Queclink Cellular Router - WR310

Queclink
2026.02.05

Queclink
Confidential

CONTENT

1 Overview **1**
- 1.1 Description . . . 1
- 1.2 Software Architecture . . . 2

2 Hardware **3**
- 2.1 Structure . . . 4
- 2.2 Interfaces . . . 5
- 2.3 Connector Definition . . . 5
- 2.4 LEDs Definition . . . 6
- 2.5 Installation . . . 6

3 Initial Configuration **9**
- 3.1 Configure the PC . . . 9
- 3.2 Login to device . . . 12
- 3.3 Control Panel . . . 13

4 Software Configuration **14**
- 4.1 Status . . . 14
  - 4.1.1 Overview . . . 14
  - 4.1.2 Device . . . 14
  - 4.1.3 Network . . . 15
    - 4.1.3.1 Mobile . . . 15
    - 4.1.3.2 WAN . . . 18
    - 4.1.3.3 LAN . . . 18
    - 4.1.3.4 WLAN . . . 19
  - 4.1.4 Applications . . . 20
  - 4.1.5 VPN . . . 20
  - 4.1.6 Routes . . . 21
  - 4.1.7 Mobile Traffic . . . 22
  - 4.1.8 Log . . . 23
- 4.2 Network . . . 24
  - 4.2.1 Link Management . . . 24
  - 4.2.2 Mobile . . . 26
    - 4.2.2.1 General . . . 26
    - 4.2.2.2 SIM Management . . . 28
    - 4.2.2.3 Data Limit . . . 29
    - 4.2.2.4 Operator . . . 30
  - 4.2.3 WAN . . . 31
  - 4.2.4 LAN . . . 35
  - 4.2.5 VLAN . . . 37
  - 4.2.6 WLAN . . . 39
  - 4.2.7 Routing . . . 42
    - 4.2.7.1 Static . . . 42
    - 4.2.7.2 RIP . . . 43

Quectlink Confidential

4.2.8 Firewall . . . 43
4.2.8.1 NAT . . . 43
4.2.8.2 Domain Filter . . . 44
4.2.8.3 IP/MAC Filter . . . 45
4.2.8.4 DMZ . . . 46
4.2.8.5 DDOS . . . 47
4.2.9 QoS . . . 48
4.2.9.1 QoS . . . 48
4.2.9.2 User Bandwidth . . . 49
4.3 Applications . . . 50
4.3.1 GPS (Available for some Models Only) . . . 50
4.3.1.1 Map . . . 50
4.3.1.2 General . . . 50
4.3.1.3 NMEA . . . 51
4.3.2 VPN . . . 52
4.3.2.1 PPTP . . . 52
4.3.2.2 L2TP . . . 54
4.3.2.3 OPENVPN . . . 57
4.3.2.4 IPSec . . . 64
4.3.2.5 GRE Tunnel . . . 67
4.3.3 SMS Utilities . . . 69
4.3.4 MQTT . . . 70
4.3.5 RS232/RS485 . . . 72
4.3.6 Modbus . . . 75
4.3.6.1 Modbus RTU . . . 76
4.3.6.2 Modbus TCP . . . 80
4.3.6.3 Modbus TCP to RTU . . . 84
4.3.7 DDNS . . . 84
4.3.8 Input . . . 85
4.3.8.1 Status . . . 86
4.3.8.2 Server . . . 86
4.3.8.3 Local Control . . . 88
4.3.8.4 Application Example . . . 90
4.3.9 Output . . . 90
4.3.9.1 Status . . . 91
4.3.9.2 Default State . . . 91
4.3.9.3 Local Control . . . 91
4.3.9.4 Periodic Control . . . 92
4.3.9.5 Server . . . 93
4.3.9.6 Application Example . . . 95
4.3.10 SNMP . . . 96
4.3.10.1 SNMP . . . 96
4.3.10.2 COMMUNITY . . . 97
4.3.11 iTracker . . . 98
4.3.11.1 General . . . 98
4.3.11.2 Device . . . 98
4.3.11.3 Report . . . 100
4.3.12 Hotspot . . . 102
4.3.12.1 General . . . 102
4.3.12.2 Local Users . . . 103
4.3.12.3 User Manage . . . 104
4.3.13 BLE (Available for some Models Only) . . . 104
4.3.13.1 General . . . 104
4.3.13.2 BLE Accessory . . . 105
4.3.13.3 Beacon . . . 106
4.3.13.4 BLE Upgrade . . . 107
4.4 System . . . 107
4.4.1 Setup Wizard . . . 107

Queclink Confidential

4.4.2 Administration . . . 109
4.4.2.1 General . . . 109
4.4.2.2 Access Control . . . 110
4.4.2.3 Configuration . . . 111
4.4.3 Reboot . . . 111
4.4.4 Diagnostic . . . 111
4.4.4.1 Ping & Trace . . . 111
4.4.4.2 Tcpdump . . . 112
4.4.4.3 Timing Task . . . 112
4.4.4.4 ICMP . . . 113
4.4.4.5 CLI . . . 114
4.4.5 NTP . . . 115
4.4.6 Nebulink . . . 116
4.4.7 Upgrade . . . 117
4.4.7.1 Local . . . 117
4.4.7.2 FOTA . . . 117
4.5 Reset Button . . . 118

5 Network services and ports 119

6 FAQ 120
6.1 SIM Slot . . . 120
6.2 No Signal . . . 120
6.3 Cannot Find SIM/UIM Card . . . 121
6.4 VPN Cannot Connect . . . 121

7 Appendices 122
7.1 General Notes . . . 122
7.2 Revision History . . . 122
7.3 Glossary . . . 122
7.4 Copyright . . . 123

Queclink Confidential

CHAPTER

ONE

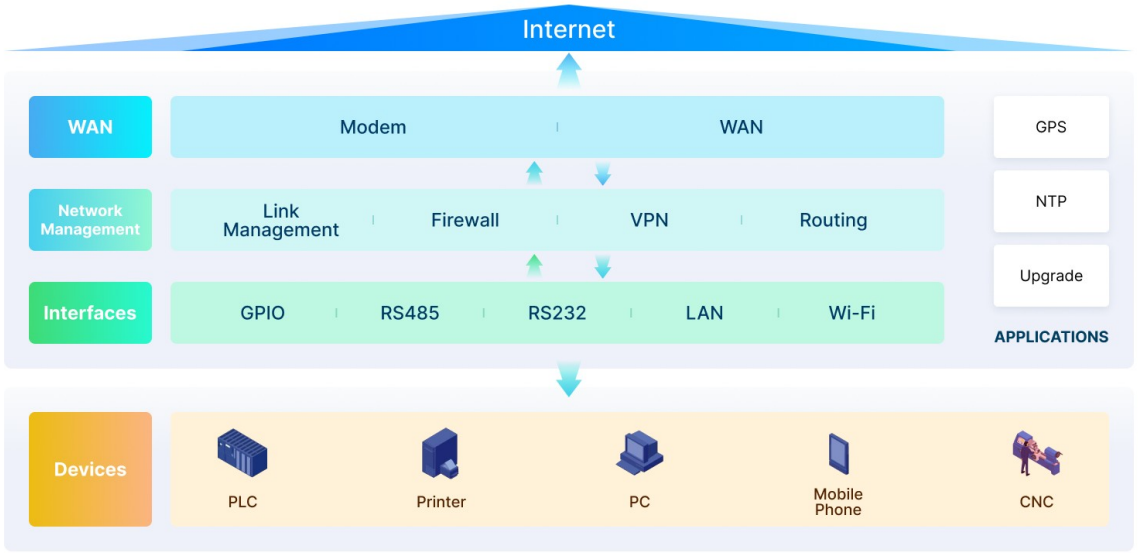
OVERVIEW

1.1 Description

The Queclink dual SIM industrial Cellular Router WR310 is a rugged router offering high-speed stable mobile connectivity for machine to machine (M2M) applications. Based on 3G/4G LTE and 5G technology, the device adopt high-performance processor and embedded operating system design. APN/VPDN private network access and dual SIM backup design guarantee data transmission security and provide high-speed, reliable routing and data transmission capabilities. Equipped with Ethernet ports, RS232/RS485 ports, Wi-Fi, GPIOs, all of which make it can be widely used in telecommunications, finance, information media, electric industry, retailing, automotive and environmental industries.



1.2 Software Architecture



Queclink Confidential

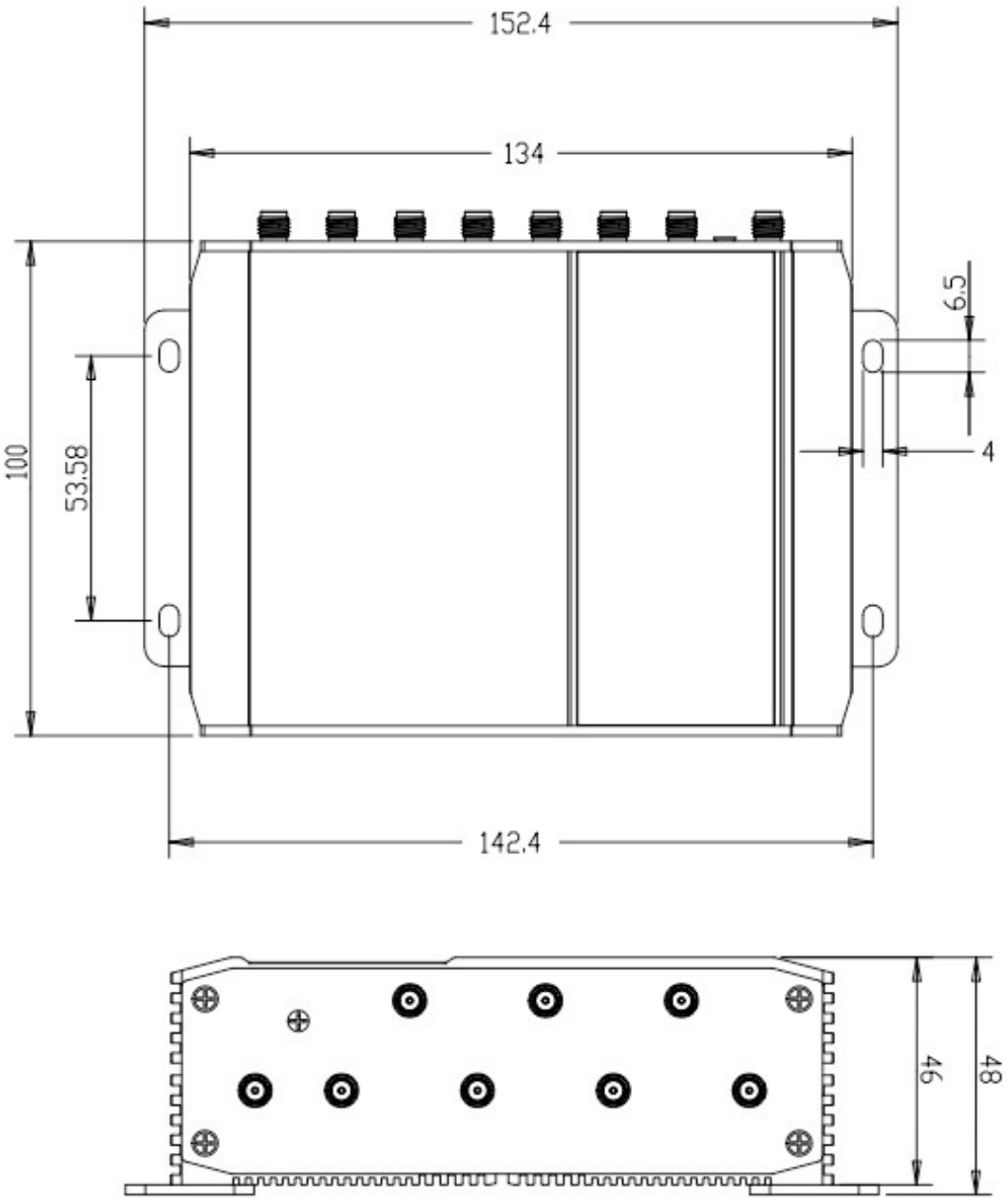
Queclink
Confidential

CHAPTER

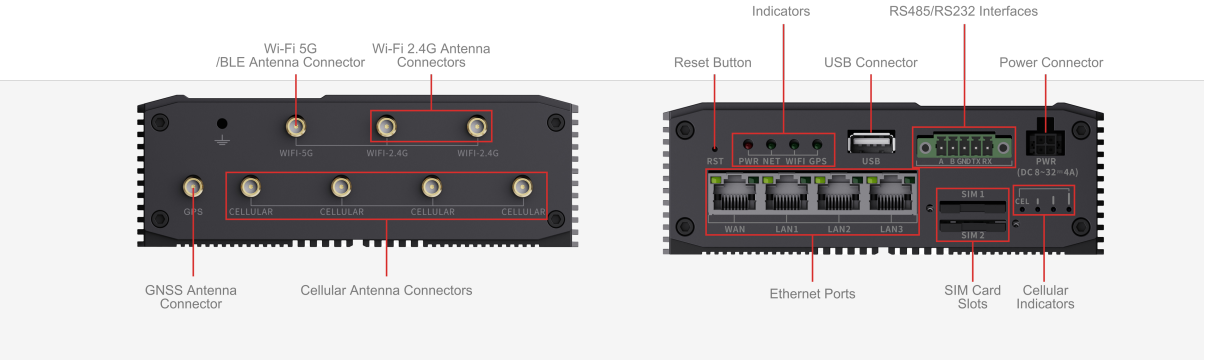
TWO

HARDWARE

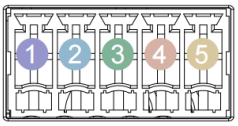
2.1 Structure



2.2 Interfaces



2.3 Connector Definition

Port	Picture
Power	 PWR 1 Power 2 Ground 3 Digital input (0-3.8 VDC: low logic level/4.3-40 VDC: high logic level) 4 Open collector output (4-pin connector) (30 VDC, 0.3A)
RS-485 / RS-232	 1 RS-485 #A 2 RS-485 #B 3 GND: Ground 4 RS-232 TX (connect with RXD of peer end) 5 RS-232 RXD (connect with TXD of peer end)

Queclink Confidential

2.4 LEDs Definition

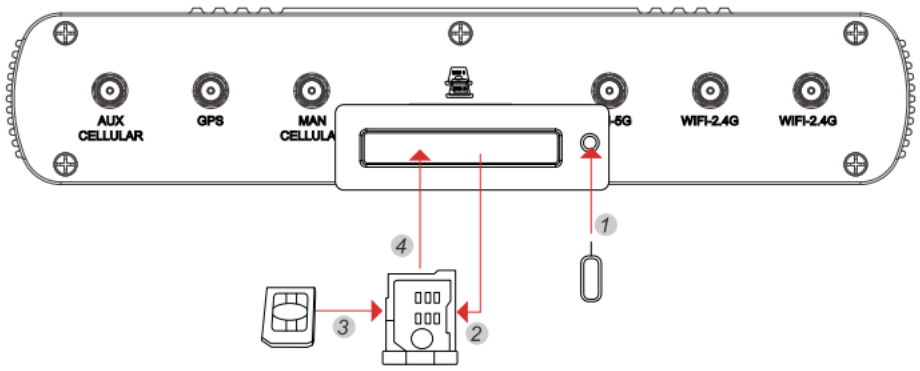
Name	Status	Description
PWR	Green, solid	Power on
	Off	Power off
Wi-Fi	Green, solid	Wi-Fi on and working
	Green blinking	Data is being transferred
	Off	Wi-Fi off or abnormal
GPS	Green, solid	GPS on and working properly
	Off	GPS off or abnormal
CEL	Red, solid	No SIM card or wrong PIN
	Green and red blinking every 1s	Connected to 2G network
	Green and red blinking every 1s	Connected to 3G network
	Green blinking every 1s	Connected to 4G network
	Green, solid	Connected to 5G network
	Red blinking	Connecting to the network
SIGNAL (RSSI)	0	0
	1	1 to 8
	2	9 to 15
	3	16 to 23
	4	23 to 32
LAN Ethernet	Yellow solid, green off	1000M link established
	Yellow blinking, green off	1000M link active
	Yellow solid, green solid	10M/100M link established
	Yellow blinking, green blinking	10M/100M link active
	Off	Connection is not established
WAN Ethernet Indicators	Yellow off, green solid	10M/100M/1000M link established
	Yellow off, green blinking	10M/100M/1000M link active
	Off	Connection is not established

2.5 Installation

This chapter provides an example description with WR310 on how to correctly insert a SIM card, install antennas and power on a device.

1. **Insert SIM card:**
    - Make sure the device is powered off.
    - Push the SIM holder button using the SIM ejection pin.
    - Pull out the SIM holder.
    - Insert your SIM card into the SIM holder.
    - Slide the SIM holder back into the device.

Queclink Confidential

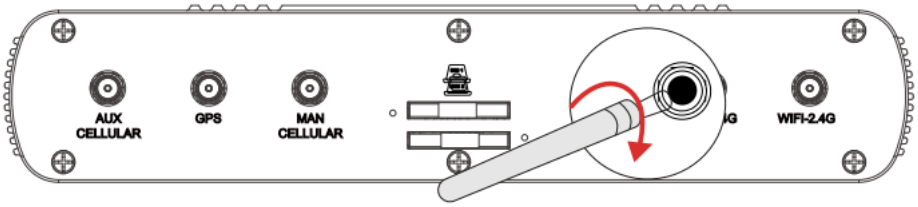


Note: The device is compatible with mini-SIM (2FF) size cards.

Note: The device is compatible with **mini-SIM (2FF)** size cards.

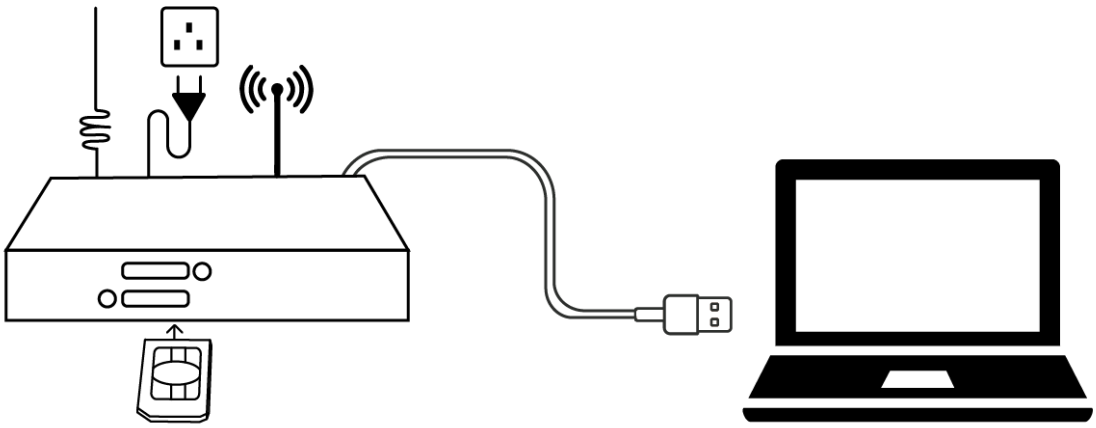
2. **Attach External LTE, Wi-Fi and GPS Antenna:**

   Attach the SMA external antenna to the device's connector and screw them tightly. Make sure that the antenna type matches to the antenna connector. You can see the antenna type by the silk printing on the antenna.



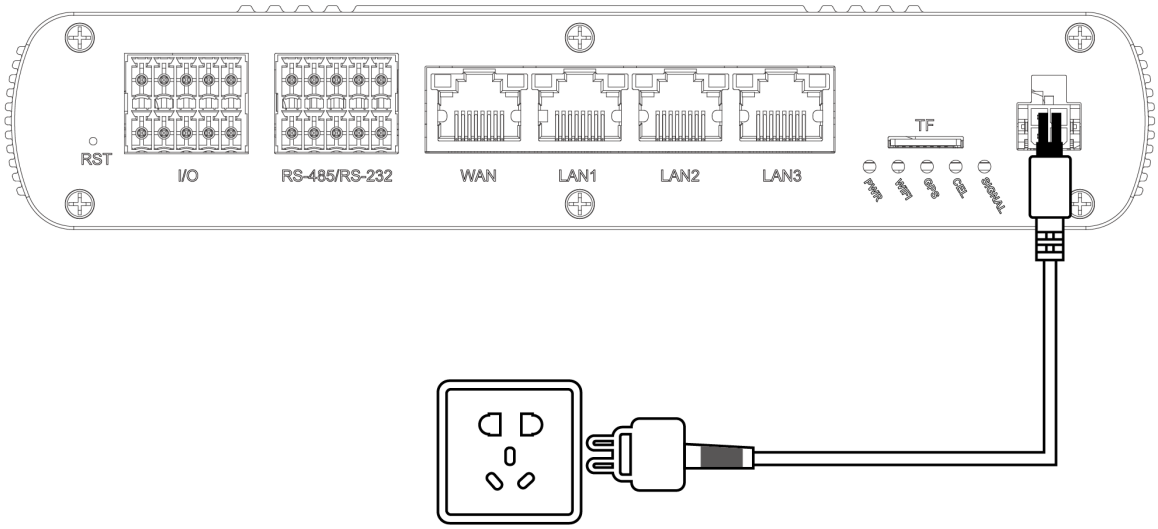
3. **Connect the device to other devices**

   Connect an Ethernet cable to any ports marked LAN on the device, and connect the other end of the cable to your computer or lower end device.



4. **Connect the 4-pin power cable to power on the device.**

   Connect the power adaptor to the socket on the front of the device and plug the other end of the power adaptor into a power outlet. The device is designed to accept input voltage between 8V DC to 32V DC. Higher voltage input may damage the device.



5. **Fix the device**

   You can use the mounting bracket to fix the device on the wall or other flat surface. WR310 can support DIN rail installation, and you can consult with local sales representatives to order related accessories.

Queclink Confidential

CHAPTER

THREE

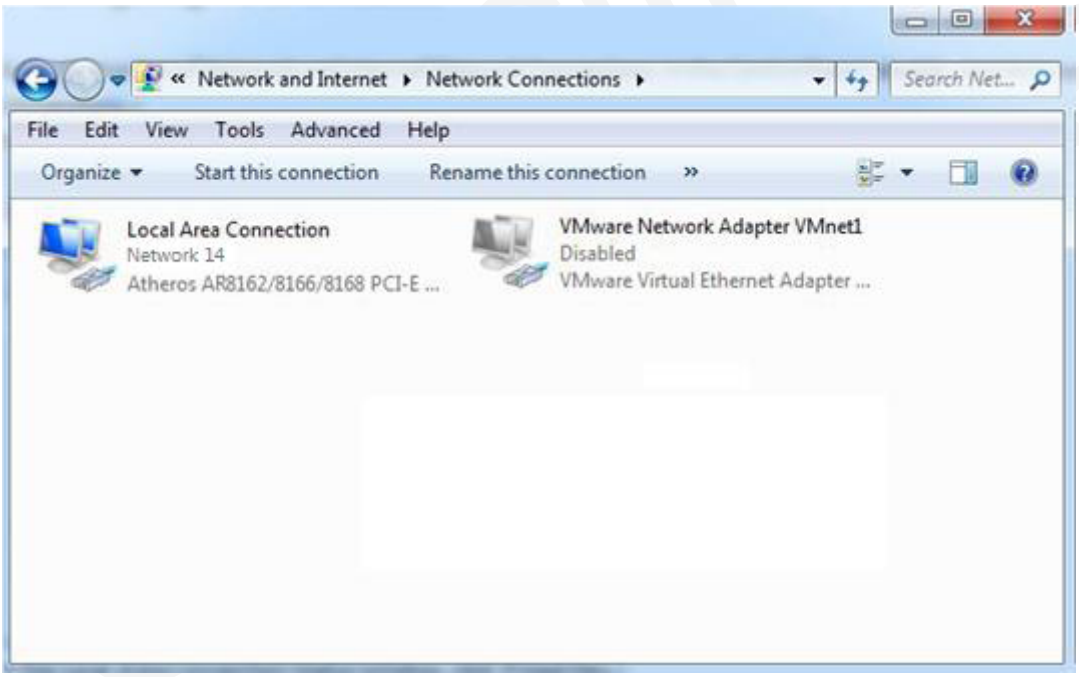
INITIAL CONFIGURATION

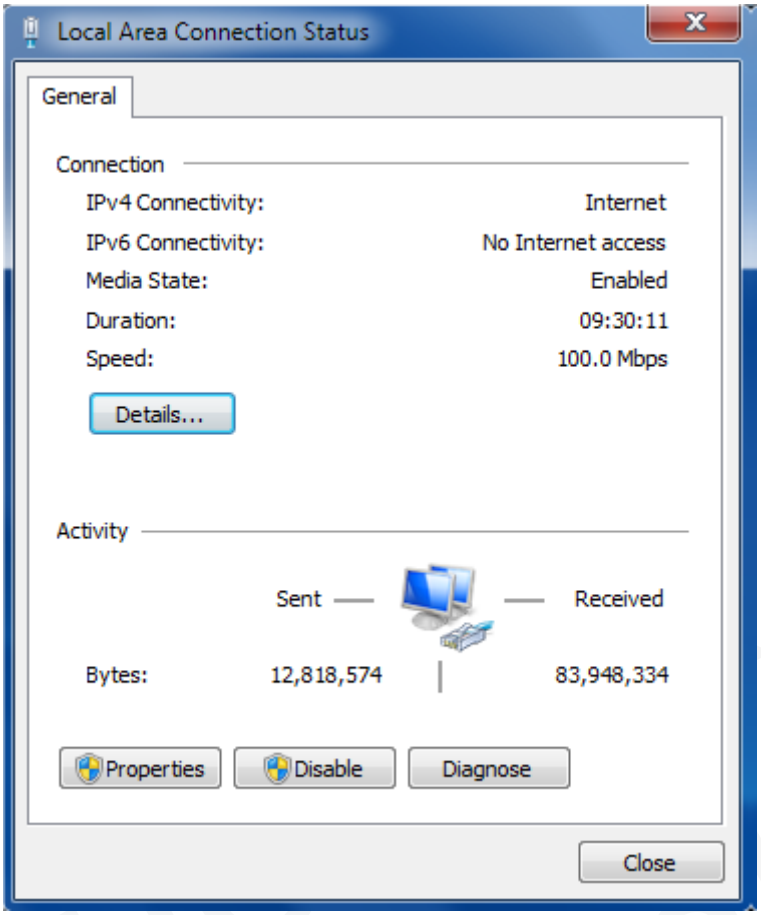
Queclink Industrial Cellular Routers have a user-friendly WebUI that makes it easy for users to configure the device. Make sure your computer has an Ethernet interface and web browser such as IE, Chrome, Firefox, etc.

3.1 Configure the PC

There are two methods to get IP address for the PC, one is to obtain an IP address automatically from “Local Area Connection”, and the other is to configure a static IP address manually within the same subnet of the device. Please refer to the steps below.

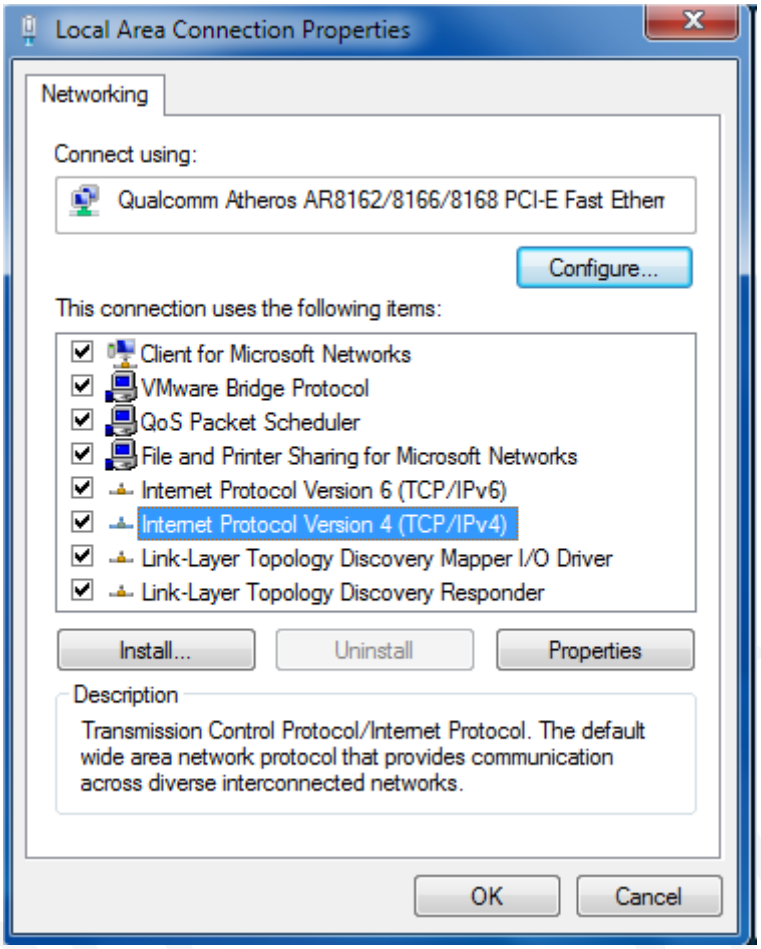
Here, we take Windows 7 as an example and the configuration for other Windows versions is similar





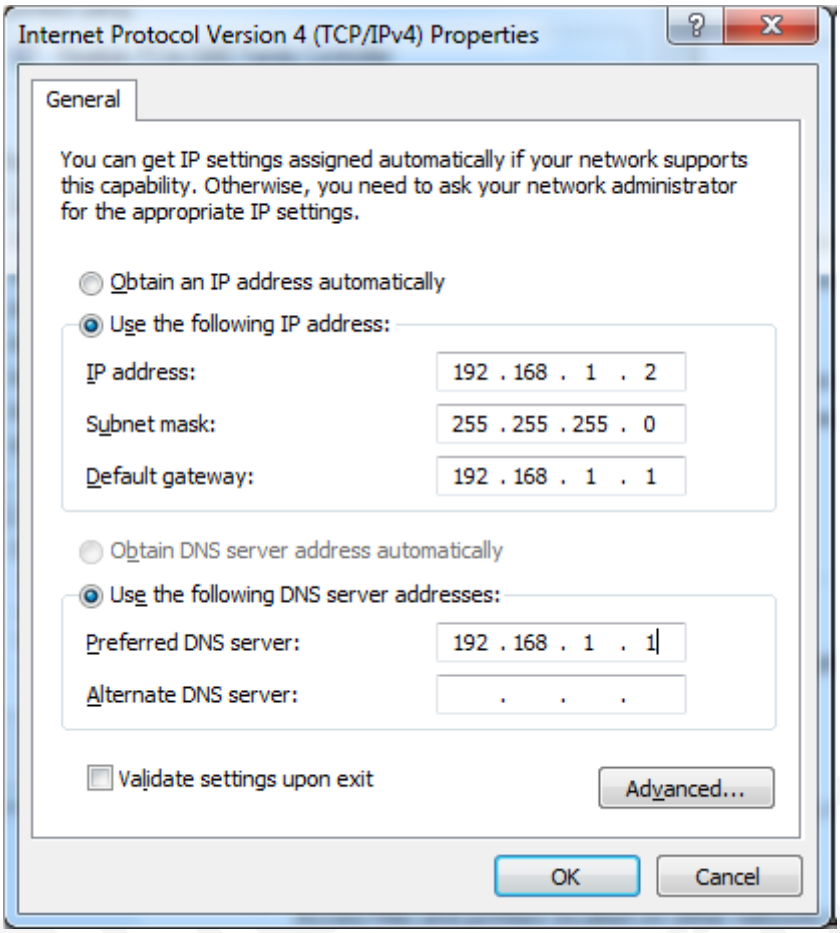
1. Click Start > Control panel, double-click Network and Sharing Center, and then double-click Local Area Connection.

Queclink Confidential



2. Click Properties in the window of Local Area Connection Status.

Queclink Confidential



3. Choose Internet Protocol Version 4 (TCP/IPv4) and click Properties.
4. Use the following IP address:

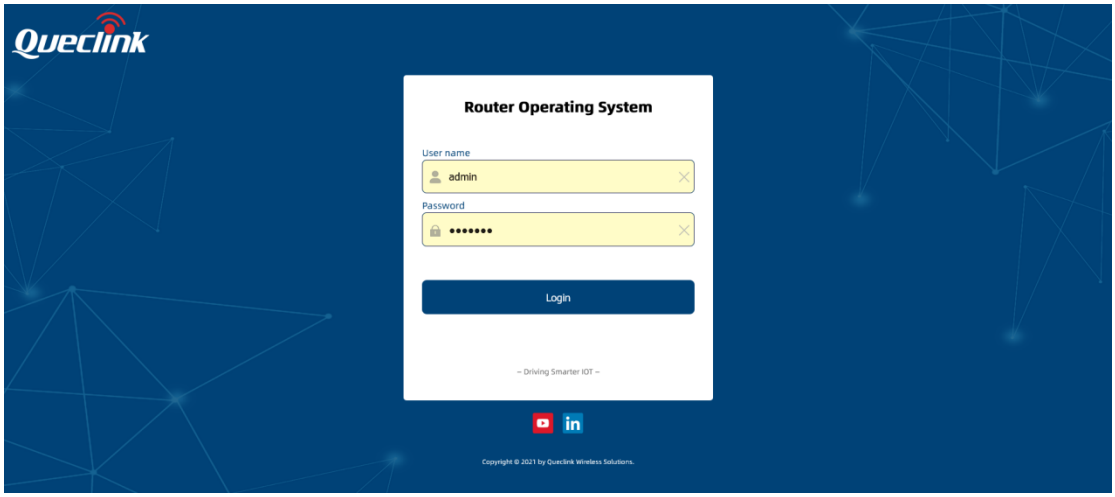
Configured a static IP address manually within the same subnet of the device, the default IP address is 192.168.1.1.

Click OK to finish the configuration.

3.2 Login to device

1. To enter the device's Web interface (WebUI), type http://192.168.1.1 into the URL field of your Internet browser.
2. Use the following login information when prompted for authentication:

Confidential

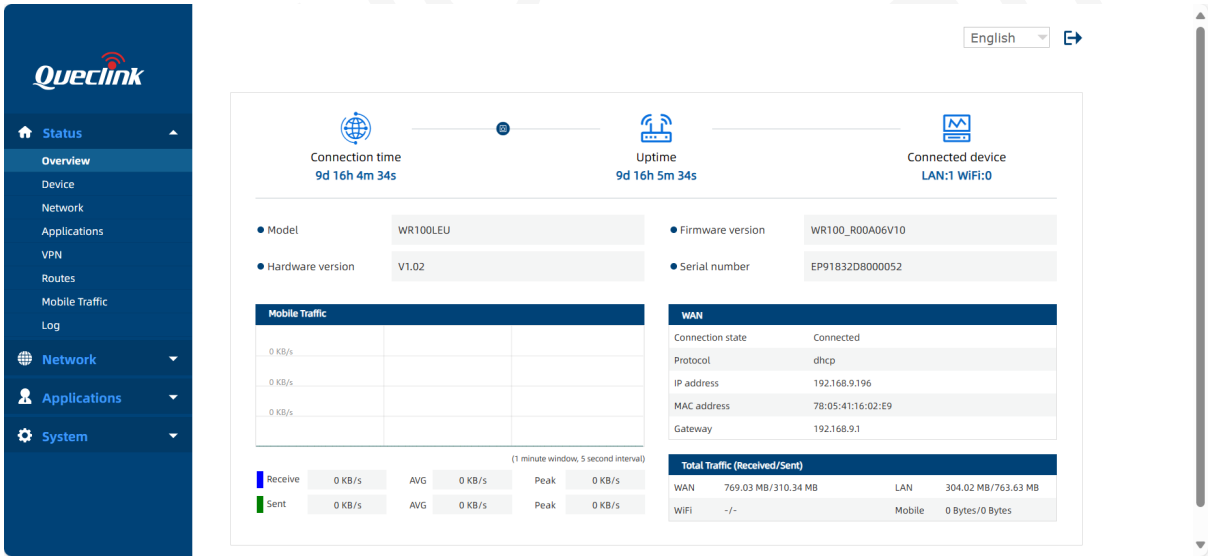


Enter the username and password, and then click LOGIN button. The default username is “admin” and password is “admin01”.

3.3 Control Panel

After logging in, the home page of the device web interface is displayed. The home page is an overview of the device. It displays the network state, mobile connection state and Wi-Fi state, etc.

The page includes a language selection drop-down menu and a logout button in the upper-right corner. You can easily change the language or log out of the system.



The following chapters provide a detailed description of all firmware features and how to configure their parameters through the web management system. Depending on your device model, some of the features may not be available in your device, you can skip the chapters without affecting your understanding of the other content.

CHAPTER

FOUR

SOFTWARE CONFIGURATION

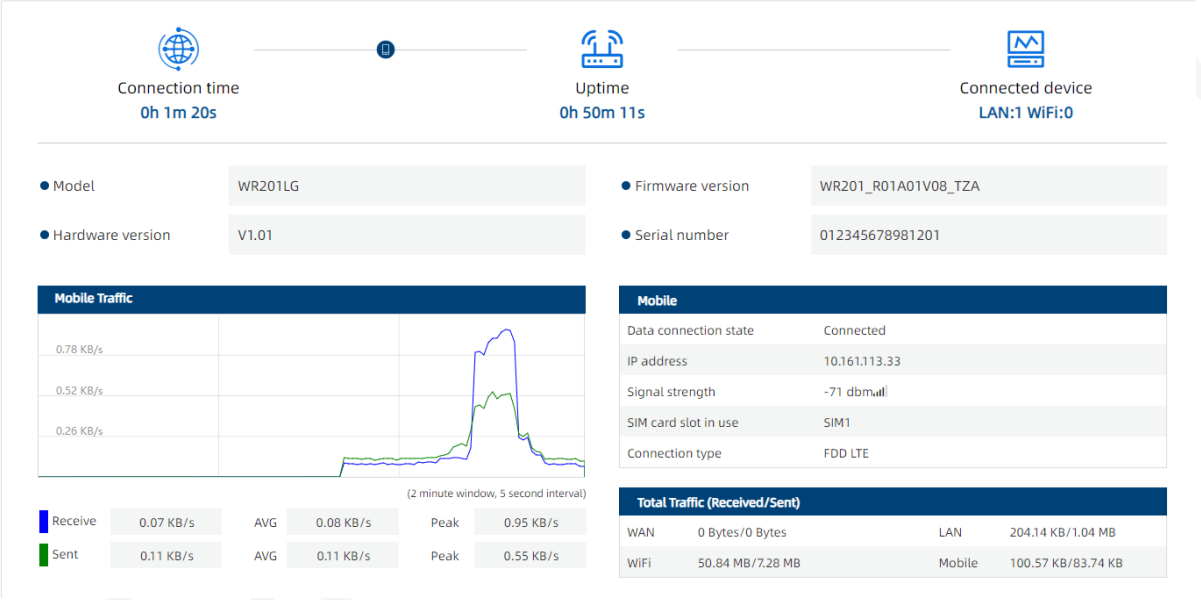
4.1 Status

This section includes the running status of the device.

4.1.1 Overview

The **Overview** page contains various information summaries, such as connection state, mobile connection state and traffic. It is also the homepage of the WebUI.

The figure below is an example of the Overview page:



4.1.2 Device

The **Device page** displays the device's hardware, software and modem related information. You can find serial number and software version in this page, which is important information for after-sales maintenance.

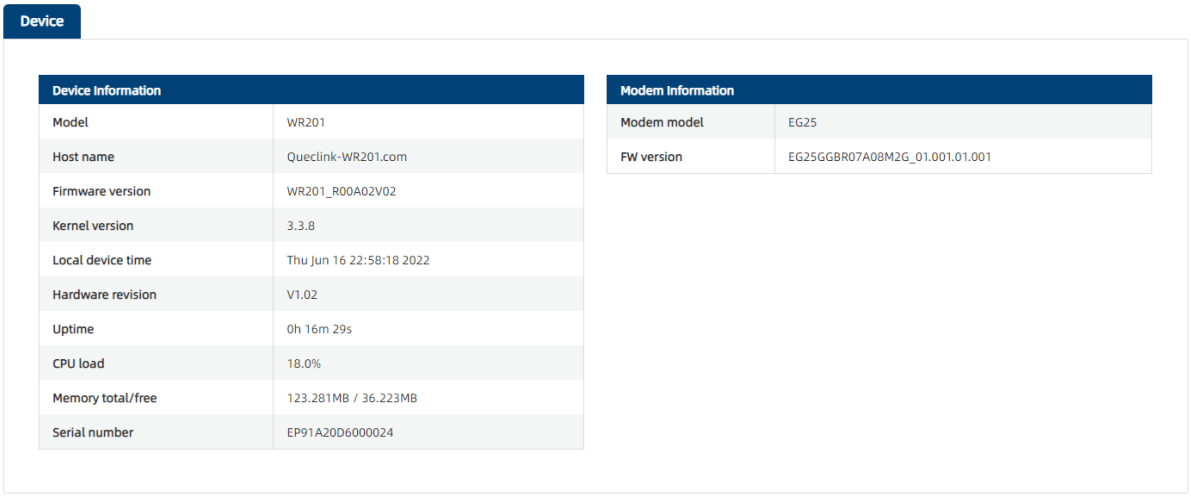


Table 1: Device Information Description

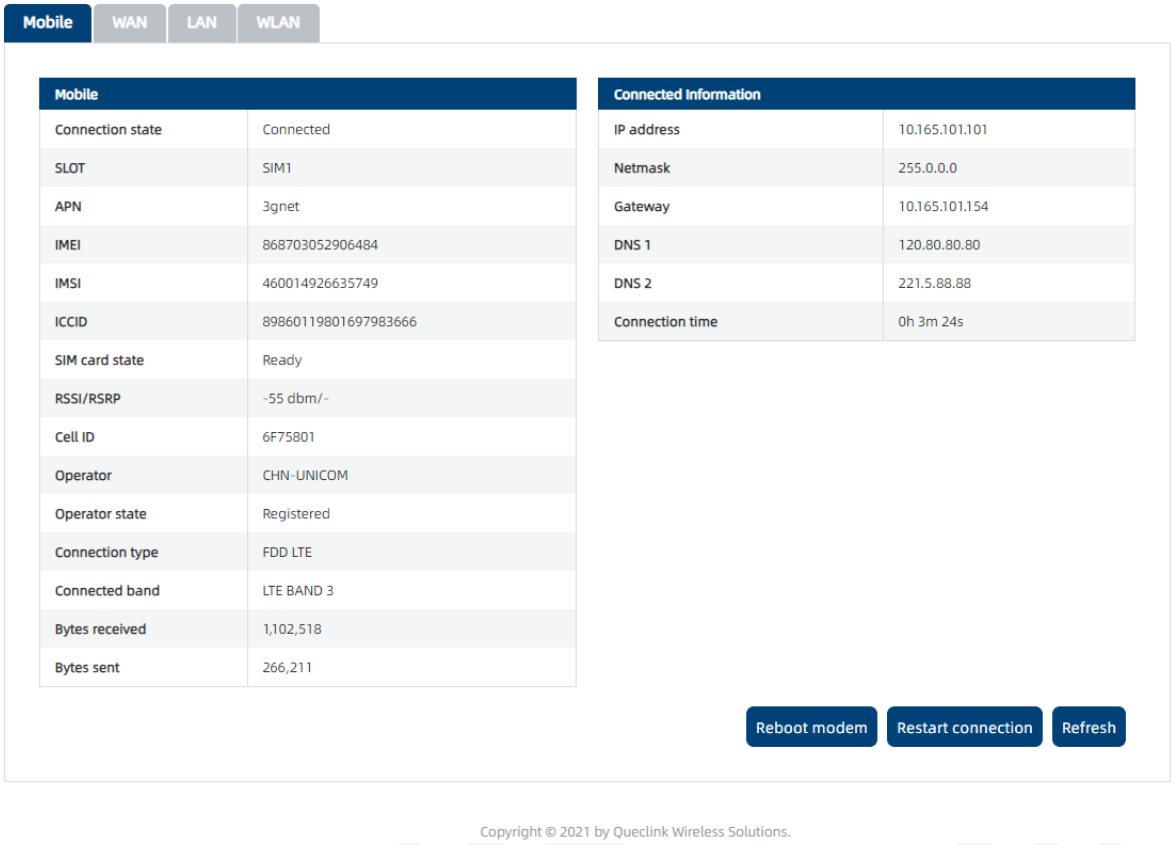
Field Name	Description
Model	Displays model number of the device.
Host name	Displays the device's host name. The hostname can be used instead of the LAN IP address to communicate with the device inside the local network.
Firmware version	Displays the firmware version currently used by the device.
Kernel version	Displays the device's kernel version. A kernel is a computer program responsible for connecting a device's software to its hardware.
Local device time	Displays the current time as perceived by the device.
Hardware version	Displays the device's hardware version.
Uptime	Displays the running time since the device's last start up.
CPU load	Displays the current CPU load of the device.
Memory total/free	Displays the amount of currently unused RAM.
Serial number	A unique device identifier.
Modem Model	The modem's model number
FW version	Modem's current firmware version

4.1.3 Network

4.1.3.1 Mobile

The Mobile page has two tables, one table displays the wireless information and the SIM card in use, another one displays the connection information, including IP address, DNS, etc. The figure below is an example of the Mobile page:

Queclink Confidential



You can click Reboot Modem or Restart Connection button to restore the connection if the connection is abnormal. The Refresh button is to refresh all information fields in the page.

Queclink Confidential

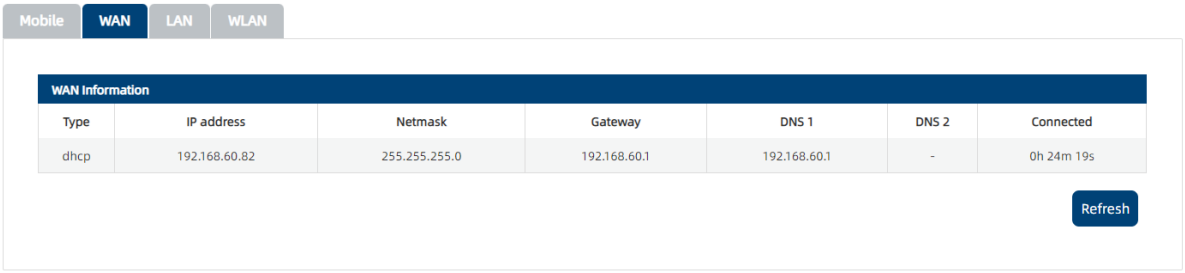
Field Name	Description
Connection State	Indicates whether the device has an active mobile data connection.
SLOT	The slot ID of the working SIM card.
APN	The APN (Access Point Name) provides a phone with the information needed to connect to wireless service.
IMEI	The IMEI (International Mobile Equipment Identity) is a unique 15 decimal digit number used to identify mobile modules. GSM network operators use the IMEI to identify devices in their networks.
IMSI	The IMSI (international mobile subscriber identity) is a unique 15 decimal digit (or less) number used to identify the user of a cellular network.
ICCID	SIM card's ICCID is a unique serial number used to identify the SIM chip.
SIM card state	The current SIM card state. Possible values are: • **Ready** - SIM card is inserted and ready to be used • **Inserted** - SIM card is inserted • **Not inserted** - SIM card is not inserted • **Unknown** - unable to obtain SIM card state value. Possible communication issue between the device and the modem.
RSSI/RSRP	Received signal strength indicator (RSSI) measured in dBm. Values closer to 0 mean a better signal strength.
Cell ID	The ID of the cell that the modem is currently connected with.
Operator	Network operator's name.
Operator state	Indicates whether the device is currently registered on a mobile network. Possible values are: • **Not registered** - not registered to a network and the device is not currently searching for a new operator to register with. • **Registered** - registered to home network. • **Registration denied** - registration to network denied by operator. • **Unknown** - operator state is currently unknown. • **Registered roaming** - registered to network, roaming conditions.
Connection type	Mobile connection type. Possible values are: • **2G:** 2G (GSM), 2G (GPRS), 2G (EDGE) • **3G:** 3G (WCDMA), 3G (HSDPA), 3G (HSUPA), 3G (HSPA), 3G (HSPA+), 3G (DC-HSPA+), 3G (HSDPA+HSUPA), UMTS • **4G:** 4G (LTE) • **- :** impossible to determine at the moment.
Connected band	Currently used frequency band.
Bytes received	Amount of data received through the mobile interface.
Bytes sent	Amount of data sent through the mobile interface.
Restart Modem	Reboots the device's cellular module.
Restart Connection	Restarts the mobile connection.
Refresh	Refreshes all information fields in the page.
Type	The dialing mode of the connection.
IP address	The device's modem IP address.
Netmask	A netmask is used to define how "large" a network is by specifying which part of the IP address denotes the network and which part denotes the device.
Gateway	Gateway of the default route - an IP address through which the device reaches the Internet.
DNS	DNS servers used by the connection.
Connection time	Currently used connection uptime.

