Queclink Industrial CPE User Manual

Version: 4.00

Driving Smarter IoT

www.queclink.com

Document Title	Queclink Industrial CPE User Manual
Version	4.0
Date	2024-03-04
Status	Released

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.

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

Contents

0. Revision History 1
1. Overview 2
1.1 Description 2
1.2 Software Architecture 2
2. Hardware 3
2.1 Structure 3
2.2 Interfaces 6
2.3 Connector Definition 7
2.4 LEDs 9
2.5 Installation 12
3. Initial Configuration 15
3.1 Configure the PC 15
3.2 Login to device 16
3.3 Control Panel 16
4. Software Configuration 18
4.1 Status 18
4.1.1 Overview 18
4.1.2 Device 18
4.1.3 Network->Mobile 19
4.1.4 Network->WAN 21
4.1.5 Network->LAN 21
4.1.6 Network->WLAN 22
4.1.7 Applications 23
4.1.8 VPN 23
4.1.9 Routes 24
4.1.10 Mobile Traffic 25
4.1.11 Log 26
4.2 Network 26
4.2.1 Link Management 26
4.2.2 Mobile 29
4.2.2.1 General 29
4.2.2.2 SIM management 30
4.2.2.3 Data Limit 31
4.2.3 WAN 32
4.2.4 LAN 36
4.2.5 WLAN 38

4.2.6 Routing 41
4.2.6.1 Static 41
4.2.6.2 Rip 42
4.2.7 Firewall 43
4.2.7.1 NAT 43
4.2.7.2 Domain Filter 44
4.2.7.3 IP/MAC Filter 45
4.2.7.4 DMZ 46
4.2.7.5 DDOS 46
4.3 Applications 48
4.3.1 GPS (Available for Specific Models Only) 48
4.3.1.1 Map 48
4.3.1.2 General 48
4.3.1.3 NMEA 49
4.3.2 VPN 50
4.3.2.1 PPTP 50
4.3.2.2 L2TP 52
4.3.2.3 OPENVPN 55
4.3.2.4 IPSec 63
4.3.2.5 GRE Tunnel 67
4.3.3 SMS Utilities 69
4.3.4 MQTT 69
4.3.5 RS232/RS485 71
4.3.6 Modbus 75
4.3.6.1 Modbus RTU 75
4.3.6.2 Modbus TCP to RTU 79
4.3.7 DDNS 79
4.3.8 Input 80
4.3.8.1 Status 81
4.3.8.2 Report 81
4.3.8.3 Local Control 84
4.3.8.4 Application Example 85
4.3.9 Output 86
4.3.9.1 Status 86
4.3.9.2 Default State 86
4.3.9.3 Switch 87
4.3.9.4 Periodic Control 87
4.3.9.5 Control 89
4.3.9.5 Application Example 90
4.3.10 Auto Recovery 91
4.3.10.1 Timing Task 91
4.3.10.2 ICMP 92
4.3.11 SNMP 94
4.3.11.1 SNMP 94

4.3.11.2 COMMUNITY 95
4.3.12 Tracker 95
4.3.12.1 General 95
4.3.12.2 Device 96
4.3.12.3 Report 98
4.3.13 Hotspot 100
4.3.14.1 General 100
4.3.14.2 Local Users 102
4.4 System 102
4.4.1 Setup Wizard 102
4.4.2 Administration 104
4.4.2.1 General 104
4.4.2.2 Access Control 104
4.4.2.3 Configuration 105
4.4.3 Reboot 106
4.4.4 Diagnostic 106
4.4.4.1 Ping&Trace 106
4.4.5 NTP 107
4.4.6 CLI 108
4.4.7 RMS 109
4.4.8 Upgrade 110
4.4.8.1 Local 110
4.4.8.2 FOTA 111
4.5 Reset Button 111
5. FAQ 112
5.1 SIM Slot 112
5.2 No Signal 112
5.3 Cannot Find SIM/UIM Card 112
5.4 VPN Cannot Connect 112
Glossary 114

0. Revision History

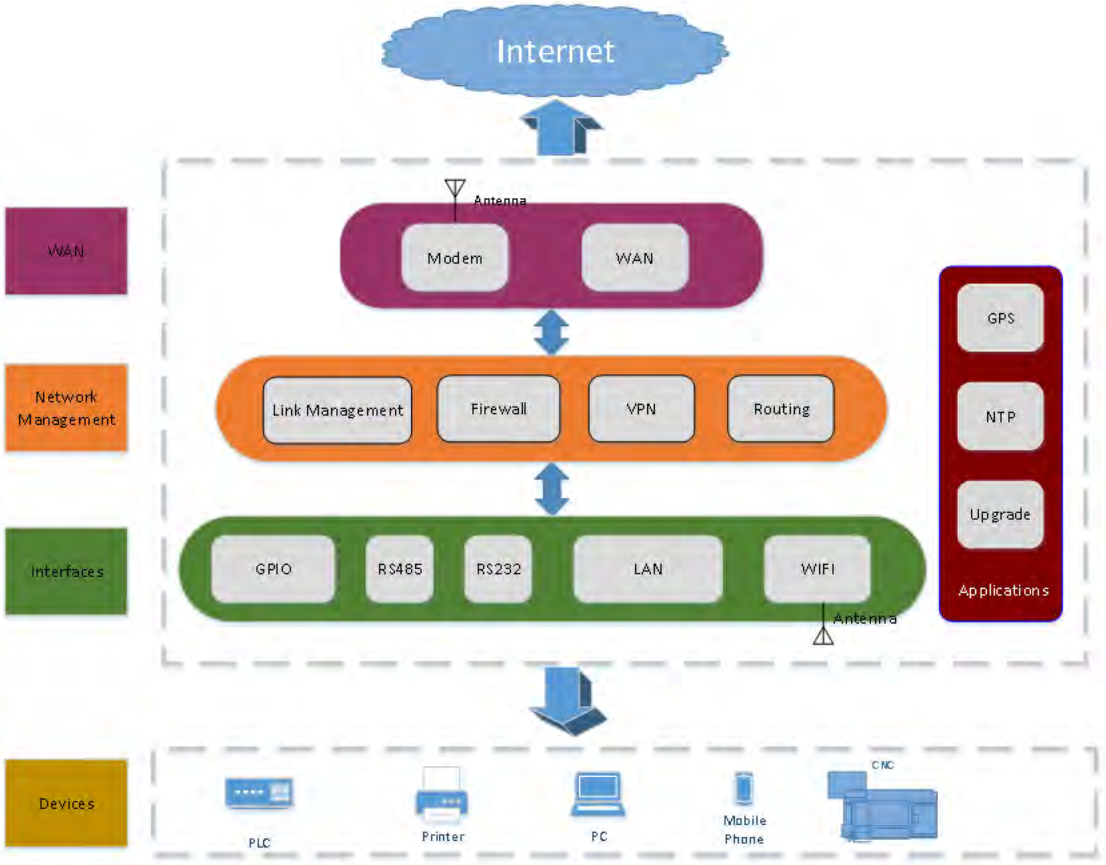
Version	Date	Author	Description of Change
1.0	2022-06-07	Vincent	Initial
3.0	2023-10-31	Vincent	Build a unified version
4.0	2024-3-4	Vincent	Change the name from Router to CPE. Update some content.

1. Overview

1.1 Description

The Queclink dual SIM industrial CPE is a series of rugged CPE offering high-speed stable mobile connectivity for machine to machine (M2M) applications. Based on 3G/4G LTE and 5G technology, the devices 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.

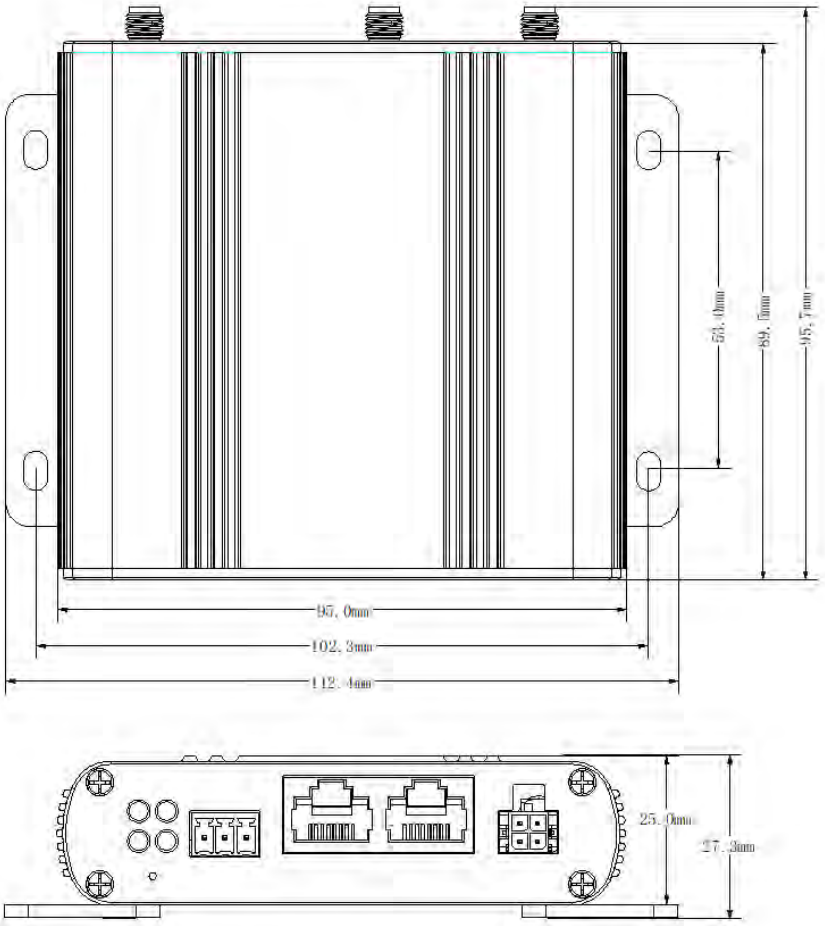
1.2 Software Architecture



2. Hardware

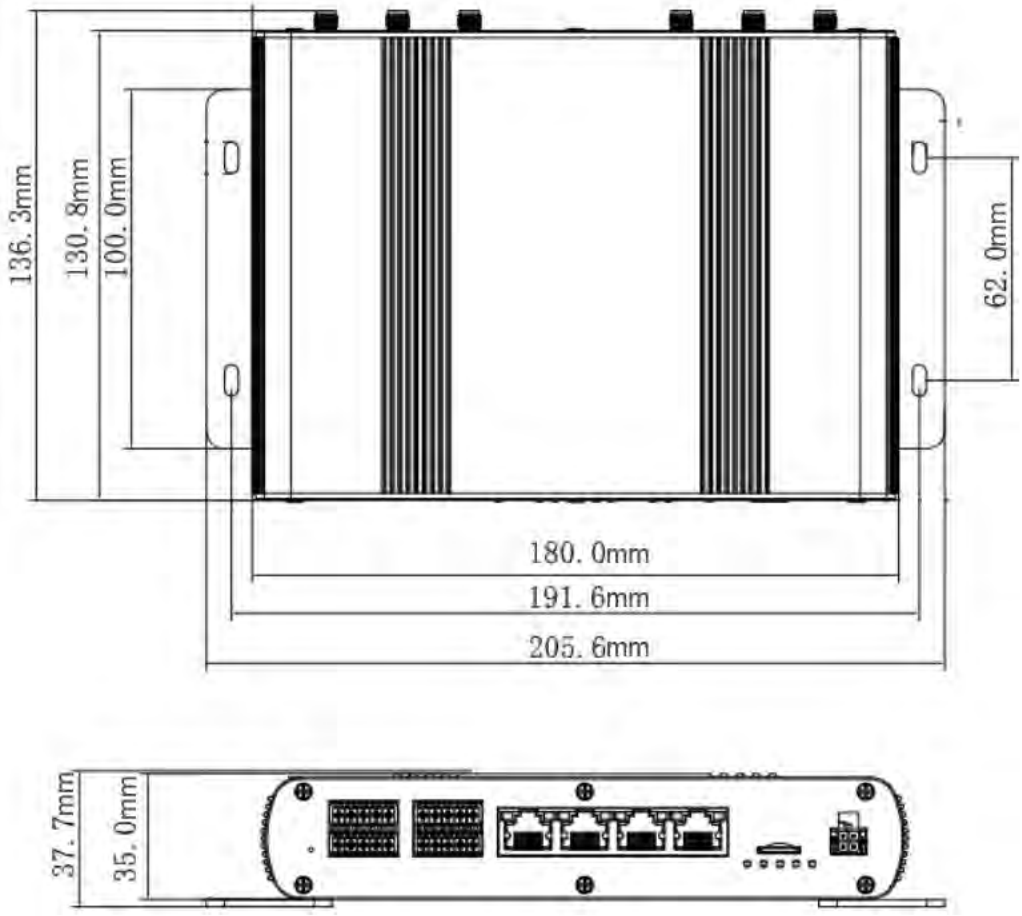
2.1 Structure

WR100:

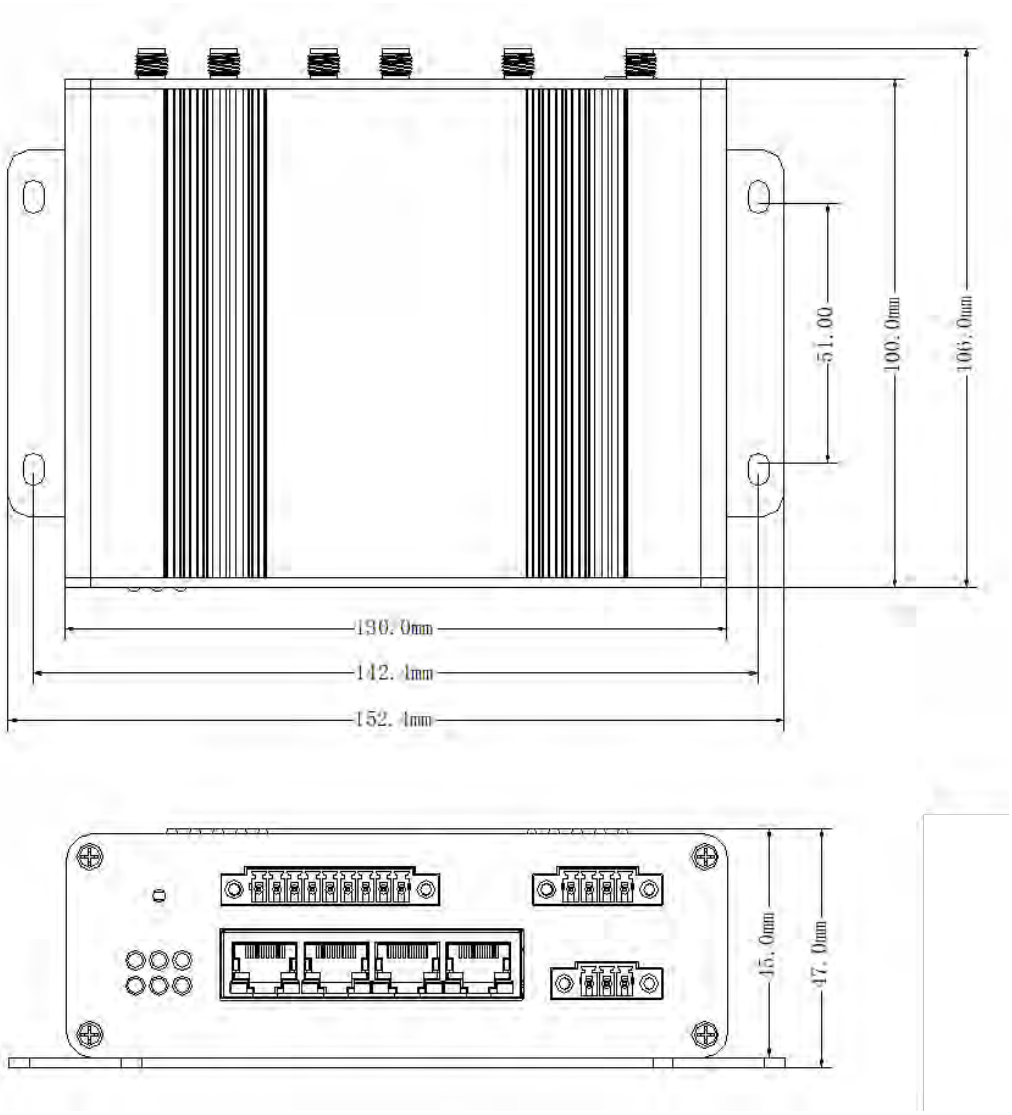


WR201:

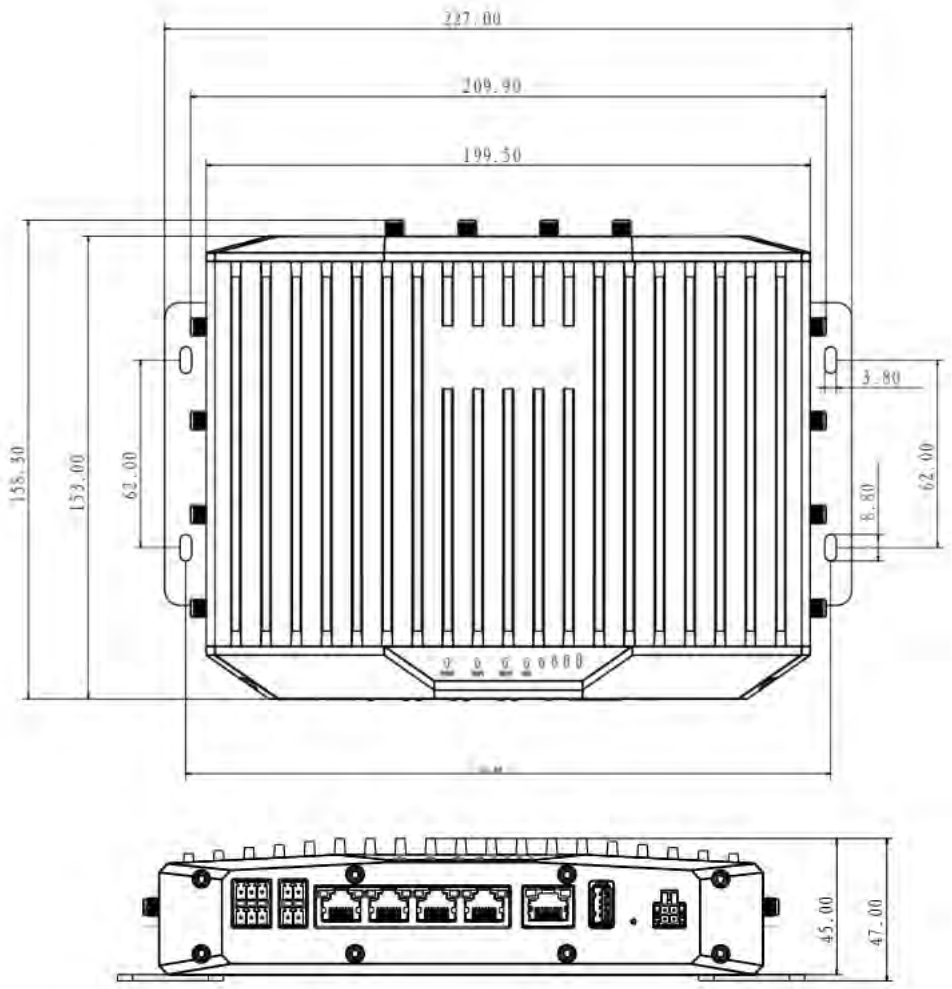
-.


136.3mm
130.8mm
100.0mm
62.0mm
180.0mm
191.6mm
205.6mm
37.7mm
35.0mm

WR210:



WR300:

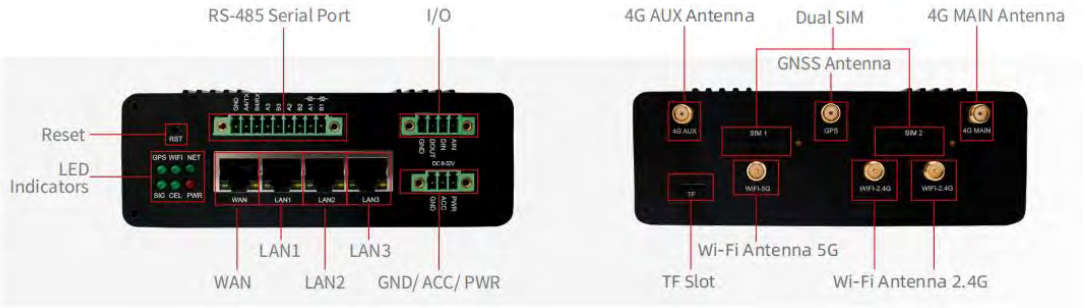


2.2 Interfaces

WR100:

WR201:

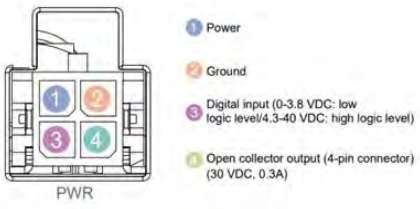
WR210:



WR300:

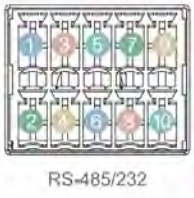
2.3 Connector Definition

WR100:

Power	

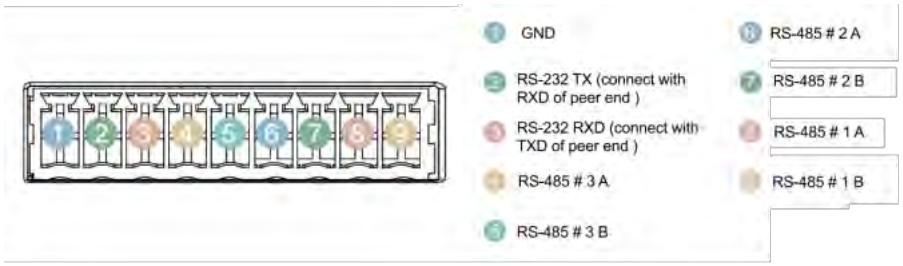
RS-485/RS-232	

WR201:

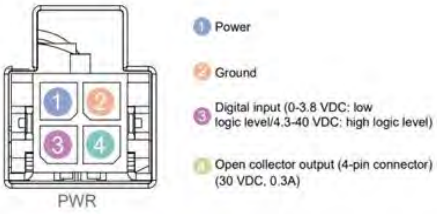
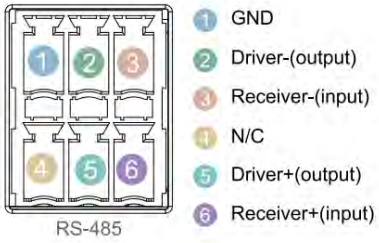
Power	
RS-485/RS-232	
I/O	

WR210:

Power	

RS-485/RS-232	
I/O	

WR300:

Power	
RS-485	
RS-232	

2.4 LEDs

WR100:

Name	Status	Description
PWR	Red, solid	Power on
	Off	Power off
Wi-Fi	Orange, solid	Wi-Fi on and working

	Orange blinking every 350ms	Data is being transferred
	Off	Wi-Fi off
CEL	Green, solid	Connecting to 4G network
	Green blinking every 0.5s	Connecting to 2G/3G network
	Off	No SIM or bad PIN
SIGNAL (RSSI)	Blue, solid	23 to 32
	Blue blinking every 1s	11 to 23
	Blue blinking every 0.5s	1 to 10
	Off	0

WR201:

Name	Status	Description
PWR	Red, solid	Power on
	Off	Power off
Wi-Fi	Orange, solid	Wi-Fi on and working properly
	Orange blinking every 250ms	Data is being transferred
	Off	Wi-Fi off or abnormal
GPS	Yellow, solid	GPS on and working properly
	Off	GPS off or abnormal
CEL	Green, solid	Connected to 4G network
	Green blinking every 0.5s	Connected to 2G/3G network
	Off	No SIM card or wrong PIN
SIGNAL (RSSI)	Blue, solid	23 to 32
	Blue blinking every 1s	11 to 23
	Blue blinking every 0.5s	1 to 10
	off	0
Ethernet Indicator	Green, solid	Connection is established
	Green blinking	Data is being transferred
	Off	Connection is not established

WR210:

Name	Status	Description
PWR	Green, solid	Power on
	Off	Power off
Wi-Fi	Green, solid	Wi-Fi on and working properly
	Green blinking every 250ms	Data is being transferred
	Off	Wi-Fi off or abnormal
GPS	Green, solid	GPS on and working properly
	Off	GPS off or abnormal
NET	Green,solid	Link connection is working
	Off	Link connection is down
CEL	Green, solid	Connected to 4G network
	Green blinking every 0.5s	Connected to 2G/3G network
	Off	No SIM card or wrong PIN
SIGNAL (RSSI)	Green, solid	23 to 32
	Green blinking every 1s	11 to 23
	Green blinking every 0.5s	1 to 10
	off	0
Ethernet Indicator	Green, solid	Connection is established
	Green blinking	Data is being transferred
	Off	Connection is not established

WR300:

Name	Status	Description
PWR	Green,solid	Power on
	Off	Power off
Wi-Fi	Green,solid	Wi-Fi on and working properly
	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 evey 1s	Connected to 2G network
	Green and red blinking evey 1s	Connected to 3G network
	Green blinking evey 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 Indicators	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 WR201 on how to correctly insert a SIM card, install antennas and power on a device.

1. Insert SIM card:

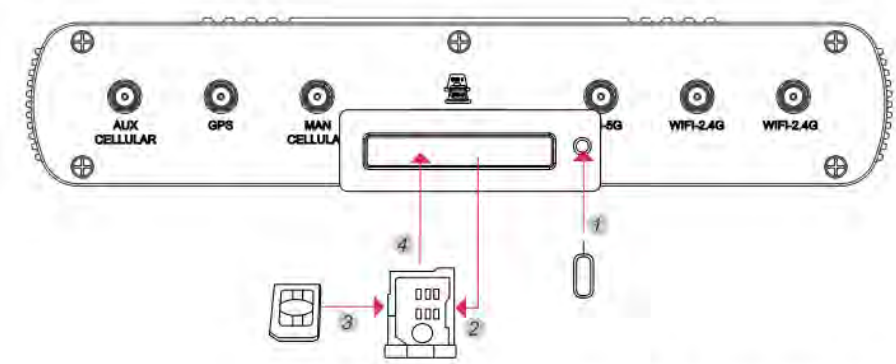
(1) Make sure the device is powered off.

(2) Push the SIM holder button with the SIM ejection pin.

(3) Pull out the SIM holder.

(4) Insert your SIM card into the SIM holder.

(5) Slide the SIM holder back into the device.

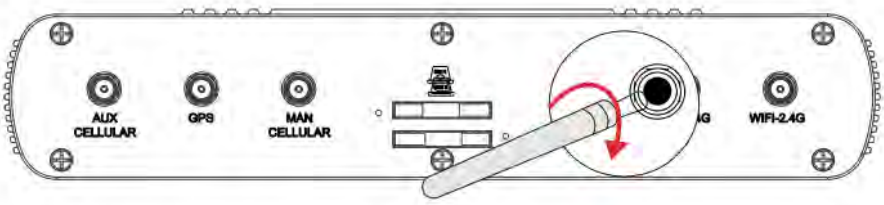


Note: The device is compatible with mini-SIM (2FF) size cards.

