HAP101 Wi-Fi HaLow Access Point



User Manual

Version: 3.2

© Vantron Technology, Inc. All rights reserved.

Revision History:

No.	Description	Date
V1.0	First release.	Jan. 10, 2024
V1.1	Broke down the steps for web login.	Jan. 25, 2024
V1.2	Updated the steps in WIFI connection as per the firmware upgrade.	Feb 2, 2024
V1.3	Added a use case for connecting Wi-Fi cameras to the network .	Feb. 5, 2024
V1.4	1. Added a new option for device web login by using the VLAN IP of the device. 2. Clarified the methods of factory resetting the device.	Jun. 24, 2024
V1.5	Updated the definition of ERR indicator.	Jul. 23, 2024
V1.6	1. Updated the back view as per design change. 2. Updated the steps for setting up the device. 3. Updated chapter 4 USE CASE.	Oct. 12, 2024
V2.0	1. Updated the interface definition as per HW design change. 2. Added description on the use of DIP switches, the Pair/Restart button, and the definition of the LED indicators based on the updated hardware version. 3. Updated the steps in 2.1 setting up the device. 4. Added description for the use of the DIP switches and LED indicators. 5. Updated the use case as per firmware upgrade.	Nov. 18, 2024
V2.1	1. Updated the screenshots as per the function update of the web portal. 2. Added description for the use of ACL, DHCP, and DPP features.	Dec. 16, 2024
V2.2	Updated the description of the device interfacing with BlueSphere GWM.	Dec. 18, 2024
V2.3	Added description on network interface bridging (2.6).	Feb. 7, 2025
V2.4	1. Updated the description on the bridge mode of 2.4 GHz Wi-Fi when switching the WAN port to LAN. 2. Updated the description and steps regarding the WAN port switching in chapter 4 USE CASE accordingly. 3. Updated the debugging method of the device in chapter 5.	Mar. 21, 2025
V2.5	1. Updated the description for AP, STA, Mesh Portal, and Mesh point. 2. Updated table 1-3 in 1.7.1 and figure 1-1 in 1.7.2. 3. Adjusted chapter 2 based on the change of the default HaLow mode to STA. 4. Updated the description for the DIP switches as per design update. 5. Updated the description on the button state for DPP pairing in HaLow Mesh Mode. 6. Added hardware setup for quick HaLow Mesh configuration in 2.2.2. 7. Modified Pair/Restore button to Pair/Restart button; 8. Updated the Table 2-3 in 2.5; 9. Separated the sections in chapter 2 and updated chapter 3; 10. Added 4.4.4 (port forwarding); 11. Updated chapter 5; 12. Removed the debugging chapter for security concern.	Jul. 28, 2025

V3.0	Regenerated chapters 2 & 3 based on the current **VantronOS 25** system UI, including device login, startup wizard, DPP pairing, device setup, etc.	Oct. 25, 2025
V3.1	1. Removed the description of automatic Ethernet mode change upon short press of the Pair button (Section 2.5) based on the new design. 2. Updated Sections 1.6 &1.7 on the button and LED definitions. 3. Updated Section 3.1 as per UI change. 4. Deleted Section 3.3.1.1 Uplink Interface, 3.3.1.2 IP Configuration Mode, 3.3.1.3 Downlink Interfaces, 3.1.4 DHCP Service & DHCP Reservation, 3.3.1.5 Ethernet Port Mode Modification, 3.3.1.6 Interface Bridging as per UI change. 5. Added Section 3.3.1.1 WAN, 3.3.1.2 LAN, and 3.3.1.3 IPv6 Settings as per UI change; included DHCP Service & DHCP Reservation in 3.3.1.2. 6. Modified Sections 3.3.2&3.4.1 Wi-Fi & HaLow settings and added Section 3.4.4 Mesh Settings. 7. Added Section 3.7 CLI.	Mar. 12, 2026
V3.2	1. Modified the definition of mesh portal (MPP) in Section 1.3 and updated the mesh network topology accordingly in Section 2.1.2. 2. Added LED status description for factory reset to Section 1.8. 3. Updated the HaLow RSSI logic description in Section 1.8.2. 4. Updated the definition of the Restart LED in Section 1.8.4. 5. Removed Section 2.4.2 (mobile login) and merged its content with the PC login procedure. 6. Removed Sections 2.8 & 2.9 and integrated BlueSphere GWM content into Section 3.7.4.1 and factory reset content into Section 1.6. 7. Updated Sections 2.6 & 2.7 to align with current product design. 8. Added description for Ethernet mode switch in Section 3.3.1. 9. Removed the PPPoE protocol description from Section 3.3.1.1. 10. Updated the interface bridging description in Section 3.3.1.2. 11. Revised Sections 3.4.1.1–3.4.2 on HaLow mode descriptions to align with the current design. 12. Added Section 3.6.3.4 (Log capture). 13. Added Chapter 4 covering industrial protocol configuration.	Oct. 23, 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 9
1.5.1 Front view 9
1.5.2 Back view 10
1.6 DIP Switches 11
1.7 Pair/Restart Button 11
1.7.1 Button Action for DPP, Mesh & Device Reset 12
1.7.2 Button Action & HaLow LED Diagram 13
1.8 LED Indicators 14
1.8.1 Wi-Fi Activity LED (WLAN) 14
1.8.2 HaLow Activity LED (HaLow) 14
1.8.3 Up & Down LEDs 16
1.8.4 Restart LED 16
1.8.5 Power LED 17
1.8.6 System LED 17
1.8.7 Error LED 17
1.9 Serial Port 18
CHAPTER 2 GETTING STARTED 19
2.1 Network Architecture 20
2.1.1 Standard HaLow Network 20
2.1.2 HaLow Mesh Network 21
2.2 Setting up the Device 22
2.3 Powering up the Device 23
2.4 Quick Access to the Device 24
2.5 Default Network Interface Status 26
2.6 DPP Pairing 26
2.6.1 Pairing via Hardware Seup 27
2.6.2 Pairing via Software Setup 28
2.6.3 Exiting DPP Pairing Mode 29
2.7 Quick Mesh Networking 30
2.8 SSH and Serial Console Access 31
CHAPTER 3 DEVICE SETUP IN VANTRONOS 33
3.1 Introduction to VantronOS 34
3.1.1 Web Overview 34
3.1.2 Log Out 35
3.2 Dashboard 36
3.3 Network 37
3.3.1 Ethernet Mode Switch 37

3.3.2 WAN Interface 38
3.3.2.1 Basic IP Configuration 39
3.3.2.2 Interface Bridging 40
3.3.2.3 Link Priority 41
3.3.2.4 Link Diagnosis 42
3.3.3 LAN Interface 43
3.3.3.1 Subnet Conflict 43
3.3.3.2 DHCP Service & DHCP Reservation 43
3.3.4 IPv6 Settings 45
3.3.5 Wi-Fi 46
3.3.5.1 AP-Mode Basic Settings 46
3.3.5.2 AP-Mode Advanced Settings 47
3.3.5.3 Client-Mode Basic Settings 48
3.3.5.4 Client-Mode Advanced Settings 49
3.3.6 QoS Bandwidth Control 50
3.3.7 Static Route 51
3.3.8 Porting Mapping 54
3.3.9 Network Security 56
3.3.9.1 Basic SSH Access Setup 56
3.3.9.2 ACL Access Control 57
3.4 HaLow 60
3.4.1 Overview 60
3.4.1.1 STA-Mode Settings 61
3.4.1.2 AP-Mode Settings 63
3.4.2 Mesh Networking 65
3.5 Terminals 67
3.6 System 68
3.6.1 Device Settings 68
3.6.1.1 Modifying Device Name 68
3.6.1.2 System Time 69
3.6.2 User Management 70
3.6.3 Diagnostics 71
3.6.3.1 Network Diagnostics 71
3.6.3.2 Web Terminal 72
3.6.3.3 Logs 73
3.6.3.4 Log Capture 74
3.6.4 System Maintenance 76
3.6.4.1 BlueSphere 76
3.6.4.2 Device Maintenance 78
3.7 Command Line Interface 79
3.8 Edge Computing 80
3.8.1 Serial to TCP 80
3.8.1.1 Server Mode Rule Setup 81
3.8.1.2 Client Mode Rule Setup 82
3.8.2 PLC 83

CHAPTER 4 INDUSTRIAL PROTOCOLPORTAL 84
4.1 Overview 85
4.2 Portal Login 85
4.3 Protocol Configuration and Application 86
4.3.1 Collection Channel Setup 86
4.3.1.1 Single Channel Configuration 87
4.3.1.2 Batch Import of Channel Configurations 89
4.3.2 Device Setup 90
4.3.3 Variable Setup 91
4.3.3.1 Global Batch Import 91
4.3.3.2 Individual Variable Configuration 92
4.4 Edge Computing Scripts Setup 94
4.5 Collection Status 96
4.6 Data Upload and Encapsulation 97
4.7 Alarm 101
4.7.1 Alarm Configuration 101
4.7.2 Alarm Broadcast 102
4.7.3 Alarm Record 103
4.8 Logs 103
4.9 System Settings 104
CHAPTER 5 DISPOSAL AND PRODUCT WARRANTY 105
5.1 Disposal 106
5.2 Warranty 107
Appendix Regulatory Compliance Statement 108

Foreword

Thank you for purchasing HAP101 Wi-Fi HaLow Access Point ("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 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

Vantron HAP101 Wi-Fi HaLow access point is designed in compliance with the prominent IEEE 802.11ah (Wi-Fi HaLow) standard and IEEE 802.11 b/g/n (2.4 GHz Wi-Fi) standard. It offers a complete Wi-Fi connectivity solution for IoT developers who seek for wireless connections with energy efficiency, extended coverage, obstacle penetration, effortless accessibility, etc.

HAP101 supports up to 1km coverage at ultra-low power consumption while still delivering optimal performance with data rates up to 150 Mbps on 2.4 GHz Wi-Fi and 32.5 Mbps on Wi-Fi HaLow. By complying with the IEEE 802.11ah standard, it supports operation in the sub-1GHz license-exempt RF bands to avoid the crowded 2.4 GHz frequency band. At the same time, the 2.4 GHz Wi-Fi capability ensures compatibility with devices that do not support HaLow.

HAP101 also offers DIP switches for quickly toggling between HaLow access point (AP) and station (STA), as well as for switching configurations between standard HaLow applications and HaLow mesh networks that involve multiple access points. This versatility makes it ideal for long-range sub-GHz networking applications such as smart home appliances, surveillance systems, industrial process control, logistics and asset management, and smart city facilities.

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:

- HAP101 Wi-Fi HaLow access point
- 2 x 2.4 GHz Wi-Fi antenna
- 1 x Wi-Fi HaLow antenna
- 1 x DC power connector
- 1 x RS485 terminal connector

Optional accessories:

- 1 x 12V⎓1A power adapter
- 1 x Power cord
- Waterproof kit for the IP54 variant: 1 x Waterproof base + 1 x 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.

Table 1-1

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 Wi-Fi, and *HaLow* refers to Wi-Fi HaLow.

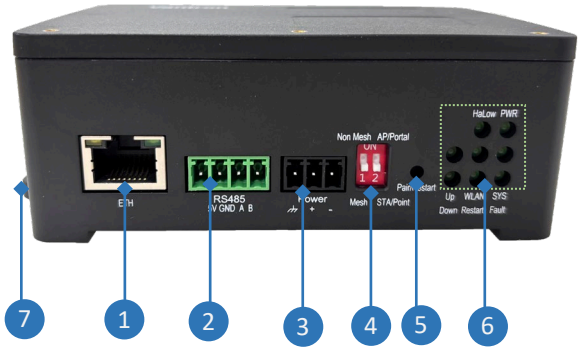
1.4 Specifications

HAP101			
System	CPU	MediaTek 580MHz MIPS® CPU	
	Wi-Fi HaLow SoC	Morse Micro MM6108	
	Memory	256MB	
	Storage	64MB	
WLAN Features	2.4 GHz Wi-Fi	Standard: IEE 802.11 b/g/n	
		Frequency range: 2.412GHz ~ 2.462GHz	
		Channel bandwidth: 20/40 MHz	
		Data rate: up to 150Mbps	
		Fast pairing: WPS fast connection supported	
		Working mode: Access point (AP), Station (STA)	
	Wi-Fi HaLow	Standard: IEE 802.11 ah	
		Frequency range: 903.5MHz~926.5MHz (US)	
		Channel bandwidth: 1/2/4/8 MHz, dynamic channel selection (DCS) supported	
		Transmit power: 21dBm	
		Data rate: up to 32.5Mbps @8MHz or 15Mbps @4MHz	
		Fast pairing: DPP Easy Connect via hardware/software setup	
		Working mode: Access point (AP), Station (STA), Mesh	
		Security: AES, WPA3	
I/O	Fast Ethernet	1 × RJ45, 10/100Mbps	
	Serial port	1 × RS485/debugging (RS485 default, 5V output, baud rate: 115200)	
	Antenna	1 × Wi-Fi HaLow antenna	2 × 2.4 GHz Wi-Fi antenna
System Control	LED indicators	1 × Power LED	1 × Wi-Fi HaLow activity LED
		1 × Uplink LED	1 × Downlink LED
		1 × WLAN activity LED	1 × Error LED
		1 × Reserved LED (user-defined)	1 × System LED
	Button	1 × Pair/Restart button	
	DIP switch	2 × DIP switch (AP & STA; Mesh & other modes)	
Mechanical	Dimensions	IP40 version (With wall mount): 130mm × 74mm × 42mm	
		IP54 version (With wall mount and water proof kit): 130mm × 119mm × 44mm	
	Casing material	Black plastics, UL94, SP6 compliant (Optional: White casing)	
	Installation	Wall mounting	
	IP rating	IP40 (Optional: IP54, enhanced with a waterproof kit)	
Power	Input	9V ~ 40V DC	
	Port	3-pin terminal (Over-current protection, reverse polarity protection)	

HAP101			
Software	Operating system	VantronOS	
	Device management	Vantron BlueSphere GWM (Optional)	
	Upgrade	Local upgrade, OTA upgrade	
	VPN	OpenVPN	
	Network protocol	IPV4, HTTPS, TCP & UPD, 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 Wi-Fi	TKIP, WPA, WPA2, AES, WPS	
	Wi-Fi HaLow	WPA3	
	Firewall	Stateful	
	Access control	MAC address, IP address, URL	
Environmental	Temperature	Operating: -20℃ ~ +70℃	Storage: -40℃ ~ +85℃
	Humidity	≤ 95% RH (non-condensing)	
	Certification	FCC, ISED	

1.5 Product Layout

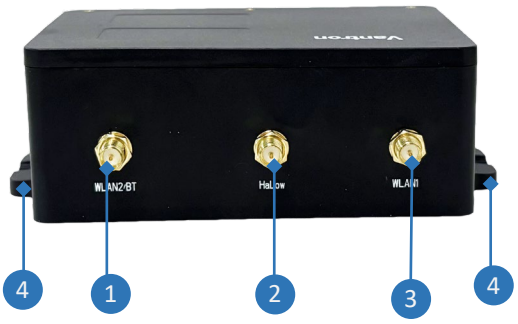
1.5.1 Front view



Description:

Item	Description			
1	Ethernet jack (100Mbps), configured as a LAN port by default			
2	RS485 for serial communication or device debugging			
	Serial communication (**default**): 115200, 8N1; device debugging: refer to chapter 5			
3	Power terminal, supporting 9V~40V DC input			
4	DIP Switches	2 × 2 DIP switch. Refer to Section 1.6 for details.		
5	Pair/Restart button	Activates the device for DPP provisioning or factory reset. Refer to Section 1.7 for details.		
6	Three-column LED indicators (Refer to Section 1.8)	/	HaLow (Wi-Fi HaLow LED)	PWR (power LED)
		Up (uplink LED)	WLAN (2.4 GHz Wi-Fi LED)	SYS (system LED)
		Down (downlink LED)	Restart (restart LED)	Fault (error LED)
7	Mounting bracket (screws recommended: M3 × 8mm/ST2.9 depending on the mounting surface)			

1.5.2 Back view



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

1.6 DIP Switches

The HAP101 offers two DIP Switches (2 x 2) that can be configured to different modes as detailed below.

Table 1-2

Switch 1	Switch 2	Description
Non-Mesh [Standard HaLow mode]	AP/Portal	The device operates as a HaLow AP
	STA/Point	The device operates as a HaLow station (STA)
Mesh [HaLow Mesh mode]	AP/Portal	The device operates as a Mesh Portal
	STA/Point	The device operates as a Mesh Point

The switches are set to the Non-mesh—STA/Point position (1: UP, 2: Down) by default, and this setting alone does **NOT** indicate the current working mode of the device. The DIP switches are designed to use in combination with the Pair/Restart button to confirm the device HaLow mode.

1.7 Pair/Restart Button

The Pair/Restart button either confirms the DIP switch setup and activates DPP pairing/mesh configuration or initiates a device reboot/reset.

Table 1-3

Button Hold	Description
<1s	Confirms the DIP switch setup, and: • Enters DPP pairing state (Standard profile); **OR** • Starts scanning for a HaLow Mesh network with the same settings (Mesh profile).
[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.

HAP101
User Manual

1.7.1 Button Action for DPP, Mesh & Device Reset

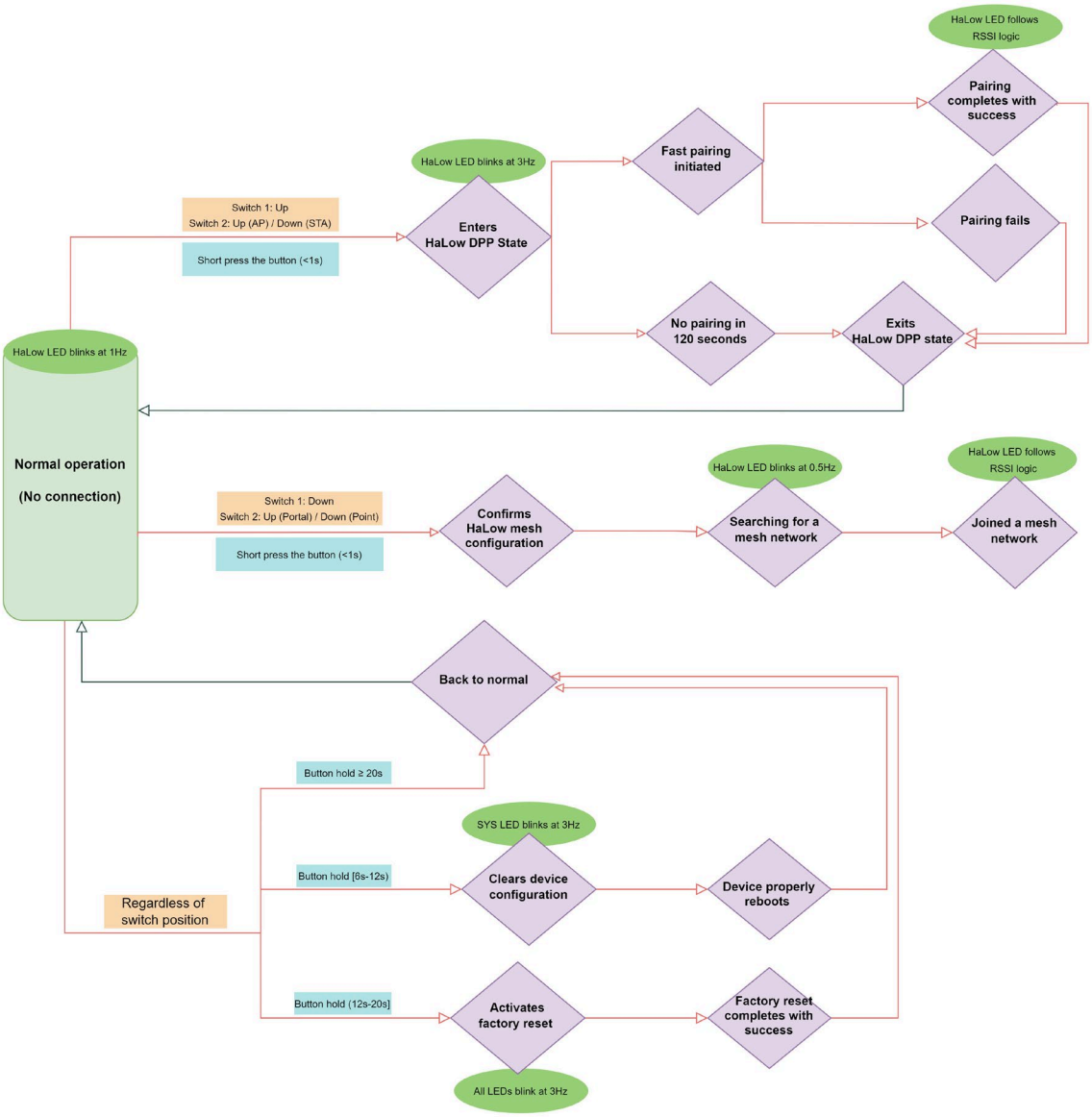
Table 1-4

Prerequisites	Intended State	Button Action	Results & Indicator Status
1. DIP switch 1: Up 2. DIP switch 2: Up or Down (device role dependent)	Enter HaLow DPP	Short press (< 1s)	• HaLow DPP state is activated upon button press, and the HaLow LED blinks at 3Hz. • When pairing completes & communication is active: The HaLow LED follows the RSSI logic (see Section 1.8.2).
Device in HaLow DPP state	Exit HaLow DPP	No action	No pairing within 120s (target device not in DPP state): Returns to normal operation.
		No action	Pairing completes or fails: Returns to normal operation.
		Short press (< 1s) within 120s validity window	Re-activates the HaLow DPP state (the device does NOT exit HaLow DPP).
1. DIP switch 1: Down 2. DIP switch 2: Up or Down (device role dependent)	Quick HaLow Mesh Configuration	Short press (< 1s)	Mesh configuration is confirmed upon button press: • Searching for a mesh network: the HaLow LED blinks at 0.5Hz. • Joins a mesh network: the HaLow LED follows the RSSI logic.
Device in normal operation state	Device Reset	Long press [6s, 12s): Configuration clear [12s, 20s): Factory reset	1. Press and hold for the required duration, then release: The System LED (configuration clear)/All LEDs (factory reset) blink at 3Hz, indicating the device is ready for the reset. 2. Reset successful: The PWR and SYS LEDs turn solid green.
N/A	Exit Reset State	Button hold ≥ 20s	Aborts reset process and returns to normal operation.

1.7.2 Button Action & HaLow LED Diagram

The Pair/Restart button can be used in combination with the DIP switches and LED indicators to better determine the status of the device as shown below.

Figure 1-1:



1.8 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.

1.8.1 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	2.4 GHz Wi-Fi module is not working.
	Blinking at 1Hz	2.4 GHz Wi-Fi is not connected.
	Solid green	A Wi-Fi client is connected.

1.8.2 HaLow Activity LED (HaLow)

HaLow Mode	LED Status	Description
HaLow STA	OFF	Wi-Fi HaLow link is down.
	Blinking at 1Hz	Not connected to a HaLow AP yet.
	Blinking at 3Hz	DPP pairing initiated. (Blinking at 1Hz after 3s upon a timeout; following the RSSI configuration logic upon a successful pairing)
	Following the RSSI logic*	Connected to a HaLow AP.

HaLow Mode	LED Status	Description
HaLow AP	OFF	Wi-Fi HaLow link is down.
	Blinking at 1Hz	No HaLow STA connected yet.
	Blinking at 3Hz	DPP pairing initiated. (Blinking at 1Hz after 3s upon a timeout; following the RSSI configuration logic upon a successful pairing)
	Following the RSSI logic*	At least one HaLow STA connected.
Mesh (Mesh + AP)	OFF	Wi-Fi HaLow link is down.
	Blinking at 0.5Hz	Not joined to a HaLow Mesh network.
	Following the RSSI logic*	Joined a HaLow Mesh network.

*** HaLow RSSI Configuration Logic:**

The HaLow LED uses the following RSSI-based logic for both Standard and Mesh connections:

Signal Strength	LED status	RSSI Range
Excellent	Solid green	0 to -30dBm
Good	Solid for 5s, blinking at 3Hz for 3s (cycle)	-30 to -50dBm
Fair	Solid for 5s, blinking at 1Hz for 3s (cycle)	-50 to -70dBm
Weak	Solid for 5s, blinking at 0.3Hz for 3s (cycle)	< -70dBm
No connection	Blinking at 1Hz	-

In the HaLow AP mode:

Connection Status	HaLow LED Status
No Connection	Blinking at 1Hz
Single station connection	Following the HaLow LED definitions.
Multiple station connection	Following the RSSI logic based on the STA with the weakest signal strength.

In the HaLow STA mode:

Connection Status	HaLow LED Status
No Connection	Blinking at 1Hz
Connected	Following the RSSI logic.

In the HaLow Mesh mode:

Connection Status	HaLow LED Status
Not in a HaLow Mesh network	OFF
In a HaLow Mesh network (multiple nodes involved)	Following the RSSI logic based on the Mesh node with the weakest signal strength in the network.

1.8.3 Up & Down LEDs

LED	Status	Description
Up	OFF	No uplink connection.
	Solid green	Uplink connected.
	Blinking	Data transferring on uplink.
Down	OFF	No downlink connection.
	Solid green	Downlink connected.
	Blinking	Data transferring on downlink.

1.8.4 Restart LED

This LED is user-defined and factory set to OFF.

1.8.5 Power LED

LED	LED Status	Description
PWR	Solid on	Device properly powered on.
	OFF	Device not powered on.

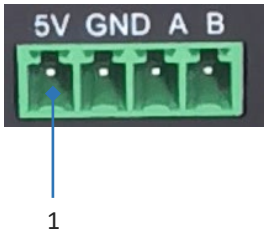
1.8.6 System LED

LED	LED Status	Description
SYS	Solid on	System working properly.
	Blinking at 3Hz	System boot / firmware upgrade / app installation in progress; device reset / factory reset.
	OFF	System boot failure; system anomaly.

1.8.7 Error LED

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

1.9 Serial Port



The HAP101 offers an RS485 connector for serial communication. The default baud rate of the port is 9600, and the pinout description is as follows:

Table 1-4

No.	Signal	Device name	Port	Type	Description
1	VCC	/dev/ttyS0	COM0	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

The serial port operates in the RS485 mode by default, and can be switched to debug mode for troubleshooting the device. The baud rate for debugging is 57600. It will automatically revert to standard RS485 operation upon each power cycle.

The operation mode swap involves uncovering the device and may expose the device to unauthorized access; therefore, it will not be described here.

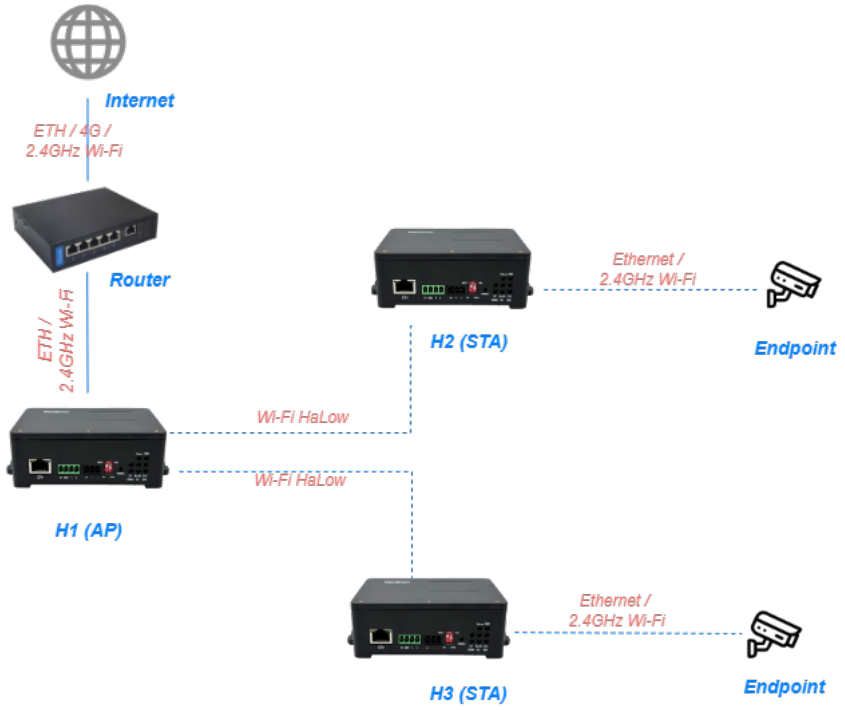
CHAPTER 2 GETTING STARTED

2.1 Network Architecture

The HAP101 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 HaLow unit to be installed in a variety of environments and layouts.