Queclink Confidential

4.1.3.2 WAN

The **WAN** section displays information about the WAN interface, the connection type, IP address, Netmask, etc.

The figure below is an example of the WAN status page:



The Refresh button is to refresh all information fields in the page.

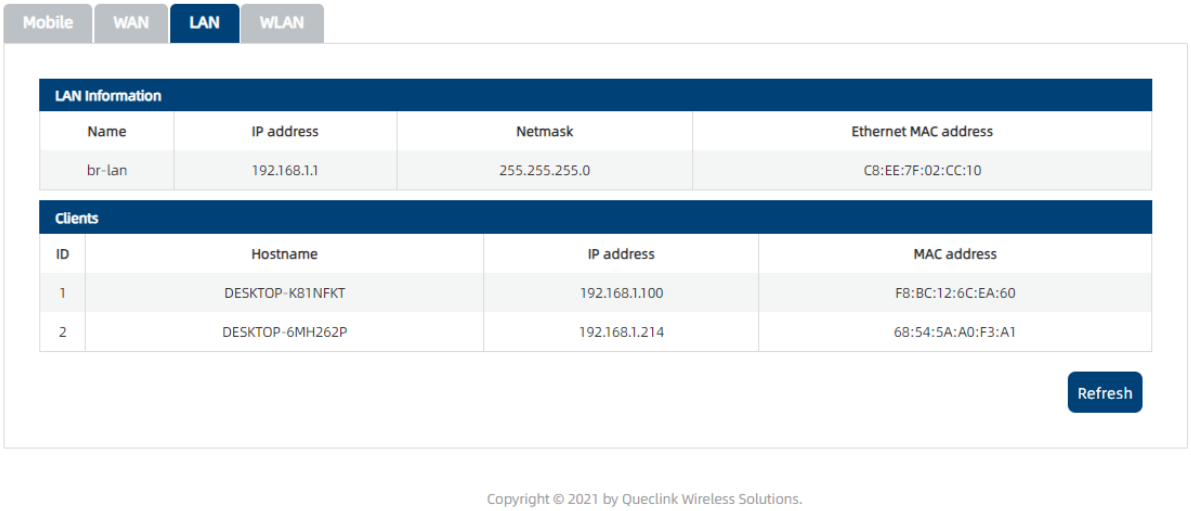
Table 2: WAN Interface Description

Field Name	Description
Type	• **Static** - WAN network interface controller configuration parameters are set manually (used when the WAN gateway is not a DHCP server) • **DHCP** - Dynamic Host Configuration Protocol; the WAN network interface controller acts as a DHCP client, meaning that it receives a dynamically assigned IP address and other network configuration parameters. • **PPPoE** - Point-to-Point Protocol over Ethernet; used to establish a Digital Subscriber Line (DSL) Internet service connection.
IP address	WAN IP address.
Netmask	A netmask is used to define how “large” a network is by specifying which part of the IP address denotes the network and which part denotes the device.
Gateway	Gateway of the default route - an IP address through which the device reaches the Internet.
DNS	DNS servers used by the main WAN connection.
Connected	Currently WAN interface connection uptime.
Refresh	Refreshes all information fields in the page.

4.1.3.3 LAN

The **LAN Information** page contains data on the device’s LAN interfaces. There are two sections on this page, one is LAN information, including IP, Netmask, MAC address, connected time, and another one is DHCP lease, which contains information about DHCP clients.

Queclink Confidential



The Refresh button is to refresh all information fields in the page.

Table 3: LAN Interface Description

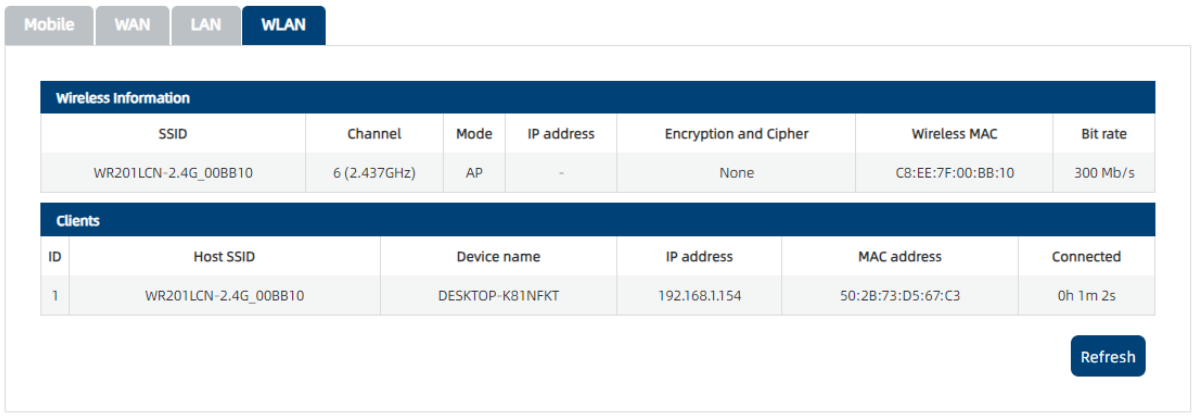
Field Name	Description
LAN Information	
Name	LAN interface name.
IP address	LAN IP address.
Netmask	A netmask is used to define how “large” a network is by specifying which part of the IP address denotes the network and which part denotes the device.
Ethernet MAC address	LAN MAC address.
Clients	
Hostname	DHCP client’s hostname.
IP address	DHCP client’s IP address.
MAC address	DHCP client’s MAC address.

4.1.3.4 WLAN

This page displays information about wireless connections and associated Wi-Fi stations. When the device is working in AP mode, the page displays AP information, otherwise, the page displays the connected station information.

The device can work either in Access Point (AP) mode or Station mode.

The figure below is an example of the WLAN status page:



The Refresh button is to refresh all information fields in the page.

Table 4: Wi-Fi Interface Description

Field Name	Description
SSID	The broadcasted SSID (Service Set Identifier) of the wireless network.
Channel	Currently used channel. In most countries there are 13 Wi-Fi channels on the 2.4 GHz band (14 in Japan) to choose from.
Mode	Connection mode. Can either be Access Point (AP) or Client. In AP mode, other devices can connect to the device wireless network through SSID. In client mode, the device can connect to other wireless networks.
Encryption and Cipher	The type of Wi-Fi encryption and Cipher used.
Wireless MAC	The MAC (Media Access Control) address of the access point radio.
Bit rate	The maximum possible physical throughput that the Router's radio can handle. Bit rate will be shared between Router and other possible devices which connect to local Access Point (AP).

4.1.4 Applications

The Services table displays the status of the device's services. Services that are currently disabled are displayed in red font; services abnormal are also displayed in red font. The user can click Change Setting button to direct to the configuration page of the services.

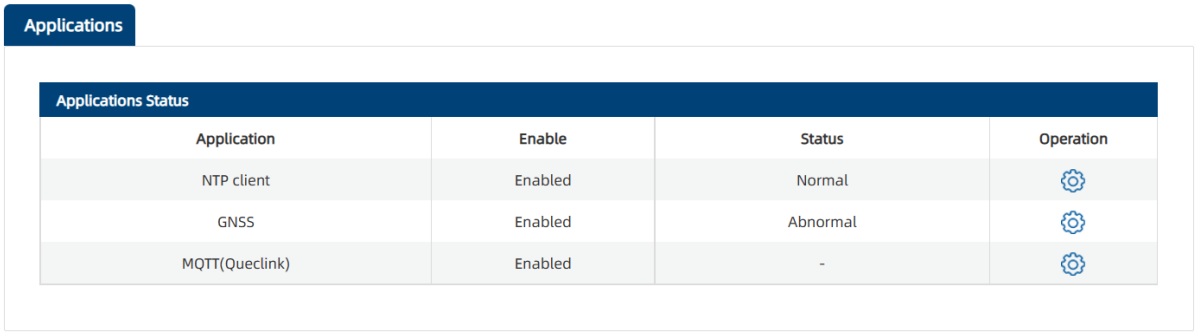


Table 5: Applications Status Information

Field Name	Description
Applications	Name of the application.
Enabled	Display the enable/disable status of this service.
Status	Display the working status of this service.
Operation	Quick button to the configuration page.

4.1.5 VPN

The VPN table displays the status and connection information of all VPN links. The status is Connected if a VPN connection is established. You can also see the IP address (working as client) or the number of connected devices (working as server) on this page.



Table 6: VPN Status Information

Field Name	Description
Name	Associated VPN name.
Enable	Display the enable/disable status of this VPN.
Status	VPN connection status
Mode	Current operating mode. Can either be Server or Client.
IP/Client Number	If the VPN is a client, it displays the IP address allocated by the server. If the VPN is a server, it displays the client number connecting to the server.
Time	The total connection time of this connection.

4.1.6 Routes

The Routes page displays the device's ARP table and active routes.

The ARP section displays the device's ARP cache (also known as ARP table) data. The ARP cache contains information about each known MAC address and its corresponding IP address. When the router receives a packet destined for a local host, the ARP program attempts to find a physical host or MAC address in the ARP cache that matches the IP address. If the ARP cache doesn't contain the needed IP address, ARP broadcasts a request packet to all LAN devices in order to find the device with the specified IP address.

The Active IP routes section displays the device's routing table. A routing table contains a list of routes to network destinations associated with and known by the device.

The figure below is an example of the ARP and IP routes section:

Queclink Confidential



ARP Parameter description:

Table 7: ARP Table Information

Field Name	Description
IP address	IP address of a local host.
MAC address	MAC address of a local host.
Interface	Interface through which the device is associated with the host.

Routes Parameter description:

Table 8: Static Routes Information

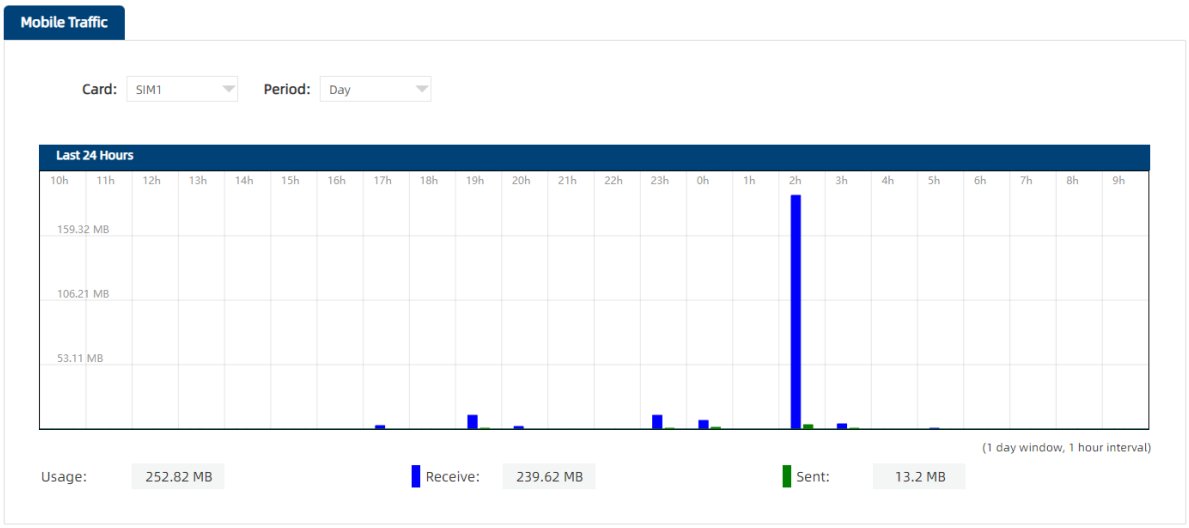
Field name	Description
Interface	Associated network interface name.
Target	Destination network address.
IP gateway	Indicates the IP address of the gateway through which the target network can be reached.
Metric	Metrics help the device choose the best route among multiple feasible routes to a destination. The route will go in the direction of the gateway with the lowest metric value.

4.1.7 Mobile Traffic

The Mobile Traffic section contains graphs that display mobile data usage values over different periods of time. Different tabs of the Mobile Traffic section display mobile data usage values over different periods of time. You can select the period by day, week and month.

The device accumulates the traffic passing through the modem interface, which may not exactly match the traffic statistics provided by the operators.

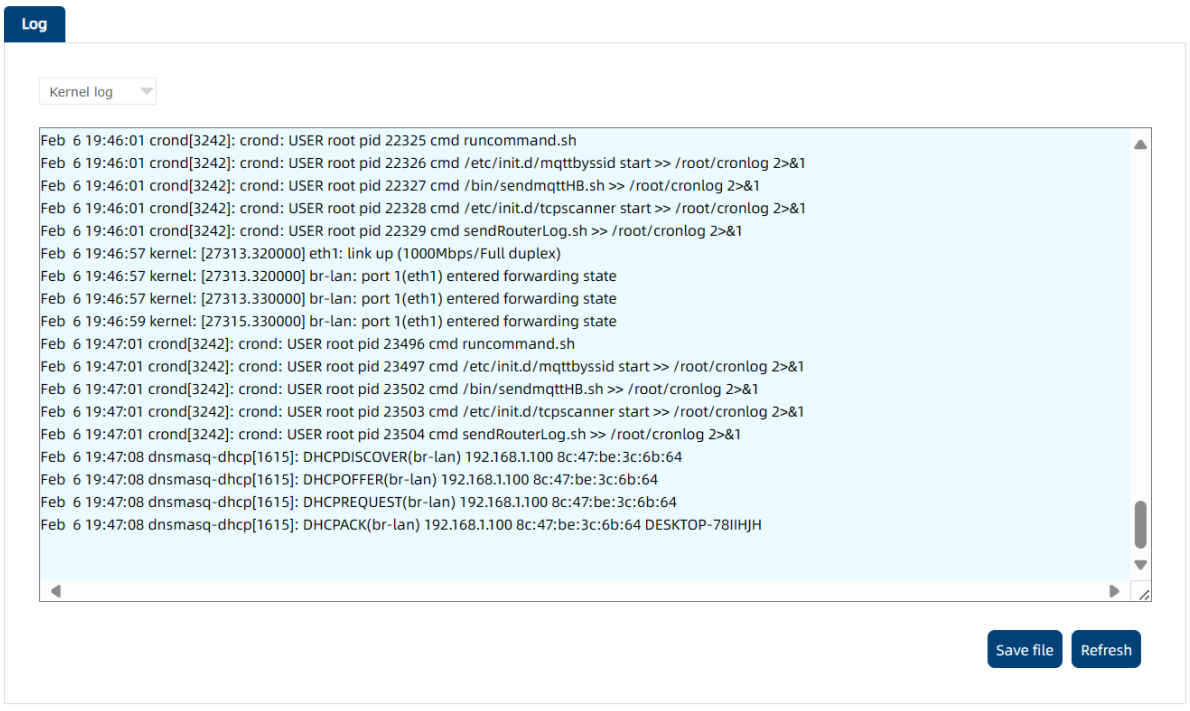
Queclink Confidential



Copyright © 2021 by Queclink Wireless Solutions.

4.1.8 Log

The Log Viewer page displays the contents of the system log or kernel log. You can select which log file to display with the drop-down box. The Refresh button is to update the content, and you can save the current log as a .rar file through the “Save file” button.



4.2 Network

This section shows you how to configure the network of the device.

4.2.1 Link Management

The link management is to manage the WAN connection of the device, the device has three interfaces can work as WAN interface: Mobile, WAN and WLAN (2.4G or 5G, station mode), the user can configure one of them as primary link and another one as backup link, if primary link goes down, the device can switch to backup link according to the failover configuration. The two links can also work in Load Balancing mode; the device will divide traffic between two interfaces.

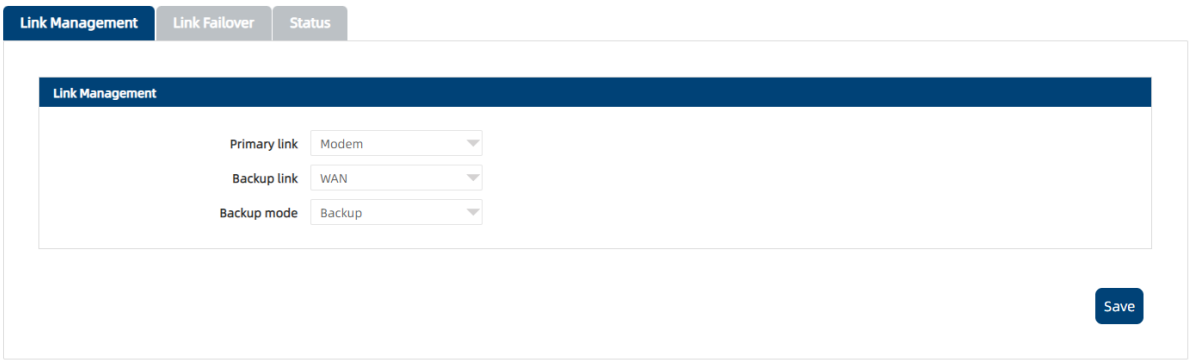
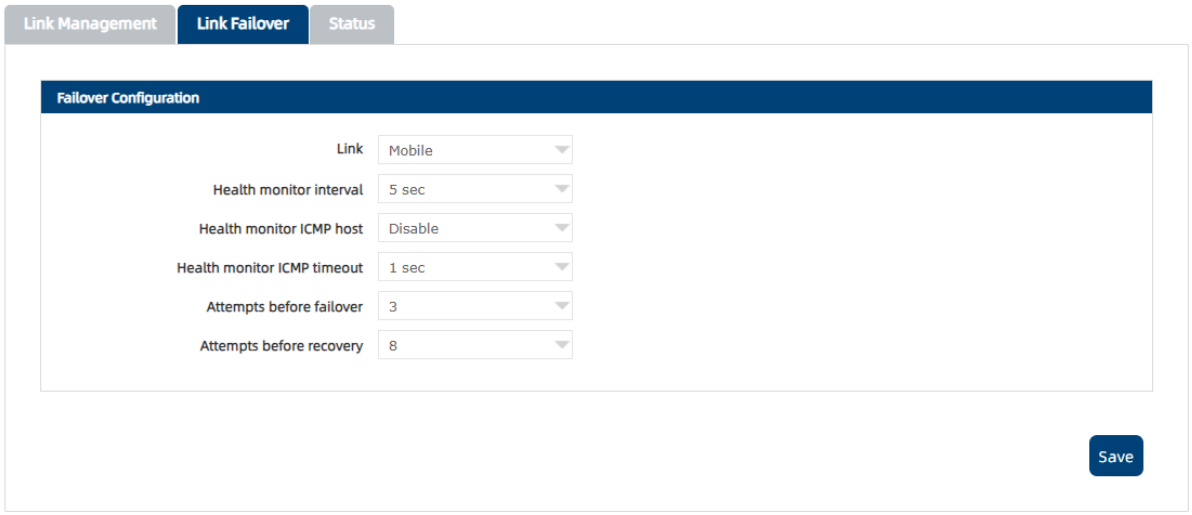


Table 9: Link Management Information

Field Name	Value	Description
Primary Link	Modem|WAN|WLAN	Select from “Modem” or “WAN”. • **Modem:** Select to make mobile as the primary wireless link. • **WAN:** Select to make WAN as the primary wire link. • **WLAN:** Select to make WLAN as the primary wire link.
Backup Link	None|Modem|WAN|WLAN	Select from “None”, “Modem”, “WAN” or “WLAN”. • **None:** Do not select any backup link. • **Modem:** Select to make mobile as the primary wireless link. • **WAN:** Select to make WAN as the primary wire link. • **WLAN:** Select to make WLAN as the primary wire link.
Backup mode	Backup|Load Balancing	Select from “Backup” or “Load Balancing”. • **Backup:** The inactive link is on standby. • **Load Balancing:** Use two links simultaneously.

The failover configuration section is used to configure the switchover rules. The device use ICMP to check the status of the link, if link is abnormal, the device will switch to the backup link.

Queclink Confidential

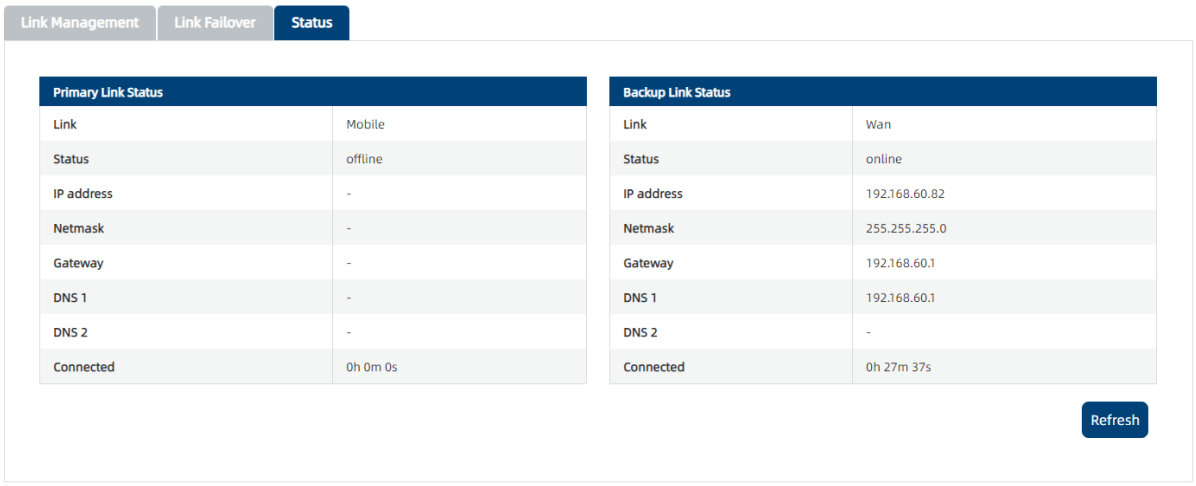


Copyright © 2021 by Queclink Wireless Solutions.

Table 10: Link Failover Information

Field Name	Value	Description
Link	Modem|Wan|Wifi2.4G|Wifi5G	Associated interface to configure the failover strategy.
Health monitor interval	Disable|5 sec|10 sec|20 sec|30 sec|60 sec|120 sec	Number of seconds between each test.
Health monitor ICMP host	Disable|DNS server|Gateway|Custom	Indicates the host try to ping, select custom to manually configure an IP address to ping.
Health monitor ICMP timeout	1 sec|3 sec|4 sec|5 sec|10sec	Set the ping timeout.
Attempts before failover	1|3|5|8|15|20	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.
Attempts before recovery	1|3|5|8|15|20	Set the max ping tries. Switch to primary link if the max continuous ping tries reached.

The status page displays the connecting link and parameters of the current connection.



4.2.2 Mobile

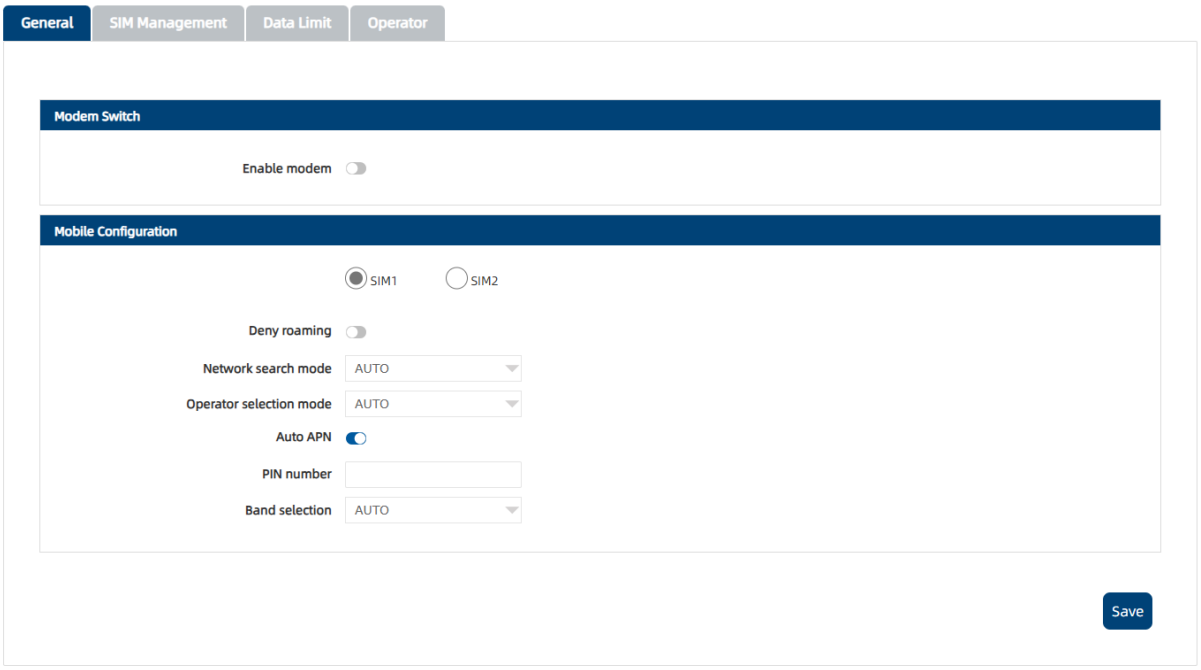
The Mobile page is used for setting parameters related to the mobile data connection. The device has two SIM slots, each slot can insert a SIM card, and the user can select one SIM as the primary SIM and allow the switchover between two SIMs.

The device has a mechanism to automatically detect SIM card and use appropriate dialing parameters in the system. Even if no parameters are configured, the device can still attempt to automatically dial to establish a connection.

4.2.2.1 General

The Mobile Configuration section is used to configure SIM card parameters.

Refer to the figure below for information on the fields contained in the section.



Confi

Table 11: Mobile Network Information

Field	Value	Description
Deny roaming	off | on; default: off	Denies data connection on roaming conditions.
Network search mode	AUTO|GSM only|WCDMA only|LTE only|TD-SCDMA only|UMTS only|CDMA only|HDR only|CDMA and HDR only; default: AUTO	The network settings for connection. The device will only connect to the network specified in this configuration. The available options depend on the type of modem within the device.
Operator selection mode	AUTO|Manual|SEMI	Operator selection method. • **AUTO** - selects the operator automatically. • **MANUAL** - requires you to configure the operator manually. Two operators are allowed to configure. • **SEMI** - prompts you to enter an operator's code, but if the router can't connect to the configured network, it will automatically connect to the available operator.
Auto APN	checkbox; default: enabled	Auto APN scans an internal Android APN database and selects an APN based on the SIM card's operator and country. If the first automatically selected APN doesn't work, it attempts to use the next existing APN from the database.
APN	string; default: none	An Access Point Name (APN) is a gateway between a GSM, GPRS, 3G or 4G mobile network and another computer network. Depending on the contract, some operators may require you to use an APN just to complete the registration on a network. In other cases, APN is used to get special parameters from the operator (e.g., a public IP address) depending on the contract. An APN Network Identifier cannot start with any of the following strings: • *rac* • *lac* • *sgsn* • *rnc* it cannot end in: • *.gprs* and it cannot contain the asterisk symbol (*).
Authentication method	CHAP|PAP|None; default: None	Authentication method that your GSM carrier uses to authenticate new connections on its network. If you select PAP or CHAP, you will also be required to enter a username and password.
PIN number	string; default: none	A 4-digit long numeric password used to authenticate the modem to the SIM card. Reminder: First boot will not reset the PIN number, it must be changed manually.
Band selection	AUTO|MANUAL default: AUTO	Configure the network frequency band. Once manual configuration is selected, users can specify the frequency band for the network connection.

Queclink Confidential

Click Save button to save the configuration and re-establish the connection.

4.2.2.2 SIM Management

The SIM Management section provides you with the function to configure which SIM card is the primary one and which one is slave one, you can setup SIM switching rules between two SIM cards. SIM switching is the failover mechanism when two SIM cards are available. For example, if the user has two SIM cards with limited data, you can setup a rule that switches the in use SIM card to the slave SIM card when the data limit is reached. You can setup similar rules for signal strength and more.

The Primary card section is used to select which SIM slot will host the device's primary SIM card. The primary SIM card is the one which is active by default, while the secondary card stays inactive until switchover happen.

The SIM switching section enables automatic SIM card switching and allows configuration of the switching check interval. When the switch is toggled on, the device will switch to the alternate SIM card if the current SIM card loses network connectivity.

"Switch back to primary SIM card after timeout" allow devices to switch back to the primary SIM card when the configured timeout is reached. The minimum allowed value of timeout is 600s.

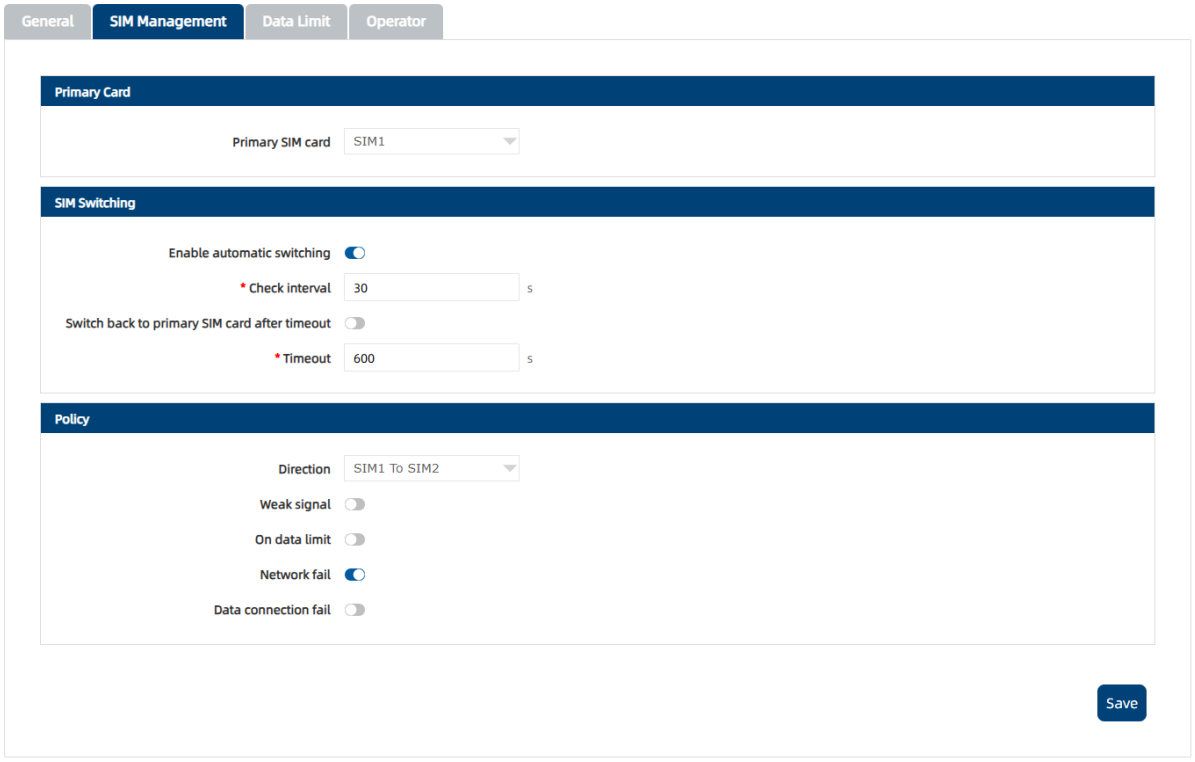


Table 12: SIM Switching Information

Field	Value	Description
Enable automatic switching	yes|no; default: yes	Turns automatic SIM Switching on or off.
Check interval	integer; default: 30	The frequency at which the device will check for condition changes corresponding to SIM switch rules. If such a condition happens, the device will perform a switchover, if not - it will check for the same conditions again after the amount of time specified in this field.
Switch back to primary SIM card after timeout	yes|no; default: no	Turns switching to the primary SIM card on or off.
Timeout	integer; default: 600	The device attempts to switch back to the primary SIM card at the configured timeout. If the primary SIM card has network connectivity, the device will switch to it; otherwise, it will continue using the backup SIM card.
On weak signal	yes|no; default: no	Performs a SIM switch when signal strength value (RSSI in dBm) falls below a specified threshold. When this field is checked you will see an additional field for entering the minimum signal strength value appear.
On data limit	yes|no; default: no	Performs a SIM switch when the SIM card reaches the specified data limit for the designated period. Mobile data limit can be configured in the Services → Mobile → Mobile Data Limit page.
On data connection fail	yes|no; default: yes	Performs a SIM switch when the device does establish network connection.

4.2.2.3 Data Limit

The Data Limit section is used to configure custom mobile data limits for your SIM card(s). When the mobile data limit set for the SIM card(s) is reached, the device will no longer use the mobile connection to establish a data connection until the limit period is over or the limit is reset by the user.

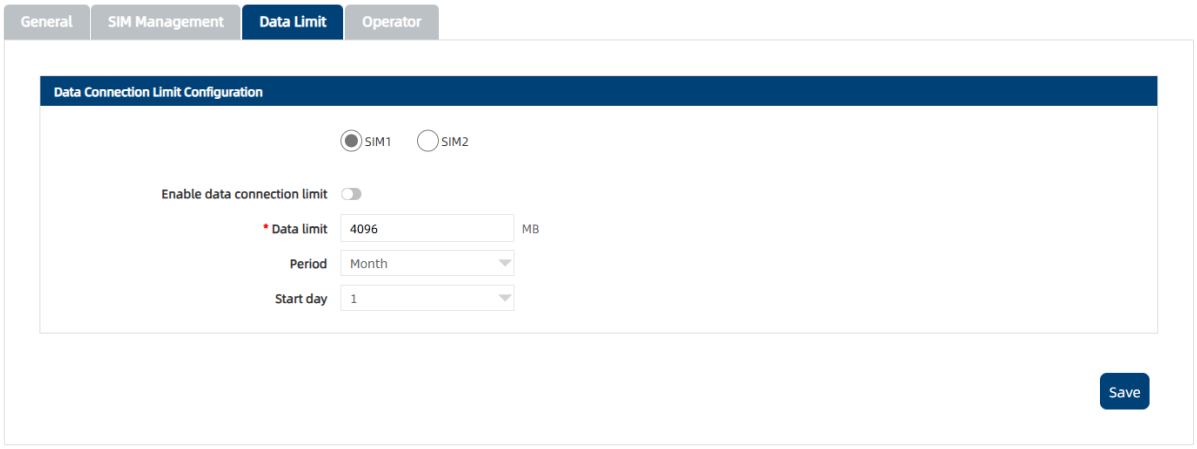


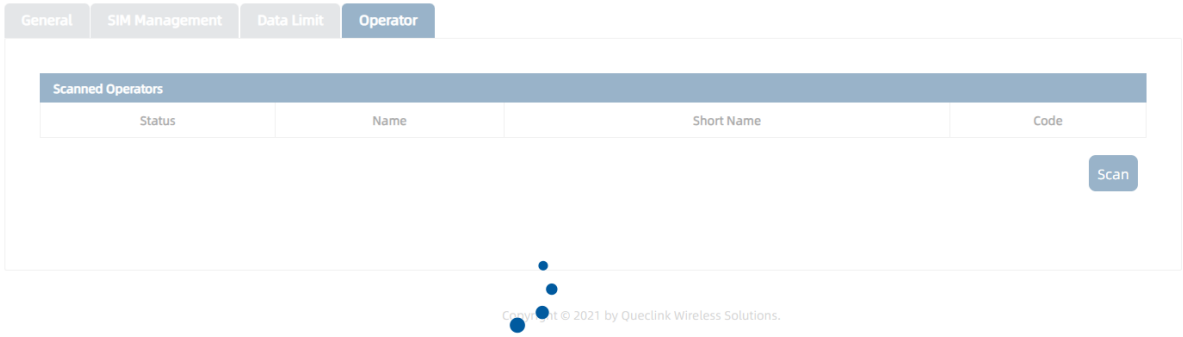
Table 13: Data Limit Information

Field	Value	Description
Enable data connection limit	yes|no; default: no	Turns mobile data limitations on or off.
Data limit* (MB)	integer; default: none	The amount of data that is allowed to be downloaded over the specified period of time. When the limit is reached, the device will no longer be able to establish a data connection until the period is over or the data limit is reset. Note: after the device has reached the data limit it will not switch to using the secondary SIM card. If you wish to configure a SIM switch system based on received data limit, instructions can be found in the SIM Management section of this page.
Period	Month|Week|Day; default: Month	Data limit period after which the data counter is reset on the specified Start day.
Start day|Start hour	day [1..31]|day [Monday..Sunday]|hour [1..24]; default: day 1	Specifies when the period of counting data usage should begin. After the period is over, the limit is reset and the count begins over again.

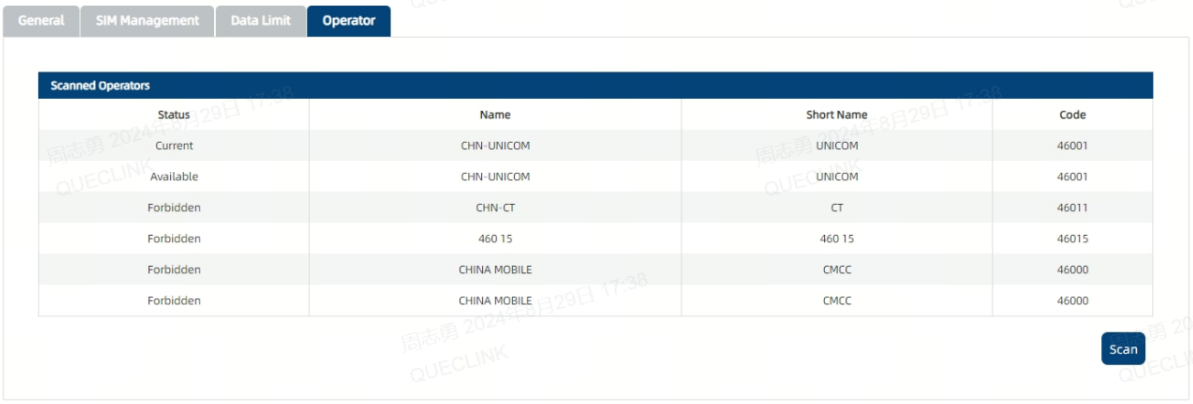
4.2.2.4 Operator

The operator section provides you with the possibility to scan for mobile network operators to which the device's SIM card can connect to.

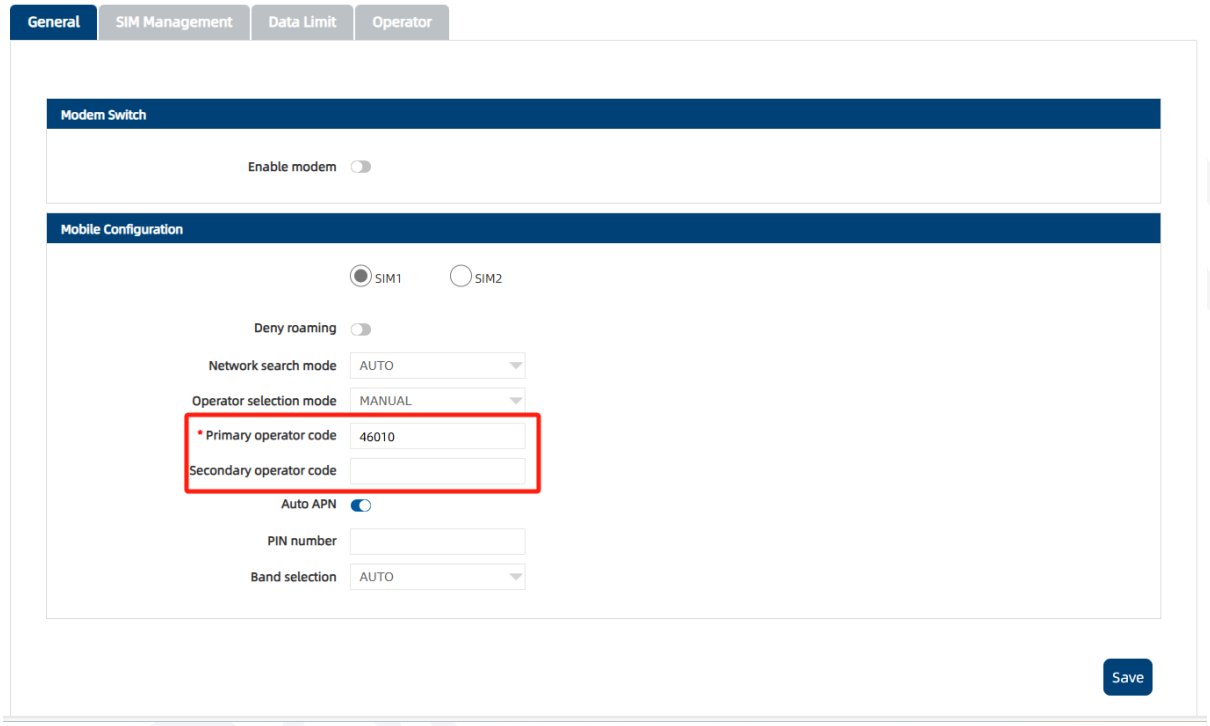
Click "Scan" button to scan the available operators. Wait for the scan to complete. As indicated by the on-screen message, the process can take up to 3-5 minutes that depends on the network environment and SIM card.



Once the scan has finished, you will see the results in the Scanned operators'.



Then you can input an operator code on the general page:



4.2.3 WAN

The WAN page is used to configure different protocols for WAN interfaces. The device supports Static, DHCP and PPPoE protocol. You can click Switch Protocol button to display and configure the parameters. The content will change according to which network protocol is selected.

The Static protocol is used when there is no DHCP server available. Therefore, you need to configure a static IP address based on the available source. The following is an example of static configuration page:

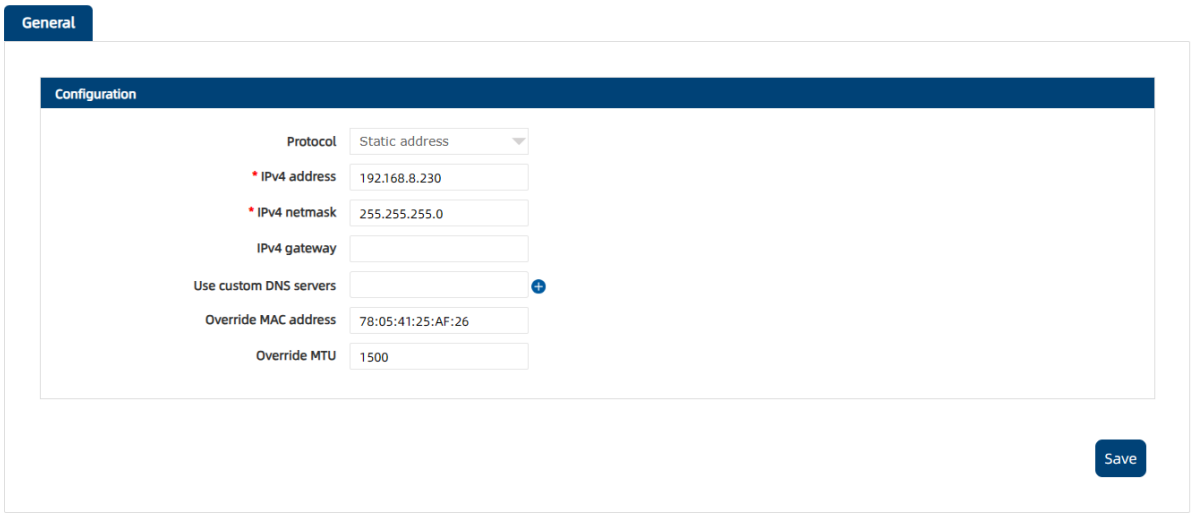
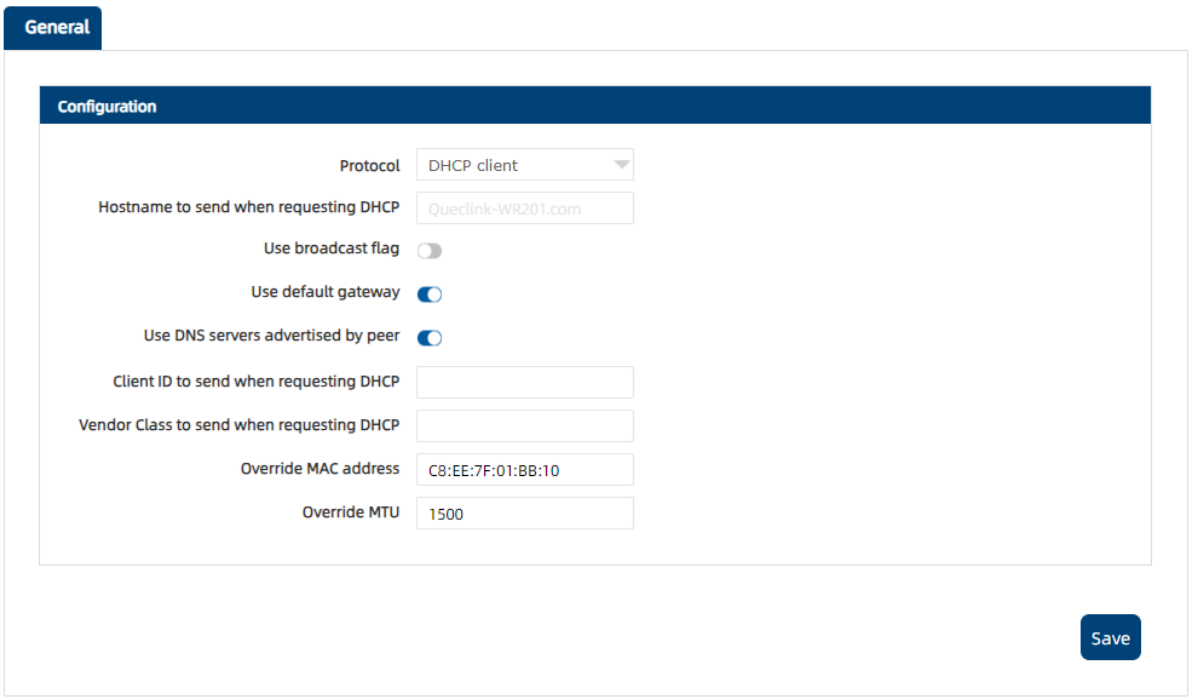


Table 14: WAN Configuration Information

Field name	Value	Description
Protocol	Static|DHCP|PPPoE; default: DHCP	The protocol used by the WAN interface.
IPv4 address	ip; default: none	IP address on the WAN network.
IPv4 netmask	ip; default: none	Netmask defines how “large” a network is.
IPv4 gateway	ip; default: none	The address where the device will send all the outgoing traffic.
Override MAC address	mac; default: none	Override MAC address of the WAN interface. For example, your ISP (Internet Service Provider) gives you a static IP address and it might also bind it to your computers MAC address (i.e., that IP will only work with your computer but not with your device). In this field you can enter your computer’s MAC address and fool the gateway in to thinking that it is communicating with your computer.
Override MTU	integer [0..1500]; default: 1500	Maximum Transmission Unit (MTU) - specifies the largest possible size of a data packet.

The DHCP protocol should be used when the source of your internet has a DHCP server. The following is an example of DHCP configuration page:

Queclink Confidential



Copyright © 2021 by Queclink Wireless Solutions.

Table 15: WAN DHCP Configuration Information

Field Name	Value	Description
Protocol	Static|DHCP|PPPoE; Default: DHCP	The protocol used by the WAN interface.
Hostname to send when requesting DHCP	ip|hostname; Default: device's hostname	Host name to which the DHCP request will be sent to.
Use broadcast flag	yes|no; Default: no	Required for certain ISPs (Internet Service Providers), e.g. Charter with DOCSIS 3.
Use default gateway	yes|no; Default: yes	Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured.
Use DNS servers advertised by peer	yes|no; Default: yes	Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored.
Client ID to send when requesting DHCP	string; Default: none	Client ID which will be sent when requesting a DHCP lease.
Vendor class to send when requesting DHCP	string; Default: none	Vendor class which will be sent when requesting a DHCP lease.
Override MAC address	mac; Default: none	Override MAC address of the WAN interface. For example, your ISP (Internet Service Provider) gives you a static IP address and it might also bind it to your computers MAC address (i.e., that IP will only work with your computer but not with your device). In this field you can enter your computer's MAC address and fool the gateway in to thinking that it is communicating with your computer.
Override MTU	integer [0..1500]; Default: 1500	Maximum Transmission Unit (MTU) - specifies the largest possible size of a data packet.

