G405 Industrial Edge Computing Gateway

User Manual

Version: 1.3

Revision History

No.		Description	Date
V1.0	VantronOS 25 - V200R003.F0000-03	First release	Jun. 5, 2025
V1.1	VantronOS 25 - V200R003.F0000-03	1. Updated I/O description and the wiring graphs. 2. Modified the description on SSH access.	Sep. 3, 2025
V1.2	VantronOS 25 - V200R003.F0000-03	1. Updated sections 2.3~2.5, and moved the network connectivity section to chapter 3. 2. Updated chapter 3 based on the current VantronOS 25 firmware. 3. Added chapter 4 of the industrial protocol configurations.	Feb. 2, 2026
V1.3	VantronOS 25 - V200R003.F0000-04	1. Updated device appearance to GEN 2. 2. Updated button and LED definitions. 3. Updated the illustrative figures in Section 2.2. 4. Updated Section 2.4 to add the Linux login method. 5. Updated Sections 3.1~3.3 based on UI changes.	Apr. 28, 2026

Table of Contents

Foreword

Thank you for purchasing G405 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:

- FCC
- ISED
- CE

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 DESCRIPTION

1.1 Overview

Vantron G405 industrial edge computing gateway is an Arm®-based high-performance solution built for industrial applications. The gateway features dual-SIM 4G connectivity, Wi-Fi, bluetooth, five 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.

The G405 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.

Optional industrial interfaces such as RS-232, RS-485, DI, DO, AI, and CAN FD 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. The G405 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 + Dual-core Arm Cortex-R5F MCU + Single-core Arm Cortex-M4F MCU
- Low power, complete industrial design
- Rich interfaces: DI, DO, AI, RS-232/RS-485, 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

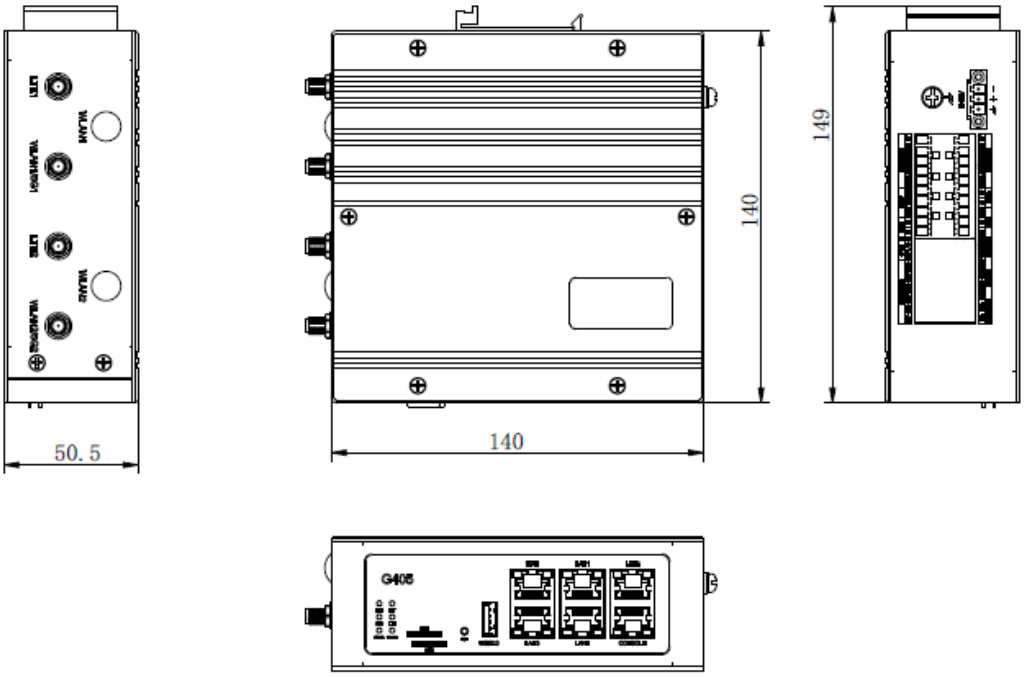
- 1 x G405 Edge computing gateway
- 2 x Wi-Fi antenna
- 2 x 4G LTE antenna
- 2 x Mating connector for CAN, RS-232/RS-485 & 5V out
- 1 x DC power connector

Optional Accessories

- 1 x 12V DC Power adapter
- 1 x Power cord
- 2 x 5G antenna
- 2 x Mating connector for DI, DO, AI

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

1.4 Product Outlines

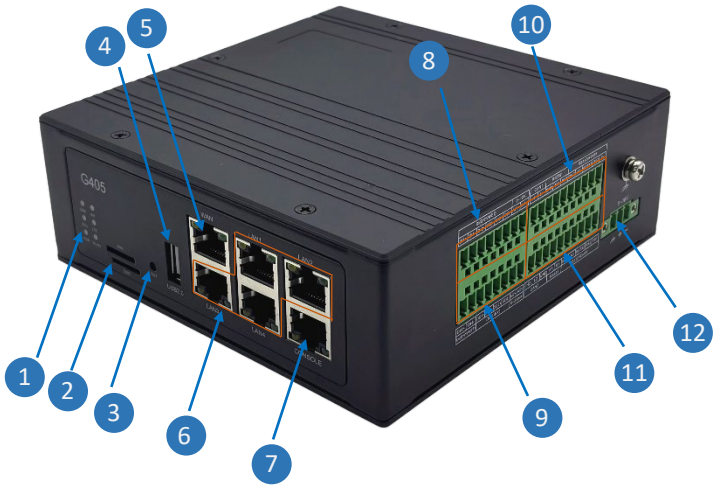


1.5 Specifications

G405 (Hardware)			
System	CPU	Single-core 64-bit Arm Cortex-A53 microprocessor, 1.0GHz (Max.) Dual-core Arm Cortex-R5F MCU, 800MHz (Max.) Single-core Arm Cortex-M4F MCU, 400MHz (Max.)	
	Memory	1GB DDR4	
	Storage	16GB eMMC	
Cellular	Modem	4G LTE, CAT 4	Optional: 5G
	SIM	2 x Micro SIM slot	
	Antenna	2 x Antenna (SMA-K connector)	
Ethernet	Port	5 x RJ45, 10/100/1000Mbps	
	Configuration	1 x WAN + 4 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	1 x RS-232 (isolated), Max. 200kbps	1 x RS-485 (isolated), Max. 500kbps
		2 x RS-232/RS-485 (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 / 0~10V)	
	CAN	2 x CAN FD (isolated)	
	Debug	1 x RJ45 console port (Baud rate: 115200)	
System Control	Button	1 x Reset button ([2, 6s): Restart; [6, 12s): Configuration clear; [12, 20s): Factory reset; [20s,+∞): Initial state)	
	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	149mm x 140mm x 50.5mm	
	Enclosure	Metal	
	Weight	841g (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	

G405 (Software)			
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 Layout



Description:

Item	Description
1	6 x LED indicator (Power, Internet, System, Cellular, Error, WLAN)
2	2 x Micro SIM slot
3	Reset pinhole button ([2s, 6s): Restart; [6, 12s): Configuration clear; [12, 20s): Factory reset; [20s,+∞): Normal operation)
4	USB 2.0 Type-A
5	WAN (ETH1), connects to an external network to provide internet access to the local network. (Software node: eth0)
6	4 x LAN (ETH2~5) , connects local devices for data communication or device management. (Software node: ETH2-eth1, ETH3-eth2, ETH4-eth4, ETH5-eth3)
7	Console, provides out-of-band management access to the device shell (Baud rate: **115200**).
8	DI 1~3 (dry / wet contact), AI 1 (0~10V or 0~5V)
9	DI 4 (dry / wet contact), DO 1~2 (5A @30V DC), AI 2 (0~10V or 0~5V)
10	CAN 1, RS-232, RS-232 / RS-485, 5V output
11	CAN 2, RS-485, RS-232 / RS-485
12	9~36V power terminal (1: GND, 2: V+, 3: V-)

Description:

Item	Description
1	Wi-Fi antenna connector 1 (used only when WLAN/5G1 is occupied by 5G)
2	Wi-Fi antenna connector 2 (used only when WLAN/5G2 is occupied by 5G)
3	Primary cellular antenna connector
4	Wi-Fi/5G antenna connector 1 (Wi-Fi by default, 5G as backup)
5	Cellular diversity antenna connector
6	Wi-Fi/5G antenna connector 2 (Wi-Fi by default, 5G as backup)
7	DIN rail mount

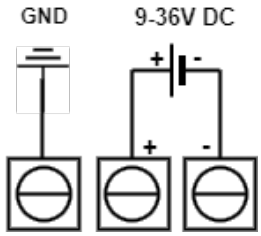
1.7 Interface Parameters

Interface	Parameter	Description
Digital input (DI 1~DI 4)	Channel #	4
	Type	Dry/Wet contact
	Input voltage (wet contact)	0~5V
	Input impedance	≥ 1000Ω
	Input mode	Level
	Logic level threshold	Low ≤ 1V; High ≥ 4V
Analog input **Current measurement** (AI 2)	Channel #	1
	Measurement range	0~20mA
	Accuracy	5‰
	Sampling frequency	860Hz
	Resolution	16 bits
	Isolation	None
	Input impedance	120Ω
	Input mode	Single-ended input
Analog input **Voltage measurement** (AI 1)	Channel #	1
	Measurement range	0~10V
	Accuracy	5‰
	Sampling frequency	860Hz
	Resolution	16 bits
	Isolation	None
	Input impedance	14.7kΩ
	Input mode	Single-ended input
Digital output (DO 1~2)	Channel #	2
	Contact	C-type relay
	Contact capacity	30V 5A DC
	Output mode	Level
Upstream COM (RS-232/RS-485)	Serial port type	RS-485/RS-232
	Channel #	4
	Baud rate range	50Kbps~1Mbps (default parameters: 9600, 8N1)

Interface	Parameter	Description
CAN (CAN 1~ CAN 2)	Channel #	2
	Bitrate ranges	4800~921600
Console port	Physical connector	RJ45
	Electrical standard	RS-232
	Baud rate	Default parameters: 115200, 8N1

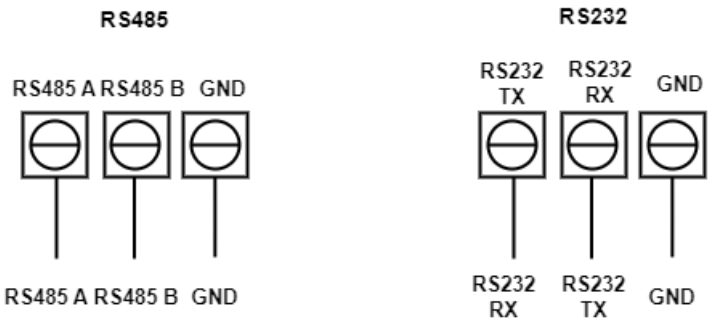
1.8 Wiring Instructions

1.8.1 Power Input



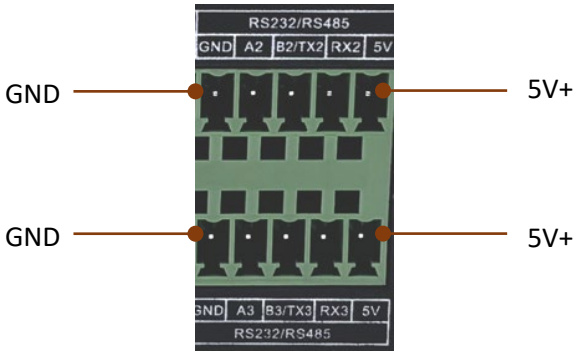
Power terminal: 1 x 3 x 3.81mm, 12V/1A DC recommended.

1.8.2 RS-232/RS-485 & 5V Output

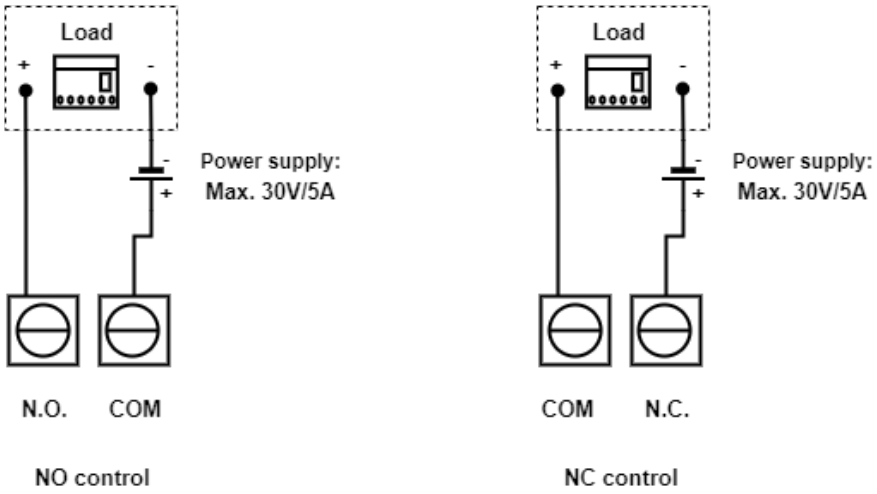


The RS-232/RS-485 multiplexers default to the RS-232 mode and can be modified via the **Edit** menu on the **Edge Computing > Serial-to-PLC** page. Refer to Section 3.7.1 for details.

The G405 provides two independent 5V power output pins, each located adjacent to an RS-232/RS-485 interface. Each 5V pin pairs with the GND pin of the RS-232/RS-485 interface to form a complete power loop. The port can deliver up to 0.1 A; exceeding this current limit may damage the device.



1.8.3 Digital Output (DO)



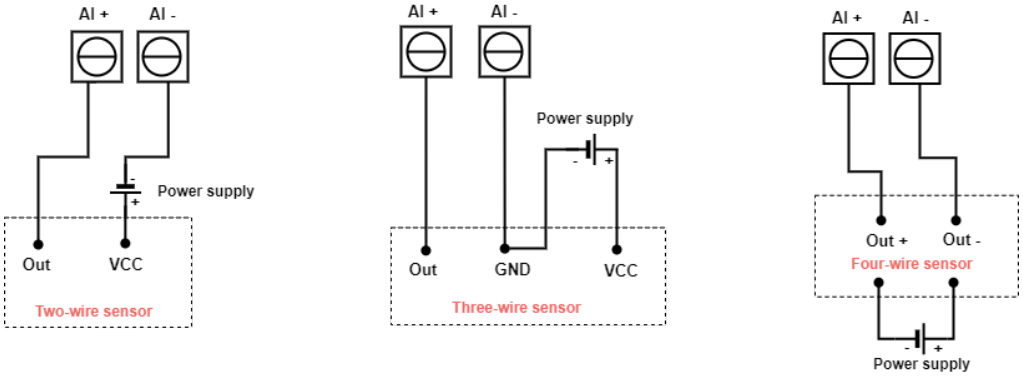
The interface connection can be controlled via software. Up to 30V/5A power supply is supported.

1.8.4 Digital Input (DI)

Each digital input channel supports software-configurable dry/wet contact mode. The wiring and behavior are as follows:

Contact mode	Wiring
Dry contact	Connect DI- to one end of the external switch/sensor and DI+ to the other. When the circuit is closed (shorted), the input reads a low level; when open, it reads a high level.
Wet contact	Connect DI- to GND and DI+ to the positive terminal of a 5V supply (5V VCC). The input is low when powered (circuit closed) and high when unpowered (open).

1.8.5 Analog Input (AI)



The G405 provides two analog input channels:

- **Channel 1 (AI1+, AI1-)** is for 0~5V or 0~10V voltage measurement. 0~10V measurement is set as the default. The measurement range is switched via software.
- **Channel 2 (AI2+, AI2-)** is for 0~20mA current measurement; the actual current value is displayed via software configuration.

1.9 LED Indicators

When a device factory reset is performed, all LED indicators blink at 3Hz until the process finishes, after which the LEDs return to normal operation.

Individual LEDs are defined as follows.

1.9.1 Power LED

LED	LED Status	Description
PWR	ON	Device properly powered on.
	OFF	Device not powered on or improperly powered.

1.9.2 ERR LED

LED	LED Status	Description
ERR	ON	Device abnormality detected.
	OFF	Device working properly or device alarm cleared.

1.9.3 Internet LED

LED	LED Status	Description
Internet	ON	Device online via Ethernet, 4G or Wi-Fi.
	OFF	No internet connection.

1.9.4 SYS LED

LED	LED Status	Description
SYS	ON	System running properly.
	Blinking at 3Hz	System boot/upgrade/reset in progress.
	OFF	System fault.

1.9.5 Cellular LED

LED	LED Status	Description
LTE	ON	Cellular module running properly.
	Blinking at 3Hz	SIM card inserted and functioning properly. Turns to solid green after dial-up finishes.
	Blinking at 0.5Hz	Connection not reachable.
	OFF	Cellular module not functioning/SIM card not inserted.

1.9.6 WLAN (Wi-Fi) LED

Mode	LED Status	Description
Wi-Fi Client	OFF	Wi-Fi module is disabled or not powered.
	Blinking at 1Hz	Scanning for / attempting to connect to an AP.
	Solid green	Connected to a Wi-Fi AP.
Wi-Fi AP	OFF	Wi-Fi module is disabled or not powered.
	Blinking at 1Hz	No Wi-Fi client connected.
	Blinking at 3Hz	WPS (quick pairing) initiated. Back to solid green after the process finishes.
	Solid green	At least one Wi-Fi client connected.

1.10 Button

The G405 offers a **Reset** (RST) pinhole button that allows the device to restart or reset as defined below:

Button Hold	Description
[2s, 6s)	Initiates a device reboot.
[6s, 12s)	Device configuration is cleared. You can re-log in to the device using the credentials provided on the device label and follow the setup wizard to finish the first-time configuration.
[12s, 20s)	The device is factory reset with all configurations, user data, and user apps cleared. You can re-log in to the device using the credentials provided on the device label and follow the setup wizard to finish the first-time configuration.
[20s, +∞)	No device action triggered.

1.11 Console Port

The G405 offers a console port as a dedicated serial management interface, providing out-of-band access to the device's command-line interface (CLI).

To access the device shell, connect the G405's console port to a host PC using an USB-to-RJ45 Console cable.

Default parameters: 115200 baud, 8N1, no flow control.

Refer to Section 2.5 for the specific debugging steps.

1.12 SIM Slot

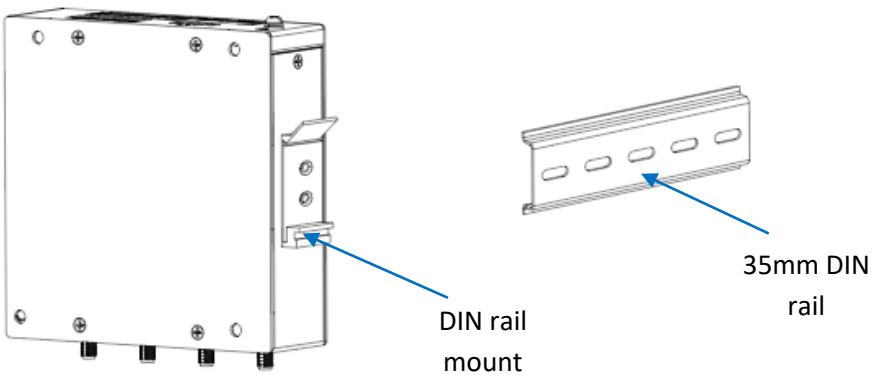
The gateway is equipped with two Micro SIM slots. With dual SIMs installed, the device automatically switches to the line with the stronger signal whenever the current cellular connection becomes unstable.

CHAPTER 2 GETTING STARTED

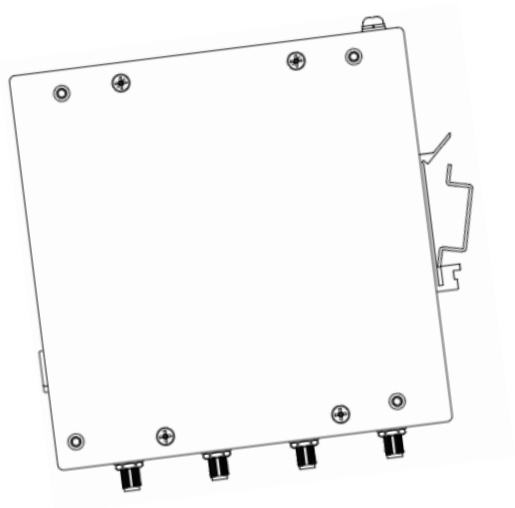
2.1 Device Installation

When mounting the G405 on a vertical surface, please ensure that the device is oriented with the LED indicators pointing down. This positioning allows the LEDs to be visible to the user on the ground.

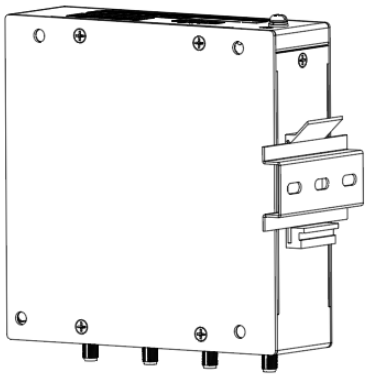
1. Hold the gateway vertically, and align the DIN rail mount of the device to the 35mm DIN rail.



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.



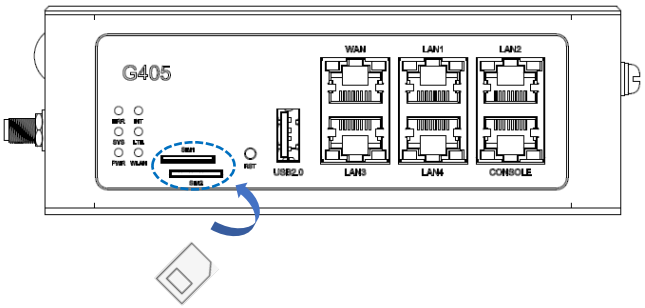
3. Push the gateway toward the DIN rail until it snaps securely into place.
4. Gently swing the device to make sure it is fixed on the DIN rail.



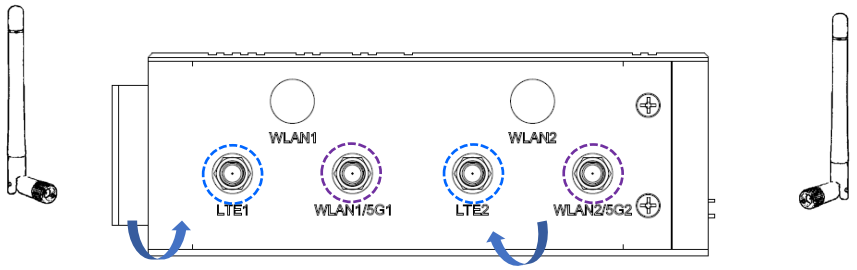
2.2 Hardware Connection

After installation, complete the hardware connections below **as needed** for smooth operation of the G405.

1. Based on your actual situation, insert an 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**.

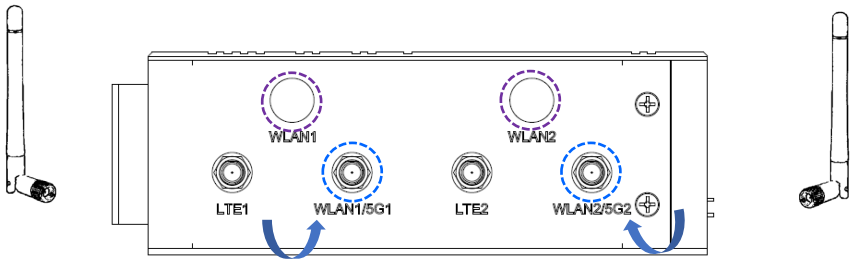


2. For 4G communication, attach the cellular antennas to the LTE 1 and LTE 2 connectors. For 5G communication, attach the two additional cellular antennas to the WLAN1/5G1 and WLAN2/5G2 connectors (See figure below).



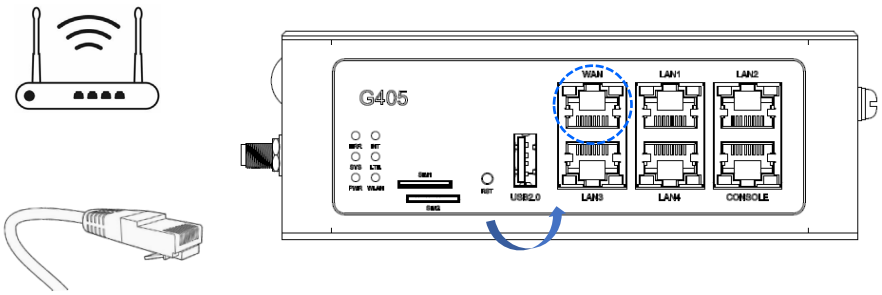
Legend: Blue = 4G LTE connection; Blue + Purple = 5G connection

3. Where 4G communication is available: Attach the Wi-Fi antennas to the WLAN1/5G1 and WLAN2/5G2 connectors. Where 5G communication is available: Attach the Wi-Fi antennas to the WLAN 1 and WLAN 2 connectors.

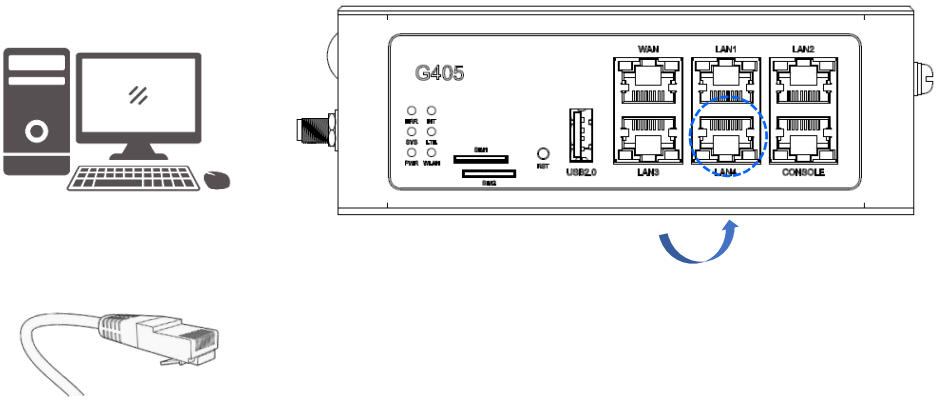


Legend: Blue = Default Wi-Fi path; Purple = Wi-Fi path under 5G mode

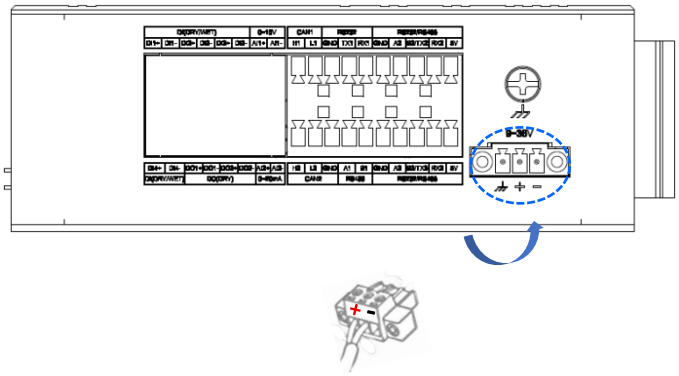
4. Connect the gateway's WAN port to the upstream network (e.g. a router).



5. Connect a PC or other network devices to the gateway's LAN port (LAN 1~LAN 4) using an Ethernet cable 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 and SYS LEDs turn solid green to indicate the device is working properly.

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 PC.

There are two login options to access VantronOS for the G405, depending on how the host PC is connected to it.

Method	Host PC Connection	Login Address
Option 1	Host connected to the device's LAN network (via Ethernet or Wi-Fi).	G405's LAN IP
Option 2	Host's WAN interface on the same IP subnet as G405's WAN interface (e.g., both connected to the same router or upstream Wi-Fi).	G405's WAN IP

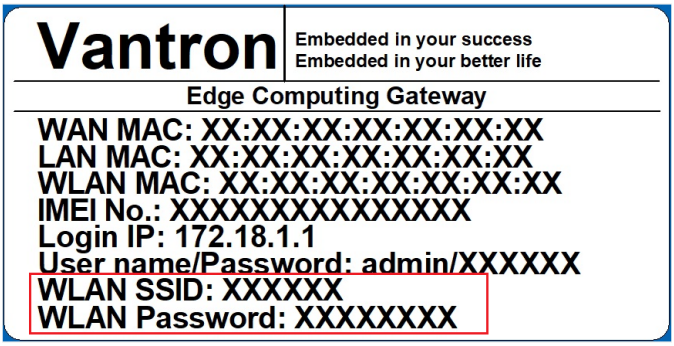
We recommend initially logging into VantronOS using Option 1. Afterwards, you may establish additional connections between G405 and your host PC, and switch to other login options as needed by referring to the device's IP addresses listed under the **Network** tab in VantronOS.

Steps:

1. Connect the host PC:
   - Via Ethernet

     Connect the host PC directly to the G405's LAN port using a standard Ethernet cable.
   - Via Wi-Fi

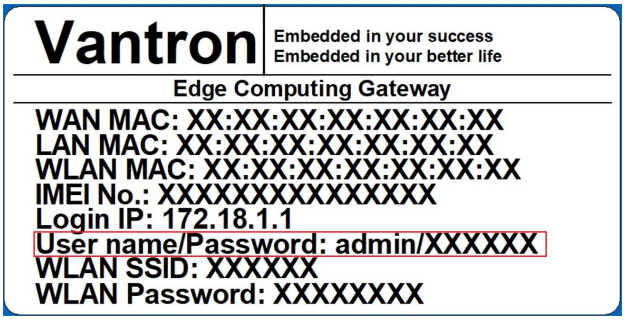
     Connect the host PC to the 2.4GHz Wi-Fi of the G405 using the default SSID and password provided on the device label.

