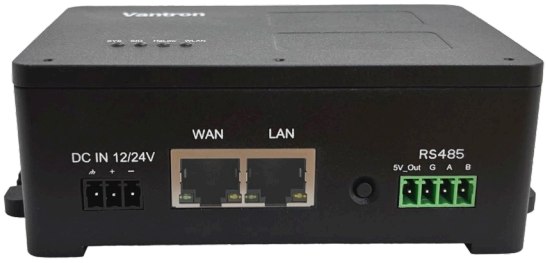
HAP202 Wi-Fi HaLow Unit



User Manual

Version: 2.0

© Vantron Technology, Inc. All rights reserved.

Revision History:

No.	Description	Date
V1.0	First release.	Oct. 20, 2025
V1.1	Modified LED definition	Nov. 13, 2025
V1.2	Updated 1.3 Terminologies and Acronyms	Dec. 5, 2025
V1.3	Deleted the Edge Computing section as the current HW version does not include the serial port.	Jan. 22, 2026
V2.0	1. Updated the definitions of mesh MPP and MP, clarifying that the MPP is the DHCP server in a HaLow mesh network. 2. Updated the interface definition to reflect the GEN2 hardware design changes. 3. Updated the installation procedures in Section 2.2 per device appearance change. 4. Removed Sections 2.4.1 & 2.4.2 and merged the mobile login method with the PC login process. 5. Removed Section 2.6.1 (DPP Pairing via Hardware Setup), as the hardware-based method is no longer available. 6. Removed Section 2.7 (Quick Mesh Networking) as the updated hardware design does not support this feature. 7. Removed Sections 2.8 & 2.9 and integrated the description of BlueSphere GWM and factory reset into Sections 3.6.4.1 and 1.6, respectively. 8. Updated Section 3.4 about HaLow mode-related operations.	Sep. 14, 2026

Table of Contents

Foreword 1
CHAPTER 1 DEVICE INTRODUCTION 5
1.1 Product Overview 6
1.2 Unpacking 6
1.3 Terminologies and Acronyms 7
1.4 Specifications 8
1.5 Product Layout 10
1.5.1 Front view 10
1.5.2 Back view 11
1.6 Reset Button 11
1.7 LED Indicators 12
1.7.1 System LED (SYS) 12
1.7.2 Wi-Fi Activity LED (WLAN) 12
1.7.3 HaLow Signal LED (SIG) 12
1.7.4 HaLow Activity LED (HaLow) 13
1.8 Serial Port 13
CHAPTER 2 GETTING STARTED 14
2.1 Network Architecture 15
2.1.1 Standard HaLow Network 15
2.1.2 HaLow Mesh Network 16
2.2 Setting up the Device 17
2.3 Powering up the Device 18
2.4 Quick Access to the Device 19
2.5 Default Network Interface Status 21
2.6 DPP Pairing 21
2.6.1 Device Setup for DPP Pairing 21
2.6.2 Exiting DPP Pairing Mode 23
2.7 SSH and Serial Console Access 24
CHAPTER 3 DEVICE SETUP IN VANTRONOS 26
3.1 Introduction to VantronOS 27
3.1.1 Web Overview 27
3.1.2 Log Out 28
3.2 Dashboard 29
3.3 Network 30
3.3.1 WAN Interface 30
3.3.1.1 Basic IP Configuration 31
3.3.1.2 Interface Bridging 33
3.3.1.3 Link Priority 34
3.3.1.4 Link Diagnosis 35
3.3.2 LAN Interface 36
3.3.2.1 Subnet Conflict 36
3.3.2.2 DHCP Service & DHCP Reservation 36
3.3.2.3 IPv6 Settings 38

3.3.3 Wi-Fi 39
3.3.3.1 AP-Mode Basic Settings 39
3.3.3.2 AP-Mode Advanced Settings 40
3.3.3.3 Client-Mode Basic Settings 41
3.3.3.4 Client-Mode Advanced Settings 42
3.3.4 QoS Bandwidth Control 43
3.3.5 Static Route 44
3.3.6 Porting Mapping 46
3.3.7 Network Security 48
3.3.7.1 Basic SSH Access Setup 48
3.3.7.2 ACL Access Control 49
3.4 HaLow 52
3.4.1 Overview 52
3.4.1.1 STA-Mode Settings 53
3.4.1.2 AP-Mode Settings 55
3.4.1.3 Mesh Networking 57
3.5 Terminals 59
3.6 System 60
3.6.1 Device Settings 60
3.6.1.1 Modifying Device Name 60
3.6.1.2 System Time 61
3.6.2 User Management 62
3.6.3 Diagnostics 63
3.6.3.1 Network Diagnostics 63
3.6.3.2 Web Terminal 64
3.6.3.3 Logs 65
3.6.4 System Maintenance 66
3.6.4.1 BlueSphere 66
3.6.4.2 Device Maintenance 68
3.7 Command Line Interface 69
3.8 Edge Computing 70
3.8.1 Serial to TCP 70
3.8.1.1 Server Mode Rule Setup 71
3.8.1.2 Client Mode Rule Setup 72
3.8.2 PLC 73
CHAPTER 4 INDUSTRIAL PROTOCOLPORTAL 74
4.1 Overview 75
4.2 Portal Login 75
4.3 Protocol Configuration and Application 76
4.3.1 Collection Channel Setup 76
4.3.2 Device Setup 80
4.3.3 Variable Setup 81
4.4 Edge Computing Scripts Setup 84
4.5 Collection Status 86
4.6 Data Upload and Encapsulation 87

4.7 Alarm 91
4.7.1 Alarm Configuration 91
4.7.2 Alarm Broadcast 92
4.7.3 Alarm Record 93
4.8 Logs 93
4.9 System Settings 94
CHAPTER 5 DISPOSAL AND PRODUCT WARRANTY 95
5.1 Disposal 96
5.2 Warranty 97
Appendix Regulatory Compliance Statement 98

Foreword

Thank you for purchasing HAP202 Wi-Fi HaLow Unit ("the Product" or "the device"). This manual intends to provide guidance and assistance necessary on setting up, operating or maintaining the Product. Please read this manual and make sure you understand the structure and functionality of the Product before putting it into use.

Unless otherwise stated, ***Wi-Fi*** in this manual refers to 2.4 GHz/5 GHz Wi-Fi, and ***HaLow*** refers to Wi-Fi HaLow.

Intended Users

This manual is intended for:

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

Copyright

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

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

Disclaimer

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

It is our practice to change part numbers when published ratings or features are changed, or when significant construction 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 contain the following information in your question:

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

Vantron Technology, Inc.

Address: 48434 Milmont Drive, Fremont, CA 94538

Tel: (650) 422-3128

Email: sales@vantrontech.com

Regulatory Information

The Product is designed to comply with:

- Part 15 of the FCC Rules
- ISED

Please refer to **Appendix** for Regulatory Compliance Statement.

Symbology

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

Note: Calls attention to critical operational or safety information.

Italic Texts: Provides supplementary details or context that are essential for proper application.

General Safety Instructions

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

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

Precautions for Power Cables and Accessories

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

⚠ Place the power cable 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 before cleaning the Product
- Do not use caustic or aggressive liquids, vapor, or spray
- 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 device is not allowed
- Do not change components unless the power cable is unplugged
- In some cases, the device may still have residual voltage even if the power cable is unplugged. Therefore, it is a must to remove and fully discharge the device before replacement of the components.

CHAPTER 1 DEVICE INTRODUCTION

1.1 Product Overview

Powered by Morse Micro's MM8108 Wi-Fi HaLow chipset, Vantron HAP202 features a new configuration with dual Ethernet ports. This design provides more flexible and convenient access to the device management portal, eliminating the need to manually switch between LAN and WAN connections when the 2.4 GHz/5 GHz Wi-Fi is operating in client mode. In addition, it is designed to maximize the chipset's throughput to ensure reliable and efficient data transfer.

Operating in both sub-1GHz (IEEE 802.11ah) and 2.4 GHz/5 GHz (IEEE 802.11 b/g/n/ac) bands, the device provides long-range connectivity up to 1km at 32.5Mbps and short-range speeds up to 867Mbps, respectively, ensuring reliable performance. The DPP (Wi-Fi Easy Connect) handles secure, effortless device pairing, and the optional IP54 waterproof kit enables reliable outdoor deployment.

Ideal for long-range, sub-GHz networking, HAP202 is well-suited for a variety of applications, including smart home systems, video surveillance, industrial process control, logistics and asset tracking, and smart city infrastructure.

1.2 Unpacking

The device has been carefully packed with special attention to quality. However, should you find any component damaged or missing, please contact your sales executive in due time.

Standard accessories:

- HAP202 Wi-Fi HaLow unit
- 2 × 2.4 GHz/5 GHz Wi-Fi antenna
- 1 × Wi-Fi HaLow antenna
- 1 × DC power connector

Optional accessories:

- 1 × 12V/1A power adapter
- 1 × Power cord
- 1 × RS485 terminal connector
- Waterproof kit for the IP54 variant: 1 × Waterproof base + 1 × Waterproof cover

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

1.3 Terminologies and Acronyms

Below is a summary of the key terminologies and acronyms that will be covered in this manual.

Glossary	Description
Access Point (AP)	A HaLow access point (AP) broadcasts the HaLow network to multiple HaLow stations (STA). It typically connects to an internet router, distributing internet connectivity to all paired STAs. In a standard HaLow network, there will always be **only one** HaLow AP.
Station (STA)	An STA is a client device that connects to a HaLow AP for a standard HaLow networking. It normally accesses external networks through the HaLow AP.
Standard HaLow network	Standard HaLow network describes the basic star-shaped HaLow network architecture. In this topology, all STAs associate with a central AP, and traffic between endpoints is relayed through the AP.
HaLow Mesh network	A HaLow Mesh network extends network range and improves reliability through multi-hop communication between interconnected nodes, which automatically determine the most efficient path for data transmission.
Mesh Portal (MPP)	A Mesh Portal (MPP) serves as the DHCP server in a mesh network. When a HaLow AP enables mesh settings, it takes on a combined AP+MPP role. Mesh nodes gain internet access when the MPP connects to an upstream router.
Mesh Point (MP)	A Mesh Point (MP) operates as an intermediate HaLow node that forwards data between other mesh nodes via multi-hop relaying. These nodes retain their original HaLow IP addresses as mesh IP addresses.
Device Provisioning Protocol (DPP)	Defined by Wi-Fi Alliance for **Wi-Fi Easy Connect™**. In this document, it refers specifically to the fast provisioning of devices via simple hardware/software setup for a standard HaLow pairing (“**DPP Pairing**”).
VantronOS	Web management portal for Vantron IoT communication devices.
Dynamic Channel Selection (DCS)	DCS is a mechanism that automatically evaluates channel conditions and selects a suitable operating channel for the radio. It avoids interference from other wireless signals and improves link stability.

Unless otherwise stated, *Wi-Fi* in this manual refers to 2.4 GHz/5 GHz Wi-Fi, and *HaLow* refers to Wi-Fi HaLow.

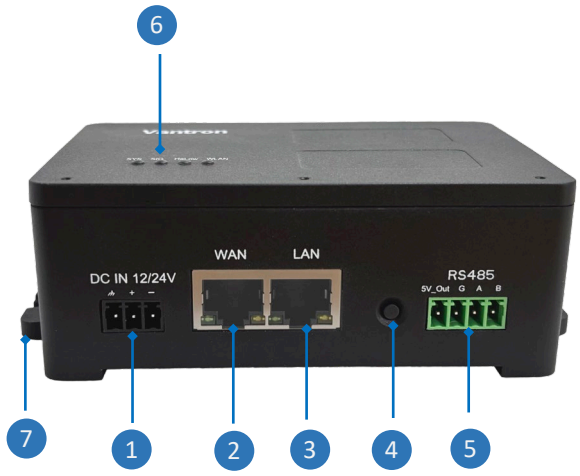
1.4 Specifications

HAP202			
System	CPU	NXP single-core Arm Cortex-A7 CPU, up to 792MHz	
	Wi-Fi HaLow chipset	Morse Micro MM8108	
	Memory	512MB (Optional: 256MB)	
	Storage	128MB	
WLAN Features	2.4 GHz/5 GHz Wi-Fi	Standard: IEEE 802.11 b/g/n/ac	
		Frequency range: 2.412GHz~2.462GHz; 5.15 GHz~5.25 GHz, 5.25 GHz~5.35 GHz, 5.47GHz~5.725 GHz, 5.725 GHz~5.85 GHz	
		Channel bandwidth: 20/40/80MHz	
		Data rate: up to 867Mbps	
		Security: AES-CCMP	
		Working mode: Access point (AP), station (STA)	
	Wi-Fi HaLow	Standard: IEEE 802.11 ah	
		Frequency range: 903.5MHz~926.5MHz (US)	
		Channel bandwidth: 1/2/4/8MHz, dynamic channel selection (DCS) supported	
		Max. transmit power: 23dBm	
		Data rate: up to 32.5Mbps@8MHz or 15Mbps@4MHz	
		Fast pairing: DPP Easy Connect via hardware/software setup	
		Security: AES, WPA3	
		Working mode: Access point (AP), station (STA), Mesh	
Bluetooth	Version	BT 5.4	
I/O	Fast Ethernet	2 × RJ45, 10/100Mbps (1 × WAN (default)/LAN, 1 × LAN)	
	Serial Port	1 × RS485 (4-pin terminal, 5V output)	
	Antenna	1 × Wi-Fi HaLow antenna	1 × 2.4 GHz/5 GHz Wi-Fi antenna
System Control	LED indicators	1 × System LED	1 × HaLow signal LED
		1 × HaLow activity LED	1 × Wi-Fi activity LED
	Button	1 × Reset button	
Mechanical	Dimensions	IP40 version (with wall mount): 130mm × 82.9mm × 42mm	
		IP54 version (with wall mount and water proof kit): 130mm × 127.9mm × 44mm	
	Casing material	Black plastics, UL94, SP6 compliant (Optional: White casing)	
	Installation	Flat mount, wall mount	
	IP rating	IP40 (Optional: IP54, independent waterproof kit provided)	
Power	Input	9V ~ 40V DC	
	Port	3-pin terminal (Over-current protection, reverse polarity protection)	

HAP202			
Software	Operating system	VantronOS	
	Device management	Vantron BlueSphere GWM	
	Upgrade	Local upgrade, OTA upgrade	
	Network protocol	IPv4, HTTPS, TCP & UDP, NTP client and server, ARP, TLS	
	Link detection	Heartbeat detection, auto reconnection	
	Network reliability	Multi-channel failover, backup between Ethernet, Wi-Fi, HaLow	
	IP application	Ping, Traceroute, DHCP Server/Client	
	IP routing	Static routing, dynamic routing	
Security	2.4 GHz/5 GHz Wi-Fi	AES-CCMP	
	Wi-Fi HaLow	AES, WPA3	
	Firewall	Stateful	
	Access control	MAC address, IP address, URL	
Environmental	Temperature	Operating: -20℃ ~ +70℃	Storage: -40℃ ~ +85℃
	Humidity	5% ~ 95%RH (Non-condensing)	
	Certification	FCC, ISED	

1.5 Product Layout

1.5.1 Front view



Item	Description	
1	Power terminal, supporting 9V~40V DC input	
2	WAN/LAN (100Mbps), configured as a WAN port by default	
3	LAN (100Mbps), mainly for device login	
4	Reset button	([2s, 6s): Restart the device; [6s, 12s): Configuration clear; [12s, 20s): Factory reset; [20s,+∞): Normal operation)
5	Serial port	RS485, 5V output
6	LED indicators (Refer to Section 1.7 for details)	1 × HaLow signal LED
		1 × HaLow activity LED
		1 × WLAN activity LED
		1 × System LED
7	Mounting brackets (screws recommended: M3 × 8mm/ST2.9 depending on the mounting surface)	

1.5.2 Back view



Interface	Description
1	2.4 GHz/5 GHz Wi-Fi & Bluetooth antenna connector
2	Wi-Fi HaLow antenna connector
3	Mounting brackets (screws recommended: M3 × 8mm/ST2.9 depending on the mounting surface)

1.6 Reset Button

The HAP202 offers a reset button for device reboot or factory 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.

1.7 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.

1.7.1 System LED (SYS)

LED Status	Description
OFF	Device not powered on; system boot failure; system anomaly
Blinking at 3Hz	Device boot / firmware upgrade / app installation in progress; device reset / factory reset
Solid on	Device working properly

1.7.2 Wi-Fi Activity LED (WLAN)

Mode	LED Status	Description
Wi-Fi Client	OFF	Wi-Fi link is down.
	Blinking at 1Hz	Not connected to a Wi-Fi AP yet.
	Solid green	Connected to a Wi-Fi AP.
Wi-Fi AP	OFF	Wi-Fi link is down.
	Blinking at 1Hz	No Wi-Fi client connected yet.
	Solid green	At least one Wi-Fi client connected.

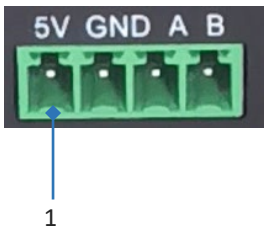
1.7.3 HaLow Signal LED (SIG)

LED Status	LED Color	Signal Strength	RSSI Range
Solid on (HaLow network established)	Red	Weak	RSSI (<-70) dBm
	Yellow	Fair	RSSI (-50, -70) dBm
	Blue	Good	RSSI (-30, -50) dBm
	Green	Excellent	RSSI (0, -30) dBm

1.7.4 HaLow Activity LED (HaLow)

HaLow Mode	LED Color	LED Status	Description
HaLow STA	Blue	OFF	Wi-Fi HaLow link is down.
		Blinking at 1Hz	Not connected to a HaLow AP yet.
		Blinking at 3Hz	DPP pairing initiated.
		Solid on	Connected to a HaLow AP.
HaLow AP	Green	OFF	Wi-Fi HaLow link is down.
		Blinking at 1Hz	No HaLow STA connected yet.
		Blinking at 3Hz	DPP pairing initiated.
		Solid on	At least one HaLow STA connected.
HaLow Mesh (Including Mesh + AP)	Cyan	OFF	Wi-Fi HaLow link is down.
		Blinking at 1Hz	Not joined to a HaLow Mesh network.
		Solid on	Joined a HaLow Mesh network.

1.8 Serial Port



The HAP202 offers an RS485 connector for serial communication. The default baud rate of the port is 9600, and the pinout description is as follows:

No.	Signal	Type	Description
1	5V_out	P	5V output
2	GND	P	Ground
3	A	I/O	RS485 A signal
4	B	I/O	RS485 B signal

Port wiring: A-A, B-B, GND-GND

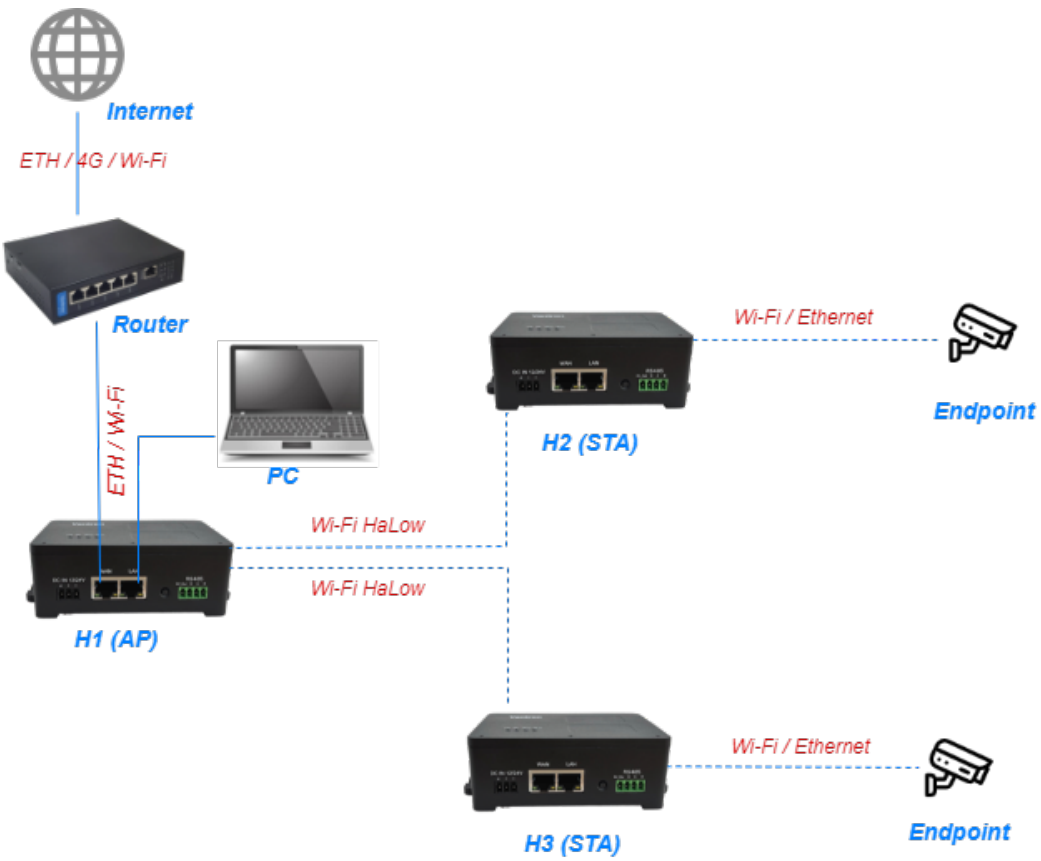
CHAPTER 2 GETTING STARTED

2.1 Network Architecture

The HAP202 can operate as either an AP or STA in a Standard HaLow network, or as a Portal or Point in a HaLow Mesh network. This flexibility allows the unit to be installed in a variety of environments and layouts.

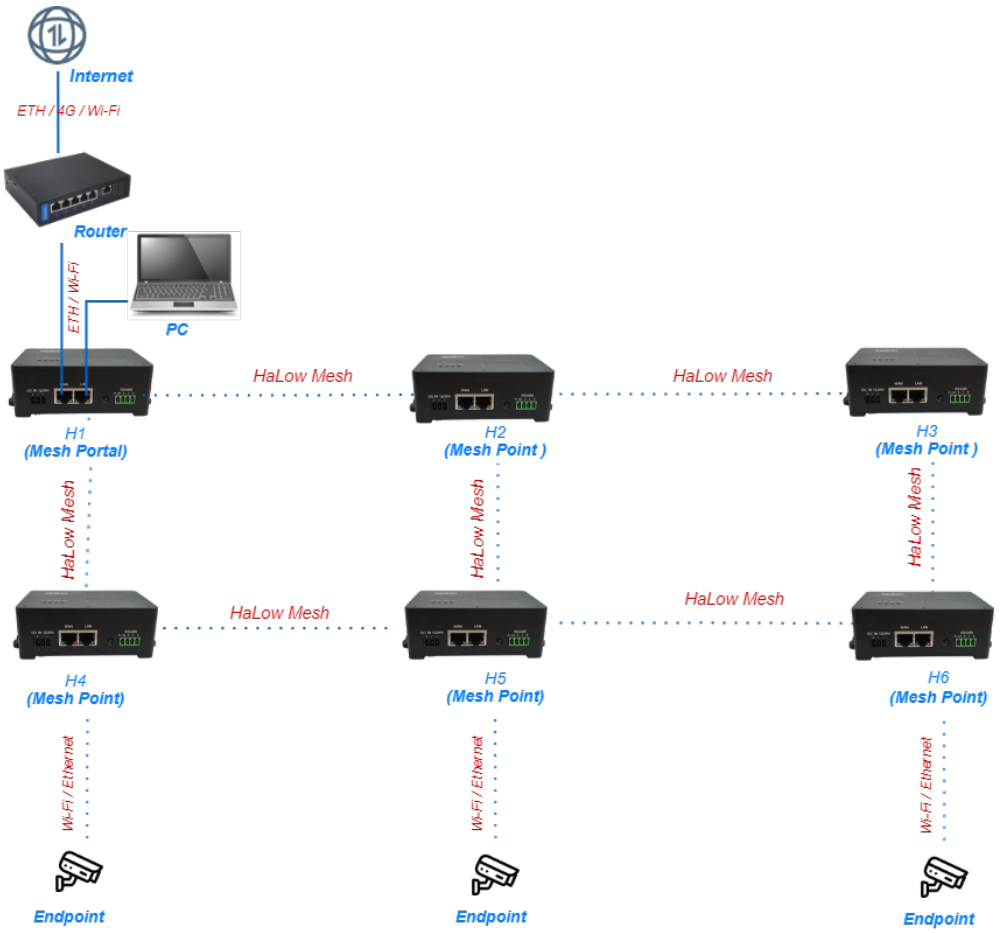
2.1.1 Standard HaLow Network

Standard HaLow mode refers to a basic HaLow network architecture, featuring direct communication between AP and STAs. Typically, the AP is connected to an internet router to distribute internet connectivity. This setup extends internet access from a central location to various points across the property — up to 1 km (~3200 Ft) — depending on bandwidth requirements, the number of STAs connected to the AP, and any obstacles between the STAs and the AP.



2.1.2 HaLow Mesh Network

A HaLow Mesh network involves multiple interconnected Mesh Points that extend the HaLow network coverage.



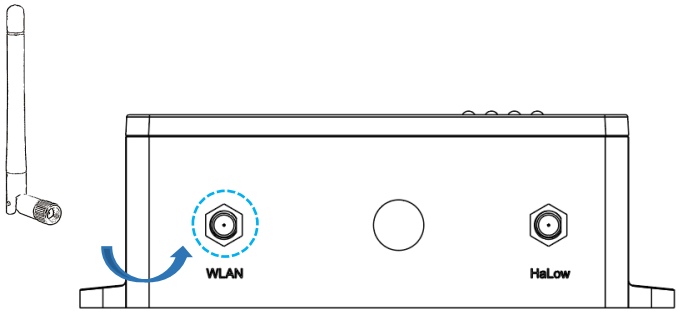
In this topology:

- H1 offers the DHCP service and relays the internet access to the entire mesh network.

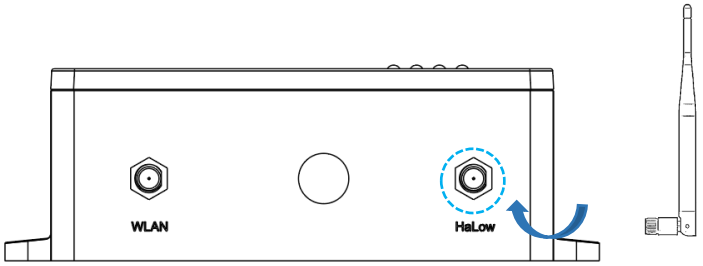
2.2 Setting up the Device

When mounting the HAP202 on a vertical surface, ensure the device is positioned so that the LED indicators are visible from ground level. For outdoor installations, it's highly recommended to use the waterproof kit to protect the electronics of the device.

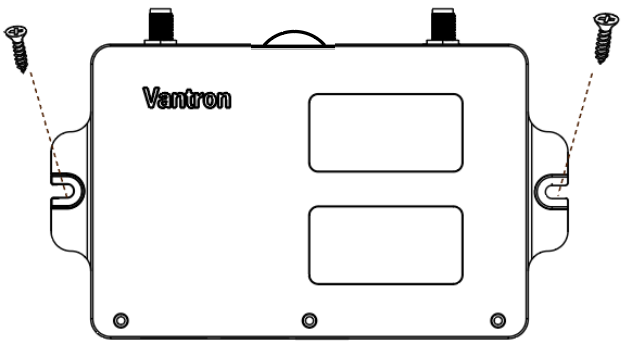
1. Install the shorter antenna onto the WLAN antenna connector (*labelled as WLAN*).