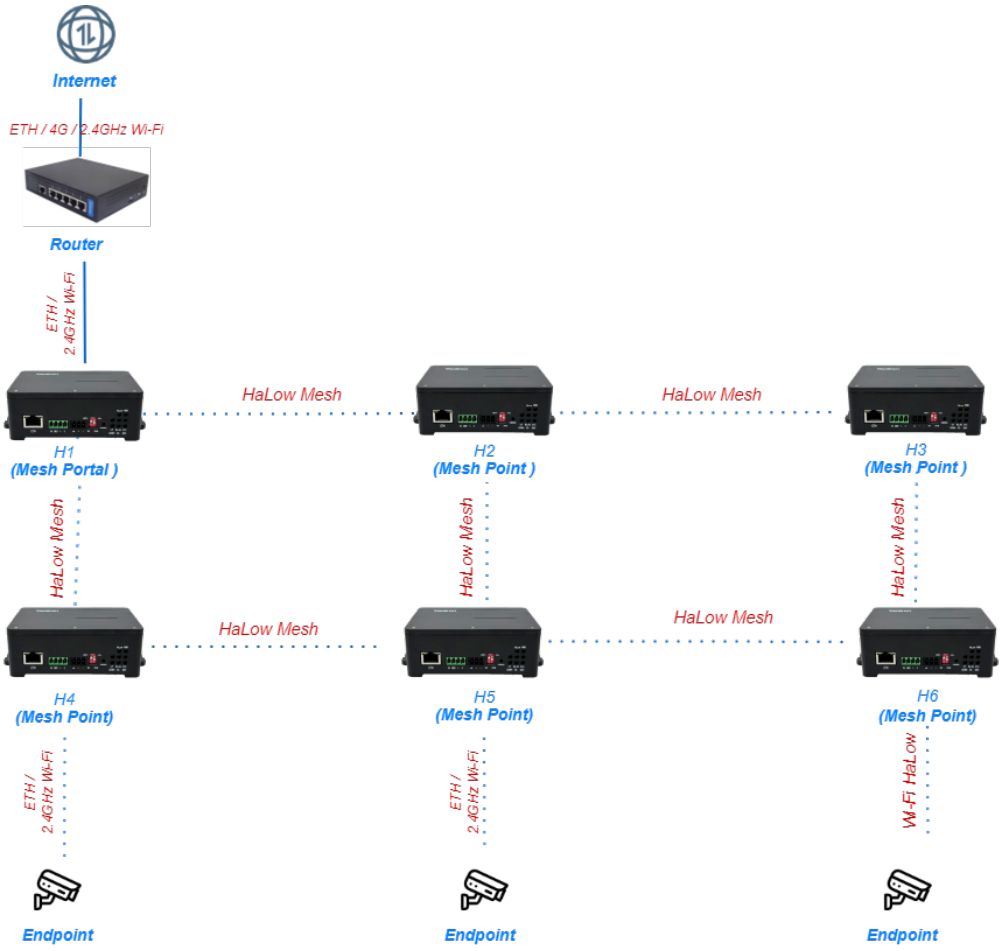
2.1.1 Standard HaLow Network

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.



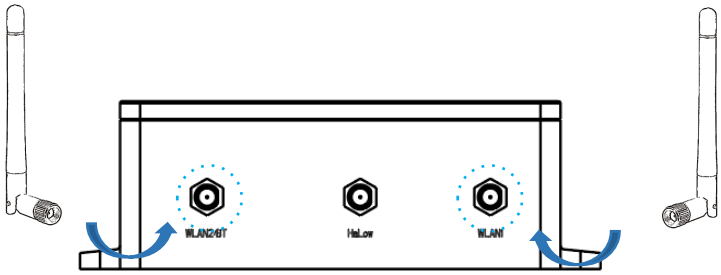
In this topology:

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

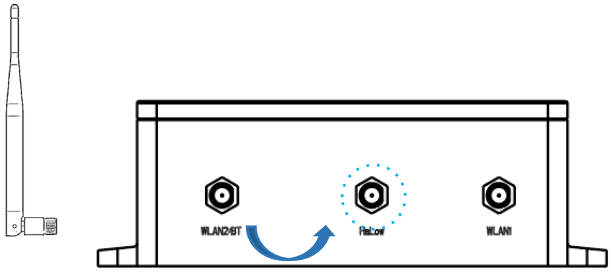
2.2 Setting up the Device

When mounting the HAP101 on a vertical surface, please ensure that 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.

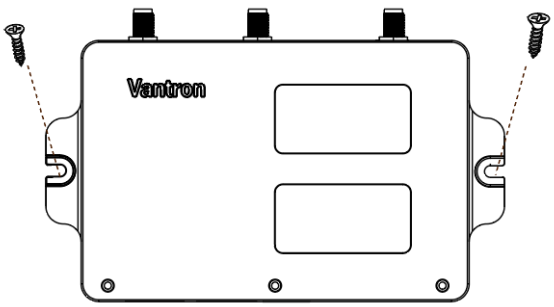
1. Install the shorter antennas to the WLAN antenna connectors (*labelled as WLAN1 and WLAN2/BT*).

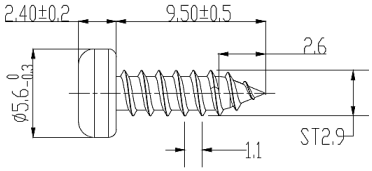


2. Install the longer antenna to the Wi-Fi HaLow antenna connector (*labelled as HaLow*).

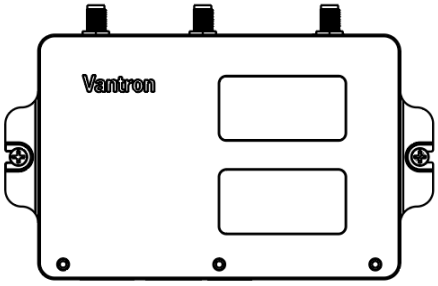


3. Depending on the material of the mounting surface, use two ST2.9 self-tapping screws (for mounting surfaces without provided screws) or two M3 x 8mm screws (for mounting surfaces with provided screws) to fix the device on the mounting surface.

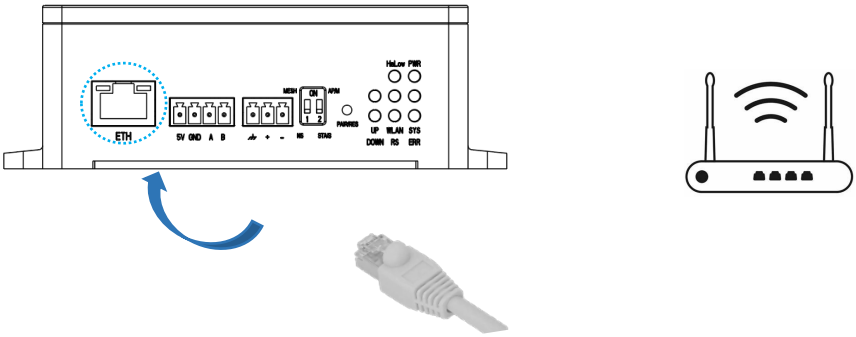




4. Tighten the screws and gently swing the device to make sure it is fastened.



5. When needed, connect the WAN port to a router using a standard Ethernet cable.



Note: The HAP101's Ethernet jack defaults to LAN mode.

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 PWR, WLAN, HaLow, and SYS indicators will turn on.

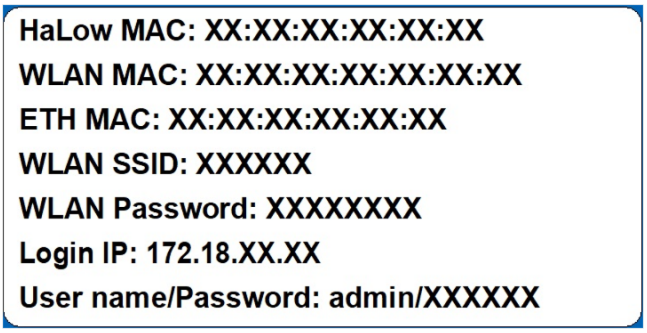


2.4 Quick Access to the Device

By default, the Ethernet port is configured to **LAN** mode and the 2.4 GHz Wi-Fi operates in **AP mode**. On power-up, the device can be accessed through either Ethernet or 2.4 GHz Wi-Fi.

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

Note: The default WLAN SSID & password, login IP address, and login credentials are all printed on the device label.



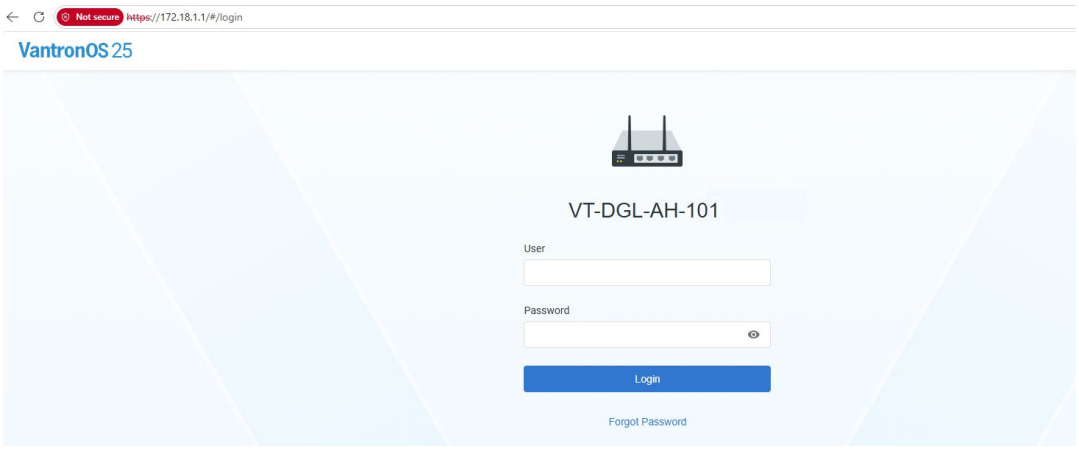
1. Connect the Windows PC or mobile device:
   - Via Ethernet

     Connect the PC or mobile device directly to the HAP101's Ethernet port using a standard Ethernet cable.
   - Via Wi-Fi

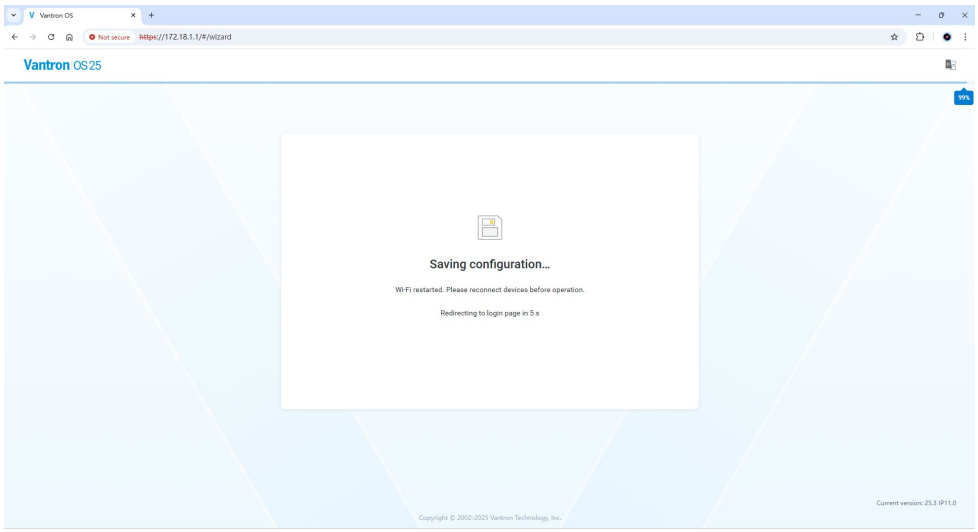
     Connect the PC or mobile device to the HAP101's 2.4 GHz Wi-Fi using the default WLAN SSID and password provided on the device label.
2. Enter the login IP in the browser for device login.

   *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 Wi-Fi AP SSID, encryption mode, and password
   - 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 HAP101 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

Table 2-1 **Default** Network Interface Status

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

Whenever you modify the network interface status, ensure at least one link — either 2.4 GHz Wi-Fi or Ethernet — operates in LAN mode to allow smooth device login.

2.6 DPP Pairing

DPP pairing refers specifically to the fast provisioning of HaLow devices for a standard HaLow connection.

The following sections describe the available DPP pairing options. You can pair two devices that are both configured via hardware or software setup, or mix methods by configuring one via hardware and the other via software in VantronOS.

When necessary, refer to Sections 1.6 and 1.7 for the definitions of the DIP switches and the Pair/Restart button, respectively.

Notes:

1. Ensure there is **no** IP conflict between the two units, as Vantron communication devices use **172.18.1.1** as the default LAN IP address.
2. Activate DPP state on the AP-mode unit first, then on the STA-mode unit. Endure the time window is less than 120 seconds.
3. A standard HaLow network shall contain only one HaLow AP. Each pairing process enrolls exactly one AP with one STA. To add additional STAs to the network, simply repeat the DPP pairing steps between the same AP and each new STA individually.

2.6.1 Pairing via Hardware Seup

With the DIP switches in the correct position, pressing the pair/restart button confirms the hardware setup and enables the DPP state, which remains active for a maximum of **120** seconds.

Table 2-4 DIP Switch Setup for DPP Pairing

Device	Switch 1	Switch 2	Description
H1	Non-mesh (up)	AP/Portal (up)	HaLow DPP state enabled in the HaLow AP mode upon button action.
H2	Non-mesh (up)	STA/Point (down)	HaLow DPP state enabled in the HaLow STA mode upon button action.
Hn	Non-mesh (up)	STA/Point (down)	HaLow DPP state enabled in the HaLow STA mode upon button action.

Follow the procedure below for a DPP pairing:

1. Prepare two HAP101 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. Configure the DIP switches for H1 (AP) and H2 (STA) as indicated in Table 2-4 above.
3. Short press (< 1s) the Pair/Restart button on H1 **first** to activate the pairing mode.
4. Repeat step 3 on H2. Make sure the time interval between button actions on both devices is within 120 seconds.
5. Upon successful connection, both devices exit HaLow DPP mode, with the HaLow LED and Up/Down LED blinking regularly.

   AP: HaLow LED + Down LED; STA: HaLow LED + Up LED

6. Repeat above steps for the same AP (H1) and each new STA (Hn), if applicable.
7. Move the devices to the desired locations after pairing completes.

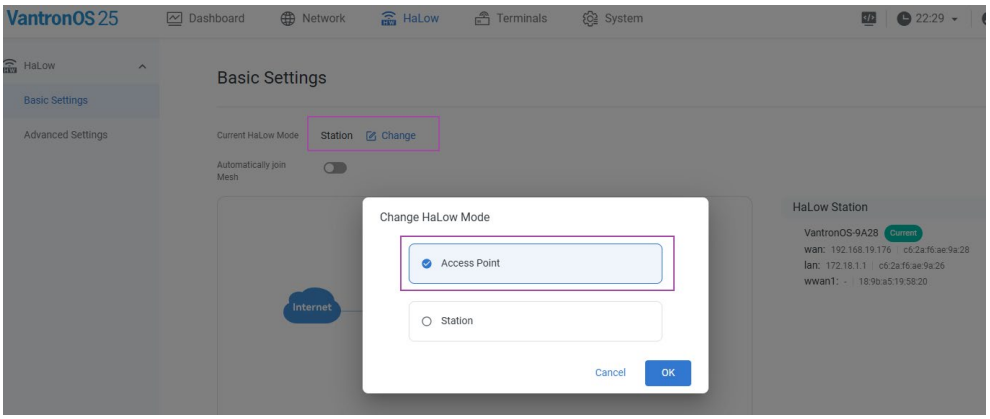
2.6.2 Pairing via Software Setup

The software setup is performed via the VantronOS web management portal. All HAP101 units are factory set to HaLow STA mode. **The following procedures apply to two HAP101 units that both start in HaLow STA mode**.

1. Prepare two HAP101 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 HAP101 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 HAP101 unit (H2).

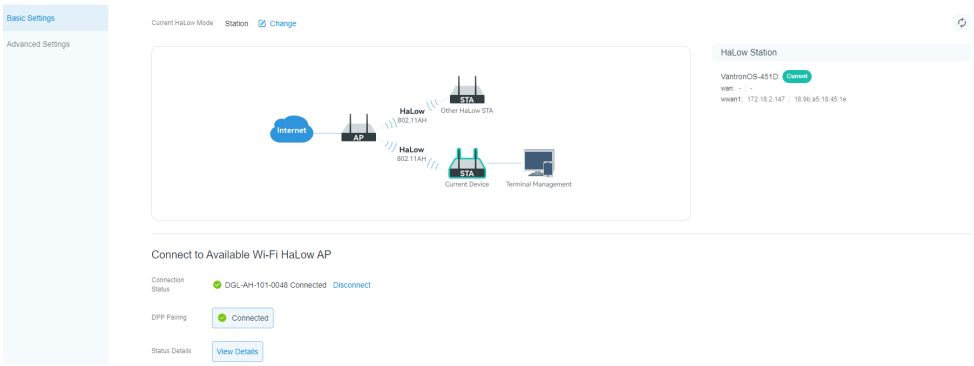
   We recommend using a separate PC or mobile device for this login operation.

6. Navigate to the **HaLow > Basic Settings** page in VantronOS for H2.
7. Activate DPP pairing state on both devices:

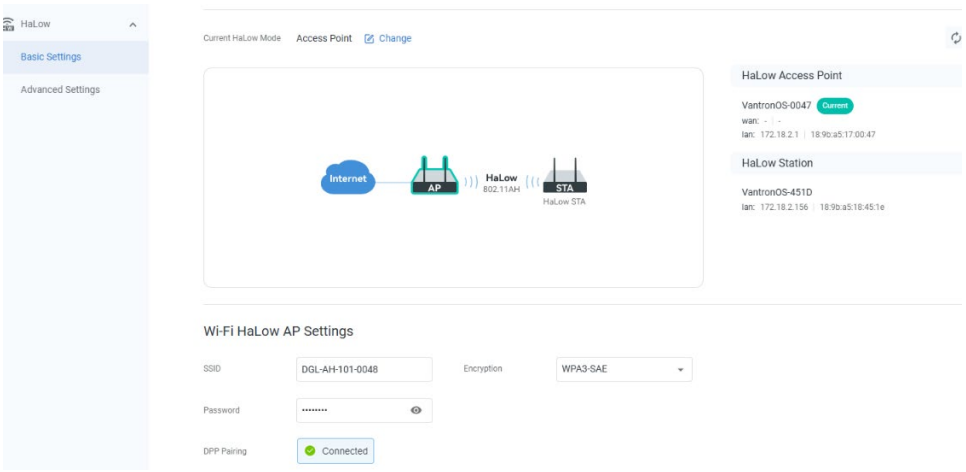
   - Enable the DPP state on the AP-mode unit (H1) **first**: Under the **Wi-Fi HaLow AP** section, click the **Pair** button next to **DPP Pairing**.
   - Immediately operate the STA-mode unit (H2): Under the **Connect to Available Wi-Fi HaLow AP** section, click the **Connect** button next to **DPP Pairing**.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

2.6.3 Exiting DPP Pairing Mode

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

- A standard HaLow connection is successfully established.
- The second unit does not activate pairing mode within the **120-second** window following the first unit.
- The HaLow connection between the two devices fails.

2.7 Quick Mesh Networking

In the current product design, the HaLow mesh network is **built on top of a standard Wi-Fi HaLow network**, where the AP serves as the MPP (Mesh Portal) and the STA serves as the MP (Mesh Point). A standard HaLow link must therefore exist between the target units before the mesh configurations are enabled.

By default, HAP101 units are pre-configured with the same mesh settings, such as mesh ID, encryption mode, and password. Units sharing these settings join the same mesh network.

- For a HaLow AP: Enabling mesh configurations designates this AP as the MPP, which allocates IP addresses for all nodes across the mesh network.
- For HaLow STAs: After the mesh configurations are enabled, the STAs automatically scan for the mesh network hosted by the AP they are associated with. They then operate as MPs and use the IP addresses assigned by that AP as their mesh IP.

Table 2-5 DIP Switch Setup for Quick Mesh Networking

Device	Switch 1	Switch 2	Description
H1	Mesh	AP/Portal	HaLow mesh configuration enabled for the MPP.
H2	Mesh	STA/Point	HaLow mesh configuration enabled for the MP.
Hn	Mesh	STA/Point	HaLow mesh configuration enabled for the MP.

Follow the procedure below to establish a HaLow mesh network on top of an existing standard HaLow network.

1. Connect HaLow STAs (H2, … Hn) to a HaLow AP (H1) via Wi-Fi HaLow.
2. Configure the DIP switches for H1, H2, … and Hn as indicated in Table 2-5.
3. Press the Pair/Restart button to activate HaLow mesh configurations on the devices.

   No time window applies between button actions.
4. Additional HaLow STAs within the original HaLow network can be added to the mesh network at any time by configuring the DIP switches and pressing the Pair/Restart button.

After the HaLow mesh network is established:

- The MPP's Ethernet port switches to WAN mode, allowing it to connect to a router for internet access. Device management is accessible via 2.4 GHz Wi-Fi or MP's Ethernet LAN.
- The MP's Ethernet and 2.4 GHz Wi-Fi interfaces are bridged to the HaLow interface. Device management is accessible via 2.4 GHz Wi-Fi or Ethernet LAN using the IP retrieved from the MP's route table.

2.8 SSH and Serial Console Access

SSH is enabled on the HAP101 by default. Prior to establishing an SSH connection, make sure the PC (client) can reach the HAP101's (server) IP.

Table 2-6 Access Options

Method	PC Connection	Login Address/Parameters
Option 1	Connected to HAP101's LAN network (via Ethernet or 2.4 GHz Wi-Fi).	HAP101's LAN IP
Option 2	Connected to HAP101's debug port (serial session rather than SSH).	57600, 8N1

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

Option 1 applies in most cases.

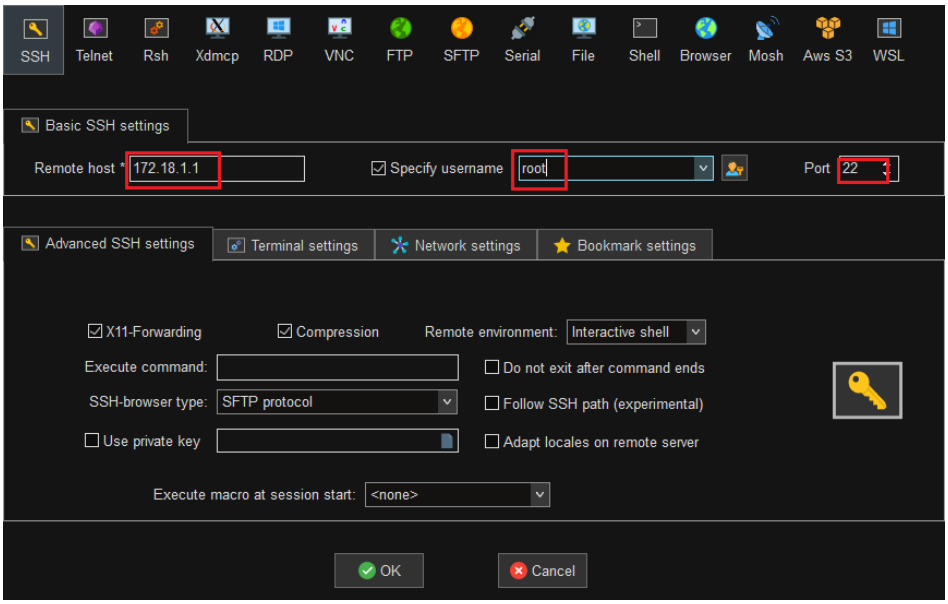
Option 2 involves uncovering the device and may expose the device to unauthorized access. Therefore, the procedure for this option is not covered in this document.

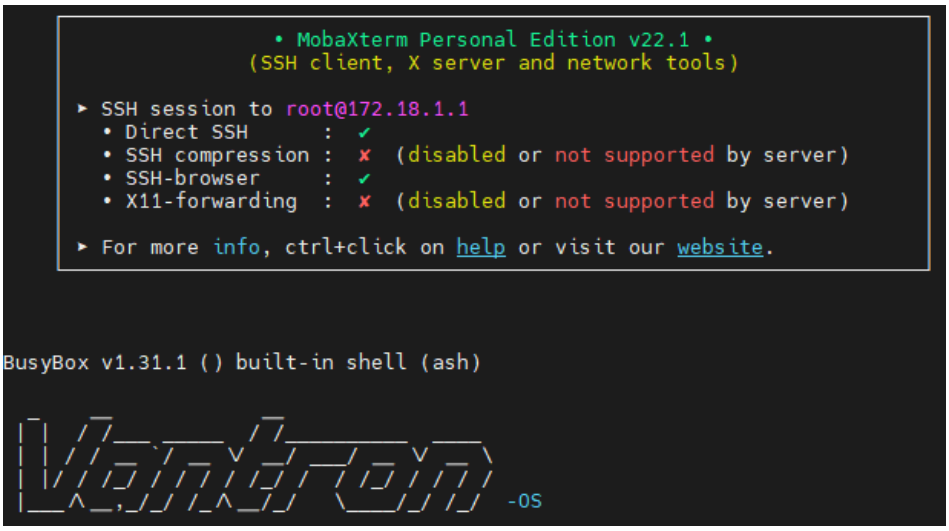
Steps for SSH login via LAN IP:

1. Connect the PC to HAP101's LAN network via Ethernet or 2.4 GHz 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.*

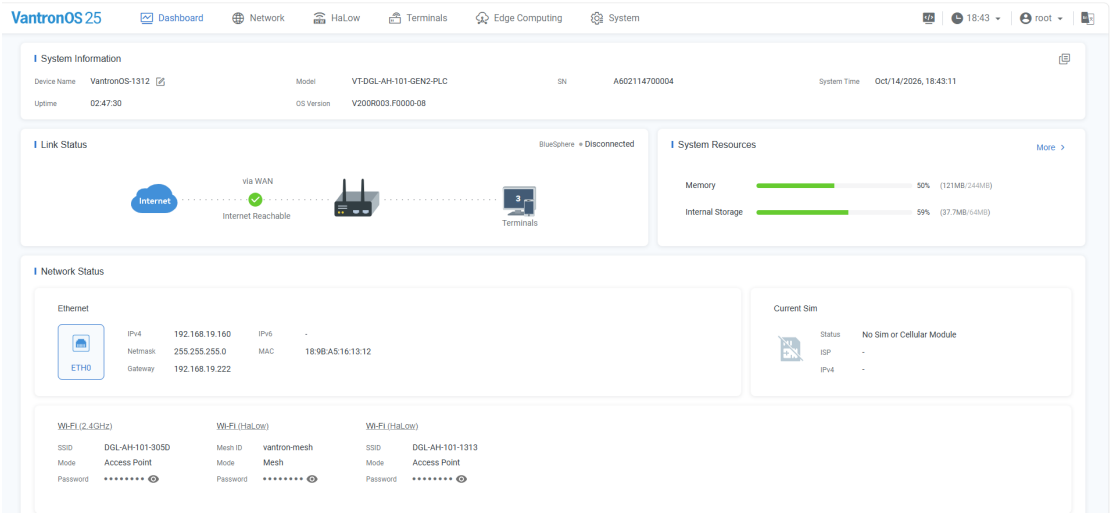
CHAPTER 3 DEVICE SETUP IN VANTRONOS

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 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.