The PPPoE protocol is used if you have a DSL internet provider, in this case, you can select the PPPoE protocol to connect to the internet. The following is an example of PPPoE configuration page:

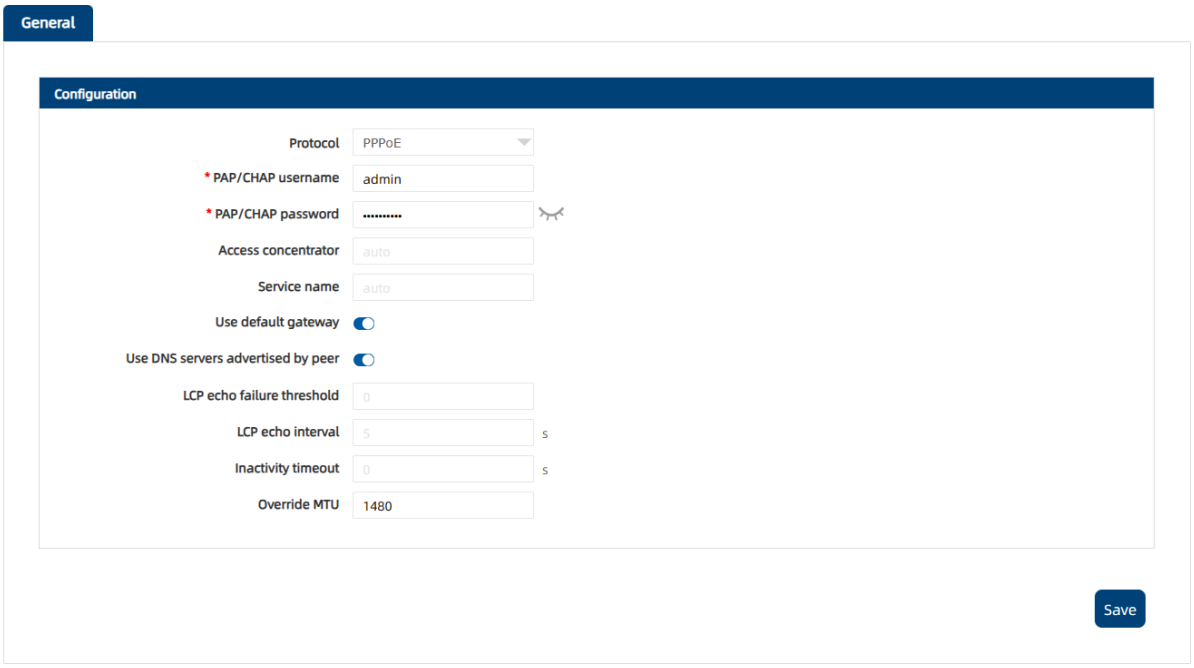
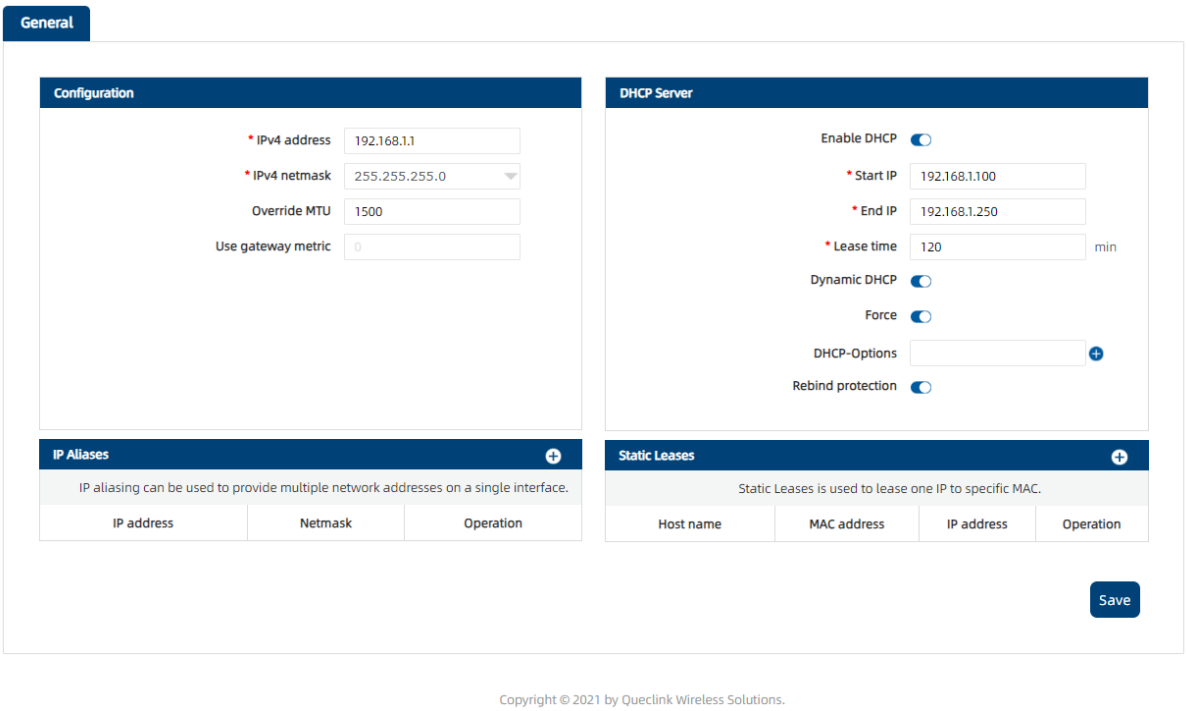


Table 16: WAN PPPoE Configuration Information

Field Name	Value	Description
Protocol	Static|DHCP|PPPoE; default: DHCP	The protocol used by the WAN interface.
PAP/CHAP username	string; default: none	The username that you use to connect to your carrier's network.
PAP/CHAP password	string; default: none	The password that you use to connect to your carrier's network.
Access concentrator	string; default: none	The name of the access concentrator. Leave empty to auto detect.
Service name	string; default: none	The name of the service. Leave empty to auto detect.
Use default gateway	yes|no; default: yes	Uses the default gateway obtained through DHCP. If left unchecked, no default route is configured.
Use DNS servers advertised by peer	yes|no; default: yes	Uses DNS servers obtained from DHCP. If left unchecked, the advertised DNS server addresses are ignored.
LCP echo failure threshold	integer; default: 0	Presumes peer to be dead after given amount of LCP echo failures. Leave it at 0 to ignore failures.
LCP echo interval	integer; default: 5	Sends LCP echo requests at the given interval in seconds. This function is only effective in conjunction with failure threshold.
Inactivity timeout	integer; default: 0	Close inactive connection after the given amount of seconds. Leave it at 0 to persist connection.
Override MTU	integer [0..1500]; default: 1480	Maximum Transmission Unit (MTU) - specifies the largest possible size of a data packet.

4.2.4 LAN

This page allows you to set the related parameters for LAN port, such as IP address, IP Netmask, etc. There are four LAN ports on WR310. The following is the example configuration page of LAN port.



A **DHCP** server is a service that can automatically configure the TCP/IP settings of any device that requests such a service (i.e., connects to the device with the operational DHCP server). The device can be configured as DHCP server. If you connect a device that has been configured to obtain an IP address automatically, the device will lease out an IP address from the available IP pool and the device will be able to communicate within the private network. You can configure DHCP settings in DHCP section. Advanced setting is also available in this section.

Static IP leases are used to reserve specific IP addresses for specific devices by binding them to their MAC address. This is useful when you have a stationary device connected to your network that you need to reach frequently, e.g., printer, server, etc. You can configure setting in static leases section.

IP Aliases section allows you to multi IP address for the device. It is a way of defining or reaching a subnet that works in the same space as the regular network. This is useful if you need to reach the device that is located in the same network but in a different subnet.

Table 17: DHCP Configuration Information

Field Name	Value	Description
Configuration		
IPv4 address	ip; Default: 192.168.1.1	IP address that the device uses on the LAN network.
IPv4 netmask	ip; Default: 255.255.255.0	A netmask is used to define how “large” the LAN network is.
Override MTU	integer [0..1500]; Default: 1500	MTU (Maximum Transmission Unit) specifies the largest possible size of a data packet.
Use gateway metric	integer; Default: 0	The LAN configuration generates an entry in the routing table. In this field you can alter the metric of that entry. Higher metric means higher priority.
DHCP Server		
Enable DHCP	Enable|Disable|DHCP Relay; Default: Enable	Enables or disables DHCP Server. If DHCP Relay is selected, you will be prompted to enter an IP address of another DHCP server in your LAN. In this case, whenever a new device connects to the device, the device will redirect any DHCP requests to the specified DHCP Server.
Start IP	ip; Default: 192.168.1.100	The starting IP address value. e.g., if your device’s LAN IP is 192.168.2.1 and your subnet mask is 255.255.255.0 that means that in your network a valid IP address has to be in the range of [192.168.2.0..192.168.2.254] (192.168.2.255 is a special unavailable address). If the Start ip is set to 192.168.2.100 then the DHCP server will only lease out addresses starting from 192.168.2.100.
End IP	ip;Default:192.168.1.250	The end IP address value. Continuing from the above example: if the start address is 192.168.2.100 and the end IP is 192.168.2.250,available addresses will be from 192.168.2.100 to 192.168.2.250.
Lease time	time in minutes; Default: 120min	The duration of an IP lease. Leased out addresses will expire after the amount of time specified in this field and the device that was using the lease will have to request a new DHCP lease. However, if the device stays connected, its lease will be renewed after half of the specified amount of time passes, e.g., if the lease time is 12 hours, then every 6 hours the device will send a request to the DHCP server asking to renew its lease. Lease time can be set in minutes (m). The minimal amount of time that can be specified is 2mins (2m).
Dynamic DHCP	yes|no; Default: yes	Enables Dynamic allocation of client addresses. If this is disabled, only clients that have static IP leases will be served
Force	yes|no; Default: yes	The DHCP force function ensures that the device will always start it’s DHCP server, even if there is another DHCP server already running in the device’s network. By default, the device DHCP server will not start when it is connected to a network segment that already has a working DHCP server.
DHCP Options	DHCP options; Default: none	Additional options to be added to the DHCP server. For example with ‘26,1470’ or ‘option:mtu, 1470’ you can assign an MTU value per DHCP.
Rebind protection	yes|no; Default: yes	Rebind protection helps prevent malicious attacks by ensuring that client devices only accept IP address assignments from legitimate DHCP servers, thus enhancing network security and stability.

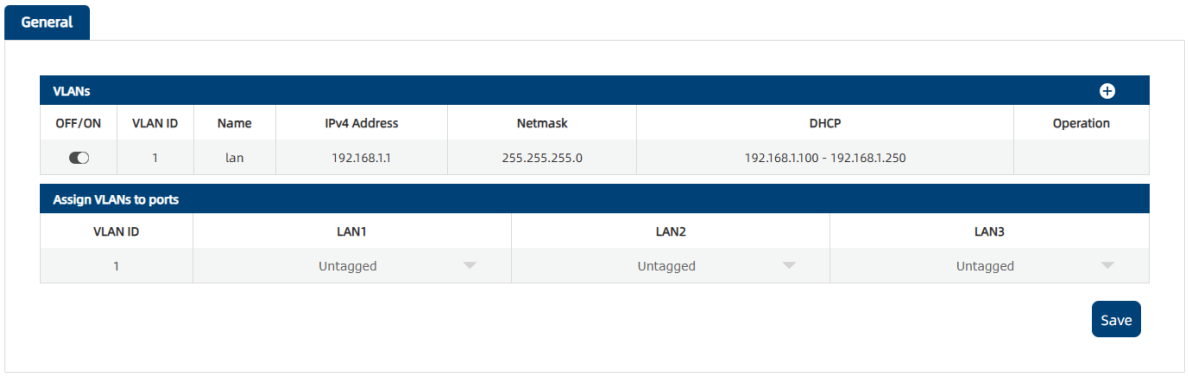
Queclink Confidential

4.2.5 VLAN

A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group. A VLAN, like the LAN it sits atop, operates at Layer 2 of the network, the Ethernet level. VLANs partition a single switched network into a set of overlaid virtual networks that can meet different functional and security requirements.

This section describes how to configure VLAN in a router.

On the general page, you can see the overview of the current VLAN setting. By default, the system comes with a VLAN (ID 1), and all LAN ports of the router are in this VLAN by default. This VLAN cannot be deleted or changed.



You can create a new VLAN by clicking the  icon in the upper right corner of the table. A configuration window will then pop up, allowing you to configure the VLAN settings.

Queclink Confidential

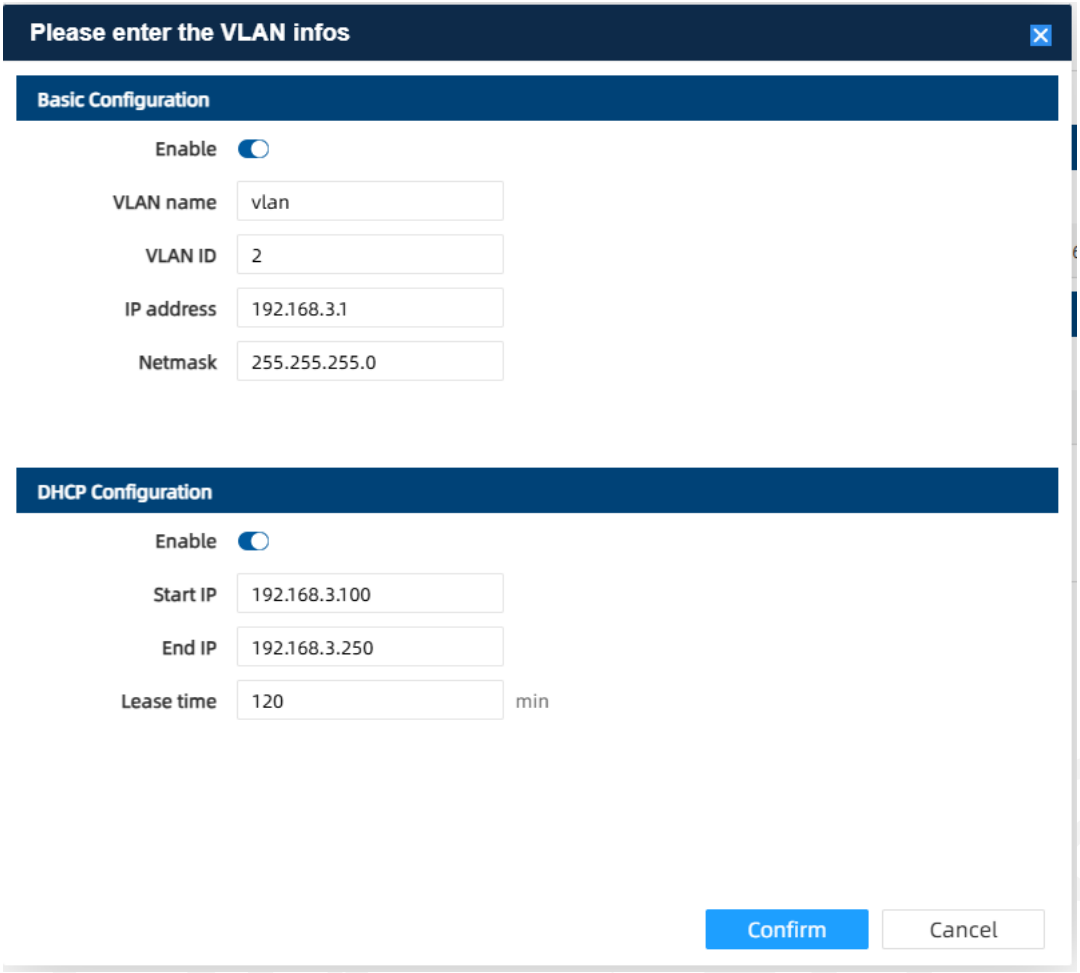
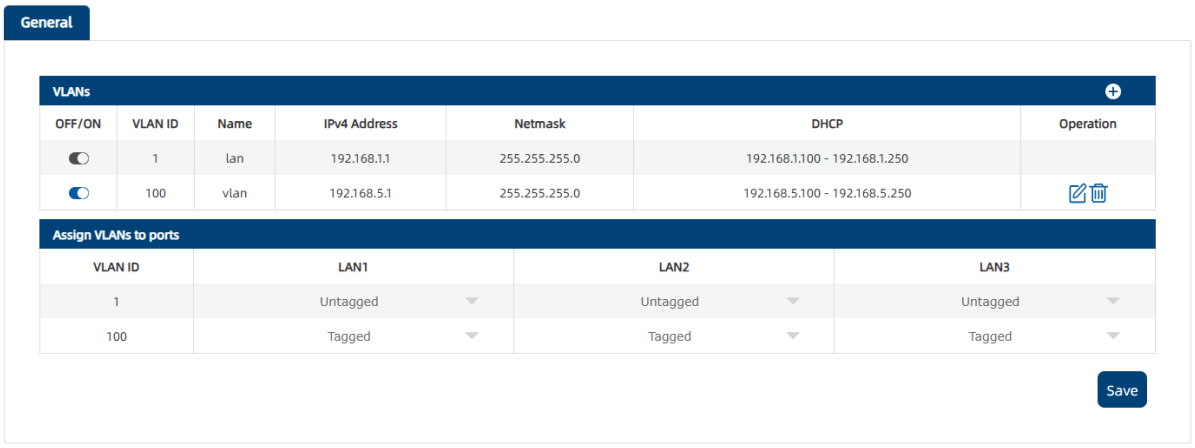


Table 18: VLAN Configuration Information

Field Name	Value	Description
Enable	yes|no; Default: no	To enable or disable this VLAN.
VLAN name	String	Name of this VLAN
VLAN ID	[1..4093]; default: none	VLAN Identification number.
IP address	ip; Default: none	The address of the VLAN.
Netmask	ip; Default: 255.255.255.255	A Mask that is applied to the Target to determine to what actual IP addresses the routing rule applies.

Click the “Confirm” button to confirm the VLAN settings. After that, this VLAN will appear on the general page.



You can assign any LAN port of the router to one VLAN by clicking the drop-down list in each cell. For each LAN port, you cannot configure more than one tagged or untagged setting at the same time.

Click the “Save” button in the lower corner to apply the settings.

4.2.6 WLAN

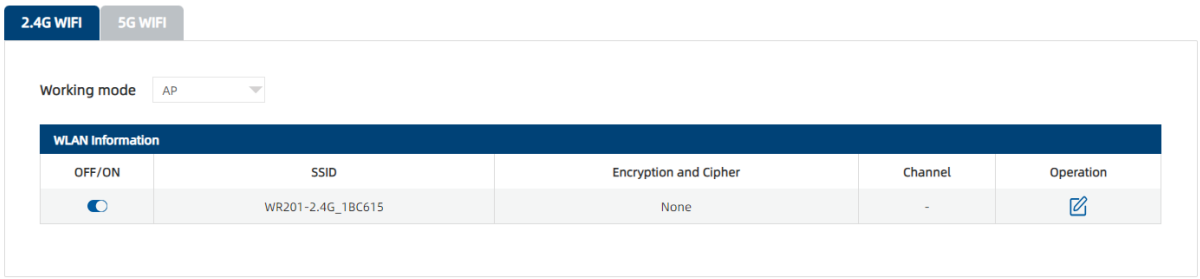
WR310 supports IEEE 802.11b/g/n/ac wireless technologies. 802.11ac is a hot new wireless technology that boasts faster and at longer ranges than 802.11n. 802.11ac works exclusively in the 5GHz band.

You can configure 2.4GHz and 5GHz Wi-Fi with different tabs. Both **Wireless** section of the Network tab can be used to manage and configure Wi-Fi Access Points (AP) and Wi-Fi Stations (STA).

You can select the Wi-Fi mode from the drop-down menu.

a) **Wireless Access Point:**

The page will display the overview of the Wireless Configuration. It displays all configured access points and stations. You can disable or enable the Wi-Fi interfaces, remove unwanted access points or stations or enter a configuration window of any Wi-Fi interface, where you can configure this interface more comprehensive. You can click the ‘edit’ button next to the Wi-Fi interface that you wish to configure to go to the configuration page.



You can configure a Wi-Fi channel according to the busyness of other channels. Use a channel with no other active Access Points and preferably one that has no active Access Point on two adjacent channels on each side as well or set the Channel field to auto and the device will pick the least busy channel in your location automatically. **SSID** is the name of your Wi-Fi interface. Wi-Fi client devices can scan the area for Wi-Fi networks they will see your network with this name. Hide SSID is used to make your Access Point invisible to other devices. To use a hidden Wi-Fi Access Point, first un-hide it, connect your device to it, then hide it again.

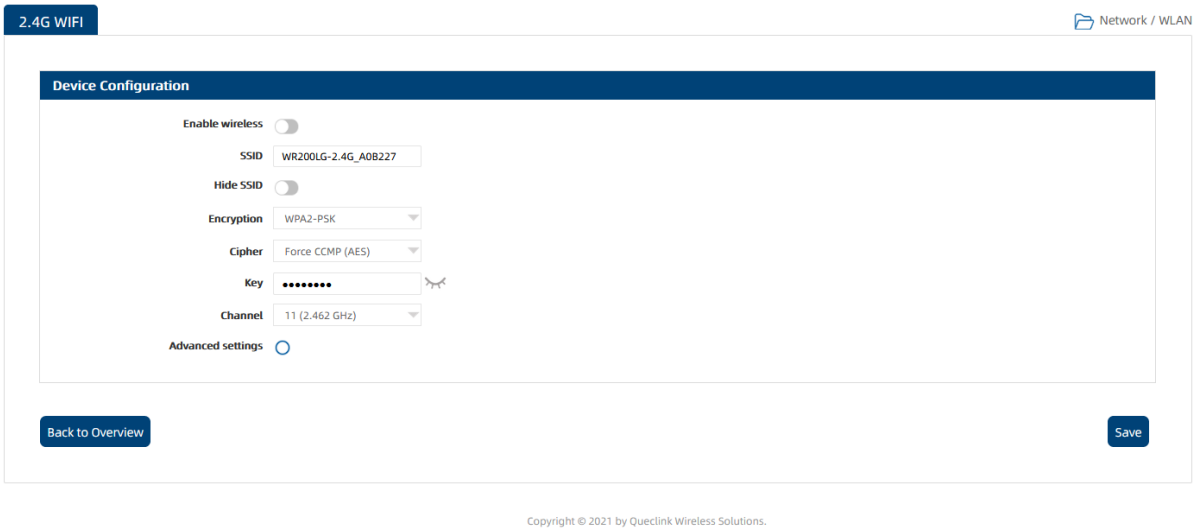


Table 19: Wireless Configuration

Field Name	Value	Description
Enable Wireless	yes|no; Default: no	To enable or disable this AP.
SSID	string; default: WR310-2.4G_(the last six digits of MAC)	Name of a Wi-Fi AP.
Hide SSID	yes|no; Default: no	Toggles to make your Access Point invisible to other devices. To use a hidden Wi-Fi Access Point, first un-hide it, connect your device to it, then hide it again.
Encryption	No encryption|WPA2-PSK|WPA-PSK/WPA2-PSK mixed mode; Default: No encryption	The type of Wi-Fi encryption used.
Cipher	Force CCMP (AES)|Force TKIP and CCMP (AES); Default: Force CCMP (AES)	An algorithm for performing encryption or decryption.
Key	string; default: none	Pre-shared key, a custom passphrase used for user authentication (at least 8 characters long).
Channel	1-13	Configure the channel of this Wi-Fi.

You can click “Advanced settings” button to display the advanced parameters. It is used to configure the hardware operating settings of the Wi-Fi radio. The settings available in this section are mostly used to find the best Wi-Fi performance conditions.

Queclink Confidential

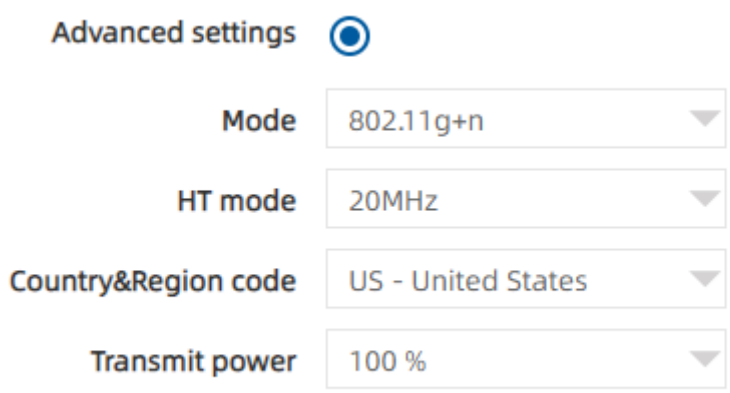


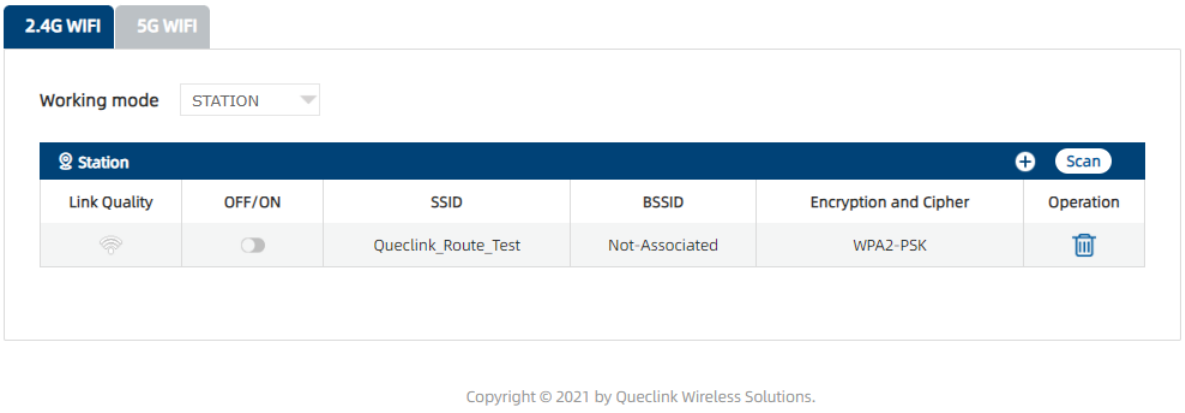
Table 20: Wi-Fi Advanced Settings

Field Name	Value	Description
Mode	802.11b|802.11g|802.11g+n; Default: 802.11g+n	Wireless protocol used. Different modes provide different wireless standard support which directly impacts the radio's throughput performance.
Country code	country code; Default: US	SO/IEC 3166 alpha2 country codes as defined in ISO 3166-1 standard.
Transmit power	100%|50%|25%|12%; Default: 100%	Wi-Fi signal power. Use lower power to reduce the device's CPU usage.

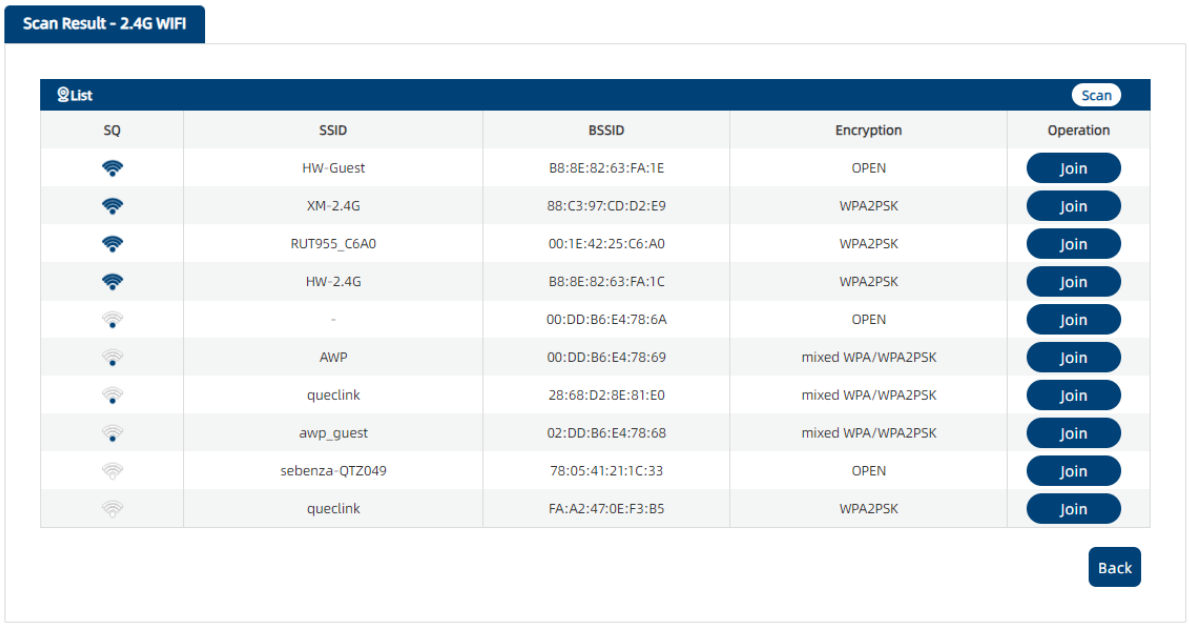
b) **Wireless Station:**

WR310 can also work as a Wi-Fi client.

You can click 'Connect' button to connect with an existing access point. Click Scan button to rescan the surrounding area and try to connect to a new wireless access point.



Once the scan is complete, you will see a list of Wi-Fi Access Points. Select the one you prefer and click the Join button next to it, enter the password to connect to that access point.



4.2.7 Routing

4.2.7.1 Static

Static routes specify over which interface and gateway a certain host or network can be reached. You can configure your own custom routes in this page. You can configure multi static route in the device.

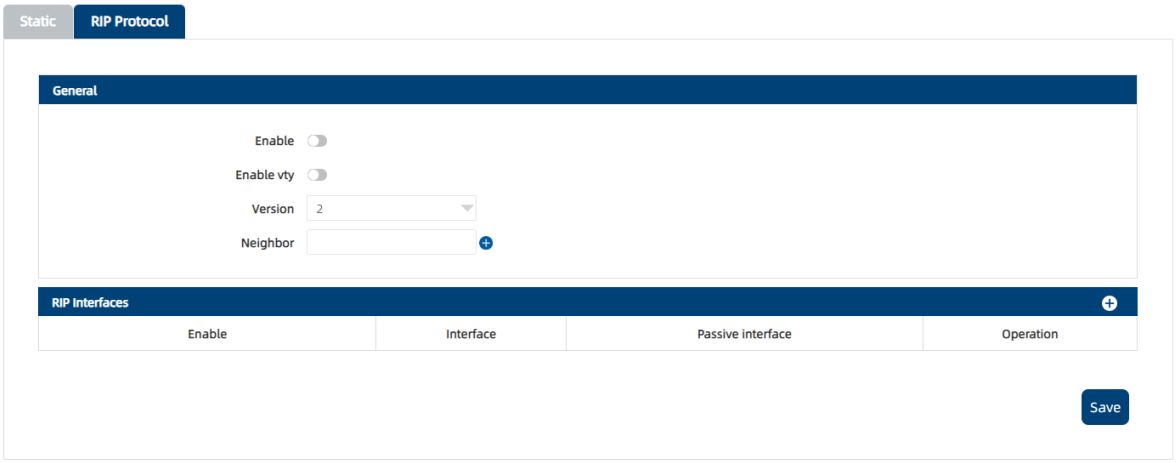


Table 21: Static Route Configuration

Field Name	Value	Description
Interface	WAN|Mobile|Wifi2.4G|Wifi5G; Default: WAN (Wired)	The zone where the target network resides.
Destination subnet IP address	ip; Default: 0.0.0.0	The address of the destination network.
Netmask	ip; Default: 255.255.255.255	A Mask that is applied to the Target to determine to what actual IP addresses the routing rule applies.
Gateway	ip; Default: none	Defines where the device should send all the traffic that applies to the rule.
Metric	integer; default: none	The Metric value is used as a sorting measure. If a packet about to be routed fits two rules, the one with the higher metric is applied.

4.2.7.2 RIP

The **Routing Information Protocol (RIP)** is a distance-vector routing protocols which employ the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. A hop count over 16 is considered an infinite distance and the route is unreachable.



You can click 'Add' button to a new RIP interface and click 'Save' button to save the configuration.

Table 22: RIP Configuration

Field Name	Value	Description
Enable	yes|no; Default: no	Toggles RIP Protocol ON or OFF.
Enable vty	yes|no; Default: no	Toggles vty access from LAN ON or OFF.
Version	2|1; Default: 2	Specifies the version of RIP.
Neighbor	ip; Default: " "	Neighbour IP address.
Enable	yes|no; Default: no	Toggles RIP Interface ON or OFF.
Interface	network interface; Default: br-lan	Network interface to be used with the RIP interface.
Passive interface	yes|no; Default: no	Sets the specified interface to passive mode. On passive mode interface, all receiving packets are processed as normal and RIP does not send either multicast or unicast RIP packets.

4.2.8 Firewall

4.2.8.1 NAT

Network Address Translation (NAT) is a process in which one or more local IP addresses are translated into one or more global IP address (SNAT) and vice versa in order to provide Internet access to the local hosts (DNAT). Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table.

The device supports both SNAT (Source NAT) and DNAT (Destination NAT). You can Click Add icon to add a new instance and can configure the setting in the corresponding section. You need to Click Save button to save all parameters you configured.

Queclink Confidential

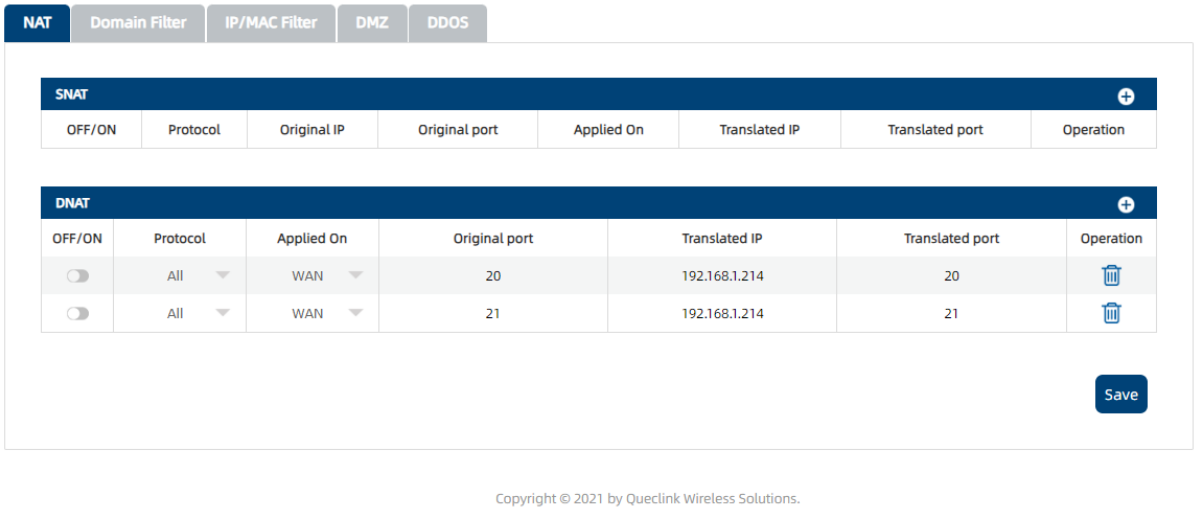


Table 23: NAT Configuration

Field Name	Value	Description
OFF/ON	ON|OFF	To turn on/off the section.
Protocol	ALL|TCP|UDP|ICMP|TCP+UDP Default: ALL	Select the protocol to translate the IP and Port.
Original IP	A.B.C.D	The initial IP address to be translated.
Original Port	1~65535	The initial port to be translated.
Applied On	LAN|WAN|PPTP|L2TP|OPENVPN|GRE default: WAN	The translated source zone.
Translated IP	A.B.C.D	The translated IP address.
Translated Port	1~65535	The translated port.

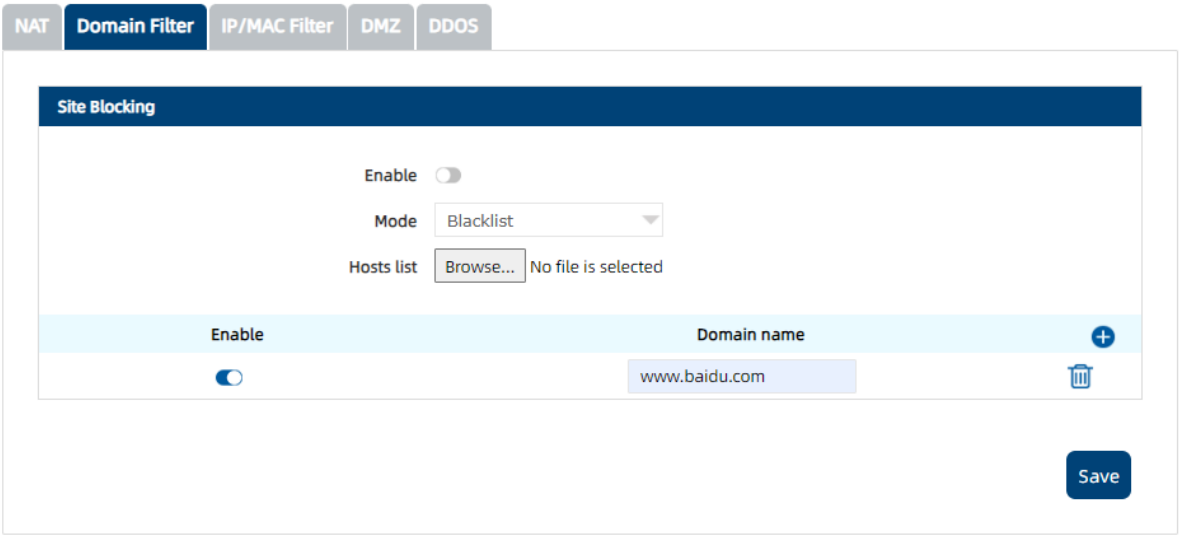
Table 24: Port Forwarding Configuration

Field Name	Value	Description
OFF/ON	ON|OFF	To turn on/off the section.
Protocol	ALL|TCP|UDP|ICMP|TCP+UDP Defaule:ALL	Select the protocol to translate the IP and Port.
Applied On	WAN|PPTP|L2TP|OPENVPN|GRE Default:WAN	The destination zone of the section.
Original port	1~65535	The initial port to be translated.
Translated IP	A.B.C.D	The translated IP address.
Translated port	1~65535	The translated port.

4.2.8.2 Domain Filter

The domain filter function provides you with the possibility to set up lists of wanted or unwanted websites (Blacklists or Whitelists). If the mode is whitelist, the device allows every site included in the list and blocks everything else. If the mode is Blacklist, the device blocks every site included in the list and allows everything else.

Queclink Confidential



Copyright © 2021 by Queclink Wireless Solutions.

Table 25: Domain Filter Configuration

Field Name	Value	Description
Enable	yes|no; Default: no	Turns Site Blocking on or off.
Mode	Blacklist|Whitelist; Default: Blacklist	Mode of operation. • Whitelist - allow every site included in the list and block everything else. • Blacklist - block every site included in the list and allow everything else.
Domain name	host; Default: none	Website name or IP address. The formats accepted are either www.website.com or website.com, i.e., the protocol and subdomains can be not specified. The rules will also be applicable for the subdomains of the specified site.

4.2.8.3 IP/MAC Filter

The domain filter function provides you an easy way to set up lists of blocking or unblocking client base on IP/MAC address. If the mode is whitelist, the device allows every IP/MAC address included in the list and blocks everything else. If the mode is Blacklist, the device blocks every IP/MAC address included in the list and allows everything else.

Queclink Confidential

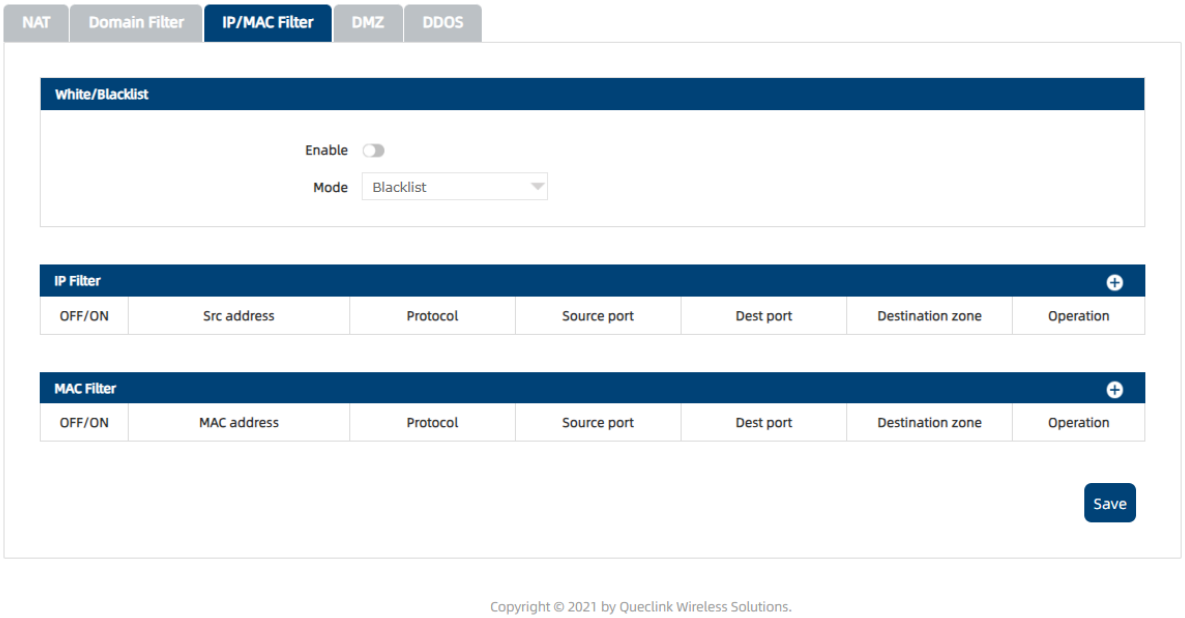


Table 26: IP/MAC Filter Configuration

Field Name	Value	Description
Enable	yes|no; Default: no	Turns Client Blocking on or off.
Mode	Blacklist|Whitelist; Default: Blacklist	Mode of operation. • Whitelist - allow every IP/MAC address included in the list and block everything else. • Blacklist - block every IP/MAC address included in the list and allow everything else.
Src address	ip; Default: 0.0.0.0	The IP address of client to be configured.
MAC address	mac; Default: none	The MAC address of client to be configured.
Protocol	All|TCP|UDP|TCP+UDP|ICMP; Default: All	Specifies the protocol to blocked/unblock.
Source Port	integer [0..65535]; default: none	TCP/UDP port number. Note: traffic on the selected port will be automatically allowed in the device's firewall rules.
Dest Port	integer [0..65535]; default: none	TCP/UDP port number. Note: traffic on the selected port will be automatically allowed in the device's firewall rules.
Destination zone	WAN|PPTP|L2TP|OPENVPN|GRE	Interface to block/unblock this IP/MAC address.

4.2.8.4 DMZ

A DMZ (Demilitarized Zone) is a perimeter network that enables organizations to protect their internal networks. It enables organizations to provide access to untrusted networks, such as the internet, while keeping private networks or local-area networks (LANs) secure.

By enabling DMZ for a specific internal host, you will expose that host and its services to the external network.

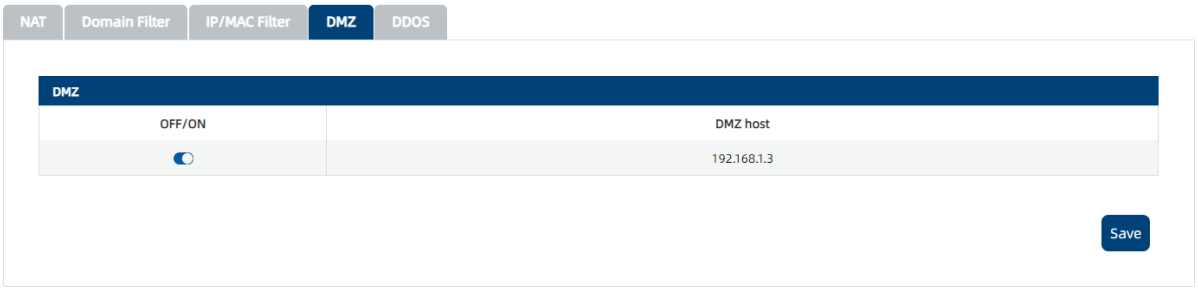
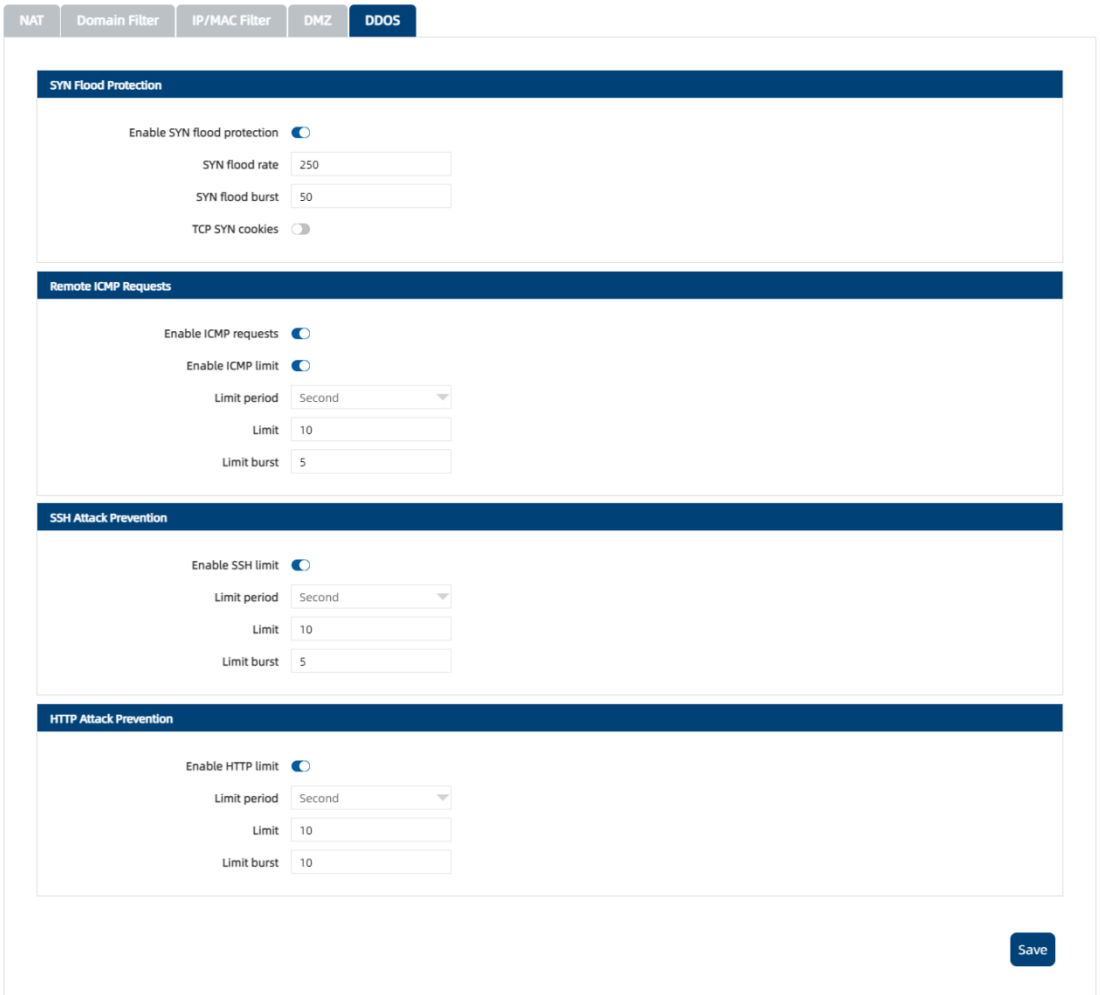


Table 27: DMZ Configuration

Field Name	Value	Description
OFF/ON	yes|no; Default: no	Toggles DMZ On or Off.
DMZ host	ip; Default: “ “	Internal host to which the DMZ rule will be applied.

4.2.8.5 DDOS

The DDOS Prevention page allows you to set up protections from various types of DDOS attacks. You will find information on all of these methods below.



SYN Flood Protection:

SYN Flood Protection allows you to protect yourself from attacks that exploit part of the normal TCP three-way

handshake to consume resources on the targeted server and render it unresponsive. Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network over-saturation.

Remote ICMP Requests:

Some attackers use ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. You can set up some custom restrictions to help protect your device from ICMP bursts.

SSH Attack Prevention:

Prevent SSH (allows a user to run commands on a machine's command prompt without them being physically present near the machine) attacks by limiting connections in a defined period.