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

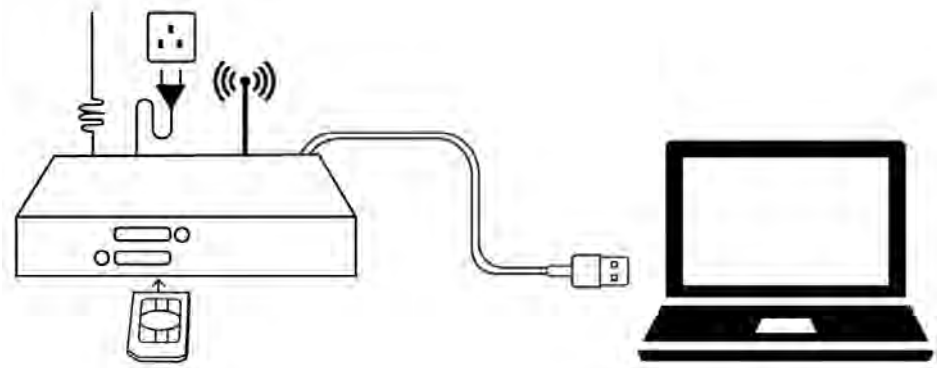
2. Attach External LTE, Wi-Fi and GPS Antenna:

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



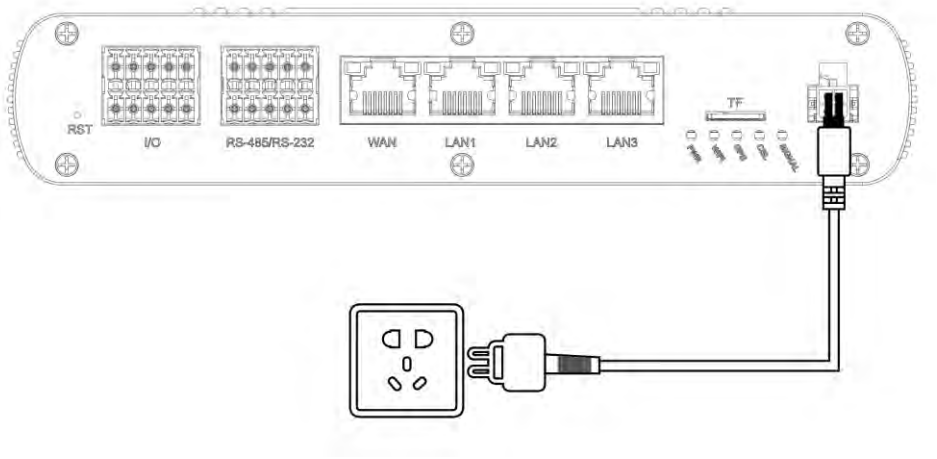
3. Connect the device to other devices

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. WR210 and WR310 series can support DIN rail installation, and you can consult with local sales representatives to order related accessories.

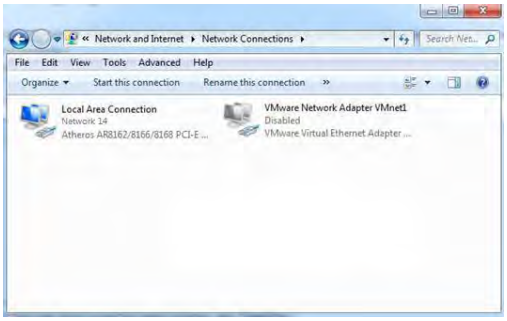
3. Initial Configuration

Queclink Industrial CPEs have a friendly WebUI which make users easily configure the device through. Make sure your computer has an Ethernet interface and web browser such as IE, Chrome, Firefox, etc.

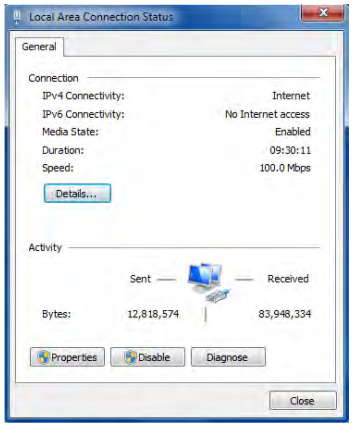
3.1 Configure the PC

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

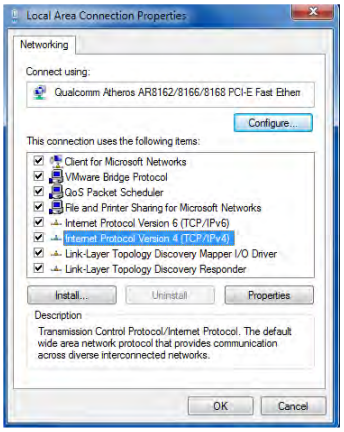
Here take **Windows 7** as example to configure a static IP address, and the configuration for windows system is similar.

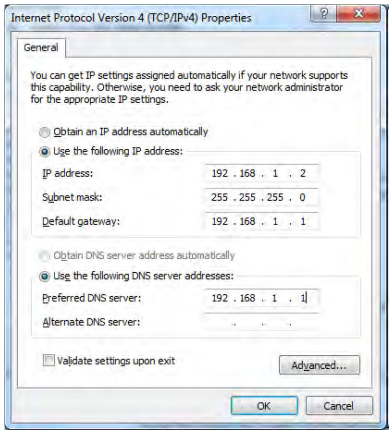


1. Click Start > Control panel, double-click Network and Sharing Center, and then double-click Local Area Connection.



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





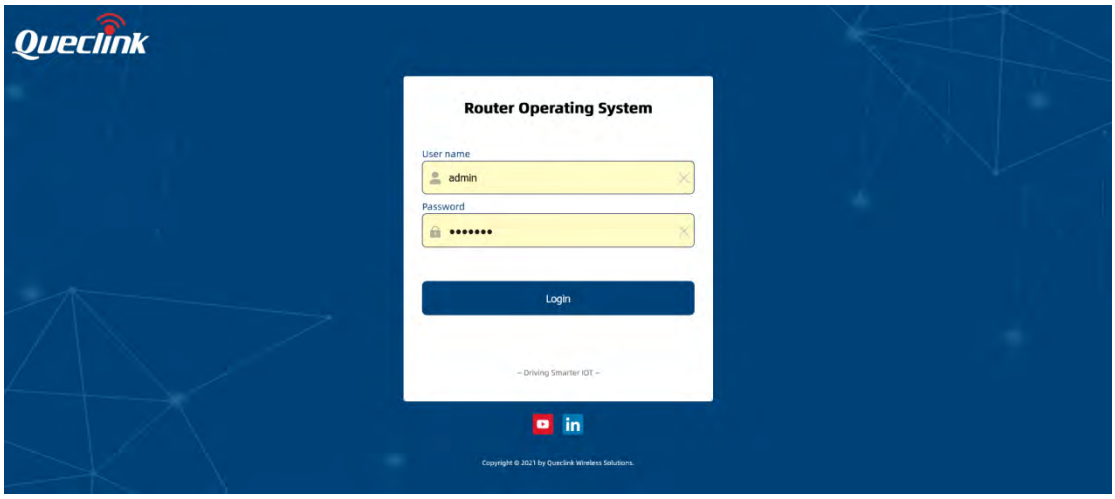
3. Choose Internet Protocol Version 4 (TCP/IPv4) and click Properties.
4. Use the following IP address:

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:

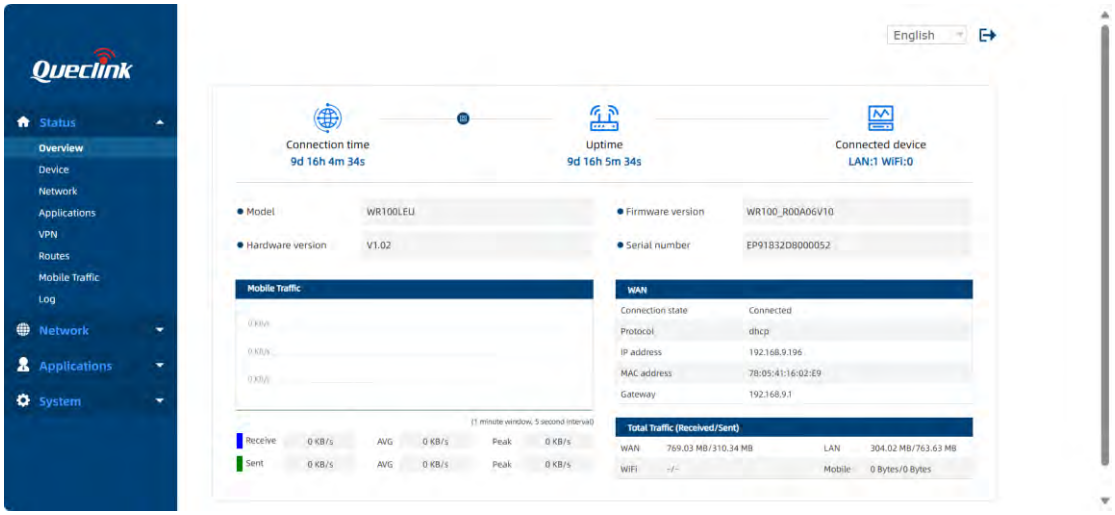


Enter the username and password, and then click LOGIN button. The default username is "admin" and password is "admin01".

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 has language selection drop down menu and exit button on the upper right corner. You can change language setting or logout the system easily.



The following chapters provide a detailed description on all firmware features and how to configure their parameters through web management system. Depending on the 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.

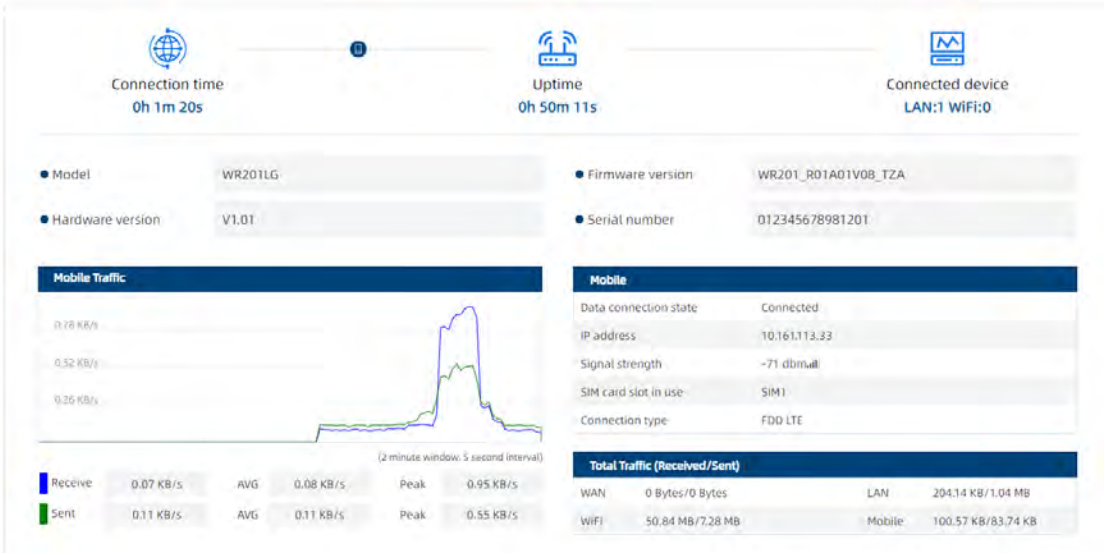
4. Software Configuration

4.1 Status

This section includes the running status of the device.

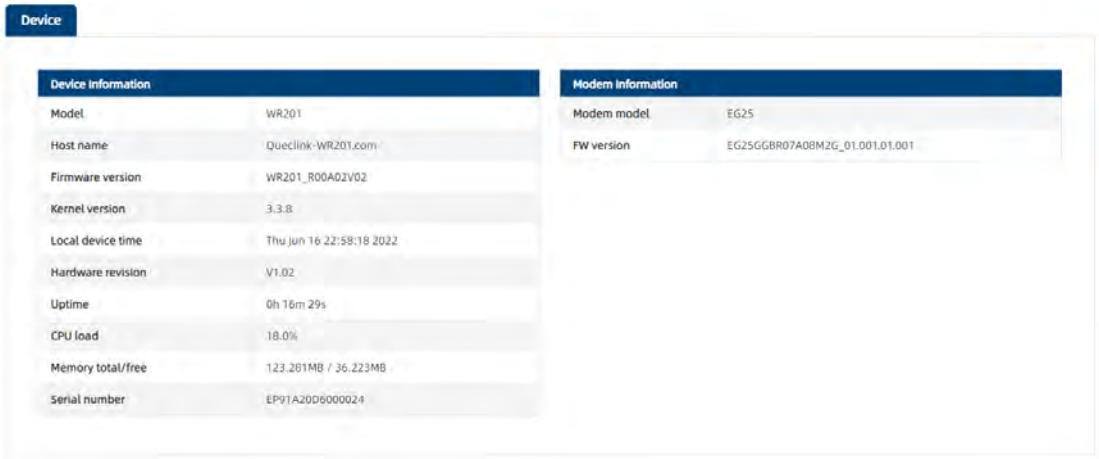
4.1.1 Overview

The **Overview** page contains various information summaries, such as connection state, mobile connection state and traffic, etc. It is also the homepage of the WebUI.
The figure bellow 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 are important information of after sales maintenance.

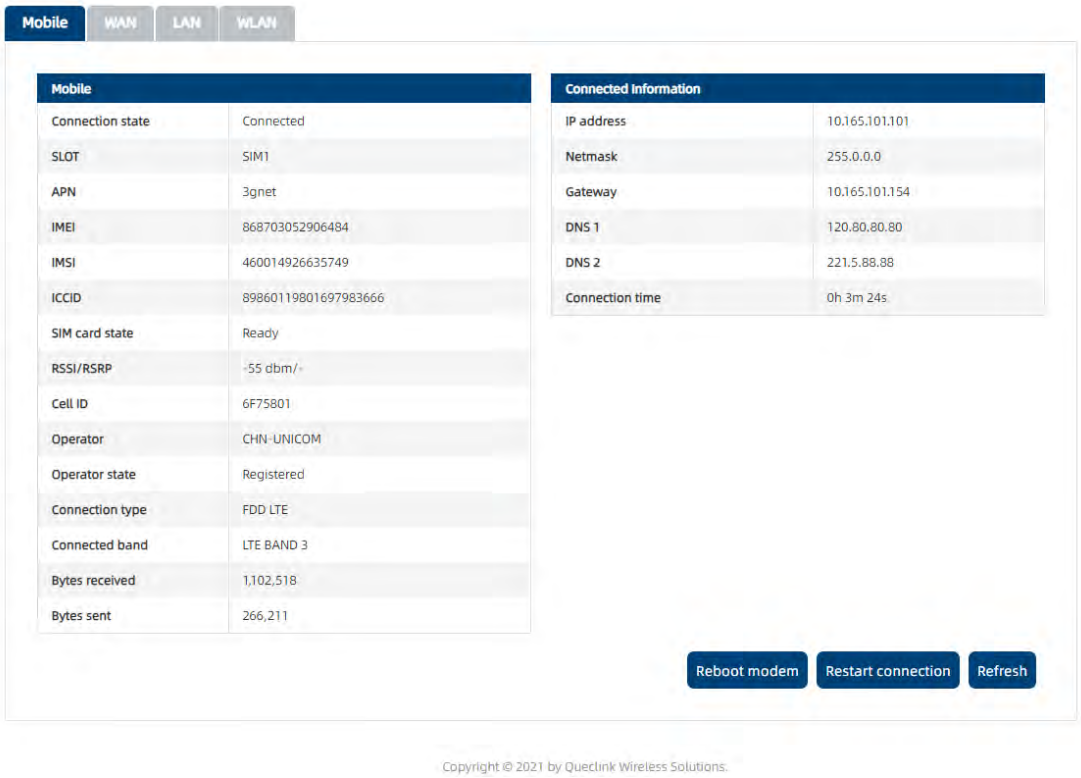


Field Name	Description
Model	Displays model number of the device.
Host name	Displays the device's host name. The hostname can be used

	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->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:



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.

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	Shows whether the network has currently indicated the registration of the mobile device. Possible values are: Not registered - not registered to a network and the device is not currently searching for a new operator to register to Registered - registered, 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) - : not possible 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.

4.1.4 Network->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.

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.

4.1.5 Network->LAN

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

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

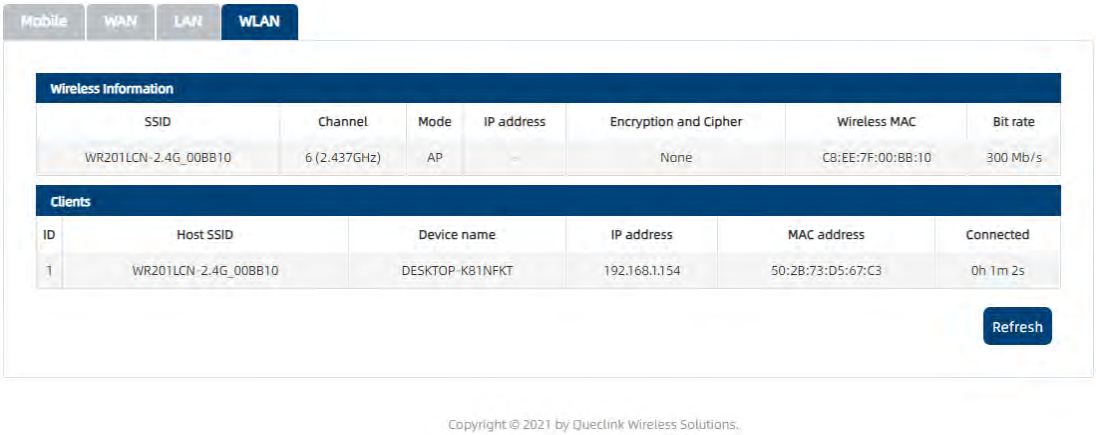
Field Name	Description
LAN Information	
Name	LAN interface name.
IP address	LAN IP address.
Netmask	A netmask is used to define how "large" a network is by specifying which part of the IP address denotes the network and which part denotes the device.
Ethernet MAC address	LAN MAC address.
Clients	
Hostname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

4.1.6 Network->WLAN

This page displays information about wireless connections and associated Wi-Fi stations. When the device 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.

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 CPE's radio can handle. Bit rate will be shared between CPE and other possible devices which connect to local Access Point (AP).

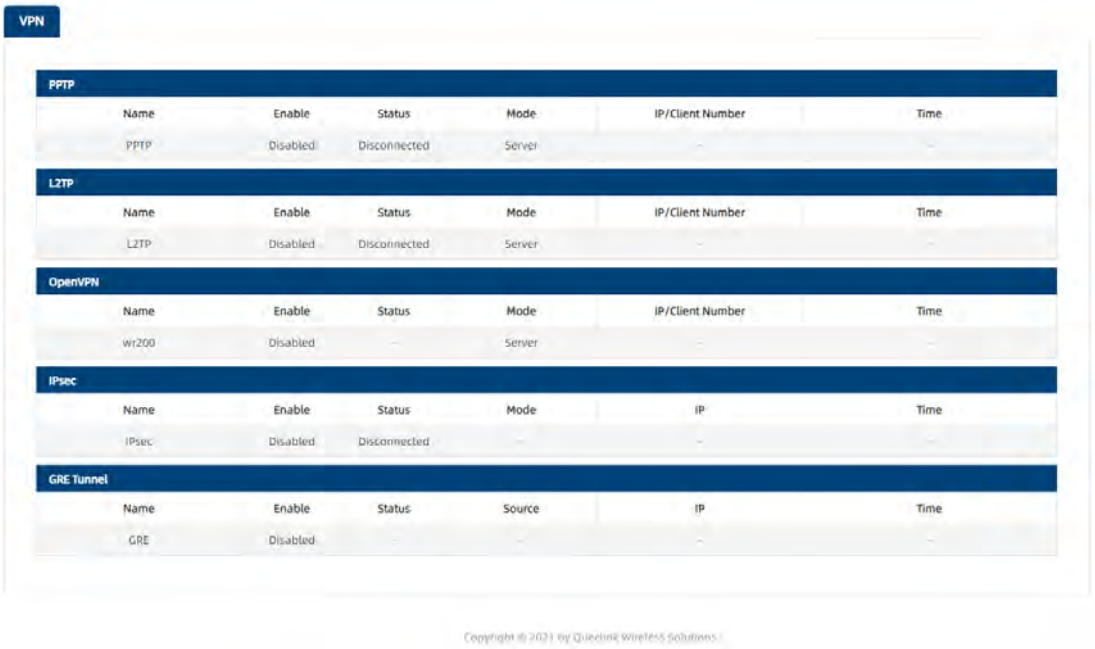
4.1.7 Applications

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

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.

4.1.8 VPN

The VPN table displays the status and connection information of all VPN link. The status is connected if a VPN connection is established. You can also see the IP address (work as client) or connected device number (work as server) in this page.



Field Name	Description
Name	Associated VPN name.
Enable	Display the enable/disable status of this VPN.
Status	Destination network address.
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.

4.1.9 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 on each known MAC address and its corresponding IP address. When the CPE 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 machines in order to find the device with the IP address in question.

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:

ARP Parameter description:

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:

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.

4.1.10 Mobile Traffic

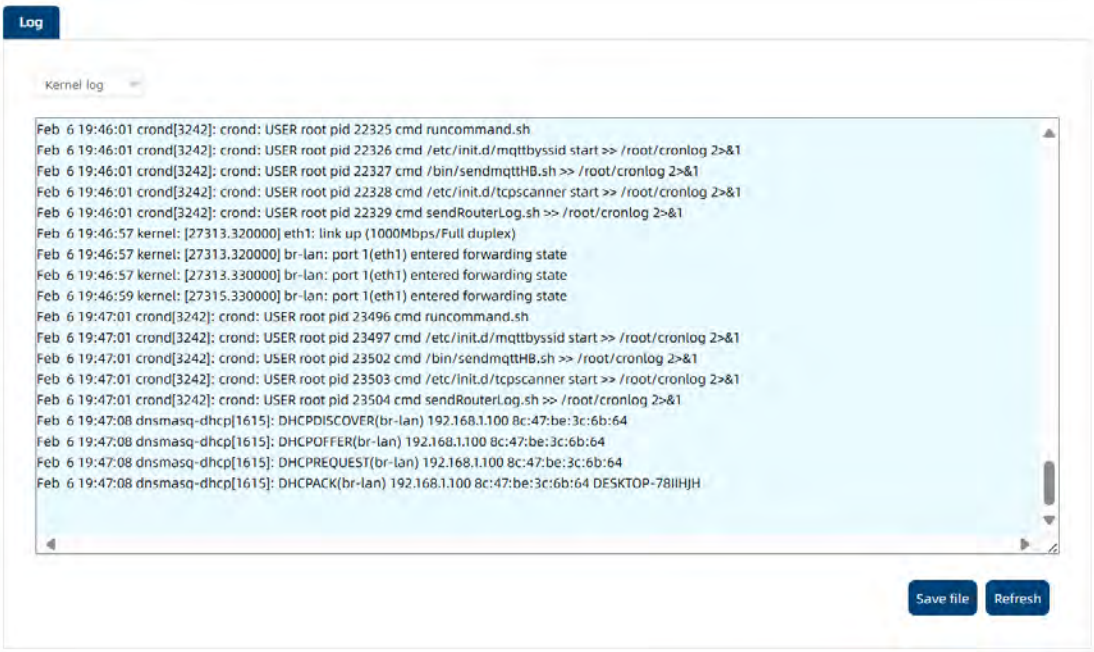
The Mobile Traffic section contains graphs that display mobile data usage values over different periods of time. Different tabs of the Mobile Traffic section display mobile data usage values over different periods of time. You can select the period by day, week and month.

The device accumulates the traffic going through the modem interface; it is not exactly the same as the traffic statistics of operators.

Copyright © 2021 by Queclink Wireless Solutions.

4.1.11 Log

The Log Viewer page is to display the contents of the system log or kernel log. You can select which log file to display with the drop-down box. Refresh button is to refresh the content. You can save the current log as txt file through the Save file button.



4.2 Network

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

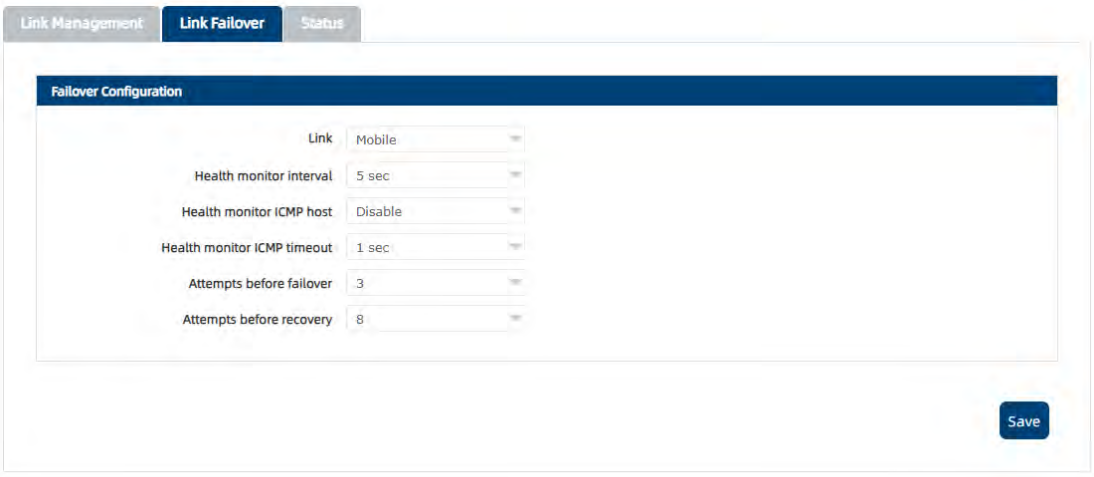
4.2.1 Link Management

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 is 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.

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.

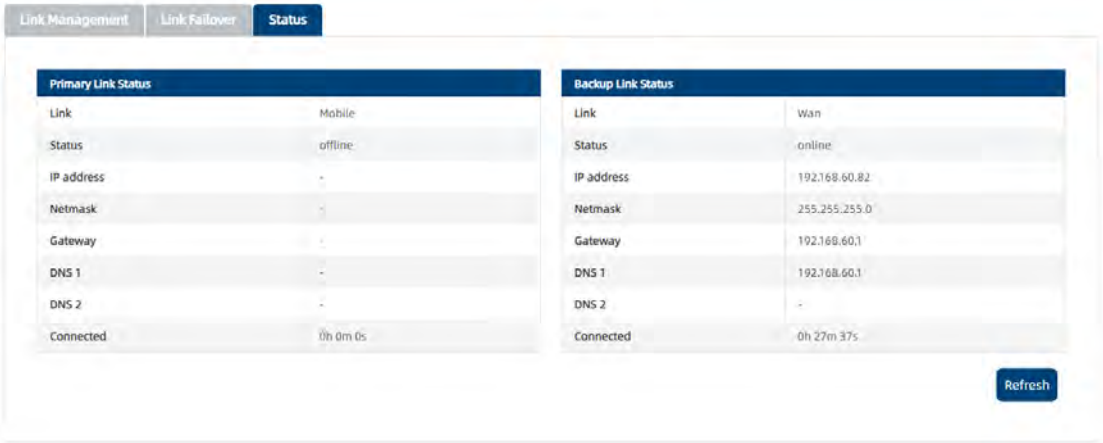
The failover configuration section is to configure the rule of switchover rule. The device use ICMP to check the status of the link, if link is abnormal, the device will switch to another backup link.



Copyright © 2021 by Queclink Wireless Solutions.

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

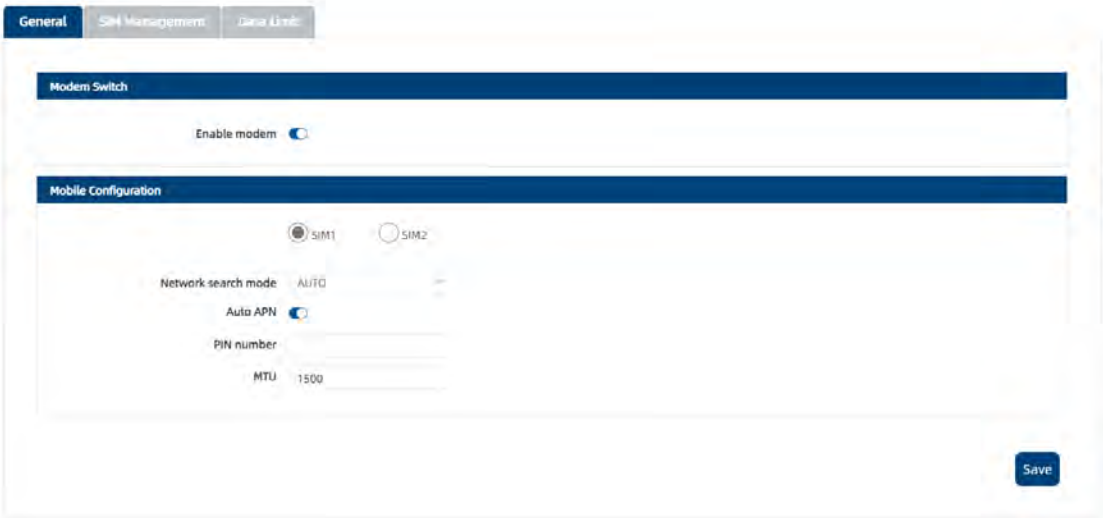
The **Mobile** page is used for setting parameters related to the mobile data connection. There have two SIM slots in the device, each slot can insert a SIM card, and the user can select one SIM as the primary SIM and allow the switchover between two SIMs.

