

G202 Industrial Edge Computing Gateway



User Manual

Version: 1.5

© Vantron Technology, Inc. All rights reserved.

Revision History

| No. | Software Version | Description | Date |
|------|------------------|---|---------------|
| V1.0 | V200R003 | First release | Jun. 21, 2021 |
| V1.1 | V200R003 | 1. Added description of OpenVPN Server 2. Modified DMP Agent and RC to PLC | Jan. 19, 2022 |
| V1.2 | V200R003 | Modified 3.5.3 4G/LTE | Apr. 12, 2022 |
| V1.3 | V200R003 | Updated serial port description | Oct. 10, 2022 |
| V1.4 | V200R003 | Updated hardware connection | Nov. 18, 2022 |
| V1.5 | V200R003 | Updated protocol portal login and configuration | Feb. 27, 2023 |

Table of Contents

| | |
|---|----|
| Foreword | 1 |
| CHAPTER 1 HARDWARE DESCRIPTION | 5 |
| 1.1 Product Overview | 6 |
| 1.2 Unpacking | 7 |
| 1.3 Specifications..... | 8 |
| 1.4 Definition of Interfaces..... | 9 |
| 1.5 Serial Port Introduction | 12 |
| CHAPTER 2 GETTING STARTED | 13 |
| 2.1 Setting up the Gateway | 14 |
| 2.2 Gateway Login | 16 |
| 2.3 Interfacing with Vantron Gateway Management Platform | 17 |
| 2.4 Network Connectivity..... | 17 |
| 2.4.1 Ethernet Network Connectivity..... | 18 |
| 2.4.2 Wi-Fi Connectivity | 18 |
| 2.4.3 Mobile Network Connectivity | 18 |
| 2.5 Custom Settings..... | 18 |
| CHAPTER 3 GATEWAY SETUP VIA VANTRONOS | 19 |
| 3.1 Introduction to VantronOS | 20 |
| 3.2 Status..... | 21 |
| 3.3 Quick Start..... | 23 |
| 3.3.1 Network Guide | 23 |
| 3.3.2 WAN Setting – DHCP | 23 |
| 3.3.3 WAN Setting – Client | 24 |
| 3.3.4 WAN Setting – 4G/LTE | 25 |
| 3.3.5 WAN Setting – PPPoE | 26 |
| 3.3.6 WAN Setting – Static..... | 27 |
| 3.3.7 Auto Routing..... | 28 |
| 3.4 Virtual Tunnel | 30 |
| 3.4.1 OpenVPN Server..... | 30 |
| 3.4.2 VPN Client..... | 31 |
| 3.5 Network..... | 32 |
| 3.5.1 Interfaces..... | 33 |
| LAN | 34 |
| 4G | 36 |
| WAN | 37 |
| 3.5.2 Wireless (WIFI) | 39 |
| Wi-Fi – AP Mode (General settings) | 39 |
| Wi-Fi – AP Mode (Advanced setting)..... | 40 |
| Wi-Fi – Client Mode..... | 41 |
| 3.5.3 4G/LTE | 42 |
| 3.5.4 Static Routes | 44 |
| 3.5.5 Firewall | 45 |
| 3.6 User Management..... | 48 |
| 3.7 Customization..... | 49 |

| | | |
|-----------|---|----|
| 3.7.1 | Custom Program | 49 |
| 3.7.2 | IPK Installer | 49 |
| 3.7.3 | Manufacturer Info Customization | 50 |
| 3.7.4 | DMP Agent | 51 |
| 3.8 | Hardware | 52 |
| 3.8.1 | Ser2TCP | 52 |
| 3.8.2 | Ser2net environment setup and verification..... | 52 |
| 3.8.3 | Protocol comparison | 58 |
| 3.9 | Services..... | 59 |
| 3.9.1 | Dynamic DNS | 59 |
| 3.9.2 | RC to PLC | 59 |
| 3.10 | System | 60 |
| 3.10.1 | System | 60 |
| 3.10.2 | NBM Setting | 61 |
| 3.10.3 | Administration..... | 62 |
| | SSH Access | 62 |
| 3.10.4 | Terminal..... | 64 |
| 3.10.5 | Mount Points | 64 |
| 3.10.6 | Backup/Flash Firmware | 65 |
| 3.10.7 | Reboot | 66 |
| 3.11 | Logout..... | 66 |
| CHAPTER 4 | INDUSTRIAL PROTOCOL CONFIGURATIONS | 67 |
| 4.1 | IPK Installation for Industrial Protocols | 68 |
| 4.2 | Protocol Configuration and Application | 69 |
| 4.2.1 | Configuration of Data Acquisition Protocols | 69 |
| 4.2.2 | Device Configuration | 71 |
| 4.2.3 | Add Variables to the Device | 72 |
| 4.2.4 | Edge Computing Scripts Setup | 75 |
| 4.2.5 | Collection Status..... | 77 |
| 4.2.6 | Data Upload and Encapsulation | 77 |
| 4.2.7 | Alarm | 80 |
| 4.2.8 | Logs..... | 82 |
| 4.2.9 | System Settings | 82 |
| CHAPTER 5 | DISPOSAL AND WARRANTY | 84 |
| 5.1 | Disposal | 85 |
| 5.2 | Warranty..... | 86 |
| | Appendix A Regulatory Compliance Statement | 87 |
| | APPENDIX B Acronyms | 88 |

Foreword

Thank you for purchasing G202 Industrial Gateway (“the Gateway” or “the Product”). 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

Vantron Technology, Inc. (“Vantron”) reserves all rights of this manual, including the right to change the content, form, product features, and specifications contained herein at any time without prior notice. An up-to-date version of this manual is available at www.vantrontech.com.

The trademarks in this manual, registered or not, are properties of their respective owners. Under no circumstances shall any part of this user manual be copied, reproduced, translated, or sold. This manual is not intended to be altered or used for other purposes unless otherwise permitted in writing by Vantron. Vantron reserves the right of all publicly released copies of this manual.

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 **Appendix A** for Regulatory Compliance Statement.

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 |
|  | 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. The Product is designed to use 9-36V DC. 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

INTRODUCTION

1.1 Product Overview

Vantron G202 industrial edge computing gateway is an entry-level gateway launched to meet the needs of Industrial IoT applications in various scenarios. It combines dual SIM LTE, Wi-Fi, Ethernet, multiple programming languages, and virtual private network to meet diversified networking requirements. With varying industrial protocols supported, it could interact with PLCs, sensors and other IoT devices on site. G202 applies a communication tactic that uses multiple channels with failover protocol, which together with the high-reliability watchdog maintains a secure and stable network access. As is compact in size, G202 supports panel mount, DIN rail mount, and wall mount to meet the requirements of varying sites. 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.

Featuring high stability and reliability, excellent cost performance, and broad protocol accessibility, G202 industrial edge computing gateway is especially suitable for large-scale data acquisition and cloud platform communication in the following scenarios:





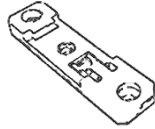

Intelligent manufacturing: injection molding machine, numerical control machine


Intelligent water conservation: water treatment

Intelligent security & intelligent transportation

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 | | Optional accessories | |
|--|-------------------------------|--|------------------------|
|  | 1 x G202 Gateway |  | 1 x Power adapter |
|  | 2 x Wi-Fi antenna |  | 1 x DC power connector |
|  | 1 x DIN rail mounting bracket |  | 2 x 4G LTE antenna |

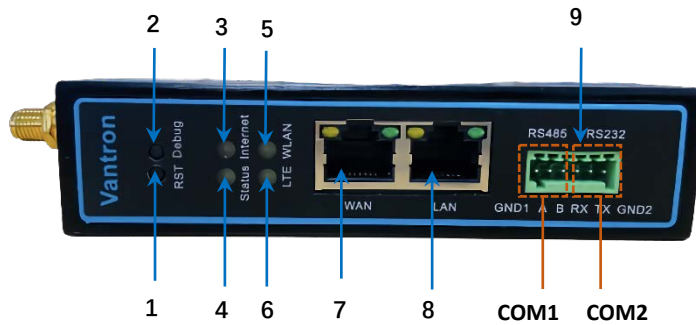
 Actual accessories might vary slightly from the list above as the customer order might differ from the standard configuration options.

1.3 Specifications

| G202 | | |
|-----------------------|----------------------------|--|
| System | Memory | 128MB DDR2 |
| | Storage | 32MB Flash 1 x Micro SD card, up to 64GB |
| Communication | Ethernet | 2 x RJ45, 10/100Mbps |
| | 4G LTE | CAT M/CAT 4 |
| | Wi-Fi | 2.4GHz, 802.11 b/g/n, 300Mbps, AP & Client |
| I/Os | Ethernet port protocol | PPP, PPPoE, DHCP, ARP |
| | Serial port | 1 x RS485 1 x RS485/RS232 (hardware determined) |
| | SIM slot | 2 x Drawer-type SIM slot |
| | Grounding | Enclosure & PCB |
| System Control | Button | 1 x Reset button 1 x Debug button |
| | LED indicator | 1 x Status 1 x Internet 1 x 4G LTE 1 x WLAN |
| Mechanical | Dimensions | 115.5mm x 85.77mm x 28.3mm |
| | Enclosure | Metal |
| | Installation | DIN rail mounting |
| | IP rating | IP30 |
| | Cooling mode | Fanless |
| Power | Input | 9-36V DC, Over-current protection, Reverse polarity protection |
| | Terminal | 3-pin 3.81mm terminal block |
| Software | OS | VantronOS |
| | SDK | Available |
| | Network management | SNMP v1/v2c/v3 |
| | Device management platform | Vantron BlueSphere |
| | IoT protocol | MQTT |
| | IPK import | Supported |
| | Interface language | Chinese and English (Default) Other languages (Optional) |
| | NTP | Supported |
| | Log | Supported |
| Security | Firewall | Supported |
| | Data security | OpenVPN, L2TP, PPTP, IPSec |
| | Link detection | Heartbeat detection, automatic reconnection |
| | Network reliability | Failover supported, link backup between Ethernet, Wi-Fi and 4G/LTE |
| | Multi-level permission | Supported |
| Application | Configuration mode | Local, remote |
| | Upgrade | Local, OTA update |
| | Networking guide | One-key configuration of LTE, Wi-Fi, and Ethernet |
| | 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 |
| Environment Condition | Temperature | Operating: -20°C ~ +60°C Storage: -40°C~+70°C |
| | Humidity | RH 5%-95% (Non-condensing) |
| | Certification | CE, FCC, PTCRB |

1.4 Definition of Interfaces

1.4.1 Front view



Button description

| No. | Button | Description |
|-----|--------|---|
| 1 | RST | The gateway will be factory reset with user data and custom configurations erased when this button is pressed for 3-10 seconds. The system will reboot upon reset of the gateway. |
| 2 | Debug | Under normal circumstances, COM2 (labeled as RS232 on the enclosure) is used for serial communication by default. Long press of the debug button before power application will switch the port to the debug mode. However, when the Gateway is powered off, the port will restore to the communication mode. Refer to 1.5 Serial Port Introduction for details. |

LED indicators

1. Internet indicator

| No. | Network connectivity of the Gateway | Description |
|-----|-------------------------------------|----------------------|
| 3 | Yes | The indicator blinks |
| | No | The indicator is off |

2. Status indicator

| No. | System action | Description |
|-----|-------------------------|------------------------------|
| 4 | System bootup | The indicator blinks |
| | System running properly | The indicator is solid green |

3. WLAN (Wi-Fi) indicator

| No. | Wi-Fi module status | Description |
|-----|--|------------------------------|
| 5 | The Wi-Fi module is on | The indicator is solid green |
| | A client is connected to the Gateway via Wi-Fi | The indicator blinks |
| | The Wi-Fi module is off | The indicator is off |

4. 4G LTE signal strength indicator

| No. | 4G LTE module status | Description |
|-----|--|------------------------------|
| 6 | The 4G LTE module is on | The indicator is solid green |
| | The 4G LTE module is off/not implemented | The indicator is off |

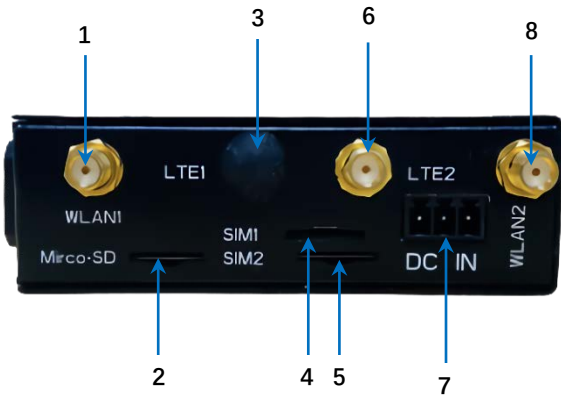
Ethernet ports description:

| No. | Port | Description |
|-----|------|---|
| 7 | WAN | Set as ETH0.2 in VantronOS and works in WAN area by default |
| 8 | LAN | Set as ETH0.1 in VantronOS and works in LAN area by default |

Green terminal block:

| No. | Enclosure label | Description |
|-----|-----------------|---|
| 9 | RS485 | Used for serial communication |
| | RS232 | Serial communication by default, serial debugging available |

1.4.2 Left side view



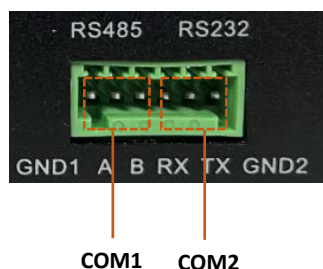
| Interface | Description |
|-----------|-------------------------|
| 1 | WLAN antenna 1 |
| 2 | Micro SD card slot |
| 3 | 4G LTE antenna 1 |
| 4 | Micro SIM card slot 1 |
| 5 | Micro SIM card slot 2 |
| 6 | 4G LTE antenna 2 |
| 7 | 9-36V DC power terminal |
| 8 | WLAN antenna 2 |

1.4.3 Right side view



| Interface | Description |
|-----------|-----------------|
| 1 | Grounding screw |

1.5 Serial Port Introduction



There are two serial ports on the green terminal block of the Gateway, one is RS485 (COM1) and the other is configurable to RS485 or RS232 (configured before shipment).