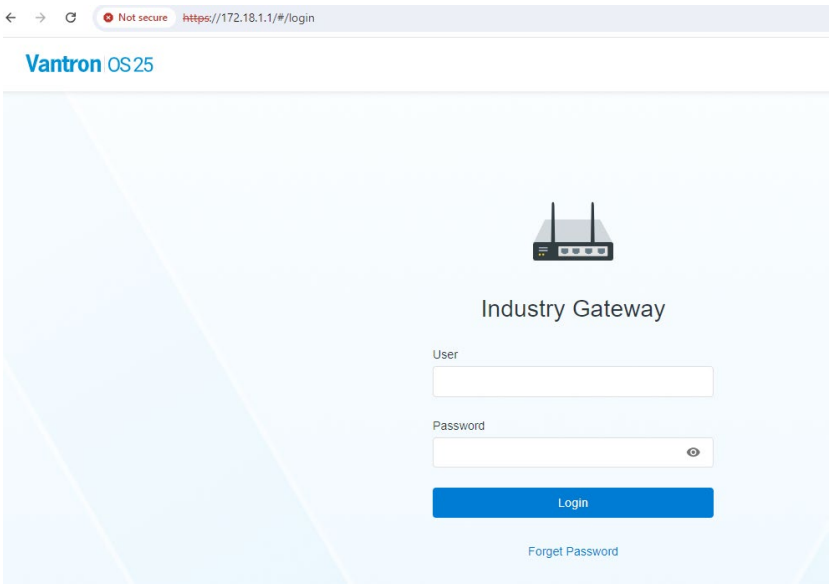


2. Enter the login IP in the browser of the host PC for device login.

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

3. Log in to the management portal using the username and password on the device label.



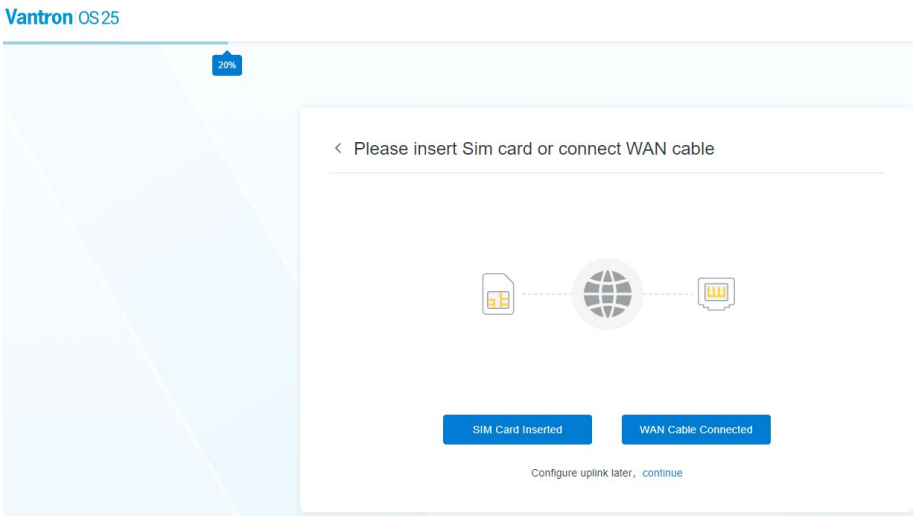


4. Upon **first** login, the system will automatically launch a setup wizard that will guide you through configuring essential settings.

2.3.1 Login Wizard

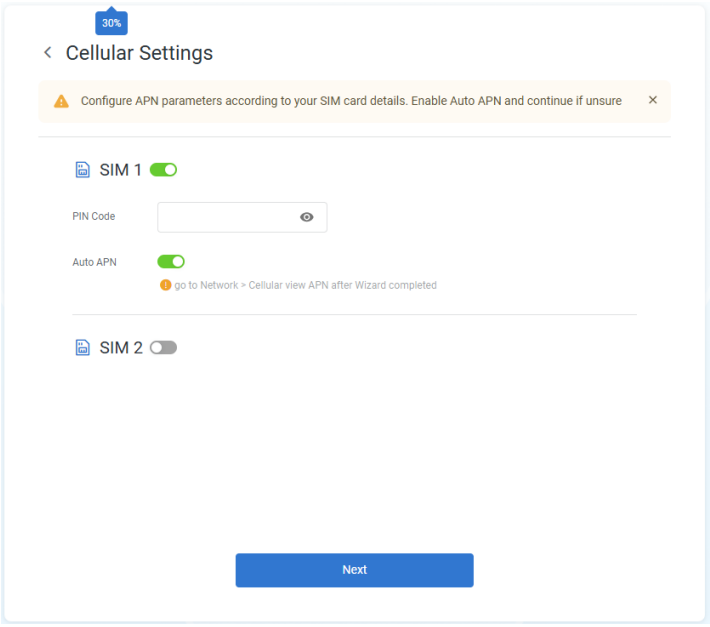
For first-time login or login after a device reset, the setup wizard will guide you through the initial setup process for quick setup.

Connect to an upstream router via the Ethernet WAN port or insert a valid SIM card, then click the corresponding button to proceed. Alternatively, click **continue** below the buttons to skip this step.



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

1. The device supports dual SIM configuration. Select the SIM slot in use and configure it on the login page accordingly. Use **Auto APN** if you are unsure of the carrier parameters.



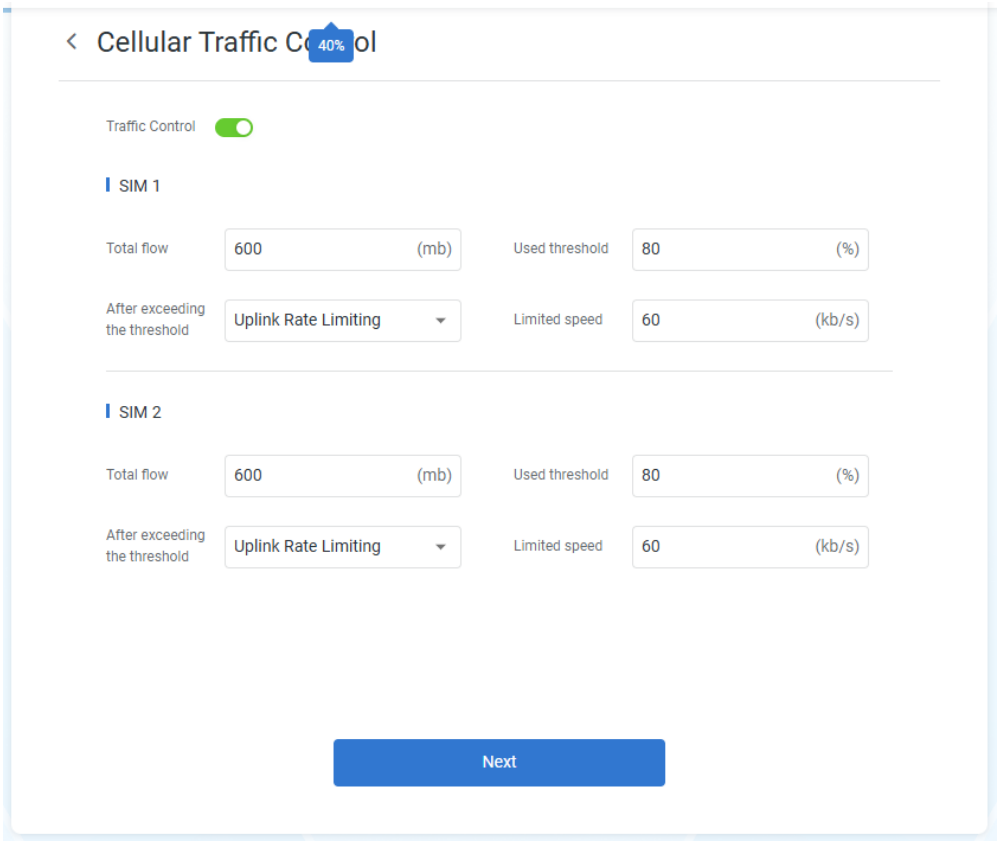
PIN: Carrier-defined, optional.

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

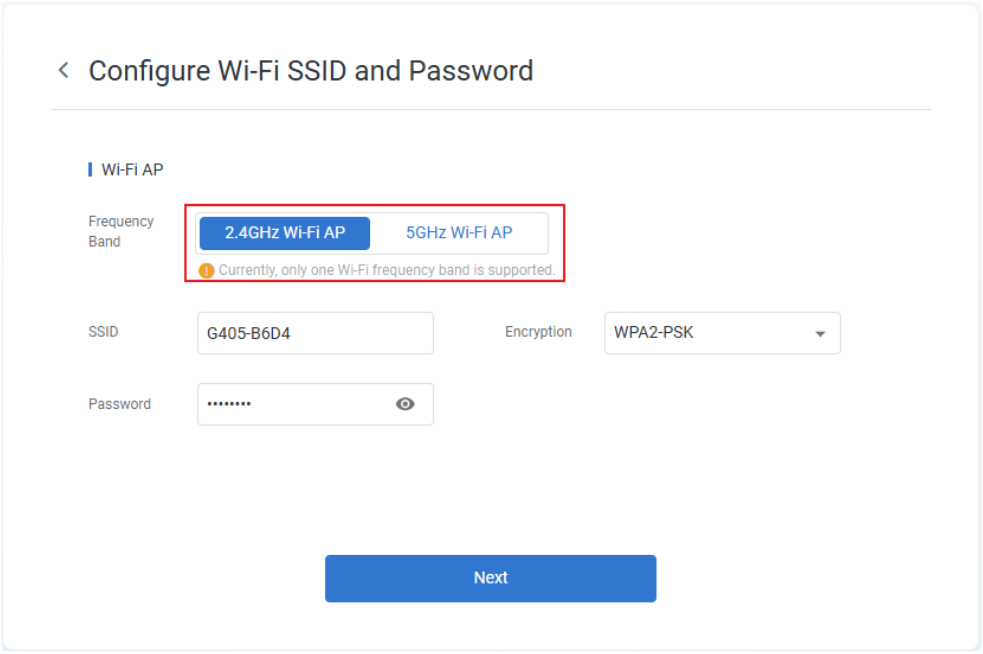
Authentication Type (None / PAP / CHAP): Carrier-defined; required when **Auto APN** is disabled.

When **Auto APN** is enabled, manual configuration of APN and authentication type is not required. These settings can be modified later on the **Network > Cellular** page.

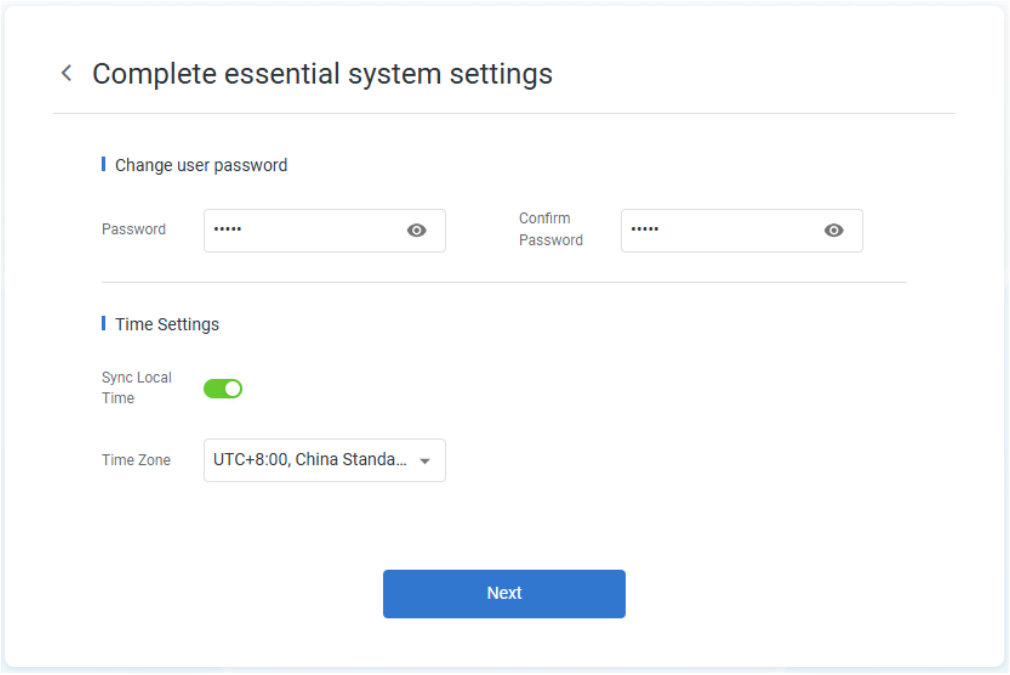
2. To manage data usage, enable **Traffic Control** and configure the relevant parameters as needed.



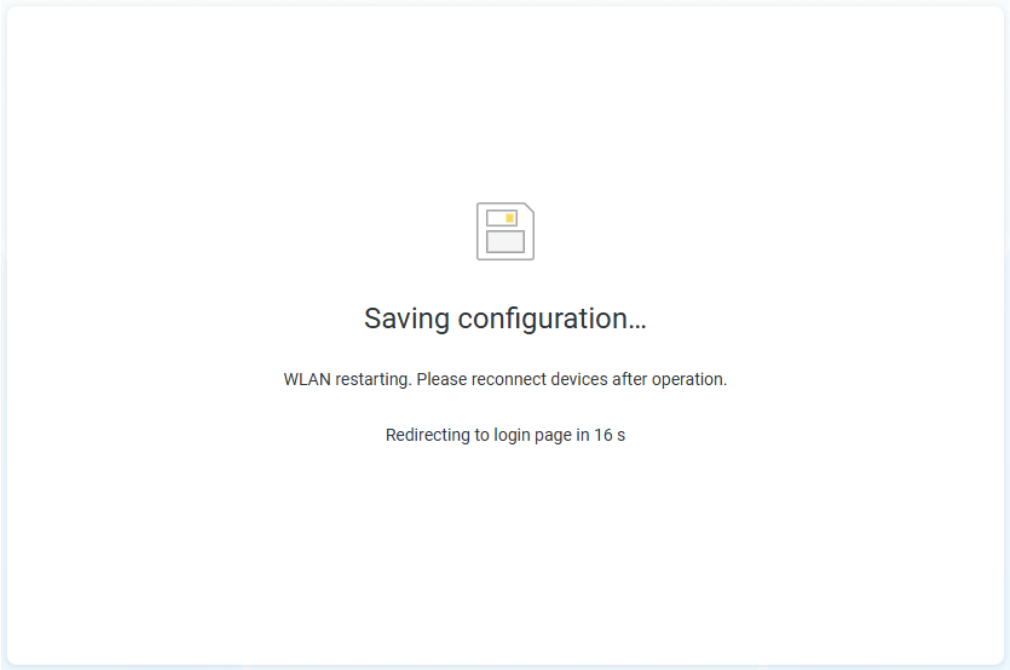
3. Configure the device's Wi-Fi AP settings for the 2.4GHz or 5GHz band (both can be configured, but only one is active at a time).



4. Set a new login password for the current user or keep the existing password by clicking **Set up later** in the subsequent pop-up window. Then select a device time zone. Enabling **Sync Local Time** will synchronize the device time with your local time.



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

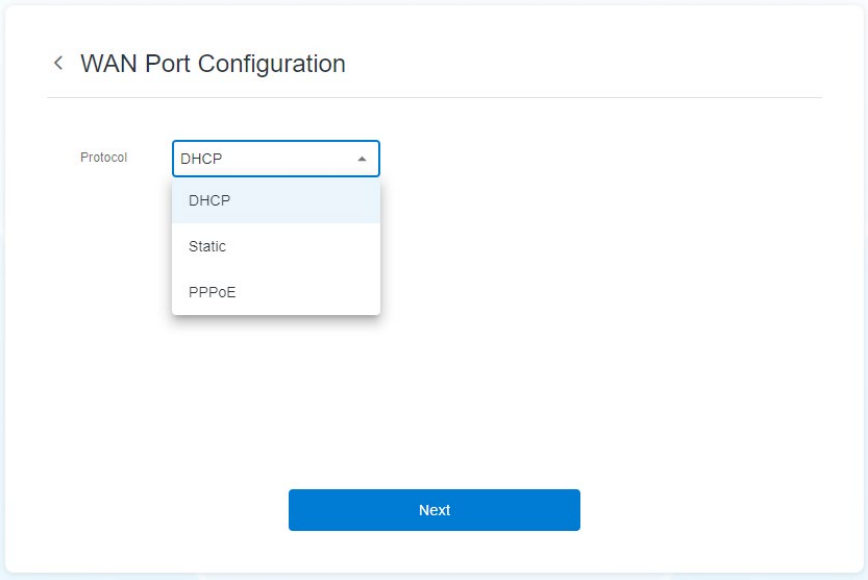


6. Log back in to the web portal using the new password.

After any device reset—including clearing configuration or factory reset—you must log in again using the credentials on the device label and complete the setup wizard again.

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

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

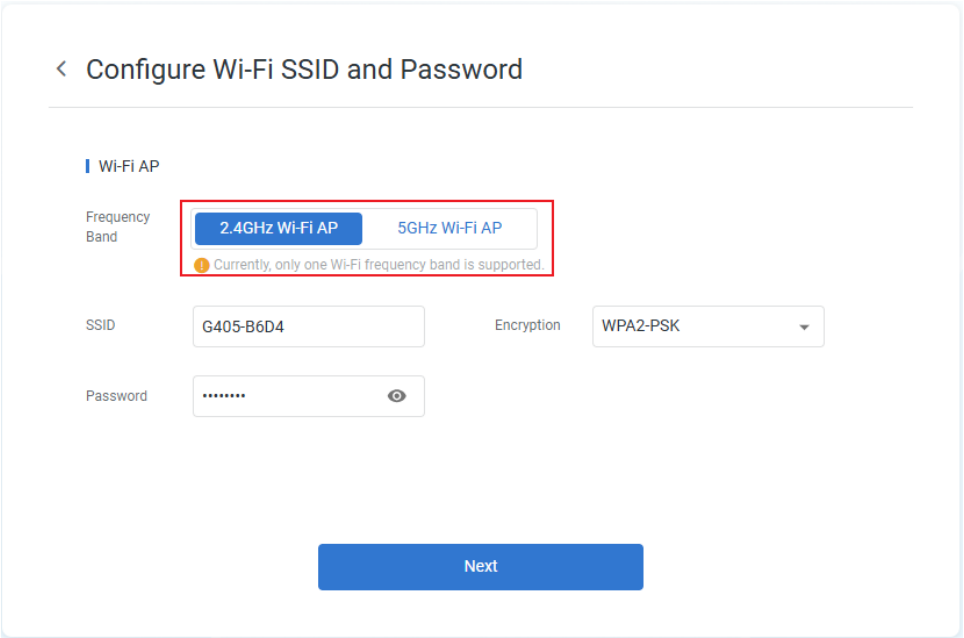


DHCP (Dynamic Host Configuration Protocol): A DHCP server **automatically** assigns IP addresses and network configuration (subnet, gateway, DNS) to the device.

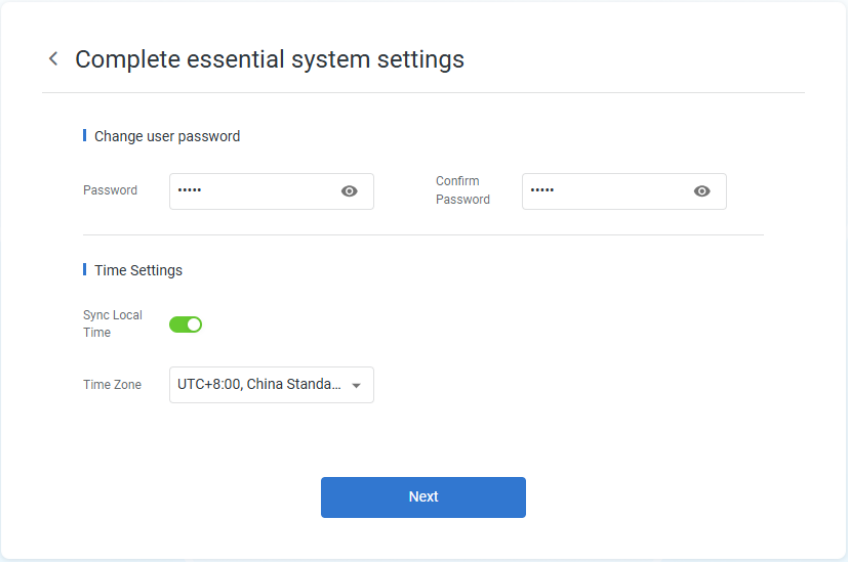
Static: IP settings are **manually** entered into the device and remain fixed until changed.

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).

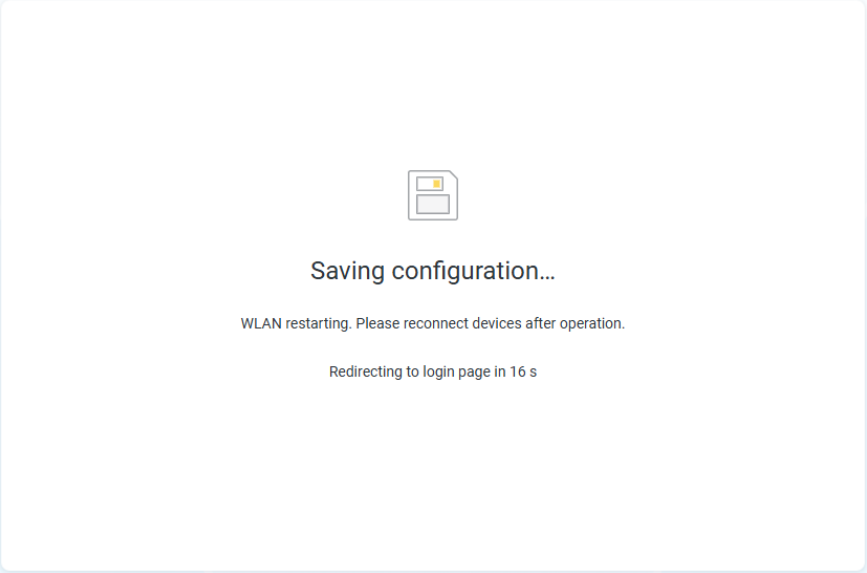
2. Configure the device's Wi-Fi AP settings for the 2.4GHz or 5GHz band (both can be configured, but only one is active at a time).



3. Set a new login password for the current user or keep the existing password by clicking **Set up later** in the subsequent pop-up window. Then select a device time zone. Enabling **Sync Local Time** will synchronize the device time with your local time.



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



5. Log back in to the web portal using the new password.

After any device reset—including clearing configuration or factory reset—you must log in again using the credentials on the device label and complete the setup wizard again.

2.3.2 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.

2.4 SSH Login

SSH is enabled on the G405 by default. Prior to establishing an SSH connection, make sure the Windows host PC (client) can reach G405's (server) IP.

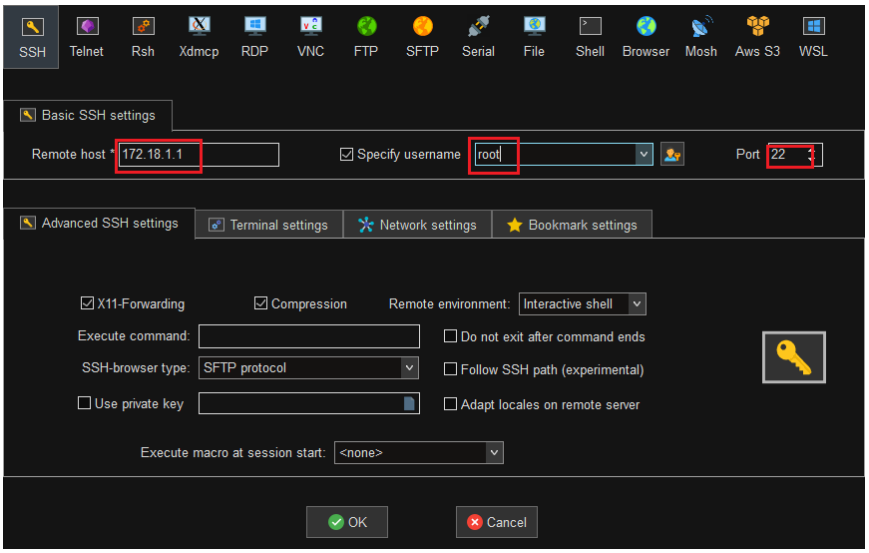
Method	Host PC Connection	Login Address
Option 1	Host connected to the device's LAN network (via Ethernet or Wi-Fi).	G405's LAN IP
Option 2	Host's WAN interface on the same IP subnet as G405's WAN interface (e.g., both connected to the same router or upstream Wi-Fi).	G405's WAN IP

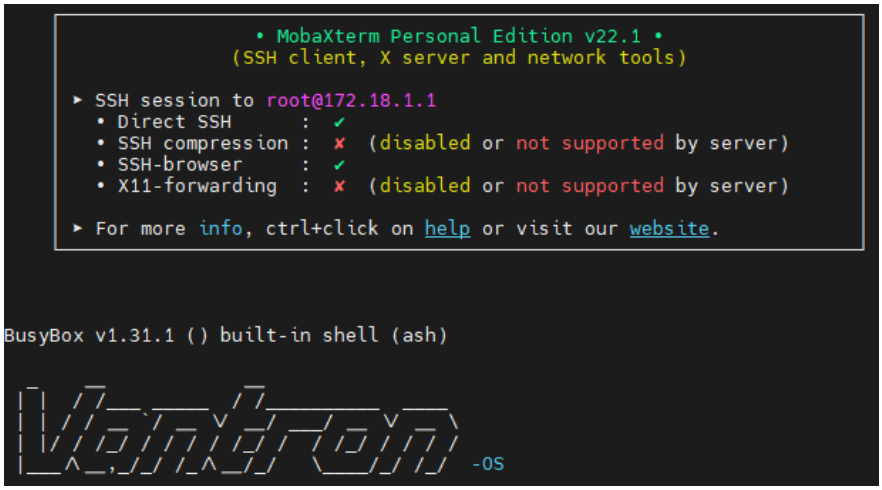
Example: SSH login via **LAN IP**

1. Connect the Windows host PC to G405's LAN network via Ethernet or Wi-Fi.
2. Install SSH client if it is not available.
   - **Windows host**:
     - PuTTY
     - Tera Term
     - MobaXterm
   - **Linux host**:

```
$ sudo apt-get update
$ sudo apt-get install ssh
```

3. **Windows host:** Launch the SSH client and log in to the device using its IP address (keep the port number 22 unchanged).





4. **Linux host**: Enter the following command and select "Yes" when prompted to log into the device.

```
$ ssh root@172.18.1.1                    // The device's IP
```

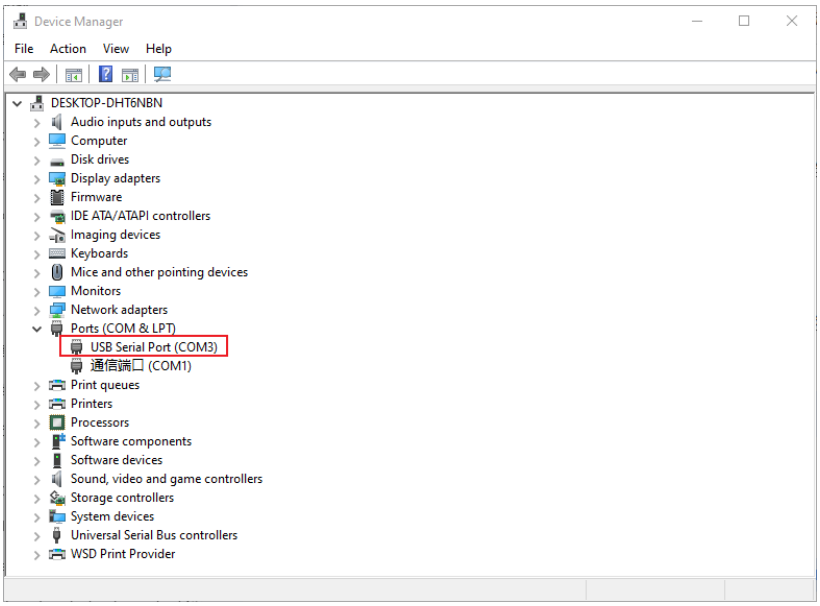
*SSH login requires **root privilege**. For security reasons, the root password is unique per device. Contact Technical Support to retrieve it.*

2.5 Debugging the Device (via Console Port)

The G405 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 are down, or the VantronOS web portal is inaccessible. All you need is a USB-to-RJ45 Console cable.

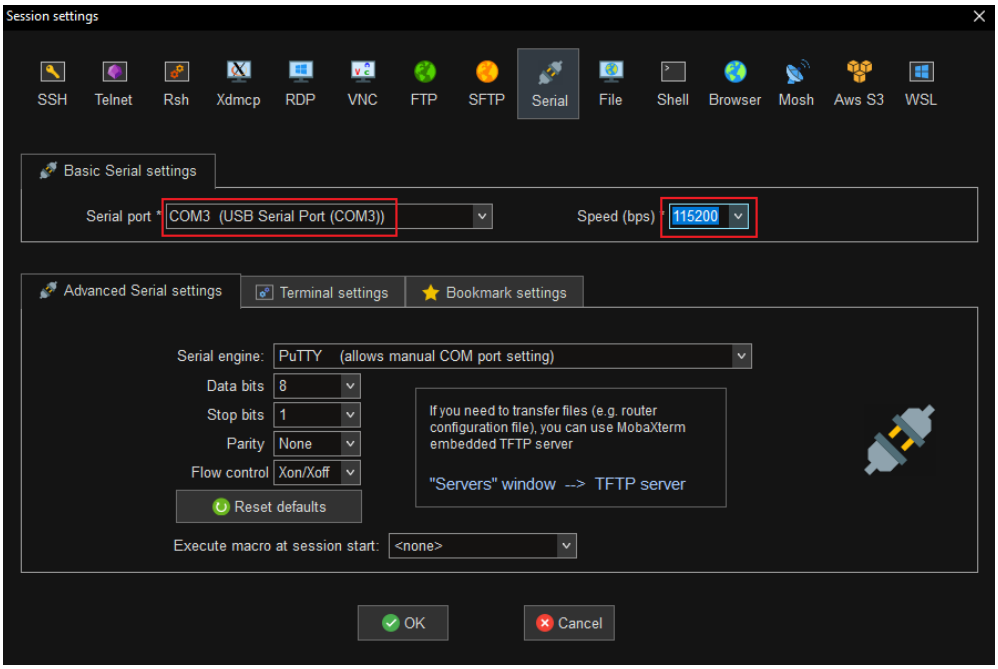
1. Connect the G405 to a Windows PC using a USB-to-RJ45 Console cable.

