G202 Industrial Edge Computing Gateway

User Manual

Version: 2.0

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 section 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
V1.6	V200R003	Added “+” and “-” description for the power terminal	May 5, 2023
V1.7	V200R003	1. Updated the description of the 4G indicator; 2. Updated RAM & storage capacity.	Jun. 30, 2025
V2.0	VantronOS25 - V200R003.F0000-03	1. Updated section 2.2 based on the current **VantronOS25** interactive interface; 2. Moved SSH login to section 2.3, and added section 2.4; 3. Updated Chapter 3 based on the new UI and updated features; 3. Added chapter 4 on the protocol portal configurations.	Sep. 8, 2025

Table of Contents

Foreword

Thank you for purchasing G202 Industrial Gateway ("the Product" or "the gateway"). 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
ℹ	Attention to important information or regulations

General Safety Instructions

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

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

Precautions for Power Cables and Accessories

⚠ Use proper power source only. Make sure the supply voltage falls within the specified range. 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:

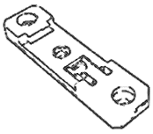
Intelligent manufacturing: injection molding machine, numerical control machine

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 12V DC Power adapter & power cord
	2 x Wi-Fi antenna		1 x DC power connector
	1 x DIN rail mounting bracket		2 x 4G LTE antenna

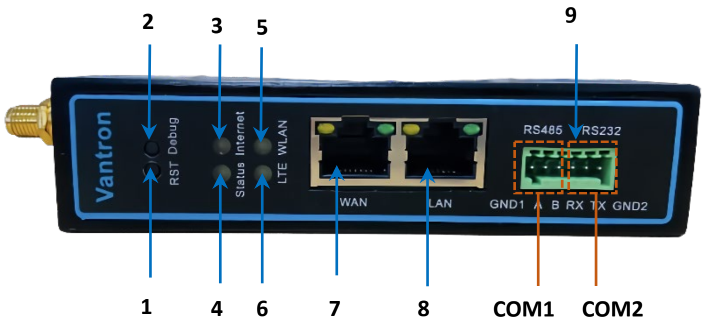
Actual accessories might vary slightly from the list above as the customer order might differ from the standard configuration options.

1.3 Specifications

G202			
System	Memory	256MB DDR2	
	Storage	64MB 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	
	Ethernet port protocol	PPP, PPPoE, DHCP, ARP	
I/Os	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 Gateway Manager	
	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℃ ~ +60℃ Storage: -40℃~+70℃	
	Humidity	RH 5%-95% (Non-condensing)	
	Certification	CE, FCC, PTCRB	

1.4 I/Os, LEDs, Buttons

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 turned on	The indicator is blinking at an interval of 0.5s
	The Cellular connectivity is established	The indicator is blinking at an interval of 1s
	The 4G LTE module is off/not implemented	The indicator is off

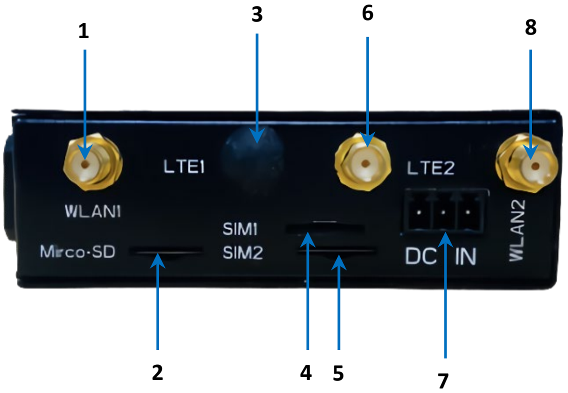
Ethernet ports description:

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

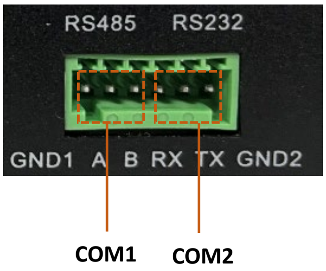


Interface	Description
1	WLAN antenna 1
2	Micro SD card slot
3	4G LTE antenna 1
4	Micro SIM card slot 1
5	Micro SIM card slot 2
6	4G LTE antenna 2
7	9-36V DC power terminal
8	WLAN antenna 2

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 (COM2) is configurable to RS485 or RS232 (configured before shipment).

The default parameters of COM1 and COM2 for serial communication are: 115200, 8N1.

COM2 is used for serial communication by default. To switch to the debug mode (default parameters: 57600 8N1), users can long press the debug button before power application and release util 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:

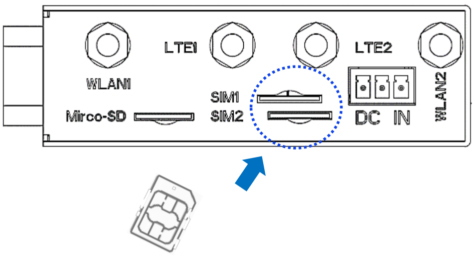
No. (Left to right)	Pin	Node name	Port	Type	Definition
1	GND1	/dev/ttyS1	COM1	P	RS485 Isolated grounding
2	A			I/O	RS485-A signal
3	B			I/O	RS485-B signal
4	RX/A	/dev/ttyS0	COM2	I	RS232 RXD signal/ RS485-A signal
5	TX/B			O	RS232 TXD signal/ RS485-B signal
6	GND2			P	Isolated grounding

CHAPTER 2 GETTING STARTED

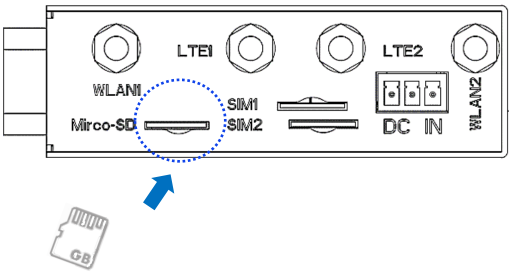
2.1 Setting up the Gateway

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

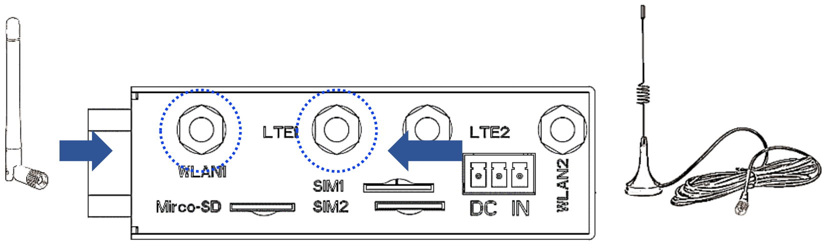
1. Use the mounting bracket and screws provided to install the gateway to a secure place;
2. Insert an activated SIM card into either SIM slot (dual SIM supported). For SIM1 slot, keep the gold contacts facing down; for SIM2 slot, keep the gold contacts facing up.



3. Push the SIM card until you feel it settle with a soft click.
4. Insert a Micro SD card into the Micro SD slot with the gold pins facing up.

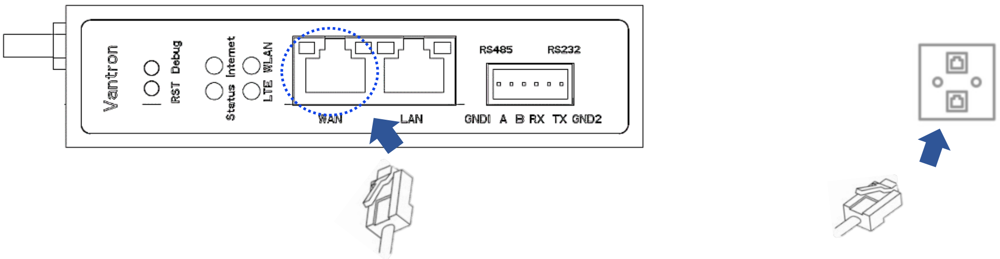


5. Install the rubber stick antennas to the WLAN ports and the sucker antennas to the LTE ports.

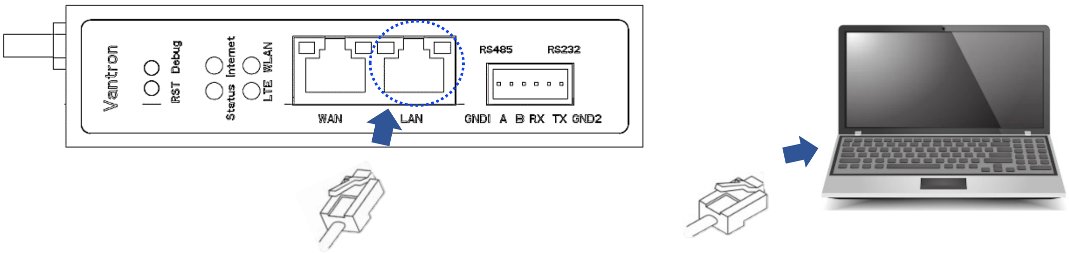


*If only one WLAN or cellular antenna is supplied, use **WLAN1** or **LTE1** for better signal strength.*

6. If wired backhaul is preferred, plug an Ethernet cable into the gateway's WAN port and the other end into an active wall outlet or switch.

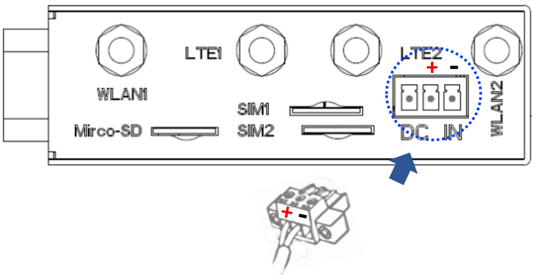


7. Similarly, to provide wired client access, connect a cable from the gateway's LAN port to your computer or other device.



Skip steps 6 & 7 if wireless network connection is preferred.

8. Connect the supplied DC power connector between the gateway's power terminal and a 9–36 V power adapter.



If you are using the DC power connector supplied by Vantron:

Red wire: +
Black wire: -

9. Plug the power adapter into a mains outlet to power up the gateway.

10. The power indicator will turn solid green upon power application.

2.2 Web Login

You can configure the network settings and manage the device on the web-based management portal (VantronOS) using a **Windows** host computer.

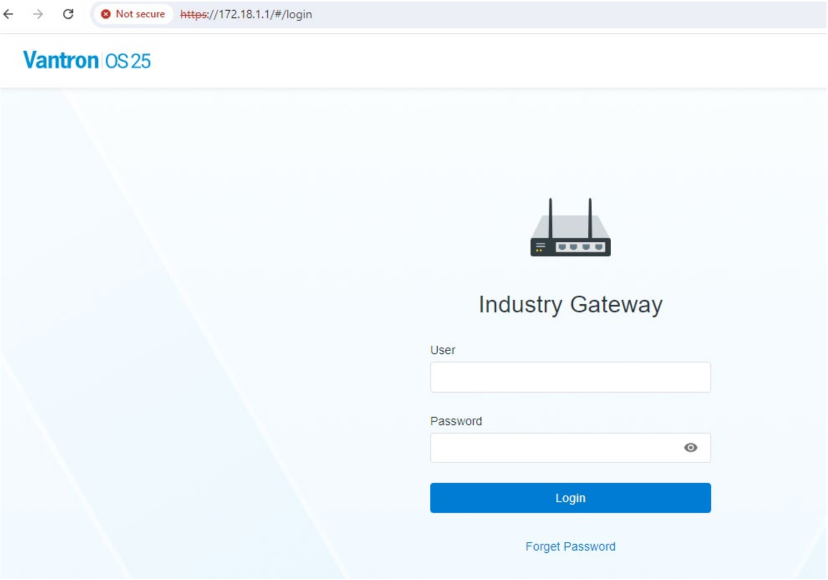
There are three login options to access VantronOS for G202, depending on how the host computer is connected to G202.

Method	Host Computer Connection	VantronOS Login Address
Option 1	Host connects to G202's Ethernet LAN port or to G202's 2.4GHz Wi-Fi.	Use G202's LAN IP (default IP address: 172.18.1.1)
Option 2	Host's WAN interface on the same IP subnet as G202's WAN interface (e.g., both connected to the same switch or upstream Wi-Fi).	Use G202's WAN IP

We recommend initially logging into VantronOS using Option 1. Afterwards, you may establish additional connections between G202 and your host computer, and switch to other login options as needed by referring to the device's IP addresses listed under the **Network** tab in VantronOS.

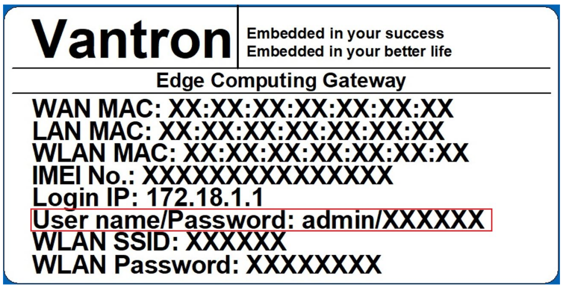
VantronOS login via Ethernet LAN connection:

1. Connect the host computer to the LAN port of G202 using an Ethernet cable.
2. Input the LAN port IP of the gateway in your browser (default: https://172.18.1.1/).



If the address is blocked, please click ***Advanced*** *to proceed.*

3. Log in to the VantronOS web portal using the provided login credentials on the device label.



Vantron | Embedded in your success
Embedded in your better life
Edge Computing Gateway
WAN MAC: XX:XX:XX:XX:XX:XX:XX
LAN MAC: XX:XX:XX:XX:XX:XX:XX
WLAN MAC: XX:XX:XX:XX:XX:XX:XX
IMEI No.: XXXXXXXXXXXXXXX
Login IP: 172.18.1.1
User name/Password: admin/XXXXXX
WLAN SSID: XXXXXX
WLAN Password: XXXXXXXX

For VantronOS login via Wi-Fi connection:

1. Connect the host computer to the gateway's Wi-Fi using the WLAN SSID and password provided on the product label.
2. Enter the gateway's WLAN IP (172.18.1.1 by default) in the browser to access the VantronOS login page.
3. Log in to the VantronOS web portal using the provided login credentials.

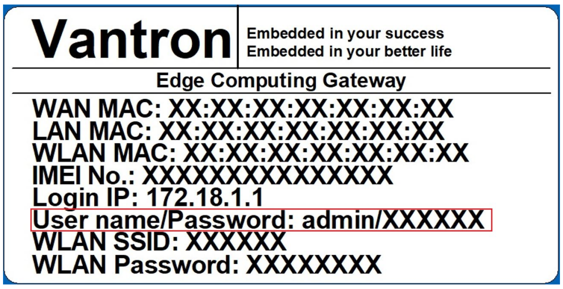
2.2.1 Password Reset

If you have reset the login password and later forget it:

1. Press the **Reset** button on the device and hold for 3-10 seconds to factory reset the device.

   Factory reset will restore all device settings—including the login password—to their defaults. You will need follow the setup wizard to complete the initial setup after a factory reset.

2. The factory reset takes about 1-10 minutes, please keep the device powered up during this process.
3. Use the provided login credentials on the device label for re-login.



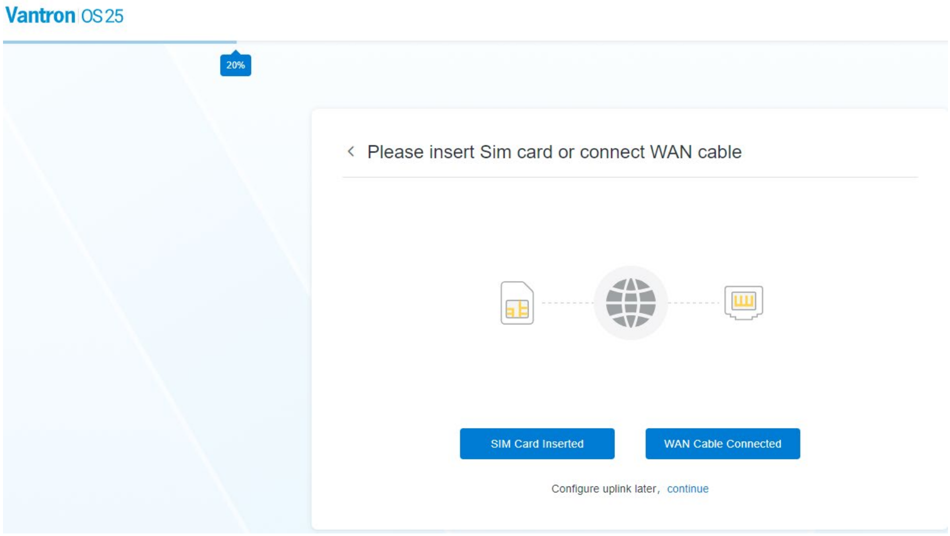
Vantron | Embedded in your success
Embedded in your better life
Edge Computing Gateway
WAN MAC: XX:XX:XX:XX:XX:XX:XX
LAN MAC: XX:XX:XX:XX:XX:XX:XX
WLAN MAC: XX:XX:XX:XX:XX:XX:XX
IMEI No.: XXXXXXXXXXXXXXX
Login IP: 172.18.1.1
User name/Password: admin/XXXXXX
WLAN SSID: XXXXXX
WLAN Password: XXXXXXXX

To reset the login password without factory resetting the device, refer to section 3.7.2 for the instructions.

2.2.2 Login Wizard

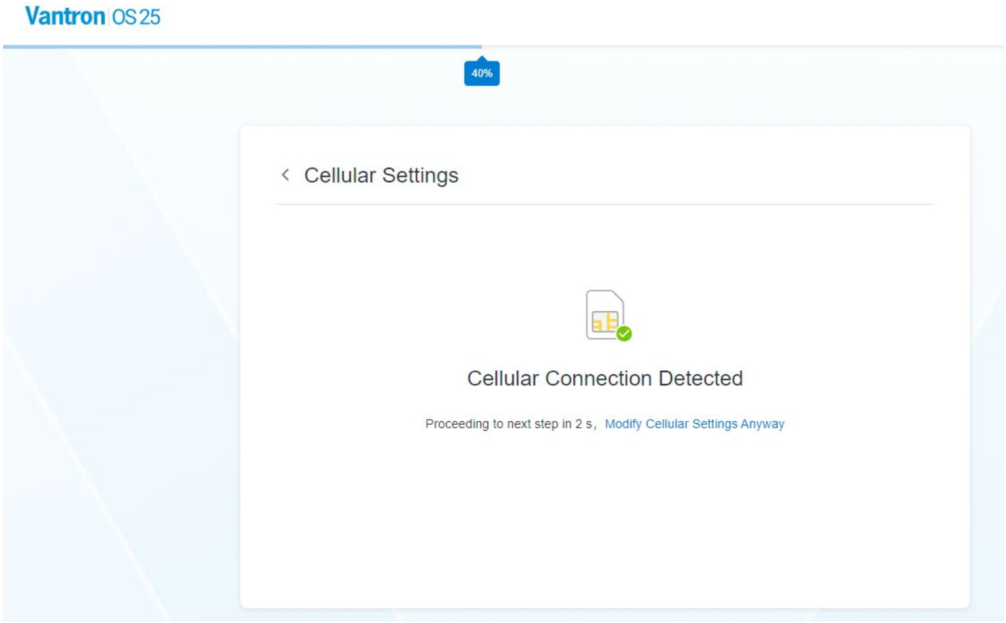
For first-time users, the setup wizard will guide you through the initial setup process, including modifying the login password.

If internet access is **not** required at the moment, click **continue** under the buttons to skip. Otherwise, connect the gateway to the internet either via either cellular data or Ethernet, and proceed.


Vantron OS25
20%
Please insert Sim card or connect WAN cable
SIM Card Inserted
WAN Cable Connected
Configure uplink later, continue

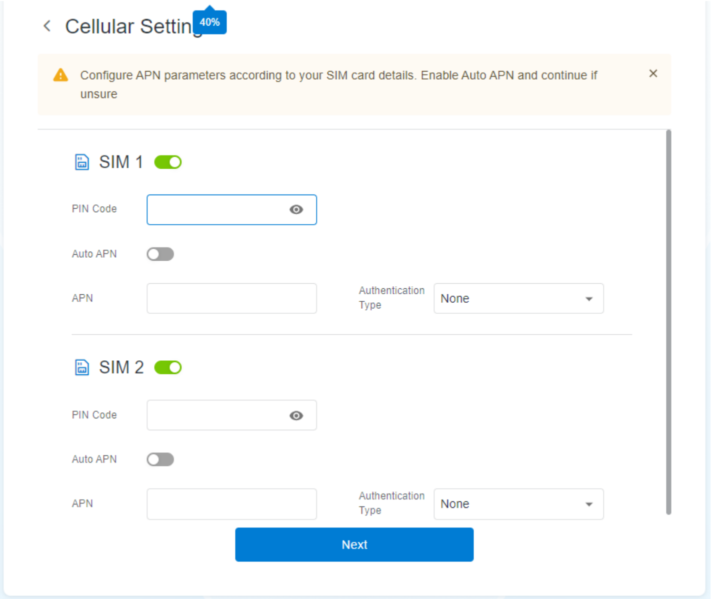
- **Cellular Settings (SIM Card Inserted)**

1. Once the system has detected the insertion of an activated SIM card, it will automatically proceed to the next setup in 5 seconds.


Vantron OS25
40%
Cellular Settings
Cellular Connection Detected
Proceeding to next step in 2 s, Modify Cellular Settings Anyway

2. If you prefer to manually configure the network, click **Modify Cellular Settings Anyway**.

3. Determine which SIM slot you are using and configure it accordingly on the login page. The device supports dual SIM configuration.



Cellular Settin 40%

Configure APN parameters according to your SIM card details. Enable Auto APN and continue if unsure

SIM 1

PIN Code:

Auto APN:

APN:

Authentication Type: None

SIM 2

PIN Code:

Auto APN:

APN:

Authentication Type: None

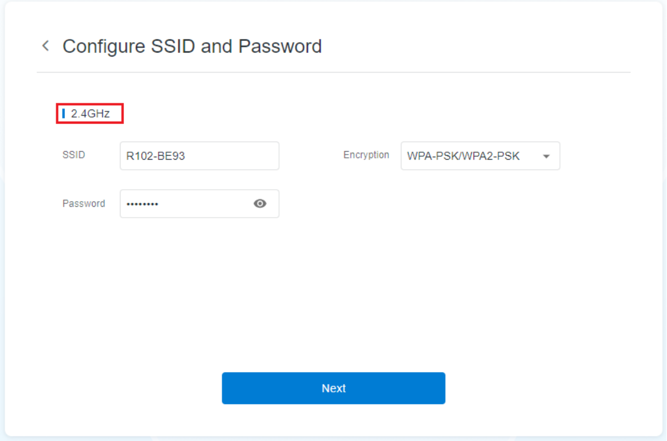
PIN: Carrier-defined, optional.

APN: Carrier-defined; required when **Auto APN** is off.

Authentication Type (None / PAP / CHAP): Carrier-defined; required when **Auto APN** is off.

When **Auto APN** is enabled, users do not need to manually configure the APN and authentication type.

4. Configure the Wi-Fi SSID, encryption, and password for the device operating as a Wi-Fi access point, then click **Next**.



Configure SSID and Password

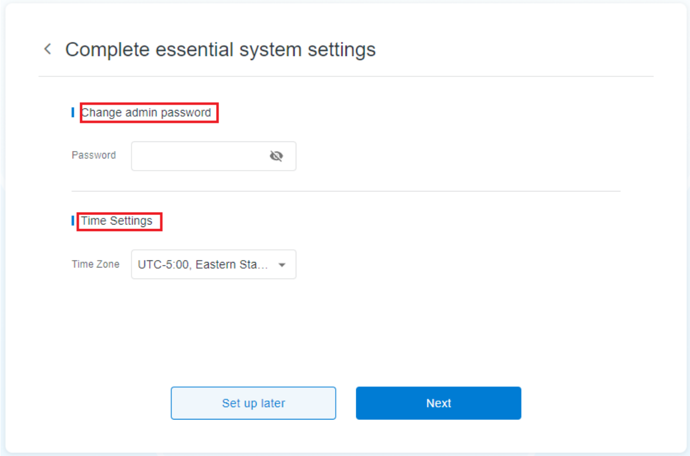
2.4GHz

SSID: R102-BE93

Encryption: WPA-PSK/WPA2-PSK

Password: ••••••••

5. Change the login password for the **Admin** user and select your time zone, then click **Next**. You can skip this by clicking **Set up later**.



Complete essential system settings

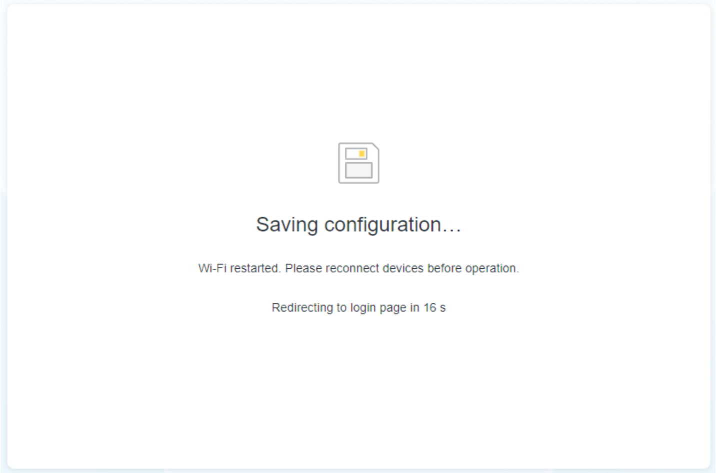
Change admin password

Password

Time Settings

Time Zone: UTC-5:00, Eastern Sta...

6. Wait about 20 seconds to allow the changes to apply. Once the countdown finishes, you will be redirected to the login page.



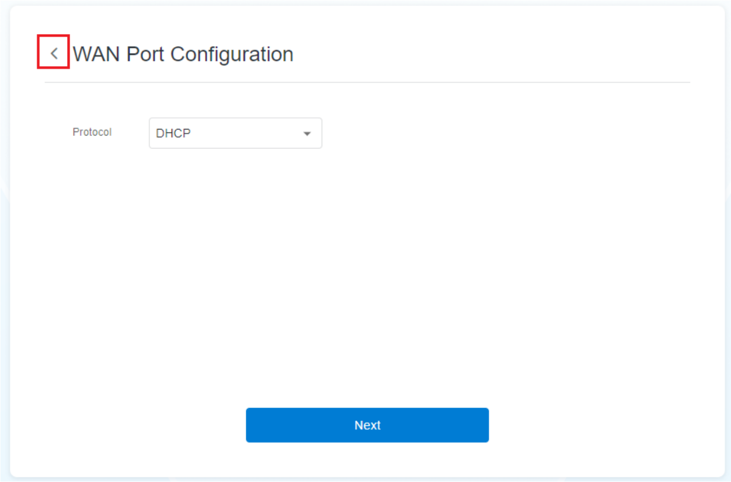
Saving configuration…

Wi-Fi restarted. Please reconnect devices before operation.

Redirecting to login page in 16 s

7. Log in to the web portal using the new Admin password (if changed previously).

Whenever you need return to the previous step, click the back arrow on the left.

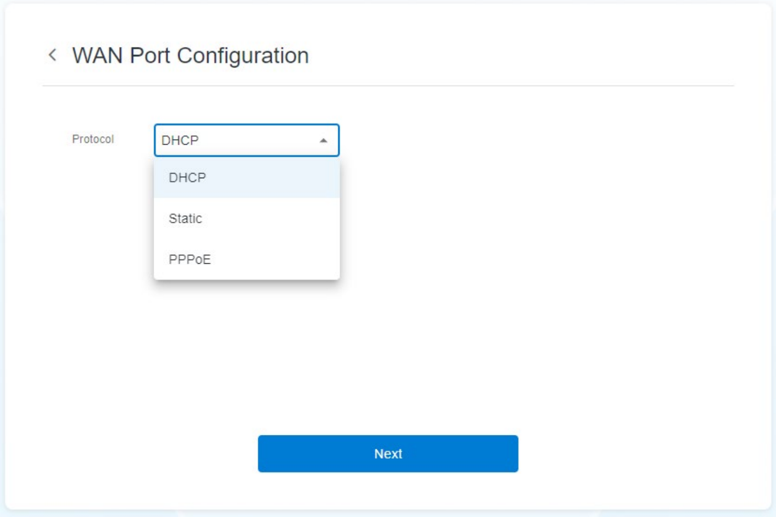


WAN Port Configuration

Protocol: DHCP

- **If you choose WAN Port Settings (WAN Cable Connected)**

1. Select an IP configuration mode for the WAN port, then click **Next**.



WAN Port Configuration

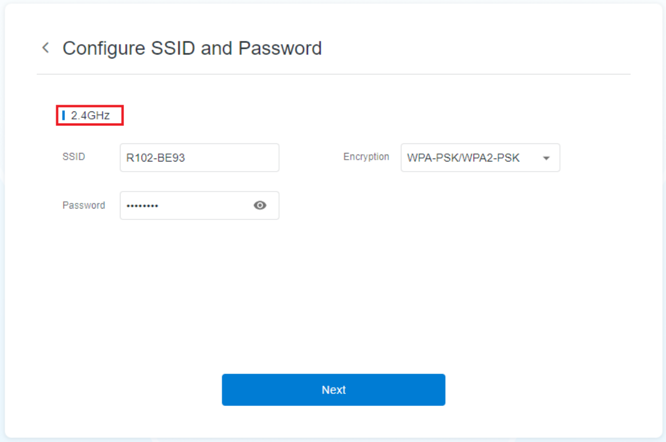
Protocol: DHCP

DHCP (Dynamic Host Configuration Protocol): A DHCP server **automatically** assigns IP addresses and network configuration (subnet, gateway, DNS) to the device.

Static: IP settings are **manually** entered into the device and remain fixed until changed.

PPPoE (Point-to-Point Protocol over Ethernet): The device **dial-ups** an ISP using a username and password encapsulated in PPP over Ethernet; the ISP then assigns IP settings dynamically (or sometimes fixed).

2. Configure the Wi-Fi SSID, encryption, and password for the device operating as a Wi-Fi access point, then click **Next**.



Configure SSID and Password

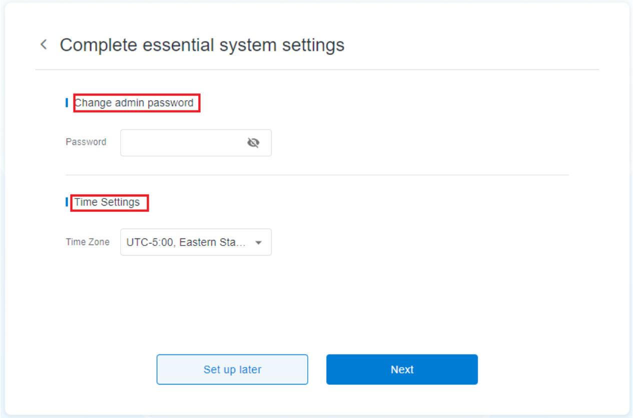
2.4GHz

SSID: R102-BE93

Encryption: WPA-PSK/WPA2-PSK

Password: ••••••••

3. Change the login password for the **Admin** user and select a device time zone, then click **Next**. You can skip this by clicking **Set up later**.



Complete essential system settings

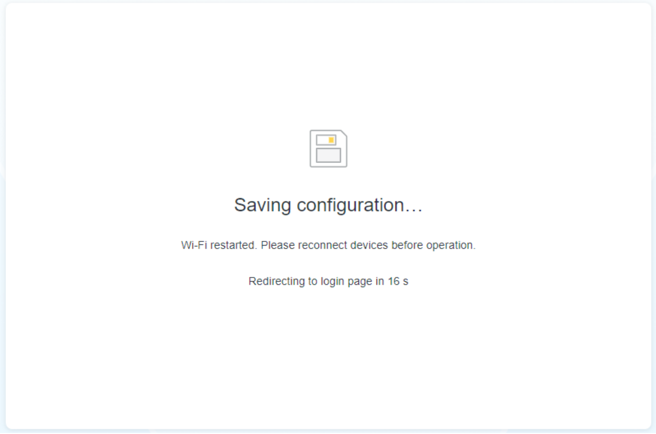
Change admin password

Password

Time Settings

Time Zone: UTC-5:00, Eastern Sta...

4. Wait about 20 seconds to allow the changes to apply. Once the countdown finishes, you will be redirected to the login page.