HTTP Attack Prevention:

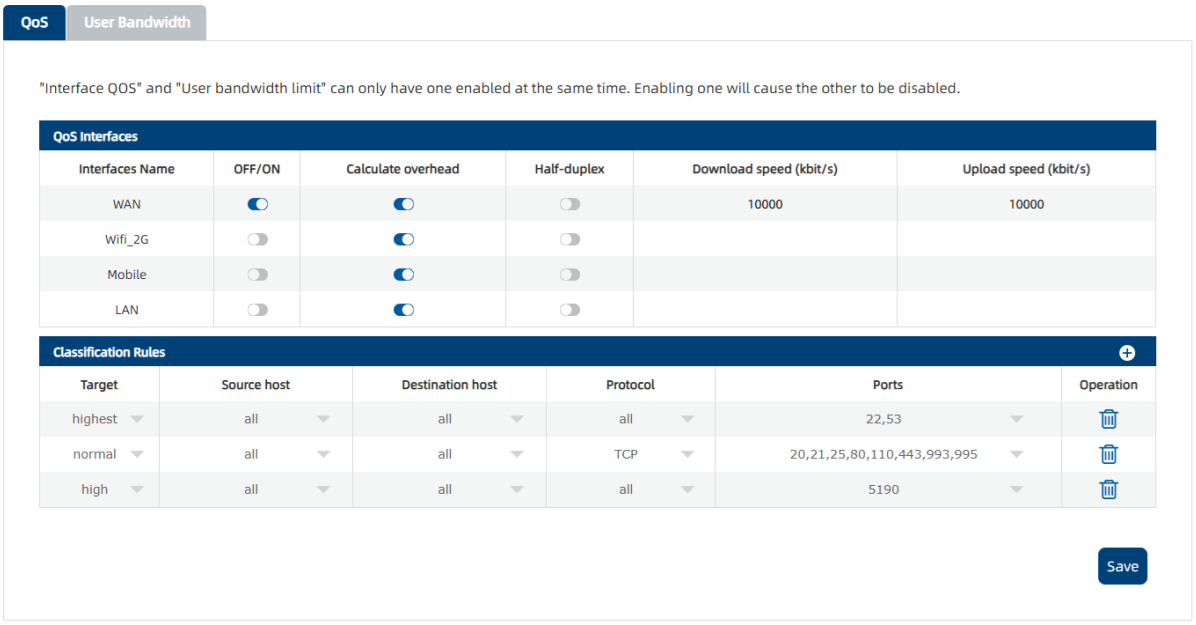
An HTTP attack sends a complete, legitimate HTTP header, which includes a 'Content-Length' field to specify the size of the message body to follow. However, the attacker then proceeds to send the actual message body at an extremely slow rate (e.g. 1 byte/100 seconds). Due to the entire message being correct and complete, the target server will attempt to obey the 'Content-Length' field in the header, and wait for the entire body of the message to be transmitted, hence slowing it down.

4.2.9 QoS

QoS provides the way to prioritize network traffic based on interfaces, hosts or services and limit download & upload speeds of each user.

4.2.9.1 QoS

QoS has two sections: QoS Interfaces and Classification Rules.



The Interfaces section is used to set up download and upload speed limits on the device's network interfaces.

Table 28: QoS Configuration

Field Name	Value	Description
Protocol	TCP|UDP|MQTT; default: TCP	Protocol that will be used to send NMEA data.
Interface Name	WAN|Wifi_2G|Mobile|LAN	Interface to which the rule applies.
OFF/ON	yes | no; default: no	Turns the rule on or off.
Calculate overhead	yes | no; default: no	Decreases upload and download ratio to prevent link saturation.
Half-duplex	yes | no; default: no	Enable half-duplex mode.
Download speed (kbit/s)	integer; default: none	Maximum download speed for the specified interface.
Upload speed (kbit/s)	integer; default: none	Maximum upload speed for the specified interface.

The Classification Rules section is used to configure rules that prioritize certain traffic over other, less important traffic. This traffic can be defined by a source or destination host, port, or a network protocol. Traffic that matches a rule with higher preference will be handled with higher priority.

Table 29: QoS Traffic Rule Configuration

Field Name	Value	Description
Target	Priority | Express | Normal | Low; default: Normal	Defines the priority of traffic defined in this rule.
Source host	All | IP; default: All	Host(s) from which data will be transmitted.
Destination host	All | IP; default: All	Host(s) to which data will be transmitted.
Protocol	All | TCP | UDP | ICMP | – custom –; default: All	Protocol to match the rule.
Ports	All | integer [0..65535]; default: none	Port numbers to match the rule. You can enter multiple ports by separating them by commas (e.g., 22,53,80).
Number of bytes	integer; default: none	Maximum number of bytes for this connection.

4.2.9.2 User Bandwidth

User Bandwidth provides the possibility to control the bandwidth of each user. The network speed for all users corresponding to the interfaces will not exceed the configured speed rate.

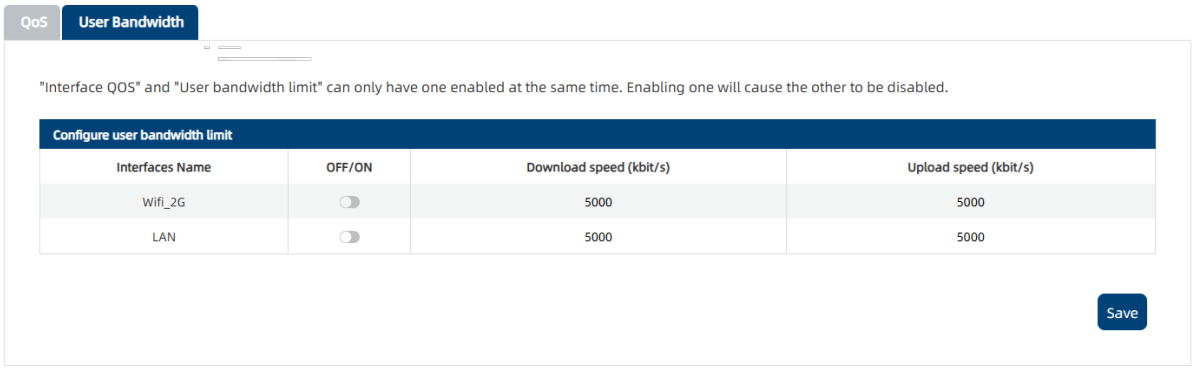


Table 30: QoS Interface Speed Configuration

Field Name	Value	Description
Download speed (kbit/s)	integer; default: none	Maximum download speed for all users connected to this interface.
Upload speed (kbit/s)	integer; default: none	Maximum upload speed for all users connected to this interface.

4.3 Applications

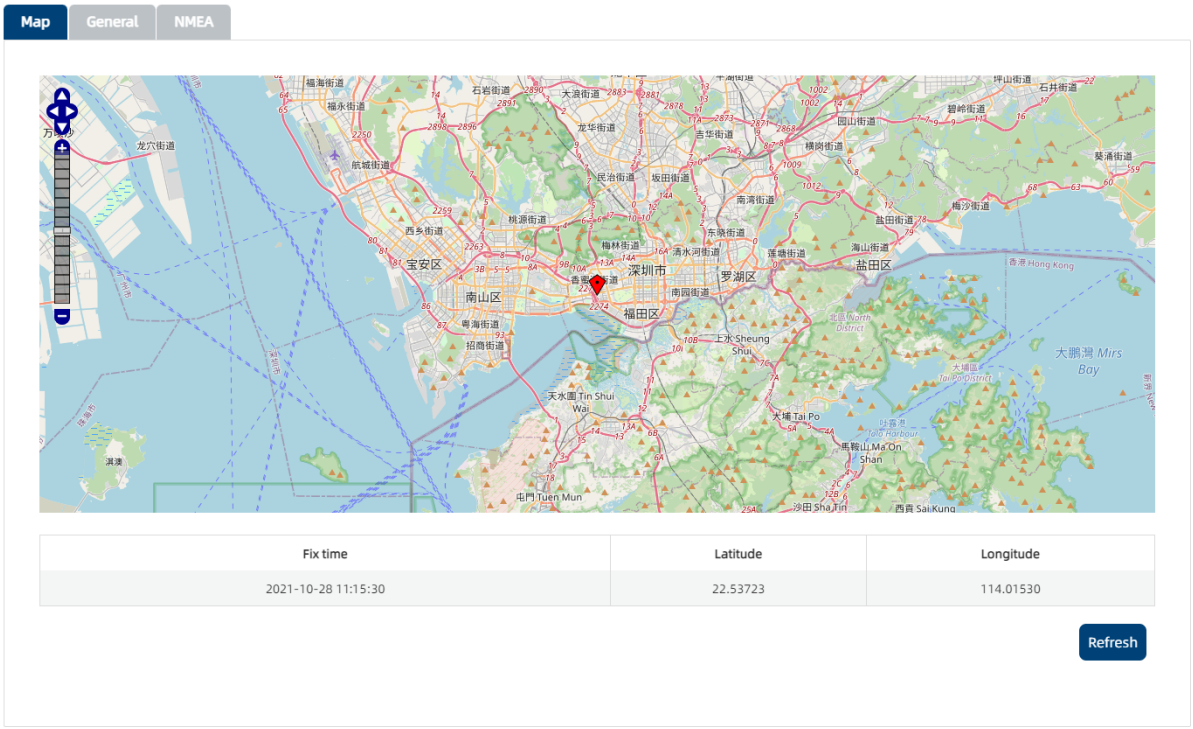
This section shows you how to configure the service applications of the device.

4.3.1 GPS (Available for some Models Only)

4.3.1.1 Map

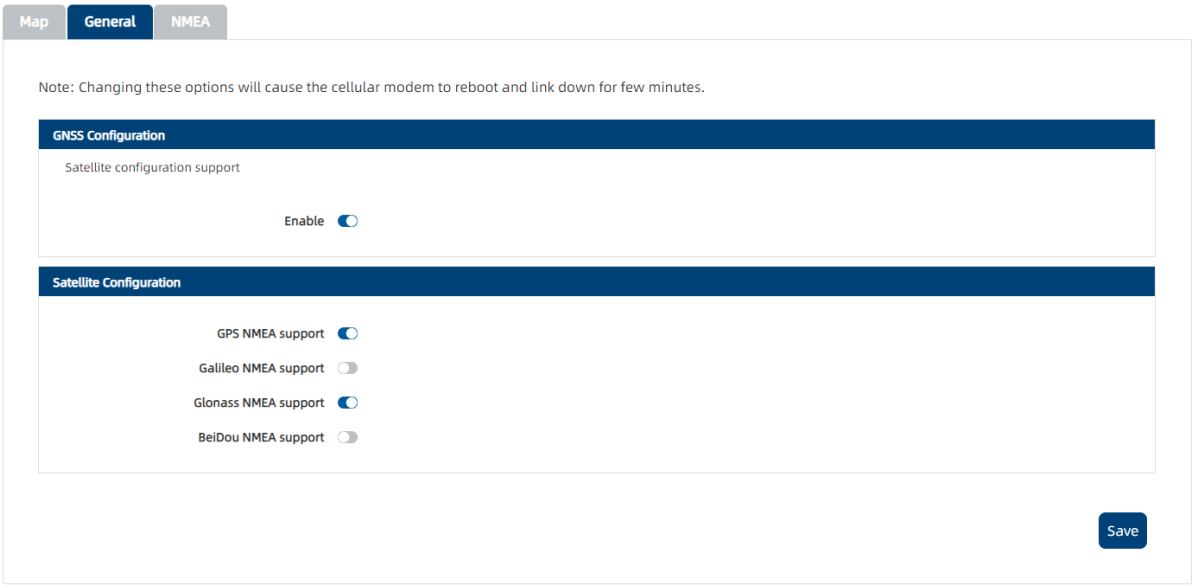
The **Global Positioning System** (**GPS**) is a space-based radio navigation system.

The **Map** page displays the device's current coordinates and position on the map. To have the device's location on the map, make sure to attach the GPS antenna on the device and place it outdoors, and GPS is enabled in the general page.



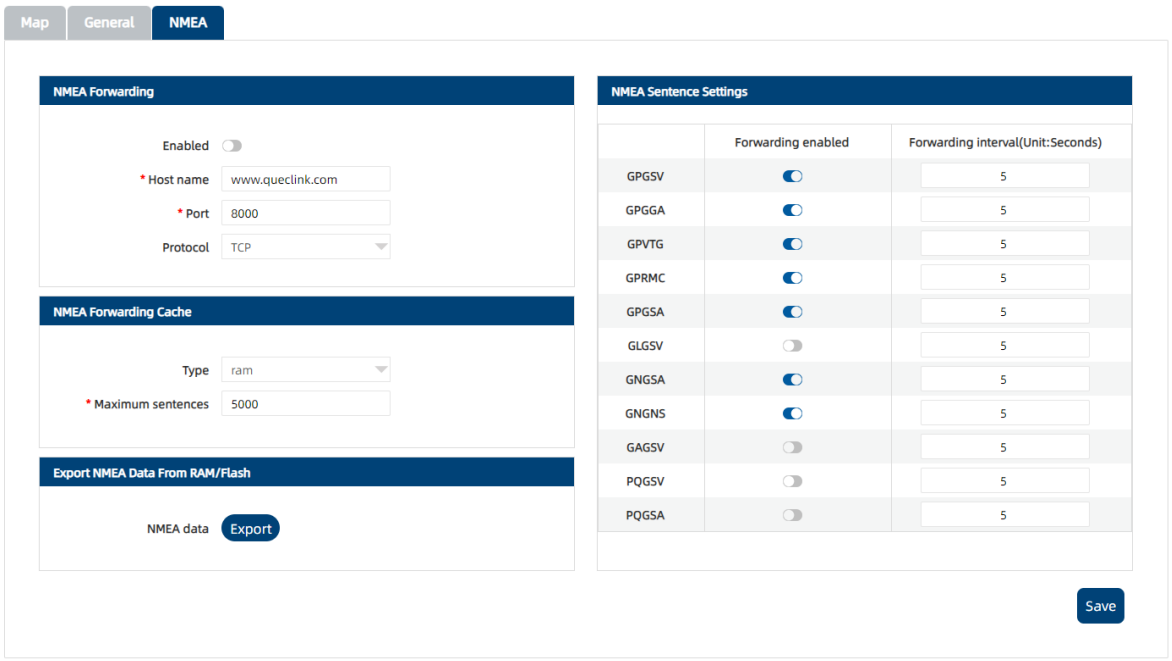
4.3.1.2 General

The **General** section is used to enable the GPS service based on different types of satellite. Once you turn on GPS, you can check the Map page in order to see if the device has obtained a GPS fix. Make sure to attach the GPS antenna on the device and place it outdoors where it can get GPS signal, otherwise, the device may not be able to obtain a GPS fix.



4.3.1.3 NMEA

The **NMEA forwarding** section is used to configure and enable NMEA forwarding to a server filled in the hostname. NMEA is a standard data format supported by all GPS manufacturers, much like ASCII is the standard for digital computer characters in the computer world.



Copyright © 2021 by Queclink Wireless Solutions.

Table 31: NMEA Forwarding Configuration

Field Name	Value	Description
Protocol	TCP|UDP|MQTT; default: TCP	Protocol that will be used to send NMEA data.
Host name	ip|host; default: 192.168.1.5	IP address or hostname of the server to which NMEA data will be forwarded.
Port	integer [0..65535]; default: 8500	Port number of the server to which NMEA data will be forwarded.

The device caches NMEA forwarding information if NMEA forwarding is enabled. This section is used to select the memory type where the cache will be stored and the maximum amount of data that will be saved.

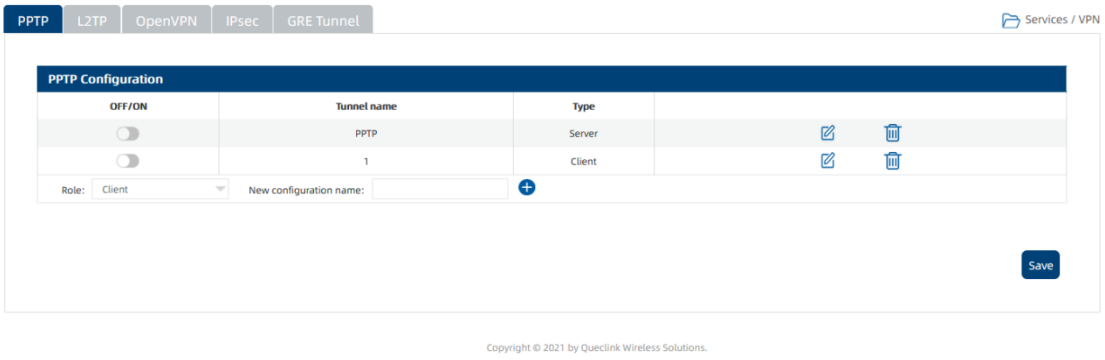
The NMEA sentence settings section provides the possibility to configure which NMEA sentences will be forwarded or collected and at specified period.

4.3.2 VPN

A virtual private network (VPN), is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. The device provides multiple VPN functions, which can be applied in different industries and application.

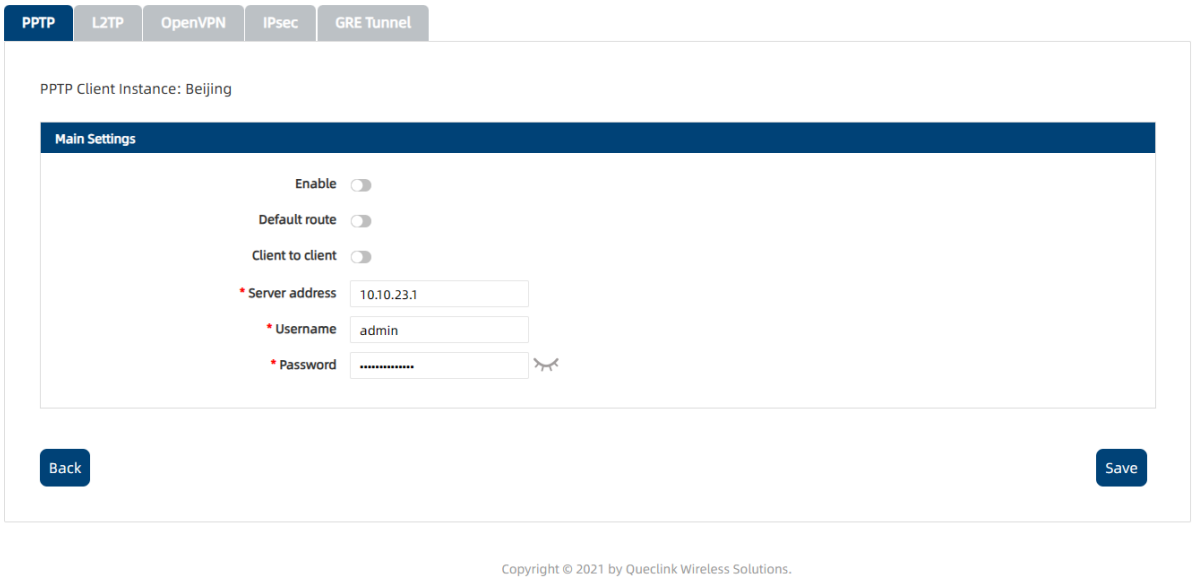
4.3.2.1 PPTP

Point-to-Point Tunneling Protocol (**PPTP**) is a type of VPN protocol that uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.



PPTP client:

A **PPTP client** is an entity that initiates a connection to a PPTP server. Select Role as Client, enter a custom name and click the Add icon to create a new client instance, then click Edit icon to go to PPTP client configuration page. You can click Edit button on the right to edit an existing PPTP instance.



Refer to the figure and table below for information on the PPTP client's configuration fields:

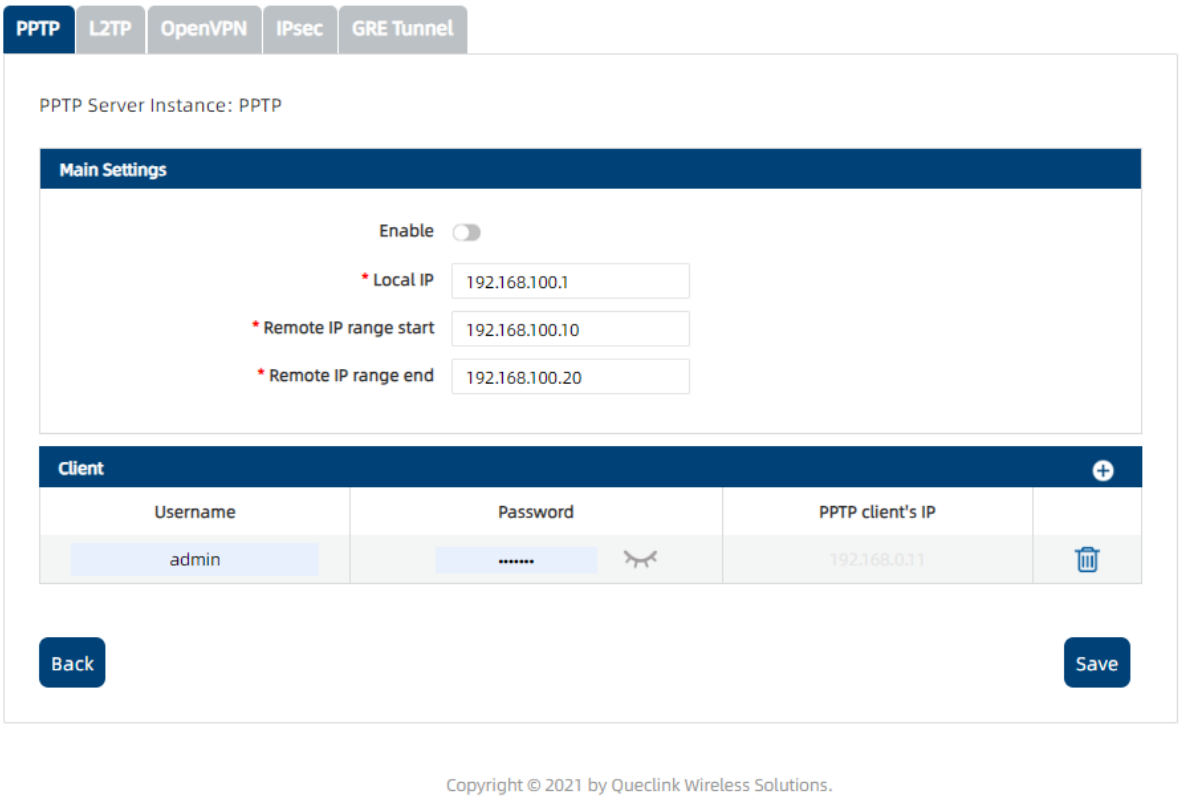
Table 32: PPTP Configuration

Field Name	Value	Description
Enable	yes|no; default: no	Turns the PPTP instance on or off.
Default route	yes|no; default: no	When turned on, this connection will become the device's default route. This means that all traffic directed to the Internet will go through the PPTP server and the server's IP address will be seen as this device's source IP to other hosts on the Internet. Note: this can only be used when WAN Failover is turned off.
Client to client	yes|no; default: no	Adds a route that makes other PPTP clients accessible within the PPTP network.
Server address	ip|host; default: none	IP address or hostname of a PPTP server.
Username	string; default: none	Username used for authentication to the PPTP server.
Password	string; default: none	Password used for authentication to the PPTP server.

PPTP server:

A **PPTP server** is an entity that waits for incoming connections from PPTP clients. To create a new server instance, select Role as Server, enter a custom name and click the Add icon to create a new server instance, then click Edit icon go to PPTP server configuration page. You can click Edit button to edit an existing PPTP instance. Only one PPTP server instance is allowed to be added. A server needs to have a public IP address in order to be available from the public network (the Internet).

Queclink Confidential



Refer to the figure and table below for information on the PPTP client's configuration fields:

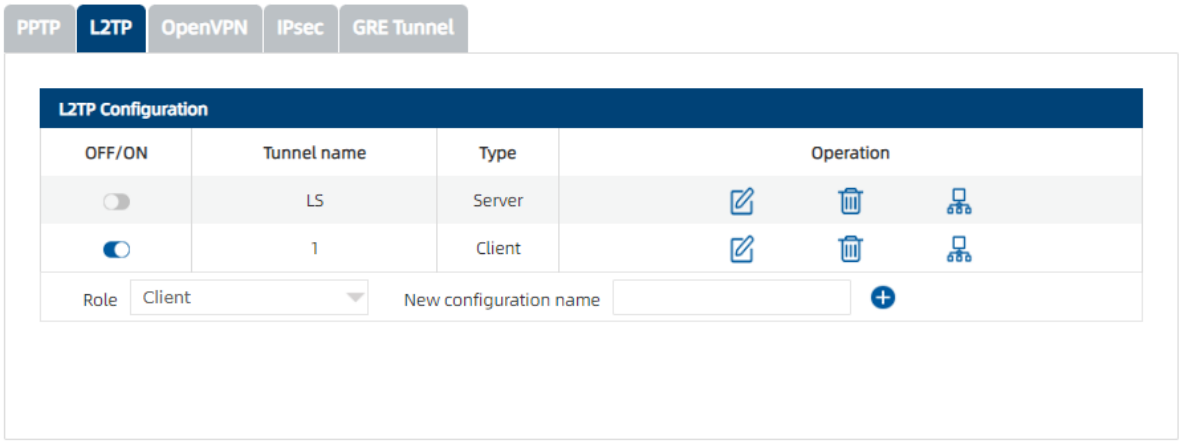
Table 33: PPTP Server Configuration

Field Name	Value	Description
Enable	yes|no; default: no	Turns the PPTP instance on or off.
Local IP	ip; default: 192.168.0.1	IP address of this PPTP network interface.
Remote IP range start	ip; default: 192.168.0.20	PPTP IP address leases will begin from the address specified in this field.
Remote IP range end	ip; default: 192.168.0.30	PPTP IP address leases will end with the address specified in this field.
Username	string; default: WR310	Username used for authentication to this PPTP server.
Password	string; default: queclink	Password used for authentication to this PPTP server.
PPTP Client's IP	ip; default: none	Assigns an IP address to the client that uses the adjacent authentication info. This field is optional and if left empty the client will simply receive an IP address from the IP pool defined above.

4.3.2.2 L2TP

Layer 2 Tunneling Protocol (**L2TP**) is a tunneling protocol used to support virtual private networks (VPNs). It can work as client or server mode.

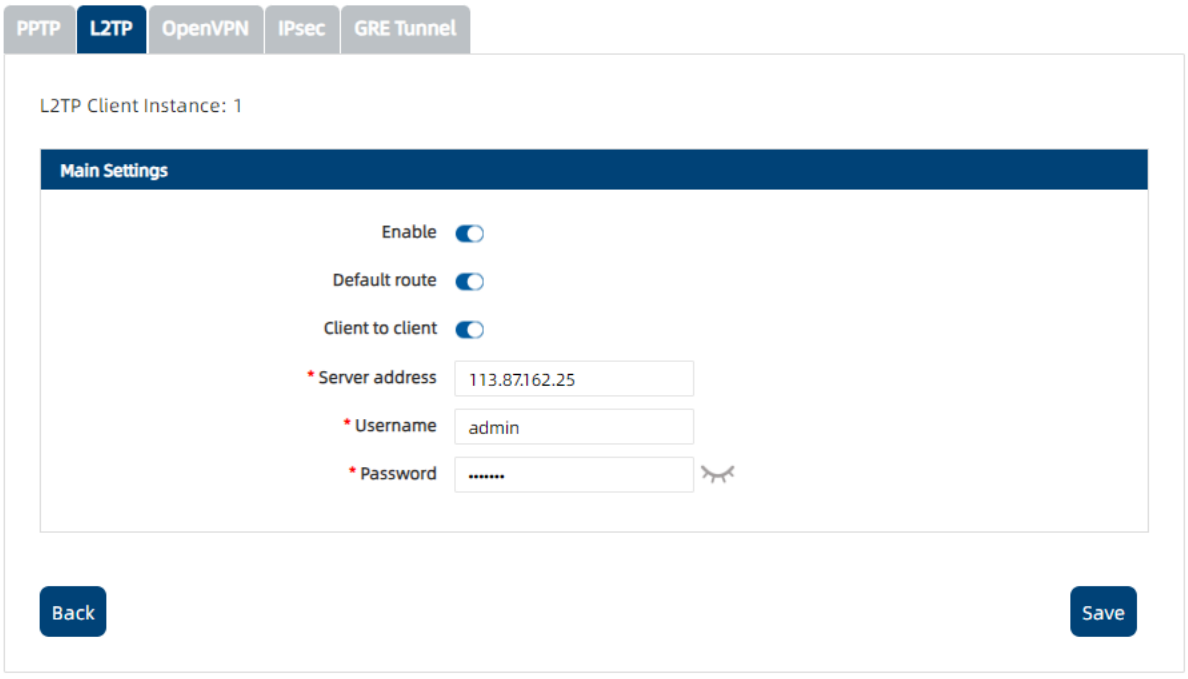
Queclink Confidential



Copyright © 2021 by Queclink Wireless Solutions.

L2TP client:

An L2TP client is an entity that initiates a connection to an L2TP server. To create a new client instance, select Role as Client, enter a custom name and click the Add icon to create a new instance, then click Edit icon to go to L2TP client configuration page. You can click Edit icon on the right to edit an existing L2TP instance.



Copyright © 2021 by Queclink Wireless Solutions.

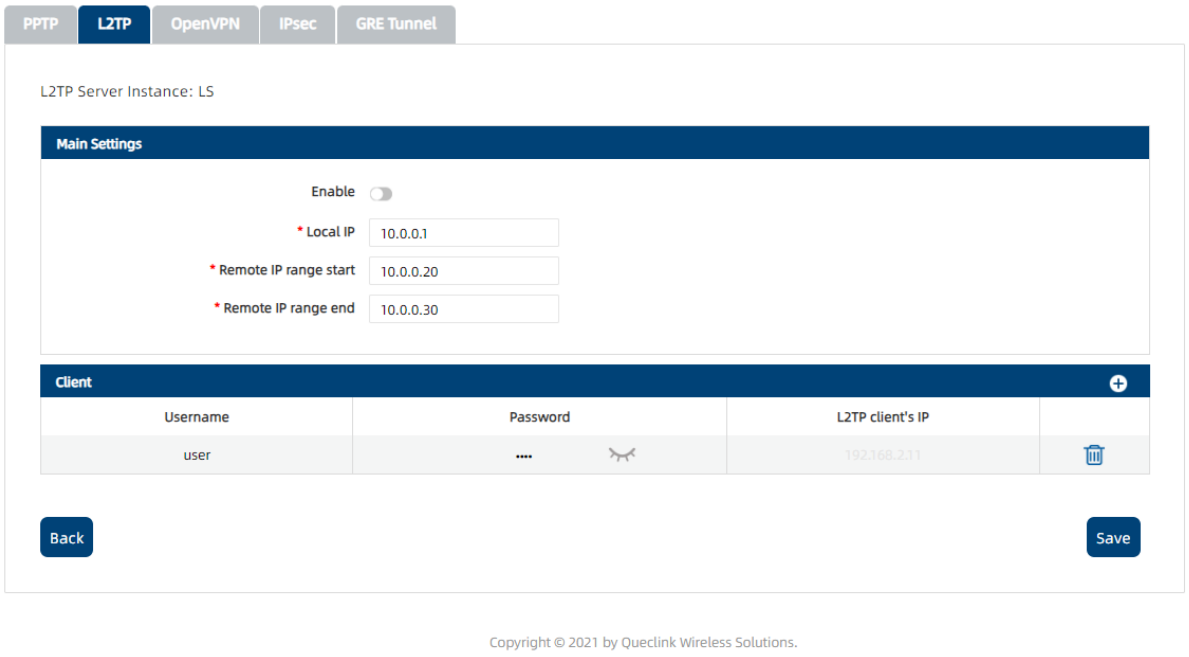
Refer to the figure and table below for information on the L2TP client's configuration fields:

Table 34: L2TP Client Configuration

Field Name	Value	Description
Enable	yes|no; default: no	Turns the L2TP instance on or off.
Server address	ip|host; default: none	IP address or hostname of an L2TP server.
Username	string; default: none	Username used for authentication to the L2TP server.
Password	string; default: none	Password used for authentication to the L2TP server.
Default route	yes|no; default: no	When turned on, this connection will become the device's default route. This means that all traffic directed to the Internet will go through the L2TP server and the server's IP address will be seen as this device's source IP to other hosts on the Internet. Note: this can only be used when WAN Failover is turned off.
Client to client	yes|no; default: no	Adds a route that makes other L2TP clients accessible within the L2TP network.

L2TP server:

An **L2TP server** is an entity that waits for incoming connections from L2TP clients. To create a new server instance, select Role as Server, enter a custom name and click the Add icon to go to L2TP server configuration page. You can click Edit icon to edit an existing L2TP instance. Only one L2TP server instance is allowed to be added. A server needs to have a public IP address in order to be available from the public network (the Internet).



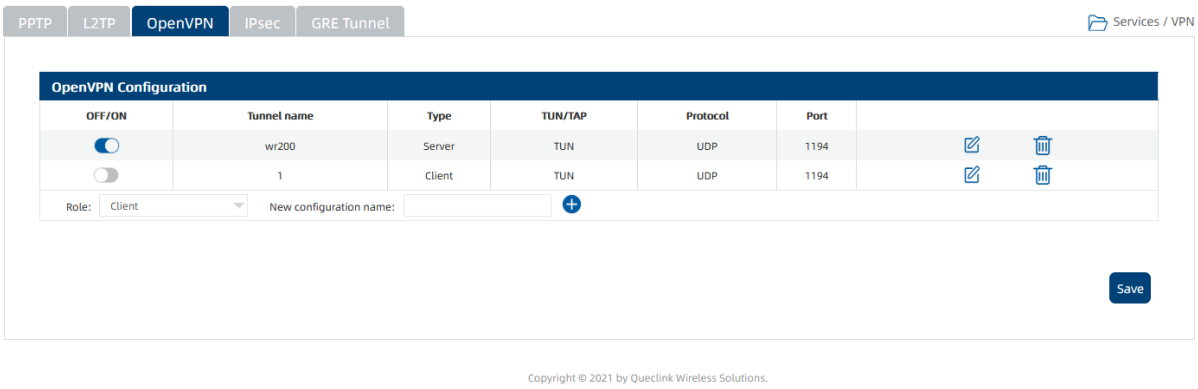
Refer to the figure and table below for information on the L2TP client's configuration fields:

Table 35: L2TP Server Configuration

Field Name	Value	Description
Enable	yes|no; default: no	Turns the L2TP instance on or off.
Local IP	ip; default: 192.168.0.1	IP address of this L2TP network interface.
Remote IP range start	ip; default: 192.168.0.20	L2TP IP address leases will begin from the address specified in this field.
Remote IP range end	ip; default: 192.168.0.30	L2TP IP address leases will end with the address specified in this field.
Username	string; default: user	Username used for authentication to this L2TP server.
Password	string; default: pass	Password used for authentication to this L2TP server.
L2TP Client's IP	ip; default: none	Assigns an IP address to the client that uses the adjacent authentication info. This field is optional and if left empty the client will simply receive an IP address from the IP pool defined above.

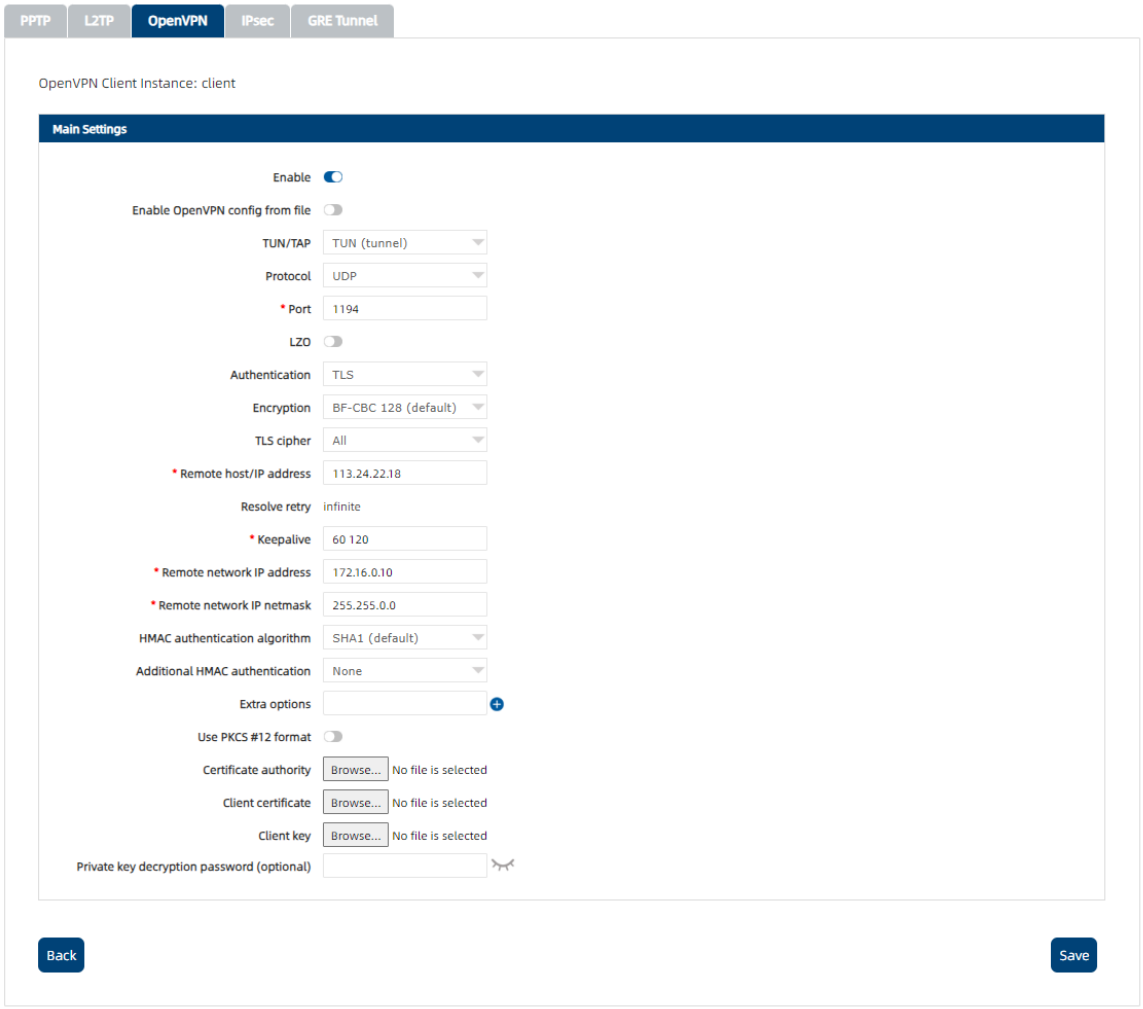
4.3.2.3 OPENVPN

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It is often regarded as being the most universal VPN protocol because of its flexibility, support of SSL/TLS security, multiple encryption methods, many networking features and compatibility with most OS platforms.



OpenVPN client:

An OpenVPN client is an entity that initiates a connection to an OpenVPN server. To create a new client instance, select Role as Client, enter a custom name and click the Add icon to go to OpenVPN client configuration page. You can click Edit icon on the right to edit an existing OpenVPN instance. A maximum of six OpenVPN client instances are allowed to be added.



Field Name	Value	Description
Enable	yes|no; default: no	Turns the OpenVPN instance on or off.
Enable OpenVPN config from file	yes|no; default: no	Enables custom OpenVPN configuration from file.
TUN/TAP	TUN (tunnel)|TAP (bridged); default: TUN (tunnel)	Virtual network device type. • TUN - a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required. • TAP - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.

continues on next page

Table 36 – continued from previous page

Field Name	Value	Description
Protocol	UDP|TCP; default: UDP	Transfer protocol used for the OpenVPN connection. Transmission Control Protocol (TCP) - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analysing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, in file transfer). User Datagram Protocol (UDP) - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, in video streaming, live calls).
Port	integer [0..65535]; default: 1194	TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. NOTE: traffic on the selected port will be automatically allowed in the device's firewall rules.
LZO	yes|no; default: no	Turns LZO data compression on or off.
Authentication	TLS|Static Key|Password|TLS/Password; default: TLS	Authentication mode, used to secure data sessions. Static key is a secret key used for server-client authentication. TLS authentication mode uses X.509 type certificates: • Certificate Authority (CA) • Client certificate • Client key All mentioned certificates can be generated using OpenVPN or Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called Easy-RSA. Password is a simple username/password based authentication where the owner of the OpenVPN server provides the login data. TLS/Password uses both TLS and username/password authentication.
Encryption	DES-CBC 64|RC2-CBC 128|DES-EDE-CBC 128|DES-EDE3-CBC 192|DESX-CBC 192|RC2-40-CBC 40|CAST5-CBC 128|RC2-64-CBC 64|AES-128-CBC 128|AES-192-CBC 192|AES-256-CBC 256|none ; default: BF-CBC 128	Algorithm used for packet encryption.
TLS: TLS cipher	All|DHE+RSA|Custom; default: All	Packet encryption algorithm cipher.
TLS: Allowed TLS ciphers	All|DHE+RSA|Custom; default: All	A list of TLS ciphers accepted for this connection.
Remote host/IP address	ip; default: none	IP address or hostname of an OpenVPN server.
Resolve retry	integer|infinite; default: infinite	In case server hostname resolve fails, this field indicates the amount of time (in seconds) to retry the resolve. Specify infinite to retry indefinitely.

continues on next page

Table 36 – continued from previous page

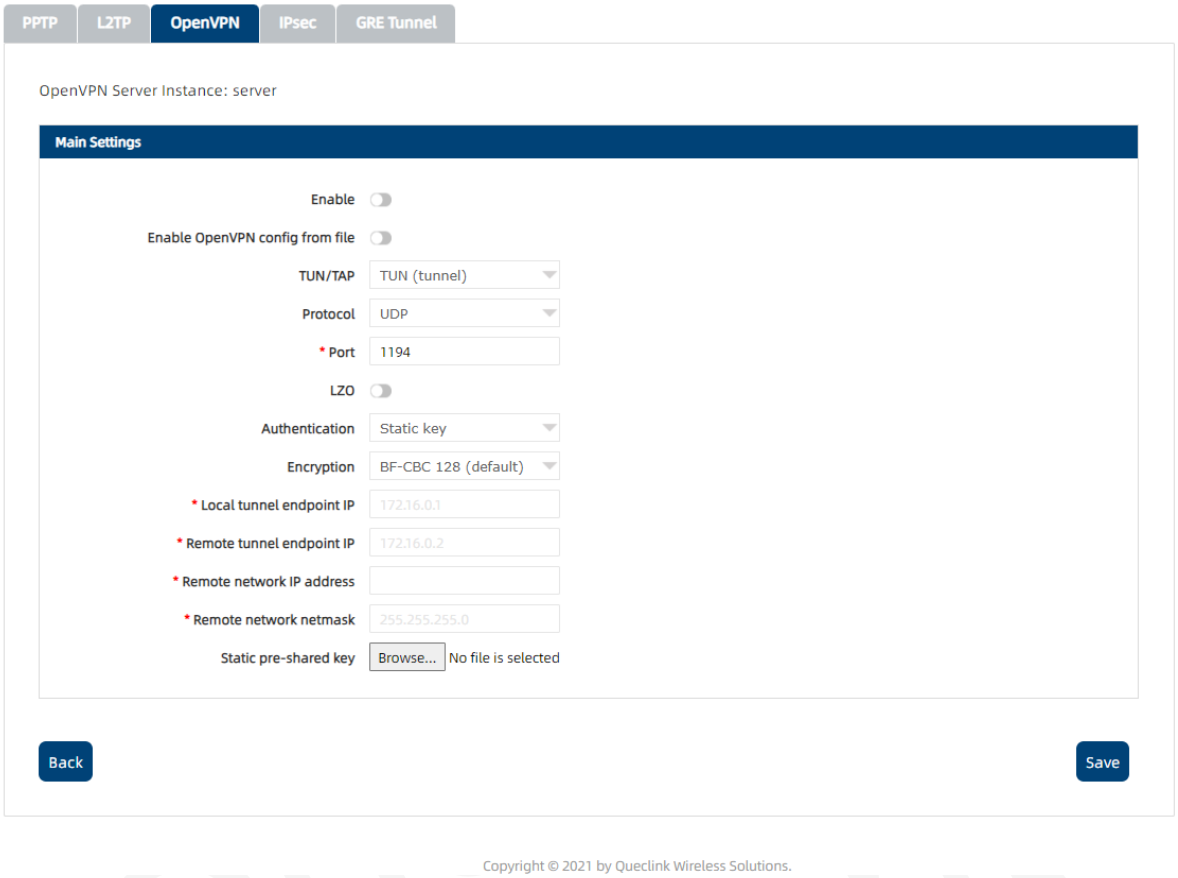
Field Name	Value	Description
Keep alive	two integers separated by a space; default: none	Defines two time intervals: • The first is used to periodically send ICMP requests to the OpenVPN server • The second defines a time window for restarting the OpenVPN service if no response is received. Example: 10 120
Static key: Local tunnel endpoint IP	ip; default: none	IP address of the local OpenVPN network interface.
Static key: Remote tunnel endpoint IP	ip; default: none	IP address of the remote OpenVPN network (server) interface.
Remote network IP address	ip; default: none	LAN IP address of the remote network (server).
Remote network IP netmask	netmask; default: none	LAN IP subnet mask of the remote network (server).
Password: Username	string; default: none	Username used for authentication to the OpenVPN server.
Password: Password	string; default: none	Password used for authentication to the OpenVPN server.
Extra options	string; default: none	Extra OpenVPN options to be used by the OpenVPN instance.
Use PKCS #12 format	yes|no; default: no	Use PKCS #12 archive file format to bundle all the members of a chain of trust.
PKCS #12 passphrase	string; default: none	Passphrase to decrypt PKCS #12 certificates.
PKCS #12 certificate chain	string; default: none	Uploads PKCS #12 certificate chain file.
TLS/Password: HMAC authentication algorithm	none|SHA1|SHA256|SHA384|SHA512; default: SHA1	HMAC authentication algorithm type.
TLS/Password: Additional HMAC authentication	none|Authentication only (tls-auth)|Authentication and encryption (tls-crypt); default: none	An additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.
TLS/Password: HMAC authentication key	.key file; default: none	Uploads an HMAC authentication key file.
TLS/Password: HMAC key direction	0|1|none; default: 1	Key direction must complement the server (0 <-> 1); or both sides omit it.
TLS/Password: Certificate authority	.ca file; default: none	Certificate authority (CA) that issues digital certificates.
TLS: Client certificate	.crt file; default: none	Digital certificate used for client authentication.
TLS: Client key	.key file; default: none	Authenticates the client to the server.
TLS: Private key decryption password (optional)	string; default: none	Password used to decrypt the server's private key.
Static key: Static pre-shared key	.key file; default: none	Uploads a secret key file used for server-client authentication.

OpenVPN server:

An **OpenVPN server** is an entity that waits for incoming connections from OpenVPN clients. To create a new server instance, select Role as Server, enter a custom name and click the 'Add New' button to go to OpenVPN server configuration page. You can click Edit button to edit an existing OpenVPN instance. Only one OpenVPN server

Queclink Confidential

instance is allowed to be added.



