robustel | User Guide

M1200

Smart Industrial IoT Gateway

2 SIM + 2 DI + 1 DO + 1 RS-232 + 1 RS-485 + 1 Mini USB

robustOS

Guangzhou Robustel LTD
www.robustel.com

About This Document

This document provides hardware and software information of the Robustel M1200, including introduction, installation, configuration and operation.

Trademarks and Permissions

 are trademarks of Guangzhou Robustel LTD. All other trademarks and trade names mentioned in this document are the property of their respective owners.

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. It is the customer's responsibility to review the advice provided in this document and its suitability for the system. Robustel makes no representations about the specific knowledge of the customer's system or the specific performance of the system. The contents of this document are subject to change without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the use of this document.

Technical Support

Tel: +86-20-29019902
Fax: +86-20-82321505
Email: support@robustel.com
Web: www.robustel.com

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the gateway is used in a normal manner with a well-constructed network, the gateway should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Robustel accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the gateway, or for failure of the gateway to transmit or receive such data.

Safety Precautions

General

- The gateway generates radio frequency (RF) power. When using the gateway, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your gateway in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Be sure that the gateway will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the gateway should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the gateway for proper operation. Only uses approved antenna with the gateway. Please contact authorized distributor on finding an approved antenna.
- Always keep the antenna with minimum safety distance of 20 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.
- RF exposure statements
    1. For mobile devices without co-location (the transmitting antenna is installed or located more than 20cm away from the body of user and nearby person)
- FCC RF Radiation Exposure Statement
    1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
    2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and human body.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Gateway may be used at this time.

Using the gateway in Vehicle

- Check for any regulation or law authorizing the use of cellular devices in vehicle in your country before installing the gateway.
- The driver or operator of any vehicle should not operate the gateway while driving.
- Install the gateway by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the gateway.
- The gateway should be connected to the vehicle's supply system by using a fuse-protected terminal in the vehicle's fuse box.
- Be careful when the gateway is powered by the vehicle's main battery. The battery may be drained after extended period.

Protecting Your Gateway

To ensure error-free usage, please install and operate your gateway with care. Do remember the following:

- Do not expose the gateway to extreme conditions such as high humidity / rain, high temperature, direct sunlight, caustic / harsh chemicals, dust, or water.
- Do not try to disassemble or modify the gateway. There is no user serviceable part inside and the warranty would be void.
- Do not drop, hit or shake the gateway. Do not use the gateway under extreme vibrating conditions.
- Do not pull the antenna or power supply cable. Attach/detach by holding the connector.
- Connect the gateway only according to the instruction manual. Failure to do it will void the warranty.
- In case of problem, please contact authorized distributor.

Regulatory and Type Approval Information

Table 1: Directives

2011/65/EU	The European RoHS2.0 2011/65/EU Directive was issued by the European parliament and the European Council on 1 July 2011 on the restriction of the use of certain Hazardous substances in electrical and electronic equipment.
2012/19/EU	The European WEEE 2012/19/EU Directive was issued by the European parliament and the European Council on 24 July 2012 on waste electrical and electronic equipment.
2013/56/EU	The European 2013/56/EU Directive is a battery Directive which published in the EU official gazette on 10 December 2013. The button battery used in this product conforms to the standard of 2013/56/EU directive.

Table 2: Standards of the electronic industry of the People's Republic of China

SJ/T 11363-2006	The electronic industry standard of the People's Republic of China SJ/T 11363-2006 "Requirements for Concentration Limits for Certain Toxic and Hazardous Substances in Electronic Information Products" issued by the ministry of information industry of the People's Republic of China on November 6, 2006, stipulates the maximum allowable concentration of toxic and hazardous substances in electronic information products. Please see **Table 3** for an overview of toxic or hazardous substances or elements that might be contained in product parts in concentrations above the limits defined by SJ/T 11363-2006.
SJ/T 11364-2014	The electronic industry standard of the People's Republic of China SJ/T 11364-2014 "Labeling Requirements for Restricted Use of Hazardous Substances in Electronic and Electrical Products" issued by the ministry of Industry and information technology of the People's Republic of China on July 9, 2014, stipulates the Labeling requirements of hazardous substances in electronic and electrical products, environmental protection use time limit and whether it can be recycled. This standard is applicable to electronic and electrical products sold within the territory of the People's Republic of China, and can also be used for reference in the logistics process of electronic and electrical products. The orange logo below is used for Robustel products: Indicates its warning attribute, that is, some hazardous substances are contained in the product. The "10" in the middle of the legend refers to the environment-friendly Use Period (EFUP) * of electronic information product, which is 10 years. It can be used safely during the environment-friendly Use Period. After the environmental protection period of use, it should enter the recycling system. *The term of environmental protection use of electronic information products refers to the term during which the toxic and hazardous substances or elements contained in electronic information products will not be leaked or mutated and cause serious pollution to the environment or serious damage to people and property under normal conditions of use.

Table 3: Toxic or Hazardous Substances or Elements with Defined Concentration Limits

Name of the Part	Hazardous Substances									
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal parts	o	o	o	o	-	-	-	-	-	-
Circuit modules	o	o	o	o	o	o	o	o	o	o
Cables and cable assemblies	o	o	o	o	o	o	o	o	o	o
Plastic and polymeric parts	o	o	o	o	o	o	o	o	o	o

o:
Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in RoHS2.0.
X:
Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in RoHS2.0.
-:
Indicates that it does not contain the toxic or hazardous substance.

Document History

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

Date	Firmware Version	Document Version	Change Description
12 Mar., 2018	1.0.0	v.1.0.0	Initial release
4 Apr., 2018	1.0.0	v.1.0.1	Updated product name
9 Apr., 2018	1.0.0	v.1.0.2	Updated EMI information
16 Apr., 2018	1.0.0	v.1.0.3	Added certification and VPN information
23 Apr., 2018	1.0.0	v.1.0.4	• Updated Key Features • Updated USB information • Updated PC configuration
29 Jun., 2018	1.0.0	v.1.0.5	Revised the company name
20 Sept., 2018	1.0.1	v.1.0.6	• Rectified the contents of Configure PC • Added AT Over COM • Added Work Mode • Added Chapter 4
12 Dec., 2018	1.0.3	v.1.0.7	Added the description of the BG96 module
30 Jan., 2019	1.0.3	v.1.0.8	Revised the approvals
27 Mar., 2019	1.0.3	v.1.0.9	• Revised the Regulatory and Type Approval Information • Revised the Disclaimer • Revised the description of PIN in Chapter 2.1 • Added the description of DIOD, RS232 and RS485 in Chapter 2.1 • Revised the Configure the PC in Chapter 3.1 • Revised the Dial Configuration of PC under Modem Mode in Chapter 5
28 May., 2019	1.0.3	v.1.1.0	Revised the approvals
14 Jun., 2019	1.0.3	v.1.1.1	Revised the related picture in chapter 2.1.2 DI/DO
1 Apr., 2020	1.0.3	V.1.1.2	• Revised the description of LED in Modem mode • Revised the Regulatory and Type Approval Information • Deleted some redundant descriptions in product specifications • Revised the key features

Contents

Chapter 1 Product Overview

1.1 Key Features

The Robustel Smart Industrial IoT Gateway M1200 is a compact cellular gateway based on 2G/3G/4G networks. This dual-SIM gateway enables remote data transmission of local serial ports and I/O, and supports multiple interfaces such as RS-232, RS-485 and mini-USB. It can be used in a variety of applications such as energy, transportation, municipal, and agriculture.

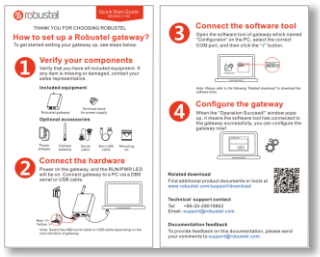
1.2 Package Contents

Before installing your M1200, verify the kit contents as following.
Note: The following pictures are for illustration purposes only, not based on their actual sizes.

- 1 x Robustel Smart Industrial IoT Gateway M1200

- 1 x 10-pin 3.5 mm RP male terminal block with lock for DI/DO connections

- 1 x *Quick Start Guide* with download link of other documents or tools



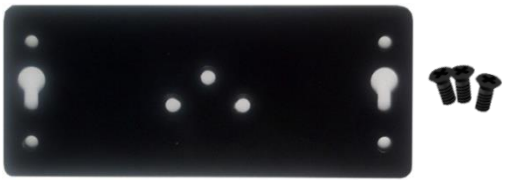
Note: If any of the above items is missing or damaged, please contact your Robustel sales representative.

Optional Accessories (sold separately)

- 3G/4G SMA cellular antenna (stubby/magnet optional)

Stubby antenna 1 Stubby antenna 2

- Wall mounting kit



- 35 mm DIN rail mounting kit

- Mini USB converter

- AC/DC power adapter (12V DC, 1.5 A; EU/US/UK/AU plug optional)

1.3 Specifications

Cellular Interface

- Number of antennas: 1
- Connector: SMA-K
- SIM slot: 2 (3.0 V & 1.8 V)

Serial Interface

- Number of ports: 1 x RS-232 + 1 x RS-485
- Connector: 10-pin 3.5 mm RP female socket with lock
- Baud rate: 300 bps to 115200 bps
- RS-232: TxD, RxD, GND
- RS-485: A (Data+), B (Data-)

Digital Input / Digital Output

- Number of ports: 2 x DI (wet contact) + 1 x DO (wet contact)
- Connector: 10-pin 3.5 mm RP female socket with lock
- ESD withstand level: contact: ±6 K, air: ±8 K
- Absolute maximum VDC: “V+” +5V DC (DI), 30V DC (DO)

USB Port

- Number of ports: 1 x Mini USB for configuration
- Connector: Mini Female
- Speed: 2.0 high speed up to 480 Mbit/s

Others

- LED indicators: 1 x RUN + 1 x RSSI (red/green bi-color light)
- Built-in: RTC, Watchdog, Timer

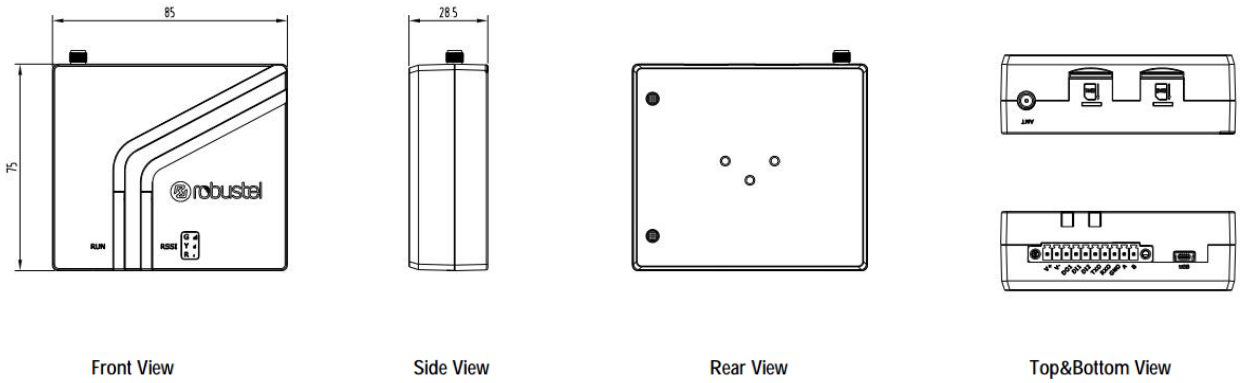
Power Supply and Consumption

- Connector: 10-pin 3.5 mm RP female socket with lock
- Input voltage: 9 to 36V DC
- Power consumption: Idle: 50 to 70 mA@12 V
  Data link: 300 mA (peak) @12 V

Physical Characteristics

- Ingress protection: IP30
- Housing & Weight: Plastic, 106 g
- Dimensions: 85 x 75 x 28.5 mm
- Installations: Desktop, wall mounting and 35 mm DIN rail mounting

1.4 Dimensions

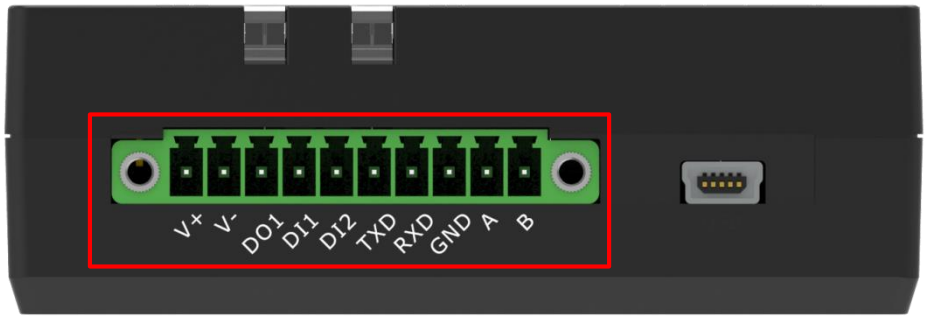


Front View | Side View | Rear View | Top&Bottom View

Chapter 2 Hardware Installation

2.1 PIN Description

2.1.1 PIN Assignment

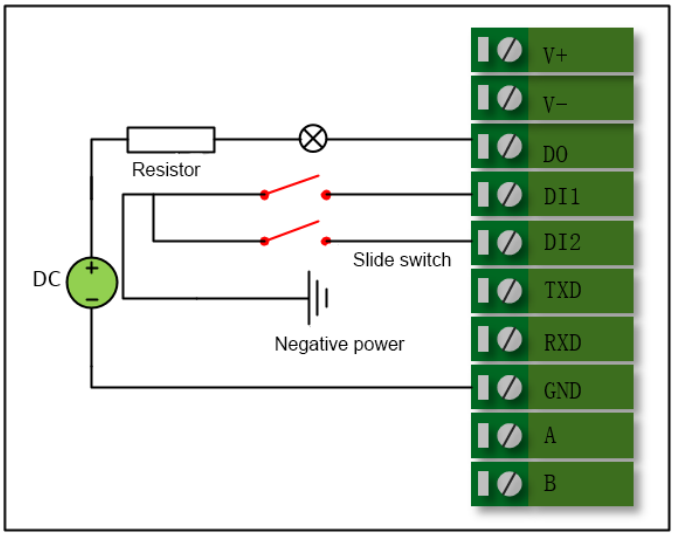


PIN	Power	Function	RS-232	RS-485	Direction
1	V+	--	--	--	M1200 ← Device
2	V-	--	--	--	M1200 ← Device
3	--	DO1	--	--	M1200 → Device
4	--	DI1	--	--	M1200 ← Device
5	--	DI2	--	--	M1200 ← Device
6	--	--	TXD	--	M1200 ← Device

7	--	--	RXD	--	M1200 → Device
8	--	--	GND	--	M1200 ↔ Device
9	--	--	--	Data+(A)	M1200 ↔ Device
10	--	--	--	Data- (B)	M1200 ↔ Device

2.1.2 DI/DO

The M1200 has two digital input connectors and one digital output connector. Please refer to the wiring diagram on the right



DI supports two inputs, the default state is 1.

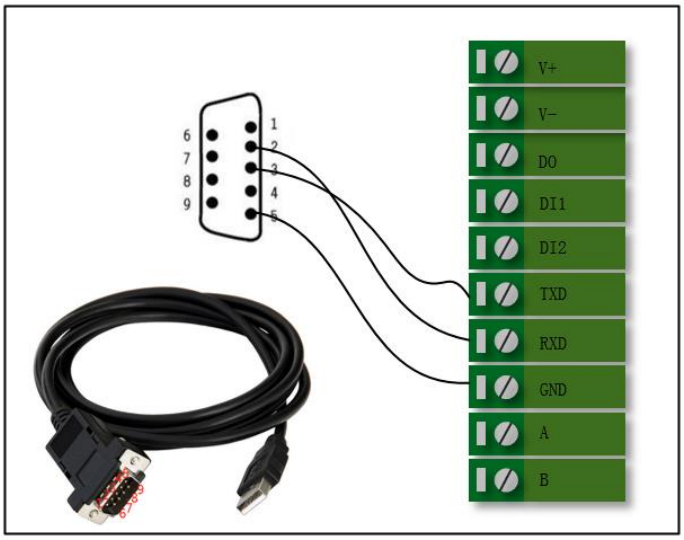
（1） NPN sensor open collector (OC) input, the emitter of the NPN sensor must be connected to the V- of the M1200.

（2） Switch signal input, one end of the switch is connected to DI, and the other end must be connected to V- of M1200.

DO is an open collector (OC) output and must limit the current on DO to no more than 10 mA. The negative pole of the DC power supply should be connected to the “GND” port.

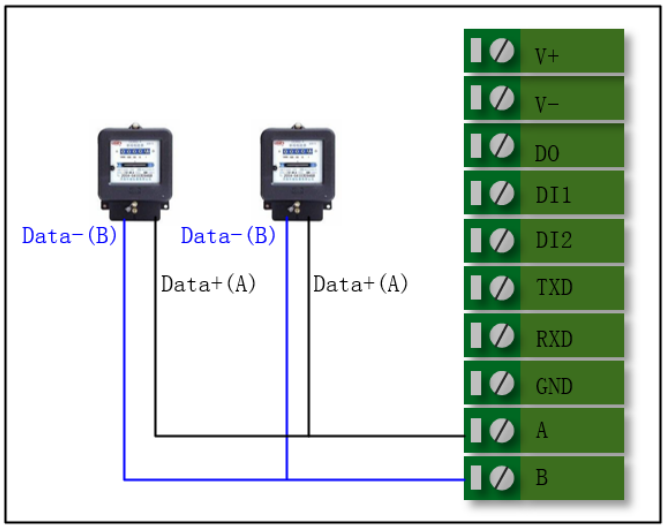
2.1.3 RS-232

The M1200 supports an RS-232 serial communication.
Please refer to the wiring diagram on the right.

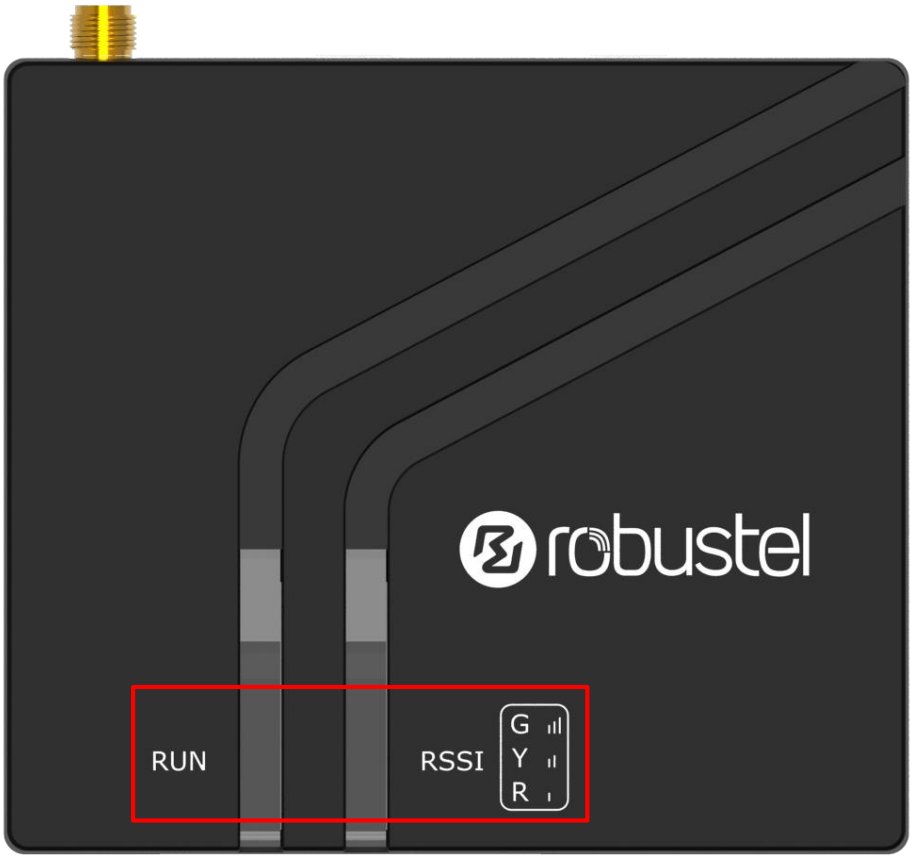


2.1.4 RS-485

The M1200 supports an RS-485 serial communication.
Please refer to the wiring diagram on the right.

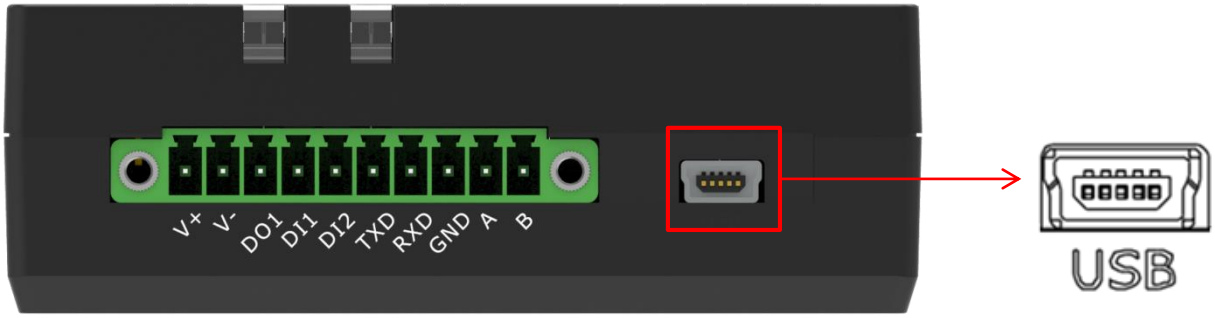


2.2 LED Indicators



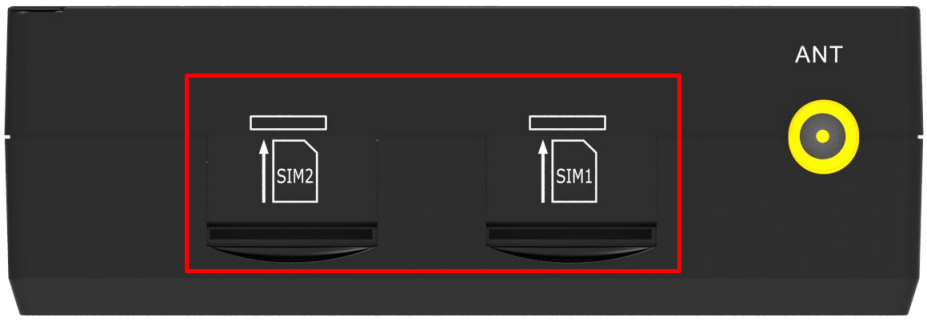
Name	Color	status	Description in DTU mode	Description in Modem mode
RUN	Yellow	On, solid	Power on	Power on
	Yellow	Fast blinking (2Hz)	System initializing	System initializing
	Yellow	On, blinking (1Hz)	Initialization completed, device operating normally	Initialization completed, device operating normally
	Green	On, blinking	Device operating normally, GPRS connected	Device operating normally, GPRS connected
	Red	Fast blinking	Device in abnormal state	Device in abnormal state
RSSI	None	Off	CSQ value 0 or 99, not registered on the network	off（The RSSI LED status is off）
	Red	On, solid	CSQ 1-10, poor signal	
	Yellow	On, solid	CSQ 11-20, normal signal	
	Green	On, solid	CSQ 21-31, good signal	

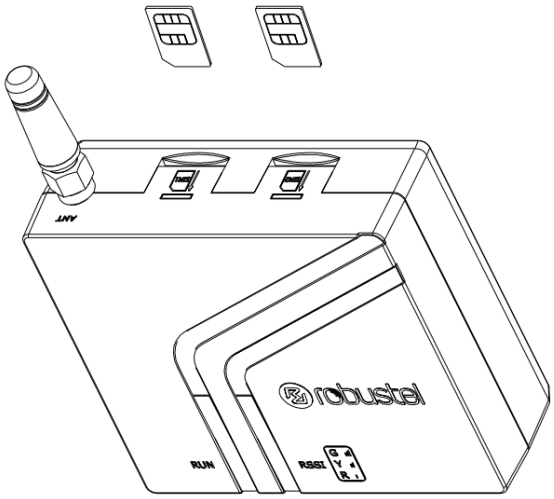
2.3 USB interface



Function	Operation
Data communication	Use a USB cable to connect the gateway's mini USB interface to an external communication device.

2.4 Insert or Remove SIM Card





Please confirm before inserting the SIM card. When the SIM card is turned on and the device is configured without the correct PIN, the SIM card is unavailable.

- **Insert SIM card**

1. Make sure gateway is powered off.
2. To insert SIM card, press the card with finger until you hear a click

- **Remove SIM card**

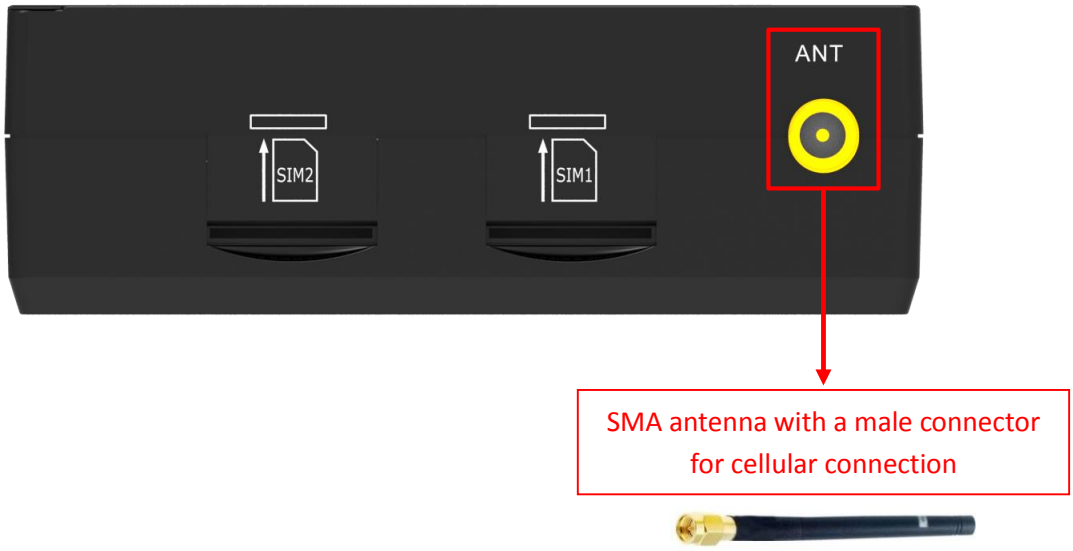
1. Make sure gateway is powered off.
2. To remove SIM card, press the card with finger until it pops out and then take out the card.

Note:

1. Recommended torque for inserting is 0.5 N.m, and the maximum allowed is 0.7 N.m.
2. Use the specific card when the device is working in extreme temperature (temperature exceeding 40 °C), because the regular card for long-time working in harsh environment will be disconnected frequently.
3. Do not touch the metal of the card surface in case information in the card will lose or be destroyed.
4. Do not bend or scratch the card.
5. Keep the card away from electricity and magnetism.
6. Make sure gateway is powered off before inserting or removing the card.

2.5 Attach External Antenna (SMA Type)

Attach an external SMA antenna to the gateway's antenna connector and twist tightly. Make sure the antenna is within the correct frequency range provided by the ISP and with 50 Ohm impedance.
Note: Recommended torque for tightening is 0.35 N.m.

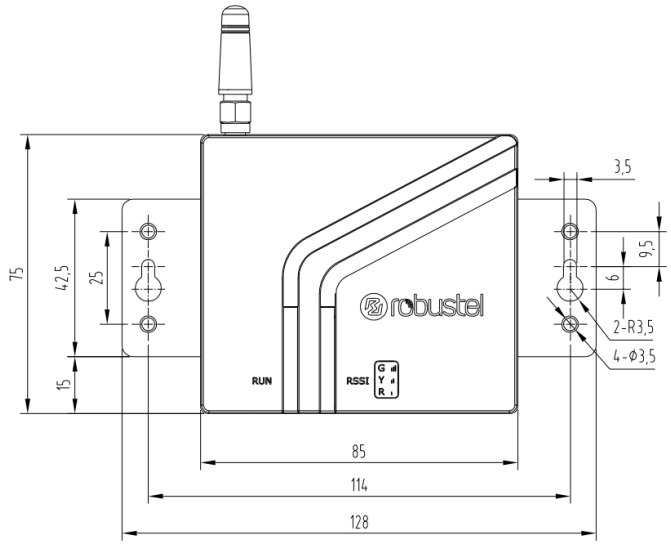


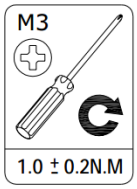
2.6 Mount the Gateway

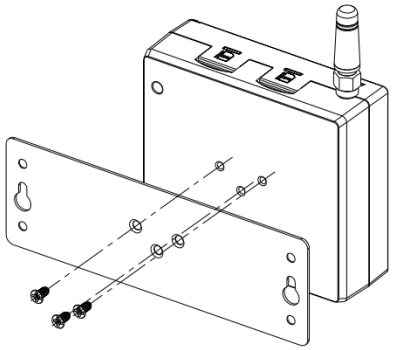
The gateway can be placed on a desktop or mounted to a wall or a 35 mm DIN rail.

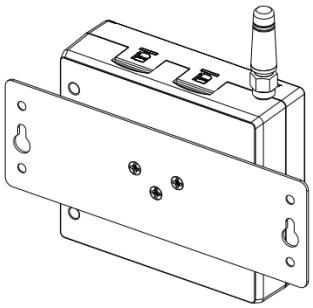
Two methods for mounting the gateway

- Wall mounting (measured in mm)





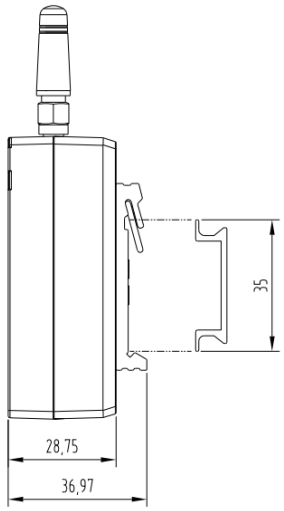


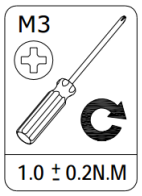


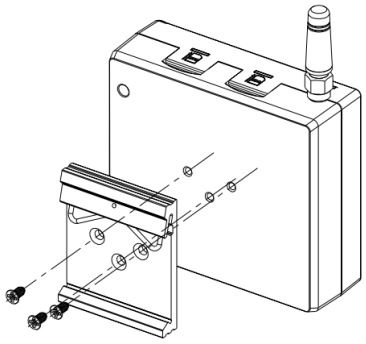
Use 3 pcs of ST2.9*6 flat head self-tapping Phillips screws to fix the wall mounting kit to the gateway, and then use 2 pcs of M3 drywall screws to mount the gateway associated with the wall mounting kit on the wall.

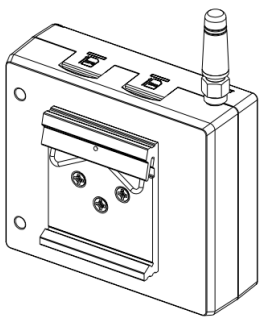
Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

- DIN rail mounting (measured in mm)





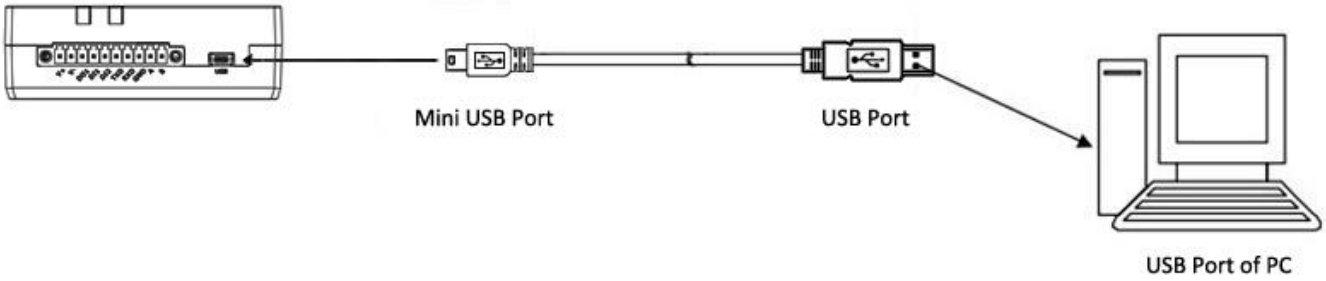




Use 3 pcs of ST3*8 flat head self-tapping Phillips screws to fix the DIN rail to the gateway, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.

Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

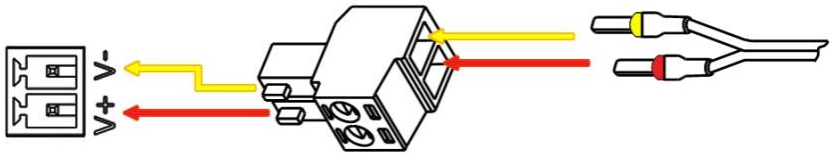
2.7 Connect the Gateway to a Computer



Connect a USB cable to the gateway's mini USB interface to an external controller or computer's USB port

2.8 Power Supply

COLOR	POLARITY
RED	+
YELLOW	-



M1200 supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way.

Note: The range of power voltage is 9 to 36V DC.

Chapter 3 Initial Configuration

The DTU supports webpage configuration. The supported browsers are IE8.0 or above, Google Chrome, Firefox, etc. The supported operating system is Windows 7 and Windows 10. For M1200, the method of connecting to the gateway is that the device connects to the PC through the USB port, so that users can configure it on the web page through the mini usb port.

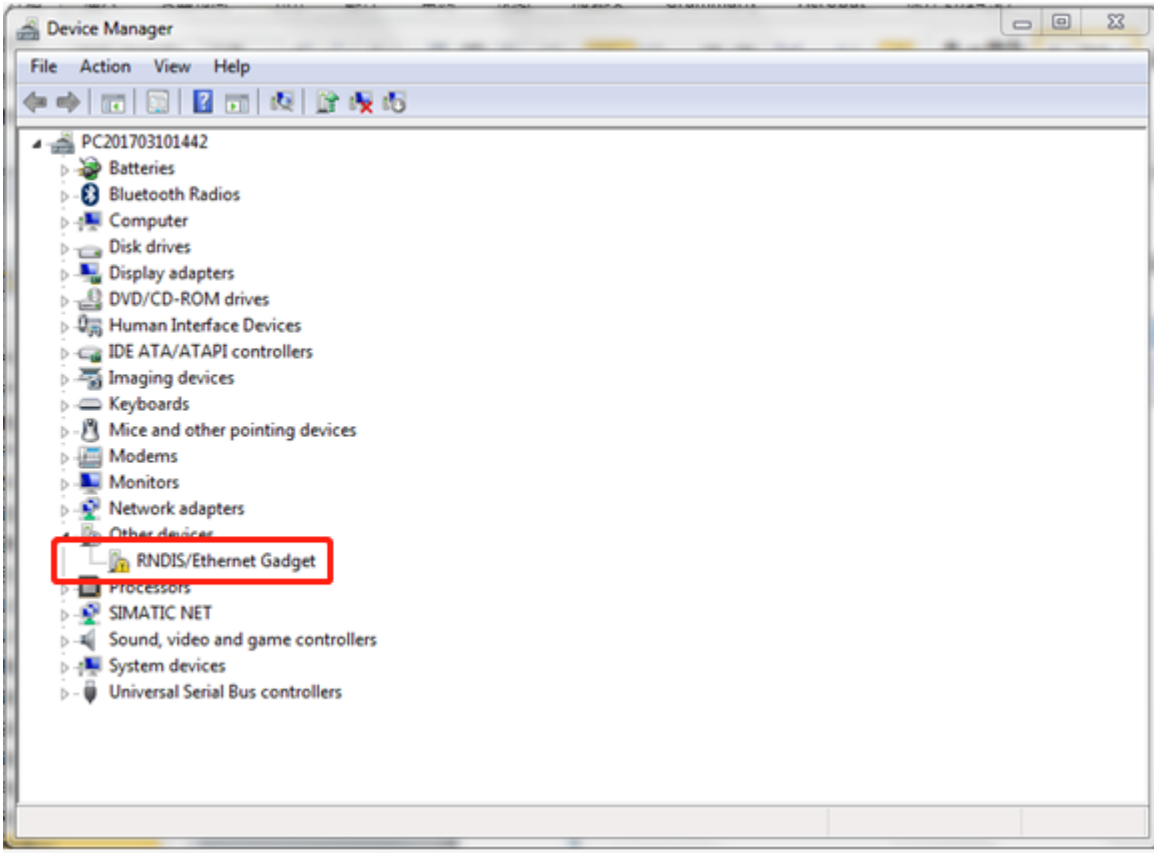
3.1 Configure the PC

M1200 connects to the PC through the USB port. The PC automatically obtains the IP address of the same network segment as the M1200 to access the device page.

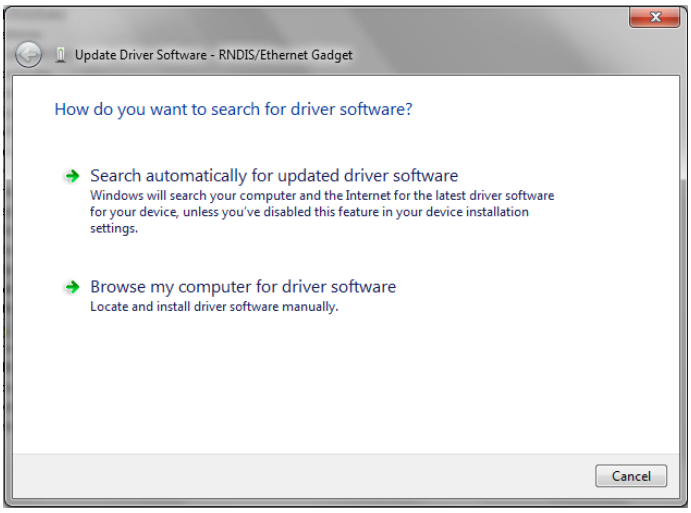
3.1.1 Windows 7 System

This part takes **the Windows 7** as the example; the configuration of Windows system is similar.

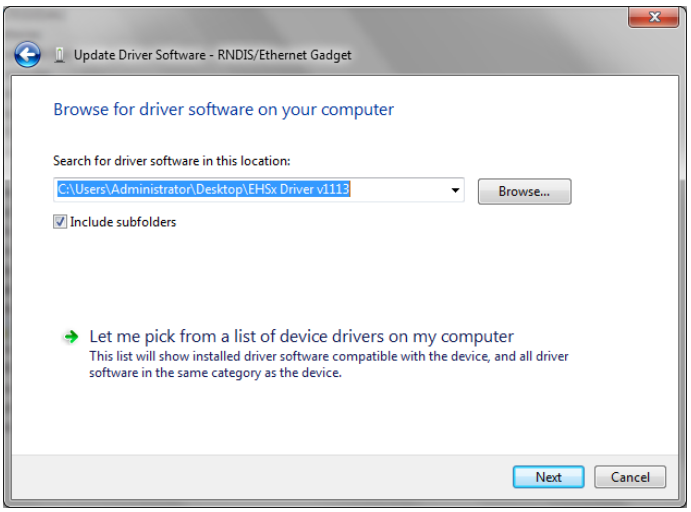
1. Click “Start > Control Panel > Device Manager”. After the device USB is connected to the computer, check the identified serial port and attempt to install the driver;



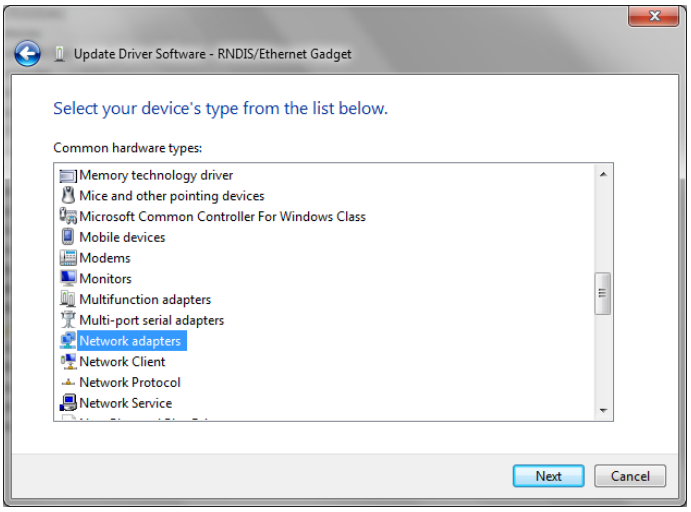
2. Press the right button to select “Update Driver Software”, and select “Browse my computer for driver software”;



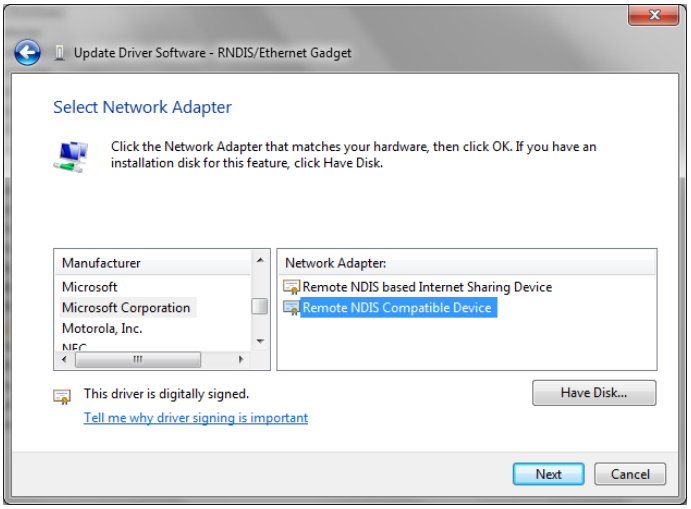
3. Select “Let me pick from a list of device drivers on my computer”;



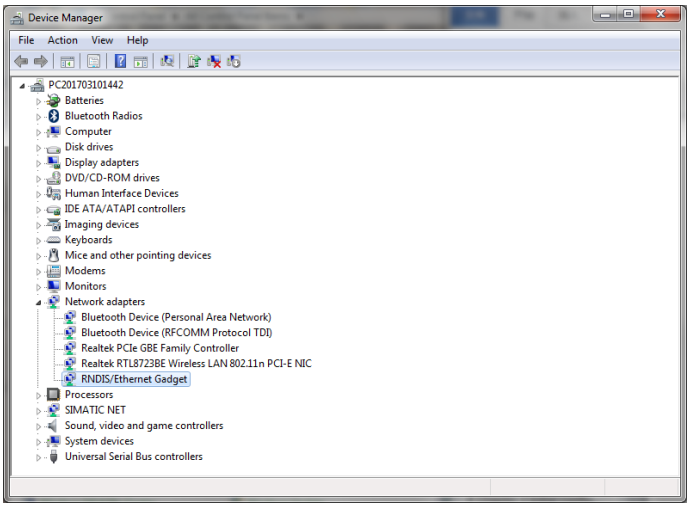
4. Select “Network Adapter” in the list and click “Next”;



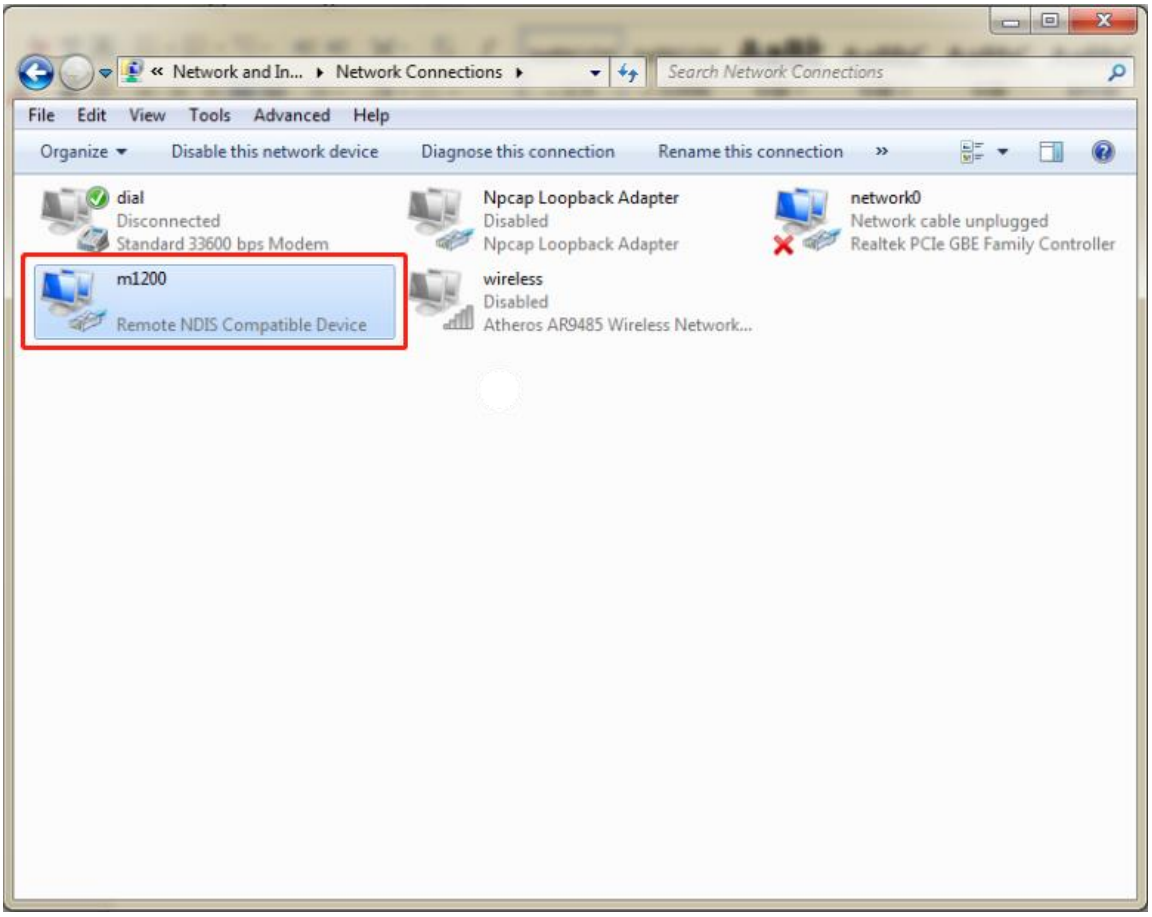
5. Find “Microsoft Corporation” on the left Manufacture, and select “Remote NDIS Compatible Device” on the right Network Adapter, then click “Next”;



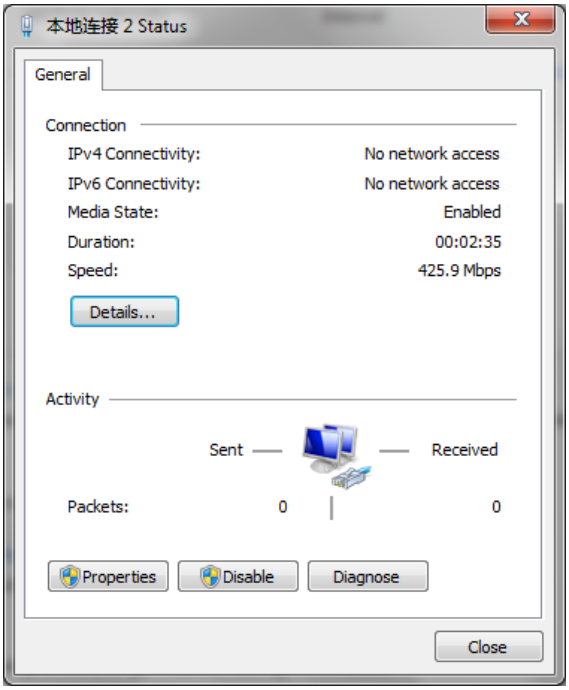
6. After installation, the newly added network adapter as shown below;



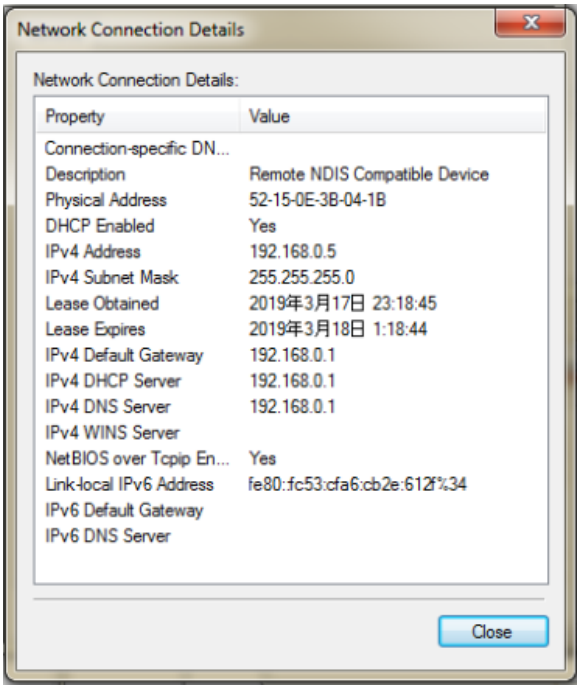
7. Click “Start > Control Panel > Network and Sharing Center> Change Adapter Settings” to view the new network;



8. Double-click on the newly added network to view the "Details";



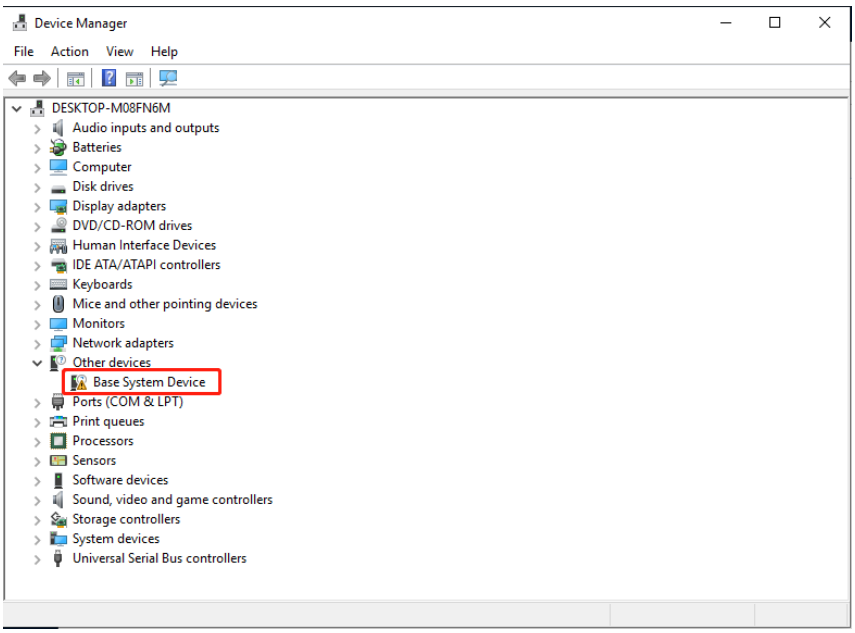
9. The default gateway is the device login page address when you see the automatically acquired IP address in network connection details (different MAC addresses get different IP addresses).



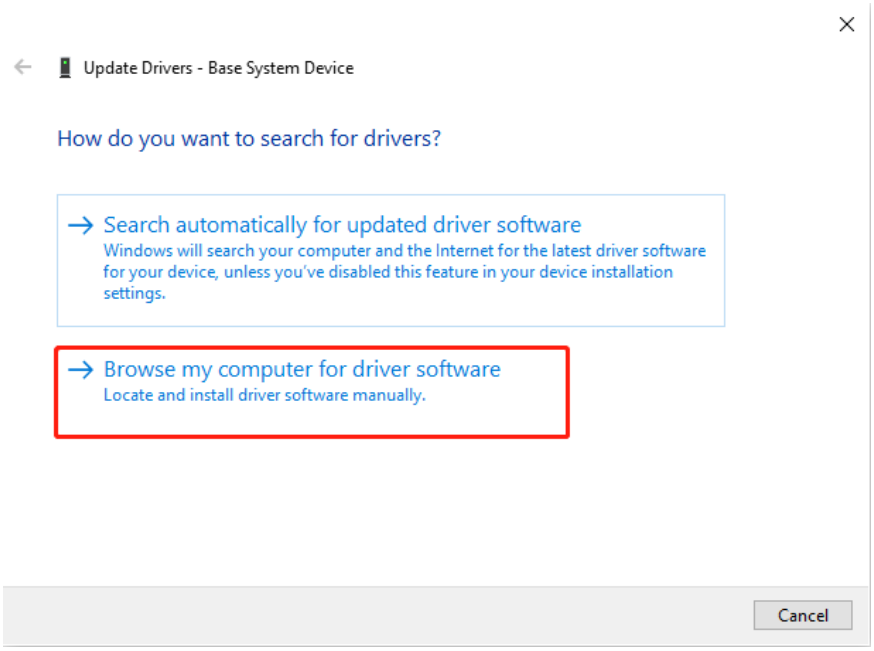
10. Open the browser and enter 192.168.0.1 to login to the device page for configuration.

3.1.2 Windows 10 System

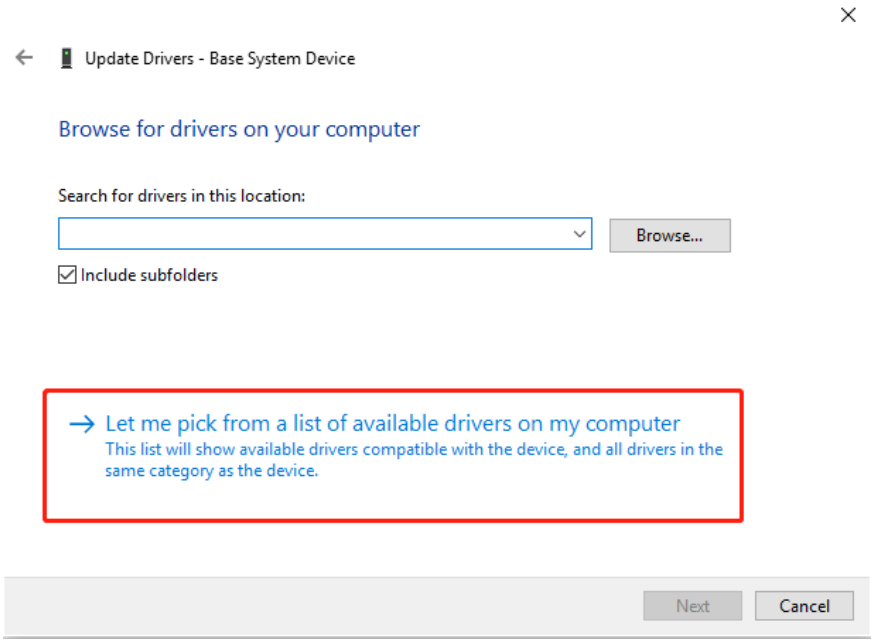
1. Click “Start > Control Panel > Device Manager”. After the device is connected to the computer, the PC check the identified serial port and attempt to install the driver;



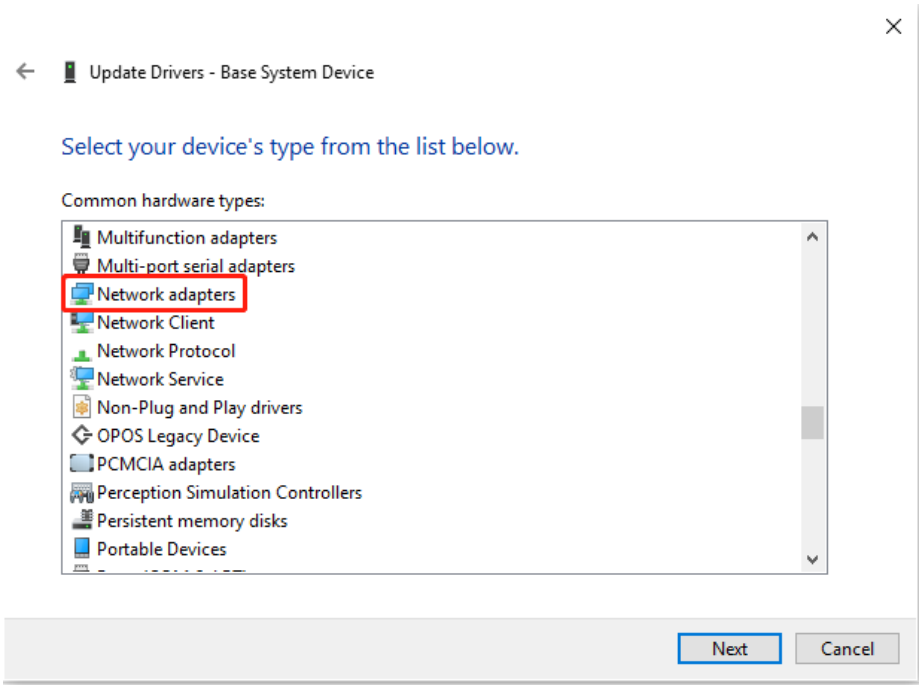
2. Press the right button to select “Update Driver Software”, and select “Browse my computer for driver software”;



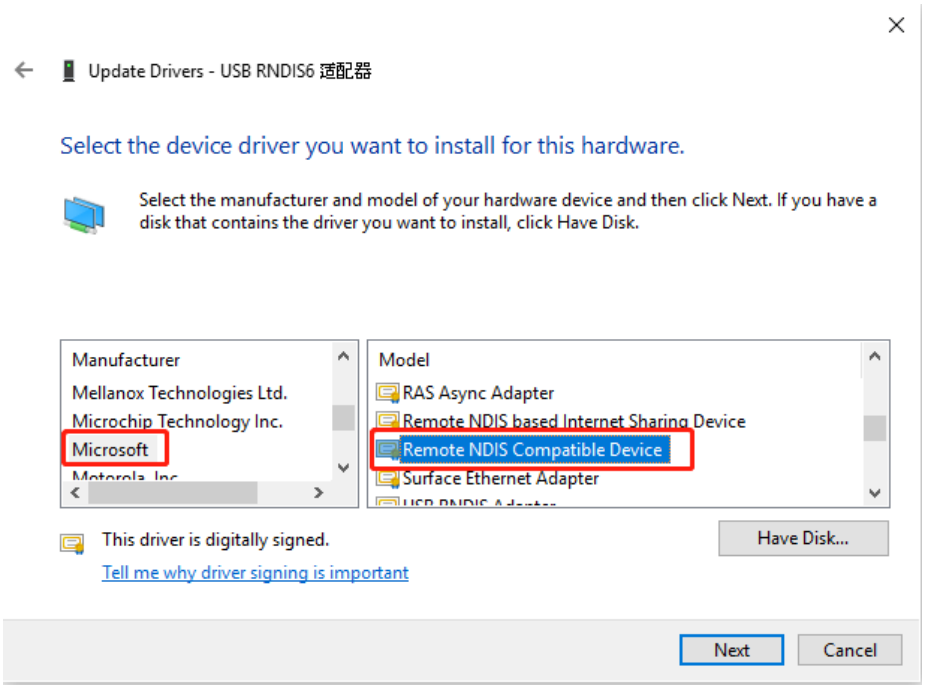
3. Select "Let me pick from a list of available drivers on my computer ";



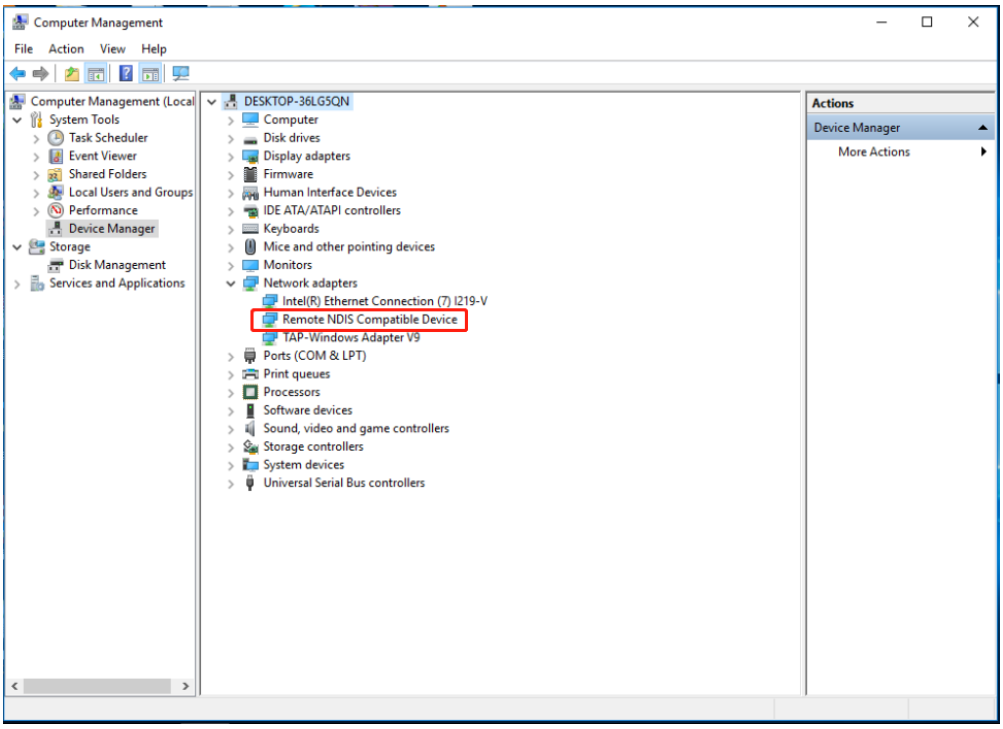
4. Select "Network Adapter" in the list and click "Next";



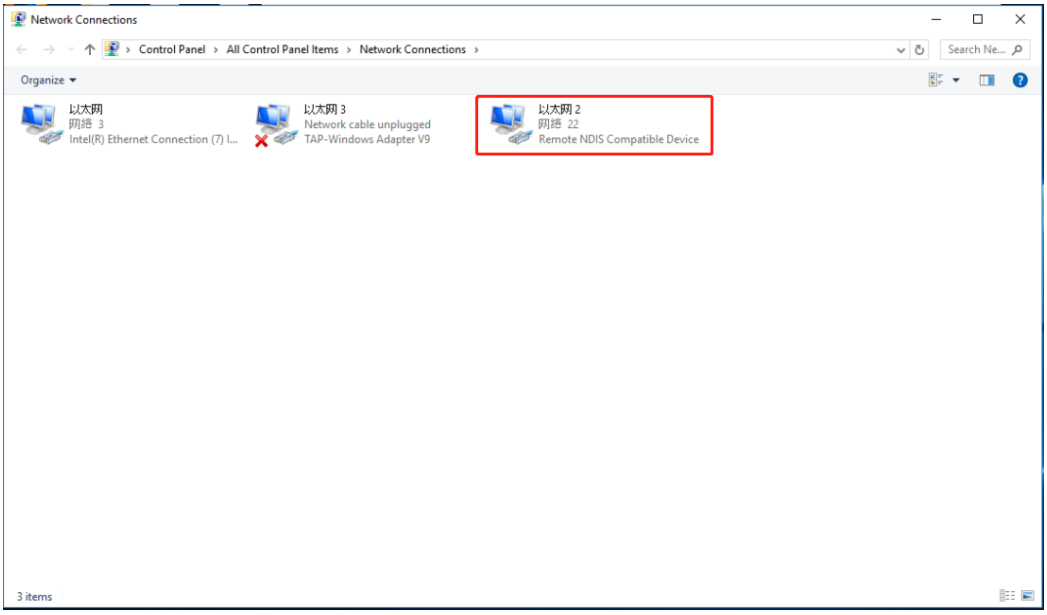
5. Find "Microsoft" in the manufacturer on the left, select "Remote NDIS compatible device" in the right network adapter, and click "Next";



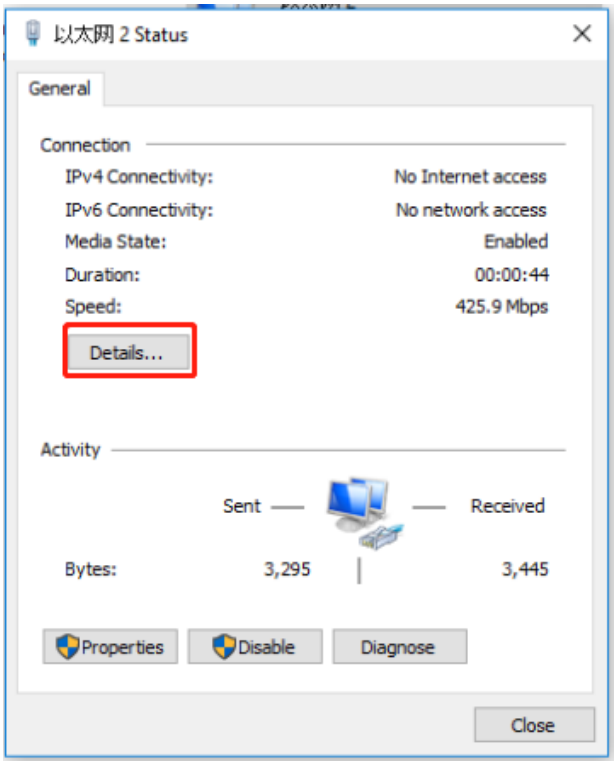
6. After installation, the new network adapter as shown below;



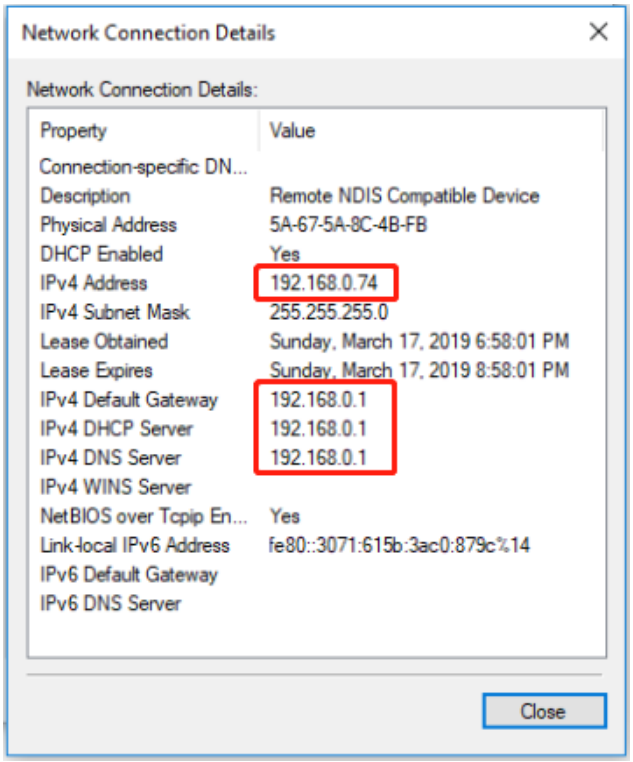
7. Click “Start > Control Panel > Network and Sharing Center” to view the new network;



8. Click “Ethernet 2” (the specific name is vary from the computer), and click “Details”;



9. The default gateway is the device login page address when you see the automatically acquired IP address in network connection details (different MAC addresses get different IP addresses);



10. Open the browser and enter 192.168.0.1 to login to the device page for configuration;

3.2 Factory Default Settings

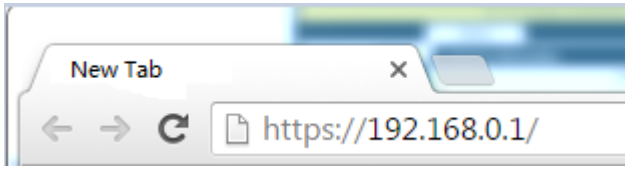
Before configuring your gateway, you need to know the following default settings.

