Software Manual

RobustOS Pro
Software Manual

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

About this Document

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

Related Products

EG5100, LG5100, EG5120, EG5101, EV8100, EG5200, R1520LG

Trademarks and Permissions

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

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to change without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the failing use of this document.

Technical Support

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

Document History

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

Date	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.
March 13, 2024	2.2.0 or newer	2.2.0	Added support for RobustOS Pro V2.2.0.
November 25, 2024	2.3.0 or newer	2.3.0	Added support for RobustOS Pro V2.3.0.

Contents

Chapter 1 Introduction

This software manual, applicable for all the RobustOS Pro-based gateway products, provides information about the web interface, including configuration and operation details.
Please refer to the specific chapter accordingly, as hardware configurations or interfaces may vary between different product models.

Product	EG5100	LG5100	EG5120	EG5101	EV8100	EG5200	R1520LG													
SIM card slots	2	2	2	2	2	2	2													
Ethernet ports	2	2	2	1	2	5	2													
Console ports	-	-	-	-	-	√	-													
HDMI	-	-	-	-	-	√	-													
POE-PD	-	√	-	-	-	-	√													
Wi-Fi	*	-	*	-	*	*	√													
Bluetooth	*	-	*	-	*	*	-													
GNSS	*	-	*	-	-	*	-													
DI	2	2	2	-	4	2	-													
DO	2	2	2	-	-	-	-													
Relay Output	-	-	-	-	1	2	-													
RS232	√	√	√	√	√	√	√													
RS485	√	√	√	√	√	√	√													
RS422	-	-	-	-	-	√	-													
USB	√	√	√	√	√	√	√													
CAN	*	-	-	-	√	-	-													
FXS	-	-	-	-	√	-	-													

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

About RobustOS Pro

RobustOS Pro is an edge gateway system independently developed by Robustel. This system is based on the standard Debian 11 (Bullseye) version and features enhanced network security, supports an advanced GUI and Docker containers, and allows for programming in languages such as C, C++, Java, Python, and Node.js, making it easy for users to independently develop and deploy their applications on the system. Additionally, users can download the latest common applications from Robustel’ s RCMS gateway cloud management platform, as well as applications from the Debian ecosystem, fully meeting the diverse needs of fragmented IoT applications.

Chapter 2 Initial Configuration

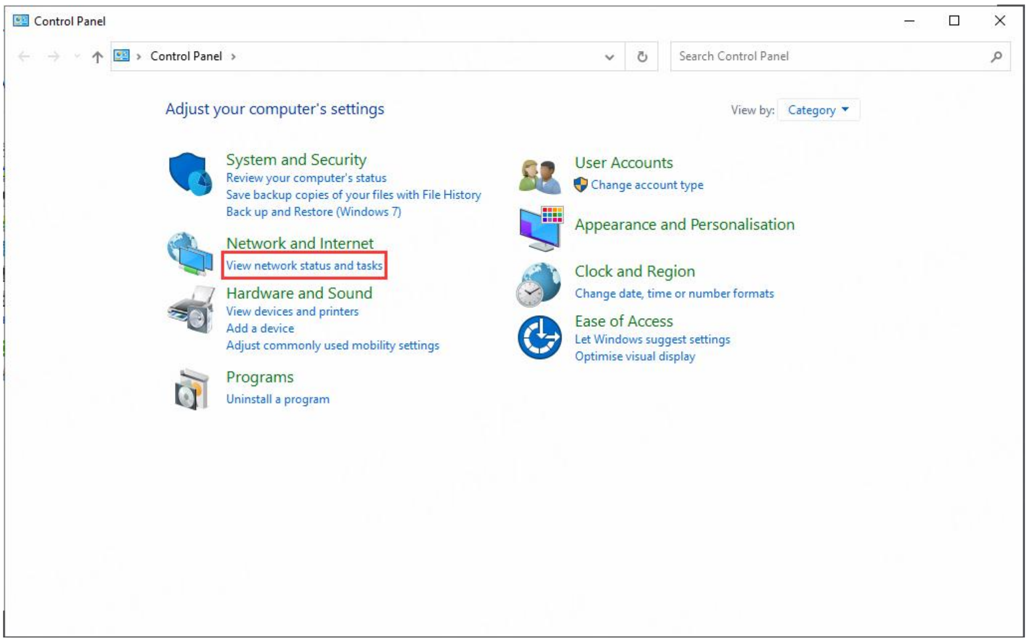
The device supports web configuration, and compatible browsers include Microsoft Edge, Google Chrome, and Firefox. Supported operating systems include Ubuntu, macOS, and Windows 7/8/10/11. There are multiple ways to connect to the gateway: it can be connected through an external repeater/hub or directly to a computer. When the gateway is directly connected to the computer's Ethernet port and acts as a DHCP server, the computer can directly obtain an IP address from the gateway. Alternatively, the computer can be set to a static IP address within the same subnet as the gateway, forming a small local area network. Once the connection between the computer and the gateway is successfully established, you can enter the device's default login address in the computer's browser to access the gateway's web login interface.

2.1 PC Configuration

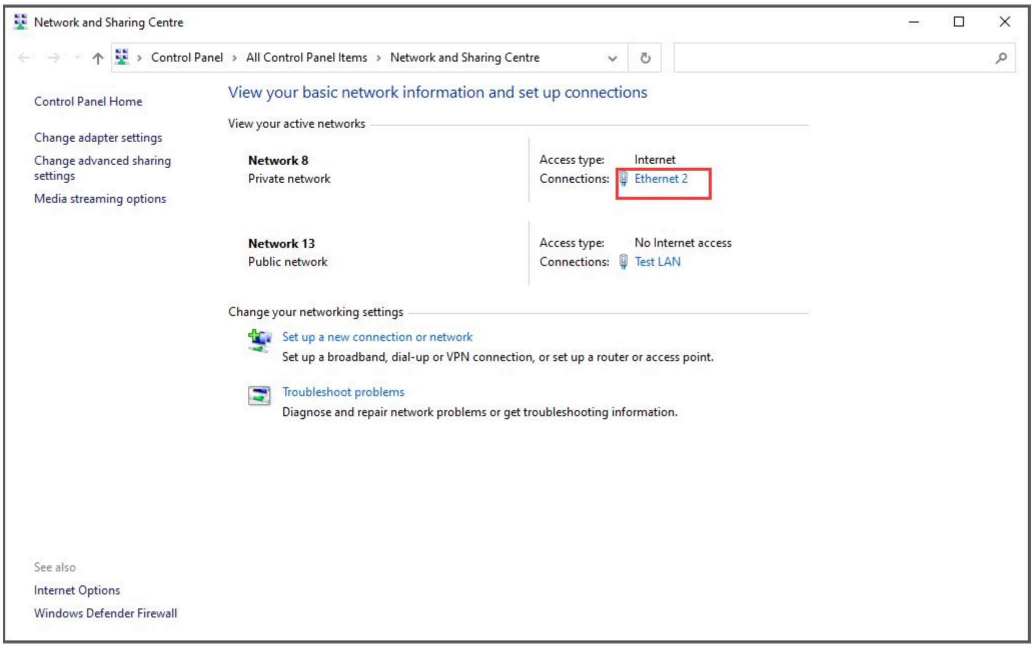
There are two ways to obtain an IP address for the computer. One option is to automatically obtain an IP address from the “Local Area Connection”, while the other is to manually configure a static IP address within the same subnet as the router. Please refer to the steps below.

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

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**".


Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Back up and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalisation
Clock and Region
Change date, time or number formats
Ease of Access
Let Windows suggest settings
Optimise visual display

2. Click “**Network and Sharing Center -> Ethernet**".



Network and Sharing Centre

Control Panel > All Control Panel Items > Network and Sharing Centre

Control Panel Home

Change adapter settings

Change advanced sharing settings

Media streaming options

View your basic network information and set up connections

View your active networks

Network 8
Private network

Access type: Internet
Connections: Ethernet 2

Network 13
Public network

Access type: No Internet access
Connections: Test LAN

Change your networking settings

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

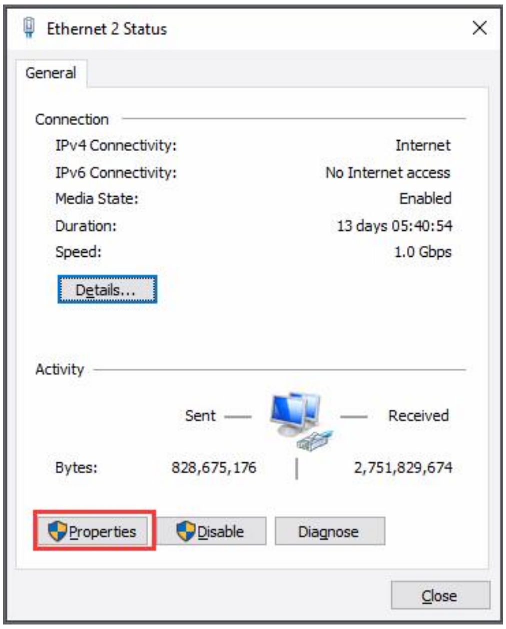
Troubleshoot problems
Diagnose and repair network problems or get troubleshooting information.

See also

Internet Options

Windows Defender Firewall

3. Click **Properties** in the window of **Ethernet Status**.



Ethernet 2 Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 13 days 05:40:54

Speed: 1.0 Gbps

Details...

Activity

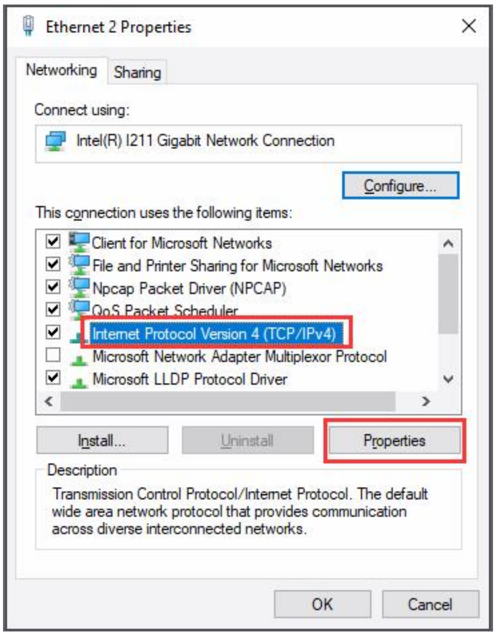
Sent — — Received

Bytes: 828,675,176 | 2,751,829,674

Properties Disable Diagnose

Close

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



Ethernet 2 Properties

Networking | Sharing

Connect using:

Intel(R) I211 Gigabit Network Connection

Configure...

This connection uses the following items:

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

Install... | Uninstall | Properties

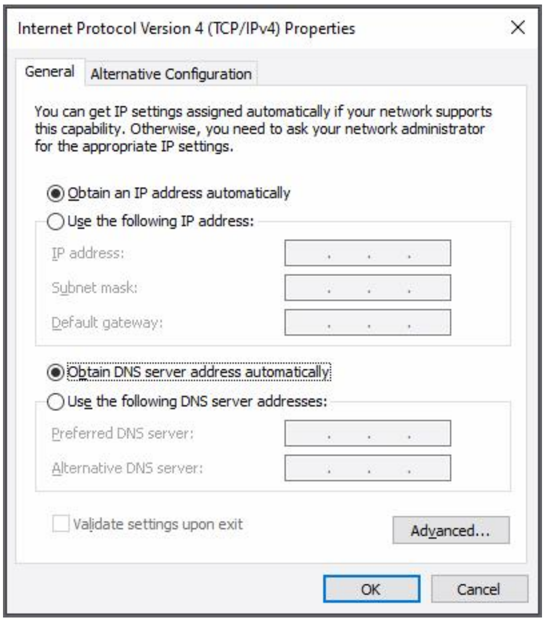
Description

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

OK | Cancel

5. Two ways to configure the computer’s IP address.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternative Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

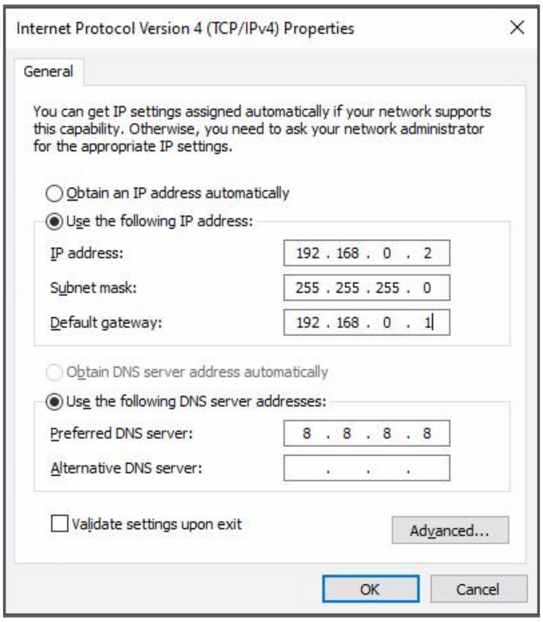
Alternative DNS server: . . .

□ Validate settings upon exit

Advanced...

OK | Cancel

(2) Manually configure the PC with a static IP address: Select "**Use the following IP address"** and enter an IP address within the same subnet as the device.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternative DNS server: . . .

□ Validate settings upon exit

6. Click OK to finish the configuration.

2.2 Factory Default Settings

Before configuring your device, please familiarize yourself with the following default settings.

Item	**Description**
Username	admin
Password	Refer to the information on the product label
ETH 0	WAN mode or 192.168.0.1/255.255.255.0 (LAN mode)
ETH 1/2 (*)	192.168.0.1/255.255.255.0 (LAN mode)
DHCP Server	Enabled

***Note:** The number of Ethernet ports may vary by model. Please refer to the product specifications for the corresponding model for the exact number.

2.3 Factory Reset

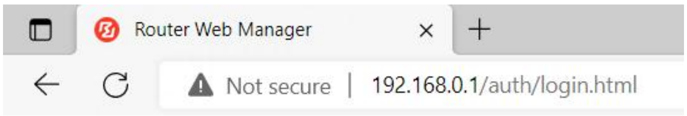
Function	**Operation**
Reboot	Press and hold the RST button for 2 to 5 seconds while the device is operational.
Restore to default configuration	Press and hold the RST button for 5 to 10 seconds while the device is operational. After that, the RUN light will flash quickly; then release the RST button, and the device will restore to its default configuration.
Restore to factory configuration	If the operation to restore the default configuration is performed twice within one minute, the device will revert to its 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.

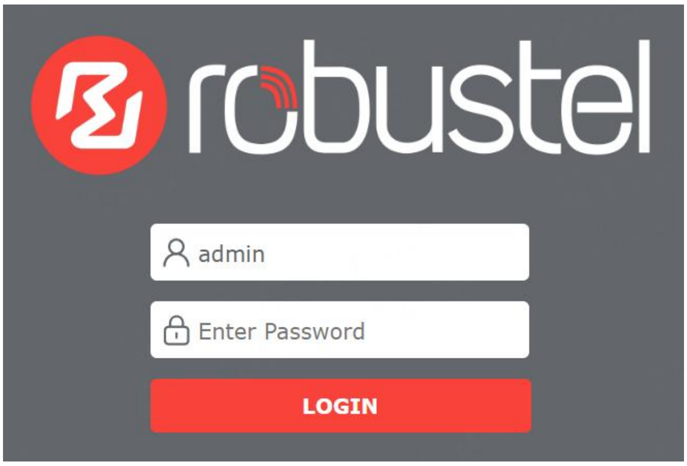
1. Open a web browser on your PC (e.g., Microsoft Edge, Google Chrome or Firefox)
2. Type the device's IP address in the address bar and press **Enter**. The default IP address of the device is http://192.168.0.1/ , actual address may vary.

   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.



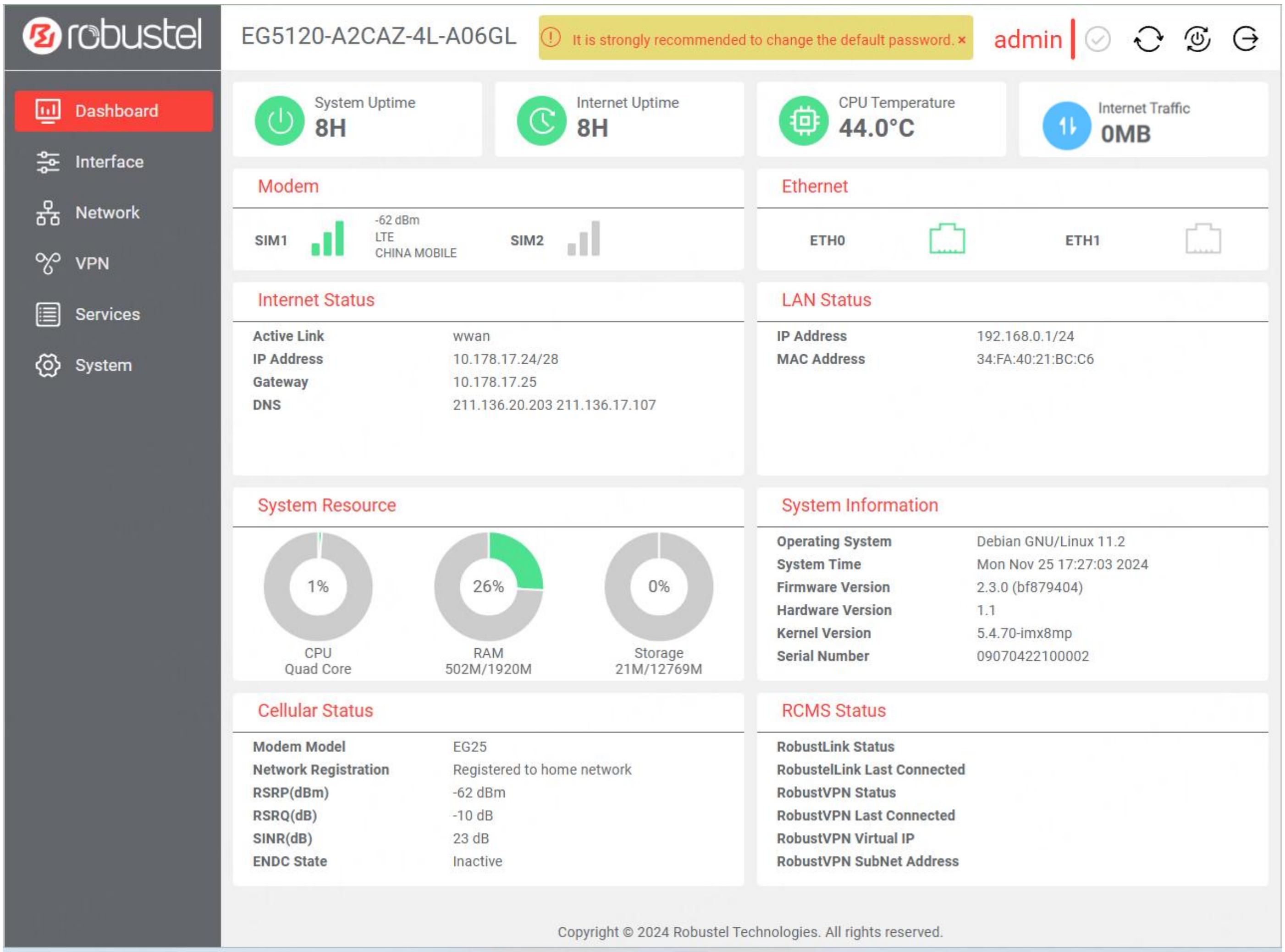
192.168.0.1/auth/login.html

3. On the login page, enter the username and password (refer to the device's label for login information), then click **LOGIN**.



2.5 Control Panel

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



It is strongly recommended to change the default password. ×

System Uptime	Internet Uptime	CPU Temperature	Internet Traffic
8H	8H	44.0°C	0MB

Modem

SIM1 -62 dBm LTE CHINA MOBILE SIM2

Ethernet

ETH0 ETH1

Internet Status

Active Link	wwan
IP Address	10.178.17.24/28
Gateway	10.178.17.25
DNS	211.136.20.203 211.136.17.107

LAN Status

IP Address	192.168.0.1/24
MAC Address	34:FA:40:21:BC:C6

System Resource

1%	26%	0%
CPU Quad Core	RAM 502M/1920M	Storage 21M/12769M

System Information

Operating System	Debian GNU/Linux 11.2
System Time	Mon Nov 25 17:27:03 2024
Firmware Version	2.3.0 (bf879404)
Hardware Version	1.1
Kernel Version	5.4.70-imx8mp
Serial Number	09070422100002

Cellular Status

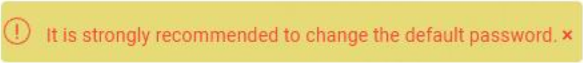
Modem Model	EG25
Network Registration	Registered to home network
RSRP(dBm)	-62 dBm
RSRQ(dB)	-10 dB
SINR(dB)	23 dB
ENDC State	Inactive

RCMS Status

RobustLink Status
RobustelLink Last Connected
RobustVPN Status
RobustVPN Last Connected
RobustVPN Virtual IP
RobustVPN SubNet Address

Copyright © 2024 Robustel Technologies. All rights reserved.

After logging in with the default username and password, the following notification will appear in a new tab:


It is strongly recommended to change the default password. ×

For security reasons, it is strongly recommended that you change the default username and/or password. Click the × button to close the notification. To change your username and/or password, refer to section **3.7.10 System > User Management**.

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

Control Panel		
Item	**Description**	**Icon**
Save & Apply	By default, this icon is gray. If any modifications are made to the configuration, it will turn red. Click this button to apply all submitted configuration changes.	✓ or ✓
Restart	Click this option to restart all applications and return to the login page.	↻
Reboot	Click this option to reboot the gateway and return to the login page.	⏻
Logout	Click this option to safely log out the current user. After logging out, you will be redirected to the login page. If the webpage is closed without logging out, the next user can log in on this browser without a password until the session times out.	⇥

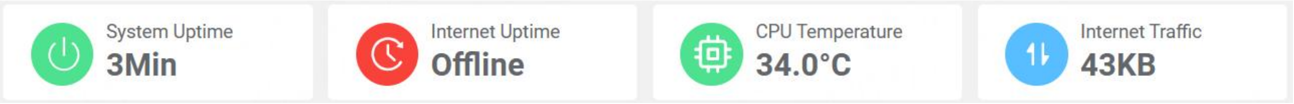
Note: The steps to modify configuration are as bellow:

1. Make modifications on one page;
2. Click Submit on this page;
3. Make modifications on another page;
4. Click Submit on this page;
5. Complete all modification;
6. Click ✓ to save and apply the changes.

Chapter 3 WebUI Descriptions

3.1 Dashboard

3.1.1 Overview



System Uptime
3Min

Internet Uptime
Offline

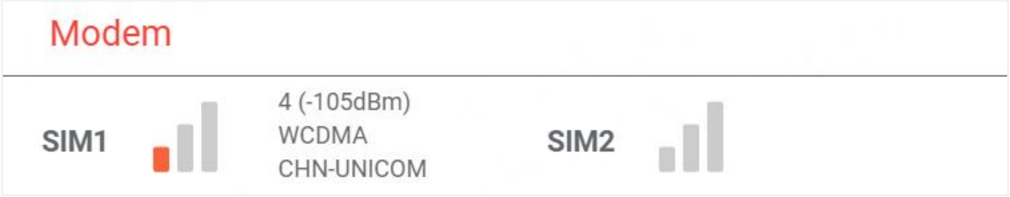
CPU Temperature
34.0°C

Internet Traffic
43KB

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

3.1.2 Modem

This page shows the status of SIM card.



Modem

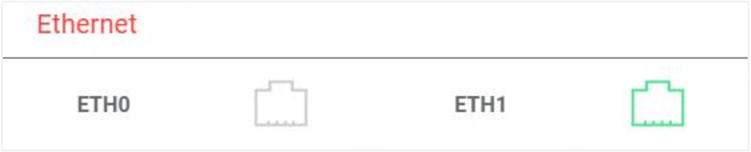
SIM1
4 (-105dBm)
WCDMA
CHN-UNICOM

SIM2

Icon	Description
⬜⬜⬜	Not connected.
🟥⬜⬜	Weak signal.
🟨🟨⬜	Medium signal.
🟩🟩🟩	Strong signal.

3.1.3 Ethernet

This page provide information about the Ethernet port status.



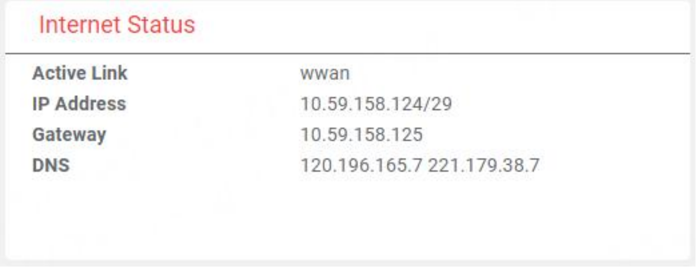
Ethernet

ETH0 □ ETH1 🟩

Icon	Description
□	Port disabled or link down.
🟩	Link up.

3.1.4 Internet Status

This page shows the device’s internet status information.



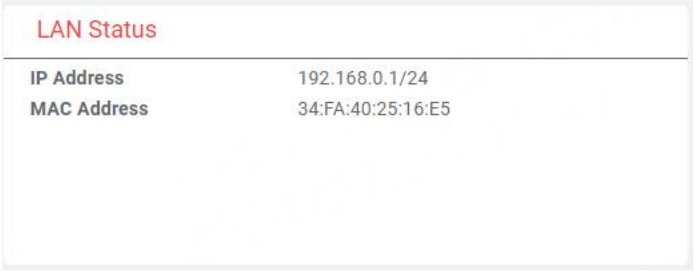
Internet Status

Active Link wwan
IP Address 10.59.158.124/29
Gateway 10.59.158.125
DNS 120.196.165.7 221.179.38.7

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

3.1.5 LAN Status

This page shows the device’s LAN status.



LAN Status

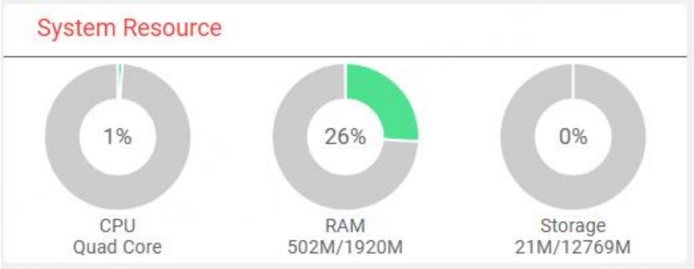
IP Address 192.168.0.1/24
MAC Address 34:FA:40:25:16:E5

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

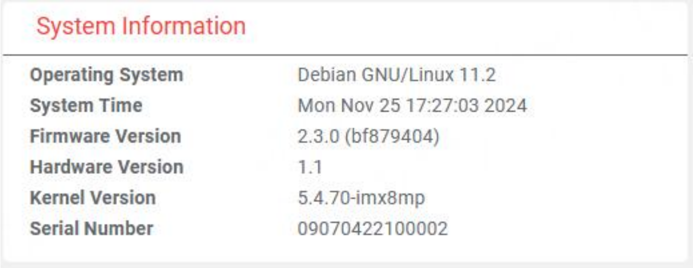
This page shows the device’s system resources usage information.

- When usage exceeds 95%, the icon will be red.
- When usage is between 80% and 94%, the icon will be yellow.
- When usage is below 79%， the icon will be green.



3.1.7 System Information

This page shows the device’s system information.



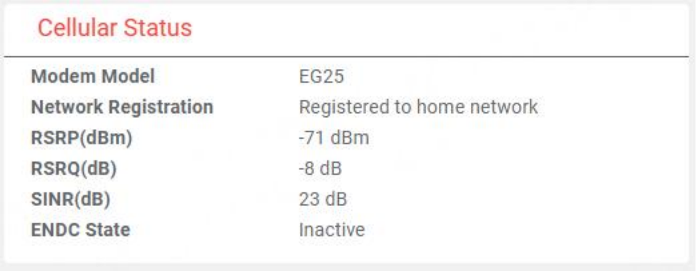
System Information

Operating System	Debian GNU/Linux 11.2
System Time	Mon Nov 25 17:27:03 2024
Firmware Version	2.3.0 (bf879404)
Hardware Version	1.1
Kernel Version	5.4.70-imx8mp
Serial Number	09070422100002

Item	Description
Operating System	Show the operating system information.
System Time	Show the current system time.
Firmware Version	Show the firmware version currently 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 displays the device’s cellular status.



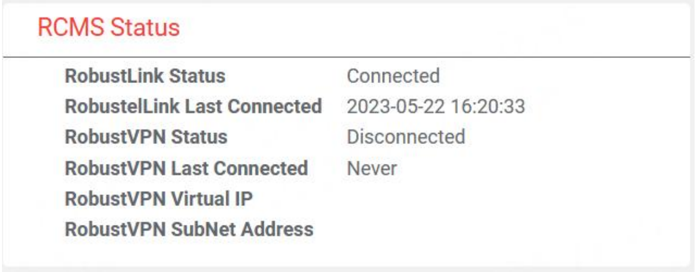
Cellular Status

Modem Model	EG25
Network Registration	Registered to home network
RSRP(dBm)	-71 dBm
RSRQ(dB)	-8 dB
SINR(dB)	23 dB
ENDC State	Inactive

Item	Description
Modem Model	Show the module information.
Network Registration	Show the current network registration information.
RSRP(dBm)	Show the current RSRP when connected to the 4G network.
RSRQ(dB)	Show the current RSRQ when connected to the 4G network.
SINR(dB)	Show the current SINR when connected 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.



RCMS Status

RobustLink Status	Connected
RobustelLink Last Connected	2023-05-22 16:20:33
RobustVPN Status	Disconnected
RobustVPN Last Connected	Never
RobustVPN Virtual IP	
RobustVPN SubNet Address	

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

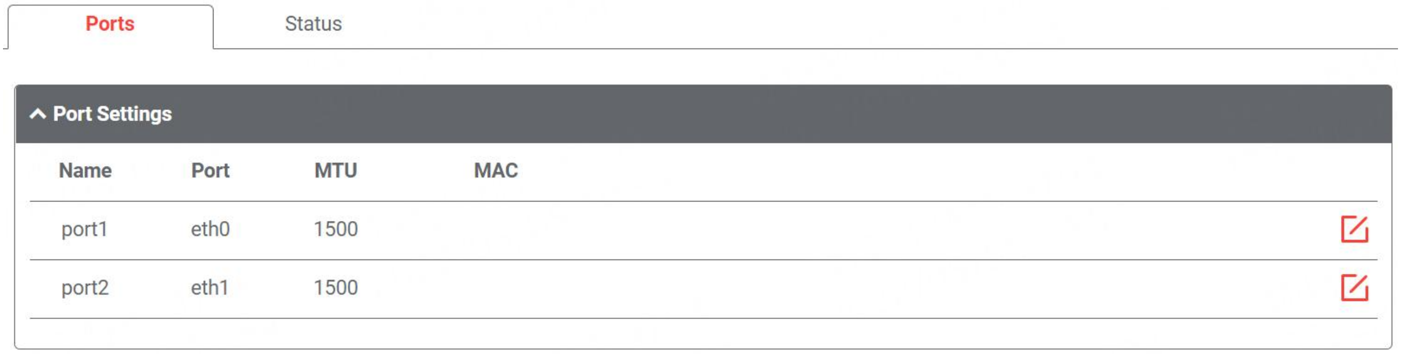
3.2 Interface

3.2.1 Ethernet

This section allows you to configure the parameters for Ethernet. The device may have multiple Ethernet ports, each of which can be set as either a WAN or LAN port. By default, all Ethernet ports are configured as **lan0**, with a default IP address of **192.168.0.1** and a subnet mask of **255.255.255.0.**

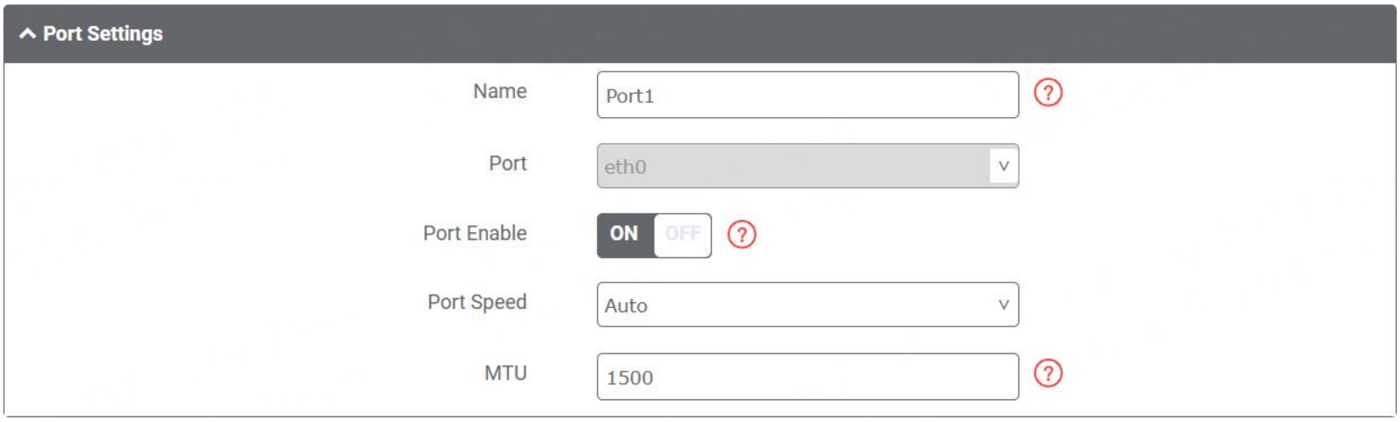
Note: Some devices may also support PoE (Power over Ethernet). For example, LG5100 and R1520LG ETH0 supports POE-PD functionality.

Ports



Name	Port	MTU	MAC
port1	eth0	1500	
port2	eth1	1500	

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

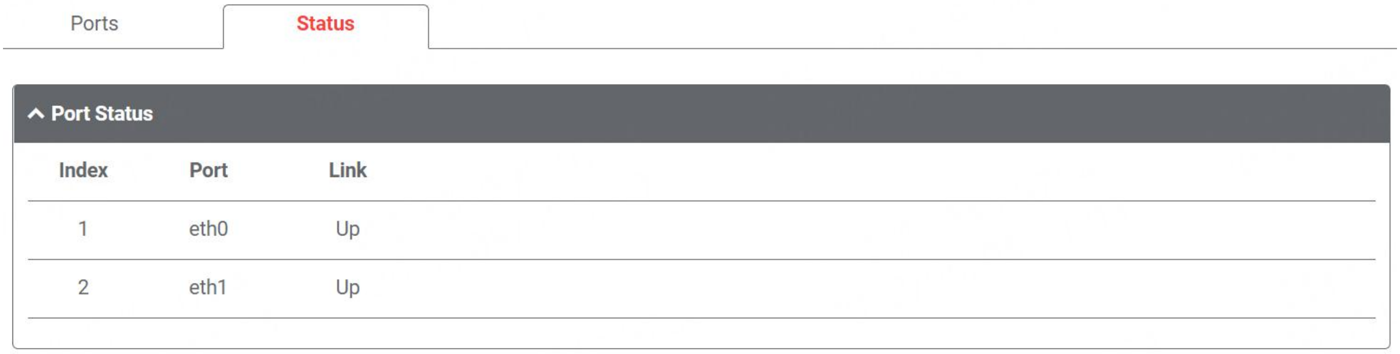


Name	Port1
Port	eth0
Port Enable	ON
Port Speed	Auto
MTU	1500

Item	Description	Default
Name	Show the name of the port.	--
Port	Show the editing port (read only).	--
Port Enable	Click the toggle button to enable or disable the Ethernet port.	ON
Port Speed	Choose from the following options: “Auto”, “10M-half”, “10M-full”, “100M-half”, “100M-full”, “1000M-half”, “1000M-full”.	Auto
MTU	Enter the value of the maximum transmission unit (MTU).	1500

Status

This page displays the status of Ethernet port.

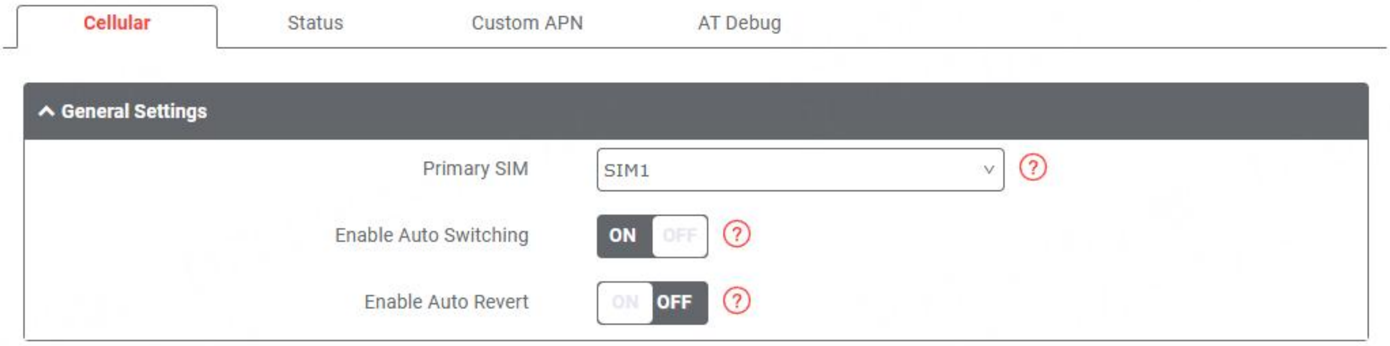


Index	Port	Link
1	eth0	Up
2	eth1	Up

3.2.2 Cellular

This section allows you to configure the parameters for the cellular connection.

Cellular

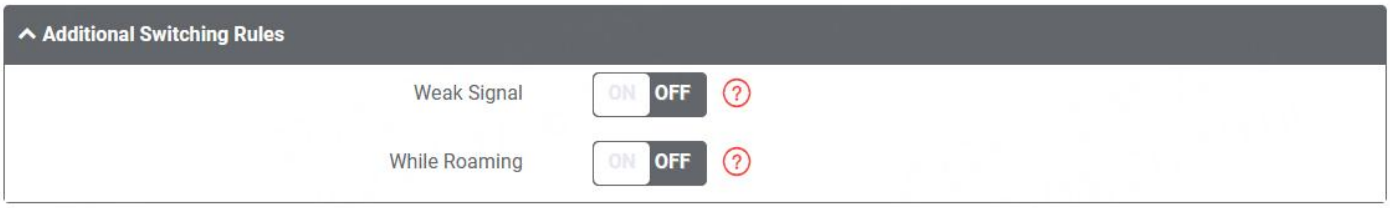


Primary SIM: SIM1

Enable Auto Switching: ON

Enable Auto Revert: OFF

Item	Description	Default
Primary SIM	Choose one SIM card to serve as the primary SIM card.	SIM1
Enable Auto Switching	When auto switching is enabled, the SIM card will automatically switch to the other one in the event of a SIM card error, connection error or ping failure by default.	ON
Enable Auto Revert	When Auto Revert is enabled, the backup SIM card will be automatically switched to the primary SIM card if its online time exceeds the revert interval time.	OFF

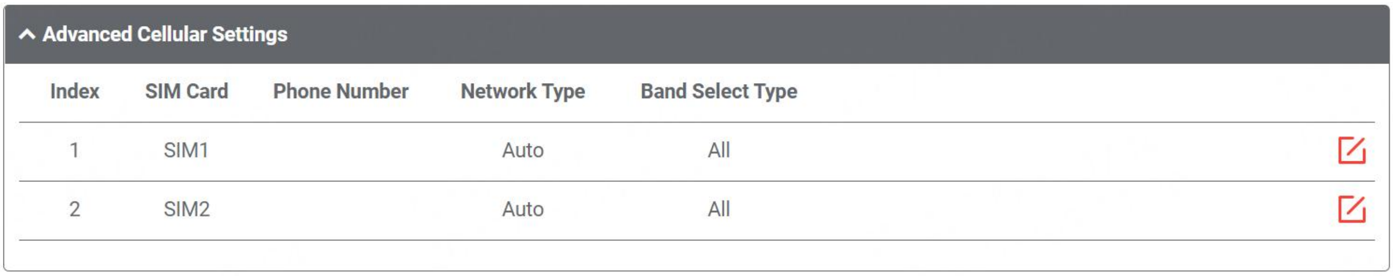


Additional Switching Rules

Weak Signal ON OFF

While Roaming ON OFF

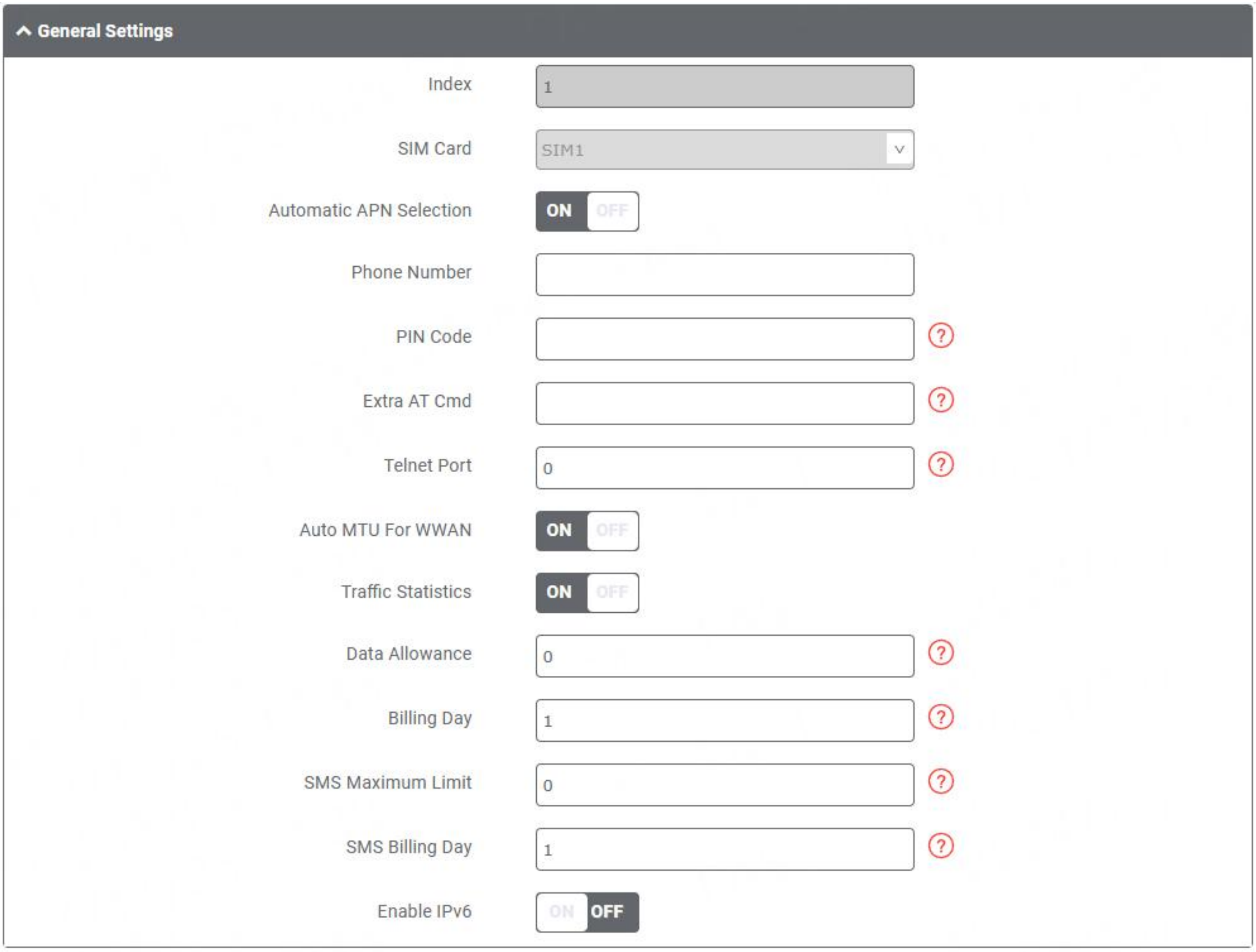
Item	Description	Default
Weak Signal	Switch to another SIM card when the signal is poor. This feature is only applicable for dual SIM backup.	ON
While Roaming	Switch to another SIM card while roaming. This feature is only applicable for dual SIM backup.	OFF



Advanced Cellular Settings

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

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



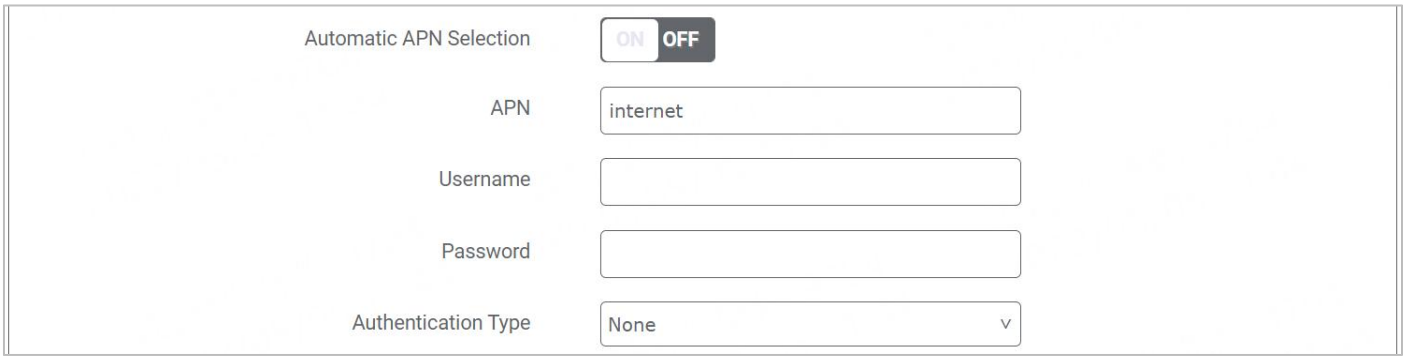
General Settings

Index	1
SIM Card	SIM1
Automatic APN Selection	ON
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0
Auto MTU For WWAN	ON
Traffic Statistics	ON
Data Allowance	0
Billing Day	1
SMS Maximum Limit	0
SMS Billing Day	1
Enable IPv6	OFF

Item	Description	Default
Index	Indicate the ordinal position in 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 automatically recognize the Access Point Name (APN). Alternatively, you can disable this option and manually enter the APN, username, password and authentication type.	ON
Phone Number	Enter the phone number associated with the SIM card.	Null
PIN Code	Enter a 4-8 character PIN code used to unlock the SIM card.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the port for the Telnet service used for AT over Telnet. A value of 0 means the feature is not supported.	0
Auto MTU For WWAN	Set the MTU (Maximum Transmission Unit) value between 1280 and 1500.	1500
Traffic Statistics	Click the toggle button to enable/disable traffic statistics tracking.	ON
Data Allowance	Set the monthly data usage limit. When a data limit is specified, the system will record data usage statistics. A value of "0" disables data usage tracking.	

Billing Day	Specifies the day of the month for billing; data traffic statistics will be recalculated from this day.	1
SMS Maximum Limit	Enter the maximum number of SMS messages that can be sent each month; enter 0 for no limit.	0
SMS Billing Day	Specify the reset date for the monthly SMS count (the starting date for the monthly SMS count).	1
Enable IPv6	Click the toggle button to enable/disable IPv6 support.	OFF

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



Automatic APN Selection: ON OFF

APN: internet

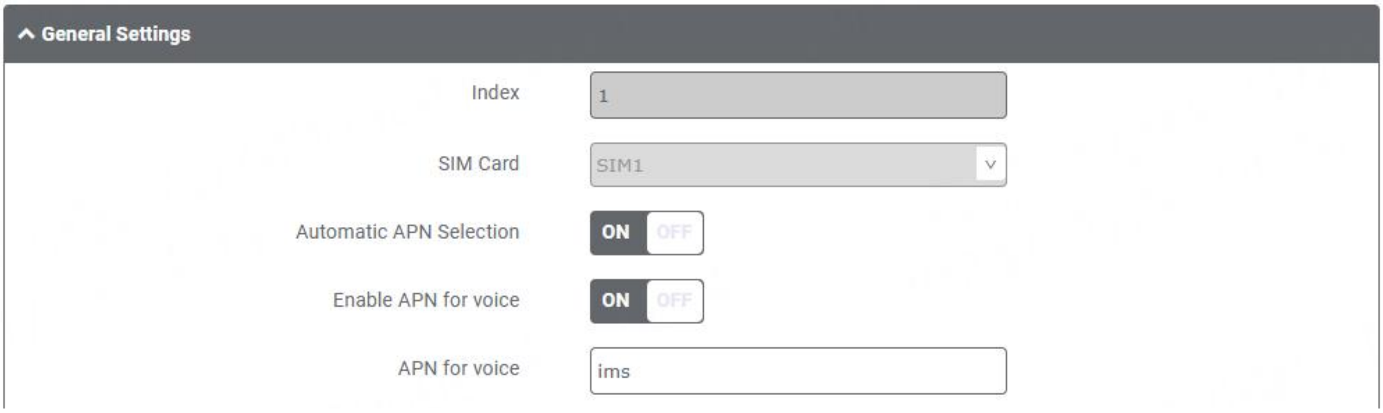
Username:

Password:

Authentication Type: None

Item	Description	Default
Automatic APN Selection	Click the toggle button to enable/disable this option. Enable this feature for automatic APN configuration.	OFF
APN	Enter the APN for cellular dial-up connection, as provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, as provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, as provided by local ISP.	Null
Authentication Type	Select the authentication type from the following options: • None: No authentication required. • CHAP: Challenge-Handshake Authentication Protocol. • PAP: Password Authentication Protocol.	None

When the **APN for Voice** is enabled, users can configure their own voice APN as needed. This feature is supported only on the **EV8100** model.



General Settings

Index: 1

SIM Card: SIM1

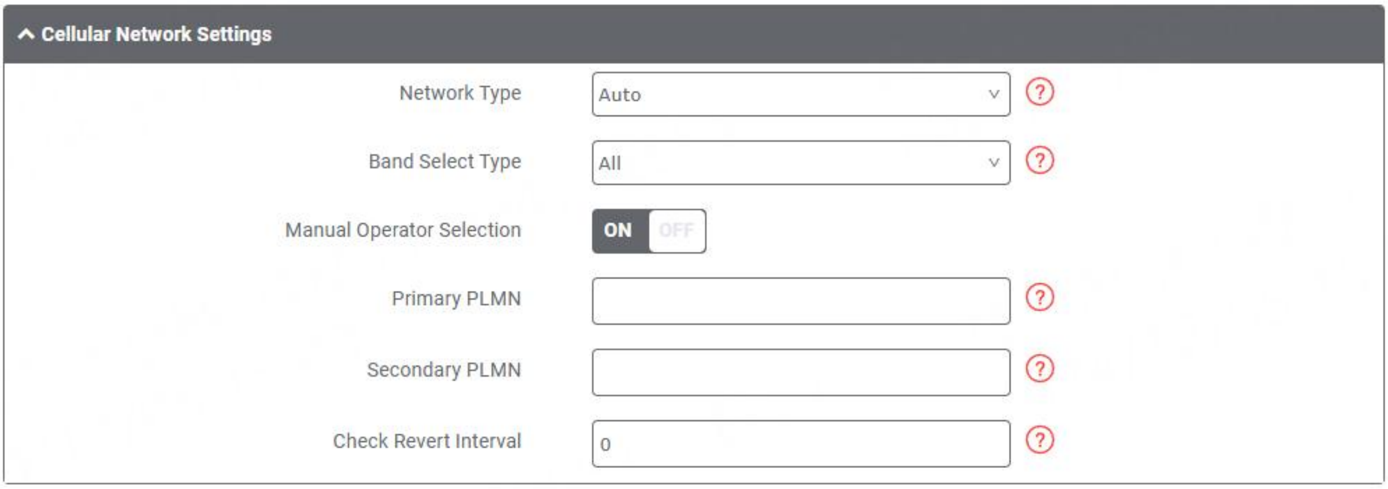
Automatic APN Selection: ON OFF

Enable APN for voice: ON OFF

APN for voice: ims

Item	Description	Default
Enable APN for voice	Click the toggle button to enable/disable the option (Supported only on EV8100).	OFF
APN for voice	Enter the APN for voice services, as provided by the local ISP.	ims

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



Cellular Network Settings

Network Type: Auto

Band Select Type: All

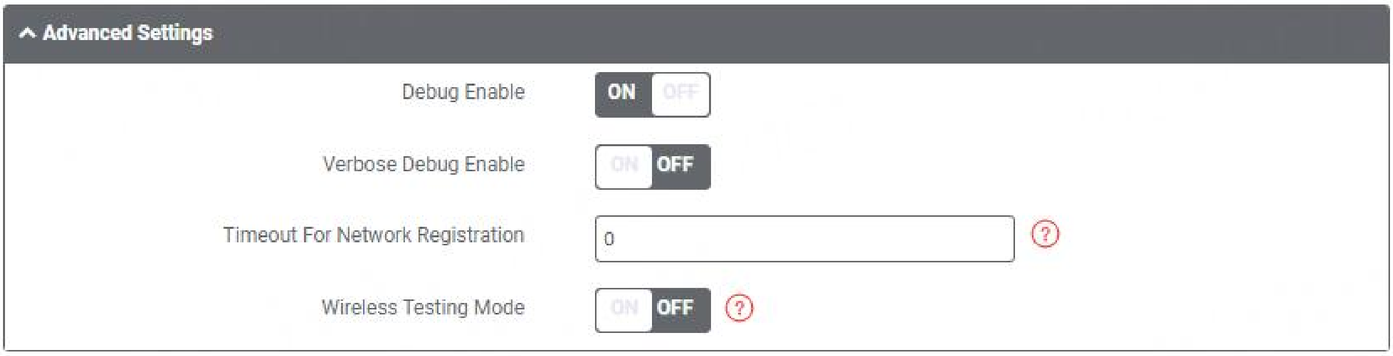
Manual Operator Selection: ON

Primary PLMN:

Secondary PLMN:

Check Revert Interval: 0

Item	Description	Default
Network Type	Select the cellular network type which determines the network access order. Choose from the following options: • Auto: Connect to the best available signal automatically. • 2G Only: Connect only to the 2G network. • 3G Only: Connect only to the 3G network. • 4G Only: Connect only to the 4G network. • 5G Only: Connect only to the 5G network. **Note:** The available network types may vary depending on the cellular module.	Auto
Band Select Type	Choose from “All” or “Specify”. You may choose certain bands if you choose “Specify”. **Note:** There may be differences in Band Settings depending on the cellular module.	All
Manual Operator Selection	Click the toggle button to enable/disable the option.	OFF
Primary PLMN	Input the primary carrier.	null
Secondary PLMN	Input the backup carrier.	null
Check Revert Interval	Input the interval for checking recovery time (unit: minutes). Enter **0** to disable the check.	0



Advanced Settings

Debug Enable: ON

Verbose Debug Enable: OFF

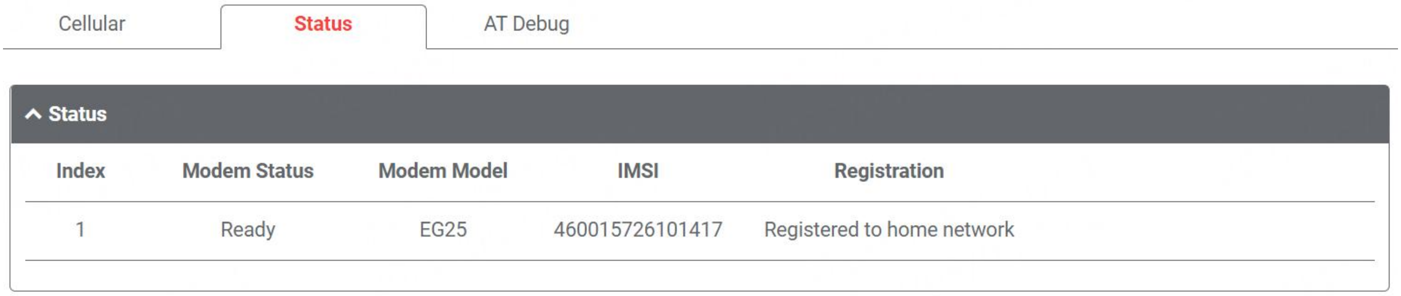
Timeout For Network Registration: 0

Wireless Testing Mode: OFF

Item	Description	Default
Debug Enable	Click the toggle button to enable/disable this option. Enable it for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable it for verbose debugging information output.	OFF
Timeout For Network Registration	Specify the timeout required for the module to register to the network (unit: seconds). Enter **0** to use the default setting.	0
Wireless Testing Mode	This option can only be enabled during laboratory testing while connected to a wireless tester. It must be turned off when connected to a real network!	OFF

Status

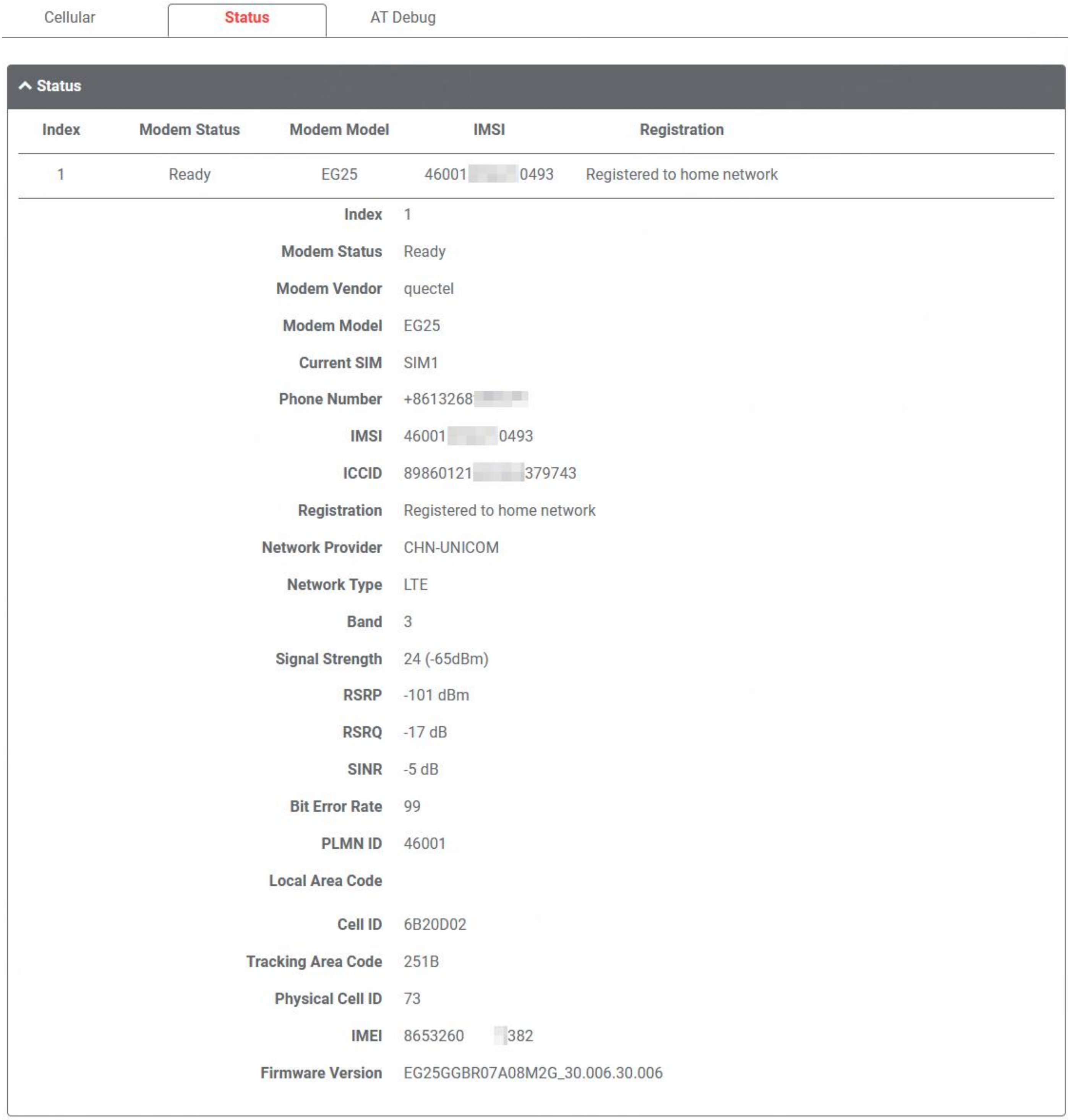
This page displays the status of the cellular connection.



Status

Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EG25	460015726101417	Registered to home network

Click the row displaying the status to view detailed status information below it.



^ Status

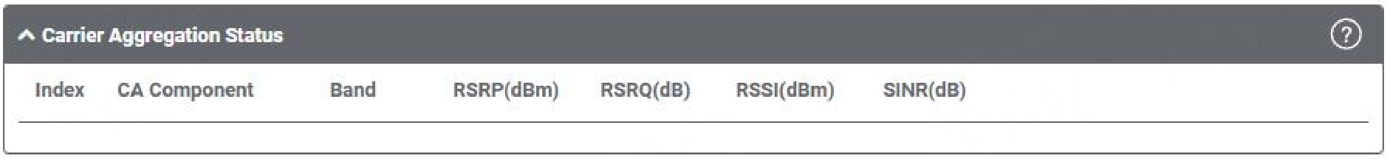
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EG25	46001[redacted]0493	Registered to home network

Index	1
Modem Status	Ready
Modem Vendor	quectel
Modem Model	EG25
Current SIM	SIM1
Phone Number	+8613268[redacted]
IMSI	46001[redacted]0493
ICCID	89860121[redacted]379743
Registration	Registered to home network
Network Provider	CHN-UNICOM
Network Type	LTE
Band	3
Signal Strength	24 (-65dBm)
RSRP	-101 dBm
RSRQ	-17 dB
SINR	-5 dB
Bit Error Rate	99
PLMN ID	46001
Local Area Code	
Cell ID	6B20D02
Tracking Area Code	251B
Physical Cell ID	73
IMEI	8653260[redacted]382
Firmware Version	EG25GGBR07A08M2G_30.006.30.006

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 associated with the current SIM.
IMSI	Show the International Mobile Subscriber Identity (IMSI) number of the current SIM.

Item	Description
ICCID	Show the Integrated Circuit Card Identifier(ICCID) number of the current SIM.
Registration	Show the current network registration status.
Network Provider	Show the name of the network provider.
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 device.
RSRP	Show the current Reference Signal Received Power (RSRP) when connected to the 4G network.
RSRQ	Show the current Reference Signal Received Quality (RSRQ) when connected to the 4G network.
SINR	Show the current Signal-to-Interference-plus-Noise Ratio (SINR) when connected to the 5G network.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current Public Land Mobile Network (PLMN) ID.
Local Area Code	Show the current local area code used for identifying different areas.
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 International Mobile Equipment Identity (IMEI) number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

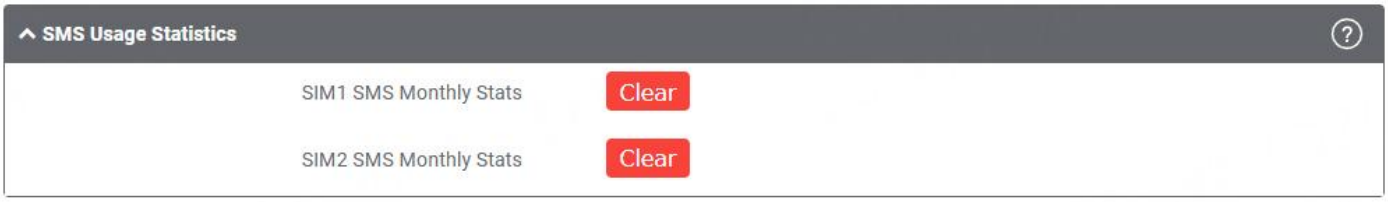
This section is used to display the status of carrier aggregation.


^ Carrier Aggregation Status

Index	CA Component	Band	RSRP(dBm)	RSRQ(dB)	RSSI(dBm)	SINR(dB)

Note: Only supported by 5G devices.

This section is used to display the SMS usage statistics status.

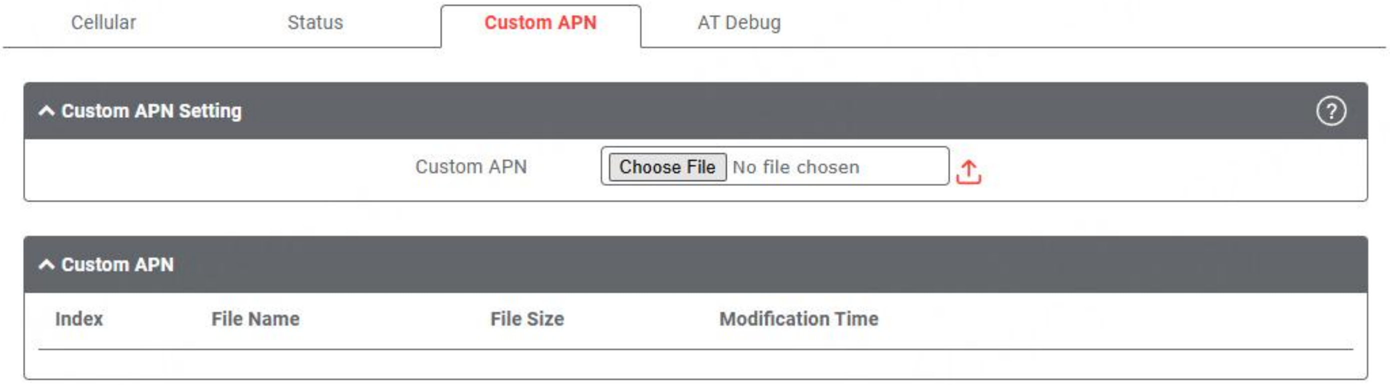

^ SMS Usage Statistics

SIM1 SMS Monthly Stats Clear

SIM2 SMS Monthly Stats Clear

Custom APN

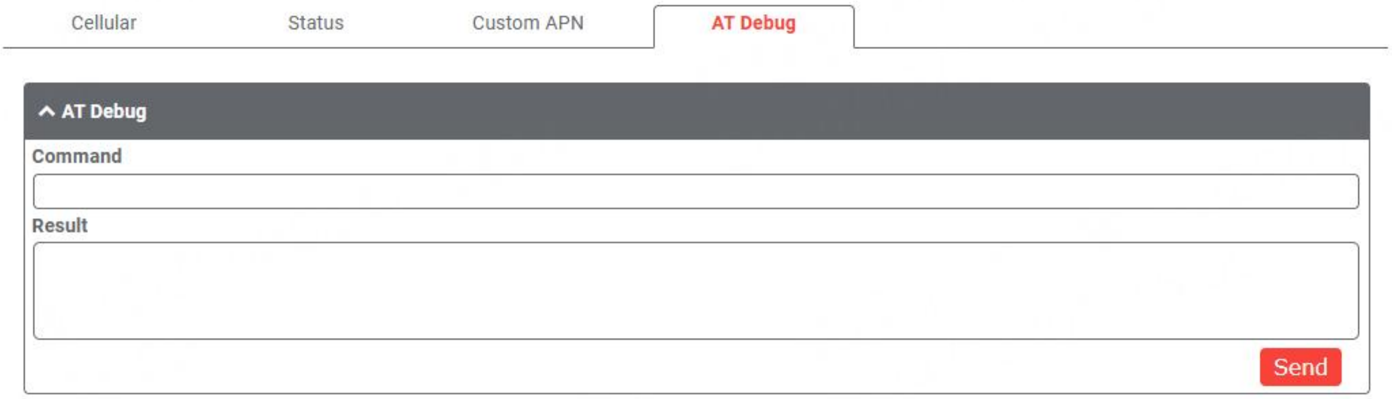
This page allows you to import the customer's custom APN list.



Index	File Name	File Size	Modification Time

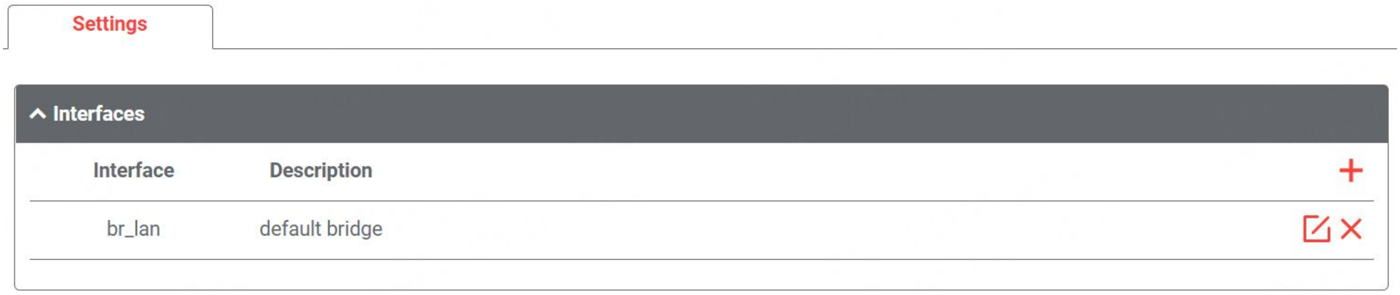
AT Debug

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



3.2.3 Bridge

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

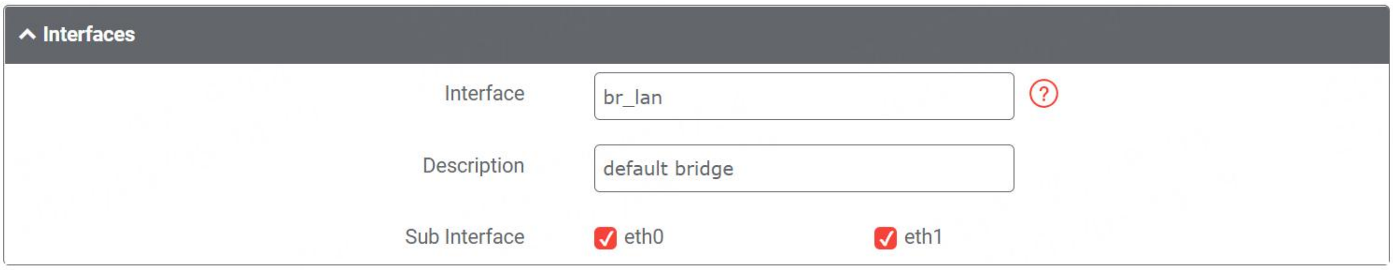


Interface	Description
br_lan	default bridge

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.



Interfaces

Interface	br_lan
Description	default bridge
Sub Interface	☑ eth0 ☑ eth1

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

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

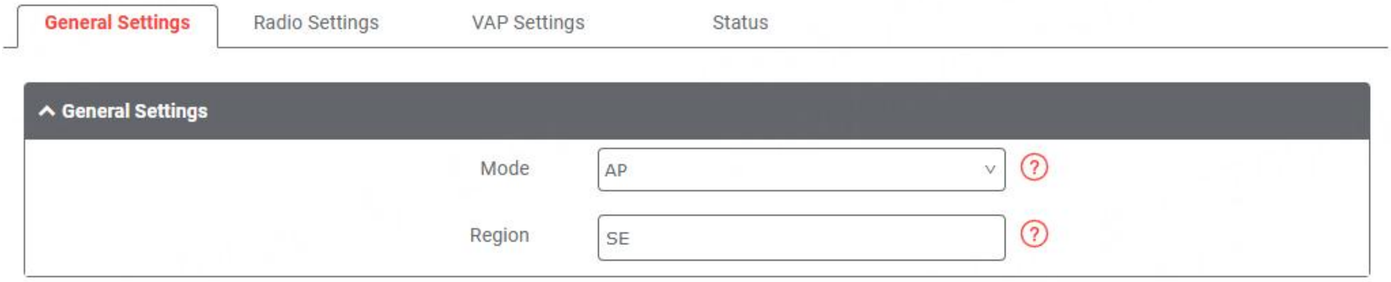
3.2.4 Wi-Fi

This section allows you to configure the parameters of Wi-Fi AP mode.

Mode

Products that support Wi-Fi AP mode or Client mode:

- EG5120, EG5100, EV8100

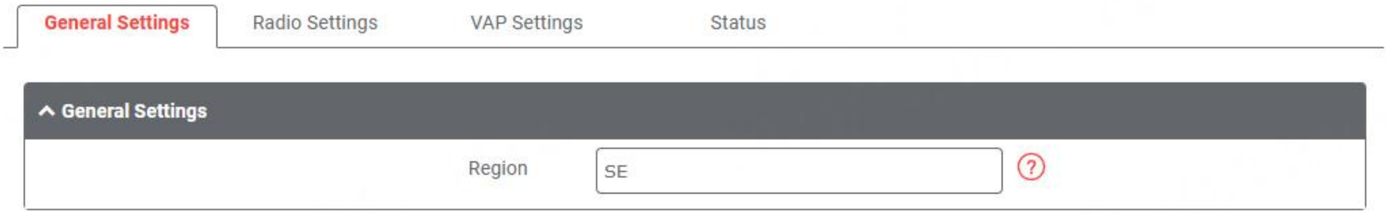


General Settings

Mode	AP
Region	SE

Products that support the simultaneous use of Wi-Fi AP mode and client mode:

- EG5200



General Settings

Region: SE

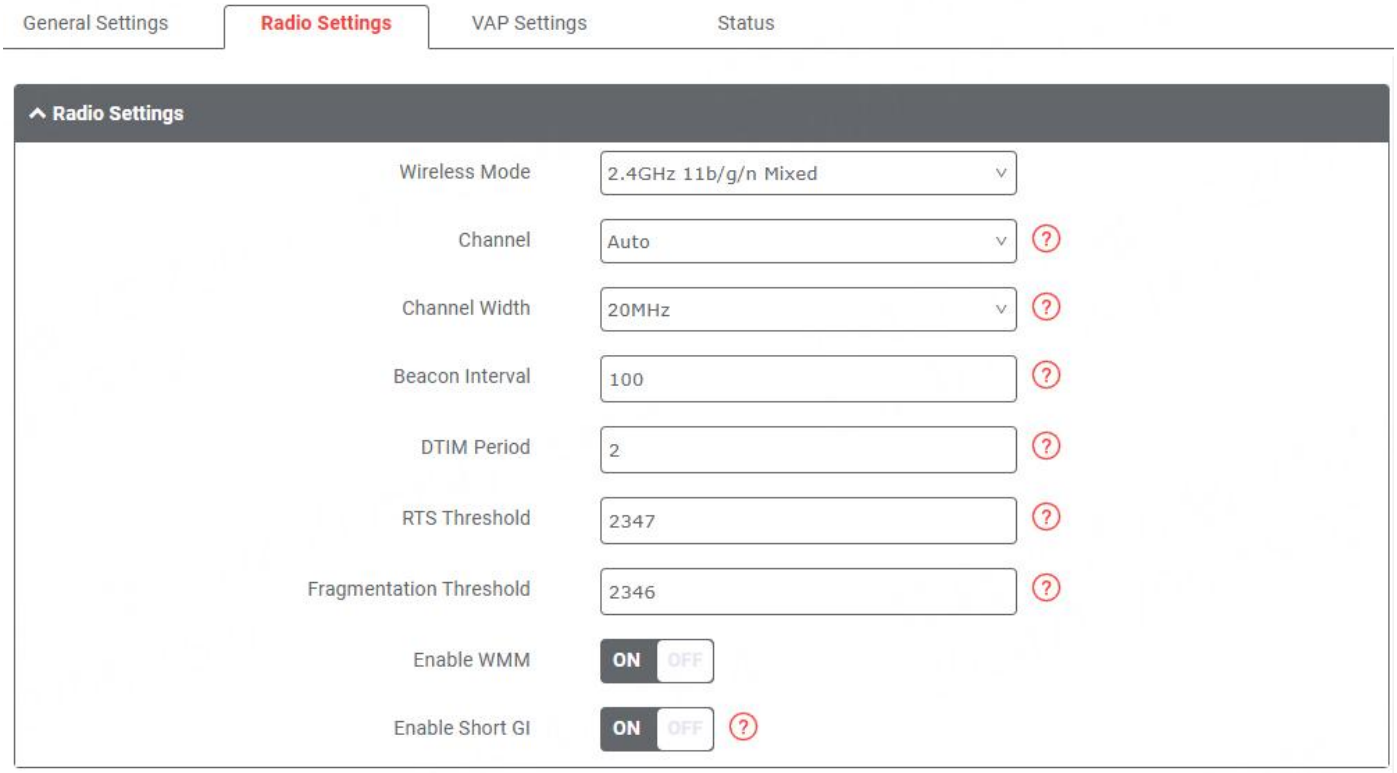
Item	Description
Mode	Select the wireless mode for the device: . ● **AP**: The device acts as the center of the network, providing wireless connections for other devices. ● **Client**: The device connects to an existing Wi-Fi network rather than creating its own network.
Region	Select the region for the Wi-Fi. The available channels vary by country and region.

Radio

Radio Settings

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

- EG5120, EG5100, EV8100



Radio Settings

Wireless Mode: 2.4GHz 11b/g/n Mixed

Channel: Auto

Channel Width: 20MHz

Beacon Interval: 100

DTIM Period: 2

RTS Threshold: 2347

Fragmentation Threshold: 2346

Enable WMM: ON

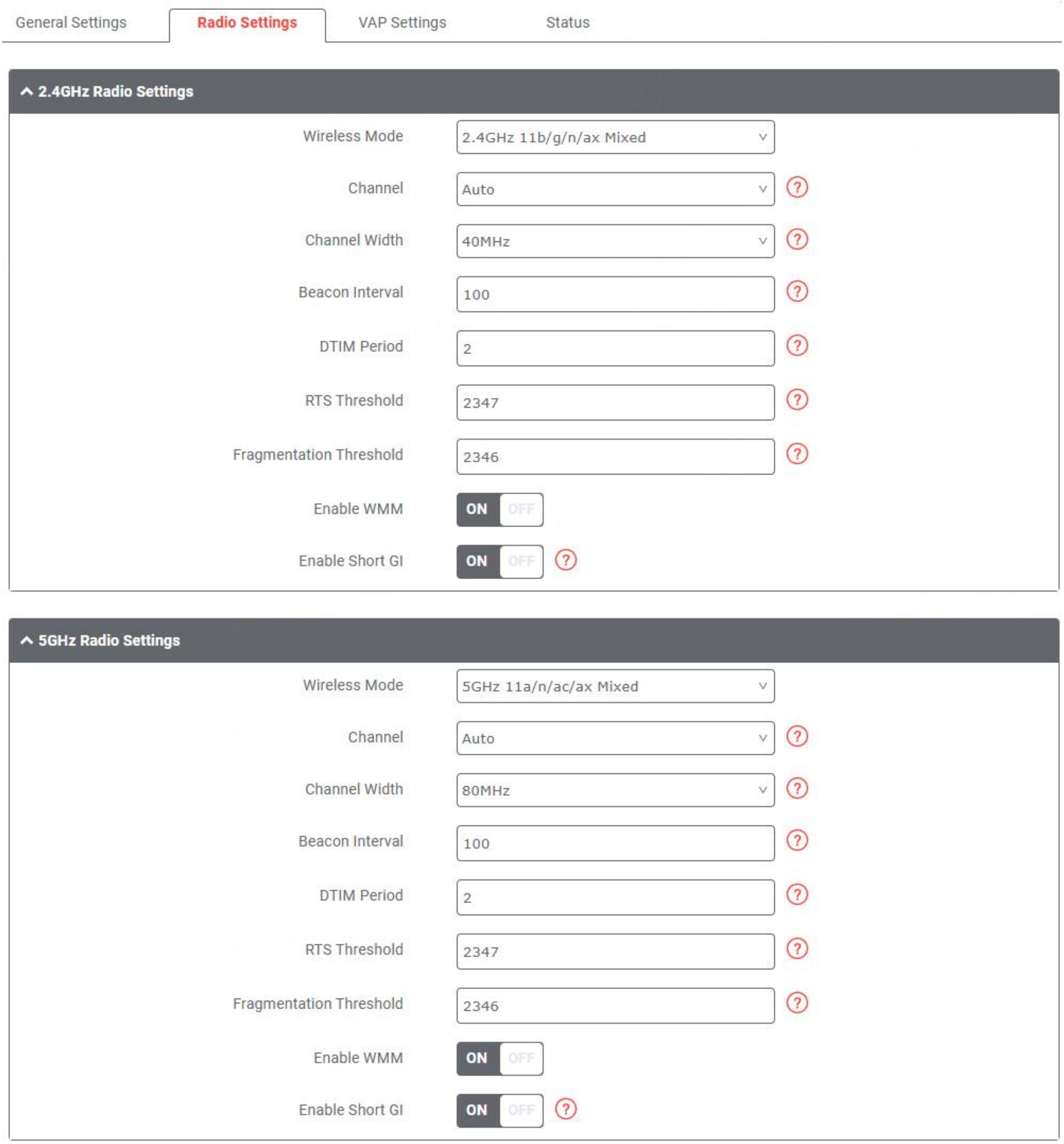
Enable Short GI: ON

Item	Description	Default
Wireless Mode	Select from "2.4GHz 11b/g/n Mixed", "2.4GHz Only 11b", "2.4GHz Only 11g", "2.4GHz Only 11n", "5GHz 11a/an/ac Mixed" or "5GHz Only 11a/n Mixed Mode". • 2.4GHz 11b/g/n Mixed Mode: Mixed IEEE 802.11b/g/n protocols for backward compatibility. • 2.4GHz Only 11b: IEEE 802.11b. • 2.4GHz Only 11g: IEEE 802.11g. • 2.4GHz Only 11n: IEEE 802.11n. • 5GHz 11a/an/ac Mixed Mode: IEEE 802.11a/an/ac. • 5GHz 11a/n Mixed Mode: IEEE 802.11a/n.	2.4GHz 11b/g/n Mixed Mode
Channel	Select a channel from "Auto", "1", "2", ··· "13" or "36", "40", "44", "48", "149", "153", "157", "161" ,"165". • 1~13: The gateway will be fixed to work with this channel. • Auto: The device will continuously scan all frequencies until a usable one is found. • Others: The gateway will be fixed to work with this channel. 2.4 GHz: 20/40 MHz bandwidth corresponding to the frequencies of channels 1~13: 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 5 GHz: 20/40/80 MHz bandwidth corresponding to the frequencies of channels 36~165: 36-5180 MHz 40-5200 MHz 44-5220 MHz 48-5240 MHz 149-5745 MHz 153-5765 MHz 157-5785 MHz 161-5805 MHz 165-5825 MHz **Note:** The above lists all available channels for 5GHz Wi-Fi at different	Auto

Item	Description	Default
	bandwidths. The available channels may vary by country and region, and the configuration area needs to be set in the WEB page.	
Channel Width	Select from “40MHz” or “20MHz”.	20MHz
Beacon Interval	Set the interval time for the gateway AP to broadcast beacons used for wireless network authentication.	100
DTIM Period	Set the Delivery Traffic Indication Message (DTIM) period; the AP will multicast data based on this time period.	2
RTS Threshold	Set the Request to Send (RTS) threshold. When set to 2347, the AP will not send a detection signal before transmitting data. When set to 0, the AP will send a detection signal before transmitting data	2347
Fragmentation Threshold	Set the fragmentation threshold for the Wi-Fi access point. It is recommended to use the default value of 2346.	2346
Enable WMM	A 40 MHz channel width provides a higher available data rate, which is twice that of a 20 MHz channel width.	ON
Enable Short GI	Click the toggle button to enable/disable Short Guard Interval. This is the time gap between two symbols that provides a buffer for signal delay. Using a short guard interval can increase the data rate by 11%, but it may also lead to a higher packet error rate.	ON

Wi-Fi supports both 2.4 GHz and 5 GHz, with products that can support both simultaneously:

- EG5200



2.4GHz Radio Settings

Wireless Mode: 2.4GHz 11b/g/n/ax Mixed
Channel: Auto
Channel Width: 40MHz
Beacon Interval: 100
DTIM Period: 2
RTS Threshold: 2347
Fragmentation Threshold: 2346
Enable WMM: ON
Enable Short GI: ON

5GHz Radio Settings

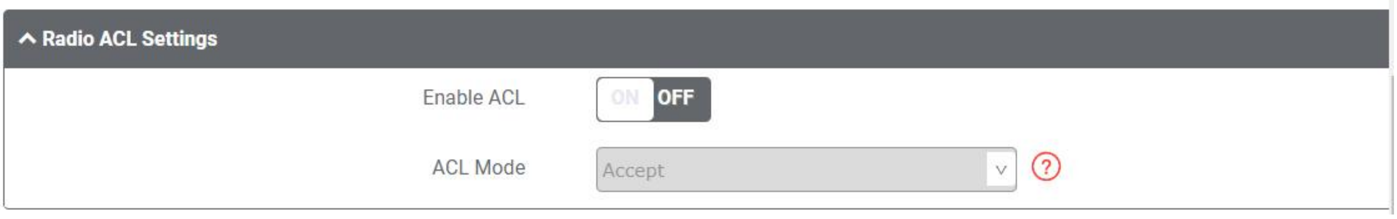
Wireless Mode: 5GHz 11a/n/ac/ax Mixed
Channel: Auto
Channel Width: 80MHz
Beacon Interval: 100
DTIM Period: 2
RTS Threshold: 2347
Fragmentation Threshold: 2346
Enable WMM: ON
Enable Short GI: ON

Item	Description	Default
Wireless Mode@2.4GHz Radio Settings	Select from “2.4GHz 11b/g/n/ax Mixed”, “2.4GHz 11b/g/n Mixed”, “2.4GHz Only 11b,”, “2.4GHz Only 11g,” or “2.4GHz Only 11n,”. • 2.4GHz 11b/g/n/ax Mixed Mode: Mixed IEEE 802.11b/g/n/ax protocols for backward compatibility.	2.4GHz 11b/g/n Mixed

Item	Description	Default
	• 2.4GHz 11b/g/n Mixed Mode: Mixed IEEE 802.11b/g/n protocols for backward compatibility. • 2.4GHz Only 11b: IEEE 802.11b. • 2.4GHz Only 11g: IEEE 802.11g. • 2.4GHz Only 11n: IEEE 802.11n.	
Wireless Mode@5GHz Radio Settings	Select from “5GHz 11a/an/ac/ax Mixed”, “5GHz 11a/an/ac Mixed” or “5GHz Only 11a/n Mixed” • 5GHz 11a/n/ac/ax Mixed Mode: Mixed IEEE 802.11a/n/ac/ax protocols for backward compatibility. • 5GHz 11a/an/ac Mixed Mode: Mixed IEEE 802.11a/an/ac protocols for backward compatibility. • 5GHz 11a/an Mixed Mode: Mixed IEEE 802.11a/an protocols for backward compatibility.	5GHz 11a/an/ac/ax Mixed
Channel@2.4GHz Radio Settings	Select a channel from “Auto,” “1,” “2,” ··· “13,” . • 1~13: The gateway will be fixed to work with this channel. • Auto: The device will continuously scan all frequencies until a usable one is found. • Others: The gateway will be fixed to work with this channel. 2.4 GHz: 20/40 MHz bandwidth corresponding to the frequencies of channels 1~13: 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
Channel@5GHz Radio Settings	Select a channel from “Auto,” “36,” “40,” ... “173.” • Auto: The device will continuously scan all frequencies until a usable one is found. • Others: The gateway will be fixed to work with this channel. 5 GHz: 20/40/80 MHz bandwidth corresponding to the frequencies of channels 36~165: 36-5180 MHz 40-5200 MHz 44-5220 MHz	Auto

Item	Description	Default
	48-5240 MHz 149-5745 MHz 153-5765 MHz 157-5785 MHz 161-5805 MHz 165-5825 MHz **Note:** The above lists all available channels for 5GHz Wi-Fi at different bandwidths. The available channels may vary by country and region, and the configuration area needs to be set in the WEB page.	
Channel Width@2.4GHz Radio Settings	Select from “40MHz” or “20MHz.”	20MHz
Channel Width@5GHz Radio Settings	Select from “80MHz” , “40MHz” or “20MHz.”	80MHz
Beacon Interval	Set the interval time for the gateway AP to broadcast beacons used for wireless network authentication.	100
DTIM Period	Set the Delivery Traffic Indication Message (DTIM) period; the AP will multicast data based on this time period.	2
RTS Threshold	Set the Request to Send (RTS) threshold. When set to 2347, the AP will not send a detection signal before transmitting data. When set to 0, the AP will send a detection signal before transmitting data	2347
Fragmentation Threshold	Set the fragmentation threshold for the Wi-Fi access point. It is recommended to use the default value of 2346.	2346
Enable WMM	A 40 MHz channel width provides a higher available data rate, which is twice that of a 20 MHz channel width.	ON
Enable Short GI	Click the toggle button to enable/disable Short Guard Interval. This is the time gap between two symbols that provides a buffer for signal delay. Using a short guard interval can increase the data rate by 11%, but it may also lead to a higher packet error rate.	ON

Radio ACL Settings



Radio ACL Settings

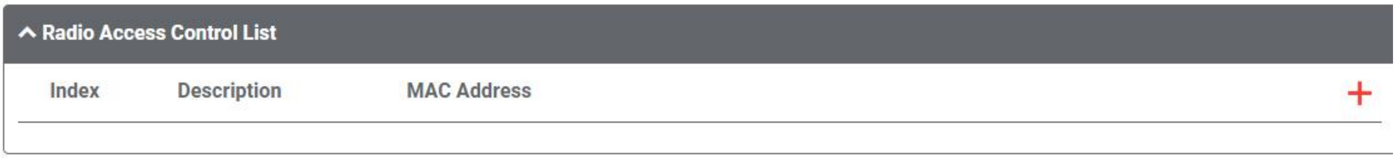
Enable ACL: ON OFF

ACL Mode: Accept

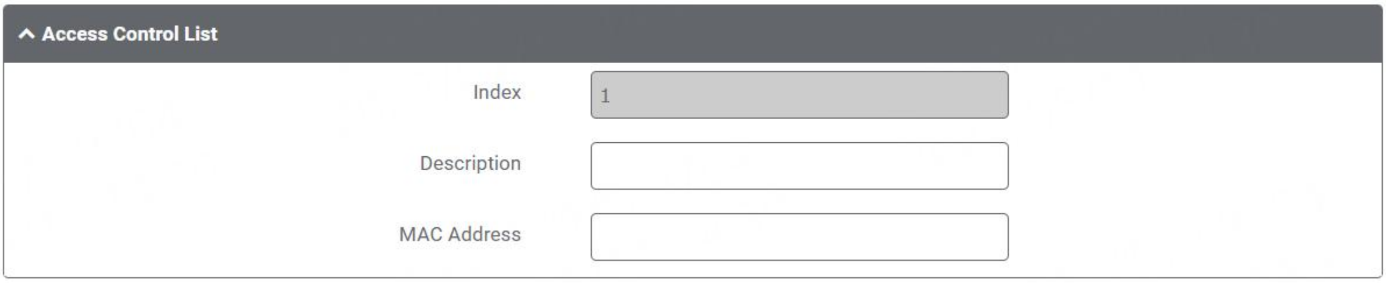
Item	Description	Default
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Choose either “Accept” or “Deny”. • Accept: Only packets that match the entries in the Access Control List	Accept

Item	Description	Default
	(ACL) will be allowed. • Deny: All packets that match the entries in the Access Control List (ACL) will be blocked. **Note:** The router can only allow or deny devices that are included in the Access Control List at any given time.	

Radio Access Control List



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



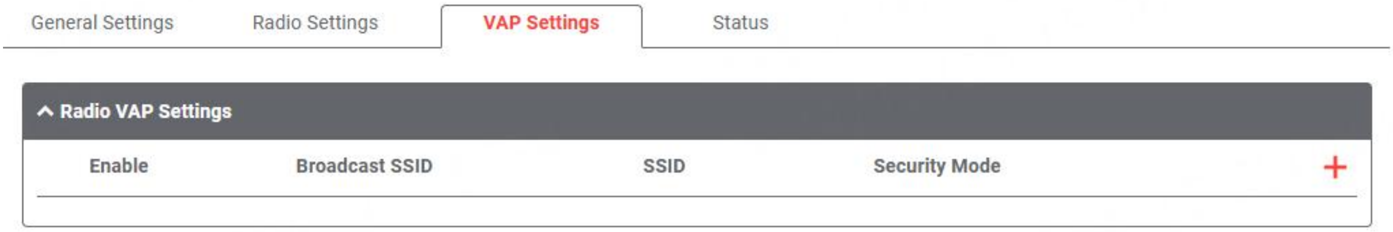
Index 1

Description

MAC Address

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

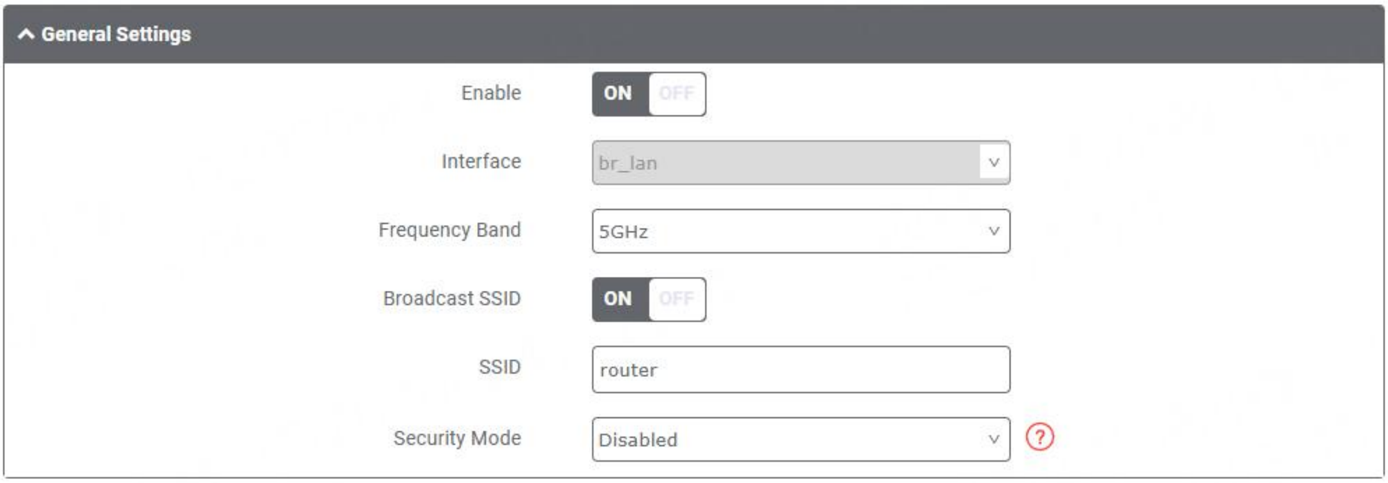
VAP Settings



Click + to add an access point. A maximum of 2 can be configured.

Click ✎ to configure the access point.

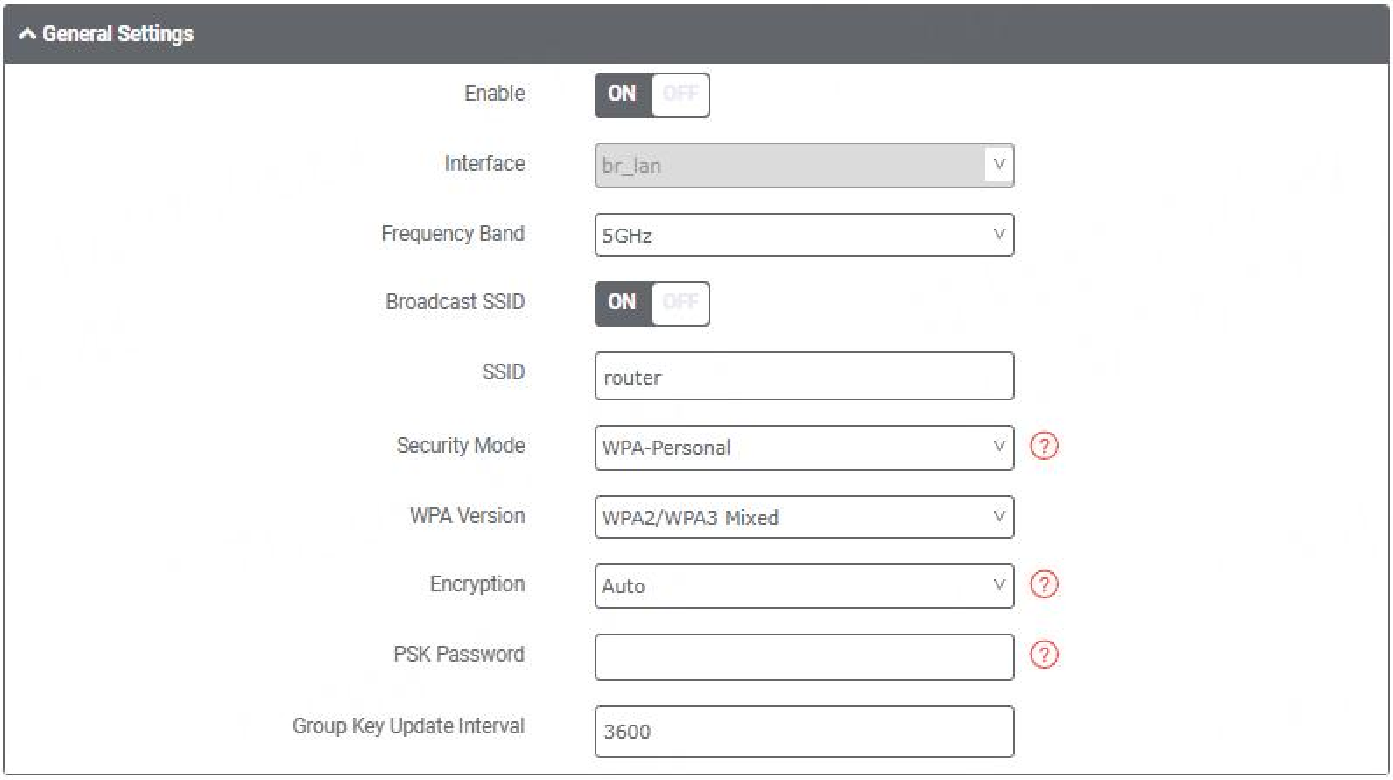
When the security mode is set to 'Disabled,' the window will display as follows.



General Settings

Enable	ON OFF
Interface	br_lan
Frequency Band	5GHz
Broadcast SSID	ON OFF
SSID	router
Security Mode	Disabled

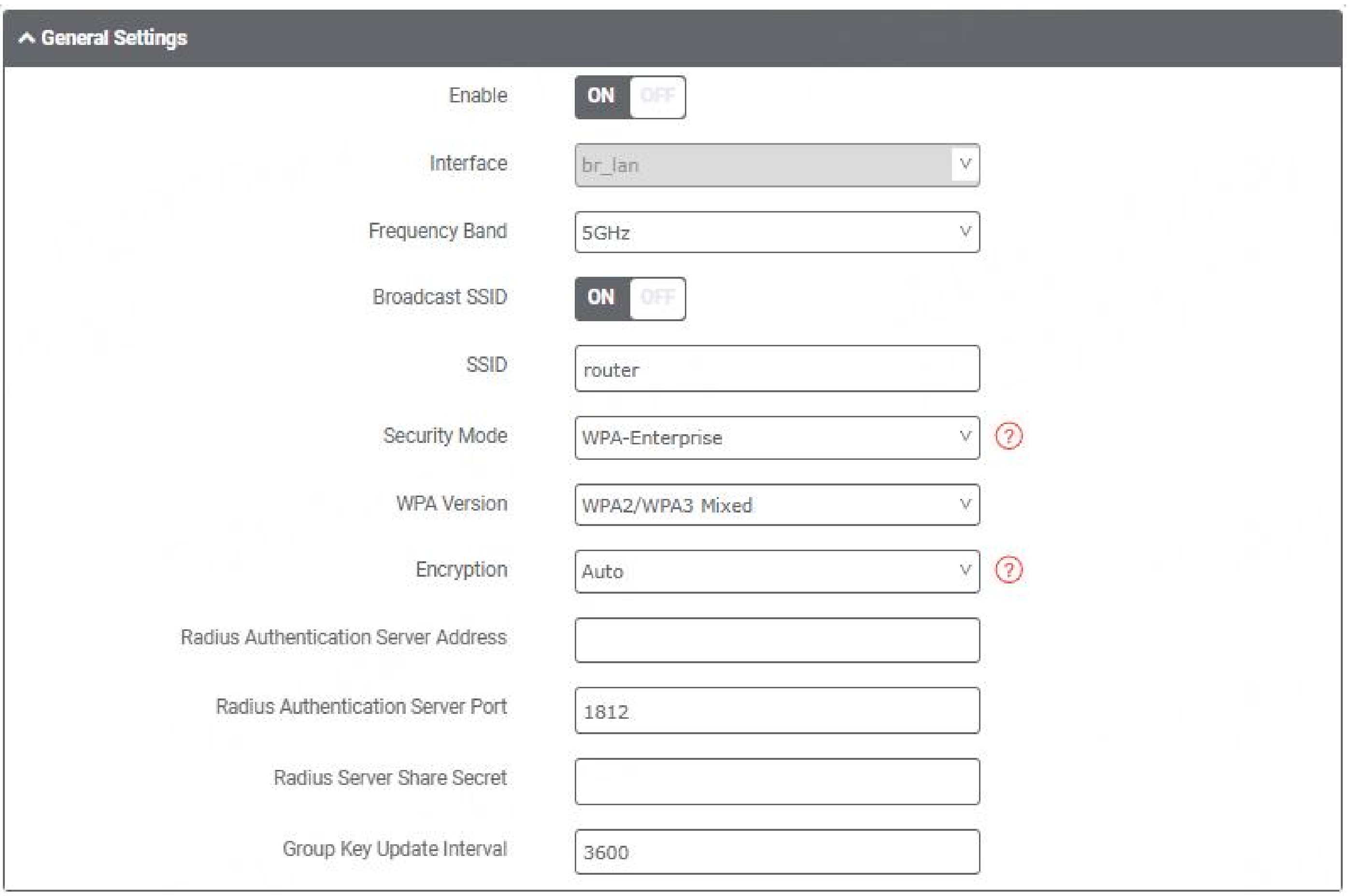
When the security mode is set to 'WPA-Personal,' the window will display as follows.



General Settings

Enable	ON OFF
Interface	br_lan
Frequency Band	5GHz
Broadcast SSID	ON OFF
SSID	router
Security Mode	WPA-Personal
WPA Version	WPA2/WPA3 Mixed
Encryption	Auto
PSK Password	
Group Key Update Interval	3600

When the security mode is set to 'WPA-Enterprise,' the window will display as follows.



