C335 Series

Edge Computing Gateways

User Manual

Version: 1.4

Revision History

No.	Software Version	Description	Date
V1.0	V200R002	First release	Jul. 19, 2020
V1.1	V200R003	Added description of serial terminals	Aug. 18, 2021
V1.2	V200R003	Updated contact information	Jun. 15, 2022
V1.3	V200R003	Updated interface description of C335L	Nov. 23, 2022
V1.4	V200R003	Updated protocol portal login and configuration	Mar. 24, 2023

Table of Contents

Foreword

Thank you for purchasing Vantron edge computing gateway (“the Gateway” or “the Product”). There are three models in C335 series gateways: C335L, C335, and C335S, so please refer to the respective part of the manual for the product you bought. This manual intends to provide guidance and assistance necessary on setting up, operating and maintaining the Product. Please read this manual and make sure you understand the structure and functionality of the Product before putting it into use.

Intended Users

This manual is intended for:

- Network architects/programmers
- Network administrators
- Technical support engineers
- Other users

Copyright

Disclaimer

While all information contained herein has been carefully checked to assure its accuracy in technical details and typography, Vantron does not assume any responsibility resulting from any error or features of this manual, nor from improper uses of this manual or the software.

It is our practice to change part numbers when published ratings or features are changed, or when significant structure changes are made. However, some specifications of the Product may be changed without notice.

Technical Support and Assistance

Should you have any question about the Product that is not covered in this manual, contact your sales representative for solution. Please include the following information in your question:

- Product name and PO number;
- Complete description of the problem;
- Error message you received, if any.

Vantron Technology, Inc.

Address: 48434 Milmont Drive, Fremont, CA 94538
Tel: (650) 422-3128
Email: sales@vantrontech.com

Regulatory Information

The Product is designed to comply with:

- Part 15 of the FCC Rules
- PTCRB

Please refer to the Appendix for Regulatory Compliance Statements.

Symbology

This manual uses the following signs to prompt users to pay special attention to relevant information.

⚠	Caution for latent damage to system or human injury
ℹ	Attention to important information or regulations

General Safety Instructions

The Product is supposed be installed by knowledgeable, skilled persons familiar with local and/or international electrical codes and regulations. For your safety and prevention of damage to the Product and other equipment connected to it, please read and observe carefully the following safety instructions prior to installation and operation. Keep this manual well for future reference.

- Do not disassemble or otherwise modify the Product. Such action may cause heat generation, ignition, electronic shock, or other damages including human injury, and may void your warranty.
- Keep the Product away from heat source, such as heater, heat dissipater, or engine casing.
- Do not insert foreign materials into any opening of the Product as it may cause the Product to malfunction or burn out.
- To ensure proper functioning and prevent overheating of the Product, do not cover or block the ventilation holes of the Product.
- Follow the installation instructions with the installation tools provided or recommended.
- The use or placement of the operation tools shall comply with the code of practice of such tools to avoid short circuit of the Product.
- Cut off the power before inspection of the Product to avoid human injury or product damage.

Precautions for Power Cables and Accessories

⚠ Use proper power source only. Make sure the supply voltage falls within the specified range. Always check whether the Product is DC powered before applying power.

⚠ Place the cables properly at places without extrusion hazards.

⚠ Use only approved antenna(s). Non-approved antenna(s) may produce spurious or excessive RF transmitting power which may violate FCC limits.

⚠ Cleaning instructions:

- Power off the Product before cleaning
- Do not use spray detergent
- Clean with a damp cloth
- Do not try to clean exposed electronic components unless with a dust collector

⚠ Power off and contact Vantron technical support engineer in case of the following faults:

- The Product is damaged
- The temperature is excessively high
- Fault is still not solved after troubleshooting according to this manual

⚠ Do not use in combustible and explosive environment:

- Keep away from combustible and explosive environment
- Keep away from all energized circuits
- Unauthorized removal of the enclosure from the Product is not allowed
- Do not change components unless the power cable is unplugged
- In some cases, the Product may still have residual voltage even if the power cable is unplugged. Therefore, it is a must to remove and fully discharge the Product before replacement of the components.

CHAPTER 1

HARDWARE DESCRIPTION

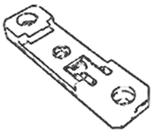
1.1 Product Overview

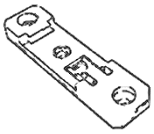
Vantron C335 series edge computing gateways were launched to meet the needs of IIoT applications in various industrial scenarios. This series supports a variety of industrial protocols to allow access by field industrial devices such as PLCs, HMIs, sensors, etc. The edge computing functionality helps to achieve data optimization at IoT edge nodes, which reduces the data volume accumulated in the field and the central console. With standard MQTT protocol, the series provides a broad access to industrial data platforms to facilitate the digital transformation of factories.

This series adopts industrial design with guaranteed quality and reliability to offer an ideal solution for your IoT application. Meanwhile it provides access to Vantron BlueSphere cloud platform for unified management to ease the efforts of users by real-time monitoring and tracking, OTA updates, remote maintenance, task assignment and follow-up.

1.2 Unpacking

The Product has been carefully packed with special attention to quality. However, should you find anything damaged or missing, please contact your sales representative in due time.

Standard accessories (C335S &C335L)		Optional accessories (C335S &C335L)	
	1 x C335S/C335L gateway		1 x Power adapter
	1 x Wi-Fi antenna		1 x DC power connector
	1 x DIN rail mounting bracket		2 x 4G LTE antenna

Standard accessories (C335)		Optional accessories (C335)	
	1 x C335 gateway		1 x Power adapter
	1 x DIN rail mounting bracket		1 x DC power connector
\	\		1 x 4G LTE antenna or 1 x Wi-Fi antenna

Actual accessories might vary slightly from the list above as the customer order might differ from the standard configuration options.

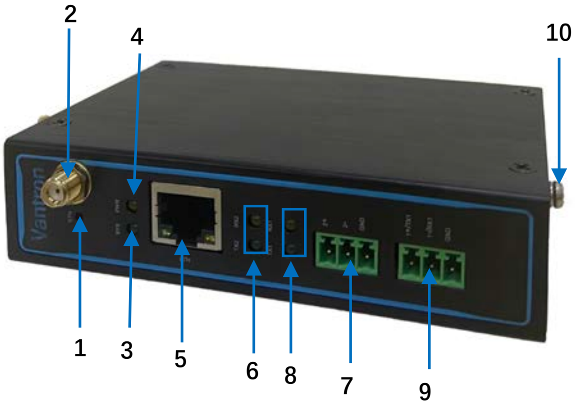
1.3 Specifications

Model		C335L	C335	C335S
System	CPU	TI, AM335x, ARM Cortex-A8, 600MHz	TI, AM335x, ARM Cortex-A8, 600MHz	TI, AM335x, ARM Cortex-A8, 1GHz
	Memory	512MB	1GB	1GB
	Storage	8GB, up to 64GB 1 x Micro SD card	8GB, up to 64GB 1 x Micro SD card	8GB, up to 64GB 1 x Micro SD card
Communication	Ethernet	1 x RJ45, 10/100Mbps	2 x RJ45, 10/100Mbps	6 x RJ45 (1 for debugging), 10/100Mbps
	LTE & Wi-Fi & Bluetooth	Mini PCIe for LTE CAT 4/ CAT M (AT&T, Verizon) On-board Wi-Fi 802.11 a/b/g/n/ac & BT 5.0	Mini PCIe for either LTE CAT 4/ CAT M (AT&T, Verizon) or Wi-Fi 802.11 a/b/g/n/ac & BT 5.0	Mini PCIe for LTE CAT 4/ CAT M (AT&T, Verizon) On-board Wi-Fi 802.11 a/b/g/n/ac & BT 5.0
	Ethernet port protocol	PPP, PPPoE, DHCP, ARP		
I/Os	Serial port	1 x RS485 1 x RS232/RS485 (default)	3 x RS485 1 x RS232/RS485 (default)	3 x RS485 1 x RS232/RS485 (default)
	DI	NA	NA	4 x Digital input
	AI	NA	NA	2 x Analog input
	SIM slot	1 x Drawer-type SIM slot		
	Grounding	Enclosure & PCB		
	RTC	Separate RTC chip, powered by button cell	Separate RTC chip, powered by button cell	Separate RTC chip, powered by system or button cell
	GPIO	4 x GPIO (Optional)	4 x GPIO (Optional)	4 x GPIO
System Control	Button	1 x Reset button	1 x Reset button 1 x Renew button	1 x Reset button 1 x Restore button
	LED indicator	1 x Power indicator 1 x System status indicator 4 x Serial port status indicator	1 x Power indicator 1 x System status indicator 8 x Serial port status indicator	1 x Power indicator 1 x System status indicator 4 x Serial port status indicator
Mechanical	Dimensions	113.5mm x 82mm x 28.5mm	125mm x 110mm x 30mm	132mm x 124mm x 40mm
	Enclosure	Metal		
	Installation	DIN rail mounting/Wall mounting/Panel mounting		
	IP rating	IP30		
	Cooling mode	Fanless		
Power	Input	9-36VDC, over-current protection, reverse polarity protection	12-48VDC, over-current protection, reverse polarity protection	12-48V DC, over-current protection, reverse polarity protection
	Terminal	3-pin 3.81mm terminal	3-pin 3.81mm terminal	3-pin 3.81mm terminal
Software	OS	VantronOS		
	SDK	Available		
	Network management	SNMP v1/v2c/v3		
	Device management platform	Vantron BlueSphere		
	IoT protocol	MQTT/ HTTPS		
	IPK import	Supported		

Model		C335L	C335	C335S
	Interface language	Chinese and English (Default) Other languages (Optional)		
	NTP	Supported		
	Log	Supported		
Security	Firewall	SYN-flood protection, port forwarding, custom rules		
	Data security	OpenVPN, L2TP, PPTP, IPSec		
	Link detection	Heartbeat detection, automatic re-connection		
	Network reliability	Failover supported, Link backup between Ethernet, Wi-Fi and 4G/LTE		
	Multi-level permission	Supported		
Function & Application	Configuration mode	Local, remote		
	Upgrade	Local, OTA update	Local, OTA update	OTA update
	Networking guide	One-key configuration of LTE, Wi-Fi, and Ethernet		
	Traffic statistics	Per month/week/day		
	IP application	Ping, Traceroute, Nslookup		
	IP Routing	Static routing		
	NAT	Supported		
Industrial Protocol	M2M protocol	Modbus TCP, Modbus RTU, EtherNet/IP, ISO-on-TCP, CC-link, etc.		
Edge Computing	Edge computing	JavaScript, MicroPython		
User Programmable	Development language	C/ C++/ Python/ Lua/ Node.js/Java/ Node-Red (Optional)		
Environment Condition	Temperature	Operating: -20℃ ~ +70℃ Storage: -30℃~+85℃	Operating: -20℃ ~ +70℃ Storage: -30℃~+85℃	Operating: -20℃ ~ +70℃ (Optional: -20℃~+85℃) Storage: -40℃~+85℃
	Humidity	RH 5%-95%		
	Certification	CE, FCC, PTCRB		

1.4 Definition of Interfaces (C335L)

1.4.1 Front view

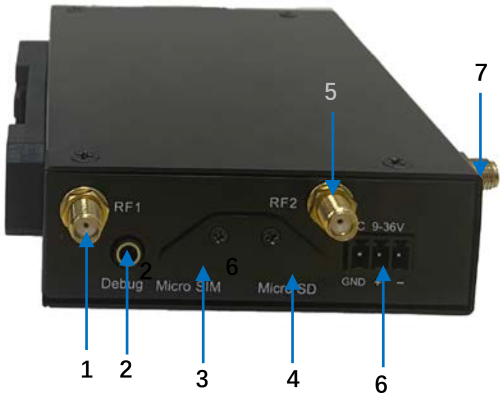


Item No.	Description	
1	BTN button (see details below)	
2	4G primary antenna	
3	System status indicator	Blinks at system bootup
		Turns solid green after system bootup
		Blinks at system upgrade or configuration cleanup
4	Power indicator	
5	Ethernet port, shown as ETH0 in VantronOS and works in LAN area by default	
6	Status indicators for serial port R2 (blinks at data transfer)	
7	Serial port R2 (RS485)	
8	Status indicators for serial port R1 (blinks at data transfer)	
9	Serial port R1 (RS232/RS485)	
10	Ground screw	

Description of the BTN button

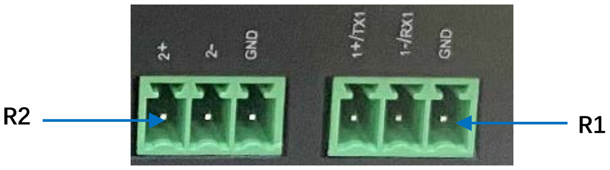
- When a system upgrade drive is inserted in the SD slot or USB port, a short press of the button for about 2 seconds will cause the status indicator to blink, suggesting system upgrade is in progress. Once the upgrade finishes, the system will reboot (from eMMC flash).
- When the button is pressed and held for 3-10 seconds, user configurations and custom settings will be removed and the Gateway will be factory reset. Once finishes, the system will reboot.
- When the button is pressed for over 10 seconds, user partitions will be formatted and data in such partitions will be cleared.

1.4.2 Left side view



Interface	Description
1	4G diversity antenna
2	Debug port
3	Micro SIM slot
4	Micro SD slot
5	Wi-Fi & BT antenna
6	9V-36V DC power terminal
7	4G primary antenna

1.4.3 Serial port



Pinout description:

Serial port	Node	Serial mode	LED indicator
R1 (right)	/dev/ttyO2	RS232 / RS485	TX1/RX1
R2 (left)	/dev/ttyO4	RS485	TX2/RX2

R1 could switch between RS232 and RS485 (default), and R2 is RS485.

1. Input the following command lines in a host device to enable **RS232** on R1 and use a serial communication program (e.g., microcom) to open the port:

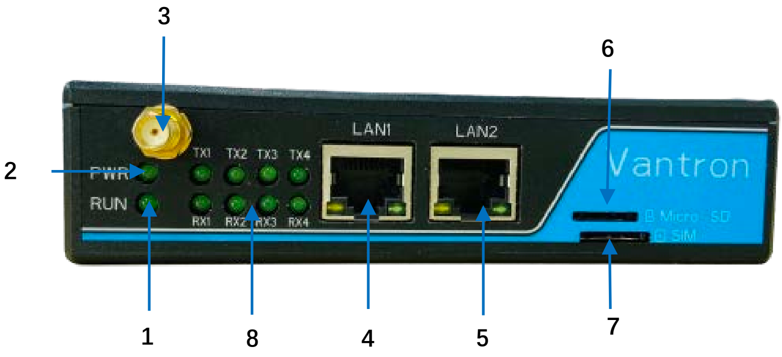
```
~# gpio set uart0 rs232 save
Or
~# gpio set uart0 rs232

~# gpio get uart0
rs232
~# microcom /dev/ttyO2 -s 115200
```

2. Input the following command lines in a host device to enable **RS485** on R1 and use a serial communication program (e.g., microcom) to open the port:

```
~# gpio set uart0 rs485 save
Or
~# gpio set uart0 rs485

~# gpio get uart0
rs485
~# microcom /dev/ttyO2 -s 115200
```

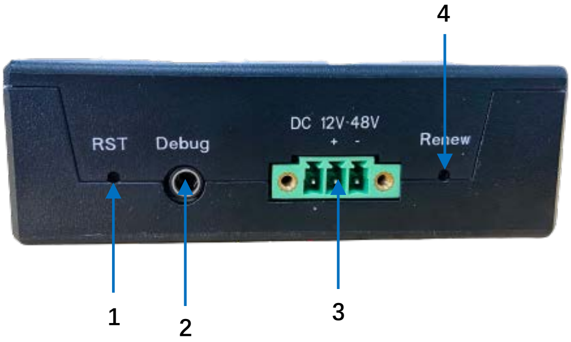
1.5 Definition of Interfaces (C335)

1.5.1 Front view



Item No.	Description	
1	System status indicator	Blinks at system bootup
		Turns solid green after system bootup
		Blinks at system upgrade or configuration cleanup
2	Power indicator	
3	Antenna connector (4G/LTE or Wi-Fi)	
4	LAN 1, shown as ETH0 in VantronOS and works in LAN area by default	
5	LAN 2, shown as ETH1 in VantronOS and works in WAN area by default	
6	Micro SD slot	
7	Micro SIM slot	
8	8 x Serial port status indicator (blinks at data transfer)	

1.5.2 Right side view

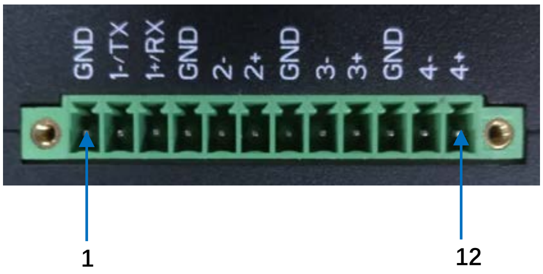


Item No.	Description
1	Reset button
2	Debug port
3	12-48V DC power terminal
4	Renew button (see details below)

Description of the Renew button

- When a system upgrade drive is inserted in the SD slot or USB port, a short press of the button for about 2 seconds will cause the status indicator to blink, suggesting system upgrade is in progress. Once the upgrade finishes, the system will reboot (from eMMC flash).
- When the button is pressed and held for 3-10 seconds, user configurations and custom settings will be removed and the Gateway will be factory reset. Once finishes, the system will reboot.
- When the button is pressed for over 10 seconds, user partitions will be formatted and data in such partitions will be cleared.

1.5.3 Serial port



Pinout description of the serial port:

No.	Signal	Node	Port name	Serial mode	LED indicator
1	GND1	/dev/ttyO2	COM2	RS232 or RS485 (default)	TX1/RX1
2	RS485_1_B/STXD2				
3	RS485_1_A/SRXD3				
4	GND2	/dev/ttyO3	COM3	RS485	TX2/RX2
5	RS485_2_B				
6	RS485_2_A				
7	GND3	/dev/ttyO4	COM4	RS485	RX4/RX4
8	RS485_3_B				
9	RS485_3_A				
10	GND4	/dev/ttyO5	COM5	RS485	RX3/RX3
11	RS485_4_B				
12	RS485_4_A				

COM2 could switch between RS232 and RS485.

Input the following command lines in a host device to enable **RS232** on COM2 and use a serial communication program (e.g., microcom) to open the port:

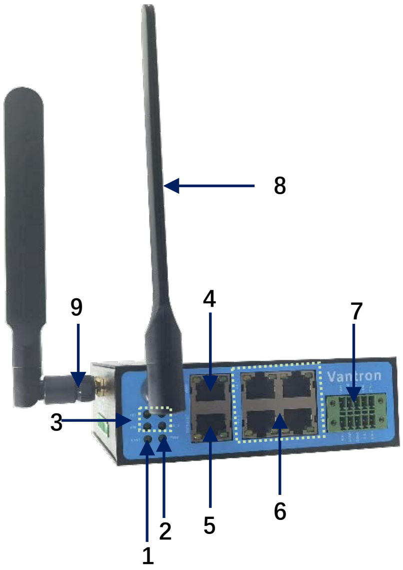
```
~# gpio set uart0 rs232 save
Or
~# gpio set uart0 rs232


~# gpio get uart0
rs232
~# microcom /dev/ttyO2 -s 115200
```

Input the following command lines in a host device to enable **RS485** on COM2 and use a serial communication program (e.g., microcom) to open the port:

```
~# gpio set uart0 rs485 save
Or
~# gpio set uart0 rs485


~# gpio get uart0
rs485
~# microcom /dev/ttyO2 -s 115200
```

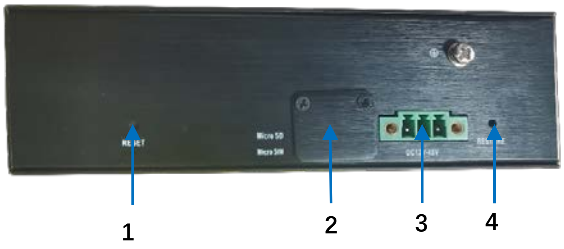
1.6 Definition of Interfaces (C335S)

1.6.1 Front view



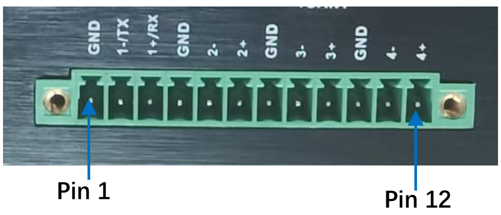
Item No.	Description	
1	System status indicator	Blinks at system bootup
		Turns solid green after system bootup
		Blinks at system upgrade or configuration cleanup
2	Power indicator	
3	4 x Serial port status indicator (blink at data transfer)	
4	WAN port, shown as ETH1 in VantronOS and works in WAN area by default	
5	Debug port, to connect an RJ45 to DB9 adapter for serial debugging	
6	4 x LAN port, shown as ETH0 in VantronOS and work in LAN area by default	
7	AI/DI port	
8	4G antenna 1	
9	4G antenna 2	

1.6.2 Right side view



Item No.	Description
1	Reset button
2	Micro SD & Micro SIM card slots
3	12V-48V DC power terminal
4	Restore button

1.6.3 Serial port



Pinout of the serial port:

No.	Signal	Node	Serial mode	LED indicator
1	GND1	/dev/ttyO1	RS232 or RS485 (default)	485_1
2	RS232_TX / RS485_1_B			
3	RS232_RX / RS485_1_A			
4	GND2	/dev/ttyO2	RS485	485_2
5	RS485_2_B			
6	RS485_2_A			
7	GND3	/dev/ttyO3	RS485	485_3
8	RS485_3_B			
9	RS485_3_A			
10	GND4	/dev/ttyO4	RS485	485_4
11	RS485_4_B			
12	RS485_4_A			

COM1 could switch between RS232 and RS485 (default).

Input the following command lines in a host device to enable **RS232** on COM1 and use a serial communication program (e.g., microcom) to open the port:

```
~# gpio set uart0 rs232 save
Or
~# gpio set uart0 rs232

~# gpio get uart0
rs232
~# microcom /dev/ttyO2 -s 115200
```

Input the following command lines in a host device to enable **RS485** on COM1 and use a serial communication program (e.g., microcom) to open the port:

```
~# gpio set uart0 rs485 save
Or
~# gpio set uart0 rs485

~# gpio get uart0
rs485
~# microcom /dev/ttyO2 -s 115200
```

1.7 Optional Functions

1.7.1 Bluetooth (C335L)

1. Open and initialize HCI device;

```
~# hciconfig hci0 up
```

2. Scan for the Bluetooth devices (the MAC addresses of the Bluetooth devices will be listed below the command line);

```
~# hcitool scan
```

3. Browse all the services available on the target device discovered after the Bluetooth scan and figure out the channel of service “OBEX Object Push”;

   For instance, the Bluetooth device with MAC address 3C:CD:5D:36:9F:A6 is running the following services and the channel of service “OBEX Object Push” is 12.

```
# sdptool browse 3C:CD:5D:36:9F:A6
Browsing 3C:CD:5D:36:9F:A6 ...
Service RecHandle: 0x10000
Service Class ID List:
  "Generic Attribute" (0x1801)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 31
……………………………………………………………….
……………………………………………………………….
Browsing 3C:CD:5D:36:9F:A6 ...
Service Name: OBEX Phonebook Access Server
Service RecHandle: 0x1000a
Service Class ID List:
  "Phonebook Access - PSE" (0x112f)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 19
  "OBEX" (0x0008)
Profile Descriptor List:
  "Phonebook Access" (0x1130)
    Version: 0x0101
```

```
Service Name: OBEX Object Push
Service RecHandle: 0x1000b
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 12
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0102
……………………………………………………………….
……………………………………………………………….
```

- If the Gateway does not support service “OBEX Object Push”, please input the command line below:

```
~# sdptool add --channel = 12 OPUSH
```

4. Use “obex_test” command to send a test file to the Bluetooth device, i.e., obex_test -b <MAC address of the Bluetooth device > <channel>;

   For instance, to send the test file to the aforementioned Bluetooth device:

```
~# obex_test -b 3C:CD:5D:36:9F:A6 12
> c
[Note: to connect to the device]

…………..
Connect OK!
[Note: the Bluetooth device is connected to the gateway.]

Version: 0x10. Flags: 0x00
> p /etc/usb-mode.json
[Note: The arguments following “p” is the path of the test file to be sent.]

PUT file (local)> name=send.txt, size=9
PUT remote filename (default: send.txt)>
Going to send 9 bytes
…………..
PUT successful!
[Note: The test file is sent to the Bluetooth device]

> q
[Note: to exit obex_test]
```

5. Exit “obex_test”, and enable page and search scan so that the target Bluetooth device is discoverable;

```
~# hciconfig hci0 piscan
```

6. Run obexd service to receive the test file, i.e., obexd -a -n -r <path for saving the file>;

   For instance, the test file is stored in “ /tmp”:

   ```
   ~# export
   DBUS_SESSION_BUS_ADDRESS="unix:path=/var/run/dbus/system_bus_socket"
   # obexd -a -n -r /tmp/
   ```

7. After the file transfer, disable page and search scan and the device will not be discoverable.

   ```
   ~# hciconfig hci0 noscan
   ```

After you go through the steps above, the test finishes.

If you need shut down the HCI device, input the command line below:

```
~# hciconfig hci0 down
```

To rename the HCI device, input the command line below:

```
~# hciconfig hci0 name “Bluez 5.21 test”

~# hciconfig hci0 down

~# hciconfig hci0 up
```

1.7.2 CAN (C335)

The following describes the communication of two C335 gateways via CAN protocol. If you have customized end devices and special data protocols requiring gateway customization from Vantron, please contact your sales executive.

1. Prepare two C335 gateways, and the CAN connection shall be as follows:

Gateway A		Gateway B
CANH	<->	CANH
CANL	<->	CANL
Transmit Data	<->	Receive Data

2. Run “candump” command on Gateway B and set the Baud rate between 100000 (100kbps) and 1000000 (1000kbps);

   ```
   ~# ip link set can0 type can bitrate 100000
   ~# ifconfig can0 up
   ~# candump can0
   ```

3. Transmit data from Gateway A;

```
~# ifconfig can0 up
~# cansend can0 5A1#11.2233.44556677.88
```

4. The data will be printed on Gateway B.

1.7.3 GPIO (C335)

The pins on the GPIO header are described below.

Name	Pin #
"gpio_in1" (gpio0_22)	22
"gpio_in2" (gpio0_23)	23
"gpio_out1" (gpio0_26)	26
"gpio_out2" (gpio0_27)	27

1. Write a GPIO pin number to “/sys/class/gpio/export” to export the pin, for instance pin 22:

```
~# echo 22 > /sys/class/gpio/export
```

2. Set the pin direction as input or output (in for input and out for output);

```
~# echo out > /sys/class/gpio/gpio22/direction
```

3. If you configured an output pin in the prior step, now you can set its value to 0 or 1 (corresponding to low or high) as follows:

```
~# echo 0 > /sys/class/gpio/gpio22/value  [set it low], or
~# echo 1 > /sys/class/gpio/gpio22/value  [set it high]
```

4. Read the GPIO value;

```
~# cat /sys/class/gpio/gpio22/value
```

5. When you finish using the pin, just unexport it. To do this, write the pin number to the unexport file:

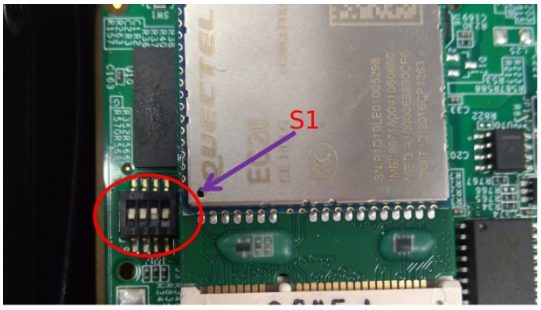
```
~# echo 22 > /sys/class/gpio/unexport
```

1.8 System Boot

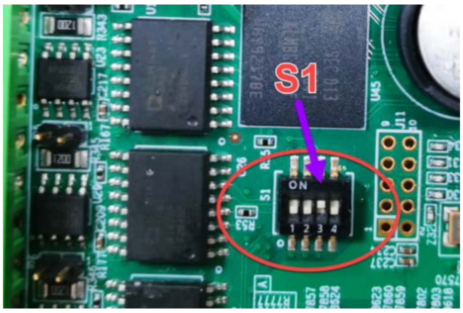
The system boots up from eMMC by default.

1.8.1 System boot and eMMC flashing from an SD card

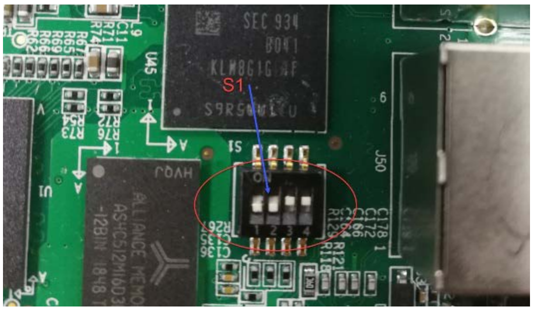
1. Open the Gateway enclosure;
2. Set DIP switch S1 to off:off:on:off (C335L & C335S) or off:off:on:on (C335) as shown below;



C335L



C335S



C335

3. Make a bootable SD card/USB drive;
   1) Insert the SD card/USB drive into a Linux host and input a dmesg command to get the path of the SD card/USB drive (for instance, /dev/sdb);
   2) Input the following command line to unzip the release package (C335S for instance) sent from Vantron;

```
~# unzip XOS_sd2mmc_VT-M2M-C335S “version number”.zip
```

   3) You will get the files as explained below:

```
├── build.date                                                    //Image built date
├── sd2emmc.sh                                                    //Script for SD card bootup
├── XOS_sd2mmc_VT-M2M-C335S_Vxxxxxxx.Fxxxxxxx.img                 //Bootup image
├── XOS_sd2mmc&sdAutoUpgrade_VT-M2M-C335S_ Vxxxxxxx.Fxxxxxxx.sha256sum
                                                                  //sha256sum file
└── XOS_sdAutoUpgrade_VT-M2M-C335S_ Vxxxxxxx.Fxxxxxxx.img.gz      //Upgrade image
```

4) Run the following command with root account to make a bootable SD card:

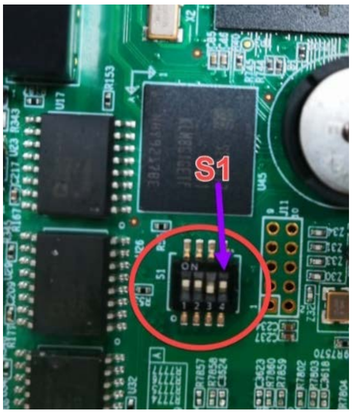
```
~# sudo ./sd2emmc.sh /dev/sdb
```

- Replace /dev/sdb with the correct SD card path.
- Removal of the SD card before a completion message pops up will cause the process to fail.
- Remove the SD card and run the command again in case the making process fails.

4. Insert the SD card to the slot;
5. Power the Gateway on. After the system boots up, the status indicator will turn solid green and eMMC flashing finishes.

1.8.2 System boot from eMMC flash

1. Open the Gateway enclosure;
2. Set DIP switch S1 to on:on:off:on as shown below;



C335S for illustration

3. Power the Gateway on. After the system boots up from eMMC, the status indicator will turn solid green.

CHAPTER 2

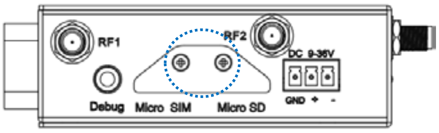
GETTING STARTED

2.1 Setting up the Gateway

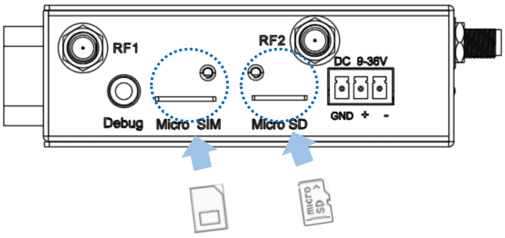
Before you proceed with the configuration of the Gateway, follow the steps below to finish hardware connection.

