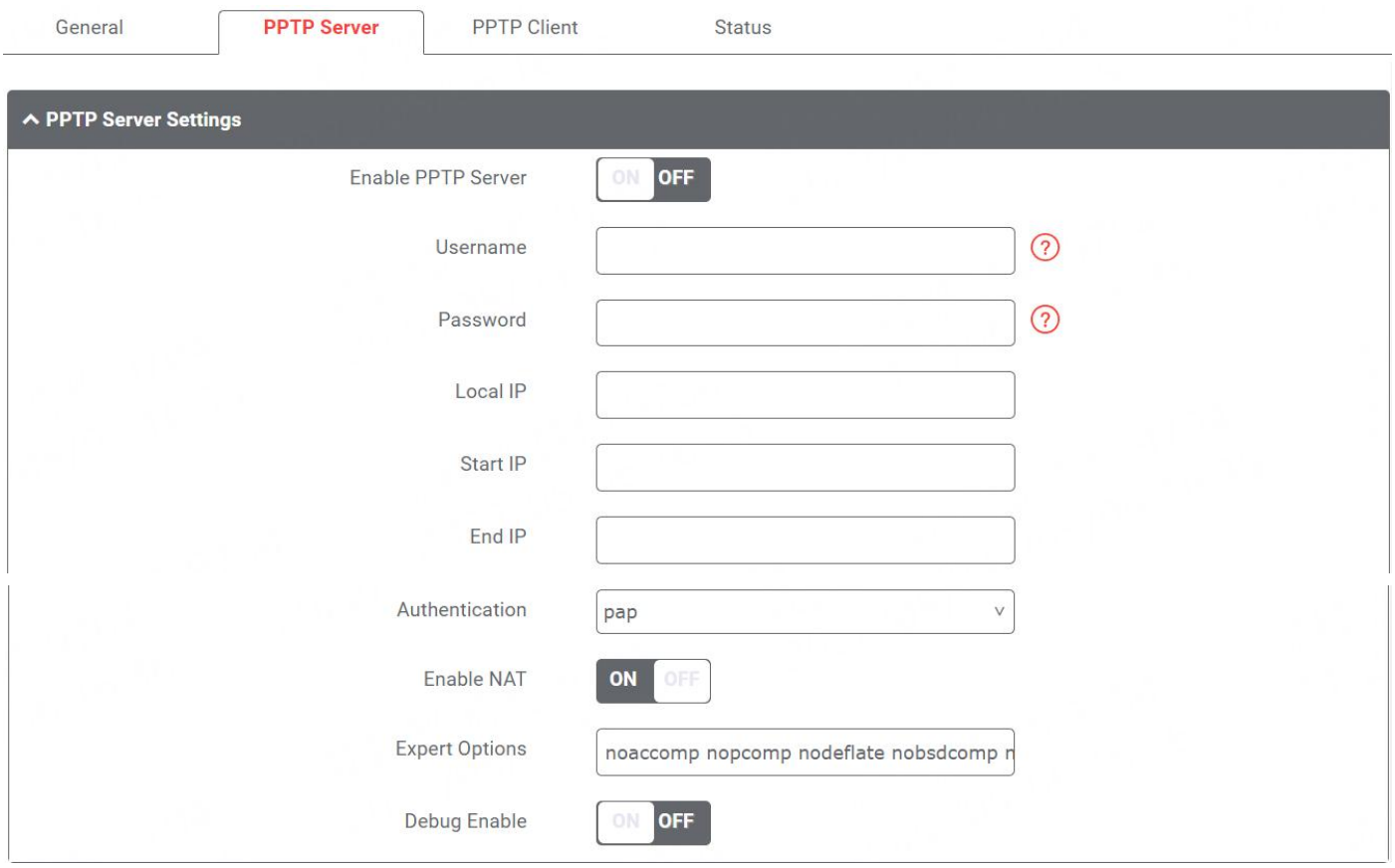
This section is used to set the parameters of PPTP, a type of VPN protocol that uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.

General

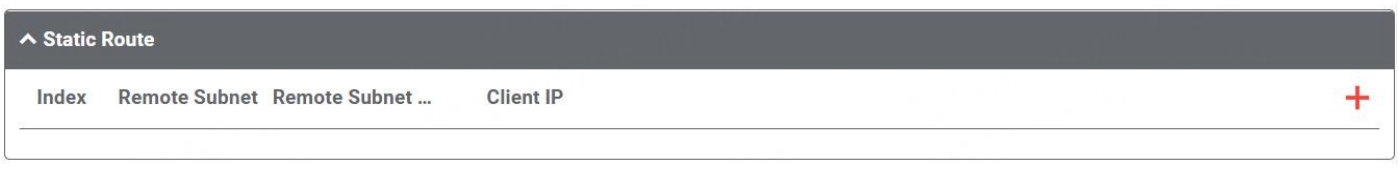


Item	Description	Default
Enable User LED	Click the toggle button to enable/disable the user LED. If User LED is enable here, it will have a higher priority.	OFF

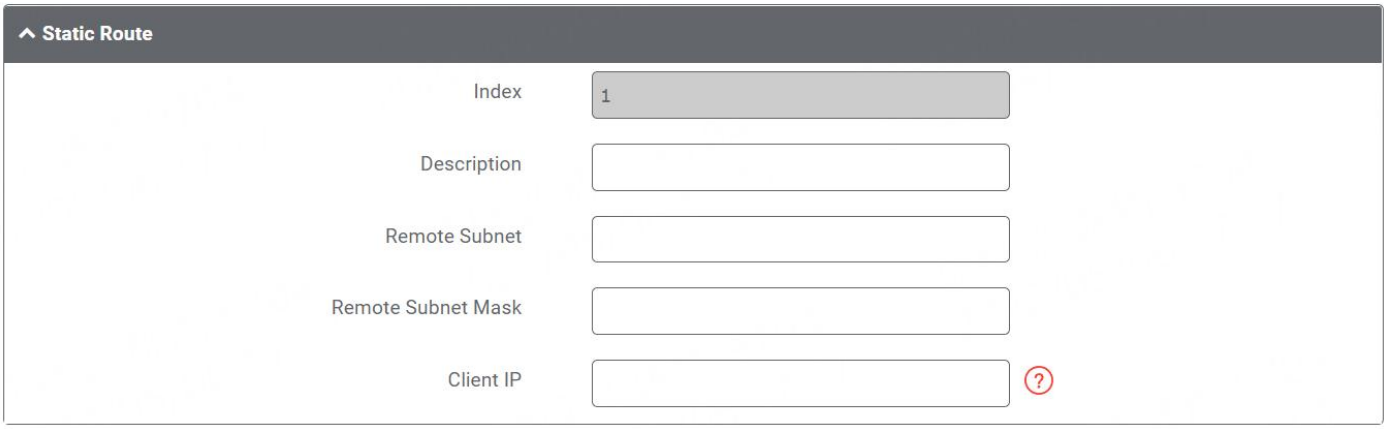
PPTP Server



Item	Description	Default
Enable PPTP Server	Click the toggle button to enable/disable the PPTP server.	OFF
Username	Enter the name for PPTP server.	Null
Password	Enter the password for PPTP server.	Null
Local IP	IP address of this PPTP network interface.	Null
Start IP	PPTP IP address leases will begin from the address specified in this field.	Null
End IP	PPTP IP address leases will end with the address specified in this field.	Null
Authentication	Select from “pap”, “chap”, “mschap v1”, “mschap v2”.	pap
Enable NAT	Click the toggle button to enable/disable NAT.	ON
Expert Options	Enter some other options of PPTP in this field. Each expression can be separated by a ‘;’ .	Null
Debug Enable	Click the toggle button to enable/disable debug.	OFF

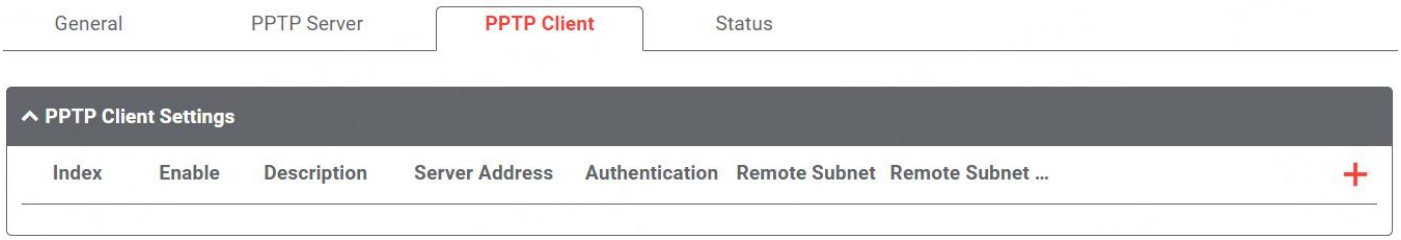


Click + to add a static route for PPTP server. The maximum count is **20.**

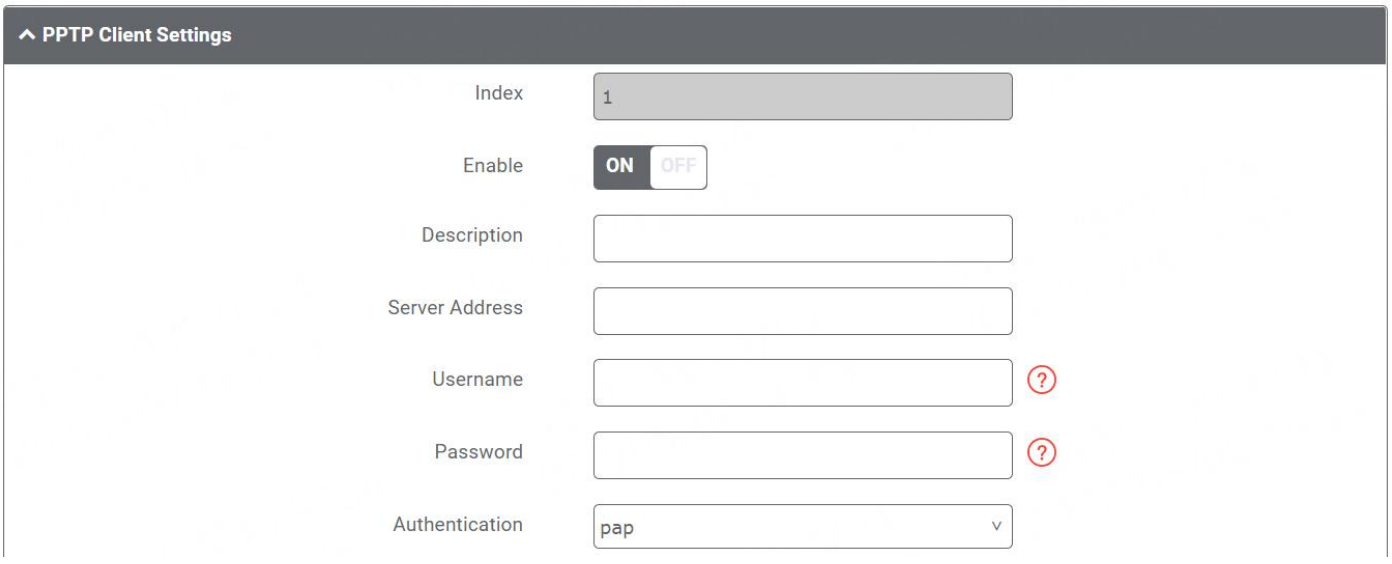


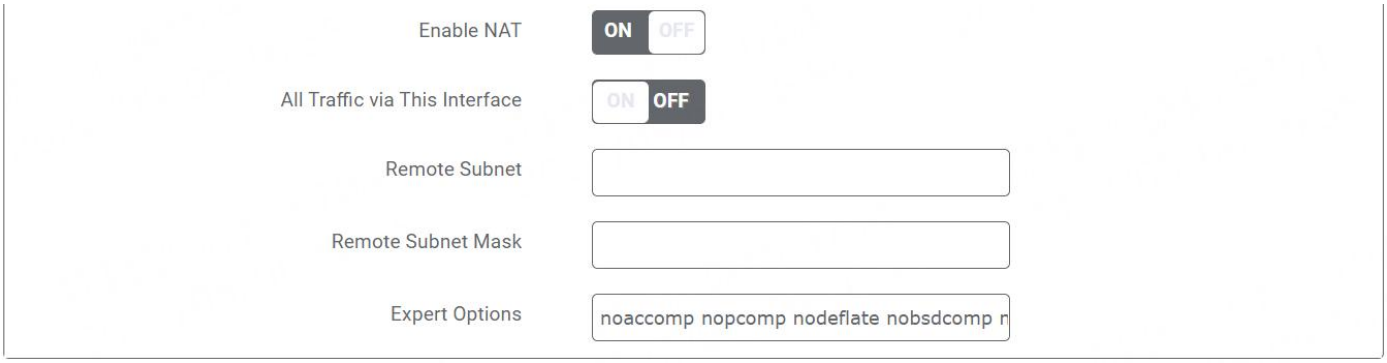
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this static route.	Null
Remote Subnet	Enter the remote subnet's address.	Null
Remote Subnet Mask	Enter the remote mask of subnet address.	Null
Client IP	Enter the client IP, empty means anywhere.	Null

PPTP Client



Click + to add a PPTP client. The maximum count is **5**.

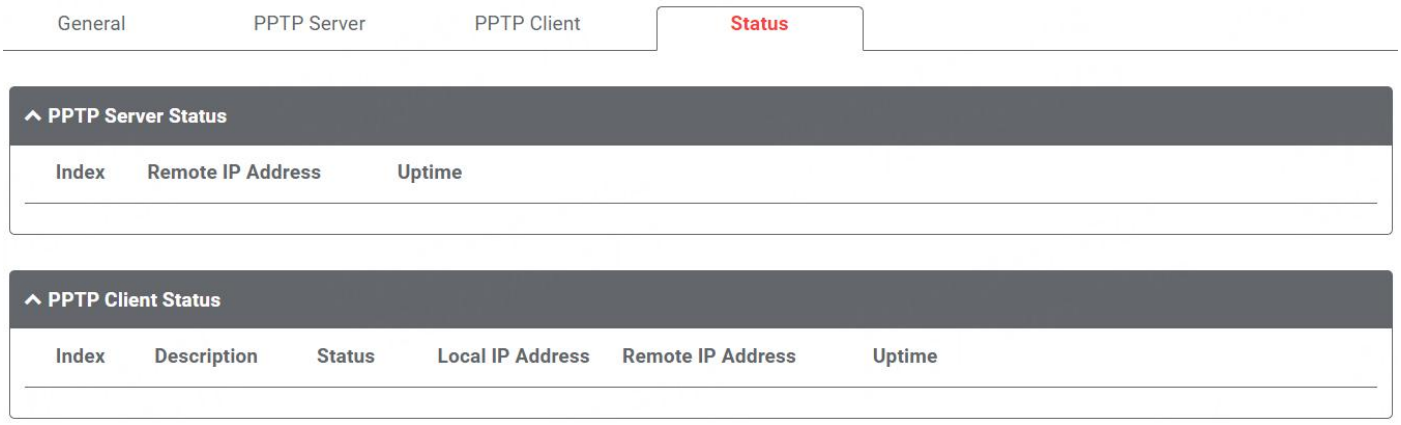




Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable the PPTP client.	OFF
Server Address	Enter the IP address or hostname of a PPTP server.	
Username	Enter the name for PPTP server	Null
Password	Enter the password for PPTP server	Null
Authentication	Select from “pap”, “chap”, “mschap v1”, “mschap v2”.	pap
Enable NAT	Click the toggle button to enable/disable NAT.	ON
All Traffic via This Interface	Click the toggle button to enable/disable this function.	OFF
Remote Subnet	Enter the remote subnet address.	Null
Remote Subnet Mask	Enter the remote subnet address mask.	Null
Expert Options	Enter some other options of PPTP in this field. Each expression can be separated by a ‘;’.	Null

Status

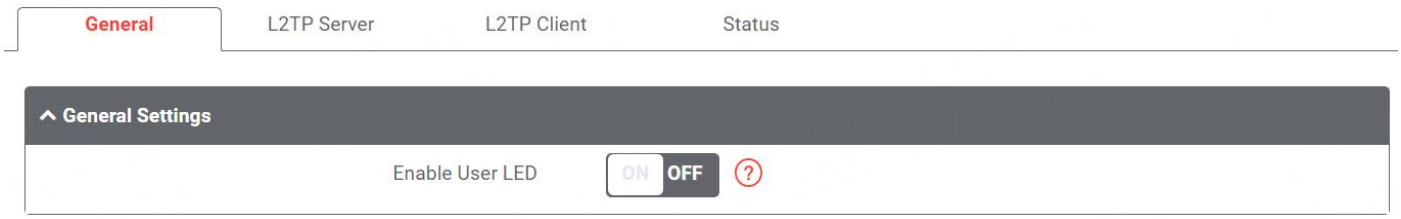
The status bar allows to view PPTP connection status. Click on one of the rows and details of its link connection will be displayed below the current row.



3.5.5 L2TP

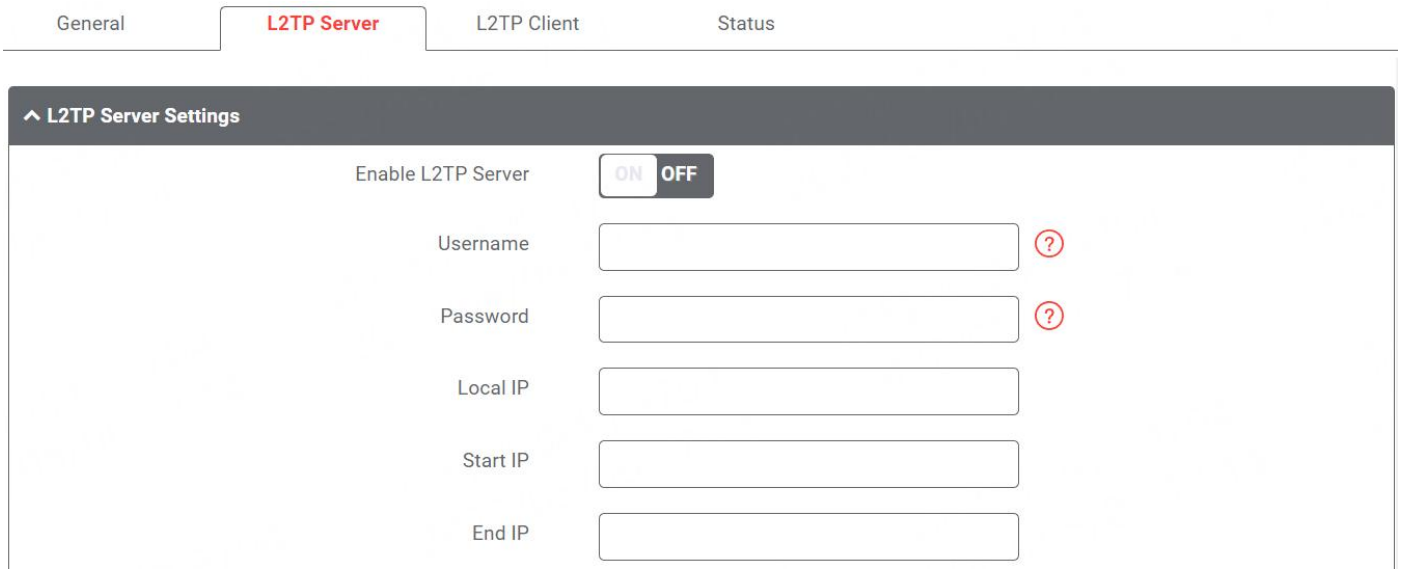
L2TP is a tunneling protocol used to support virtual private networks. It is more secure than PPTP because it encapsulates the transferred data twice, but it is slower and uses more CPU power.

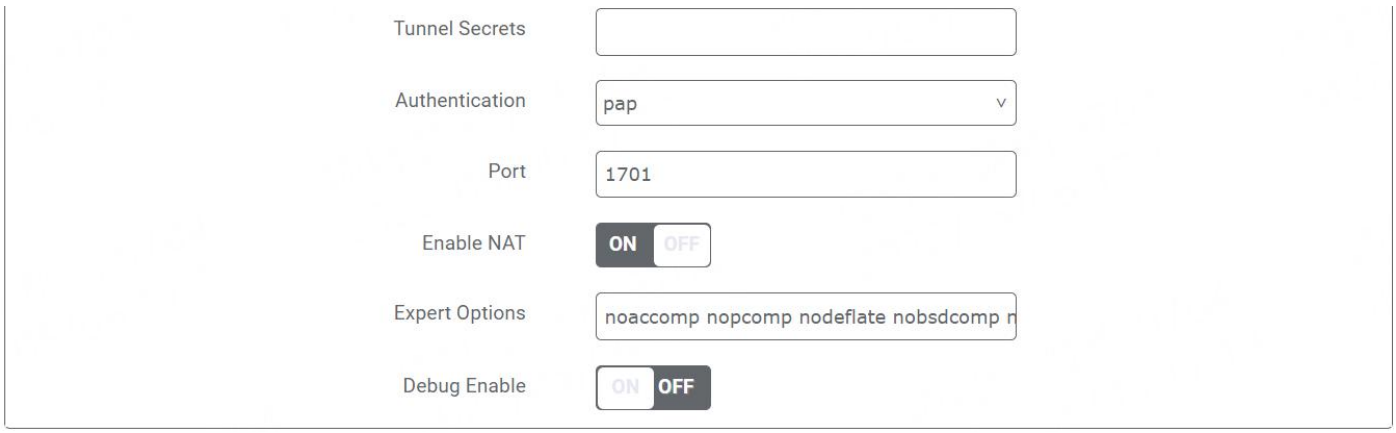
General



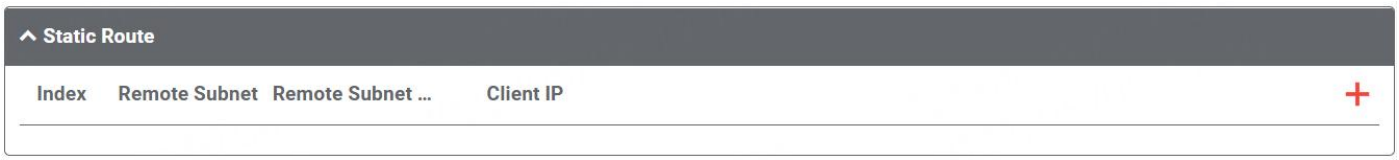
Item	Description	Default
Enable User LED	Click the toggle button to enable/disable the user LED. If User LED is enable here, it will have a higher priority.	OFF

L2TP Server

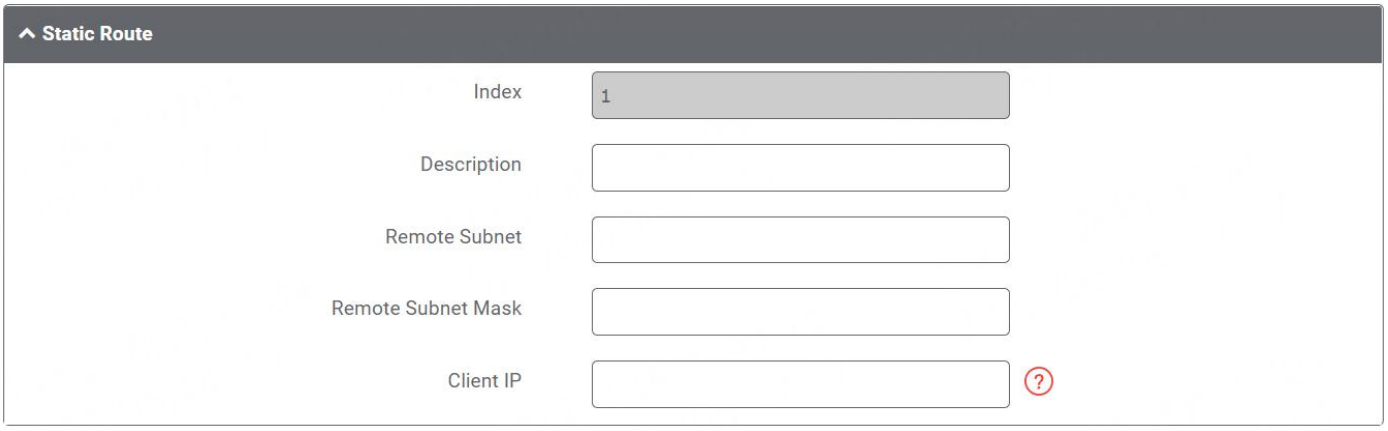




Item	Description	Default
Enable L2TP Server	Click the toggle button to enable/disable the L2TP server.	OFF
Username	Enter the name for L2TP server	Null
Password	Enter the password for L2TP server	Null
Local IP	IP address of this L2TP network interface.	Null
Start IP	L2TP IP address leases will begin from the address specified in this field.	Null
End IP	L2TP IP address leases will end with the address specified in this field.	Null
Tunnel Secrets	Enter the tunnel password.	Null
Authentication	Select from “pap”, “chap”, “mschap v1”, “mschap v2”.	pap
Port	Enter the port of this tunnel.	1701
Enable NAT	Click the toggle button to enable/disable NAT.	OFF
Expert Options	Enter some other options of L2TP in this field. Each expression can be separated by a ‘;’ .	Null
Debug Enable	Click the toggle button to enable/disable debug.	OFF

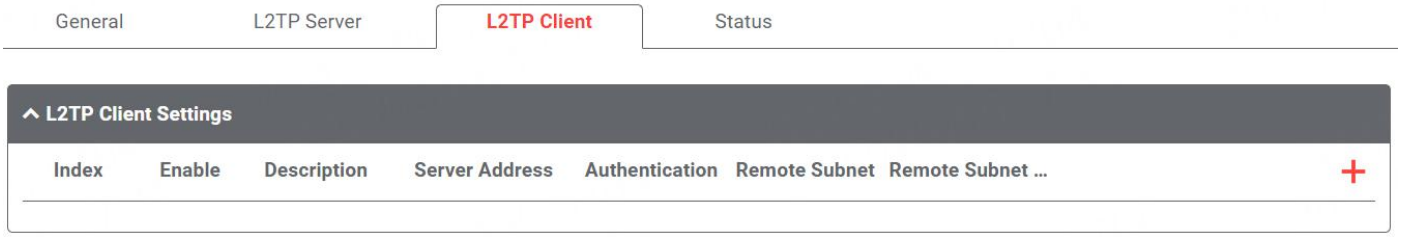


Click + to add a static route for L2TP server. The maximum count is **20.**

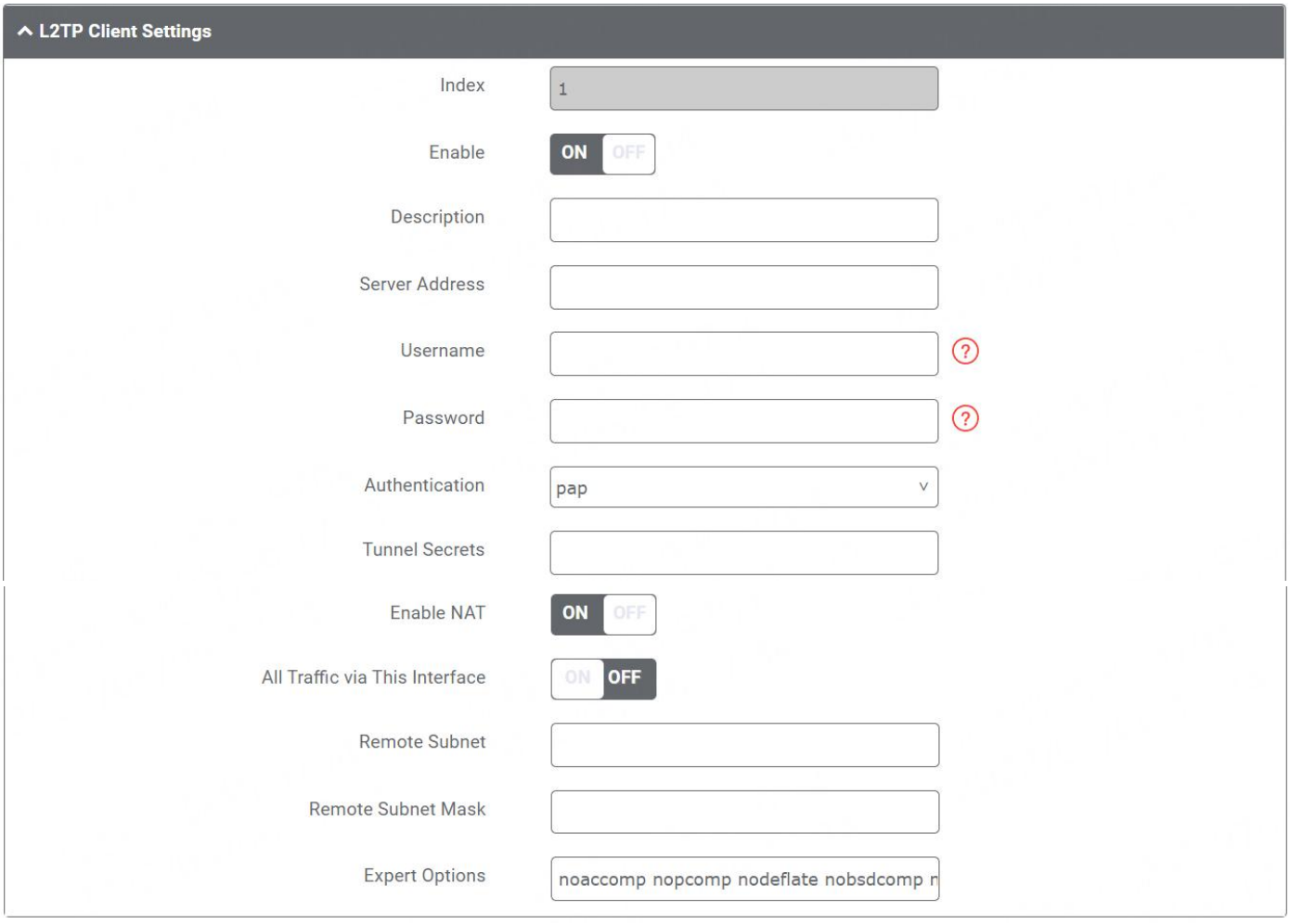


Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this L2TP server.	Null
Remote Subnet	Enter the remote subnet address	Null
Remote Subnet Mask	Enter the remote subnet address mask	Null
Client IP	Enter the Client IP	Null

L2TP Client



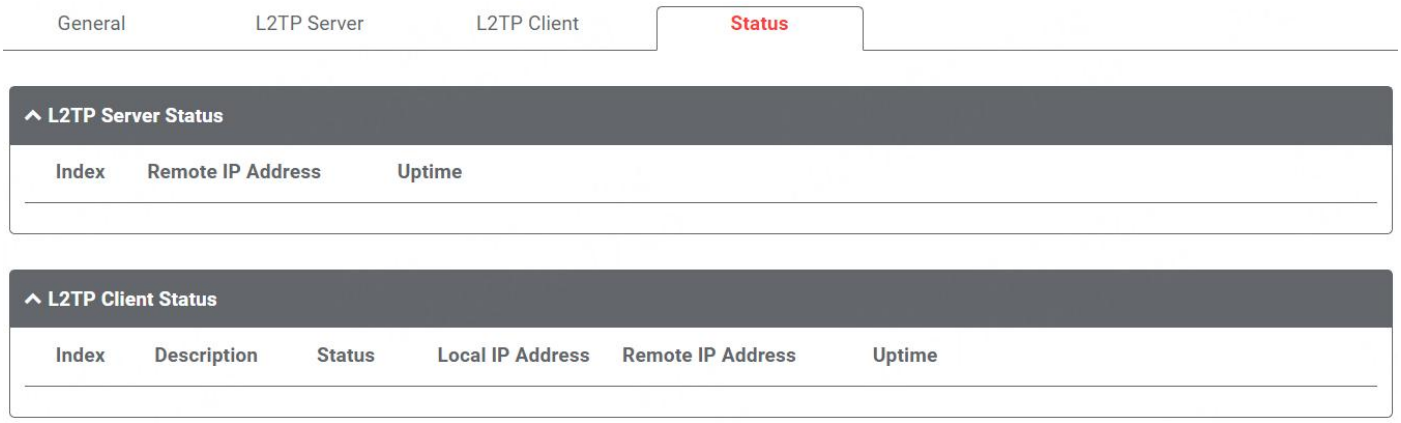
Click + to add a L2TP client. The maximum count is 5.



Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable the PPTP client.	OFF
Description	Enter a description for this L2TP client.	Null
Server Address	Enter the IP address or hostname of a L2TP server.	Null
Username	Enter the name for PPTP server	Null
Password	Enter the password for PPTP server	Null
Authentication	Select from “pap”, “chap”, “mschap v1”, “mschap v2”.	pap
Tunnel Secrets	Enter the tunnel password.	Null
Enable NAT	Click the toggle button to enable/disable NAT.	ON
All Traffic via This Interface	Click the toggle button to enable/disable this function.	OFF
Remote Subnet	Enter the remote subnet address.	Null
Remote Subnet Mask	Enter the remote subnet address mask.	Null
Expert Options	Enter some other options of PPTP in this field. Each expression can be separated by a ‘;’.	Null

Status

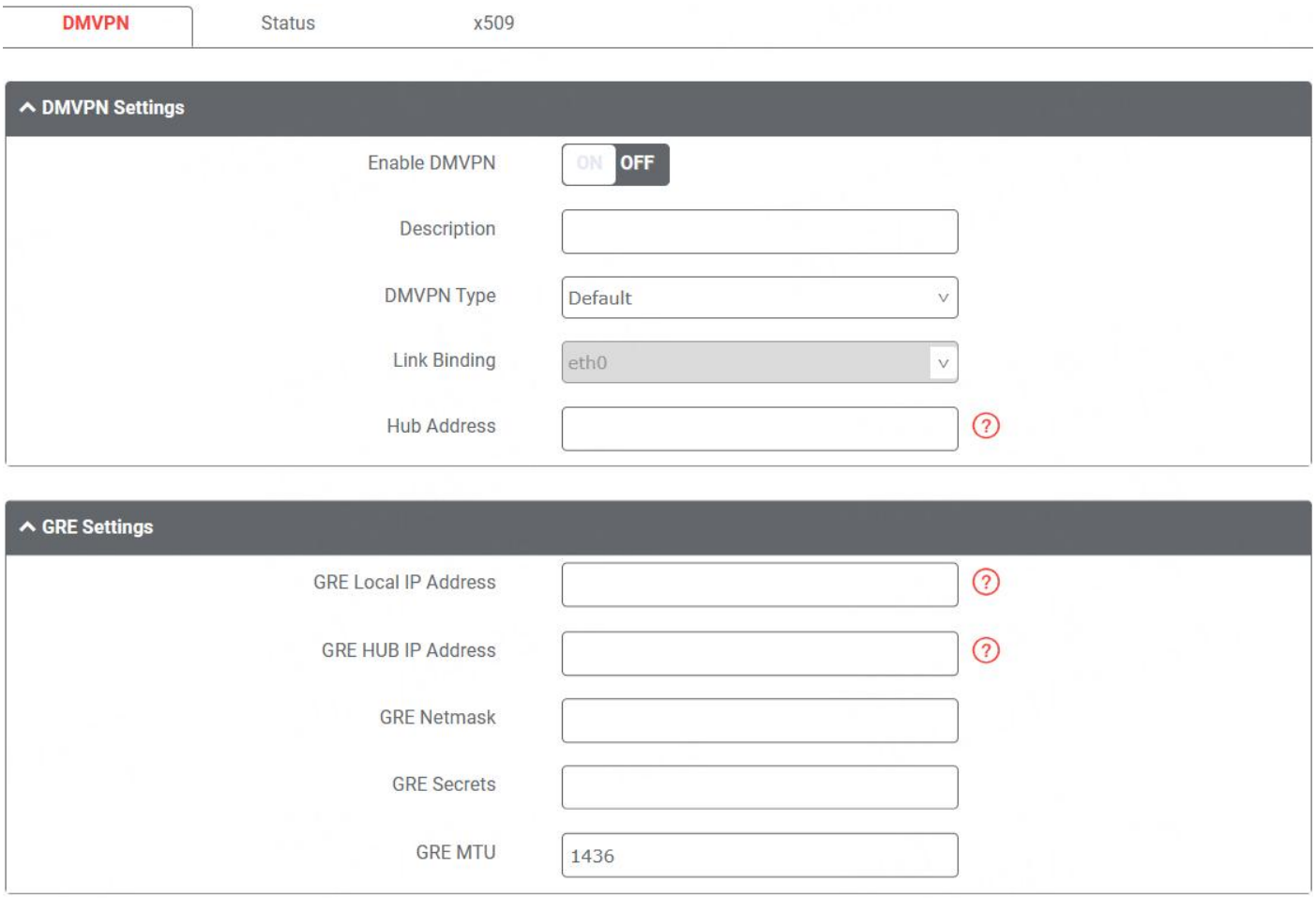
The status bar allows to view L2TP connection status. Click on one of the rows and details of its link connection will be displayed below the current row.