Enable: ON

Interface: br_lan

Frequency Band: 5GHz

Broadcast SSID: ON

SSID: router

Security Mode: WPA-Enterprise

WPA Version: WPA2/WPA3 Mixed

Encryption: Auto

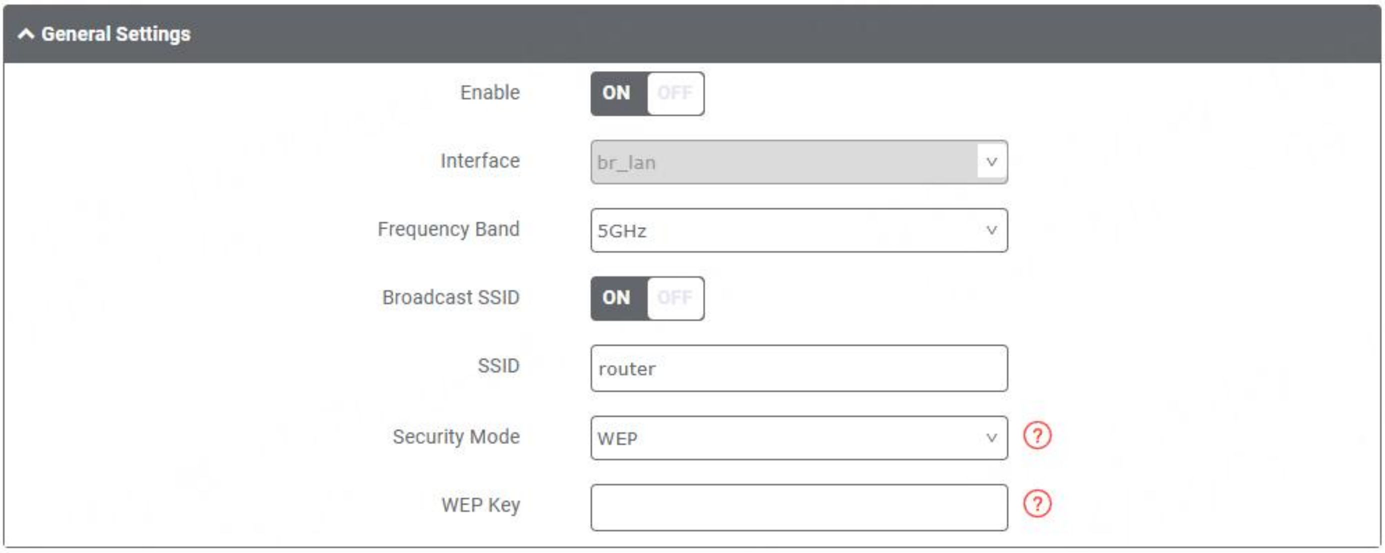
Radius Authentication Server Address:

Radius Authentication Server Port: 1812

Radius Server Share Secret:

Group Key Update Interval: 3600

When the security mode is set to 'WEP,' the window will display as follows.



Enable: ON

Interface: br_lan

Frequency Band: 5GHz

Broadcast SSID: ON

SSID: router

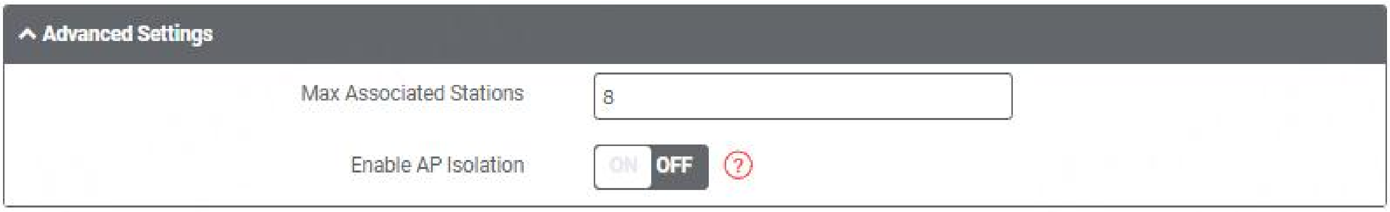
Security Mode: WEP

WEP Key:

Item	Description	Default
Enable	Click the toggle button to enable/disable Wi-Fi AP functionality.	ON
Interface	Select the bound interface.	br_lan
Frequency Band	Select from "5GHz" or "2.4GHz."	5GHz

Item	Description	Default
	Note: This option is only displayed on the EG5200, which supports simultaneous use of Wi-Fi 2.4G and 5G.	
Broadcast SSID	Enter the SSID (Service Set Identifier), which is the network name of the WLAN. The SSID of the client and the AP must match exactly for them to communicate with each other. When the device is in client mode, enter the SSID of the access point to which it is to connect. Please enter 1-32 characters.	ON
SSID	Service Set Identifier.	router
Security Mode	Choose from "Disabled", "WPA-Personal", "WEP", "WPA-Enterprise". • Disabled: Users can access the AP without a password, without authentication or data encryption. Note: For security reasons, avoid setting the security mode to "Open." • WPA-Personal: Wi-Fi Protected Access, which provides a single password for authentication. • WEP: Wired Equivalent Privacy, which provides encrypted data transmission for wireless devices. • WPA-Enterprise: Each user connected to the network must provide a personal username and password, digital certificate, or other credentials for authentication.	Disabled
WPA version	Choose from "WPA2/WPA3 Mixed", "WPA/WPA2 Mixed", "WPA", "WPA2", and "WPA3". • WPA2/WPA3 Mixed: The device will automatically choose the most appropriate WPA mode, either WPA2 or WPA3. • WPA/WPA2 Mixed: The device will automatically choose the most appropriate WPA mode, either WPA or WPA2. • WPA: An earlier Wi-Fi security standard that uses TKIP (Temporal Key Integrity Protocol) encryption to protect data transmission, providing a certain level of data protection. • WPA2: WPA2 is an upgraded version of WPA, using a more powerful AES (Advanced Encryption Standard) encryption protocol to provide enhanced data protection. • WPA3: WPA3 is a further improvement over WPA2, offering stronger protection against password cracking, increasing security for public wireless networks, and improving password selection methods.	WPA/WPA2 Mixed
Encryption	Choose from "TKIP" and "AES." • TKIP: Temporal Key Integrity Protocol (TKIP) encryption is used over wireless connections. TKIP encryption can be used with WPA-PSK and WPA 802.1x authentication. • AES: AES encryption is used over wireless networks. It can be used with CCMP for WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm compared to TKIP. **Note:** The encryption mode can affect wireless rates, and different wireless modes support different encryption modes. For example, 802.11n does not support WEP security mode or TKIP algorithm; if enforced, the	TKIP

Item	Description	Default
	wireless rate will drop to 54Mbps, effectively switching to 802.11g mode. It is recommended to use the AES encryption algorithm in 802.11n mode.	
PSK Password	Enter the pre-shared key. Please enter 8-63 characters.	null
Radius Authentication Server Address	Enter the Radius authentication server address.	0.0.0.0
Radius Authentication Server Port	Enter the Radius authentication server port.	1812
Radius Server Shared Password	Enter the Radius server shared password, limited to 8-128 characters.	null
Group Key Update Interval	Enter the group key update interval.	3600
WEP Key	Enter the WEP key. The key length should be either 10 or 26 hexadecimal characters, depending on whether 64-bit or 128-bit WEP is used.	null


^ Advanced Settings

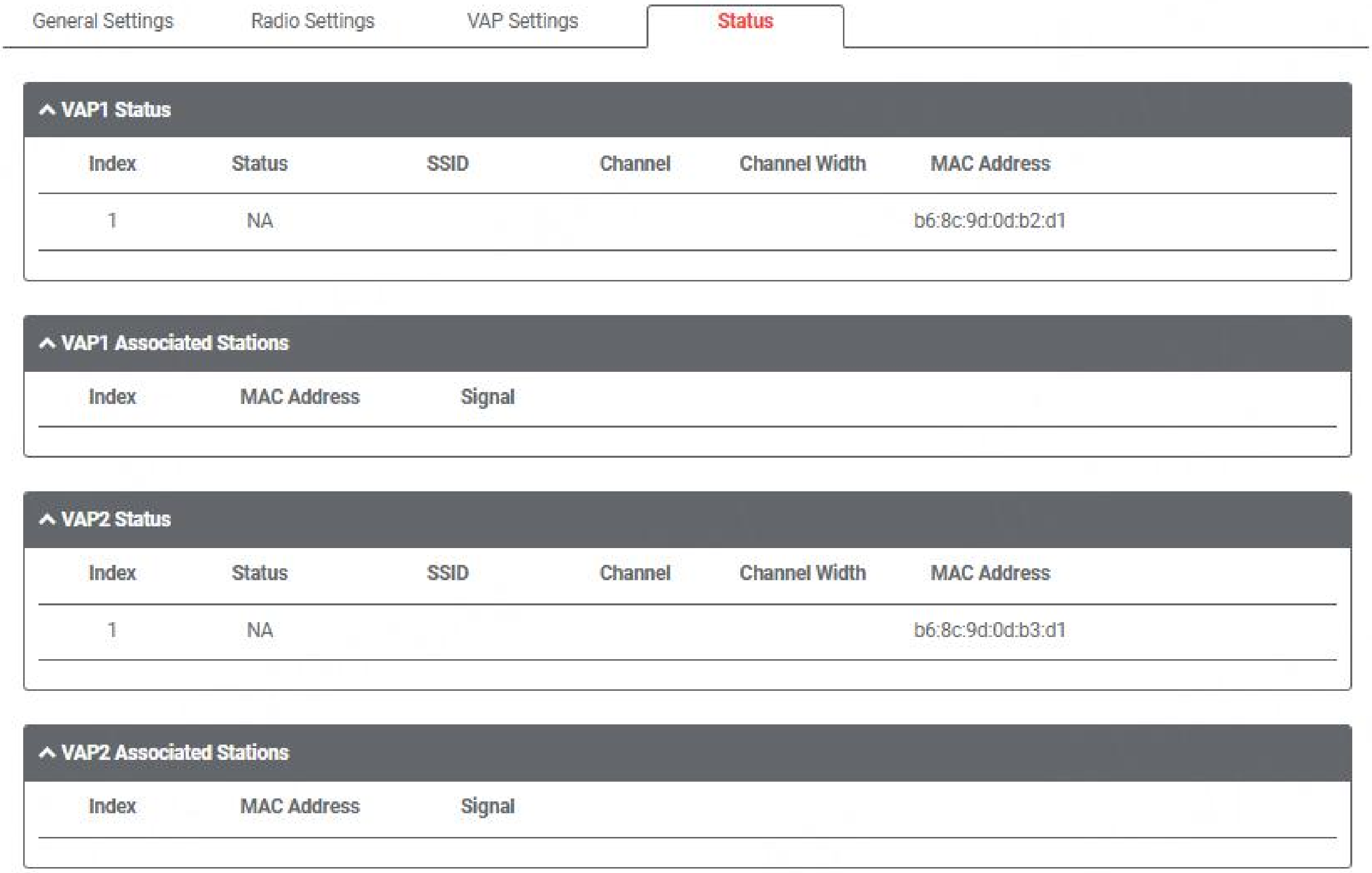
Max Associated Stations: 8

Enable AP Isolation: ON OFF

Item	Description	Default
Maximum number of access points	Set the maximum number of clients allowed to access the gateway AP.	8 （EG5200:64）
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, it isolates all connected wireless devices, preventing individual wireless devices from accessing each other.	OFF

Status

This section allows you to view the status of AP.



^ VAP1 Status

Index	Status	SSID	Channel	Channel Width	MAC Address
1	NA				b6:8c:9d:0d:b2:d1

^ VAP1 Associated Stations

Index	MAC Address	Signal

^ VAP2 Status

Index	Status	SSID	Channel	Channel Width	MAC Address
1	NA				b6:8c:9d:0d:b3:d1

^ VAP2 Associated Stations

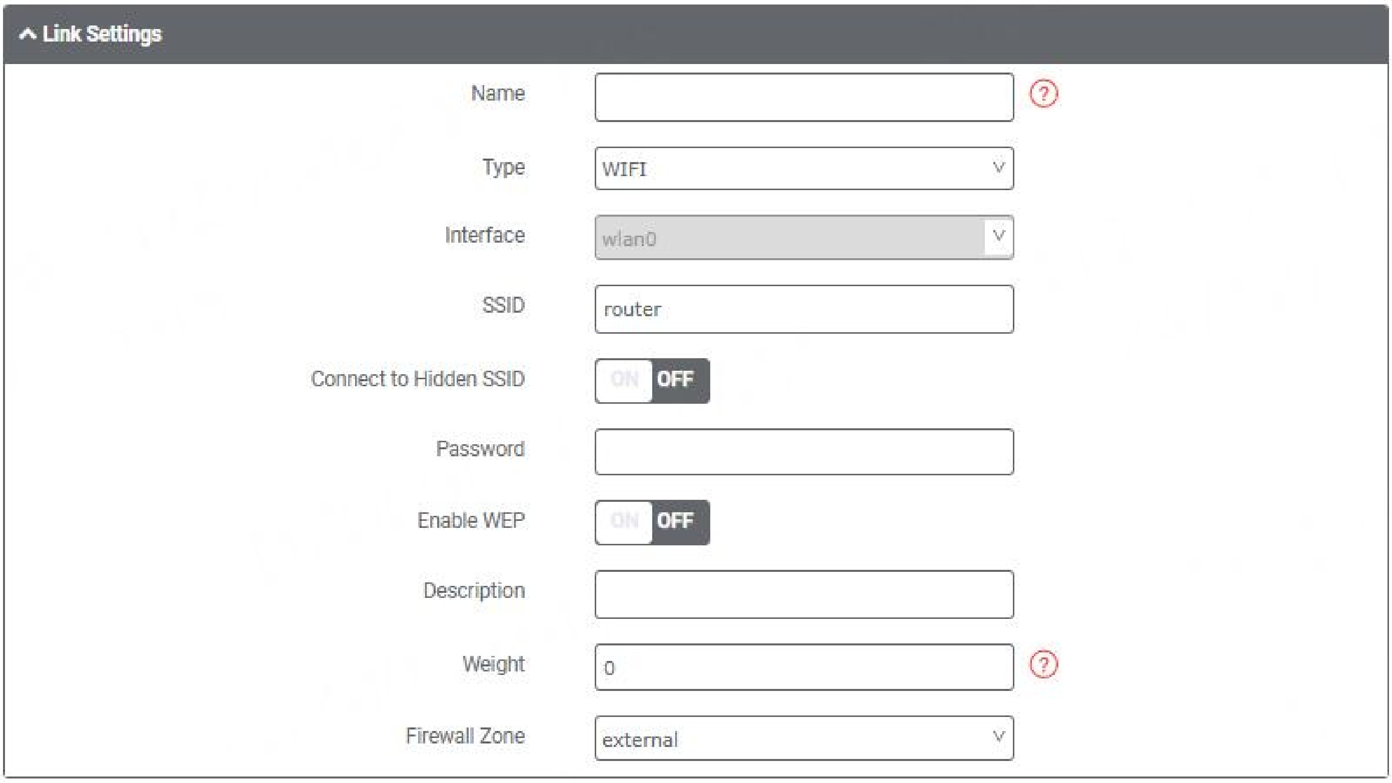
Index	MAC Address	Signal

Wi-Fi Client

User can configure the device as a Wi-Fi client by following steps.

Note: Before setting up Wi-Fi Client for EG5100, EV8100, and EG5120, you need to switch the Wi-Fi mode to Client.

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

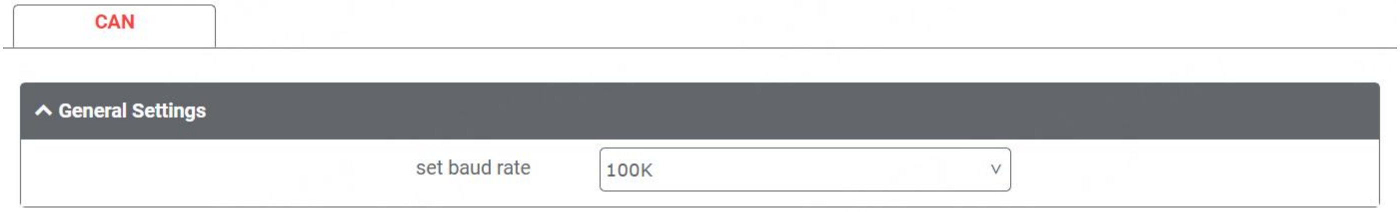


Name	
Type	WIFI
Interface	wlan0
SSID	router
Connect to Hidden SSID	ON OFF
Password	
Enable WEP	ON OFF
Description	
Weight	0
Firewall Zone	external

3.2.5 CAN

This section allows you to configure the parameters of CAN.

- The EG5100 supports a CAN interface (optional).
- The EV8100 supports a CAN interface.

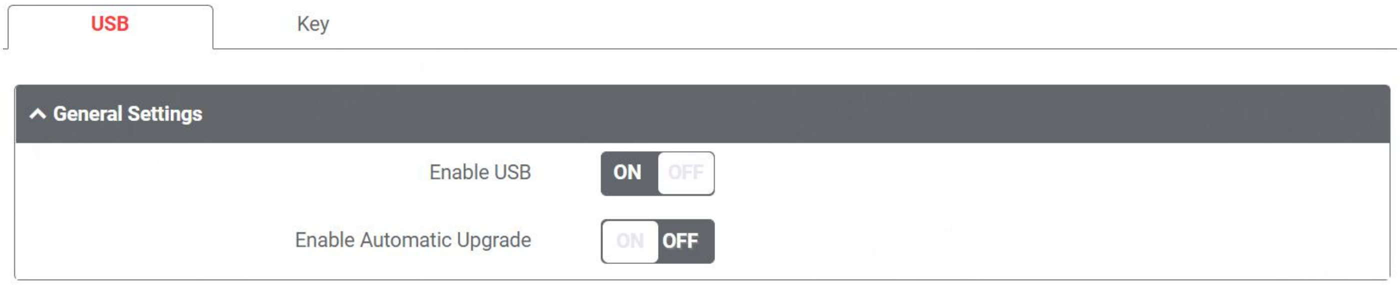


set baud rate	100K

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 for firmware upgrades and configuration updates.



USB　Key

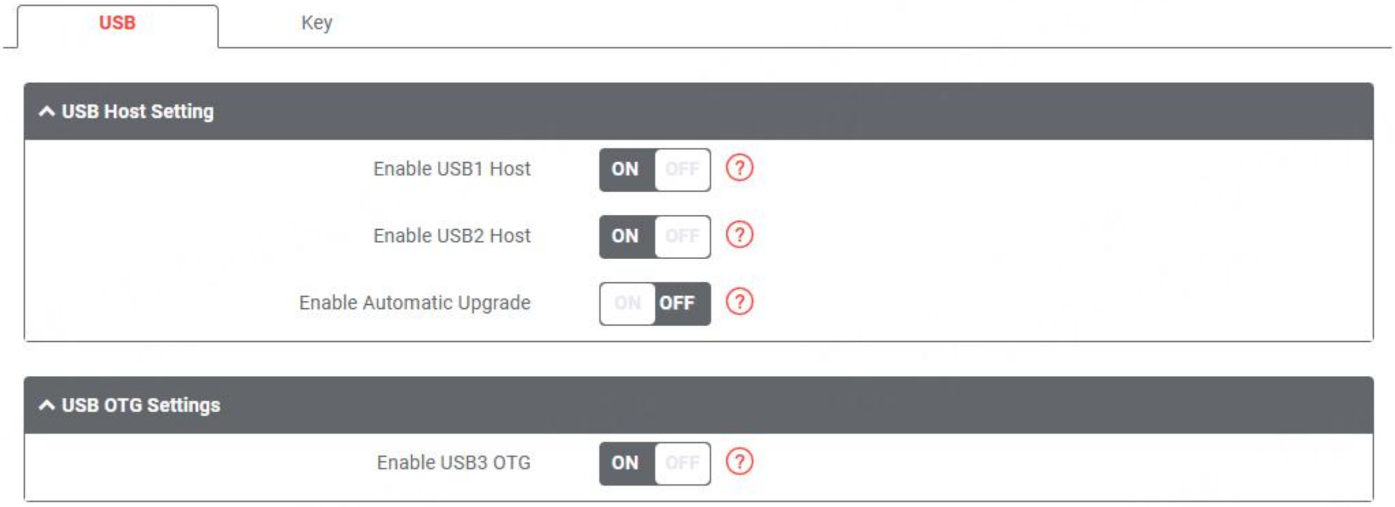
General Settings

Enable USB: ON

Enable Automatic Upgrade: OFF

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 or disable this feature. When enabled, the router will automatically update its firmware upon inserting a USB storage device containing the router firmware.	OFF

- EG5200



USB　Key

USB Host Setting

Enable USB1 Host: ON

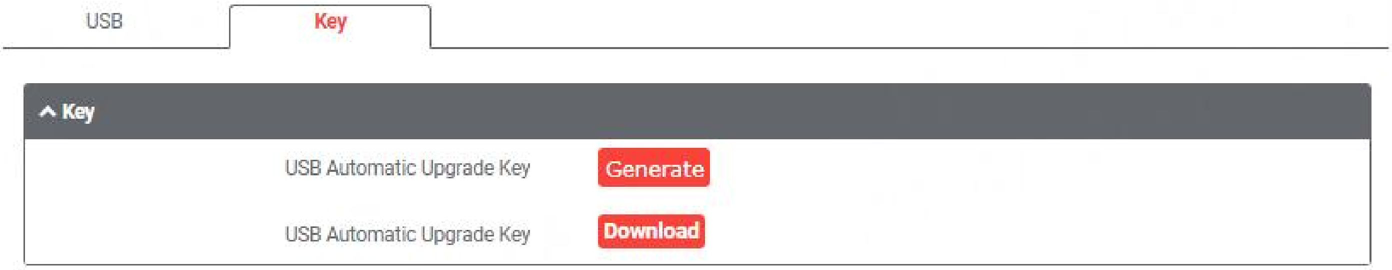
Enable USB2 Host: ON

Enable Automatic Upgrade: OFF

USB OTG Settings

Enable USB3 OTG: ON

Item	Description	Default
Enable USB1 Host	Click the toggle button to enable or disable the USB1 Host option.	ON
Enable USB2 Host	Click the toggle button to enable or disable the USB2 Host option.	ON
Enable Automatic Upgrade	Click the toggle button to enable or disable this option. When enabled, this option allows the gateway's firmware to be automatically updated when a USB storage device containing the gateway firmware is inserted.	OFF
Enable USB3 OTG	Click the toggle button to enable or disable the USB 3 OTG option, which allows USB OTG to access the microSD.	ON



USB　Key

Key

USB Automatic Upgrade Key: Generate

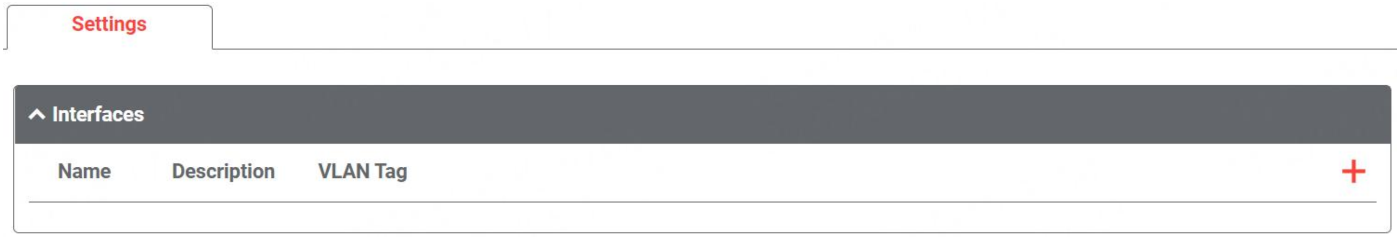
USB Automatic Upgrade Key: Download

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

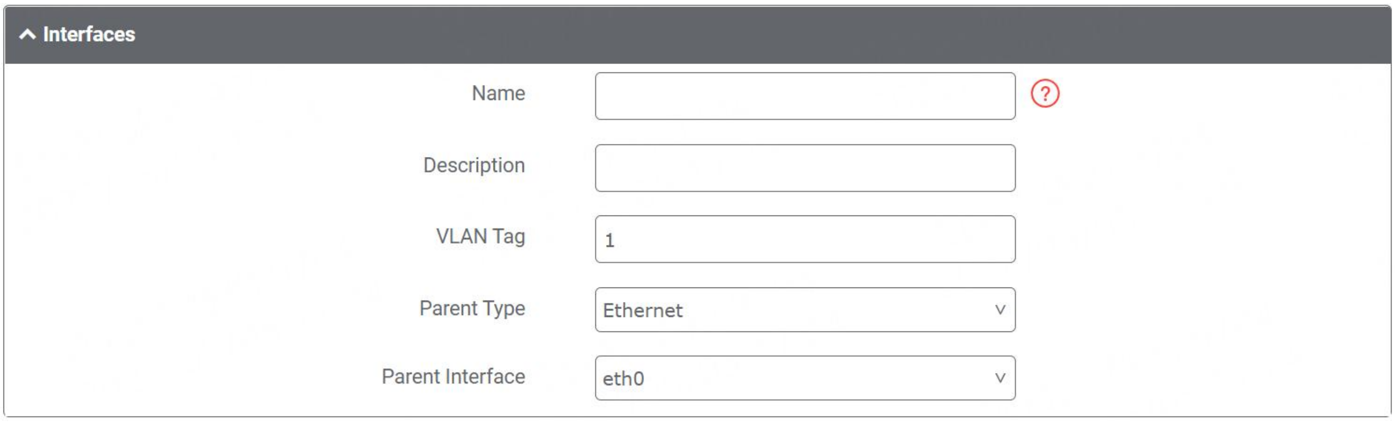
Note: When using the USB automatic upgrade feature, the LEDs will start blinking one by one to indicate that the upgrade is in progress. When the LEDs stop blinking and the user indicator light turns on, it means the upgrade is complete. After the upgrade, the device will not automatically restart. If the LEDs do not start blinking one by one, it indicates an error, and the automatic upgrade process will not proceed.

3.2.7 VLAN

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



Click + to add a new VLAN. A maximum of **10** VLANs can be configured.



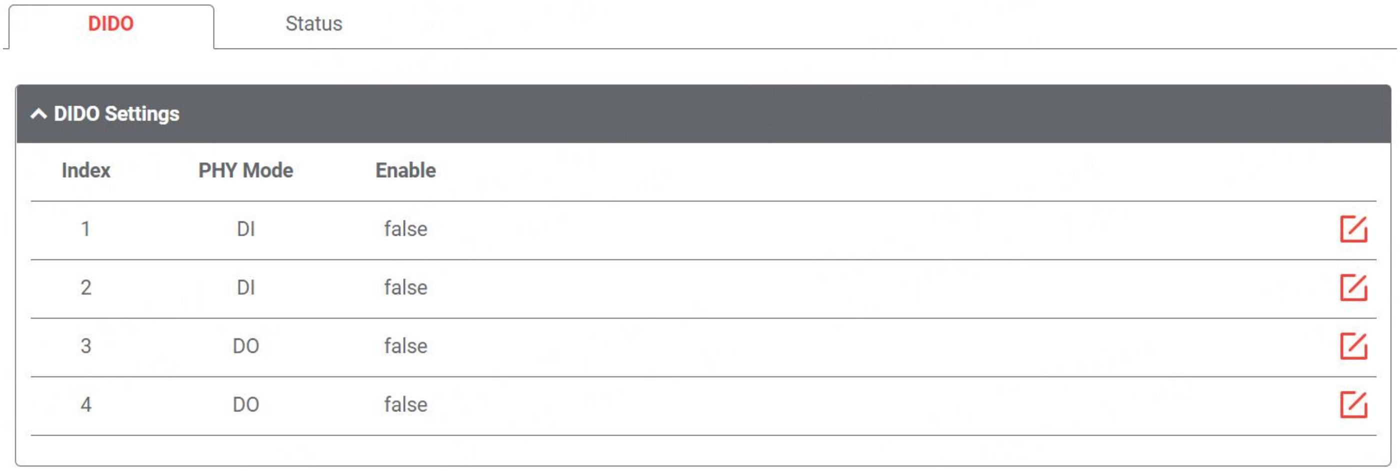
Name	
Description	
VLAN Tag	1
Parent Type	Ethernet
Parent Interface	eth0

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

3.2.8 DI/DO

This section can be used to configure the DI/DO parameters. The DI interface can be used to trigger alarms, while the DO interface can be used to control external devices for real-time monitoring. In some devices, users can configure the IO as either DI or DO.

DI/DO

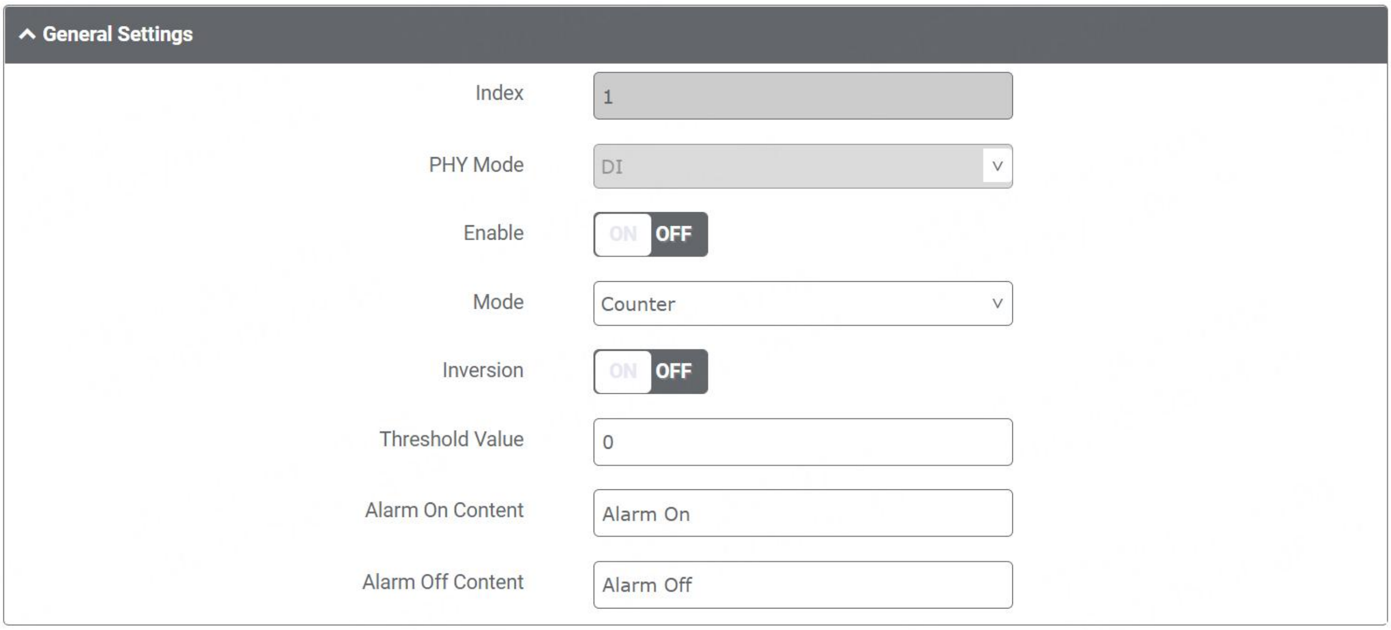


DIDO Settings

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

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

DI



General Settings

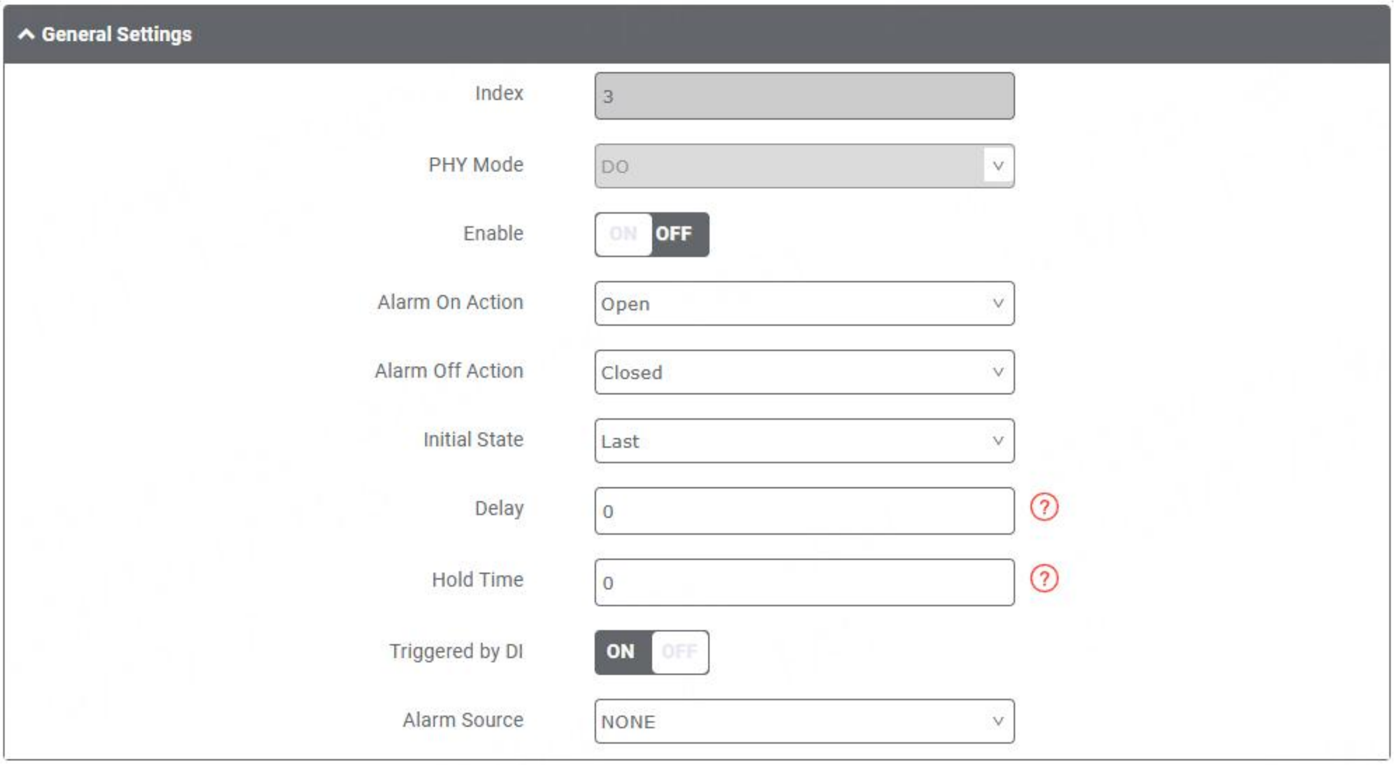
Index	1
PHY Mode	DI
Enable	ON [✓ OFF]
Mode	Counter
Inversion	ON [✓ OFF]
Threshold Value	0
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off

Item	Description	Default
Index	Indicate the ordinal position in the list.	--

Item	Description	Default
PHY Mode	DI, fixed, read only.	--
Enable	Click the toggle button to enable/disable the digital input function.	OFF
Mode	Select either “ON-OFF” or “Counter”. • ON-OFF: Alarm mode can be triggered when the DI input transitions from ON to OFF. • Counter: Event counter mode.	ON-OFF
Inversion	The count can be based on either a rising edge count or a falling edge count. If the current count is based on rising edges, the inverse count will be based on falling edges.	OFF
Threshold Value	The threshold value is a unique parameter when the mode is set to **Count**. Set the threshold value to trigger the DI alarm when the count value reaches this threshold.	0
Alarm On Content	Display the content when the alarm is triggered.	Alarm On
Alarm Off Content	Display the content when the alarm is deactivated.	Alarm Off

Note: The default alarm is triggered by a high level; when "Inversion" is enabled, it changes to a low-level alarm.

DO



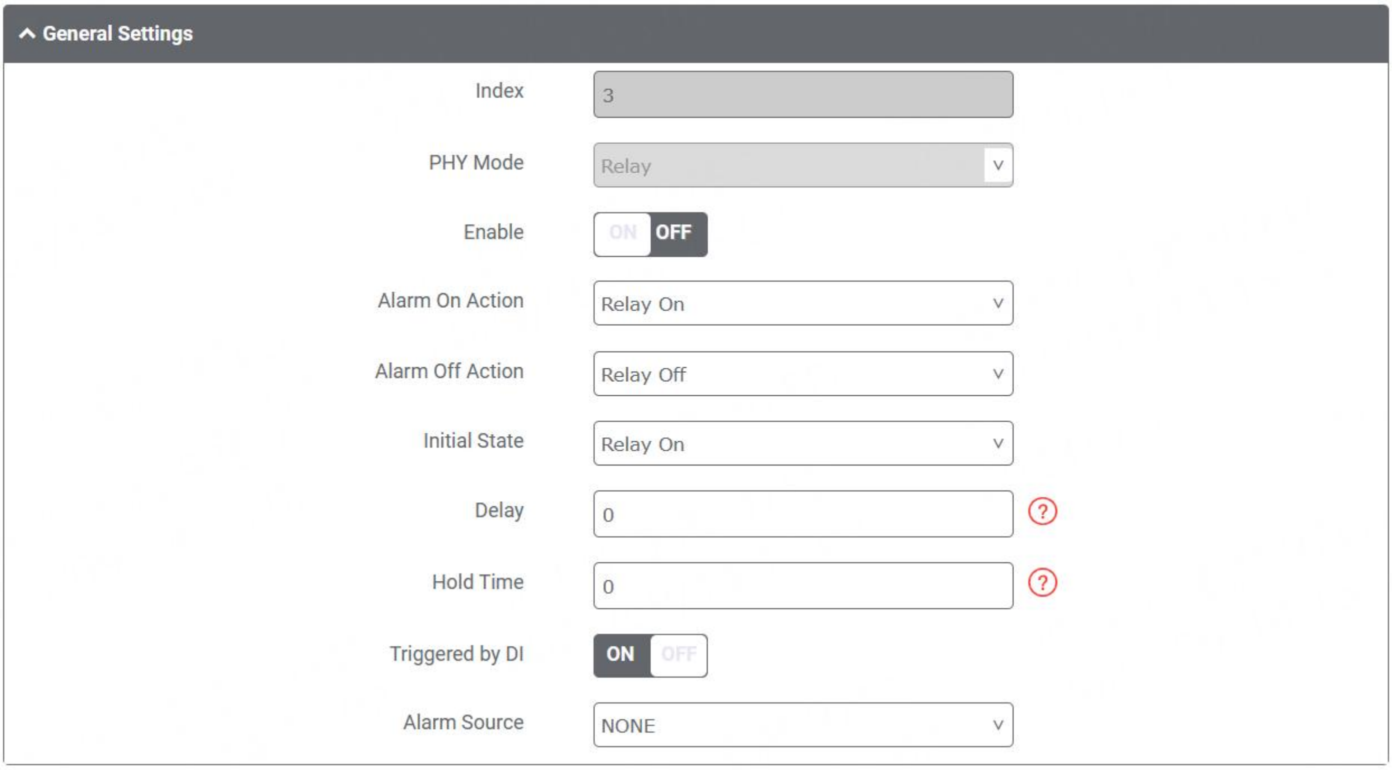
Index: 3
PHY Mode: DO
Enable: ON OFF
Alarm On Action: Open
Alarm Off Action: Closed
Initial State: Last
Delay: 0
Hold Time: 0
Triggered by DI: ON OFF
Alarm Source: NONE

Item	Description	Default
Index	Indicate the ordinal position in the list.	--
PHY Mode	DO, fixed, read only.	--
Enable	Click the toggle button to enable/disable this digital output (DO).	OFF
Alarm On Action	The digital output is activated when an alarm occurs. Select from “Open”, “Closed”, or “Pulse”.	Open

Item	Description	Default
	- Open: Outputs a high electrical level. - Closed: Outputs a low electrical level. - Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.	
Alarm Off Action	The digital output is activated when the alarm is removed. Select from “Open”, “Closed”, or “Pulse”. - Open: Outputs a high electrical level. - Closed: Outputs a low electrical level. - Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.	Closed
Initial State	Specify the digital output status when powered on. Selected from “Last”, “High” or “Low”. - Last: The DO status will match the status at the last power off. - High: The DO interface will be at a high electrical level. - Low: The DO interface will be at a low electrical level.	Last
Delay (unit: 100ms)	Set the delay time for the DO alarm startup. The first pulse will be generated after the specified delay. Enter a value from 0 to 3000 (0 = generate pulse without delay).	0
Hold Time (unit: s)	Set the hold time for the DO status (Alarm On Action/Alarm Off Action). When the action time reaches this specified duration, the DO will stop the action. Enter a value from 0 to 3000 seconds (0 = keep on until the next action).	0
Low-level Width (unit: ms)	Set the low-level width. This option is available when “Pulse” is selected for 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, with low-level widths set here. Enter a value from 1000 to 3000.	1000
High-level Width (unit: ms)	Set the high-level width. This option is available when “Pulse” is selected for 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, with high-level widths set here. Enter a value from 1000 to 3000.	1000
Triggered by DI	The state of the DO is triggered by the DI.	OFF
Alarm Source	The activation of the digital output can be triggered by this alarm.	None

Relay Output

- EV8100 and EG5200 support a relay output interface.



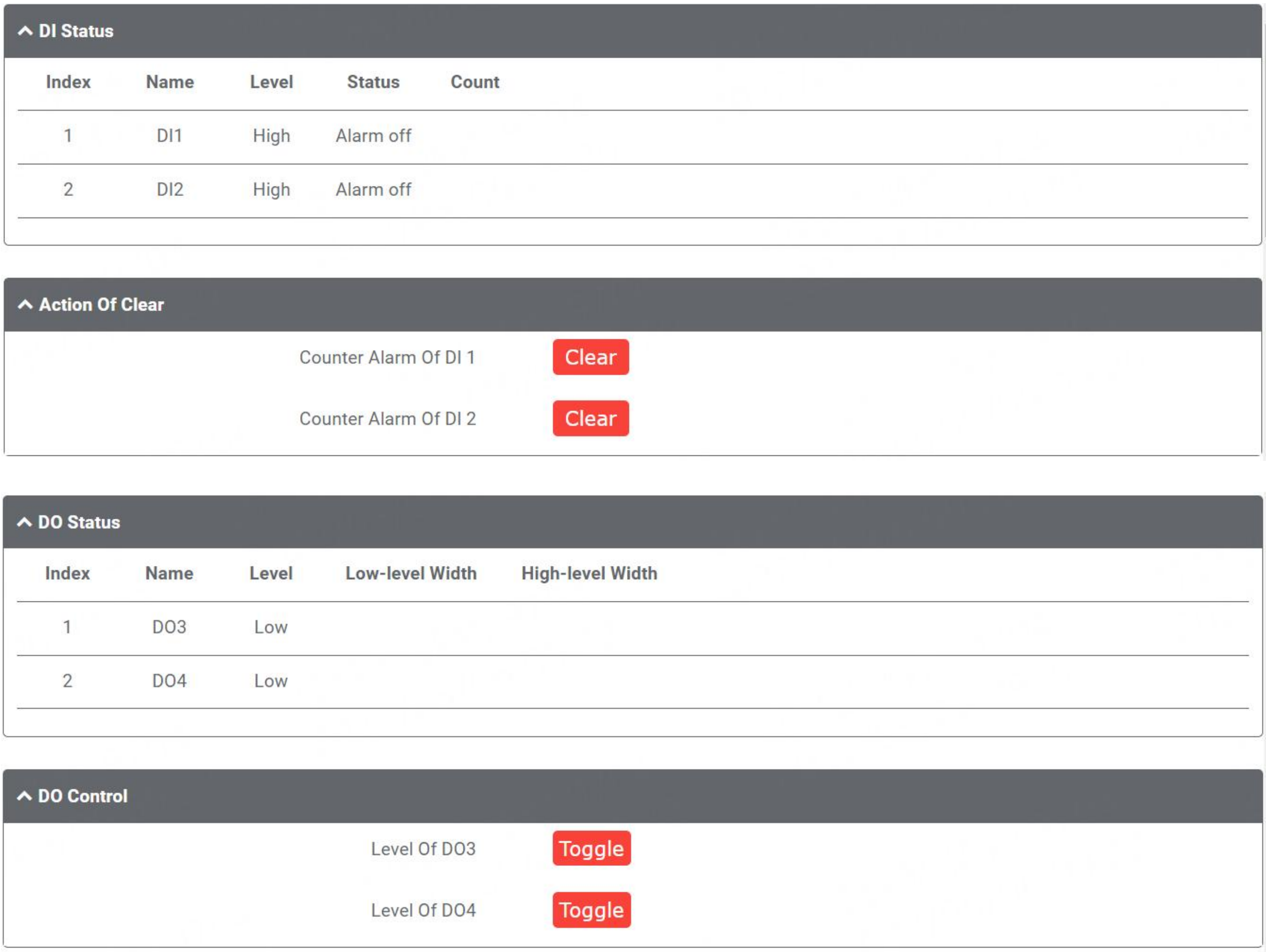
General Settings

Index	3
PHY Mode	Relay
Enable	ON OFF
Alarm On Action	Relay On
Alarm Off Action	Relay Off
Initial State	Relay On
Delay	0
Hold Time	0
Triggered by DI	ON OFF
Alarm Source	NONE

Item	Description	Default
Index	Indicates the ordinal position in the list.	--
PHY Mode	Relay only available on Relay Output device.	Relay
Enable	Click the toggle button to enable/disable this Relay Output.	OFF
Alarm On Action	The Relay Output is activated when an alarm occurs. • Relay On: The relay will connect. • Relay Off: The relay will disconnect.	Relay On
Alarm Off Action	The Relay Output is activated when the alarm is 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 the relay alarm startup. The first action will occur after the specified delay. Enter a value from 0 to 3000 (0 = no delay).	0
Hold Time (unit: s)	Set the hold time for the relay status during Alarm On Action/Alarm Off Action. Once the specified time is reached, the relay will stop the action. Enter a value from 0 to 3000 seconds (0 = hold 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	The activation of the relay output can be triggered by this alarm.	None

Status

This window allows you to view the status of the Digital Input (DI) and Digital Output (DO) interface. You can also clear the counter alarm of DI from this window. Click the Clear button to clear the monthly usage statistics for the counter alarm for DI 1 or DI 2. Click the Toggle button to switch the electrical level output.



DI Status

Index	Name	Level	Status	Count
1	DI1	High	Alarm off	
2	DI2	High	Alarm off	

Action Of Clear

Counter Alarm Of DI 1 Clear

Counter Alarm Of DI 2 Clear

DO Status

Index	Name	Level	Low-level Width	High-level Width
1	DO3	Low		
2	DO4	Low		

DO Control

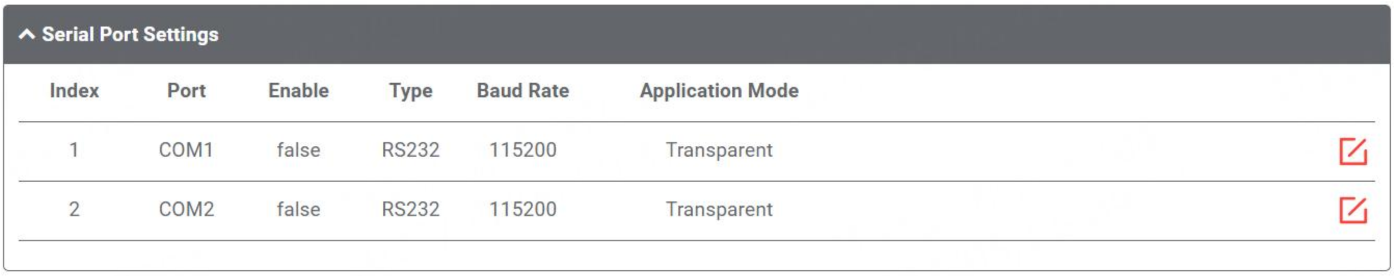
Level Of DO3 Toggle

Level Of DO4 Toggle

3.2.9 Serial Port

This section allows you to set the serial port parameters. The device may support two serial ports, which can be configured as RS232, RS485, or RS422 as needed. Serial data can be converted to IP data, or IP data can be converted to serial data, enabling transparent data transmission over wired or wireless networks.

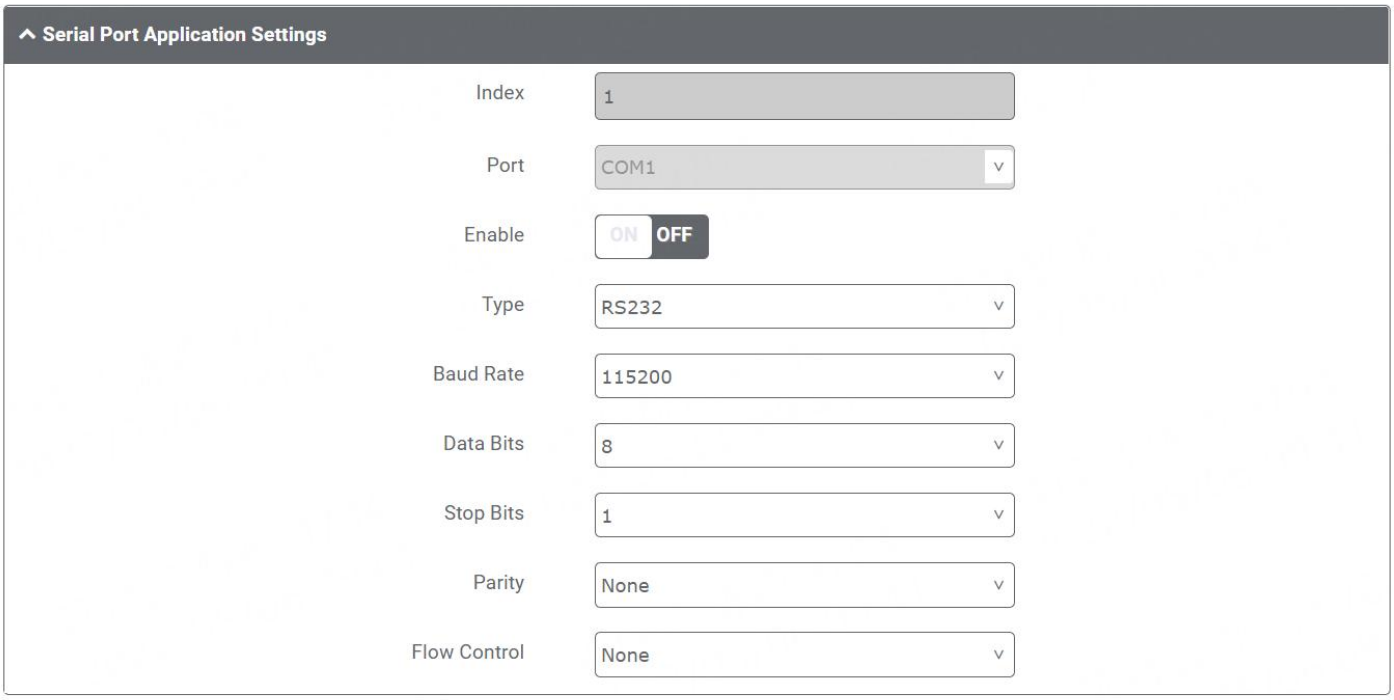
Serial Port



Serial Port Settings

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

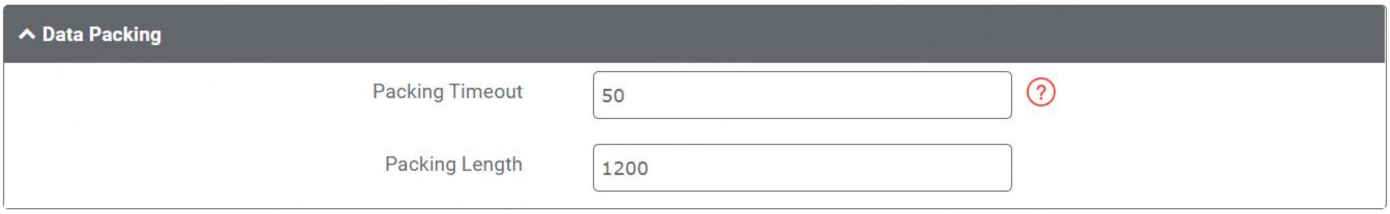
Click ✎ to configure the parameters in the pop-up window.



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 position in the list.	--
Port	Show the current serial's name (read only).	COM1
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Type	Select from "RS232", "RS485" or "RS422". NOTE: The options displayed depend on the device model.	RS232
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" or "115200".	115200
Data Bits	Select either "7" or "8".	8
Stop Bits	Select either "1" or "2".	1
Parity	Select from "None", "Odd" or "Even".	None
Flow Control	Select from "None", "Software" or "Hardware".	None



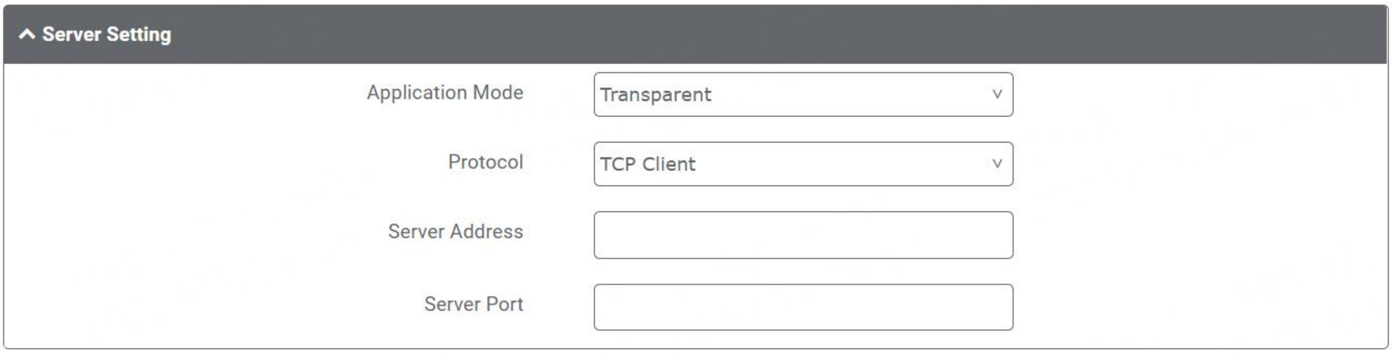
^ Data Packing

Packing Timeout: 50

Packing Length: 1200

Item	Description	Default
Packing Timeout	Set the packet timeout. This parameter determines the timeout duration for packaging data. The serial port arranges data in a buffer, and when the specified timeout interval is reached, it sends the data to the mobile wide area network (WAN) or Ethernet WAN. The unit of measurement is milliseconds. **Note:** Data will be sent even if the timeout interval has not been reached, as long as it matches the specified packet length or the configured delimiter.	50
Packing Length	Set the packet data length. The packet length setting defines the maximum amount of data that can accumulate in the serial port buffer before it is sent. When a packet length between 1 and 3000 bytes is specified, the data in the buffer will be sent immediately once the specified length is reached.	1200

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



^ Server Setting

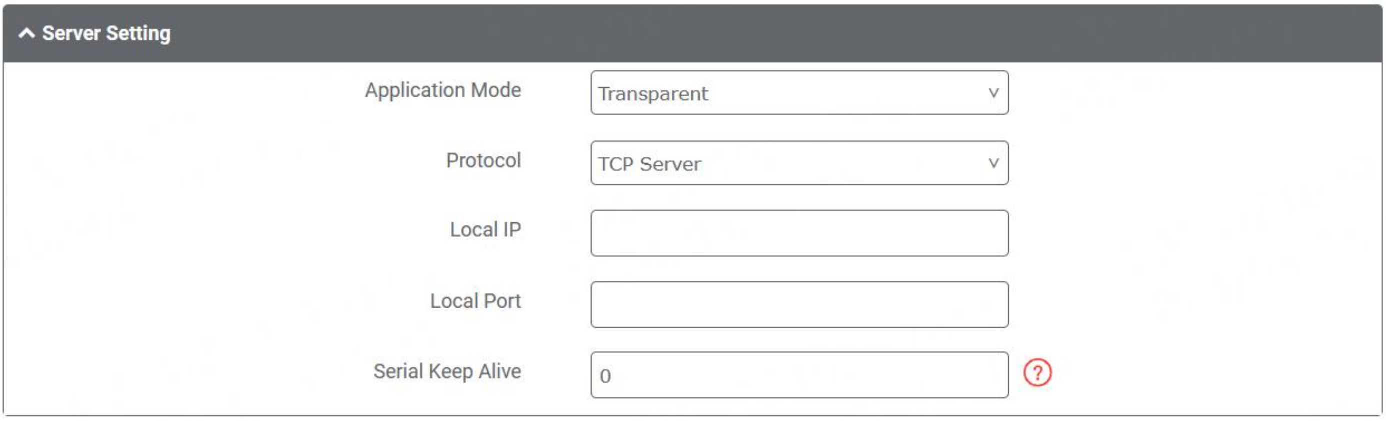
Application Mode: Transparent

Protocol: TCP Client

Server Address:

Server Port:

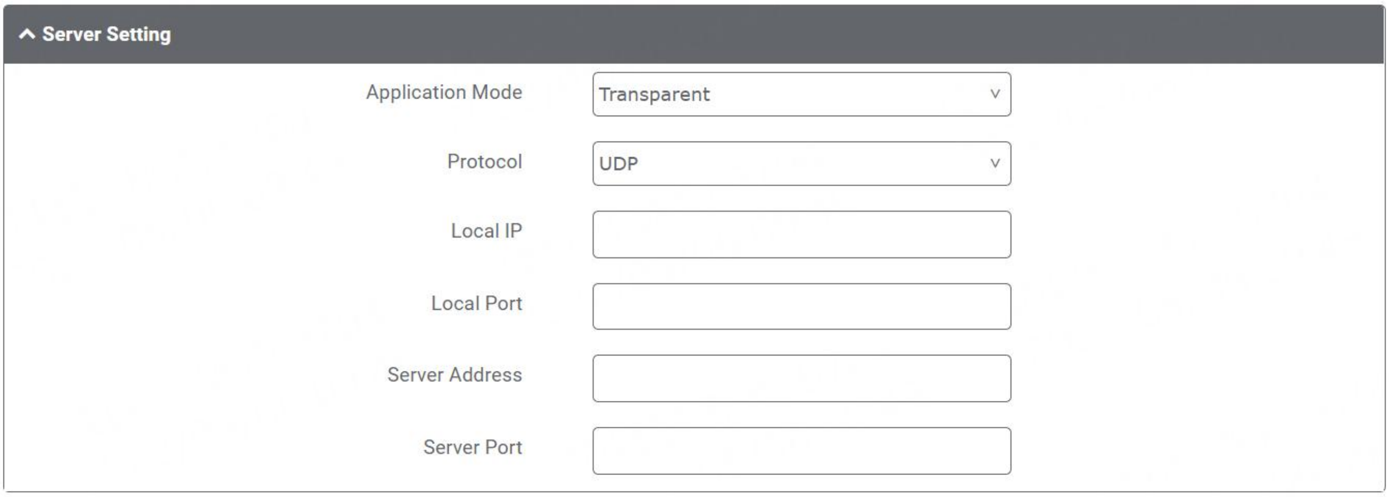
When "Transparent” is selected as the application mode and "TCP Server" as the protocol, the window displays as follows:



^ Server Setting

Application Mode	Transparent
Protocol	TCP Server
Local IP	
Local Port	
Serial Keep Alive	0

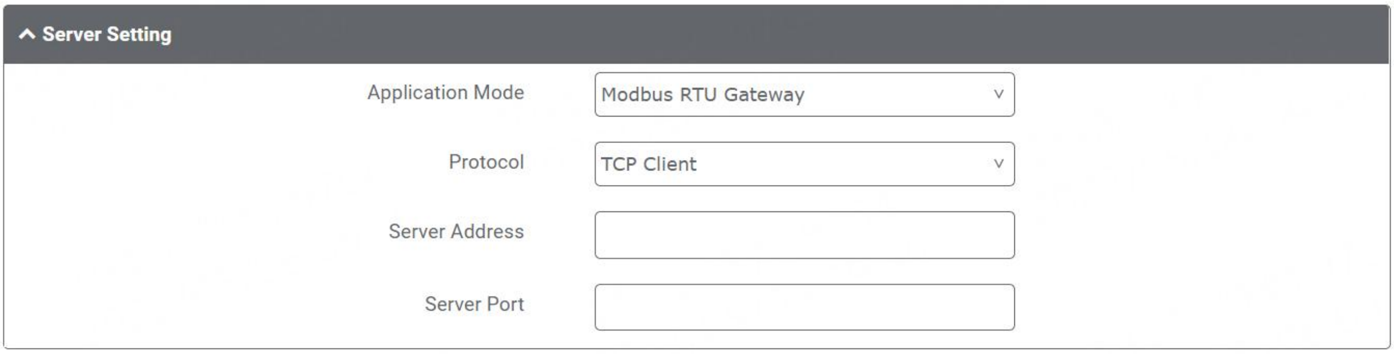
When "Transparent” is selected as the application mode and "UDP" is used as the protocol, the window displays as follows:



^ Server Setting

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

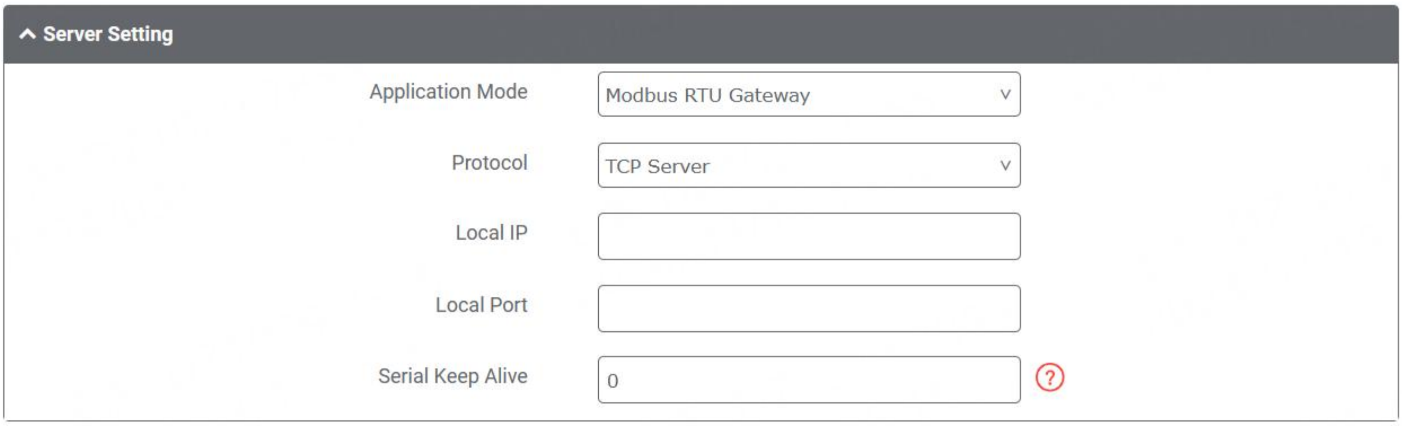
When “Modbus RTU Gateway” is selected as the application mode and “TCP Client” as the protocol, the window displays as follows:



^ Server Setting

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

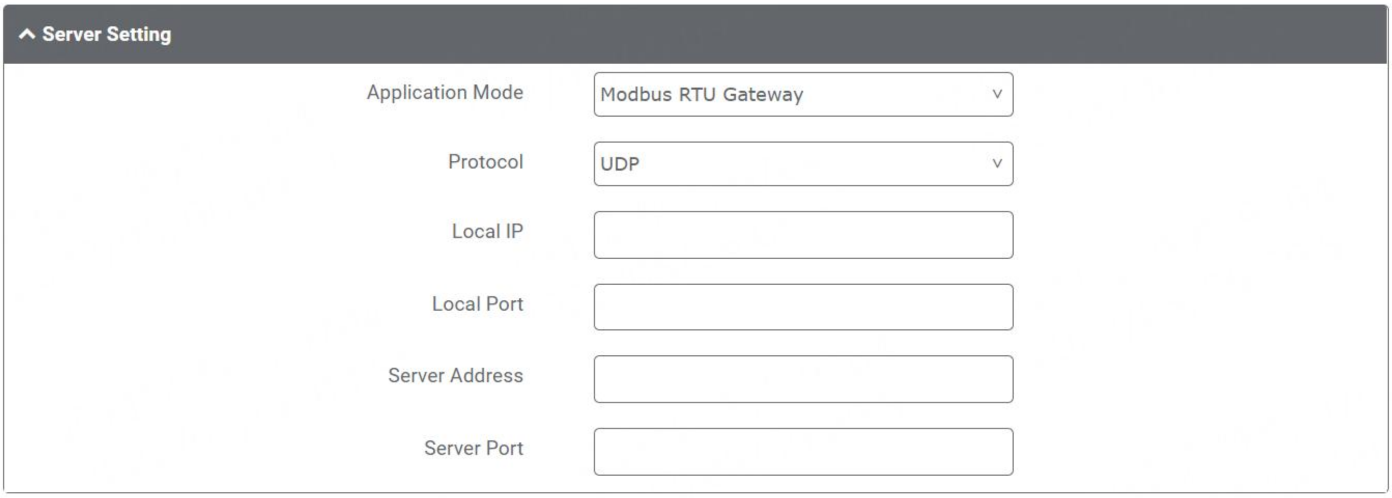
When "Modbus RTU Gateway" is selected as the application mode and "TCP Server" as the protocol, the window displays as follows:



^ Server Setting

Application Mode	Modbus RTU Gateway
Protocol	TCP Server
Local IP	
Local Port	
Serial Keep Alive	0

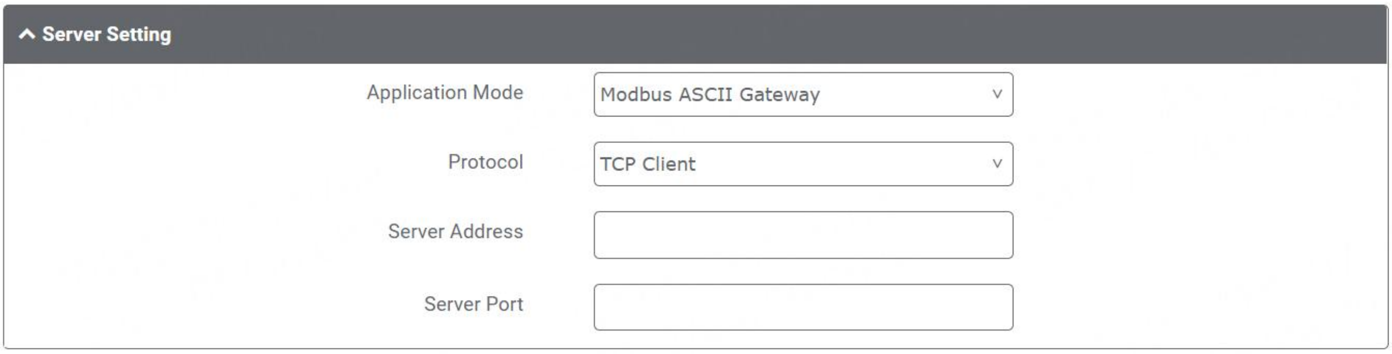
When selecting "Modbus RTU Gateway" as the application mode and "UDP" as the protocol, the window displays as follows:



^ Server Setting

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

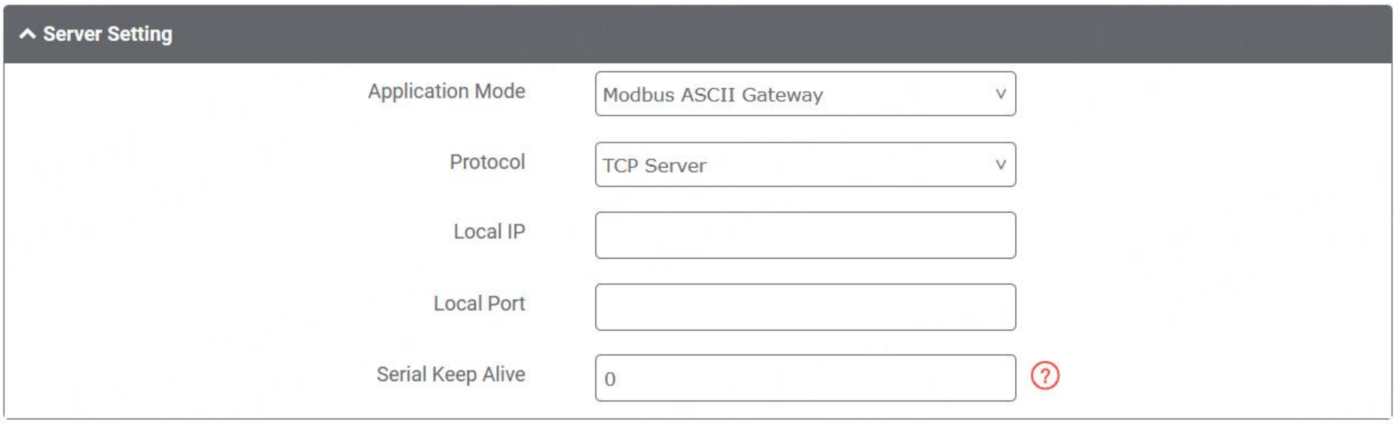
When “Modbus ASCII Gateway” is selected as the application mode and “TCP Client” as the protocol, the window displays as follows:



^ Server Setting

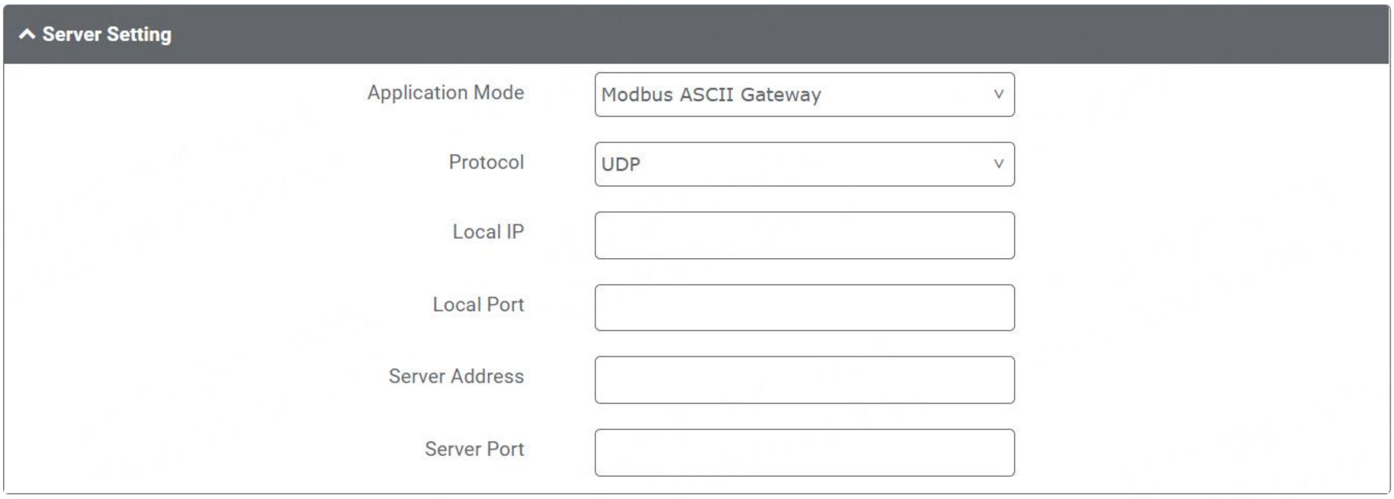
Application Mode	Modbus ASCII Gateway
Protocol	TCP Client
Server Address	
Server Port	

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



Application Mode	Modbus ASCII Gateway
Protocol	TCP Server
Local IP	
Local Port	
Serial Keep Alive	0

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



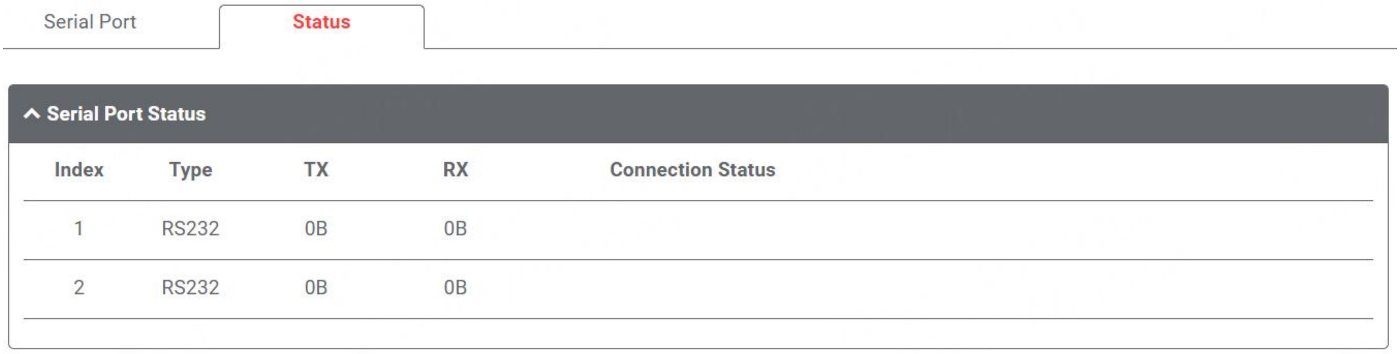
Application Mode	Modbus ASCII Gateway
Protocol	UDP
Local IP	
Local Port	
Server Address	
Server Port	

Item	Description	Default
Application Mode	Select from “Transparent”, “Modbus RTU Gateway” or “Modbus ASCII Gateway”. • Transparent: The device will transmit serial data transparently. • Modbus RTU Gateway: The device will translate Modbus RTU data to Modbus TCP data for transmission, and vice versa. • Modbus ASCII Gateway: The device will translate Modbus ASCII data to Modbus TCP data for transmission, and vice versa.	Transparent
Protocol	Select from “TCP Client”, “TCP Server”, or “UDP”. • TCP Client: The device operates as a TCP client, initiating a TCP connection to a TCP server. The server address can be specified using either an IP address or a domain name. • TCP Server: The device operates as a TCP server, listening for connection requests from TCP clients. • UDP: The device functions as a UDP client.	TCP Client
Server Address	Enter the address of the server that will receive data from the device’s	Null

Item	Description	Default
	serial port. Both IP addresses and domain names are accepted.	
Server Port	Enter the specified port of server used for receiving serial data.	Null
Local IP @ Transparent	Enter the device’s LAN IP address that will be used to forward data to the internet port of the device.	Null
Local Port @ Transparent	Enter the port number associated with the device’s LAN IP.	Null
Local IP @ Modbus	Enter the local IP address for Modbus mode.	Null
Local Port @ Modbus	Enter the local port number for Modbus mode.	Null
Serial Keep Alive	Specify the keepalive period for the serial port. If no data is received on the serial port during this keepalive period, all client connections will be disconnected.	0

Status

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



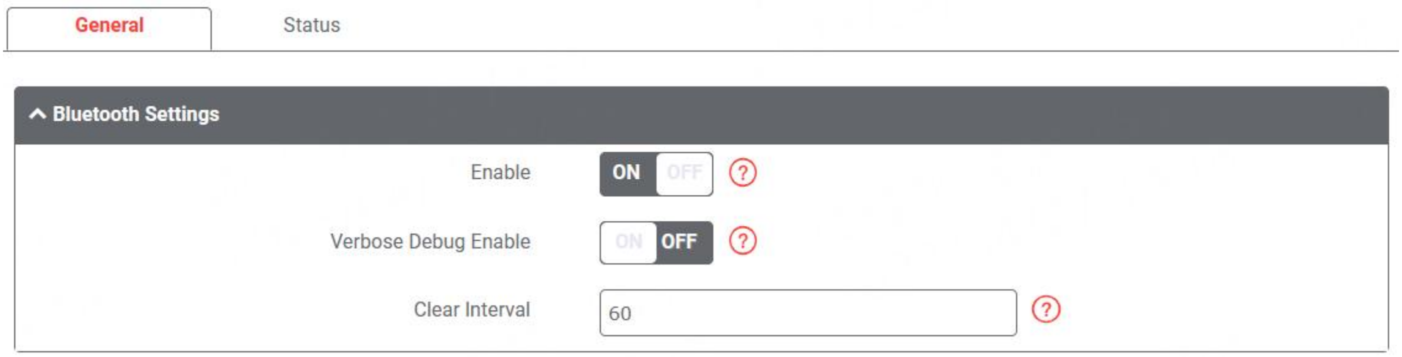
Index	Type	TX	RX	Connection Status
1	RS232	0B	0B	
2	RS232	0B	0B	

3.2.10 Bluetooth

This section allows you to configure Bluetooth parameters. The Bluetooth feature can scan for other nearby Bluetooth devices.

- EG5100, EG5120, EV8100 support an Bluetooth interface (optional).

General



General | Status

^ Bluetooth Settings

Enable: ON

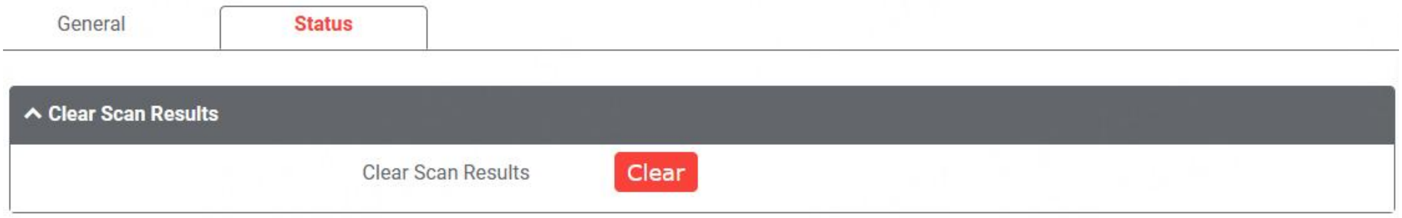
Verbose Debug Enable: OFF

Clear Interval: 60

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 time interval for clearing Bluetooth scan results. Unit: seconds. Valid range: 5-3600	60

Status

Click the "Status" column to view the current Bluetooth status.

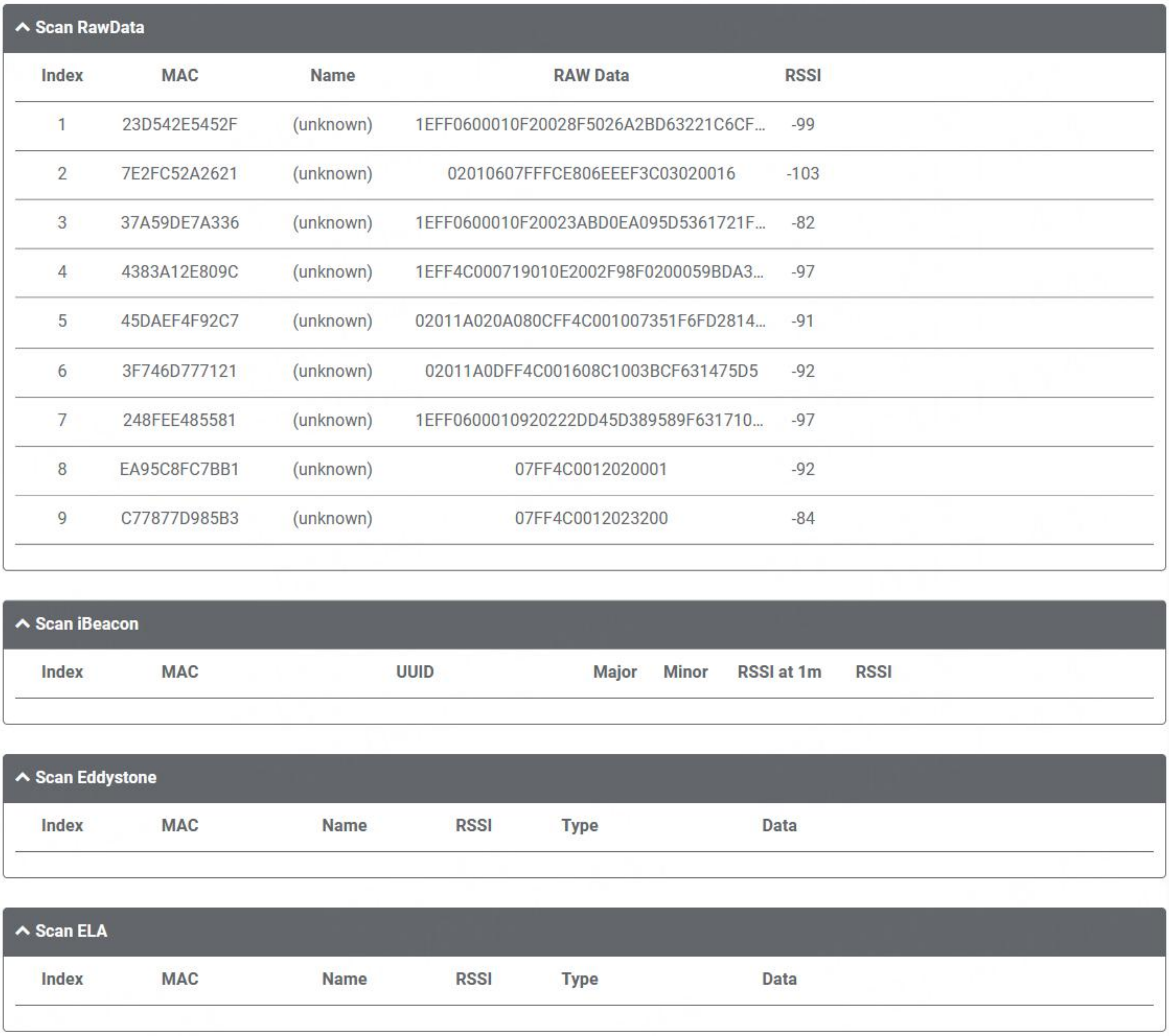


General | Status

^ Clear Scan Results

Clear Scan Results: Clear

Click Clear to clear the scan results.



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)	1EFF060001092022DD45D389589F631710...	-97
8	EA95C8FC7BB1	(unknown)	07FF4C0012020001	-92
9	C77877D985B3	(unknown)	07FF4C0012023200	-84

Index	MAC	UUID	Major	Minor	RSSI at 1m	RSSI

Index	MAC	Name	RSSI	Type	Data

Index	MAC	Name	RSSI	Type	Data

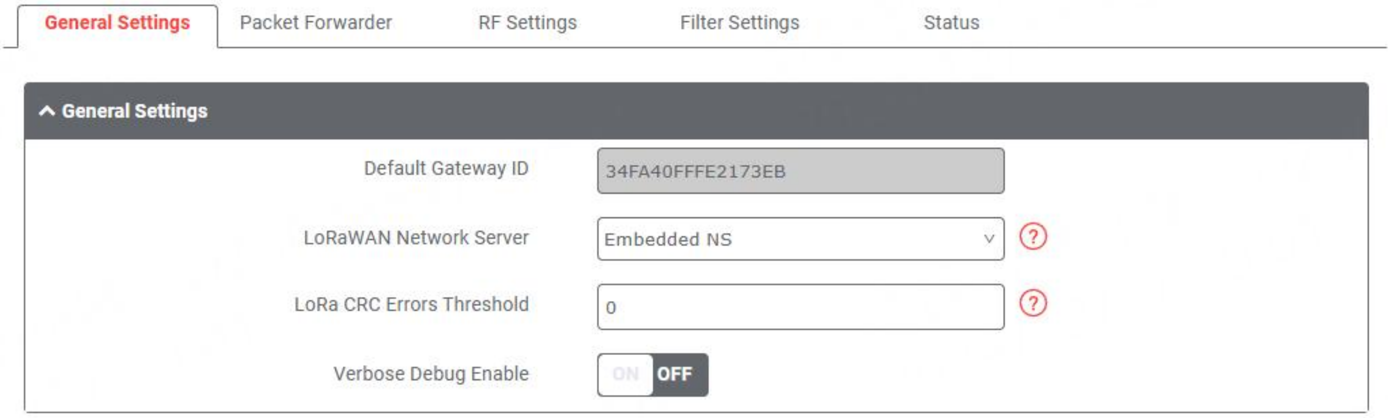
3.3 LoRaWAN

3.3.1 Lora Settings

This section allows you to set the LoRaWAN parameters.

- LG5100 supports a LoRa interface.

General Settings



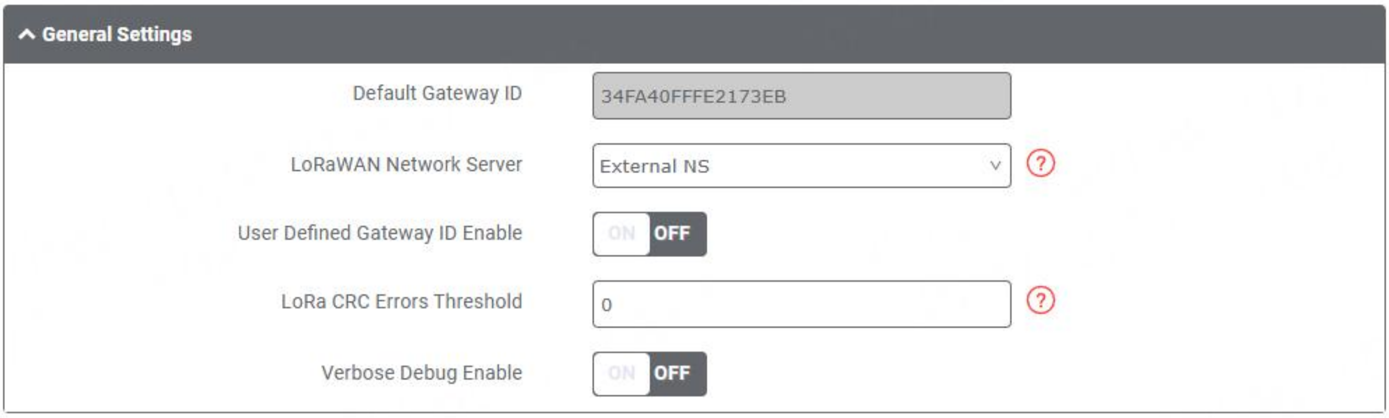
General Settings

Default Gateway ID: 34FA40FFFE2173EB

LoRaWAN Network Server: Embedded NS

LoRa CRC Errors Threshold: 0

Verbose Debug Enable: ON OFF



General Settings

Default Gateway ID: 34FA40FFFE2173EB

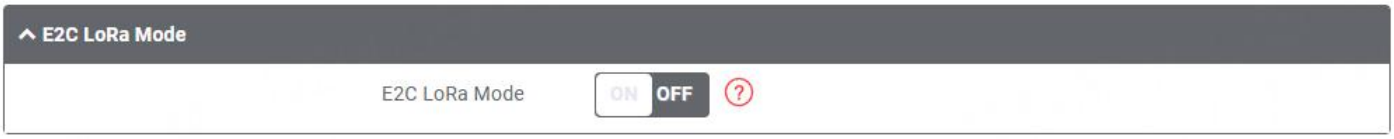
LoRaWAN Network Server: External NS

User Defined Gateway ID Enable: ON OFF

LoRa CRC Errors Threshold: 0

Verbose Debug Enable: ON OFF

Item	Description	Default
Default Gateway ID	The default gateway ID.	--
Network Server	Type of LoRaWAN network server. ● Embedded NS: Embedded Chirpstack network server. ● External NS: When selecting an external NS, further configuration is required on the packet forwarder tab. **Note:** External NS provides options for users with other network servers (e.g., TTI, Loriot).	Embedded NS
Enable User-defined Gateway ID	Click the toggle button to enable/disable the user-defined gateway ID option. **Note:** This applies to external NS.	OFF
LoRa CRC Error Threshold	An event will be generated when the CRC error rate of received LoRa packets exceeds the threshold. 0 means disabled.	0
Output Detailed Debug Information	Click the toggle button to enable debugging functionality to generate log information.	OFF

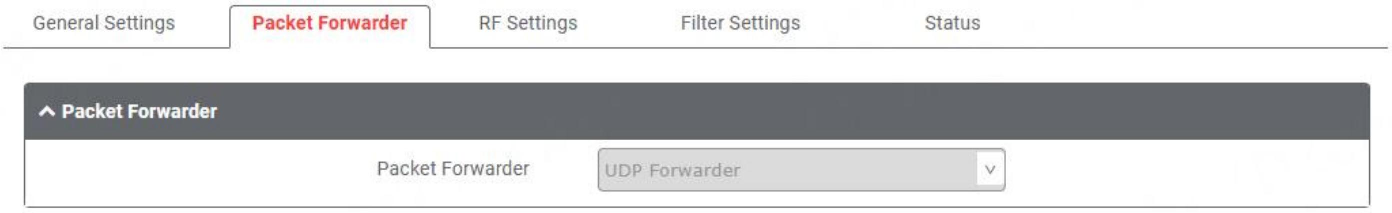


E2C LoRa Mode

E2C LoRa Mode: ON OFF

Item	Description	Default
Enable E2C Mode	Click the toggle button to enable/disable the E2C LoRa mode. When this mode is enabled, LoRa packets will be routed to the specified cloud through the Robustel E2C framework software. **Note:** This option is bundled with the E2C framework software and requires prior installation of E2C Chirpstack.	OFF

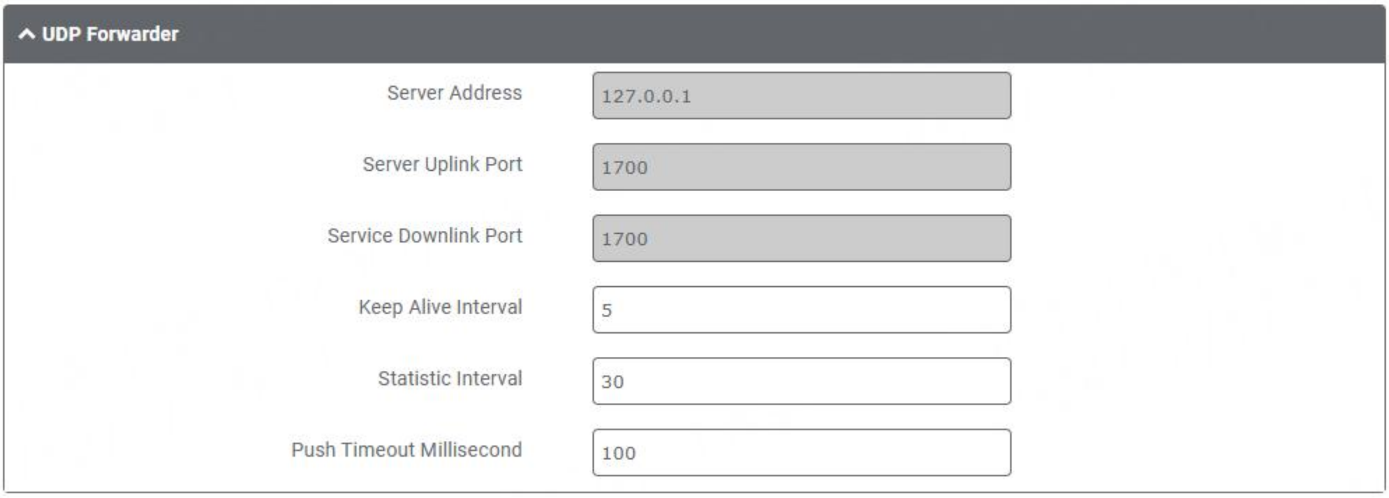
Packet Forwarder



Packet Forwarder

Packet Forwarder: UDP Forwarder

Item	Description	Default
Packet Forwarder	Select from “UDP Forwarder”, “Basic Station” or “Loriot(Coming Soon)”.	UDP Forwarder



UDP Forwarder

Server Address: 127.0.0.1

Server Uplink Port: 1700

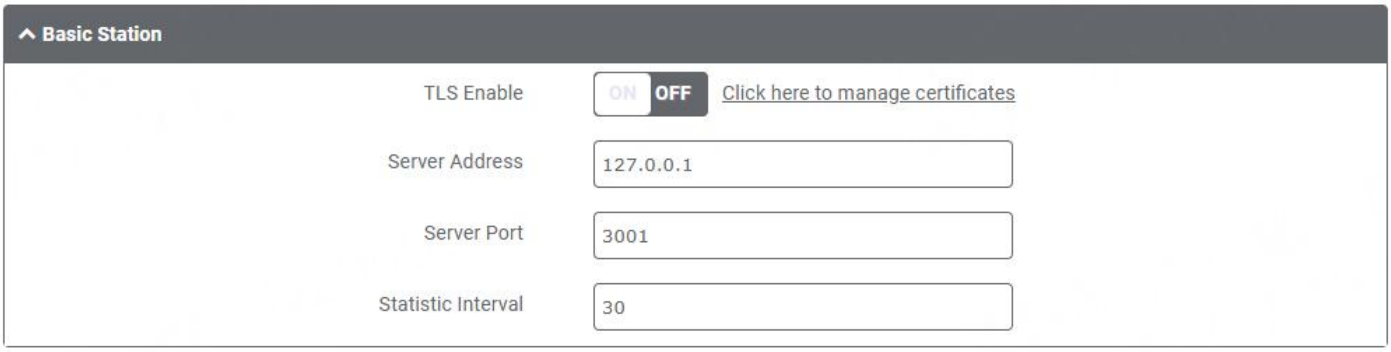
Service Downlink Port: 1700

Keep Alive Interval: 5

Statistic Interval: 30

Push Timeout Millisecond: 100

Item	Description	Default
Server IP	Set the LoRaWAN network server address.	127.0.0.1
Server Uplink Port	Set the uplink port for the LoRaWAN network server.	1700
Server Downlink Port	Set the downlink port for the LoRaWAN network server.	1700
Keep Alive Interval	Time interval for receiving downlink data.	5
Statistics Interval	Interval for statistics and USI update time.	30
Push Timeout (milliseconds)	Uplink data timeout duration.	100



^ Basic Station

TLS Enable: ON OFF [Click here to manage certificates]

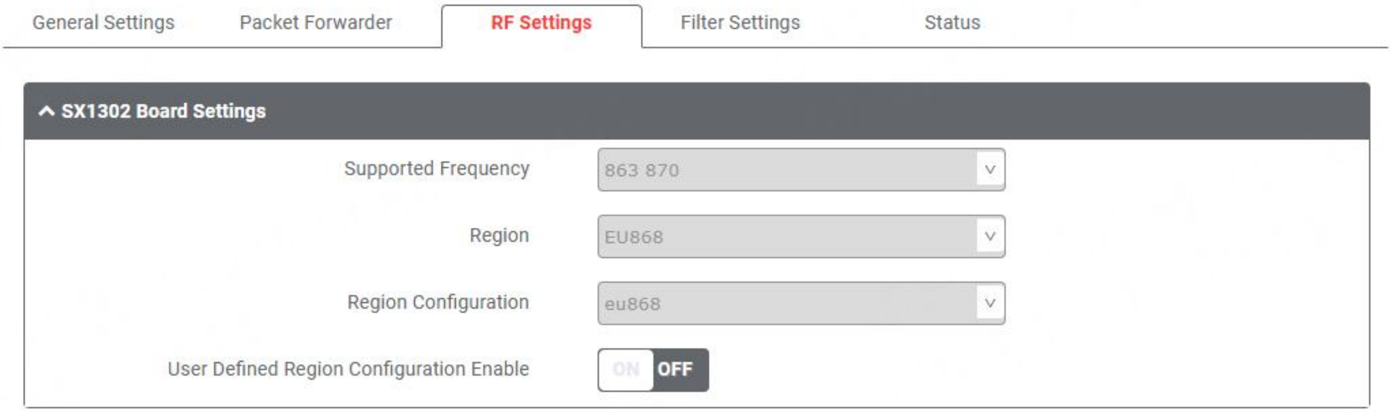
Server Address: 127.0.0.1

Server Port: 3001

Statistic Interval: 30

Item	Description	Default
Enable Encryption	Click the toggle button to enable/disable TLS encrypted transmission. **Note:** You need to go to **System->Certificate Manager->Import Certificate for the LoRa base station** to import the certificates.	OFF
Server Address	Set the server address.	127.0.0.1
Server Port	Set the server port.	3001
Statistics Interval	Interval for statistics and USI update time.	30

RF Settings



General Settings | Packet Forwarder | RF Settings | Filter Settings | Status

^ SX1302 Board Settings

Supported Frequency: 863 870

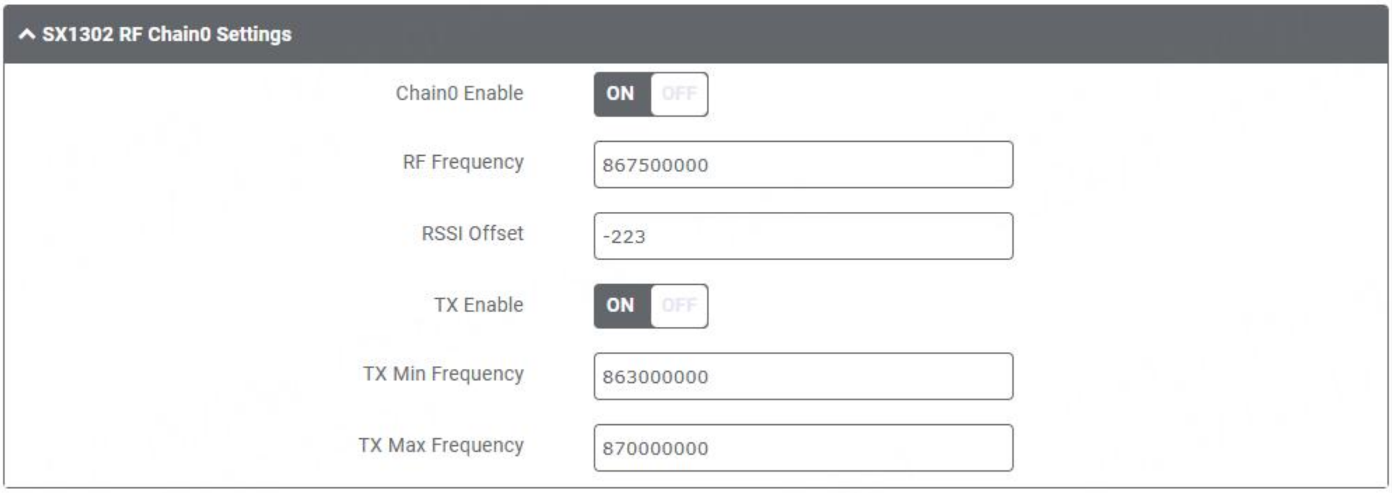
Region: EU868

Region Configuration: eu868

User Defined Region Configuration Enable: ON OFF

Item	Description	Default
Frequency Band Range	Displays the supported frequencies: “868 870”, “470 510”, “902 928”	Displays based on device model.
Region	EU868/CN470/AU915/US915	Displays based on device model.
Frequency Band	Select the frequency bands supported by the device.	Displays based on device model.
Custom Frequency Band Configuration	When enabled, allows users to configure custom frequency bands.	OFF

When the user-defined region configuration is enabled, users can set up RF Chain 0/Chain 1/Multi channels on their own.



SX1302 RF Chain0 Settings

Chain0 Enable: ON

RF Frequency: 867500000

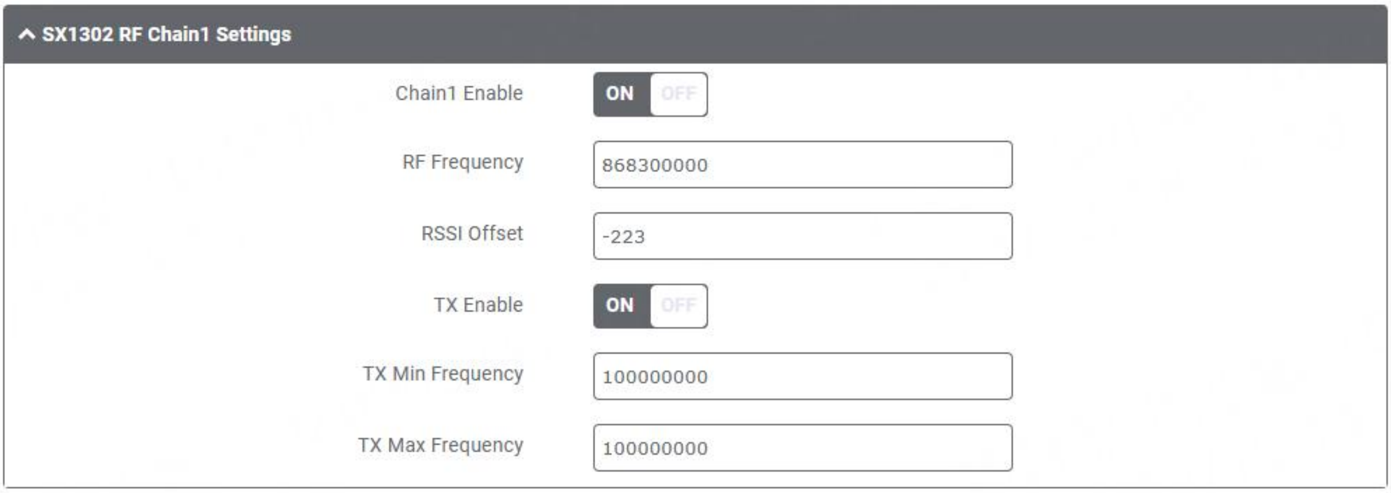
RSSI Offset: -223

TX Enable: ON

TX Min Frequency: 863000000

TX Max Frequency: 870000000

Item	Description	Default
Link 0 Enable	Click the toggle button to enable/disable Link 0.	ON
RF Frequency	Set the frequency for RF Link 0.	Set according to device model.
RSSI Offset Value	Set the offset value for RF Link 0.	0
Transmission Enable	Click the toggle button to enable/disable transmission mode.	ON
Minimum Transmission Frequency	Set the minimum transmission frequency for RF Link 0.	Set according to device model.
Maximum Transmission Frequency	Set the maximum transmission frequency for RF Link 0.	Set according to device model.



