G402 Industrial Edge Computing Gateway

User Manual

Version: 1.2

Revision History

No.	Description	Date
V1.0	First release	May 21, 4025
V1.1	1. Updated I/O description and the wiring graphs. 2. Modified the description on SSH access.	Jun. 5, 4025
V1.2	1. Updated sections 2.3~2.5, and moved the network connectivity section to chapter 3; 2. Updated chapter 3 based on the current VantronOS25 firmware; 3. Added chapter 4 of the industrial protocol configurations.	Sep. 3, 4025

Table of Contents

Foreword

Thank you for purchasing G402 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

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 HARDWARE INTRODUCTION

1.1 Overview

Vantron G402 industrial edge computing gateway is an Arm®-based cost-effective solution built for industrial applications. The gateway features dual-SIM 4G connectivity, Wi-Fi, bluetooth, dual Ethernet jacks, while supporting virtual private network (VPN) to address diversified networking requirements. It also offers multiple DI, DO, and AI channels for status monitoring, control, and data visualization.

G402 features edge computing capabilities, enabling data processing and analysis directly at the edge for faster decision-making. It supports various southbound protocols, including Modbus TCP, Modbus RTU, EtherNet/IP, ISO-on-TCP, and CC-Link, ensuring seamless communication with industrial devices. The MQTT northbound protocol allows for flexible transfer of edge data to cloud servers. Meanwhile it supports interfacing with prevailing cloud platforms, including the self-developed BlueSphere GWM platform, for remote management to ease the efforts of users by real-time monitoring, OTA updates, remote maintenance, and task assignment.

Industrial interfaces such as RS232/RS485, DI, DO, AI, and CAN bus enable communication with a wide range of peripherals, while the DIN rail mount offers compact and efficient space utilization in cabinets, automation systems, and industrial control panels. G402 is an ideal solution for industrial applications such as industrial automation, grid infrastructure, and water management.

1.2 Features

- Single-core 64-bit Arm Cortex-A53 MPU + Single-core Arm Cortex-R5F MCU + Single-core Arm Cortex-M4F MCU
- Low-power, complete industrial design
- Rich interfaces: DI, DO, AI, RS232/RS485, CAN
- Dual GbE, dual SIM backup, Wi-Fi, Bluetooth for flexible connectivity
- Support for both southbound and northbound protocols for seamless data transfer
- Local edge computing support
- SDK available, with system APIs
- Optional BlueSphere GWM support for remote control
- Industrial extended temperature and input voltage
- Space-efficient design for flexible installation

1.3 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

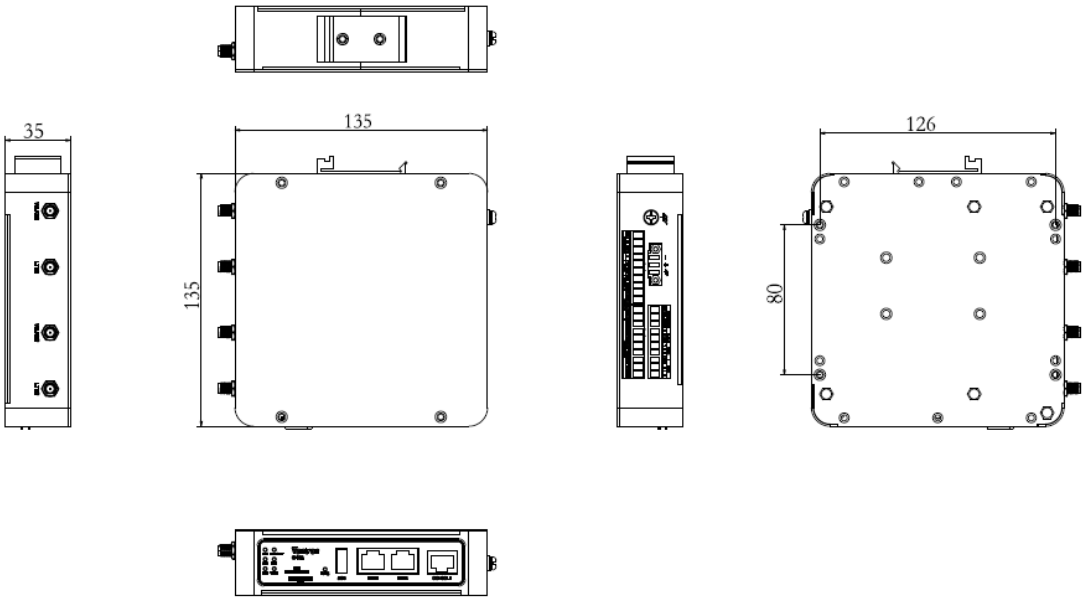
- 1 x G402 Edge computing gateway
- 2 x Wi-Fi antenna
- 2 x 4G LTE antenna
- 3 x 10-pin I/O mating connector
- 1 x DC power connector

Optional accessories

- 1 x 12V DC Power adapter
- 1 x Power cord

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

1.4 Product Outlines

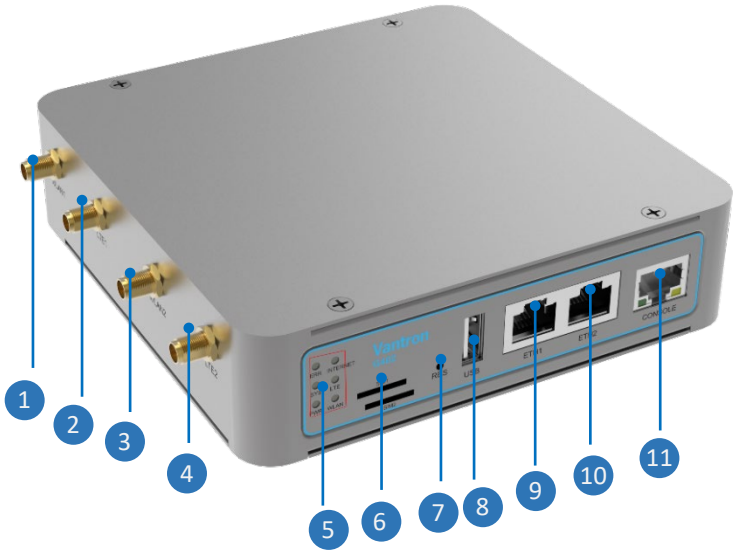


1.5 Specifications

G402			
System	CPU	Single-core 64-bit Arm Cortex-A53 microprocessor, 1.0GHz (Max.) Single-core Arm Cortex-R5F MCU, 800MHz (Max.) Single-core Arm Cortex-M4F MCU, 400MHz (Max.)	
	Memory	512MB DDR4	
	Storage	8GB eMMC	
Cellular	Modem	4G LTE, CAT 4	
	SIM	2 x Micro SIM slot	
	Antenna	2 x Antenna (SMA-K connector)	
Ethernet	Port	2 x RJ45, 10/100/1000Mbps	
	Configuration	1 x WAN + 1 x LAN	
Wi-Fi	Standard	IEEE 802.11 b/g/n/ac	
	Frequency band	2.4GHz, 5GHz	
	Working mode	AP, Station	
	Antenna	2 x Antenna (RPSMA-K connector)	
	Security	AES, WPS	
Bluetooth	Bluetooth	Bluetooth 5.2	
I/O	Serial port	2 x RS232/RS485 (isolated), Max. 250kbps	1 x 5V output
	USB	1 x USB 2.0 Type-A	
	DI	4 x DI (dry / wet contact)	
	DO	2 x DO, 5A @30V DC	
	AI	2 x AI (measurement signal: 0~20mA or 4~20mA / 0~5V or 0~10V)	
	CAN	2 x CAN bus (isolated)	
	Debug	1 x RJ45 Console port (Baud rate: 115200)	
System Control	Button	1 x Restore button (≤ 2s: restart; 3s-5s: factory reset; ≥10s: clear all data and apps)	
	LED indicator	1 x Power indicator	1 x Internet indicator
		1 x Status indicator	1 x 4G LTE indicator
		1 x Error indicator	1 x WLAN indicator
	Watchdog timer	Hardware watchdog	
	RTC	Supported	
Power	Input	9V-36V DC	
	Socket	1 x 3-pin x 3.81mm	
	Protection	Over-current protection, Reverse polarity protection	
Physical Characteristics	Dimensions	135mm x 135mm x 35mm	
	Enclosure	Metal	
	Weight	716g (not including accessories)	
	Installation	DIN rail mounting	
	IP rating	IP40	
	Cooling mode	Heat sink	
	Mechanical test	Drop: IEC60068-2-32	Shock: IEC60068-2-27
		Vibration: IEC60068-2-6	
EMC	ESD	IEC 61000-4-2 (Contact: 6kV, Air: 8kV)	
Environmental Condition	Temperature	Operating: -40℃ ~ +80℃	Storage: -40℃ ~ +85℃
	Humidity	5%-95% RH (non-condensing)	
Certification	Compliance	FCC, ISED, CE	
	Carrier certification	AT & T, Verizon, T-Mobile	

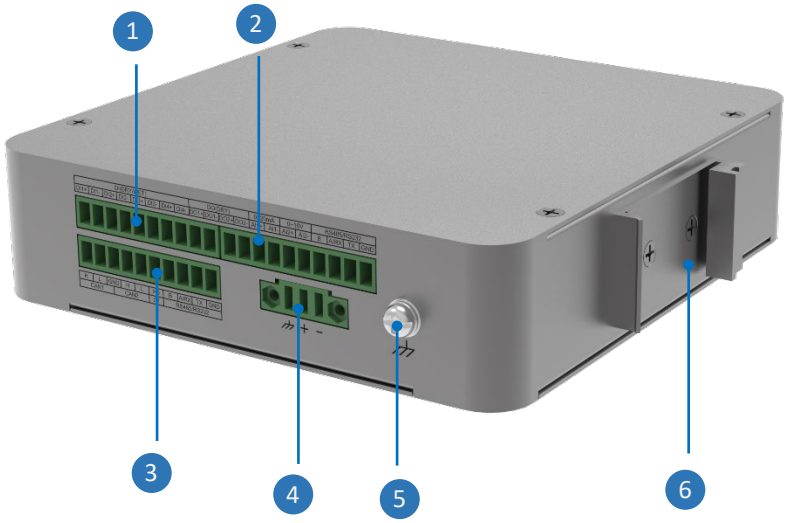
G402			
Edge Computing	Edge computing script	JavaScript, MicroPython	
	Southbound protocol	Modbus TCP, Modbus RTU, EtherNet/IP, ISO-on-TCP, CC-link, etc.	
	Northbound protocol	MQTT	
Custom Development	IPK import	Supported	
	Documentation support	SDK available, API documentation	
Device Management	Operating system	Web-based VantronOS	
	Configuration	VantronOS, SSH, console port, cloud-based BlueSphere GWM (Optional)	
	Remote management	BlueSphere GWM (Optional)	
	Upgrade	VantronOS, BlueSphere GWM (Optional)	
Routing & Network Reliability	Network protocol	IPV4, HTTPS, TCP & UPD, NTP client and server, ARP, TLS	
	Link detection & report	Address: IP, URL	Protocol: ICMP, TCP, HTTP
	Failover	Auto routing, Auto reconnection	Network priority: Ethernet > Wi-Fi client > Cellular (def.)
	Dual SIM	Dual SIM failover, automatic switch	
	NAT	Dynamic, Static	
	WAN protocol	DHCP client, PPPoE, Static IP	
	Network management	SNMP v1/v2c/v3	
	IP application	Ping, Traceroute, Nslookup, DHCP Server/Client, DDNS	
	IP routing	Static routing	
Network Diagnostics	Network capture	By time or packet count	
	Statistics	Traffic data and up time at Ethernet WAN, Wi-Fi client WAN, cellular WAN Cellular and Wi-Fi signal strength; SIM card switch frequency	
	Health check	Usage of CPU, memory, disk Service running status Alarm on Ethernet/Wi-Fi/cellular hardware abnormality	
	Log	System log, diagnostic log	Log export supported
Security	Firewall	Stateful, whitelist control, port mapping	
	Access control	MAC address filtering, IP address filtering	
	VPN	PPTP, L2TP, GRE, IPSec, OpenVPN	
	Firmware validation	SHA256 checksum	

1.6 Product Views



I/O Description:

No.	Description
1	Wi-Fi primary antenna (RPSMA-K)
2	Cellular primary antenna (SMA-K)
3	Wi-Fi diversity antenna (RPSMA-K)
4	Cellular diversity antenna (SMA-K)
5	LED indicators (power indicator, internet indicator, status indicator, 4G LTE indicator, error indicator, WLAN indicator)
6	2 x SIM slot
7	Reset pinhole button ≤ 2s: restart; 3s-5s: factory reset; ≥10s: clear all data and apps (not recommended)
8	USB 2.0 Type-A
9	RJ45 (ETH1), 10/100/1000Mbps (WAN port)
10	RJ45 (ETH2), 10/100/1000Mbps (LAN port)
11	RJ45, Console port, baud rate: 115200



I/O Description:

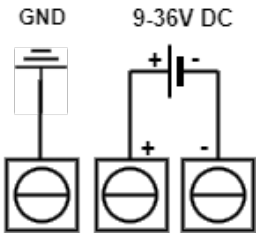
No.	Description
1	I/O 1 (left to right: 4 x DI + 1 x DO)
2	I/O 2 (left to right: 1 x DO + 2 x AI + 1 x RS232/RS485)
3	I/O 3 (left to right: 2 x CAN + 5V power output + 1 x RS232/RS485)
4	Power terminal
5	Grounding screw
6	DIN rail mount

1.7 Interface Parameters

Interface	Parameter	Description
Digital input (DI)	Channel #	4
	Type	Dry/Wet contact
	Input mode	Level
Analog input **Current measurement** (AI)	Channel #	1
	Measurement range	0~20mA
	Accuracy	5‰
	Sampleing frequency	860Hz
	Resolution	16 bits
	Isolation	None
	Input impedance	120Ω
	Input mode	Single-ended input
Analog input **Voltage measurement** (AV)	Channel #	1
	Measurement range	0~5V/0~10V
	Accuracy	5‰
	Sampleing frequency	860Hz
	Resolution	16 bits
	Isolation	None
	Input impedance	14.7kΩ
	Input mode	Single-ended input
Digital output (DO)	Channel #	2
	Contact	C-type relay
	Contact capacity	250V/3A
	Output mode	Level
Upstream COM (RS232/RS485)	Serial port type	RS485/RS232
	Channel #	2
	Baud rate range	50Kbps~1Mbps (default parameters: 9600，8N1)
	Protocol	Modbus
CAN	Channel #	2
	Bitrate ranges	4800~921600

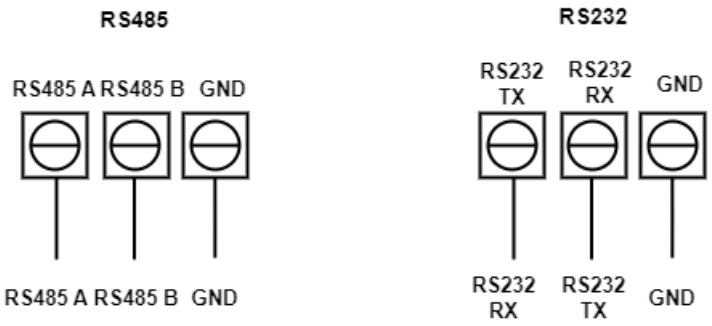
1.8 Wiring Instructions

1.8.1 Power Input

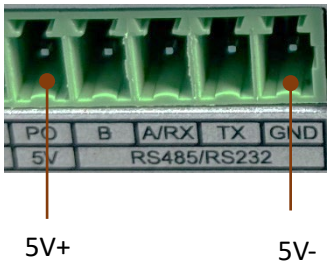


Power terminal: 1 x 3 x 3.81mm, 12V/1A DC recommended.

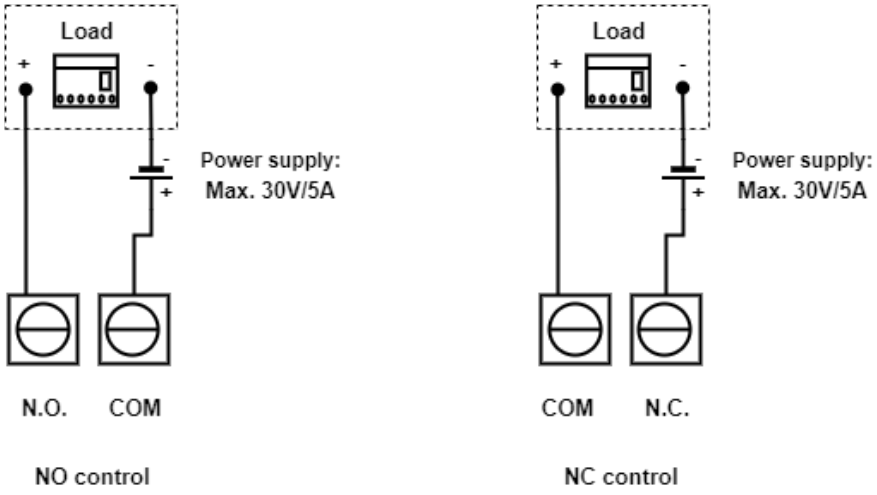
1.8.2 RS232/RS485 & 5V Output



G402 provides a 5 V power-output port: pin PO serves as the positive rail, and the RS485/RS232 GND pin serves as the negative return. The port can deliver up to 0.1 A; exceeding this current will impair RS485 operation.



1.8.3 Digital Output (DO)



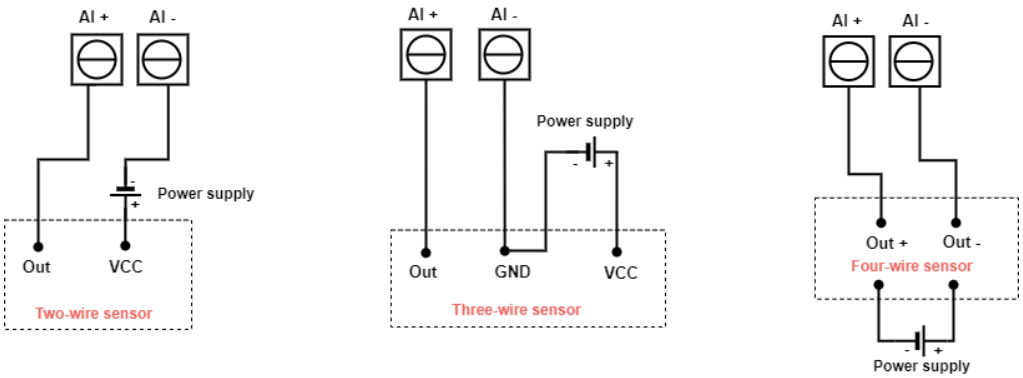
The interface connection can be controlled via software. Up to 30V/5A power supply is supported.

1.8.4 Digital Input (DI)

Each digital input channel can be switched—via software—between dry-contact and wet-contact modes. In the dry-contact mode: after DI+ and DI- are shorted together, the channel is read as low level. In the wet-contact mode: wire DI+ to the positive rail of the on-board 3.3V supply and DI- to the negative rail; when the circuit is closed, the channel is read as low level.

Contact mode	Wiring
Dry contact	Connect DI- to one end of the line and DI+ to the other. When the circuit is closed, the input reads a low level; when open, it reads a high level.
Wet contact	Connect DI- to 3.3V GND and DI+ to 3.3V VCC. The input is low when powered (circuit closed) and high when unpowered (open).

1.8.5 Analog Input (AI)



G402 provides two analog input channels:

- **Channel 1 (AI1+, AI1-)** is for 0~20mA current measurement; the actual current value is displayed via software configuration.
- **Channel 2 (AI2+, AI2-)** is for 0~5V or 0~10V voltage measurement. 0~10V measurement is set as the default. To switch this channel to 0~5V, open the device enclosure and configure the on-board jumper (J8):
  – Pins 1-2 shorted → 0~5V range
  – Pins 2-3 shorted → 0~10V range

1.9 LED Indicators

LED	Function	Description
ERR	Device fault	Solid green: Device abnormality detected
INTERNET	Internet status	Solid green: Device online via Ethernet, 4G or Wi-Fi
		Off: No internet connection
SYS	System running condition	Blinking: System running properly
		Off: System fault
LTE	Cellular status	Blinking: 4G module running properly
		Off: 4G module fault
PWR	Power status	Solid green: Device powered up
WLAN	Wi-Fi status	Blinking: Wi-Fi module running properly in the AP mode
		Off: Wi-Fi module not in the AP mode

1.10 Button

G402 offers a RES (Reset) pinhole button that combines restart and factory-recovery functions:

- **Short press** (< 2s) – restarts the gateway
- **Long press** (3~5s) – restores factory settings
- **Very long press** (> 10s) – erases all user data and applications (not recommended)

1.11 Console Port

Connect the gateway's console port to a PC using an RS232-to-RJ45 cable for device configuration or management.

Default baud rate: 115200.

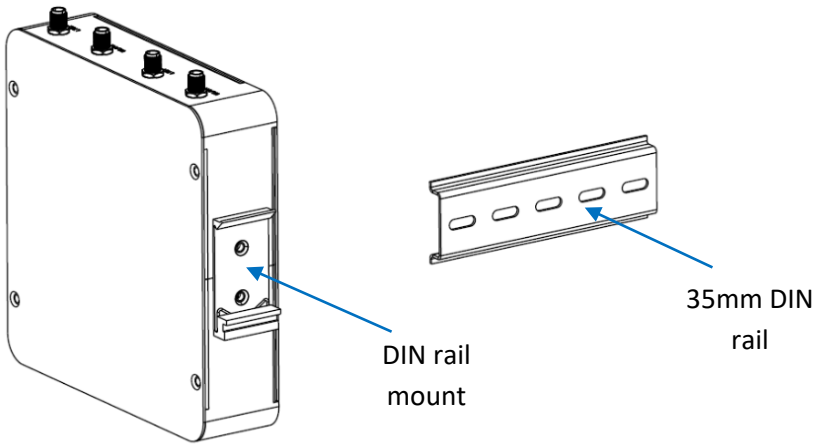
1.12 SIM Slot

The gateway is equipped with two Micro SIM slots. With dual SIMs installed, the device automatically switches to the line with the stronger signal whenever the current cellular connection becomes unstable.

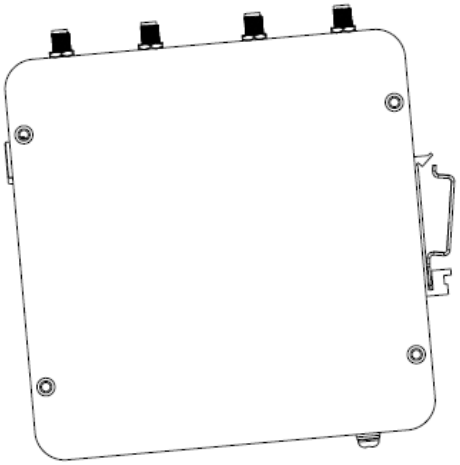
CHAPTER 2 GETTING STARTED

2.1 Device Installation

1. Hold the gateway vertically, and align the DIN rail mount of the device to the 35mm DIN rail.

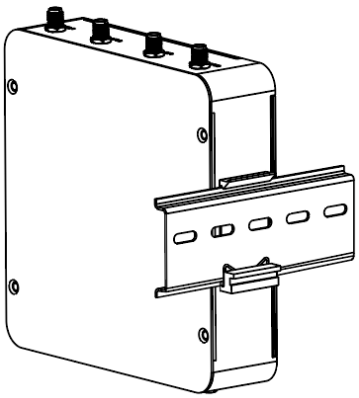


2. Align the lower edge of the DIN rail with the bottom clip of the DIN rail mount and position it behind the triangular fixing piece.



3. Push the gateway toward the DIN rail until it snaps securely into place.

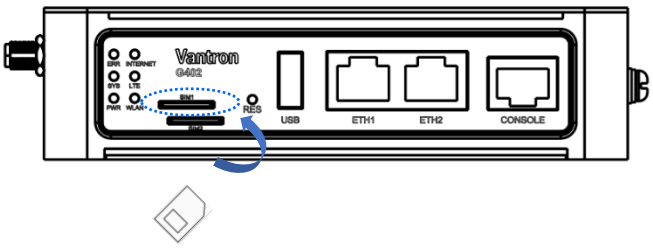
4. Gently swing the device to make sure it is fixed on the DIN rail.



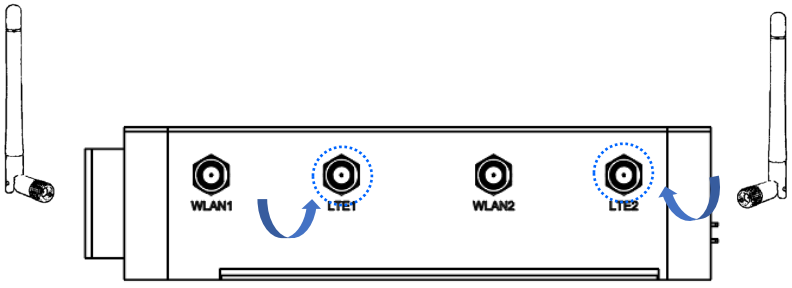
2.2 Hardware Connection

After installation, complete the hardware connections below **as needed** for smooth operation of G402.

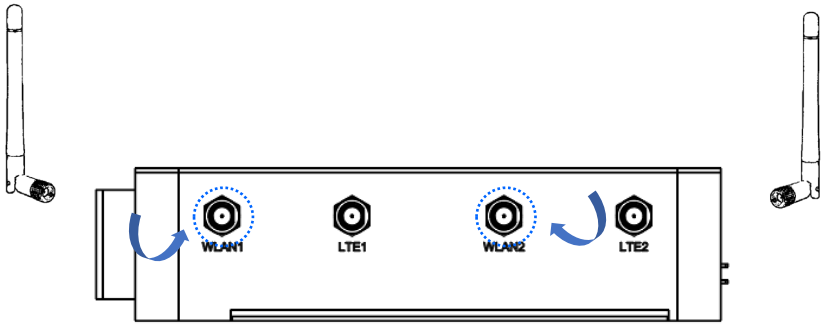
1. Based on your actual situation, insert the activated Micro SIM card into the desired slot and push the card in until it clicks.
   - For SIM 1: gold contacts facing **down**;
   - For SIM 2: gold contacts facing **up**.



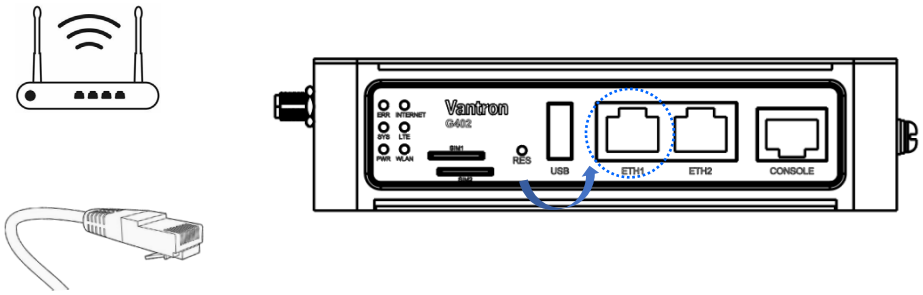
2. Attach the 4G antennas to the LTE 1 and LTE 2 connectors.



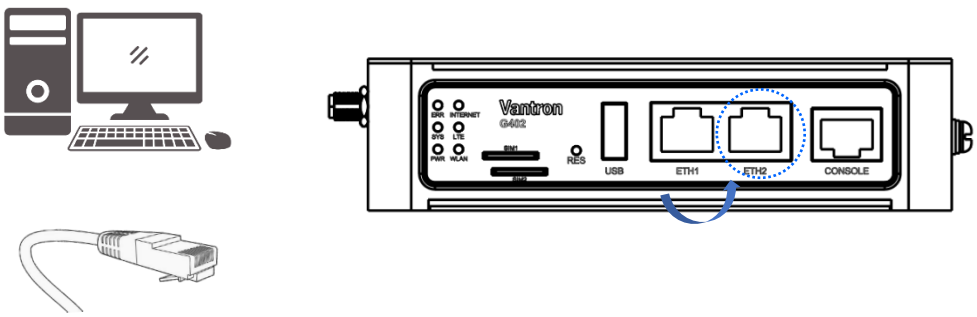
3. Attach the Wi-Fi antennas to the WLAN 1 and WLAN 2 connectors.