COM2 is used for serial communication by default. To activate the debug mode (settings: 57600 8N1), users can long press the debug button before power application and release until there is output data on the host PC. When the Gateway is powered off, the port will restore to the communication mode. However, it is recommended that COM2 is not used for serial debugging when it is configured to RS485 due to the likeliness of garbled data and the need of an RS232 to RS485 adapter.

Pinout description:

| No. (Left to right) | Pin | Node name | Port | Type | Definition |
|------------------------|------|------------|------|------|-------------------------------------|
| 1 | GND1 | /dev/ttyS1 | COM1 | P | RS485 Isolated grounding |
| 2 | A | | | I/O | RS485-A signal |
| 3 | B | | | I/O | RS485-B signal |
| 4 | RX/A | /dev/ttyS0 | COM2 | I | RS232 RXD signal/ RS485-A signal |
| 5 | TX/B | | | O | RS232 TXD signal/ RS485-B signal |
| 6 | GND2 | | | P | Isolated grounding |

Input the following command lines in a terminal to use a serial communication program (e.g., microcom) to open the serial ports:

1. To open COM2:

```
~# microcom /dev/ttyS0 -s 115200
```

2. To open COM1:

```
~# microcom /dev/ttyS1 -s 115200
```

 Please refer to **Appendix B** for the definition of the acronyms mentioned above.

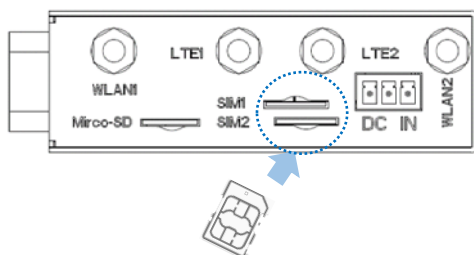
CHAPTER 2

GETTING STARTED

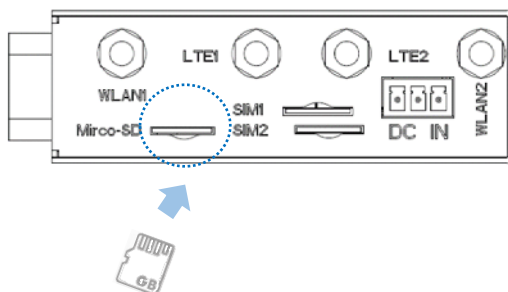
2.1 Setting up the Gateway

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

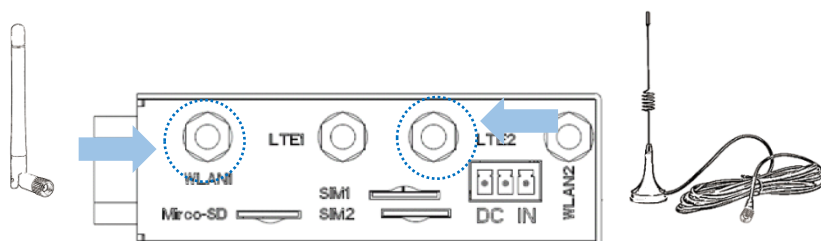
1. Use the mounting bracket and screws provided to install the Gateway to a secure place;
2. Insert an activated SIM card into SIM1 slot with the gold-colored contacts facing down, or, insert into SIM2 slot with the gold-colored contacts facing up, or, insert two activated SIM cards to the slots, respectively;



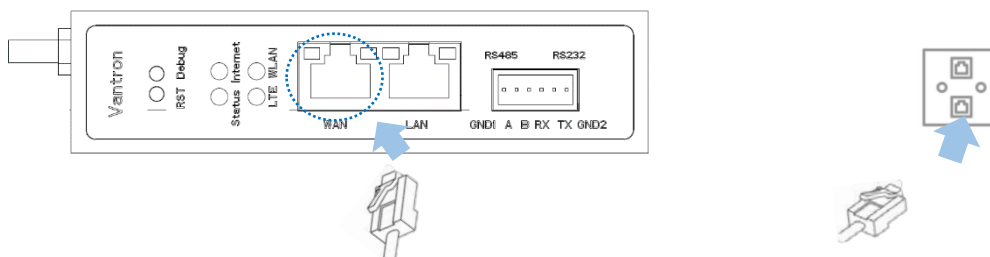
3. Push the SIM card to secure it;
4. Insert a Micro SD card into the Micro SD slot with the gold-colored pins facing up;



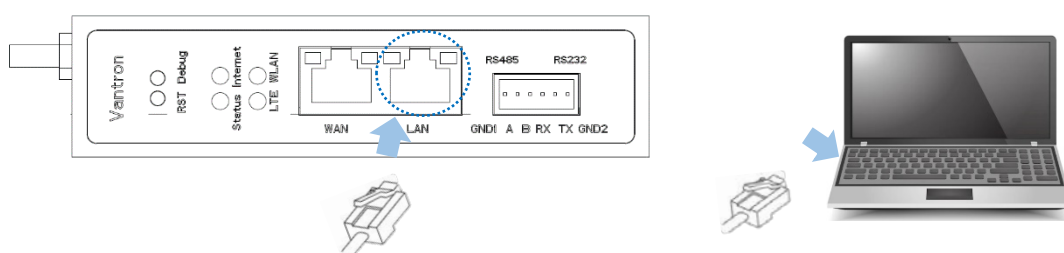
5. Install the rubber stick antennas to the WLAN antenna connectors and the sucker antennas to the LTE antenna connectors;



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

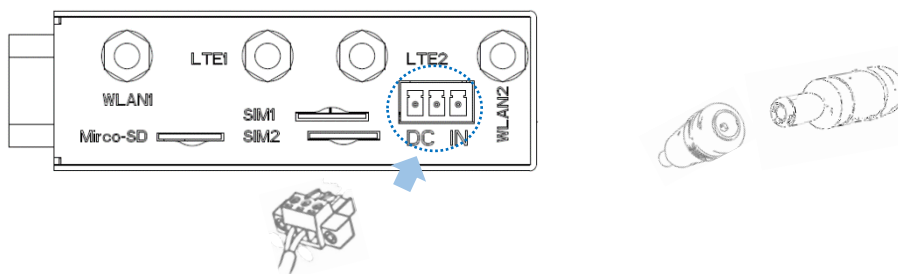


7. Connect one end of an Ethernet cable to the LAN port of the Gateway and the other to your PC;



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

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 turn on the Gateway;
10. The power indicator will turn solid green upon power application.

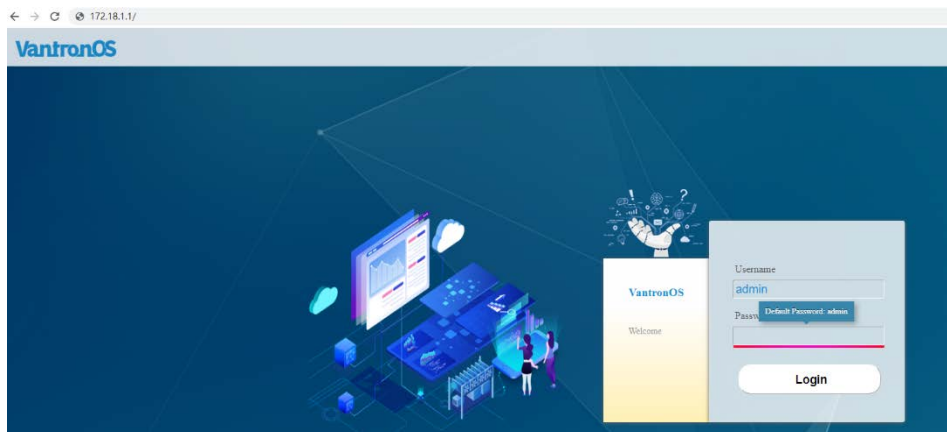
▶ The antennas might be different from what used for illustration here. Should you have any trouble installing the antennas, please contact the sales executive for solution.

▶ Customers have the option for 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 the 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 [3.10.3](#) 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.



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 the IP addresses manually.

2.4.2 Wi-Fi Connectivity

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

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 the interconnection and interaction between users and the Industrial Internet of Things.


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.



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 |
|--------------|-------------------|
| 172.18.1.1 | 12:21:d5:11:c5:d0 |
| 172.18.1.1 | 86:a2:a0:2e:22:43 |
| 172.18.1.1 | 02:a5:e3:ea:a3:91 |
| 172.18.1.1 | f8:c3:9e:97:a4:ff |
| 172.18.1.1 | 62:54:8b:61:7f:8a |
| 172.18.1.1 | 42:63:de:da:77:85 |
| 172.18.1.1 | 18:c0:4d:43:ad:8b |

11. Details of the access port

- ▶ The image illustration varies when the Gateway has cellular connection.



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

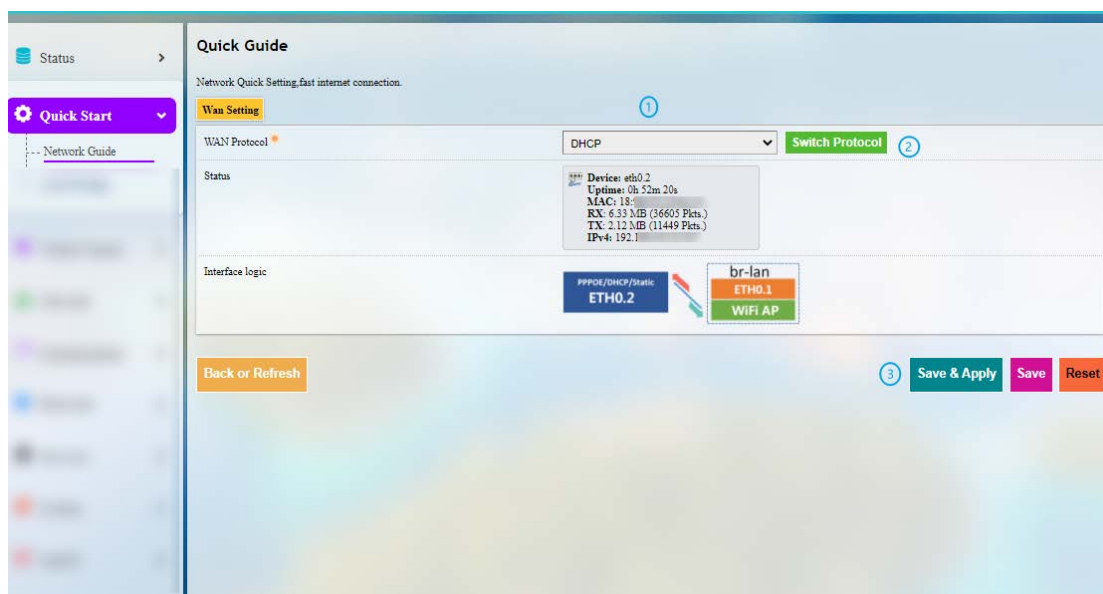
This page provides a quick guide to such functions as rapid networking of the Gateway and a display of the network port status and interface logic diagram. Refer to [3.5.1 Interfaces](#) for advanced settings.

▶ Application of the network setup wizard will clear customer-defined configuration parameters.

▶ Please refer to [1.4 Definition of Interfaces](#) for the definition of the ports.