For C335L

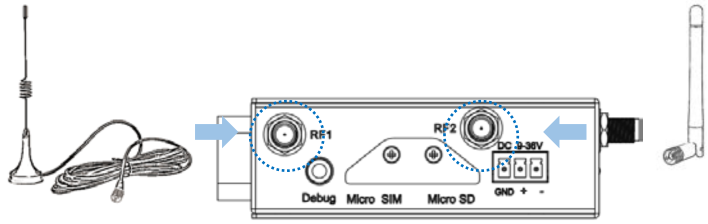
1. Use the mounting bracket and screws to install the Gateway to a secure place;
2. Unscrew the cover plate from the SIM & SD slots on the left side of the Gateway;



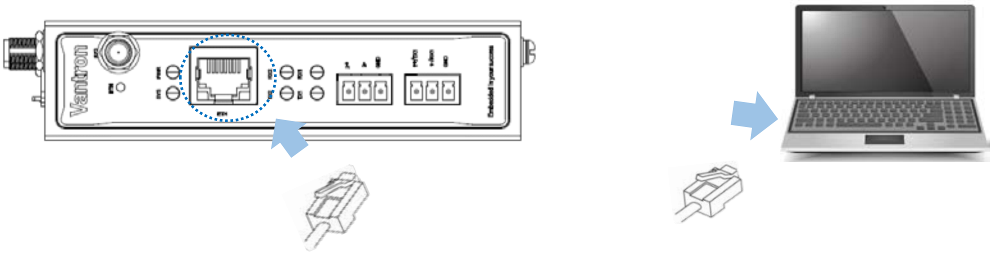
3. Insert an activated SIM card and an SD card into the corresponsive slots with the gold-colored contacts/pins facing down;



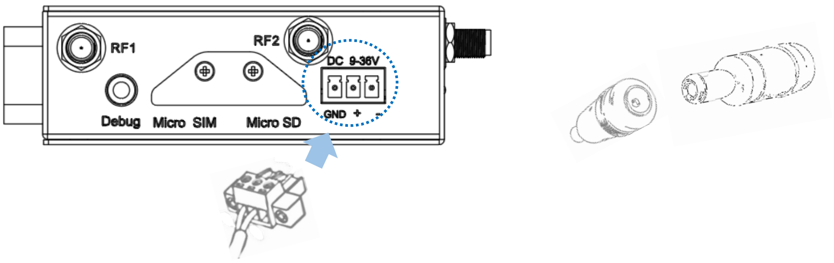
4. Push the cards to secure them;
5. Place the cover plate back over the slots and tighten the screws;
6. Install the rubber stick antenna to the Wi-Fi/BT antenna connector (RF2) and the sucker antenna to the 4G/LTE antenna connector (RF1), then tighten the connectors;



7. Connect one end of an Ethernet cable to the Ethernet port of the Gateway and the other to your PC (the Ethernet port is used as a LAN port by default);



8. Connect the terminal end of the DC power connector to the power terminal of the Gateway and the round end to the adapter;



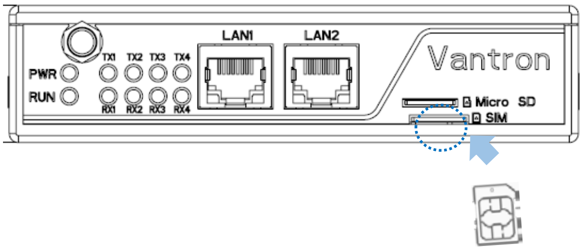
9. Plug the adapter to a DC power outlet that meets the supply voltage requirement (9V to 36V) to power up the Gateway;

10. The power and status indicators will turn solid green upon power application.

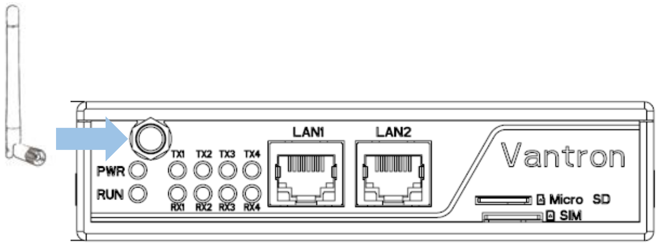
The antennas might be different from what used for illustration here. Should you have any trouble installing the antennas, please contact the sales executive for solution.

For C335

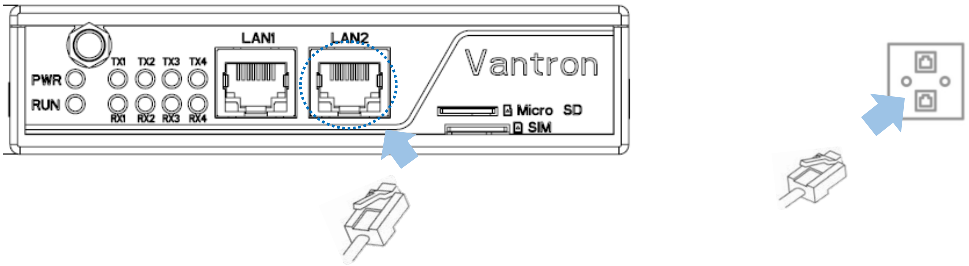
1. Use the mounting bracket and screws to install the Gateway to a secure place;
2. Insert an activated SIM card into the SIM slot with the gold-colored contacts facing up;



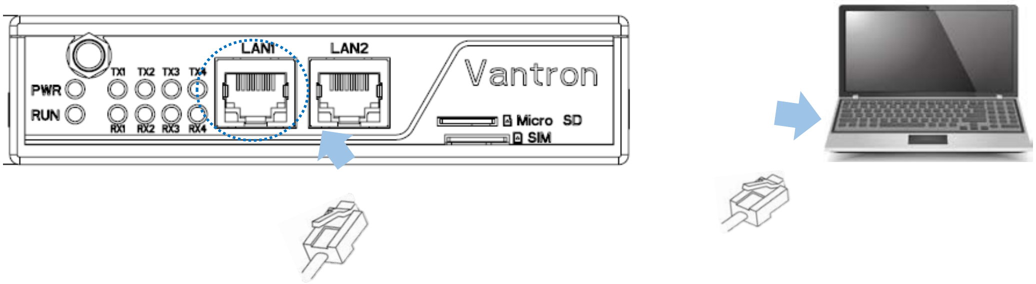
3. Push the SIM card to secure it;
4. Install the Micro SD card likewise with the gold-colored pins facing down;
5. Install the antenna (function depending on user selection) to the antenna connector and tighten the connector;



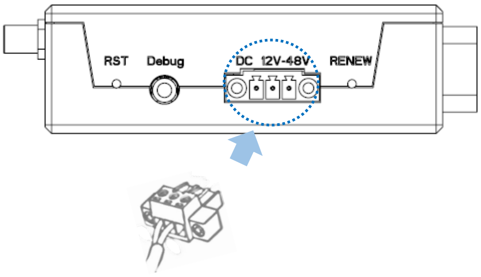
6. Connect one end of an Ethernet cable to LAN2 port (WAN) of the Gateway and the other to a live Ethernet port;

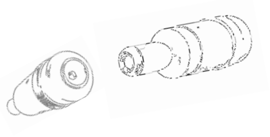


7. Connect one end of an Ethernet cable to LAN1 port (LAN) of the Gateway and the other to your PC;



8. Connect the terminal end of the DC power connector to the power terminal of the Gateway and the round end to the adapter;





9. Plug the adapter to a DC power outlet that meets the supply voltage requirement (12V to 48V) to turn on the Gateway;

10. The power and status indicators will turn solid green upon power application.

Skip steps 6 & 7 if you choose wireless network connection.

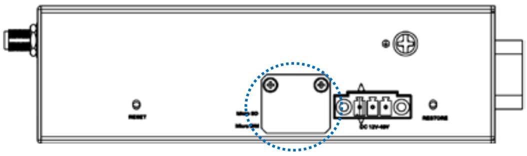
The antennas might be different from what used for illustration here. Should you have any trouble installing the antennas, please contact the sales executive for solution.

The min-PCIe module in C335 is either used for 4G/LTE or Wi-Fi & Bluetooth, so the function of the antenna depends on which communication module you choose.

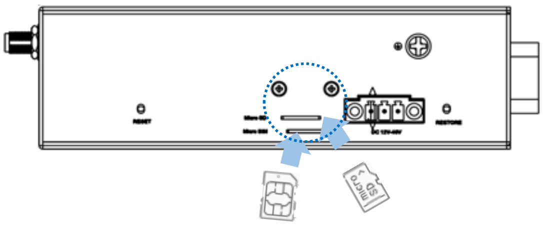
For C335S

1. Use the mounting bracket and screws to install the Gateway to a secure place;

2. Unscrew the cover plate from the SIM & SD slots on the right side of the Gateway;



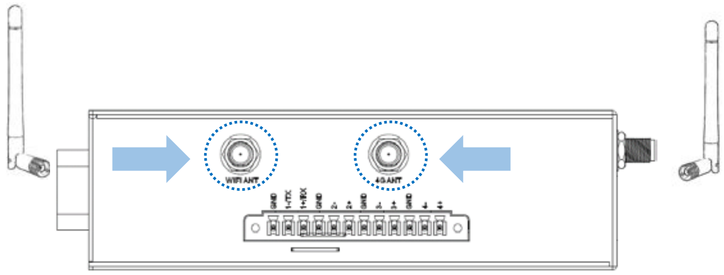
3. Insert an activated SIM card with the gold-colored contacts facing up and an SD card with the gold-colored pins facing down;



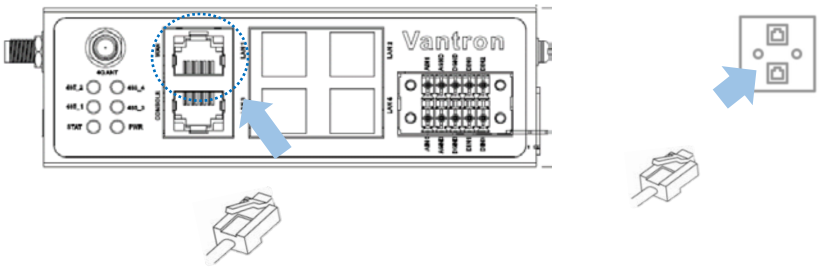
4. Push the cards to secure them;

5. Place the cover plate back over the slots and tighten the screws;

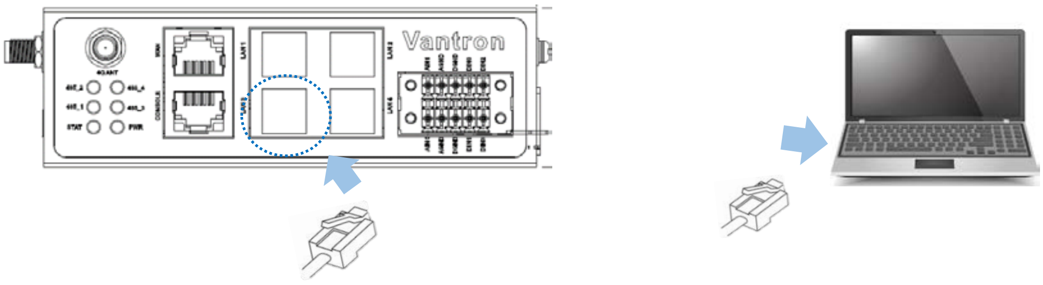
6. Install the antennas to the antenna connectors and tighten the connectors;



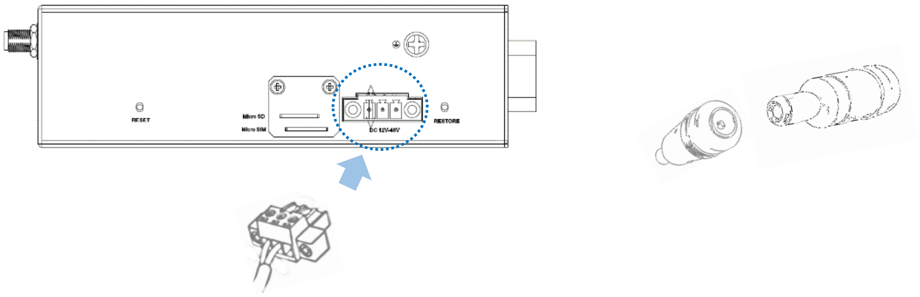
7. Connect one end of an Ethernet cable to the WAN port of the Gateway and the other to a live Ethernet port;



8. Connect one end of another Ethernet cable to any of the LAN port and the other to your PC;



9. Connect the terminal end of the DC power connector to the power terminal of the Gateway and the round end to the adapter;



10. Plug the adapter to a DC power outlet that meets the supply voltage requirement (12V to 48V) to turn on the Gateway;

11. The power and status indicators will turn solid green upon power application.

Skip steps 7 & 8 if you choose wireless network connection.

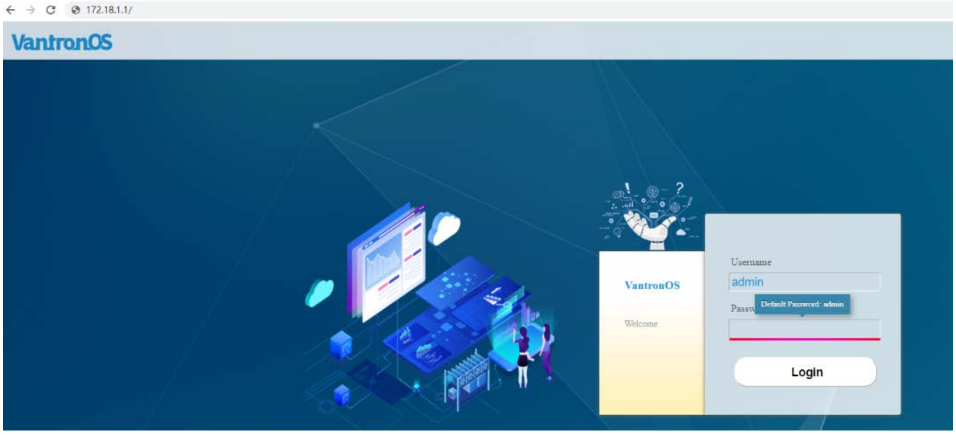
The antennas might be different from what used for illustration here. Should you have any trouble installing the antennas, please contact the sales executive for solution.

Customers may choose a 4G/LTE module that is AT&T and Verizon pre-certified. Before you use a SIM card to provide wireless network access for the Gateway, make sure the SIM card is activated with data plans (refer to 3.5.3 4G/LTE for application of the SIM card from the carriers if the module is pre-certified).

2.2 Gateway Login

The Gateway is designed to allow network connectivity with minimal configuration. That said, you can configure the network settings and customize the Gateway from VantronOS interface.

1. Input the default web login address of VantronOS in your browser: http://172.18.1.1/.
   - Default user name: **admin** / Super user: **root**
   - Default password: **admin** / Super user password: **rootpassword**



2. You'll be directed to the web interface of VantronOS, and you can configure and change the settings of the Gateway here.
3. For SSH login, use the IP address: 172.18.1.1 (default).
   - Port: **22**
   - Account: **root**
   - Password: **rootpassword**

- The web login address coincides with the LAN port IP address of the Gateway, so you might have to change the login address when you reset the IP address.
- Refer to **SSH Access** included in 3.9.3 for more details.
- The latest version of Google Chrome or Firefox is recommended.

2.3 Interfacing with Vantron Gateway Management Platform

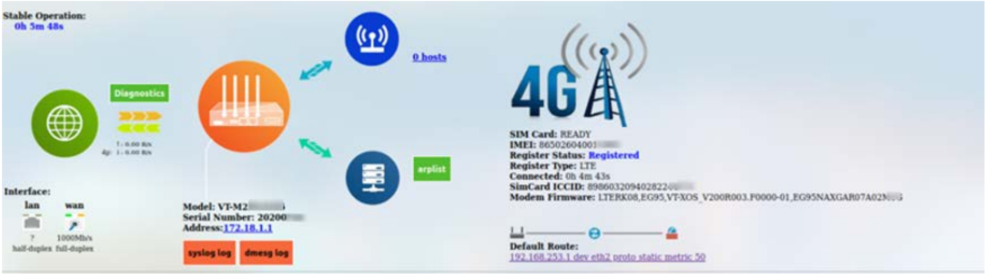
BlueSphere GWM, Vantron gateway management platform, is a web-based console where multiple gateways/routers could be managed in groups to provide the required information. If the gateway/router supports data collection/upload protocols, users can also set up the data collection tasks, collection variables, uploading rules, etc. on the platform.

Before you can use the BlueSphere GWM for remote management of gateways/routers, please make sure the following prerequisites are met:

- You have obtained a license for login to the BlueSphere GWM
- DMP agent is installed on the target gateway/router
- DMP agent is "enabled" on the configuration page in VantronOS (Refer to [3.7.4 DMP Agent](#) for the configuration)
- The serial number of the gateway/router is added to the BlueSphere GWM

2.4 Network Connectivity

When the Gateway has network connections, the status page may display like below.



Stable Operation:
0h 5m 48s

Interface:
lan wan
? 1000Mb/s
half-duplex full-duplex

Model: VT-M2[redacted]
Serial Number: 20200[redacted]
Address: 172.18.1.1

SIM Card: READY
IMEI: 86502604001[redacted]
Register Status: Registered
Register Type: LTE
Connected: 0h 4m 43s
SimCard ICCID: 898603209402822[redacted]
Modem Firmware: LTERK08,EG95,VT-XOS_V200R003.F0000-01,EG95NAXGAR07A02[redacted]

Default Route:
192.168.253.1 dev eth2 proto static metric 50

2.4.1 Ethernet Network Connectivity

The default WAN settings allow your gateway to join an Ethernet network without any additional configuration.

The Gateway uses a DHCP protocol to assign IP addresses, subnet masks, default gateway addresses, and Domain Name System (DNS) server addresses by default. If you switch DHCP to static protocol, you'll need to set all of these IP addresses manually.

2.4.2 Wi-Fi Connectivity

The Gateway is configurable to both client mode and AP mode.

For C335 gateways, however, Wi-Fi and 4G/LTE are designed to be alternative. Therefore, if you choose Wi-Fi for wireless connection, 4G/LTE will not be available, and vice versa.

Refer to 3.5.2 Wireless (WIFI) for advanced settings of the wireless network.

2.4.3 Mobile Network Connectivity

For customers using a SIM card for network connectivity of the Gateway, the 4G/LTE function under **Network** tab allows you to make changes to the cellular network settings. Before you configure for 4G/LTE network, be sure to activate and install the SIM card properly.

Refer to 3.5.3 4G/LTE for advanced settings of the mobile network.

2.5 Custom Settings

As Vantron provides an SDK, users can upload their own scripts or programs or IPK packages to the Gateway and set them to run at startup or to support certain protocols.

Refer to 3.7 Customization for advanced settings of customized packages and programs.

CHAPTER 3

GATEWAY SETUP VIA VANTRONOS

3.1 Introduction to VantronOS

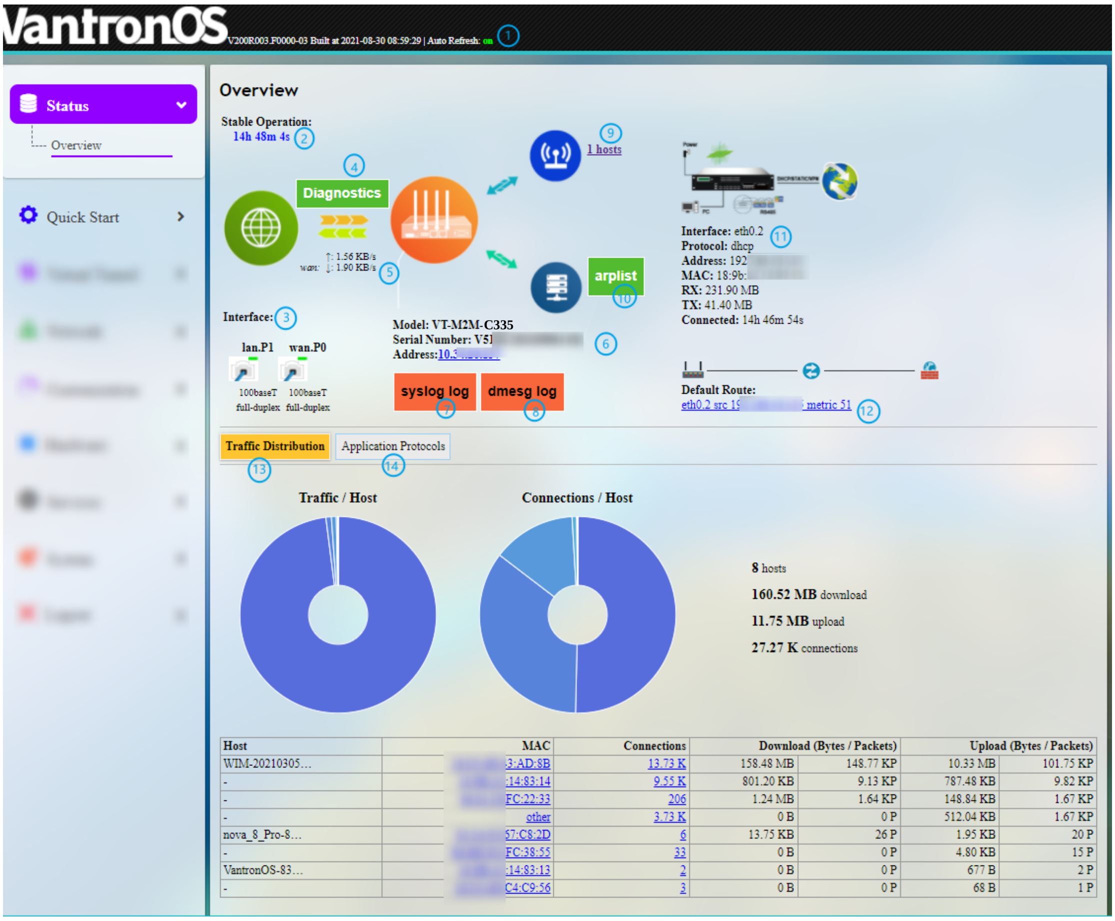
Featuring independent development of system and functions, VantronOS is an intelligent operating system that interprets the joint efforts of Vantron team based on Linux system and embedded hardware. It employs modular design and plug-in expansion design ideas, running Linux kernel with firewall to secure Internet connection of devices without being attacked. The UI interface is based on the MVC framework to provide a simple and efficient setting entry. VantronOS also realizes connectivity with cloud management platforms, including self-developed BlueSphere GWM, Azure, Alibaba Cloud, Huawei Cloud, and RootCloud to allow users to monitor, operate and diagnose remote devices without sending technical support engineer to the equipment site, achieving interconnection and interaction between users and Industrial Internet of Things.

In the following sections, a collection of configurations and functions will be introduced covering the entire C335 series gateways, therefore, the actual web portal displaying your gateway configurations may be different from the screenshots here.

Use the navigation pane of this document for the specific configurations/functions you wish to explore.

3.2 Status

This page provides the overall information of the Gateway, including stable operation duration, number of devices connected to the Gateway via wireless or Ethernet connection, default routing, hardware information, traffic statistics, etc.



V200R003.F0000-03 Built at 2021-08-30 08:59:29 | Auto Refresh: on

Overview

Stable Operation:
14h 48m 4s

wan: ↑: 1.56 KB/s
↓: 1.90 KB/s

Interface:

Model: VT-M2M-C335
Serial Number: V51[redacted]
Address: 10.3[redacted]

Interface: eth0.2
Protocol: dhcp
Address: 192[redacted]
MAC: 18:9b:[redacted]
RX: 231.90 MB
TX: 41.40 MB
Connected: 14h 46m 54s

Default Route:
eth0.2 src 19[redacted] metric 51

8 hosts
160.52 MB download
11.75 MB upload
27.27 K connections

Host		MAC	Connections	Download (Bytes / Packets)		Upload (Bytes / Packets)	
WIM-20210305…		[redacted]3:AD:8B	13.73 K	158.48 MB	148.77 KP	10.33 MB	101.75 KP
-		[redacted]:14:83:14	9.55 K	801.20 KB	9.13 KP	787.48 KB	9.82 KP
-		[redacted]FC:22:33	206	1.24 MB	1.64 KP	148.84 KB	1.67 KP
-		other	3.73 K	0 B	0 P	512.04 KB	1.67 KP
nova_8_Pro-8…		[redacted]57:C8:2D	6	13.75 KB	26 P	1.95 KB	20 P
-		[redacted]FC:38:55	33	0 B	0 P	4.80 KB	15 P
VantronOS-83…		[redacted]:14:83:13	2	0 B	0 P	677 B	2 P
-		[redacted]C4:C9:56	3	0 B	0 P	68 B	1 P

Description of the numbered areas

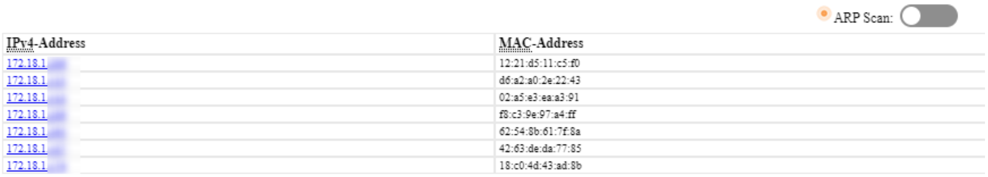
1. Firmware version and auto refresh on/off
2. Stable running time of the Gateway since network connection
3. Current working status of Ethernet ports
4. A collection of network diagnostic tools
5. Instant default exit traffic
6. Model, serial number, and IP address of the gateway in use
7. System log information
8. Kernel log information

9. Number of clients connected to the Gateway via Wi-Fi

Wi-Fi settings will be accessed upon a click of the number.

10. Address information of clients connected to the Gateway

ARP scan is disabled by default, and it can be enabled when you click on **arplist** icon and toggle on ARP scan in the pop-up.

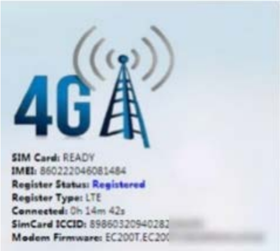


ARP Scan:

IPv4-Address	MAC-Address
172.18.1[redacted]	12:21:d5:11:c5:f0
172.18.1[redacted]	d6:a2:a0:2e:22:43
172.18.1[redacted]	02:a5:e3:ea:a3:91
172.18.1[redacted]	f8:c3:9e:97:a4:ff
172.18.1[redacted]	62:54:8b:61:7f:8a
172.18.1[redacted]	42:63:de:da:77:85
172.18.1[redacted]	18:c0:4d:43:ad:8b

11. Details of the access port

The image illustration varies when the Gateway has cellular connection.



SIM Card: READY
IMEI: 860222046081484
Register Status: Registered
Register Type: LTE
Connected: 0h 14m 42s
SimCard ICCID: 8986032094028[redacted]
Modem Firmware: EC200T.EC20[redacted]

12. Default route currently used by the Gateway

13. Traffic distribution of clients connected to the Gateway displayed by MAC addresses

Clicking on each MAC address in the table at the page bottom will get the detailed traffic information of the clients.

14. Application layer protocols

HTTPS, HTTP, and POP3S represent the top 3 protocols for data download and upload. HTTPS, HTTP and DNS represent the top 3 protocols for device connection.

3.3 Quick Start

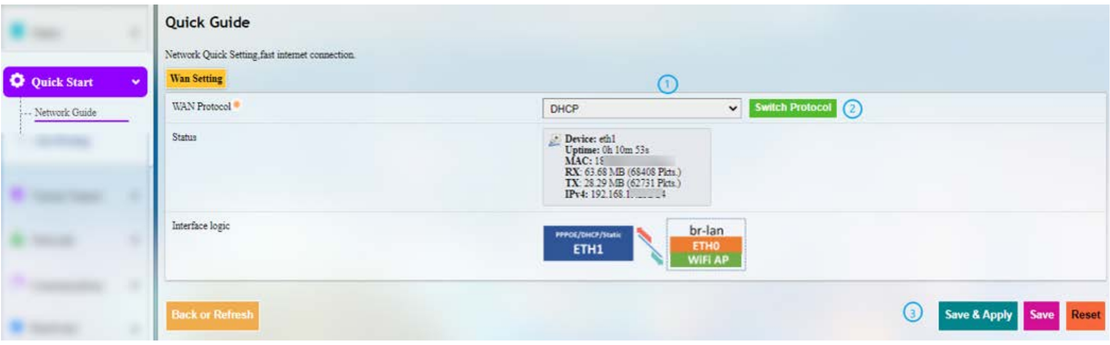
3.3.1 Network Guide

This page provides a quick guide to such functions as rapid networking of the Gateway and a display of the network port status and interface logic diagram. Refer to 3.5.1 Interfaces for advanced settings.

- **Application of the network setup wizard will clear user-defined configuration parameters.**
- **Since C335L has only one Ethernet port that works in LAN area, WAN port settings are not applicable to this model unless you configure it as a WAN port, in which case, WiFi AP is bounded with the network bridge (br-lan) and ETH0 is to connect the higher-level network for PPPOE/DHCP/Static mode settings.**
- **For C335, Wi-Fi and 4G/LTE are designed to be alternative. Therefore, if you choose 4G/LTE for wireless connection, WiFi AP/client connections will not be applicable.**
- **Please refer to 1.4/1.5/1.6 Definition of Interfaces for the definition of the ports.**

3.3.2 WAN setting – DHCP

DHCP: **ETH0** and **WiFi (AP mode)** are bounded with the network bridge (br-lan). **ETH1** is designed as the WAN port to connect the higher-level network. The cellular interface does not work under this mode.



Quick Guide

Network Quick Setting,fast internet connection.

WAN Protocol: DHCP

Status:
Device: eth1
Uptime: 0h 10m 53s
MAC: [redacted]
RX: 63.68 MB (68408 Pkts.)
TX: 28.29 MB (62731 Pkts.)
IPv4: 192.168.1.[redacted]

DHCP setup procedures:

Step 1: Select **DHCP** for **WAN Protocol**;

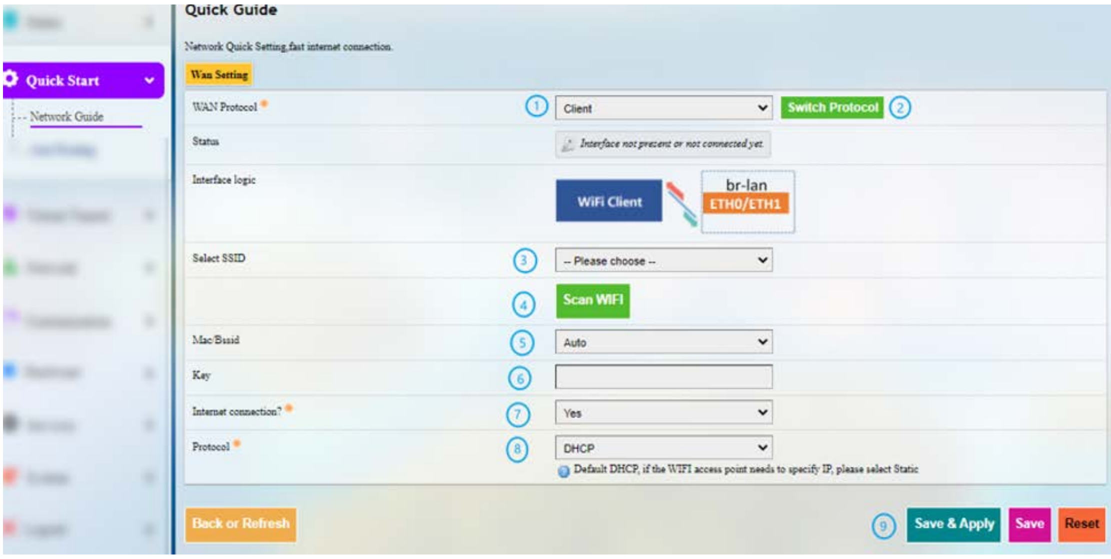
Step 2: Click to switch the protocol to **DHCP**;

Step 3: Click **Save & Apply**.

- Switch of WAN protocol will reset the network port topology and network parameters to default values.

3.3.3 WAN Setting – Client

Client: **ETH0** and **ETH1** are bounded with the network bridge (br-lan). **WiFi Client** is designed as the WAN port.



Quick Guide

Network Quick Setting,fast internet connection.