SX1302 RF Chain1 Settings

Chain1 Enable: ON

RF Frequency: 868300000

RSSI Offset: -223

TX Enable: ON

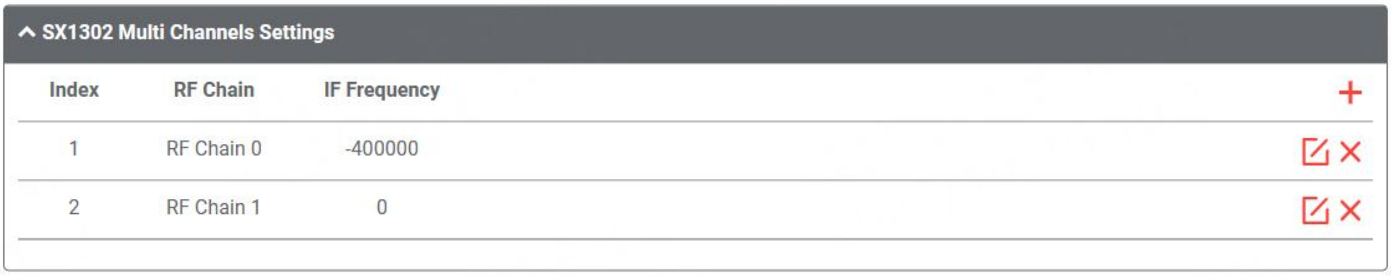
TX Min Frequency: 100000000

TX Max Frequency: 100000000

Item	Description	Default
Link 1 Enable	Click the toggle button to enable/disable Link 1.	ON

Item	Description	Default
RF Frequency	Set the frequency for RF Link 1.	Set according to device model.
RSSI Offset Value	Set the offset value for RF Link 1.	0
Transmission Enable	Click the toggle button to enable/disable transmission mode.	OFF
Minimum Transmission Frequency	Set the minimum transmission frequency for RF Link 1.	Set according to device model.
Maximum Transmission Frequency	Set the maximum transmission frequency for RF Link 1.	Set according to device model.

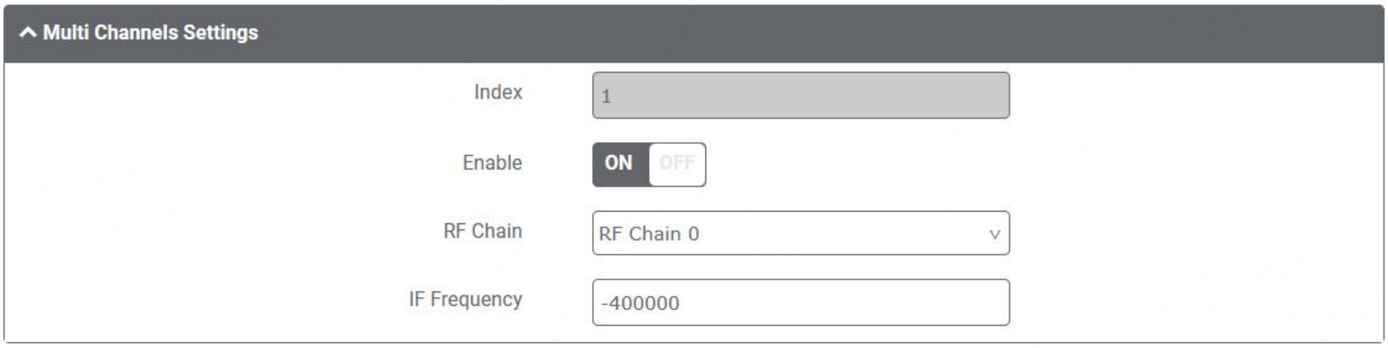
You can enable multi-channel in this setting.



^ SX1302 Multi Channels Settings

Index	RF Chain	IF Frequency
1	RF Chain 0	-400000
2	RF Chain 1	0

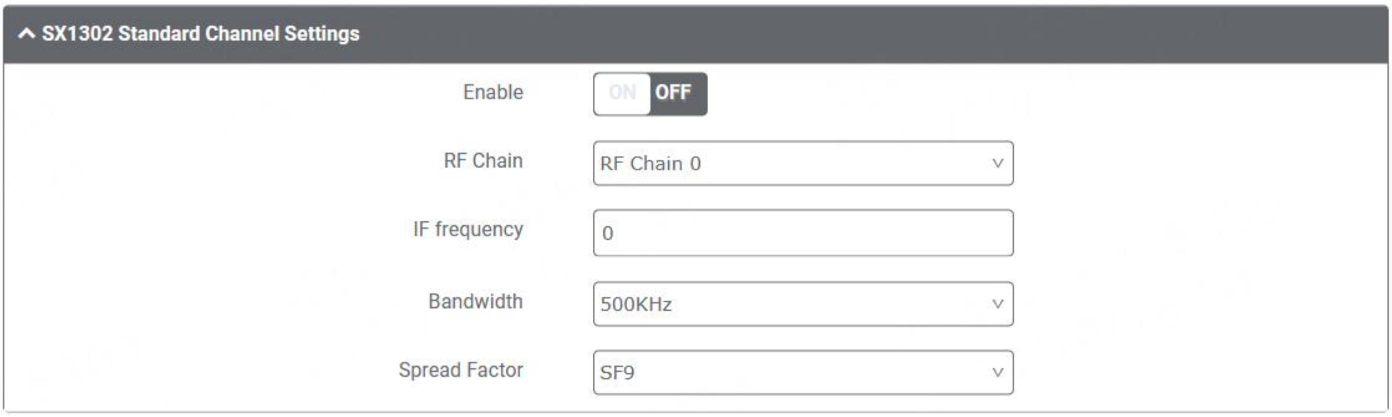
Click ☑ to edit the RF Chain settings. RF Chain 0 is used as an example.



^ Multi Channels Settings

Index	1
Enable	ON OFF
RF Chain	RF Chain 0
IF Frequency	-400000

Item	Description	Default
Index	Specifies the sequence number of the list.	--
Enable	Click the toggle button to enable/disable this option.	ON
RF Chain	Select the RF link.	RF Chain 0
IF Frequency	Enter a center frequency within the range of -500000 to 500000 (in Hz). This is the offset between the center frequency of the specific channel and the center frequency of RF Link 0/1.	0



^ SX1302 Standard Channel Settings

Enable: ON OFF

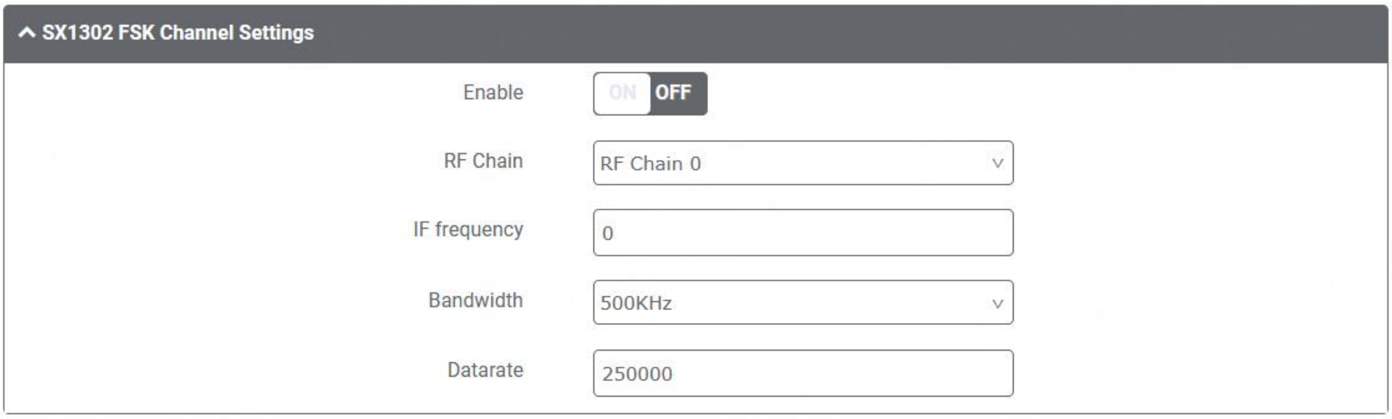
RF Chain: RF Chain 0

IF frequency: 0

Bandwidth: 500KHz

Spread Factor: SF9

Item	Description	Default
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Select the RF link.	RF Chain 0
IF Frequency	Enter a center frequency within the range of -500000 to 500000 (in Hz). This is the offset between the center frequency of the specific channel and the center frequency of RF Link 0/1.	0
Bandwidth	Select the optional bandwidth (in KHz).	500KHz
Spread Factor	Enter the optional spreading factor. A high spreading factor corresponds to a low data rate, while a low spreading factor corresponds to a high data rate.	SF9



^ SX1302 FSK Channel Settings

Enable: ON OFF

RF Chain: RF Chain 0

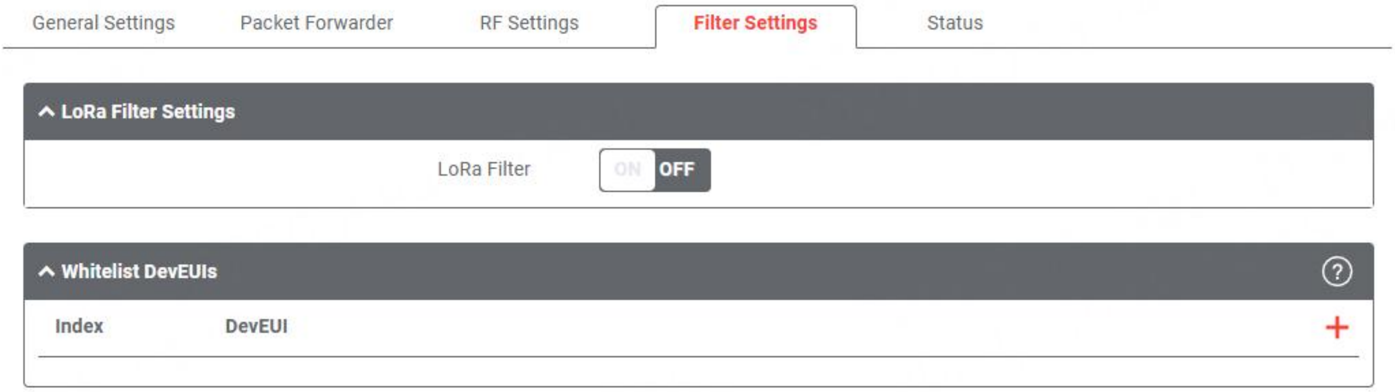
IF frequency: 0

Bandwidth: 500KHz

Datarate: 250000

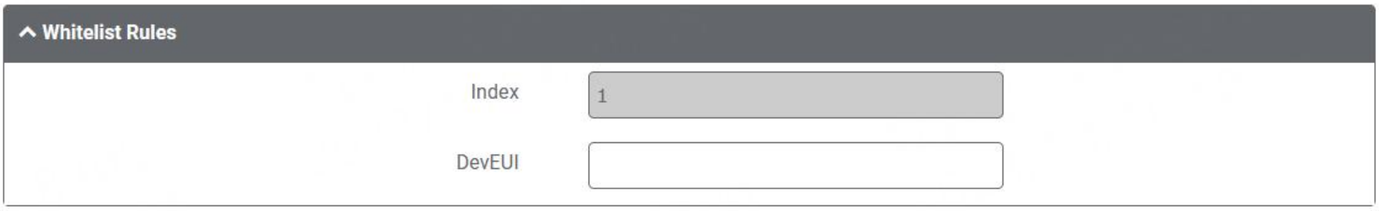
Item	Description	Default
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Select the RF link.	RF Chain 0
IF Frequency	Enter a center frequency within the range of -500000 to 500000 (in Hz). This is the offset between the center frequency of the specific channel and the center frequency of RF Link 0/1.	0
Bandwidth	Select the optional bandwidth (in KHz).	500KHz
Datarate	Enter the data rate.	250000

Filter Settings



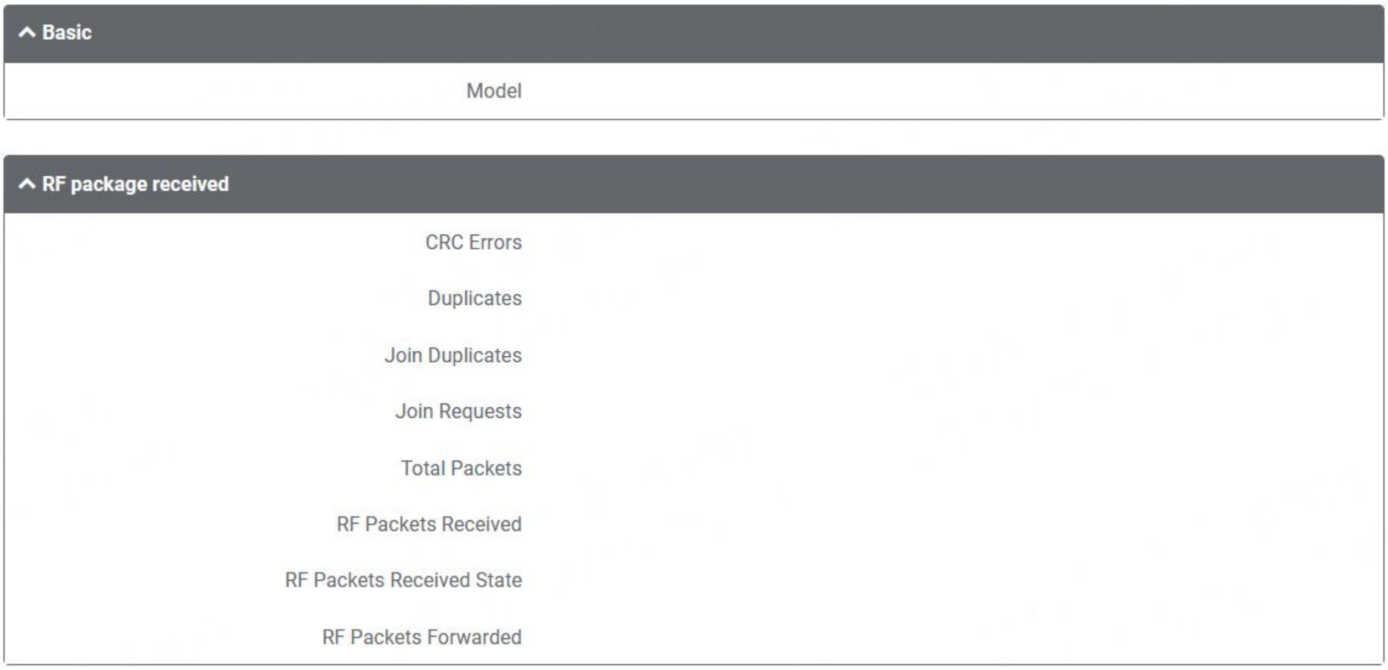
Item	Description	Default
LoRa Filter	Click the toggle button to enable/disable this option.	OFF

Click + to add a whitelist rule.



Item	Description	Default
Index	Specify the sequence number of the list.	--
DevEUI	Enter the device's DevEUI, which is usually provided by the device manufacturer. The DevEUI is typically an 8-byte (16 hexadecimal characters) identifier.	Null

Status



^ Basic

Model

^ RF package received

CRC Errors

Duplicates

Join Duplicates

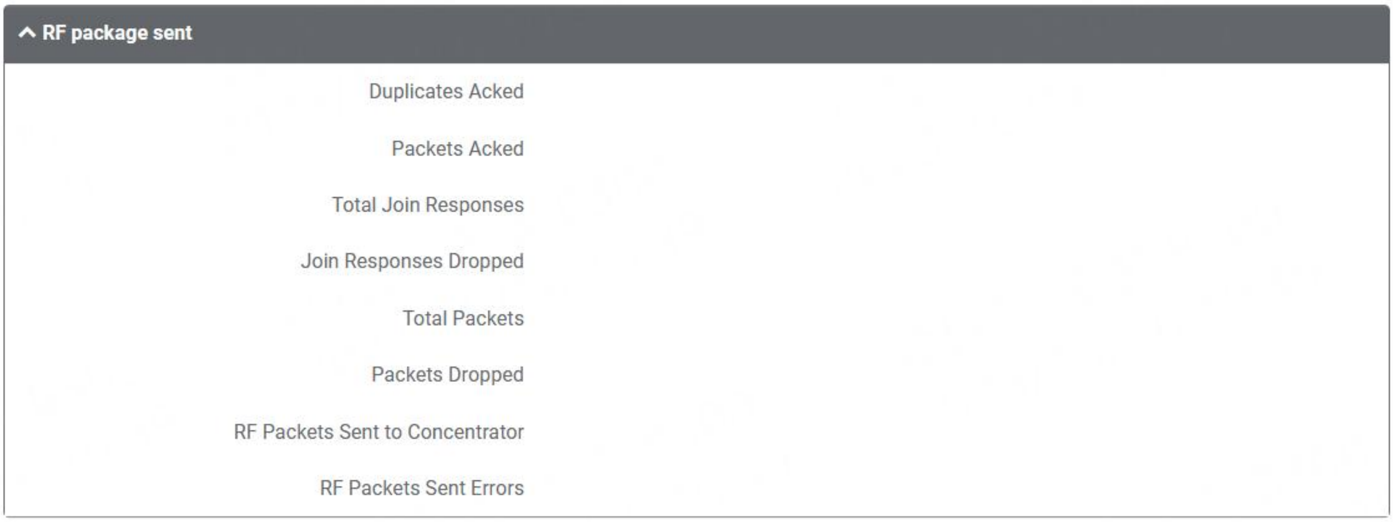
Join Requests

Total Packets

RF Packets Received

RF Packets Received State

RF Packets Forwarded



^ RF package sent

Duplicates Acked

Packets Acked

Total Join Responses

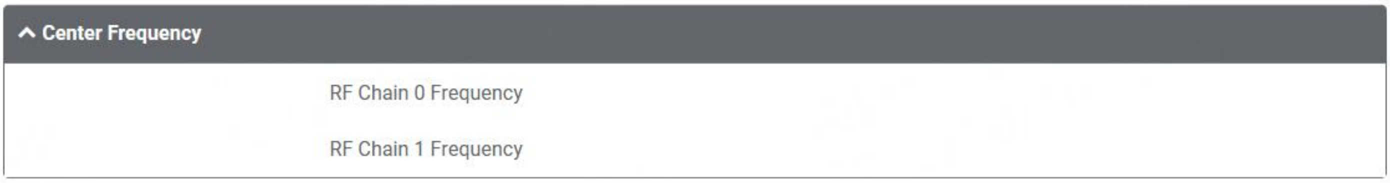
Join Responses Dropped

Total Packets

Packets Dropped

RF Packets Sent to Concentrator

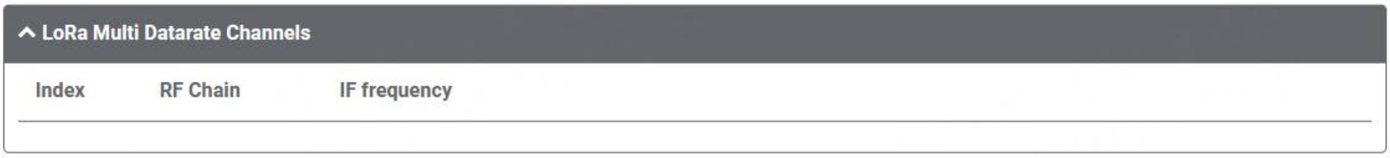
RF Packets Sent Errors



^ Center Frequency

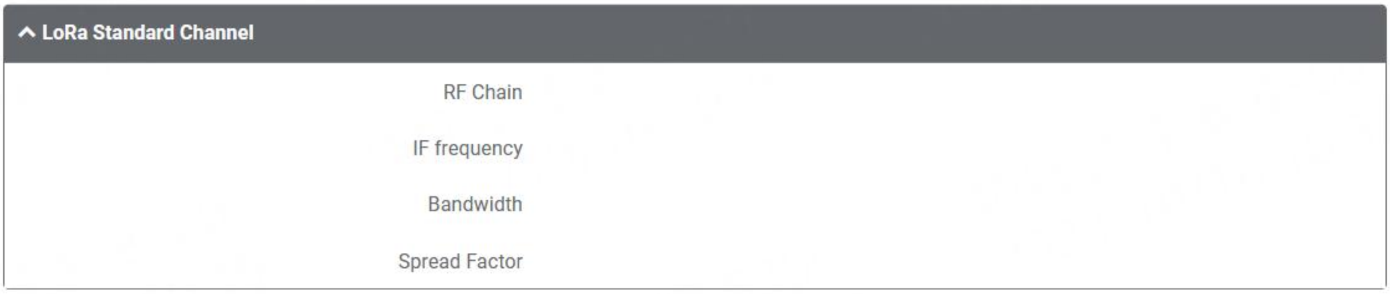
RF Chain 0 Frequency

RF Chain 1 Frequency



^ LoRa Multi Datarate Channels

Index	RF Chain	IF frequency



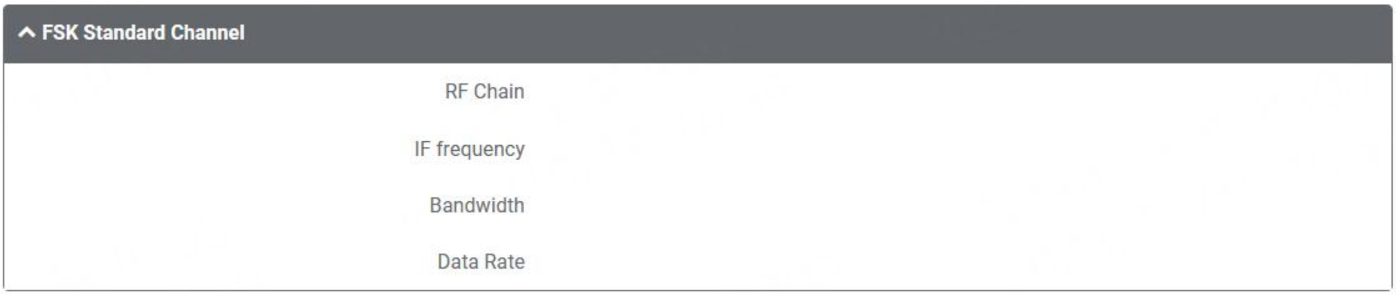
^ LoRa Standard Channel

RF Chain

IF frequency

Bandwidth

Spread Factor



^ FSK Standard Channel

RF Chain

IF frequency

Bandwidth

Data Rate

Status	
Item	**Description**
Basic	
Model	Show the LoRa module model.
RF Package received	
CRC Errors	Show the value of incorrectly received RF packets.
Duplicates	Show the value of received duplicate RF packets.
Join Duplicates	Show the value of received duplicate RF join request packets.
Join Requests	Show the value of received RF join request packets.
Total Packets	Show the value of received RF packets.
RF Packets Received	Show the number of packets from the node to the gateway.
RF Packets Received State	Show the RF packets reception status. • CRC_OK: Percentage of CRC validated packets • CRC_Fail: Percentage of packets with CRC validation failures • NO_CRC: Percentage of abnormal packets without CRC
RF Packets Forwarded	Show the values of incorrectly received RF packets.
Packets sent	
Duplicates Acked	Show the value of sent duplicate RF response packets.

Status	
Item	**Description**
Packets Acked	Show the value of sent RF response packets.
Total Join Responses	Show the value of sent duplicate RF join response packets.
Join Responses Dropped	Show the value of failed RF join response packets.
Total Packets	Show the value of sent RF packets.
Packets Dropped	Show the value of RF dropped packets.
RF Packets Sent to Concentrator	Show the value of RF packets sent to the concentrator.
RF Packets Sent Errors	Show the value of RF packets transmission errors.
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	
Index	Index of LoRa channel.
RF Chain	Show the IF frequency of LoRa channel.
IF Frequency	Display the channel frequency offset.
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.

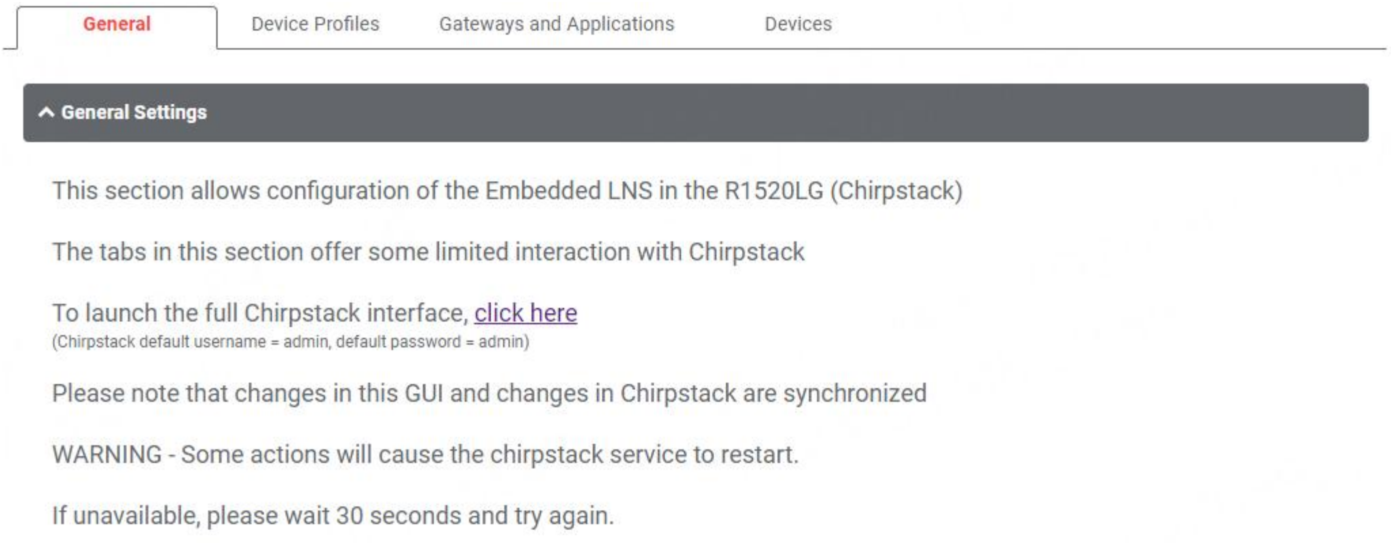
3.3.2 Embedded LNS

This section allows for the configuration of the embedded LNS (Chirpstack).
The tabs in this section provide some limited interaction with Chirpstack.

Please note that changes made in this GUI are synchronized with changes in Chirpstack.
Warning: Certain operations will cause the Chirpstack service to restart. If unavailable, please wait 30 seconds and try again.

For more configuration instructions, please refer to https://www.chirpstack.io/docs/.

General



General Settings

This section allows configuration of the Embedded LNS in the R1520LG (Chirpstack)

The tabs in this section offer some limited interaction with Chirpstack

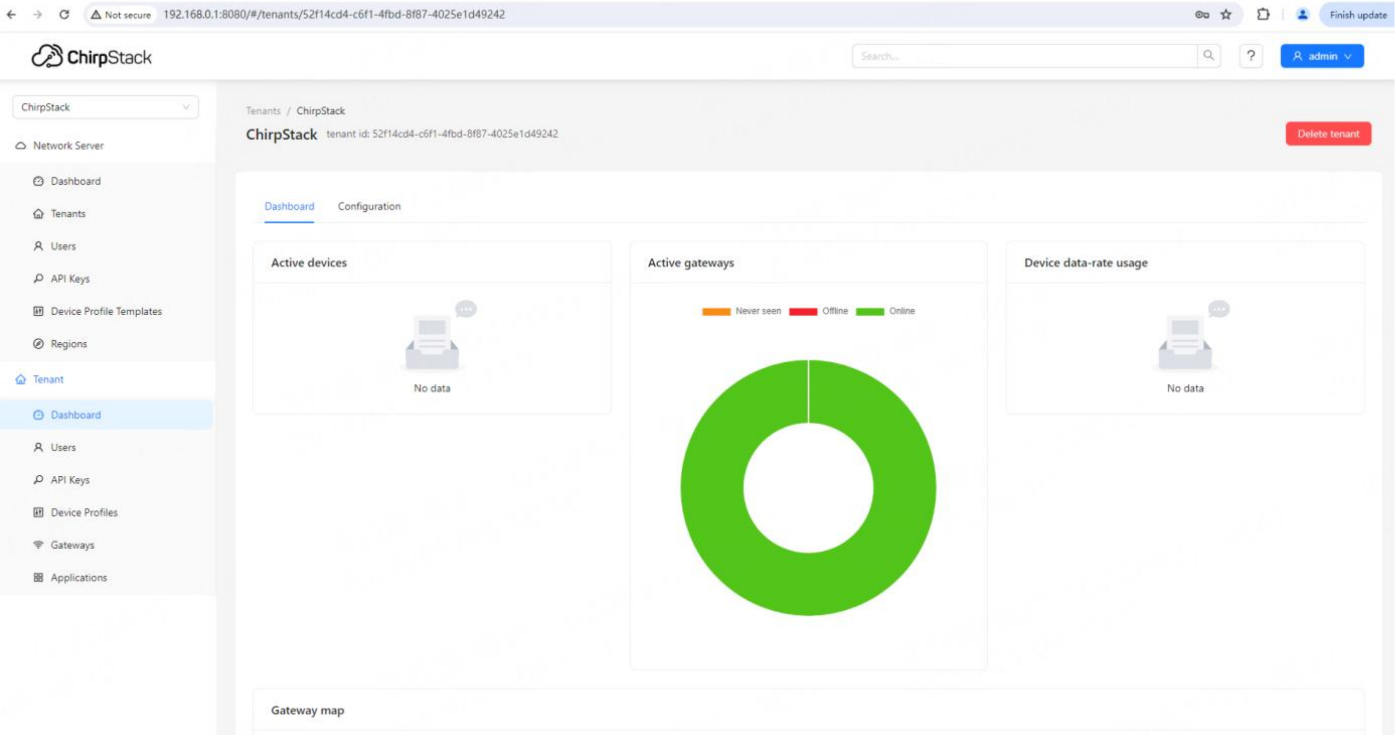
To launch the full Chirpstack interface, click here
(Chirpstack default username = admin, default password = admin)

Please note that changes in this GUI and changes in Chirpstack are synchronized

WARNING - Some actions will cause the chirpstack service to restart.

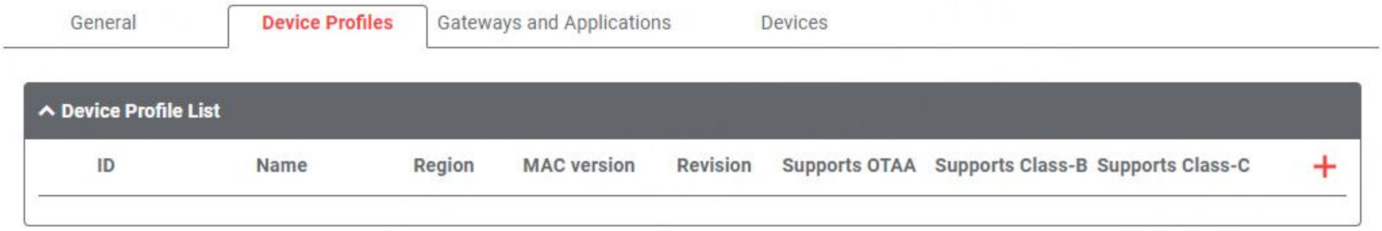
If unavailable, please wait 30 seconds and try again.

To launch the full Chirpstack interface, please go to the http://192.168.0.1:8080.
(Chirpstack default username = admin, default password = admin).



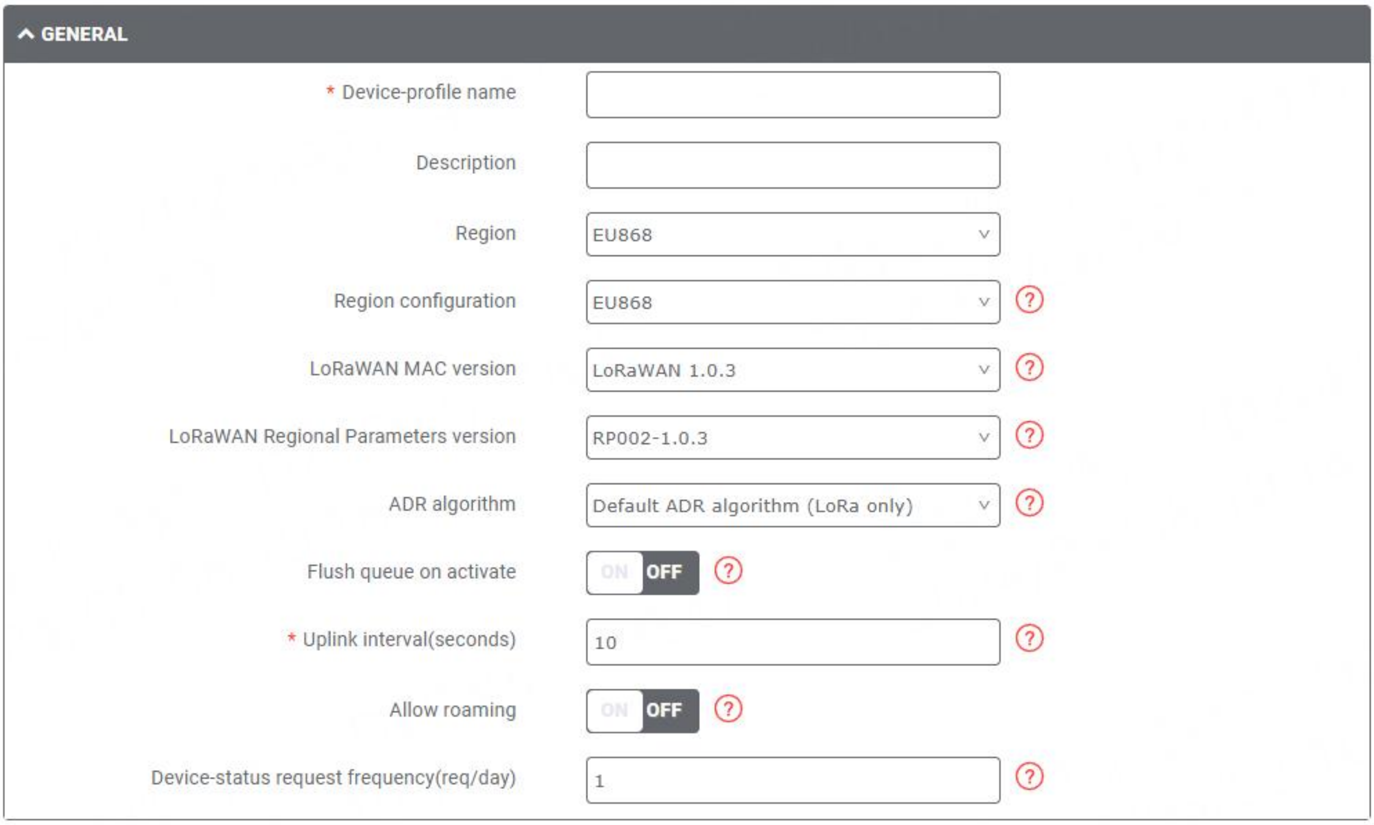
Device Profiles

This section allows to create/edit/delete the device profile.



ID	Name	Region	MAC version	Revision	Supports OTAA	Supports Class-B	Supports Class-C	+

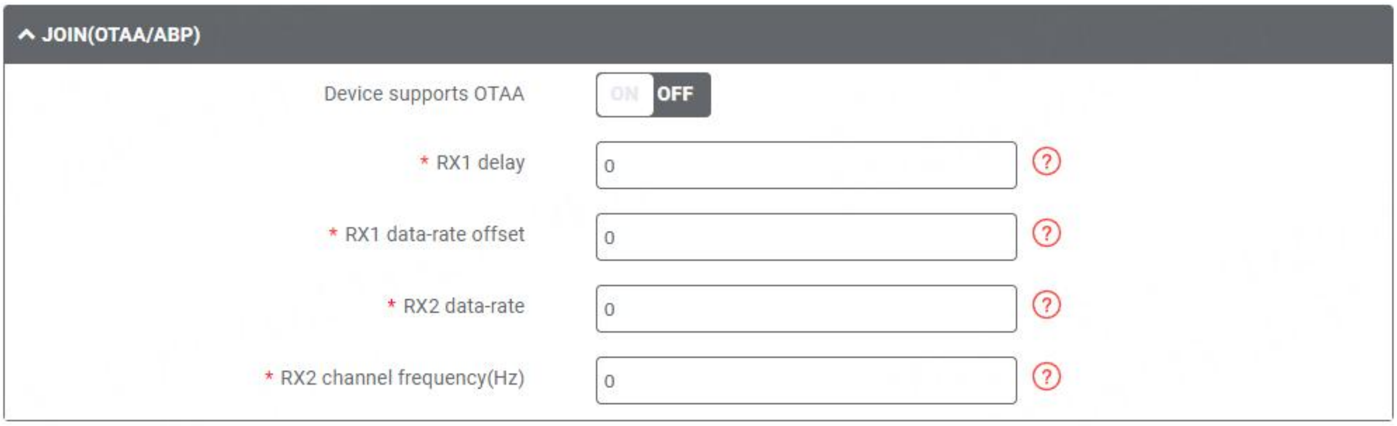
Click + to add a device profile.



* Device-profile name	
Description	
Region	EU868
Region configuration	EU868
LoRaWAN MAC version	LoRaWAN 1.0.3
LoRaWAN Regional Parameters version	RP002-1.0.3
ADR algorithm	Default ADR algorithm (LoRa only)
Flush queue on activate	ON OFF
* Uplink interval(seconds)	10
Allow roaming	ON OFF
Device-status request frequency(req/day)	1

Item	Description	Default
*Device-profile name	The name of the device profile.	Null
Description	The description of the device profile.	Null
Region	Select the appropriate region based on the device model.	Set according to device model.
Region configuration	Select the relevant region configuration according to the device model.	Set according to device model.
LoRaWAN MAC version	Select the LoRaWAN version supported by the end-device.	LoRaWAN 1.0.3
LoRaWAN Regional	Select the version of the LoRaWAN regional parameters supported by	PR002-1.0.3

Item	Description	Default
Parameters version	the end-device.	
ADR algorithm	The ADR algorithm is used for controlling the device data-rate. Select from “LoRa Only”, “LoRa & LR-FHSS” or “LR-FHSS Only”.	LoRa Only
Flush queue on activate	If enabled, the device queue will be flushed on ABP or OTAA activation.	OFF
*Uplink interval(seconds)	The expected interval (in seconds) for the device to send uplink messages, used to determine device activity.	10
Allow roaming	If enabled (and configured on the server), this allows the device to use roaming.	OFF
Device-status request frequency(req/day)	The frequency for initiating an end-device status request (requests per day). Set to 0 to disable.	1



JOIN(OTAA/ABP)

Device supports OTAA: ON OFF

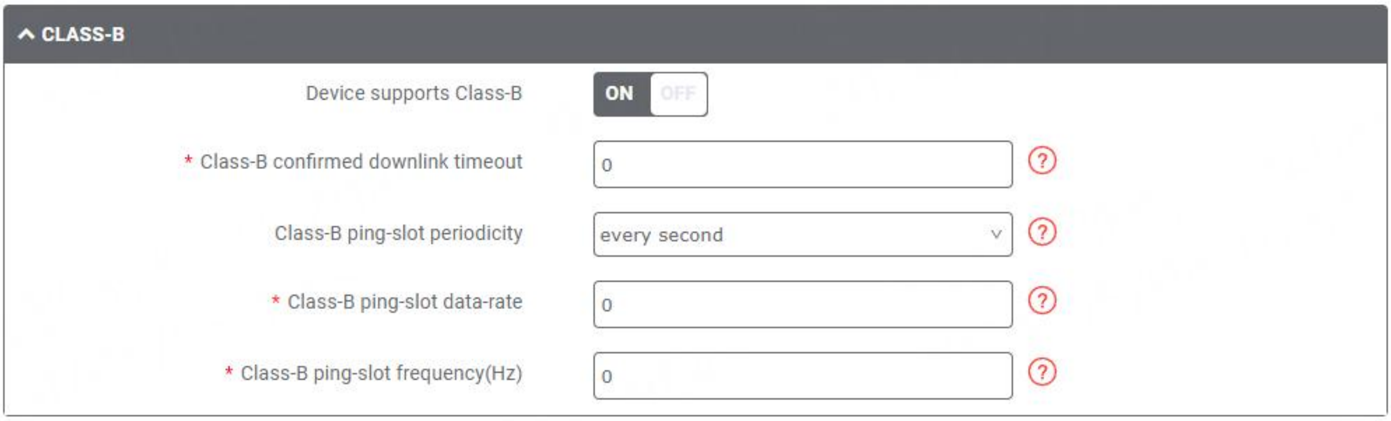
* RX1 delay: 0

* RX1 data-rate offset: 0

* RX2 data-rate: 0

* RX2 channel frequency(Hz): 0

Item	Description	Default
Device supports OTAA	Click to enable the join type as OTAA, otherwise, it will default to ABP.	ON
*RX1 delay	This needs to be set to the same value as the end device.	0
*RX1 data-rate offset	This needs to be set to the same value as the end device.	0
*RX2 data-rate	This needs to be set to the same value as the end device.	0
*RX2 channel frequency(Hz)	This needs to be set to the same value as the end device.	0



CLASS-B

Device supports Class-B: ON

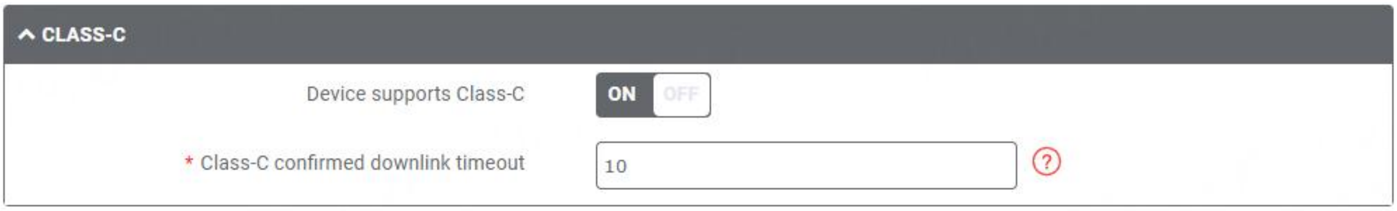
* Class-B confirmed downlink timeout: 0

Class-B ping-slot periodicity: every second

* Class-B ping-slot data-rate: 0

* Class-B ping-slot frequency(Hz): 0

Item	Description	Default
Device supports Class-B	Click to enable the Class-B mode.	OFF
*Class-B confirmed downlink timeout	Confirm the Class-B timeout for downlink transmission (in seconds).	0
*Class-B ping-slot periodicity	Select a value ranging from every second to every 128 seconds.	Every second
*Class-B ping-slot data-rate	This needs to be set to the same value as the end device.	0
*Class-B ping-slot frequency(Hz)	This needs to be set to the same value as the end device.	0

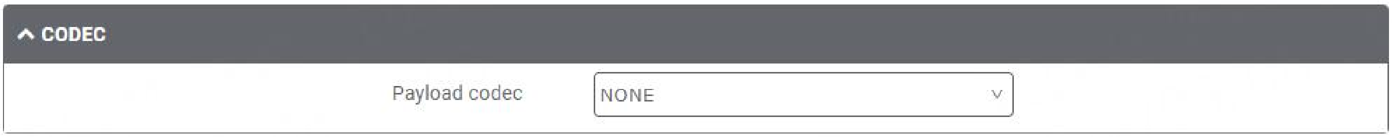


CLASS-C

Device supports Class-C: ON

* Class-C confirmed downlink timeout: 10

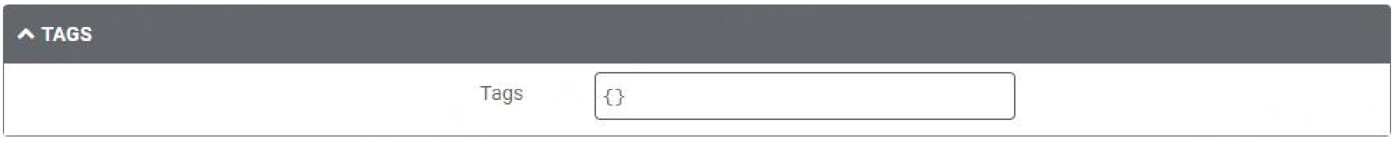
Item	Description	Default
Device supports Class-C	Click to enable the Class-C mode.	OFF
*Class-C confirmed downlink timeout	Confirm the Class-C timeout for downlink transmission (in seconds).	10



CODEC

Payload codec: NONE

Item	Description	Default
Payload codec	Select from “NONE”, “CAYENNE_LPP” or “JS”.	NONE



^ TAGS

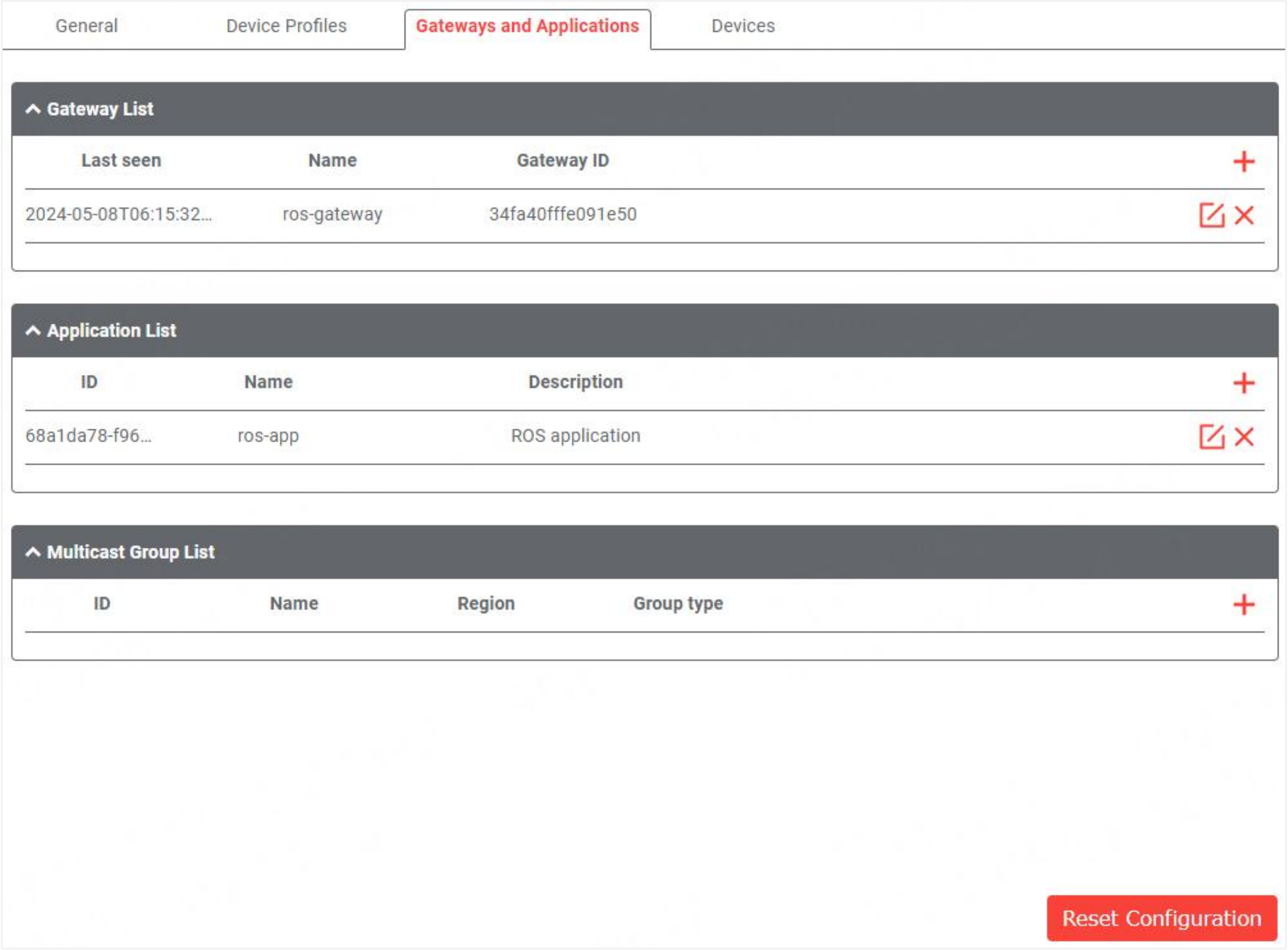
Tags: {}

Item	Description	Default
Tags	In this tab, you can assign additional tags to the device profile. These tags will be exposed in device events and can include other metadata, such as: vendor name, device model...	Null

Gateways and Applications

This section allows to create/edit/delete the gateways and applications.

The gateway is equipped with a default gateway and default application, enabling users to quickly set up their own LoRaWAN system.



^ Gateway List

Last seen	Name	Gateway ID
2024-05-08T06:15:32...	ros-gateway	34fa40fffe091e50

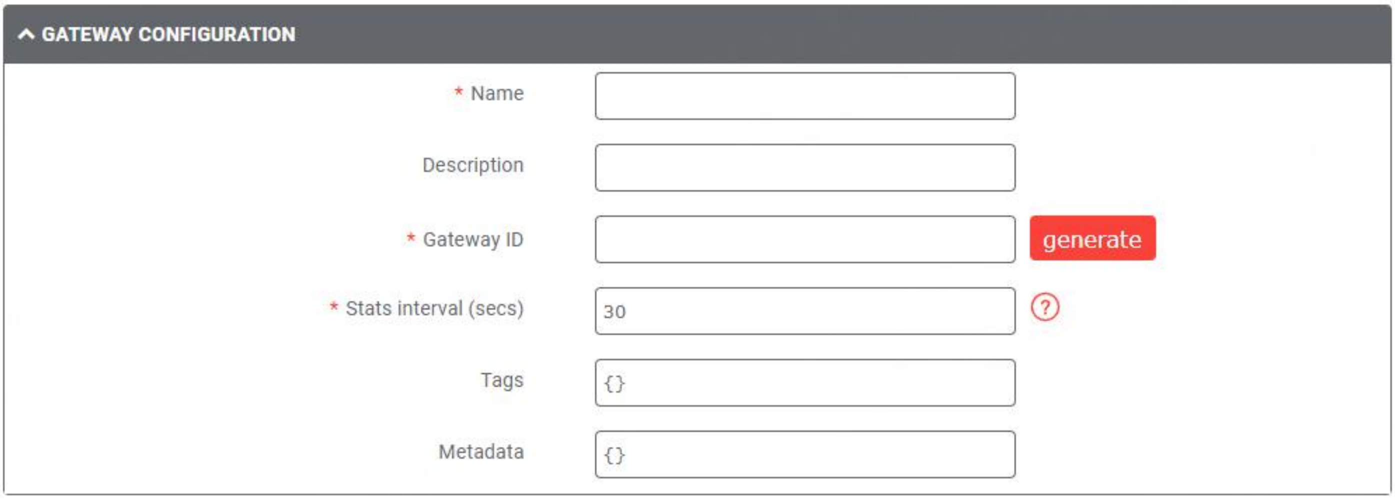
^ Application List

ID	Name	Description
68a1da78-f96...	ros-app	ROS application

^ Multicast Group List

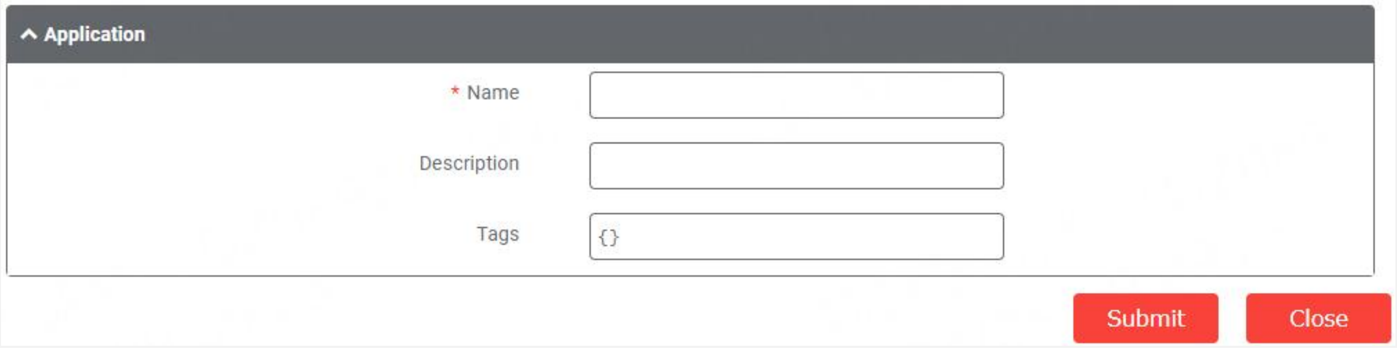
ID	Name	Region	Group type

Click + to add a gateway.

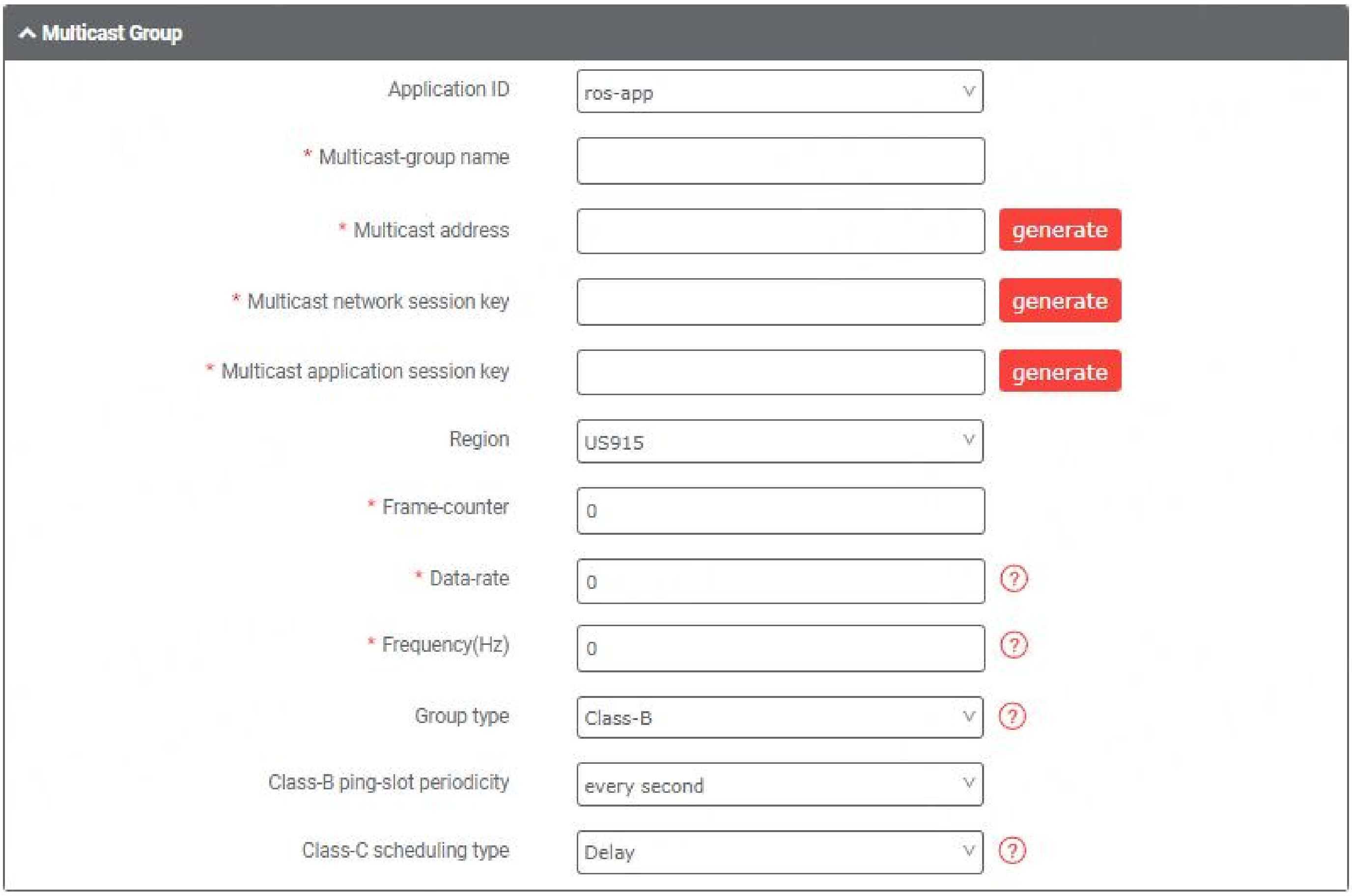


Item	Description	Default
*Name	Set the gateway name.	Null
Description	Set the description of the gateway.	Null
*Gateway ID	Set the gateway ID, which can also be generated randomly by clicking the **generate** button.	Null
*Stats interval (secs)	Expected interval in seconds for the gateway to send its statistics.	30
Tags	Set tags.	Null
Metadata	Set metadata.	Null

An application is a collection of devices with the same purpose or of the same type.



Item	Description	Default
*Name	The name of the application.	Null
Description	The description of the application.	Null
Tags	The additional tags of the application.	Null



^ Multicast Group

Application ID: ros-app

* Multicast-group name:

* Multicast address: generate

* Multicast network session key: generate

* Multicast application session key: generate

Region: US915

* Frame-counter: 0

* Data-rate: 0

* Frequency(Hz): 0

Group type: Class-B

Class-B ping-slot periodicity: every second

Class-C scheduling type: Delay

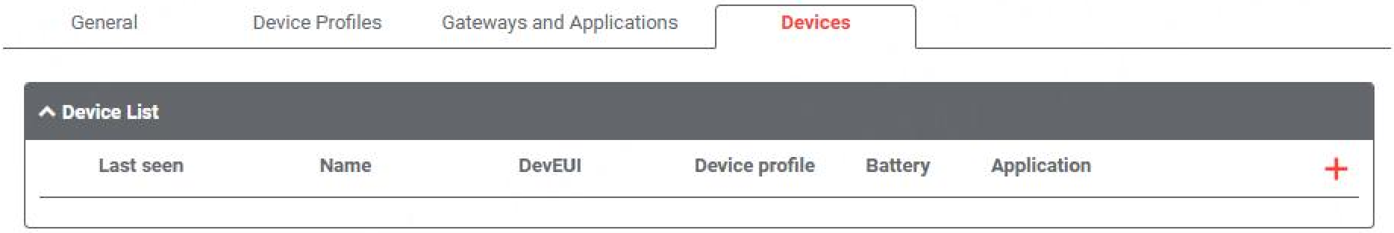
Item	Description	Default
Application ID	Select from the created applications.	ros-app
*Multicast-group name	The name of the multicast-group.	Null
*Multicast address	The address of the multicast-group.	Null
*Multicast network session key	Enter the value for the multicast network session key. You can generate a random key by clicking the button.	Null
*Multicast application session key	Enter the value for the multicast application session key. You can generate a random key by clicking the button.	Null
Region	Select the appropriate option based on the device.	Set according to device model.
*Frame-counter	Enter the value of frame-counter.	0
*Data-rate	Enter the value of data-rate.	0
*Frequency(Hz)	Enter the value of frequency, in Hz.	0
Group type	The multicast group type defines how the network server schedules multicast frames. Choose between 'Class-B' and 'Class-C.'	Class-B
Class-B ping-slot periodicity	Select from once every second to once every 128 seconds.	every second
Class-C scheduling type	Select either “Delay” or “GPS Time”.	Delay

By creating a multicast group, a single downlink payload can be sent to the load of a group of devices (the multicast group). All these devices share the same multicast address, session key, and frame counter.

Once a multicast group is created, devices can be assigned to that group. Please note that the devices must already be created.

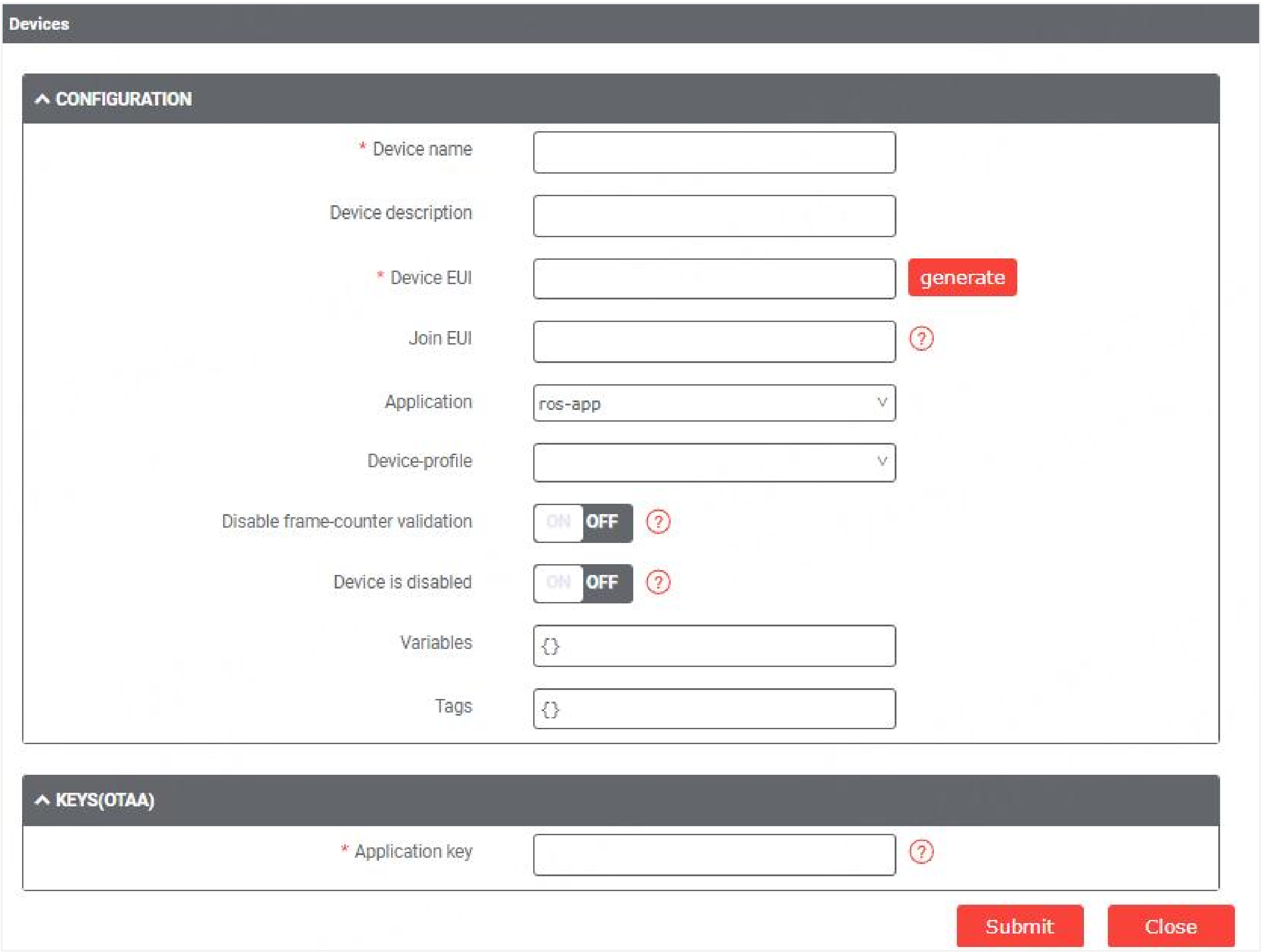
Devices

This section allows to create/edit/delete the devices.
A device is the end-device that connect and communicate through a LoRaWAN® network.



Item	Description	Default
Last seen	The time of end-device was on line.	--
Name	The name of end-device.	--
DevEUI	The unique ID of end-device.	--
Device Profile	The device profile of end-device.	--
Battery	The battery level of end-device if it had.	--
Application	The application of end-device.	--

Click + to add a device.



Devices

^ CONFIGURATION

* Device name

Device description

* Device EUI

Join EUI

Application: ros-app

Device-profile

Disable frame-counter validation: OFF

Device is disabled: OFF

Variables: {}

Tags: {}

^ KEYS(OTAA)

* Application key

Item	Description	Default
Device name	The name of end-device.	Null
Device description	The description of end-device.	Null
Device EUI	The unique ID of end-device. You can generate it by clicking the button.	Null
Join EUI	The Join EUI will be automatically set/updated on OTAA. However, in some cases, this field must be configured before OTAA (for example, when using a relay for OTAA).	Null
Application	Select from the created applications.	ros-app
Device-profile	Select from the created device profiles.	Null
Disable frame-counter validation	Click the toggle button to enable/disable this option. You must reactivate your device before this setting to take effect. Please note that disabling frame counter validation compromises security as it allows replay attacks.	OFF
Device is disabled	Click the toggle button to enable/disable this option. When this option is enabled, received uplink frames and connection requests will be ignored.	OFF

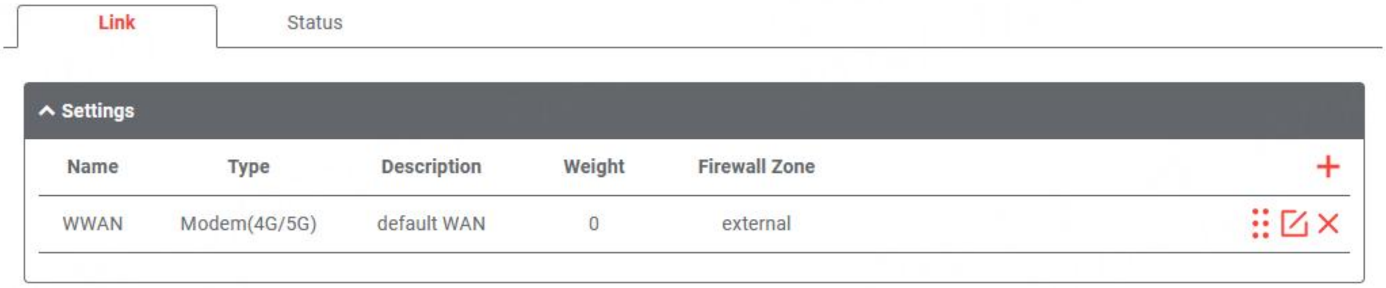
Item	Description	Default
Variables	Set the variables. Variables are used for integration and may contain API tokens.	Null
Tags	Set the additional tags. Tags are exposed when ChirpStack publishes device events and can be used to add other metadata, e.g. for aggregation.	Null
Application key	Set the application key. **Note:** For LoRaWAN 1.0 devices. If your device supports LoRaWAN 1.1, please update the device profile first.	Null

3.4 Network

3.4.1 WAN

WAN stands for Wide Area Network, providing a connection to the internet. You can configure WAN based on Ethernet, cellular modem or Wi-Fi (if supported).

Link



Name	Type	Description	Weight	Firewall Zone	+
WWAN	Modem(4G/5G)	default WAN	0	external	⠿ ✎ ×

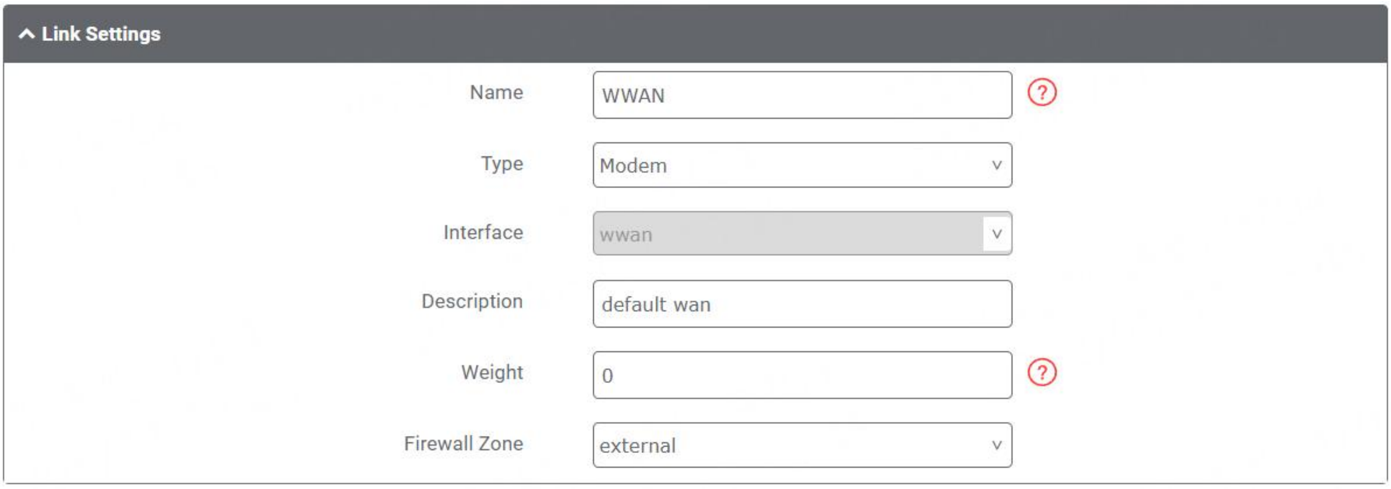
Click + to add a new WAN link.

Click × to delete the link.

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

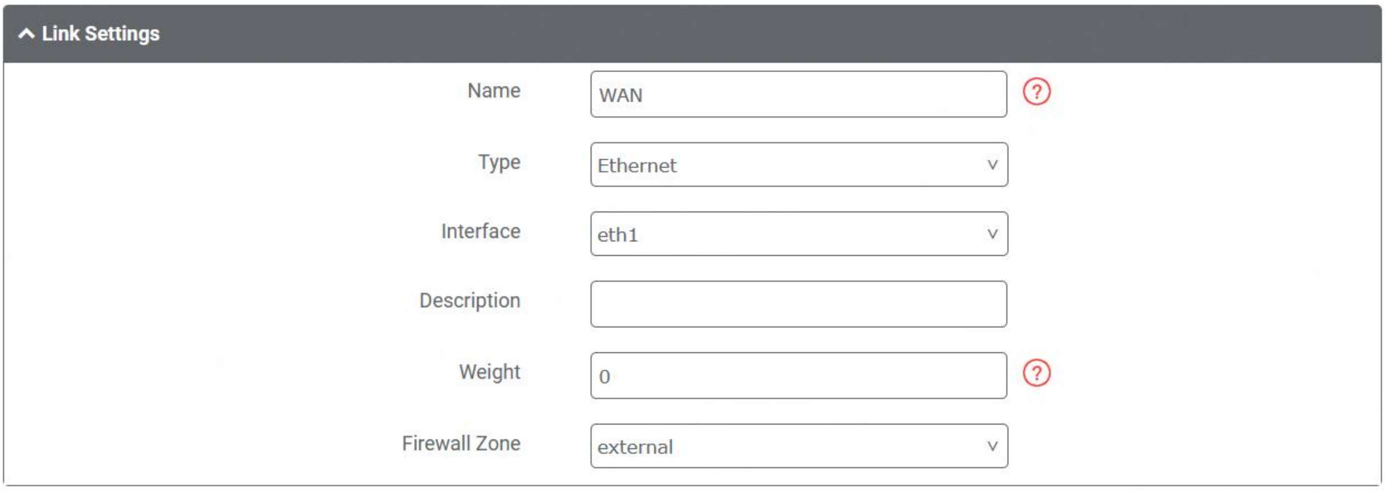
Click ✎ to edit the link.

You can manage link connections in this section. It provides four types of internet connection, including Modem, Ethernet, VLAN and Wi-Fi.



^ Link Settings

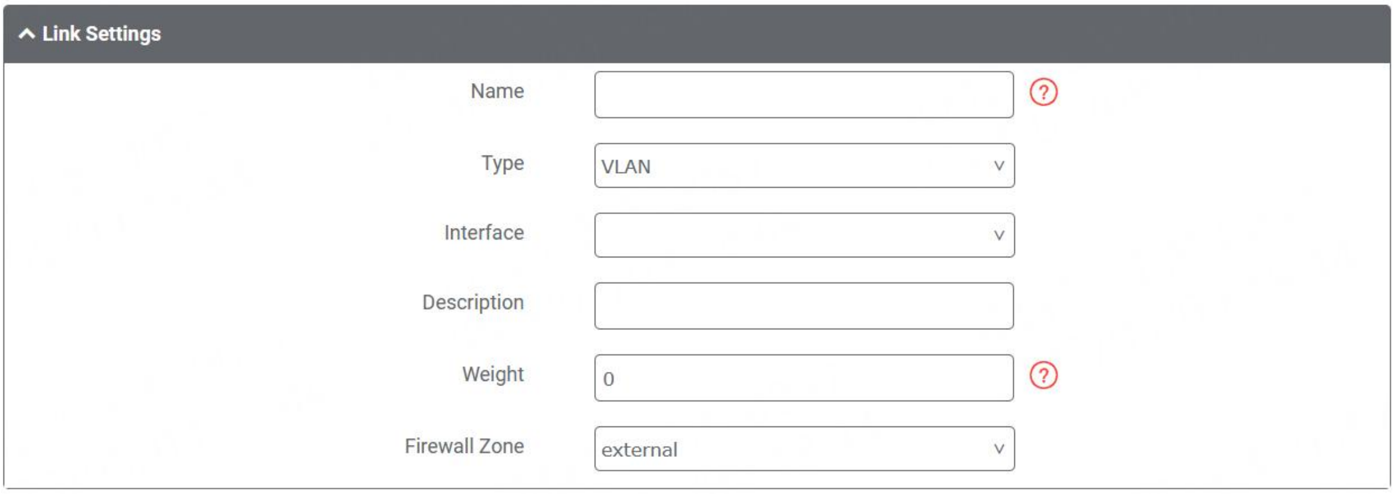
Name	WWAN
Type	Modem
Interface	wwan
Description	default wan
Weight	0
Firewall Zone	external



^ Link Settings

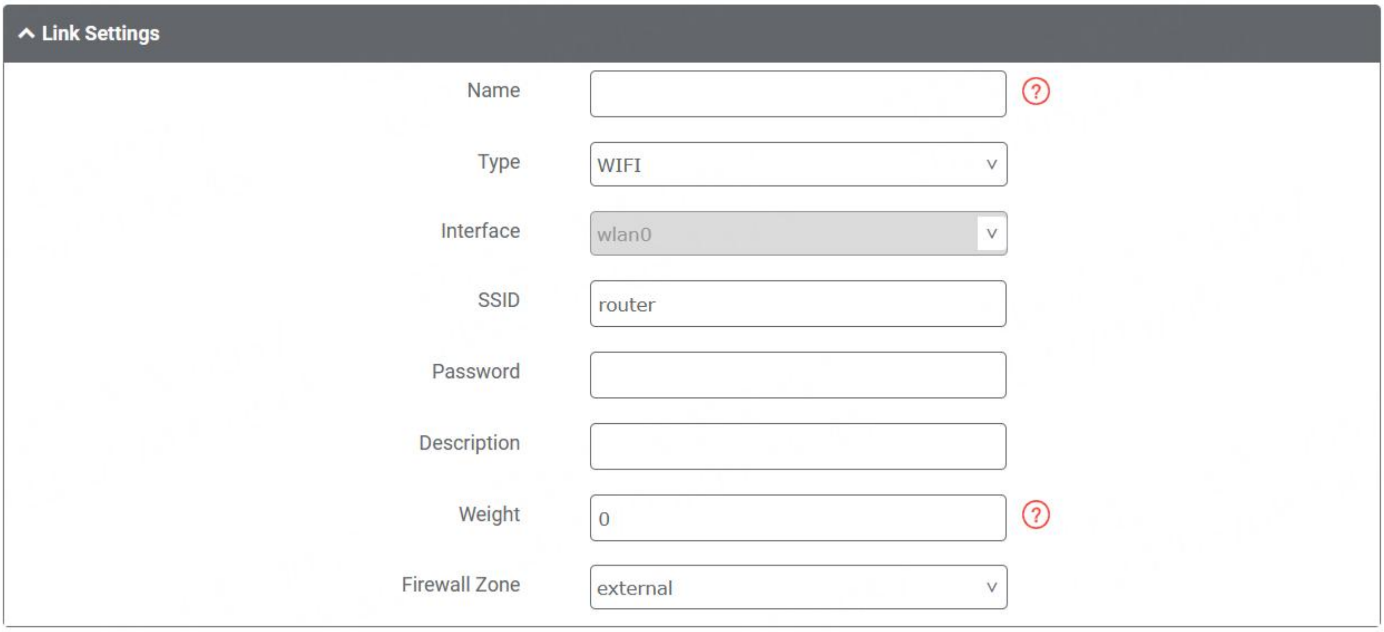
Name	WAN
Type	Ethernet
Interface	eth1
Description	
Weight	0
Firewall Zone	external

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



^ Link Settings

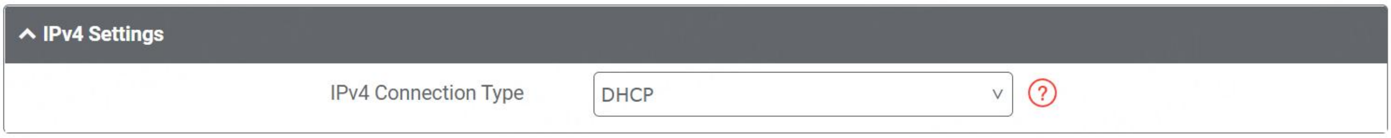
Name	
Type	VLAN
Interface	
Description	
Weight	0
Firewall Zone	external



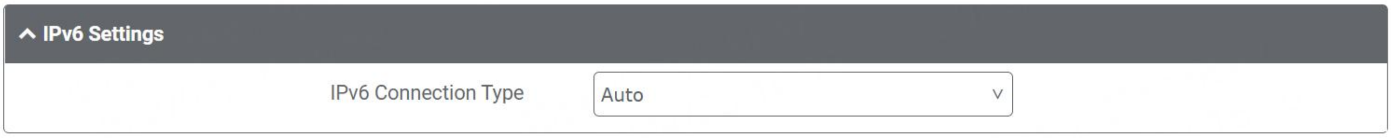
Link Settings	
Name	
Type	WIFI
Interface	wlan0
SSID	router
Password	
Description	
Weight	0
Firewall Zone	external

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

Item	Description	Default
Name	The name of link.	--
Type	Connection Type: • Modem: connect via cellular network. • Ethernet: connect via wired Ethernet network. • VLAN: connect via VLAN network. • Wi-Fi: connect via wireless network.	--
Interface	Set the related interface. If the type is Modem, please see the **3.3.2 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. If the type is Wi-Fi, refer to 3.2.4 Wi-Fi.	--
Description	The description of the link.	--
SSID	The name of Wi-Fi network.	router
Password	The Password of Wi-Fi network.	--
Weight	The weight of this link among all links. 0 means not involved.	0
Firewall Zone	The chosen set of firewall rules, please see the 3.4.5 Firewall.	external

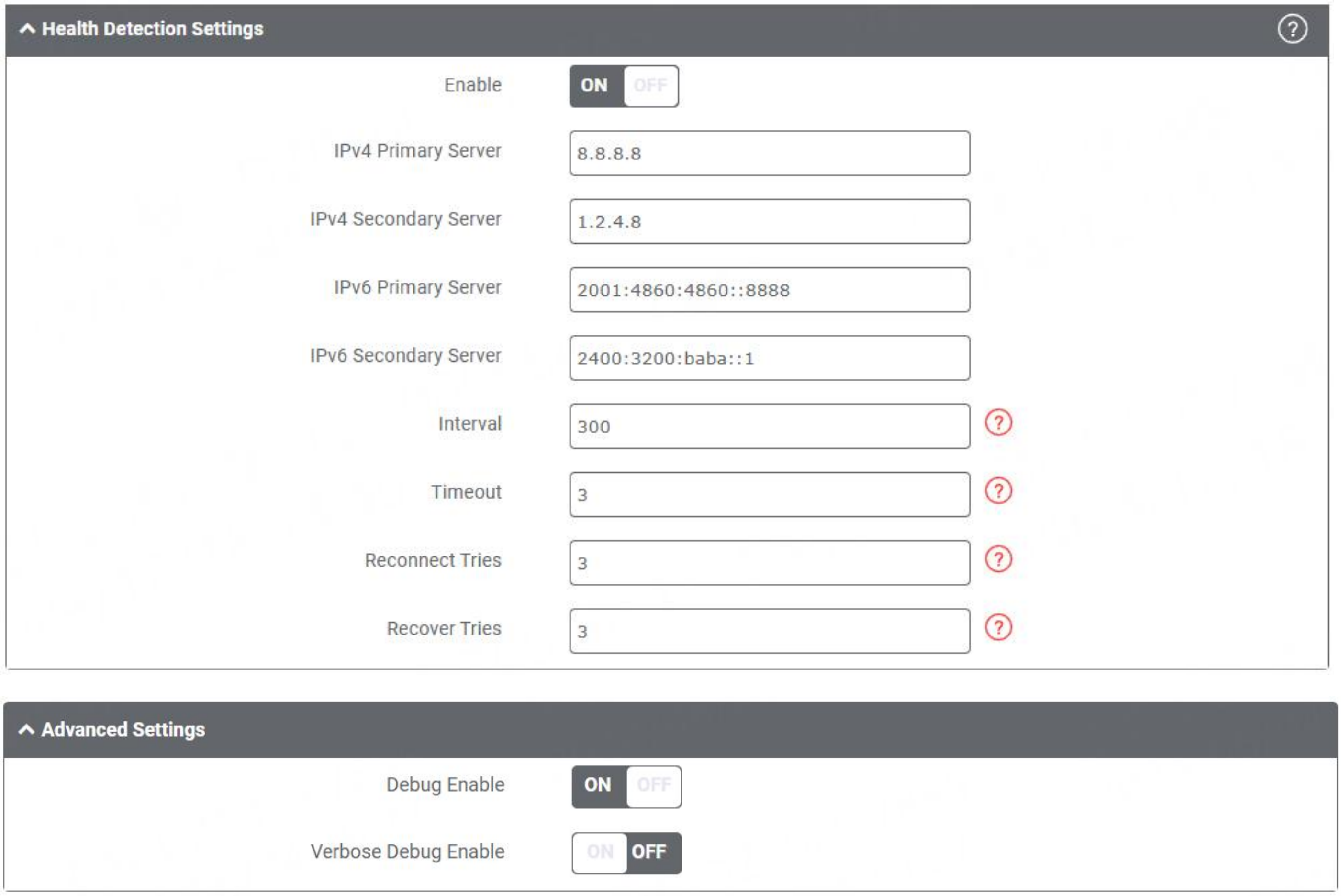


IPv4 Settings	
IPv4 Connection Type	DHCP



IPv6 Settings	
IPv6 Connection Type	Auto

Item	Description	Default
IPv4 Connection Type	The type of IPv4 connection. • DHCP. • PPPoE. • Manual. • Disable. Select the appropriate type. **Note:** PPPoE-based IPv6 is not currently supported, so if PPPoE is selected here, please disable IPv6.	DHCP
IPv6 Connection Type	The type of IPv6 connection. • Auto. • Manual. • Disable. Select the appropriate type.	Auto


Health Detection Settings

Enable: ON

IPv4 Primary Server: 8.8.8.8

IPv4 Secondary Server: 1.2.4.8

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

IPv6 Secondary Server: 2400:3200:baba::1

Interval: 300

Timeout: 3

Reconnect Tries: 3

Recover Tries: 3

Advanced Settings

Debug Enable: ON

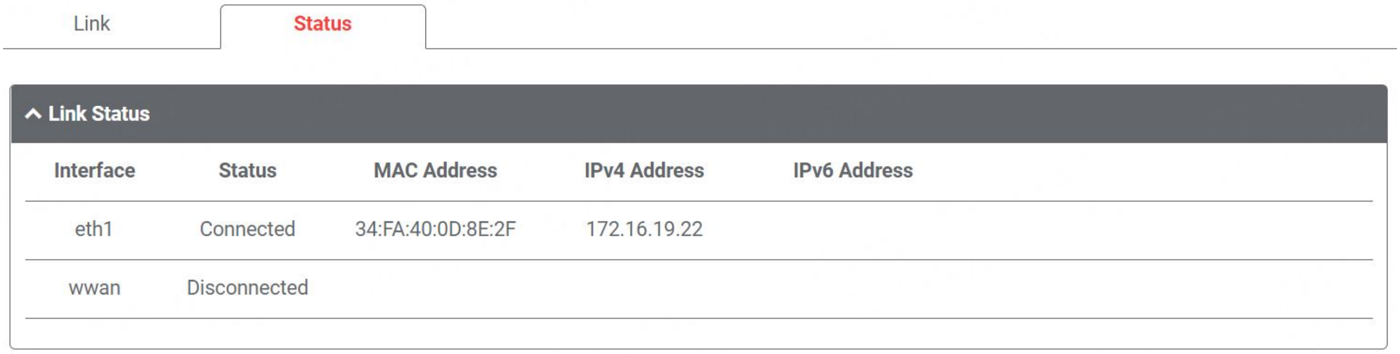
Verbose Debug Enable: OFF

Item	Description	Default
Enable	Click the toggle button to enable/disable the Ping detection mechanism.	ON
IPv4 Primary Server	The gateway pings the primary IPv4 address/domain name to check if the current network connection is functioning properly.	8.8.8.8
IPv4 Secondary Server	The gateway pings the secondary IPv4 address/domain name to check if the current network connection is functioning properly.	114.114.114.114

Item	Description	Default
IPv6 Primary Server	The gateway pings the primary IPv6 address/domain name to check if the current network connection is functioning properly.	2001:4860:4860::8888
IPv6 Secondary Server	The gateway pings the secondary IPv6 address/domain name to check if the current network connection is functioning properly.	2400:3200:baba::1
Interval	Set the interval time for the Ping.	30
Timeout	Set the timeout duration for the Ping.	3
Reconnect Tries	Attempt to reconnect this link in the event of consecutive failed pings.	3
Recover Tries	Restore this link in the event of consecutive successful pings.	3
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable Debug Mode. You can check the information in Syslog.	ON
Verbose Debug Enable	Click the toggle button to enable/disable Debug Mode. You can check the verbose information in Syslog.	OFF

Status

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



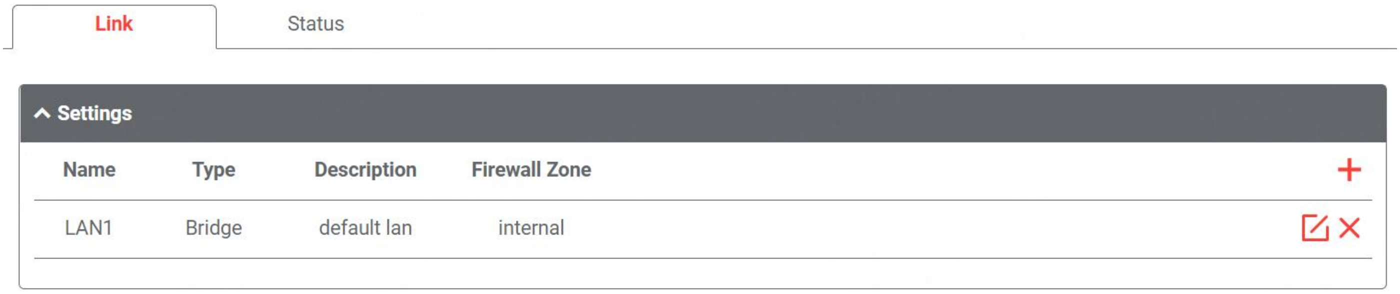
Link Status

Interface	Status	MAC Address	IPv4 Address	IPv6 Address
eth1	Connected	34:FA:40:0D:8E:2F	172.16.19.22	
wwan	Disconnected			

3.4.2 LAN

Local Area Network (LAN) connects network devices (such as Ethernet or bridges) within a logical Layer 2 network. The default link (br_lan) is always available.

Link



Settings

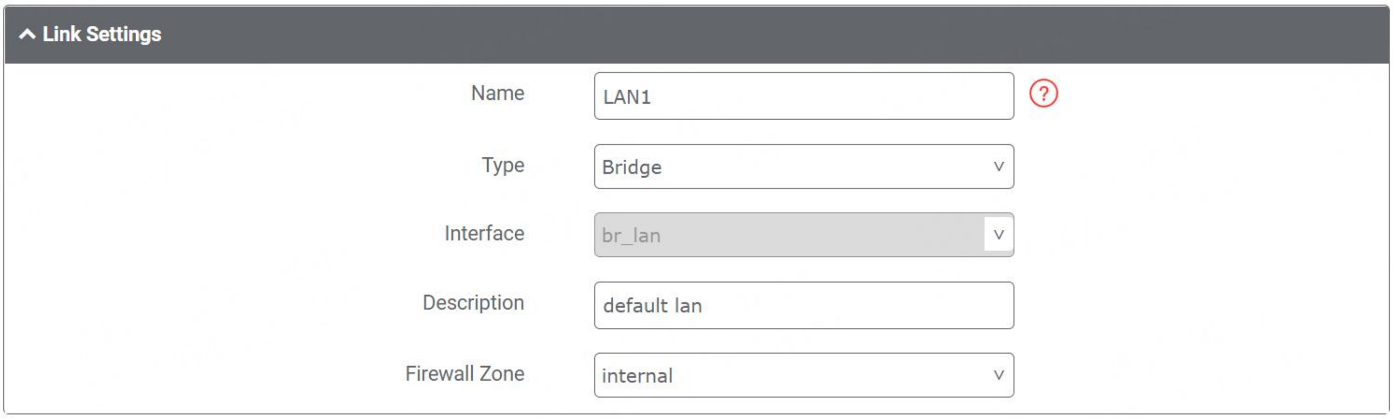
Name	Type	Description	Firewall Zone
LAN1	Bridge	default lan	internal

Click + to add a new LAN link.

Click ✕ to delete the LAN link.

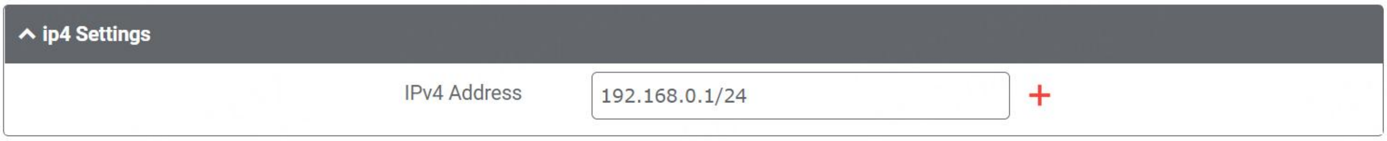
Click ☑ to edit the LAN link.

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



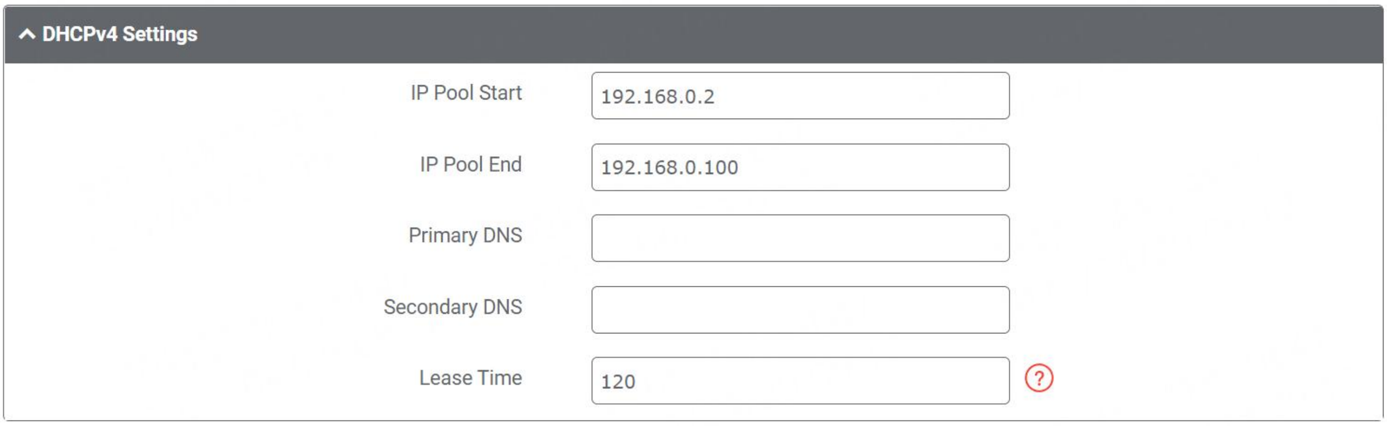
Name	LAN1
Type	Bridge
Interface	br_lan
Description	default lan
Firewall Zone	internal

Item	Description	Default
Name	The name of the LAN link.	Null
Type	Connection type. Select from "Bridge", "Ethernet" and "VLAN". • Bridge: connect via Bridge network. • Ethernet: connect via wired Ethernet network. • VLAN: connect via VLAN network.	Bridge
Interface	Set the relevant interfaces. 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.	Null
Firewall Zone	The chosen set of firewall rules, please see the 3.4.5 Firewall.	internal



^ ip4 Settings

IPv4 Address: 192.168.0.1/24 +



^ DHCPv4 Settings

IP Pool Start: 192.168.0.2

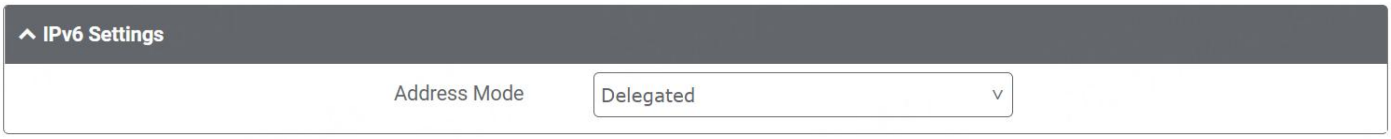
IP Pool End: 192.168.0.100

Primary DNS:

Secondary DNS:

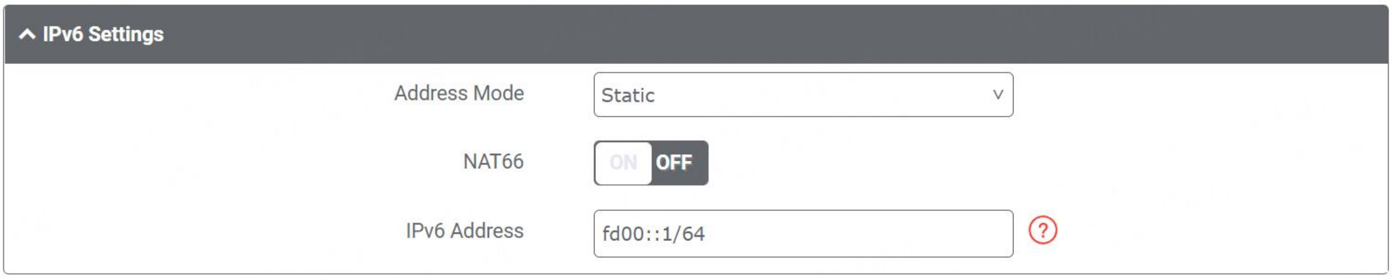
Lease Time: 120 ?

Item	Description	Default
IPv4 Address	Enter the LAN address. The format is "IP/Mask," for example, 192.168.0.1/24.	192.168.0.1/24
IP Pool Start	Define the start of the IP address pool to be assigned to DHCP clients.	192.168.0.2
IP Pool End	Define the end of the IP address pool to be assigned to DHCP clients.	192.168.0.100
Primary DNS	Define the primary DNS server assigned by the DHCP server to clients.	Null
Secondary DNS	Define the secondary DNS server assigned by the DHCP server to clients.	Null
Lease Time	Set the lease time, in minutes. The lease time refers to the duration for which a dynamic IP address is allocated to a network user.	120



^ IPv6 Settings

Address Mode: Delegated v



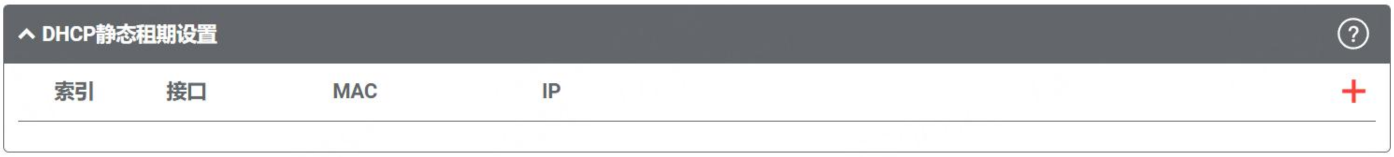
^ IPv6 Settings

Address Mode: Static v

NAT66: ON OFF

IPv6 Address: fd00::1/64 ?

Item	Description	Default
Address Mode	Delegated or Static.	Delegated
NAT66	Enable or disable IPv6 address translation in static mode.	OFF
IPv6 Address	Enter an IPv6 address with a 64-bit network prefix in static mode.	fd00::1/64



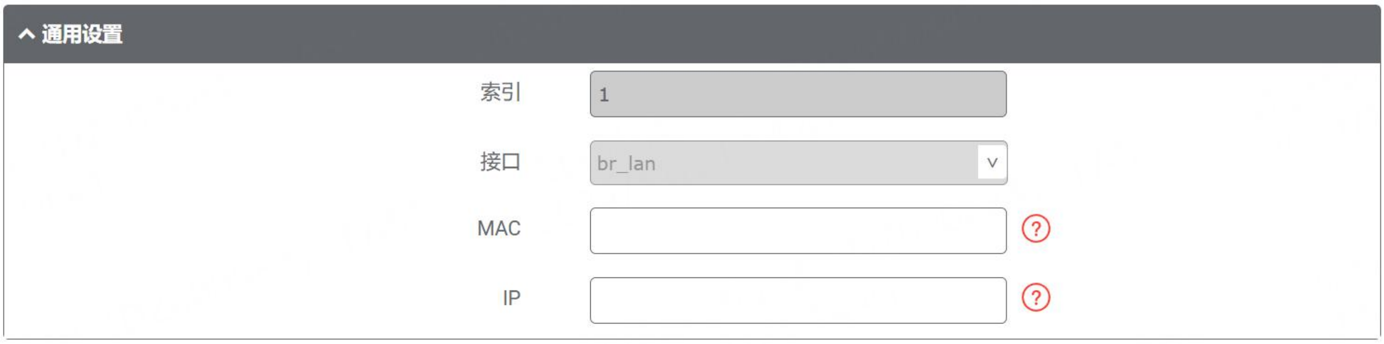
^ DHCP静态租期设置

索引	接口	MAC	IP

Click + to add a new static lease IP for the bound MAC address. A maximum of 50 entries is supported.

Click ✕ to delete the static lease IP for the bound MAC address.

Click ✎ to edit the static lease IP for the bound MAC address.



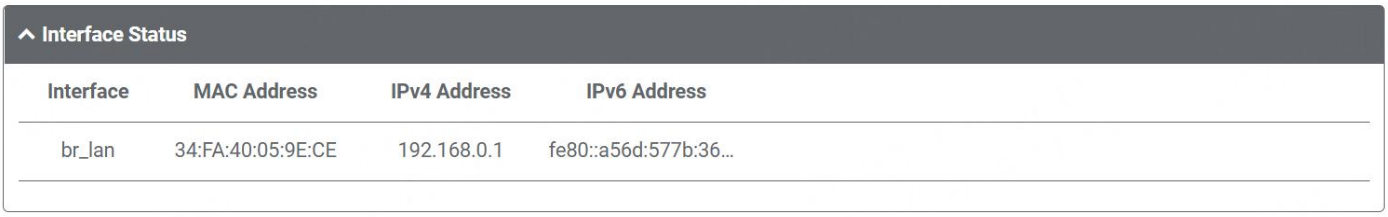
^ 通用设置

索引	1
接口	br_lan
MAC	
IP	

Item	Description	Default
Interface	Select the bound interface.	br_lan
MAC	Set the MAC address for the bound lease IP, for example: FF:ED:CB:A0:98:01.	Null
IP	Set the bound lease IP, for example: 192.168.0.200.	Null

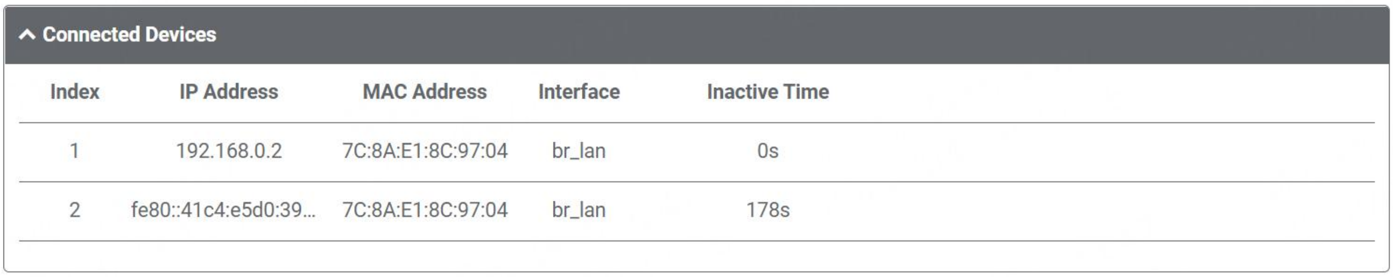
Status

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



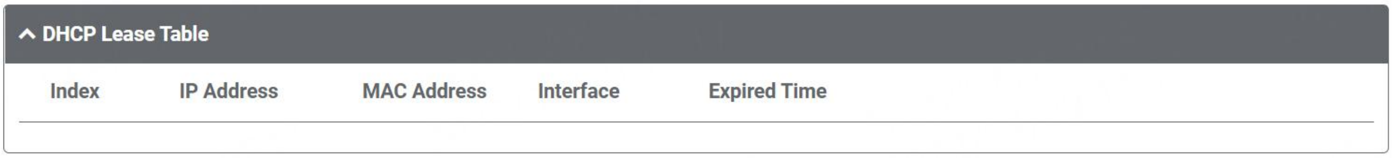
^ Interface Status

Interface	MAC Address	IPv4 Address	IPv6 Address
br_lan	34:FA:40:05:9E:CE	192.168.0.1	fe80::a56d:577b:36...



^ Connected Devices

Index	IP Address	MAC Address	Interface	Inactive Time
1	192.168.0.2	7C:8A:E1:8C:97:04	br_lan	0s
2	fe80::41c4:e5d0:39...	7C:8A:E1:8C:97:04	br_lan	178s



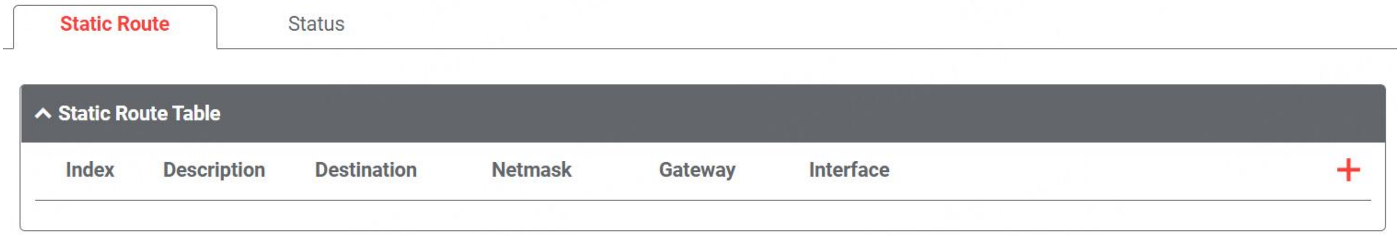
^ DHCP Lease Table

Index	IP Address	MAC Address	Interface	Expired Time

3.4.3 Route

Routes ensure that network traffic can find a path to the target network. Static routes refer to fixed routing entries in the routing table.