3.3.2 WAN Setting – DHCP

DHCP: ETH0.1 and **WiFi AP** are bounded with the network bridge (br-lan). **ETH0.2** is designed as the WAN port to connect the higher-level network. The cellular interface does not work under this mode.



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: ETH0.1 and ETH0.2 are bounded with the network bridge (br-lan). **WiFi Client** is designed as the WAN port.

The screenshot displays the 'WAN Setting' configuration page for a 'Client' protocol. The page is titled 'Quick Guide' and includes a 'Network Quick Setting, fast internet connection.' header. The configuration fields are as follows:

- WAN Protocol:** Client (Step 1)
- Status:** Interface not present or not connected yet.
- Interface logic:** WiFi Client (Step 2)
- Select SSID:** -- Please choose -- (Step 3)
- Scan WIFI:** (Step 4)
- Mac Bssid:** Auto (Step 5)
- Key:** (Step 6)
- Internet connection?:** Yes (Step 7)
- Protocol:** DHCP (Step 8)

At the bottom, there is a 'Back or Refresh' button and a 'Save & Apply' button (Step 9). A note at the bottom states: 'Default DHCP, if the WIFI access point needs to specify IP, please select Static'.

Client (Wi-Fi) 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: ETH0.1, ETH0.2 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.

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;

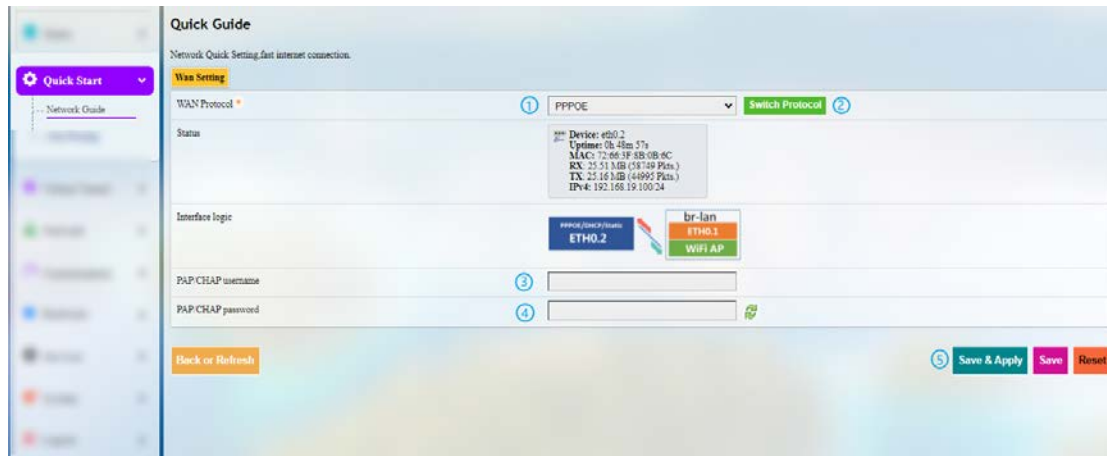
Step 6: Enter the password provided by the carrier for PAP/CHAP authentication;

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

-  Leave the field as is if not applicable.
-  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: ETH0.1 and WiFi AP are bounded with the network bridge (br-lan). **ETH0.2** is designed as the WAN port to connect the higher-level network.



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: **ETH0.1** and **WiFi AP** are bounded with the network bridge (br-lan). **ETH0.2** is designed as the WAN port to connect the higher-level network.

The screenshot displays the 'WAN Setting' page for a static IP configuration. The interface includes a sidebar with 'Quick Start' and 'Network Guide' options. The main content area is titled 'Quick Guide' and 'Network Quick Setting, fast internet connection.' The 'WAN Setting' section shows the 'WAN Protocol' set to 'Static' (Step 1). A 'Switch Protocol' button is available (Step 2). The 'Status' section displays device information for eth0.2. The 'Interface logic' section shows a diagram with 'br-lan' connected to 'ETH0.1' and 'WiFi AP', and 'ETH0.2' connected to the WAN. The 'IPv4 address' field is empty (Step 3). The 'IPv4 netmask' is set to '255.255.255.0' (Step 4). The 'IPv4 gateway' field is empty (Step 5). The 'IPv4 broadcast' field is empty (Step 6). The 'Use custom DNS servers' section shows '8.8.8.8' and '114.114.114.114' (Step 7). The 'Back or Refresh' button is at the bottom left, and 'Save & Apply', 'Save', and 'Reset' buttons are at the bottom right (Step 8).

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;

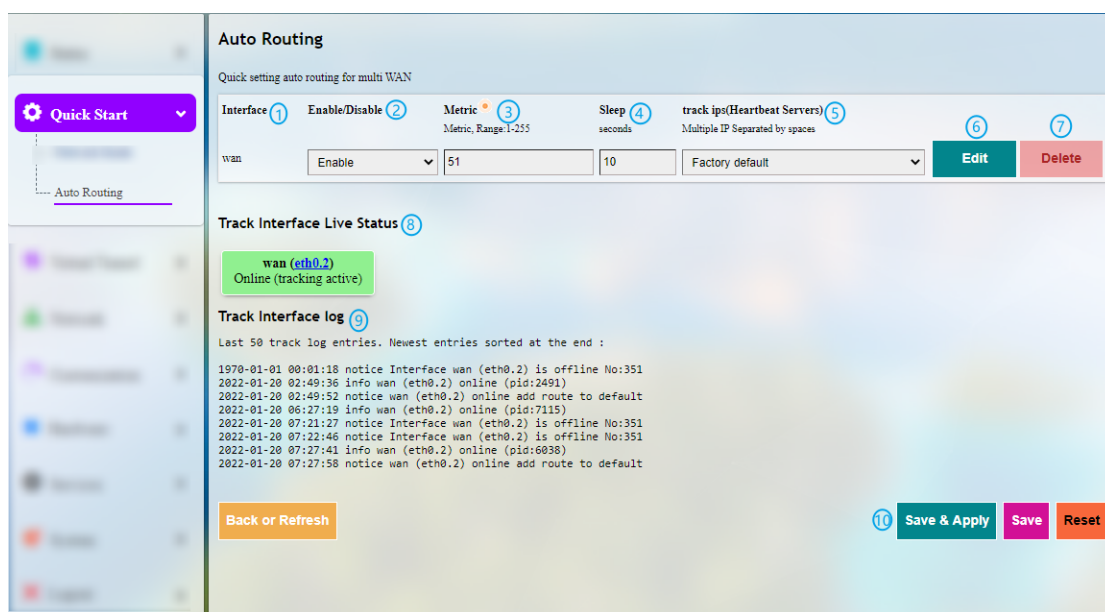
Step 8: Click **Save & Apply**.

 Leave the field as is if not applicable.


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.



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)
 Use spaces to separate multiple IP addresses. If you don't 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.

The screenshot shows the 'Advanced Setting' page for route tracking. The settings are as follows:

| Setting | Value | Unit/Options |
|--------------------------------|-----------------|--|
| Enable/Disable | Enable | Dropdown |
| Network | wan | Dropdown (Interface) |
| Metric | 51 | Metric, Range:1-255 |
| Count | 2 | times |
| Timeout | 8 | seconds |
| Online | 2 | times |
| Offline | 4 | times |
| Sleep | 10 | seconds |
| track ip(s)(Heartbeat Servers) | Factory default | Dropdown (Multiple IP Separated by spaces) |

Buttons at the bottom: Back or Refresh, Save & Apply, Save, Reset.

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.

Follow the steps below to build an OpenVPN Server:

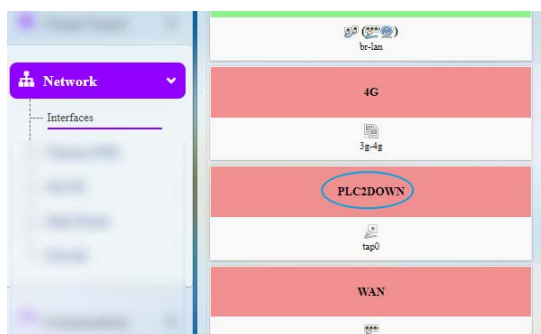
1. Synchronize the Gateway time with the browser (local) time;
2. Enable the server;
3. Select a protocol;
 - ▶ TCP provides an ordered delivery of data from user to server (and vice versa), whereas UDP is not dedicated to end-to-end communications, nor does it check the readiness of the receiver.
4. 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 network IP for the client;

8. Input the extension configuration for the client;
9. Download the configuration file for client connection (not necessary for server setup);
10. Save 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

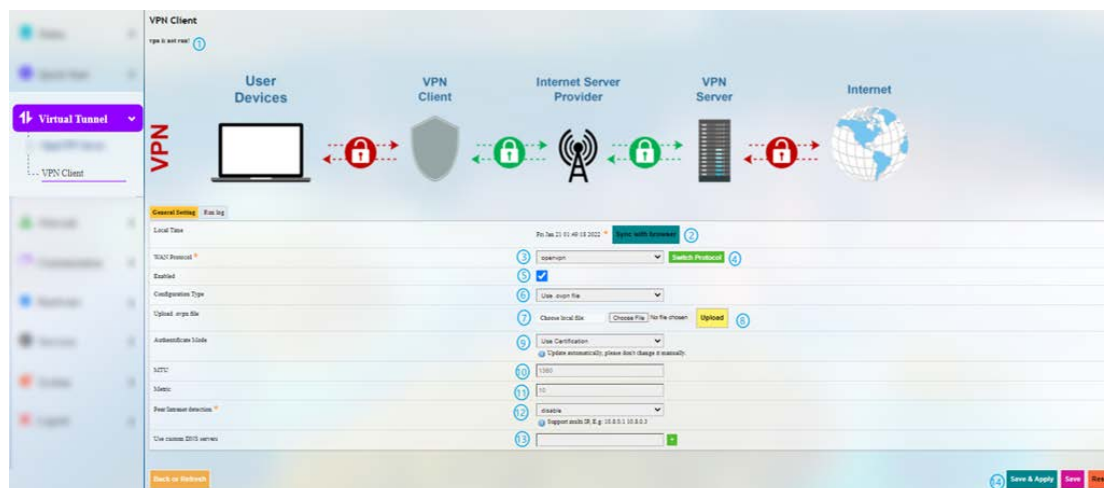
- ▶ Once the OpenVPN server is set up, an interface named PLC2DOWN will be added automatically so that users could make further changes.



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.



Description of the numbered areas

1. Status of the VPN


 If you haven't installed a VPN, there will not be any detailed information.

2. Synchronize your VPN time with the browser (local) time


3. Select a WAN protocol for the virtual line

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

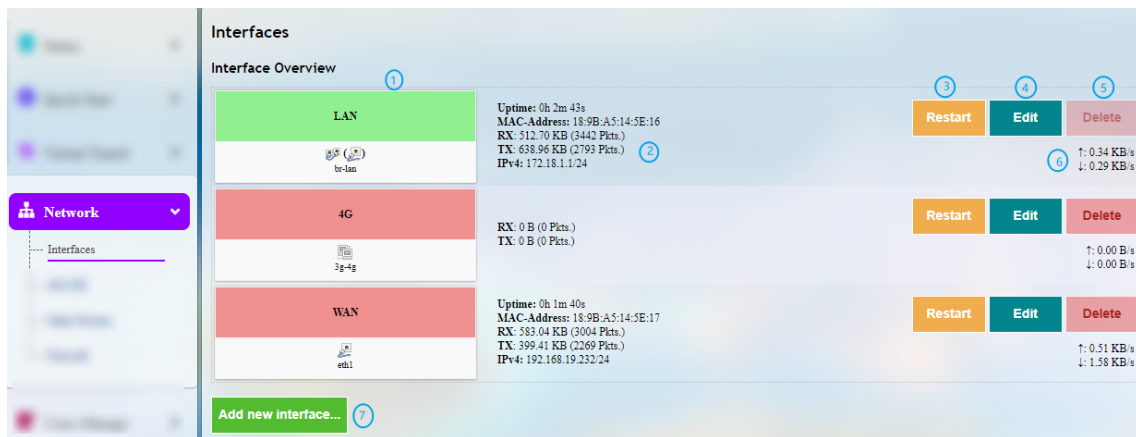
3.5 Network

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.

 The settings will be overridden if you make changes in the **Network Guide** page under **Quick Start** tab later.


3.5.1 Interfaces

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



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 devices do/do not have the module that makes 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.