Wan Setting

WAN Protocol * ① Client

Status: Interface not present or not connected yet

Interface logic: WiFi Client — br-lan ETH0/ETH1

Select SSID ③ -- Please choose --

Mac/Bssid ⑤ Auto

Key ⑥

Internet connection? * ⑦ Yes

Protocol * ⑧ DHCP

Default DHCP, if the WIFI access point needs to specify IP, please select Static

Client setup procedures:

Step 1: Select **Client** for **WAN Protocol**;

Step 2: Click to switch the protocol to **Client**;

Step 3: Select the Wi-Fi network that the Gateway is to connect;

Step 4: Click **Scan WIFI** to refresh the Wi-Fi list if the target Wi-Fi network is not identified;

Step 5: Select the MAC address of the AP to be connected (leave it to Auto if not certain);

Step 6: Enter the password of the Wi-Fi network to be connected;

Step 7: Confirm if the Wi-Fi network is accessible. If not, select **No** as the heartbeat detection method might be different;

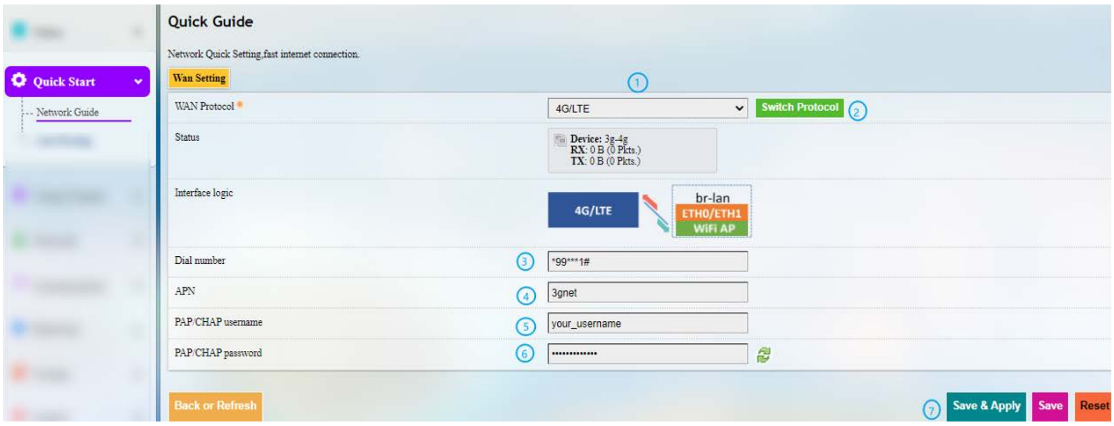
Step 8: Select the protocol for IP addressing (DHCP by default);

Step 9: Click **Save & Apply**.

3.3.4 WAN Setting – 4G/LTE

Before you configure for 4G/LTE connection, make sure you have inserted the activated SIM card in the slot and the LTE antennas are installed. Refer to 3.5.3 4G/LTE for advanced settings.

4G/LTE: ETH0, **ETH1** and **WiFi AP** are bounded with the network bridge (br-lan). Normally, if the Gateway is using a common 4G module, the device port for 4G/LTE communication displayed under the protocol will be “3g-4g” which is the WAN port. When using a carrier pre-certified 4G module provided by Vantron, the device port for 4G/LTE communication displayed under the protocol will be “eth2” which is the WAN port.



Quick Guide

Network Quick Setting,fast internet connection.

Wan Setting

WAN Protocol: 4G/LTE

Status: Device: 3g-4g
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Dial number: *99***1#

APN: 3gnet

PAP/CHAP username: your_username

PAP/CHAP password: ••••••••••••••

4G/LTE setup procedures:

Step 1: Select **4G/LTE** for **WAN Protocol**;

Step 2: Click to switch the protocol to **4G/LTE**;

Step 3: Enter the SIM card ICCID provided by the carrier;

Step 4: Enter the APN of the SIM card inserted (provided by the carrier);

Step 5: Enter the username provided by the carrier for PAP/CHAP authentication;

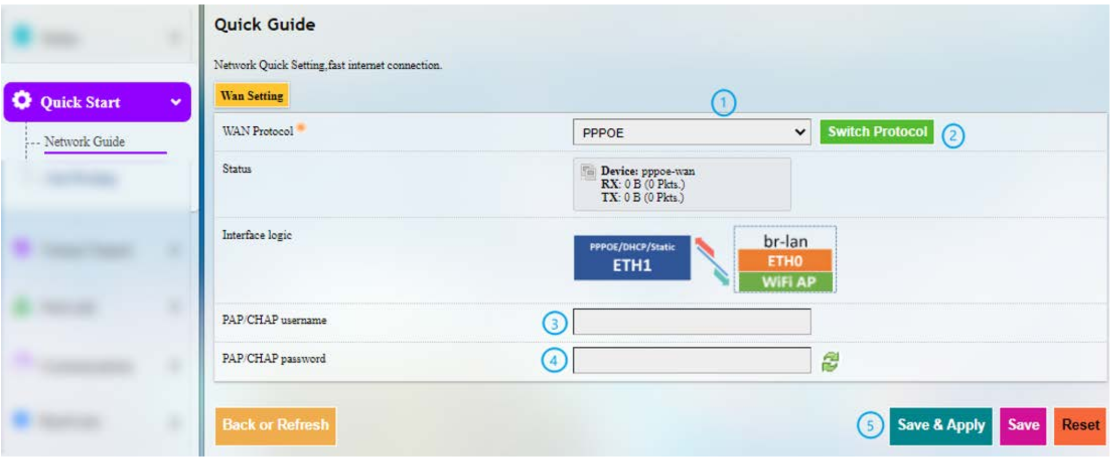
Step 6: Enter the password provided by the carrier for PAP/CHAP authentication;

Step 7: Click **Save & Apply**.

- Leave the field as is if not available.
- PAP/CHAP username and password are to be specified only if your carrier has setup APN with user name and password.

3.3.5 WAN Setting – PPPoE

PPPoE: ETH0 and **WiFi AP** are bounded with the network bridge (br-lan). **ETH1** is designed as the WAN port to connect the higher-level network.



Quick Guide

Network Quick Setting,fast internet connection.

Wan Setting

WAN Protocol: PPPOE

Status: Device: pppoe-wan
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

Interface logic

PAP/CHAP username

PAP/CHAP password

PPPoE setup procedures:

Step 1: Select **PPPoE** for **WAN Protocol**;

Step 2: Click to switch the protocol to **PPPoE**;

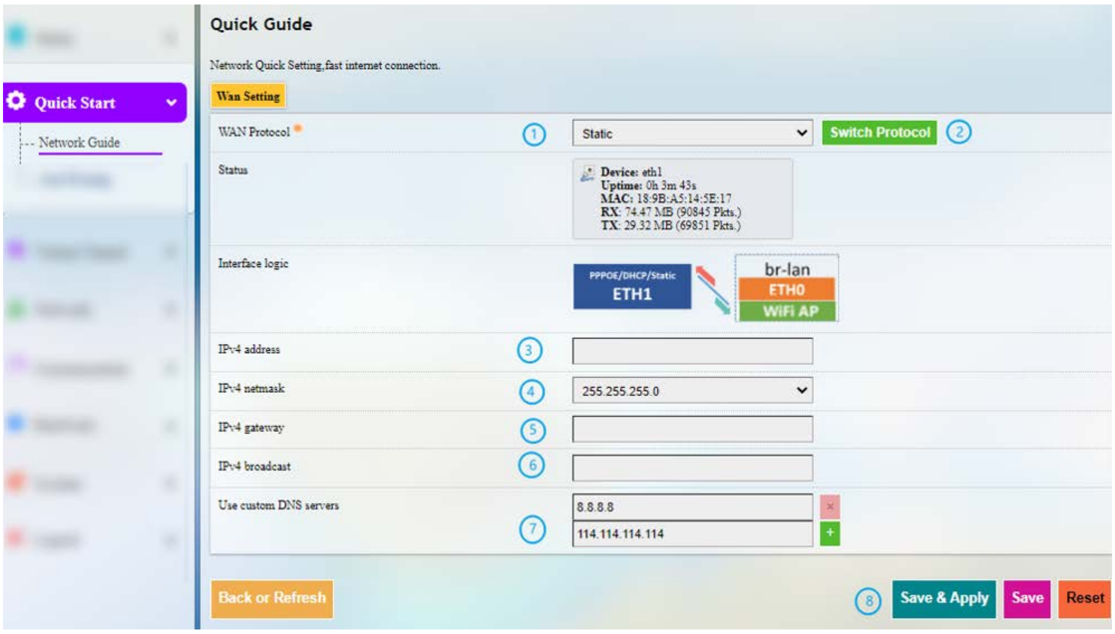
Step 3: Enter the username for PAP/CHAP authentication;

Step 4: Enter the password for PAP/CHAP authentication;

Step 5: Click **Save & Apply**.

3.3.6 WAN Setting – Static

Static: ETH0 and **WiFi AP** are bounded with the network bridge (br-lan). **ETH1** is designed as the WAN port to connect the higher-level network.



Network Quick Setting,fast internet connection.

WAN Protocol: Static

Status: Device: eth1
Uptime: 0h 3m 43s
MAC: 18:9B:A5:14:5E:17
RX: 74.47 MB (90845 Pkts.)
TX: 29.32 MB (69851 Pkts.)

Interface logic

IPv4 address:

IPv4 netmask: 255.255.255.0

IPv4 gateway:

IPv4 broadcast:

Use custom DNS servers: 8.8.8.8
114.114.114.114

Static protocol setup procedures:

Step 1: Select **Static** for **WAN Protocol**;

Step 2: Click to switch the protocol to **Static**;

Step 3: Specify the IPv4 address;

Step 4: Specify the subnet mask;

Step 5: Specify the IPv4 gateway;

Step 6: Specify the IPv4 broadcast;

Step 7: Set the DNS server;

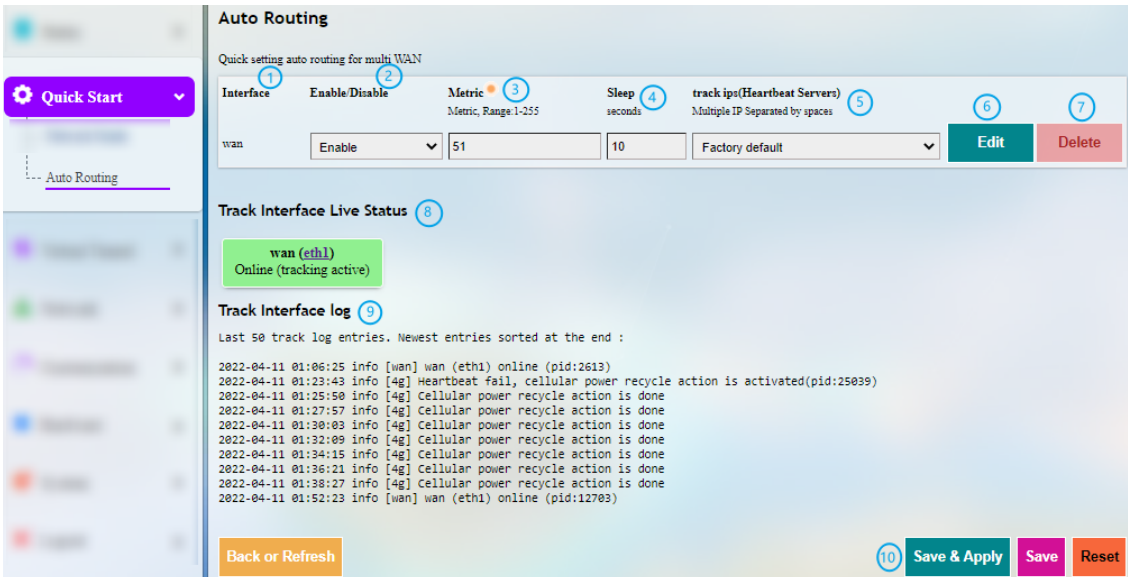
Step 8: Click **Save & Apply**.

Leave the field as is if not available.

3.3.7 Auto Routing

Automatic routing features functions briefed below:

- Enable heartbeat detection upon connection to a single 4G network interface;
- When there are multiple WAN ports, users can specify the data port according to the metric priority of the Gateway. When one of the ports is offline, auto routing helps automatically switch to other available ports. When the failed port recovers and comes online again, it can automatically re-connect to the network;
- Initiate automatic recognition, add the automatically detected port when a network port plugs in/out.



Auto Routing

Quick setting auto routing for multi WAN

Interface	Enable/Disable	Metric Metric, Range:1-255	Sleep seconds	track ips(Heartbeat Servers) Multiple IP Separated by spaces
wan	Enable	51	10	Factory default

Track Interface Live Status

wan (eth1)
Online (tracking active)

Track Interface log

```
Last 50 track log entries. Newest entries sorted at the end :

2022-04-11 01:06:25 info [wan] wan (eth1) online (pid:2613)
2022-04-11 01:23:43 info [4g] Heartbeat fail, cellular power recycle action is activated(pid:25039)
2022-04-11 01:25:50 info [4g] Cellular power recycle action is done
2022-04-11 01:27:57 info [4g] Cellular power recycle action is done
2022-04-11 01:30:03 info [4g] Cellular power recycle action is done
2022-04-11 01:32:09 info [4g] Cellular power recycle action is done
2022-04-11 01:34:15 info [4g] Cellular power recycle action is done
2022-04-11 01:36:21 info [4g] Cellular power recycle action is done
2022-04-11 01:38:27 info [4g] Cellular power recycle action is done
2022-04-11 01:52:23 info [wan] wan (eth1) online (pid:12703)
```

Description of the numbered areas

1. Interface for route tracking
2. Enable/Disable route tracking
3. Metric settings (The smaller the number, the higher the priority)
4. Tracking interval, defined as from the completion of one tracking to the initiation of the next tracking
5. Traceable IP (heartbeat server)

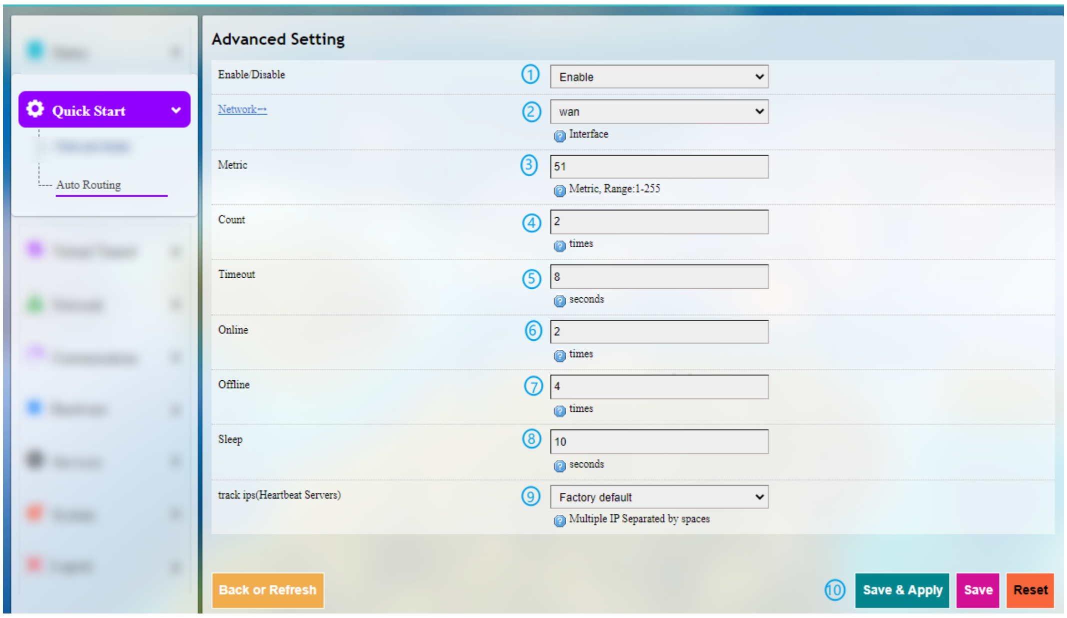
ℹ Use spaces to separate multiple IP addresses. If you do not have internet access or private network, set the traceable IP to that of the upper layer gateway.

6. Edit rules
7. Delete rules
8. Status overview of interfaces tracked

9. Interface track log with the newest entry at the bottom

10. **Save & Apply** the changes made

Clicking on the **Edit** button will direct you to the rule editing page as follows.



Advanced Setting

Enable/Disable	①	Enable
Network→	②	wan Interface
Metric	③	51 Metric, Range:1-255
Count	④	2 times
Timeout	⑤	8 seconds
Online	⑥	2 times
Offline	⑦	4 times
Sleep	⑧	10 seconds
track ips(Heartbeat Servers)	⑨	Factory default Multiple IP Separated by spaces

Description of the numbered areas

1. Enable/Disable route tracking
2. Select the interface for route tracking
3. Metric settings (The smaller the number, the higher the priority)
4. The maximum retry number for a single tracking failure
5. The maximum timeout for a single tracking failure
6. Number of online interfaces

   If a tracking is confirmed successful, the interface will be considered online.

7. Number of offline interfaces

   If a tracking is confirmed failed and the confirmation number reaches/exceeds the pre-set value, the interface will be considered offline.

8. Tracking interval, defined as from the completion of one tracking to the initiation of the next tracking
9. Traceable IP (heartbeat server)

   Use spaces to separate multiple IP addresses. If you do not have internet access or private network, set the traceable IP to that of the upper layer device.

10. **Save & Apply** the settings

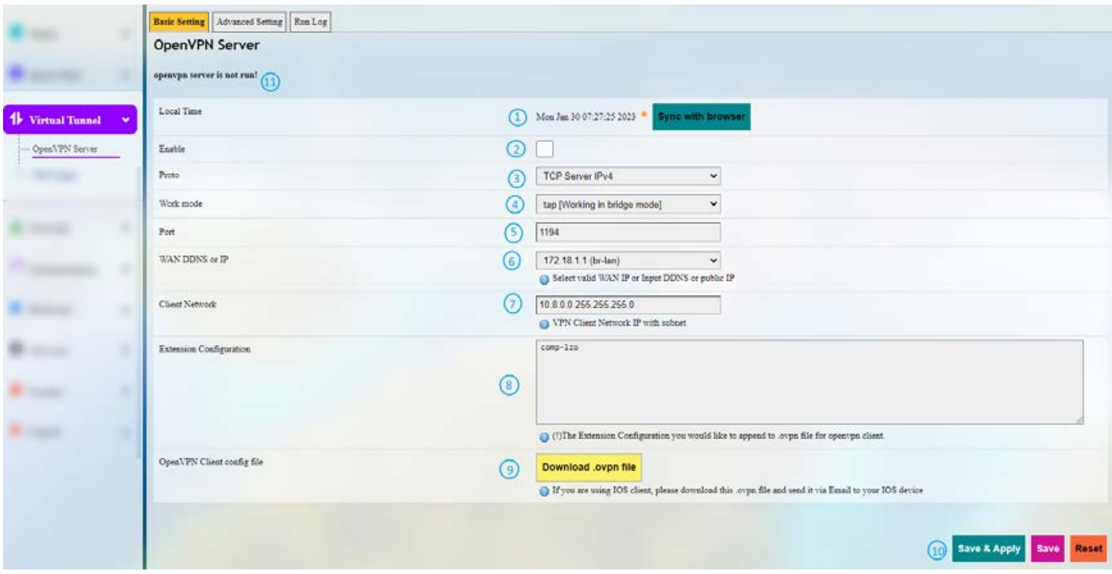
3.4 Virtual Tunnel

A virtual private network (VPN) lets you use the Internet to securely access your network remotely. The Gateway supports such VPN protocols as OpenVPN, L2TP, PPTP, and IPSec to ensure data confidentiality and undisturbedness.

You can configure the Gateway either as an OpenVPN server or a client based on needs.

3.4.1 OpenVPN Server

Basic and advanced settings for OpenVPN server are accessible on this page.



OpenVPN Server

openvpn server is not run! (11)

Local Time (1) Mon Jan 30 07:27:25 2023

Enable (2) □

Proto (3) TCP Server IPv4

Work mode (4) tap [Working in bridge mode]

Port (5) 1194

WAN DDNS or IP (6) 172.18.1.1 (br-lan)
Select valid WAN IP or Input DDNS or public IP

Client Network (7) 10.8.0.0 255.255.255.0
VPN Client Network IP with subnet

Extension Configuration (8) comp-lzo
(!)The Extension Configuration you would like to append to .ovpn file for openvpn client

OpenVPN Client config file (9)
If you are using IOS client, please download this .ovpn file and send it via Email to your IOS device

(10)

Follow the steps below to build an OpenVPN Server:

1. Synchronize the Gateway time with the browser (local) time;
2. Enable the server;
3. Select a protocol;

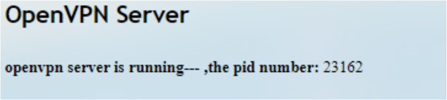
TCP provides an ordered delivery of data from user to server (and vice versa), whereas UDP is not dedicated to end-to-end communications, nor does it check the readiness of the receiver.

4. Select a working mode between **tap** and **tun**;

Tap bridges two ethernet segments at different locations, so use **tap** if you need to connect to remote network (remote desktops, PLCs, controllers, etc.). If you only need network connection, then use **tun**.

5. Set a port that the server is to monitor;
6. Choose the WAN port IP or DDNS or public IP that the server is to monitor;

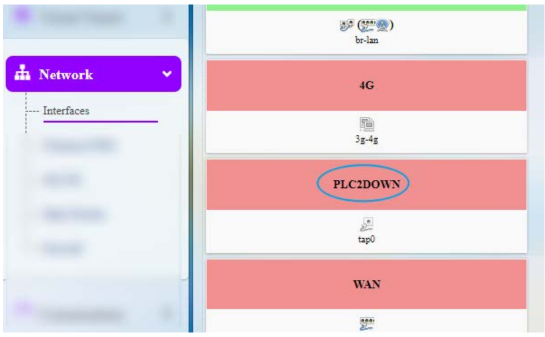
7. Assign a virtual IP network for the clients;
8. Input the extension configuration for the client;
9. Download the configuration file for client connection (not necessary for server setup);
10. Save the above settings and apply;
11. When the configuration finishes, the status will change as follows.



OpenVPN Server

openvpn server is running--- ,the pid number: 23162

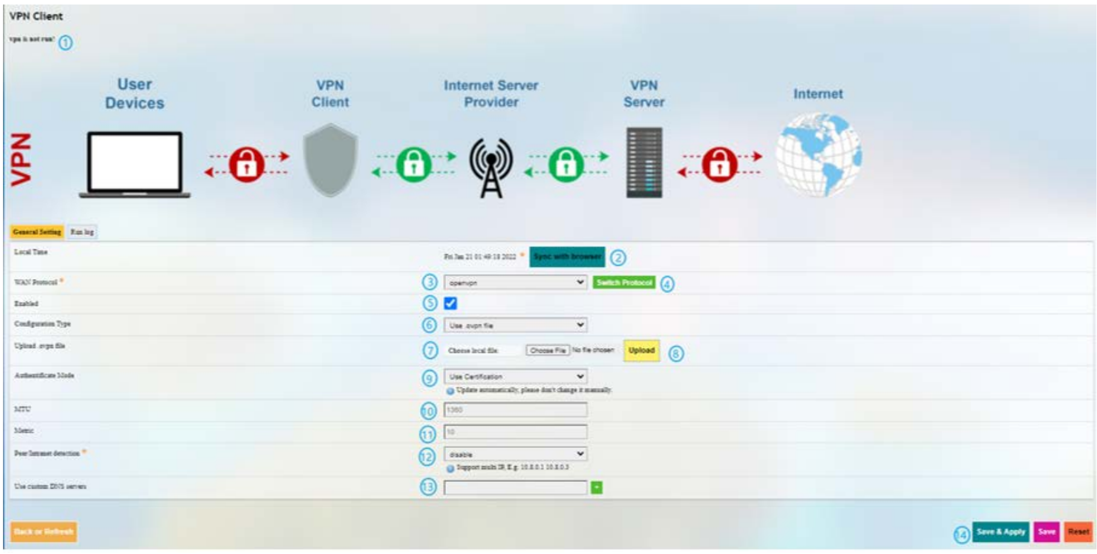
Once the OpenVPN server is set up, an interface named PLC2DOWN will be added automatically so that users could make further changes.



3.4.2 VPN Client

To configure a VPN client on the Gateway, navigate to **Virtual Tunnel > VPN Client** for specific settings.

Before enabling the VPN client, please update the time zone of the client with that of the browser, and complete a time synchronization.



VPN Client

vpn is not run! ①

Local Time	Fri Jan 21 01:49:18 2022 * ②
WAN Protocol *	③ openvpn ④
Enabled	⑤ ☑
Configuration Type	⑥ Use .ovpn file
Upload .ovpn file	⑦ Choose local file: No file chosen ⑧
Authentificate Mode	⑨ Use Certification Update automatically, please don't change it manually.
MTU	⑩ 1360
Metric	⑪ 10
Peer Internet detection *	⑫ disable Support multi IP, E.g. 10.8.0.1 10.8.0.3
Use custom DNS servers	⑬

⑭

Description of the numbered areas

1. Status of the VPN
2. Synchronize your VPN time with the browser (local) time
3. Select a WAN protocol for the virtual line (OPENVPN & PPTP available)
4. Click to switch to the protocol
5. Check or uncheck the box to enable/disable the protocol

Only when the protocol is enabled will subsequent options be displayed. The subsequent options correspond to which one you have selected as WAN protocol.

6. If you select OpenVPN as the WAN protocol, you'll have to continue with the configuration using a .ovpn file

If you select PPTP as the WAN protocol, you shall input the PPTP server IP, user name and password as indicated.

7. Select the local .ovpn file for configuration
8. Upload the local profile
9. Select to use a certification or username & password as for authentication
10. MTU settings
11. Metric settings

The smaller the number, the higher the priority.

12. Disable/Enable heartbeat detection

Select **custom** and enter the IP address for heartbeat detection to enable the mechanism.

13. Enter custom DNS Servers
14. **Save & Apply** the settings

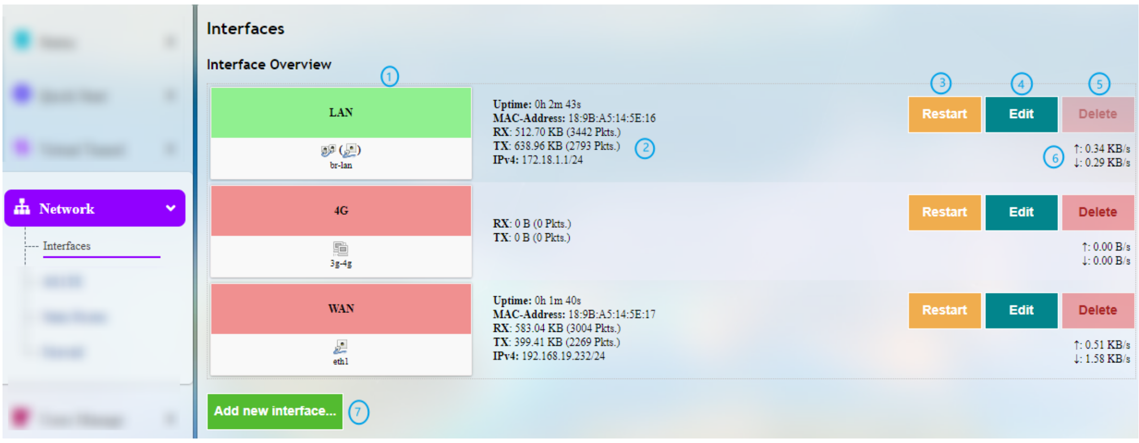
3.5 Network

Despite the fact that the **Network Guide** page under **Quick Start** tab provides access to quick settings of the network, you can check the detailed information of the networks under **Network** tab and make changes accordingly.

No matter where you make the changes to the network, previous settings will be overridden once you save and apply the current settings.

3.5.1 Interfaces

All the network interfaces currently available and configurable are displayed under **Network > Interfaces.**



Uptime: 0h 2m 43s
MAC-Address: 18:9B:A5:14:5E:16
RX: 512.70 KB (3442 Pkts.)
TX: 638.96 KB (2793 Pkts.)
IPv4: 172.18.1.1/24

↑: 0.34 KB/s
↓: 0.29 KB/s

RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)

↑: 0.00 B/s
↓: 0.00 B/s

Uptime: 0h 1m 40s
MAC-Address: 18:9B:A5:14:5E:17
RX: 583.04 KB (3004 Pkts.)
TX: 399.41 KB (2269 Pkts.)
IPv4: 192.168.19.232/24

↑: 0.51 KB/s
↓: 1.58 KB/s

Description of the numbered areas

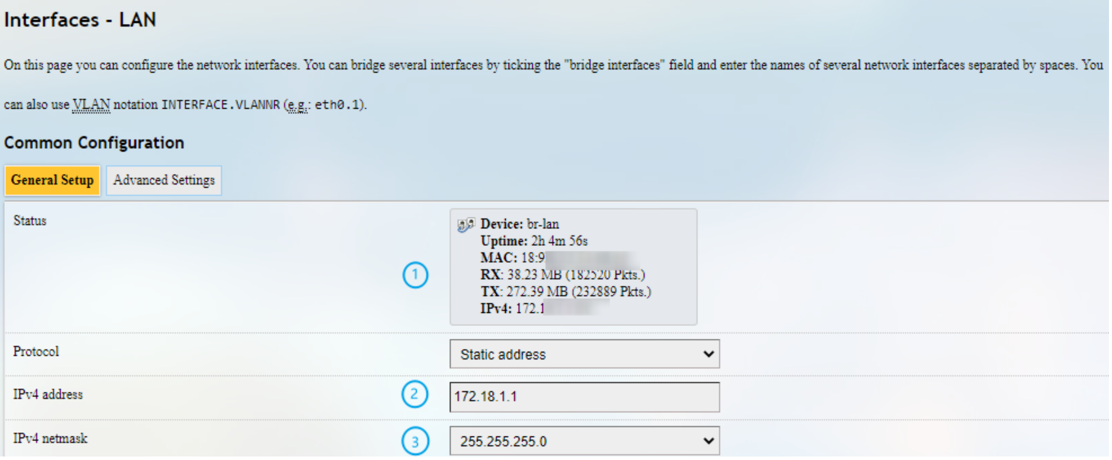
1. Interface overview
2. Interface details
3. Restart the interface manually
4. Edit the interface settings
5. Delete the interface (available only when you log in as a root user)
6. Instantaneous traffic of the interface
7. Add a new interface (available only when you log in as a root user)

The interfaces may differ from what is shown above as certain models do/do not have the module that make corresponding interface available.

The interfaces will be described in detail in the following sections.

LAN

Upon a click on the **Edit** button behind **LAN**, you'll be directed to the **General Setup** page by default.



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

General Setup | Advanced Settings

Status: Device: br-lan
Uptime: 2h 4m 56s
MAC: 18:9[redacted]
RX: 38.23 MB (182520 Pkts.)
TX: 272.39 MB (232889 Pkts.)
IPv4: 172.1[redacted]

Protocol: Static address

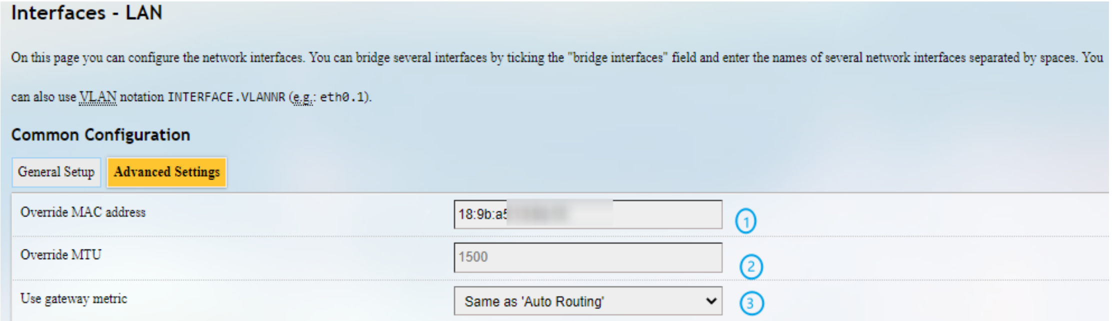
IPv4 address: 172.18.1.1

IPv4 netmask: 255.255.255.0

Description of the numbered areas

1. Status of the interface
2. IP address of the LAN interface
3. Select a LAN interface subnet mask

In the common configuration area, click **Advanced Settings**:



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

General Setup | Advanced Settings

Override MAC address: 18:9b:a[redacted]

Override MTU: 1500

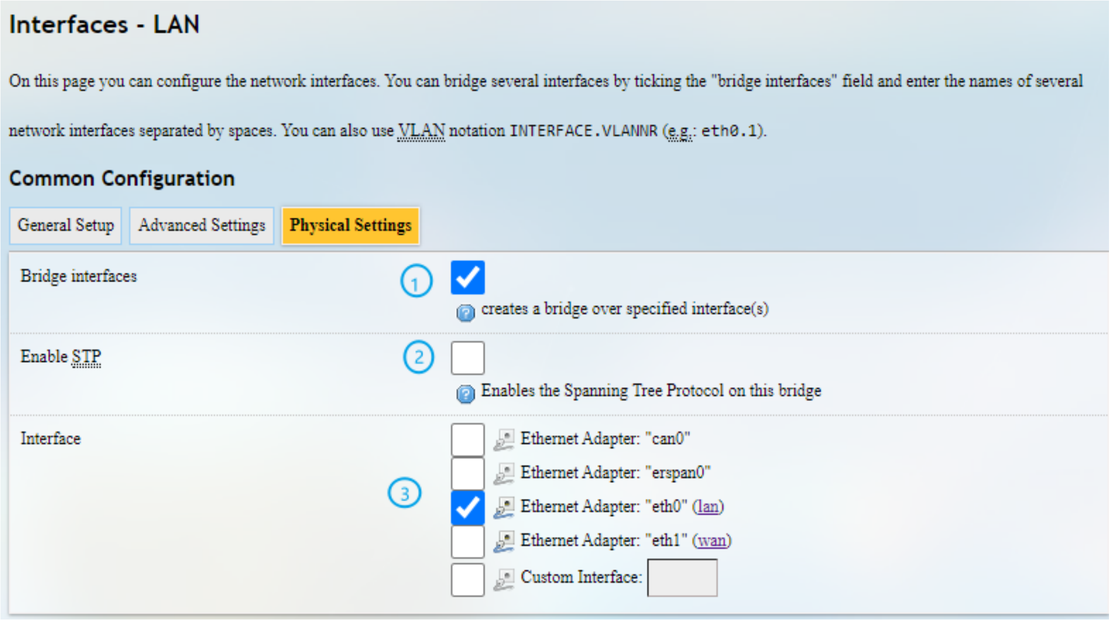
Use gateway metric: Same as 'Auto Routing'

Description of the numbered areas

1. MAC address cloning
2. MTU settings
3. Keep the metric same as Auto Routing or customize the metric

Be sure to save the settings before you exit the page.