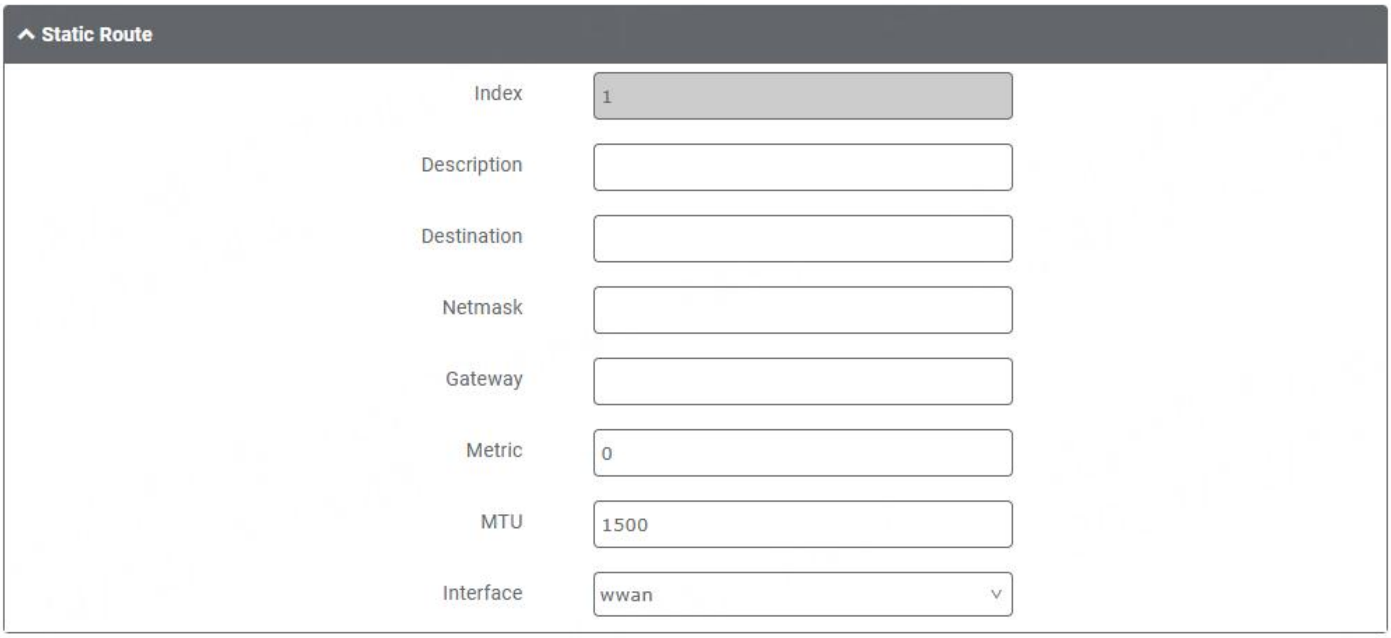
Static Route



^ Static Route Table

Index	Description	Destination	Netmask	Gateway	Interface

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



^ Static Route

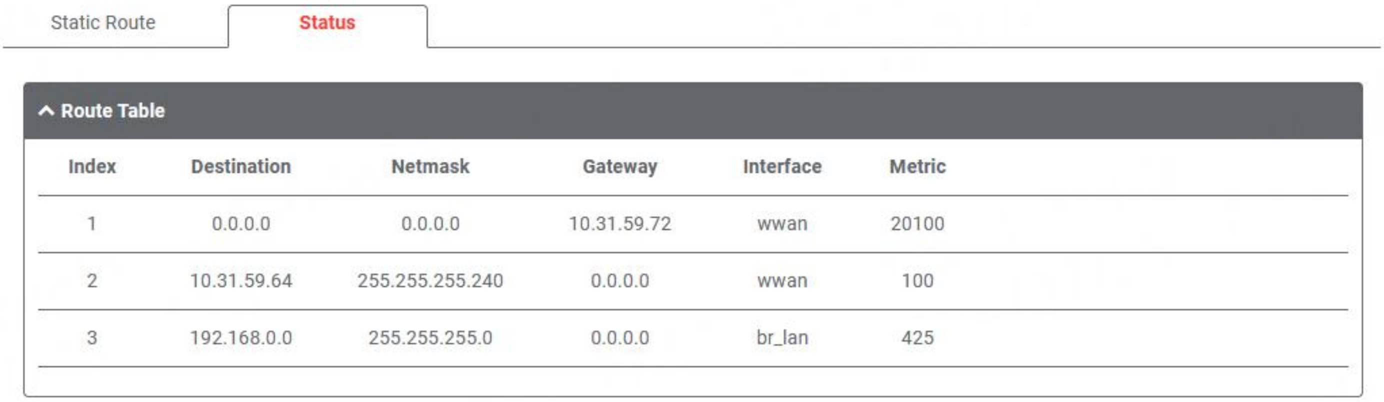
Index	1
Description	
Destination	
Netmask	
Gateway	
Metric	0
MTU	1500
Interface	wwan

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

Item	Description	Default
Metric	Enter the Metric value. Metrics help the gateway choose the best route among multiple feasible routes to a destination. The route will go in the direction of the gateway with the lowest metric value.	0
MTU	Enter the MTU value, 1280~1500.	1500
Interface	Choose the corresponding port of the link that you want to configure.	wwan

Status

This window allows you to view the status of route.

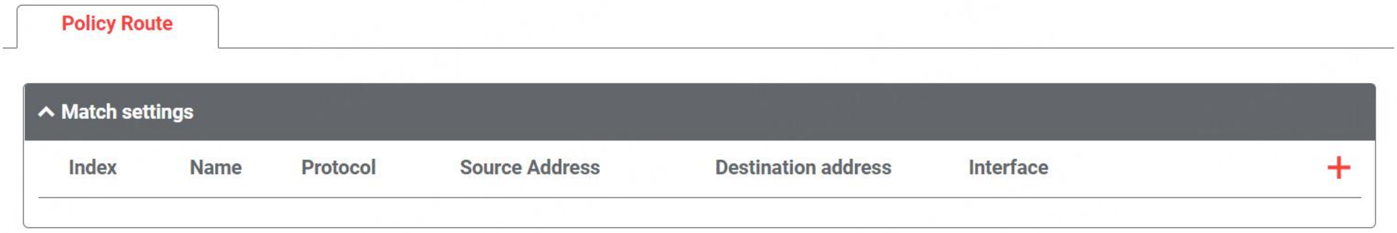


Index	Destination	Netmask	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	10.31.59.72	wwan	20100
2	10.31.59.64	255.255.255.240	0.0.0.0	wwan	100
3	192.168.0.0	255.255.255.0	0.0.0.0	br_lan	425

3.4.4 Policy Route

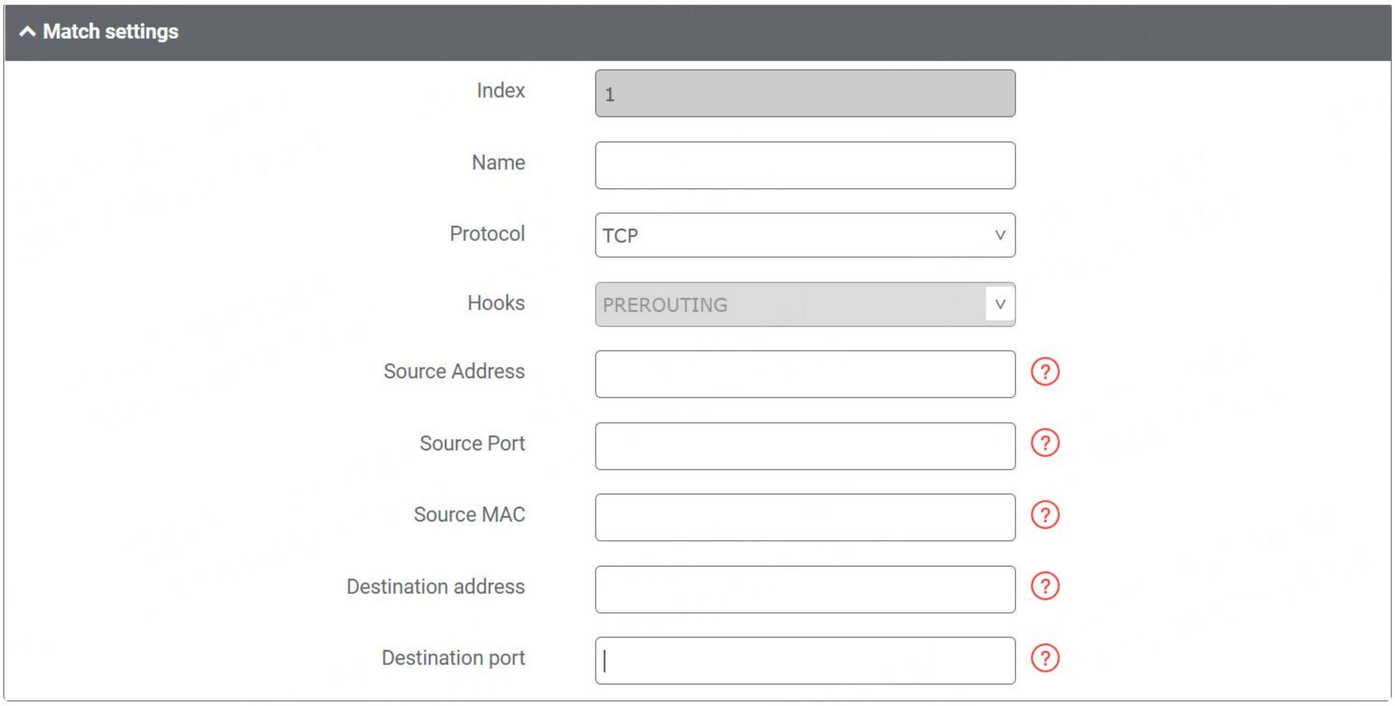
In this window, you can manage the outbound route based on the IP address, port number in the packet.

Policy Route



Index	Name	Protocol	Source Address	Destination address	Interface

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



^ Match settings

Index: 1

Name:

Protocol: TCP

Hooks: PREROUTING

Source Address:

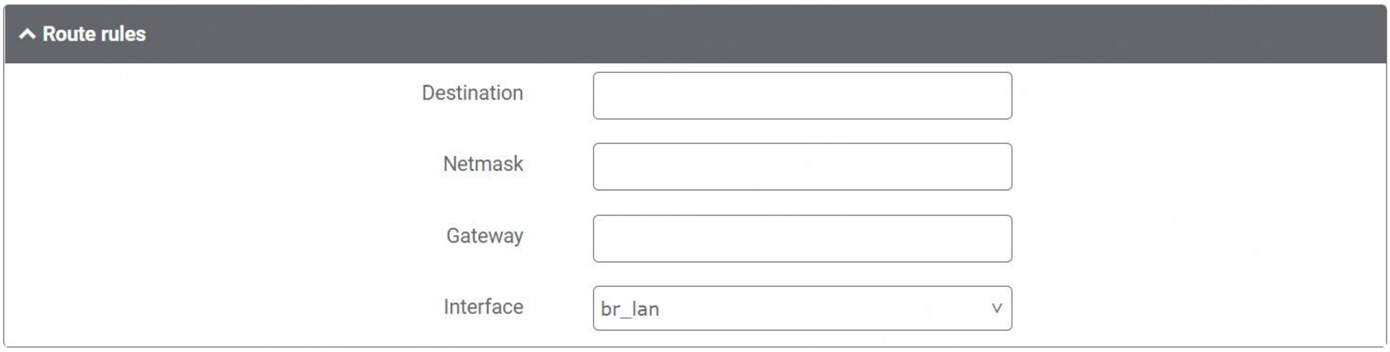
Source Port:

Source MAC:

Destination address:

Destination port:

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



^ Route rules

Destination:

Netmask:

Gateway:

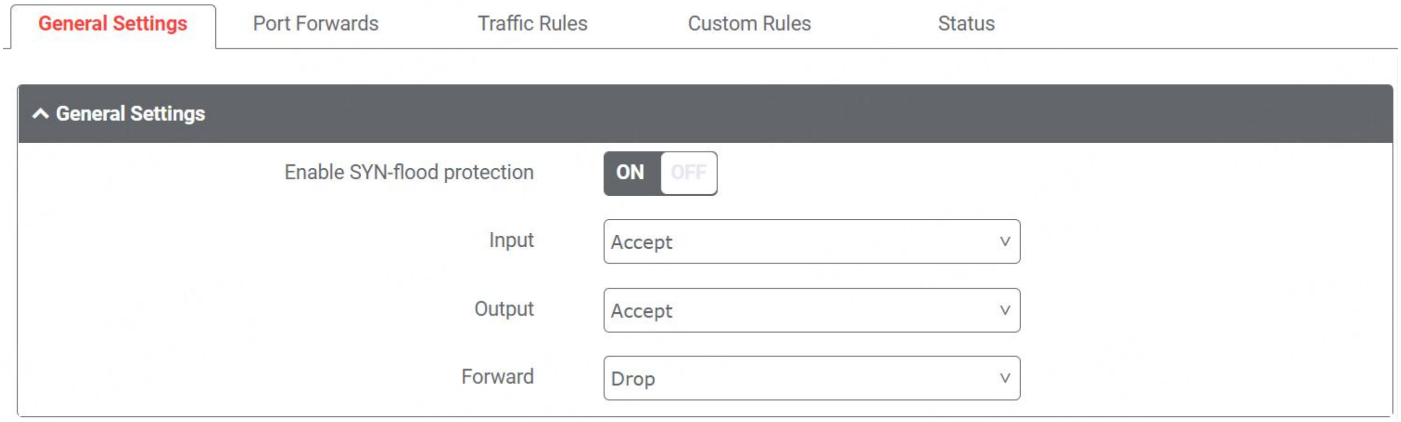
Interface: br_lan

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

3.4.5 Firewall

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

General Setting



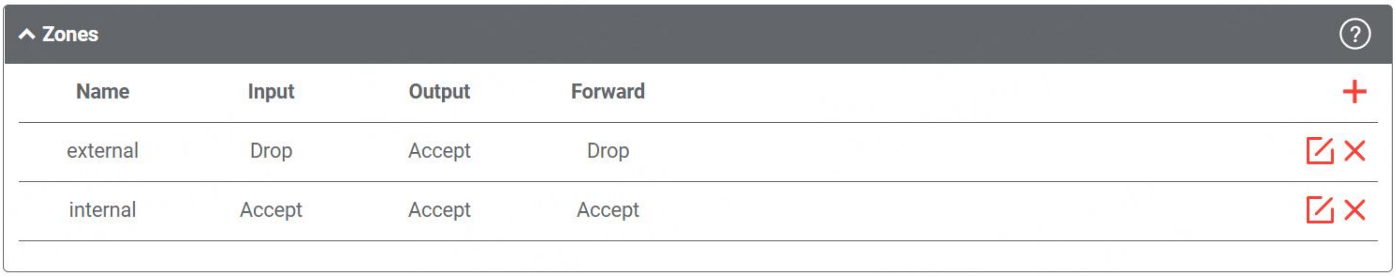
Enable SYN-flood protection: ON

Input: Accept

Output: Accept

Forward: Drop

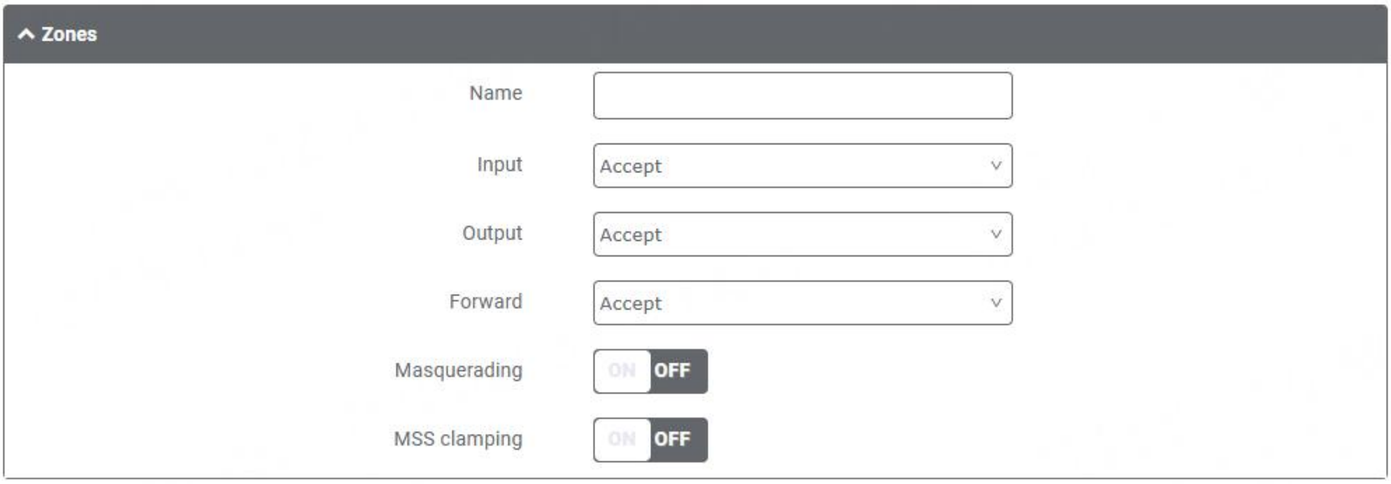
Item	Description	Default
Enable SYN-flood protection	Countermeasures to protect against SYN flood attacks, click the toggle button to enable/disable.	ON
Input	Default action of the Input chain if a packet does not match any exist rule on that chain. • Accept: Packet gets to continue to the next chain. • 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.*		



Name	Input	Output	Forward
external	Drop	Accept	Drop
internal	Accept	Accept	Accept

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**



^ Zones

Name

Input: Accept

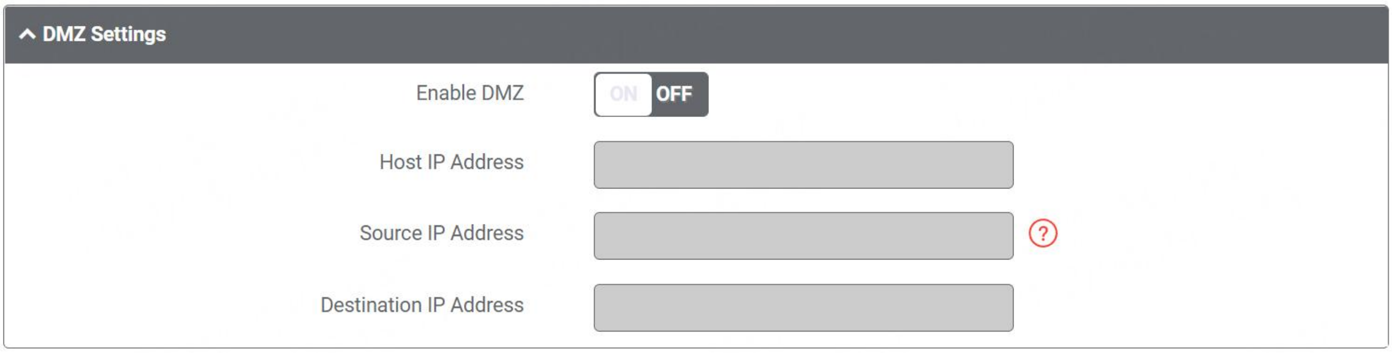
Output: Accept

Forward: Accept

Masquerading: ON OFF

MSS clamping: ON OFF

Item	Description	Default
Name	The name of the firewall zone.	Null
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.	Accept
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).	OFF
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.	OFF



^ DMZ Settings

Enable DMZ: ON OFF

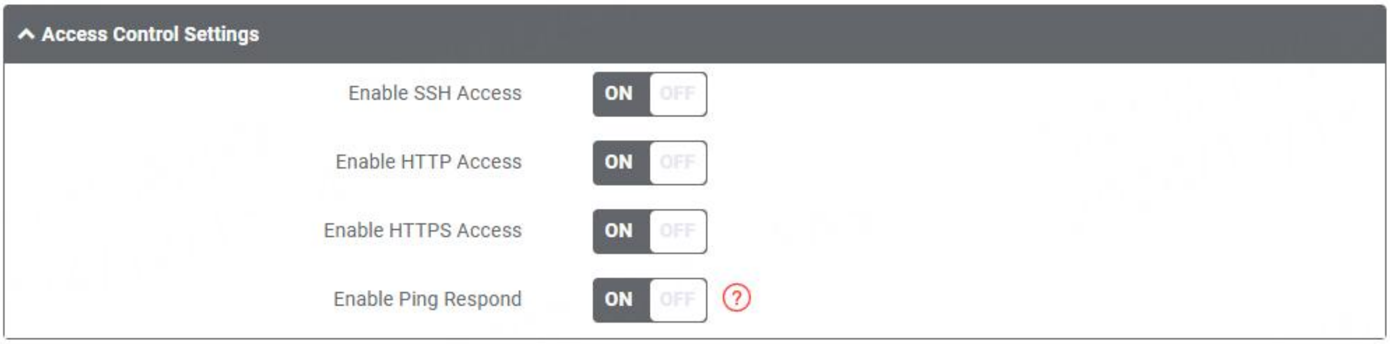
Host IP Address

Source IP Address

Destination IP Address

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



^ Access Control Settings

Enable SSH Access: ON OFF

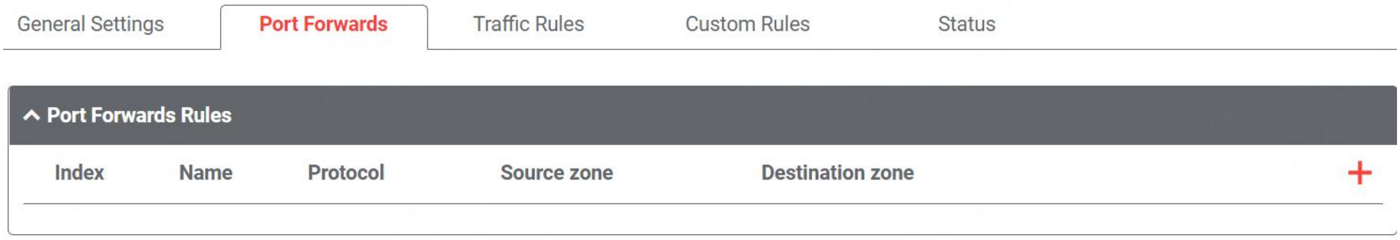
Enable HTTP Access: ON OFF

Enable HTTPS Access: ON OFF

Enable Ping Respond: ON OFF

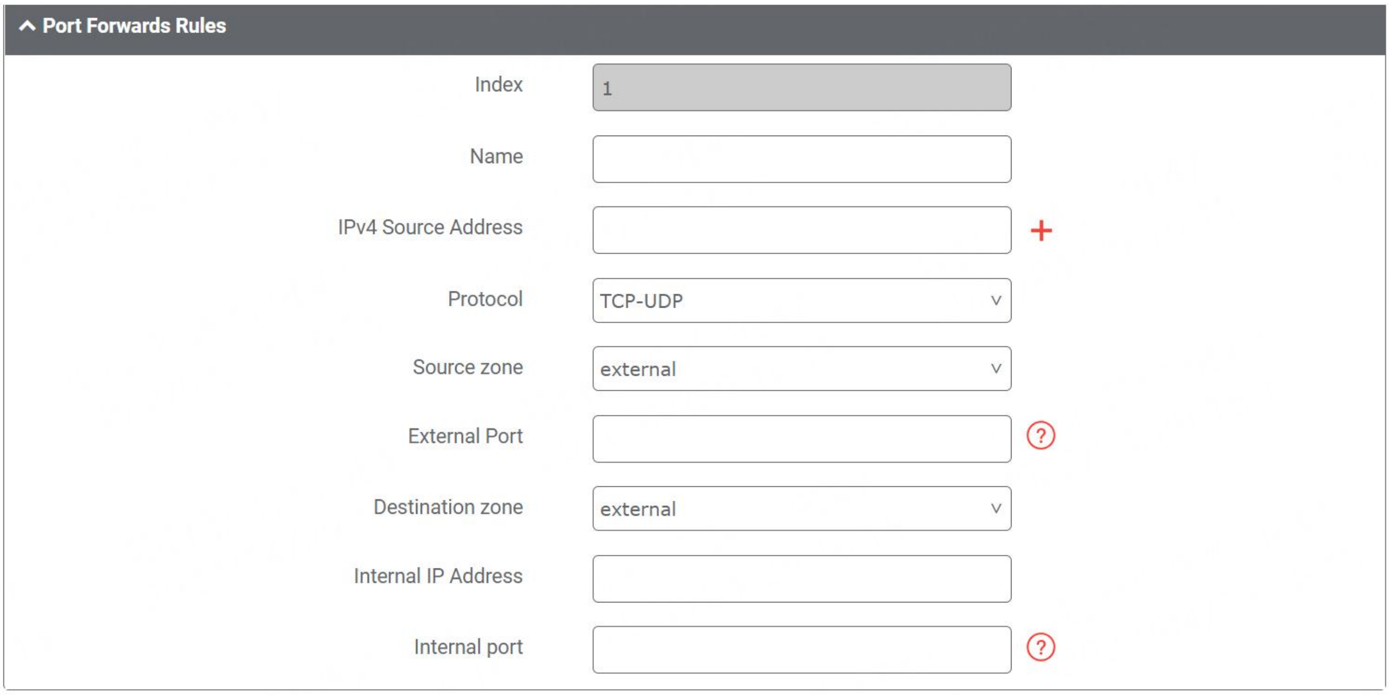
Item	Description	Default
Enable SSH Access	Click the toggle button to enable/disable this option. When enabled, the zone user can access the device via SSH.	ON
Enable HTTP Access	Click the toggle button to enable/disable this option. When enabled, the zone user can access the device via HTTP.	ON
Enable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

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.

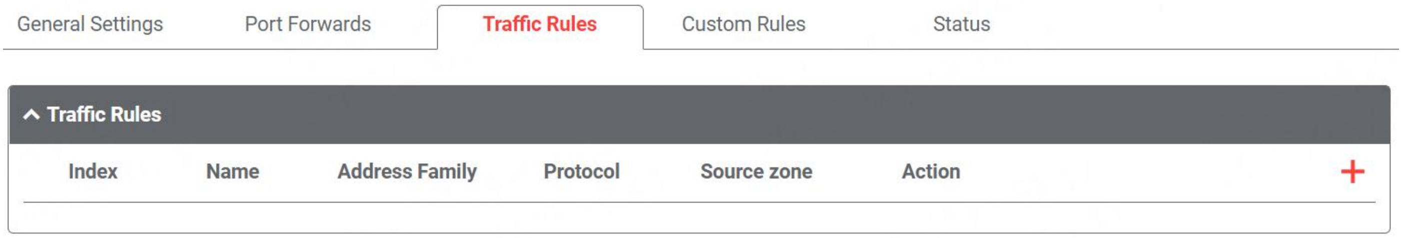
Click + to add one. The maximum count is **50.**



Index	1
Name	
IPv4 Source Address	+
Protocol	TCP-UDP
Source zone	external
External Port	
Destination zone	external
Internal IP Address	
Internal port	

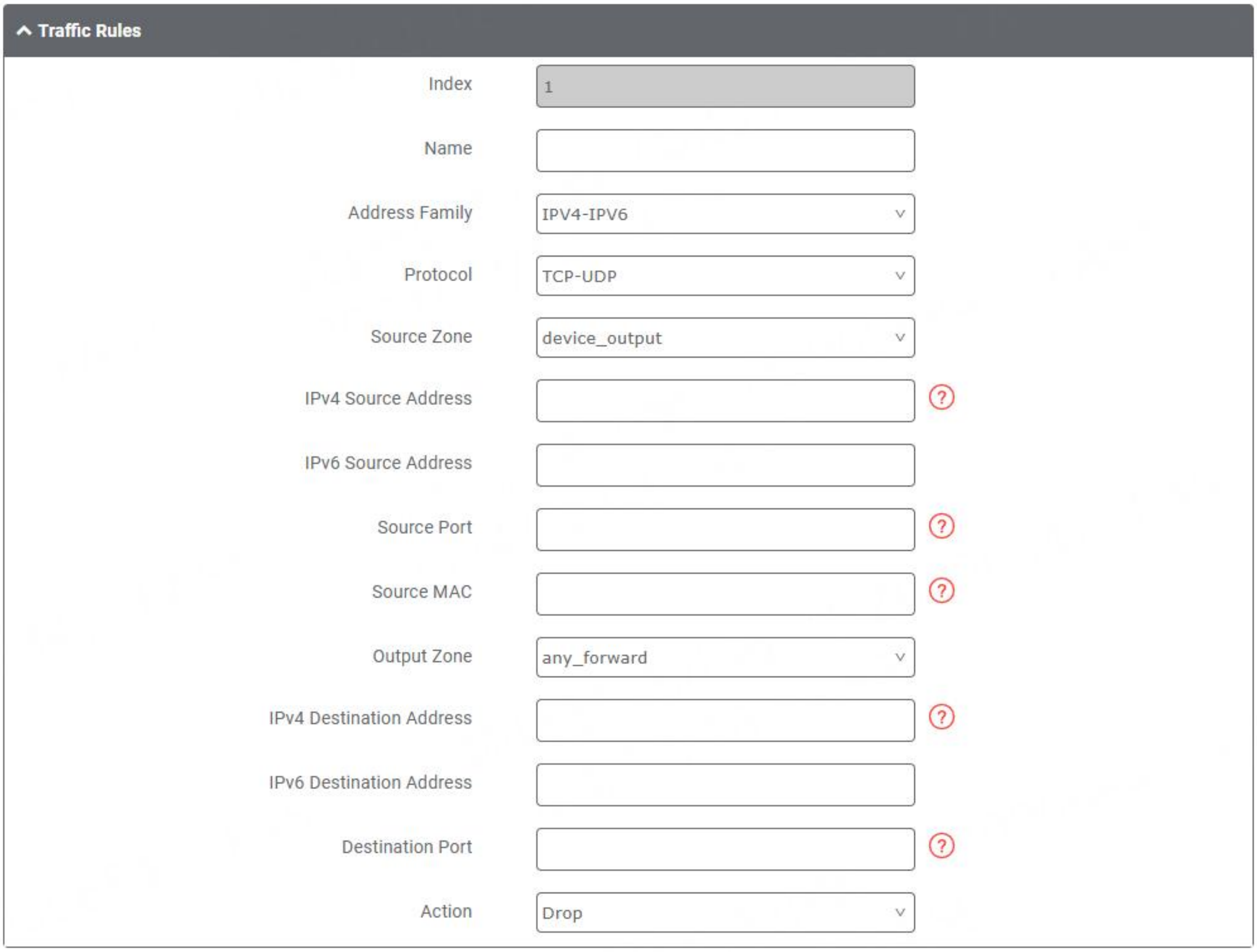
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	Name of the rule.	Null
IPv4 Source Address	IP address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field.	Null
Protocol	Select from "TCP", "UDP" 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.**

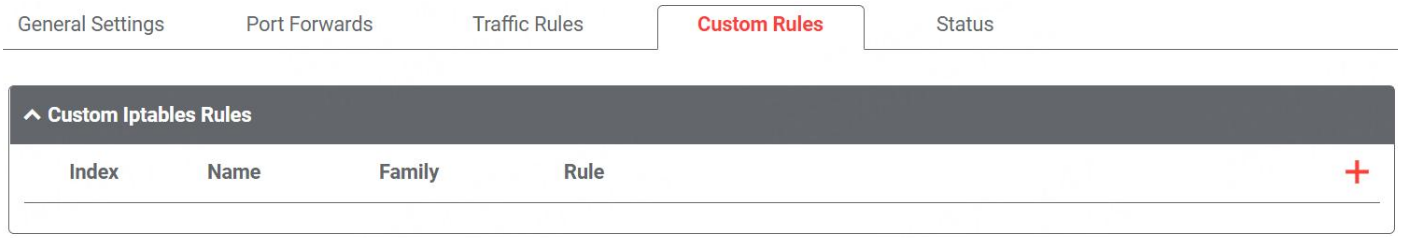


Index	1
Name	
Address Family	IPV4-IPV6
Protocol	TCP-UDP
Source Zone	device_output
IPv4 Source Address	
IPv6 Source Address	
Source Port	
Source MAC	
Output Zone	any_forward
IPv4 Destination Address	
IPv6 Destination Address	
Destination Port	
Action	Drop

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

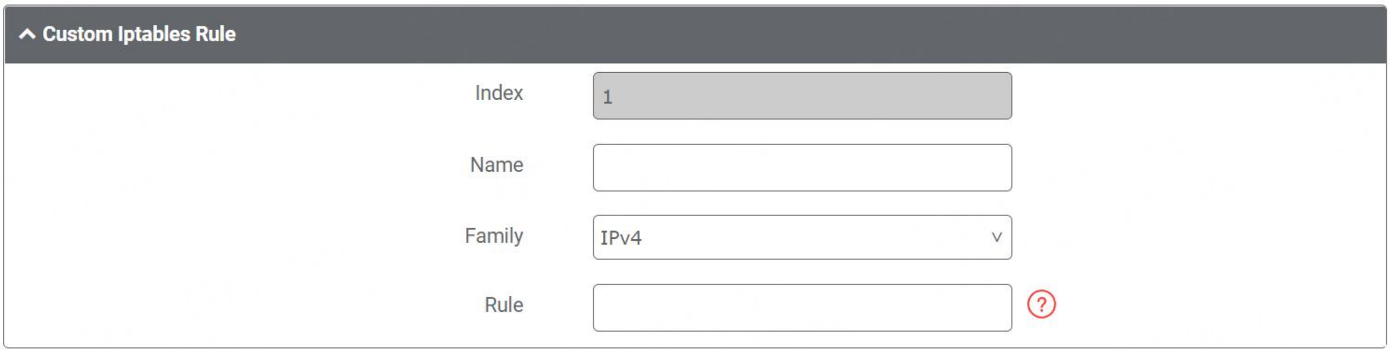
Item	Description	Default
Source zone	The zone to which the third party will be connecting.	device_output
IPv4 Source Address	The IPv4 address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field.	Null
IPv6 Source Address	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.	Drop

Custom Rules



This window allows you to view the custom rules.

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

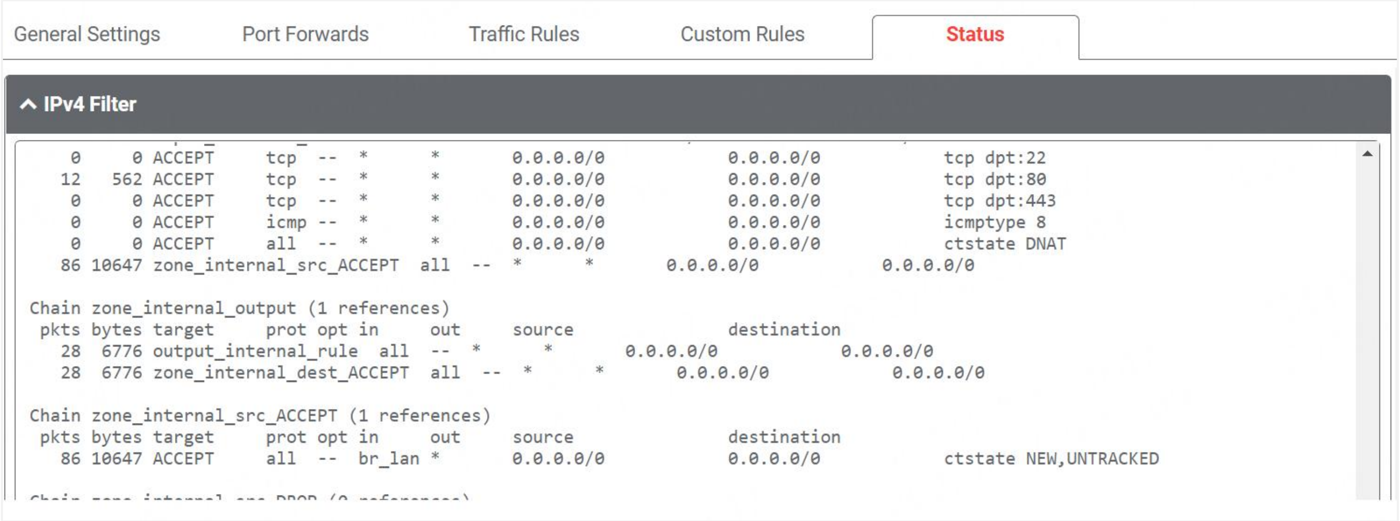


Index	1
Name	
Family	IPv4
Rule	

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.

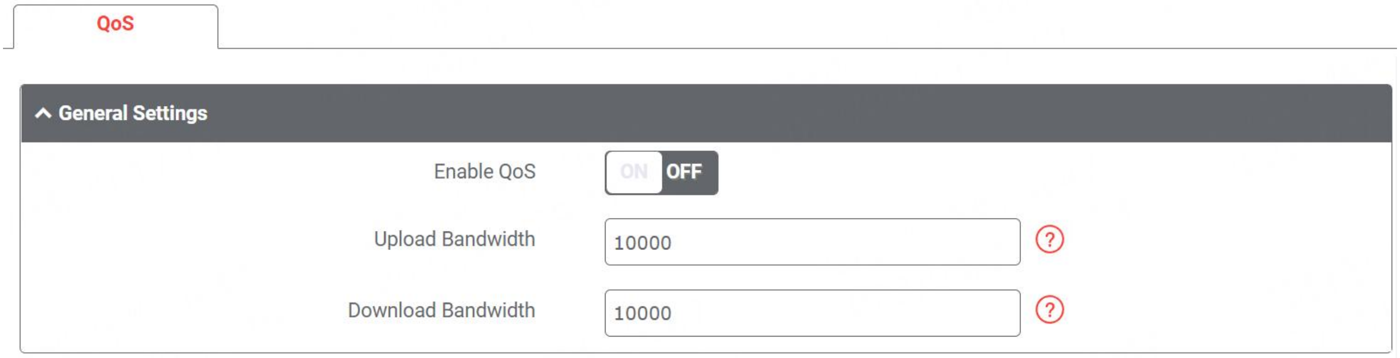


```
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
   12   562 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:443
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0            icmptype 8
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            ctstate DNAT
   86 10647 zone_internal_src_ACCEPT  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain zone_internal_output (1 references)
 pkts bytes target     prot opt in     out     source               destination
   28  6776 output_internal_rule  all  --  *      *       0.0.0.0/0            0.0.0.0/0
   28  6776 zone_internal_dest_ACCEPT  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain zone_internal_src_ACCEPT (1 references)
 pkts bytes target     prot opt in     out     source               destination
   86 10647 ACCEPT     all  --  br_lan *       0.0.0.0/0            0.0.0.0/0            ctstate NEW,UNTRACKED

Chain zone_internal_src_DROP (0 references)
```

3.4.6 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



Enable QoS: OFF

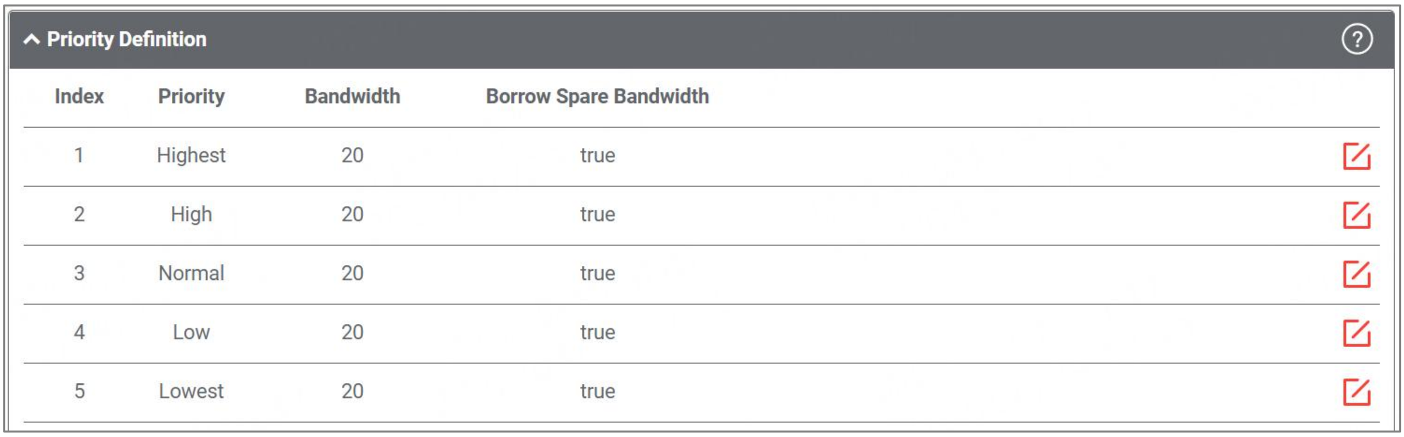
Upload Bandwidth: 10000

Download Bandwidth: 10000

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

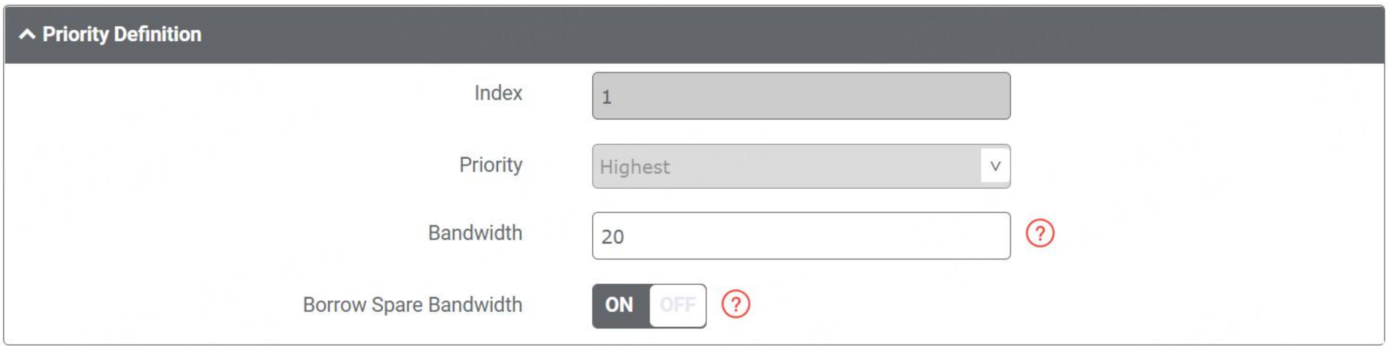
Priority Definition



Priority Definition

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

Click to set the priority.

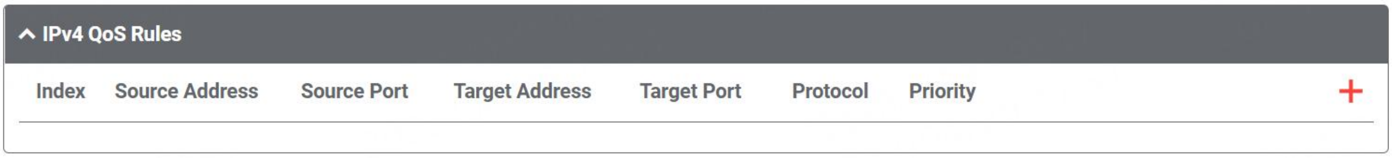


Priority Definition

Index	1
Priority	Highest
Bandwidth	20
Borrow Spare Bandwidth	ON OFF

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

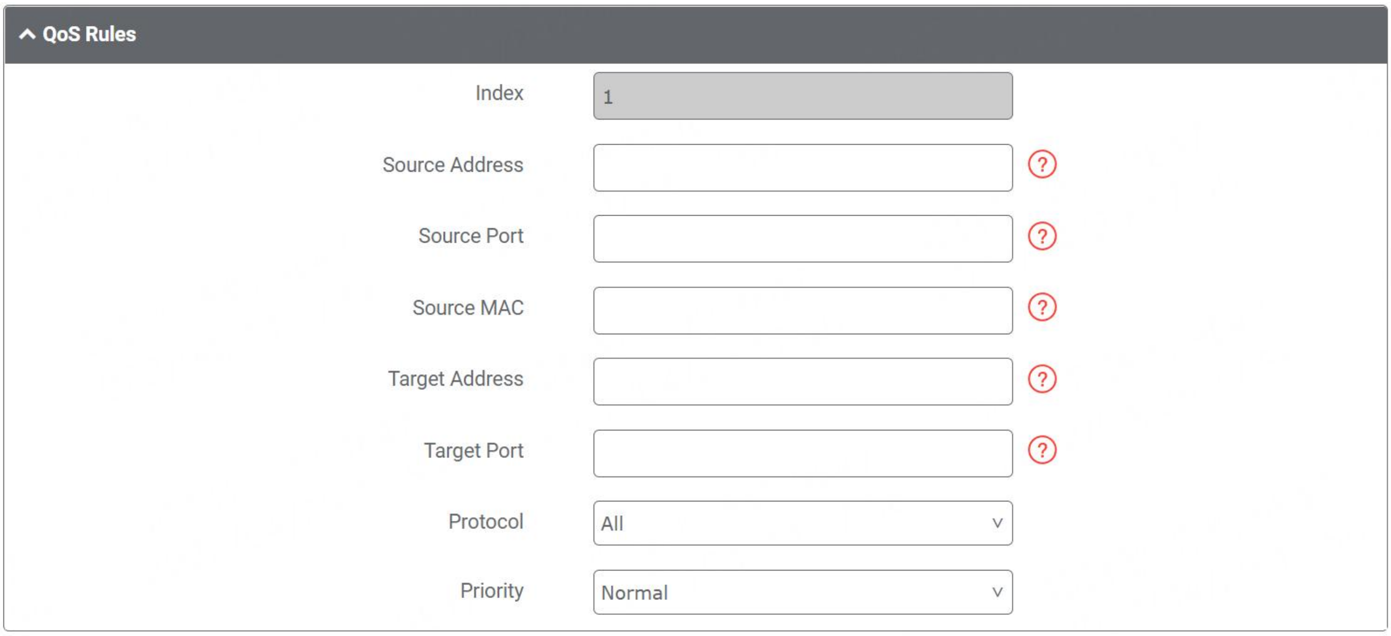
IPv4 QoS Rules



IPv4 QoS Rules

Index	Source Address	Source Port	Target Address	Target Port	Protocol	Priority

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

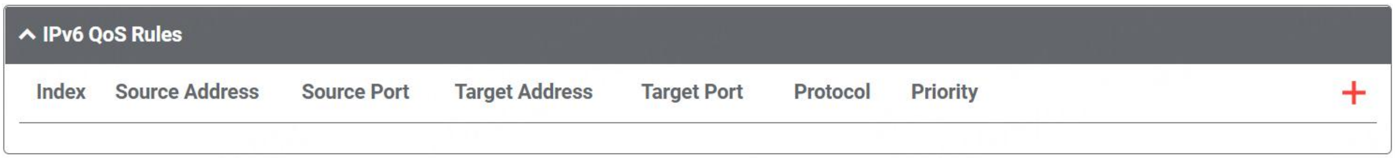


QoS Rules

Index	1
Source Address	
Source Port	
Source MAC	
Target Address	
Target Port	
Protocol	All
Priority	Normal

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

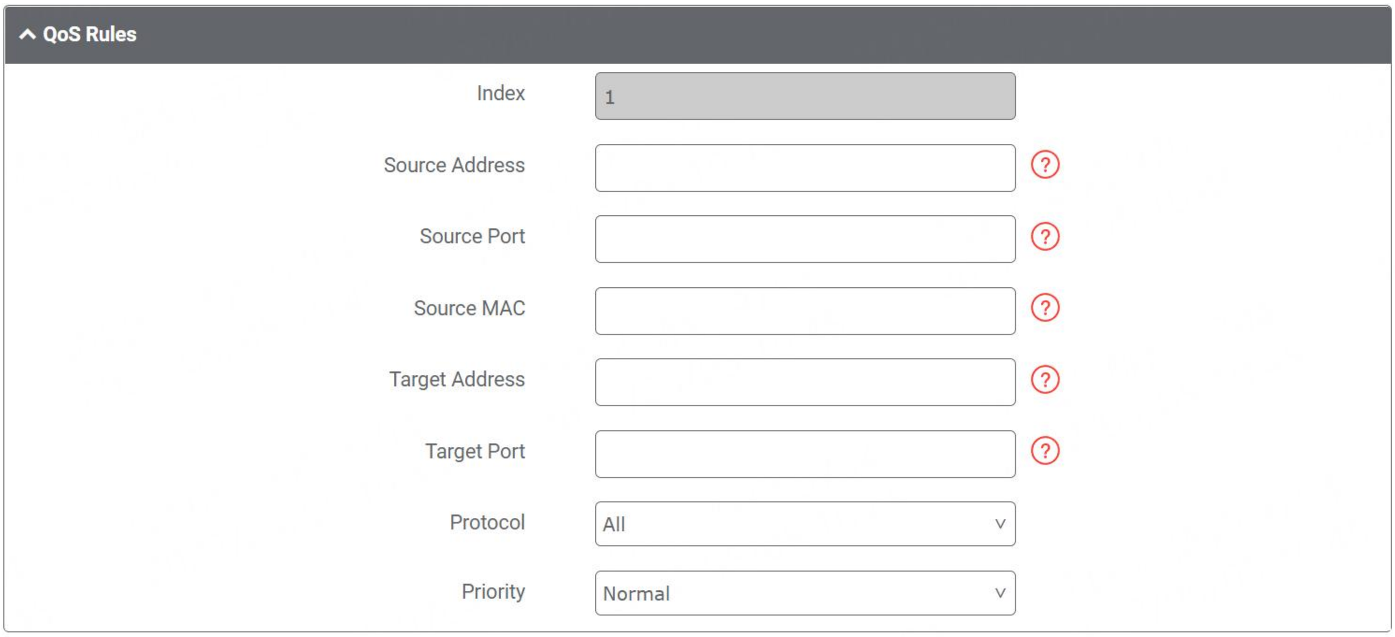
IPv6 QoS Rules



IPv6 QoS Rules

Index	Source Address	Source Port	Target Address	Target Port	Protocol	Priority

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



QoS Rules

Index	1
Source Address	
Source Port	
Source MAC	
Target Address	
Target Port	
Protocol	All
Priority	Normal

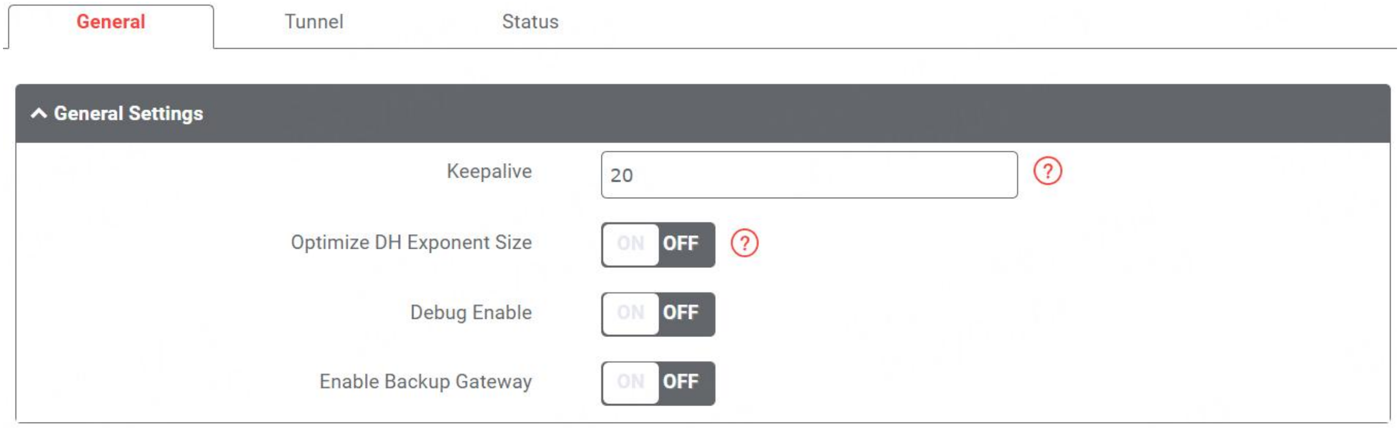
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Source Address	The address of Host(s) from which data will be transmitted.	Null
Source Port	The port of Host(s) from which data will be transmitted.	Null
Source MAC	The MAC address of Host(s) from which data will be transmitted.	Null
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

3.5 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



Keepalive: 20

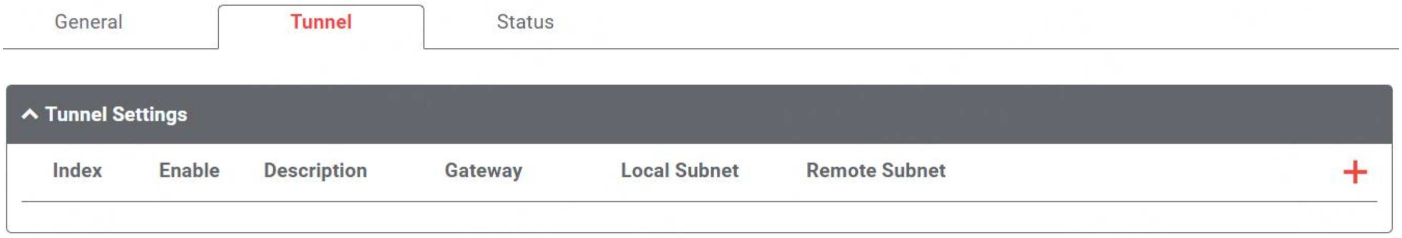
Optimize DH Exponent Size: ON OFF

Debug Enable: ON OFF

Enable Backup Gateway: ON OFF

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

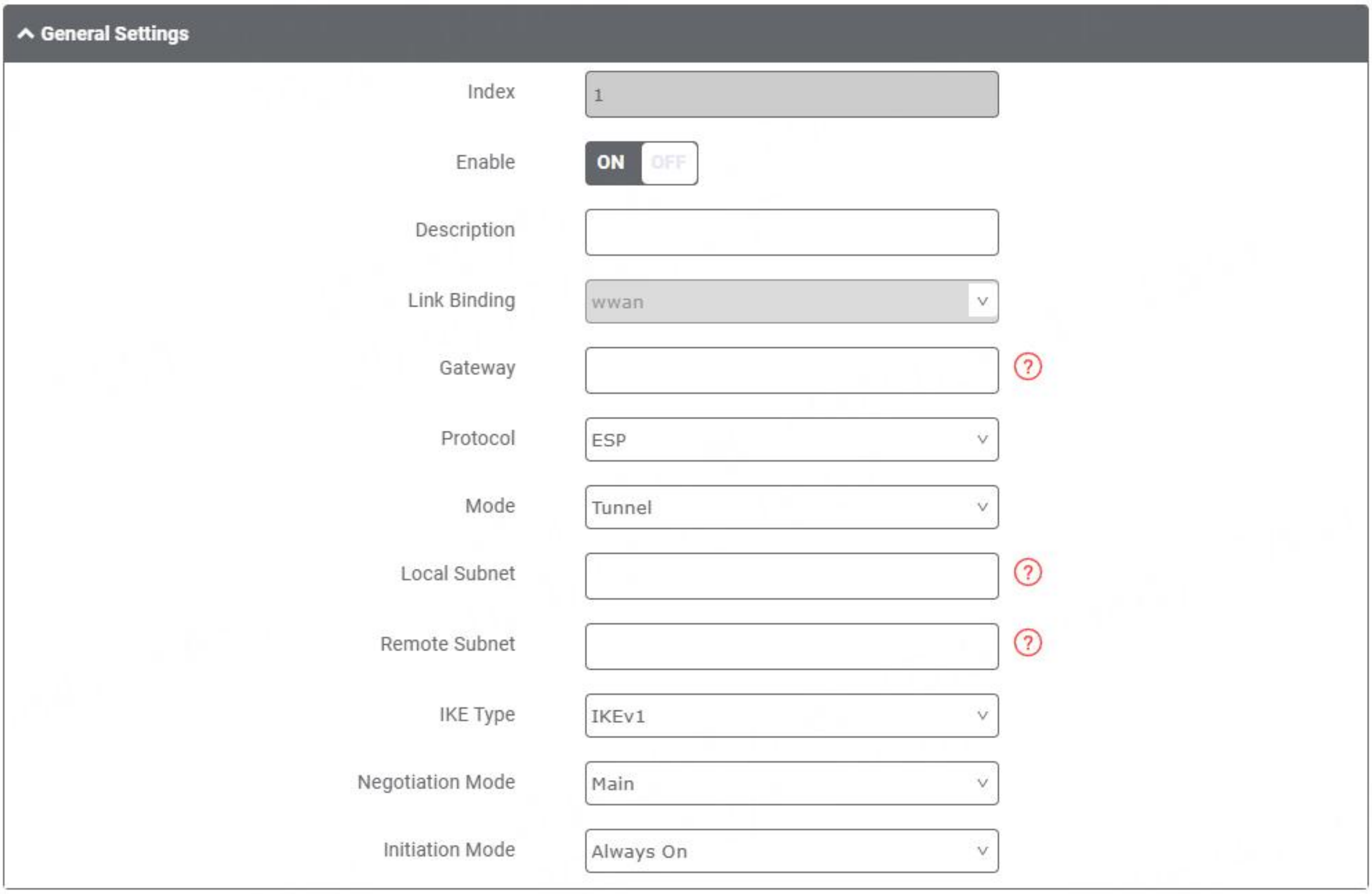
Tunnel



Index	Enable	Description	Gateway	Local Subnet	Remote Subnet

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

General Setting



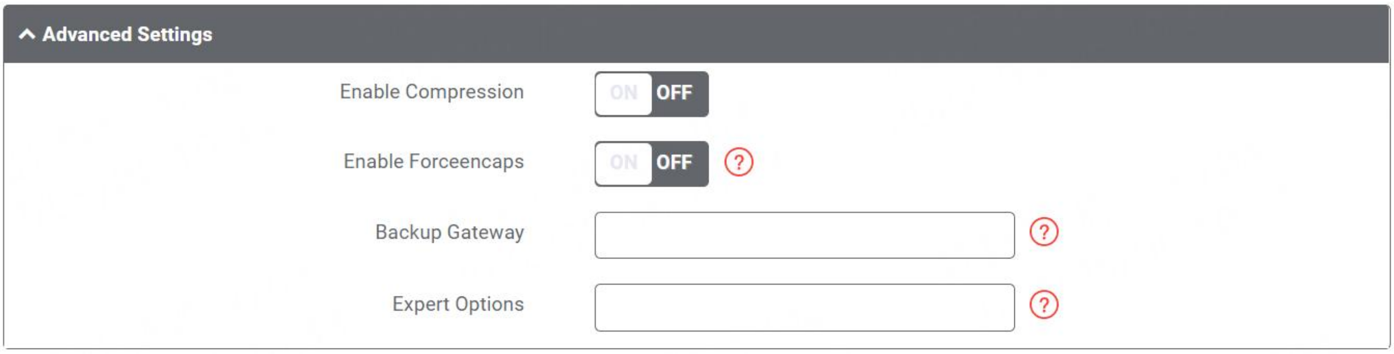
General Settings

Index	1
Enable	ON OFF
Description	
Link Binding	wwan
Gateway	
Protocol	ESP
Mode	Tunnel
Local Subnet	
Remote Subnet	
IKE Type	IKEv1
Negotiation Mode	Main
Initiation Mode	Always On

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.	wwan
Protocol	Select the security protocols from “ESP” and “AH”. • ESP: Use the ESP protocol • AH: Use the AH protocol	ESP
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

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


Advanced Settings

Enable Compression: ON OFF

Enable Forceencaps: ON OFF

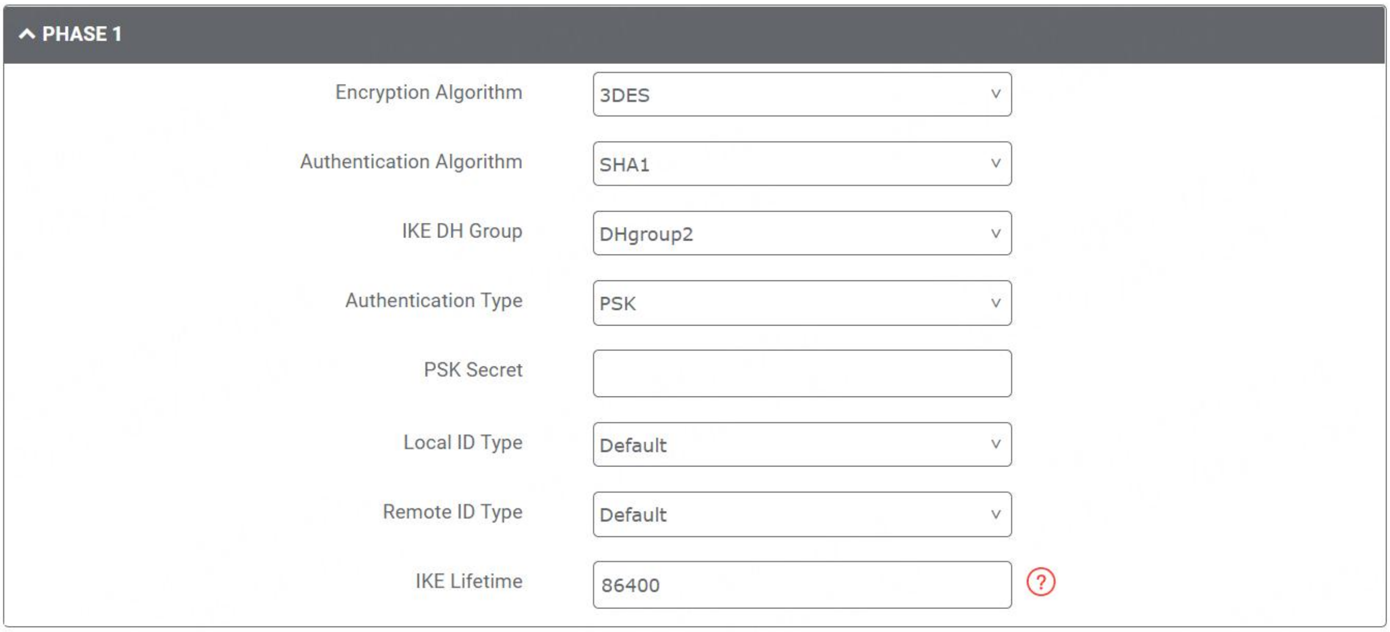
Backup Gateway:

Expert Options:

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

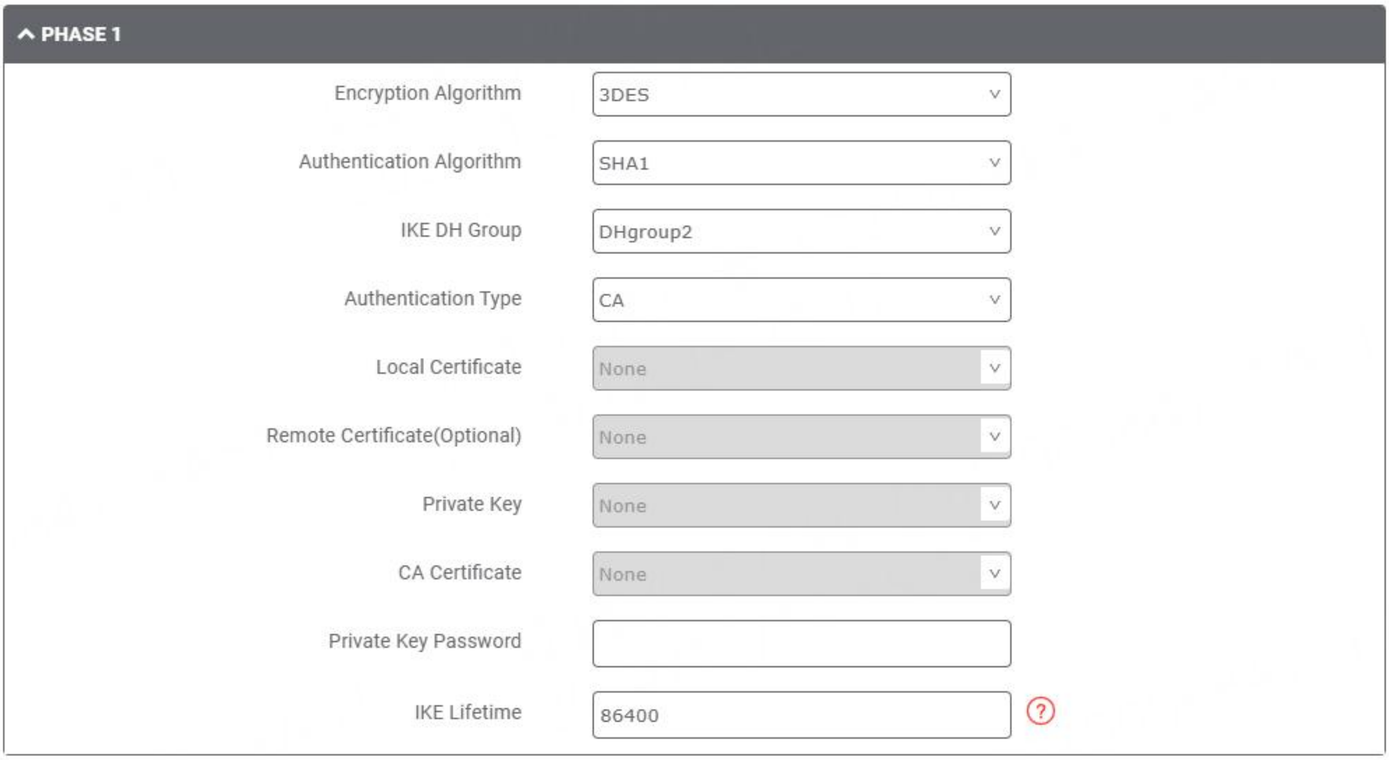
The window is displayed as below when choosing "PSK" as the authentication type.



^ PHASE 1

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

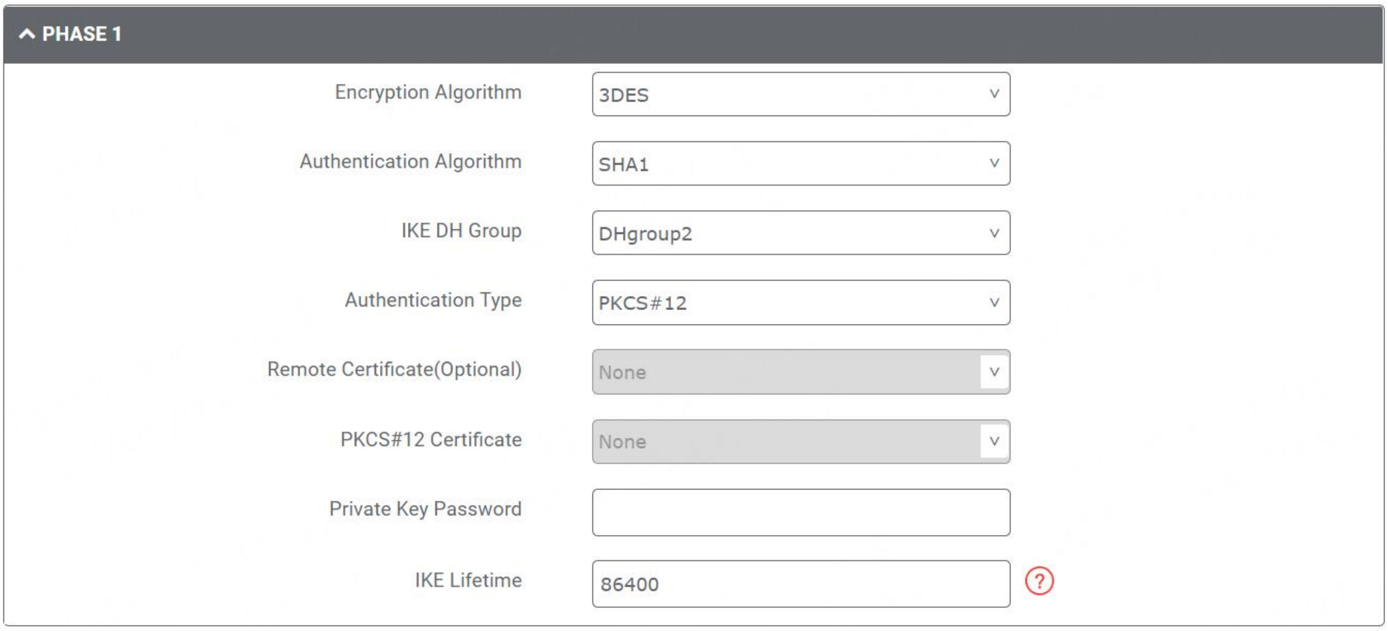
The window is displayed as below when choosing "CA" as the authentication type.



^ PHASE 1

Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	CA
Local Certificate	None
Remote Certificate(Optional)	None
Private Key	None
CA Certificate	None
Private Key Password	
IKE Lifetime	86400

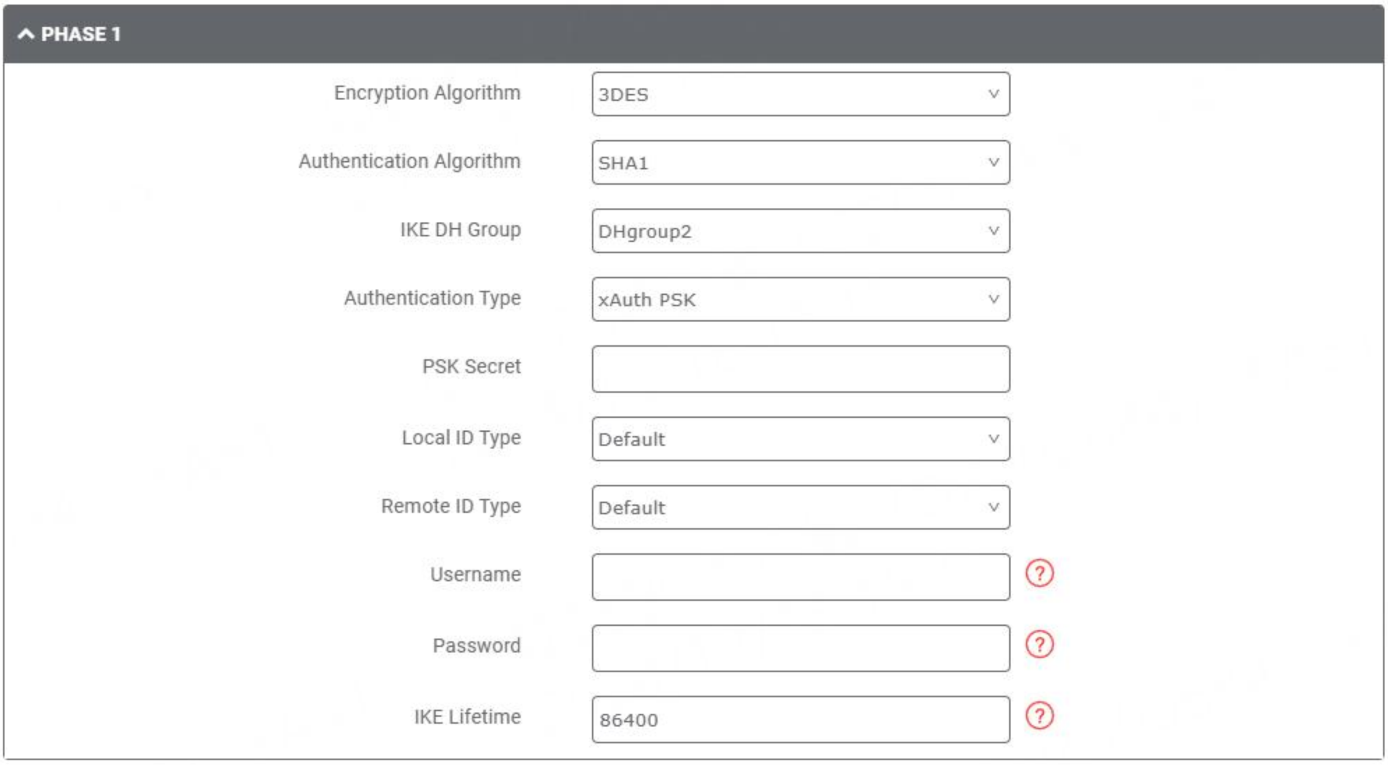
The window is displayed as below when choosing “PKCS#12” as the authentication type.



PHASE 1

Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PKCS#12
Remote Certificate(Optional)	None
PKCS#12 Certificate	None
Private Key Password	
IKE Lifetime	86400

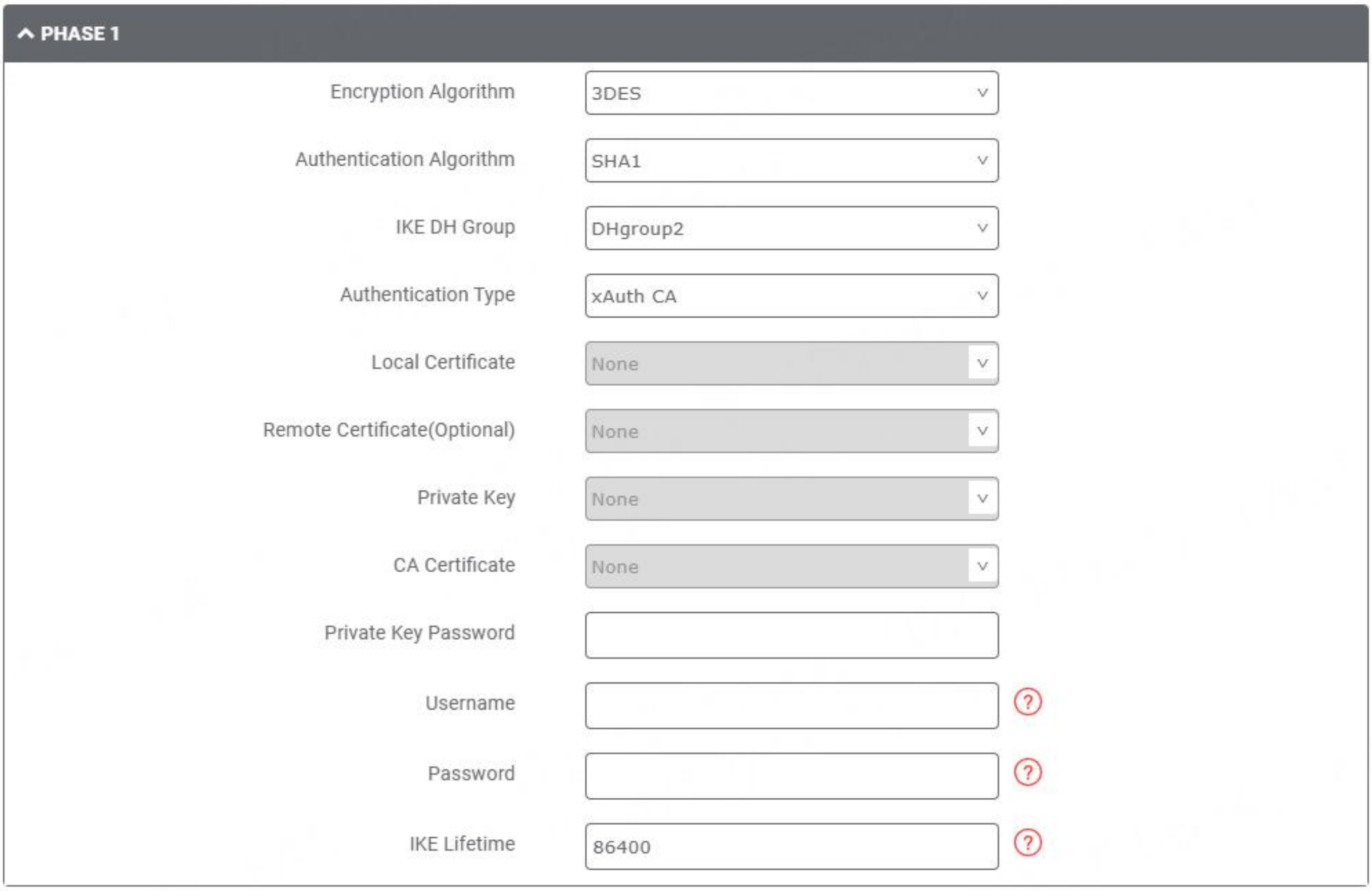
The window is displayed as below when choosing “xAuth PSK” as the authentication type.



PHASE 1

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

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



Encryption Algorithm: 3DES

Authentication Algorithm: SHA1

IKE DH Group: DHgroup2

Authentication Type: xAuth CA

Local Certificate: None

Remote Certificate(Optional): None

Private Key: None

CA Certificate: None

Private Key Password:

Username:

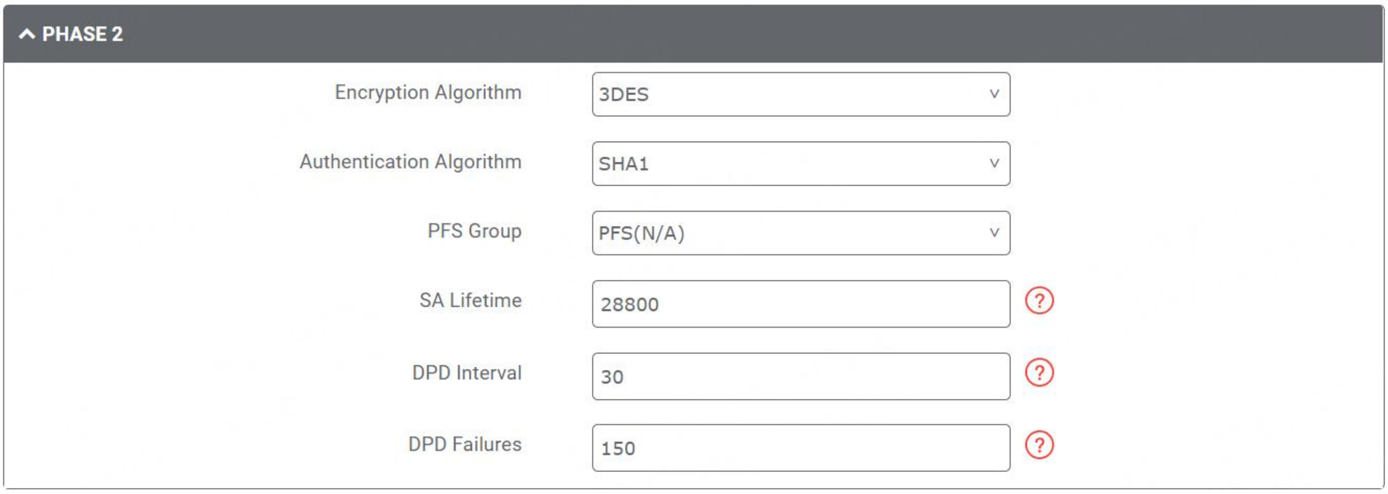
Password:

IKE Lifetime: 86400

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	Default

Item	Description	Default
	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	
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



Encryption Algorithm: 3DES

Authentication Algorithm: SHA1

PFS Group: PFS(N/A)

SA Lifetime: 28800

DPD Interval: 30

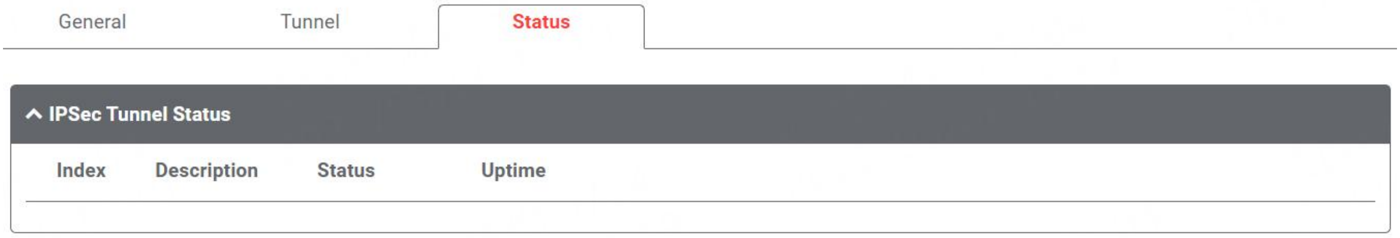
DPD Failures: 150

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

Item	Description	Default
PFS Group	Select from “PFS(N/A)”, “DHgroup1”,“DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in SA negotiation.	DHgroup2
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.

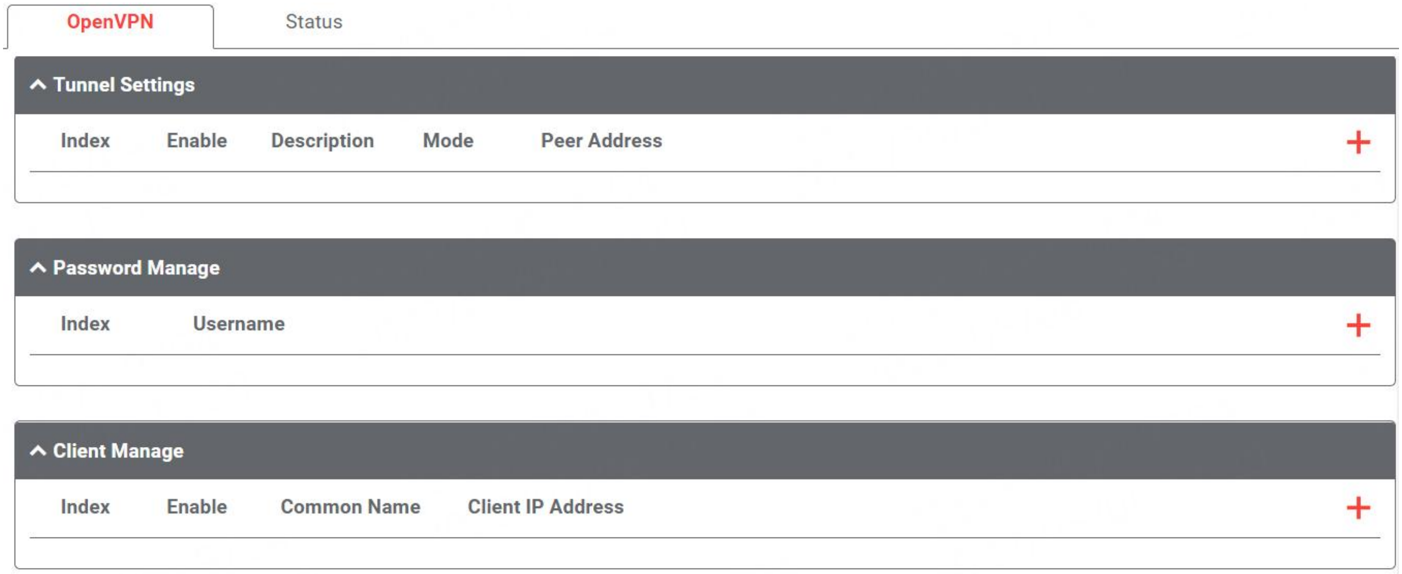


Index	Description	Status	Uptime

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



OpenVPN | Status

^ Tunnel Settings

Index	Enable	Description	Mode	Peer Address	+

^ Password Manage

Index	Username	+

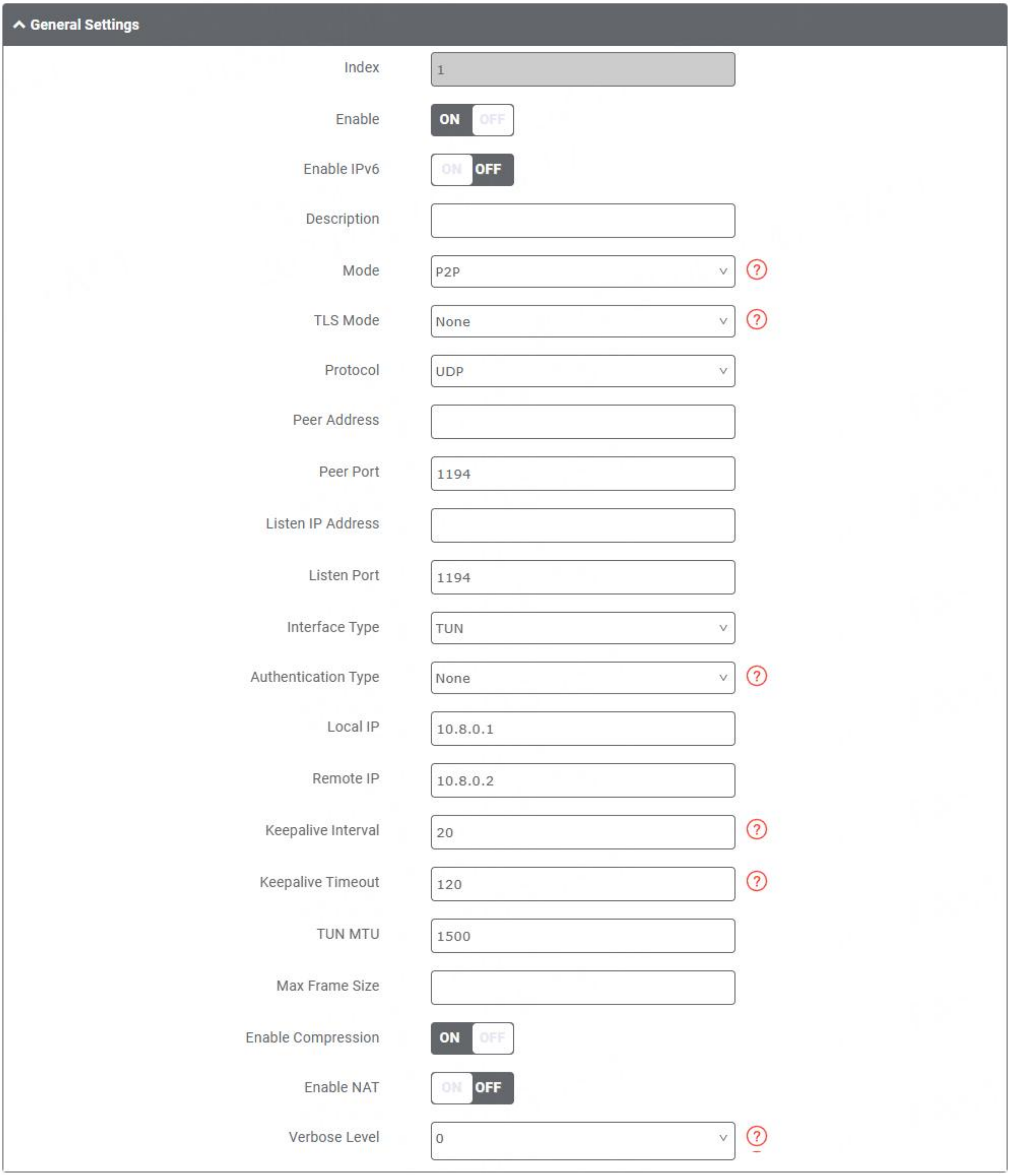
^ Client Manage

Index	Enable	Common Name	Client IP Address	+

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.

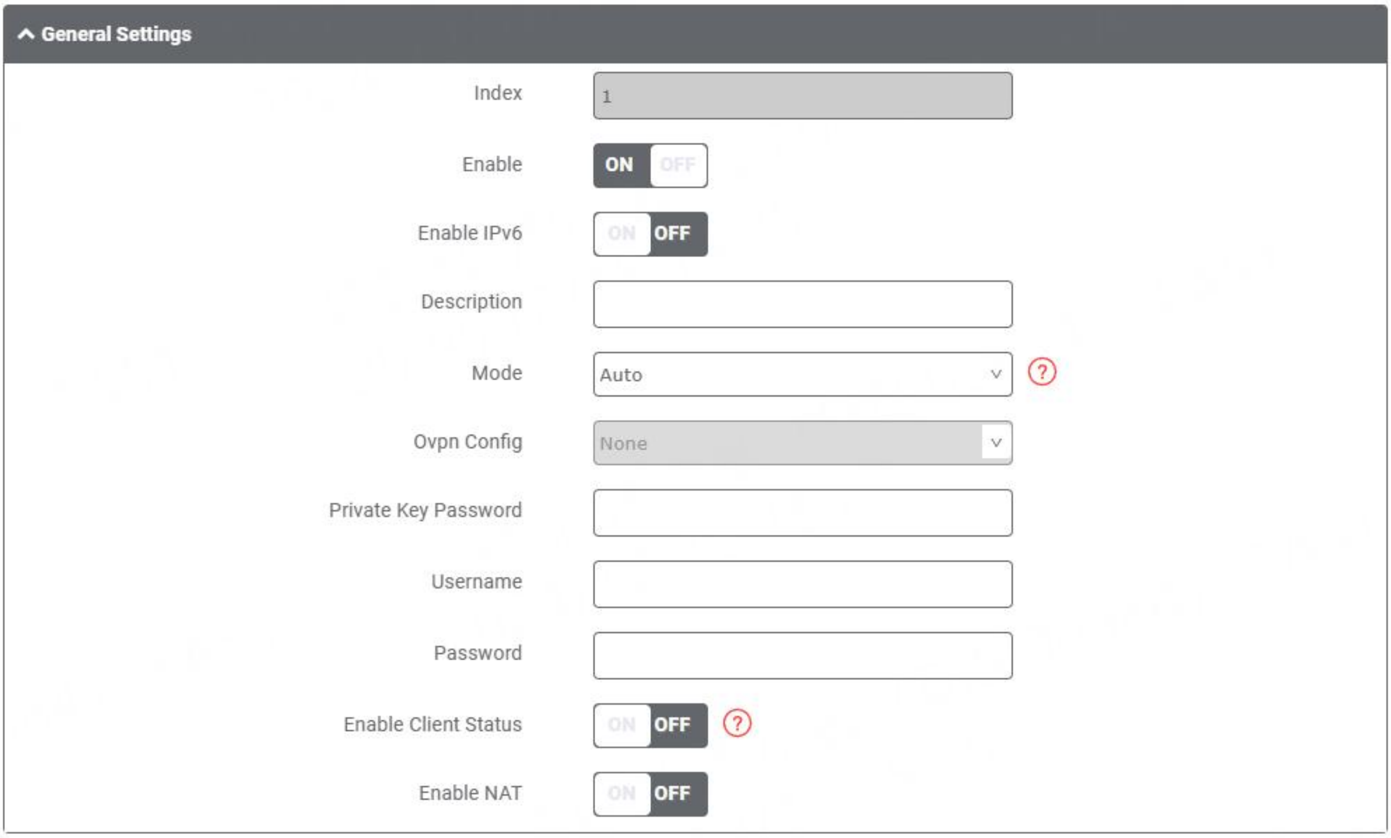
By default, the mode is “P2P”. The window is displayed as below when choosing “P2P” as the mode.



General Settings

Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	P2P
TLS Mode	None
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

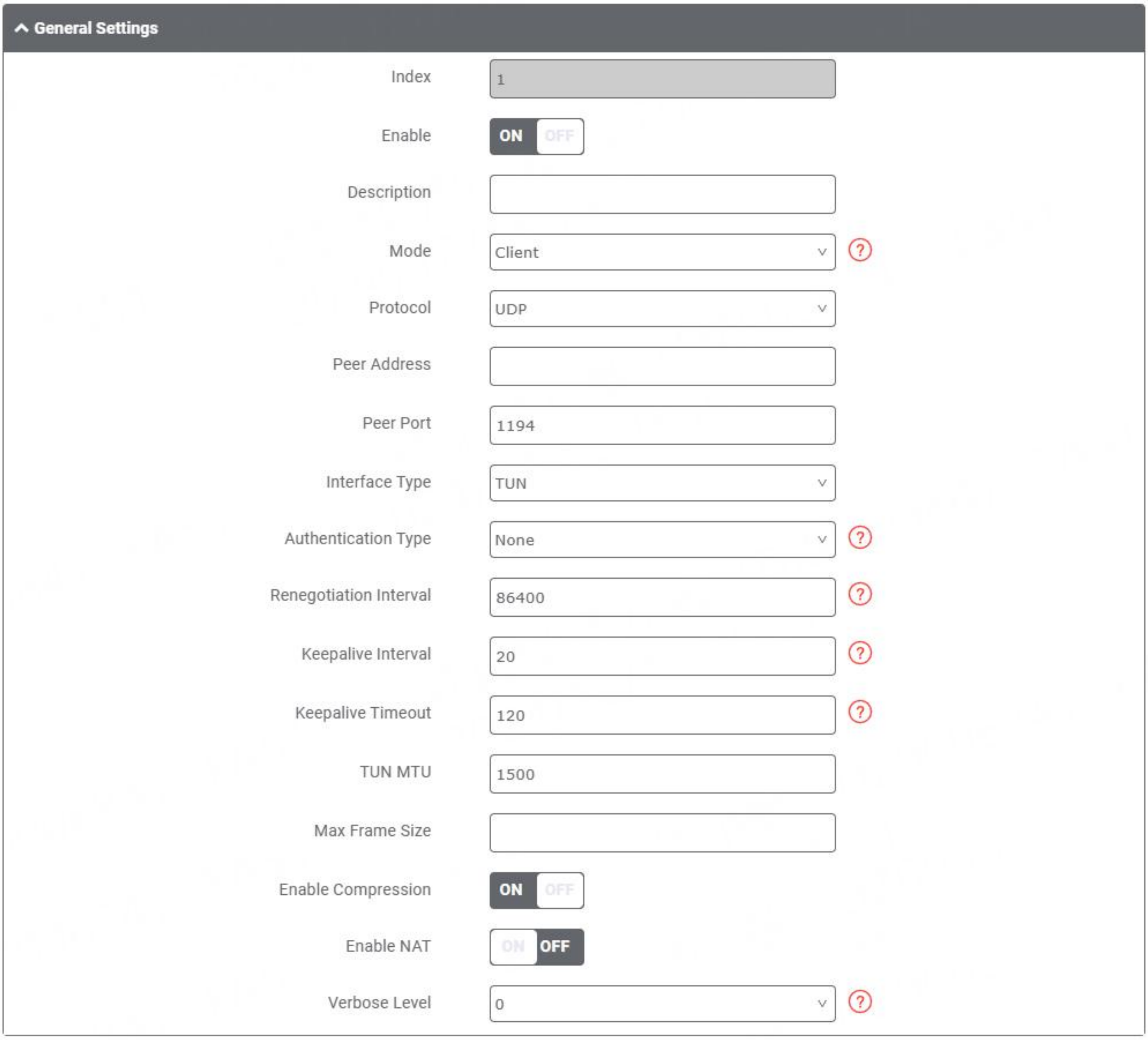
The window is displayed as below when choosing “Auto” as the mode.



General Settings

Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	Auto
Ovpn Config	None
Private Key Password	
Username	
Password	
Enable Client Status	OFF
Enable NAT	OFF

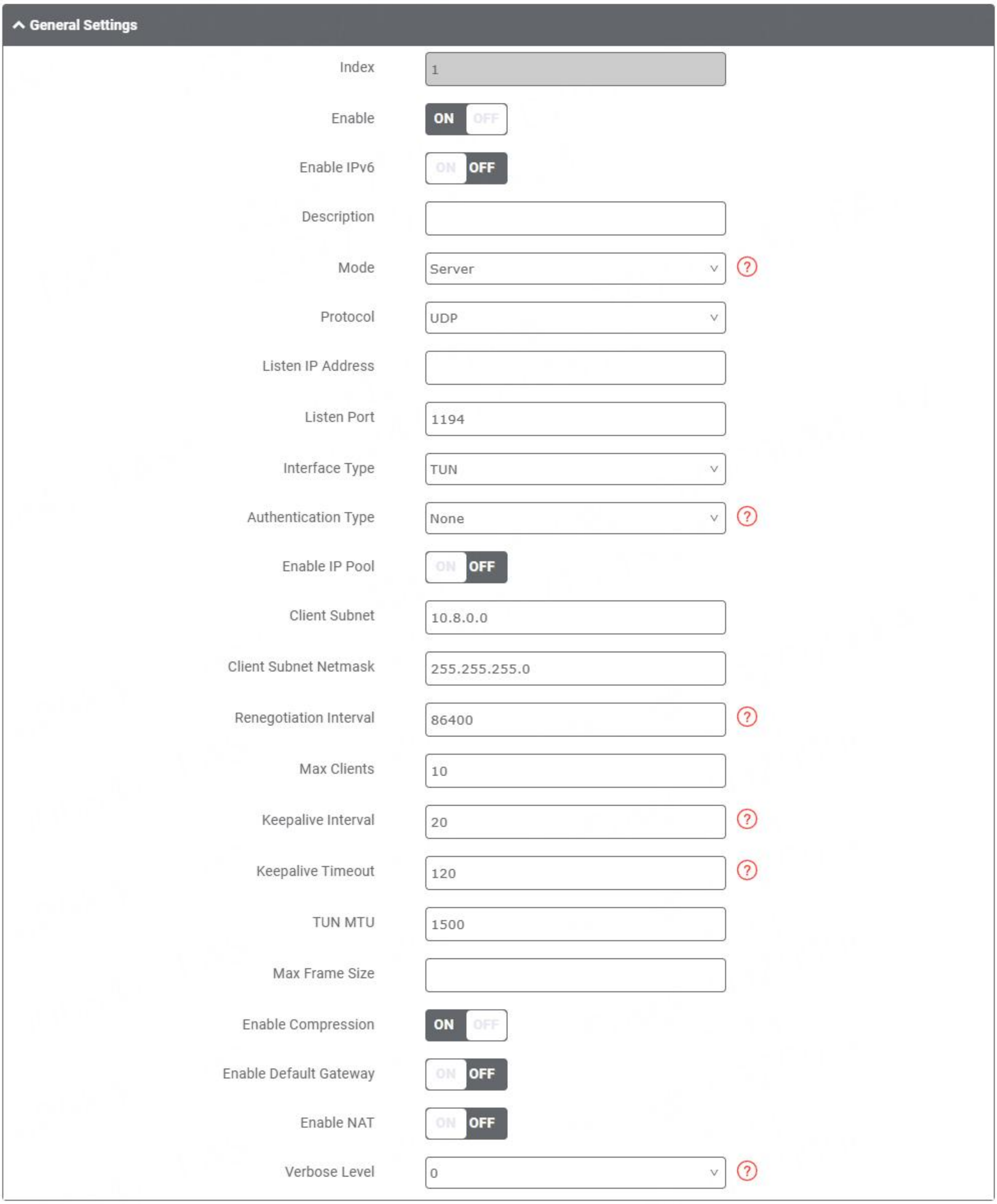
The window is displayed as below when choosing "Client" as the mode.



General Settings

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

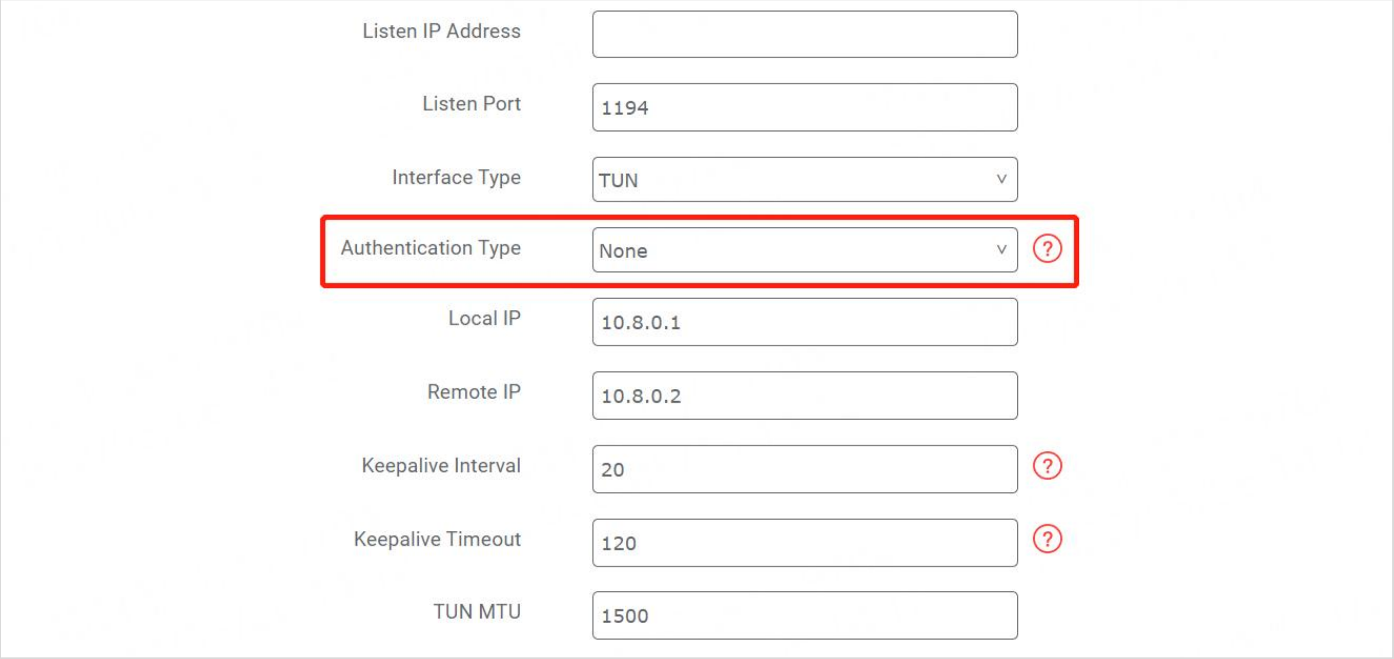
The window is displayed as below when choosing “Server” as the mode.