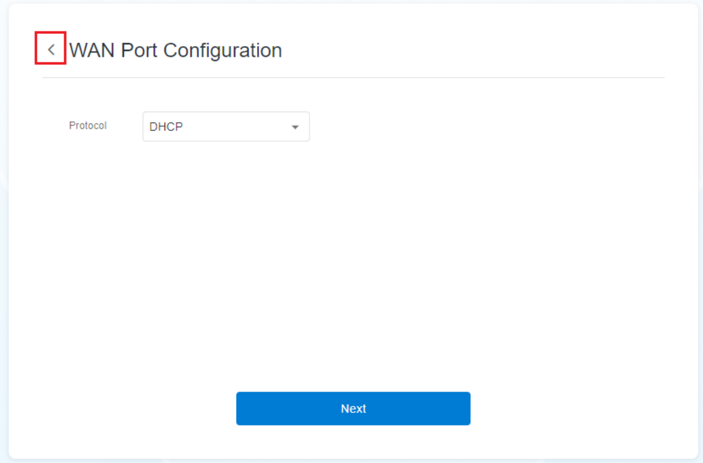
Saving configuration…

Wi-Fi restarted. Please reconnect devices before operation.

Redirecting to login page in 16 s

5. Log in to the web portal using the new Admin password (if changed).

Whenever you need return to the previous step, click the back arrow on the left.



WAN Port Configuration

Protocol: DHCP

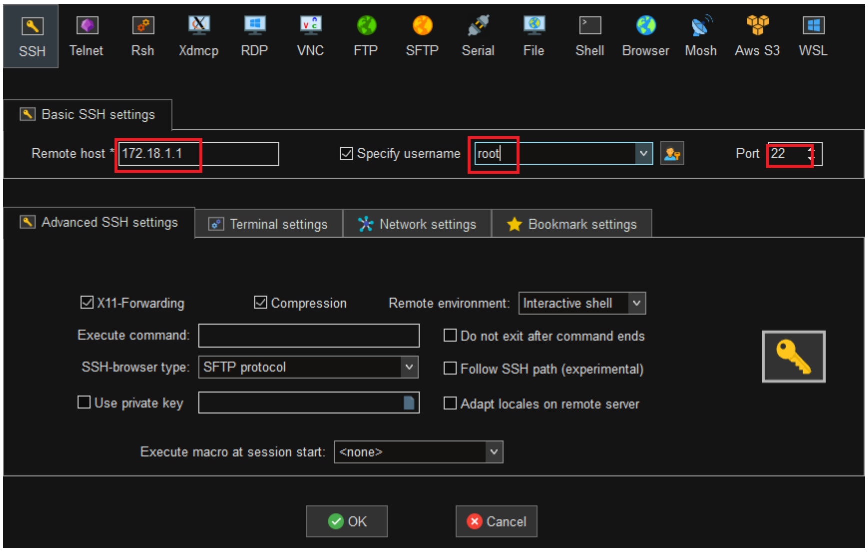
2.3 SSH Login

SSH is enabled on G202 by default. Prior to establishing an SSH connection, make sure the Windows host computer (client) can reach G202's (server) IP, and the SSH port on G202 is enabled.

Method	Host Computer Connection	Login Address
Option 1	Ethernet connection to G202's LAN port or 2.4GHz Wi-Fi connection to G202	Use G202's LAN IP (default IP address: 172.18.1.1)
Option 2	Host's WAN interface on the same IP subnet as G202's WAN interface (e.g., both connected to the same switch or upstream Wi-Fi).	Use G202's WAN IP

SSH login via LAN IP:

1. Connect the Windows host computer to G202's LAN port via Ethernet or connect to its 2.4GHz Wi-Fi.
2. Open a serial debug program (PuTTY or MobaXterm recommended) on the host computer.
3. Select **SSH** session.
4. Enter G202's LAN IP, keep the default SSH port No. (22) unchanged, and use "root" as the username.



Remote host * 172.18.1.1 ☑ Specify username root Port 22

☑ X11-Forwarding ☑ Compression Remote environment: Interactive shell

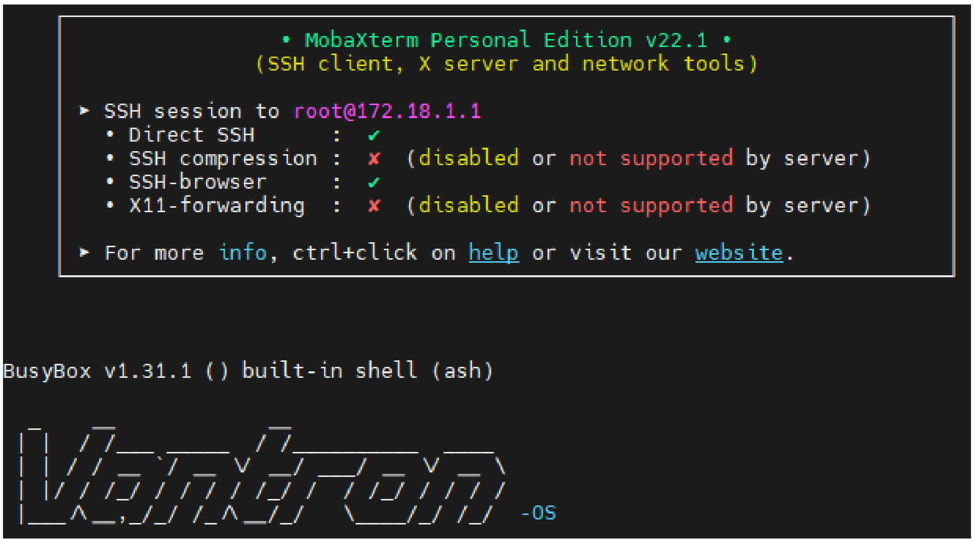
Execute command: ☐ Do not exit after command ends

SSH-browser type: SFTP protocol ☐ Follow SSH path (experimental)

☐ Use private key ☐ Adapt locales on remote server

Execute macro at session start: <none>

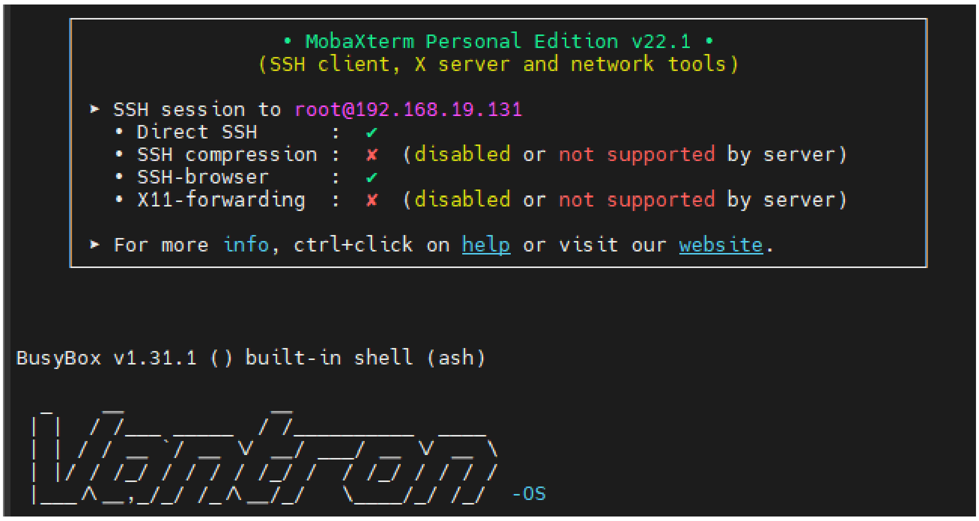
5. Click **OK** to open the session.



```
                    • MobaXterm Personal Edition v22.1 •
                  (SSH client, X server and network tools)

  ➤ SSH session to root@172.18.1.1
    • Direct SSH      :  ✔
    • SSH compression :  ✘  (disabled or not supported by server)
    • SSH-browser     :  ✔
    • X11-forwarding  :  ✘  (disabled or not supported by server)

  ➤ For more info, ctrl+click on help or visit our website.


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

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

SSH login via WAN IP:

1. Connect both the Windows host computer and G202 to the same switch via Ethernet or Wi-Fi.
2. Determine G202's WAN IP.
3. Follow steps 2 through 5 above to complete the login. Remember to replace the LAN IP with the determined WAN IP while filling in the 'Remote host' field.



```
                    • MobaXterm Personal Edition v22.1 •
                  (SSH client, X server and network tools)

  ➤ SSH session to root@192.168.19.131
    • Direct SSH      :  ✔
    • SSH compression :  ✘  (disabled or not supported by server)
    • SSH-browser     :  ✔
    • X11-forwarding  :  ✘  (disabled or not supported by server)

  ➤ For more info, ctrl+click on help or visit our website.


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

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

SSH login requires root privileges. The root password is unique to each device due to security concern. Please contact the Vantron FAE team to obtain it.

2.4 Device Name Modification

By default, the operating system identifies the device as VantronOS-XXXX, and this name can be changed. Refer to section 3.7.1 for the instructions.

2.5 Interfacing with Vantron Gateway Manager

BlueSphere Gateway Manager (hereinafter referred to as "GWM") is a cloud-based management portal that empowers organizations to seamlessly provision, monitor, and manage Vantron IoT communication devices, including gateways, routers, and DTUs. By leveraging BlueSphere GWM, organizations can streamline device setup, ensure real-time visibility into device performance, and effortlessly control device configurations. This contributes to enhanced operational efficiency and improved decision-making.

To use BlueSphere GWM for remote management of G202, ensure you are an authorized BlueSphere GWM user with a valid customer ID. Refer to section 3.7.4.1 for adding your device to BlueSphere GWM for centralized management.

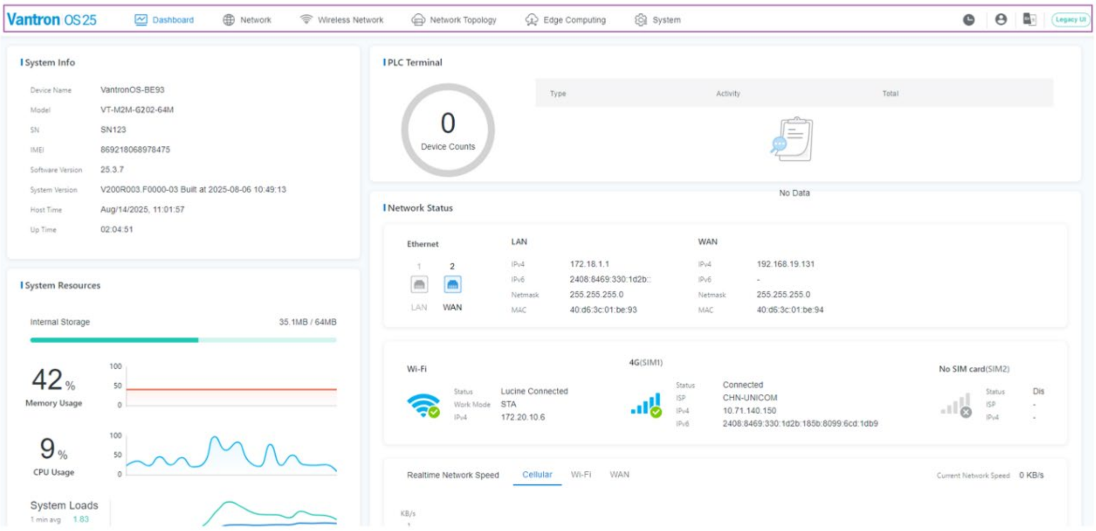
CHAPTER 3 DEVICE SETUP VIA VANTRONOS

3.1 Introduction to VantronOS

VantronOS is an intelligent operating system developed by the Vantron team, featuring independent system and function development. It is built upon the Linux system and optimized for embedded hardware. The operating system follows a modular design and plug-in expansion approach, utilizing the Linux kernel with a built-in firewall to ensure secure internet connectivity for Vantron IoT communication devices, protecting them from potential attacks.

VantronOS incorporates a user-friendly UI interface based on the MVC framework, providing a simple and efficient setting entry for users. Additionally, it offers seamless interfacing with various cloud management platforms, including the self-developed BlueSphere GWM, as well as popular platforms like Azure, Alibaba Cloud, Huawei Cloud, and RootCloud. This enables users to remotely monitor, operate, and diagnose devices without the need for on-site technical support engineers. VantronOS facilitates the interconnection and interaction between users and the Industrial Internet of Things, enhancing the overall efficiency and convenience of device management.

3.1.1 Web Overview



System Info

Device Name	VantronOS-BE93
Model	VT-M2M-G202-64M
SN	SN123
IMEI	869218068978475
Software Version	25.3.7
System Version	V200R003.F0000-03 Built at 2025-08-06 10:49:13
Host Time	Aug/14/2025, 11:01:57
Up Time	02:04:51

Internal Storage 35.1MB / 64MB

	LAN	WAN
IPv4	172.18.1.1	192.168.19.131
IPv6	2408:8469:330:1d2b::	-
Netmask	255.255.255.0	255.255.255.0
MAC	40:d6:3c:01:be:93	40:d6:3c:01:be:94

Wi-Fi: Status Lucine Connected; Work Mode STA; IPv4 172.20.10.6

4G(SIM1): Status Connected; ISP CHN-UNICOM; IPv4 10.71.140.150; IPv6 2408:8469:330:1d2b:185b:8099:6cd:1db9

No SIM card(SIM2): Status Dis; ISP -; IPv4 -

Current Network Speed 0 KB/s

VantronOS25 is the latest version of the operating system, built on the legacy VantronOS2, consisting of the following components:

Dashboard: Displays general device information and dynamic status updates.

Network: Manages network settings, including interface setup, link management, and security configurations.

Wireless Network: Configures device settings for Wi-Fi and cellular connectivity.

Network Topology: Provides information of connected devices (downlink devices). Devices connected via a bridged interface will be invisible.

Edge Computing: Configures the device for field endpoint connection and data processing.

System: Displays device information, system settings, network diagnostics, connection with BlueSphere GWM.

Time Settings:

- "Current Time" reflects the time zone chosen in the setup wizard.
- "Sync Local Time" aligns the device clock with the host computer.
- "Time Settings" opens additional options for manual configuration.

Refer to section 3.7.1.2 for modifying the time settings.

User Avatar: For log out selection upon a click.

Language Toggle: English ⇄ Chinese.

Legacy UI: For opening VantronOS2's web UI.

3.1.2 Log Out

To sign out:

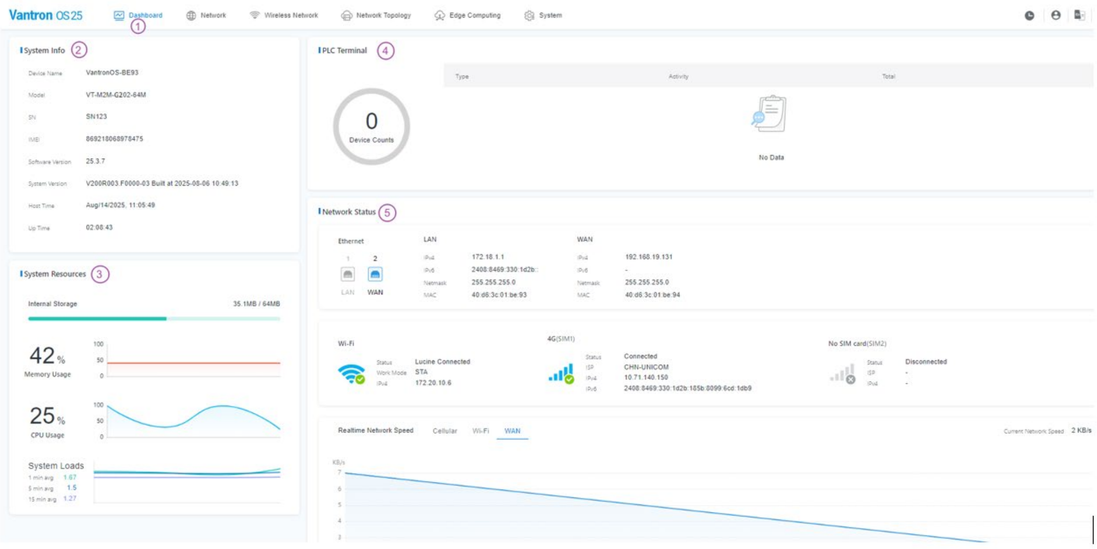
1. Click the user avatar in the upper right corner.
2. Select **Logout**.
3. Confirm the action by clicking **Logout** again.

3.1.3 Language Change

The system supports English and Chinese. Users can click the language icon to toggle between the languages.

3.2 Dashboard

This page provides the overall information of the gateway, including system information, device resource usage, connected PLCs, interface connection status, traffic statistics, etc.



System Info

Device Name VantronOS-BE93
Model VT-M2M-G202-64M
SN SN123
IMEI 869218068978475
Software Version 25.3.7
System Version V200R003.F0000-03 Built at 2025-08-06 10:49:13
Host Time Aug/14/2025, 11:05:49
Up Time 02:08:43

System Resources

Internal Storage 35.1MB / 64MB

42 % Memory Usage

25 % CPU Usage

System Loads
1 min avg 1.67
5 min avg 1.5
15 min avg 1.27

PLC Terminal

0 Device Counts

Type	Activity	Total

No Data

Network Status

Ethernet: 1 LAN, 2 WAN

LAN		WAN	
IPv4	172.18.1.1	IPv4	192.168.19.131
IPv6	2408:8469:330:1d2b::	IPv6	-
Netmask	255.255.255.0	Netmask	255.255.255.0
MAC	40:d6:3c:01:be:93	MAC	40:d6:3c:01:be:94

Wi-Fi
Status Lucine Connected
Work Mode STA
IPv4 172.20.10.6

4G(SIM1)
Status Connected
ISP CHN-UNICOM
IPv4 10.71.140.150
IPv6 2408:8469:330:1d2b:185b:8099:6cd:1db9

No SIM card(SIM2)
Status Disconnected
ISP -
IPv4 -

Realtime Network Speed: Cellular Wi-Fi WAN
Current Network Speed 2 KB/s

Description of the numbered areas

1. **Menu Tabs**—the active menu is highlighted in blue.
2. **System Information**—including: device name, model, serial number, IMEI, software version, firmware version, current host time, and uptime.
3. **System Resources**—indicating the device’s performance, mainly including: storage space (used/total), memory & CPU usage, and system load (1-, 5-, 15-minute averages).
4. **PLC Terminals**—displaying controller type, activity status, and device count.
5. **Network Status**—live status and throughput for each interface.
    - Ethernet: LAN/WAN port IP addresses, subnet masks and MAC addresses

      Clicking Ethernet port icons will direct you to corresponding interface settings.
    - Wireless networks: Wi-Fi (operation mode and corresponding information); Cellular (network status, carrier, and IP addresses)
    - Real-time network speeds: Uplink Cellular/Wi-Fi (client)/WAN speeds

3.3 Network

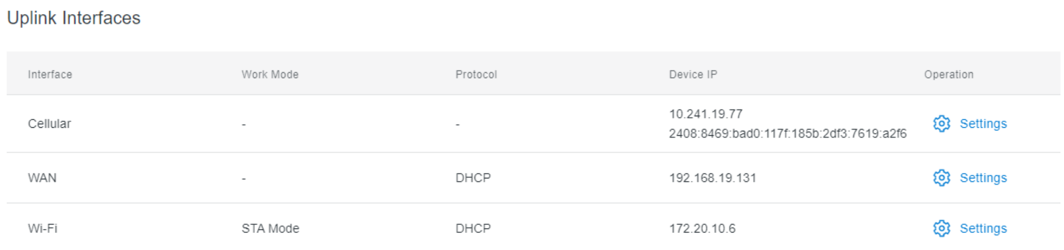
The **Network** menu centralizes critical network management functions, including interface settings, link redundancy, static routing, and more. These features enable precise control over connectivity, ensuring optimal performance and high availability. By integrating these tools, the system reduces administrative overhead and enhances operational efficiency, allowing you to build a resilient, secure, and fully customized network fabric.

3.3.1 Interface Settings

Interfaces are categorized into uplink and downlink domains.

On G202, uplink interfaces include the cellular modem, Ethernet WAN port, and Wi-Fi client; downlink interfaces consist of the Ethernet LAN port and Wi-Fi access point.

3.3.1.1 Uplink Interfaces



Uplink Interfaces

Interface	Work Mode	Protocol	Device IP	Operation
Cellular	-	-	10.241.19.77 2408:8469:bad0:117f:185b:2df3:7619:a2f6	Settings
WAN	-	DHCP	192.168.19.131	Settings
Wi-Fi	STA Mode	DHCP	172.20.10.6	Settings

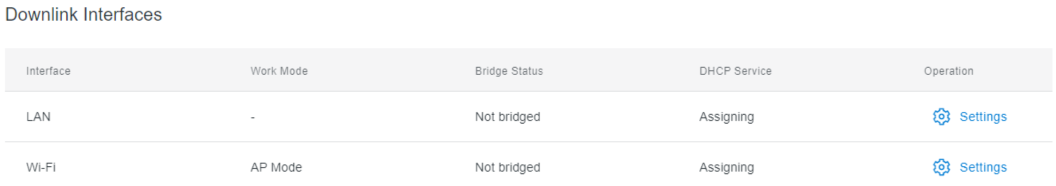
Clicking the **Settings** icon after the **Cellular** interface redirects you to the settings page of the cellular interface. Refer to section 3.4.1 for the details.

The **Settings** icons for the WAN and Wi-Fi client interfaces allow you to select an IP configuration mode for the interface. Refer to section 3.3.1.4 for the configurations.

IP configuration modes:

- **DHCP (Dynamic Host Configuration Protocol)**: A DHCP server **automatically** assigns IP addresses and network configuration (subnet, gateway, DNS) to the device.
- **Static**: IP settings are **manually** entered into the **device** and remain fixed until changed.
- **PPPoE (Point-to-Point Protocol over Ethernet)**: The device **dial-ups** an ISP using a username and password encapsulated in PPP over Ethernet; the ISP then assigns IP settings dynamically (or sometimes fixed). This protocol applies to Ethernet **WAN port** only.

3.3.1.2 Downlink Interfaces



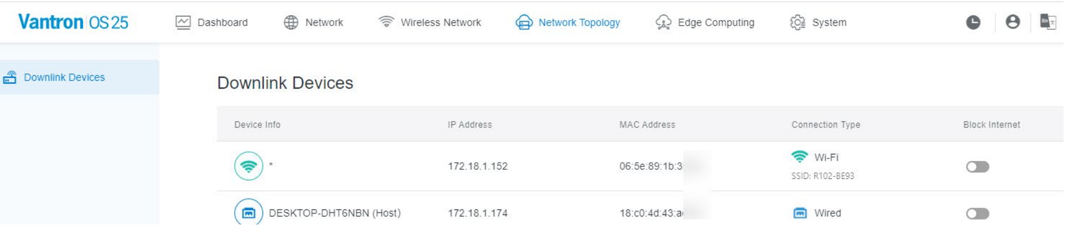
Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
LAN	-	Not bridged	Assigning	⚙ Settings
Wi-Fi	AP Mode	Not bridged	Assigning	⚙ Settings

The **Settings** icons for the LAN and Wi-Fi AP interfaces allow you to select whether to bridge the interface to an uplink interface that connects to a DHCP server. If enabled, client devices connected to G202 through this link will receive an IP from the DHCP server. Refer to section 3.3.1.5 for the configurations.

When **DHCP Service** is displaying **Assigning**, DHCP service on the corresponding port is enabled.

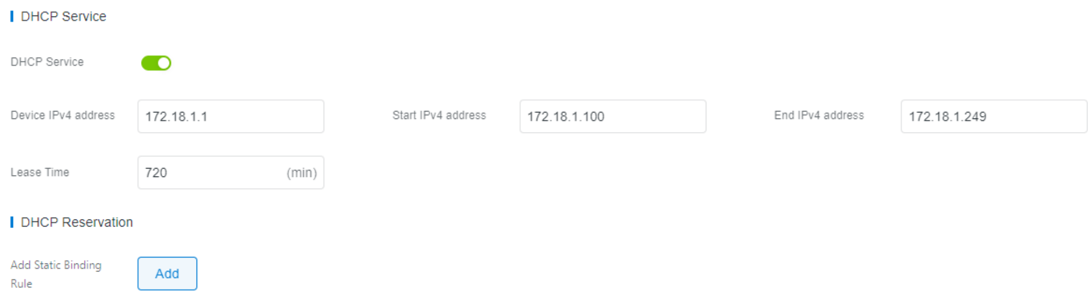
IP information of connected devices can be viewed under the **Network Topology** menu.



Downlink Devices

Device Info	IP Address	MAC Address	Connection Type	Block Internet
*	172.18.1.152	06:5e:89:1b:3	Wi-Fi SSID: R102-BE93	○
DESKTOP-DHT6NBN (Host)	172.18.1.174	18:c0:4d:43:a	Wired	○

3.3.1.3 DHCP Service & DHCP Reservation



DHCP Service

DHCP Service	●				
Device IPv4 address	172.18.1.1	Start IPv4 address	172.18.1.100	End IPv4 address	172.18.1.249
Lease Time	720 (min)				

DHCP Reservation

Add Static Binding Rule: Add

DHCP Service and **DHCP Reservation** are specific to downlink interfaces. **DHCP Reservation** is available **only** when **DHCP Service** is enabled.

Editable fields under **DHCP Service**:

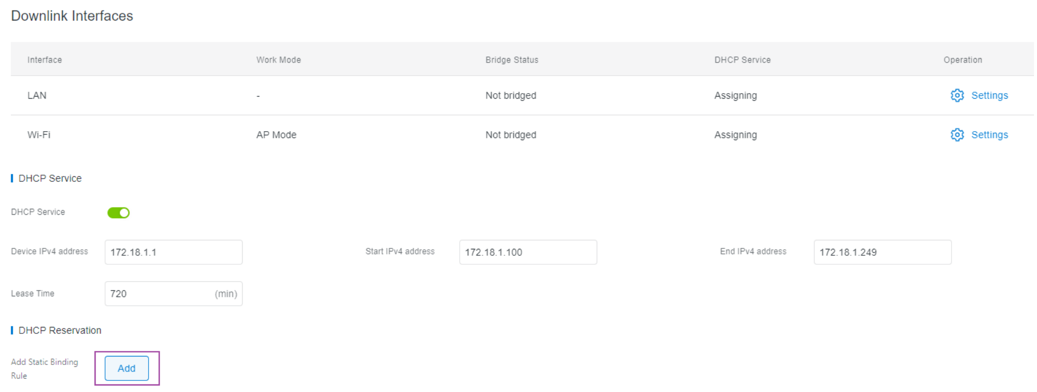
- Device IPv4 address: G202’ own IP address on the downlink domain.
- Start & End IPv4 addresses: The pool from which addresses are leased to clients.
- Lease Time: The valid duration for which G202, as the DHCP server, assigns an IP address to a client. Before expiry of the lease time, the client will send a renew request to G202 to extend the lease. If the renewal fails and the lease expires, the client must release this IP address and initiate a new DHCP discovery.

DHCP Reservation allows a DHCP server to reserve a specific IP address for a particular device (client) based on its MAC address. When enabled, the server will always assign the same IP address to that device whenever it connects to the network, optimizing the network's IP address space and enhancing network security.

By adding a DHCP reservation rule to G202, the specified client device will maintain the allocated IP address to reduce configuration errors.

Steps of adding a DHCP reservation rule:

1. Click **Add** under **DHCP Reservation**.



Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
LAN	-	Not bridged	Assigning	Settings
Wi-Fi	AP Mode	Not bridged	Assigning	Settings

DHCP Service

DHCP Service: on

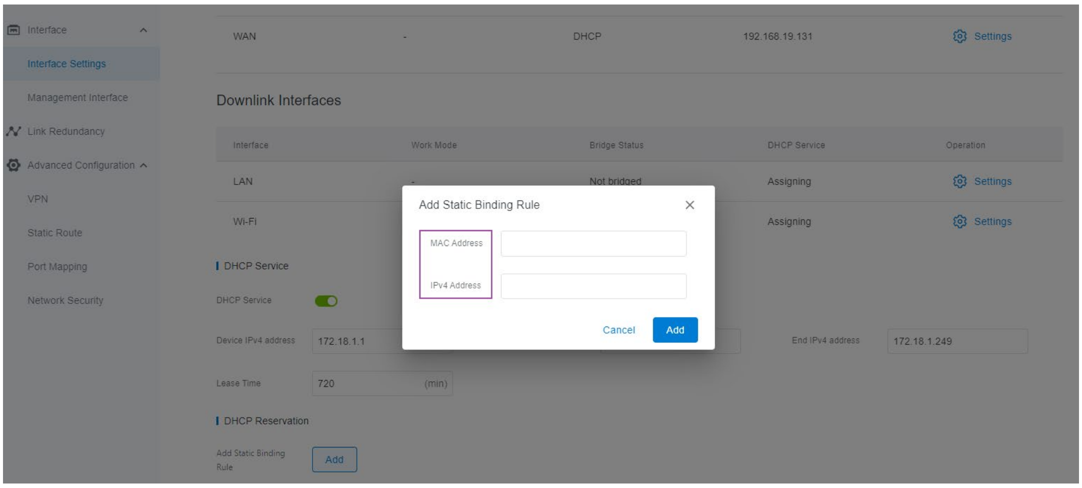
Device IPv4 address: 172.18.1.1 Start IPv4 address: 172.18.1.100 End IPv4 address: 172.18.1.249

Lease Time: 720 (min)

DHCP Reservation

Add Static Binding Rule: Add

2. Enter the client's MAC address and allocate an IP between the start and end IPv4 addresses specified under **DHCP Service**.



WAN	-	DHCP	192.168.19.131	Settings

Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
LAN	-	Not bridged	Assigning	Settings
Wi-Fi			Assigning	Settings

Add Static Binding Rule

MAC Address:

IPv4 Address:

Cancel Add

DHCP Service

DHCP Service: on

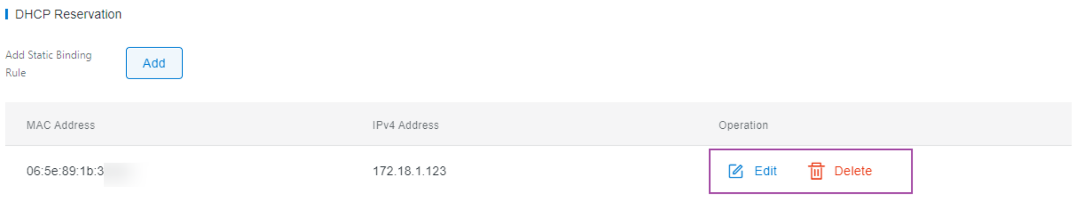
Device IPv4 address: 172.18.1.1 End IPv4 address: 172.18.1.249

Lease Time: 720 (min)

DHCP Reservation

Add Static Binding Rule: Add

3. After adding the rule, you can edit or delete it as needed.

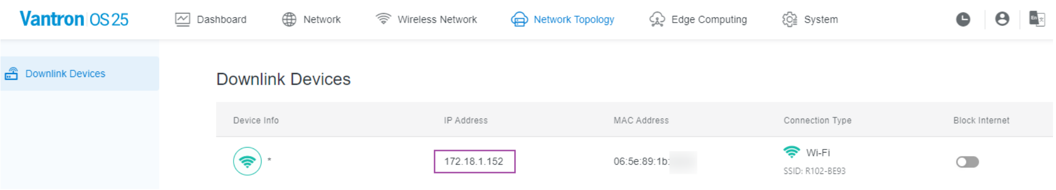


DHCP Reservation

Add Static Binding Rule: Add

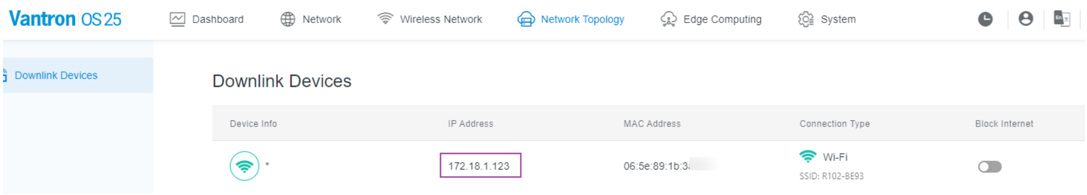
MAC Address	IPv4 Address	Operation
06:5e:89:1b:3[redacted]	172.18.1.123	Edit Delete

4. If you have assigned a fixed IP to the MAC address of a connected device, reconnect the device to G202, and its IP will update accordingly as shown under **Network Topology**.