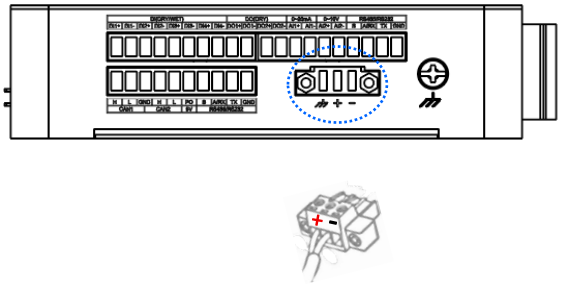
4. Connect the gateway to the upstream network (router or switch) using an Ethernet cable plugged into ETH 1 (WAN).



5. Connect a PC or other network devices to the gateway using an Ethernet cable plugged into ETH 2 (LAN) for local management or Internet access.



6. For wiring of the AI/DI/DO channels, refer to the wiring instructions in Section 1.8.
7. Insert the terminal block of the DC power connector into the gateway's power terminal and connect the other end to the power cord.



8. Plug the power adapter into a DC outlet that meets the device's operating voltage requirement (9V~36V DC) to power on the gateway.
9. After power-on, the PWR indicator will turn solid green.

2.3 Web Login

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

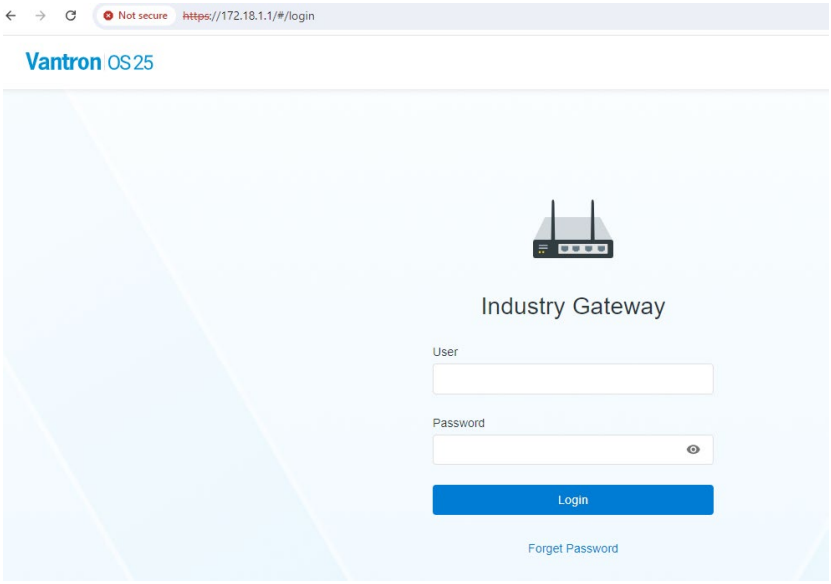
There are two login options to access VantronOS for G402, depending on how the host computer is connected to it.

Method	Host Computer Connection	VantronOS Login Address
Option 1	Host connects to G402's Ethernet LAN port or to G402's Wi-Fi.	Use G402's LAN IP (default IP address: 172.18.1.1)
Option 2	Host's WAN interface on the same IP subnet as G402's WAN interface (e.g., both connected to the same switch or upstream Wi-Fi).	UseG402's WAN IP

We recommend initially logging into VantronOS using **Option 1**. Afterwards, you may establish additional connections between G402 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.

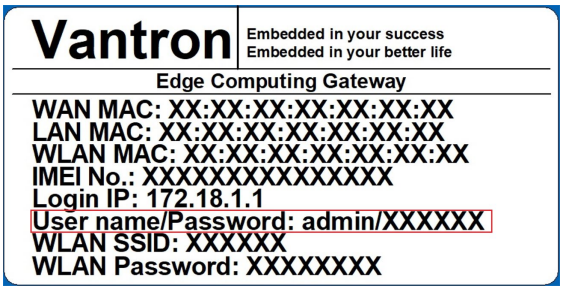
VantronOS login via Ethernet LAN connection:

1. Connect the host computer to the LAN port (ETH 2) of G402 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.



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.

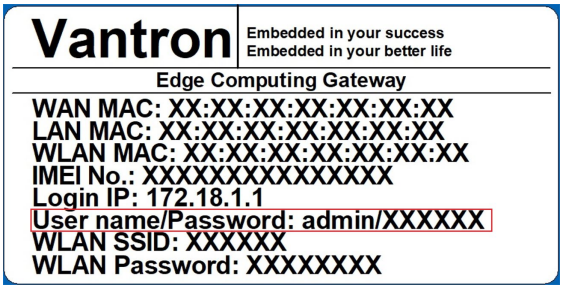
2.3.1 Password Reset

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

1. Press the **Reset** button on the device and hold for 3~5 seconds to factory reset the device.

   Factory reset restores all settings—including the login password—to their defaults. You will need follow the setup wizard for the initial setup after a factory reset. ***Holding the Reset button for more than 10 seconds erases all data and applications****, locking you out of VantronOS. Therefore, do not hold that long unless absolutely necessary.*

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

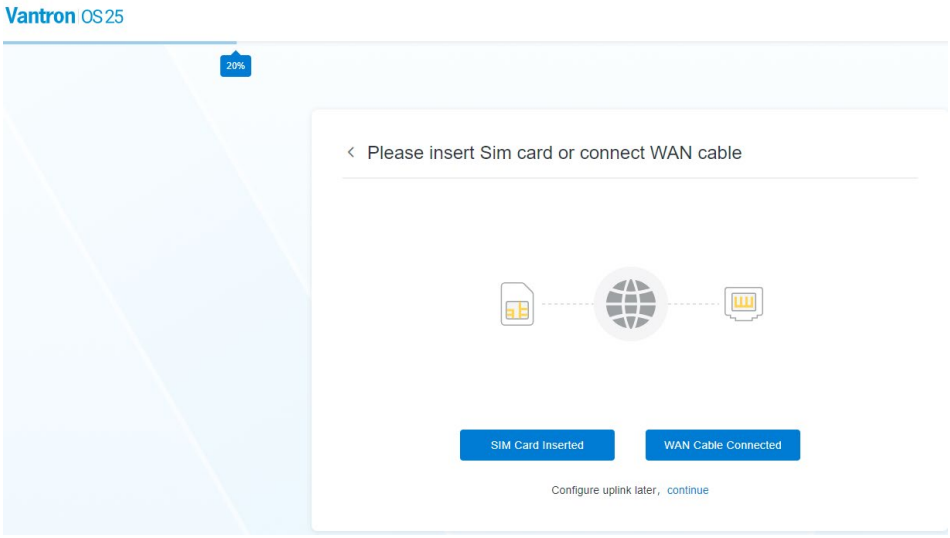


To reset the login password without factory resetting the device, refer to section 3.7.2 for the instructions.

2.3.2 Login Wizard

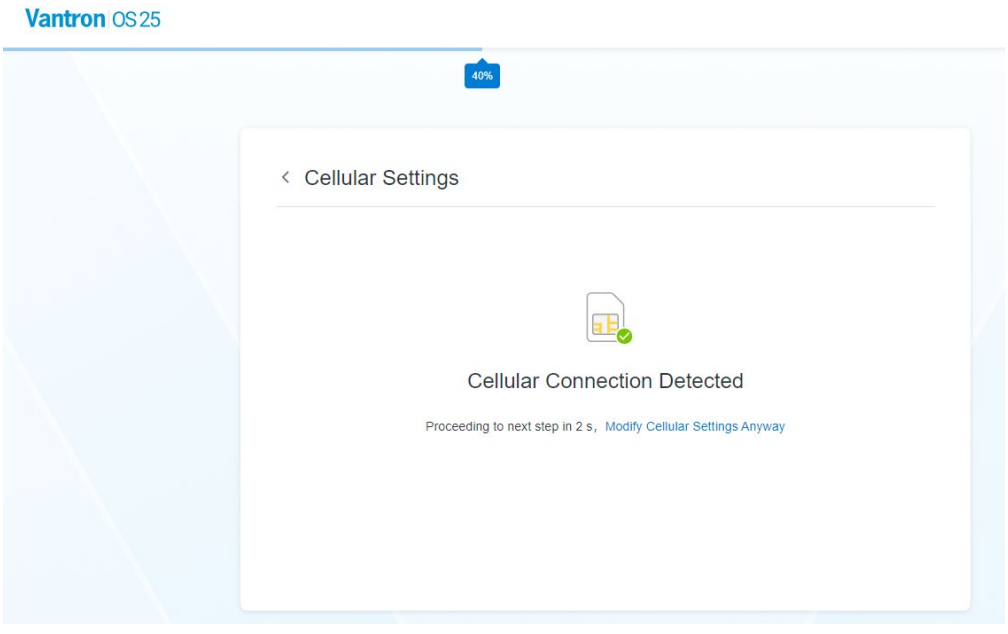
For first-time users, the setup wizard will guide you through the initial setup process, including modifying the login password.

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.

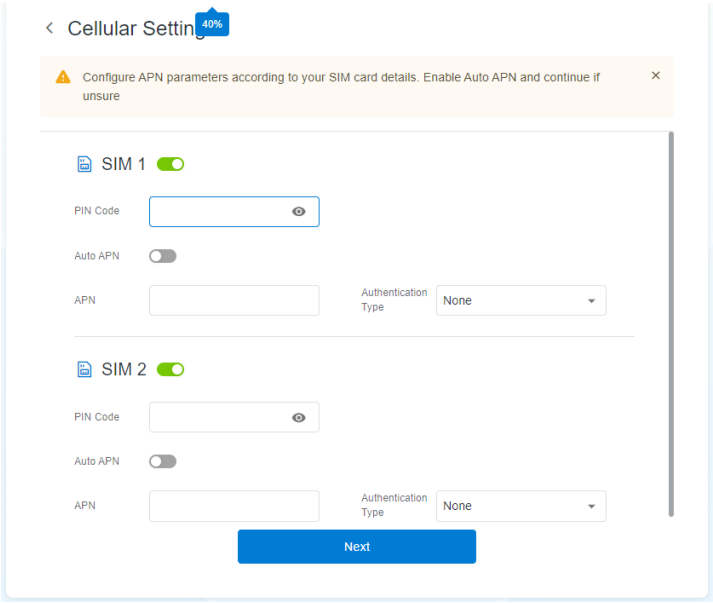


- **Cellular Settings (SIM Card Inserted)**

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



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.



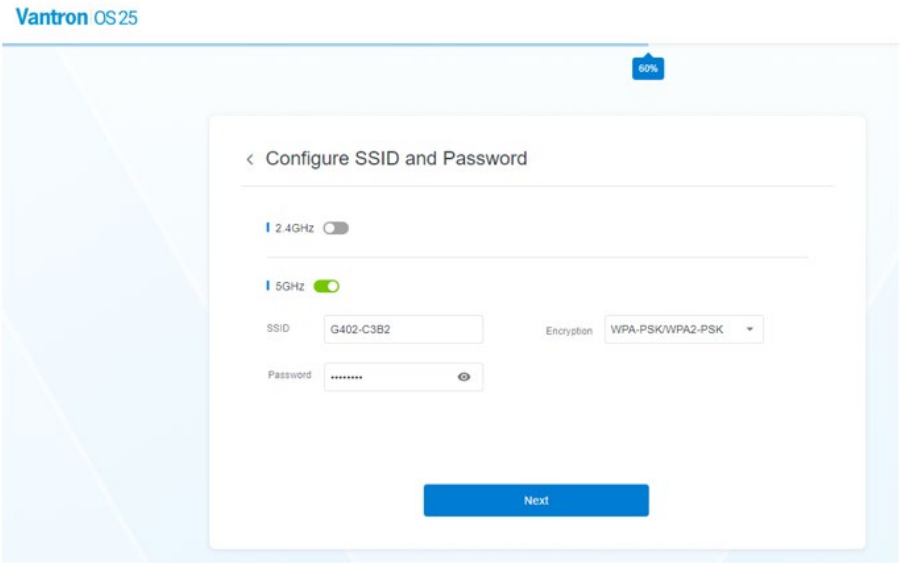
PIN: Carrier-defined, optional.

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

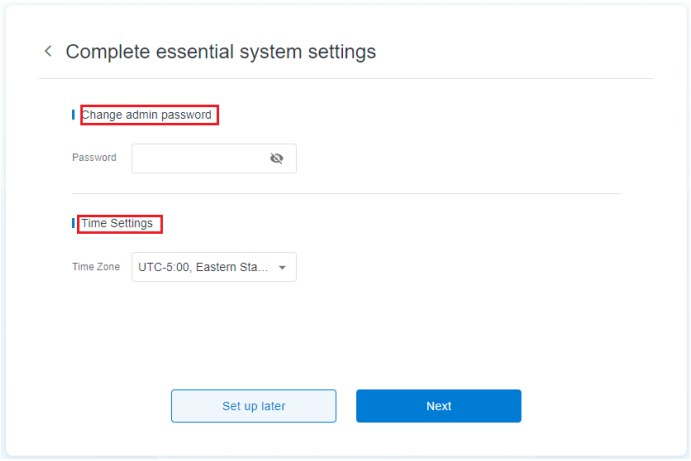
Authentication Type (None / PAP / CHAP): Carrier-defined; required when **Auto APN** is off.

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

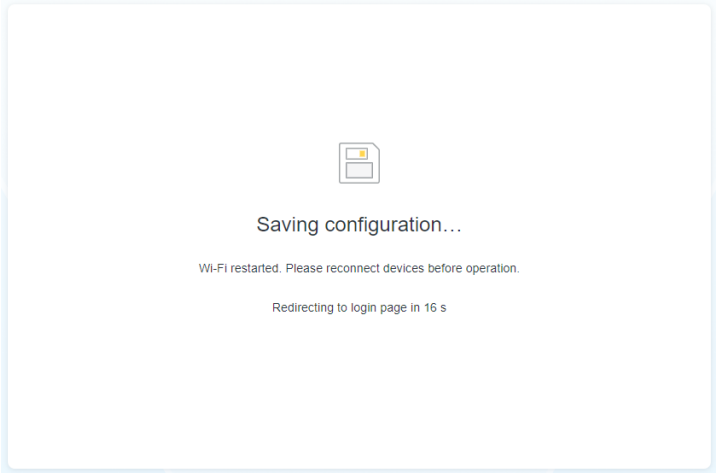
4. Configure the Wi-Fi SSID, encryption, and password for the device operating as a Wi-Fi access point, then click **Next**.



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**.

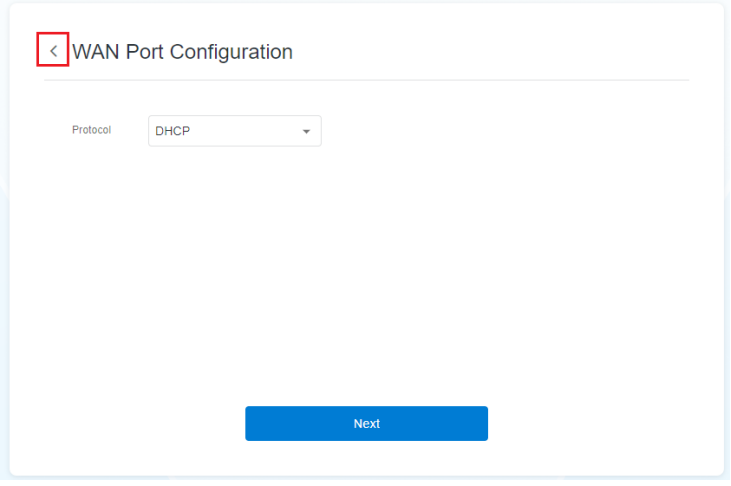


6. Wait about 20 seconds to allow the changes to apply. Once the countdown finishes, you will be redirected to the login page.



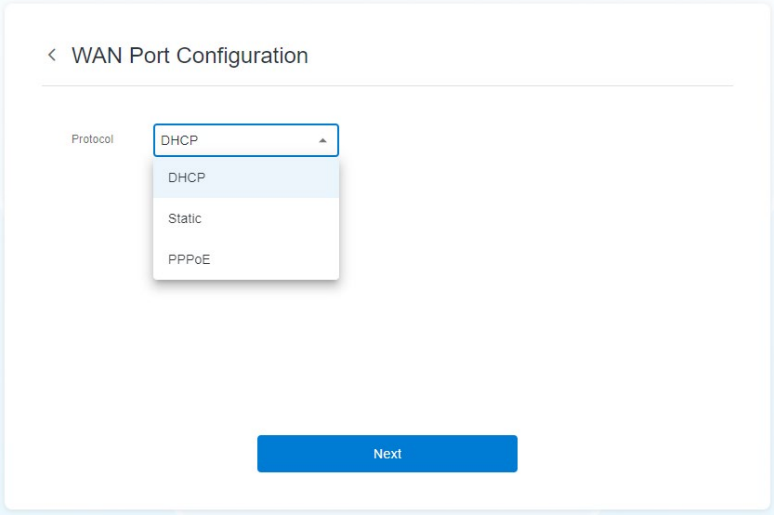
7. Log in to the web portal using the new Admin password (if changed previously).

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



- **WAN Port Settings (WAN Cable Connected)**

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

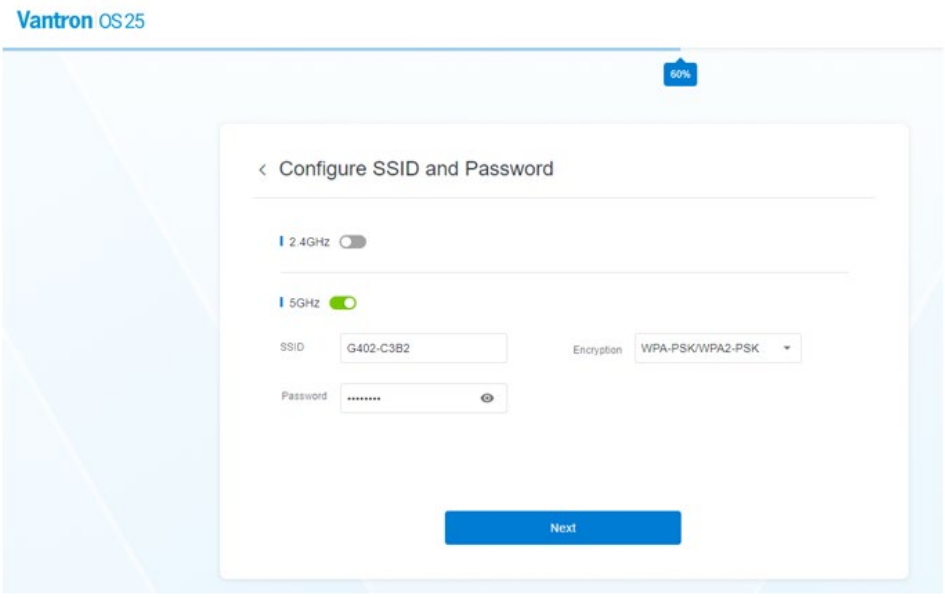


DHCP (Dynamic Host Configuration Protocol): A DHCP server **automatically** assigns IP addresses and network configuration (subnet, gateway, DNS) to the device.

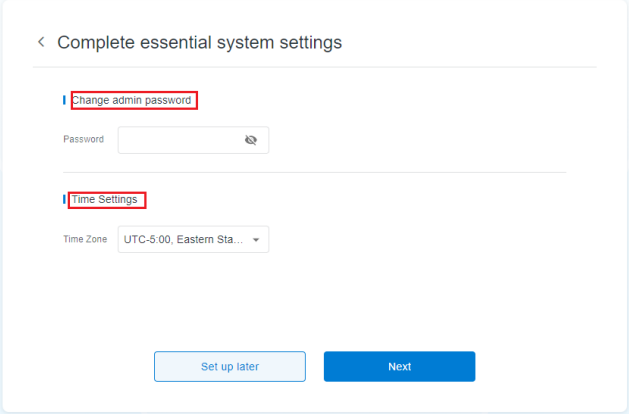
Static: IP settings are **manually** entered into the device and remain fixed until changed.

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).

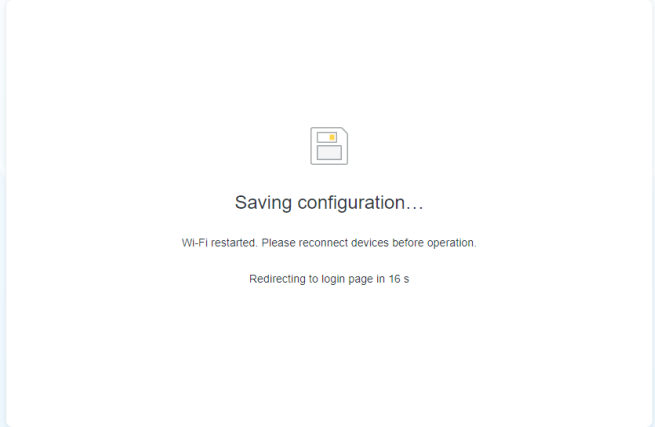
2. Configure the Wi-Fi SSID, encryption, and password for the device operating as a Wi-Fi access point, then click **Next**.



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**.

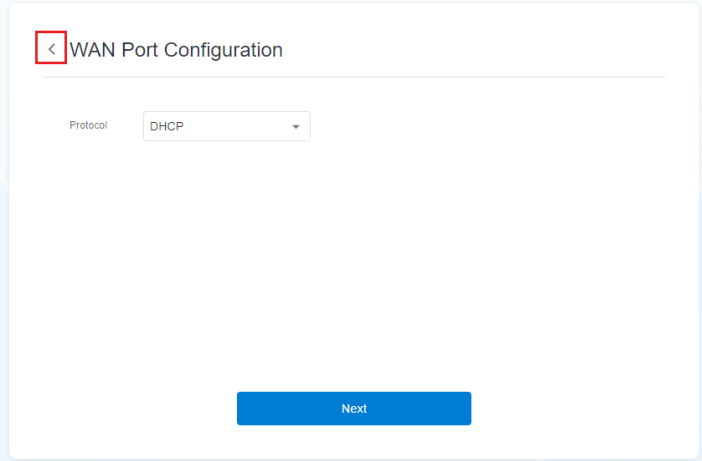


4. Wait about 20 seconds to allow the changes to apply. Once the countdown finishes, you will be redirected to the login page.



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 of the page.



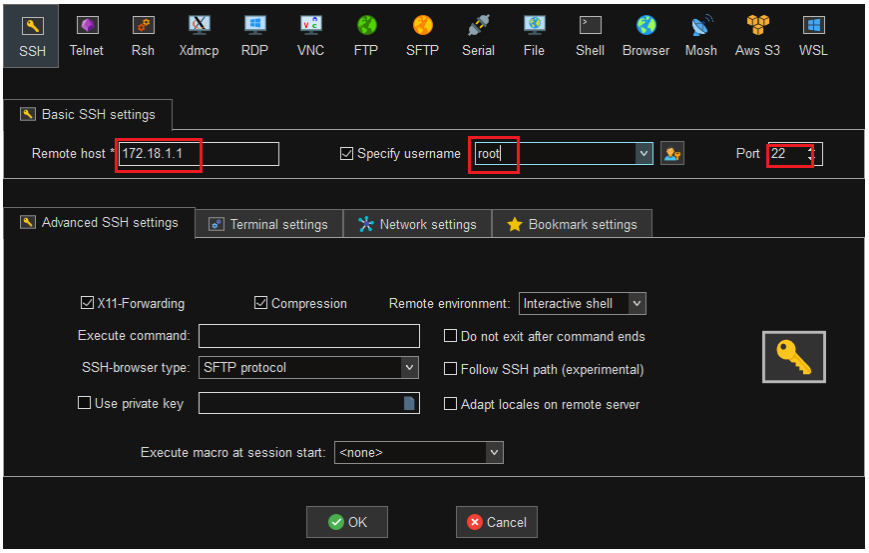
2.4 SSH Login

SSH is enabled on G402 by default. Prior to establishing an SSH connection, make sure the Windows host computer (client) can reach G402's (server) IP.

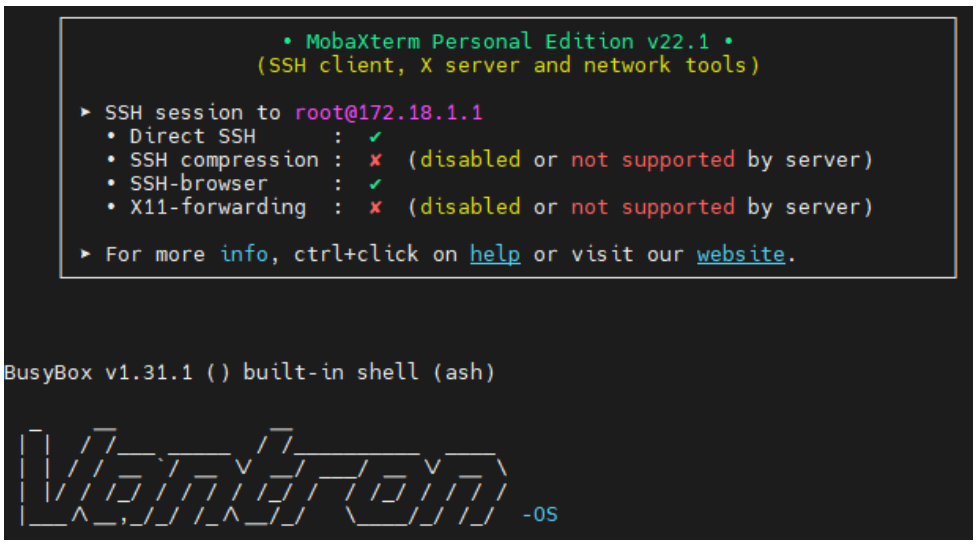
Method	Host Computer Connection	Login Address
Option 1	Host connects to G402's Ethernet LAN port or to G402's Wi-Fi.	Use G402's LAN IP (default IP address: 172.18.1.1)
Option 2	Host's WAN interface on the same IP subnet as G402's WAN interface (e.g., both connected to the same switch or upstream Wi-Fi).	Use G402's WAN IP

SSH login via LAN IP:

1. Connect the Windows host computer to G402's LAN port (ETH 2) via Ethernet or connect to its Wi-Fi.
2. Open a serial debug program (PuTTY or MobaXterm recommended) on the host computer.
3. Select **SSH** session.
4. Enter G402's LAN IP, keep the default SSH port No. (22) unchanged, and use "root" as the username.

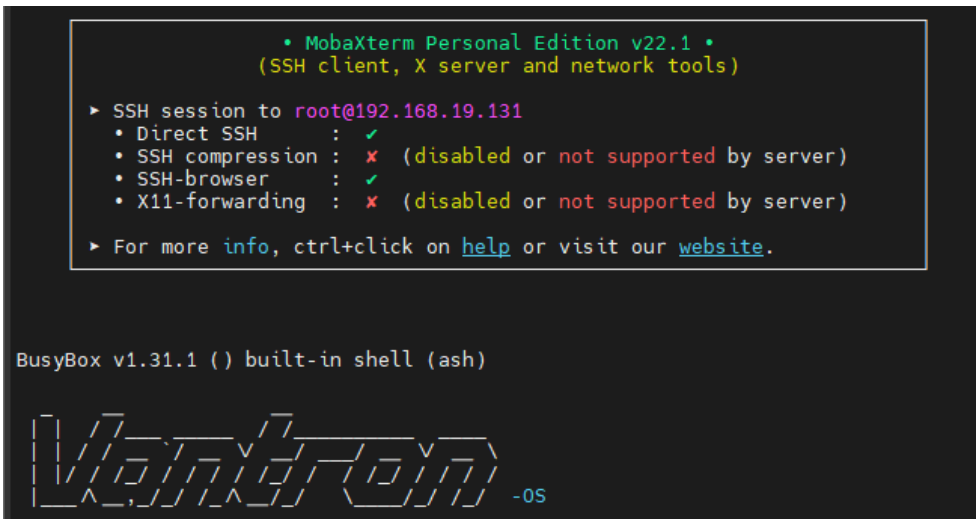


5. Click **OK** to open the session.



SSH login via Ethernet WAN port:

1. Connect both the Windows host computer and G402 to the same switch via ETH 1 or Wi-Fi.
2. Determine the device'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.