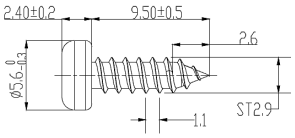


2. Install the longer antenna onto the Wi-Fi HaLow antenna connector (*labelled as HaLow*).

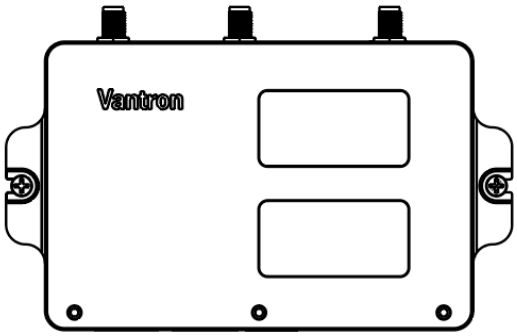


3. Depending on the condition of the mounting surface, secure the device with two ST2.9 self-tapping screws for surfaces without pre-tapped holes, or two M3 × 8 mm screws for surfaces with matching pre-tapped threaded holes.

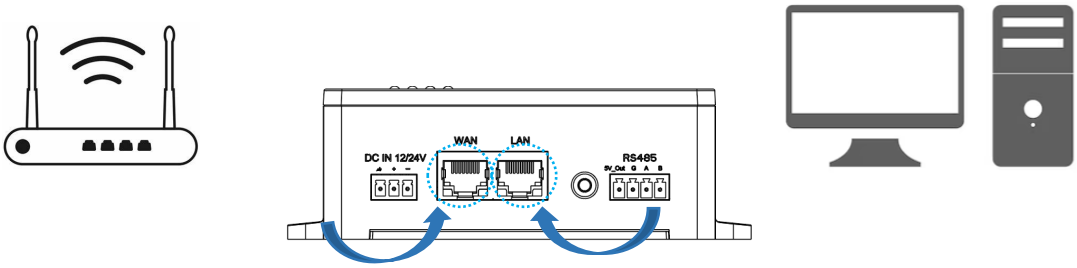




4. Tighten the screws and gently swing the device to make sure it is fastened.



5. When needed, connect the WAN port to a router for internet access, and connect the LAN port to a PC for device management.



2.3 Powering up the Device

Plug the DC power connector into the power terminal of the device and connect it to the power source using a 12V DC adapter to start it. It takes 2-3 minutes for the system to transition to normal operation, at which point the WLAN, HaLow, and SYS indicators will turn on.



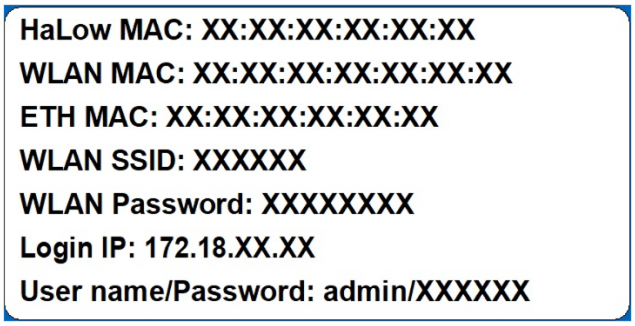
2.4 Quick Access to the Device

You may configure network settings and manage the device via the web-based management portal (VantronOS) using a Windows PC or mobile device.

There are two login options to access VantronOS for the HAP202, depending on how the host PC or mobile device connects to it.

Method	PC/Mobile Device Connection	Login Address
Option 1	Connected to HAP202's LAN network (via Ethernet or Wi-Fi).	HAP202's LAN IP
Option 2	WAN interface on the same IP subnet as HAP202's WAN interface (e.g., both connected to the same router or bridged network).	HAP202's WAN IP

By default, the device's 2.4 GHz/5 GHz Wi-Fi operates in **AP mode**. The default WLAN SSID & password, login IP address, and login credentials are all printed on the device label.



For quick device management, LAN access to the HAP202 is recommended.

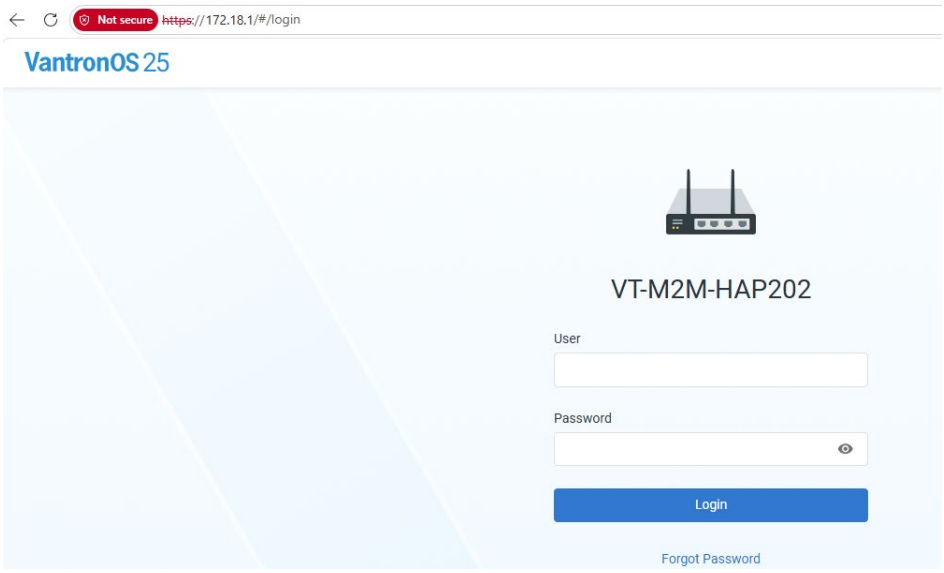
1. Connect the Windows PC or mobile device:
   - Via Ethernet

     Connect the PC or mobile device directly to the HAP202's LAN port using a standard Ethernet cable.
   - Via Wi-Fi

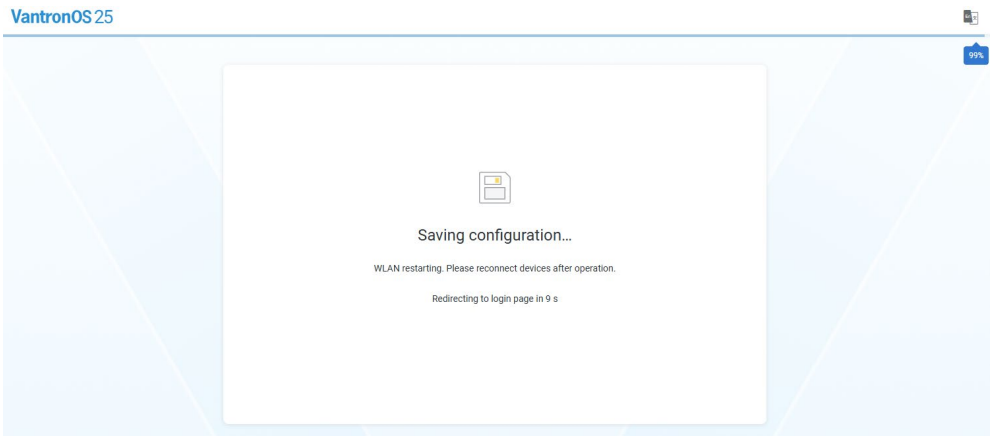
     Connect the PC or mobile device to the HAP202's Wi-Fi AP using the default WLAN SSID and password printed on the device label.
2. Enter the login IP in the browser for device login.

   *If a browser security warning appears, click **Advanced** to continue.*

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



4. Upon first-time login or login after a device reset, the system will automatically launch a setup wizard to guide you through essential configuration settings, including:
   - 2.4 GHz/5 GHz Wi-Fi AP SSID, encryption mode, and password (Both bands can be configured, but only the blue-highlighted tab represents the currently active band)
   - User password (Retain the existing password by clicking **Set up later** in the subsequent pop-up window)
   - Time zone (Enabling **Sync Local Time** synchronizes the device time with your local time)
5. Modify the settings as needed and wait about 10 seconds for new configurations to take effect.



6. After the wizard finishes, the HAP202 will restart its wireless radio. Reconnect the PC or mobile device to the device network if your connection drops.
7. On the reloaded login page, enter the new password (if you changed it during the setup) to access the web portal.

After any device reset, the setup wizard will be relaunched. A configuration clear requires your user-defined password, while a factory reset requires the credentials on the device label.

2.5 Default Network Interface Status

Network Interface	Default Working Mode	Default IP Address
2.4 GHz/5 GHz Wi-Fi	AP	172.18.1.1
Ethernet LAN	LAN	172.18.1.1
Ethernet WAN/LAN	WAN	Allocated by upstream DHCP server
Wi-Fi HaLow	STA	Allocated by upstream DHCP server

2.6 DPP Pairing

DPP pairing refers specifically to the fast provisioning of HaLow devices for a Standard HaLow connection. There is always only **one** HaLow AP within a standard HaLow network.

Each DPP pairing process enrolls exactly one AP with one STA. To add more STAs to the network, simply repeat the DPP pairing steps separately between the same AP and each new STA.

2.6.1 Device Setup for DPP Pairing

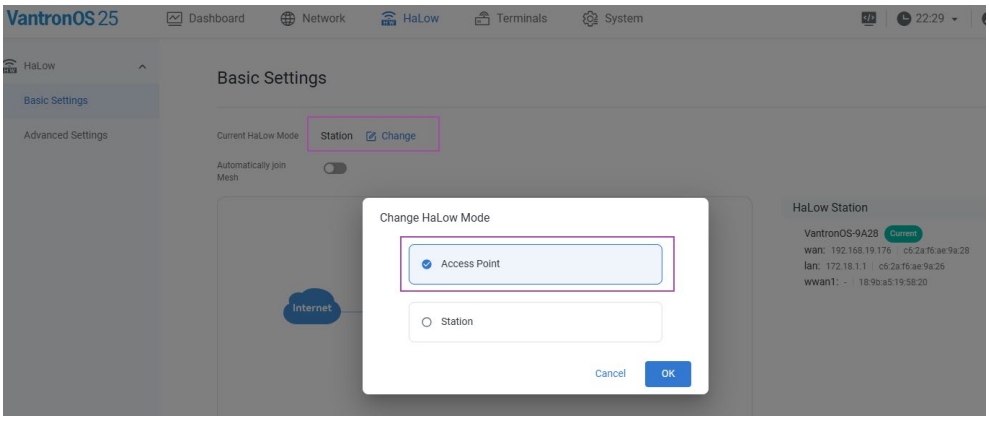
The device setup is completed via the VantronOS web management portal. All HAP202 units are factory set to HaLow STA mode. **The following procedures apply to two HAP202 units that both start in HaLow STA mode.**

1. Prepare two HAP202 units (H1 & H2). Power both units on and position them within a suitable short range for pairing.

   Do not place the devices too close to each other. Excessive proximity may cause radio interference and result in pairing failure.

2. Refer to Section 2.4 to log in to the VantronOS web portal for one HAP202 unit (H1).
3. Navigate to the **HaLow > Basic Settings** page in VantronOS.

4. Click **Change** and select the **Access Point** mode, then click **OK** to confirm and exit.



5. Refer to Section 2.4 to log in to the VantronOS web portal for the second HAP202 unit (H2).

   We recommend using a separate PC or mobile device for this login operation.

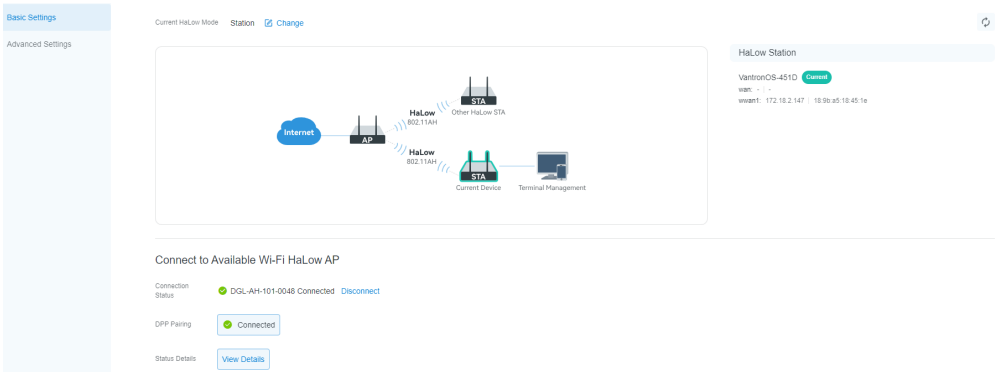
6. Navigate to the **HaLow > Basic Settings** page in VantronOS for H2.

7. Activate DPP pairing state on both devices:

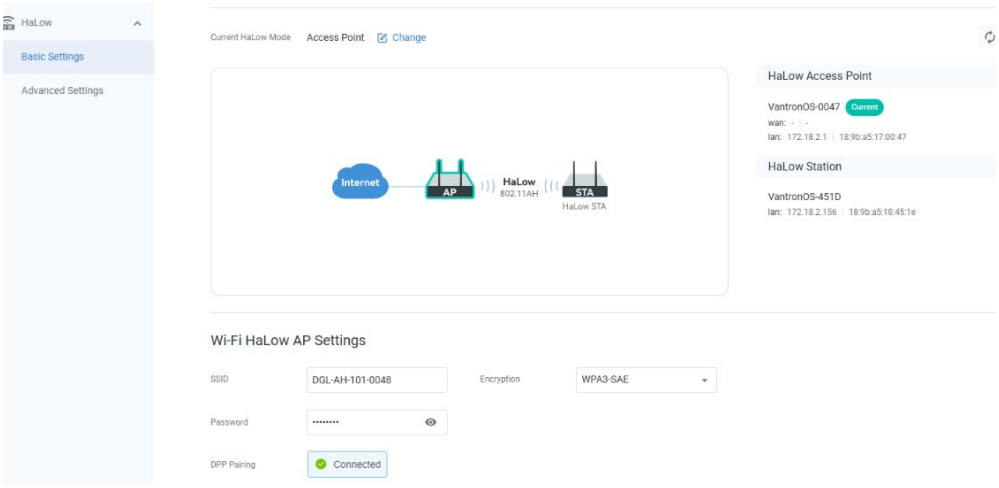
   - Enable the DPP state on the AP-mode unit (H1) **first**: Under the **Wi-Fi HaLow AP** section, click the **Pair** button next to **DPP Pairing**.
   - Immediately operate the STA-mode unit (H2): Under the **Connect to Available Wi-Fi HaLow AP** section, click the **Connect** button next to **DPP Pairing**.
   - Complete the two button clicks within a **120-second** window.

8. A **Connected** status indicates successful pairing.

   STA-side connection:



AP-side connection:



- For the STA: Click **View Details** to check connection information.
- For the AP: View connection details on the **Terminals** tab page.

9. Brief connection information appears beside the topology view.
10. Enable DPP state on the AP (H1) and repeat the above steps for any additional STAs.
11. Relocate the devices to their target positions once pairing finishes.

2.6.2 Exiting DPP Pairing Mode

The devices **exit** HaLow DPP pairing mode under any of the following conditions:

a. A standard HaLow connection is successfully established.

b. The second unit does not activate pairing mode within the **120-second** window following the first unit.

c. The HaLow connection between the two units fails.

2.7 SSH and Serial Console Access

SSH is enabled on the HAP202 by default. Prior to establishing an SSH connection, make sure the PC (client) can reach HAP202's (server) IP.

Method	PC Connection	Login Address/Parameters
Option 1	Connected to HAP202's LAN network (via Ethernet or Wi-Fi).	HAP202's LAN IP
Option 2	WAN interface on the same IP subnet as HAP202's WAN interface (e.g., both connected to the same router or residing on the same bridged network).	HAP202's WAN IP
Option 3	Connected to HAP202's debug port (serial session rather than SSH).	57600, 8N1

Unless otherwise configured, the HAP202's 2.4 GHz/5 GHz WLAN and Ethernet LAN interfaces are assigned the default IP address of 172.18.1.1.

Option 1 applies in most cases.

Option 2 requires retrieving the device's WAN IP from the upstream router.

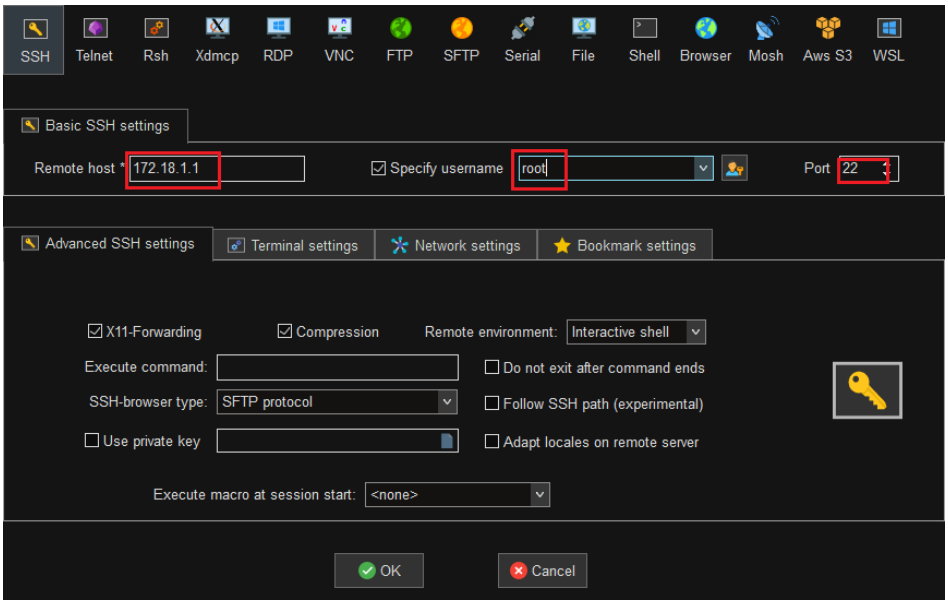
Option 3 involves uncovering the device and may expose the device to unauthorized access. Therefore, procedures for this option are not covered in this document.

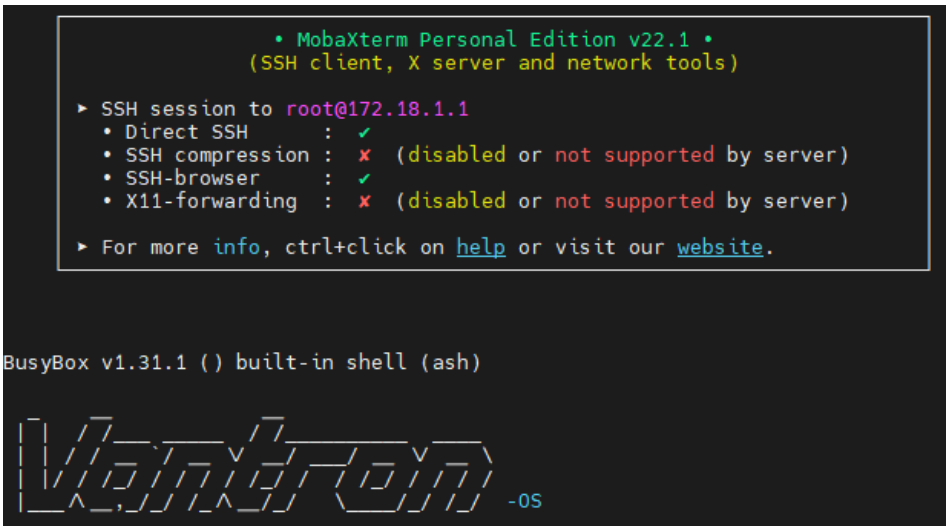
Example: SSH login via **LAN IP**

1. Connect the host PC to HAP202's LAN network via Ethernet or Wi-Fi.
2. Install an SSH client if it is not available.
   - **Windows PC**:
     - PuTTY
     - Tera Term
     - MobaXterm
   - **Linux PC**:

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

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





4. **Linux PC**: 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 privileges**. For security reasons, the root password is unique per device. Contact Technical Support to retrieve it.*

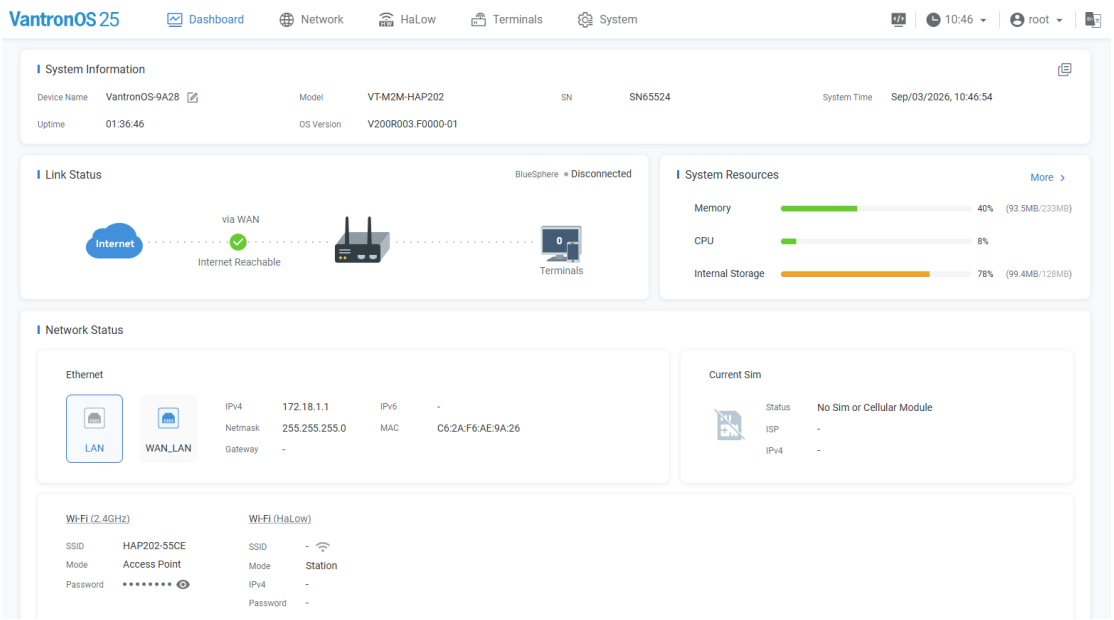
CHAPTER 3 DEVICE SETUP IN VANTRONOS

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, 2.4 GHz/5 GHz Wi-Fi setup, and advanced network configurations, such as static route, port mapping, and security configurations.

HaLow: Configures device settings for Wi-Fi HaLow connectivity.

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 access the device's shell for debugging.

Time Settings:

- Current time reflects the time zone chosen at initial device setup or on the time settings page.
- "Sync Local Time" aligns the device clock with the local time.
- "Time Settings" opens additional options for manual configuration.

Refer to Section 3.6.1.2 for modifying the time settings.

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

- Toggle the edge computing functionality which configures the device for field endpoint connection and data processing.
- Log out

Language Toggle: English ⇄ Chinese.

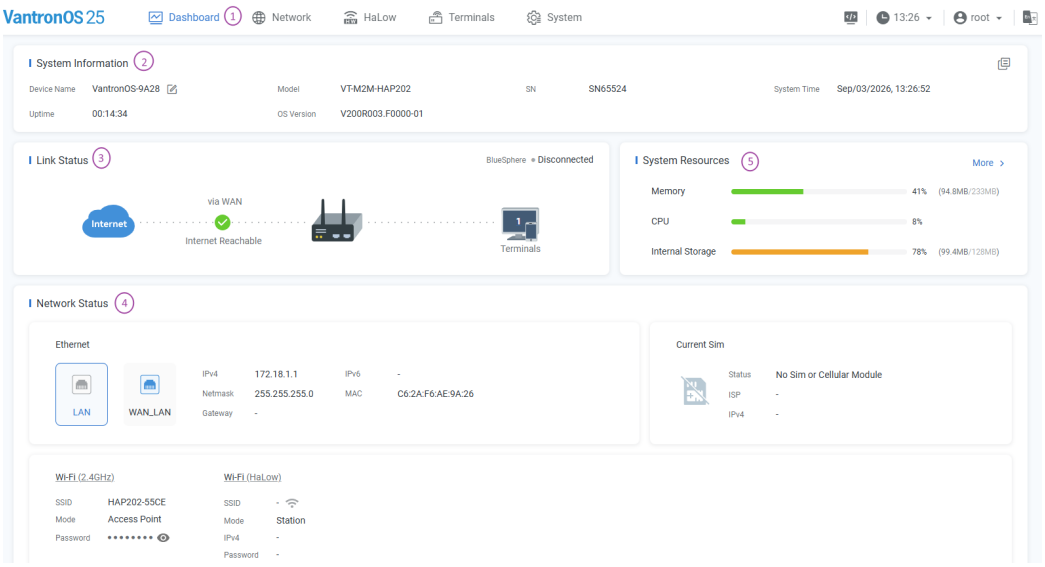
3.1.2 Log Out

To sign out:

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

3.2 Dashboard

Dashboard provides overall information of the device, including system information, device resource usage, interface connection status, current traffic, etc.



Description:

1. **Menu Tabs** — Highlights the active menu in blue.
2. **System Information** — Includes the device name, model, SN, IMEI, current system time, system uptime, and OS version.
   - Clicking the pencil icon next to the device name enables device name modification.
   - Clicking the copy icon in the upper-right corner copies all system information.
   - Pressing Ctrl + F12 switches between the baseline OS version and the specific build version.
3. **Link Status** — Shows a simplified network topology of the current device.
   - If the device has Internet connectivity, its access path will be shown (e.g. via WAN).
   - Clicking the count of connected terminals navigates to **Terminals** page, where detailed endpoint information is displayed.
   - If the device is enrolled with the BlueSphere GWM, a connected status will be displayed.
4. **Network Status** — Displays the live status of 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.
   - 2.4 GHz/5 GHz Wi-Fi / Wi-Fi HaLow: Displays device operation mode (e.g., AP or STA) and associated network details.
   - Cellular: Displays mobile network information (not applicable to the HAP202).

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, link redundancy, static routing, and more. These features enable precise control over connectivity, ensuring optimal performance and high availability. By integrating these tools, the system reduces administrative overhead and enhances operational efficiency, allowing you to build a resilient, secure, and fully customized network fabric.

Interfaces on the HAP202 are categorized as either WAN or LAN.

WAN interfaces include: 2.4 GHz Wi-Fi client, HaLow STA, and Ethernet WAN.

LAN interfaces include: 2.4 GHz Wi-Fi AP, HaLow AP, and Ethernet LAN.

3.3.1 WAN Interface

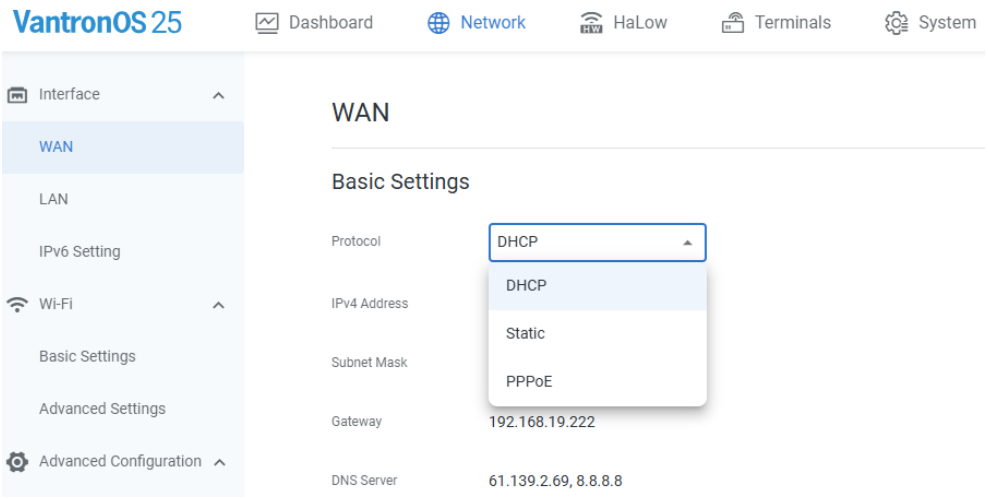
The WAN interface page includes the following three functionalities:

1. **Basic IP configuration** — Selects the IP protocol for the Ethernet WAN interface (e.g., DHCP, Static IP, PPPoE).
2. **Interface bridging** — Places all interfaces into the same Layer 2 bridge for transparent forwarding, with the selected interface serving as the uplink, and allows upstream DHCP to assign addresses to connected endpoints.
3. **Link priority IPv4** — Displays all upstream links and the port status, allowing you to modify their priority.