Downlink Devices

Device Info	IP Address	MAC Address	Connection Type	Block Internet
*	172.18.1.152	06:5e:89:1b:[redacted]	Wi-Fi SSID: R102-BE93	○



Downlink Devices

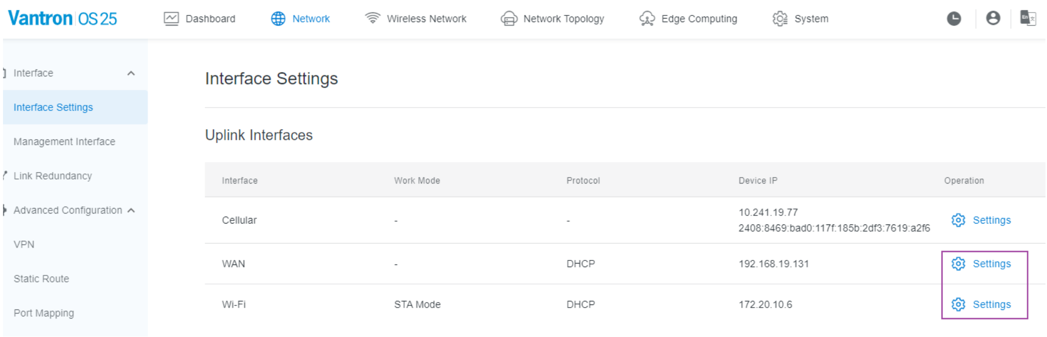
Device Info	IP Address	MAC Address	Connection Type	Block Internet
*	172.18.1.123	06:5e:89:1b:3[redacted]	Wi-Fi SSID: R102-BE93	○

3.3.1.4 IP Configuration Mode

As described earlier, there are different IP configuration modes for uplink interfaces.

To select the IP configuration mode:

1. Click the **Settings** icon after the WAN or Wi-Fi client interface on the **Uplink Interface** page.

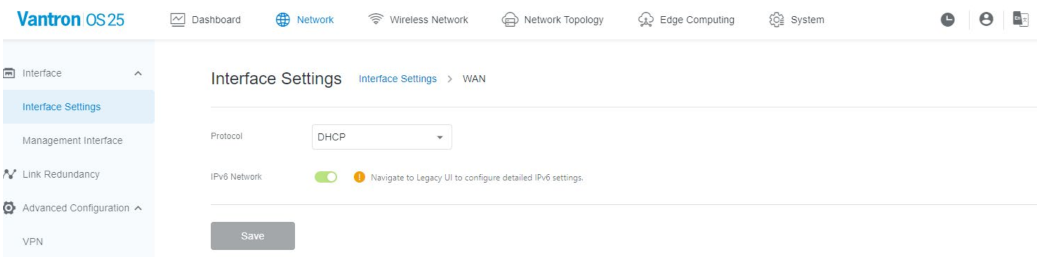


Interface Settings

Uplink Interfaces

Interface	Work Mode	Protocol	Device IP	Operation
Cellular	-	-	10.241.19.77 2408:8469:bad0:117f:185b:2df3:7619:a2f6	Settings
WAN	-	DHCP	192.168.19.131	Settings
Wi-Fi	STA Mode	DHCP	172.20.10.6	Settings

- **DHCP**: The DHCP server will **automatically** assign an IP address for the interface.



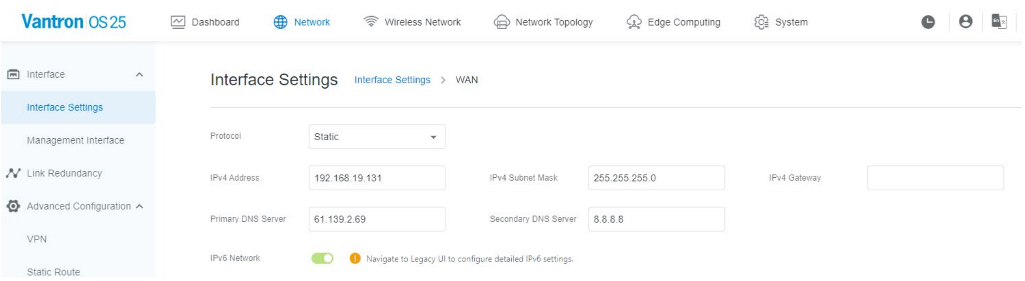
Interface Settings   Interface Settings > WAN

Protocol: DHCP

IPv6 Network: ● Navigate to Legacy UI to configure detailed IPv6 settings.

If you need configure IPv6, please navigate to **Network > Interfaces** on the legacy UI, and modify the settings of the target interface accordingly.

- **Static**: You need **manually** configure the IP address for the interface, inducing the subnet, gateway, and DNS.



Interface Settings Interface Settings > WAN

Protocol: Static

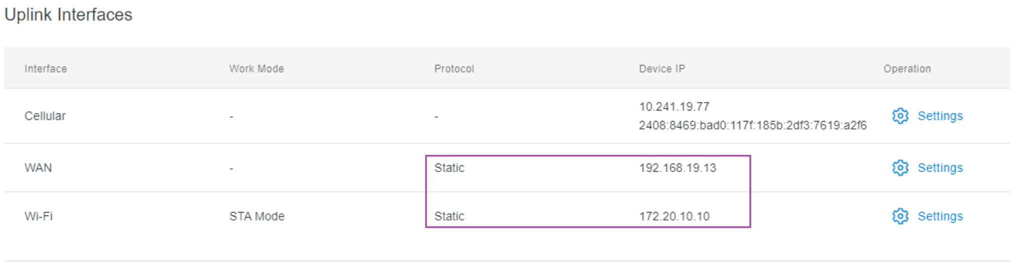
IPv4 Address: 192.168.19.131 IPv4 Subnet Mask: 255.255.255.0 IPv4 Gateway:

Primary DNS Server: 61.139.2.69 Secondary DNS Server: 8.8.8.8

IPv6 Network Navigate to Legacy UI to configure detailed IPv6 settings.

- **PPPoE** (**WAN** port applicable)**:** You need enter the ISP username and password to establish the PPP-over-Ethernet session.

2. After configuring the interfaces, you may need **relog** in to VantronOS depending on the connection between the host computer and G202.



Uplink Interfaces

Interface	Work Mode	Protocol	Device IP	Operation
Cellular	-	-	10.241.19.77 2408:8469:bad0:117f:185b:2df3:7619:a2f6	Settings
WAN	-	Static	192.168.19.13	Settings
Wi-Fi	STA Mode	Static	172.20.10.10	Settings

Ensure the host computer and G202 are on the same subnet for VantronOS login.

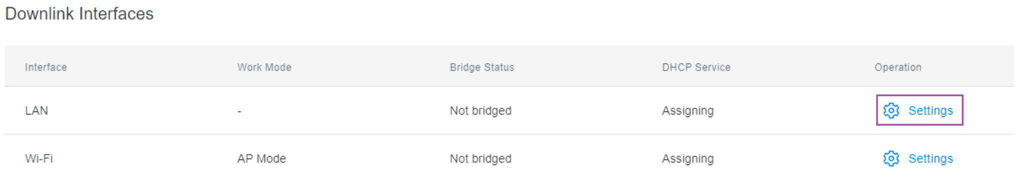
3.3.1.5 Interface Bridging

By enabling the bridge mode for a downlink interface (Ethernet LAN/Wi-Fi AP), both the bridged interface and uplink interface will be added to the same Layer 2 bridge, sharing the same broadcast domain:

- Any device connected to the bridged interface is placed on the upstream network.
- G202 stops performing NAT or DHCP for that LAN/Wi-Fi interface. Instead, the upstream (WAN-side) DHCP server handles all client addressing.

To enable the bridge mode on a downlink interface:

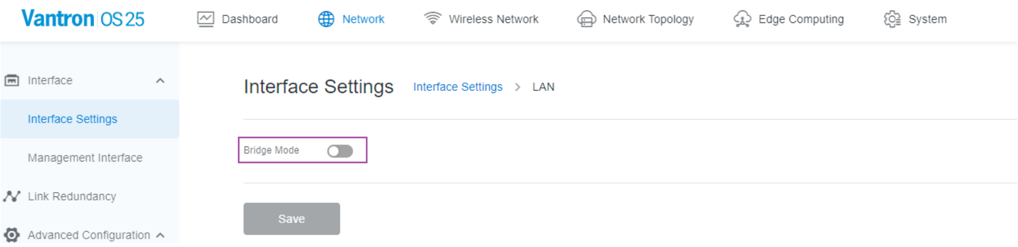
1. Click the **Settings** icon after a downlink interface (Ethernet LAN for instance).



Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
LAN	-	Not bridged	Assigning	Settings
Wi-Fi	AP Mode	Not bridged	Assigning	Settings

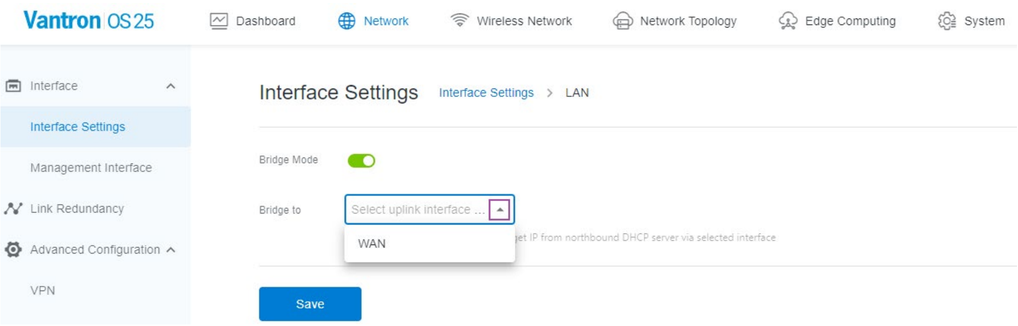
2. Turn on **Bridge Mode**.



Interface Settings Interface Settings > LAN

Bridge Mode ○

3. Select the uplink interface to bridge to, and click **Save**.



Interface Settings Interface Settings > LAN

Bridge Mode ●

Bridge to: Select uplink interface ...

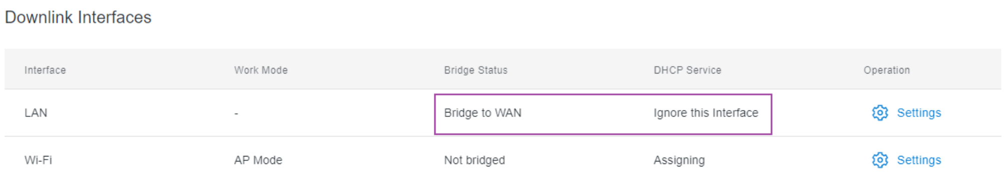
WAN

...et IP from northbound DHCP server via selected interface

4. If you have connected the host computer to the device via the Ethernet LAN port and use the LAN IP to access the device, this operation may disconnect the host computer from the device. In this circumstance, switch to another connection method (for instance, Wi-Fi or same WAN connection), and log in with the corresponding IP address.

   Always ensure the host computer and G202 are on the same subnet for VantronOS login.

5. When bridged, DHCP service will **not** take effect on this interface.



Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
LAN	-	Bridge to WAN	Ignore this Interface	Settings
Wi-Fi	AP Mode	Not bridged	Assigning	Settings

3.3.2 Management Interface

A management interface is a designated **downlink port** used for device administration through the VantronOS web UI or SSH.

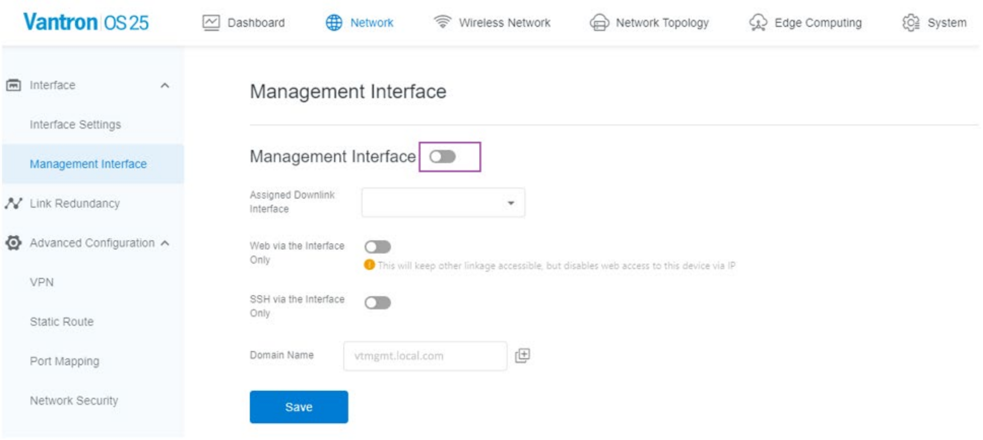
- If a management interface is selected and specified for web/SSH login, users can only manage the device through this interface (and its associated IP, typically 172.18.1.1).
- If a management interface is selected without specifying it for web/SSH login, any downlink or uplink port may be used for device administration.

This also applies when both downlink interfaces are designated as management interfaces.

When "Web via the Interface Only" is enabled, only the specified domain name is accessible for VantronOS login; all other interface IPs (downlink and uplink) are inaccessible. Ensure the host computer has automatic DNS enabled to resolve the management interface's address.

To set a management interface:

1. Toggle the **Management Interface** option.



Management Interface

Management Interface

Assigned Downlink Interface

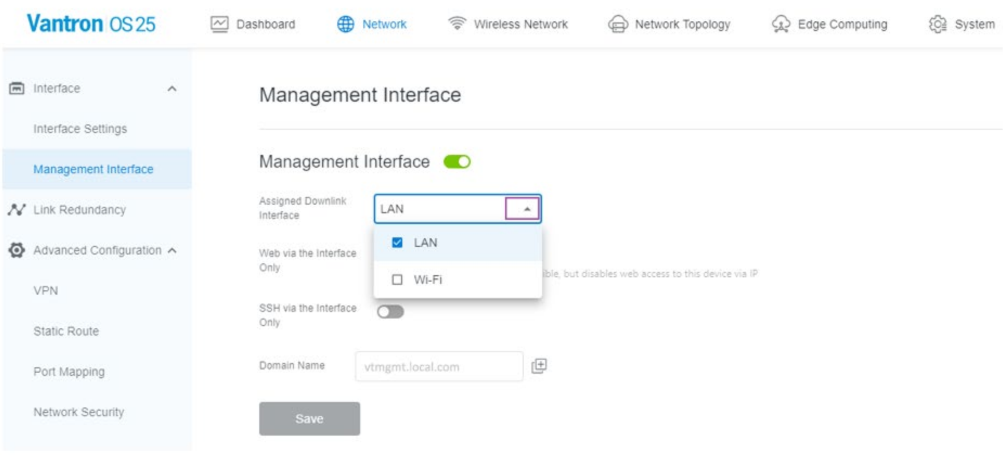
Web via the Interface Only

This will keep other linkage accessible, but disables web access to this device via IP

SSH via the Interface Only

Domain Name: vtmgmt.local.com

2. Select one downlink interface or both as the management interface(s).



Management Interface

Management Interface

Assigned Downlink Interface: LAN

☑ LAN

□ Wi-Fi

Web via the Interface Only

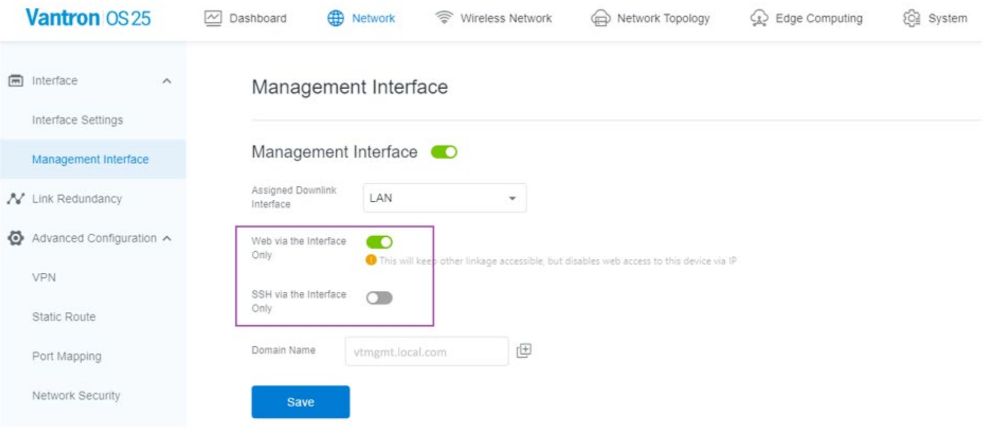
...ble, but disables web access to this device via IP

SSH via the Interface Only

Domain Name: vtmgmt.local.com

- **LAN**: Ethernet LAN port
- **Wi-Fi**: Wi-Fi AP interface

3. Determine whether to enable **web/SSH login via the selected interface** only.



Management Interface

Management Interface ●

Assigned Downlink Interface: LAN

Web via the Interface Only ●

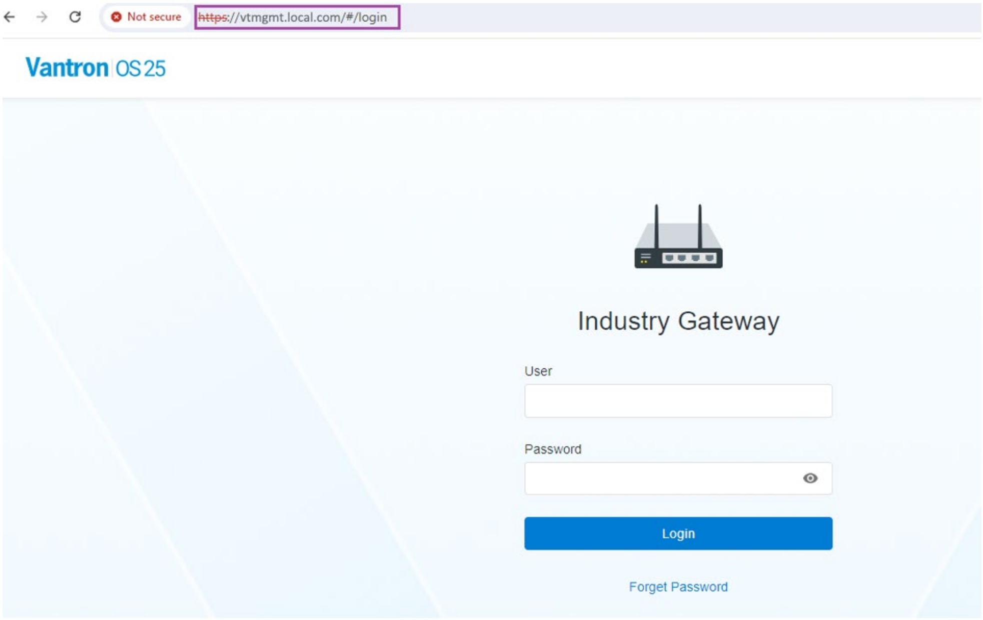
This will keep other linkage accessible, but disables web access to this device via IP

SSH via the Interface Only ○

Domain Name: vtmgmt.local.com

4. Click “+” to copy the domain name for VantronOS login, then click **Save**.

5. Paste the domain name in the browser for VantronOS re-login.



~~https~~://vtmgmt.local.com/#/login

*If **SSH via the Interface Only** is enabled, other methods described in section 2.3 will not be available for SSH login.*

*If **Web via the Interface Only** is enabled, VantronOS can be reached only through the specified domain; otherwise, login is also permitted via the IP addresses of the uplink and downlink interfaces.*

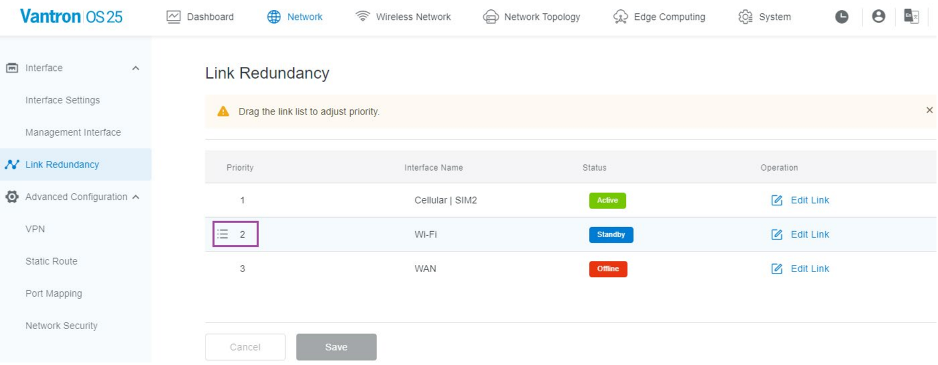
3.3.3 Link Redundancy

Link redundancy ensures network reliability by running multiple connections in parallel. If the primary link fails, traffic is instantly switched to a backup path, minimizing downtime and protecting critical environments from single points of failure.

The default link detection and data forwarding are prioritized based on the following rule: Ethernet (WAN) > Wi-Fi (Client) > LTE > others.

To manually set the network priority:

1. Hover over the target link to highlight it with a light blue background.

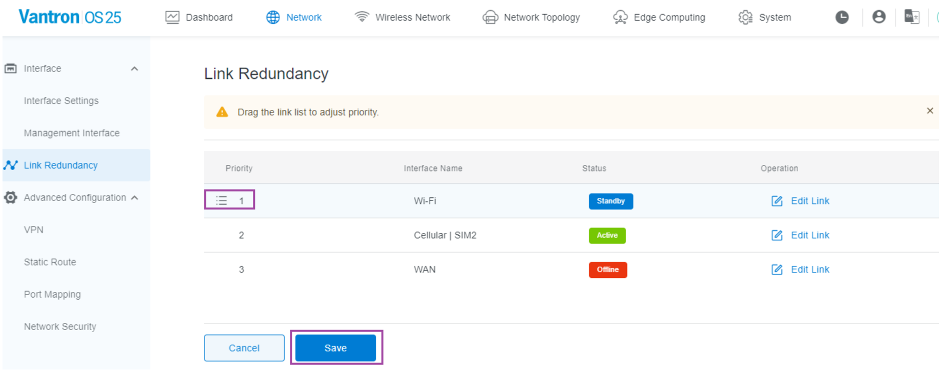


Link Redundancy

Drag the link list to adjust priority.

Priority	Interface Name	Status	Operation
1	Cellular | SIM2	Active	Edit Link
2	Wi-Fi	Standby	Edit Link
3	WAN	Offline	Edit Link

2. Drag the link up or down to the desired position, then click **Save**.



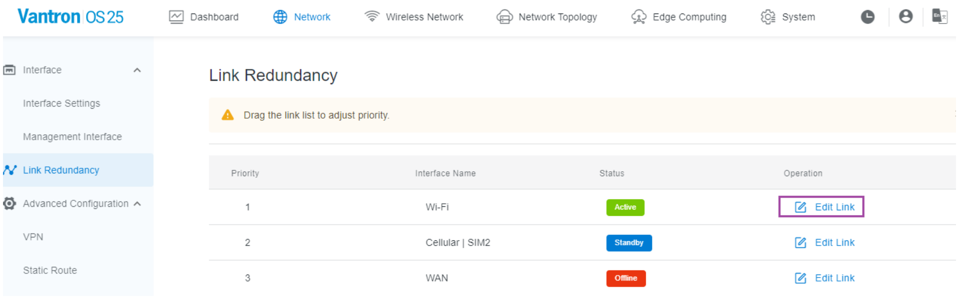
Link Redundancy

Drag the link list to adjust priority.

Priority	Interface Name	Status	Operation
1	Wi-Fi	Standby	Edit Link
2	Cellular | SIM2	Active	Edit Link
3	WAN	Offline	Edit Link

Moving a standby link to the top will change the current active link to the ***Standby*** *status.*

3. Use the **Edit Link** option to modify the probe settings for the link as needed.



Link Redundancy

Drag the link list to adjust priority.

Priority	Interface Name	Status	Operation
1	Wi-Fi	Active	Edit Link
2	Cellular | SIM2	Standby	Edit Link
3	WAN	Offline	Edit Link

Editable fields include: primary & secondary probe addresses, and probe interval.

3.3.4 VPN

A virtual private network (VPN) lets you use the Internet to securely access your network remotely. G202 supports PPTP, L2TP, GRE, IPSec, and OpenVPN protocols to ensure data confidentiality and undisturbedness.

Currently, the OpenVPN protocol is available and other protocols are under development.

You can configure the device either as an OpenVPN server or an OpenVPN client based on needs. Both OpenVPN server and OpenVPN client provide virtual private network based on SSL connection and transmission, which features simple and flexible configurations, better security, and no interference.

3.3.4.1 OpenVPN Server-Client Network Settings

Scenario	Use Case
Server has a public IP (or DDNS); Client connects over the Internet	Standard deployment across public networks, mostly used
Port Forwarding (NAT)	Server sits behind NAT; UDP/1194 (or a self-defined port) has been forwarded to the server's LAN IP
Local area network communication	Intercommunication in the same LAN (Local testing)

You can set up your OpenVPN server and client based on actual situation.

The IP/domain for the **remote** field when connecting an OpenVPN client to a server is as follows:

1. When the server has a public IP: Public IP of the server.
2. When the server has a DDNS: DDNS domain (e.g., vpn.example.com).
3. When the server behind NAT (port forwarding): public IP or DDNS of the front-end gateway.
4. When both server and client are in the same LAN: Local IP of the server in the LAN.

If you are using two G202 gateways for the connection, make sure there is no IP conflict when they are in the same LAN.

The port number specified in the client configuration's remote directive must exactly match the listening port configured on the OpenVPN server.

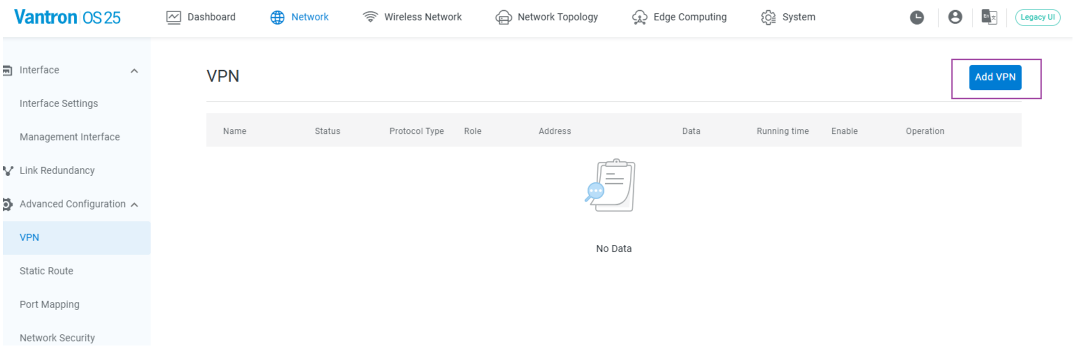
3.3.4.2 OpenVPN Server Setup

Please note that the configuration method provided here is for test only. You are recommended to modify the certificates and keys in the configuration file to your own.

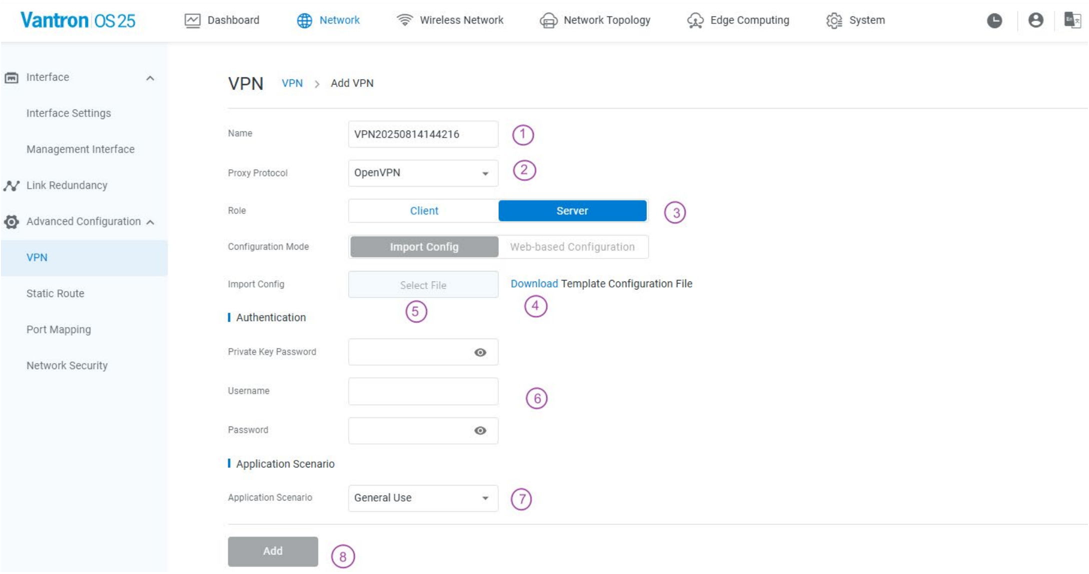
To add an OpenVPN **server** rule for the current G202:

1. Synchronize both G202 and the client to the same NTP server.

2. Click **Add VPN** in the upper right side.



3. In the configuration page, set up the OpenVPN server:



Name: VPN20250814144216

Proxy Protocol: OpenVPN

Role: Server

Configuration Mode: Import Config

Import Config

Authentication

Application Scenario

Application Scenario: General Use

Description of the numbered areas:

1) Enter a configuration file name (current timestamp is the default).

2) Select the OpenVPN protocol (other protocols will be available soon).

3) Select the **Server** role.

   *Currently, web-based configuration is unavailable; download and import the configuration file by following steps 4) and 5). If you have **pre-configured** an OpenVPN server file, just skip step 4), and import it directly from the local directory.*

4) If you do not have a pre-configured file, click **Download** to export the template .conf file.

   - **TAP** mode operates at Layer 2 of the OSI model, creating an Ethernet bridge between the VPN and physical network.
   - **TUN** mode works at Layer 3, handling only IP packets (both IPv4 and IPv6) while creating a separate routed network for VPN clients. **TUN** is the **preferred choice** for general-purpose VPN use cases like remote work, secure web browsing, and cloud access, offering better performance and simpler configuration compared to TAP mode.

5) Click **Select File** to import the pre-configured file or the modified template file.

6) Set the authentication credentials, if necessary.

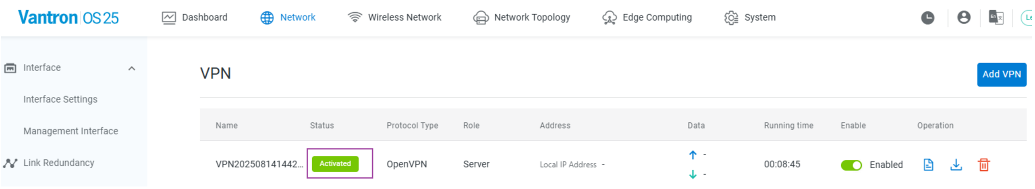
7) Select an application scenario.

   Refer to section 3.3.4.4 for details on the application scenarios.

8) Click **Add** to complete the rule setup.

4. The newly created rule is enabled by default, and shows an **Initializing** status while the device is being configured.

5. When device status changes to **Activated**, the device's role as an OpenVPN server is activated.



Name	Status	Protocol Type	Role	Address	Data	Running time	Enable	Operation
VPN202508141442...	Activated	OpenVPN	Server	Local IP Address -	↑ - ↓ -	00:08:45	Enabled	

After setup, you can enable/disable the rule, view its logs, download its configuration, or delete it.

3.3.4.3 OpenVPN Client Setup

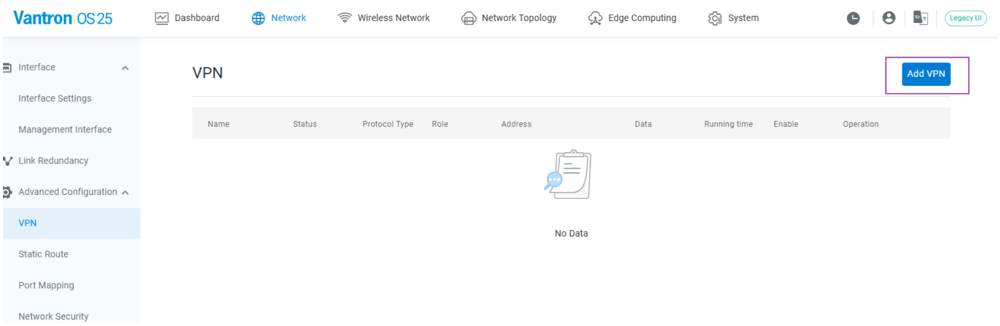
Please note that the configuration method provided here is for test only. You are recommended to modify the certificates and keys in the configuration file to your own.

To add an OpenVPN **Client** rule for the current G202 and connect it to an OpenVPN server:

1. Check the OpenVPN server-client network settings outlined in section 3.3.4.1, and determine the remote IP/domain that fits your situation.