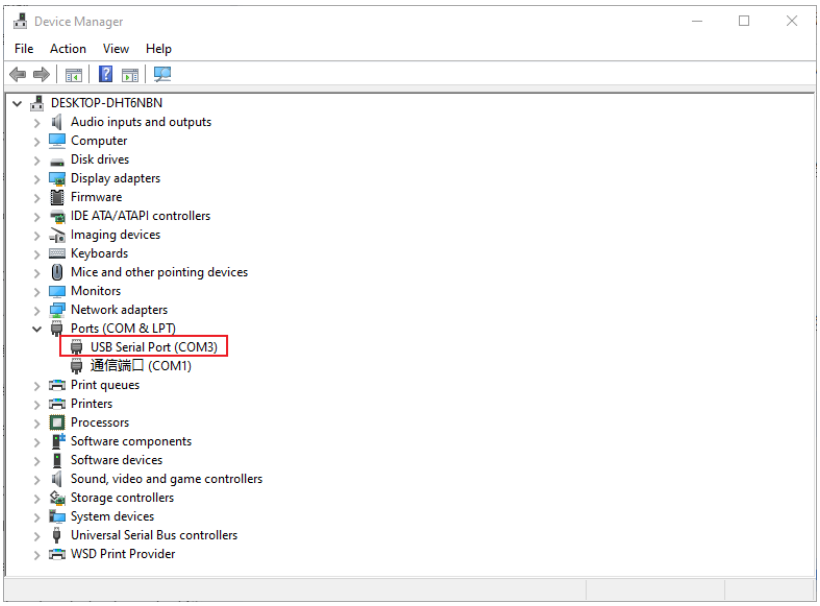
SSH login requires root privileges. The root password is unique to each device due to security concern. Please contact the Vantron FAE team to obtain it.

2.5 Debugging the Device (via Console Port)

G402 provides an RJ45 Console port for low-level debugging. This port provides direct access to the device as long as the hardware is intact—even if the network is misconfigured, the IP address is lost, network interfaces have failed, or the VantronOS web portal is inaccessible. All you need is a USB-to-RJ45 Console cable.

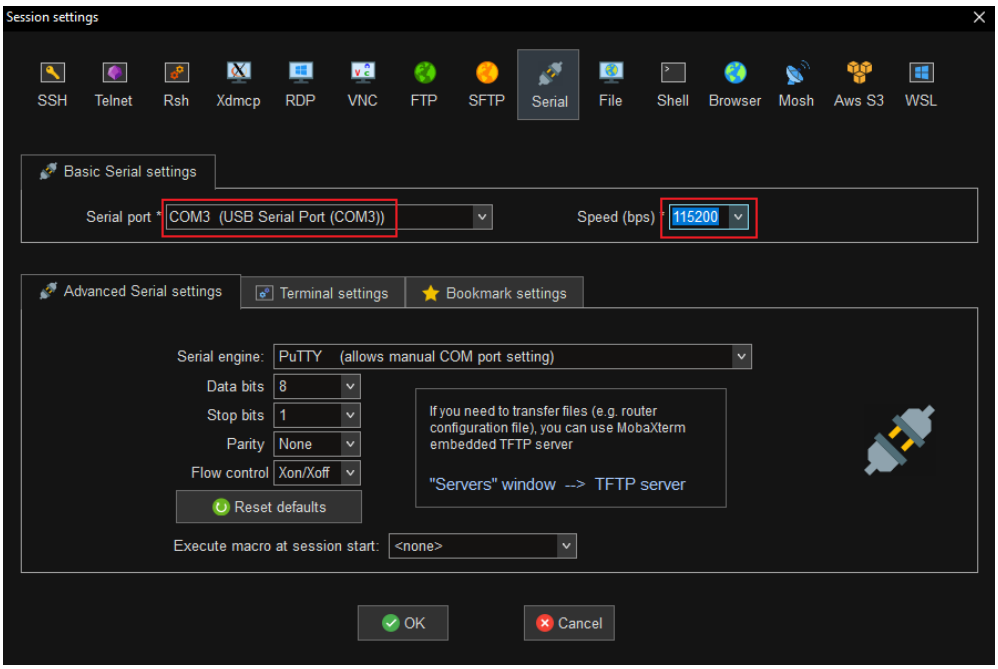
1. Connect G402 to the Windows PC using the USB-to-RJ45 Console cable.

2. Install the cable's driver on the PC depending on cable model.
3. Check **Device Manager** for the COM port number assigned to the cable.



4. Launch a serial terminal on the PC (PuTTY or MobaXterm is recommended).
5. Start a serial session.

6. Select the COM port identified by the host computer and select the 115200 baud rate.



7. Click **OK** to start the session.

2.6 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.

2.7 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 G402, 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.

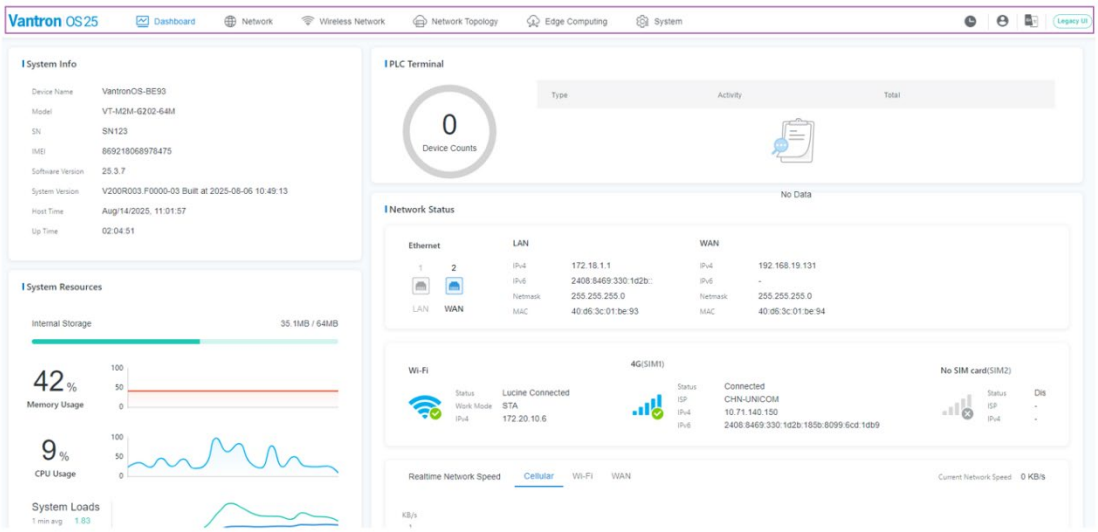
CHAPTER 3 DEVICE SETUP VIA VANTRONOS

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



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:

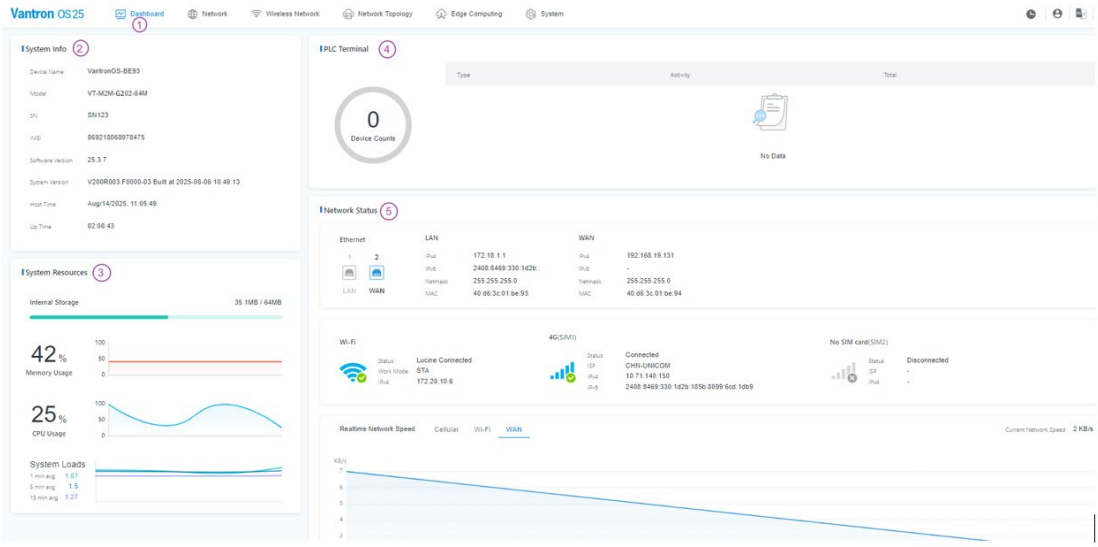
1. Click the user avatar in the upper right corner.
2. Select **Logout**.
3. Confirm the action by clicking **Logout** again.

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.



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

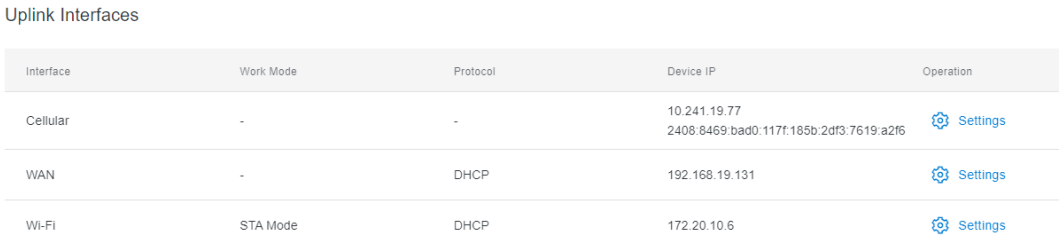
The **Network** menu centralizes critical network management functions, including interface settings, link redundancy, static routing, and more. These features enable precise control over connectivity, ensuring optimal performance and high availability. By integrating these tools, the system reduces 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 G402, 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



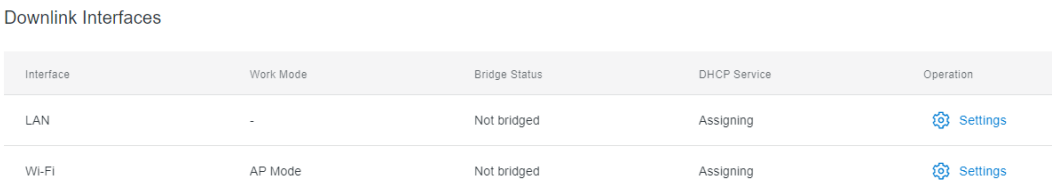
Clicking the **Settings** icon after the **Cellular** interface redirects you to the settings page of the cellular interface. Refer to section 3.4.1 for the details.

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.

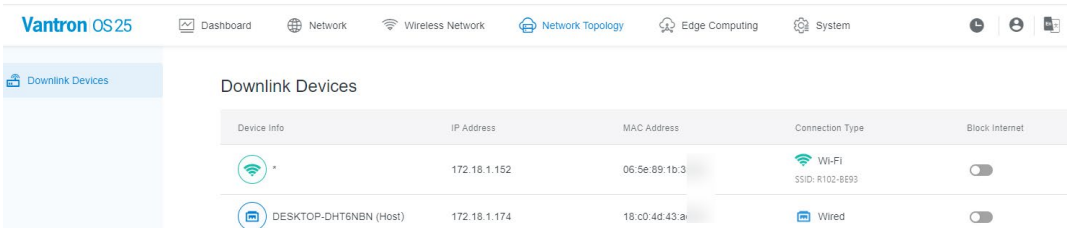
3.3.1.2 Downlink Interfaces



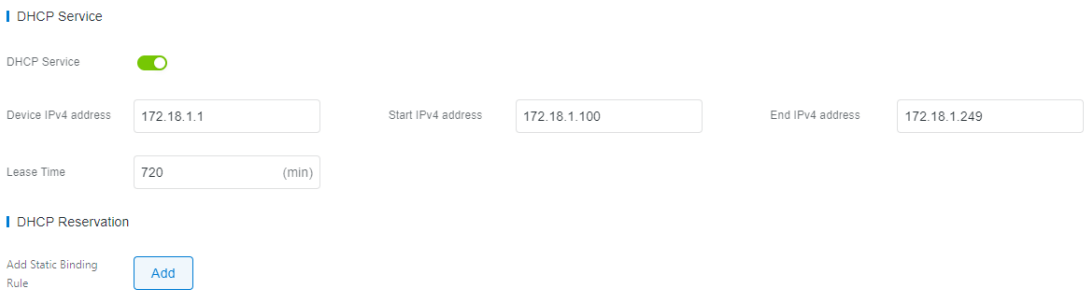
The **Settings** icons for the LAN and Wi-Fi AP interfaces allow you to select whether to bridge the interface to an uplink interface that connects to a DHCP server. If enabled, client devices connected to G402 through this link will receive an IP from the DHCP server. Refer to section 3.3.1.5 for the 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.



3.3.1.3 DHCP Service & DHCP Reservation



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**:

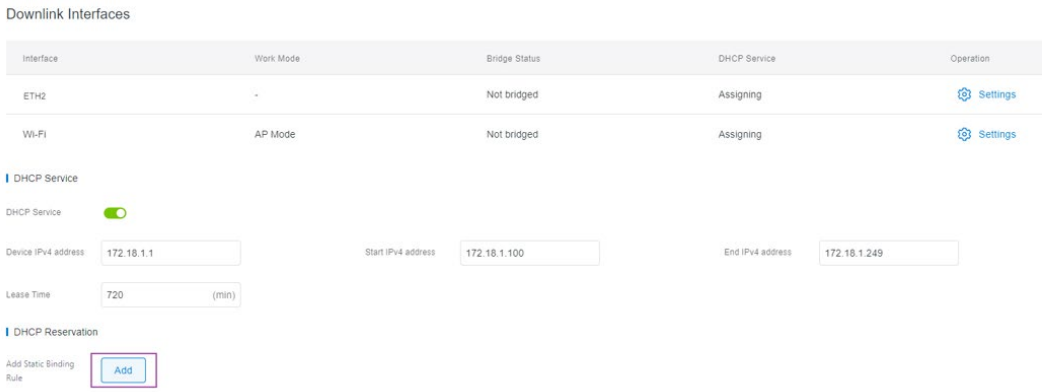
- Device IPv4 address: G402' own IP address on the downlink domain.
- Start & End IPv4 addresses: The pool from which addresses are leased to clients.
- Lease Time: The valid duration for which G402, as the DHCP server, assigns an IP address to a client. Before expiry of the lease time, the client will send a renew request to G402 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.

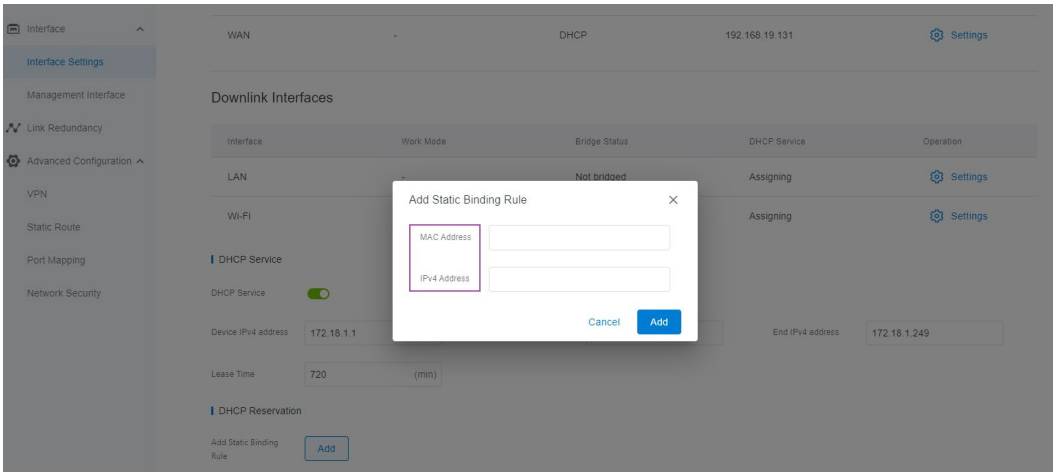
By adding a DHCP reservation rule to G402, the specified client device will maintain the allocated IP address to reduce configuration errors.

Steps of adding a DHCP reservation rule:

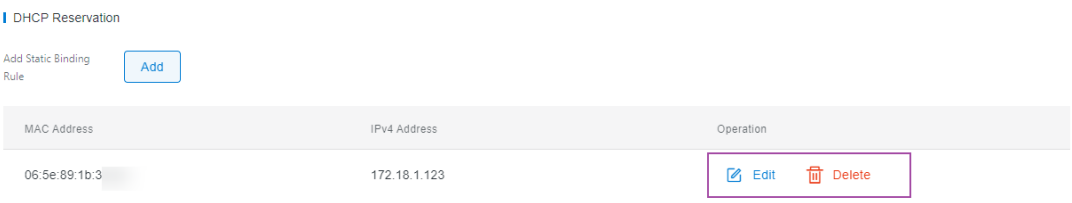
1. Click **Add** under **DHCP Reservation**.



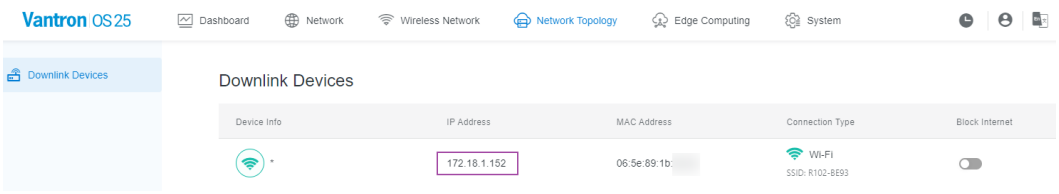
2. Enter the client's MAC address and allocate an IP between the start and end IPv4 addresses specified under **DHCP Service**.

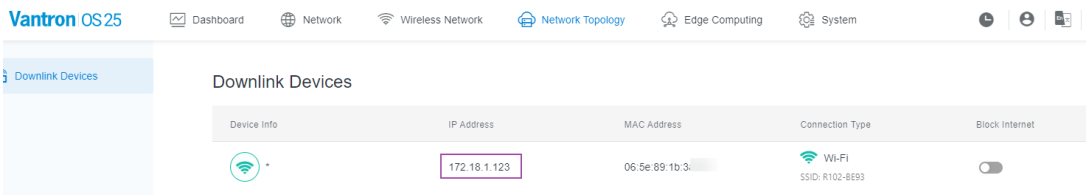


3. After adding the rule, you can edit or delete it as needed.



4. If you have assigned a fixed IP to the MAC address of a connected device, reconnect the device to G402, and its IP will update accordingly as shown under **Network Topology**.



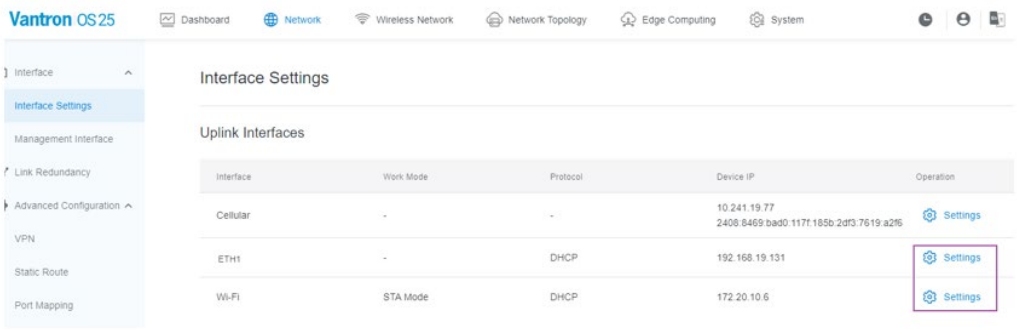


3.3.1.4 IP Configuration Mode

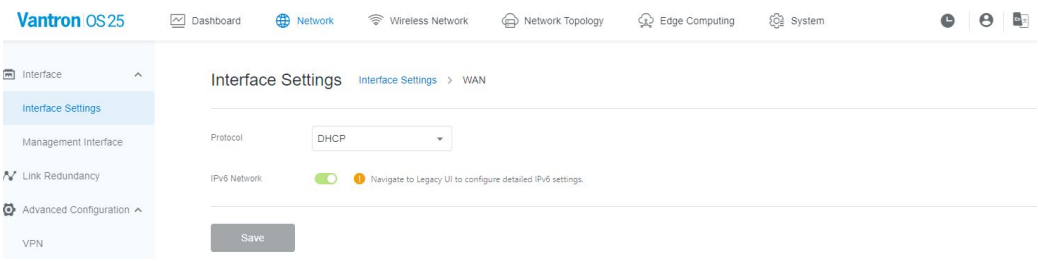
As described earlier, there are different IP configuration modes for uplink interfaces.

To select the IP configuration mode:

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

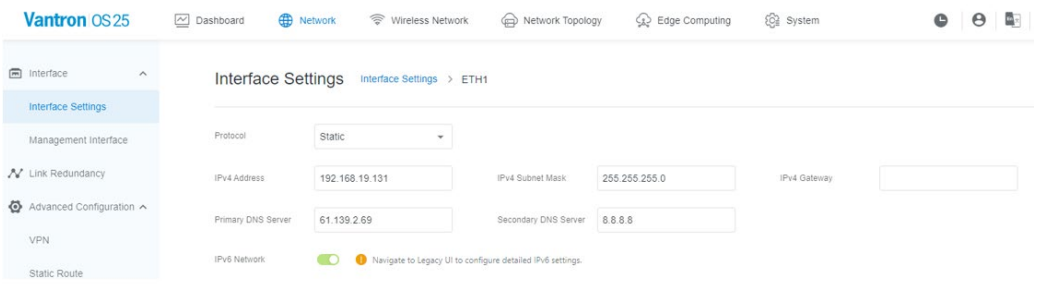


- **DHCP**: The DHCP server will **automatically** assign an IP address for the interface.



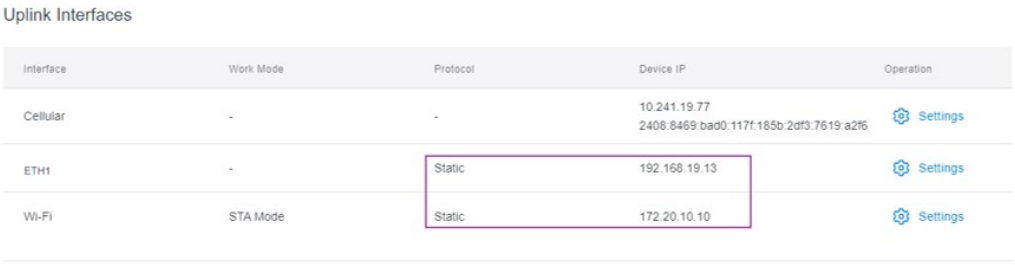
If you need configure IPv6, please navigate to **Network > Interfaces** on the legacy UI, and modify the settings of the target interface accordingly.

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



- **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 G402.



Ensure the host computer and G402 are on the same subnet for VantronOS login.

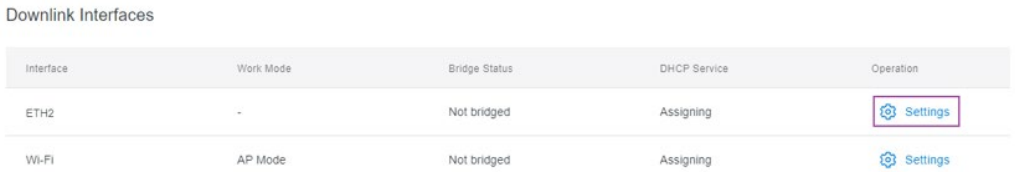
3.3.1.5 Interface Bridging

By enabling the bridge mode for a downlink interface (Ethernet LAN (ETH2)/Wi-Fi AP), both the bridged interface and uplink interface will on the same subnet, sharing the same broadcast domain:

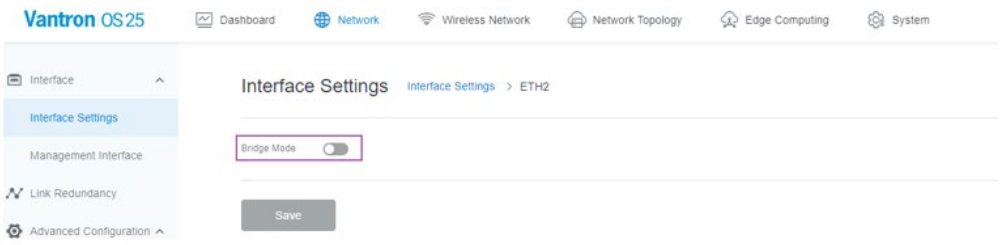
- Any device connected to the bridged interface is placed on the upstream network.
- G402 stops providing NAT or DHCP for that LAN (ETH2)/Wi-Fi interface. Instead, the upstream (WAN-side) DHCP server handles all client addressing.

To enable the bridge mode on a downlink interface:

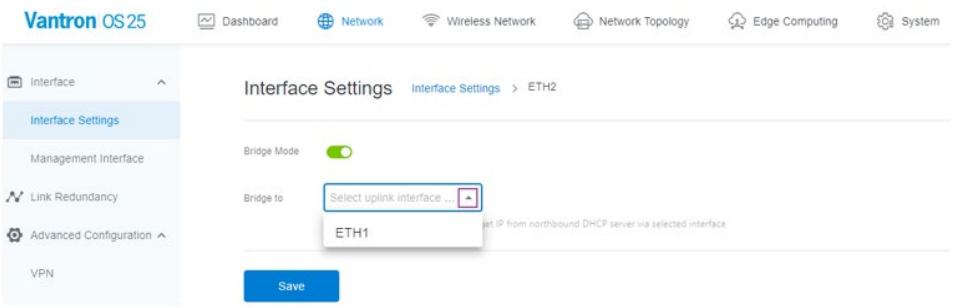
1. Click the **Settings** icon after a downlink interface (Ethernet LAN for instance).



2. Turn on **Bridge Mode**.



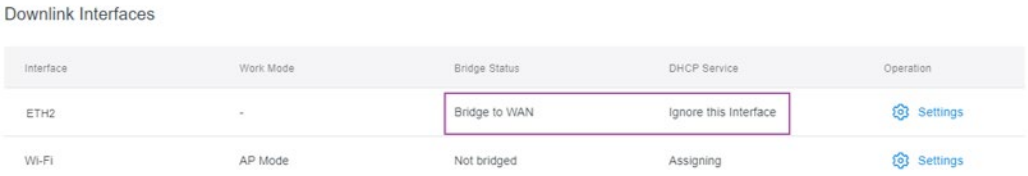
3. Select the uplink interface to bridge to, and click **Save**.



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 G402 are on the same subnet for VantronOS login.