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 still can try 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.



Field	Value	Description
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	Network connection type to connect.
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.

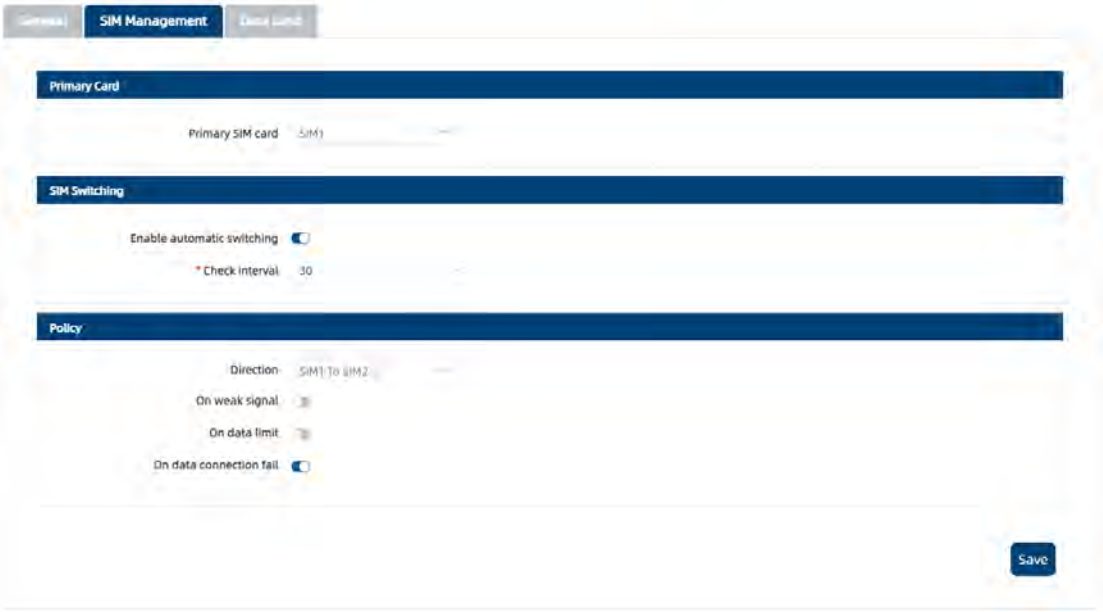
Click Save button to save the configuration and reestablish the connection.

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 the user has two SIM cards. 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 is used to enable automatic SIM switching and to set the SIM switching check interval.

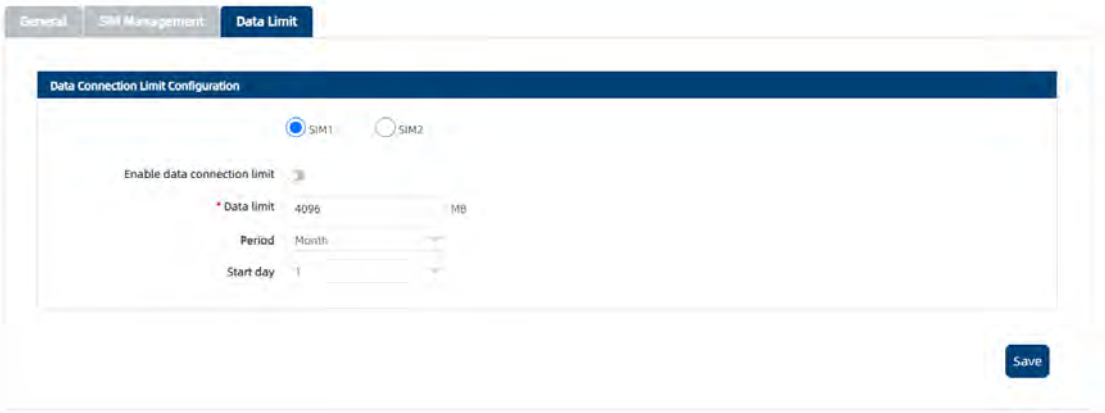


Field	Value	Description
Enable automatic switching	yes|no; default: yes	Turns automatic SIM Switching on or off.
Check interval	integer; default: **30**	The frequency at which the device will check for condition changes corresponding to SIM switch rules. If such a condition happens, the device will perform a switchover, if not - it will check for the same conditions again after the amount of time specified in this field.
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.

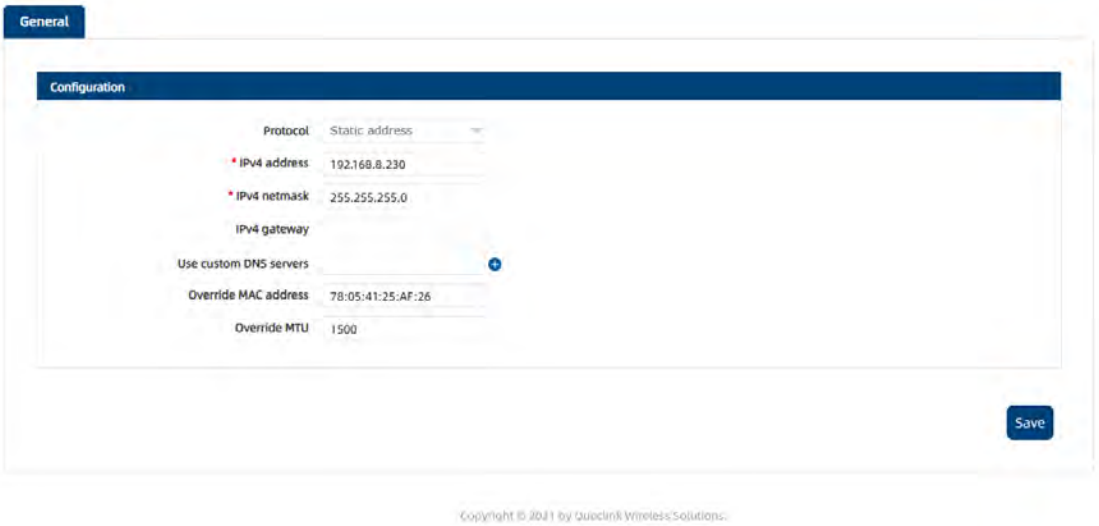


Field	Value	Description
Enable data connection limit	yes|no; default: no	Turns mobile data limitations on or off.
Data limit* (MB)	integer; default: none	The amount of data that is allowed to be downloaded over the specified period of time. When the limit is reached, the device will no longer be able 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 Switching rules 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.

4.2.3 WAN

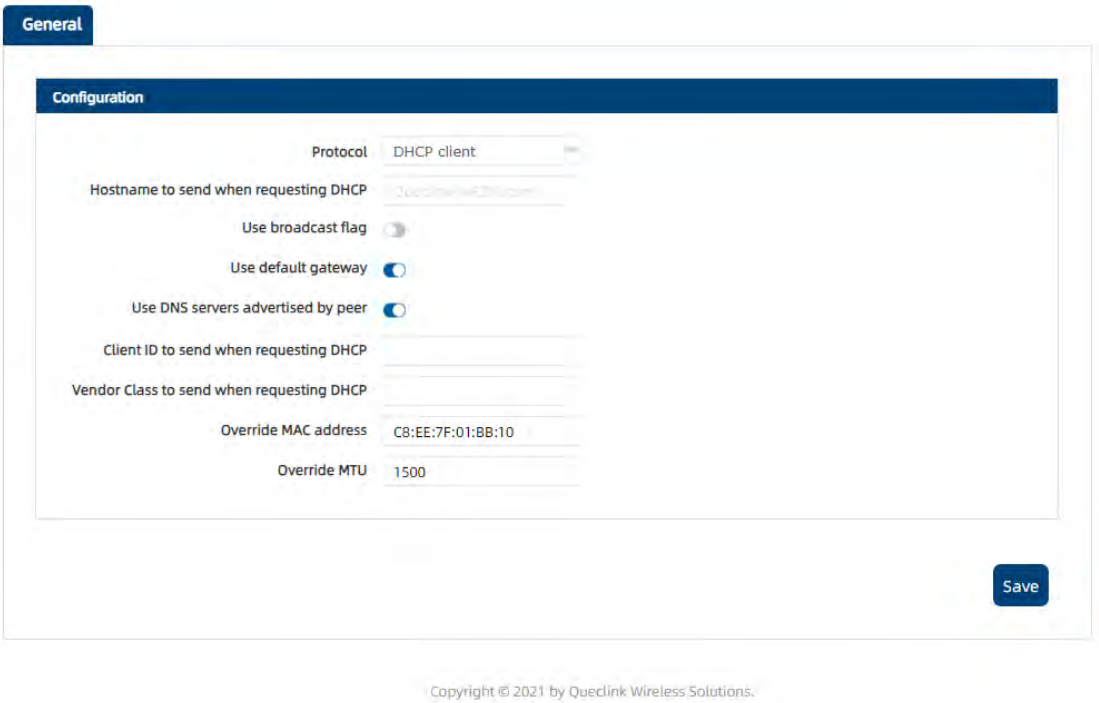
The WAN page is used to configure different protocols for WAN interfaces. The device supports Static, DHCP and PPPoE protocol. You can click Switch Protocol button to display and configure the parameters. The content will change according to which network protocol is selected.

The Static protocol is used when there is no DHCP server available. Therefore, in order to connect to the internet, you configure a static IP address in accordance to that source. The following is an example of static configuration page:



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.

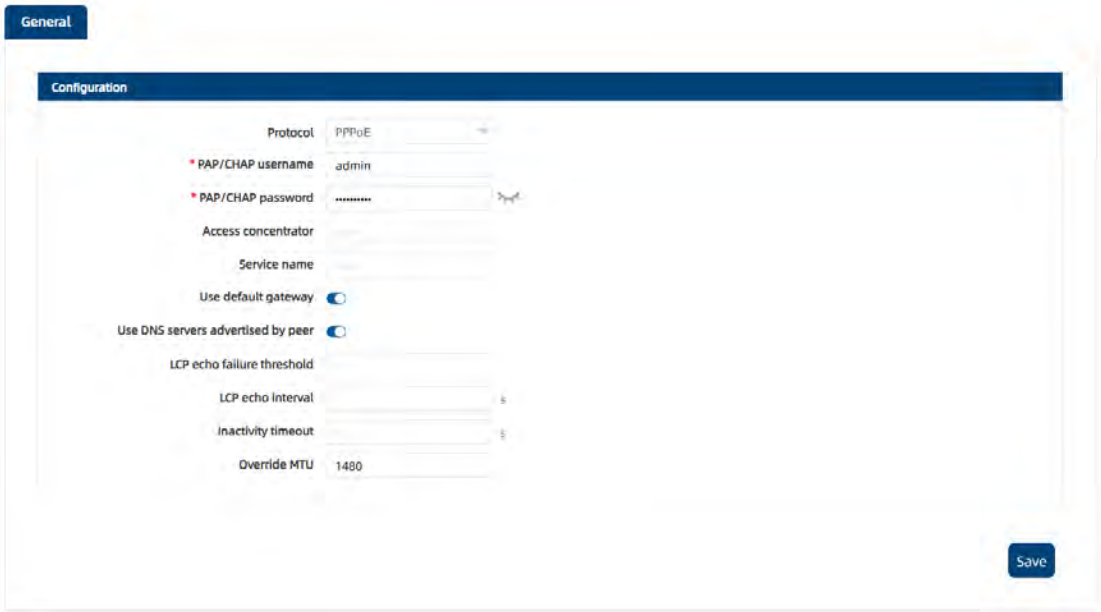
The DHCP protocol should be used when the source of your internet has a DHCP server. The following is an example of DHCP configuration page:



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 with the internet. The following is an example of PPPoE configuration page:

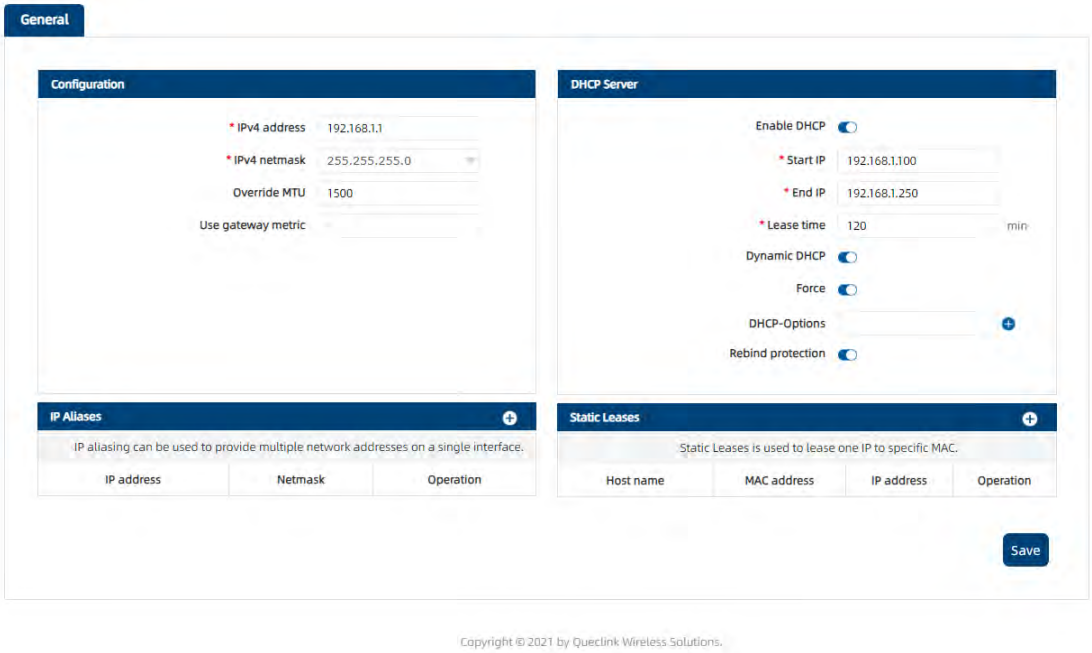


Field Name	Value	Description
Protocol	Static|DHCP|PPPoE; default: **DHCP**	The protocol used by the WAN interface.
PAP/CHAP username	string; default: **none**	The username that you use to connect to your carrier's network.
PAP/CHAP password	string; default: **none**	The password that you use to connect 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 WR201. The following is the example configuration page of LAN port.



Copyright © 2021 by Queclink Wireless Solutions.

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 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.

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 2min (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.

4.2.5 WLAN

WR201 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:

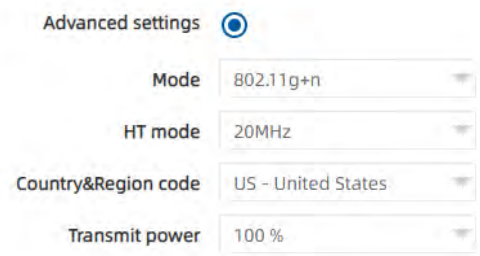
The page will display the overview of the Wireless Configuration. It displays all configured access points and stations. You can disable or enable the Wi-Fi interfaces, remove unwanted access points or stations or enter a configuration window of any Wi-Fi interface, where you can configure this interface 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.

Field Name	Value	Description
Enable Wireless	yes|no; Default: **no**	To enable or disable this AP.
SSID	string; default: WR201-2.4G_(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.

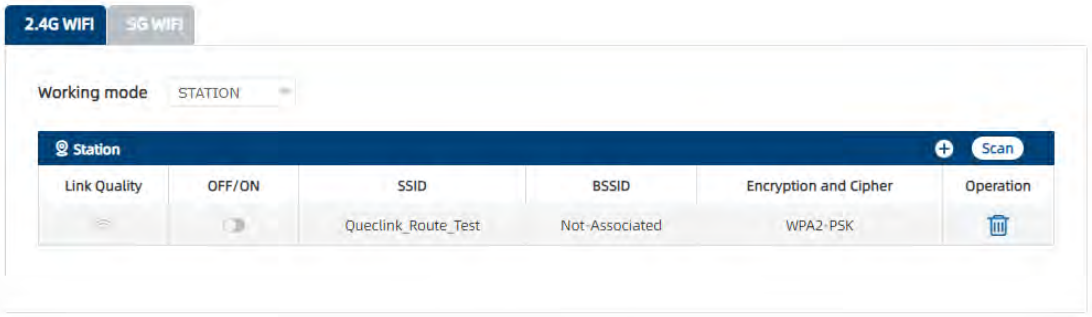


Field Name	Value	Description
Mode	802.11b|802.11g| 802.11g+n; Default: 802.11g+n	Wireless protocol used. Different modes provide different wireless standard support which directly impacts the radio's throughput performance.
Country code	country code; Default: US	SO/IEC 3166 alpha2 country codes as defined 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:**

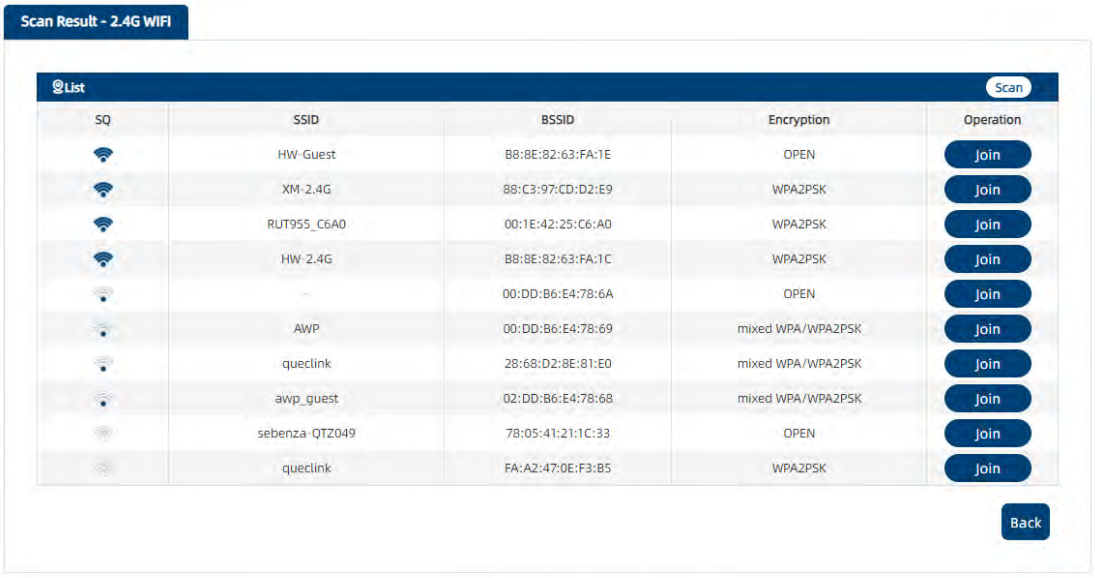
WR201 can also work as a Wi-Fi client.

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.



Copyright © 2021 by Queclink Wireless Solutions.

After the scan finishes, you will see a list of Wi-Fi Access Points. Choose one according to your liking and click the Join button next to it, enter the password to connect to that access point.



Copyright © 2021 by Queclink Wireless Solutions.

4.2.6 Routing

4.2.6.1 Static

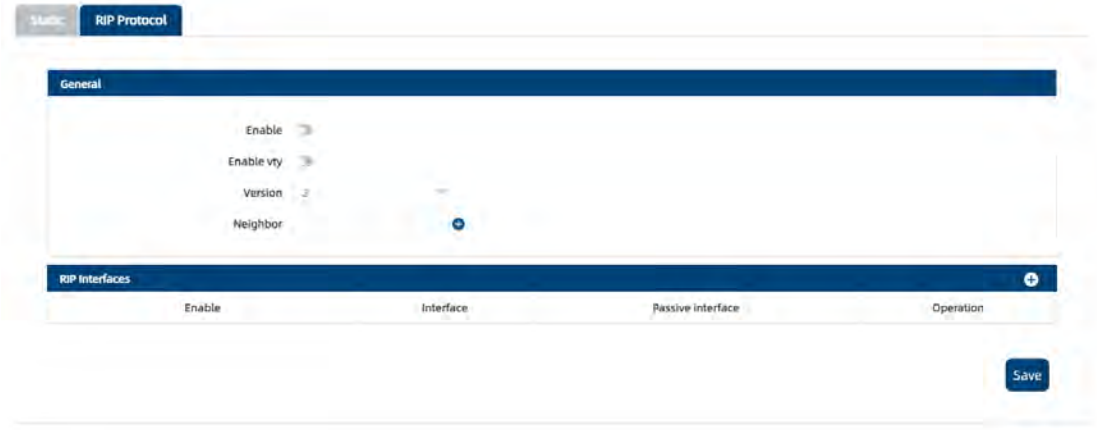
Static routes specify over which interface and gateway a certain host or network can be reached. You can configure your own custom routes in this page. You can configure multi static route in the device.

Copyright © 2021 By Queclink Wireless Solutions.

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.

4.2.6.2 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.

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 addres.
Enable	yes|no; Default: no	Toggles RIP Interface ON or OFF.

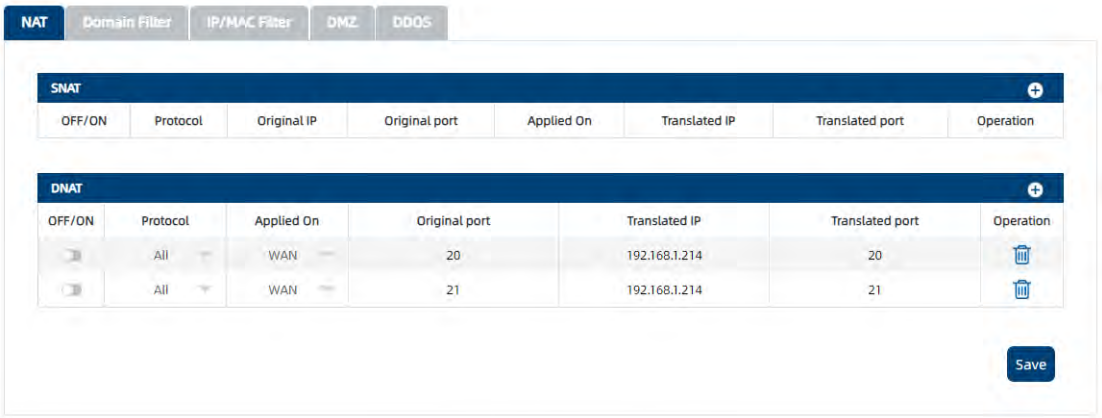
Interface	network interface; Default: br-lan	Network interface to be used with the RIP interface.
Passive interface	yes|no; Default: no	Sets the specified interface to passive mode. On passive mode interface, all receiving packets are processed as normal and rip does not send either multicast or unicast RIP packets.

4.2.7 Firewall

4.2.7.1 NAT

Network Address Translation (NAT) is a process in which one or more local IP address is 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.



Copyright © 2021 by Queclink Wireless Solutions.

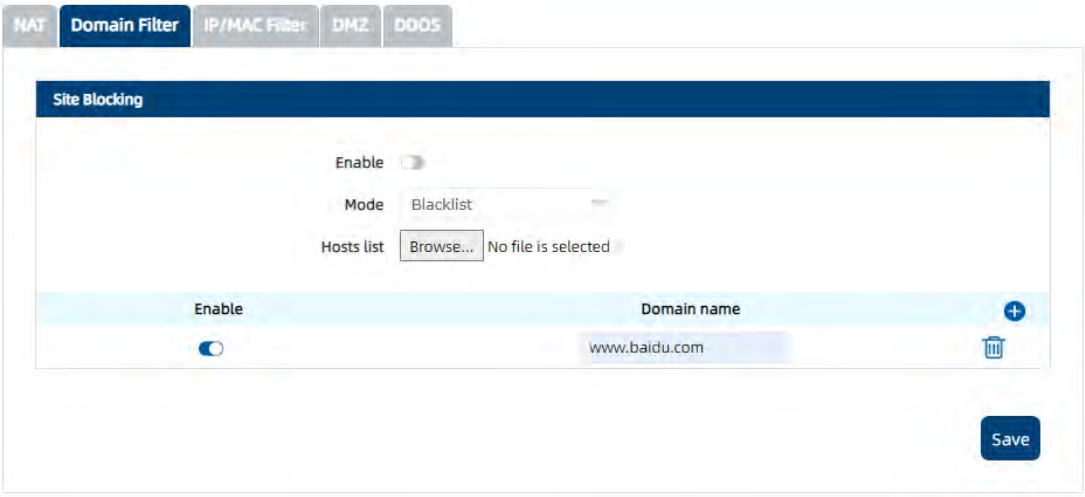
Field Name	Value	Description
OFF/ON	ON|OFF	To turn on/off the section.
Protocol	ALL|TCP|UDP|ICMP|TCP +UDP Default: ALL	Select the protocol to translate the IP and Port.
Original IP	A.B.C.D	The initial IP address to be translated.
Original Port	1~65535	The initial port to be translated.
Applied On	LAN|WAN|PPTP|L2TP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

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.

4.2.7.2 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.



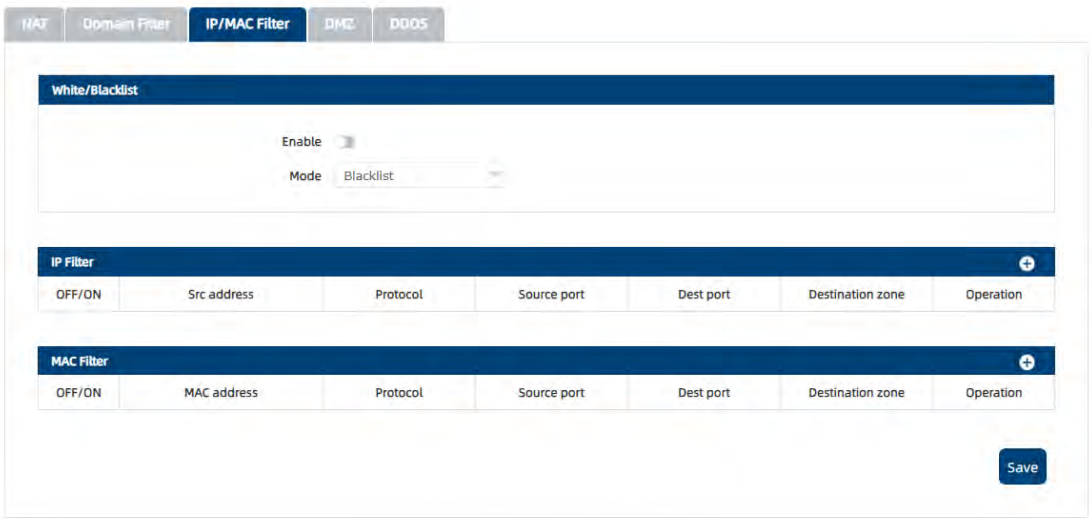
Copyright © 2021 by Queclink Wireless Solutions.

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.

4.2.7.3 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.



Copyright © 2021 by Quectlink Wireless Solutions

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.