2. Synchronize both G202 and the server to the same NTP server.

3. Click **Add VPN** in the upper right side.

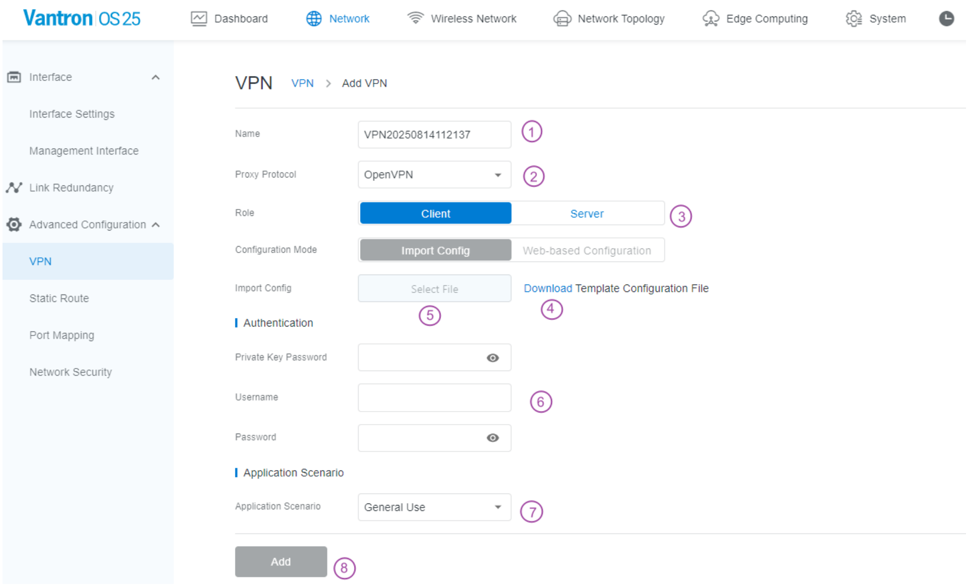


VPN

Name	Status	Protocol Type	Role	Address	Data	Running time	Enable	Operation

No Data

4. On the configuration page, set up the OpenVPN client:



VPN VPN > Add VPN

Name: VPN20250814112137 ①

Proxy Protocol: OpenVPN ②

Role: Client | Server ③

Configuration Mode: Import Config | Web-based Configuration

Import Config: Select File ⑤ Download Template Configuration File ④

Authentication

Private Key Password:

Username: ⑥

Password:

Application Scenario

Application Scenario: General Use ⑦

Add ⑧

Description of the numbered areas

1) Enter a configuration file name (current timestamp is the default).

2) Select the OpenVPN protocol (other protocols will be available soon).

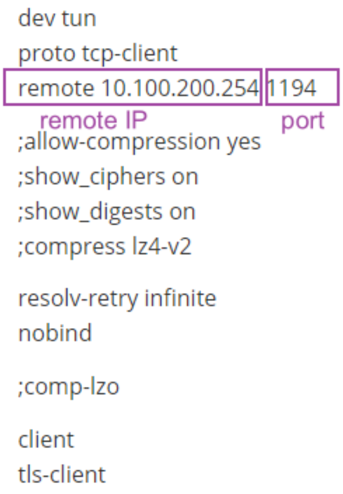
3) Select the **Client** role.

   Currently, web-based configuration is unavailable; download and import the configuration file by following steps 4), 5), and 6). If you have ***pre-configured*** *an OpenVPN client file, just skip steps 4) and 5), and import it directly from the local directory.*

4) If you do not have a pre-configured file, click **Download** to export the template .conf file.

   - **TAP** mode operates at Layer 2 of the OSI model, creating an Ethernet bridge between the VPN and physical network.
   - **TUN** mode works at Layer 3, handling only IP packets (both IPv4 and IPv6) while creating a separate routed network for VPN clients. **TUN** is the preferred choice for general-purpose VPN use cases like remote work, secure web browsing, and cloud access, offering better performance and simpler configuration compared to TAP mode.

5) Modify the **remote** line based on your situation.



```
dev tun
proto tcp-client
remote 10.100.200.254 1194
;allow-compression yes
;show_ciphers on
;show_digests on
;compress lz4-v2

resolv-retry infinite
nobind

;comp-lzo

client
tls-client
```

Refer to section 3.3.4.1 for information on the remote IP/domain. Make sure the port corresponds to that configured on the server.

6) Click **Select File** to import the pre-configured file or the modified template file.

7) Set the authentication credentials, if necessary.

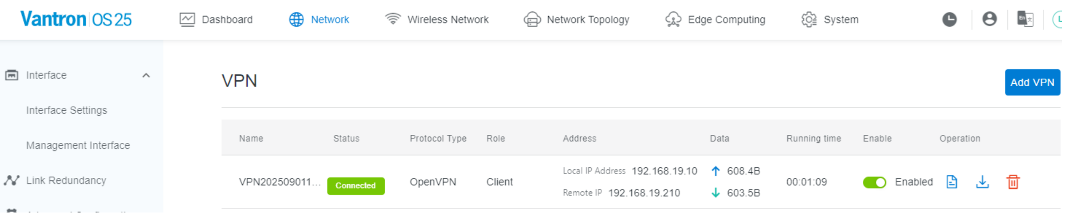
8) Select an application scenario.

Refer to section 3.3.4.4 for details on the application scenarios.

9) Click **Add** to complete the rule setup.

5. The newly created rule is enabled by default and shows an **Initializing** status while the device is being configured.

6. When device status changes to **Connected**, the device is successfully connected to an OpenVPN server as a client.



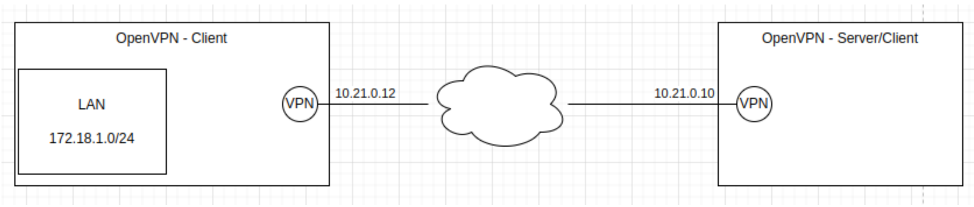
VPN

Name	Status	Protocol Type	Role	Address	Data	Running time	Enable	Operation
VPN202509011...	Connected	OpenVPN	Client	Local IP Address 192.168.19.10 Remote IP 192.168.19.210	↑ 608.4B ↓ 603.5B	00:01:09	Enabled	

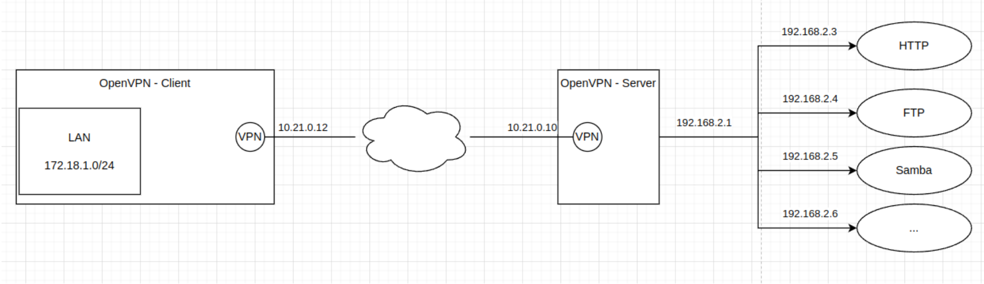
After setup, you can enable/disable the rule, view its logs, download its configuration, or delete it.

3.3.4.4 Application Scenario Topology

- General Use (point-to-point)

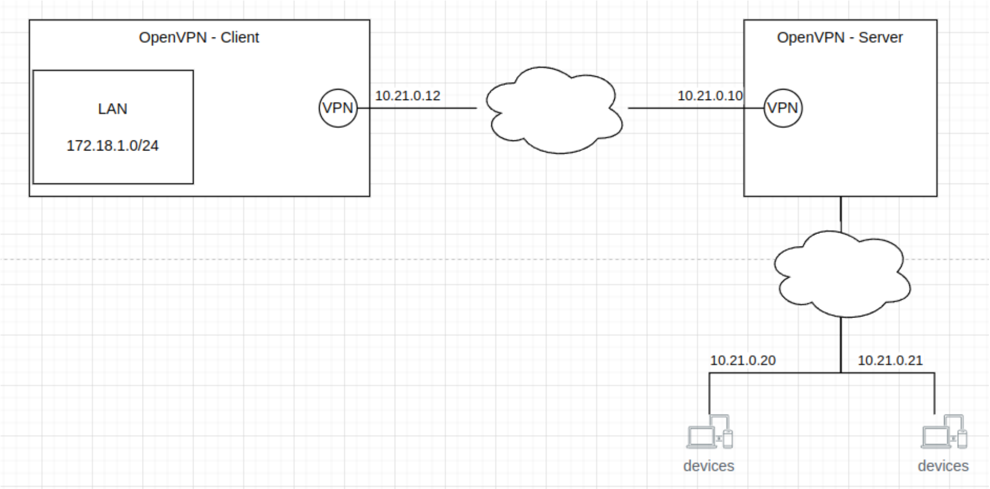


- Routing Mode (client-to-network)



OpenVPN server needs to add one or more static route for the routing.

- DNAT Port Forwarding (client-to-clients)

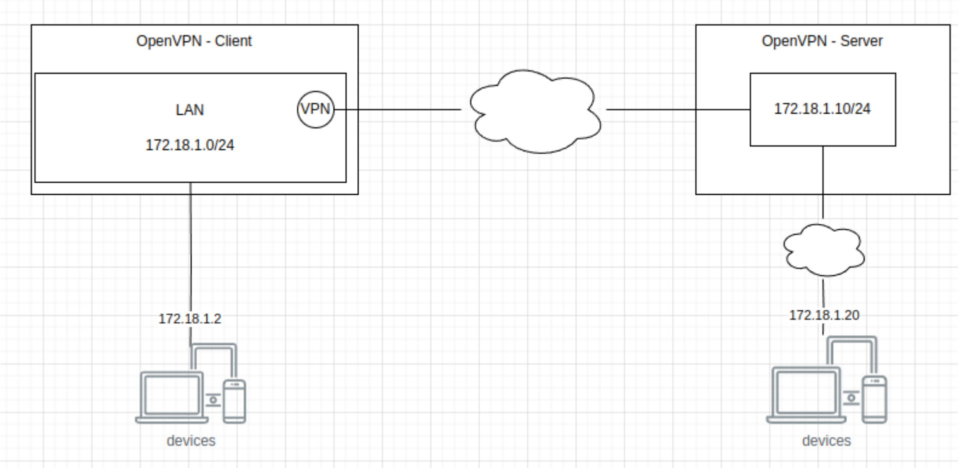


In this scenario, the OpenVPN client is assigned an IP: 10.21.0.12, on the same subnet as the remote devices (10.21.0.20 & 10.21.0.21). So, they can communicate with each other.

When configuring for this application scenario, 'Destination Internal IP' is allocated to the OpenVPN client.

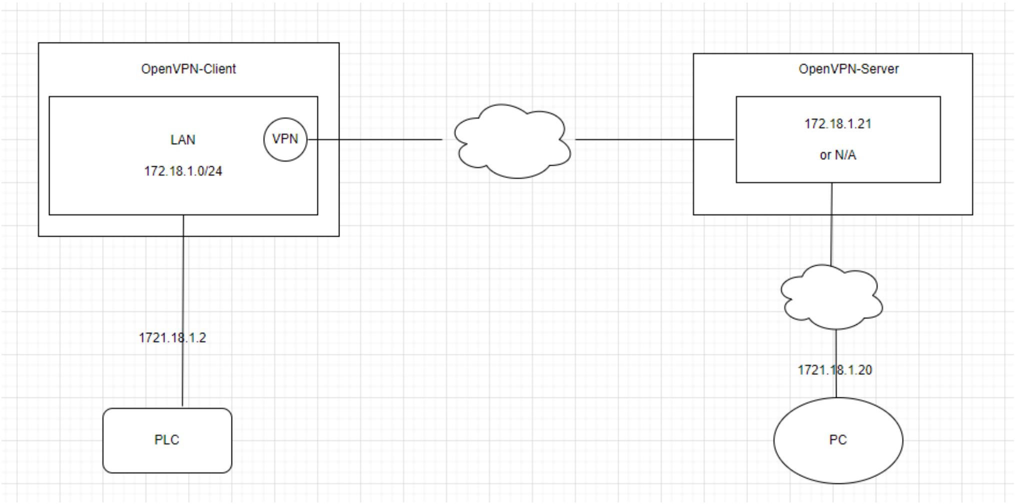
- Bridging Mode (clients-to-clients)

Option 1: IP addresses are assigned by the OpenVPN server



This requires to assign the OpenVPN server an IP in the same subnet as the local LAN, making sure it doesn't clash with any existing device.

Option 2: IP addresses are assigned by the OpenVPN client



In this scenario, (a) OpenVPN client is customized; (b) DHCP should be started after VPN connection is established or a static IP is added to the VPN interface after the connection is established.

3.3.5 Static Route

Static routing is a manual network configuration method where administrators explicitly define paths for traffic through specific network interfaces. This provides precise control over routing behavior, particularly useful for: multi-WAN load balancing, traffic segregation, or backup link configuration.

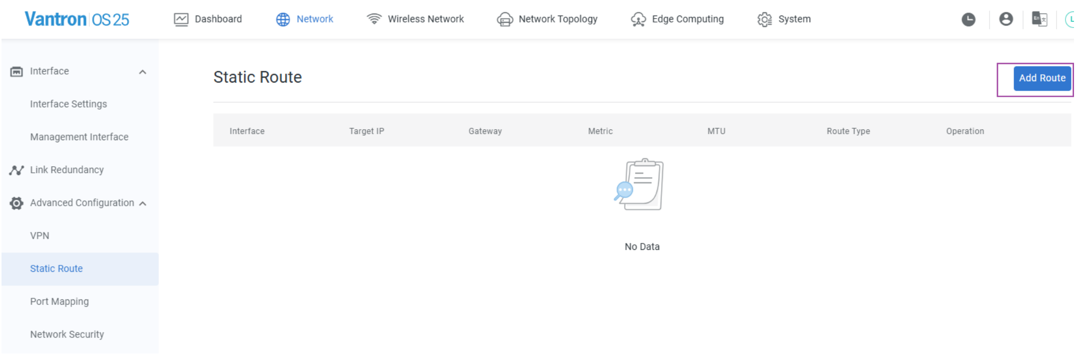
Example:

Scenario: Dual-WAN connection: 1. Ethernet WAN interface; 2. 4G LTE backup interface.

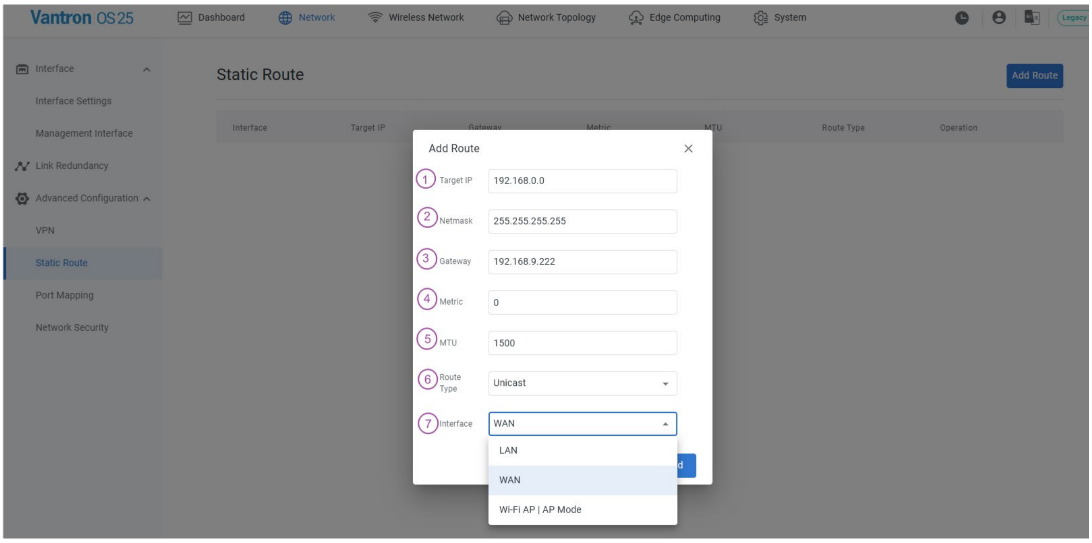
Goal: When the gateway has both 4G and WAN network connection, route the internal network (192.168.0.0 - 192.168.255.254) traffic through WAN interface, and all other data traffic via the 4G interface.

Steps:

1. Click **Add Route** to set a new static route.



2. Configure the rules for the route:



Add Route

1 Target IP: 192.168.0.0
2 Netmask: 255.255.255.255
3 Gateway: 192.168.9.222
4 Metric: 0
5 MTU: 1500
6 Route Type: Unicast
7 Interface: WAN

Description of the numbered areas

1) Input the IP address of the host.

2) Input the subnet mask (e.g., 255.255.255.255).

3) Input the address of the IPv4 gateway.

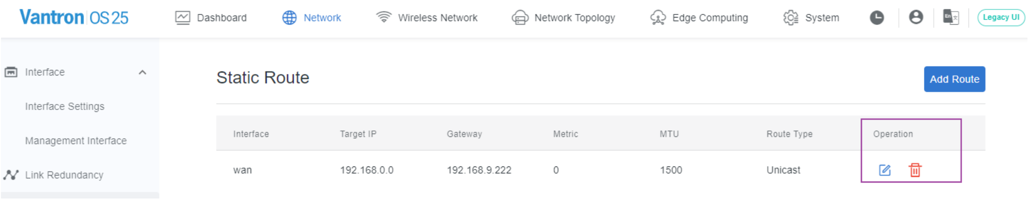
4) Gateway metric (**The smaller the number, the higher the priority**).

5) Set the MTU.

6) Select a route type (refer to the details in the table below).

7) Select an outbound interface for the route (WAN in this case).

3. After creation, you can edit or delete this rule as needed.



Static Route

Interface	Target IP	Gateway	Metric	MTU	Route Type	Operation
wan	192.168.0.0	192.168.9.222	0	1500	Unicast	

Description of the route type:

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

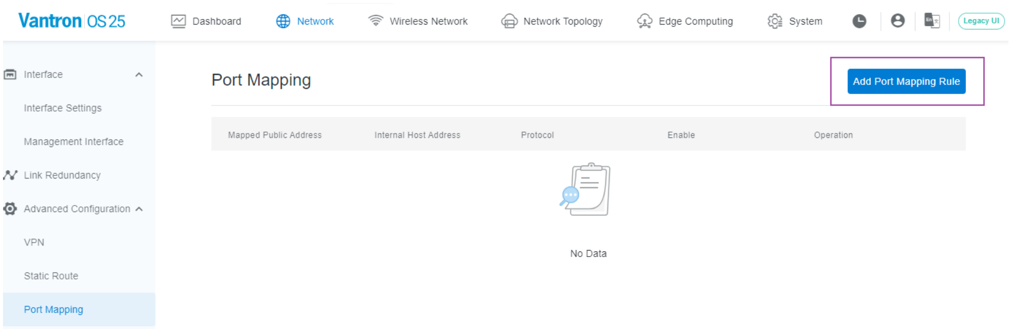
3.3.6 Porting Mapping

Port mapping is a NAT-based technique that redirects traffic arriving on an external **port** combination to a different (internal) **IP:port**—typically from a public address/port on a gateway/firewall to a private address/port inside the LAN. In essence, it “opens a door” so external users can reach services that sit behind NAT without exposing the entire internal network.

To add a port mapping rule, please make sure:

- G202 has both a LAN (internal) and a WAN (external) connection configured, and that NAT is enabled between them.
- Port mapping (Destination NAT) operates based on this NAT boundary.

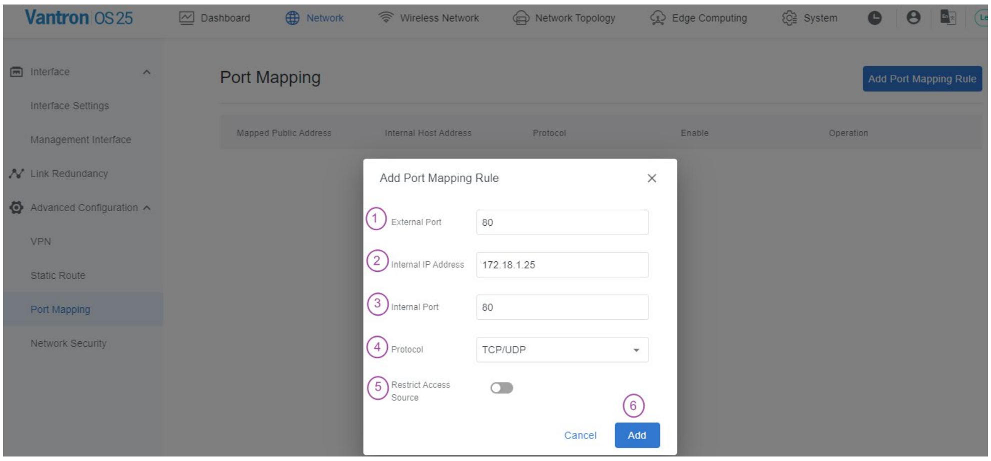
1. Click **Add Port Mapping Rule** in the upper right side.



Port Mapping

Mapped Public Address	Internal Host Address	Protocol	Enable	Operation

2. Fill in the rule information.



Add Port Mapping Rule

1 External Port: 80
2 Internal IP Address: 172.18.1.25
3 Internal Port: 80
4 Protocol: TCP/UDP
5 Restrict Access Source: off

Description of the numbered areas

1) External port – the port outsiders will hit.

2) Internal IP – the LAN address of the target host.

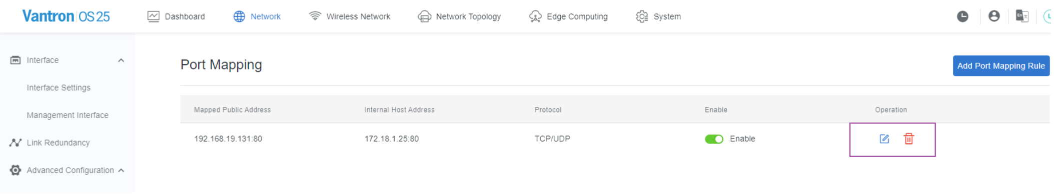
3) Internal port – the port the target host is actually listening on.

4) Protocol – TCP / UDP / both.

5) When **Restrict Access Source** is enabled, only the source IP with corresponding port and MAC you listed are allowed to reach the forwarded port. If **Restrict Access Source** is disabled, any public IP can access the device's IP and forward it to the internal IP.

6) Click **Add** to finish the configuration.

3. The newly created rule is enabled by default, and you can edit or delete this rule as needed.



Port Mapping

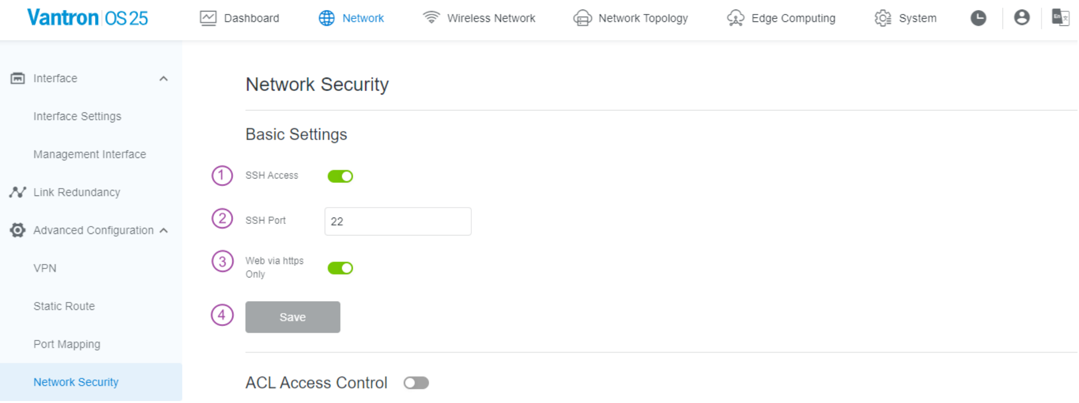
Mapped Public Address	Internal Host Address	Protocol	Enable	Operation
192.168.19.131:80	172.18.1.25:80	TCP/UDP	● Enable	

4. Use another PC connected to a different network to test from outside: telnet <mapped public address> <port number> or using an online port checker.

3.3.7 Network Security

The **Network Security** page provides comprehensive security policy configuration capabilities, enabling granular control over network access behaviors to minimize attack surfaces and enhance overall network protection levels for connected devices.

3.3.7.1 Basic SSH Access Setup



Network Security

Basic Settings

SSH Access ●

SSH Port 22

Web via https Only ●

ACL Access Control ○

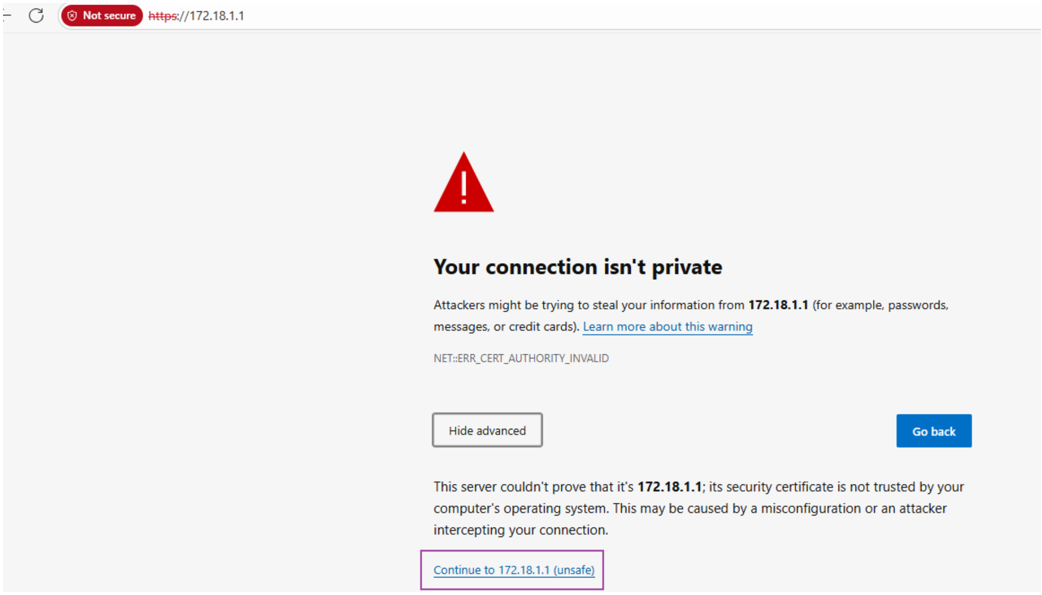
Description of the numbered areas

1. SSH access is enabled by default. You can disable it for security concern.

   Refer to 2.3 for the login method.

2. Default SSH port is 22.

3. Web via HTTPS Only— VantronOS accepts logins only over HTTPS. This is why you may encounter login failure as HTTP attempts are rejected. In this case, click **Advanced** → **Continue** to proceed.



Not secure ~~https~~://172.18.1.1

Your connection isn't private

Attackers might be trying to steal your information from **172.18.1.1** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **172.18.1.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Continue to 172.18.1.1 (unsafe)

4. If you have modified the settings, click **Save** to apply.

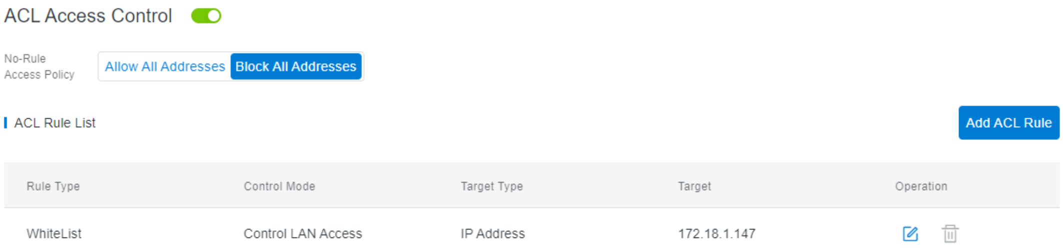
3.3.7.2 ACL Access Control

The device's access control consists of no-rule access policy and ACL rule list.

- **No-Rule Access Policy**

Allow all addresses: All valid IP addresses are allowed to access the device.

Block all addresses: When enabled, this policy **denies all WAN-side access**—only whitelisted IPs can reach the device—and **prevents** LAN-side devices from using it to **reach the WAN**. If no whitelist rules exist at activation, the device automatically adds the host computer's current IP to prevent lock-out. This entry cannot be deleted until at least one additional IP is whitelisted, though the rule itself remains editable.



ACL Access Control

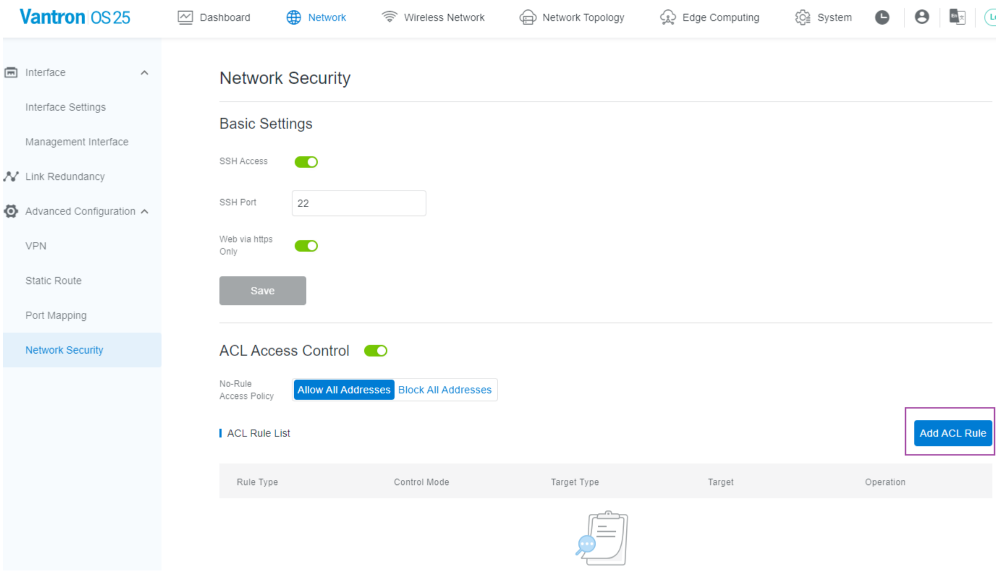
No-Rule Access Policy: Allow All Addresses | Block All Addresses

Rule Type	Control Mode	Target Type	Target	Operation
WhiteList	Control LAN Access	IP Address	172.18.1.147	

- **ACL Rule List**

To add an ACL rule:

1. Click **Add ACL Rule**.



Network Security

Basic Settings

SSH Access: on

SSH Port: 22

Web via https Only: on

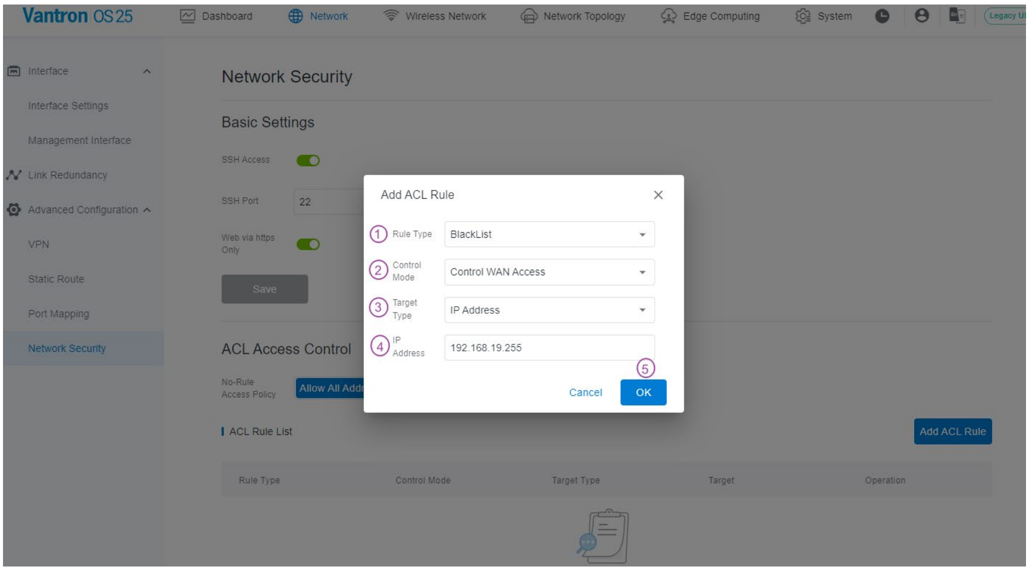
ACL Access Control: on

No-Rule Access Policy: Allow All Addresses | Block All Addresses

ACL Rule List

Rule Type	Control Mode	Target Type	Target	Operation

2. Configure the rule in the pop-up.



Add ACL Rule

Rule Type: BlackList

Control Mode: Control WAN Access

Target Type: IP Address

IP Address: 192.168.19.255

Description of the numbered areas

1) Select a rule type:

Whitelist policy: Listed addresses have the access (typically configured when **Block All Addresses** is enabled).