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



3.3.2 Management Interface

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

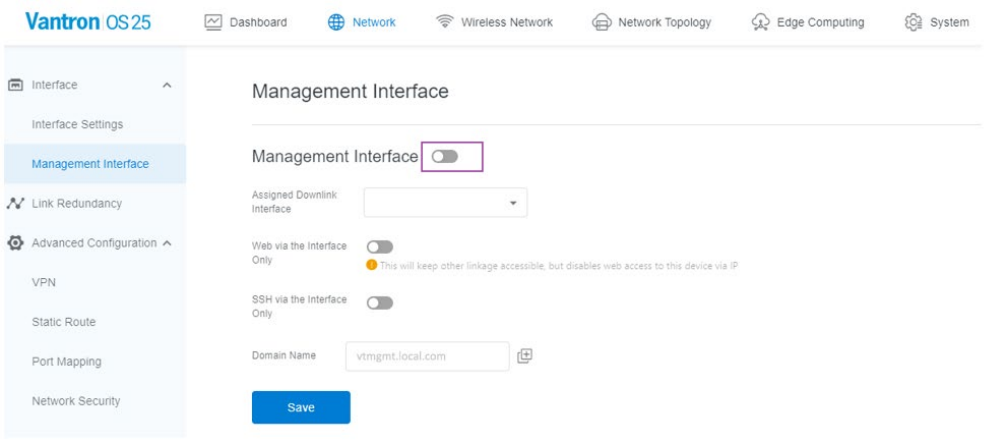
- If a management interface is selected and specified for web/SSH login, users can only manage the device through this interface (and its associated IP, 172.18.1.1 by default).
- If a management interface is selected without specifying it for web/SSH login, any downlink or uplink port may be used for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

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

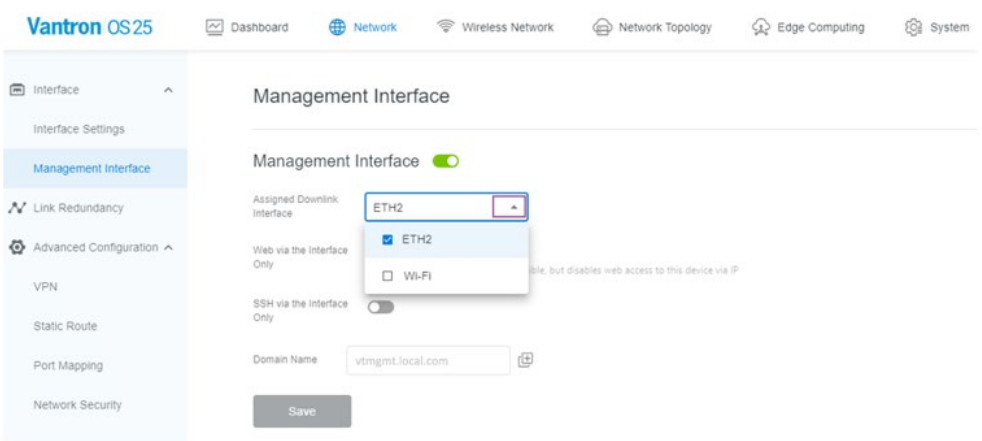
When "Web via the Interface Only" is enabled, only the specified domain name is accessible for VantronOS login; all other interface IPs (downlink and uplink) are inaccessible. Ensure the host computer has automatic DNS enabled to resolve the management interface's address.

To set a management interface:

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

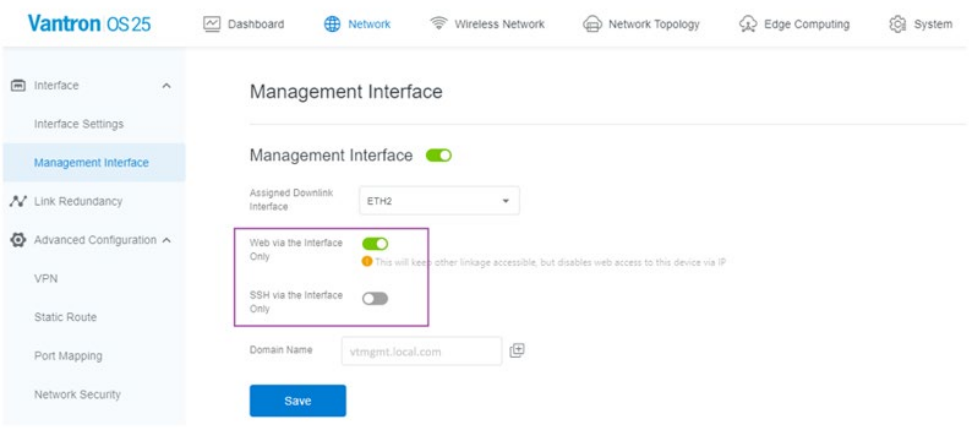


2. Select one downlink interface or both as the management interface(s).

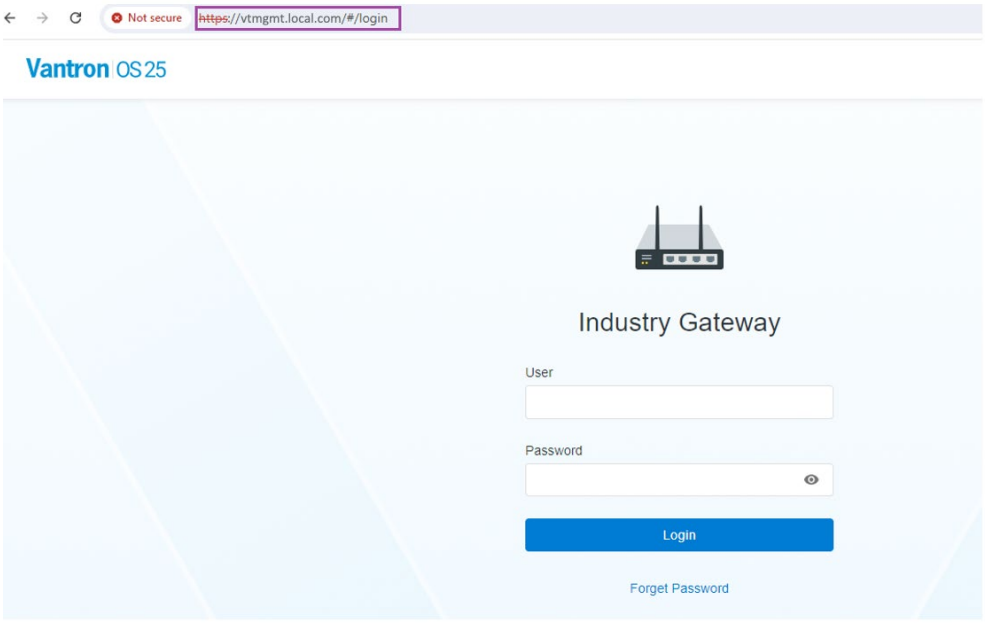


- **ETH2**: Ethernet LAN port
- **Wi-Fi**: Wi-Fi AP interface

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



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.



*If **SSH via the Interface Only** is enabled, other methods described in section 2.4 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.*

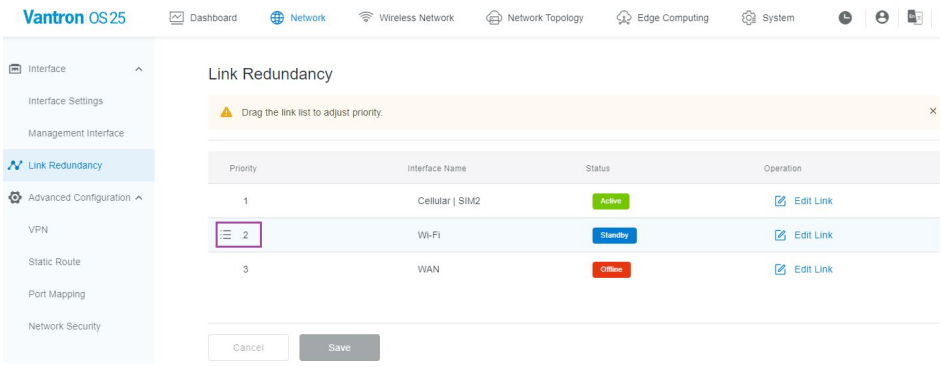
3.3.3 Link Redundancy

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.

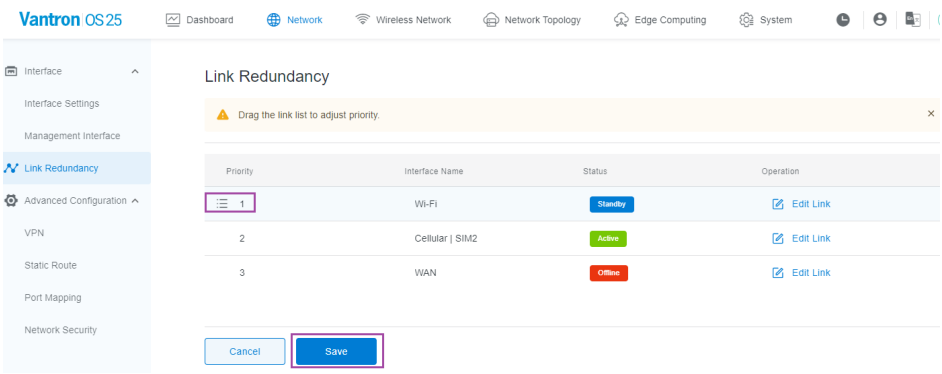
The default link detection and data forwarding are prioritized based on the following rule: Ethernet (WAN) > Wi-Fi (Client) > LTE > others.

To manually set the network priority:

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

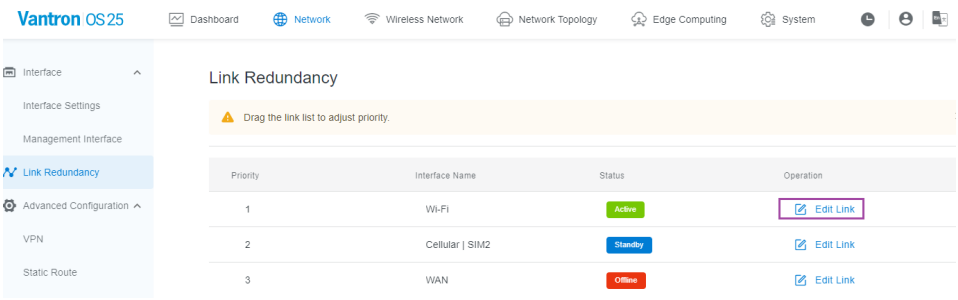


2. Drag the link up or down to the desired position, then click **Save**.



*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.



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. G402 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 in the configuration file 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 G402 gateways for the connection, make sure there is no IP conflict when they are in the same LAN.

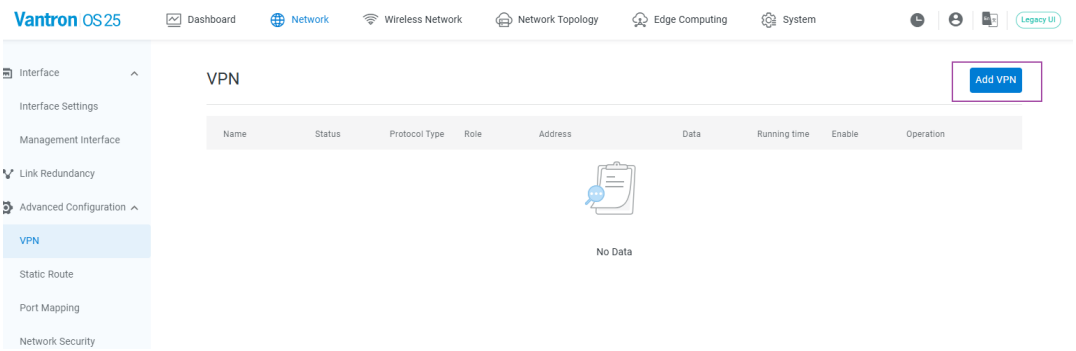
The port number specified in the client configuration's remote field must exactly match the listening port configured on the OpenVPN server.

3.3.4.2 OpenVPN Server Setup

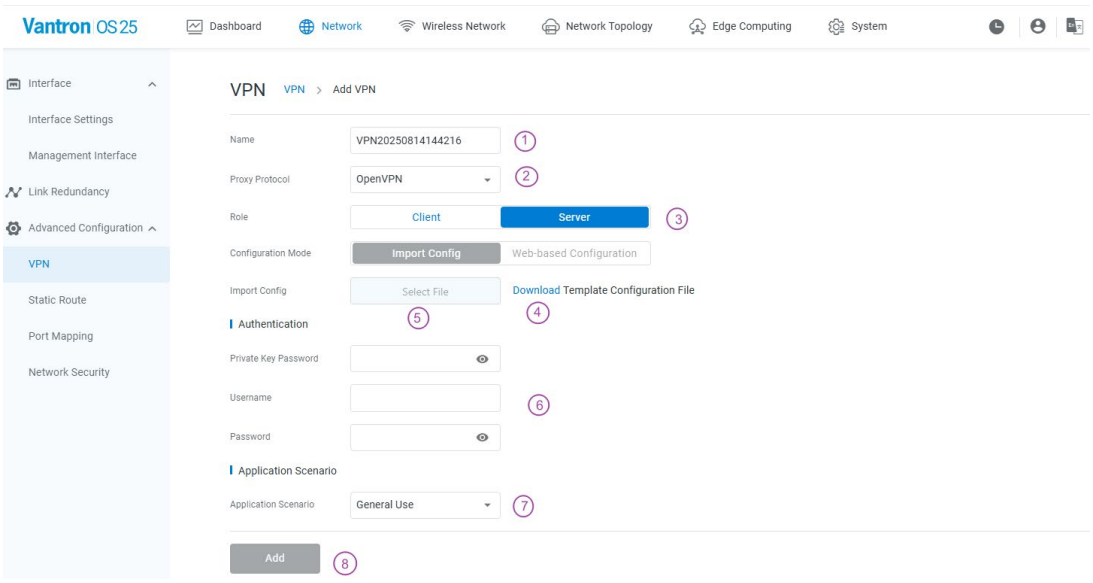
Please note that the configuration method provided here is for test only. You are recommended to modify the certificates and keys in the configuration file to your own.

To add an OpenVPN **server** rule for the current G402:

1. Synchronize both G402 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:



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.

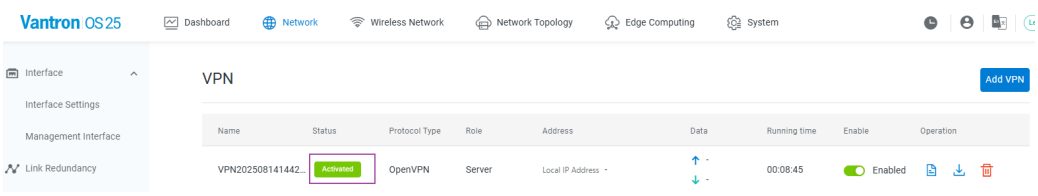
7) Select an application scenario.

   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.



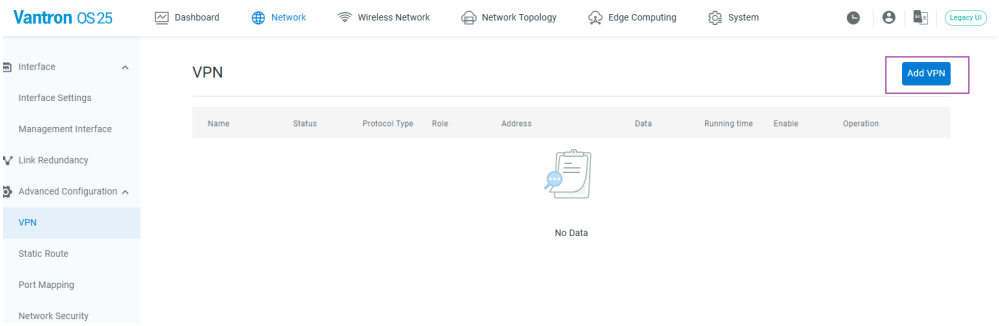
After setup, you can enable/disable the rule, view its logs, download its configuration, or delete it.

3.3.4.3 OpenVPN Client Setup

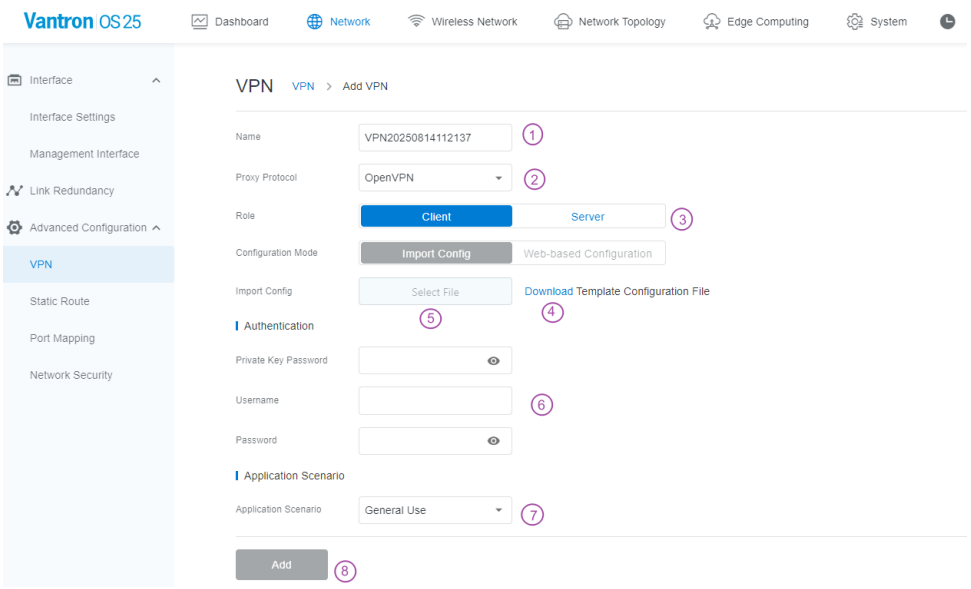
Please note that the configuration method provided here is for test only. You are recommended to modify the certificates and keys in the configuration file to your own.

To add an OpenVPN **Client** rule for the current G402 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 G402 and the server to the same NTP server.
3. Click **Add VPN** in the upper right side.



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



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).

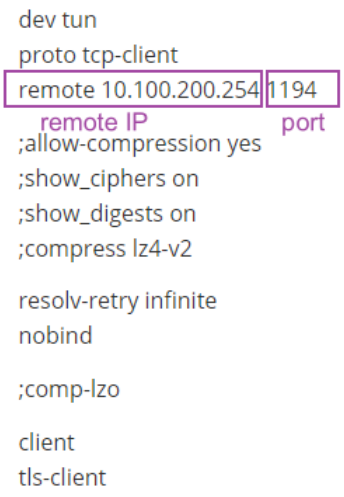
3) Select the **Client** role.

   *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.



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.

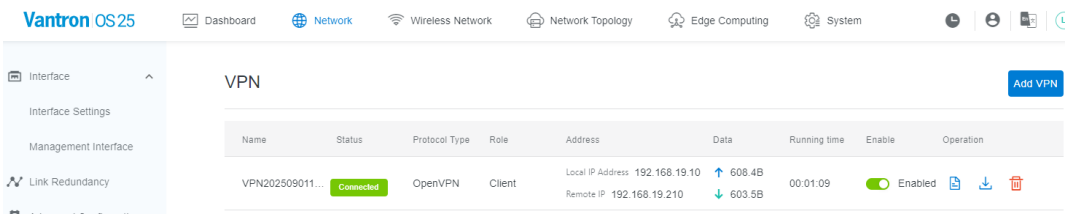
8) Select an application scenario.

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.

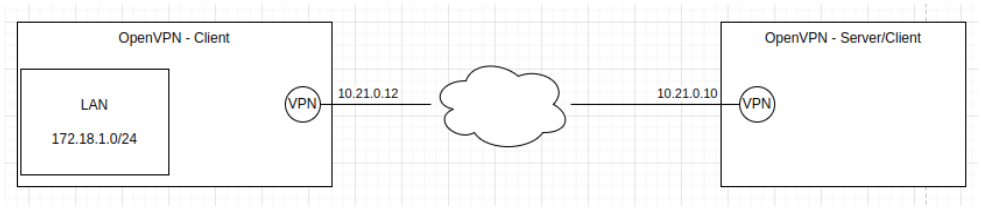
6. When device status changes to **Connected**, the device is successfully connected to an OpenVPN server as a client.



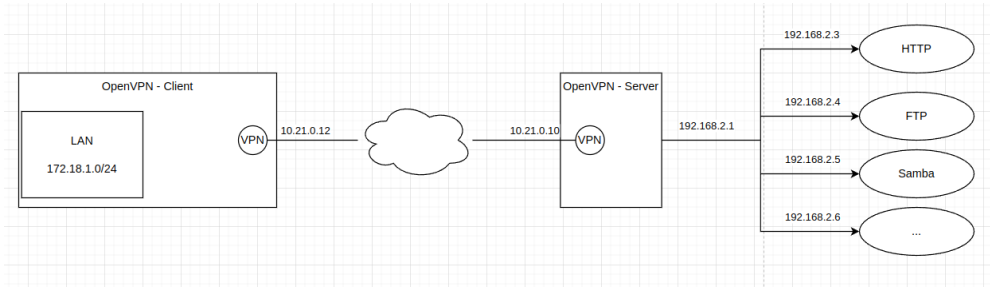
After setup, you can enable/disable the rule, view its logs, download its configuration, or delete it.

3.3.4.4 Application Scenario Topology

- General Use (point-to-point)

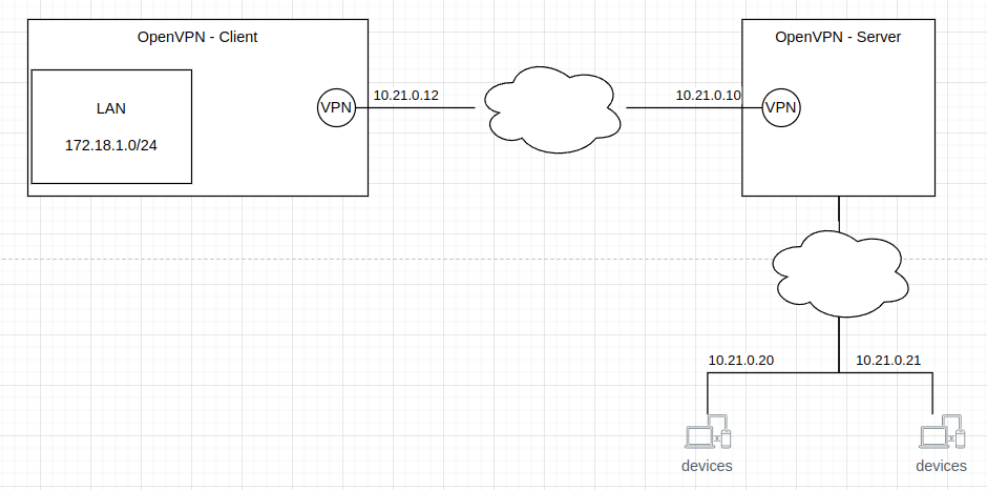


- Routing Mode (client-to-network)



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

- DNAT Port Forwarding (client-to-clients)

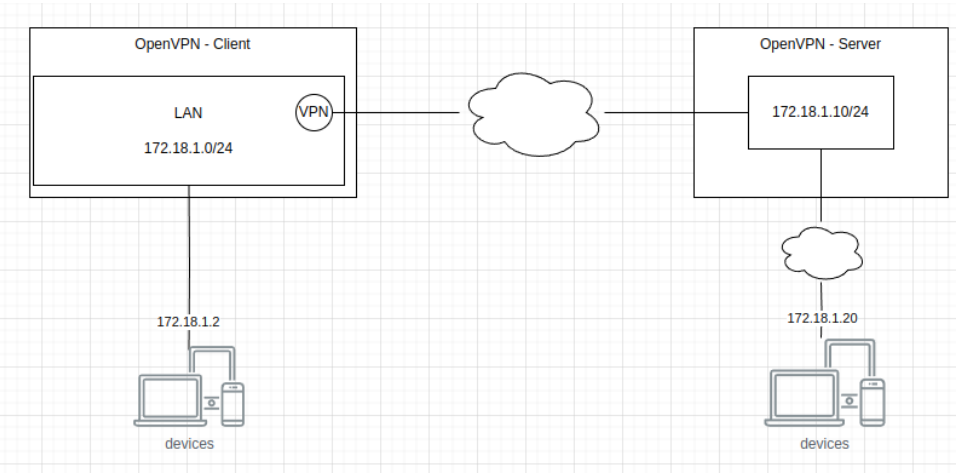


In this scenario, the OpenVPN client is assigned an IP: 10.21.0.12, on the same subnet as the remote devices (10.21.0.20 & 10.21.0.21). So, they can communicate with each other.

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

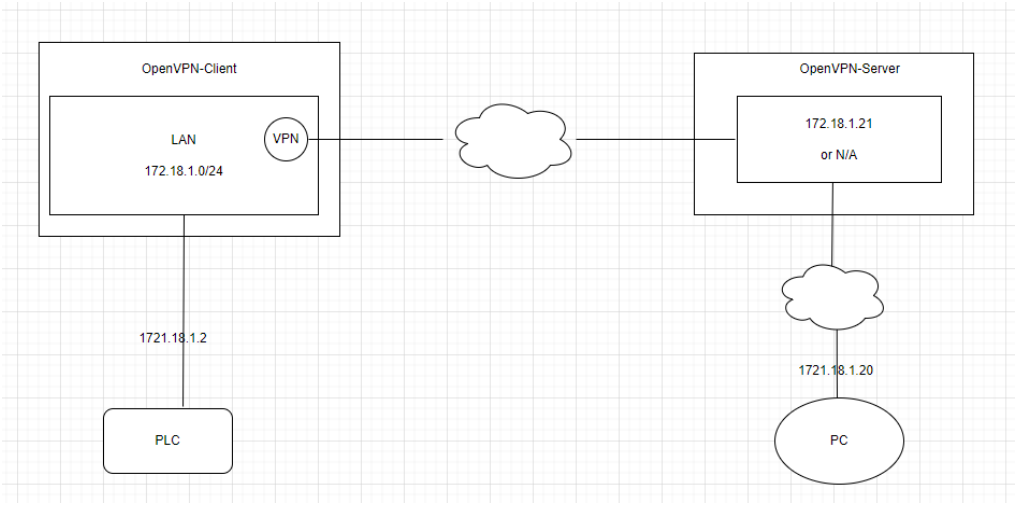
- Bridging Mode (clients-to-clients)

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.

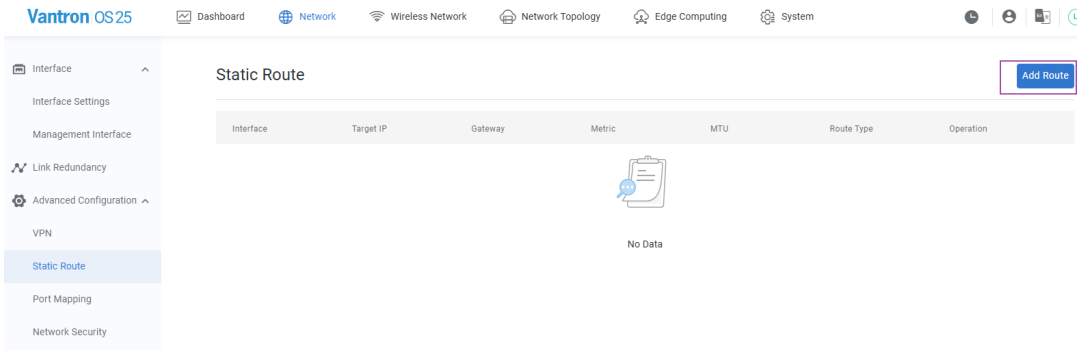
Example:

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

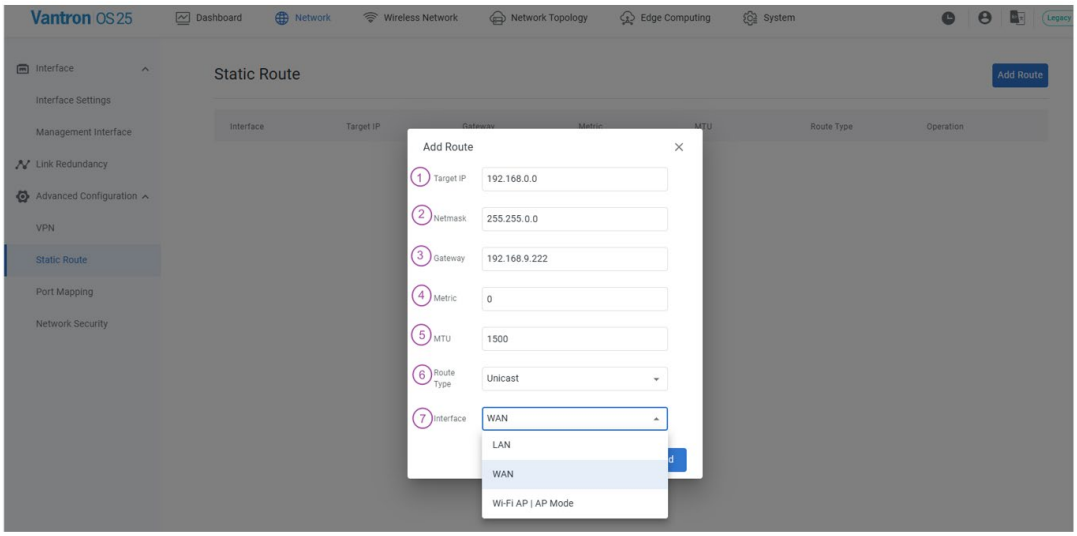
Goal: When the gateway has both 4G and WAN network connection, route the internal network (192.168.0.0 - 192.168.255.255) traffic through the Ethernet WAN interface, and all other data traffic via the 4G interface.