The screenshot shows the 'Interfaces - LAN' configuration page. At the top, there is a description of the page and a note about VLAN notation. Below this is the 'Common Configuration' section with two tabs: 'General Setup' (selected) and 'Advanced Settings'. The 'General Setup' tab contains several fields: 'Status' (with a tooltip showing device details like 'Device: br-lan', 'Uptime: 24h 4m 10s', 'MAC: 7d...', 'RX: 164.29 MB (862113 Pkts.)', 'TX: 1.08 GB (1086694 Pkts.)', and 'IPv4: 172.18.1.1'), 'Protocol' (set to 'Static address'), 'IPv4 address' (set to '172.18.1.1'), and 'IPv4 netmask' (set to '255.255.255.0'). Numbered callouts 1, 2, and 3 point to the Status field, the IPv4 address field, and the IPv4 netmask field respectively.

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**:

The screenshot shows the 'Interfaces - LAN' configuration page, specifically the 'Advanced Settings' tab. It contains three fields: 'Override MAC address' (set to '7d:d1:b8'), 'Override MTU' (set to '1500'), and 'Use gateway metric' (set to 'Same as 'Auto Routing''). Numbered callouts 1, 2, and 3 point to the Override MAC address field, the Override MTU field, and the Use gateway metric field respectively.

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

General Setup | Advanced Settings | **Physical Settings**

Bridge interfaces 1 ☒ creates a bridge over specified interface(s)

Enable STP 2 ☐ Enables the Spanning Tree Protocol on this bridge

Interface 3

- ☐ 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

General Setup | Advanced Settings


Ignore interface 1 ☐ Disable DHCP for this interface.

Start 2 Lowest leased address as offset from the network address.

Limit 3 Maximum number of leased addresses.

Lease time 4 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

General Setup **Advanced Settings**

Dynamic DHCP ① ☒ Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

Force ② ☐ Force DHCP on this network even if another server is detected.

IPv4-Netmask ③ Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options ④ 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'll 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: eth0.2 Uptime: 22h 5m 9s MAC: 8E:D9:97:00:00:02 RX: 929.56 MB (1193522 Pkts.) TX: 135.71 MB (645207 Pkts.) IPv4: 192.168.1.2 |
| Protocol | 2 | DHCP client |
| Hostname to send when requesting DHCP | 3 | VantronOS-B4A7 |

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 | <input checked="" type="checkbox"/> If unchecked, no default route is configured |
| Use DNS servers advertised by peer | 2 | <input checked="" type="checkbox"/> If unchecked, the advertised DNS server addresses are ignored |
| Use gateway metric | 3 | Same as 'Auto Routing' |
| Override MAC address | 4 | 8E:D9:97:00:00:02 |
| 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

General Setup

Status

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

Protocol: Static address

Really switch protocol?

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 applicable.
- ▶ 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.

Wi-Fi – AP Mode (General settings)

The screenshot displays the 'Wireless(WiFi)' settings page. The 'General Setting' tab is active. The 'WIFI mode' is set to 'AP'. The 'SSID' is 'Vantron-2B8892'. The 'Channel' is '1(2412MHz)'. The 'Encryption' is 'WPA-PSK/WPA2-PSK Mixed Mode'. The 'Cipher' is 'Force CCMP (AES)'. The 'Key' is masked with dots. The 'Associated Stations' table shows one station with MAC address 'D6-A2-A0-...' and signal strength '-37 / -95 dBm'. The interface includes a 'Switch Mode' button and 'Save & Apply', 'Save', and 'Reset' buttons at the bottom.

| Network | MAC-Address | Host | Signal / Noise | RX Rate / TX Rate |
|---------------------------|--------------|-------|----------------|--|
| (Master "Vantron-2B8892") | D6-A2-A0-... | 172.1 | -37 / -95 dBm | 65.0 kbps, 0.0 Hz 65.0 kbps, 0.0 Hz |

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)

Wireless(WiFi)

WiFi Settings

General Setting **Advanced Setting**

Enable/Disable WIFI ① **Disable WIFI**

WIFI Frequency ② 2.4G **Switch Frequency** ③

Band ④ HT40
Note: select HT option for 80211n mode.


Network ⑤ ☒ lan ☐ plc2down ☐ vpn ☐ wan
Choose the network(s) you want to attach to this wireless interface

Associated Stations

| Network | MAC-Address | Host | Signal / Noise | RX Rate / TX Rate |
|---------------------------|-------------------|--------------|----------------|--|
| (Gaster "Vantron-237CA6") | 76:4B:3F:E6:BC:39 | 172.18.1.189 | -69 / -95 dBm | 13.0 Mbit/s, 0MHz 13.0 Mbit/s, 0MHz |

Description of the numbered areas

1. Turn on/off Wi-Fi
2. Set Wi-Fi frequency (determined by hardware)
3. Click to switch the frequency
4. Select the frequency band
5. The network interface to which Wi-Fi belongs

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

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 (as shown in the Interface page) when Wi-Fi client mode is enabled.

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.

3.5.3 4G/LTE

Before you configure for 4G/LTE, be sure to install the activated SIM card and the LTE 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 representative 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-mPCle**.
- provide AT&T with the pre-certified module name **VT-MOB-MPCIE-4G**.

The screenshot displays the '4G/LTE' configuration page. At the top, it shows 'SIM Card: READY', 'Sig: 94%', 'GET IP: 10.211.150.186', and 'IMEI: 86022...'. Below this are tabs for 'General Setting', 'Advanced Setting', 'Run log', and '4G traffic'. The 'General Setting' tab is active, showing a 'Status' section with a '6' icon, a 'Device' info box (3g-4g, Uptime: 1h 47m 10s, RX: 252.01 KB, TX: 201.70 KB, IPv4: 10.211.150.186/32), and a list of settings: 'Enable/Disable' (set to 'enable' with a '1' icon), 'Dial number' (set to '*99***1#' with a '2' icon), 'APN' (set to '3gnet' with a '3' icon), 'PAP/CHAP username' (set to 'your_username' with a '4' icon), and 'PAP/CHAP password' (masked with dots and a '5' icon). Below the settings is a 'General Information' table.

| 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...003 |
| 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 applicable.
- 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...

General Setting **Advanced Setting** Run log 4G traffic

SIM card switching ① 2
② When SIM dialing fails the preset number of times, switch to another SIM card

Restart Module ② **Re-power**

Auto Re-power Module ③ 5 min
④ Re-power the module, when the internet connection is offline more than preset time

PDP Type ④ ALL
⑤ PDP Type: ALL or IPV4_Only or IPV6_Only

CID Value ⑤ 1
⑥ CID, default: 1

Provider ⑥ AT&T/TMO/Canada

Override MTU ⑦ 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: | 8 003 |
| 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 | IPv4-Netmask | IPv4-Gateway | Metric | MTU | Route type |
|-----------|--------------------|------------------------|---------------|--------|------|------------|
| | Host-IP or Network | if target is a network | | | | |
| wan | 192.168.0.0/16 | 255.255.255.255 | 192.168.9.222 | 0 | 1500 | unicast |

Add **Save & Add** **Delete** **Reset**

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

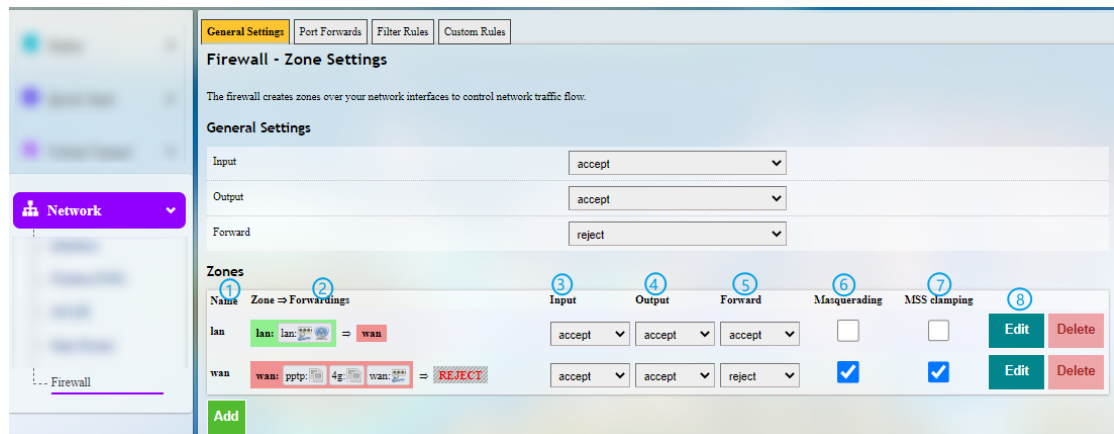
The following is a summary of the configuration items that the firewall can define. The minimum firewall configurations usually contain a basic setting item, at least two zones (LAN and WAN) and a forwarding to allow packets to be forwarded from LAN to WAN.

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.



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):

General Settings | **Port Forwards** | Filter Rules | Custom Rules

Firewall - Port Forwards

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

| 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 | <input checked="" type="checkbox"/> | Up | Down | Edit | Delete |

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 | Add |

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:

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.

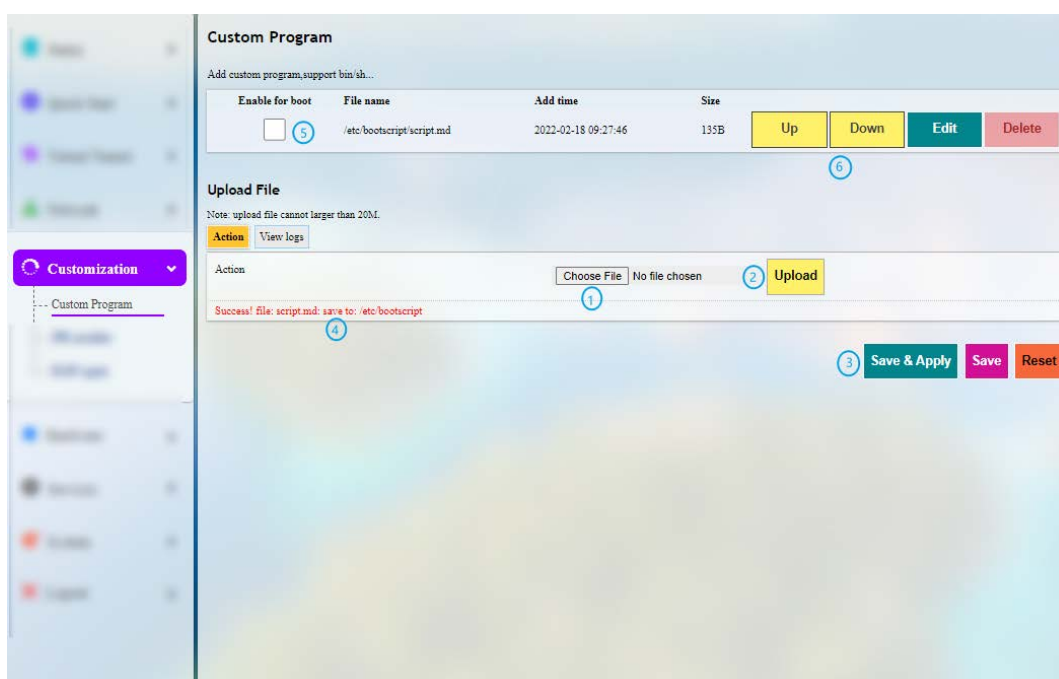
The **Edit** and **Delete** buttons behind a user allow you to enable/disable certain functions for this user or delete this user.

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.



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

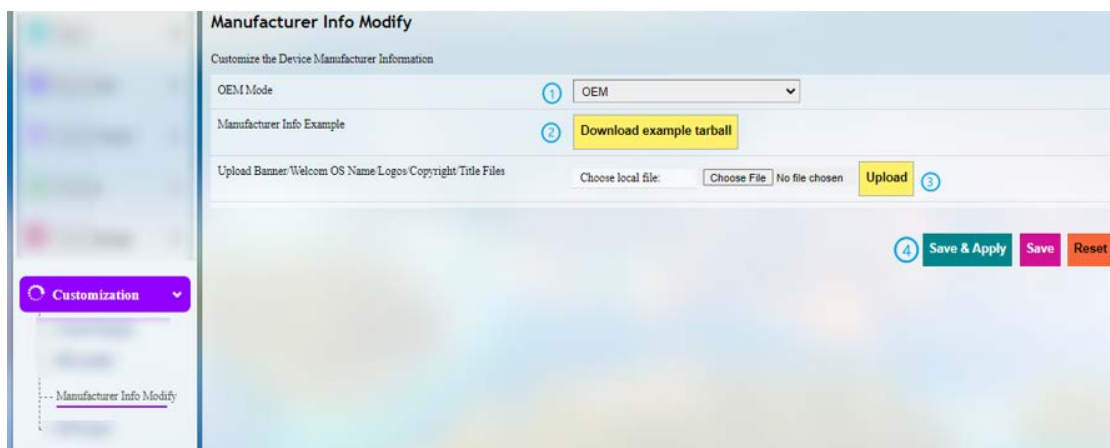
With IPK Installer, customers can install self-compiled IPK packages to the Gateway. Vantron industrial protocol packages are also uploaded from here. Refer to [4.2 Protocol Configuration and Application](#) for Industrial Protocols.