Item	Description
Username	admin
Password	admin

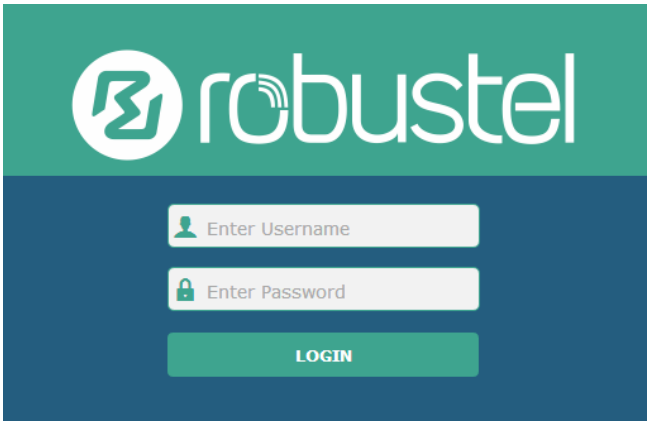
3.3 Log in the Gateway

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

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

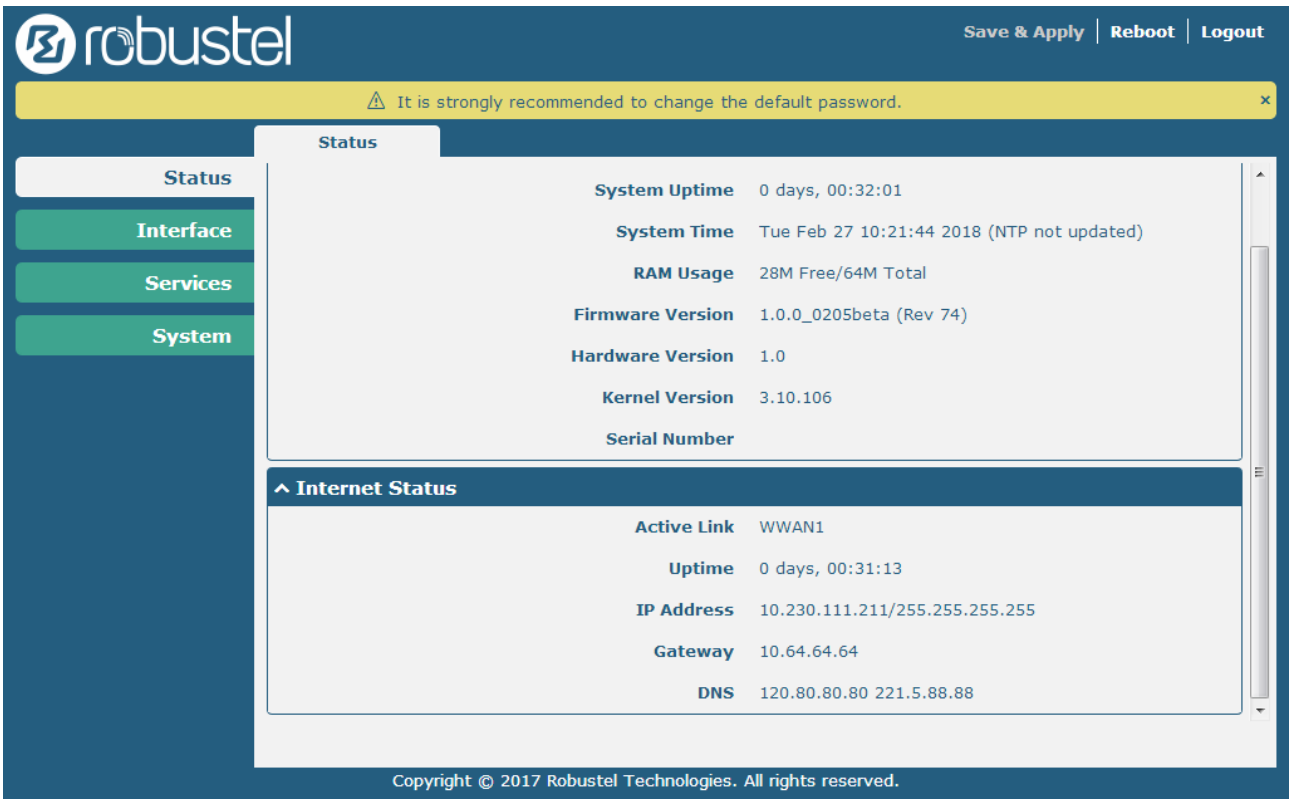


3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password are "admin".
   Note: If enter the wrong username or password over six times, the login web will be locked for 5 minutes.

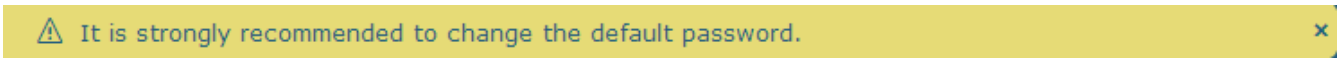


3.4 Control Panel

After logging in, the home page of the M1200's web interface is displayed, for example.



Using the original password to log in the gateway, the page will pop up the following tab



It is strongly recommended for security purposes that you change the default username and/or password. To change your username and/or password, see **3.25 System > User Management**.

Control Panel		
Item	**Description**	**Button**
Save & Apply	Click to save the current configuration into gateway's flash and apply the modification on every configuration page, to make the modification taking effect.	Save & Apply
Reboot	Click to restart the gateway.	Reboot
Logout	Click to log the current user out safely.	Logout
Submit	Click to save the modification on current configuration page.	Submit
Cancel	Click to cancel the modification on current configuration page.	Cancel

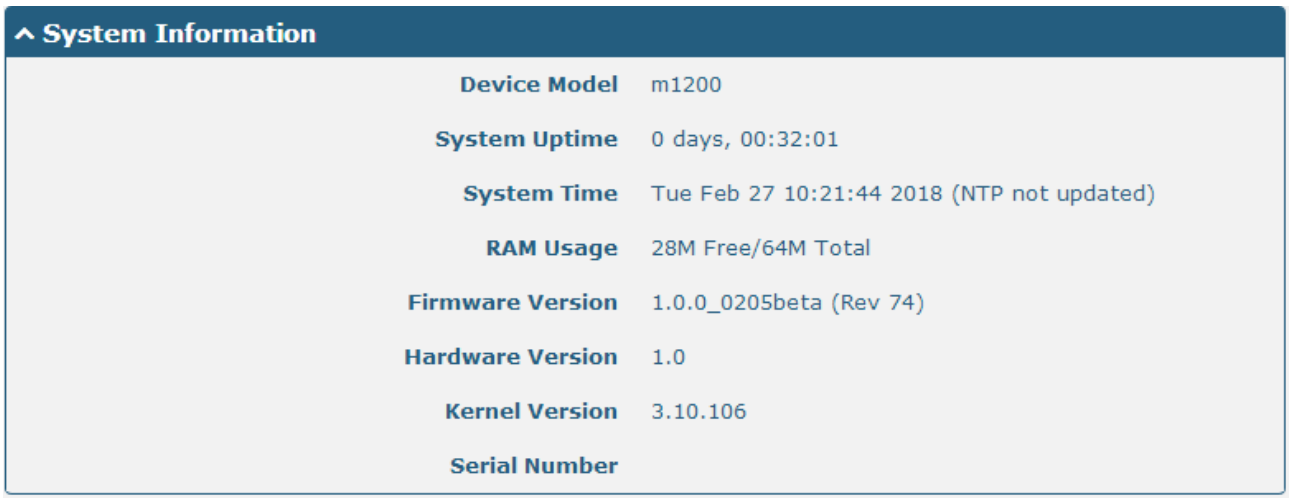
Note: The steps of how to modify configuration are as bellow:

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

3.5 Status

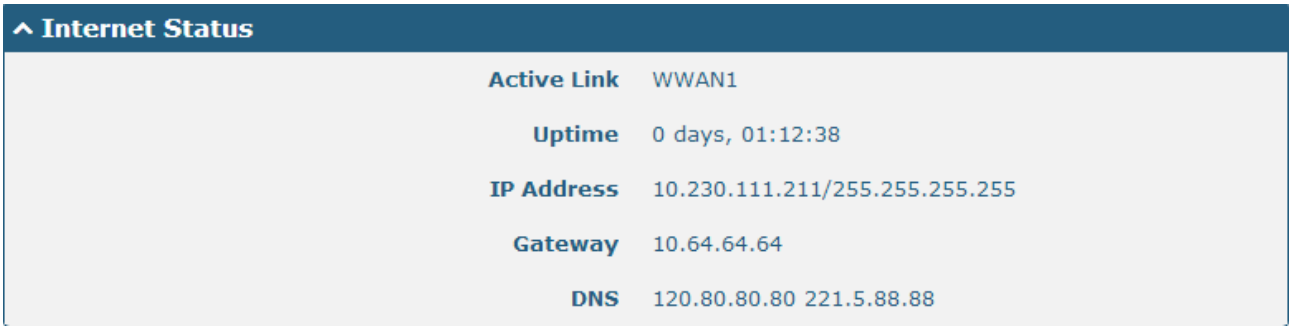
This page allows you to view the System Information, Internet Status and LAN Status of your gateway.

System Information



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

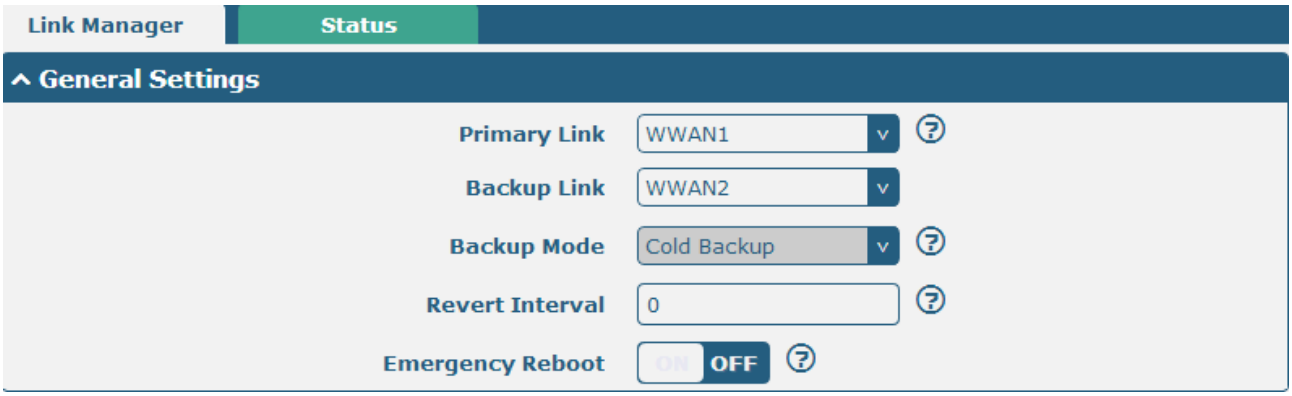
Internet Status



Internet Status	
Item	**Description**
Active Link	Show the current active link.
Uptime	Show the current amount of time the link has been connected.
IP Address	Show the IP address of current link.
Gateway	Show the gateway address of the current link.
DNS	Show the current primary DNS server and secondary server.

3.6 Interface > Link Manager

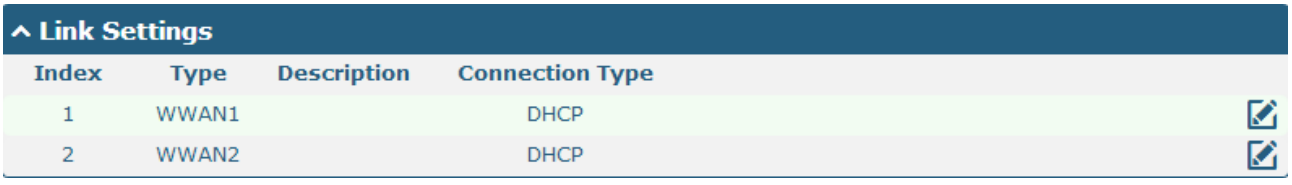
This section allows you to setup the link connection.



General Settings @ Link Manager		
Item	**Description**	**Default**
Primary Link	Select from "WWAN1" or "WWAN2". • WWAN1: Select to make SIM1 as the primary wireless link • WWAN2: Select to make SIM2 as the primary wireless link	WWAN1
Backup Link	Select from "WWAN1", "WWAN2", or "None". • WWAN1: Select to make SIM1 as backup wireless link • WWAN2: Select to make SIM2 as backup wireless link • None: Do not select any backup link	WWAN2
Backup Mode	Can only select from "Cold Backup". • Cold Backup: The inactive link is offline on standby	Cold Backup
Revert Interval	Specify the number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking.	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links available.	OFF

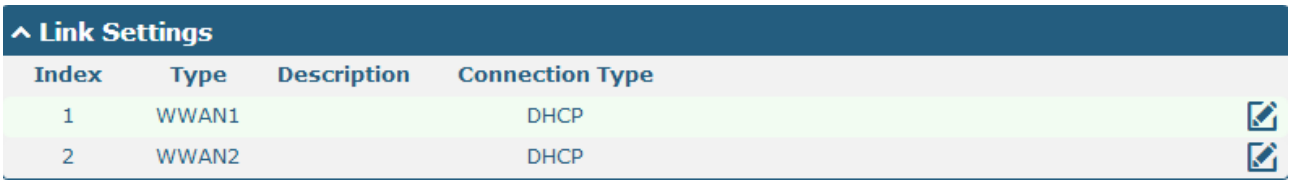
Note: Click ⑦ for help.

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

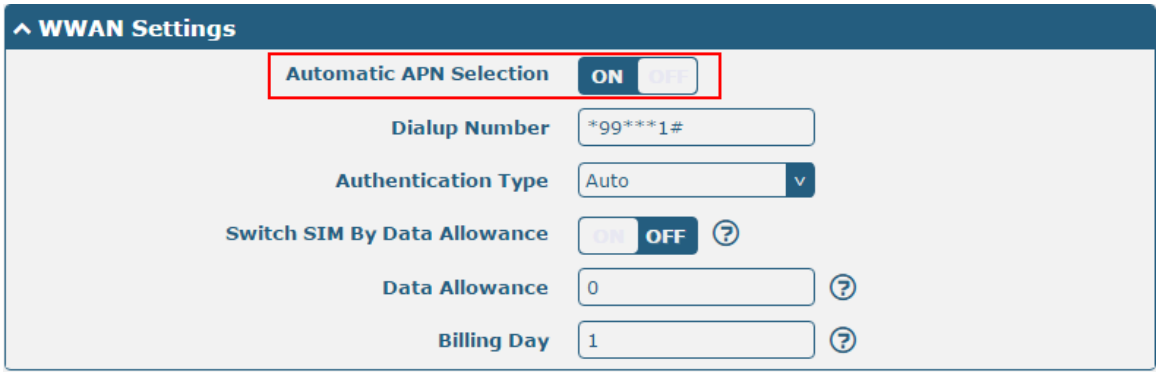


Click on the right-most of WWAN1/WWAN2 to enter the configuration window.

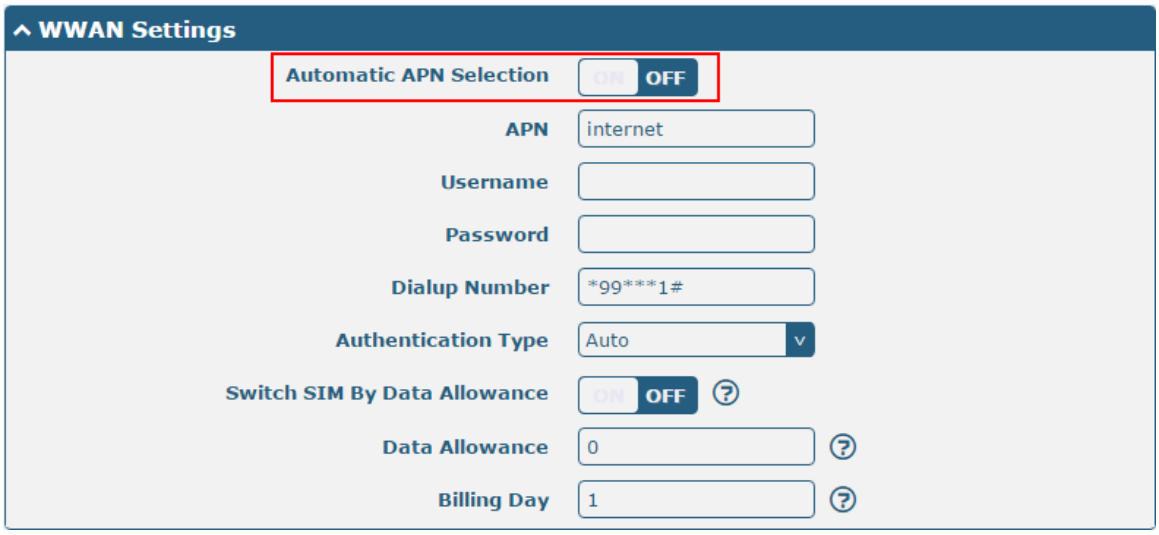
WWAN1/WWAN2

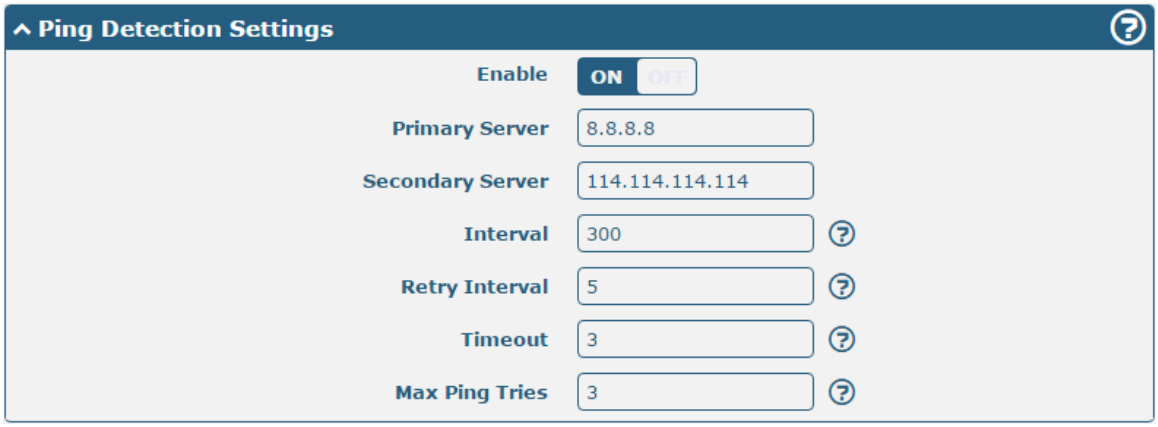


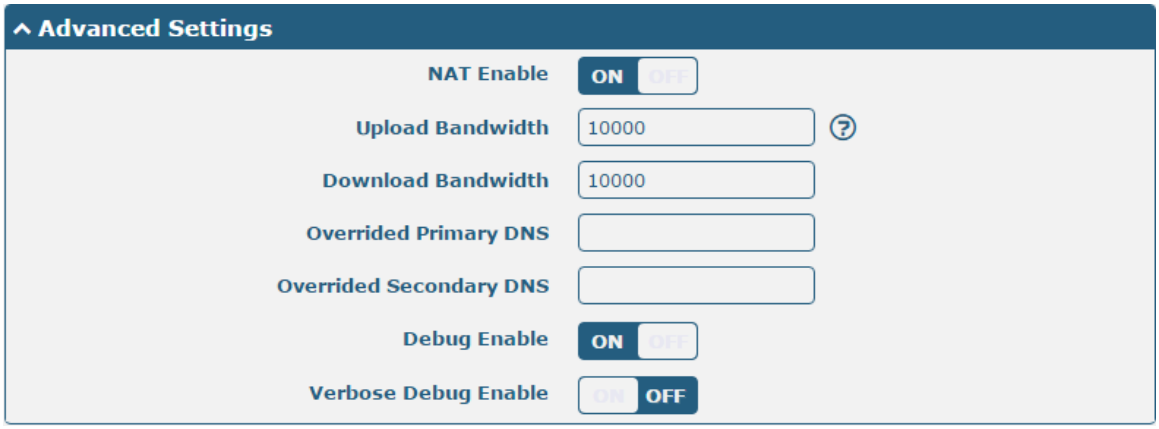
The window is displayed as below when enabling the "Automatic APN Selection" option.



The window is displayed as below when disabling the "Automatic APN Selection" option.





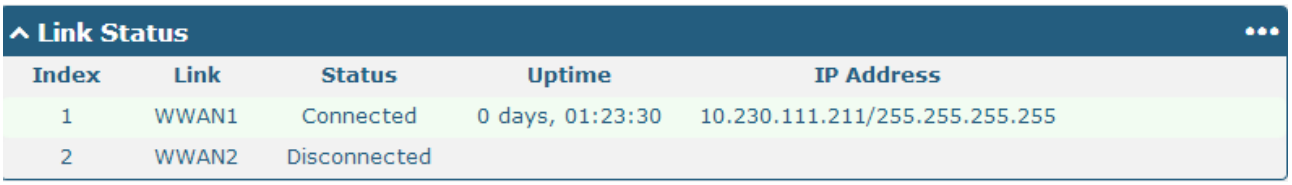


Link Settings (WWAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null
WWAN Settings		
Automatic APN Selection	Click the toggle button to enable/disable the "Automatic APN Selection" option. After enabling, the device will recognize the access point name automatically. Alternatively, you can disable this option and manually add the access point name.	ON
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Dialup Number	Enter the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from "Auto", "PAP" or "CHAP" as the local ISP required.	Auto
Switch SIM By Data Allowance	Click the toggle button to enable/disable this option. After enabling, it will switch to another SIM when the data limit reached. **Note**: Only used for dual-SIM backup.	OFF
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in **Interface > Link Manager > Status > WWAN Data Usage Statistics**. 0 means disable data traffic record.	0
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the gateway.	ON
Primary Server	Gateway will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8

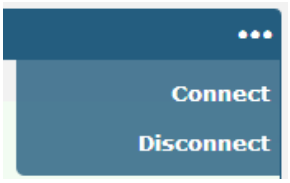
Link Settings (WWAN)		
Item	**Description**	**Default**
Secondary Server	Gateway will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the gateway will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

Status

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



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

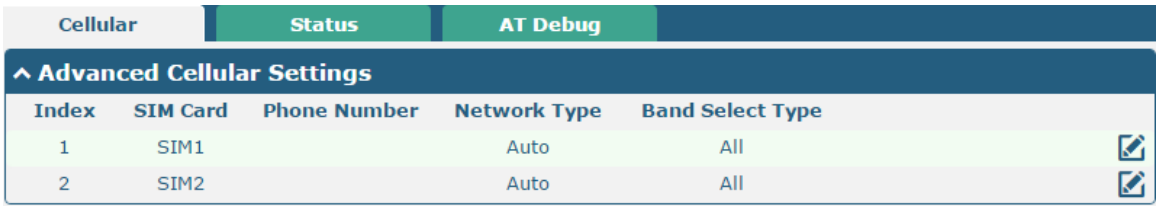


Click the row of the link, and it will show the details information of the current link connection under the row.

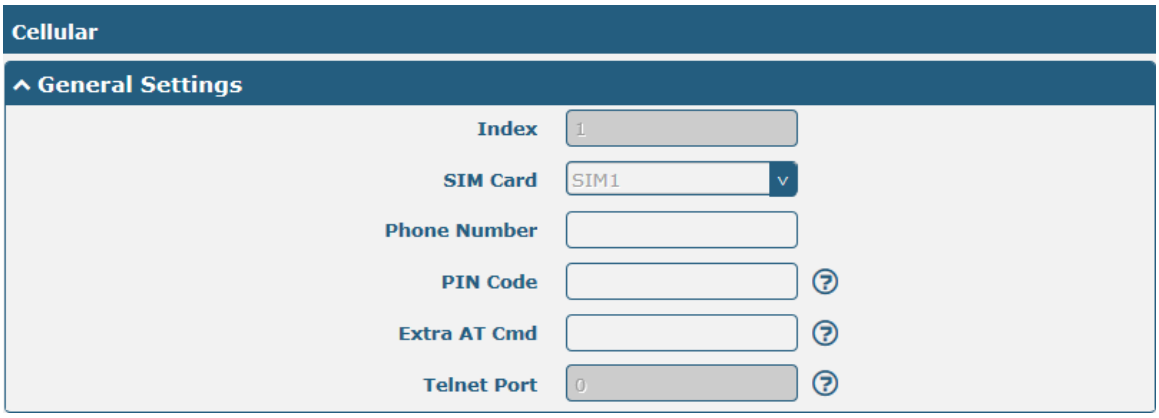
Click the Clear button to clear SIM1 or SIM2 monthly data traffic usage statistics. Data statistics will be displayed only if enable the Data Allowance function in **Interface > Link Manager > Link Settings > WWAN Settings > Data Allowance**.

3.7 Interface > Cellular

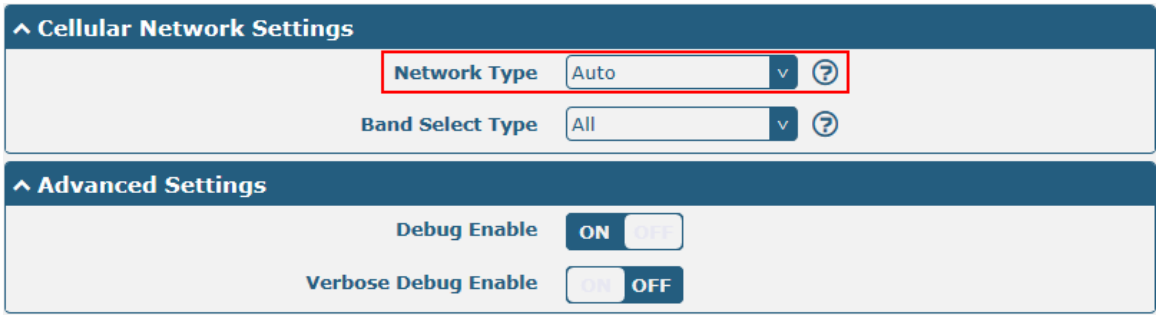
This section allows you to set the related parameters of Cellular. M1200 has two SIM card slots, but do not support two SIM cards online simultaneously due to its single-module design. If insert single SIM card at the first time, SIM1 slot and SIM2 slots are available.



Click of SIM 1 to edit the parameters.

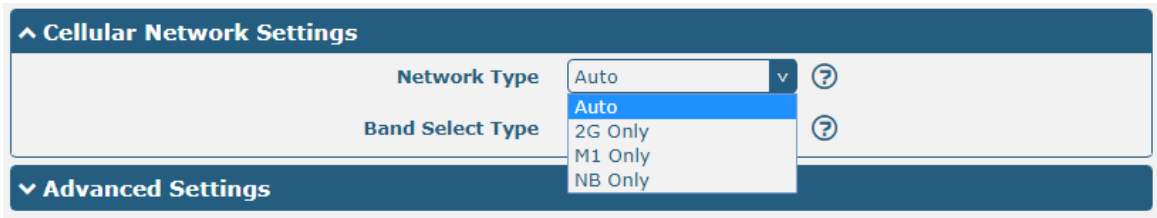


The window is displayed as below when choosing “Auto” as the network type.



The window is displayed as below when choosing “Specify” as the band select type.

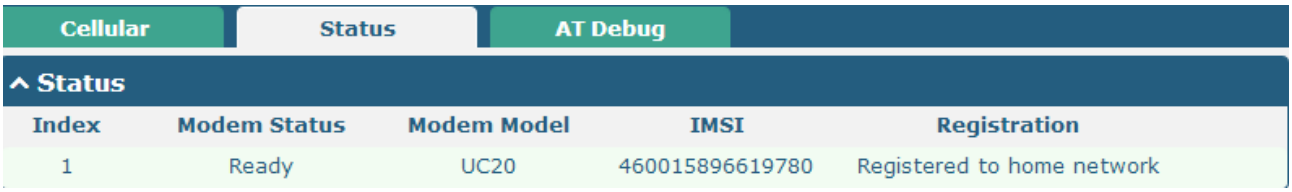
Note: When the device selection module is BG96, the options in "Network Type" are as follows.