General Settings

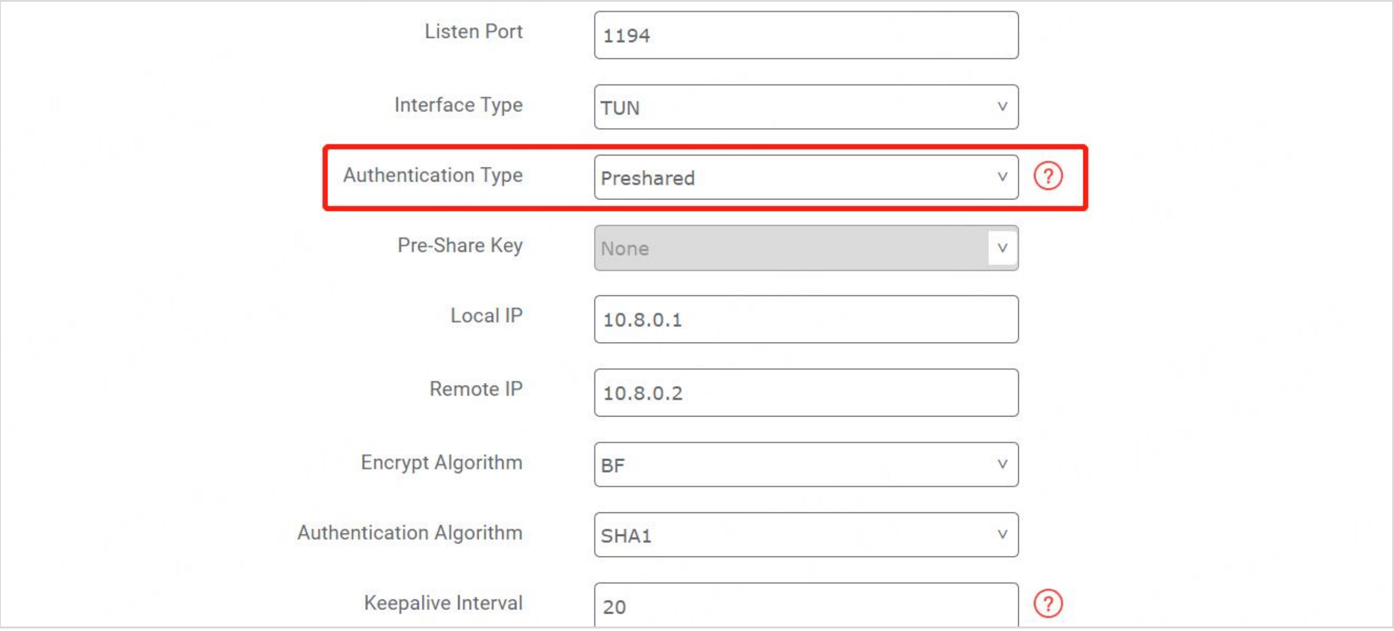
Index	1
Enable	ON
Enable IPv6	OFF
Description	
Mode	Server
Protocol	UDP
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Enable IP Pool	OFF
Client Subnet	10.8.0.0
Client Subnet Netmask	255.255.255.0
Renegotiation Interval	86400
Max Clients	10
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON
Enable Default Gateway	OFF
Enable NAT	OFF
Verbose Level	0

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



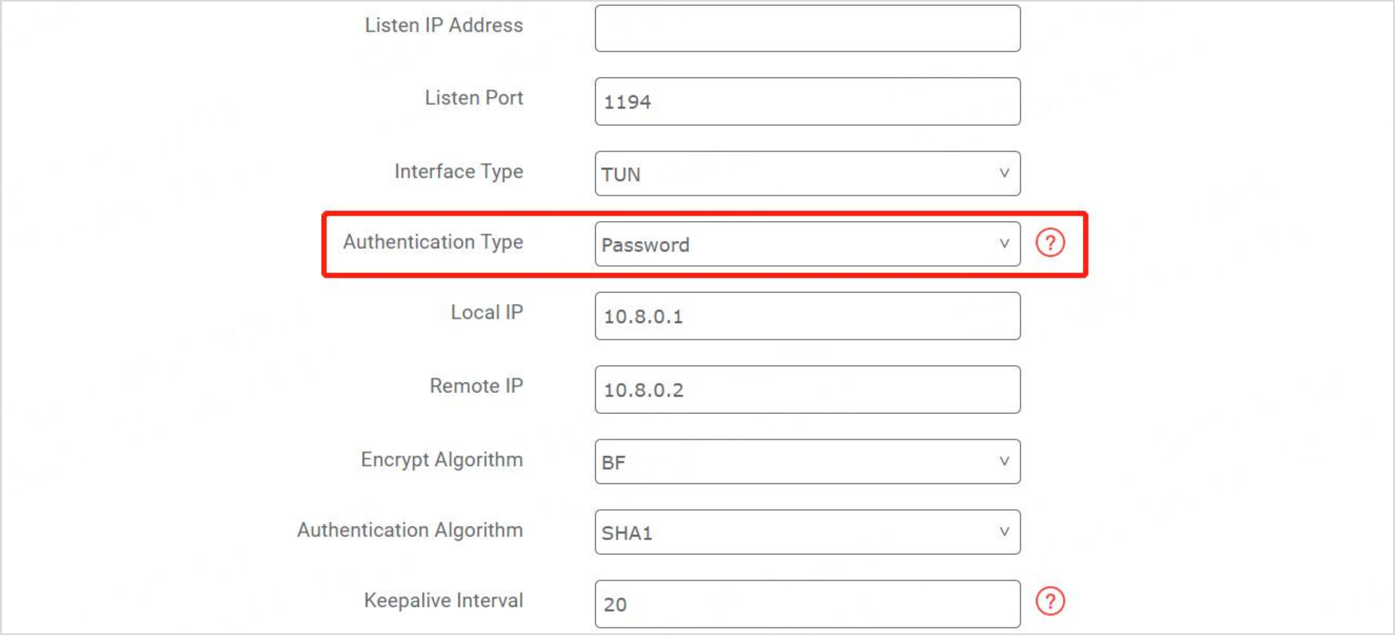
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500

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



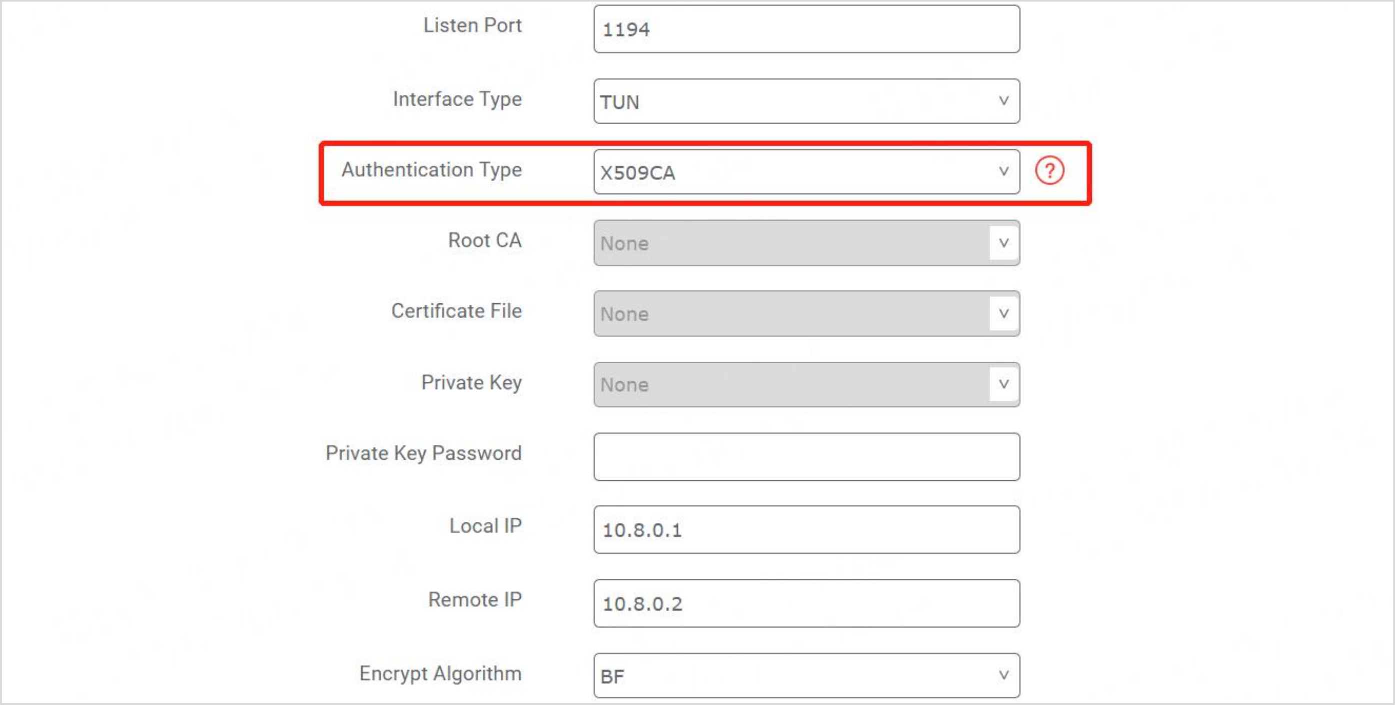
Listen Port	1194
Interface Type	TUN
Authentication Type	Preshared
Pre-Share Key	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Keepalive Interval	20

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



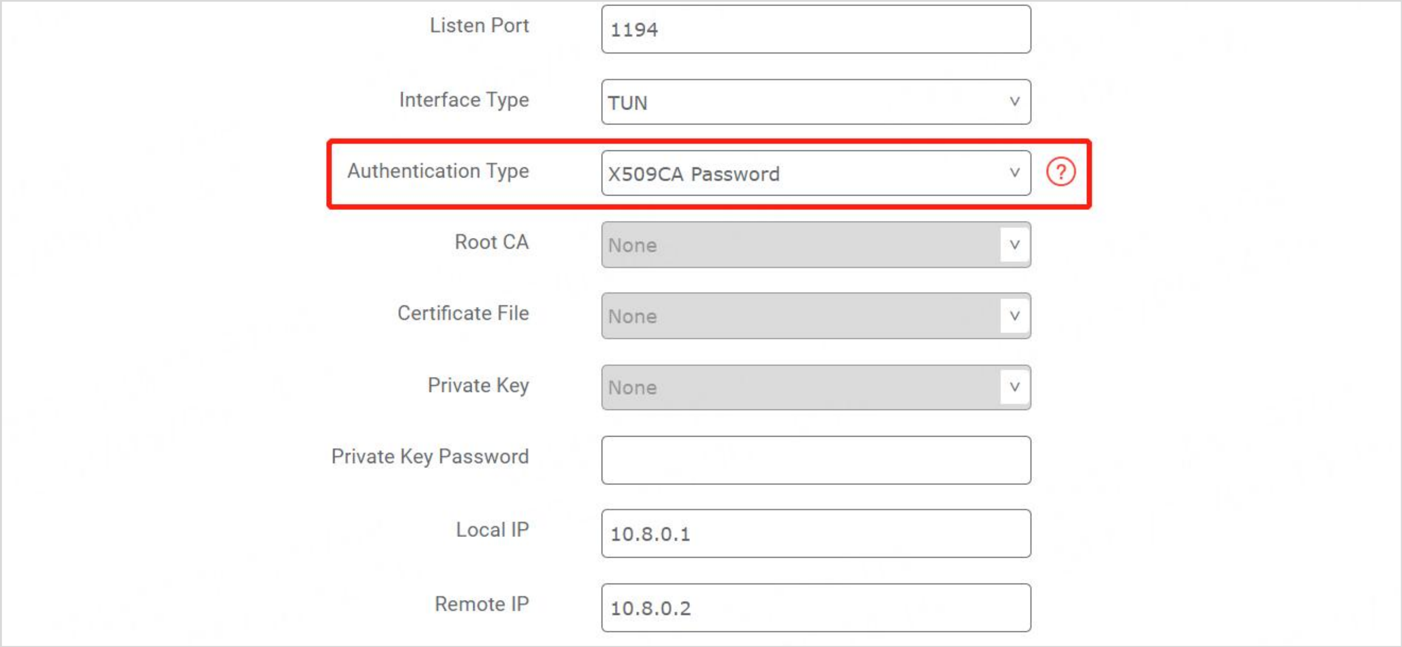
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	Password
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Keepalive Interval	20

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



Listen Port	1194
Interface Type	TUN
Authentication Type	X509CA
Root CA	None
Certificate File	None
Private Key	None
Private Key Password	
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF

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



Listen Port: 1194

Interface Type: TUN

Authentication Type: X509CA Password

Root CA: None

Certificate File: None

Private Key: None

Private Key Password:

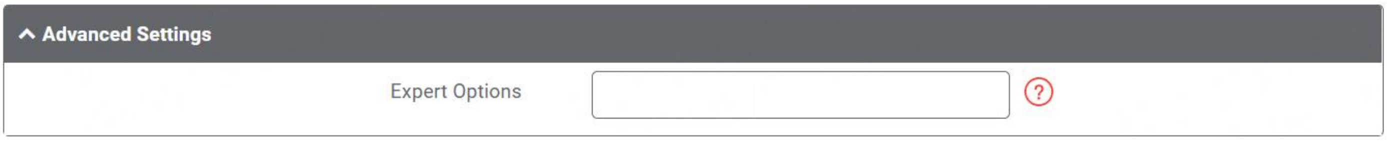
Local IP: 10.8.0.1

Remote IP: 10.8.0.2

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

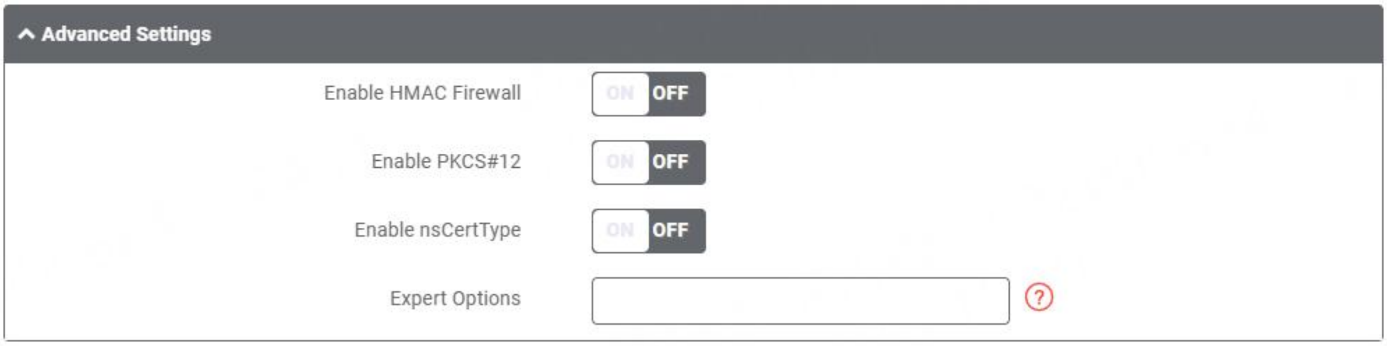
Item	Description	Default
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES-128", "AES-192" and "AES-256". • BF: Use 128-bit BF encryption algorithm in CBC mode • DES: Use 64-bit DES encryption algorithm in CBC mode • DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode • AES128: Use 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

Advanced settings for P2P/ Auto mode



Item	Description	Default
Expert Options	Enter some additional options for OpenVPN in this field. Multiple parameters can be separated by ';'.	Null

Advanced settings for Client mode:



^ Advanced Settings

Enable HMAC Firewall: ON OFF

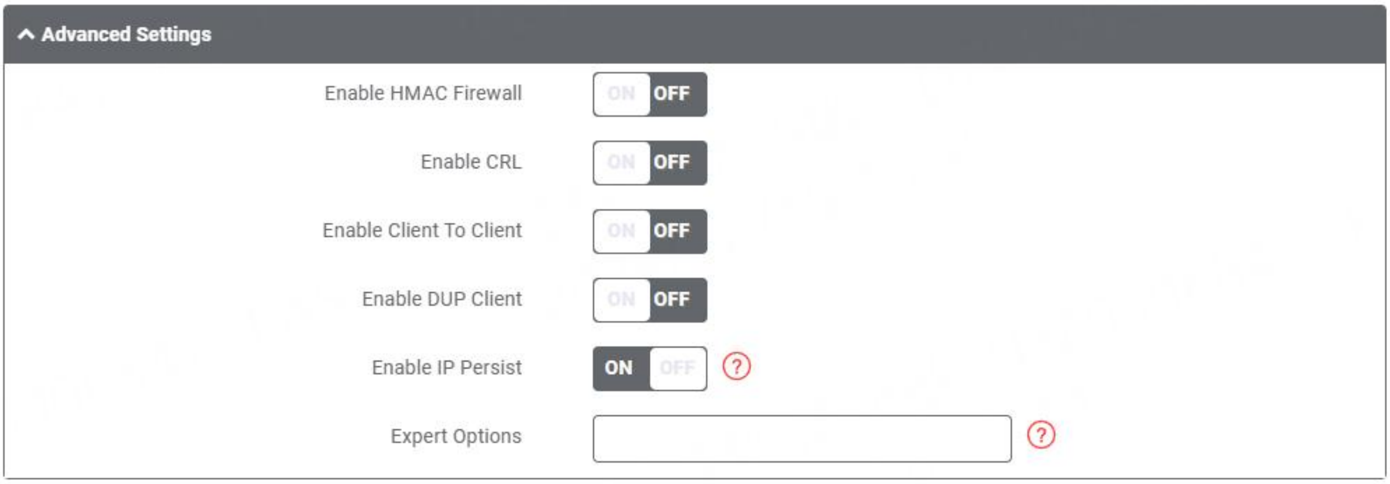
Enable PKCS#12: ON OFF

Enable nsCertType: ON OFF

Expert Options:

Item	Description	Default
Enable HMAC Firewall	Click the toggle button to enable/disable HMAC Firewall. Adds an additional HMAC (Hash Message Authentication Code) authentication on top of the TLS control channel to protect the link from DoS attacks.	OFF
Enable PKS#12	Click the toggle button to enable/disable PKCS#12. PKS#12 is a digital certificate encryption standard used to identify personally identifiable information.	OFF
Enable nsCertType	Click the toggle button to enable/disable nsCertType. nsCertType is an option in OpenVPN that specifies the client and server certificate types.	OFF
Expert Options	Enter some additional options for OpenVPN in this field. Multiple parameters can be separated by ';'.	Null

Advanced settings for Server mode:



^ Advanced Settings

Enable HMAC Firewall: ON OFF

Enable CRL: ON OFF

Enable Client To Client: ON OFF

Enable DUP Client: ON OFF

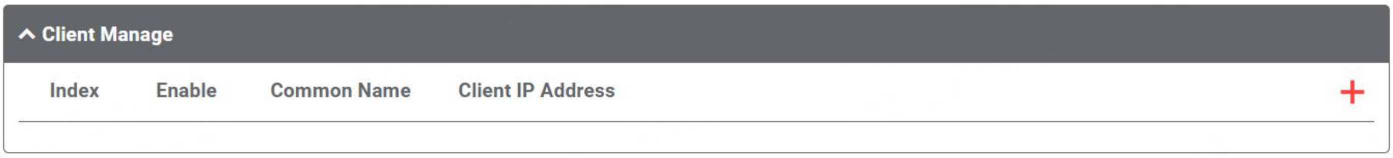
Enable IP Persist: ON OFF

Expert Options:

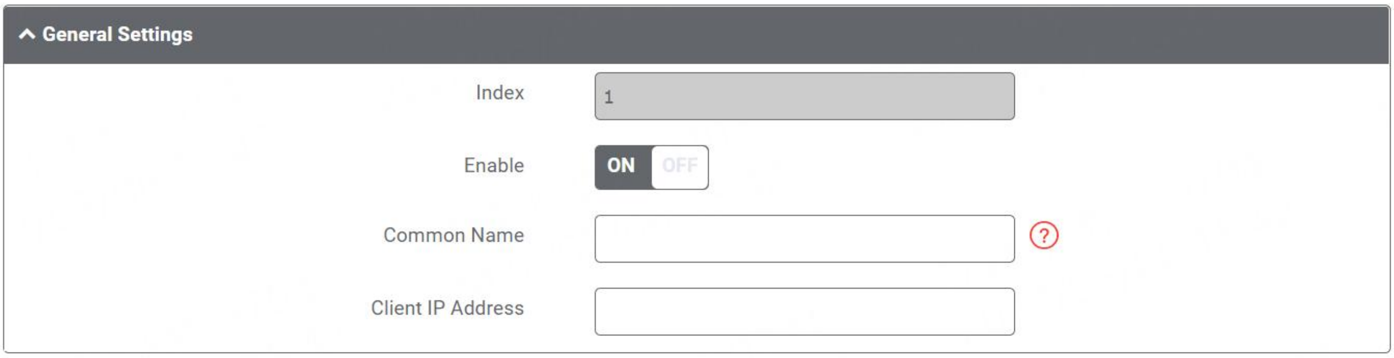
Item	Description	Default
Enable HMAC Firewall	Click the toggle button to enable/disable HMAC Firewall. Adds an additional HMAC (Hash Message Authentication Code) authentication on top of the TLS control channel to protect the link from DoS attacks.	OFF
Enabl CRL	Click the toggle button to enable/disable CRL.	OFF
Enable Client to Client	Click the toggle button to enable/disable Client to Client.	OFF
Enable DUP Client	Click the toggle button to enable/disable DUP Client. Allows multiple	OFF

Item	Description	Default
	clients to use the same certificate.	
Enable IP Persist	Click the toggle button to enable/disable IP Persist.	ON
Expert Options	Enter some additional options for OpenVPN in this field. Multiple parameters can be separated by ';'.	Null

Client Management



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



Index 1

Enable ON

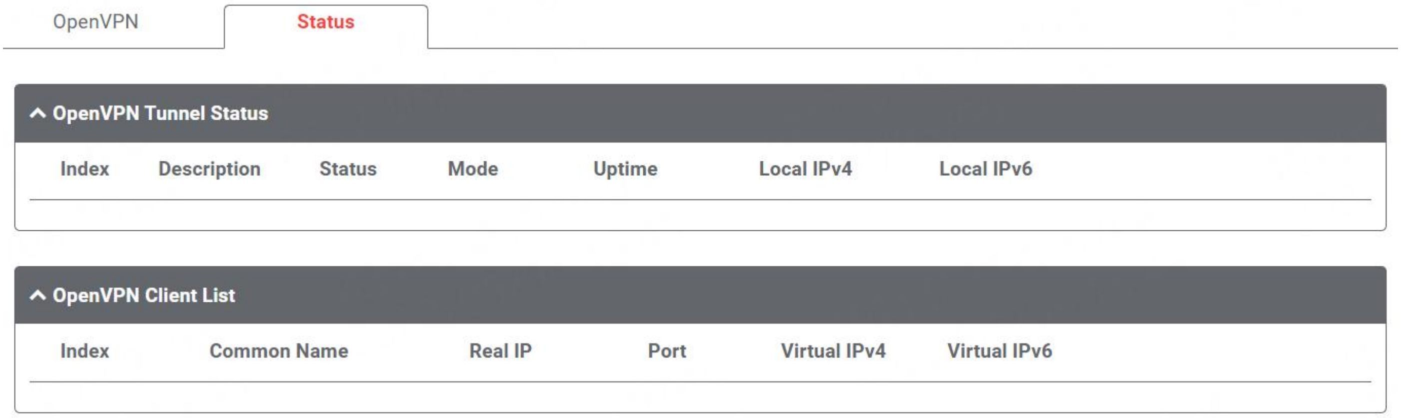
Common Name

Client IP Address

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.



OpenVPN Tunnel Status

Index	Description	Status	Mode	Uptime	Local IPv4	Local IPv6

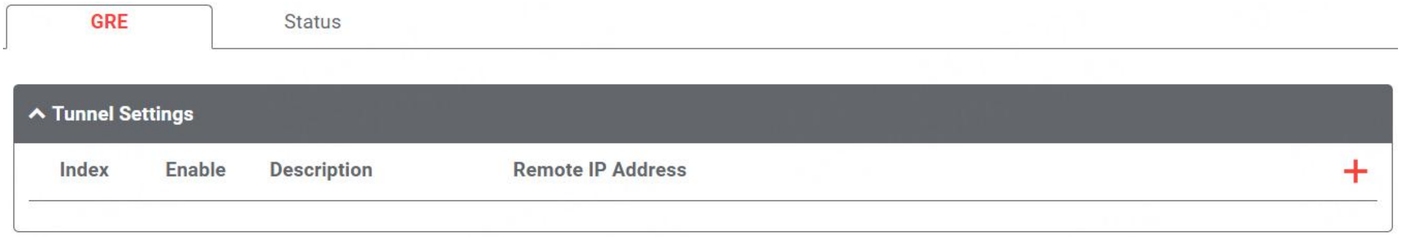
OpenVPN Client List

Index	Common Name	Real IP	Port	Virtual IPv4	Virtual IPv6

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.

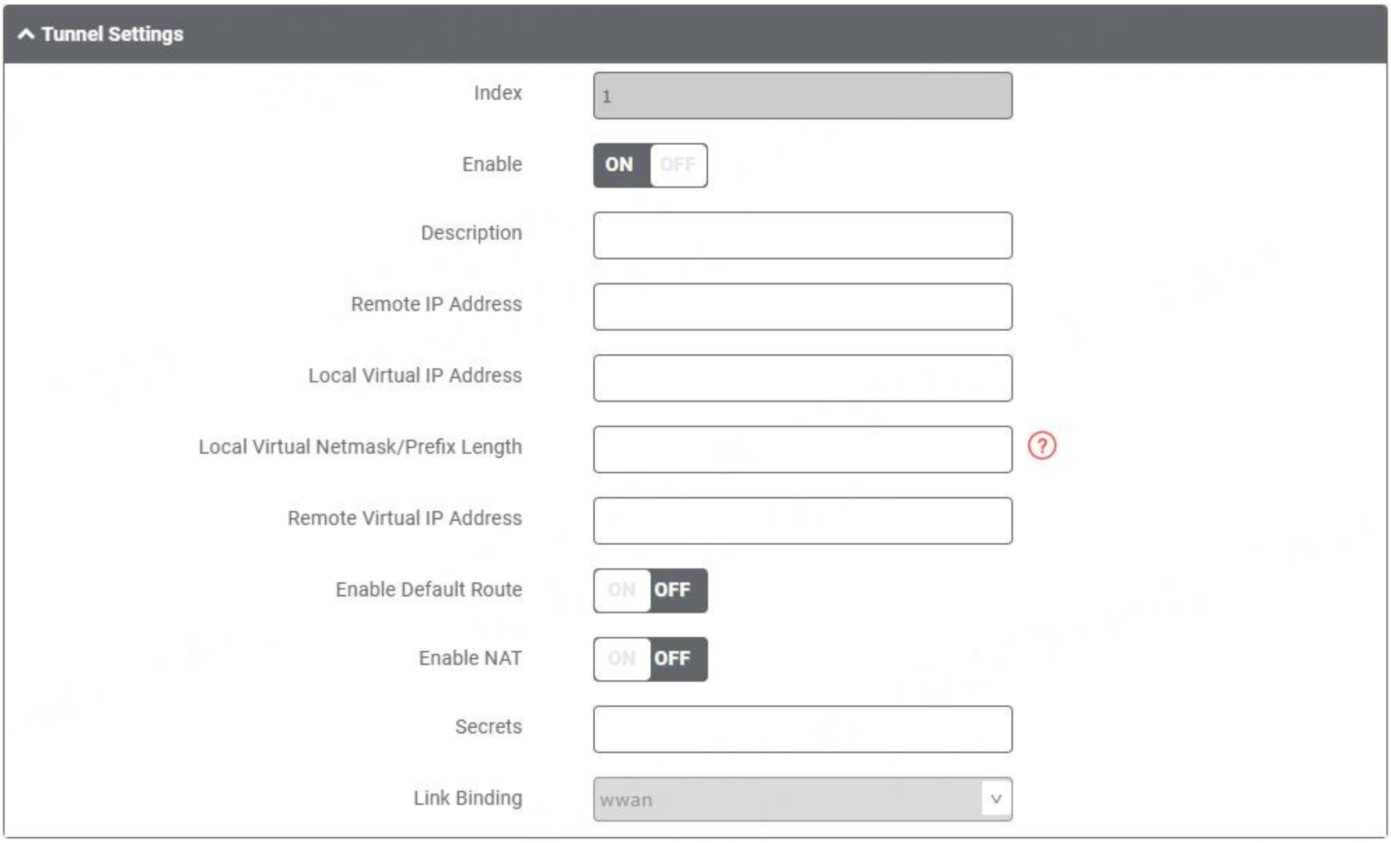
GRE



Tunnel Settings

Index	Enable	Description	Remote IP Address

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



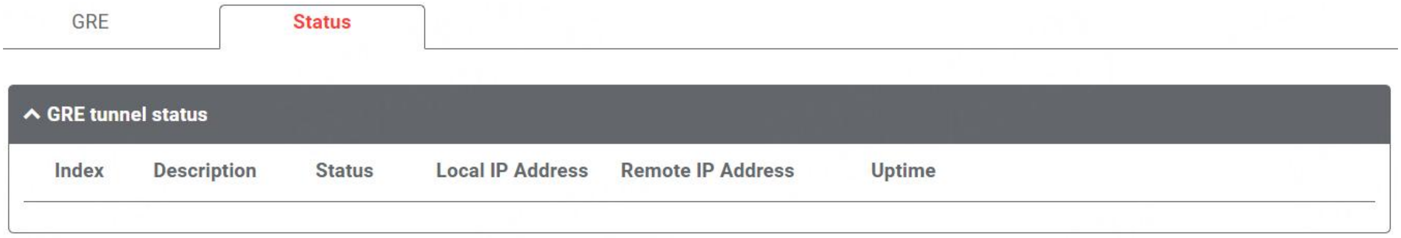
^ Tunnel Settings

Index	1
Enable	ON OFF
Description	
Remote IP Address	
Local Virtual IP Address	
Local Virtual Netmask/Prefix Length	
Remote Virtual IP Address	
Enable Default Route	ON OFF
Enable NAT	ON OFF
Secrets	
Link Binding	wwan

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.

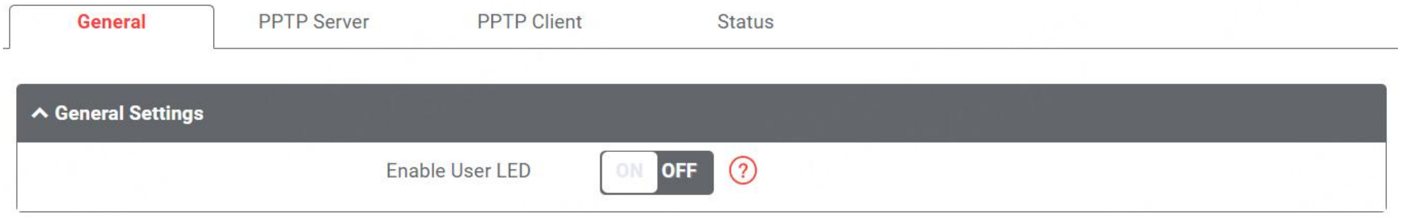


Index	Description	Status	Local IP Address	Remote IP Address	Uptime

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.

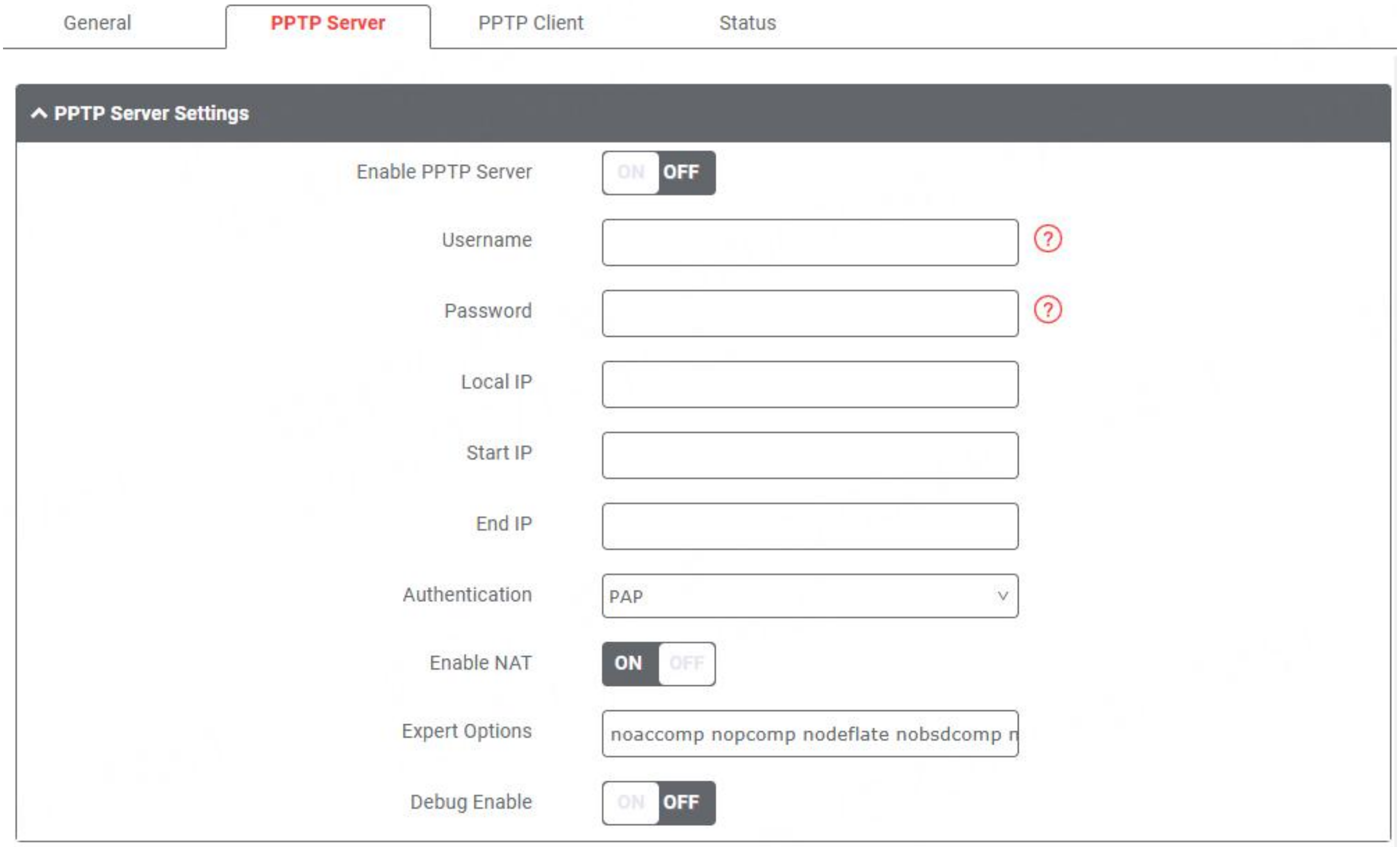
General



Enable User LED OFF

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



Enable PPTP Server: ON OFF

Username:

Password:

Local IP:

Start IP:

End IP:

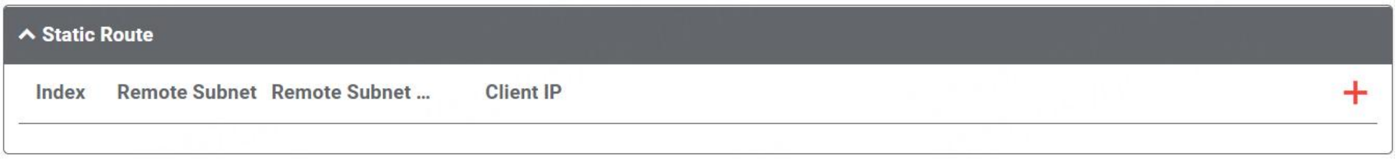
Authentication: PAP

Enable NAT: ON OFF

Expert Options: noaccomp nopcomp nodeflate nobsdcomp n

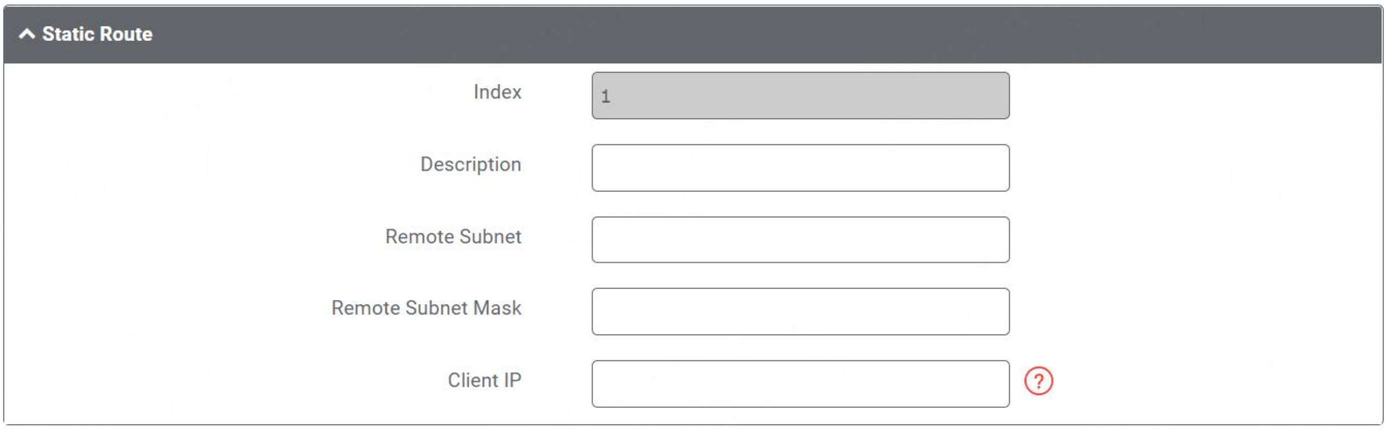
Debug Enable: ON OFF

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



Index	Remote Subnet	Remote Subnet ...	Client IP

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

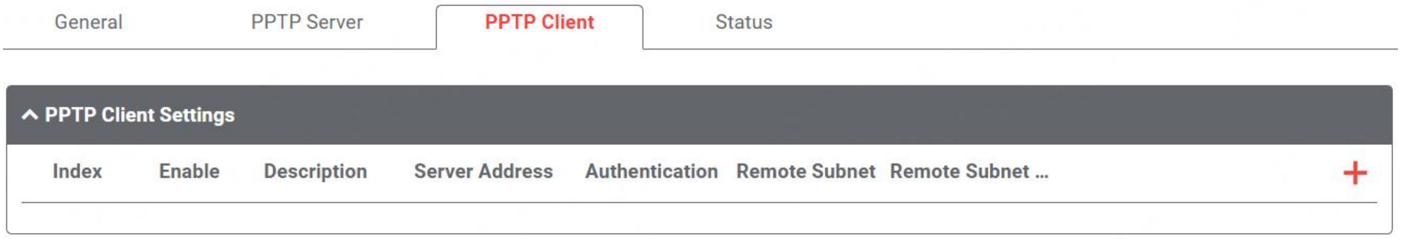


Static Route

Index	1
Description	
Remote Subnet	
Remote Subnet Mask	
Client IP	

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

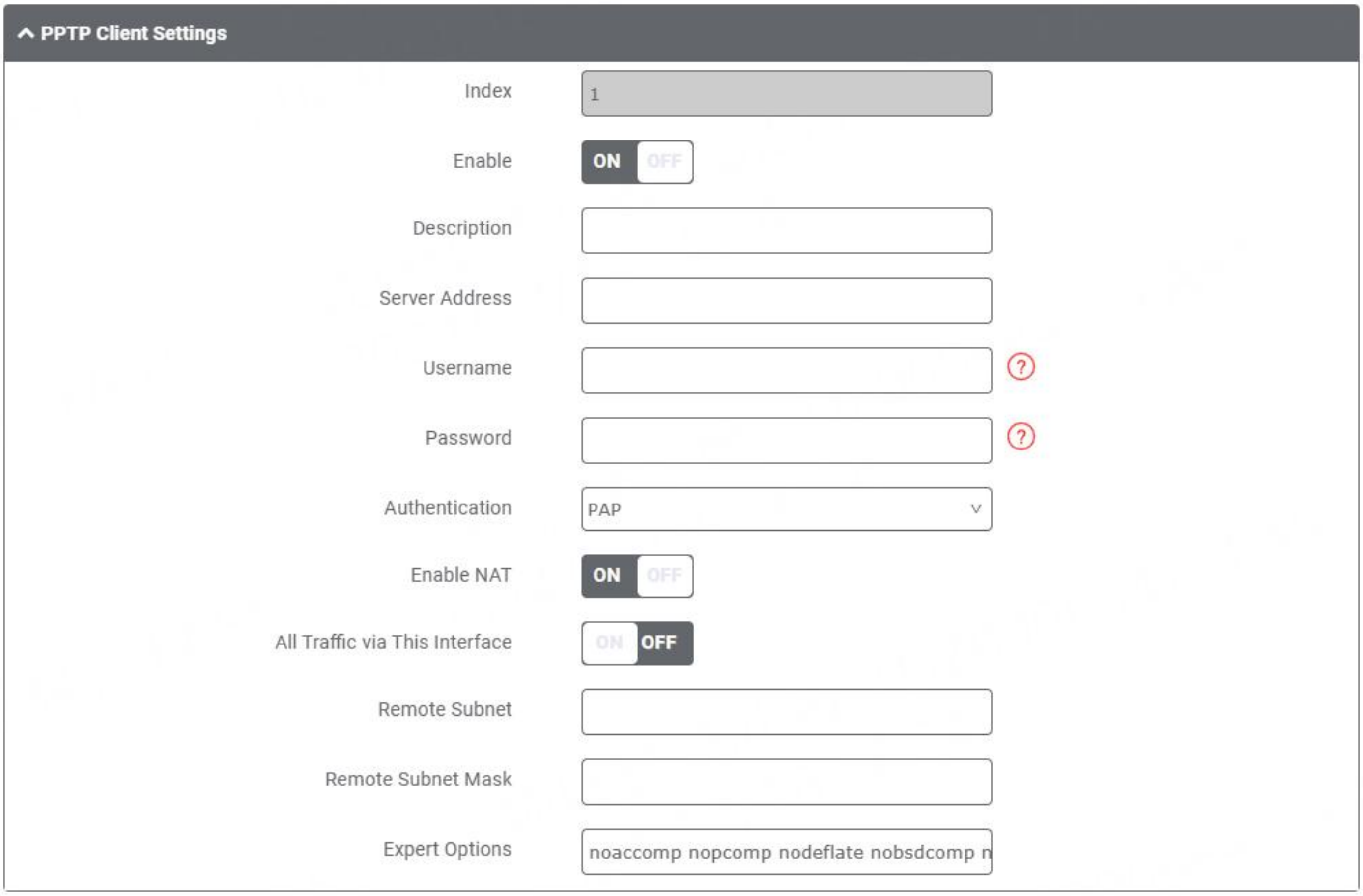
PPTP Client



PPTP Client Settings

Index	Enable	Description	Server Address	Authentication	Remote Subnet	Remote Subnet ...

Click + to add a PPTP client. The maximum count is **6**.



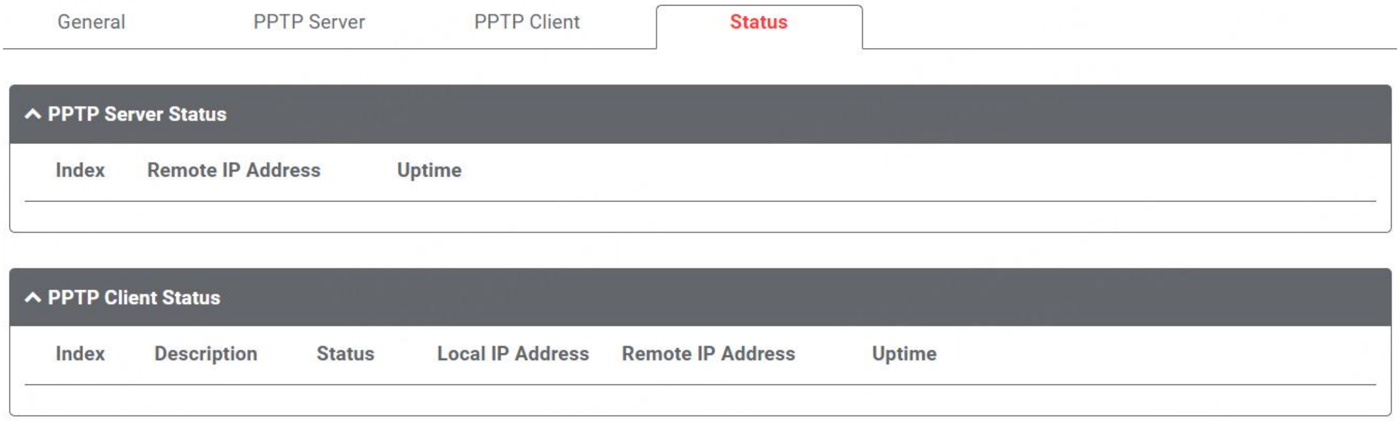
PPTP Client Settings

Index	1
Enable	ON
Description	
Server Address	
Username	
Password	
Authentication	PAP
Enable NAT	ON
All Traffic via This Interface	OFF
Remote Subnet	
Remote Subnet Mask	
Expert Options	noaccomp nopcomp nodeflate nobsdcomp n

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.	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
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

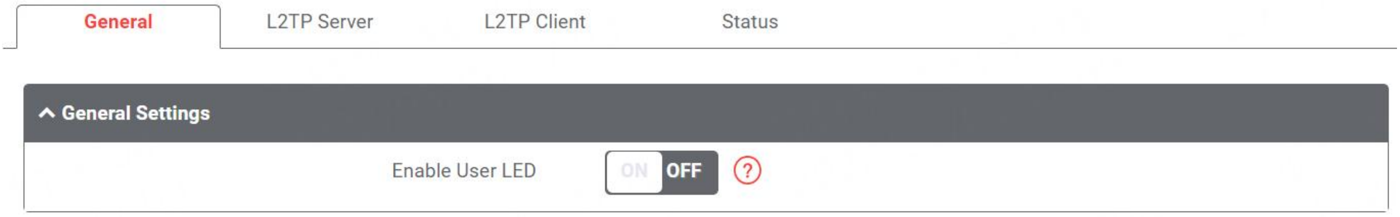
The status bar allows to view PPTP connection status. Click on one of the rows and details of its link connection will be displayed below the current row.



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.

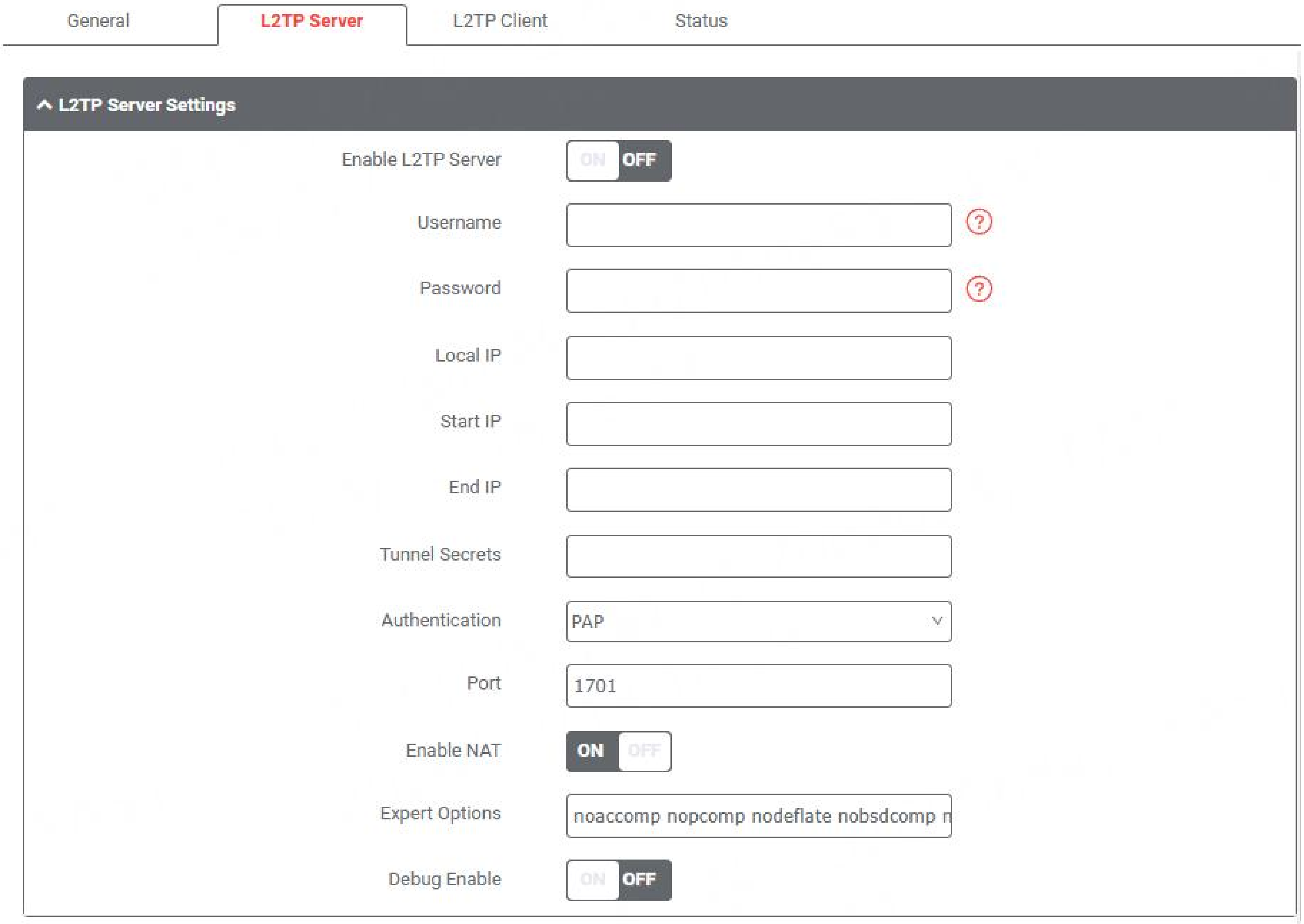
General



Enable User LED ON OFF

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



L2TP Server Settings

Enable L2TP Server: ON ● OFF

Username:

Password:

Local IP:

Start IP:

End IP:

Tunnel Secrets:

Authentication: PAP

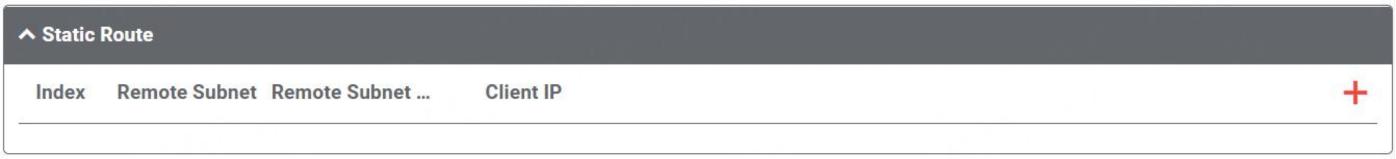
Port: 1701

Enable NAT: ● ON OFF

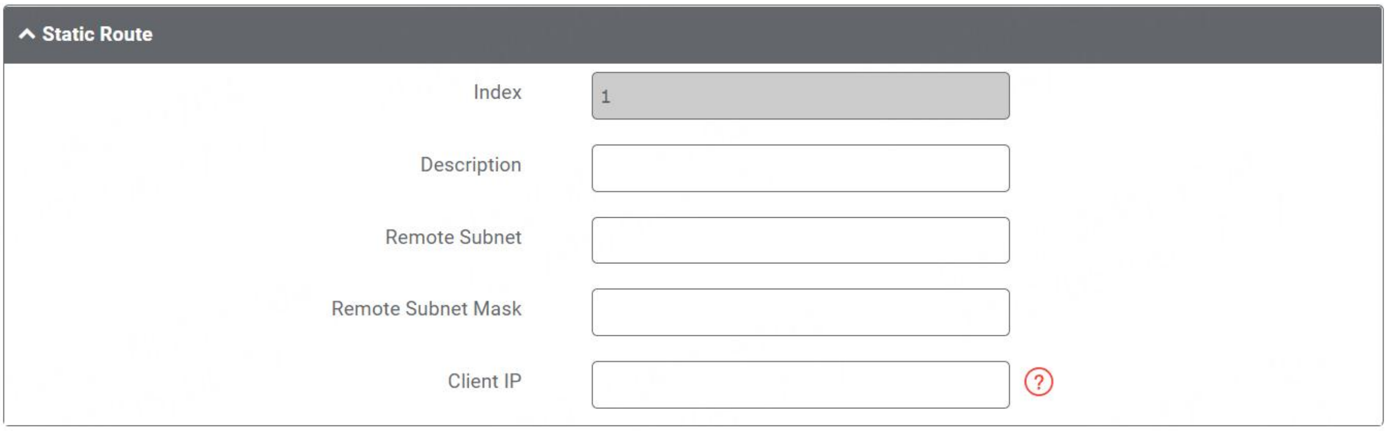
Expert Options: noaccomp nopcomp nodeflate nobsdcomp n

Debug Enable: ON ● OFF

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



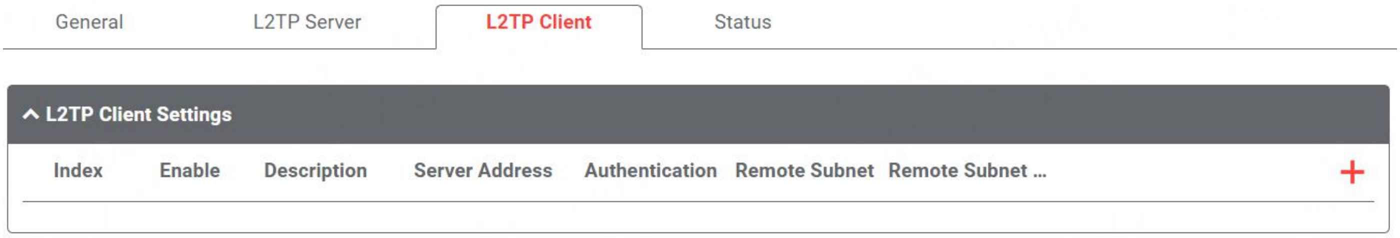
Click + to add a static route for L2TP server. The maximum count is **20.**



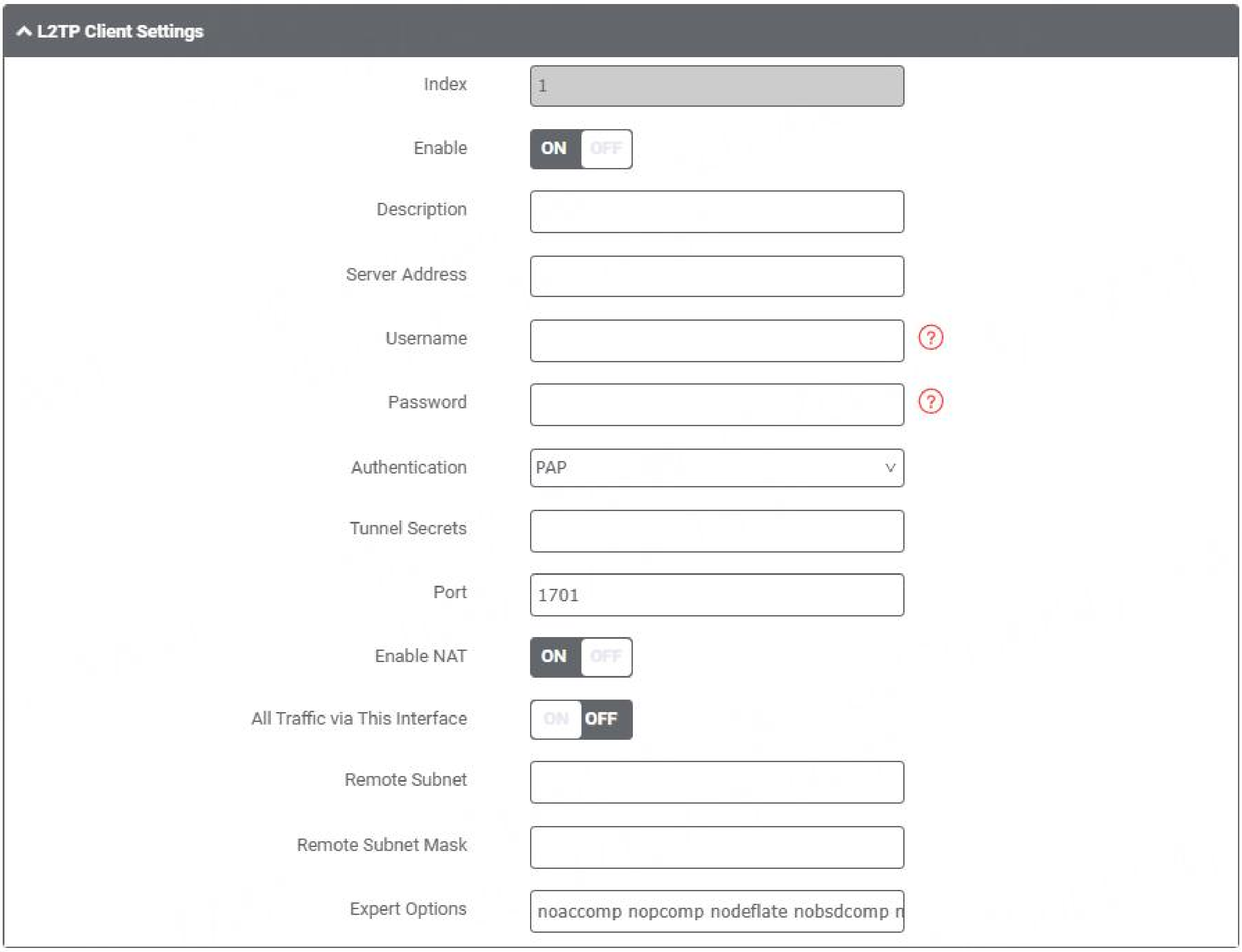
Index	1
Description	
Remote Subnet	
Remote Subnet Mask	
Client IP	

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 **3**.



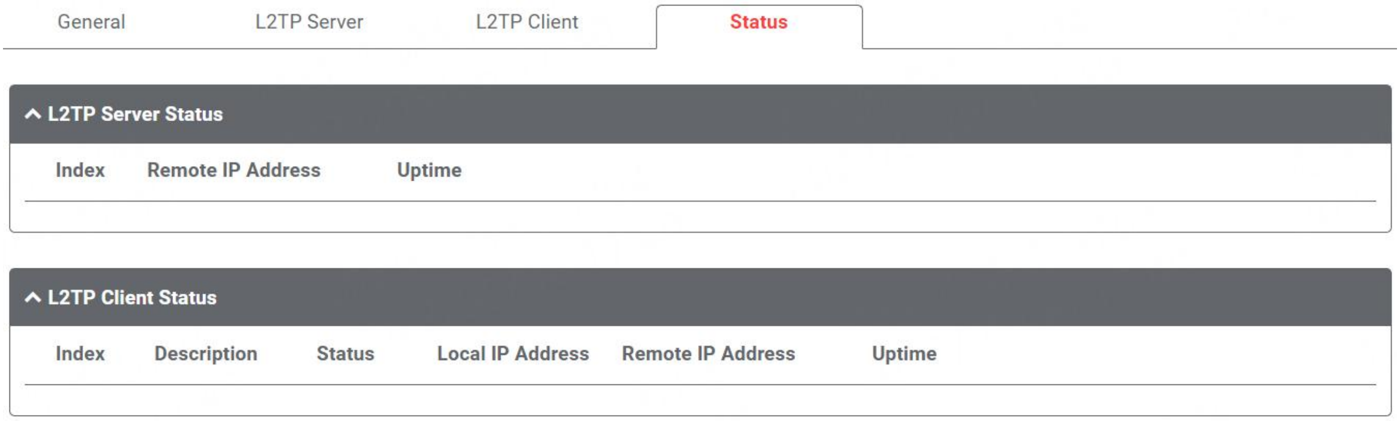
^ L2TP Client Settings

Index	1
Enable	ON
Description	
Server Address	
Username	
Password	
Authentication	PAP
Tunnel Secrets	
Port	1701
Enable NAT	ON
All Traffic via This Interface	OFF
Remote Subnet	
Remote Subnet Mask	
Expert Options	noaccomp nopcomp nodeflate nobsdcomp n

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.



L2TP Server Status

Index	Remote IP Address	Uptime

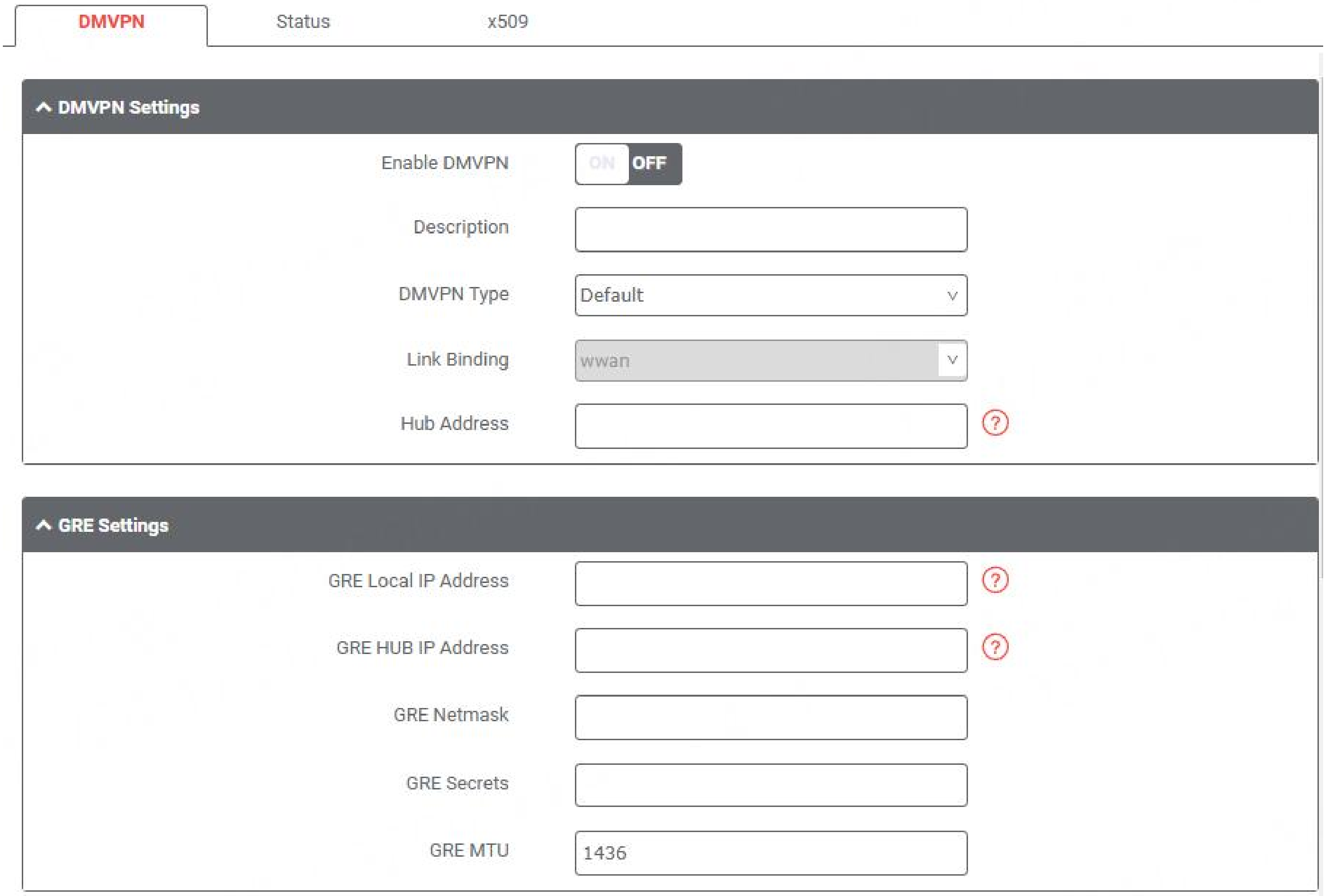
L2TP Client Status

Index	Description	Status	Local IP Address	Remote IP Address	Uptime

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



DMVPN | Status | x509

DMVPN Settings

Enable DMVPN: ON **OFF**

Description:

DMVPN Type: Default

Link Binding: wwan

Hub Address:

GRE Settings

GRE Local IP Address:

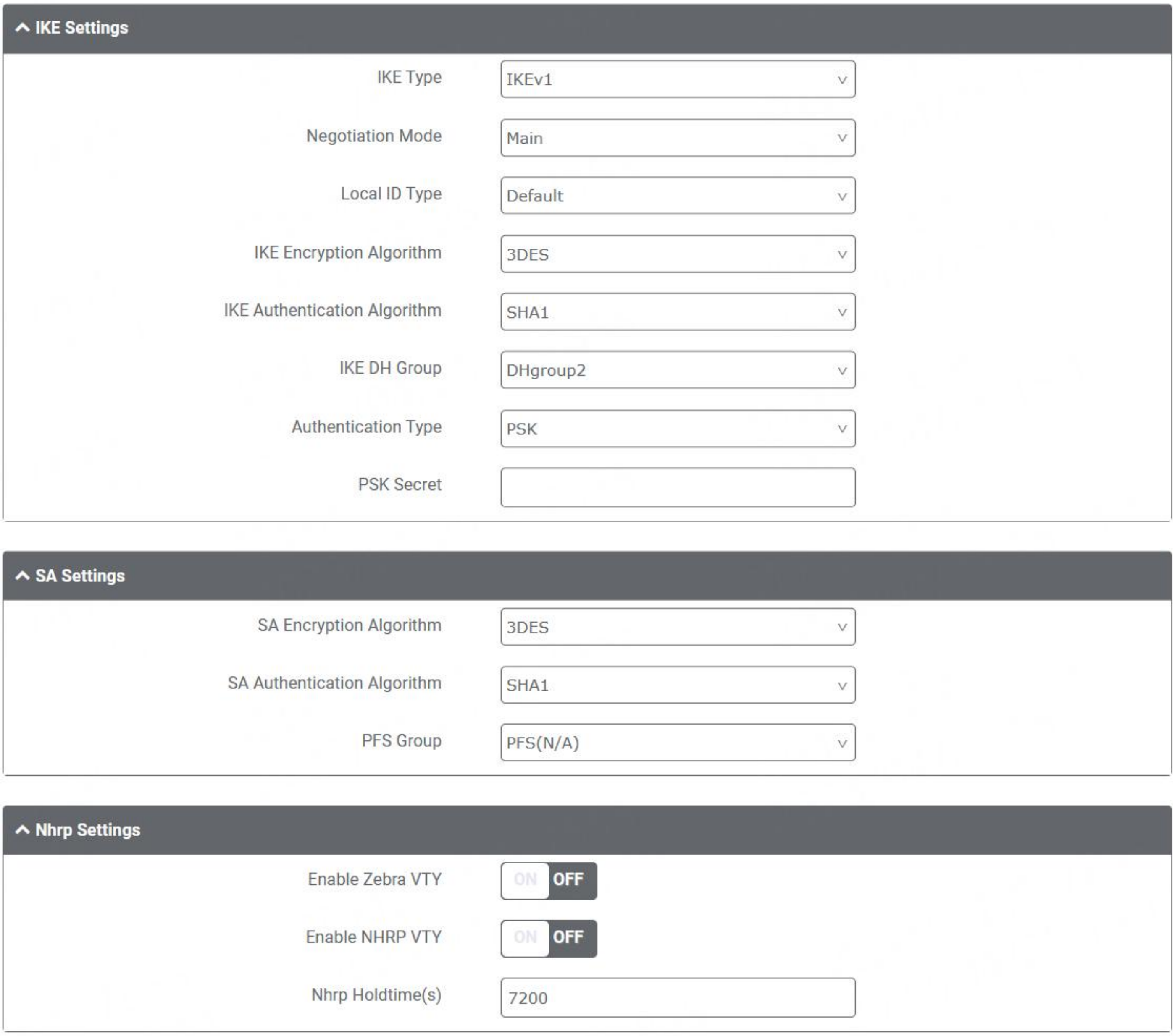
GRE HUB IP Address:

GRE Netmask:

GRE Secrets:

GRE MTU: 1436

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



IKE Settings

IKE Type: IKEv1

Negotiation Mode: Main

Local ID Type: Default

IKE Encryption Algorithm: 3DES

IKE Authentication Algorithm: SHA1

IKE DH Group: DHgroup2

Authentication Type: PSK

PSK Secret:

SA Settings

SA Encryption Algorithm: 3DES

SA Authentication Algorithm: SHA1

PFS Group: PFS(N/A)

Nhrp Settings

Enable Zebra VTY: ON OFF

Enable NHRP VTY: ON OFF

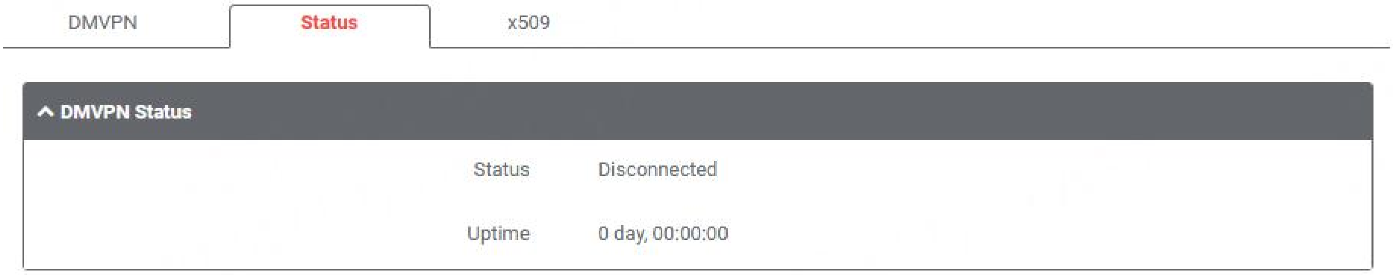
Nhrp Holdtime(s): 7200

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

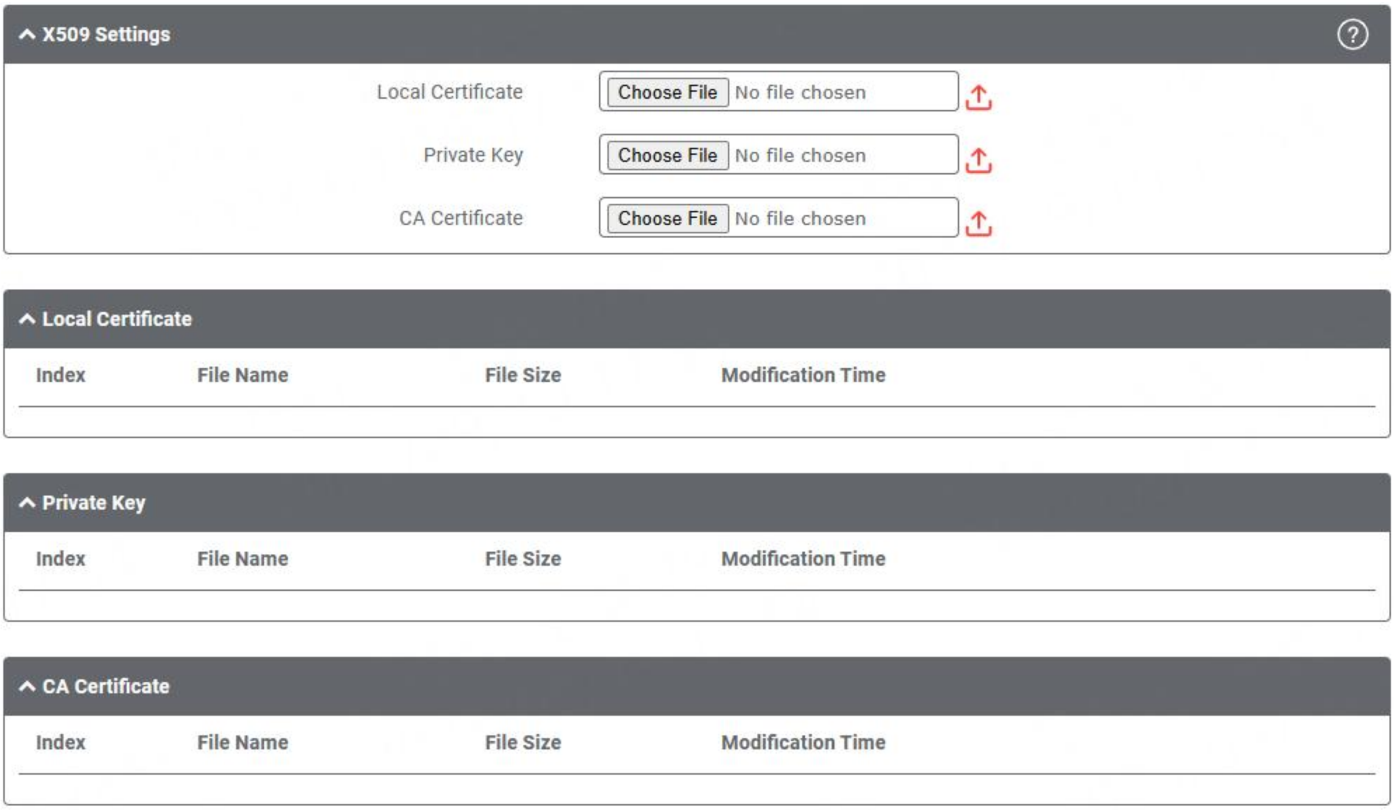
The status bar allows to view DMVPN connection status.



Status Disconnected

Uptime 0 day, 00:00:00

X509



X509 Settings

Local Certificate — Choose File No file chosen

Private Key — Choose File No file chosen

CA Certificate — Choose File No file chosen

Local Certificate

Index	File Name	File Size	Modification Time

Private Key

Index	File Name	File Size	Modification Time

CA Certificate

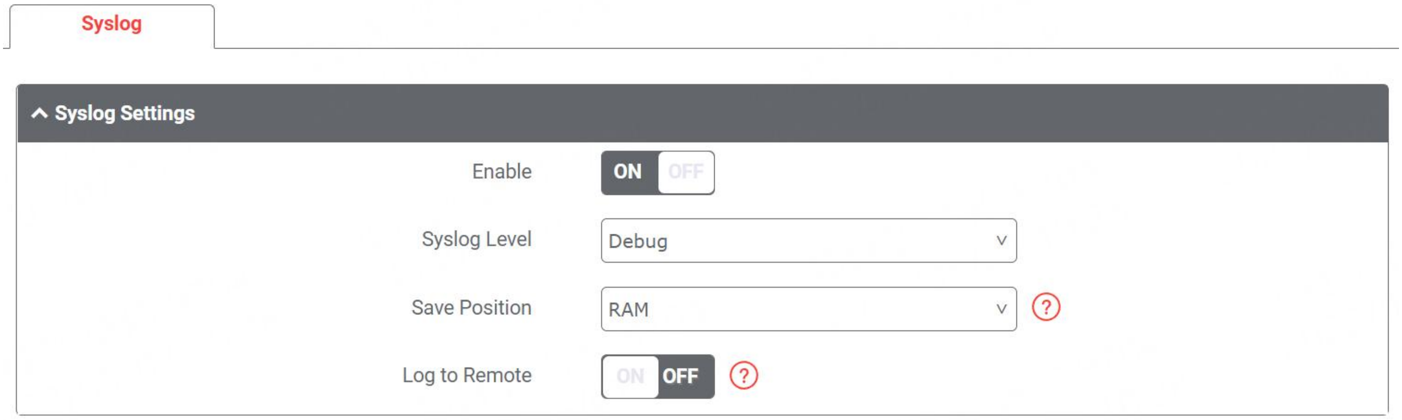
Index	File Name	File Size	Modification Time

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.



Syslog

^ Syslog Settings

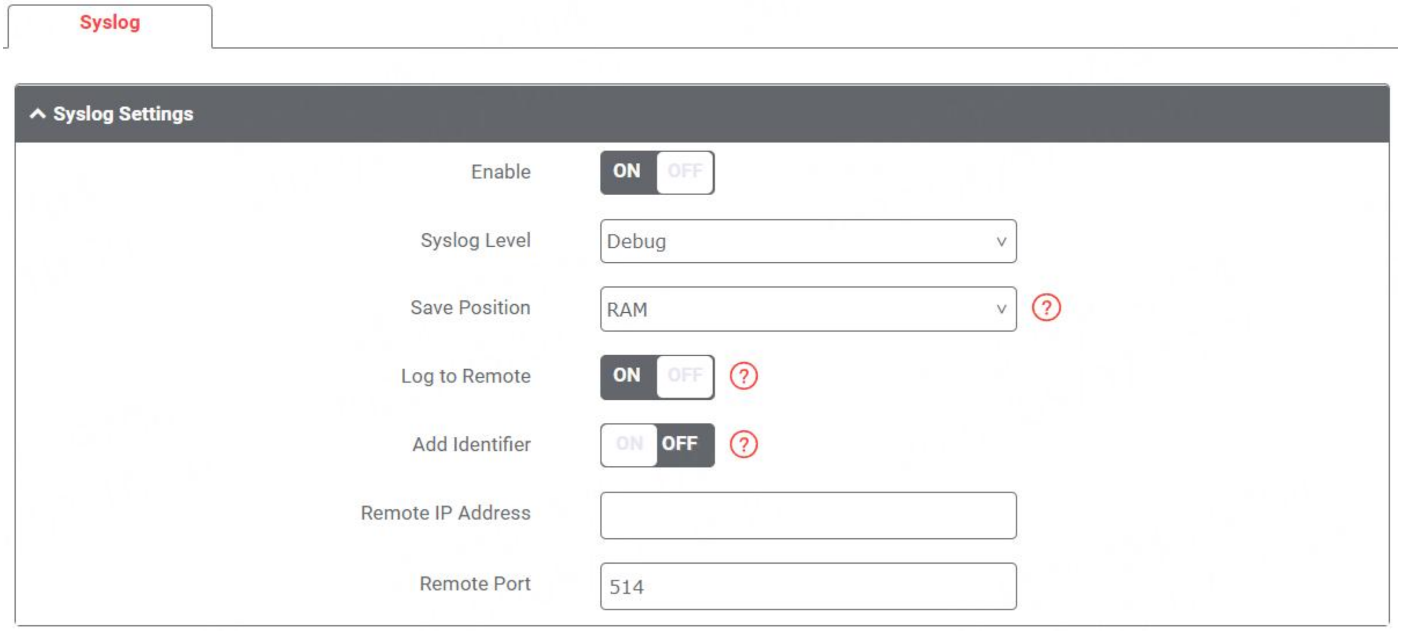
Enable: ON

Syslog Level: Debug

Save Position: RAM

Log to Remote: OFF

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



Syslog

^ Syslog Settings

Enable: ON

Syslog Level: Debug

Save Position: RAM

Log to Remote: ON

Add Identifier: OFF

Remote IP Address:

Remote Port: 514

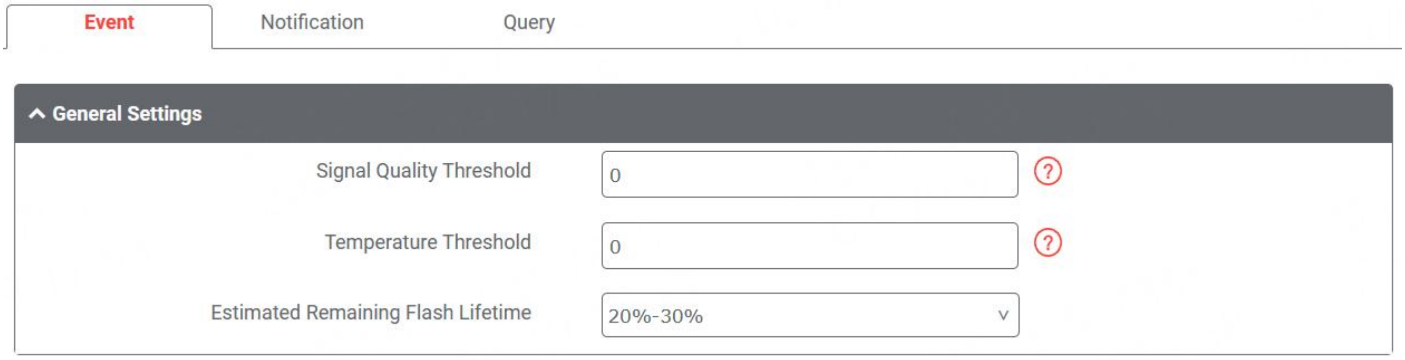
Item	Description	Default
Enable	Click the toggle button to enable/disable the Syslog settings option.	ON
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. The lower level will output more syslog in details.	Debug
Save Position	Select the save position from “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	RAM

	Memory) for a long time.	
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



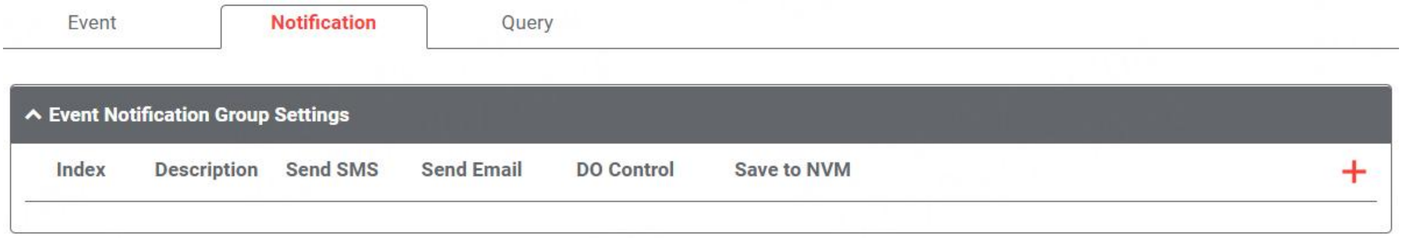
Signal Quality Threshold: 0

Temperature Threshold: 0

Estimated Remaining Flash Lifetime: 20%-30%

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

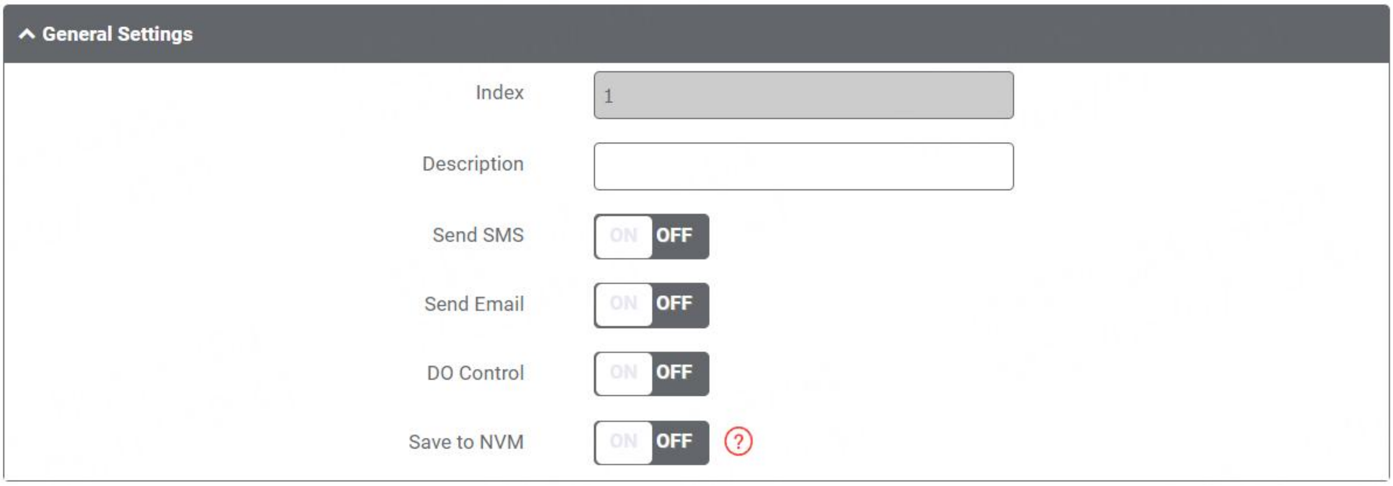


Event | Notification | Query

Event Notification Group Settings

Index | Description | Send SMS | Send Email | DO Control | Save to NVM | +

Click + button to add an Event parameters.



General Settings

Index: 1

Description:

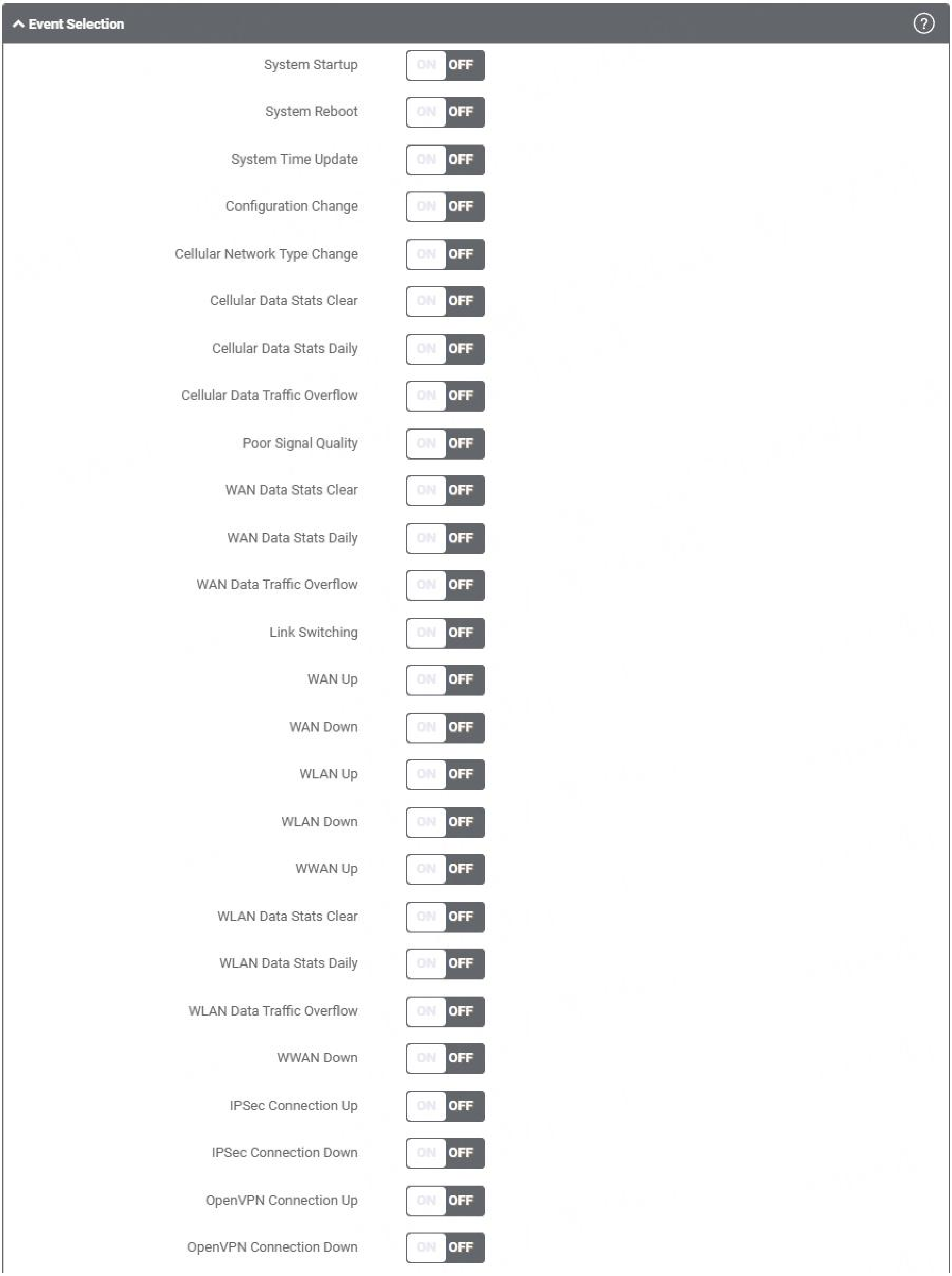
Send SMS: ON OFF

Send Email: ON OFF

DO Control: ON OFF

Save to NVM: ON OFF ?

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



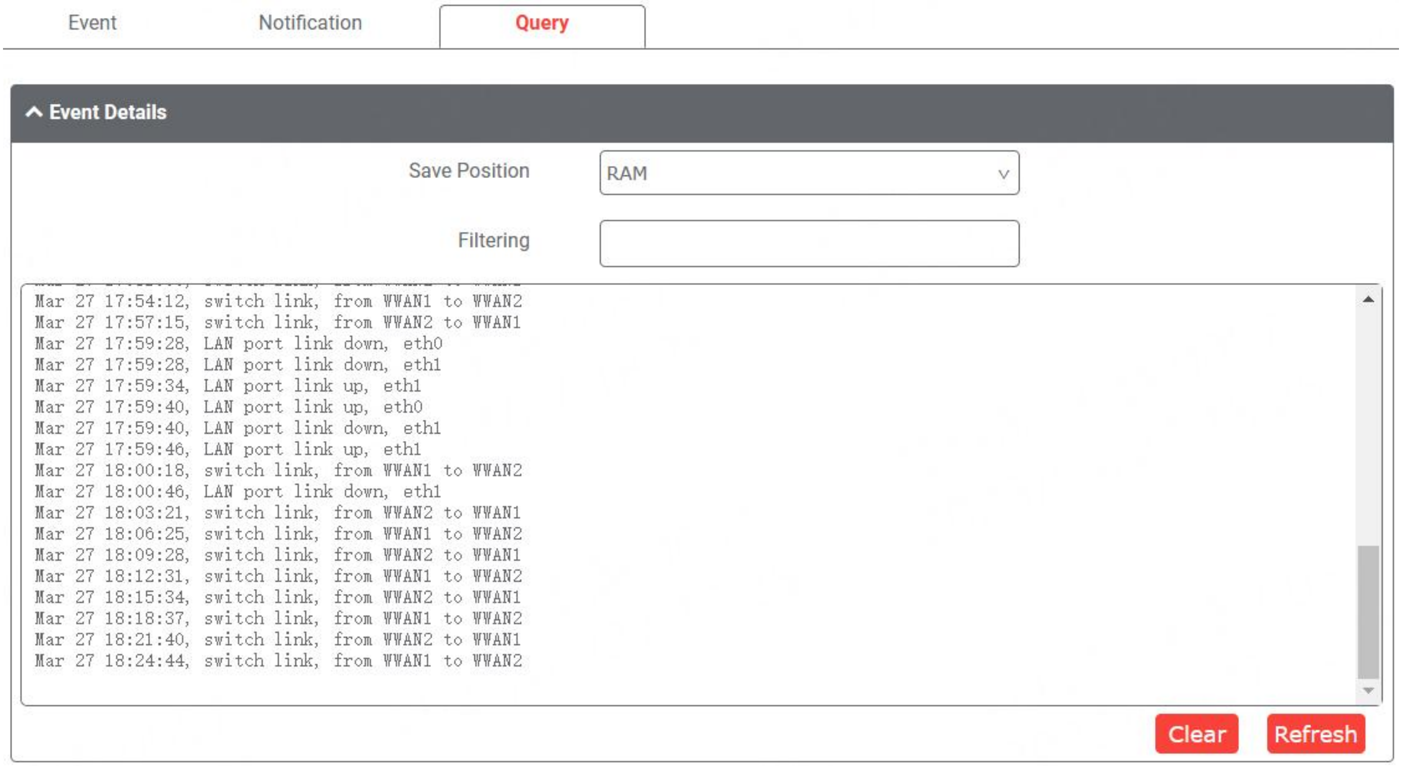
Event Selection

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



Save Position: RAM

Filtering:

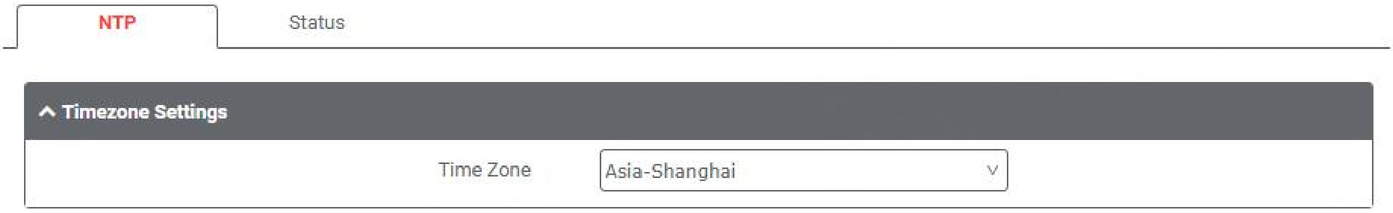
```
Mar 27 17:54:12, switch link, from WWAN1 to WWAN2
Mar 27 17:57:15, switch link, from WWAN2 to WWAN1
Mar 27 17:59:28, LAN port link down, eth0
Mar 27 17:59:28, LAN port link down, eth1
Mar 27 17:59:34, LAN port link up, eth1
Mar 27 17:59:40, LAN port link up, eth0
Mar 27 17:59:40, LAN port link down, eth1
Mar 27 17:59:46, LAN port link up, eth1
Mar 27 18:00:18, switch link, from WWAN1 to WWAN2
Mar 27 18:00:46, LAN port link down, eth1
Mar 27 18:03:21, switch link, from WWAN2 to WWAN1
Mar 27 18:06:25, switch link, from WWAN1 to WWAN2
Mar 27 18:09:28, switch link, from WWAN2 to WWAN1
Mar 27 18:12:31, switch link, from WWAN1 to WWAN2
Mar 27 18:15:34, switch link, from WWAN2 to WWAN1
Mar 27 18:18:37, switch link, from WWAN1 to WWAN2
Mar 27 18:21:40, switch link, from WWAN2 to WWAN1
Mar 27 18:24:44, switch link, from WWAN1 to WWAN2
```

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.

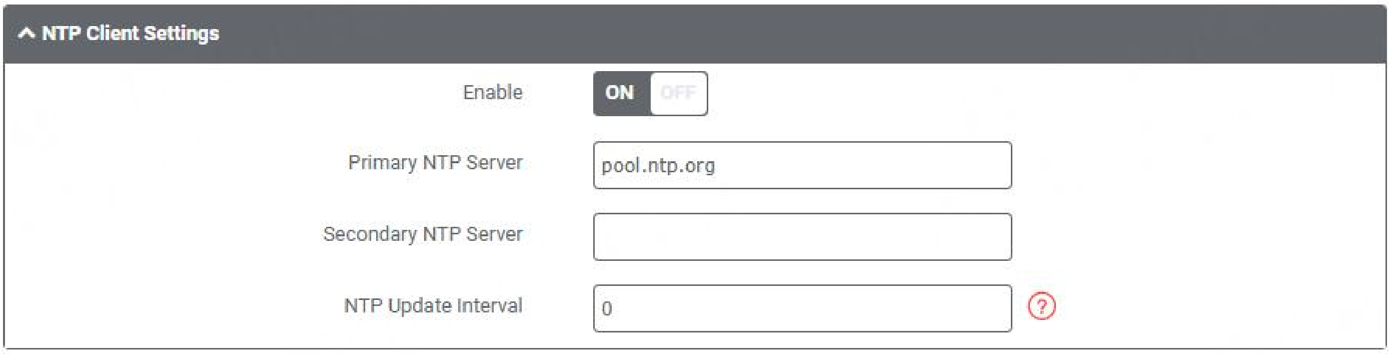
NTP



^ Timezone Settings

Time Zone: Asia-Shanghai

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



^ NTP Client Settings

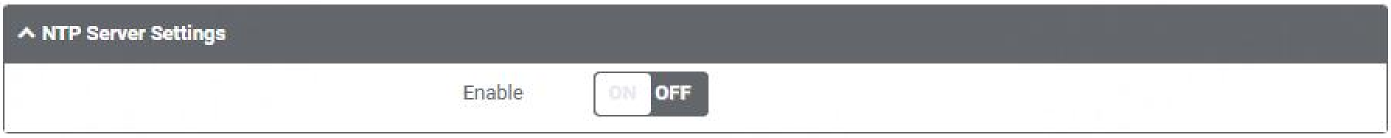
Enable: ON OFF

Primary NTP Server: pool.ntp.org

Secondary NTP Server:

NTP Update Interval: 0

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

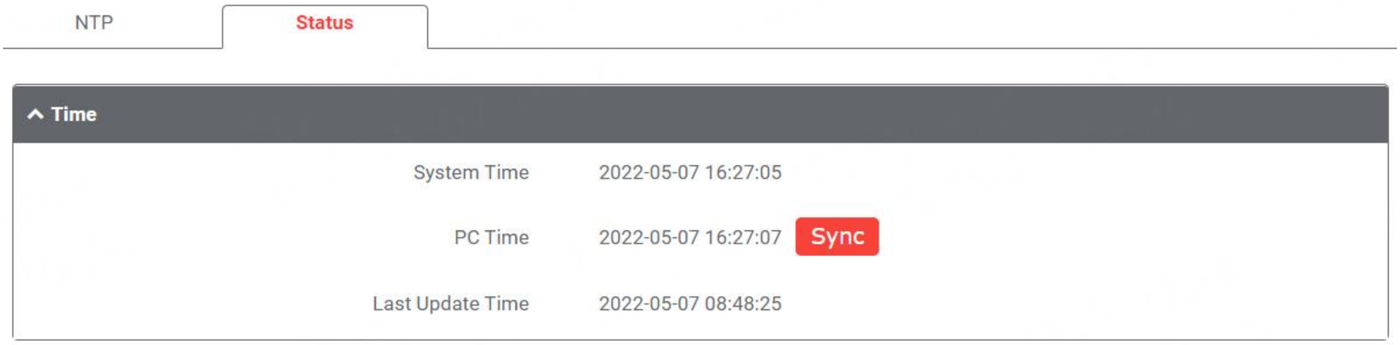


Enable ON OFF

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.



System Time 2022-05-07 16:27:05

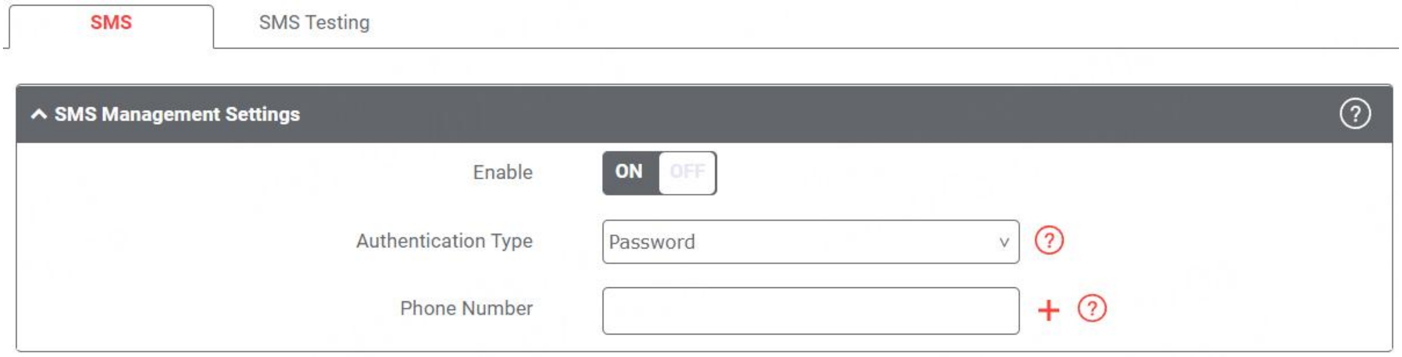
PC Time 2022-05-07 16:27:07

Last Update Time 2022-05-07 08:48:25

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



Enable ON OFF

Authentication Type Password

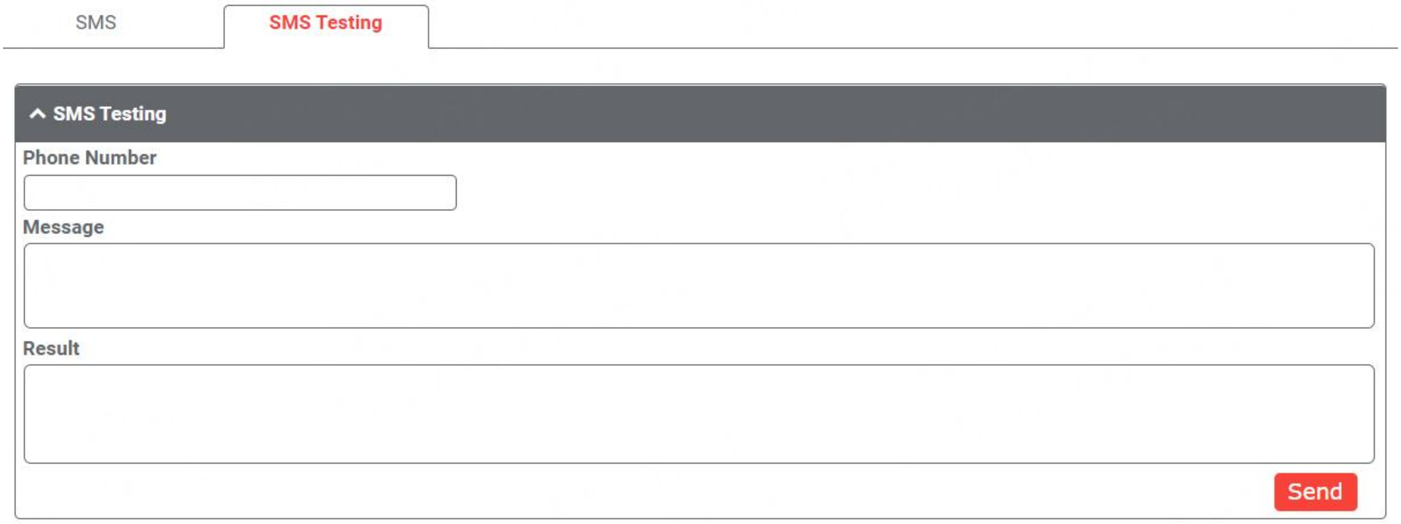
Phone Number

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	Select Authentication Type from "Password", "Phonenum" or "Both".	Password

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

SMS Testing

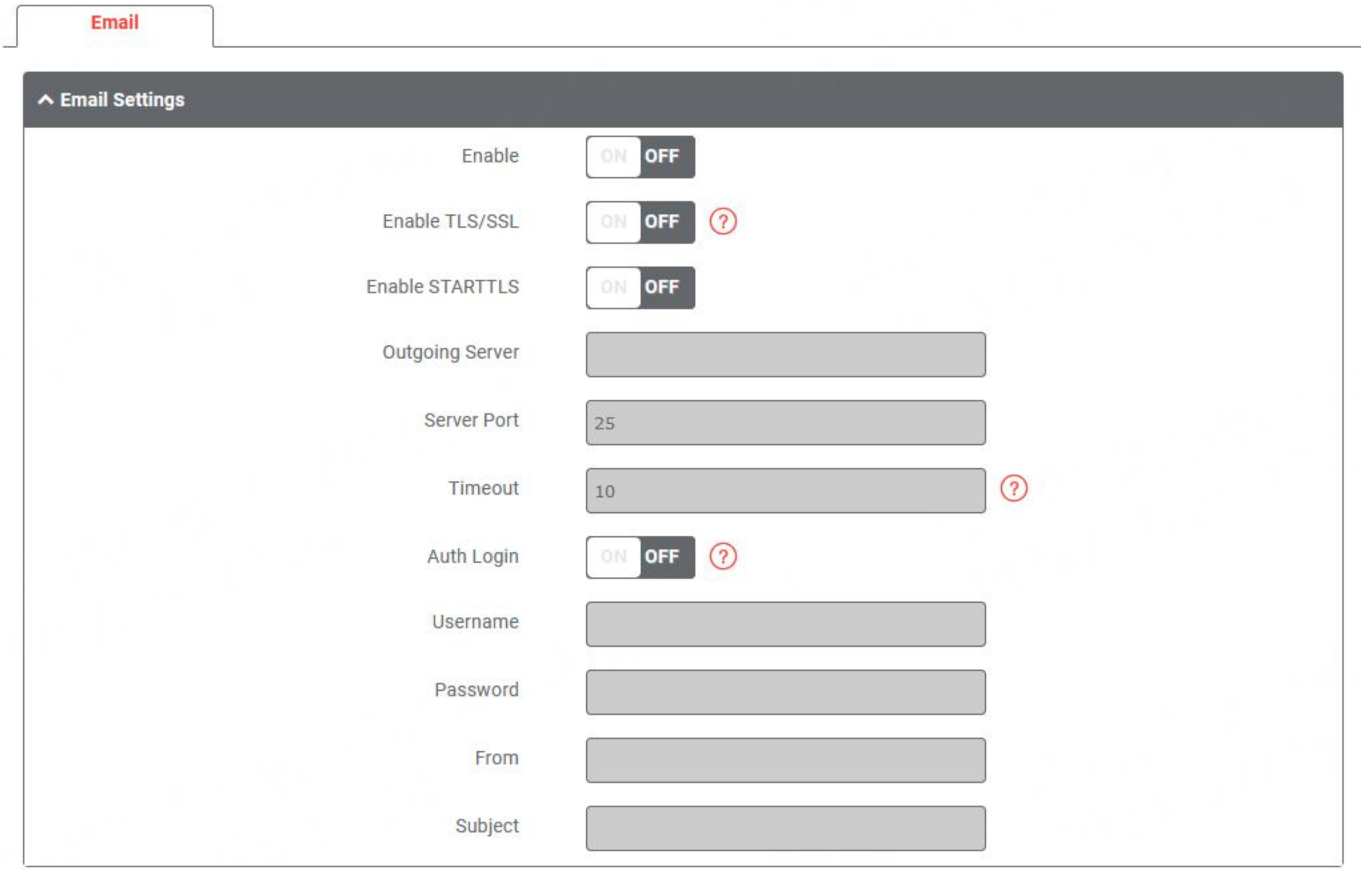
User can test the current SMS service whether it is available in this section.