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 host PC.
   - PuTTY
   - Tera Term
   - MobaXterm

5. Start a Serial session with the following parameters:
   - Serial port: COMx (identified in Windows **Device Manager**)
   - Speed: 115200
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None



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

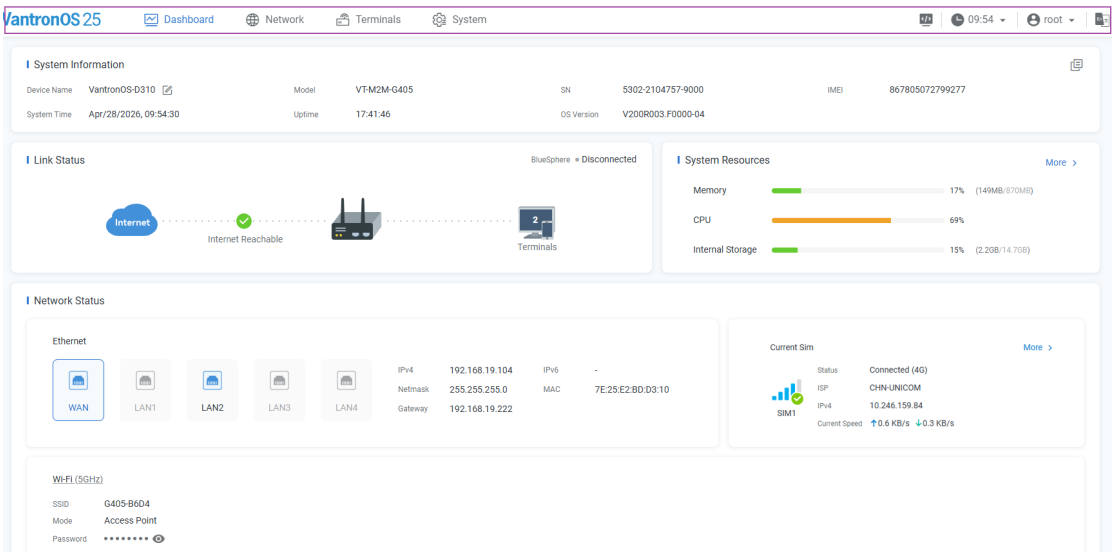
CHAPTER 3 DEVICE SETUP VIA VANTRONOS

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



VantronOS 25 is the latest version of the operating system, built on the legacy VantronOS 2, consisting of the following components:

Dashboard: Displays general device information and dynamic status updates.

Network: Manages network settings, including interface setup, link management, 2.4GHz/5GHz Wi-Fi setup, and advanced network configurations, such as static route, port mapping, and security configurations.

Terminals: Provides information of connected end nodes.

System: Displays device information, system settings, user password reset, network diagnostics, connection with BlueSphere GWM, device upgrade, etc.

Command Line Interface: Allows users to t access the device's shell for debugging.

Time Settings:

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

Refer to Section 3.7.1.2 for modifying the time settings.

User Avatar: Displays current user and offers a dropdown menu with the following options:

- Toggle Edge Computing functionality
- Log out

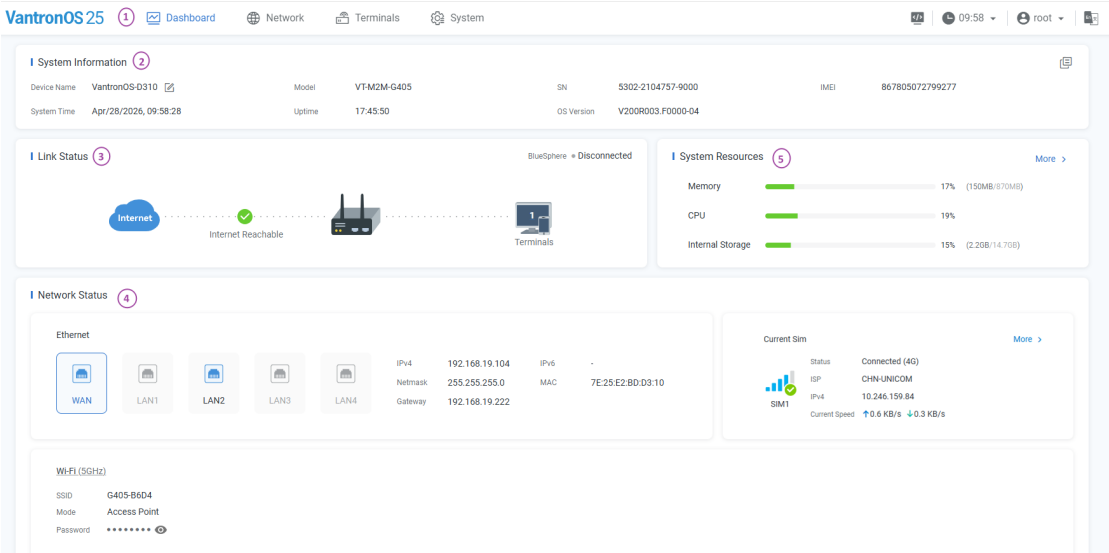
Language Toggle: English ⇄ Chinese.

3.1.2 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, interface connection status, traffic statistics, etc.



Description:

1. **Menu Tabs** — Highlights the active menu in blue.
2. **System Information** — Includes the device name, model, SN, IMEI, current system time, link uptime, and OS version.
   - Clicking the pencil icon next to the device name allows you to modify the device name as needed.
   - Clicking the copy icon in the upper-right corner copies all system information.
3. **Link Status** — Shows a simplified network topology of the current device.
   - Clicking the connected terminal count navigates to the end node page, where detailed end node information is displayed.
4. **Network Status** — Displays the live status for each network interface.
   - Ethernet: Active ports are highlighted in blue, with IPv4 and IPv6 addresses, subnet mask, gateway, and MAC address displayed for the selected port.
   - 2.4GHz/5GHz Wi-Fi: Operation mode (e.g., AP or STA) and associated network details.
   - Cellular: Mobile network information. Clicking **More** redirects you to the cellular configuration page.
5. **System Resources** — Shows dynamic device performance metrics, including memory usage (used/total), CPU usage, and storage usage (used/**total**).
   - Clicking **More** expands the information for external storage, if available.

3.3 Network

The **Network** menu centralizes critical network management functions, including interface settings, wireless configurations, VPN, 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.

Interfaces on the G405 are categorized as either WAN or LAN.

WAN interfaces include: 2.4GHz/5GHz Wi-Fi client, 4G LTE, and Ethernet WAN.

LAN interfaces include: 2.4GHz/5GHz Wi-Fi AP and Ethernet LAN.

3.3.1 WAN Interface

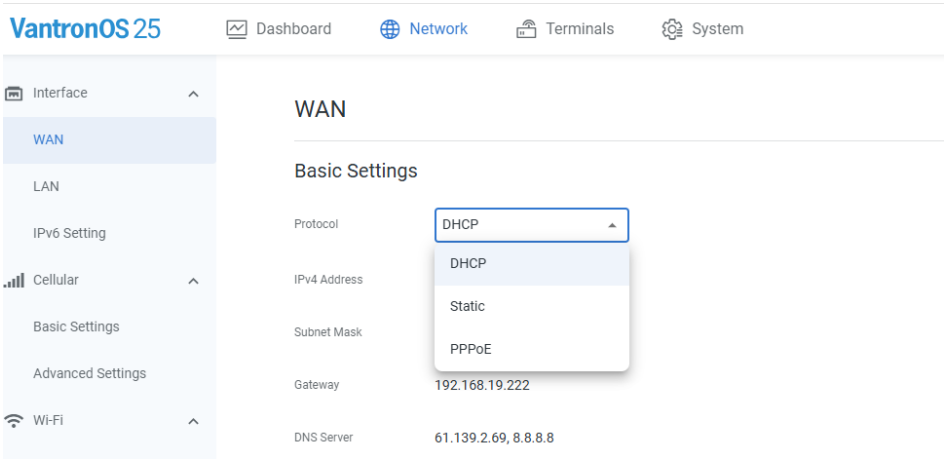
The WAN interface page includes the following three functionalities:

1. **Basic IP configuration** — Selects the WAN interface IP protocol (e.g., DHCP, Static IP, PPPoE).
2. **Interface bridging** — Converts the bridged interface to a WAN interface and places it on the same network level as other LAN interfaces, thereby causing it to lose local management and DHCP server capabilities.
3. **Link priority IPv4** — Displays all upstream links and the port status, letting you change their priority.

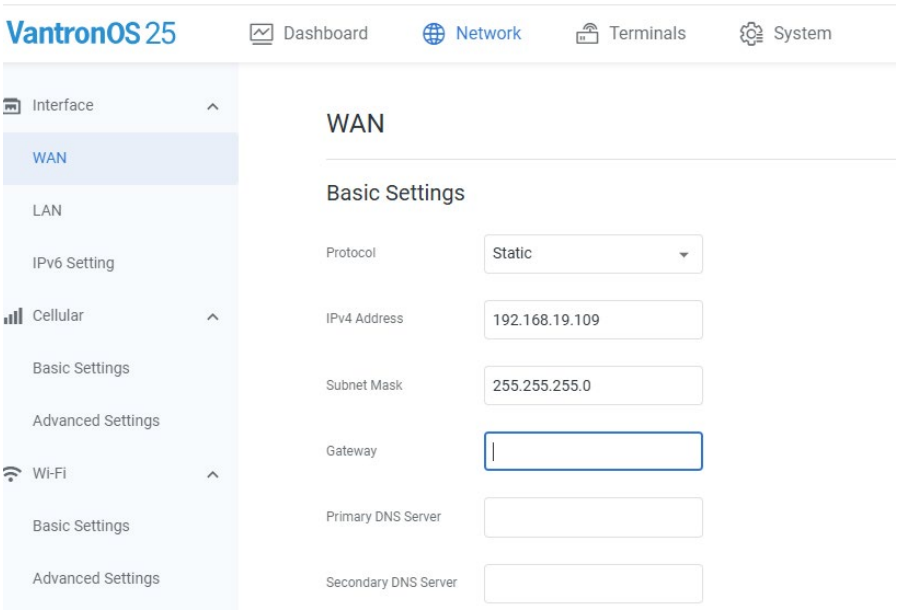
Whenever you make a change, always ensure the host PC and the G405 are on the same subnet for smooth VantronOS login.

3.3.1.1 Basic IP Configuration

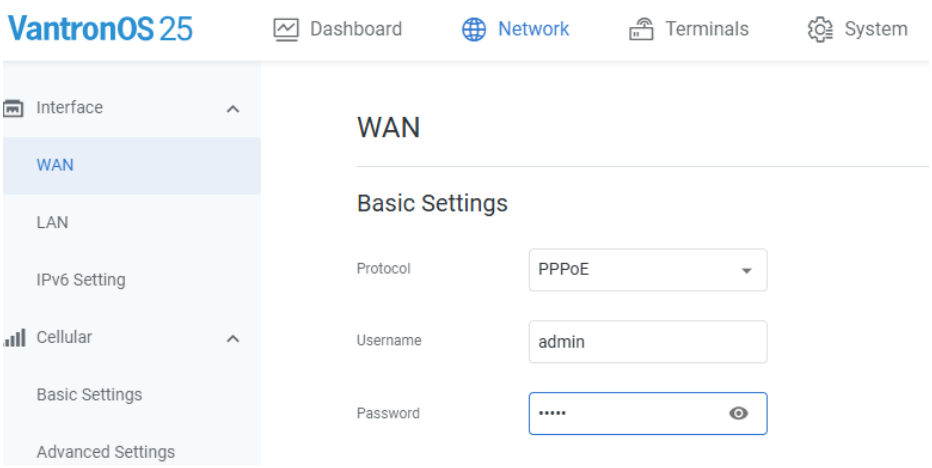
DHCP: The DHCP server will **automatically** assign an IP address for the interface.



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



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



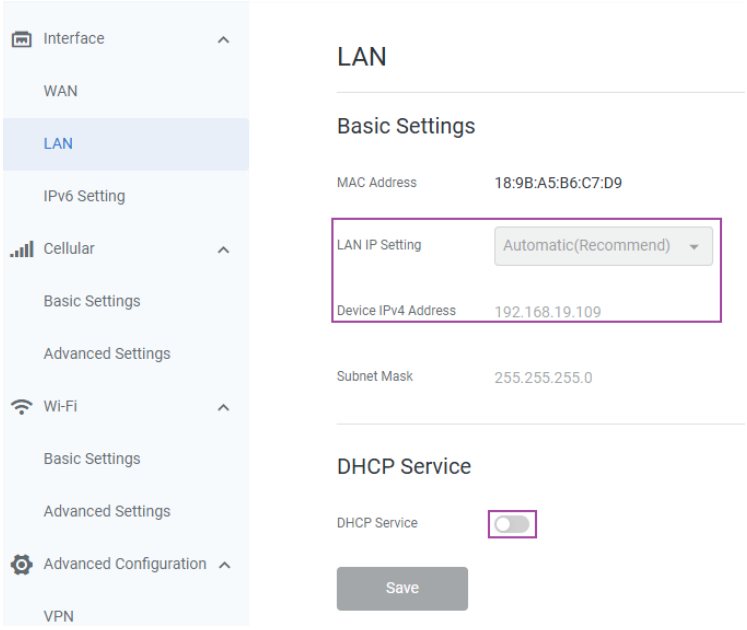
*Whenever you make a change, be sure to click **Save** for the change to take effect.*

3.3.1.2 Interface Bridging

You can choose to bridge either Wi-Fi or Ethernet interface. Bridging an interface places it at the same network level as the LAN interfaces.

After bridging:

- The LAN interfaces **no longer** provide NAT and DHCP services to connected devices.
- Bridging either an Ethernet WAN or Wi-Fi STA interface also moves the other into the LAN domain.
- The bridged interface obtains an IP address from the upstream DHCP server, just like other LAN interfaces, leaving the device with only **one** effective LAN IP.



- Devices connected to the LAN interfaces of the G405 will obtain IP addresses from the upstream DHCP server. Consequently, to manage the device, you must retrieve its IP address from the upstream DHCP server.
- If you connect the device's Ethernet WAN port to an upstream router before bridging the Ethernet interface, the IP address assigned by the router will be displayed in seconds.
- If you choose to bridge the Wi-Fi interface, available SSIDs will be displayed for quick connection.
- To cancel **interface bridging**, enable the **DHCP service** on the **Interface > WAN** page.

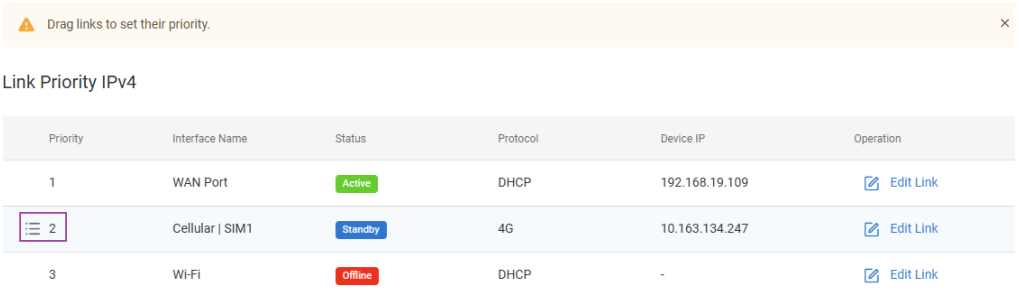
3.3.1.3 Link Priority

In the **WAN > Link Priority** section, all available upstream links on the device are displayed with detailed status information.

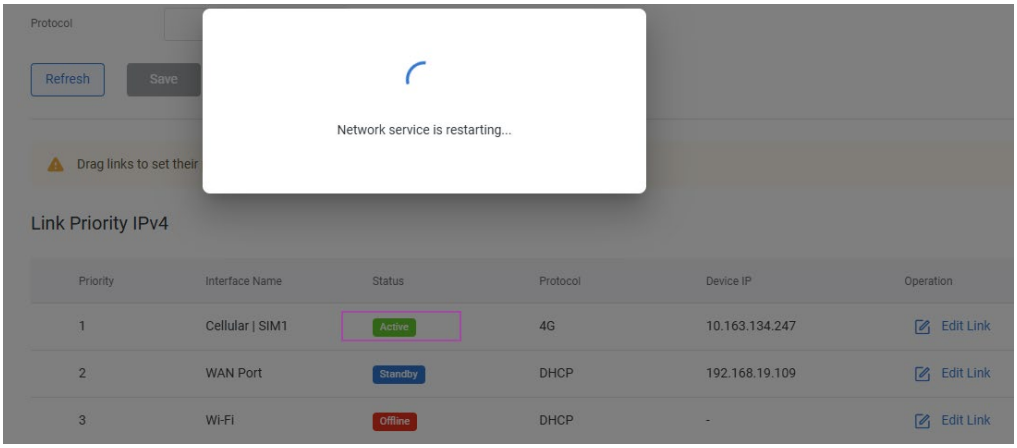
Active links are prioritized based on the following rule by default: Ethernet (WAN) > Wi-Fi (Client) > Cellular > others. The device supports multi-link failover. If a higher-priority link goes offline, the first available standby link takes over to ensure the device remains online.

To manually set the network priority:

1. Hover over the target link; it will be highlighted with a light blue background.

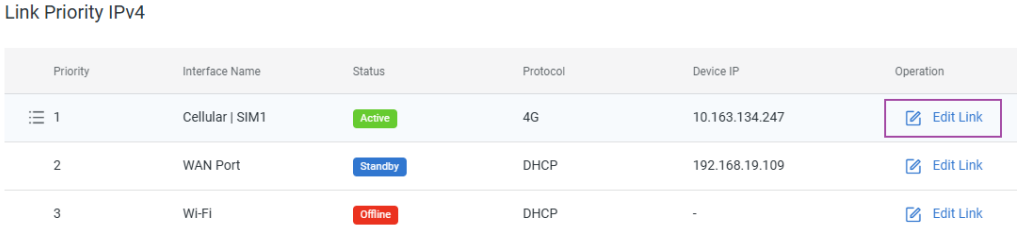


2. Drag the target link up or down to the desired position. If moved to the top, the link status will change to **Active** (if online).



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

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

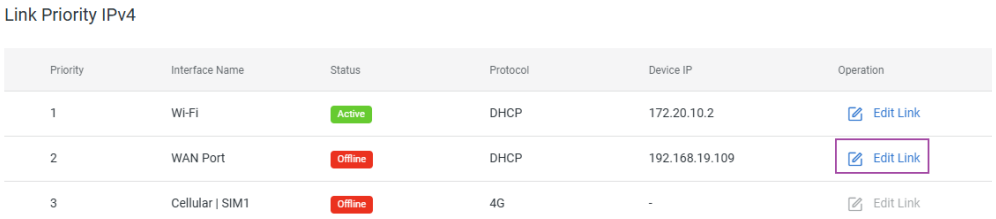


Editable fields include: primary & secondary probe addresses, and probe interval.

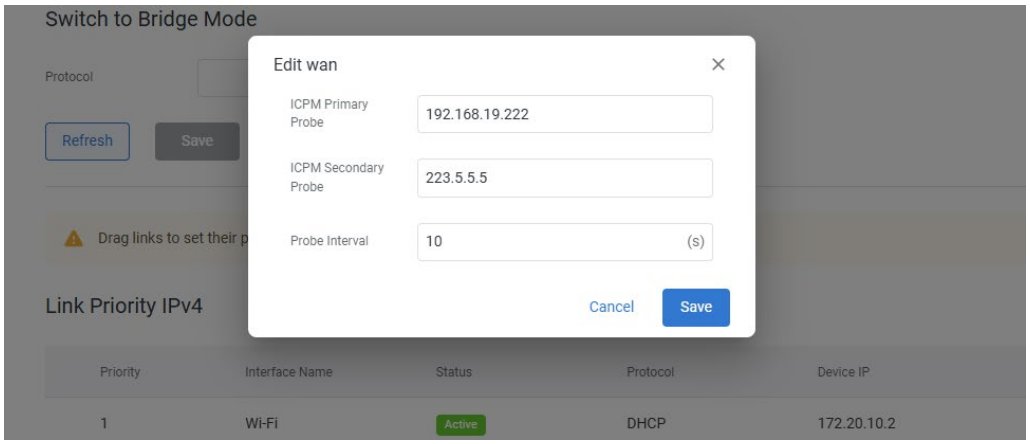
3.3.1.4 Link Diagnosis

When a link is shown as **Offline**, first make sure the interface is connected to the upstream network. Once verified, you can run a reachability test by setting ICMP probe's destination address to the desired target (e.g., the gateway IP) on that link.

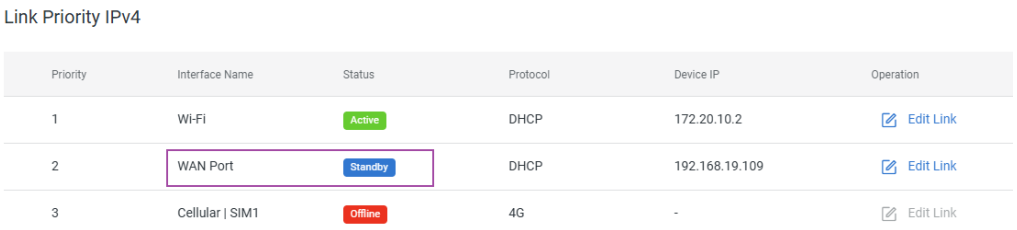
1. Locate the target link, and click **Edit Link**.



2. In the configuration menu, enter a reachable probe address and save.

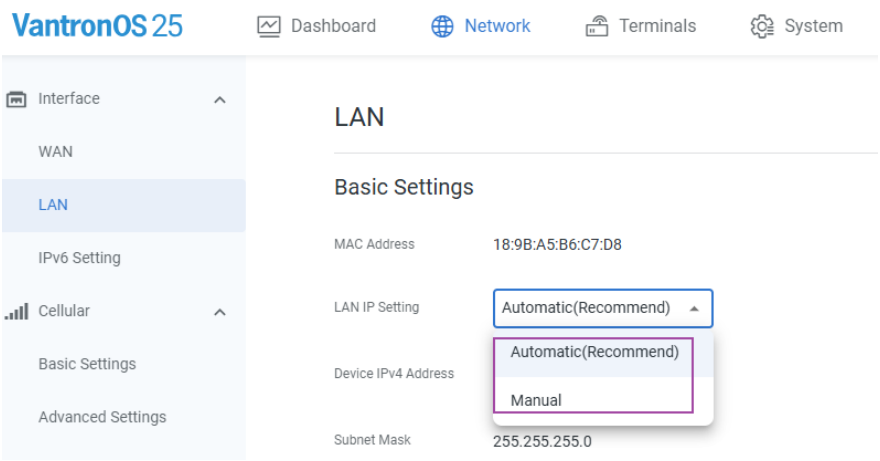


3. Check the link status to verify if it becomes reachable.



3.3.2 LAN Interface

The G405 defaults to the 172.18.1.1 subnet for IP assignment.



3.3.2.1 Subnet Conflict

A subnet conflict may occur when a Vantron communication device (router/gateway/HaLow AP) acts as a DHCP server for the G405's uplink interface and its factory LAN address (172.18.1.1) overlaps with the G405's default LAN subnet.

As a best practice, we recommend reconfiguring the G405's LAN IP address to a different subnet when connecting to a Vantron communication device to avoid IP conflicts.

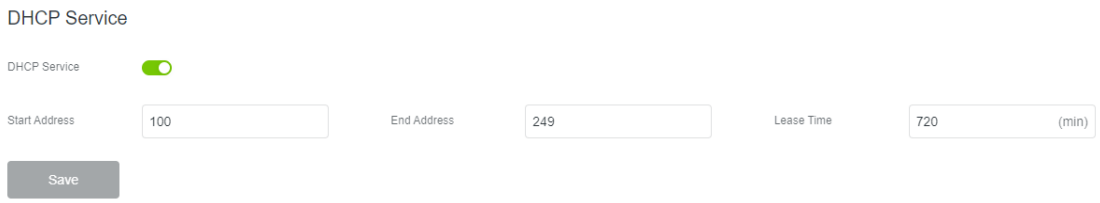
Manual IPv4 address configuration requires entering an IPv4 address and the subnet mask. If you modify the device's LAN IP address, reconnect the host PC to the device to maintain access.

3.3.2.2 DHCP Service & DHCP Reservation

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

Editable fields under **DHCP Service**:

- Start & End addresses: IP addresses within this range are leased to clients.
- Lease Time: The valid duration for which the G405, 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 the G405 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.

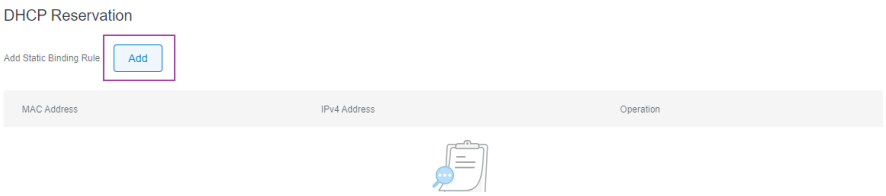


DHCP Reservation allows a DHCP server to reserve a specific IP address for a particular device (client) based on its MAC address. When enabled, the server will always assign the same IP address to that device whenever it connects to the network, optimizing the network's IP address space and enhancing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

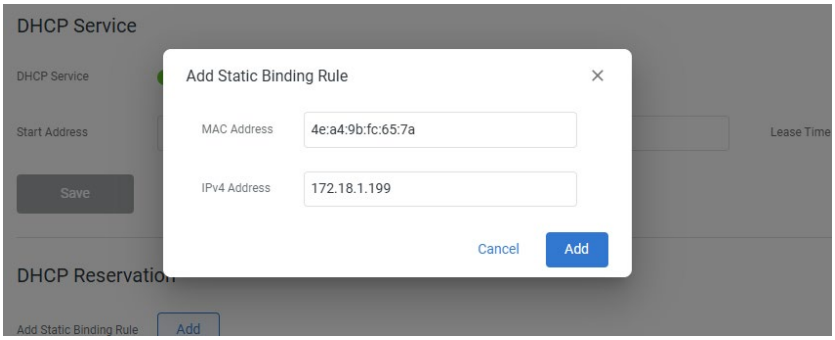
By adding a DHCP reservation rule to the G405, the specified client device will maintain the allocated IP address to reduce configuration errors.

Steps of adding a DHCP reservation rule:

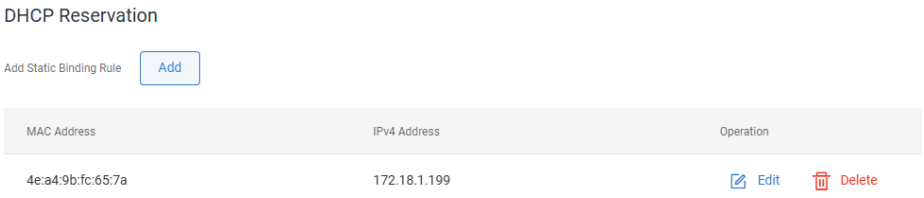
1. Click **Add** under **DHCP Reservation**.



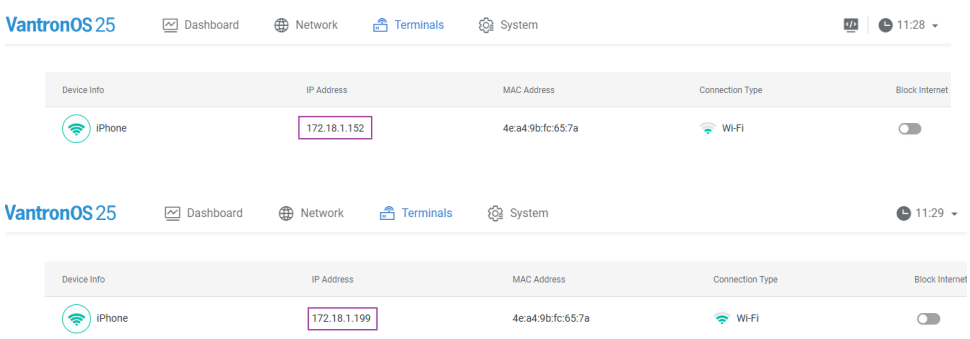
2. Enter the client's MAC address and allocate an IP between the start and end addresses specified under **DHCP Service**.



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



4. If you have reserved a different IP for a connected device, reconnect the device to the G405, and its IP will update accordingly as shown under **Terminals**.



3.3.3 IPv6 Settings

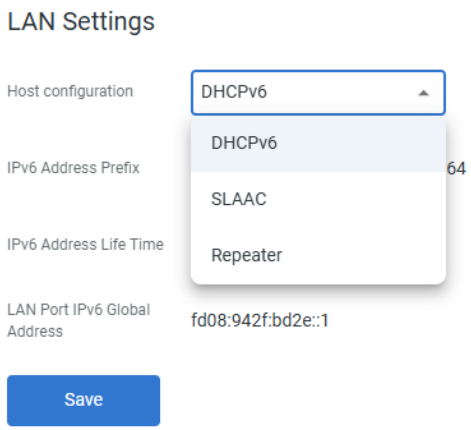
IPv6 (Internet Protocol version 6) is an advanced network layer protocol succeeding IPv4. It is designed to solve IPv4 address exhaustion and support enhanced networking features. It provides 128-bit addresses, eliminating the need for NAT and enabling end-to-end connectivity.

IPv6 is disabled by default, and you can enable this feature as needed.

When IPv6 is enabled:

- The **WAN** interface defaults to DHCPv6 to automatically obtain an IPv6 address from the upstream network, requiring no manual input.
- The **LAN** interface defaults to DHCPv6 for address assignment, which requires manual configuration of the IPv6 prefix and address lifetime.

In LAN settings, you can further modify the IPv6 assignment method.