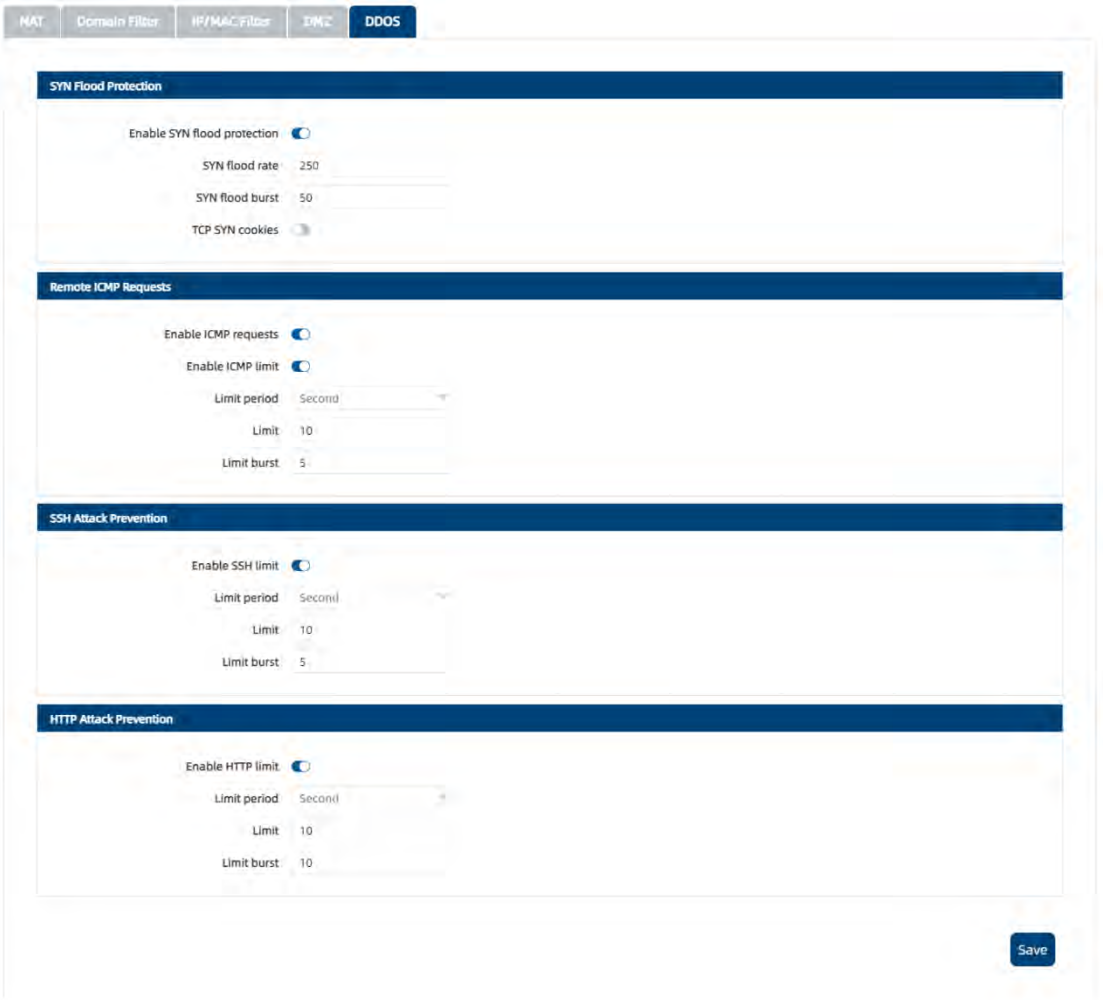
4.2.7.4 DMZ

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.

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.

4.2.7.5 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.

4.3 Applications

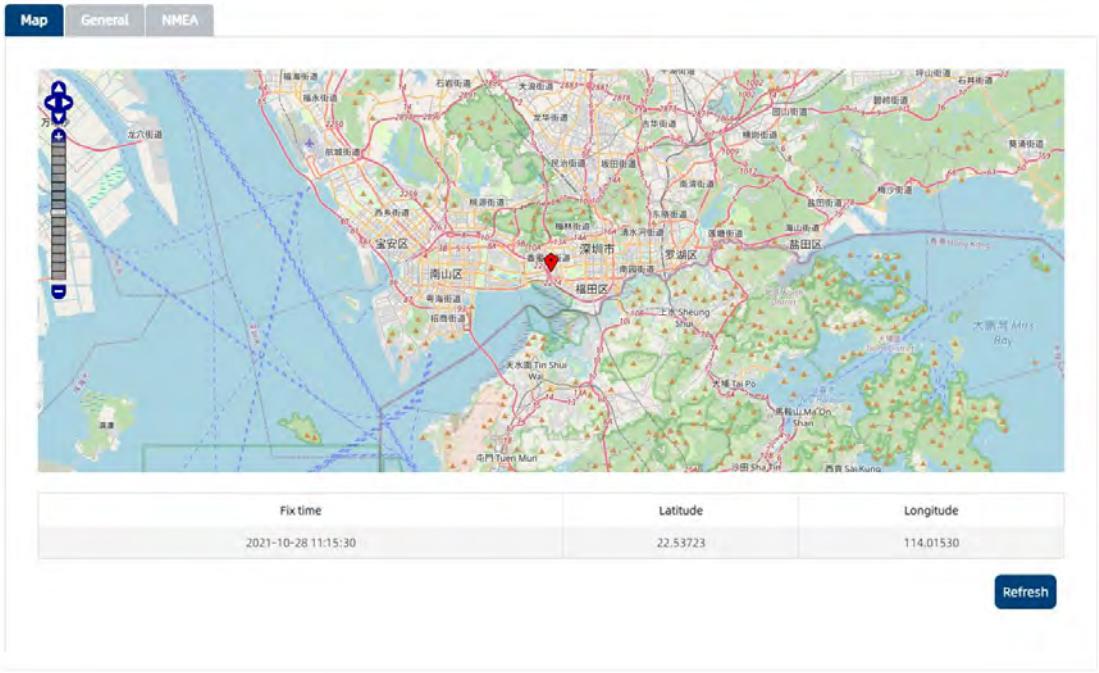
This section shows you how to configure the service applications of the device.

4.3.1 GPS (Available for Specific Models Only)

4.3.1.1 Map

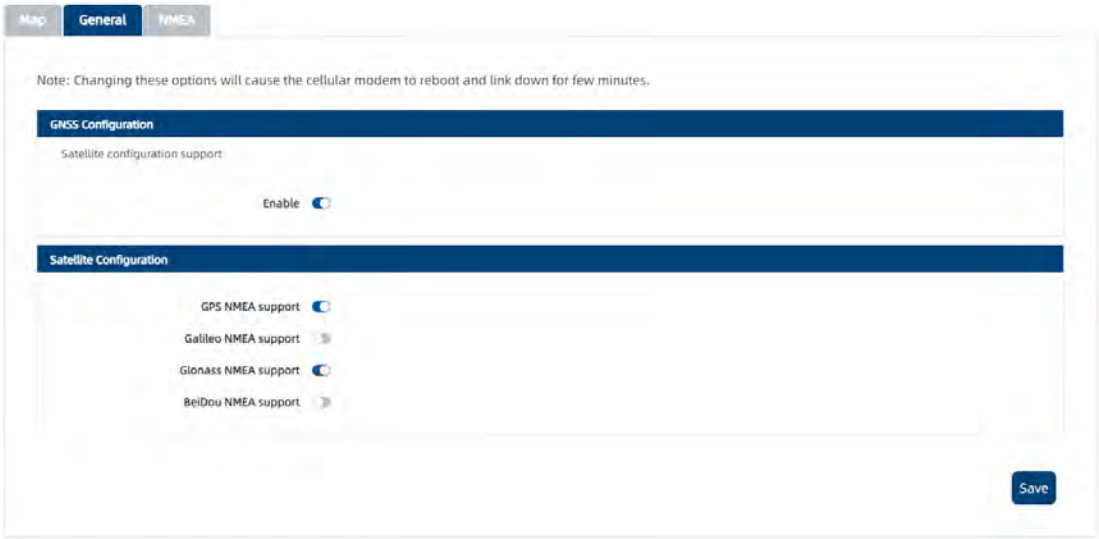
The **Global Positioning System** (**GPS**) is a space-based radio navigation system.

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 outside, and GPS is enabled in the general page.



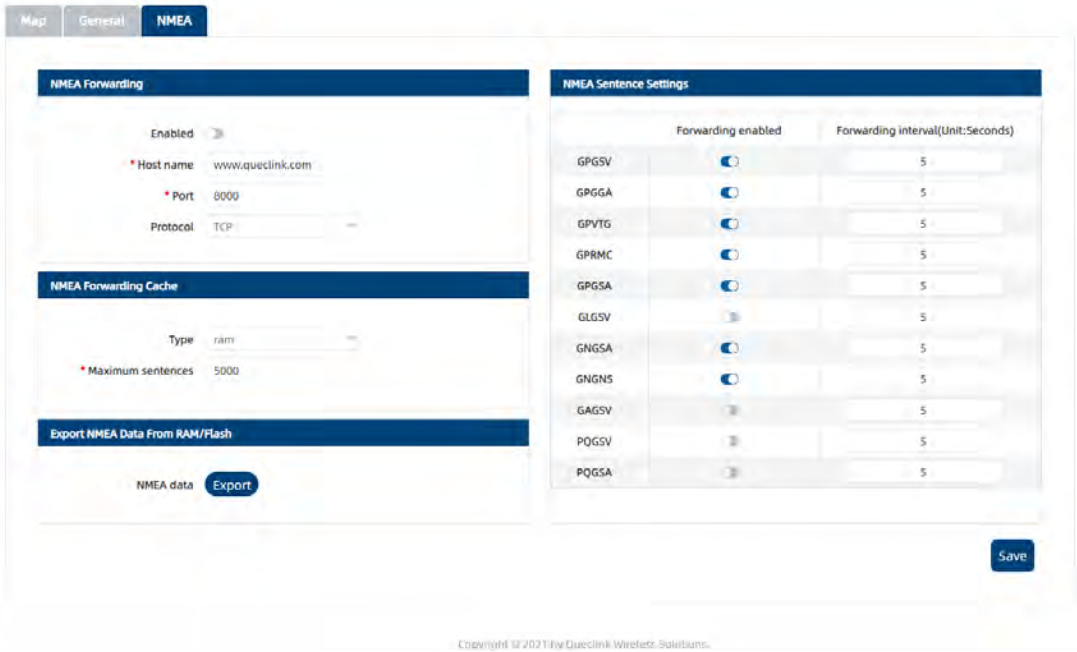
4.3.1.2 General

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 you attach the GPS antenna on the device and place it outside 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.



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];	Port number of the server to which NMEA data

	default: 8500	will be forwarded.

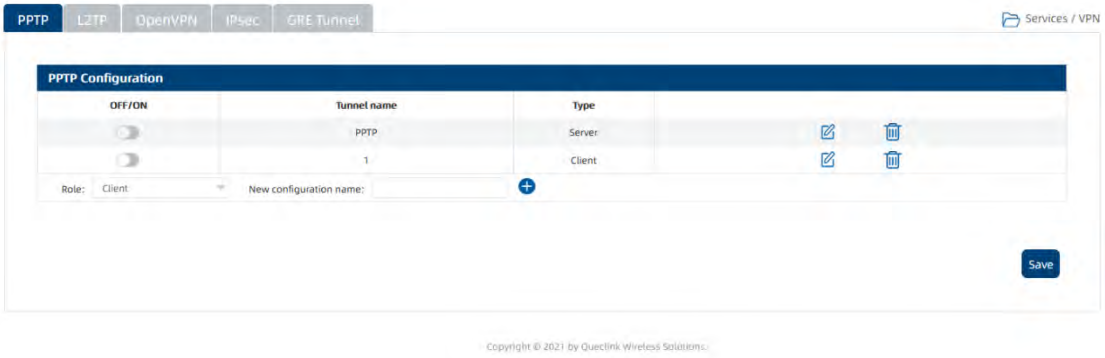
The device caches NMEA forwarding information if NMEA forwarding is enabled. This section is used to select the memory type where the cache will be stored and the maximum amount of data that will be saved.
The NMEA sentence settings section provides the possibility to configure which NMEA sentences will be forwarded or collected and at specify period.

4.3.2 VPN

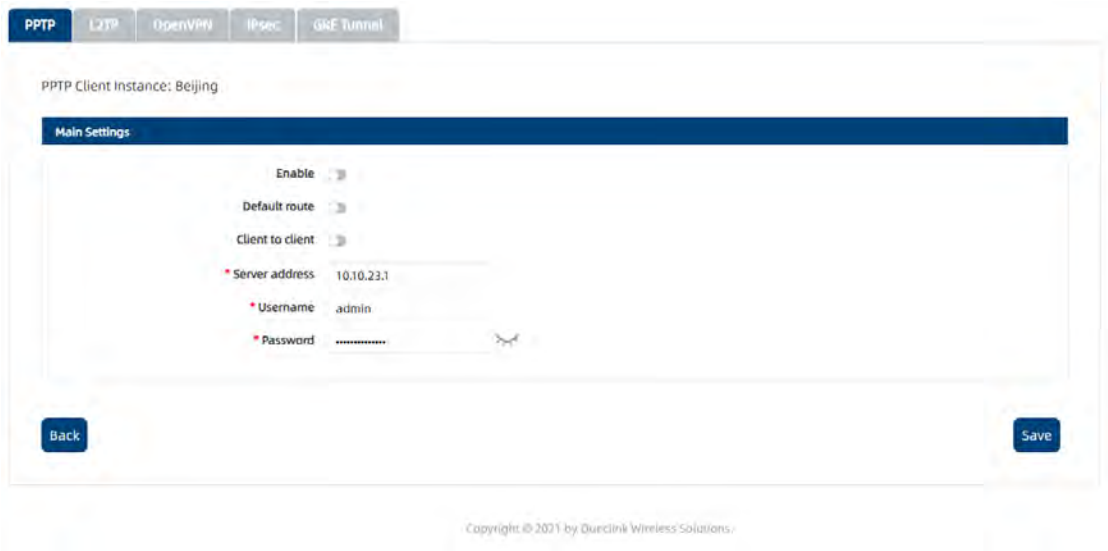
A virtual private network (VPN), is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. The 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.

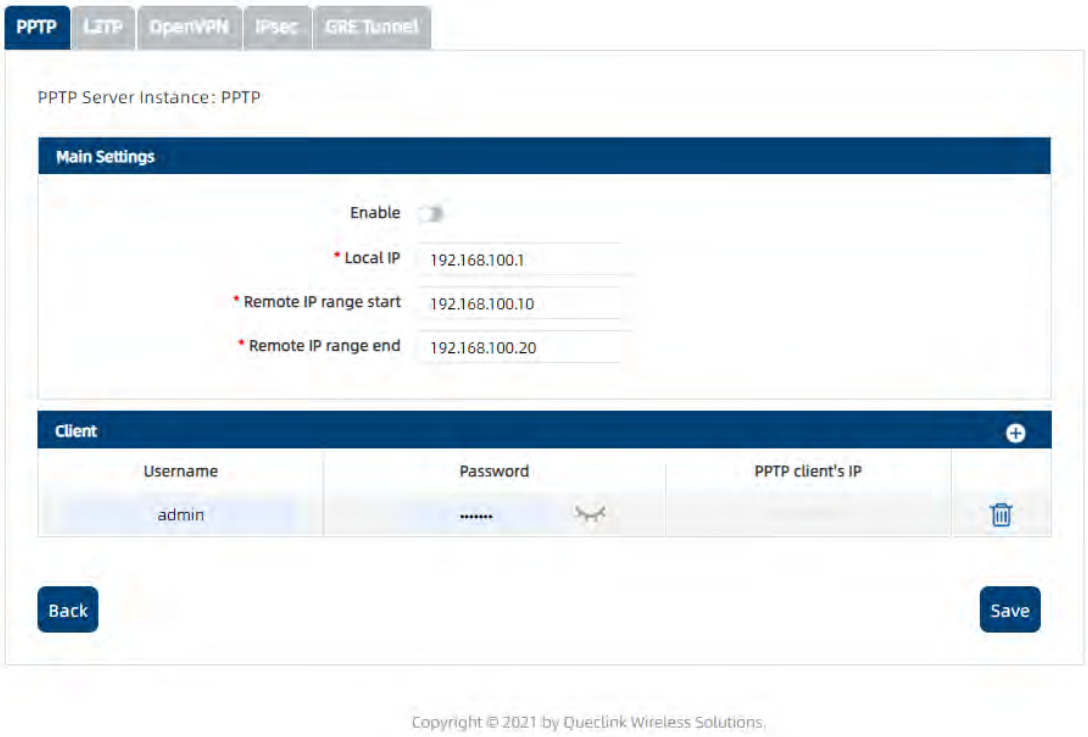


Refer to the figure and table below for information on the PPTP client's configuration fields:

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:

An **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).

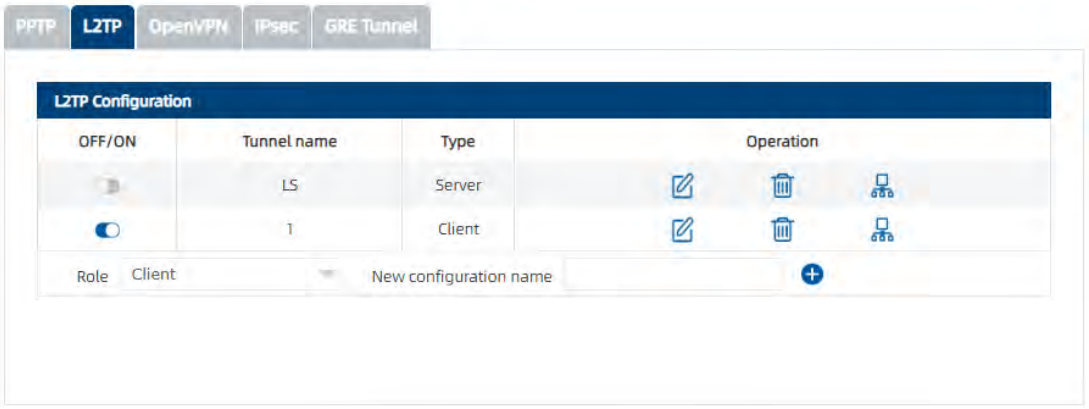


Refer to the figure and table below for information on the PPTP client's configuration fields:

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: WR201	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

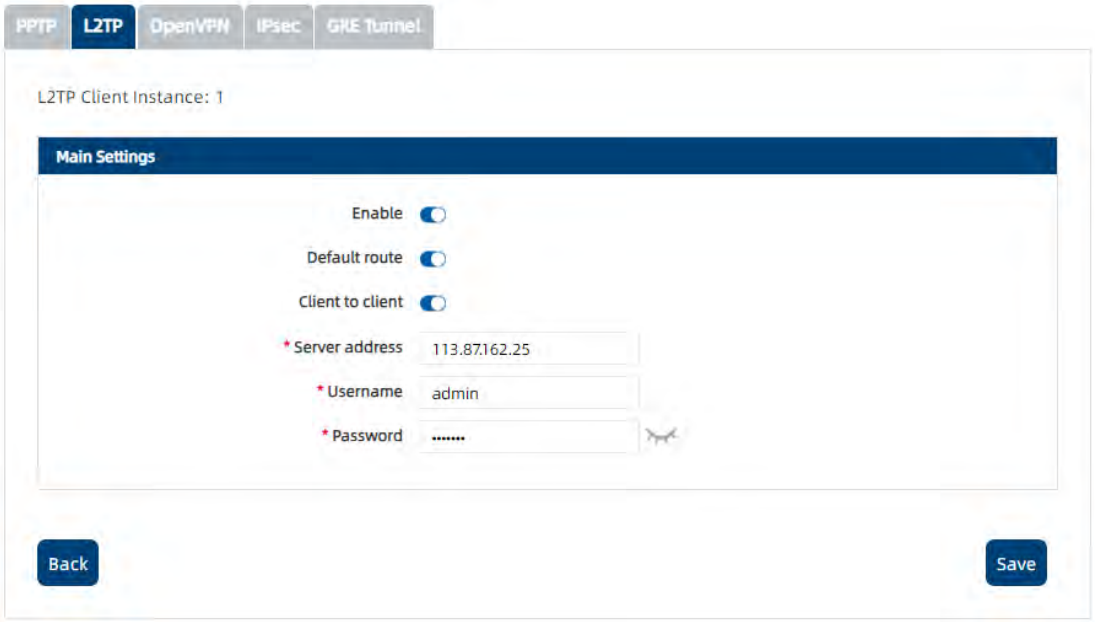
Layer 2 Tunneling Protocol (**L2TP**) is a tunneling protocol used to support virtual private networks (VPNs). It can work as client or server mode.



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.

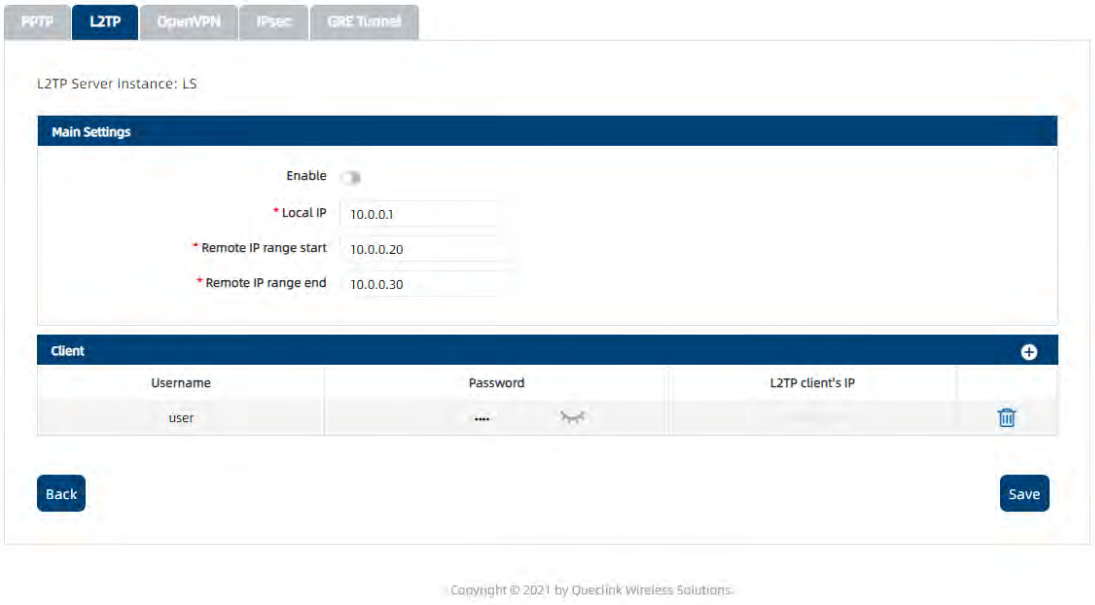
Refer to the figure and table below for information on the L2TP client's configuration fields:

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:

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.

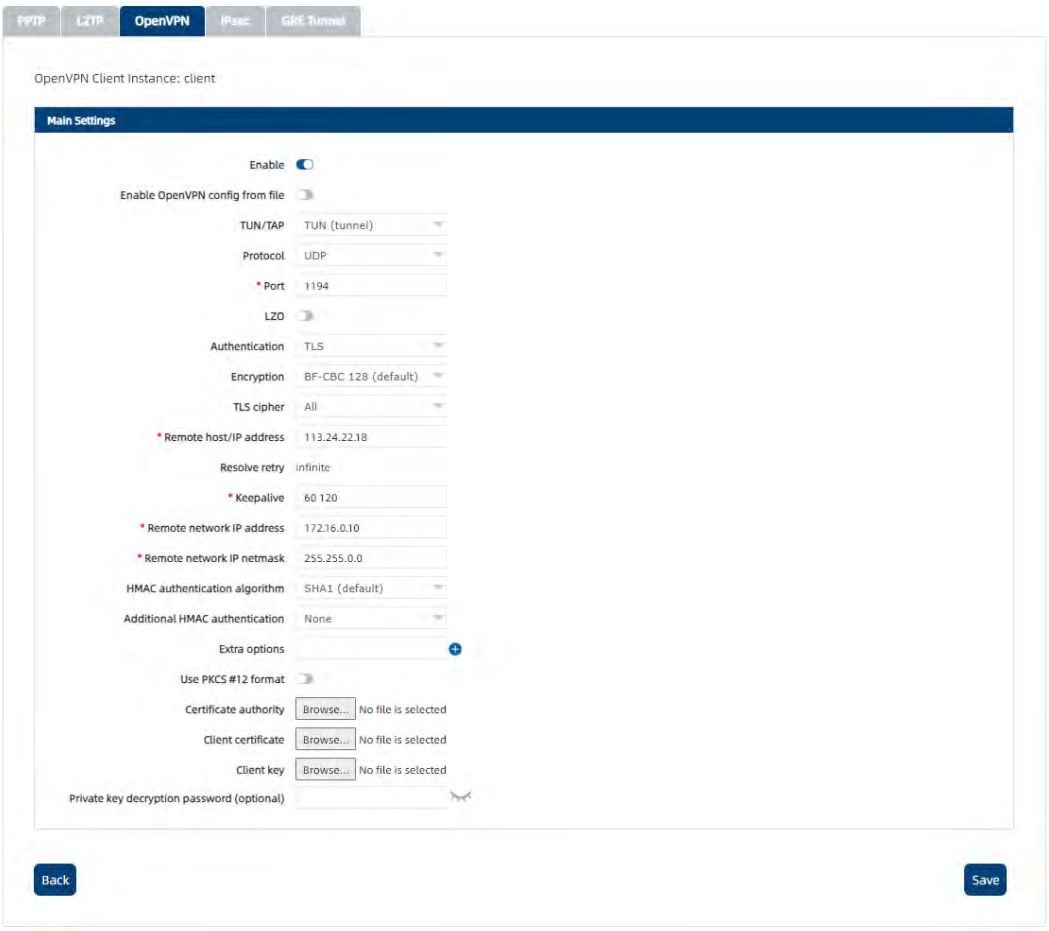
Username	string; default: user	Username used for authentication to this L2TP server.
Password	string; default: pass	Password used for authentication to this L2TP server.
L2TP Client's IP	ip; default: none	Assigns an IP address to the client that uses the adjacent authentication info. This field is optional 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.
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

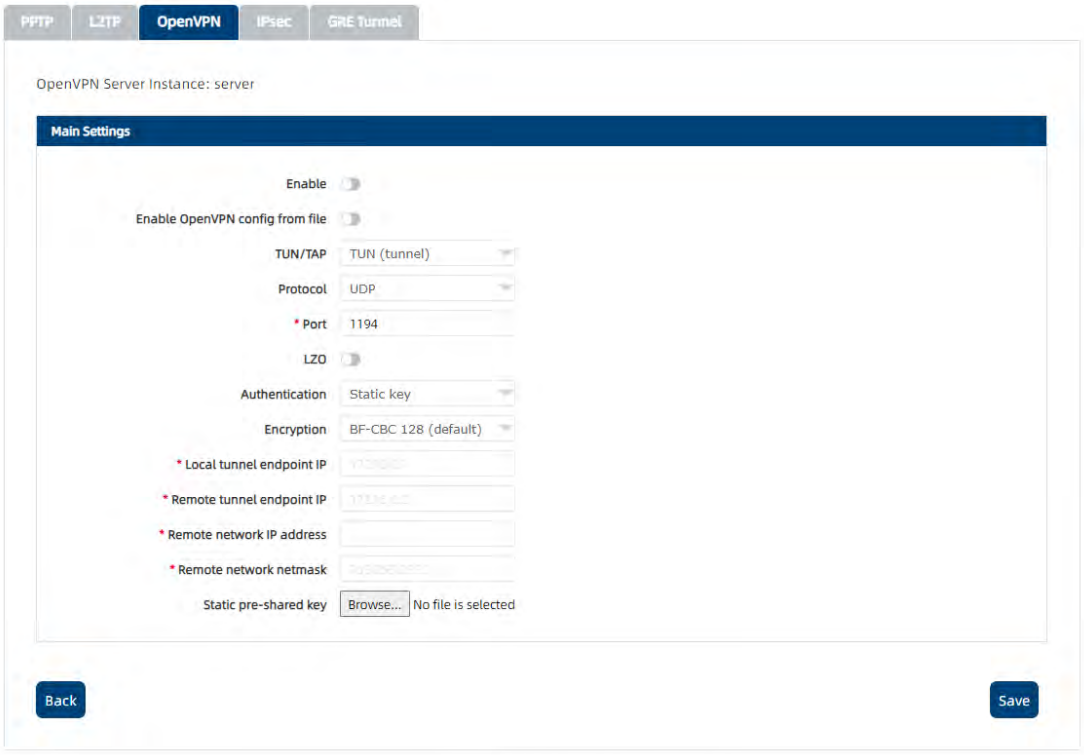
		when reliability is crucial (for example, in file transfer). User Datagram Protocol (UDP) - packets are sent to the recipient without error-checking or back-and-forth quality control, meaning that when packets are lost, they are gone forever. This makes it less reliable but faster than TCP; therefore, 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	Algorithm used for packet encryption.