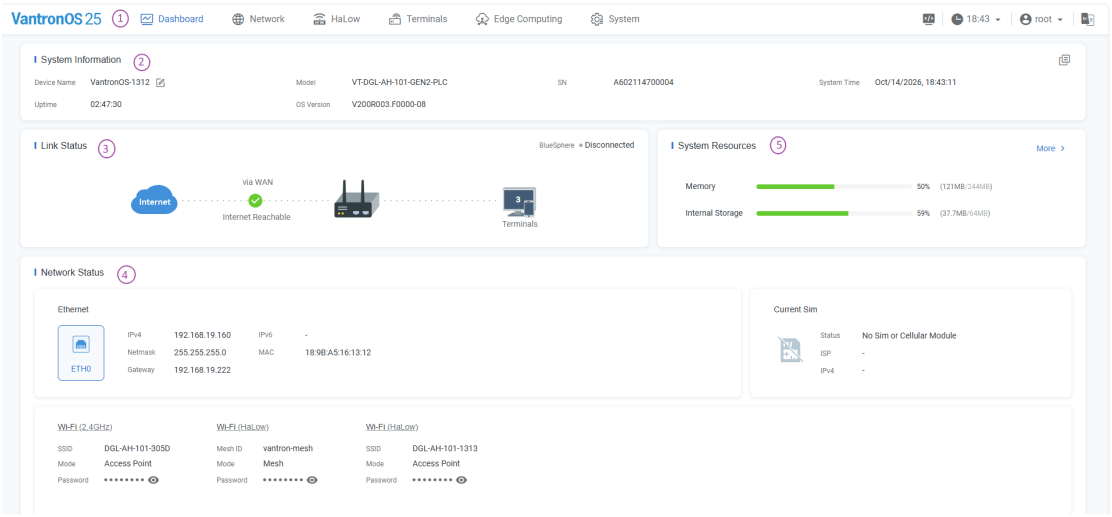
3.1.2 Log Out

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

The **Dashboard** provides overall information of the HAP101, 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.
4. **Network Status** — Displays the live status for each network interface.
   - Ethernet: Active ports are highlighted in blue, with IPv4 and IPv6 addresses, subnet mask, gateway, and MAC address displayed for the selected port.
   - 2.4 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 HAP101).
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 WAN/LAN interface settings, 2.4 GHz Wi-Fi settings, 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 HAP101 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.

Changing an interface's operating mode (e.g., LAN to WAN) may disrupt local network access. If this occurs, reconnect your host PC to an active LAN interface (for example, switch from the wired Ethernet connection to the Wi-Fi AP) to regain access to the device.

To ensure successful device login, **at least one LAN** connection—either Ethernet LAN or 2.4 GHz Wi-Fi AP—should be kept active.

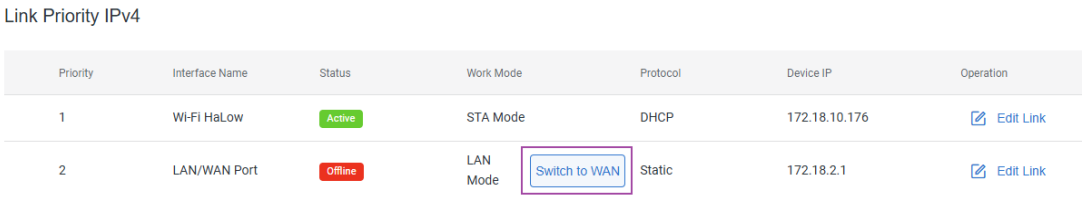
3.3.1 Ethernet Mode Switch

The Ethernet port defaults to **LAN** mode for local management access. When configured to WAN mode, it serves as the uplink to an external network.

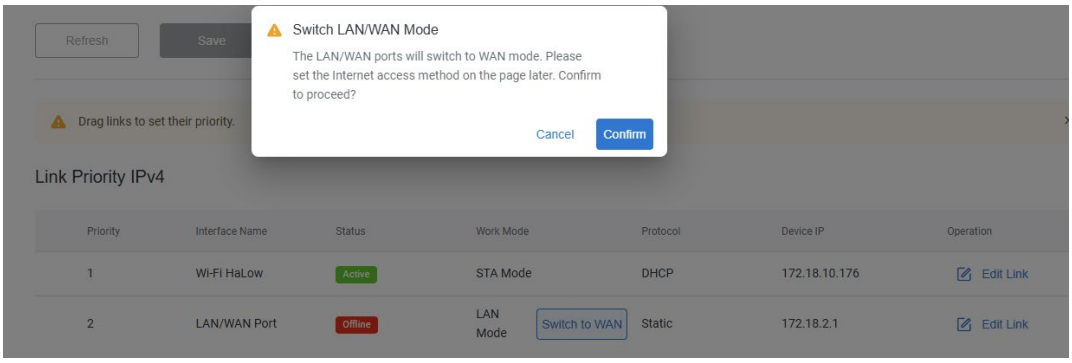
Unplug the Ethernet cable prior to changing the Ethernet mode. This ensures the new network settings apply properly.

To manually switch the mode of the Ethernet port:

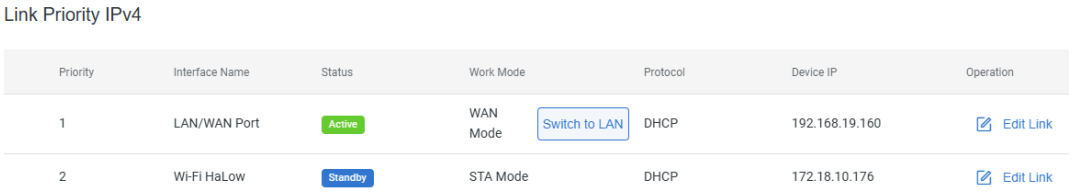
1. Ensure the 2.4GHz Wi-Fi operates in AP mode to maintain local access to the device.
2. Navigate to **Network > Interface > WAN**.
3. Under **Link Priority IPv4**, click **Switch to WAN/LAN** next to the Ethernet port's work mode.



4. Click **Confirm** in the pop-up window to apply the change.



5. Reconnect the PC over 2.4 GHz Wi-Fi if you were previously using the Ethernet LAN.



3.3.2 WAN Interface

The WAN interface page includes the following functionalities:

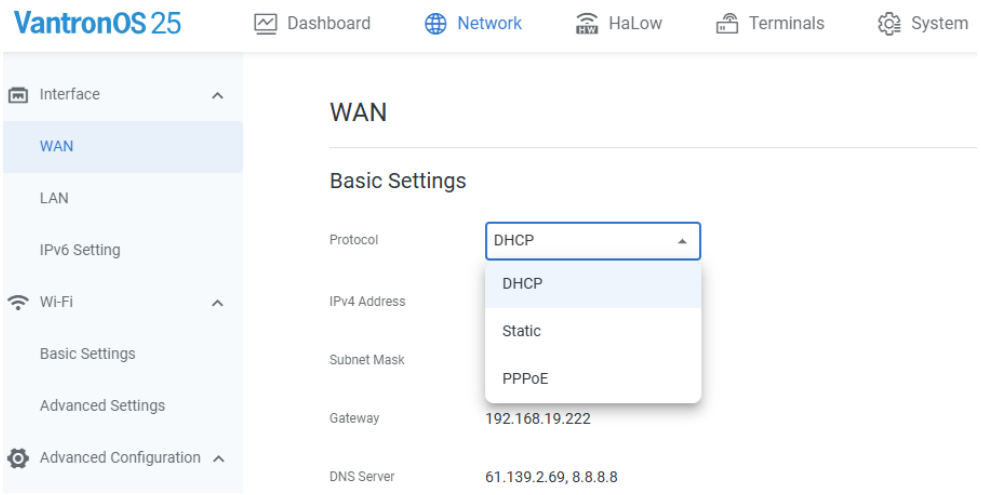
1. **Basic IP configuration** – Selects the IP protocol for the Ethernet WAN interface (e.g., DHCP, Static IP).
2. **Interface bridging** – Places all interfaces into the same Layer 2 bridge for transparent forwarding, with the selected interface serving as the uplink, and allows upstream DHCP to assign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

Whenever you make a change, always ensure the host PC and the HAP101 are on the same subnet for smooth VantronOS login.

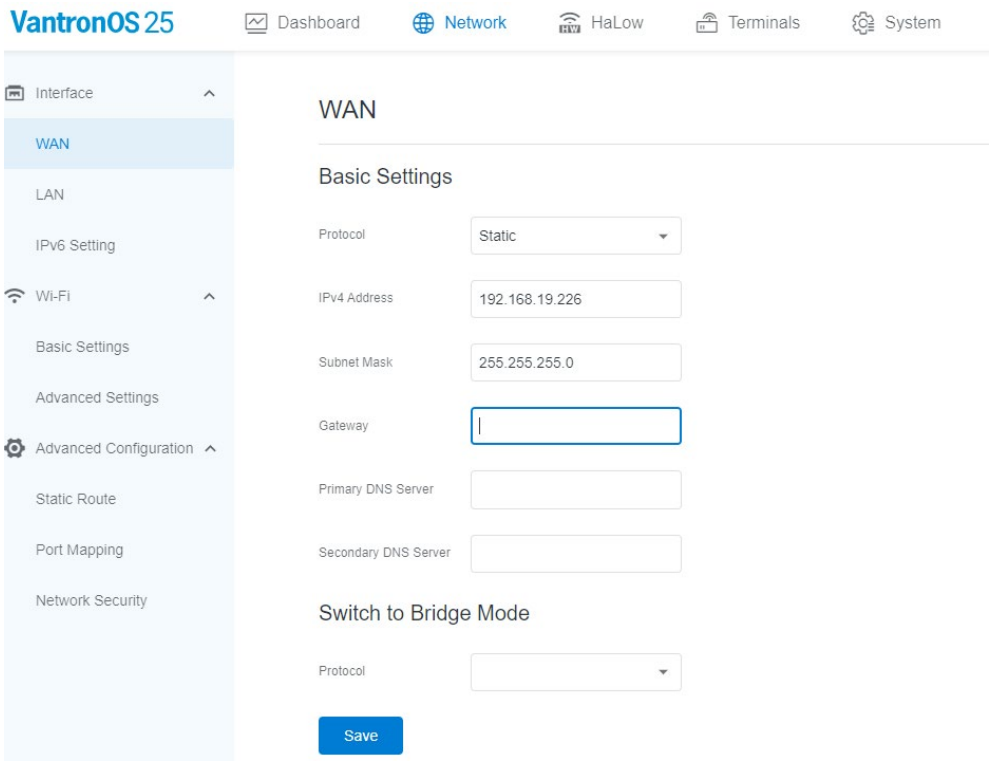
*Basic IP configuration and interface bridging are available when the Ethernet port operates in **WAN** mode. We recommend using the 2.4 GHz Wi-Fi AP for device management while configuring the Ethernet port.*

3.3.2.1 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, inducing the IP address, subnet, gateway, and DNS.



3.3.2.2 Interface Bridging

Interface bridging on the HAP101 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.

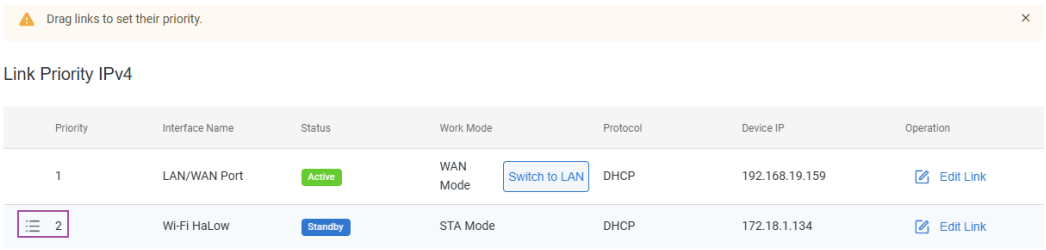
- After bridging is enabled, LAN interfaces **no longer** provide NAT and DHCP services to connected endpoints.
- When you bridge either the Ethernet WAN or Wi-Fi STA interface, the selected interface becomes the uplink. All other interfaces are moved into the same Layer 2 bridge, leaving the device 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 router.
- For HAP101 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 Wi-Fi interface, available SSIDs will be displayed for quick connection.
- To **cancel interface bridging**, enable the **DHCP service** on the **Interface > WAN** page, or use the DIP switch + Pair/Restart button for a working mode change. You may need to log back into the device using its original LAN IP after DHCP service is re-enabled.

3.3.2.3 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.

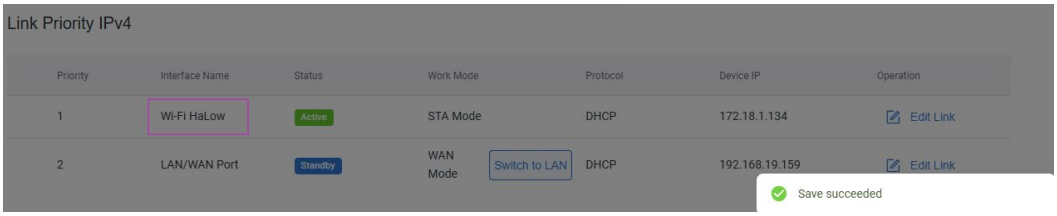
To manually set the network priority:

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



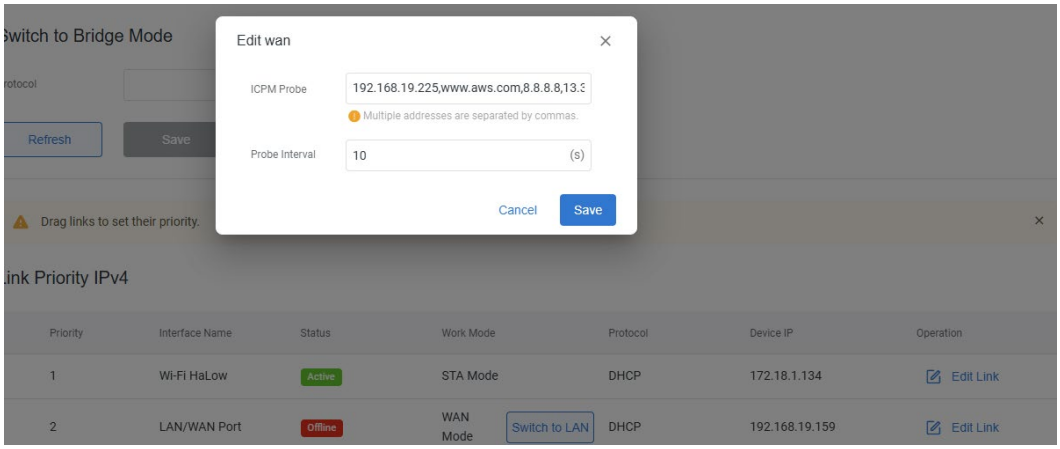
The screenshot is for illustration only. In a typical deployment, individual HaLow stations would not be connected as standalone units to an external network.

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.*

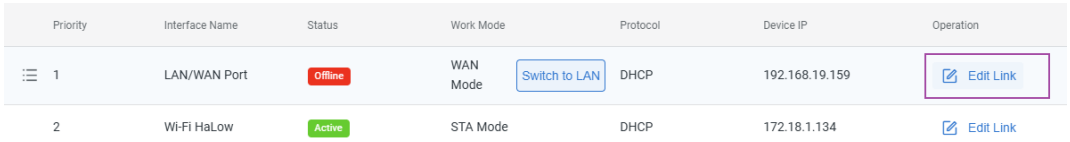
3. Use the **Edit Link** option to modify the probe settings for the link as needed.



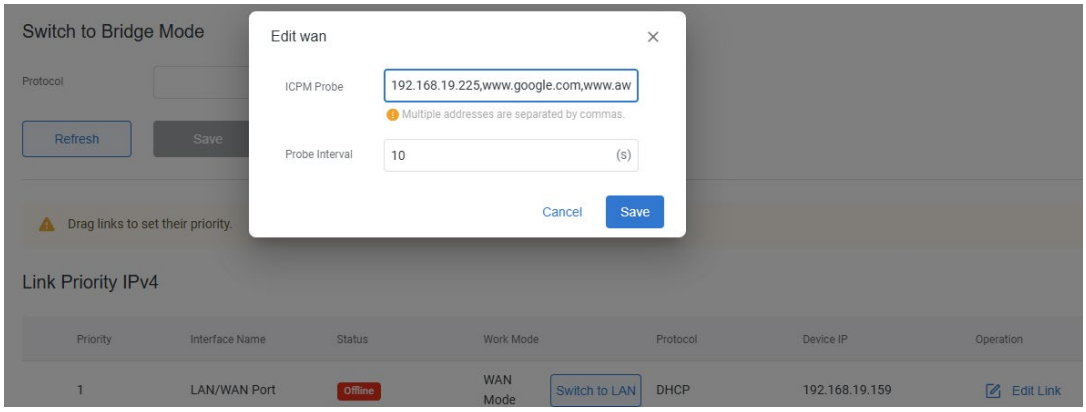
3.3.2.4 Link Diagnosis

When a link is shown as **Offline**, first make sure 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.

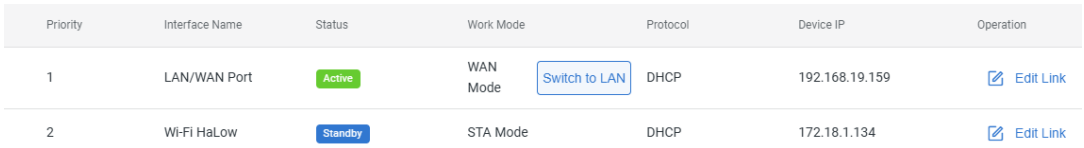
1. Locate the target link, and click **Edit Link**.



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.



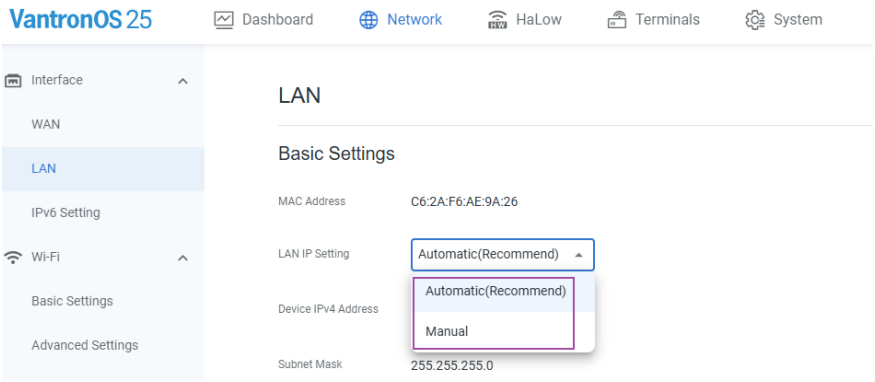
3. Check the link status to verify if it becomes reachable.



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

3.3.3 LAN Interface

The HAP101 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.



3.3.3.1 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 HAP101's uplink interface, and its factory LAN address (172.18.1.1) overlaps with the HAP101's default LAN subnet.

As a best practice, we recommend reconfiguring the HAP101'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.

3.3.3.2 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**:

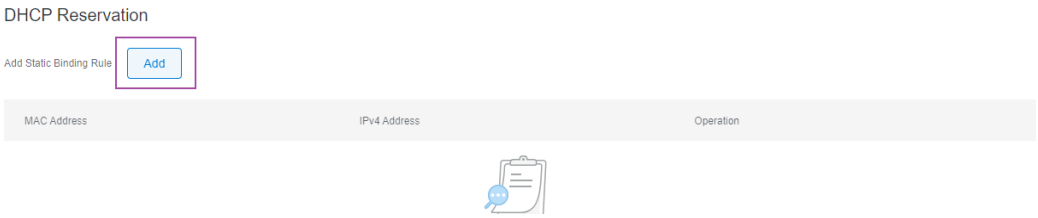
- Start & End addresses: IP addresses within this range are leased to clients.
- Lease Time: The valid duration for which the HAP101, as the DHCP server, assigns an IP address to a client. Before expiry of the lease time, the client will send a renew request to the HAP101 to extend the lease. If the 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.

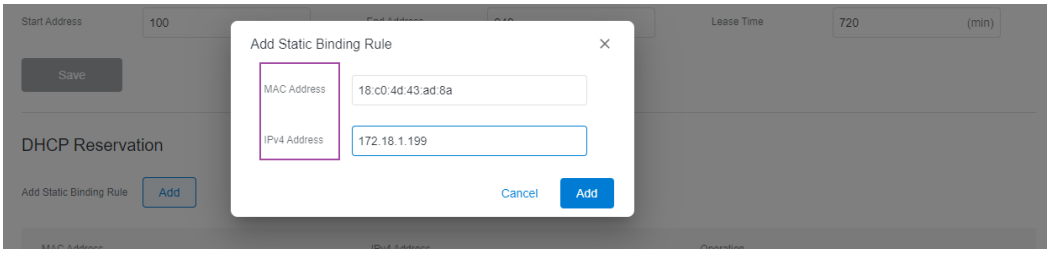
By adding a DHCP reservation rule to the HAP101, the specified client device will maintain the allocated IP address to reduce configuration errors.

Steps of adding a DHCP reservation rule:

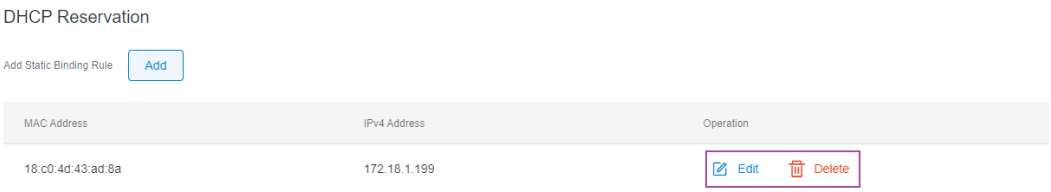
1. After enabling the DHCP service, click **Add** under **DHCP Reservation**.



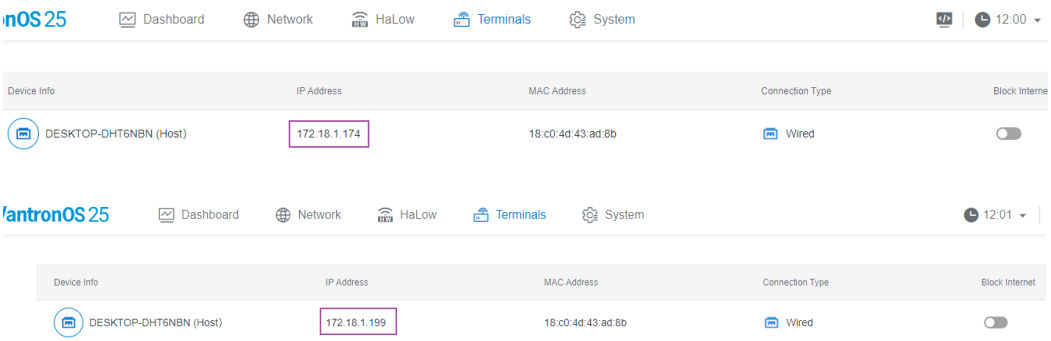
2. Enter the client's MAC address and allocate an IP on the same subnet as the HAP101.



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



4. If you have reserved a different IP for a connected device, reconnect the device to the HAP101, and its IP will update accordingly as shown under **Terminals**.



3.3.4 IPv6 Settings

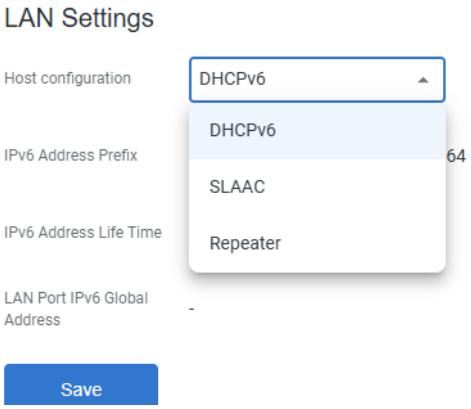
IPv6 (Internet Protocol version 6) is an advanced network layer protocol succeeding IPv4. It is designed to solve IPv4 address exhaustion and support enhanced networking features. It provides 128-bit addresses, eliminating the need for NAT and enabling end-to-end connectivity.

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 HAP101 acts as a stateful DHCPv6 server, assigning full IPv6 addresses to LAN devices with configurable prefix and lease time.
- **SLAAC:** The HAP101 advertises an IPv6 prefix via RA messages. LAN devices automatically generate their own addresses for plug-and-play use.
- **Repeater:** The HAP101 relays upstream IPv6 configurations transparently. LAN devices obtain addresses directly from the upstream network, with no local address assignment.

3.3.5 Wi-Fi

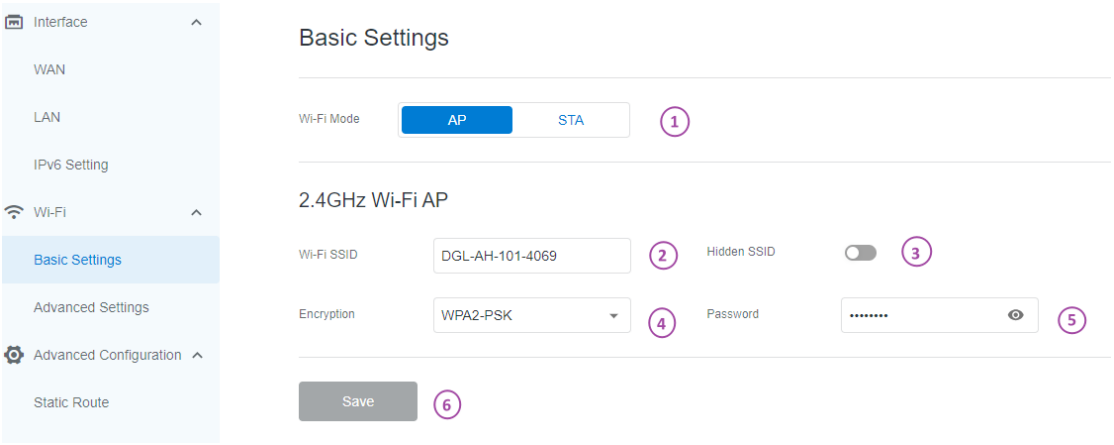
During the initial login wizard, the device's 2.4 GHz Wi-Fi is pre-configured as an access point (AP), and these configurations are retained. Users can modify these settings as needed.

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.

Before switching the 2.4 GHz Wi-Fi operation mode, **ensure** your host PC is connected to the HAP101 via an alternative link (such as Ethernet LAN). Otherwise, you may lose local access to the device.