Blacklist policy: Listed addresses are blocked (typically configured when **Allow All Addresses** is enabled).

2) Select the domain for access control: WAN or LAN.

3) Target type (changes with the domain selected).

Description for the rule settings:

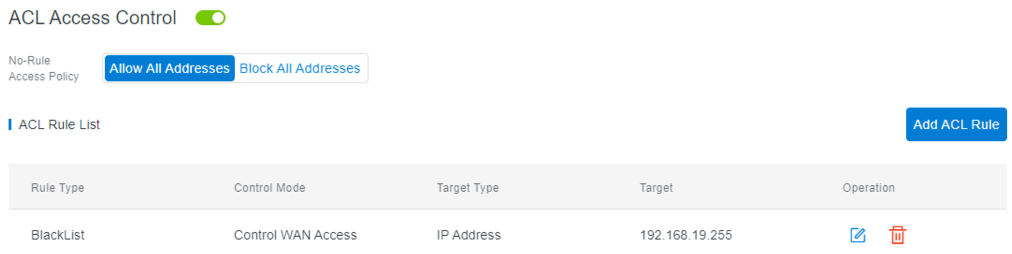
Rule Type	Control Mode	Target Type	Result
Whitelist	WAN	IP address (Source)	The designated WAN IP has access to G202 or its LAN devices.
		Destination IP/ URL/URL keyword	G202 or its LAN devices has access to the designated WAN IP/URL/URL keyword.
	LAN	IP/MAC/OUI	The designated LAN devices are allowed to access the WAN domain.
Blacklist	WAN	IP address (Source)	The designated WAN IP is blocked from accessing G202 or its LAN devices.
		Destination IP/ URL/URL keyword	G202 or its LAN devices has no access to the designated WAN IP/URL/URL keyword.
	LAN	IP/MAC/OUI	The designated LAN devices are blocked from accessing the WAN domain.

Each IP address listed in the table may optionally be followed by a subnet mask to specify a continuous range of IP addresses.

4) Target: the specific content corresponding to the target type.

5) Click **OK** to complete.

3. After configuration, the target is controlled by the rule. You can modify or delete the rule as needed.



Rule Type	Control Mode	Target Type	Target	Operation
BlackList	Control WAN Access	IP Address	192.168.19.255	

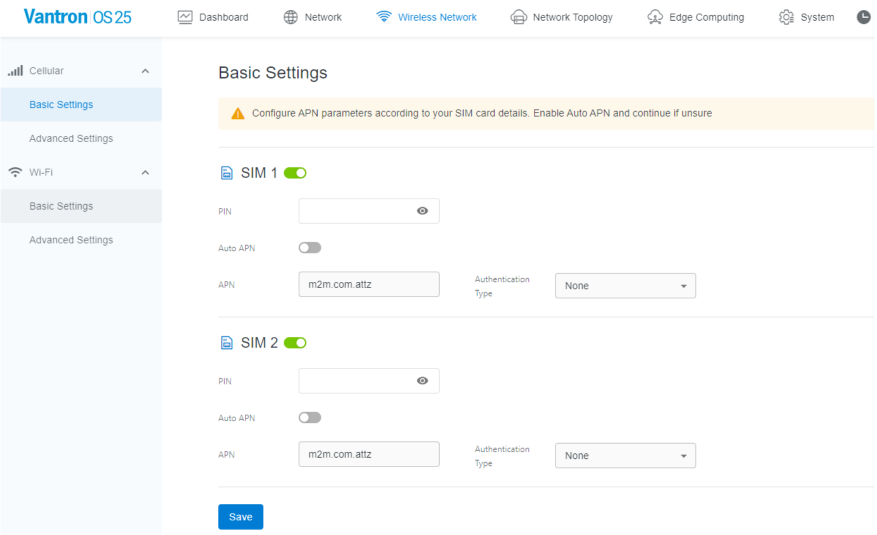
3.4 Wireless Network

Cellular and Wi-Fi related settings are configured on the **Wireless Network** page.

3.4.1 Cellular

Basic SIM card settings include PIN, APN, and Authentication type, which are provisioned by the carrier.

PIN is optional. If you are not sure about the APN and authentication type, you can enable **Auto APN**.



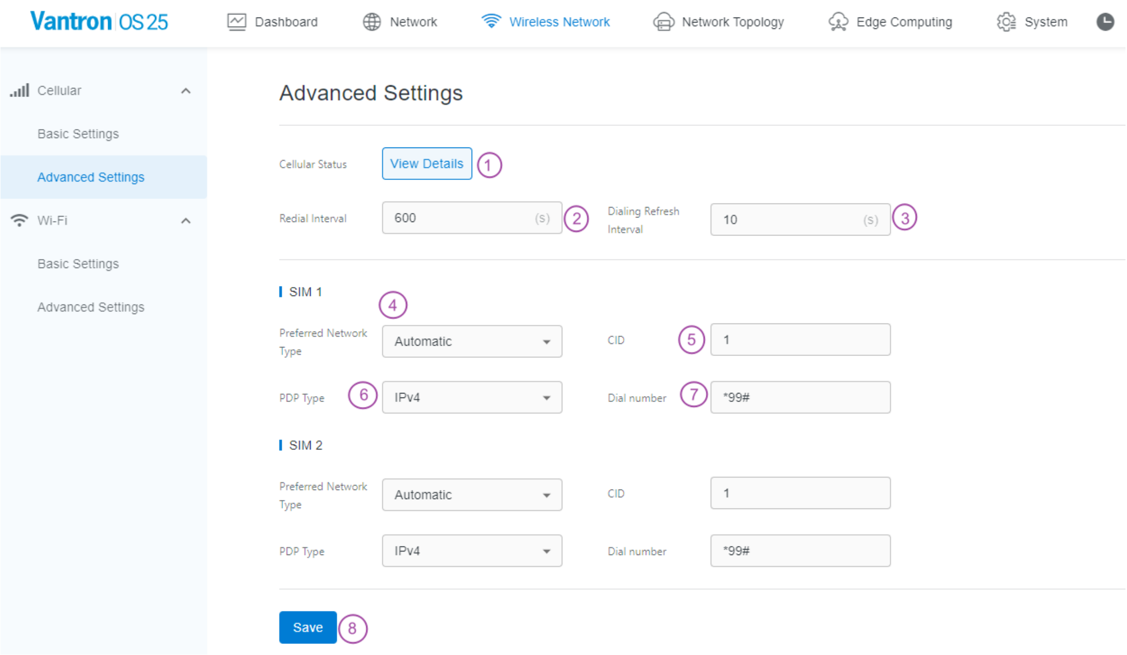
Basic Settings

Configure APN parameters according to your SIM card details. Enable Auto APN and continue if unsure

SIM 1
PIN
Auto APN
APN: m2m.com.attz
Authentication Type: None

SIM 2
PIN
Auto APN
APN: m2m.com.attz
Authentication Type: None

Advanced Settings:



Advanced Settings

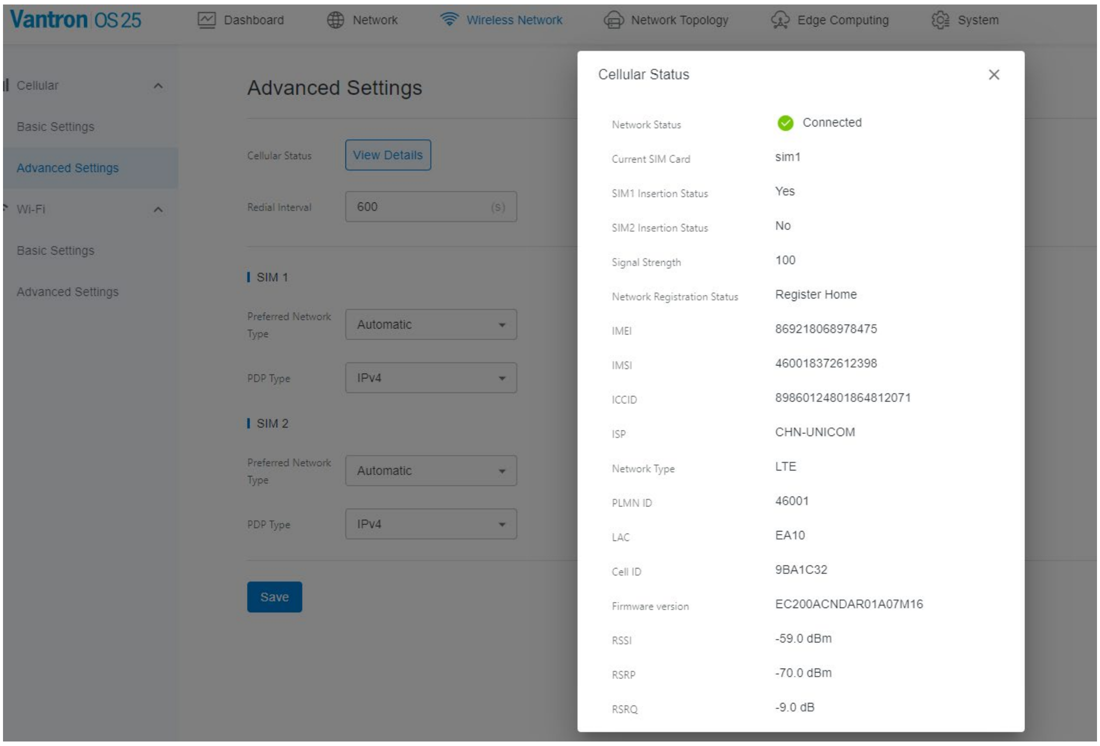
Cellular Status: View Details
Redial Interval: 600 (s)
Dialing Refresh Interval: 10 (s)

SIM 1
Preferred Network Type: Automatic
CID: 1
PDP Type: IPv4
Dial number: *99#

SIM 2
Preferred Network Type: Automatic
CID: 1
PDP Type: IPv4
Dial number: *99#

Description of the numbered areas

1) Cellular Status—Clicking **View Details** will display the detailed cellular information of the device, including SIM insertion status, signal strength, firmware information, etc.



Advanced Settings

Cellular Status: View Details

Redial Interval: 600 (s)

SIM 1

Preferred Network Type: Automatic

PDP Type: IPv4

SIM 2

Preferred Network Type: Automatic

PDP Type: IPv4

Cellular Status

Network Status	✓ Connected
Current SIM Card	sim1
SIM1 Insertion Status	Yes
SIM2 Insertion Status	No
Signal Strength	100
Network Registration Status	Register Home
IMEI	869218068978475
IMSI	460018372612398
ICCID	89860124801864812071
ISP	CHN-UNICOM
Network Type	LTE
PLMN ID	46001
LAC	EA10
Cell ID	9BA1C32
Firmware version	EC200ACNDAR01A07M16
RSSI	-59.0 dBm
RSRP	-70.0 dBm
RSRQ	-9.0 dB

2) Redial interval—Redials at the specified interval in case of a connection failure (in seconds)

3) Dialing Refresh Interval—Specifies the interval (in seconds) to refresh the last dal-up status

The following settings are SIM specific. Be sure to select the SIM in use before editing.

4) Preferred network type—Currently only 'Automatic' is supported.

5) CID value—Cell identity

6) PDP type—Packet data protocol type

7) Dial number—*99# is for general use.

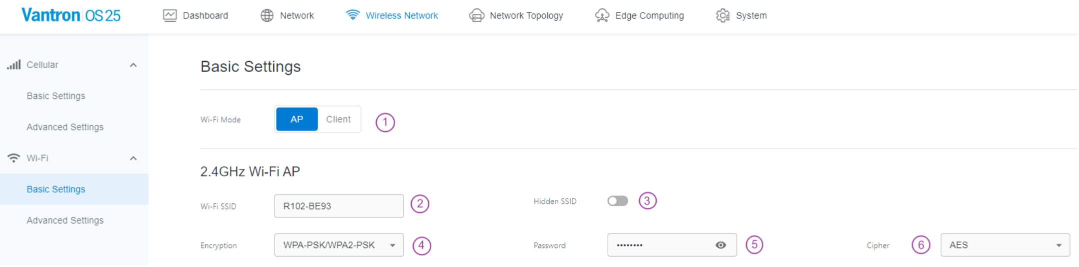
8) If you have made any changes, click **Save** to apply.

Leave the field as-is if not applicable or unsure.

3.4.2 Wi-Fi

During the initial login wizard, the device's Wi-Fi is pre-configured as an access point (AP). Users can modify the configurations as needed.

AP-mode basic settings:



Basic Settings

Wi-Fi Mode: AP | Client

2.4GHz Wi-Fi AP

Wi-Fi SSID: R102-BE93

Hidden SSID

Encryption: WPA-PSK/WPA2-PSK

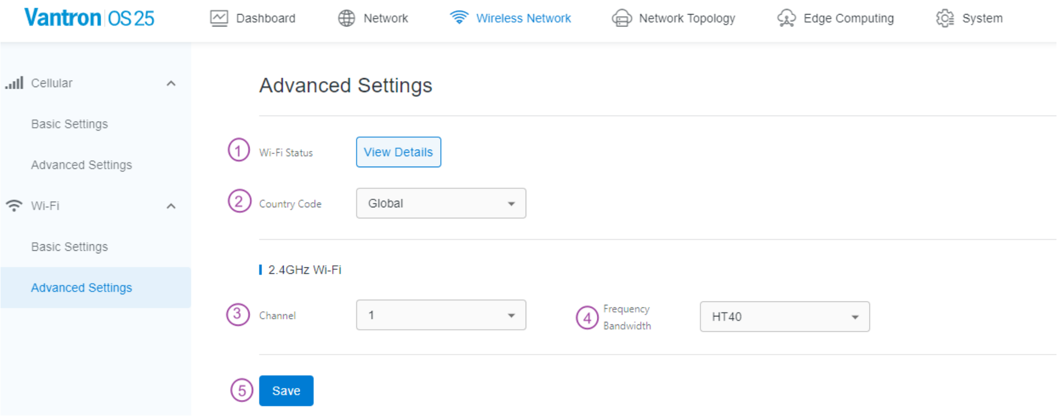
Password: ••••••••

Cipher: AES

Description of the numbered areas

1. Operation mode switch between AP and client: Selected mode is shown in dark blue. A prompt message will display to confirm your operation.
2. Wi-Fi SSID—the Wi-Fi AP's name.
3. Hide the SSID: Once hidden, client devices clients cannot scan the device's SSID and must manually enter the exact name and password to connect.
4. Encryption—The basic protocols for establishing secure communication. (None, WPA-PSK, WPA2-PSK, WPS-PSK/WPA2-PSK)
5. Password—Credential for connecting the device's Wi-Fi.
6. Cypher—The algorithm that performs the encryption & integrity check.

AP-mode advanced settings:



Advanced Settings

Wi-Fi Status

Country Code: Global

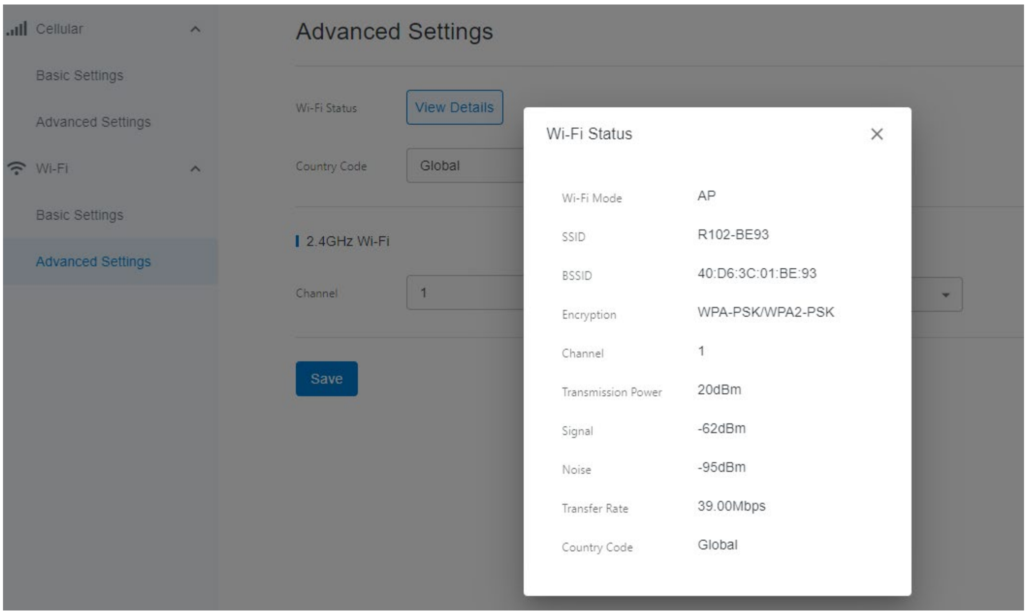
2.4GHz Wi-Fi

Channel: 1

Frequency Bandwidth: HT40

Description of the numbered areas

1. Wi-Fi Status—Clicking **View Details** will display the detailed Wi-Fi settings of the device, including Wi-Fi mode, SSID, encryption, channel, transmit power.



Advanced Settings

Wi-Fi Status

Country Code: Global

2.4GHz Wi-Fi

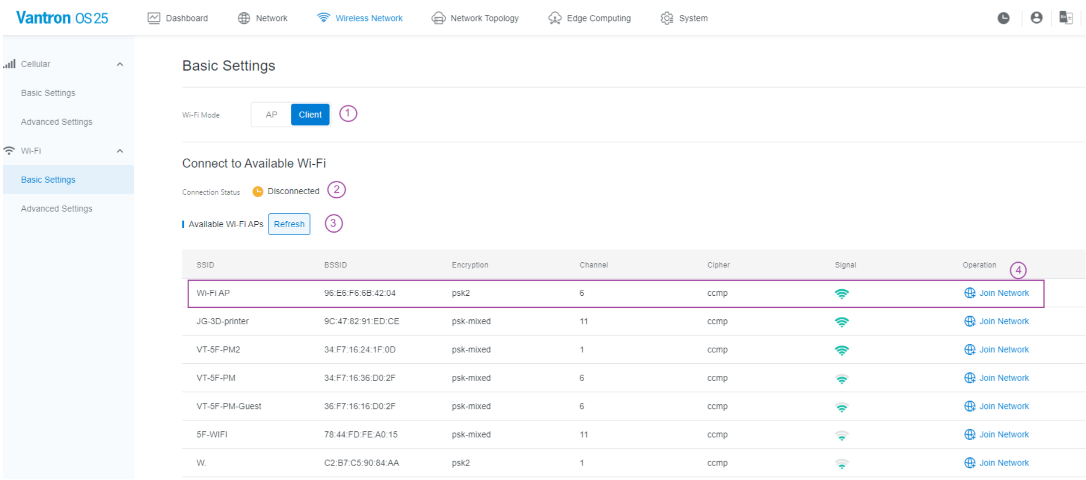
Channel: 1

Wi-Fi Status

Wi-Fi Mode	AP
SSID	R102-BE93
BSSID	40:D6:3C:01:BE:93
Encryption	WPA-PSK/WPA2-PSK
Channel	1
Transmission Power	20dBm
Signal	-62dBm
Noise	-95dBm
Transfer Rate	39.00Mbps
Country Code	Global

2. Country code ('global' by default)
3. Channel options
4. Frequency bandwidth ('HT40' by default)
5. If you have modified the parameters, click **Save** to apply.

Client-mode basic settings:



Basic Settings

Wi-Fi Mode: AP [✓ Client]

Connect to Available Wi-Fi

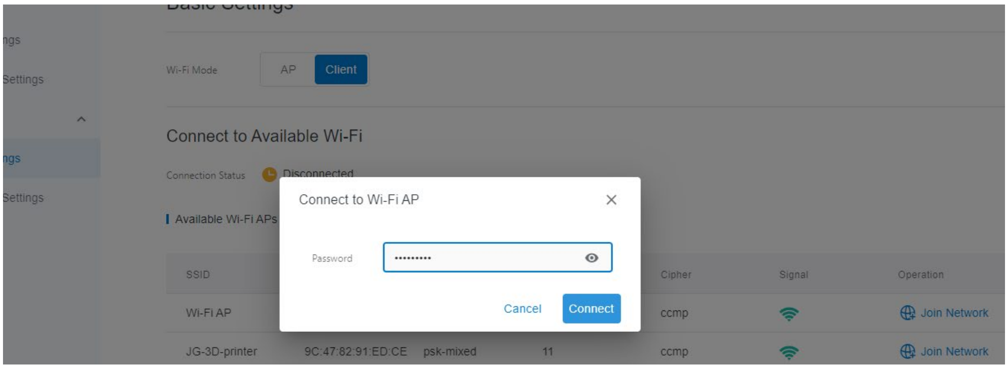
Connection Status: Disconnected

Available Wi-Fi APs Refresh

SSID	BSSID	Encryption	Channel	Cipher	Signal	Operation
Wi-Fi AP	96:E6:F6:6B:42:04	psk2	6	ccmp	📶	Join Network
JG-3D-printer	9C:47:82:91:ED:CE	psk-mixed	11	ccmp	📶	Join Network
VT-5F-PM2	34:F7:16:24:1F:0D	psk-mixed	1	ccmp	📶	Join Network
VT-5F-PM	34:F7:16:36:D0:2F	psk-mixed	6	ccmp	📶	Join Network
VT-5F-PM-Guest	36:F7:16:16:D0:2F	psk-mixed	6	ccmp	📶	Join Network
5F-WIFI	78:44:FD:FE:A0:15	psk-mixed	11	ccmp	📶	Join Network
W.	C2:B7:C5:90:84:AA	psk2	1	ccmp	📶	Join Network

Description of the numbered areas

1. Operation mode switch between AP and client: Selected mode is shown in dark blue. A prompt message will display to confirm your operation.
2. Current connection status.
3. If the target SSID is not included in the list, click to refresh the list.
4. Information of available Wi-Fi APs is displayed. Click **Join Network** and enter the password to connect to it.



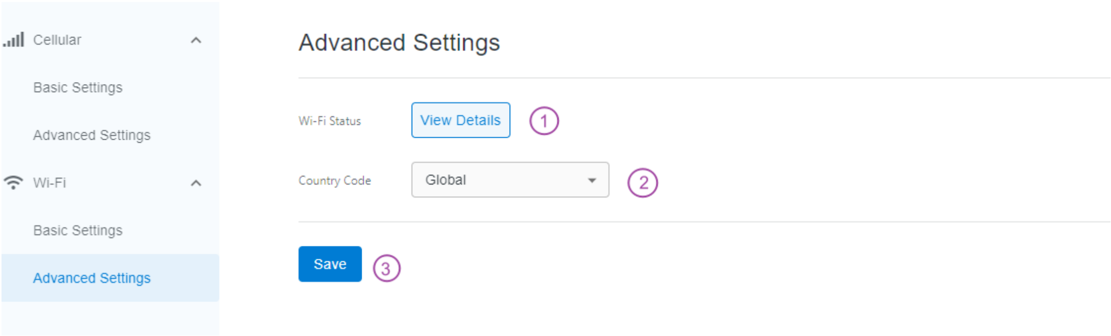
Connect to Wi-Fi AP

Password: ••••••••••

Cancel Connect

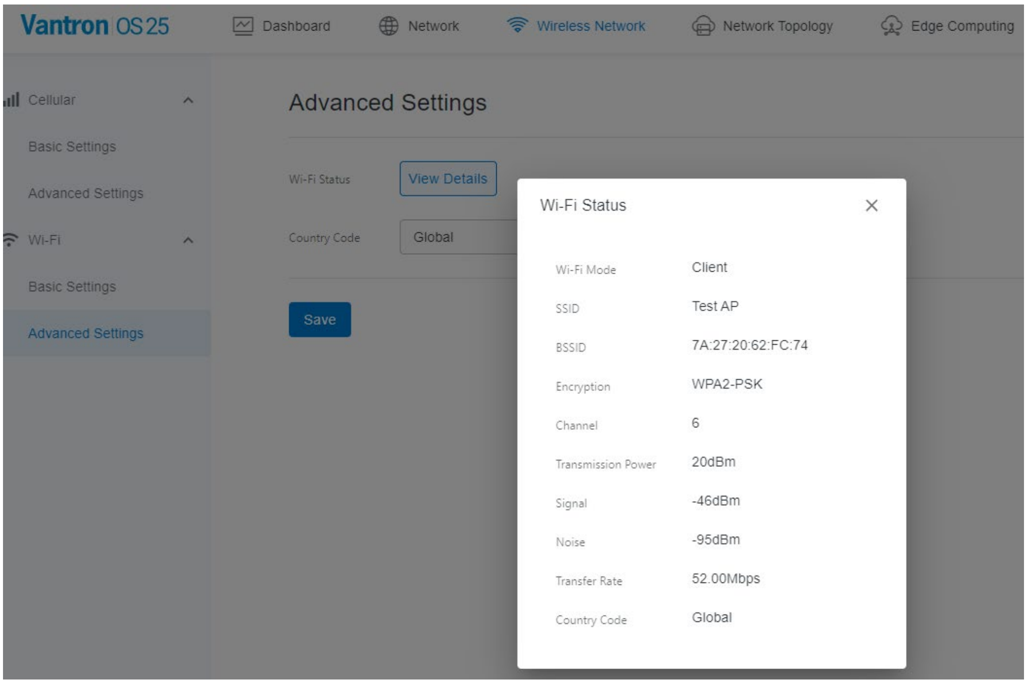
The connection status will change to ***Connected*** *with corresponding SSID upon successful connection.*

Client-mode advanced settings:



Description of the numbered areas

1. Wi-Fi Status—Clicking **View Details** will display the detailed connection information of the device, including Wi-Fi mode, and—if connected—the SSID of the target AP, encryption, channel, transmit power.



Wi-Fi Status

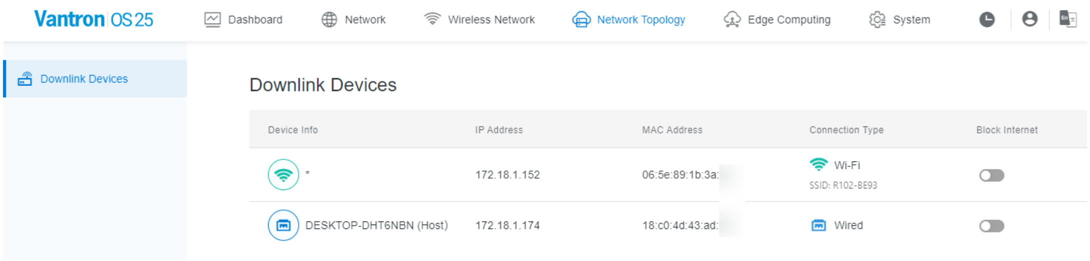
Wi-Fi Mode	Client
SSID	Test AP
BSSID	7A:27:20:62:FC:74
Encryption	WPA2-PSK
Channel	6
Transmission Power	20dBm
Signal	-46dBm
Noise	-95dBm
Transfer Rate	52.00Mbps
Country Code	Global

2. Country code (‘global’ by default)

3. If you have modified the parameters, click **Save** to apply.

3.5 Network Topology

Network topology displays the information of connected clients in the LAN domain (exclusive of PLCs), including the device name, IP address, MAC address, and connection type. Users can manage internet access of such devices by enabling the **Block Internet** option.



Downlink Devices

Device Info	IP Address	MAC Address	Connection Type	Block Internet
*	172.18.1.152	06:5e:89:1b:3a:[redacted]	Wi-Fi SSID: R102-BE93	○
DESKTOP-DHT6NBN (Host)	172.18.1.174	18:c0:4d:43:ad:[redacted]	Wired	○

3.6 Edge Computing

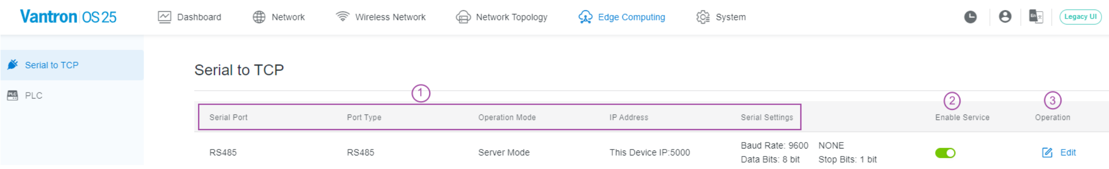
3.6.1 Serial to TCP

Serial-to-TCP transparently converts local serial traffic into Ethernet data, enabling bidirectional remote communication. When using the Serial-to-TCP feature, please make sure:

- The serial parameters (baud rate, data bits, parity, stop bits) on both the serial peripheral and the gateway shall match.
- The server's listening port matches the client's target port.
- Both ends use the same protocol (TCP).
- Server and client are mutually IP-reachable.

A pre-configured conversion rule is provided. Users can modify the rule between server and client modes as needed. Adding or deleting a conversion rule is not supported.

- **Server mode** turns the device's serial port into a TCP listener, allowing remote clients to connect and exchange data.
- **Client mode** makes the device's serial port a TCP client, automatically tunneling all traffic to a specified remote server.



Serial to TCP

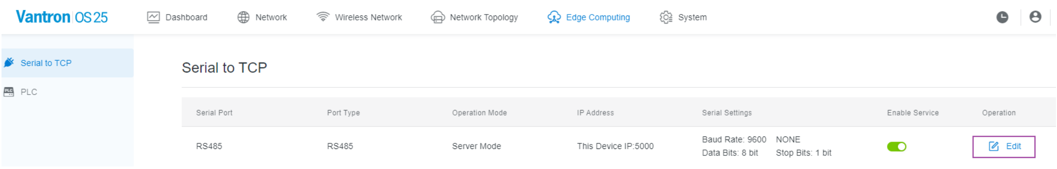
Serial Port	Port Type	Operation Mode	IP Address	Serial Settings	Enable Service	Operation
RS485	RS485	Server Mode	This Device IP:5000	Baud Rate: 9600 NONE Data Bits: 8 bit Stop Bits: 1 bit	●	Edit

Description of the numbered areas

1. Details of the conversion rule, including the serial port name and type, current operation mode, IP address of the device + port, and serial parameters.
2. Enable/disable the rule
3. Edit the rule

3.6.1.1 Server Mode Rule Setup

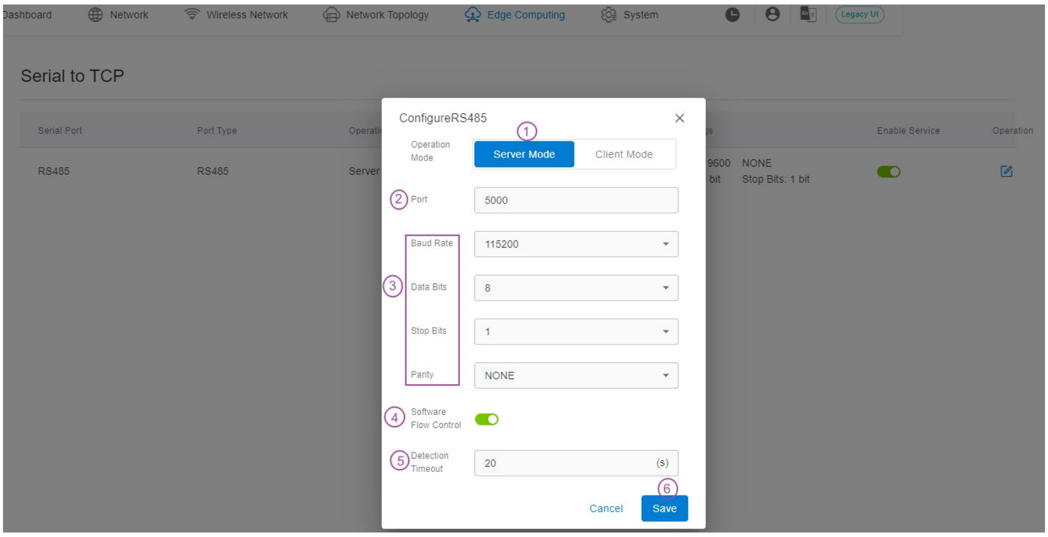
1. Click the edit icon after the rule.



Serial to TCP

Serial Port	Port Type	Operation Mode	IP Address	Serial Settings	Enable Service	Operation
RS485	RS485	Server Mode	This Device IP:5000	Baud Rate: 9600 NONE Data Bits: 8 bit Stop Bits: 1 bit	●	Edit

2. Modify the parameters and make sure they are consistent on both the server and client.



ConfigureRS485

Operation Mode: Server Mode | Client Mode

Port: 5000

Baud Rate: 115200

Data Bits: 8

Stop Bits: 1

Parity: NONE

Software Flow Control: ●

Detection Timeout: 20 (s)

Description of the numbered areas

1) Select **Server Mode.**

2) Designate a TCP port to listen to (0~65535). Make sure the port on both the server and client are the same.