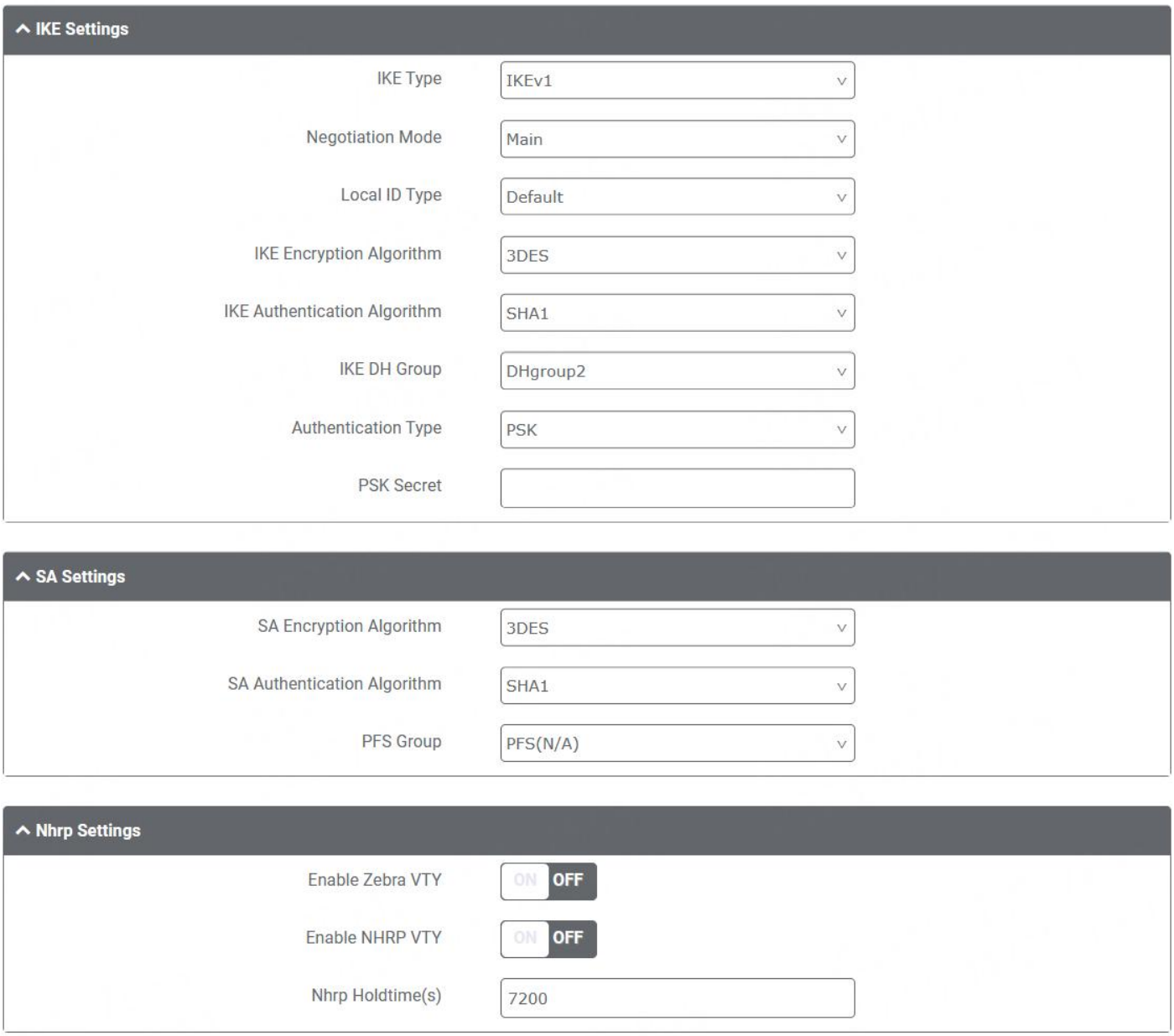
3.5.6 DMVPN

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

DMVPN



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



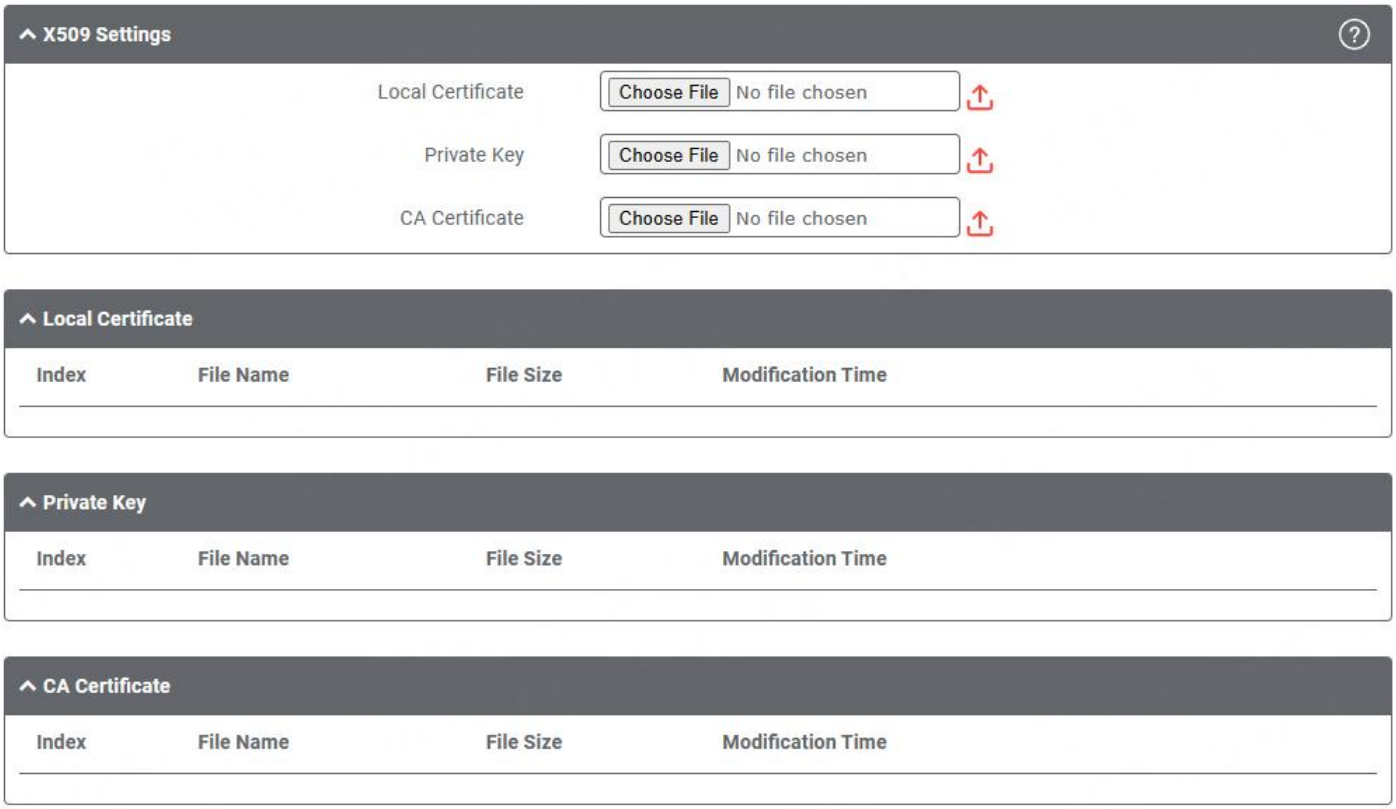
Item	Description	Default
IKE Type	Select IKE Type	IKEv1
Negotiation Mode	Select from “Main” and “aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established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

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

Status

The status bar allows to view DMVPN connection status.

X509



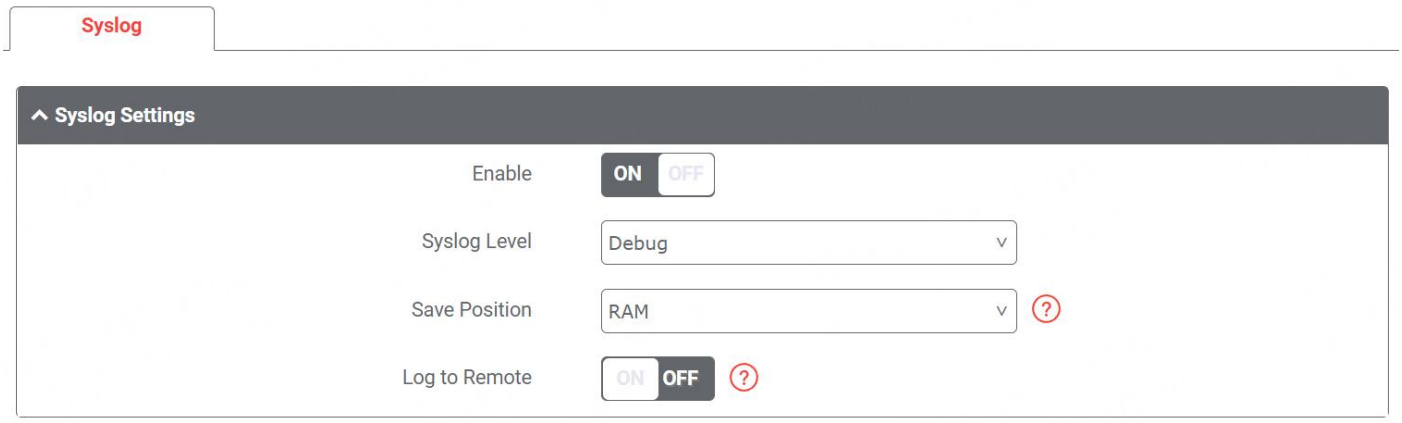
x509		
Item	**Description**	**Default**
X509 Settings		
Local Certificate	Click “Choose File” to locate Local Certificate file and then import this file into your device.	--
Private Key	Click “Choose File” to locate Private Key file, and then import this file into your device.	--
CA Certificate	Click “Choose File” to locate CA 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

3.6 Services

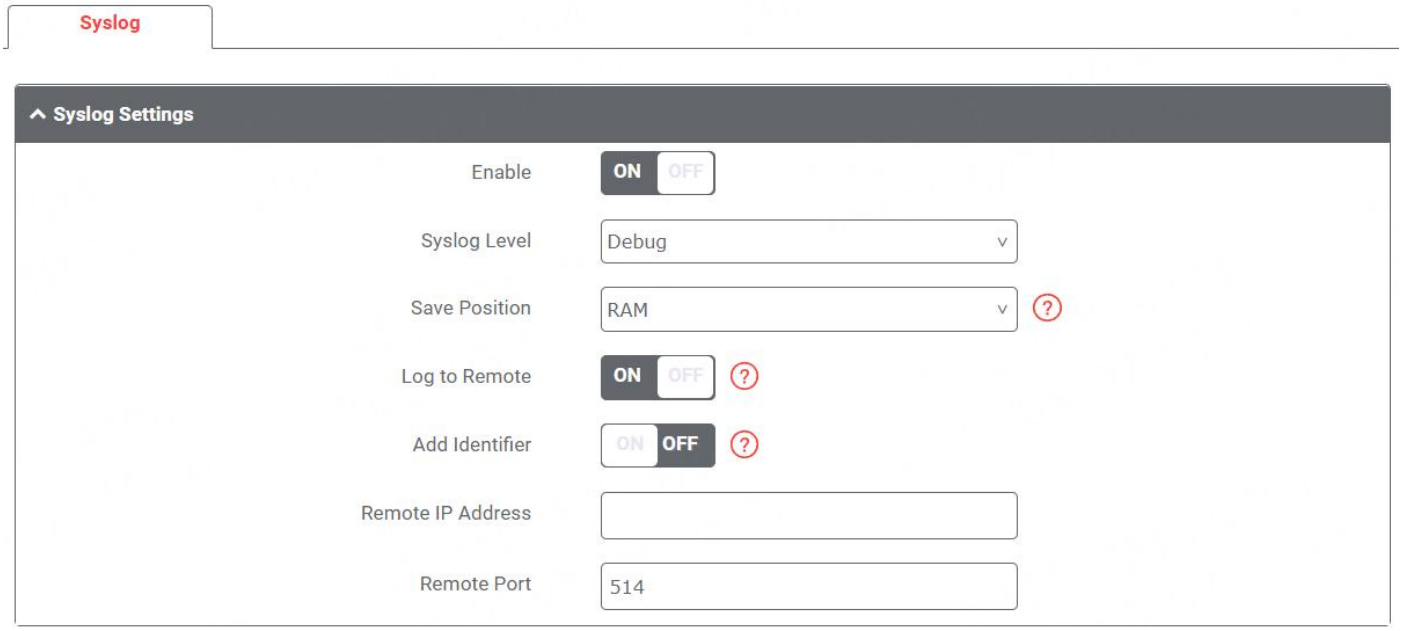
3.6.1 Syslog

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

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



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



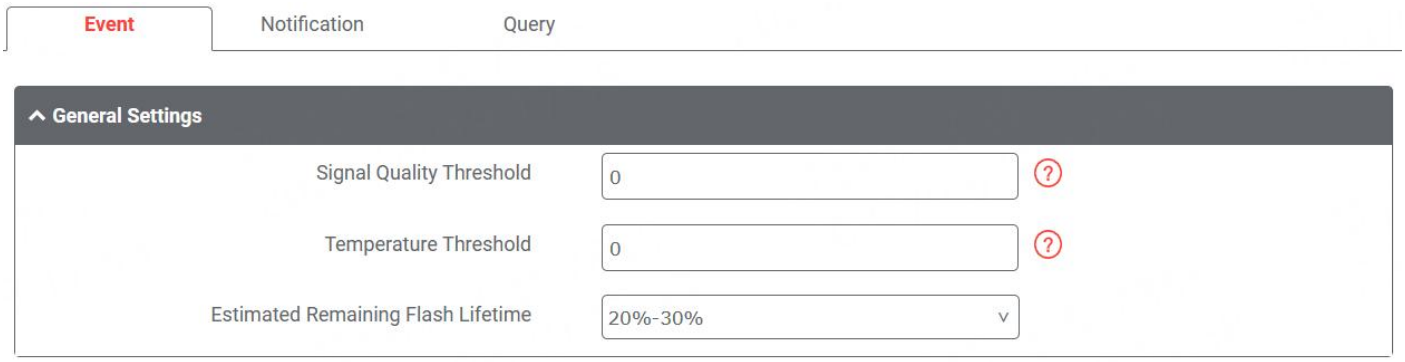
Item	Description	Default
Enable	Click the toggle button to enable/disable the Syslog settings option.	ON
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. The lower level will output more syslog in details.	Debug
Save Position	Select the save position from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

Remote Port	Enter the port of syslog server when enabling the “Log to Remote” option.	514

3.6.2 Event

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

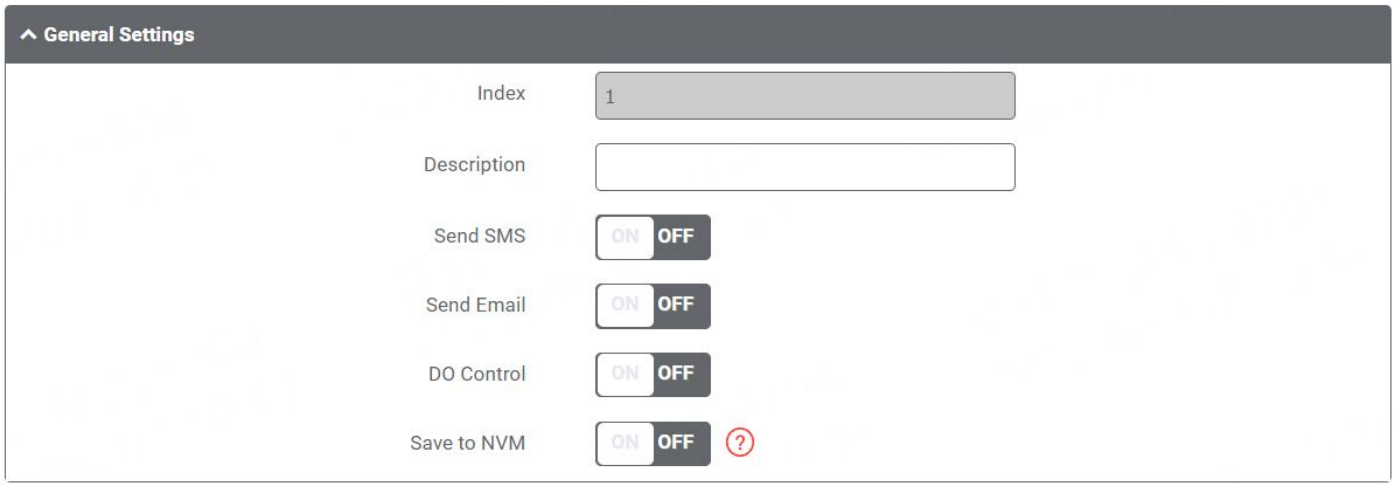
Event



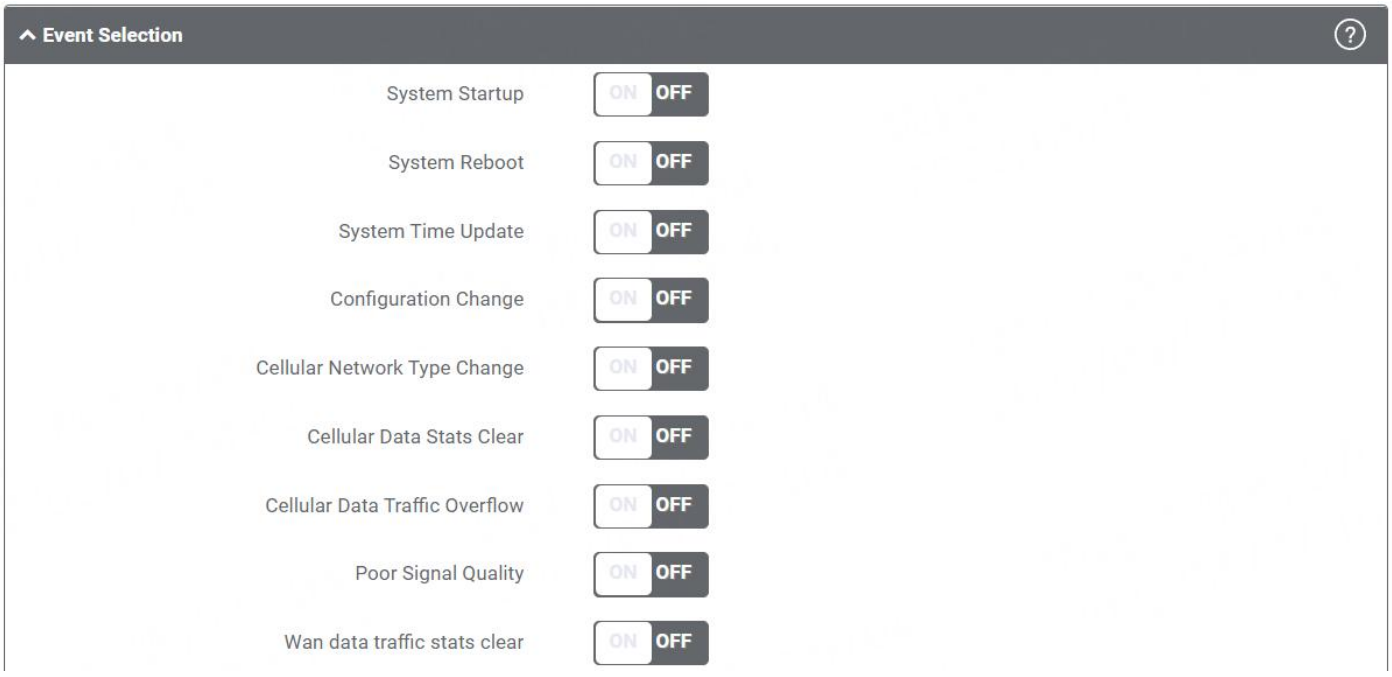
Item	Description	Default
Signal Quality Threshold	Set the threshold for signal quality. Device will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0
Temperature Threshold	Set the threshold for temperature. Device will generate a log event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

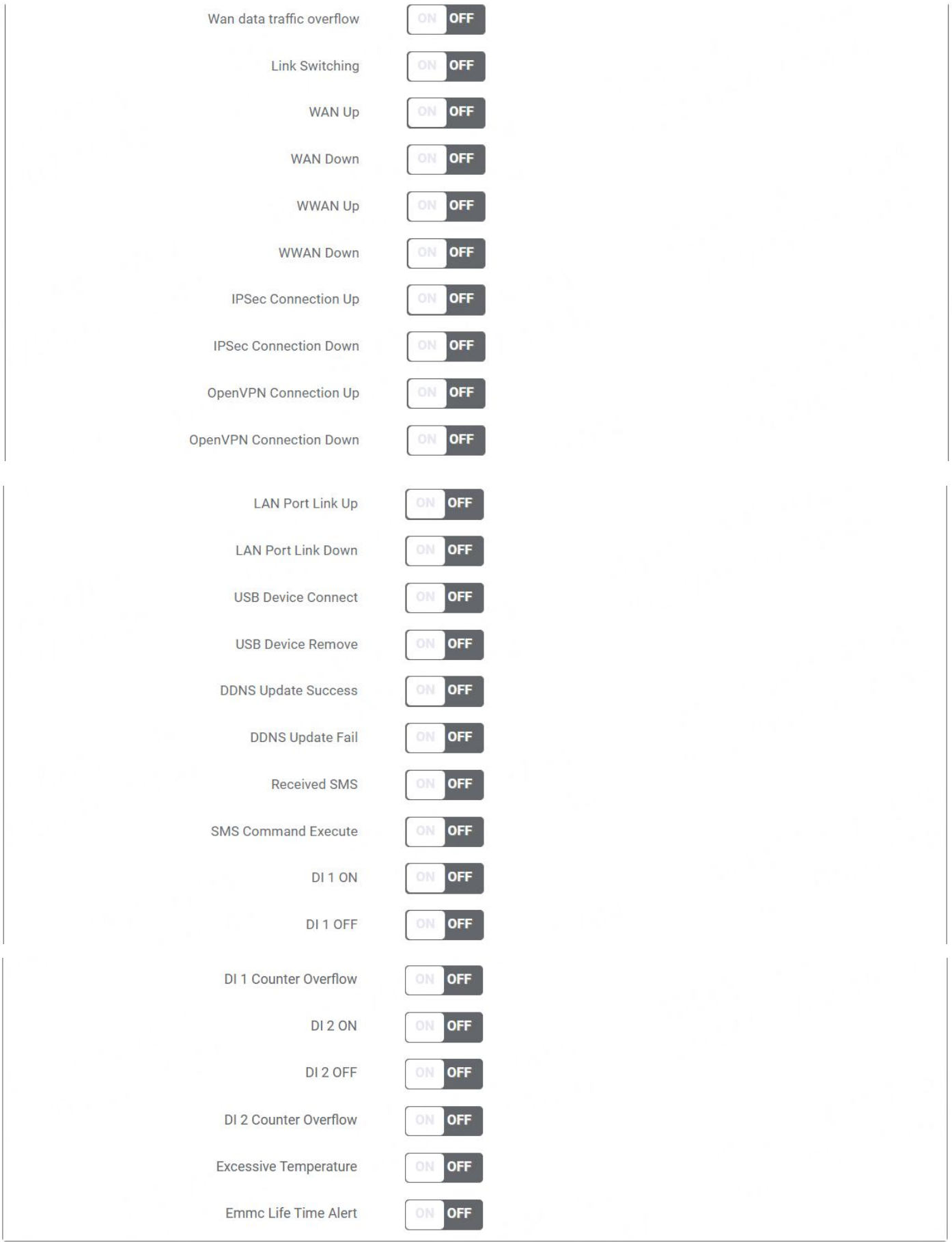
Notification

Click + button to add an Event parameters.



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

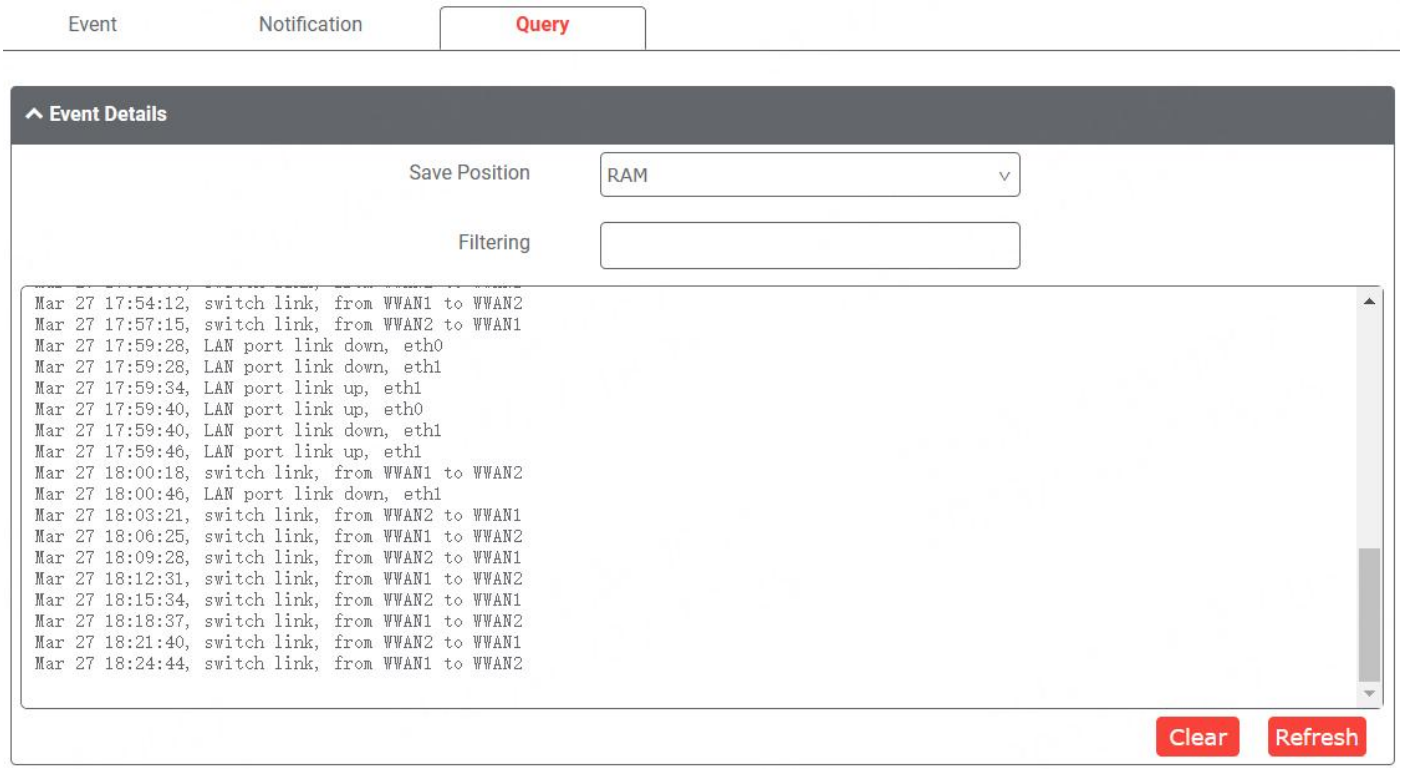



Wan data traffic overflow
Link Switching
WAN Up
WAN Down
WWAN Up
WWAN Down
IPSec Connection Up
IPSec Connection Down
OpenVPN Connection Up
OpenVPN Connection Down
LAN Port Link Up
LAN Port Link Down
USB Device Connect
USB Device Remove
DDNS Update Success
DDNS Update Fail
Received SMS
SMS Command Execute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

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

Query

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

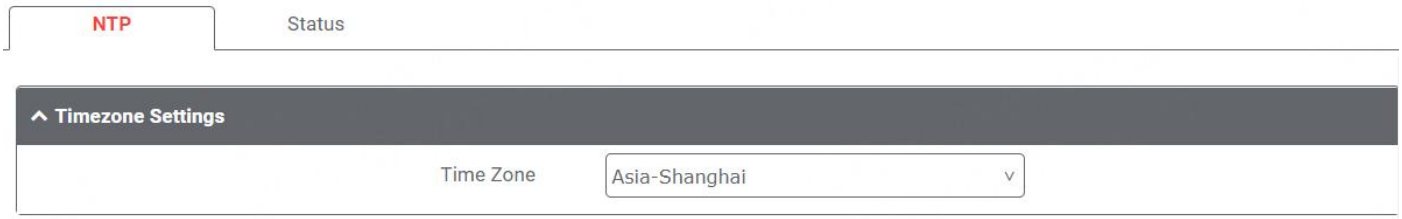


Item	Description	Default
Save Position	Select the events' save position from "RAM" or "NVM". • RAM: Random-access memory • NVM: Non-Volatile Memory	RAM
Filtering	Enter the filtering message based on the keywords set by users. Click the "Refresh" button, the filtered event will be displayed in the follow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

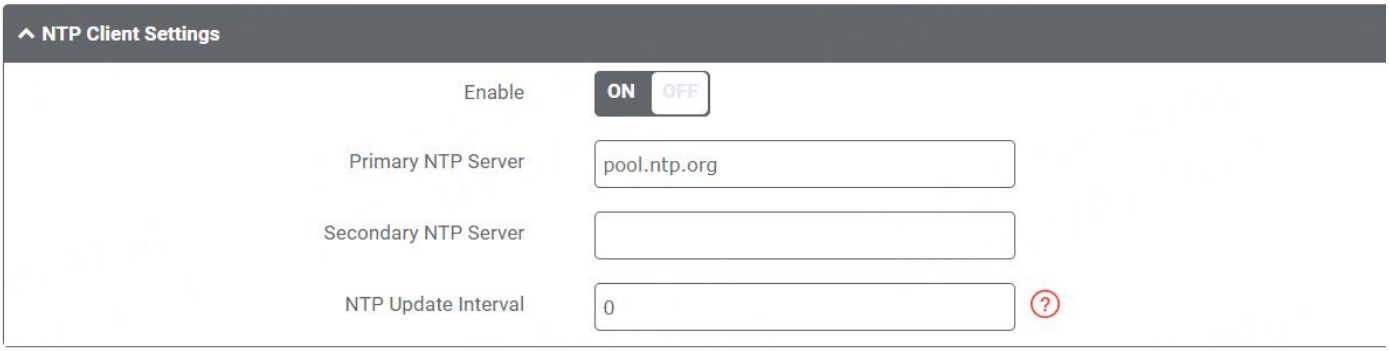
3.6.3 NTP

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

NTP



Item	Description	Default
Time Zone	Click the drop down list to select the time zone you are in.	Asia-Shanghai

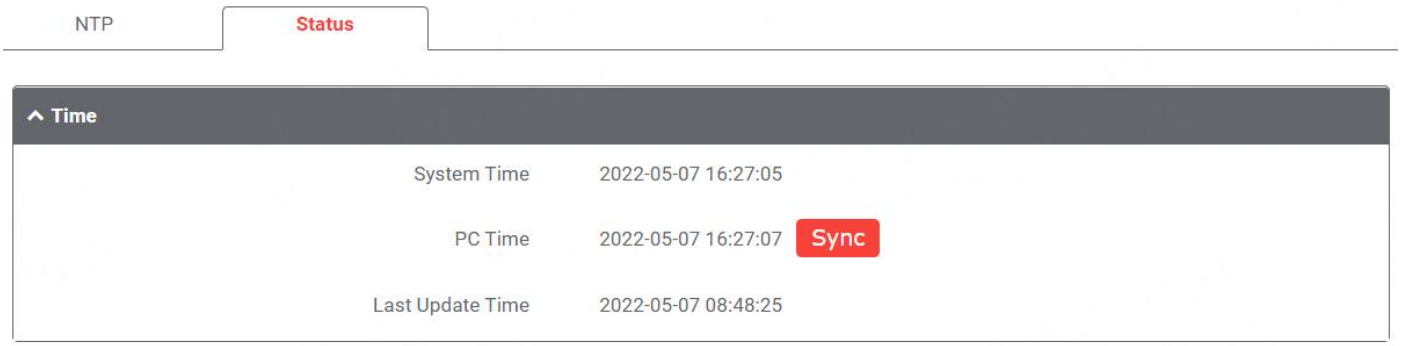


Item	Description	Default
Enable	Click the toggle button to enable/disable this option. Enable to synchronize time with the NTP server.	ON
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.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

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

Status

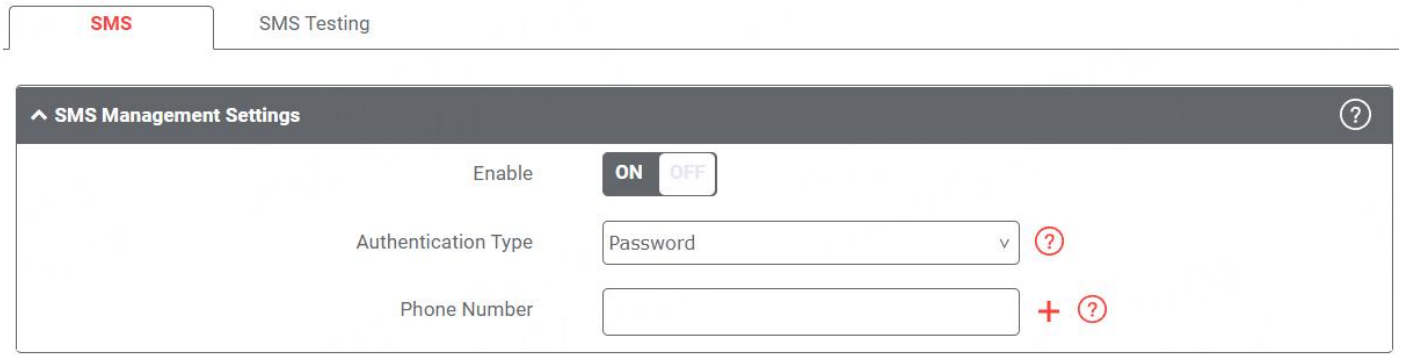
This window allows you to view the current time of router and also synchronize the router time. Click Sync button to synchronize the router time with the PC's time.



3.6.4 SMS

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

SMS

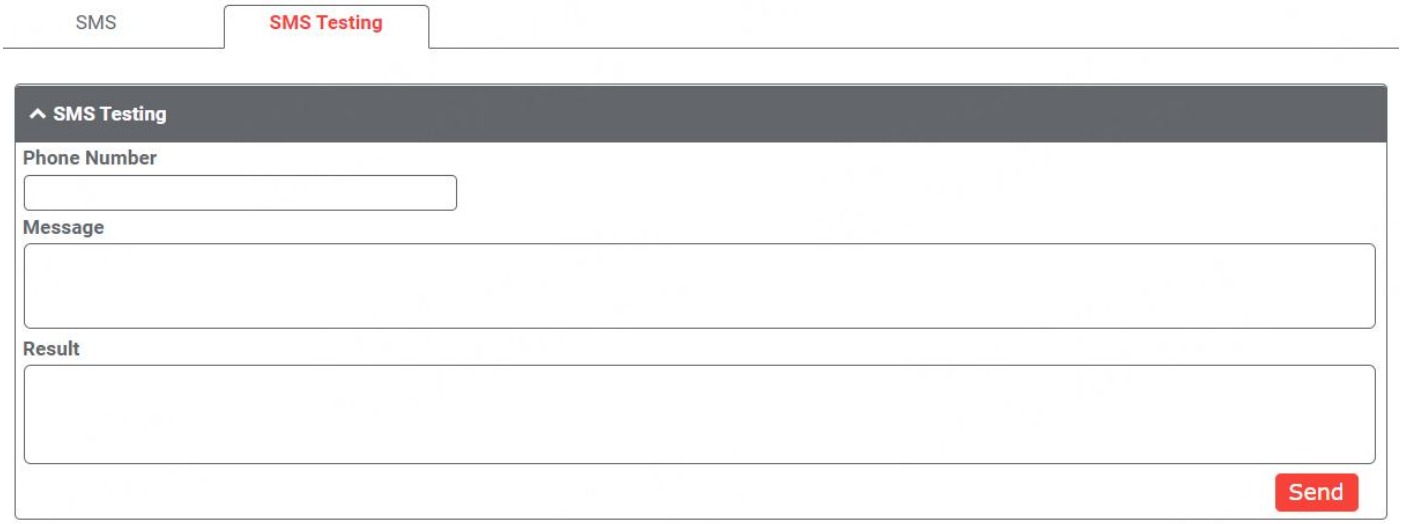


Item	Description	Default
Enable	Click the toggle button to enable/disable the SMS Management option. **Note**: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from “Password”, “Phonenum” or “Both”. Password: Use the same username and password as WEB manager for authentication. For example, the format of the SMS should be “username: password; cmd1; cmd2; …” Note: Set the WEB manager password in System > User Management section. Phonenum: Use the Phone number for authentication, and user should set the Phone Number that is allowed for SMS management. The format of the SMS should be “cmd1; cmd2; …” Both: Use both the “Password” and “Phonenum” for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be “username: password; cmd1; cmd2; …”	Password
Phone Number	Set the phone number used for SMS management, and click + to add new phone number.	Null

	Note: *It can be null when choose "Password" as the authentication type.*	

SMS Testing

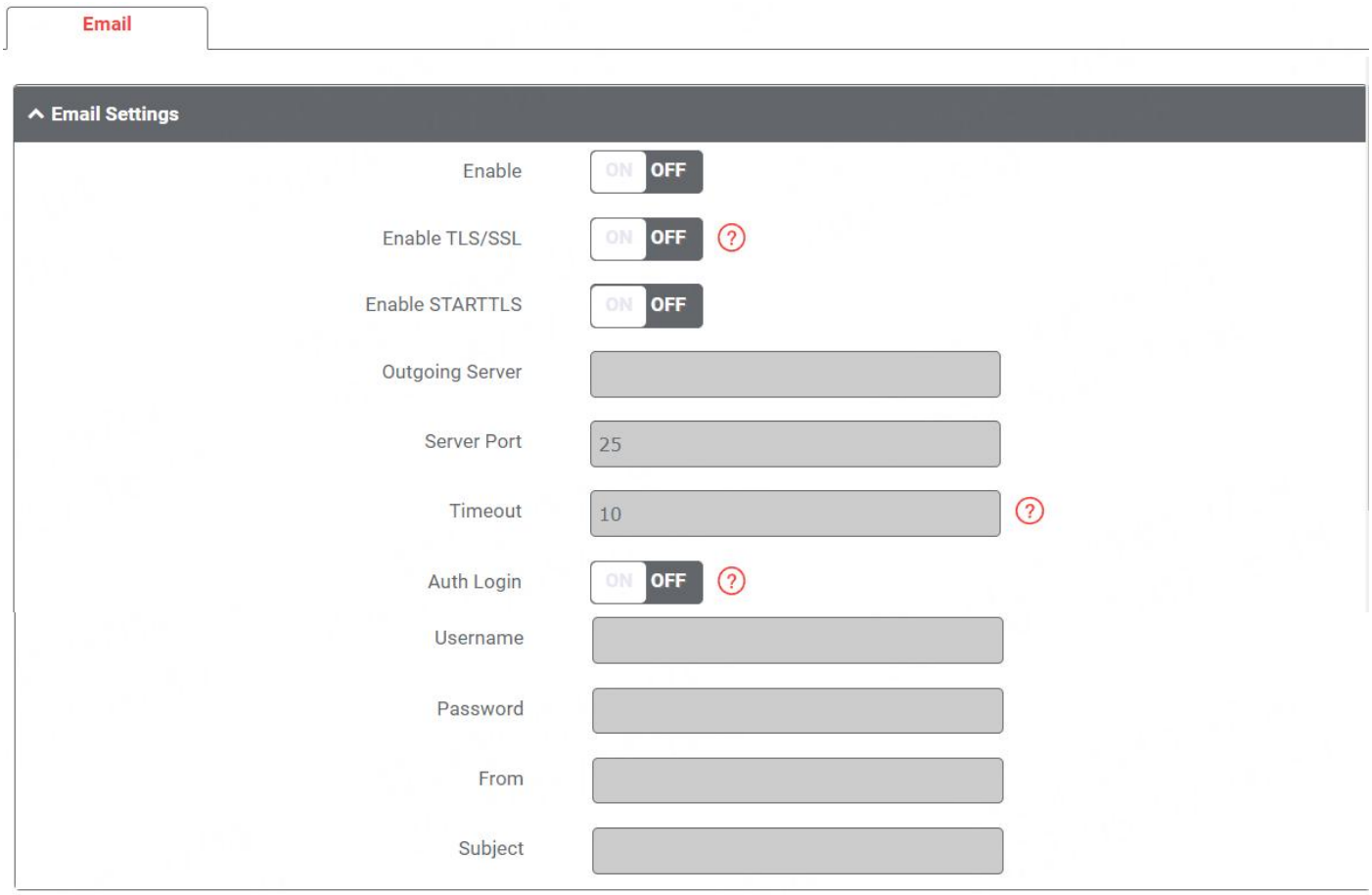
User can test the current SMS service whether it is available in this section.