When you log in to VantronOS as a root user (**password: rootpassword**), there will be a **Physical Settings** tab next to **Advanced settings**, which allows you to configure the LAN port for network bridge.



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Bridge interfaces ☑
creates a bridge over specified interface(s)

Enable STP □
Enables the Spanning Tree Protocol on this bridge

Interface
□ Ethernet Adapter: "can0"
□ Ethernet Adapter: "erspan0"
☑ Ethernet Adapter: "eth0" (lan)
□ Ethernet Adapter: "eth1" (wan)
□ Custom Interface:

Description of the numbered areas

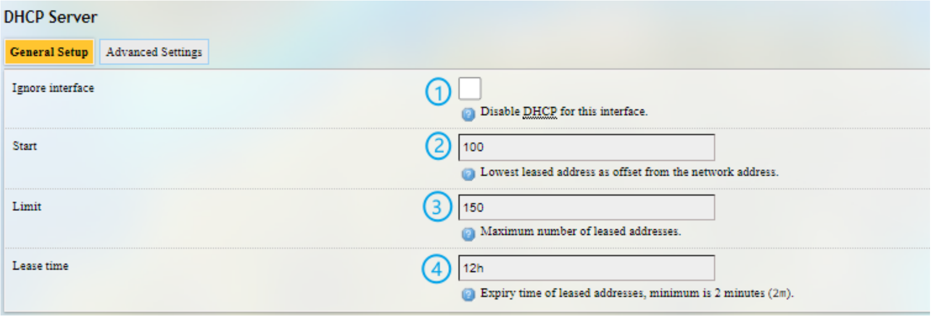
1. Enable the interface for network bridge

2. Enable STP protocol

3. Select the interface for bridge connection

LAN – DHCP

In the **General Setup** page of DHCP Server under **Common Configuration** of LAN port**,** DHCP could be set up with more details:



DHCP Server

Ignore interface □
Disable DHCP for this interface.

Start 100
Lowest leased address as offset from the network address.

Limit 150
Maximum number of leased addresses.

Lease time 12h
Expiry time of leased addresses, minimum is 2 minutes (2m).

Description of the numbered areas

1. Disable DHCP service

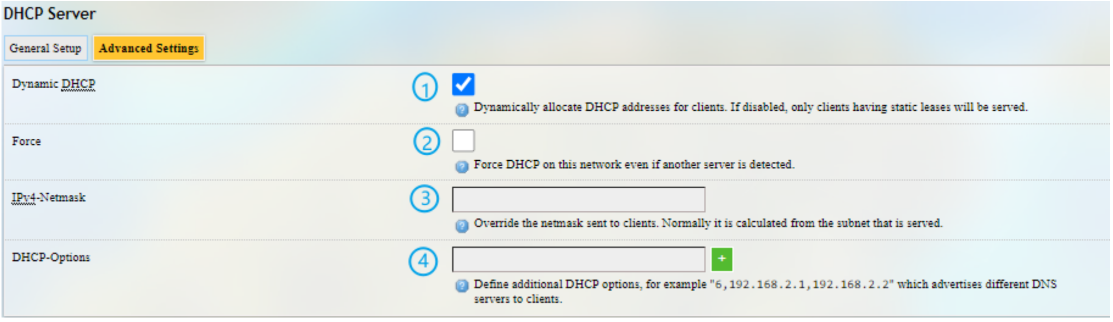
If disabled, DHCP service will not be available to devices connected to the LAN interface..

2. DHCP start address

3. Maximum number of leased addresses (up to 150)

4. Expiry time of leased addresses (min. 2m)

Advanced Settings of DHCP Server:



DHCP Server

Dynamic DHCP ☑
Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force □
Force DHCP on this network even if another server is detected.

IPv4-Netmask
Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options
Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

Description of the numbered areas

1. Enable dynamic allocation of addresses for clients

If disabled, clients shall have static leases.

2. Force enablement of DHCP service (to bypass other servers)
3. Override the netmask sent to clients

Normally it is calculated from the subnet that is served

4. Add different DNS servers for clients

Be sure to save the settings before you exit the page. Clicking on **Back or Refresh** will get you back to interface settings.

4G

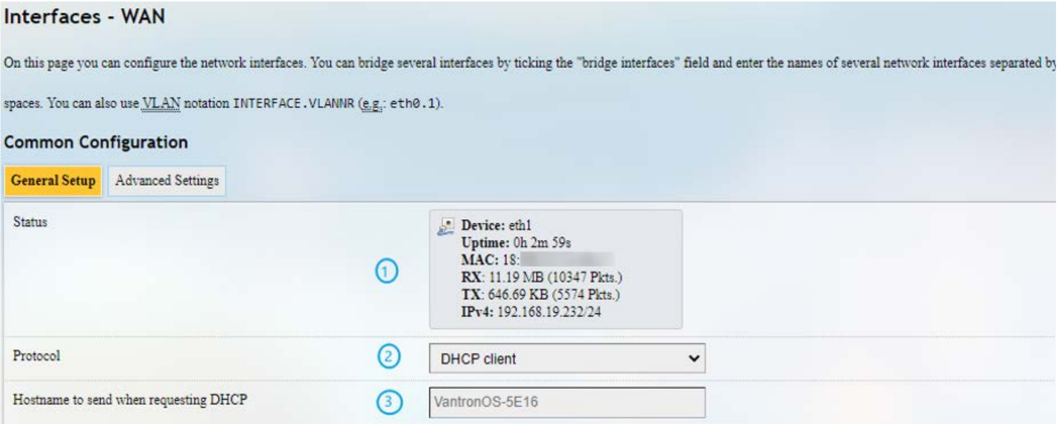
You will be redirected to 4G/LTE configuration page upon a click of the **Edit** button behind 4G interface. Refer to 3.5.3 4G/LTE for details.

WAN

General and advanced settings of WAN interface are configured here.

WAN – DHCP Client

General DHCP protocol settings for WAN interface are shown below.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

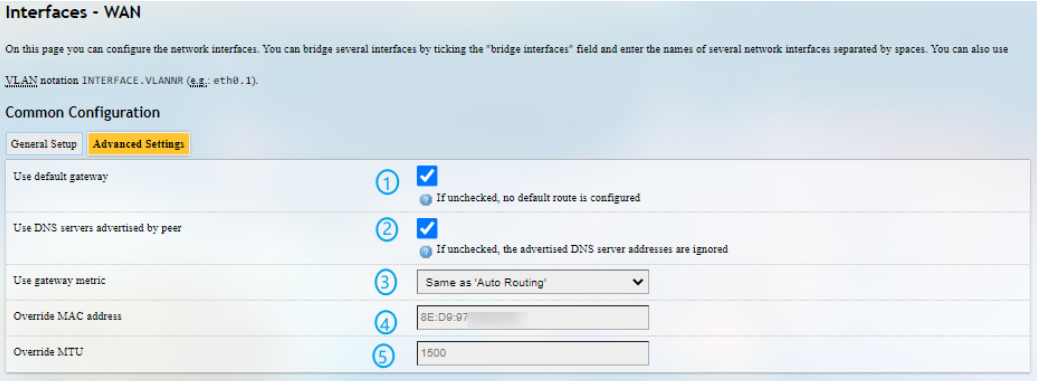
General Setup | Advanced Settings

Status	1	**Device:** eth1 **Uptime:** 0h 2m 59s **MAC:** 18:[redacted] **RX:** 11.19 MB (10347 Pkts.) **TX:** 646.69 KB (5574 Pkts.) **IPv4:** 192.168.19.232/24
Protocol	2	DHCP client
Hostname to send when requesting DHCP	3	VantronOS-5E16

Description of the numbered areas

1. Status of the WAN port
2. Select DHCP client as WAN protocol or switch to another protocol
3. Hostname to send when requesting DHCP

Advanced DHCP protocol settings for WAN interface are shown below.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup | Advanced Settings

Use default gateway	1	☑ If unchecked, no default route is configured
Use DNS servers advertised by peer	2	☑ If unchecked, the advertised DNS server addresses are ignored
Use gateway metric	3	Same as 'Auto Routing'
Override MAC address	4	8E:D9:97[redacted]
Override MTU	5	1500

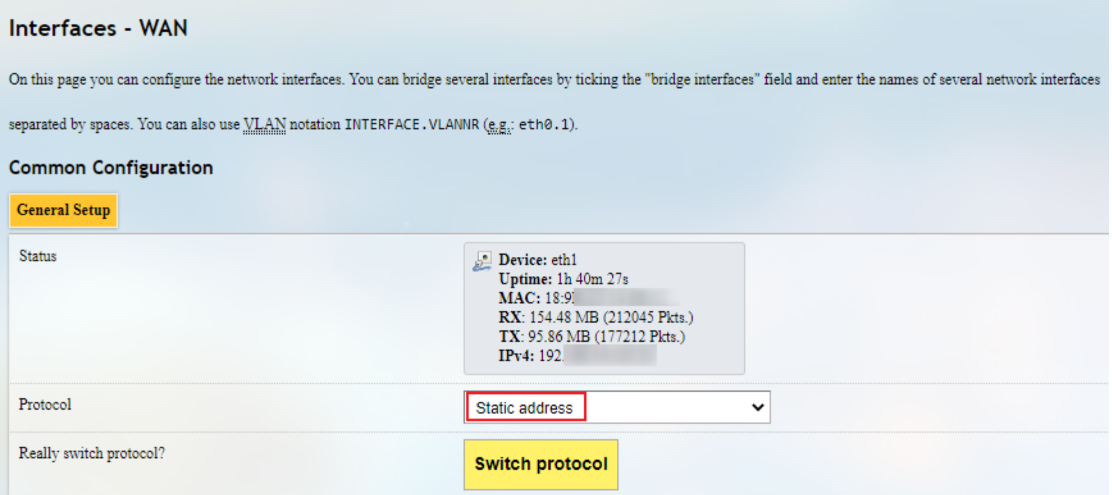
Description of the numbered areas

1. Enable **Use default gateway**
2. Enable **Use DNS server advertised by peer**
3. Gateway metric
4. MAC address cloning
5. Network MTU

Be sure to save the settings before you exit the page.

WAN – Static Address

To activate static address protocol, select **Static address** in the drop-down list in the **General Setup** page as the protocol and click **Switch protocol**.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Status: **Device:** eth1
Uptime: 1h 40m 27s
MAC: 18:9[redacted]
RX: 154.48 MB (212045 Pkts.)
TX: 95.86 MB (177212 Pkts.)
IPv4: 192.[redacted]

Protocol: Static address

Really switch protocol?

Upon click of **Switch protocol**, you'll need to input the IPv4 address, subnet mask, IPv4 gateway, and the IPv4 broadcast. Custom DNS server could also be added.

- Leave the field as is if not available.
- When static address protocol is selected, DHCP server will be automatically disabled.
- The advanced settings are basically same as those for DHCP protocol.

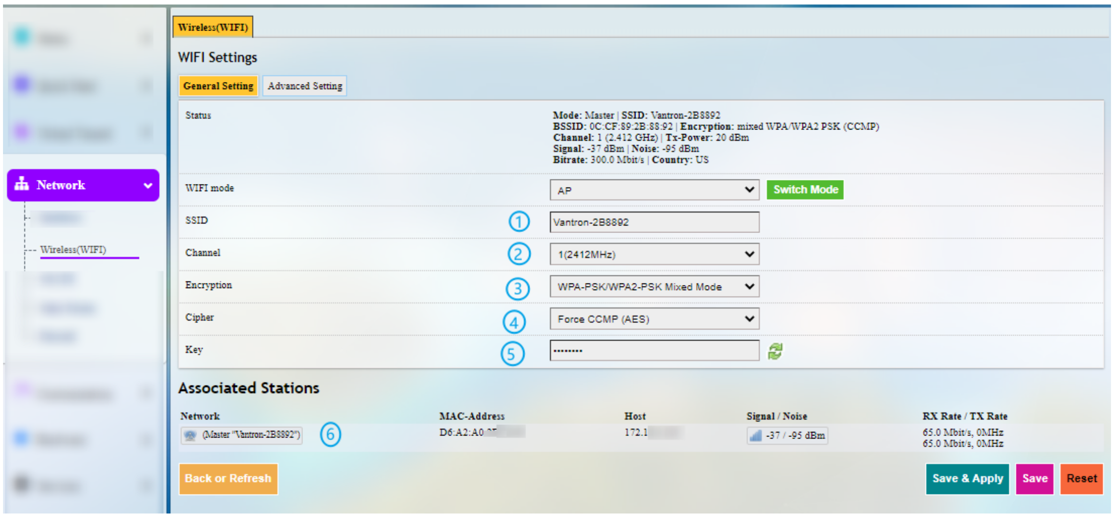
WAN – PPPoE

The general and advanced PPPoE settings for the WAN port are literally the same as those above. Clicking on **Back or Refresh** will get you back to interface settings.

3.5.2 Wireless (WIFI)

You can switch between AP and client modes for wireless connection. Once again, this is not applicable to C335 if 4G/LTE is chosen for wireless connection.

Wi-Fi – AP Mode (General settings)



WIFI Settings

Status
Mode: Master | **SSID:** Vantron-2B8892
BSSID: 0C:CF:89:2B:88:92 | **Encryption:** mixed WPA/WPA2 PSK (CCMP)
Channel: 1 (2.412 GHz) | **Tx-Power:** 20 dBm
Signal: -37 dBm | **Noise:** -95 dBm
Bitrate: 300.0 Mbit/s | **Country:** US

WIFI mode: AP
SSID ① Vantron-2B8892
Channel ② 1(2412MHz)
Encryption ③ WPA-PSK/WPA2-PSK Mixed Mode
Cipher ④ Force CCMP (AES)
Key ⑤ ••••••••

Associated Stations

Network		MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
(Master "Vantron-2B8892")	⑥	D6:A2:A0 [redacted]	172.1 [redacted]	-37 / -95 dBm	65.0 Mbit/s, 0MHz 65.0 Mbit/s, 0MHz

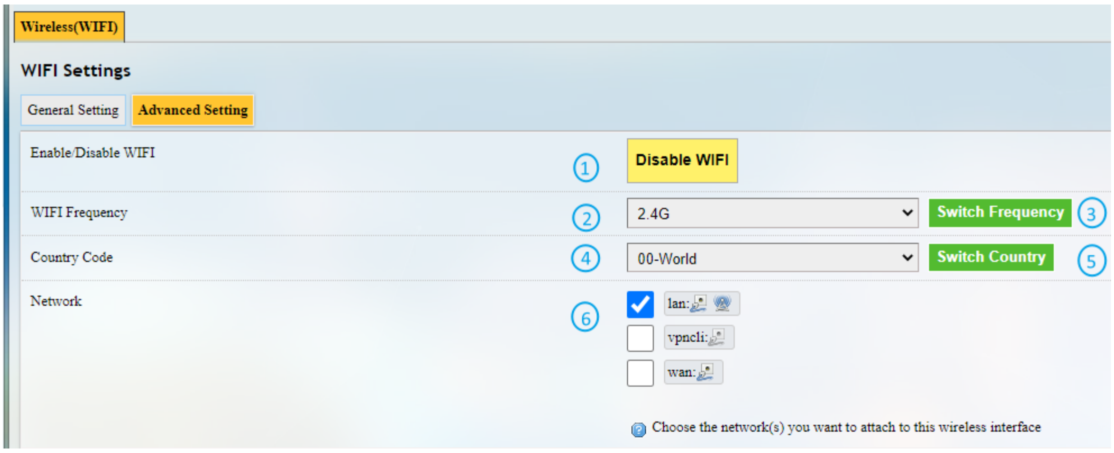
Description of the numbered areas

1. Set an SSID for the Gateway

The ID name shall not contain characters including $, `, \.

2. Select a Wi-Fi channel
3. Select an encryption method (the following options vary with the encryption method)
4. Select an encryption algorithm
5. Assign a Wi-Fi password (no less than 8 characters)
6. List of currently connected devices

Wi-Fi – AP Mode (Advanced setting)



Choose the network(s) you want to attach to this wireless interface

Description of the numbered areas

1. Turn on/off Wi-Fi
2. Set Wi-Fi frequency (determined by hardware)
3. Click to switch frequency
4. Set the country code
5. Click to switch the country

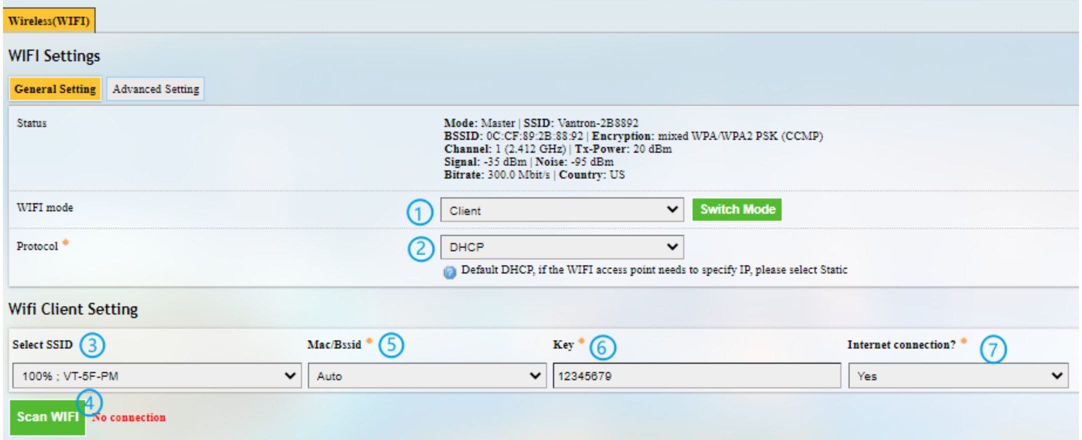
As modification of fields 2 and 4 will have impact on the Wi-Fi signal, the web interface will return to the general settings page upon a clicking of the switch button.

6. The network interface to which Wi-Fi belongs

Wi-Fi – Client Mode

When the Gateway is set as a client on a wireless network, the page below allows you to make changes to the network settings.

- The parameters will be overwritten if you change the settings under 3.3.3 WAN Setting – Client.
- A wwan0 port will be added automatically when client mode is being configured.



WIFI Settings

Status: **Mode:** Master | **SSID:** Vantron-2B8892
BSSID: 0C:CF:89:2B:88:92 | **Encryption:** mixed WPA/WPA2 PSK (CCMP)
Channel: 1 (2.412 GHz) | **Tx-Power:** 20 dBm
Signal: -35 dBm | **Noise:** -95 dBm
Bitrate: 300.0 Mbit/s | **Country:** US

WIFI mode: Client

Protocol *: DHCP
Default DHCP, if the WIFI access point needs to specify IP, please select Static

Wifi Client Setting

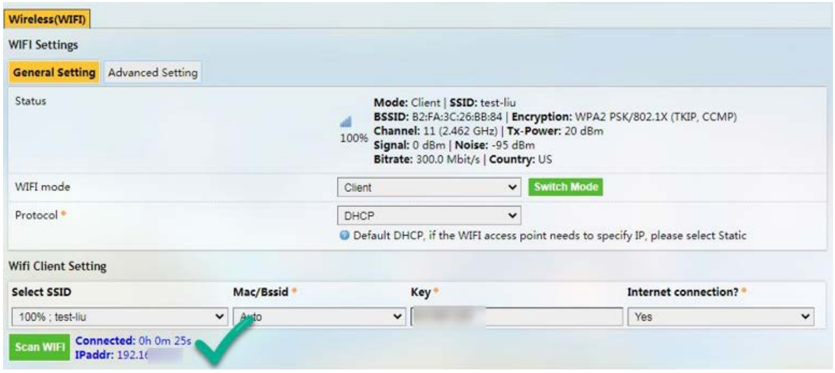
Select SSID	Mac/Bssid *	Key *	Internet connection? *
100% ; VT-5F-PM	Auto	12345679	Yes

No connection

Description of the numbered areas

1. Switch to **Client mode**
2. Select DHCP protocol to automatically get an IP or Static Address protocol to specify an IP for the Gateway
3. Select a wireless network for internet access
4. Click **Scan WIFI** to refresh the Wi-Fi list if the target Wi-Fi is not identified
5. Select the MAC address of the Wi-Fi, or leave it to Auto if not clear
6. Input the password of the Wi-Fi
7. Confirm that the target Wi-Fi has internet connection

When the Gateway is successfully connected as a client, there will be the network information next to **Scan WIFI** button.



WIFI Settings

Status: 100% **Mode:** Client | **SSID:** test-liu
BSSID: B2:FA:3C:26:BB:84 | **Encryption:** WPA2 PSK/802.1X (TKIP, CCMP)
Channel: 11 (2.462 GHz) | **Tx-Power:** 20 dBm
Signal: 0 dBm | **Noise:** -95 dBm
Bitrate: 300.0 Mbit/s | **Country:** US

WIFI mode: Client

Protocol *: DHCP
Default DHCP, if the WIFI access point needs to specify IP, please select Static

Wifi Client Setting

Select SSID	Mac/Bssid *	Key *	Internet connection? *
100% ; test-liu	Auto	[redacted]	Yes

Connected: 0h 0m 25s
IPaddr: 192.1[redacted]

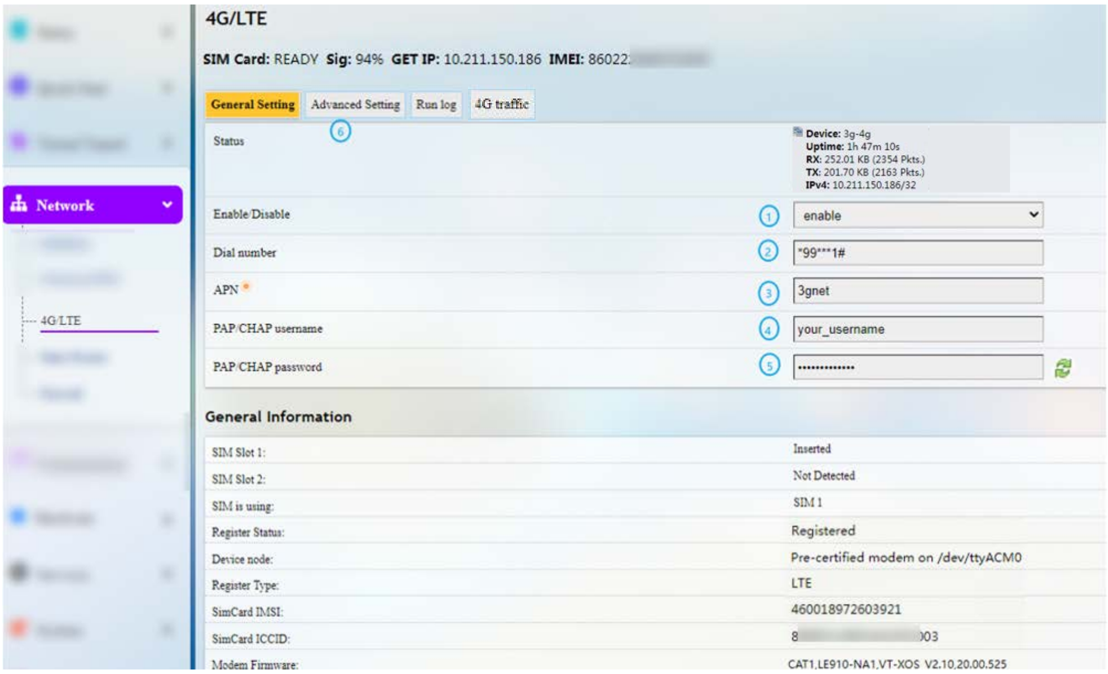
3.5.3 4G/LTE

For C335 gateways, this page might be invisible if you had chosen Wi-Fi for connection.

Before you configure for 4G/LTE, be sure to install the activated SIM card and the LET antennas. After installation, the SIM card information will display on the top of the page, including signal strength, IP, and IMEI. While register status and other general information will display at the bottom of the page.

Confirm (with your sales executive) whether the 4G module is AT&T or Verizon pre-certified. If so, when you apply for SIM cards from the carriers,

- provide Verizon with the pre-certified module name **VT-MOB-CELL-mPCIe**.
- provide AT&T with the pre-certified module name **VT-MOB-MPCIE-4G**.



4G/LTE

SIM Card: READY **Sig:** 94% **GET IP:** 10.211.150.186 **IMEI:** 86022[redacted]

Status
Device: 3g-4g
Uptime: 1h 47m 10s
RX: 252.01 KB (2354 Pkts.)
TX: 201.70 KB (2163 Pkts.)
IPv4: 10.211.150.186/32

Enable/Disable: enable
Dial number: *99***1#
APN *: 3gnet
PAP/CHAP username: your_username
PAP/CHAP password: ••••••••••••••

General Information

SIM Slot 1:	Inserted
SIM Slot 2:	Not Detected
SIM is using:	SIM 1
Register Status:	Registered
Device node:	Pre-certified modem on /dev/ttyACM0
Register Type:	LTE
SimCard IMSI:	460018972603921
SimCard ICCID:	8[redacted]03
Modem Firmware:	CAT1,LE910-NA1,VT-XOS V2.10.20.00.525

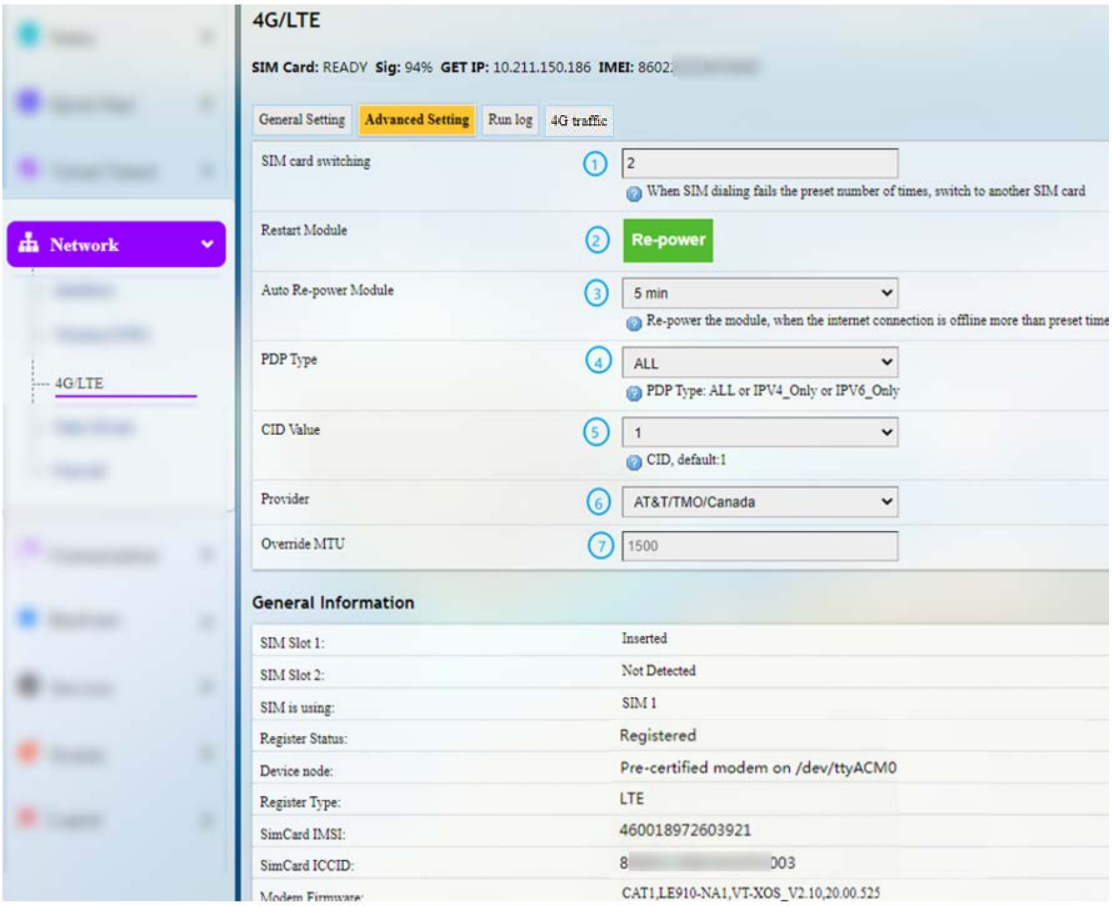
Description of the numbered areas

1. Enable/disable 4G/LTE service
2. Input *99***1# for AT&T SIM cards and *99***3# for Verizon SIM cards
3. Input the APN provided by the carrier
4. Enter the username provided by the carrier for PAP/CHAP authentication
5. Enter the password provided by the carrier for PAP/CHAP authentication
6. Click **Advanced Setting** for more configuration options

Leave the field as is if not available.

PAP/CHAP username and password are to be specified only if your carrier has setup APN with user name and password.

In the **Advanced Setting** page, you can further configure the cellular network.



4G/LTE

SIM Card: READY Sig: 94% GET IP: 10.211.150.186 IMEI: 8602[redacted]

SIM card switching: 2
When SIM dialing fails the preset number of times, switch to another SIM card

Restart Module: Re-power

Auto Re-power Module: 5 min
Re-power the module, when the internet connection is offline more than preset time

PDP Type: ALL
PDP Type: ALL or IPV4_Only or IPV6_Only

CID Value: 1
CID, default:1

Provider: AT&T/TMO/Canada

Override MTU: 1500

General Information

SIM Slot 1:	Inserted
SIM Slot 2:	Not Detected
SIM is using:	SIM 1
Register Status:	Registered
Device node:	Pre-certified modem on /dev/ttyACM0
Register Type:	LTE
SimCard IMSI:	460018972603921
SimCard ICCID:	8[redacted]003
Modem Firmware:	CAT1,LE910-NA1,VT-XOS_V2.10,20.00.525

Description of the numbered areas

1. Maximum number of dial failures allowed for current SIM card (only for devices with dual SIM cards, better to leave it as is)
2. Click to restart the 4G module
3. Time scheduled for automatic restart of the 4G module when it is offline
4. Select a PDP type (leave it as is)
5. Select **custom** from the drop-down list, input 1 for AT&T SIM cards and 3 for Verizon SIM cards
6. Select **AT&T/TMO/Canada** or **Verizon** from the drop-down list for AT&T SIM cards and Verizon SIM cards, respectively
7. Default MTU value (1500)

Remember to save the settings to have the configurations take effect.

If the 4G module is not AT&T and Verizon pre-certified, the provider information will not be available in **Advanced Setting**, and the **General Setting** options are the same as those for pre-certified 4G modules. You can keep the default values of the fields unchanged.

The **Run Log** next to the **Advanced Setting** tab displays the last 50 log entries of the module.

Under **4G traffic** tab, traffic information measured in real time or on the monthly and daily basis is available. You can also set the interval for submitting the temporary in-memory database to the persistent database directory.