3) Make sure the serial parameters on both the peripheral and gateway are set the same.

4) Enable/Disable software flow control to prevent packet loss (but this reduces throughput).

5) Set the timeout to automatically drop the connection if no data is received (0=disabled).

6) Save the changes to let them take effect.

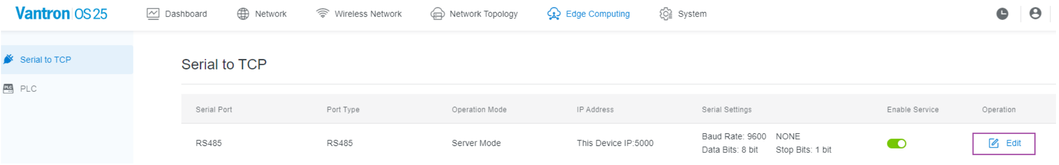
3. Enable the conversion rule.

4. Make sure both the client and server are on the same reachable IP network.

5. Verify the data transmission between the devices.

3.6.1.2 Client Mode Rule Setup

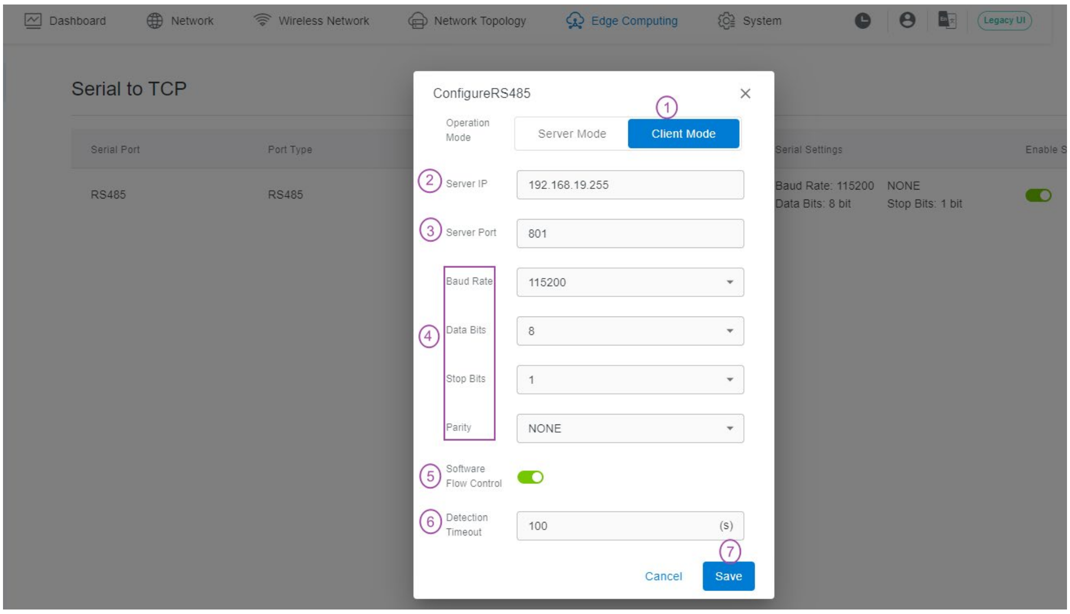
1. Click the edit icon after the rule.



Serial to TCP

Serial Port	Port Type	Operation Mode	IP Address	Serial Settings	Enable Service	Operation
RS485	RS485	Server Mode	This Device IP:5000	Baud Rate: 9600 NONE Data Bits: 8 bit Stop Bits: 1 bit	●	Edit

2. Modify the parameters and make sure they are consistent on both the server and client.



ConfigureRS485

Operation Mode: Client Mode

Server IP: 192.168.19.255

Server Port: 801

Baud Rate: 115200

Data Bits: 8

Stop Bits: 1

Parity: NONE

Software Flow Control: ●

Detection Timeout: 100 (s)

Description of the numbered areas

1) Select **Client Mode.**

2) Enter the IP of the server.

3) Enter the target port and make sure it matches the TCP port on the server.

4) Make sure the serial parameters on both the peripheral and gateway are set the same.

5) Enable/Disable software flow control to prevent packet loss (but this reduces the throughput).

6) Set the timeout to automatically drop the connection if no data is received (0=disabled).

7) Save the changes to let them take effect.

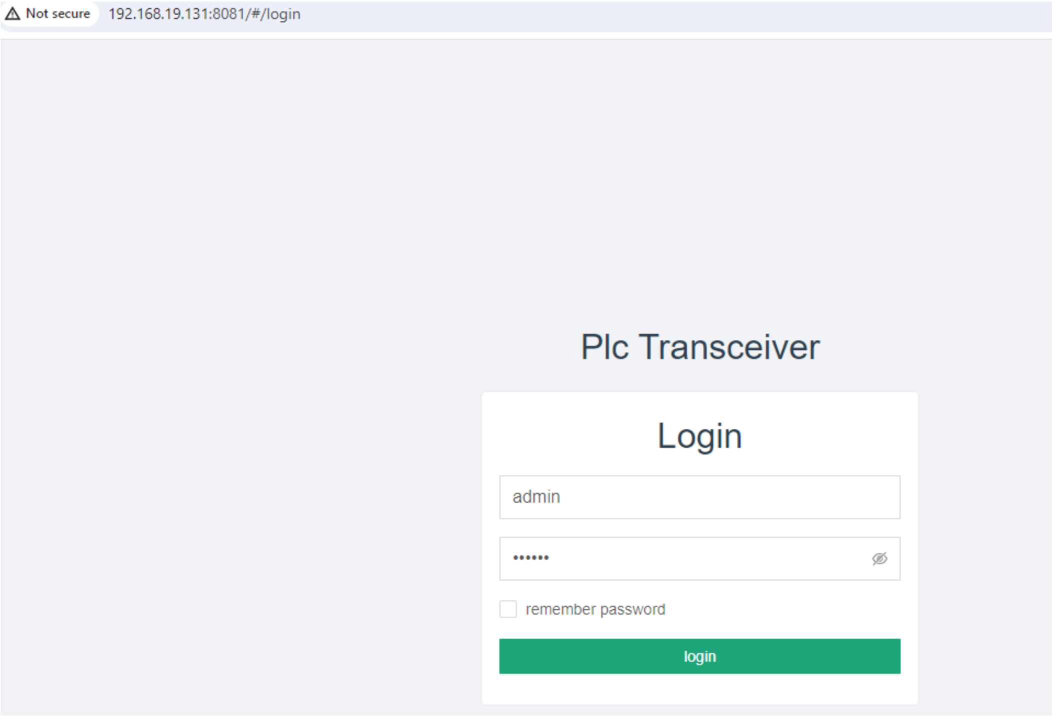
3. Enable the conversion rule.

4. Make sure both the client and server are on the same reachable IP network.

5. Verify the data transmission between the devices.

3.6.2 PLC

The industrial protocol support is an **optional** feature of G202. If this feature is purchased, a PLC **menu** appears under **Edge Computing.** Selecting it launches the industrial protocol configuration portal, where users can fine-tune all gateway- and PLC-specific parameters (e.g., protocol type, station address, register address, data mapping, polling intervals) required for seamless fieldbus integration.



Refer to Chapter 4 for the detailed information.

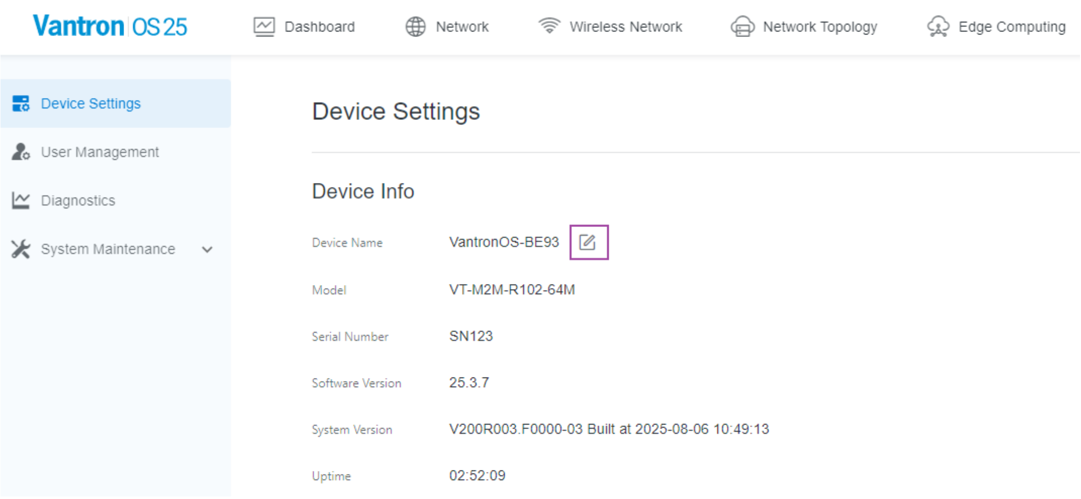
3.7 System

Under **System**, users can view and edit all system-level settings.

3.7.1 Device Settings

3.7.1.1 Modifying Device Name

Device Info display core information—device name, model, serial number, software and system versions, and uptime.



Device Settings

Device Info

Device Name VantronOS-BE93

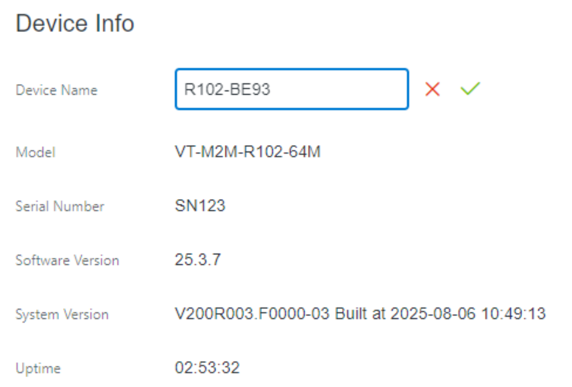
Model VT-M2M-R102-64M

Serial Number SN123

Software Version 25.3.7

System Version V200R003.F0000-03 Built at 2025-08-06 10:49:13

Uptime 02:52:09


Device Info

Device Name R102-BE93

Model VT-M2M-R102-64M

Serial Number SN123

Software Version 25.3.7

System Version V200R003.F0000-03 Built at 2025-08-06 10:49:13

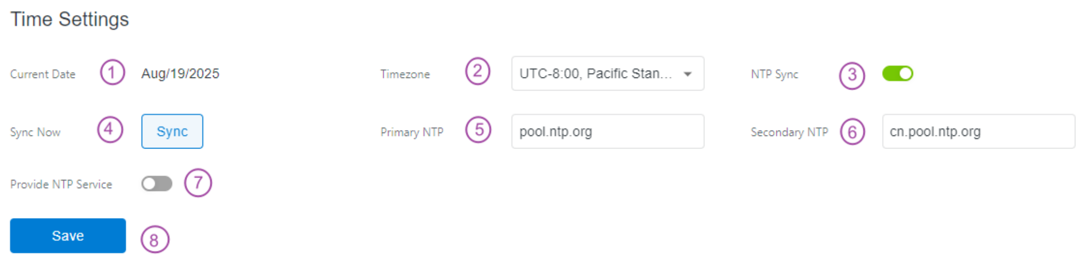
Uptime 02:53:32

To modify the device name:

1. Click the pencil icon next to the device name.
2. Enter a favorable name.
3. Click √ to save the change or ×to cancel.

3.7.1.2 System Time

Time Settings provide system-level time configuration, including current date, current time zone, NTP sync, and NTP servers.



Time Settings

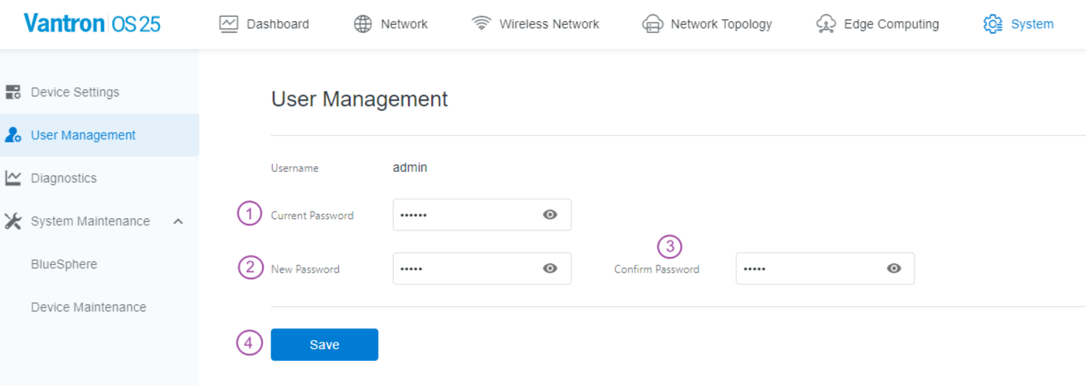
Current Date ① Aug/19/2025
Timezone ② UTC-8:00, Pacific Stan...
NTP Sync ③ ●
Sync Now ④ Sync
Primary NTP ⑤ pool.ntp.org
Secondary NTP ⑥ cn.pool.ntp.org
Provide NTP Service ○ ⑦
Save ⑧

Description of the numbered areas

1. Current Date—Displays today's date for the selected time zone or the host PC's local time (after **Sync Local Time**). The date resets after every power cycle because G202 lacks an RTC.
2. Time Zone—Users can choose the desired time zone from the drop-down list.
3. NTP Sync—Toggle automatic time synchronization with NTP servers.
4. Sync Now—Trigger a one-time NTP update immediately.
5. Primary NTP—Preferred NTP server.
6. Secondary NTP—Backup NTP server.
7. Provide NTP Service—Enable/Disable G202 to act as an NTP server for LAN devices.
8. If you have made any changes, click **Save** to apply.

3.7.2 User Management

User Management allows users to reset the login password without factory resetting the device.



User Management

Username admin
① Current Password ••••••
② New Password •••••
③ Confirm Password •••••
④ Save

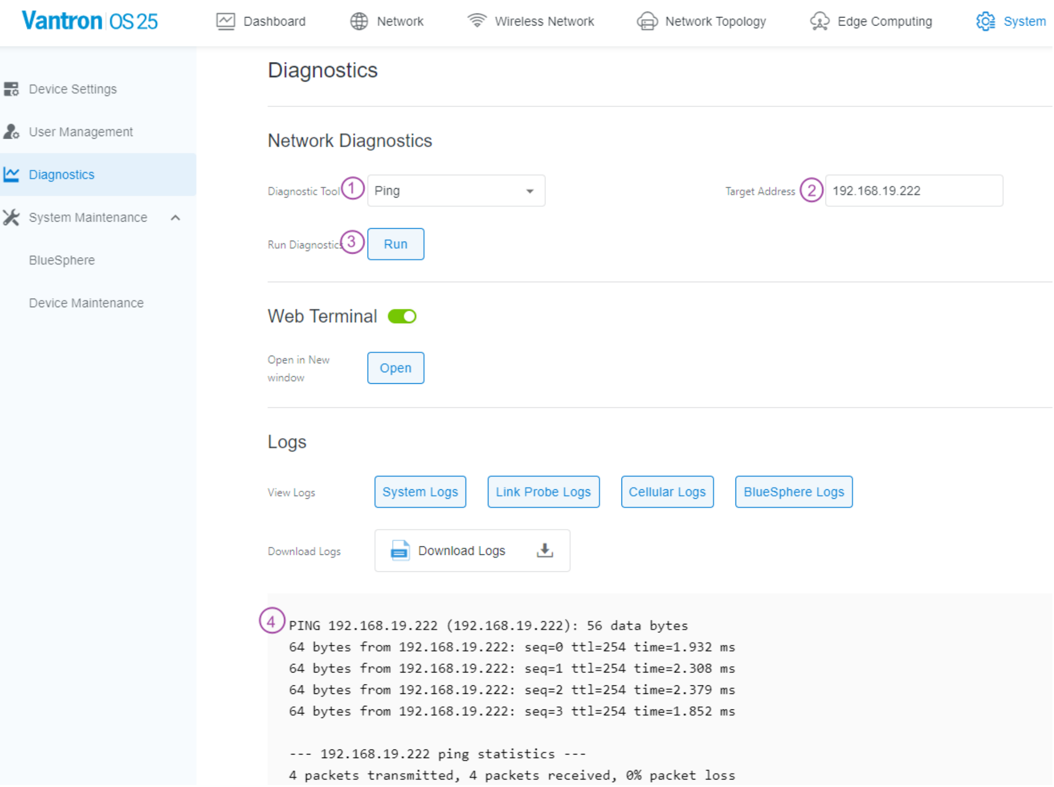
Description of the numbered areas

1. Enter the current password.
2. Enter the new password.
3. Confirm the new password.
4. Save the change.

3.7.3 Diagnostics

On the **Diagnostics** page, users can run network tests, turn on the web terminal for troubleshooting, and view the device log for maintenance or diagnosis purposes.

3.7.3.1 Network Diagnostics



Diagnostic Tool: Ping

Target Address: 192.168.19.222

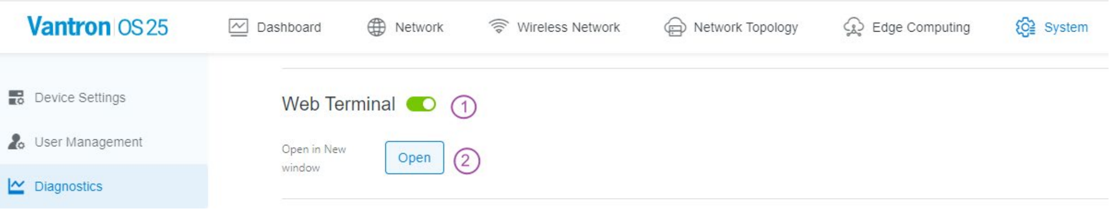
```
PING 192.168.19.222 (192.168.19.222): 56 data bytes
64 bytes from 192.168.19.222: seq=0 ttl=254 time=1.932 ms
64 bytes from 192.168.19.222: seq=1 ttl=254 time=2.308 ms
64 bytes from 192.168.19.222: seq=2 ttl=254 time=2.379 ms
64 bytes from 192.168.19.222: seq=3 ttl=254 time=1.852 ms

--- 192.168.19.222 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
```

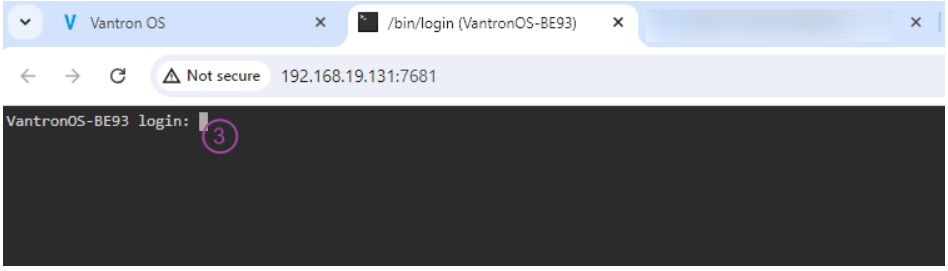
Description of the numbered areas

1. Select a diagnostic tool from the drop-down list.
2. Enter the target address (IP/Domain address).
3. Run the test.
4. The test results are displayed correspondingly.

3.7.3.2 Web Terminal

The **Web Terminal** allows users to toggle the web shell and access the device's shell for debugging.





```
VantronOS-BE93 login:
```

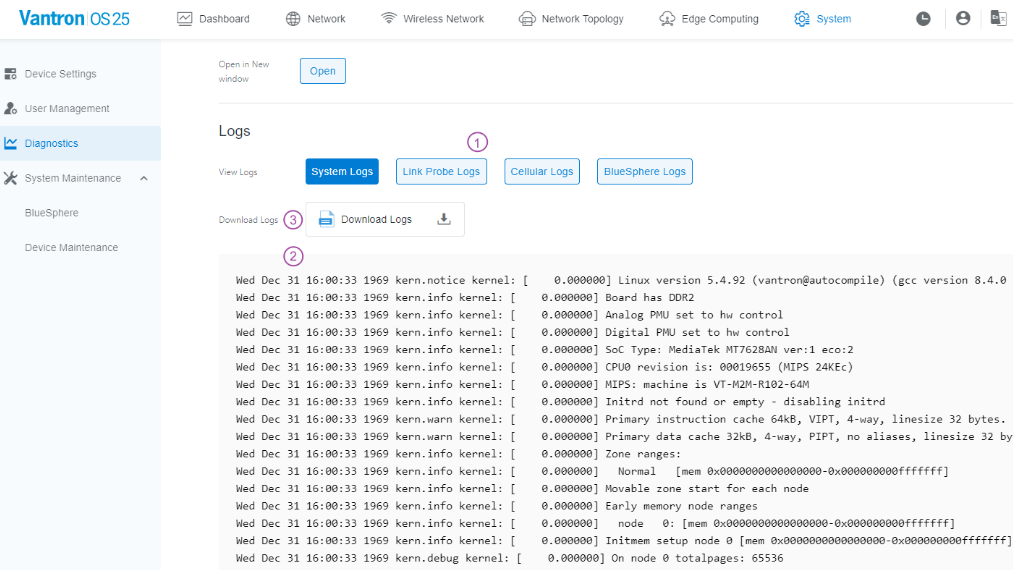
Description of the numbered areas

1. Toggle the web terminal.
2. Click **Open** to launch the device's shell in a new window.
3. Log in within the valid session (60 seconds) to debug the device.

Web terminal login requires root privileges. The root password is unique to each device due to security concern. Please contact the Vantron FAE team to obtain it.

3.7.3.3 Logs

The system offers different device logs for maintenance or troubleshooting.



```
Wed Dec 31 16:00:33 1969 kern.notice kernel: [    0.000000] Linux version 5.4.92 (vantron@autocompile) (gcc version 8.4.0
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] Board has DDR2
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] Analog PMU set to hw control
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] Digital PMU set to hw control
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] SoC Type: MediaTek MT7628AN ver:1 eco:2
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] CPU0 revision is: 00019655 (MIPS 24KEc)
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] MIPS: machine is VT-M2M-R102-64M
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] Initrd not found or empty - disabling initrd
Wed Dec 31 16:00:33 1969 kern.warn kernel: [    0.000000] Primary instruction cache 64kB, VIPT, 4-way, linesize 32 bytes.
Wed Dec 31 16:00:33 1969 kern.warn kernel: [    0.000000] Primary data cache 32kB, 4-way, PIPT, no aliases, linesize 32 by
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] Zone ranges:
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000]   Normal   [mem 0x0000000000000000-0x000000000fffffff]
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] Movable zone start for each node
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] Early memory node ranges
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000]   node   0: [mem 0x0000000000000000-0x000000000fffffff]
Wed Dec 31 16:00:33 1969 kern.info kernel: [    0.000000] Initmem setup node 0 [mem 0x0000000000000000-0x000000000fffffff]
Wed Dec 31 16:00:33 1969 kern.debug kernel: [    0.000000] On node 0 totalpages: 65536
```

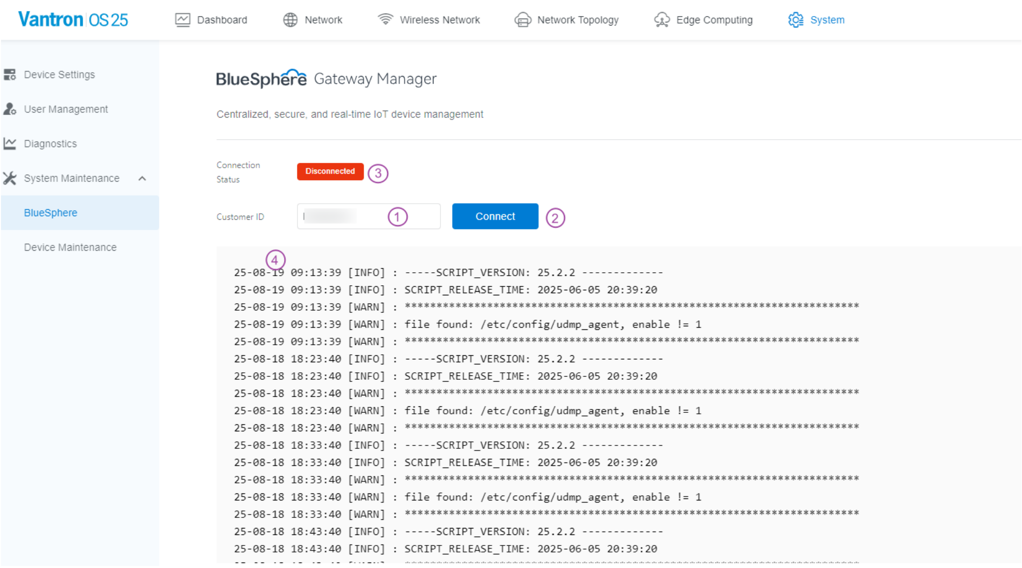
Description of the numbered areas

1. Click on a log tab to initiate log printing.
2. The live log is displayed.
3. Click the **Download Logs** button to export **all** logs.

3.7.4 System Maintenance

3.7.4.1 BlueSphere

If you have an authorized BlueSphere GWM user account, you can add your device to the GWM portal for centralized management.



Centralized, secure, and real-time IoT device management

Connection Status: Disconnected

Customer ID: [redacted]

```
25-08-19 09:13:39 [INFO] : -----SCRIPT_VERSION: 25.2.2 ------------
25-08-19 09:13:39 [INFO] : SCRIPT_RELEASE_TIME: 2025-06-05 20:39:20
25-08-19 09:13:39 [WARN] : ************************************************************************
25-08-19 09:13:39 [WARN] : file found: /etc/config/udmp_agent, enable != 1
25-08-19 09:13:39 [WARN] : ************************************************************************
25-08-18 18:23:40 [INFO] : -----SCRIPT_VERSION: 25.2.2 ------------
25-08-18 18:23:40 [INFO] : SCRIPT_RELEASE_TIME: 2025-06-05 20:39:20
25-08-18 18:23:40 [WARN] : ************************************************************************
25-08-18 18:23:40 [WARN] : file found: /etc/config/udmp_agent, enable != 1
25-08-18 18:23:40 [WARN] : ************************************************************************
25-08-18 18:33:40 [INFO] : -----SCRIPT_VERSION: 25.2.2 ------------
25-08-18 18:33:40 [INFO] : SCRIPT_RELEASE_TIME: 2025-06-05 20:39:20
25-08-18 18:33:40 [WARN] : ************************************************************************
25-08-18 18:33:40 [WARN] : file found: /etc/config/udmp_agent, enable != 1
25-08-18 18:33:40 [WARN] : ************************************************************************
25-08-18 18:43:40 [INFO] : -----SCRIPT_VERSION: 25.2.2 ------------
25-08-18 18:43:40 [INFO] : SCRIPT_RELEASE_TIME: 2025-06-05 20:39:20
```

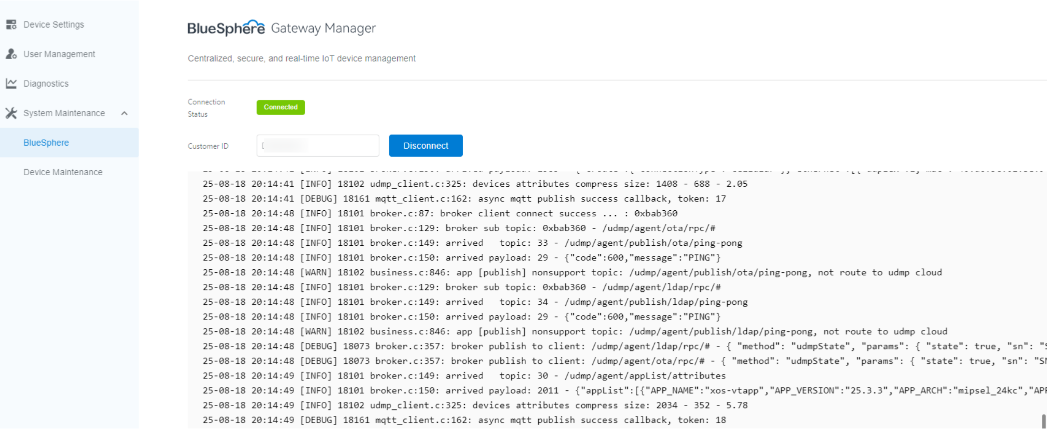
Prerequisite:

G202 must have internet access.

Description of the numbered areas

1. Enter the customer ID that is retrievable in the user profile on the GWM portal.
2. Click **Connect** to initiate the interfacing between the device and the GWM portal.
3. When the handshake succeeds, the device status changes to **Connected**.
4. The real-time log will display the whole connection process.

Here is a screenshot of the device successfully communicating with the GWM portal.



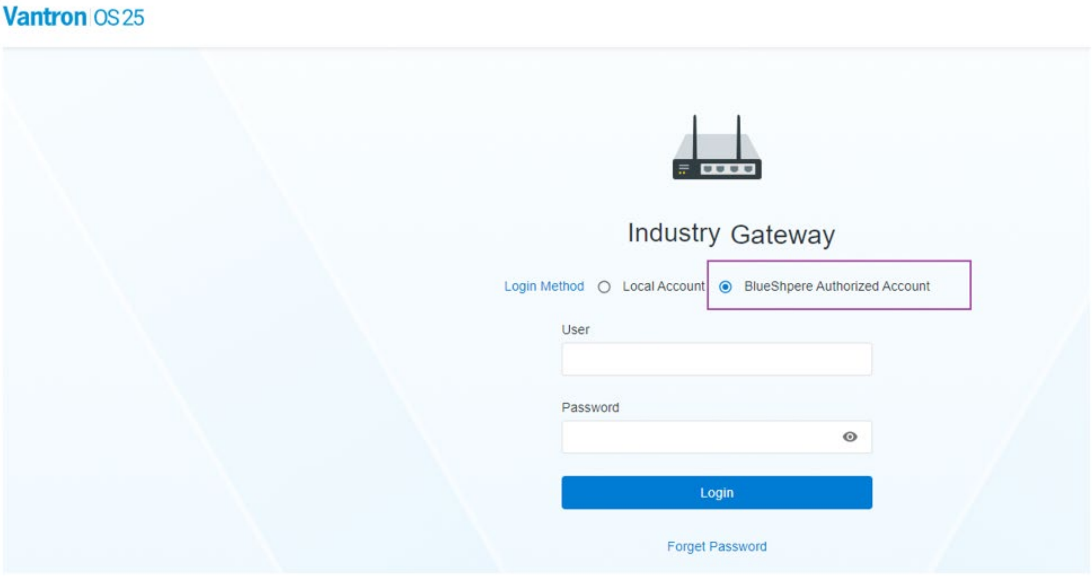
Centralized, secure, and real-time IoT device management

Connection Status: Connected

Customer ID: [redacted]

```
25-08-18 20:14:41 [INFO] 18102 udmp_client.c:325: devices attributes compress size: 1408 - 688 - 2.05
25-08-18 20:14:41 [DEBUG] 18161 mqtt_client.c:162: async mqtt publish success callback, token: 17
25-08-18 20:14:48 [INFO] 18101 broker.c:87: broker client connect success ... : 0xbab360
25-08-18 20:14:48 [INFO] 18101 broker.c:129: broker sub topic: 0xbab360 - /udmp/agent/ota/rpc/#
25-08-18 20:14:48 [INFO] 18101 broker.c:149: arrived   topic: 33 - /udmp/agent/publish/ota/ping-pong
25-08-18 20:14:48 [INFO] 18101 broker.c:150: arrived payload: 29 - {"code":600,"message":"PING"}
25-08-18 20:14:48 [WARN] 18102 business.c:846: app [publish] nonsupport topic: /udmp/agent/publish/ota/ping-pong, not route to udmp cloud
25-08-18 20:14:48 [INFO] 18101 broker.c:129: broker sub topic: 0xbab360 - /udmp/agent/ldap/rpc/#
25-08-18 20:14:48 [INFO] 18101 broker.c:149: arrived   topic: 34 - /udmp/agent/publish/ldap/ping-pong
25-08-18 20:14:48 [INFO] 18101 broker.c:150: arrived payload: 29 - {"code":600,"message":"PING"}
25-08-18 20:14:48 [WARN] 18102 business.c:846: app [publish] nonsupport topic: /udmp/agent/publish/ldap/ping-pong, not route to udmp cloud
25-08-18 20:14:48 [DEBUG] 18073 broker.c:357: broker publish to client: /udmp/agent/ldap/rpc/# - { "method": "udmpState", "params": { "state": true, "sn": "S
25-08-18 20:14:48 [DEBUG] 18073 broker.c:357: broker publish to client: /udmp/agent/ota/rpc/# - { "method": "udmpState", "params": { "state": true, "sn": "SI
25-08-18 20:14:49 [INFO] 18101 broker.c:149: arrived   topic: 30 - /udmp/agent/appList/attributes
25-08-18 20:14:49 [INFO] 18101 broker.c:150: arrived payload: 2011 - {"appList":[{"APP_NAME":"xos-vtapp","APP_VERSION":"25.3.3","APP_ARCH":"mipsel_24kc","APF
25-08-18 20:14:49 [INFO] 18102 udmp_client.c:325: devices attributes compress size: 2034 - 352 - 5.78
25-08-18 20:14:49 [DEBUG] 18161 mqtt_client.c:162: async mqtt publish success callback, token: 18
```

If you log out the portal now, you will find two login methods available. You can sign back in with either your local credentials or an authorized GWM account.