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

3.6.5 Email

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



Email

^ Email Settings

Enable: ON OFF

Enable TLS/SSL: ON OFF

Enable STARTTLS: ON OFF

Outgoing Server:

Server Port: 25

Timeout: 10

Auth Login: ON OFF

Username:

Password:

From:

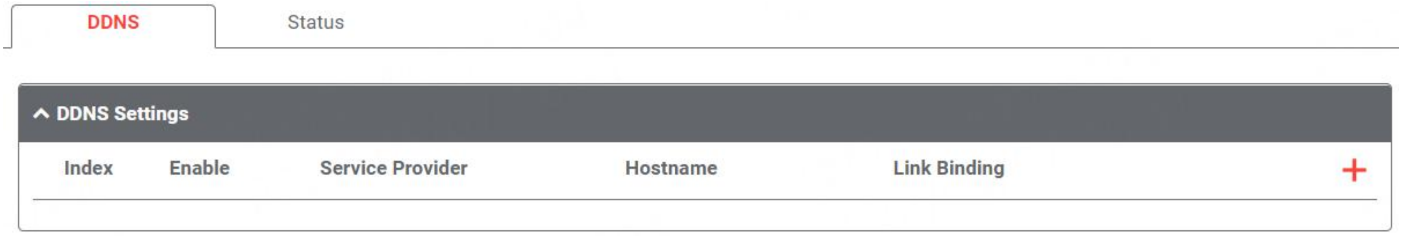
Subject:

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

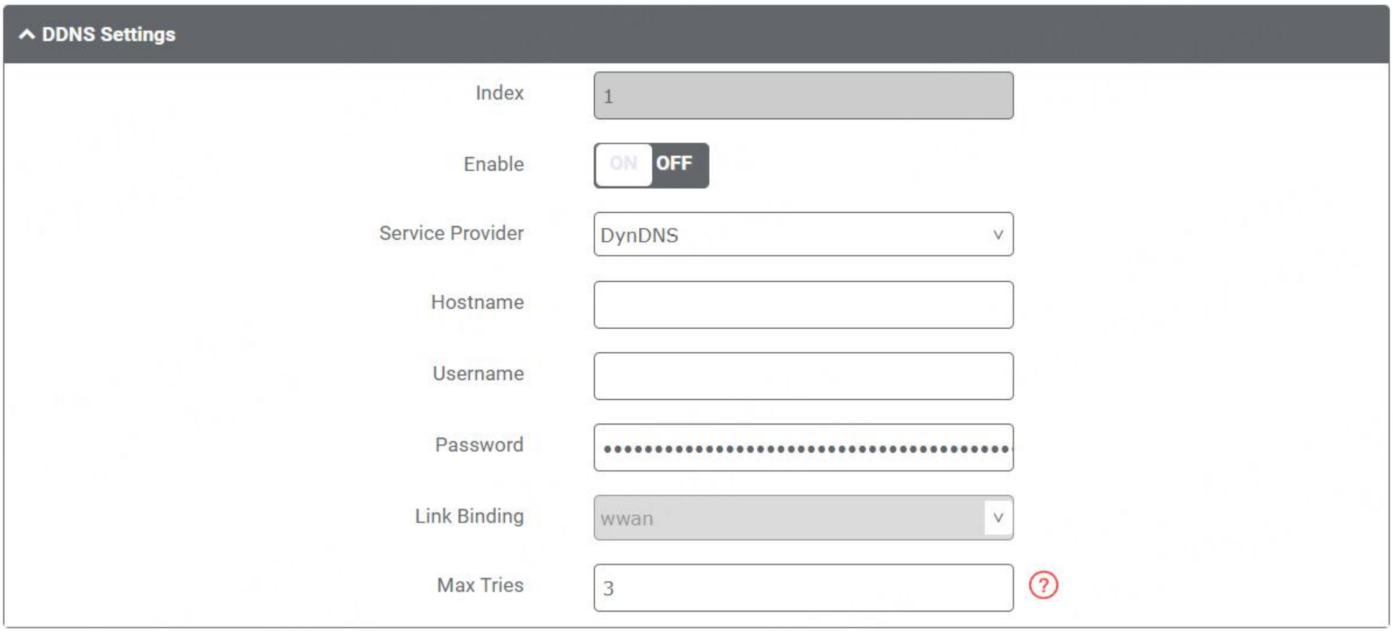
This section allows you to set the DDNS parameters. The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows you whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that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



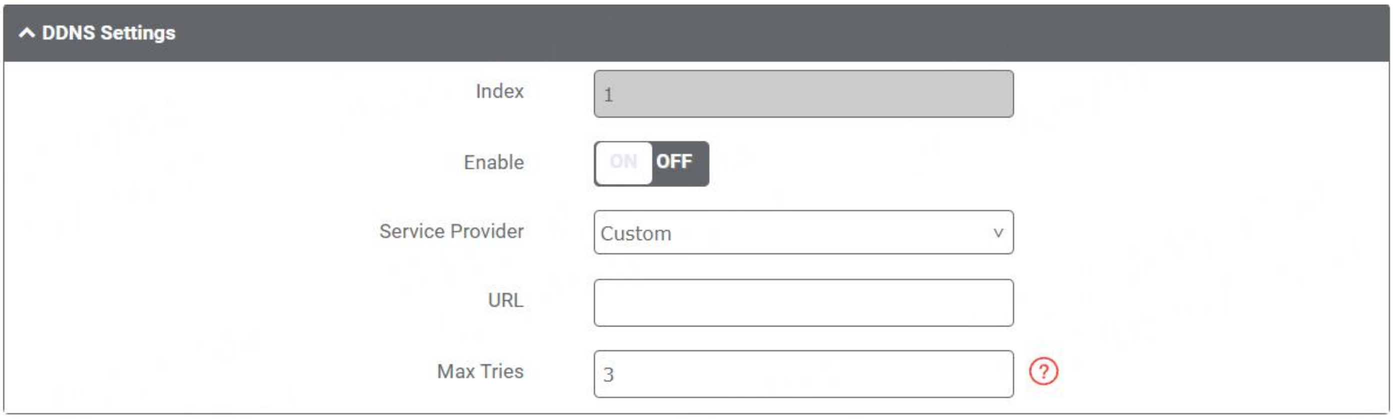
Index	Enable	Service Provider	Hostname	Link Binding	+

Click + to add a new Dynamic Domain Name Server.



Index	1
Enable	ON OFF
Service Provider	DynDNS
Hostname	
Username	
Password	•••
Link Binding	wwan
Max Tries	3

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



DDNS Settings

Index: 1

Enable: ON OFF

Service Provider: Custom

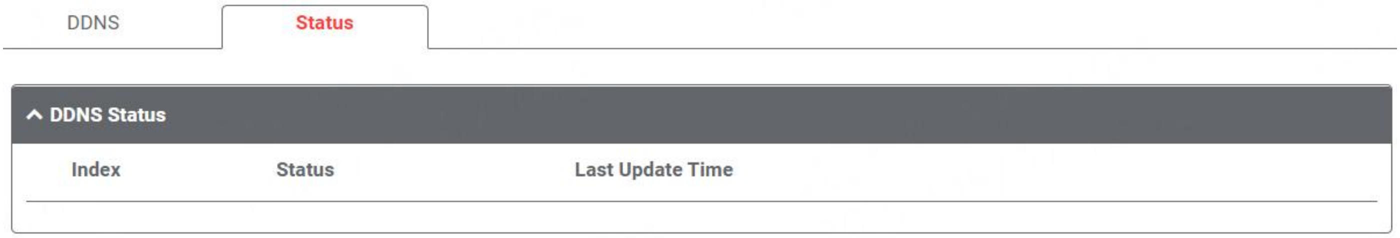
URL:

Max Tries: 3

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.



DDNS Status

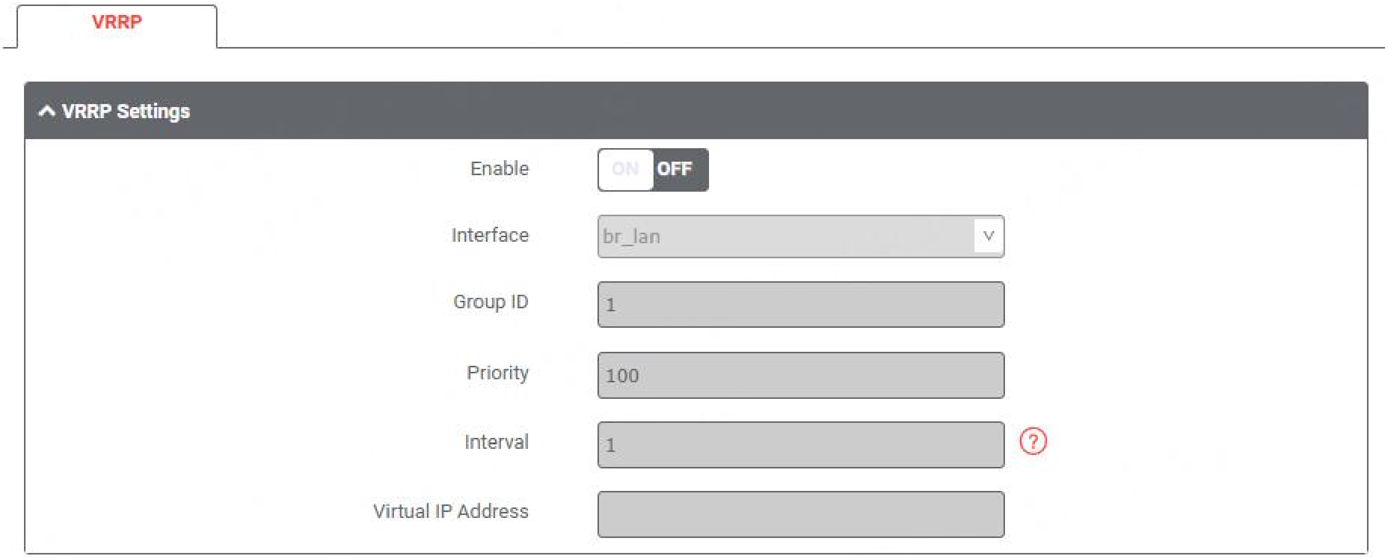
Index	Status	Last Update Time

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



Enable ON OFF

Interface br_lan

Group ID 1

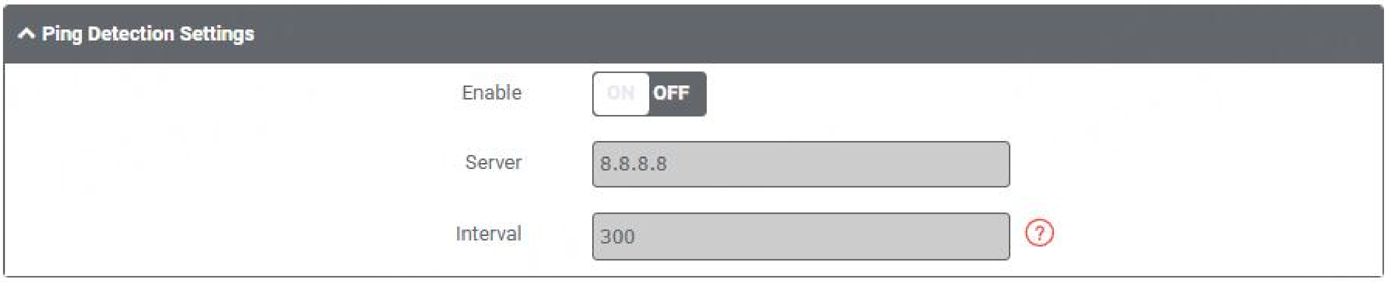
Priority 100

Interval 1

Virtual IP Address

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



Enable ON OFF

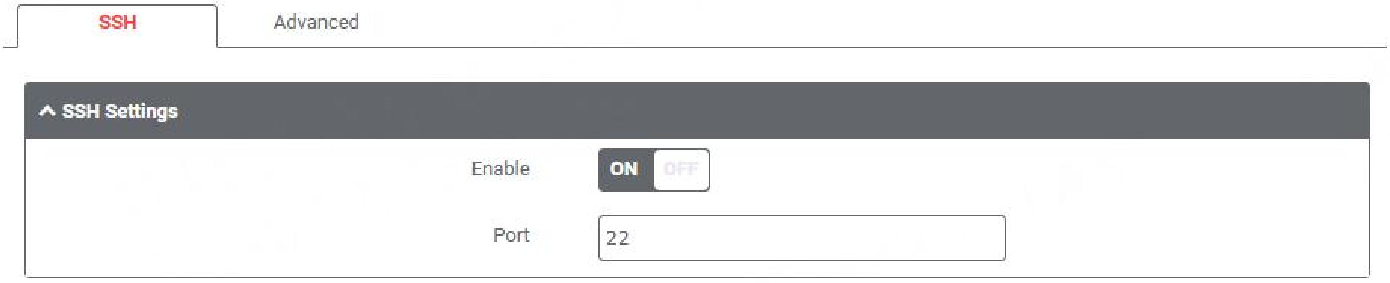
Server 8.8.8.8

Interval 300

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

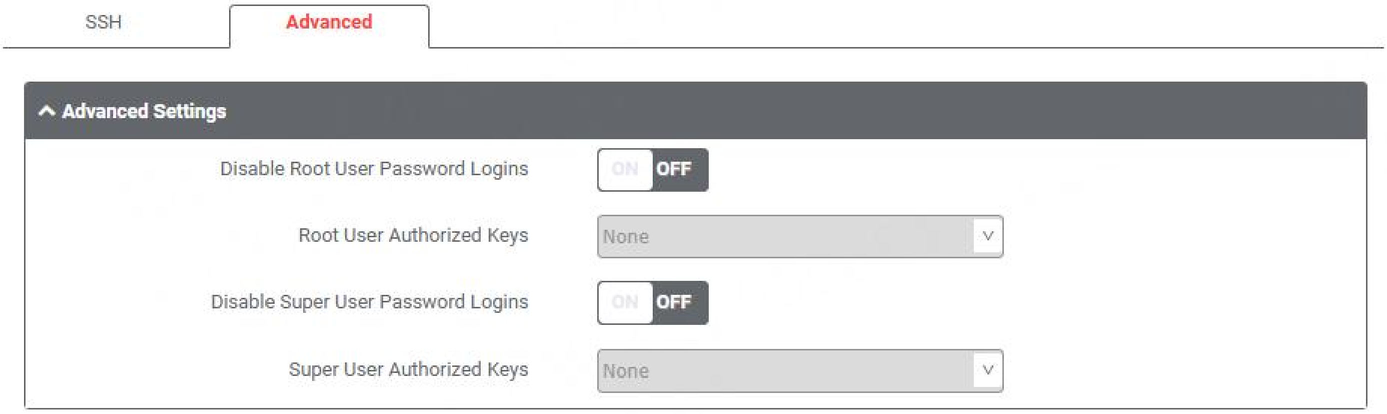
The gateway supports SSH password access and key access.



Enable: ON

Port: 22

Item	Description	Default
Enable	Click the toggle button to enable/disable this option. Once enabled, you can access the gateway via SSH.	ON
Port	Set the port for SSH access.	22



Disable Root User Password Logins: OFF

Root User Authorized Keys: None

Disable Super User Password Logins: OFF

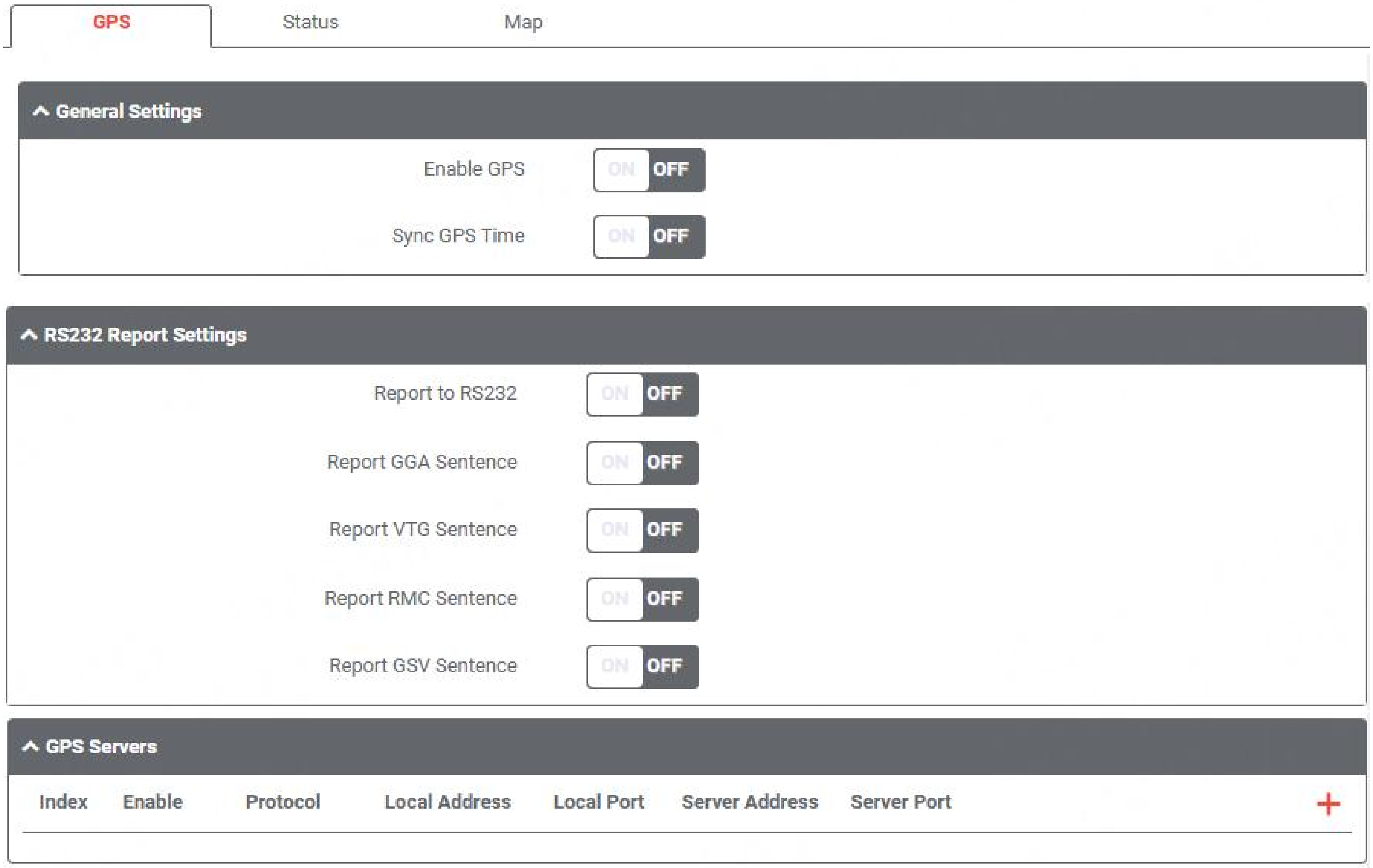
Super User Authorized Keys: None

Item	Description	Default
Disable Root Password Login	Click the toggle button to enable/disable this option. Once enabled, you cannot access the gateway via SSH using a username and password. In this case, only keys can be used for login.	OFF
Disable Super Password Login	Click the toggle button to enable/disable this option. Once enabled, you cannot access the gateway via SSH using a username and password. In this case, only keys 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



General Settings

Enable GPS	ON OFF
Sync GPS Time	ON OFF

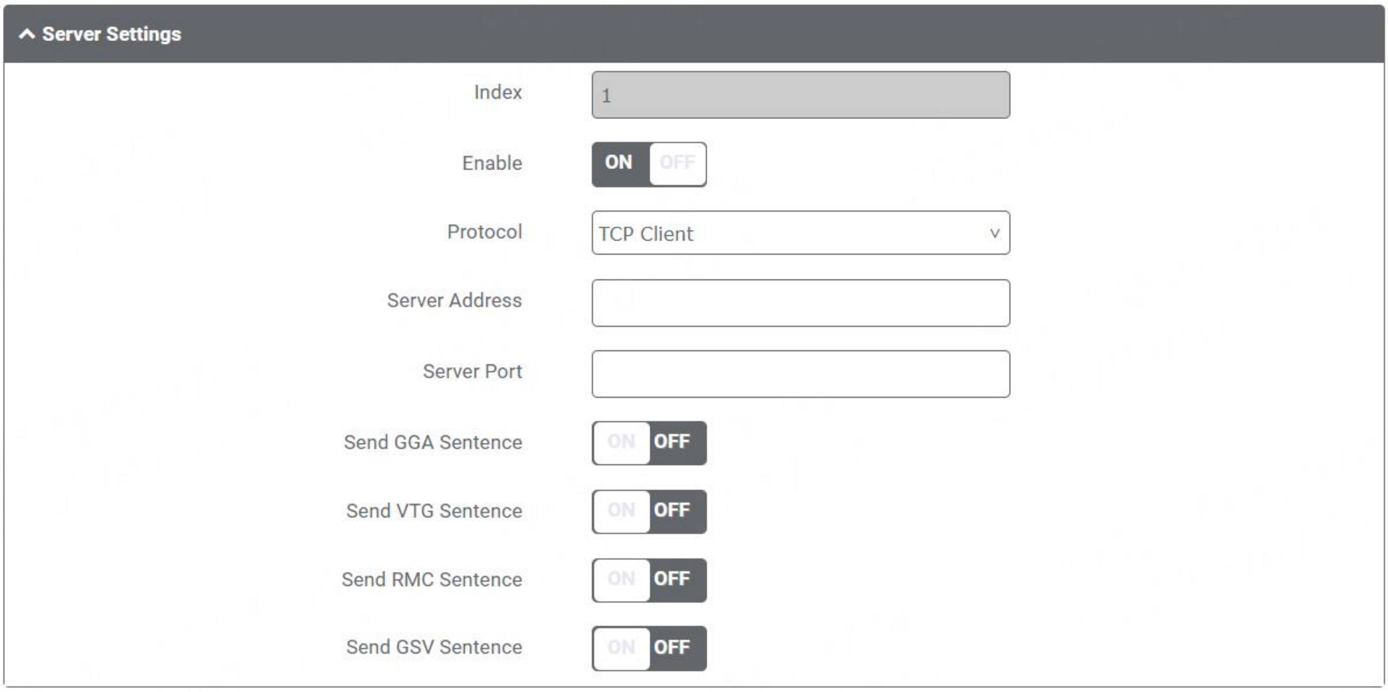
RS232 Report Settings

Report to RS232	ON OFF
Report GGA Sentence	ON OFF
Report VTG Sentence	ON OFF
Report RMC Sentence	ON OFF
Report GSV Sentence	ON OFF

GPS Servers

Index	Enable	Protocol	Local Address	Local Port	Server Address	Server Port	+

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



Index: 1

Enable: ON OFF

Protocol: TCP Client

Server Address:

Server Port:

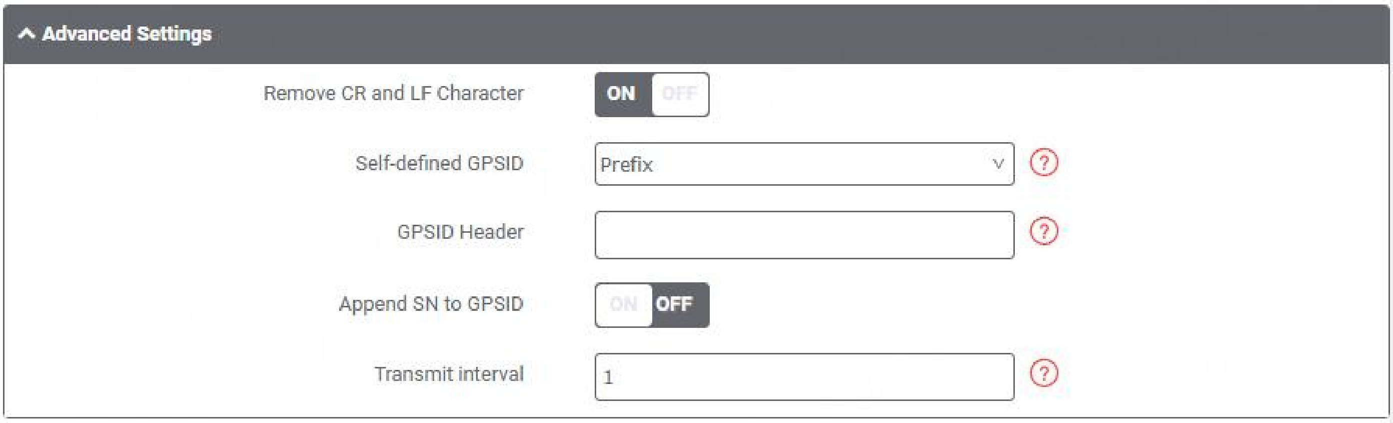
Send GGA Sentence: ON OFF

Send VTG Sentence: ON OFF

Send RMC Sentence: ON OFF

Send GSV Sentence: ON OFF

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



Remove CR and LF Character: ON OFF

Self-defined GPSID: Prefix

GPSID Header:

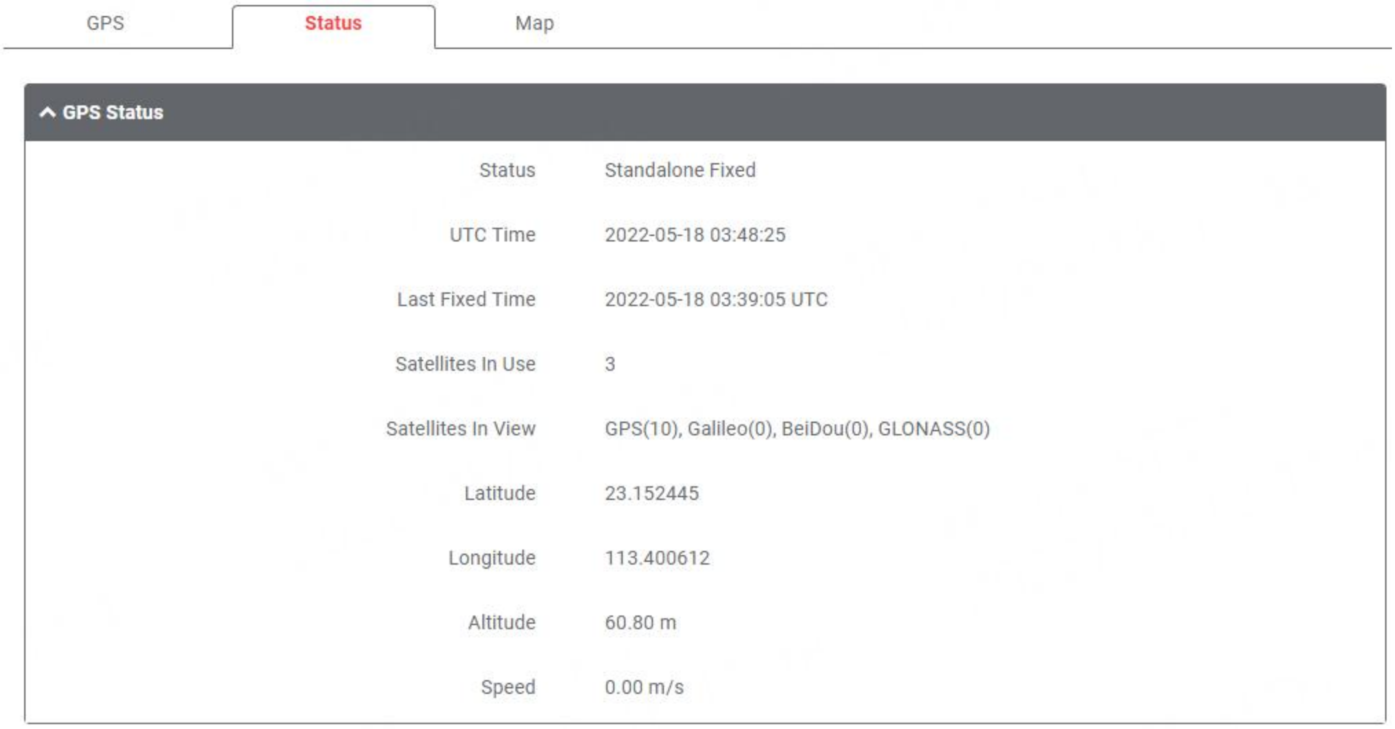
Append SN to GPSID: ON OFF

Transmit interval: 1

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
GPSID Header	Enter the GPS ID Header, usually 7 uppercase letters	Null
Append SN to GPSID	Click the toggle button to enable/disable this option.	OFF
Transmit Interval	Enter the data reporting period. 0 means no data upload.	1

Status



Status Standalone Fixed

UTC Time 2022-05-18 03:48:25

Last Fixed Time 2022-05-18 03:39:05 UTC

Satellites In Use 3

Satellites In View GPS(10), Galileo(0), BeiDou(0), GLONASS(0)

Latitude 23.152445

Longitude 113.400612

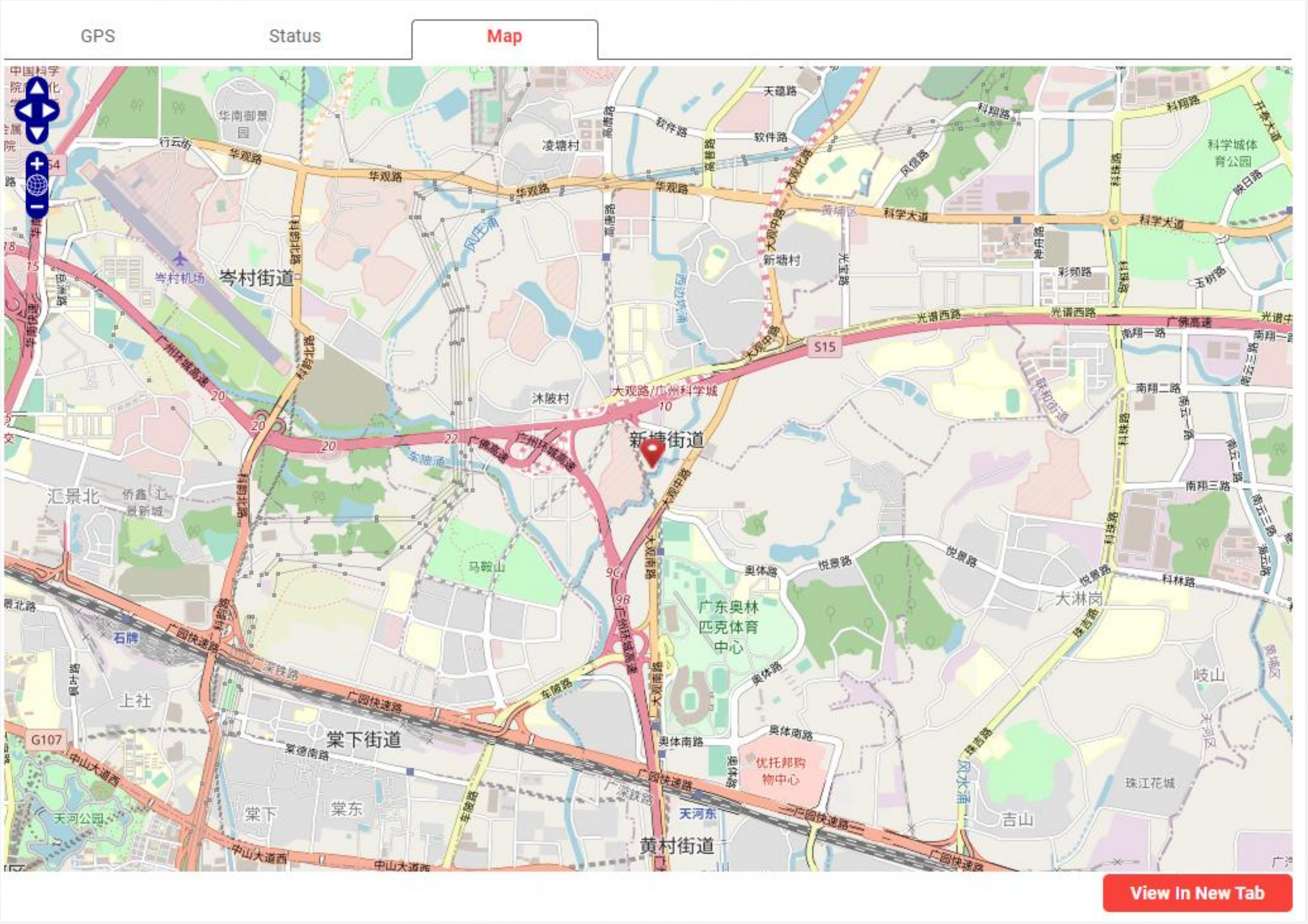
Altitude 60.80 m

Speed 0.00 m/s

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.

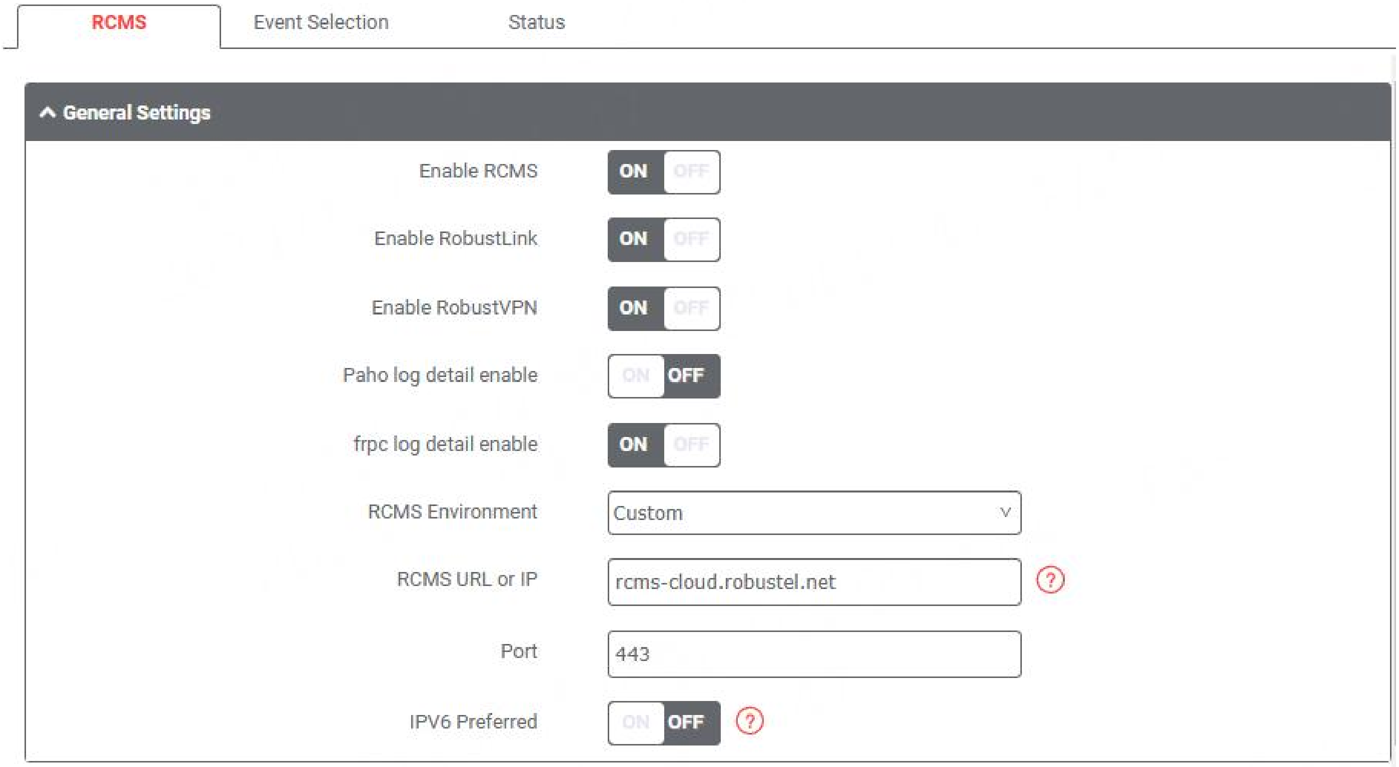


Click the View In New Tab button to view in a new tab.

3.6.10 RCMS

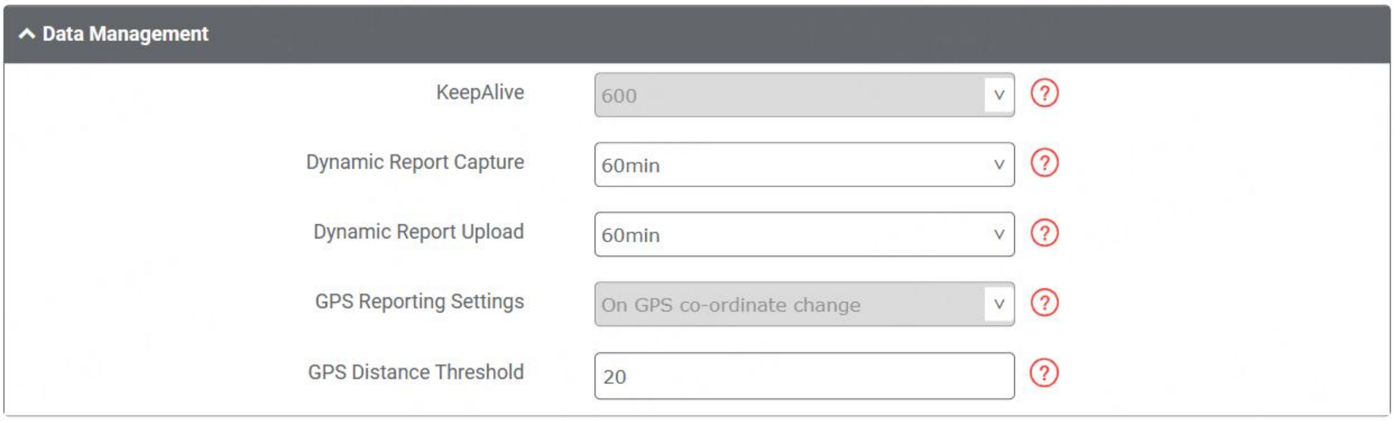
This section allows you to set the RCMS parameters. Robustel Cloud Manager Service (RCMS) is a modular IoT cloud software platform compatible with all Robustel products.

RCMS



Enable RCMS: ON
Enable RobustLink: ON
Enable RobustVPN: ON
Paho log detail enable: OFF
frpc log detail enable: ON
RCMS Environment: Custom
RCMS URL or IP: rcms-cloud.robustel.net
Port: 443
IPV6 Preferred: OFF

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.	ON
Enable RobustVPN	Click the toggle button to enable/disable this option.	ON
Paho log detail enable	Click the toggle button to enable/disable this option.	OFF
frpc log detail enable	Click the toggle button to enable/disable this option.	ON
RCMS Environment	Select RCMS Environment	Custom
RCMS URL or IP	Enter IP Address or URL of RCMS server.	rcms-cloud.robustel.net
Port	Enter the Port of RCMS.	443
IPV6 Preferred	Click the toggle button to enable/disable this option. Prioritize using IPv6 to connect to RCMS.	OFF



Data Management

KeepAlive: 600

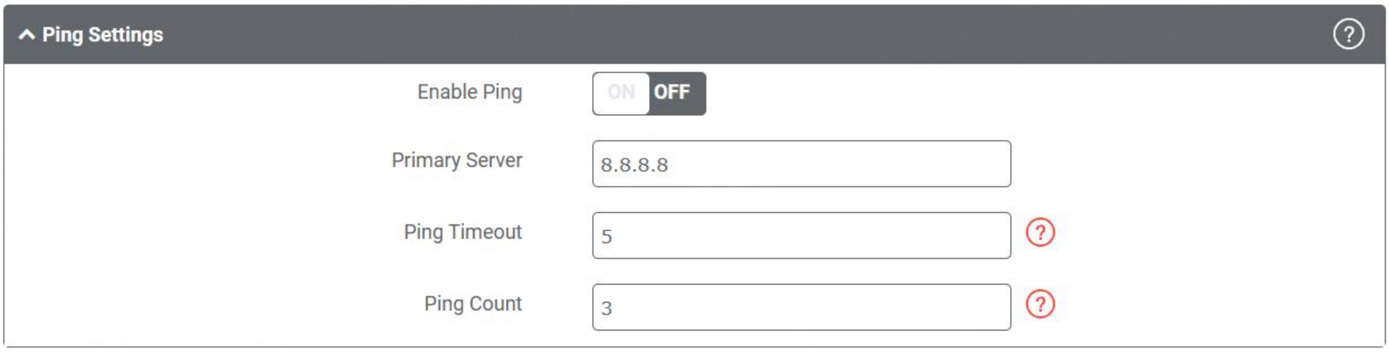
Dynamic Report Capture: 60min

Dynamic Report Upload: 60min

GPS Reporting Settings: On GPS co-ordinate change

GPS Distance Threshold: 20

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



Ping Settings

Enable Ping: ON OFF

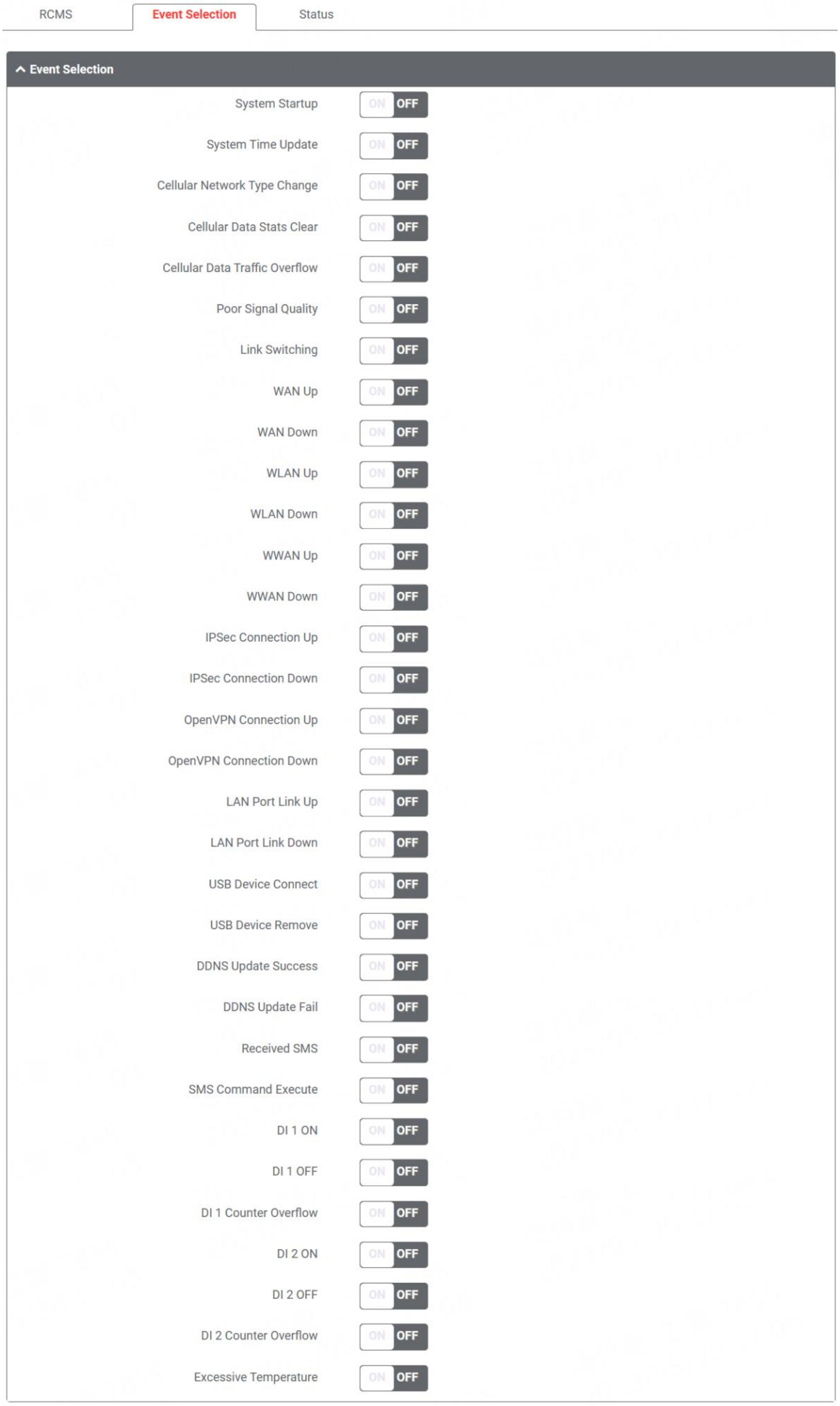
Primary Server: 8.8.8.8

Ping Timeout: 5

Ping Count: 3

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

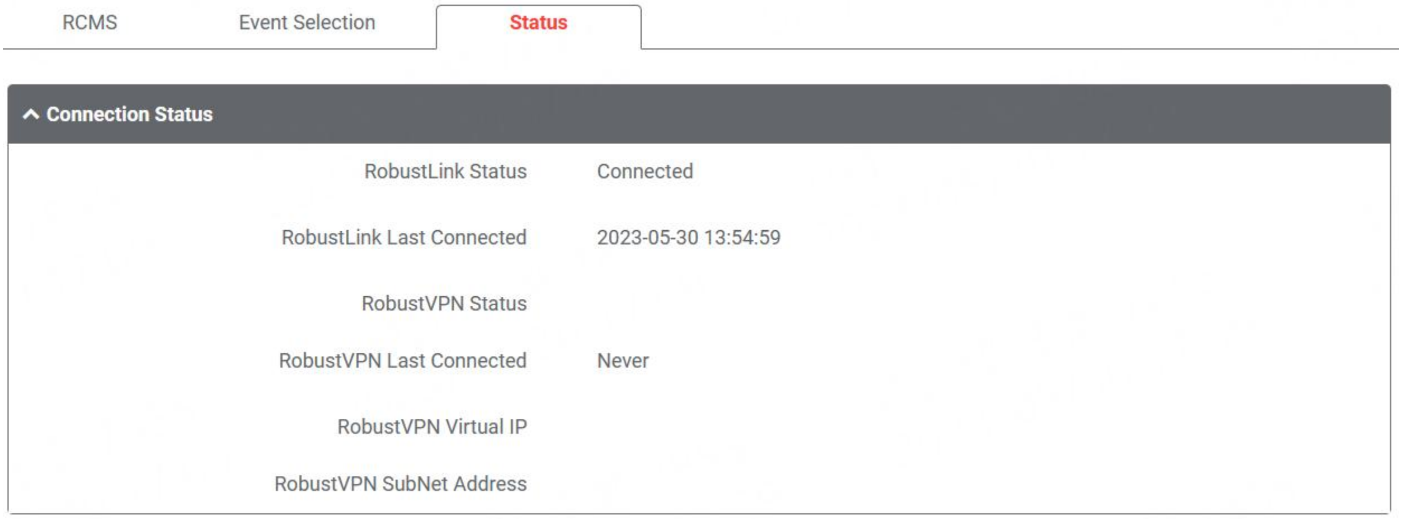
Event Selection



Event Selection

System Startup	ON OFF
System Time Update	ON OFF
Cellular Network Type Change	ON OFF
Cellular Data Stats Clear	ON OFF
Cellular Data Traffic Overflow	ON OFF
Poor Signal Quality	ON OFF
Link Switching	ON OFF
WAN Up	ON OFF
WAN Down	ON OFF
WLAN Up	ON OFF
WLAN Down	ON OFF
WWAN Up	ON OFF
WWAN Down	ON OFF
IPSec Connection Up	ON OFF
IPSec Connection Down	ON OFF
OpenVPN Connection Up	ON OFF
OpenVPN Connection Down	ON OFF
LAN Port Link Up	ON OFF
LAN Port Link Down	ON OFF
USB Device Connect	ON OFF
USB Device Remove	ON OFF
DDNS Update Success	ON OFF
DDNS Update Fail	ON OFF
Received SMS	ON OFF
SMS Command Execute	ON OFF
DI 1 ON	ON OFF
DI 1 OFF	ON OFF
DI 1 Counter Overflow	ON OFF
DI 2 ON	ON OFF
DI 2 OFF	ON OFF
DI 2 Counter Overflow	ON OFF
Excessive Temperature	ON OFF

Status



RobustLink Status Connected

RobustLink Last Connected 2023-05-30 13:54:59

RobustVPN Status

RobustVPN Last Connected Never

RobustVPN Virtual IP

RobustVPN SubNet Address

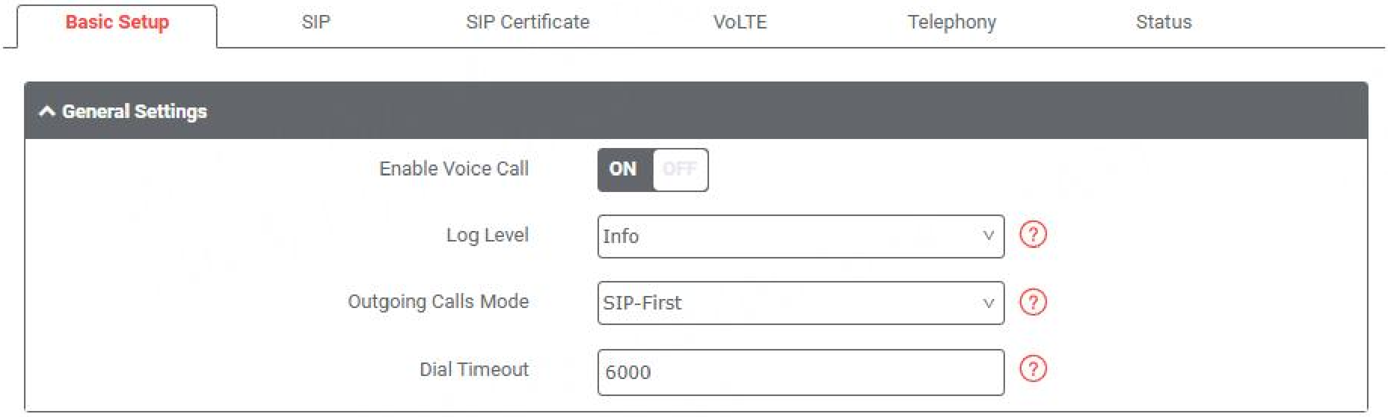
Item	Description
RobustLink Status	Show the status of RobustLink
RobustelLink Last Connected	Show the last connected times of RobustLink
RobustVPN Status	Show the status of RobustVPN
RobustVPN Last Connected	Show the last connected times of RobustVPN
RobustVPN Virtual IP	Show the virtual IP of RobustVPN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

3.6.11 Voice Call

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.

- EV8100 support Voice Call feature.

Basic Setup



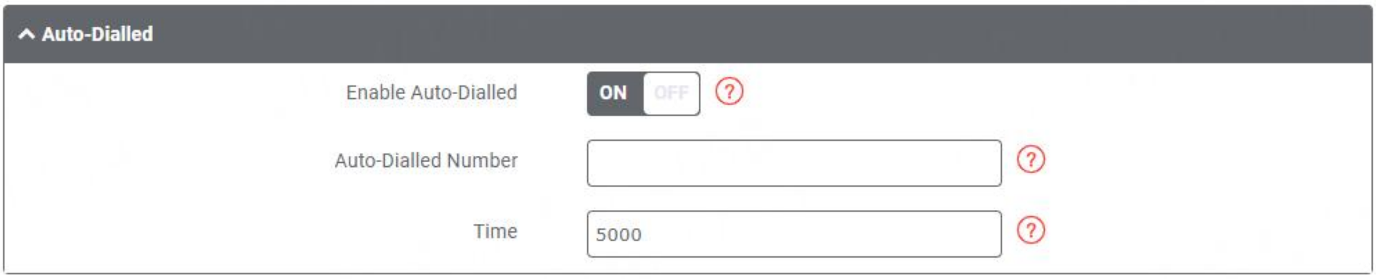
Enable Voice Call: ON OFF

Log Level: Info

Outgoing Calls Mode: SIP-First

Dial Timeout: 6000

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



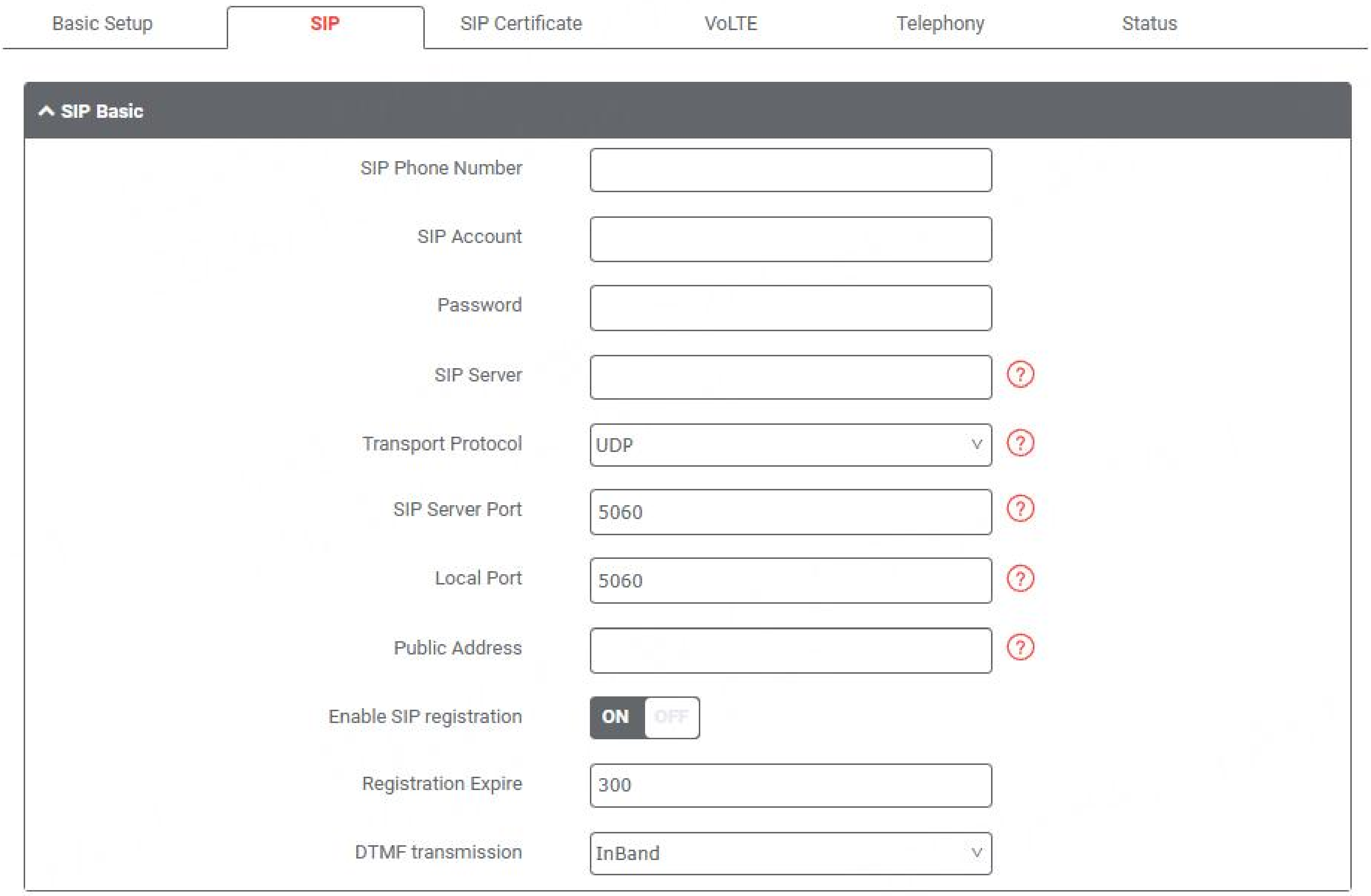
Enable Auto-Dialled: ON OFF

Auto-Dialled Number:

Time: 5000

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.	Null
Time	The time in milliseconds for the call to be made when the user does not dial after off-hooking.	5000

SIP



SIP Phone Number

SIP Account

Password

SIP Server

Transport Protocol: UDP

SIP Server Port: 5060

Local Port: 5060

Public Address

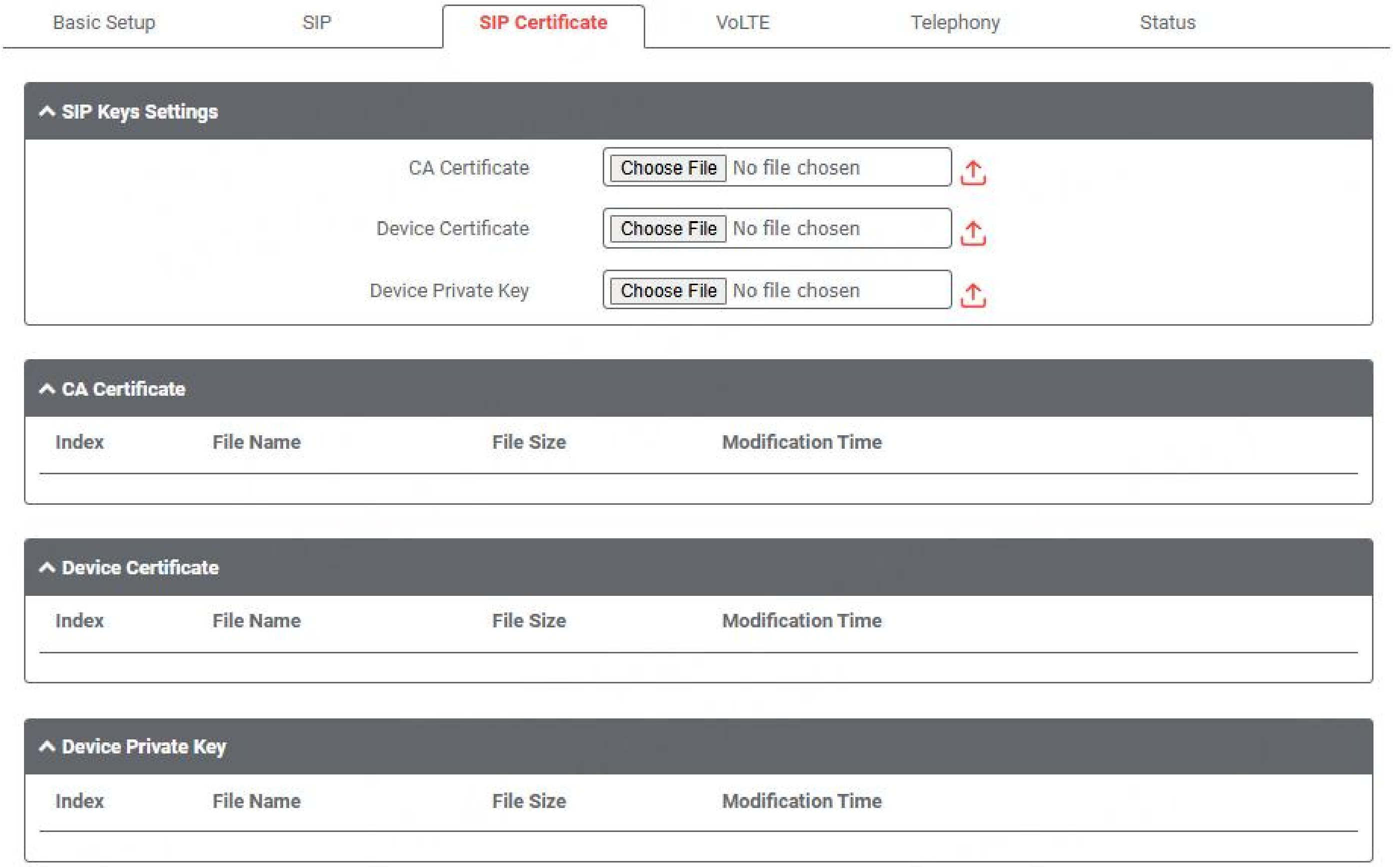
Enable SIP registration: ON OFF

Registration Expire: 300

DTMF transmission: InBand

Item	Description	Default
SIP Phone Number	Enter the phone number to 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



SIP Keys Settings

CA Certificate: Choose File No file chosen

Device Certificate: Choose File No file chosen

Device Private Key: Choose File No file chosen

CA Certificate

Index	File Name	File Size	Modification Time

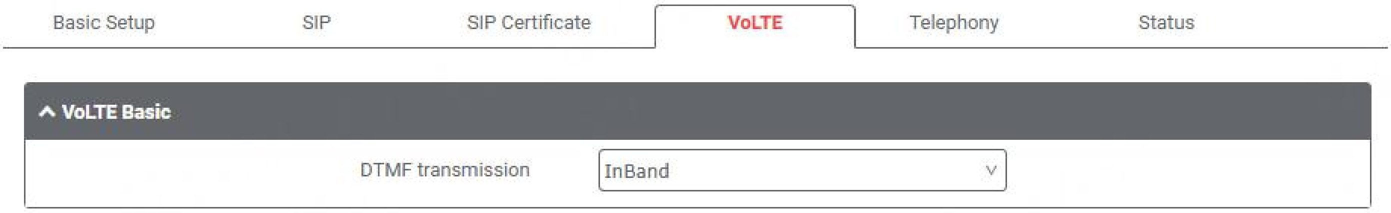
Device Certificate

Index	File Name	File Size	Modification Time

Device Private Key

Index	File Name	File Size	Modification Time

VoLTE

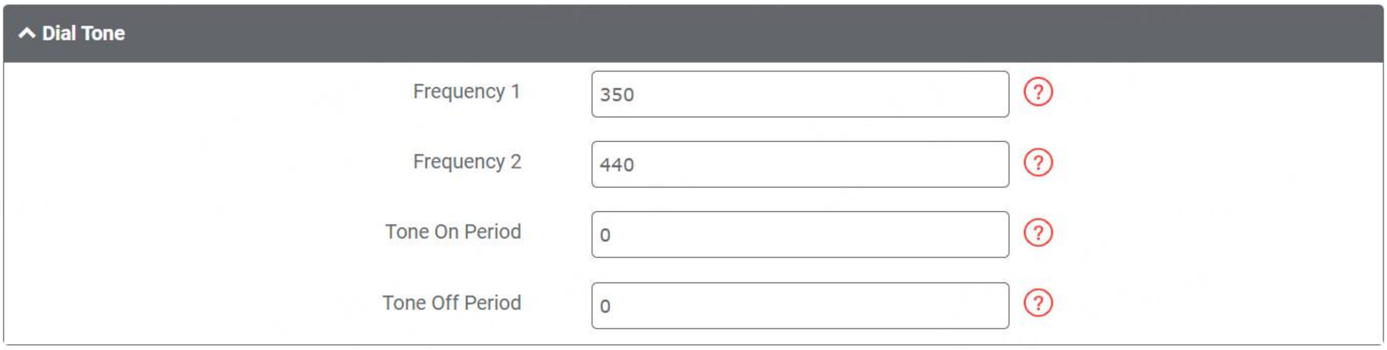


VoLTE Basic

DTMF transmission: InBand

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

Telephony



Dial Tone

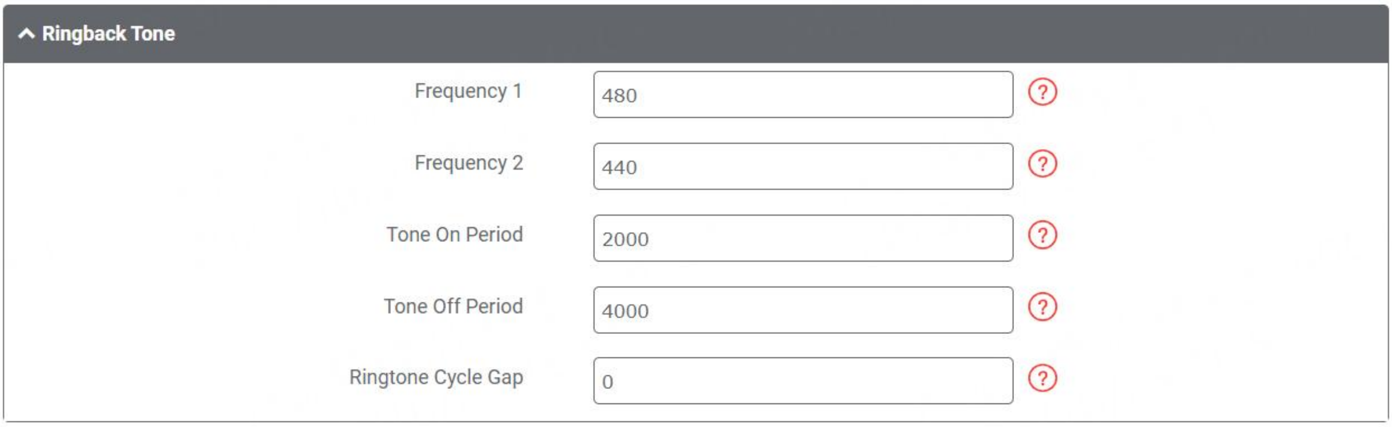
Frequency 1: 350

Frequency 2: 440

Tone On Period: 0

Tone Off Period: 0

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



Ringback Tone

Frequency 1: 480

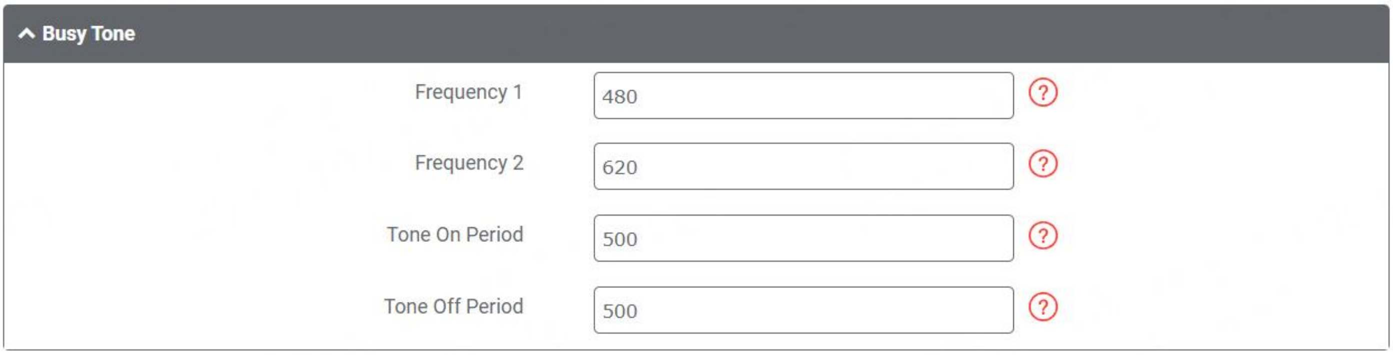
Frequency 2: 440

Tone On Period: 2000

Tone Off Period: 4000

Ringtone Cycle Gap: 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



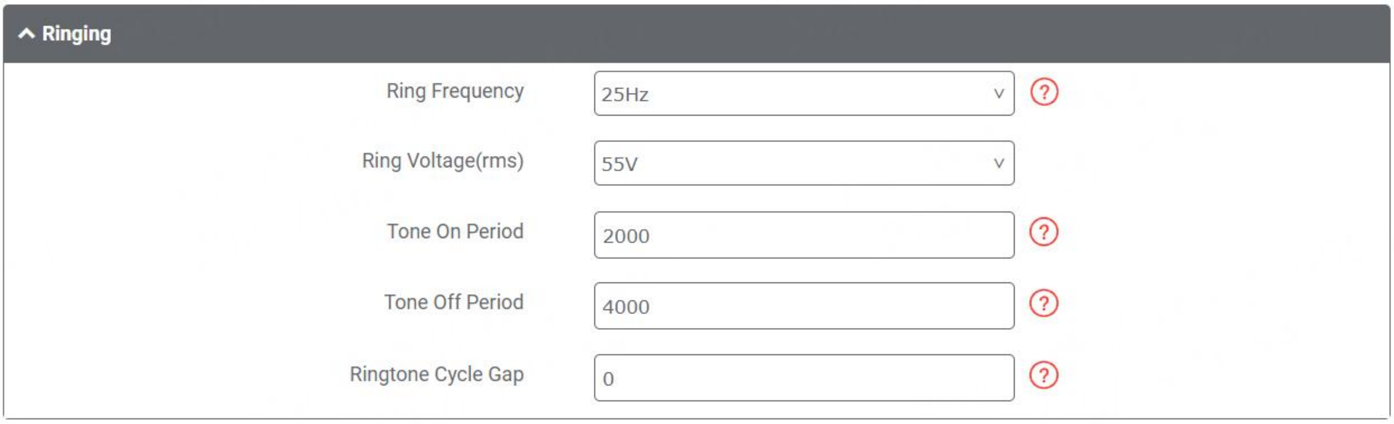
Frequency 1: 480

Frequency 2: 620

Tone On Period: 500

Tone Off Period: 500

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



Ring Frequency: 25Hz

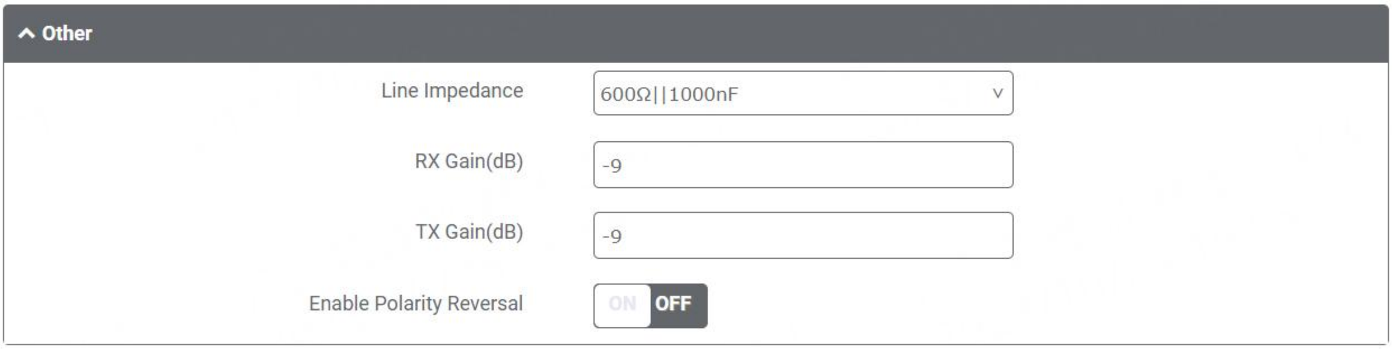
Ring Voltage(rms): 55V

Tone On Period: 2000

Tone Off Period: 4000

Ringtone Cycle Gap: 0

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



Line Impedance: 600Ω||1000nF

RX Gain(dB): -9

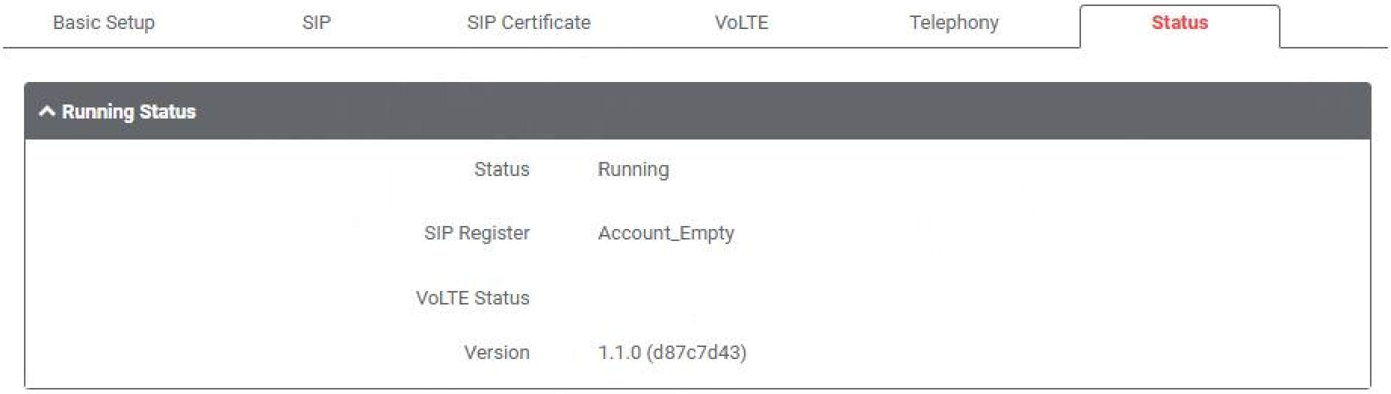
TX Gain(dB): -9

Enable Polarity Reversal: ON OFF

Item	Description	Default
Line Impendance	Select from“600Ω”,“270Ω+750Ω||150nF”,“370Ω+620Ω||310nF”,“220Ω+820Ω||120nF”, “600Ω||1000nF”,“200Ω+680Ω||100nF” or “220Ω+820Ω||115nF”.	600Ω
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.



Status Running

SIP Register Account_Empty

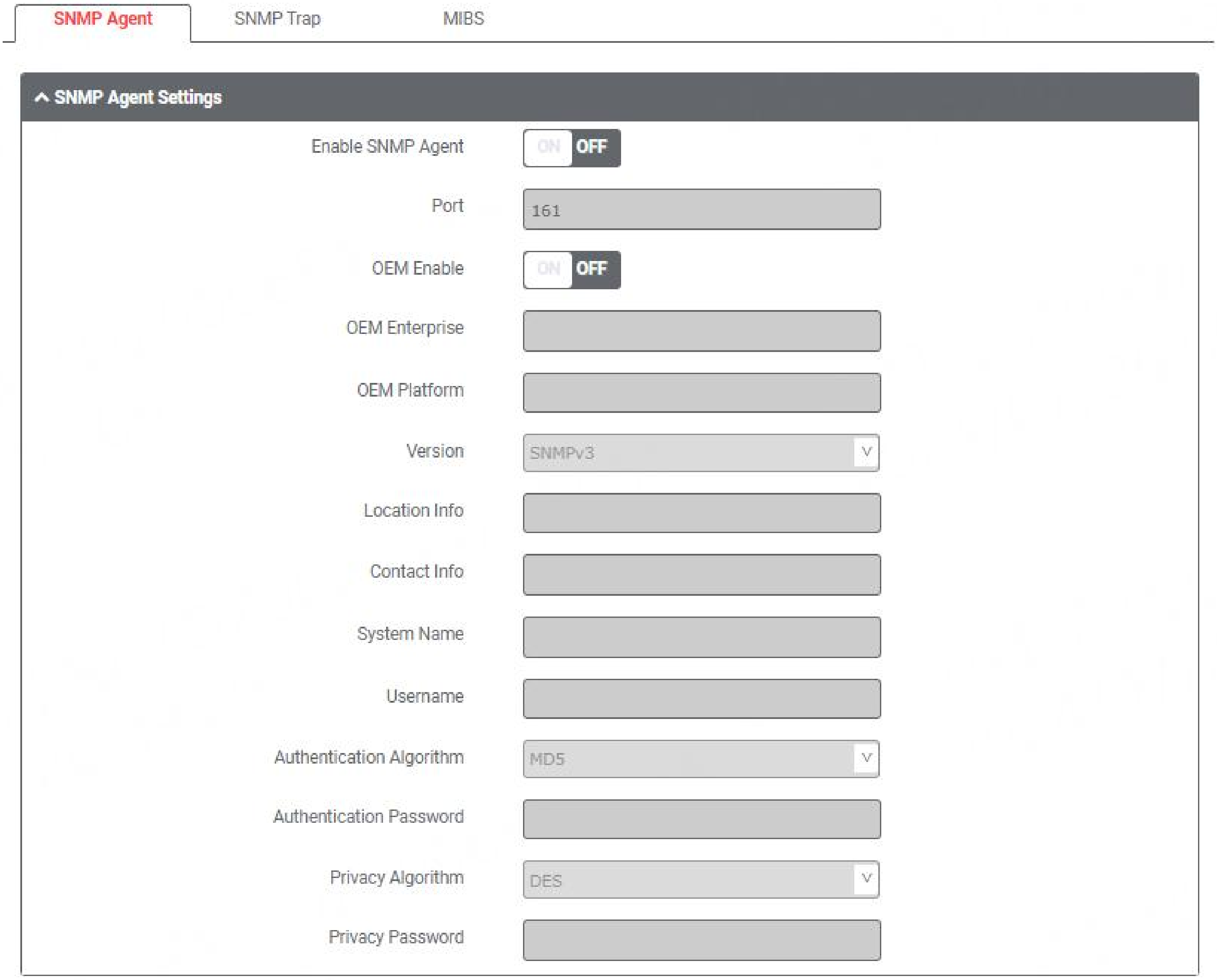
VoLTE Status

Version 1.1.0 (d87c7d43)

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



Enable SNMP Agent: ON OFF

Port: 161

OEM Enable: ON OFF

OEM Enterprise:

OEM Platform:

Version: SNMPv3

Location Info:

Contact Info:

System Name:

Username:

Authentication Algorithm: MD5

Authentication Password:

Privacy Algorithm: DES

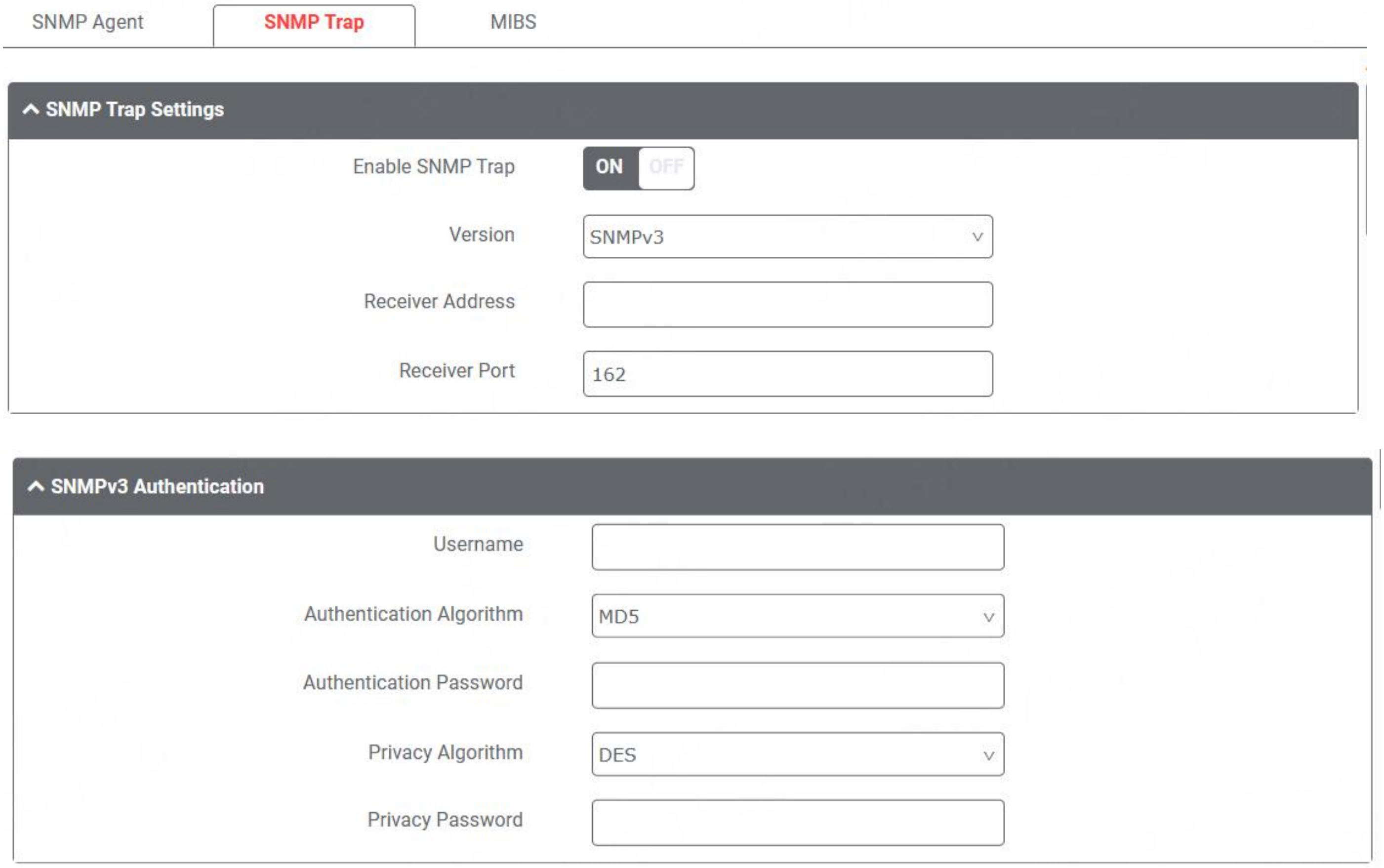
Privacy Password:

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.



Enable SNMP Trap: ON

Version: SNMPv3

Receiver Address:

Receiver Port: 162

Username:

Authentication Algorithm: MD5

Authentication Password:

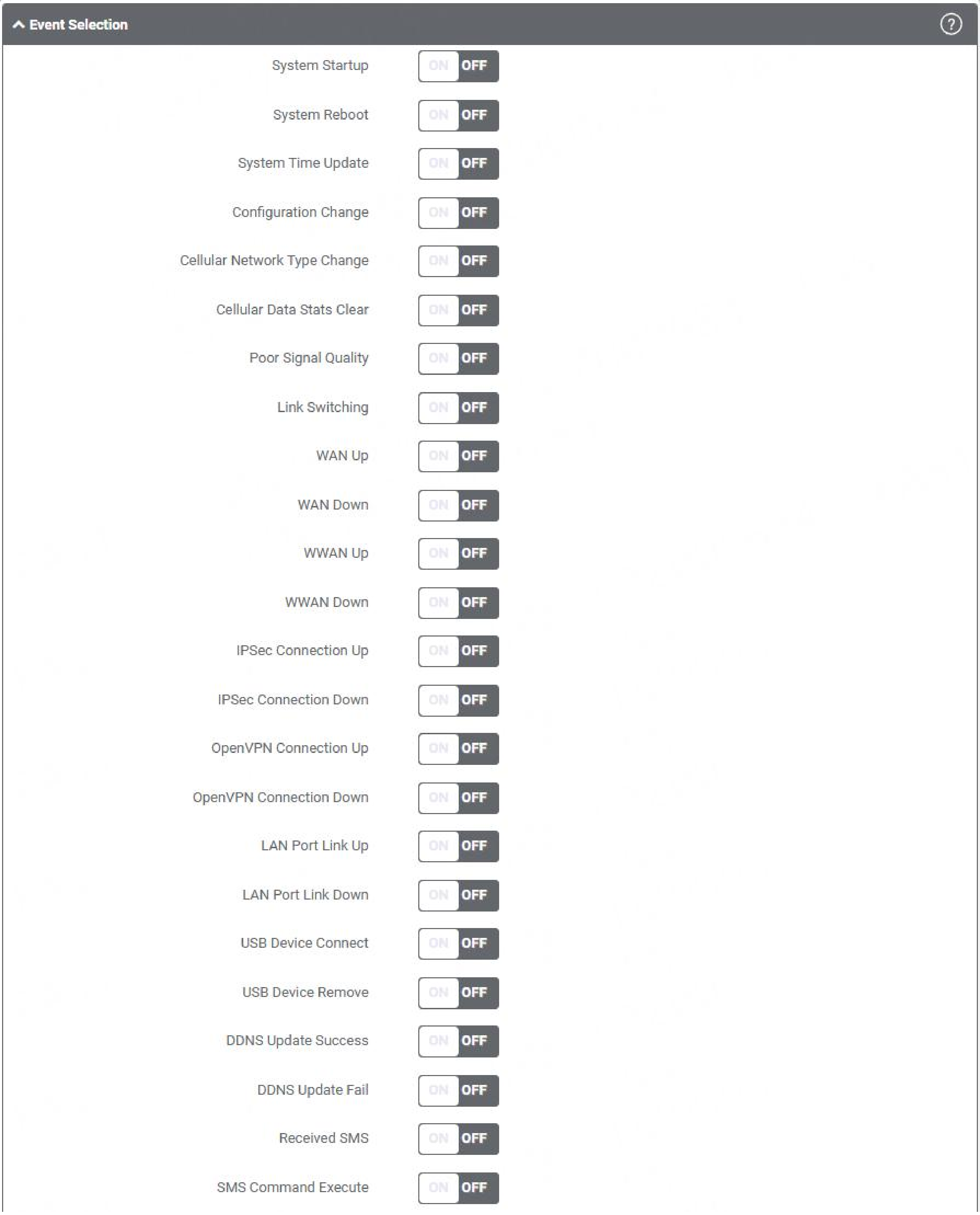
Privacy Algorithm: DES

Privacy Password:

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 ON OFF

System Reboot ON OFF

System Time Update ON OFF

Configuration Change ON OFF

Cellular Network Type Change ON OFF

Cellular Data Stats Clear ON OFF

Poor Signal Quality ON OFF

Link Switching ON OFF

WAN Up ON OFF

WAN Down ON OFF

WWAN Up ON OFF

WWAN Down ON OFF

IPSec Connection Up ON OFF

IPSec Connection Down ON OFF

OpenVPN Connection Up ON OFF

OpenVPN Connection Down ON OFF

LAN Port Link Up ON OFF

LAN Port Link Down ON OFF

USB Device Connect ON OFF

USB Device Remove ON OFF

DDNS Update Success ON OFF

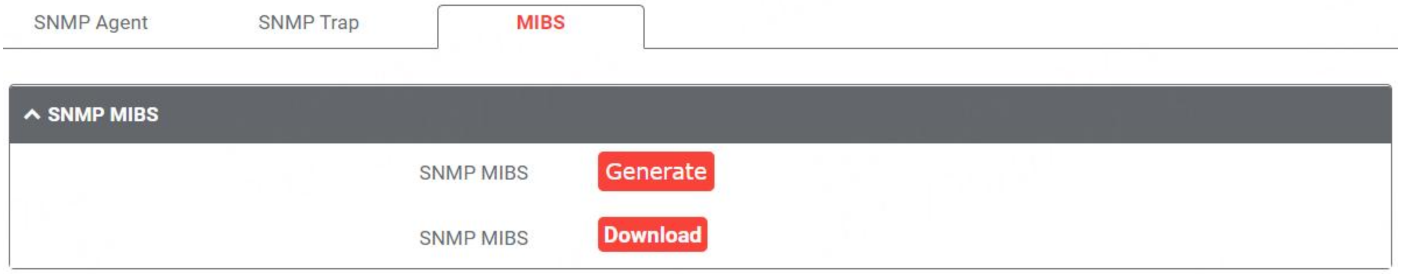
DDNS Update Fail ON OFF

Received SMS ON OFF

SMS Command Execute 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.



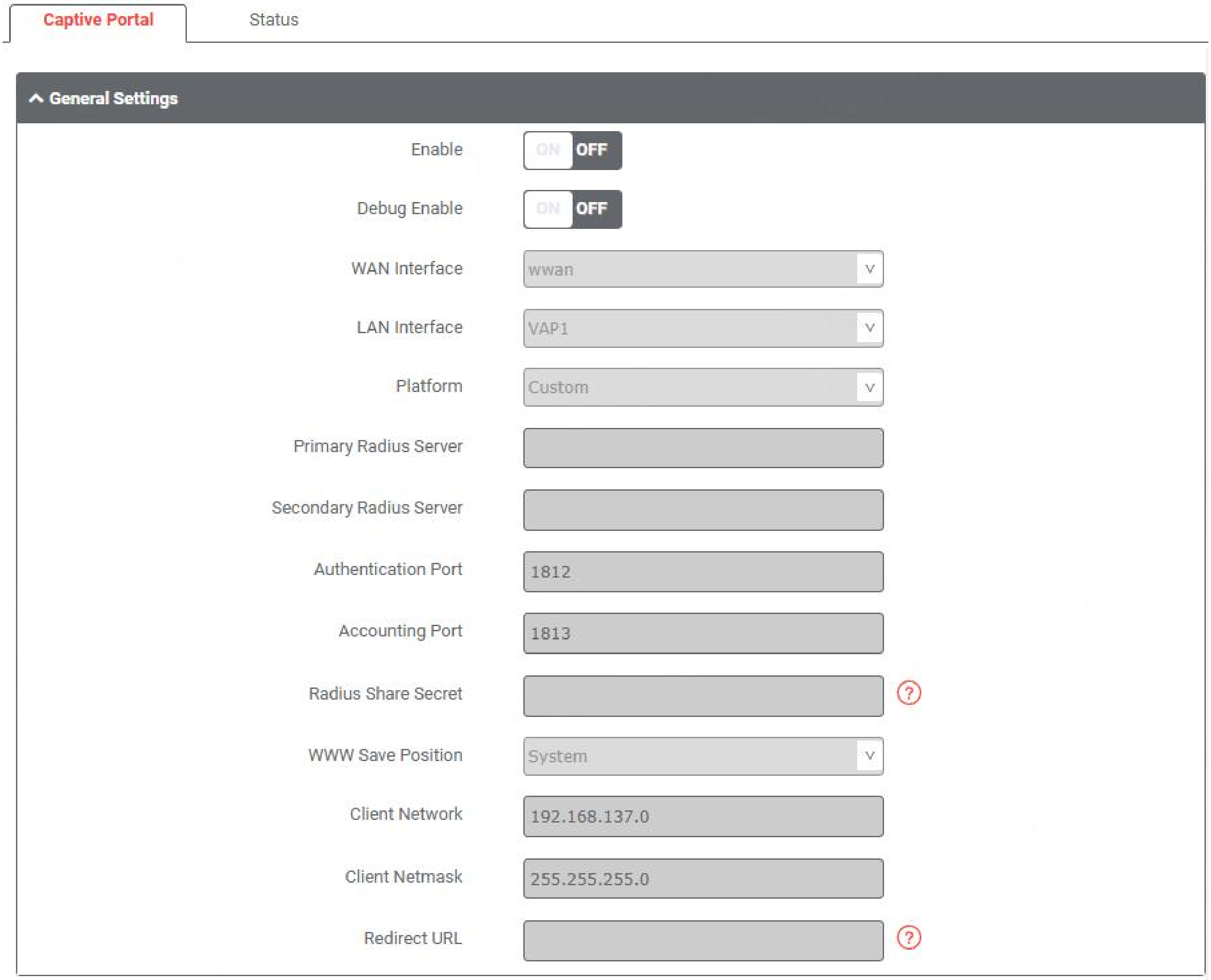
Item	Description	Default
MIBS	Click Generate to generate and click Download to download the device's MIB file.	--

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.



Enable ON OFF

Debug Enable ON OFF

WAN Interface: wwan

LAN Interface: VAP1

Platform: Custom

Primary Radius Server:

Secondary Radius Server:

Authentication Port: 1812

Accounting Port: 1813

Radius Share Secret:

WWW Save Position: System

Client Network: 192.168.137.0

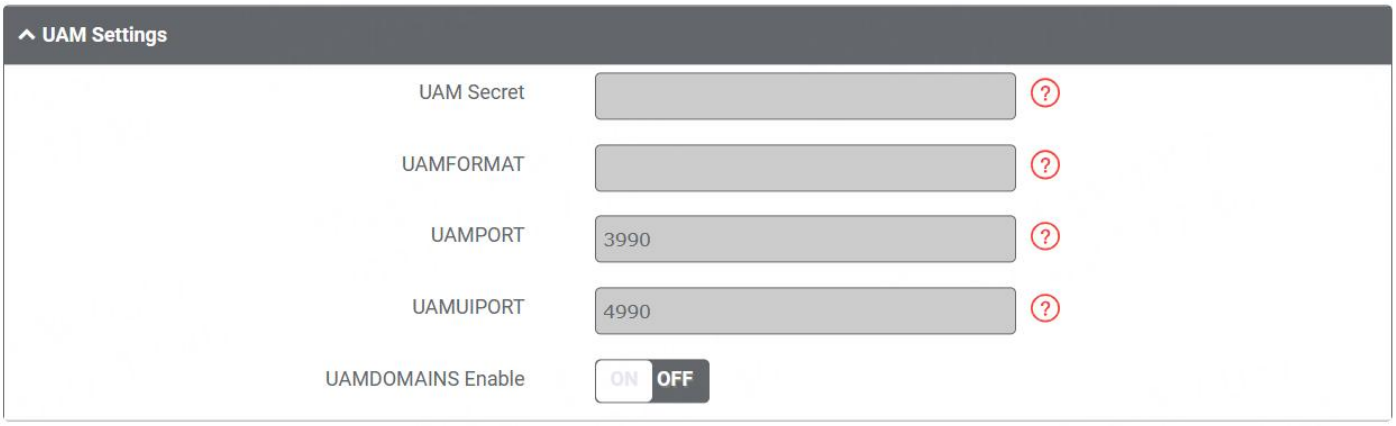
Client Netmask: 255.255.255.0

Redirect URL:

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.	wwan
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.	Null

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.


UAM Settings

UAM Secret

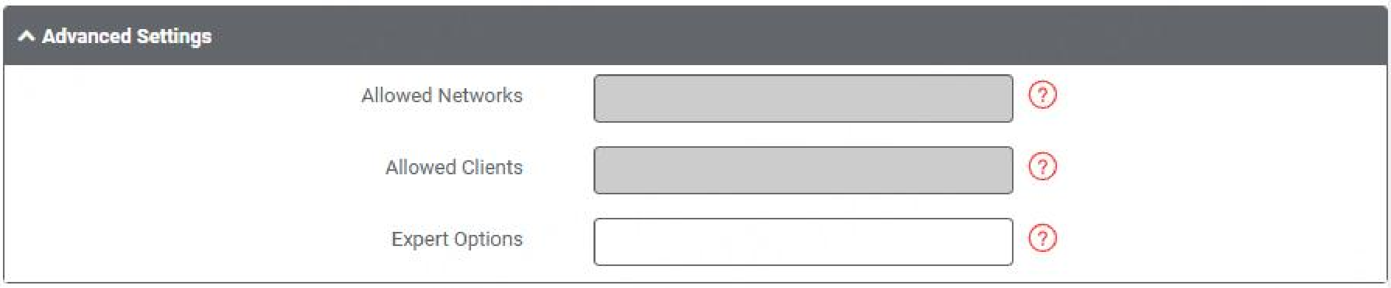
UAMFORMAT

UAMPORT 3990

UAMUIPORT 4990

UAMDOMAINS Enable OFF

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. Click the toggle button to enable/disable this option.	OFF



^ Advanced Settings

Allowed Networks

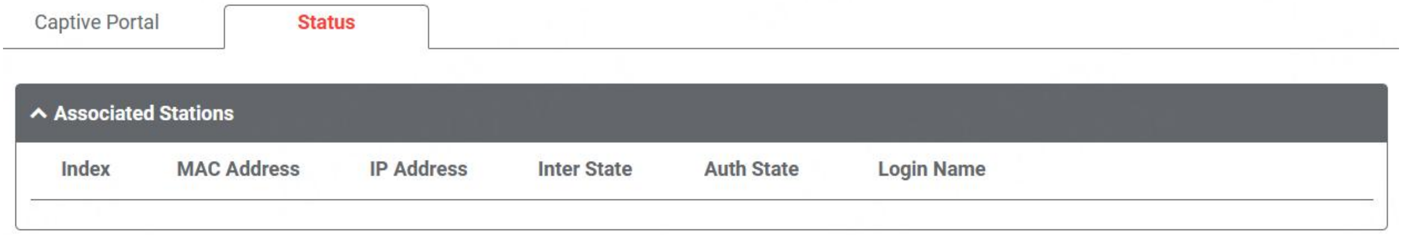
Allowed Clients

Expert Options

Item	Description	Default
Allowed Networks	Enter the network whitelist. Networks that are allowed to be accessed before logging in. Multiple networks are separated by ",".	Null
Allowed Clients	Enter the client whitelist. The MAC address that can access the Internet without authentication.	Null
Expert Options	Enter Expert Option.	Null

Status

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

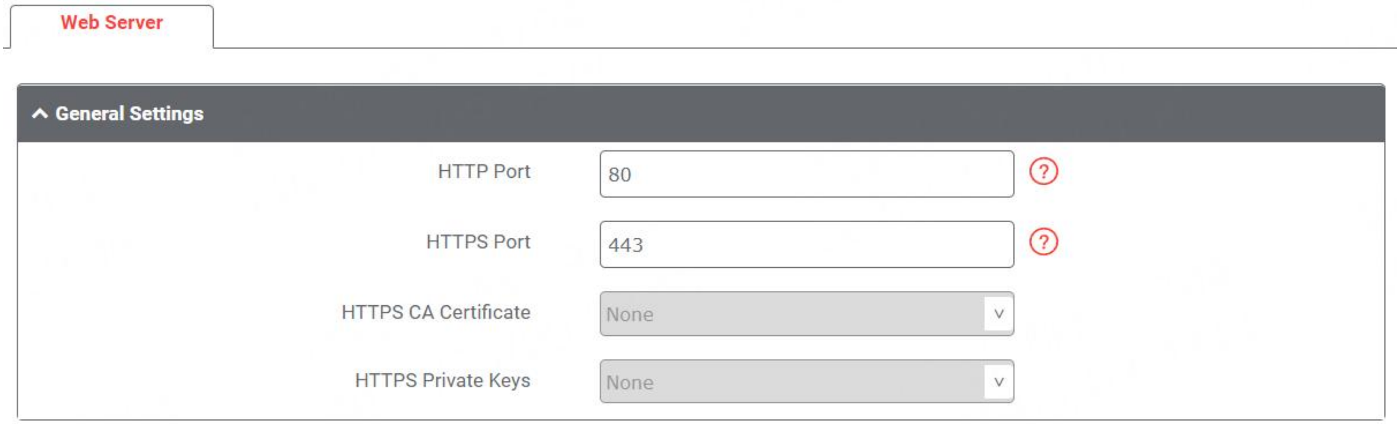


^ Associated Stations

Index	MAC Address	IP Address	Inter State	Auth State	Login Name

3.6.14 Web Server

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



^ General Settings

HTTP Port: 80

HTTPS Port: 443

HTTPS CA Certificate: None

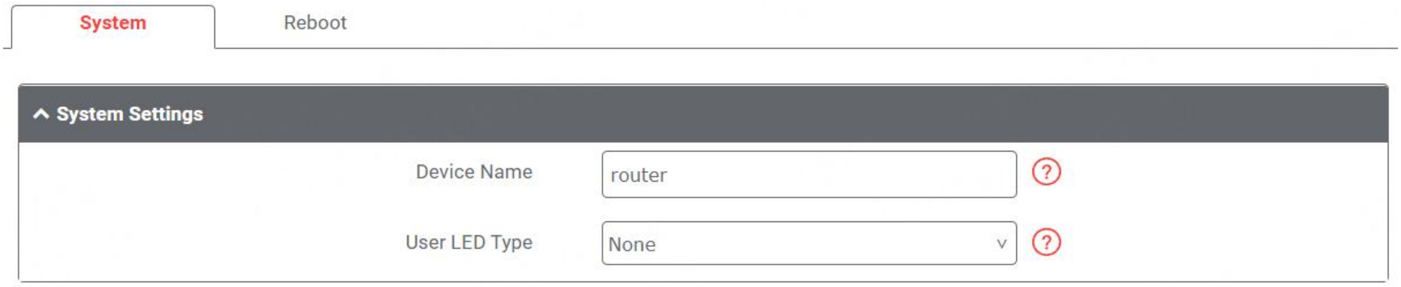
HTTPS Private Keys: None

Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in router's Web Server.	80

	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.	
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

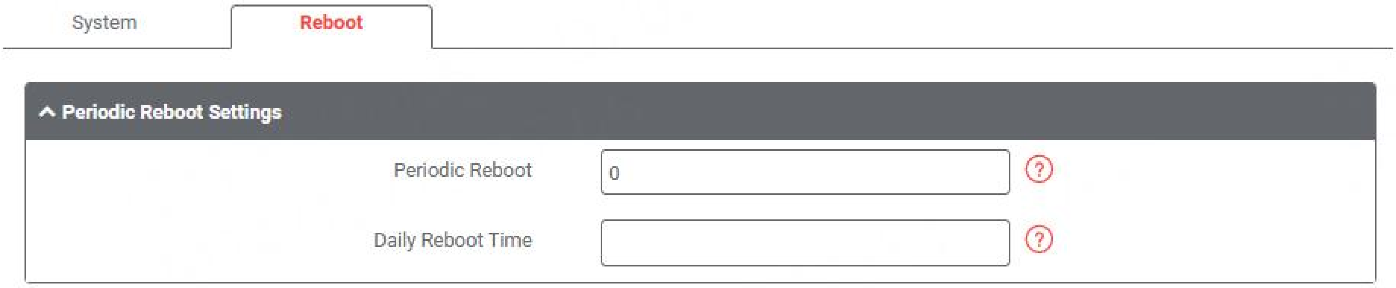
This section allows you to set the Advanced and parameters. Advanced router settings include system settings and reboot.