Field Name	Value	Description
Enable	yes|no; default: no	Turns the OpenVPN instance on or off.
Enable OpenVPN config from file	yes|no; default: no	Enables custom OpenVPN configuration from file.
TUN/TAP	TUN (tunnel)|TAP (bridged); default: TUN (tunnel)	Virtual network device type. • TUN - a virtual point-to-point IP link which operates at the network layer (OSI layer 3), used when routing is required. • TAP - a virtual Ethernet adapter (switch), operates at the data link layer (OSI layer 2), used when bridging is required.

continues on next page

Table 37 – continued from previous page

Field Name	Value	Description
Protocol	UDP|TCP; default: UDP	Transfer protocol used for the connection. • Transmission Control Protocol (TCP) - most commonly used protocol in the Internet Protocol (IP) suite. It ensures the recipient will receive packets in the order they were sent by numbering, analyzing response messages, checking for errors and resending them if an issue occurs. It should be used when reliability is crucial (for example, file transfer). • User Datagram Protocol (UDP) - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, it should be used when transfer speed is crucial (for example, video streaming, live calls).
Port	integer [0..65535]; default: 1194	TCP/UDP port number used for the connection. Make sure it matches the port number specified on the server side. NOTE: traffic on the selected port will be automatically allowed in the device's firewall rules.
LZO	yes|no; default: no	Turns LZO data compression on or off.
Authentication	TLS|Static Key|TLS/Password|Password; default: TLS	Authentication mode, used to secure data sessions. • Static key is a secret key used for server-client authentication. • TLS authentication mode uses X.509 type certificates: – Certificate Authority (CA) – Client certificate – Client key All mentioned certificates can be generated using OpenVPN or OpenSSL utilities on any type of host machine. One popular utility is Easy-RSA. • TLS/Password uses both TLS and username/password authentication.
Encryption	DES-CBC 64|RC2-CBC 128|DES-EDE-CBC 128|DES-EDE3-CBC 192|DESX-CBC 192|RC2-40-CBC 40|CAST5-CBC 128|RC2-64-CBC 64|AES-128-CBC 128|AES-192-CBC 192|AES-256-CBC 256|none ; default: BF-CBC 128	Algorithm used for packet encryption.
Static key: Local tunnel endpoint IP	ip; default: none	IP address of the local OpenVPN network interface.
Static key: Remote tunnel endpoint IP	ip; default: none	IP address of the remote OpenVPN network (client) interface.
Static key: Remote network IP address	ip; default: none	LAN IP address of the remote network (client).
Static key: Remote network IP netmask	netmask; default: none	LAN IP subnet mask of the remote network (client).

continues on next page

Table 37 – continued from previous page

Field Name	Value	Description
TLS/TLS/Password: TLS cipher	All|DHE+RSA|Custom; default: All	Packet encryption algorithm cipher.
TLS/Password: Allowed TLS ciphers	All|DHE+RSA|Custom; default: All	A list of TLS ciphers accepted for this connection.
TLS/TLS/Password: Client to client	yes|no; default: no	Allows OpenVPN clients to communicate with each other on the VPN network.
TLS/TLS/Password: Keep alive	two integers separated by a space; default: none	Defines two time intervals: • The first is used to periodically send ICMP requests to the OpenVPN server. • The second defines the time window used to restart OpenVPN if no ICMP response is received. Example: 10 120
TLS/TLS/Password: Virtual network IP address	ip; default: none	IP address of the OpenVPN network.
TLS/TLS/Password: Virtual network netmask	netmask; default: none	Subnet mask of the OpenVPN network.
TLS/TLS/Password: Push option	OpenVPN options; default: none	Push options are used to “push” routes or other settings to connecting clients.
TLS/TLS/Password: Allow duplicate certificates	yes|no; default: no	Allows multiple clients to connect using the same certificates.
Use PKCS #12 format	yes|no; default: no	Use PKCS #12 archive file format to bundle chain-of-trust certificates.
PKCS #12 passphrase	string; default: none	Passphrase to decrypt PKCS #12 certificates.
PKCS #12 certificate chain	string; default: none	Uploads PKCS #12 certificate chain file.
TLS/Password: User name	string; default: none	Username used for authentication to this OpenVPN server.
TLS/Password: Password	string; default: none	Password used for authentication to this OpenVPN server.
Static key: Static pre-shared key	.key file; default: none	Uploads a secret key file used for server-client authentication.
TLS/TLS/Password: Certificate authority	.ca file; default: none	Certificate authority that issues digital certificates.
TLS/TLS/Password: Server certificate	.crt file; default: none	Certificate used to identify the OpenVPN server.
TLS/TLS/Password: Server key	.key file; default: none	Authenticates clients to the server.
TLS/TLS/Password: Diffie Hellman parameters	.pem file; default: none	DH parameters define how OpenSSL performs Diffie-Hellman key exchange.
TLS/TLS/Password: CRL file (optional)	.pem file|.crl file; default: none	Certificate revocation list (CRL) containing revoked certificates.

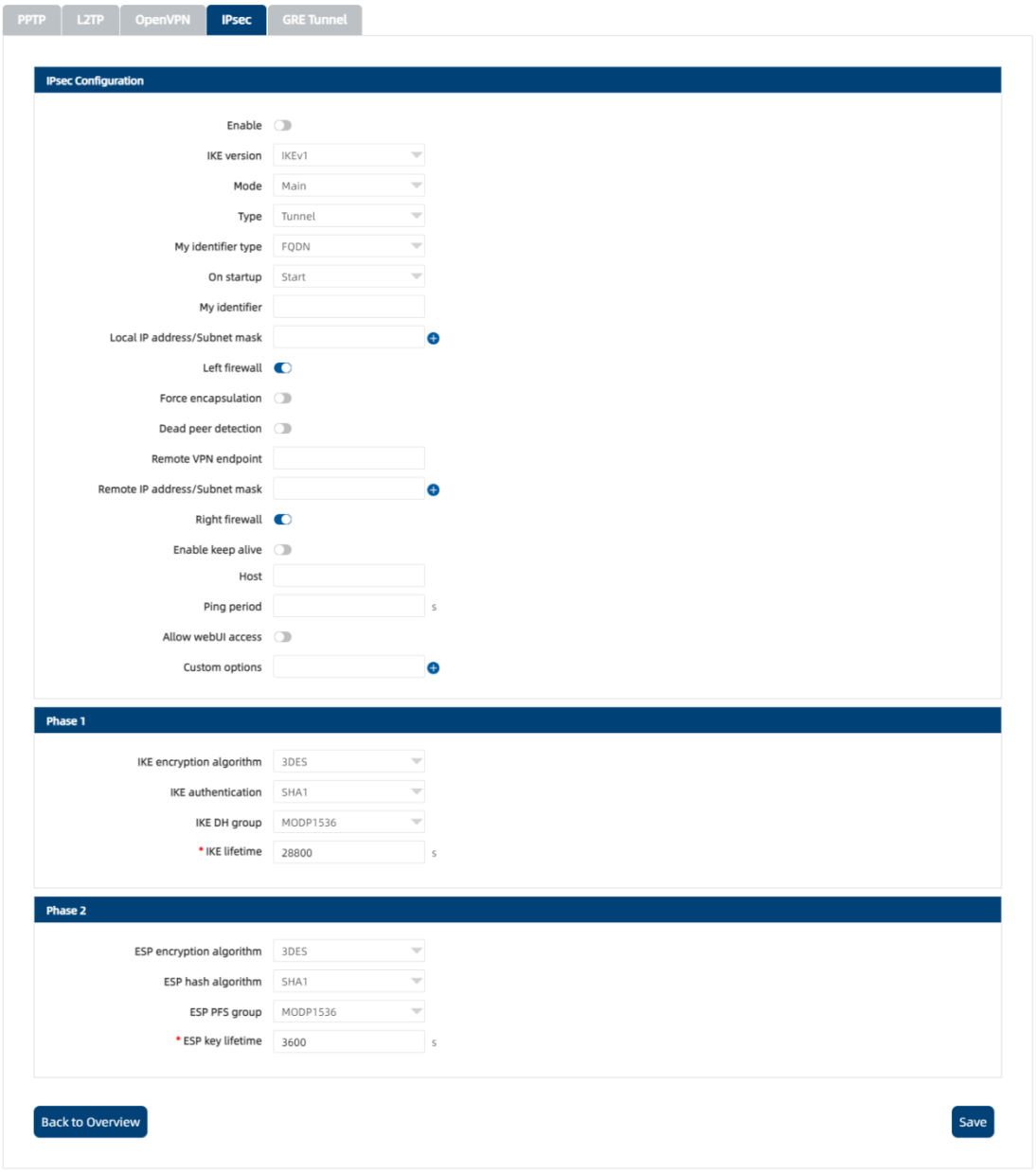
A server needs to have a public IP address in order to be available from the public network (the Internet).

Queclink Confidential

4.3.2.4 IPSec

To create a new IPsec instance, go to the Services → VPN → IPsec section, enter a custom name and click Add icon.

Queclink Confidential


PPTP
L2TP
OpenVPN
IPsec
GRE Tunnel
IPsec Configuration
Enable
IKE version
IKEv1
Mode
Main
Type
Tunnel
My identifier type
FQDN
On startup
Start
My identifier
Local IP address/Subnet mask
Left firewall
Force encapsulation
Dead peer detection
Remote VPN endpoint
Remote IP address/Subnet mask
Right firewall
Enable keep alive
Host
Ping period
s
Allow webUI access
Custom options
Phase 1
IKE encryption algorithm
3DES
IKE authentication
SHA1
IKE DH group
MODP1536
* IKE lifetime
28800
s
Phase 2
ESP encryption algorithm
3DES
ESP hash algorithm
SHA1
ESP PFS group
MODP1536
* ESP key lifetime
3600
s
Back to Overview
Save

Field Name	Value	Description
Enable	yes|no; default: no	Turns the IPsec instance on or off.
IKE version	IKEv1|IKEv2; default: IKEv1	Internet Key Exchange (IKE) version used for key exchange. • IKEv1 - more commonly used but contains known issues, for example, dealing with NAT. • IKEv2 - updated version with increased and improved capabilities, such as integrated NAT support, supported multihosting, deprecated exchange modes (does not use main or aggressive mode; only 4 messages required to establish a connection).
Mode	Main|Aggressive; default: Main	Internet Security and Key Management Protocol (ISAKMP) phase 1 exchange mode. • Main - performs three two-way exchanges between the initiator and the receiver (a total of 9 messages). • Aggressive - performs fewer exchanges than main mode (a total of 6 messages) by storing most data into the first exchange. In aggressive mode, the information is exchanged before there is a secure channel, making it less secure but faster than main mode.
Type	Tunnel|Transport; default: Tunnel	Type of connection. Tunnel - protects internal routing information by encapsulating the entire IP packet (IP header and payload); commonly used in site-to-site VPN connections; supports NAT traversal. Transport - only encapsulates IP payload data; used in client-to-site VPN connections; does not support NAT traversal; usually implemented with other tunneling protocols (for example, L2TP).
On startup	Ignore|Add|Route|Start; default: Start	Defines how the instance should act on the device startup. • Ignore - does not start the tunnel. • Add - loads a connection without starting it. • Route - starts the tunnel only if there is traffic. • Start - starts the tunnel on startup.
My identifier	ip|string; default: none	Defines how the user (IPsec instance) will be identified during authentication.
Tunnel: Local IP address/Subnet mask	ip/netmask|default: none	Local IP address and subnet mask used to determine which part of the network can be accessed in the VPN network. Netmask range [0..32]. If left empty, IP address will be selected automatically.
Left firewall	off|on; default: on	Adds necessary firewall rules to allow traffic of this IPsec instance on this device.
Force encapsulation	yes|no; default: no	Forces UDP encapsulation for ESP packets even if a “no NAT” situation is detected.
Dead Peer Detection	yes|no; default: no	A function used during Internet Key Exchange (IKE) to detect a “dead” peer. It used to reduce traffic by minimizing the number of messages when the opposite peer in unavailable and as failover mechanism.
Dead Peer Detection: Delay (sec)	integer; default: none	The frequency of checking whether a peer is still available or not.
Dead Peer Detection: Timeout (sec)	integer; default: none	Time limit after which the IPsec instance will stop checking the availability of a peer and determine it to be “dead” if no response is received.
Remote VPN endpoint	host|ip; default: none	IP address or hostname of the remote IPsec instance.
Remote identifier	ip|string; default: none	Defines remote IPsec instance identification.
Tunnel: Remote IP address/subnet mask	ip/netmask; default: none	Remote network IP address and subnet mask used to determine which part of the network can be accessed in the VPN network. Netmask range [0..32]. This value must differ from the device’s LAN IP.
Right firewall	yes|no; default: yes	Adds necessary firewall rules to allow traffic from the opposite IPsec instance on this device.
Transport: Use with DMVPN	yes|no; default: no	Adds several necessary options to make DMVPN work.
Passthrough net-	None|LAN|Wired|Wi	Select networks which should be passthrough and excluded from routing

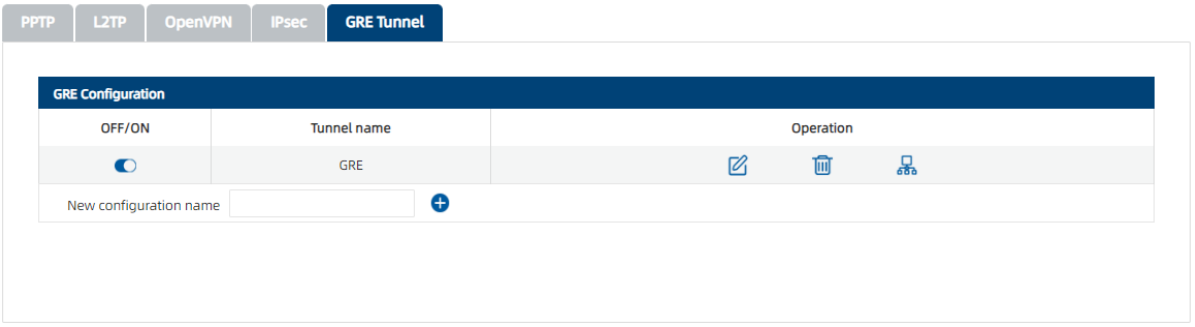
IKE (Internet Key Exchange) is a protocol used to set up security associations (SAs) for the IPsec connection. This process is required before the IPsec tunnel can be established. It is done in two phases:

Field Name	Value	Description
Encryption algorithm	DES|3DES|AES128|AES192|AES256; default: 3DES	Algorithm used for data encryption.
Authentication/Hash algorithm	MD5|SHA1|SHA256|SHA384|SHA512; default: SHA1	Algorithm used for exchanging authentication and hash information.
DH group/PFS group	MODP768|MODP1024|MODP1536|MODP2048|MODP3072|MODP4096; default: MODP1536	Diffie-Hellman (DH) group used in the key exchange process. Higher group numbers provide more security, but take longer and use more resources to compute the key.
Lifetime	integer; default: 8 hours	Defines a time period after which the phase will re-initiate its exchange of information.

4.3.2.5 GRE Tunnel

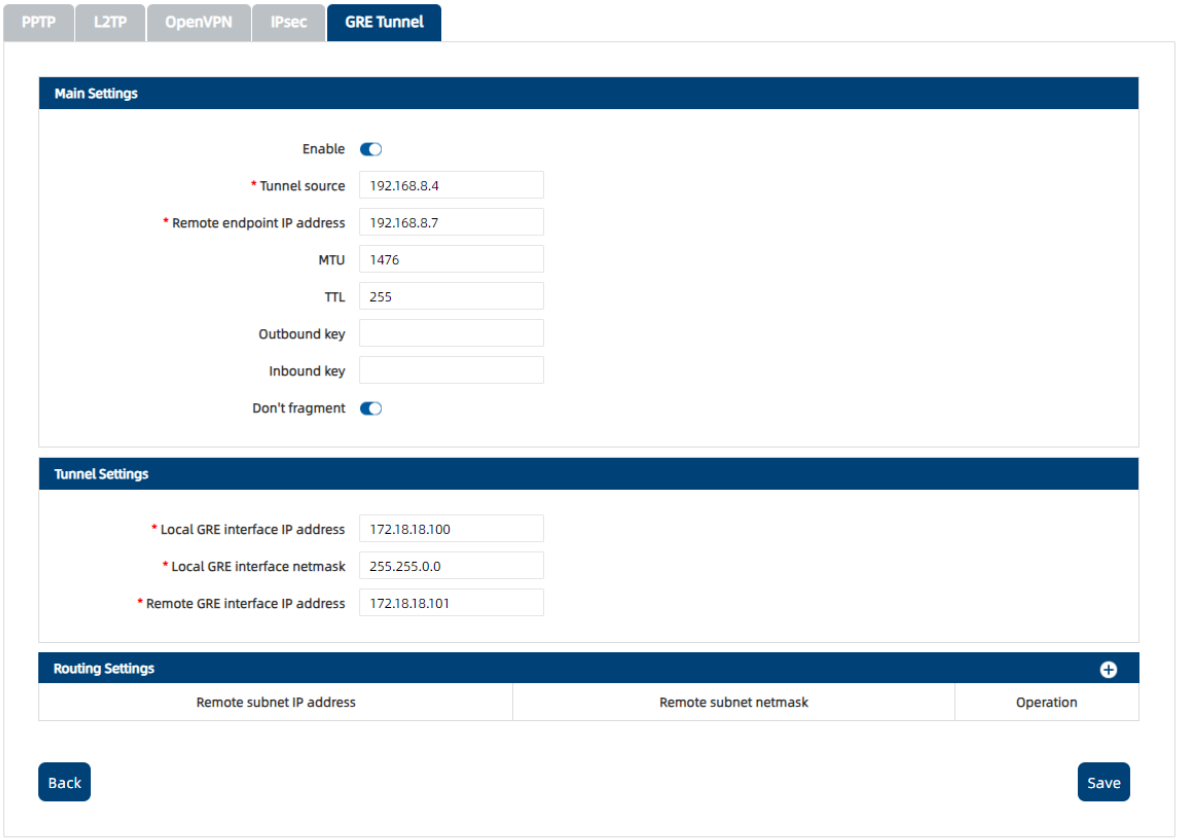
Generic Routing Encapsulation (**GRE**) is a tunneling protocol used to establish point-to-point connections between remote private networks. GRE tunnels encapsulate data packets in order to route other protocols over IP networks.

To create a new GRE Tunnel instance, enter a custom name and click the 'Add' icon to go to the configuration page.



Copyright © 2021 by Queclink Wireless Solutions.

You can click edit button on the right to edit an existing GRE instance.



Copyright © 2021 by Queclink Wireless Solutions.

Queclink Confidential

Field Name	Value	Description
Enabled	yes|no; default: no	Turns the GRE Tunnel instance on or off.
Tunnel source	network interface; default: none	Network interface used to establish the GRE Tunnel.
Remote endpoint IP address	ip; default: none	External IP address of another GRE instance used to establish the initial connection between peers.
MTU	integer; default: 1476	Sets the maximum transmission unit (MTU) size. It is the largest size of a protocol data unit (PDU) that can be transmitted in a single network layer transaction.
TTL	integer [0..255]; default: 255	Sets a custom TTL (Time to Live) value for encapsulated packets. TTL is a field in the IP packet header which is initially set by the sender and decreased by 1 on each hop. When it reaches 0 it is dropped and the last host to receive the packet sends an ICMP "Time Exceeded" message back to the source.
Outbound key	integer [0..65535]; default: none	A key used to identify outgoing packets. A This value should match the "Inbound key" value set on the opposite GRE instance or both key values should be omitted on both sides.
Inbound key	integer [0..65535]; default: none	A key used to identify incoming packets. This value should match the "Outbound key" value set on the opposite GRE instance or both key values should be omitted on both sides.
Don't fragment	yes|no; default: yes	When unchecked, sets the nopmtudisc option for tunnel. Cannot be used together with the TTL option.
Local GRE interface IP address	ip; default: none	IP address of the local GRE Tunnel network interface.
Local GRE interface netmask	netmask; default: none	Subnet mask of the local GRE Tunnel network interface.
Remote GRE interface IP address	ip; default: none	IP address of the Remote GRE Tunnel network interface.

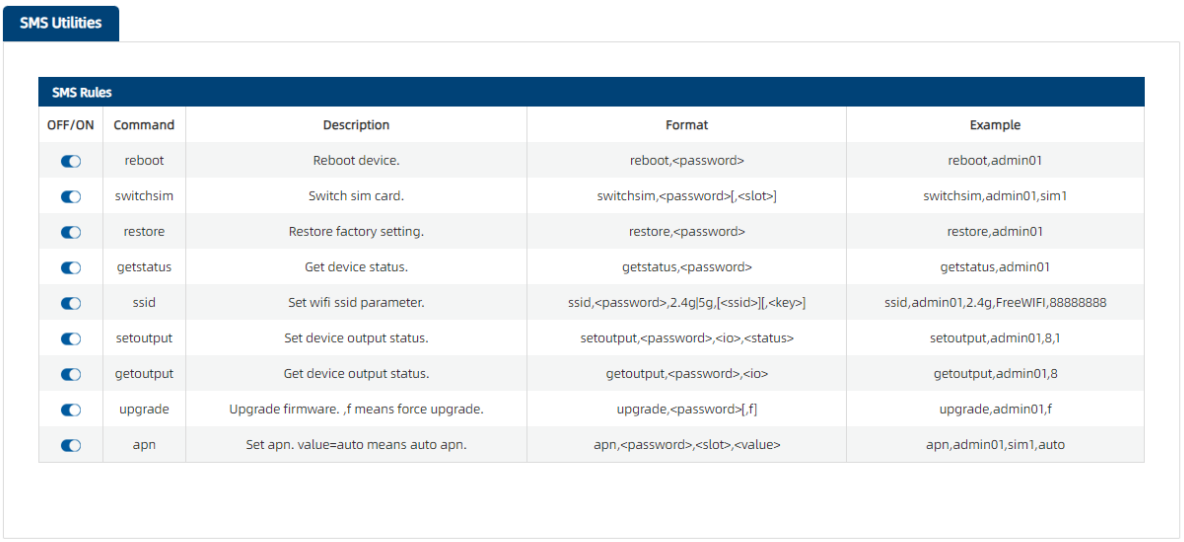
Routing settings are used to configure routes to networks that are behind the device that hosts the opposite GRE instance. To add a new route, simply click the 'Add' button. For information on configuring the route refer to the figure and table below.

Field Name	Value	Description
Remote subnet IP address	ip; default: none	IP address of the network behind the device that hosts the remote GRE instance.
Remote subnet netmask	netmask; default: none	Subnet mask of the network behind the device that hosts the remote GRE instance.

4.3.3 SMS Utilities

The SMS Utilities page is used to configure SMS commands related to device control. It contains a list of rules that perform certain actions when they are activated by SMS messages.

Queclink Confidential



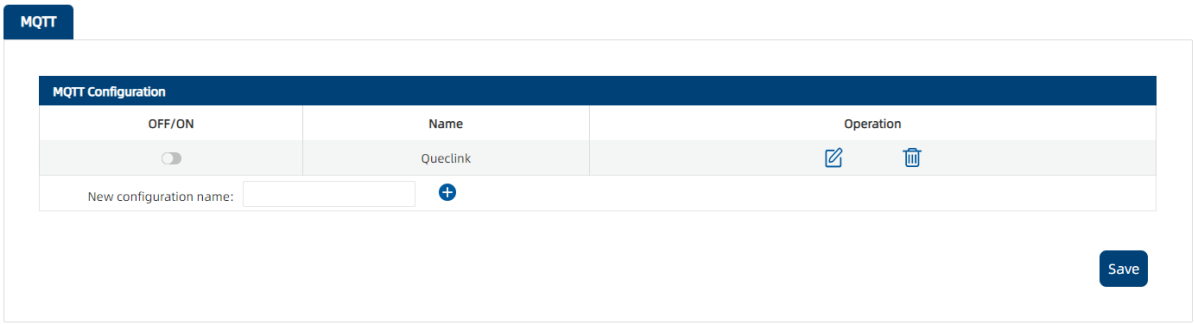
Copyright © 2021 by Queclink Wireless Solutions.

The entire list contains 9 commands. The user can reboot, switch SIM card, restore to factory settings or get device status by sending an SMS text following the rule: “SMS text” password, for example, to reboot a device, you can send ‘reboot admin01’ SMS to the mobile number of this device.

The user can turn on/off specified command by OFF/ON switch button.

4.3.4 MQTT

The MQTT page is to configure the MQTT servers which can subscribe or publish a topic(s). The device supports this functionality via an open source Mosquitto broker. A client (subscriber) subscribes to a topic(s); a publisher posts a message to that specific topic(s). The broker then checks who is subscribed to that particular topic(s) and transmits data from the publisher to the subscriber.



Enter a custom MQTT server name and click the Add icon to create a new MQTT server instance and go to the configuration page. You can click Edit button on the right to edit an existing MQTT server instance.

Currently, the device supports only one MQTT server instance running at the same time.

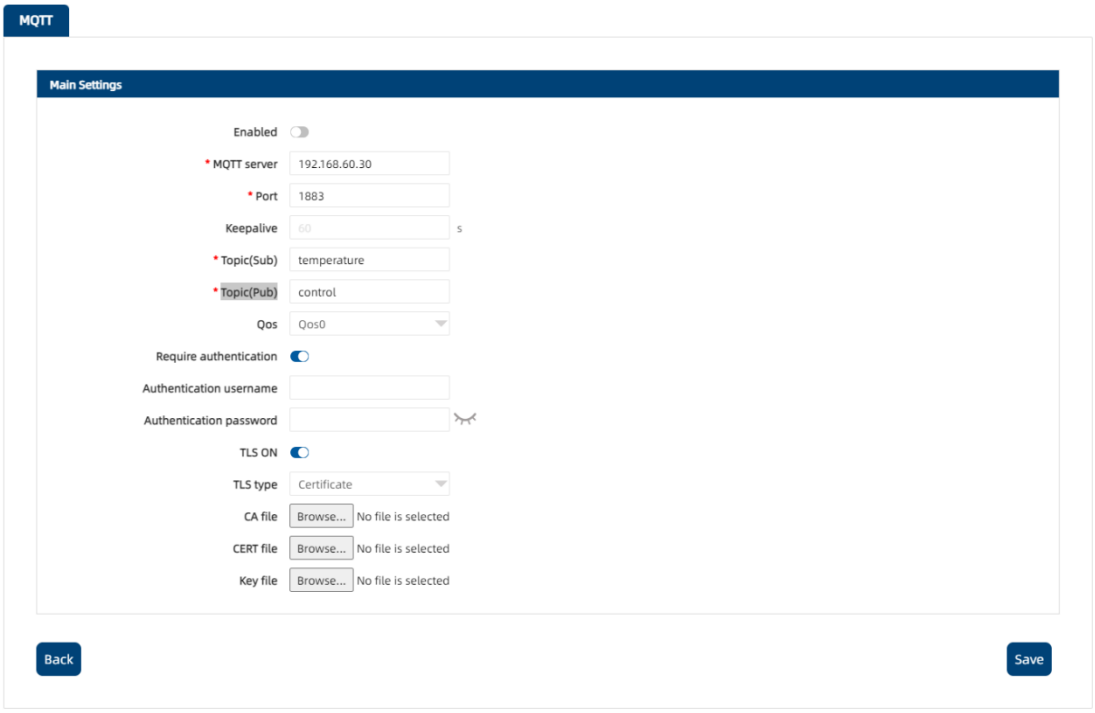


Table 38: MQTT Configuration

Field Name	Value	Description
Enabled	yes|no; default: no	Turns the MQTT server connection on or off.
MQTT server	host|ip; default: none	MQTT server IP address or hostname.
Port	integer [0..65535]; default: 1883	Specifies the port used for connecting to the Broker.
Keeplive	Integer [0..65535]; default: 60	The time interval to keep the connection.
Topic(Sub)	string; default: none	The topic to subscribe from the broker.
Topic(Pub)	string; default: none	The topic to publish to the broker.
Qos	Qos0| Qos1|Qos2; default: Qos0	The Qos level of the MQTT connection.
Require authentication	yes|no; default: no	Toggles the Require authentication between ON or OFF.
Authentication username	string; default: none	Username used for authentication when connecting to the Broker.
Authentication password	string; default: none	Password used for authentication when connecting to the Broker.
TLS	yes|no; default: no	Toggles the TLS authentication between ON or OFF.
TLS type	Certificate; default: Certificate	The type of TLS encryption.
CA file	.ca file; default: none	Certificate authority is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
Certificate file	.crt file; default: none	Certificate file is a type of digital certificate that is used by client systems to make authenticated requests to a remote server. Client certificates play a key role in many mutual authentication designs, providing strong assurances of a requester's identity.
Key file	.key file; default: none	Private key for client to establish connection.

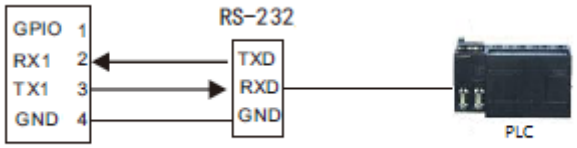
4.3.5 RS232/RS485

RS232 and RS485 functions use the available serial interfaces to transfer data through the device to the Internet. This section allows the user to set the parameters of serial ports. WR310 supports one RS232 and three RS485 ports. The Serial port provides a way to transfer serial data to an IP network, or vice versa.

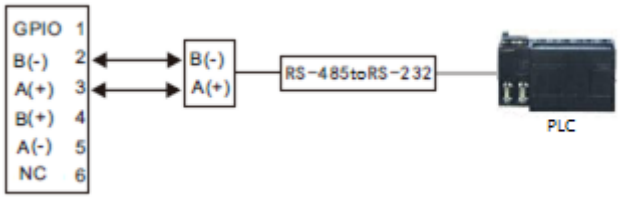
Hardware connection:

The following figure shows how to connect the lower-end device through serial port.

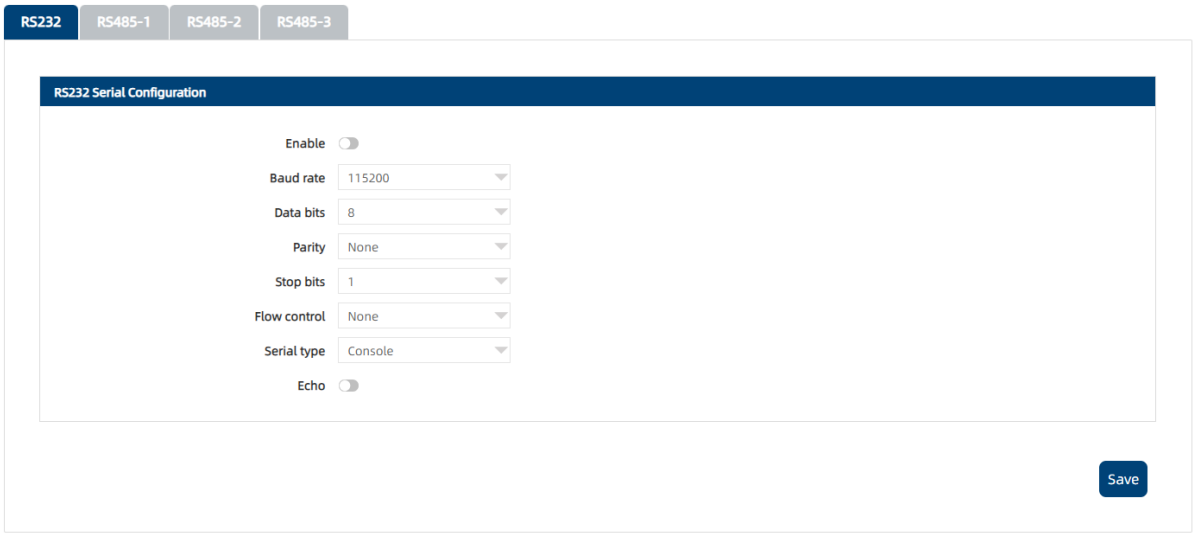
RS232 connection:



RS485 connection:



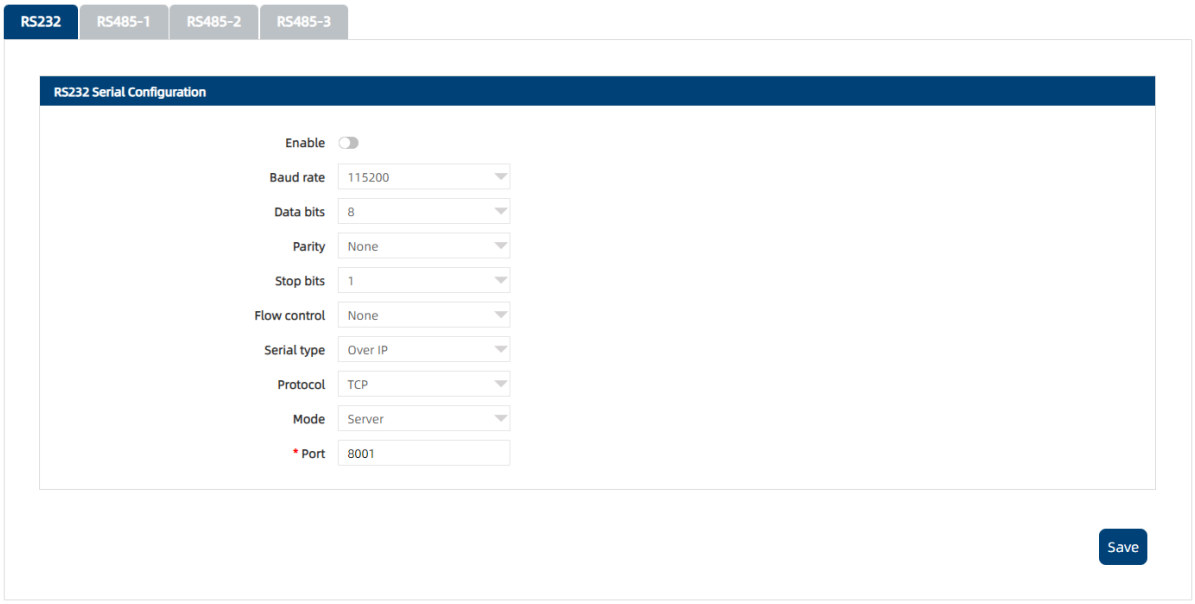
The user can configure the parameters of RS232 port, including baud rate, data bits, etc. The serial type is the working type of RS232. By default, RS232 is working as a console port.



Field Name	Value	Description
Enabled	yes|no; Default: no	When checked, enables the RS232 service
Baud rate	300|1200|2400|4800|9600|19200|38400|57600|115200; Default: 115200	Sets the data rate for serial data transmission (in bits per second)
Data bits	5|6|7|8; Default: 8	The number of data bits for each character
Parity	None|Odd|Even; Default: None	In serial transmission, parity is a method of detecting errors. An extra data bit is sent with each data character, arranged so that the number of bits in each character, including the parity bit, is always odd or always even. If a byte is received with the wrong number of 1s, then it must have been corrupted. However, an even number of errors can pass the parity check. None (N) - no parity method is used Odd (O) - the parity bit is set so that the number of "logical ones (1s)" has to be odd Even (E) - the parity bit is set so that the number of "logical ones (1s)" has to be even
Stop bits	1|2; Default: 1	Stop bits sent at the end of every character allow the receiving signal hardware to detect the end of a character and to resynchronize with the character stream. Electronic devices usually use one stop bit. Two stop bits are required if slow electromechanical devices are used
Flow control	None|Xon/Xoff; Default: None	In many circumstances a transmitter might be able to send data faster than the receiver is able to process it. To cope with this, serial lines often incorporate a "handshaking" method, usually distinguished between hardware and software handshaking. Xon/Xoff - software handshaking. The Xon and Xoff characters are sent by the receiver to the sender to control when the sender will send data, i.e., these characters go in the opposite direction to the data being sent. The circuit starts in the "sending allowed" state. When the receiver's buffers approach capacity, the receiver sends the Xoff character to tell the sender to stop sending data. Later, after the receiver has emptied its buffers, it sends an Xon character to tell the sender to resume transmission
Serial type	Modem Console|Over IP| Modbus|Console; Default: Console	Specifies the serial connection type.
Echo	yes|no; Default: no	Toggles RS232 echo ON or OFF. RS232 echo is a loopback test usually used to check whether the RS232 cable is working properly

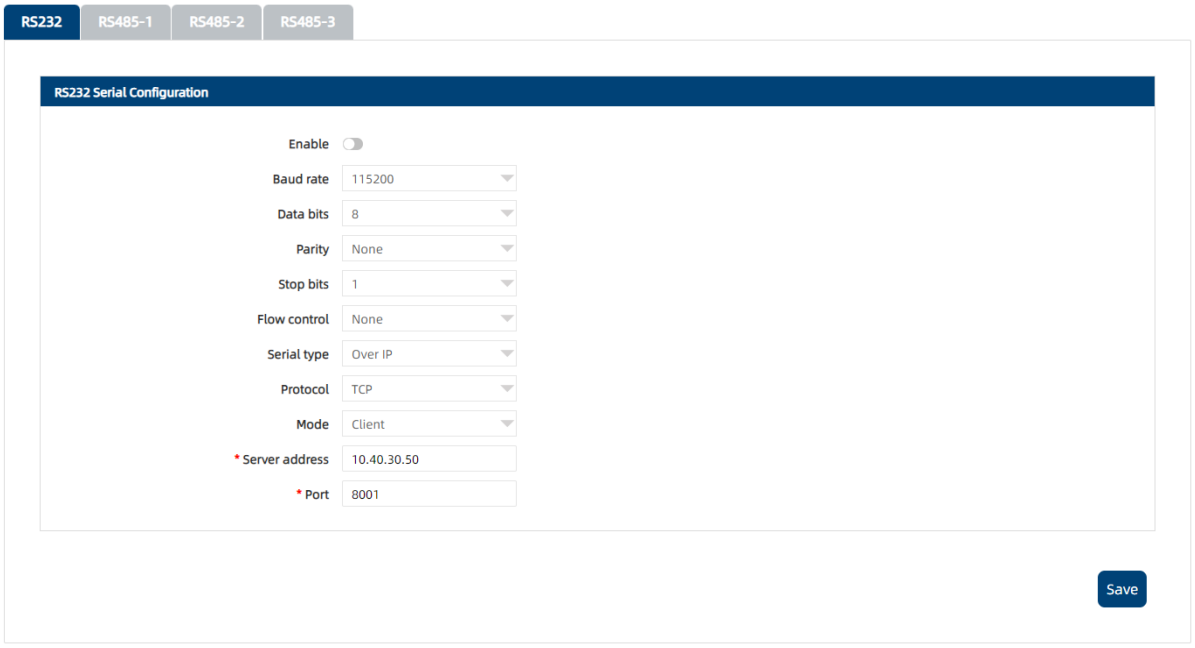
The device can transfer data between RS232/RS485 ports and IP network. When selecting serial type as "Over IP" and "Mode" as "Server", the page will display IP configuration parameters:

Queclink Confidential



Field Name	Value	Description
Protocol	TCP|UDP; Default: TCP	Specifies the protocol used in the communication process.
Mode	Server|Client; Default: Server	Specifies the device's role in the connection: • **Server** - the device waits for incoming connections. • **Client** - the device initiates the connection.
TCP port	integer [0..65535]; Default: " "	The port number used to connect to the server.

When selecting serial type as "Over IP" and "Mode" as "Client", the page will display IP configuration parameters:



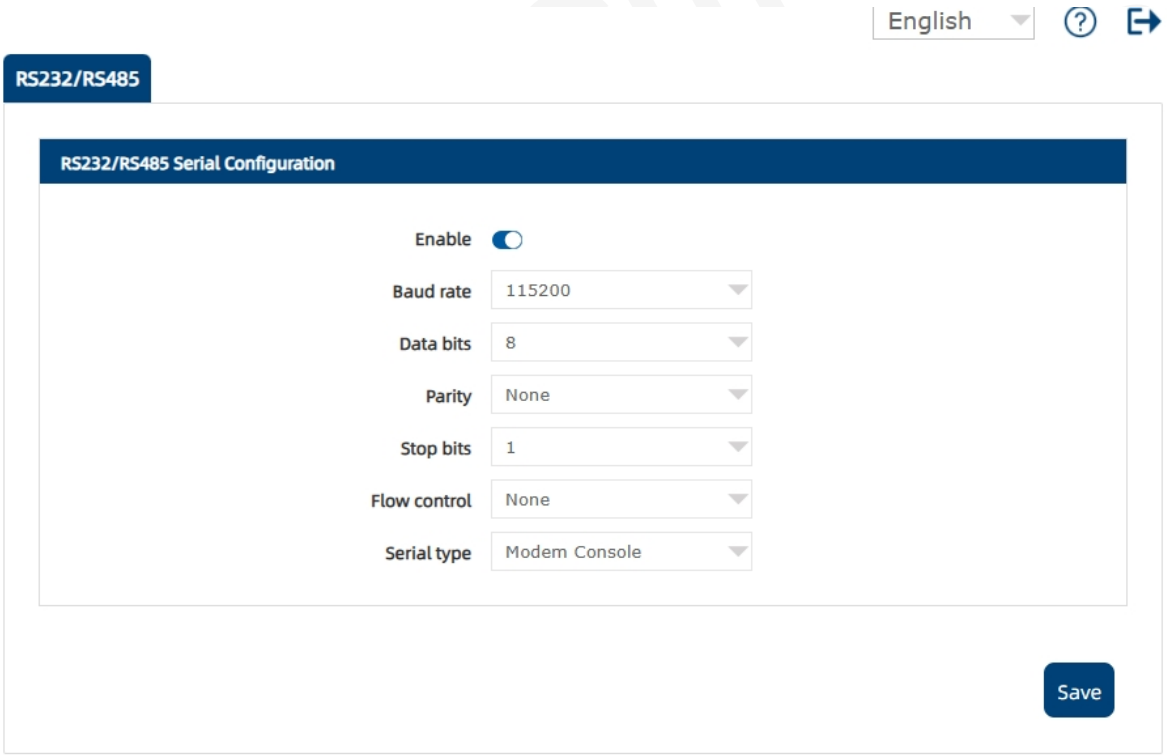
Field Name	Value	Description
Protocol	TCP|UDP; Default: TCP	The protocol used for data transmission.
Mode	Server|Client; Default: Server	**Server** - waits for incoming connection. **Client** - initiates the connection.
Server address	hostlip; Default: no	Server address to which the client will connect to.
Port	integer [0..65535]; Default: " "	The port number used to listen for incoming connections.

The configuration of RS485 is very similar to RS232, you can use the same way to configure the RS485 interface.

When selecting serial type as "Modbus", the serial port will work as a Modbus interface, the device can receive and forward Modbus commands from MQTT server or Modbus TCP master. You can configure relevant parameters in the "Application->Modbus" page.

When the serial type is set to "Modem Console" mode, the device operates like a wireless modem, which allows users to communicate with the internal modem via the serial port, for example, sending and receiving SMS directly from the modem. In this mode, the mobile module's network connection and SMS functionalities are automatically disabled. This is because these features also rely on AT commands to interact with the modem, and disabling them prevents operational interference.

To establish communication, configure the serial port parameters as follows. For detailed instructions on operating this mode, please contact our technical engineer for further support.



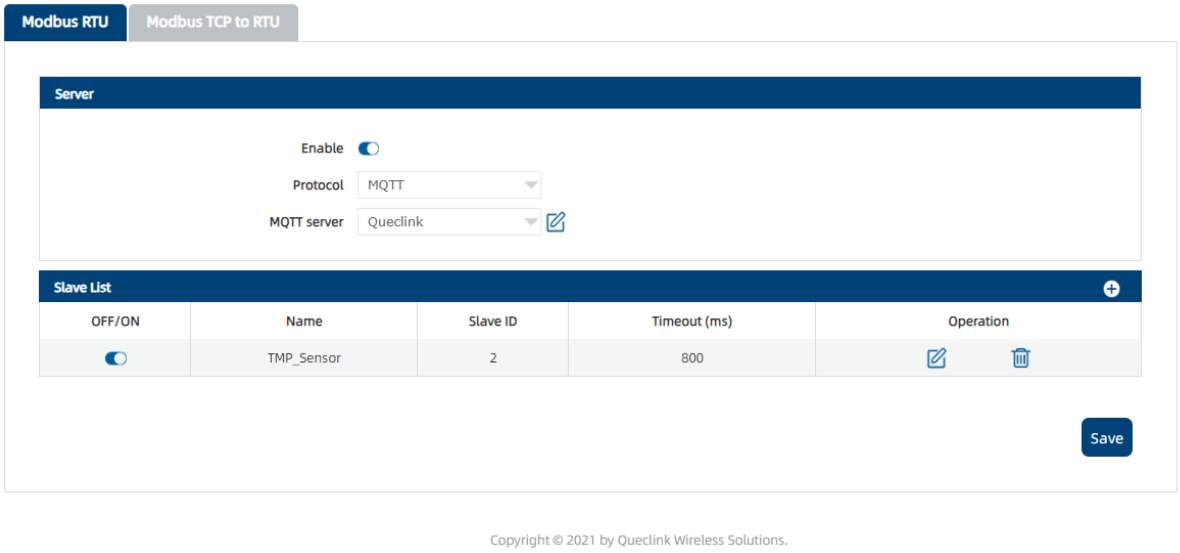
4.3.6 Modbus

This page is for configuring the parameters related to the Modbus function. Before configuring any parameters, you need to set the type of serial ports as Modbus.

4.3.6.1 Modbus RTU

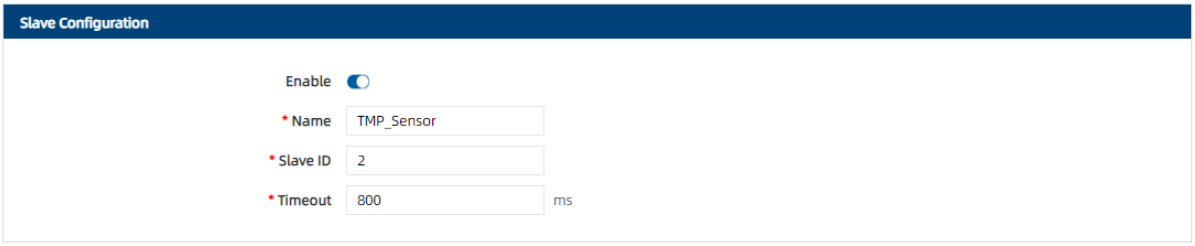
In this page, you can configure the device as a Modbus master, which can request data from Modbus slaves through RS-232/RS485 interfaces and forward the data to a specified server, such as MQTT, HTTP and TCP servers.

The figure below is an example of the configuration:



Copyright © 2021 by Queclink Wireless Solutions.

To forward the Modbus data to an MQTT server, you must select an MQTT server in the server section. Then click the “Add” button in the slave list table to add a Modbus request.



Field Name	Value	Description
Enabled	yes	no; default: no	Turns the slave on or off.
Name	characteristic	Name of a slave
Slave ID	integer [1..255]; default: no	Slave ID. Each slave in a network is assigned a unique identifier ranging from 1 to 255. When the master requests data from a slave, the first byte it sends is the Slave ID.
Timeout	integer [1..9999]/; default: 800	Maximum time to wait for the terminal response (in milliseconds). If no response is received after the amount of time specified in this field, the request is considered to have failed

A Modbus request is a way of obtaining data from Modbus slaves. The master sends a request to a slave specifying the function code to be performed. The slave then sends the requested data back to the Modbus master.

Note: Modbus Serial Master uses Register Number instead of Register Address for pointing to a register. For example, to request the Uptime of a device, you must use 2 in the First Register field.

The figure below is an example of the Requests configuration section and the table below provides information contained in the fields of that section:

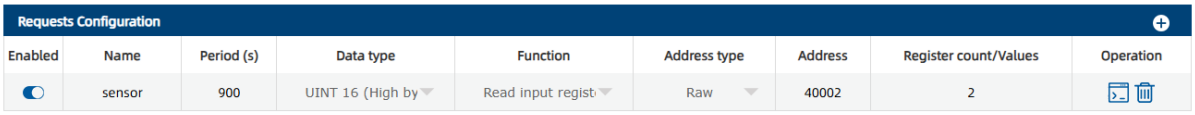


Table 39: Modbus Request Configuration

Field Name	Value	Description
Enabled	yes | no; default: no	Turns the request on or off.
Name	characteristic	Name of a request
Period	integer [1..9999]/; default: 60	Interval (in minutes) at which requests are sent to the slave device.
Data Type	Hex|UNIT 8|SINT 8|UINT 16| SINT 16|UINT 32|Float 32|BOOL; default: Hex	Defines how read data will be stored.
Function	Read Coils (01H)|Write Single Coil (05H)| Write Multiple Coils (0FH)|Read Input Register (04H)| Read Multiple Holding Register (03H)| Write Single Holding Register (06H)| Write Multiple Holding Register (10H); default: Read Coils	Modbus function used in Modbus request.
Address Type	Register | Raw; Default: Register	The address format is as follows: The "Register" is the standard PLC address, like 40001. The "Raw" is the raw address based on different function codes, such as 10.
Address	Integer; default: none	First Modbus register from which data will be read.
Register count (Hex)	Integer; default: none	Number of Modbus registers that will be read during the request
Values (Hex)	String, 128 bits length; default: none	Value to be wrote into a register

When a user configures a request, the device will collect data according to the specified period and report the collected information in the defined JSON format. The data format is defined as follows:

Report message format is:

Table 40: Modbus Query Description

Field Name	Value	Description
time	String	Acquisition time of the query.
IMEI	String	The device's IMEI,Used to identify unique devices.
name	String	Name of the register.
slave	Integer	Modbus slave ID
data_type	String	The data type of the data to be read out.
function	Integer	Function code
modbus_address	Integer	The start address of the register, The starting value is 0. For example, 0 represents 4001 and 1 represents 4002.
values	String	Return data, the length of the string = data_len*2.
crc	String	Modbus CRC checking,

The following is an example,

Queclink Confidential

```
{"time":"2024-11-29
15:04:19","IMEI":"865235054144742","name":"15","slave":1,"data_type":"HEX",
↪"function":16,"modbus_address":0,"values":"A0
BB C0 00","crc":"41 C8"}
```

Users can also send requests directly through the MQTT server instead of requesting via local configuration.