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

3.6.5 Email

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



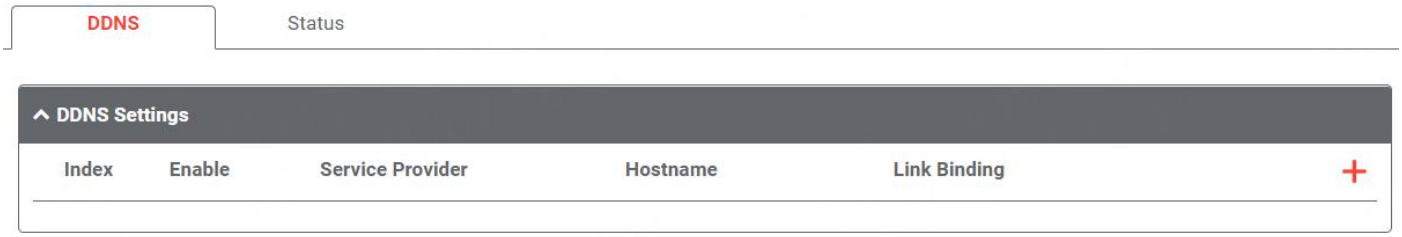
Item	Description	Default
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Enable STARTTLS	Click the toggle button to enable / disable STARTTLS encryption.	OFF
Outgoing server	Enter the SMTP server IP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

3.6.6 DDNS

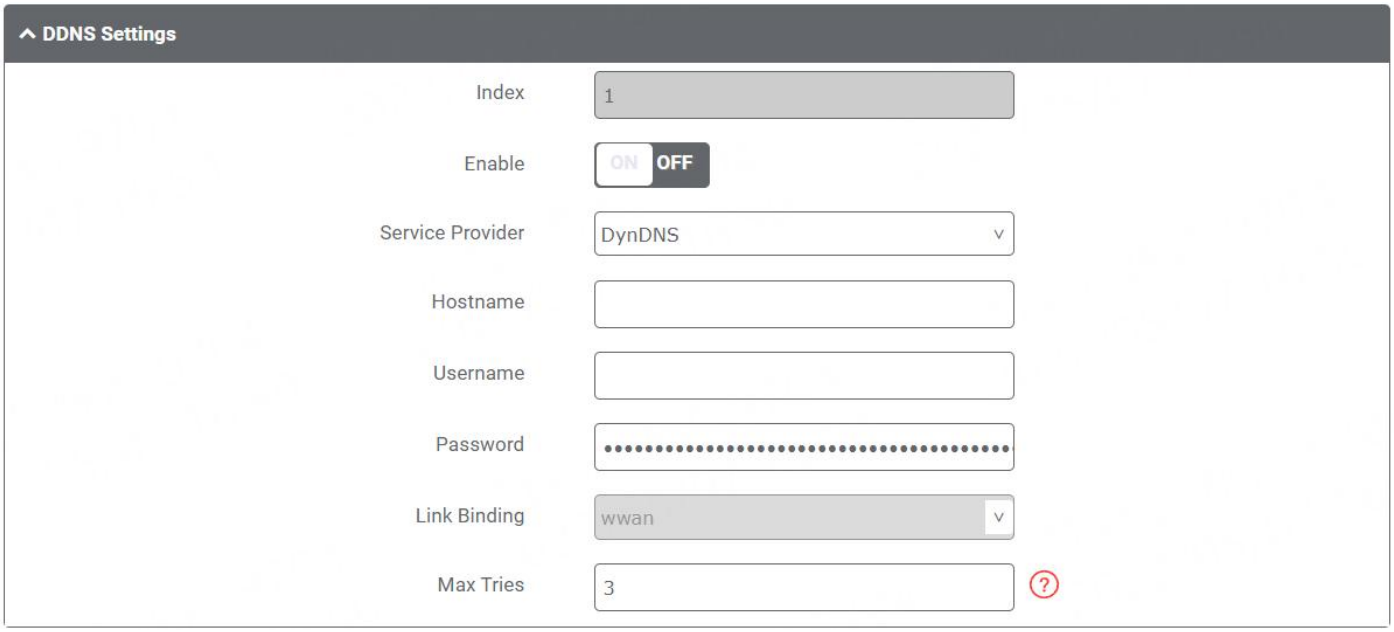
This section allows you to set the DDNS parameters. The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows you whose ISP does not assign them a static IP address to use a domain

name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP. The service provider defaults to “DynDNS”, as shown below.

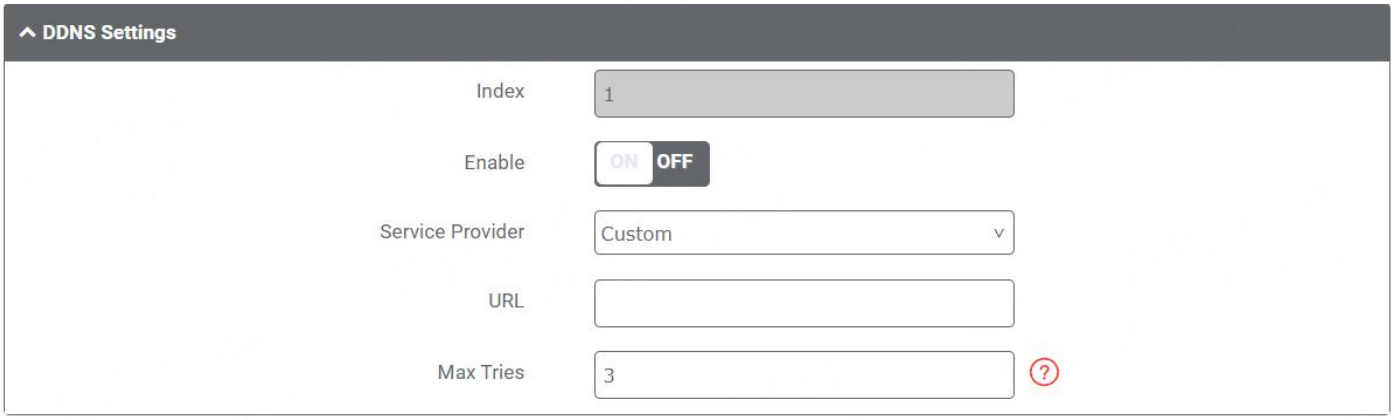
DDNS



Click + to add a new Dynamic Domain Name Server.



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

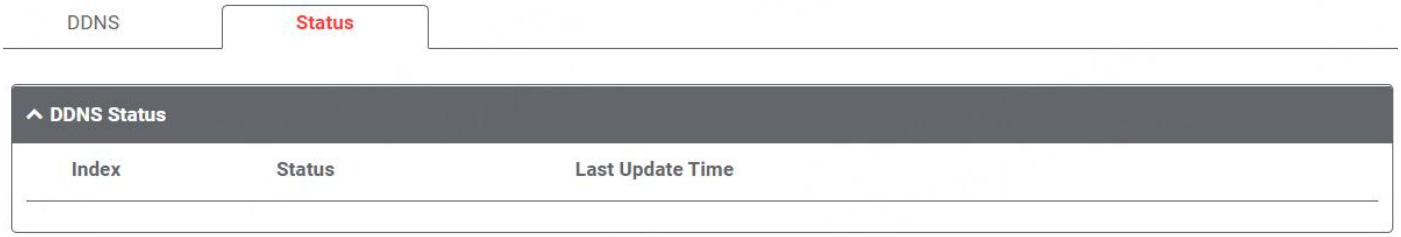


Item	Description	Default

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

Status

The status bar allows to view DDNS connection status.

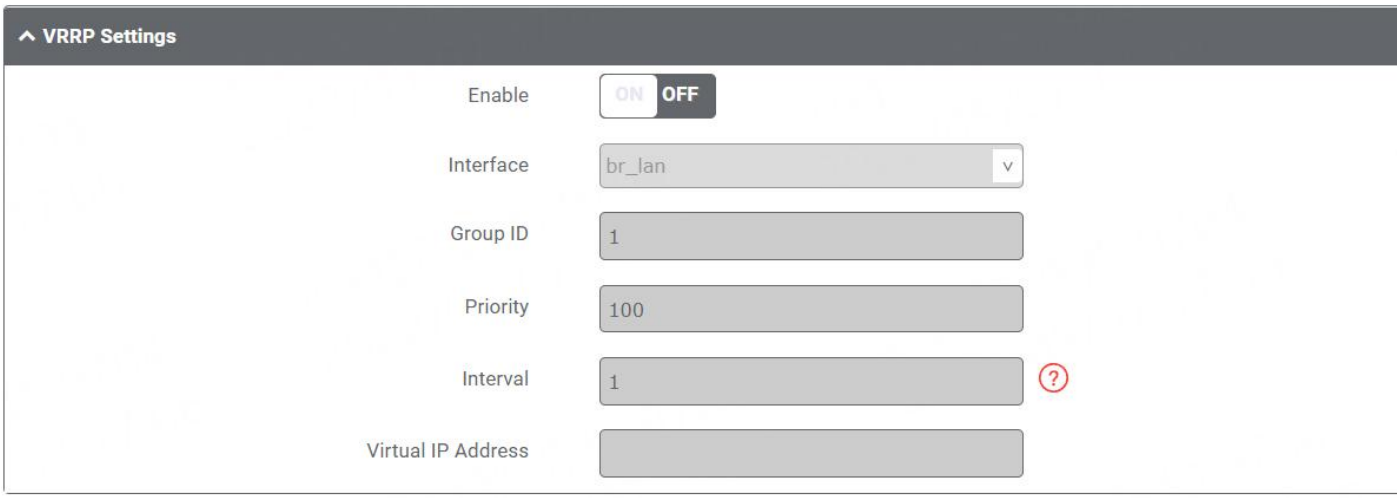


Item	Description
Status	Display the current status of the DDNS.
Last Update Time	Display the date and time for the DDNS was last updated successfully.

3.6.7 VRRP

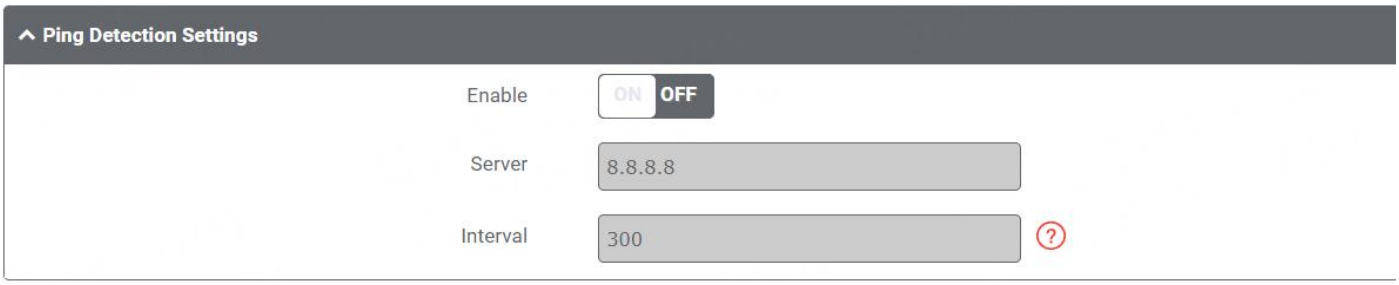
This section allows you to set the VRRP parameters. VRRP stands for Virtual Router Redundancy Protocol, is a standard for device redundancy and failover that creates a virtual router with a floating IP address.

VRRP Settings



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

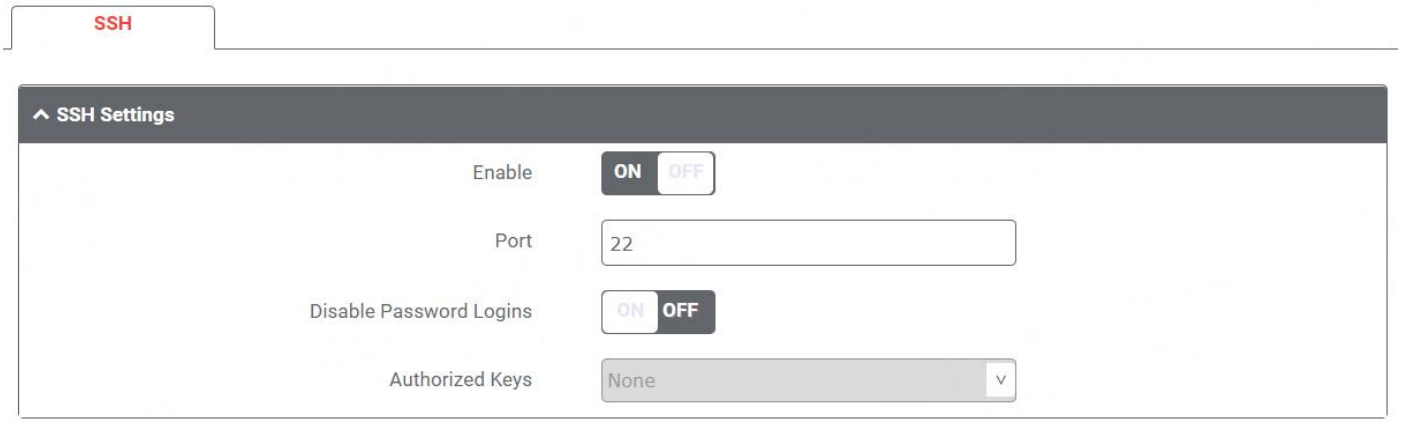
Ping Detection Settings



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

3.6.8 SSH

Device supports SSH password access and secret-key access.

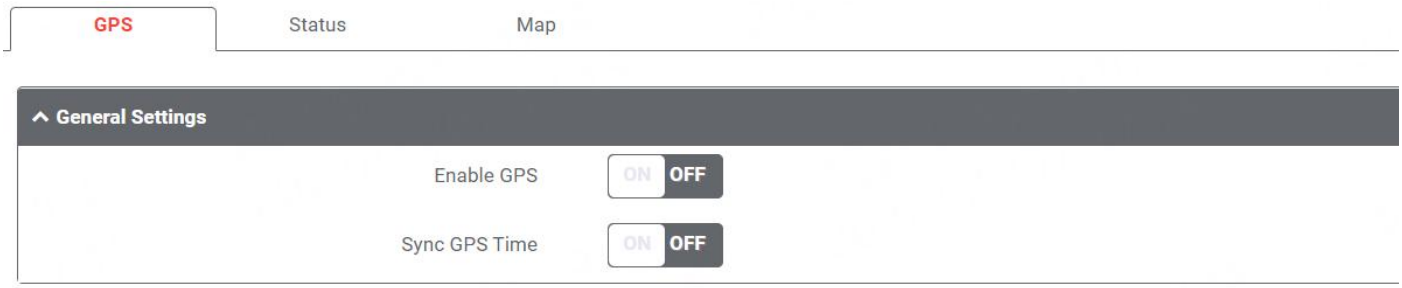


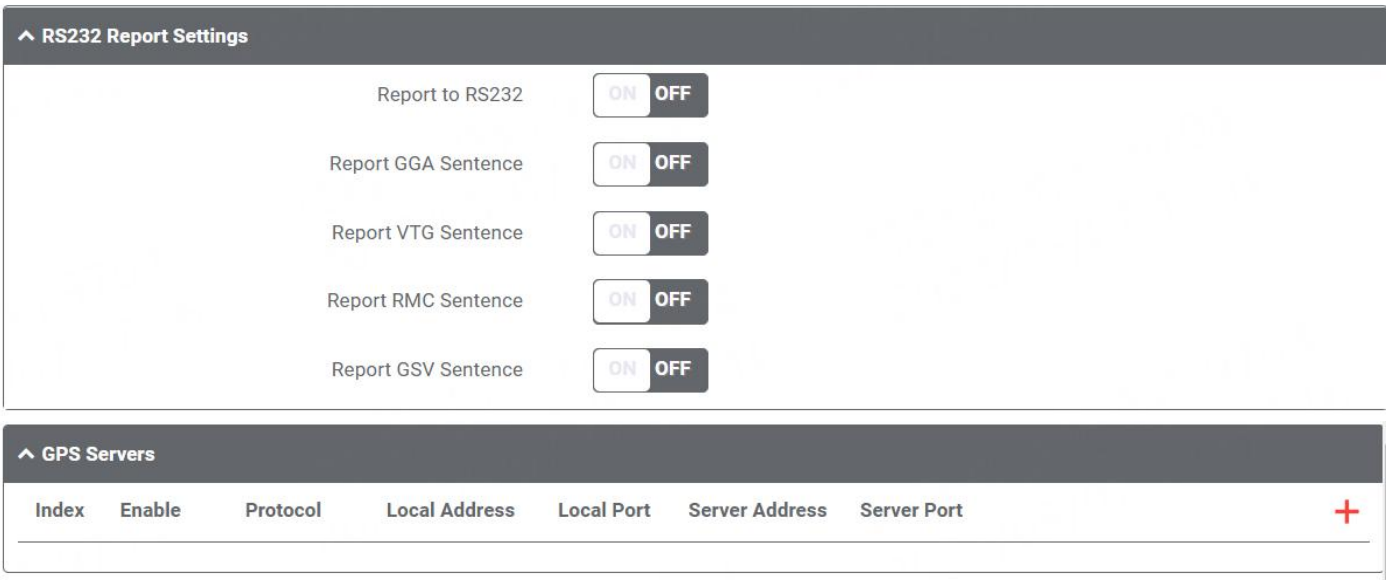
Item	Description	Default
Enable	Click the toggle button to enable/disable this option. When enabled, you can access the router via SSH.	ON
Port	Set the port of the SSH access.	22
Disable Password Logins	Click the toggle button to enable/disable this option. When enabled, you cannot use username and password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

3.6.9 GPS

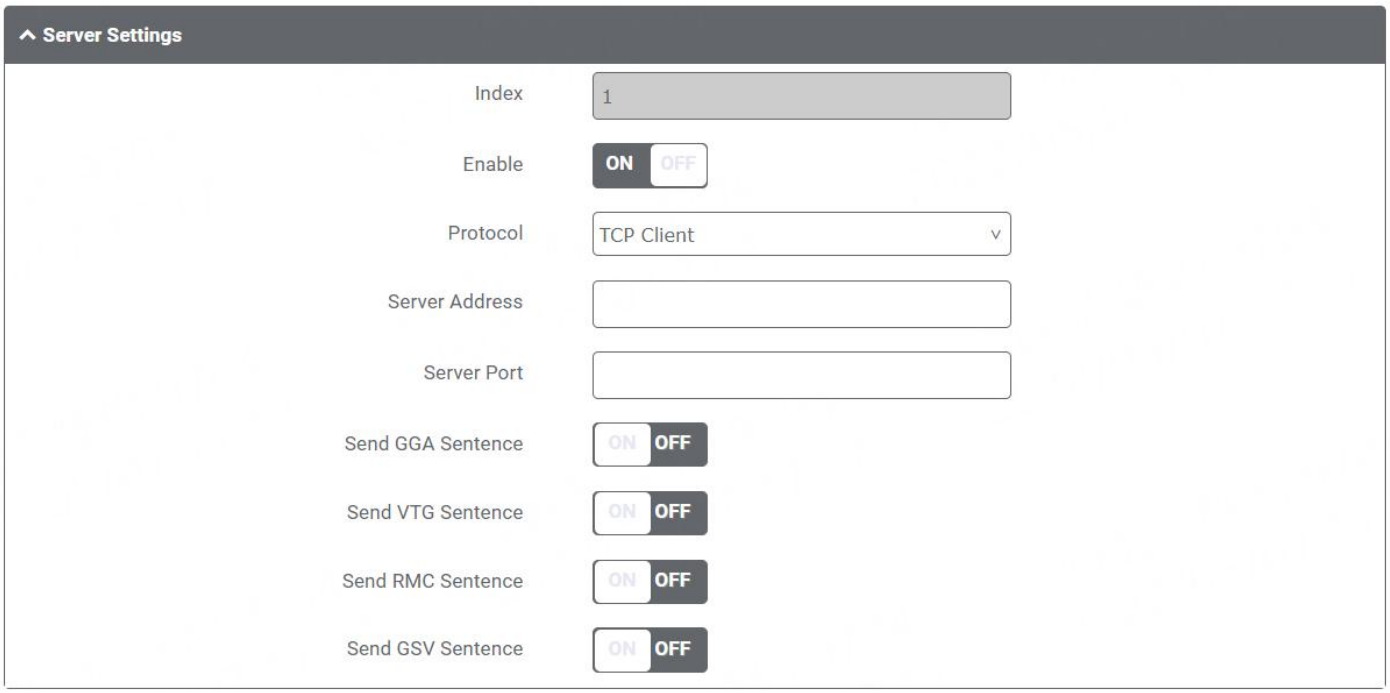
This section is used to configure the parameters of GPS. The GPS function of device can locate and acquire the location information of the device and report it to the designated server.

GPS





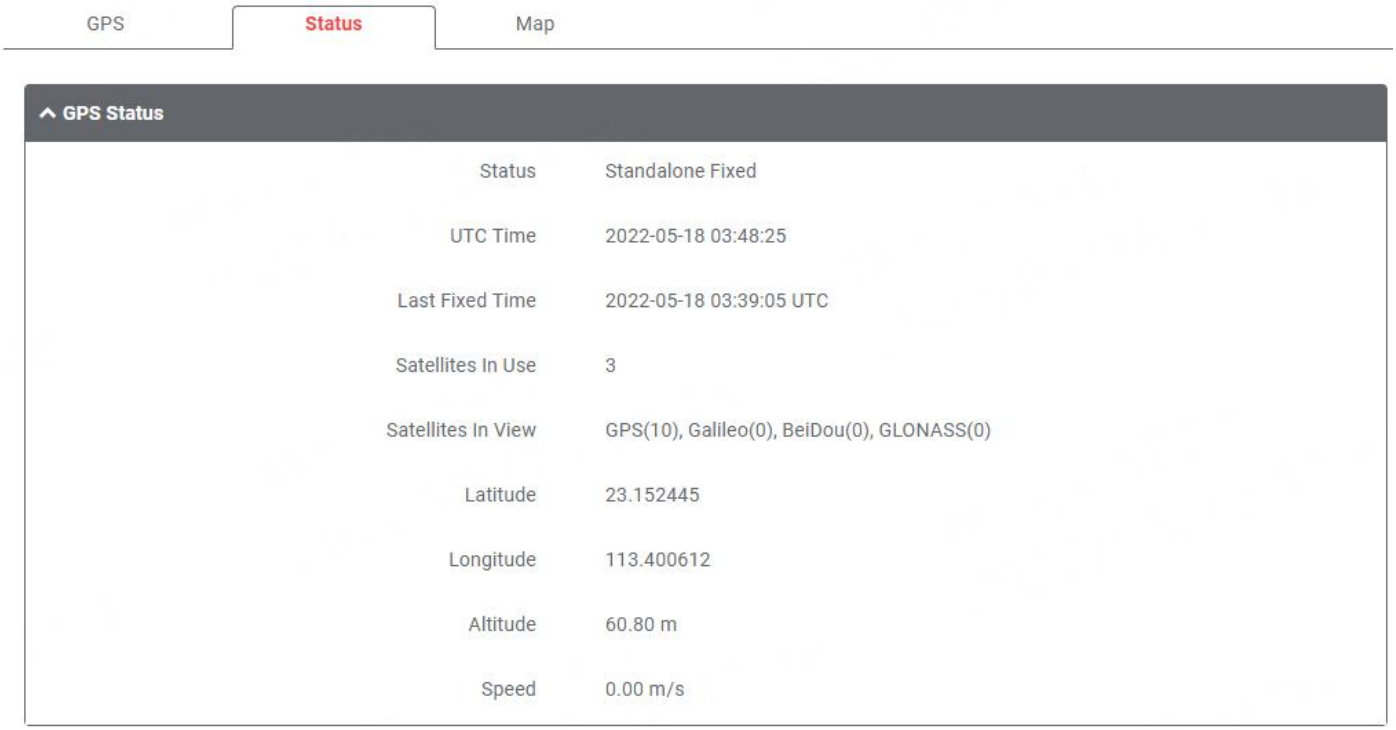
Click + to add a new GPS Server. The maximum count is **5.**



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

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

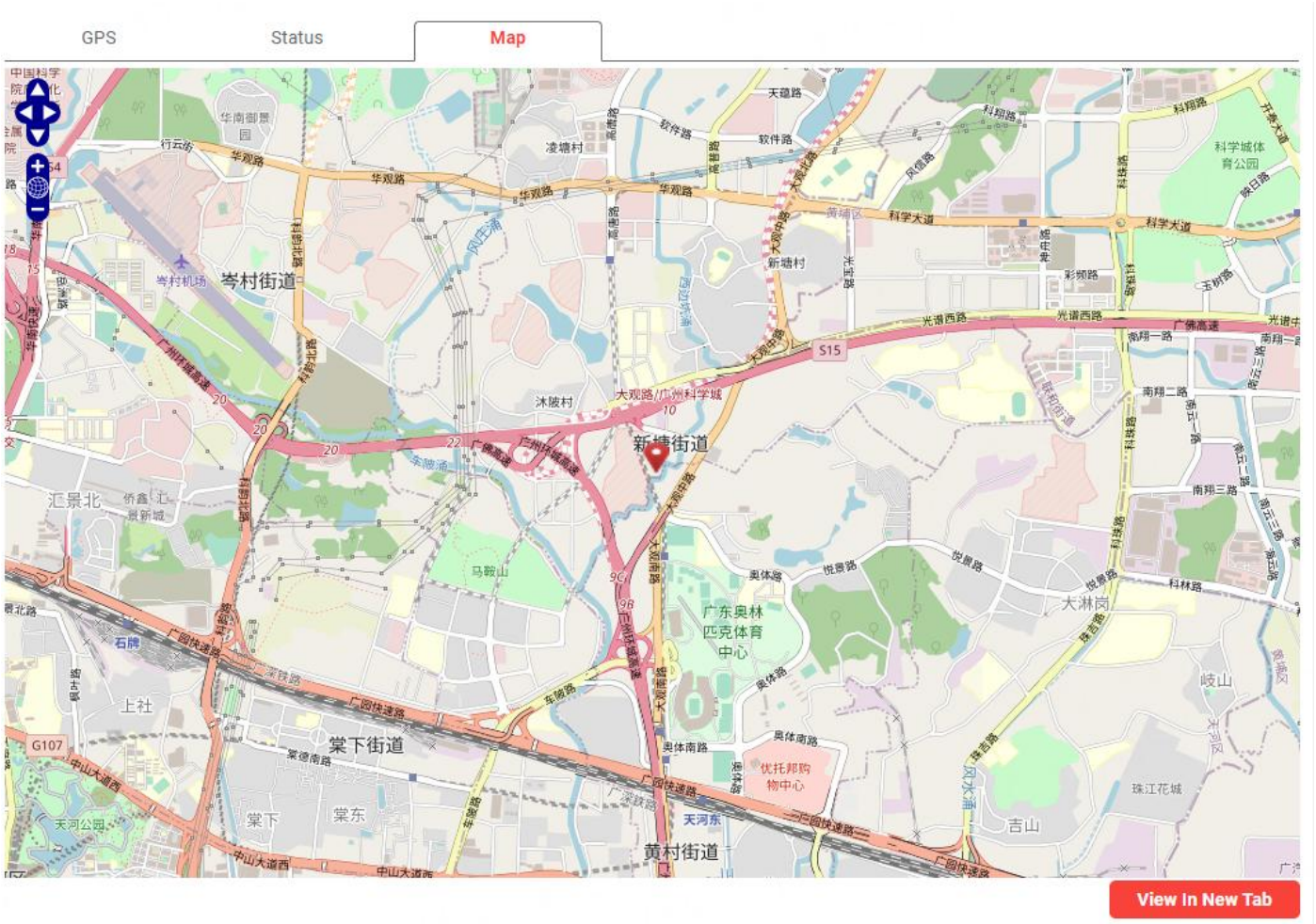
Status



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

Map

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

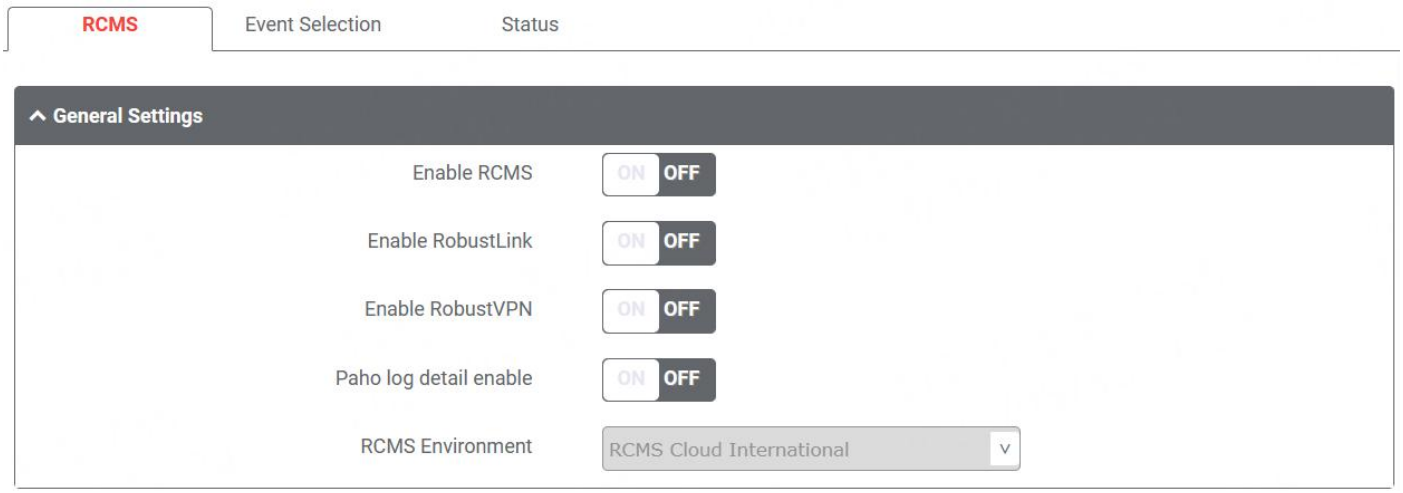


Click the View In New Tab button to view in a new tab.

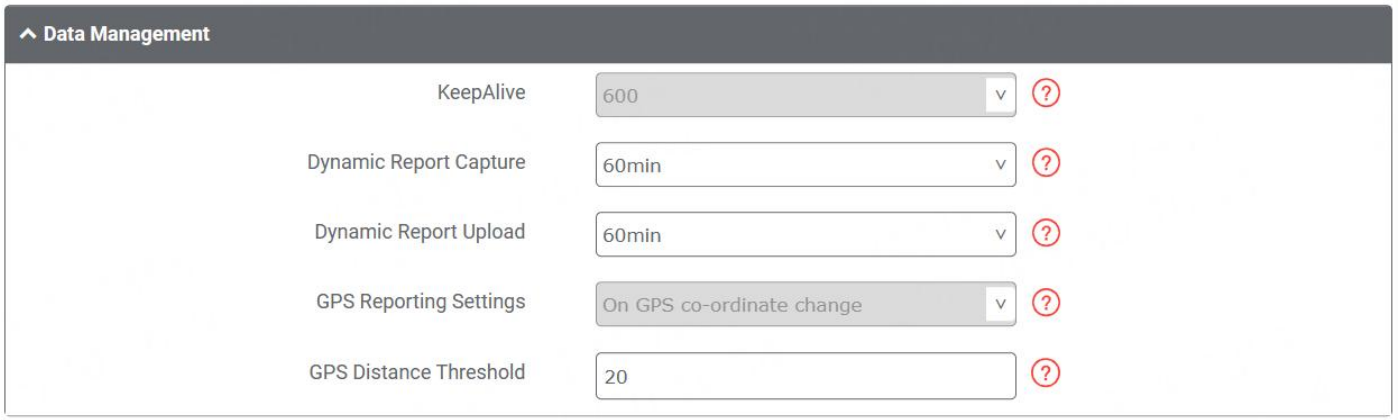
3.6.10 RCMS

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

RCMS



Item	Description	Default
Enable RCMS	Click the toggle button to enable/disable this option.	OFF
Enable RobustLink	Click the toggle button to enable/disable this option.	OFF
Enable RobustVPN	Click the toggle button to enable/disable this option.	OFF
Paho log detail enable	Click the toggle button to enable/disable this option.	OFF
RCMS Environment	Select RCMS Environment	RCMS Cloud International
RCMS URL or IP	Enter IP Address or URL of RCMS server.	rcms-cloud.robustel.net
Port	Enter the Port of RCMS.	443

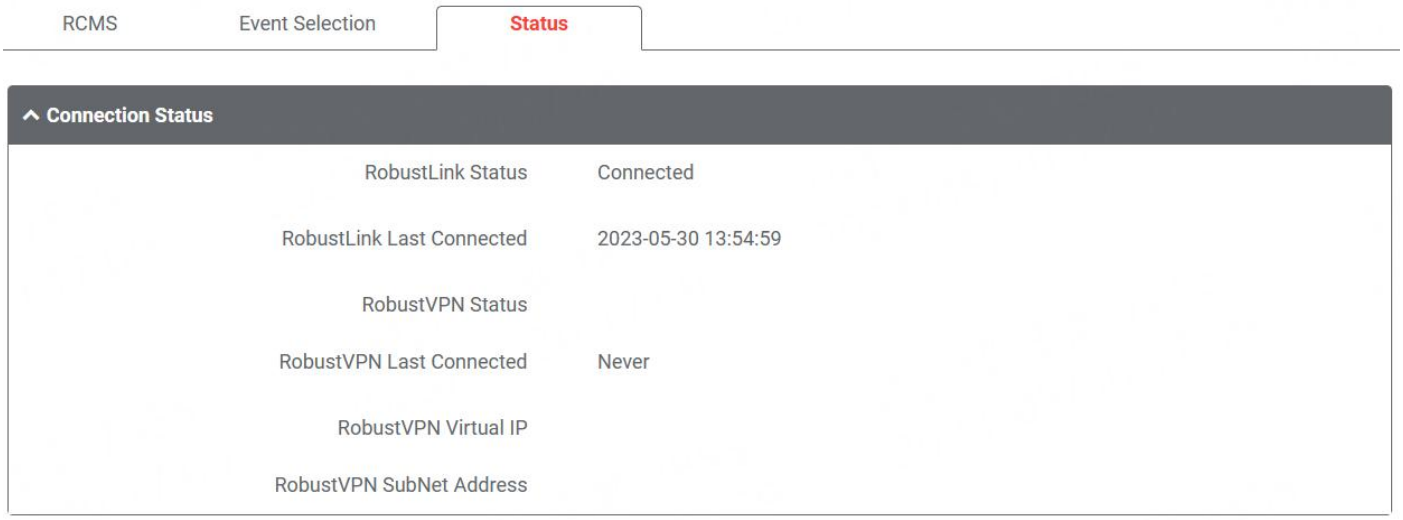


Item	Description	Default
KeepAlive	KeepAlive determines how long your device checks in with RCMS. A shorter KeepAlive will update RCMS more frequently but consume more data.	600
Dynamic Report Capture	Select the capture period of dynamic data is logged in the device	60min
Dynamic Report Upload	Select the upload period of dynamic data is update in the device	60min
GPS Reporting Settings	Select GPS Reporting way: - On GPS co-ordinate change - Report when GPS is updated - Only with Dynamic Report - Collect and report in sync with the Data Collection Interval and Data Reporting Frequency	On GPS co-ordinate change
GPS Distance Threshold	GPS data will be updated when the current position exceeds this value; Unit:meters Valid Range:10-10000	20

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

Event Selection

Status

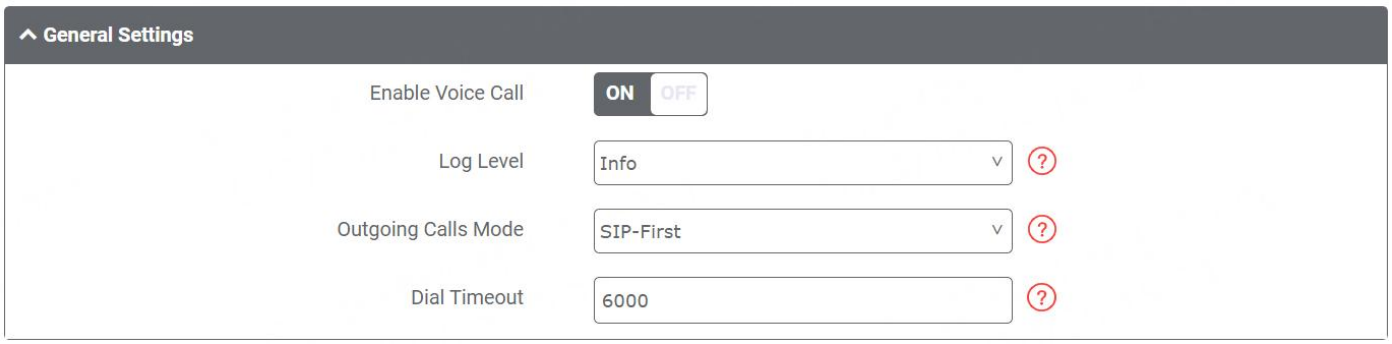


Item	Description
RobustLink Status	Show the status of RobustLink
RobustelLink Last Connected	Show the last connected times of RobustLink
RobustVPN Status	Show the status of RobustVPN
RobustVPN Last Connected	Show the last connected times of RobustVPN
RobustVPN Virtual IP	Show the virtual IP of RobustVPN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

3.6.11 Voice call (Supported in EV8100)

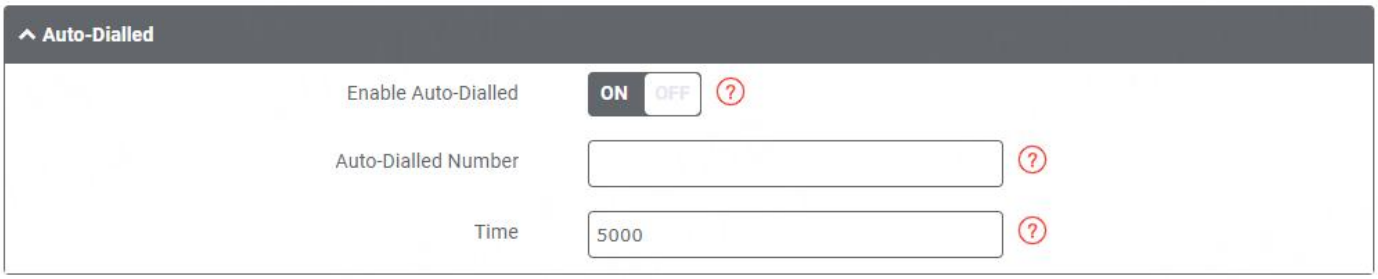
This section allows you to set the Voice Call parameters. This allows you to customize and configure parameters related to voice calls, including the SIP protocol and VoLTE protocol.