	128|AES-192-CBC 192|AES-256-CBC 256|none ; default: BF-CBC 128	
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.
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 one defines a time window, which is used to restart the OpenVPN service if no ICMP response is received during the specified time slice. When this value is specfiied on the OpenVPN server, it overrides the 'keep alive' values set on client instances. 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	string; default: none	Uploads PKCS #12 certificate chain file.

chain		
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	The value of the key direction parameter should be complementary on either side (client and server) of the connection. If one side uses 0, the other side should use 1, or both sides should omit the parameter altogether.
TLS/Password: Certificate authority	.ca file; default: none	Certificate authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
TLS: Client certificate	.crt file; default: none	Client certificate 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.
TLS: Client key	.key file; default: none	Authenticates the client to the server and establishes precisely who they are.
TLS: Private key decryption password (optional)	string; default: none	A password used to decrypt the server's private key. Use only if server's .key file is encrypted with a password.
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 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.
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 Open SSL utilities on any type of host machine. One of the most popular utilities used for this purpose is called 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.

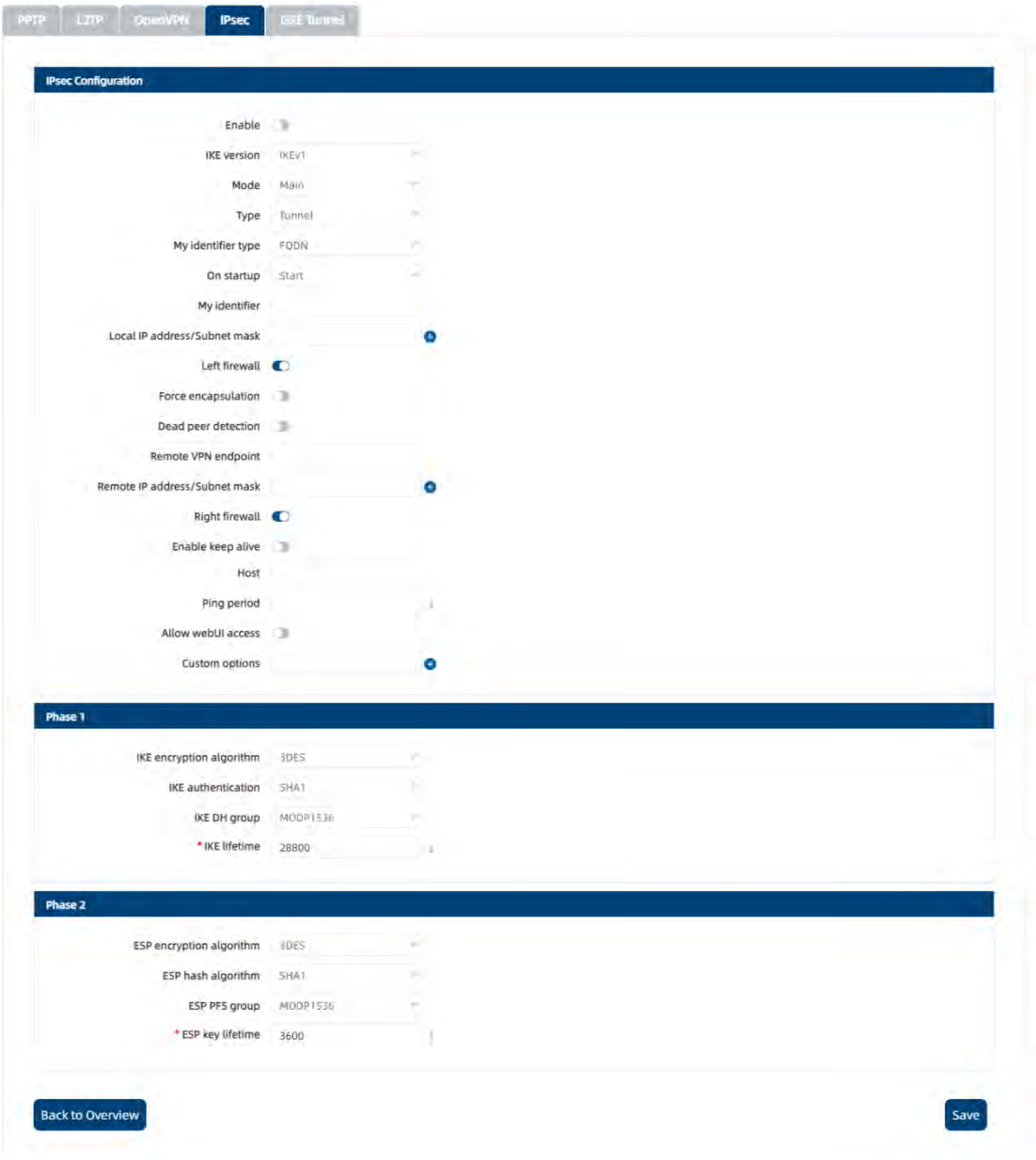
Static key: Remote network IP address	ip; default: none	LAN IP address of the remote network (client).
Static key: Remote network IP netmask	netmask; default: none	LAN IP subnet mask of the remote network (client).
TLS/TLS/Password: TLS cipher	All|DHE+RSA|Custom; default: All	Packet encryption algorithm 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 one defines a time window, which is used to restart the OpenVPN service if no ICMP response is received during the specified time slice. When this value is specified on the OpenVPN server, it overrides the 'keep alive' values set on client instances. 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 a way to "push" routes and other additional OpenVPN options to connecting clients.
TLS/TLS/Password: Allow duplicate certificates	yes|no; default: no	When enabled 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 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: 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	.key file; default: none	Uploads a secret key file used for server–

pre-shared key		client authentication.
TLS/TLS/Password: Certificate authority	.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.
TLS/TLS/Password: Server certificate	.crt file; default: none	A type of digital certificate that is 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 the Diffie-Hellman (DH) key-exchange.
TLS/TLS/Password: CRL file (optional)	.pem file|.crl file; default: none	A certificate revocation list (CRL) file is a list of certificates that have been revoked by the certificate authority (CA). It indicates which certificates are no longer accepted by the CA and therefore cannot be authenticated to the server.

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

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.



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 of 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 networks	None|LAN|Wired|Wi-Fi|Mobile|custom; default: none	Select networks which should be passthrough and excluded from routing through tunnel
Allow WebUI access	yes|no; default: no	Allows WebUI access for hosts in the VPN network.
Custom options	ipsec options; default: none	Provides the possibility to further customize the connection by adding extra IPsec options.

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|MODP	Diffie-Hellman (DH) group used in the key exchange process. Higher group numbers

	3072|MODP4096; default: MODP1536	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.

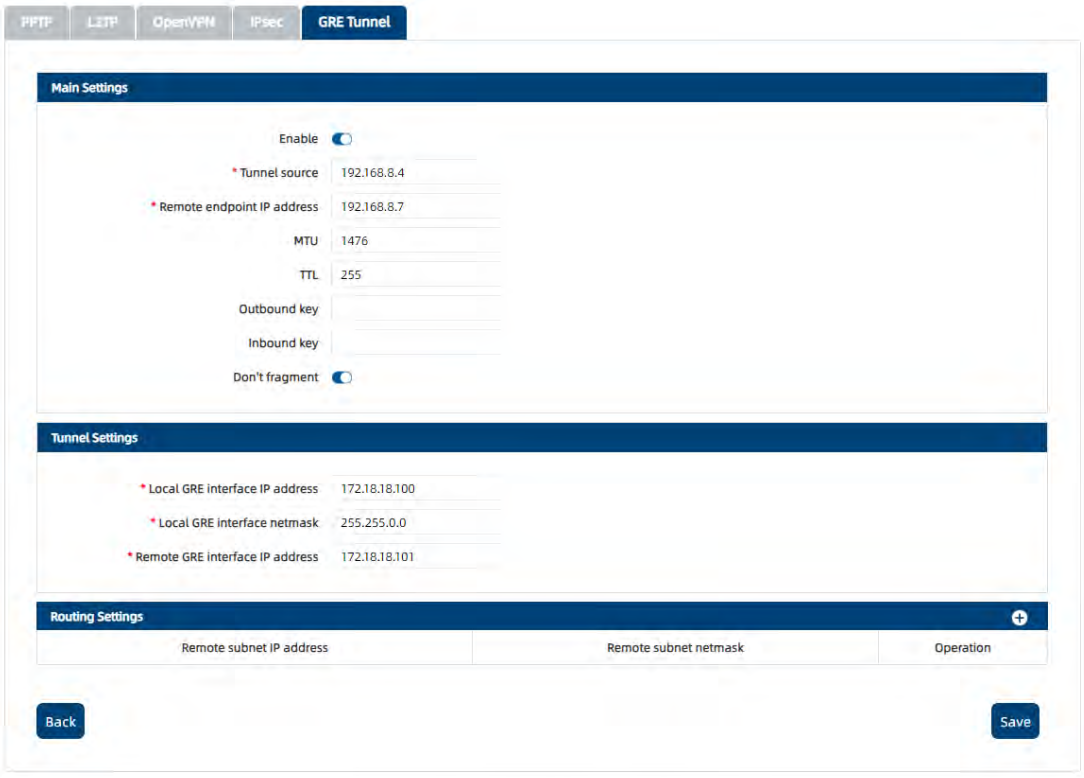
4.3.2.5 GRE Tunnel

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 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.

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.

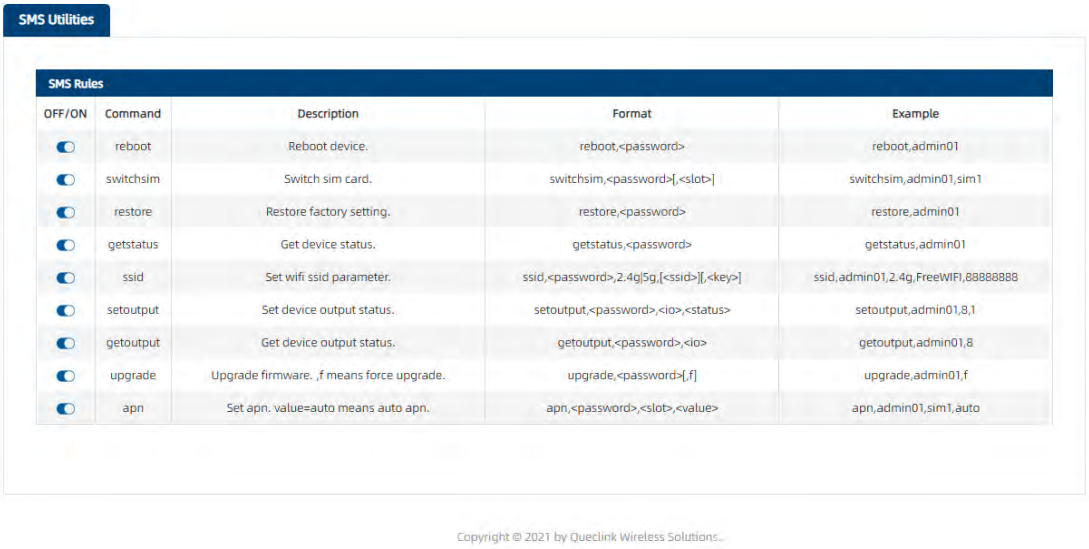
Routing settings are used to configure routes to networks that are behind the device that hosts the opposite GRE instance. To add a new route, simply click the 'Add' button. For information on

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 device control. It contains a list of rules that perform certain actions when they are activated by SMS messages.

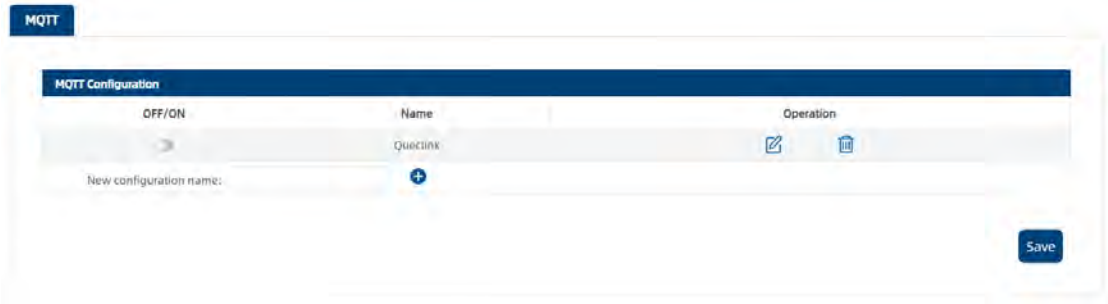


The entire list contains 9 commands. The user can reboot, switch SIM card, restore to factory setting or get device status by sending a SMS text following the rule: “SMS text” password, for example, to reboot a device, you can send ‘reboot admin01’ SMS to the mobile number of this device.

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

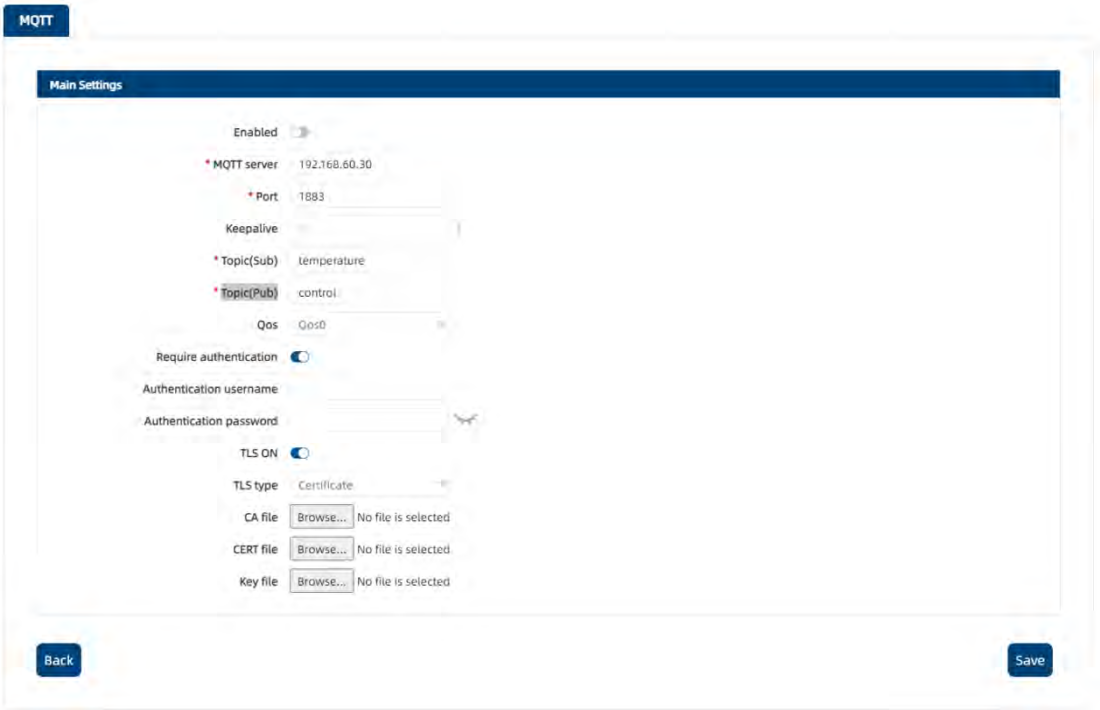
4.3.4 MQTT

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 running at the same time.



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.

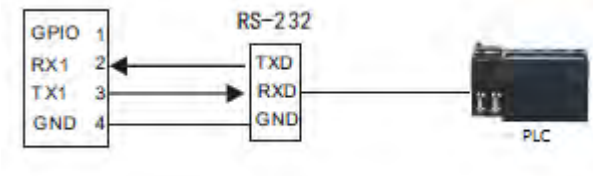
4.3.5 RS232/RS485

RS232 and RS485 functions are to 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. WR201 supports one RS232 and three RS-485 ports. Serial port provides a way to transfer serial data to IP network, or vice versa.

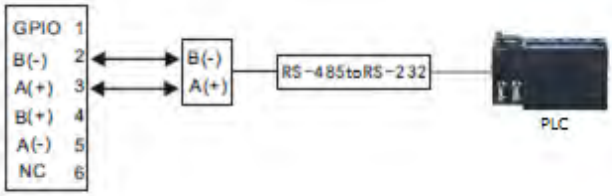
Hardware connection:

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

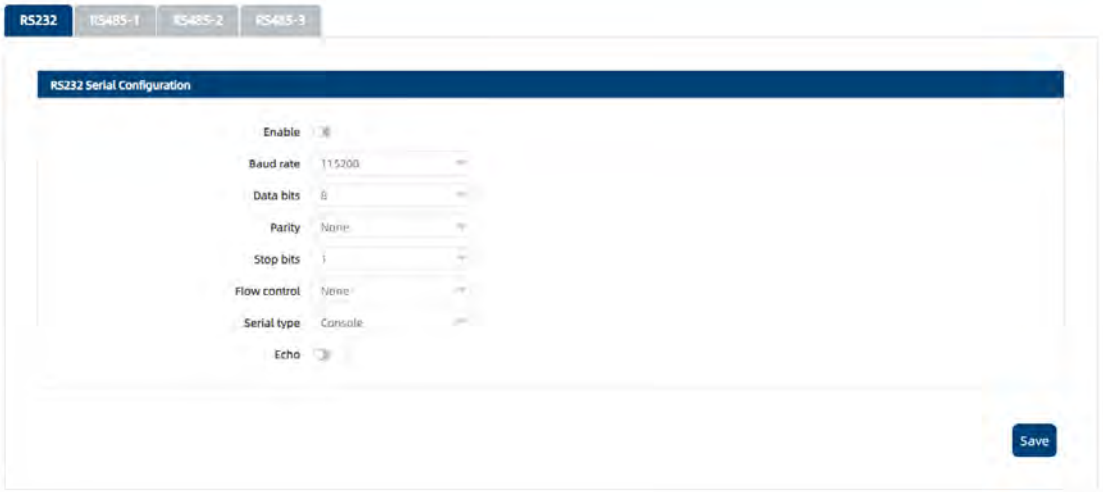
RS232 connection:



RS485 connection:



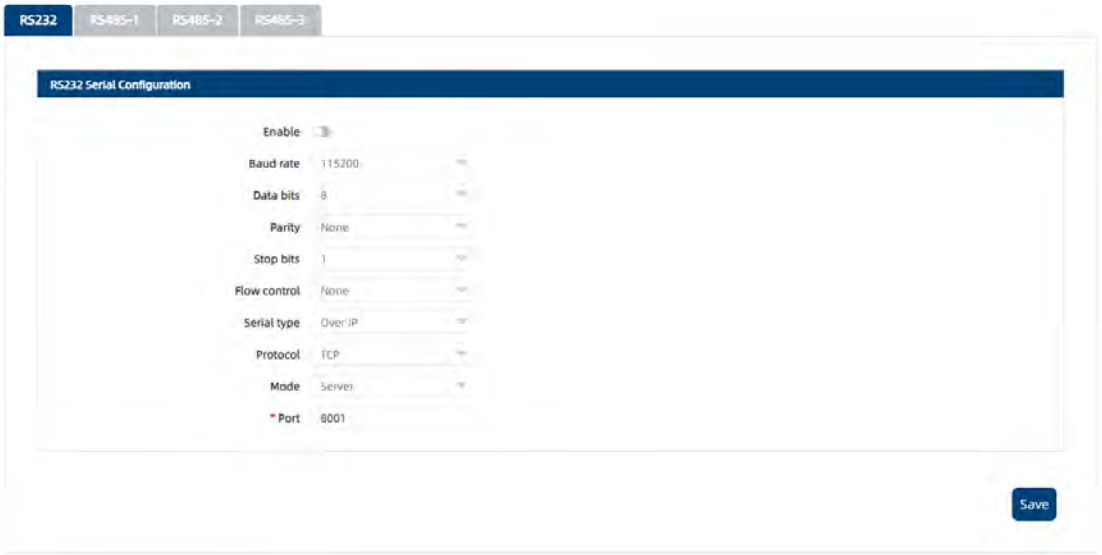
The user can configure the parameters of RS232 port, including baud rate, data bits, etc. The serial type is the working type of RS232. By default, RS232 is working as a console port.



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

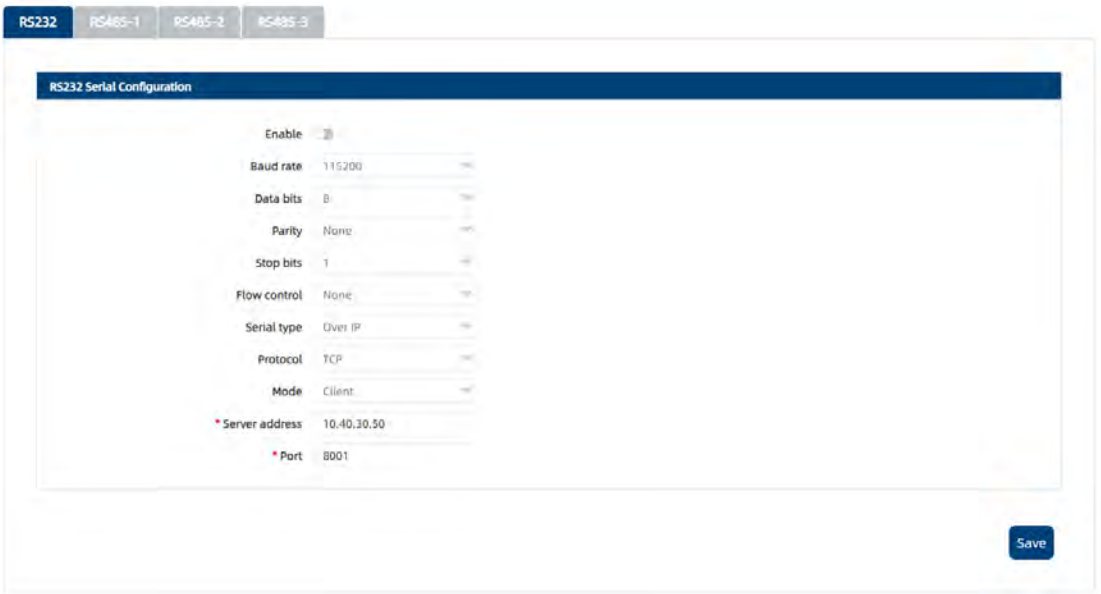
		Even (**E**) - the parity bit is set so that the number of "logical ones (1s)" has to be even
Stop bits	1|2; Default: **1**	Stop bits sent at the end of every character allow the receiving signal hardware to detect the end of a character and to resynchronize with the character stream. Electronic devices 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	Console|Over IP|Modbus; 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 the data between RS232/RS385 ports and IP network. When selecting serial type as “Over IP” and “Mode” as “Server”, the page will display IP configuration parameters:



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	host|ip; 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.

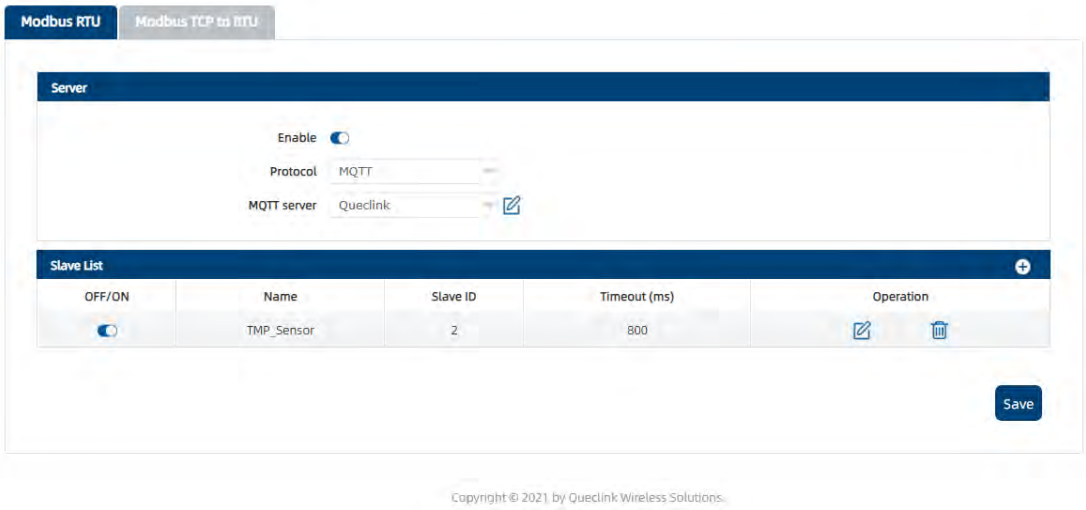
When selecting serial type as “Modbus”, the serial port will work as a Modbus interface, the device can receive and forward Modbus commands from MQTT server or Modbus TCP master. You can configure relevant parameters in the “Application->Modbus” page.

4.3.6 Modbus

This page is to configure the functions related to Modbus function. Before configuring any parameters, you need to configure the type of serial port 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:



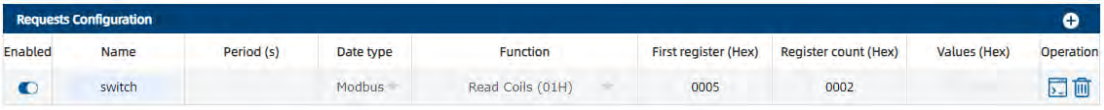
To forward the Modbus data to MQTT server, you must select a MQTT server in the server section. Then click “add” button on the slave list table to add a Modbus request.

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:



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	Modbus PDU	Only support PDU now.
Function	Read Coils (01H) | Write Single Coil (05H) | Write Multiple Coils (0FH) | Read Input Register (04H) | Read	Modbus function used in Modbus request.