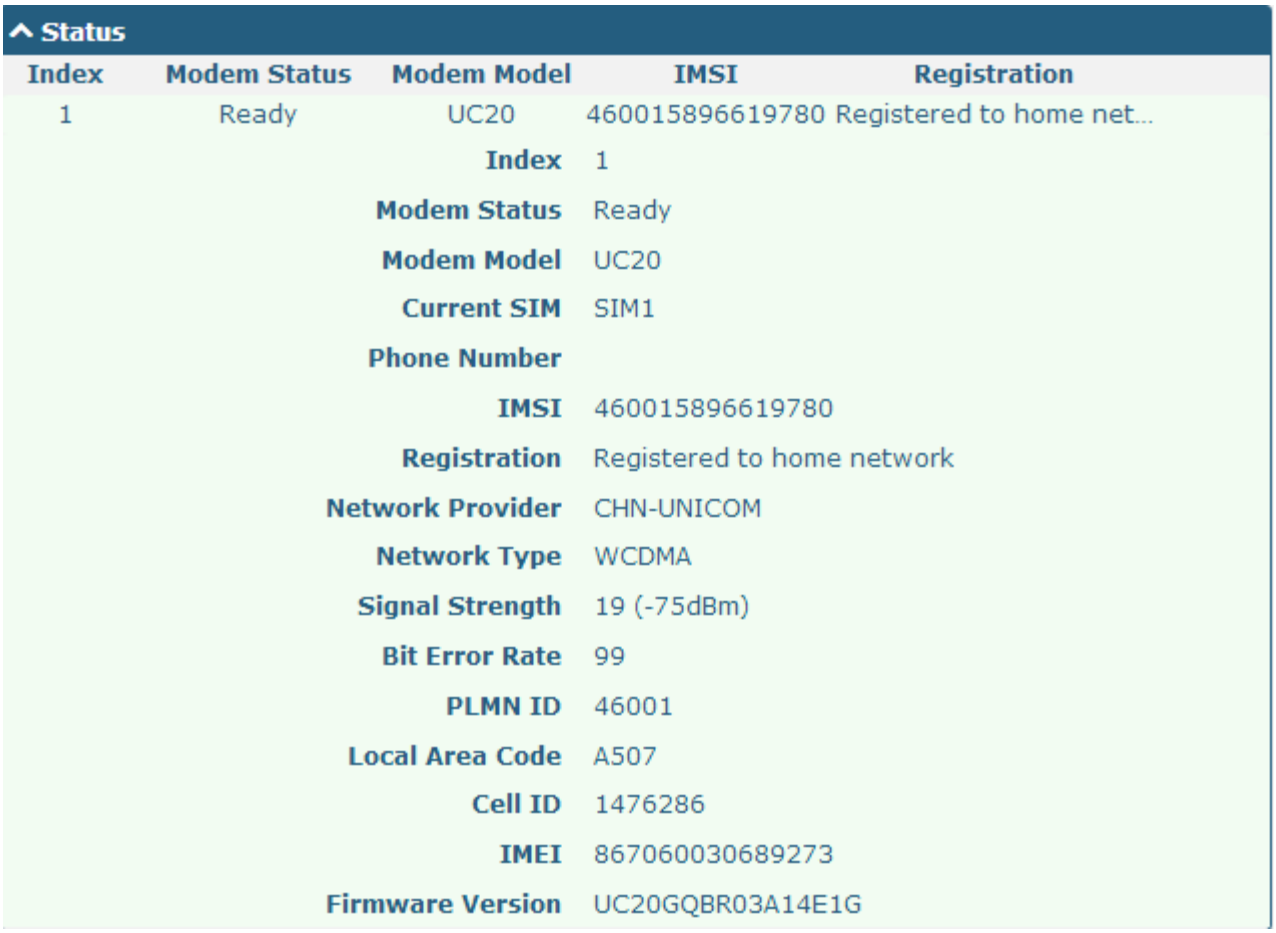
Cellular		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
SIM Card	Show the currently editing SIM card.	SIM1
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Cellular Network Settings		

Cellular		
Item	**Description**	**Default**
Network Type	Select the cellular network type, which is the network access order. Select from "Auto", "2G Only", "2G First", "3G Only", "3G First". • Auto: Connect to the best signal network automatically • 2G Only: Only the 2G network is connected • 2G First: Connect to the 2G Network preferentially • 3G Only: Only the 3G network is connected • 3G First: Connect to the 3G Network preferentially Note: When the device selection module is BG96, select from "Auto", "2G Only", "M1 only", "NB Only". • Auto: Connect to the best signal network automatically • 2G Only: Only the 2G network is connected • M1 Only: Only the CAT M1 network is connected • NB Only: Only the NB-IOT network is connected	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

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



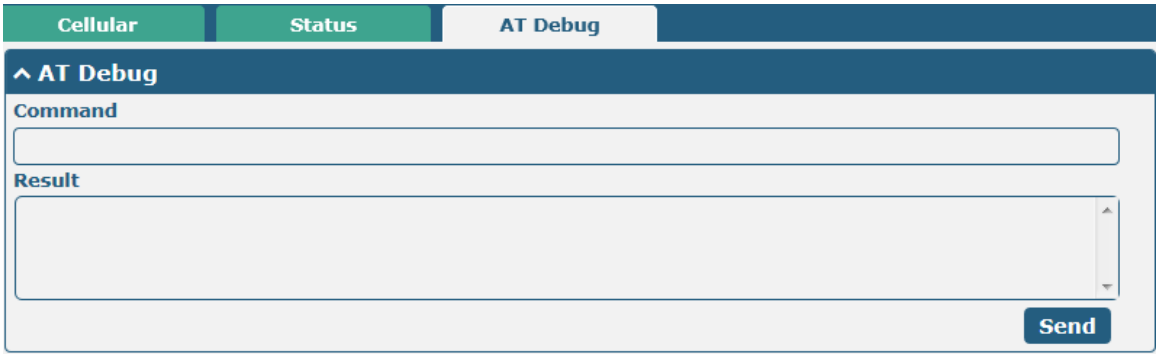
Click the row of status, the details status information will be displayed under the row.



Status	
Item	**Description**
Index	Indicate the ordinal of the list.
Modem Status	Show the status of the radio module.
Modem Model	Show the model of the radio module.
Current SIM	Show the SIM card that your gateway is using.
Phone Number	Show the phone number of the current SIM. **Note:** This option will be displayed if enter manually in **Cellular > Advanced Cellular Settings > SIM1/SIM2 > General Settings > Phone Number**.
IMSI	Show the IMSI number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. WCDMA.

Status	
Item	**Description**
Signal Strength	Show the signal strength detected by the mobile.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the gateway.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

This page allows you to check the AT Debug.

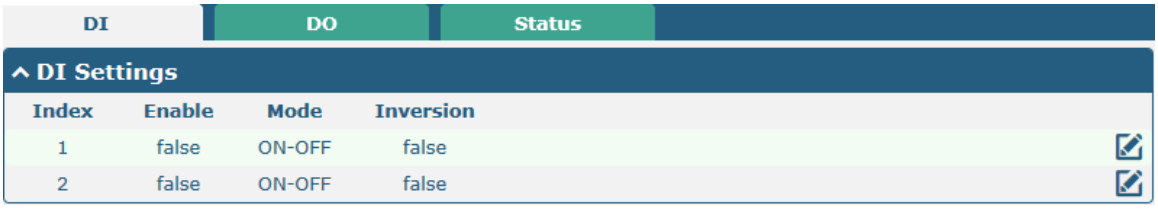


AT Debug		
Item	**Description**	**Default**
Command	Enter the AT command that you want to send to cellular module in this text box.	Null
Result	Show the AT command responded by cellular module in this text box.	Null
Send	Click the button to send AT command.	--

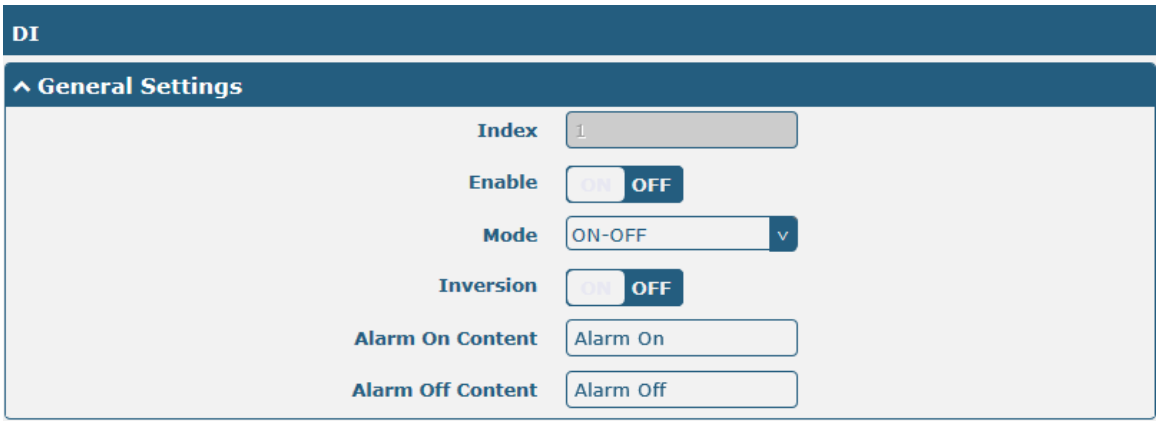
3.8 Interface > DIDO

This section allows you to set the DI and DO parameters. Digital Input and Digital Output are the specific interfaces for M1200. The DI interface can be used for triggering alarm, while the DO can be used for controlling the slave device so as to realize real-time monitoring.

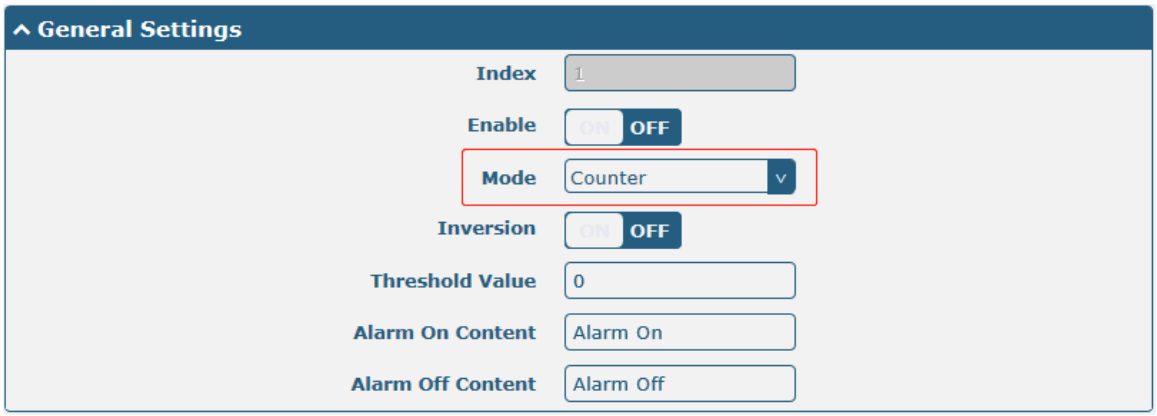
DI



Click the right-most button of index 1 as below. The default mode is “ON-OFF”.



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



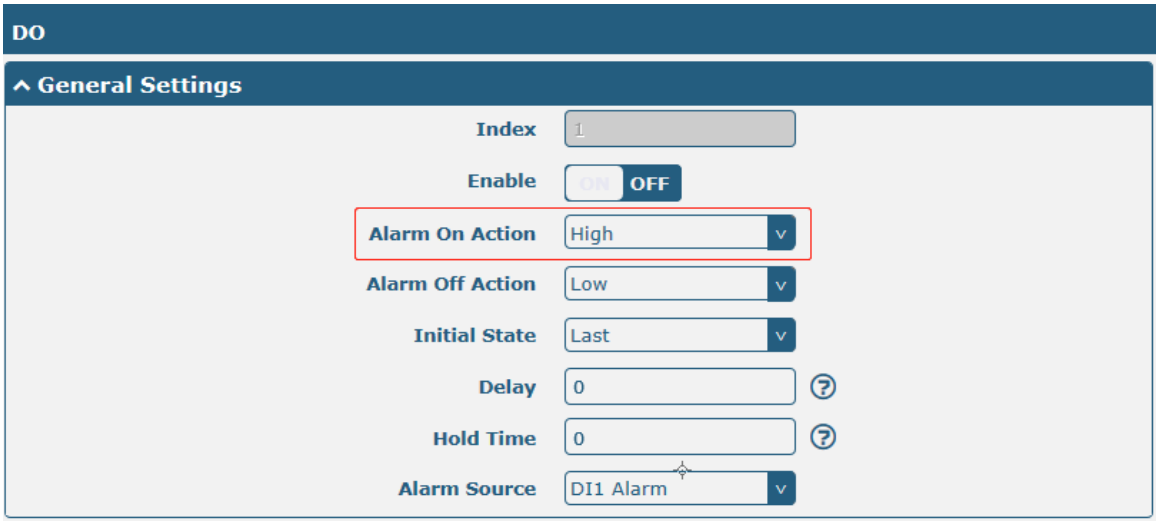
General Settings @ DI		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this DI.	OFF
Mode	Select from “ON-OFF” or “Counter”.	ON-OFF

General Settings @ DI		
Item	**Description**	**Default**
	• ON-OFF: DI interface support ON and OFF mode (high or low level electrical) trigger DI alarm. The mode default to ON, and OFF mode is available only when enabling the inversion feature ON—Under this mode, DI alarm status will be triggered to ON when DI interface open from GND or input a high level electrical (logic 1), on the contrary DI alarm status will be trigged to OFF when DI interface connect to GND or input a low level electrical (logic 0) OFF—Under this mode, DI alarm status will be triggered to ON when DI interface connect to GND or input a low level electrical (logic 0), on the contrary DI alarm status will be trigged to OFF when DI interface open from GND or input a high level electrical (logic 1) • Counter: Event counter mode	
Inversion	Click the toggle button to enable/disable this option. Enable to set DI mode as OFF mode.	OFF
Threshold Value	Set the threshold vale. It will trigger alarm when event counter reaches this figure. After triggering alarm, DI will keep counting but not trigger alarm again. Enter 0 to 65535 digits. (0=will not trigger alarm) **Note**: This option is only available when DI under the "Counter" mode.	Null
Alarm on Content	When alarm is on, show its content	Alarm On
Alarm off Content	When alarm is off, show its content.	Alarm Off

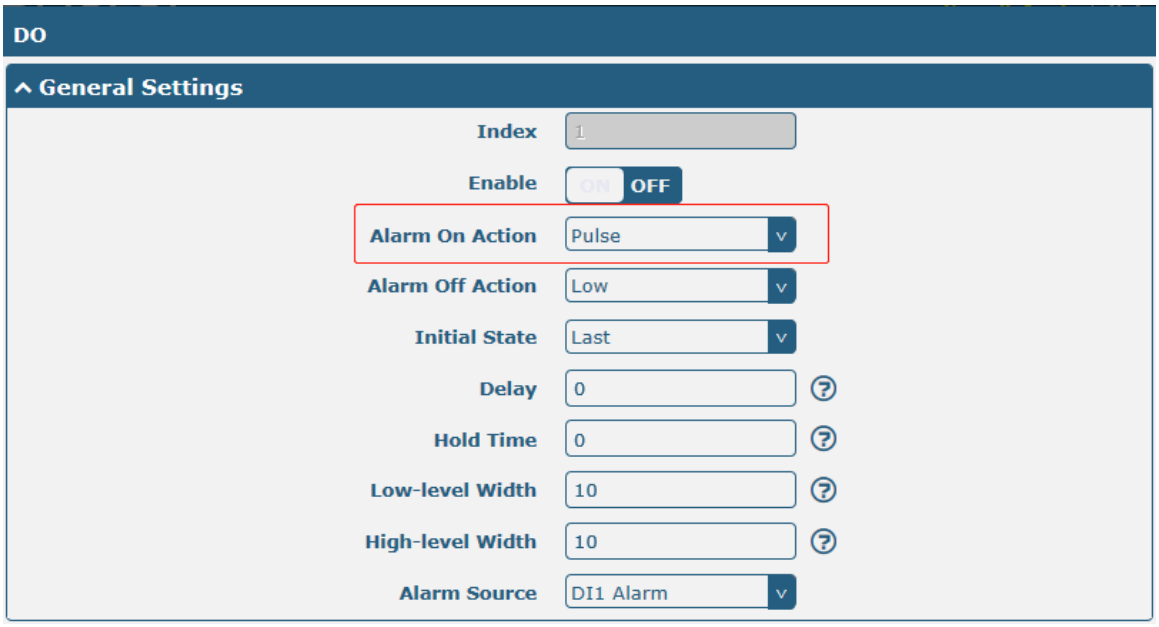
Note: It defaults as high alarm, while turns to low alarm after enabling the "Inversion" button.

DO

Click to enter the DO configuration window.



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



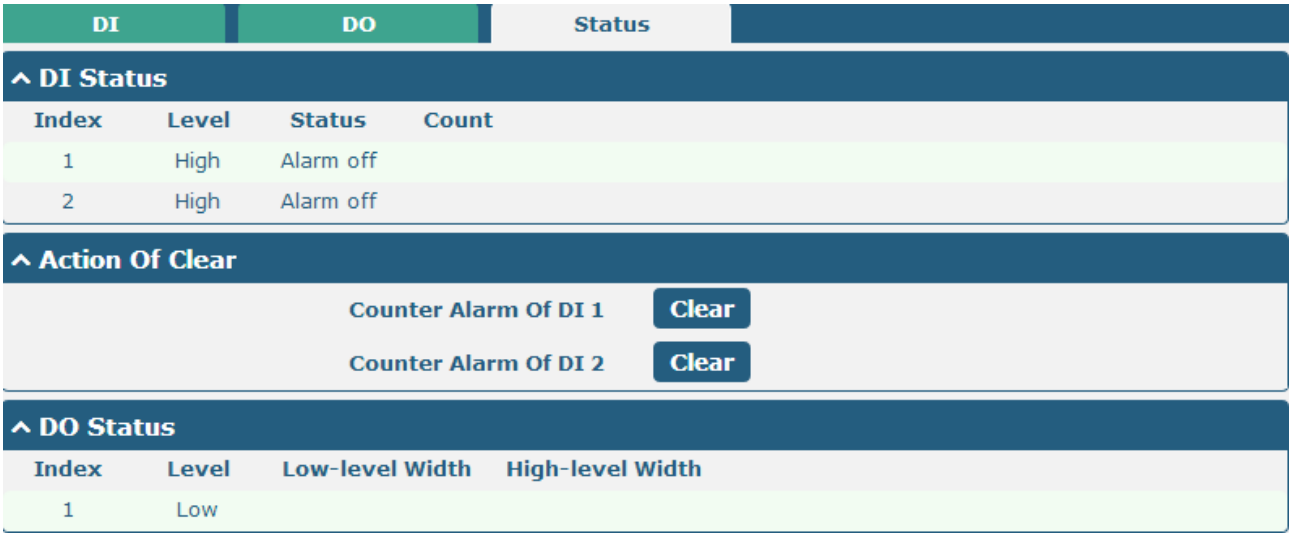
The window is displayed as below when choosing “Pulse” as the alarm off action.

General Settings @ DO		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this DO.	OFF
Alarm On Action	Digital Output initiates when there is an alarm. Selected from “High”, “Low” or “Pulse”. • High: a high electrical level output • Low: a low electrical level output • Pulse: Generates a square wave as specified in the pulse mode parameters when triggered	High

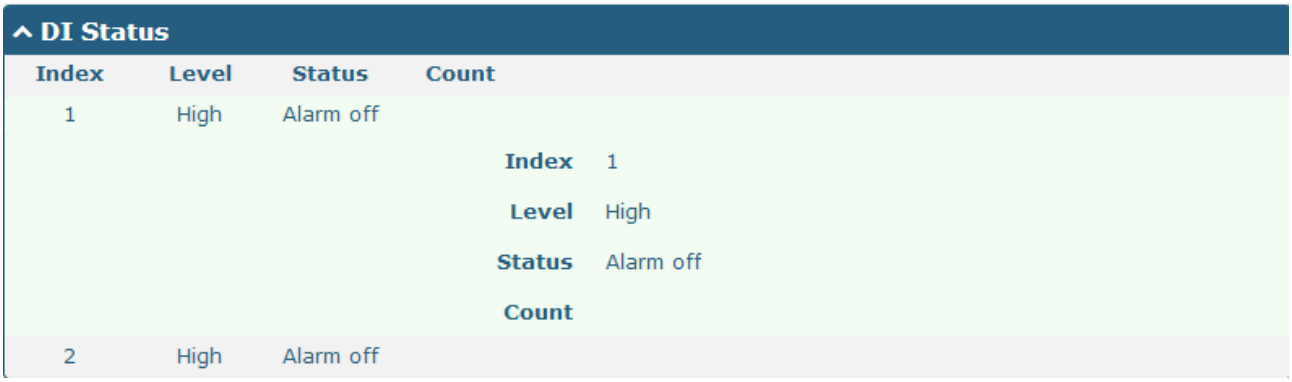
General Settings @ DO		
Item	**Description**	**Default**
Alarm Off Action	Digital Output initiates when alarm removed. Selected from “High”, “Low” or “Pulse”. • High: a high electrical level output • Low: a low electrical level output • Pulse: Generates a square wave as specified in the pulse mode parameters when triggered	Low
Initial State	Specify the Digital Output status when powered on. Selected from “Last”, “High” or “Low”. • Last: DO’s status will consist with the status of last power off • High: DO interface is in high electrical level • Low: DO interface is in low electrical level	Low
Delay	Set the delay time for DO alarm start-up. The first pulse will be generated after a “Delay”. Enter from 0 to 30000ms. (0=generate pulse without delay)	0
Hold Time	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reach this specified time, DO will stop the action. Enter from 0 to 255 seconds. (0=keep on until the next action)	0
Low-level Width	Set the low-level width. It is available when enabling Pulse as “Alarm On Action/Alarm Off Action”. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Enter from 1 to 300000 ms.	10
High-level Width	Set the high-level width. It is available when enabling Pulse as “Alarm On Action/Alarm Off Action”. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Enter from 1 to 300000 ms.	10
Alarm Source	Digital Output initiates according to different alarm source. Selected from “DI1 Alarm”, “DI2 Alarm”. DI1/DI2 Alarm: Digital Output triggers the related action when there is alarm from Digital Input.	DI1 Alarm

Status

This window allows you to view the status of DO and DI interfaces. It also can clear the counter alarm of DI in here. Click **Clear** button to clear DI1 or DI2 monthly usage statistics info for counter alarm.

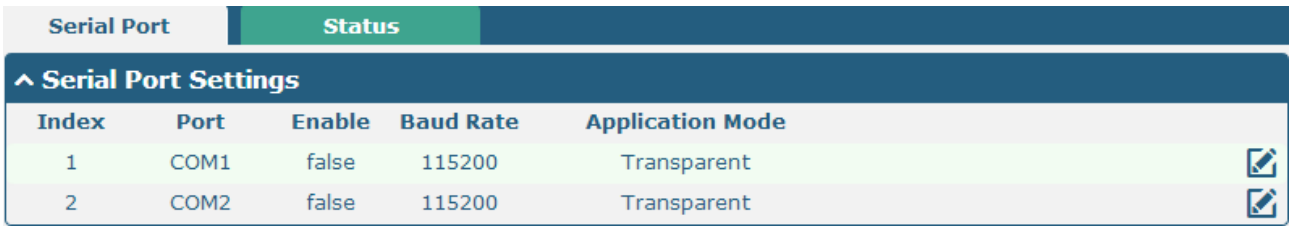


Click one row to view.

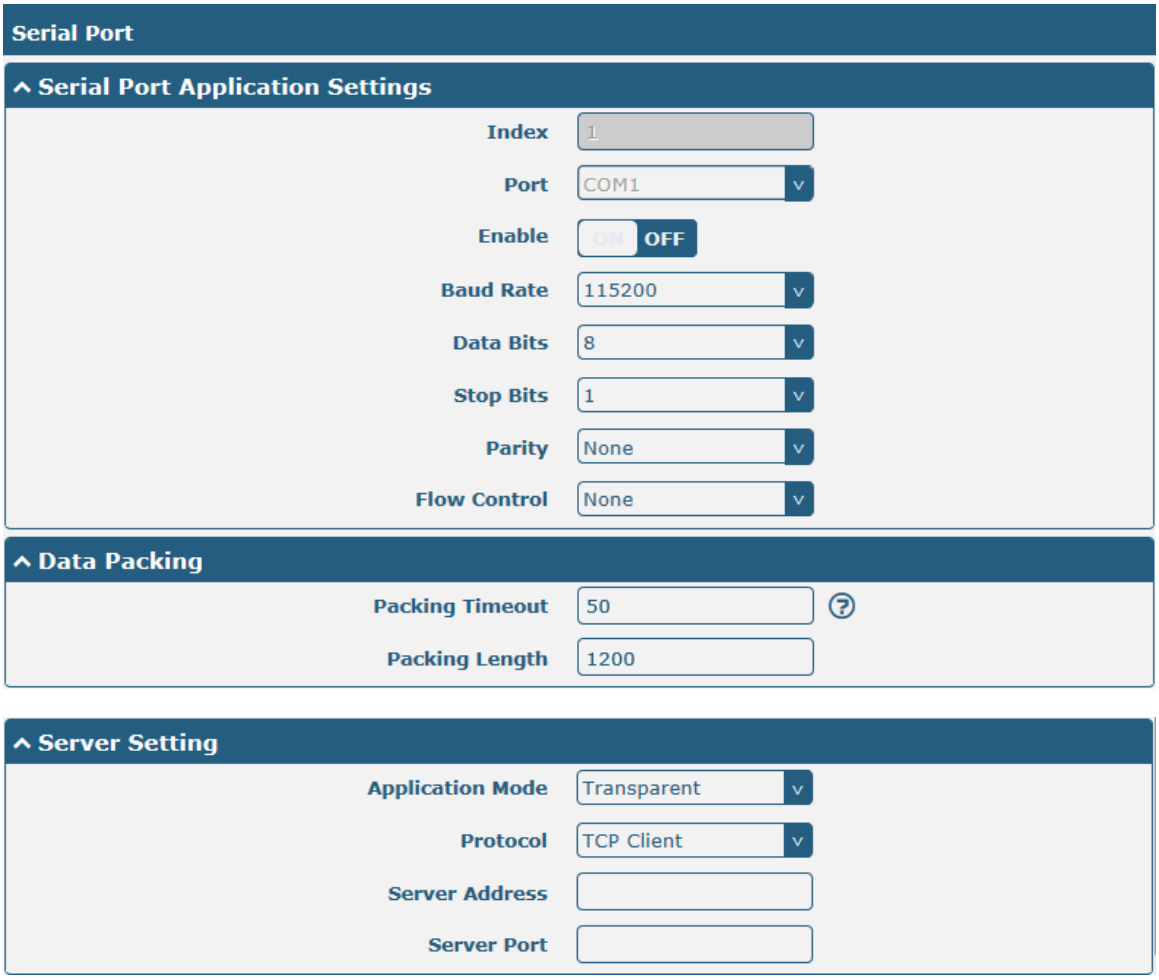


3.9 Interface > Serial Port

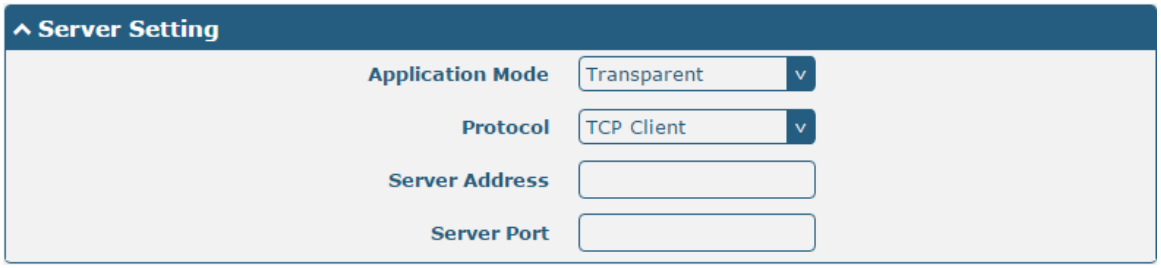
This section allows you to set the serial port parameters. M1200 supports one RS-232s and one RS-485. Serial port provides a way to transfer serial data to IP data, or vice versa, and transmit these data via wired or wireless network to achieve data transparent transmission.



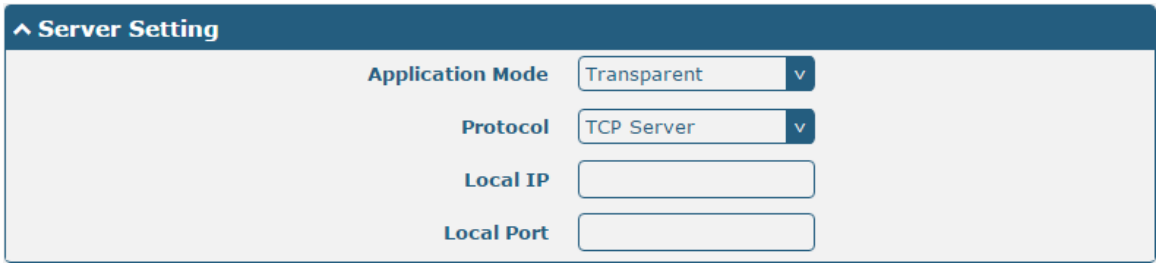
Click the edit button of COM1.



- The window is displayed as below when choosing “Transparent” as the application mode and “TCP Client” as the protocol.

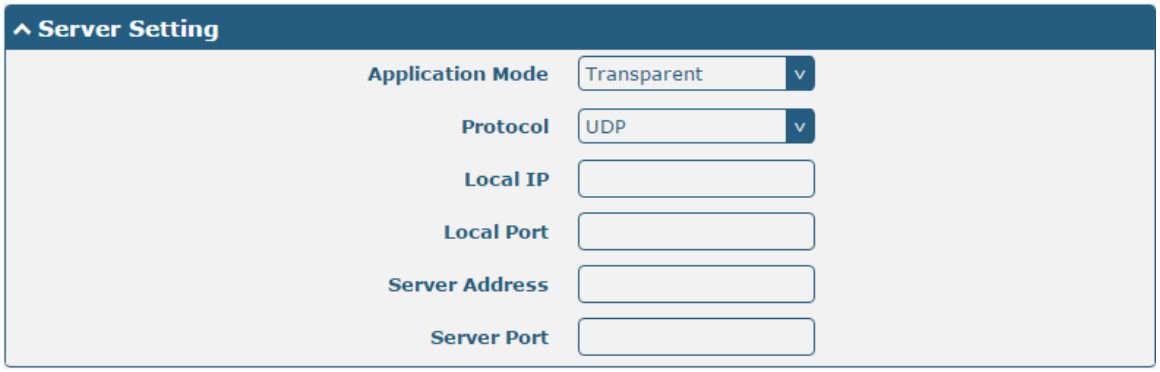


The window is displayed as below when choosing “Transparent” as the application mode and “TCP Server” as the protocol.

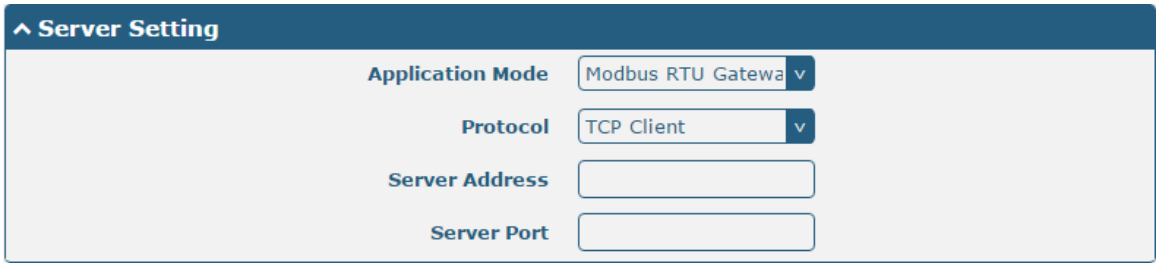


The window is displayed as below when choosing “Transparent” as the application mode and “UDP” as the

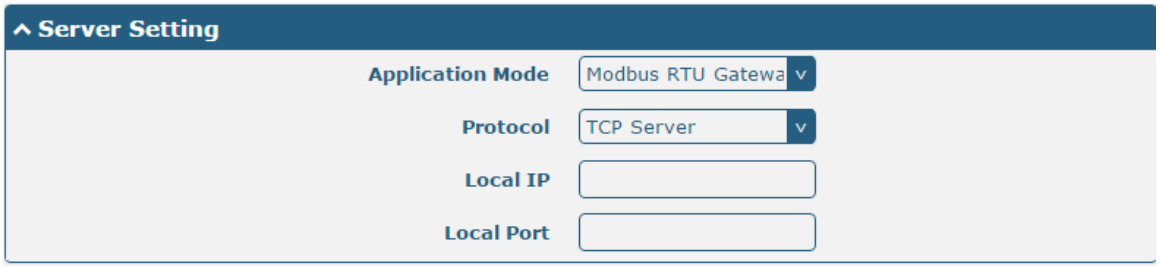
protocol.



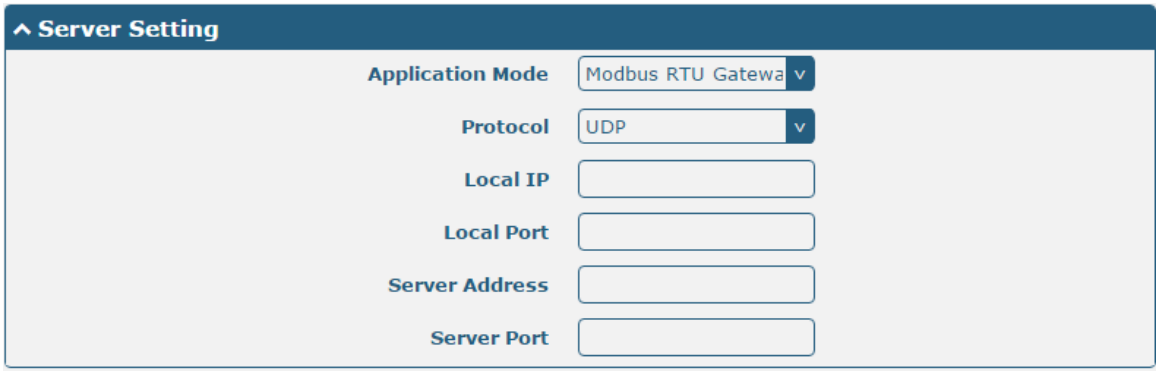
- The window is displayed as below when choosing “Modbus RTU Gateway” as the application mode and “TCP Client” as the protocol.