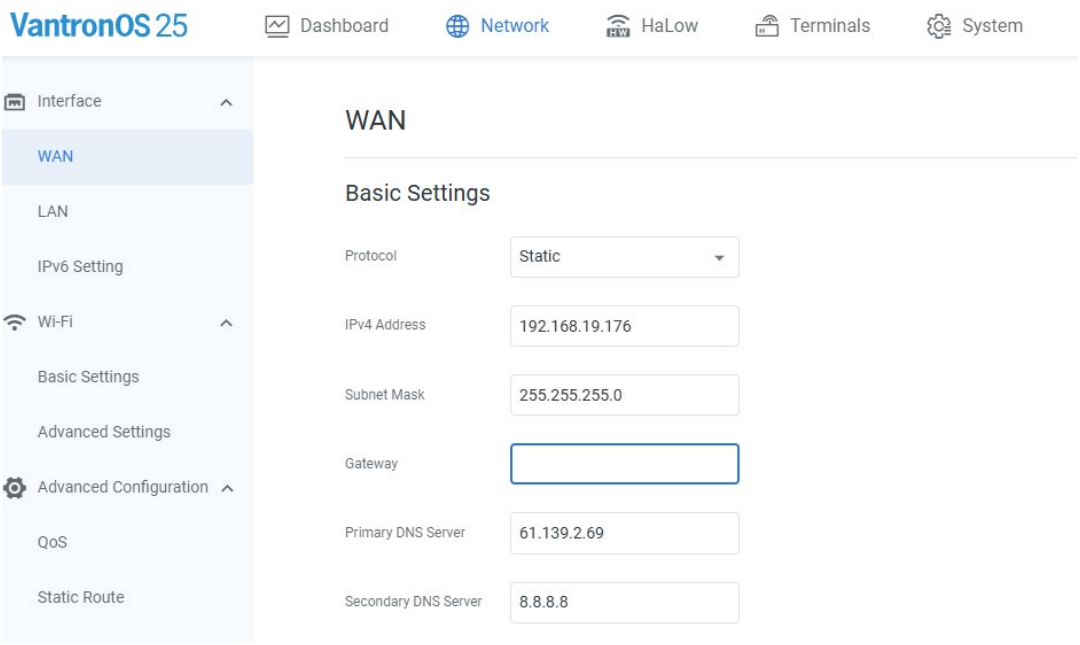
Whenever you make a change, always ensure the host PC and the HAP202 are on the same subnet for smooth VantronOS login.

3.3.1.1 Basic IP Configuration

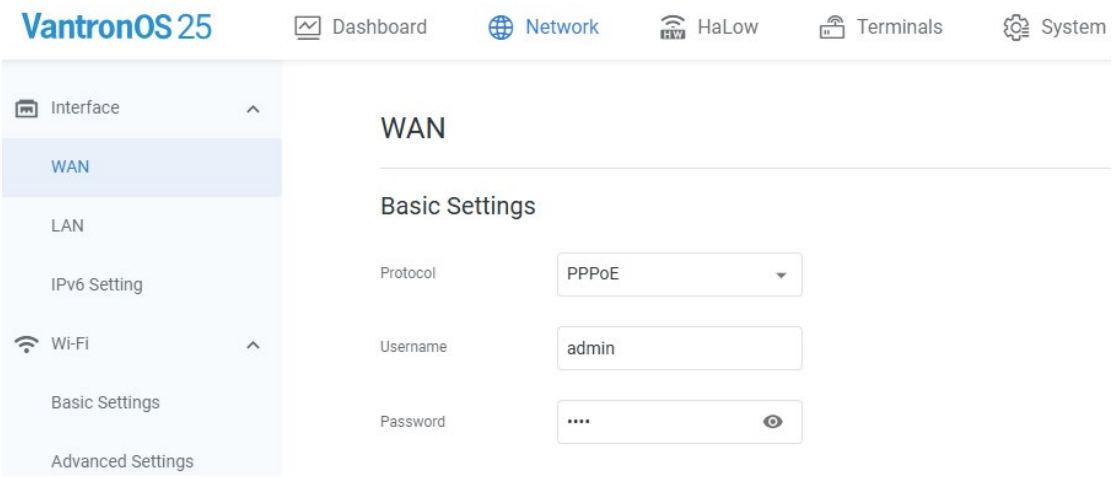
DHCP: The WAN interface obtains its IP address **automatically** from an upstream DHCP server.



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



PPPoE (Point-to-Point Protocol over Ethernet): The device initiates a dial-up connection to the ISP using a username and password encapsulated in PPP over Ethernet. The ISP then provides dynamic or static IP configuration.



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

3.3.1.2 Interface Bridging

Interface bridging on the HAP202 removes WAN/LAN zone separation, placing all interfaces into the same Layer 2 bridge for transparent forwarding. After bridging, IP addressing is centrally managed by an accessible upstream DHCP server. You may select either the Wi-Fi STA interface or the Ethernet WAN interface for bridging; the selected interface acts as the uplink to reach the DHCP server.

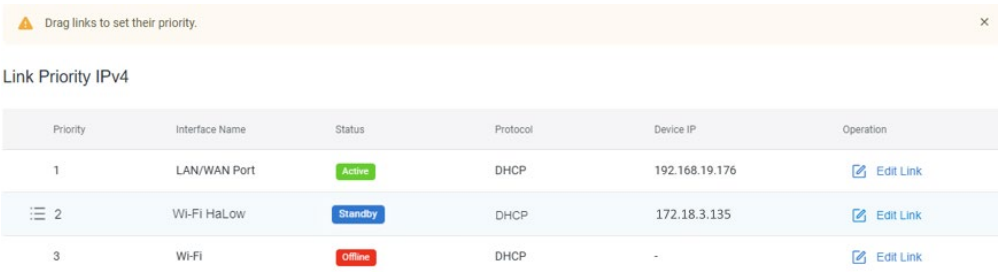
- After bridging is enabled, LAN interfaces **no longer** provide NAT and DHCP services to connected endpoints.
- When you bridge either the Ethernet WAN or Wi-Fi STA interface, the selected interface becomes the uplink. All other interfaces are moved into the same Layer 2 bridge, leaving the device with a single effective IP address for management access. You can retrieve this IP from the upstream router's DHCP client table.
- Management access is available from a PC connected to either this device or the upstream network.
- For HAP202 units, the Wi-Fi HaLow (mesh) interface of an MP is automatically bridged when the MP successfully joins a HaLow mesh network, and its IP address is assigned by the MPP (formerly HaLow AP) in the network.
- 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 conventional Wi-Fi STA interface, available SSIDs will be displayed for quick connection.
- To **disable interface bridging**, enable the **DHCP service** on the **Interface > WAN** page. You may need to log back into the device using its original LAN IP once the DHCP service is re-enabled if the host PC connects to the device over LAN.

3.3.1.3 Link Priority

Link Priority defines the preferred order of available uplink interfaces for automatic failover. When multiple uplink candidates are available, the device uses the highest-priority healthy link as the active uplink. If the primary link fails, the device automatically switches to the next available lower-priority uplink.

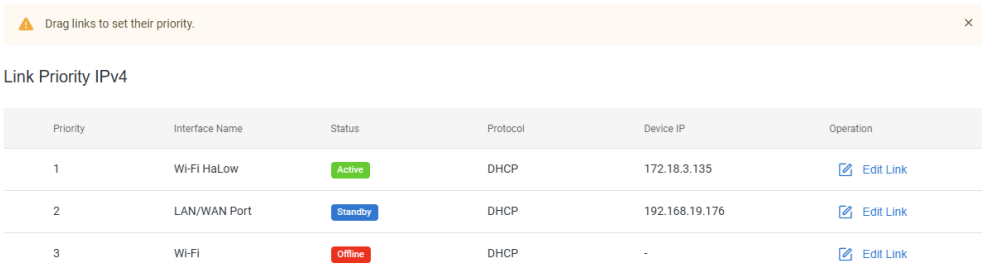
To manually set the network priority:

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



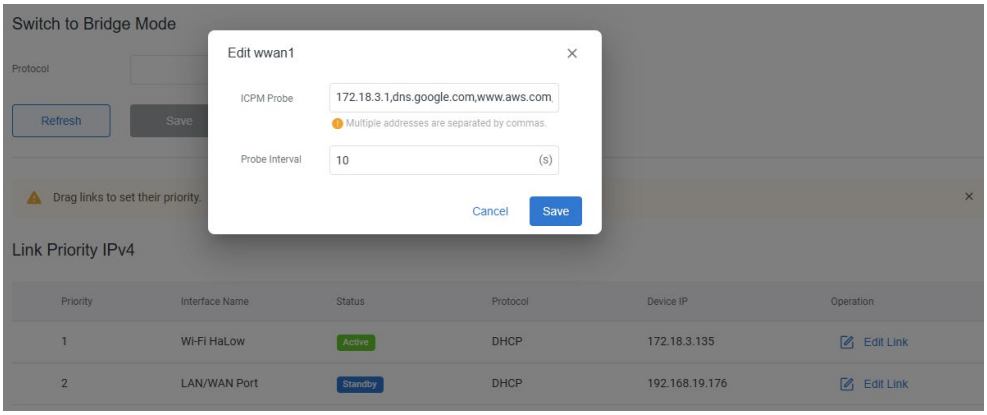
The screenshot is for illustration only. In a typical deployment, individual HaLow stations would not be connected as standalone units to an external network.

2. Drag the target link up or down to the desired position and wait a few seconds to allow the changes to apply.



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

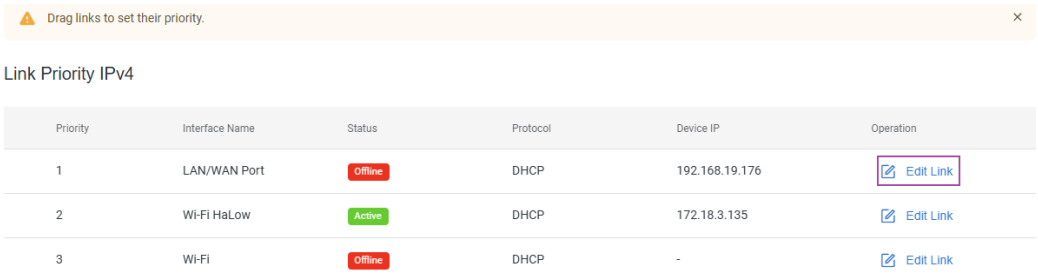
3. Use the **Edit Link** option to modify the probe settings for the link as needed.



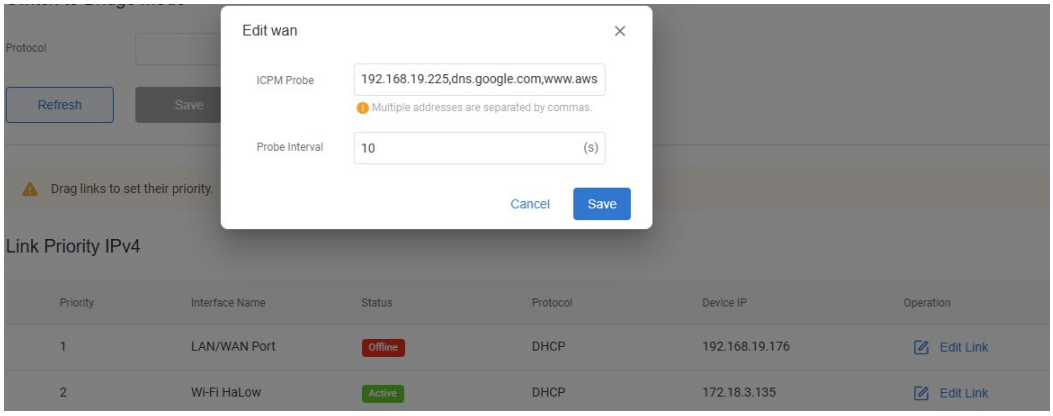
3.3.1.4 Link Diagnosis

When a link status shows **Offline**, first confirm that the interface is connected to the upstream network. After physical connectivity is validated, run a reachability test by configuring an ICMP probe target (e.g., the gateway IP or a public DNS such as 8.8.8.8) for that link.

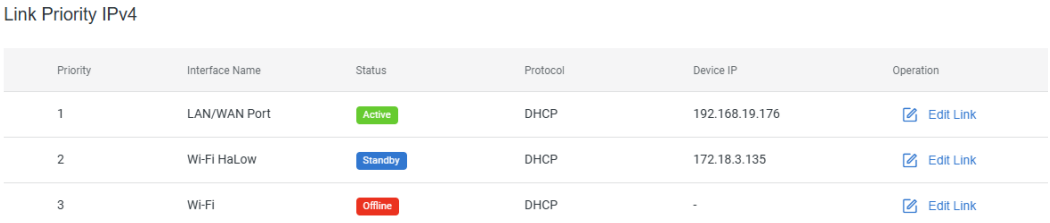
1. Locate the target link, and click **Edit Link**.



2. Enter valid IP addresses or domain names as the ICMP probe targets in the configuration menu and set the probe interval. Multiple entries are supported and separated by commas.



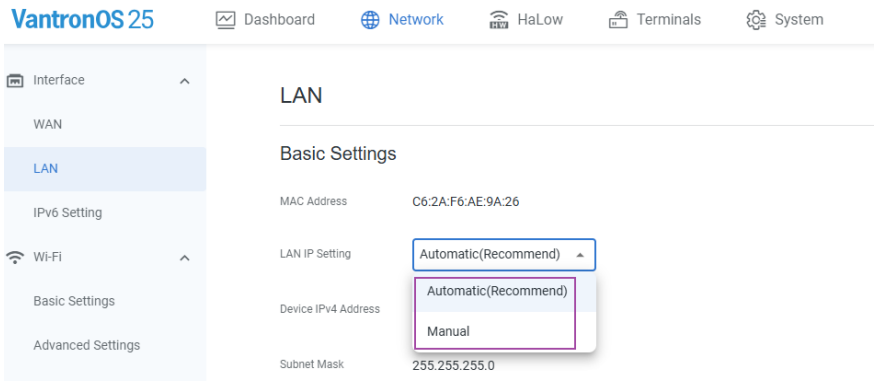
3. Check the link status to verify if it becomes reachable.



If the link still shows offline, verify the physical connection and network connectivity.

3.3.2 LAN Interface

The HAP202 defaults to the 172.18.1.1 subnet for IP assignment. This IP address can be adjusted manually to avoid IP address conflicts and subsequent network anomalies.



3.3.2.1 Subnet Conflict

A subnet conflict may occur when a Vantron communication device (router/gateway/HaLow AP/mesh MPP) acts as a DHCP server for the HAP202's uplink interface, and its factory LAN address (172.18.1.1) overlaps with the HAP202's default LAN subnet.

As a best practice, we recommend reconfiguring the HAP202'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. Enabling or disabling DHCP Service takes effect after the changes are saved.

Editable fields under **DHCP Service**:

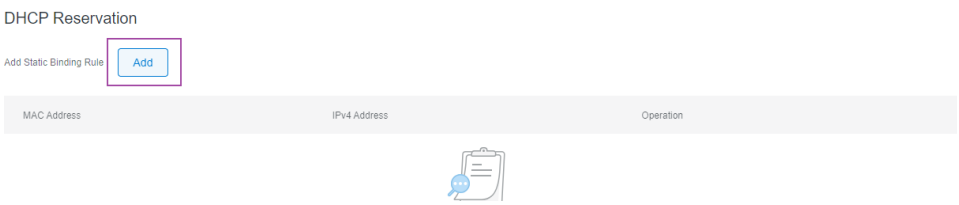
- Start & End addresses: IP addresses within this range are leased to clients.
- Lease Time: The valid duration for which the HAP202, as the DHCP server, assigns an IP address to a client. Before expiry of the lease time, the client will send a renewal request to the HAP202 to extend the lease. If the 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.

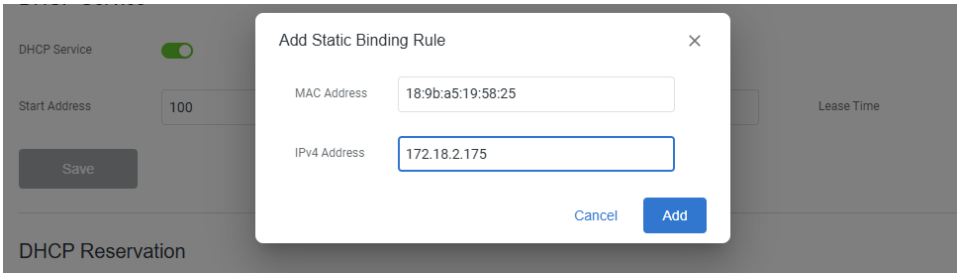
By adding a DHCP reservation rule to the HAP202, the specified client device will maintain the allocated IP address to reduce configuration errors.

Steps of adding a DHCP reservation rule:

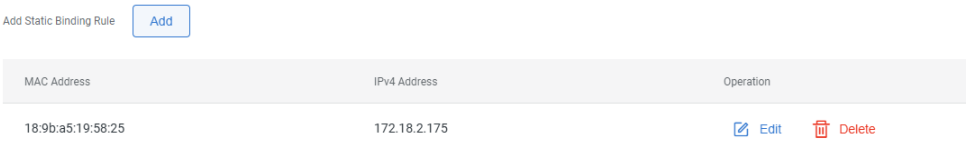
1. After enabling the DHCP service, click **Add** under **DHCP Reservation**.



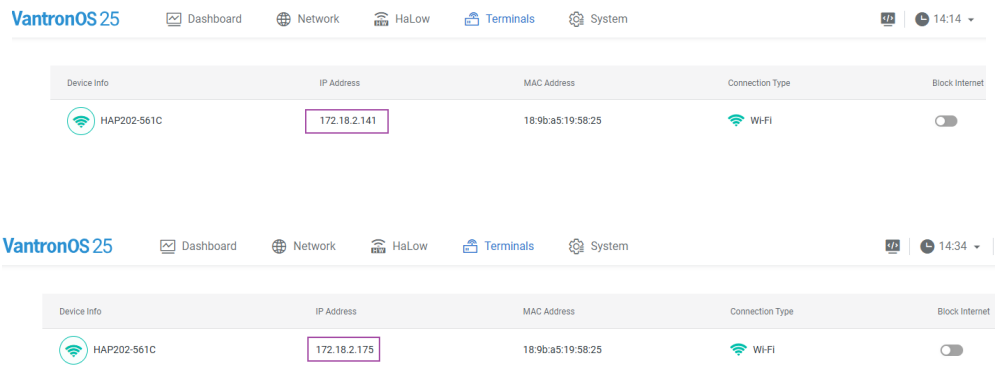
2. Enter the client's MAC address and allocate an IP on the same subnet as the HAP202.



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



4. If you have assigned a fixed IP to the MAC address of a connected device, reconnect the device to the HAP202, and its IP will update accordingly as shown under **Network Topology**.



3.3.3 IPv6 Settings

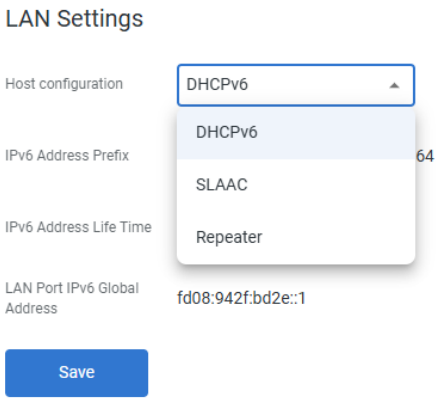
IPv6 (Internet Protocol version 6) is an advanced network layer protocol succeeding IPv4. It is designed to solve IPv4 address exhaustion and support enhanced networking features. It provides 128-bit addresses, eliminating the need for NAT and enabling end-to-end connectivity.

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, using a default IPv6 prefix and address lifetime that can be customized as needed.

The IPv6 options under **LAN Settings** let you further configure the address assignment method.



- **DHCPv6**: The HAP202 acts as a stateful DHCPv6 server, assigning full IPv6 addresses to LAN devices with configurable prefix and lease time.
- **SLAAC:** The HAP202 advertises an IPv6 prefix via RA messages. LAN devices automatically generate their own addresses for plug-and-play use.
- **Repeater:** The HAP202 relays upstream IPv6 configurations transparently. LAN devices obtain addresses directly from the upstream network, with no local address assignment.

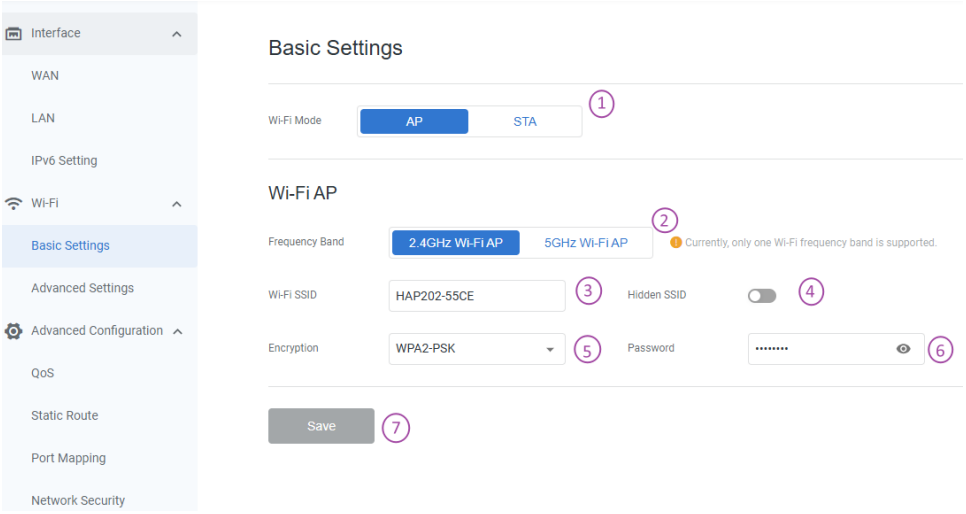
3.3.4 Wi-Fi

During the initial login wizard, the device's 2.4 GHz Wi-Fi/5 GHz Wi-Fi is pre-configured as an access point (AP), and these configurations are retained. 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.

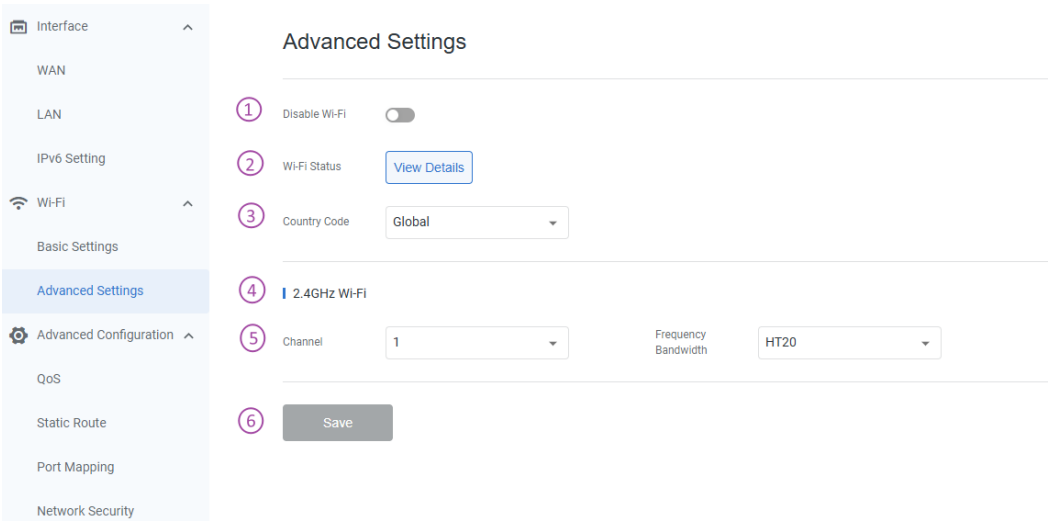
3.3.4.1 AP-Mode Basic Settings



Description:

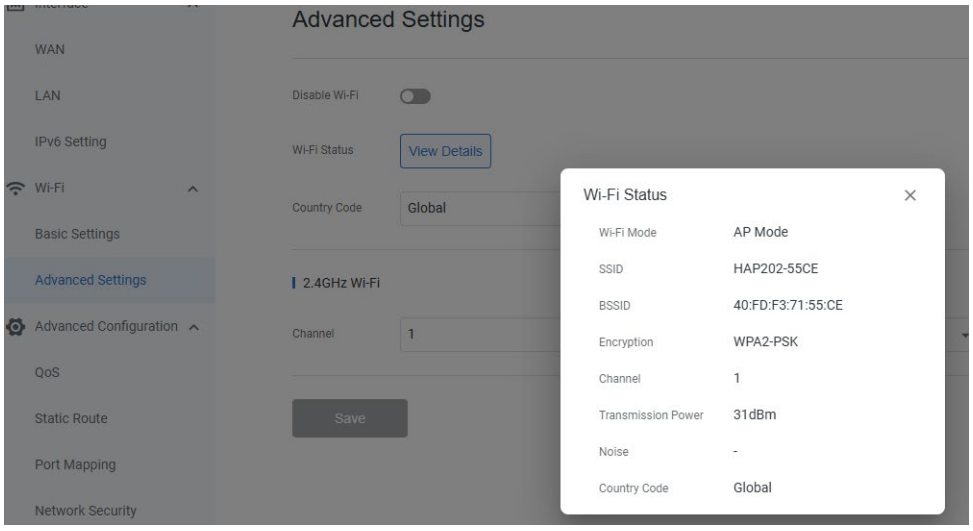
1. The device is factory set to operate in **AP** mode, and you can switch the mode here.
2. Both 2.4 GHz and 5 GHz frequency bands can be configured, but only the blue-highlighted tab represents the currently active band.
3. Wi-Fi SSID—The Wi-Fi AP's name.
4. Hide SSID—Once hidden, clients cannot scan 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, WPA2-EAP)
6. Password—Credential for connecting the device's Wi-Fi.
7. Click **Save** to allow changes to take effect.

3.3.4.2 AP-Mode Advanced Settings



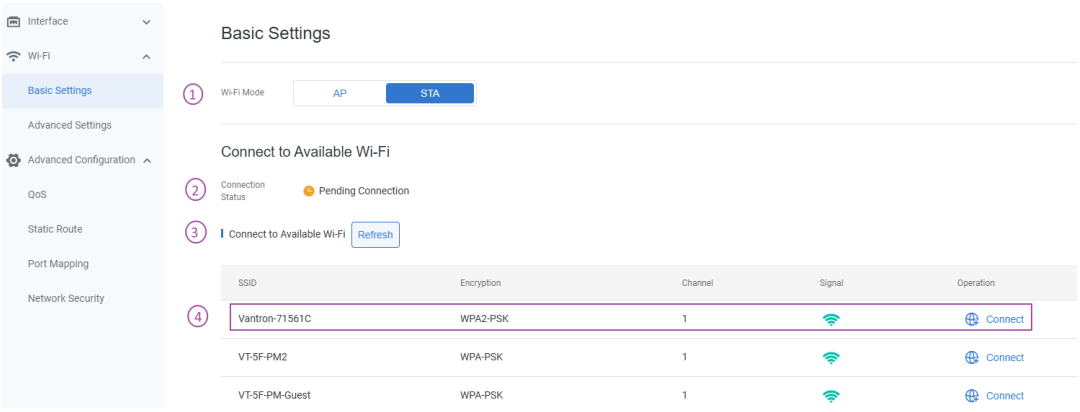
Description:

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 mode, channel, transmit power.