Steps:

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



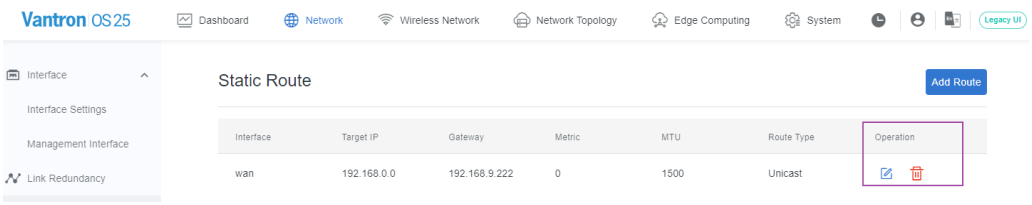
2. Configure the rules for the route:



Description of the numbered areas

1) Input the destination IP address.
2) Input the subnet mask (e.g., 255.255.0.0 = /16 = 192.168.0.0 - 192.168.255.255).
3) Input the address of the upstream router.
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 (the interface that leads to the gateway, WAN in this case).

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



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.

Example:

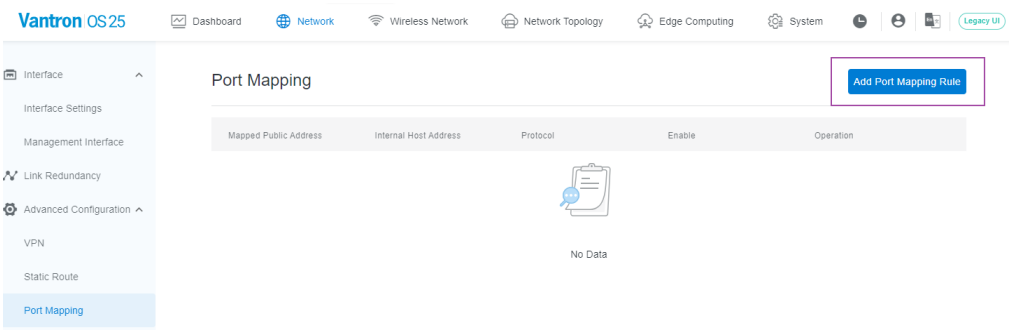
Scenario:

- G402 has both an internal zone (e.g., Wi-Fi AP) and an external WAN zone (e.g., Ethernet WAN) configured, with NAT enabled from internal to external.
- Port mapping (Destination NAT) operates based on this NAT boundary.

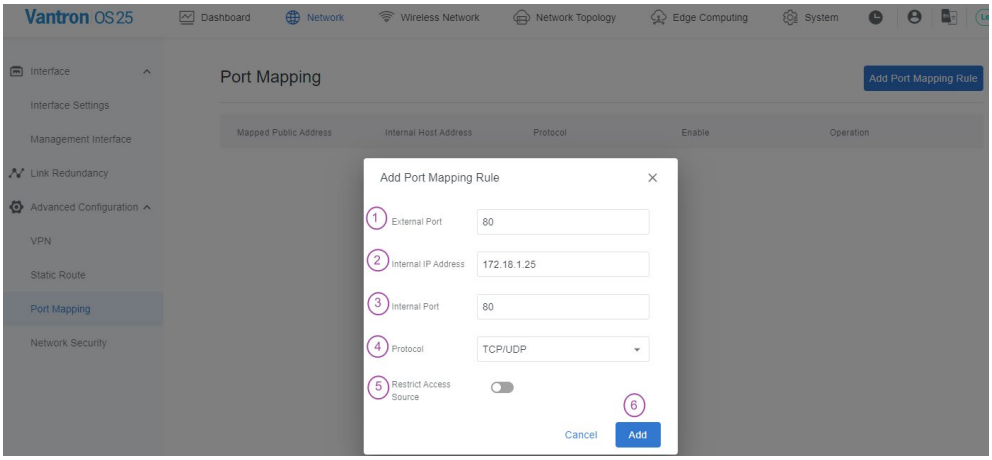
Goal:

- Allow external users to access the internal service (on port 80) by connecting to the WAN IP (on port 80).

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



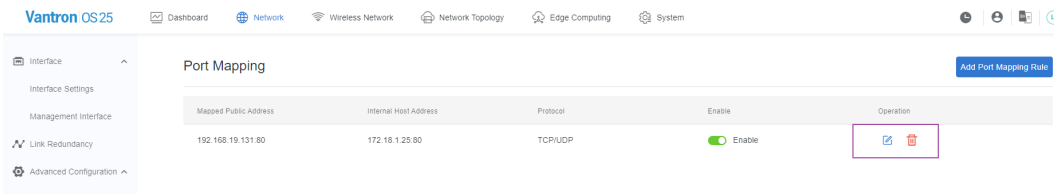
2. Fill in the rule information.



Description of the numbered areas

1) External port – The port number on the WAN side that outsiders will use to connect (e.g., 80).
2) Internal IP – The IP address of the target host (the internal device that provides the actual service).
3) Internal port – The port the target host is actually listening is actually listening for the service (e.g., 8080).
4) Protocol – The protocol used by the service (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.



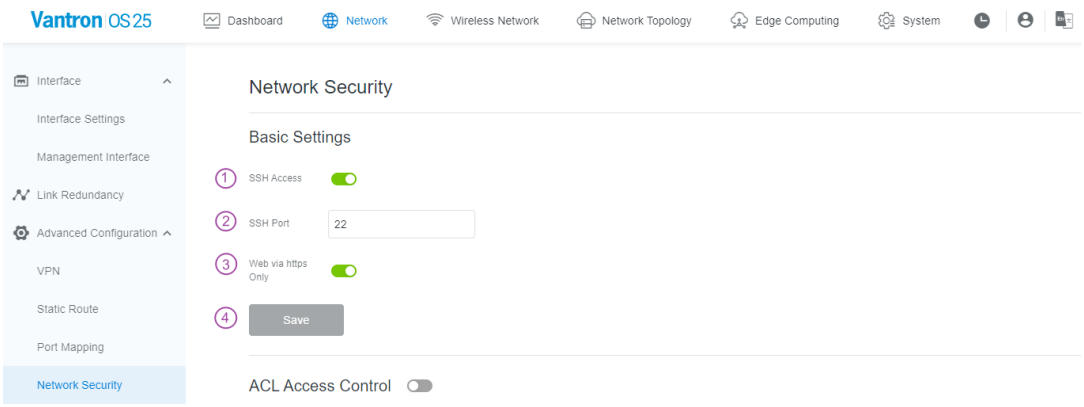
Note: *The mapped public address is determined by your WAN connection and may change.*

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



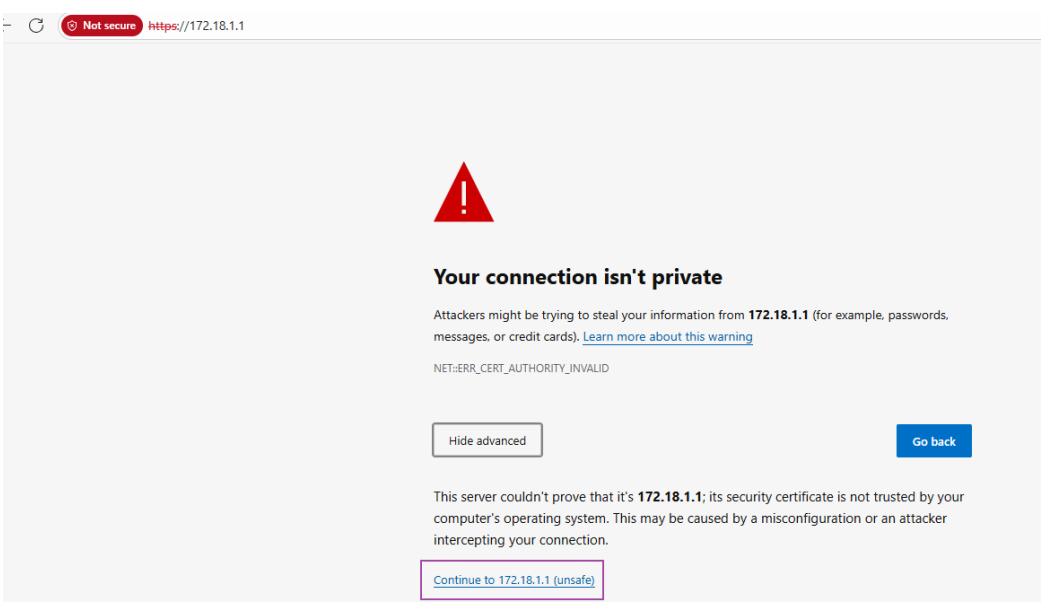
Description of the numbered areas

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

   Refer to 2.4 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.



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

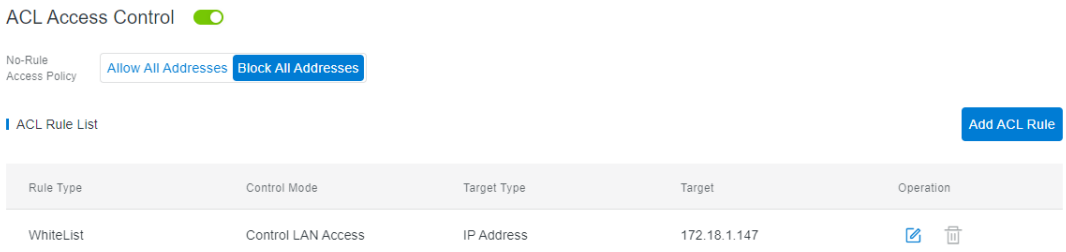
3.3.7.2 ACL Access Control

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.

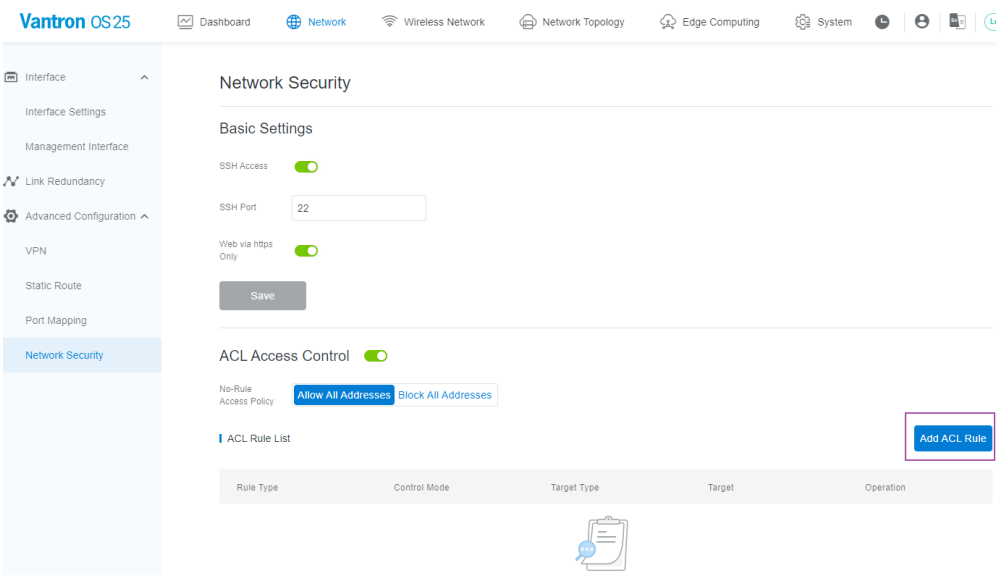
Block all addresses: When enabled, this policy **denies all WAN-side access**—only whitelisted IPs can reach the device—and **prevents** LAN-side devices from using it to **reach the WAN**. If no whitelist rules exist at activation, the device automatically adds the host computer's current IP to prevent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



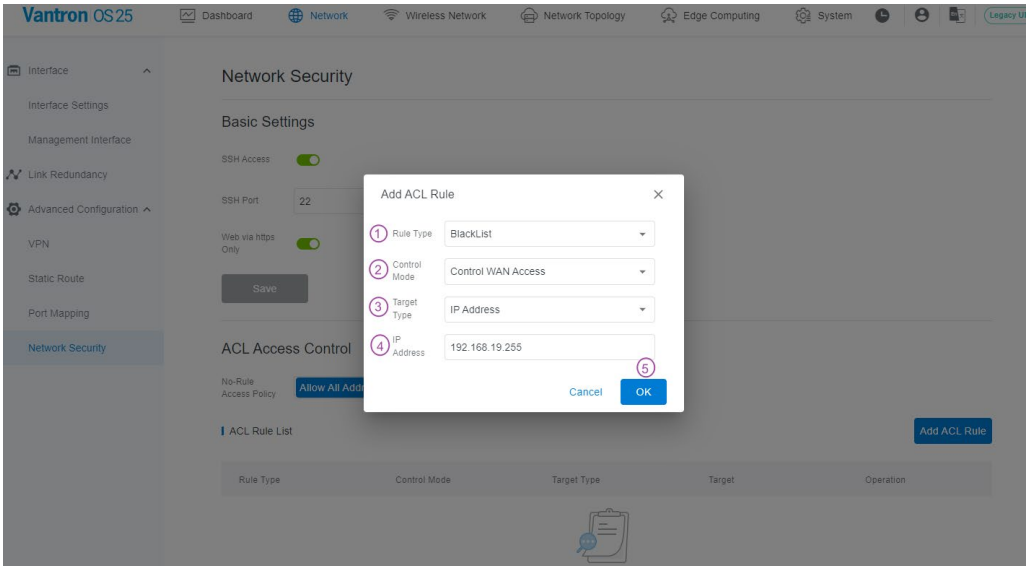
- **ACL Rule List**

To add an ACL rule:

1. Click **Add ACL Rule**.



2. Configure the rule in the pop-up.



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).

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

5) Click **OK** to complete.

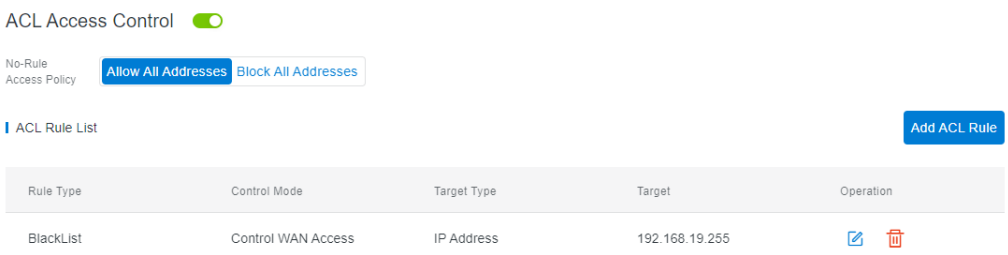
Description for the rule settings:

Rule Type	Control Mode	Target Type	Result
Whitelist	WAN	IP address (Source)	The designated WAN IP has access to G402 or its LAN devices.
		Destination IP/ URL/URL keyword	G402 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.

Rule Type	Control Mode	Target Type	Result
Blacklist	WAN	IP address (Source)	The designated WAN IP is blocked from accessing G402 or its LAN devices.
		Destination IP/ URL/URL keyword	G402 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.

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



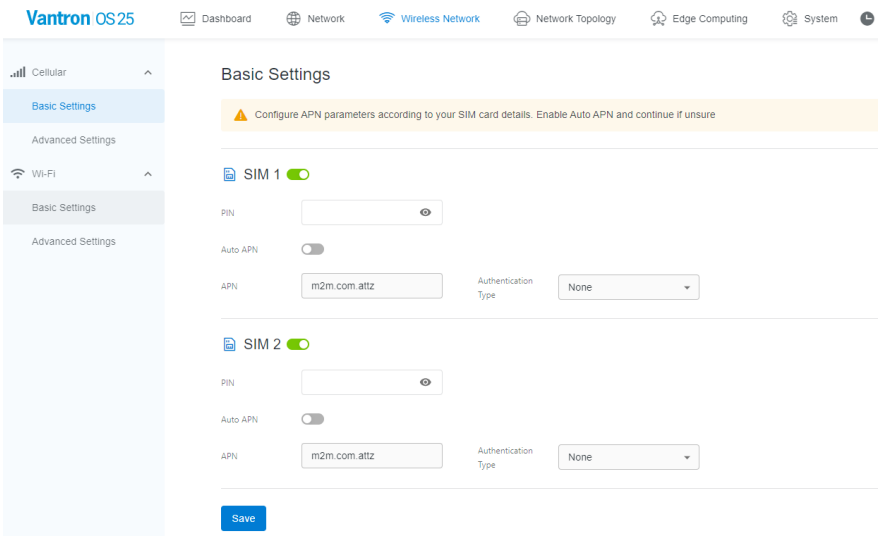
3.4 Wireless Network

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

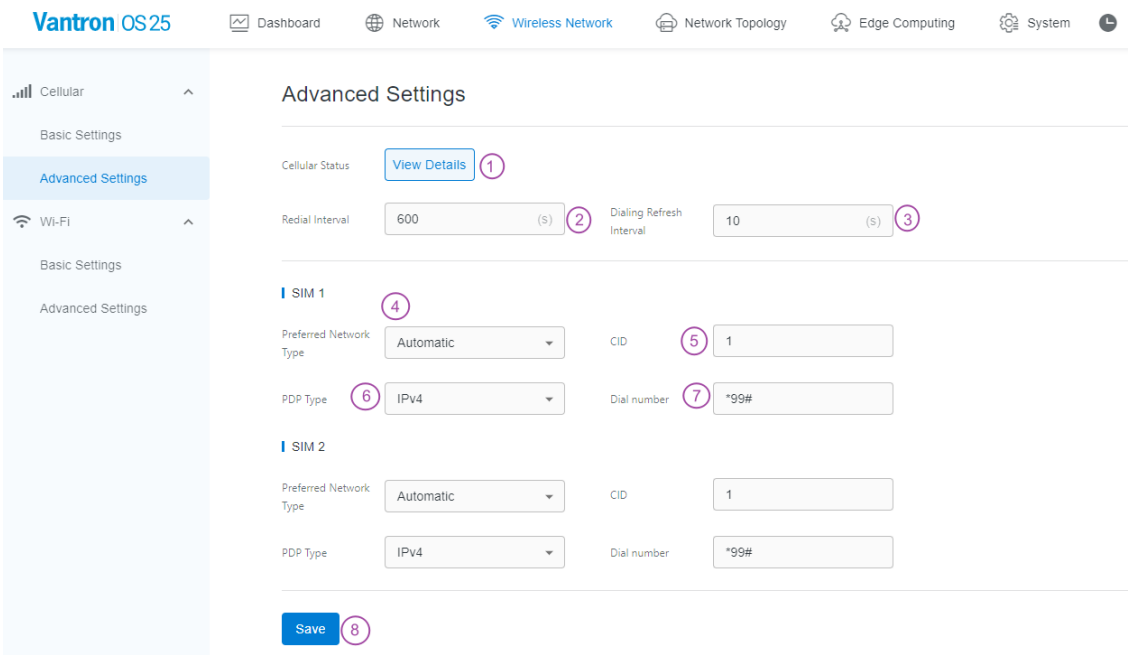
3.4.1 Cellular

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**.

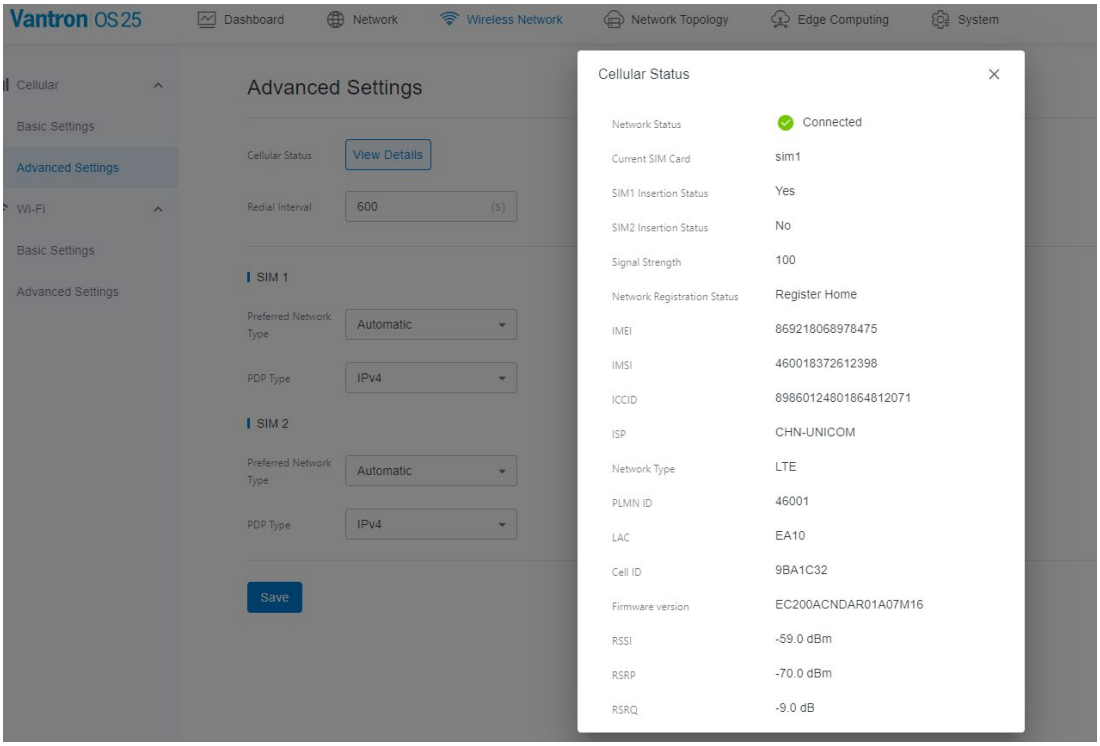


Advanced Settings:



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.



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.

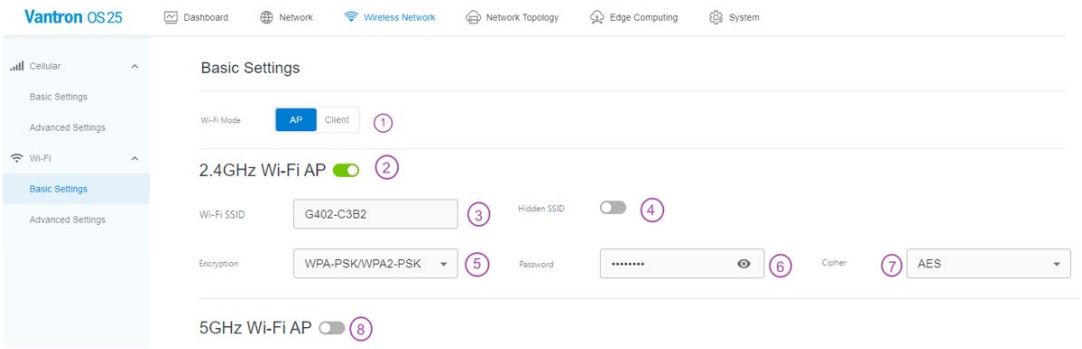
8) If you have made any changes, click **Save** to apply.

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.

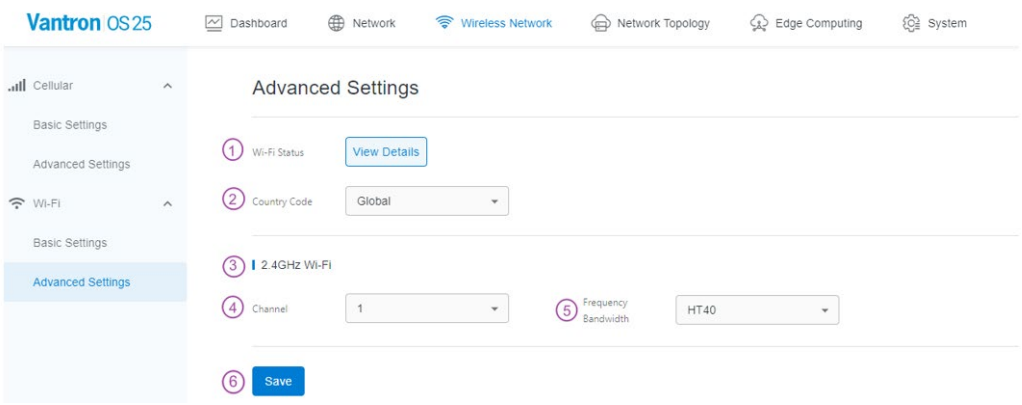
AP-mode basic settings:



Description of the numbered areas

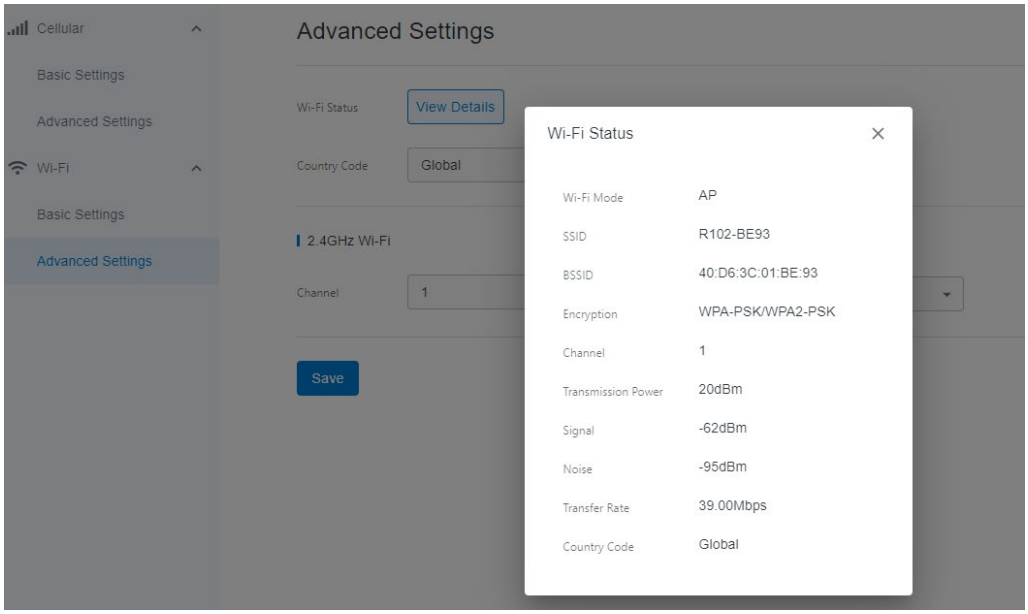
1. Operation mode switch between AP and client: Selected mode is shown in dark blue. A prompt message will display to confirm your operation.
2. G402 supports dual-band Wi-Fi, and 2.4GHz Wi-Fi is enabled by default.
3. Wi-Fi SSID—The Wi-Fi AP's name.
4. Hide SSID—Once hidden, clients cannot scan the device's SSID and must manually enter the exact name and password to connect.
5. Encryption—The basic protocols for establishing secure communication. (None, WPA-PSK, WPA2-PSK, WPA/WPA2-PSK)
6. Password—Credential for connecting the device's Wi-Fi.
7. Cypher—The algorithm that performs the encryption & integrity check.