- **DHCPv6**: The G405 acts as a stateful DHCPv6 server, assigning full IPv6 addresses to LAN devices with configurable prefix and lease time.
- **SLAAC:** The G405 advertises an IPv6 prefix via RA messages. LAN devices automatically generate their own addresses for plug-and-play use.
- **Repeater:** The G405 relays upstream IPv6 configurations transparently. LAN devices obtain addresses directly from the upstream network, with no local address assignment.

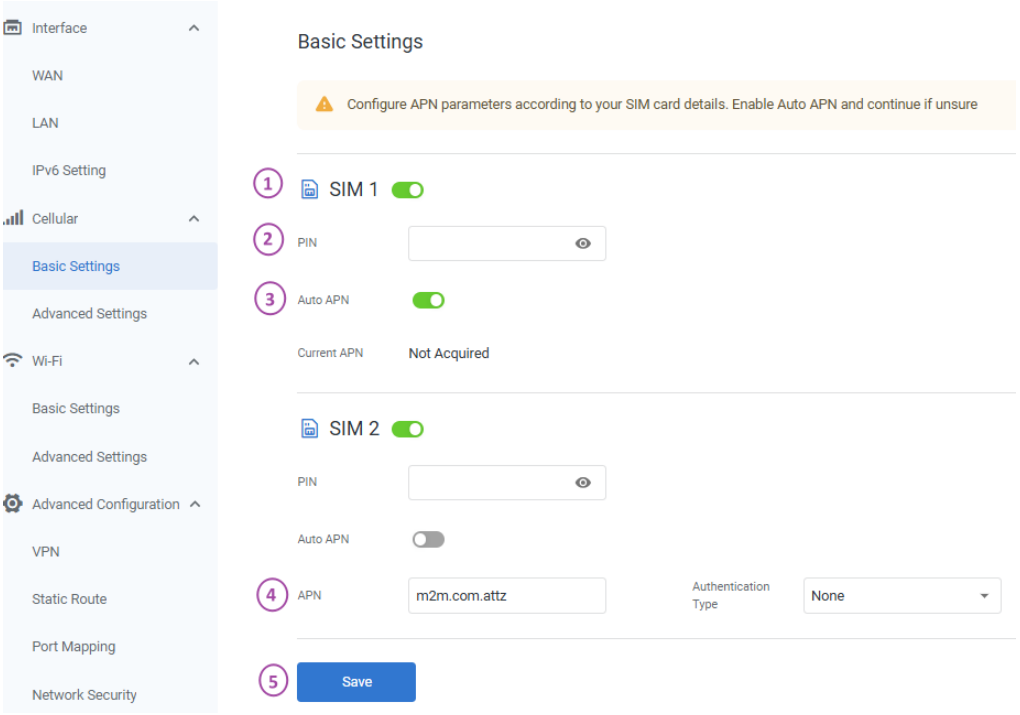
3.3.4 Cellular

The G405 supports dual-SIM communication. Default cellular configurations from the initial setup wizard are retained if available. To modify settings for a SIM card, ensure it is enabled first.

3.3.4.1 Basic Settings

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

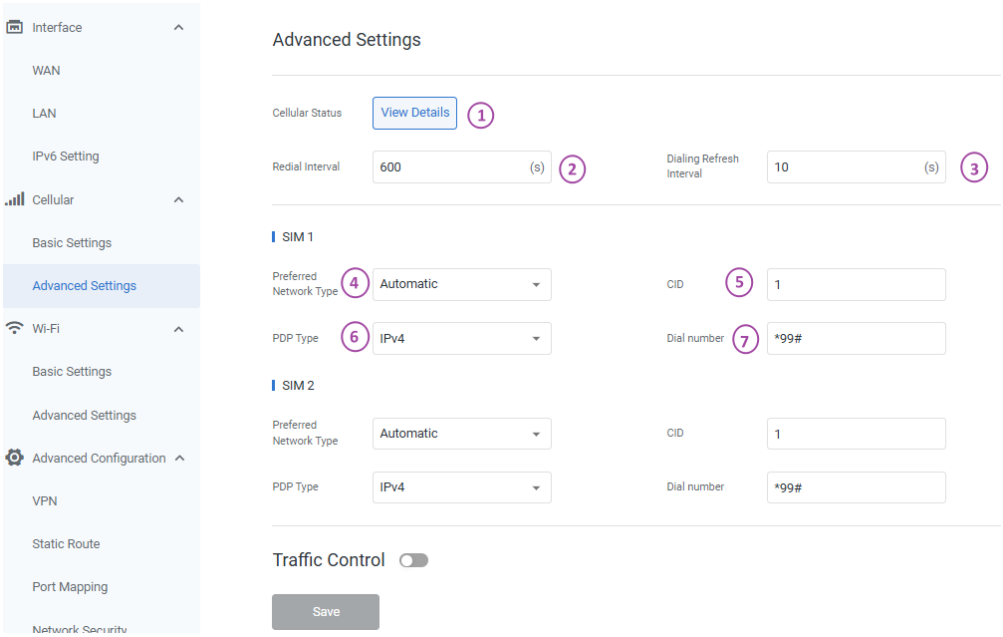
PIN is optional. If you are not sure about the APN and authentication type, you can enable **Auto APN**.



Description:

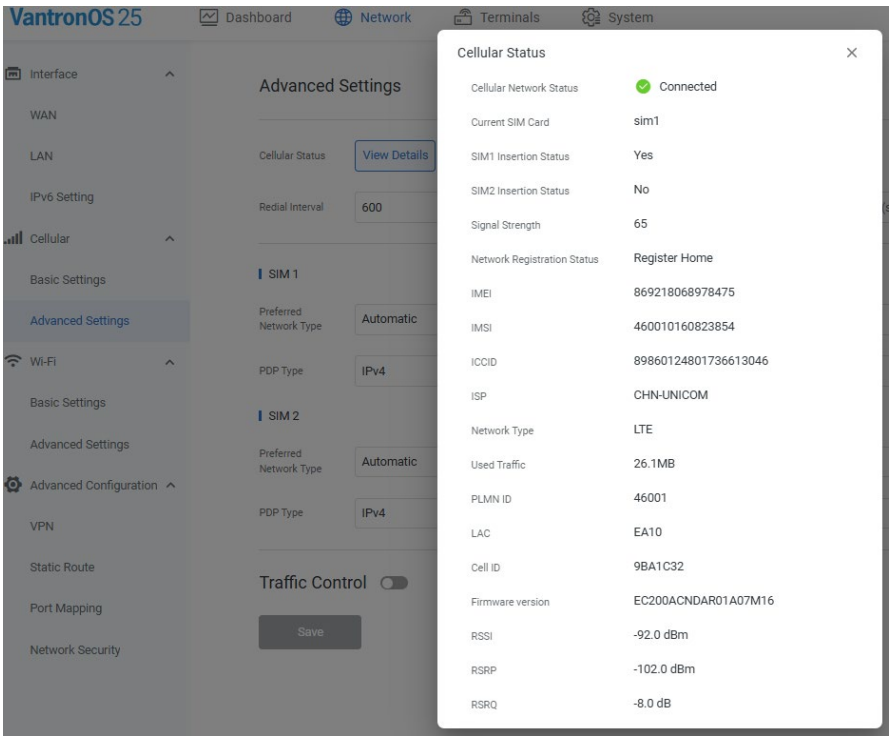
1. Insert an activated SIM card into the Micro SIM slot and enable the corresponding SIM card before configuration.
2. The SIM card PIN code is optional.
3. If you are unsure of the carrier parameters, enable **Auto APN**.
4. You can also enter the parameters manually.
5. Click **Save** to allow the changes to apply.

3.3.4.2 Advanced Settings



Description:

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).

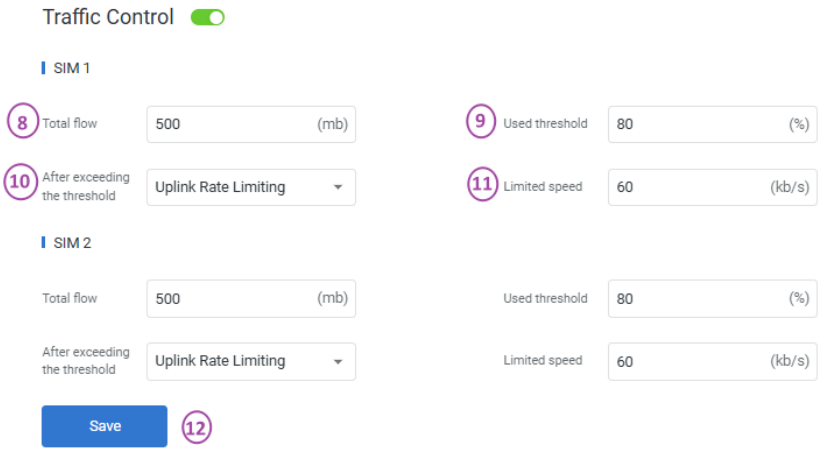
3. Dialing refresh interval — Specifies the interval (in seconds) to refresh the last dal-up status.

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.

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

If you need to control the data traffic of a specific SIM card, enable the **Traffic Control** feature, then edit the parameters for the corresponding SIM card.



8. Total flow — Sets the maximum data usage (in MB) available for the G405.
9. Threshold — Defines a data usage percentage (in %) that triggers a restriction action when exceeded.
10. You can select to either: Restrict data speed or cut off the link.
11. If uplink rate limit is selected, enter a speed limit (in KB/s) to control data rate.
12. If you have made any changes, click **Save** to apply.

    In the example screenshot, upon reaching 80% of the preset total flow (500MB), the system will limit the data rate to 60 KB/s.

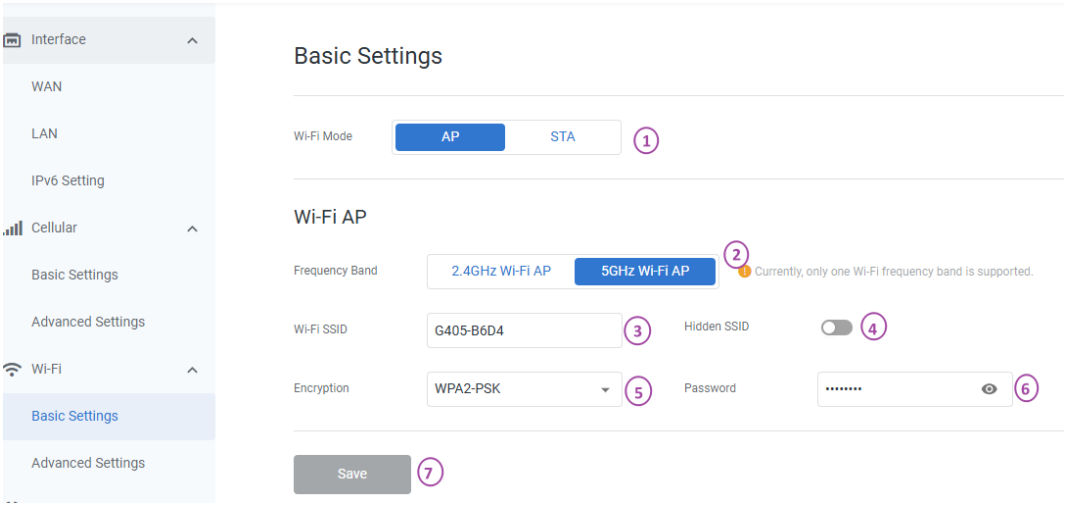
3.3.5 Wi-Fi

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

On the **Basic Settings** page, you can switch the Wi-Fi operation mode and modify the basic parameters accordingly.

On the **Advanced Settings** page, you can disable or enable the Wi-Fi feature, and configure additional parameters according to the Wi-Fi mode selected in the **Basic Settings** page.

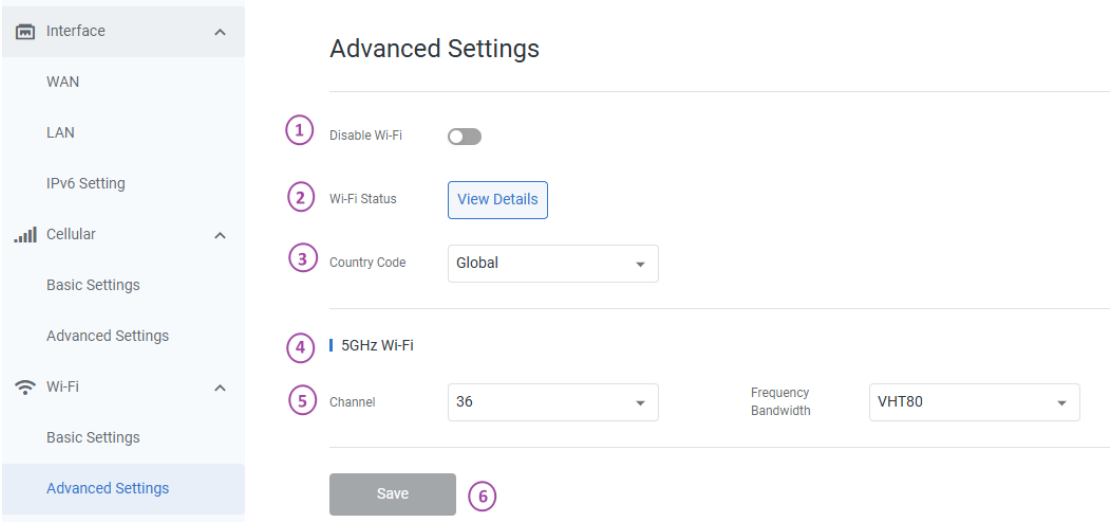
3.3.5.1 AP-Mode Basic Settings



Description:

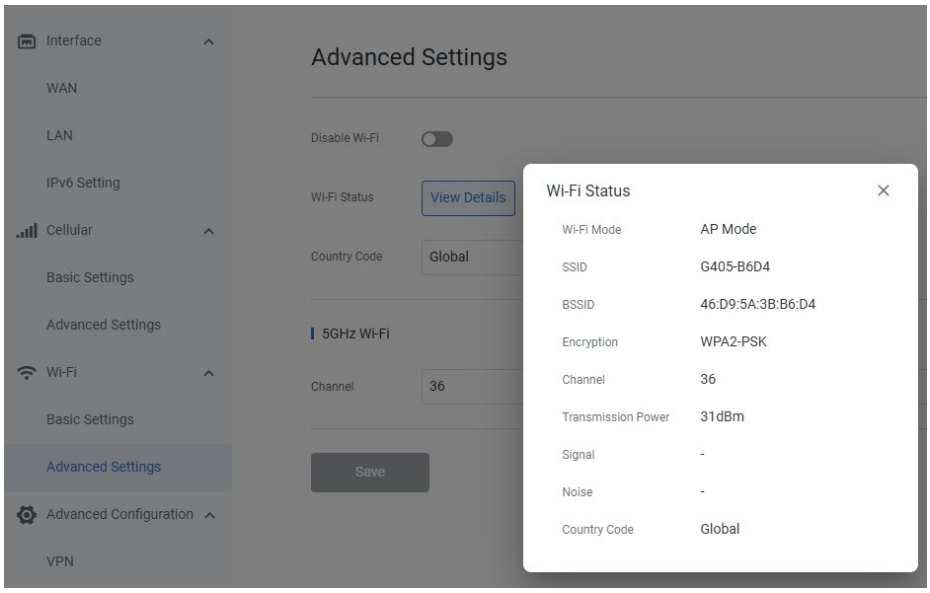
1. Click **AP** and confirm the action in the pop-up to enable the AP mode.
2. The G405 supports dual-band Wi-Fi operation. Both bands are configurable, but only the selected band will be active.
3. Wi-Fi SSID — The Wi-Fi AP's name.
4. Hide SSID — Once hidden, clients cannot scan the device's SSID and must manually enter the exact SSID and password to connect.
5. Encryption mode — The basic protocols for establishing secure communication. (None, WPA-PSK, WPA2-PSK)
6. Password — Credential for connecting the device's Wi-Fi.
7. Click **Save** to allow changes to tack effect.

3.3.5.2 AP-mode advanced settings



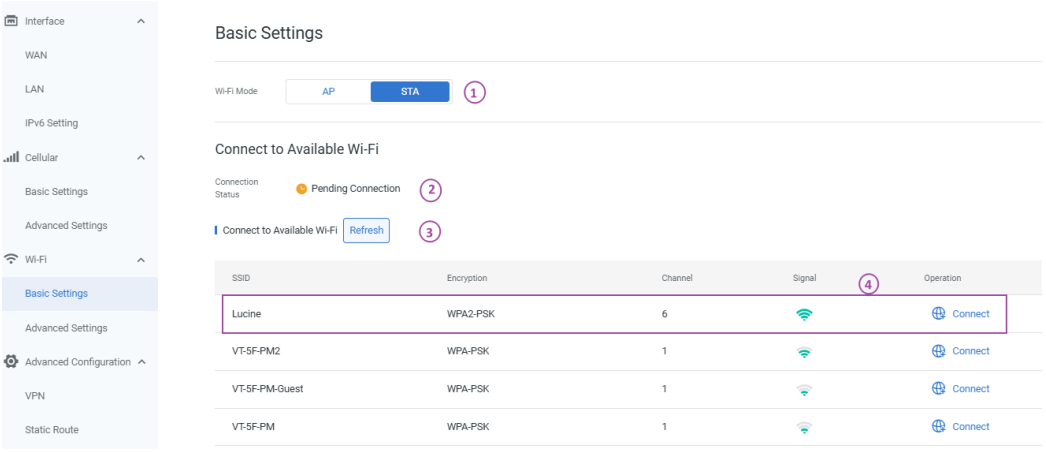
Description:

1. Disable/Enable the Wi-Fi feature.
2. 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.



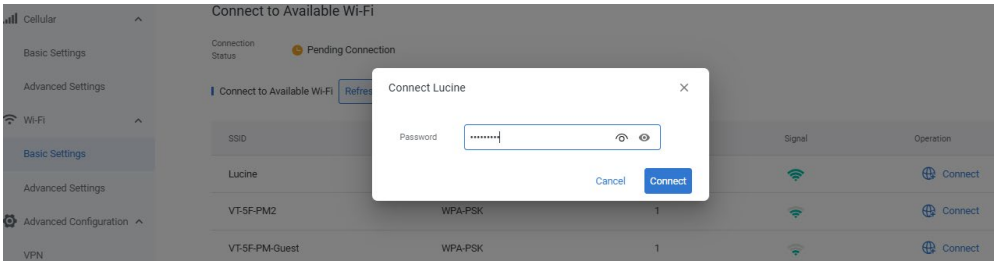
3. Country code (‘global’ by default).
4. The currently active band matches the selection made in the basic settings.
5. Channel options (configurable) and default frequency bandwidth.
6. If you have modified the parameters, click **Save** to apply.

3.3.5.3 Client-Mode Basic Settings

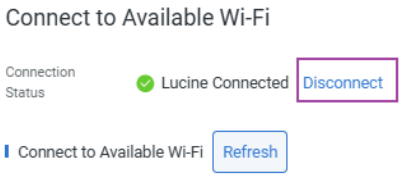


Description:

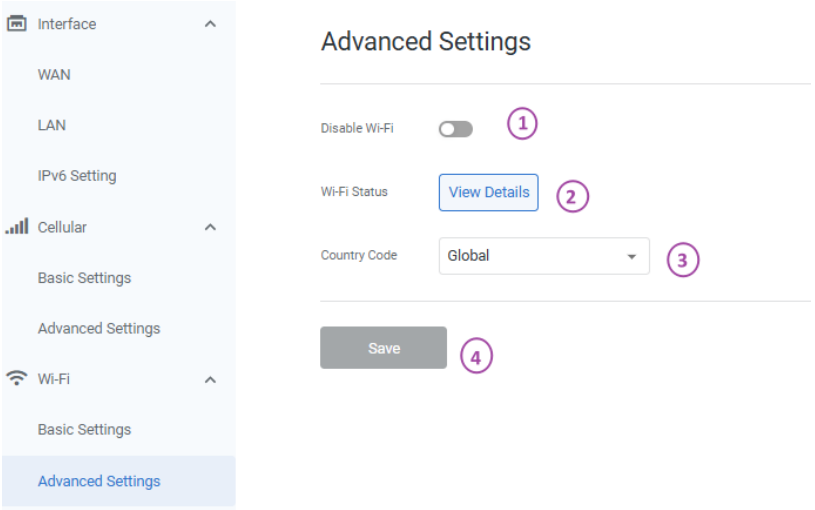
1. Click **STA** and confirm the action in the pop-up to enable the **Client** mode.
2. Current Wi-Fi connection status.
3. If the target SSID is not included in the list, click the button to refresh the list.
4. Information of available Wi-Fi APs is displayed. Click **Connect** and enter the password to connect to the target AP.



When the device successfully establishes a connection to the target Wi-Fi AP, ***Disconnect*** *becomes available, next to the connected SSID.*

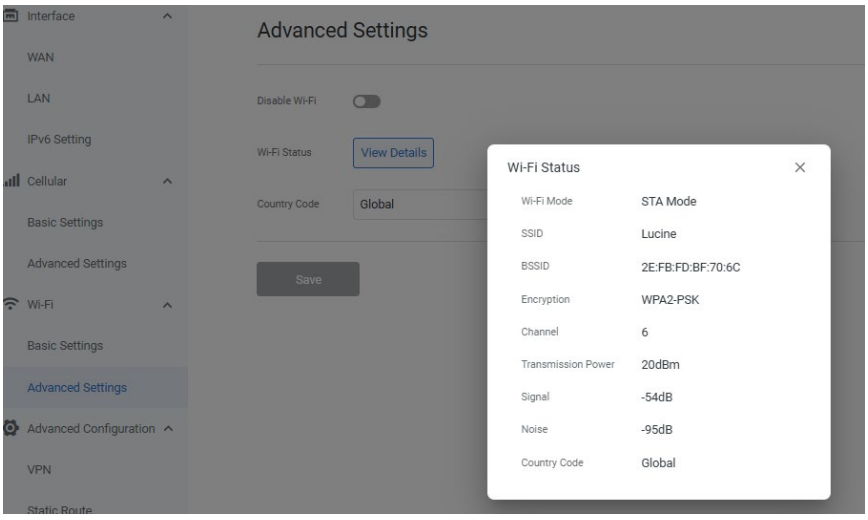


3.3.5.4 Client-Mode Advanced Settings



Description:

1. Disable/Enable the Wi-Fi feature.
2. 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 mode, channel, transmit power, etc.



3. Country code (‘global’ by default).
4. If you have modified the parameters, click **Save** to apply.

3.3.6 VPN

A virtual private network (VPN) lets you use the Internet to securely access your network remotely. The G405 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.

3.3.6.1 OpenVPN Server-Client Network Settings

Scenario	Description
Server has a public IP (or DDNS); Client connects over the Internet	Standard deployment across public networks. Server is directly accessible from the Internet. (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	Server and client are on the same LAN. (Local testing)

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

Client configuration:

The IP/domain for the **remote** field in the configuration file for an OpenVPN client 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 is 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 G405 gateways for the connection, make sure there is no IP address 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.

Server configuration:

In a typical VPN deployment, clients are supposed to access the internal network via the server. Therefore, users need to modify the following directives in the configuration file for an OpenVPN server.

TUN mode

- **port:** The listening port you want the server to use (e.g., port 1194).
- **push "route…":** Internal network subnet.
- **push "dhcp-option DNS…":** The IP address of the DNS server on the internal network.
- **server:** The virtual IP pool of the VPN tunnel for the client to use.

TAP mode

- **port:** The listening port you want the server to use (e.g., port 1194).
- **ifconfig:** Internal network subnet.
- **ifconfig-pool:** The virtual IP pool that defines a start IP and an end IP for the client to use.

In a VPN network:

TAP mode operates at Layer 2 of the OSI model, creating an Ethernet bridge between the VPN and physical network.

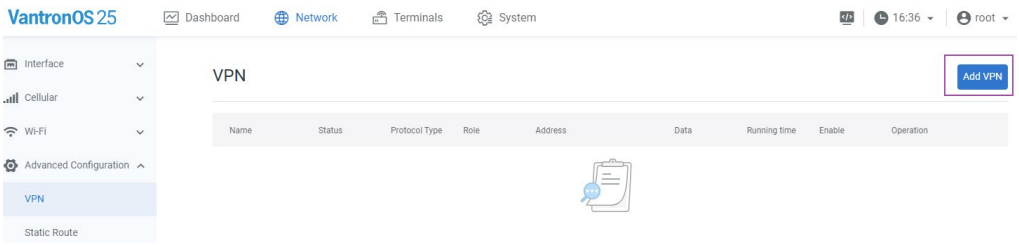
TUN mode works at Layer 3, handling only IP packets (both IPv4 and IPv6) while creating a separate routed network for VPN clients. **TUN** is the **preferred choice** for general-purpose VPN use cases like remote work, secure web browsing, and cloud access, offering better performance and simpler configuration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

3.3.6.2 OpenVPN Server Setup

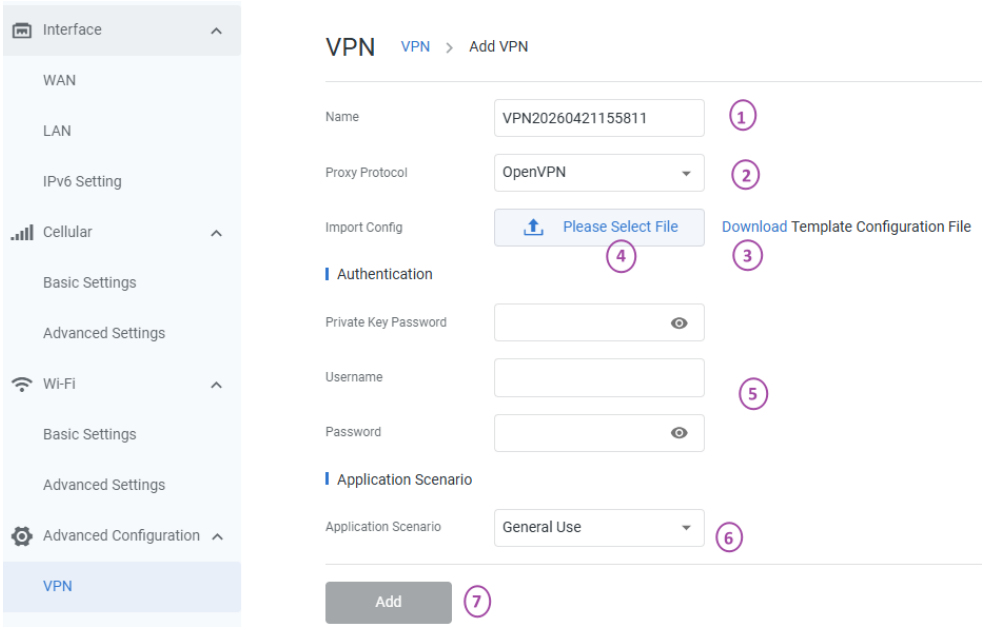
Please note that the configuration templates provided here are for test only. You are recommended to modify the certificates and keys in the configuration file to your own.

To add an OpenVPN **server** rule for the current G405:

1. Synchronize both the G405 (server) and the client to the same NTP server (for certificate validation).
2. Navigate to **Network > Advanced Configuration > VPN,** and click **Add VPN**.



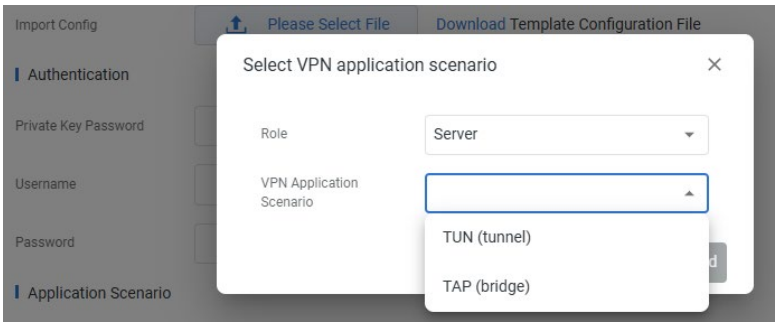
3. In the configuration page, set up the OpenVPN server:



Description:

1) Enter a VPN rule name (current timestamp is the default).
2) Select the OpenVPN protocol (other protocols will be available soon).

3) Click **Download** to select the protocol mode and export the corresponding template .conf file for modification. (Skip this step if you use a pre-configured file)



Refer to Section 3.3.6.1 for the configuration instructions.

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

5) Set the authentication credentials, if necessary.

6) Select an application scenario.

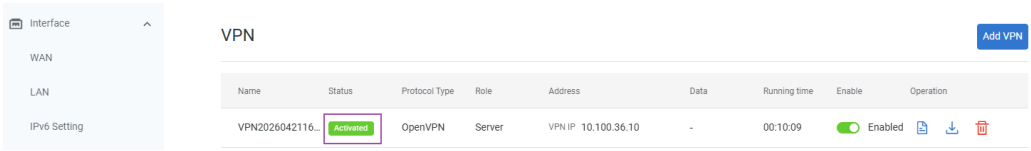
Refer to Section 3.3.6.4 for details on the application scenarios.

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

4. The newly created rule is enabled by default and shows an **Initializing** status during device configuration.

*If the status shows **Disconnected**, ensure your configuration is correct and there is no conflict with other rules, then recreate the rule if necessary.*

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



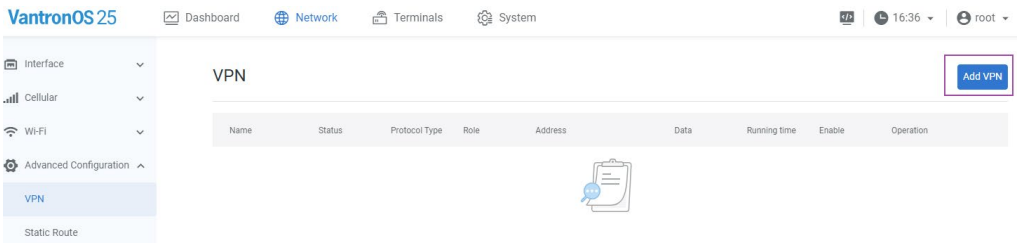
After the setup, you can enable/disable the rule, view its logs (useful for troubleshooting if the rule fails to activate), download the configuration file, or delete it.