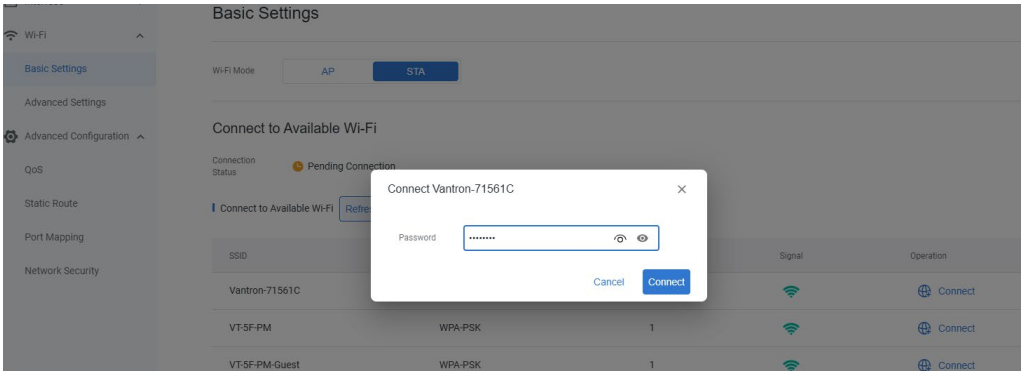
3. Country code (‘global’ by default).
4. The currently active band matches the selection in the basic settings.
5. Channel options (configurable) and default frequency bandwidth.
6. If you have modified the parameters, click **Save** to apply.

3.3.4.3 Client-Mode Basic Settings

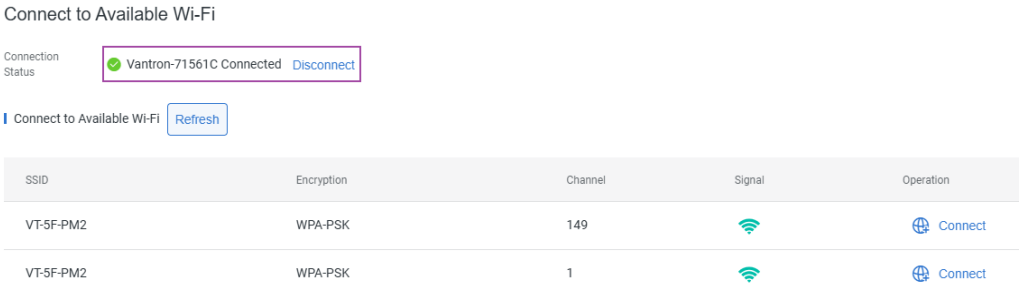


Description:

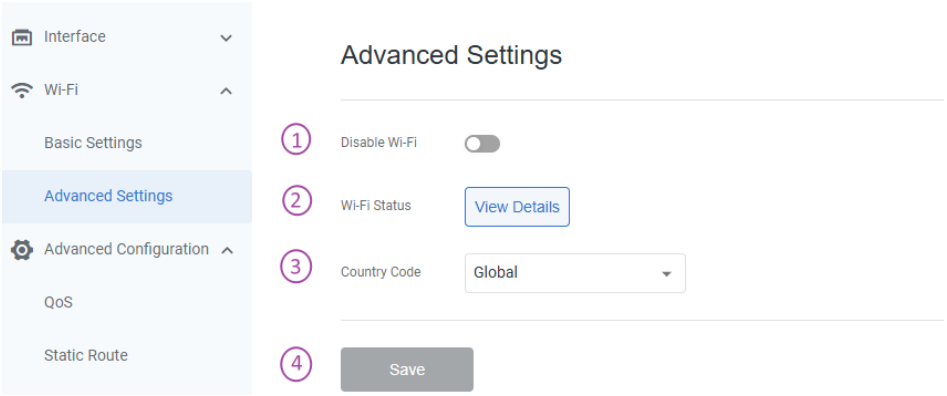
1. Current Wi-Fi mode is displayed in dark blue, and you can switch the mode here.
2. Current Wi-Fi connection status.
3. If the target SSID is not included in the list, click the button to refresh the list.
4. Information of available Wi-Fi APs is displayed. Click **Connect** and enter the password to connect to the target AP.



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

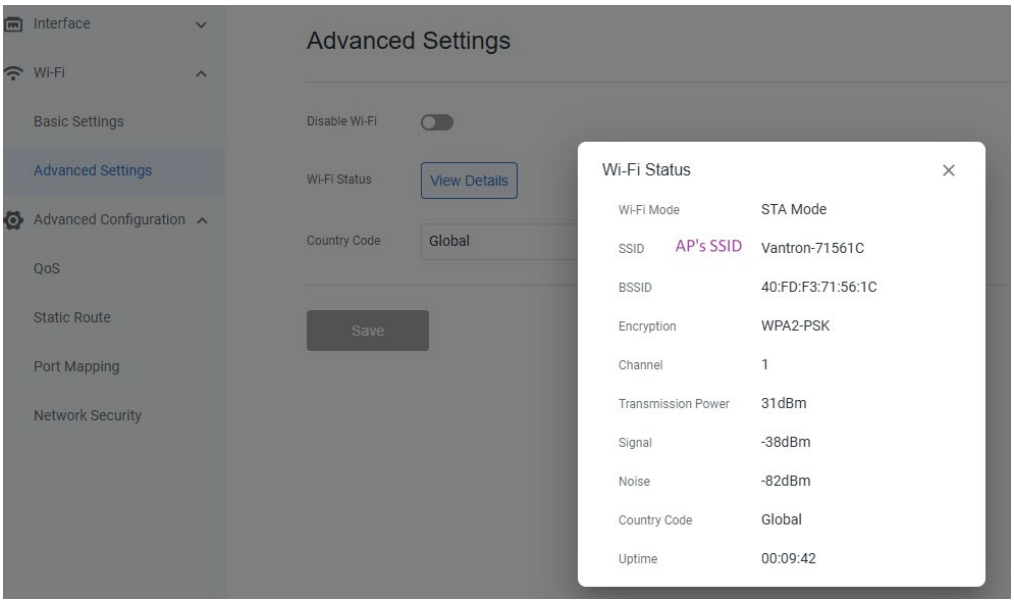


3.3.4.4 Client-Mode Advanced Settings



Description:

1. Disable/Enable the Wi-Fi feature.
2. Wi-Fi Status—Clicking **View Details** displays 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.



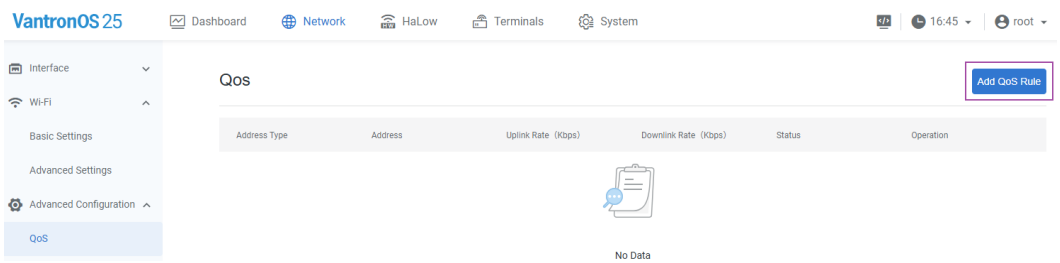
3. Country code (‘global’ by default).
4. If you have modified the parameters, click **Save** to apply.

3.3.5 QoS Bandwidth Control

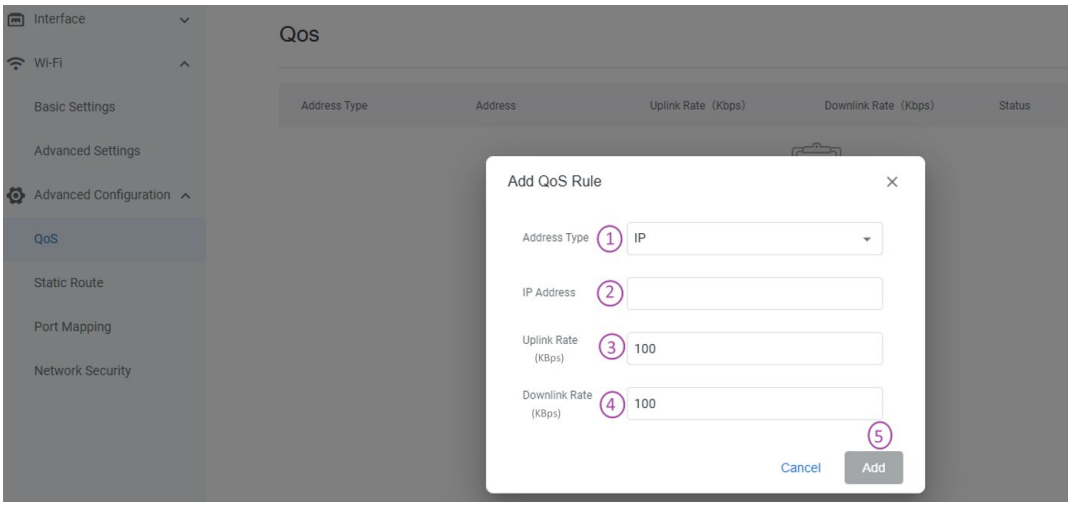
The QoS feature provides fine-grained bandwidth shaping rules to limit uplink and downlink traffic of designated terminals, preventing bandwidth preemption and stabilizing industrial communication quality.

Follow the steps below to create a QoS rule:

1. Navigate to **Network > Advanced Configuration > QoS,** and click **Add QoS Rule**.



2. On the configuration page, set up the rule:



Description:

1) Select the address type (IP, IP range, MAC).

2) Fill in the corresponding parameters.

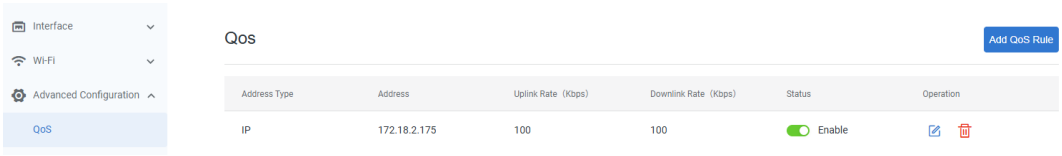
- **IP:** Apply rate limits to a single specified IPv4 device. This option is ideal for precise bandwidth control of key equipment such as PLCs and industrial controllers.
- **IP Range:** Restrict traffic for a continuous IP address range, enabling batch bandwidth control for groups of sensors or surveillance cameras.
- **MAC:** Restrict device traffic by MAC addresses.

3) Specify the maximum uplink bandwidth in KBps.

4) Specify the maximum downlink bandwidth in KBps.

5) Click **Add** to save the configuration.

3. Newly created QoS rules are enabled by default. You can further edit or delete the rule as needed.



3.3.6 Static Route

Static routing is a manual network configuration method where administrators explicitly define the path for traffic destined to a specific network, along with the outbound interface and next-hop gateway. It provides precise, deterministic control over where traffic is sent, making it useful for traffic segregation, directing specific subnets to a preferred link, and building multi-WAN or backup-link setups.

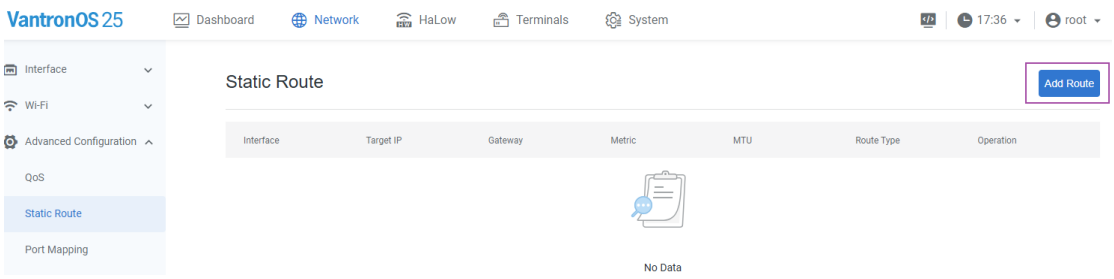
Example:

Goal: Allow HaLow stations on the HAP202's LAN side (172.18.1.0/24) to reach an internal server (192.168.0.0/16) located behind the upstream router.

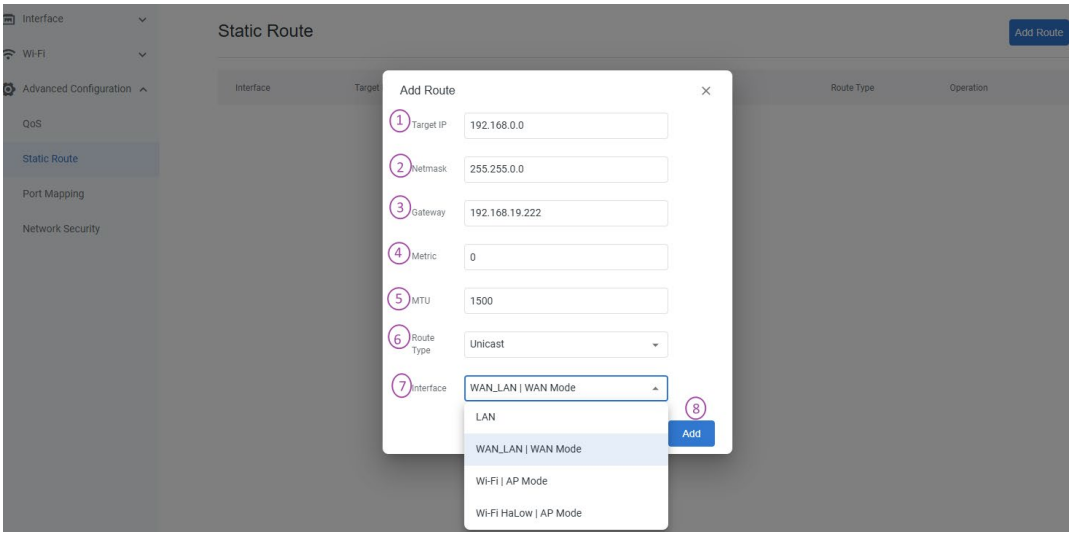
Topology: HaLow Stations (172.18.1.x) -> HaLow AP (LAN: 172.18.1.1, WAN: 192.168.19.176) -> Upstream router (Gateway: 192.168.19.222) -> internal network server (192.168.0.0/16).

Steps:

1. Ensure DHCP is enabled on the Ethernet WAN port and Ethernet WAN is set as the primary link.
2. Navigate to **Network > Advanced Configuration > Static Route**.
3. Click **Add Route** to create a routing rule.



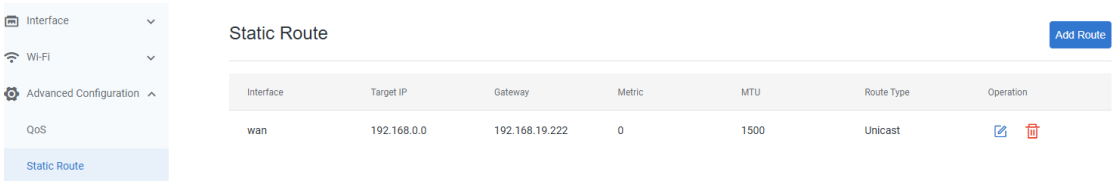
4. Configure the parameters for the route:



Description:

1) Enter the destination network address.
2) Enter the subnet mask (e.g., 255.255.0.0 = /16 = 192.168.0.0 - 192.168.255.255).
3) Enter the next-hop gateway address (the gateway on the selected outbound link, 192.168.19.222 in this example).
4) Set the route metric (default: 0; lower value = higher priority).
5) Set the MTU (default: 1500; adjust only if required by the upstream link).
6) Select a route type (refer to the table below).
7) Select an outbound interface (the interface that reaches the next-hop gateway).
8) Click **Add** to save the configuration.

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



6. Verify connectivity from a HaLow STA: ping 192.168.0.1.

*A **return route** is also required on the upstream router. Otherwise, requests can reach the internal server, but reply traffic cannot route back to the HaLow stations.*

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.

3.3.7 Port 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:

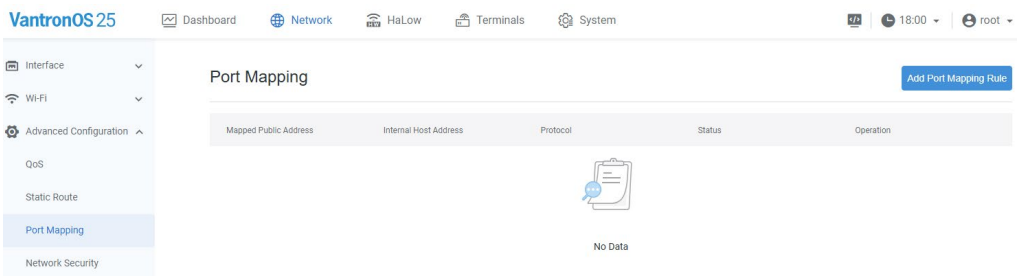
Scenario:

- The HAP202 has both an internal zone (e.g., HaLow 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.

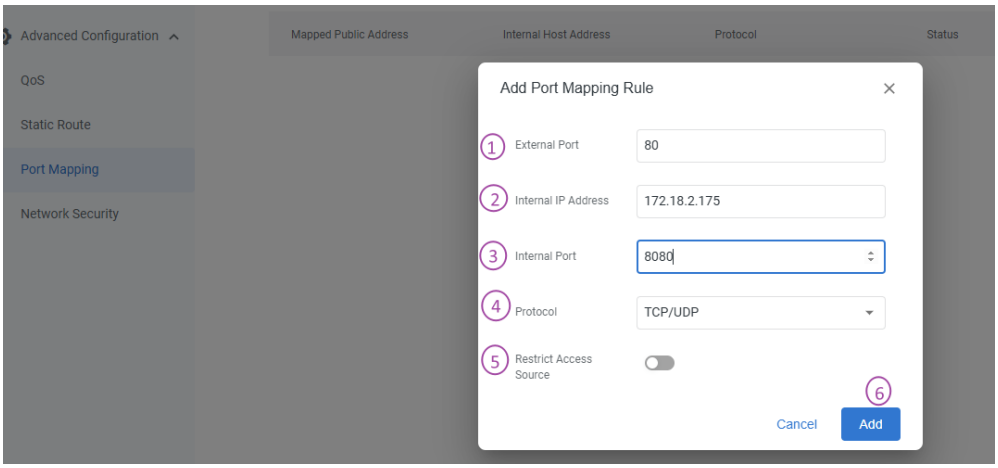
Goal:

Allow external users to access the internal service (on port 8080) by connecting to the WAN IP (on port 80).

1. Navigate to **Network > Advanced Configuration > Port Mapping**.



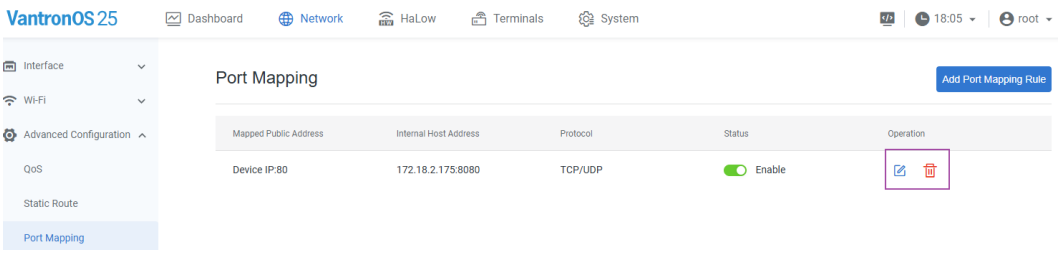
2. Click **Add Port Mapping Rule** in the upper right side.
3. Fill in the rule information.



Description:

1) External port – The port number on the WAN side that outsiders will use to connect (e.g., 80).
2) Internal IP Address – 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.

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



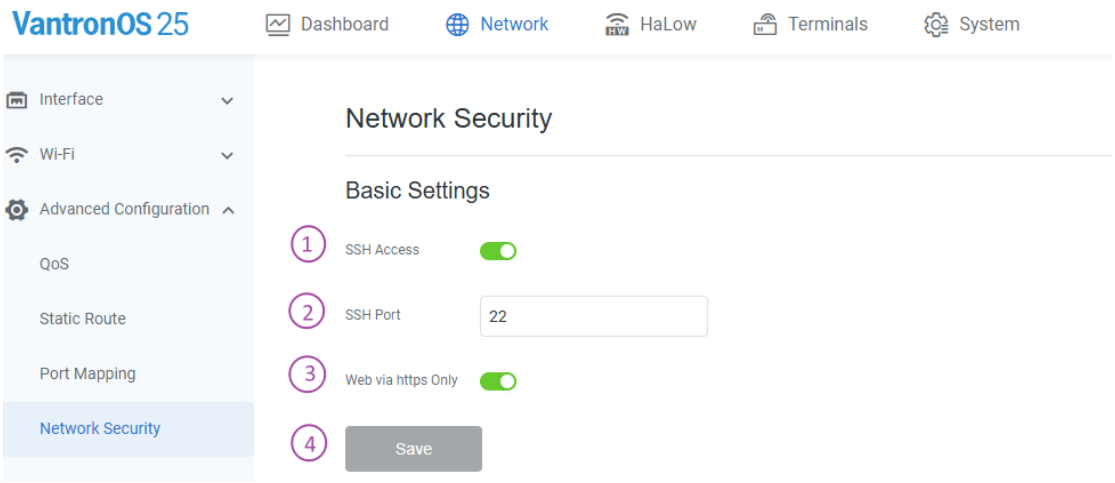
The mapped public address is determined by your WAN connection and may change.

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

3.3.8 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.

3.3.8.1 Basic SSH Access Setup



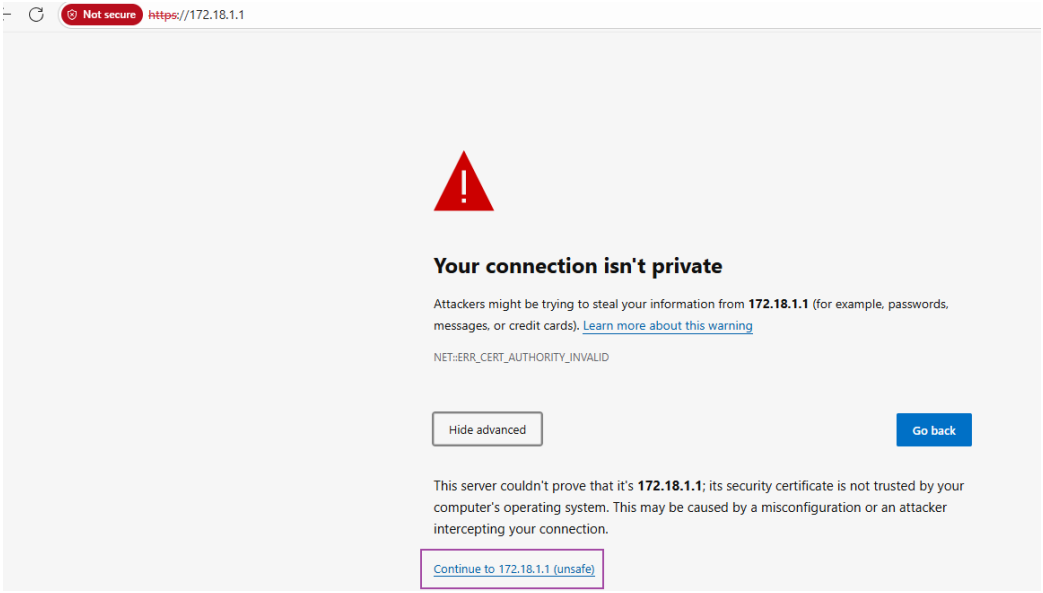
Description:

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

   Refer to 2.7 for the login method.

2. Default SSH port is 22.

3. Web via HTTPS Only — VantronOS accepts logins only over HTTPS. When visiting the HTTPS web UI, a browser privacy warning may pop up. In this case, click **Advanced** → **Continue** to proceed.



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

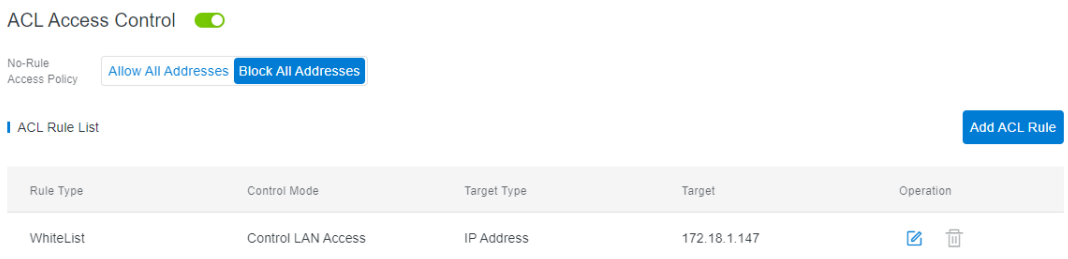
3.3.8.2 ACL Access Control

The device's access control uses a default base policy plus ACL rules when **ACL Access Control** is enabled.

- **No-Rule Access Policy**

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

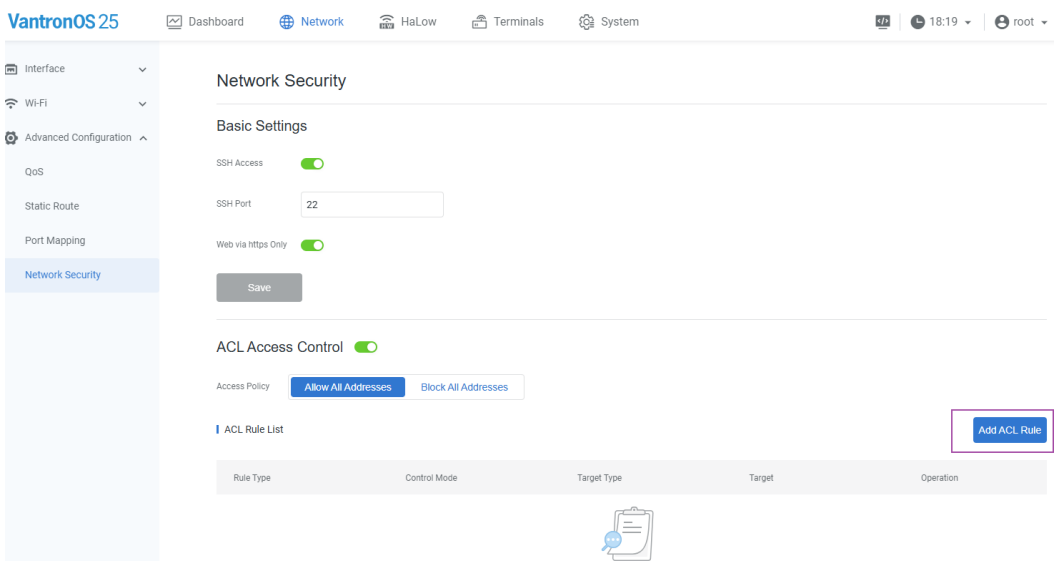
Block all addresses: When enabled, this policy **denies all WAN-side access**—only whitelisted IPs can reach the device—and **prevents** LAN-side devices from using the device to **reach the WAN**. If no whitelist rules exist at activation, the device automatically adds the host computer's current IP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



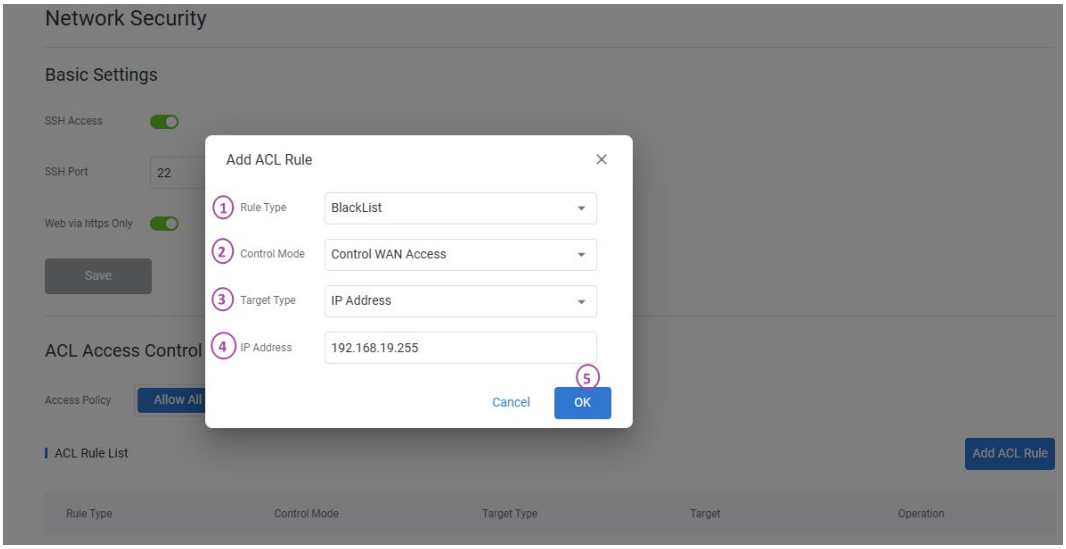
- **ACL Rule List**

To add an ACL rule:

1. 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.