AP-mode advanced settings:



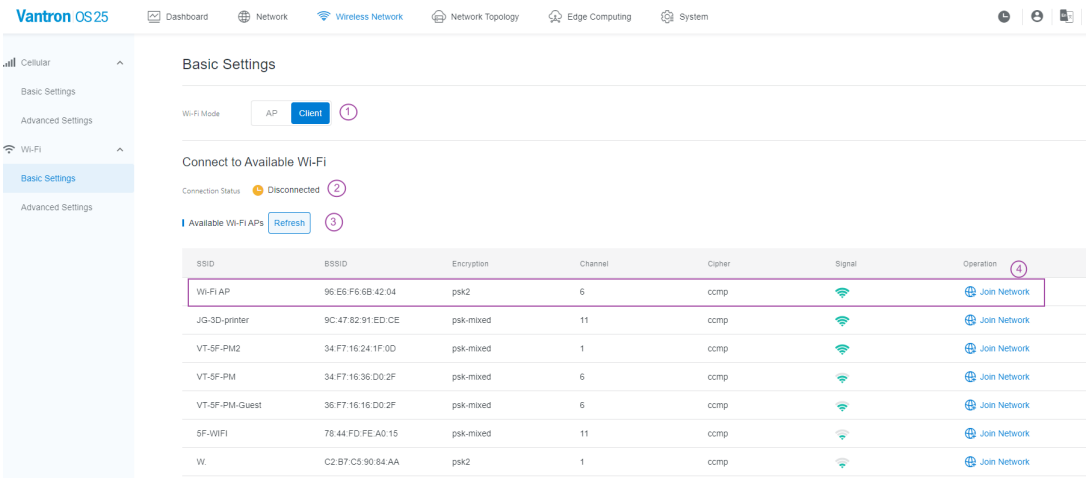
Description of the numbered areas

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.



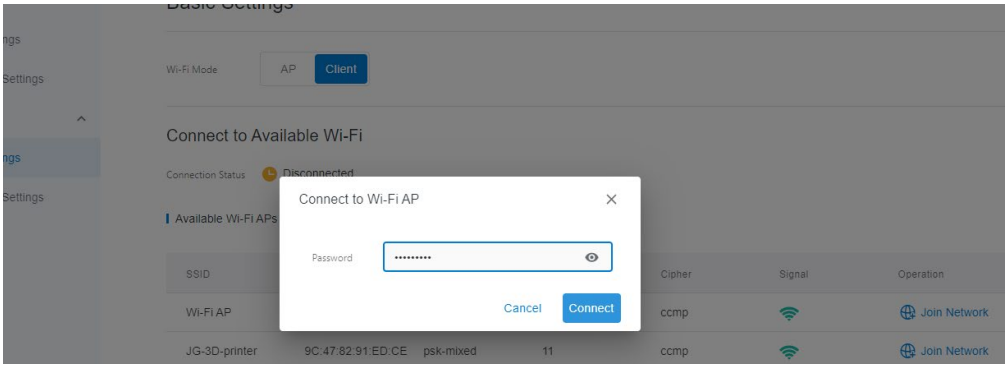
2. Country code (‘global’ by default)
3. Here displays the band selected in the basic settings
4. Channel options
5. Frequency bandwidth (‘HT40’ by default)
6. If you have modified the parameters, click **Save** to apply.

Client-mode basic settings:



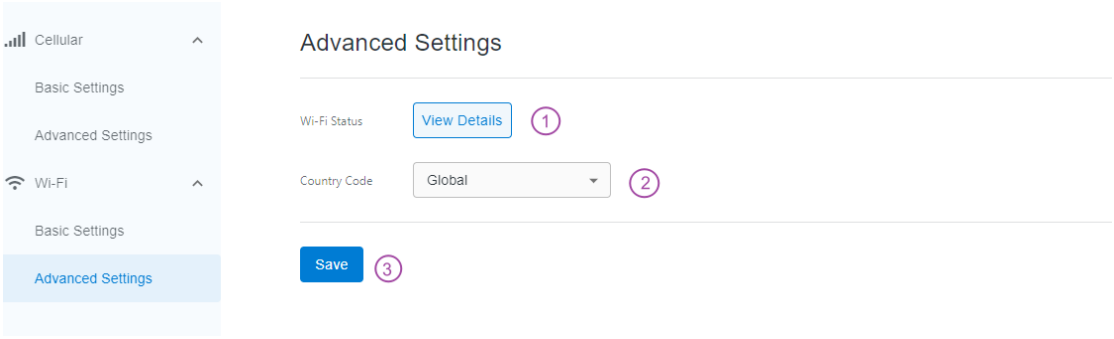
Description of the numbered areas

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 the button to refresh the list.
4. Information of available Wi-Fi APs is displayed. Click **Join Network** and enter the password to connect to the target AP.



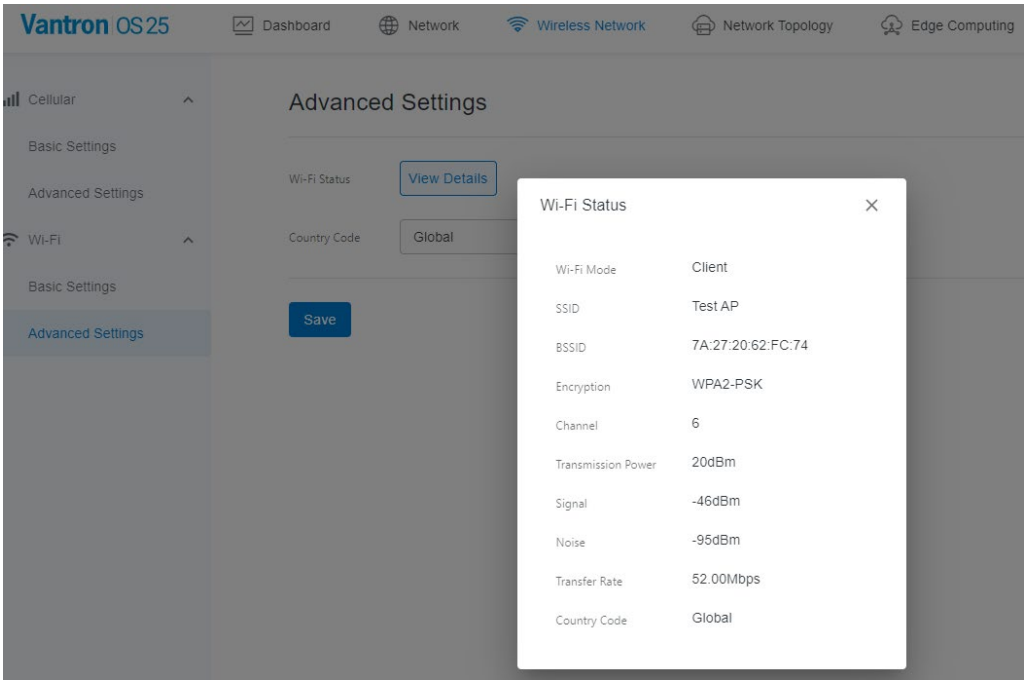
*The connection status will change to **Connected** with corresponding SSID upon successful connection.*

Client-mode advanced settings:



Description of the numbered areas

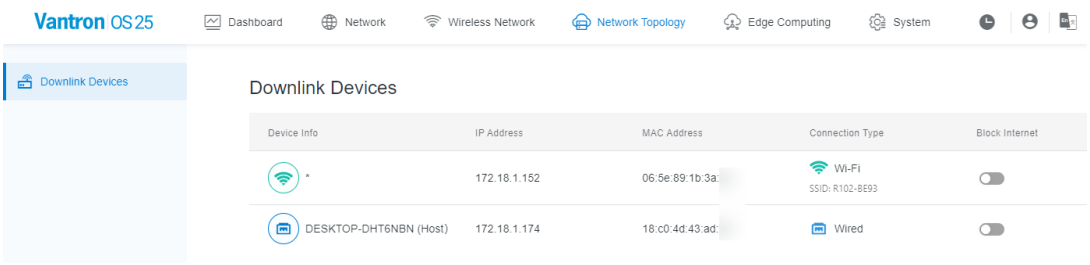
1. Wi-Fi Status—Clicking **View Details** will display the detailed connection information of the device, including Wi-Fi mode, and—if connected—the SSID of the target AP, encryption, channel, transmit power, etc.



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.



3.6 Edge Computing

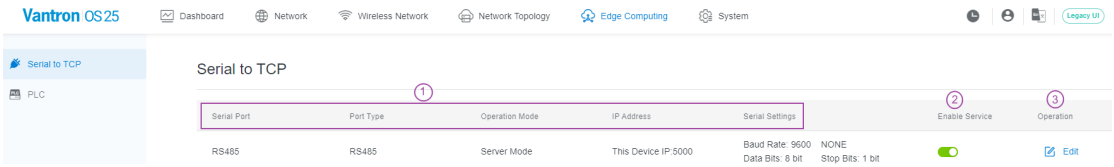
3.6.1 Serial to TCP

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.



Description of the numbered areas

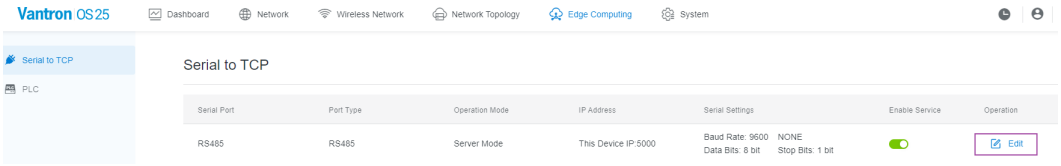
1. Details of the conversion rule, including the serial port name and type, current operation mode, IP address of the device + port, and serial parameters.
2. Enable/disable the rule
3. Edit the rule

Default parameters of the serial ports: 9600, 8N1

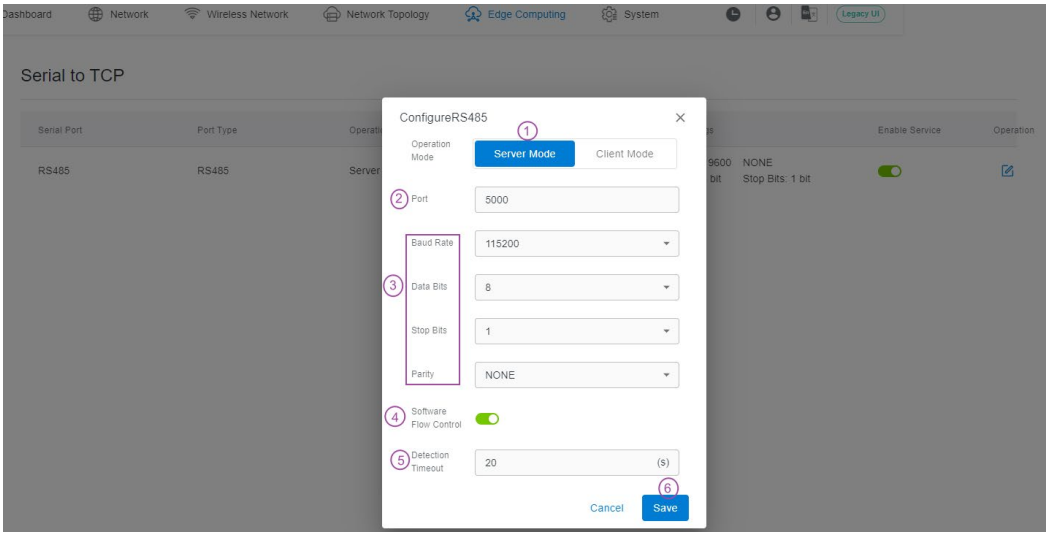
The serial ports are multiplexed as both RS485 and RS232. The mapping relationship between the software interface and the hardware interface is shown below:

3.6.1.1 Server Mode Rule Setup

1. Select a rule, and click the edit icon after the rule.



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



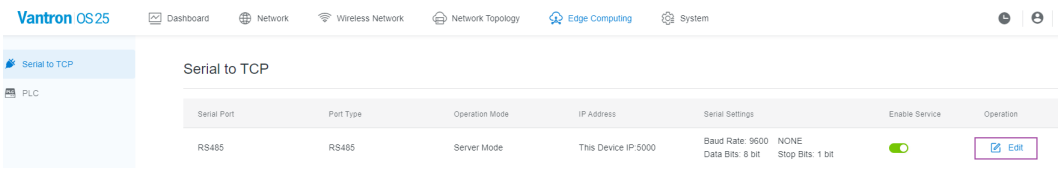
Description of the numbered areas

1) Select a serial mode for the multiplexer.
2) Select **Server Mode.**
3) Designate a TCP port to listen to (0~65535). Make sure the port on both the server and client are the same.
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 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.

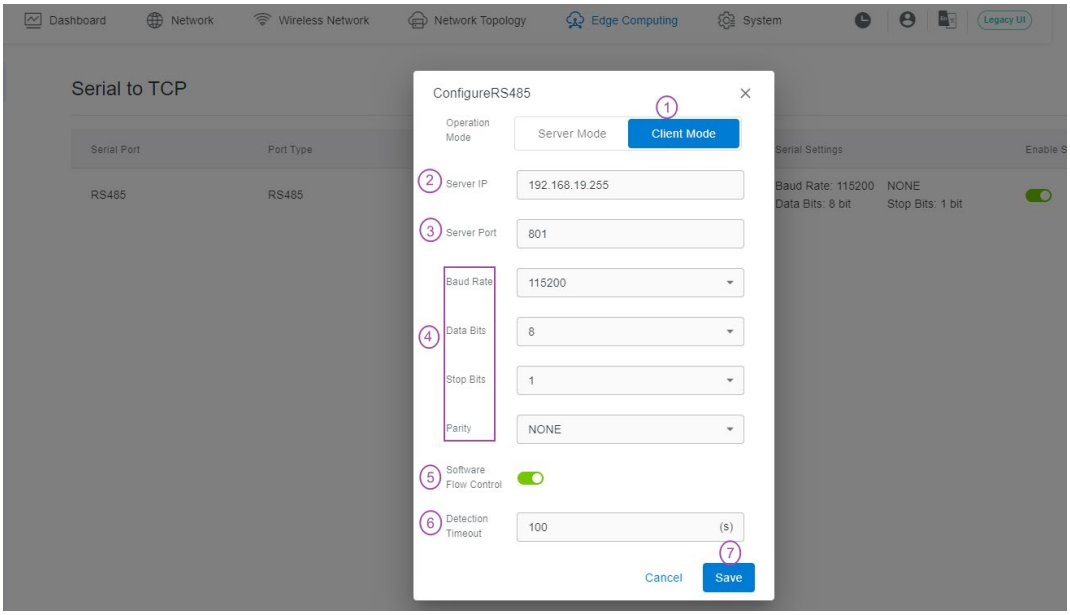
3. Enable the conversion rule.
4. Make sure both the client and server are on the same reachable IP network.
5. Verify the data transmission between the devices.

3.6.1.2 Client Mode Rule Setup

1. Click the edit icon after the rule.



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



Description of the numbered areas

1) Select a serial mode for the multiplexer.
2) Select **Client Mode.**
3) Enter the IP of the server.
4) Enter the target port and make sure it matches the TCP port on the server.
5) Make sure the serial parameters on both the peripheral and gateway are set the same.

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

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

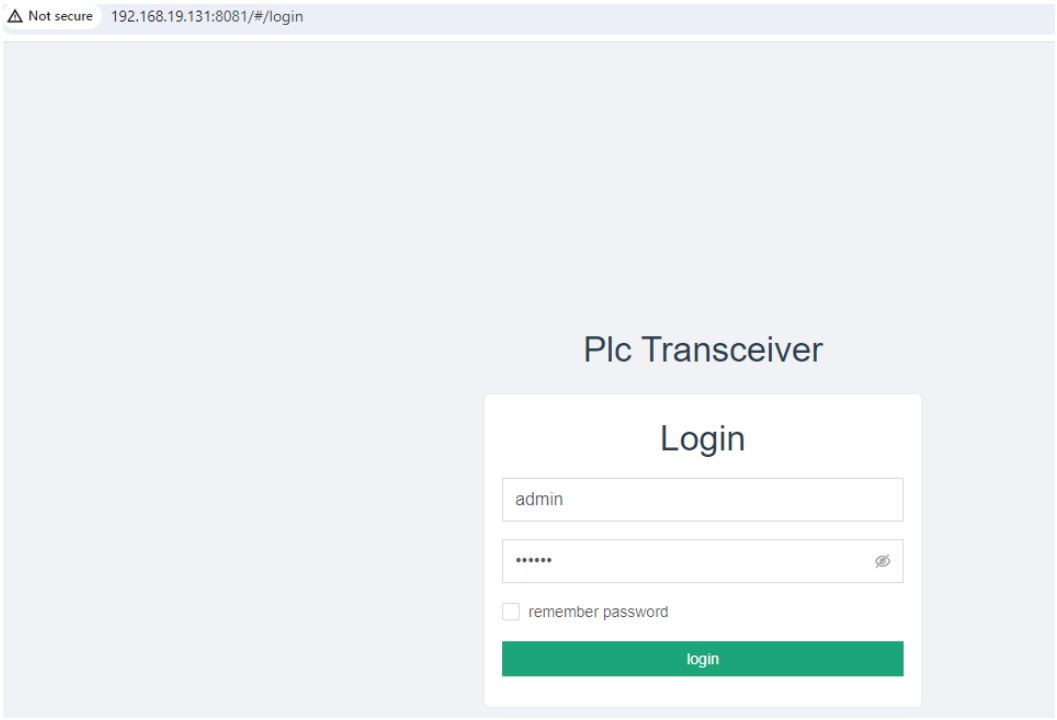
8) Save the changes to let them take effect.

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

G402 supports a wide range of edge-computing protocols. Southbound protocols include Modbus TCP, Modbus RTU, EtherNet/IP, ISO-on-TCP, CC-Link, etc. Northbound protocol primarily includes MQTT.

Clicking **Edge Computing > PLC** in VatronOS opens the industrial-protocol configuration portal, where users can precisely set every parameter related to G402 and the associated PLCs (protocol type, station address, register address, data mapping, polling interval, etc.) to achieve seamless integration with the field bus.



Refer to Chapter 4 for the detailed information.

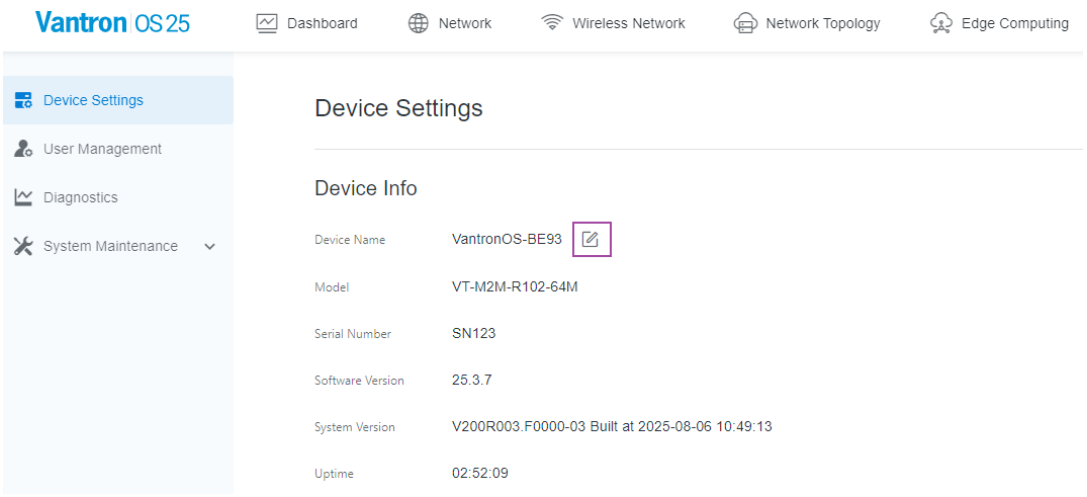
3.7 System

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.

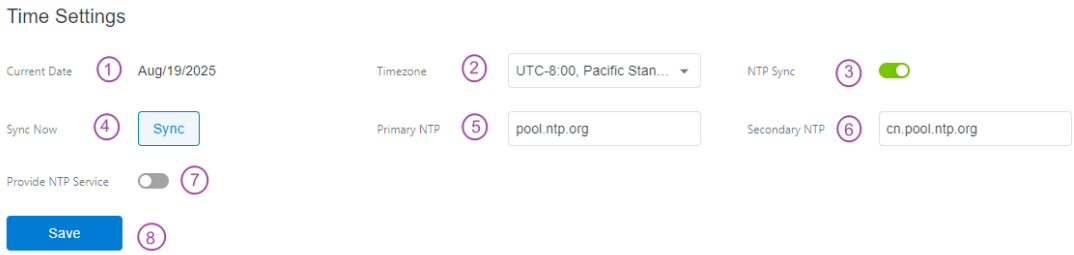


To modify the device name:

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.

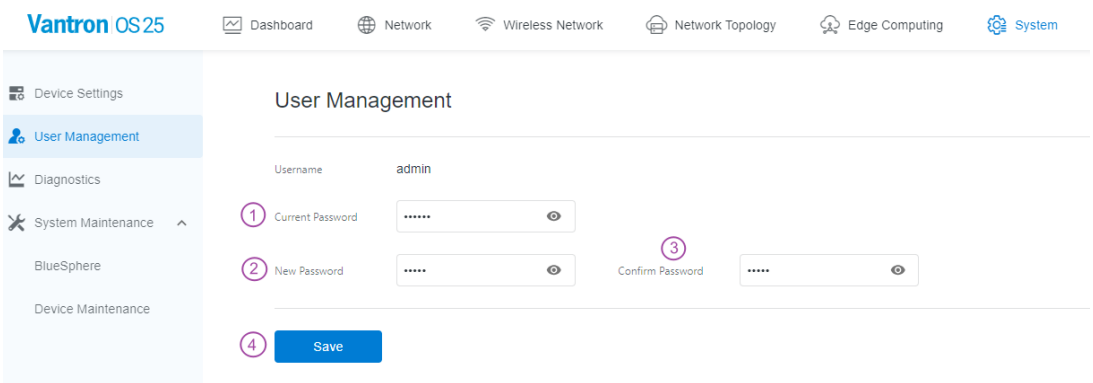


Description of the numbered areas

1. Current Date—Displays today's date for the selected time zone or the host PC's local time (after **Sync Local Time**).
2. Time Zone—Users can choose the desired time zone from the drop-down list.
3. NTP Sync—Toggles automatic time synchronization with NTP servers. The date resets after every power cycle because G402 lacks an RTC.
4. Sync Now—Triggers a one-time NTP update immediately.
5. Primary NTP—Preferred NTP server.
6. Secondary NTP—Backup NTP server.
7. Provide NTP Service—Enables/Disables G402 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.



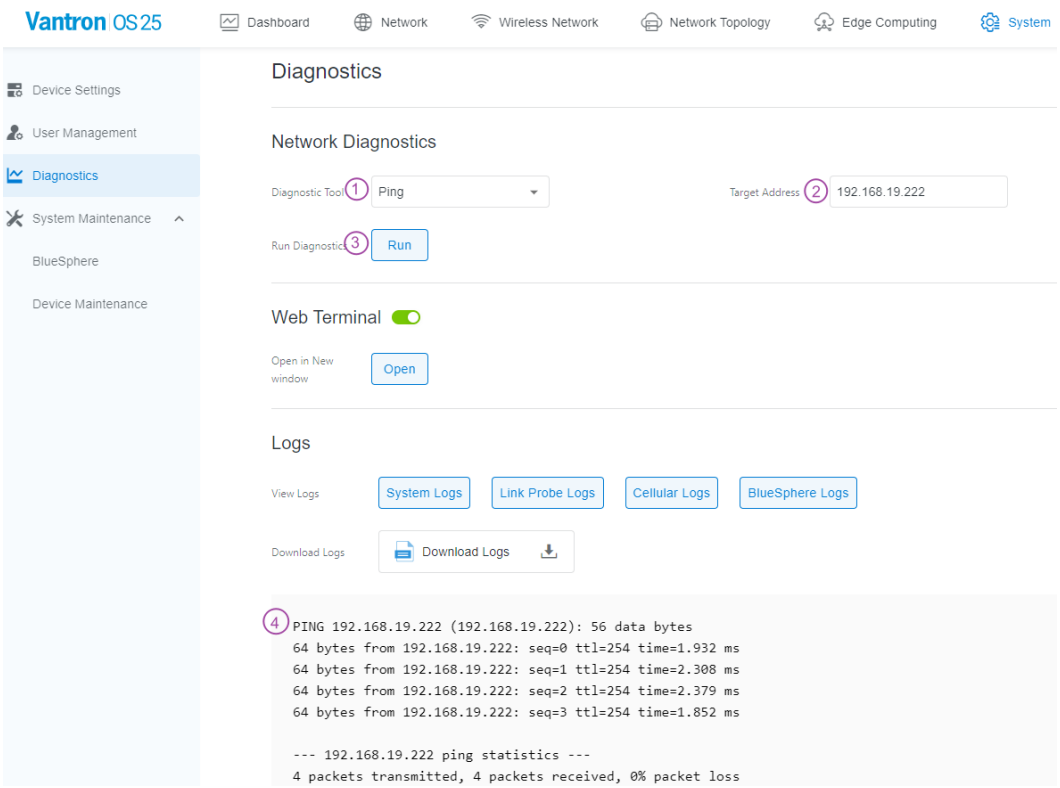
Description of the numbered areas

1. Enter the current password.
2. Enter a 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

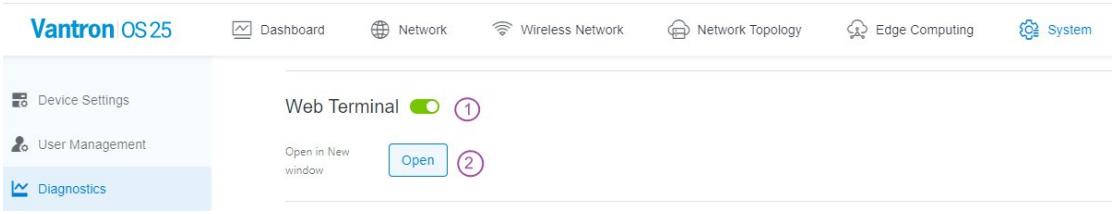


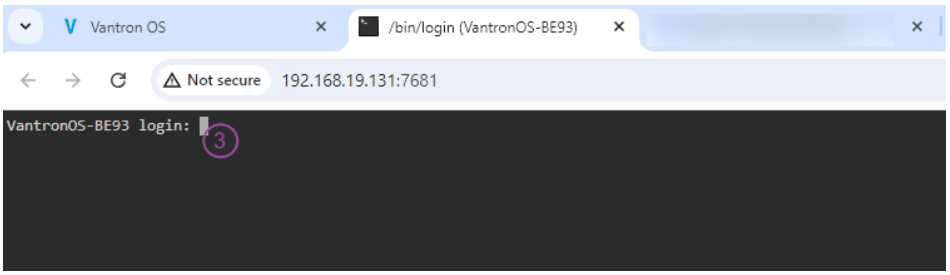
Description of the numbered areas

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.