	Multiple Holding Register (03H) | Write Single Holding Register (06H) | Write Multiple Holding Register (10H); default: **Read Coils**	
First Register (Hex)	String [1..FFFF]; default: **1**	First Modbus register from which data will be read.
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

The device communicates with MQTT server with JSON format. The format from the MQTT server to the device is:

Field Name	Value	Description
service	String	Service ID. Used to identify the corresponding service. 1 represents UART port.
id	Integer	ID of the message, to identify the message
slave	Integer	MODBUS slave ID
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
First Register (Hex)	String [1..FFFF]	The start address of the register, The starting value is 0. For example, 0 represents 4001 and 1 represents 4002
Register count (Hex)	String [1..FFFF];	The length of register
Values (Hex)	String, 128 bits length;	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,

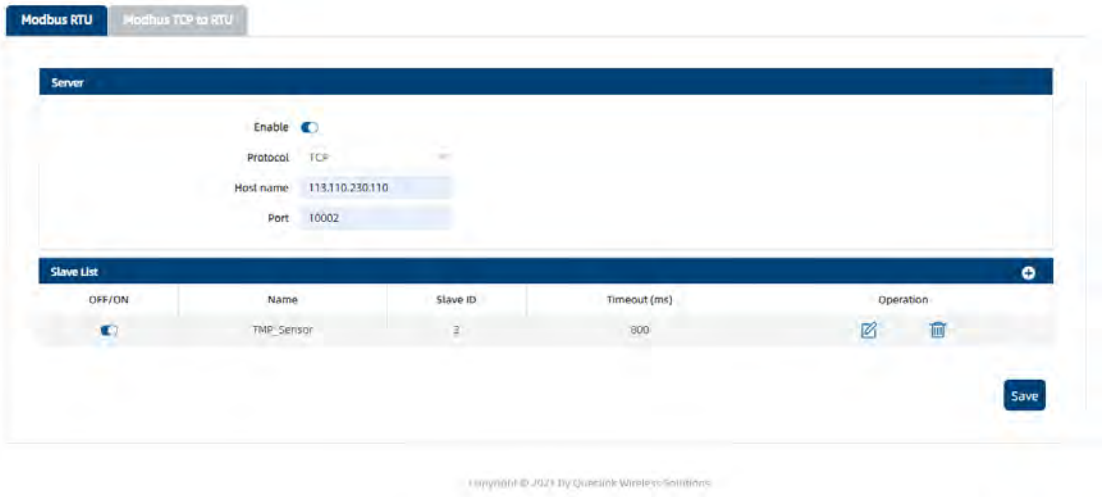
{"service":"1", "id":1, "slave":1, "function":3, "first_register":"0001", "length":3}

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.
id	Integer	ID of the message, to identify the message
slave	Integer	Modbus slave ID
function	Integer	Function code
values_len	Integer	The length of return value
values	String	Return data, the length of the string = data_len*2.
crc	String	Modbus CRC checking,

The following is an example,
{"time":"2022-05-08 17:39:05", "IMEI":"863553065142923", "id":1, "slave":1, "function":3, "values_len":6, "values":"040200080008", "crc":"D935"}

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



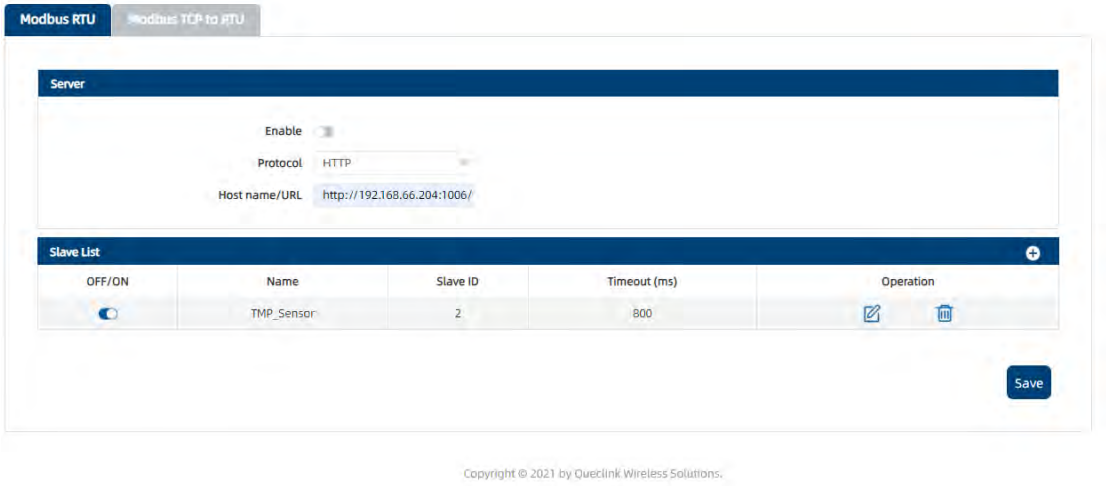
The format from the TCP server to the device follows the MQTT format,but a starting symbol "@" and an ending symbol "$" need to be added in the message.

The following is an example,
@{"service":"1", "id":1, "slave":1, "function":3, "first_register":"0001", "length":3}$

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

The following is an example,
@{"time":"2022-05-08 17:39:05", "IMEI":"863553065142923", "id":1, "slave":1, "function":3, "values_len":6, "values":"040200080008", "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.

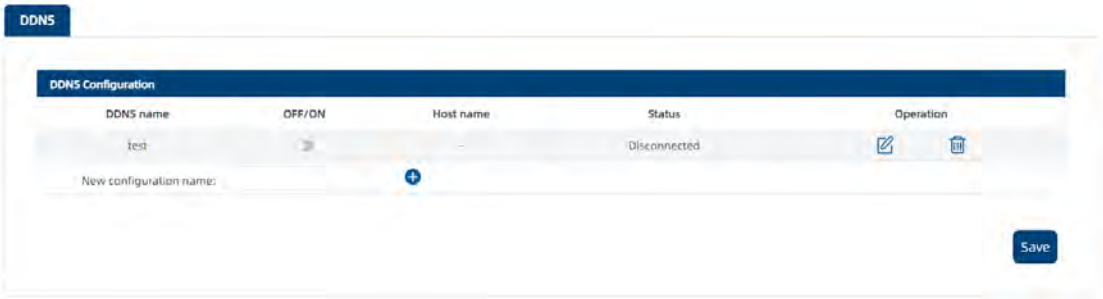
4.3.6.2 Modbus TCP to RTU

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.

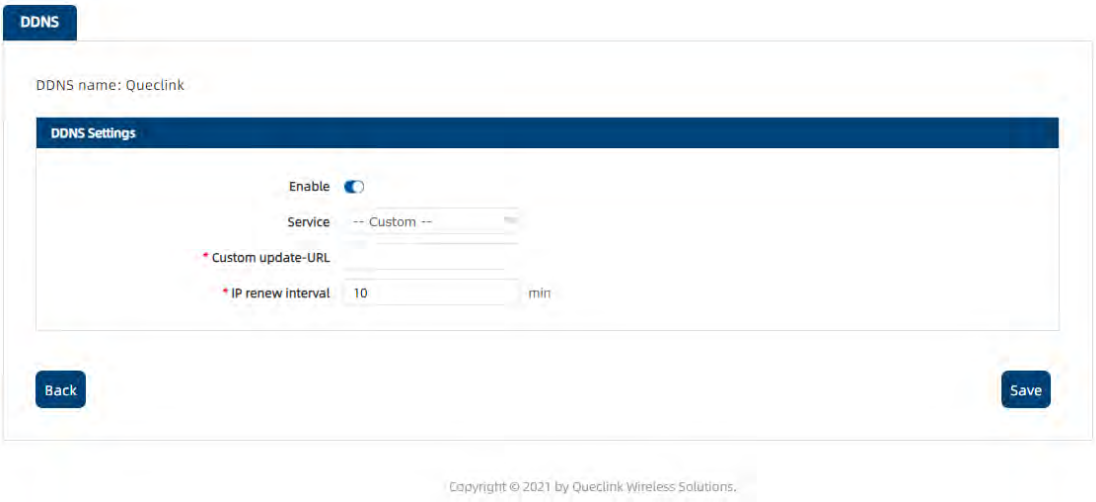
4.3.7 DDNS

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:



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 it's IP address has changed

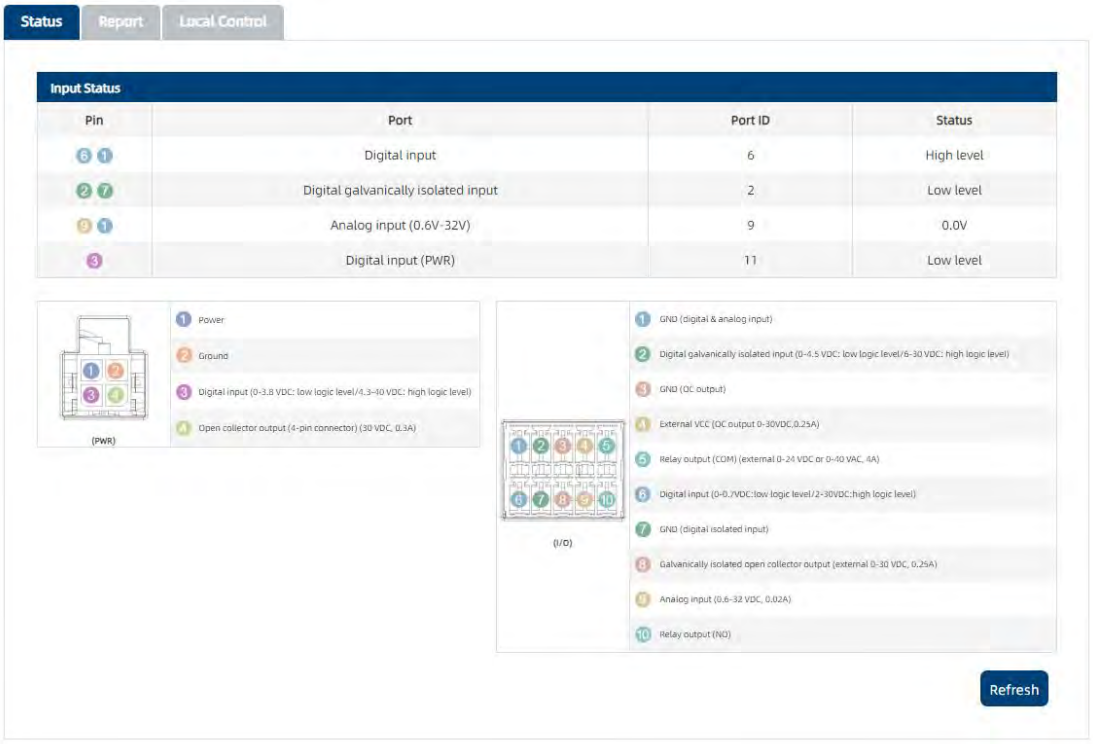
4.3.8 Input

All devices can support more than one digital or analog input, for example, WR201 has 4 inputs.

This section is to provide the control on the input ports.

4.3.8.1 Status

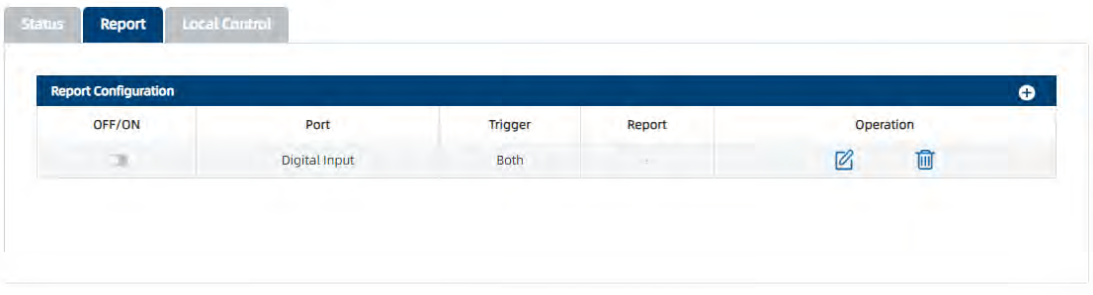
The Status page displays the current states of the device's input ports:



Copyright © 2021 by Queclink Wireless Solutions.

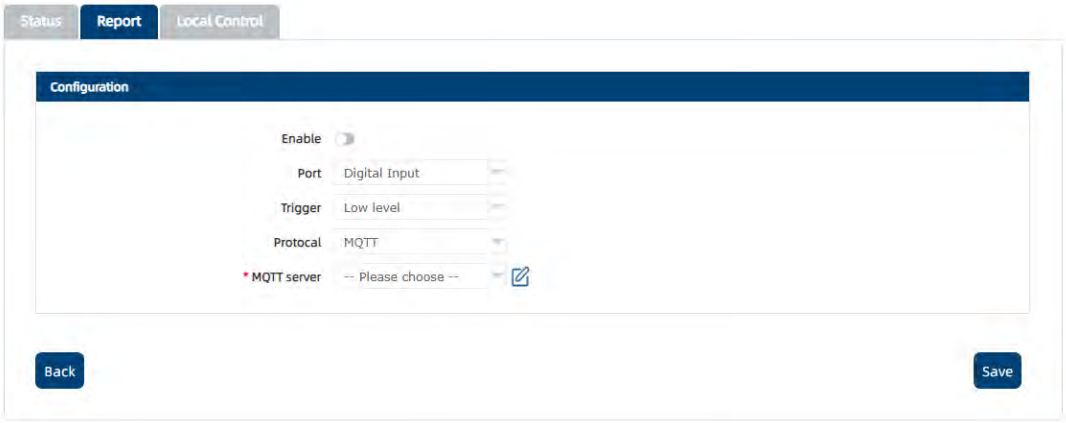
4.3.8.2 Report

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



Copyright © 2021 by Queclink Wireless Solutions.

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



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.
Protocal	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 report generated by a device to a MQTT server (in JSON format):

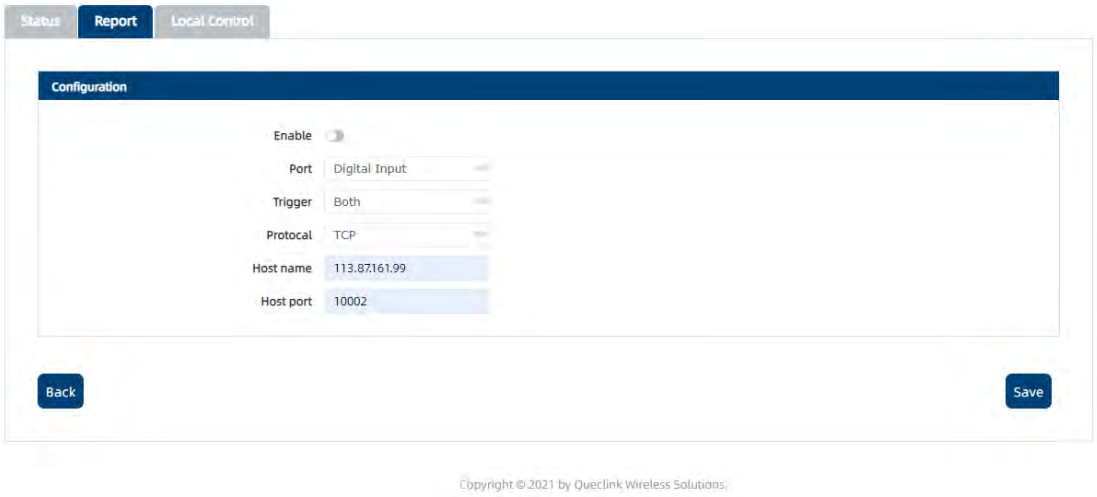
{"time":"2022-05-08 17:39:05", "IMEI":"863553065142923", "rtn":"success", "port": "6", "value": "0"} **Field Name**	**Value**	**Description**
time	String	The generation time of the report.

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 command for querying IO status (in JSON format):
{"service":"0", "port": "6,8,5,12"}

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.

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": "0"} $

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

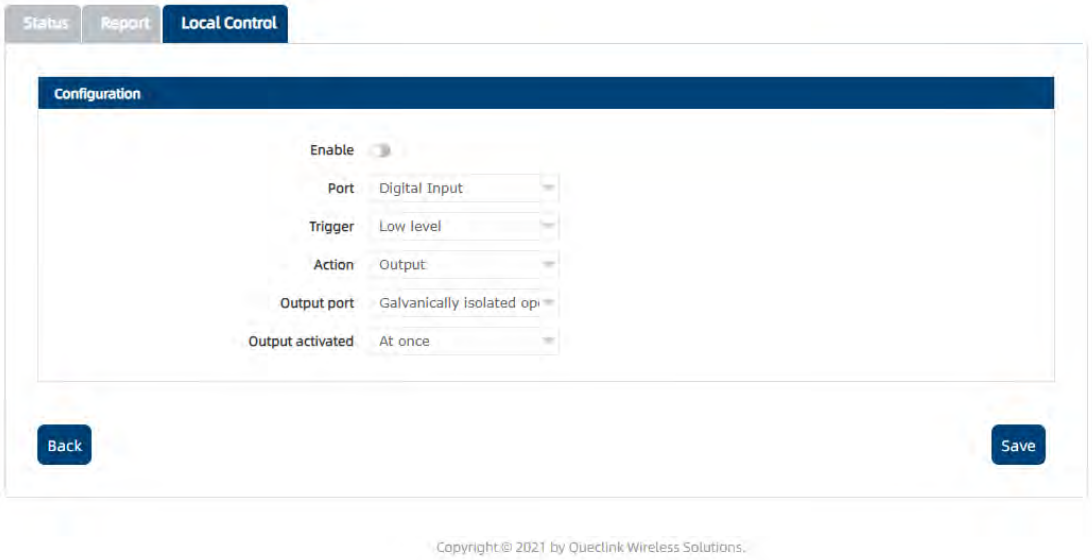
The following is an example,
@{"service":"0", "port": "6,8,5,12"}$

The mapping table of port index, input port and value:

Port	IO	Value
6	Digital input	0: Low level; 1: High level
2	Digital galvanically isolated input	0: High level; 1: Low level
9	Analog input	ADC value
11	Digital input (PWR)	0: High Level; 1: Low Level

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.



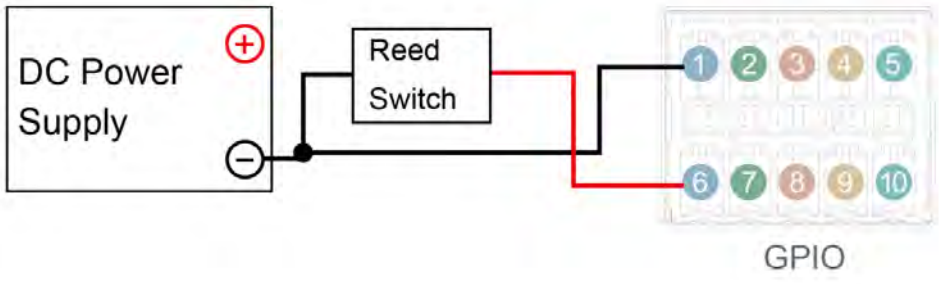
Field Name	Value	Description
Enable	yes|no; default: yes	Turns the LocalControl rule on or off.
Port	Digital Input|Digital isolated|Analog|Digital Input(PWR); default: Digital Input	Select which input pin the rule will apply.
Trigger	Both |Low level |High level; default: both Inside range |Outside range |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	Used to select the output port you want to control.

	output|Relay|Open collector output; Default:Galvanically isolated open collector output	
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

- WR201 digital input can be used for security applications. You can connect PIR sensor or reed switch to digital input. Then configure WR201 input.

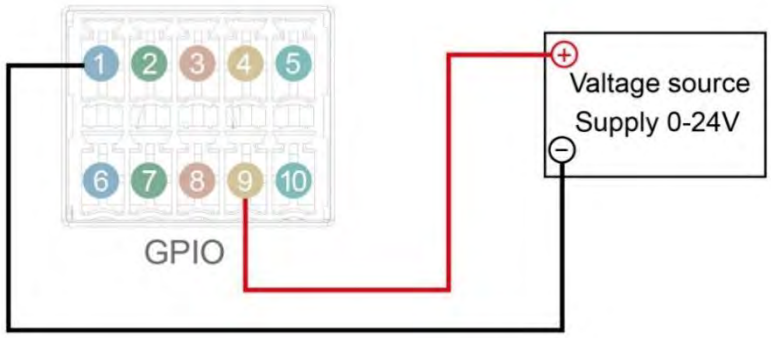
This is an example of how to connect digital input:



- Example of using WR201 digital isolated input:

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

- If you want to measure the voltage with WR201 you need to connect the voltage source as the picture below. Note that voltage on pin 9 must never exceed 24V.

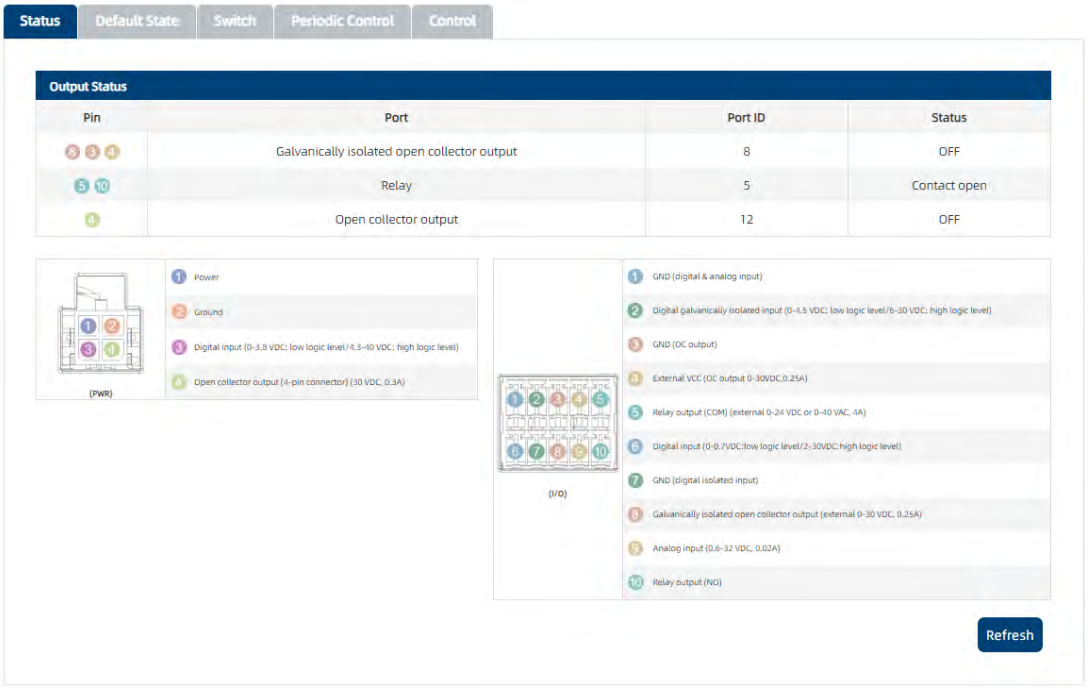


4.3.9 Output

All devices can support more than one digital or analog output, for example, WR201 has 3 outputs. This section is to provide the control on the output ports.

4.3.9.1 Status

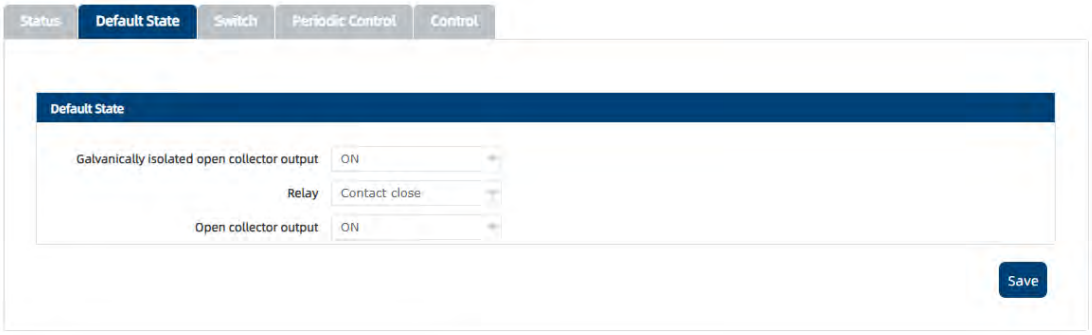
The Status page displays the current states of the device's output ports:



Copyright © 2021 by Queclink Wireless Solutions

4.3.9.2 Default State

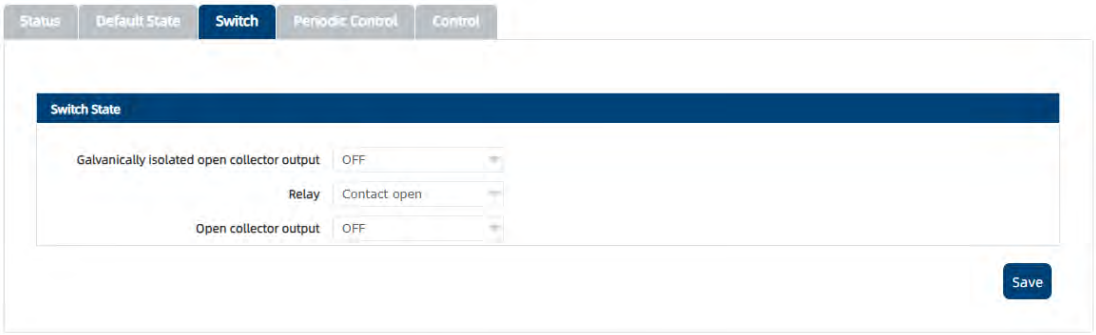
The page is to set the default state of the output ports when the device powers on. You can select specified state by the drop down menu.



Copyright © 2021 by Queclink Wireless Solutions.

4.3.9.3 Switch

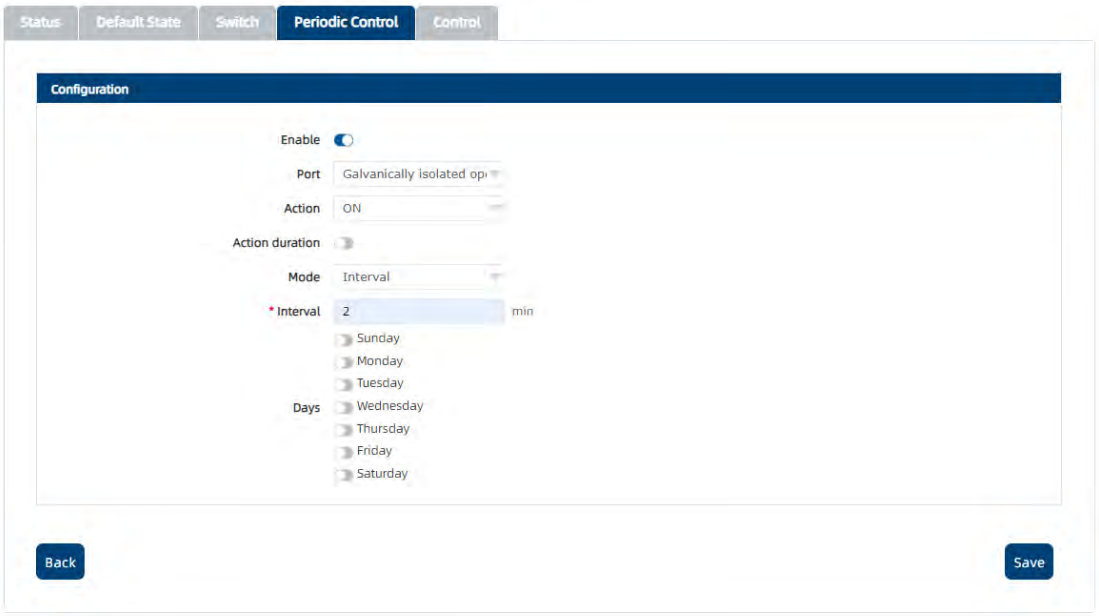
The Switch page is used to turn the device's outputs on or off manually. This action does not save the state permanently, meaning that after a reboot the states will revert back to their default values.



Copyright © 2021 by Queclink Wireless Solutions.

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.



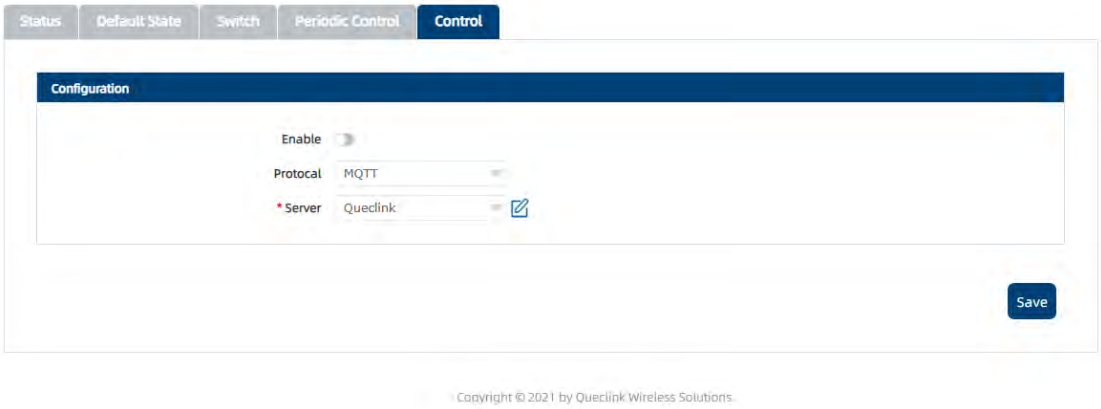
Copyright © 2021 by Queclink Wireless Solutions.

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 set to enable, 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	The day or multiple days on which the device

	which the CPE will perform the action	will perform the action.

4.3.9.5 Control

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



The MQTT server sends control and query command with JSON format message.