3.7.3 Manufacturer Info Customization

As modifications made to this function will change system information, it is required that users log in to the system with **root** account and password as indicated in [2.2 Gateway Login](#).

- Account: **root**
- Password: **rootpassword**

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



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:

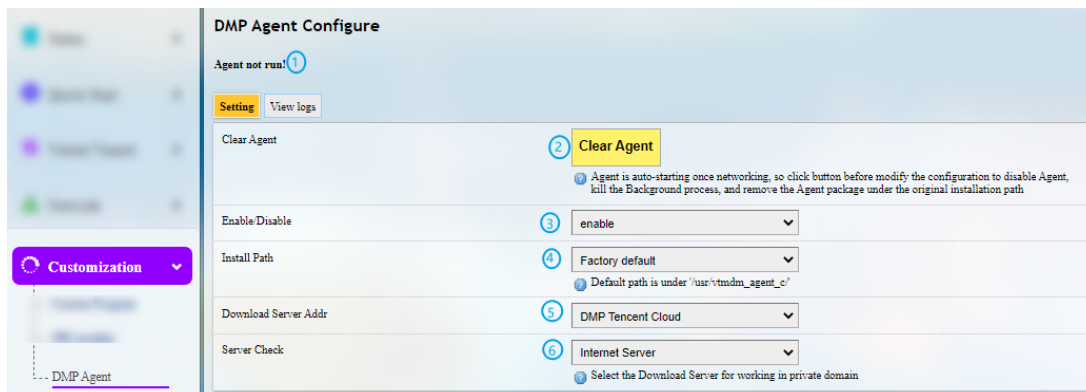
Vantron: All the information included in the files will be about Vantron.

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.



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 Interfacing with 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
 - ▶ The Agent is installed in “/usr” by default. In case there is not enough space, it is recommended that the directory is mounted to /mnt/sda1, the mounting directory of the Micro SD card. Therefore, remember to format the SD card to ext4 file system and install the SD card before configuration.
5. Set up the download address of the Agent server
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.

3.8 Hardware

3.8.1 Ser2TCP

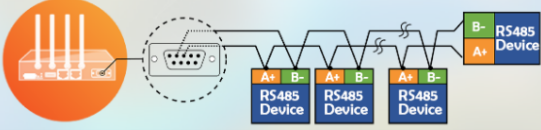
Serial to TCP provides an easy way to convert local serial data into Ethernet data and enables two-way communication with remote devices. Each conversion rule can be independently configured to server-side or client-side mode. You can also add, edit or delete a conversion rule on this page.

Ser2TCP
A tool that converts serial to TCP

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

Add

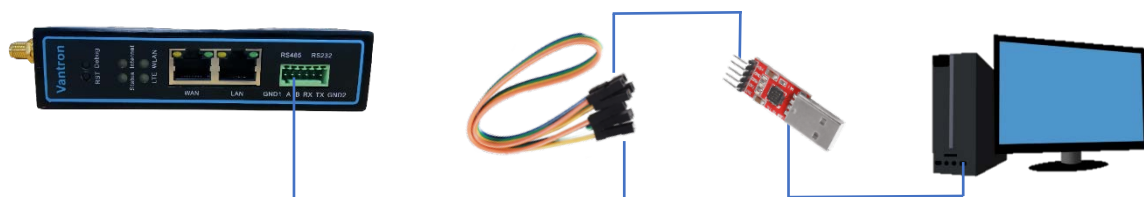
Serial list and details



| Serial dev | Baud Rate | Status | Called by PID | Program name |
|--------------|-----------|--------|---------------|----------------|
| /dev/ttyS0 | 57600 | using | 562 | /sbin/askfirst |
| /dev/ttyS1 | 9600 | idle | null | null |
| /dev/ttyS2 | null | idle | null | null |
| /dev/ttyUSB0 | 9600 | idle | null | null |
| /dev/ttyUSB1 | 9600 | idle | null | null |
| /dev/ttyUSB2 | 9600 | idle | null | null |

3.8.2 Ser2net environment setup and verification

- Prerequisites
 - A G202 gateway
 - An Ubuntu host
 - A USB to TTL serial adapter
 - A DuPont cable
 - Connect the serial port (e.g., RS232/RS485 COM2) of the gateway to the host



- Client mode

(1) Settings on VantronOS web interface

Ser2TCP
A tool that converts serial to TCP

| Device | Enable/Disable | Baud Rate <small>The speed the device port should operate at.</small> | | |
|---------------|----------------|--|------|--------|
| /dev/tty/Demo | Disable | 115200 | Edit | Delete |
| /dev/tty/USB0 | Disable | 115200 | Edit | Delete |
| /dev/tty/USB1 | Disable | 9600 | Edit | Delete |
| | Enable | 115200 | Edit | Delete |

Add

Serial list and details

| Serial dev | Baud Rate | Status | Called by PID | Program name |
|--------------|-----------|--------|---------------|----------------|
| /dev/ttyS0 | 115200 | using | 562 | /sbin/askfirst |
| /dev/ttyS1 | 9600 | using | 26415 | null |
| /dev/ttyS2 | null | idle | null | null |
| /dev/ttyUSB0 | 9600 | using | 26415 | null |
| /dev/ttyUSB1 | 9600 | using | 26415 | null |
| /dev/ttyUSB2 | 9600 | using | 26415 | null |

Back or Refresh **Save & Apply** **Save** **Reset**

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 <small>Eg: 177.6.6.6:678</small> | 3 |
| Device | /dev/ttyS0 | 4 |
| Baud Rate | 115200 <small>The speed the device port should operate at.</small> | 5 |
| Timeout | 20 <small>Seconds</small> | 6 |
| Data Bits | 8 bits | 7 |
| Parity | None | 8 |
| Stop Bits | 1 | 9 |

[Back or Refresh](#) [Save & Apply](#) [Save](#) [Reset](#)