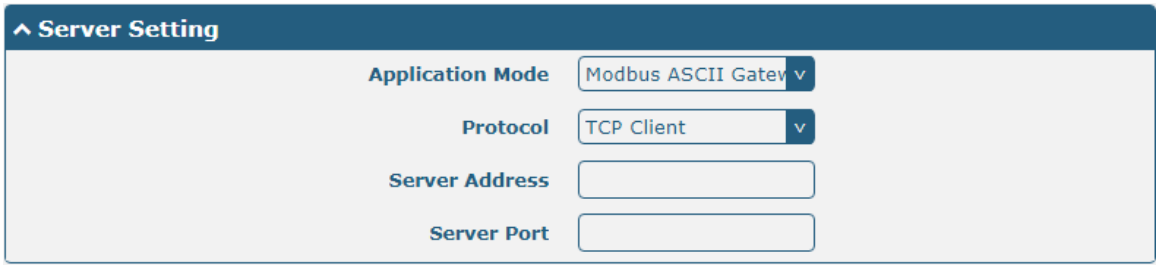
The window is displayed as below when choosing “Modbus RTU Gateway” as the application mode and “TCP Server” as the protocol.



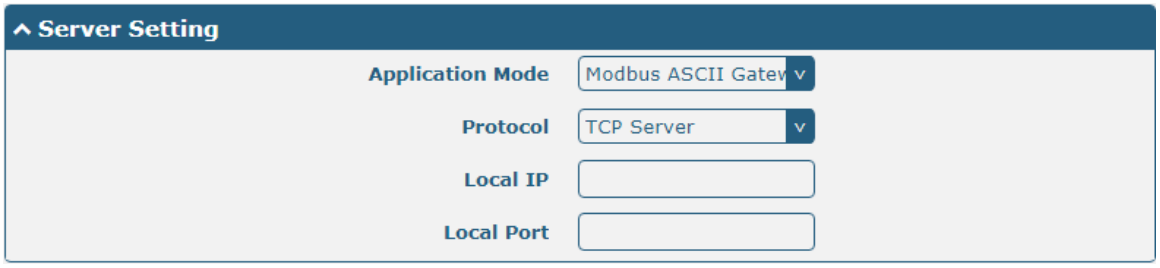
The window is displayed as below when choosing “Modbus RTU Gateway” as the application mode and “UDP” as the protocol.



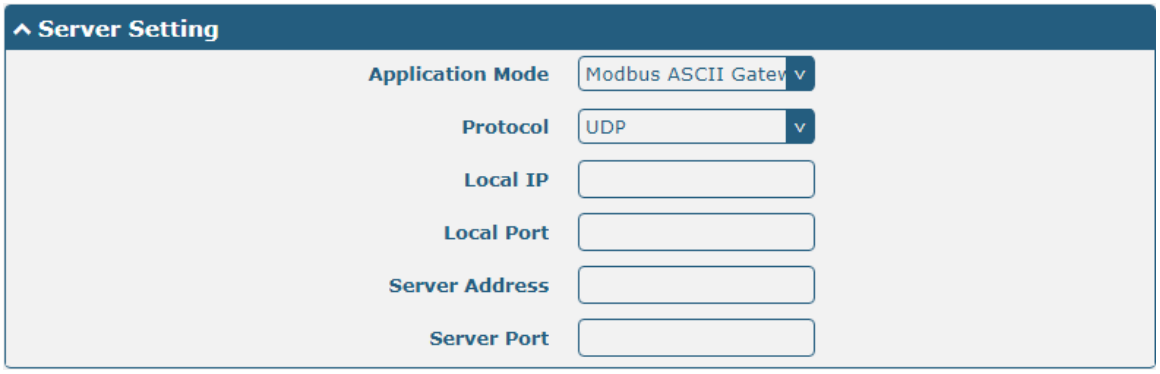
- The window is displayed as below when choosing “Modbus ASCII Gateway” as the application mode and “TCP Client” as the protocol.



The window is displayed as below when choosing “Modbus ASCII Gateway” as the application mode and “TCP Server” as the protocol.



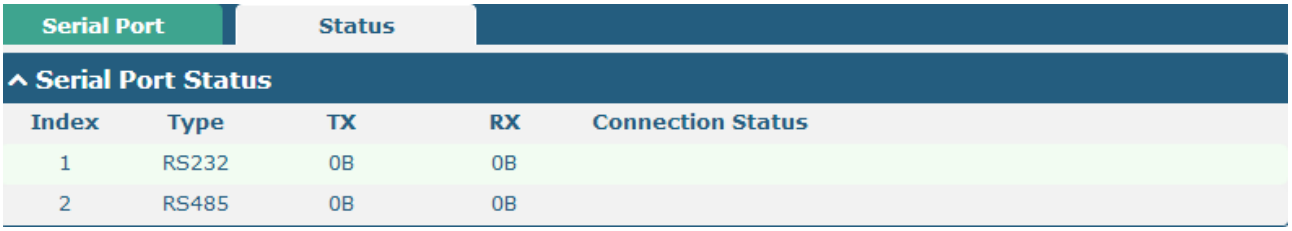
The window is displayed as below when choosing “Modbus ASCII Gateway” as the application mode and “UDP” as the protocol.



Serial Port		
Item	**Description**	**Default**
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
Port	Show the current serial’s name, read only.	--
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from “300”, “600”, “1200”, “2400”, “4800”, “9600”, “19200”, “38400”, “57600” , “115200” or “230400”.	115200
Data Bits	Select from “7” or “8”.	8
Stop Bits	Select from “1” or “2”.	1
Parity	Select from “None”, “Odd” or “Even”.	None
Data Packing		
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN	50

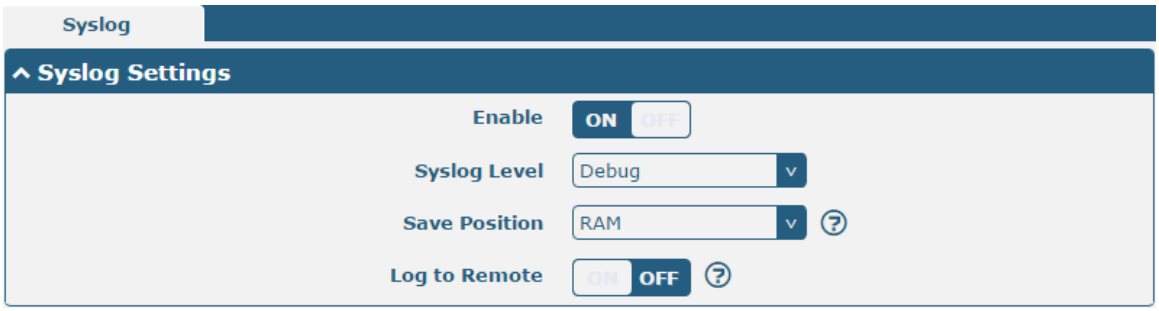
Serial Port		
Item	**Description**	**Default**
	when it reaches the Interval Timeout in the field. **Note**: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	1200
Server Setting		
Application Mode	Select from "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway". • Transparent: gateway will transmit the serial data transparently • Modbus RTU Gateway: gateway will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa • Modbus ASCII Gateway: gateway will translate the Modbus ASCII data to Modbus TCP data and sent out, and vice versa	Transparent
Protocol	Select from "TCP Client", "TCP Server" or "UDP". • TCP Client: Gateway works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name • TCP Server: Gateway works as TCP server, listening for connection request from TCP client • UDP: Gateway works as UDP client	TCP Client
Server Address	Enter the address of server which will receive the data sent from gateway's serial port. IP address or domain name will be available.	Null
Server Port	Enter the specified port of server which is used for receiving the serial data.	Null
Local IP	Enter the IP of TCP or UDP.	Null
Local Port	Enter the port of TCP or UDP.	Null

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

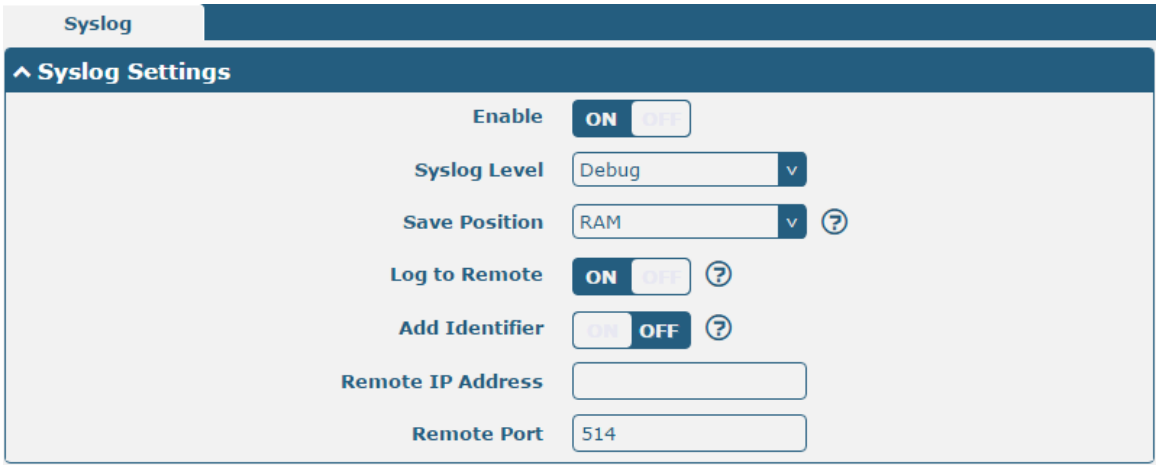


3.10 Services > Syslog

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



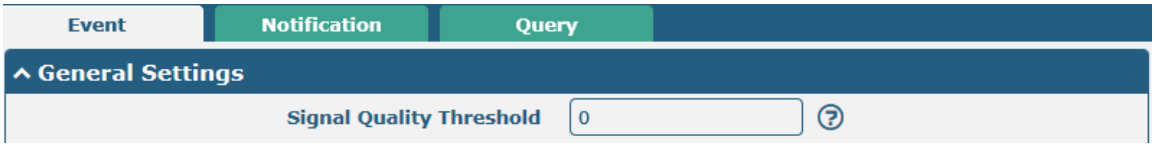
The window is displayed as below when enabling the “Log to Remote” option.



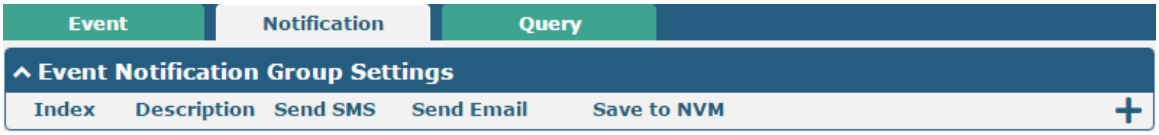
Syslog Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Syslog settings option.	OFF
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. **Note:** The lower level will output more syslog in details.	Debug
Save Position	Select the save position from “RAM”, “NVM” or “Console”. Choose “RAM”. The data will be cleared after reboot. **Note**: It's not recommended that you save syslog to NVM for a long time.	RAM
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow gateway sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	OFF
Remote IP Address	Enter the IP address of syslog server when enabling the “Log to Remote” option.	Null
Remote Port	Enter the port of syslog server when enabling the “Log to Remote” option.	514

3.11 Services > Event

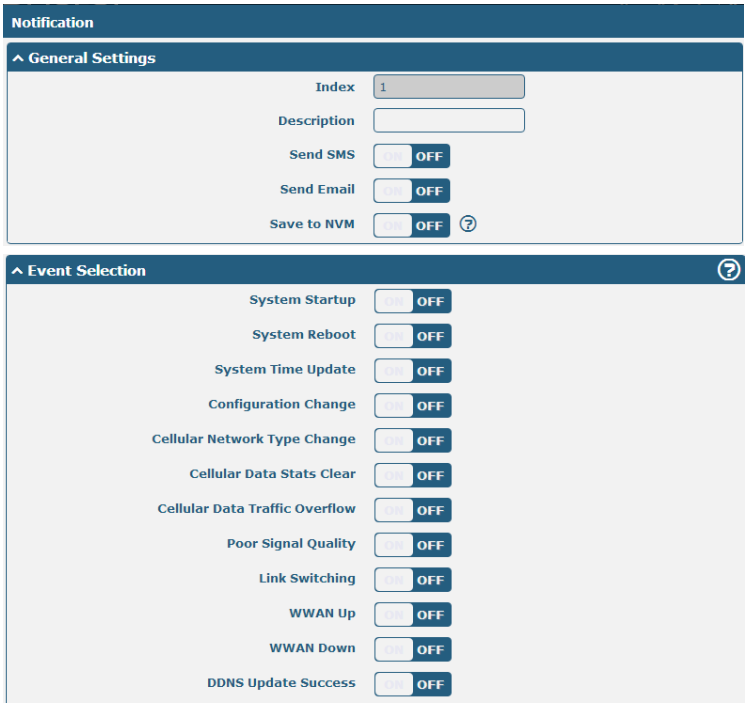
This section allows you to set the event parameters. Event feature provides an ability to send alerts by SMS or Email when certain system events occur.

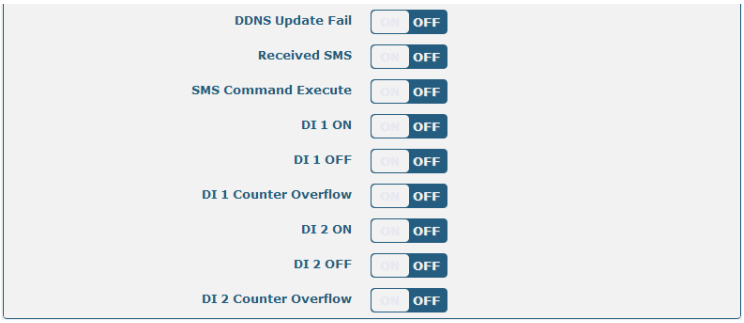


General Settings @ Event		
Item	**Description**	**Default**
Signal Quality Threshold	Set the threshold for signal quality. Gateway will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0



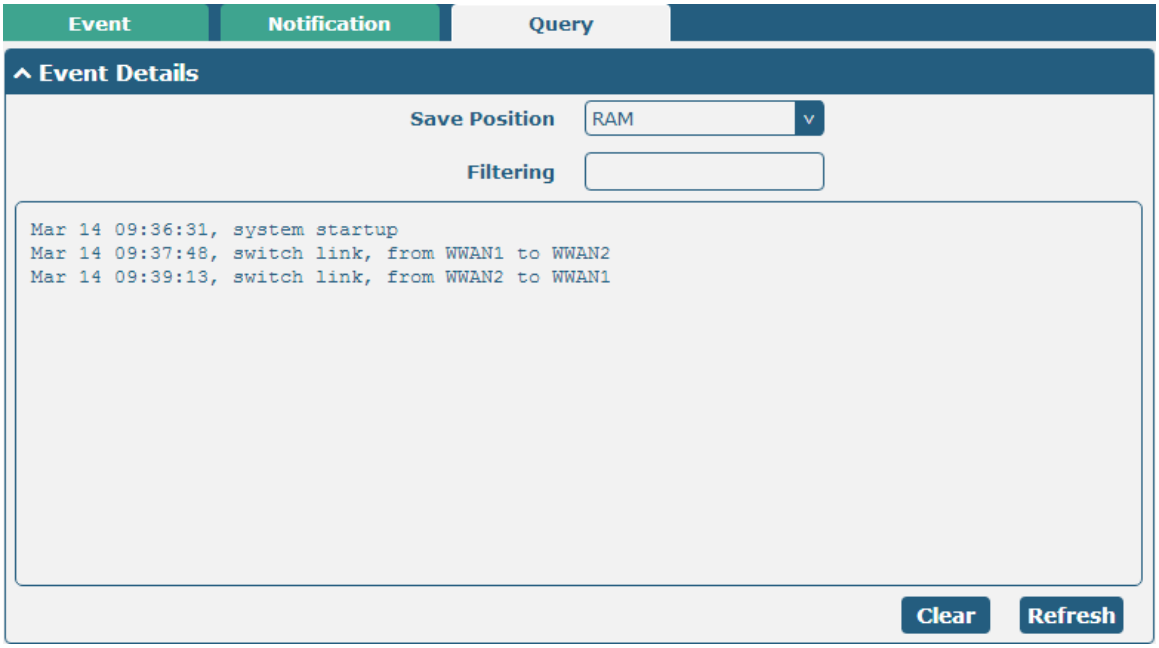
Click + button to add an Event parameters.





General Settings @ Notification		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the gateway will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in "3.14 Services > Email", and use ';'to separate each number.	OFF
Phone Number	Enter the phone numbers used for receiving event notification. Use a semicolon (;) to separate each number.	Null
Send Email	Click the toggle button to enable/disable this option. When enabled, the gateway will send notification to the specified email box via Email if event occurs. Set the related email address in "3.14 Services > Email".	OFF
Email Address	Enter the email addresses used for receiving event notification. Use a space to separate each address.	Null
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

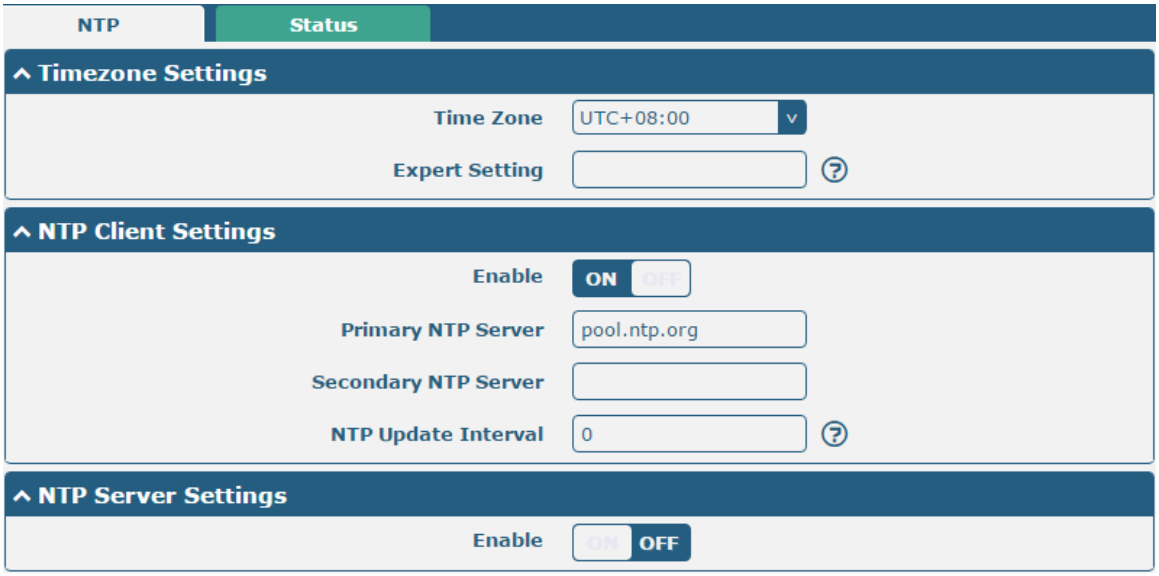
In the following window you can query various types of events record. Click **Refresh** to query filtered events while click **Clear** to clear the event records in the window.



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

3.12 Services > NTP

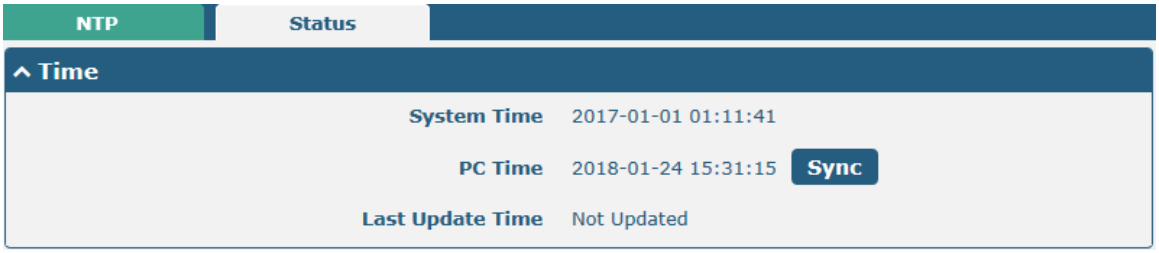
This section allows you to set the related NTP (Network Time Protocol) parameters, including Time zone, NTP Client and NTP Server.



NTP		
Item	**Description**	**Default**
Timezone Settings		
Time Zone	Click the drop down list to select the time zone you are in.	UTC +08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
NTP Client Settings		
Enable	Click the toggle button to enable/disable this option. Enable to synchronize time with the NTP server.	ON
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null
NTP Update interval	Enter the interval (minutes) synchronizing the NTP client time with the NTP server's. Minutes wait for next update, and 0 means update only once.	0
NTP Server Settings		

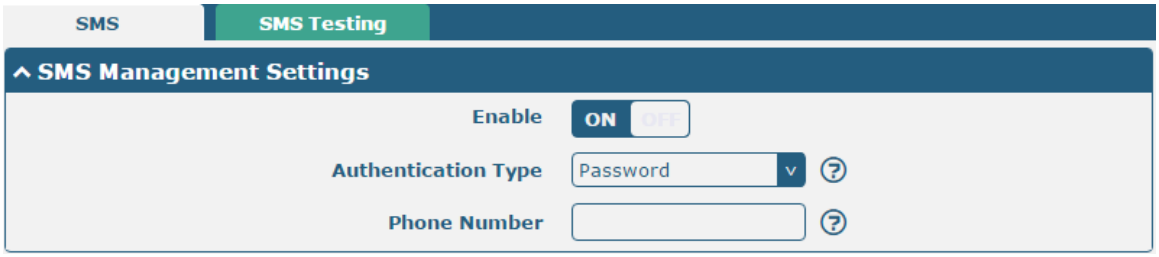
Enable	Click the toggle button to enable/disable the NTP server option.	OFF

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



3.13 Services > SMS

This section allows you to set SMS parameters. Gateway supports SMS management, and user can control and configure their gateways by sending SMS.



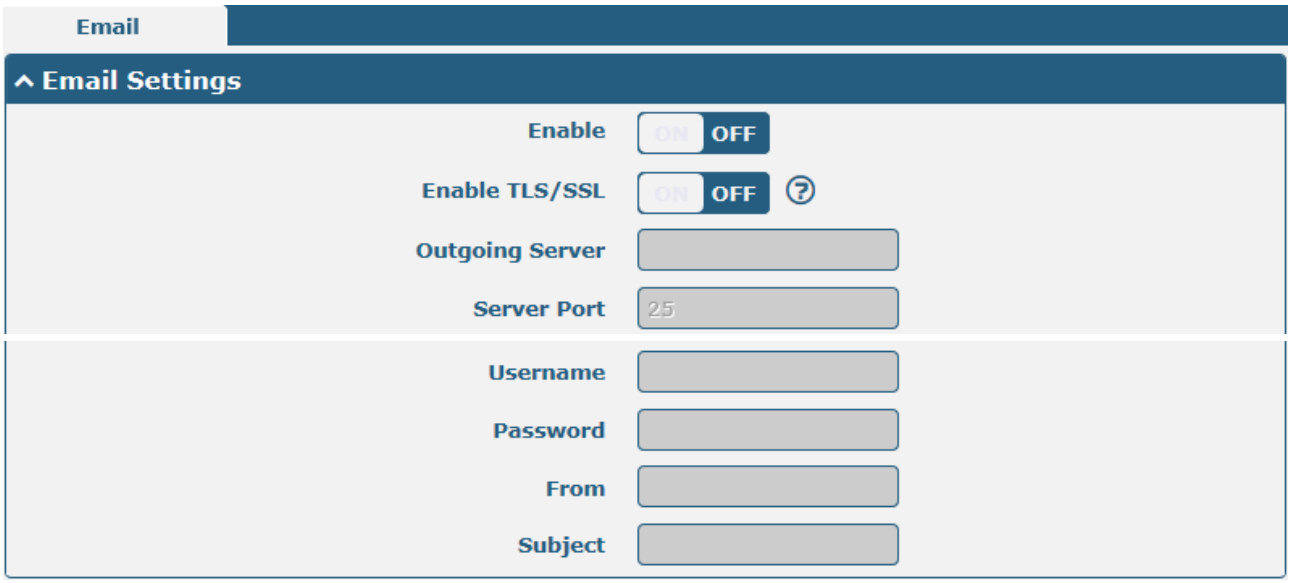
SMS Management Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the SMS Management option. **Note**: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from "Password", "Phonenum" or "Both". • Password: Use the same username and password as WEB manager for authentication. For example, the format of the SMS should be "username: password; cmd1; cmd2; …" **Note:** Set the WEB manager password in **System > User Management** section. • Phonenum: Use the Phone number for authentication, and user should set the Phone Number that is allowed for SMS management. The format of the SMS should be "cmd1; cmd2; …" • Both: Use both the "Password" and "Phonenum" for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be "username: password; cmd1; cmd2; …"	Password
Phone Number	Set the phone number used for SMS management, and use '; 'to separate each number. **Note**: It can be null when choose "Password" as the authentication type.	Null

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

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

3.14 Services > Email

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

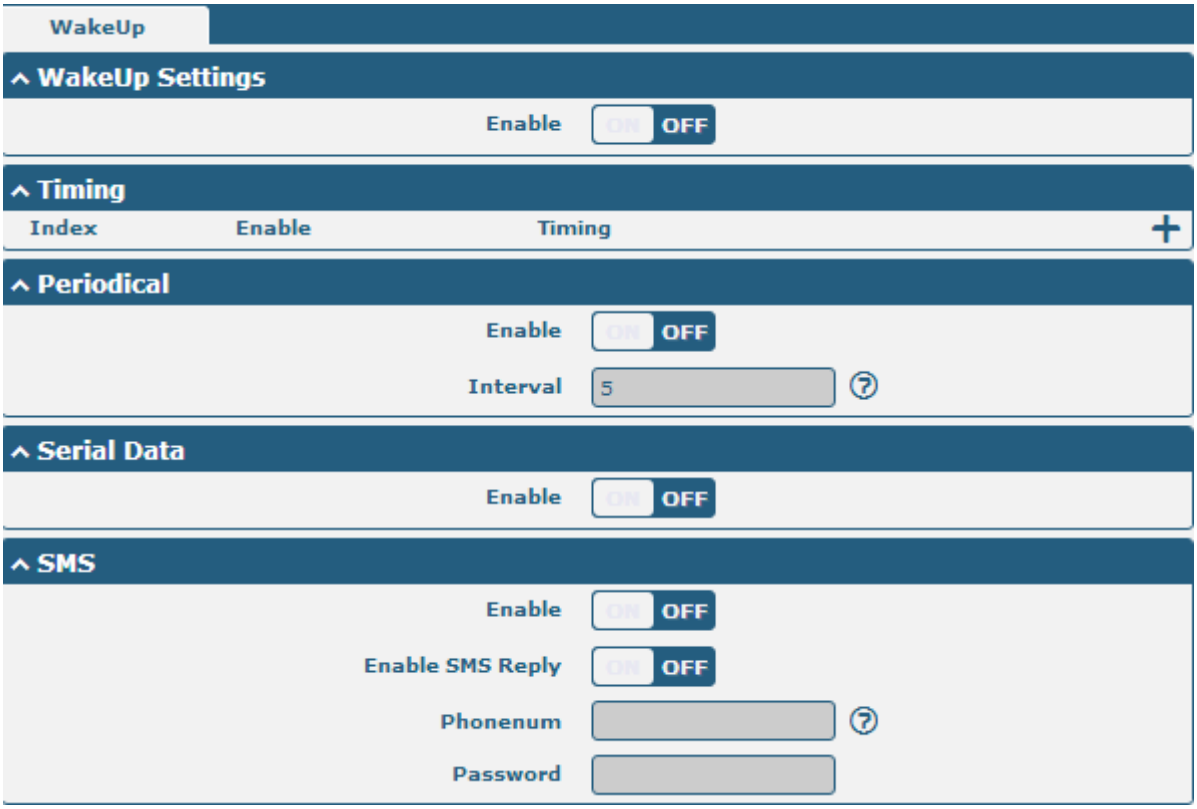


Email Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null

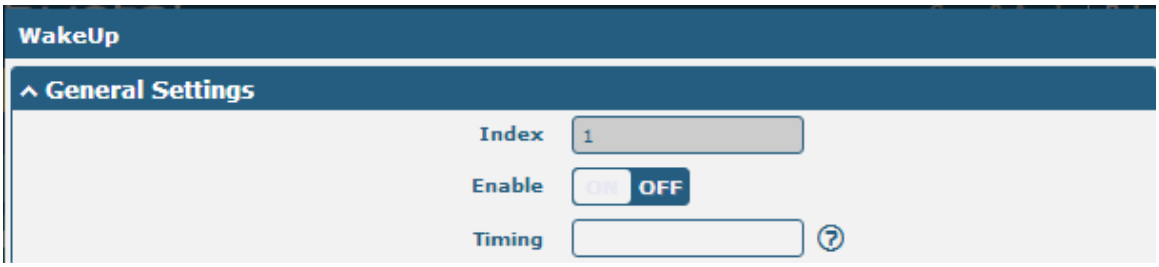
Email Settings		
Item	**Description**	**Default**
Server port	Enter the SMTP server port.	25
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

3.15 Services > WakeUp

Gateway supports a variety of wake-up dialing policies, including regular wake-up, interval wake-up, serial data wake-up, and SMS wake-up. Here, users can set different wake-up policies.



Click on the right side + of the Timing to add a wake-up time point. Up to 3 can be added.

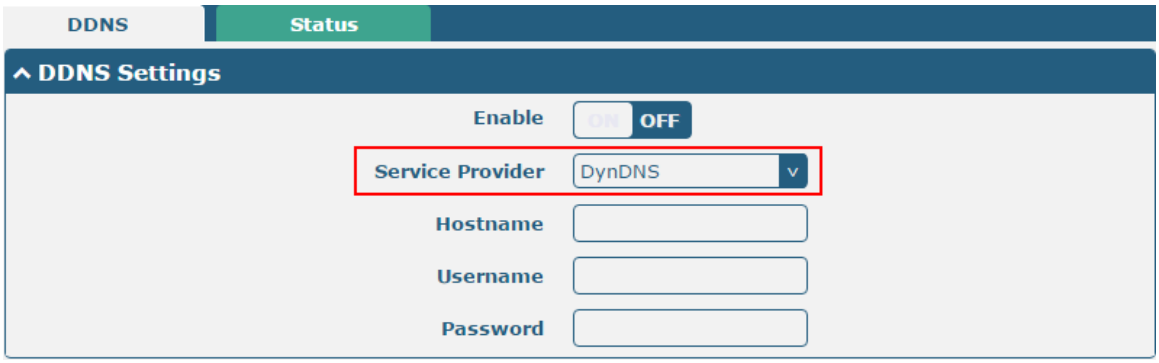


WakeUp		
Item	**Description**	**Default**

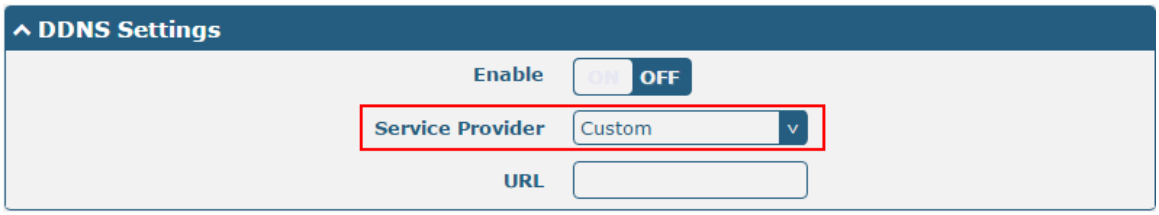
WakeUp		
Item	**Description**	**Default**
General Settings		
Enable	Click the toggle button to enable/disable this option. When it is set to ON, the current link is disconnected, while set to OFF, the device restarts GPRS dial-up.	OFF
Timing General Settings		
Index	Display number.	--
Enable	Click the toggle button to enable/disable this option. When it is set to ON, the gateway make GPRS dial-up on the set timing.	OFF
Timing	Every day at the timing (HH:MM) the gateway makes GPRS dial-up.	Null
Periodical		
Periodical WakeUp	Click the toggle button to enable/disable this option. When it is set to ON, the gateway will periodically make GPRS dial-up.	OFF
Interval	Set the interval time for Periodical WakeUp, ranging 3-720 min.。	5
Serial Data		
Serial Data WakeUp	Click the toggle button to enable/disable this option. When it is set to ON, while sending data to the serial port, the gateway make GPRS dial-up.	OFF
SMS		
SMS WakeUp	Click the toggle button to enable/disable this option. When it is set to ON, while gateway receives SMS from the set phone number, the gateway make GPRS dial-up.	OFF
Enable SMS Reply	Click the toggle button to enable/disable this option. When it is set to ON, while the gateway makes GPRS dial-up via SMS WakeUp, it will send a reply message to the WakeUp phone number.	OFF
Phonenum	The phone number which is allowed to wake up the gateway, separated each number by a ';' character.	Null
Password	The phone number needs to send the password to the gateway. If the sent content and the set password do not match, the GPRS dial-up cannot be performed.	Null

3.16 Services > DDNS

This section allows you to set the DDNS parameters. The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows you whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WWAN IP address of the gateway, which is assigned to you by your ISP. The service provider defaults to “DynDNS”, as shown below.