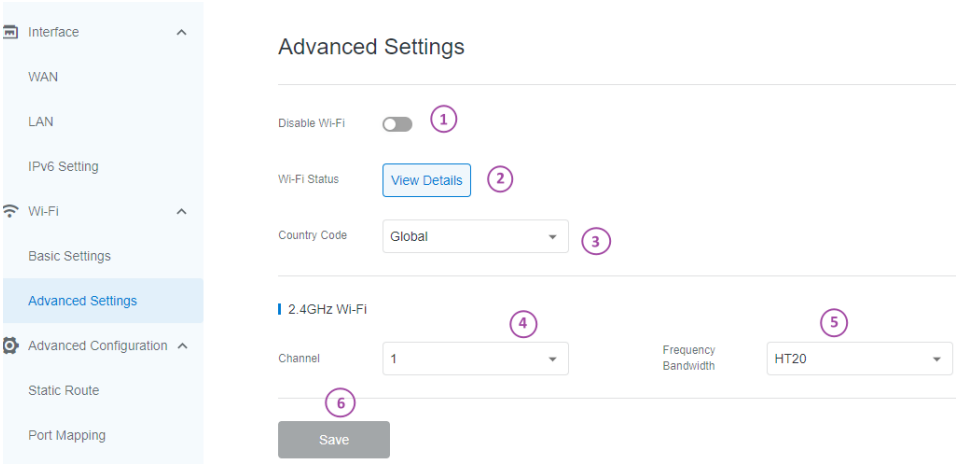
3.3.5.1 AP-Mode Basic Settings



Description:

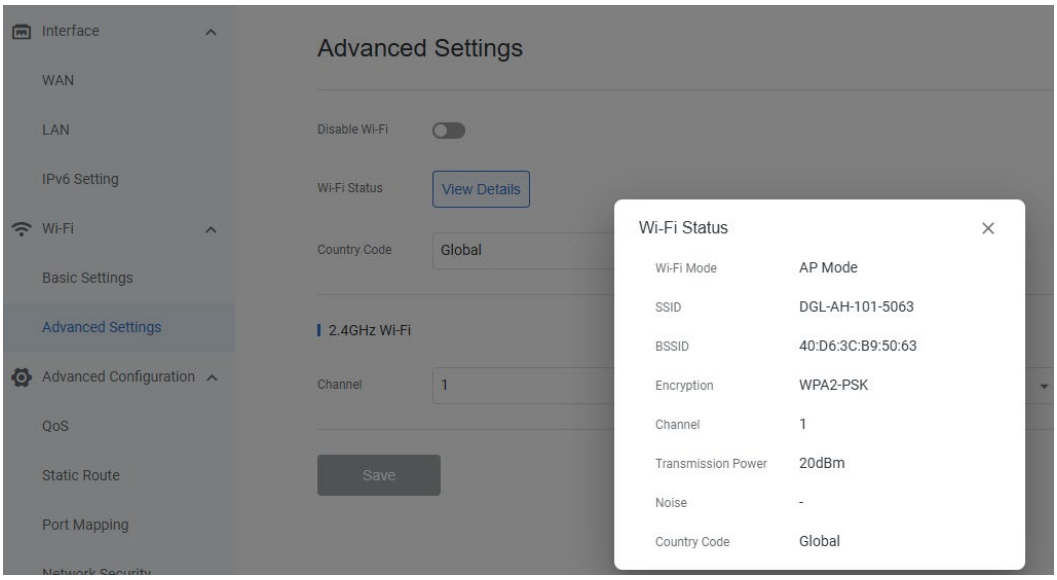
1. The device is factory set to operate in **AP** mode, and you can switch the mode here.
2. Wi-Fi SSID — The Wi-Fi AP's name.
3. Hide SSID — Once hidden, clients cannot scan the device's SSID and must manually enter the exact SSID and password to connect.
4. Encryption mode — The basic protocols for establishing secure communication. (None, WPA-PSK, WPA2-PSK, WPA2-EAP)
5. Password — Credential for connecting the device's Wi-Fi.
6. Click **Save** to allow changes to tack effect.

3.3.5.2 AP-Mode Advanced Settings



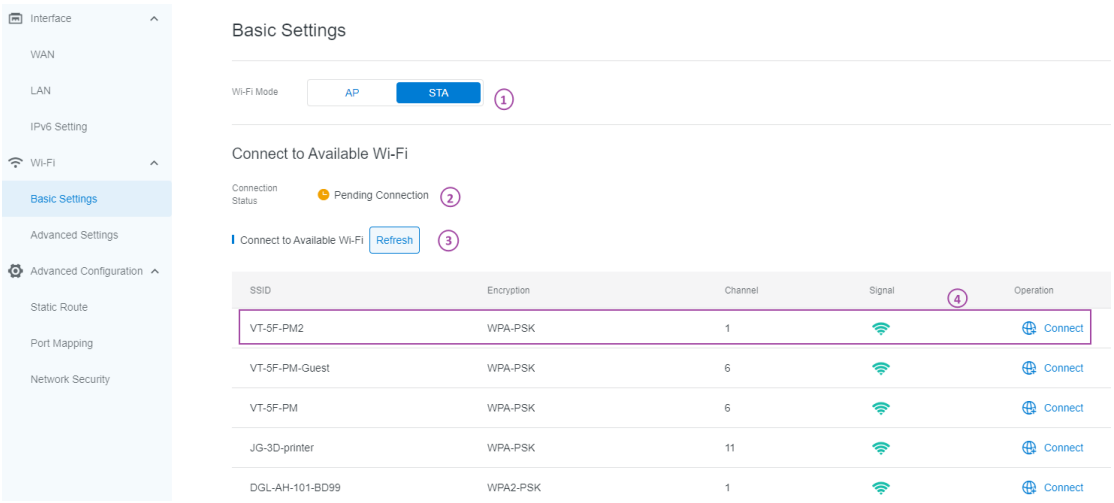
Description:

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



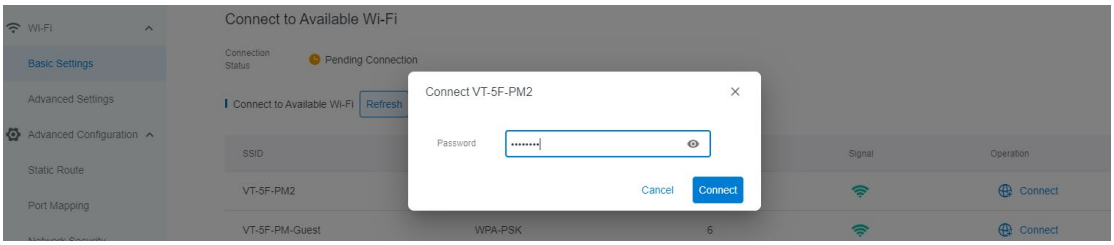
3. Country code (‘global’ by default)
4. Channel options (configurable) and default frequency bandwidth.
5. If you have modified the parameters, click **Save** to apply.

3.3.5.3 Client-Mode Basic Settings

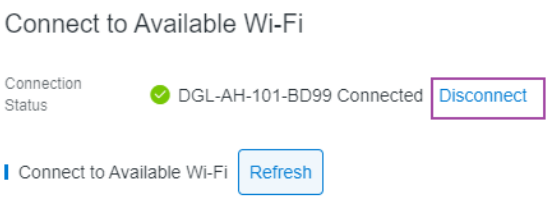


Description:

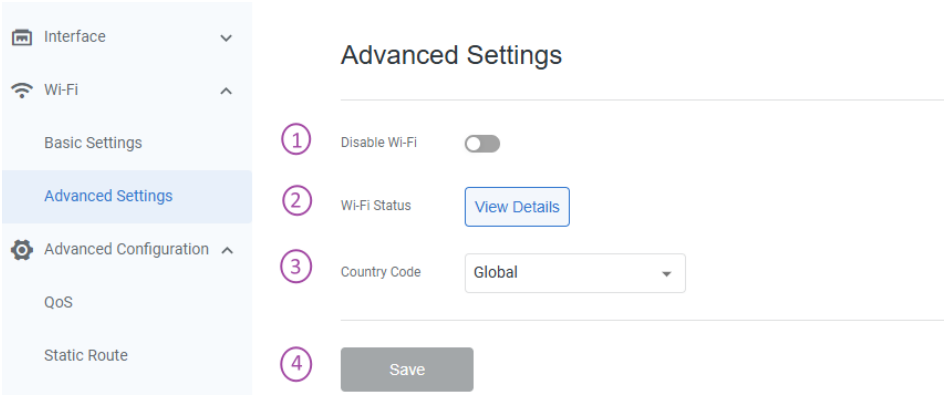
1. Click **STA** and confirm the action in the pop-up to enable the **Client** mode.
2. Current Wi-Fi connection status.
3. If the target SSID is not included in the list, click the button to refresh the list.
4. Information of available Wi-Fi APs is displayed. Click **Connect** and enter the password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



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

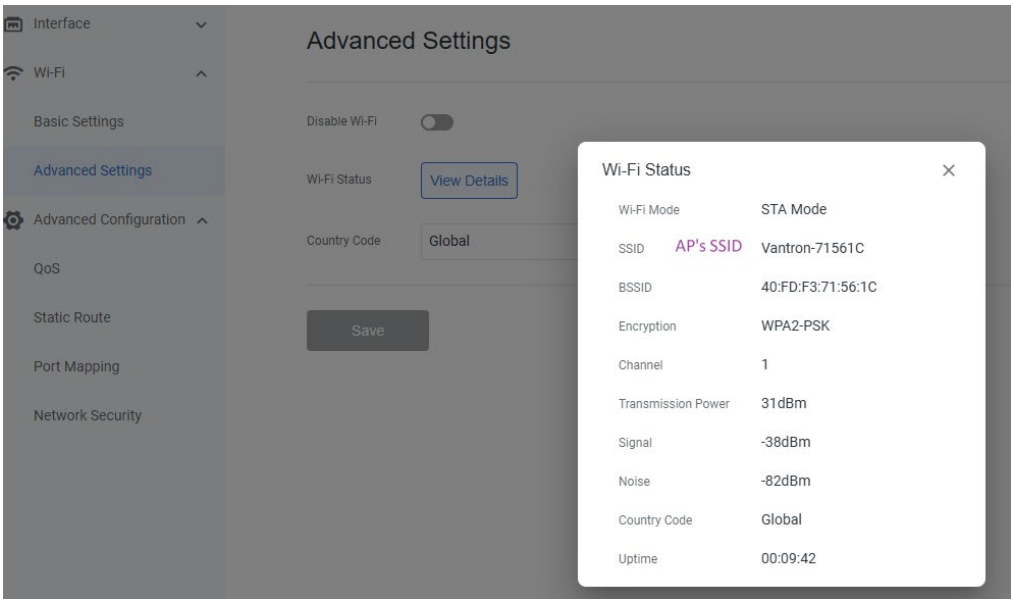


3.3.5.4 Client-Mode Advanced Settings



Description:

1. Disable/Enable the Wi-Fi feature.
2. Wi-Fi Status—Clicking **View Details** displays the detailed connection information of the device, including Wi-Fi mode, and—if connected—the SSID of the target AP, encryption, channel, transmit power, etc.



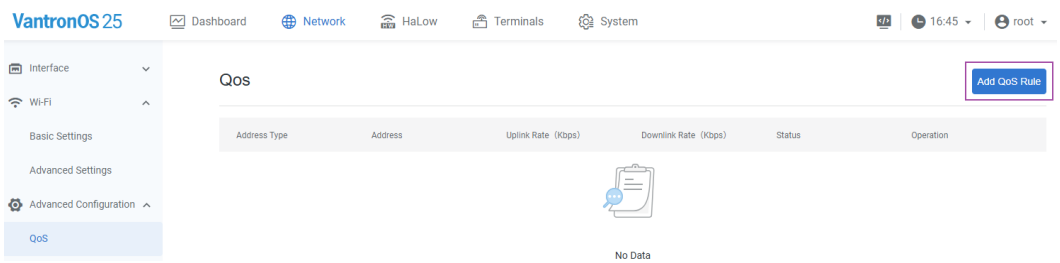
3. Country code (‘global’ by default).
4. If you have modified the parameters, click **Save** to apply.

3.3.6 QoS Bandwidth Control

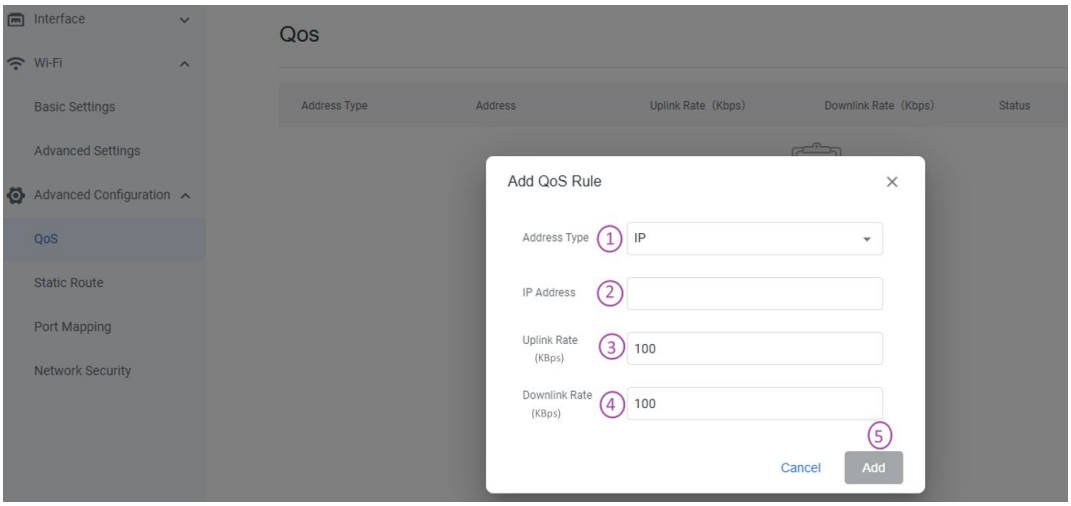
The QoS feature provides fine-grained bandwidth shaping rules to limit uplink and downlink traffic of designated terminals, preventing bandwidth preemption and stabilizing industrial communication quality.

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.

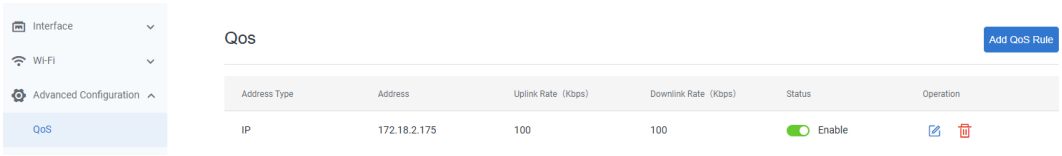
- **IP:** Apply rate limits to a single specified IPv4 device. This option is ideal for precise bandwidth control of key equipment such as PLCs and industrial controllers.
- **IP Range:** Restrict traffic for a continuous IP address range, enabling batch bandwidth control for groups of sensors or surveillance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



3.3.7 Static Route

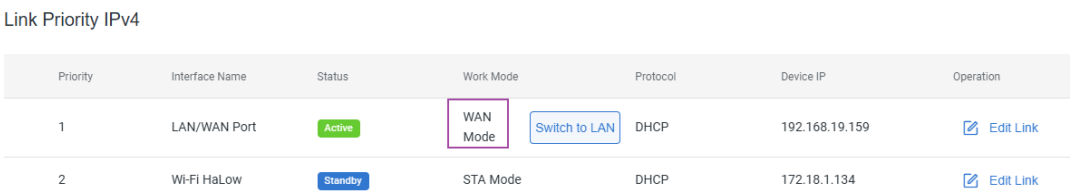
Static routing is a manual network configuration method that uses explicitly defined paths to direct traffic through specific interfaces. This provides precise control over routing behavior and is particularly useful for multi-WAN load balancing, traffic segregation, and backup link configuration.

Example:

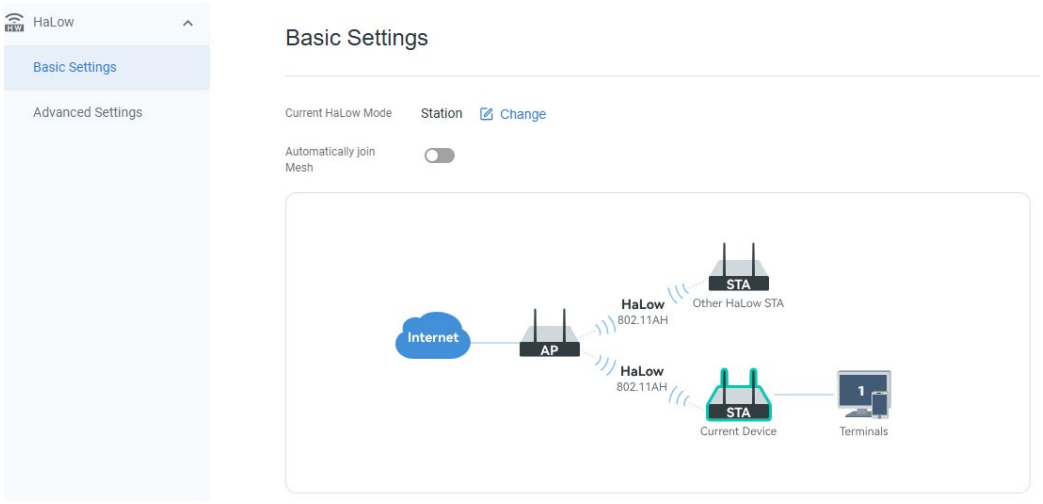
Goal: The device obtains internet access via the Ethernet WAN interface, while HaLow-based data transmission (to a specific remote network or device) is carried out through the HaLow STA interface.

Steps:

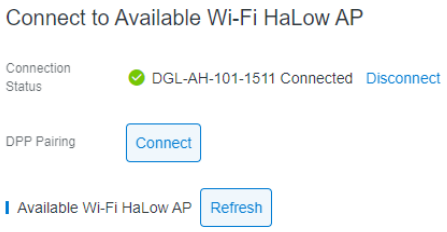
1. Ensure your host PC is connected to the device via 2.4 GHz Wi-Fi AP for local access.
2. Navigate to **Network > Interface > WAN**.
3. In the **Link Priority** section, switch the Ethernet port to WAN mode with DHCP enabled, and designate Ethernet WAN as the primary link.



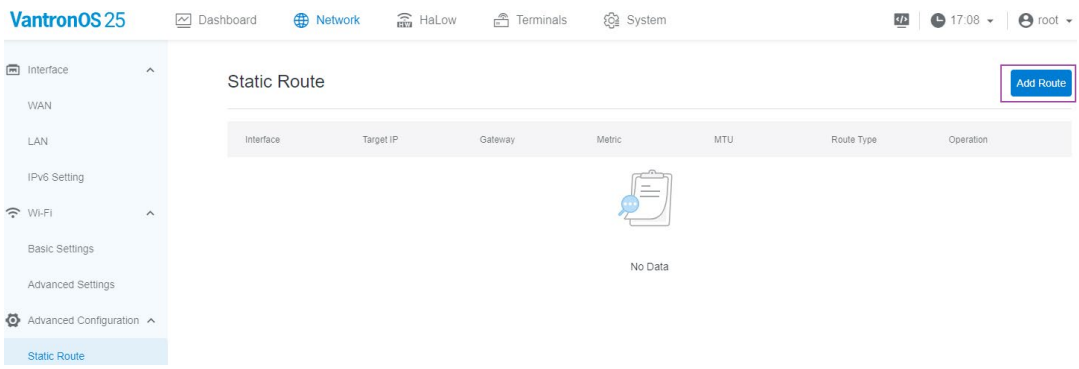
4. Navigate to **HaLow > Basic Settings**, and ensure the device operates in the HaLow STA mode.



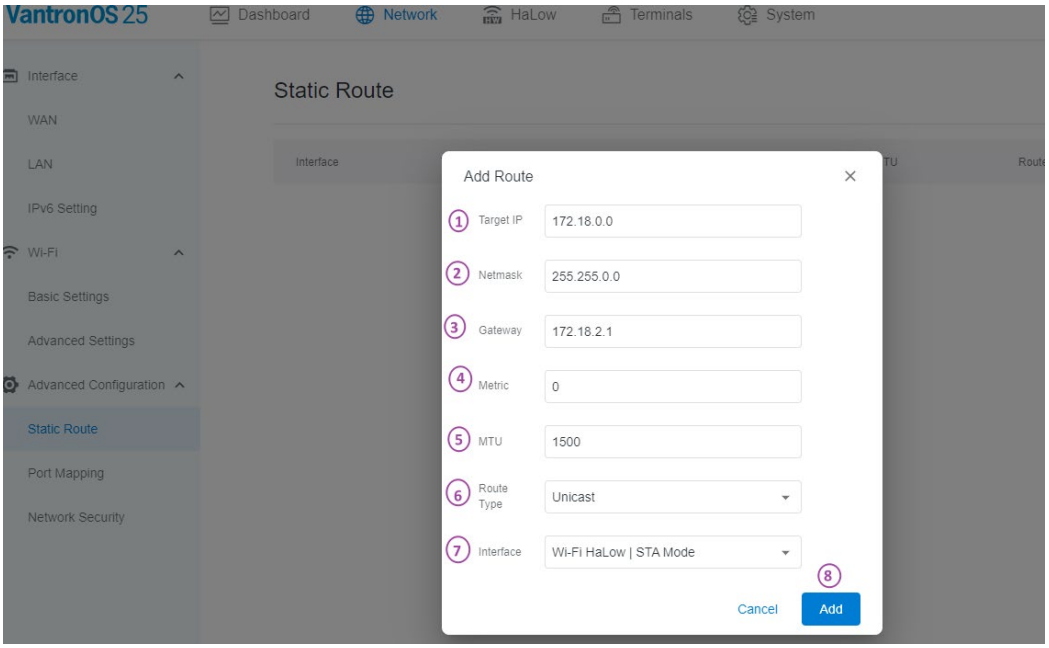
5. Connect the Ethernet port to an external router (primary WAN uplink).
6. Also connect the device to an AP-mode HaLow unit (HaLow uplink).



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



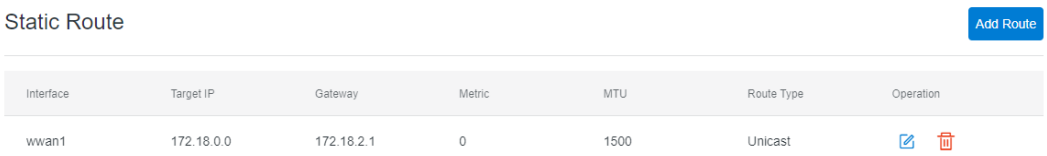
8. Configure the static route with the following parameters:



Description:

1) Target IP address: The destination network you want to reach via HaLow.
2) Netmask: Subnet mask of the destination network.
3) The upstream HaLow AP on the HaLow network.
4) Gateway metric: The smaller the number, the higher the priority.
5) MTU: 1500 by default.
6) Route type (refer to the details in the table below).
7) Select an outbound interface for the route (the interface that leads to the gateway, HaLow STA in this case).
8) Click **Add** to create the rule.

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



*A **return route** is also required on the remote HaLow AP. Otherwise, requests can reach the remote HaLow network, but reply traffic cannot route back to endpoints on the local LAN.*

Table 3-1 Description of the route type:

Type	Description
Unicast	The route entry describes real paths to the destinations covered by the route prefix.
Local	The destinations are assigned to this host. The packets are looped back and delivered locally.
Broadcast	The destinations are broadcast addresses. The packets are sent as link broadcasts.
Multicast	IP datagrams are sent to a group of interested receivers in a single transmission. It is not present in normal routing tables.
Unreachable	The destinations are unreachable. Packets are discarded and the ICMP message of host unreachable is generated. The local senders will receive an EHOSTUNREACH error.
Prohibit	The destinations are unreachable. Packets are discarded and the ICMP message of communication administratively prohibited is generated. The local senders will receive an EACCES error.
Blackhole	The destinations are unreachable. Packets are discarded silently. The local senders will receive an EINVAL error.
Anycast	The destinations are any cast addresses assigned to this host. They are mainly equivalent to local with one difference that such addresses are invalid when used as the source address of any packet.

3.3.8 Porting Mapping

Port mapping is a NAT-based technique that redirects traffic arriving on an external **port** combination to a different (internal) **IP:port**—typically from a public address/port on a router/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:

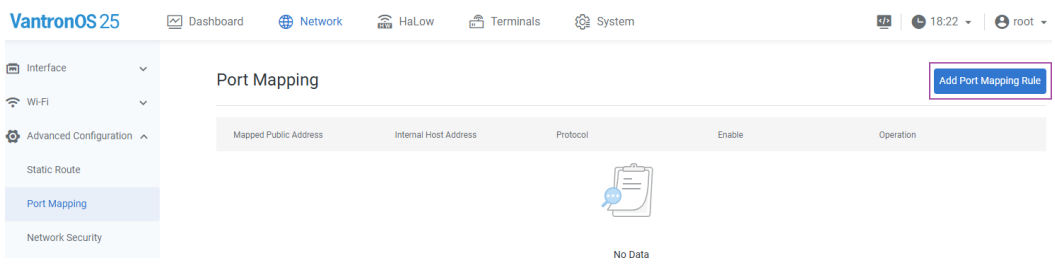
Scenario:

- The HAP101 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.

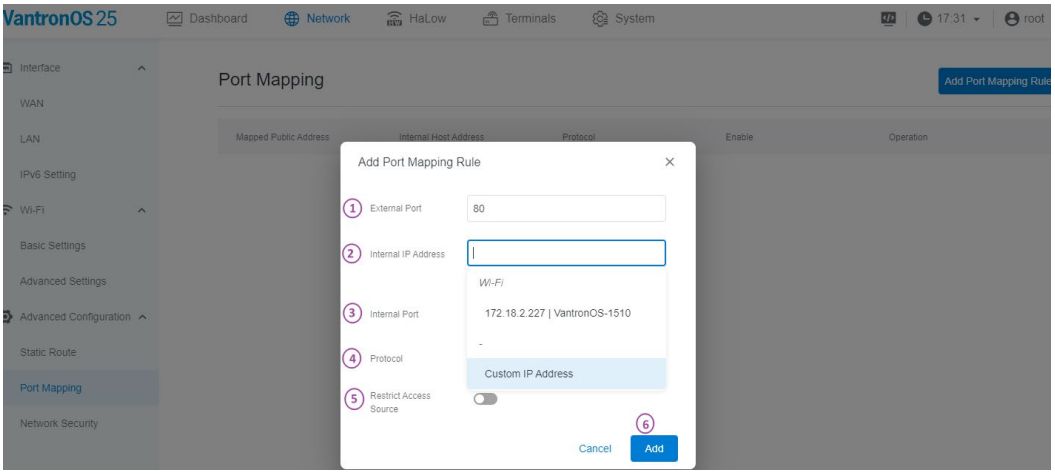
Goal:

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

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



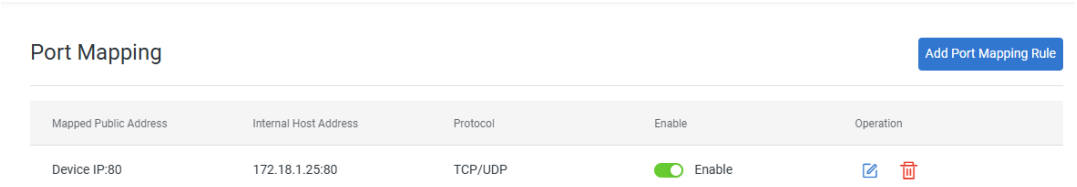
2. Fill in the rule information.



Description:

1) External port – The port number on the WAN side that outsiders will use to connect (e.g., 80).
2) Internal IP – The IP address of the target host (the internal device that provides the actual service).
3) Internal port – The port the target host is actually listening for the service (e.g., 8080).
4) Protocol – The protocol used by the service (TCP / UDP / both).
5) When **Restrict Access Source** is enabled, only the source IP with corresponding port and MAC you listed are allowed to reach the forwarded port. If **Restrict Access Source** is disabled, any public IP can access the device's IP and forward it to the internal IP.
6) Click **Add** to finish the configuration.