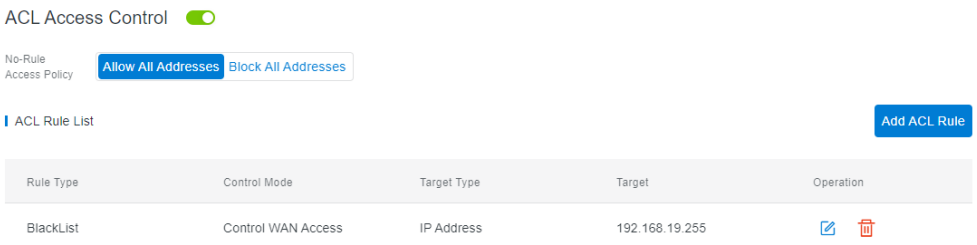
5) Click **OK** to complete.

Description for the rule settings:

Rule Type	Control Mode	Target Type	Result
Whitelist	WAN	IP address (Source)	The designated WAN IP has access to HAP202 or its LAN devices.
		Destination IP/ URL/URL keyword	HAP202 or its LAN devices has access to the designated WAN IP/URL/URL keyword.
	LAN	IP/MAC/OUI	The designated LAN devices are allowed to access the WAN domain.
Blacklist	WAN	IP address (Source)	The designated WAN IP is blocked from accessing HAP202 or its LAN devices.
		Destination IP/ URL/URL keyword	HAP202 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.



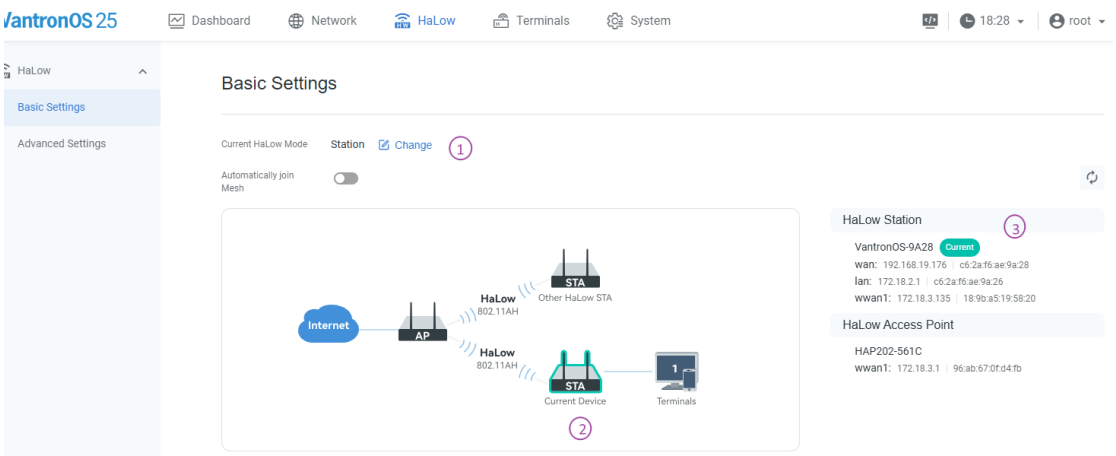
3.4 HaLow

Wi-Fi HaLow related settings are configured on the **HaLow** page.

The device's Wi-Fi HaLow is pre-configured as a station (STA) for a standard HaLow connection. Users can modify the configurations as needed.

3.4.1 Overview

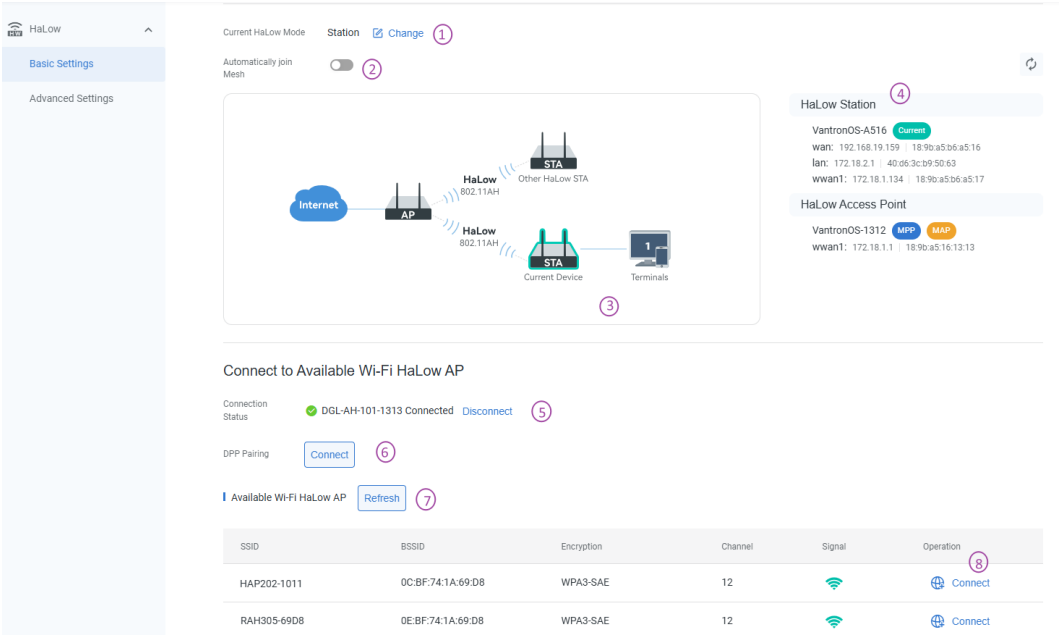
Under **Basic Settings**, a topology is displayed, indicating the role of the current device. If a HaLow network is established, brief information of the connection will display next to the topology.



Description:

1. Click to change HaLow operation mode.
   - Access Point (AP): Broadcasts the HaLow network for stations to connect to.
   - Station (STA): Connects to an existing Wi-Fi HaLow AP.
2. Network topology: Displays the layout of the current HaLow network connections. The local device is highlighted with a **cyan** outline.
3. Device Information: Shows brief connection information for the current device in the topology. Clicking the sync button refreshes the device information.
   - wan: WAN domain IP
   - lan: LAN domain IP
   - wwan0: Wi-Fi STA IP
   - wwan1: HaLow STA IP

3.4.2 STA-Mode Settings



Description:

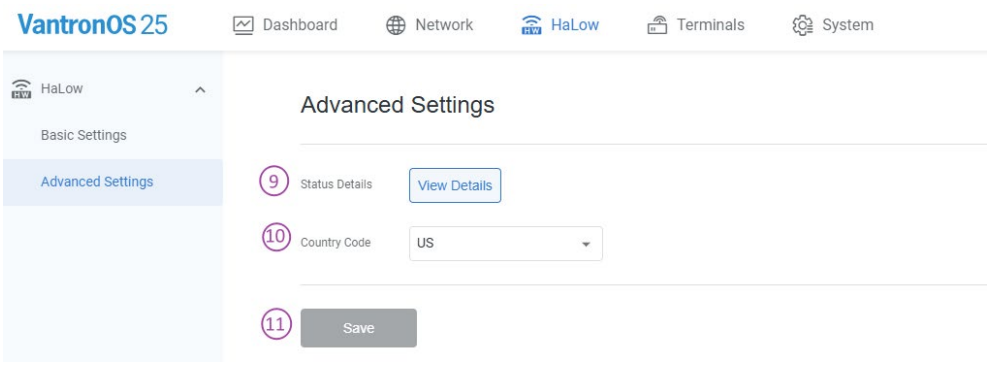
For basic settings

1. Click to change HaLow operation mode (Access Point/Station).
2. When this option is enabled, the HaLow STA automatically joins the mesh network that the connected HaLow AP is in. The STA then operates as an MP and retains the IP address assigned by the AP as its mesh IP, since the connected HaLow AP/MPP is the DHCP server for STAs/MPs within the network.

   The HaLow STA must first connect to the target HaLow AP (over a standard HaLow link) before this option can take effect.
3. Network topology in current HaLow mode. Local device is highlighted with a **cyan** outline.
4. Summary of device connection information: "**Current"** indicates the local device. Clicking the sync icon refreshes the information.

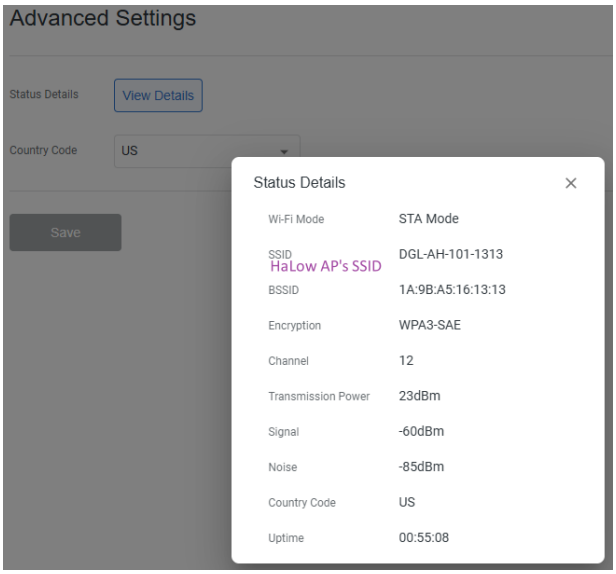
   MPP/MAP role tags on associated HaLow AP indicate mesh settings are enabled on the AP.
5. Connection status:
   - Pending Connection: Not connected to an AP.
   - xxx Disconnect: Connected to the indicated SSID. Clicking **Disconnect** cuts off the link.
   - Connection Failed: Failed to connect to the target AP.
6. DPP pairing: Click **Connect** to initiate a quick HaLow connection. Ensure to press this button after the target AP activates the DPP mode. The time window is 120 seconds. See Section 2.6.2 for instructions.

7. Available Wi-Fi HaLow APs: Detected HaLow SSIDs are listed. Clicking the **Refresh** button reloads the list.
8. To connect/switch connection to a target AP: Click **Connect** next to the target SSID and enter the password in the pop-up.



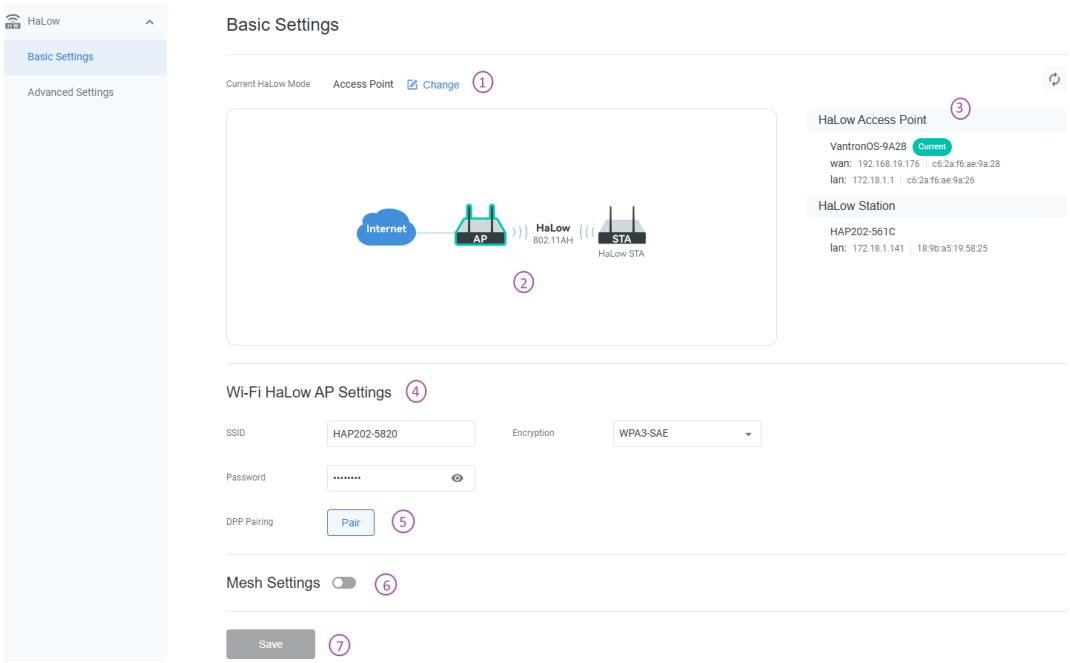
For basic settings

9. Status Details—Clicking **View Details** displays the detailed connection information of the device, including HaLow mode, and—if connected—the SSID of the target HaLow AP, encryption mode, channel, transmit power, etc.



10. Country Code—Select the code based on local radio frequency regulations.
11. Apply the changes by clicking **Save**.

3.4.3 AP-Mode Settings

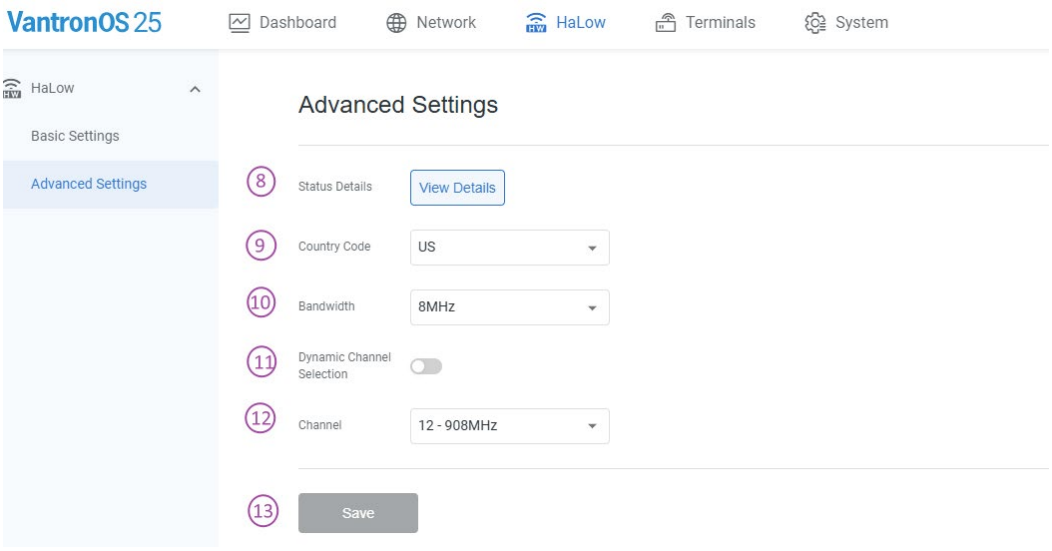


Description:

For basic settings

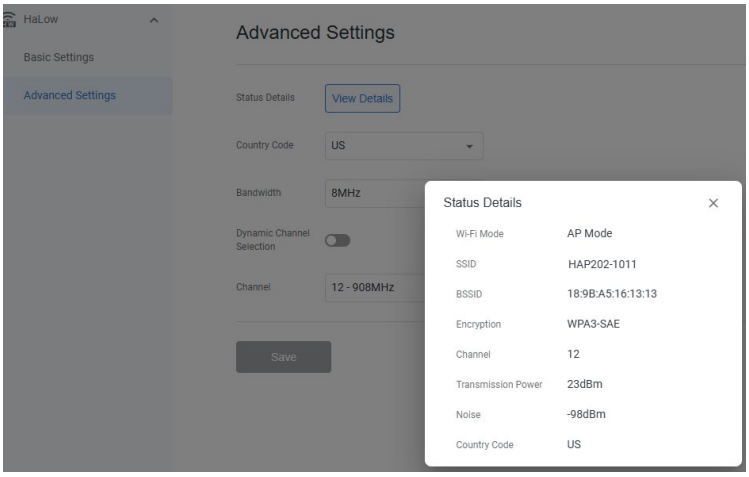
1. Click to change HaLow operation mode (Access Point/Station).
2. Network topology — Displays the layout of the current HaLow network connections. The local device is highlighted with a **cyan** outline.
3. Device Information — Shows brief connection information about the current device within the network topology.
   - “Current” indicates the local device.
   - Clicking the sync button refreshes the information.
4. AP settings — SSID, encryption mode, and password. You can modify these parameters as needed. HaLow STAs adopt these credentials to establish a standard HaLow connection.
5. DPP pairing — Click **Pair** to initiate a quick HaLow connection. The target HaLow STA shall press the button within the 120-second time window for a successful connection. Refer to Section 2.6 for pairing instructions.
6. Enable or disable mesh settings. When enabled, the device functions as both a HaLow AP and a Mesh MPP. Connected STAs retain their originally assigned IP when they join the mesh as MPs.

   All mesh nodes share the same parameters. Modifying mesh settings on the MPP automatically update those settings on connected MPs.
7. Click **Save** to apply the changes.



For advanced settings

8. Status Details—Clicking **View Details** displays the detailed connection information of the device, including HaLow mode, SSID, encryption mode, transmit power, etc.



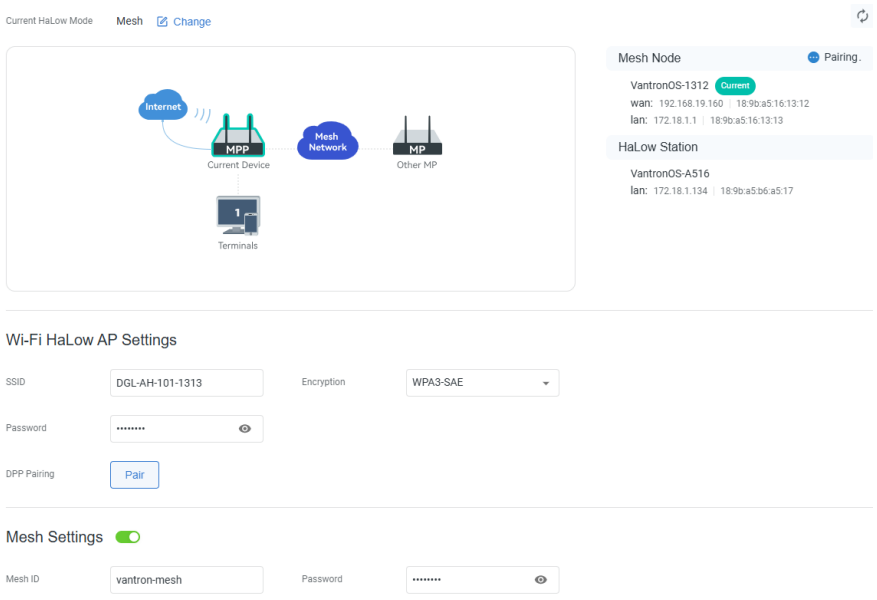
9. Country Code—Select the code based on local radio frequency regulations.
10. Channel bandwidth: A wider bandwidth typically offers higher throughput.
11. DCS: Once enabled, the device will automatically select the channel with the strongest signal within the selected bandwidth for optimal performance.
12. Select an operating channel from the drop-down list.
13. Apply the changes by clicking **Save**.

When the HaLow AP is connected to an external router, all devices on the HaLow link gain internet access.

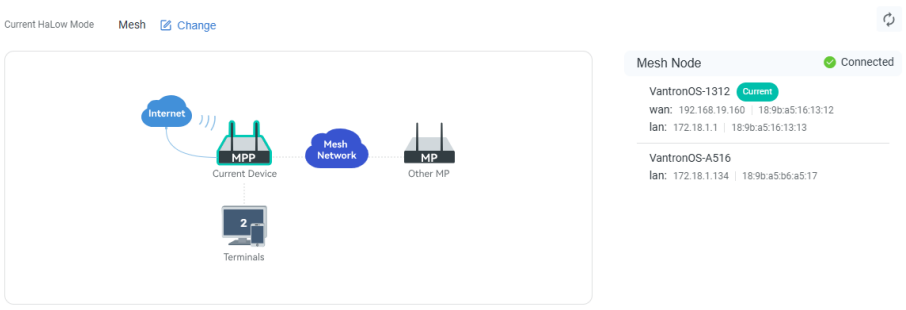
3.4.4 Mesh Networking

Mesh networking extends basic Wi-Fi HaLow connectivity to form a self-organizing multi-node wireless network. As per current design, a HaLow mesh network is built upon a standard Wi-Fi HaLow network.

- For a HaLow AP:
  - When mesh settings are enabled, this device takes on a combined AP+MPP role under Mesh mode, providing standard HaLow access for regular STAs and mesh networking for MPs.
  - The HaLow AP function handles initial association and DHCP IP assignment for STAs on the HaLow link.
  - Associated HaLow STAs with auto-join mesh enabled automatically join the mesh as MPs, retaining their assigned IP for mesh communication.
  - When the HaLow AP/MPP connects to an external router, all devices on the network gain internet access.

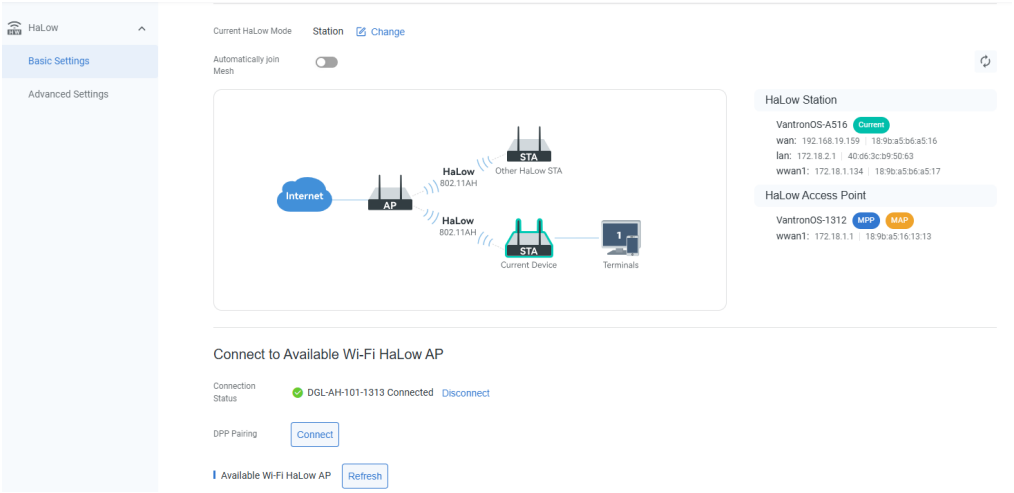


(Mesh settings enabled)

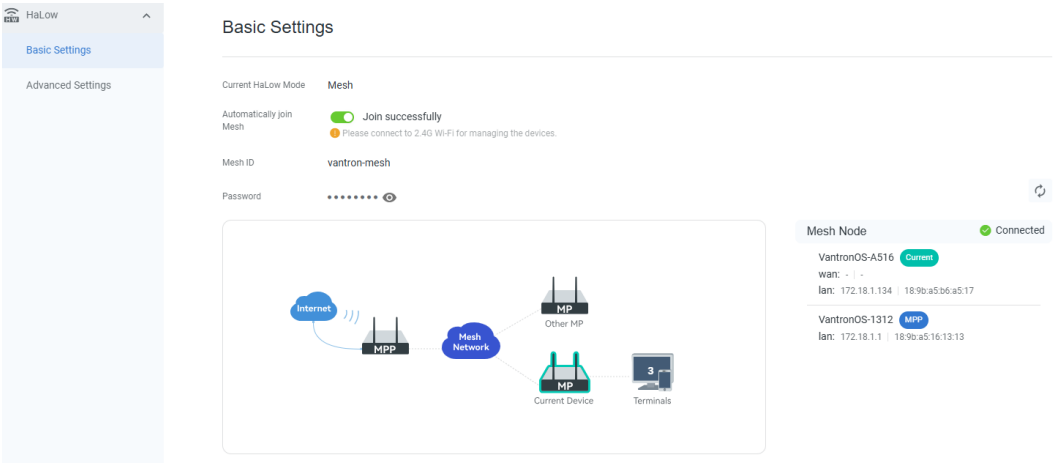


(MPs joined the mesh)

- For HaLow STAs:
  - HaLow STAs must first associate with a HaLow AP over the HaLow link.
  - When auto-join mesh is enabled, they automatically join the mesh as MPs, retaining the HaLow IP assigned by the AP for mesh traffic. If auto-join mesh remains disabled, the STAs stay as regular HaLow STAs and do not participate in mesh operations.
  - When the associated HaLow AP/MPP connects to an external router, the STAs/MPs gain internet access.
  - After joining the mesh, the STA's Ethernet and Wi-Fi interfaces are **automatically bridged**. Management access is available via Ethernet or Wi-Fi using the previously assigned HaLow IP.



(Connected to an AP with mesh settings enabled)



(Successfully joined a mesh after auto-join mesh is enabled)

To quickly exit a mesh network and switch to non-mesh HaLow operating mode, click Change on the Basic Settings page. On exiting the mesh, the STA's Ethernet and Wi-Fi interfaces are no longer bridged, and the Wi-Fi reverts to AP mode.

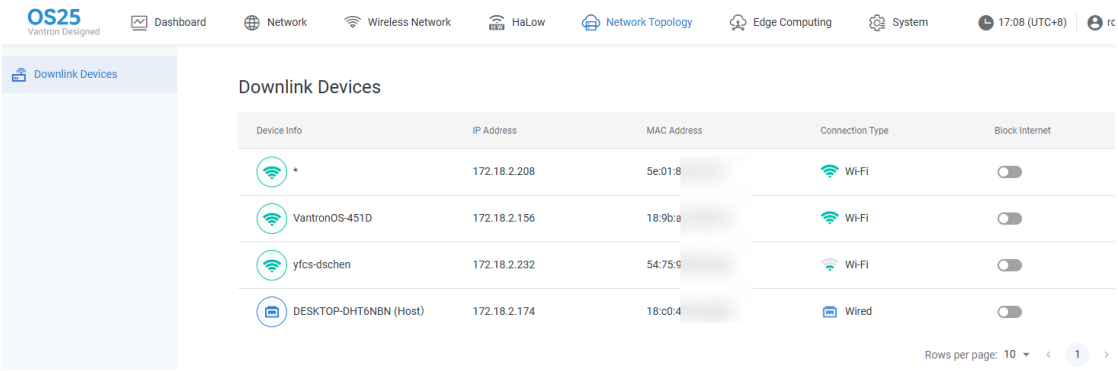
3.5 Terminals

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.