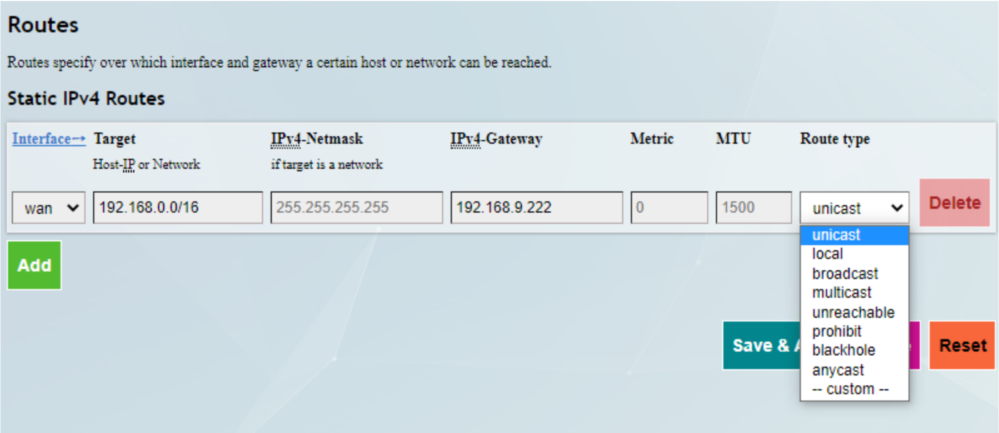
3.5.4 Static Routes

This is an advanced function allowing you to specify interface rules for route access.

Example:

Requirement: When the Gateway has 4G and WAN network interfaces, the internal network (192.168.0.0 - 192.168.255.254) is accessed via the WAN interface by the internal server. Other data access is realized via the 4G interface.

Click **Add** and select an interface to configure.



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target Host-IP or Network	IPv4-Netmask if target is a network	IPv4-Gateway	Metric	MTU	Route type
wan	192.168.0.0/16	255.255.255.255	192.168.9.222	0	1500	unicast

Description of the route type:

Type	Description
Unicast	The route entry describes real paths to the destinations covered by the route prefix.
Local	The destinations are assigned to this host. The packets are looped back and delivered locally.
Broadcast	The destinations are broadcast addresses. The packets are sent as link broadcasts.
Multicast	IP datagrams are sent to a group of interested receivers in a single transmission. It is not present in normal routing tables.
Unreachable	The destinations are unreachable. Packets are discarded and the ICMP message of host unreachable is generated. The local senders will receive an EHOSTUNREACH error.

Type	Description
Prohibit	The destinations are unreachable. Packets are discarded and the ICMP message of communication administratively prohibited is generated. The local senders will receive an EACCES error.
Blackhole	The destinations are unreachable. Packets are discarded silently. The local senders will receive an EINVAL error.
Anycast	The destinations are any cast addresses assigned to this host. They are mainly equivalent to local with one difference that such addresses are invalid when used as the source address of any packet.

3.5.5 Firewall

Firewall – General Settings

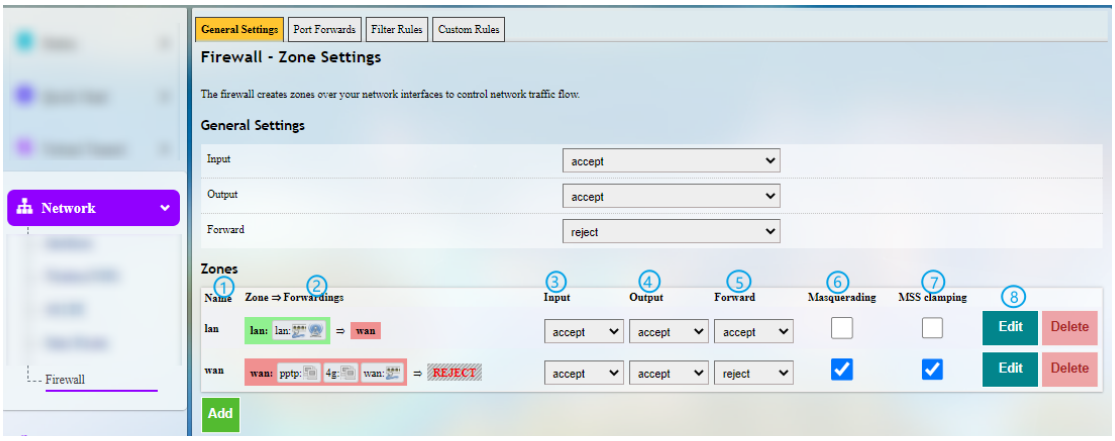
The following is a summary of the configuration items that the firewall can define. The minimum firewall configurations usually contain a basic setting item, at least two zones (LAN and WAN) and a forwarding to allow packets to be forwarded from LAN to WAN.

General Settings define the global settings that do not depend on a specific area. The following options can be defined:

Name	Type	Mandatory or not	Default value	Description
Input	String	N	ACCEPT	INPUT chain default strategy (ACCEPT, REJECT, DROP)
Output	String	N	ACCEPT	OUTPUT chain default strategy (ACCEPT, REJECT, DROP)
Forward	String	N	REJECT	FORWARD chain default strategy (ACCEPT, REJECT, DROP)

Firewall – Zone Settings

A zone section groups multiple interfaces and serves as a source or destination for forwardings, rules and redirects. Masquerading (NAT) of outgoing traffic is controlled on a per-zone basis.



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Input	accept
Output	accept
Forward	reject

Zones

Name	Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan	lan: lan: ⇒ wan	accept	accept	accept	□	□	Edit Delete
wan	wan: pptp: 4g: wan: ⇒ REJECT	accept	accept	reject	☑	☑	Edit Delete

Description of the numbered areas

1. Unique zone name

At least LAN and WAN shall be listed under the zone name.

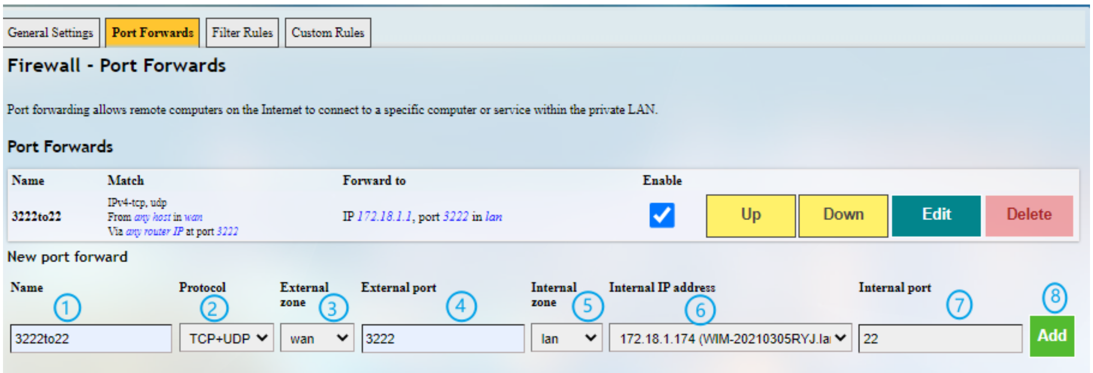
2. Zone forwarding model description
3. Default policy (ACCEPT, REJECT, DROP) for incoming zone traffic
4. Default policy (ACCEPT, REJECT, DROP) for outgoing zone traffic
5. Default policy (ACCEPT, REJECT, DROP) for forwarded zone traffic
6. Masquerading (NAT)
7. MSS clamping
8. Zone editing

A click of the **Edit** button following each zone will direct you to the detailed zone setting page where general settings, advanced settings and forwarding rules are available.

Firewall – Port Forwards

The forwarding sections control the traffic flow between zones and may enable MSS clamping for specific directions. Only one direction is covered by a forwarding rule. To allow bidirectional traffic flows between two zones, two forwardings are required, with src and dest reversed in each.

Illustrative example on port forwarding (Forwarding port 3222 (WAN) to port 22 of LAN host 172.18.1.174):



Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable
3222to22	IPv4-tcp, udp From *any host* in *wan* Via *any router IP* at port *3222*	IP *172.18.1.1*, port *3222* in *lan*	☑

New port forward

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
3222to22	TCP+UDP	wan	3222	lan	172.18.1.174 (WIM-20210305RYJ.la	22

Description of the numbered areas

1. Rule name
2. Protocol (TCP/UDP/TCP + UDP are supported)
3. External zone: WAN
4. External port: 3222
5. Internal zone: Select the LAN port
6. LAN host: 172.18.1.174
7. Target host port number of the internal zone: 22
8. Add rules (mandatory)

Firewall – Custom Rules

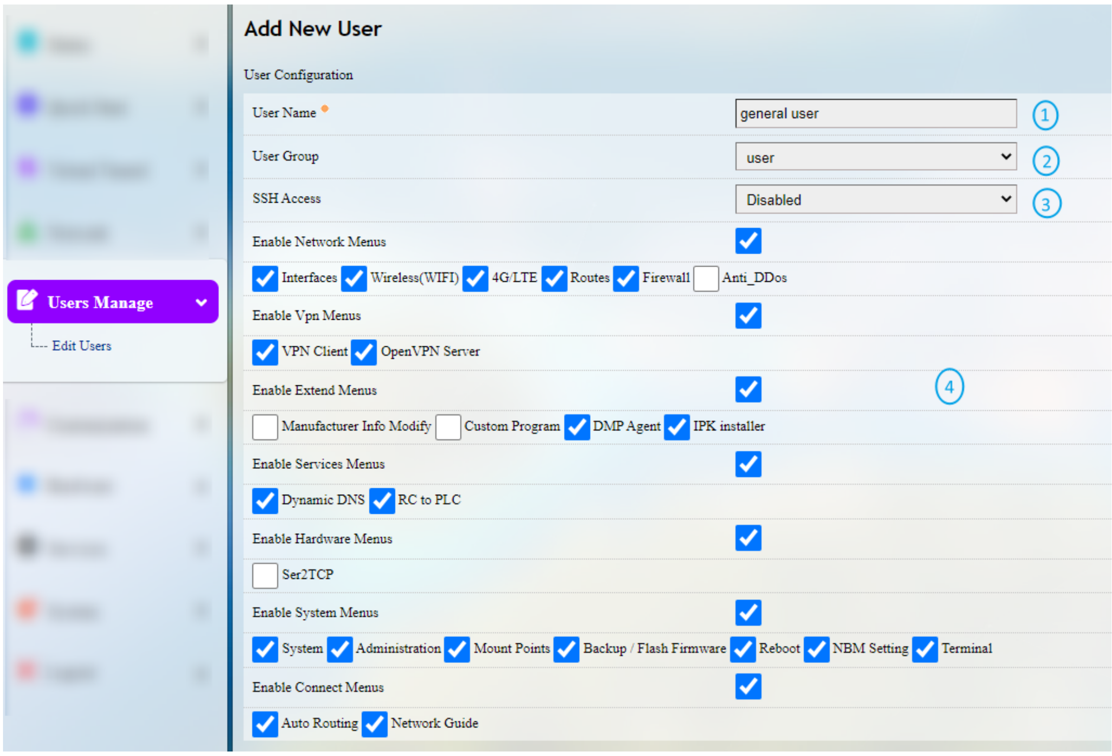
Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default rule settings have been loaded.

3.6 User Management

As this function may change system settings, you need log in with the root account (Refer to 2.2 for the username and password) to enable the function.

In the **Edit Users** page, you can add new users or edit the existing users.

To **add** a new user, click the button below the existing user information：



Users Manage

Edit Users

Add New User

User Configuration

User Name * : general user ①

User Group: user ②

SSH Access: Disabled ③

Enable Network Menus ☑

☑ Interfaces ☑ Wireless(WIFI) ☑ 4G/LTE ☑ Routes ☑ Firewall □ Anti_DDos

Enable Vpn Menus ☑

☑ VPN Client ☑ OpenVPN Server

Enable Extend Menus ☑ ④

□ Manufacturer Info Modify □ Custom Program ☑ DMP Agent ☑ IPK installer

Enable Services Menus ☑

☑ Dynamic DNS ☑ RC to PLC

Enable Hardware Menus ☑

□ Ser2TCP

Enable System Menus ☑

☑ System ☑ Administration ☑ Mount Points ☑ Backup / Flash Firmware ☑ Reboot ☑ NBM Setting ☑ Terminal

Enable Connect Menus ☑

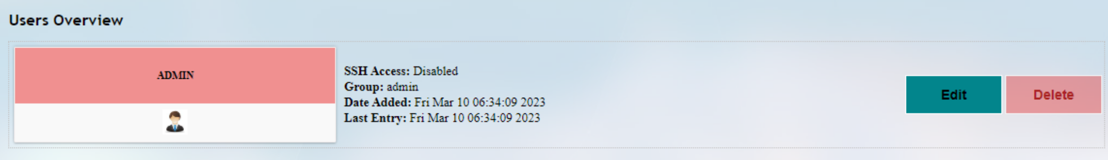
☑ Auto Routing ☑ Network Guide

Description of the numbered areas

1. Input a username
2. Select a group for the new user
3. Enable SSH access or not for the new user
4. Enable the specific functions for the new user

Be sure to save the settings before you exit the page.

The **Edit** and **Delete** buttons behind a user allow you to enable/disable certain functions for this user or delete this user.



Users Overview

ADMIN

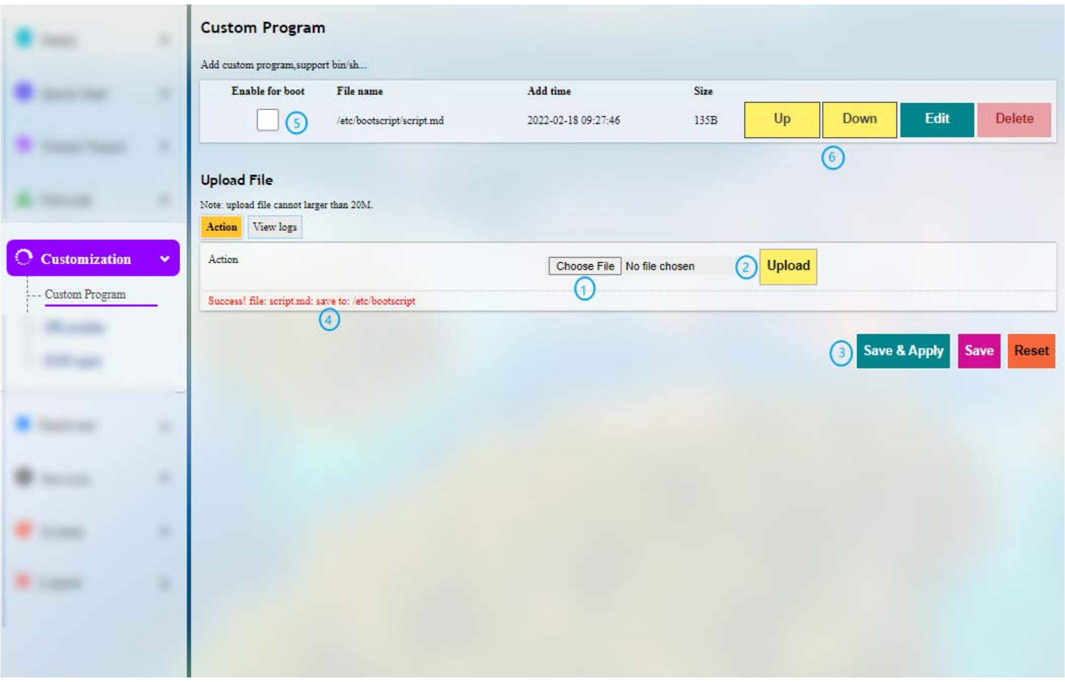
SSH Access: Disabled
Group: admin
Date Added: Fri Mar 10 06:34:09 2023
Last Entry: Fri Mar 10 06:34:09 2023

3.7 Customization

As certain functions under this tab may change system settings, you need log in with the root account (Refer to 2.2 for the username and password) to enable the function.

3.7.1 Custom Program

Custom program allows users to upload scripts or programs (sh/bin) to the Gateway and run them at the startup.



Custom Program

Add custom program,support bin/sh...

Enable for boot	File name	Add time	Size
□	/etc/bootscript/script.md	2022-02-18 09:27:46	135B

Upload File

Note: upload file cannot larger than 20M.

Action: Choose File No file chosen

Success! file: script.md: save to: /etc/bootscript

Description of the numbered areas

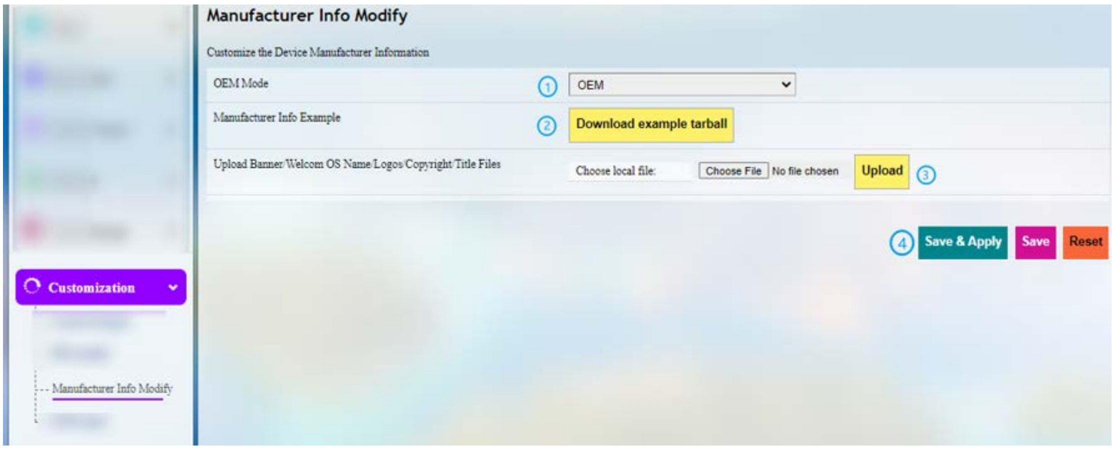
1. Select a script to upload
2. Upload the script to the Gateway
3. **Save & Apply** the settings
4. When the script is uploaded successfully, the file name and file directory will be displayed
5. Enable the script, and it will run next time when the Gateway starts up
6. If more than one script is uploaded, you can move any of them up or down to rearrange the script order, and edit/delete the script

3.7.2 IPK Installer

With IPK Installer, customers can install self-compiled IPK packages to the Gateway. Vantron industrial protocol packages are also uploaded from here. Refer to 4.2 Protocol Configuration and Application for data collection and transfer.

3.7.3 Manufacturer Info Customization

Once you need to customize the manufacturer information, navigate to **Customization > Manufacturer Info Modify**, and select OEM from the **OEM Mode** drop-down list.



Manufacturer Info Modify

Customize the Device Manufacturer Information

OEM Mode ① OEM

Manufacturer Info Example ②

Upload Banner/Welcom OS Name/Logos/Copyright/Title Files — Choose local file: No file chosen ③

Description of the numbered areas

1. Select OEM mode
2. Download illustrative tarball
3. Replace the files in the package as needed and upload the file one by one
4. **Save & Apply** the settings

The three modes that customers can choose from the drop-down list based on needs are explained as follows:

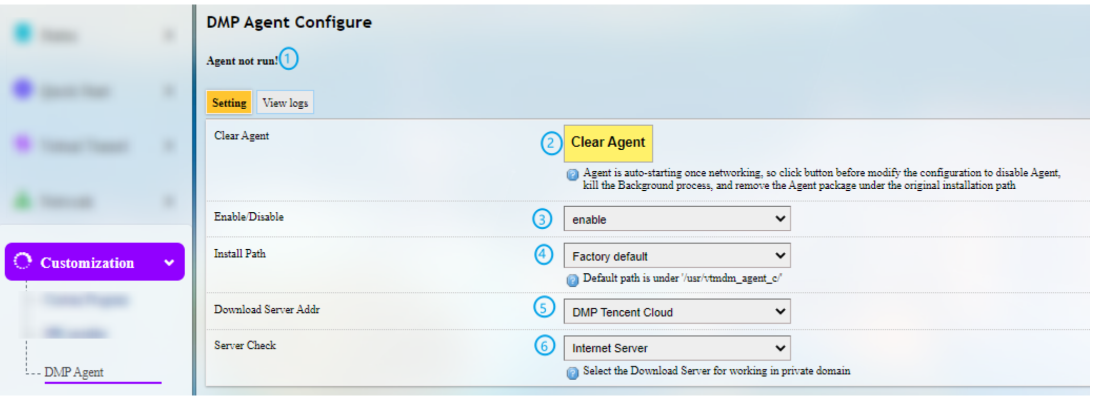
Vantron: All the information included in the files will be about Vantron.

Standard: Some of the fields included in the files will be "Gateway" by default, and some information like the copyright will be left blank.

OEM: All the information displayed will be user tailored.

3.7.4 DMP Agent

Gateways/routers are interfacing with BlueSphere GWM via DMP Agent. Please refer to the descriptions below for enabling the DMP agent before you can manage the gateways/routers remotely.



DMP Agent Configure

Agent not run!

Clear Agent

Agent is auto-starting once networking, so click button before modify the configuration to disable Agent, kill the Background process, and remove the Agent package under the original installation path

Enable/Disable: enable

Install Path: Factory default

Default path is under '/usr/vtmdm_agent_c/'

Download Server Addr: DMP Tencent Cloud

Server Check: Internet Server

Select the Download Server for working in private domain

Description of the numbered areas

1. Status of DMP Agent
2. Click **Clear Agent** before changing the configurations

Provided that the remaining prerequisites (refer to 2.3 Connection to Vantron Gateway Management Platform) are met, the DMP Agent, once enabled, will run automatically when there is internet access. Clicking this button will disable DMP Agent, kill all the processes running at the background, and remove the Agent package from the original installation directory.

3. Enable/Disable the Agent
4. You can customize the installation path of the Agent here (default path: "/usr")
5. Set up the download address of the Agent server (the default address is recommended)
6. Check the server

Factory reset of the Gateway will deactivate the Gateway on the BlueSphere GWM platform. If you wish to activate the Gateway again on the GWM, please click **Clear Agent** on the VantronOS portal, then **enable** the agent and wait a moment to allow the device to come online.

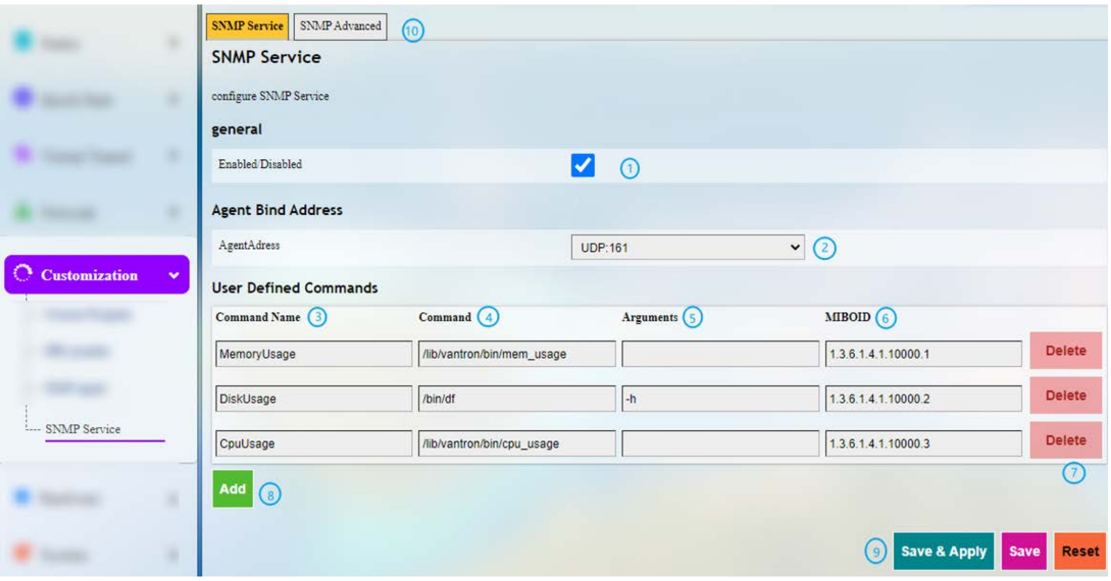
3.7.5 SNMP Service

A typical SNMP implementation consists of three factors:

Network management system (NMS)—A combination of hardware (devices) and software (the SNMP manager) that is used to monitor and administer a network. The SNMP manager collects information about network connectivity, activity, and events by polling the managed devices.

Managed device—A managed device (also called a network element) is any device on a network that is managed by the NMS. Routers and switches are common examples of managed devices.

SNMP agent—The SNMP agent responds to requests for information and actions from the manager. The agent also controls access to the agent's management information base (MIB), a collection of objects that can be viewed or changed by the SNMP manager. MIB contains the name, datatype, and the object identifier (OID) which is a numerical address used to check the status of the components on network devices (like CPU, memory, power supply, network traffic, etc.).



SNMP Service

configure SNMP Service

general

Enabled/Disabled ☑

Agent Bind Address

AgentAdress: UDP:161

User Defined Commands

Command Name	Command	Arguments	MIBOID
MemoryUsage	/lib/vantron/bin/mem_usage		1.3.6.1.4.1.10000.1
DiskUsage	/bin/df	-h	1.3.6.1.4.1.10000.2
CpuUsage	/lib/vantron/bin/cpu_usage		1.3.6.1.4.1.10000.3

Description of the numbered areas

1. Enable/Disable SNMP service
2. The SNMP agent listens on UDP port 161 by default for any SNMP GET and other requests from the manager
3. Name of the user-defined SNMP command
4. Content of the command
5. Command argument
6. The OID (each number provides a piece of corresponding information)

7. Delete the existing command
8. Add a new command
9. **Save & Apply** the settings
10. Advanced settings

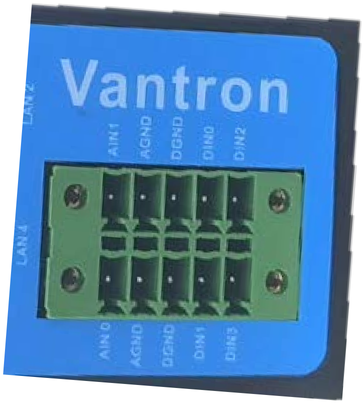
Leave the field as is if not available.

An SNMP agent is considered an authoritative SNMP engine. The Engine ID is only used by SNMPv3 entities to uniquely identify them. In the advanced settings tab, you can edit the information about the server and the engine ID.

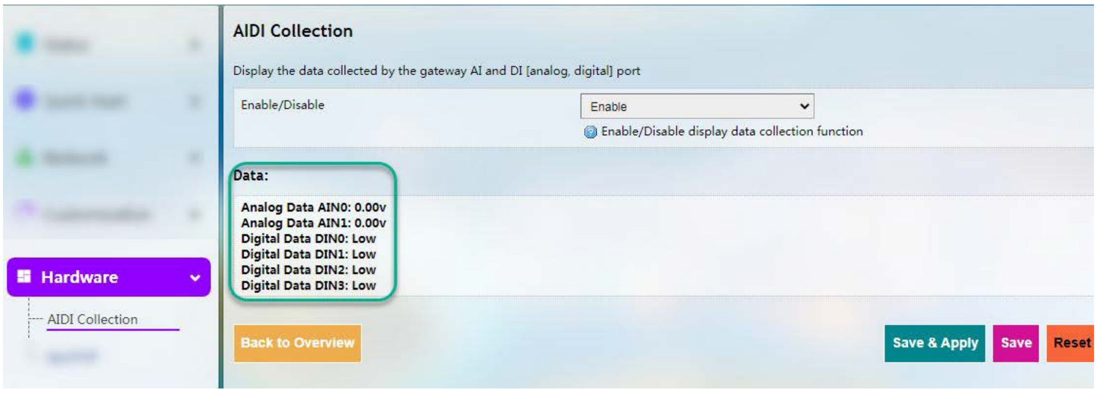
3.8 Hardware

3.8.1 AIDI Collection

C335S implements 2 analog input interfaces (AIN0 & AIN1) and 4 digital input interfaces (DIN0, DIN1, DIN2, DIN3).



Here you can enable the display function and access the data collected by the interfaces.



AIDI Collection

Display the data collected by the gateway AI and DI [analog, digital] port

Enable/Disable: Enable

Enable/Disable display data collection function

Data:

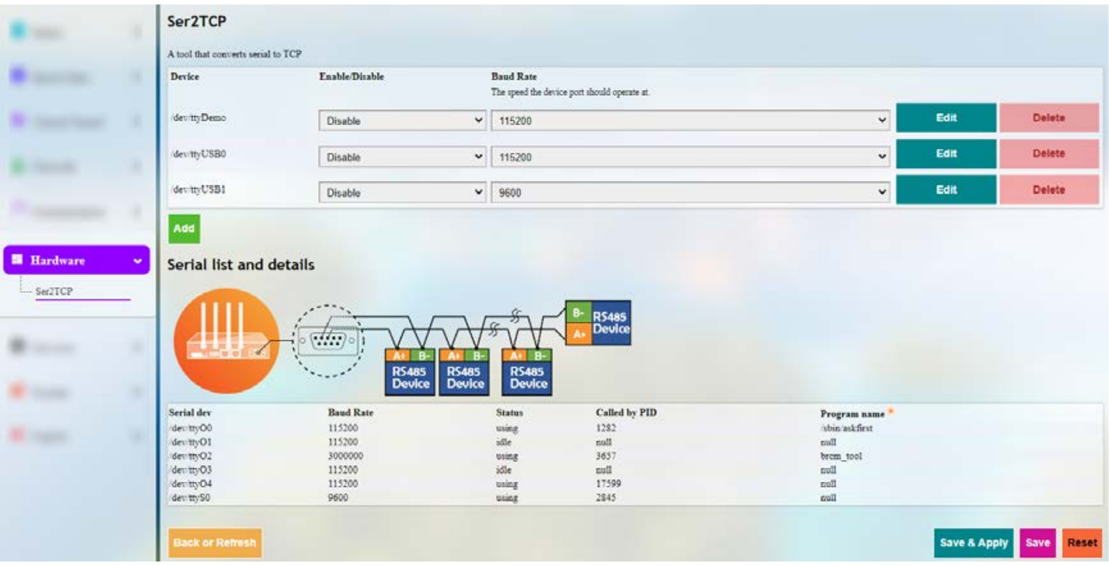
Analog Data AIN0: 0.00v
Analog Data AIN1: 0.00v
Digital Data DIN0: Low
Digital Data DIN1: Low
Digital Data DIN2: Low
Digital Data DIN3: Low

AIN input voltage range: 0-8V.

DIN input voltage range: 0-3.3V.

3.8.2 Ser2TCP

Serial to TCP provides an easy way to convert local serial data into Ethernet data and enables two-way communication with remote devices. Each conversion rule can be independently configured to server-side or client-side mode. You can also add, edit or delete a conversion rule on this page.