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



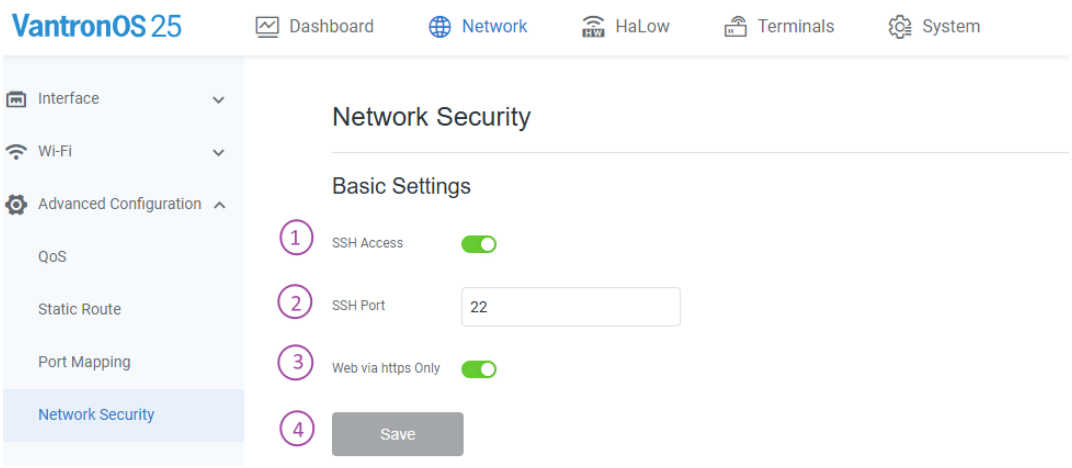
Note: *The mapped public address is determined by your WAN connection and may change.*

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

3.3.9 Network Security

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

3.3.9.1 Basic SSH Access Setup



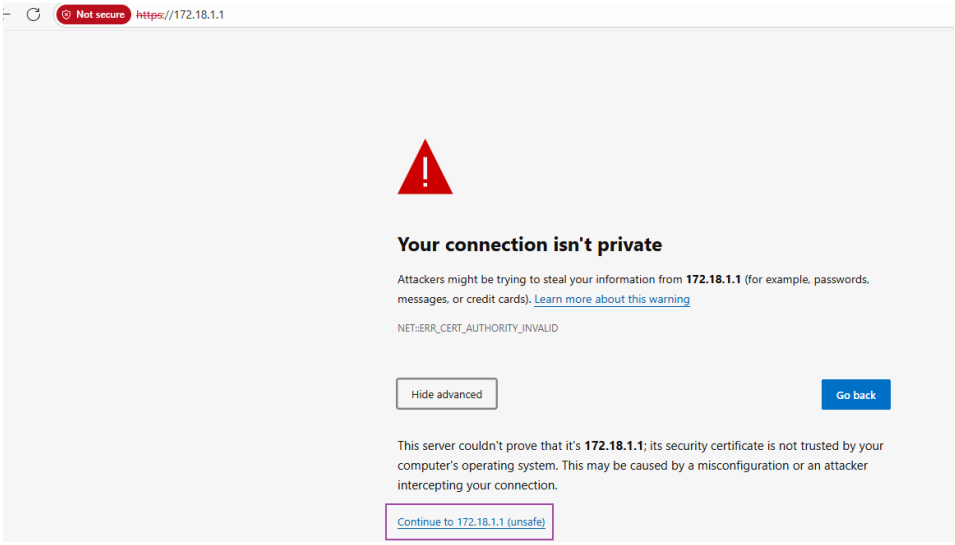
Description:

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

   Refer to Section 2.8 for the login method.

2. Default SSH port is 22. You can modify it as needed.

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.

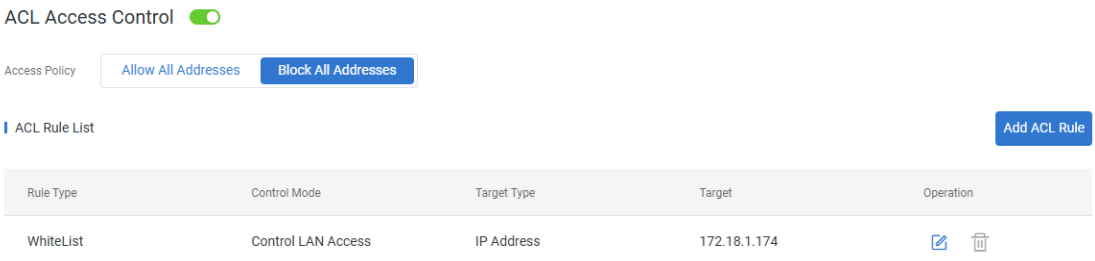
3.3.9.2 ACL Access Control

The device's access control consists of no-rule access policies and ACL rules after the ACL access control feature is enabled.

- **No-Rule Access Policies**

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

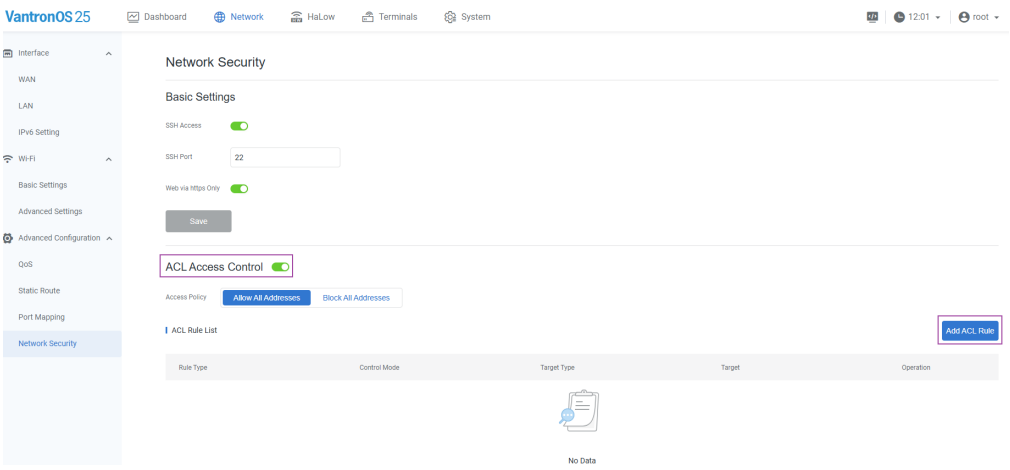
Block all addresses: When enabled, this policy **denies all WAN-side access**—only whitelisted IPs can reach the device—and **prevents** LAN-side devices from using the device to **reach the WAN**. If no whitelist rules exist at activation, the device automatically adds the host PC's **current IP** to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



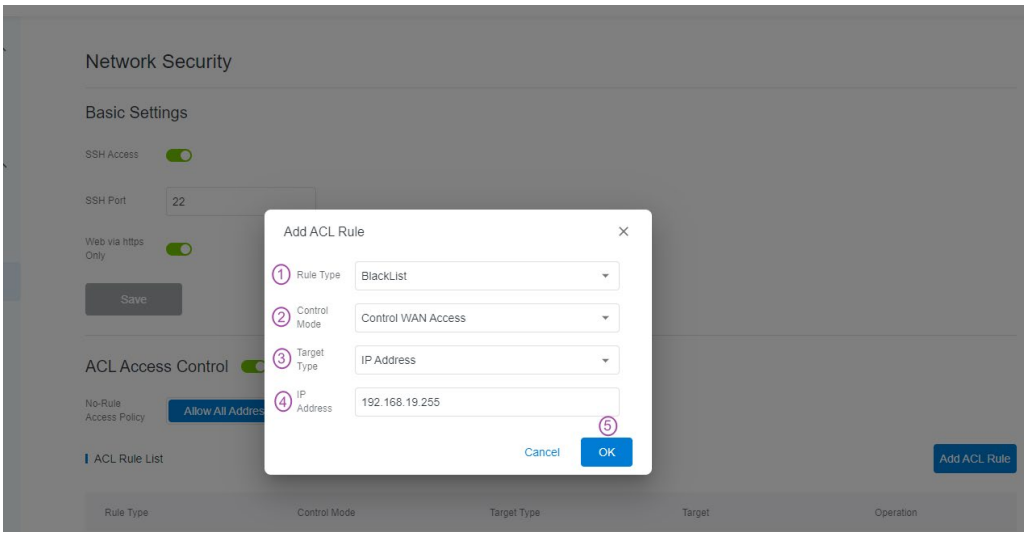
- **ACL Rules**

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 (control mode): WAN or LAN.

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

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

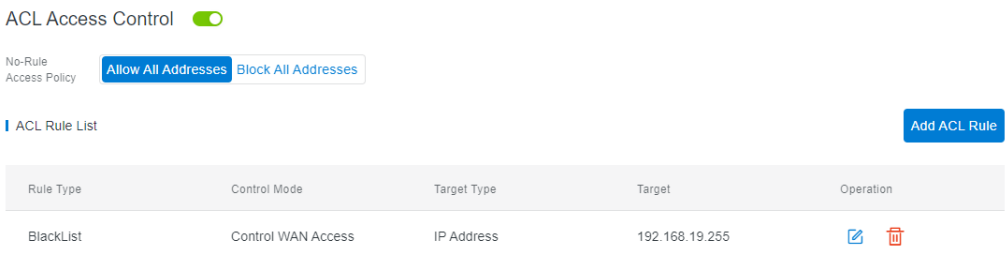
5) Click **OK** to complete.

Description for the rule settings:

Rule Type	Control Mode	Target Type	Result
Whitelist	WAN	IP address (Source)	The designated WAN IP has access to HAP101 or its LAN devices.
		Destination IP/ URL/URL keyword	HAP101 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 HAP101 or its LAN devices.
		Destination IP/ URL/URL keyword	HAP101 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.



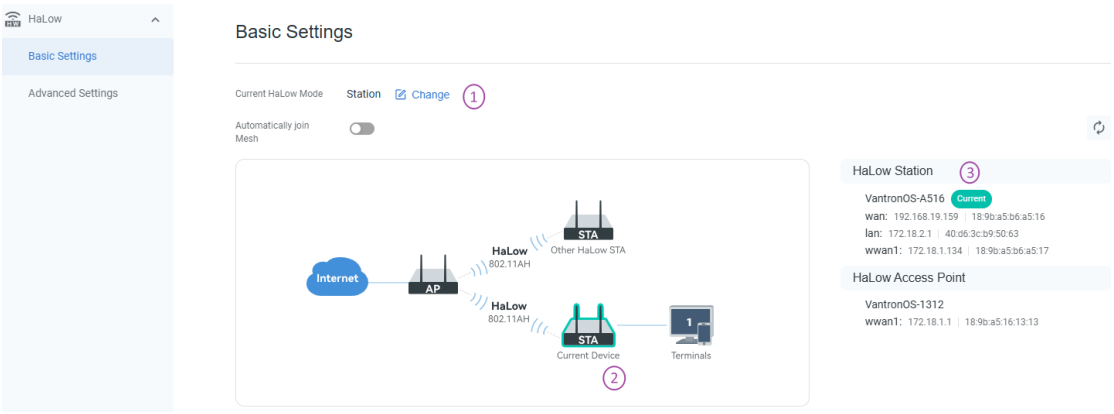
3.4 HaLow

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

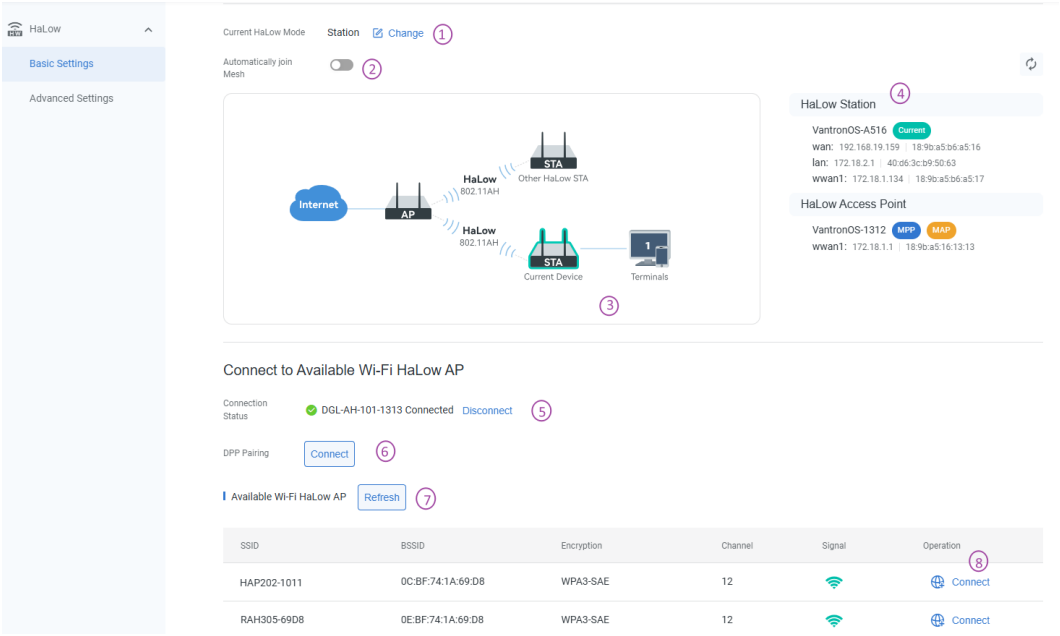
Under **Basic Settings**, a topology is displayed, indicating the role of the current device. If a HaLow network is established, brief information of the connection will display next to the topology.



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

3.4.1.1 STA-Mode Settings



Description:

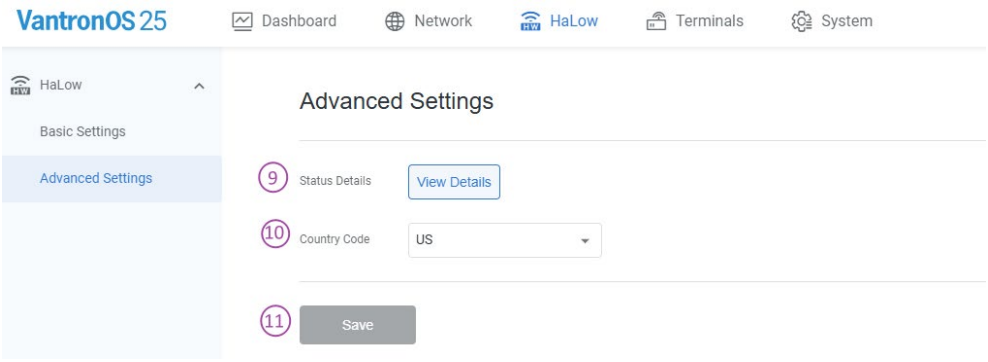
For basic settings

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.

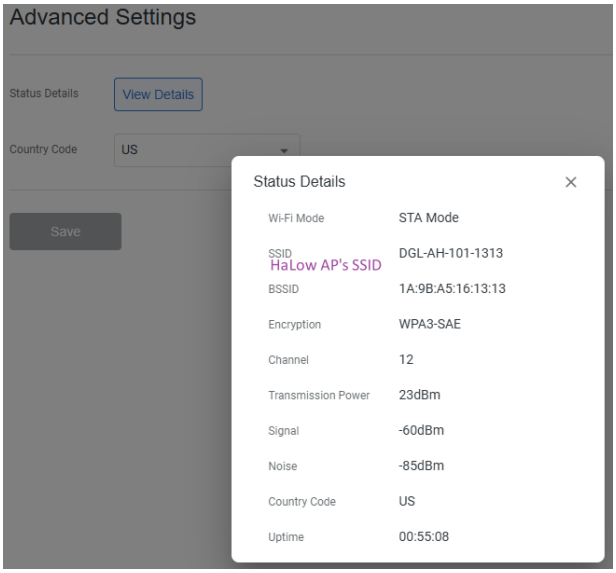
   MPP/MAP role tags on associated HaLow AP indicate mesh settings are enabled on the AP.
5. Connection status:
   - Pending Connection: Not connected to an AP.
   - xxx Disconnect: Connected to the indicated SSID. Clicking **Disconnect** cuts off the link.
   - Connection Failed: Failed to connect to the 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 advanced settings

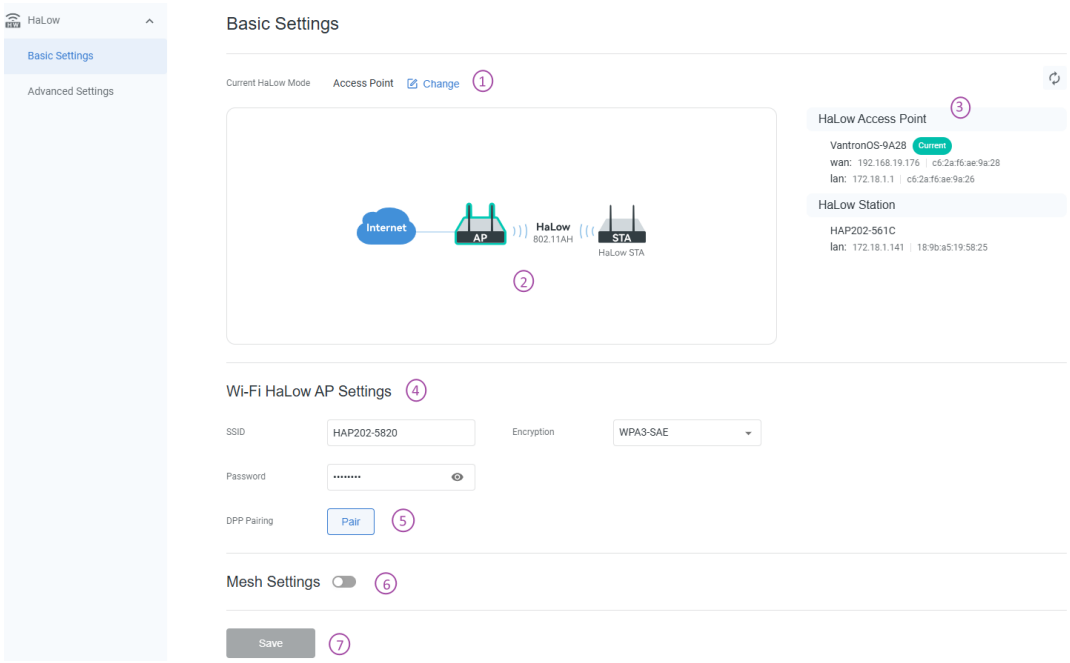
9. Status Details—Clicking **View Details** displays the detailed connection information of the device, including HaLow mode, and—if connected—the SSID of the target HaLow AP, encryption mode, channel, transmit power, etc.



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

When the associated HaLow AP is connected to an external router, the STA gains internet access through the HaLow link.

3.4.1.2 AP-Mode Settings

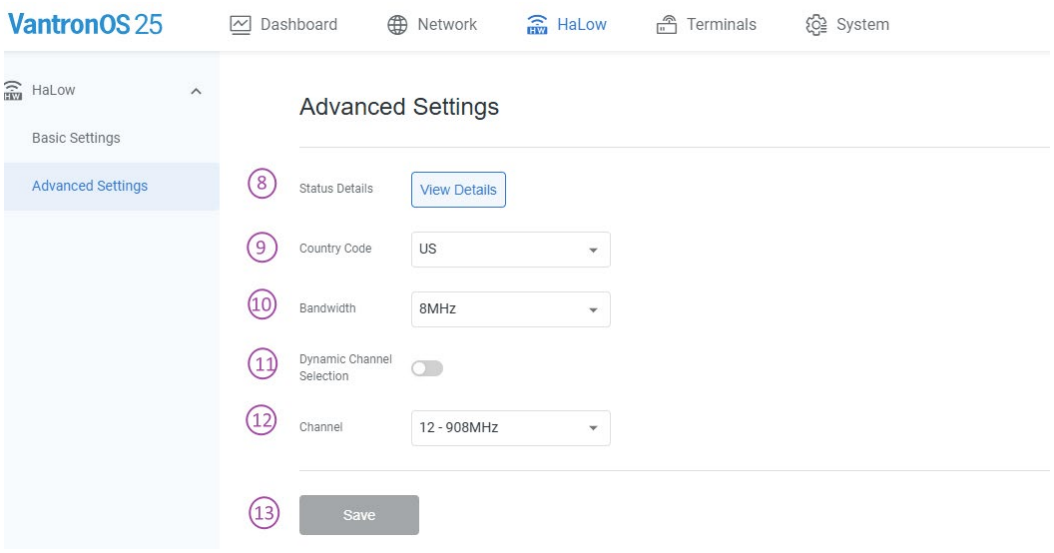


Description:

For basic settings

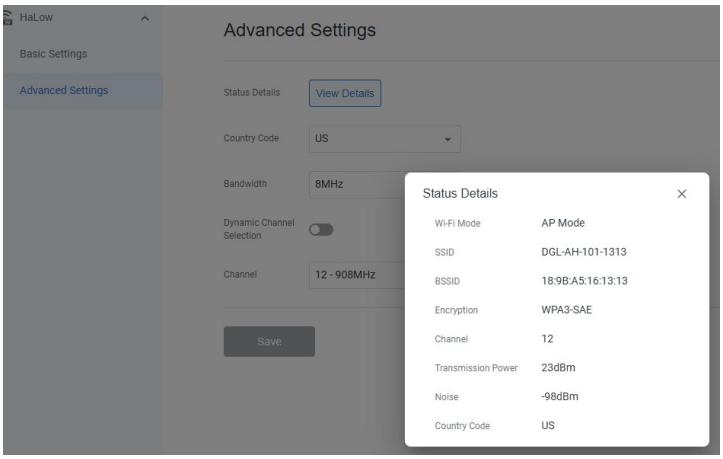
1. Click to change HaLow operation mode (Access Point/Station).
2. Network topology for the current mode. The local device is highlighted with a **cyan** outline.
3. Summary of device connection information: "**Current"** indicates the local device. Clicking the sync button refreshes the information.
4. AP settings: SSID, encryption mode, and password. You can modify these parameters as needed.
5. DDP pairing: Click **Pair** to initiate a quick HaLow connection. The target HaLow STA shall press the pairing button, either on the web portal or on the device, within the 120-second time window for a successful connection. Refer to Section 2.6.2 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.



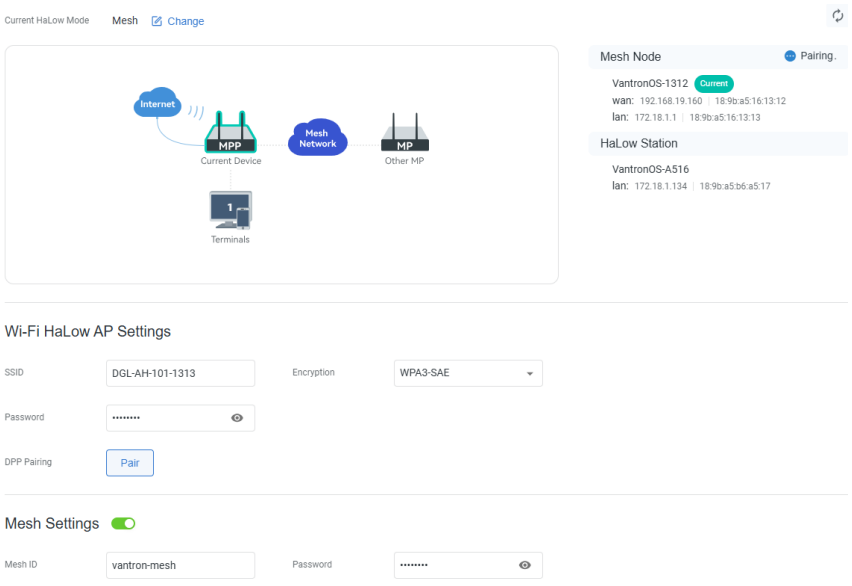
9. Country Code—Select the code based on local radio frequency regulations.
10. Channel bandwidth: A wider bandwidth typically offers higher throughput.
11. DCS: Once enabled, the device will automatically select the channel with the strongest signal within the selected bandwidth for optimal performance.
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.

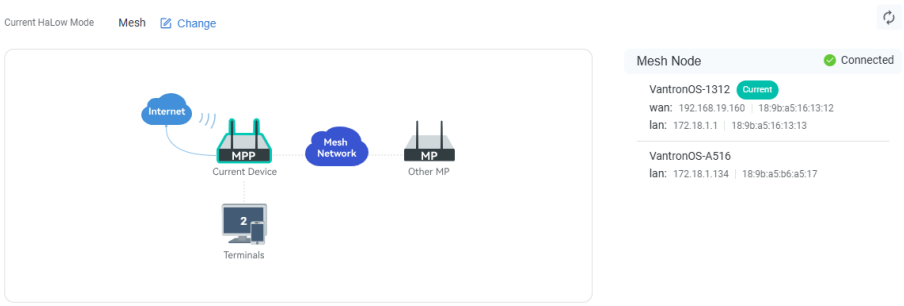
3.4.2 Mesh Networking

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.

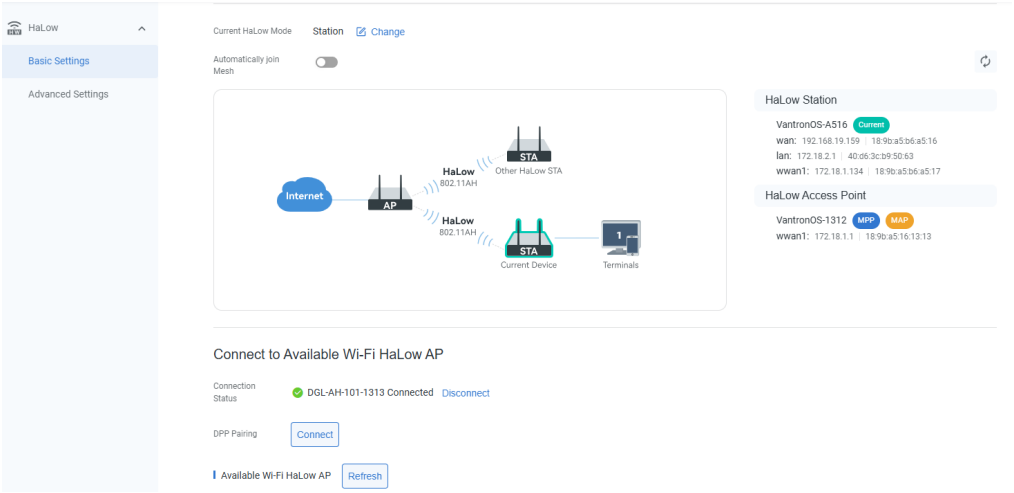


(Mesh settings enabled)

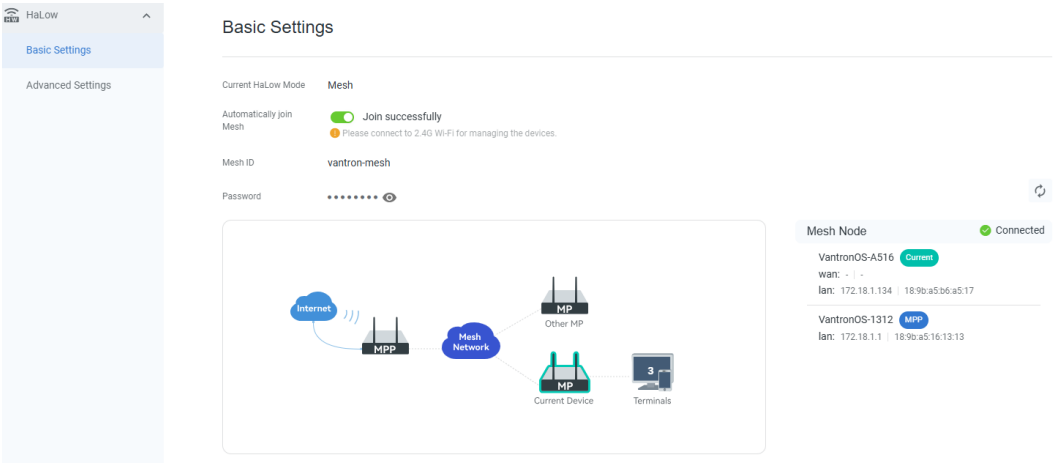


(MPs joined the mesh)

- 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 from a PC connected 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, use the DIP switches and the Pair/Restart button. On exiting the mesh, the STA's Ethernet and Wi-Fi interfaces are no longer bridged; its Ethernet port reverts to WAN mode, while Wi-Fi switches back to AP.

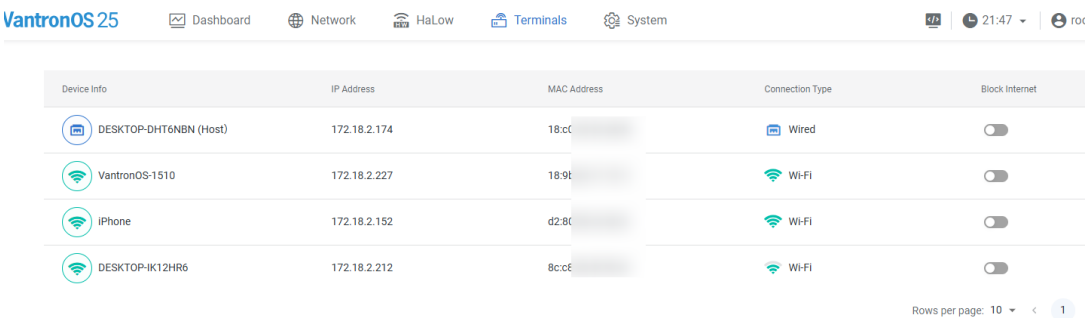
3.5 Terminals

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

2.4 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.