2.4 GHz/5 GHz Wi-Fi and Wi-Fi HaLow connections are both classified to the **Wi-Fi** Connection Type.

Users can manage internet access of these client devices by enabling the **Block Internet** option.

A DHCP reservation for a specified device (identified by its MAC address) also appears on this page when the device is connected. Refer to Section 3.3.2.2 for details on DHCP reservation.



3.6 System

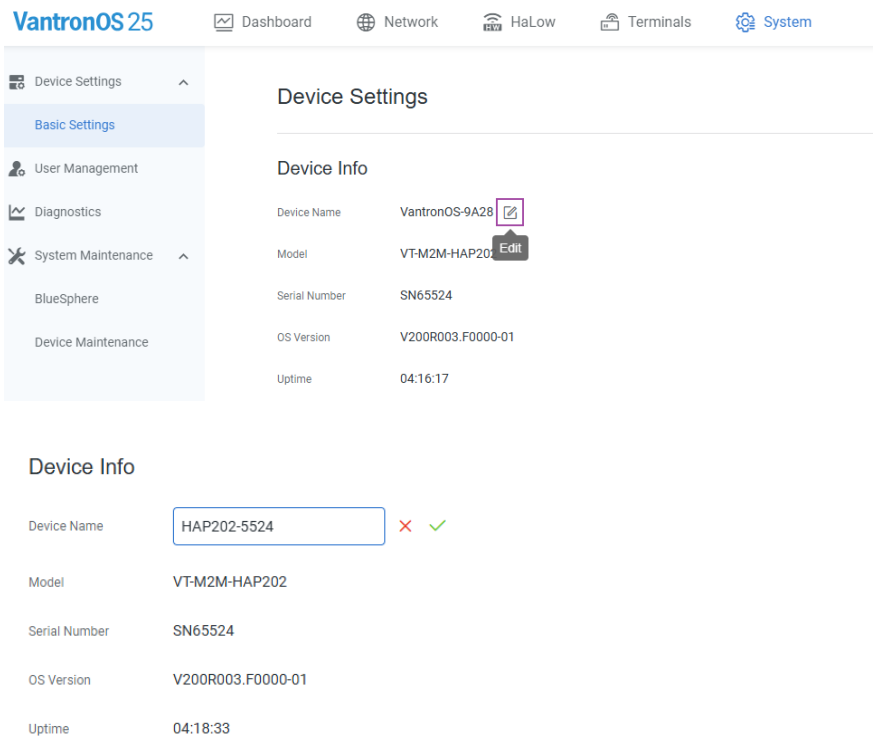
Under **System**, users can view and edit all system-level settings.

3.6.1 Device Settings

Device settings comprise basic device information and its time settings.

3.6.1.1 Modifying Device Name

Device Info displays core information—device name, model, serial number, system version, and uptime.

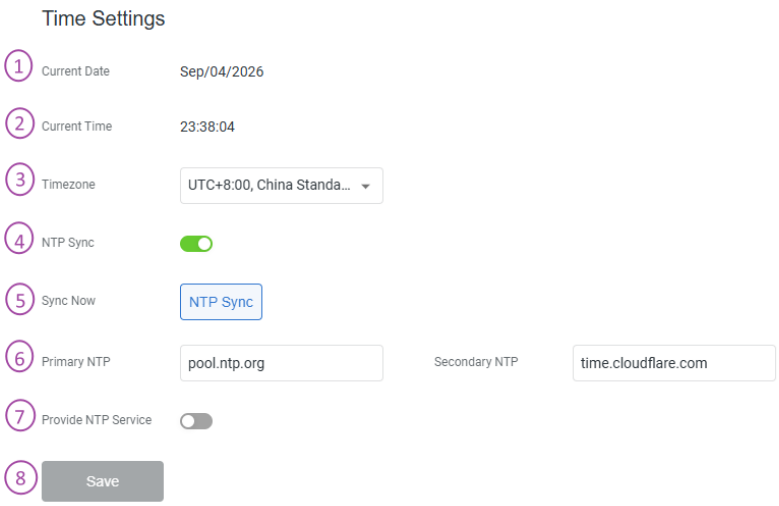


To modify the device name:

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

3.6.1.2 System Time

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

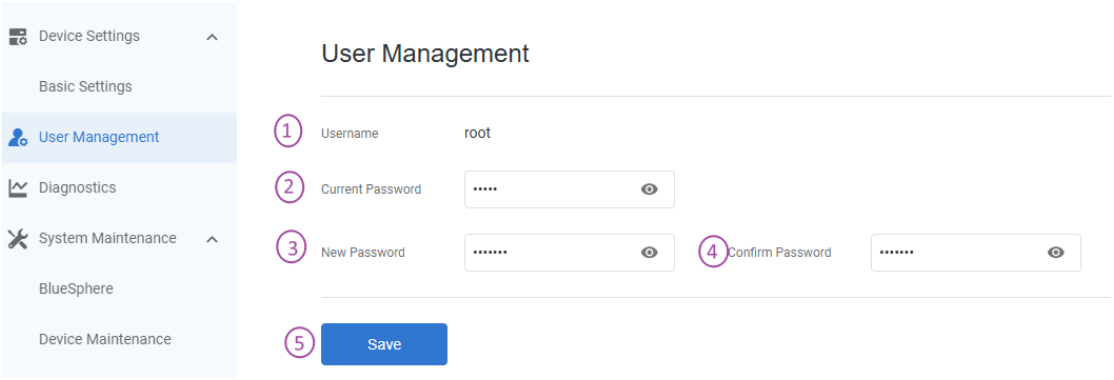


Description:

1. Current Date — Displays today's date for the selected time zone.
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 following options can be configured only when this feature is enabled.
5. Sync Now — Triggers a one-time NTP update immediately. The date resets after every power cycle because the HAP202 lacks an RTC.
6. Primary NTP — Preferred NTP server; Secondary NTP—Backup NTP server.
7. Provide NTP Service — Enables/Disables the HAP202 to act as an NTP server for LAN devices.
8. If you have made any changes, click **Save** to apply.

3.6.2 User Management

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



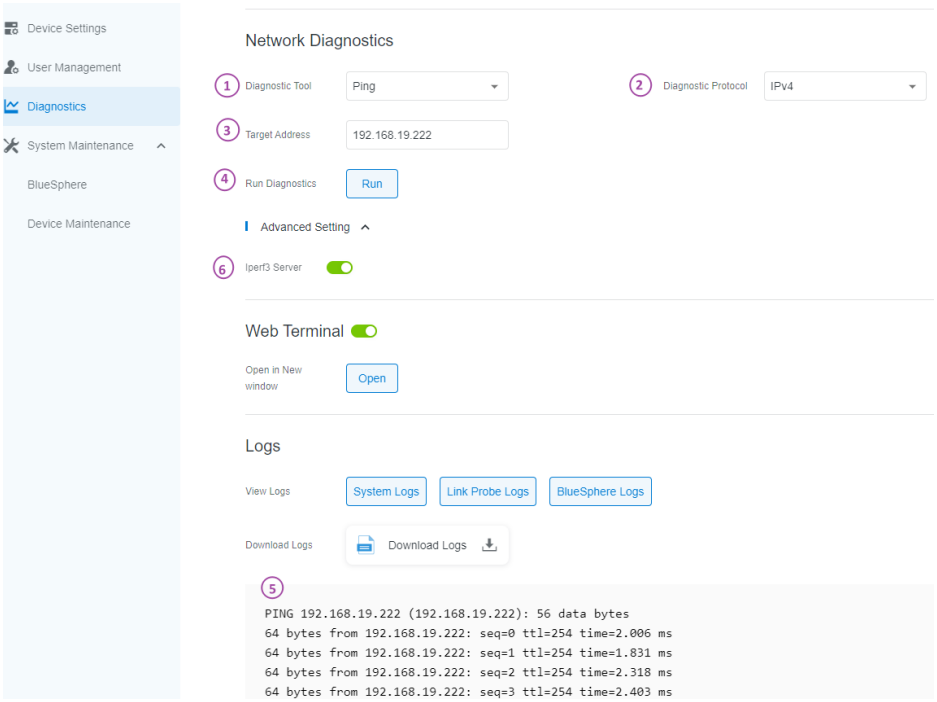
Description (Fields 2–5 for password modification):

1. Current user.
2. Enter the current password.
3. Enter a new password.
4. Confirm the new password.
5. Save the change.

3.6.3 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.

3.6.3.1 Network Diagnostics

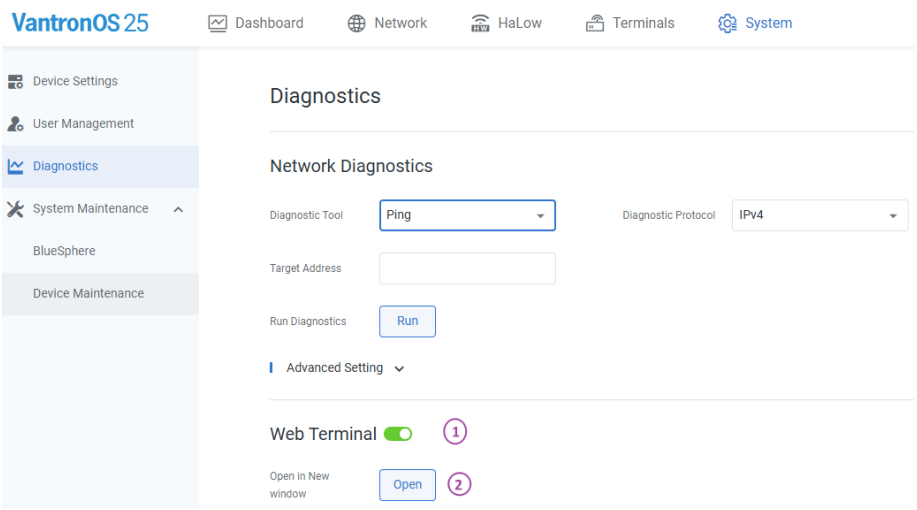


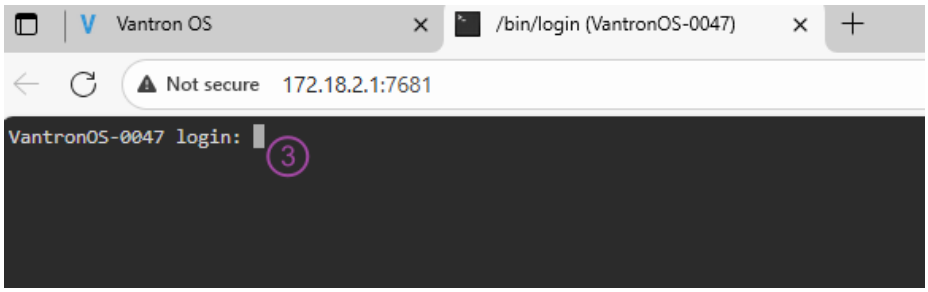
Description:

1. Select a diagnostic tool from the drop-down list (**ping, traceroute, nslookup, iPerf3 client**).
2. For the Ping and Traceroute tools, select either IPv4 or IPv6 as the protocol.
3. Enter the destination IP address or domain name for the test.
4. Initiate a diagnostic test.
5. The test results are displayed correspondingly.
6. The HAP202's iPerf3 server is enabled by default, allowing remote clients to start a throughput test immediately without manual activation.

3.6.3.2 Web Terminal

The **Web Terminal** option allows users to enable the command line interface and access the device shell for debugging.





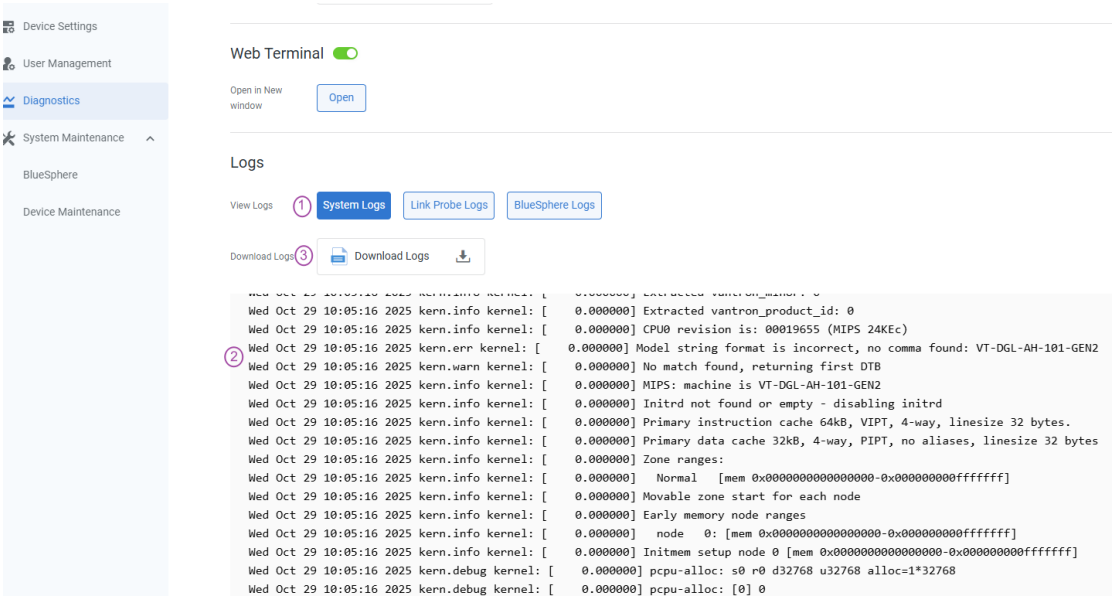
Description:

1. The web terminal option is enabled by default.
2. Click **Open** to launch the device shell in a new window.
3. Log in within the valid session (60 seconds) to debug the device.

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

3.6.3.3 Logs

The system offers different device logs for maintenance or troubleshooting.



Description:

1. Click on a log tab to print the corresponding log (System log, Link probing log, BlueSphere integration log).
2. The live log is displayed.
3. Click the **Download Logs** button to export **all** logs.

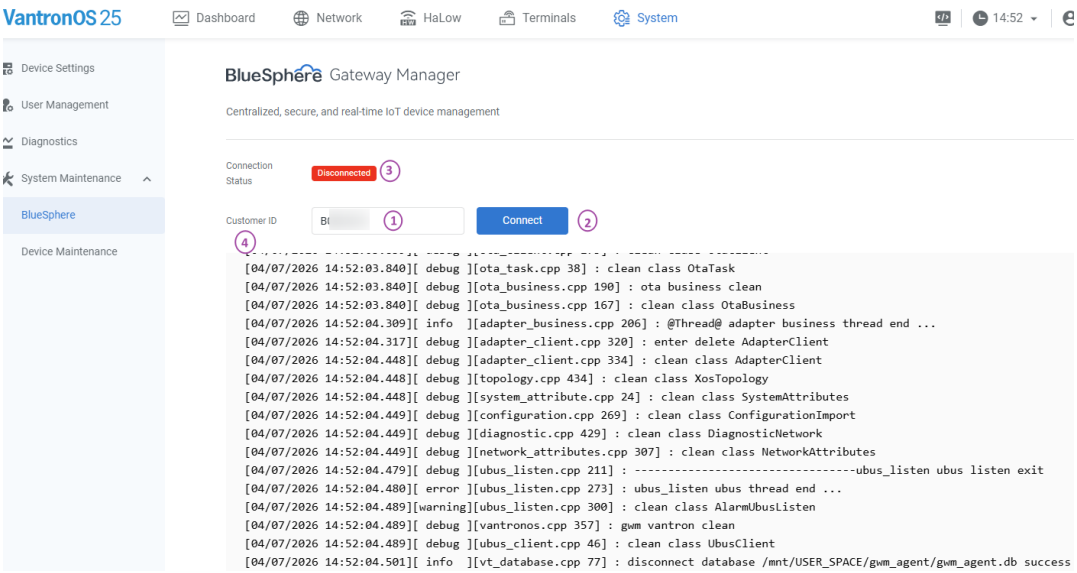
3.6.4 System Maintenance

3.6.4.1 BlueSphere

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

Prerequisites:

- **The HAP202 has internet access.**
- **You have an authorized BlueSphere GWM user account.**



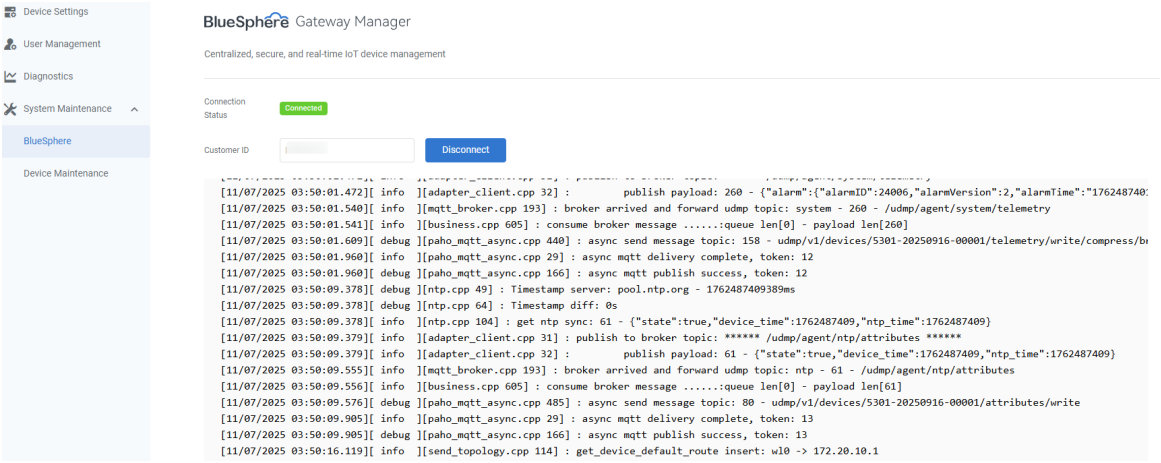
Description:

1. Enter the customer ID that is retrievable in the user profile on your GWM portal.

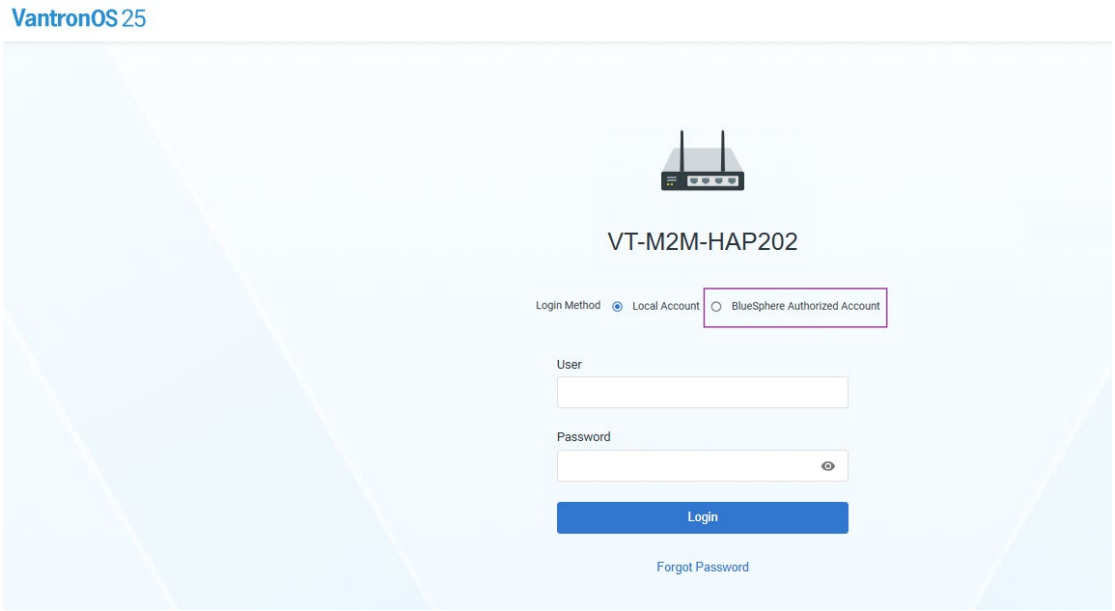
   *If a customer ID is pre-filled, you can click **Disconnect** first and fill in your own.*

2. Click **Connect** to initiate the interfacing between the device and the GWM portal.
3. When the handshake succeeds, the device status changes to **Connected**.
4. The real-time log will display the whole connection process. Check the log for any issues encountered during the process.

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



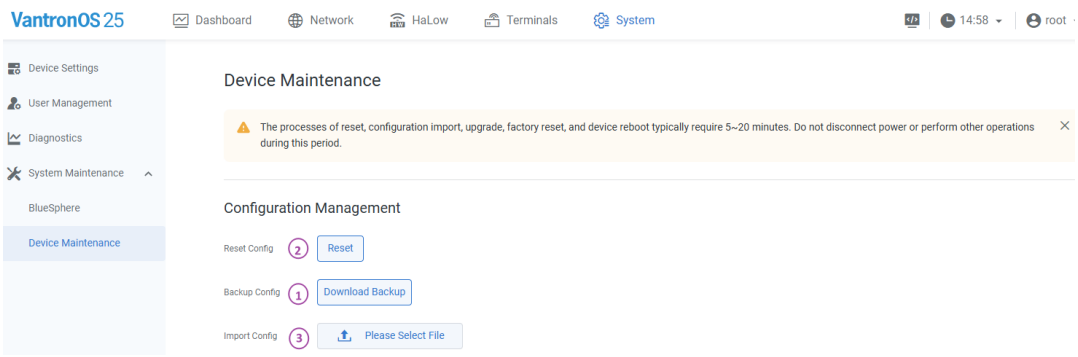
If you log out the portal now, you will find two login methods available. You can sign back in with either your local credentials or your authorized GWM account.



3.6.4.2 Device Maintenance

As indicated on the top of this page, operations including configuration reset, configuration import, upgrade, factory reset, and device reboot typically require **5~20 minutes**. Please stay on the page and **keep the device powered on** until the process finishes.

- Configuration Management

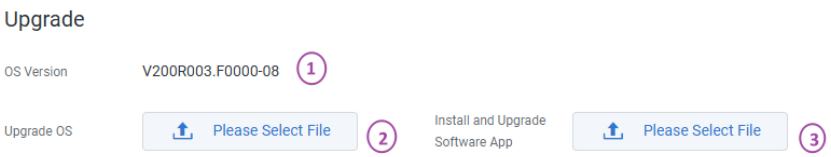


Description:

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 your existing password and follow the setup wizard to finish the first-time configuration.

- Upgrade

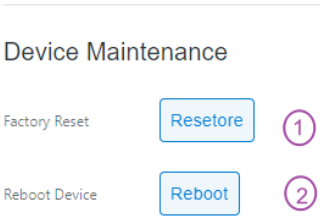


Description:

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 applications, 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:

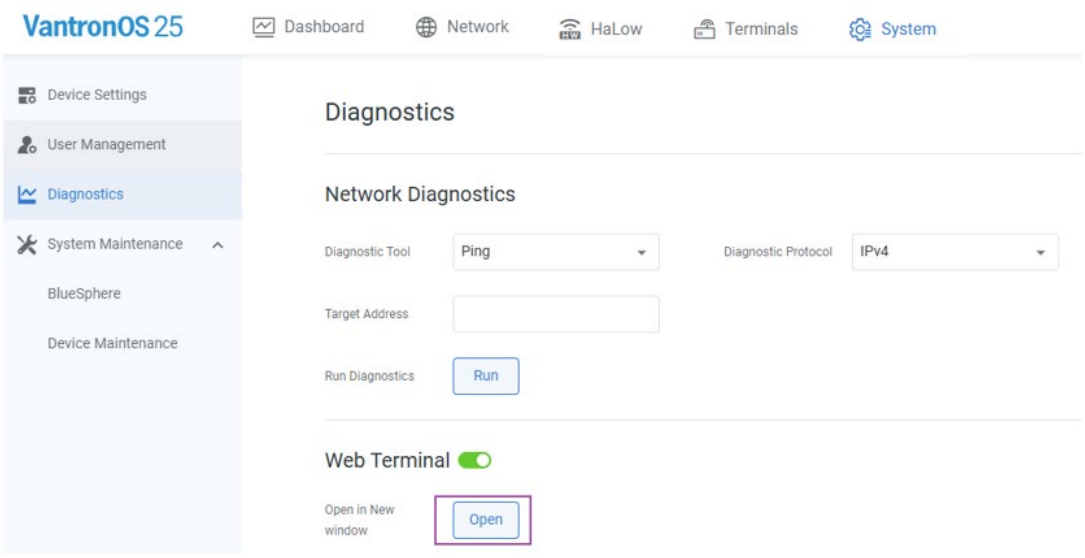
1. Factory reset the device with device configuration, user data and custom applications (including VantronOS 25 APP) cleared.
2. Manually restart the device.

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

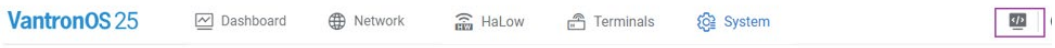
3.7 Command Line Interface

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 3.6.3.2.

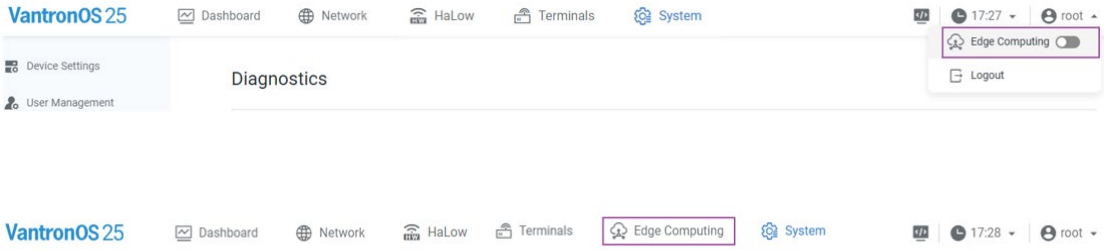


- Click the CLI icon on the menu tab.



3.8 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.



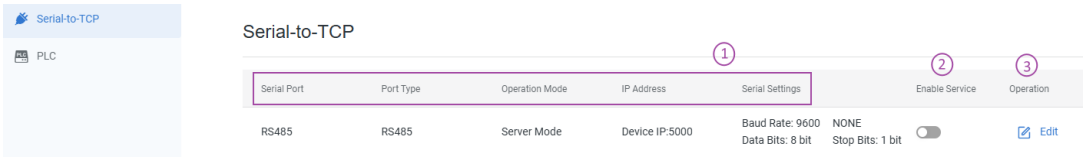
3.8.1 Serial to TCP

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 HAP202 shall match.
- The server's listening port matches the client's target port.
- Both ends use the same protocol (TCP).
- Server and client are mutually IP-reachable.