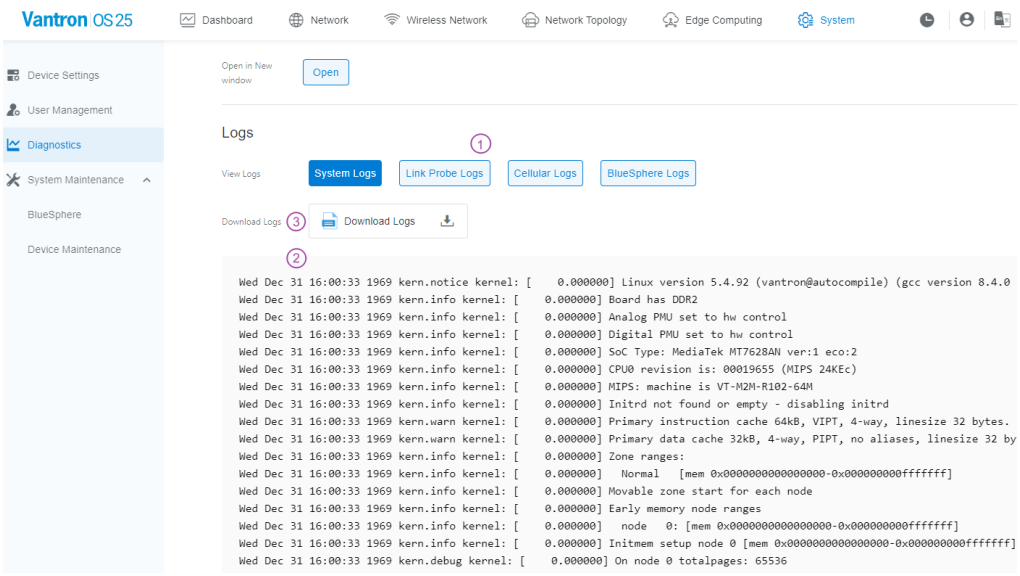
Description of the numbered areas

1. Enable/Disable 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.



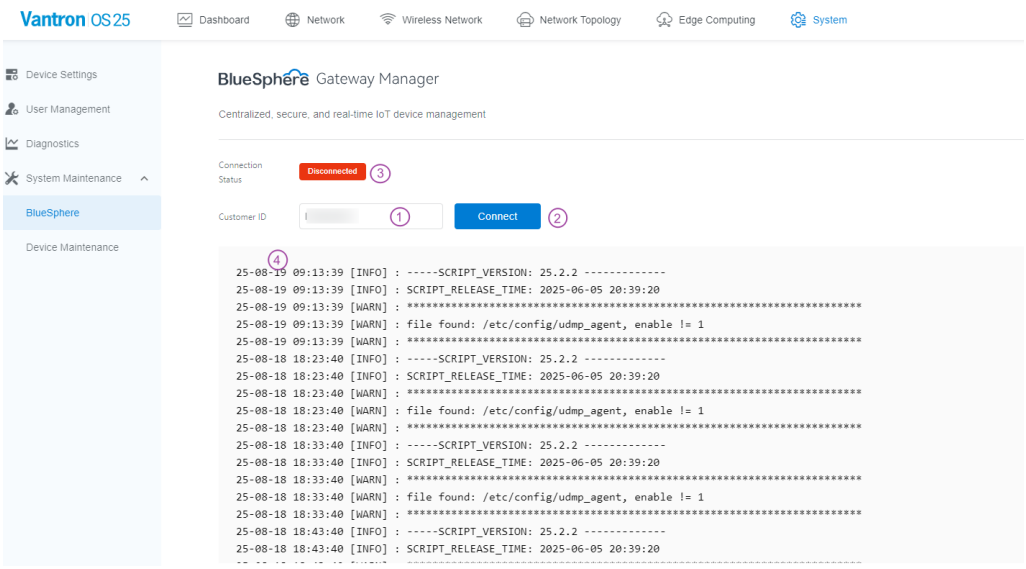
Description of the numbered areas

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.



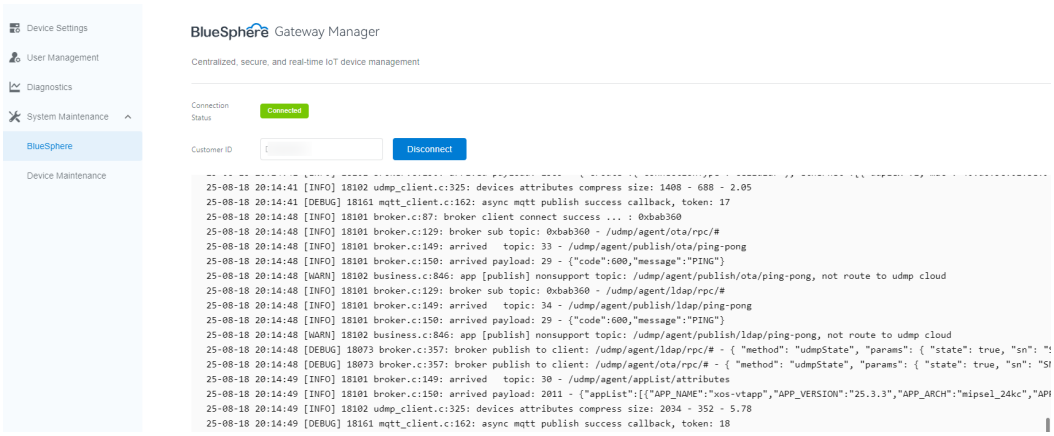
Prerequisite:

G402 must have internet access.

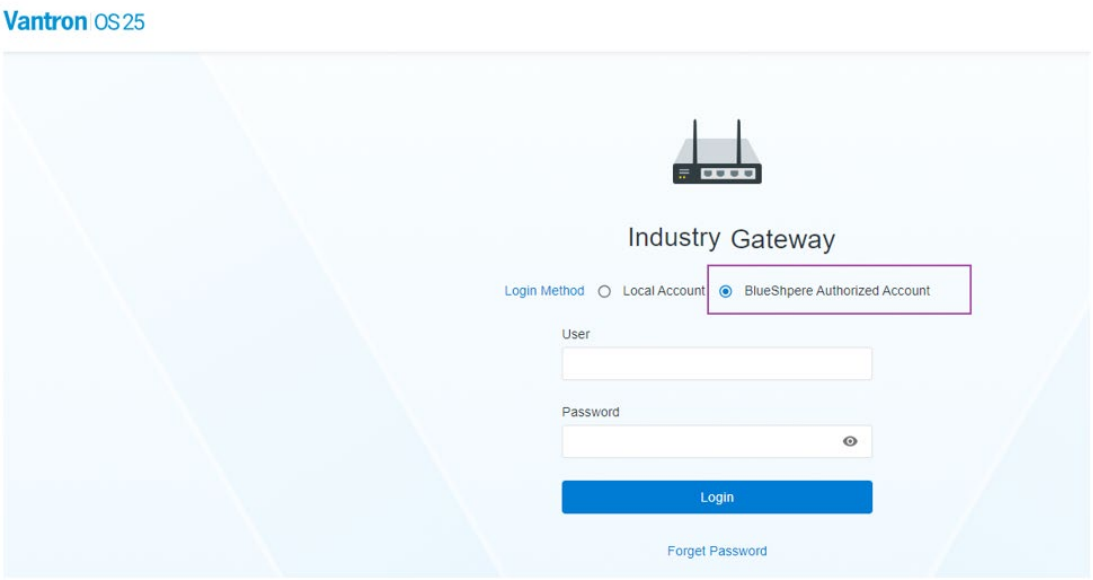
Description of the numbered areas

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.



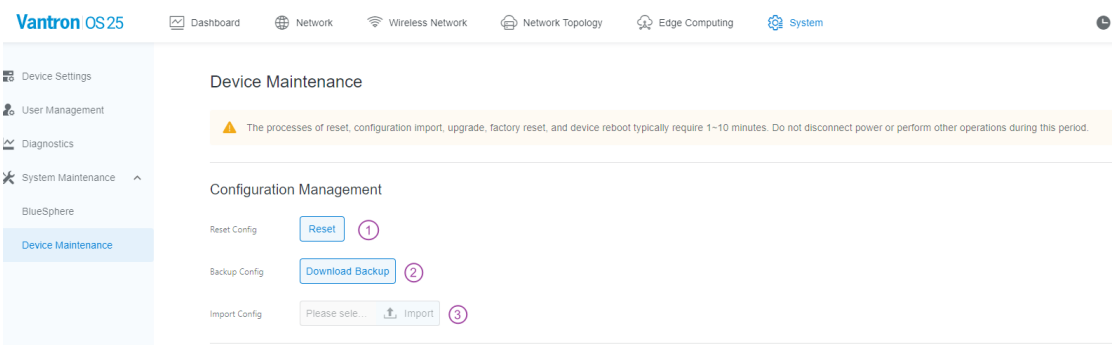
If you log out the portal now, you will find two login methods available. You can sign back in with either your local credentials or an authorized GWM account.



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.

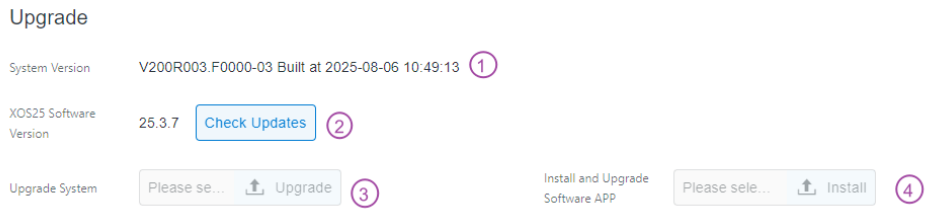
- Configuration Management



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



Description of the numbered areas

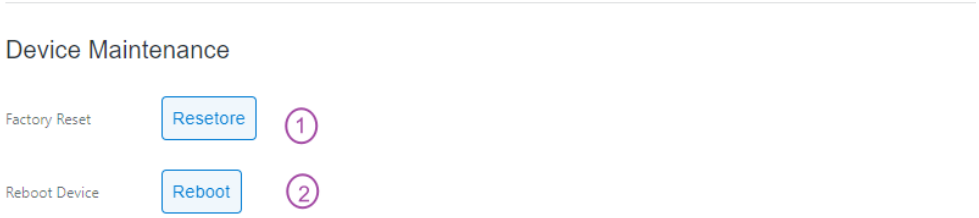
1. Current firmware version.
2. Query the GWM portal for a newer OTA package. If one exists, users can trigger an upgrade; the device will be upgraded to the target version (version selection is not possible).

   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



Description of the numbered areas

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

CHAPTER 4 INDUSTRIAL PROTOCOLPORTAL

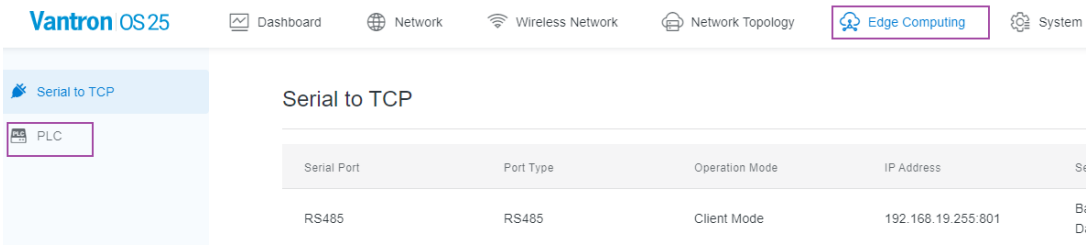
4.1 Overview

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.

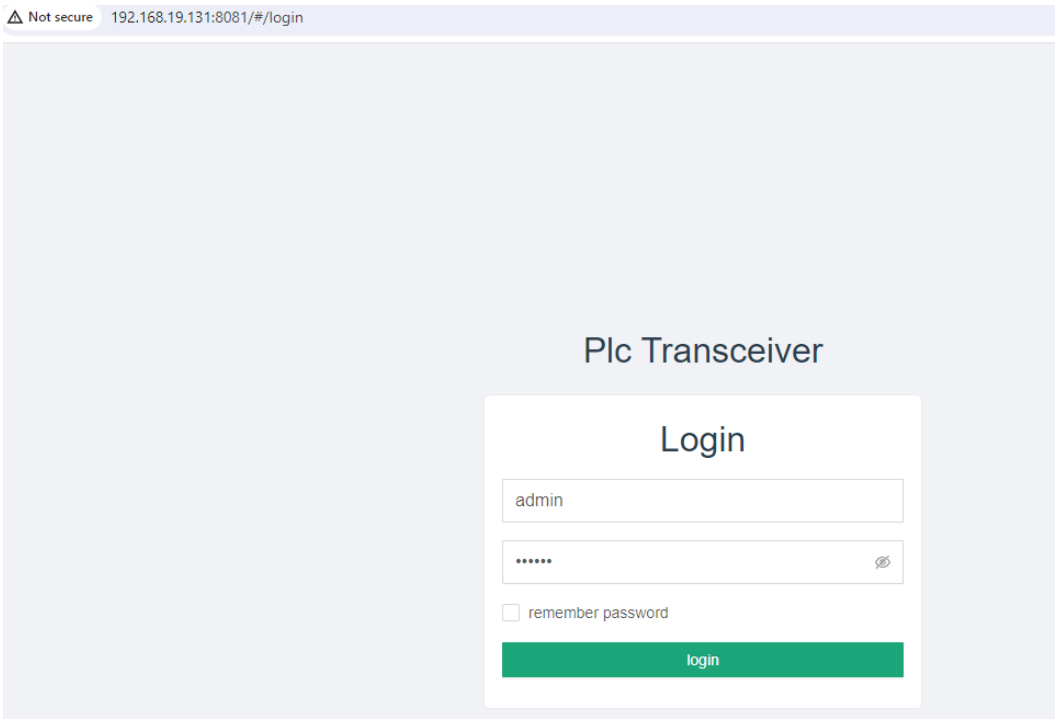
VantronOS industrial protocol portal supports varied wired industrial protocols, spanning both fieldbus and industrial-Ethernet standards to meet diverse on-site requirements.

4.2 Portal Login

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

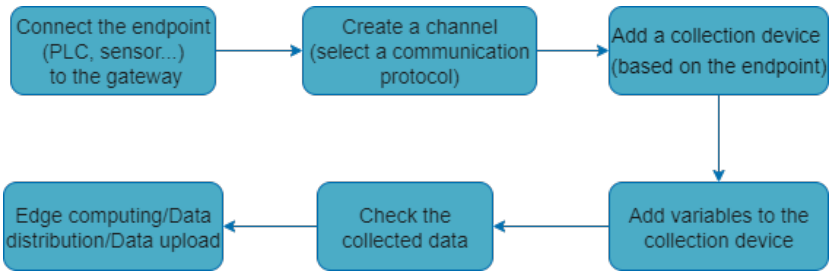


Users will be redirected to a new window. Please use your VantronOS credentials to log in.



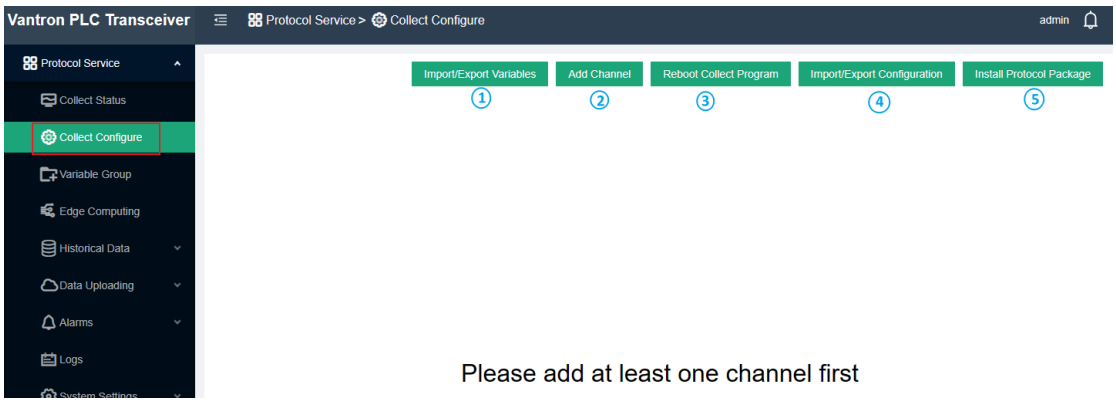
4.3 Protocol Configuration and Application

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:



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.



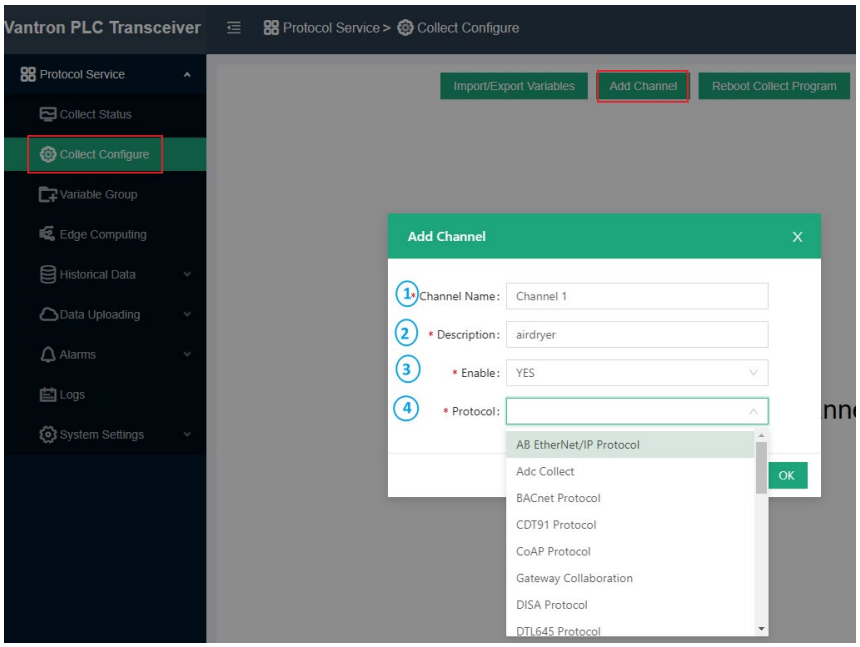
Description of the numbered areas

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.

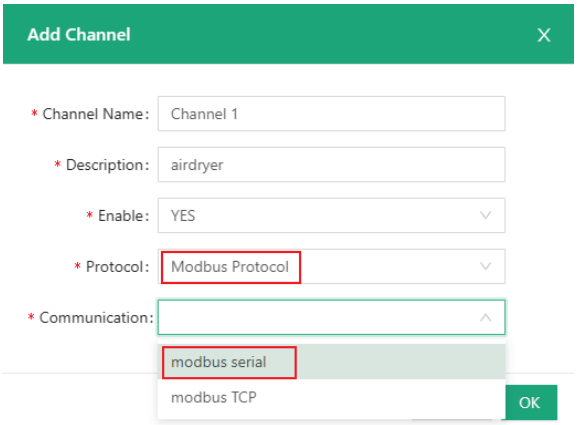


Description of the numbered areas

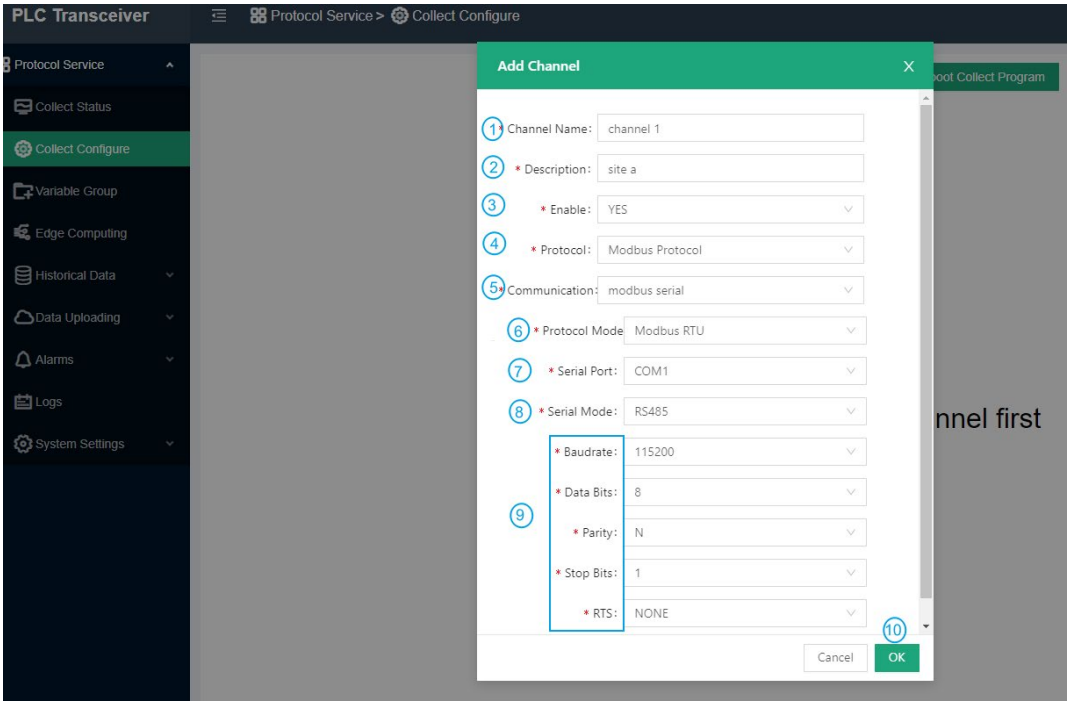
1. Enter a channel name that shall not be any one of the names in use.
2. Describe the channel.
3. To enable the channel or not (‘Yes’ by default).
4. Select a protocol type from the drop-down list based on the model of the endpoint (the available protocols are dependent on the installed package file).

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.



To further configure the protocol:

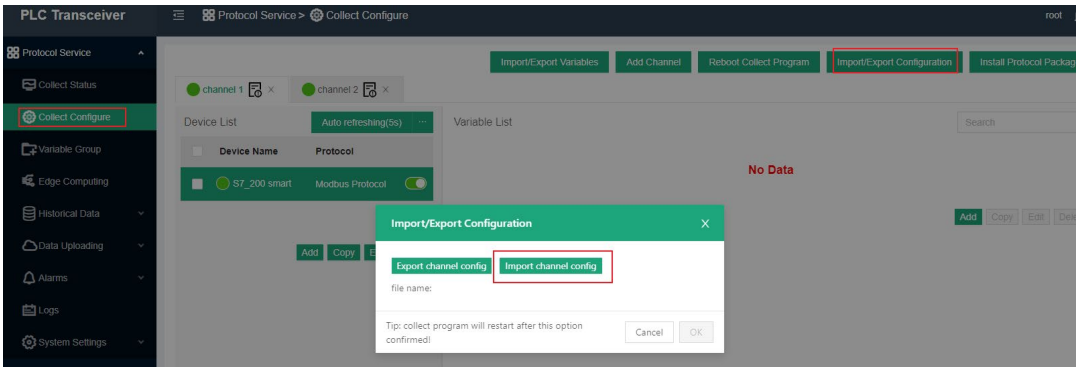


Description of the numbered areas

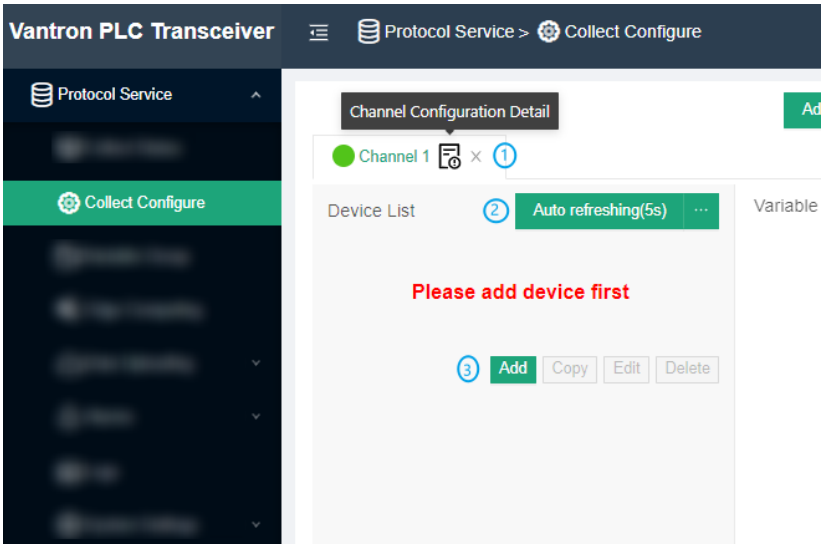
4. Select **Modbus protocol** from the drop-down list.
5. Choose **modbus serial** as the communication type.
6. Select **Modbus RTU/Modbus ASCII** as the protocol mode (Modbus RTU for illustration).
7. Select the correct serial port from the drop-down list that corresponds to the serial port in use on the gateway (the mapping relationship is provided in section 3.6.1).
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**.



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

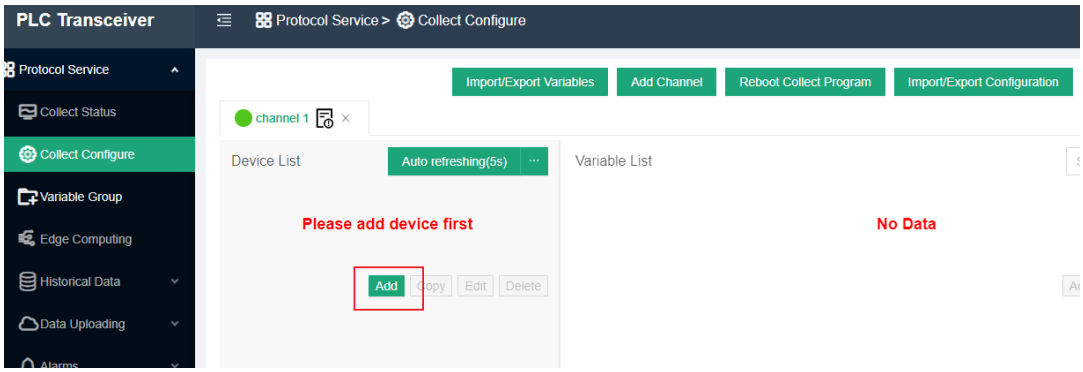


Description of the numbered areas

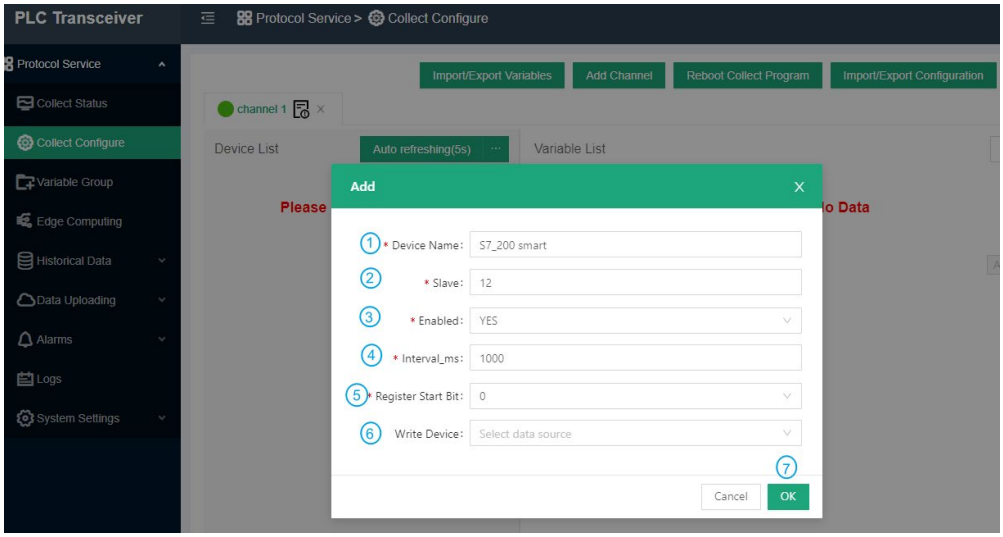
1. Delete the channel (x) or access the detail page ( ) of the channel and make changes accordingly, including disabling the channel.
2. The channel is set to refresh automatically every 5 seconds, and you can assign an optional value between 1 and 99 for auto refreshing by clicking the (…) button.
3. 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.



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



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.