Basic Setup



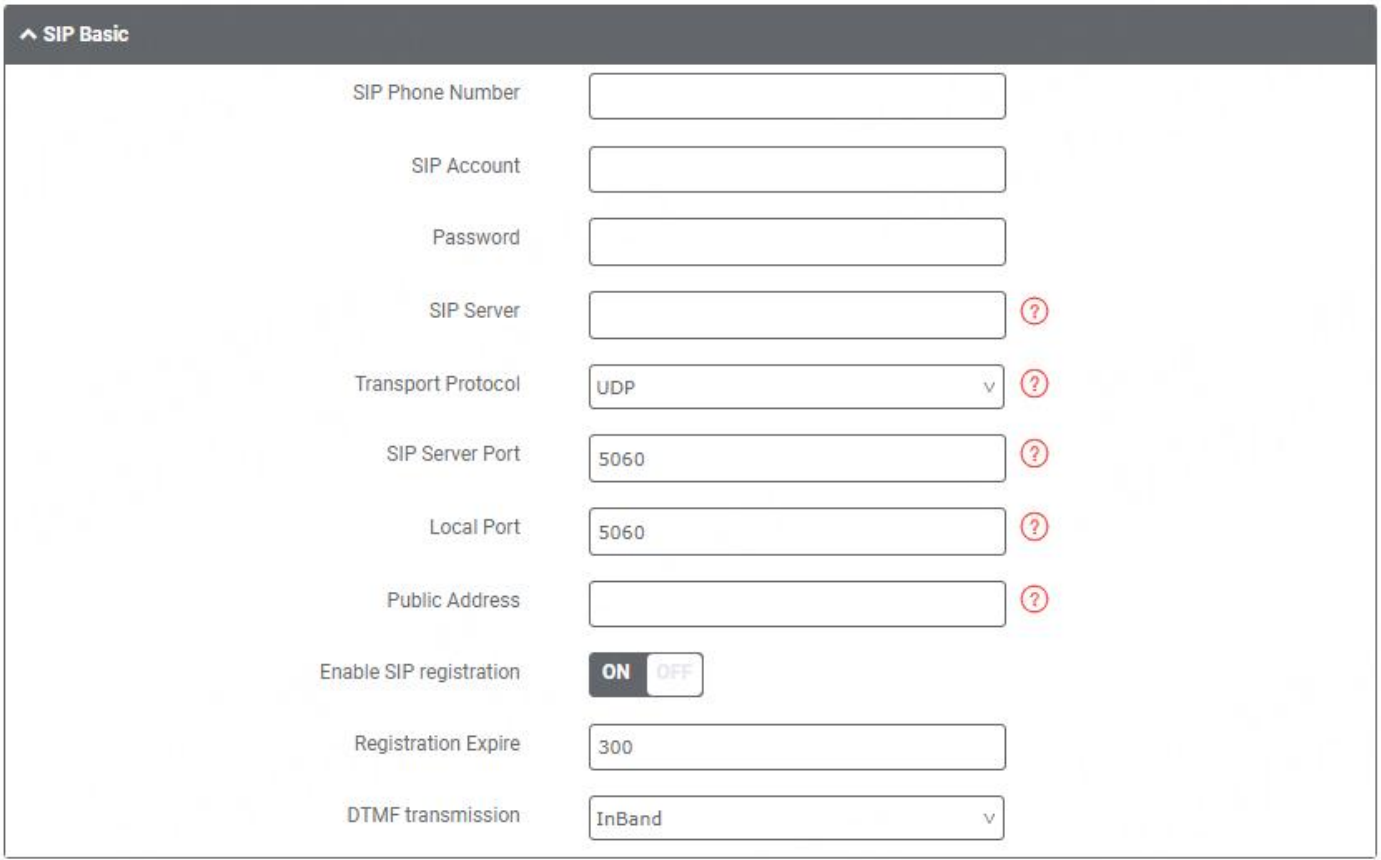
Item	Description	Default
Enable Voice Call	Click the toggle button to enable/disable this option.	ON
Log Level	Select from “Trace”,“Debug”,“Info”,“Warning”,“Error”,“Critical” or “Off”	Info

Outgoing Calls Mode	Select from “Block”,“SIP-First”,“SIP-Only” or “LTE-Only”	SIP-First
Dial Timeout	Unit: milliseconds.	6000



Item	Description	Default
Enable Auto-Dialled	Click the toggle button to enable/disable this option.	OFF
Auto-Dialled Number	The phone number to be called when Auto-Dialled is enabled.	--
Time	The time in milliseconds for the call to be made when the user does not dial after off-hooking.	5000

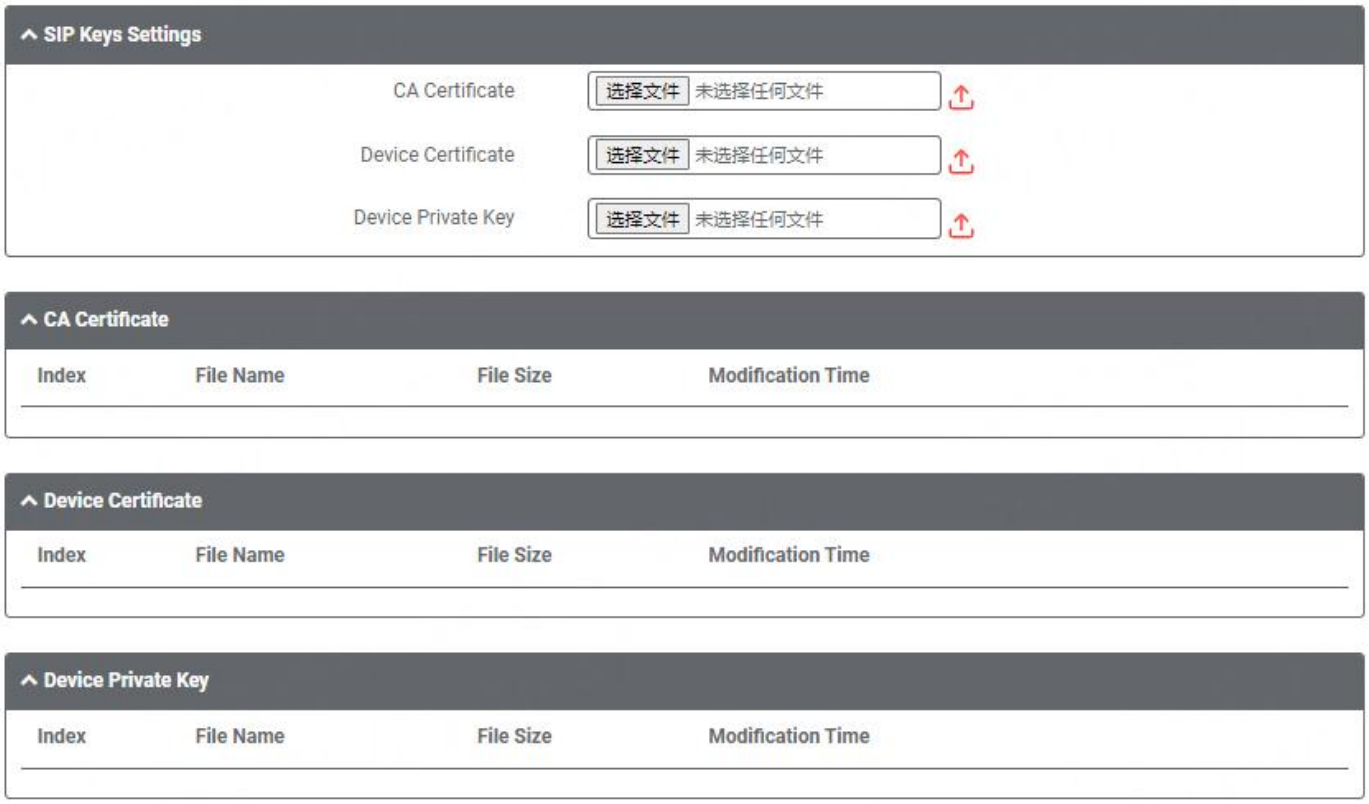
SIP



Item	Description	Default
SIP Phone Number	Enter the phone numberto identify the device uniquely for calls.	--
SIP Account	Enter the registration username for the SIP account.	--

Password	Enter the registration password.	--
SIP Server	Enter the SIP Proxy server URL.	--
Transport Portocol	Select the SIP signaling method. Select from “UDP”,“TCP”,“TLS” or “UDP+TCP”.	UDP
SIP Server Port	Set the server port.	5060
Local Port	Set the local port.	5060
Public Address	Enter the public address.	--
Enable SIP registration	Click the toggle button to enable/disable the registration by SIP calls.	ON
Registration Expire	Enter the re-registration timeout.	300
DTMF transmission	Set the DTMF transmission method. Select from “InBand”,“RTP RFC2833” or “SIP INFO”.	InBand

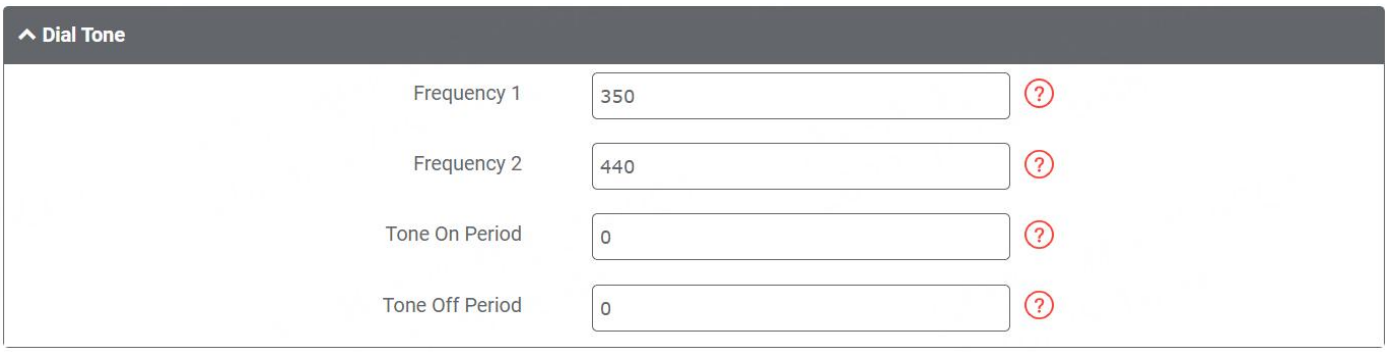
SIP Certificate



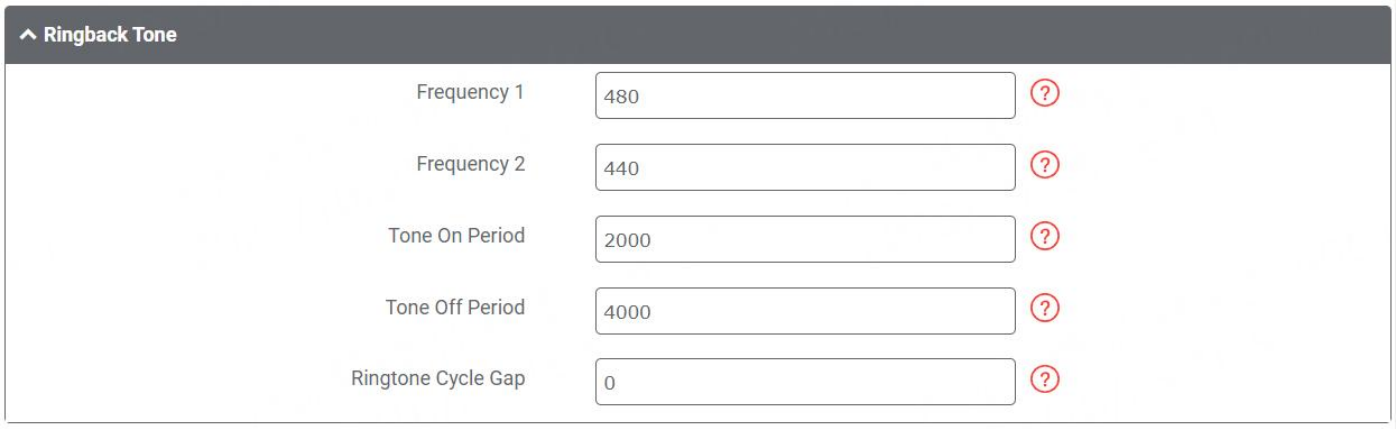
VoLTE

Item	Description	Default
DTMF transmission	Select from “InBand” or “RTP RFC2833”.	InBand

Telephony

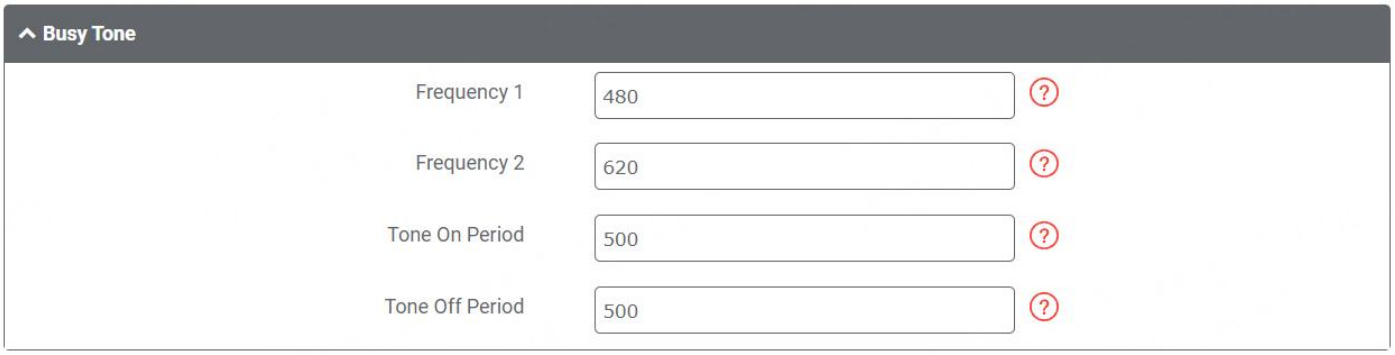


Item	Description	Default
Frequency 1	The frequency(Hz) of the first dial tone, 0 for no signal output.	350
Frequency 2	The frequency(Hz) of the second dial tone, 0 for no signal output.	440
Tone On Period	The duration(ms) of the dial tone active, 0 for disable dial tone only as off_duration > 0.	0
Tone Off Period	The duration(ms) of the dial tone inactive, 0 for continuous.	0

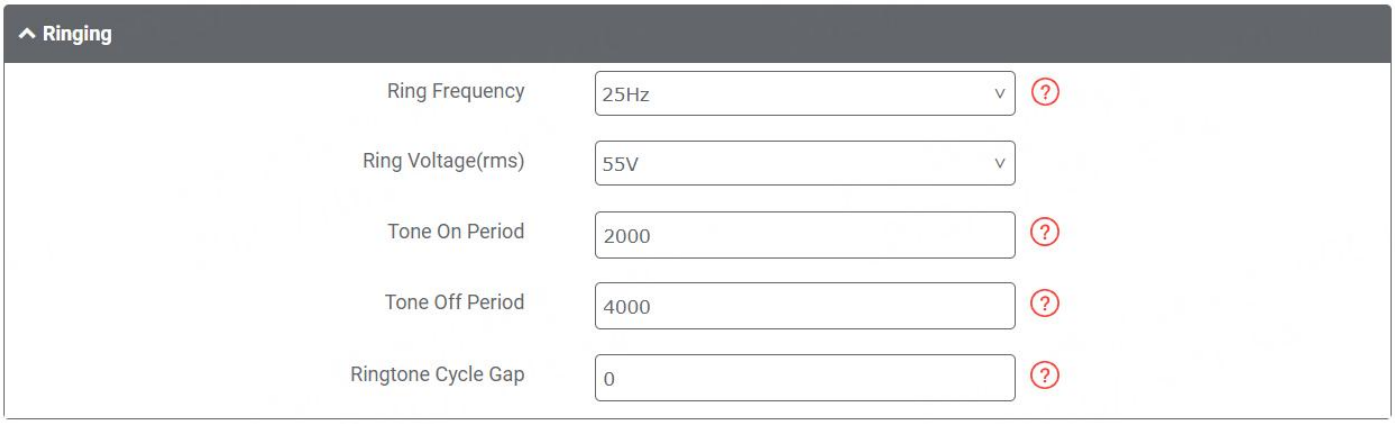


Item	Description	Default
Frequency 1	The frequency(Hz) of the first ringback tone, 0 for no signal output.	480
Frequency 2	The frequency(Hz) of the second ringback tone, 0 for no signal output.	440

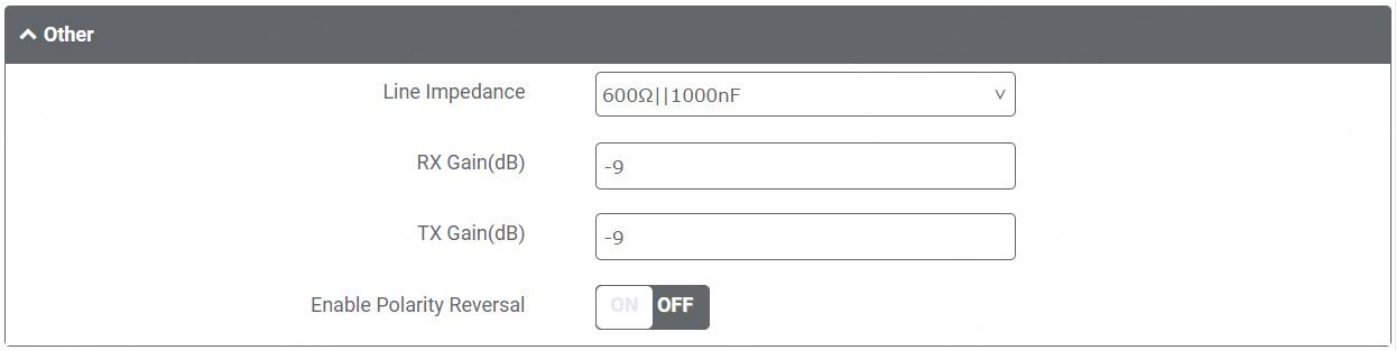
Tone On Period	The duration(ms) of the ringback tone active, 0 for disable ringback tone only as off_duration > 0.	2000
Tone Off Period	The duration(ms) of the ringback tone inactive, 0 for continuous.	4000
Ringtone Cycle Gap	The duration(ms) of the gap.	0



Item	Description	Default
Frequency 1	The frequency(Hz) of the first busy tone, 0 for no signal output.	480
Frequency 2	The frequency(Hz) of the second busy tone, 0 for no signal output.	620
Tone On Period	The duration(ms) of the busy tone active, 0 for disable busy tone only as off_duration > 0.	500
Tone Off Period	The duration(ms) of the busy tone inactive, 0 for continuous.	500



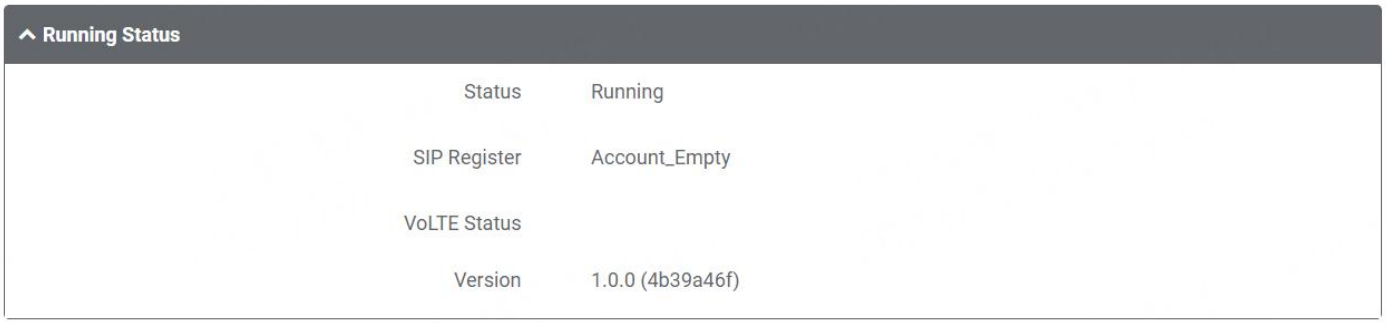
Item	Description	Default
Ring Frequency	The frequency(Hz) of ringing. Select from“16Hz”,“25Hz” or “50Hz”.	25Hz
Ring Voltage(rms)	Select from“35V”,“45V”,“50V” or “55V”.	55V
Tone On Period	The duration(ms) of the busy tone active.	2000
Tone Off Period	The duration(ms) of the busy tone inactive, 0 for continuous.	4000
Ringtone Cycle Gap	The duration(ms) of the gap.	0



Item	Description	Default
Line Impendance	Select from“600 Ω ”,“270 Ω +750 Ω ||150nF”,“370 Ω +620 Ω ||310nF”,“220 Ω +820 Ω ||120nF”, “600 Ω ||1000nF”,“200 Ω +680 Ω ||100nF” or “220 Ω +820 Ω ||115nF”.	600 Ω
RX Gain(dB)	Enter the RX Gain.	-9
TX Gain(dB)	Enter the TX Gain.	-9
Enable Polarity Reversal	Click the toggle button to enable/disable this option.	OFF

Status

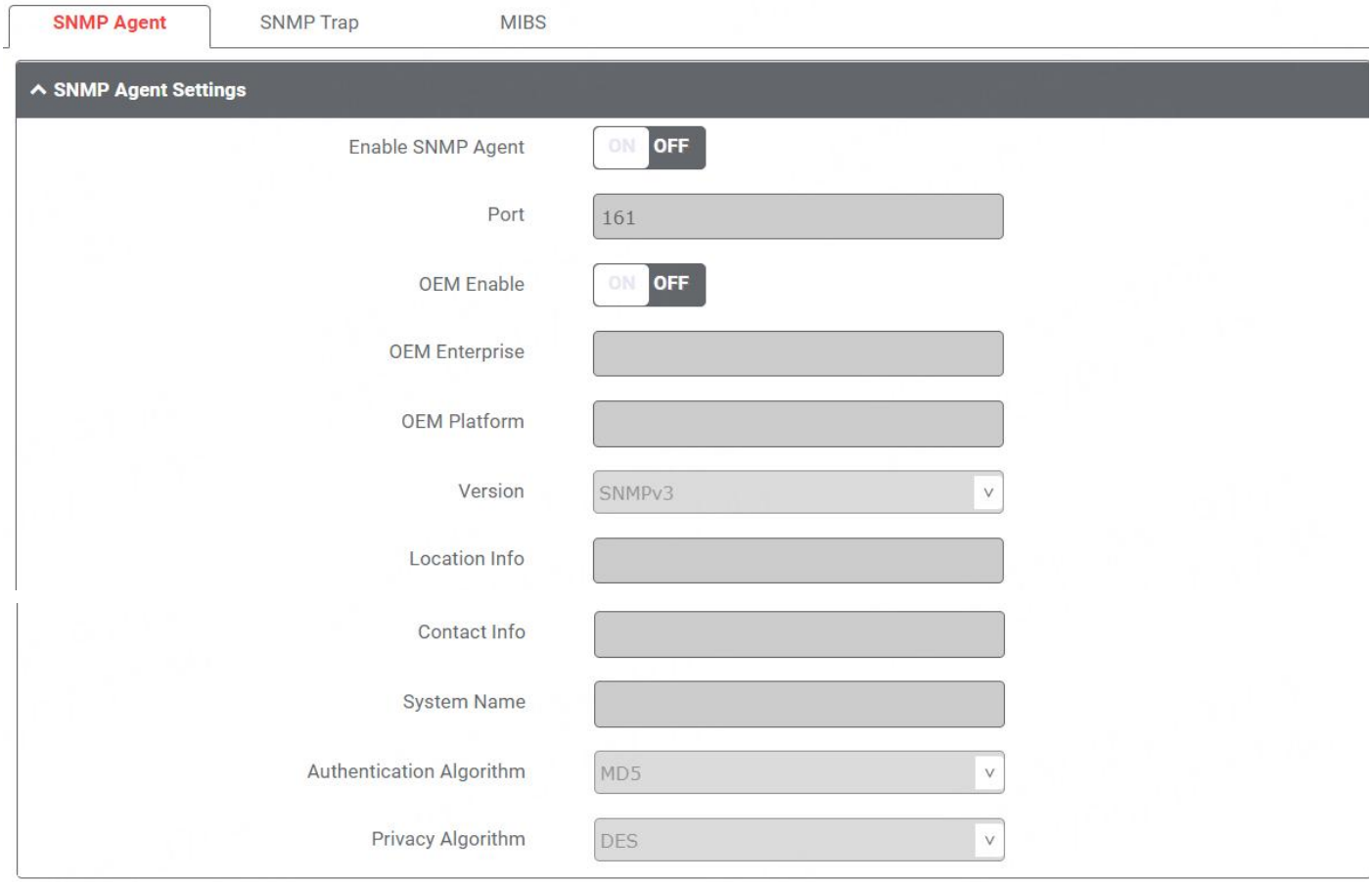
This page allows you to view the status of SIP or VoLTE.



3.6.12 SNMP

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

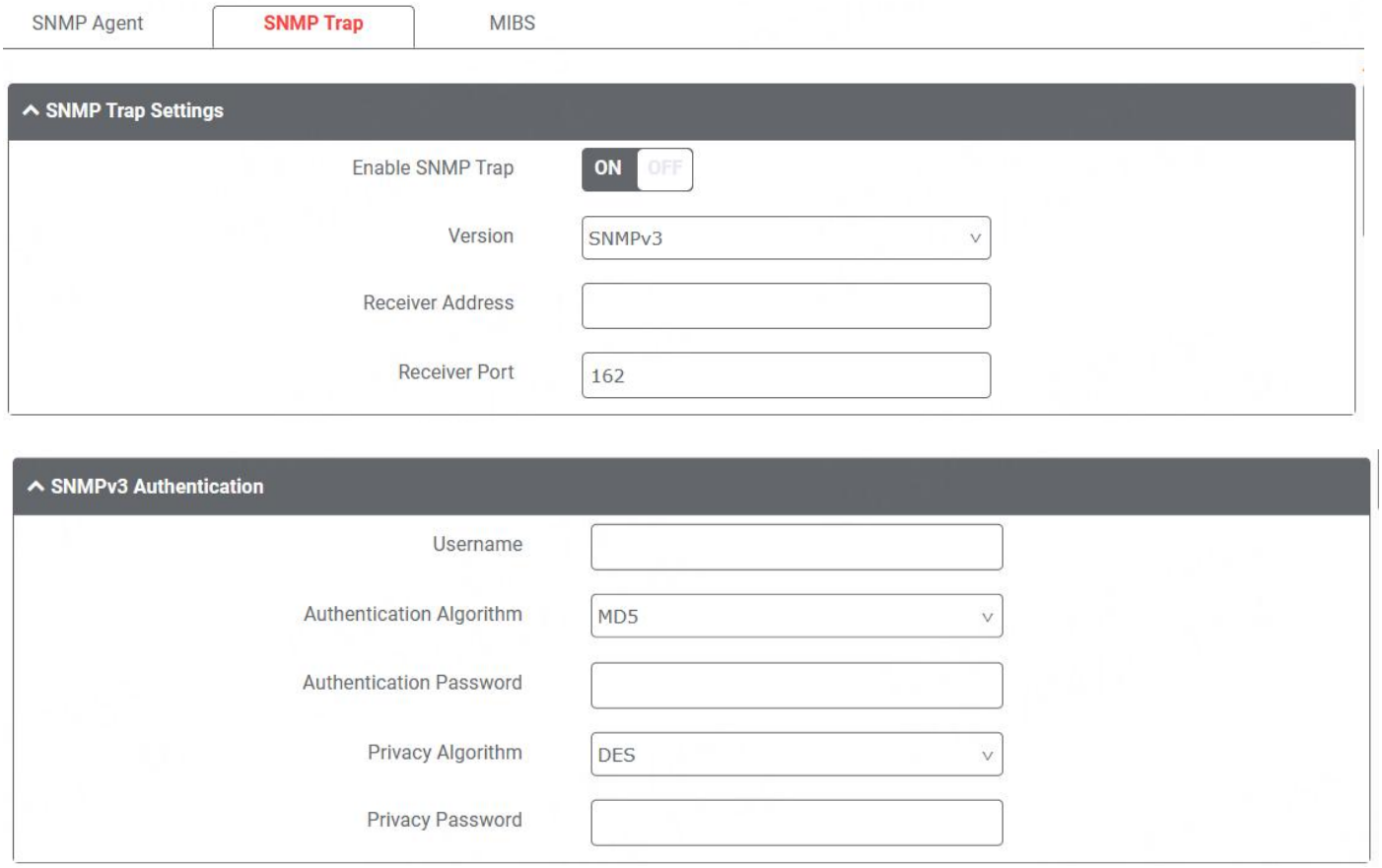
SNMP Agent



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

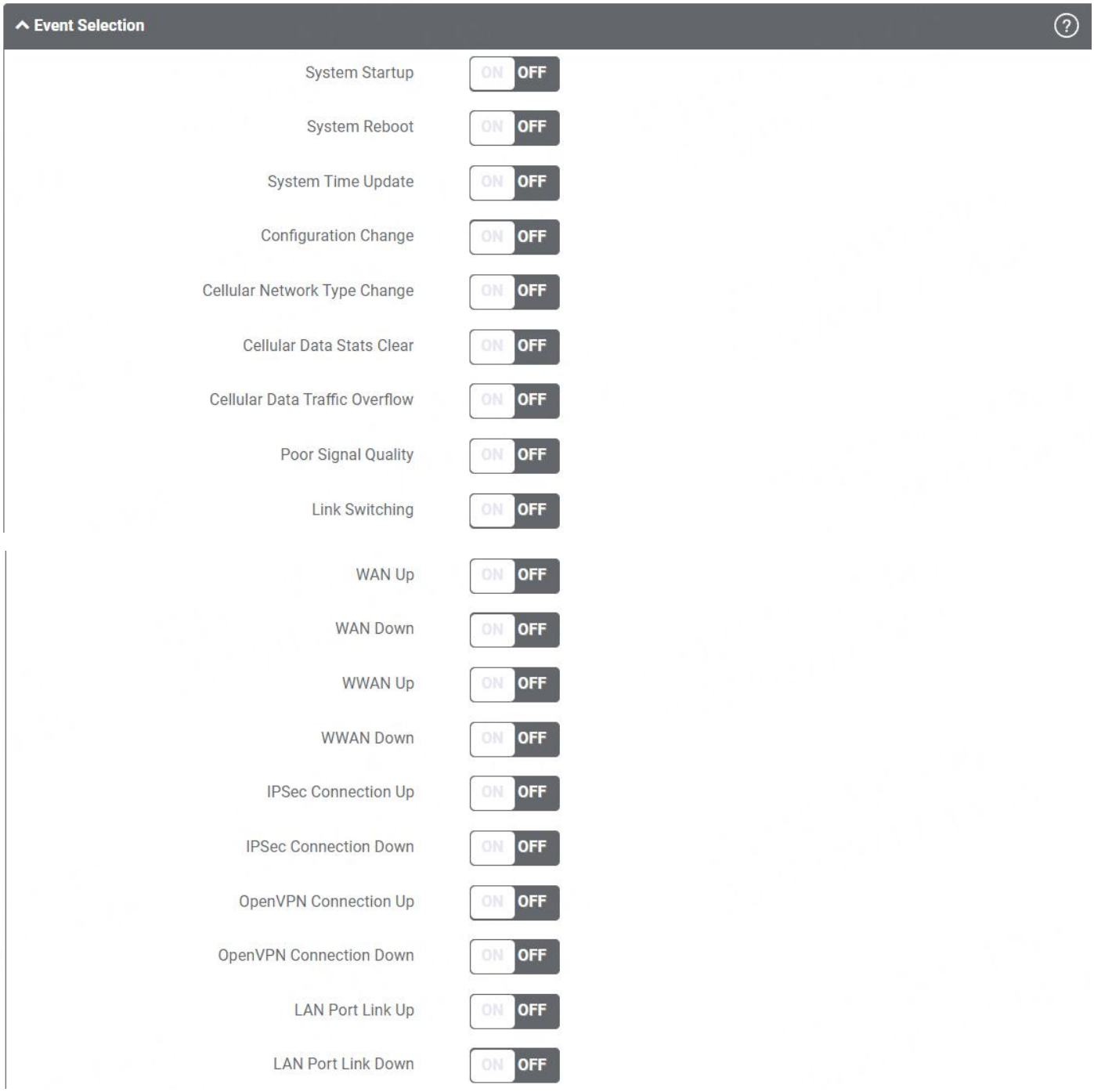
SNMP Trap

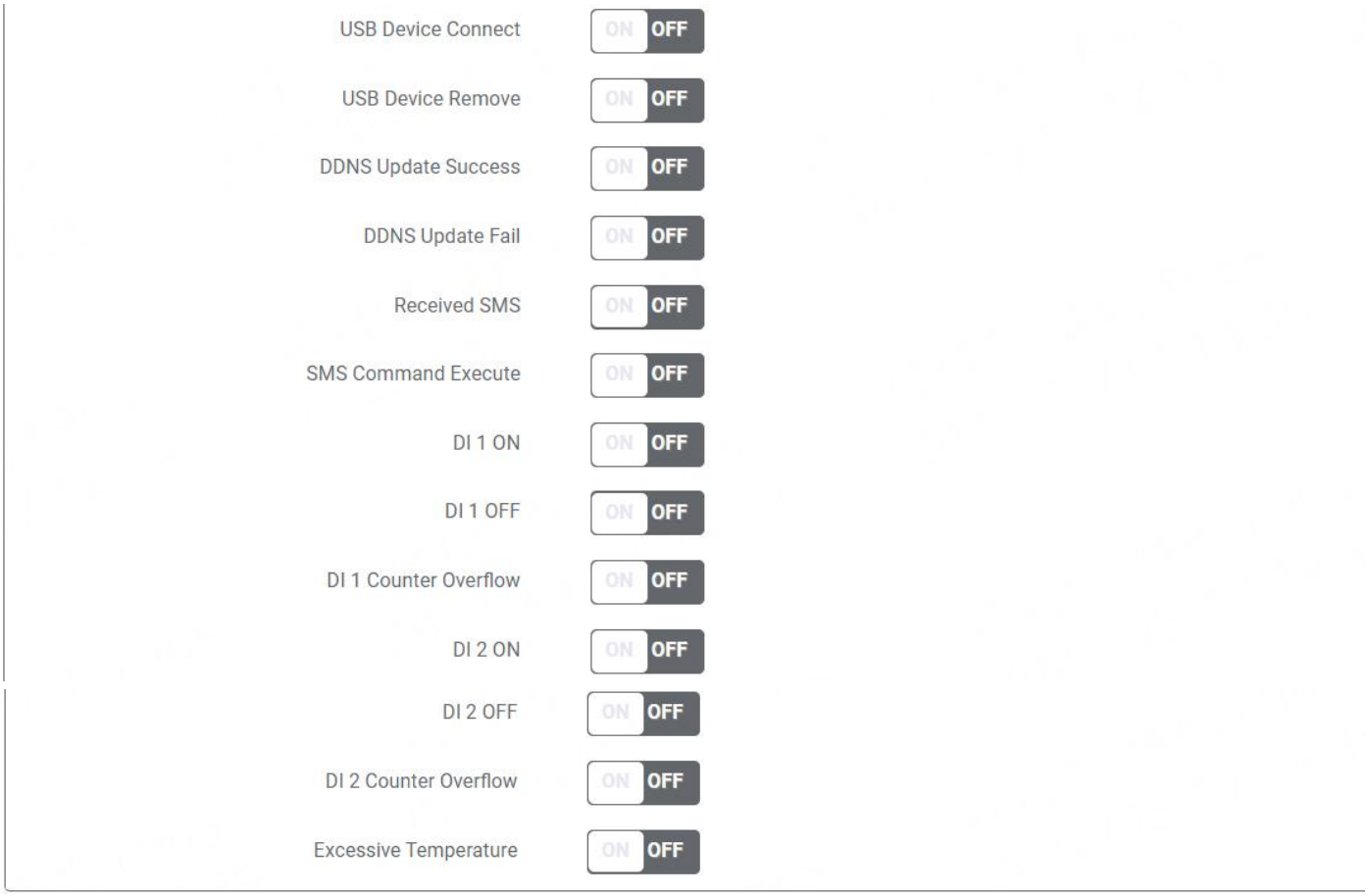
SNMP Trap Rules are alerts that trigger when certain user-specified events occur. When the trigger event happens, the trap will notify known SNMP hosts.