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)
1. Select the serial device from the drop-down (RS232/RS485 (COM2) for illustration, node name /dev/ttyS0 as described in [1.5](#))
2. Select 115200 as the baud rate (the default value will be the one selected when setting up the rule)
3. Set a timeout value
4. Select “8 bits” for the data bit
5. Select “None” for parity
6. 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/ttyS0 -b 115200 -a 8 -r none -s 1 -o 20
```

(3) Settings on the Ubuntu host

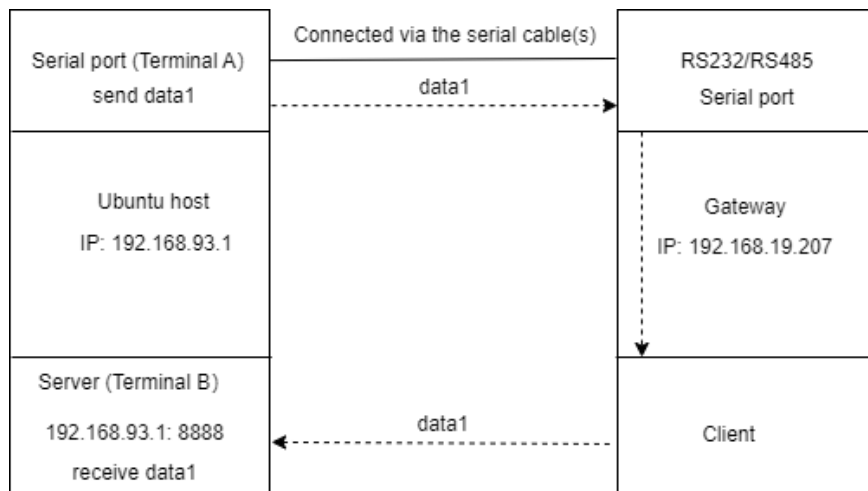
- Use microcom to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
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 <small>The speed the device port should operate at.</small> | | |
|---------------|----------------|--|------|--------|
| /dev/tty/Demo | Disable | 115200 | Edit | Delete |
| /dev/tty/USB0 | Disable | 115200 | Edit | Delete |
| /dev/tty/USB1 | Disable | 9600 | Edit | Delete |
| | Enable | 115200 | Edit | Delete |

Add

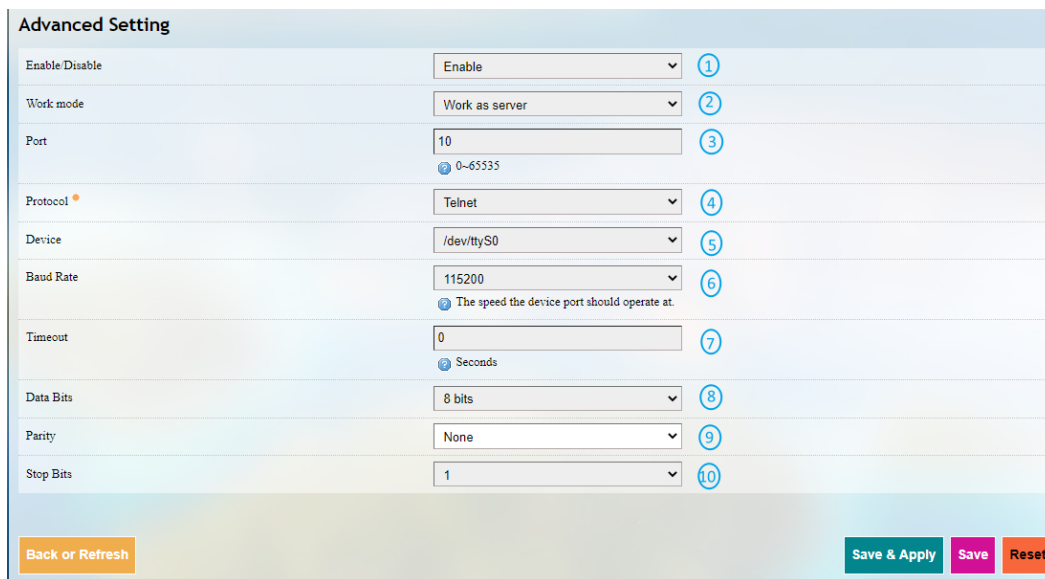
Serial list and details

| Serial dev | Baud Rate | Status | Called by PID | Program name |
|--------------|-----------|--------|---------------|----------------|
| /dev/ttyS0 | 115200 | using | 562 | /sbin/askfirst |
| /dev/ttyS1 | 9600 | using | 26415 | null |
| /dev/ttyS2 | null | idle | null | null |
| /dev/ttyUSB0 | 9600 | using | 26415 | null |
| /dev/ttyUSB1 | 9600 | using | 26415 | null |
| /dev/ttyUSB2 | 9600 | using | 26415 | null |

Back or Refresh **Save & Apply** **Save** **Reset**

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 ③ <small>0~65535</small> |
| Protocol | Telnet ④ |
| Device | /dev/ttyS0 ⑤ |
| Baud Rate | 115200 ⑥ <small>The speed the device port should operate at.</small> |
| Timeout | 0 ⑦ <small>Seconds</small> |
| Data Bits | 8 bits ⑧ |
| Parity | None ⑨ |
| Stop Bits | 1 ⑩ |

Back or Refresh Save & Apply Save Reset

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 [3.8.3](#) for the difference between the protocols)
5. Select the serial device from the drop-down (RS232/RS485 (COM2) for illustration, node name /dev/ttyS0 as described in [1.5](#))
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

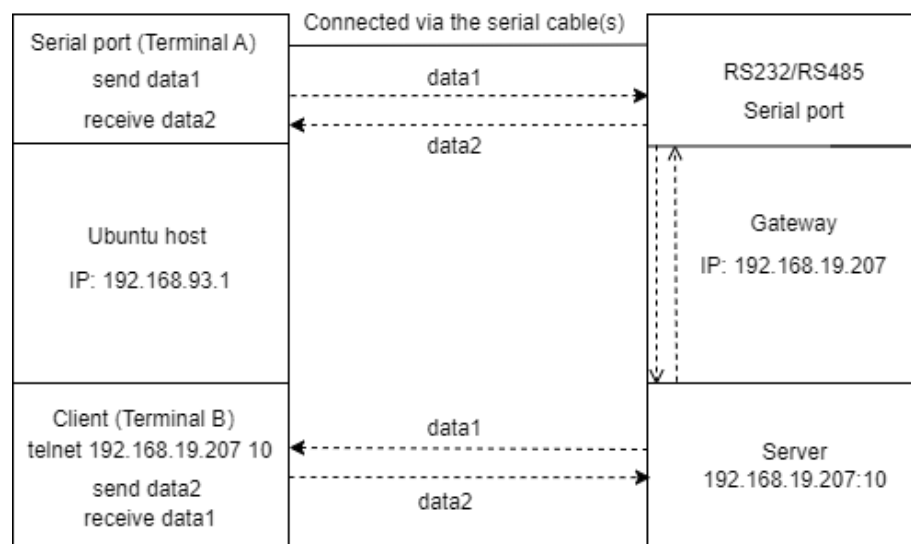
- Use microcom to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
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)



3.8.3 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 Dynamic DNS

Dynamic DNS is a technology in domain name system (DNS) that automatically updates the content of Name Server, often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information.

Input a name of the subdomain or root domain and click **Add** button, you will be directed to the setup page of the dynamic DNS. Then you can edit the service as needed.

3.9.2 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).

| 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 built by 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.

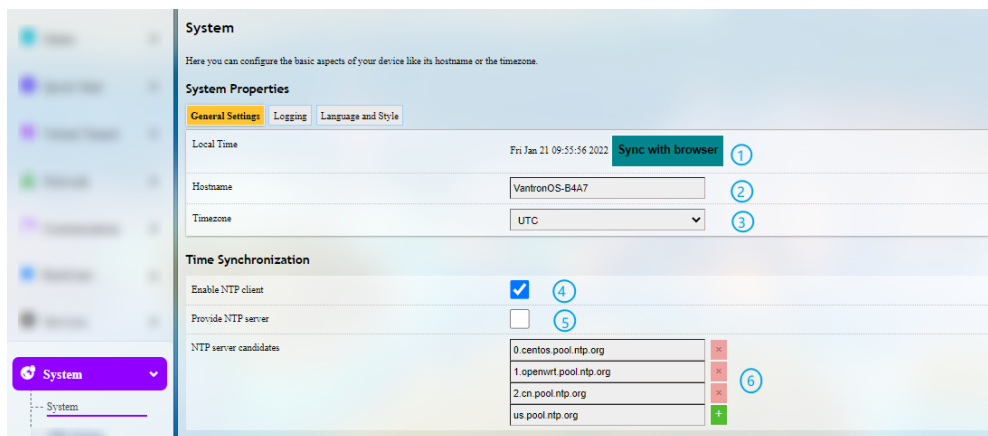
Before you can manage the PLC device remotely, please:

- 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

3.10 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



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.

3.10.2NBM Setting

General Settings

Netlink Bandwidth Monitor - Configuration

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

General Settings | Advanced Settings | Protocol Mapping

Accounting period 1
 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 2
 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 February.

Local interfaces 3 ☒ lan ☐ ppp ☐ wan
 Only comtrack streams from or to any of these networks are counted.

Local subnets 4

| | |
|----------------|---|
| 192.168.0.0/16 | x |
| 172.16.0.0/12 | x |
| 10.0.0.0/8 | + |

 Only comtrack 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 day in 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.

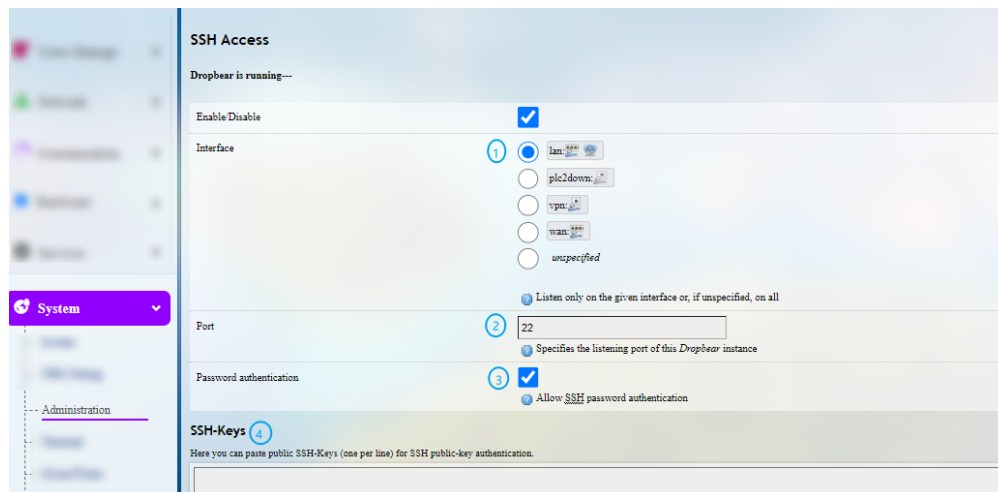
Step 1: Log out the interface by clicking **Logout** at the bottom left corner;

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


Account: root

Password: rootpassword

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



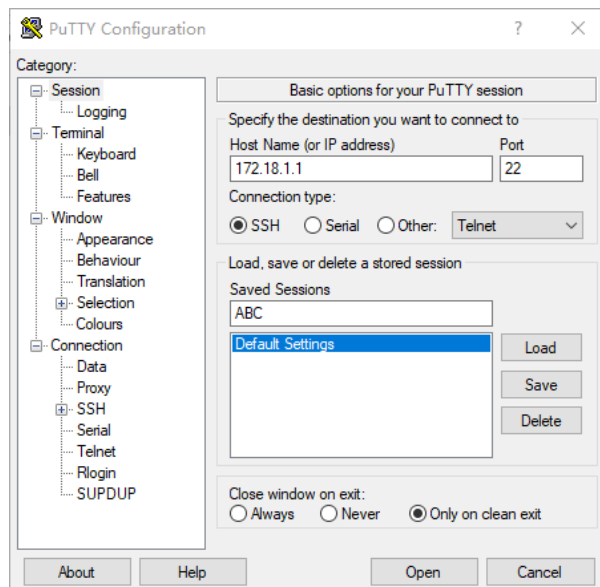
Description of the numbered areas

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

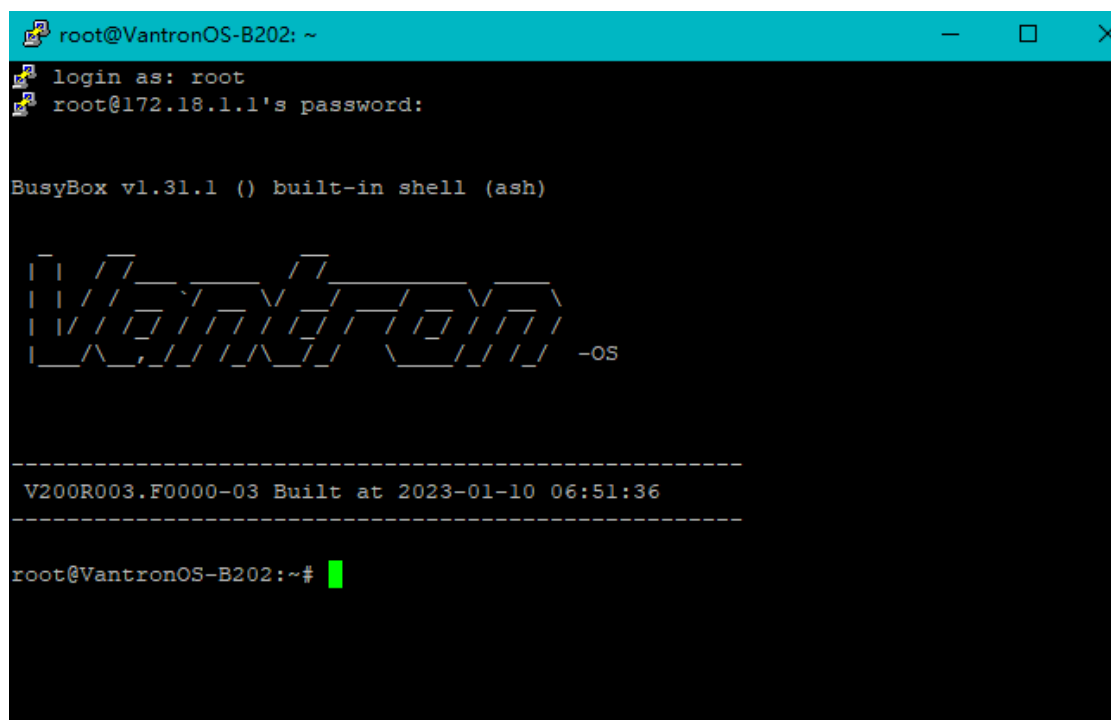
Step 4: Open an SSH client (PuTTY or MobaXterm recommended) in the Windows host;

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**;

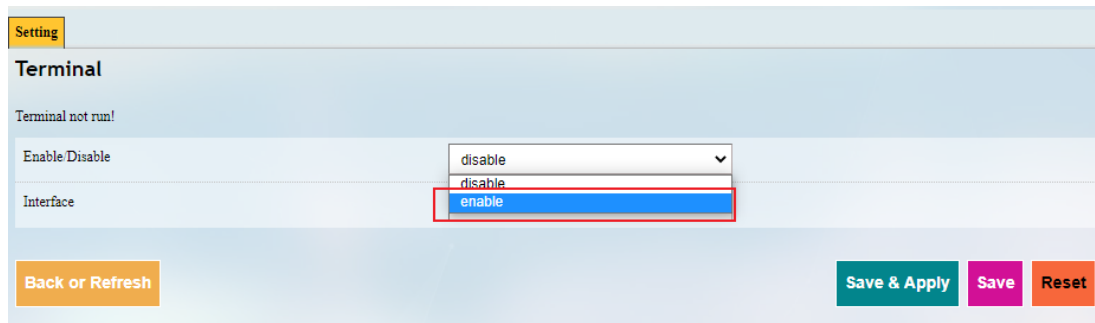


Step 7: Log in to the root account (password same as the gateway login password as shown above), and start an SSH remote session.



3.10.4 Terminal

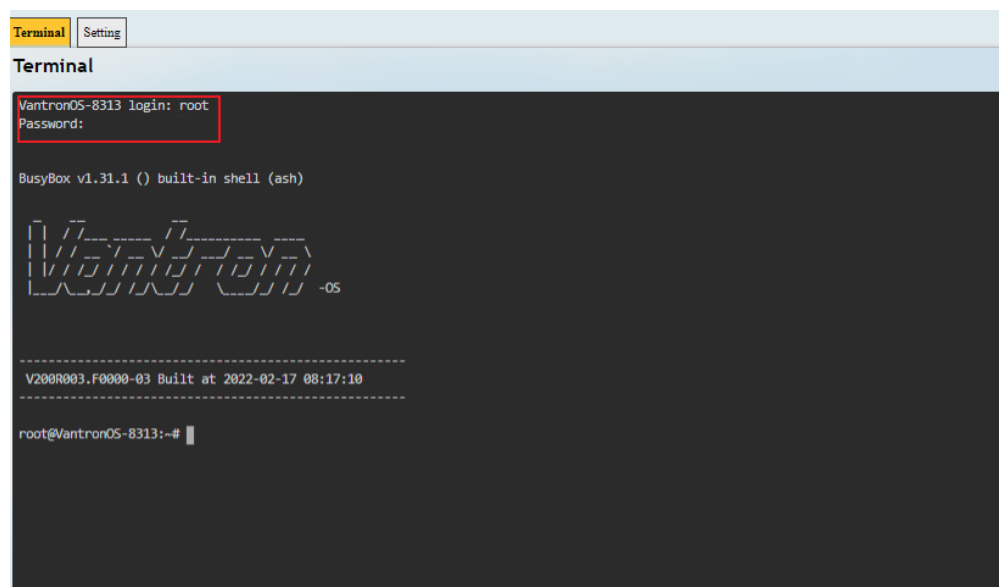
Under the **Setting** tab, users can click **enable** from the drop-down box and **Save & Apply** to enable the web terminal and input command lines here.