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

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

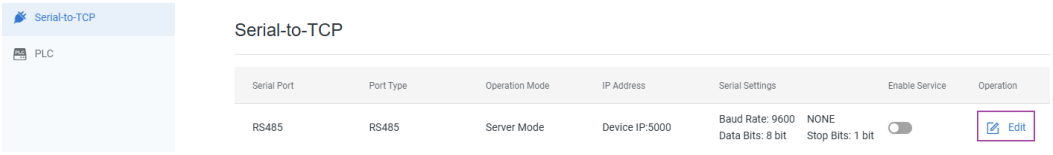


Description:

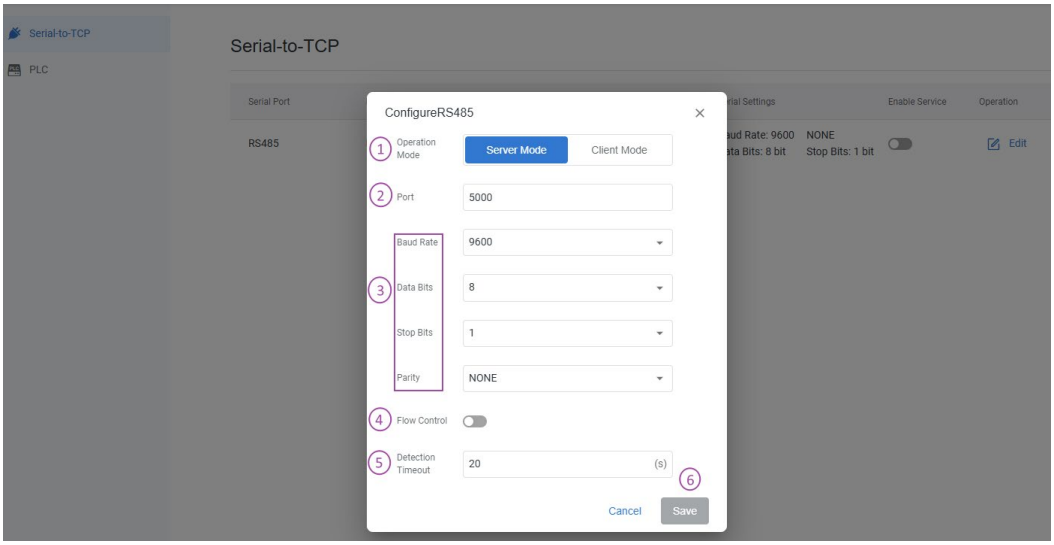
1. Details of the conversion rule, including the serial port name and type, current operation mode, IP address of the device + port, and serial parameters.
2. Enable/disable the rule.
3. Edit the rule.

3.8.1.1 Server Mode Rule Setup

1. Click the edit icon next to the rule.



2. Modify the parameters, ensuring consistency between the server and client on the network, and between the serial peripheral and the HAP202 on the serial link.



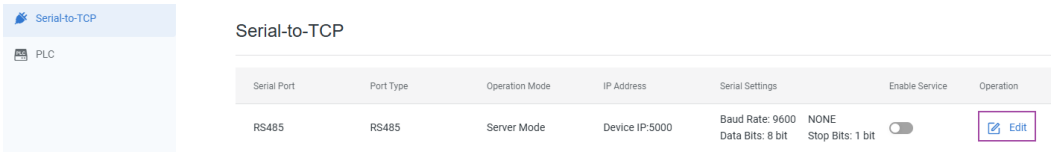
Description:

1) Select **Server Mode.**
2) Designate a TCP port (0~65535) for the server to listen on. The client must connect to the same port.
3) Make sure the serial parameters on both the peripheral and HAP202 are set the same.
4) Enable/Disable software flow control to prevent packet loss (enabling flow control reduces throughput).
5) Set the timeout to automatically drop the connection if no data is received (0=disabled).
6) Save the changes to let them take effect.

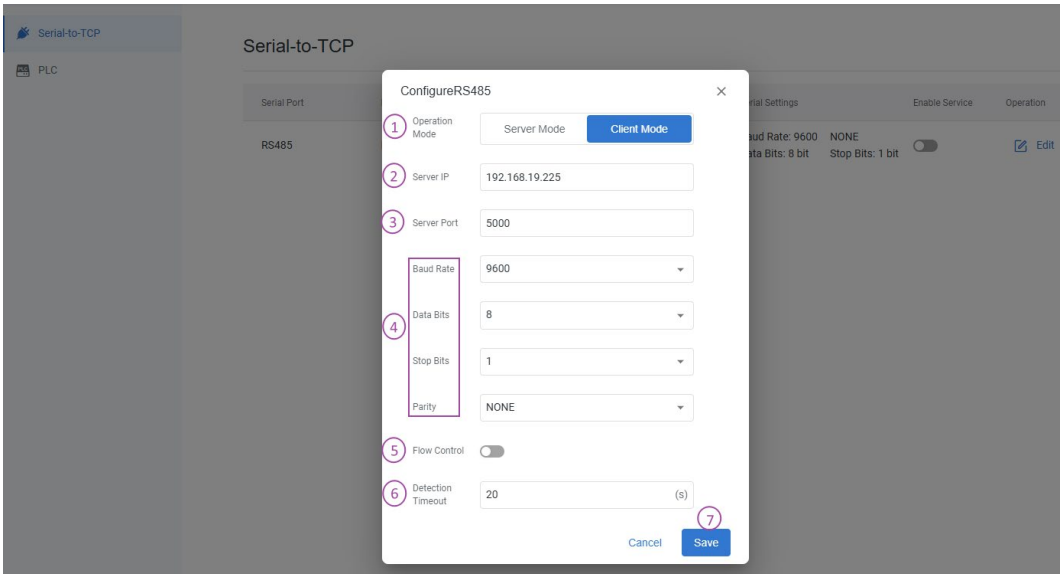
3. Enable the conversion rule after modification.
4. Make sure both the client and server are on the same reachable IP network.
5. Verify the data transmission between the devices.

3.8.1.2 Client Mode Rule Setup

1. Click the edit icon next to the rule.



2. Modify the parameters, ensuring consistency between the server and client on the network, and between the serial peripheral and the HAP202 on the serial link.



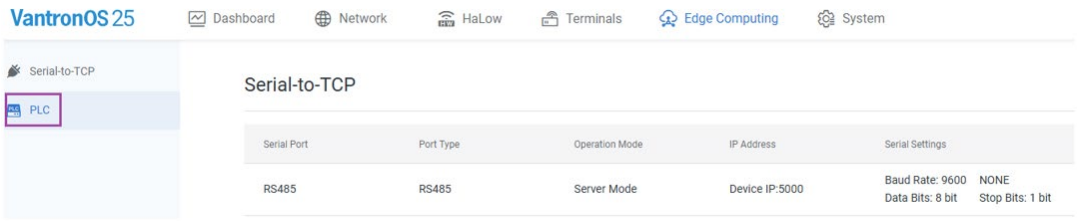
Description:

1) Select **Client Mode.**
2) Enter the server's IP address.
3) Enter the target port and make sure it matches the TCP port on the server.
4) Make sure the serial parameters on both the peripheral and HAP202 are set the same.
5) Enable/Disable software flow control to prevent packet loss (enabling flow control reduces the throughput).
6) Set the timeout to automatically drop the connection if no data is received (0=disabled).
7) Save the changes to let them take effect.

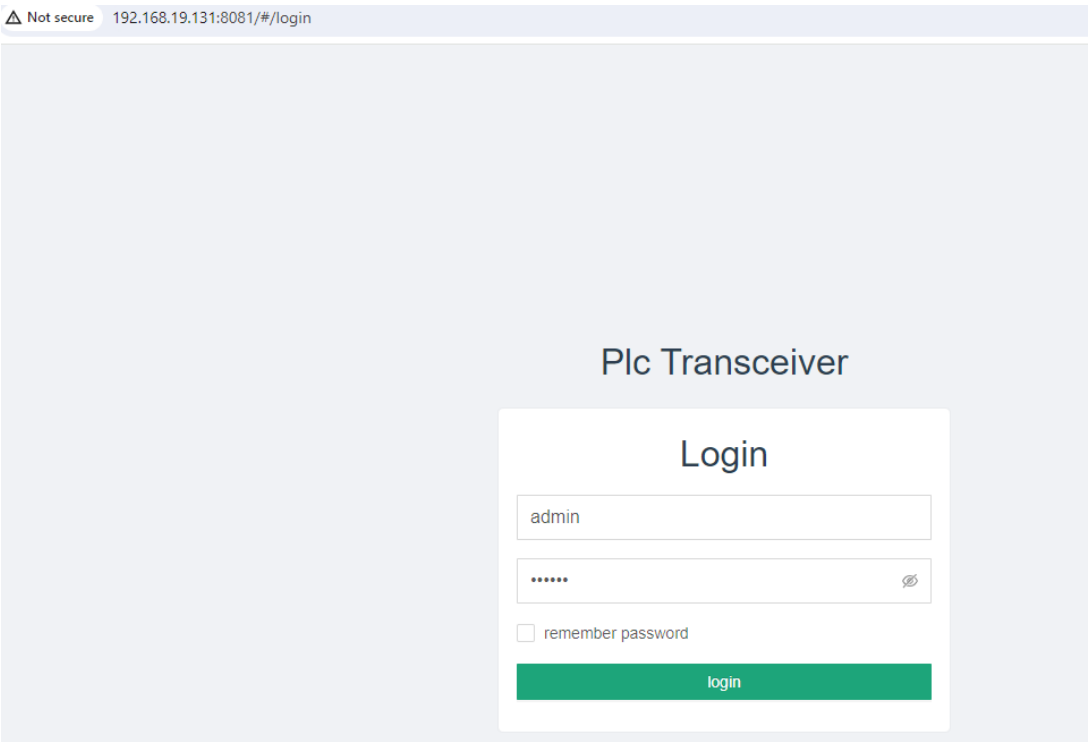
3. Enable the conversion rule.
4. Make sure both the client and server are on the same reachable IP network.
5. Verify the data transmission between the devices.

3.8.2 PLC

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

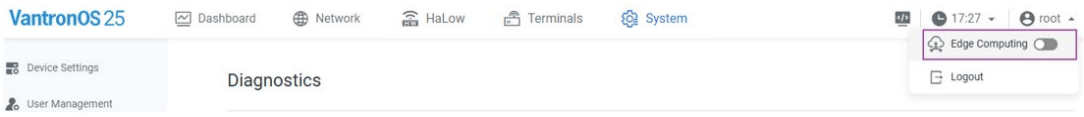
4.1 Overview

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 Portal Login

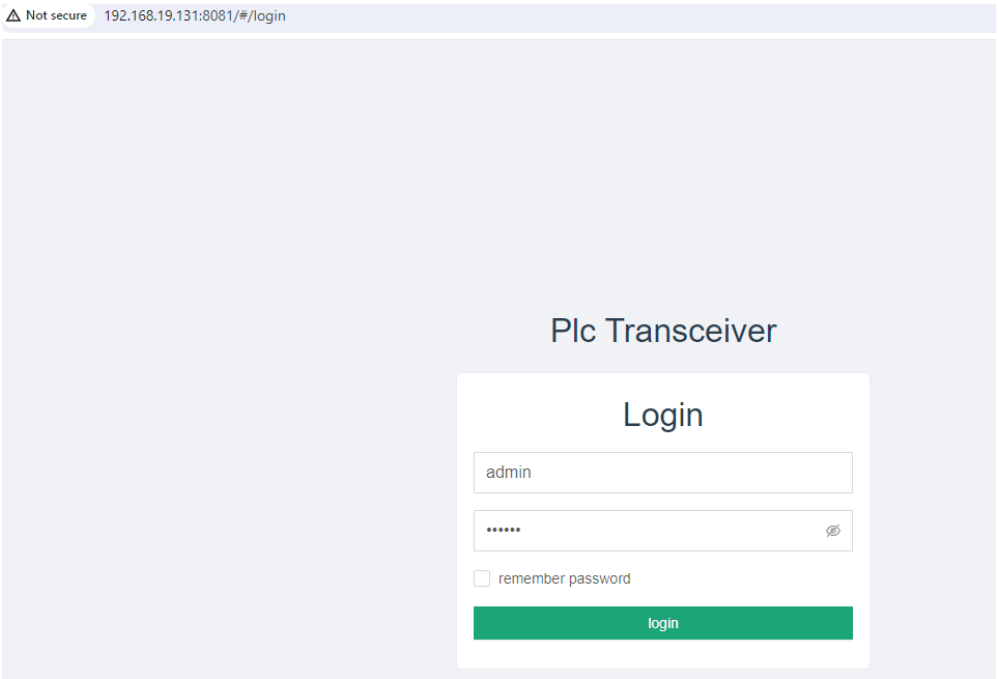
1. Enable the **Edge Computing** feature from the user account drop-down list.



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

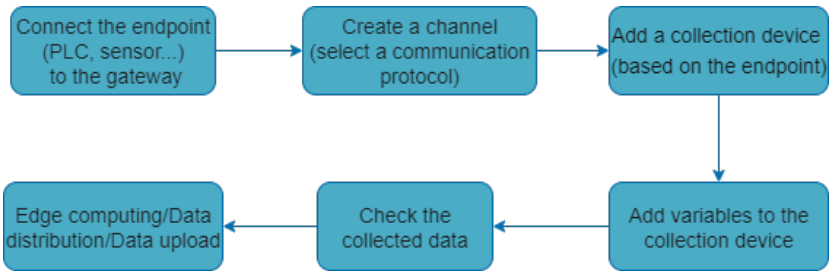


3. Users will be redirected to a new window. Use your VantronOS credentials to log in.



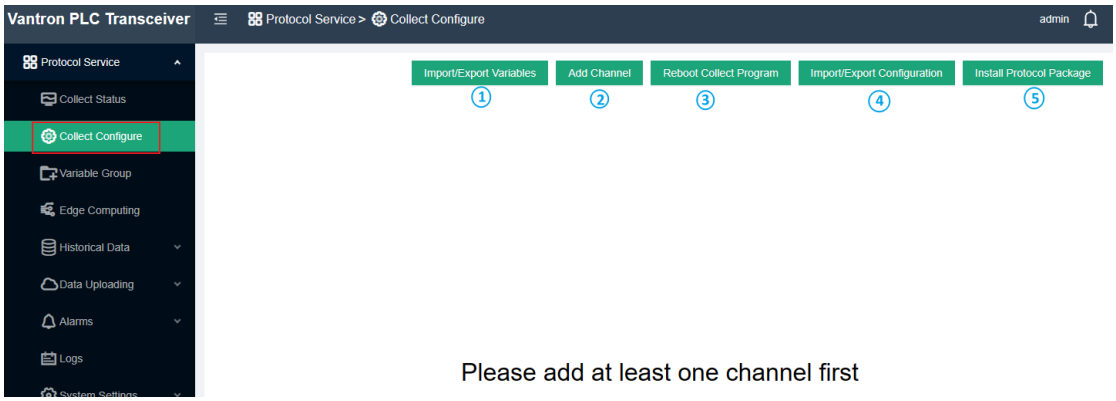
4.3 Protocol Configuration and Application

To use a protocol for data acquisition and edge computing, figure out the device model you are using for data collection and configure the protocol accordingly. Typical setup procedure is as follows:



4.3.1 Collection Channel Setup

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



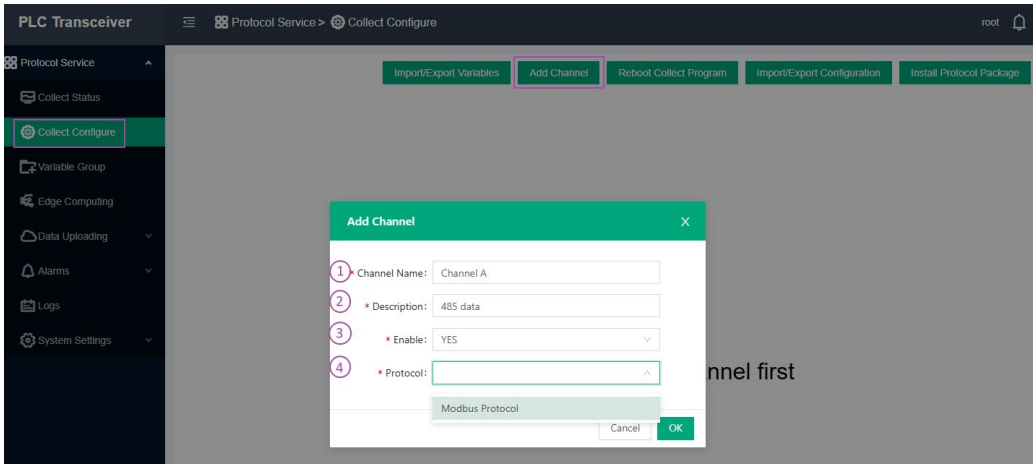
Description:

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.

4.3.1.1 Single Channel Configuration

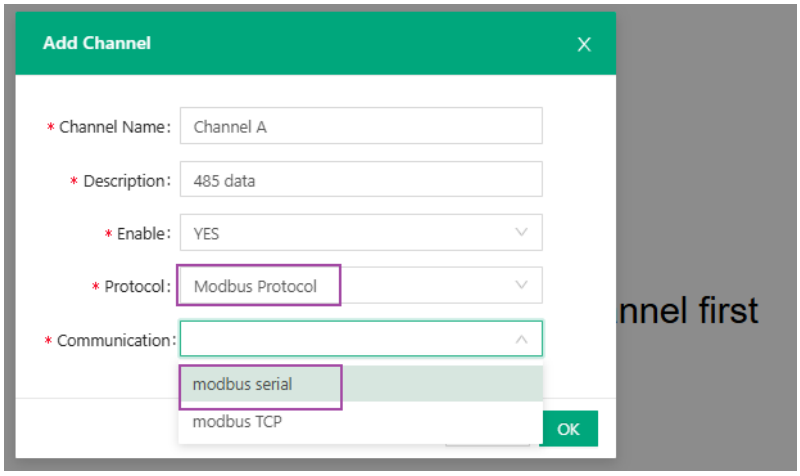
Click **Add Channel** under the **Collect Configure** menu to add a single channel.



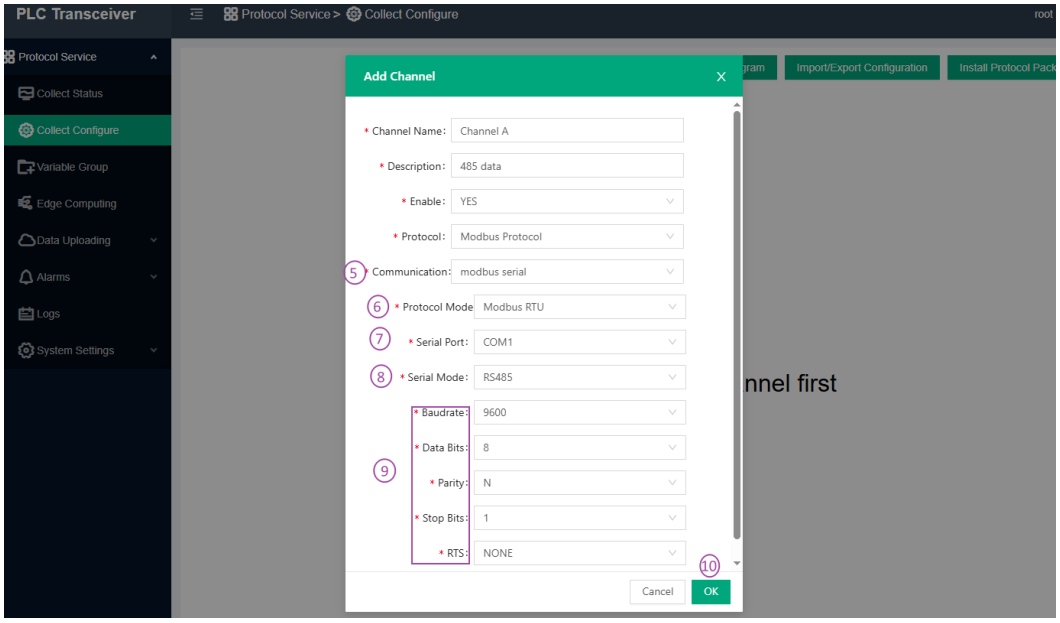
Description:

1. Enter a channel name that shall not be any one of the names in use.
2. Describe the channel.
3. Choose to enable the channel or not upon creation (‘Yes’ by default).
4. Select a protocol type from the drop-down list. The protocol must match the native protocol of the target endpoint.

Modbus Serial and **Modbus TCP** are supported on the HAP202. Take the **Modbus Serial** protocol for illustration. Ensure the endpoint is connected to the HAP202 via the RS485 serial port.



To further configure the protocol:

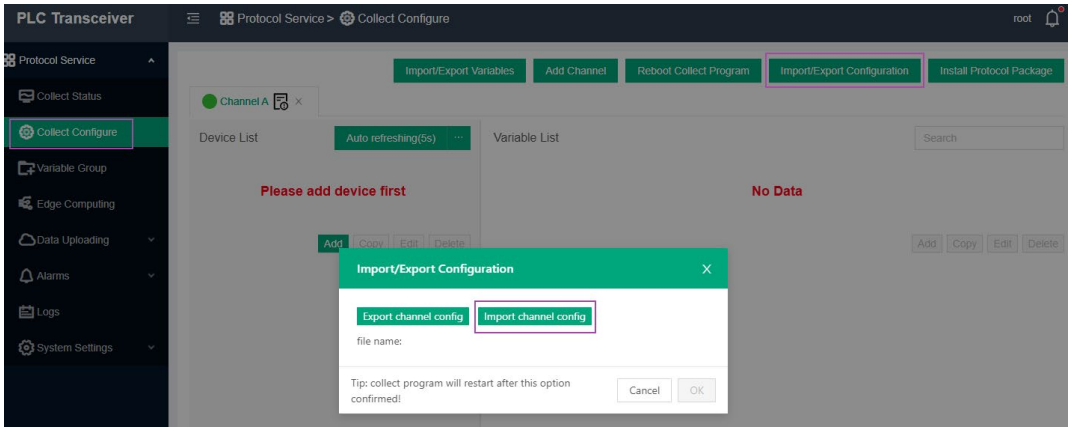


Description:

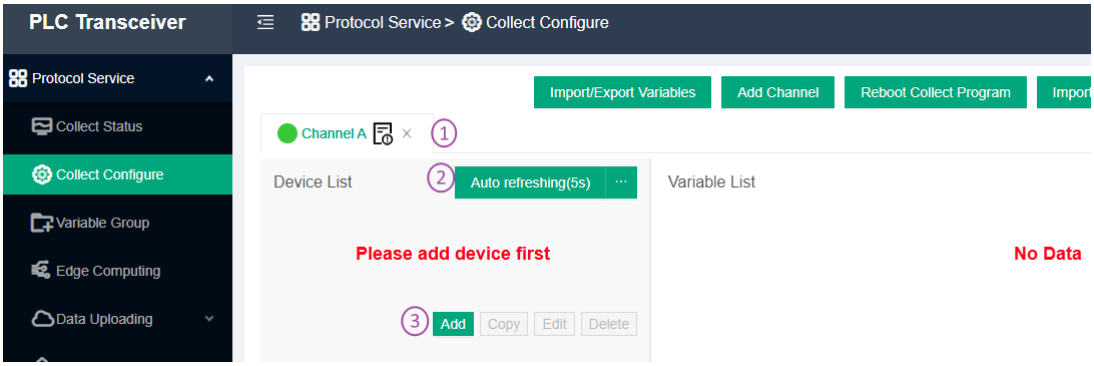
5. Choose **modbus serial** as the communication type.
6. Select **Modbus RTU/Modbus ASCII** as the protocol mode (Modbus RTU for illustration).
7. The HAP202 provides one serial port, mapped to the device software node (COM1).
8. Serial mode is bound to the device's serial port.
9. Fill in the serial parameters of the endpoint connected to the HAP202. Make sure the parameters match on both devices.
10. Click **OK** to complete the channel configuration.

4.3.1.2 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.



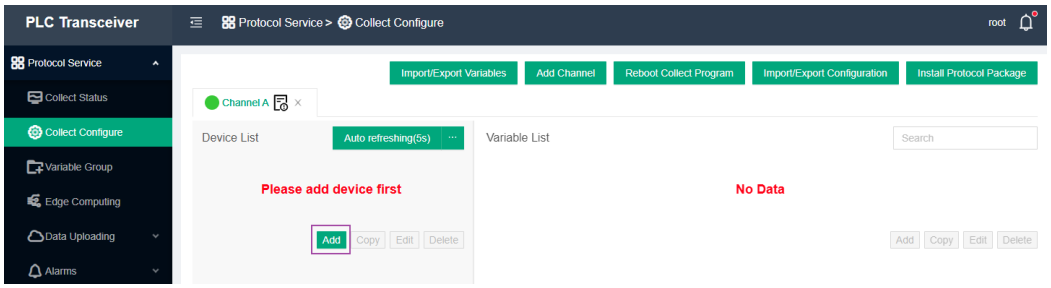
Description:

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.

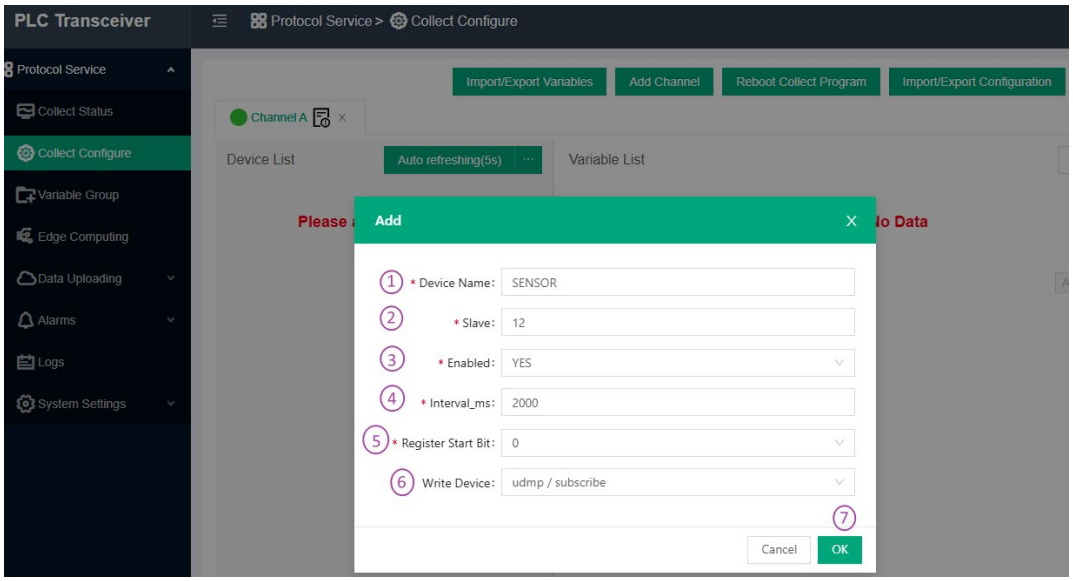
4.3.2 Device Setup

After creating a channel, the data collection endpoint that connects to the HAP202 can be added to this channel.

Click the **Add** button under **Device List** and input the endpoint information in the pop-up.



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



Description:

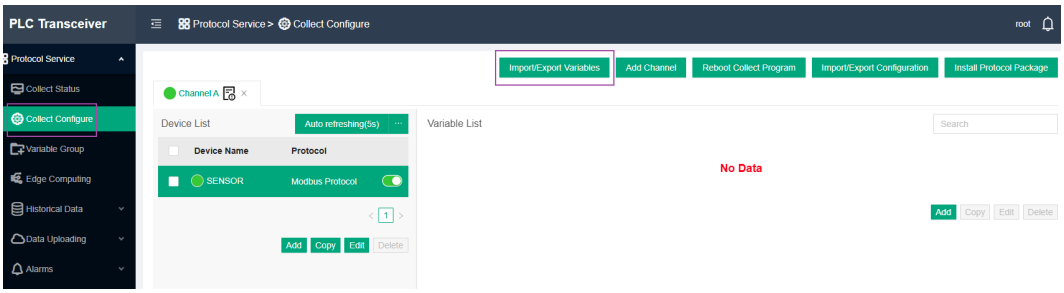
1. Enter a device name for the endpoint.
2. Input a slave address between 0 and 255.
3. Choose to enable the device or not.
4. Set an interval for data collection (you can leave it as-is).
5. Set a start bit for the register.
6. Select the path to write the data.
7. Click **OK** to complete adding the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

4.3.3 Variable Setup

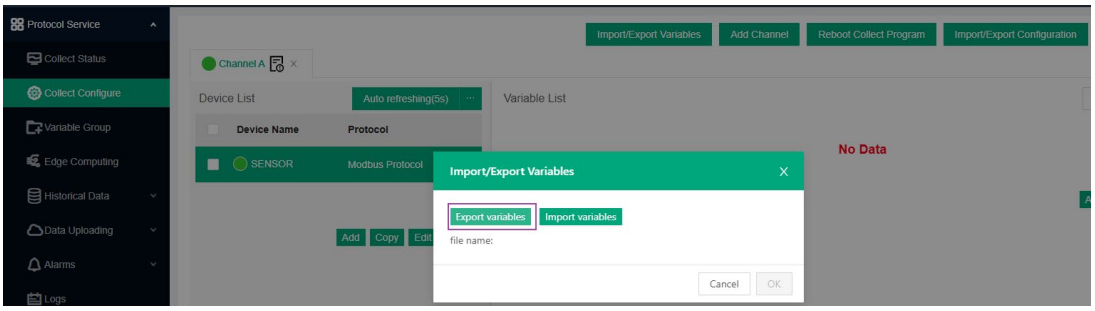
After channel and endpoint setup, users can choose to batch import the variables or configure individual variables for the target endpoints.