The format of the requests from the server is as follows:

Field Name	Value	Description
service	String	Service ID. Used to identify the corresponding service. 1 represents Modbus RTU service.
id	Integer	ID of the message, to identify the message.
IMEI	String	The IMEI of the device. This is an optional field. If this field is not included, it indicates that the message is for broadcasting. If it is included, it specifies that the device with this IMEI should respond to this instruction.
slave	Integer	ID of MODBUS slave device.
Data_type	String	The data type of the data to be read out.
Function	Integer, include 1 | 5 | 15 | 4 | 3 | 6 | 16	Function code of the Modbus request, 3 represents read register and 6 represents write register.
address_type	String	Register or Raw.
modbus_register	Integer	The start address of the register. The starting value is 0. For example, 0 represents 4001 and 1 represents 4002.
register_count	Integer	The length of register.
Values (Hex)	String	Value to be wrote into a register.
period	Integer	The time interval between two requests. The field is optional. If this field is empty, it means to only send one request; otherwise, the device will send the request at specified period.
crc	Integer	Modbus CRC checking. (Optional)

The following is an example,

```
{"service":"1","id":1,"IMEI":"861157040079259","slave":1,"data_type":"HEX",
↪"function":3,"address_type":"Raw","modbus_address":6,"register_count":3}
```

Return message format is:

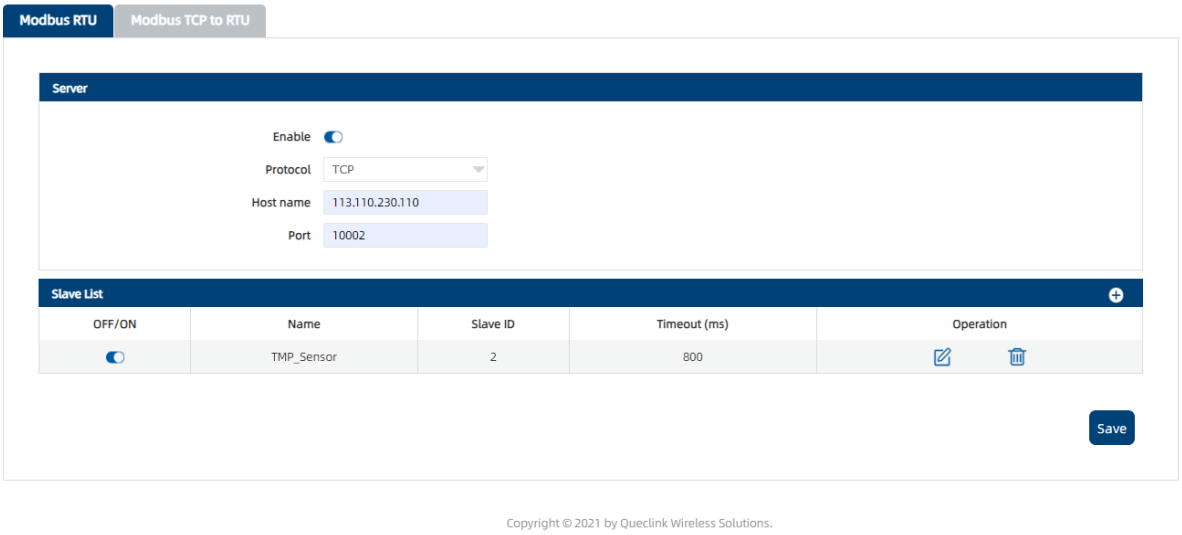
Field Name	Value	Description
time	String	Acquisition time of the query.
id	Integer	ID of the message, to identify the message.
IMEI	String	The device's IMEI, used to identify unique devices.
slave	Integer	Modbus slave ID.
data_type	String	The data type of the data to be read out.
function	Integer	Function code.
modbus_address	Integer	The start address of the Raw register.
values	String	Register values.
crc	String	Modbus CRC checking.

The following is an example,

```
{"time":"2024-11-29 15:23:19", "IMEI":"861157040079259", "id":1,
"slave":1,"data_type":"HEX" "function":3, "modbus_address":6,
"values":"04 02 00 08 00 08", "crc":"D935"}
```

To forward the Modbus data to a TCP server, you must select a TCP server in the server section.

Queclink Confidential



The format from the TCP server to the device follows the MQTT format, but a starting symbol “@” and an ending symbol “$” need to be added in the message.

The following is an example,

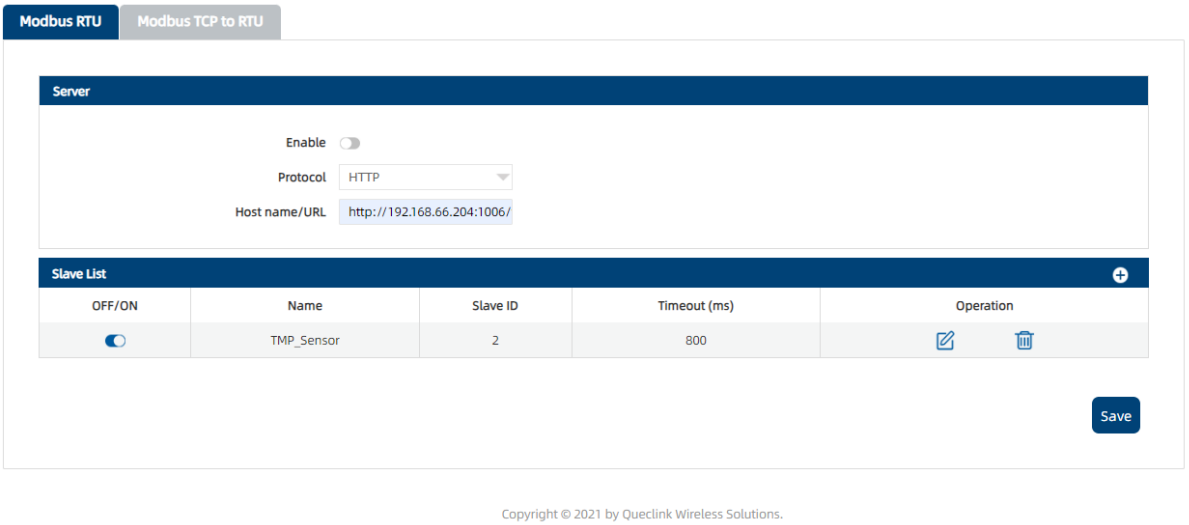
```
@{"service":"1","id":1,"IMEI":"861157040079259","slave":1,"data_type":"HEX",
↪"function":3,"address_type":"Raw","modbus_address":6,"register_count":3}$
```

A starting symbol “@” and and ending symbol “$” will also be added in the return message.

The following is an example,

```
@{"time":"2024-11-29 15:23:19", "IMEI":"861157040079259", "id":1,
"slave":1,"data_type":"HEX" "function":3, "modbus_address":6,
"values":"04 02 00 08 00 08", "crc":"D935"}$
```

You can also forward the data to HTTP servers. Select the protocol as HTTP:

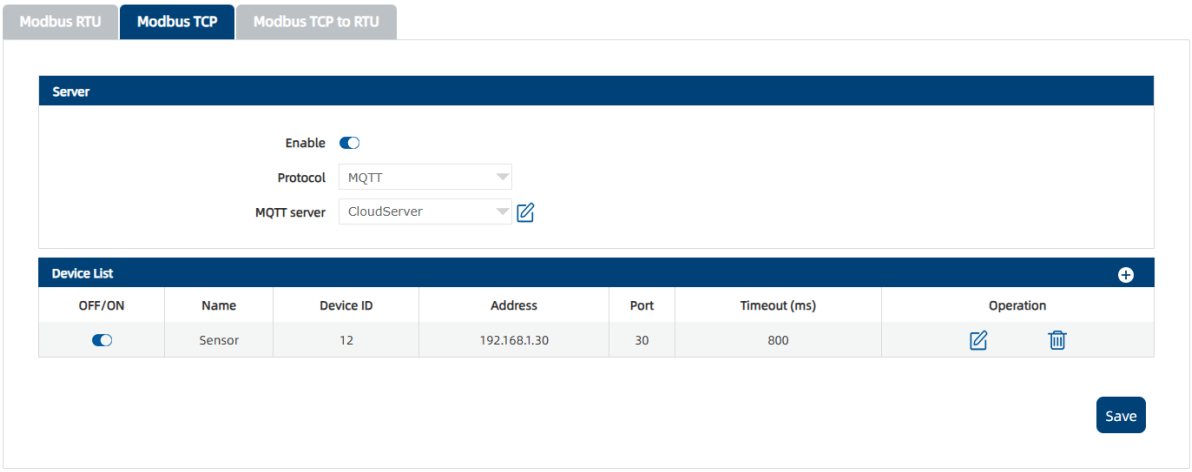


In HTTP mode, only the device can send messages to the server. The format is the same as MQTT.

4.3.6.2 Modbus TCP

In this page, you can configure the device as a Modbus TCP master, which can request data from Modbus TCP slaves through TCP/IP network and forward the data to a specified server, such as MQTT, HTTP and TCP servers.

The figure below is an example of the configuration:



To forward the Modbus data to an MQTT server, you must select a MQTT server in the server section. Then click the “Add” button on the slave list table to add a Modbus request.



Table 41: Modbus TCP Slave Configuration

Field Name	Value	Description
Enabled	yes | no; default: no	Turns the slave on or off.
Name	characteristic	Name of a slave
Device ID	integer [1..255]; default: no	Slave device ID. Each slave in a network is assigned a unique identifier ranging from 1 to 255. When the master requests data from a slave, the first byte it sends is the Slave ID.
Address	ip4; default: none	Slave device’s IP address.
Port	integer [0..65535]; default: none	Server device’s Modbus TCP port.
Timeout	integer [1..9999]/; default: 800	Maximum time to wait for the terminal response (in milliseconds). If no response is received after the amount of time specified in this field, the request is considered to have failed.

A Modbus request is a way of obtaining data from Modbus slaves. The master sends a request to a slave specifying the function code to be performed. The slave then sends the requested data back to the Modbus master.

Note: Modbus Serial Master uses Register Number instead of Register Address for pointing to a register. For example, to request the Uptime of a device, you must use 2 in the First Register field.

The figure below is an example of the Requests configuration section and the table below provides information contained in the fields of that section:

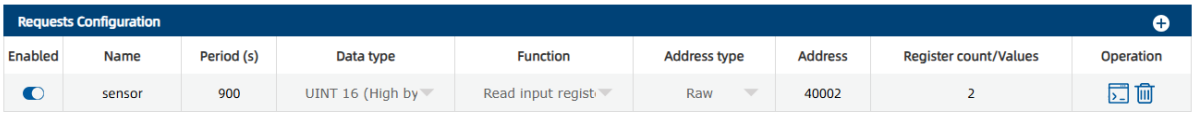


Table 42: Modbus Request Configuration Fields

Field Name	Value	Description
Enabled	yes	no; default: **no**	Turns the request on or off.
Name	characteristic	Name of a request
Period	integer [1..9999]/; default: 60	Interval (in minutes) at which requests are sent to the slave device.
Data Type	Hex	UNIT 8	SINT 8	UINT 16	SINT 16	UINT 32	Float 32	BOOL; default: Hex	Defines how read data will be stored.
Function	Read Coils (01H)	Write Single Coil (05H)	Write Multiple Coils (0FH)	Read Input Register (04H)	Read Multiple Holding Register (03H)	Write Single Holding Register (06H)	Write Multiple Holding Register (10H); default: **Read Coils**	Modbus function used in Modbus request.
Address Type	Register	Raw; Default: Register	The address format is as follows: The “Register” is the standard Modbus address, like 40001. The “Raw” is the raw address based on different function codes, such as 10.
Address	Integer; default: none	First Modbus register from which data will be read. Depending on the different Address Types, addresses in different formats can be entered.
Register count (Hex)	String [1..FFFF]; default: **none**	Number of Modbus registers that will be read during the request
Values (Hex)	String, 128 bits length; default: **none**	Value to be wrote into a register

When a user configures a request, the device will collect data according to the specified period and report the collected information in the defined JSON format. The data format is defined as follows:

The report message format is:

Table 43: Modbus TCP Data Format

Field Name	Value	Description
time	String	Acquisition time of the query.
IMEI	String	The device's IMEI, used to identify unique devices.
name	String	Name of the register.
device_id	Integer	Modbus TCP device ID.
device_address	String	Modbus TCP device address.
device_port	Integer	Modbus TCP device port.
data_type	String	The data type of the data to be read out.
function	Integer	Function code.
modbus_address	Integer	The start address of the register. The starting value is 0. For example, 0 represents 4001 and 1 represents 4002.
values	String	Return data, the length of the string = data_len*2.
crc	String	Modbus CRC checking.

The following is an example,

```
{"time":"2024-11-27
11:06:30","IMEI":"860195059424736","name":"1","device_id":"1","device_address":
↪"192.168.1.188","device_port":502,"data_type":"HEX","function":16,"modbus_address
↪":0,"values":"00
02"}
```

Users can also send requests directly through the MQTT server instead of requesting via local configuration.

The format of the requests sent by the server is as follows:

Table 44: Modbus TCP Request Format

Field Name	Value	Description
service	String	Service ID. Used to identify the corresponding service. 1 represents Modbus RTU service.
id	Integer	ID of the message, to identify the message.
IMEI	String	The IMEI of the device. This is an optional field. If this field is not included, it indicates that the message is for broadcasting. If it is included, it specifies that the device with this IMEI should respond to this instruction.
device_id	String	Modbus TCP device ID.
device_address	String	Modbus TCP device address.
device_port	Integer	Modbus TCP device port.
Data_type	String	The data type of the data to be read out.
Function	Integer, include 1 | 5 | 15 | 4 | 3 | 6 | 16	Function code of the Modbus request, 3 represents read register and 6 represents write register.
address_type	String	Register or Raw.
modbus_address	Integer	The start address of the register. The starting value is 0. For example, 0 represents 4001 and 1 represents 4002.
register_count	Integer	The length of register.
Values (Hex)	String	Value to be wrote into a register.
period	Integer	The time interval between two requests. The field is optional. If this field is empty, it means to only send one request; otherwise, the device will send the request at specified period.
crc	Integer	Modbus CRC checking.

The following is an example,

Queclink Confidential

```
{"service":"1","id":1,"data_type":"HEX","device_id":10,
"device_address":"192.168.1.188", "device_port":502, "function":4,
"address_type":"Raw", "modbus_address":1, "register_count":1}
```

Return message format is:

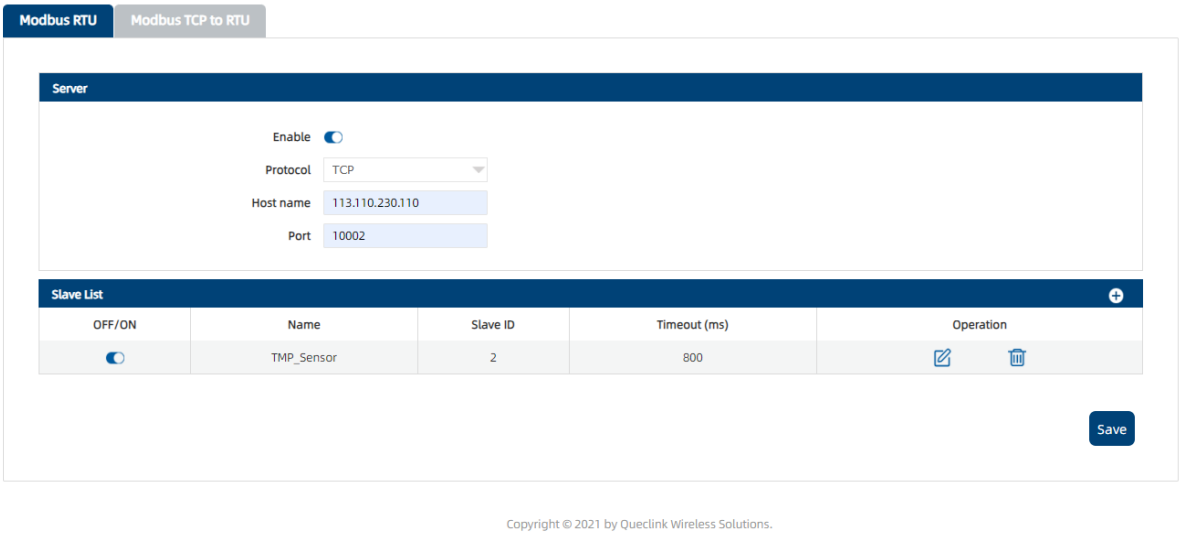
Table 45: Modbus TCP Response Format

Field Name	Value	Description
time	String	Acquisition time of the query.
id	Integer	ID of the message, to identify the message.
IMEI	String	The device's IMEI, used to identify unique devices.
device_id	String	Modbus TCP device ID.
device_address	String	Modbus TCP device address.
device_port	Integer	Modbus TCP device port.
data_type	String	The data type of the data to be read out.
function	Integer	Function code.
values	String	Return data, the length of the string = data_len*2.

The following is an example,

```
{"time":"2024-11-28
15:56:43","id":123,"IMEI":"869182060010614","name":"1","device_id":"10","device_
↪address":"192.168.1.10","device_port":5020,"data_type":"HEX","function":2,
↪"modbus_address":1,"values":"FF
00 01 00"}
```

To forward the Modbus data to a TCP server, you must select a TCP server in the server section.



The format from the TCP server to the device follows the MQTT format, but a starting symbol "@" and an ending symbol "$" need to be added in the message.

The following is an example,

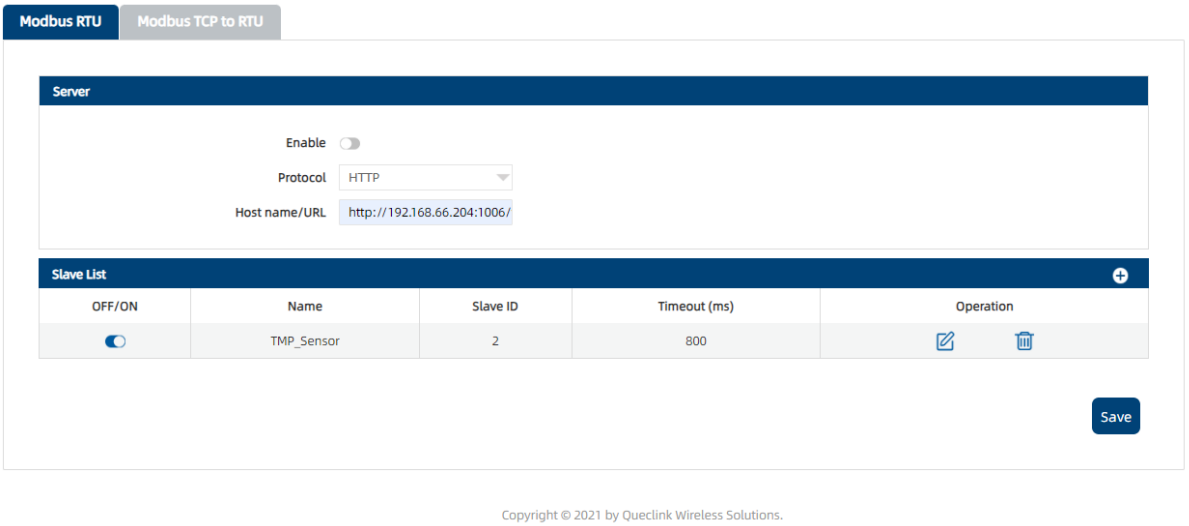
```
@{"service":"1","id":13,"data_type":"HEX","slave":1, "function":3,
"address_type":"Raw", "modbus_address":1, "register_count":3,
"period":60}$
```

A starting symbol "@" and ending symbol "$" will also be added in the return message.

The following is an example,

```
@{"service":"1","id":13,"data_type":"HEX","slave":1, "function":3,
"address_type":"Raw", "modbus_address":1, "register_count":3,
"period":60}$
```

You can also forward the data to HTTP servers. Select the protocol as HTTP:

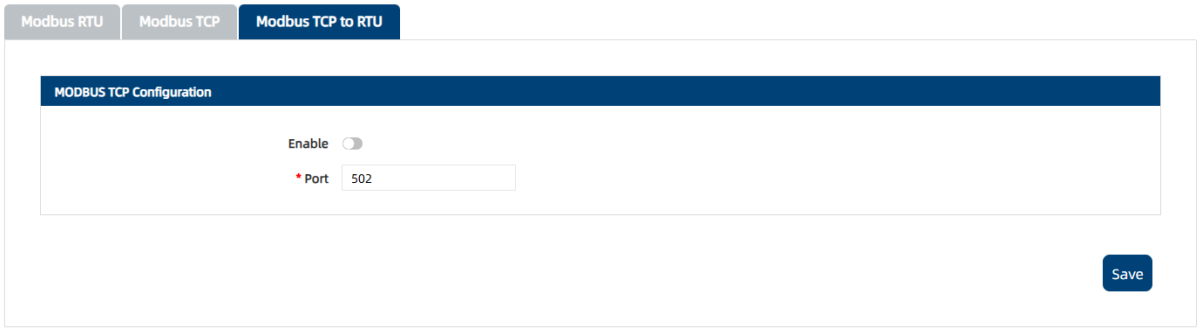


Copyright © 2021 by Queclink Wireless Solutions.

In HTTP mode, only the device can send messages to the server. The format is the same as MQTT.

4.3.6.3 Modbus TCP to RTU

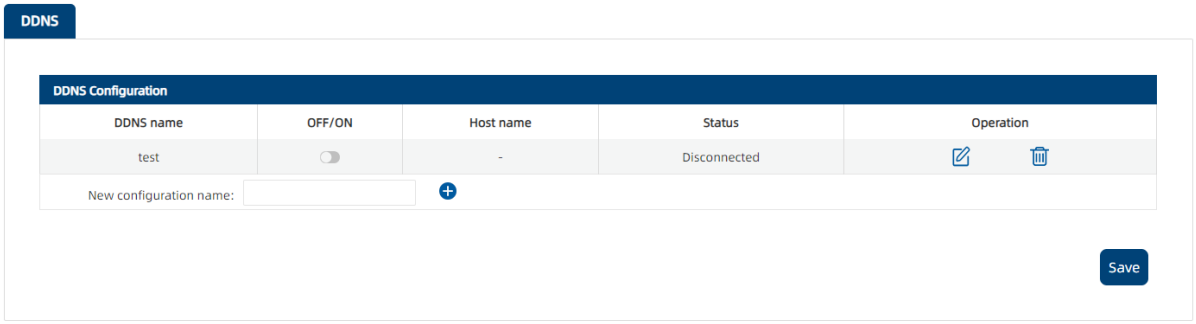
This function allows redirecting Modbus TCP data coming to a specified port to RTU specified by the Slave ID. Firstly, the device receives the data from a Modbus TCP master, then converts it into Modbus RTU data and redirect to the specified Slave ID.



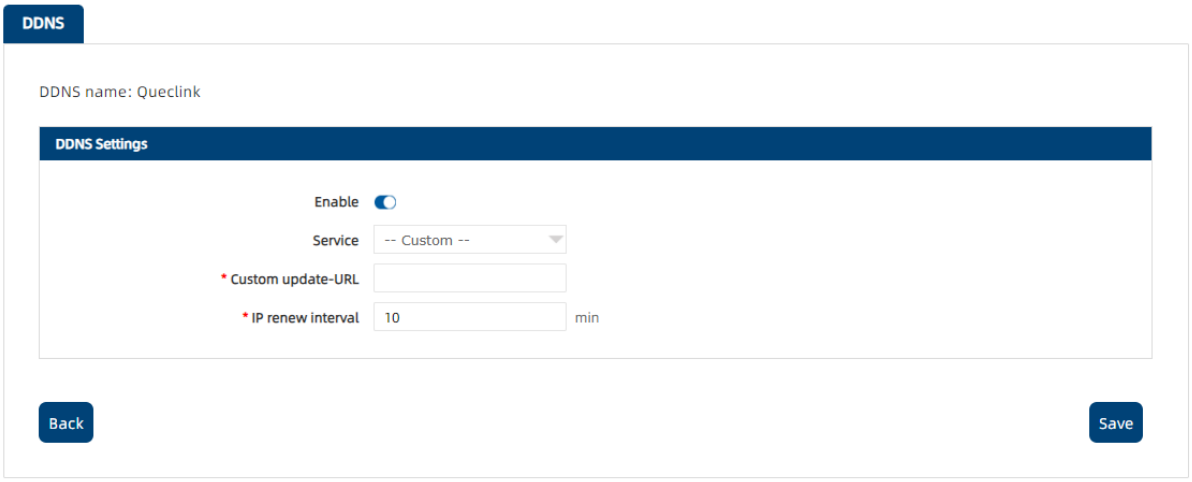
4.3.7 DDNS

Dynamic DNS (DDNS or DynDNS) is a method of automatically updating a name server in the Domain Name System (DNS). This is most often utilized when the end user has a dynamic IP address and wants to bind it to a static hostname.

The device is compatible with many different third party DNS services that provide the possibility to create a custom hostname and bind it to an IP address. The DDNS service periodically updates the IP address information of the hostname, making sure that the device remains reachable via the same hostname even in cases when its IP address has changed.



To configure a DDNS instance, click the Add icon button or the Edit icon of the existing instance. The figure below is an example of the edit page of the default DDNS instance:



Copyright © 2021 by Queclink Wireless Solutions.

Table 46: DDNS Configuration

Field Name	Value	Description
Enable	yes|no; Default: no	Turns the DDNS instance ON or OFF.
Service	third party DNS service (chosen from list*)|– custom –; Default: custom	Third party DNS service provider.
Hostname	host; Default: " "	Hostname that will be linked with the device's IP address.
Username	string; Default: " "	User name required to login to the third party DNS service; used to periodically login to your DNS service account and make necessary updates.
Password	string; Default: " "	Password required to login to the third party DNS service; used to periodically login to your DNS service account and make necessary updates.
IP renew interval	integer [5..600000]; Default: 10	Frequency at which the device will check whether its IP address has changed.

4.3.8 Input

All devices can support more than one digital or analog inputs. For example, WR310 has 4 input ports. This section is to provide the control on the input ports.

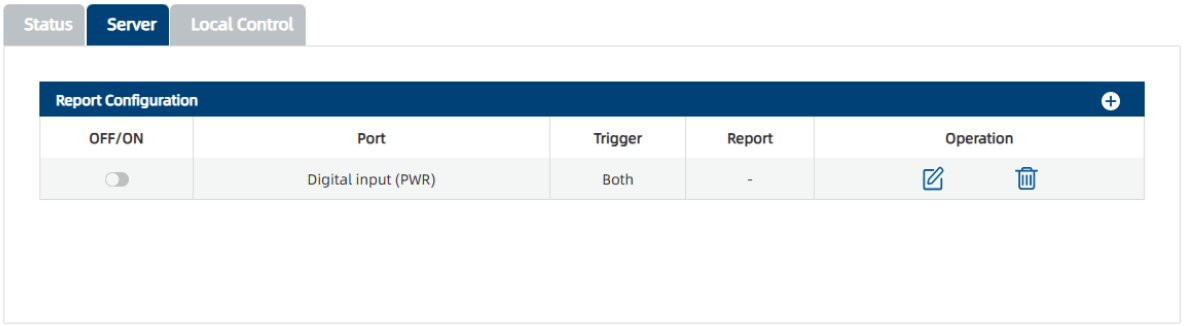
4.3.8.1 Status

The Status page displays the current states of the device's input ports,The definitions of different models are as follows:

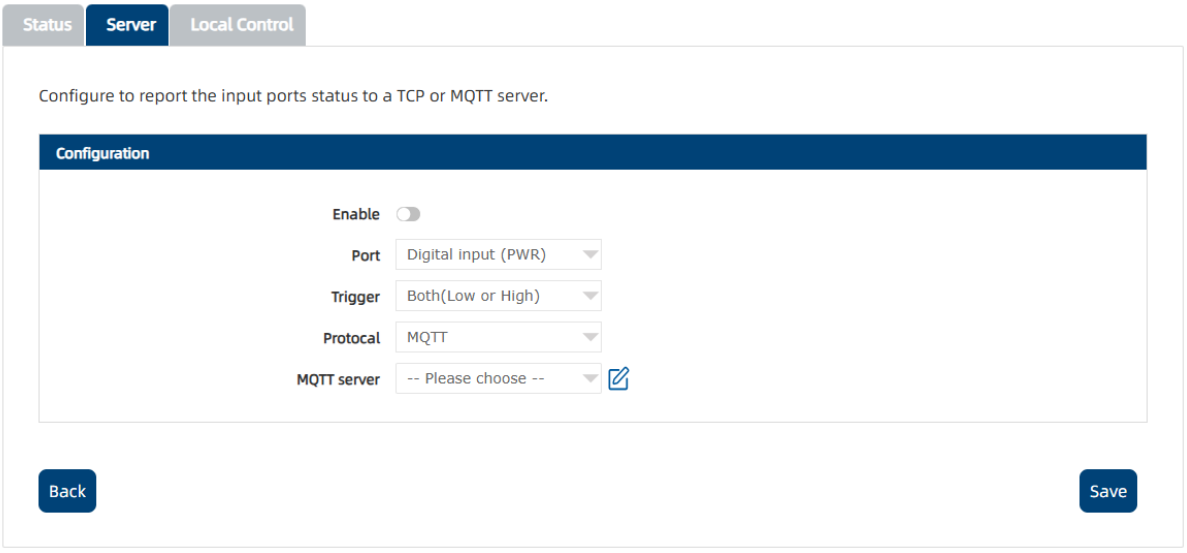


4.3.8.2 Server

The page provides a way to report an input event to a MQTT/TCP server. To add a new report, Click the Icon to enter the configuration page.



You can also configure an existing report by clicking Edit button.



The following table provides an explanation of each parameter.

Table 47: Input Rule Configuration

Field Name	Value	Description
Enable	yes|no; default: yes	Turns the input rule on or off.
Port	Digital Input|Digital isolated|Analog|Digital Input(PWR); default: Digital Input	Selects to which input pin the rule will apply.
Trigger	Both | Low level | High level; default: both Inside range | Outside range | Over max | Lower min; default: Inside range	Selects which input state will trigger the report.
Check interval	integer [1..9999]; Default: 0	The frequency at which the device will check for condition changes of the input port.
Min	integer [1..9999]; Default: 0	The minimum value to trigger a report.
Max	integer [1..9999]; Default: 0	The maximum value to trigger a report.
Protocol	MQTT|TCP; Default: MQTT	The protocol used for data transmission.
Server	String; default: none	Select a MQTT/TCP server to report the event.

The following is an example of a report generated by Routers to a MQTT server (in JSON format):

Table 48: Input Report Format

Field Name	Value	Description
time	String	The generation time of the report.
IMEI	String	The device's IMEI, used to identify unique devices.
rtn	String	Execution result. "success" indicates success; "fail" indicates failure.
port	String	Index of I/O port.
value	String	The value of this input port.

The following is an example of the report.

```
{"time":"2022-05-08 17:39:05", "IMEI":"863553065142923",
"rtn":"success", "port": "6", "value": "High level"}
```

MQTT servers can initiate a status query request to Routers to inquire about the status of I/O Ports.

The following is an example command for querying input status (in JSON format):

```
{"service":"0", "port": "6,8,5,12"}
```

Table 49: I/O Service Format

Field Name	Value	Description
service	String	Service number. Used to identify the corresponding service. 0 is I/O service.
port	String	Index of I/O port.

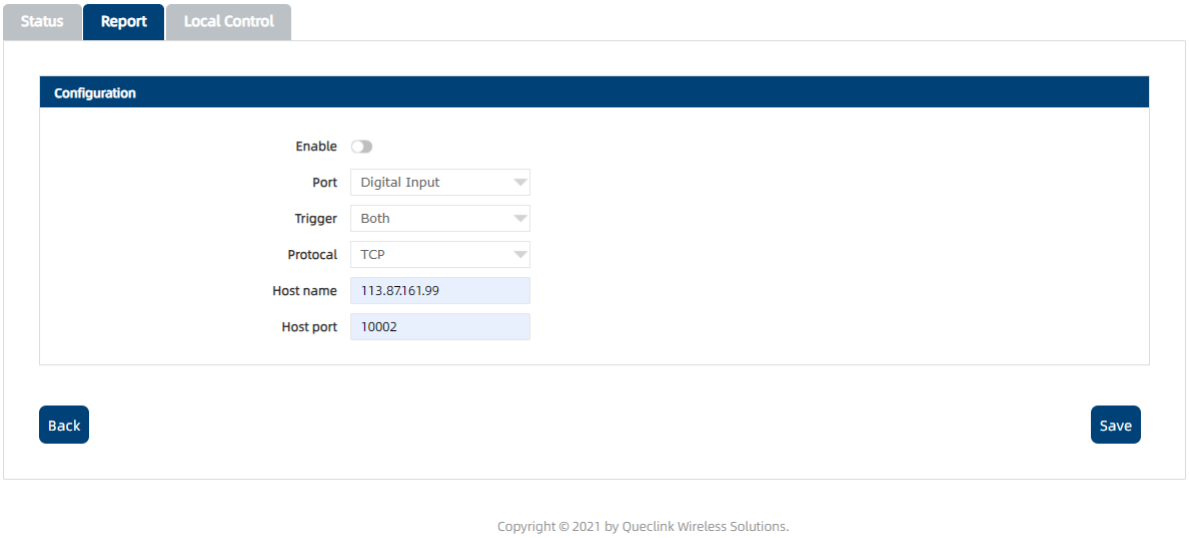
The following is the mapping table of port index, input port and value:

Queclink Confidential

Table 50: WR310 I/O Port Mapping

Port	IO	Value
11	Digital input (PWR)	Low level; High level

To forward the data to a TCP server, you must select Protocol as TCP.



The format from the device to a TCP server follows the MQTT format, but you need to add a starting symbol "@" and an ending symbol "$" in the reports.

The following is an example,

```
@{"time":"2022-05-08 17:39:05", "IMEI":"863553065142923",
"rtn":"success", "port": "6", "value": "High level"} $
```

A starting symbol "@" and an ending symbol "$" also need to be added in the querying I/O status command.

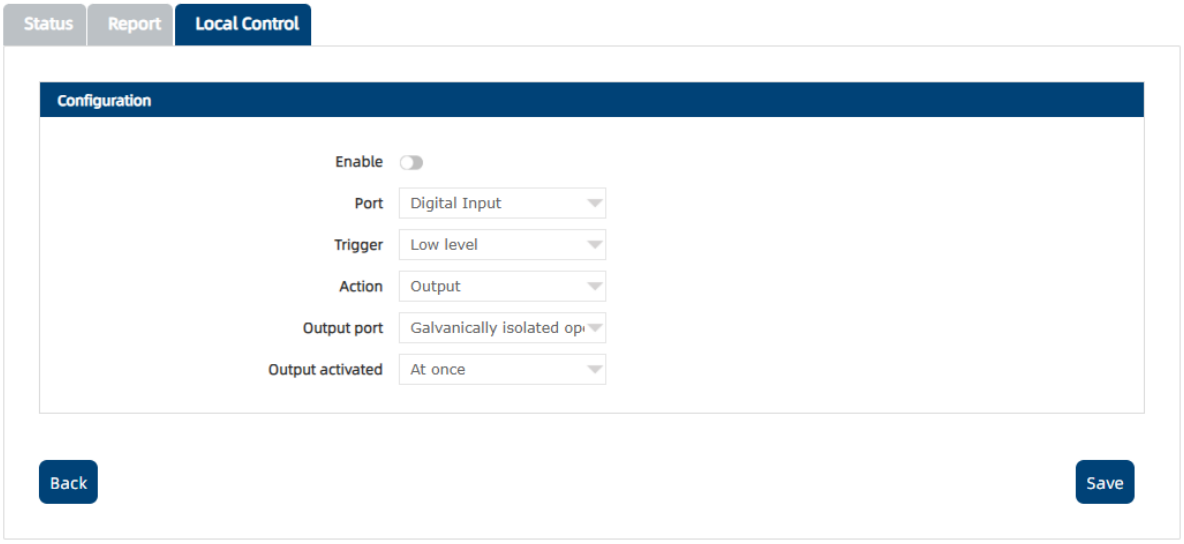
The following is an example,

```
@{"service":"0", "port": "6,8,5,12"}$
```

4.3.8.3 Local Control

"Local Control" is used to switch the Output on or off based on different states of the input port.

Queclink Confidential



Copyright © 2021 by Queclink Wireless Solutions.

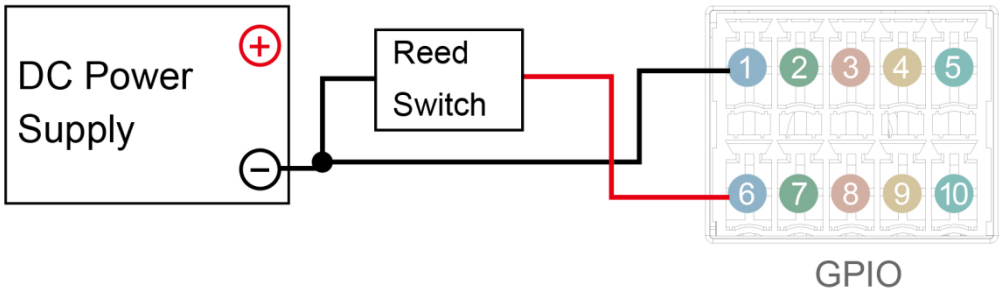
Table 51: Local Control Rule Configuration

Field Name	Value	Description
Enable	yes|no; default: yes	Turns the Local Control rule on or off.
Port	Digital Input|Digital isolated|Analog|Digital Input(PWR); default: Digital Input	Select which input pin the rule will apply.
Trigger	Both|Low level|High level; default: both Inside range|Outside range|Over max|Lower min; default: Inside range	Select which input state will trigger the report.
Min	integer [1..9999]; Default: 0	The minimum value to trigger a report.
Max	integer [1..9999]; Default: 0	The maximum value to trigger a report.
Output port	Galvanically isolated open collector output|Relay|Open collector output; Default: Galvanically isolated open collector output	Used to select the output port you want to control.
Output activated	At once|Second|Delayed action; Default: At once	Used to set the activated time for the output port. • **At once:** Activate the output port immediately when the input port switches to the set state. • **Second:** After the input port switches to the set state, activate the output port immediately and return it OFF after "second". • **Delayed action:** After the input port switches to the set state, enable the output port with a delay of "Trigger delay", keep it active for "Action stop", and then turn it off.

4.3.8.4 Application Example

- WR310 digital input can be used for security applications. You can connect a PIR sensor or reed switch to digital input. Then configure WR310 input.

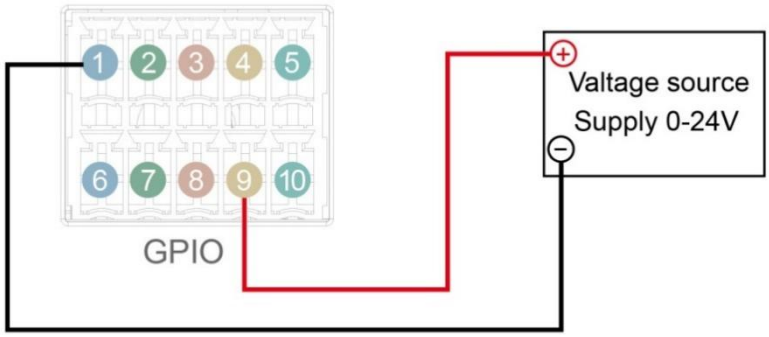
This is an example of how to connect digital input:



- Example of using WR310 digital isolated input:

Note: you can only connect passive sensors to digital input.

- If you want to measure the voltage with WR310, you need to connect the voltage source as the picture below. Note that voltage on pin 9 must never exceed 24V.

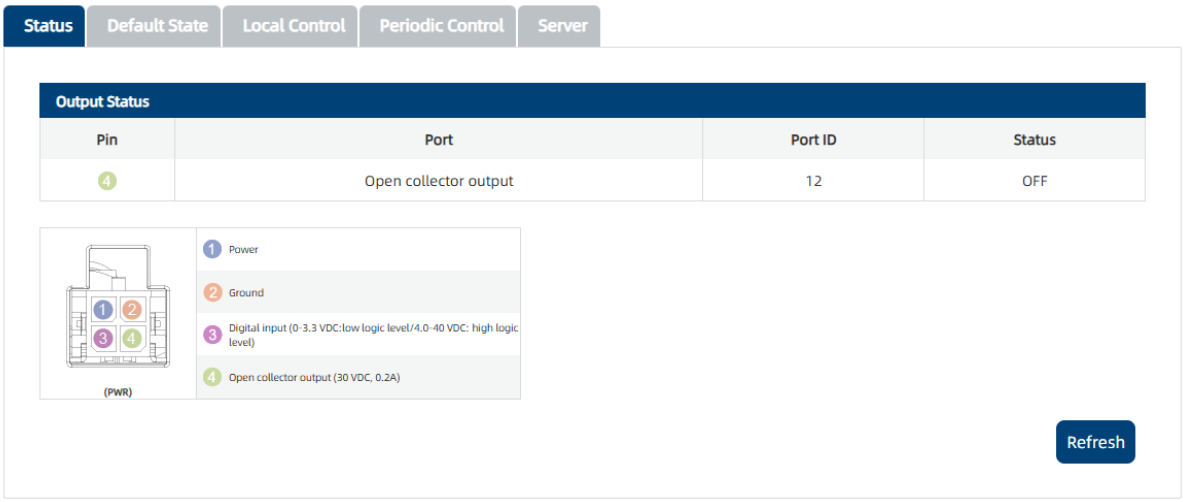


4.3.9 Output

All devices can support output,Different devices support different outputs. This section is to provide the control on the output ports.

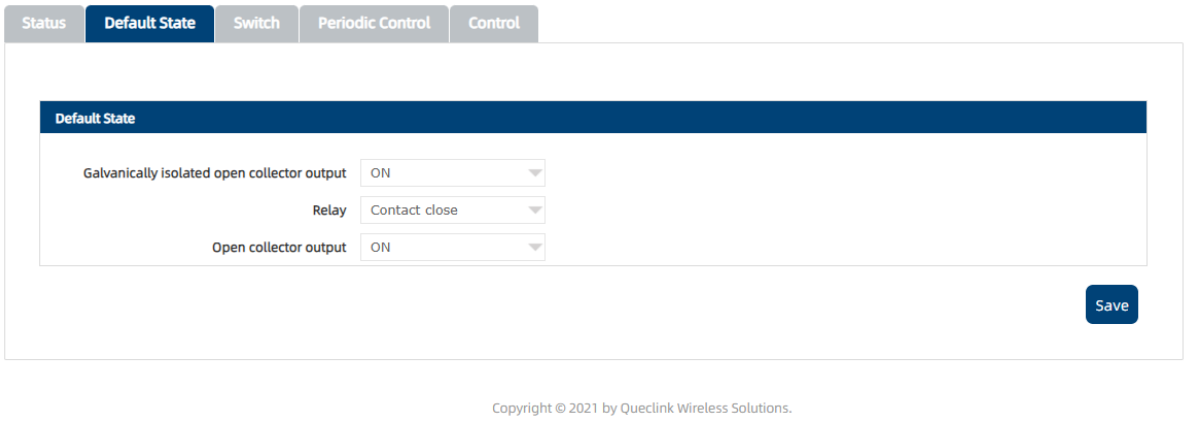
4.3.9.1 Status

The Status page displays the current states of the device's output ports:



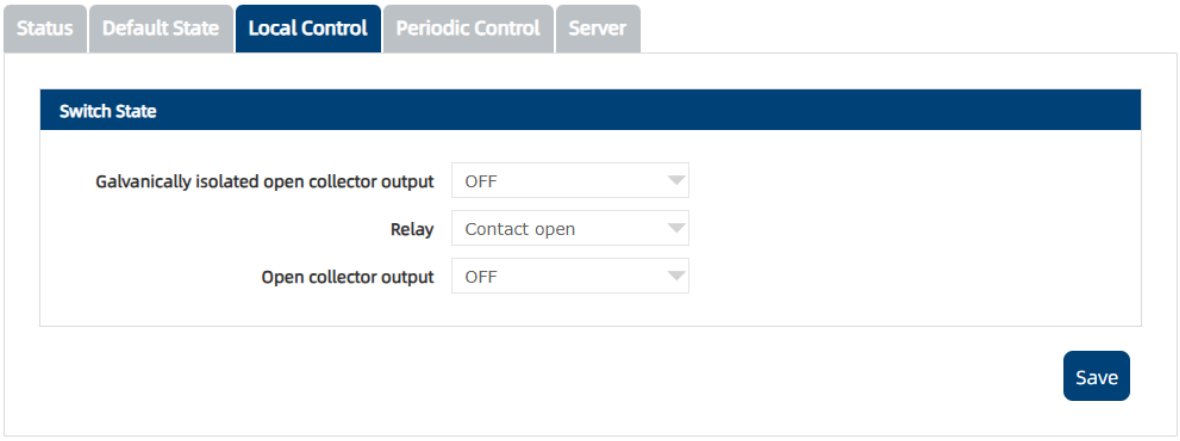
4.3.9.2 Default State

The page is to set the default state of the output ports when the device powers on. You can select specified state by the drop down menu.



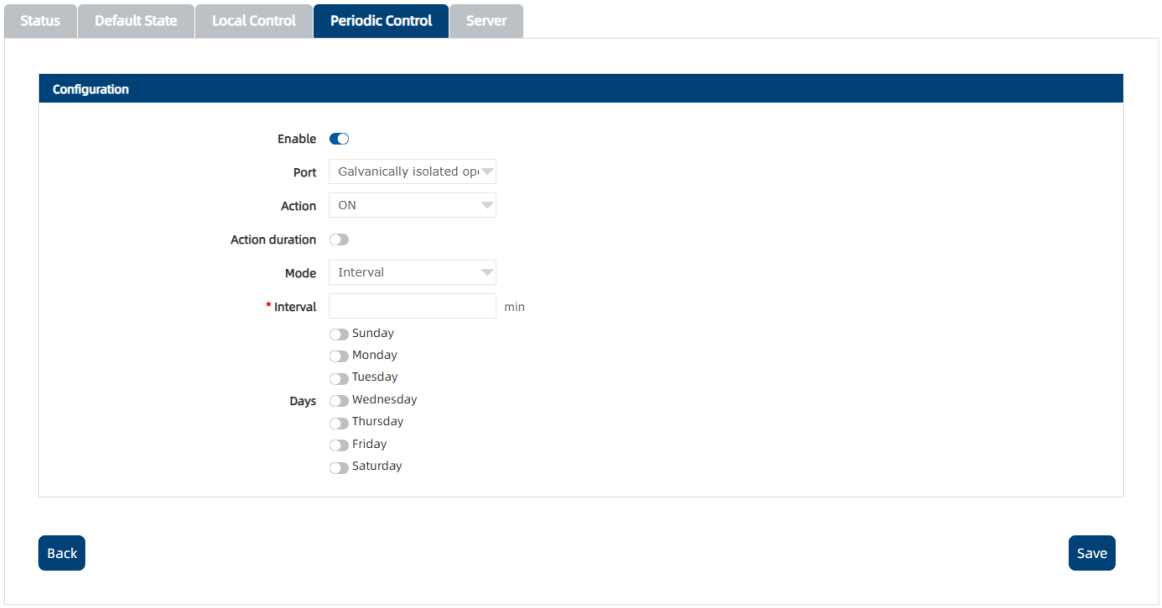
4.3.9.3 Local Control

The Local Control page is used to turn the device's outputs on or off manually. This action does not save the state permanently, meaning that after a reboot the states will revert back to their default values.



4.3.9.4 Periodic Control

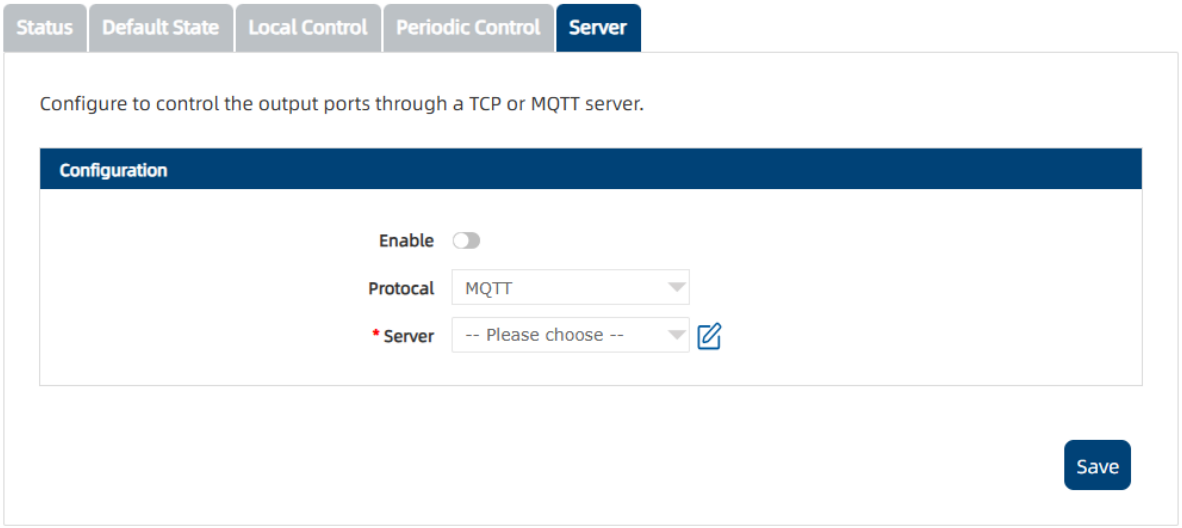
The periodic control can be used to configure a timetable of when an output should be turned on or off.