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



3.6 System

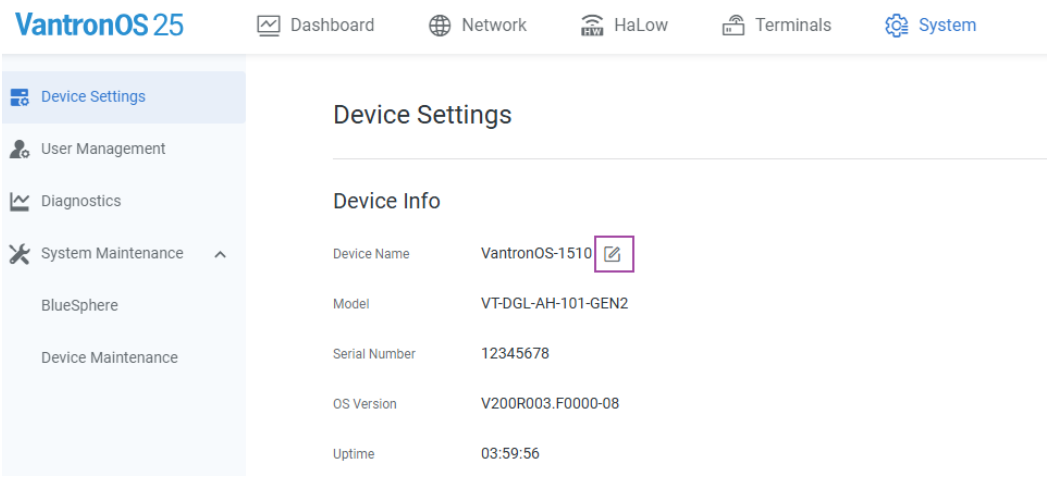
Under **System**, users can view and edit all system-level settings.

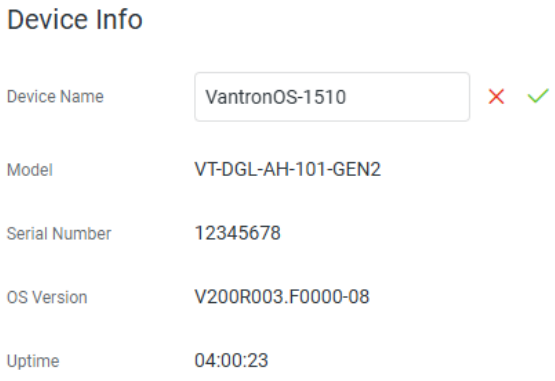
3.6.1 Device Settings

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.



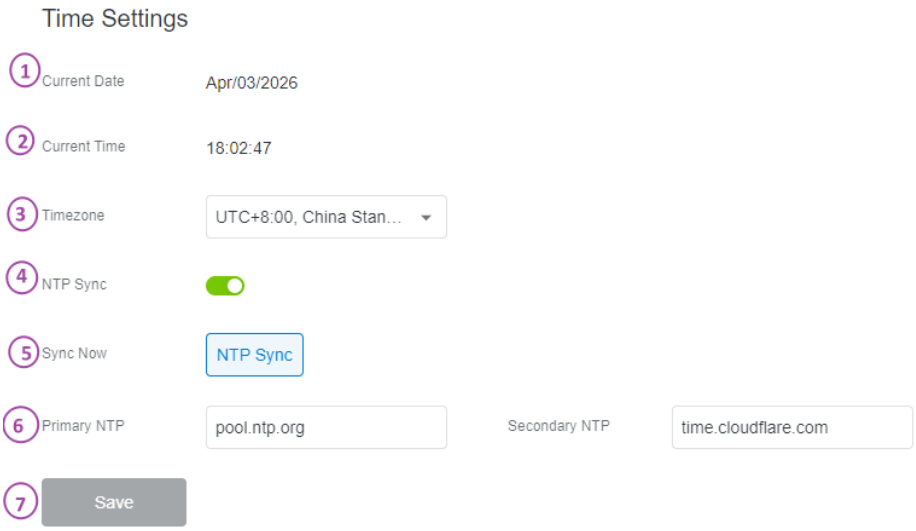


To modify the device name:

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.

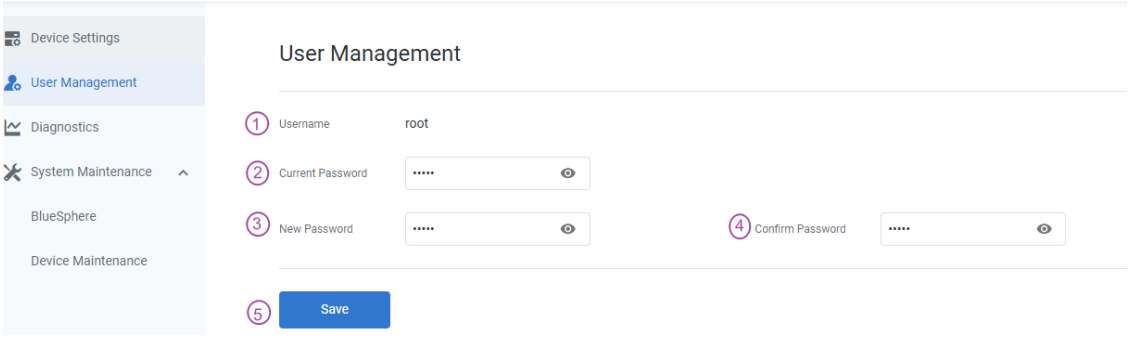


Description:

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 HAP101 lacks an RTC.
6. Primary NTP—Preferred NTP server. Secondary NTP—Backup NTP server.
7. If you have made any changes, click **Save** to apply.

3.6.2 User Management

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



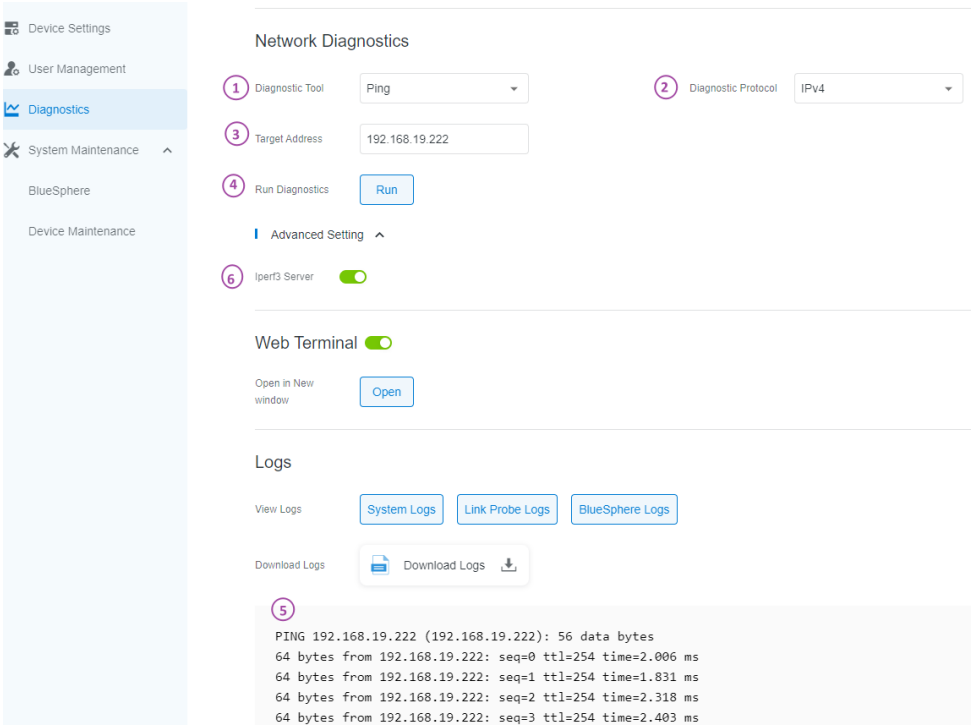
Steps to reset the login password:

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

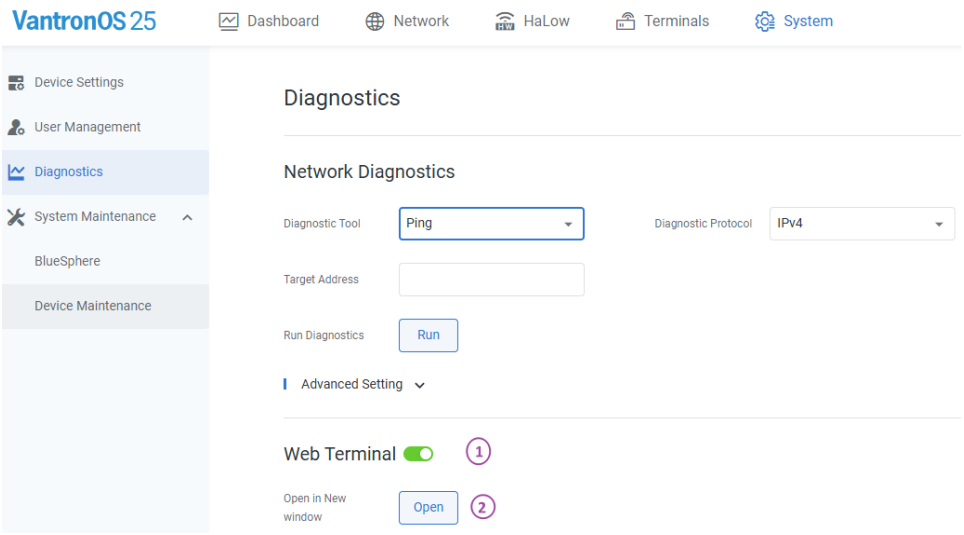


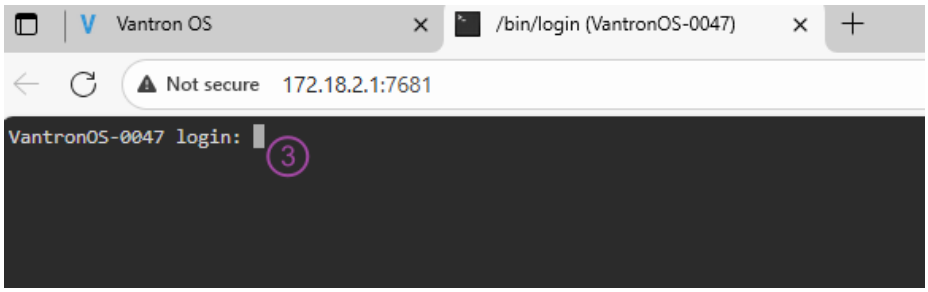
Description:

1. Select a diagnostic tool from the drop-down list (**ping, traceroute, nsloopup, 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 HAP101'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.





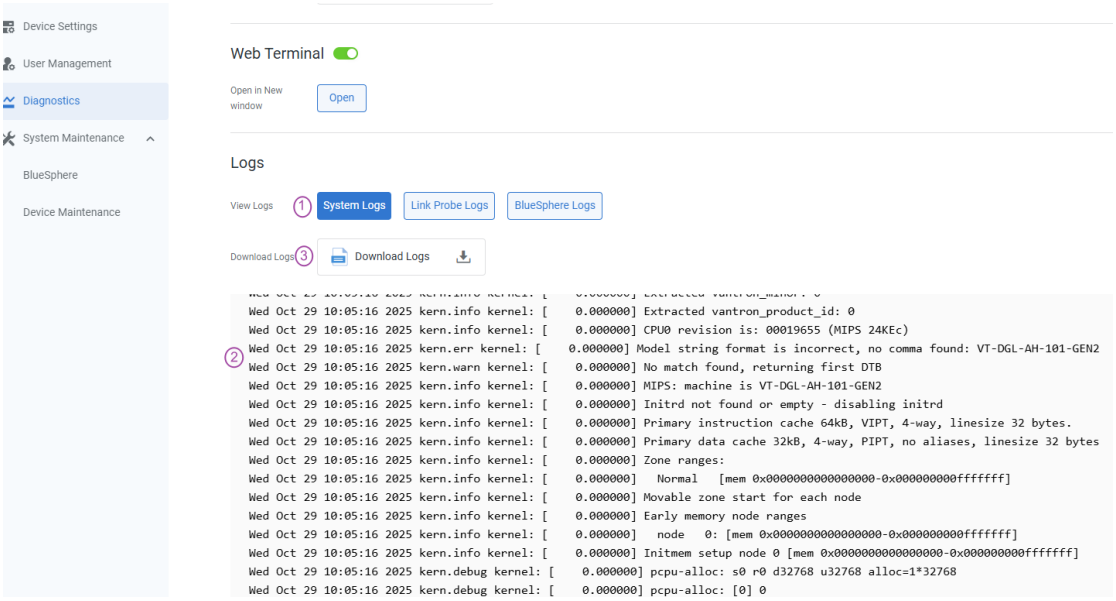
Description:

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.



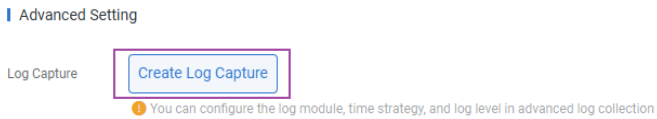
Description:

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.

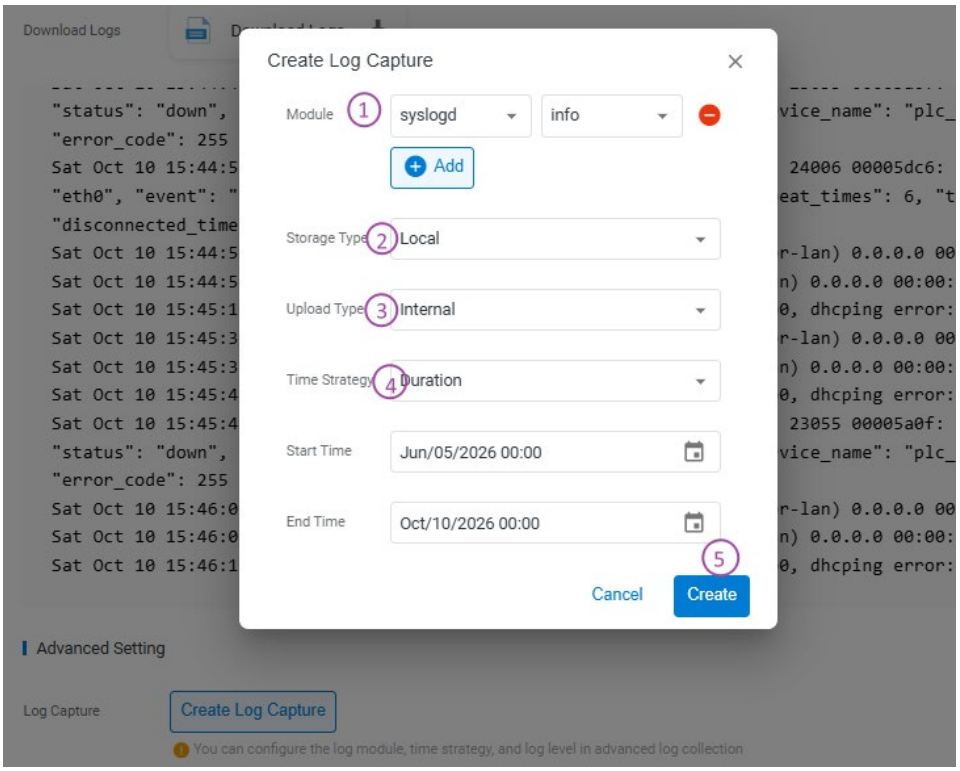
3.6.3.4 Log Capture

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

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



4. Configure the rule.



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

```
root@VantronOS-CA22:~# cd /tmp/log
root@VantronOS-CA22:/tmp/log# ls
cellulard.log       hotplug.log         restapi.log          vt_udmp_agent.log    vtled.log.1
health.checking.log  lastlog            syslog.log.old       vtled.log            wtmp
root@VantronOS-CA22:/tmp/log# cat health.checking.log
1791614350.732 - info    - health checking started---
1791614350.737 - info    - add check target for platform VT-M2M-G405
1791614350.738 - notice - add check target -  60 → service status
1791614350.738 - notice - add check target - 600 → vtos agent
1791614350.738 - notice - add check target - 300 → time sync
1791614350.739 - notice - add check target - 120 → Disk Writable Testing
1791614350.739 - notice - add check target - 120 → hardware status
1791614350.739 - notice - add check target -  50 → refresh ARP table
1791614350.740 - notice - add check target - 120 → IP Address Conflict Detection
1791614350.740 - notice - add check target - 300 → Local IP Address Conflict Detection
1791614350.740 - notice - add check target - 300 → Gateway IP Address Conflict Detection
1791614350.741 - notice - add check target - 300 → Network Address Conflict Detection
1791614350.741 - notice - add check target - 300 → Sub-Network Address Conflict Detection
1791614350.741 - notice - add check target - 300 → Multiple DHCP Server Detection
1791614350.741 - notice - add check target - 300 → Console AutoLogin system.ttylogin
1791614350.742 - notice - add check target - 600 → Checking System Reboot Abnormally
1791614350.742 - notice - add check target -  60 → Checking System Logging
1791614350.742 - notice - add check target - 600 → Checking System Reboot Wireless MCU Abnormally
1791614350.743 - notice - add check target -  60 → check cellulard traffic statistics
1791614410.888 - notice - ubus send event.health_checking '{"service": "vtapp_restapi", "status": "up", "event_ty
pe": "service.status", "event_id": 19}'
1791614410.894 - notice - ubus send event.health_checking '{"service": "snmpd", "status": "up", "event_type": "se
rvice.status", "event_id": 19}'
1791614410.899 - notice - ubus send event.health_checking '{"service": "cellulard", "status": "up", "event_type":
```

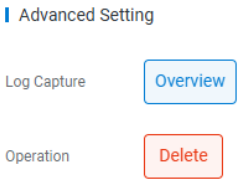
- GWM: Logs are exported to the BlueSphere GWM platform.
- FTP: Logs are exported to the designated FTP server as configured.

4) **Time Strategy**

- Duration: Logs of a specified time period are captured.
- Permanent: Logs are captured continuously without interruption.

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

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



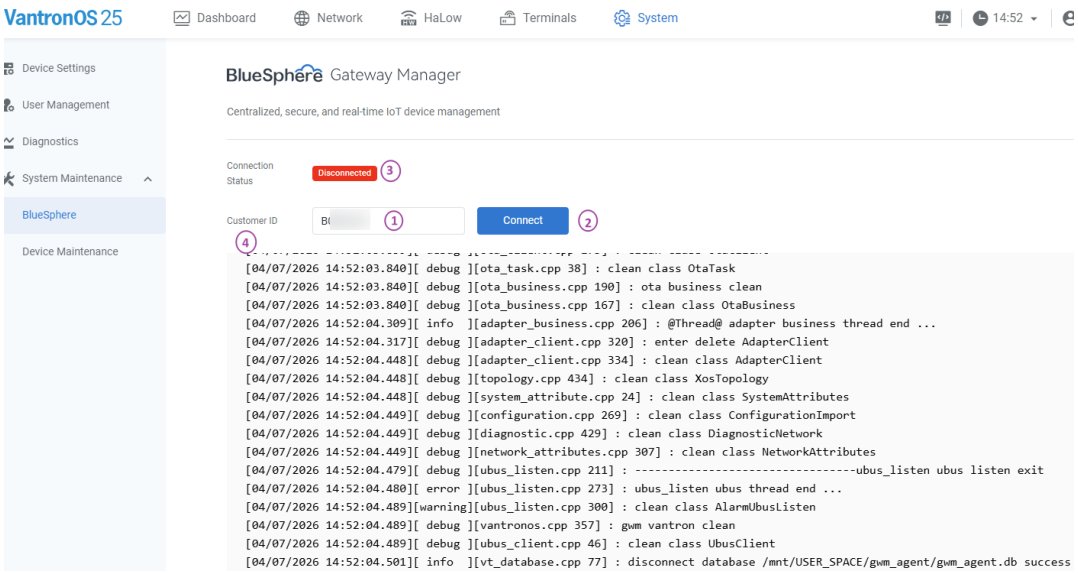
3.6.4 System Maintenance

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 HAP101 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.

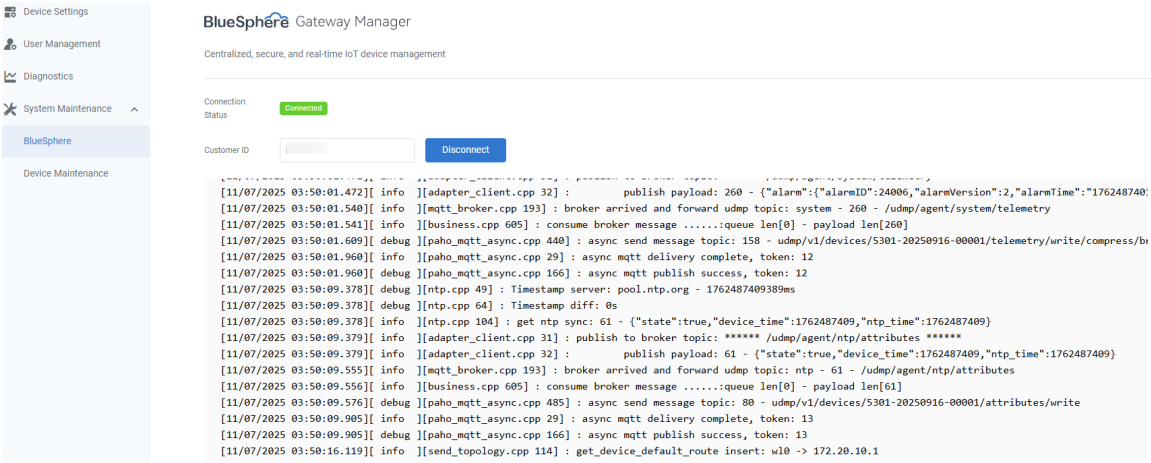
   *If a customer ID is pre-filled, you can click **Disconnect** first and fill in your own.*

2. Click **Connect** to initiate the interfacing between the device and the GWM portal.

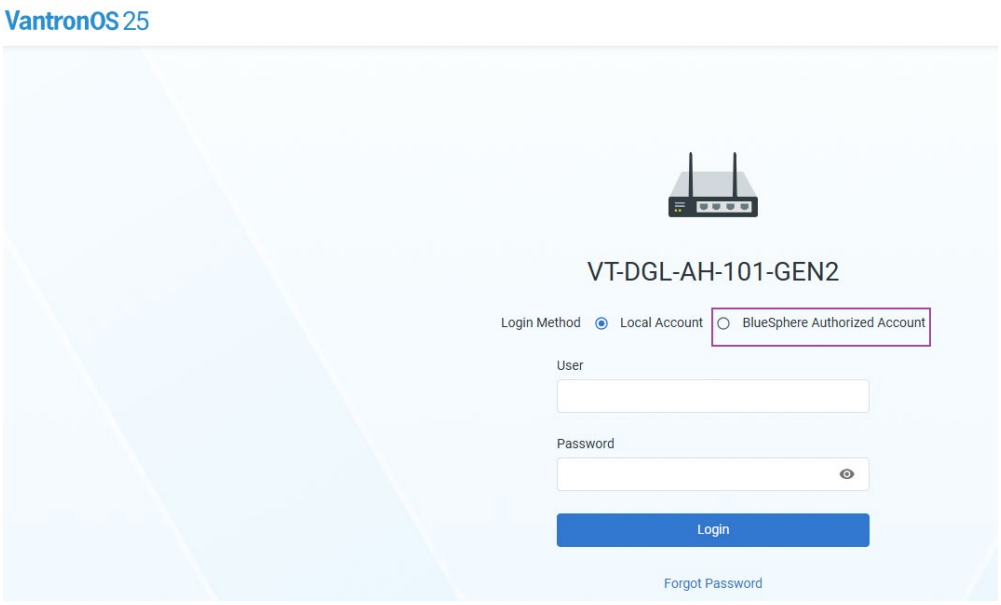
3. When the handshake succeeds, the device status changes to **Connected**.

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.



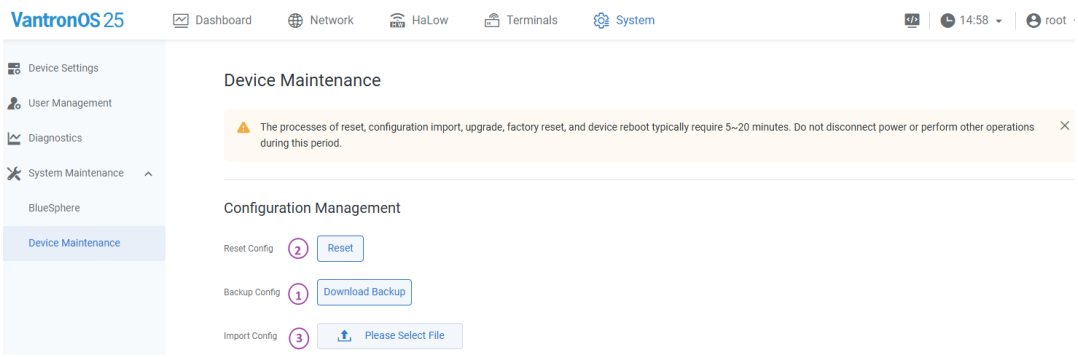
If you log out the portal now, you will find two login methods available. You can sign back in with either your local credentials or your authorized GWM account.



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

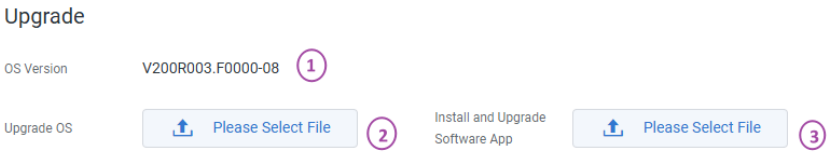


Description:

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

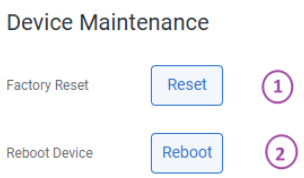


Description:

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:

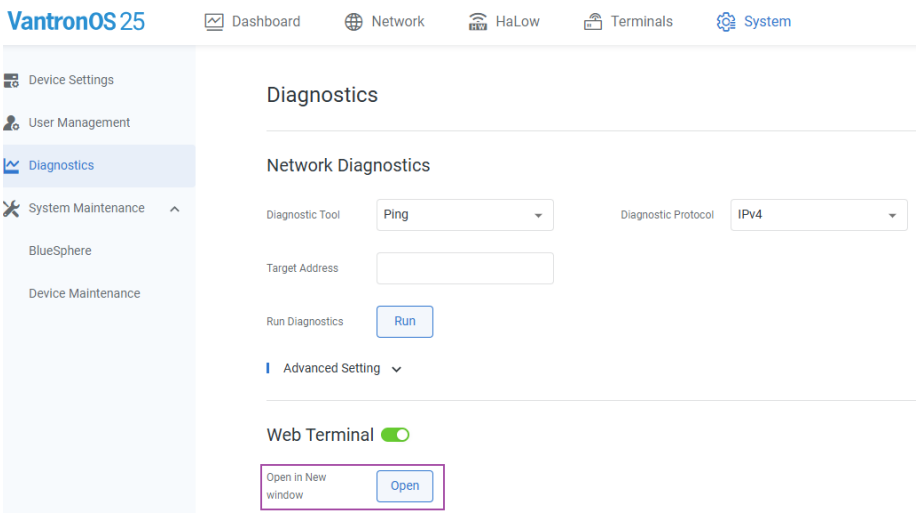
1. Factory reset the device with device configuration, user data and custom applications (including VantronOS 25 APP) cleared.
2. Manually restart the device.

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

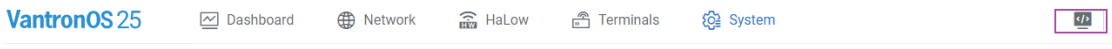
3.7 Command Line Interface

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

- Click **Open** web terminal on the **Diagnostics** page, as described in Section 3.6.3.2.