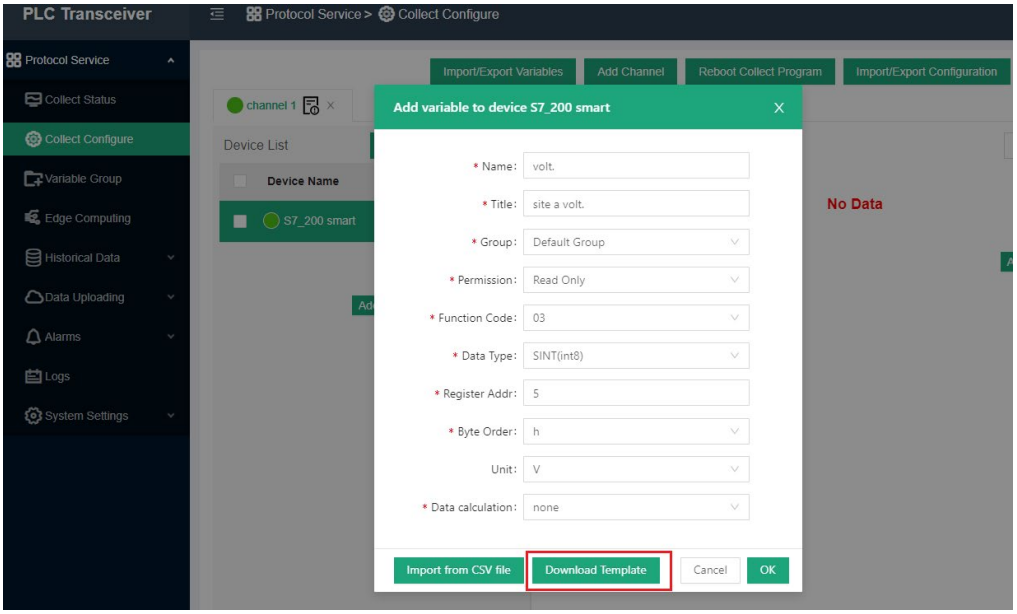
4.3.3 Variable Setup

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

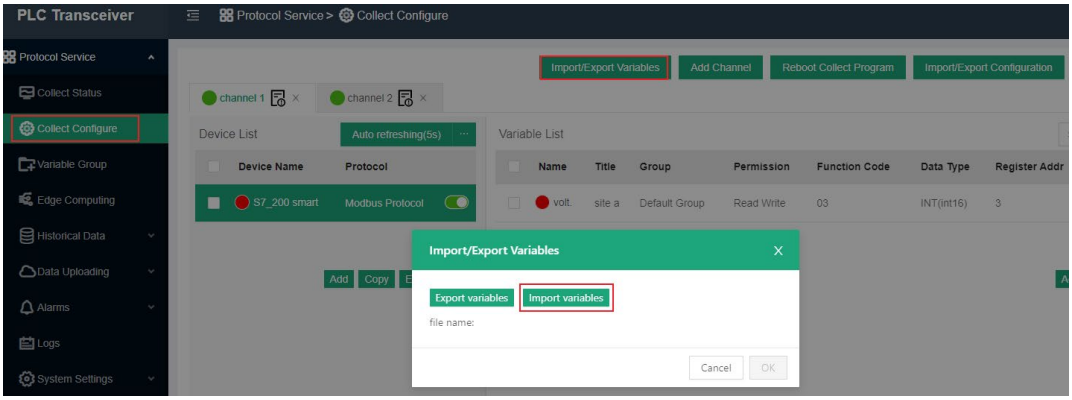
- **Batch Import**

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.

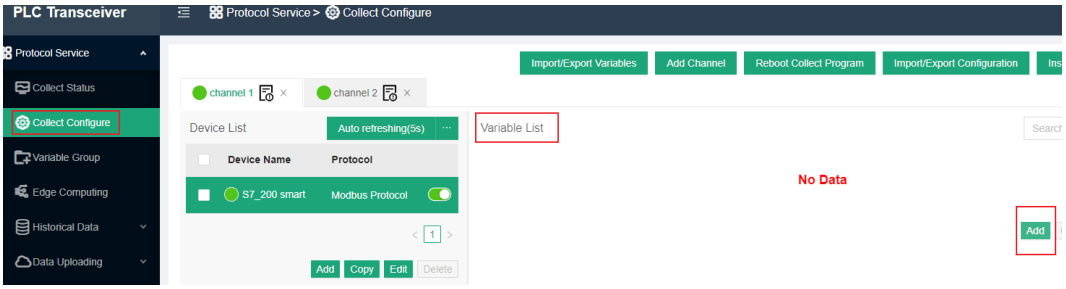


For non-first bulk import, you can directly click the **Import/Export Variables** tab under the **Collect Configure** menu, then select **Import variables**.

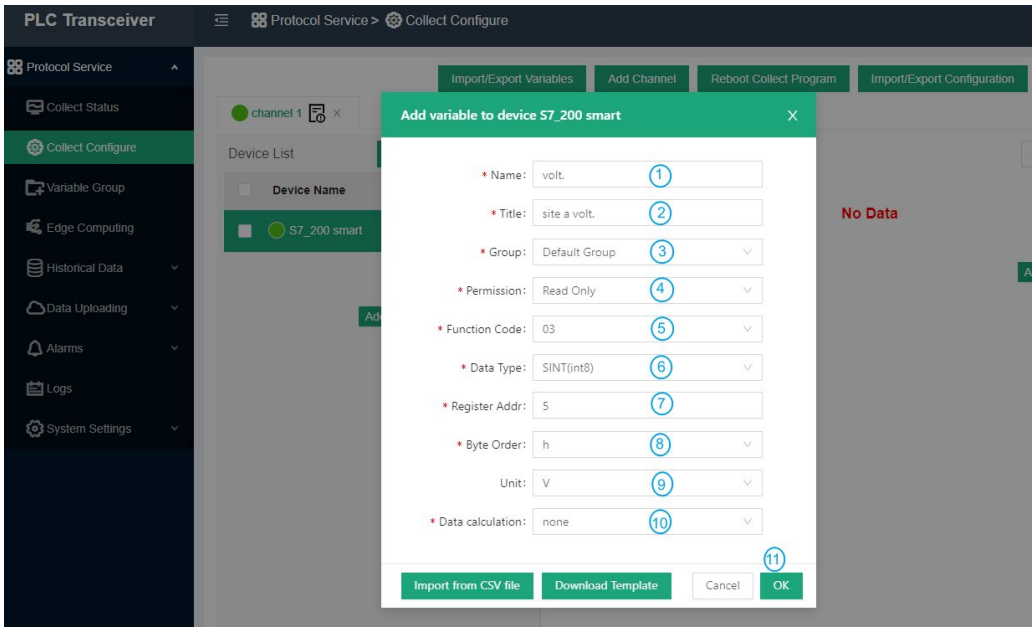


- **Individual Variable Configuration**

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.



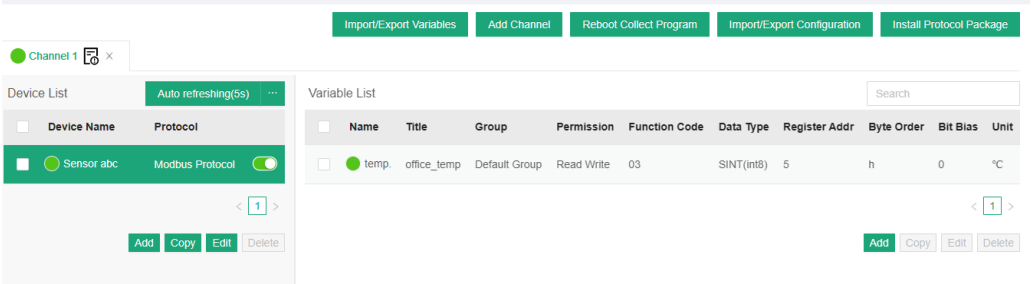
Description of the numbered areas

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).

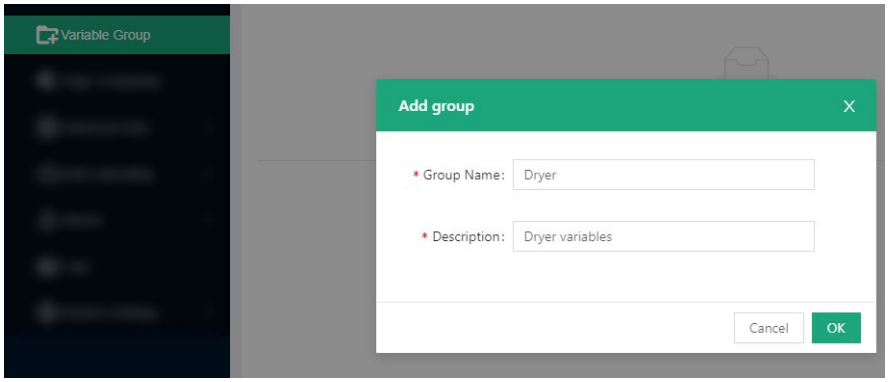
7. Input or adjust the register address from 1 to 65535.
8. Set the byte order.
9. Select a unit for the variable (determined by the collection device).
10. Set a method for data calculation.

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.

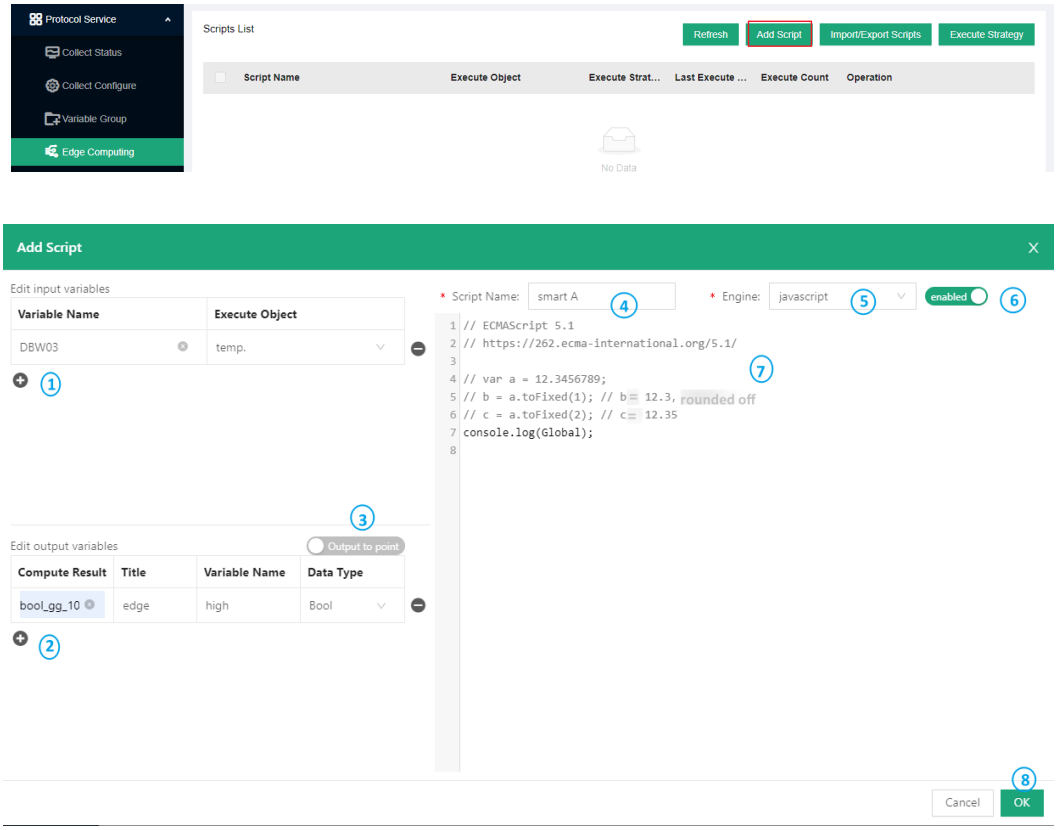


If multiple variables are involved, you can add variable groups for different variables from the **Variable Group** tab on the left menu pane.



4.4 Edge Computing Scripts Setup

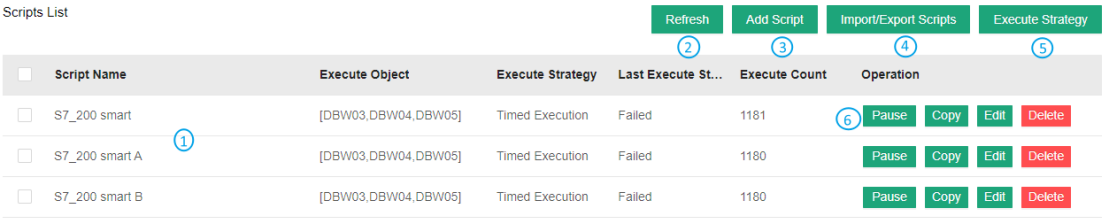
To add a script for edge computing, click **Edge Computing** from the navigation pane on the left, then click **Add Script** to input the script information in the pop-up.



Description of the numbered areas

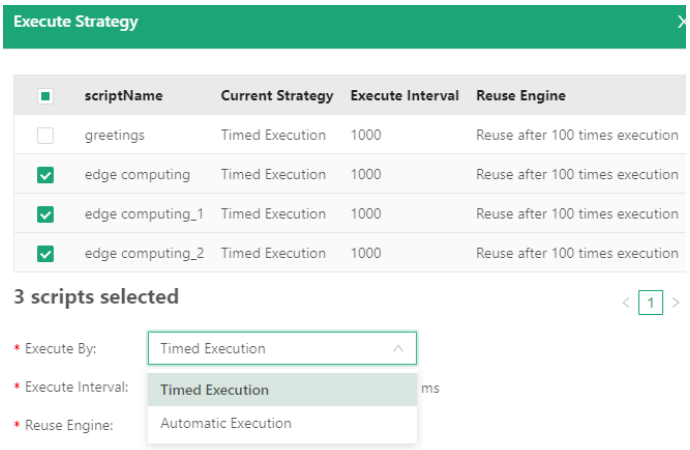
1. Edit input variables: add a name for the input variable and an object for executing the script (more than one variable could be added).
2. Edit output variable: add the computation result, title, variable name, and data type.
3. Toggle between outputting the results to the variables or edge nodes.
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.



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).



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.

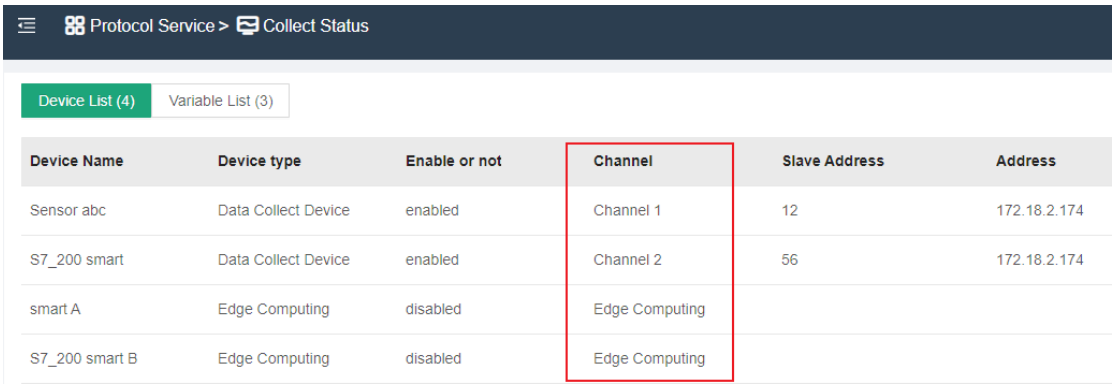
Reuse Context allows you to set a restart mechanism for the scripts

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).

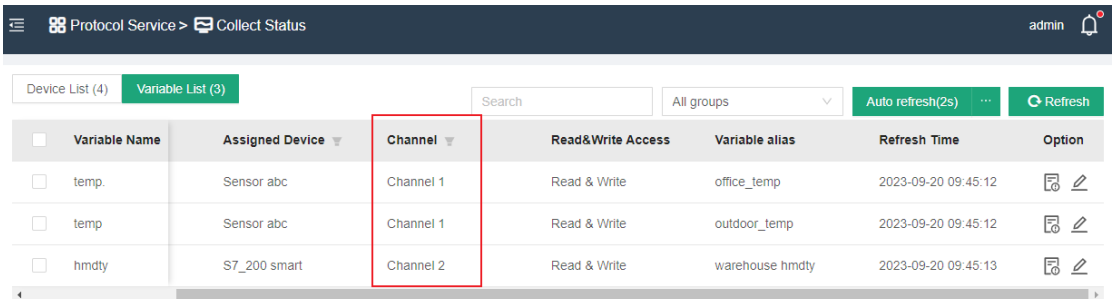
4.5 Collection Status

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

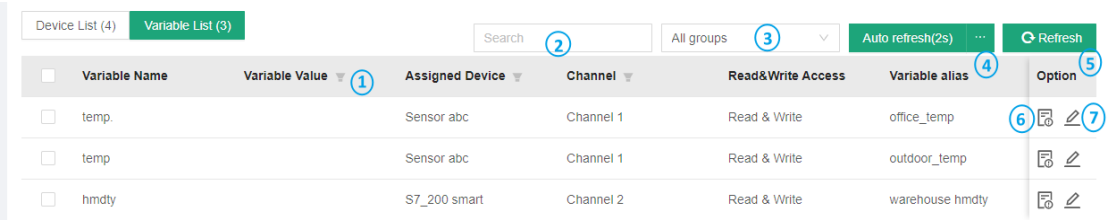
The **Device List** displays information about the collection devices, edge computing, historical data, etc. Users can differentiate the data based on the collection channels.



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.



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



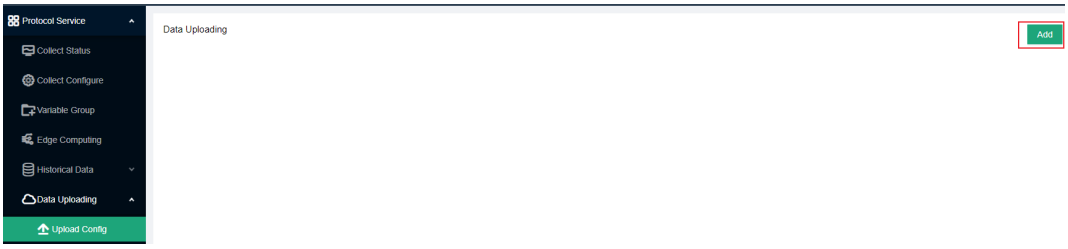
Description of the numbered areas

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).

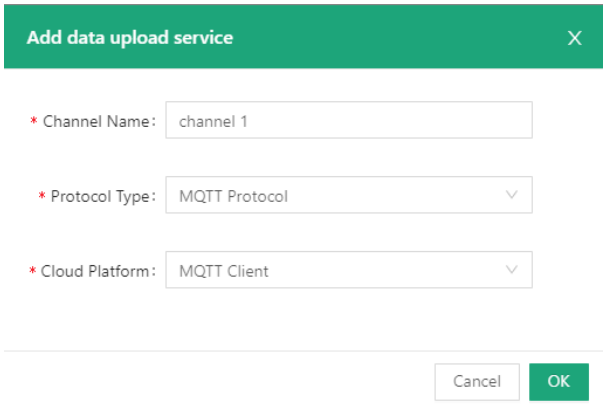
4.6 Data Upload and Encapsulation

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.

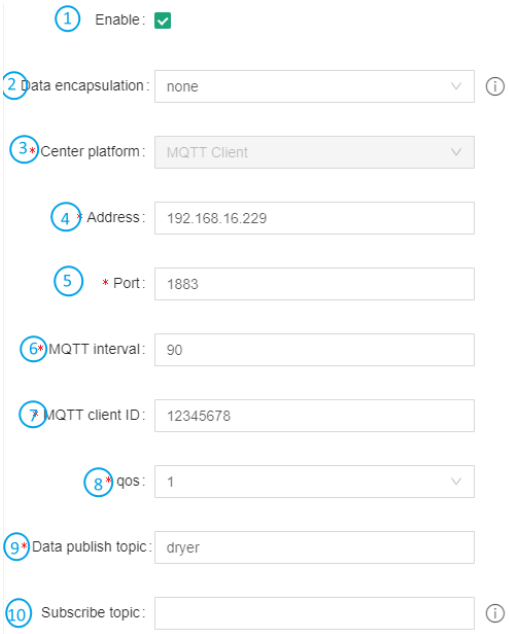
1. Expand the **Data Uploading** tab from the navigation pane and click **Upload Config**.
2. Click the **Add** button on the upper right corner to add a data upload task.



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



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



Description of the numbered areas

1) Select to enable data uploading or not after the configuration, and the data collected will be automatically uploaded to the cloud platform if enabled.
2) Determine the data encapsulation format (no format by default).
3) The center platform is automatically filled and not changeable.
4) Fill in the IP address of the MQTT server.
5) The port number is automatically filled (1883).
6) The client will send a message to the server within a heartbeat interval (90 seconds by default and adjustable), otherwise the client network will be disconnected.

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

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

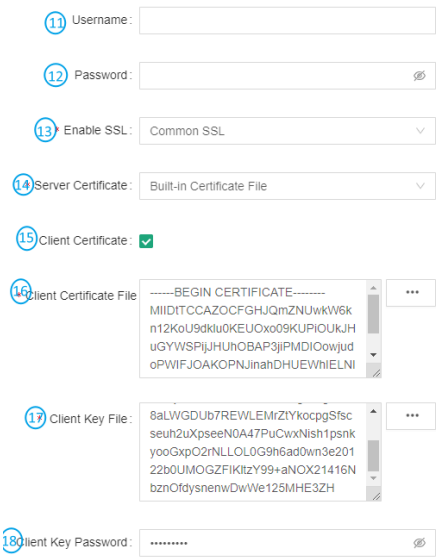
   QoS 0: The message will be sent once at the maximum. If the client is not available, the message will get lost.

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

   QoS 2: The message will be sent only once.

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

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



11) 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).

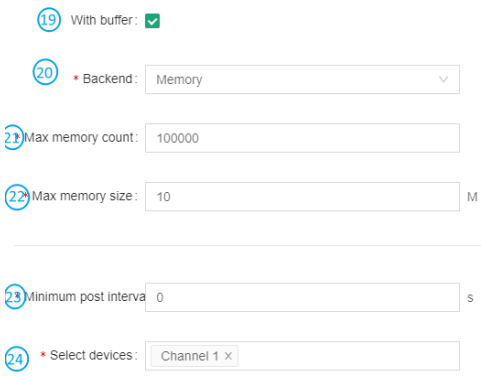
14) If common SSL is enabled, select a certification mode for the server.

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) 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.

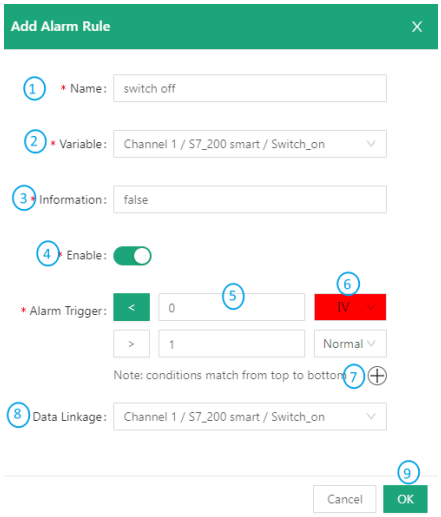
Description of the numbered areas

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.

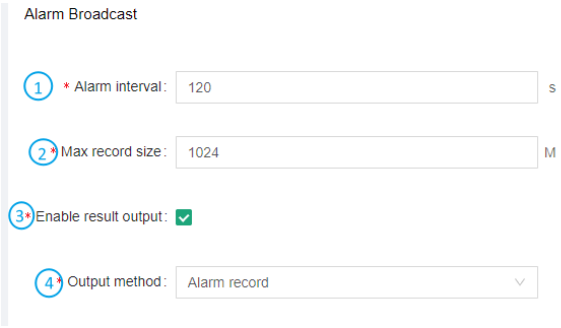


Description of the numbered areas

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

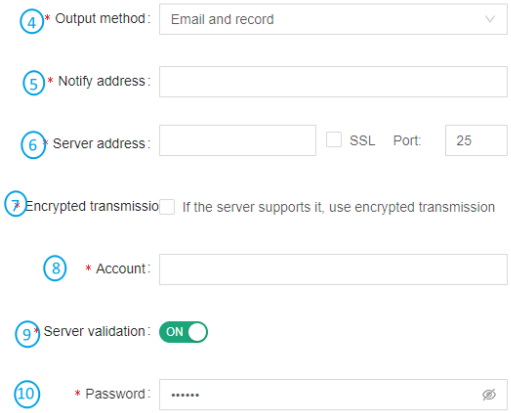
When the alarm rules are created, you can set the parameters for pushing an alarm on the **Alarm Broadcast** page.



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.



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.

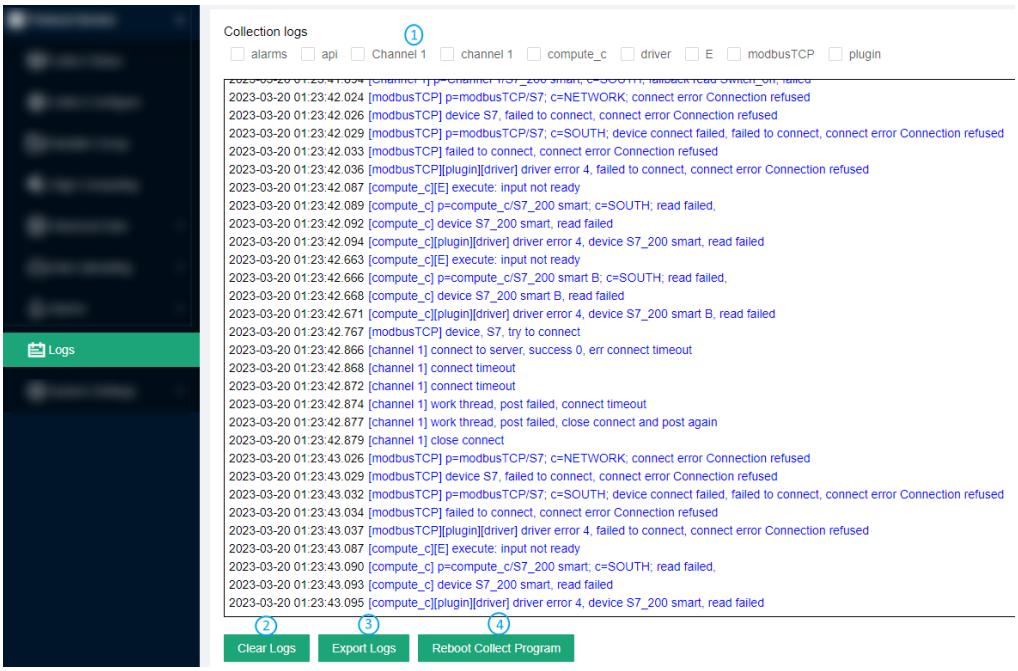
When you are all set, you can send a test email to check if the settings are ok, then submit the settings.

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.



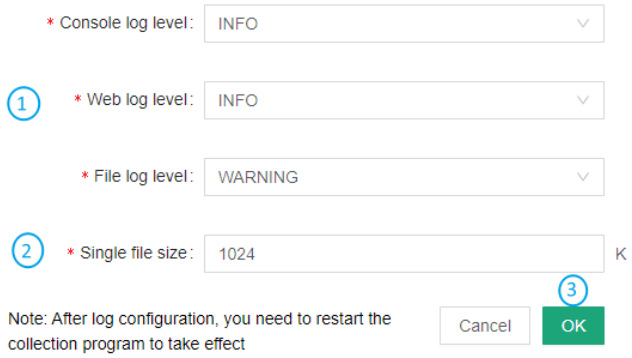
Description of the numbered areas

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.**



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.

IC Statement

This device complies with ISED Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Exposure to radio frequency energy:

The radiated output power of this device meets the limits of ISED Canada radio frequency exposure limits. This device should be operated with a minimum separation distance of 20cm (8 inches) between the equipment and a person's body.

Le présent appareil est conforme aux CNR d'ISDE Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

La bande 5150–5250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

L'exposition à l'énergie radiofréquence:

La puissance de sortie rayonné de cet appareil est conforme aux limites de la ISDE Canada limites d'exposition aux fréquences radio. Cet appareil doit être utilisé avec une distance minimale de séparation de 20cm entre (8 pouces) l'appareil et le corps d'une personne.