4.3.3.1 Global Batch Import

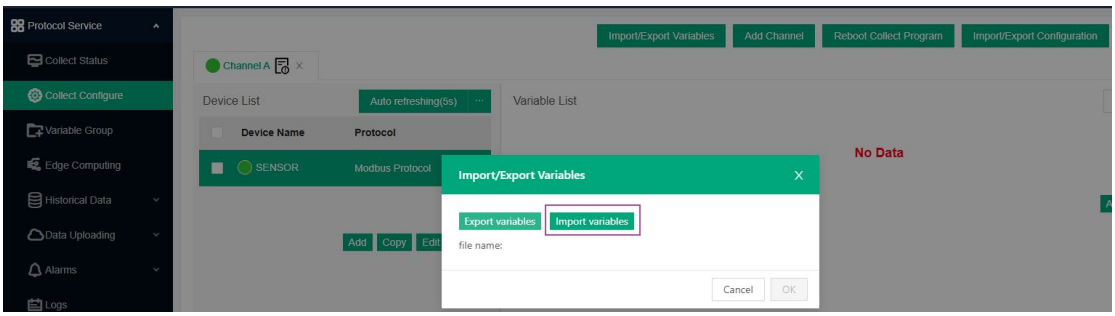
The **Import/Export Variables** tab on the **Collect Configure** menu allows users to import or export variables in bulk across different channels or endpoint devices.



For the **first** bulk import, you can click **Export variables** to get a reference template and fill in the fields accordingly.



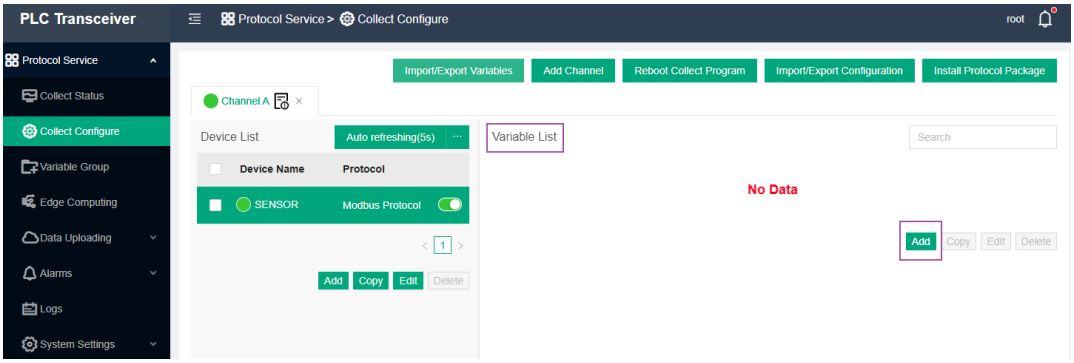
Then click **Import Variables** to upload the file.



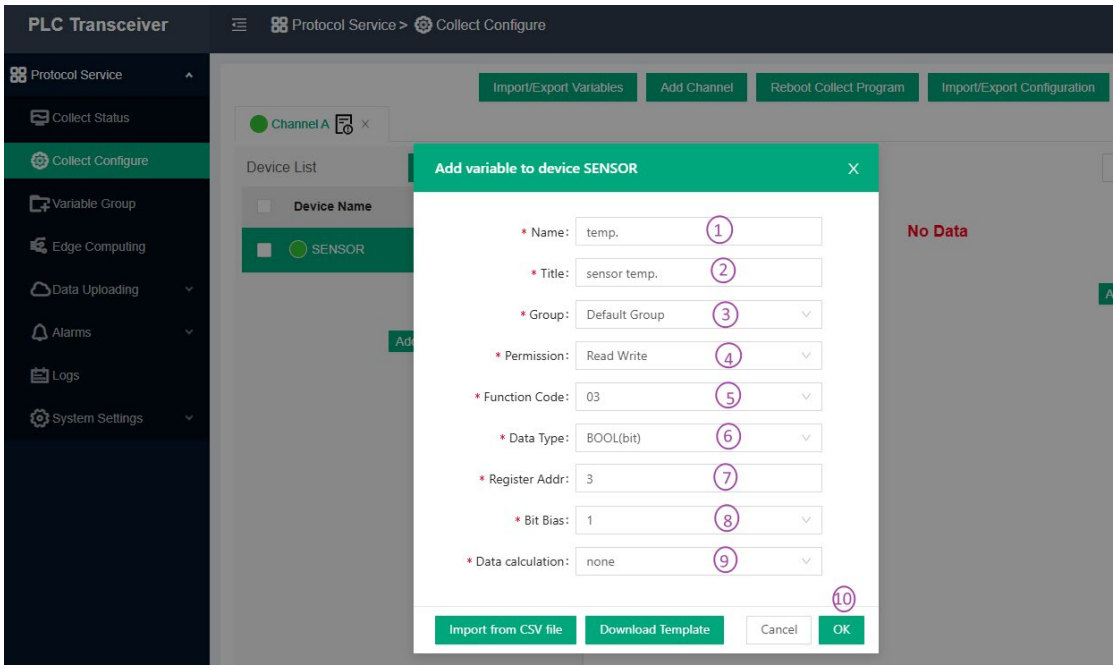
4.3.3.2 Individual Variable Configuration

Individual variable configuration applies to a selected endpoint device.

1. Click the **Add** button under **Variable List** next to the channel and device list.



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



Description:

Download Template: Template CSV file for reference

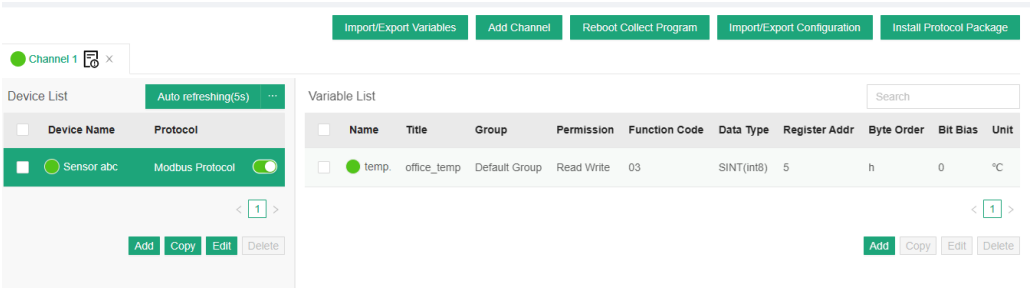
Import from CSV file: Bulk variable upload (replaced with **Export variables** for setups with existing variables)

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).

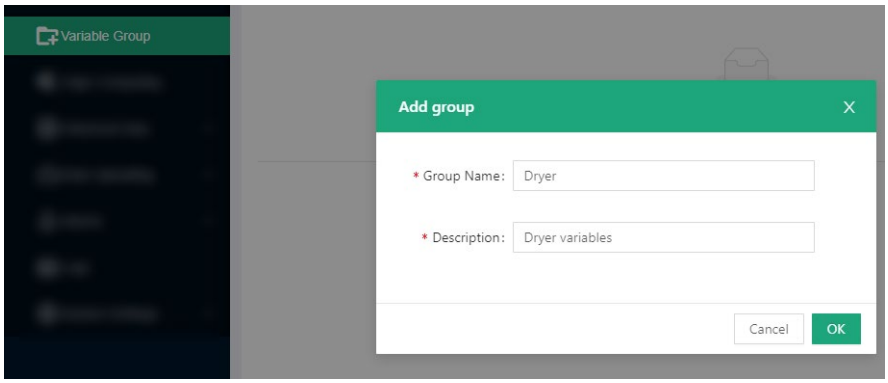
4) Set the access permission of the variable.
   a. Read only: You can only read the measured parameters
   b. Write only: You can only distribute values from the web portal to the field device
   c. Read Write: You can both read the measured parameters and distribute the values to the device
5) Select 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 bit bias.
9) Select a unit for the variable (determined by the collection device).
10) Select 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. You may add/copy/edit the variables as needed.

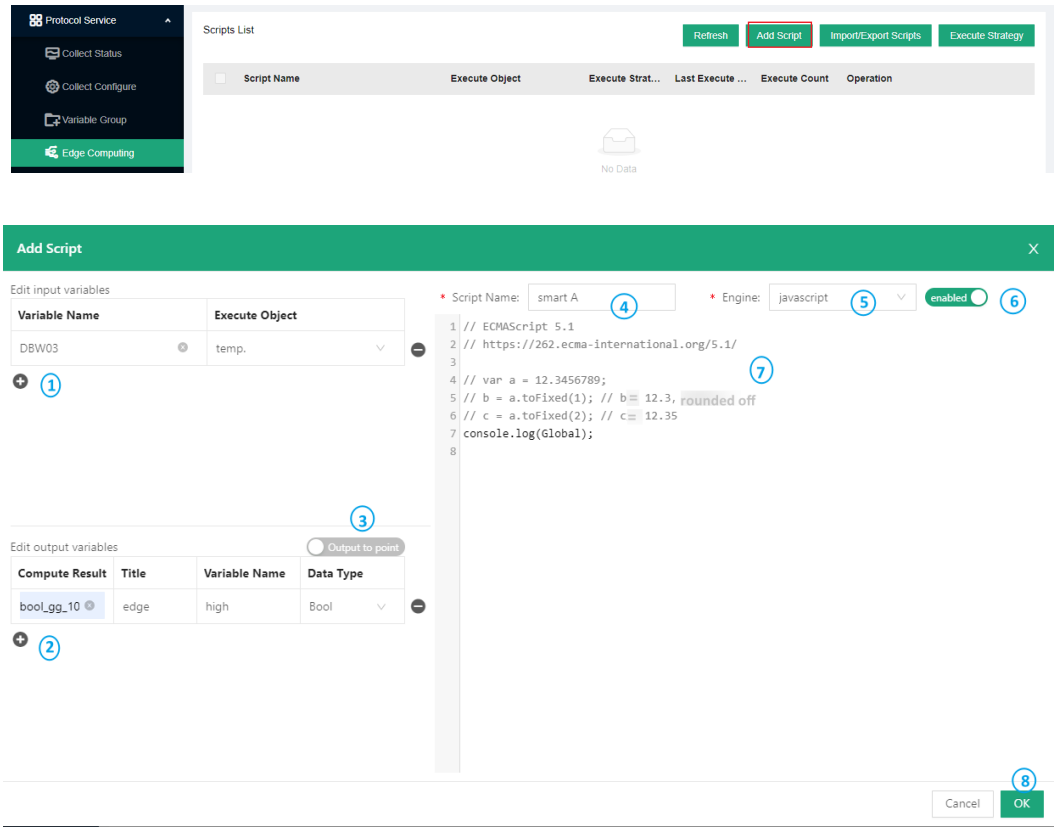


If multiple variables are involved, you can add variable groups for different variables from the **Variable Group** tab on the left menu pane.



4.4 Edge Computing Scripts Setup

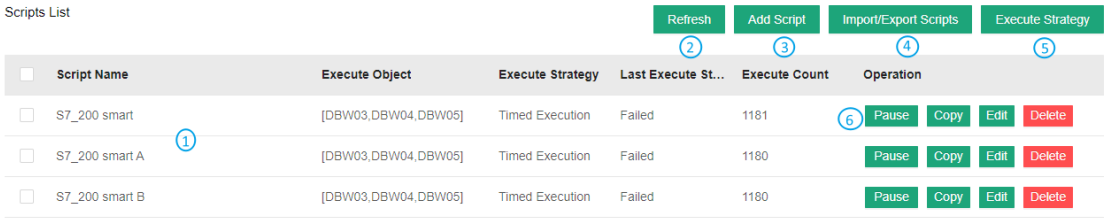
To add a script for edge computing, click **Edge Computing** from the navigation pane on the left, then click **Add Script** to input the script information in the pop-up.



Description:

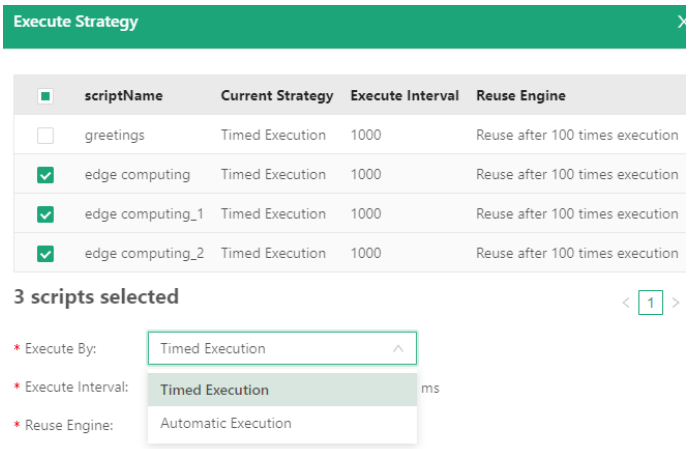
1. Edit input variables: add a name for the input variable and an object for executing the script (more than one variable could be added).
2. Edit output variable: add the computation result, title, variable name, and data type.
3. Toggle between outputting the results to the variables or edge nodes.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

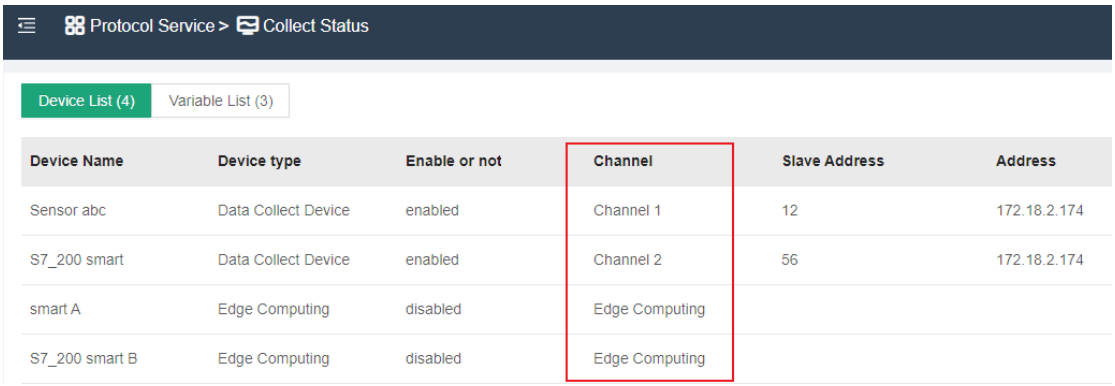
Reuse Context allows you to set a restart mechanism for the scripts

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).

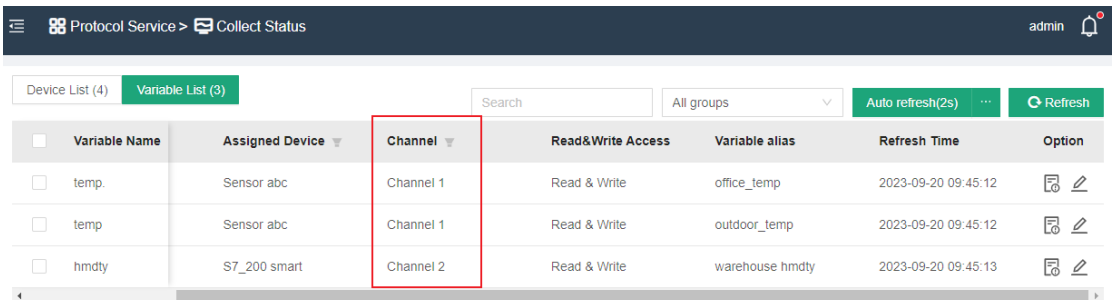
4.5 Collection Status

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

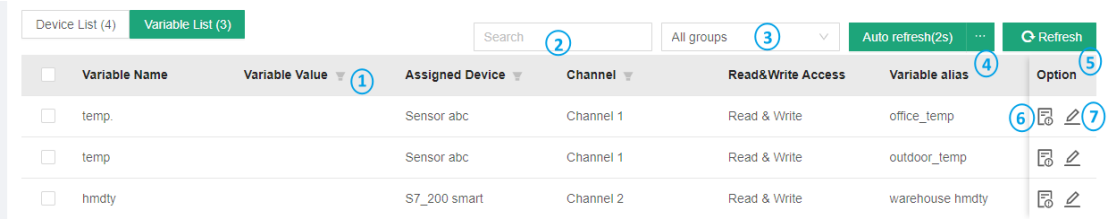
The **Device List** displays information about the collection devices, edge computing, historical data, etc. Users can differentiate the data based on the collection channels.



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



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



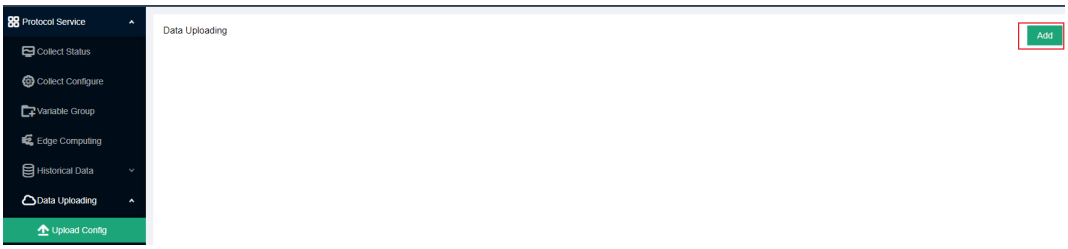
Description:

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).

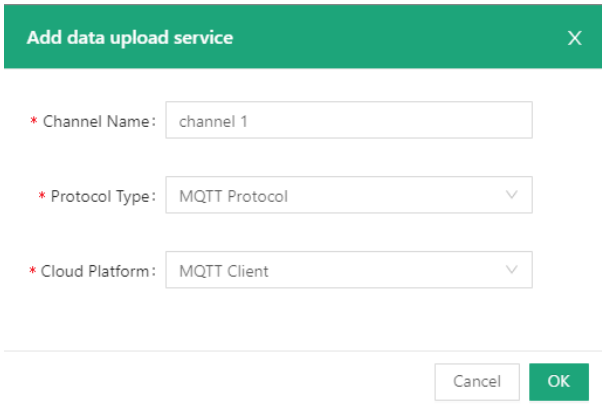
4.6 Data Upload and Encapsulation

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

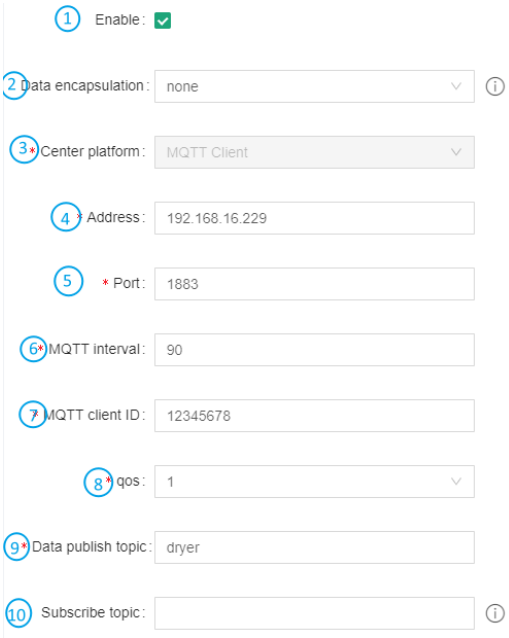
1. Expand the **Data Uploading** tab from the navigation pane and click **Upload Config**.
2. Click the **Add** button on the upper right corner to add a data upload task.



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



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



Description:

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 .

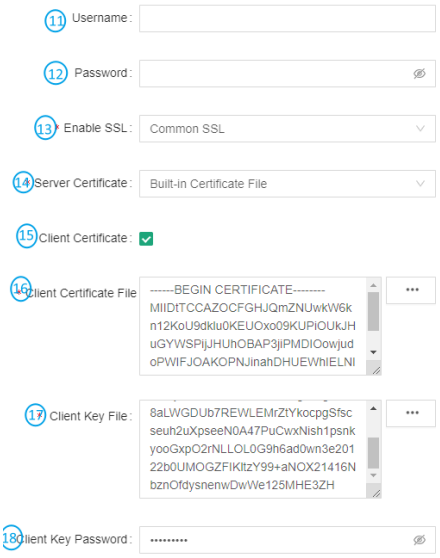
   QoS 0: The message will be sent once at the maximum. If the client is not available, the message will get lost.

   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).

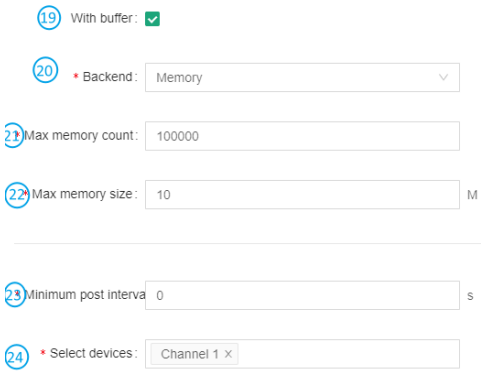
14) If common SSL is enabled, select a certification mode for the server.

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.



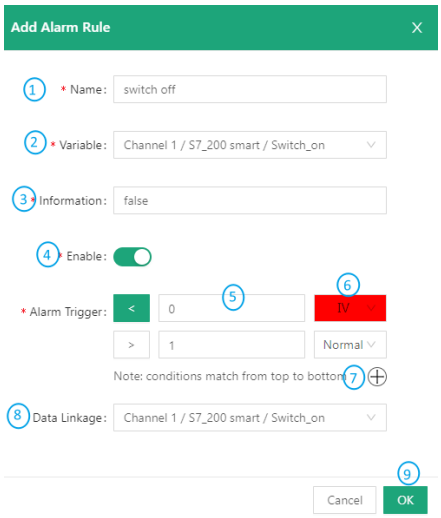
Description:

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

4.7 Alarm

4.7.1 Alarm Configuration

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

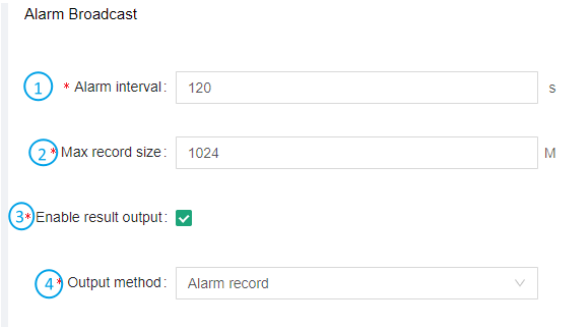


Description:

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

4.7.2 Alarm Broadcast

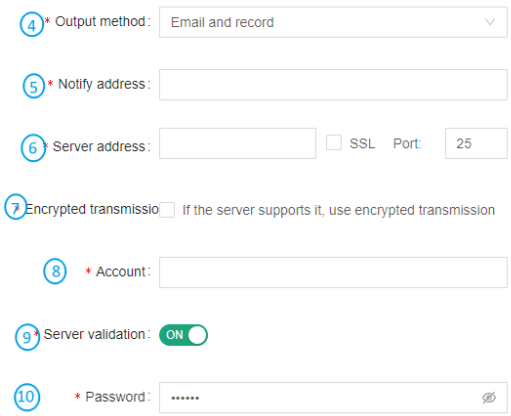
When the alarm rules are created, you can set the parameters for pushing an alarm on the **Alarm Broadcast** page.



Description:

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

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



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

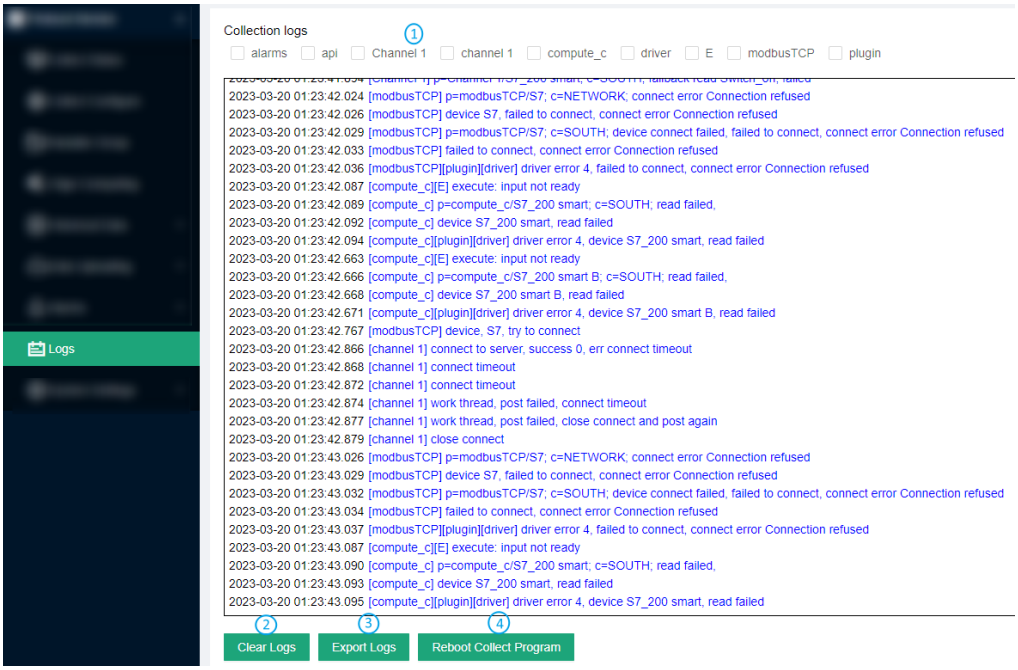
When you are all set, you can send a test email to check if the settings are ok, then submit the settings.

4.7.3 Alarm Record

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

4.8 Logs

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



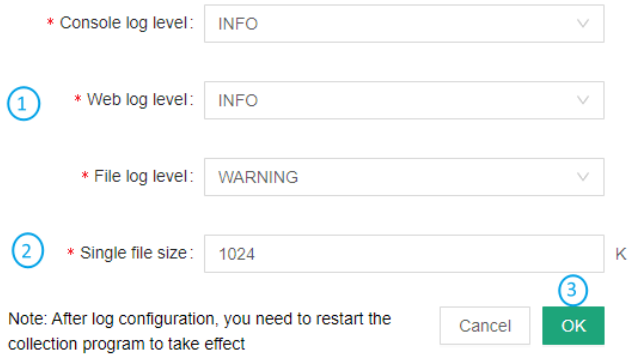
Description:

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

4.9 System Settings

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

- **Log Config.**



Description:

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 PRODUCT 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 Compliance Statement

This device complies with part 15 of the 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Exposure to radio frequency energy:

The radiated output power of this device meets the limits of FCC 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.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses 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.

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.