Ser2TCP

A tool that converts serial to TCP

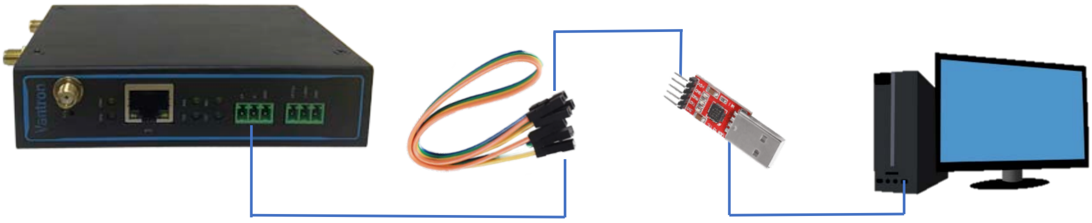
Device	Enable/Disable	Baud Rate The speed the device port should operate at.		
/dev/ttyDemo	Disable	115200	Edit	Delete
/dev/ttyUSB0	Disable	115200	Edit	Delete
/dev/ttyUSB1	Disable	9600	Edit	Delete

Serial list and details

Serial dev	Baud Rate	Status	Called by PID	Program name *
/dev/ttyO0	115200	using	1282	/sbin/askfirst
/dev/ttyO1	115200	idle	null	null
/dev/ttyO2	3000000	using	3657	brom_tool
/dev/ttyO3	115200	idle	null	null
/dev/ttyO4	115200	using	17599	null
/dev/ttyS0	9600	using	2845	null

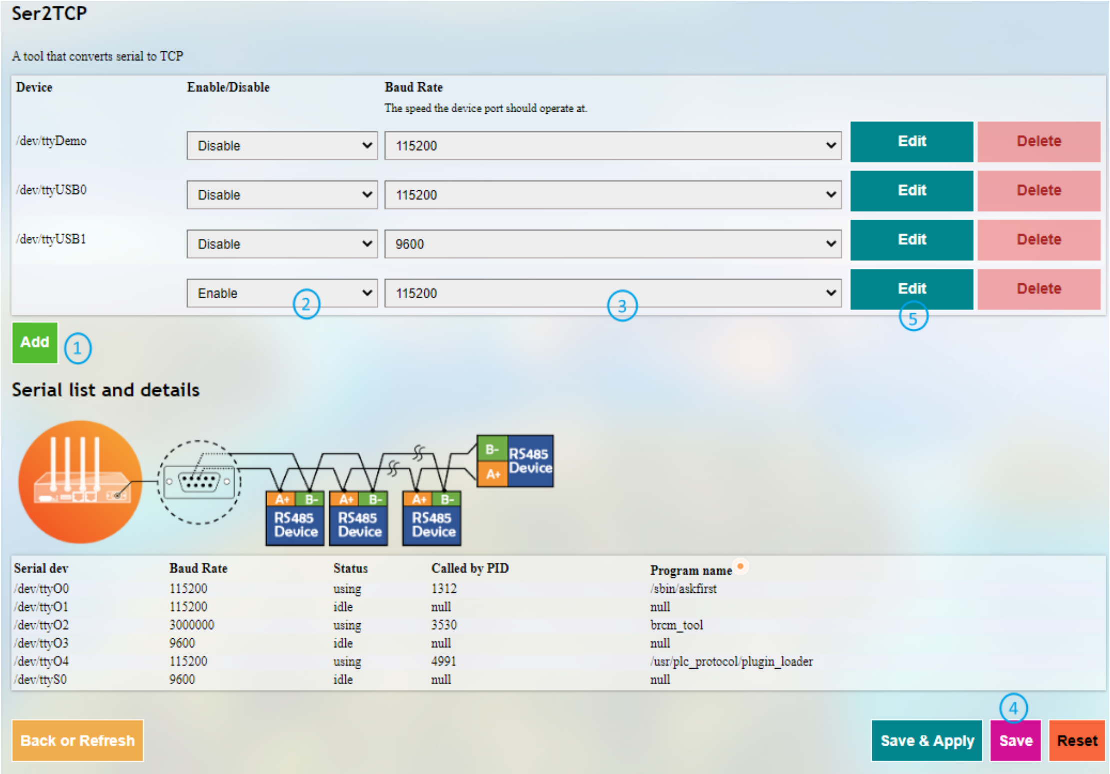
3.8.3 Ser2net environment setup and verification

- Prerequisites
  - A C335 gateway (**C335L for showcase**)
  - An Ubuntu host
  - A USB to TTL serial adapter
  - A DuPont cable
  - Connect the serial port (e.g., RS485 serial port (R2) on the left side) of the C335L gateway to the host as follows



- Client mode

(1) Settings on VantronOS web interface



Ser2TCP

A tool that converts serial to TCP

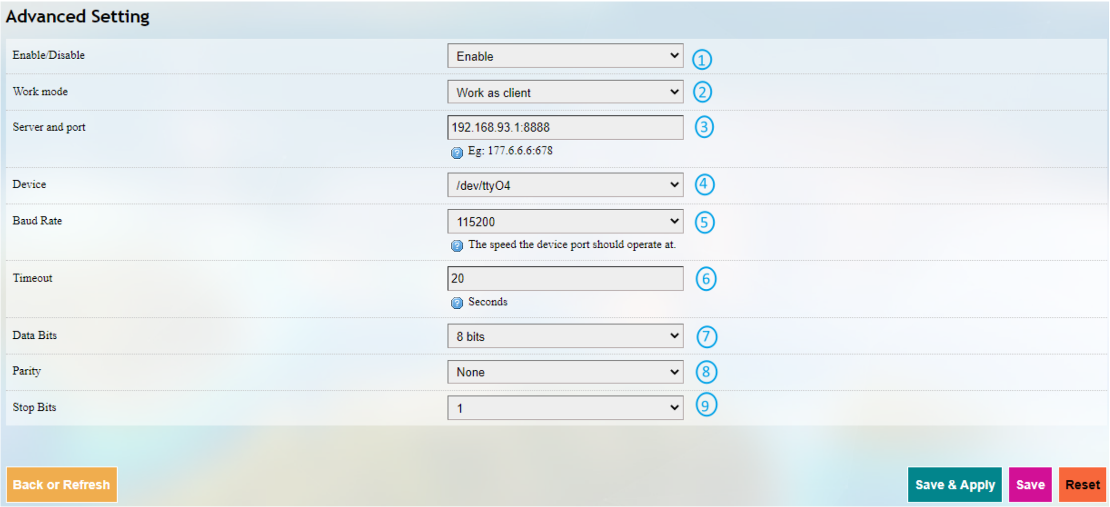
Device	Enable/Disable	Baud Rate The speed the device port should operate at.		
/dev/ttyDemo	Disable	115200	Edit	Delete
/dev/ttyUSB0	Disable	115200	Edit	Delete
/dev/ttyUSB1	Disable	9600	Edit	Delete
	Enable	115200	Edit	Delete

Serial list and details

Serial dev	Baud Rate	Status	Called by PID	Program name
/dev/ttyO0	115200	using	1312	/sbin/askfirst
/dev/ttyO1	115200	idle	null	null
/dev/ttyO2	3000000	using	3530	brcm_tool
/dev/ttyO3	9600	idle	null	null
/dev/ttyO4	115200	using	4991	/usr/plc_protocol/plugin_loader
/dev/ttyS0	9600	idle	null	null

Description of the numbered areas

1. Click **Add** to add a conversion rule
2. Select **Enable** from the drop-down
3. Set the Baud rate to 115200
4. Save the settings
5. Click **Edit** after the rule to enter the advanced settings page



Advanced Setting

Enable/Disable	Enable	①
Work mode	Work as client	②
Server and port	192.168.93.1:8888 Eg: 177.6.6.6:678	③
Device	/dev/ttyO4	④
Baud Rate	115200 The speed the device port should operate at.	⑤
Timeout	20 Seconds	⑥
Data Bits	8 bits	⑦
Parity	None	⑧
Stop Bits	1	⑨

Description of the numbered areas

1. **Enable** the rule
2. Select the **Work as client** mode
3. Input the server address and port number (Ubuntu host shall be the server, and port number is user-defined)
4. Select the serial device from the drop-down (RS485 serial port (R2) for illustration, node name /dev/ttyO4 as described in1.4.3)
5. Select 115200 as the baud rate (the default value will be the one selected when setting up the rule)
6. Set a timeout value
7. Select “8 bits” for the data bit
8. Select “None” for parity
9. Select “1” as the stop bit

(2) The Ser2net process is running as follows:

```
uart2net -c -d 192.168.93.1 -p 8888 -t /dev/ttyO4 -b 115200 -a 8 -r none -s 1 -o 20
```

(3) Settings on the Ubuntu host

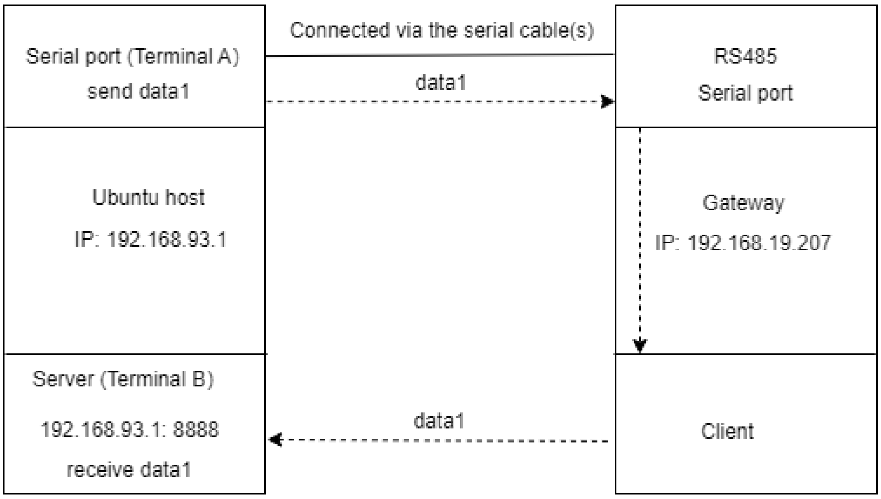
- Use microcom to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- Monitor the designated port (8888 as assigned in prior steps)

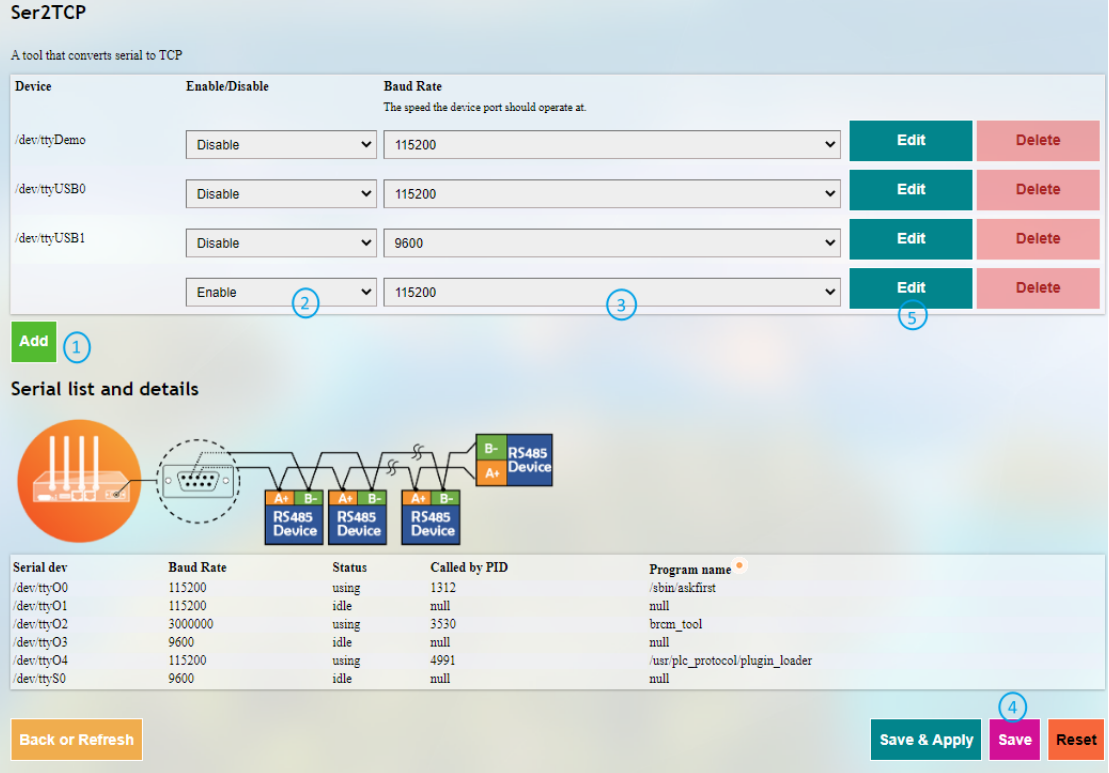
```
tcpudp_test tcp server:tcpudp_test -p 8888
```

- Input data in terminal A and receive in terminal B (the topology is as follows)



- Server mode

(1) Settings on VantronOS web interface



Ser2TCP

A tool that converts serial to TCP

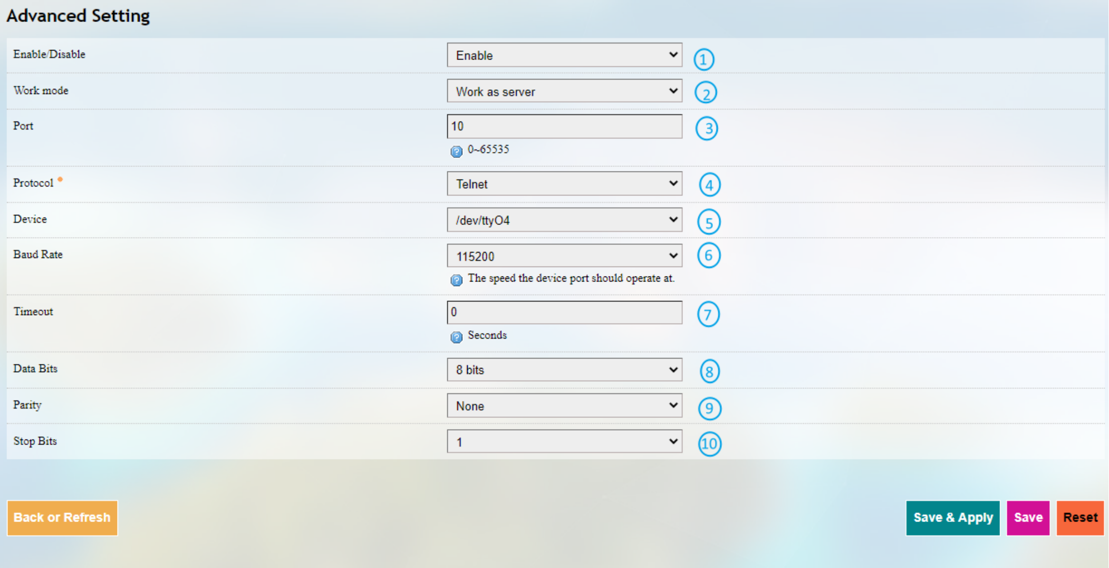
Device	Enable/Disable	Baud Rate The speed the device port should operate at.		
/dev/ttyDemo	Disable	115200	Edit	Delete
/dev/ttyUSB0	Disable	115200	Edit	Delete
/dev/ttyUSB1	Disable	9600	Edit	Delete
	Enable	115200	Edit	Delete

Serial list and details

Serial dev	Baud Rate	Status	Called by PID	Program name
/dev/ttyO0	115200	using	1312	/sbin/askfirst
/dev/ttyO1	115200	idle	null	null
/dev/ttyO2	3000000	using	3530	brcm_tool
/dev/ttyO3	9600	idle	null	null
/dev/ttyO4	115200	using	4991	/usr/plc_protocol/plugin_loader
/dev/ttyS0	9600	idle	null	null

Description of the numbered areas

1. Click **Add** to add a conversion rule
2. Select **Enable** from the drop-down
3. Set the Baud rate to 115200
4. Save the settings
5. Click **Edit** after the rule to enter the advanced settings page



Advanced Setting

Enable/Disable	Enable	①
Work mode	Work as server	②
Port	10 0~65535	③
Protocol *	Telnet	④
Device	/dev/ttyO4	⑤
Baud Rate	115200 The speed the device port should operate at.	⑥
Timeout	0 Seconds	⑦
Data Bits	8 bits	⑧
Parity	None	⑨
Stop Bits	1	⑩

Description of the numbered areas

1. **Enable** the rule
2. Select the **Work as server** mode
3. Input the port number (user-defined)
4. Select the **Telnet** protocol from the drop-down (see 3.8.4 for the difference between the protocols)
5. Select the serial device from the drop-down (RS485 serial port (R2) for illustration, node name /dev/ttyO4 as described in1.4.3)
6. Select 115200 as the baud rate (the default value will be the one selected when setting up the rule)
7. Set a timeout value
8. Select “8 bits” for the data bit
9. Select “None” for parity
10. Select “1” as the stop bit

Save and Apply above settings after the settings.

(2) The Ser2net process is running as follows:

```
/usr/sbin/ser2net -n -c /tmp/ser2net.conf
```

(3) Settings on the Ubuntu host

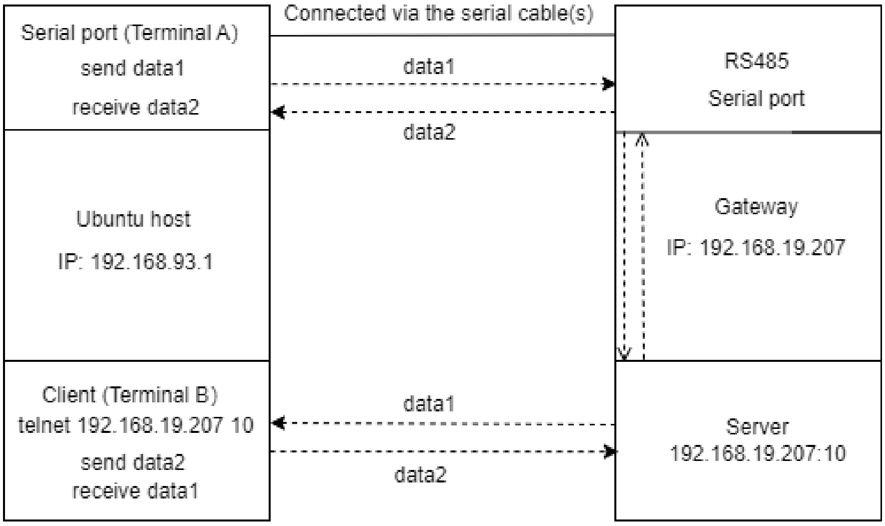
- Use microcom to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- Monitor the designated port (10 as assigned in prior steps) in terminal B using Telnet protocol

```
telnet 192.168.19.207 10
```

- Terminals A and B can send and receive data in both directions (the topology is as follows)



3.8.4 Protocol comparison

Under the server mode, three protocols are available which are differentiated as below:

1) Raw: enables the port and transfers all data as-is between the port and the long integer.

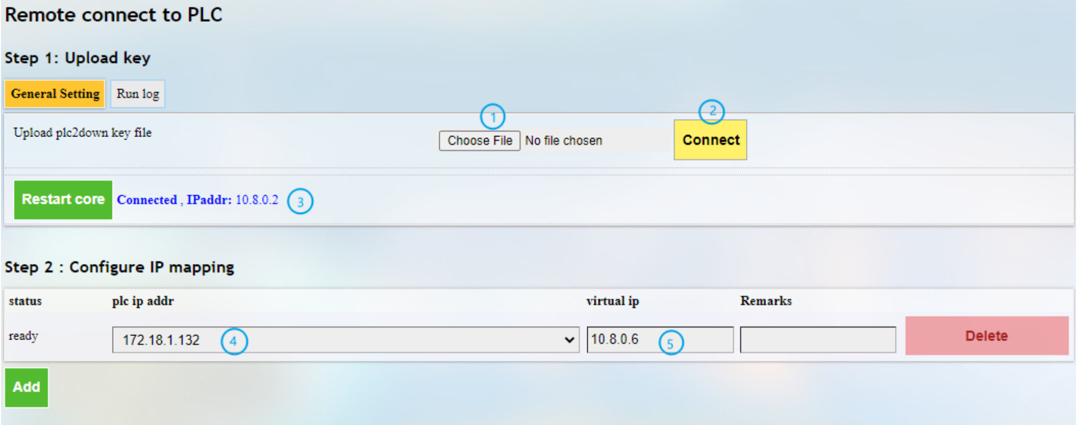
2) Rawlp: enables the port and transfers all input data to a gateway that is open without any Termios settings, allowing to use /dev/lpx devices and printers connected.

3) Telnet: enables the port and runs the telnet protocol on the port to set up telnet parameters (less used).

3.9 Services

3.9.1 RC to PLC

For remote access and control of PLC devices via OpenVPN protocol, you will need two gateways and a host PC that are on the same network. One gateway (G1) is for building an OpenVPN server (Refer to 3.4.1 OpenVPN Server for the setup), and the other (G2) is for connecting the OpenVPN server built by G1 (see details below).



Remote connect to PLC

Step 1: Upload key

Upload plc2down key file — No file chosen

Connected , IPaddr: 10.8.0.2

Step 2 : Configure IP mapping

status	plc ip addr	virtual ip	Remarks
ready	172.18.1.132	10.8.0.6	

Description of the numbered areas

1. Download and save the .opv file after setting up the OpenVPN server on G1, then click this button to open the directory of the file
2. Click **Connect** to connect G2 to the OpenVPN server of G1
3. After connection, an IP address assigned by the OpenVPN server will be displayed here
4. Input the IP address of the PLC (on the same IP network as the LAN port of G2)
5. Input a virtual IP (on the same IP network as the one assigned by the OpenVPN server and not occupied by other clients)

Please save and apply above settings.

Before you can manage the PLC device remotely, please:

- Connect the PLC to the LAN port of G2 with an Ethernet cable
- Install an OpenVPN client on the host PC to connect the OpenVPN server built by G1 and install a PLC control program to manage the PLC settings like the IP address

3.9.2 Protocol Service

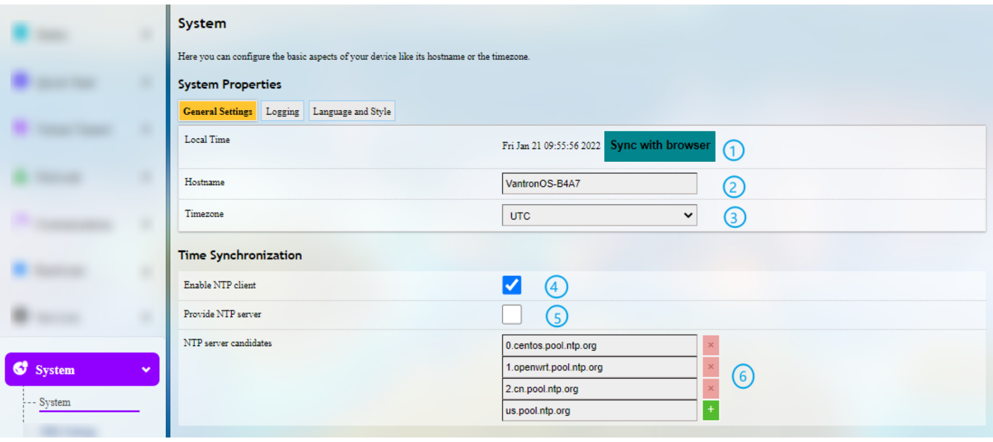
If a protocol-related .ipk file is installed previously, the protocol-related service information will be accessible on VantronOS with root account login, which shall be the same as that displayed on the protocol specific portal.

Please refer to **chapter 4** for the configuration and application of industrial protocols.

3.10 System

Apart from the device settings you might make in the previous sections, here you can configure your Gateway in more details, including host name, time zone, administrative password and so on.

3.10.1 System



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Local Time: Fri Jan 21 09:55:56 2022

Hostname: VantronOS-B4A7

Timezone: UTC

Time Synchronization

Enable NTP client: ☑

Provide NTP server: □

NTP server candidates: 0.centos.pool.ntp.org, 1.openwrt.pool.ntp.org, 2.cn.pool.ntp.org, us.pool.ntp.org

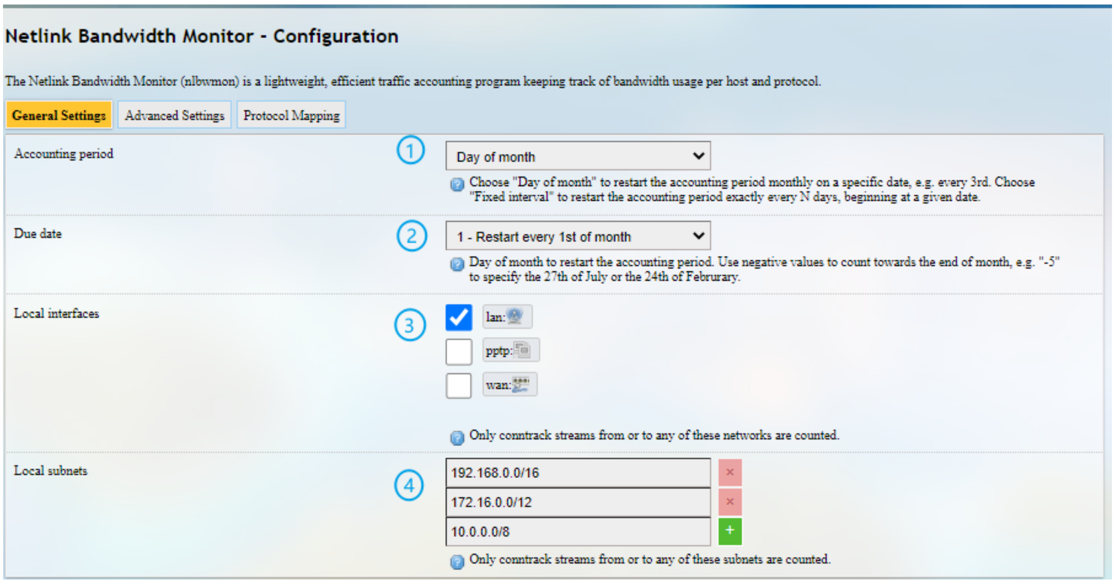
Description of the numbered areas

1. Synchronize the Gateway time with the browser (local) time
2. Assign a name to the host
3. Select a time zone
4. Enable NTP online time adjustment
5. Start the NTP server (the Gateway)
6. NTP online time server

For log-related settings, click **Logging** tab next to the **General settings** tab. If you want to change the interface language, just navigate to **Language and Style** tab following behind.

3.10.2 NBM Setting

General Settings



Netlink Bandwidth Monitor - Configuration

The Netlink Bandwidth Monitor (nlbwmon) is a lightweight, efficient traffic accounting program keeping track of bandwidth usage per host and protocol.

General Settings | Advanced Settings | Protocol Mapping

Accounting period: Day of month
Choose "Day of month" to restart the accounting period monthly on a specific date, e.g. every 3rd. Choose "Fixed interval" to restart the accounting period exactly every N days, beginning at a given date.

Due date: 1 - Restart every 1st of month
Day of month to restart the accounting period. Use negative values to count towards the end of month, e.g. "-5" to specify the 27th of July or the 24th of Februrary.

Local interfaces:
☑ lan:
□ pptp:
□ wan:
Only conntrack streams from or to any of these networks are counted.

Local subnets:
192.168.0.0/16
172.16.0.0/12
10.0.0.0/8
Only conntrack streams from or to any of these subnets are counted.

Description of the numbered areas

1. Set how long you would like the monitoring activities to be summarized
2. Specify a date in a month for restarting another round of monitoring activities

Applicable when Day of month is selected in 1

3. Statistics interface
4. Local subnets

Under **Advanced Settings** tab, each setting item is explained in detail so that users can figure out how to configure accordingly.

Protocol Mapping can be used to distinguish traffic types per host. Each mapping takes one line, with the first value being the IP protocol, the second value being the port number, and the third value being the name of the mapping protocol.

3.10.3 Administration

Under **Router Password** section, you can reset a password for accessing the Gateway.

SSH Access

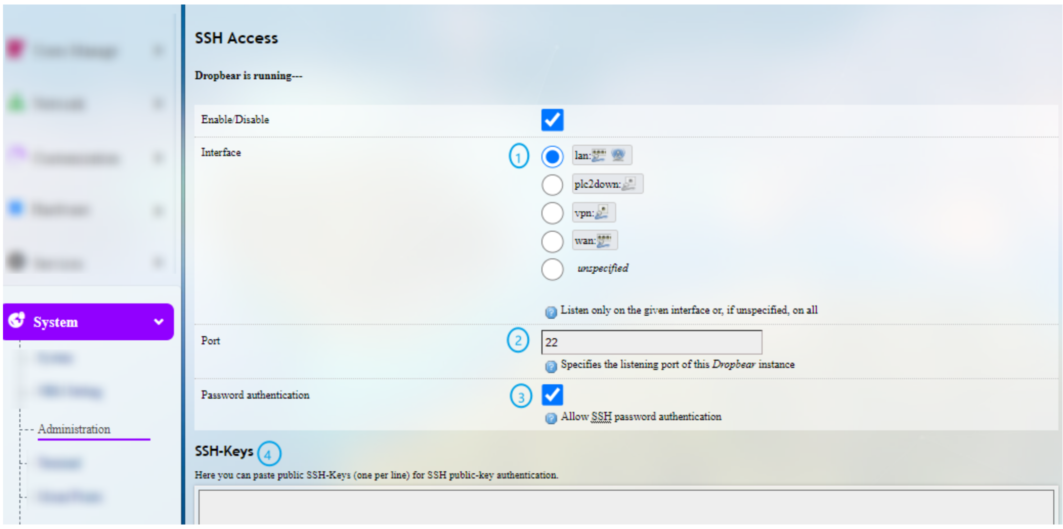
As this function might compromise the security of the network, you have to log in the web interface with a root account.

Step 1: Log out the interface by clicking **Logout** at the bottom left corner;

Step 2: Log in with the root account and password;

- Account: root
- Password: rootpassword

Step 3: Navigate to **System > Administration**, and enable dropbear.



SSH Access

Dropbear is running---

Enable/Disable ☑

Interface
● lan:
○ plc2down:
○ vpn:
○ wan:
○ *unspecified*

Listen only on the given interface or, if unspecified, on all

Port: 22

Specifies the listening port of this *Dropbear* instance

Password authentication ☑

Allow SSH password authentication

SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

Description of the numbered areas

1. Select a port to access (LAN by default)

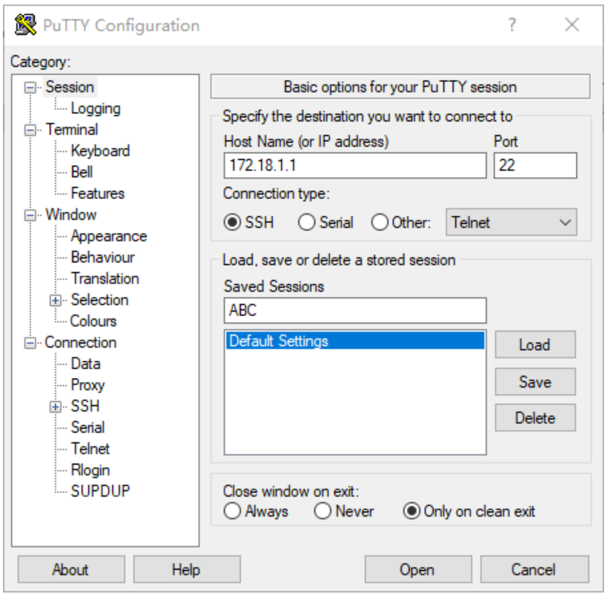
When “unspecified” is selected, all the ports will be monitored.

2. Specify a port for monitoring (port 22 by default)
3. Allow SSH password authentication
4. Add SSH-Keys for public key authentication

Step 4: Open an SSH client (PuTTY or MobaXterm recommended) in the Windows host;

Step 5: Input the host name or IP address (LAN port address by default: 172.18.1.1), keep the default port No. (22), and select **SSH** for the connection type;

Step 6: Set the session name and **Save**, keep the other settings unchanged, then click **Open**;



Specify the destination you want to connect to

Host Name (or IP address): 172.18.1.1

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

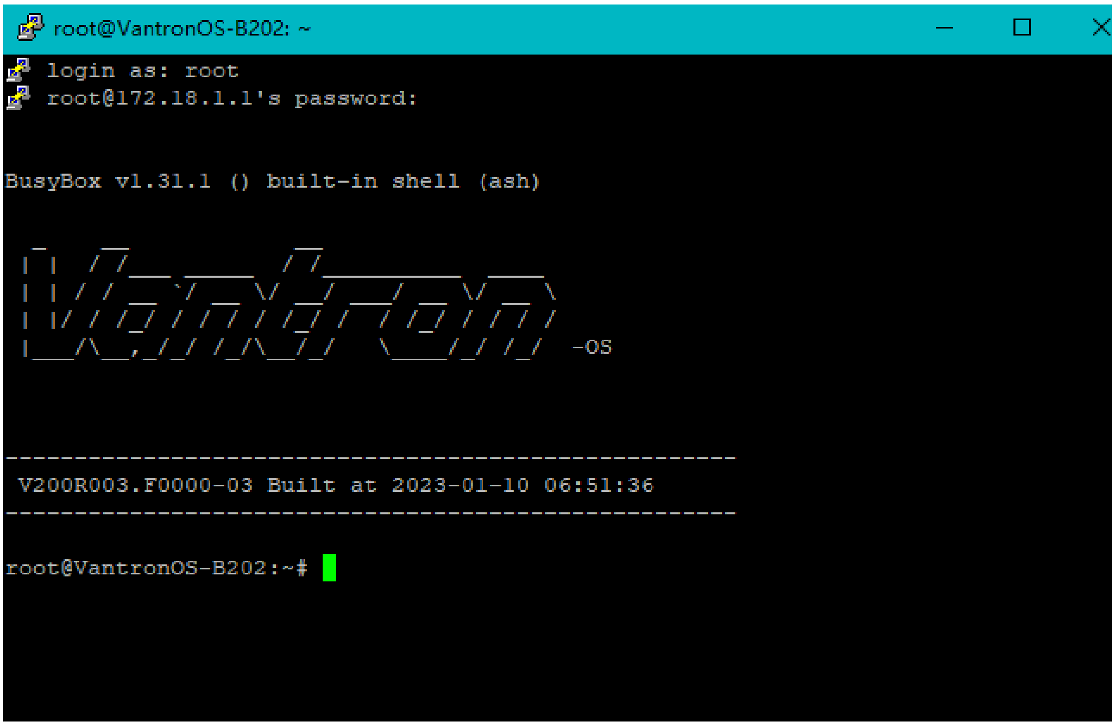
Load, save or delete a stored session

Saved Sessions: ABC

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

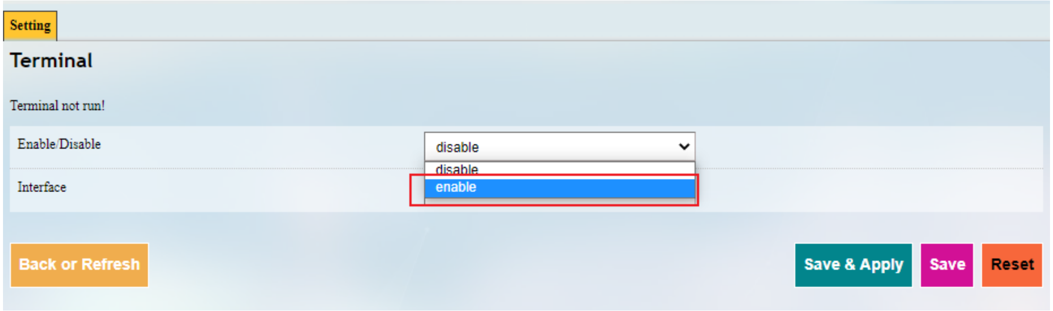
Step 7: Log in to the root account (password same as the gateway login password as shown above), and start an SSH remote session.



```
login as: root
root@172.18.1.1's password:


BusyBox v1.31.1 () built-in shell (ash)

  _    __            __
 | |  / /___ _____  / /__________  ____
 | | / / __ `/ __ \/ __/ ___/ __ \/ __ \
 | |/ / /_/ / / / / /_/ /  / /_/ / / / /
 |___/\__,_/_/ /_/\__/_/   \____/_/ /_/  -OS



-----------------------------------------------------
 V200R003.F0000-03 Built at 2023-01-10 06:51:36
-----------------------------------------------------

root@VantronOS-B202:~#
```

3.10.4 Terminal

Under the **Setting** tab, users can click **enable** from the drop-down box and **Save & Apply** to enable the web terminal and input command lines here.