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 an example of control message:
{"service": "0", "port": "8,5,12", "value": "0,0,1"}

The following is an example of query message:
{"service": "0", "port": "8,5,12"}

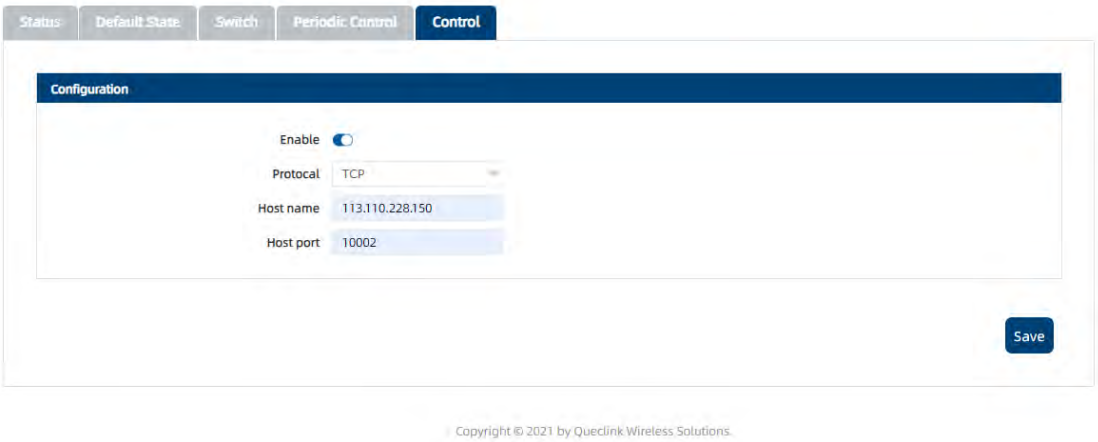
Return message format is:

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": "0,0,1"}

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



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

The following is an example of control messages:
@{"service": "0", "port": "8,5,12", "value": "0,0,1"}$

The following is an example of query messages:
@{"service": "0", "port": "8,5,12"}$

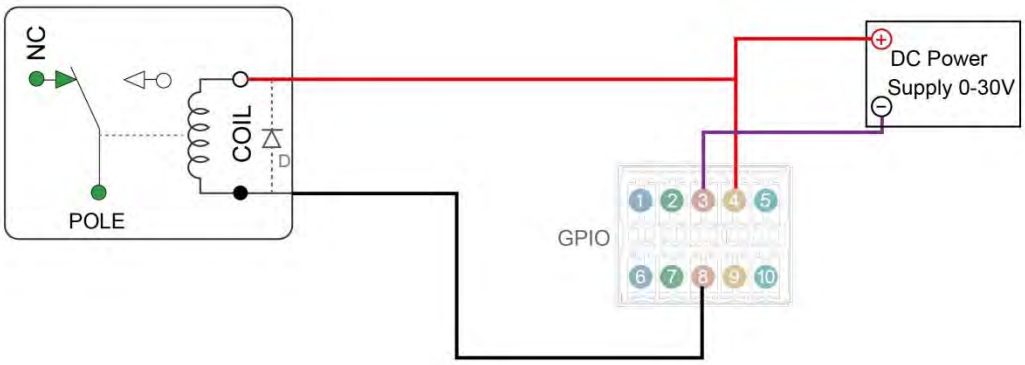
The following is an example of return messages:
@{"time":"2022-05-08 17:39:05", "IMEI":"863553065142923", "rtn":"success", "port": "8,5,12", "value": "0,0,1"}$

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

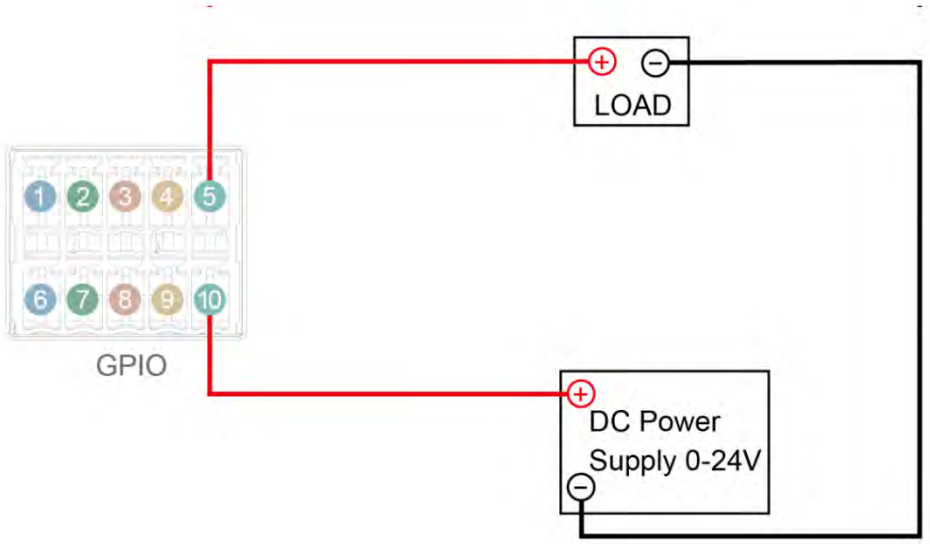
Index	IO	Status
8	Galvanically isolated open collector output	0: OFF; 1: ON
5	Relay output	0：Contact open；1：Contact close
12	Open collector output (PWR)	0： OFF； 1： ON

4.3.9.5 Application Example

- This is example on how to connect a relay to WR201 Galvanically isolated open collector output:



- In some cases, you may want WR201 release to automatically press the key to turn on the high-power load, which can be connected according to the following figure:

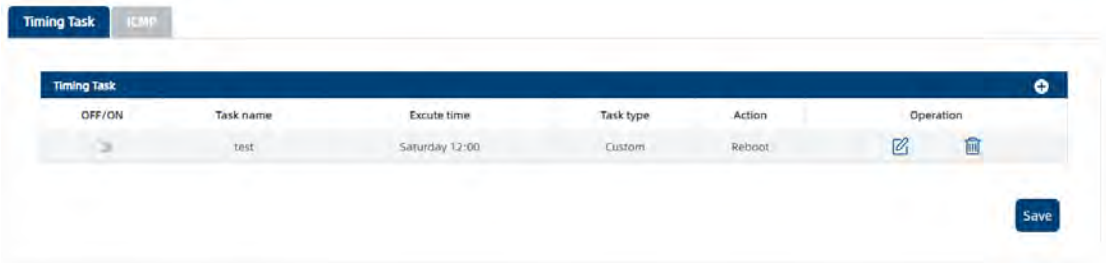


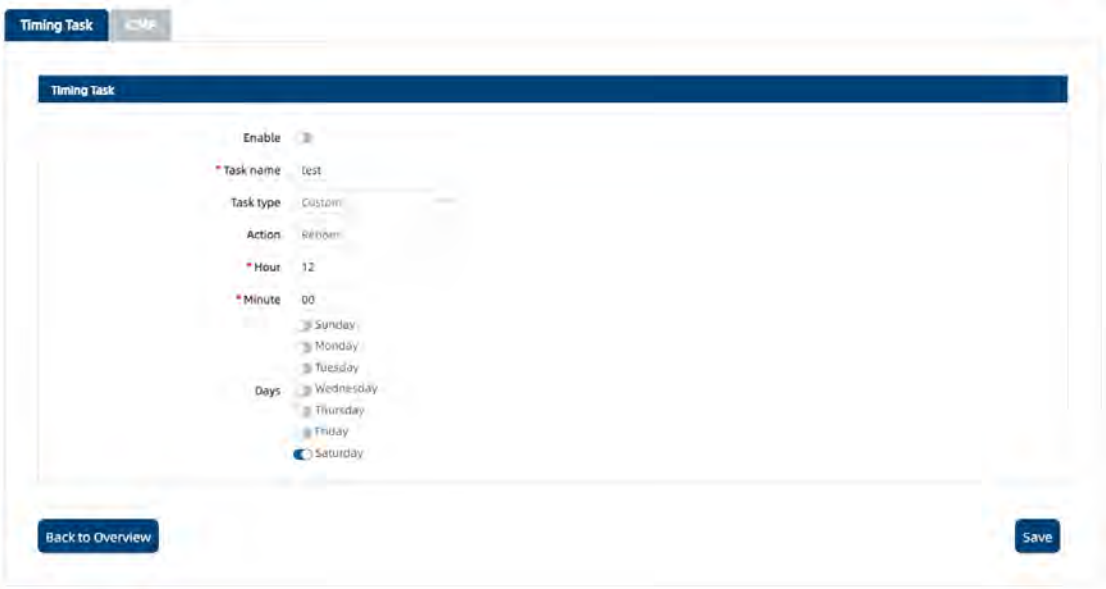
4.3.10 Auto Recovery

Auto Recovery pages provides you several applications as a precautionary measure to ensures the device will recover from unexpected issues, such as mobile connection is down.

4.3.10.1 Timing Task

Timing Task is a function that executes a specified action at a specified time interval. It can be used as prophylactic measure to recover the device back to normal condition, for example, to reboot the device one time at the mid night of each day.

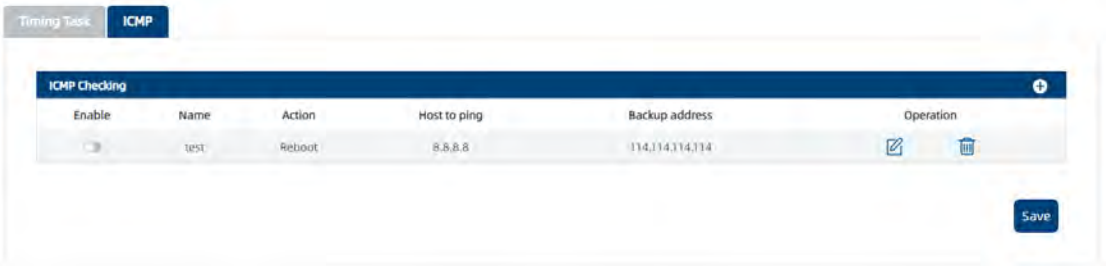




Field Name	Value	Description
Enable	yes|no; Default: no	Turns the rule ON or OFF
Task Name	string	Name of ICMP rule
Action	Reboot|Restart modem|Restart mobile connection; Default: Reboot	The action that will be taken when timer reached
Hour	integer [0..23]; Default: 23	The hour of the day on which the device will perform the action
Minute	integer [0..59]; Default: 0	The minute of the hour on which the device will perform the action
Days	Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday; Default: none	The day or multiple days on which the device will perform the action

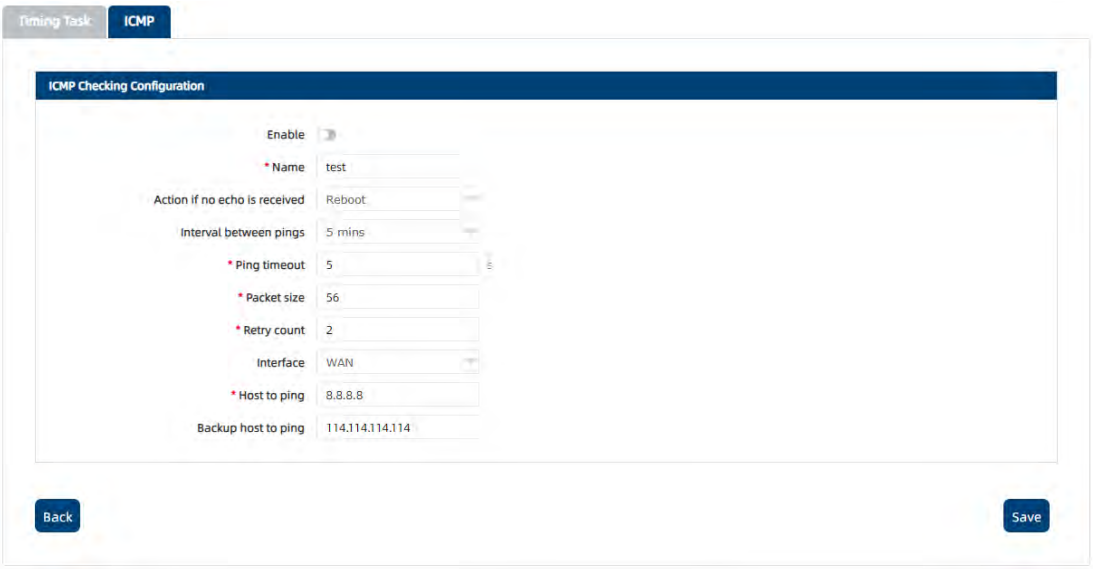
4.3.10.2 ICMP

The ICMP is a function periodically sending Ping commands to a specified IP address and wait for received responses. If no response is received, the device will execute specified actions if sending a defined number of times at a defined frequency.



The figure below is an example of that rule and the table below provides information on the

fields that make up that rule:



Copyright © 2021 by Queclink Wireless Solutions.

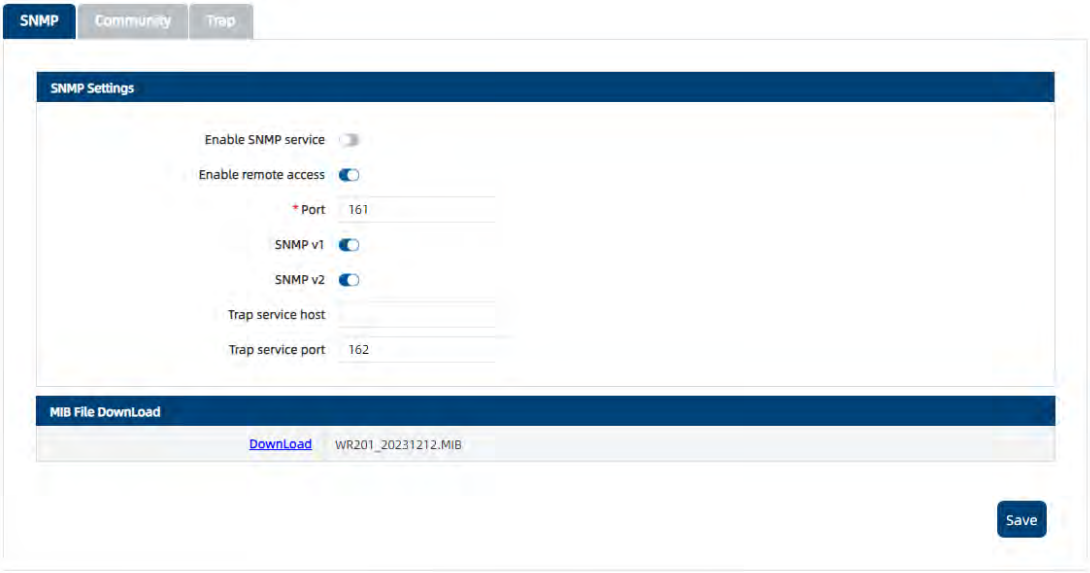
Field Name	Value	Description
Enable	yes|no; Default: **no**	Turns the rule ON or OFF
Name	string	Name of ICMP rule
Action if no echo is received	Reboot|Restart modem|Restart mobile connection|; Default: Reboot	The action that will be taken if no ICMP echo is received
Interval between pings	1 mins|2 mins|3 mins|4 mins|5 mins|15 mins|30 mins|1 hour|2 hours; Default: 5 mins	Interval at which ping requests are sent to the specified host
Ping timeout	integer [1..9999]; Default: 5	Maximum response time (in seconds). If no echo is received after the amount of time specified in this field, the ping request is considered to have failed
Retry count	integer [1..9999]; Default: 2	Indicates how many additional times the device will try sending ping requests if the initial one fails
Interface	WAN|Mobile; Default: WAN	Specifies through which interface the pings will be sent.
Host to ping	host|ip; Default: 8.8.8.8	Indicates the host to which ping requests will be sent
Backup host to ping	host|ip; Default: 114.114.114.114	Indicates the backup host to which ping requests will be sent

4.3.11 SNMP

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

4.3.11.1 SNMP

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

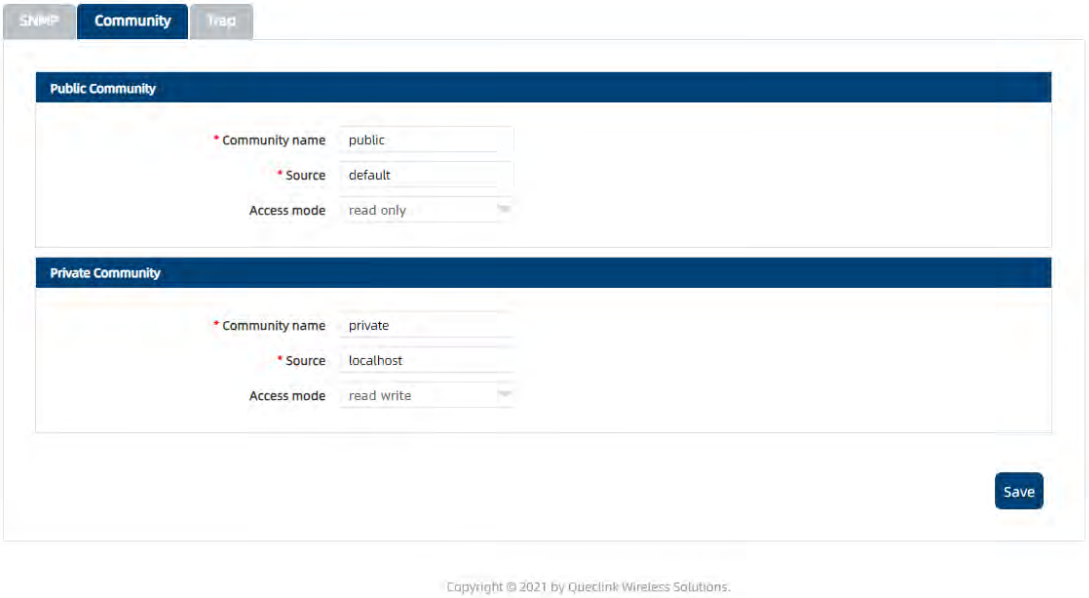


Copyright © 2021 by Queclink Wireless Solutions.

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.Hostname or IP address to transfer SNMP traffic to.Hostname or IP address to transfer SNMP traffic to.
Trap service port	integer [0..65535]; default: 162	Trap host's port number.

4.3.11.2 COMMUNITY

The Community page is used to manage SNMP access rights.



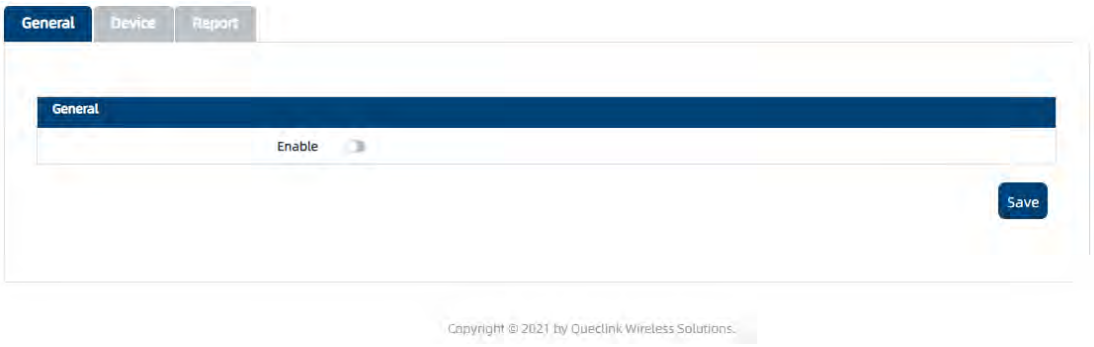
Field Name	Value	Description
Community name	string; default: public	Name of the community.
source	ip; default:default	IP address of the community.
Access Mode	read-only |read-write; default: read-only	Access mode for current community.
Community name	string; default: private	Name of the community.
source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

4.3.12 Tracker

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

4.3.12.1 General

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



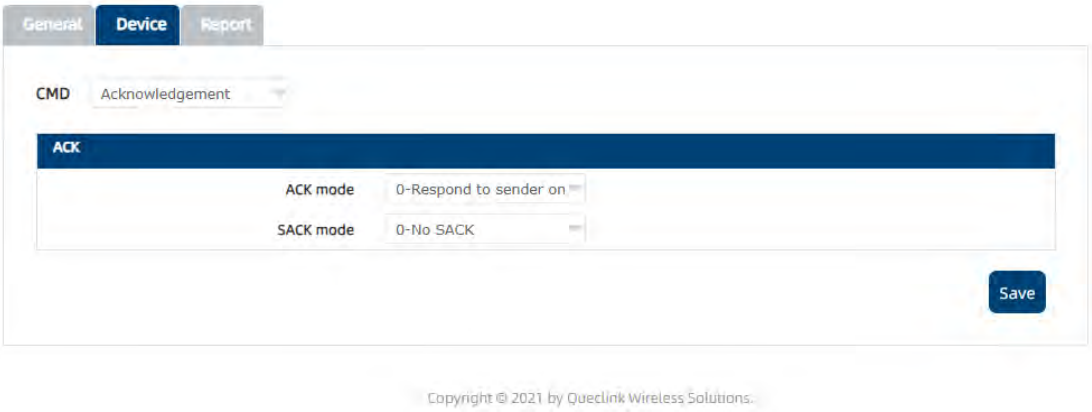
4.3.12.2 Device

The Device page is used to configure Backend Server /Acknowledgement and Hearbeat 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.

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 feature.



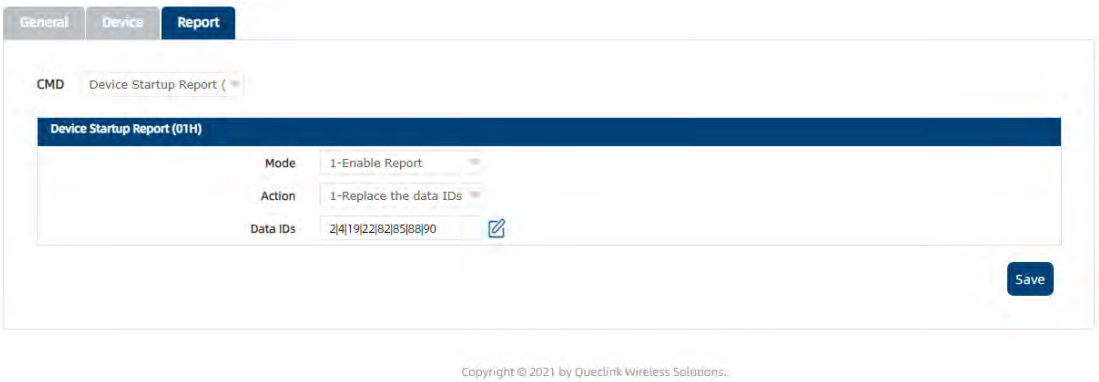
Field Name	Value	Description
ACK mode	0-Respond to sender only|1-Respond to sender and backend server; default:0-Respond to sender only	0 - Respond to sender only. The terminal receives the command from which physical path (for example, Cellular Network, SMS, RS232.), and replies the ACK (or NACK) only 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.
Heartbead 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 (periodic). 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 from the terminal, and the terminal will diagnose its connection status with the backend server according to the SHBD frame.

4.3.12.3 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).



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	

4.3.13 Hotspot

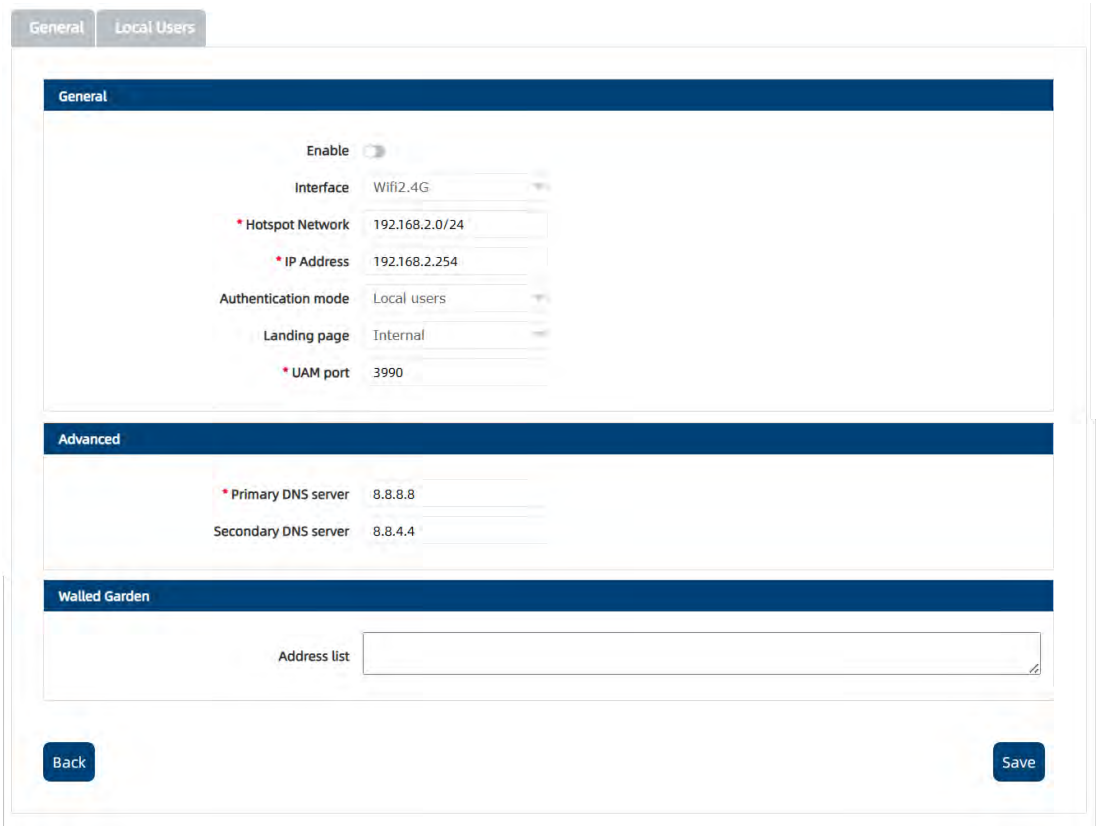
A hotspot is a physical location where people can access the Internet, using Wi-Fi, via a wireless local area network (WLAN) with a device connected to an Internet service provider.

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

4.3.14.1 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.

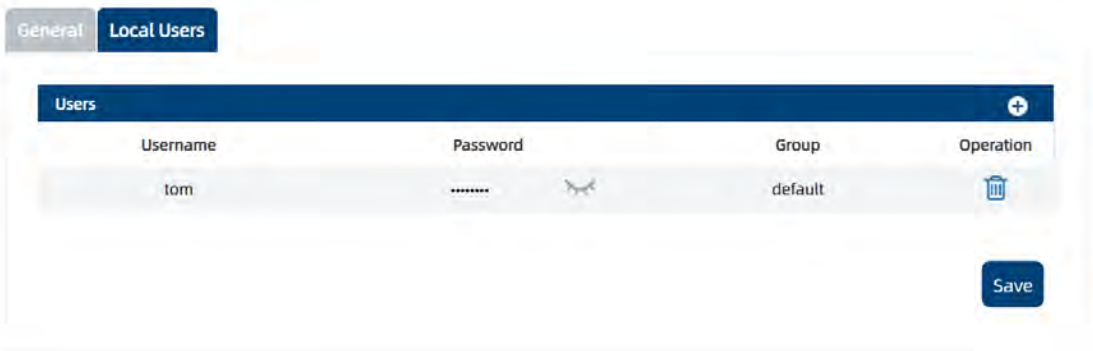


Field Name	Value	Description
Enable	off | on; default: on	Turns the Hotspot instance on or off.
Interface	Wifi2.4G|Wifi5G	Interface to provide hotspot service.
Hotspot Network	ip/netmask; default: 192.168.2.0/24	IP address and subnet of the Hotspot network.
IP Address	ip; default: 192.168.2.254	Defines 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, new section, to enter website address, will appear, e.g., http://www.example.com
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.