Field Name	Value	Description
Enable	yes|no; default: yes	Turns the Periodic Control rule on or off.
Port	Galvanically isolated open collector output|Relay|Open collector output (PWR); default: Galvanically isolated open collector output	Selects which output pin the rule will apply.
Action	ON|OFF|Contact open|Contact close; default: ON	The state of the selected output will be set to this value during the time interval defined in the fields below.
Action duration	yes|no; default: no	Turns the action duration rule on or off. When enabled, the output port will maintain the state you set for "Duration" and then revert back to its original state.
Duration	integer [1..86400]; Default: None	Duration of action time.
Mode	Interval|Fix; default: Interval	Selects the Mode to use.
Interval	integer [1..1440]; Default: None	Interval mode — the frequency at which the device will perform the action.
Hour	integer [0..23]; Default: 23	Fix mode — the hour of the day on which the device will perform the action.
Minute	integer [0..59]; Default: 0	Fix mode — the minute of the hour on which the device will perform the action.
Days	The minute of the hour on which the router will perform the action	The day or multiple days on which the device will perform the action.

4.3.9.5 Server

The page provides two ways to control the output port through MQTT and TCP servers.



The MQTT server sends control and query commands in JSON formatted messages.

Table 52: Output Control Command

Field Name	Value	Description
service	String	Service number. Used to identify the corresponding service. 0 is I/O service.
port	String	The index of the output port
value	String	Target control status

The following is the mapping table of index, output port and status:

Table 53: WR310 Output Port Mapping

Port	IO	Value
12	Open collector output	OFF; ON

The following is an example of a control message:

```
{"service": "0", "port": "8,5,12", "value": "OFF,Contact close,ON"}
```

The following is an example of query message:

```
{"service": "0", "port": "8,5,12"}
```

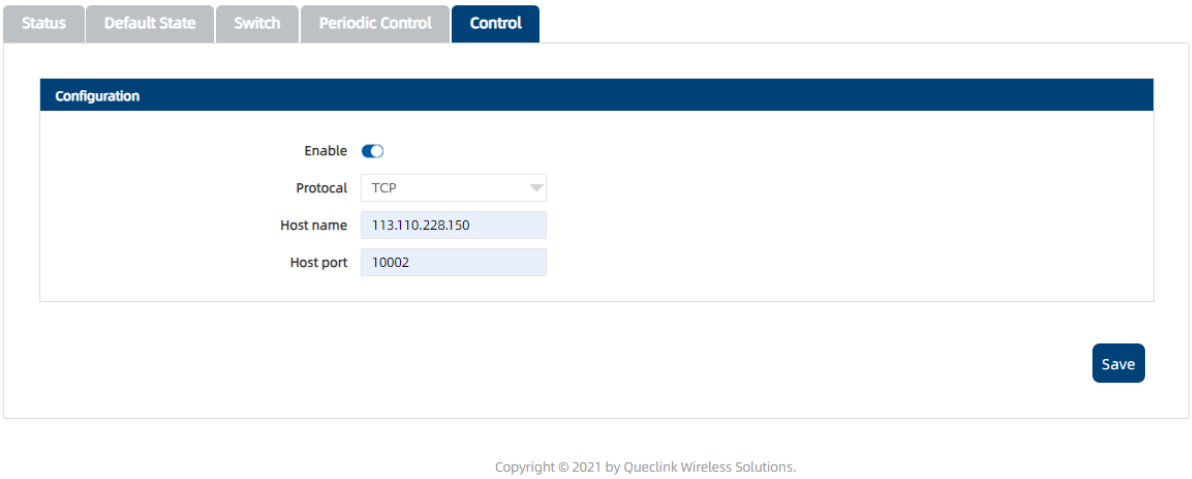
Return message format is:

Field Name	Value	Description
time	String	Acquisition time of the query.
IMEI	String	The device's IMEI, used to identify unique devices.
rtn	String	The execution result. "success" means successful; "fail" means failure.
port	String	The index of the output port.
value	String	Target control status.

The following is an example of responses,

```
{"time":"2022-05-08 17:39:05", "IMEI":"863553065142923",
"rtn":"success", "port": "8,5,12", "value": "OFF,Contact close,ON"}
```

To forward the data to TCP server, you must select Protocol as TCP.



The message format follows the MQTT format, a starting symbol "@" and an ending symbol "$" need to be added in the message.

The following is an example of control messages:

```
@{"service": "0", "port": "8,5,12", "value": "OFF,Contact close,ON"}$
```

The following is an example of query messages:

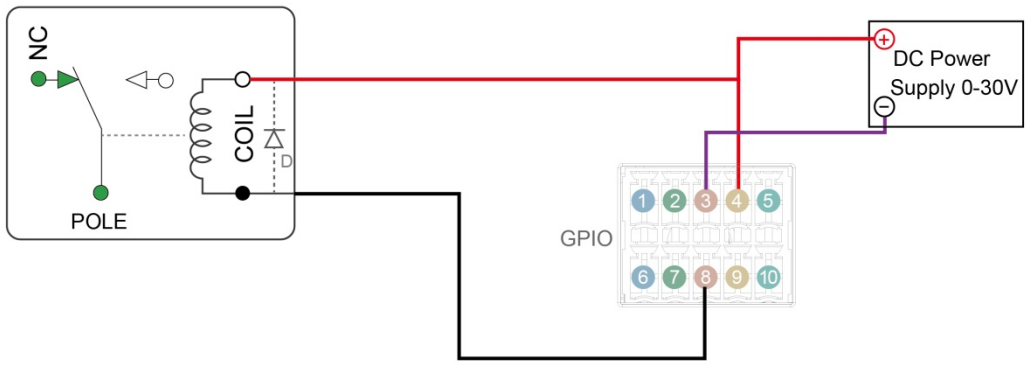
```
@{"service": "0", "port": "8,5,12"}$
```

The following is an example of return messages:

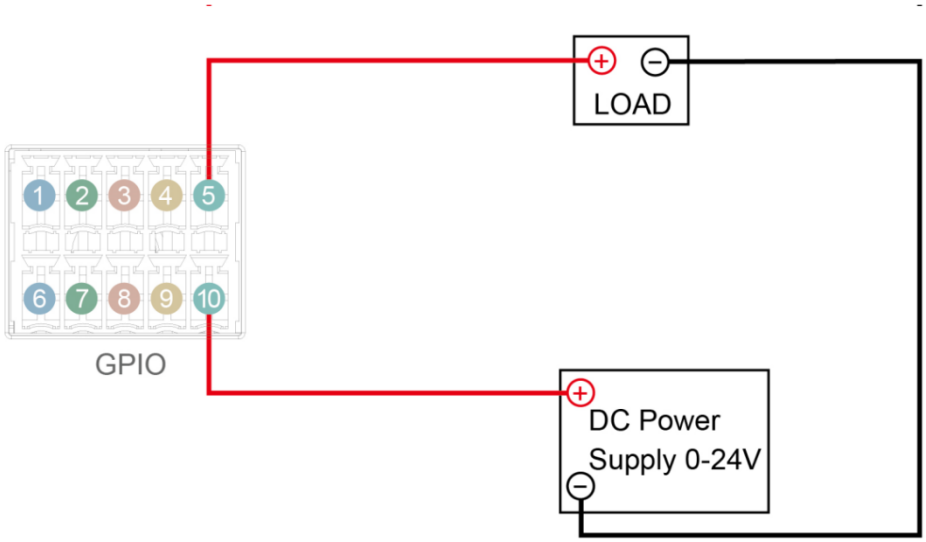
```
@{"time":"2022-05-08 17:39:05", "IMEI":"863553065142923",
"rtn":"success", "port": "8,5,12", "value": "OFF,Contact close,ON"}$
```

4.3.9.6 Application Example

- This is an example on how to connect a relay to WR310 galvanically isolated open collector output:



- In some cases, you may want WR310 release to automatically press the key to turn on the high-power load, which can be connected according to the following figure:

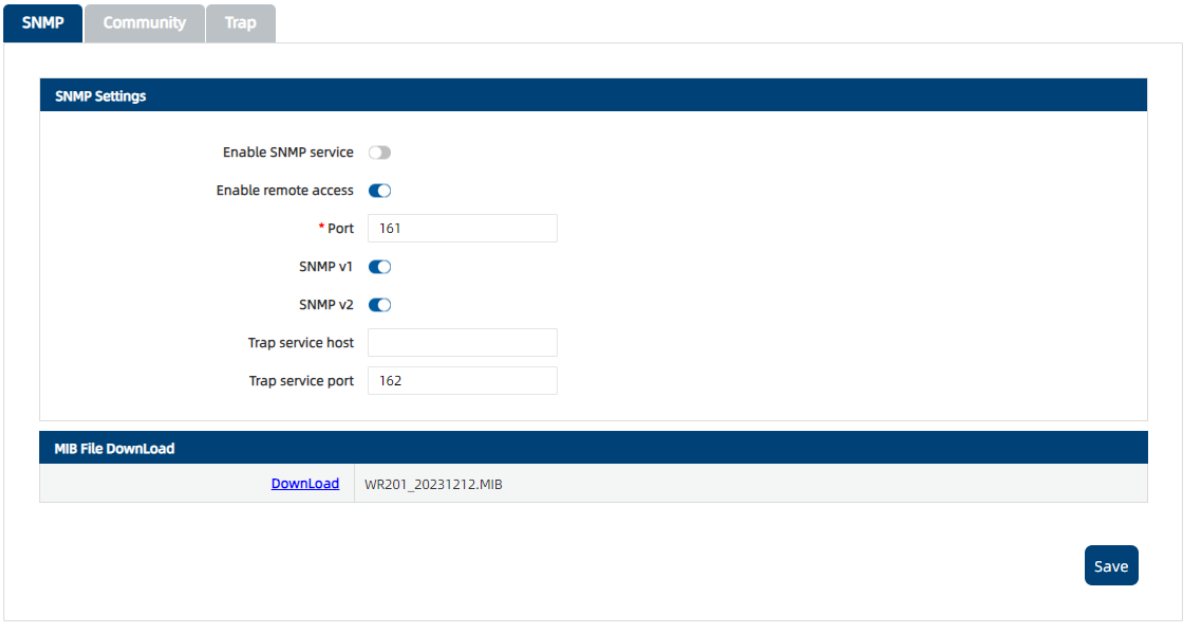


4.3.10 SNMP

Simple Network Management Protocol (SNMP) is a network management protocol used for collecting information and configuring network devices.

4.3.10.1 SNMP

The SNMP settings page is used to configure SNMP connectivity and general SNMP information for your device.



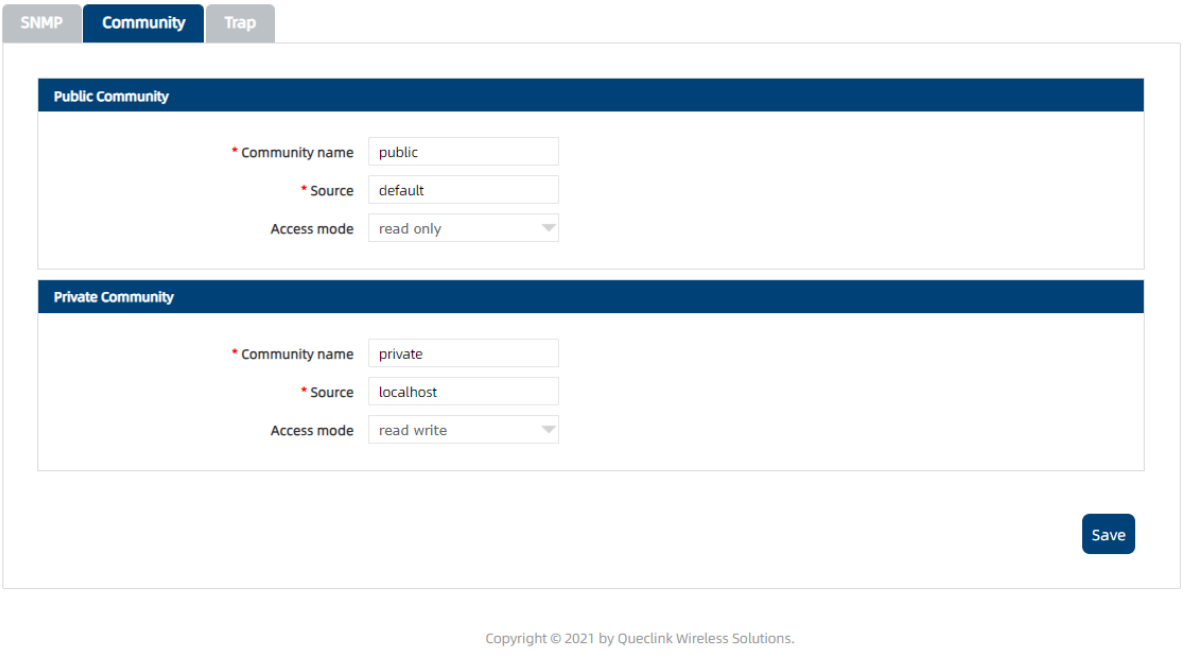
Copyright © 2021 by Queclink Wireless Solutions.

Table 54: SNMP Service Configuration

Field Name	Value	Description
Enable SNMP service	off | on; default: off	Enable/disable SNMP service.
Enable remote access	off | on; default: on	Open port in firewall so that SNMP service may be reached from WAN.
Port	integer [0..65535]; default: 161	SNMP service's port.
SNMP v1	off | on; default: on	Enable/disable SNMP v1 Mode.
SNMP v2	off | on; default: on	Enable/disable SNMP v2 Mode.
Trap service host	url | ip; default: none	Hostname or IP address to transfer SNMP traffic to.
Trap service port	integer [0..65535]; default: 162	Trap host's port number.

4.3.10.2 COMMUNITY

The Community page is used to manage SNMP access rights.



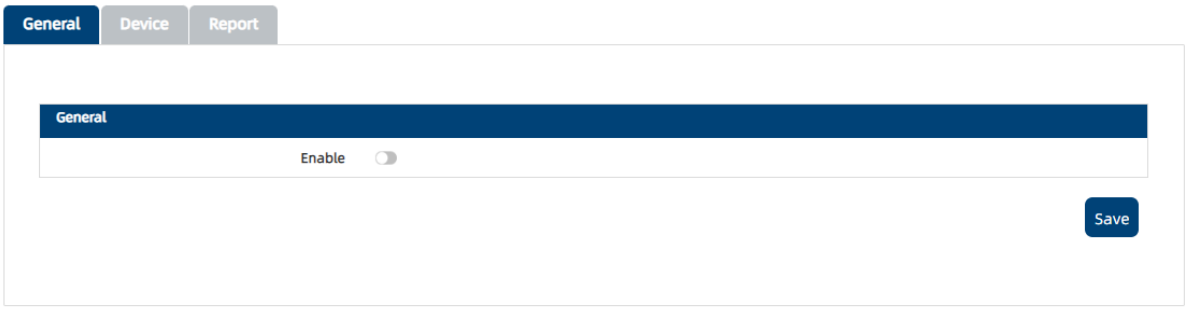
Field Name	Value	Description
Community name	string; default: public	Name of the community.
source	ip; default: default	IP address of the community.
Access Mode	read-only|read-write; default: read-only	Access mode for current community.
Community name	string; default: private	Name of the community.
source	ip; default: localhost	IP address of the community.
Access Mode	read-only|read-write; default: read-only	Access mode for current community.

4.3.11 iTracker

The Tracker section is used to configure the device to send GNSS reports with Queclink 2nd Generation Tracker Protocol. Please contact our FEA engineers to get the document of the protocol.

4.3.11.1 General

The General is used to enable or disable tracker function. Before using the tracker, you must turn it on first (off by default).

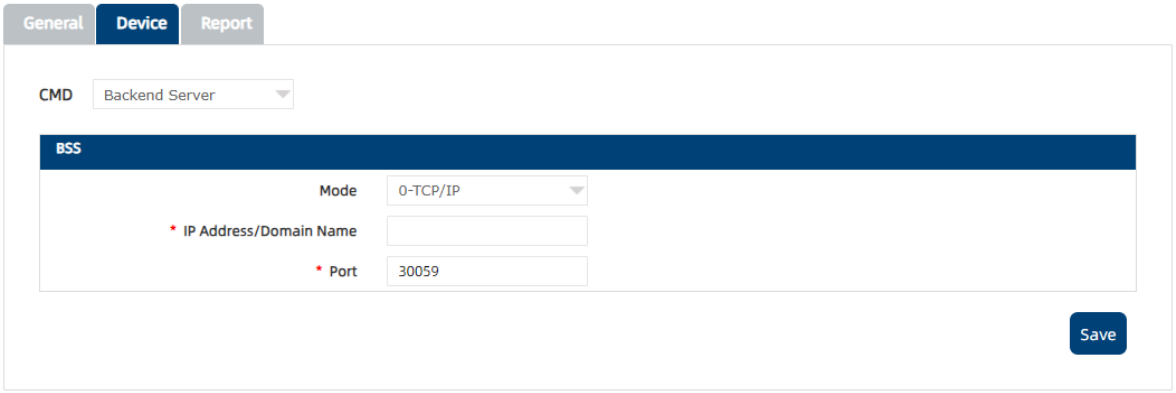


Copyright © 2021 by Queclink Wireless Solutions.

4.3.11.2 Device

The Device page is used to configure Backend Server /Acknowledgement and Heartbeat information for Tracker. You can click CMD drop-down button to display and configure the parameters. The content will change according to which CMD is selected.

Backend Server is used to configure the IP address (or domain name) and port of the backend server, Transmission Mode, etc.

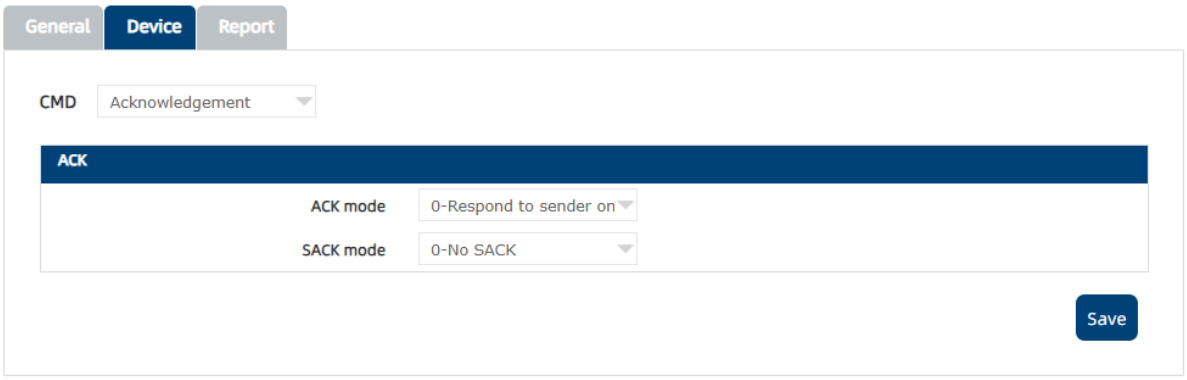


Copyright © 2021 by Queclink Wireless Solutions.

Table 55: Communication Configuration

Field Name	Value	Description
Mode	0-TCP/IP|1-UDP/IP; default:0-TCP/IP	Specifies the protocol used in the communication process.
IP Address/Domain Name	ip|host; default: none	The IPv4/IPv6 address or domain name of the backend server.
Port	integer [0..65535]; default:none	The port of the backend server.

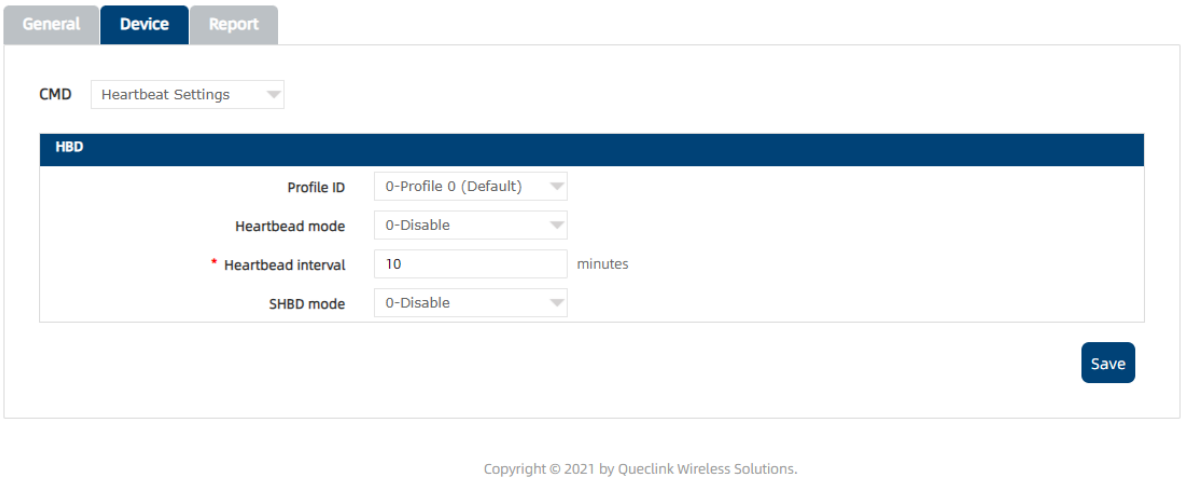
Acknowledgement is used to configure the ACK and SACK features.



Copyright © 2021 by Queclink Wireless Solutions.

Field Name	Value	Description
ACK mode	0-Respond to sender only|1-Respond to sender and backend server; default: 0-Respond to sender only	• 0 - Respond to sender only. The terminal receives the command from which physical path (for example, Cellular Network, SMS, RS232.), and replies the ACK (or NACK) only from which physical path. • 1 - Respond to sender and backend server. The terminal receives the command from which physical path (for example, Cellular Network, SMS, RS232.), and replies the ACK (or NACK) from which physical path. At the same time, if the legal command is not received from the backend server, the terminal will reply an ACK (or NACK) to the server to inform the server.
SACK mode	0-No SACK|1-With SACK. And device will check the serial number in the SACK|2-With SACK. But device won't check the serial number in the SACK; default: 0-No SACK	• 0 - The backend server does not reply a SACK frame after receiving a report from the terminal. • 1 - The backend server not only replies a SACK frame after receiving a report from the terminal but also requires the device to check the serial number in the SACK frame. • 2 - The backend server replies a SACK frame after receiving a report from the terminal, but does not require the device to check the serial number in the SACK frame.

Heartbeat Settings is used to configure the HBD and SHBD feature.

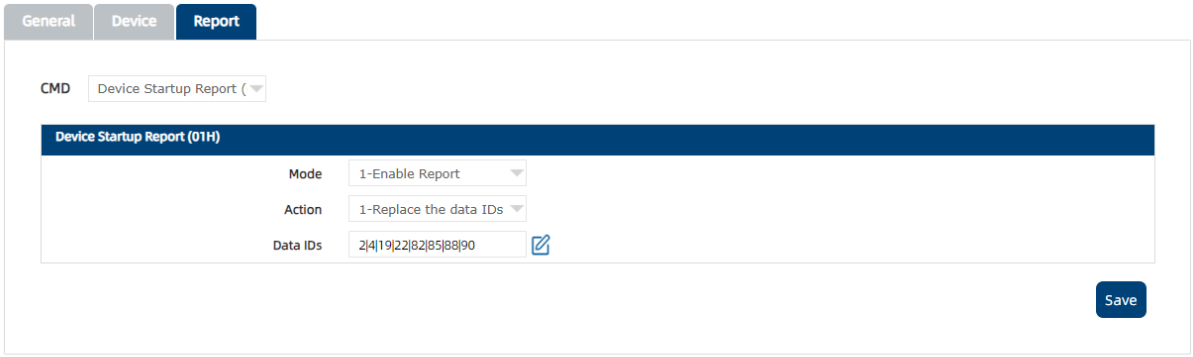


Field Name	Value	Description
Profile ID	0-Profile 0 (Default)	Specify the associated profile ID.
Heartbeat mode	0 - Disable|1 - Enable (periodic)|2 - Enable (aperiodic); default: 0 - Disable	• 0 - Disable. The terminal does not send the HBD frame to the backend server. • 1 - Enable (periodic). The terminal will periodically send the HBD frame to the backend server according to “Heartbeat Interval”. • 2 - Enable (aperiodic). Only when the terminal has not sent any information to the backend server within the time indicated by “Heartbeat Interval”, the terminal will send the HBD frame to the server.
Heartbeat Interval	integer [3..99]; default: 161	The interval for the terminal to send the HBD frame to the backend server.
SHBD Mode	0 - Disable|1 - Enable; default: 0 - Disable	• 0 - Disable. The backend server has no need to reply the SHBD frame after receiving the HBD frame from the terminal. • 1 - Enable. The backend server needs to reply the SHBD frame after receiving the HBD frame, and the terminal will diagnose its connection status with the backend server according to the SHBD frame.

4.3.11.3 Report

Report refers to the frame that the terminal device actively generates and sends to the backend server when it reaches certain established conditions. This page is used to configure the following reports: Device Startup Report (01H),Connection Starts Report (03H),Device Basic Information Report (11H),Real-time Location Report (12H), and Fixed Report (50H).

Queclink Confidential



Copyright © 2021 by Queclink Wireless Solutions.

Field Name	Value	Description
CMD	Device Startup Report (01H)|Connection Starts Report (03H)|Device Basic Information Report (11H)|Real-time Location Report (12H)|Fixed Report (50H); default: Device Startup Report (01H)	Select the report to configure.
Mode	0 - Disable|1 - Enable Report| 11 - Enable Report (Location first)| 12 - Enable Report (Event first); default:1 - Enable Report	• 0 - Disable. The terminal no longer generates and sends the record. • 1 - Enable Report. The terminal generates and sends the record. If the location information needs to be included, the terminal directly uses the currently existing location information (even if the location information has expired). • 11 - Enable Report (Location first). The terminal generates and sends the record, if the location information has expired, wait for real-time positioning before generating. If waiting for the real-time positioning timeout, the last valid position information will be used. • 12 - Enable Report (Event first). In order to report the event in time, the terminal immediately generates and sends a report. If the location information contained in this sent report has expired, the terminal will wait for real-time positioning, then generate and send one more report (Note: To distinguish between the two reports, the highest bit of the event code for the appended report is set to 1, i.e. plus 80H).
Data IDs	Varies depending on the report	The data IDs contained in the record.
Time interval	integer [0,10..86400]; Default: 600	Time interval

Queclink Confidential

4.3.12 Hotspot

A hotspot is a physical location where people can access the Internet, using Wi-Fi, via a wireless local area network (WLAN) with a device connected to an Internet service provider.

Queclink router can configure a Hotspot service that provides authorization and accounting for a network. This chapter describes how to configure a WIFI hotspot.

4.3.12.1 General

The General page displays the created instance and its major parameters. By default, a Hotspot instance does not exist on the device. To create a new instance:

Input a hotspot name and click the 'Add' button. A new Hotspot configuration page will appear as figure below.

Users have three options to create a Hotspot:

(1) Local Configuration

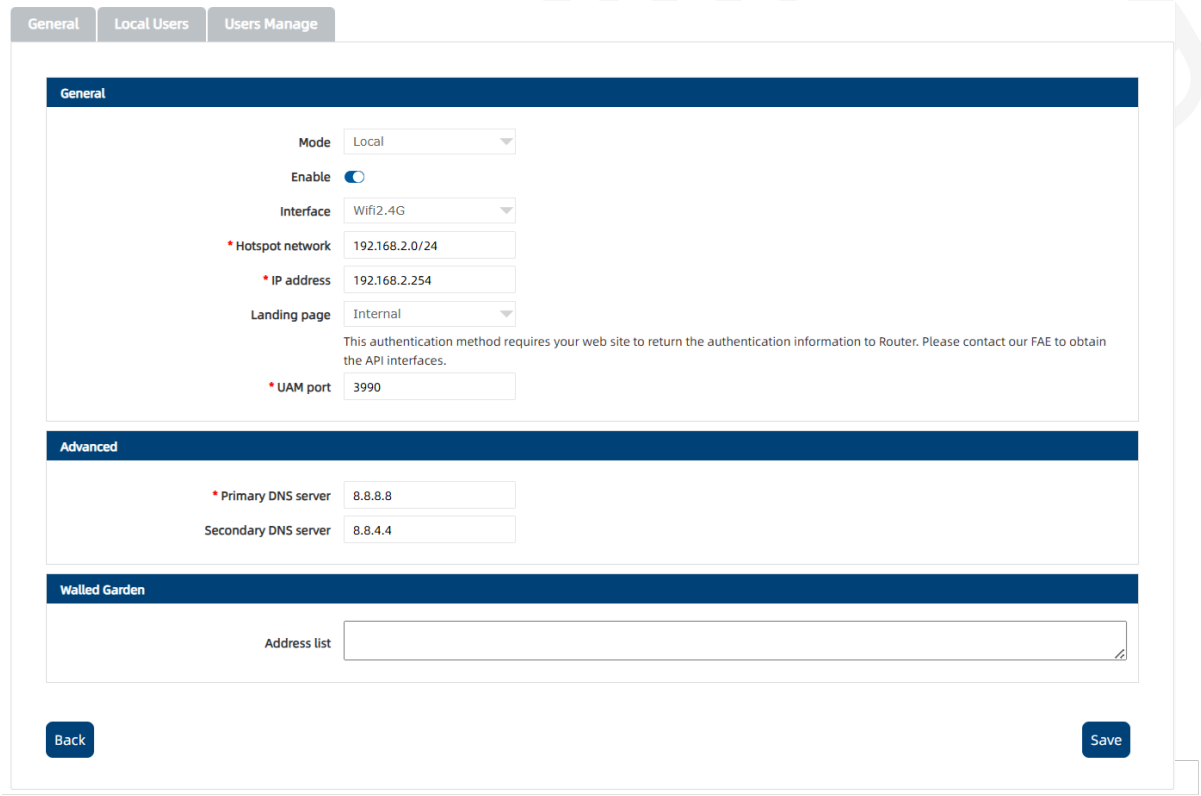
Create a local Hotspot using pre-configured parameters and authenticate via locally configured users.

(2) RMS (Nebulink System)

Create a Hotspot through Nebulink on RMS and push the configuration to the device.

(3) Radius Server

Create a Hotspot with configured parameters and use a pre-configured Radius server for authentication.

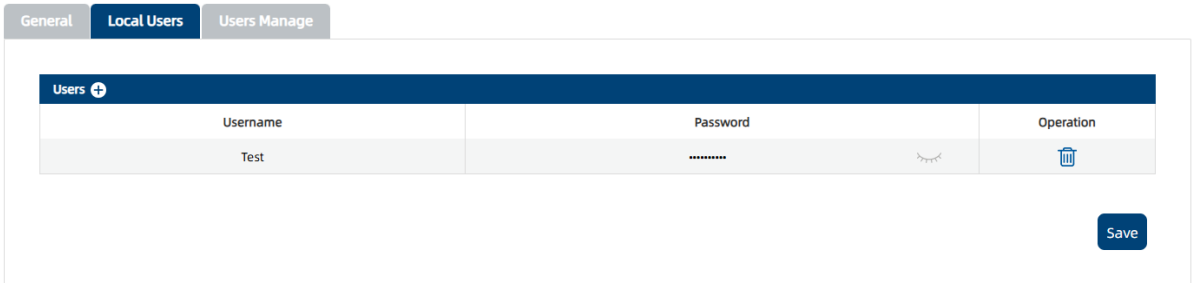


Field Name	Value	Description
Mode	Local|RMS|Radius; default: Local	Local: Configure a local Hotspot with parameters and the Portal specified by local parameters. Authenticate through the locally configured users. • RMS: Configure a Hotspot on Nebulink system and apply it to the device remotely. • Radius: Configure a local Hotspot with parameters and the Portal specified by local parameters. Authenticate through a configured Radius server.
Enable	off | on; default: on	Turns the Hotspot instance on or off.
Interface	Wifi2.4G|Wifi5G	Interface to provide hotspot service.
Hotspot Network	ip/netmask; default: 192.168.2.0/24	IP address and subnet of the Hotspot network.
IP Address	ip; default: 192.168.2.254	Defines the IP address of your Hotspot in network.
Authentication mode	Local user; default: Local users	Authentication mode defines how users will connect to the Hotspot.
Landing Page	Internal | External; default: Internal	If External Landing Page is chosen, a new section (website address) will appear, e.g., http://www.example.com
Radius server1	ip; default: none	The IP address of the RADIUS server 1 that is to be used for authenticating the clients.
Radius server2	ip; default: none	The IP address of the RADIUS server 2 that is to be used for authenticating the clients.
Authentication/Authorization port	integer [0..65535]; default: 1812	RADIUS server authentication port.
Accounting port	integer [0..65535]; default: 1813	RADIUS server accounting port.
NAS coa port	integer [0..65535]; default: 3799	RADIUS server NAS coa port.
NAS identifier	string; default: none	NAS-Identifier is one of the basic RADIUS attributes.
Radius secret key	string; default: none	The secret key is a password used for authentication with the RADIUS server.
UAM Port	integer; default: 3990	Port to bind for authenticating clients.
DNS server 1	ip; default: 8.8.8.8	Additional DNS servers that are to be used by the Hotspot.
DNS server 2	ip; default: 8.8.4.4	Additional DNS servers that are to be used by the Hotspot.
Walled Garden	default: empty	A list of addresses that users connected to the Hotspot will be able to reach without any authentication.

4.3.12.2 Local Users

The Local Users page is used to create and manage users that can connect to the Hotspot. To add a local user:

Click the 'Add' icon to create a new user instance, enter a Username and Password, and then click the 'Save' button to apply the changes.



Confidential

4.3.12.3 User Manage

User Management allows users to monitor and manage Hotspot users. Users can view the status of connected clients and disconnect any user.

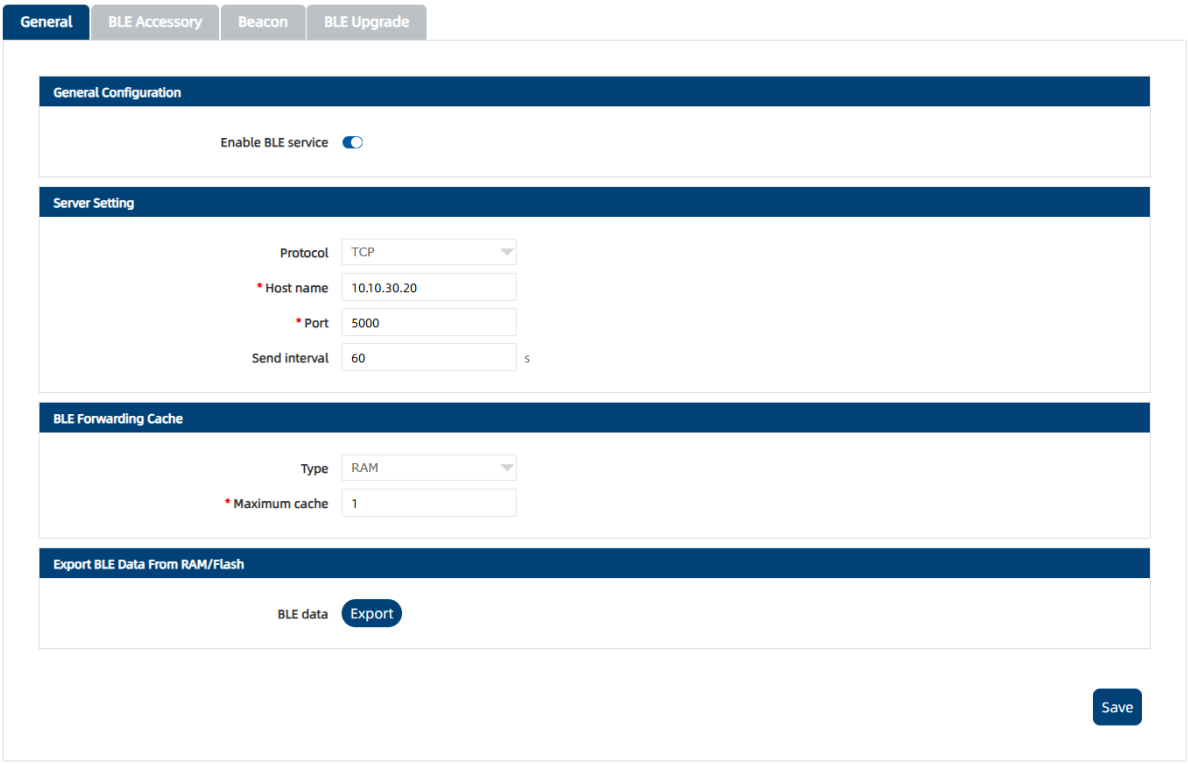
4.3.13 BLE (Available for some Models Only)

Some router models are equipped with BLE (Bluetooth Low Energy) functionality. This feature allows customers to connect BLE terminals such as temperature&humidity sensors through the router, as well as standard BEACON devices. It also enables the router to forward data from the sensors or BEACON devices to a platform.

4.3.13.1 General

The General section is used to configure the general setting of the BLE. On this page, users can enable and disable BLE, configure a server to receive the reports from BLE or Beacon.

The device caches BLE reports forwarding information.The Forwarding Cache section is used to select the memory type where the cache will be stored and the maximum amount of data that will be saved.

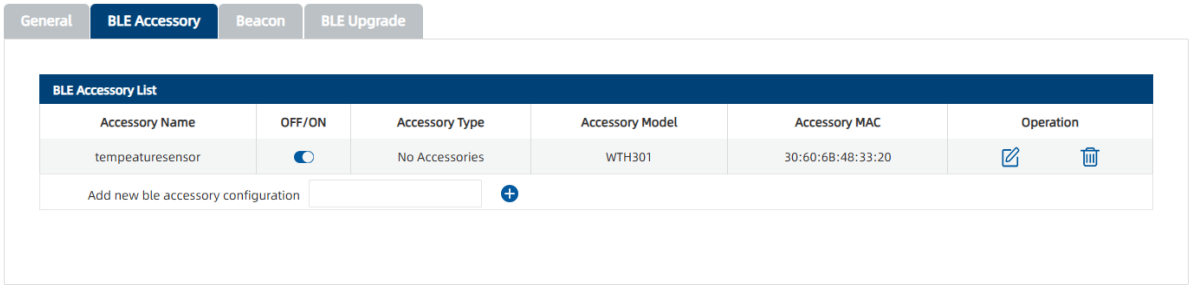


Field Name	Value	Description
Enable	off | on; default: on	Turns the BLE module on or off.
Protocol	TCP|UDP|MQTT; default: TCP	Protocol that will be used to send NMEA data.
Host name	ip|host; default: 192.168.1.5	IP address or hostname of the server to which BLE reports will be forwarded.
Port	integer [0..65535]; default: 8500	Port number of the server to which BLE reports will be forwarded.
Send Interval	integer [1..9999]/; default: 30	Interval (in seconds) at which the device forwards the BLE reports.

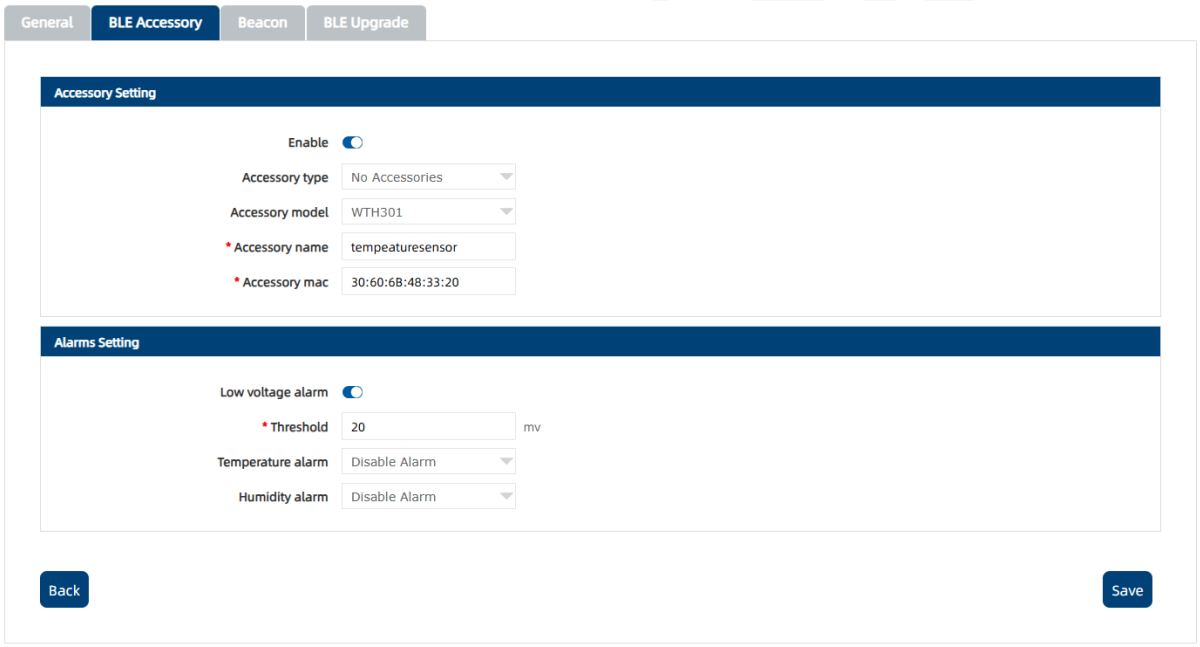
The device caches BLE reports if BLE report is enabled and there are BLE accessories connected to the device. This section is used to select the memory type where the cache will be stored and the maximum amount of data that will be saved.

4.3.13.2 BLE Accessory

The BLE Accessory page allows you to configure BLE accessories for device connection. To add a new accessory, enter a device name and click the Add Icon to navigate to the configuration page. Users can also use the Edit and Delete icons to modify or remove existing instances.



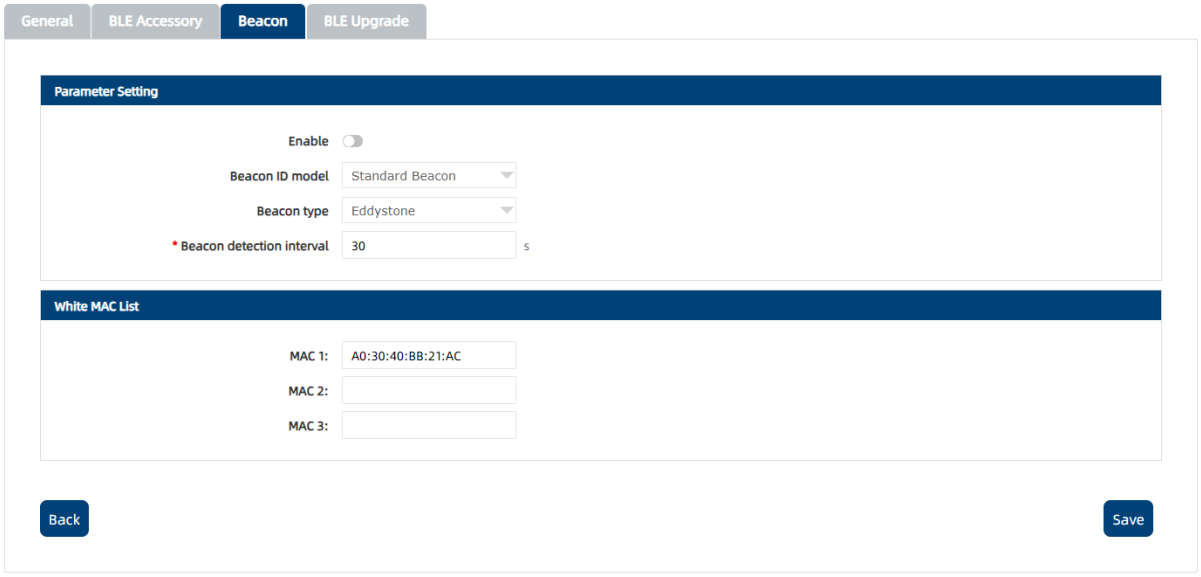
On the accessory configuration page, you can select an accessory from the list of supported devices and configure its MAC address and other parameters.



Field Name	Value	Description
Enable	off	on; default: on	Turns the BLE accessory on or off.
Accessory Type	No Accessories| Beacon Multi-Functional sensor	Select the BLE accessory type.
Accessory model	WTH301| WMS301| WID330	Select a BLE accessory model from the list of all supported models. For detailed accessory information, please contact our technical engineers.
Accessory name	String	Input a name for the accessory.
Accessory mac	mac; Default: none	MAC address of the BLE accessory
Low voltage alarm switch	off	on; default: off	Turns the low voltage alarm on or off. When the battery level of the BLE accessory is lower than the configured threshold, the device will send an alarm to the server.
Temperature alarm	Disable alarm| Report once exit/enter	Switches the temperature alarm on or off and selects the alarm trigger.
Low temperature	integer [-40-80]; default: none	Set the lower temperature of the temperature range.
High temperature	integer [-40-80]; default: none	Set the higher temperature of the temperature range.
Temperature validity	integer [1..9999]; default: 30	The validity period of the temperature refers to the duration in which the temperature must be maintained for longer than this validity period for the alarm to be triggered.
Humidity alarm	Disable alarm| Report once exit/enter	Switches the humidity alarm on or off and selects the alarm trigger.
Low humidity	integer [-40-80]; default: none	Set the lower humidity of the temperature range.
High humidity	integer [-40-80]; default: none	Set the higher humidity of the temperature range.
Humidity validity	integer [1..9999]; default: 30	The validity period of the humidity refers to the duration in which the humidity must be maintained for longer than this validity period for the alarm to be triggered.

4.3.13.3 Beacon

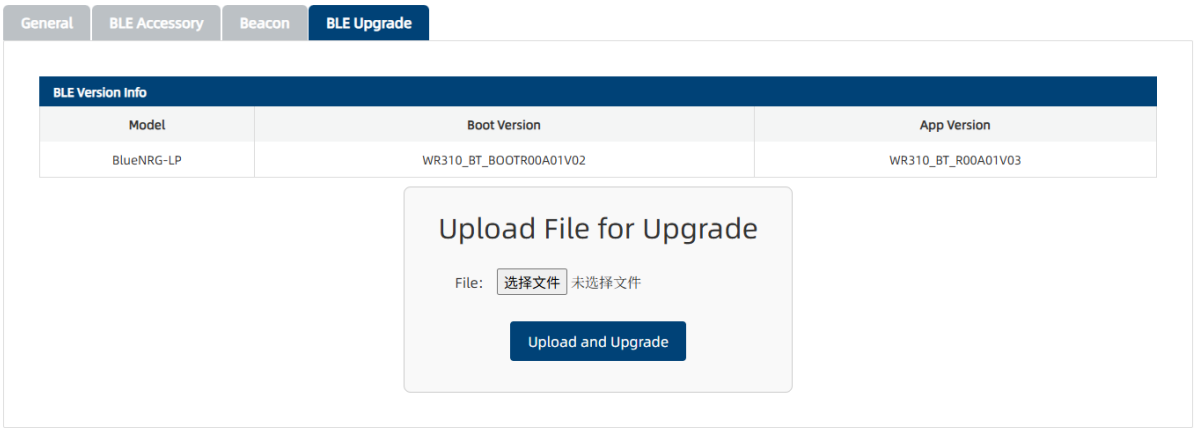
The Beacon page allows you to configure multiple BLE Beacons can be connected by the device.



Field Name	Value	Description
Enable	off | on; default: on	Turns the BLE accessory on or off.
Beacon ID model	Standard Beacon	Beacon ID model.
Beacon type	iBea-conlEddystoneliBeacon or Eddystone	Select the type of iBeacon. Currently only support iBeacon and Eddystone.
Beacon detection interval	integer [1..99]; default: 30	The interval for detecting each configured beacon.
MAC X	mac; Default: none	MAC address of the Beacon

4.3.13.4 BLE Upgrade

BLE upgrade page is for you to upgrade the software of the BLE chip. Click Browse button to select the new software from your computer and click “Upload and Upgrade” to upgrade the software. During the upgrade, please do not power off the router. After upgrade finished, the software version will be renewed. The whole upgrade process will take 30 seconds.