3.3.6.3 OpenVPN Client Setup

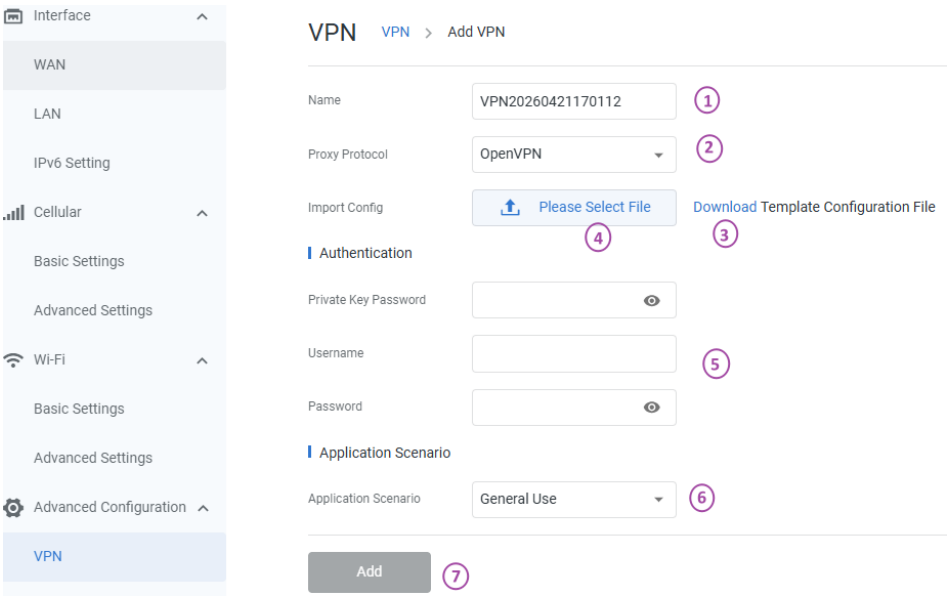
Please note that the configuration templates provided here are for test only. You are recommended to modify the certificates and keys in the configuration file to your own.

To add an OpenVPN **Client** rule for the current G405 and connect it to an OpenVPN server:

1. Synchronize both the G405 (client) and the server to the same NTP server (for certificate validation).
2. Navigate to **Network > Advanced Configuration > VPN,** and click **Add VPN**.



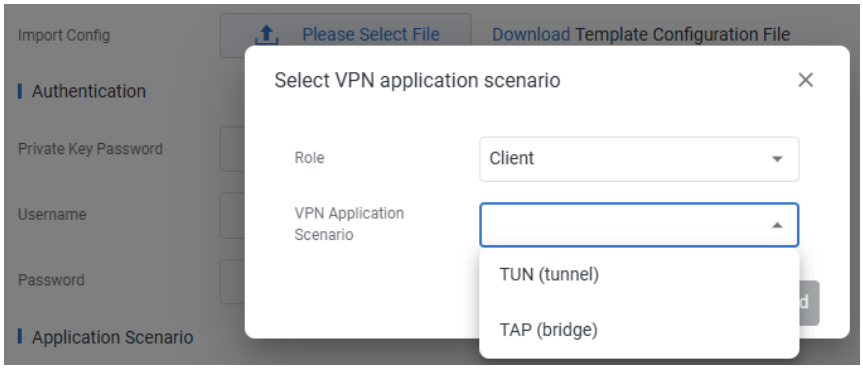
3. On the configuration page, set up the OpenVPN client:



Description:

1) Enter a VPN rule name (current timestamp is the default).
2) Select the OpenVPN protocol (other protocols will be available soon).

3) Click **Download** to select the protocol mode and export the corresponding template .conf file for modification. (Skip this step if you use a pre-configured file)



Refer to Section 3.3.6.1 for the configuration instructions.

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

5) Set the authentication credentials, if necessary.

6) Select an application scenario.

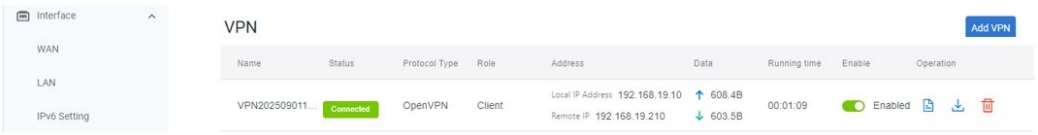
Refer to Section 3.3.6.4 for details on the application scenarios.

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

4. The newly created rule is enabled by default and shows an **Initializing** status during device configuration.

*If the status shows **Disconnected**, ensure your configuration is correct and there is no conflict with other rules, then recreate the rule if necessary.*

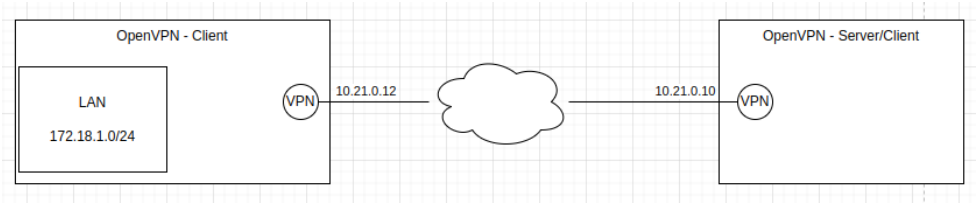
5. When the status changes to **Activated**, the device successfully establishes a connection with a server.



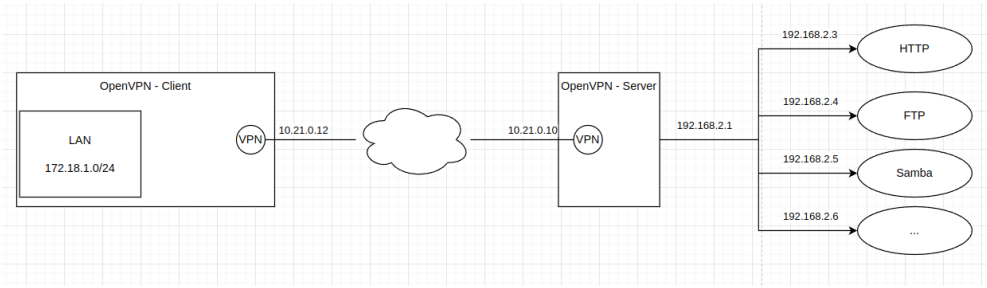
After setup, you can enable/disable the rule, view its logs (useful for troubleshooting if the rule fails to activate), download the configuration file, or delete it.

3.3.6.4 Application Scenario Topology

- General Use (point-to-point)

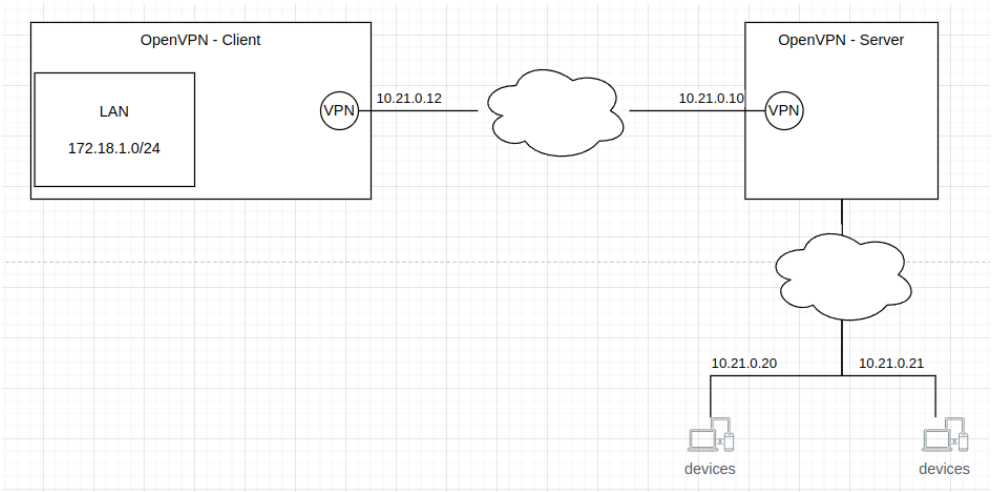


- Routing Mode (client-to-network)



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

- DNAT Port Forwarding (client-to-clients)

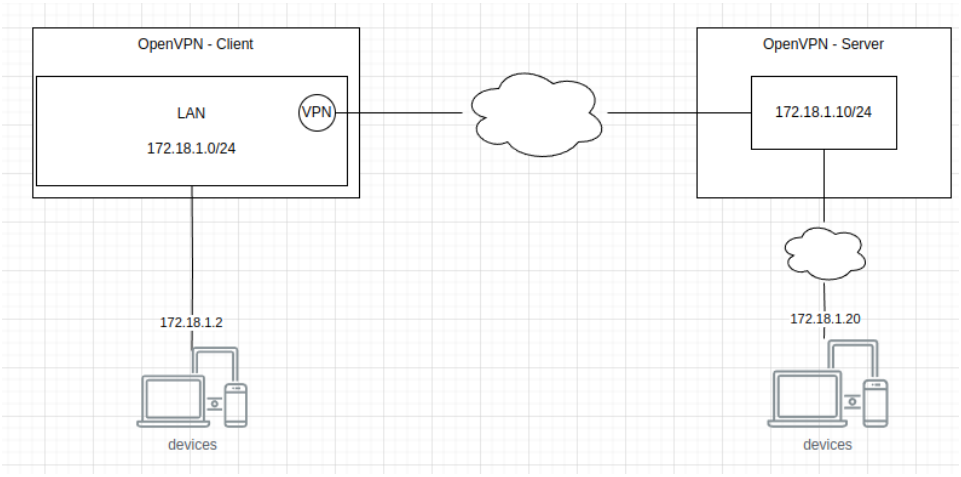


In this scenario, the OpenVPN client is assigned an IP: 10.21.0.12, on the same subnet as the remote devices (10.21.0.20 & 10.21.0.21). So, they can communicate with each other.

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

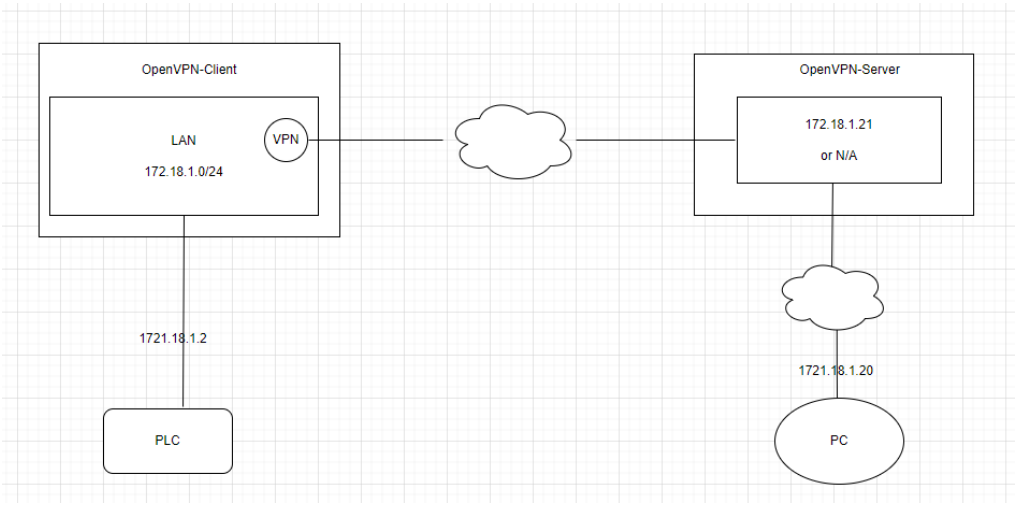
- Bridging Mode (clients-to-clients)

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.

3.3.7 Static Route

Static routing is a manual network configuration method that uses explicitly defined paths to direct traffic through specific interfaces. This provides precise control over routing behavior and is particularly useful for multi-WAN load balancing, traffic segregation, and backup link configuration.

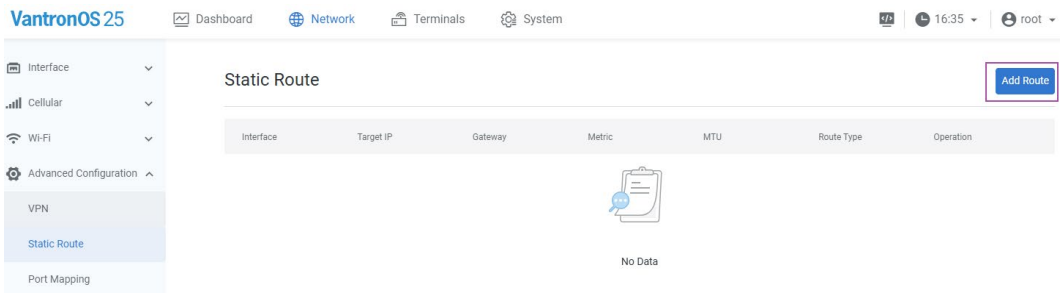
Example:

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

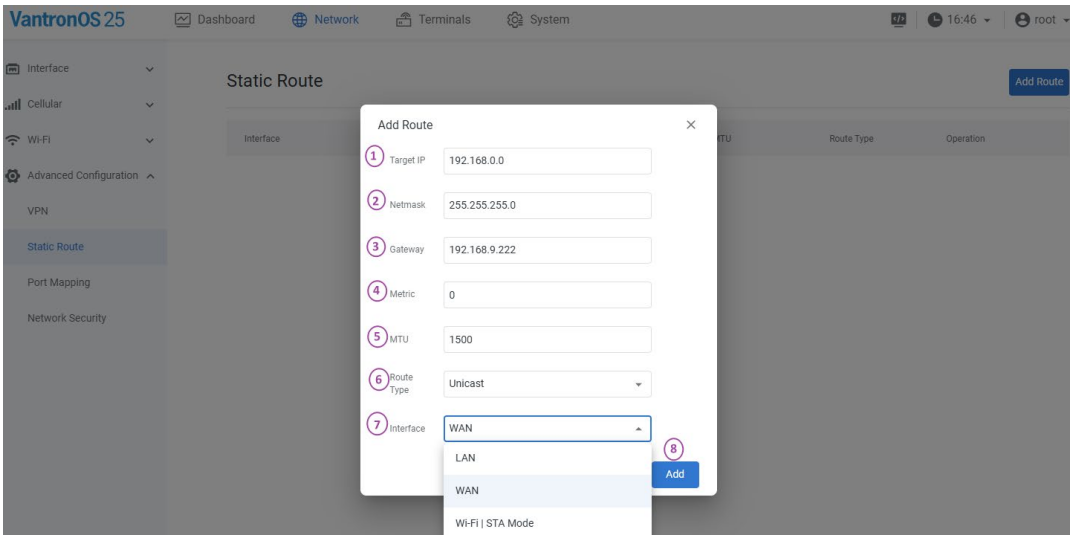
Goal: When the gateway has both 4G and WAN network connection, route the internal network (192.168.0.0 - 192.168.255.255) traffic through the Ethernet WAN interface, and all other data traffic via the 4G interface.

Steps:

1. Navigate to **Network > Advanced Configuration > Static Route**, and click **Add Route**.



2. Configure the routing rule.



Description:

1) Input the destination IP address.

2) Input the subnet mask (e.g., 255.255.255.0 = /24 = 192.168.0.0 - 192.168.0.255).

3) Input the address of the upstream router.

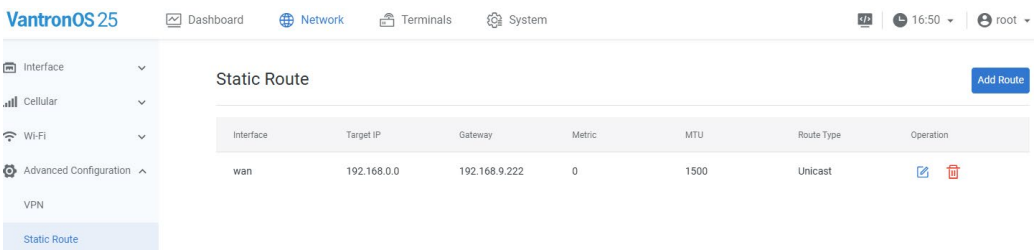
4) Gateway metric (**The smaller the number, the higher the priority**).

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.

3.3.8 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:

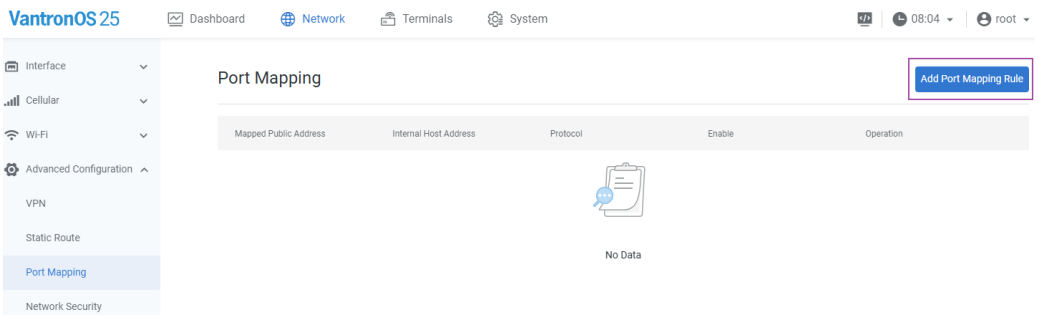
Scenario:

- The G405 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.

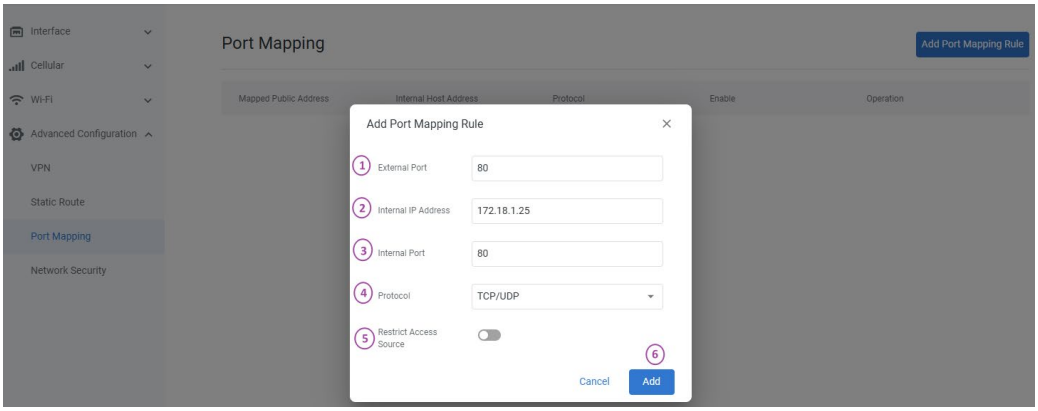
Goal:

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

1. Navigate to **Network > Advanced Configuration > Static Route**, and click **Add Port Mapping Rule**.



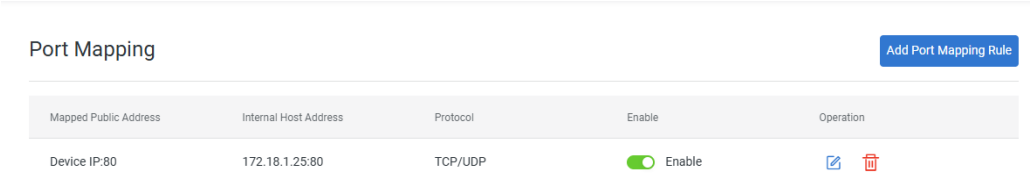
2. Fill in the rule information.



Description:

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 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.



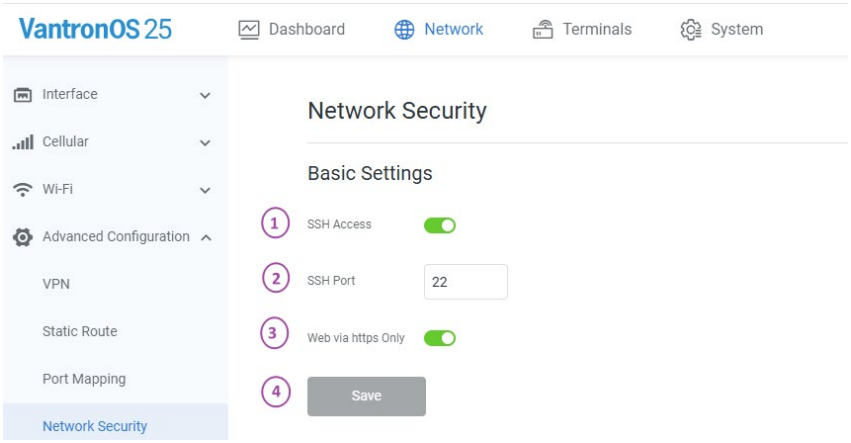
Note: *The mapped public address is determined by your WAN connection and may change.*

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.

3.3.9 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.

3.3.9.1 Basic SSH Access Setup



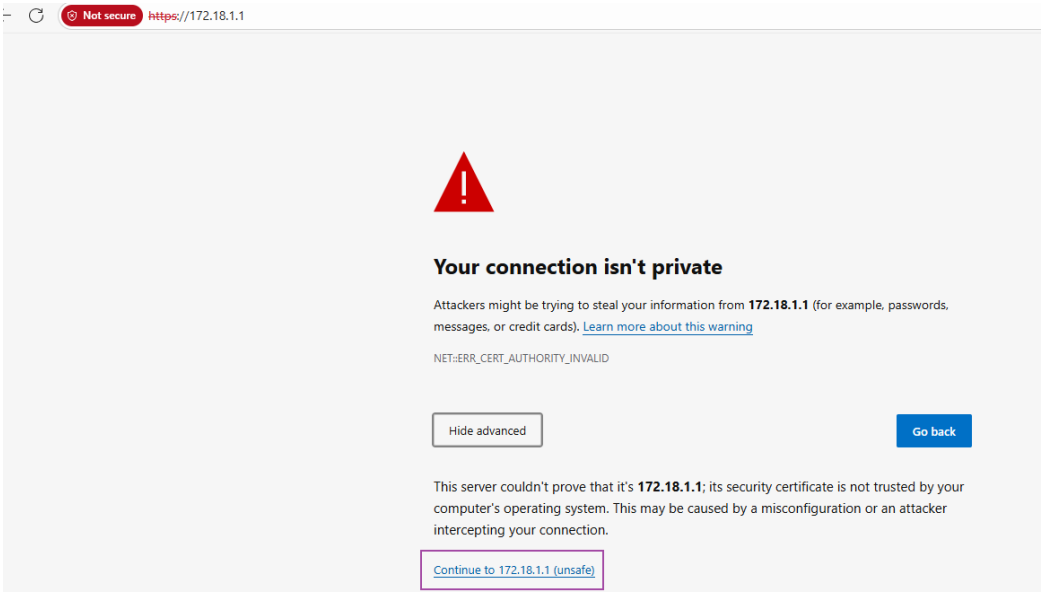
Description:

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

   Refer to 2.3 for the login method.

2. Default SSH port is 22.

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



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

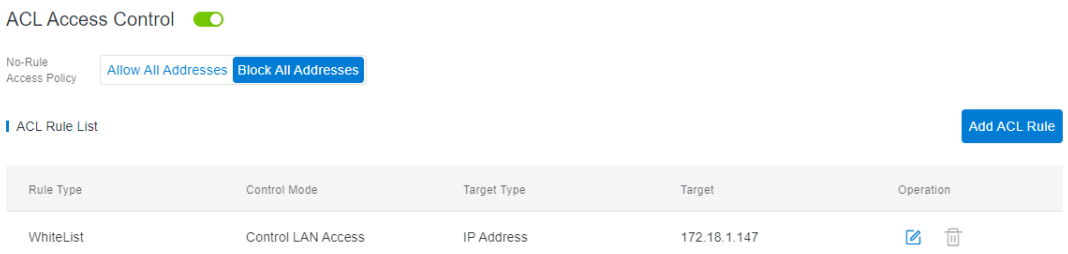
3.3.9.2 ACL Access Control

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.

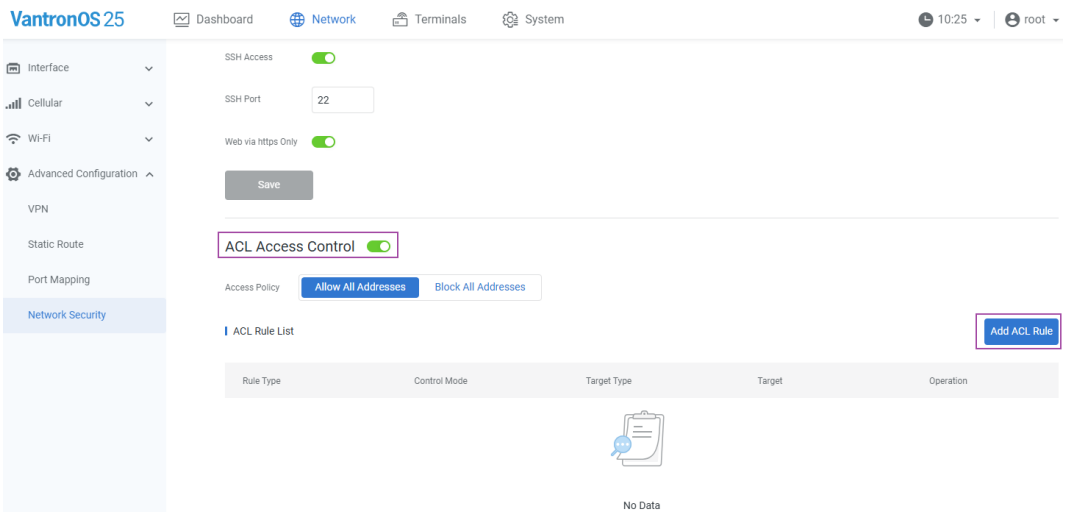
Block all addresses: When enabled, this policy **denies all WAN-side access** — only whitelisted IPs can reach the device — and **prevents** LAN-side devices from using it to **reach the WAN**. If no whitelist rules exist at activation, the device automatically adds the host PC's current IP to prevent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



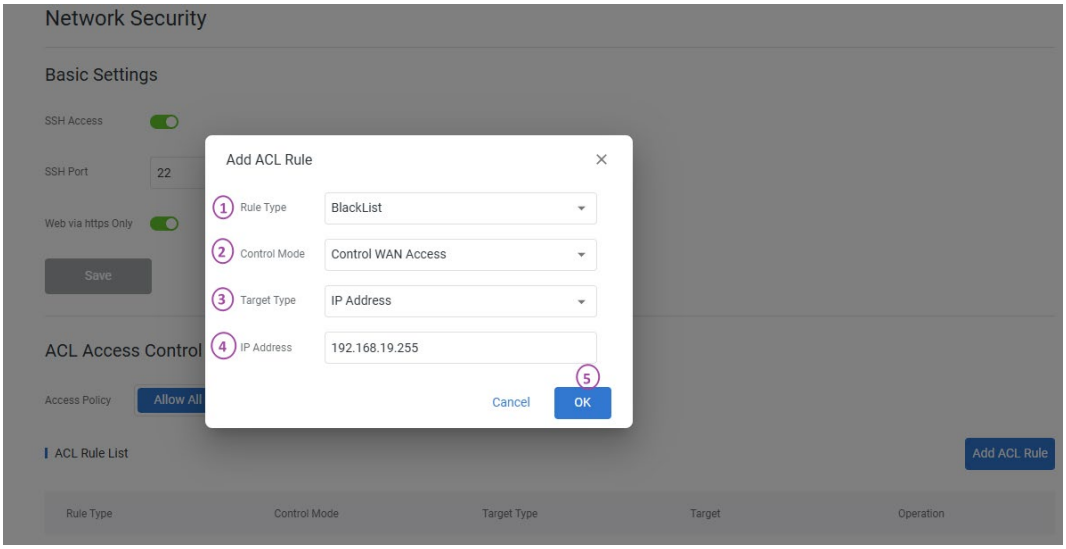
- **ACL Rule List**

To add an ACL rule:

1. Navigate to **Network > Network Security**, enable the **ACL Access Control** menu tab.
2. Click **Add ACL Rule**.



3. Configure the rule in the pop-up.



Description:

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 configuration.

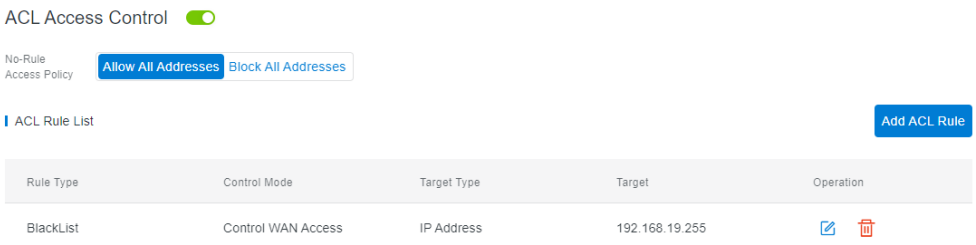
Description for the rule settings:

Rule Type	Control Mode	Target Type	Result
Whitelist	WAN	IP address (Source)	The designated WAN IP has access to G405 or its LAN devices.
		Destination IP/ URL/URL keyword	G405 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 G405 or its LAN devices.
		Destination IP/ URL/URL keyword	G405 or its LAN devices has no access to the designated WAN IP/URL/URL keyword.
	LAN	IP/MAC/OUI	The designated LAN devices are blocked from accessing the WAN domain.

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

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



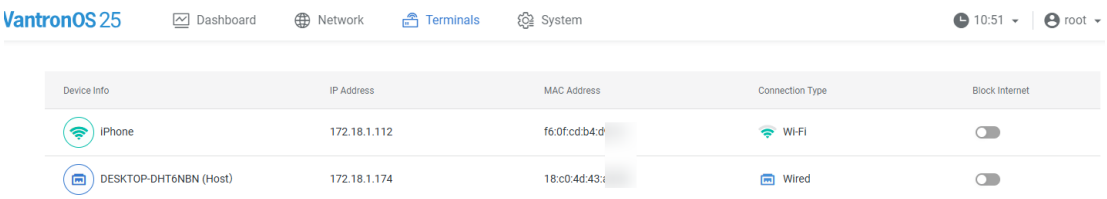
3.4 Terminals

The **Terminals** page displays the information of connected end nodes in the **LAN** domain, including the device name, IP address, MAC address, and connection type.