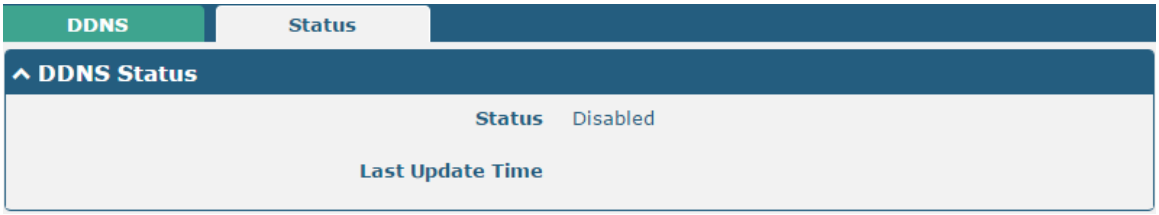


When “Custom” service provider chosen, the window is displayed as below.



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

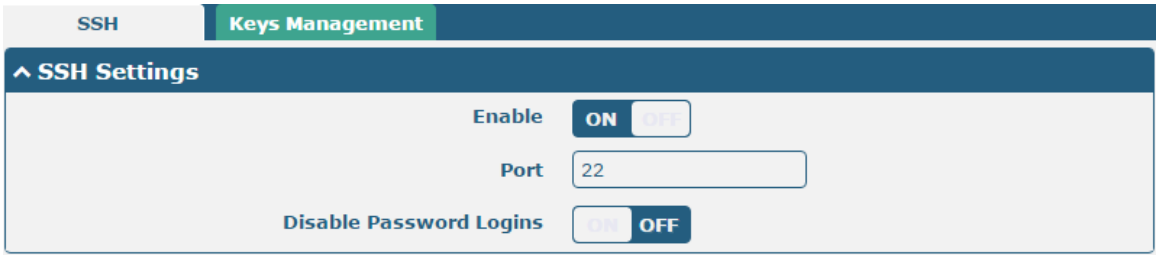
Click “Status” bar to view the status of the DDNS.



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

3.17 Services > SSH

Gateway supports SSH password access and secret-key access.

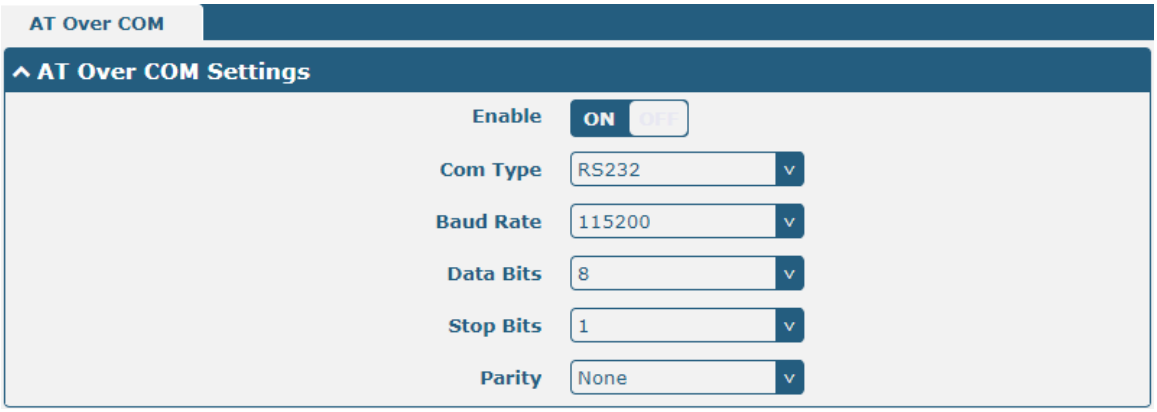


SSH Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable this option. When enabled, you can access the gateway via SSH.	ON
Port	Set the port of the SSH access.	22
Disable Password Logins	Click the toggle button to enable/disable this option. When enabled, you cannot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

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

3.18 Service > AT Over COM

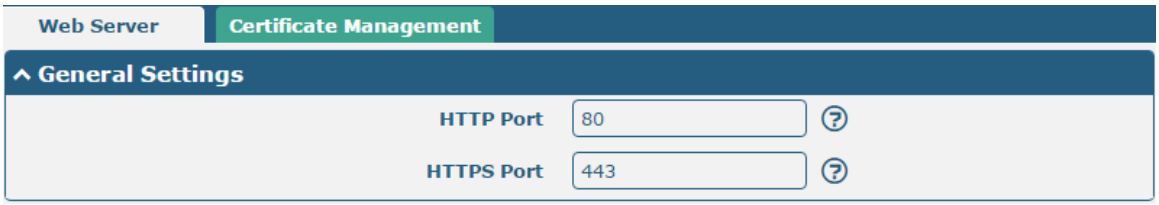
This part is used for setting parameters in AT Over COM.



Settings of AT Over COM		
Items	**Description**	**Default**
Enable	Click switch button to enable/disable the AT Over COM function.	OFF
Com Type	Select between “RS232” and “RS485”.	RS232
Baud Rate	Select among “300”, “600”, “1200”, “2400”, “4800”, “9600”, “19200”, “38400”, “57600”, “115200” and “230400”.	115200
Data Bits	Select between “7” and “8”.	8
Stop Bits	Select between “1” and “2”.	1
Parity	Select among “None”, “Odd Parity” and “Even Parity”.	None

3.19 Services > Web Server

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



General Settings @ Web Server		
Item	**Description**	**Default**
HTTP Port	Enter the HTTP port number you want to change in gateway’s Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the gateway with other HTTP Port	80

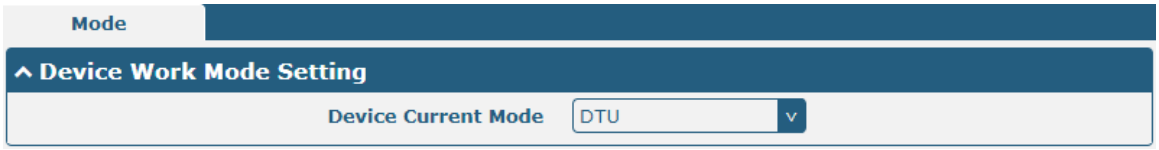
	number except 80, only adding that port number then you can login gateway's Web Server.	
HTTPS Port	Enter the HTTPS port number you want to change in gateway's Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the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

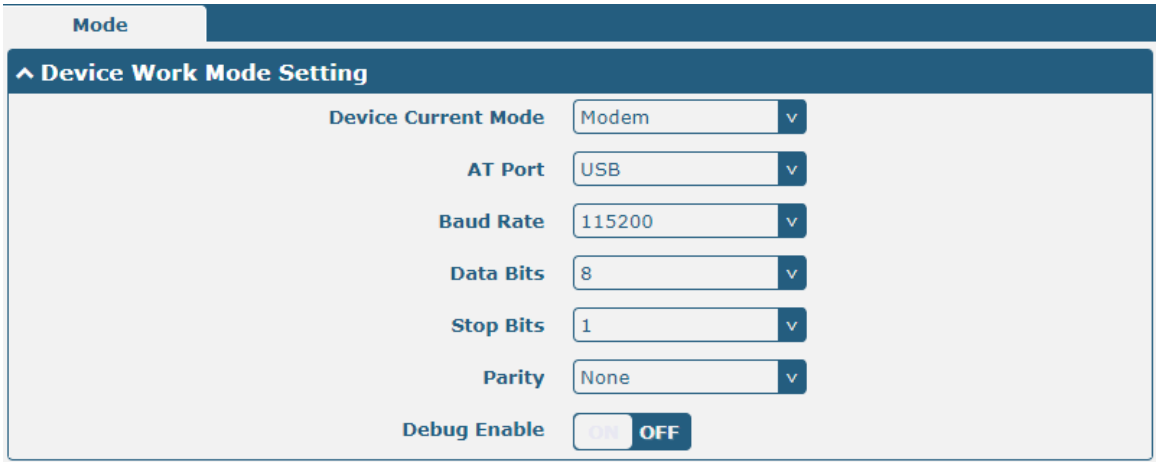
This section allows you to import the certificate file into the gateway.

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

3.20 Service > Work Mode

This part is used for setting work mode, including DTU and Modem.

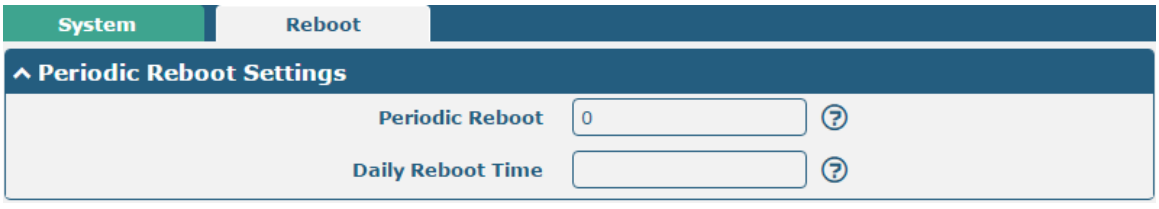




Settings of Work Mode		
Items	**Description**	**Default**
Device Current Mode	Select between “DTU” and “Modem”.	DTU
AT Port	Select between “USB”, “RS232” and “RS485”. • USB: dial through USB, and configure CLI through RS232 • RS232: dial through RS232, configure CLI through USB • RS485: dial through RS485, configure CLI through RS232	USB
Baud Rate	Select between “300”, “600”, “1200”, “2400”, “4800”, “9600”, “19200”, “38400”, “57600”, “115200” and “230400”.	115200
Data Bits	Select between “7” and “8”.	8
Stop Bits	Select between “1” and “2”.	1
Parity	Select among “None”, “Odd Parity” and “Even Parity”.	None
Debug Enable	Click switch button to enable/disable logs.	OFF

3.21 Services > Advanced

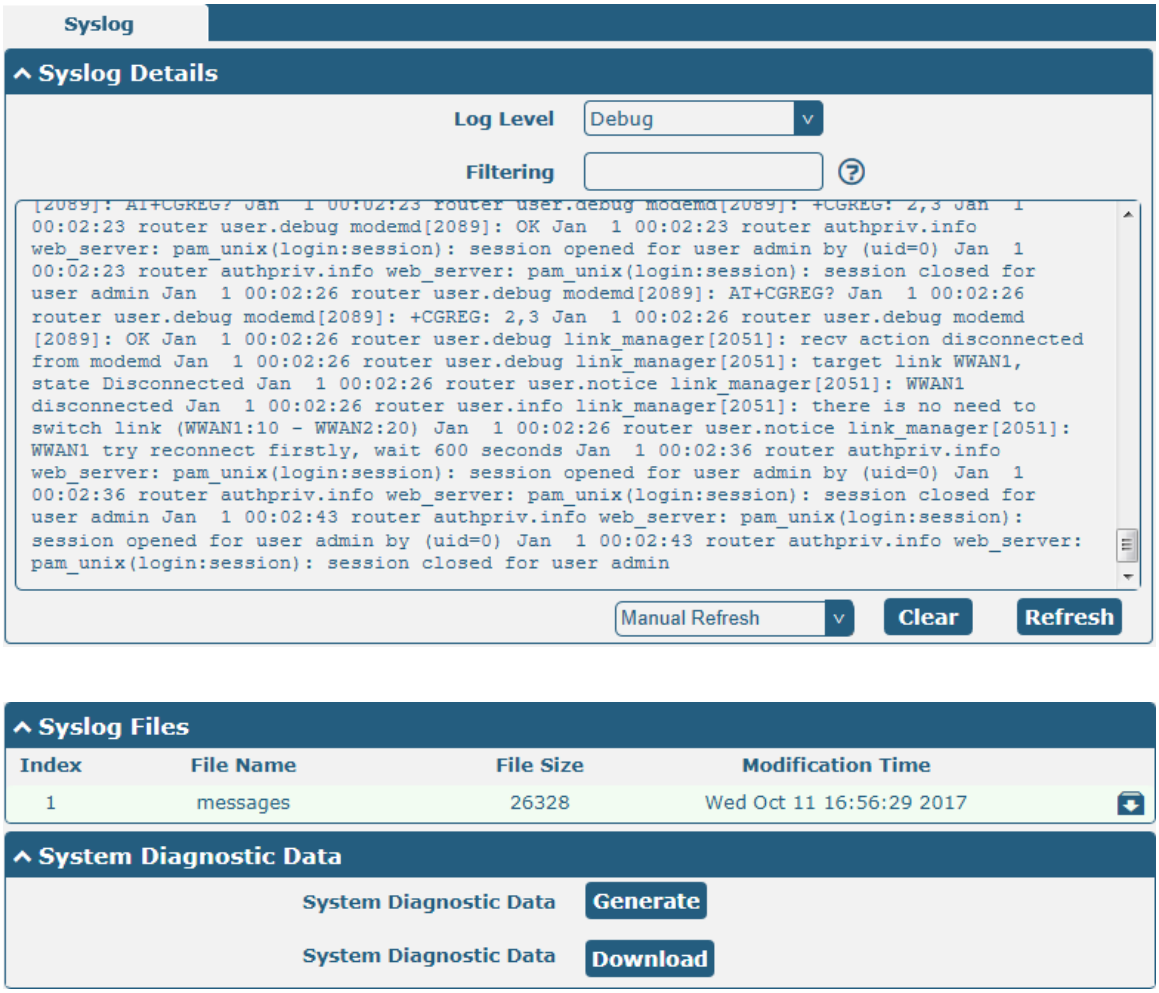
This section allows you to set the reboot.



Periodic Reboot Settings		
Item	**Description**	**Default**
Periodic Reboot	Set the reboot period of the gateway by every X hours. 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the gateway. You should follow the format as HH: MM, in 24h time frame. Leave it empty means disable.	Null

3.22 System > Debug

This section allows you to check and download the syslog details.



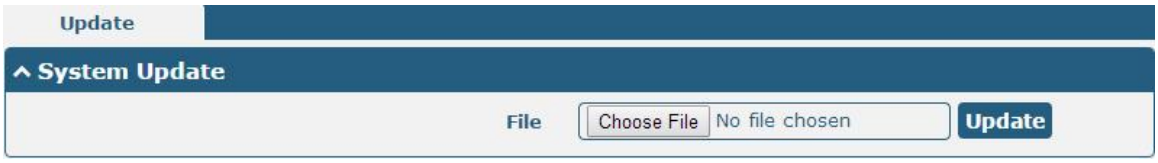
Syslog		
Item	**Description**	**Default**
Syslog Details		
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, “Error” which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Enter the filtering message based on the keywords. Use “&” to separate more than one filter message, such as “keyword1&keyword2”.	Null
Refresh	Select from “Manual Refresh”, “5 Seconds”, “10 Seconds”, “20 Seconds” or “30 Seconds”. You can select these intervals to refresh the log information displayed in the follow box. If selecting “manual refresh”, you should click the refresh button to refresh the syslog.	Manual Refresh
Clear	Click the button to clear the syslog.	--
Refresh	Click the button to refresh the syslog.	--
Syslog Files		
Syslog Files List	It can show at most 5 syslog files in the list, the files’ name range from message0 to message 4. And the newest syslog file will be placed on the top of the list.	--

System Diagnosing Data		
Generate	Click to generate the syslog diagnosing file.	--
Download	Click to download system diagnosing file.	--

3.23 System > Update

This section allows you to upgrade the firmware of your gateway. Click **System > Update > System Update**, and click on "Choose File" to locate the firmware file to be used for the upgrade. Once the latest firmware has been chosen, click "Update" to start the upgrade process. The upgrade process may take several minutes. Do not turn off your gateway during the firmware upgrade process.

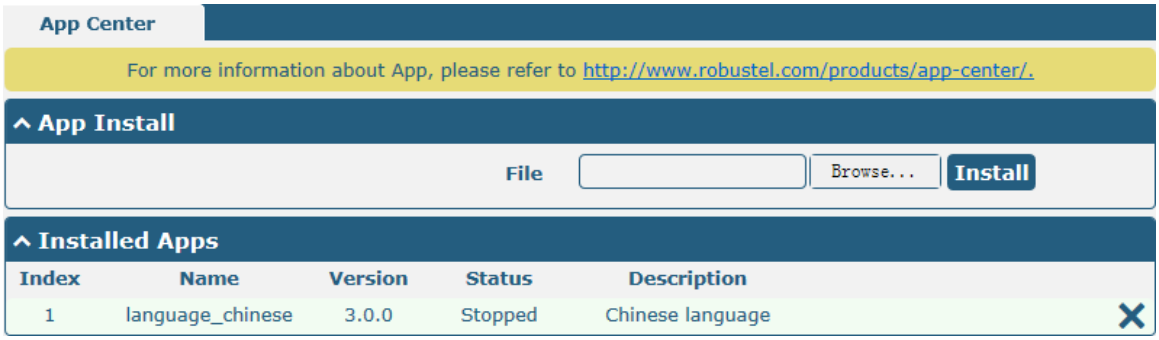
Note: To access the latest firmware file, please contact your technical support engineer.



3.24 System > App Center

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

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

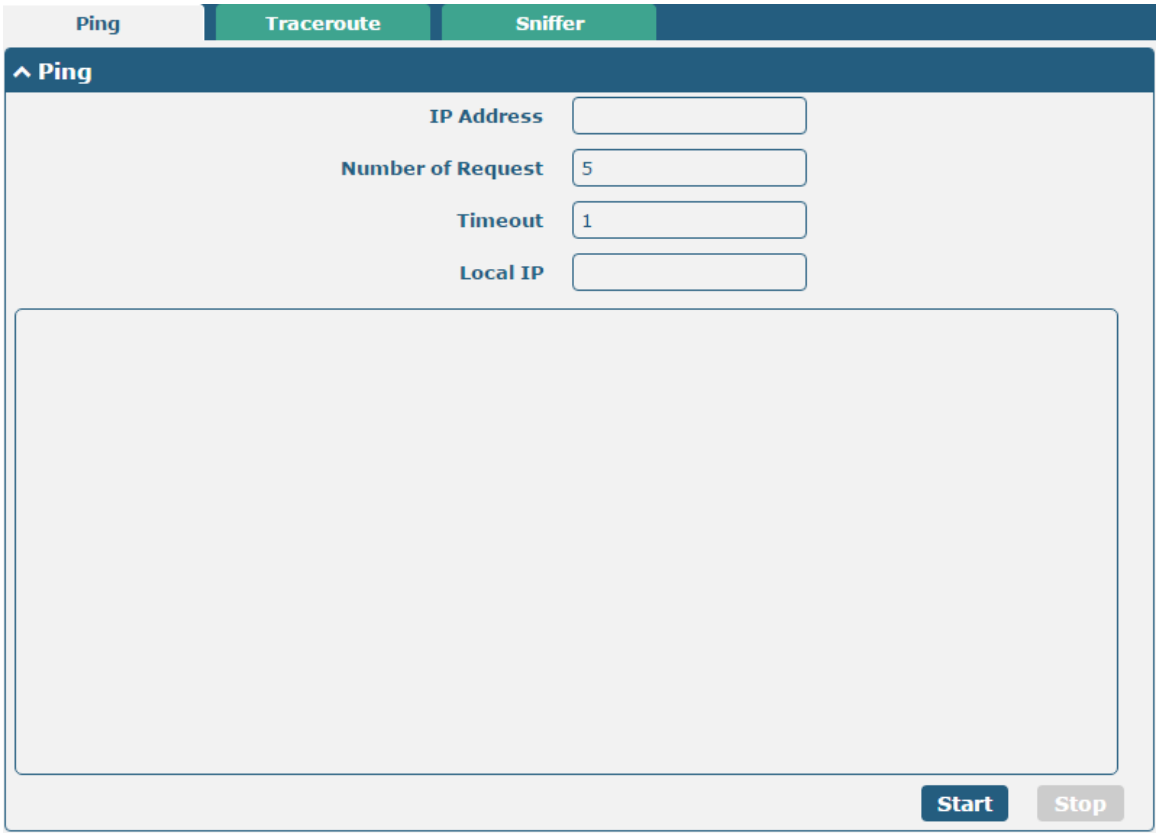


App Center		
Item	**Description**	**Default**
App Install		
File	Click on "Choose File" to locate the App file from your computer, and then click Install to import this file into your gateway. **Note**: File format should be *xxx.rpk*, e.g. *M1200-robustlink-1.0.0.rpk*.	--
Installed Apps		
Index	Indicate the ordinal of the list.	--

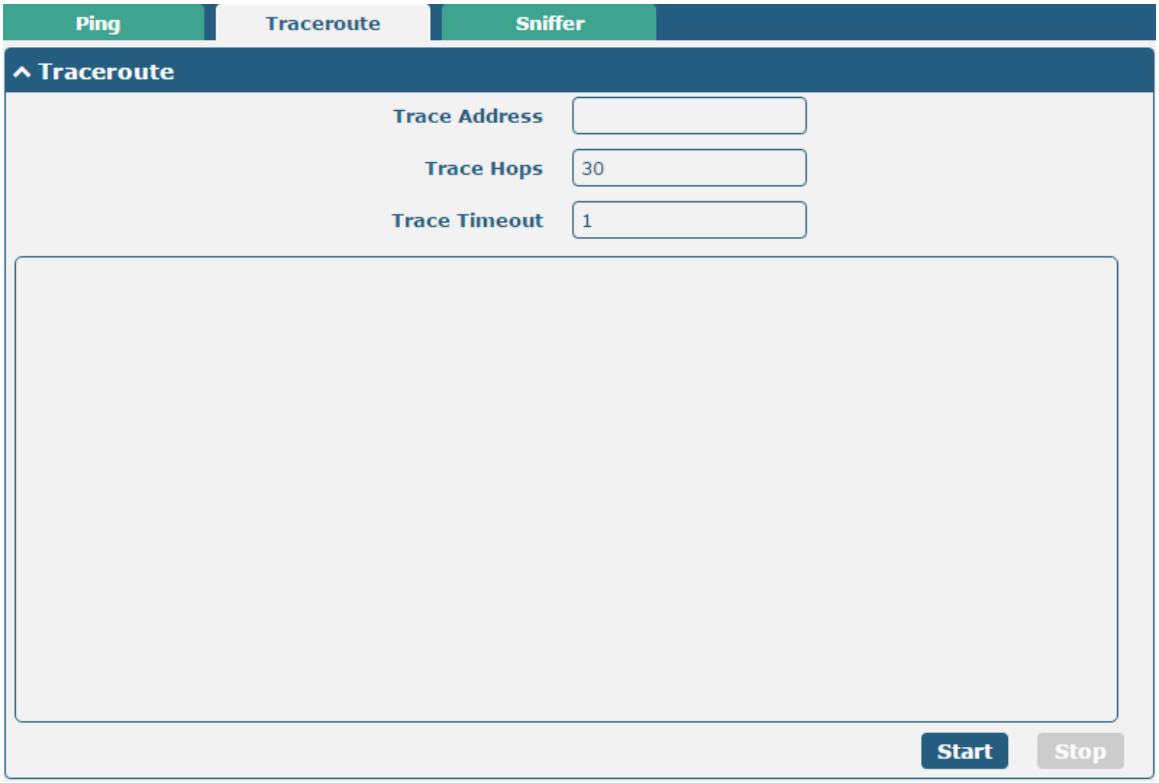
App Center		
Item	**Description**	**Default**
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

3.25 System > Tools

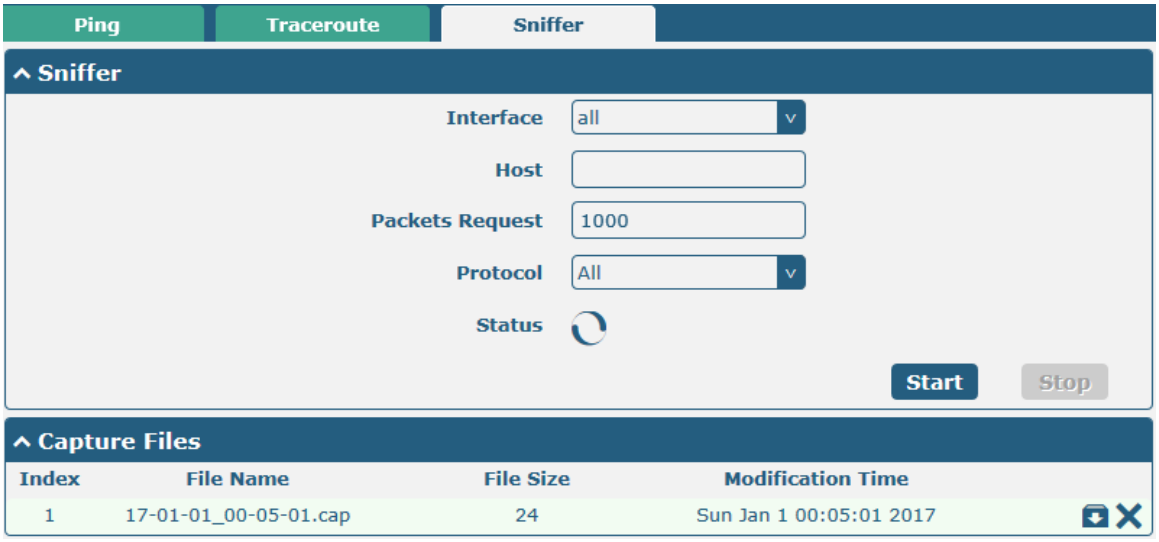
This section provides users three tools: Ping, Traceroute and Sniffer.



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



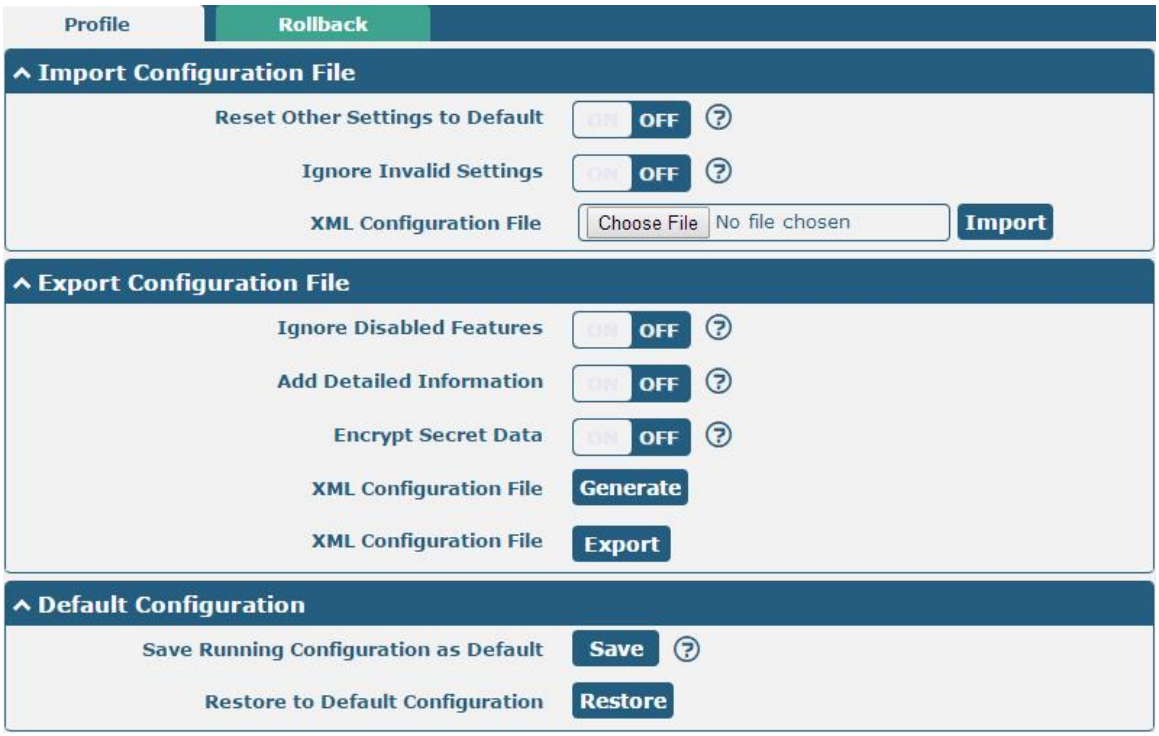
Traceroute		
Item	**Description**	**Default**
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. gateway will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify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



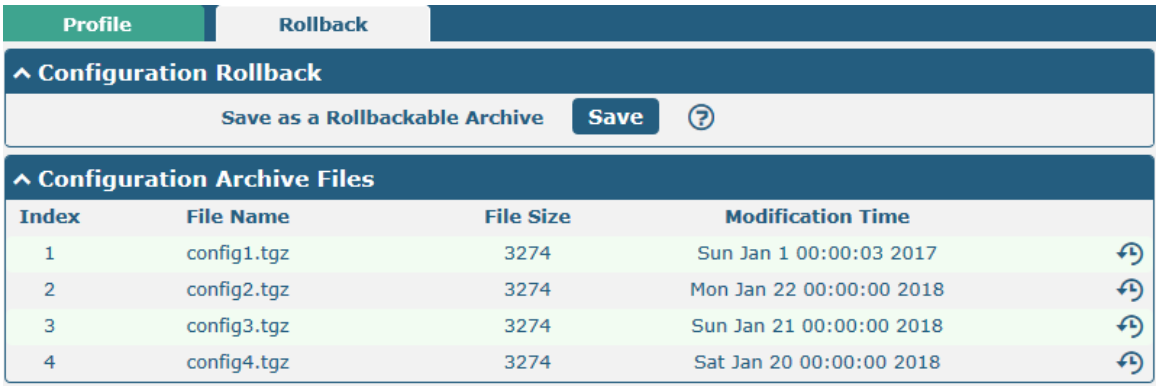
Sniffer		
Item	**Description**	**Default**
Interface	Select the interface according to the "Ethernet" configuration and select from "All", "PPP1", "WWAN" and "IO".	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the gateway can sniffer at a time.	1000
Protocol	Select from “All”, “IP”, “TCP”, “UDP” and “ARP”.	All
Status	Show the current status of sniffer.	Null
Start	Click this button to start the sniffer.	--
Stop	Click this button to stop the sniffer. Once you click this button, a new log file will be displayed in the following List.	--
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List and click to download the log, click to delete the log file. It can cache a maximum of 5 files.	Null

3.26 System > Profile

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



Profile		
Item	**Description**	**Default**
Import Configuration File		
Reset Other Settings to Default	Click the toggle button as "ON" to return other parameters to default settings.	OFF
Ignore Invalid Settings	Click the toggle button as "OFF" to ignore invalid settings.	OFF
XML Configuration File	Click on Choose File to locate the XML configuration file from your computer, and then click Import to import this file into your gateway.	--
Export Configuration File		
Ignore Disabled Features	Click the toggle button as "OFF" to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as "On" to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as "ON" to encrypt the secret data.	OFF
XML Configuration File	Click Generate button to generate the XML configuration file, and click Export to export the XML configuration file.	--
Default Configuration		
Save Running Configuration as Default	Click this button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click this button to restore the factory defaults.	--

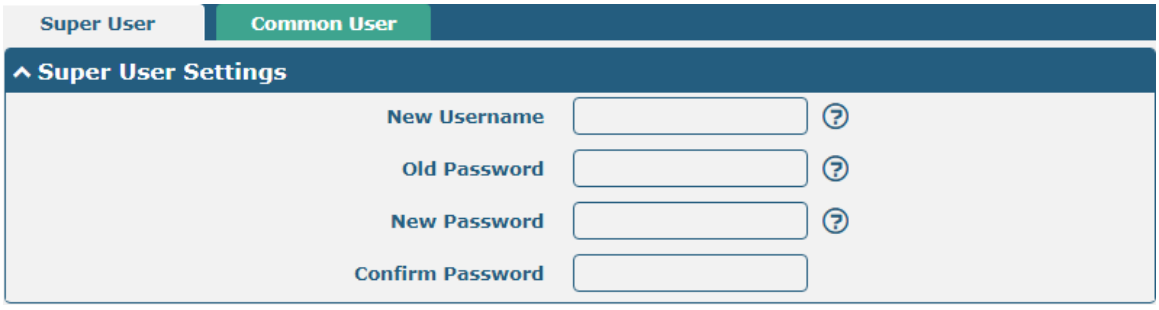


Rollback		
Item	**Description**	**Default**
Configuration Rollback		
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point every day automatically if configuration changes.	--
Configuration Archive Files		
Configuration Archive Files	View the related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

3.27 System > User Management

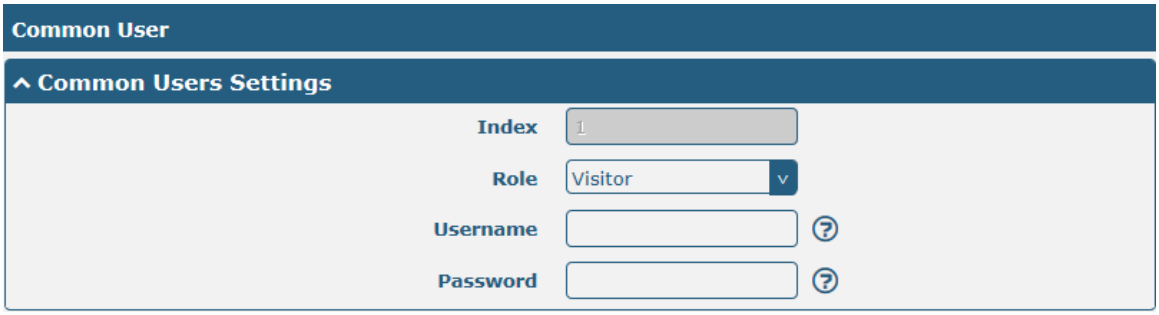
This section allows you to change your username and password, and create or manage user accounts. One gateway has only one super user who has the highest authority to modify, add and manage other common users.