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

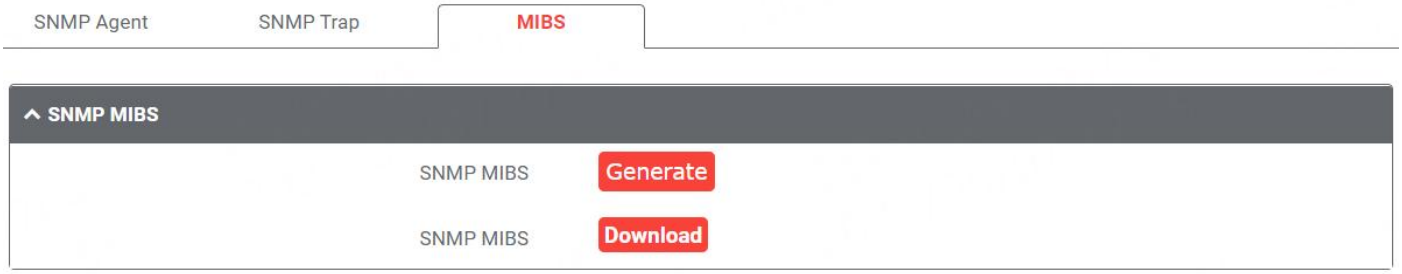
Click the toggle button the enable or disable the related event.


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



MIBS

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

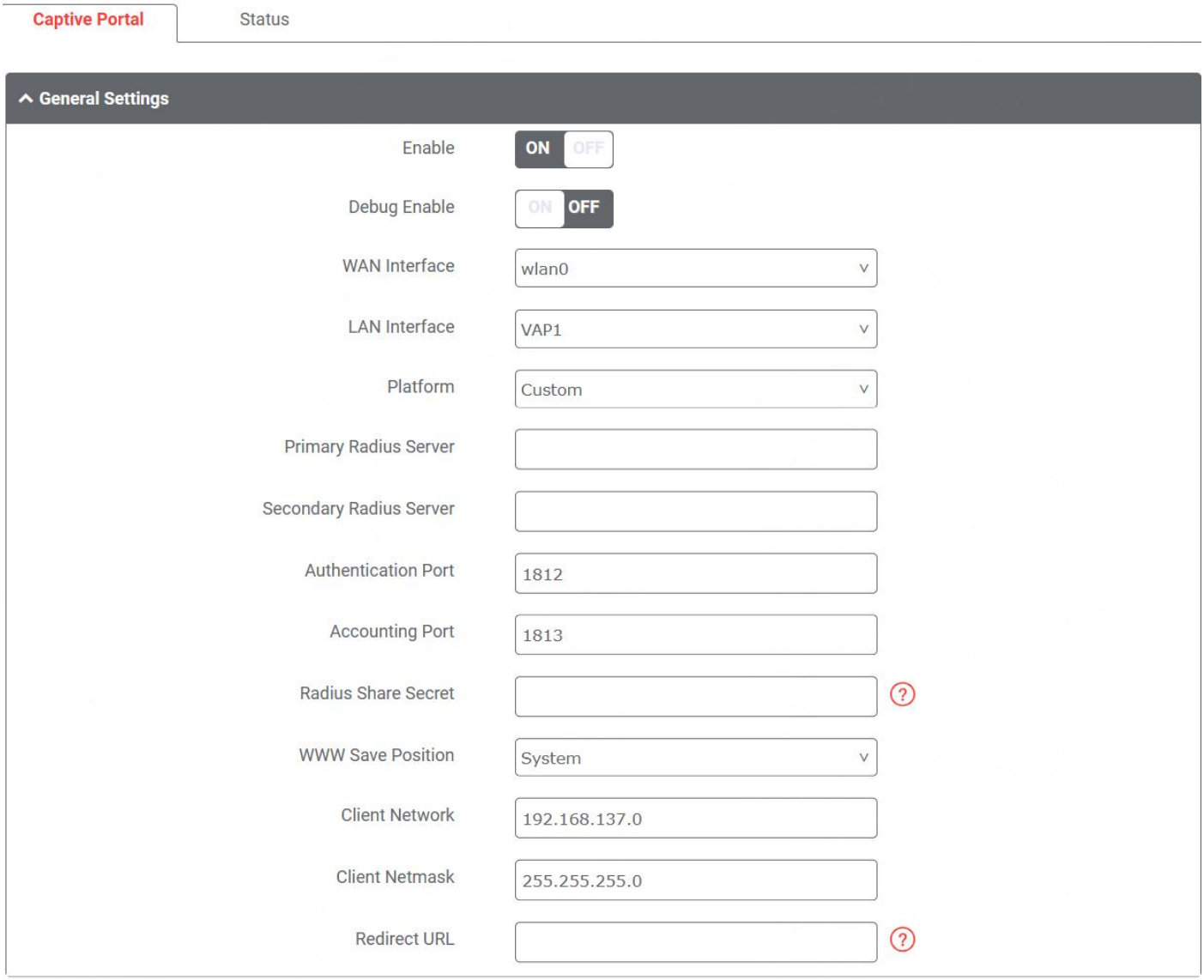


Item	Description	Default
MIBS	Click Generate to generate and click Download to download the device's MIB file.	--

3.6.13 Captive Portal

Captive Portal

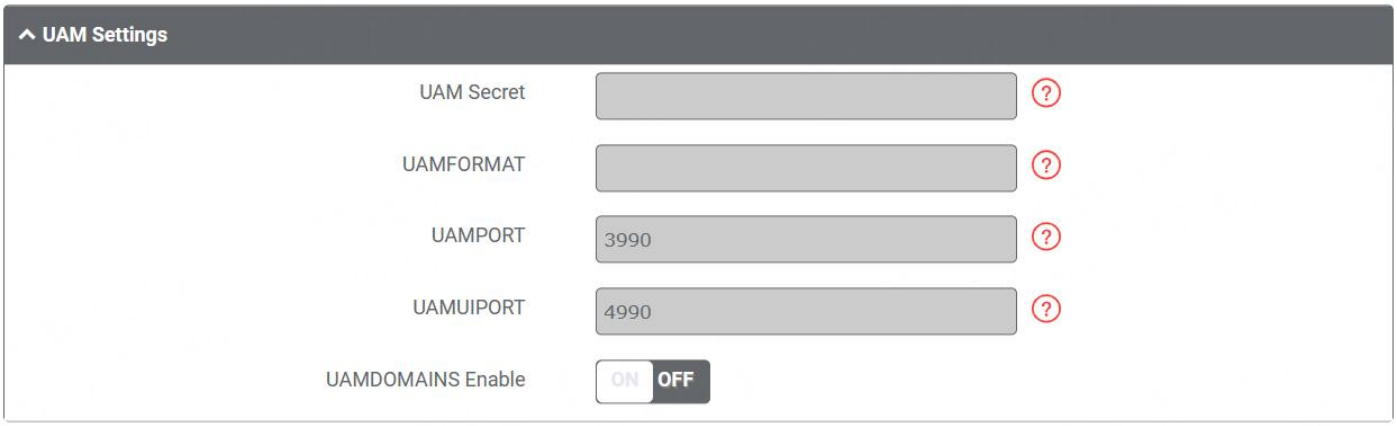
This section allows you to modify the parameters of Captive Portal.
Captive Portal is a web-based authentication setup that serves as a "login" page presented to users by network operators or devices before they can access the internet.



Item	Description	Default
Enable	Click the toggle button to enable/disable this option.	OFF
Debug Enable	Click the toggle button to enable/disable debug mode. When debug mode enabled, the captive portal running log will be displayed in syslog.	OFF
WAN Interface	Select WAN Interface.	wlan0
LAN Interface	Select LAN Interface.	VAP1
Platform	Select a radius platform.	Custom

Primary Radius Server	Enter the Primary Radius Server.	Null
Secondary Radius Server	Enter the Secondary Radius Server.	Null
Authentication Port	Enter the Radius Server 's Authentication Port.	1812
Accounting Port	Enter the Radius Server 's Accounting Port.	1813
Radius Share Secret	Enter the Radius Share Secret, it is a security setting used in RADIUS servers and clients to establish a secure communication channel. Usually in 8 - 128 characters.	
WWW Save Position	Select the WWW Save Position, the WWW information will save in the specific position	System
Client Network	Enter the Client Network. If the client IP address is within the range, the RADIUS server assumes that the request comes from a trusted client and proceeds with the authentication process.	192.168.137.0
Client Netmask	Enter the Client Netmask. If the client Netmask is within the range, the RADIUS server assumes that the request comes from a trusted client and proceeds with the authentication process.	255.255.255.0
Redirect URL	Enter the Redirect URL. It will be redirected to this URL after authentication success	Null

UAM (Universal Access Method) is a technology used for user authentication and authorization in Wi-Fi networks. Here is the parameter settings for Captive Portal.

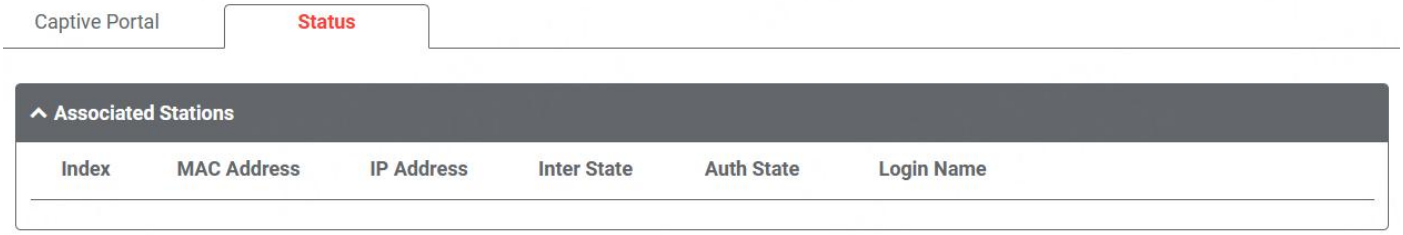


Item	Description	Default
UAM Secret	Enter the UAM Secret. UAM Secret is a security key used in the authentication process between a wireless access point and a RADIUS server. Usually use 5 - 128 characters.	Null
UAM Format	UAM Format refers to the format of the web page that is presented to users for authentication in UAM systems.	Null
UAM Port	The UAM Port is used to send authentication requests and responses between the device and the authentication server.	3990
UAM UI Port	UAM UI Port is used to serve the authentication web page to the user's browser, and to receive the user's authentication credentials.	4990
UAM Domains Enable	UAM Domain refers to the domain or subdomain that is used to host the login or captive portal page for a user authentication and management system.	OFF

	Click the toggle button to enable/disable this option.	

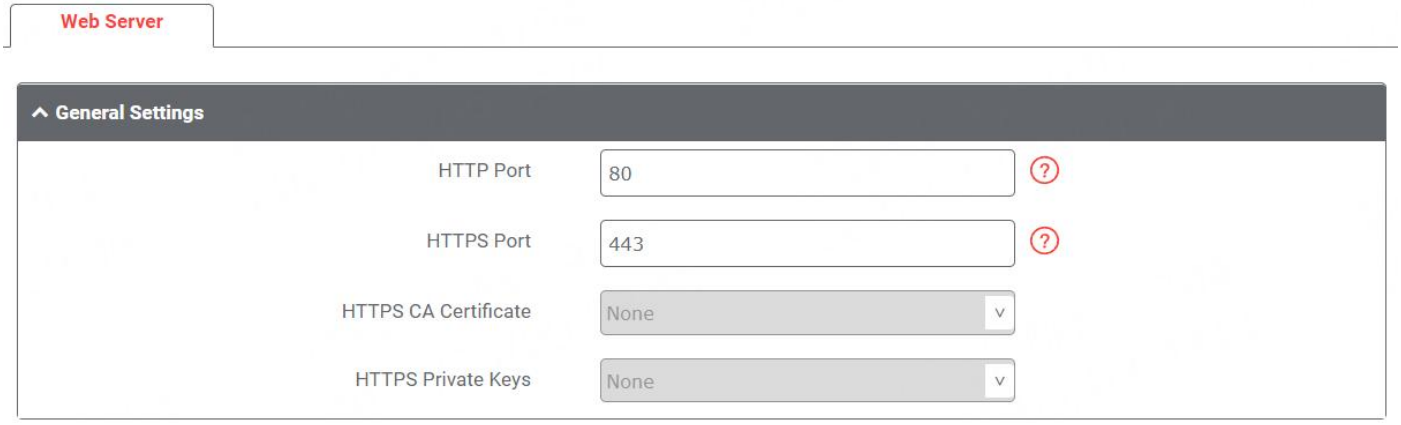
Status

The status bar allows you to view Captive Portal associated stations status.



3.6.14 Web Server

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

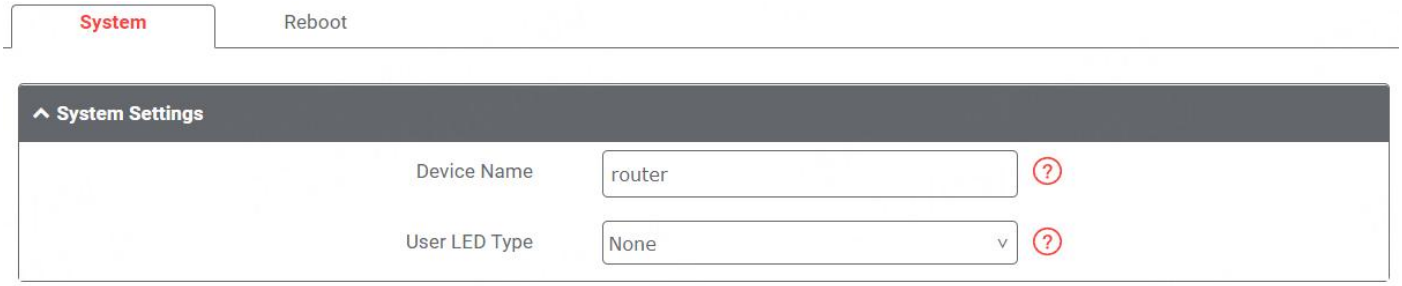


Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in router's Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port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

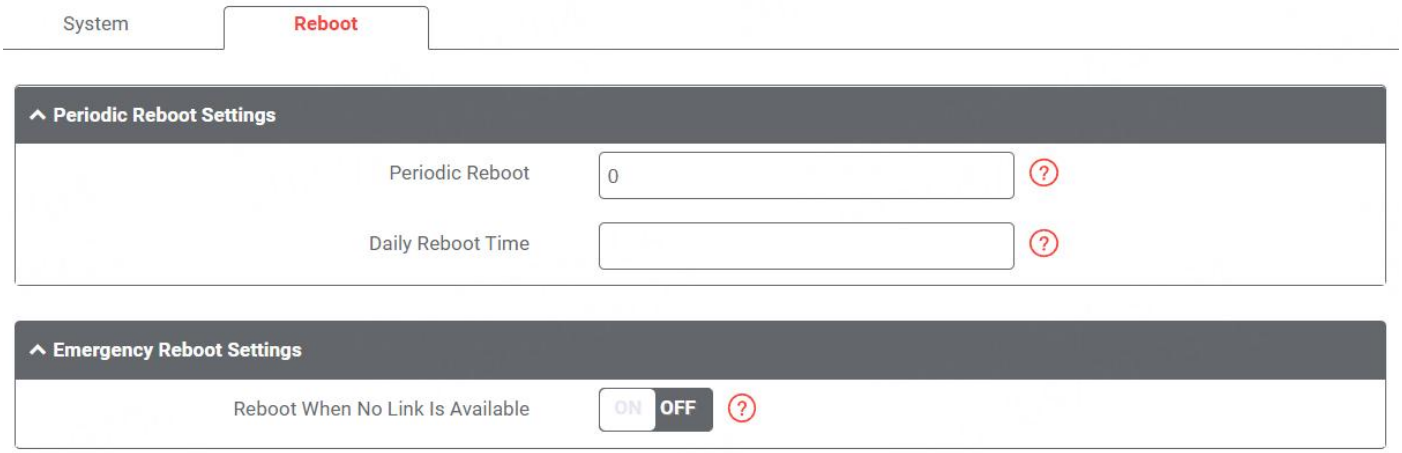
HTTPS CA Certificate	Select one once the certification is imported, see 3.7.2 Certificate Manager	
HTTPS Private Keys	Select one once the certification is imported, see 3.7.2 Certificate Manager	

3.6.15 Advanced

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



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



Periodic Reboot Settings		
Item	**Description**	**Default**
Periodic Reboot	Set the reboot period of the router. 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the router. You should follow the format as HH:	Null

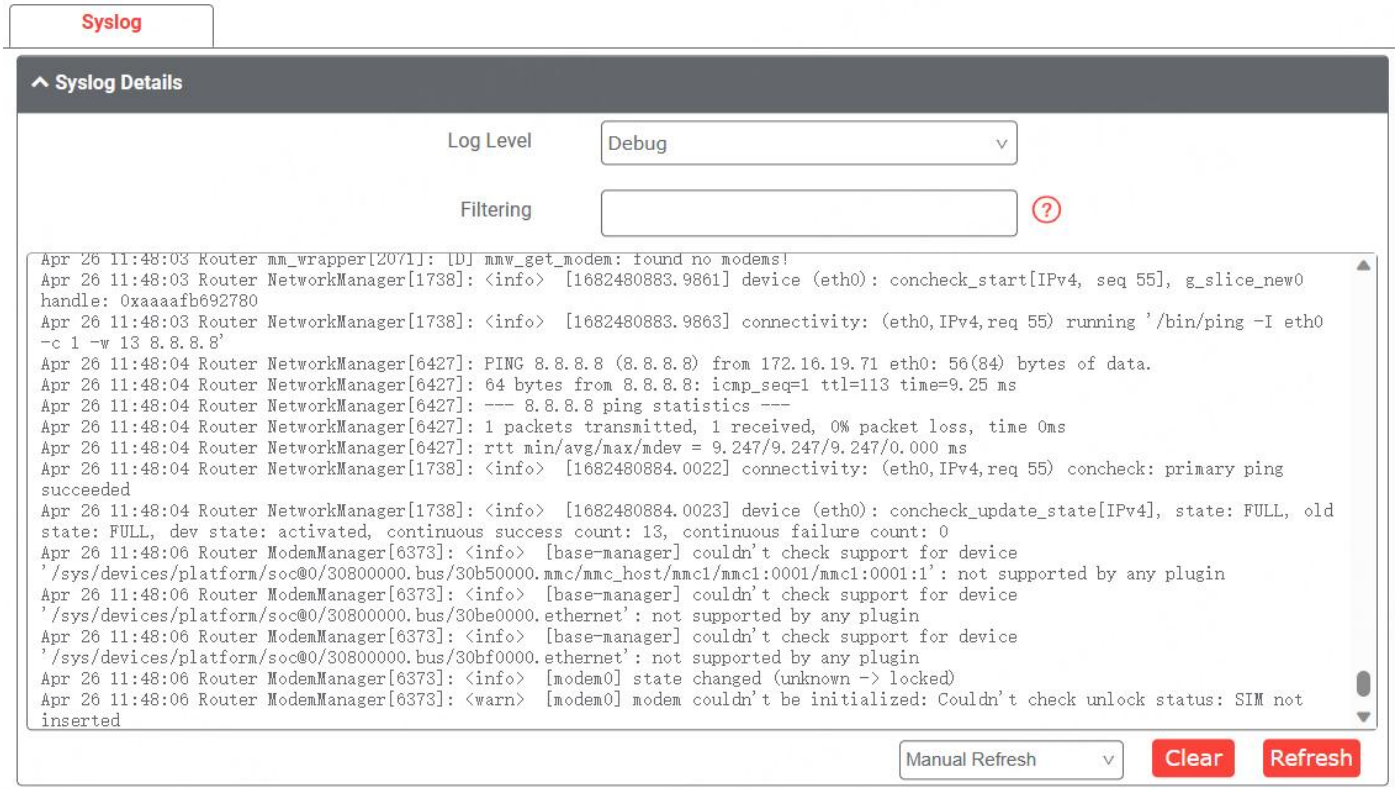
	MM, in 24h time frame, otherwise the data will be invalid. Leave it empty means disable.	
Reboot When No Link Is Available	Click the toggle button to enable/disable this option.	OFF

3.7 System

3.7.1 Debug

3.6.1 Debug

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



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

Refresh	Click the button to refresh the syslog.	--

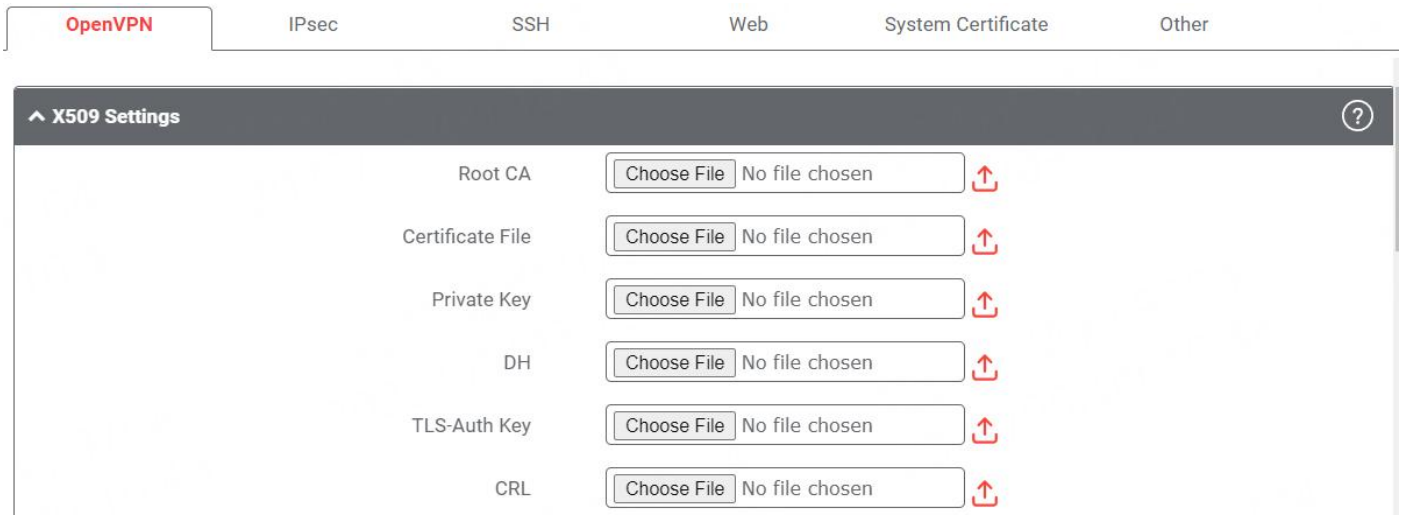
Item	Description	Default
System Journal File	Click Generate to generate and click Download to download the system journal file.	--

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

3.7.2 Certificate Manager

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

OpenVPN

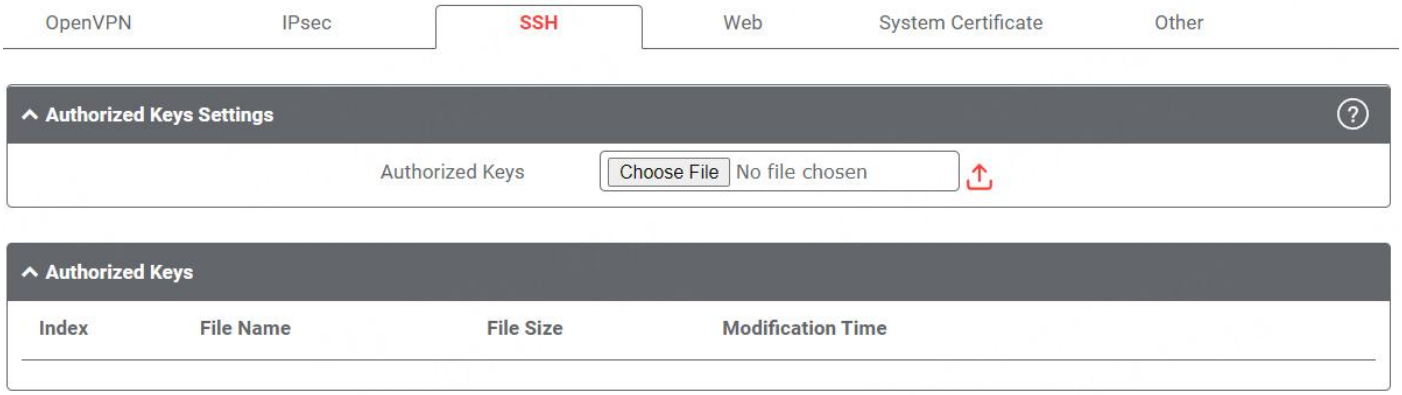


Item	Description	Default
Root CA	Click on Choose File to locate the root ca file, and then click on to import this file into your device.	--
Certificate File	Click on Choose File to locate the certificate file, and then click on to import this file into your device.	--
Private Key	Click on Choose File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

IPsec

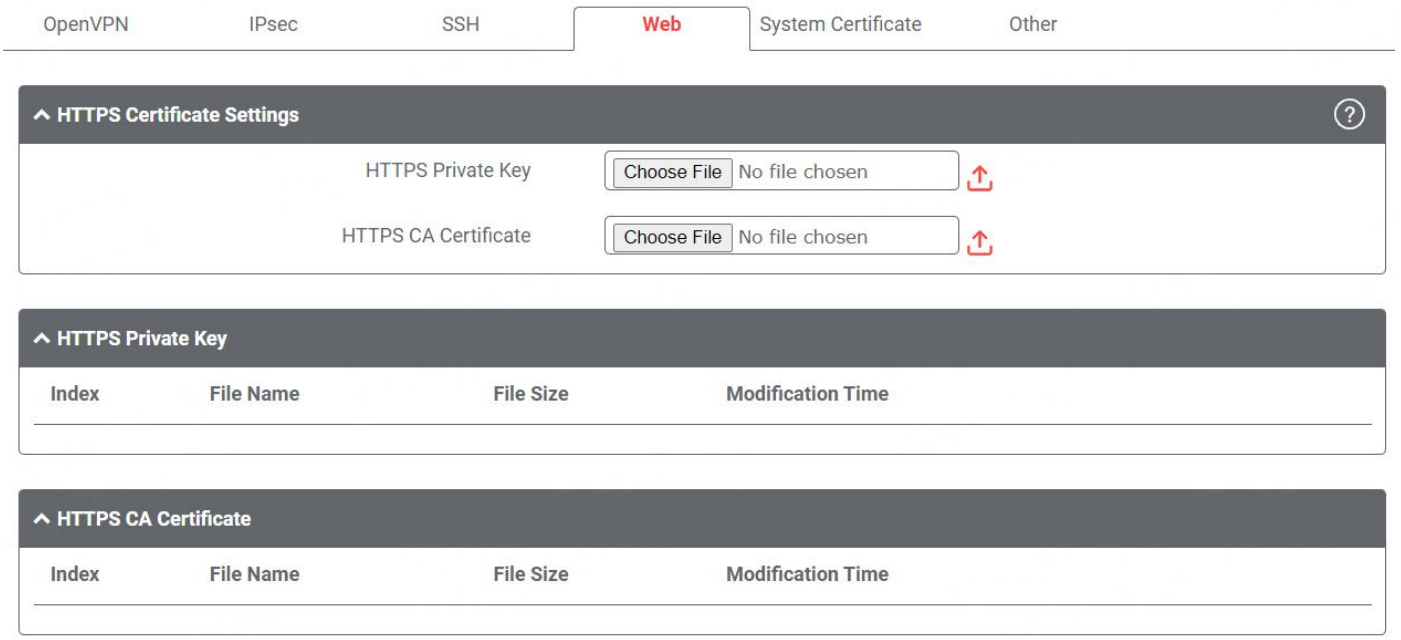
Item	Description	Default
Local Certificate	Click on Choose File to locate the Local Certificate file, and then click on to import this file into your device.	--
Remote Certificate	Click on Choose File to locate the Remote Certificate file, and then click on to import this file into your device.	--
Private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

SSH



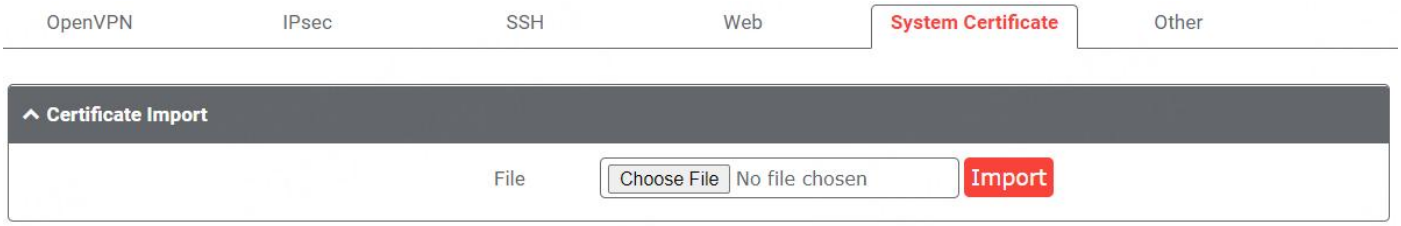
Item	Description	Default
Authorized Keys	Click on Choose File to locate the Authorized Keys file, and then click on to import this file into your device.	--

Web



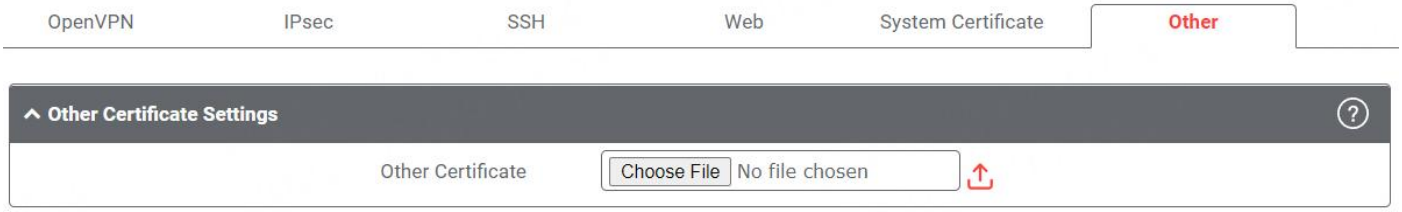
Item	Description	Default
HTTPS Private Key	Click on Choose File to locate the Authorized Keys file, and then click on to import this file into your device.	--
HTTPS CA Certificate	Click on Choose File to locate the Certificate file, and then click on to import this file into your device.	

System Certificate



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

Other

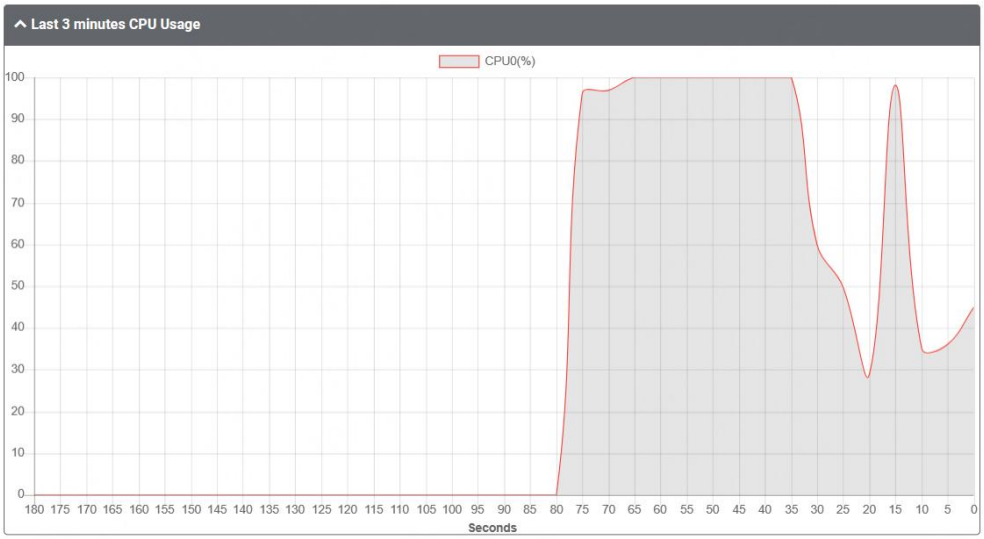


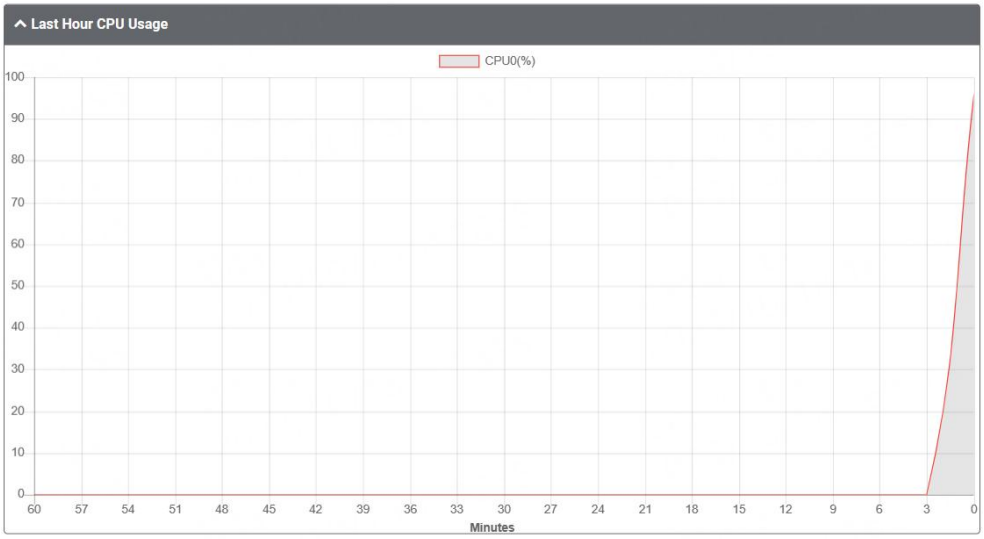
Item	Description	Default
Other Certificate	Click on Choose File to locate the Other Certificate file, and then click on to import this file into your device.	--

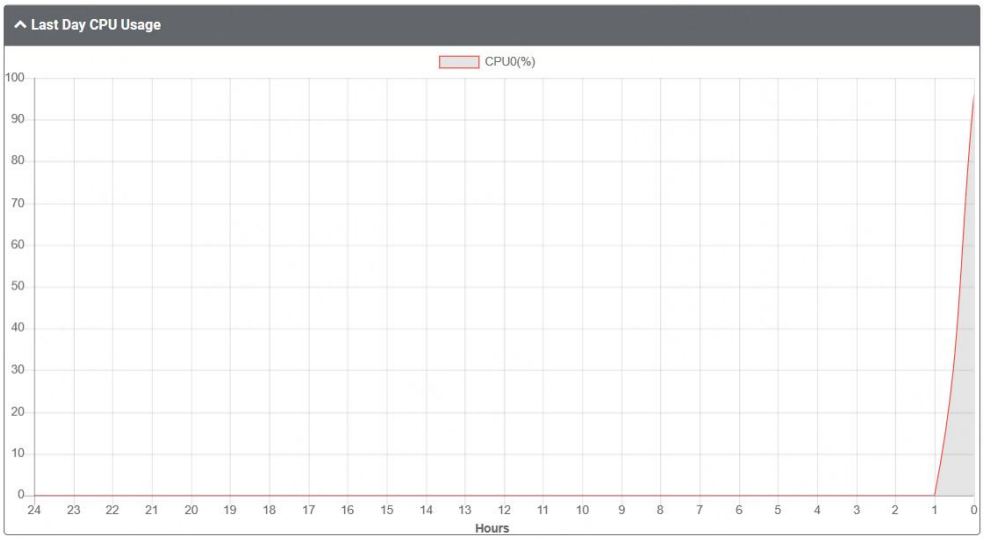
3.7.3 Resource Graph

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

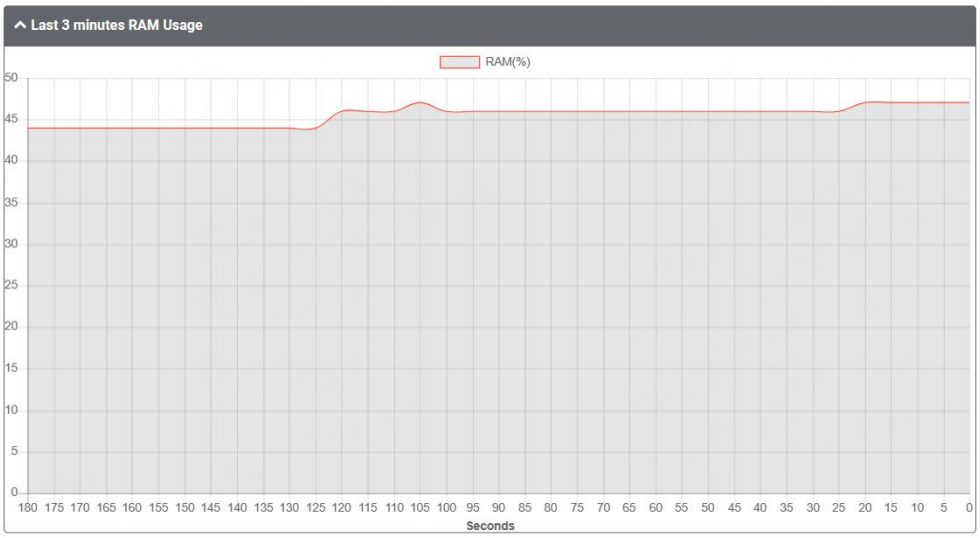
CPU Usage

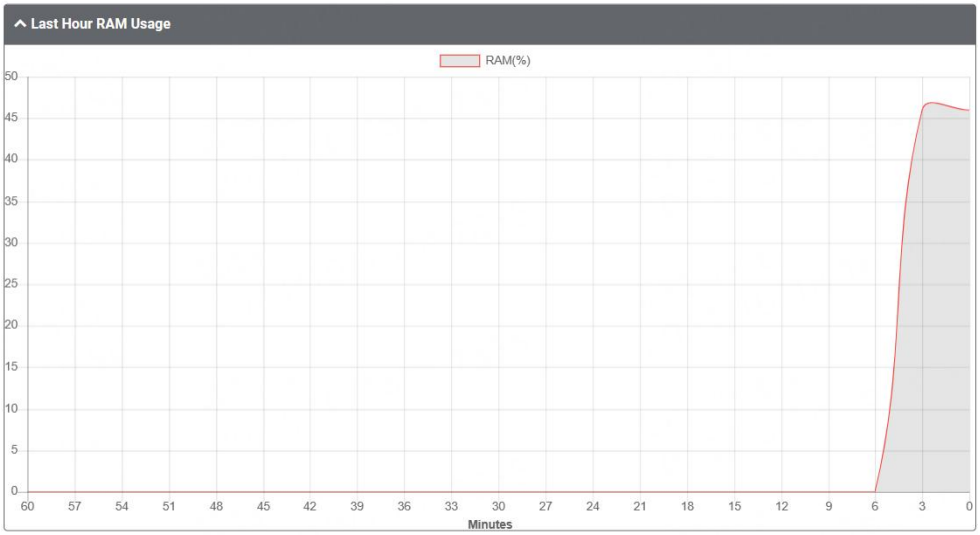

Last 3 minutes CPU Usage
CPU0(%)
100 90 80 70 60 50 40 30 20 10 0
180 175 170 165 160 155 150 145 140 135 130 125 120 115 110 105 100 95 90 85 80 75 70 65 60 55 50 45 40 35 30 25 20 15 10 5 0
Seconds