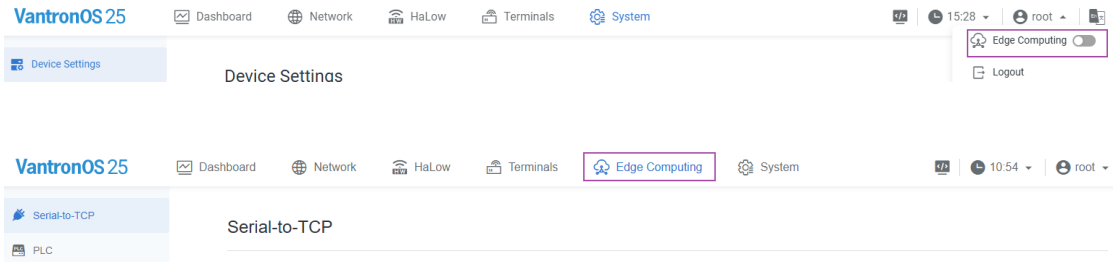


- Click the CLI icon on the menu tab.



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.



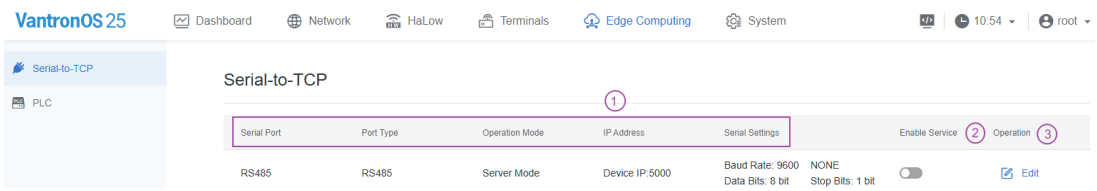
3.8.1 Serial to TCP

The Serial-to-TCP feature 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 HAP101 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.

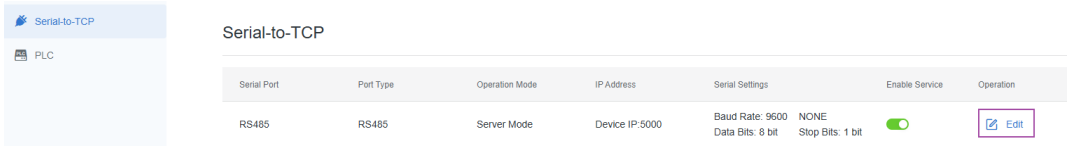


Description:

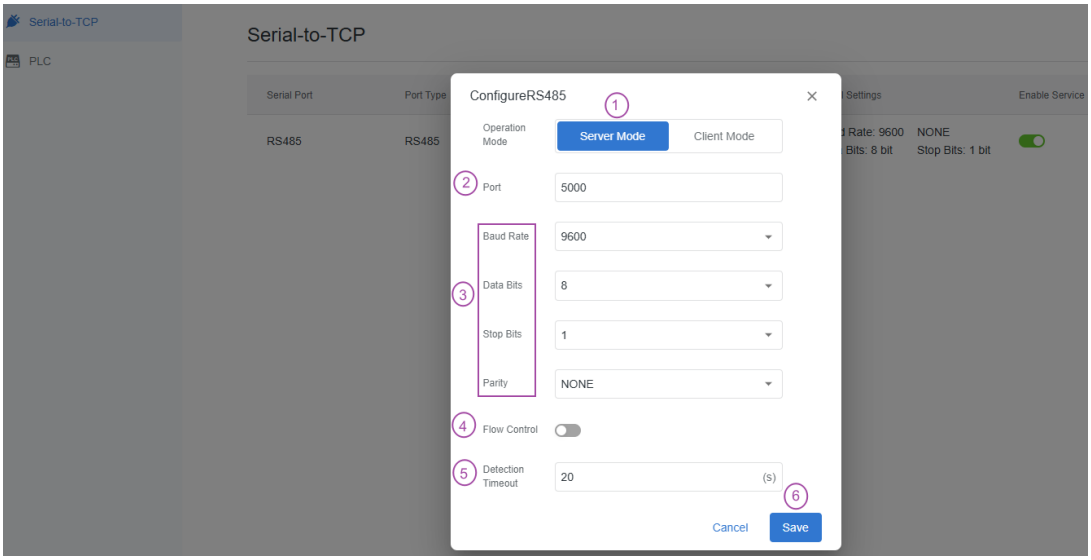
1. Details of the conversion rule, including the serial port name and type, current operation mode, IP address of the device + port, and serial parameters.
2. Enable/disable the rule.
3. Edit the rule.

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 HAP101 on the serial link.



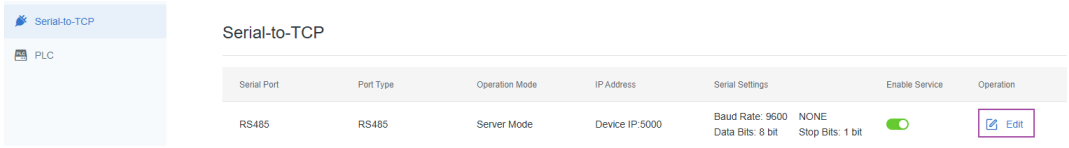
Description:

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 HAP101 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.

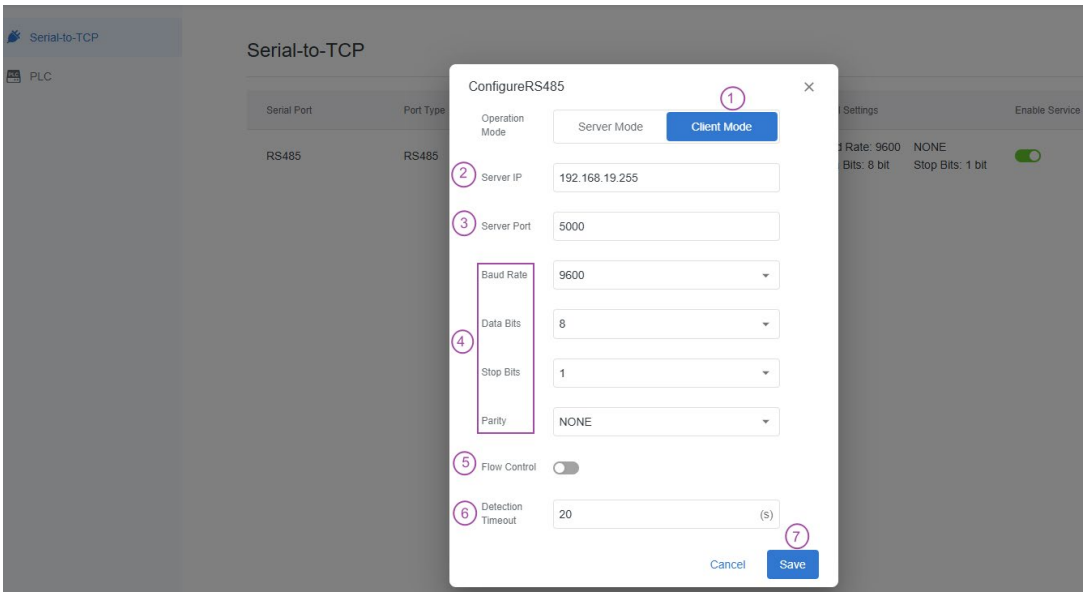
3. Enable the conversion rule after modification.
4. Make sure both the client and server are on the same reachable IP network.
5. Verify the data transmission between the devices.

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 HAP101 on the serial link.



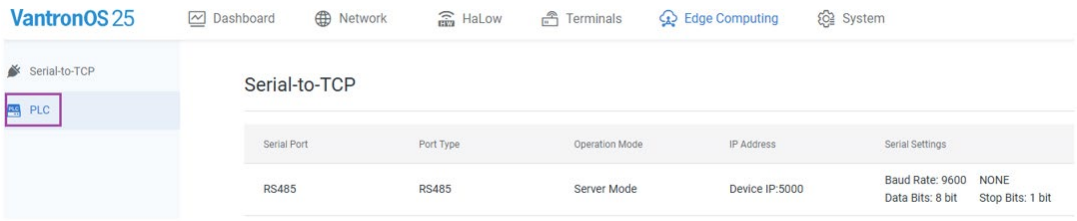
Description:

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 HAP101 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.

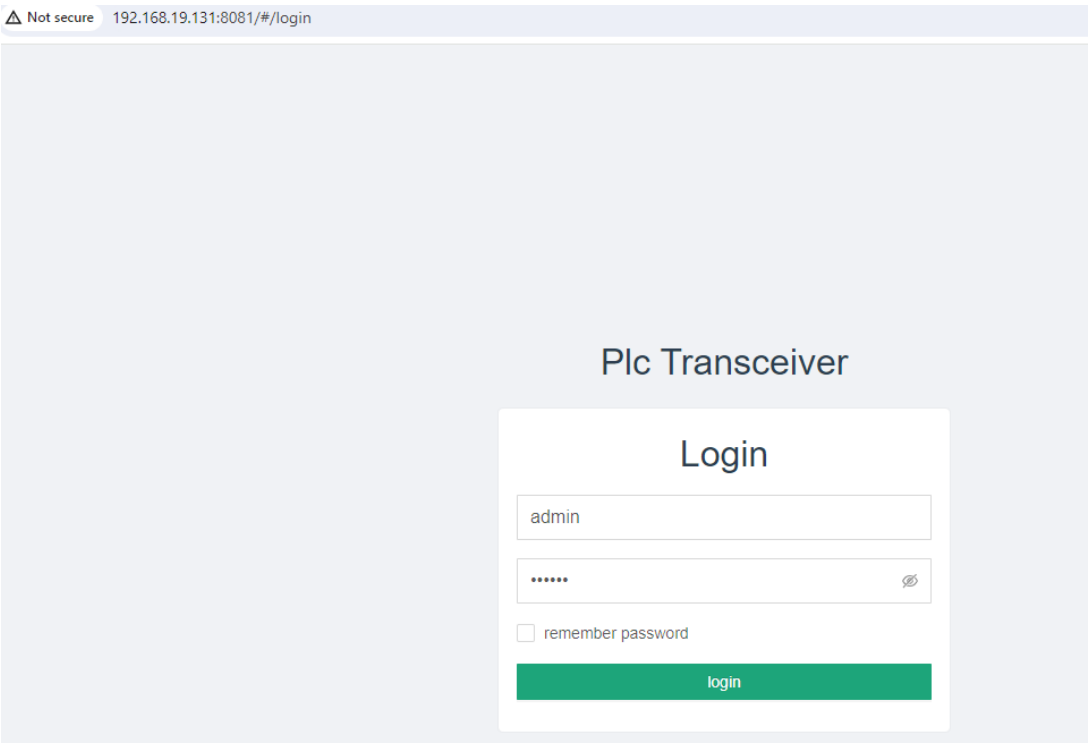
3. Enable the conversion rule.
4. Make sure both the client and server are on the same reachable IP network.
5. Verify the data transmission between the devices.

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

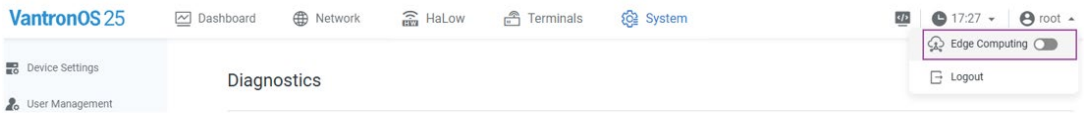
4.1 Overview

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.

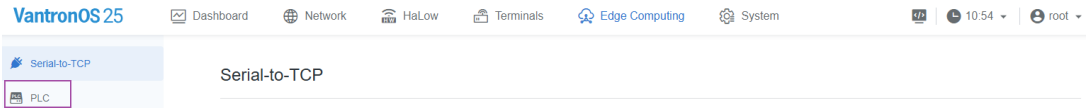
VantronOS industrial protocol portal supports varied wired industrial protocols, spanning both fieldbus and industrial-Ethernet standards to meet diverse on-site requirements.

4.2 Portal Login

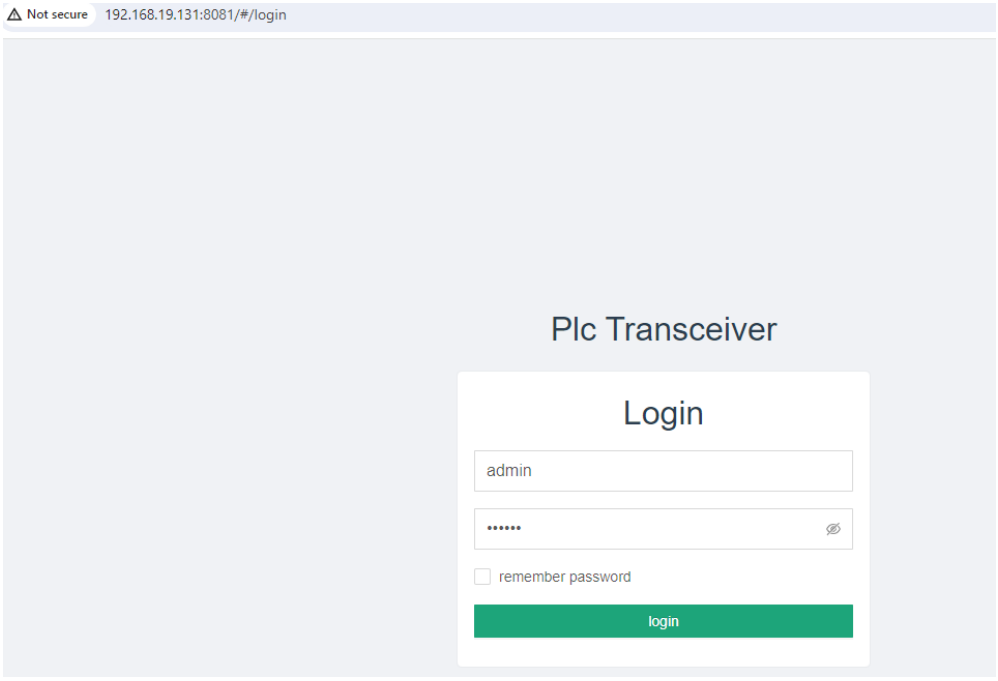
1. Enable the **Edge Computing** feature from the user account drop-down list.



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

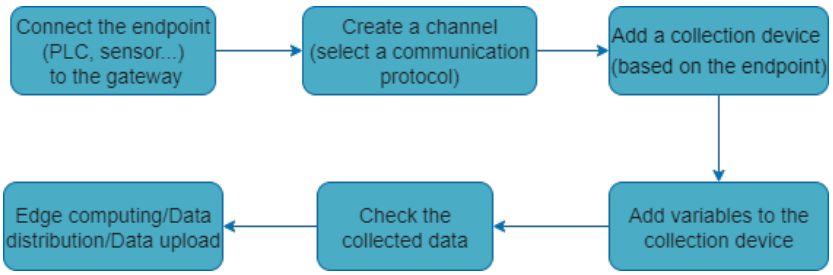


3. Users will be redirected to a new window. Use your VantronOS credentials to log in.



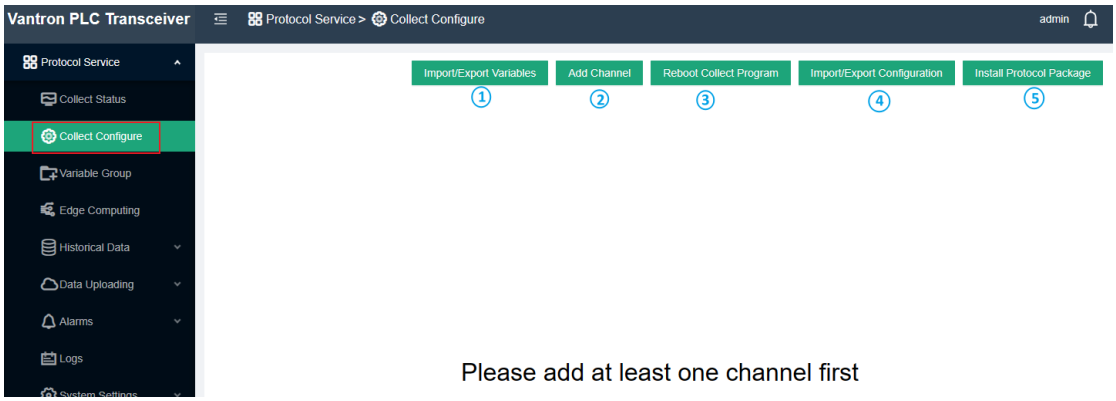
4.3 Protocol Configuration and Application

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.



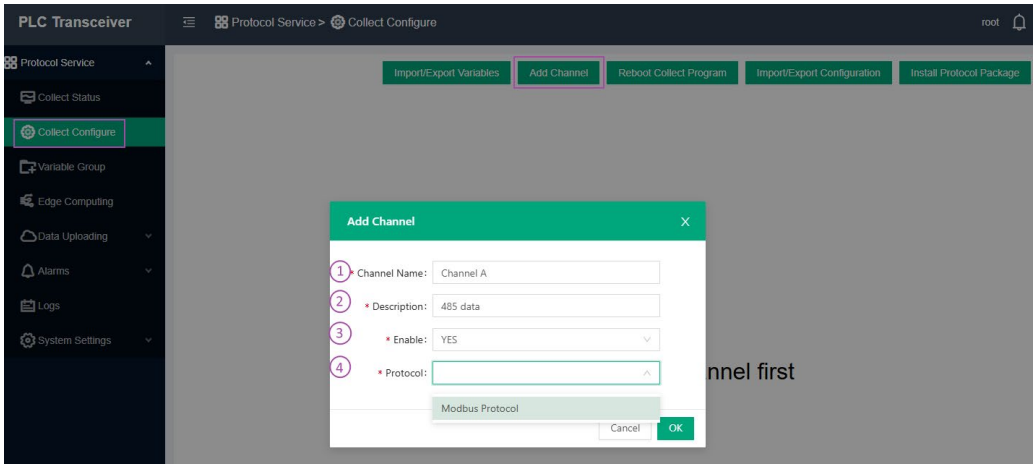
Description:

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

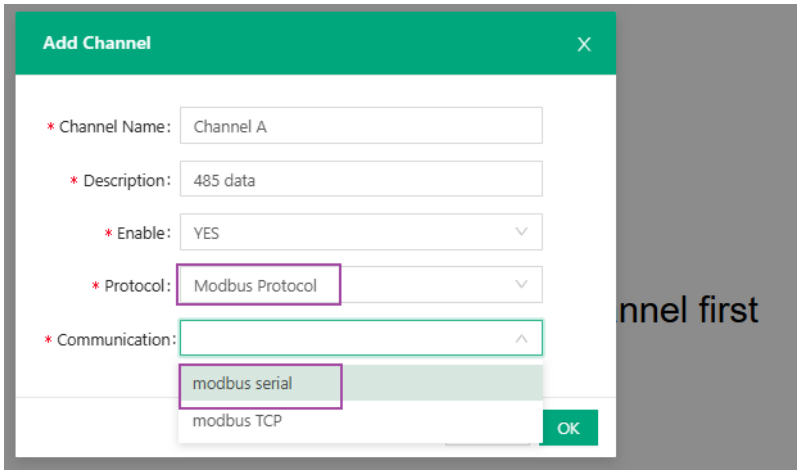
Click **Add Channel** under the **Collect Configure** menu to add a single channel.



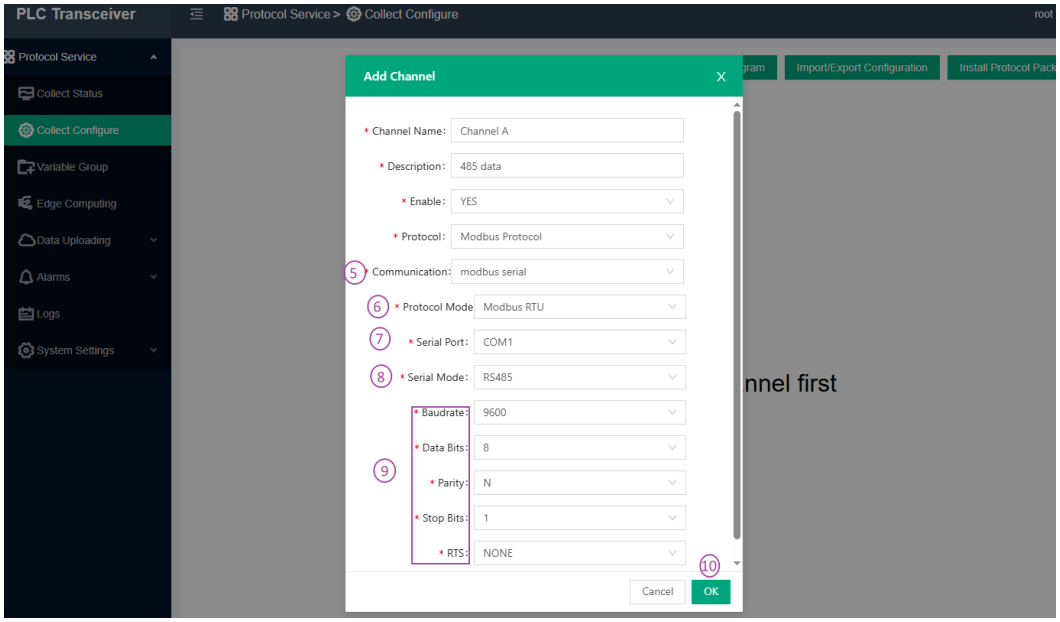
Description:

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 HAP101. Take the **Modbus Serial** protocol for illustration. Ensure the endpoint is connected to the HAP101 via the RS485 serial port.



To further configure the protocol:

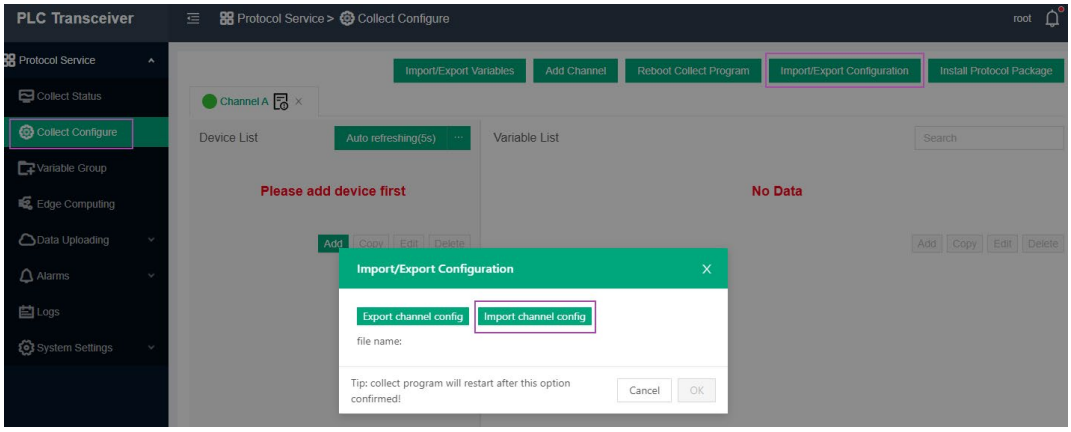


Description:

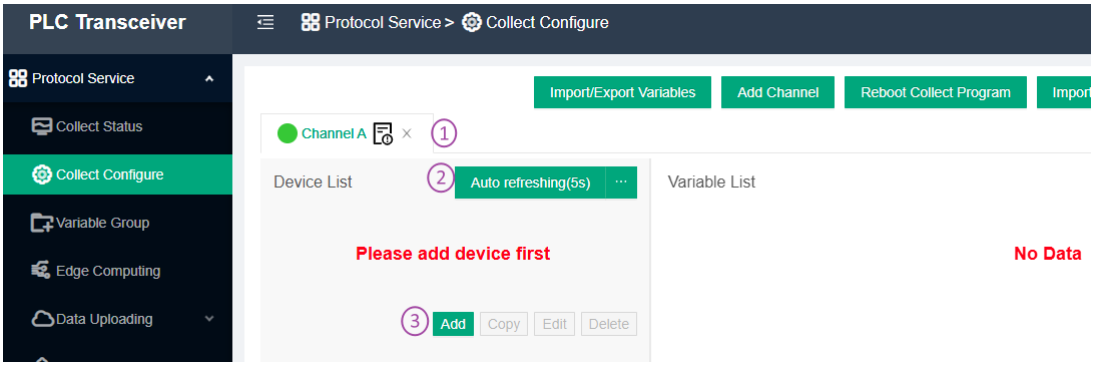
5. Choose **modbus serial** as the communication type.
6. Select **Modbus RTU/Modbus ASCII** as the protocol mode (Modbus RTU for illustration).
7. The HAP101 provides one serial port, mapped to the device software node (COM1).
8. Serial mode is bound to the device's serial port.
9. Fill in the serial parameters of the endpoint connected to the HAP101. 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.



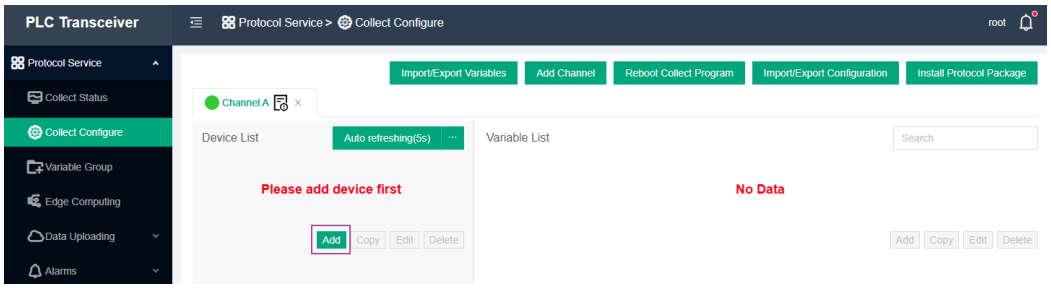
Description:

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.