After the web Terminal is enabled, the **Terminal** tab will be available next to the **Setting** tab.

Login name: root

Login password: rootpassword (invisible while typing)



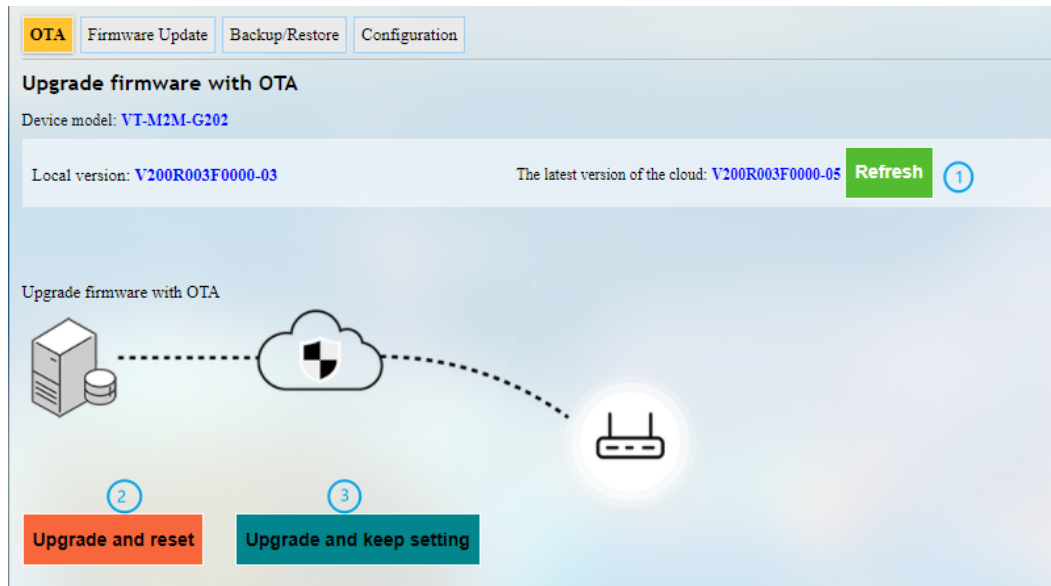
3.10.5 Mount Points

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



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

OTA **Firmware Update** Backup/Restore Configuration

Flash new firmware image

Upload a sysupgrade image here to replace the running firmware form local.(Device model: VT-M2M-G202)

Keep settings: ☒ 1

Image: 2 Choose File XOS_sd2m...0000-03.zip 3 Upload image...

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.

OTA **Firmware Update** Backup/Restore Configuration

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.

Cancel Proceed

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 do not have any ongoing process before rebooting the Gateway.

3.11 Logout

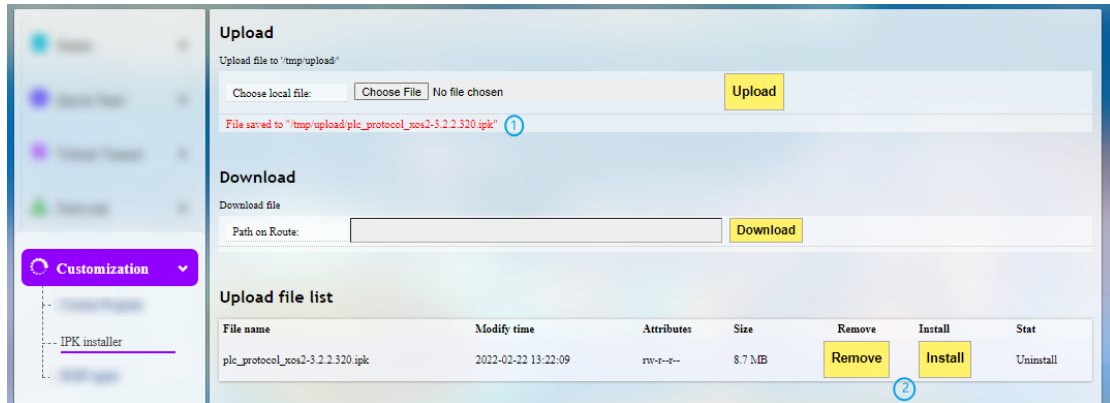
You will exit the web interface with a click on the **Logout** tab. If you need re-log the web, use the default password: **admin**. Make sure you have saved the changes before logout.

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.



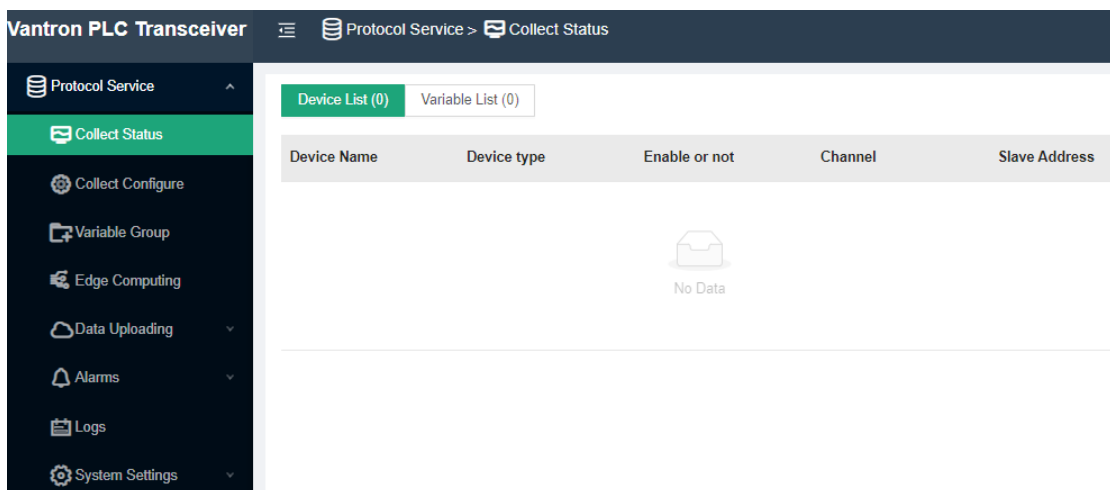
Description of the numbered areas

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

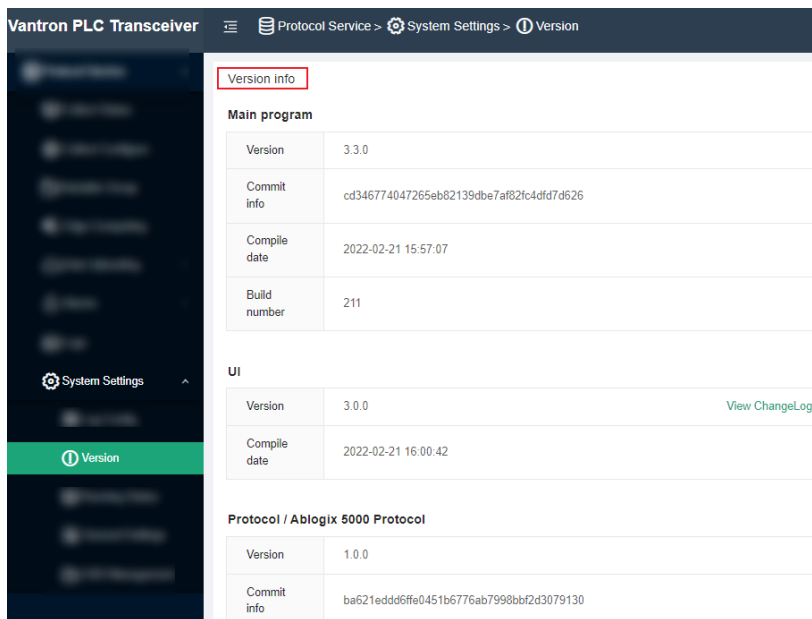
Once the .ipk file is installed, a message will be displayed suggesting the status of the file installation as shown below.



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.



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

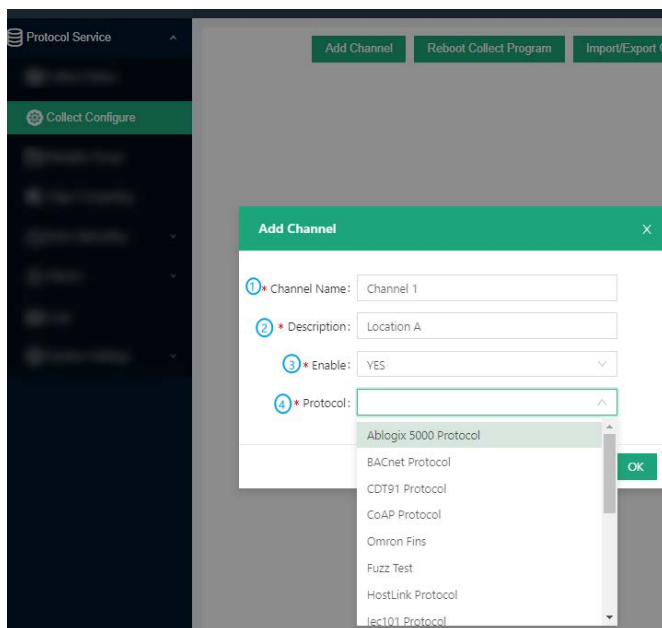


4.2 Protocol Configuration and Application

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.



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)

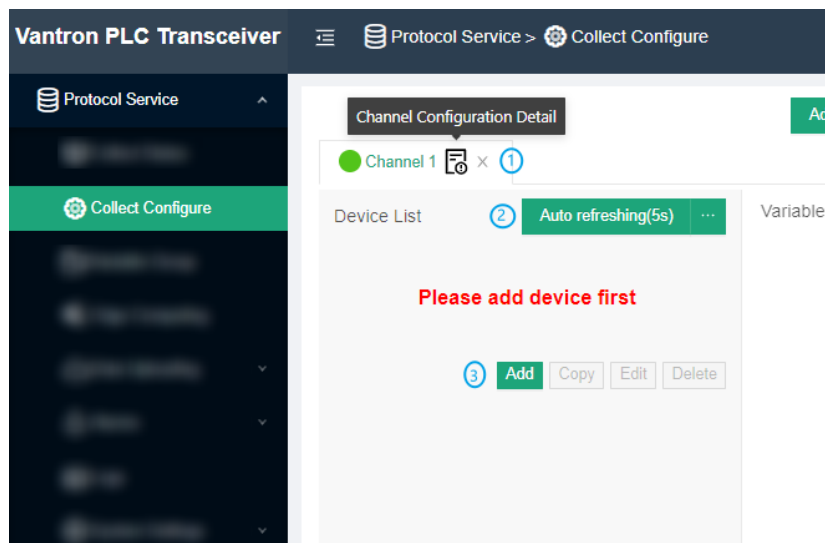
For certain protocol, more configuration parameters are required. Taking Modbus RTU protocol as an example, further information is needed.

The screenshot shows a dialog box titled "Add Channel" with a close button (X) in the top right corner. The dialog contains 13 numbered fields, each with a red asterisk indicating it is required. The fields are: 1. Channel Name: (text input, value: Channel 1), 2. Description: (text input, value: location A), 3. Enable: (dropdown menu, value: YES), 4. Protocol: (dropdown menu, value: Modbus Protocol), 5. Communication: (dropdown menu, value: modbus serial), 6. Protocol Mode: (dropdown menu, value: Modbus RTU), 7. Serial Port: (dropdown menu, value: COM3), 8. Serial Mode: (dropdown menu, value: RS232), 9. Baudrate: (dropdown menu, value: 115200), 10. Data Bits: (dropdown menu, value: 8), 11. Parity: (dropdown menu, value: N), 12. Stop Bits: (dropdown menu, value: 1), and 13. RTS: (dropdown menu, value: NONE). At the bottom right, there are "Cancel" and "OK" buttons.

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.



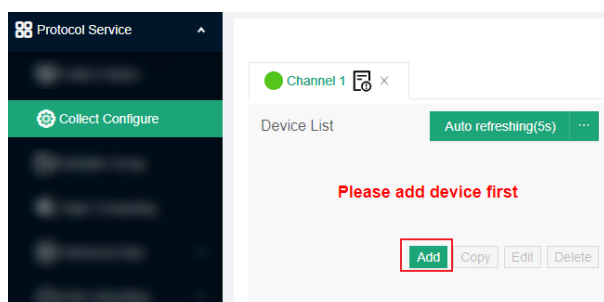
Description of the numbered areas

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 [X]

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

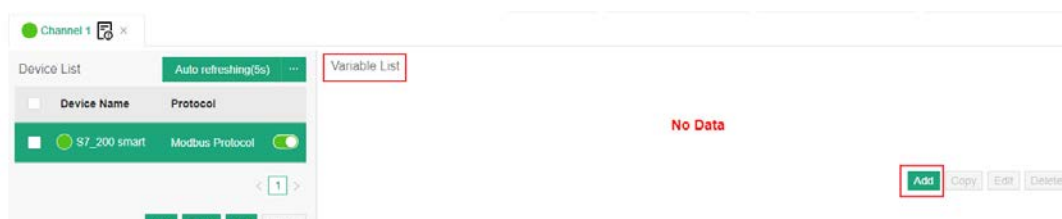
Cancel OK

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.



Add variable to device S7_200 smart

X

1

* Name:

Switch_on

2

* Title:

Tag_1

3

* Permission:

Read Only

▼

4

* Function Code:

01

▼

5

* Data Type:

BOOL(bit)

▼

6

* Register Addr:

32

7

* Data calculation:

none

▼

8

9

Import from CSV file

Download Template

Cancel

OK

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 above steps and upload a csv file for the setup of variables in bulk
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)

Import from CSV file

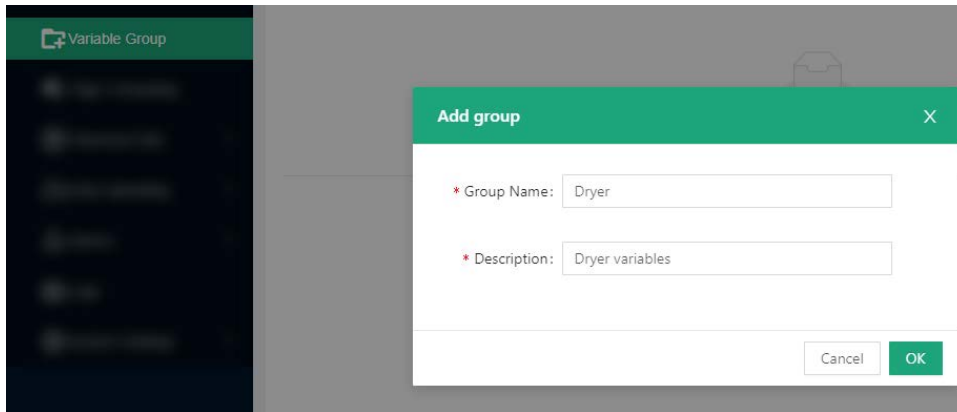
Export variables

Cancel

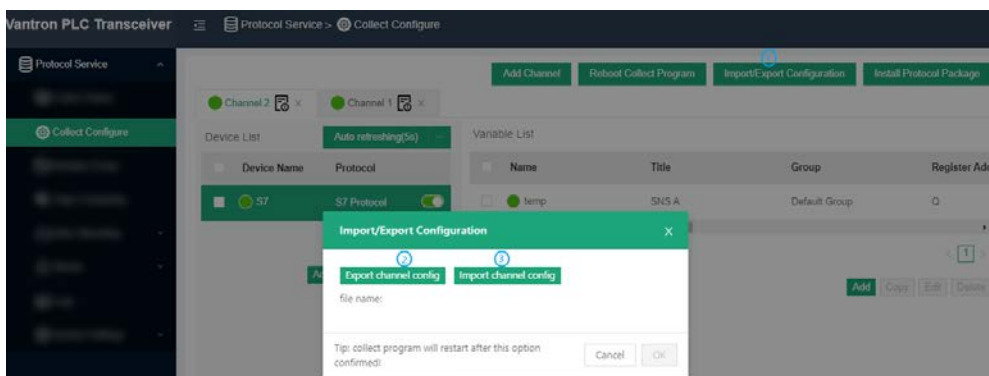
OK

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

If multiple variables are created, you can add variable groups for different variables from the **Variable Group** tab.



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



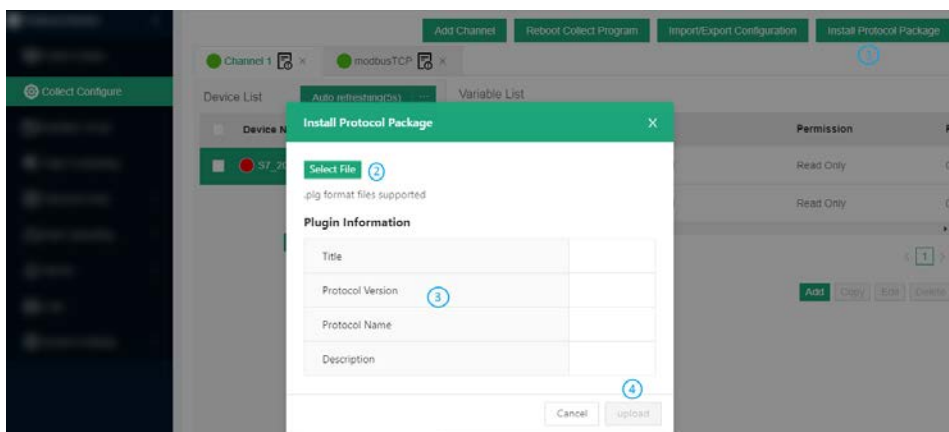
Description of the numbered areas

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.



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, you need click **Edge Computing** from the navigation pane on the left, then click **Add Script** to input the script information in the pop-up.

Add Script

Edit input variables

| Variable Name | Execute Object |
|---------------|----------------|
| DBW03 | Switch_on |
| DBW04 | Switch_off |
| DBW05 | Switch_on |

+

Edit output variables

| Compute Result | Data Type |
|----------------|-----------|
| bool_gg_10 | Bool |
| bool_gg_11 | Bool |
| bool_gg_12 | Bool |

Output to point

Script Name: S7_200 smart

Engine: javascript

enabled