2.4GHz/5GHz Wi-Fi connections are classified to the **Wi-Fi** Connection Type. Ethernet connections are classified to the **Wired** Connection type.

Users can restrict internet access of these end nodes by enabling the **Block Internet** option.

DHCP reserved for a specified device using its MAC addresses is also displayed here, if connected. Refer to Section 3.3.2.2 for details on DHCP reservation.



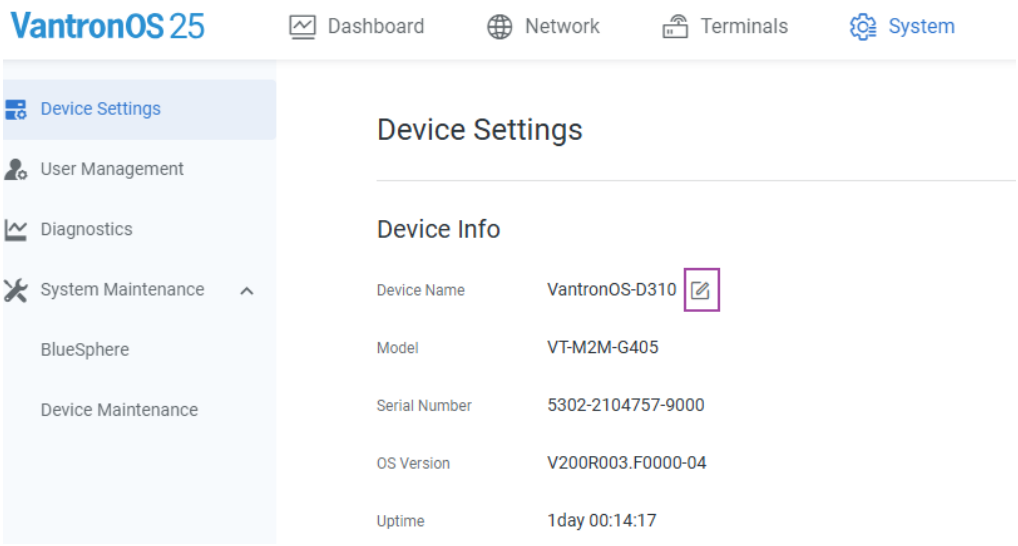
3.5 System

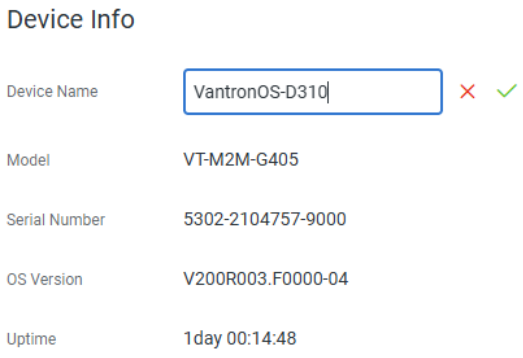
Under **System**, users can view and edit all system-level settings.

3.5.1 Device Settings

3.5.1.1 Modifying Device Name

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



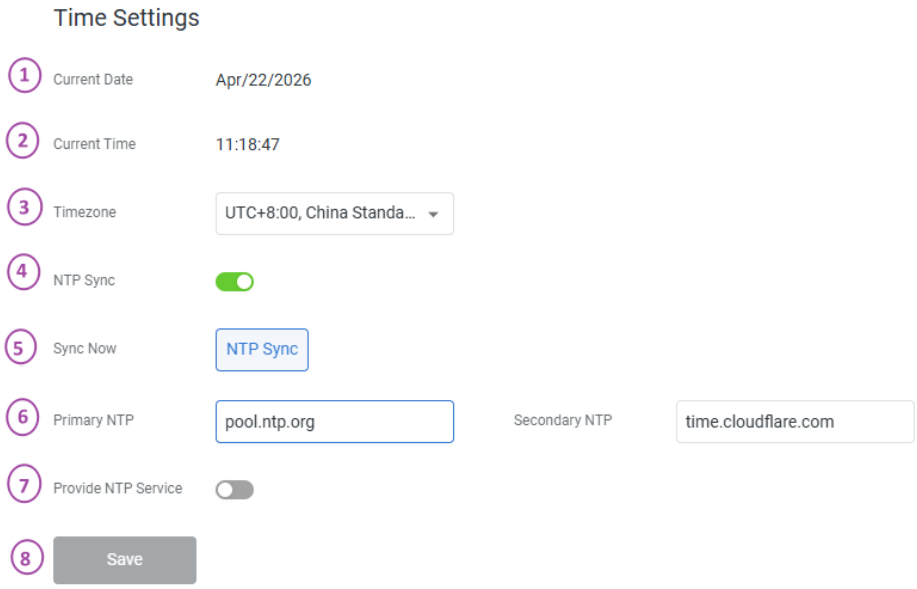


To modify the device name:

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

3.5.1.2 System Time

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

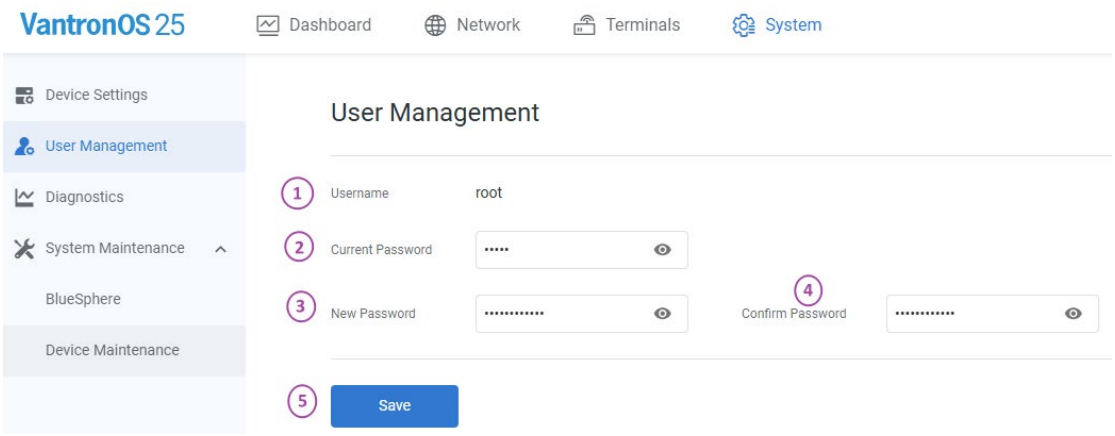


Description:

1. Current Date — Displays today's date for the selected time zone or the host PC's local time after time synchronization.
2. Current Time — Displays the current time.
3. Time Zone — Users can choose the desired time zone from the drop-down list.
4. NTP Sync — Toggles automatic time synchronization with NTP servers. The date resets after every power cycle because the G405 lacks an RTC.
5. Sync Now — Triggers a one-time NTP update immediately.
6. Primary NTP — Preferred NTP server. Secondary NTP—Backup NTP server.
7. Provide NTP Service — Enables/Disables the G405 to act as an NTP server for LAN devices.
8. If you have made any changes, click **Save** to apply.

3.5.2 User Management

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



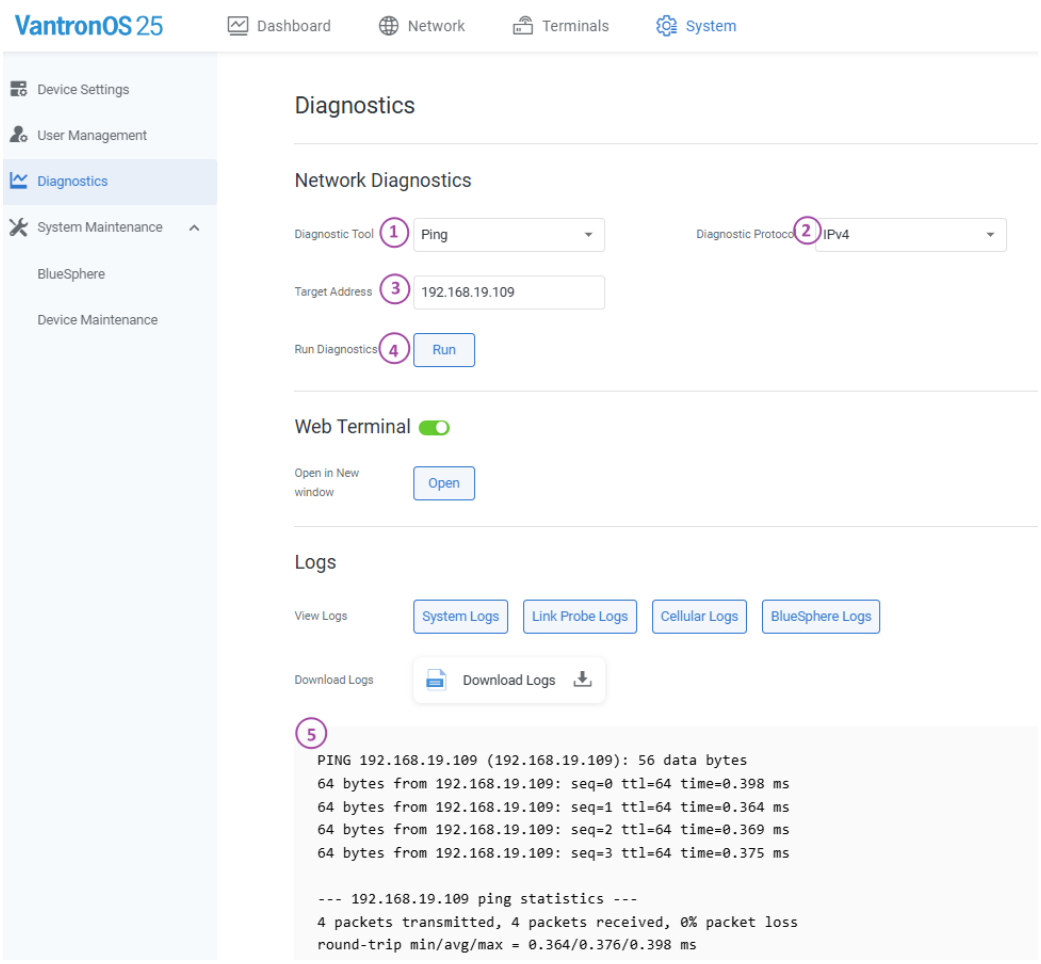
Steps to reset the login password:

1. Username displays the current account you are logged in with.
2. Enter the current password.
3. Enter a new password.
4. Confirm the new password.
5. Save the changes.

3.5.3 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.

3.5.3.1 Network Diagnostics

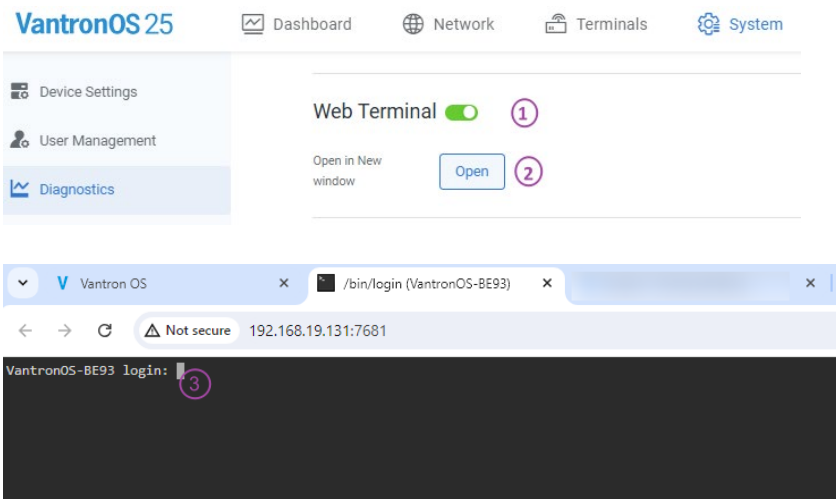


Description:

1. Select a diagnostic tool from the drop-down list.
2. For the Ping and Traceroute tools, select either IPv4 or IPv6 as the protocol.
3. Enter the target address (IP/Domain address).
4. Run the test.
5. The test results are displayed accordingly.

3.5.3.2 Web Terminal

Enabling the **Web Terminal** allows users to access the device's shell.



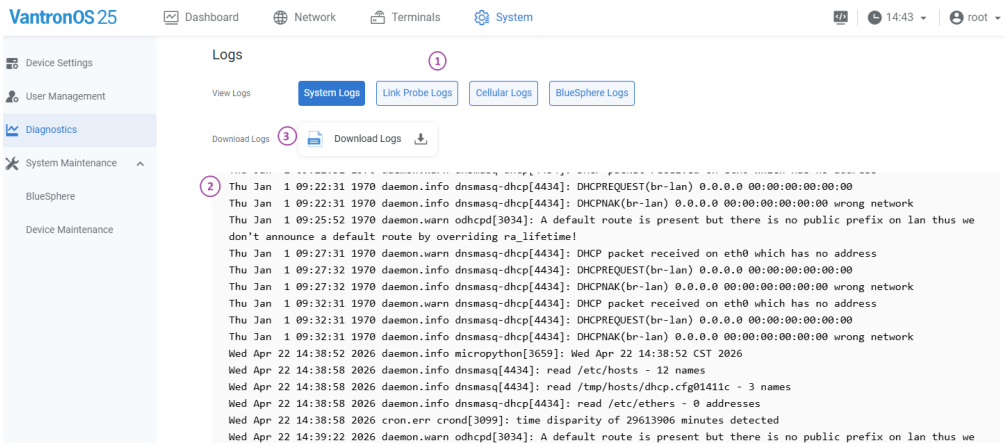
Description:

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

Use the credentials provided on the device label for web terminal login.

3.5.3.3 Logs

The system offers different device logs for maintenance or troubleshooting.



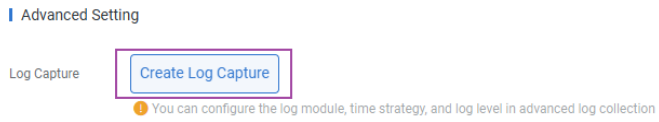
Description:

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.

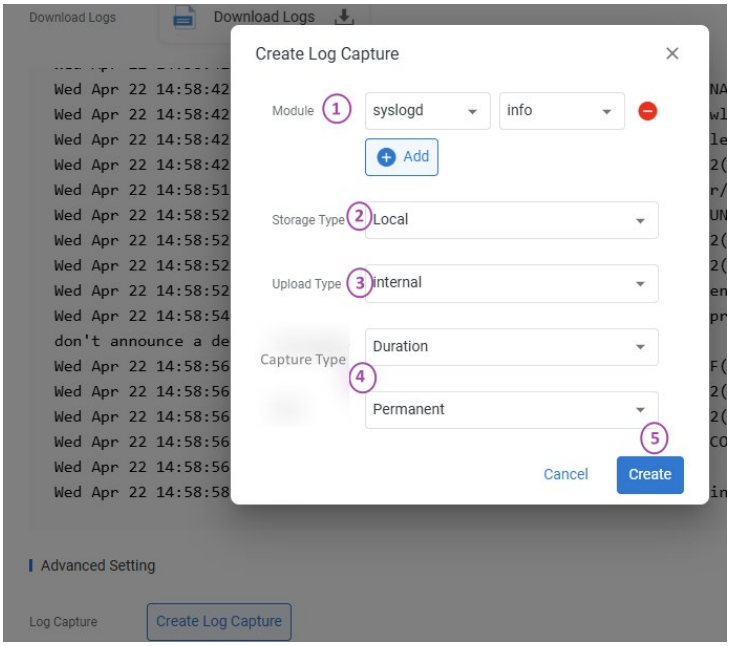
3.5.3.4 Log Capture

In the **Advanced Settings** section, you can create a log capture rule to define how the log is captured.

1. Navigate to **System > Diagnostics > Advanced Setting**.
2. Delete the existing rule, if any.
3. Click **Create Log Capture**.



4. Configure the rule.



1) **Module:** Select one or more modules for log generation.
2) **Storage Type:** Specifies where the logs are saved.
3) **Upload type**
   - Internal: Logs are saved to the device's **/tmp/log** directory and can be accessed using the `cd` and `cat` commands in the terminal console (**valid until the next device reboot**).

```
root@VantronOS-C7D8:/# cd /tmp/log
root@VantronOS-C7D8:/tmp/log# ls
able-startup.log                        restapi.log
cellulard.log                           vt_udmp_agent.log
health.checking.log                     vtapp_cmd_result
hotplug.log                             vtapp_config_reset.log
lastlog                                 vtled.log
openvpn-VPN20260422094839.log           vtled.log.1
openvpn-VPN20260422094839.status.log    wtmp
root@VantronOS-C7D8:/tmp/log# cat health.checking.log
   130.704 - info   - health checking started---
   130.794 - info   - add check target for platform VT-M2M-G202
   130.800 - notice - add check target -  60 → service status
   130.801 - notice - add check target - 600 → vtos agent
   130.805 - notice - add check target - 300 → time sync
   130.813 - notice - add check target - 120 → Disk Writable Testing
   130.816 - notice - add check target - 120 → hardware status
   130.818 - notice - add check target - 300 → refresh ARP table
   130.824 - notice - add check target - 120 → IP Address Conflict Detection
   130.827 - notice - add check target - 300 → Local IP Address Conflict Detection
   130.834 - notice - add check target - 300 → Gateway IP Address Conflict Detection
   130.841 - notice - add check target - 300 → Network Address Conflict Detection
```

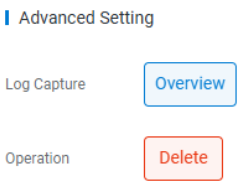
- SD card: Logs are exported to the **/log** directory on the SD card (ensure a valid SD card is inserted).

4) **Capture Type**

- Duration: The logs are captured as scheduled.
- Permanent: The logs are captured continuously without interruption.

5) Click **Create** to complete the rule setting.

5. After the rule is created, you can view its information or delete it as needed.



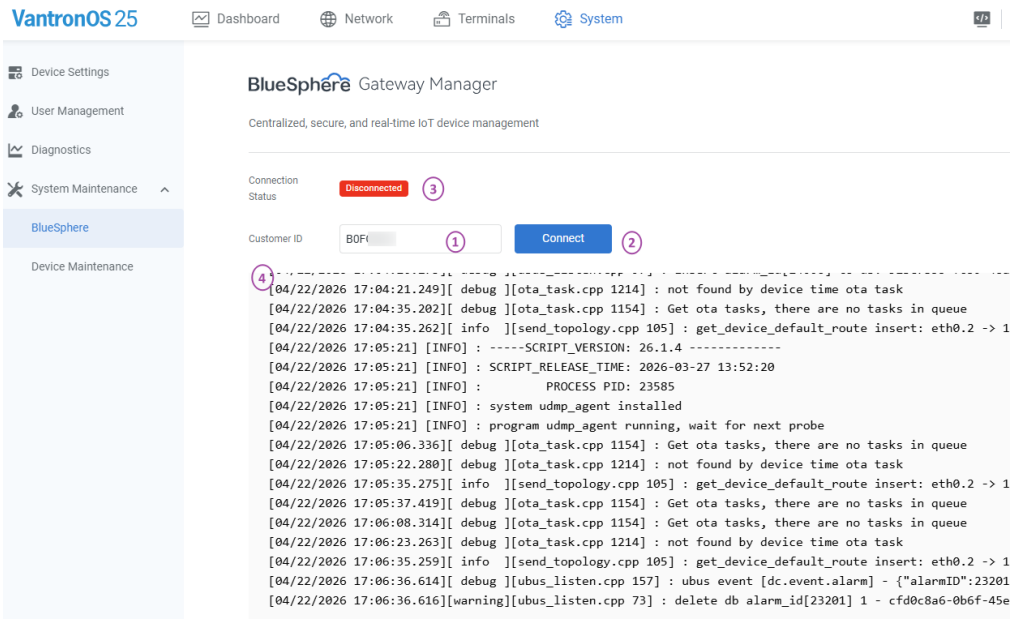
3.5.4 System Maintenance

3.5.4.1 BlueSphere

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

Prerequisite:

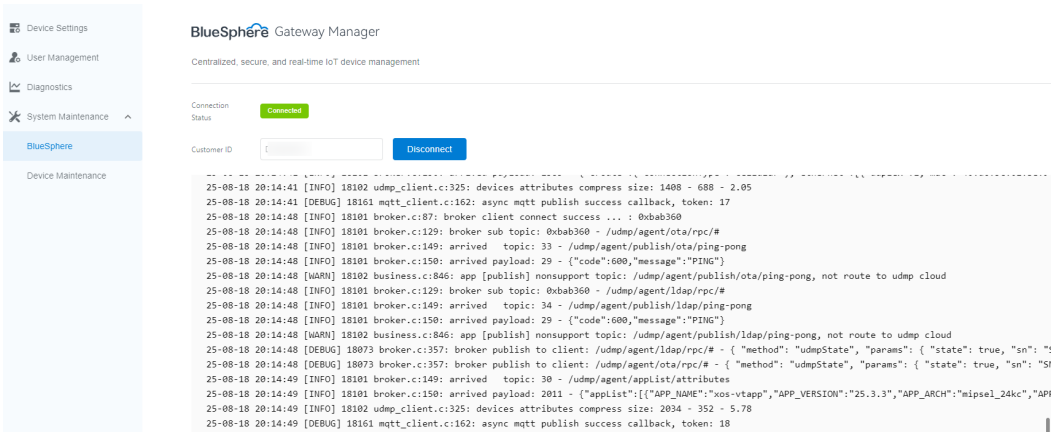
The G405 must have internet access.



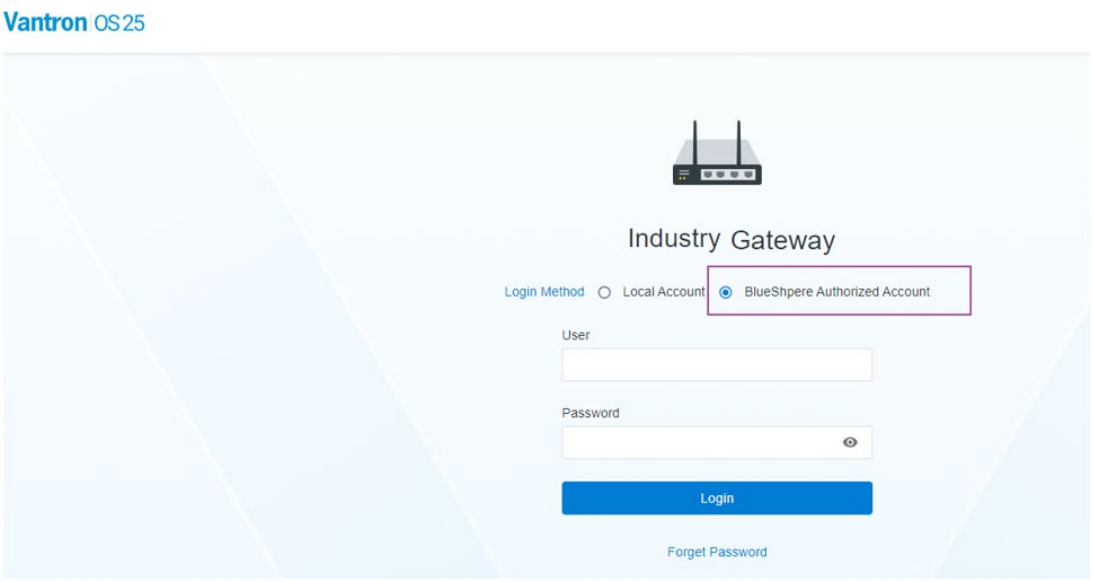
Description:

1. Enter the customer ID that is retrievable in the user profile on the GWM portal.
2. Click **Connect** to establish a connection 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.



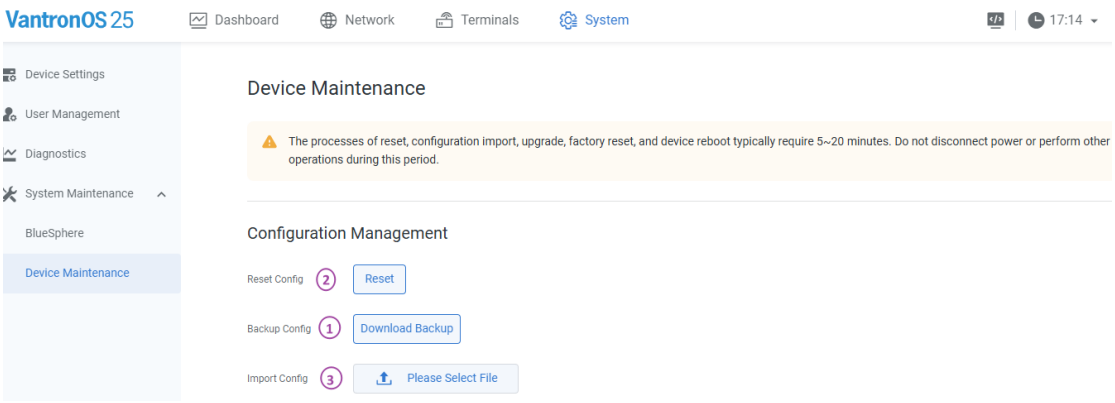
If you log out the portal now, you will find two login methods available. You can sign back in with either your local credentials or an authorized GWM account.



3.5.4.2 Device Maintenance

As indicated on the top of the web, 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

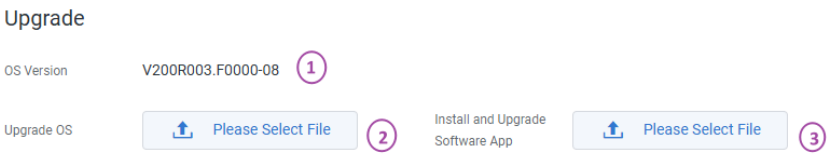


Description:

1. Download the current device configuration for backup purposes as needed.
2. Reset the device configuration (this action clears user-defined settings).
3. After resetting the device, import a configuration file if necessary. Only configuration files compatible with the same device model are supported.

Once the device configuration is cleared, you can re-log in to the device using the credentials provided on the device label and follow the setup wizard to finish the first-time configuration.

- Upgrade

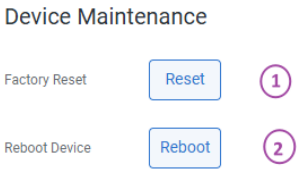


Description:

1. Current firmware version.
2. Select a system image from a local directory to upgrade the operating system.
3. Install new apps or upgrade existing ones from a local directory.

VantronOS 25 consists of the operating system and the VantronOS 25 app, which can be upgraded separately by following step 2 or 3 above. Upgrades are allowed only from an older to a higher version.

- Device Maintenance



Description

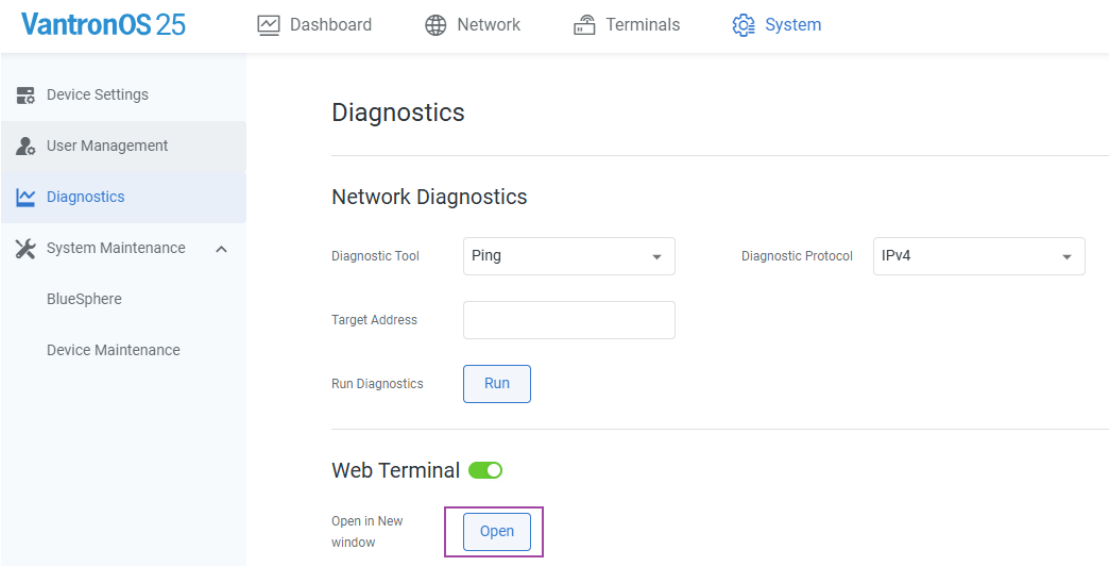
1. Factory reset the device with device configuration, user data and custom applications (including the VantronOS 25 app) cleared.
2. Manually restart the device.

*If needed, back up the existing configuration before factory reset by clicking the **Download Backup** button under **Configuration Management**.*

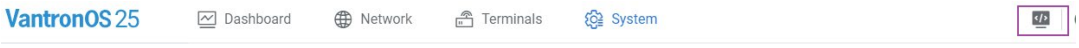
3.6 Command Line Interface

You can open the device's command line interface using either of the following methods:

- Click **Open** web terminal on the **System > Diagnostics** page, as described in Section 3.5.3.2.

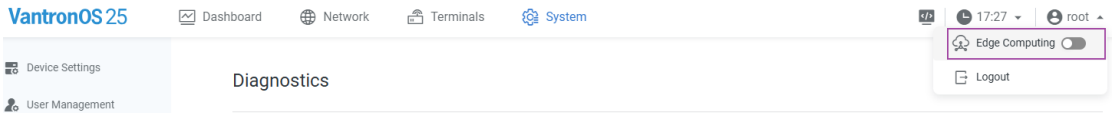


- Click the CLI icon on the menu tab.