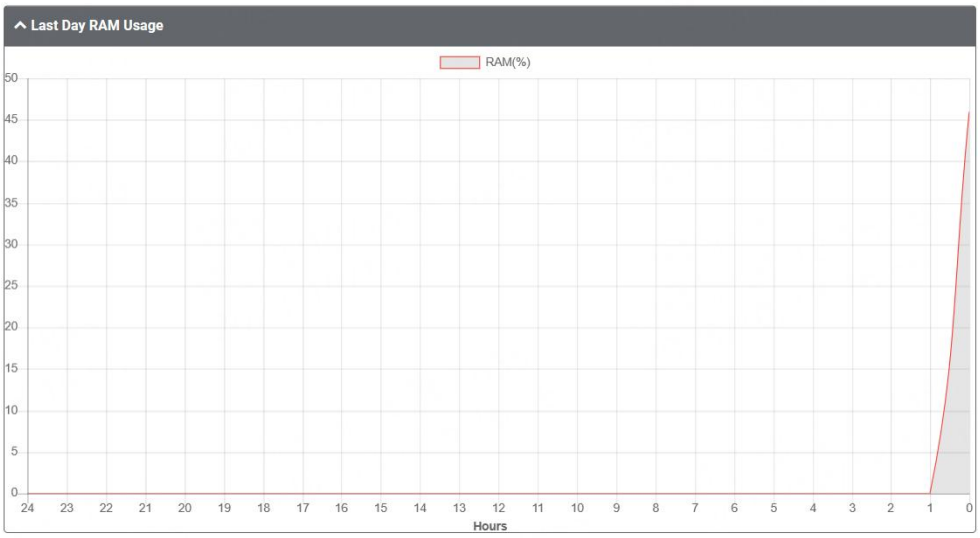

Last Hour CPU Usage
CPU0(%)
100 90 80 70 60 50 40 30 20 10 0
60 57 54 51 48 45 42 39 36 33 30 27 24 21 18 15 12 9 6 3 0
Minutes


Last Day CPU Usage
CPU0(%)
100 90 80 70 60 50 40 30 20 10 0
24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Hours

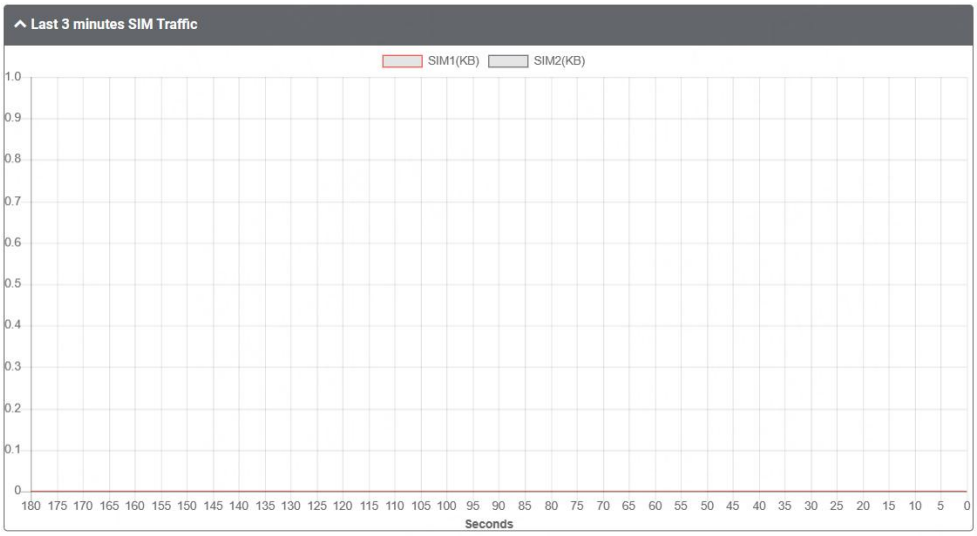
RAM Usage

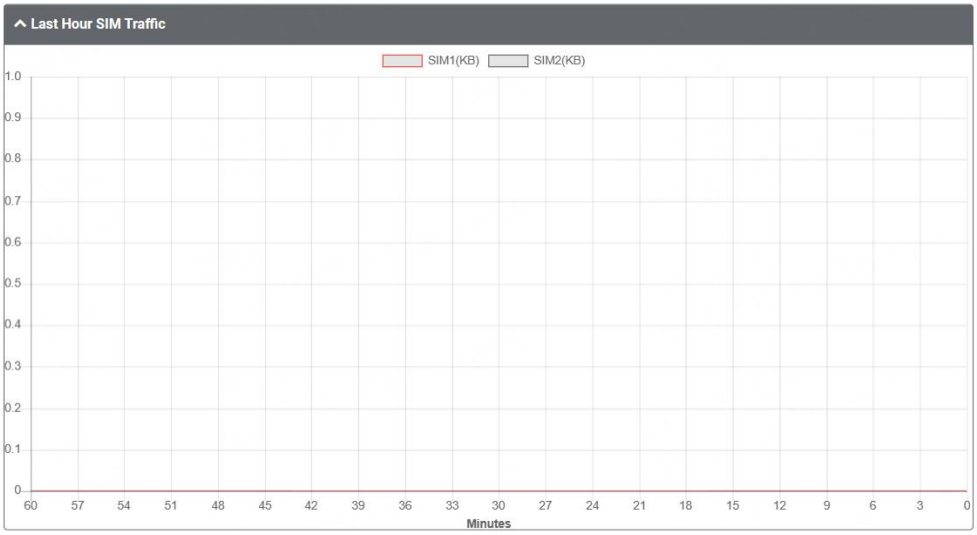

Last 3 minutes RAM Usage
RAM(%)
50 45 40 35 30 25 20 15 10 5 0
180 175 170 165 160 155 150 145 140 135 130 125 120 115 110 105 100 95 90 85 80 75 70 65 60 55 50 45 40 35 30 25 20 15 10 5 0
Seconds

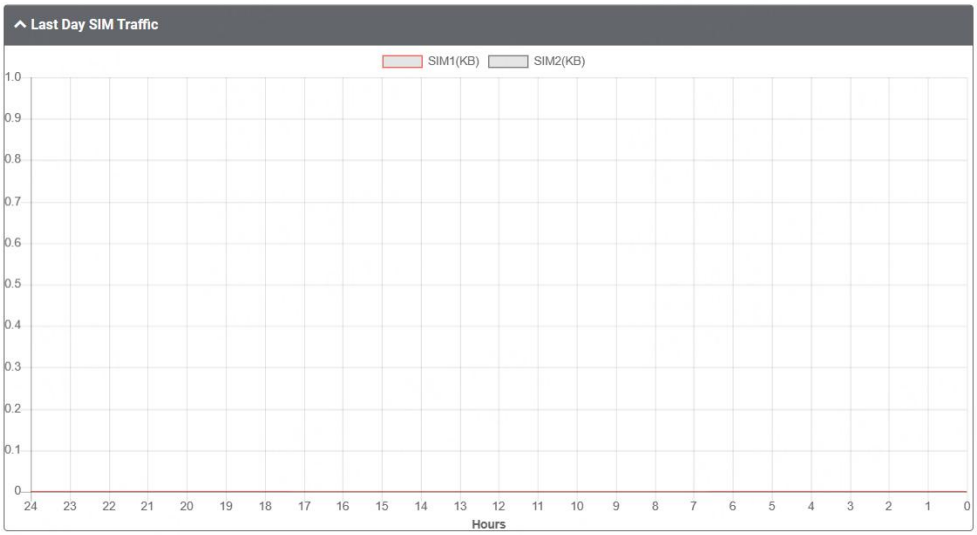

Last Hour RAM Usage
RAM(%)
50 45 40 35 30 25 20 15 10 5 0
60 57 54 51 48 45 42 39 36 33 30 27 24 21 18 15 12 9 6 3 0
Minutes


Last Day RAM Usage
RAM(%)
50 45 40 35 30 25 20 15 10 5 0
24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Hours

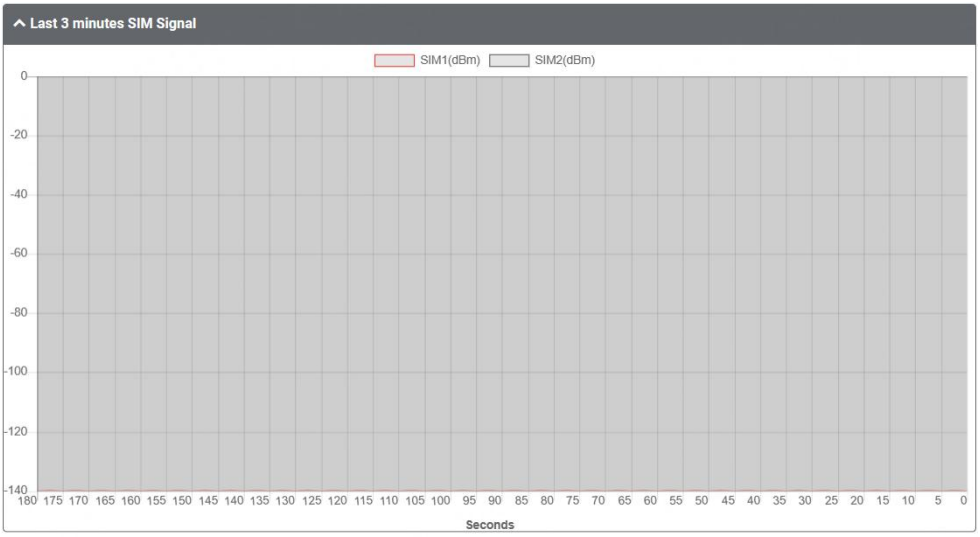
SIM Traffic

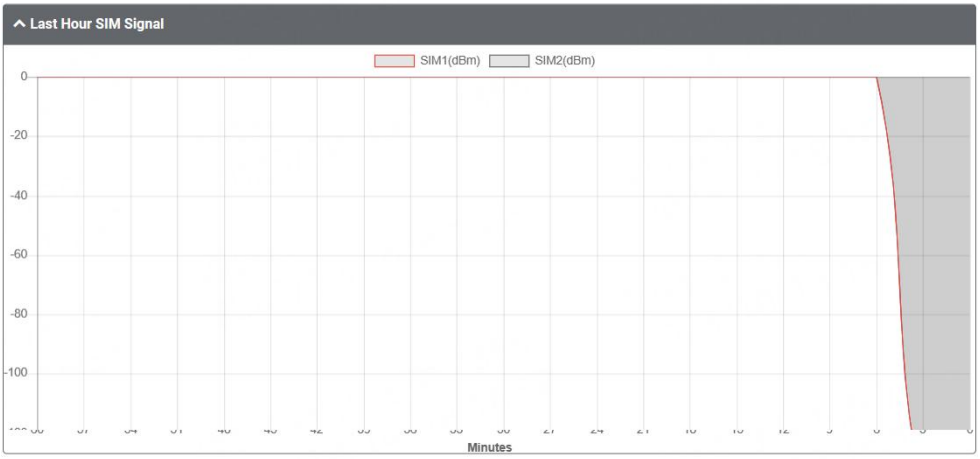

Last 3 minutes SIM Traffic
SIM1(KB)
SIM2(KB)
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
180 175 170 165 160 155 150 145 140 135 130 125 120 115 110 105 100 95 90 85 80 75 70 65 60 55 50 45 40 35 30 25 20 15 10 5 0
Seconds

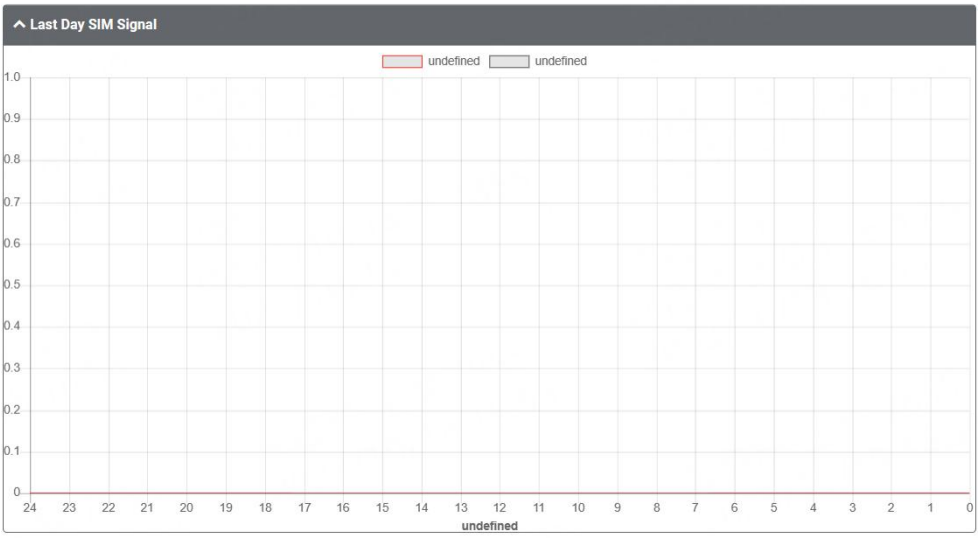

Last Hour SIM Traffic
SIM1(KB)
SIM2(KB)
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
60 57 54 51 48 45 42 39 36 33 30 27 24 21 18 15 12 9 6 3 0
Minutes


Last Day SIM Traffic
SIM1(KB)
SIM2(KB)
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Hours

SIM Signal


Last 3 minutes SIM Signal
SIM1(dBm)
SIM2(dBm)
0
-20
-40
-60
-80
-100
-120
-140
180 175 170 165 160 155 150 145 140 135 130 125 120 115 110 105 100 95 90 85 80 75 70 65 60 55 50 45 40 35 30 25 20 15 10 5 0
Seconds

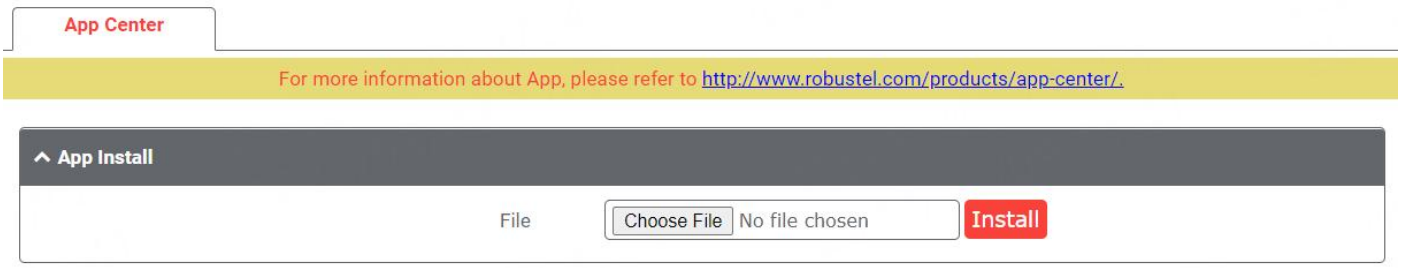

Last Hour SIM Signal
SIM1(dBm)
SIM2(dBm)
0
-20
-40
-60
-80
-100
Minutes


Last Day SIM Signal
undefined
undefined
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
undefined

3.7.4 App Center

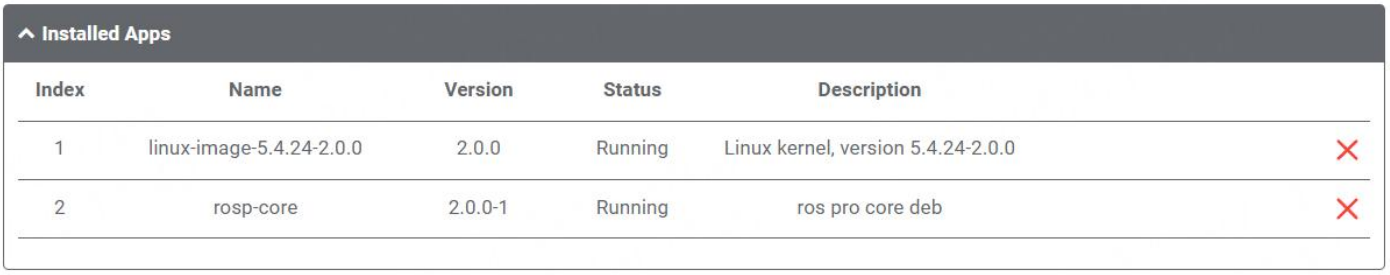
This section allows you to add some required or customized applications to the router. Import and install your applications to the App Center, and reboot the device according to the system prompts. Each installed application will be displayed under the “Services” menu, while other applications related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

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



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

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

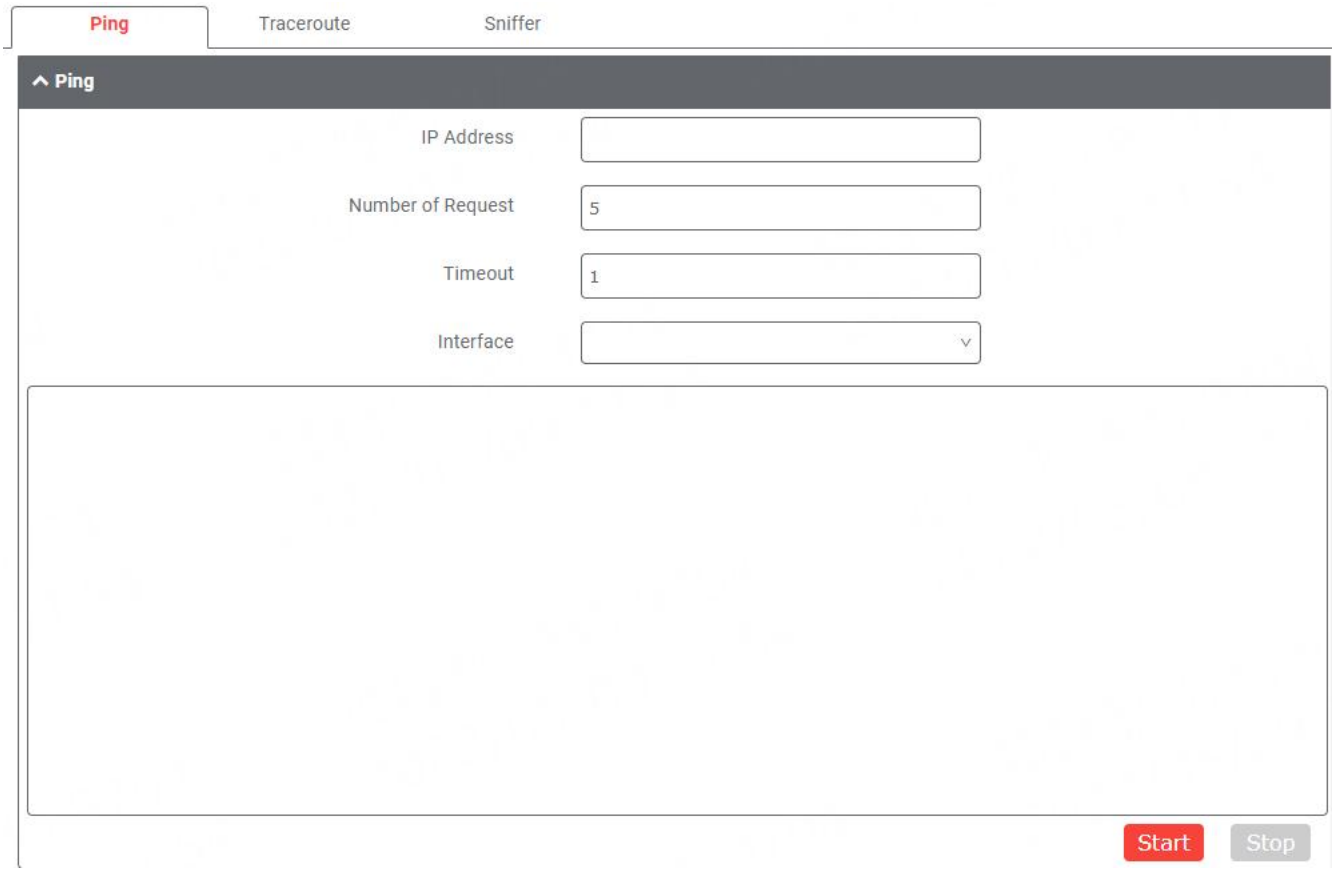


Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

3.7.5 Tools

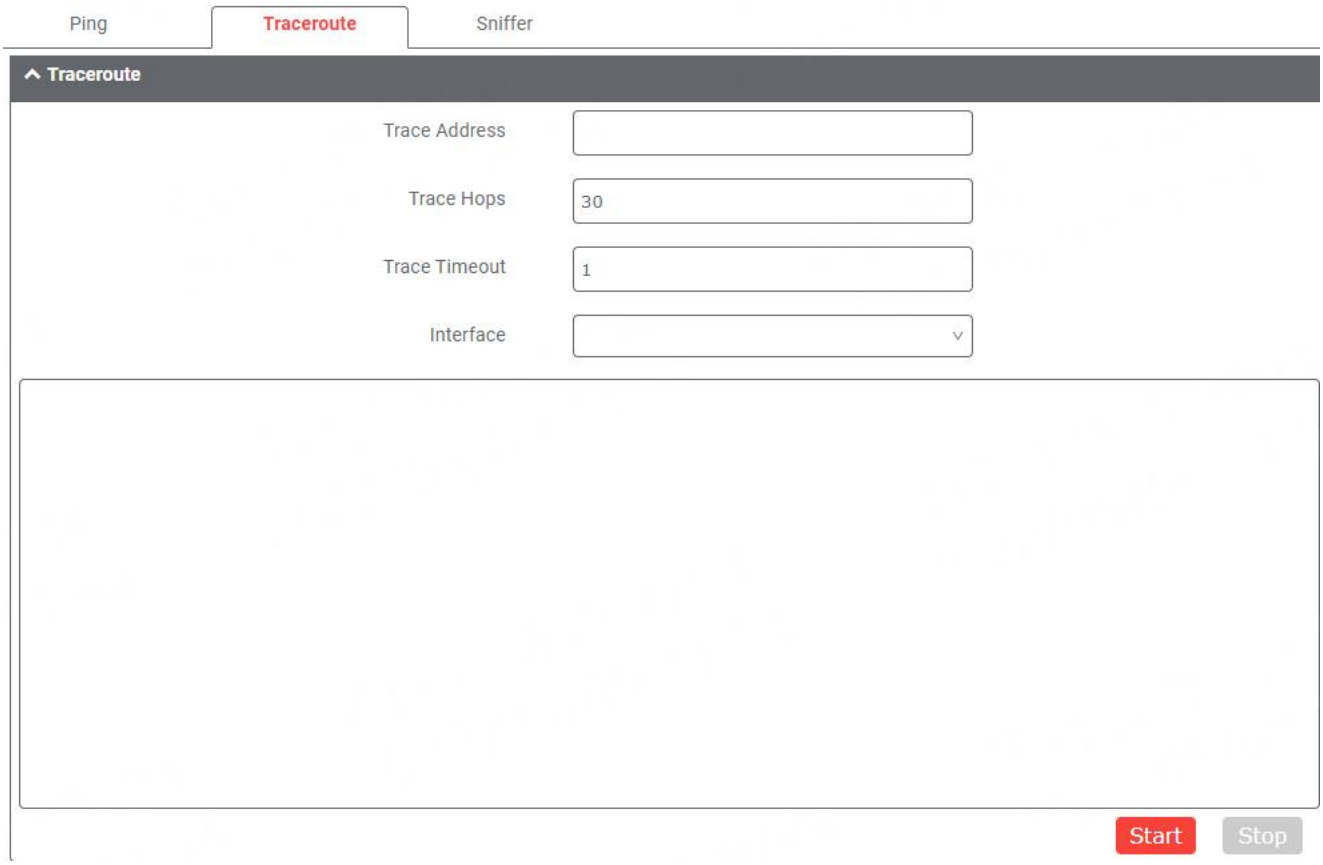
This section provides users three tools: Ping, Traceroute and Sniffer. The Ping is used to check the network connectivity.

Ping



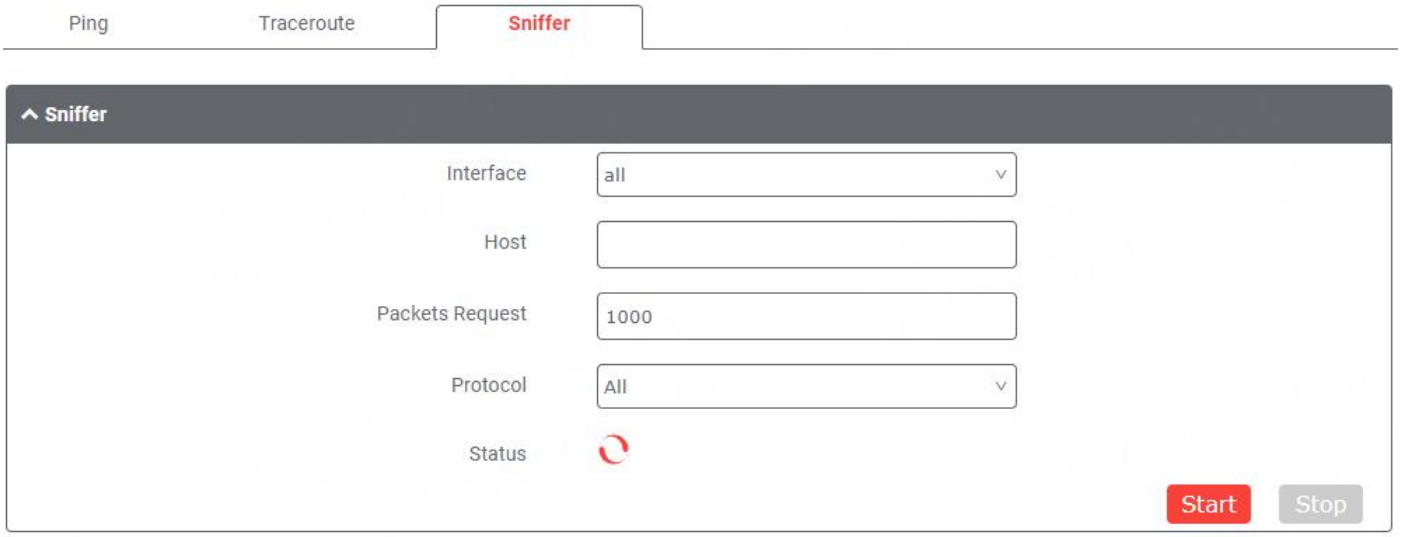
Item	Description	Default
IP address	Enter the ping's destination IP address or destination domain.	Null
Number of Requests	Specify the number of ping requests.	5
Timeout	Specify the timeout of ping requests.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands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

Traceroute



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

Sniffer



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

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

3.7.6 Flash Manager

This section allows you to manage the device’s flash memory life, you can easily check the flash status or thoughput

and start a period test on this section .

Status

This page shows the flash status and data throughput details.

Status | Flash Memory Tests

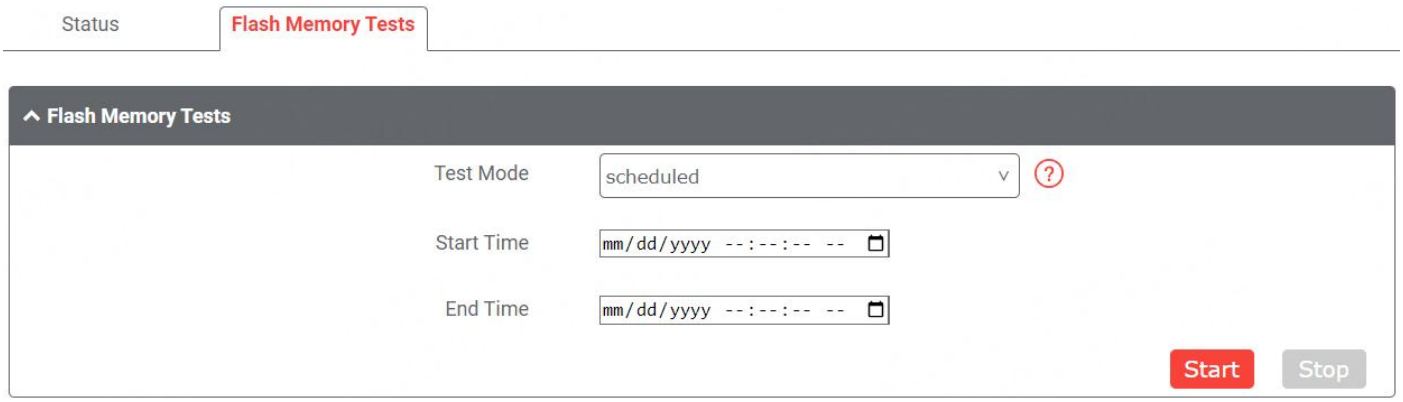
Flash Status

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

Data Throughput

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

Flash Memory Tests

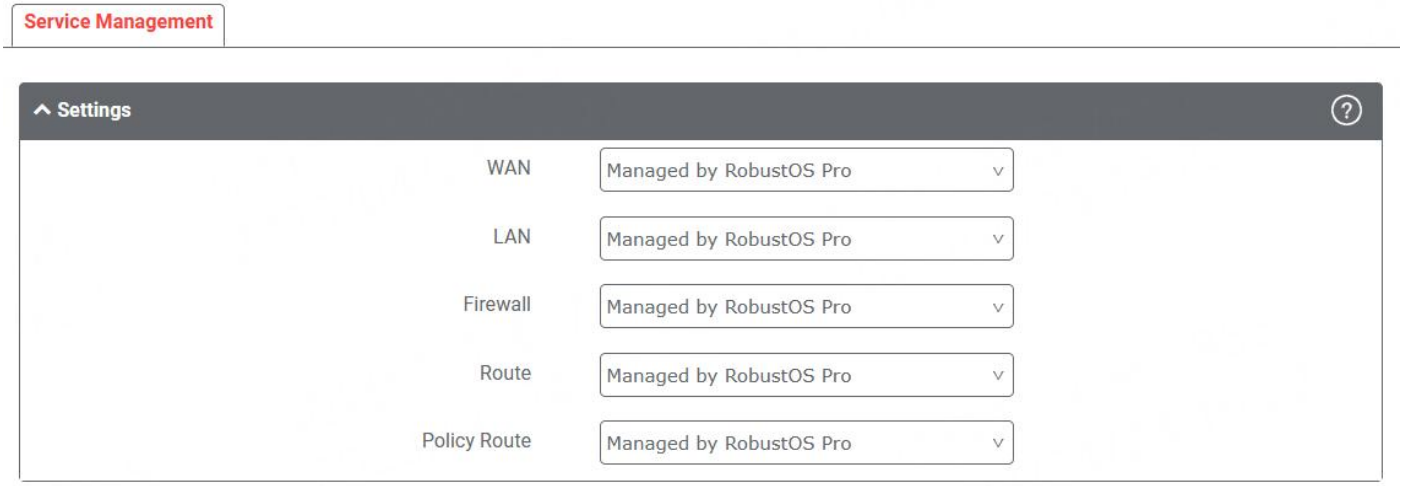


Flash Memory Tests @ Flash Manager	
Item	**Description**
Test Mode	**Manual**: When choosing 'manual', click 'start' to run a test, you can click 'stop' to end the test; **Scheduled**: Input the 'start' and 'end' time for a scheduled test. You can click 'stop' button under whatever mode.
Start Time	Enter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

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

3.7.7 Service Management

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

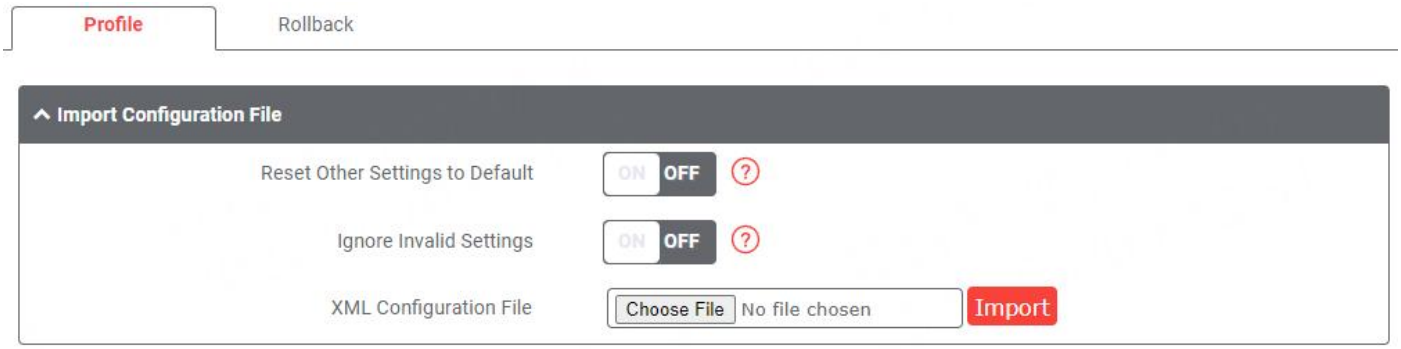


Mode	View Status on RobustOS Pro	Configure via RobustOS Pro	Configure via Linux Shell
Managed By RobustOS Pro	√	√	X
Managed By Third-Party	X	X	√

3.7.8 Profile

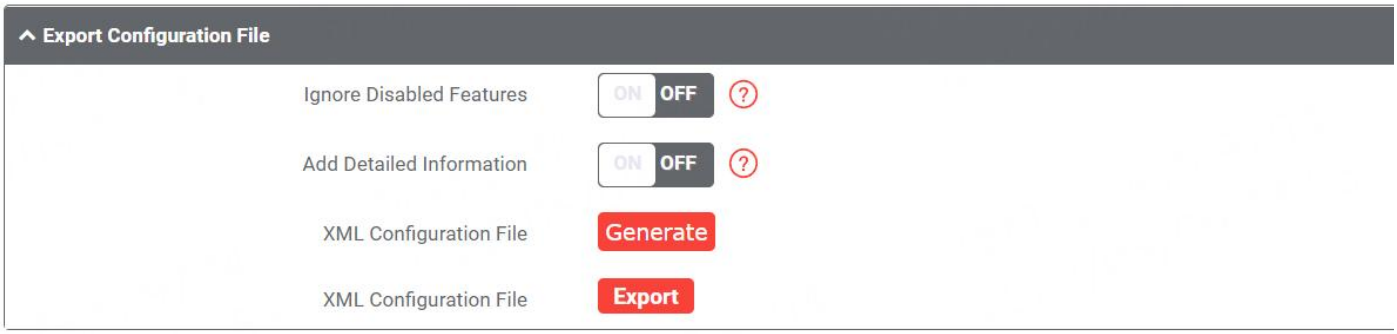
This section allows you to import or export the configuration file, or rollback the device to a previous configuration.