Vantron OS25

Industry Gateway

Login Method ○ Local Account ● BlueShpere Authorized Account

User

Password

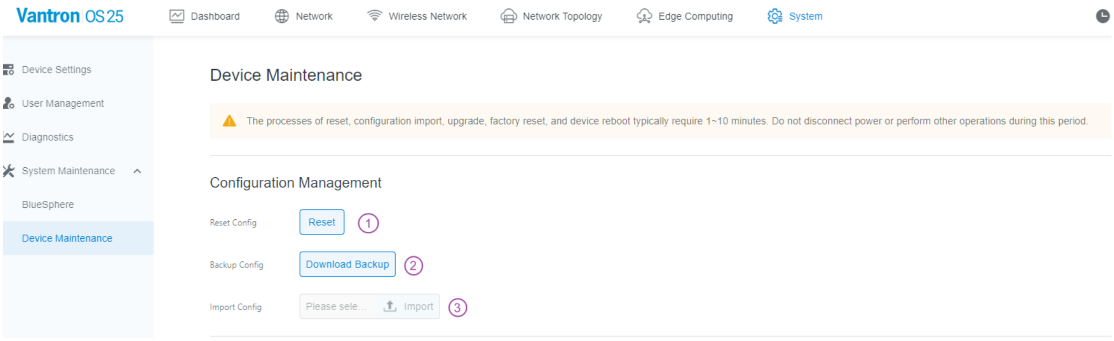
Login

Forget Password

3.7.4.2 Device Maintenance

As indicated on the top of this page, operations including configuration reset, configuration import, upgrade, factory reset, and device reboot typically require 1~10 minutes. Please stay on the page and **keep the device powered on** until the process finishes.

- Configuration Management



Device Maintenance

The processes of reset, configuration import, upgrade, factory reset, and device reboot typically require 1~10 minutes. Do not disconnect power or perform other operations during this period.

Configuration Management

Reset Config: Reset ①

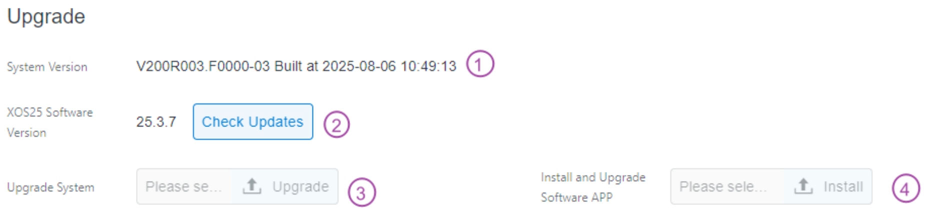
Backup Config: Download Backup ②

Import Config: Please sele... Import ③

Description of the numbered areas

1. Reset the device configuration (this applies to VantronOS25 related applications only).
2. Download the current configuration.
3. Import a configuration file (only configuration file of the same device model is supported).

- Upgrade



Upgrade

System Version V200R003.F0000-03 Built at 2025-08-06 10:49:13

XOS25 Software Version 25.3.7

Description of the numbered areas

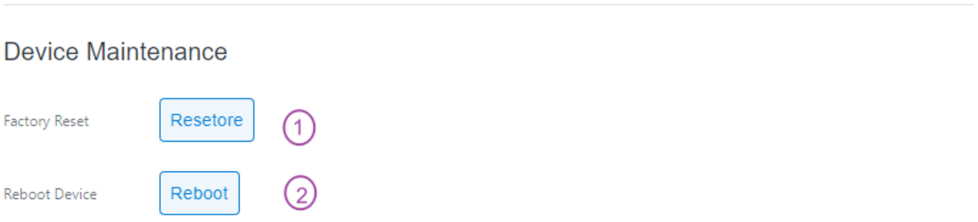
1. Current firmware version.
2. Query the GWM portal for a newer OTA package. If one exists, users can trigger an upgrade; the device will be upgraded to the target version (version selection is not possible).

   The device must already be registered in the GWM portal.
3. Upgrade the firmware manually from a local directory.

   Upgrades are allowed only from an older to a higher version.
4. Install new apps or upgrade existing ones from a local directory.

   Upgrades are allowed only from an older to a higher version.

- Device Maintenance



Device Maintenance

Description of the numbered areas

1. Factory reset the device.
2. Manually restart the device.

CHAPTER 4 INDUSTRIAL PROTOCOLPORTAL

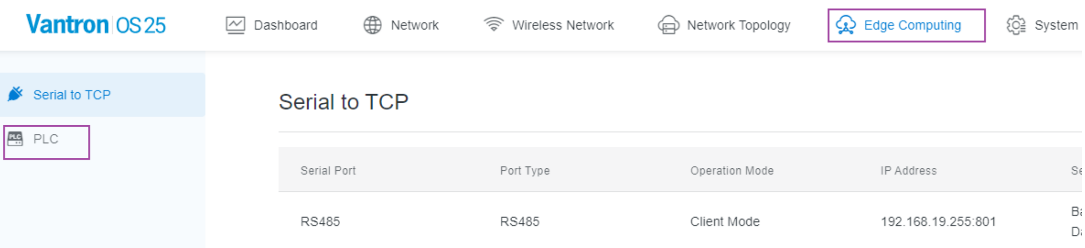
4.1 Overview

Industrial control networks aggregate hundreds of, even thousands of, end points for control and monitoring, often operating in harsh environments—subject to strong electromagnetic interference, mechanical vibration, and extreme outdoor temperatures. Consequently, they impose stringent demands on connectivity and communication, giving rise to numerous proprietary and application-specific protocols.

VantronOS industrial protocol portal supports varied wired industrial protocols, spanning both fieldbus and industrial-Ethernet standards to meet diverse on-site requirements.

4.2 Portal Login

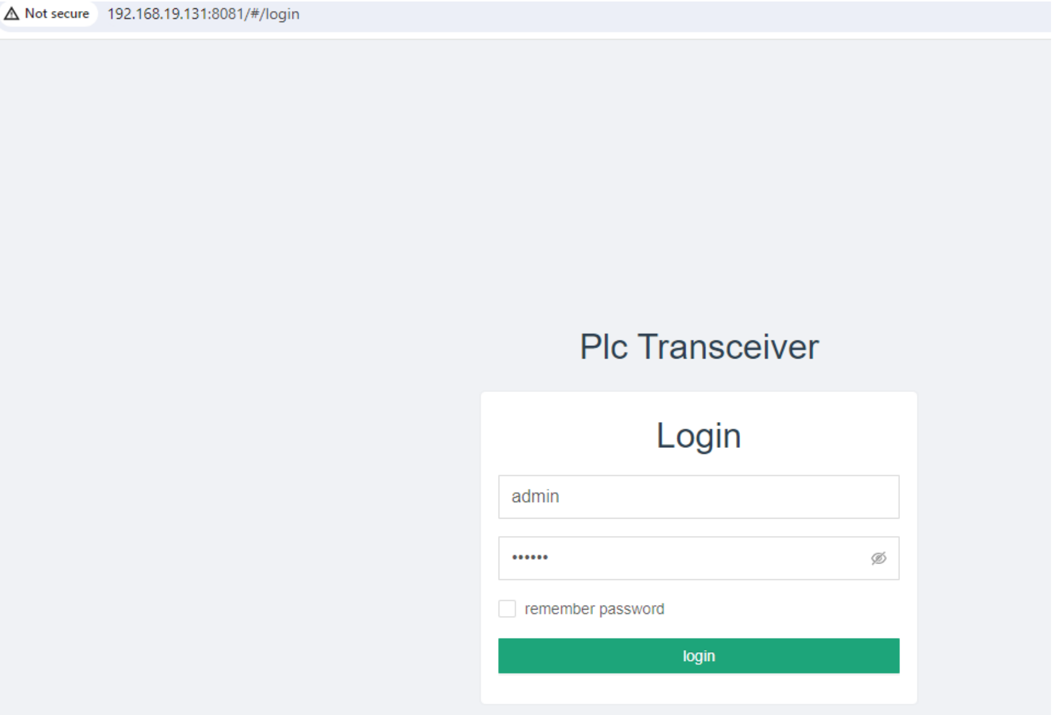
Navigate to **Edge Computing > PLC** in VantronOS.



Serial to TCP

Serial Port	Port Type	Operation Mode	IP Address	Se
RS485	RS485	Client Mode	192.168.19.255:801	Ba Da

Users will be redirected to a new window. Please use your VantronOS credentials to log in.



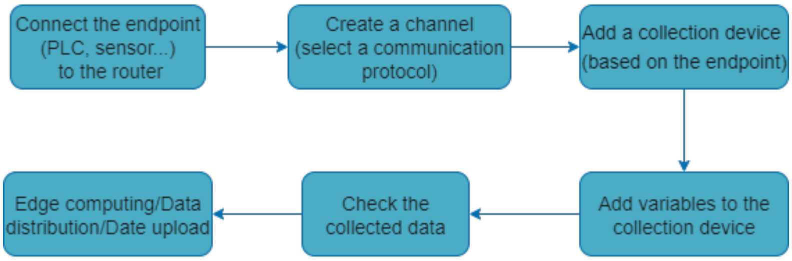
admin

••••••

□ remember password

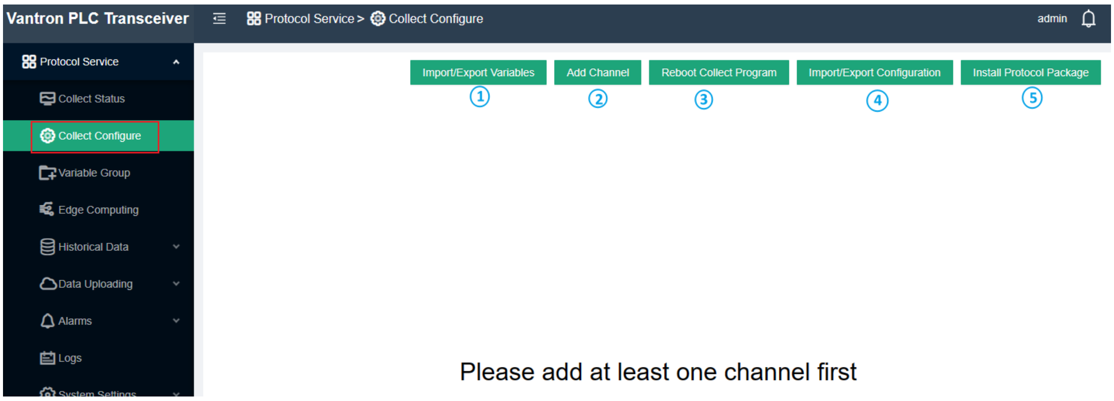
4.3 Protocol Configuration and Application

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. Typical setup procedure is as follows:


Connect the endpoint (PLC, sensor...) to the router
Create a channel (select a communication protocol)
Add a collection device (based on the endpoint)
Add variables to the collection device
Check the collected data
Edge computing/Data distribution/Date upload

4.3.1 Collection Channel Setup

If you are using the portal for the first time, click **Collect Configure** on the menu pane and you will be prompted to add a channel for data collection.



Please add at least one channel first

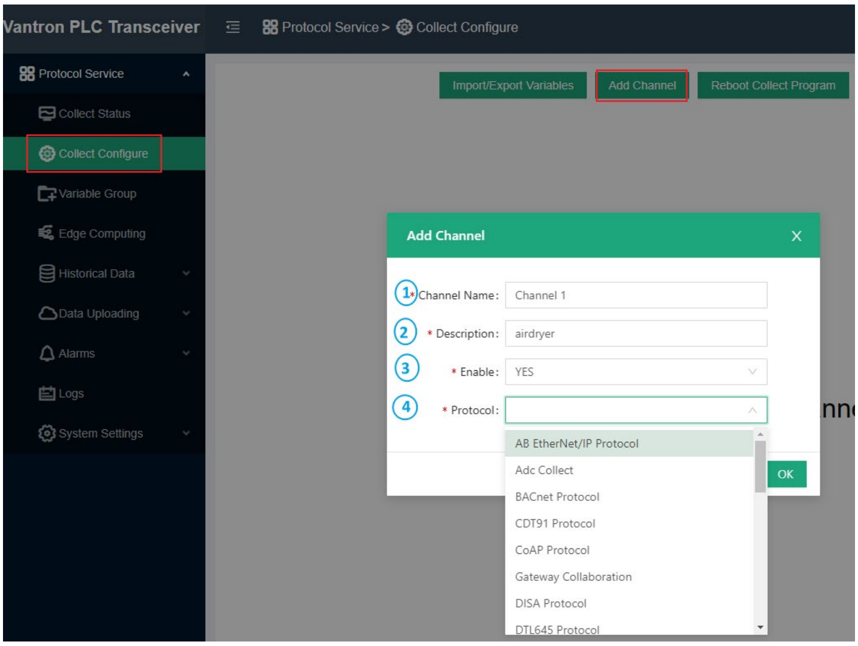
Description of the numbered areas

1. Batch import / export of variables.
2. Create a single collection channel.
3. Restart the collection program (both the collection channel and task will be restarted).
4. Batch import / export of channel configurations.
5. Upload a protocol package—add new protocols or update existing ones.

When creating a channel, users can select to create individual channels (2) one by one or import a CSV configuration file (4) for batch configuration.

○ Create a Single Channel

Click **Add Channel** under the **Collect Configure** menu to add a single channel.



Add Channel

* Channel Name: Channel 1

* Description: airdryer

* Enable: YES

* Protocol:

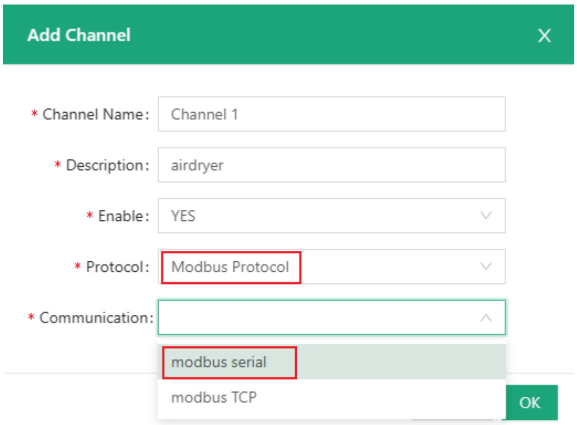
AB EtherNet/IP Protocol
Adc Collect
BACnet Protocol
CDT91 Protocol
CoAP Protocol
Gateway Collaboration
DISA Protocol
DTL645 Protocol

Description of the numbered areas

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

Certain protocols may require more configuration parameters.

Take Modbus Protocol as example, when "modbus serial" is selected, ensure the endpoint is connected to the gateway via a serial port.



Add Channel

* Channel Name: Channel 1

* Description: airdryer

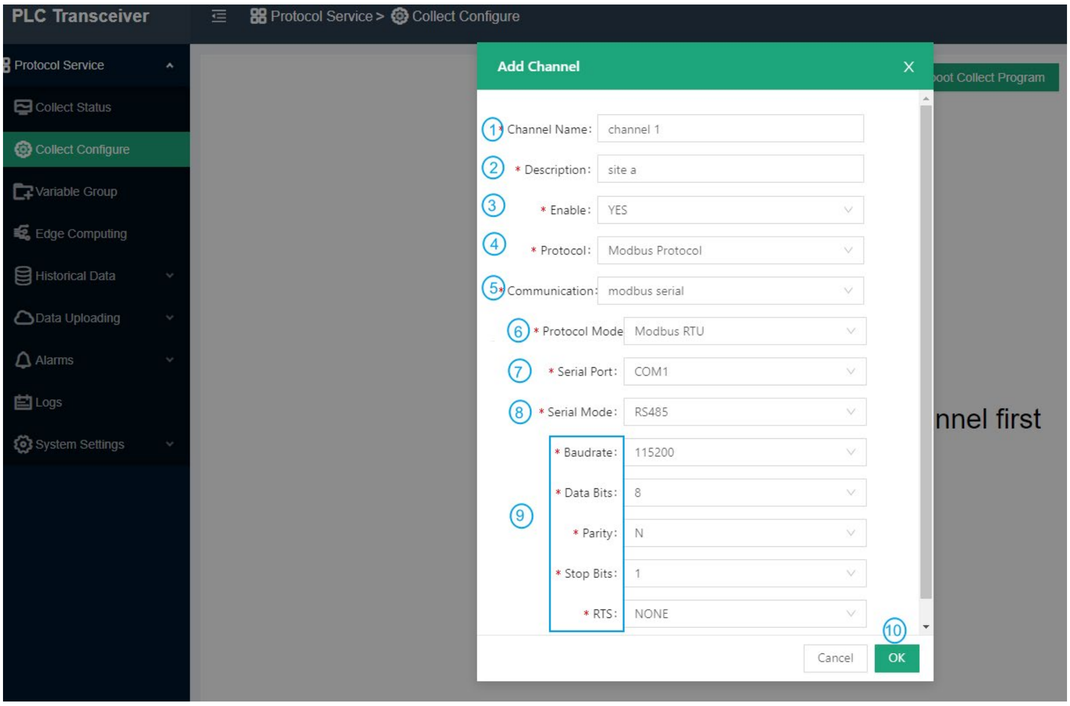
* Enable: YES

* Protocol: Modbus Protocol

* Communication:

modbus serial
modbus TCP

To further configure the protocol:



Add Channel

Channel Name: channel 1
* Description: site a
* Enable: YES
* Protocol: Modbus Protocol
* Communication: modbus serial
* Protocol Mode Modbus RTU
* Serial Port: COM1
* Serial Mode: RS485
* Baudrate: 115200
* Data Bits: 8
* Parity: N
* Stop Bits: 1
* RTS: NONE

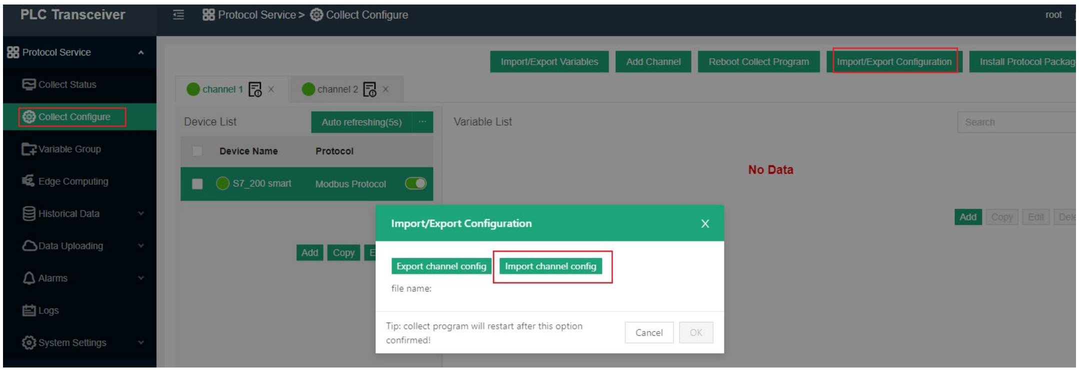
Cancel OK

Description of the numbered areas

4. Select **Modbus protocol** from the drop-down list.
5. Choose **modbus serial** as the communication type.
6. Select **Modbus RTU/Modbus ASCII** as the protocol mode (Modbus RTU for illustration).
7. Select the correct serial port from the drop-down list that corresponds to the serial port in use on the gateway.
8. Determine the mode of the serial port (the serial mode is determined by the serial port in use).
9. Fill in the serial parameters of the serial endpoint connected to the gateway.
10. Click **OK** to complete the channel configuration.

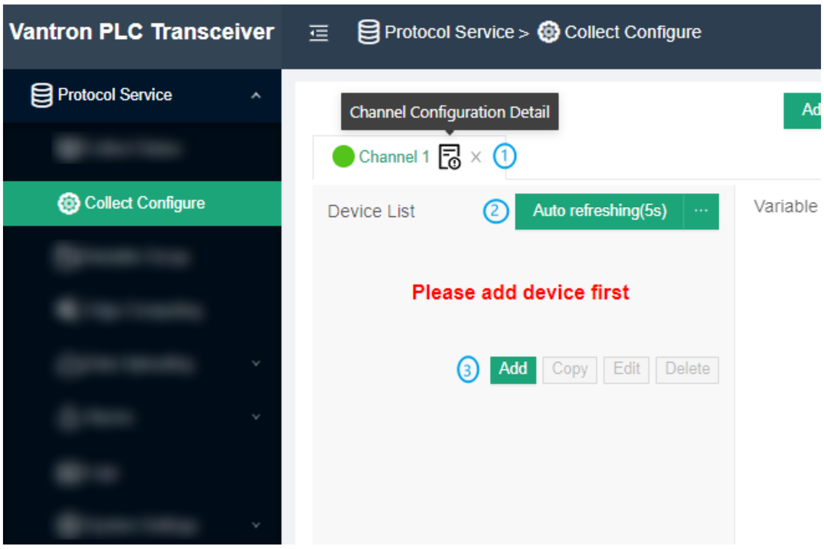
- **Batch Import of Channel Configurations**

To import the channel configurations in bulk, users can click **Import/Export Configuration** under the **Collect Configure** menu, then select **Import channel config**.



Tip: collect program will restart after this option confirmed!

After the configuration, the channel will display on the portal. You can make subsequent changes like deleting or editing the channel.

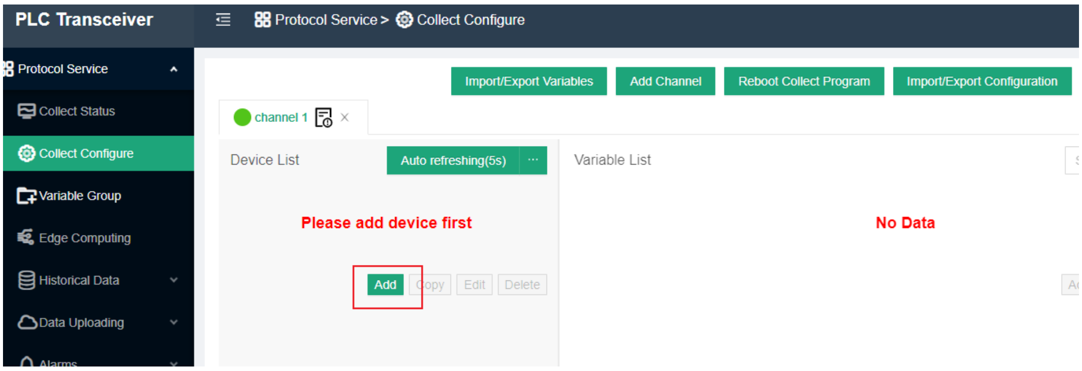


Description of the numbered areas

1. Delete the channel (x) 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 by clicking the (…) button.
3. Add a device (e.g., a PLC/sensor) for data collection.

4.3.2 Device Setup

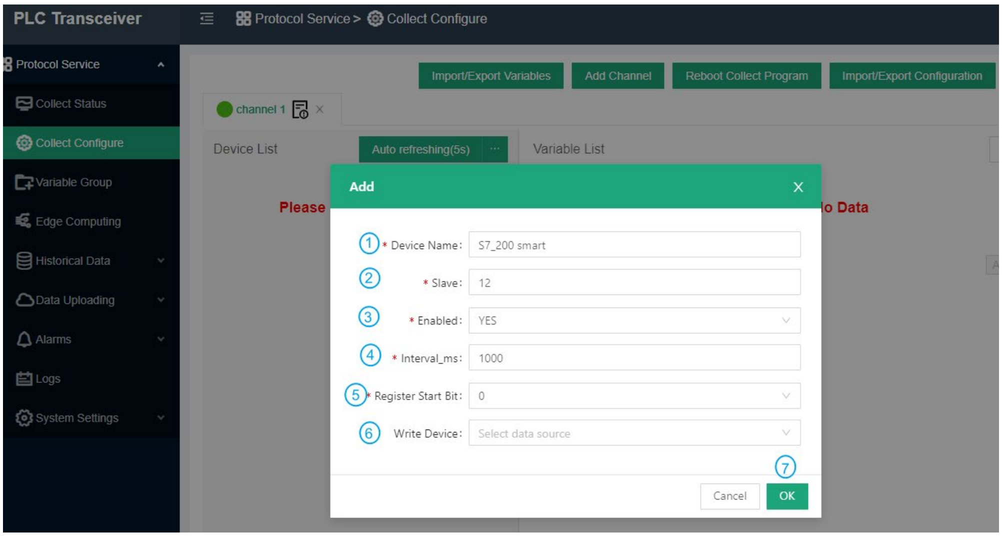
After creating a channel, the data collection endpoint that connects to the gateway can be added to the channel. Click the **Add** button under **Device List** and input the device information in the pop-up.



Please add device first

No Data

The device information to be input varies with the protocol you added for communication (still taking Modbus RTU protocol as example).



* Device Name: S7_200 smart
* Slave: 12
* Enabled: YES
* Interval_ms: 1000
* Register Start Bit: 0
Write Device: Select data source

Description of the numbered areas

1. Enter a device name.
2. Input a slave address between 0 and 255.
3. Choose to enable the device or not.
4. Set an interval for data collection (you can leave it as-is).
5. Set a start bit for the register.
6. Select the data source for distribution (unless there is collected data).
7. Click **OK** to complete adding the device.

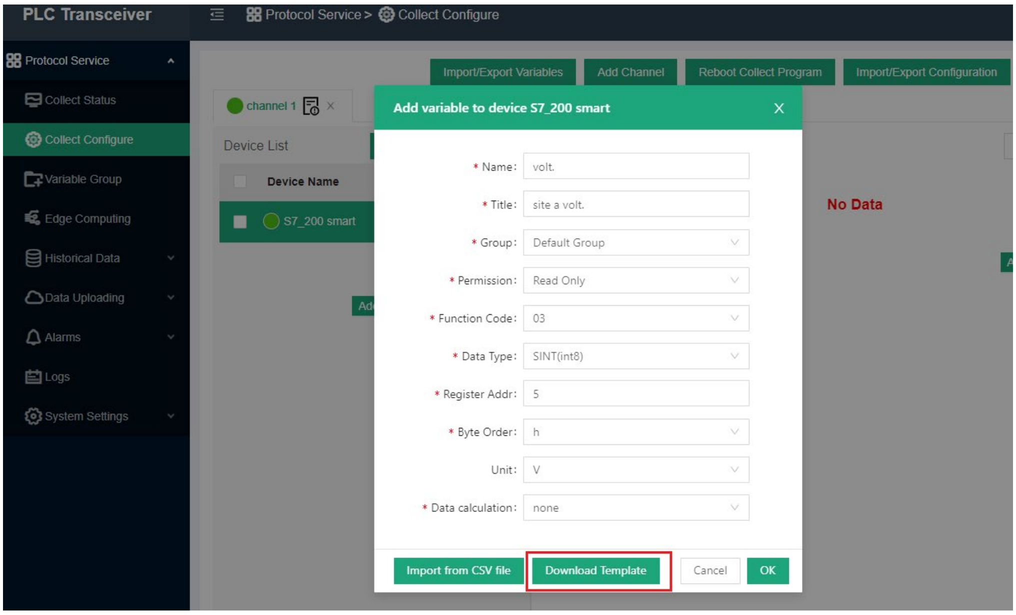
4.3.3 Variable Setup

After configuring the endpoint, users can choose to batch import the variables or configure individual variables one by one.

○ **Batch Import**

The **Import/Export Variables** tab under the **Collect Configure** menu allows users to import or export variables in bulk. For the **first** bulk import, you can download the template as a reference and edit the fields as needed for batch import.

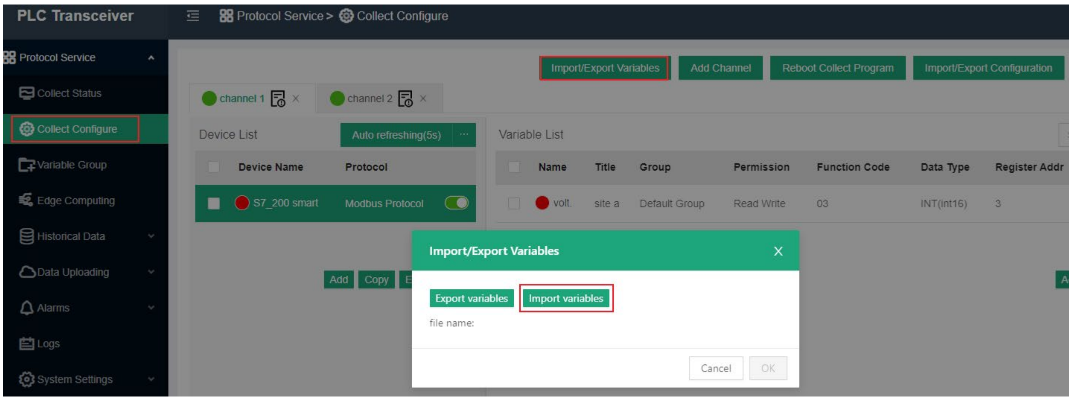
The **Download Template** option appears only when no variables have been configured yet as shown below. Once variables exist, an **export variables** option replaces it.



Add variable to device S7_200 smart

* Name: volt.
* Title: site a volt.
* Group: Default Group
* Permission: Read Only
* Function Code: 03
* Data Type: SINT(int8)
* Register Addr: 5
* Byte Order: h
Unit: V
* Data calculation: none

For non-first bulk import, you can directly click the **Import/Export Variables** tab under the **Collect Configure** menu, then select **Import variables**.



Device List

Device Name	Protocol
S7_200 smart	Modbus Protocol

Variable List

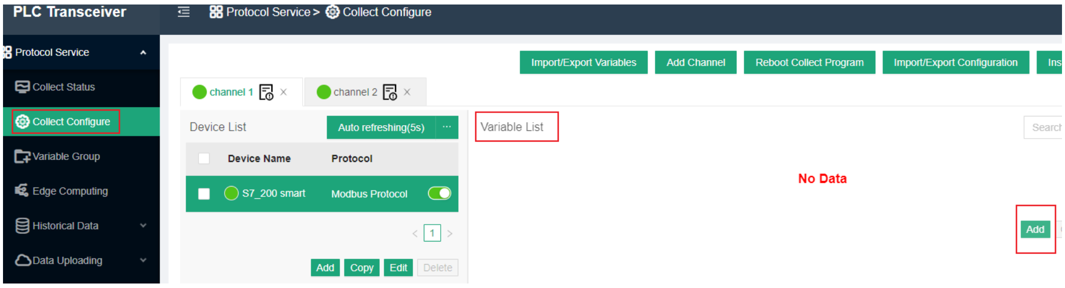
Name	Title	Group	Permission	Function Code	Data Type	Register Addr
volt.	site a	Default Group	Read Write	03	INT(int16)	3

Import/Export Variables

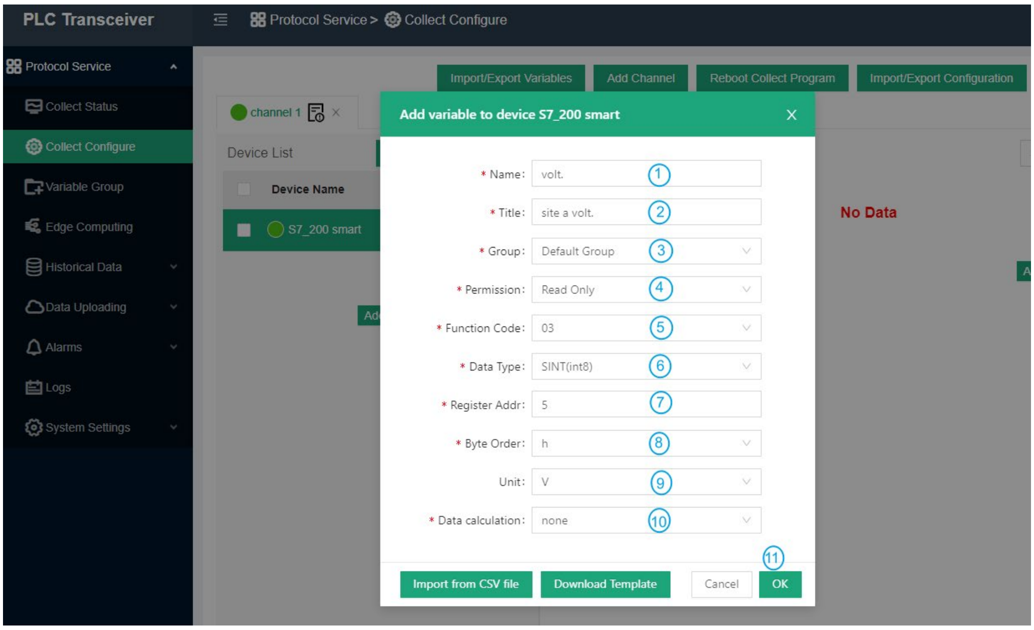
file name:

○ Individual Variable Configuration

Click the **Add** button under **Variable List** on the right side to set the variables for the device.