```
1 function toInt(v)
2 {
3   return !!v ? 1:0;
4 }
5 bool_gg_10 = !!(DBW03);
6 bool_gg_11 = !!(toInt(DBW03) ^ toInt(DBW04));
7 bool_gg_12 = !!(toInt(DBW04) ^ toInt(DBW05));
8
```

Cancel OK

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.

Scripts List

| | | | | | | Refresh | Add Script | Import/Export Scripts | Execute Strategy |
|--------------------------|----------------|---------------------|------------------|--------------------|---------------|-----------|------------|-----------------------|------------------|
| <input type="checkbox"/> | Script Name | Execute Object | Execute Strategy | Last Execute St... | Execute Count | Operation | | | |
| <input type="checkbox"/> | S7_200 smart | [DBW03,DBW04,DBW05] | Timed Execution | Failed | 1181 | Pause | Copy | Edit | Delete |
| <input type="checkbox"/> | S7_200 smart A | [DBW03,DBW04,DBW05] | Timed Execution | Failed | 1180 | Pause | Copy | Edit | Delete |
| <input type="checkbox"/> | 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)

Execute Strategy

| <input type="checkbox"/> | scriptName | Current Strategy | Execute Interval | Reuse Engine |
|-------------------------------------|------------------|------------------|------------------|---------------------------------|
| <input type="checkbox"/> | greetings | Timed Execution | 1000 | Reuse after 100 times execution |
| <input checked="" type="checkbox"/> | edge computing | Timed Execution | 1000 | Reuse after 100 times execution |
| <input checked="" type="checkbox"/> | edge computing_1 | Timed Execution | 1000 | Reuse after 100 times execution |
| <input checked="" type="checkbox"/> | edge computing_2 | Timed Execution | 1000 | Reuse after 100 times execution |

3 scripts selected

* Execute By: Timed Execution

* Execute Interval: Timed Execution ms

* Reuse Engine: Automatic Execution

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**.

The screenshot shows the 'Collect Status' interface. At the top, there are tabs for 'Device List (5)' (1) and 'Variable List (5)' (2). To the right, there is a filter dropdown 'All groups' (4), an 'Auto refresh(2s)' button (5), and a 'Refresh' button (6). Below these is a table with columns: 'Variable Name', 'Variable Value', 'Assigned De...', 'Channel' (3), 'Read&Write Acc...', 'Variable alias' (5), and 'R Option' (6). The table contains five rows of data. The last row has two icons in the 'R Option' column, labeled 7 and 8.

| 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**;

The screenshot shows a dialog box titled 'Add data upload service' with a close button (X). It contains three input fields: 'Channel Name' with the value 'channel 1', 'Protocol Type' with a dropdown menu showing 'MQTT Protocol', and 'Cloud Platform' with a dropdown menu showing 'MQTT Client'. At the bottom, there are 'Cancel' and 'OK' buttons.

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

The image shows a configuration window for an MQTT client. It contains several fields and a checkbox, each with a numbered callout (1-10) indicating its function. The fields are: 'Enable' (checkbox), 'Data encapsulation' (dropdown), 'Center platform' (dropdown), 'Address' (text), 'Port' (text), 'MQTT interval' (text), 'MQTT client ID' (text), 'QoS' (dropdown), 'Data publish topic' (text), and 'Subscribe topic' (text). The 'Enable' checkbox is checked. The 'Center platform' dropdown is set to 'MQTT Client'. The 'Address' field contains '192.168.16.229'. The 'Port' field contains '1883'. The 'MQTT interval' field contains '90'. The 'MQTT client ID' field contains '12345678'. The 'QoS' dropdown is set to '1'. The 'Data publish topic' field contains 'dryer'. The 'Subscribe topic' field is empty.

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-----
MIIDITCCAZOQCFGHUQmZNUwkW6k
n12KoU9dku0KEUOxo09KUPIOUKJH
uGYWSPijJHUhOBAP3jiPMDOowjud
oPWIFJOKOPN.JinahDHUEWHIELNI

17 Client Key File:

8aLWGDUb7REWLEMrZtYkocpgSfsc
seuh2uXpseeN0A47PuCwxNish1psnk
yooGxpO2rNLL0L0G9h6ad0wn3e201
22b0UMOGZFikitzY99+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:

22 Max memory size: M

23 Minimum post interval: s

24 Select devices: Channel 1 x

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.

| 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 (lux) | { "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 [X]

1 * Name: switch off

2 * Variable: Channel 1 / S7_200 smart / Switch_on

3 Information: false

4 Enable: ☒

* Alarm Trigger: < 0 5 6 > 1 Normal

Note: conditions match from top to bottom 7

8 Data Linkage: Channel 1 / S7_200 smart / Switch_on

9 [Cancel] [OK]

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.

The screenshot shows the 'Alarm Broadcast' configuration page. It contains four numbered fields: 1. 'Alarm interval' set to 120 seconds. 2. 'Max record size' set to 1024 M. 3. 'Enable result output' checked with a green checkmark. 4. 'Output method' set to '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.

This screenshot shows the continuation of the 'Alarm Broadcast' configuration page. It includes fields 4 through 10: 4. 'Output method' set to 'Email and record'. 5. 'Notify address' (empty). 6. 'Server address' (empty), with 'SSL' checkbox and 'Port' set to 25. 7. 'Encrypted transmission' checkbox, with a note 'If the server supports it, use encrypted transmission'. 8. 'Account' (empty). 9. 'Server validation' toggle set to 'ON'. 10. 'Password' (masked with dots) with a show/hide icon.

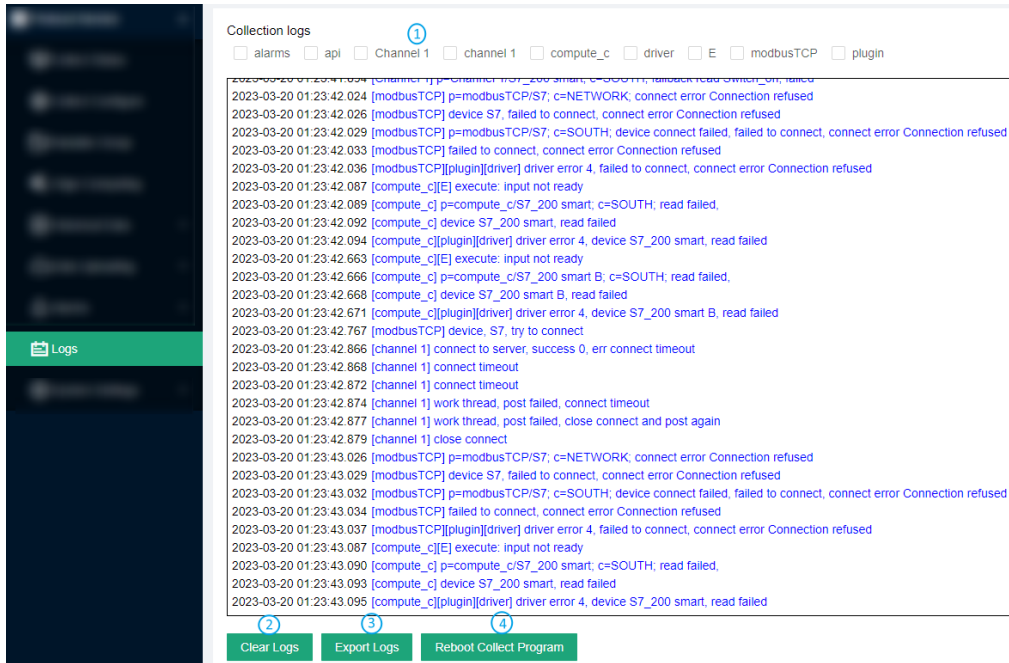
5. Input an email account for receiving the alarm messages
6. Input the outgoing server address (check the settings of the email server in use)
7. Enable encrypted transmission if the server supports
8. Input an email account for sending the alarm messages (could be same as the receiving email)
9. Toggle 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.



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

1 * Web log level: INFO

* File log level: WARNING

2 * Single file size: 1024 K

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

Cancel OK

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; and 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 A Regulatory Compliance Statement

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.

APPENDIX B Acronyms

| Acronym | Description |
|---------|---------------|
| RXD | Receive data |
| TXD | Transmit data |
| GND | Ground |
| NC | No connection |