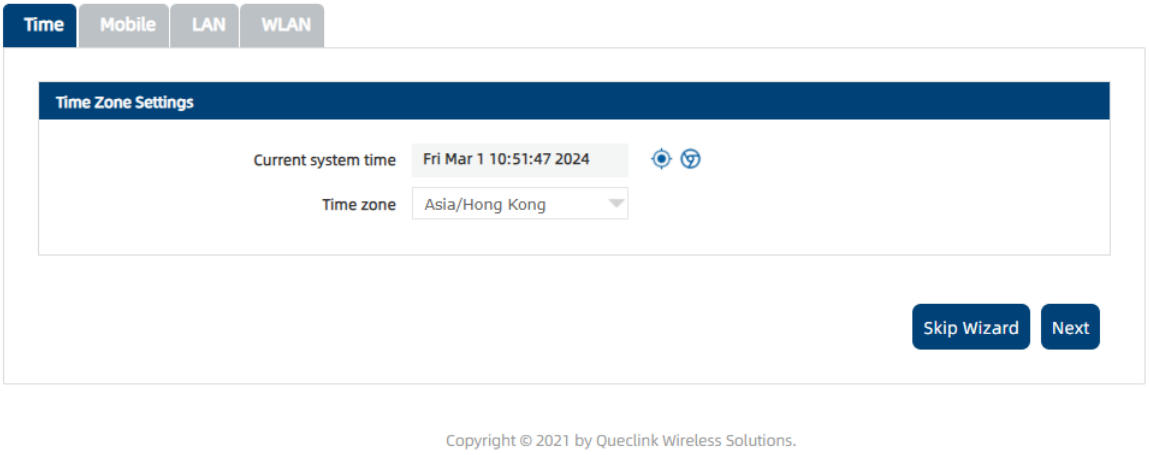
4.4 System

This section shows you how to configure the system settings of the device.

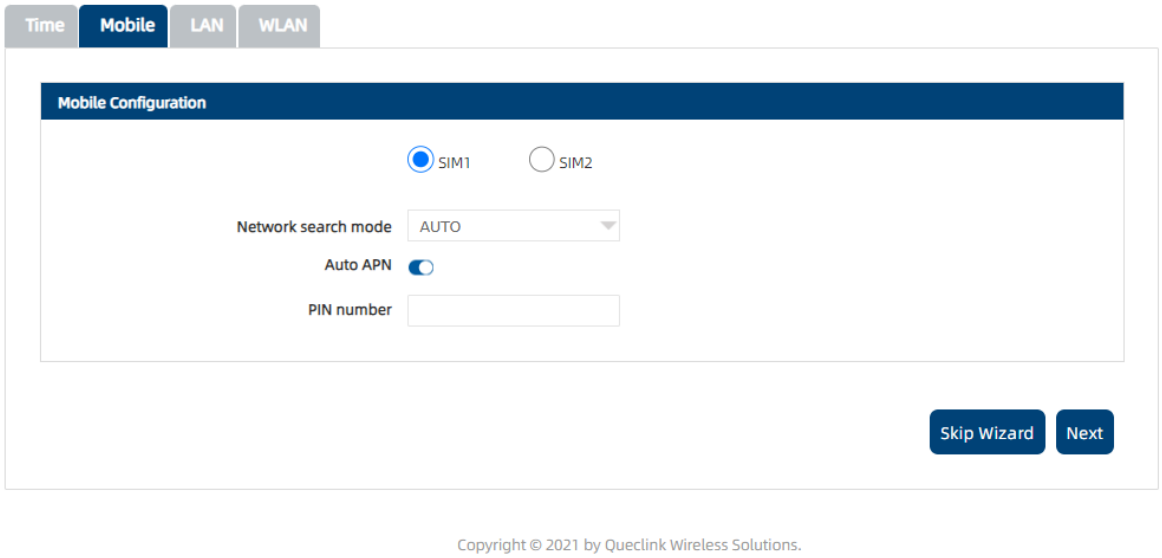
4.4.1 Setup Wizard

The **Setup Wizard** is to offer a simplified version of other WebUI pages used to set some of the device ‘s most relevant parameters. It’s a quick and easy way for you to set up the device.

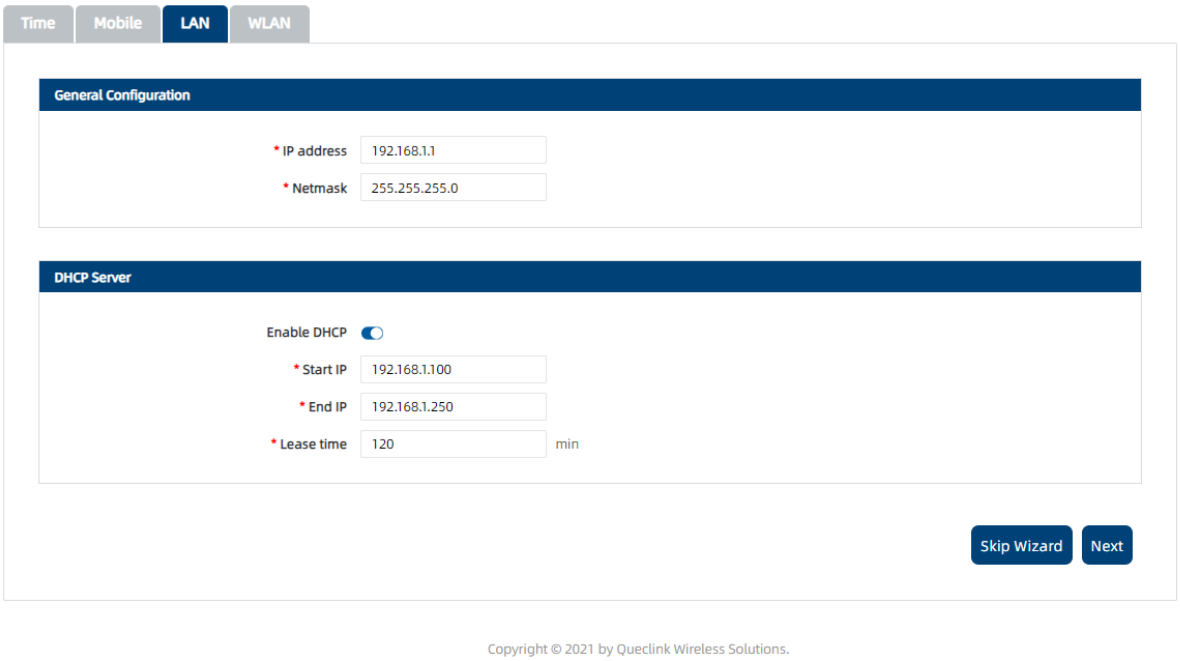
Step 1 is used to configure the device’s time settings. Time is essential for many applications, such as RMS, scheduled tasks.



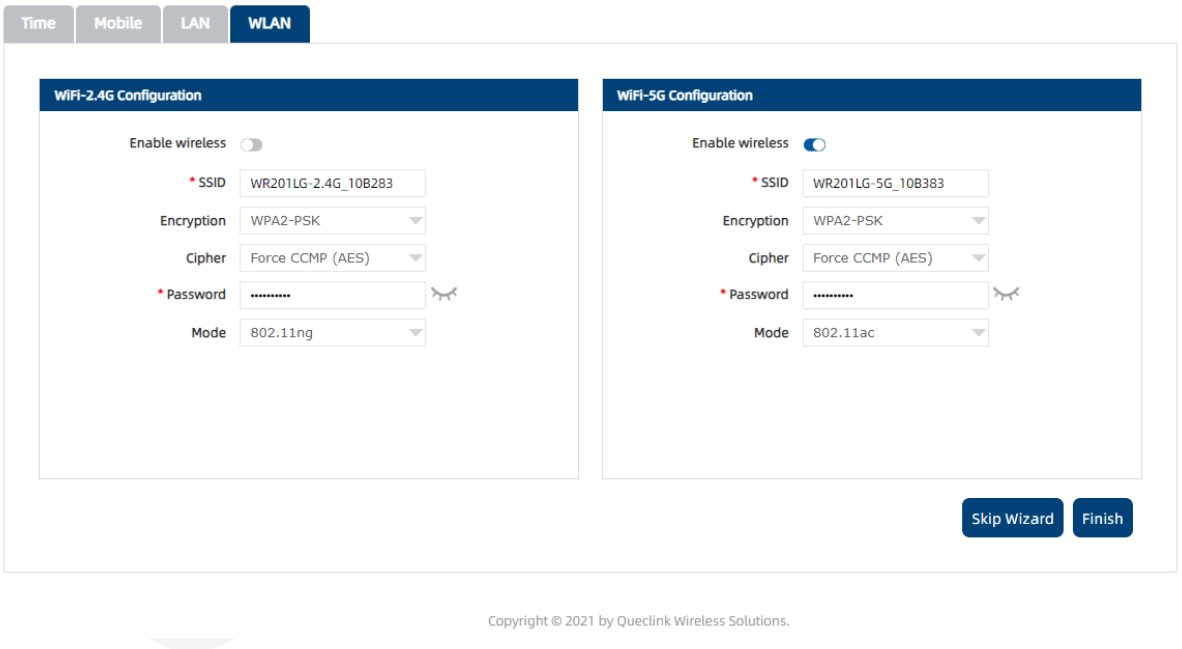
Step2 is used to configure the device's SIM card parameters.



Step3 is used to configure the device's local area network (LAN) and DHCP server settings.



Step4 is used to configure the device's Wi-Fi access point (AP).

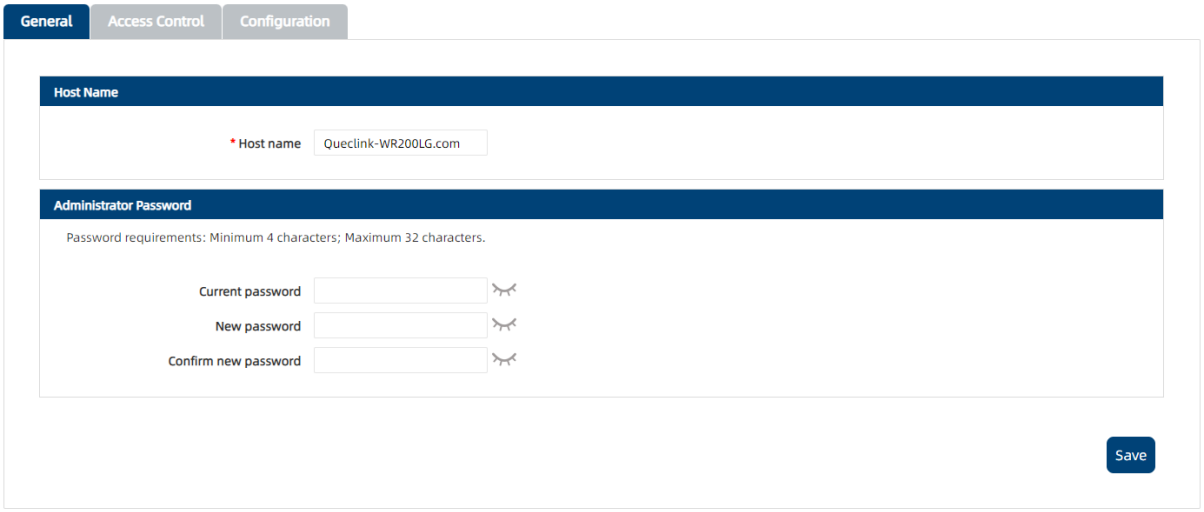


You can also skip any of above steps and configure the settings later in the corresponding section.

4.4.2 Administration

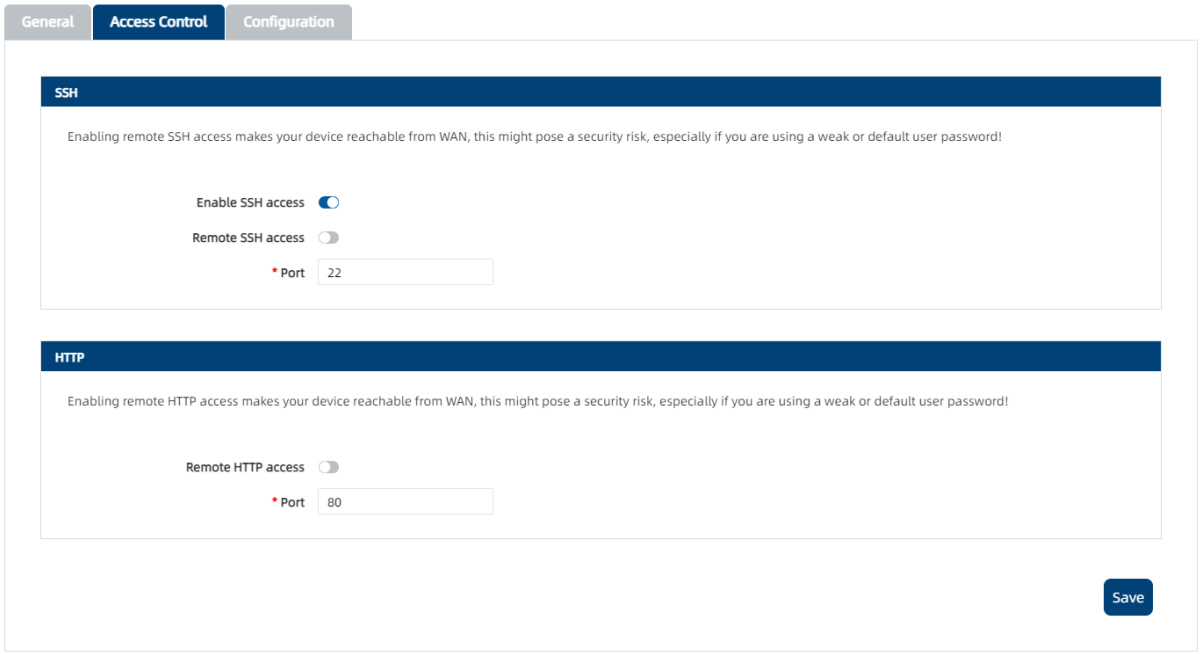
4.4.2.1 General

This page is for you to set up some of the device's system parameters, such as password, host name. To change the password, you must input your current password and then enter your new password.



4.4.2.2 Access Control

The section is used to manage SSH and HTTP(S) access to the device. You can click check box to enable or disable access by other devices remote or locally, enable access might pose a security risk to the device, especially if you are using a weak or default user password.

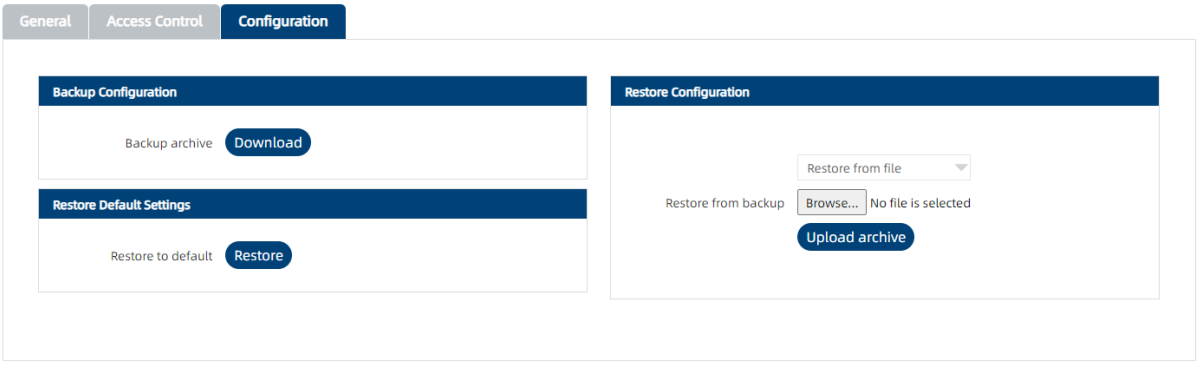


Field Name	Value	Description
Enable SSH access	yes|no; default: yes	Turns SSH access from the local network (LAN) on or off.
Remote SSH access	yes|no; default: no	Turns SSH access from remote networks (WAN) on or off.
Port	integer [0..65535]; default: 22	Selects which port to use for SSH access.

4.4.2.3 Configuration

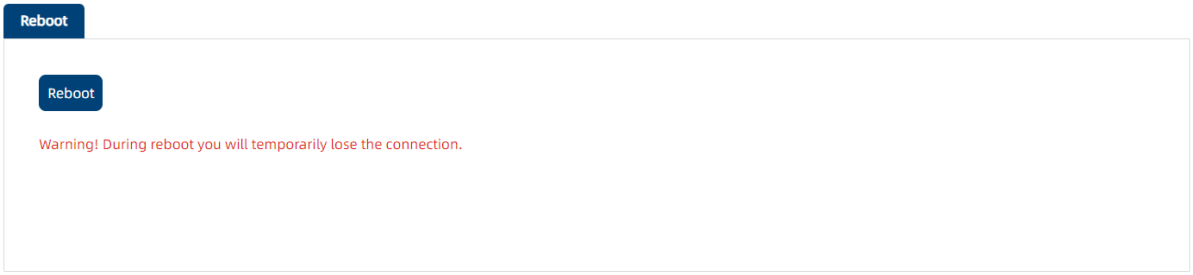
The Configuration page is used to generate the user's defaults configuration and download or upload backup files to the device.

Backup files can be uploaded only from identical devices with same model. Once a backup file is uploaded to a device, that device will have same configuration as the device from which the backup file originated.



4.4.3 Reboot

This page is used only to reboot the device. Click the Reboot button if you wish to reboot the device.

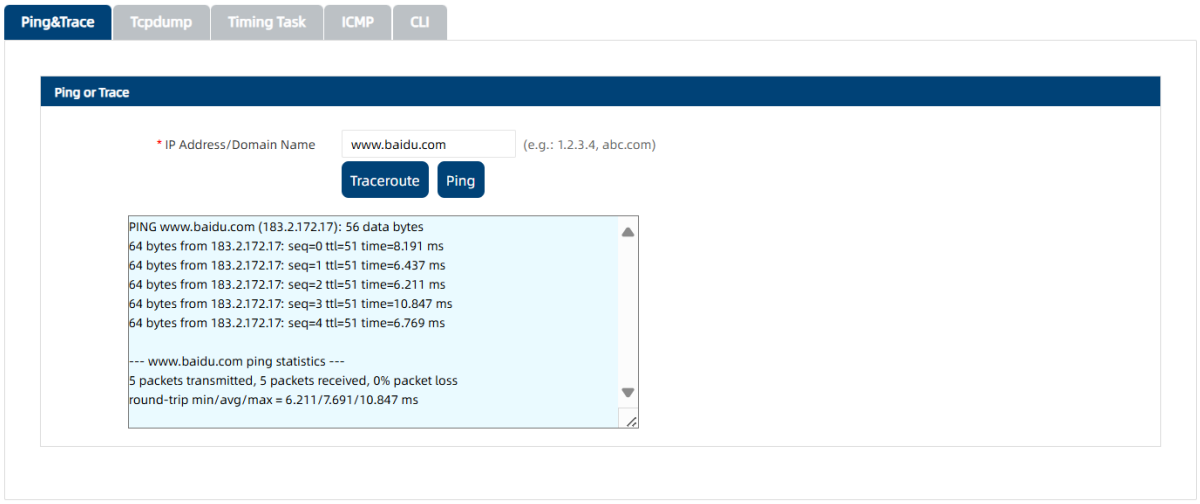


4.4.4 Diagnostic

The Diagnostic is used to execute network diagnostic tests, including traceroute, ping and Tcpdump.

4.4.4.1 Ping & Trace

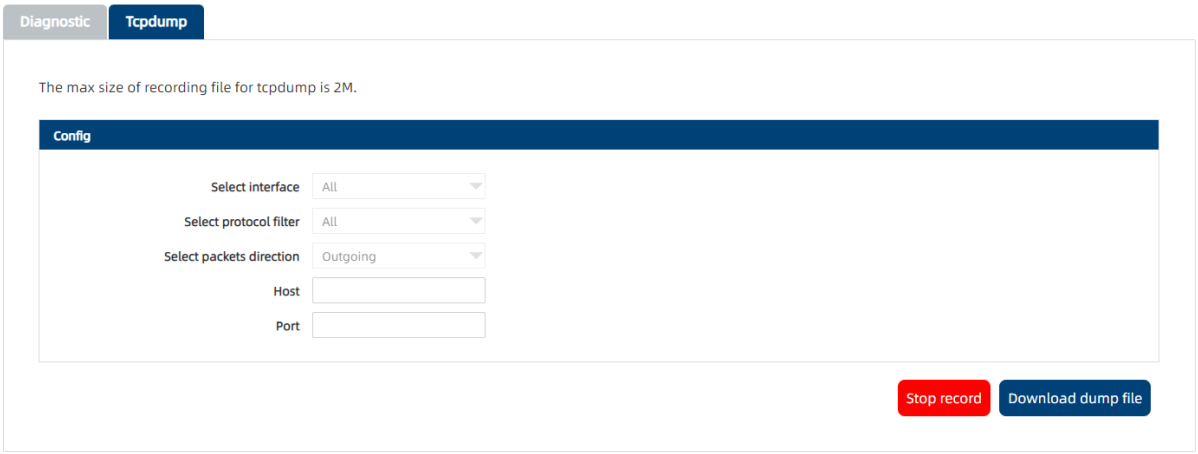
The user inputs an IP address or domain name, then clicks Traceroute or Ping button to check the connection between the device and the target IP address/domain name.



4.4.4.2 Tcpdump

Tcpdump is a Linux tool used to capture packets moving through network interfaces. By default, the device does not store TCP dump information. You must start Tcpdump before you can download the file.

After finishing the capture, remember to click Stop record button to close Tcpdump.

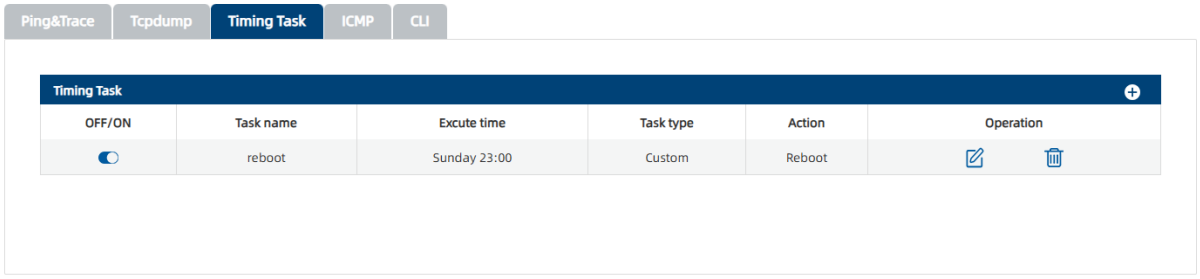


Field Name	Value	Description
Select interface	network interface; default: All	Only captures packets that move through the specified network interface.
Select protocol filter	All | ICMP | TCP | UDP | ARP; default: All	Only captures packets that match the specified protocol.
Select packets direction	Incoming | Outgoing | Bidirect; default: Bidirect	Only captures packets coming from the specified direction.
Host	ip | host; default: none	Captures packets related to the specified host.
Port	integer [0..65535]; default: none	Captures packets related to the specified port.

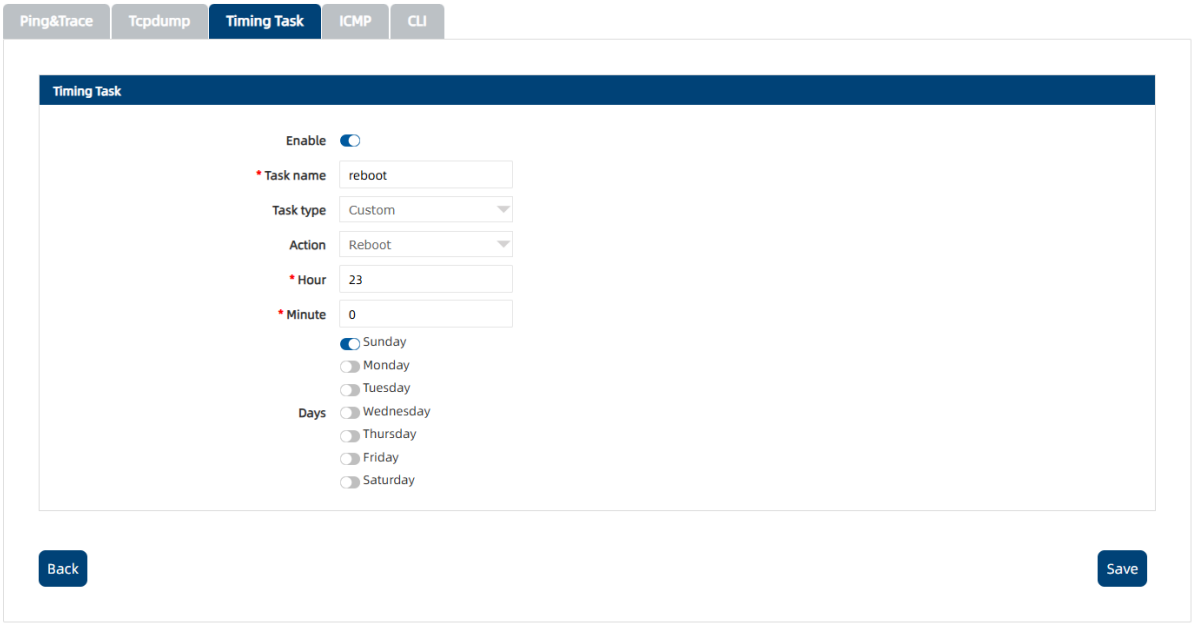
4.4.4.3 Timing Task

The Timing Task is a function that allows users to configure a reboot at a specified time. It can be used to prevent potential anomalies in equipment operation, and recover the operation through reboot.

You can add more rules with the 'Add' button or delete them using the 'Delete' button.

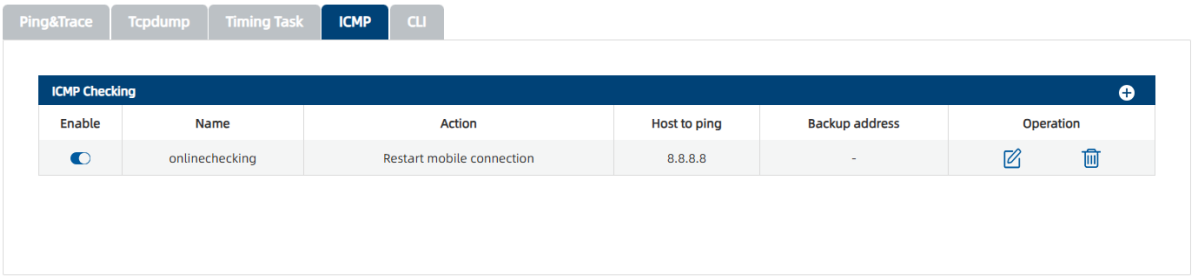


The figure below is an example of the Timing Task configuration page:

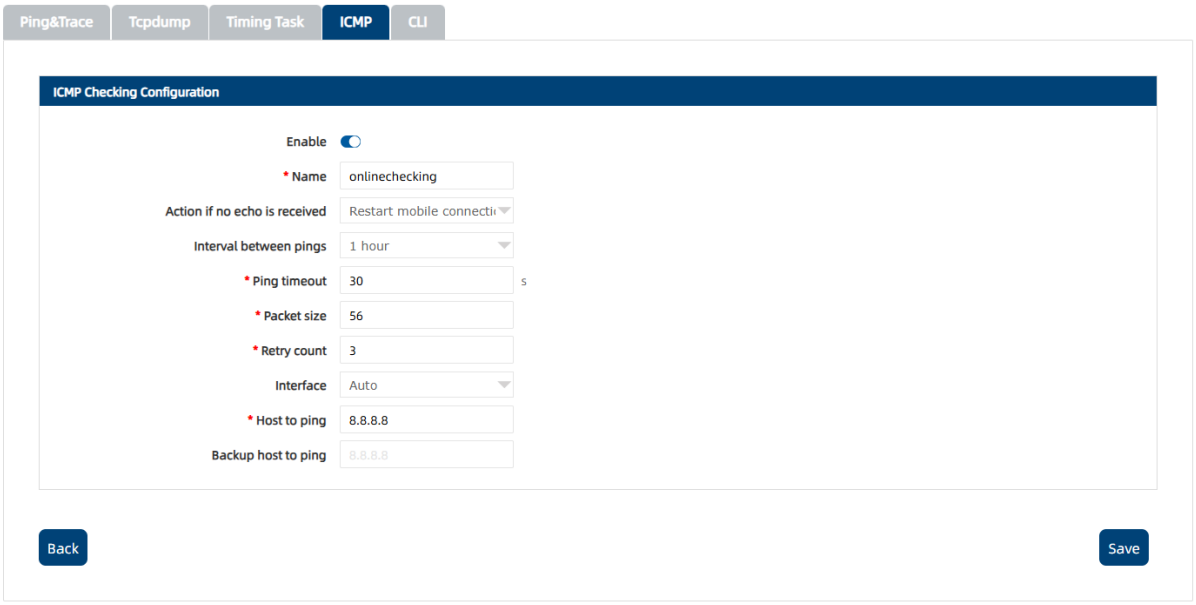


4.4.4.4 ICMP

The ICMP function periodically send ICMP requests to a specified IP address or host and waits for a response. If no response is received, the device will attempt the same action a defined number of times at a defined frequency. If there is still no response, the device will execute the specified action, for example, reboot the device.



You can create rules with the ‘Add’ button or delete them using the ‘Delete’ button. If you wish to customize a rule, click the ‘Edit’ button.

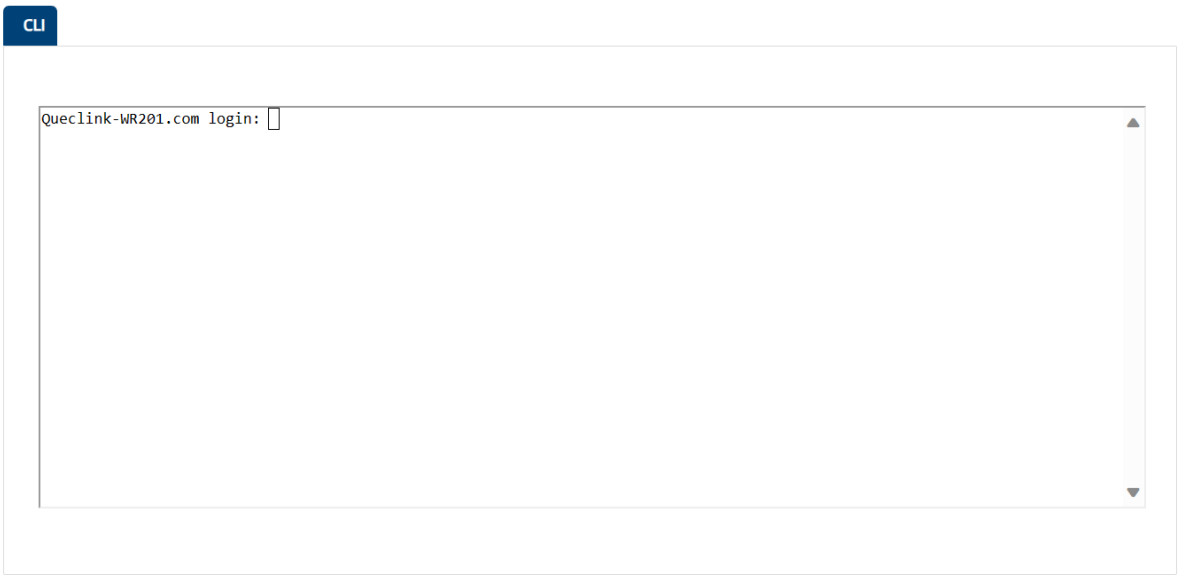


Field Name	Value	Description
Enable	off | on; default: off	Turns the rule on or off.
Name	String	The name of item.
Action if no echo is received	Reboot| Restart mobile connection| Switch SIM; default: Reboot	The action that will be taken if no ICMP echo is received
Interval between pings	5 mins | 15 mins | 30 mins | 1 hour | 2 hours; default: 1 mins	The frequency at which ping/Wget requests are sent to the specified host.
Ping timeout	integer [1..9999]; default: 30	Maximum response time. If no echo is received after the amount of time specified in this field has passed, the ping/wget request is considered to have failed.
Packet size	integer [0..1000]; default: 56	ICMP packet size in bytes.
Retry count	integer [1..9999]; default: 3	Indicates how many additional times the device will try sending ping requests if the initial one fails
Interface	Automatically selected | Ping from mobile; default: Automatically selected	Specifies through which interface the pings will be sent. If Automatically selected is set, the pings will go through the main WAN interface.
Host to ping	host | ip; default: 8.8.8.8	Hostname or IP address to which the Ping/Wget requests will be sent.
Backup host to ping	host | ip; default: 8.8.8.8	Hostname or IP address to which the Ping/Wget requests will be sent.

4.4.4.5 CLI

command-line interface (CLI) is a command line program that accepts text input to execute operating system functions. You can login the CLI with root account and password to execute any commands supported by Linux or Queclink's applications.

Queclink Confidential



4.4.5 NTP

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

In general section, you can configure general time settings, like selecting the local time zone, setting a time update interval, synchronizing the time, etc.

The Time Servers section displays the NTP servers that the device uses, you can configure maximum four time servers in this section.

WR310 uses GPS for time synchronization by default. When GPS is not available and NTP server synchronization function is enabled, WR310 will synchronize the time through NTP server.

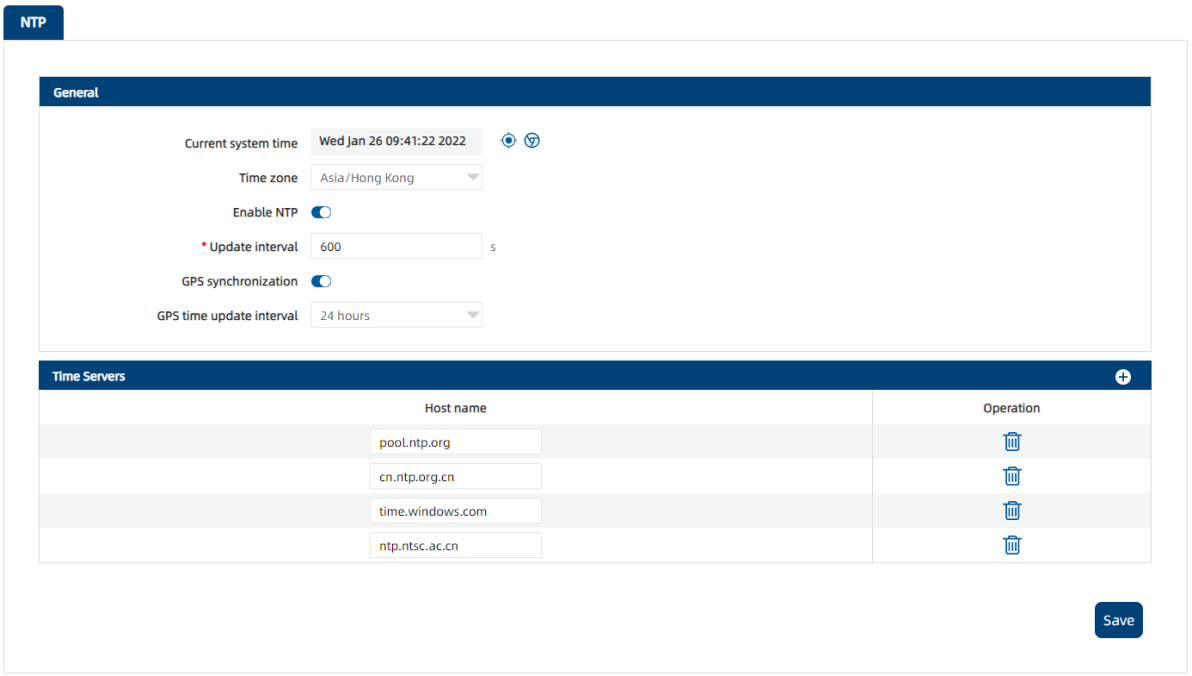


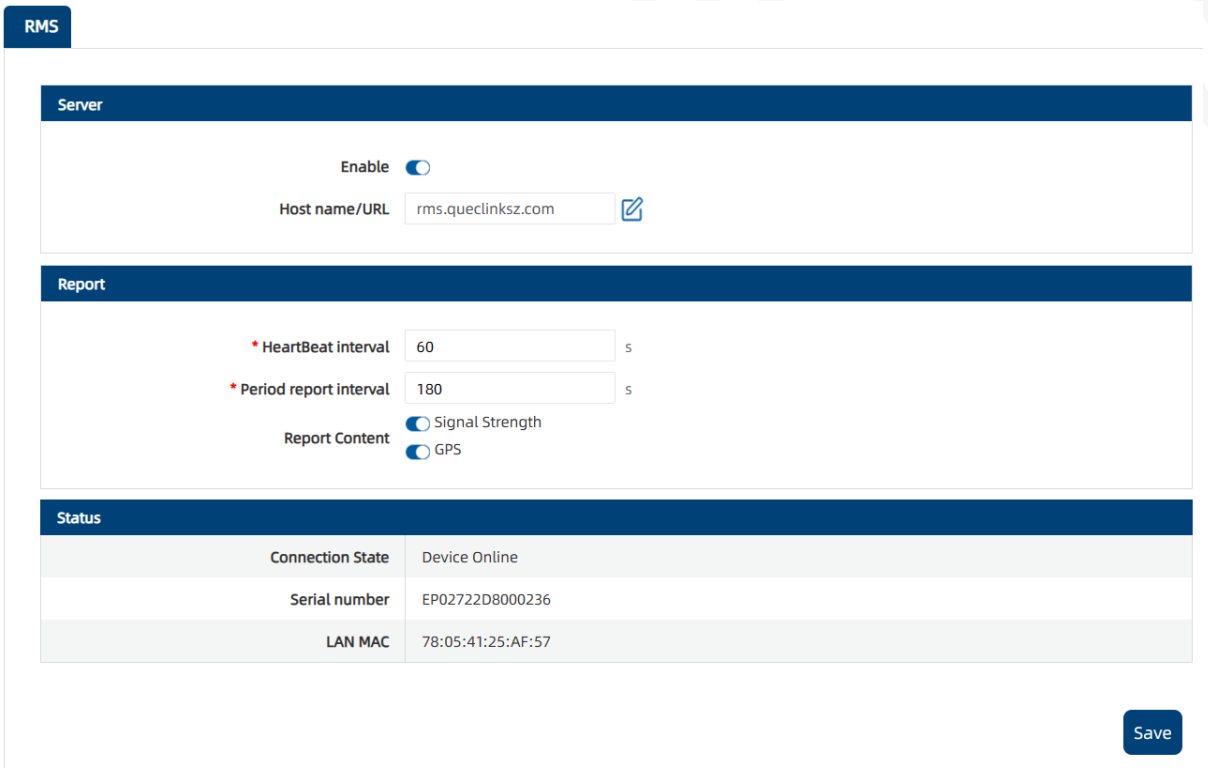
Table 56: Time Synchronization Settings

Field Name	Value	Description
Time zone	time zone; default: UTC	The device will sync time in accordance with the selected time zone.
Enable NTP	yes|no; default: yes	Turns NTP on or off.
Update interval (in seconds)	integer; default: 3660	Defines how often the device will update the time.
GPS synchronization	yes|no; default: no	Enables periodic time synchronization for the system using the GPS module (does not require an Internet connection).
GPS time update interval	5, 30 minutes|1, 6, 12, 24 hours|1 week|1 month; default: Every 24 hours	Defines how often the device will update the time using the GPS module.
Hostname	String	The name of NTP server.

4.4.6 Nebulink

RMS (Remote Management System) is a cloud-based platform designed by Queclink and used for remote monitoring and management of Queclink Router products.

The figure below is an example of the RMS section for a device which has been connected to RMS:



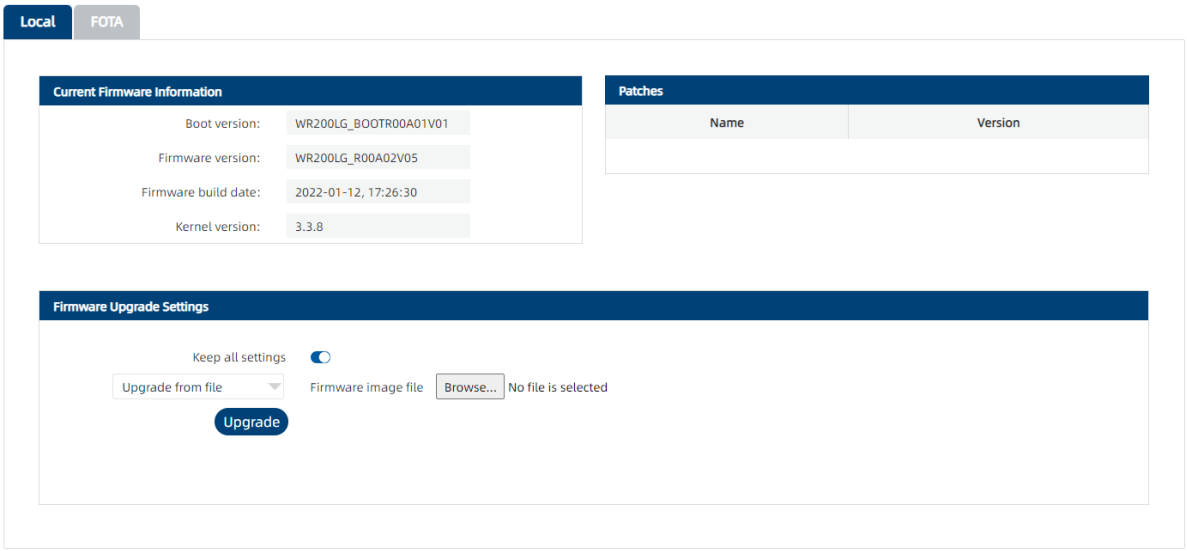
Field Name	Value	Description
Enable	yes|no; default: yes	Turns RMS service on or off.
Host name/URL	Host | ip; default: rms.quecklinksz.com	Address of the RMS server. If you're using Queclink RMS, just leave the default address.
HeartBeat Interval	integer; default: 60	The interval of heartbeat between device and RMS server. It is used to detect whether the device is on-line or not.
Period report interval	integer; default: 180	The interval the device sends reports to the RMS server. The report content is changeable by toggling the items below.
Connection State	String	To display the RMS connection status.

4.4.7 Upgrade

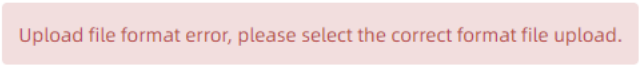
This section is to check the current firmware version of the device and to upgrade the device's firmware. Firmware can be upgraded either from server or from an image file uploaded from your computer.

4.4.7.1 Local

The Local section is used to upgrade the software from the local file. Click Browse button to select the new software from your computer and click Upgrade to upgrade the software. During the upgrade, please do not power off the router, the LEDs of the device will flash at the same time. After upgrade finished, the device will restart automatically. The whole upgrade process will take 5 minutes.



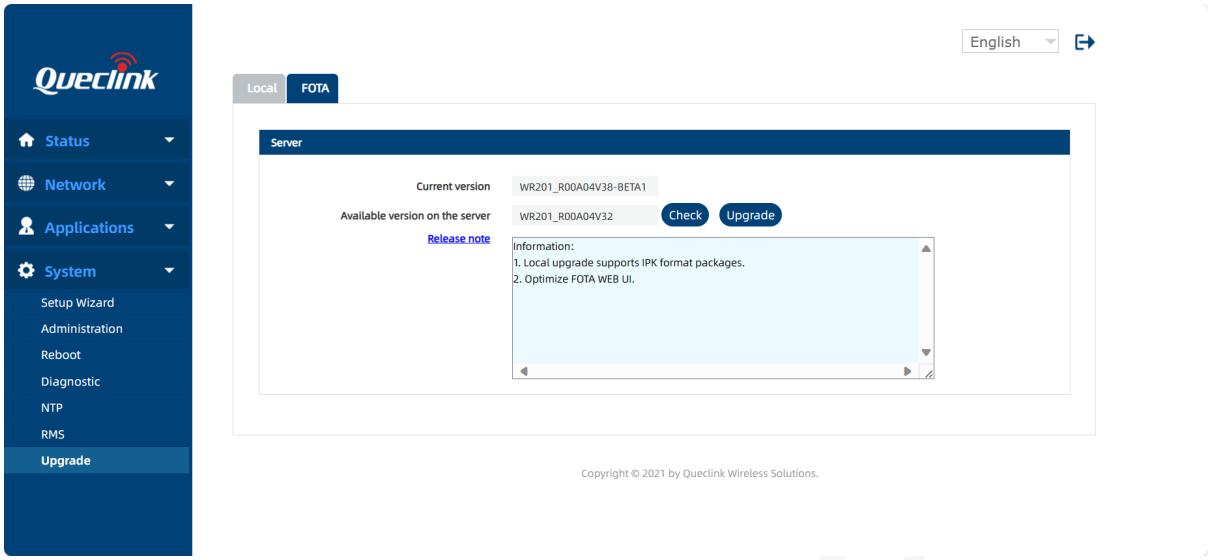
If the uploaded firmware file that is incompatible with your device, you will see a warning as below:



4.4.7.2 FOTA

This page is used to upgrade the firmware over the air. By default, the device supports RMS for remote upgrade.

By default, the page will display the latest FW version on the RMS with the release note. The user can click upgrade button to upgrade to this version. Users can also click Check button to check if there is a available version on the server.



4.5 Reset Button

All Queclink Cellular Routers has a reset button to return the device back to its default factory settings, please kindly note returning to default factory setting means the device will delete all custom configurations. We strongly recommend you to back up the configuration before the operation.

The reset button has two functions:

- **Reboot the device** - If the reset button is pressed for up to 4 seconds, the device will reboot.
- **Factory reset** - If the reset button is pressed for at least 5 seconds (by default), the device will perform a factory reset and then reboot.

All LEDs indicate the elapsed time while holding the reset button.

Queclink Confidential

CHAPTER

FIVE

NETWORK SERVICES AND PORTS

Default open ports for LAN network:

Service	port
DNS	53/TCP
http	80/TCP
https	443/TCP

Queclink Confidential

CHAPTER

SIX

FAQ

6.1 SIM Slot

Phenomenon:

Discontinue during dialing, dial failure

Possible Reason:

- SIM card network type do not match
- SIM charges owed
- Power supply do not match
- Modem setting wrong

Solution:

- Change to a suitable SIM card
- Recharge SIM card
- Change to suitable power supply
- Change Modem setting, please check related chapter

6.2 No Signal

Phenomenon:

Modem status show no signal

Possible Reasons:

- Antenna connect wrong
- Modem cannot online
- Modem offline

Solution:

- Connect suitable antenna
- Modem cannot online, check SIM and modem setting
- Modem offline, check the device setting, like wake up setting, ICMP setting, check if there are any setting make the device offline

6.3 Cannot Find SIM/UIM Card

Phenomenon:

Cannot find SIM card

Queclink Confidential

Possible Reason:

- SIM card damage
- SIM bad contact

Solution:

- Replace SIM card
- Re-install SIM card

6.4 VPN Cannot Connect

Phenomenon

VPN cannot establish connection

Possible Reason:

- VPN port abnormal
- VPN parameter setting wrong
- VPN peer server abnormal

Solution:

- Make sure the device is online
- Set the correct port to VPN
- Check all VPN parameters
- Check VPN peer server

Queclink Confidential

CHAPTER

SEVEN

APPENDICES

7.1 General Notes

Queclink offers this information as a service to its customers, to support application and engineering efforts that use the products designed by Queclink. The information provided is based upon requirements specifically provided to Queclink by the customers. Queclink has not undertaken any independent search for additional relevant information, including any information that may be in the customer's possession. Furthermore, system validation of this product designed by Queclink within a larger electronic system remains the responsibility of the customer or the customer's system integrator. All specifications supplied herein are subject to change.

7.2 Revision History

Version	Date	Description of Change
1.00	2022-06-07	Initial
3.00	2023-10-31	Build a unified version
4.00	2024-03-04	Update some content.
5.00	2024-08-29	Add Hotspot, QoS and some other features.
6.00	2024-12-31	Optimize description.
6.10	2025-01-09	Modify Modbus description.
6.50	2025-03-13	Optimize wording.
7.00	2025-06-10	1. Add BLE function. 1. Optimize some wording. 2. Optimize diagnostic section description.
7.20	2025-07-30	1. Add ID descriptions for the input and output ports. 1. Add VLAN description.

7.3 Glossary

Abbr.	Description
APN	Access Point Name
CHAP	Challenge Handshake Authentication Protocol
dB	Decibel
DC	Direct Current
DI	Digital Input
DO	Digital Output
FDD LTE	Frequency Division Duplexing Long Term Evolution
GRE	generic route encapsulation
GSM	Global System for Mobile Communications

continues on next page

Queclink Confidential

Table 1 – continued from previous page

Abbr.	Description
HSPA	High Speed Packet Access
ID	identification data
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
M2M	Machine to Machine
MS	Mobile Station
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PIN	Personal Identity Number
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
RF	Radio Frequency
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
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network
QoS	Quality of Service

7.4 Copyright

This document contains proprietary technical information which is the property of Queclink. Copying of this document, distribution to others or using or communication of the contents thereof is forbidden without express authority. Offenders are liable to the payment of damages. All rights are reserved in the event of a patent grant or registration of a utility model or design. All specifications supplied herein are subject to change without notice at any time.

Copyright © Queclink Wireless Solutions Co., Ltd. 2022