Set the parameters of the variable in the pop-up window.



Add variable to device S7_200 smart

- * Name: volt. (1)
- * Title: site a volt. (2)
- * Group: Default Group (3)
- * Permission: Read Only (4)
- * Function Code: 03 (5)
- * Data Type: SINT(int8) (6)
- * Register Addr: 5 (7)
- * Byte Order: h (8)
- Unit: V (9)
- * Data calculation: none (10)
- (11)

Description of the numbered areas

1. Set a variable name for the data that the endpoint collects.
2. Enter a title to describe the variable.
3. Select a group for the variable (create groups first via the **Variable Group** tab included in the menu pane on the left side).
4. Set the access permission of the variable.
   a. Read only: You can only read the measured parameters
   b. Write only: You can only distribute values from the web portal to the field device
   c. Read Write: You can both read the measured parameters and distribute values to the device
5. Select a function code.
6. Choose the data type (determined by the endpoint).

7. Input or adjust the register address from 1 to 65535.

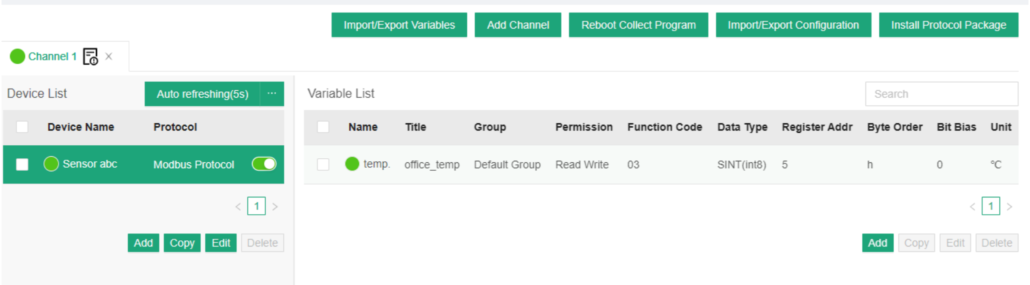
8. Set the byte order.

9. Select a unit for the variable (determined by the collection device).

10. Set a method for data calculation.

For fields that require manual input of the information, please avoid using special characters.

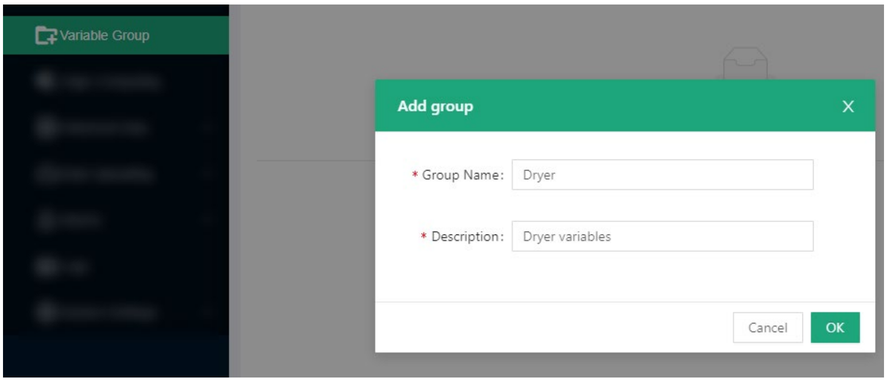
After completing the configurations, refresh the portal to check the collection settings or add/copy/edit the variables.



□	Device Name	Protocol
□	Sensor abc	Modbus Protocol

□	Name	Title	Group	Permission	Function Code	Data Type	Register Addr	Byte Order	Bit Bias	Unit
□	temp.	office_temp	Default Group	Read Write	03	SINT(int8)	5	h	0	℃

If multiple variables are involved, you can add variable groups for different variables from the **Variable Group** tab on the left menu pane.

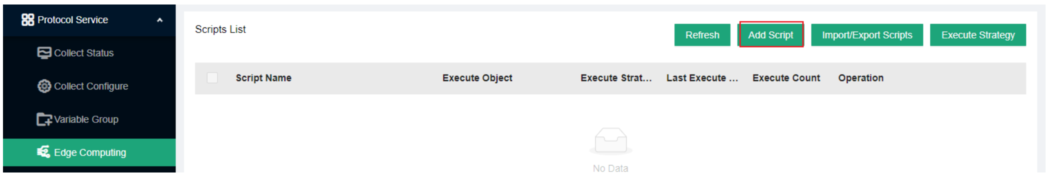


* Group Name: Dryer

* Description: Dryer variables

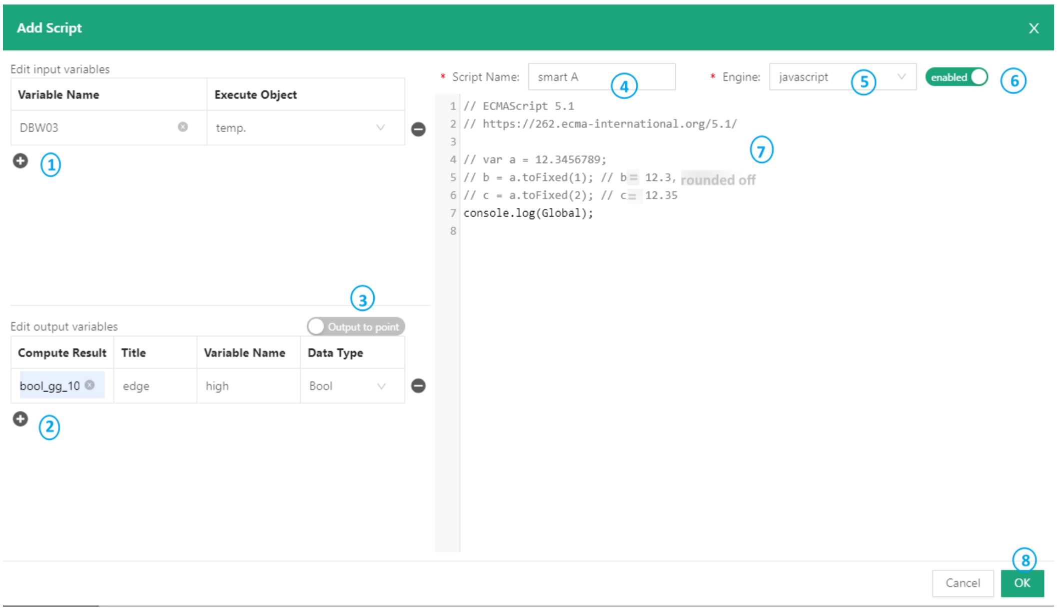
4.4 Edge Computing Scripts Setup

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



Scripts List

Script Name	Execute Object	Execute Strat...	Last Execute ...	Execute Count	Operation



Edit input variables

Variable Name	Execute Object
DBW03	temp.

Edit output variables

Compute Result	Title	Variable Name	Data Type
bool_gg_10	edge	high	Bool

* Script Name: smart A

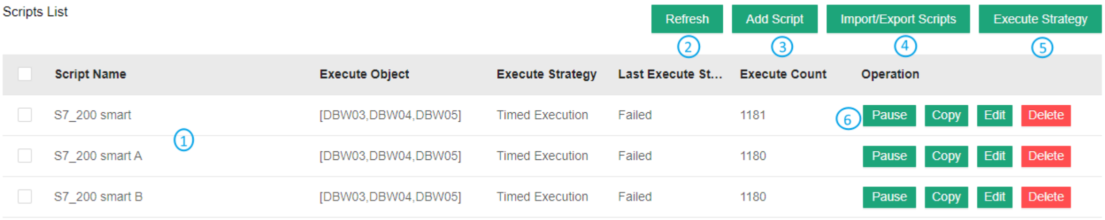
* Engine: javascript

```
// ECMAScript 5.1
// https://262.ecma-international.org/5.1/

// var a = 12.3456789;
// b = a.toFixed(1); // b= 12.3, rounded off
// c = a.toFixed(2); // c= 12.35
console.log(Global);
```

Description of the numbered areas

1. Edit 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 output variable: add the computation result, title, variable name, and data type.
3. Toggle between outputting 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.
8. After compilation, click **OK** to exit.

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

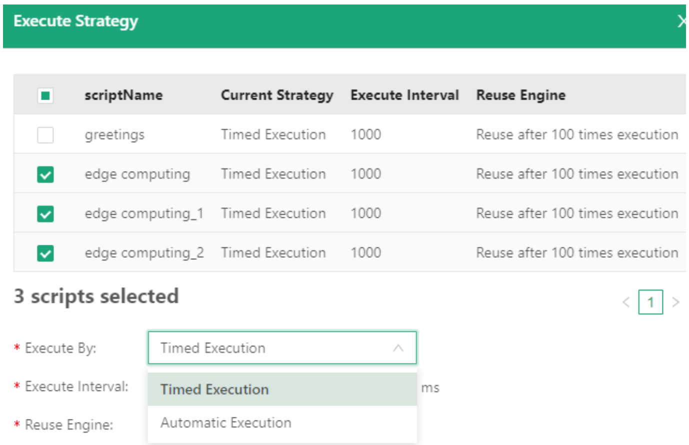


Scripts List

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

Description of the numbered areas

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



Execute Strategy

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

3 scripts selected

* Execute By: Timed Execution
* Execute Interval:
* Reuse Engine:

Timed Execution
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 is supposed to be used together with the **Execution interval:** the system is scheduled to execute the script every 1000ms by default, and you can adjust the interval.

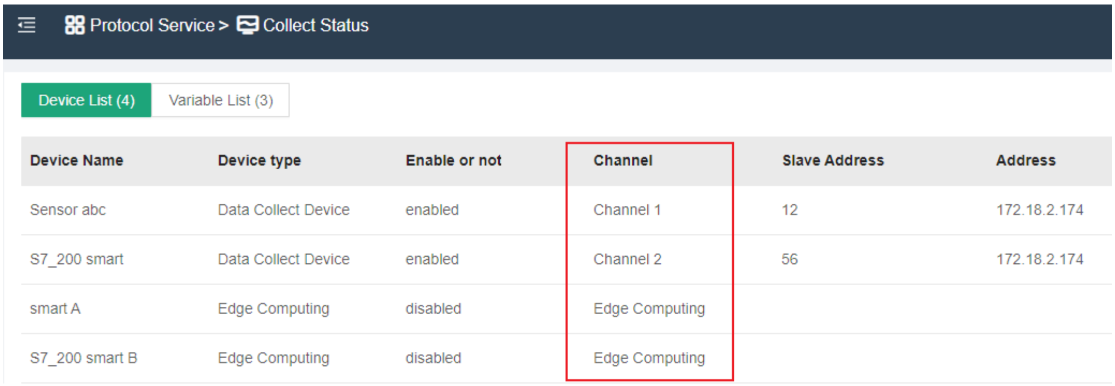
Reuse Context allows you to set a restart mechanism for the scripts

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).

4.5 Collection Status

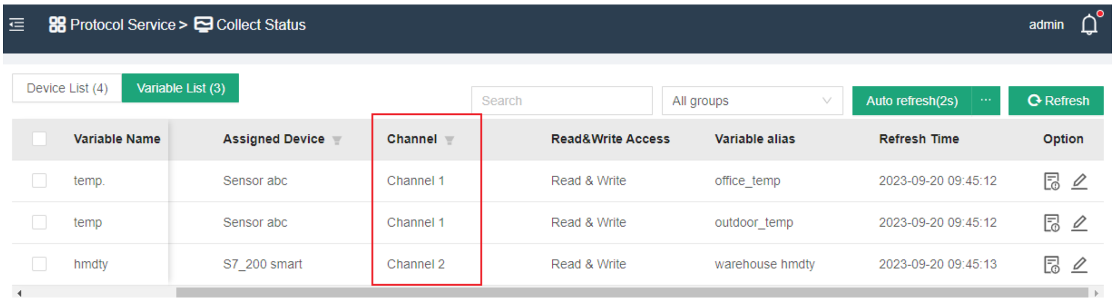
When the setup finishes, you can check the information about the devices and variables by clicking the **Collect Status** tab on the left.

The **Device List** displays information about the collection devices, edge computing, historical data, etc. Users can differentiate the data based on the collection channels.



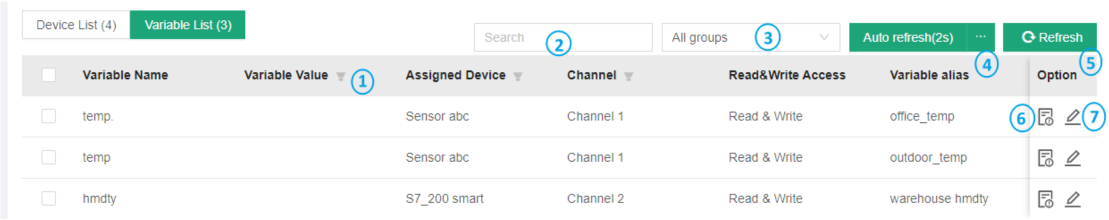
Device Name	Device type	Enable or not	Channel	Slave Address	Address
Sensor abc	Data Collect Device	enabled	Channel 1	12	172.18.2.174
S7_200 smart	Data Collect Device	enabled	Channel 2	56	172.18.2.174
smart A	Edge Computing	disabled	Edge Computing		
S7_200 smart B	Edge Computing	disabled	Edge Computing		

The **Variable List** displays information about the variables, collection devices, user permission to the variables, etc. Users can differentiate the data based on the collection channels.



□	Variable Name	Assigned Device	Channel	Read&Write Access	Variable alias	Refresh Time	Option
□	temp.	Sensor abc	Channel 1	Read & Write	office_temp	2023-09-20 09:45:12	
□	temp	Sensor abc	Channel 1	Read & Write	outdoor_temp	2023-09-20 09:45:12	
□	hmdty	S7_200 smart	Channel 2	Read & Write	warehouse hmdty	2023-09-20 09:45:13	

The **Variable List** offers the user more feasibility to set or access the variables.



□	Variable Name	Variable Value	Assigned Device	Channel	Read&Write Access	Variable alias	Option
□	temp.		Sensor abc	Channel 1	Read & Write	office_temp	
□	temp		Sensor abc	Channel 1	Read & Write	outdoor_temp	
□	hmdty		S7_200 smart	Channel 2	Read & Write	warehouse hmdty	

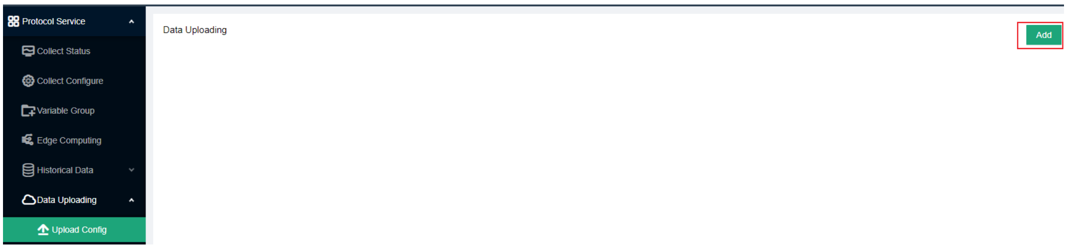
Description of the numbered areas

1. Use the filters to screen out the target information (you can screen variables, collection devices, channels).
2. Fuzzy search for the target variable .
3. Search for a variable group.
4. Click ... to set the Auto refresh interval.
5. Manual refresh.
6. Variable details.
7. Data distribution is available to variables with the **write** permission (you can tick the checkboxes before multiple variables to distribute a value to the target device).

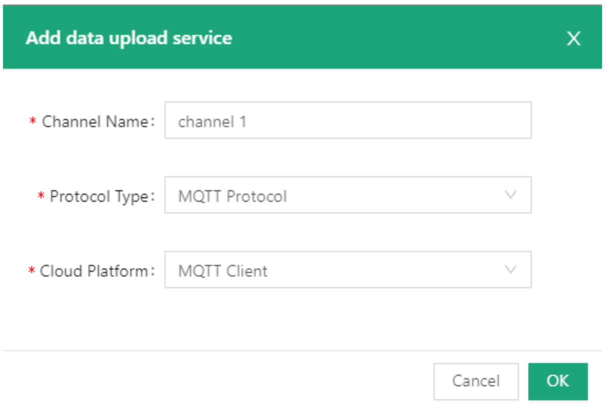
4.6 Data Upload and Encapsulation

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

1. Expand the **Data Uploading** tab from the navigation pane and click **Upload Config**.
2. Click the **Add** button on the upper right corner to add a data upload task.



3. Create an upload task in the pop-up and click **OK**.



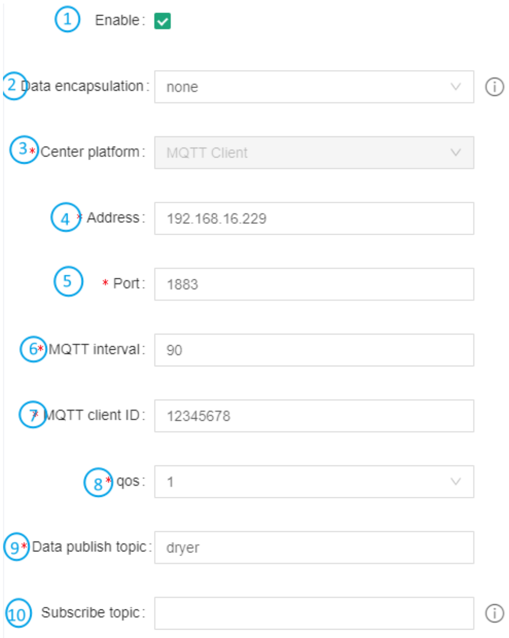
Add data upload service

* Channel Name: channel 1

* Protocol Type: MQTT Protocol

* Cloud Platform: MQTT Client

4. Configure the MQTT client in the following pop-up.



Enable: ☑

Data encapsulation: none

* Center platform: MQTT Client

* Address: 192.168.16.229

* Port: 1883

* MQTT interval: 90

* MQTT client ID: 12345678

* qos: 1

* Data publish topic: dryer

Subscribe topic:

Description of the numbered areas

1) Select to enable data uploading or not after the configuration, and the data collected will be automatically uploaded to the cloud platform if enabled.

2) Determine the data encapsulation format (no format by default).

3) The center platform is automatically filled and not changeable.

4) Fill in the IP address of the MQTT server.

5) The port number is automatically filled (1883).

6) The client will send a message to the server within a heartbeat interval (90 seconds by default and adjustable), otherwise the client network will be disconnected.

7) Input the MQTT client ID: a unique identifier, unrepeatable.

8) Set the quality of service (QoS) to ensure the reliability of the message .

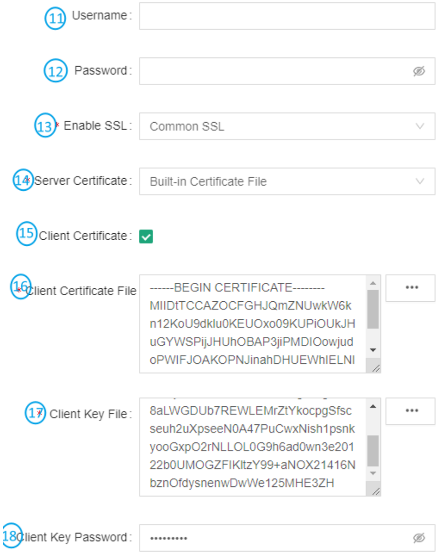
   QoS 0: The message will be sent once at the maximum. If the client is not available, the message will get lost.

   QoS 1: The message will be sent at least once.

   QoS 2: The message will be sent only once.

9) Data publish topic: used for MQTT messaging to identify which message channel the payload data is supposed to be published.

10) Topic for MQTT message subscription which enables the server to send message to a client for the control purpose.



Username:

Password:

* Enable SSL: Common SSL

* Server Certificate: Built-in Certificate File

Client Certificate: ☑

* Client Certificate File

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

* Client Key File:

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

Client Key Password: ••••••••••

11) Input a username (non-compulsory).

12) Input the password (non-compulsory).

13) Select to enable SSL or not (if yes, choose between common SSL and national SSL).

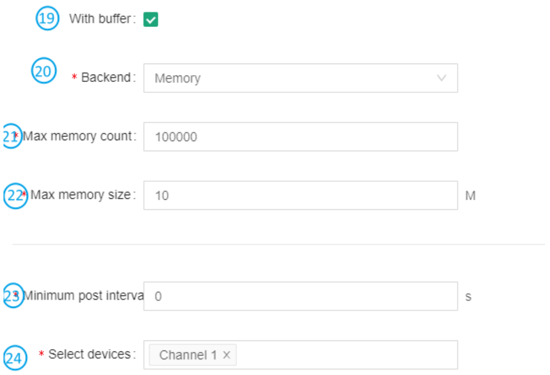
14) If common SSL is enabled, select a certification mode for the server.

15) Select to enable client certificate or not.

16) If yes, a client certificate file is needed.

17) If yes, a client key file is also needed.

18) Input a client key password (non-compulsory).



19 With buffer: ☑

20 * Backend: Memory

21 * Max memory count: 100000

22 * Max memory size: 10 M

23 Minimum post interva 0 s

24 * Select devices: Channel 1 ×

19) Select to enable data caching or not.

20) If yes, choose a medium for data caching (caching to memory by default).

21) Determine the maximum memory count.

22) Determine the maximum memory size.

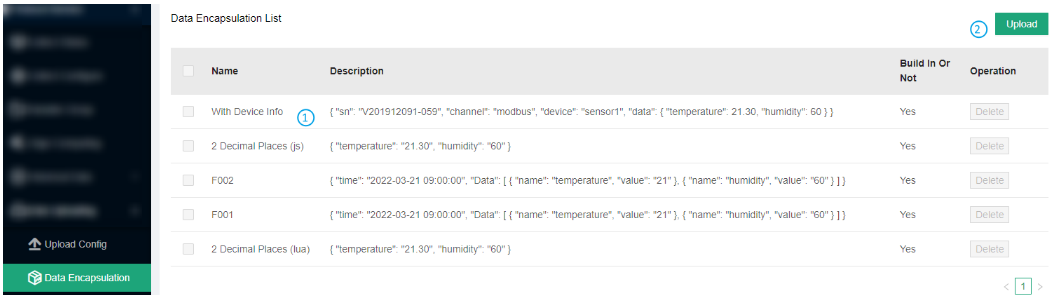
23) Input a minimum post interval.

24) Select the device of the source data.

5. Click **Submit** when finishing the configuration.

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

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



Data Encapsulation List

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

< 1 >

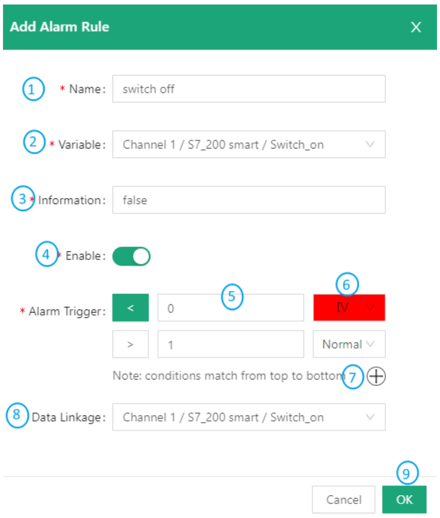
Description of the numbered areas

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

4.7 Alarm

4.7.1 Alarm Configuration

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.



* Name: switch off

* Variable: Channel 1 / S7_200 smart / Switch_on

* Information: false

* Enable: ●

* Alarm Trigger: < 0 IV
> 1 Normal

Note: conditions match from top to bottom

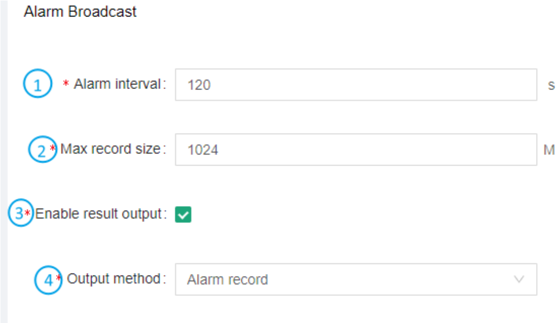
Data Linkage: Channel 1 / S7_200 smart / Switch_on

Description of the numbered areas

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

4.7.2 Alarm Broadcast

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



Alarm Broadcast

* Alarm interval: 120 s

* Max record size: 1024 M

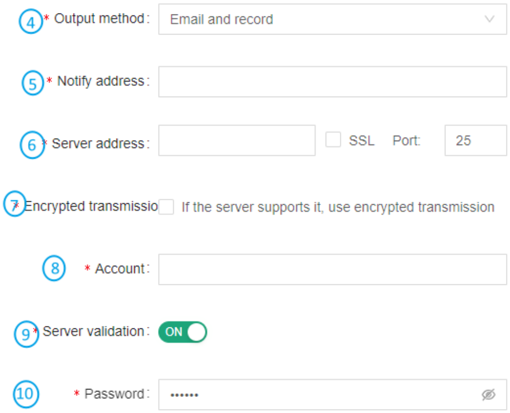
* Enable result output: ☑

* Output method: Alarm record

Description of the numbered areas

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

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



* Output method: Email and record

* Notify address:

* Server address: □ SSL Port: 25

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

* Account:

* Server validation: ON

* Password: ••••••

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

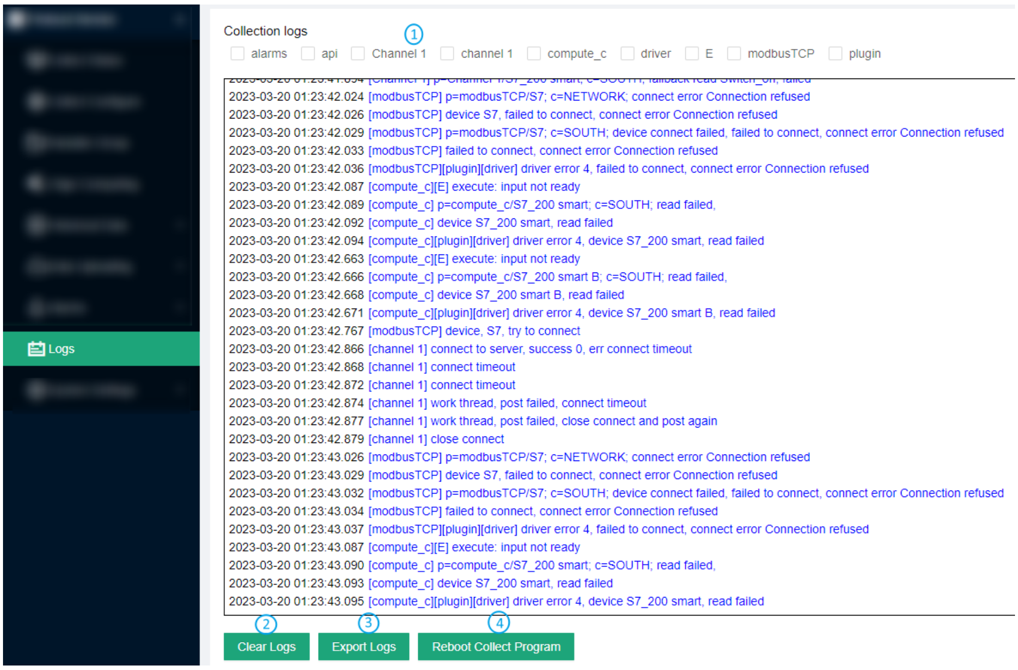
When you are all set, you can send a test email to check if the settings are ok, then submit the settings.

4.7.3 Alarm Record

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

4.8 Logs

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


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

```
2023-03-20 01:23:41.094 [Channel 1] p=Channel 1/S7_200 smart; c=SOUTH; fallback read Switch_on, failed
2023-03-20 01:23:42.024 [modbusTCP] p=modbusTCP/S7; c=NETWORK; connect error Connection refused
2023-03-20 01:23:42.026 [modbusTCP] device S7, failed to connect, connect error Connection refused
2023-03-20 01:23:42.029 [modbusTCP] p=modbusTCP/S7; c=SOUTH; device connect failed, failed to connect, connect error Connection refused
2023-03-20 01:23:42.033 [modbusTCP] failed to connect, connect error Connection refused
2023-03-20 01:23:42.036 [modbusTCP][plugin][driver] driver error 4, failed to connect, connect error Connection refused
2023-03-20 01:23:42.087 [compute_c][E] execute: input not ready
2023-03-20 01:23:42.089 [compute_c] p=compute_c/S7_200 smart; c=SOUTH; read failed,
2023-03-20 01:23:42.092 [compute_c] device S7_200 smart, read failed
2023-03-20 01:23:42.094 [compute_c][plugin][driver] driver error 4, device S7_200 smart, read failed
2023-03-20 01:23:42.663 [compute_c][E] execute: input not ready
2023-03-20 01:23:42.666 [compute_c] p=compute_c/S7_200 smart B; c=SOUTH; read failed,
2023-03-20 01:23:42.668 [compute_c] device S7_200 smart B, read failed
2023-03-20 01:23:42.671 [compute_c][plugin][driver] driver error 4, device S7_200 smart B, read failed
2023-03-20 01:23:42.767 [modbusTCP] device, S7, try to connect
2023-03-20 01:23:42.866 [channel 1] connect to server, success 0, err connect timeout
2023-03-20 01:23:42.868 [channel 1] connect timeout
2023-03-20 01:23:42.872 [channel 1] connect timeout
2023-03-20 01:23:42.874 [channel 1] work thread, post failed, connect timeout
2023-03-20 01:23:42.877 [channel 1] work thread, post failed, close connect and post again
2023-03-20 01:23:42.879 [channel 1] close connect
2023-03-20 01:23:43.026 [modbusTCP] p=modbusTCP/S7; c=NETWORK; connect error Connection refused
2023-03-20 01:23:43.029 [modbusTCP] device S7, failed to connect, connect error Connection refused
2023-03-20 01:23:43.032 [modbusTCP] p=modbusTCP/S7; c=SOUTH; device connect failed, failed to connect, connect error Connection refused
2023-03-20 01:23:43.034 [modbusTCP] failed to connect, connect error Connection refused
2023-03-20 01:23:43.037 [modbusTCP][plugin][driver] driver error 4, failed to connect, connect error Connection refused
2023-03-20 01:23:43.087 [compute_c][E] execute: input not ready
2023-03-20 01:23:43.090 [compute_c] p=compute_c/S7_200 smart; c=SOUTH; read failed,
2023-03-20 01:23:43.093 [compute_c] device S7_200 smart, read failed
2023-03-20 01:23:43.095 [compute_c][plugin][driver] driver error 4, device S7_200 smart, read failed
```

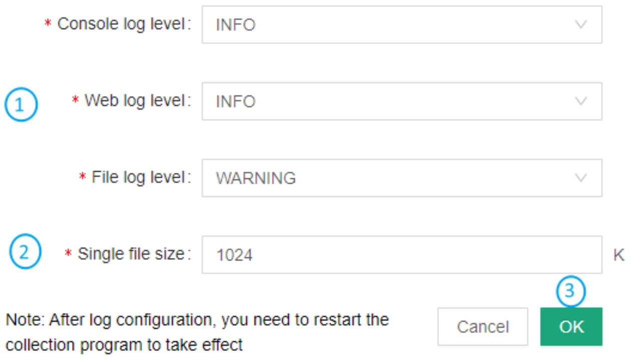
Description of the numbered areas

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

4.9 System Settings

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

- **Log Config.**



* Console log level: INFO

* Web log level: INFO

* File log level: WARNING

* Single file size: 1024 K

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

Description of the numbered areas

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

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

- **Version**

  The **Version** page displays system-related information.

- **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 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.

RF Radiation Exposure Statement:

1. This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body.
2. The device has been evaluated to meet general RF exposure requirement.