3.7 Edge Computing

The **Edge Computing** menu is hidden in the user account drop-down list. You can manually enable this feature to make it visible. Once enabled, it will show on the menu tab.



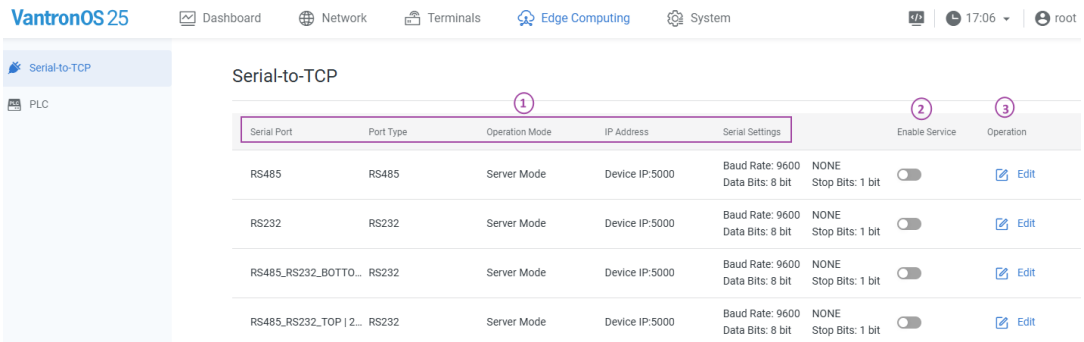
3.7.1 Serial to TCP

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.

Pre-configured conversion rules for existing serial ports are 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:

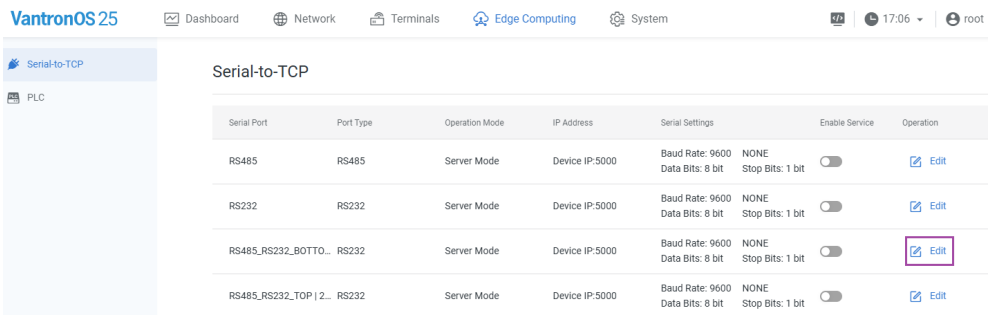
1. Details of the conversion rule, including the serial port name and type, current operation mode, device's IP address and listening port for data access, and serial parameters.

   *Serial port names correspond to the silk screens on the device enclosure. The RS-232/RS-485 multiplexers default to the RS-232 mode and can be modified via the **Edit** menu.*

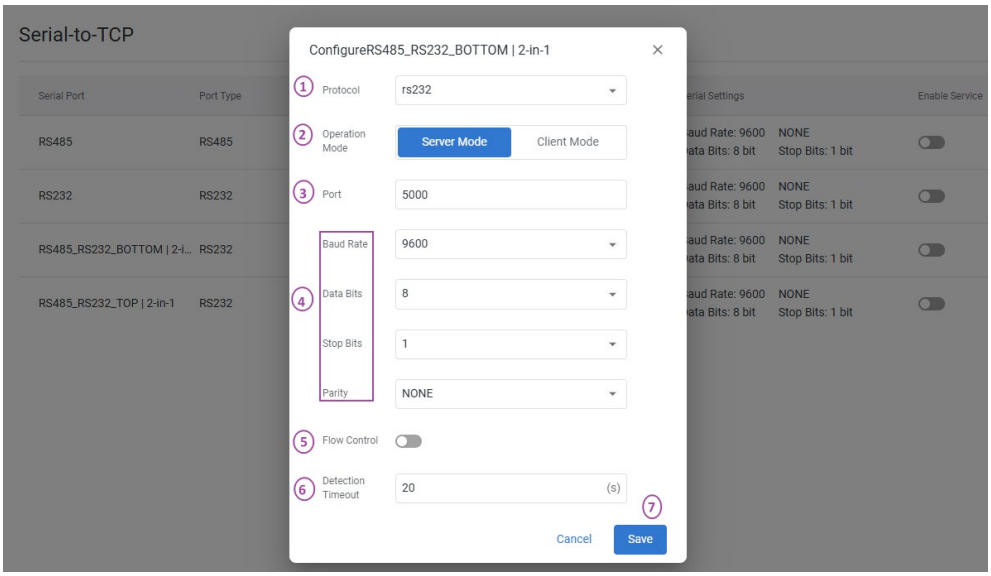
2. Enable/disable the rule.
3. Edit the rule.

3.7.1.1 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.

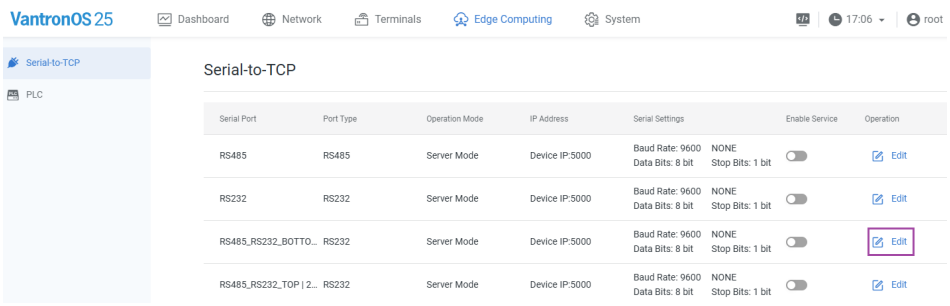


1) Select a serial mode for the multiplexer.
2) Select **Server Mode.**
3) Designate a TCP port (0~65535) for the server to listen on. The client must connect to the same port.
4) Make sure the serial parameters on both the peripheral and gateway are set the same.
5) Enable/Disable software flow control to prevent packet loss (this may reduce 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.

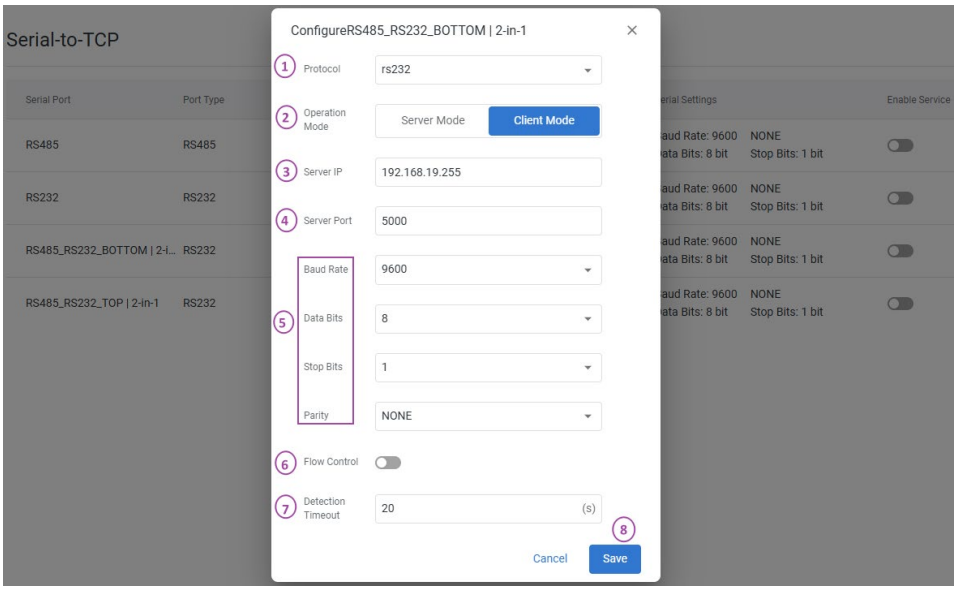
3. Enable the conversion rule.
4. Make sure both the client and server are on the same reachable IP network.
5. Verify the data transmission between the devices.

3.7.1.2 Client Mode Rule Setup

1. Select a rule, and click the **Edit** icon.



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



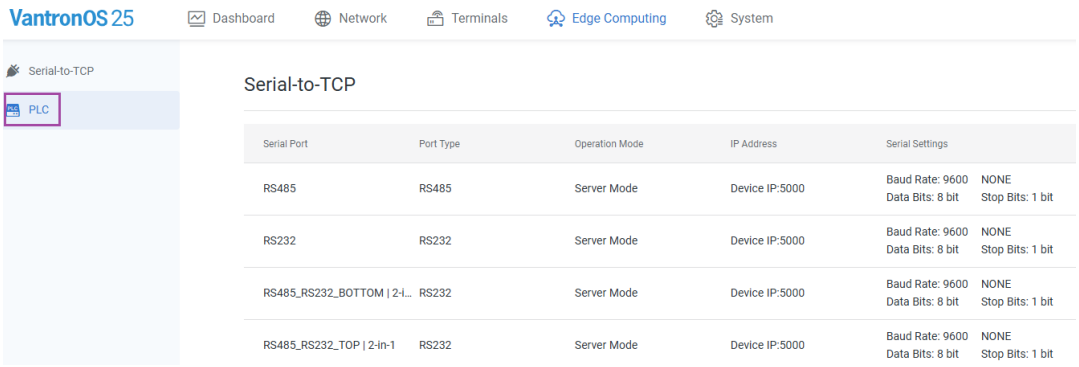
1) Select a serial mode for the multiplexer.
2) Select **Client Mode.**
3) Enter the server's IP address.
4) Enter the target port and make sure it matches the TCP port on the server.
5) Make sure the serial parameters on both the peripheral and gateway are set the same.
6) Enable/Disable software flow control to prevent packet loss (this may reduce 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.

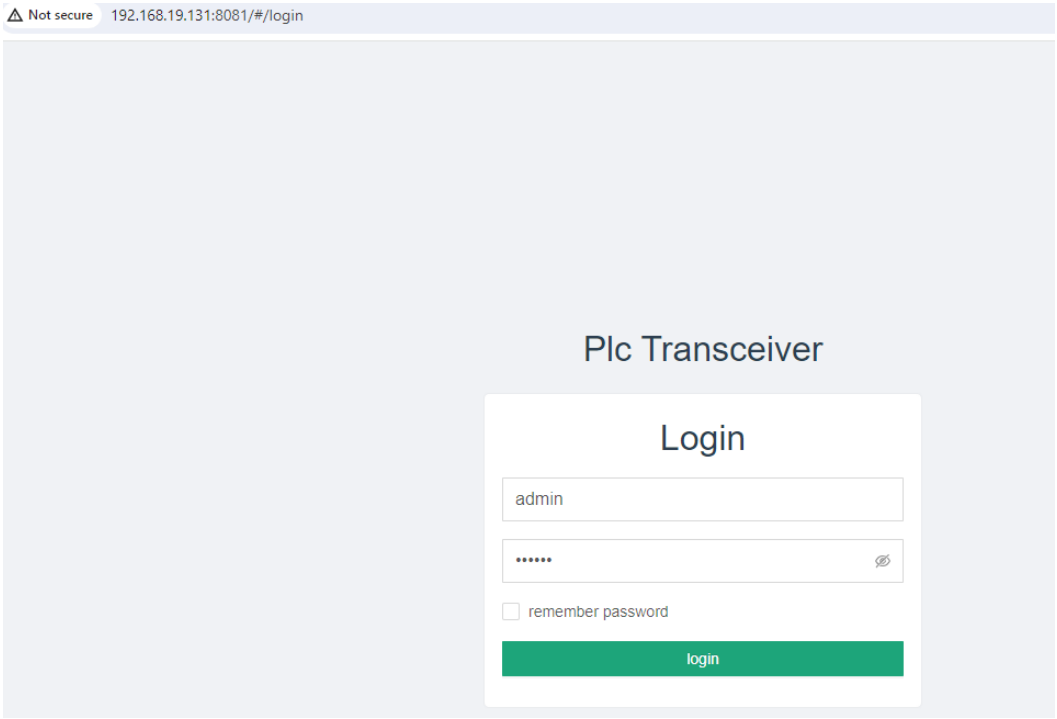
3.7.2 PLC

The G405 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.

The **Edge Computing** tab includes a dedicated **PLC** menu, enabling users to configure edge computing parameters for data processing.



Clicking **PLC** launches the industrial protocol configuration portal, where users can fine-tune all gateway- and PLC-specific parameters (e.g., protocol type, station address, register address, data mapping, polling intervals) required for seamless fieldbus integration.



Refer to Chapter 4 for the detailed information.

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 I/O Configuration

The G405 provides 4 digital input (DI) channels, 2 analog input (AI) channels (one for current and one for voltage measurement), and 2 digital output (DO) channels for edge data transfer.

4.2.1 DO Configuration

Refer to Sections 1.7 and 1.8.3 for the interface parameters and wiring instructions, respectively.

The DO channels are dry contact relay outputs. You can set the channels to normally open (NO) or normally closed (NC) status using the following commands in the device shell.

1. Refer to Section 2.3 to log in to the device.
2. Click the **CLI** icon to access the device shell.

3. Set the DO channel state:
   - Set to NC: `# gpio set do1 off`
   - Set to No: `# gpio set do1 on`

   do1 = DO channel 1, do2 = DO channel 2.

4.2.2 DI Configuration

Refer to Sections 1.7 and 1.8.4 for the interface parameters and wiring instructions, respectively.

You can switch the DI channels to dry/wet contact mode and verify the input status using the following commands in the device shell.

1. Refer to Section 2.3 to log in to the device.
2. Click the **CLI** icon to access the device shell.

3. Run the following command to switch the **DI 1** channel (wet_dry_nodes_group**1**) to:
   - Dry-contact mode: `# gpio set wet_dry_nodes_group1 dry`
   - Wet-contact mode: `# gpio set wet_dry_nodes_group1 wet`
4. Confirm that the mode has been successfully changed by reading the status:

```
# gpio get wet_dry_nodes_group1 status          // value "1" indicates successful setup
```

5. Use the `gpioget` command to read the real-time input level of the **DI 1** channel:

```
# gpioget gpiochip0 8
```

*When DI1+ and DI1- are **disconnected**, the command returns **1** (high level).*

*When DI1+ and DI1- are **shorted**, the command returns **0** (low level).*

6. For other DI channels, the mode switch commands are identical, only the **group number** varies by channel. Use the following commands to read input levels:

```
# gpioget gpiochip0 6          // DI 2
# gpioget gpiochip0 4          // DI 3
# gpioget gpiochip0 0          // DI 4
```

4.2.3 AI Configuration

AI Channels 1 and 2 are designed for external voltage input and current input, respectively.

Refer to Sections 1.7 and 1.8.5 for the interface parameters and wiring instructions, respectively.

You can read the converted values using the following command in the device shell.

1. Refer to Section 2.3 to log in to the device.
2. Click the **CLI** icon to access the device shell.

3. Run the following command to read the output values:

```
~# read_adc <LSB_value> <reference_voltage>
```

- <LSB_value>: ADC step coefficient (0.00833 for this gateway, unit: mV/step)

- <reference_voltage>: ADC reference voltage (4.03 for this gateway, unit: V)

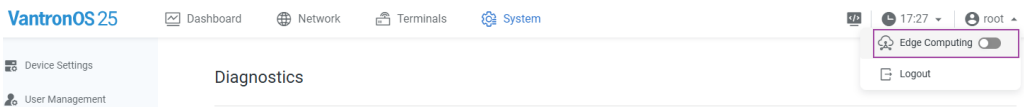
Example Usage:

```
~# read_adc 0.00833 4.03
Vout1 = 1364.625(mV)            // Voltage input (Channel 1)
Aout2 = 1368.375(mV)          // Converted voltage from current input (Channel 2)
```

For current measurement, use the external shunt resistor value to convert Ain1 to the actual current.

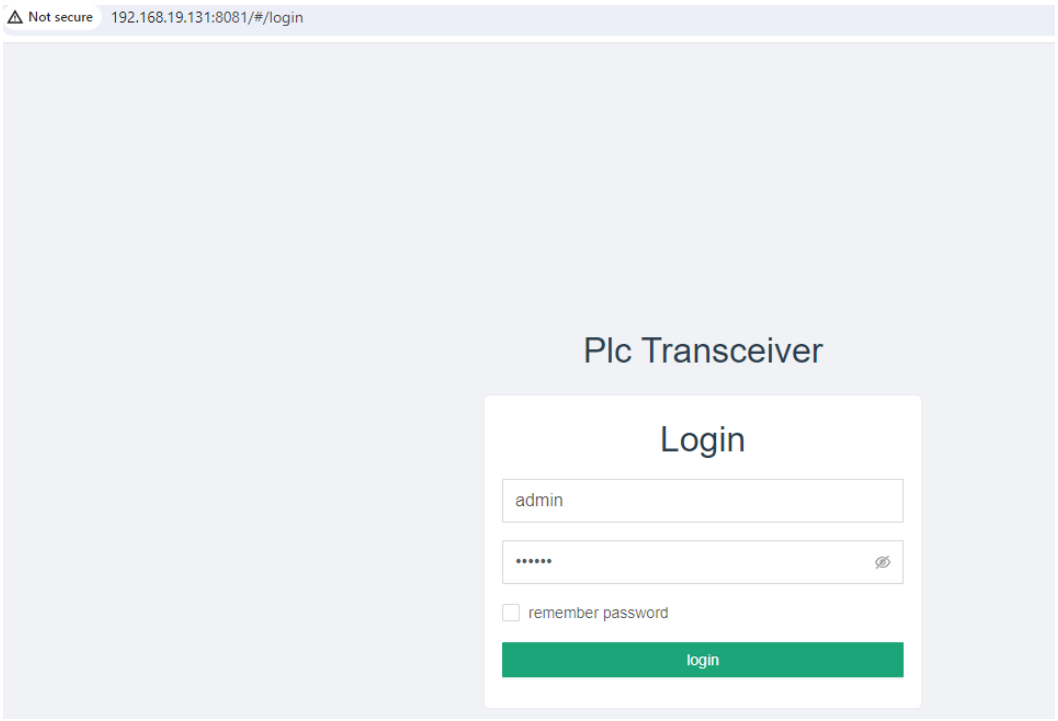
4.3 Portal Login

1. Enable the **Edge Computing** feature from the user account drop-down list.



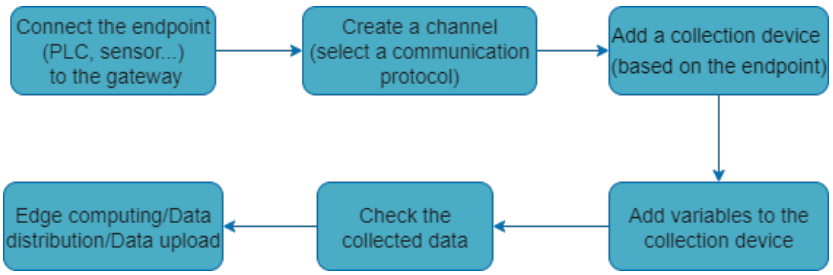
2. Navigate to **Edge Computing > PLC** in VantronOS.

3. Users will be redirected to a new window. Use your VantronOS credentials to log in.



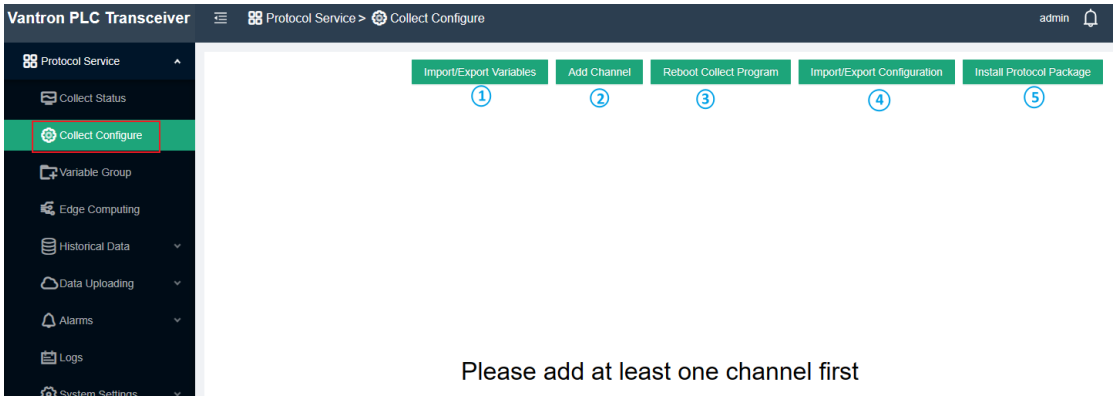
4.4 Protocol Configuration and Application

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:



4.4.1 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.



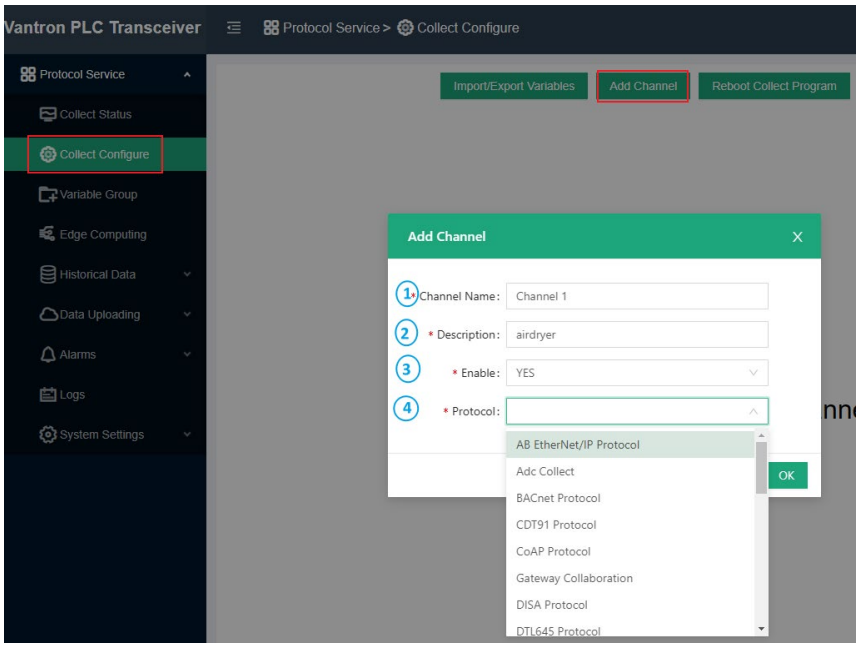
Description:

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.

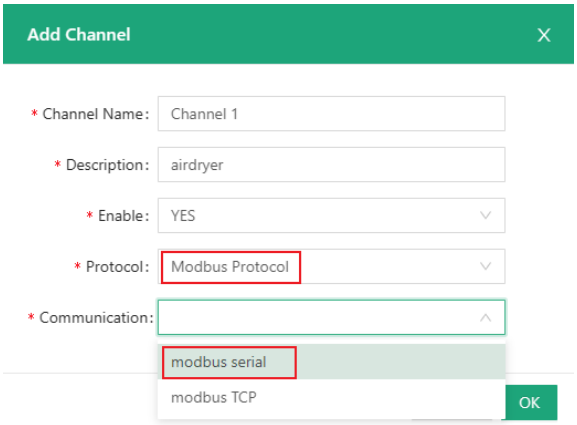


Description:

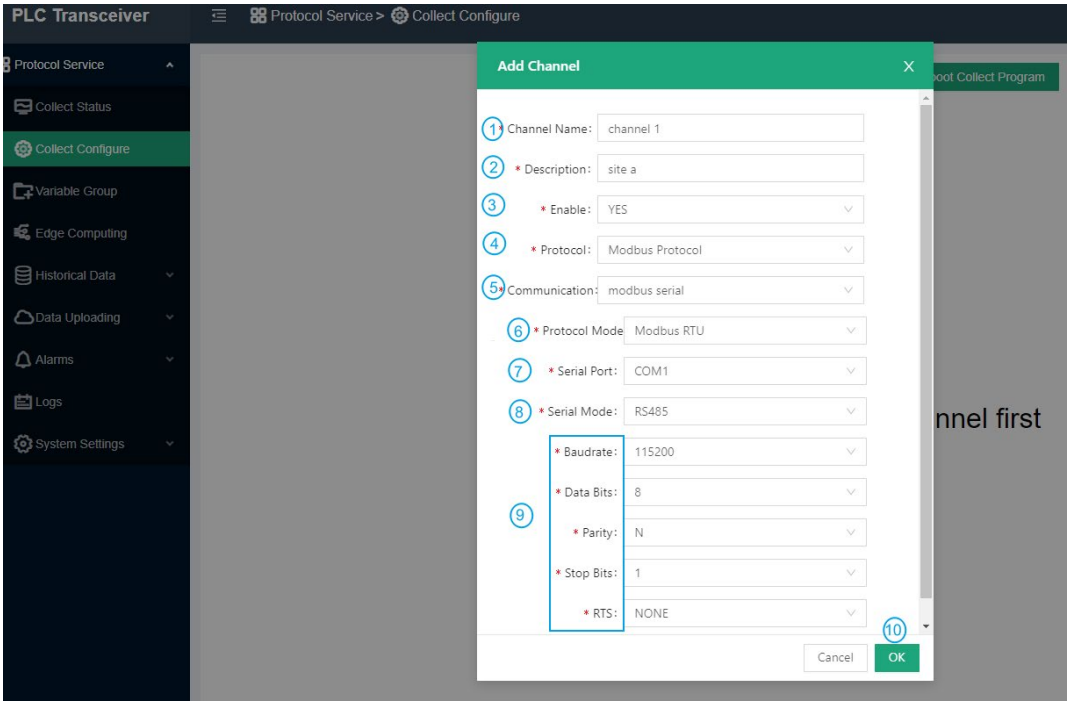
1. Enter a channel name that shall not be any one of the names in use.
2. Describe the channel.
3. To enable the channel or not (‘Yes’ by default).
4. Select a protocol type from the drop-down list based on the model of the endpoint (the available protocols are dependent on the installed package file).

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:

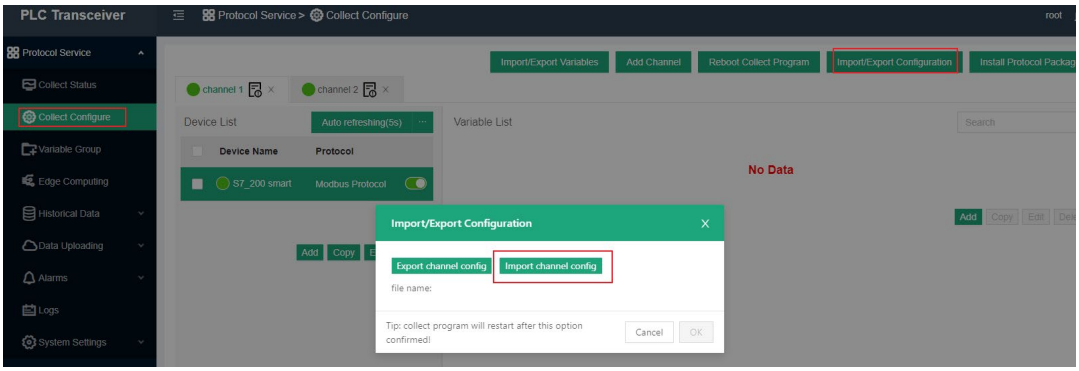


Description:

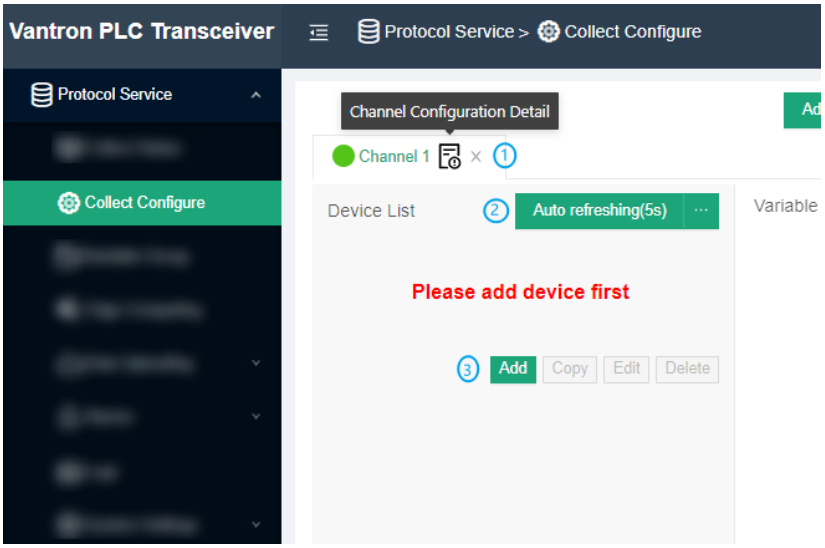
4. Select **Modbus protocol** from the drop-down list.
5. Choose **modbus serial** as the communication type.
6. Select **Modbus RTU/Modbus ASCII** as the protocol mode (Modbus RTU for illustration).
7. Select the correct serial port from the drop-down list that corresponds to the serial port in use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

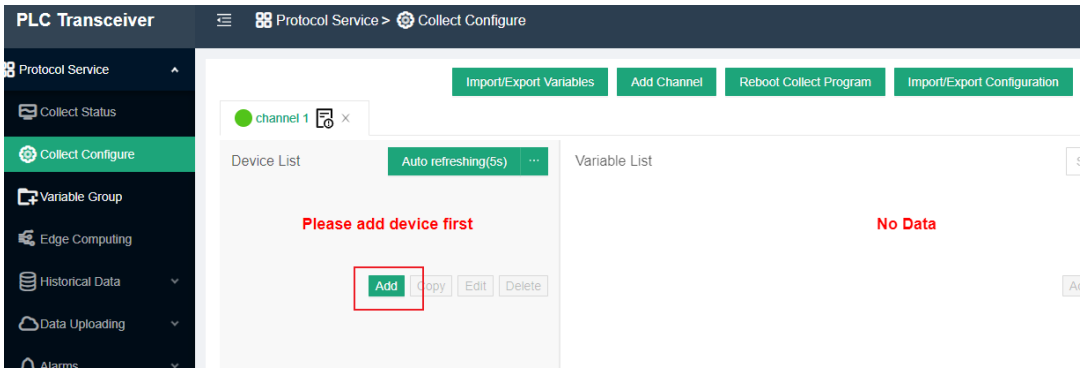


Description:

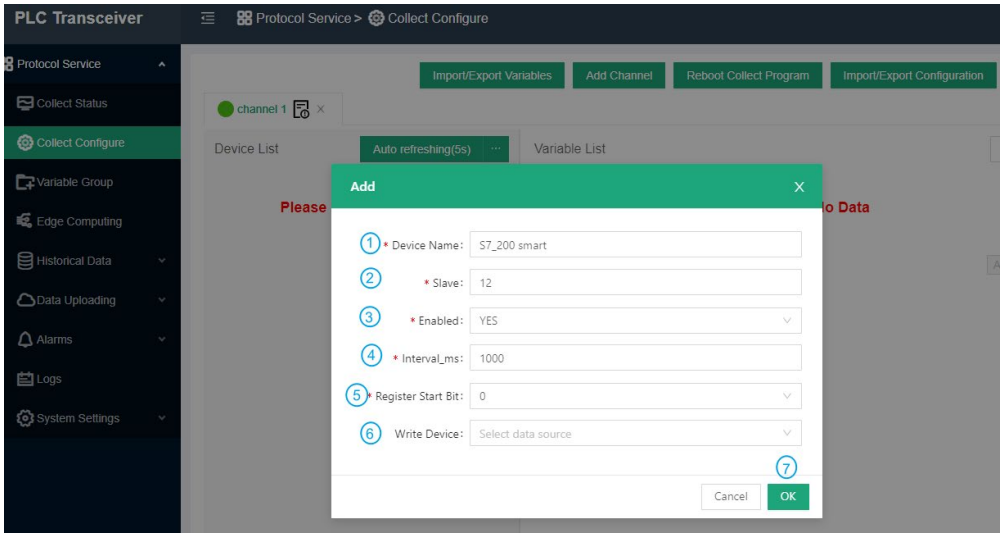
1. Delete the channel (x) or access the detail page ( ) of the channel and make changes accordingly, including disabling the channel.
2. The channel is set to refresh automatically every 5 seconds, and you can assign an optional value between 1 and 99 for auto refreshing by clicking the (…) button.
3.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

4.4.2 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:

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.