Profile



Item	Description	Default
Reset Other Settings to Default	Click the toggle button as “ON” to return other parameters to default settings.	OFF

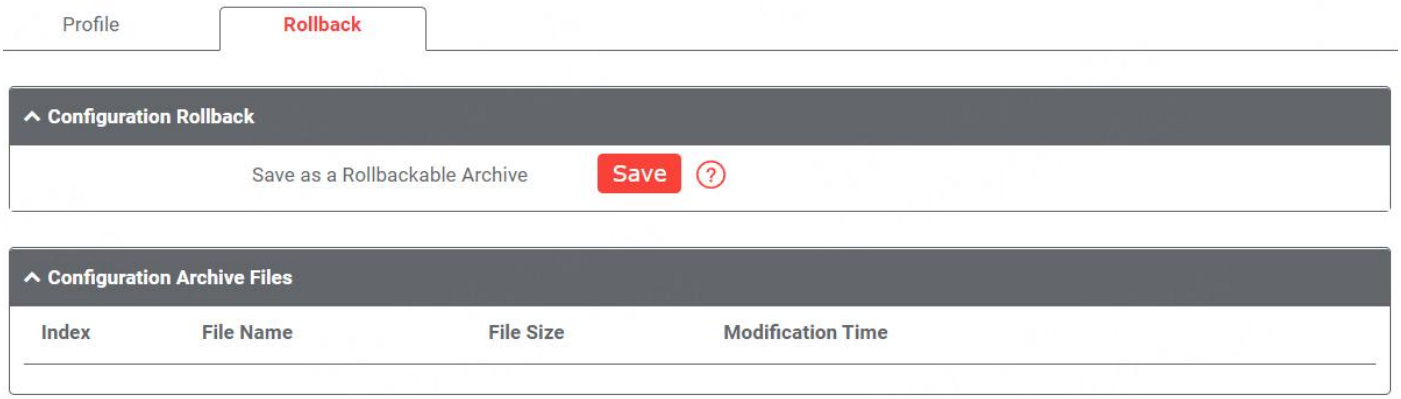
Ignore Invalid Settings	Click the toggle button as “ON” to ignore invalid settings.	OFF
XML Configuration File	Click on Choose File to locate the XML configuration file from your PC, and then click Import to import this file into your device.	--



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

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

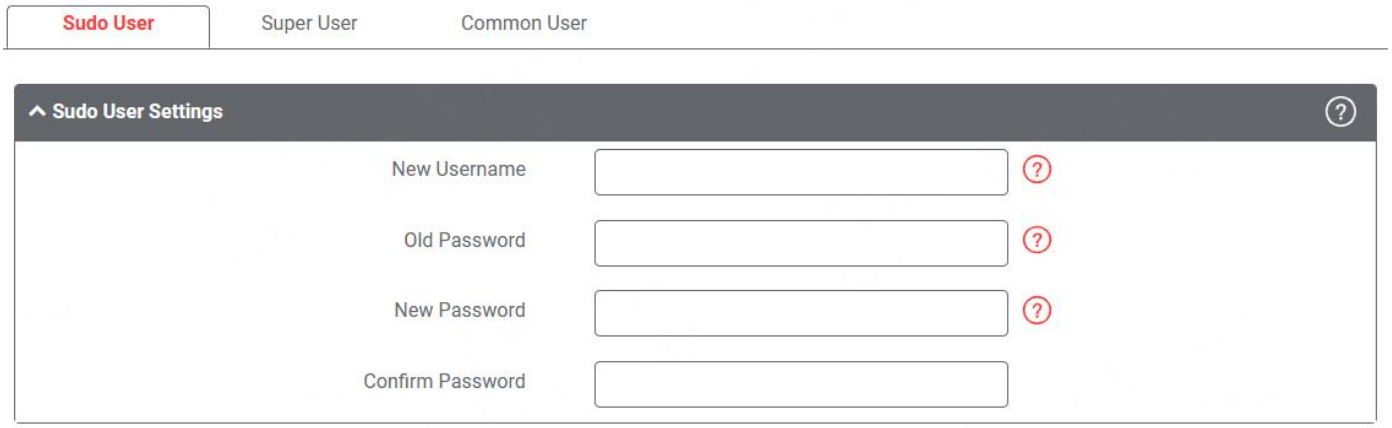
Rollback



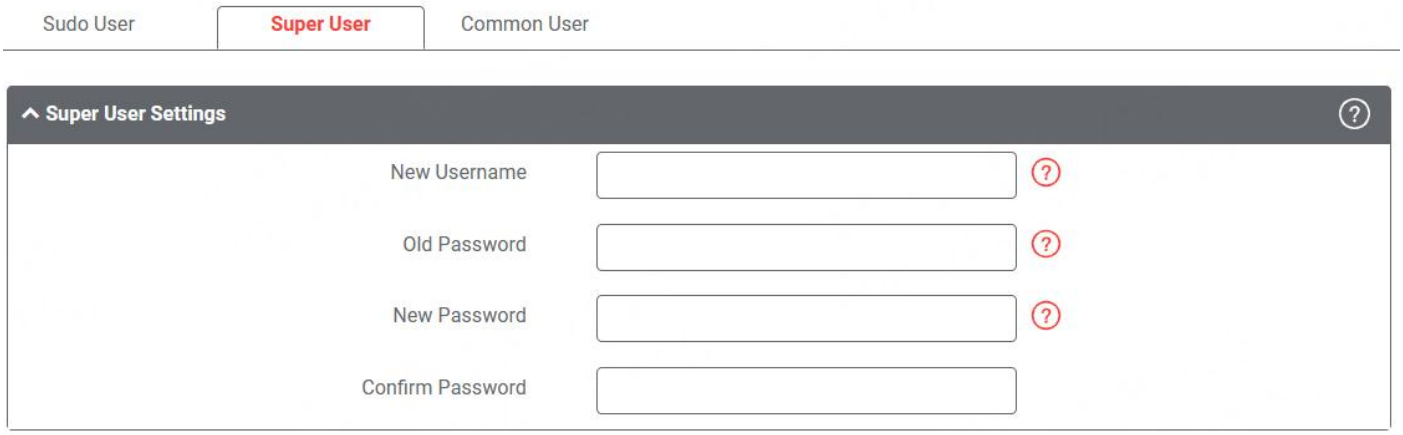
Item	Description	Default
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point every day automatically if configuration changes.	--
Configuration Archive Files	View the related information about configuration archive files, including name, size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

3.7.9 User Management

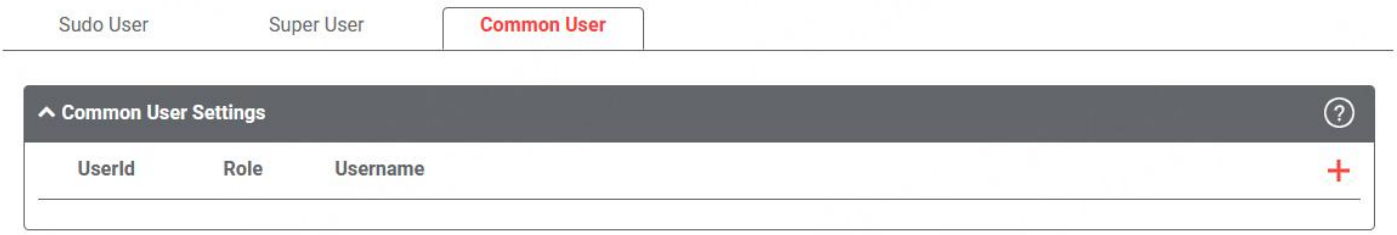
This section allows you to change your username and password, and create or manage user accounts. One device has only one super user who has the highest authority to modify, add and manage other common users.



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



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

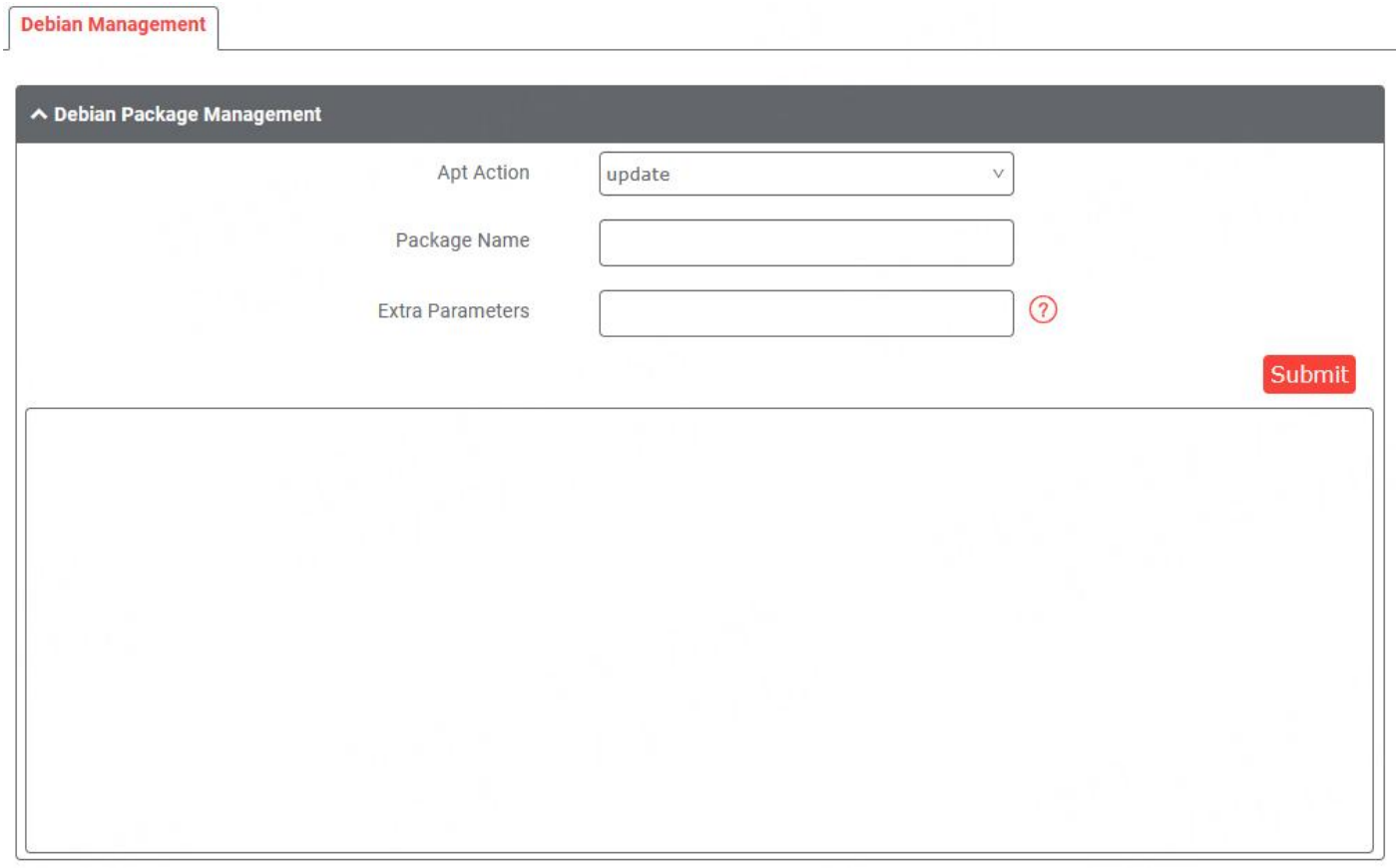


Click + button to add a new common user. The maximum rule count is 5.

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

3.7.10 Debian Management

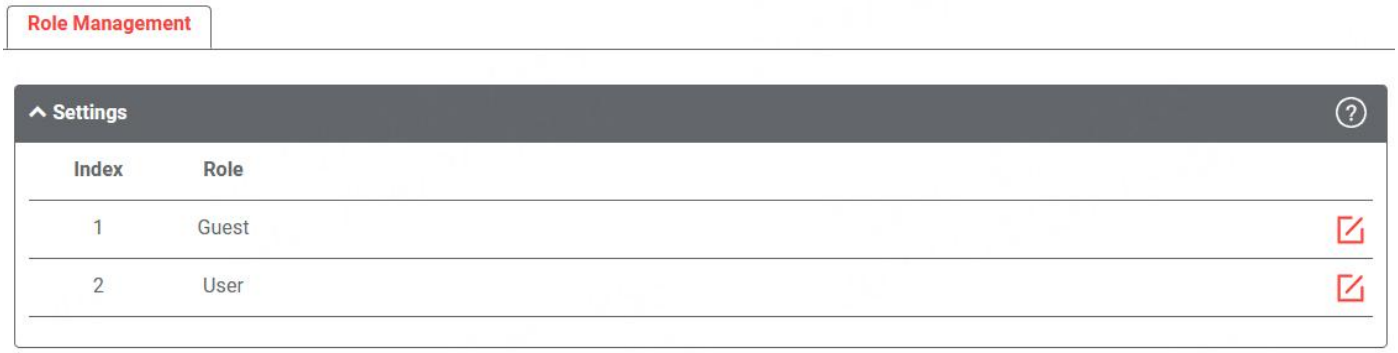
This section allows you to manage your own Debian packages.



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

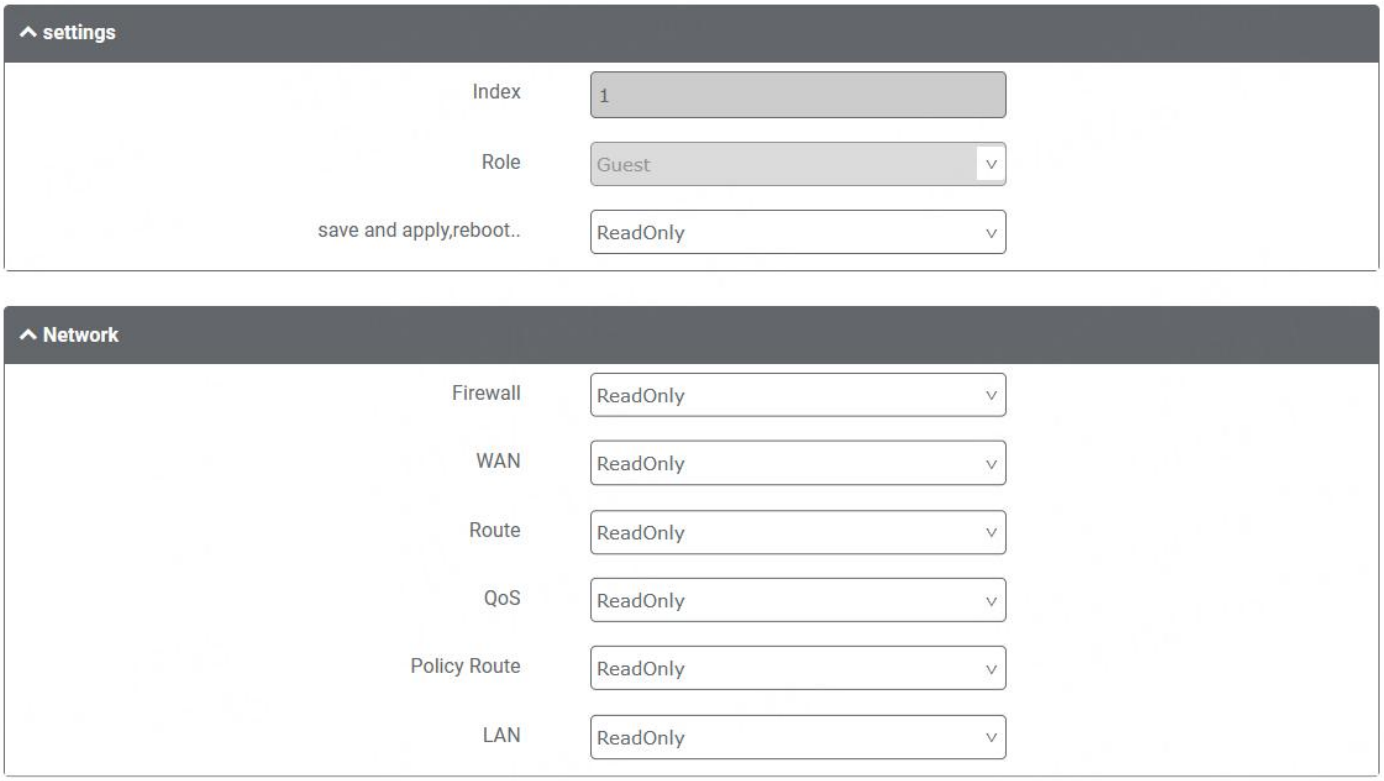
3.7.11 Role Management

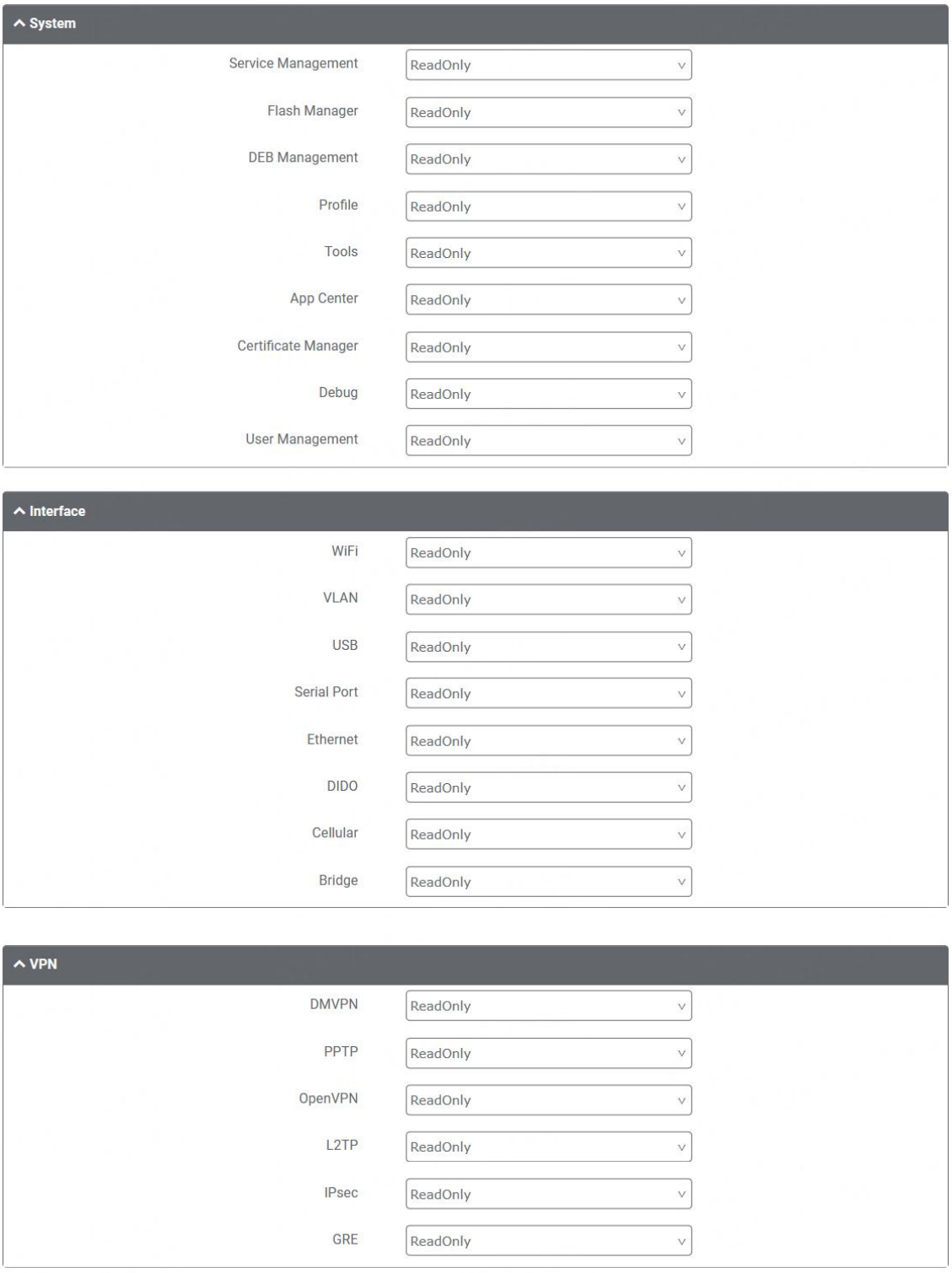
This section is used to manage user roles and manage permissions for users in different roles.

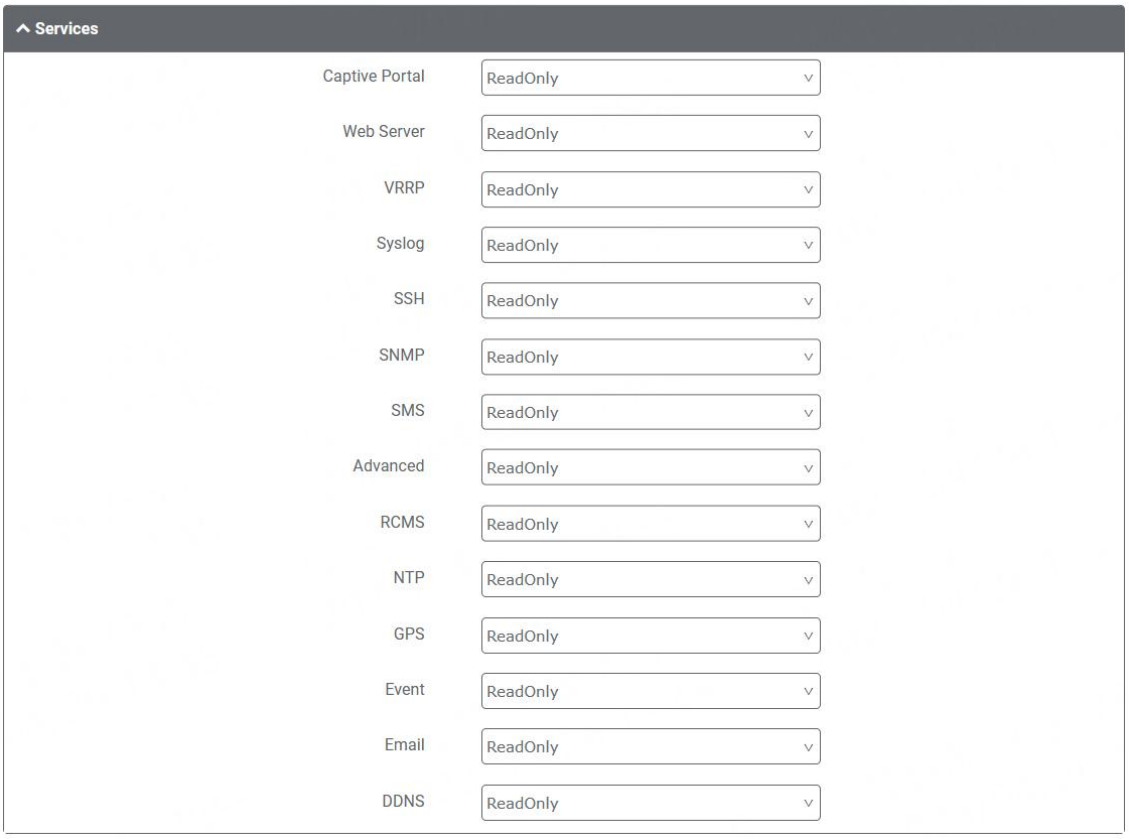


Role Names @ Role Management		
Item	**Description**	**Default**
Guest	Enter a visitor name; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Guest
User	Enter a editor name; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	User

Click to edit Visitor/Editor permission.




System
Service Management
ReadOnly
Flash Manager
ReadOnly
DEB Management
ReadOnly
Profile
ReadOnly
Tools
ReadOnly
App Center
ReadOnly
Certificate Manager
ReadOnly
Debug
ReadOnly
User Management
ReadOnly
Interface
WiFi
ReadOnly
VLAN
ReadOnly
USB
ReadOnly
Serial Port
ReadOnly
Ethernet
ReadOnly
DIDO
ReadOnly
Cellular
ReadOnly
Bridge
ReadOnly
VPN
DMVPN
ReadOnly
PPTP
ReadOnly
OpenVPN
ReadOnly
L2TP
ReadOnly
IPsec
ReadOnly
GRE
ReadOnly



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

Note:

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

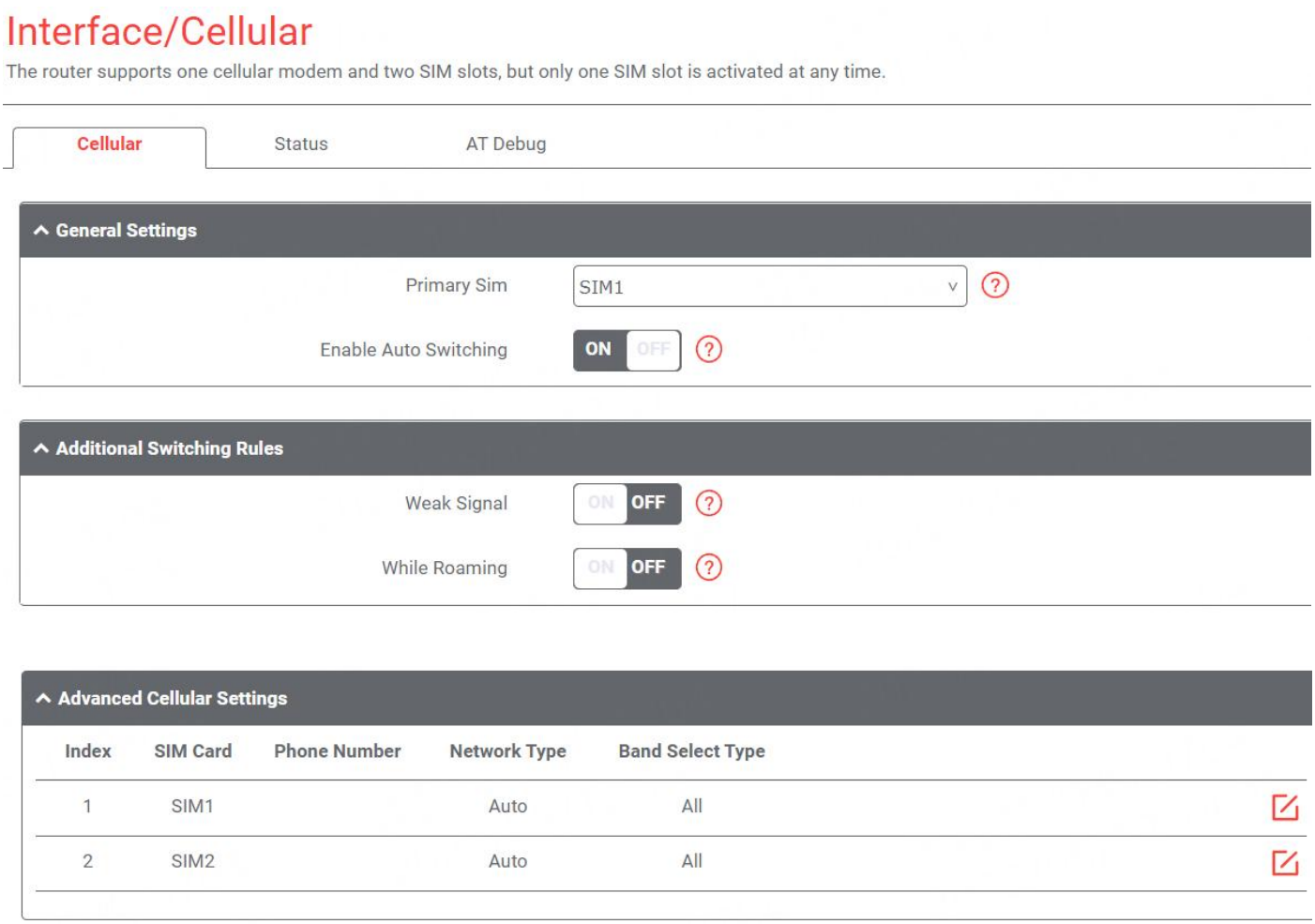
Chapter 4 Configuration Examples

4.1 Cellular

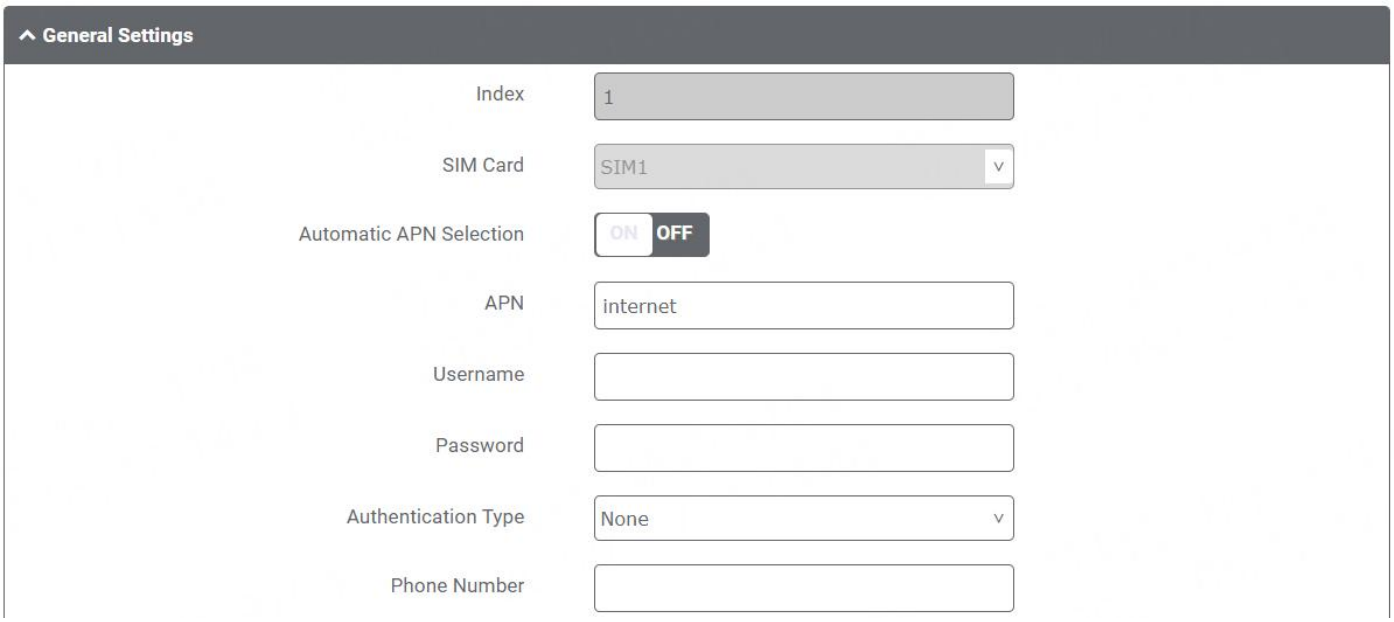
4.1.1 Cellular APN Manual Setting and Cellular Dial-up.

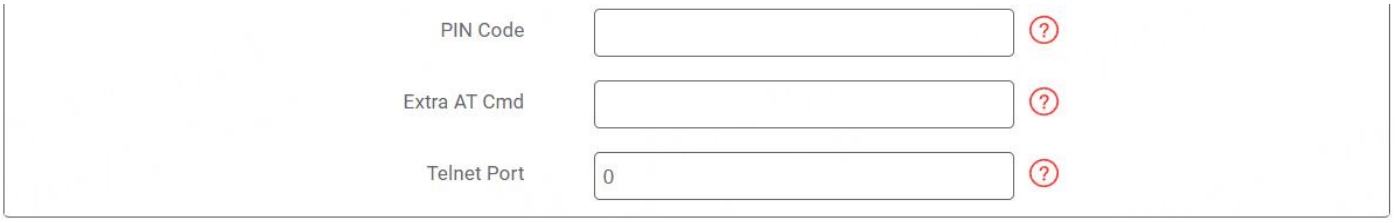
This section shows you how to configure the APN for Cellular Dial-up. Connect the device correctly and insert the SIM card, then open the web configuration page. Under the homepage menu, click “**Interface > Cellular > Cellular ”** to go

to the cellular configuration page.

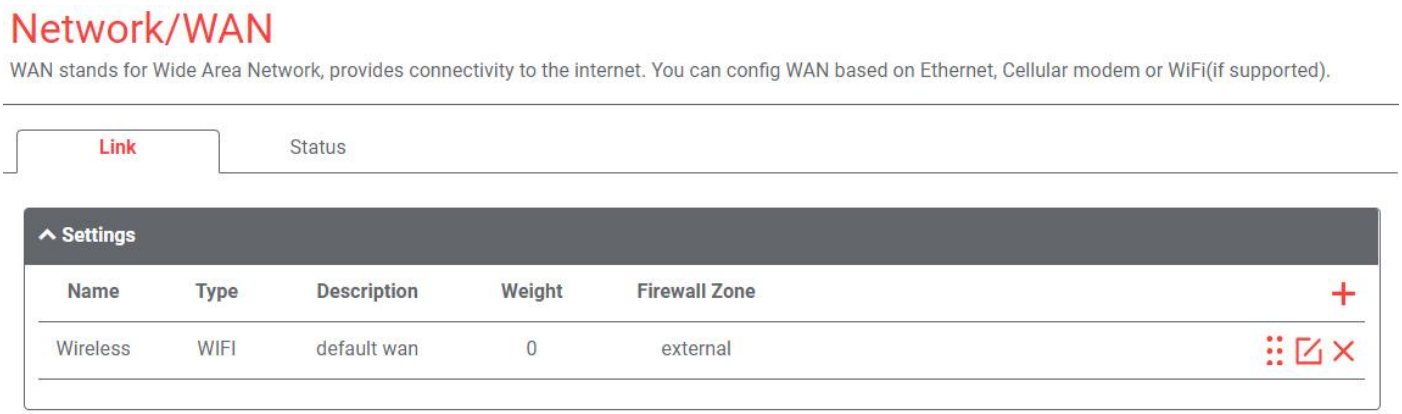


Click  to set its parameters according to the current ISP.

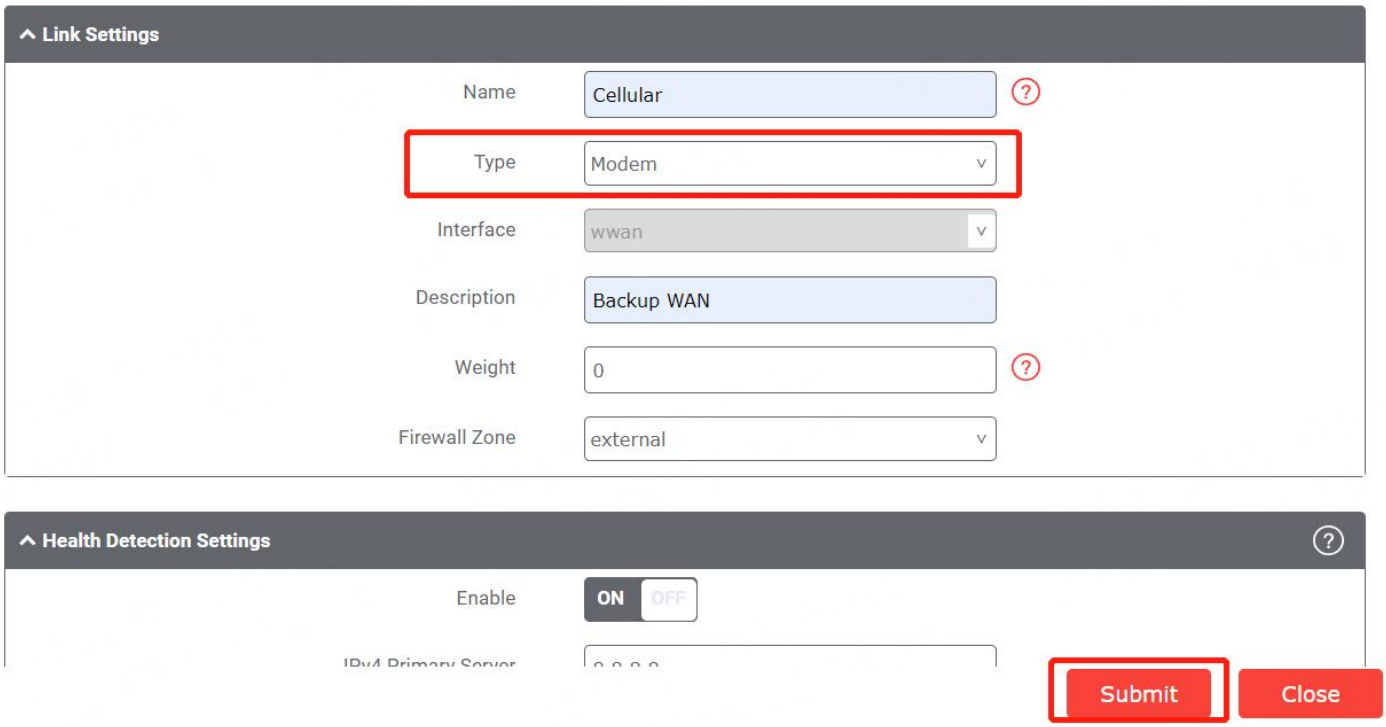




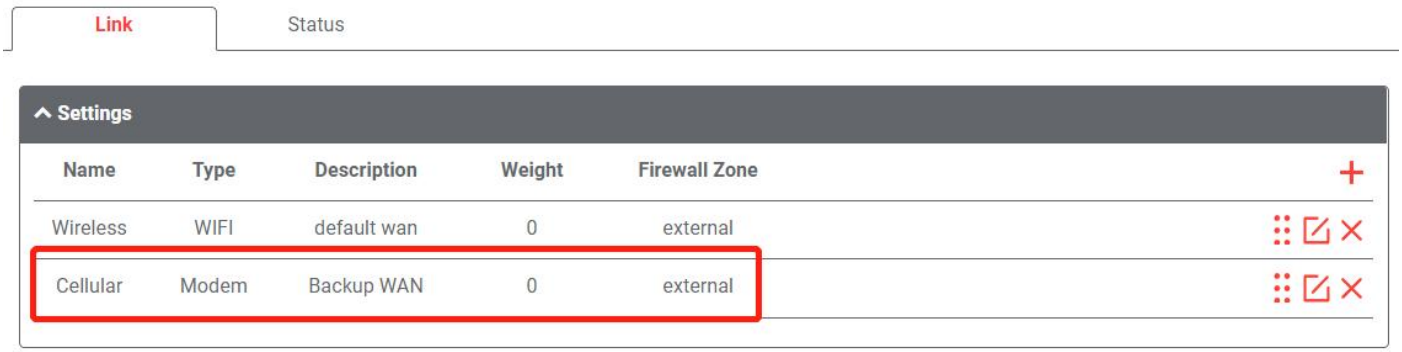
Then Click **"Network> WAN> Link"** go to the WAN configuration page.



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



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



4.1.2 SMS Remote Control

EG51xx supports remote control via SMS. You can use following commands to get the status of the router, and set all the parameters of the router.