Device Name: router

User LED Type: None

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



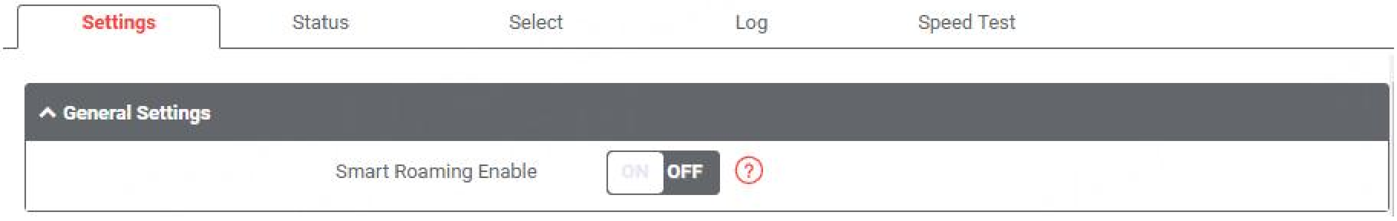
Periodic Reboot: 0

Daily Reboot Time:

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

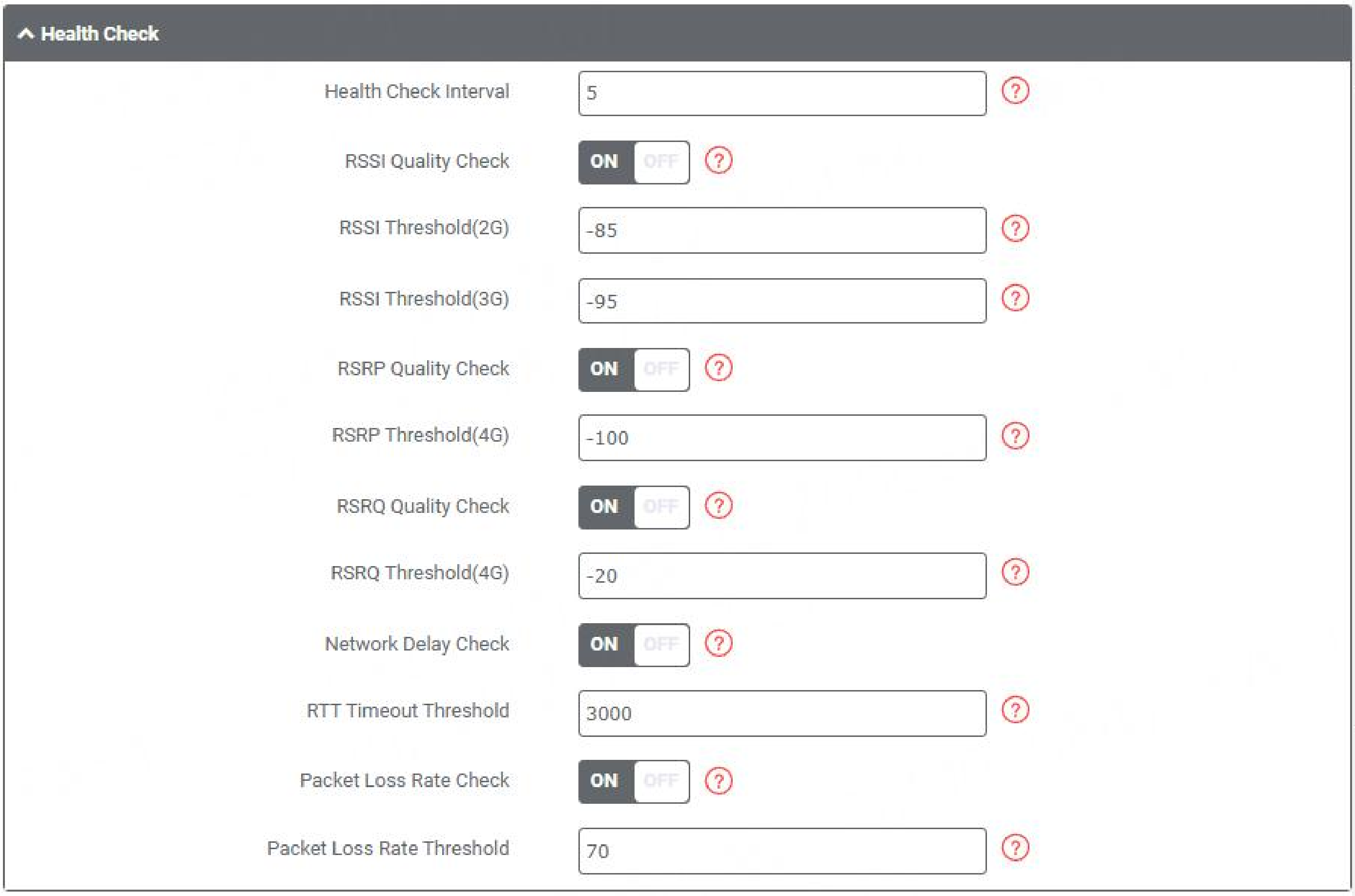
3.6.16 Smart Roaming V2

Smart Roaming Settings include common settings, health checks, PING settings, and advanced settings.



Smart Roaming Enable: ON OFF

Item	Description	Default
Enable Smart Roaming	Click the toggle button to enable/disable the "Smart Roaming" feature.	OFF



Health Check Interval: 5

RSSI Quality Check: ON OFF

RSSI Threshold(2G): -85

RSSI Threshold(3G): -95

RSRP Quality Check: ON OFF

RSRP Threshold(4G): -100

RSRQ Quality Check: ON OFF

RSRQ Threshold(4G): -20

Network Delay Check: ON OFF

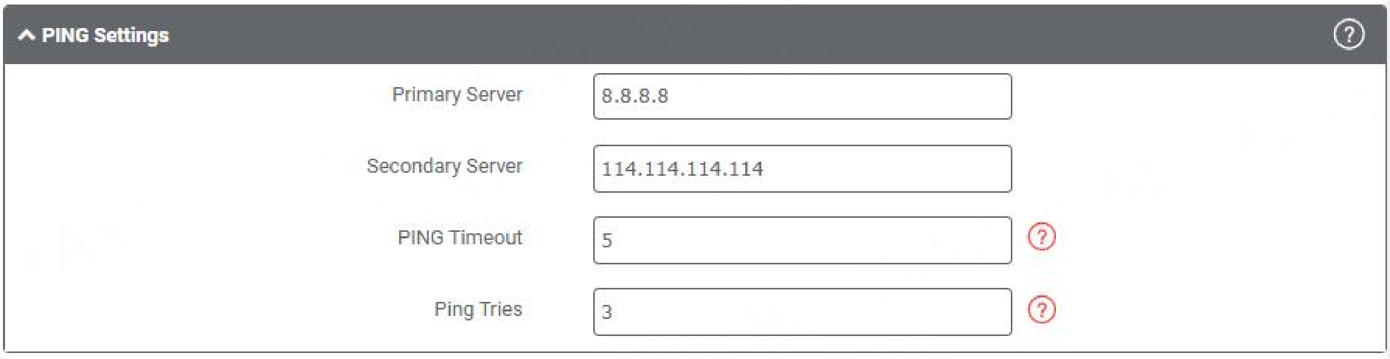
RTT Timeout Threshold: 3000

Packet Loss Rate Check: ON OFF

Packet Loss Rate Threshold: 70

Item	Description	Default
Health Check Interval	The current health check interval time for the connected network, in minutes. If the health check fails, Smart Roaming will attempt to switch to another carrier network. Note not to set all check conditions to theoretically unreachable values.	5 minutes
RSSI Quality Check	Click the toggle button to enable/disable the "RSSI Quality Check" feature.	OFF
RSSI Threshold (2G)	The signal strength threshold for the 2G network.	-85
RSSI Threshold (3G)	The signal strength threshold for the 3G network.	-95
RSSI Threshold (4G)	The signal strength threshold for the 4G network.	-100
RSRP Quality Check	Click the toggle button to enable/disable the "RSRP Quality Check" feature.	OFF
RSRP Threshold (4G)	The reference signal received power threshold for the 4G network.	-100
RSRQ Quality Check	Click the toggle button to enable/disable the "RSRQ Quality Check" feature.	OFF
RSRQ Threshold (4G)	The reference signal receive quality threshold for the 4G network.	-20
Network Delay Check	Click the toggle button to enable/disable the "Network Delay Check" feature.	ON
RTT Timeout	The round-trip time (RTT) timeout duration.	3000

Threshold		
Packet Loss Rate Check	Click the toggle button to enable/disable the "Packet Loss Rate Check" feature.	ON
Packet Loss Rate Threshold	Set the packet loss rate threshold.	70 %



PING Settings

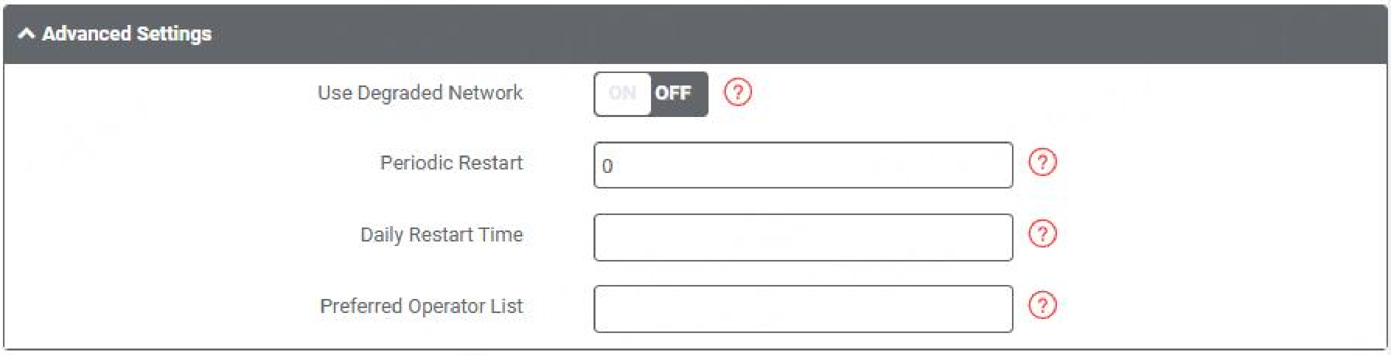
Primary Server: 8.8.8.8

Secondary Server: 114.114.114.114

PING Timeout: 5

Ping Tries: 3

Item	Description	Default
Preferred Server	This device pings the primary address/domain name to check if the current connection is consistently available.	8.8.8.8
Backup Server	This device pings the backup address/domain name to check if the current connection is consistently available.	114.114.114.114
Ping Timeout	Set the timeout duration for the Ping request.	5
Ping Attempt Count	The number of ping attempts during each health check. Each ping attempt will by default send 3 ping packets, so the total number of ping packets sent during each health check will be (3 * ping attempt count).	3



Advanced Settings

Use Degraded Network: ON OFF

Periodic Restart: 0

Daily Restart Time:

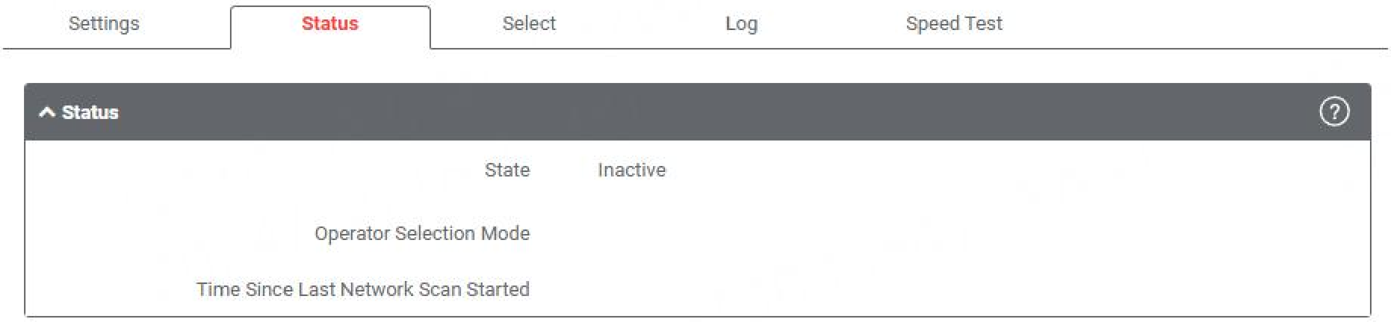
Preferred Operator List:

Item	Description	Default
Use Degraded Network	Click the toggle button to enable/disable the "Use Degraded Network" feature. A degraded network is defined as a network that can connect to the internet, but the network quality does not meet the health check thresholds.	OFF
Regular Restart	Set the cycle for restarting the "Smart Roaming" feature, in hours. A value of 0 means that regular restart is disabled. Restarting "Smart Roaming" will rescan for available carrier networks and reset the current status. Since searching for available carrier networks can take time, a restart may	0

	take 3 to 5 minutes.	
Daily Restart Time	Set the time for the daily restart of "Smart Roaming," in the format HH:MM (24-hour format). If this field is empty, it means that scheduled restarts are turned off.	Null
Preferred Carrier List	Set the preferred operator list using PLMN. If multiple operators are needed, separate them with a semicolon, for example: 46000;46001.	Null

Stauts

This section is used to view the status of the current connection.

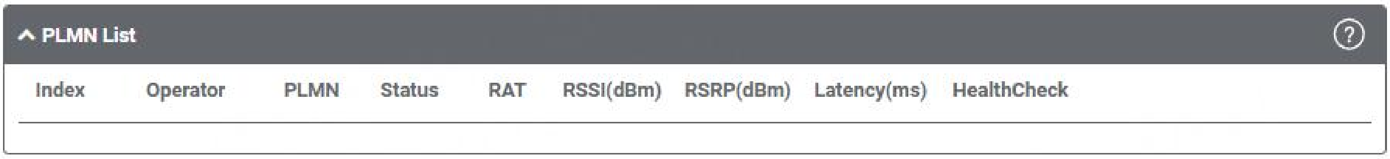


State Inactive

Operator Selection Mode

Time Since Last Network Scan Started

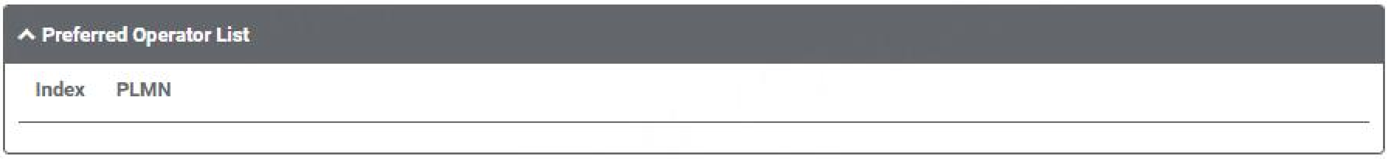
Item	Description	Default
Status	Displays the current status of "Smart Roaming." This includes statuses such as Scanning, Connecting, Connected, and Inactive, indicating whether the device is searching for available networks, connecting to a network, the network is connected, or the feature is not activated.	Inactive
Carrier Selection Mode	Displays the current method of carrier network selection. There are two modes: Automatic and Manual, referring to standard automatic selection and software-based selection based on network quality. The software will cycle between these two modes.	--
Time Elapsed Since Last Network Search	Displays the time elapsed since the last search for available networks began. A restart of "Smart Roaming" will refresh this time.	--



Index	Operator	PLMN	Status	RAT	RSSI(dBm)	RSRP(dBm)	Latency(ms)	HealthCheck

Item	Description
Index	PLMN list index.
PLMN	PLMN = MCC + MNC, which is a combination of the Mobile Country Code and the Mobile Network Code.
Status	Current network status, including Current, Visible, Forbidden, and Unknown, indicating whether the network is currently in use, available, prohibited, or unknown.

RAT	Current Radio Access Technology, including 3G, 4G, and 5G.
RSSI	Current signal quality, used for 3G and 4G networks.
RSRP	Current Reference Signal Received Power, used for 4G and 5G networks. **Note:** When connected to 5G, signal strength RSSI cannot be viewed; only signal power RSRP can be checked.
Latency	Current network latency.
Packet Loss Rate	Current network packet loss rate.
Health Check Status	Current health check status, including Pending, Good, Degraded, and Failed, indicating whether the network has not yet undergone a health check, the network quality is good, it is a degraded network, or the network quality is poor (including network disconnection or not meeting health check thresholds).



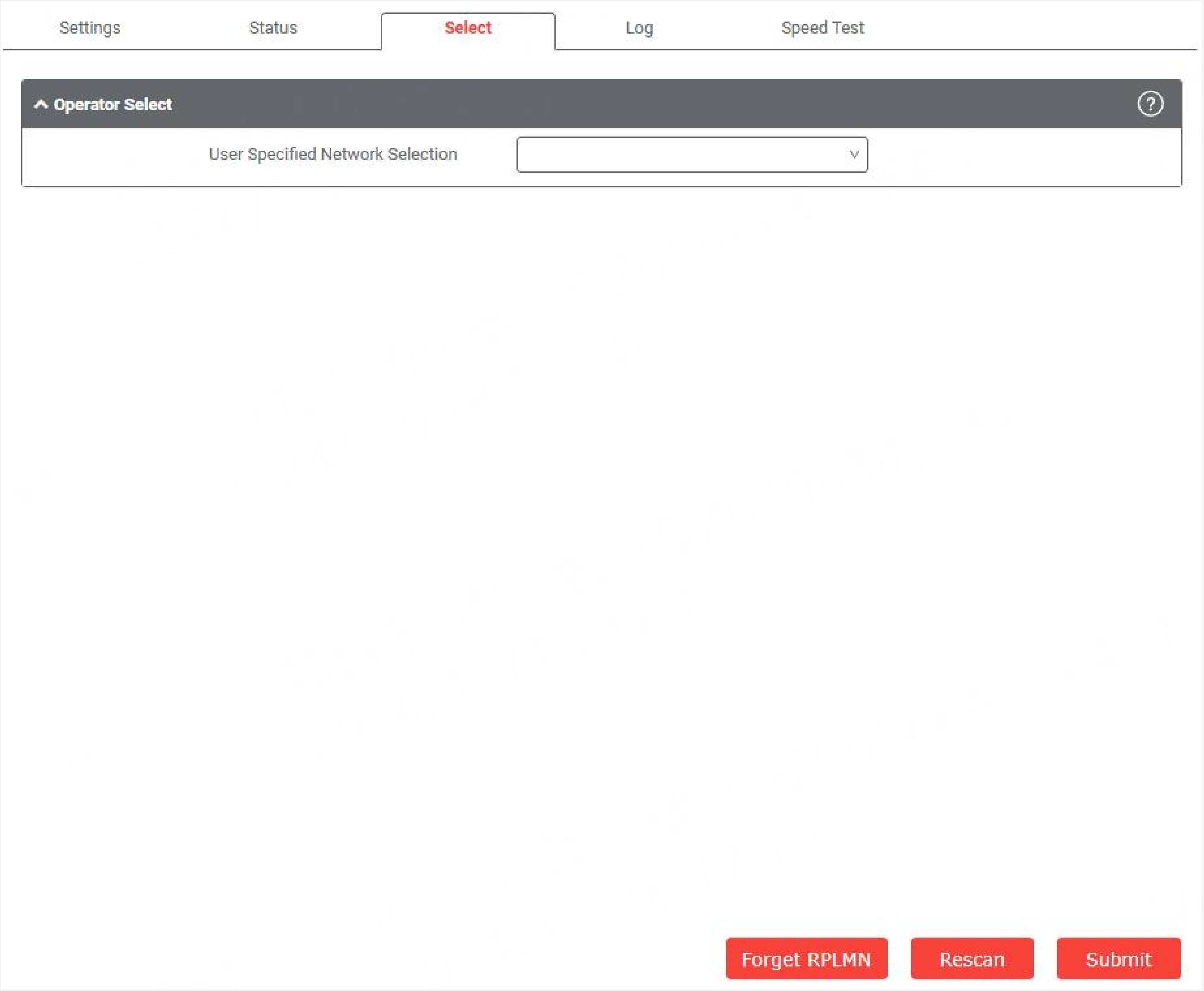
^ Preferred Operator List

Index	PLMN

Item	**Description**
Index	PLMN list index.
PLMN	PLMN = MCC + MNC, which is a combination of the Mobile Country Code and the Mobile Network Code.

Select

This section is used to configure network selection.

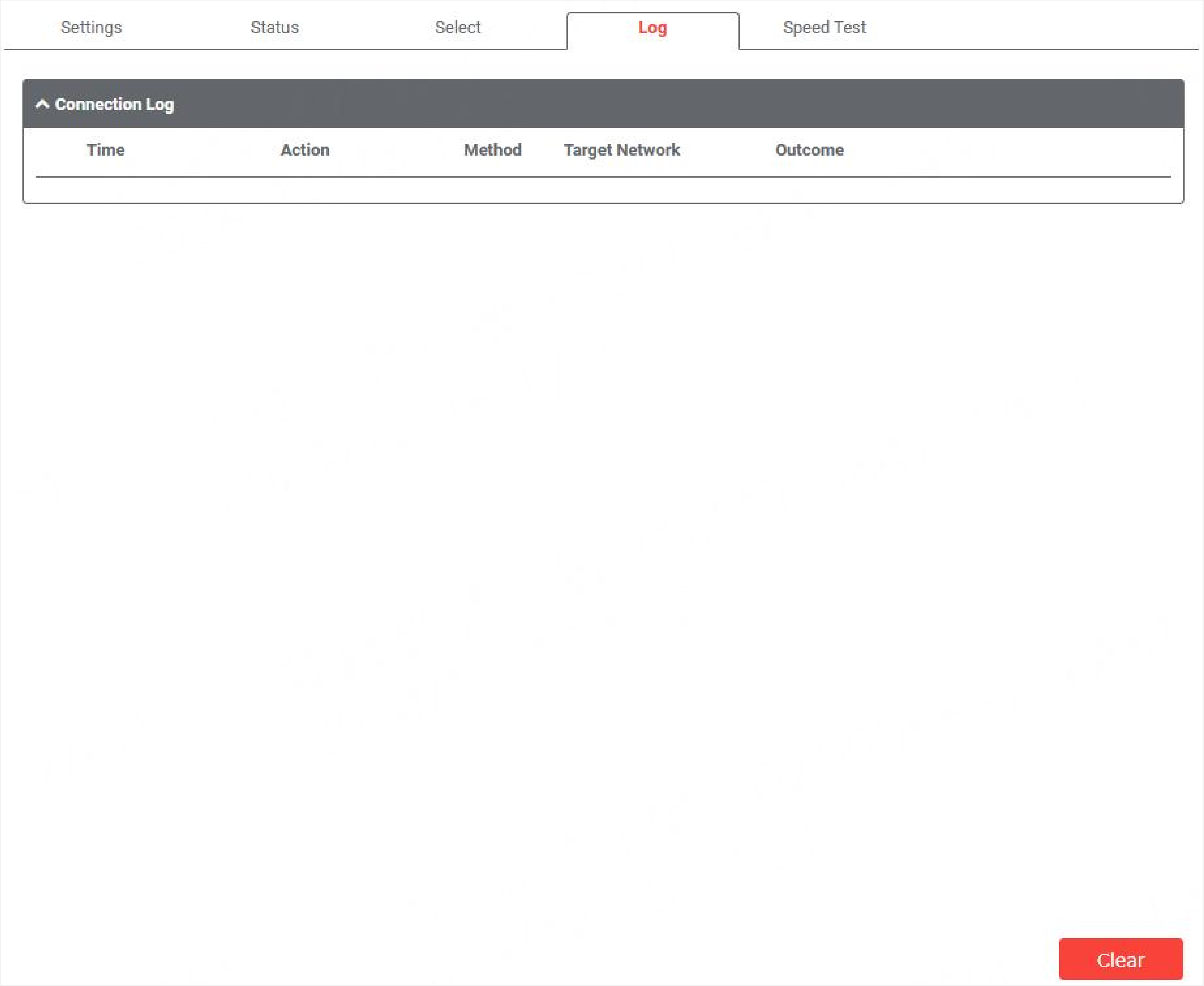


User Specified Network Selection

Item	Description	Default
User-Specified Network Selection	Choose the specified network.	Null
Forget RPLMN	Forcefully remove all location information from the SIM.	--
Rescan	Rescan the carrier network list.	--
Submit	Submit the user-specified network selection.	--

Log

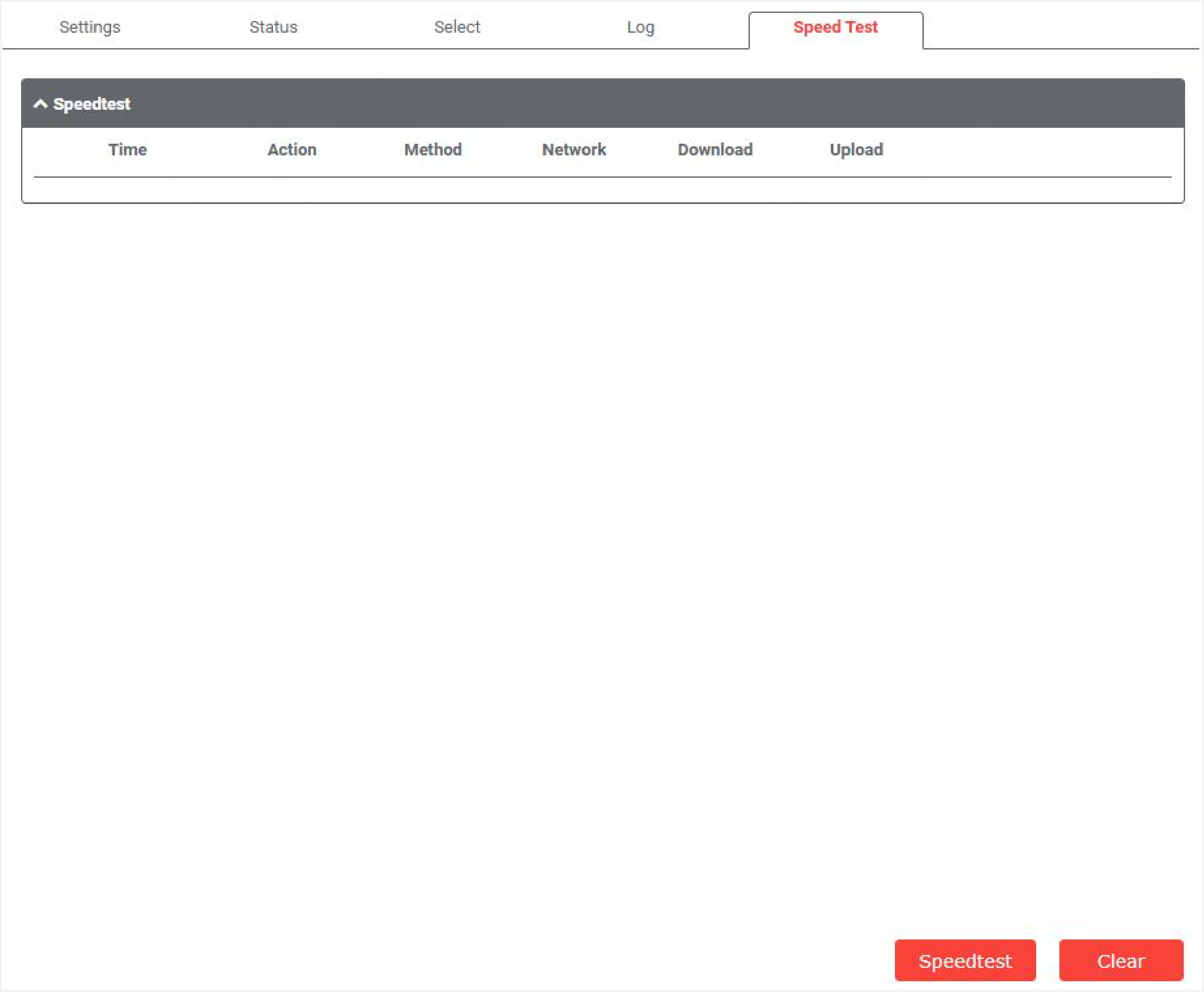
This section is used to view the connection logs.



Time	Action	Method	Target Network	Outcome

Item	Description	Default
Clear	Click the button to clear the connection logs.	--

Speed Test



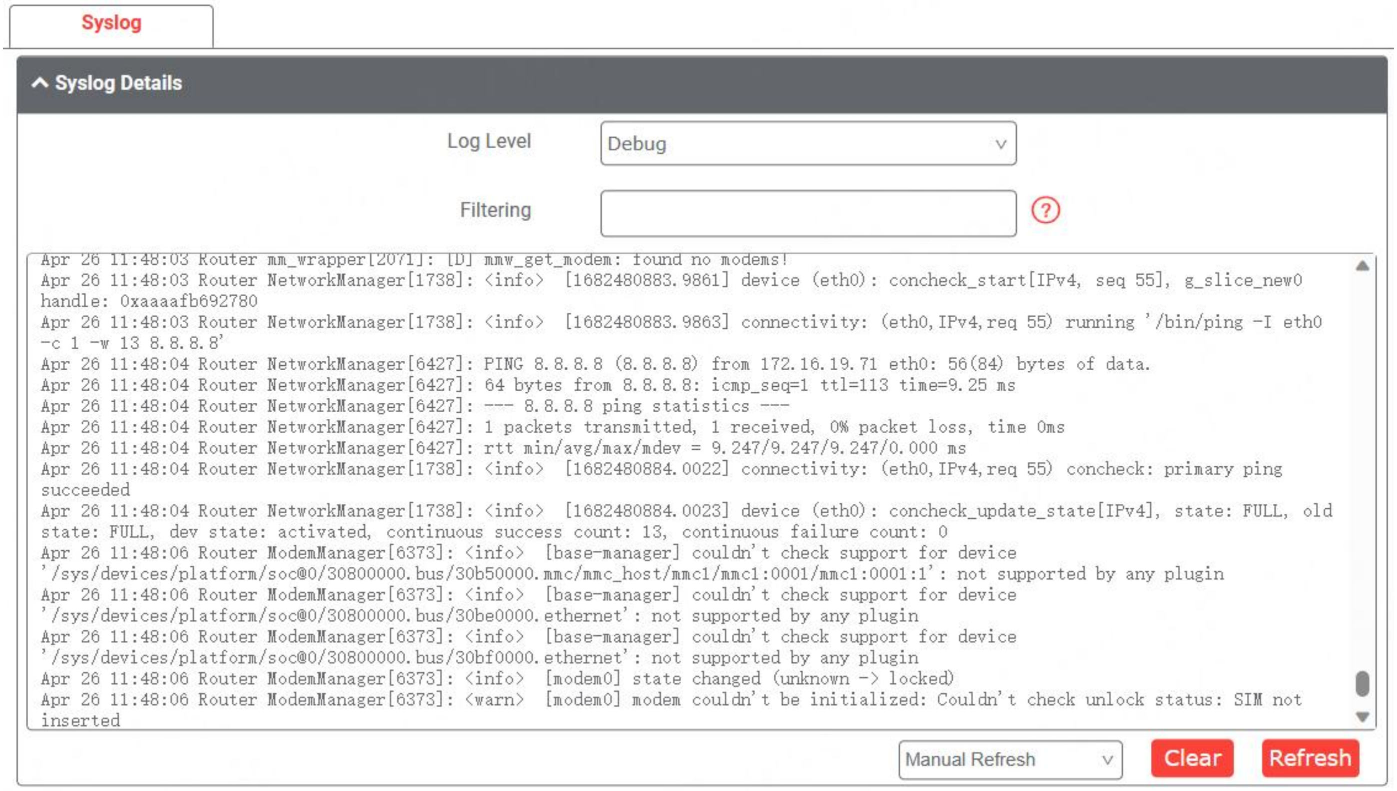
Time	Action	Method	Network	Download	Upload

Item	Description	Default
Speedtest	Click the button to start the network speed test.	--
Clear	Click the button to clear the speed test logs.	--

3.7 System

3.7.1 Debug

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

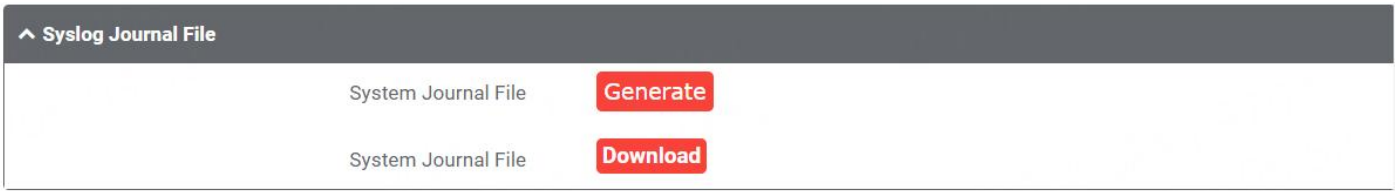


Log Level: Debug

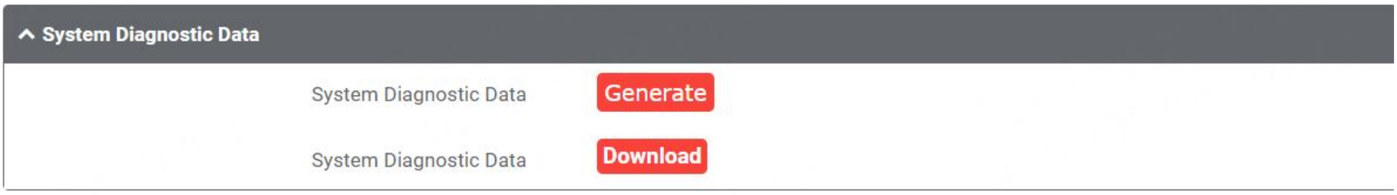
Filtering:

```
Apr 26 11:48:03 Router mm_wrapper[2071]: [D] mmw_get_modem: found no modems!
Apr 26 11:48:03 Router NetworkManager[1738]: <info>  [1682480883.9861] device (eth0): concheck_start[IPv4, seq 55], g_slice_new0
handle: 0xaaaafb692780
Apr 26 11:48:03 Router NetworkManager[1738]: <info>  [1682480883.9863] connectivity: (eth0,IPv4,req 55) running '/bin/ping -I eth0
-c 1 -w 13 8.8.8.8'
Apr 26 11:48:04 Router NetworkManager[6427]: PING 8.8.8.8 (8.8.8.8) from 172.16.19.71 eth0: 56(84) bytes of data.
Apr 26 11:48:04 Router NetworkManager[6427]: 64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=9.25 ms
Apr 26 11:48:04 Router NetworkManager[6427]: --- 8.8.8.8 ping statistics ---
Apr 26 11:48:04 Router NetworkManager[6427]: 1 packets transmitted, 1 received, 0% packet loss, time 0ms
Apr 26 11:48:04 Router NetworkManager[6427]: rtt min/avg/max/mdev = 9.247/9.247/9.247/0.000 ms
Apr 26 11:48:04 Router NetworkManager[1738]: <info>  [1682480884.0022] connectivity: (eth0,IPv4,req 55) concheck: primary ping
succeeded
Apr 26 11:48:04 Router NetworkManager[1738]: <info>  [1682480884.0023] device (eth0): concheck_update_state[IPv4], state: FULL, old
state: FULL, dev state: activated, continuous success count: 13, continuous failure count: 0
Apr 26 11:48:06 Router ModemManager[6373]: <info>  [base-manager] couldn't check support for device
'/sys/devices/platform/soc@0/30800000.bus/30b50000.mmc/mmc_host/mmc1/mmc1:0001/mmc1:0001:1': not supported by any plugin
Apr 26 11:48:06 Router ModemManager[6373]: <info>  [base-manager] couldn't check support for device
'/sys/devices/platform/soc@0/30800000.bus/30be0000.ethernet': not supported by any plugin
Apr 26 11:48:06 Router ModemManager[6373]: <info>  [base-manager] couldn't check support for device
'/sys/devices/platform/soc@0/30800000.bus/30bf0000.ethernet': not supported by any plugin
Apr 26 11:48:06 Router ModemManager[6373]: <info>  [modem0] state changed (unknown -> locked)
Apr 26 11:48:06 Router ModemManager[6373]: <warn>  [modem0] modem couldn't be initialized: Couldn't check unlock status: SIM not
inserted
```

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.	--

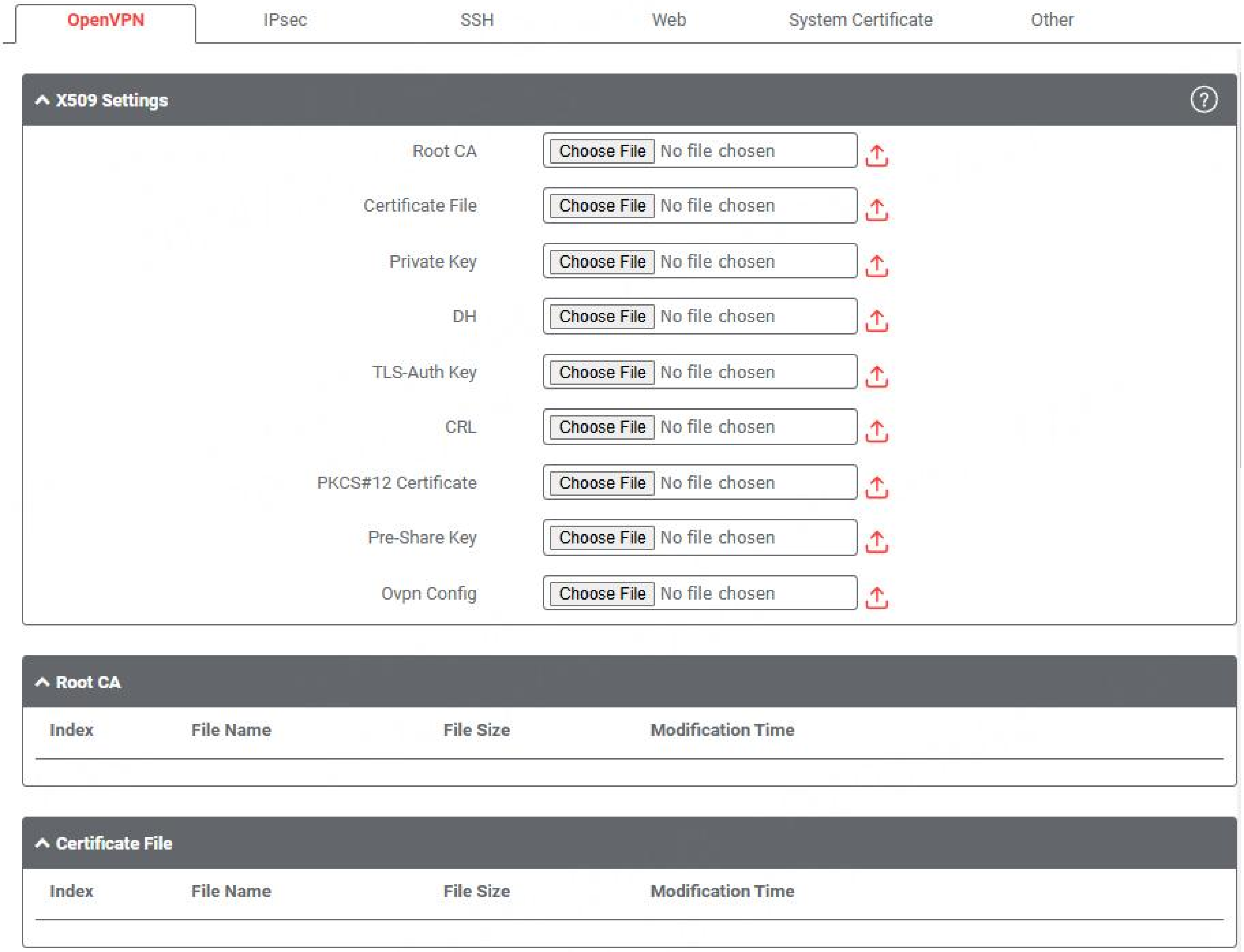


Item	Description	Default
System Diagnostic Data	Click Generate to generate and click Download to download the system diagnostic data.	--

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



X509 Settings

Root CA	Choose File No file chosen ↥
Certificate File	Choose File No file chosen ↥
Private Key	Choose File No file chosen ↥
DH	Choose File No file chosen ↥
TLS-Auth Key	Choose File No file chosen ↥
CRL	Choose File No file chosen ↥
PKCS#12 Certificate	Choose File No file chosen ↥
Pre-Share Key	Choose File No file chosen ↥
Ovpn Config	Choose File No file chosen ↥

Root CA

Index	File Name	File Size	Modification Time

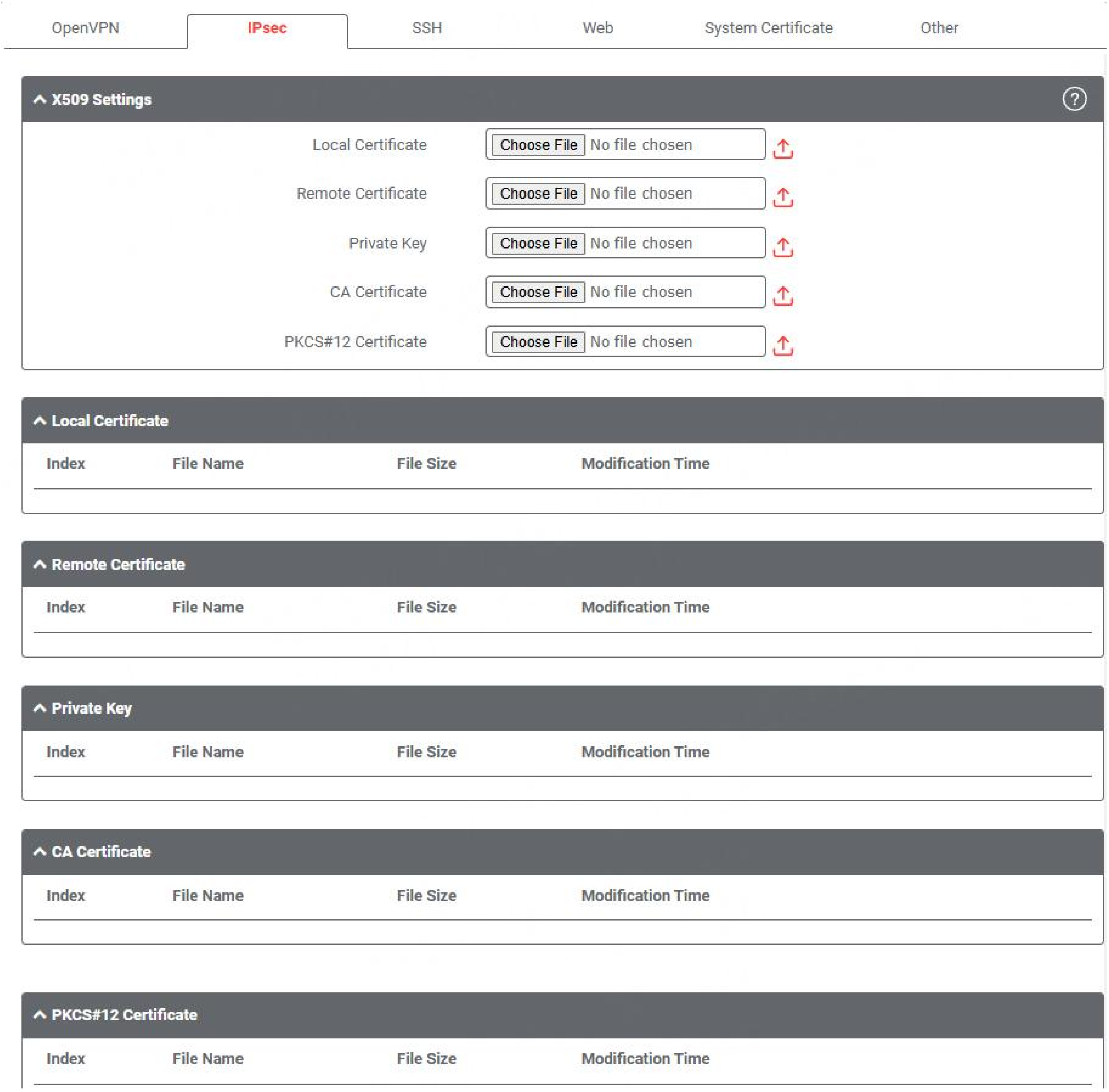
Certificate File

Index	File Name	File Size	Modification Time

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



X509 Settings

Local Certificate	Choose File No file chosen
Remote Certificate	Choose File No file chosen
Private Key	Choose File No file chosen
CA Certificate	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen

Local Certificate

Index	File Name	File Size	Modification Time

Remote Certificate

Index	File Name	File Size	Modification Time

Private Key

Index	File Name	File Size	Modification Time

CA Certificate

Index	File Name	File Size	Modification Time

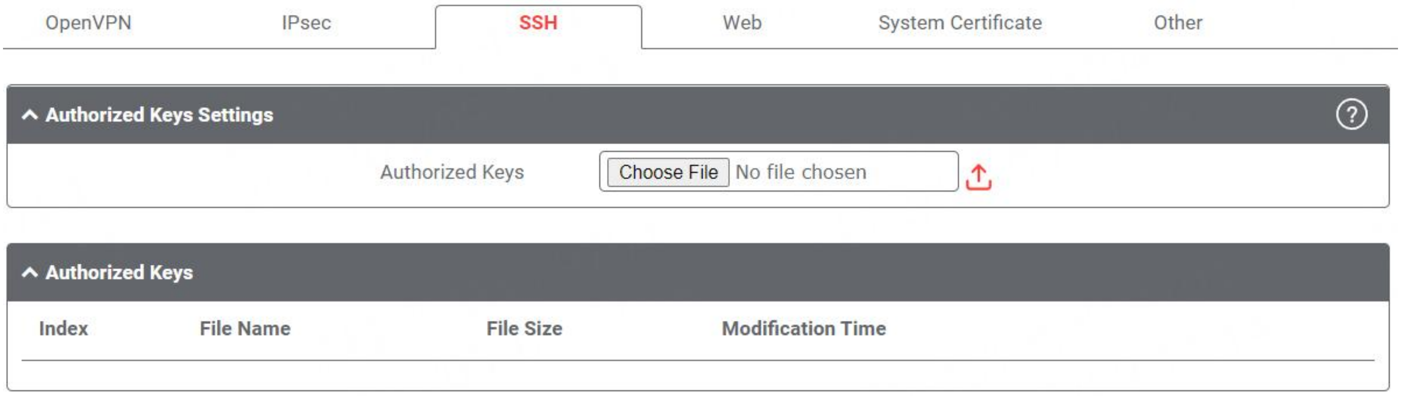
PKCS#12 Certificate

Index	File Name	File Size	Modification Time

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.	--

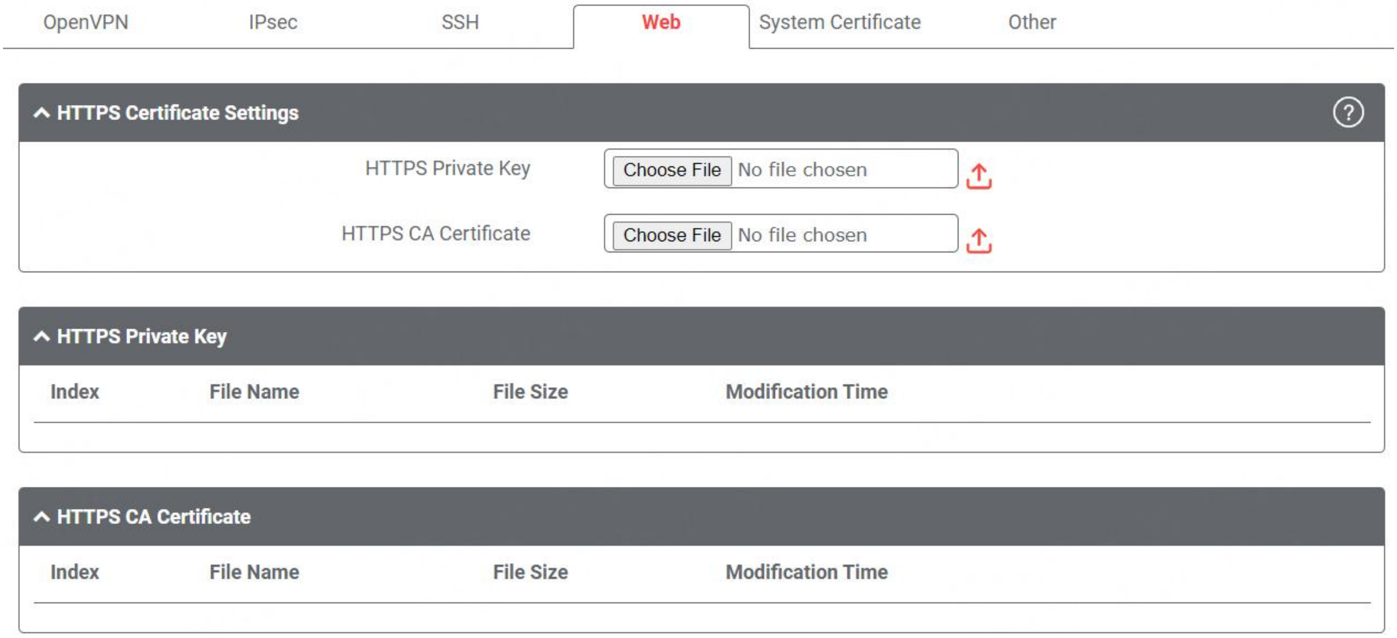
SSH



Index	File Name	File Size	Modification Time

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



HTTPS Certificate Settings

HTTPS Private Key: Choose File No file chosen ↥

HTTPS CA Certificate: Choose File No file chosen ↥

HTTPS Private Key

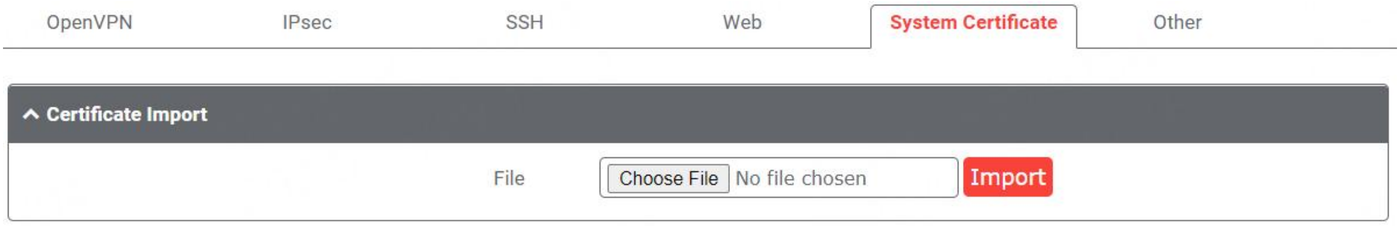
Index	File Name	File Size	Modification Time

HTTPS CA Certificate

Index	File Name	File Size	Modification Time

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

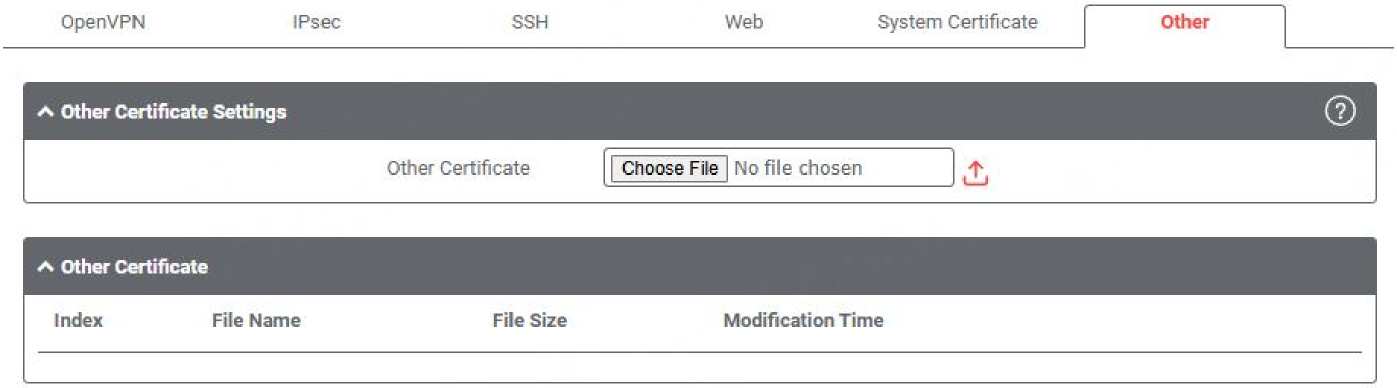


Certificate Import

File: Choose File No file chosen Import

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



Other Certificate Settings

Other Certificate: Choose File No file chosen

Other Certificate

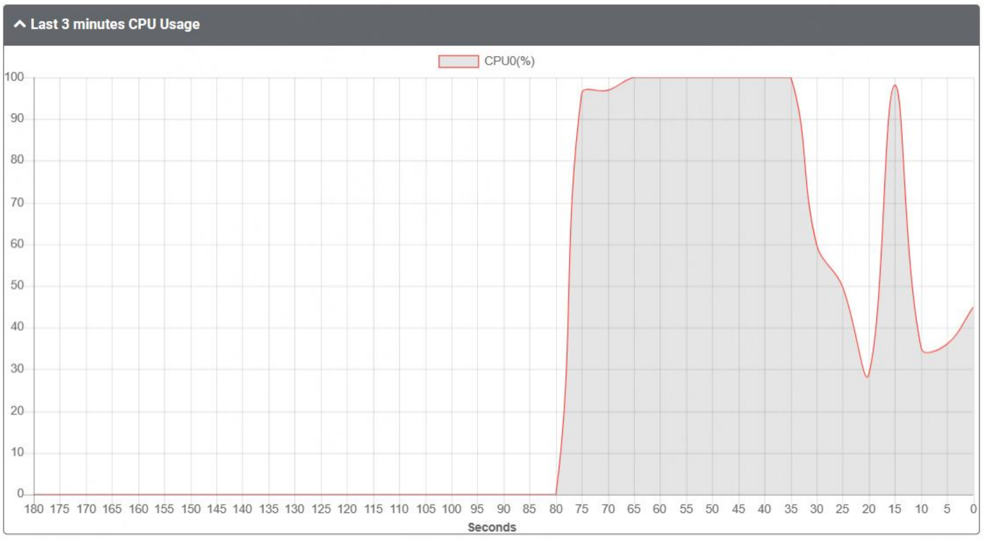
Index	File Name	File Size	Modification Time

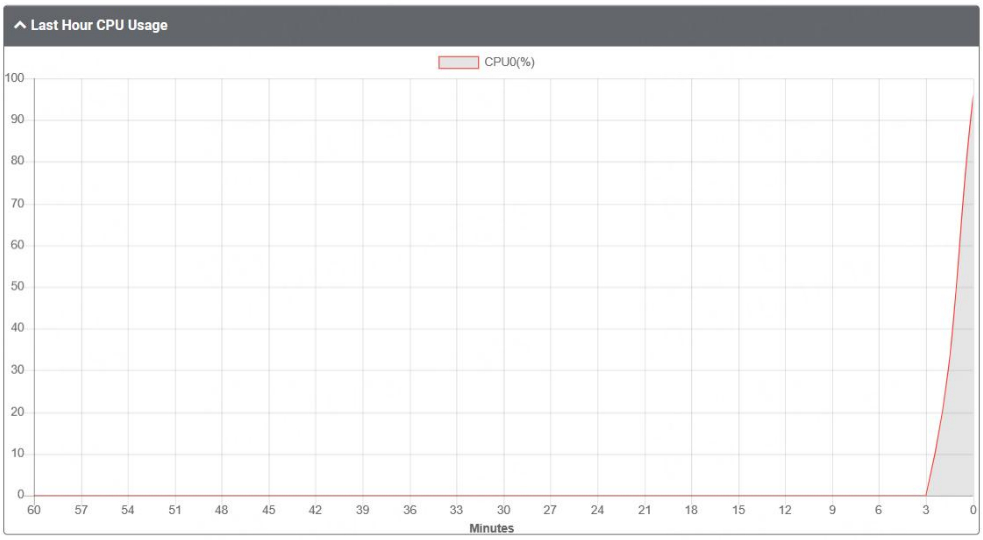
Item	Description	Default
Other Certificate	Click on Choose File to locate the Other Certificate file, and then click on ⤒ to import this file into your device.	--

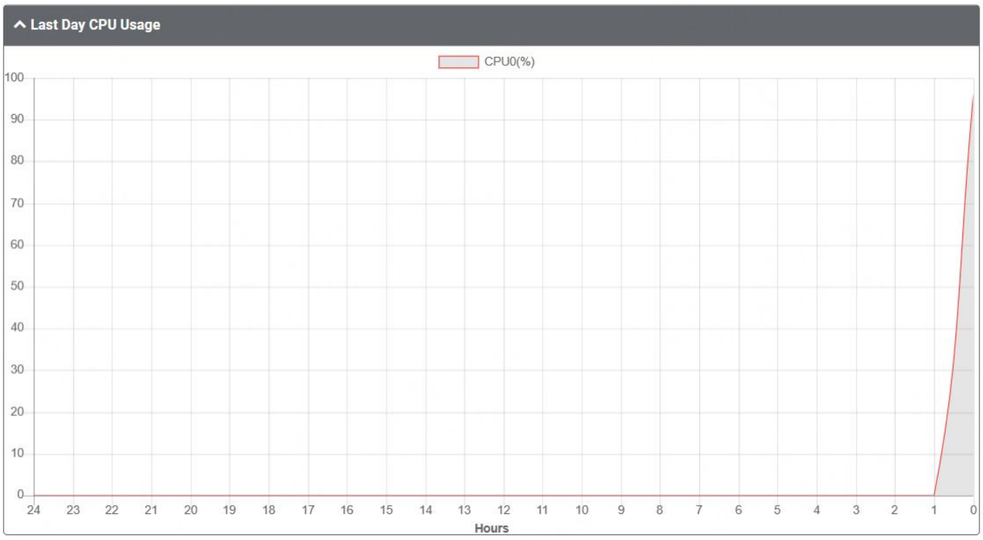
3.7.3 Resource Graph

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.

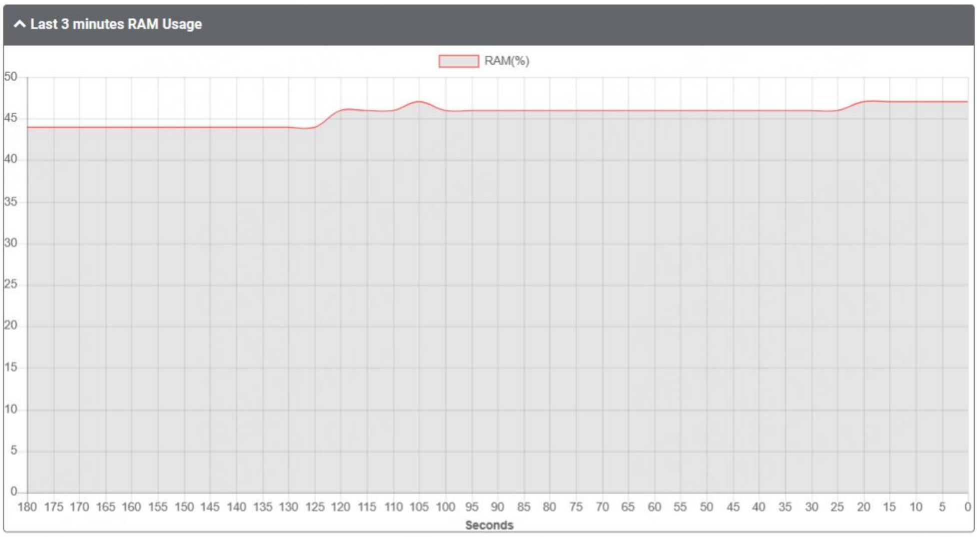
CPU Usage

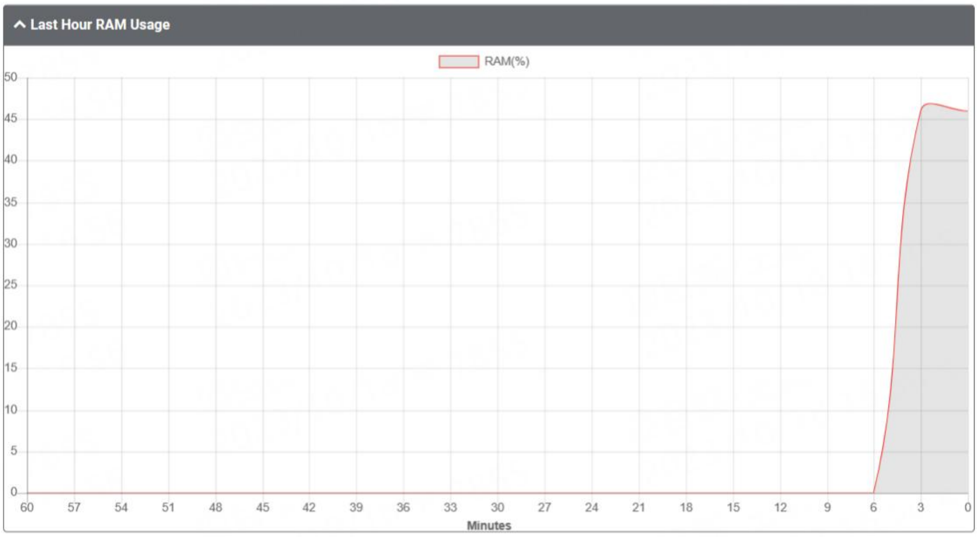

Last 3 minutes CPU Usage
CPU0(%)
100
90
80
70
60
50
40
30
20
10
0
180 175 170 165 160 155 150 145 140 135 130 125 120 115 110 105 100 95 90 85 80 75 70 65 60 55 50 45 40 35 30 25 20 15 10 5 0
Seconds

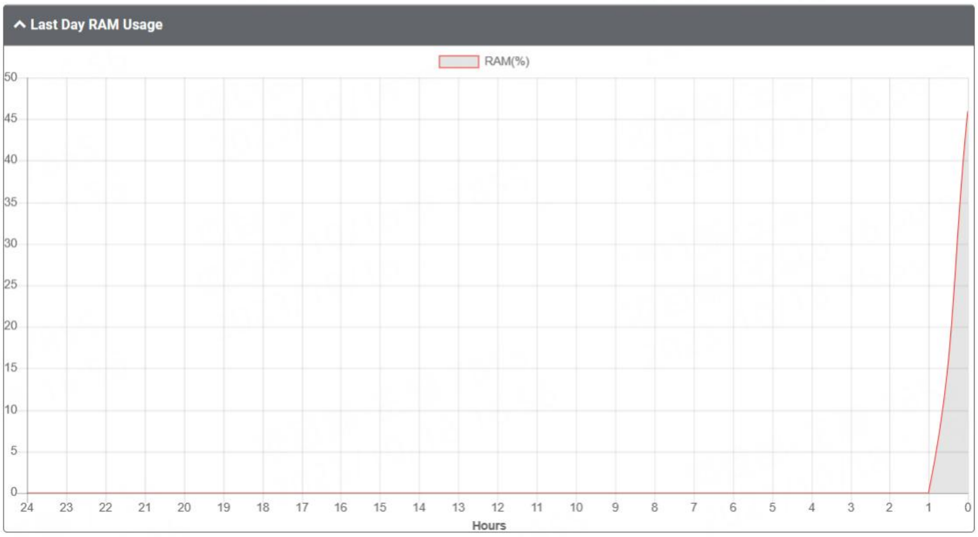

Last Hour CPU Usage
CPU0(%)
100
90
80
70
60
50
40
30
20
10
0
60 57 54 51 48 45 42 39 36 33 30 27 24 21 18 15 12 9 6 3 0
Minutes


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

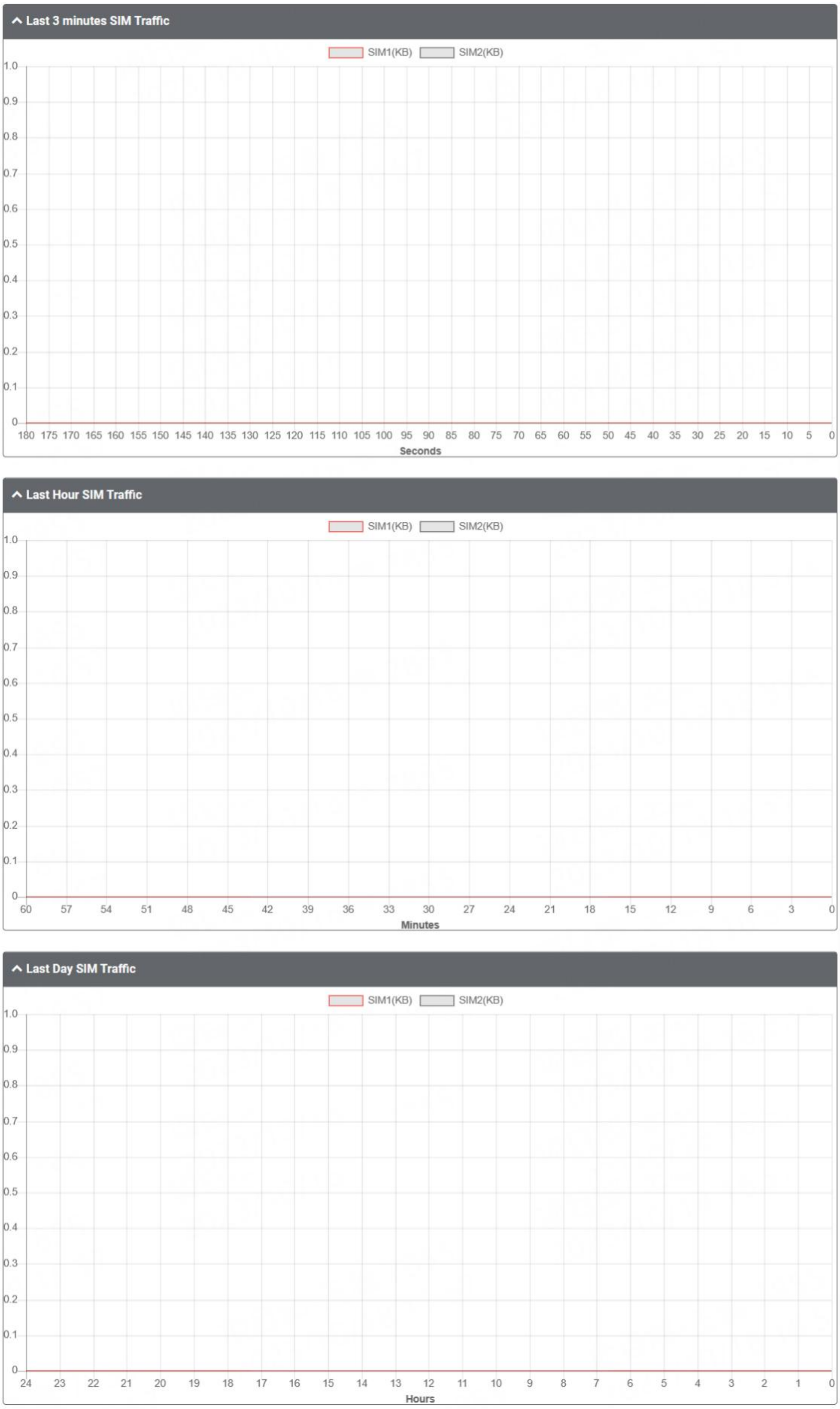
RAM Usage


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

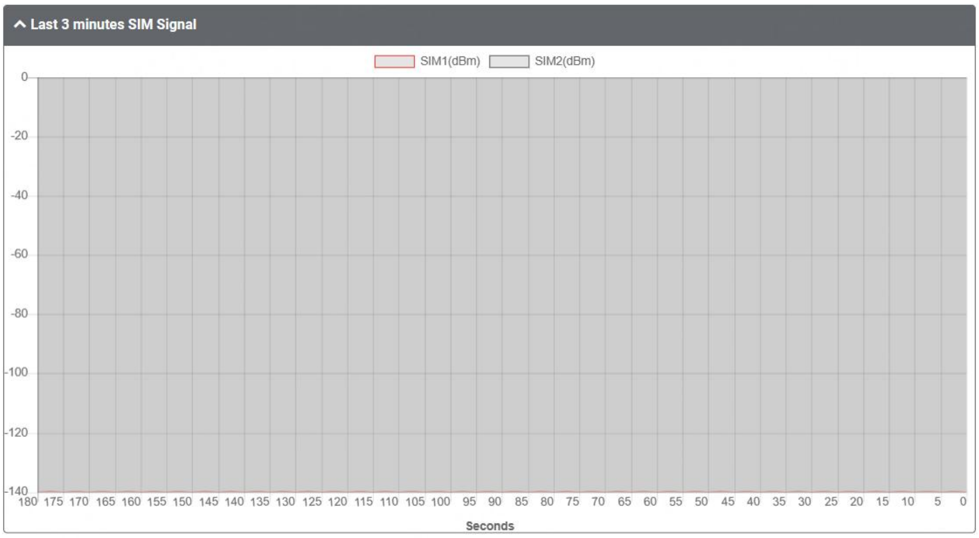

Last Hour RAM Usage
RAM(%)
50
45
40
35
30
25
20
15
10
5
0
60 57 54 51 48 45 42 39 36 33 30 27 24 21 18 15 12 9 6 3 0
Minutes

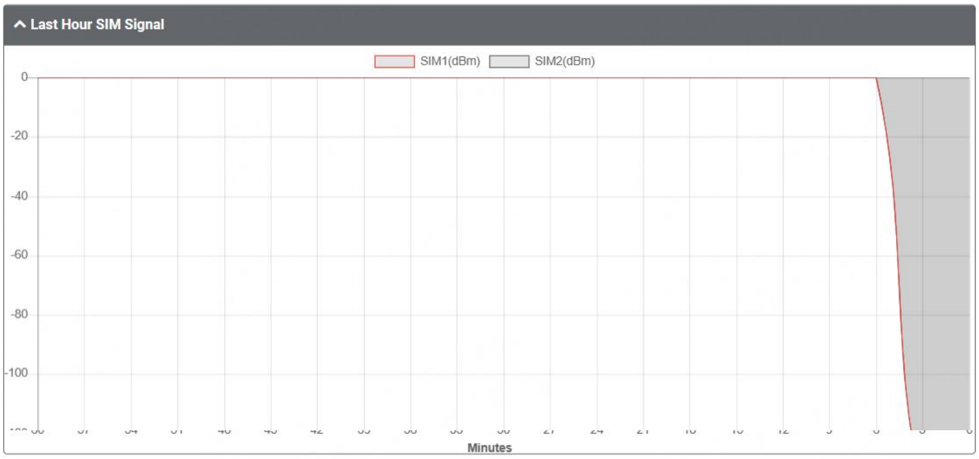

Last Day RAM Usage
RAM(%)
50
45
40
35
30
25
20
15
10
5
0
24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
Hours

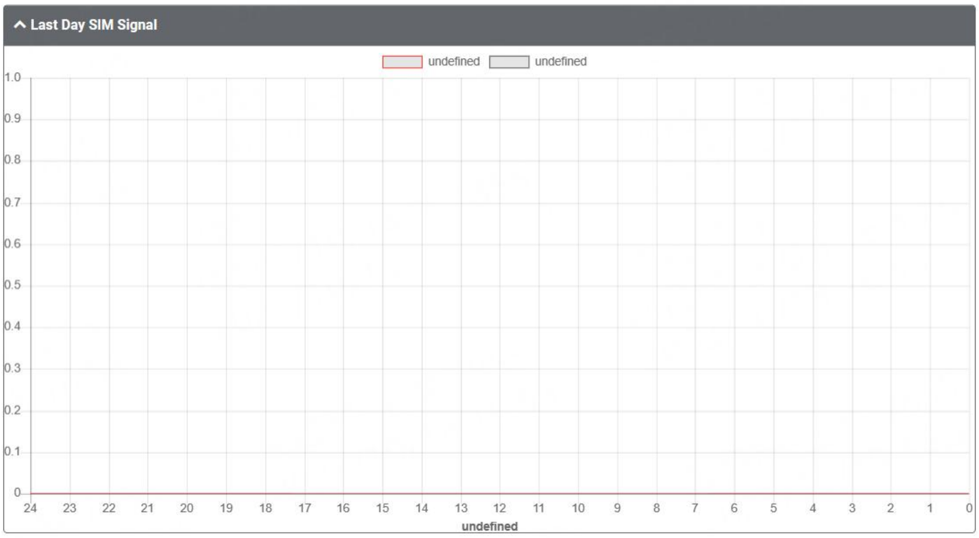
SIM Traffic


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)
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)
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

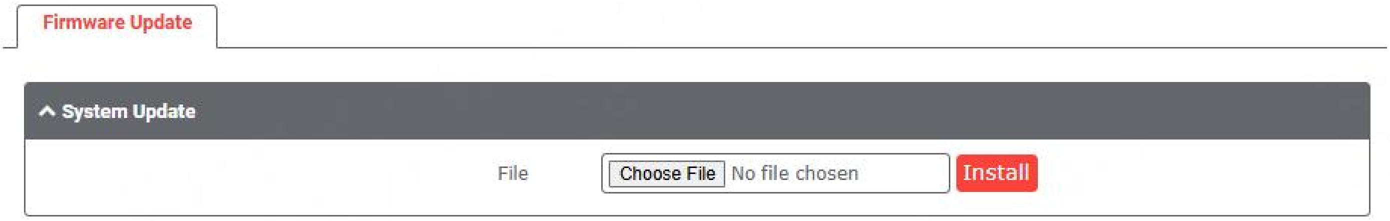

Last 3 minutes SIM Signal
SIM1(dBm)
SIM2(dBm)
0
-20
-40
-60
-80
-100
-120
-140
180 175 170 165 160 155 150 145 140 135 130 125 120 115 110 105 100 95 90 85 80 75 70 65 60 55 50 45 40 35 30 25 20 15 10 5 0
Seconds


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 Software Update

This section is used to upgrade the system of this device by importing and updating firmware files. Import the firmware file from the computer to this device, click Install, and follow the system prompts to restart the device to complete the firmware update.



Firmware Update

System Update

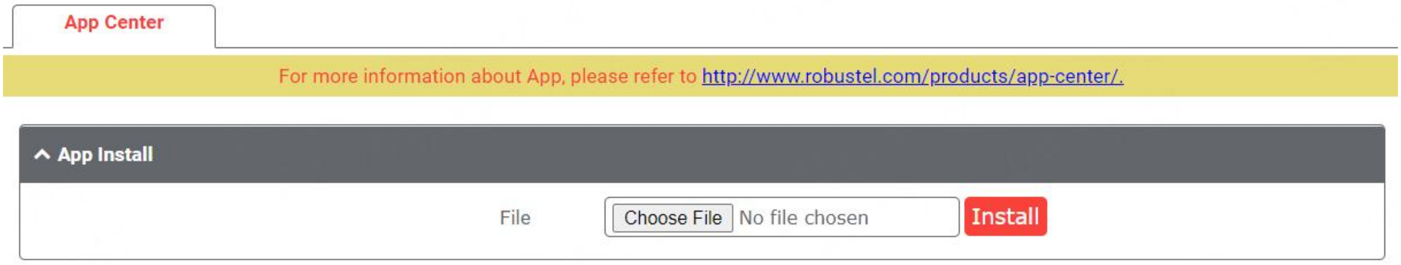
File | Choose File | No file chosen | Install

Item	Description	Default
File	Click "Select File" to find the application file from your PC, then click Install to import this file into the gateway.	--

3.7.5 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.



App Center

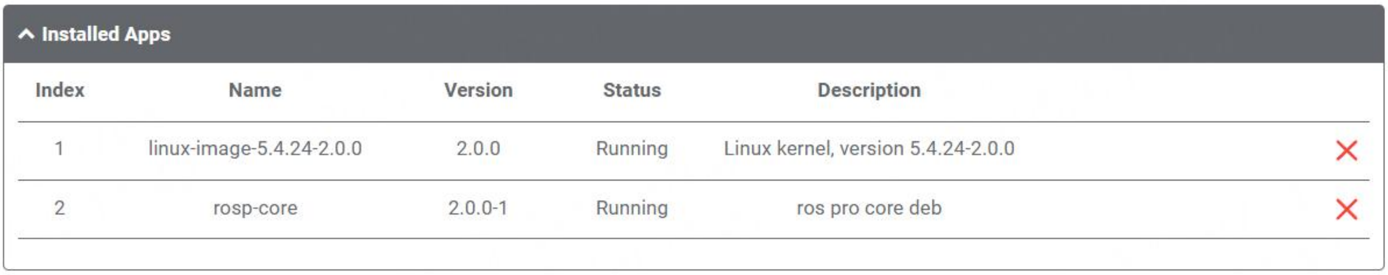
For more information about App, please refer to http://www.robustel.com/products/app-center/.

App Install

File | Choose File | No file chosen | Install

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.



Installed Apps

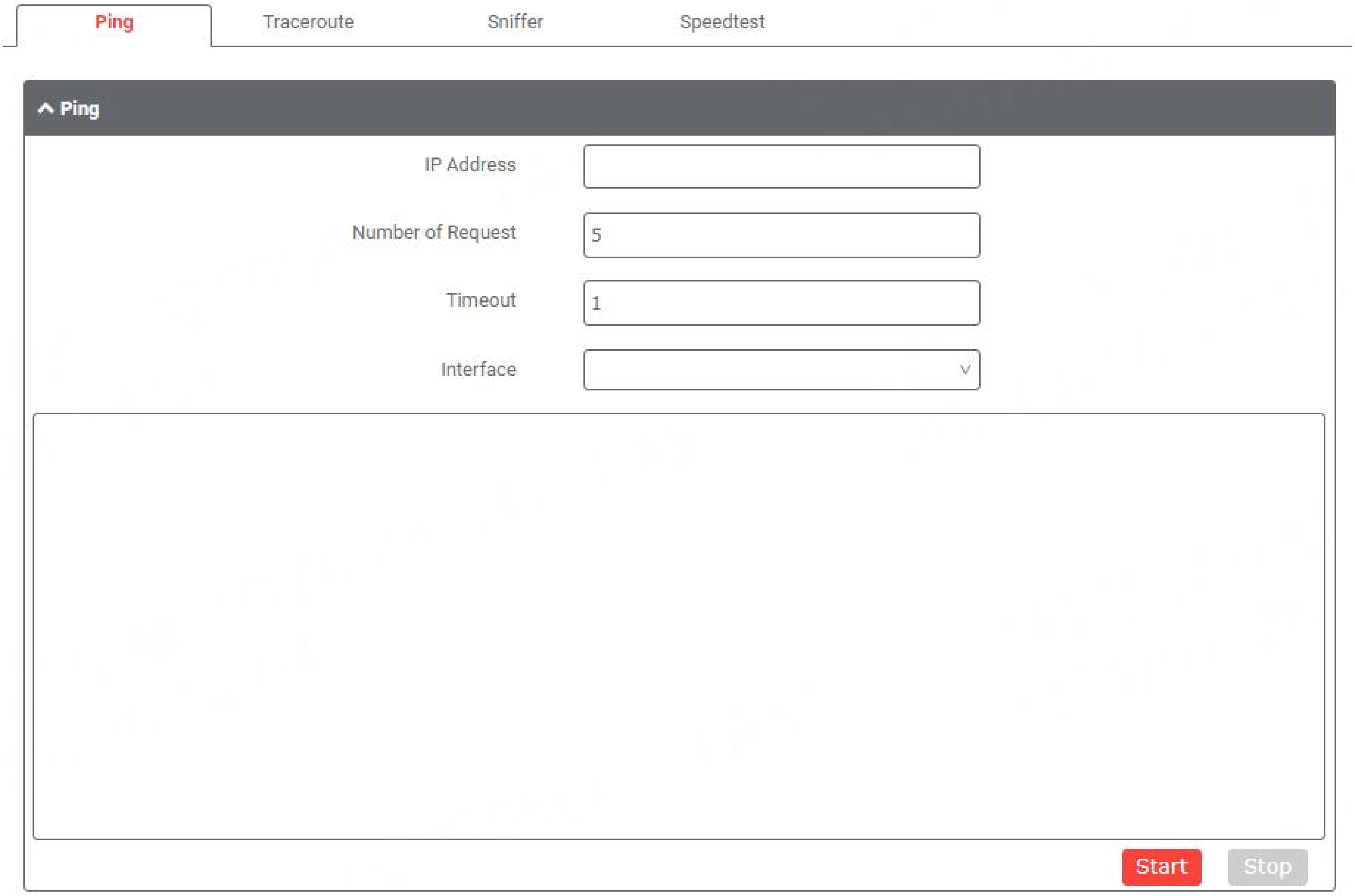
Index	Name	Version	Status	Description	
1	linux-image-5.4.24-2.0.0	2.0.0	Running	Linux kernel, version 5.4.24-2.0.0	✕
2	rosp-core	2.0.0-1	Running	ros pro core deb	✕

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

3.7.6 Tools

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

Ping



IP Address

Number of Request 5

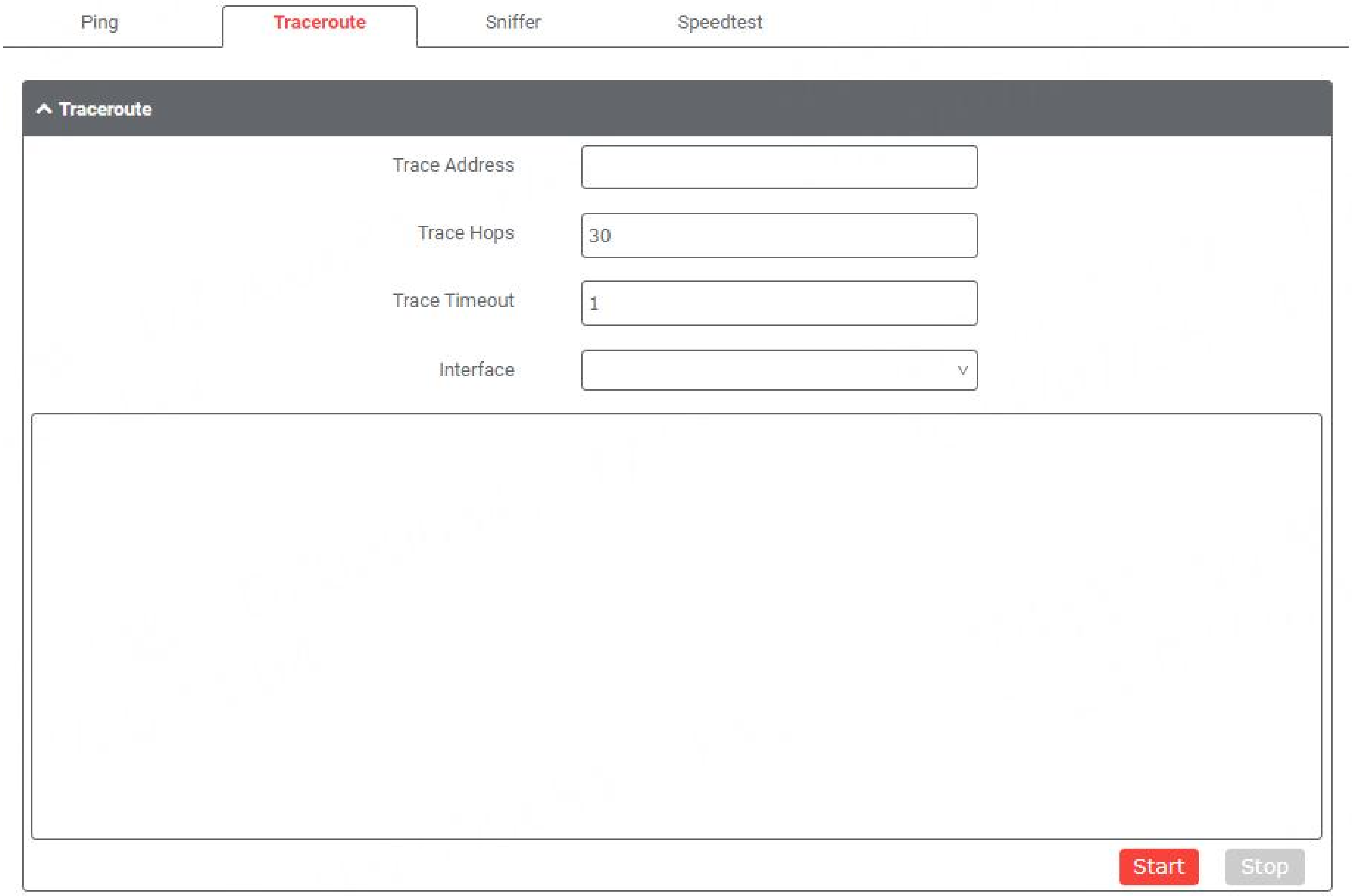
Timeout 1

Interface

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

	Null stands for selecting local IP address from these three automatically.	
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



Trace Address

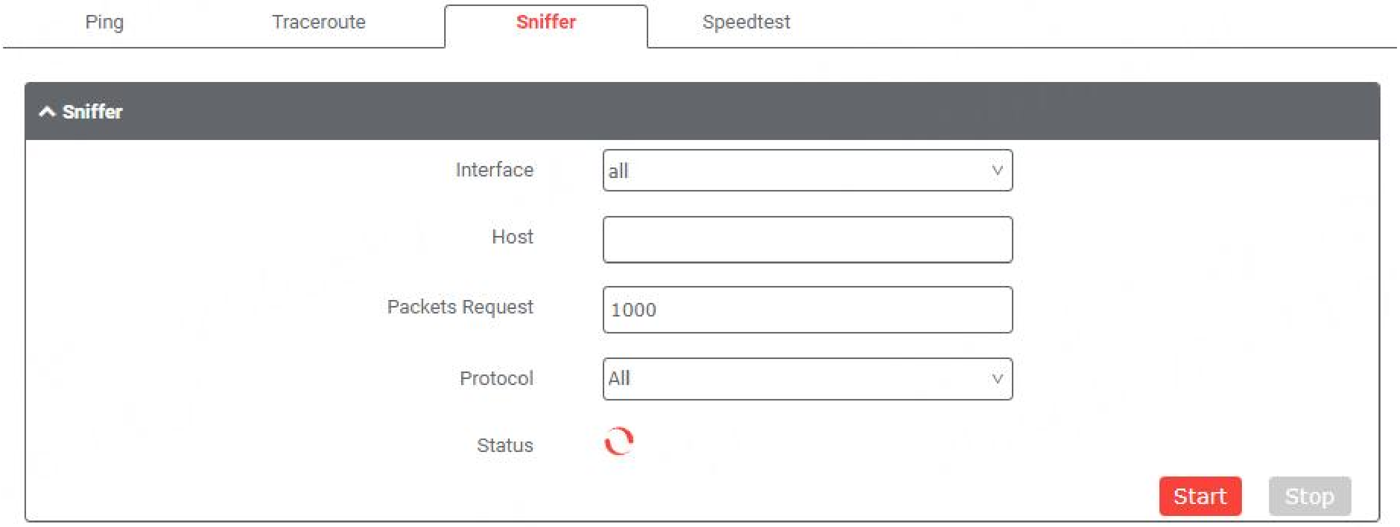
Trace Hops 30

Trace Timeout 1

Interface

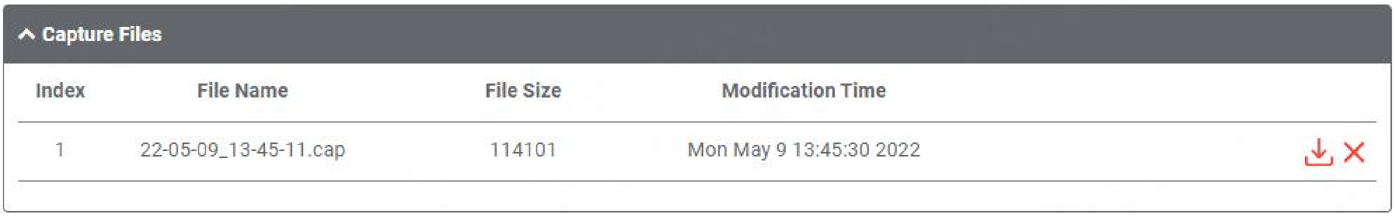
Item	Description	Default
Trace Address	Enter the trace’s destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify the timeout of Traceroute 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



Interface: all
Host:
Packets Request: 1000
Protocol: All
Status:

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.	--

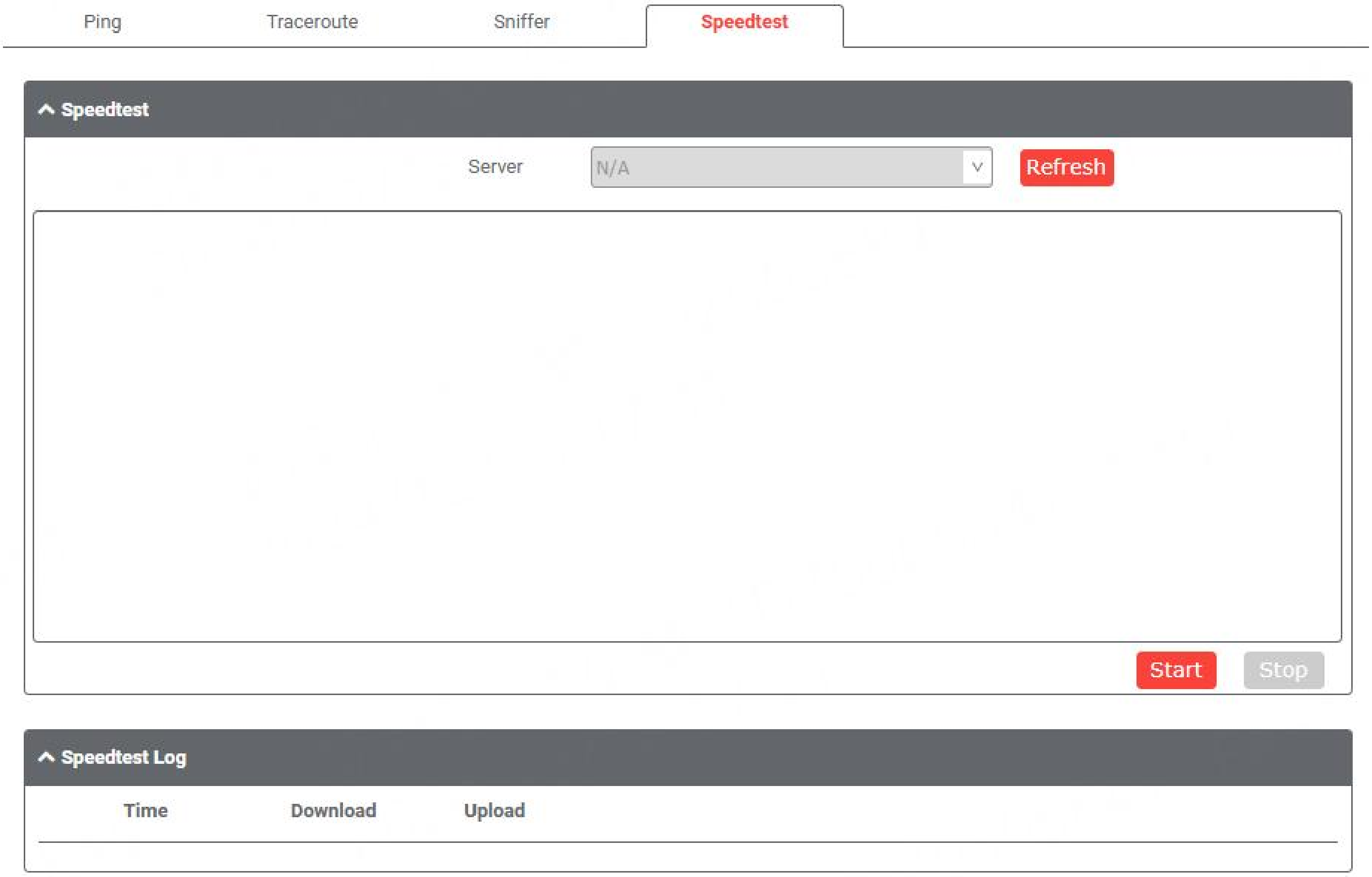


Index	File Name	File Size	Modification Time	
1	22-05-09_13-45-11.cap	114101	Mon May 9 13:45:30 2022	⤓ ✕

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.	--

Speed Test

This section allows you to use the Speed Test tools.



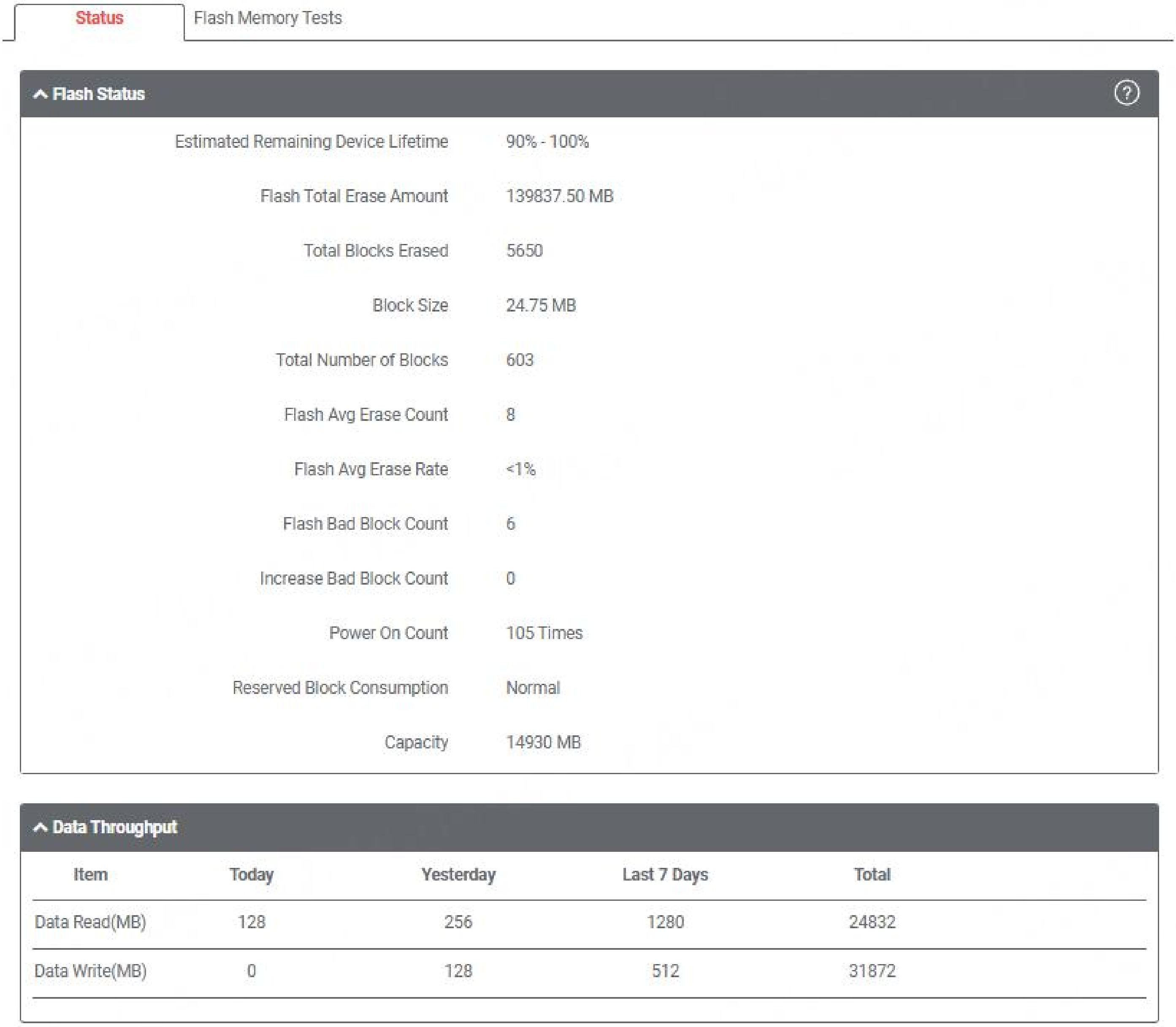
Speed Test		
Item	**Description**	**Default**
Refresh	Click this button to refresh the list of available speed test servers.	--
Start	Click this button to start the speed test, and the test information will be displayed in real time in the upper window.	--
Stop	Click this button to stop execution of the current test.	--
Clear	Clear speed test records.	

3.7.7 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.



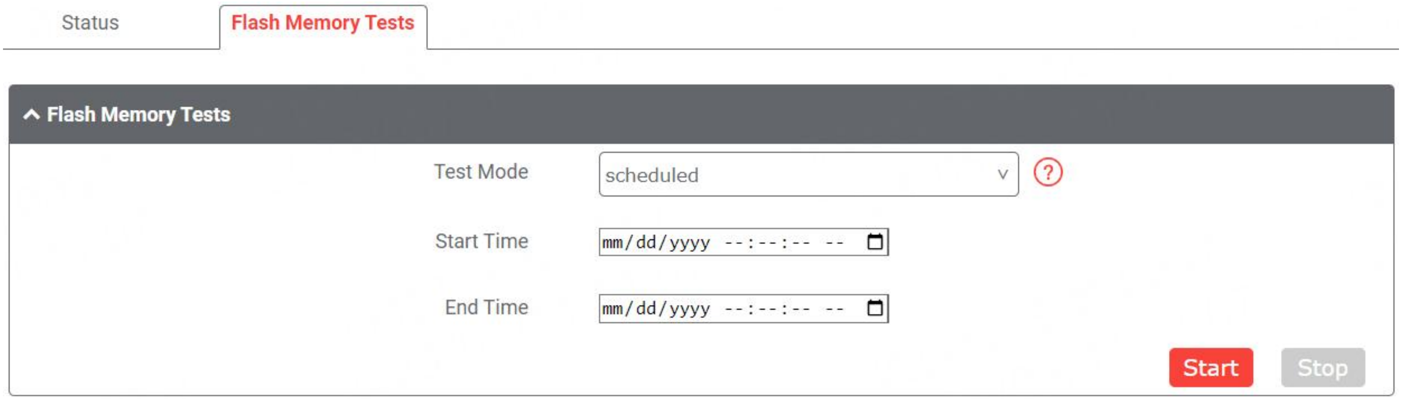
Flash Status

Estimated Remaining Device Lifetime	90% - 100%
Flash Total Erase Amount	139837.50 MB
Total Blocks Erased	5650
Block Size	24.75 MB
Total Number of Blocks	603
Flash Avg Erase Count	8
Flash Avg Erase Rate	<1%
Flash Bad Block Count	6
Increase Bad Block Count	0
Power On Count	105 Times
Reserved Block Consumption	Normal
Capacity	14930 MB

Data Throughput

Item	Today	Yesterday	Last 7 Days	Total
Data Read(MB)	128	256	1280	24832
Data Write(MB)	0	128	512	31872

Flash Memory Tests



Test Mode: scheduled

Start Time: mm/dd/yyyy --:--:-- --

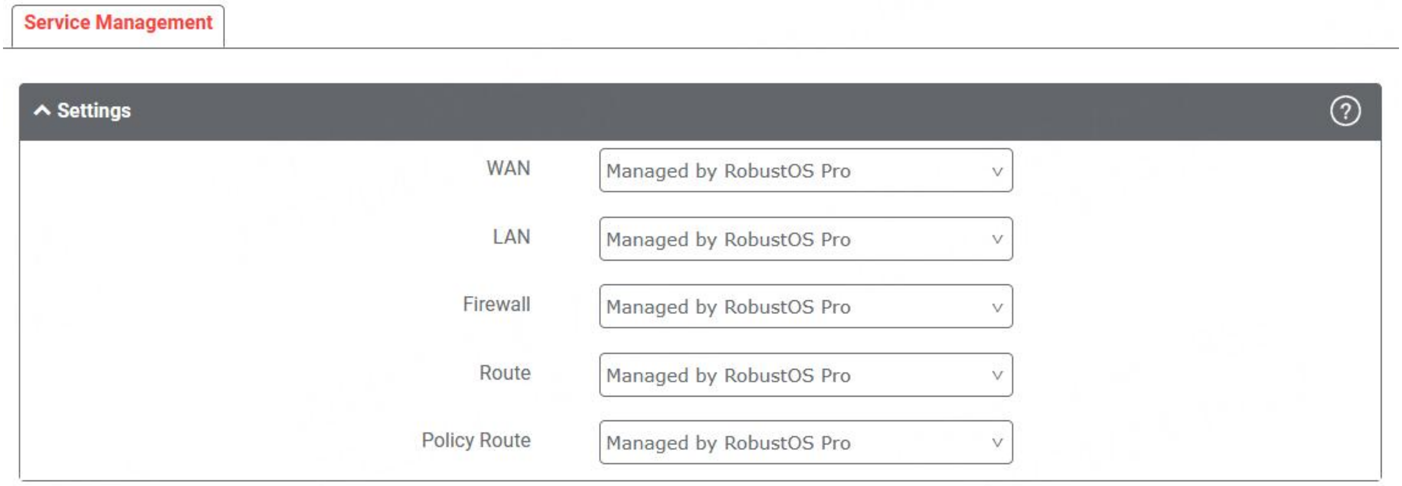
End Time: mm/dd/yyyy --:--:-- --

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.