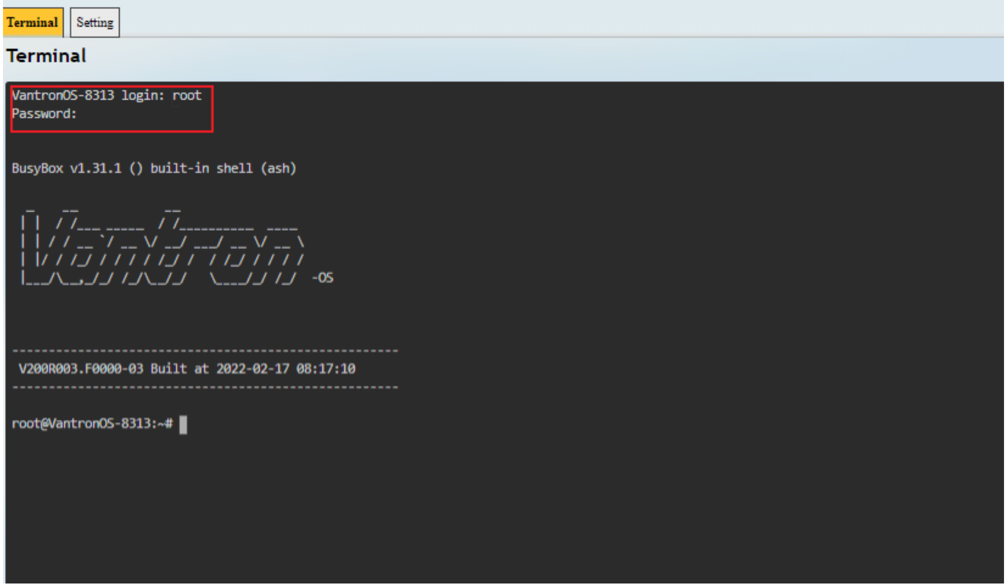
Terminal

Terminal not run!

Enable/Disable	disable
Interface	

Login name: root

Login password: rootpassword (invisible while typing)



Terminal

```
VantronOS-8313 login: root
Password:


BusyBox v1.31.1 () built-in shell (ash)

  _    __            __
 | |  / /___ _____  / /__________  ____
 | | / / __ `/ __ \/ __/ ___/ __ \/ __ \
 | |/ / /_/ / / / / /_/ /  / /_/ / / / /
 |___/\__,_/_/ /_/\__/_/   \____/_/ /_/  -OS



-----------------------------------------------------
 V200R003.F0000-03 Built at 2022-02-17 08:17:10
-----------------------------------------------------

root@VantronOS-8313:~#
```

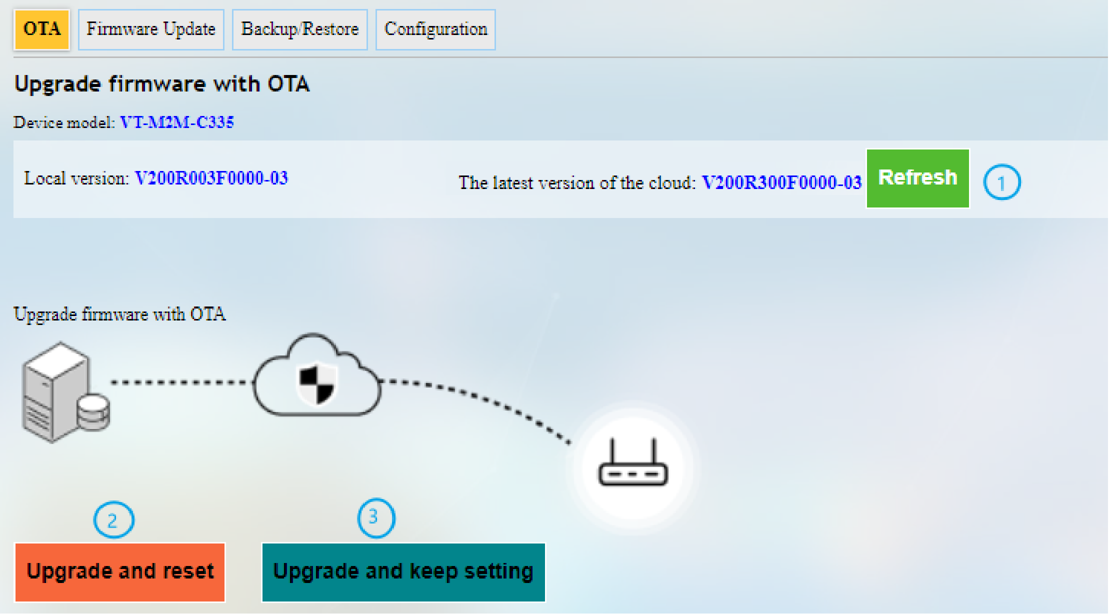
3.10.5 Mount Points

You can enable/disable automount and check the mounting information here.

3.10.6 Backup/Flash Firmware

On this page, you can backup/restore parameters, restore factory settings (clear user settings), and upgrade the firmware from local or with OTA application.

OTA upgrade

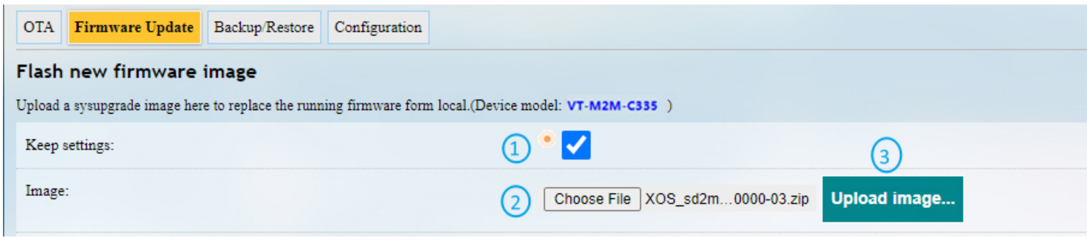

OTA
Firmware Update
Backup/Restore
Configuration
Upgrade firmware with OTA
Device model: VT-M2M-C335
Local version: V200R003F0000-03
The latest version of the cloud: V200R300F0000-03
Refresh
1
Upgrade firmware with OTA
2
3
Upgrade and reset
Upgrade and keep setting

Description of the numbered areas

1. Refresh the cloud version to the latest (internet access required)
2. Upgrade the Gateway and reset to default settings
3. Upgrade the Gateway and keep the existing settings unchanged

If the cloud version is shown **Failure**, the Gateway is not activated from the cloud, please contact your sales executive for solution.

Firmware Update



Flash new firmware image

Upload a sysupgrade image here to replace the running firmware form local.(Device model: VT-M2M-C335)

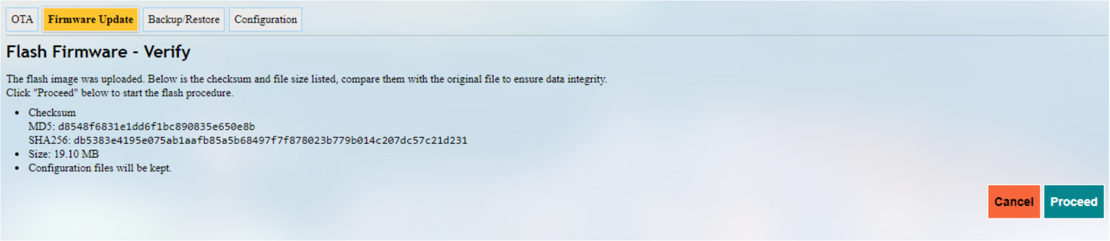
Keep settings: ☑

Image: XOS_sd2m...0000-03.zip

Description of the numbered areas

1. Check the box to keep the user settings (not recommended)
2. Select the firmware from the local directory
3. Click the button to upload the firmware

When the detailed information of the firmware is displayed, check if the firmware is correct, then click **Proceed** to start the upgrading. DO NOT power off the Gateway when firmware upgrading is in process. The login page will be refreshed once the upgrading finishes.



Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

- Checksum
  MD5: d8548f6831e1dd6f1bc890835e650e8b
  SHA256: db5383e4195e075ab1aafb85a5b68497f7f878023b779b014c207dc57c21d231
- Size: 19.10 MB
- Configuration files will be kept.

Under **Backup/Restore** tab, you can download the backup package of your settings, including configuration files and pre-set folders, restore the factory settings of the Gateway, and upload the backup package saved before.

Under **Configuration** tab, you can customize the configuration files or directories to be retained during the upgrade.

3.10.7 Reboot

Make sure you don't have any ongoing process before rebooting the Gateway.

3.11 Logout

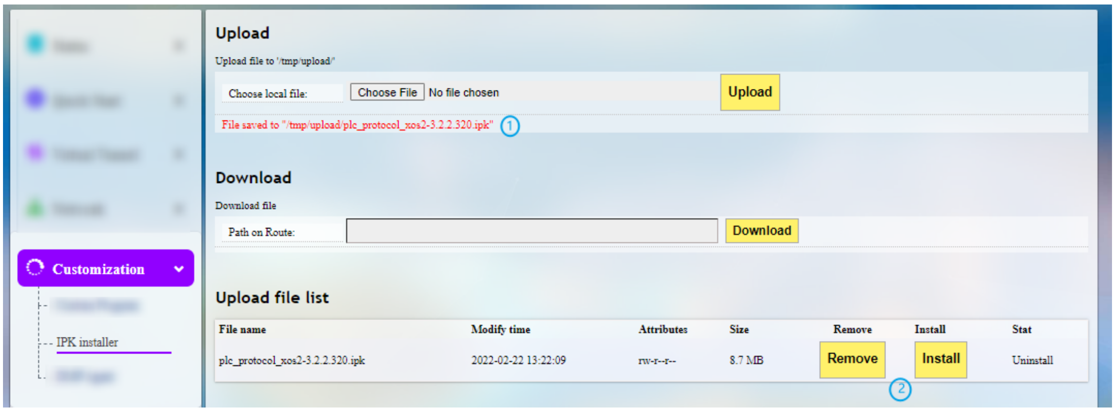
You will exit the web interface with a click on the **Logout** tab. If you need re-log the web, use the default password: **admin**. Make sure you have saved the changes before logout.

CHAPTER 4

INDUSTRIAL PROTOCOL CONFIGURATIONS

4.1 IPK Installation for Industrial Protocols

In VantronOS web interface, navigate to **Customization > IPK installer**, and upload the .ipk file for industrial protocol configuration.



Upload file to '/tmp/upload/'

Choose local file: No file chosen

File saved to "/tmp/upload/plc_protocol_xos2-3.2.2.320.ipk"

Download file

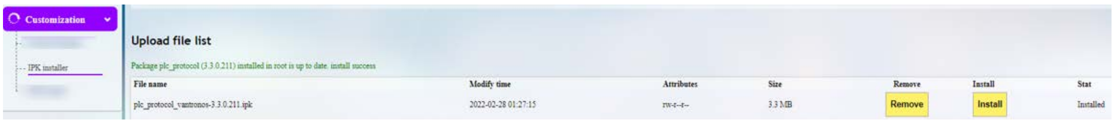
Path on Route:

File name	Modify time	Attributes	Size	Remove	Install	Stat
plc_protocol_xos2-3.2.2.320.ipk	2022-02-22 13:22:09	rw-r--r--	8.7 MB	Remove	Install	Uninstall

Description of the numbered areas

1. After the .ipk file is uploaded to the Gateway, the directory of the file will be displayed
2. You can remove or install the .ipk thereafter

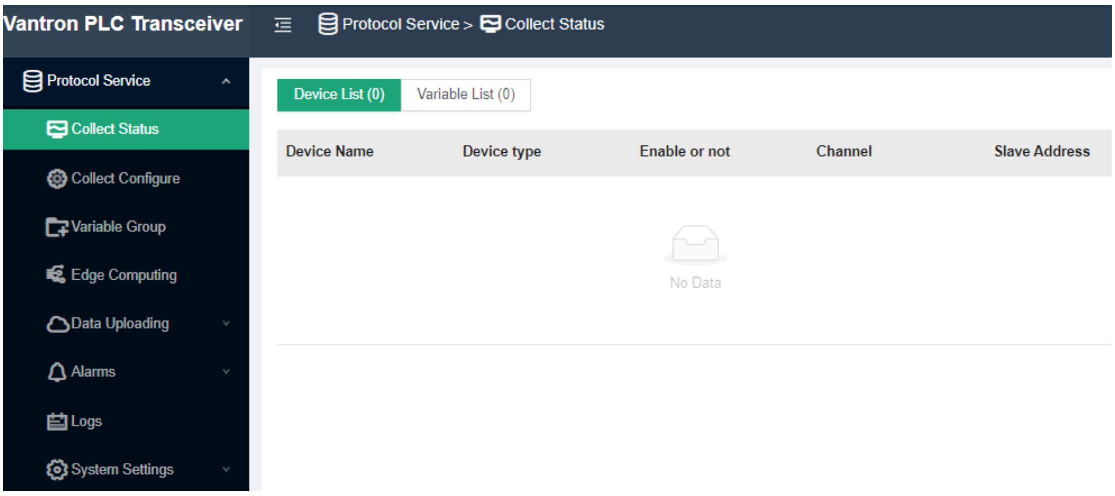
Once the .ipk file is installed, a message will be displayed suggesting the status of the file installation as shown below.



Package plc_protocol (3.3.0.211) installed in root is up to date. install success

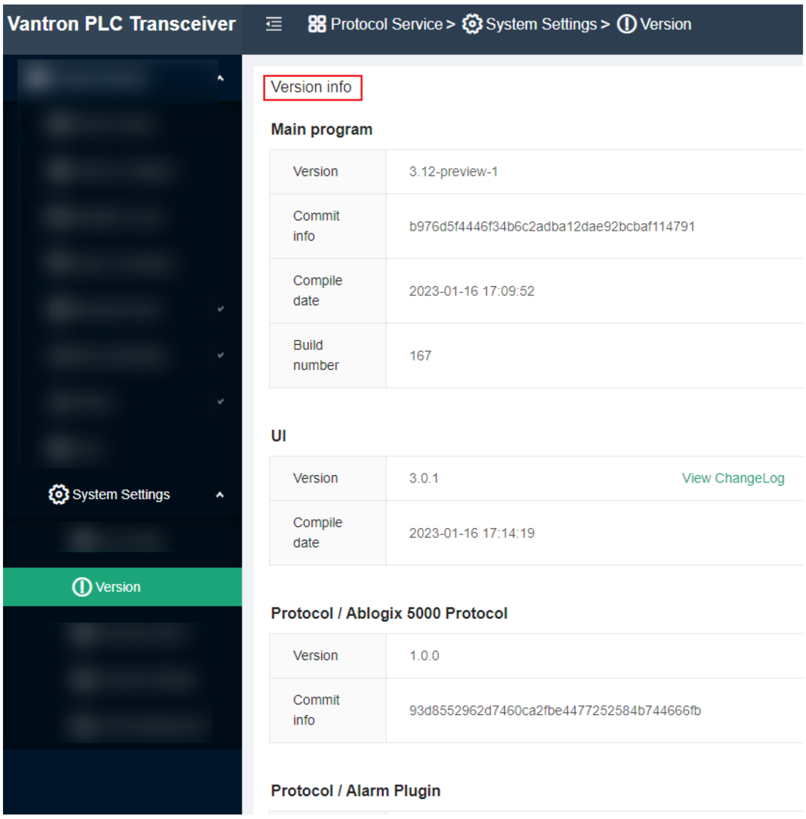
File name	Modify time	Attributes	Size	Remove	Install	Stat
plc_protocol_vantronos-3.3.0.211.ipk	2022-02-28 01:27:15	rw-r--r--	3.3 MB	Remove	Install	Installed

Input the port number (8081) after the Gateway IP in the address bar, for instance: 172.18.1.1:8081, and enter the protocol web interface which looks like below.



Device Name	Device type	Enable or not	Channel	Slave Address

You can check the version information of the protocol package under **System Settings**.



Main program

Version	3.12-preview-1
Commit info	b976d5f4446f34b6c2adba12dae92bcbaf114791
Compile date	2023-01-16 17:09:52
Build number	167

UI

Version	3.0.1	View ChangeLog
Compile date	2023-01-16 17:14:19	

Protocol / Ablogix 5000 Protocol

Version	1.0.0
Commit info	93d8552962d7460ca2fbe4477252584b744666fb

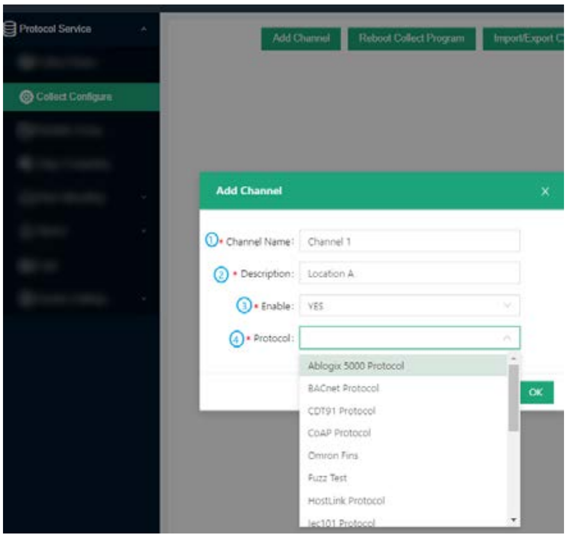
Protocol / Alarm Plugin

4.2 Protocol Configuration and Application

To use a protocol for data acquisition and edge computing, figure out the device model you are using for data collection and configure the protocol accordingly.

4.2.1 Configuration of Data Acquisition Protocols

Click **Collect Configure** on the left navigation pane to add a channel for data collection.

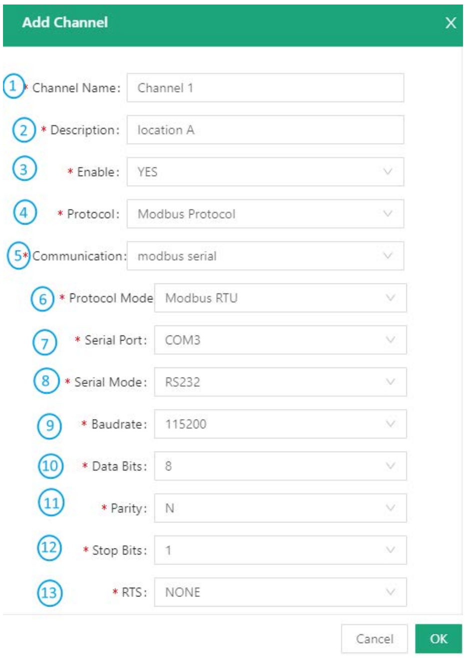


① * Channel Name: Channel 1
② * Description: Location A
③ * Enable: YES
④ * Protocol:

Description of the numbered areas

1. Enter a channel name that shall not be any one of the names in use
2. Describe the channel
3. To enable the channel or not (Yes by default)
4. Select a protocol type from the drop-down list based on the model of the data collection device (the protocols are supported by the .ipk file installed)

For certain protocol, more configuration parameters are required. Taking Modbus RTU protocol as an example, further information is needed.

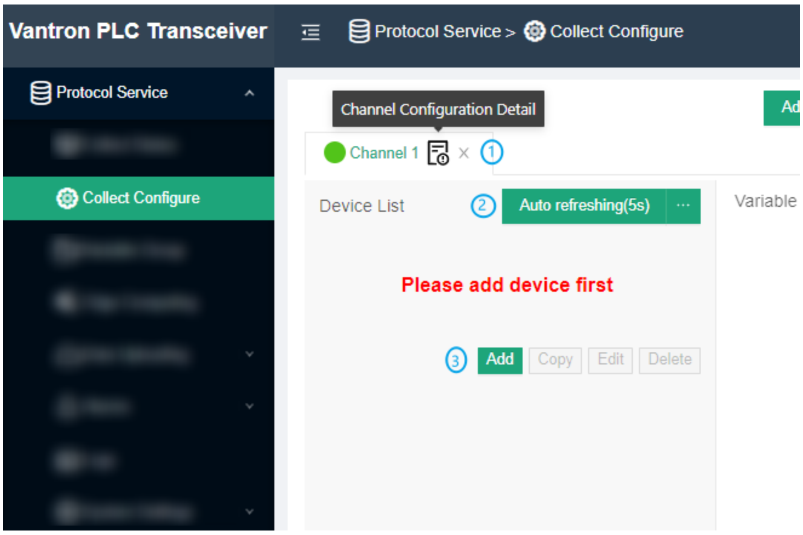


* Channel Name: Channel 1
* Description: location A
* Enable: YES
* Protocol: Modbus Protocol
* Communication: modbus serial
* Protocol Mode Modbus RTU
* Serial Port: COM3
* Serial Mode: RS232
* Baudrate: 115200
* Data Bits: 8
* Parity: N
* Stop Bits: 1
* RTS: NONE

Description of the numbered areas

4. Select Modbus protocol from the drop-down list
5. Choose serial communication (TCP communication also available)
6. Both Modbus RTU and Modbus ASCII are available (Modbus RTU for illustration)
7. Select related serial port as identified by the device manager
8. Determine the mode of the serial port (the options vary with the gateway model)
9. Choose the baud rate
10. The data bit in communication (8 bits for RTU communication by default)
11. There are three parity bits: even, odd, and non-parity
12. The stop bit represents the last bit in a single package, and the typical value includes 1, 1.5 and 2
13. Select to enable request to send (RTS) protocol or not

After configuration of the protocol channel, the protocol will be displayed on the page. You can make subsequent changes to the channel like deletion or edition.



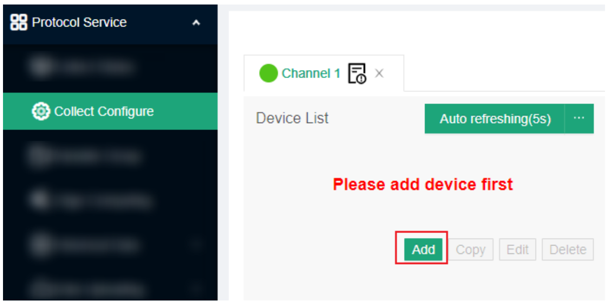
Description of the numbered areas

1. Delete the channel or access the detail page of the channel and make changes accordingly, including disabling the channel
2. The channel is set to refresh automatically every 5 seconds, and you can assign an optional value between 1 and 99 for auto refreshing
3. Add a device (e.g., a PLC) for data collection

4.2.2 Device Configuration

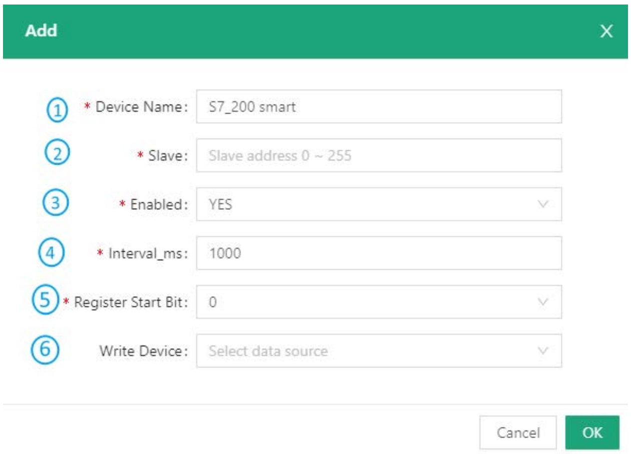
Before you can add a data collection or upload task for a data collection device (PLC for illustration purpose hereinafter) on the web portal, please connect the PLC to the gateway first, then add the device on the configuration page of the portal.

Click **Add** and input the device information in the pop-up.



The device information to be input varies with the protocol you added for communication.

Take Siemens S7-200 Smart PLC for example, if you use Ethernet communication, you have to make sure **S7 protocol** is included in the .ipk file and you have created a channel for the protocol. Then you can proceed with the PLC setup under the channel.



Add

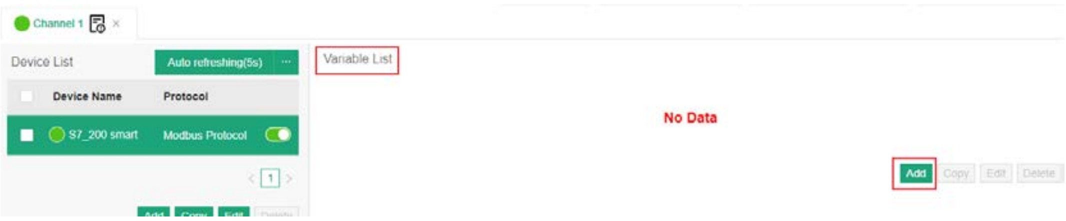
1. * Device Name: S7_200 smart
2. * Slave: Slave address 0 ~ 255
3. * Enabled: YES
4. * Interval_ms: 1000
5. * Register Start Bit: 0
6. Write Device: Select data source

Description of the numbered areas

1. Enter a device name
2. Input a slave address between 0 and 255
3. Choose to enable the device or not
4. Set an interval for data collection
5. Set a start bit for the register
6. Select the data source for distribution (provided there is collected data)

4.2.3 Add Variables to the Device

After configuration of the PLC for data collection, click **Add** under the **Variable List** next to the channel and device to set the variables for the PLC.

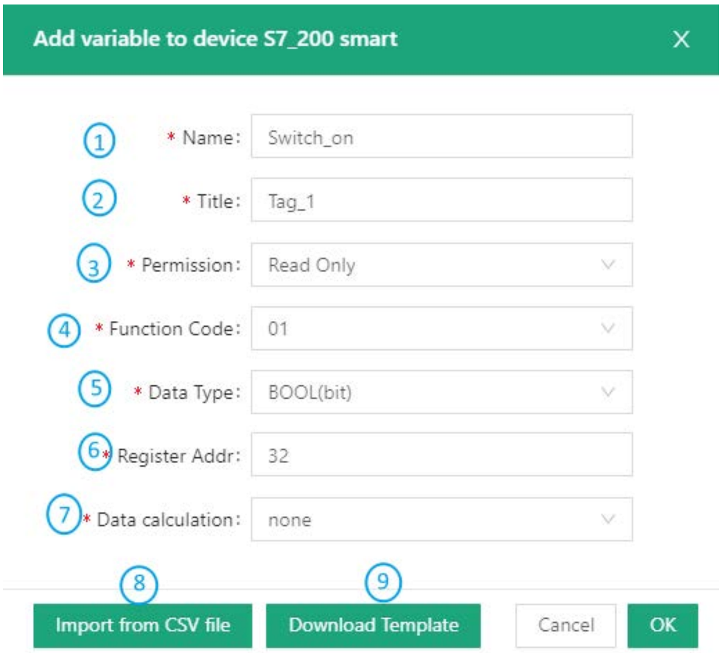


Device List

□	Device Name	Protocol
□	S7_200 smart	Modbus Protocol

Variable List

No Data

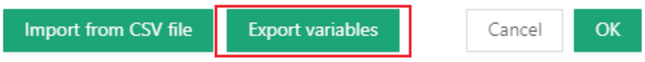


Add variable to device S7_200 smart

* Name: Switch_on
* Title: Tag_1
* Permission: Read Only
* Function Code: 01
* Data Type: BOOL(bit)
* Register Addr: 32
* Data calculation: none

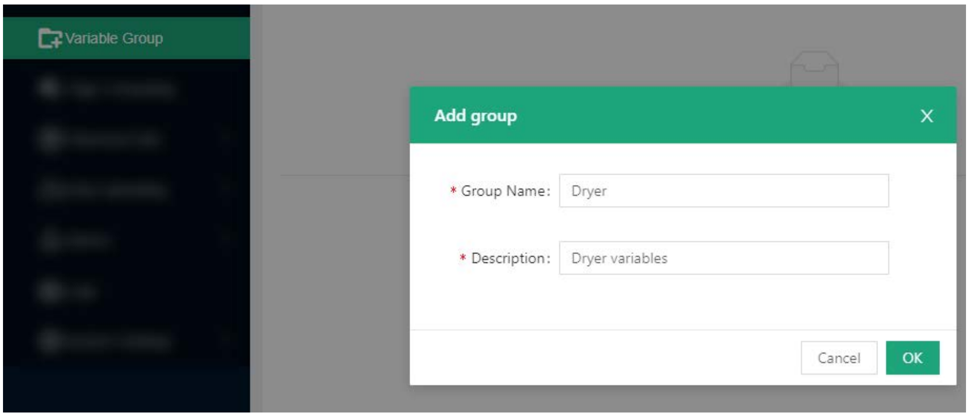
Description of the numbered areas

1. Set a variable name that the PLC collects
2. Enter a title to describe the variable
3. Set the access permission of the variable
4. Select a function code
5. Choose the data type (Bool)
6. Input or adjust the register address from 1 to 65535
7. Set a method for data calculation
8. You can skip the fields above and upload a csv file for bulk setup of the variables
9. If case you don’t know where to get started for the first-time setup, you can download the template for the compulsory fields in creating a csv file (If you have already added the variables, you can export the variables for future use)



The data type (5) is subject to the type of PLC connected to the gateway.

After configuration of the PLC and the variables at different nodes, you can export the configurations to the local for backup, or, you can import the configurations backed up earlier.

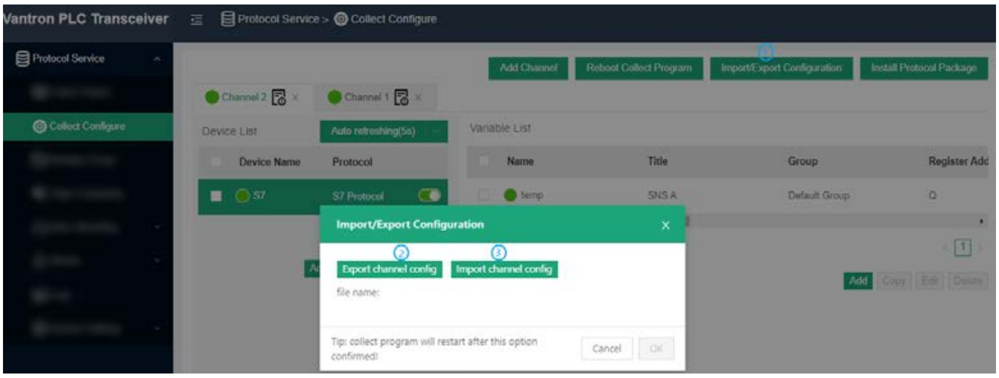


Add group

* Group Name: Dryer

* Description: Dryer variables

After setting up the PLC and variables, you can export the configurations for local backup, or, you can import the configurations backed up earlier.



Import/Export Configuration

file name:

Tip: collect program will restart after this option confirmed!