Note: Your new password must be more than 5 character and less than 32 characters and may contain numbers, upper and lowercase letters, and standard symbols.



Super User Settings		
Item	**Description**	**Default**
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *. If you do not want to modify the username, leave it blank.	Null
Old Password	Enter the old password of your gateway. The default is “admin”.	Null
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Confirm Password	Enter the new password again to confirm.	Null

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



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

Chapter 4 Dial Configuration of PC under Modem Mode

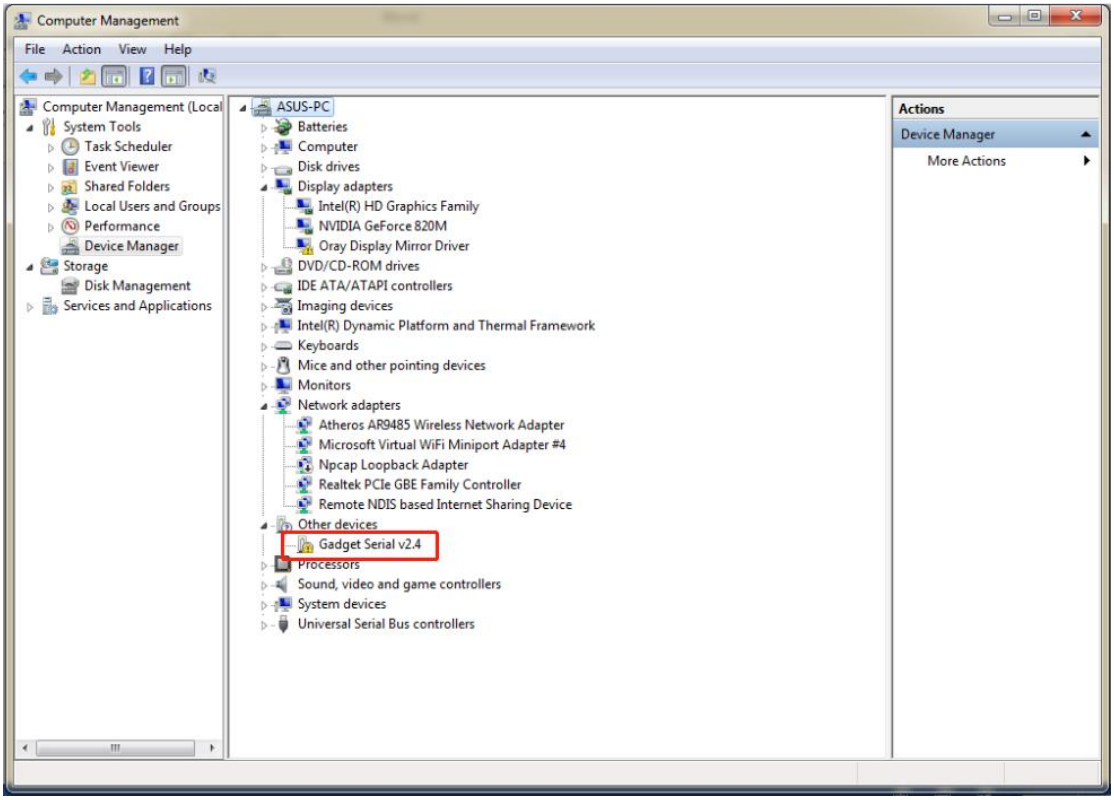
When M1200 is working under the Modem mode, PC can dial to access internet through device. After the first successful configuration of the same PC, the same dial-up connection does not need to be configured again. Different operating systems need to be configured differently. This chapter describes the Modem mode dialing configuration of Windows system and Linux system in detail.
Note: Under the Modem mode, only SIM1 is used for dialing.

4.1 Window System

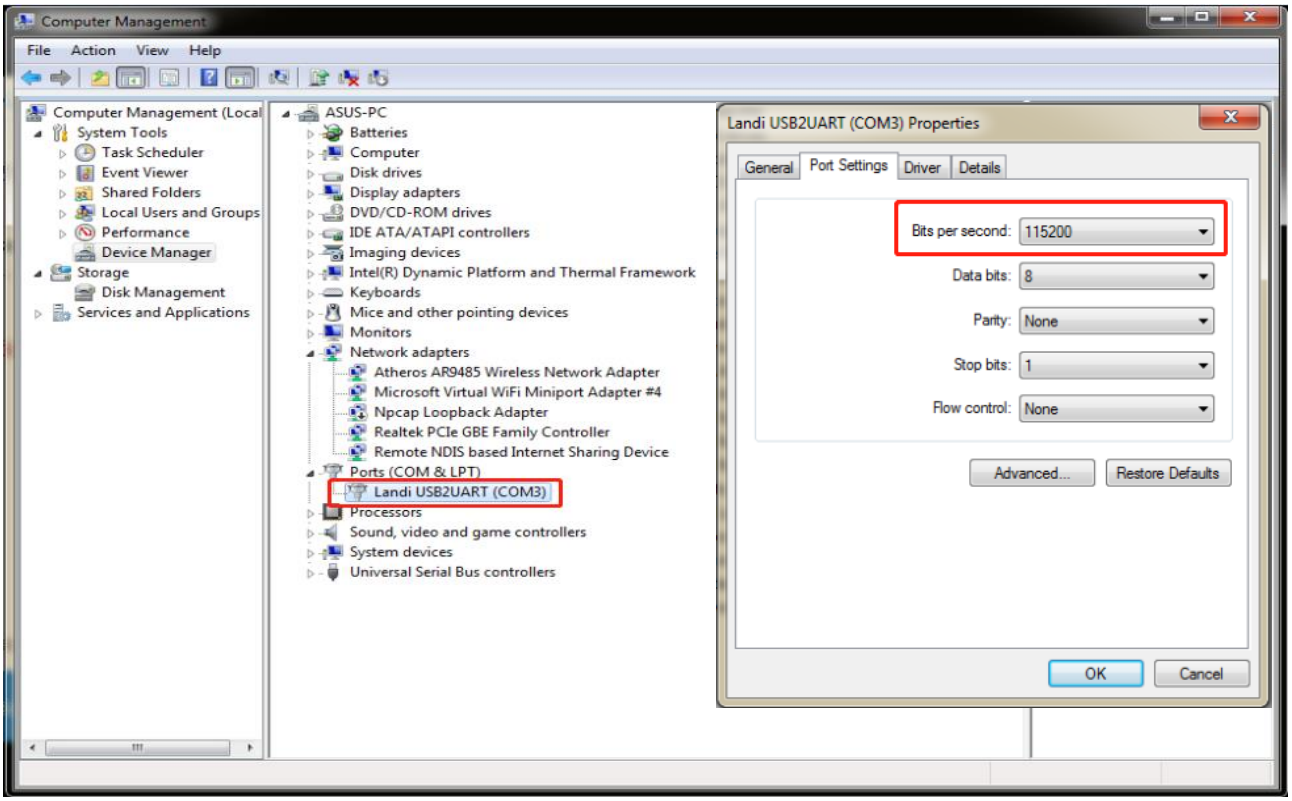
This chapter sets Windows 7 as the example to introduce how PC dials to access internet through device.

1. Install the serial port driver

（1） After device is connected, PC checked the new serial port and attempted to install the driver. As shown below, if PC cannot automatically install the driver, the user can manually add the driver and operate according to the readme under m1200_ppp_configure\usb_driver, and the related appendix can be downloaded on the official website or request for the technical support.

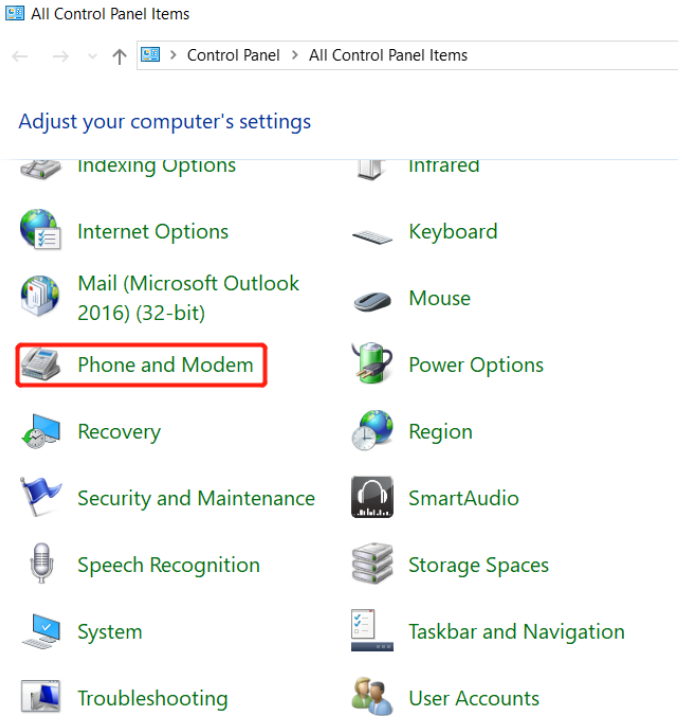


（2） After USB is connected to the PC, check the identified serial port. Different ports of different USB interfaces are different. Right-click and select “Properties” to set the serial port speed to 115200, and click “OK”;

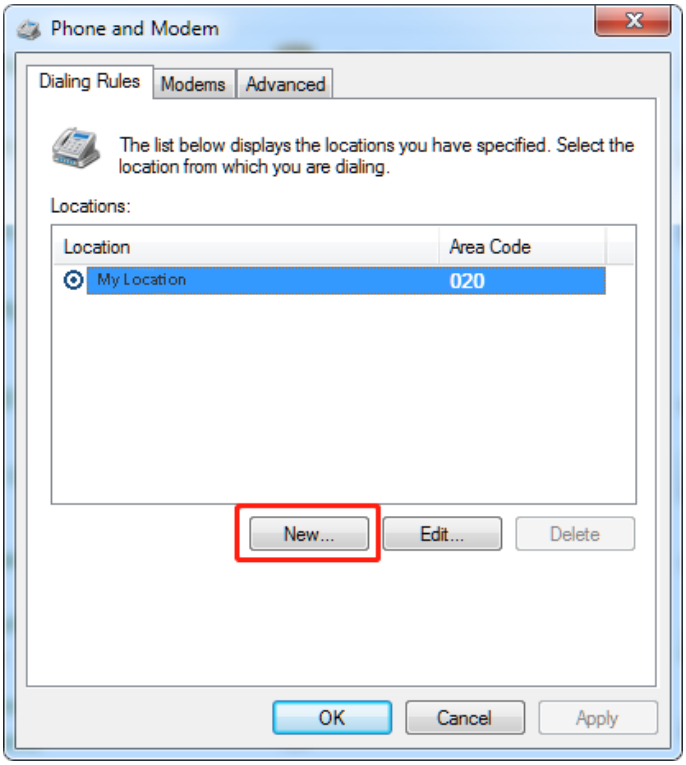


2. Add a Modem

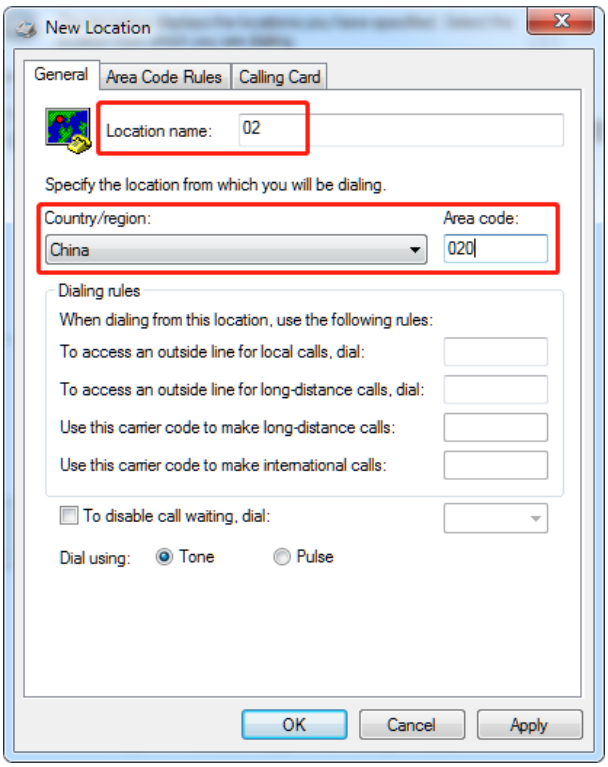
（1） In the Control Panel, select “Phone and Modem”, and add a modem;



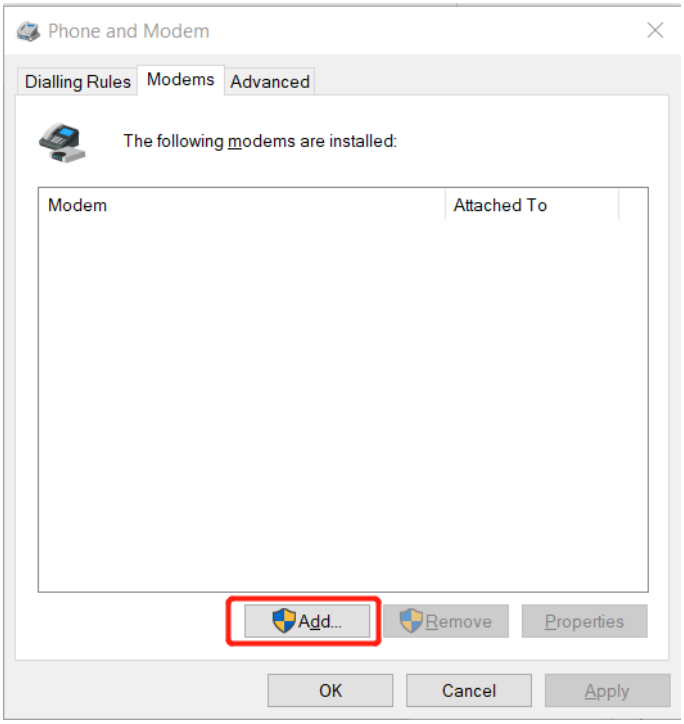
（2） Click "Dialing Rules" → "New" to add a new location;



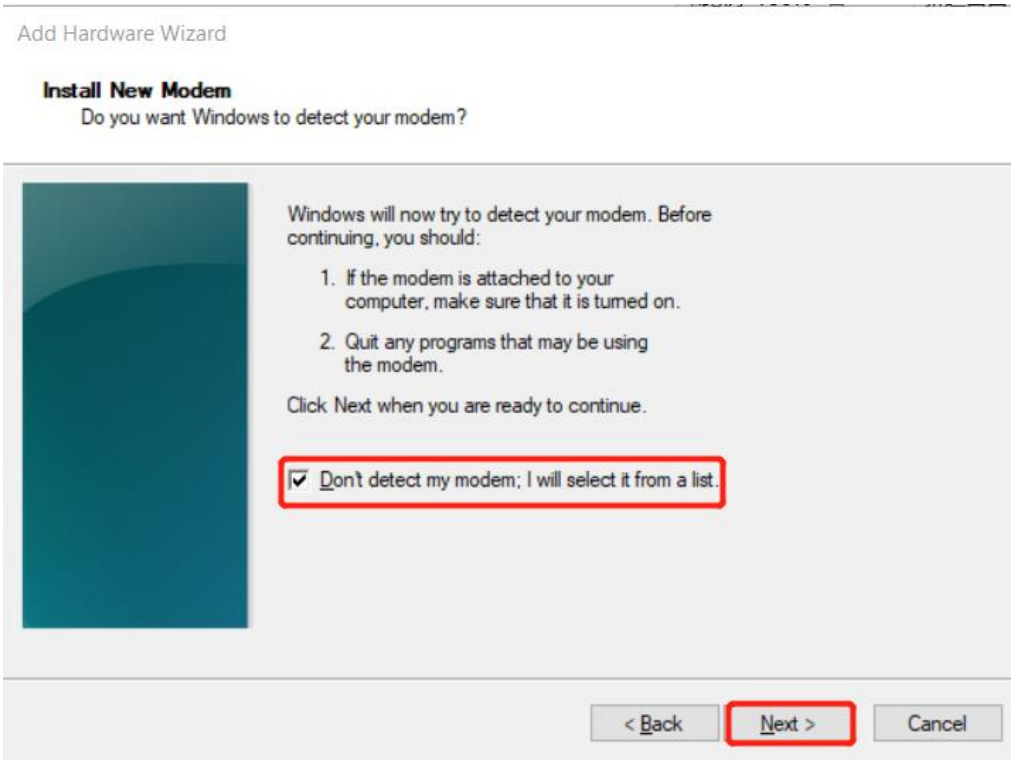
（3） Fill in the location name (optional), the dialing location is based on the actual selected country/region, fill in the correct area code and click “OK”;



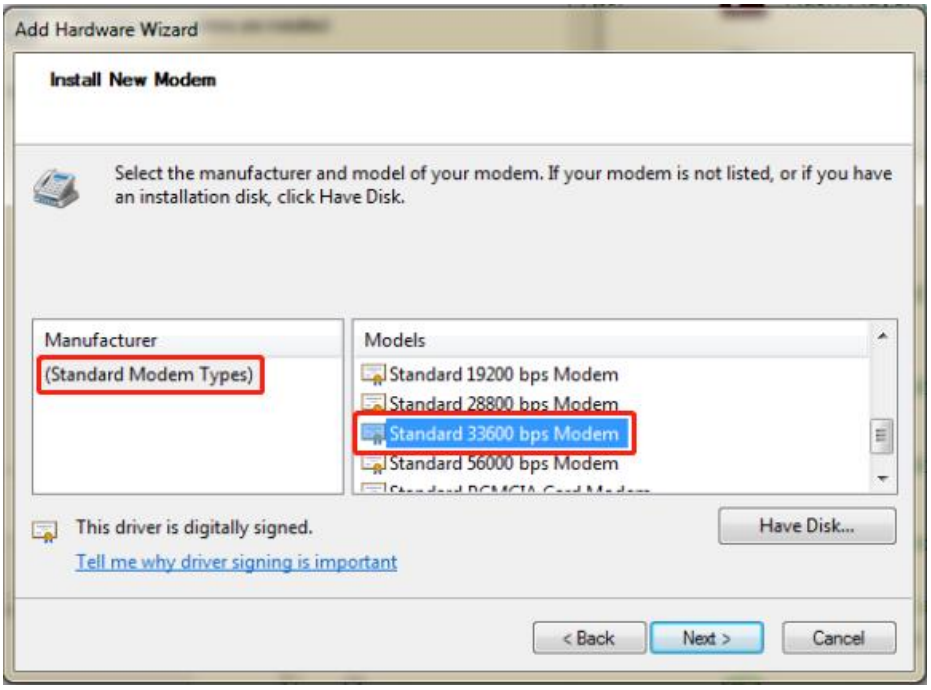
（4） Enter into the "Modem" item and click "Add";



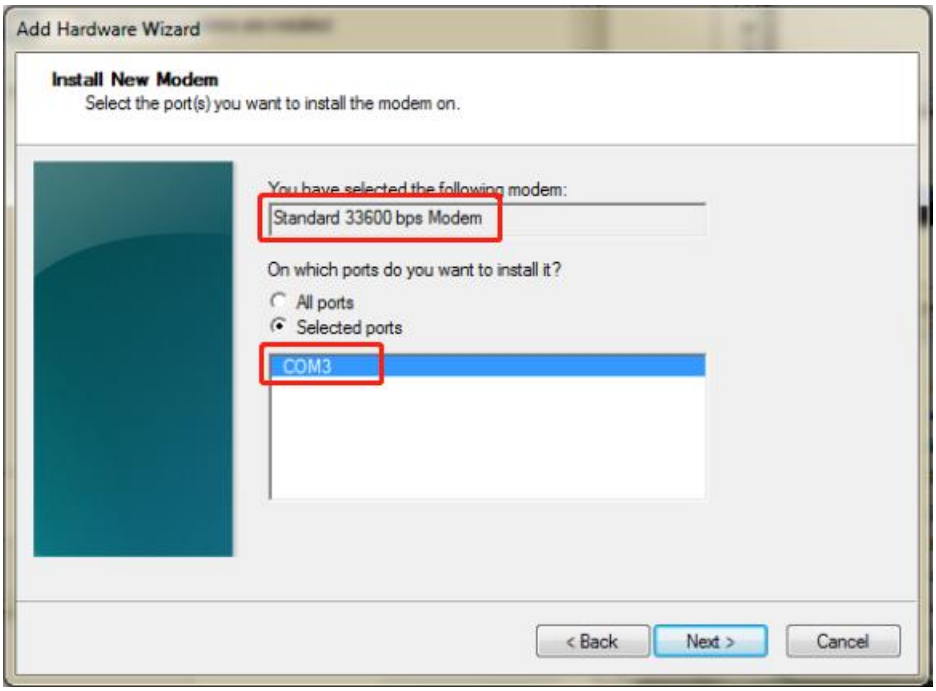
（5） Select "Don’t detect my modem, I will select it from a list" and click “Next”;



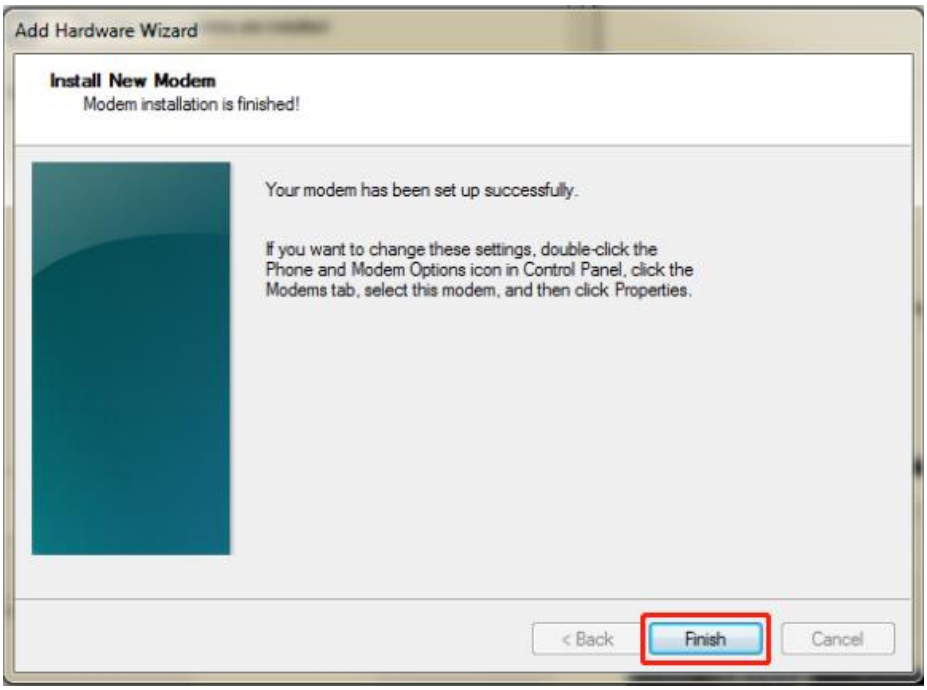
（6） Select the correct manufacturer and model according to the content shown in the figure. If the Standard Modem Types list does not exit, please refer to the readme under m1200_ppp_configure\ modem_inf, and the related appendix can be downloaded on the official website or requested for the technical support.



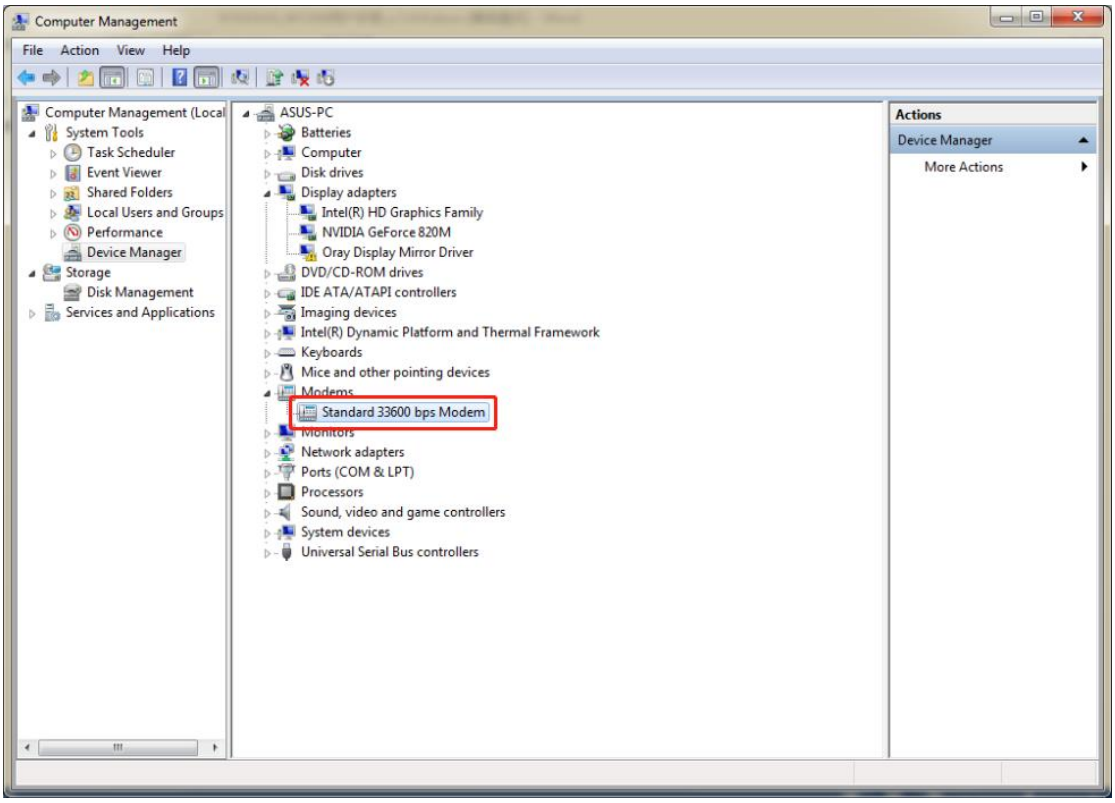
（7） According to the COM port corresponding to the device in step 1, select the actual corresponding port and click next.



（8） After the modem is installed, click “Finish”;



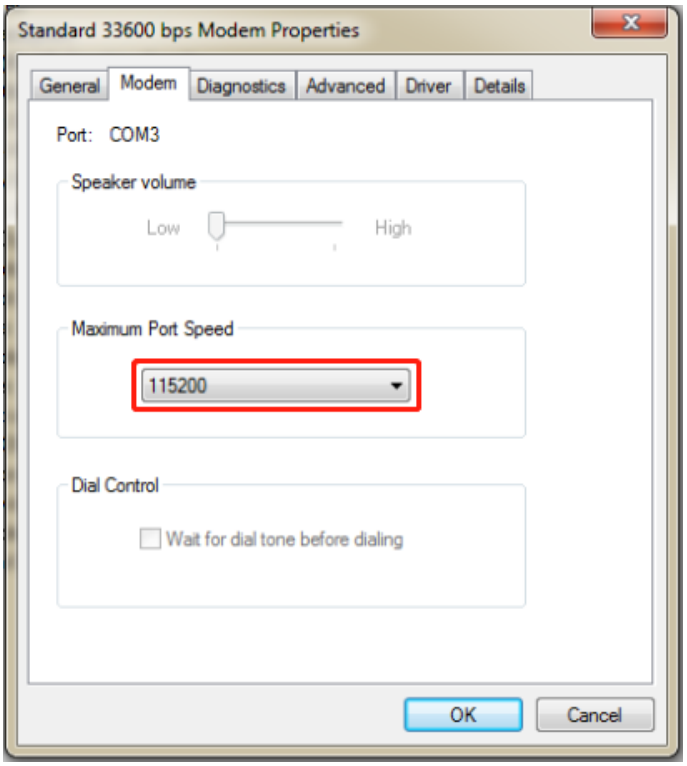
（9） Enter into the device manager of your computer and see the newly added modem.