3.7.8 Service Management

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



WAN: Managed by RobustOS Pro

LAN: Managed by RobustOS Pro

Firewall: Managed by RobustOS Pro

Route: Managed by RobustOS Pro

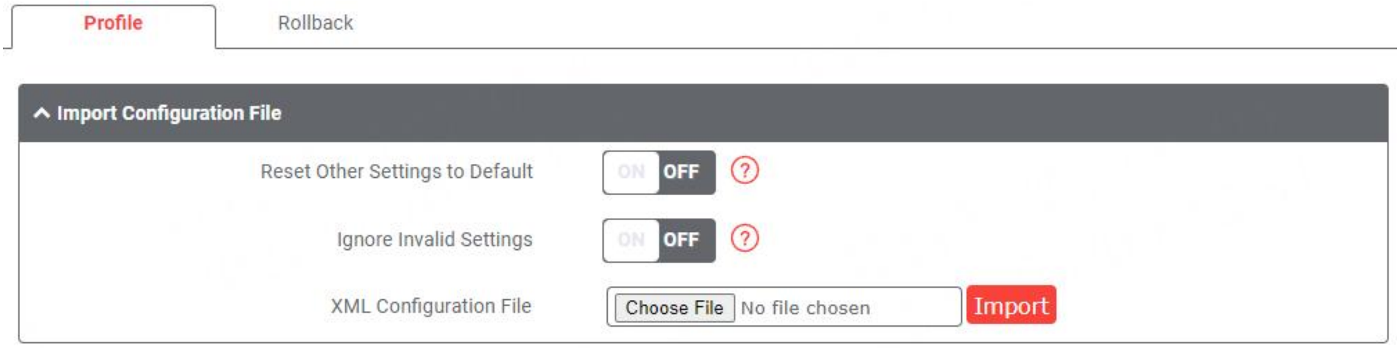
Policy Route: Managed by RobustOS Pro

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	√

3.7.9 Profile

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

Profile



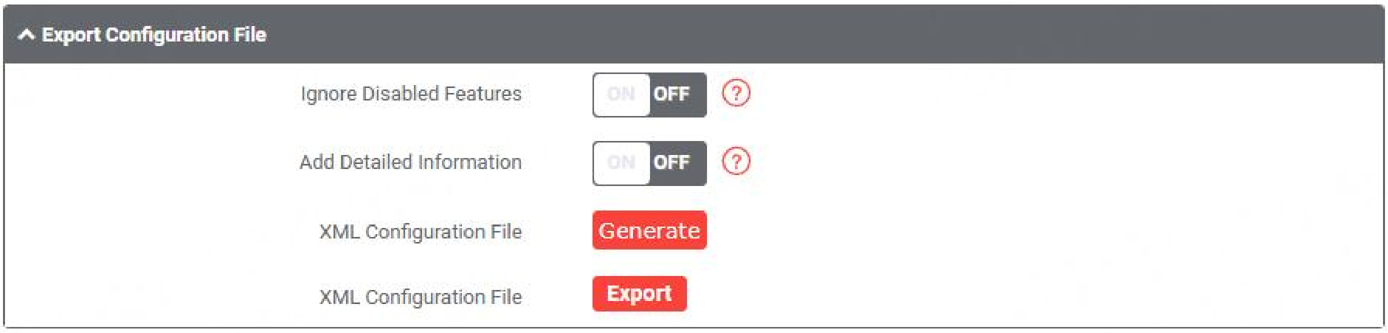
Reset Other Settings to Default: ON OFF

Ignore Invalid Settings: ON OFF

XML Configuration File: Choose File No file chosen Import

Item	Description	Default
Reset Other	Click the toggle button as "ON" to return other parameters to default	OFF

Settings to Default	settings.	
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.	--



Export Configuration File

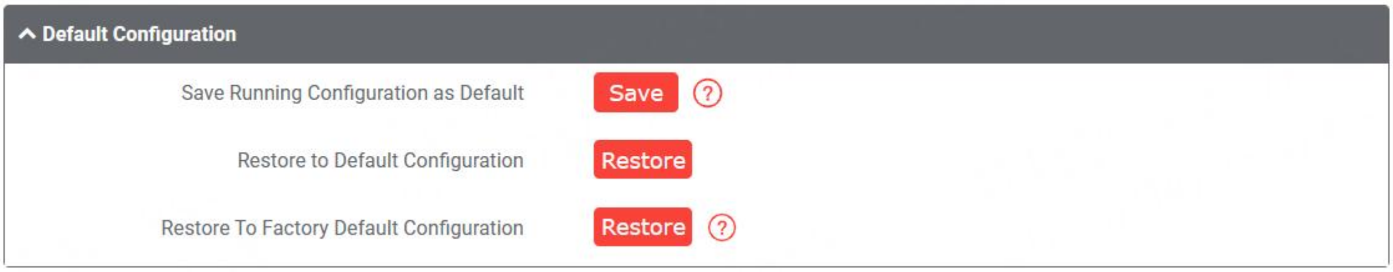
Ignore Disabled Features: ON OFF

Add Detailed Information: ON OFF

XML Configuration File: Generate

XML Configuration File: Export

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.	--



Default Configuration

Save Running Configuration as Default: Save

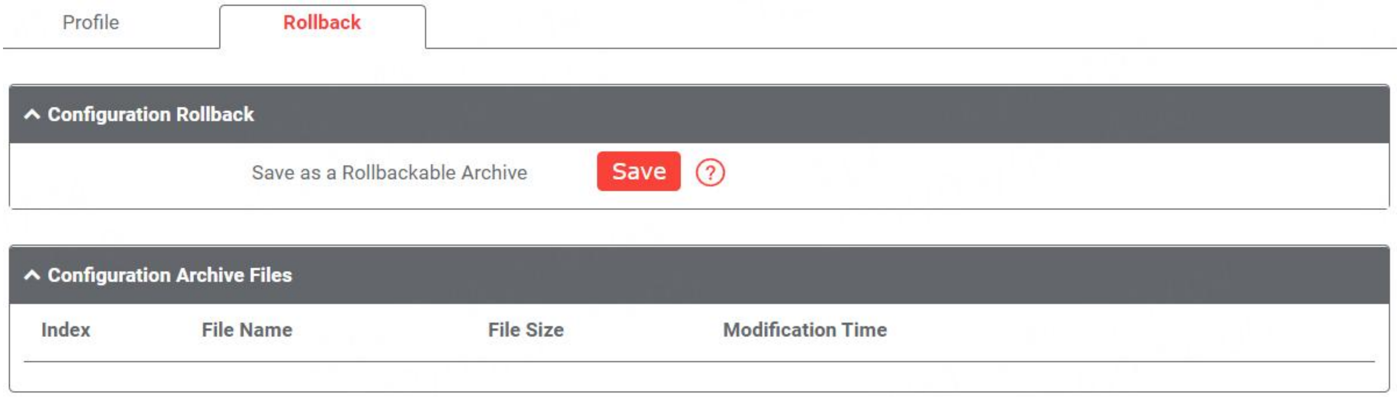
Restore to Default Configuration: Restore

Restore To Factory Default Configuration: Restore

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. **Important: Performing a factory reset will clear all data and personal**	--

	settings on your device and perform a system reset. This process is expected to take about 1 minute and will automatically restart the device. **** To avoid data loss or device damage, please ensure that the device has sufficient power during the entire process. If power is lost during the operation, you may need to restore the device by flashing the device with a USB flash drive. ****	

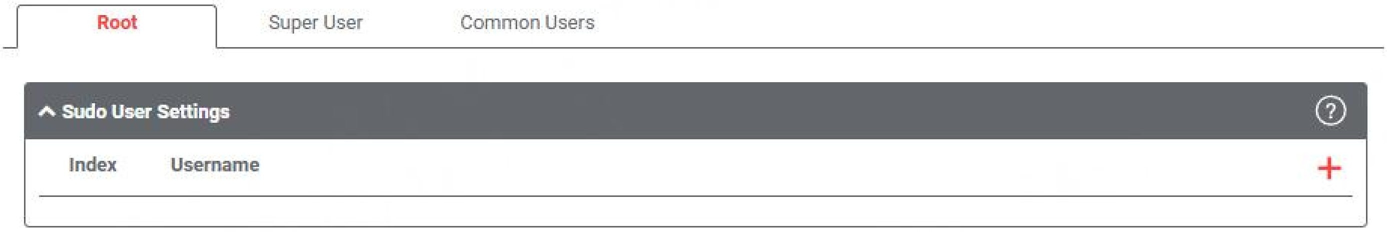
Rollback



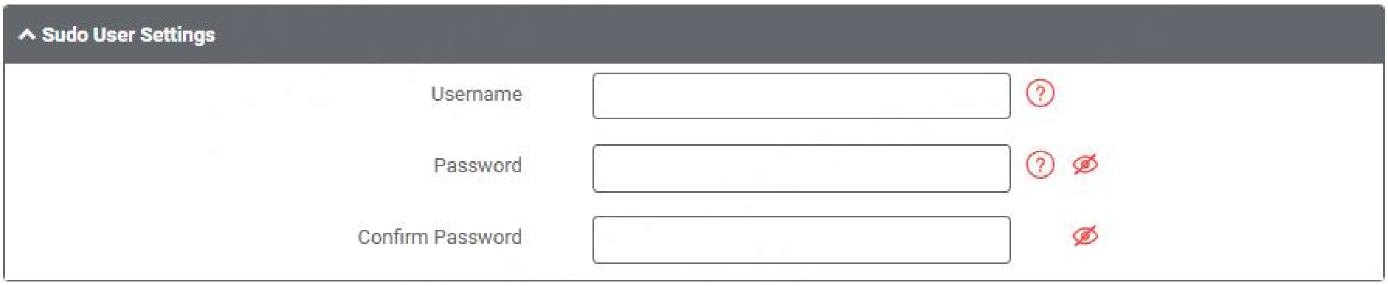
Item	Description	Default
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point every day automatically if configuration changes.	--
Configuration Archive Files	View the related information about configuration archive files, including name, size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

3.7.10 User Management

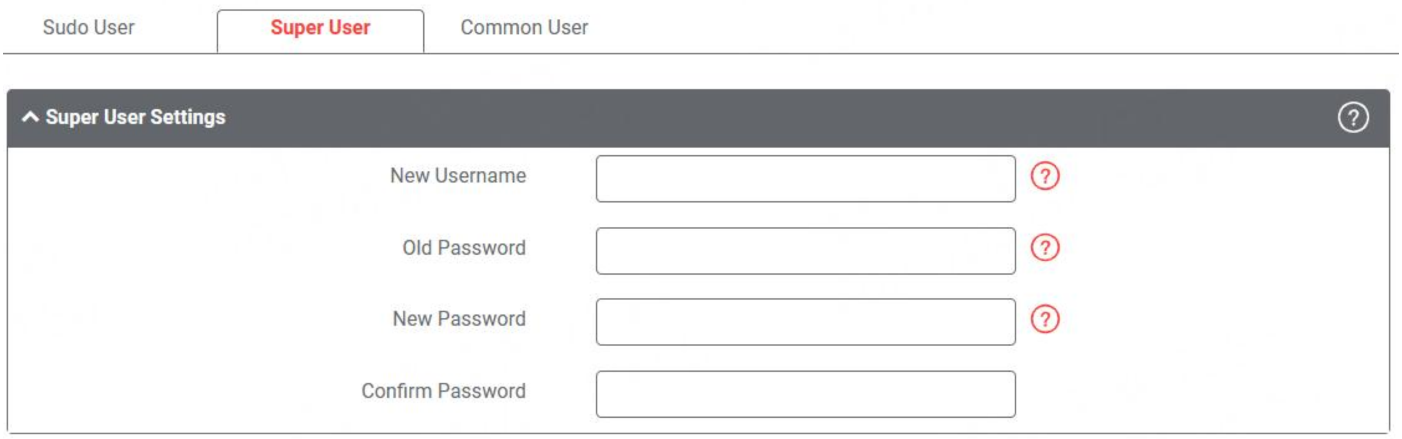
This section allows you to change your username and password, and create or manage user accounts. One device has only one super user who has the highest authority to modify, add and manage other common users.



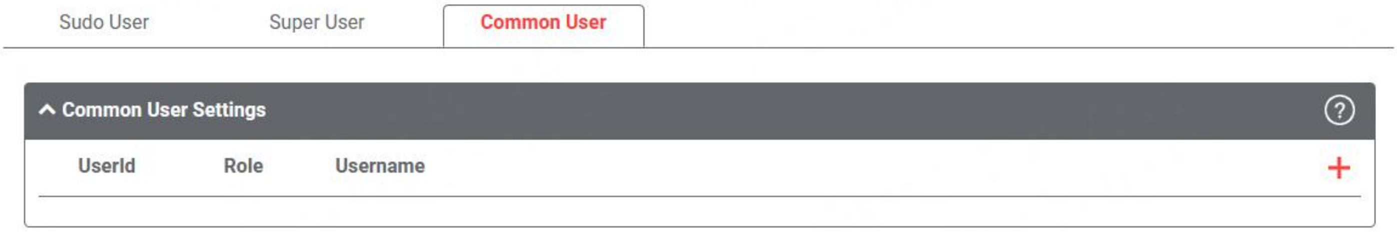
Click + button to add a new sudo user. A maximum of 1 sudo user can be configured.



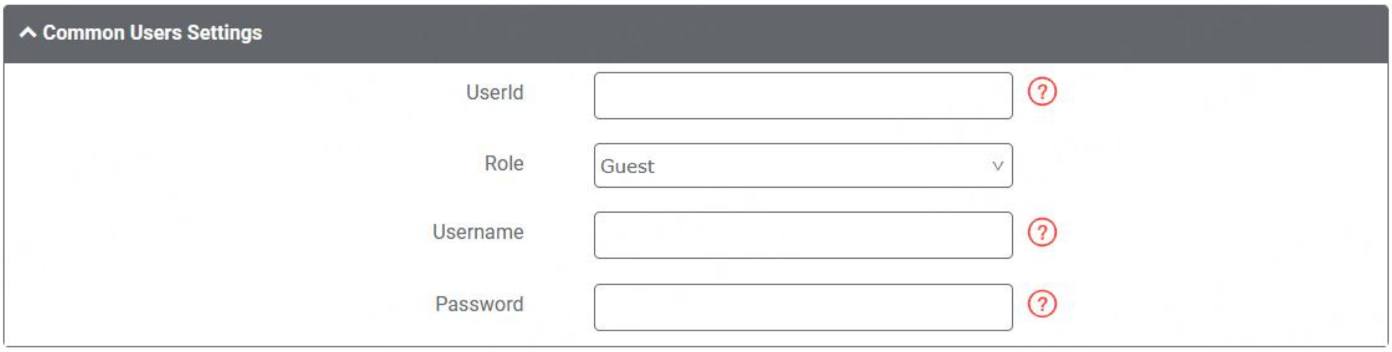
Item	Description	Default
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, $, and *.	Null
Old Password	Enter the old password for the sudo account. This option will be displayed when you need to change the sudo password.	Null
New Password	Enter a new 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.



UserId

Role: Guest

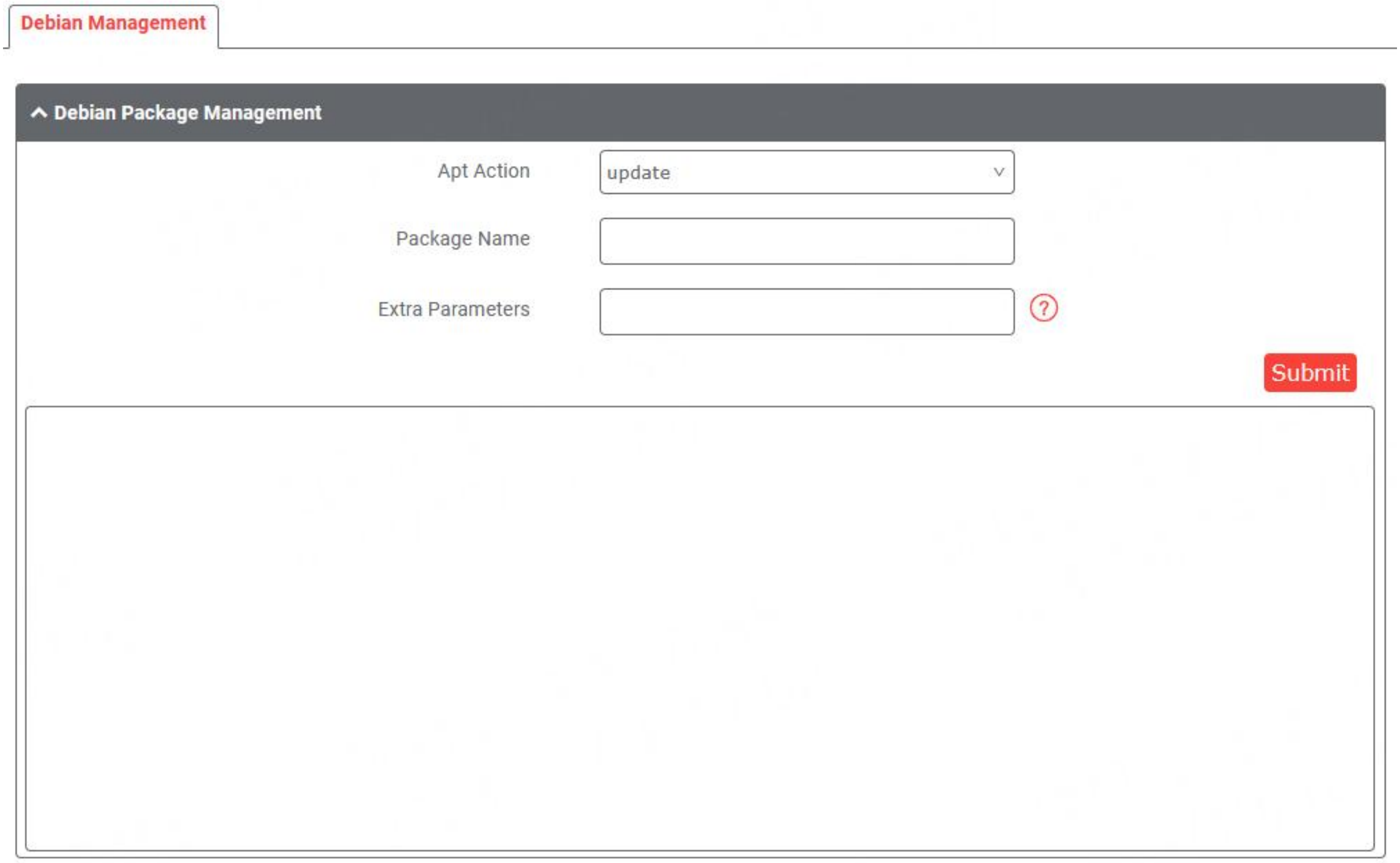
Username

Password

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

3.7.11 Debian Management

This section allows you to manage your own Debian packages.



Debian Management

Debian Package Management

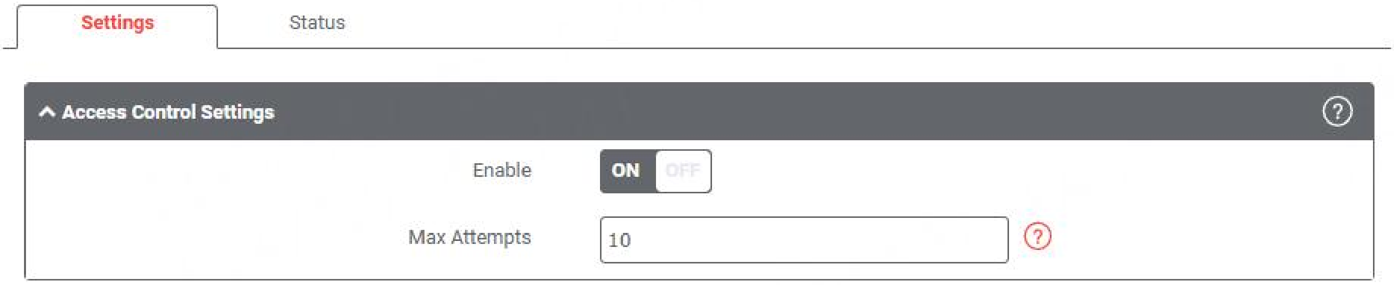
Apt Action	update
Package Name	
Extra Parameters	

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

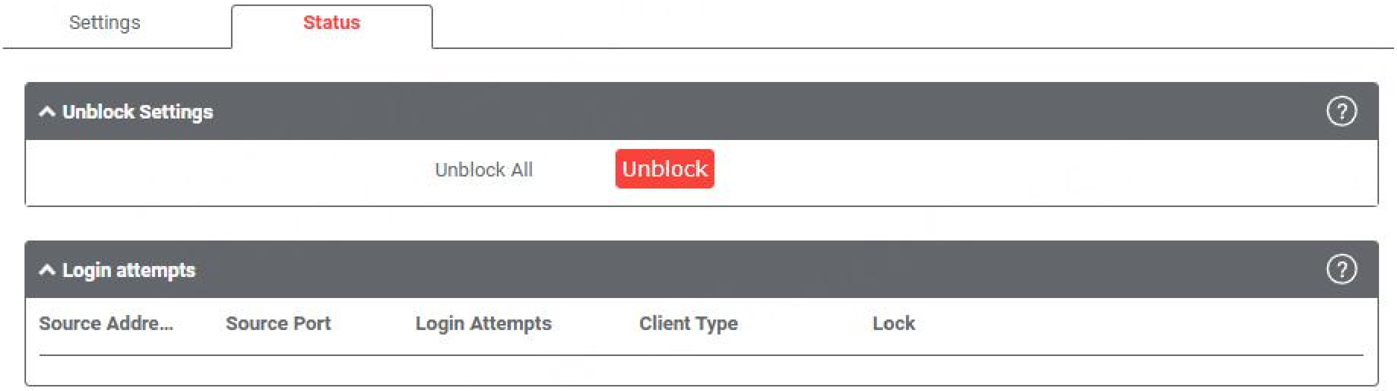
3.7.12 Access Control

This section is used for device security access control management related settings. If the same IP address enters incorrect account or password a specified number of times, this IP will be restricted from accessing the device. It also provides the function of removing restrictions on IP addresses in batches or individually.

Note: Before reaching the upper limit of incorrect login attempts, the accumulated number of errors will be cleared after successful login.



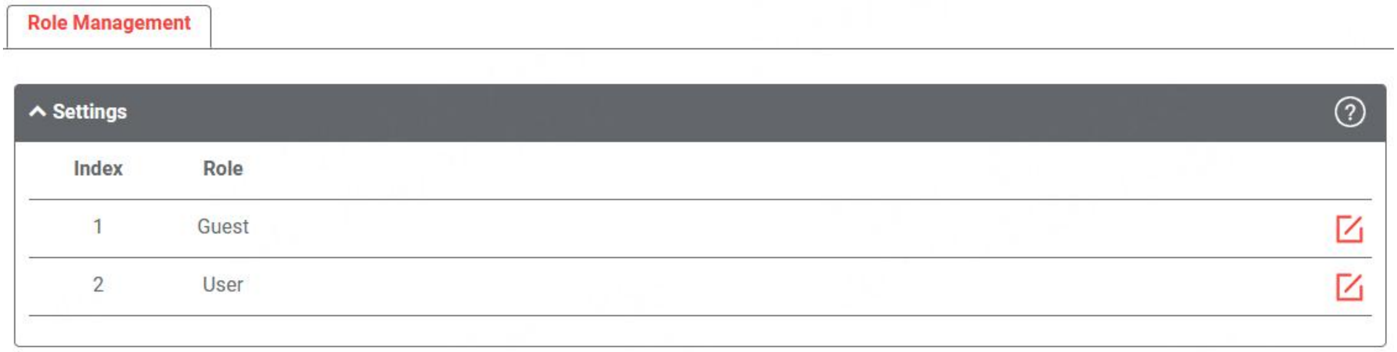
Item	Description	Default
Enable	Enable/disable secure login access.	On
Max Attempts	If the same IP address enters incorrect account or password for a specified number of times, this IP will be restricted from accessing the device. The value range is 1 to 30.	10



Item	Descripton	Default
Unblock All	Click Unblock button to remove the restricted access IP addresses recorded on the device in batches.	--

3.7.13 Role Management

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

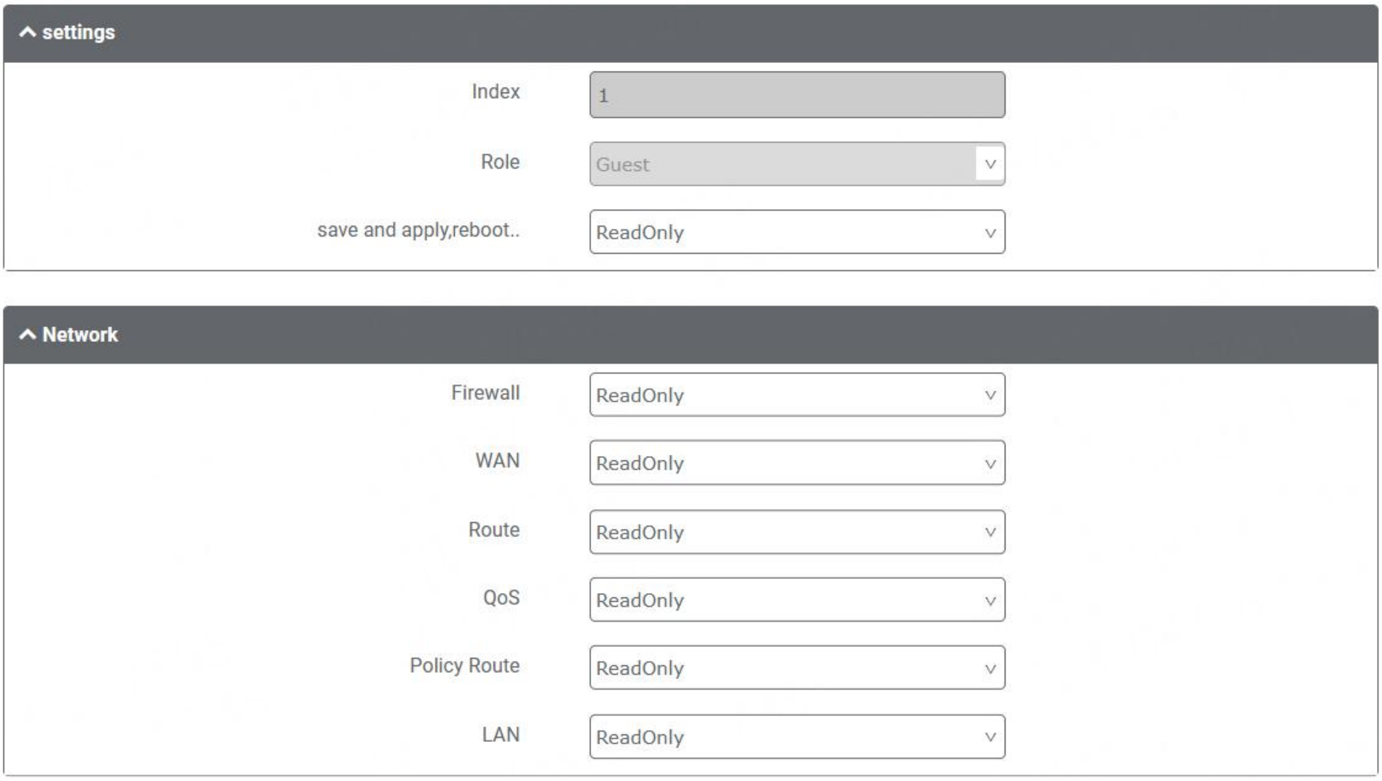


Role Management

Settings

Index	Role
1	Guest
2	User

Click ✎ to edit Visitor/Editor permission.

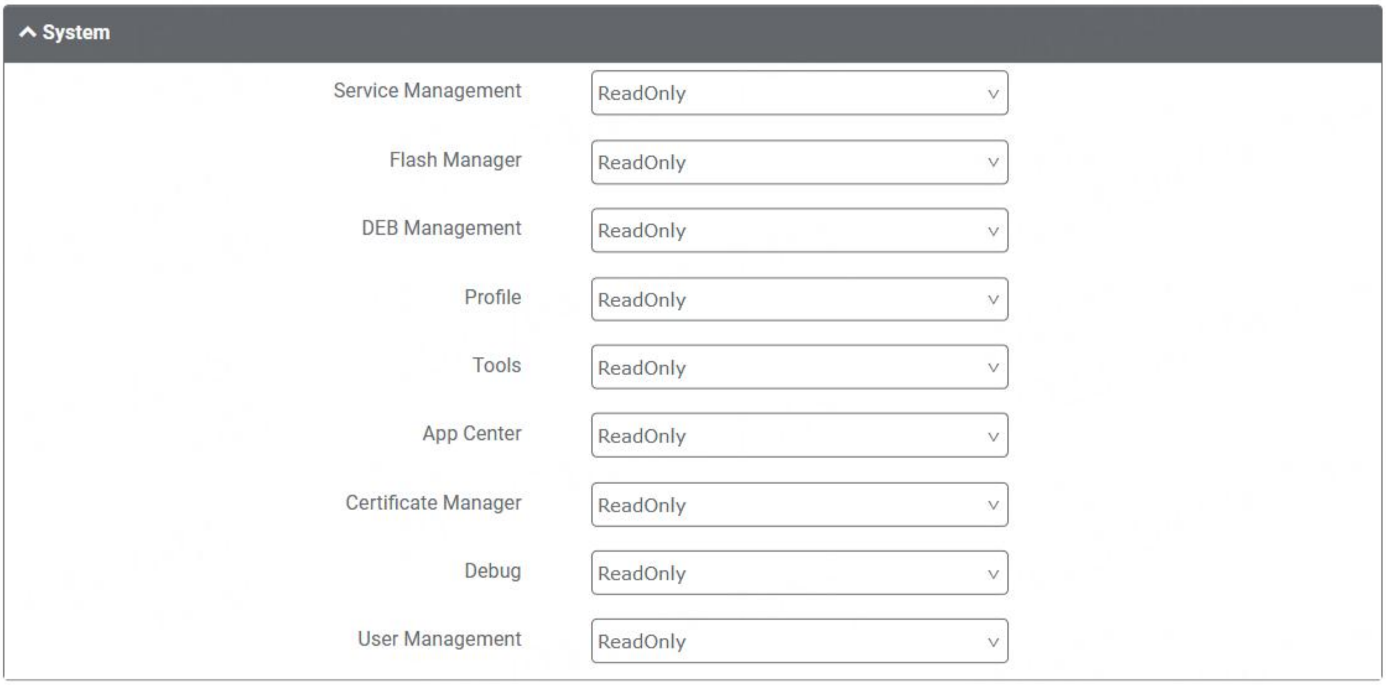


settings

Index	1
Role	Guest
save and apply,reboot..	ReadOnly

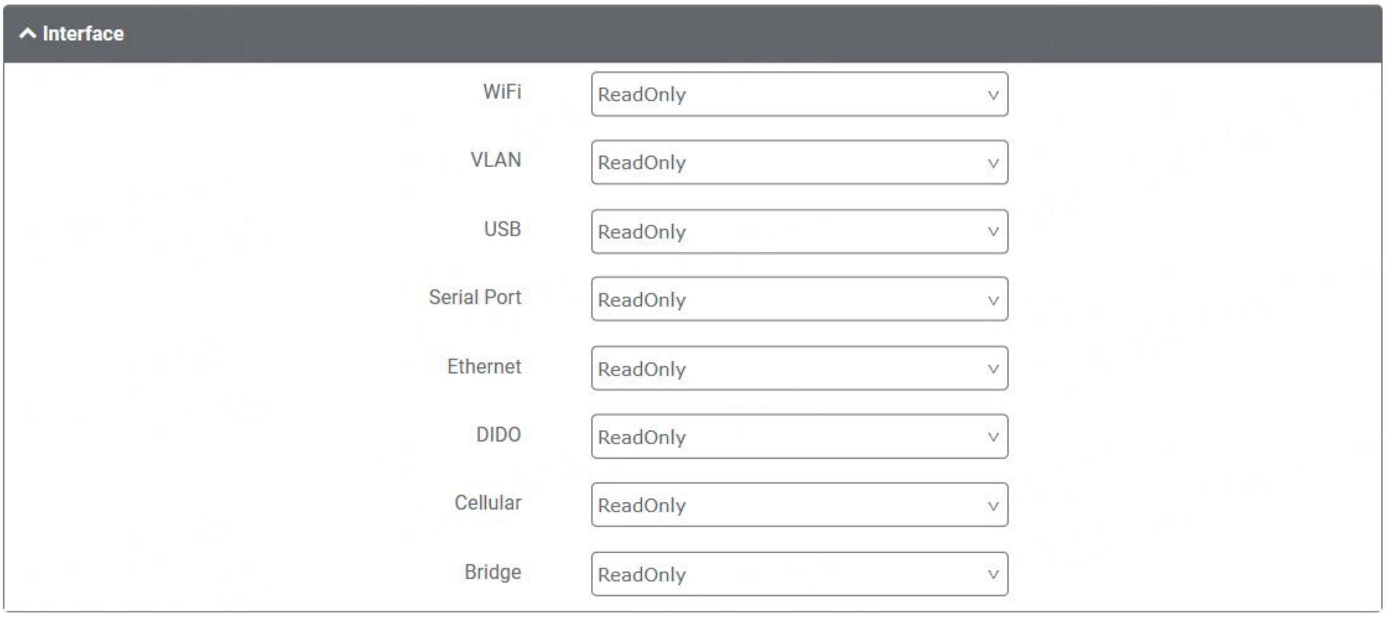
Network

Firewall	ReadOnly
WAN	ReadOnly
Route	ReadOnly
QoS	ReadOnly
Policy Route	ReadOnly
LAN	ReadOnly



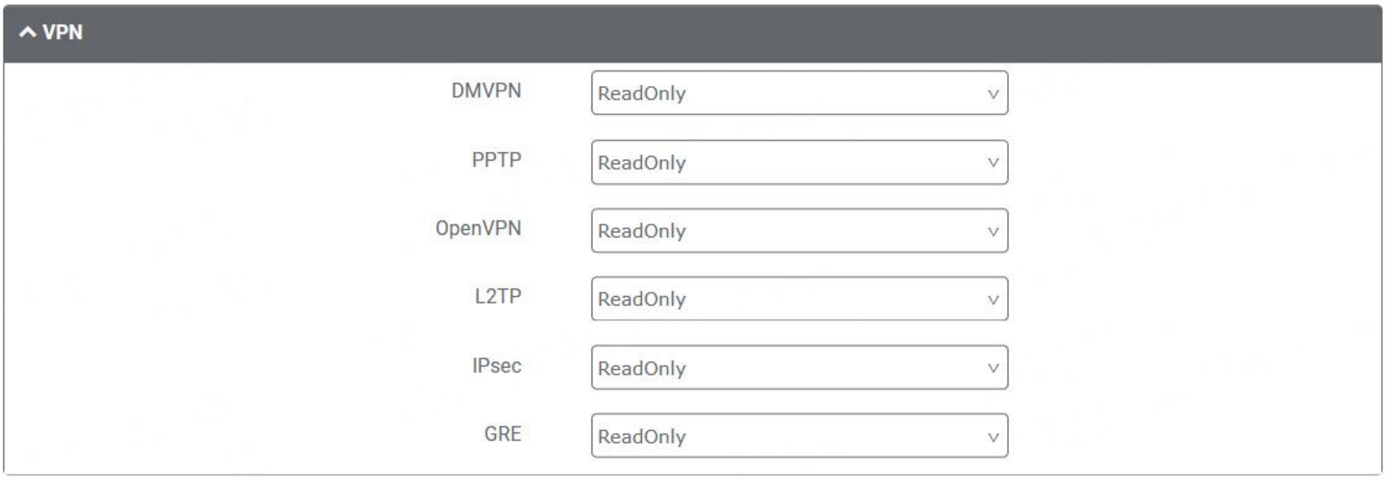
System

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



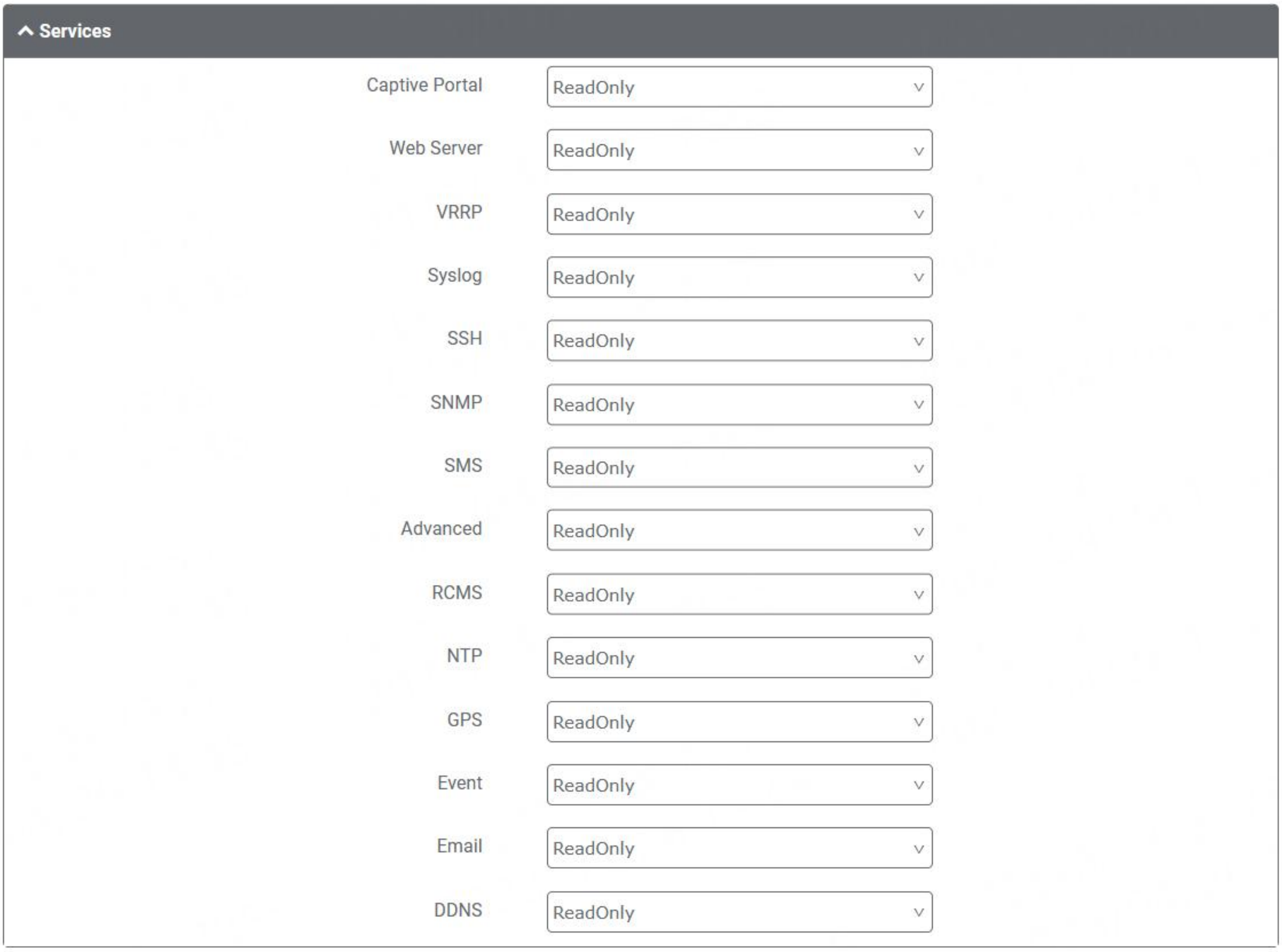
Interface

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



^ Services

Captive Portal	ReadOnly
Web Server	ReadOnly
VRRP	ReadOnly
Syslog	ReadOnly
SSH	ReadOnly
SNMP	ReadOnly
SMS	ReadOnly
Advanced	ReadOnly
RCMS	ReadOnly
NTP	ReadOnly
GPS	ReadOnly
Event	ReadOnly
Email	ReadOnly
DDNS	ReadOnly

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:

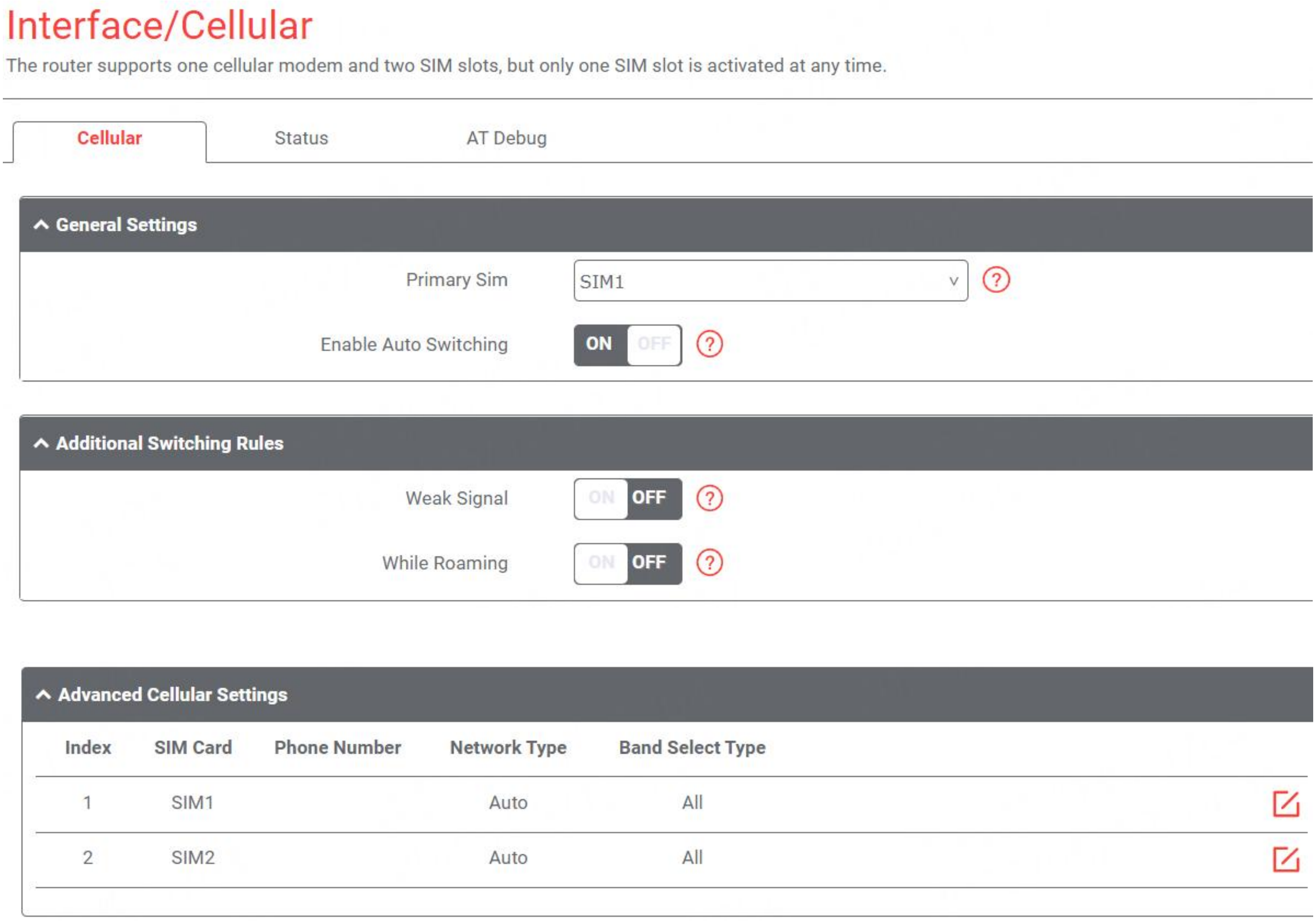
1. When logging in with Guest/User, “Profile” is not available.
2. When Guest “Save and apply, reboot” permission was set to “ReadOnly”. After logging as Guest, “save and apply”, “reboot” buttons will not be displayed.

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.



Interface/Cellular

The router supports one cellular modem and two SIM slots, but only one SIM slot is activated at any time.

General Settings

Primary Sim	SIM1
Enable Auto Switching	ON

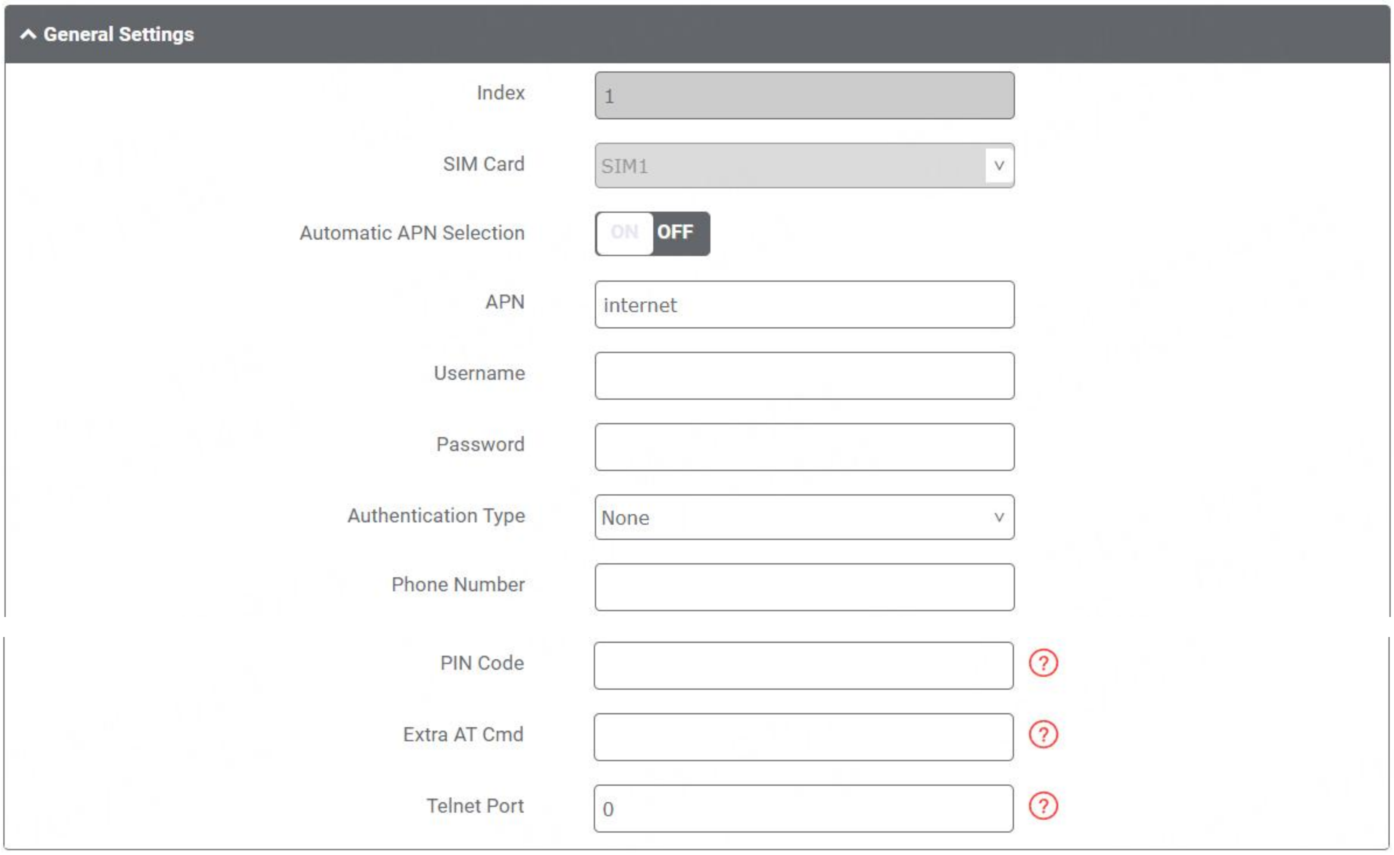
Additional Switching Rules

Weak Signal	OFF
While Roaming	OFF

Advanced Cellular Settings

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

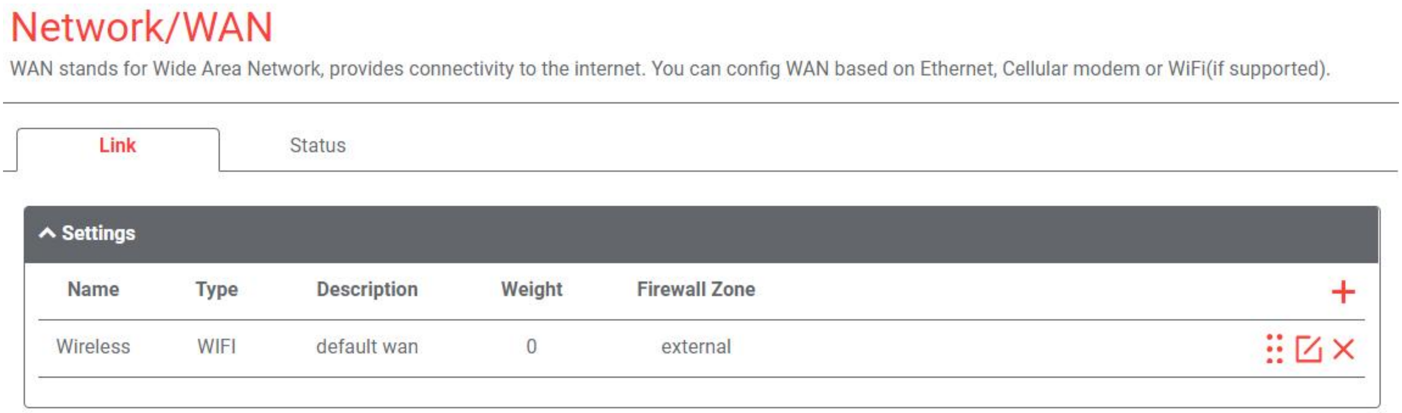
Click ✎ to set its parameters according to the current ISP.



^ General Settings

Index	1
SIM Card	SIM1
Automatic APN Selection	ON OFF
APN	internet
Username	
Password	
Authentication Type	None
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0

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

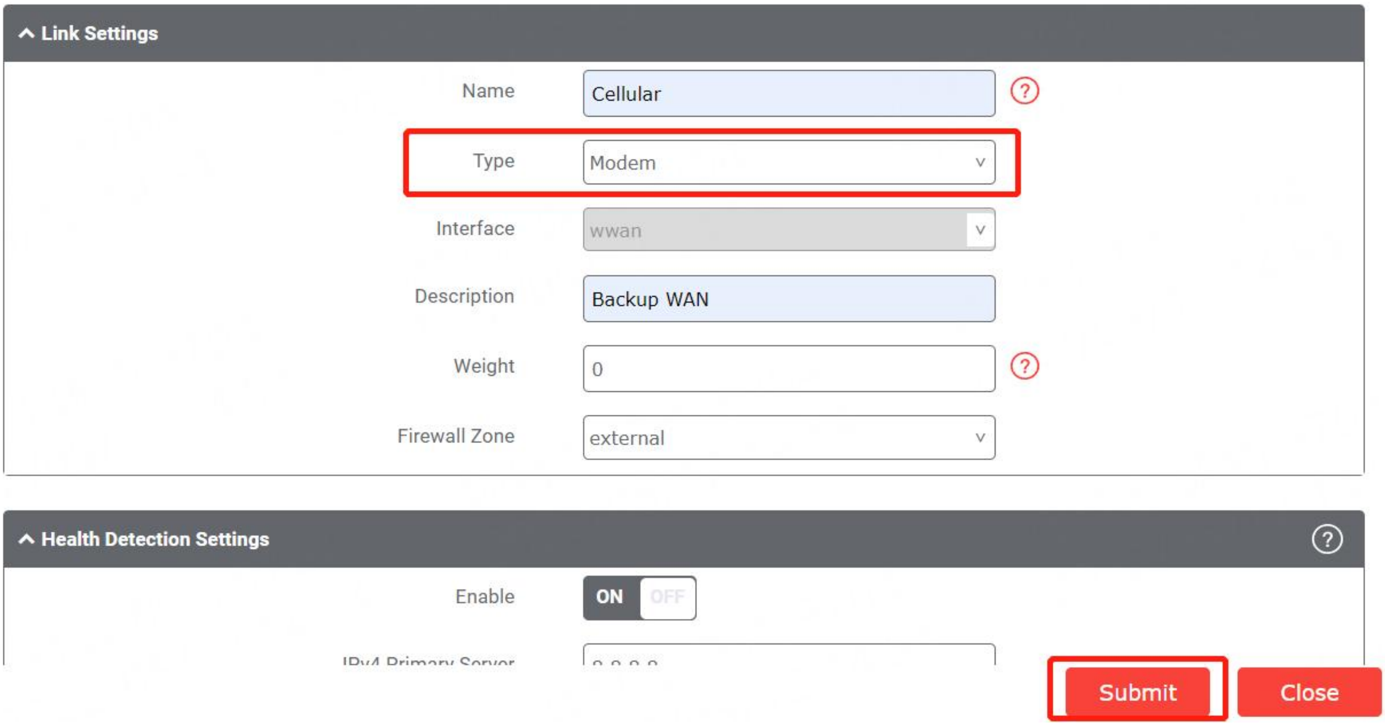


Network/WAN

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

Name	Type	Description	Weight	Firewall Zone
Wireless	WIFI	default wan	0	external

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



Link Settings

Name: Cellular

Type: Modem

Interface: wwan

Description: Backup WAN

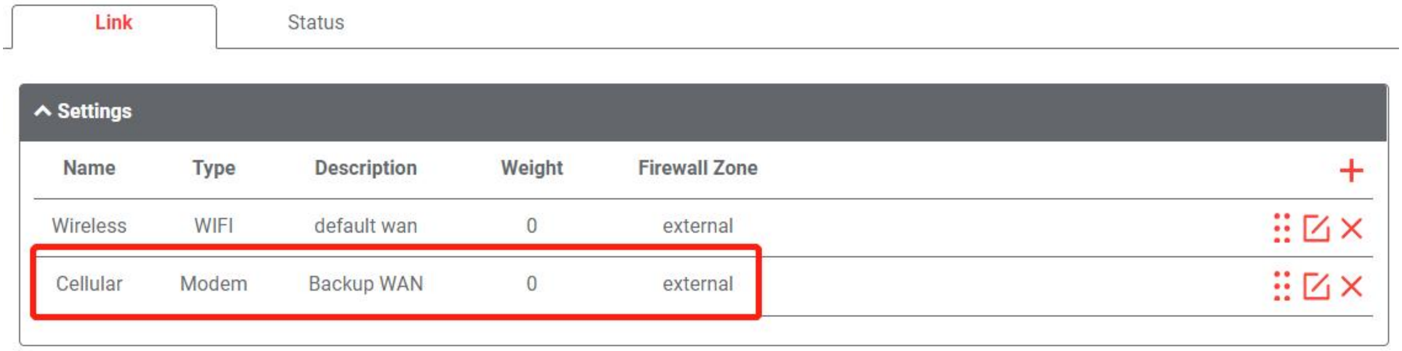
Weight: 0

Firewall Zone: external

Health Detection Settings

Enable: ON

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



Name	Type	Description	Weight	Firewall Zone
Wireless	WIFI	default wan	0	external
Cellular	Modem	Backup WAN	0	external

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.

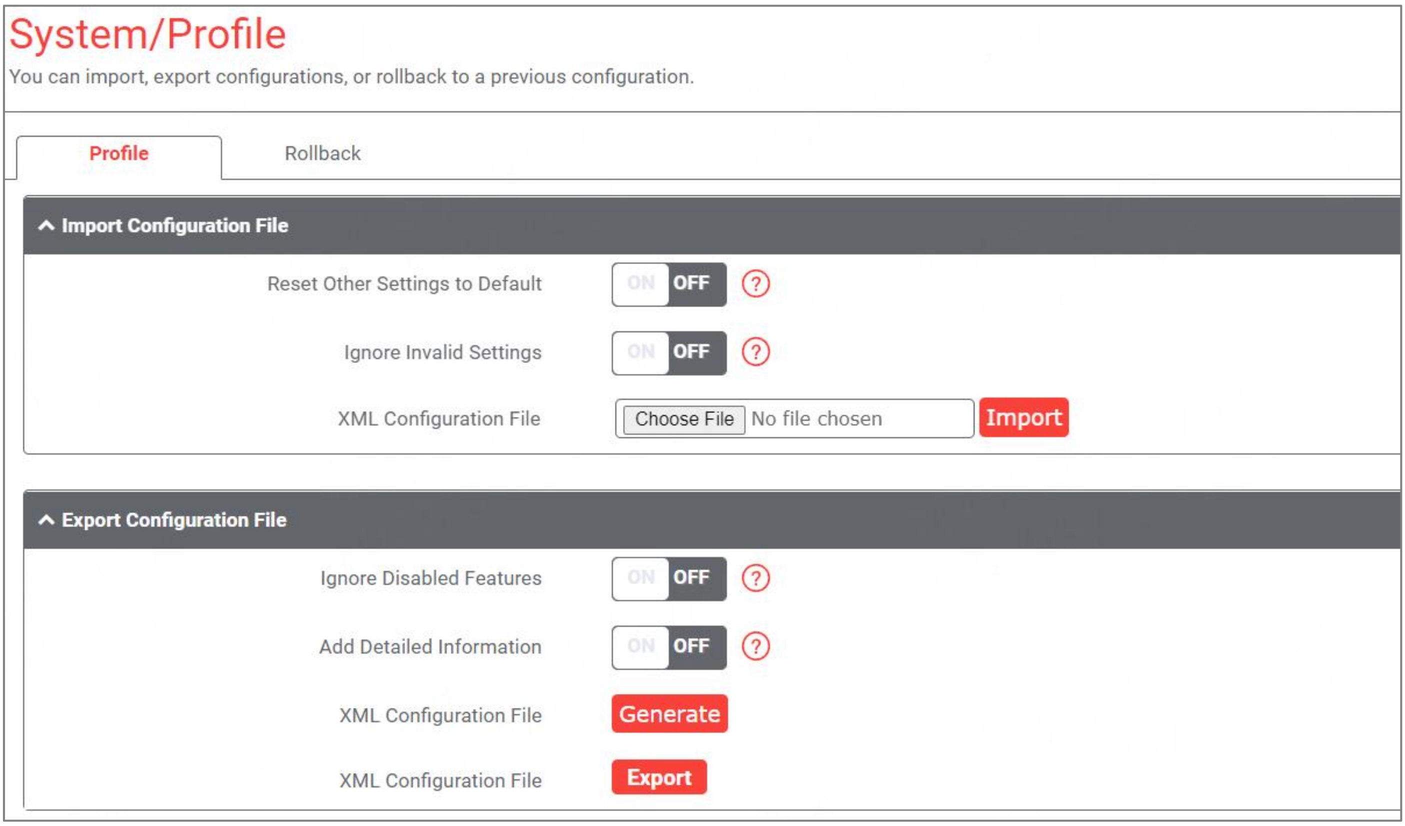
SMS command Explanation:

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.



System/Profile

You can import, export configurations, or rollback to a previous configuration.

Import Configuration File

Reset Other Settings to Default: ON OFF

Ignore Invalid Settings: ON OFF

XML Configuration File: Choose File No file chosen Import

Export Configuration File

Ignore Disabled Features: ON OFF

Add Detailed Information: ON OFF

XML Configuration File: Generate

XML Configuration File: Export

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.

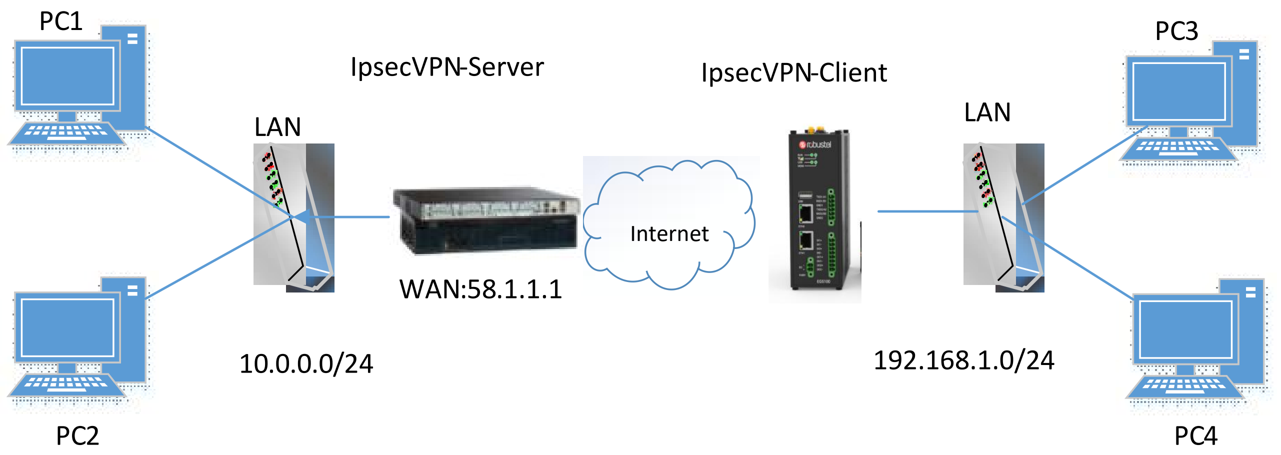
SMS received:

```
OK
OK
OK
OK
```

4.2 VPN Configuration Examples

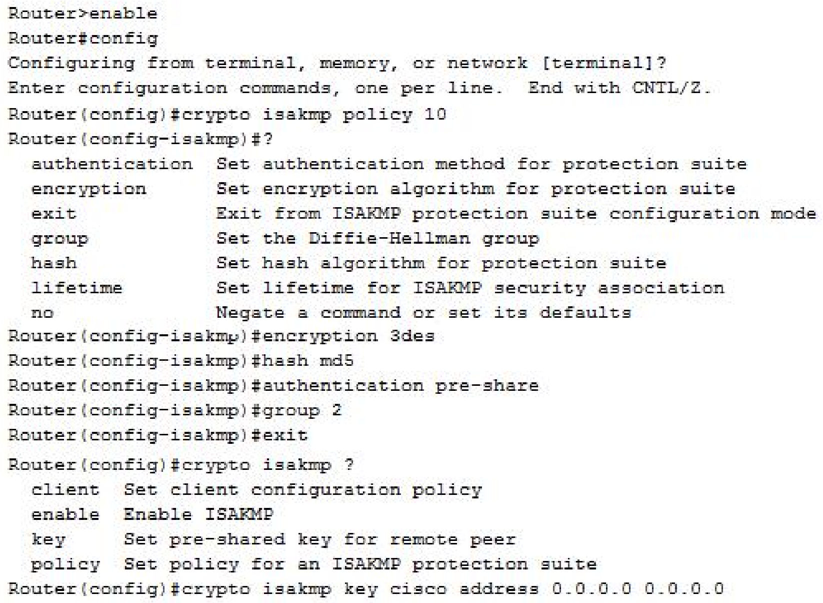
4.2.1 IPsec VPN

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

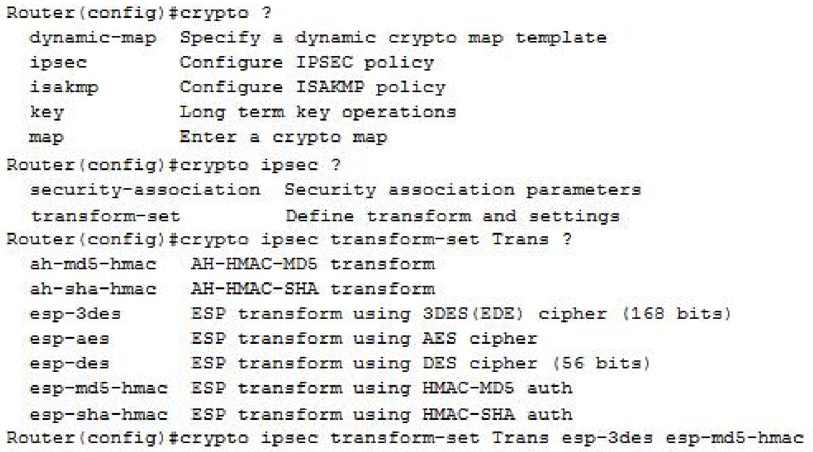


IPsecVPN_Server:

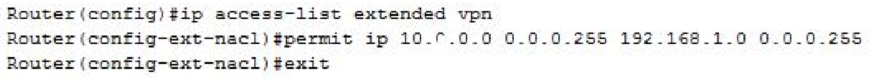
Cisco 2811:



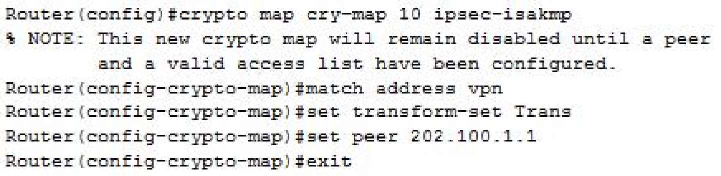
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set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



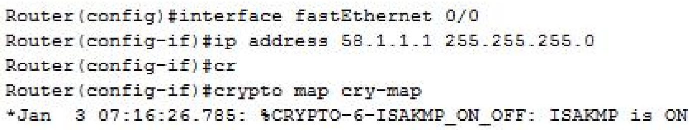
```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association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



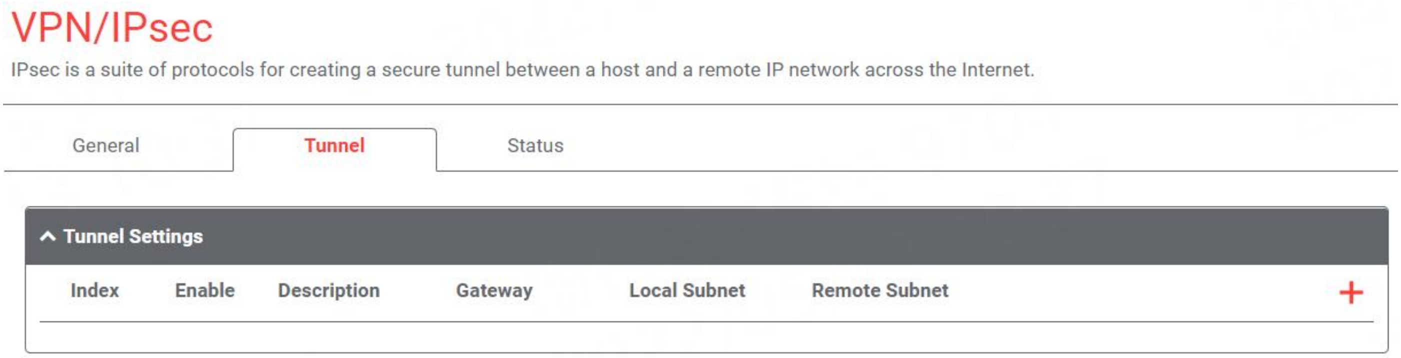
```
Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1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

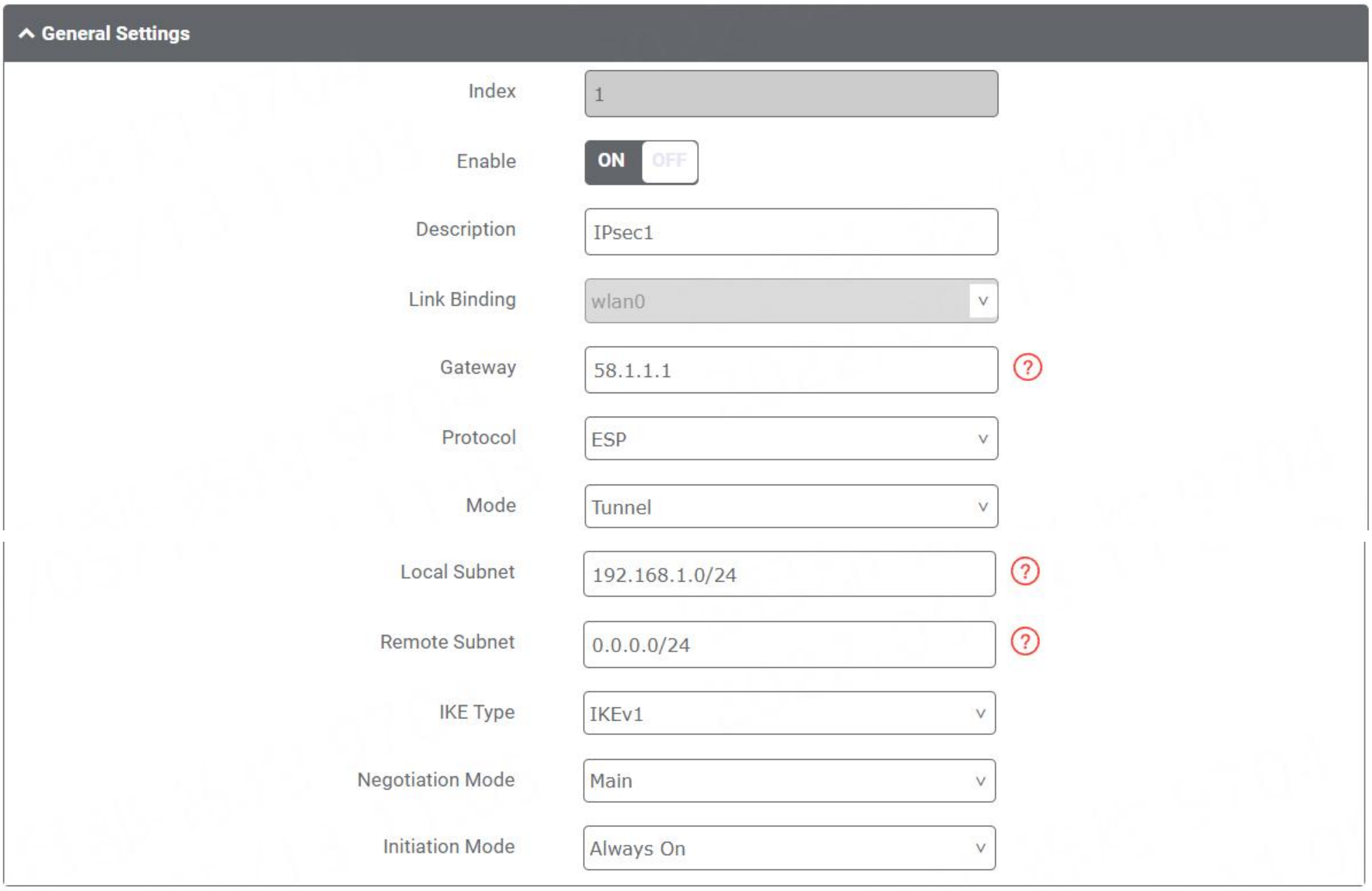


VPN/IPsec

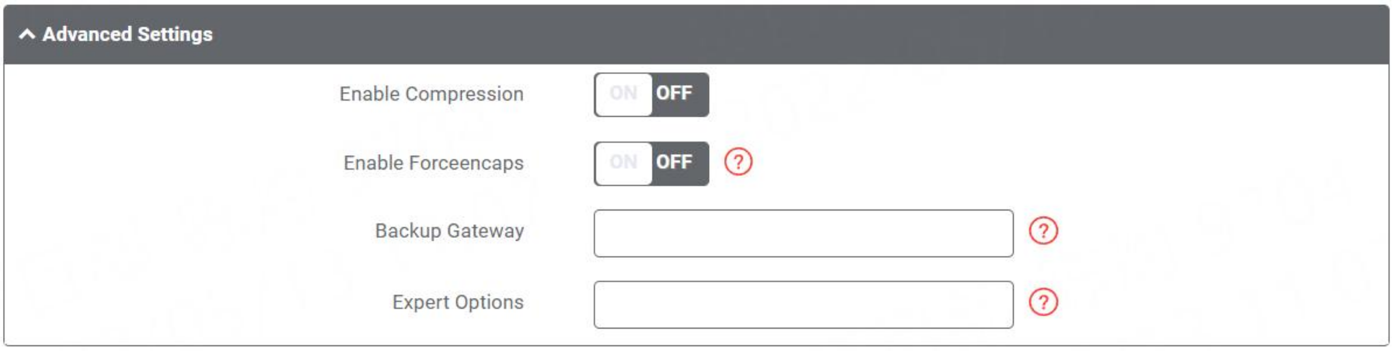
IPsec is a suite of protocols for creating a secure tunnel between a host and a remote IP network across the Internet.

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet

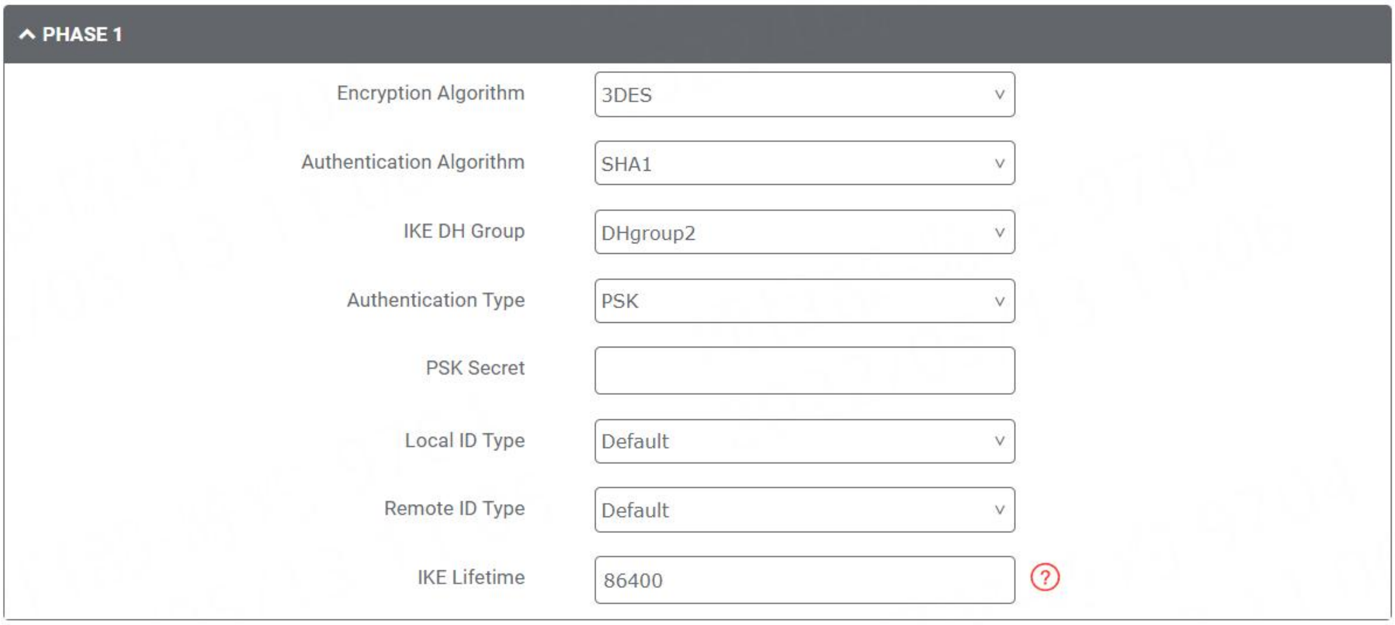
Click + button and set the parameters of IPsec Client as below.



Index	1
Enable	ON
Description	IPsec1
Link Binding	wlan0
Gateway	58.1.1.1
Protocol	ESP
Mode	Tunnel
Local Subnet	192.168.1.0/24
Remote Subnet	0.0.0.0/24
IKE Type	IKEv1
Negotiation Mode	Main
Initiation Mode	Always On

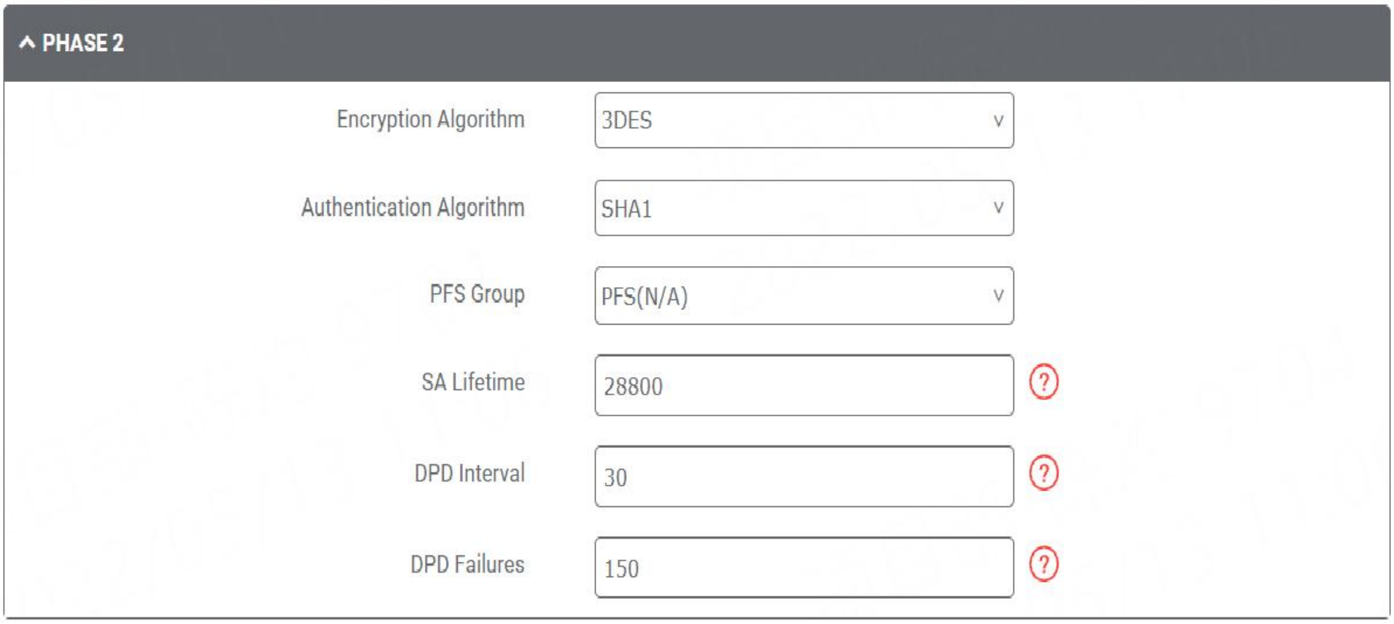


Enable Compression	OFF
Enable Forceencaps	OFF
Backup Gateway	
Expert Options	



^ PHASE 1

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



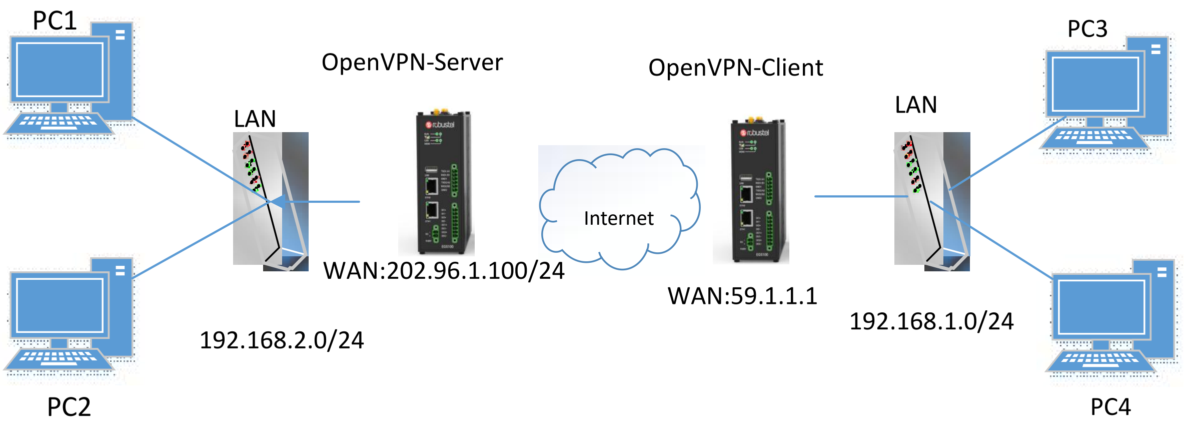
^ PHASE 2

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

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:

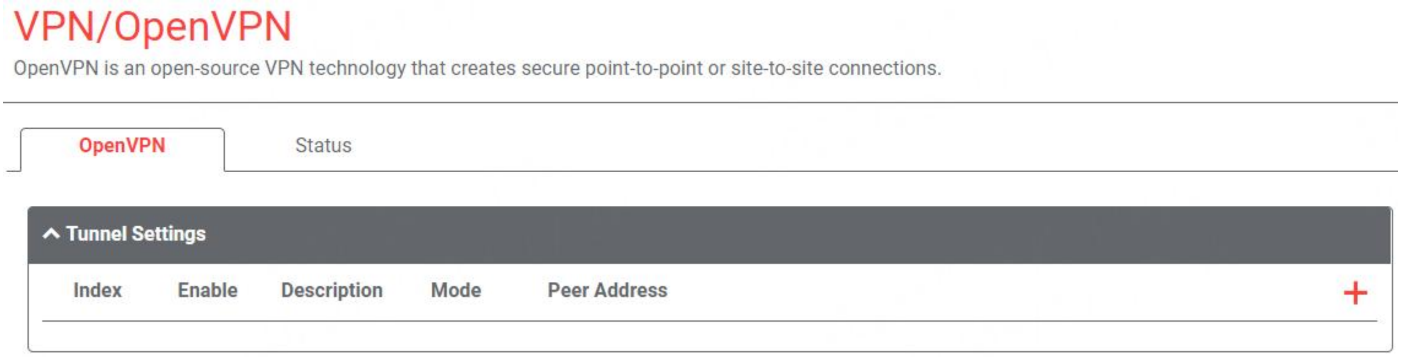
Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server:

```
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.



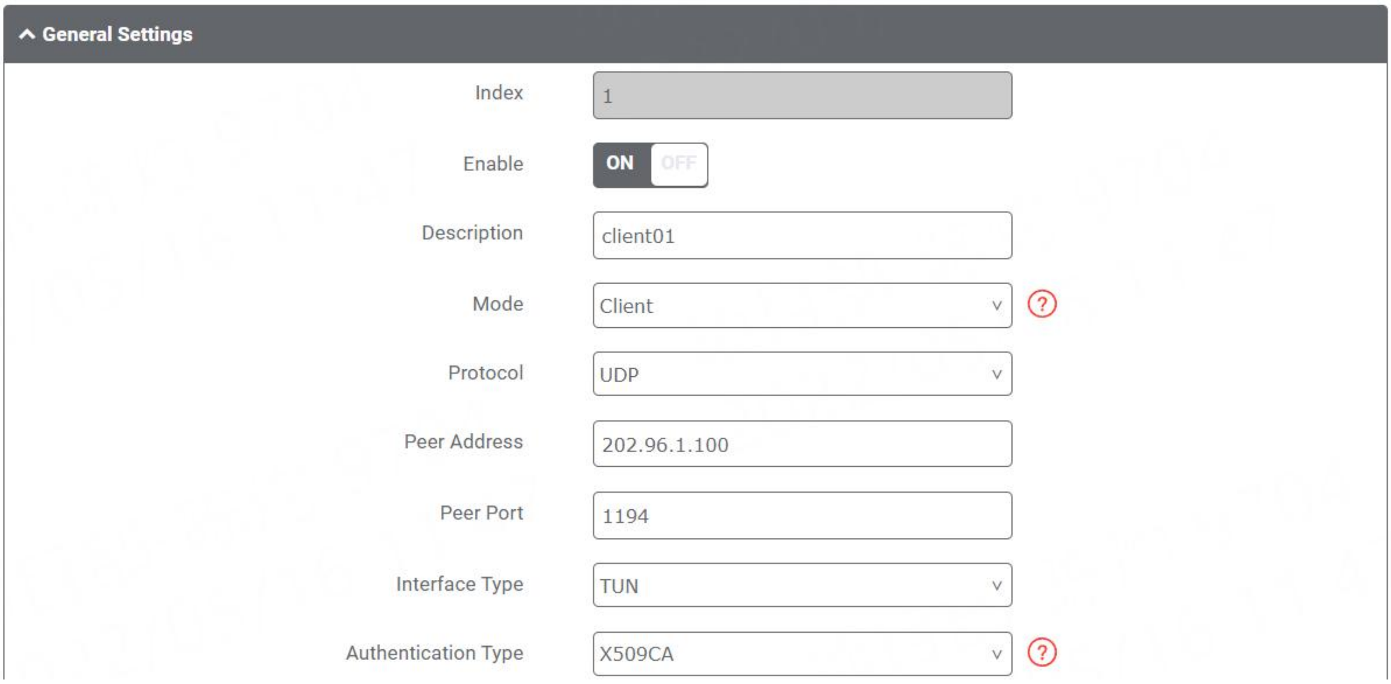
VPN/OpenVPN

OpenVPN is an open-source VPN technology that creates secure point-to-point or site-to-site connections.

Tunnel Settings

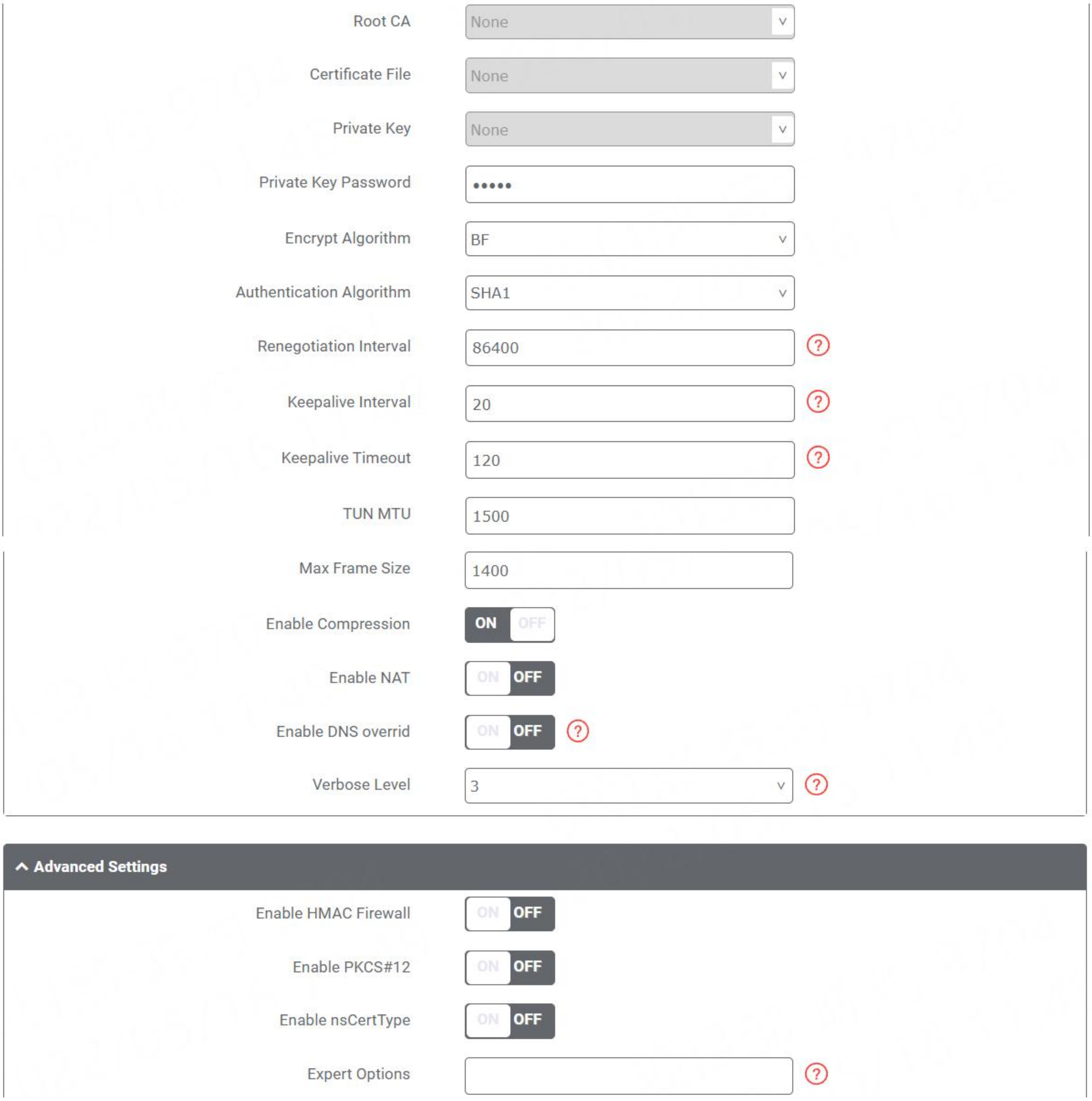
Index	Enable	Description	Mode	Peer Address

Click + to configure the Client01 as below.



General Settings

Index	1
Enable	ON OFF
Description	client01
Mode	Client
Protocol	UDP
Peer Address	202.96.1.100
Peer Port	1194
Interface Type	TUN
Authentication Type	X509CA



Root CA	None
Certificate File	None
Private Key	None
Private Key Password	•••••
Encrypt Algorithm	BF
Authentication Algorithm	SHA1
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	1400
Enable Compression	ON
Enable NAT	OFF
Enable DNS overrid	OFF
Verbose Level	3

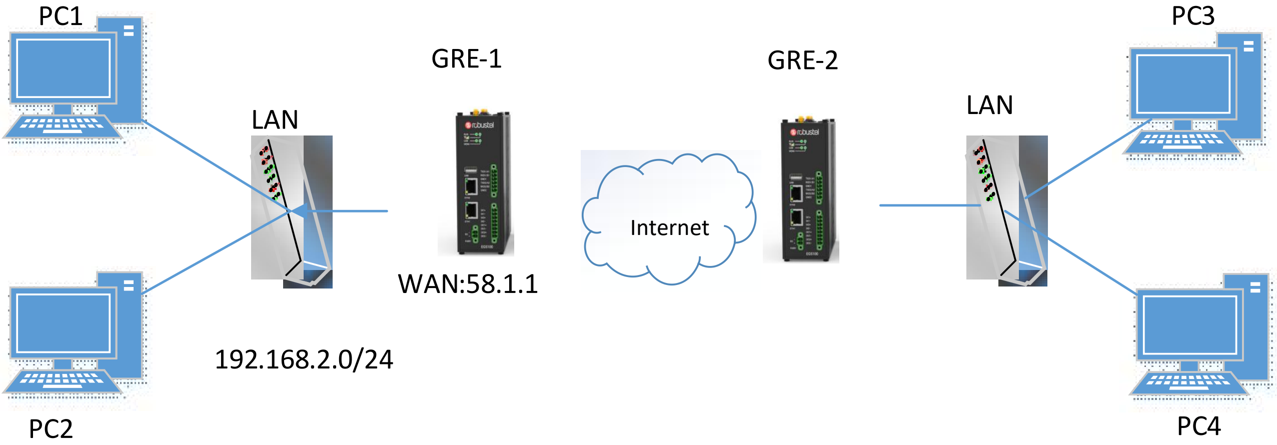
Advanced Settings

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

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

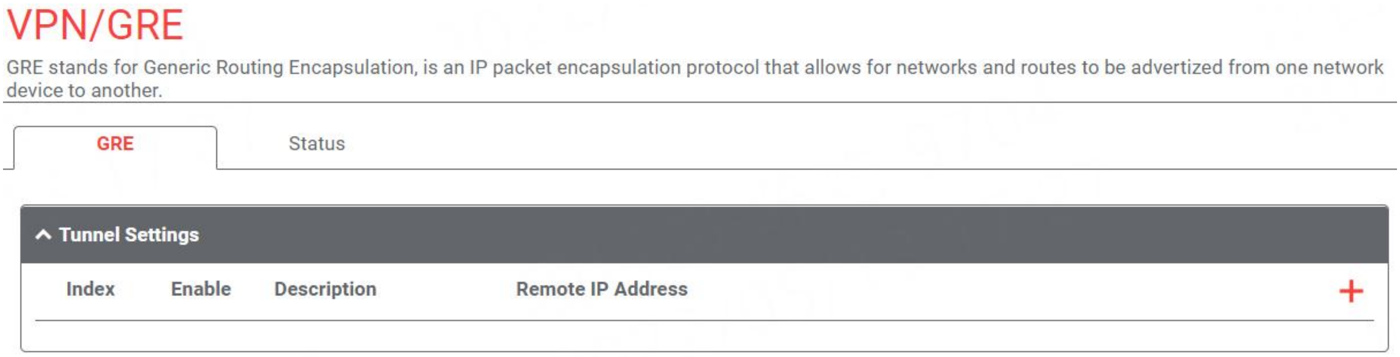
4.2.3 GRE VPN

GRE VPN topology



GRE-1：

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

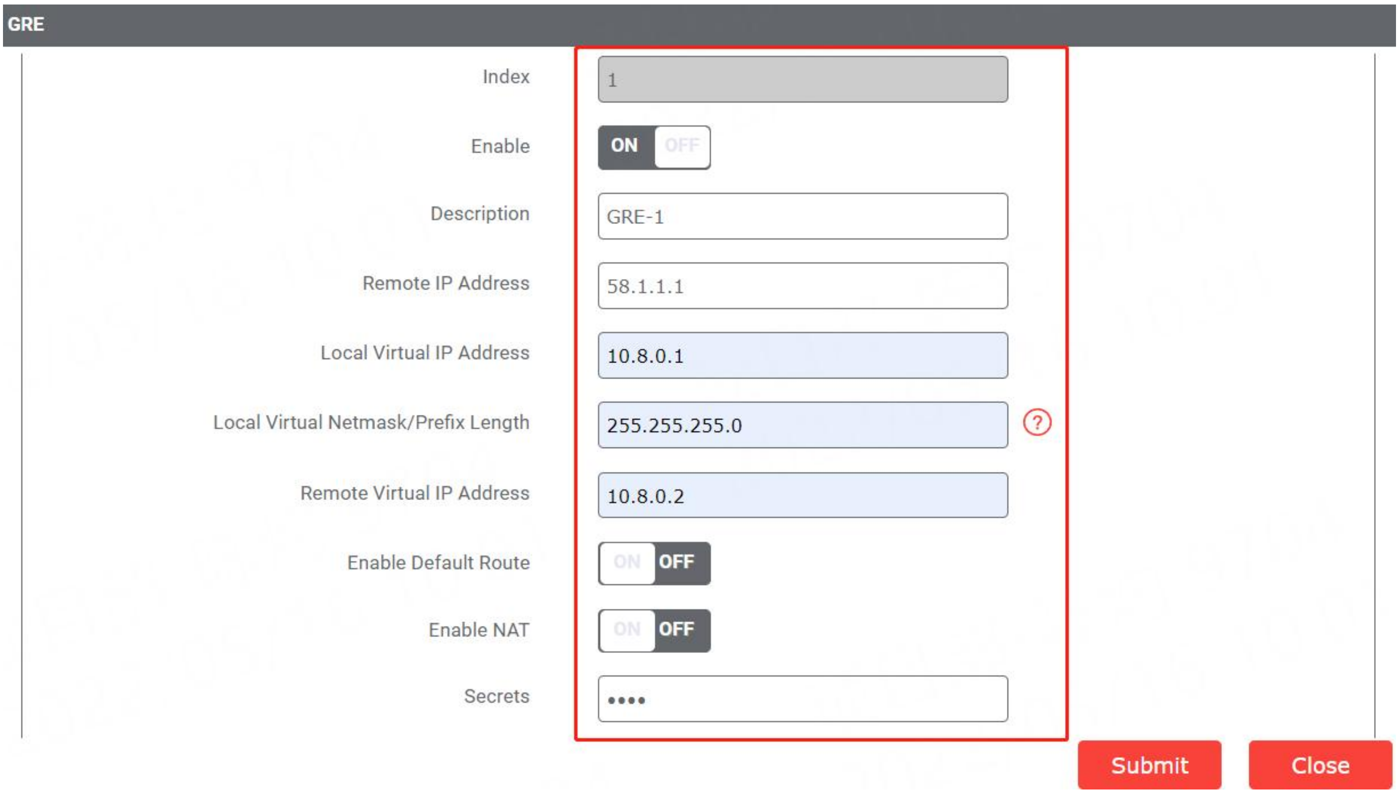


VPN/GRE

GRE stands for Generic Routing Encapsulation, is an IP packet encapsulation protocol that allows for networks and routes to be advertized from one network device to another.

Index	Enable	Description	Remote IP Address	+

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



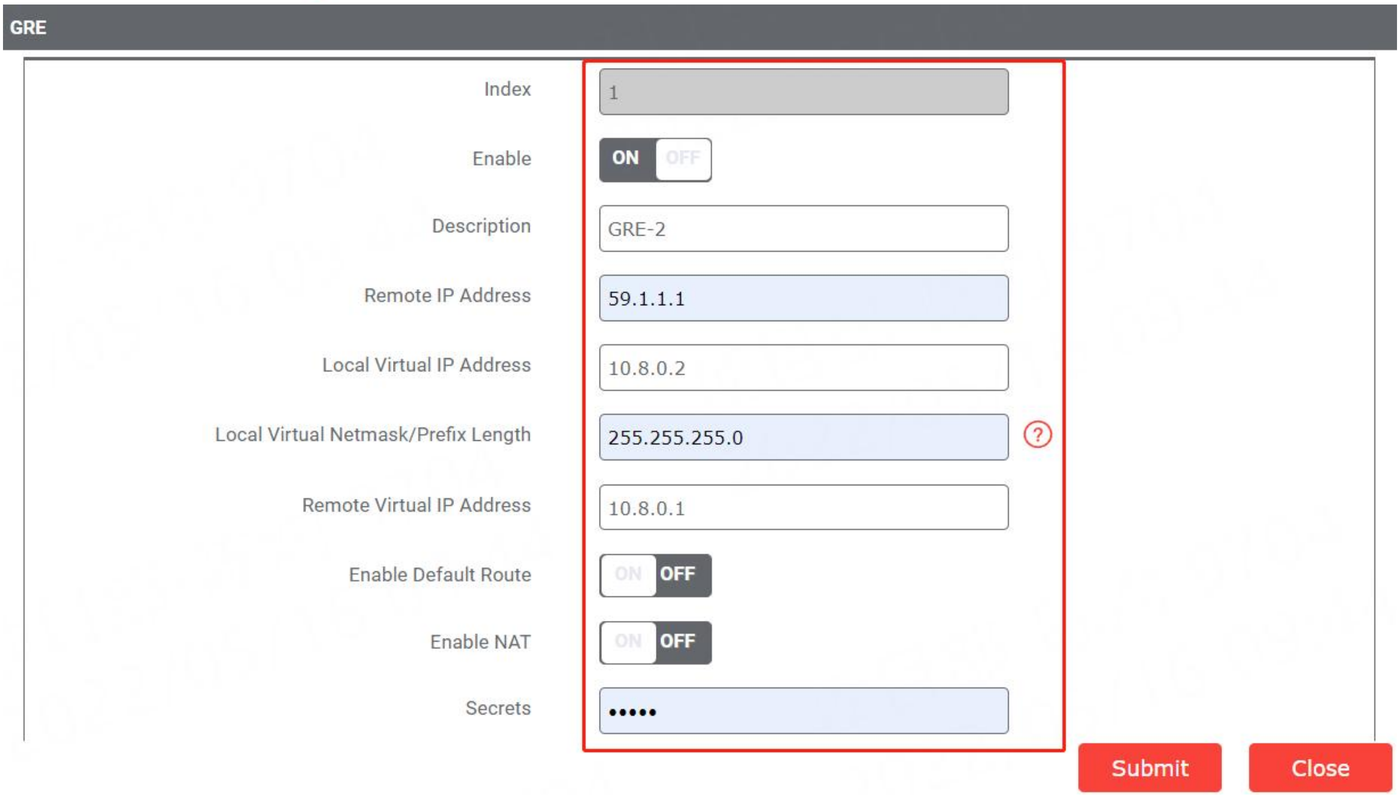
GRE

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

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.

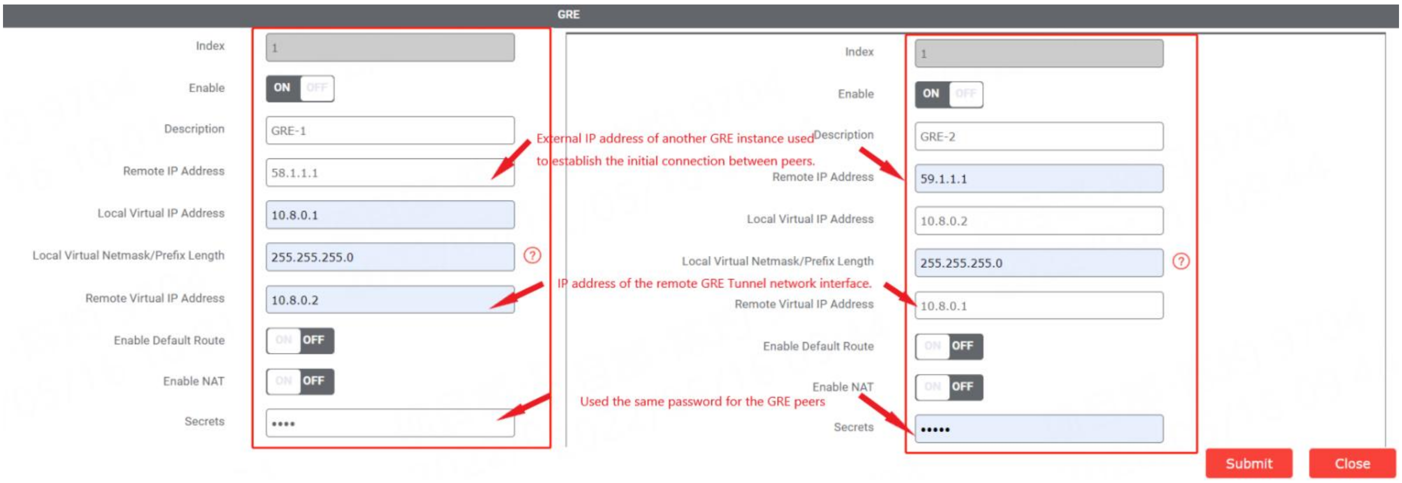


GRE

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

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.



GRE

	GRE-1	GRE-2
Index	1	1
Enable	ON	ON
Description	GRE-1	GRE-2
Remote IP Address	58.1.1.1	59.1.1.1
Local Virtual IP Address	10.8.0.1	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0	255.255.255.0
Remote Virtual IP Address	10.8.0.2	10.8.0.1
Enable Default Route	OFF	OFF
Enable NAT	OFF	OFF
Secrets	••••	•••••

External IP address of another GRE instance used to establish the initial connection between peers.

IP address of the remote GRE Tunnel network interface.

Used the same password for the GRE peers

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: View 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: Set Up the Mobile Network CLI

```
# show cellular all
sim {
        id = 1
        card = sim1
        phone_number = ""
        pin_code = ""
        extra_at_cmd = ""
        telnet_port = 0
        network_type = auto
        band_select_type = all
        band_settings {
                gsm_850 = false
                gsm_900 = false
                gsm_1800 = false
                gsm_1900 = false
                wcdma_800 = false
                wcdma_850 = false
                wcdma_900 = false
                wcdma_1900 = false
                wcdma_2100 = false
                wcdma_1700 = false
                wcdma_band19 = false
                lte_band1 = false
                lte_band2 = false
                lte_band3 = false
                lte_band4 = false
                lte_band5 = false
                lte_band7 = false
                lte_band8 = false
                lte_band13 = false
                lte_band17 = false
                lte_band18 = false
                lte_band19 = false
                lte_band20 = false
                lte_band21 = false
                lte_band25 = false
                lte_band28 = false
                lte_band31 = false
                lte_band38 = false
                lte_band39 = false
                lte_band40 = false
                lte_band41 = false
        }
        telit_band_settings {
                gsm_band = 900_and_1800
                wcdma_band = 1900
        }
        debug_enable = true
        verbose_debug_enable = false
}
# set(space+space)
cellular          ddns              dido              email             ethernet
event             firewall          gre               ip_passthrough    ipsec
l2tp              lan               link_manager      ntp               openvpn
pptp              reboot            route             serial_port       sms
ssh               syslog            system            user_management   web_server
# set cellular(space+?)
  sim    SIM Settings
# set cellular sim(space+?)
  Integer    Index (1..1)

# set cellular sim 1(space+?)
    card                        SIM Card
    phone_number                Phone Number
    pin_code                    PIN Code
    extra_at_cmd                Extra AT Cmd
    telnet_port                 Telnet Port
```

```
   network_type              Network Type
   band_select_type          Band Select Type
   band_settings             Band Settings
   telit_band_settings       Band Settings
   debug_enable              Debug Enable
   verbose_debug_enable      Verbose Debug Enable
# set cellular sim 1 phone_number 18620435279
OK
…
# config save_and_apply
OK                                    // Save the current configuration of the application and make the
configuration take 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

Abbr.	Description
kbps	kbits per second
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
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

Abbr.	Description
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Guangzhou Robustel Co., Ltd.

Add: 501, Building#2, 63 Yongan Road, Huangpu District,
Guangzhou, China 511350

Email: info@robustel.com

Web: www.robustel.com