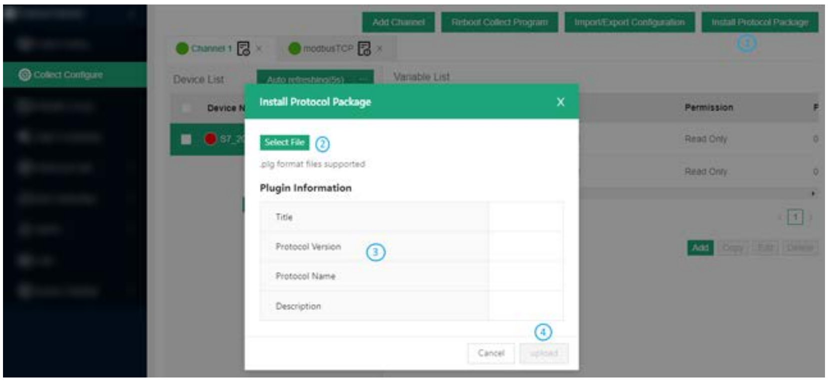
Description of the numbered areas

1. Click **Import/Export Configuration** to access the page
2. Export the channel configurations to the local
3. Import the channel configurations from the local

Exporting the configurations will back up the configurations of every single channel on the page.

If you click the **Reboot Collect Program** button, the channels and respective collection tasks will be restarted.

Clicking the **Install Protocol Package** button allows you to upload protocol plugins here.



Install Protocol Package

.plg format files supported

Plugin Information

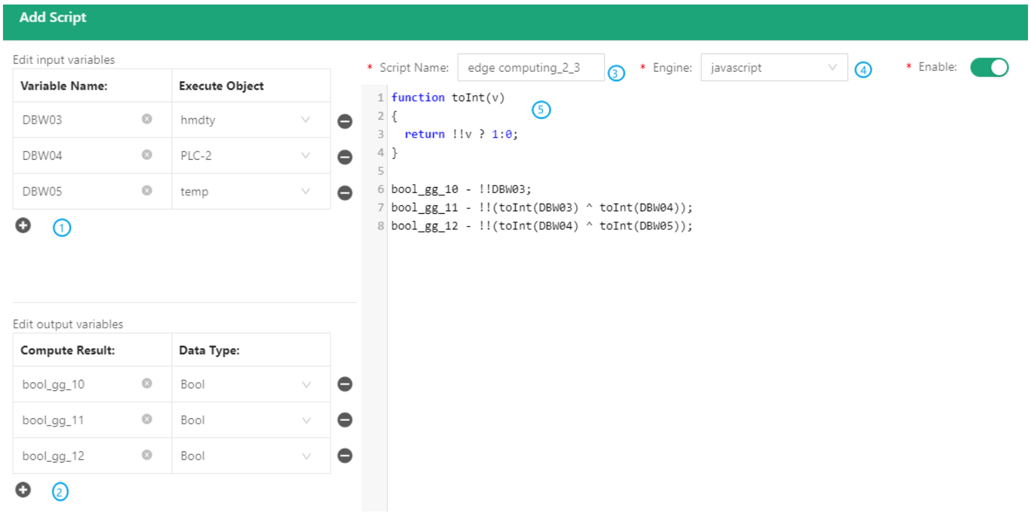
Title	
Protocol Version	
Protocol Name	
Description	

Description of the numbered areas

1. Click **Install Protocol Package** to access the upload page
2. Select the plugin from the local directory (.plg format supported)
3. The detailed plugin information will display after uploading the plugin
4. Click the button to upload the plugin

4.2.4 Edge Computing Scripts Setup

To add a script for edge computing, click **Edge Computing** from the navigation pane on the left, and input the script information in the pop-up window upon a click on **Add Script**.



Edit input variables

Variable Name:	Execute Object
DBW03	hmdty
DBW04	PLC-2
DBW05	temp

Edit output variables

Compute Result:	Data Type:
bool_gg_10	Bool
bool_gg_11	Bool
bool_gg_12	Bool

* Script Name: edge computing_2_3
* Engine: javascript
* Enable:

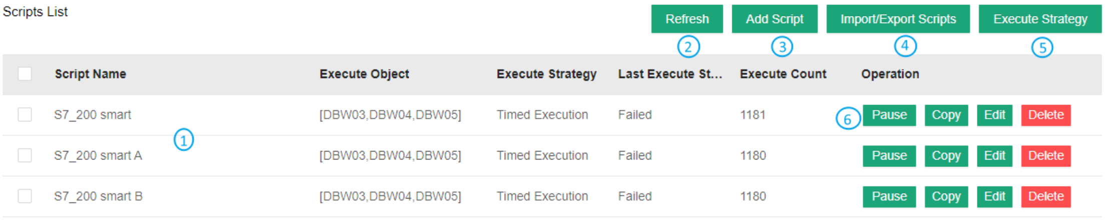
```
function toInt(v)
{
  return !!v ? 1:0;
}

bool_gg_10 - !!DBW03;
bool_gg_11 - !!(toInt(DBW03) ^ toInt(DBW04));
bool_gg_12 - !!(toInt(DBW04) ^ toInt(DBW05));
```

Description of the numbered areas

1. Edit the input variables: add a name for the input variable and an object for executing the script (more than one variable could be added)
2. Edit the output variable: add the computation result and data type
3. Click the toggle button to choose to output the results to the variables or edge nodes
4. Enter a name for the computing script
5. Select the format of the script (JavaScript, Lua and Python supported)
6. Select to enable the script or not
7. Compile the script in the window

After compilation, click **OK** to exit.

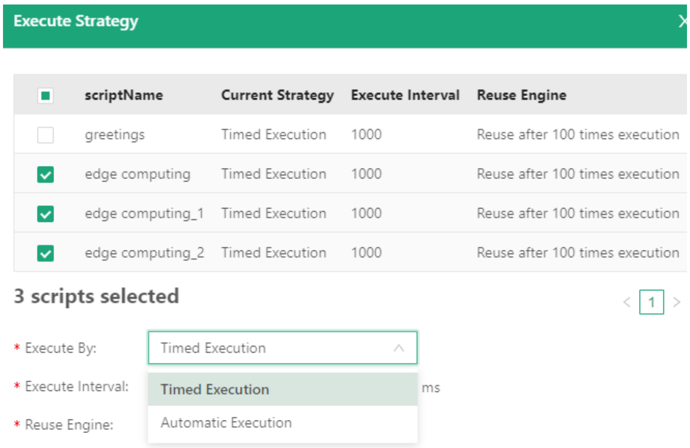
Under **Scripts List**, you can perform a series of actions to the scripts.



□	Script Name	Execute Object	Execute Strategy	Last Execute St...	Execute Count	Operation
□	S7_200 smart	[DBW03,DBW04,DBW05]	Timed Execution	Failed	1181	Pause Copy Edit Delete
□	S7_200 smart A	[DBW03,DBW04,DBW05]	Timed Execution	Failed	1180	Pause Copy Edit Delete
□	S7_200 smart B	[DBW03,DBW04,DBW05]	Timed Execution	Failed	1180	Pause Copy Edit Delete

Description of the numbered areas

1. Script list
2. Refresh the script
3. Add a script
4. Import/export scripts
5. Script execution strategy (you can assign a strategy to multiple scripts upon click of this button)



■	scriptName	Current Strategy	Execute Interval	Reuse Engine
□	greetings	Timed Execution	1000	Reuse after 100 times execution
☑	edge computing	Timed Execution	1000	Reuse after 100 times execution
☑	edge computing_1	Timed Execution	1000	Reuse after 100 times execution
☑	edge computing_2	Timed Execution	1000	Reuse after 100 times execution

3 scripts selected

* Execute By: Timed Execution
* Execute Interval: Timed Execution / Automatic Execution ms
* Reuse Engine:

The scripts are designed to be executed automatically or at a scheduled time.

Automatic execution: triggered when there is abnormality with the execution object.

Timed execution: the system is scheduled to execute the script every 1000ms by default, and you can adjust the interval.

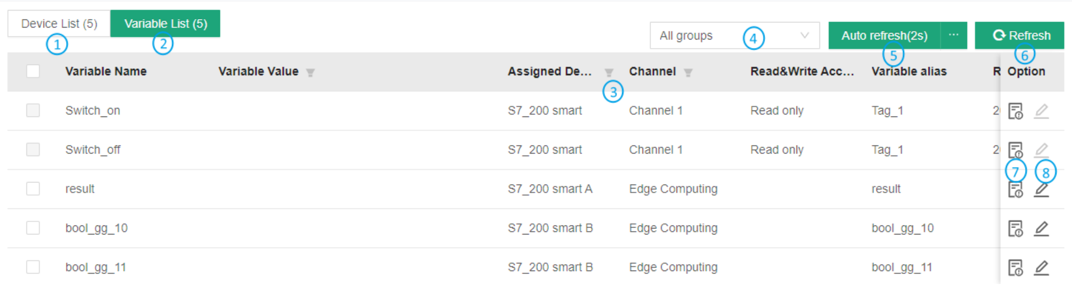
Execution interval refers to the time elapsed before next execution (1000ms by default)

Reuse Context allows you to set a restart mechanism for the scripts

6. Start/pause, copy, edit or delete the script. (You can access the script information and the execution log upon a click of the **Edit** button)

4.2.5 Collection Status

When the setup finishes, you can check the information about the devices and variables under **Collect Status**.



	Variable Name	Variable Value	Assigned De...	Channel	Read&Write Acc...	Variable alias	R	Option
□	Switch_on		S7_200 smart	Channel 1	Read only	Tag_1	2	
□	Switch_off		S7_200 smart	Channel 1	Read only	Tag_1	2	
□	result		S7_200 smart A	Edge Computing		result		
□	bool_gg_10		S7_200 smart B	Edge Computing		bool_gg_10		
□	bool_gg_11		S7_200 smart B	Edge Computing		bool_gg_11		

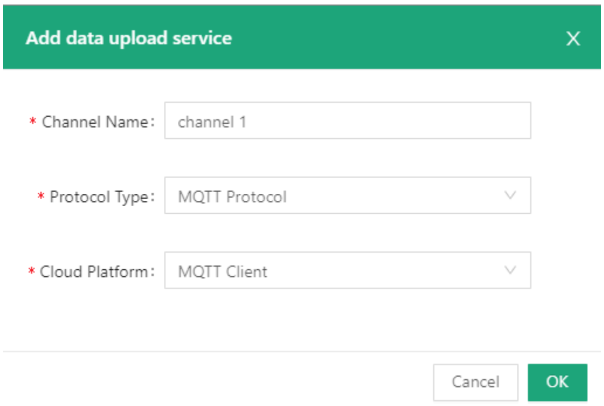
Description of the numbered areas

1. Device list
2. Variable list
3. Use the filter to screen out the specific information
4. Select a variable group
5. Auto refresh interval
6. Manual refresh
7. Variable details
8. Data distribution settings

4.2.6 Data Upload and Encapsulation

Field data collected will be uploaded to the cloud platform via protocols after edge computing. Take MQTT protocol as an example, follow the steps below for relevant settings.

- Expand **Data Uploading** tab from the navigation pane and click **Upload Config**;
- Click the **Add** button on the upper right corner to add a data upload task, and click **OK**;

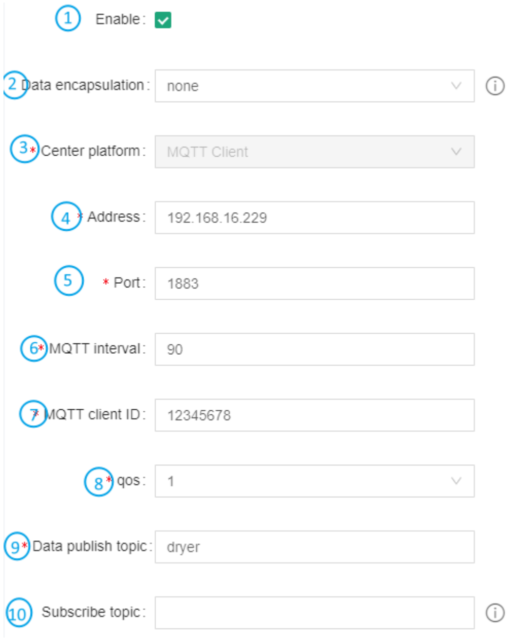


* Channel Name: channel 1

* Protocol Type: MQTT Protocol

* Cloud Platform: MQTT Client

- Configure the MQTT client in the pop-up window.



Enable: ☑

Data encapsulation: none

* Center platform: MQTT Client

* Address: 192.168.16.229

* Port: 1883

* MQTT interval: 90

* MQTT client ID: 12345678

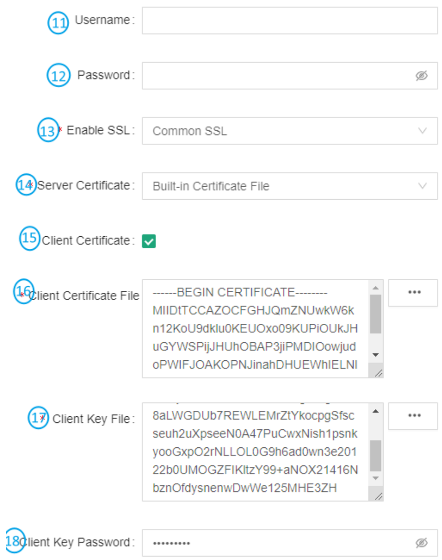
* qos: 1

* Data publish topic: dryer

Subscribe topic:

Description of the numbered areas

1. Select to enable data uploading or not after the configuration, and the data collected will be automatically uploaded to the cloud platform if enabled
2. Determine the data encapsulation format (no format by default)
3. The center platform is automatically filled and not changeable
4. Fill in the IP address of the MQTT server
5. The port number is automatically filled (1883)
6. The client will send a message to the server within a heartbeat interval (90 seconds by default and adjustable), otherwise the client network will be disconnected
7. Input the MQTT client ID: a unique identifier, unrepeatable
8. Set the quality of service (QoS) to ensure the reliability of the message
    - QoS 0: The message will be sent once at the maximum. If the client is not available, the message will get lost.
    - QoS 1: The message will be sent at least once.
    - QoS 2: The message will be sent only once.
9. Data publish topic: used for MQTT messaging to identify which message channel the payload data is supposed to be published
10. Topic for MQTT message subscription which enables the server to send message to a client for the control purpose



11 Username:

12 Password:

13 * Enable SSL: Common SSL

14 * Server Certificate: Built-in Certificate File

15 Client Certificate: ☑

16 * Client Certificate File

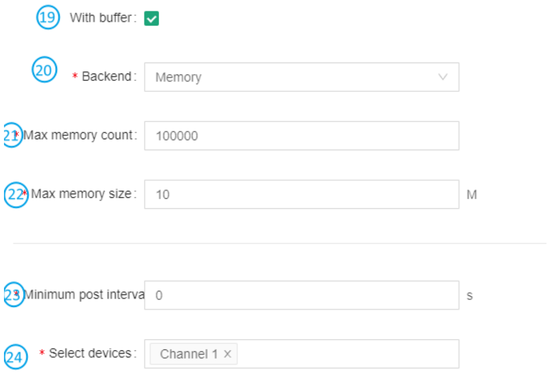
```
------BEGIN CERTIFICATE--------
MIIDtTCCAZOCFGHJQmZNUwkW6k
n12KoU9dklu0KEUOxo09KUPiOUkJH
uGYWSPijJHUhOBAP3jiPMDIOowjud
oPWIFJOAKOPNJinahDHUEWhIELNI
```

17 * Client Key File:

```
8aLWGDUb7REWLEMrZtYkocpgSfsc
seuh2uXpseeN0A47PuCwxNish1psnk
yooGxpO2rNLLOL0G9h6ad0wn3e201
22b0UMOGZFIKltzY99+aNOX21416N
bznOfdysnenwDwWe125MHE3ZH
```

18 Client Key Password: •••••••••

11. Input a username (non-compulsory)
12. Input the password (non-compulsory)
13. Select to enable SSL or not (if yes, choose between common SSL and national SSL)
14. If common SSL is enabled, select a certification mode for the server
15. Select to enable client certificate or not
16. If yes, a client certificate file is needed
17. If yes, a client key file is also needed
18. Input a client key password (non-compulsory)



19 With buffer: ☑

20 * Backend: Memory

21 * Max memory count: 100000

22 * Max memory size: 10 M

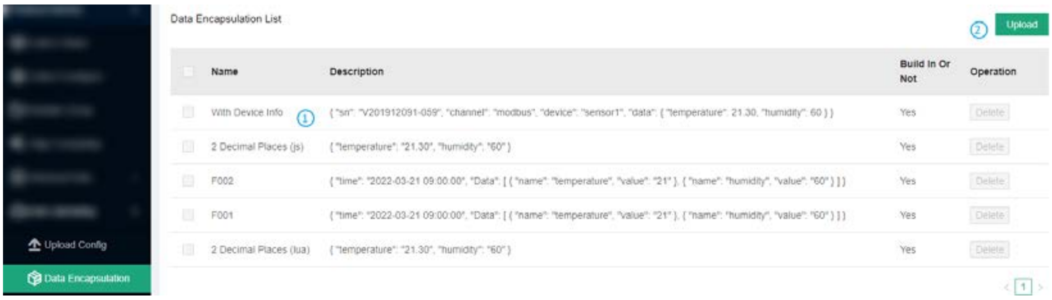
23 * Minimum post interva 0 s

24 * Select devices: Channel 1 ×

19. Select to enable data caching or not
20. If yes, choose a medium for data caching (caching to memory by default)
21. Determine the maximum memory count
22. Determine the maximum memory size
23. Input a minimum post interval
24. Select the device of the source data

The configurations will take effect after you click **Submit**. Then users can browse the data uploaded to the MQTT platform for data view, statistics, analysis, etc.

In the Data Encapsulation page, you can upload encapsulated data or configure the encapsulation format of the data.



Data Encapsulation List

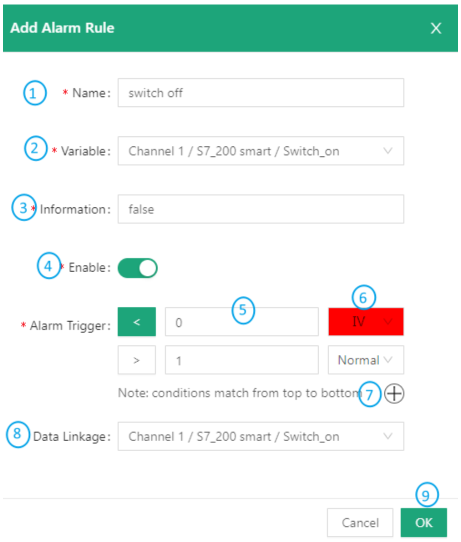
	Name	Description	Build In Or Not	Operation
□	With Device Info	{ "sn": "V201912091-059", "channel": "modbus", "device": "sensor1", "data": { "temperature": 21.30, "humidity": 60 } }	Yes	Delete
□	2 Decimal Places (js)	{ "temperature": "21.30", "humidity": "60" }	Yes	Delete
□	F002	{ "time": "2022-03-21 09:00:00", "Data": [{ "name": "temperature", "value": "21" }, { "name": "humidity", "value": "60" }] }	Yes	Delete
□	F001	{ "time": "2022-03-21 09:00:00", "Data": [{ "name": "temperature", "value": "21" }, { "name": "humidity", "value": "60" }] }	Yes	Delete
□	2 Decimal Places (lua)	{ "temperature": "21.30", "humidity": "60" }	Yes	Delete

Description of the numbered areas

1. Description of the built-in data encapsulation format
2. Click to upload. json data for encapsulation

4.2.7 Alarm

Under **Alarms > Alarm Config**, you can add alarm rules for the variables. The device will alarm when a rule is triggered and the alarm mutes when the condition changes to not meeting the rule.



Add Alarm Rule

* Name: switch off

* Variable: Channel 1 / S7_200 smart / Switch_on

* Information: false

* Enable: ●

* Alarm Trigger: < 0 IV
> 1 Normal

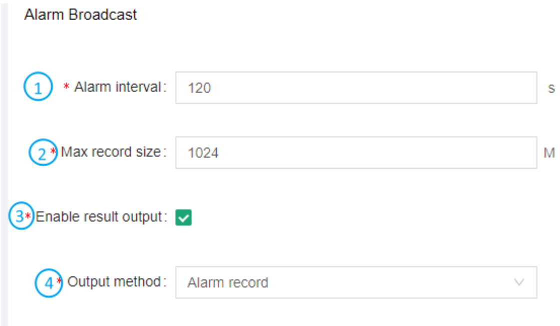
Note: conditions match from top to botton

Data Linkage: Channel 1 / S7_200 smart / Switch_on

Description of the numbered areas

1. Set a name for the alarm rule
2. Select the variable for the alarm rule to be applied to
3. Input the alarm message to be display in case of an alarm
4. Select to enable the alarm rule or not
5. Set the thresholds for triggering the alarm (thresholds will be applied from top down)
6. Set an alarm level (under normal level, no alarm will be triggered)
7. Click "+" to add a trigger condition, click "-" to delete a trigger condition
8. Select a data linkage
9. Click to save the alarm rule

When the alarm rules are created, you can set the parameters for pushing an alarm on the **Alarm Broadcast** page.



Alarm Broadcast

1 * Alarm interval: 120 s

2 * Max record size: 1024 M

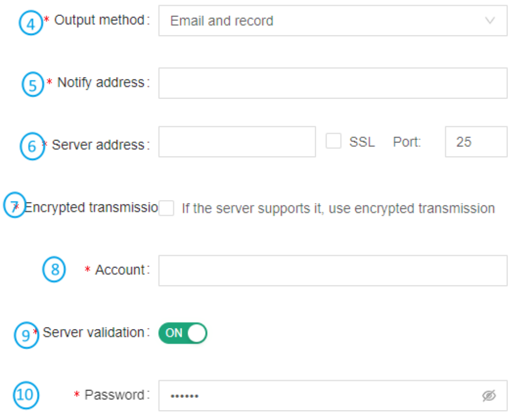
3 * Enable result output: ☑

4 * Output method: Alarm record

Description of the numbered areas

1. Set the interval for an alarm, 120 seconds by default
2. The maximum storage space for the alarm log is 1024M by default
3. Select to enable result output or not
4. Select to output the alarms to the alarm log or alarm log + email

If you choose the latter, please add information about the email.



4 * Output method: Email and record

5 * Notify address:

6 * Server address: □ SSL Port: 25

7 Encrypted transmissio □ If the server supports it, use encrypted transmission

8 * Account:

9 * Server validation: ON

10 * Password: ••••••

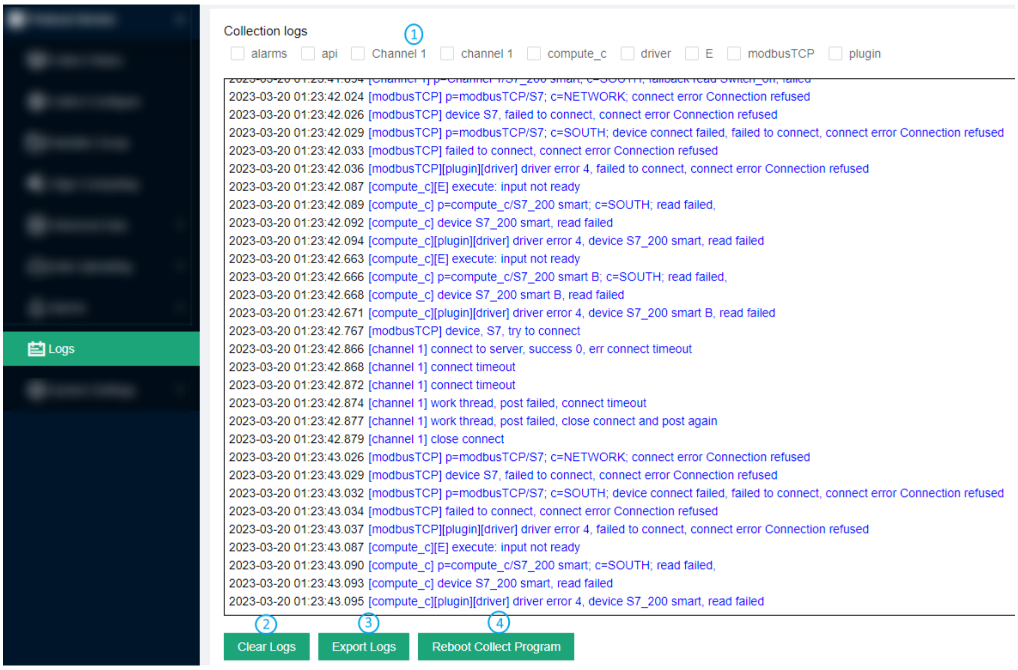
5. Input an email account for receiving the alarm messages
6. Input the outgoing server address (check the settings of the email server in use)
7. Enable encrypted transmission if the server supports
8. Input an email account for sending the alarm messages (could be same as the receiving email)
9. Toggle the server validation or not
10. If server validation is enabled, you need set the password

When you are all set, you can send a test email to check if the settings are ok, then submit the settings.

The alarm logs will be displayed on the **Alarm Record** page if any rules are triggered.

4.2.8 Logs

Data collection log and cloud service log are displayed on **Logs** page. You can make changes accordingly.


Logs
Collection logs
1
□ alarms □ api □ Channel 1 □ channel 1 □ compute_c □ driver □ E □ modbusTCP □ plugin
2
3
4
Clear Logs
Export Logs
Reboot Collect Program

```
2023-03-20 01:23:41.894 [Channel 1] p=Channel 1/S7_200 smart; c=SOUTH; fallback read Switch_on, failed
2023-03-20 01:23:42.024 [modbusTCP] p=modbusTCP/S7; c=NETWORK; connect error Connection refused
2023-03-20 01:23:42.026 [modbusTCP] device S7, failed to connect, connect error Connection refused
2023-03-20 01:23:42.029 [modbusTCP] p=modbusTCP/S7; c=SOUTH; device connect failed, failed to connect, connect error Connection refused
2023-03-20 01:23:42.033 [modbusTCP] failed to connect, connect error Connection refused
2023-03-20 01:23:42.036 [modbusTCP][plugin][driver] driver error 4, failed to connect, connect error Connection refused
2023-03-20 01:23:42.087 [compute_c][E] execute: input not ready
2023-03-20 01:23:42.089 [compute_c] p=compute_c/S7_200 smart; c=SOUTH; read failed,
2023-03-20 01:23:42.092 [compute_c] device S7_200 smart, read failed
2023-03-20 01:23:42.094 [compute_c][plugin][driver] driver error 4, device S7_200 smart, read failed
2023-03-20 01:23:42.663 [compute_c][E] execute: input not ready
2023-03-20 01:23:42.666 [compute_c] p=compute_c/S7_200 smart B; c=SOUTH; read failed,
2023-03-20 01:23:42.668 [compute_c] device S7_200 smart B, read failed
2023-03-20 01:23:42.671 [compute_c][plugin][driver] driver error 4, device S7_200 smart B, read failed
2023-03-20 01:23:42.767 [modbusTCP] device, S7, try to connect
2023-03-20 01:23:42.866 [channel 1] connect to server, success 0, err connect timeout
2023-03-20 01:23:42.868 [channel 1] connect timeout
2023-03-20 01:23:42.872 [channel 1] connect timeout
2023-03-20 01:23:42.874 [channel 1] work thread, post failed, connect timeout
2023-03-20 01:23:42.877 [channel 1] work thread, post failed, close connect and post again
2023-03-20 01:23:42.879 [channel 1] close connect
2023-03-20 01:23:43.026 [modbusTCP] p=modbusTCP/S7; c=NETWORK; connect error Connection refused
2023-03-20 01:23:43.029 [modbusTCP] device S7, failed to connect, connect error Connection refused
2023-03-20 01:23:43.032 [modbusTCP] p=modbusTCP/S7; c=SOUTH; device connect failed, failed to connect, connect error Connection refused
2023-03-20 01:23:43.034 [modbusTCP] failed to connect, connect error Connection refused
2023-03-20 01:23:43.037 [modbusTCP][plugin][driver] driver error 4, failed to connect, connect error Connection refused
2023-03-20 01:23:43.087 [compute_c][E] execute: input not ready
2023-03-20 01:23:43.090 [compute_c] p=compute_c/S7_200 smart; c=SOUTH; read failed,
2023-03-20 01:23:43.093 [compute_c] device S7_200 smart, read failed
2023-03-20 01:23:43.095 [compute_c][plugin][driver] driver error 4, device S7_200 smart, read failed
```

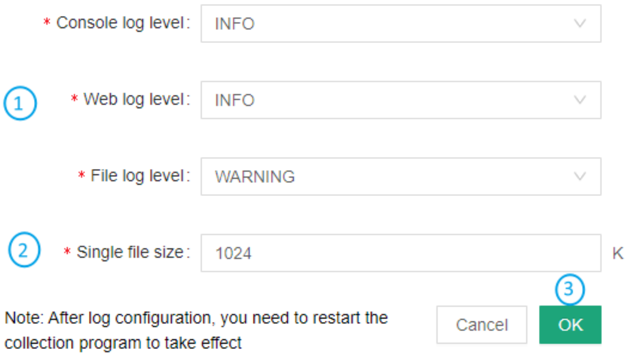
Description of the numbered areas

1. Select one or more checkboxes to screen the data collection logs
2. Clear the logs
3. Export the logs
4. Restart the collection

4.2.9 System Settings

Under **System Settings**, you can configure system parameters and check the system information concerned.

- Log Config.



* Console log level: INFO

* Web log level: INFO

* File log level: WARNING

* Single file size: 1024 K

Note: After log configuration, you need to restart the collection program to take effect

Description of the numbered areas

1. Select a level for each type of log (including NONE, FATAL, ERROR, WARNING, INFO, DEBUG, TRACE based on the emergency level)
2. Set the size of a single log (1024K by default)
3. Click **OK** to save the settings

If you have changed the settings, be sure to return to **Logs > Reboot Collect Program** to restart the collection to make the settings valid.

- Log Storage

  In the **Log Config > Log Storage** page, users can delete or download a single log/all logs.

- Running Status

  The **Running Status** page displays the system time, and the start point and running duration of the collection program.

- General Settings

  You can change the system language on the **General Settings** page.

- GSD Management

Users can upload the general station description (GSD) files on the **GSD Management** page for PROFIBUS DP or PROFINET IO communication.

CHAPTER 5

DISPOSAL AND WARRANTY

5.1 Disposal

When the device comes to end of life, you are suggested to properly dispose of the device for the sake of the environment and safety.

Before you dispose of the device, please back up your data and erase it from the device.

It is recommended that the device is disassembled prior to disposal in conformity with local regulations. Please ensure that the abandoned batteries are disposed of according to local regulations on waste disposal. Do not throw batteries into fire or put in common waste canister as they are explosive. Products or product packages labeled with the sign of "explosive" should not be disposed of like household waste but delivered to specialized electrical & electronic waste recycling/disposal center.

Proper disposal of this sort of waste helps avoid harm and adverse effect upon surroundings and people's health. Please contact local organizations or recycling/disposal center for more recycling/disposal methods of related products.

5.2 Warranty

Product warranty

VANTRON warrants to its CUSTOMER that the Product manufactured by VANTRON, or its subcontractors will conform strictly to the mutually agreed specifications and be free from defects in workmanship and materials (except that which is furnished by the CUSTOMER) upon shipment from VANTRON. VANTRON's obligation under this warranty is limited to replacing or repairing, at its option, of the Product which shall, within **24 months** after shipment, effective from invoice date, be returned to VANTRON's factory with transportation fee paid by the CUSTOMER and which shall, after examination, be disclosed to VANTRON's reasonable satisfaction to be thus defective. VANTRON shall bear the transportation fee for the shipment of the Product to the CUSTOMER.

Out-of-Warranty Repair

VANTRON will furnish the repair services for the Product which are out-of-warranty at VANTRON's then-prevailing rates for such services. At customer's request, VANTRON will provide components to the CUSTOMER for non-warranty repair. VANTRON will provide this service as long as the components are available in the market; the CUSTOMER is requested to place a purchase order up front. Parts repaired will have an extended warranty of 3 months.

Returned Products

Any Product found to be defective and covered under warranty pursuant to Clause above, shall be returned to VANTRON only upon the CUSTOMER's receipt of and with reference to a VANTRON supplied Returned Materials Authorization (RMA) number. VANTRON shall supply an RMA, when required within three (3) working days of request by the CUSTOMER. VANTRON shall submit a new invoice to the CUSTOMER upon shipping of the returned products to the CUSTOMER. Prior to the return of any products by the CUSTOMER due to rejection or warranty defect, the CUSTOMER shall afford VANTRON the opportunity to inspect such products at the CUSTOMER's location and no Product so inspected shall be returned to VANTRON unless the cause for the rejection or defect is determined to be the responsibility of VANTRON. VANTRON shall in turn provide the CUSTOMER turnaround shipment on defective Product within **fourteen (14) working days** upon its receipt at VANTRON. If such turnaround cannot be provided by VANTRON due to causes beyond the control of VANTRON, VANTRON shall document such instances and notify the CUSTOMER immediately.

Appendix Regulatory Compliance Statements

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user’s authority to operate this equipment.