SMS command have the following structures:

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

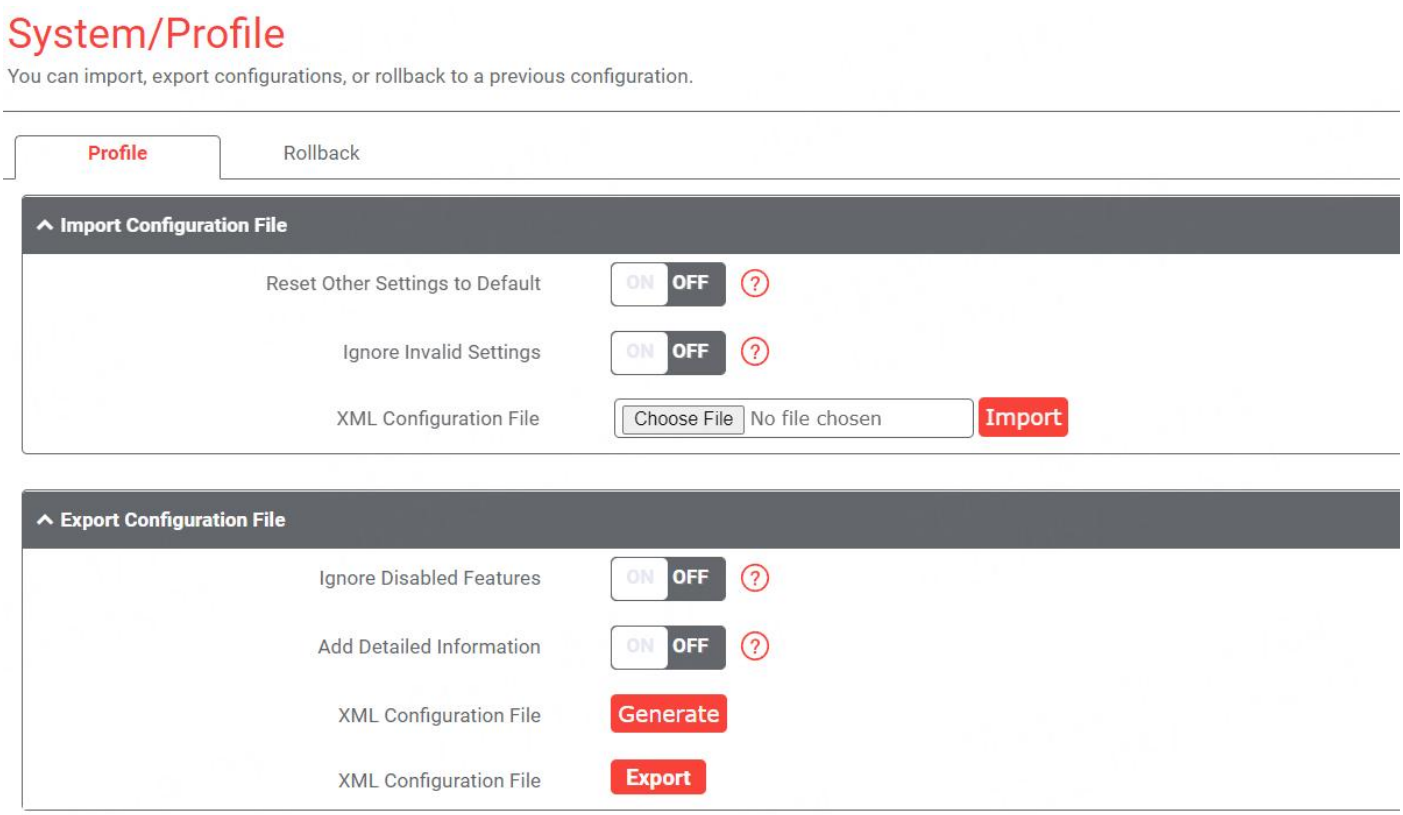
Note: All command symbols must be entered in the half-angle mode of the English input method.

SMS command Explanation:

1. Username and Password: Use the same username and password as WEB manager for authentication.
2. **cmd1, cmd2, cmd3 to cmdn**, the command format is the same as the CLI command, more details about CLI cmd please refer to **5.1 What Is CLI**.

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

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



XML command:

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

SMS cmd:

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

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

admin:admin;status system

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

SMS received:

firmware_version = 2.0.0
firmware_version_full = "2.0.0 (60b55c0)"
kernel_version = 5.4.24-2.0.0
hardware_version = 0.0
operation_system = "Debian GNU/Linux 11.3"

device_model = ""
serial_number = 2204190667030003
temperature_interval = 53.0
uptime = "0 days, 00:12:06"
system_time = "Thu May 19 16:52:22 2022"
ram_usage = 392M/448M
cpu_usage = "22569s Idle/71405s Total /1 cpus"
disk_usage = 1.9G/7.1G

admin:admin;reboot

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

SMS received:

OK

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

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

SMS received:

OK
OK

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

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

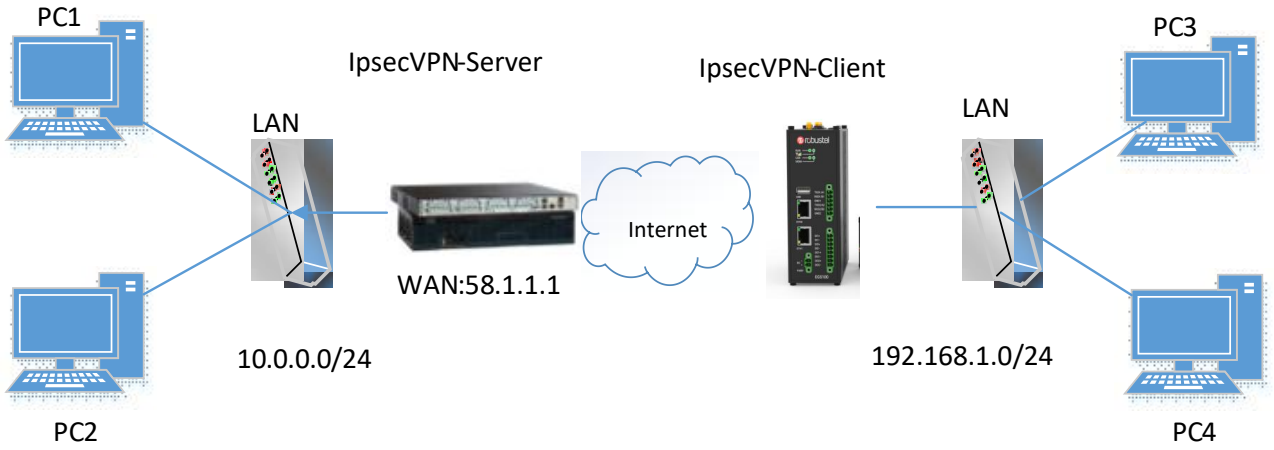
SMS received:

OK
OK
OK
OK

4.2 VPN Configuration Examples

4.2.1 IPsec VPN

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



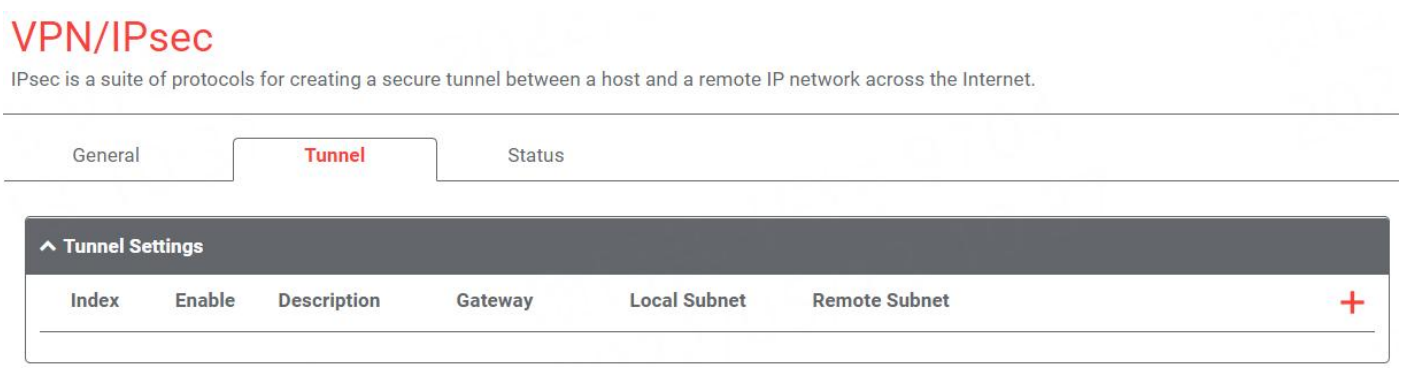
IPsecVPN_Server:

Cisco 2811:

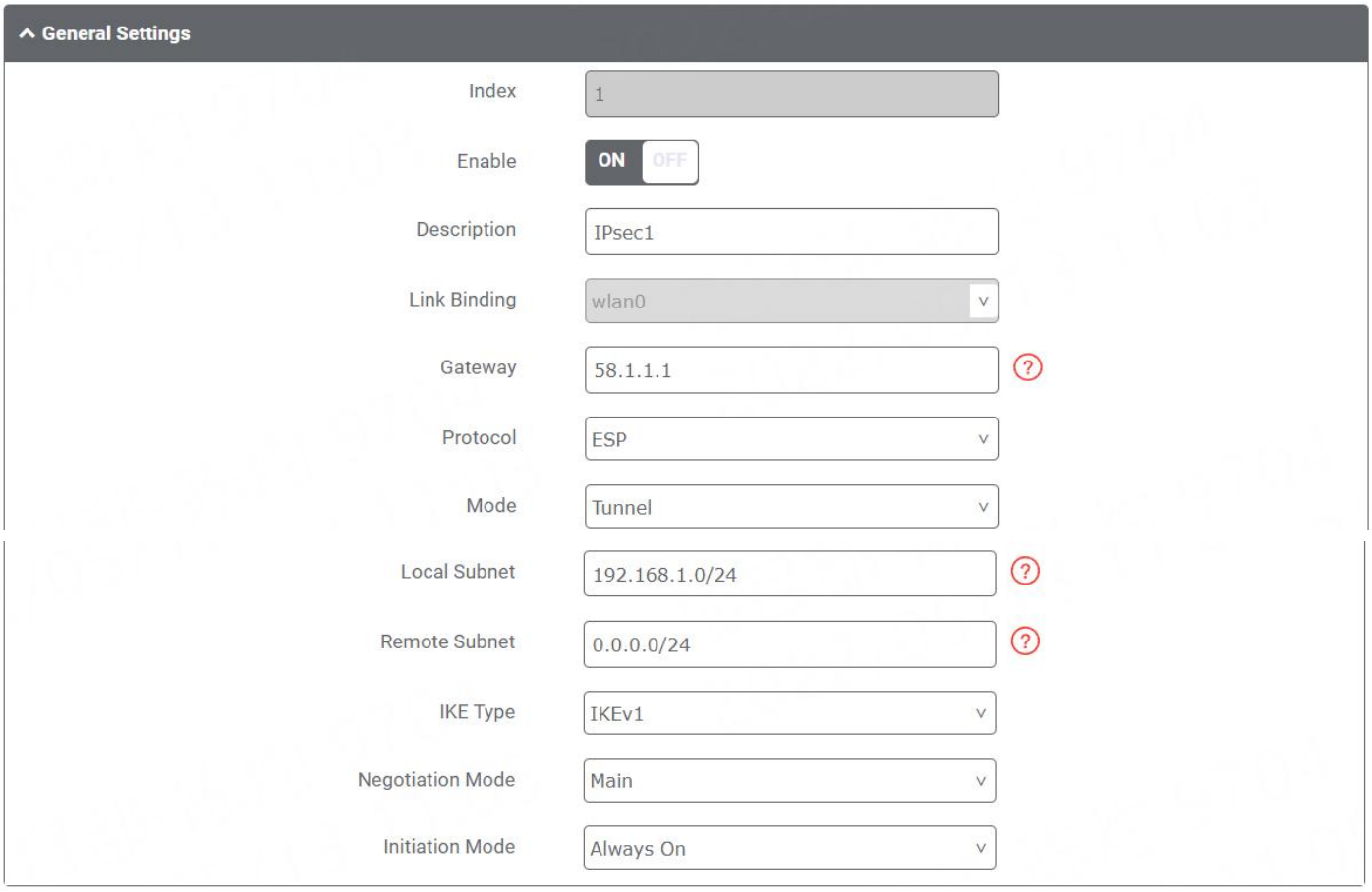
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set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


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


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


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


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

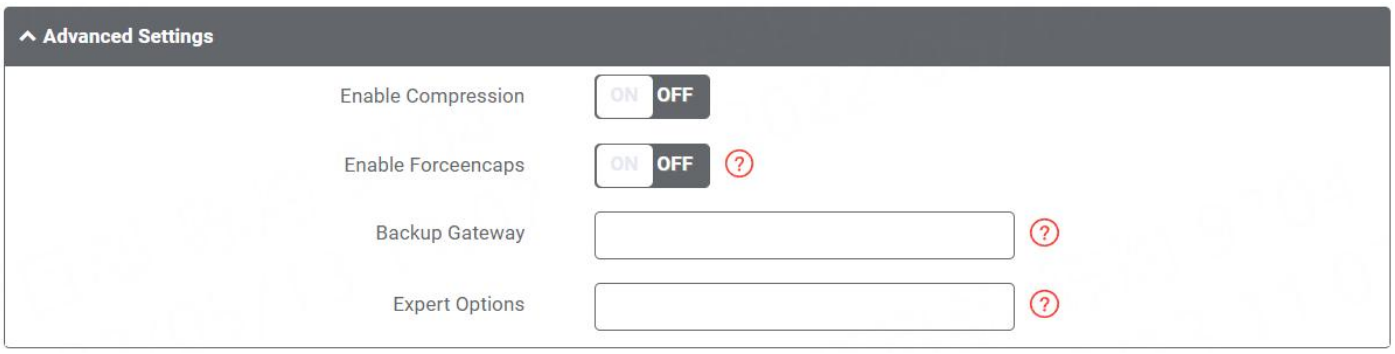
IPsec VPN_Client:

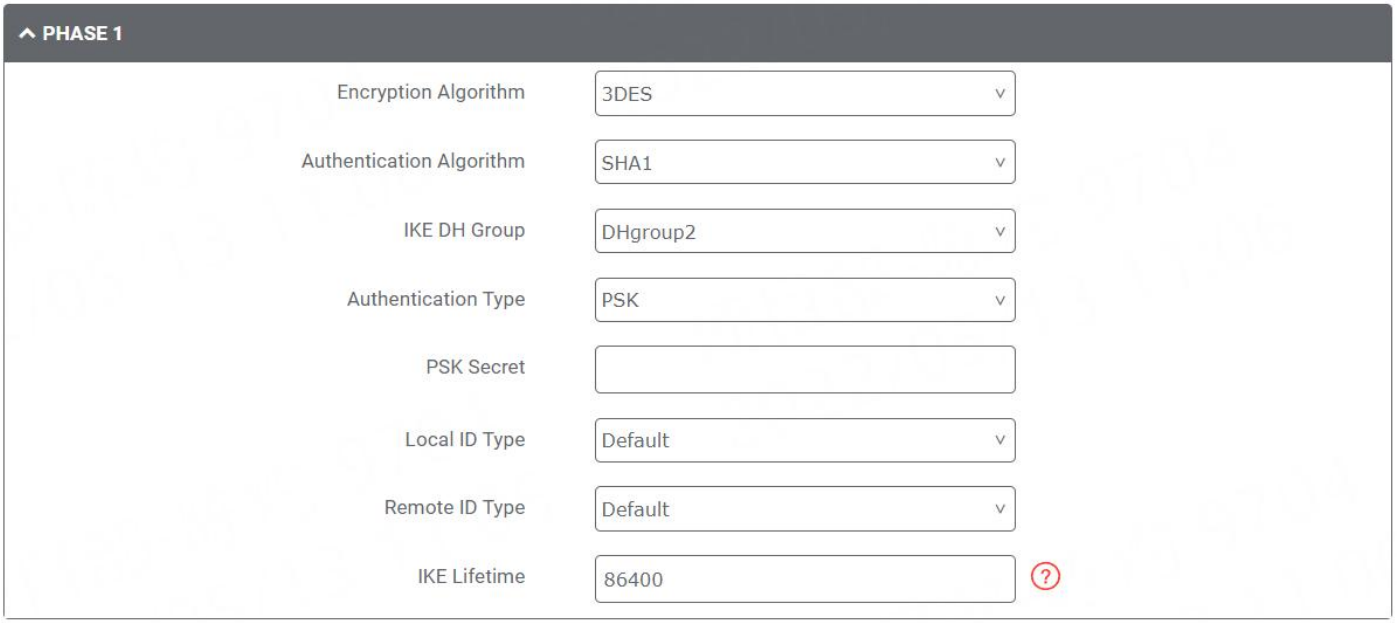
The window is displayed as below by clicking "**VPN > IPsec > Tunnel**."

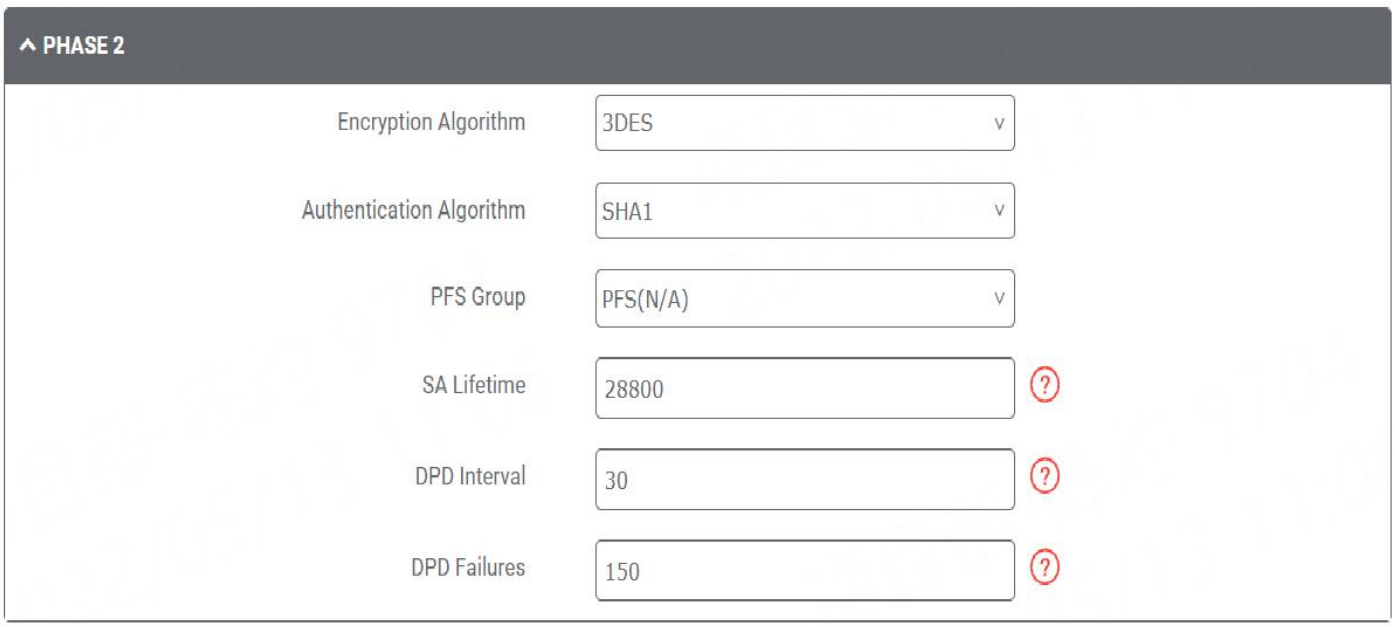


Click + button and set the parameters of IPsec Client as below.





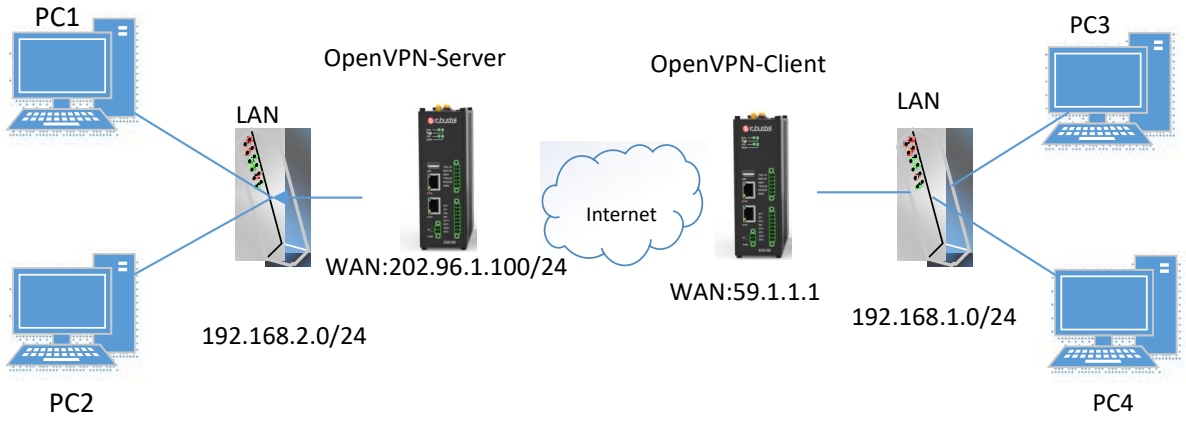




When finished, click Submit to submit and click for the configuration to take effect.

4.2.2 OpenVPN

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



OpenVPN_Server:

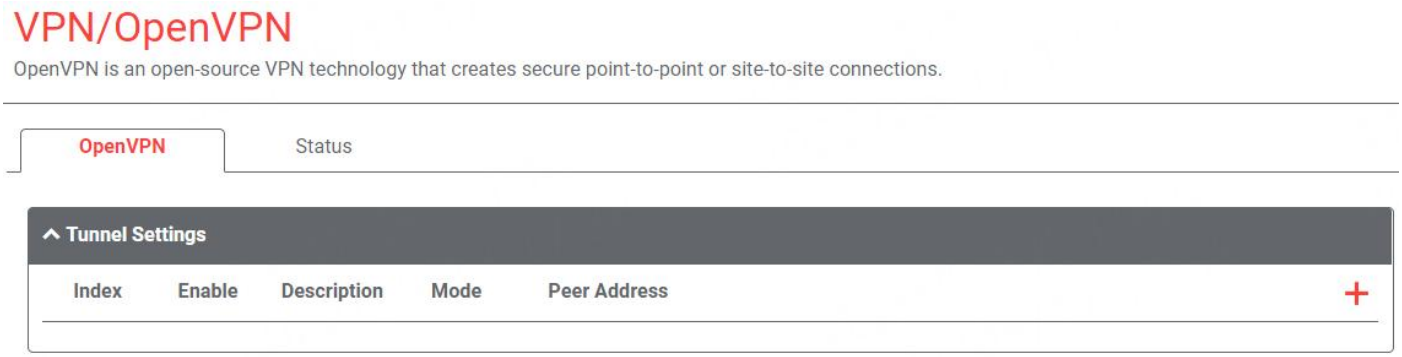
Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server:

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

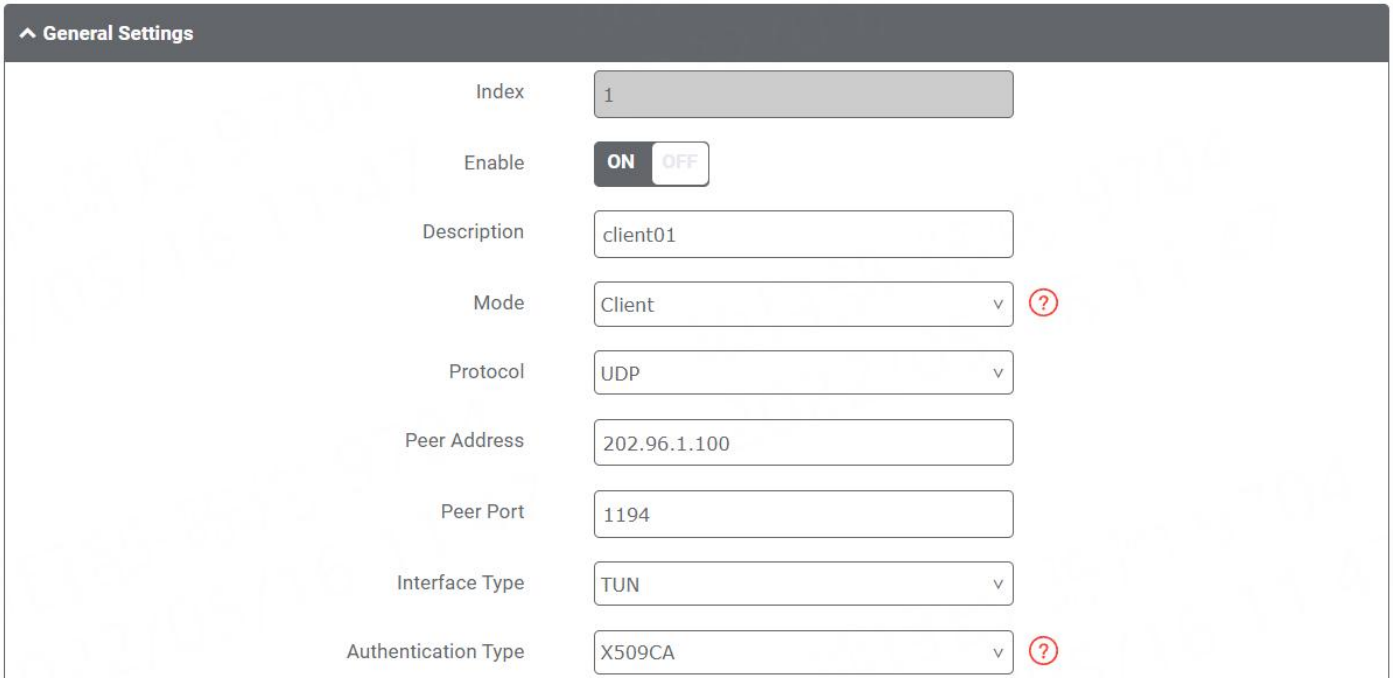
Note: For more configuration details, please contact your technical support engineer.

OpenVPN_Client:

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



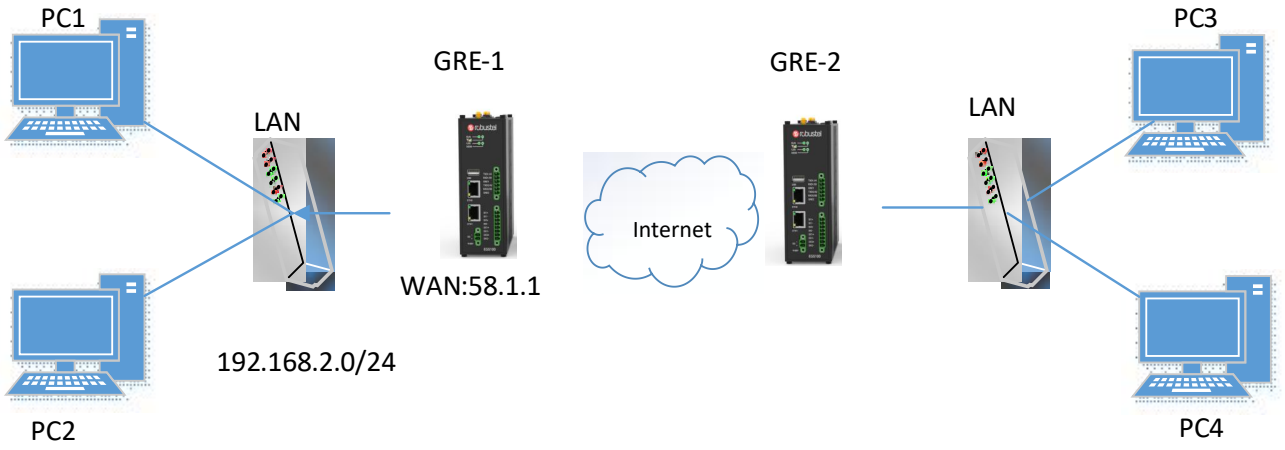
Click + to configure the Client01 as below.



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

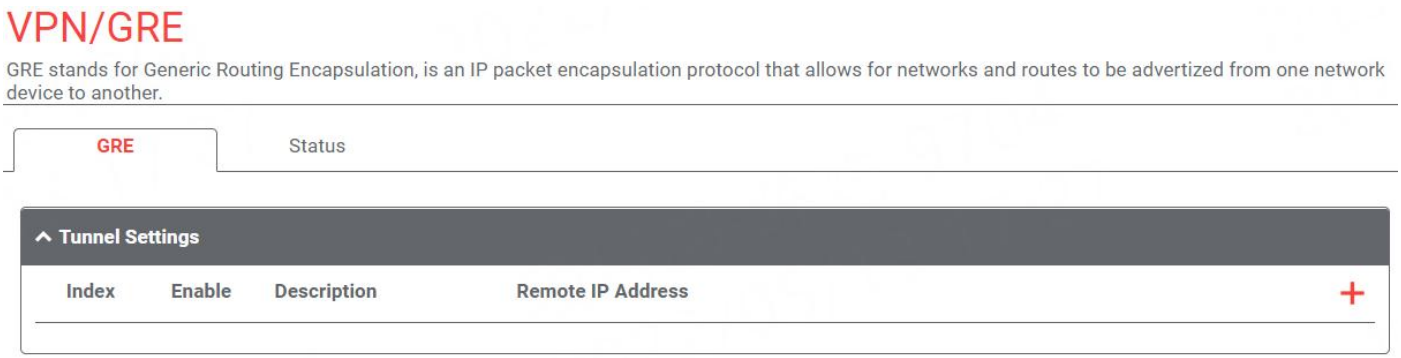
4.2.3 GRE VPN

GRE VPN topology

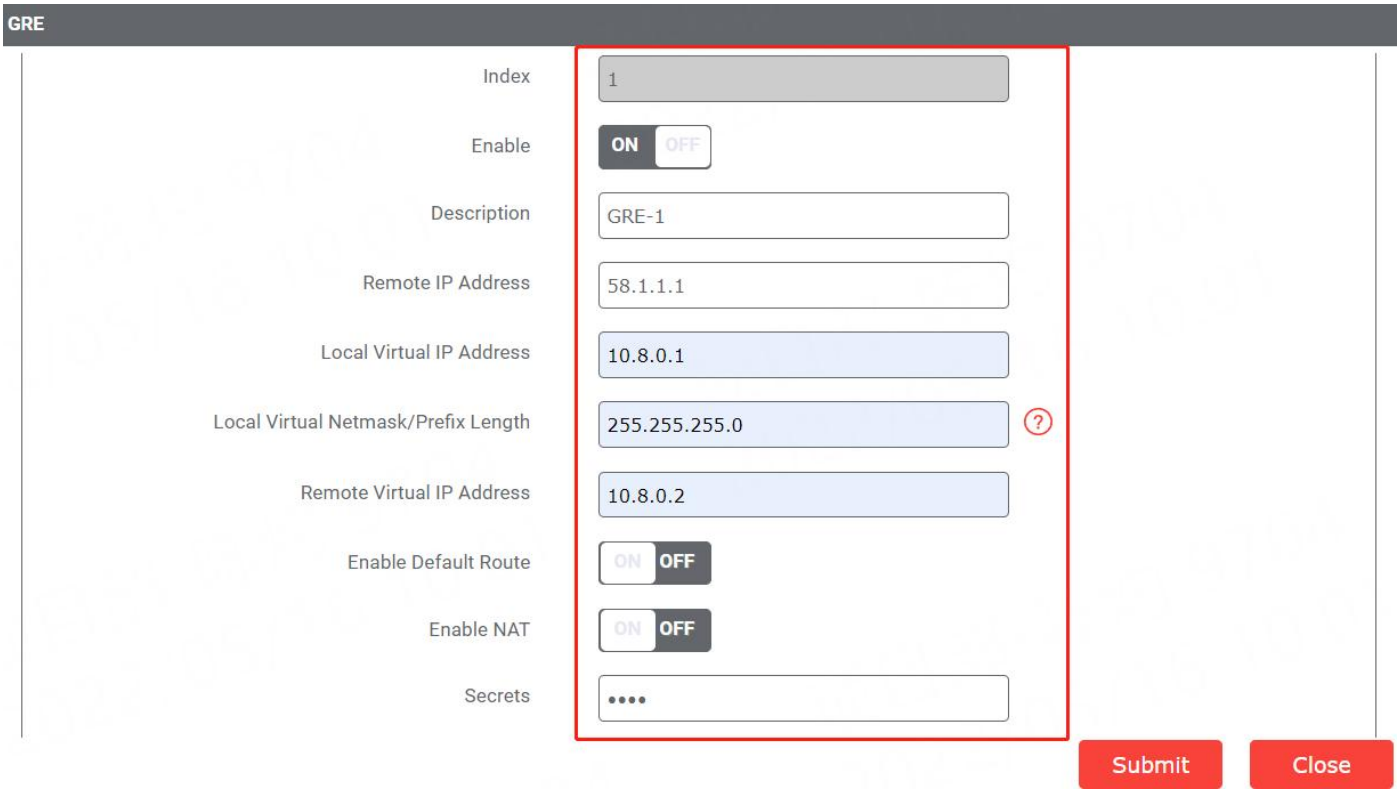


GRE-1：

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



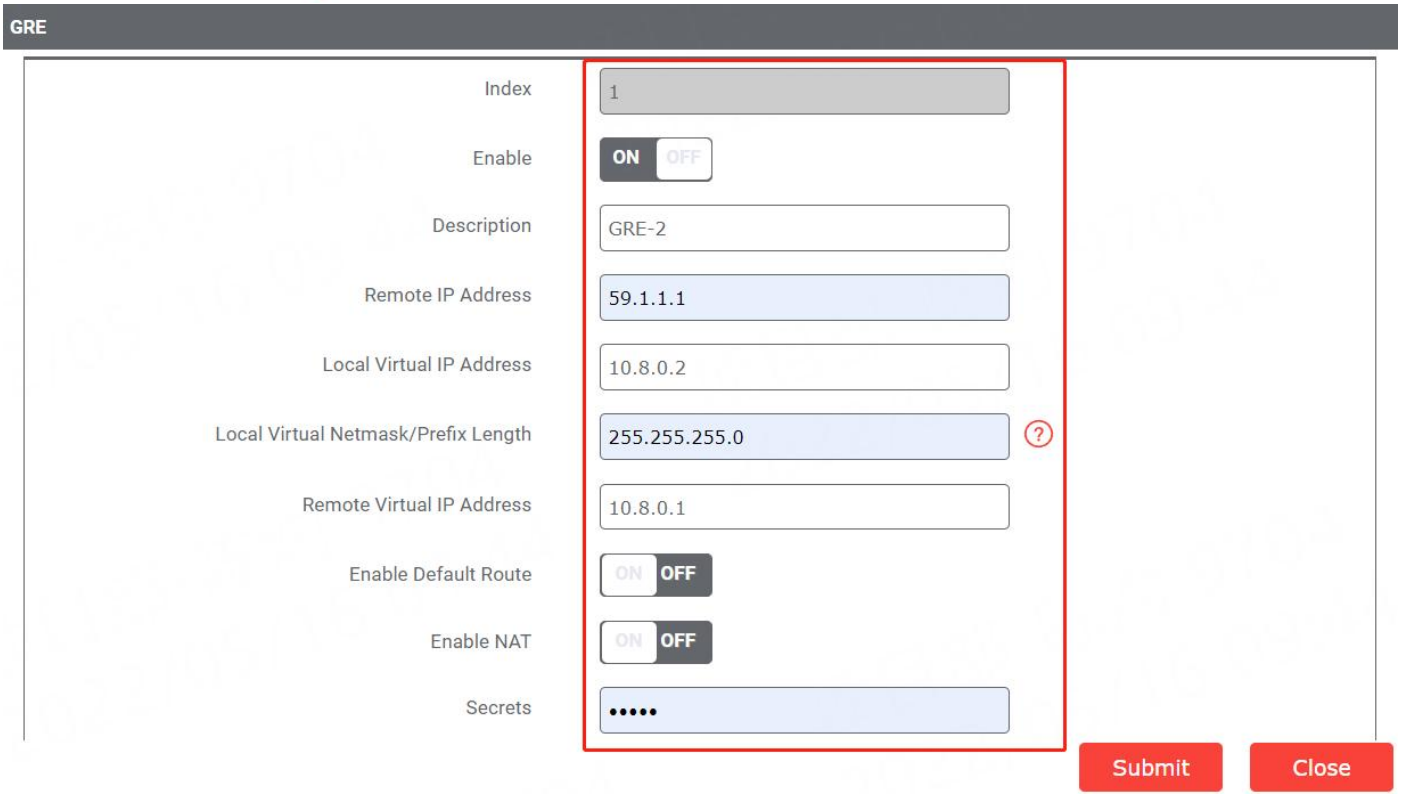
Click + button and set the parameters of GRE-1 as below.



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

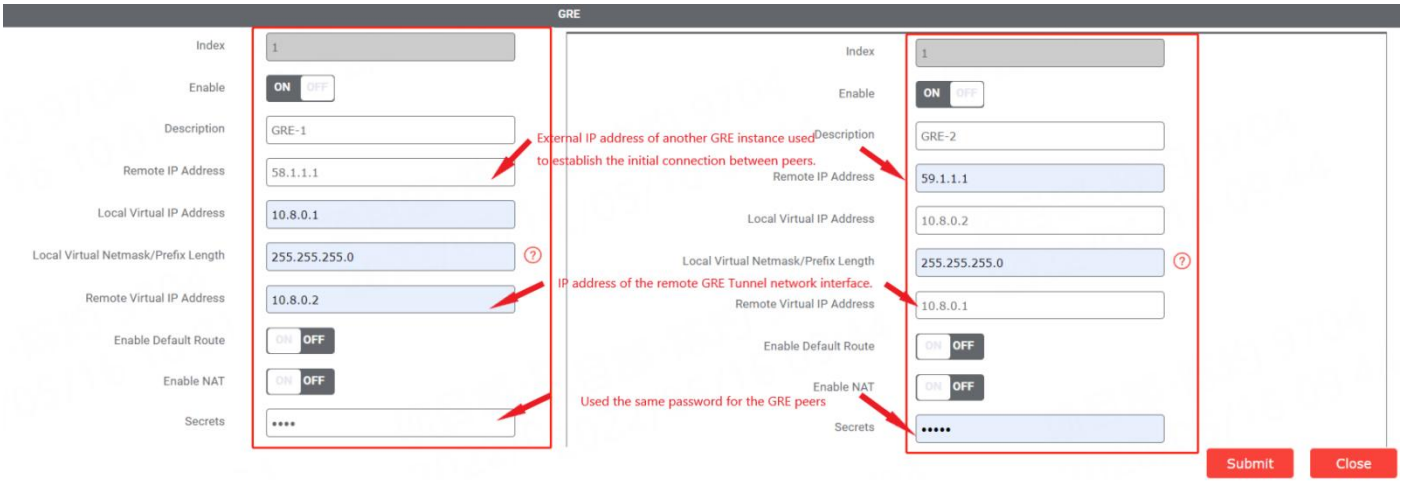
GRE-2:

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



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

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



Chapter 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 router, enter the login account and password (here take admin/admin for example) to enter the configuration mode of the router, as shown below.

Route login:

Router login: admin

Password: admin(could be different)

#

CLI commands:

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

5.2 How to Configure the CLI

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

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

5.3 Commands Reference

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

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

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 learn to configure it with some reference examples.

Example 1: Show current version

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

Example 2: CLI for setting Cellular

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

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

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

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

Glossary

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

Abbr.	Description
LAN	local area network
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
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

Abbr.	Description
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