4.3.14.2 Local Users

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

Clicking Add icon to create a new user instance, and entering a Username, Password. Clicking Save button to apply the change.



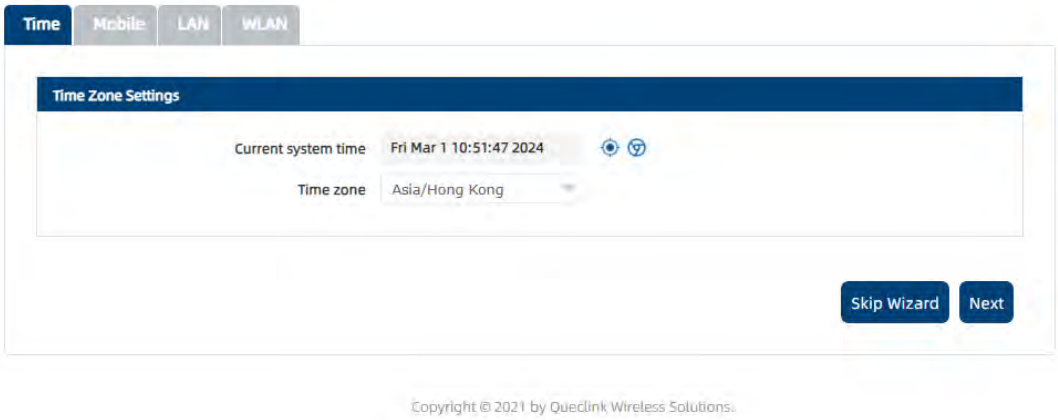
4.4 System

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

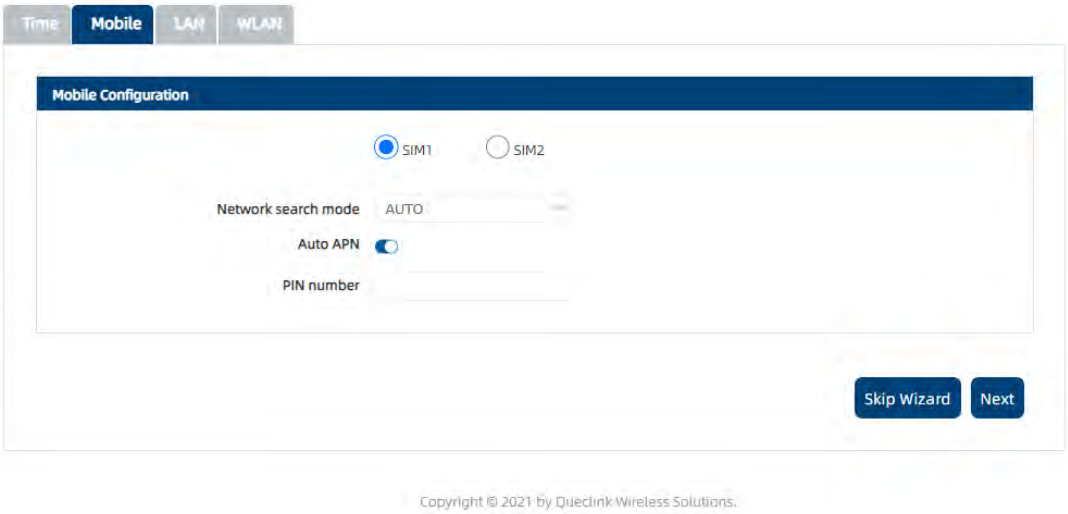
4.4.1 Setup Wizard

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 setup the device.

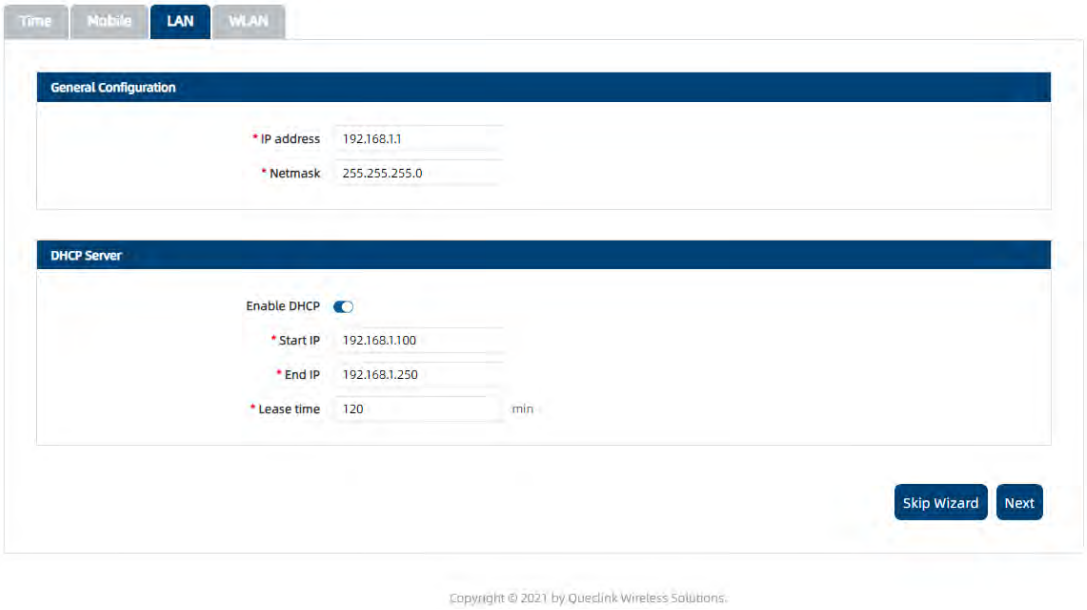
Step1 is used to configure the device's time settings. Time is very important for many applications, such as RMS, scheduled task.



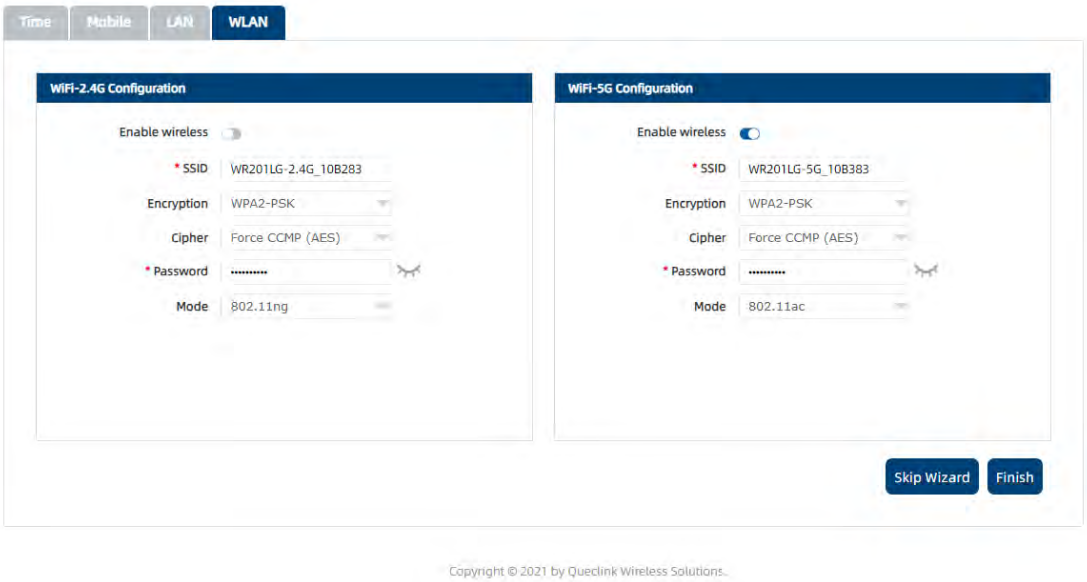
Step2 is used to configure the device's SIM card parameters.



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).

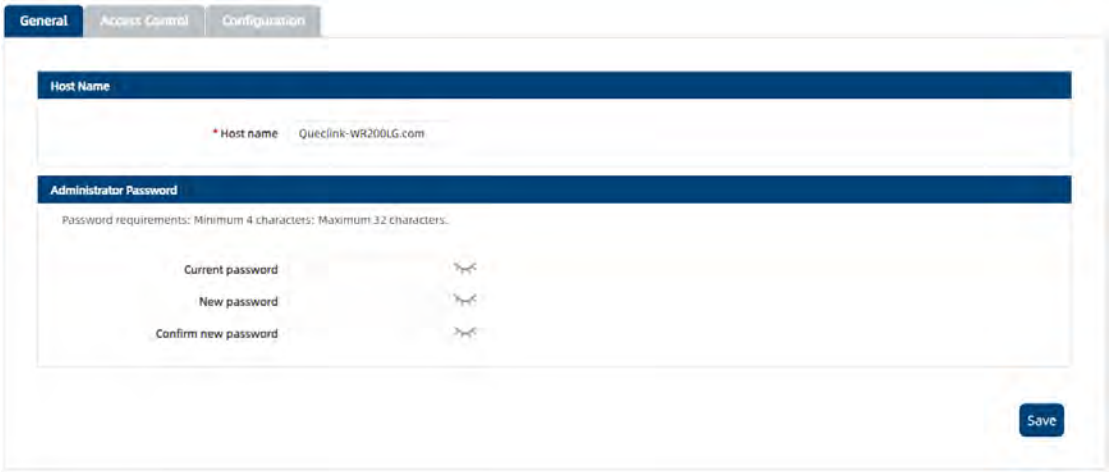


You can also skip any of above steps and configure the setting later in the according section.

4.4.2 Administration

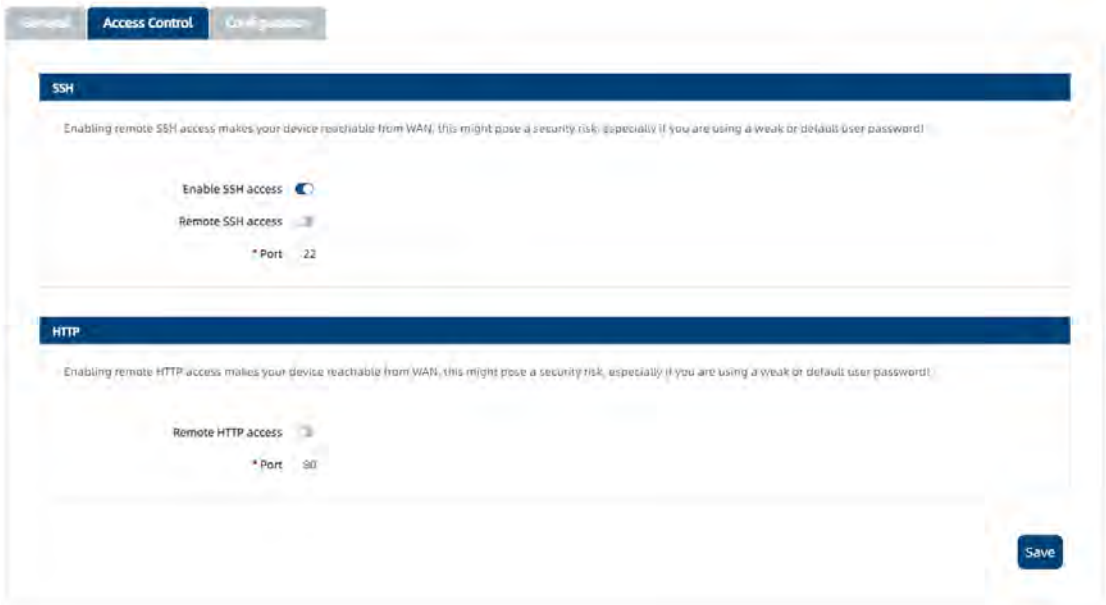
4.4.2.1 General

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

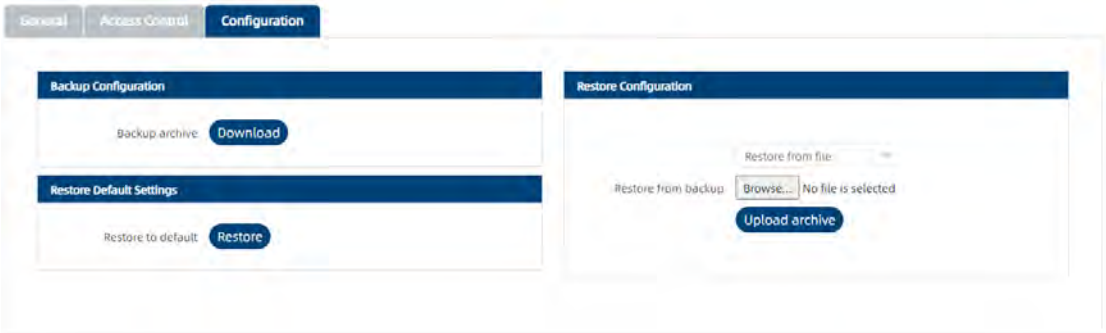


Field Name	Value	Description
Enable SSH access	yes|no; default: yes	Turns SSH access from the local network (LAN) on or off.
Remote SSH access	yes|no; default: no	Turns SSH access from remote networks (WAN) on or off.
Port	integer [0..65535]; default: 22	Selects which port to use for SSH access.

4.4.2.3 Configuration

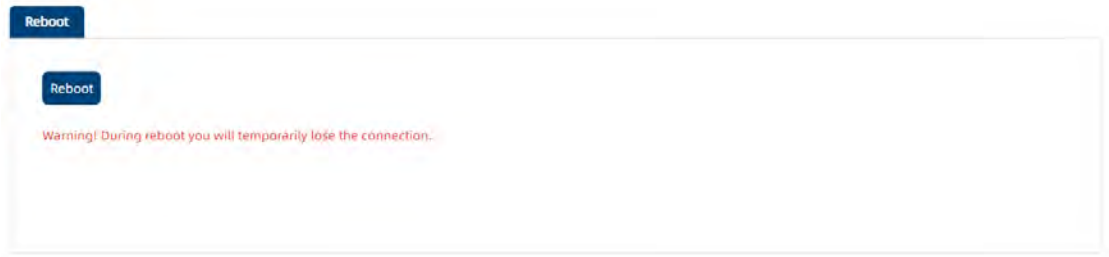
The Configuration page is used to generate the user's defaults configuration and download or upload backup files to the device.

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.

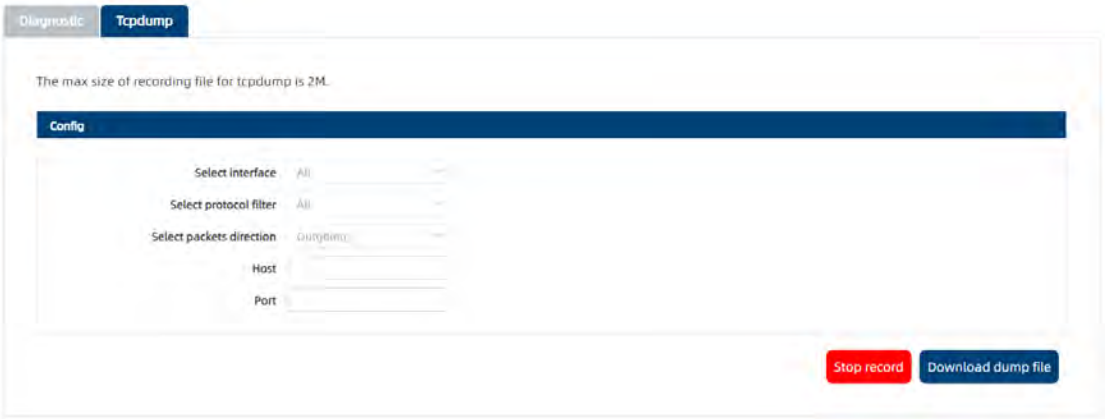
4.4.4.1 Ping&Trace

The user inputs an IP address or domain name, then click Traceroute or Ping button to check the link 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.

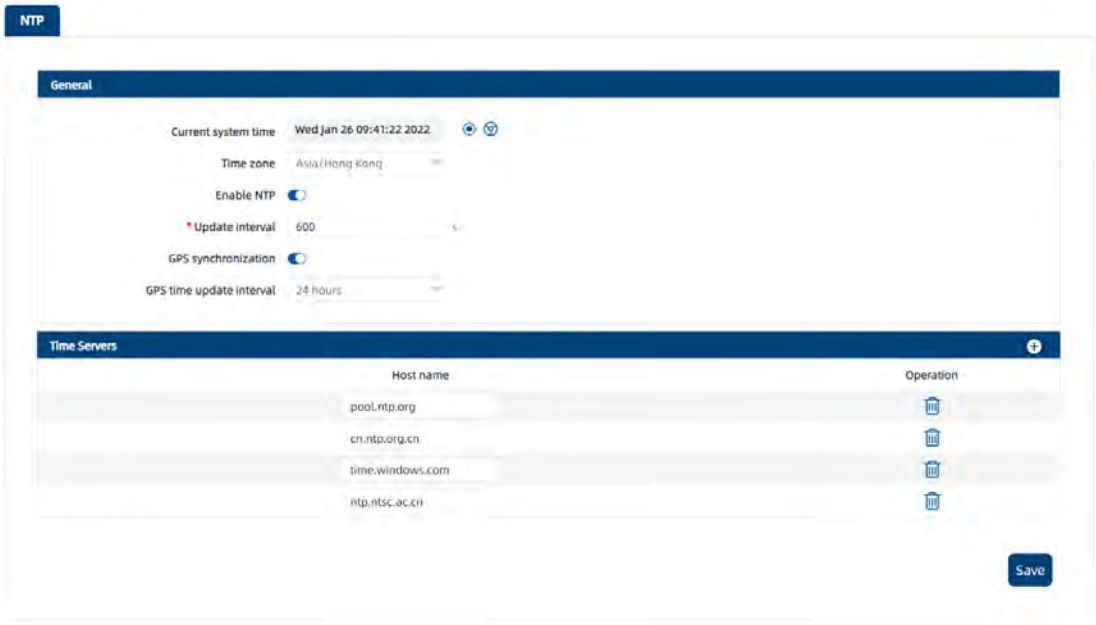
4.4.5 NTP

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.

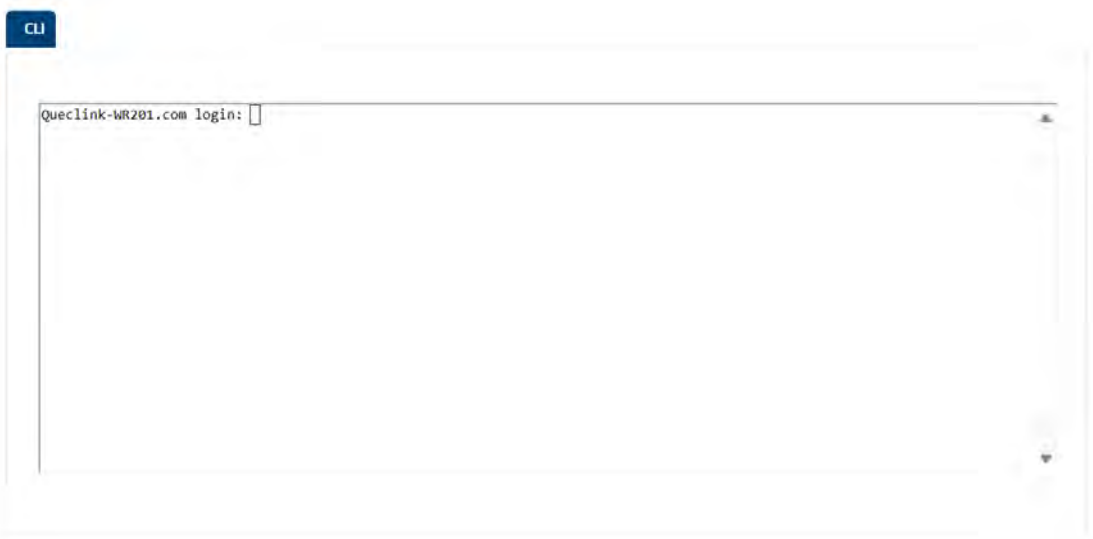
WR201 uses GPS for time synchronization by default. When GPS is not available and NTP server synchronization function is enable, WR201 will synchronize the time through NTP server.



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 CLI

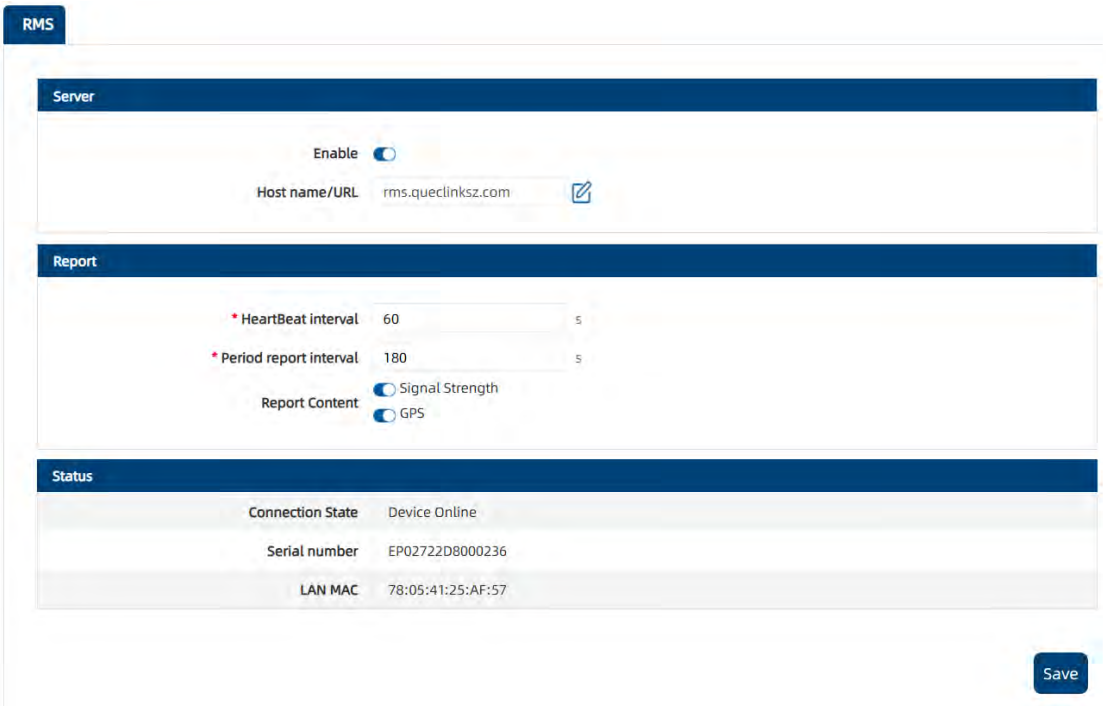
command-line interface (CLI) is a command line program that accepts text input to execute operating system functions. You can login the CLI with root account and password to execute any commands supported by Linux or Queclink's applications.



4.4.7 RMS

RMS (Remote Management System) is a cloud system designed by Queclink and used for remote monitoring and management of Queclink CPE products.

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



Field Name	Value	Description

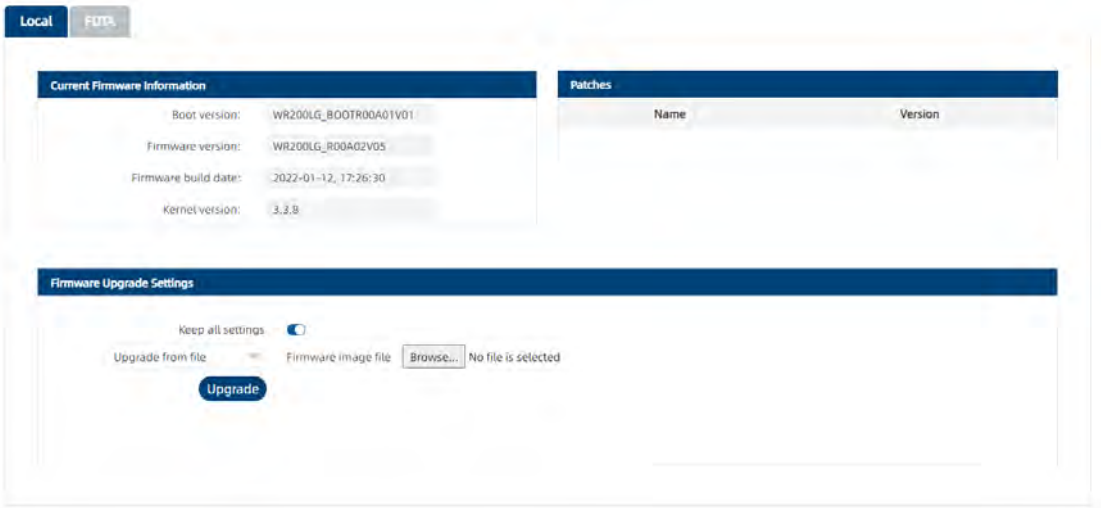
Enable	yes|no; default: yes	Turns RMS service on or off.
Host name/URL	Host | ip; default:rms.quecklinksz.com	Address of the RMS server. If you're using Queclink RMS, just leave the default address.
HeartBeat Interval	integer; default: 60	The interval of heartbeat between device and RMS server. It’s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

4.4.8 Upgrade

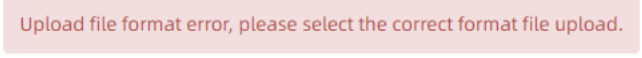
This section is to check the current firmware version of the device and to upgrade the device’s firmware. Firmware can be upgraded either from server or from an image file uploaded from your computer.

4.4.8.1 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 route, 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.



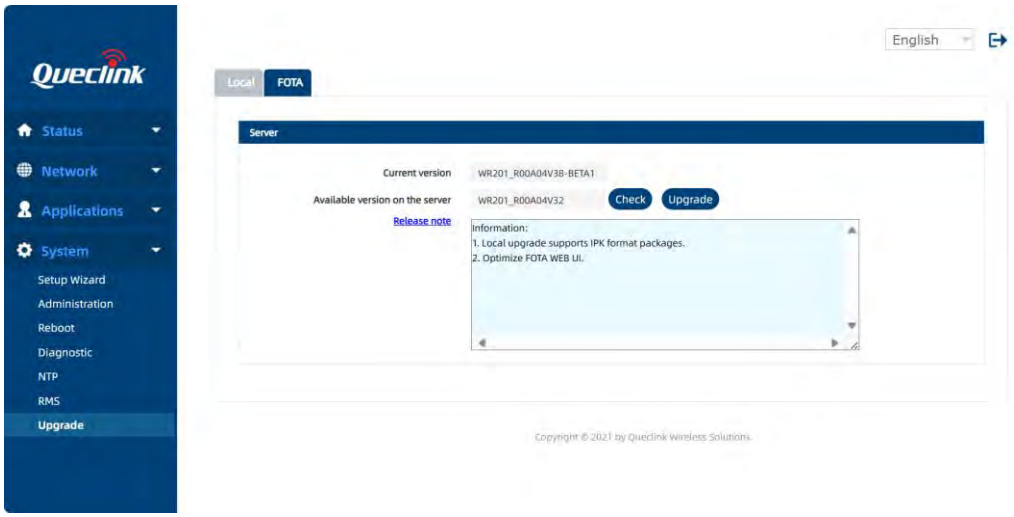
If the uploaded firmware file that is incompatible with your device, you will see a warning as below:



4.4.8.2 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 CPEs 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.

5. FAQ

5.1 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

5.2 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

5.3 Cannot Find SIM/UIM Card

Phenomenon:

Cannot find SIM card

Possible Reason:

- SIM card damage
- SIM bad contact

Solution:

- Replace SIM card
- Re-install SIM card

5.4 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

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
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

Appendix

This device complies with part 15 of the FCC Rules.
Operation is subject to the following two conditions: (1) This device may not cause harmful interf erence, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliancecould void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digit al device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide re asonable protection against harmful interference in a residential installation. This equipme nt generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communica tions. However, there is no guarantee that interference will not occur in a particular inst allation.
If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment into an outlet on a circuit different from that to which the re ceiver is connected.
-- Consult the dealer or an experienced radio/TV technician for help.

Contains FCC ID: "XMR202008EC25AFXD"

Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 2 0 cm between the radiator & your body.