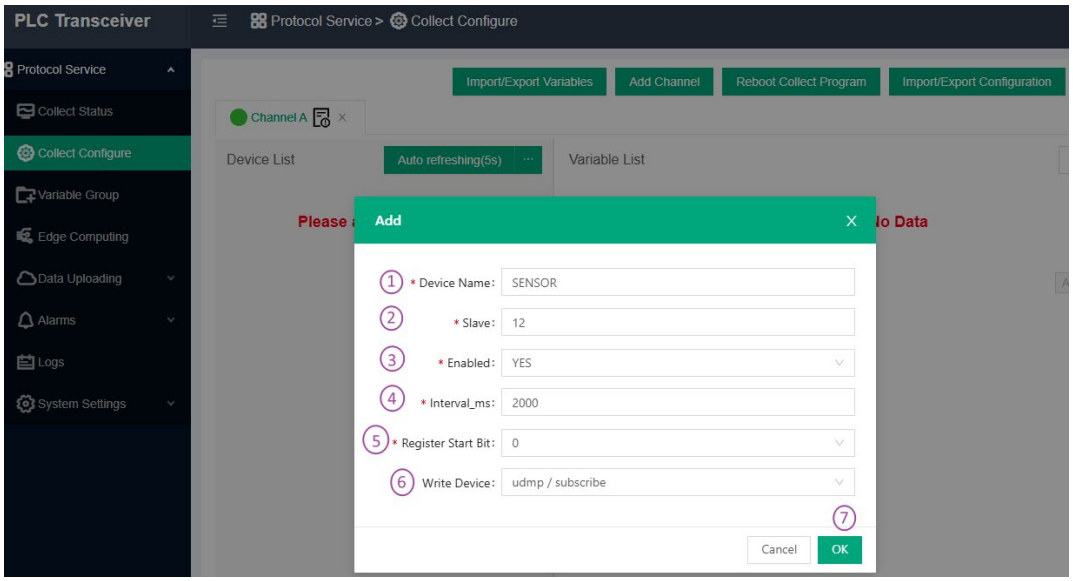
4.3.2 Device Setup

After creating a channel, the data collection endpoint that connects to the HAP101 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:

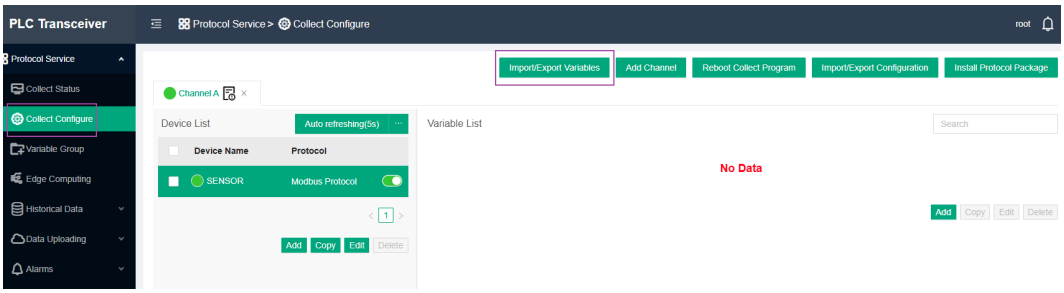
1. Enter a device name for the endpoint.
2. Input a slave address between 0 and 255.
3. Choose to enable the device or not.
4. Set an interval for data collection (you can leave it as-is).
5. Set a start bit for the register.
6. Select the path to write the data.
7. Click **OK** to complete adding the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

4.3.3 Variable Setup

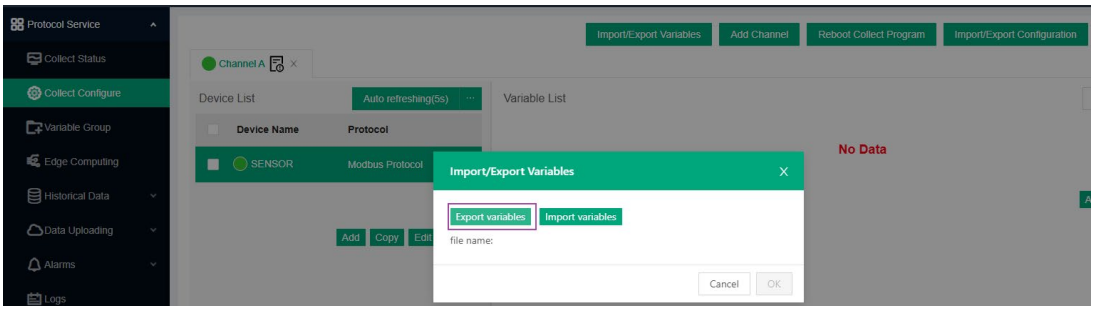
After channel and endpoint setup, users can choose to batch import the variables or configure individual variables for the target endpoints.

4.3.3.1 Global Batch Import

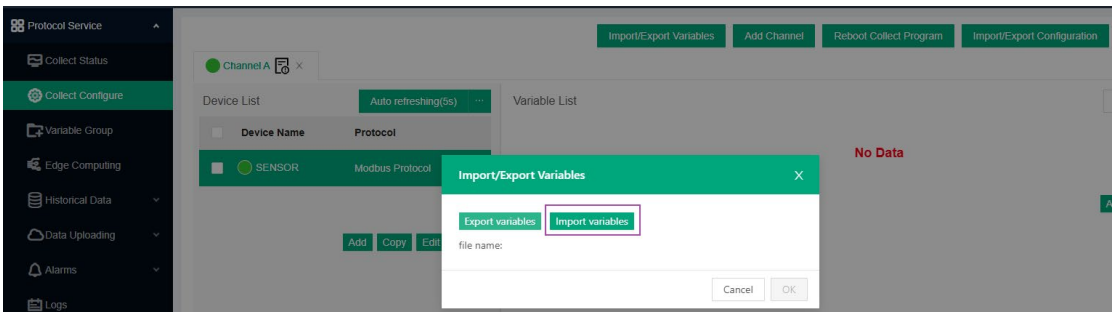
The **Import/Export Variables** tab on the **Collect Configure** menu allows users to import or export variables in bulk across different channels or endpoint devices.



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



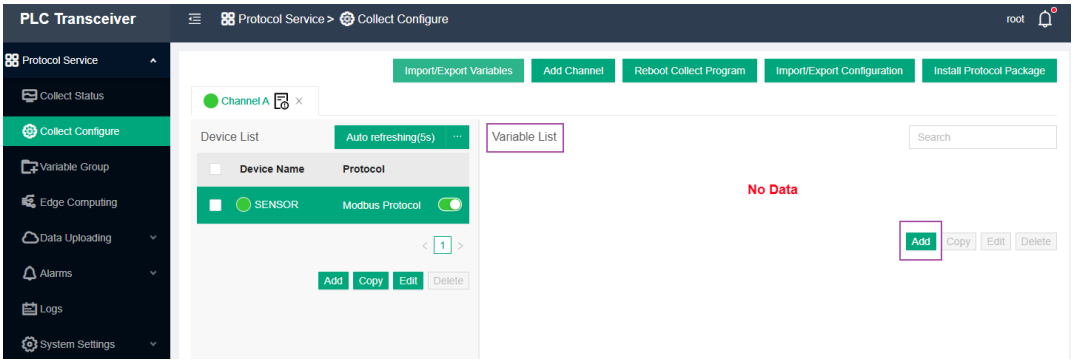
Then click **Import Variables** to upload the file.



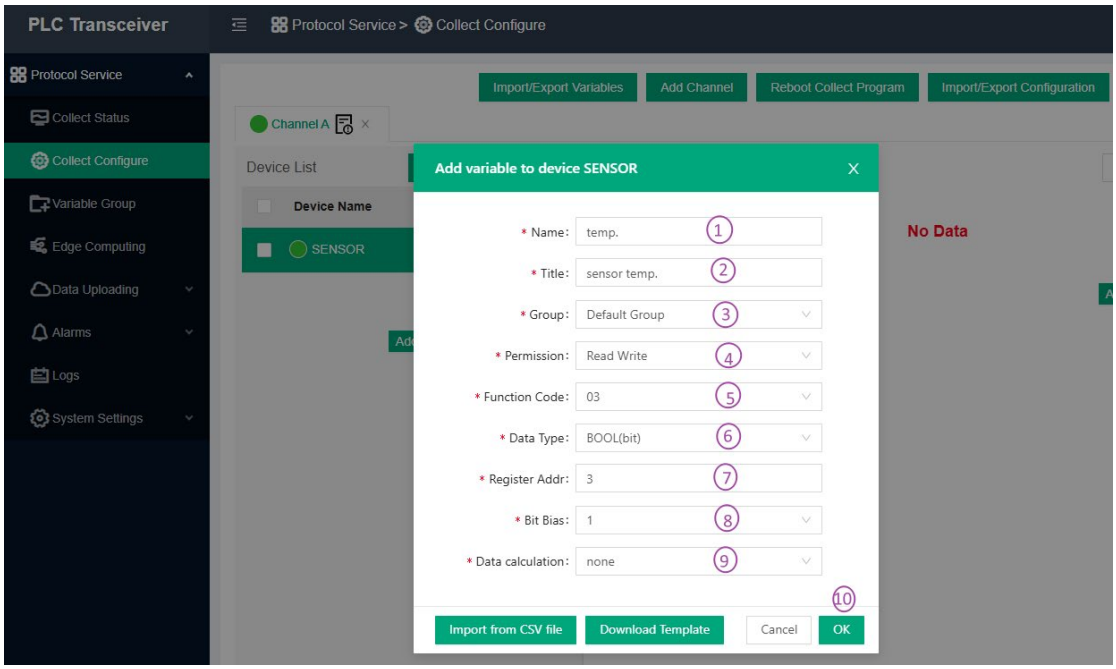
4.3.3.2 Individual Variable Configuration

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

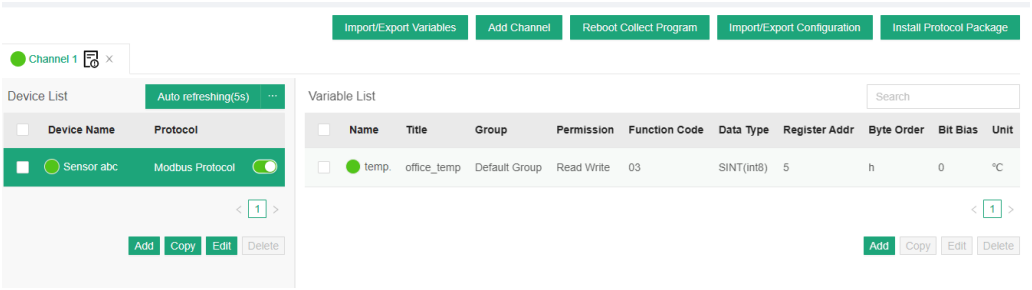
Import from CSV file: Bulk variable upload (replaced with **Export variables** for setups with existing variables)

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).

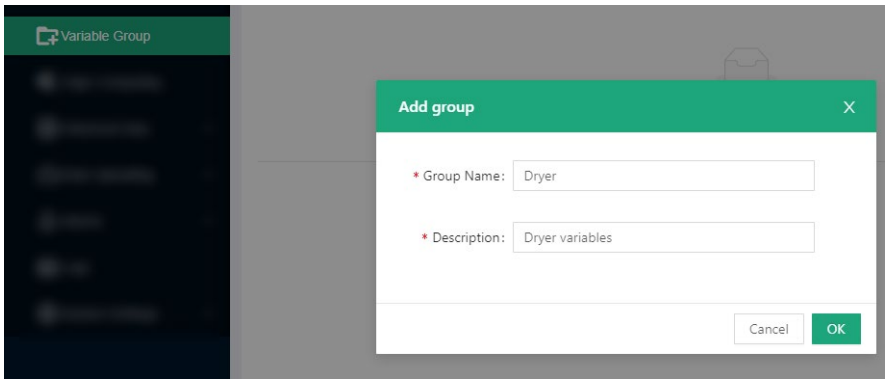
4) Set the access permission of the variable.
   a. Read only: You can only read the measured parameters
   b. Write only: You can only distribute values from the web portal to the field device
   c. Read Write: You can both read the measured parameters and distribute the values to the device
5) Select 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.

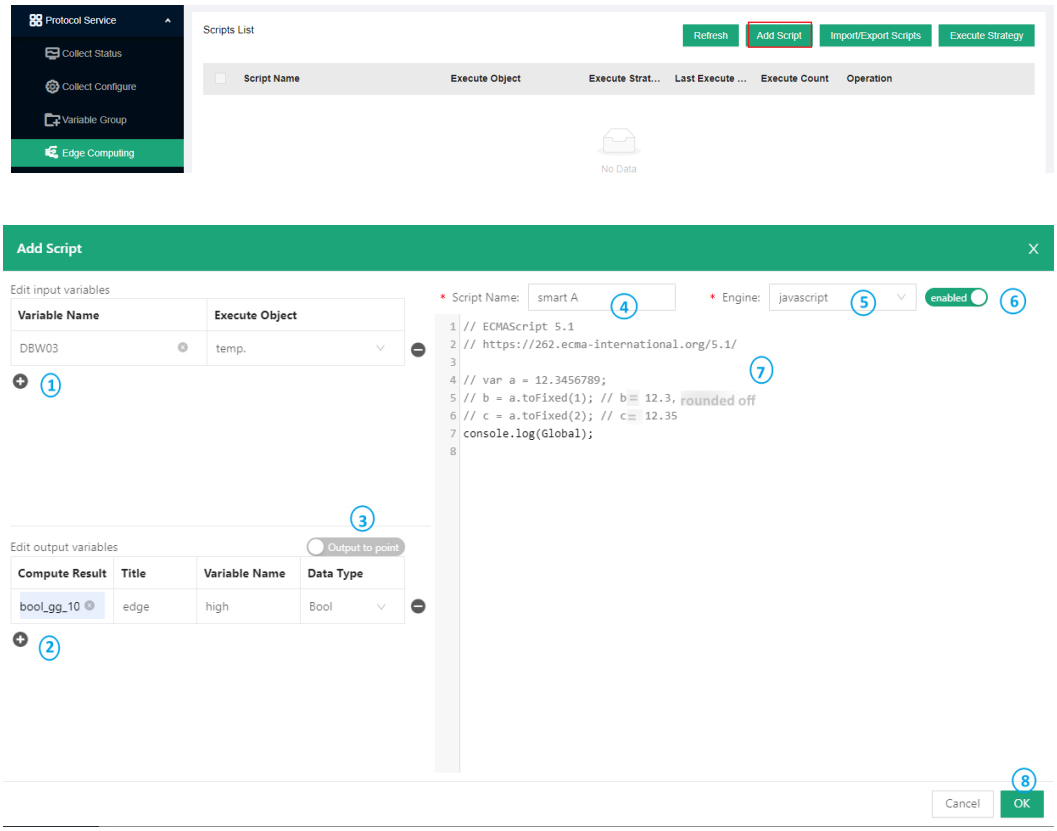


If multiple variables are involved, you can add variable groups for different variables from the **Variable Group** tab on the left menu pane.



4.4 Edge Computing Scripts Setup

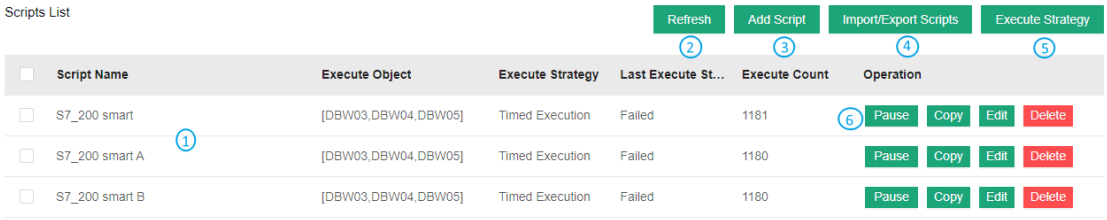
To add a script for edge computing, click **Edge Computing** from the navigation pane on the left, then click **Add Script** to input the script information in the pop-up.



Description:

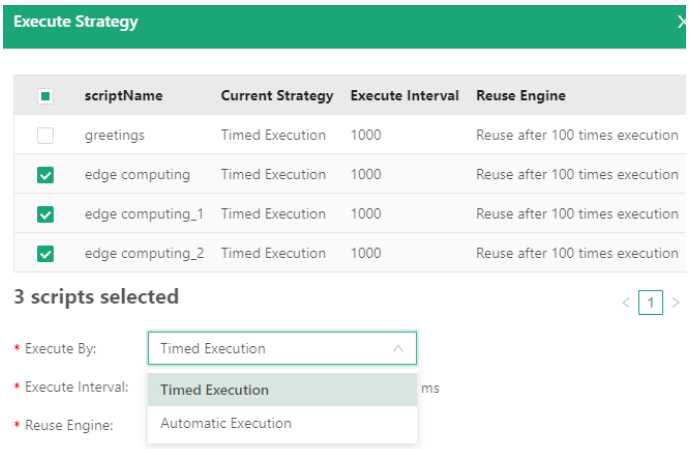
1. Edit input variables: add a name for the input variable and an object for executing the script (more than one variable could be added).
2. Edit output variable: add the computation result, title, variable name, and data type.
3. Toggle between outputting the results to the variables or edge nodes.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

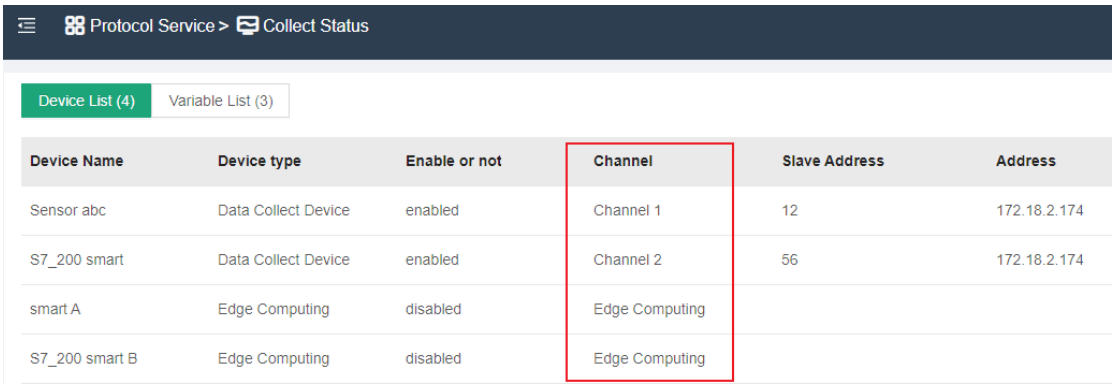
Reuse Context allows you to set a restart mechanism for the scripts

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).

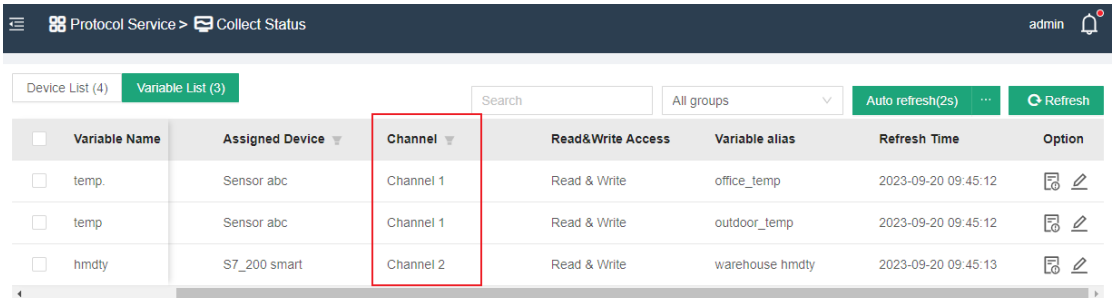
4.5 Collection Status

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

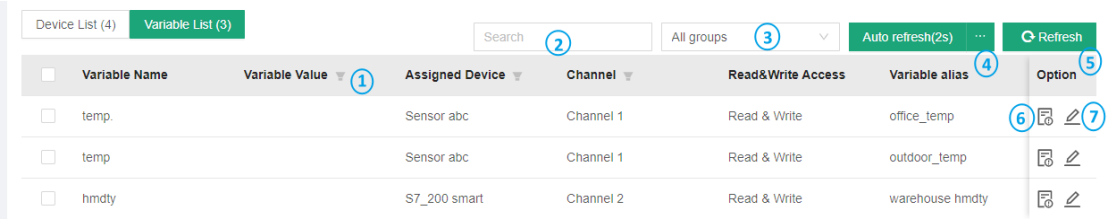
The **Device List** displays information about the collection devices, edge computing, historical data, etc. Users can differentiate the data based on the collection channels.



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.



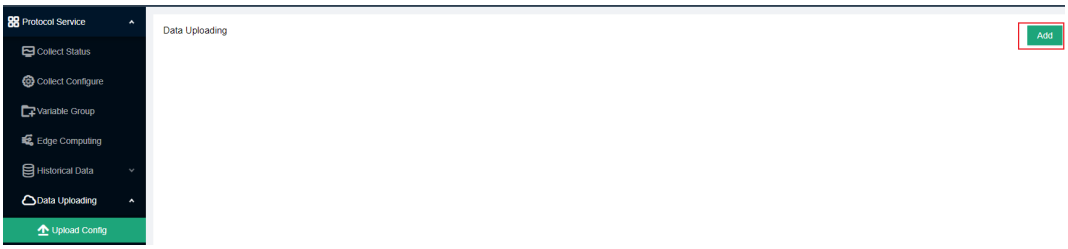
Description:

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).

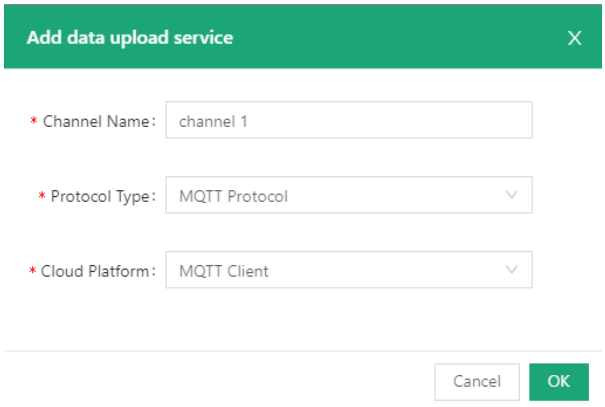
4.6 Data Upload and Encapsulation

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.

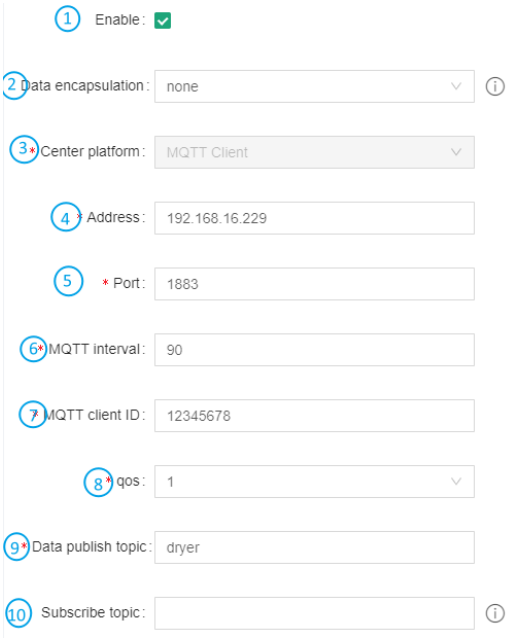
1. Expand the **Data Uploading** tab from the navigation pane and click **Upload Config**.
2. Click the **Add** button on the upper right corner to add a data upload task.



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 .

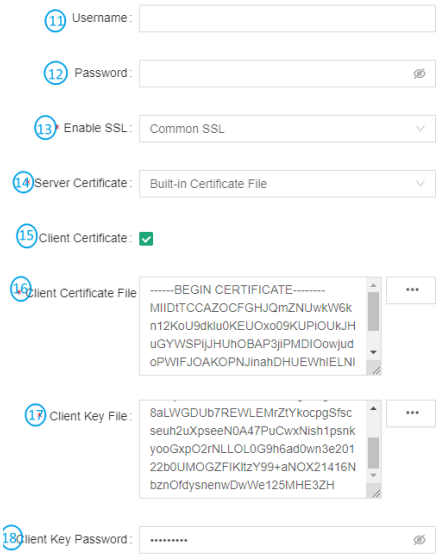
   QoS 0: The message will be sent once at the maximum. If the client is not available, the message will get lost.

   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).

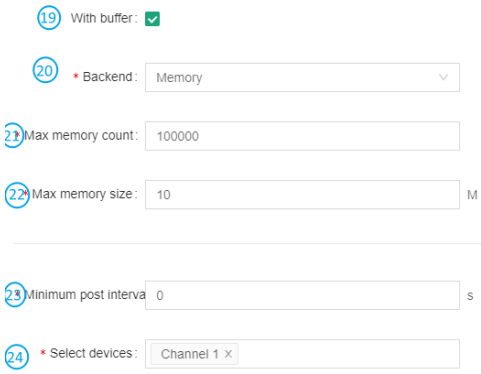
14) If common SSL is enabled, select a certification mode for the server.

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.



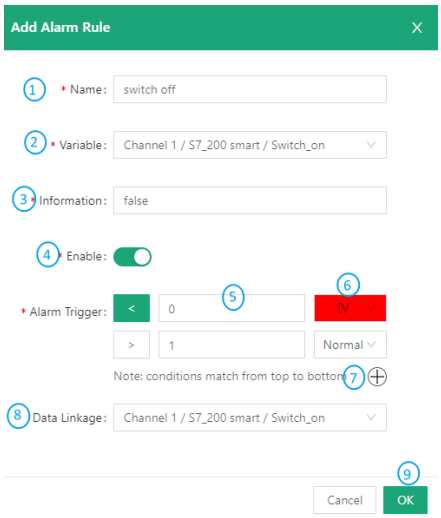
Description:

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.

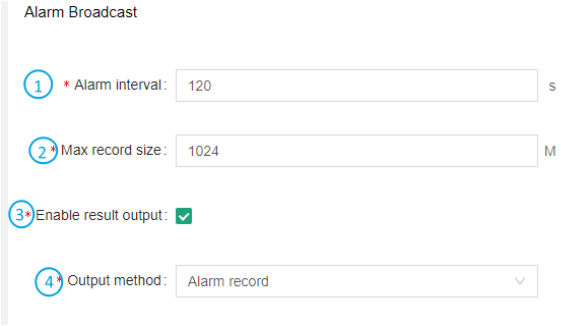


Description:

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

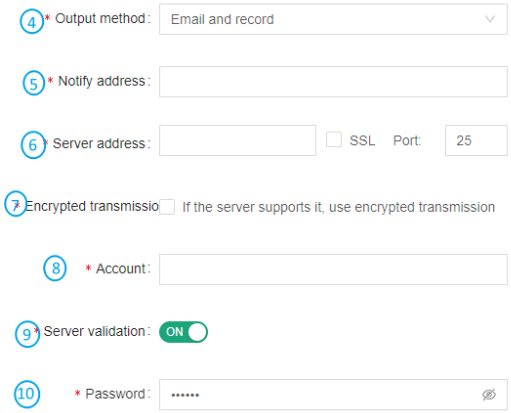
When the alarm rules are created, you can set the parameters for pushing an alarm on the **Alarm Broadcast** page.



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.

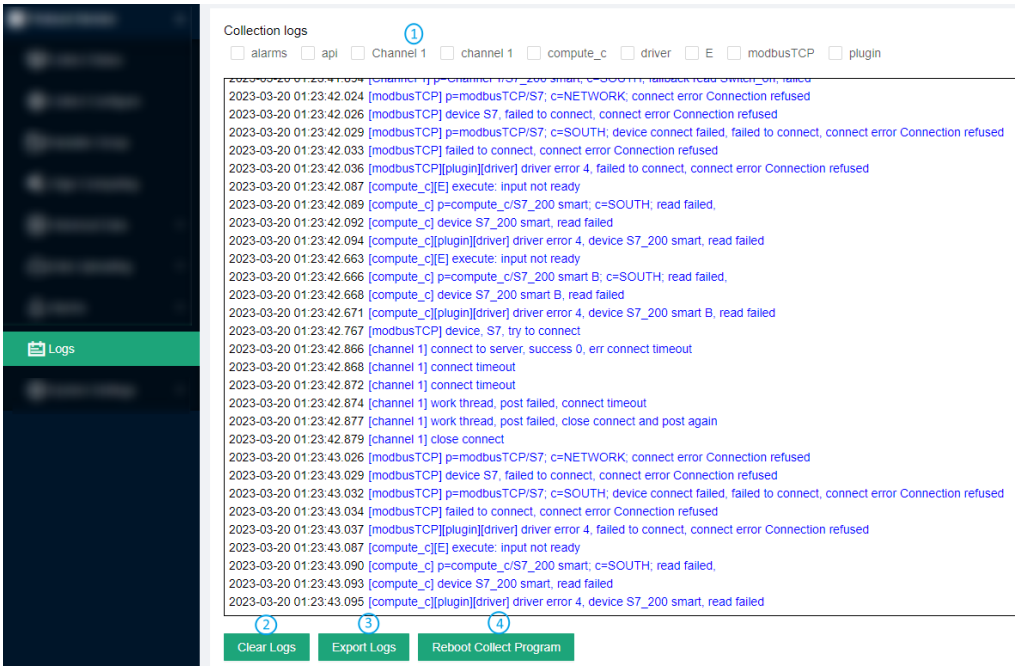
When you are all set, you can send a test email to check if the settings are ok, then submit the settings.

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.



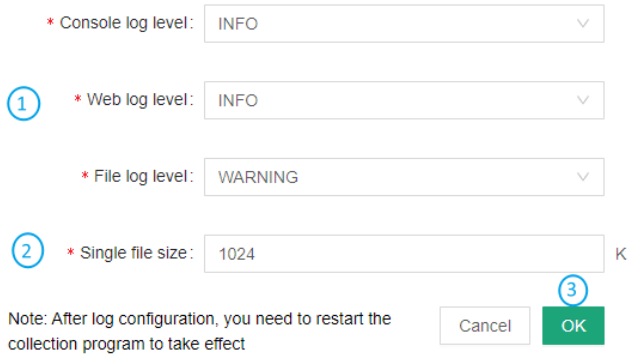
Description:

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.