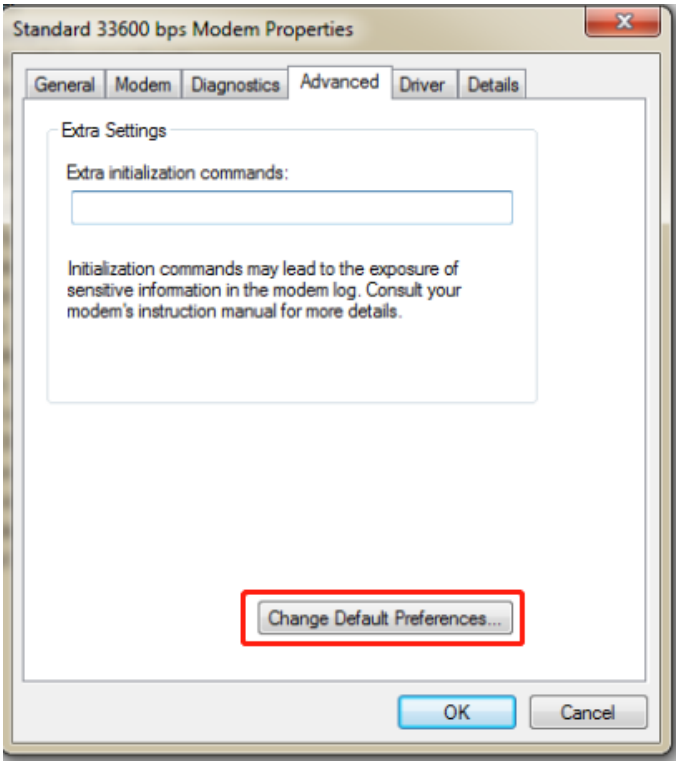
3. Configuring the modem

Right click on the new added modem and select "Properties" to configure it:

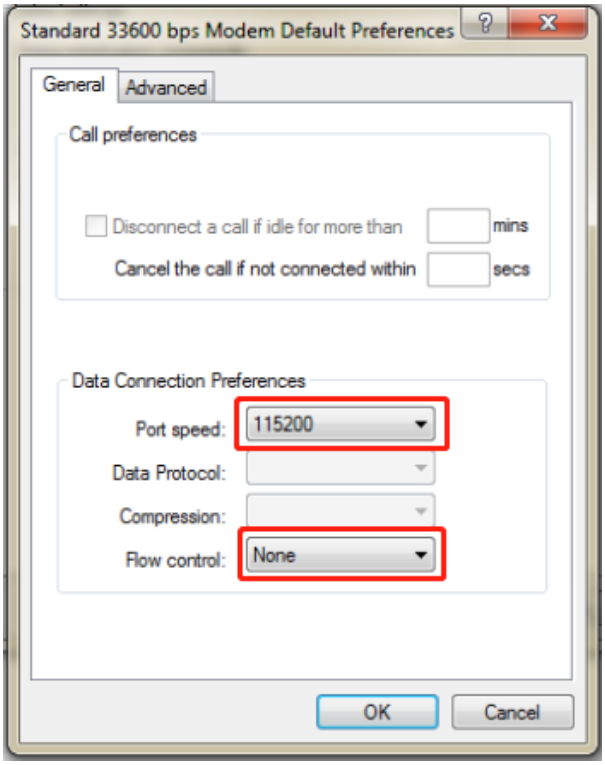
（1）Select the "Modem" item and select "115200" for the maximum port speed;



（2）Select the "Advanced" item and click "Change default preferences";



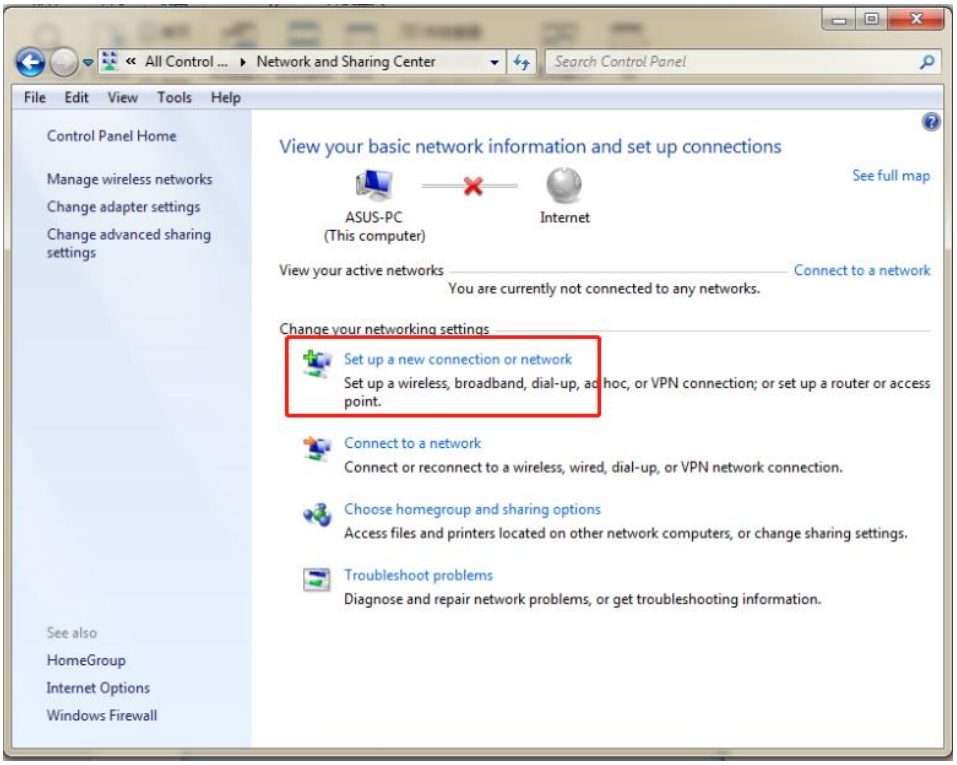
（3）Enter the "General" item, set the port speed to "115200", and select "None" for the data flow control;



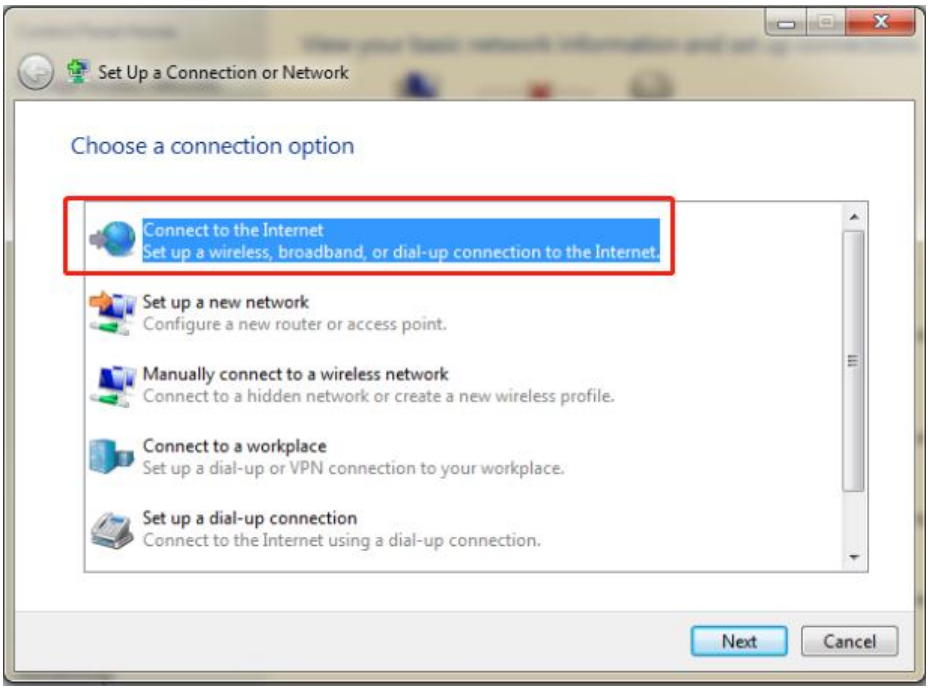
（4）Modem configuration is complete, click OK.

4. Create a new dial-up connection

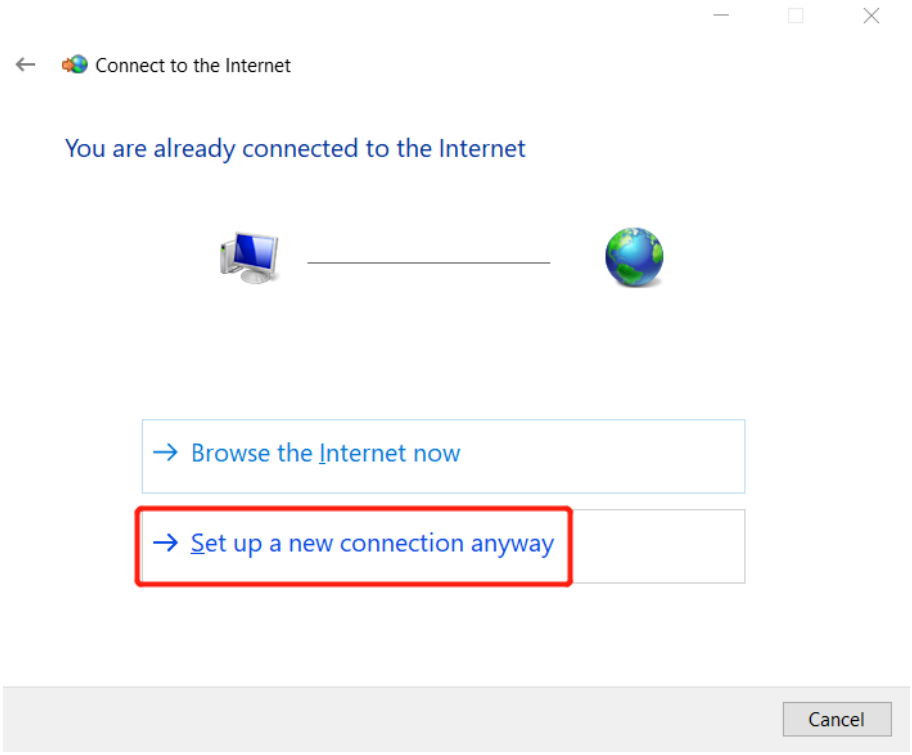
（1） Open your computer's Network Sharing Center, under "Change network settings," select "Set up a new connection or network";



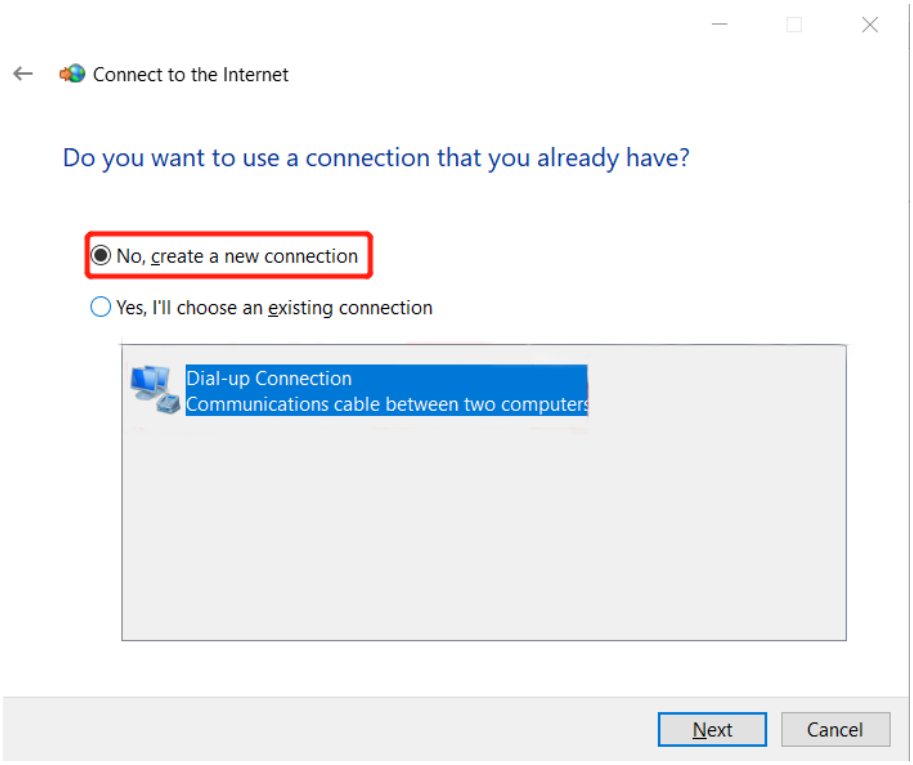
（2） Select "Connect to the Internet" and click Next;



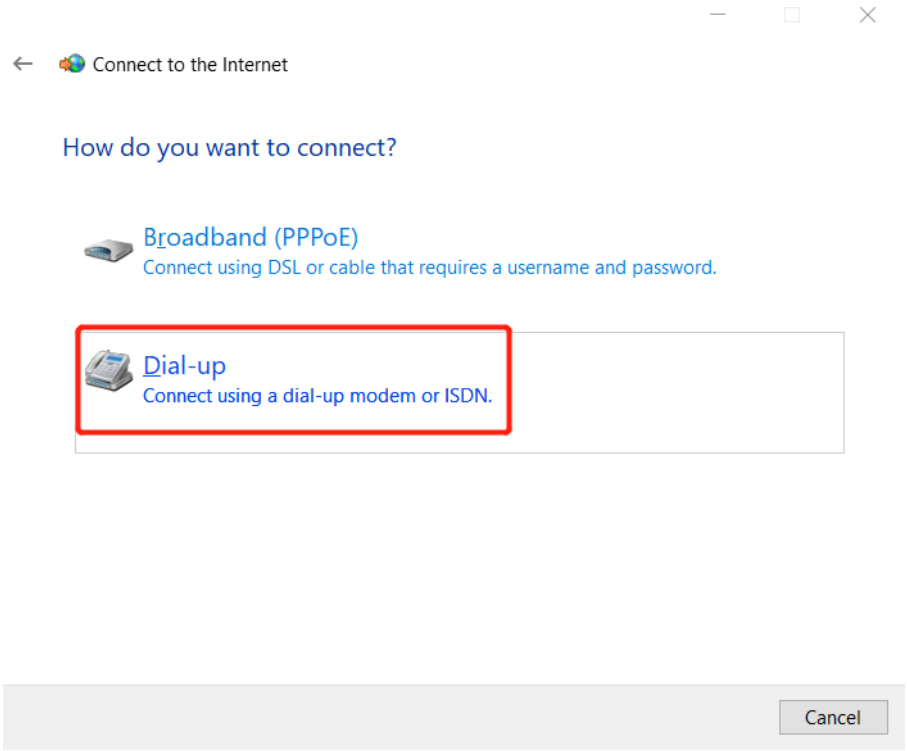
（3） In the new pop-up window, select " Set up a new connection anyway";



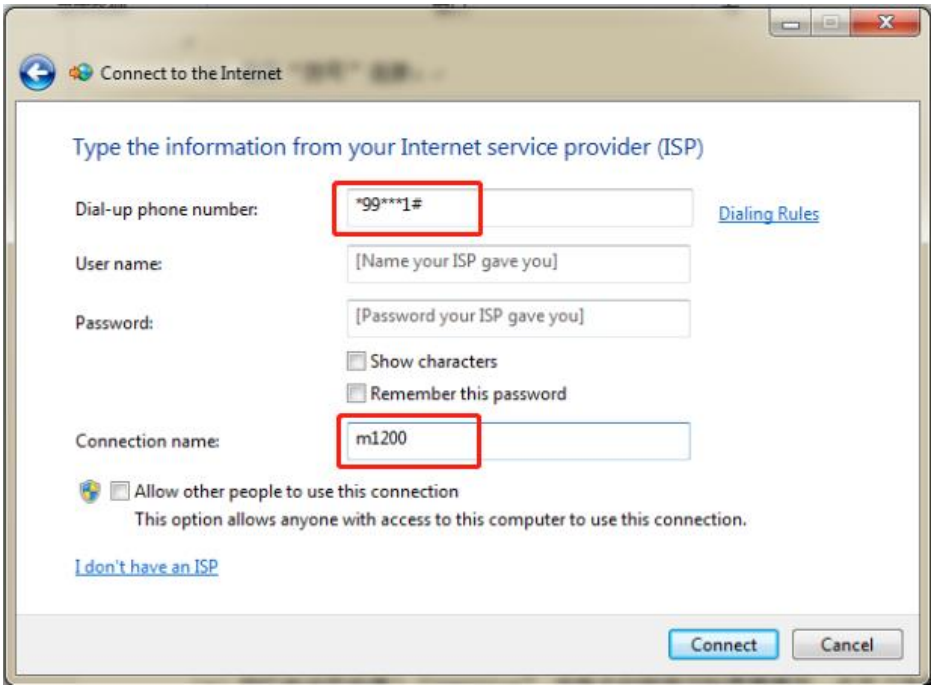
（4） Click "No, create a new connection" and click Next;



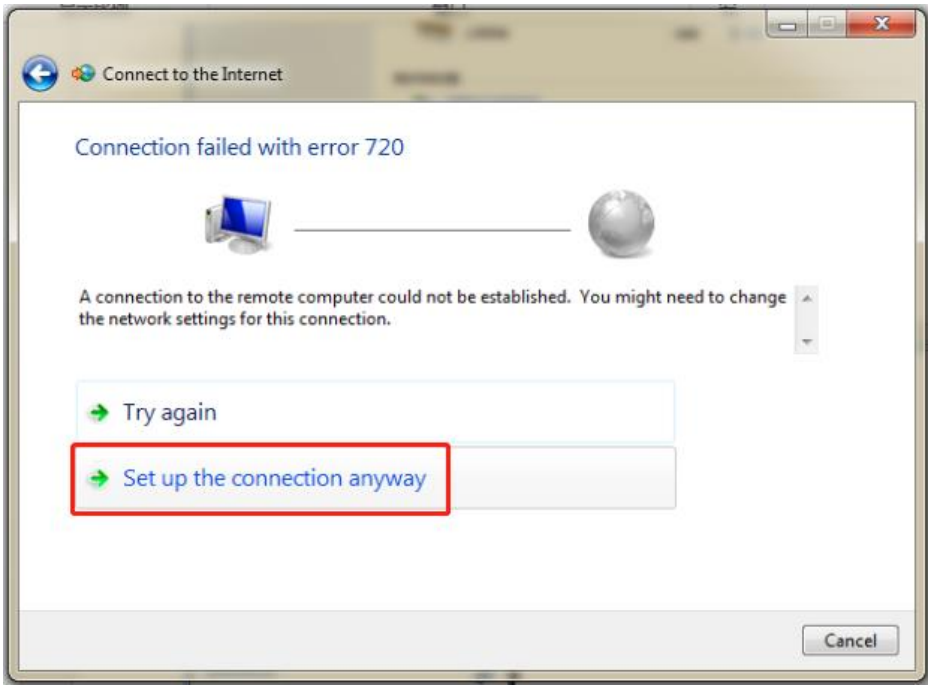
（5） Select the "Dial-up" connection;



（6） Dial the phone number and fill in "*99***1#". Fill in the connection name according to actual needs. Click "connect".

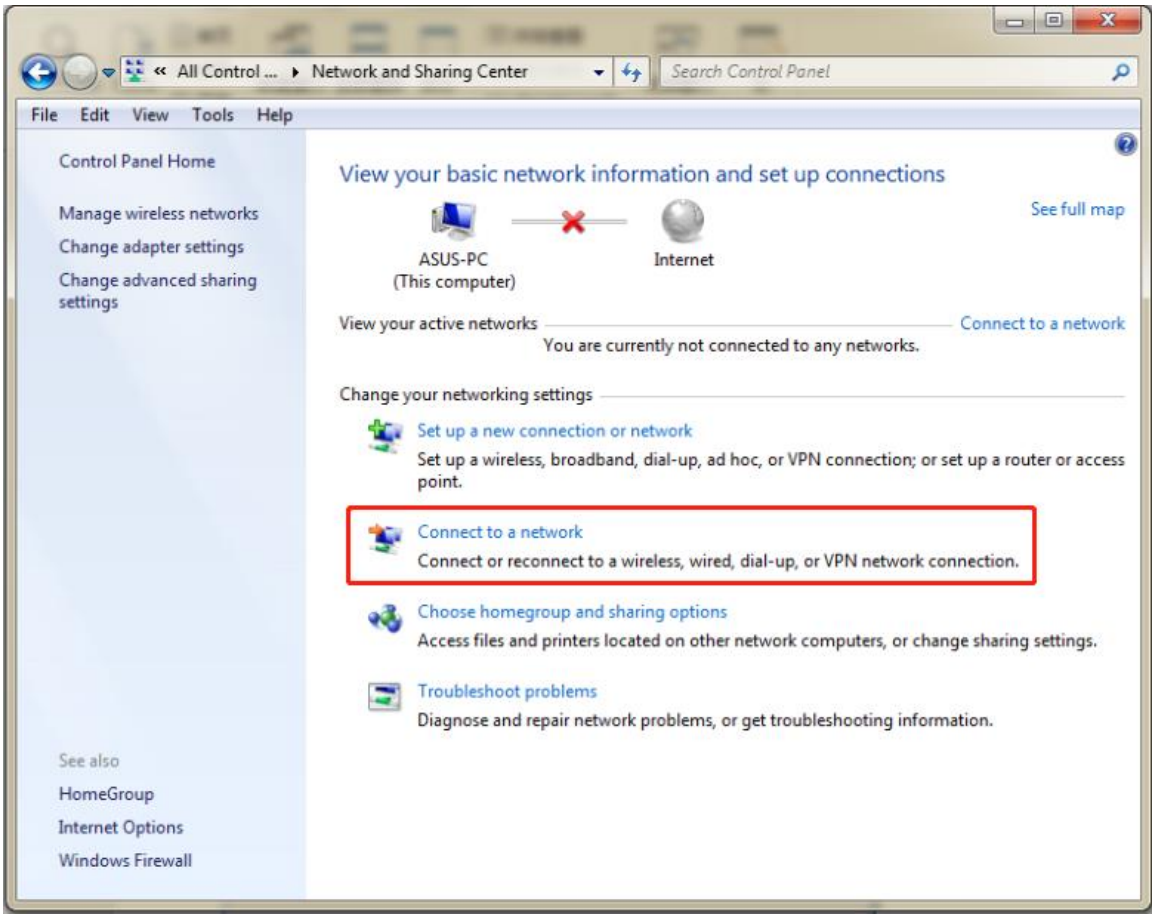


（7） After the connection fails, click "Always set up connection" to close this page.

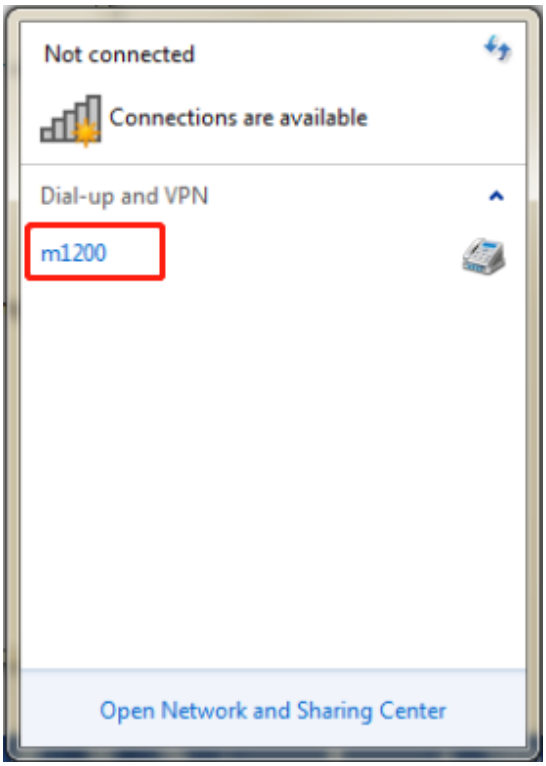


5. Dial-up connection

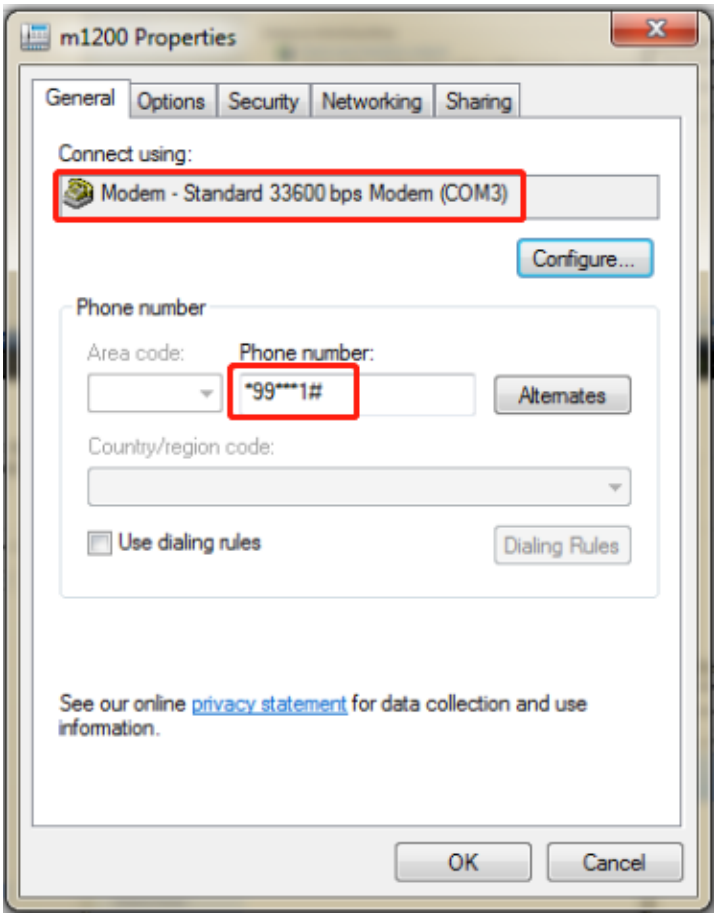
（1） Open your computer's “Network Sharing Center”, under "Change network settings," select "Set up a new connection or network”；



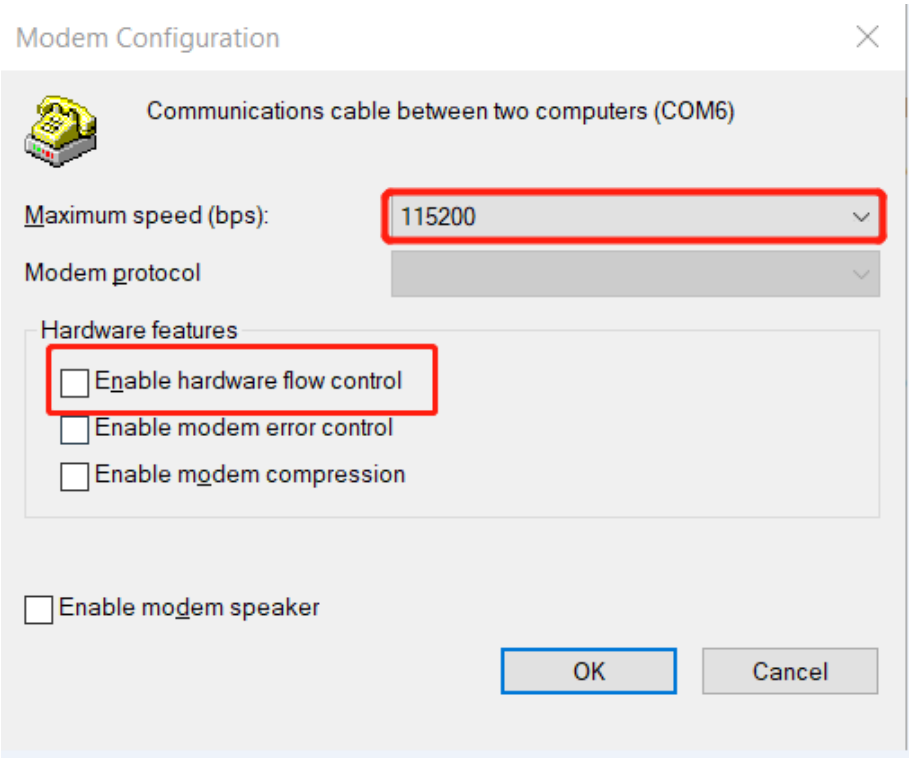
（2） Select the newly established dial-up connection in the new pop-up box, right-click and select "Properties";



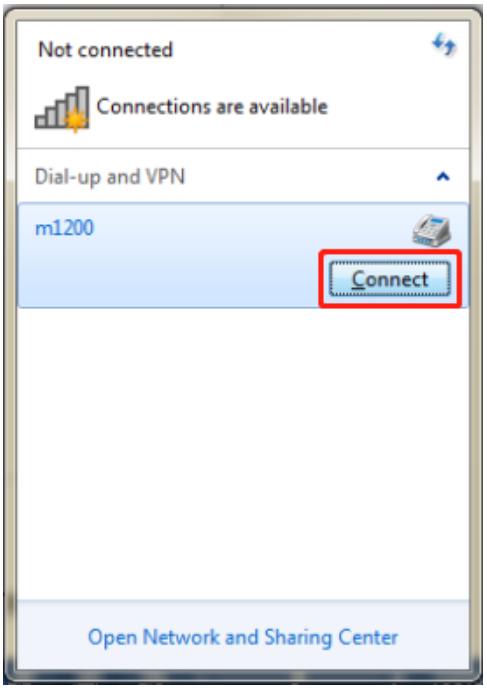
（3） Under “General”, select the added modem, confirm that the phone number is added correctly, and click “Configure”;



（4） The maximum speed is selected as “115200”, and the hardware function is unchecked “Enable Hardware Flow Control”, as shown below;



（5） After the configuration is complete, click “Connect” and select “Dial-up” in the pop-up page box to establish a connection with the device


Not connected
Connections are available
Dial-up and VPN
m1200
Connect
Open Network and Sharing Center

4.2 Linux System

The M1200 modem mode supports Linux system. This part takes R3000 (the device uses Linux system) as an example, dialing through RS 232 serial port.

1. Verify device connectivity

Connect M1200 with R3000 through RS 232 serial port. If the connection is completed, input command in R3000: microcom -s 115200 /dev/ttyCOM1, and then the command window will return CSQ value continually as shown below, CTRL + X can stop AT port.

```
~ # microcom -s 115200 /dev/ttyCOM1
+CSQ: 15,99
OK
+CSQ: 15,99
OK
+CSQ: 15,99
OK
+CSQ: 15,99
OK
```

2. Dial interface configuration

（1）Input ls -l /dev/ttyCOM1 to view the name of COM1 port, which same as the name of the script.

```
~ # ls -l /dev/ttyCOM1
lrwxrwxrwx    1 root     root            10 Jan  1  1970 /dev/ttyCOM1 -> /dev/ttyS4
```

（2）Copy the U disk which with the dialing script to the corresponding content through the USB port of R3000, the details as shown below:

~ # cp /mnt/usb/dialscript/modem.chat /etc/ppp

~ # cp /mnt/usb/dialscript/modem.options /etc/ppp/peers/

~ # ln -s /etc/ppp/resolv.conf /etc/resolv.conf

（3）The script content as shown below. The red box mark in the figure changes according to the actual situation. The name of interface and baud rate are required to same as the configuration of M1200:

modem.options

```
1  /dev/ttyS4 115200 nocrtscts
2  connect "chat -f /etc/ppp/modem.chat"
3  lock
4  noauth
5  debug
6  logfile /tmp/m1200_modem_log
7  defaultroute
8  modem
9  usepeerdns
10 idle 0
11
```

modem.chat

modem.options | modem.chat

```
1   ABORT   BUSY
2   ABORT   'NO CARRIER'
3   ABORT   ERROR
4   REPORT  CONNECT
5   TIMEOUT 10
6   ""      "AT"
7   OK      "ATE0"
8   OK      'AT+CGDCONT=1,"IP","3gnet"'
9   TIMEOUT 30
10  OK      "ATD*99***1#"
11  CONNECT ''
```

3. Enter the dialing command to dial
   ~ # pppd call modem.options

4. View the dialing logs
   ~ # cat /tmp/m1200_modem_log

5. If it needs dial again, input ps command to view the process number of pppd process, then kill the process, input dial command to dial again.

```
 1022 root       0:00 -sh
 1103 root       0:00 [kworker/u2:0]
 1257 root       0:00 [kworker/0:1H]
 1479 root       0:00 [kworker/u2:1]
 1986 root       0:00 link_manager
 1999 root       0:00 [kworker/0:0]
 2244 root       0:00 syslogd -L -b 5 -s 1024 -l 8 -f /var/etc/syslog.conf
 2246 root       0:00 klogd
 2389 root       0:00 modemd
 2529 root       0:00 qmi_wwan
 2531 root       0:08 /usr/sbin/slqssdk 0
 2757 root       0:00 pppd call modem.options
 2862 root       0:00 ps
~ # kill 2757
~ # pppd call modem.options
```

4.3 CLI to Change the Configuration of Modem

When device is under the mode of Modem, it can be configured through CLI command. If the current “selection of dialing port” (i.e. at_port), input the following command and keep it:

1. view the current mode by inputting show mode all:

```
# show mode all
current_mode = modem
at_port = rs232
baud_rate = 115200
data_bits = 8
stop_bits = 1
parity = none
debug_enable = true
```

2. Revise the parameter of Modem.

For example, revise “selection of dialing port” (i.e. at_port), input the following command and keep it:

```
# set mode at_port rs232
# config save_and_apply
```

3. Revise the baud rate of the device:

```
# set mode baud_rate 115200
# config save_and_apply
```

To modify other parameters, modify the at_port and the parameters that follow it.

4. Switch to the DTU mode

There are two ways:

（1） Configured to DTU mode via CLI settings:

Set the mode to DTU mode:

set mode current_mode dtu

Save the configuration:

config save_and_apply

Reboot the device:

reboot

（2）Send commands through the dial interface to configure DTU mode:

_dtu

Reboot the device:

_rbt

Description:

（1）USB is used as at_port. At this time, you can log in to the device through RS232 and configure the device to DTU mode by using the CLI.

（2）RS232 is used as the at_port. At this time, the command can be sent to the RS232 (the command is sent through the dial interface) to configure the DTU mode. In this case, the USB cannot log in to the device.

Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface for batch scripting
CSD	Circuit Switched Data
CTS	Clear to Send
dB	Decibel
dBi	Decibel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DI	Digital Input
DO	Digital Output
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EDGE	Enhanced Data rates for Global Evolution of GSM and IS-136
EMC	Electromagnetic Compatibility
EMI	Electro-Magnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
EVDO	Evolution-Data Optimized
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
ID	identification data
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
kbps	kbits per second
L2TP	Layer 2 Tunneling Protocol

Abbr.	Description
LAN	local area network
LED	Light Emitting Diode
LoRa	Long Range
LoRaWAN	LoRa Wide Area Network
LPWAN	Low Power Wide Area Network
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct current

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

Guangzhou Robustel LTD

Add: 3rd Floor, Building F, Kehui Park, No.95 Daguan Road, Guangzhou, China 510660

Tel: 86-20-29019902

Email: info@robustel.com

Web: www.robustel.com