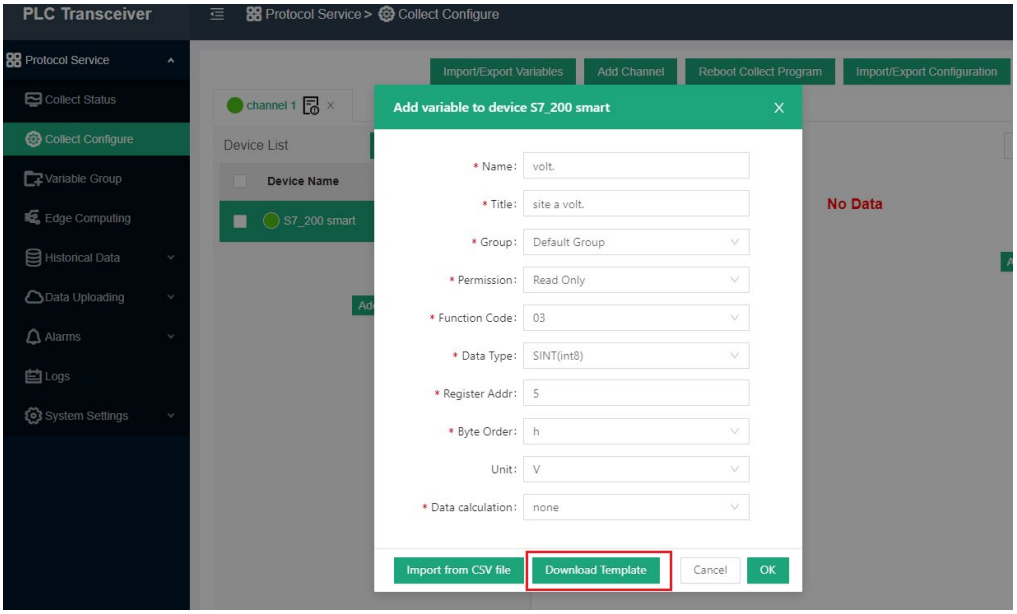
4.4.3 Variable Setup

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

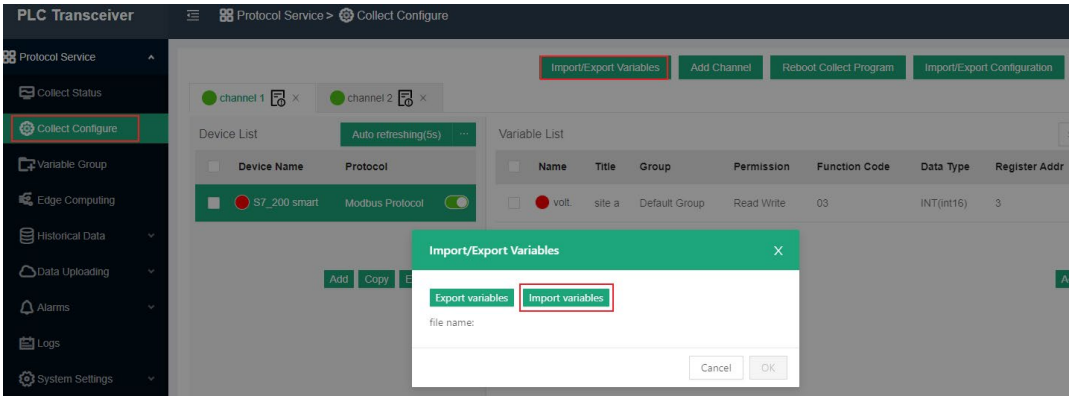
- **Batch Import**

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.

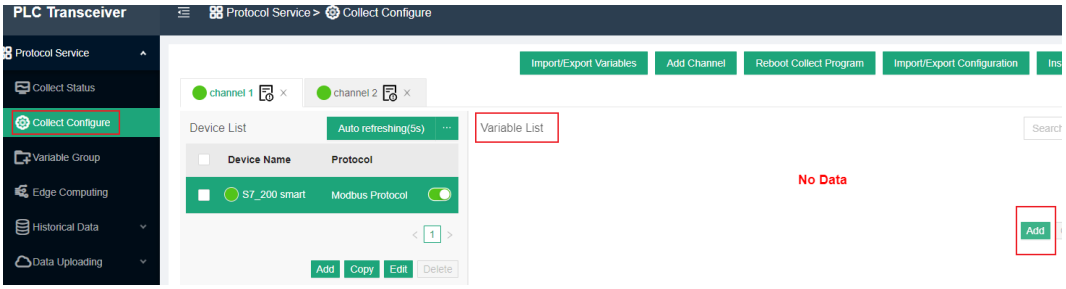


For non-first bulk import, you can directly click the **Import/Export Variables** tab under the **Collect Configure** menu, then select **Import variables**.

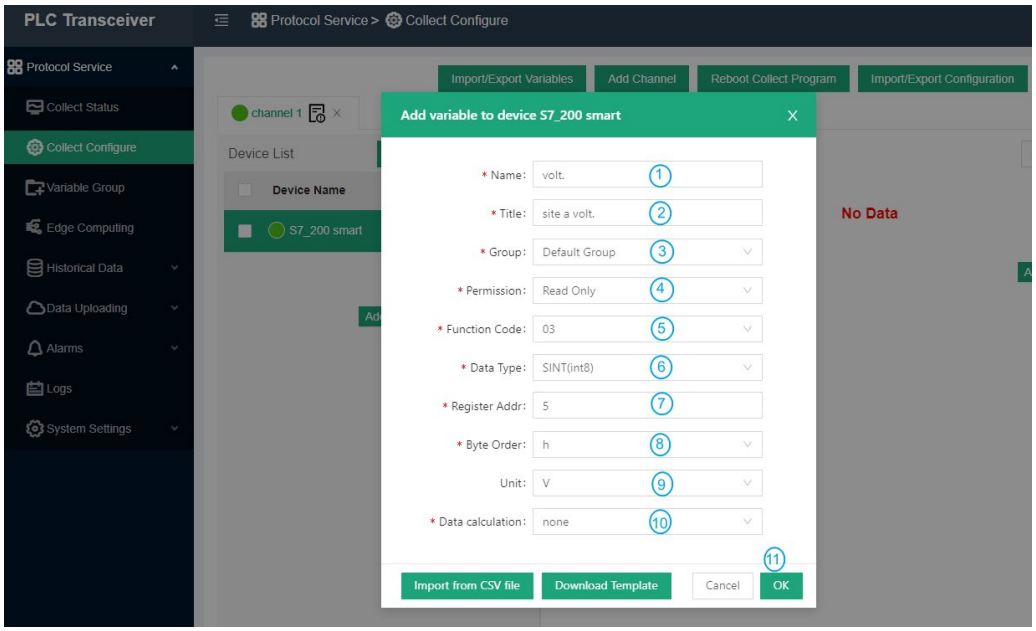


- **Individual Variable Configuration**

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.



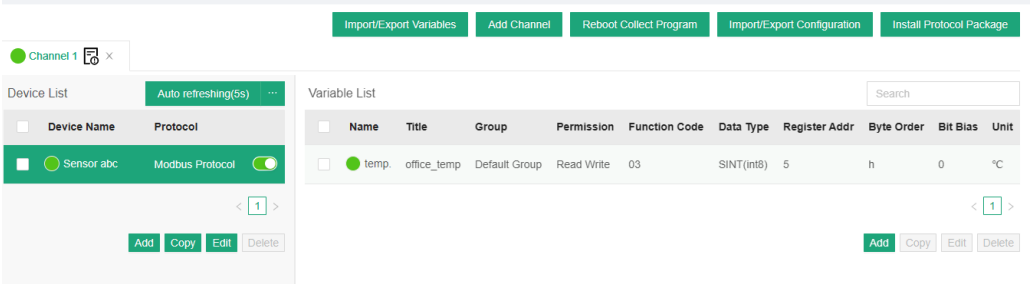
Description:

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).

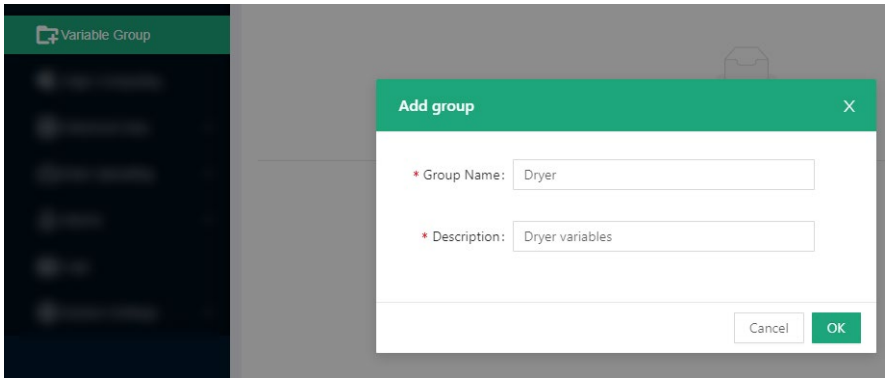
7. Input or adjust the register address from 1 to 65535.
8. Set the byte order.
9. Select a unit for the variable (determined by the collection device).
10. Set a method for data calculation.

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.

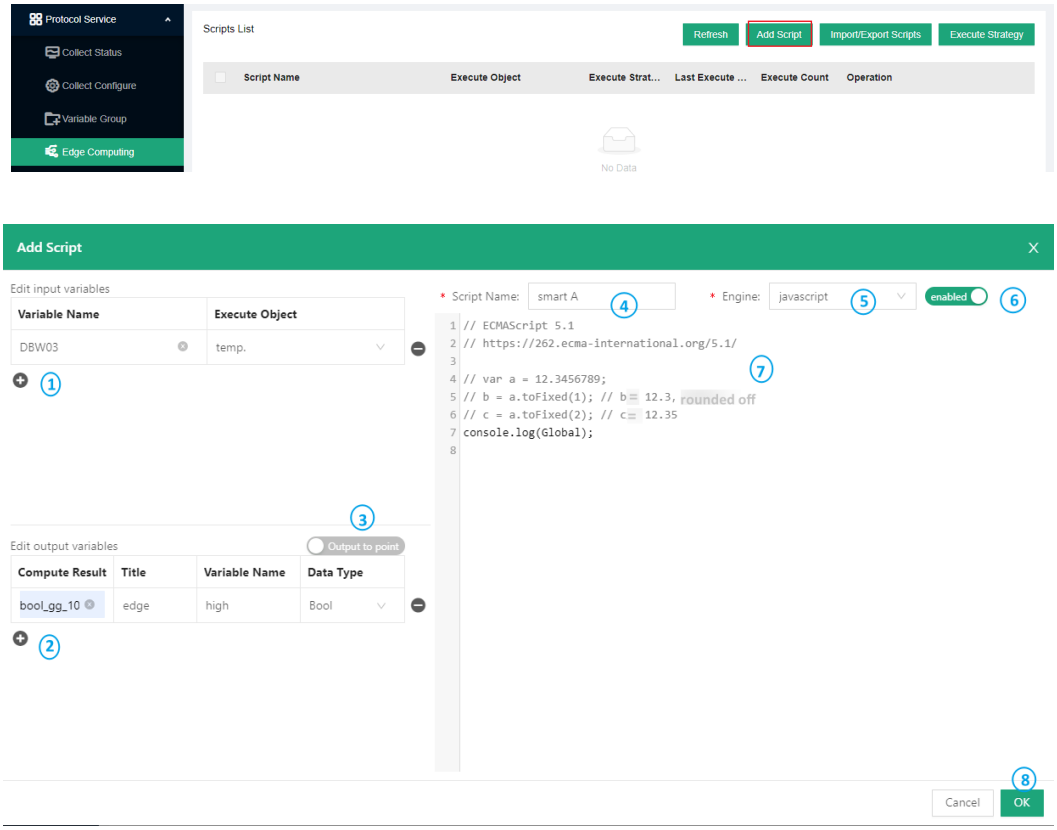


If multiple variables are involved, you can add variable groups for different variables from the **Variable Group** tab on the left menu pane.



4.5 Edge Computing Scripts Setup

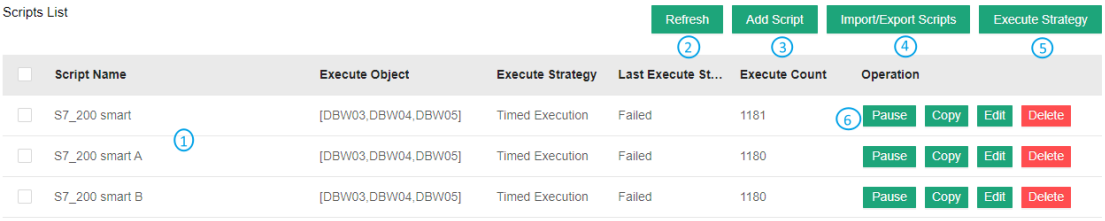
To add a script for edge computing, click **Edge Computing** from the navigation pane on the left, then click **Add Script** to input the script information in the pop-up.



Description:

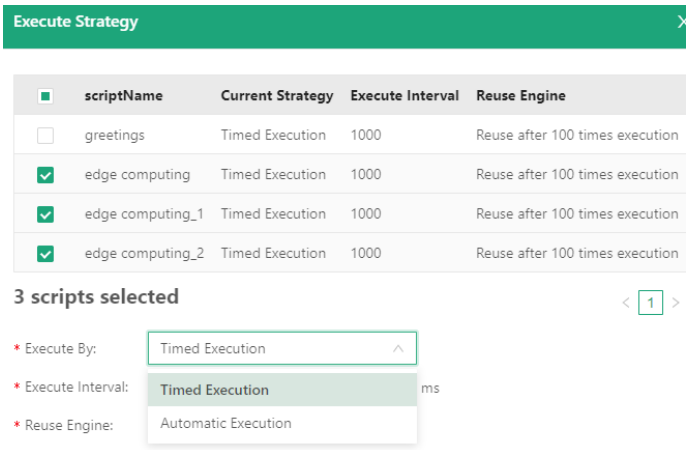
1. Edit input variables: add a name for the input variable and an object for executing the script (more than one variable could be added).
2. Edit output variable: add the computation result, title, variable name, and data type.
3. Toggle between outputting the results to the variables or edge nodes.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

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.

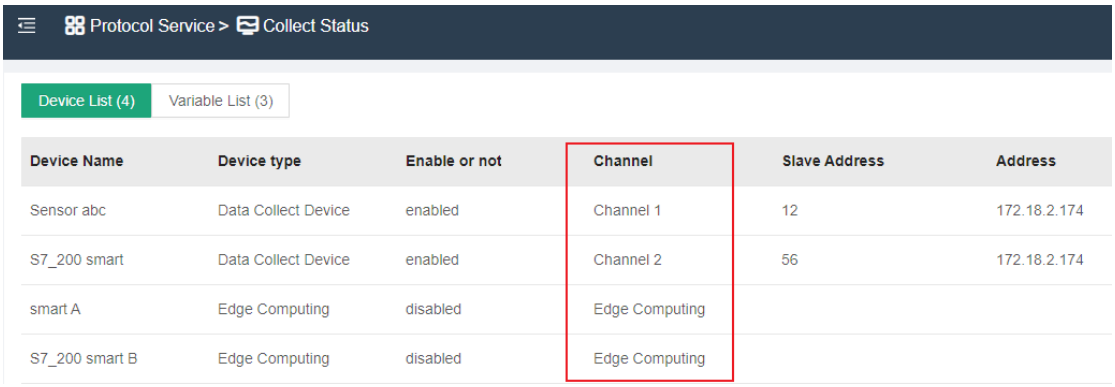
Reuse Context allows you to set a restart mechanism for the scripts

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).

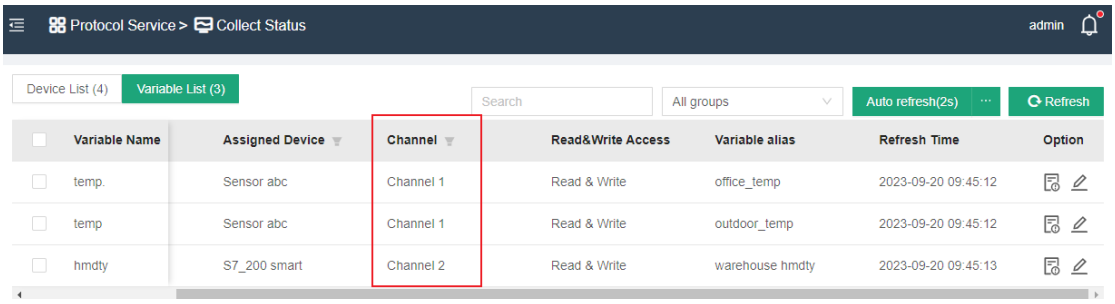
4.6 Collection Status

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

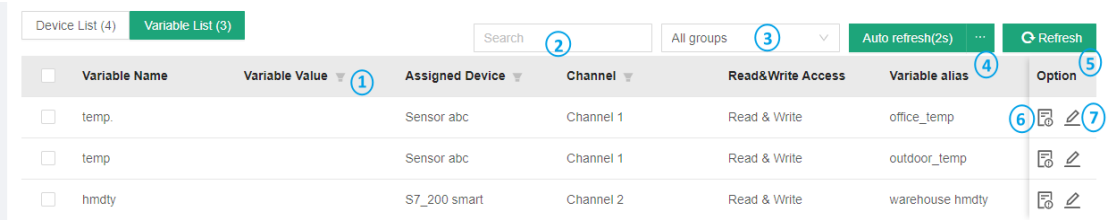
The **Device List** displays information about the collection devices, edge computing, historical data, etc. Users can differentiate the data based on the collection channels.



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.



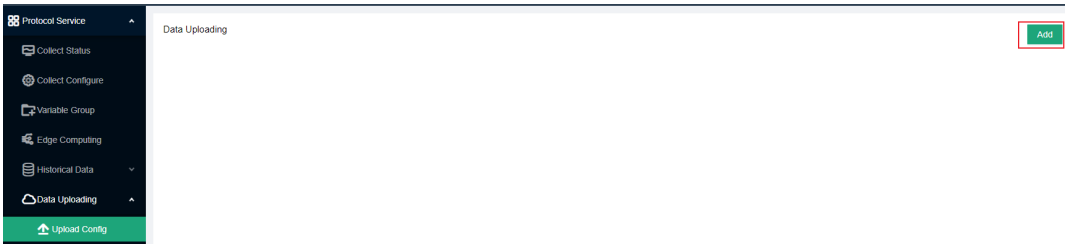
Description:

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).

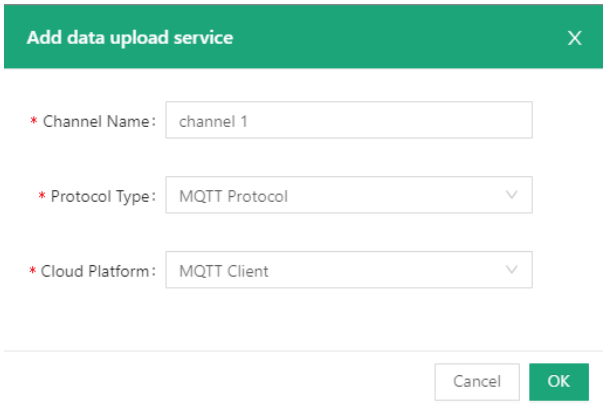
4.7 Data Upload and Encapsulation

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.

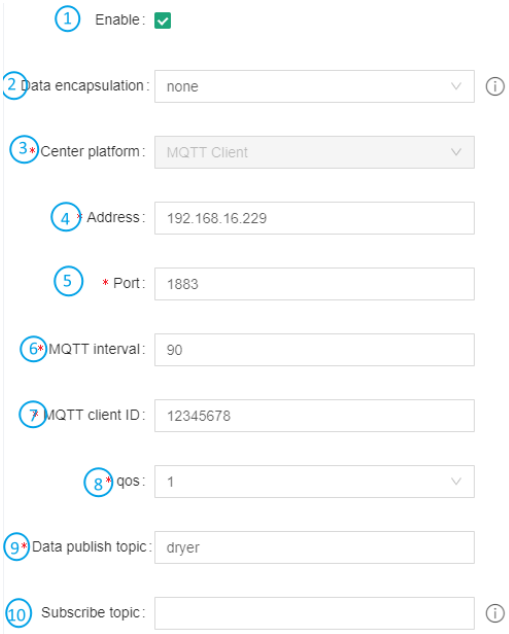
1. Expand the **Data Uploading** tab from the navigation pane and click **Upload Config**.
2. Click the **Add** button on the upper right corner to add a data upload task.



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



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



Description:

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 .

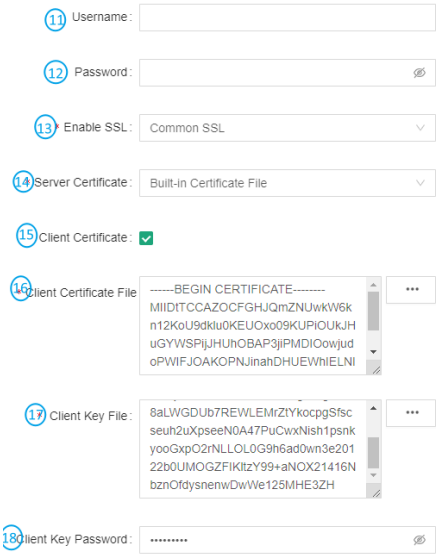
   QoS 0: The message will be sent once at the maximum. If the client is not available, the message will get lost.

   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).

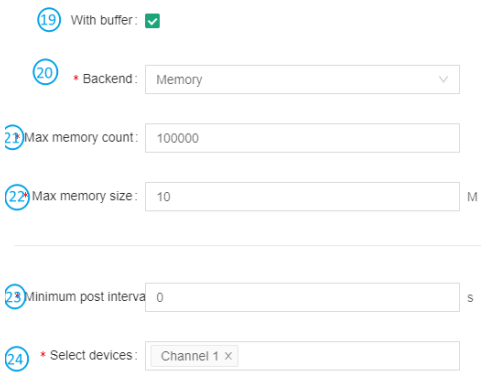
14) If common SSL is enabled, select a certification mode for the server.

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.

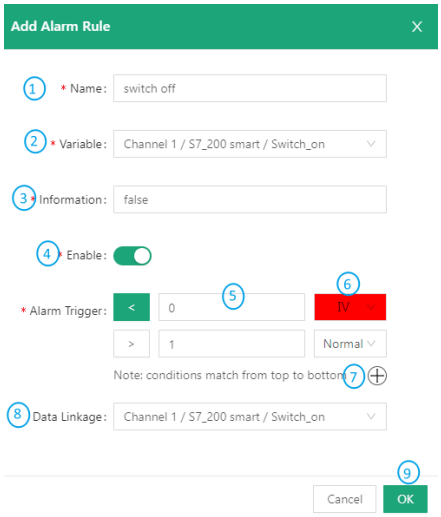
Description:

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

4.8 Alarm

4.8.1 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.

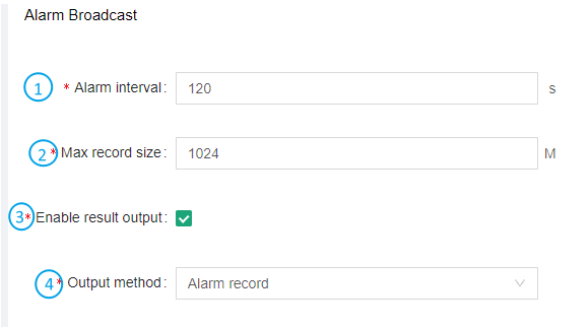


Description:

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.

4.8.2 Alarm Broadcast

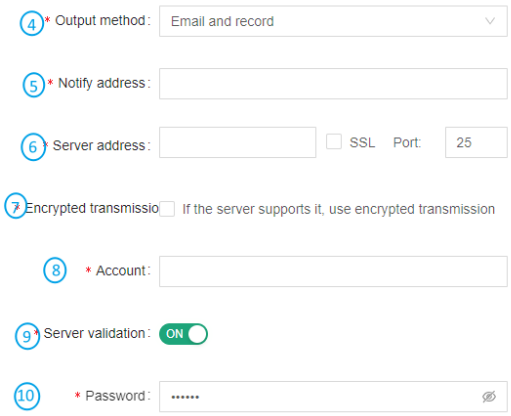
When the alarm rules are created, you can set the parameters for pushing an alarm on the **Alarm Broadcast** page.



Description:

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.

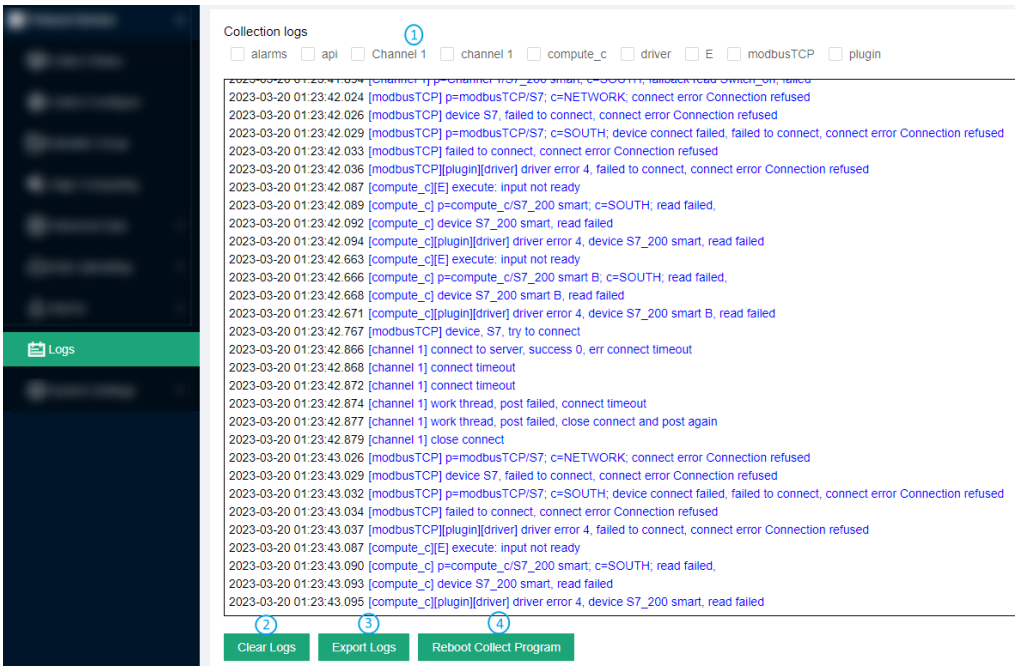
When you are all set, you can send a test email to check if the settings are ok, then submit the settings.

4.8.3 Alarm Record

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

4.9 Logs

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



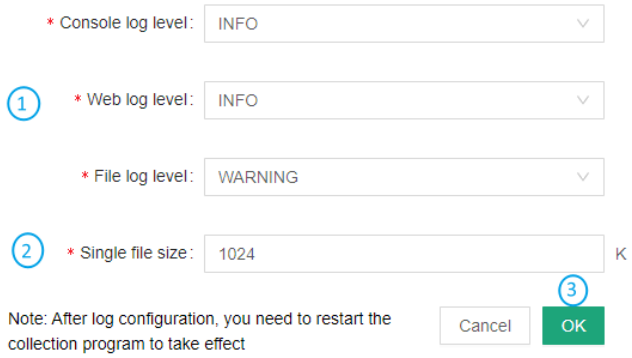
Description:

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

4.10 System Settings

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

- **Log Config.**



Description:

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.