

RAH305 Wi-Fi HaLow Router



User Manual

Version: 1.3

© Vantron Technology, Inc. All rights reserved.

Revision History

No.		Description	Date
V1.0	VantronOS 25 - V200R003.F0000-03	First release	Aug. 5, 2025
V1.1	VantronOS 25 - V200R003.F0000-03	1. Updated I/O description and the wiring description. 2. Modified the description on SSH access.	Oct. 3, 2025
V1.2	VantronOS 25 - V200R003.F0000-03	1. Updated chapter 3 based on the current VantronOS 25 firmware. 2. Added chapter 4 for industrial protocol configurations and explained incomplete contents.	Feb. 13, 2026
V1.3	VantronOS 25 - V200R003.F0000-04	1. Updated button and LED definitions. 2. Updated the illustrative figures in Section 2.2. 3. Updated Section 2.4 to add the Linux login method. 4. Added the wireless quick pairing instructions for Wi-Fi WPS and HaLow DPP pairing.	Jul. 3, 2026

Table of Contents

Foreword.....	4
CHAPTER 1 HARDWARE DESCRIPTION.....	8
1.1 Overview	9
1.2 Features.....	9
1.3 Unpacking.....	10
1.4 Mechanical Outline	10
1.5 Terminologies and Acronyms	11
1.6 Specifications.....	13
1.7 Product Layout	15
1.8 Wiring Instructions	17
1.8.1 Power Input.....	17
1.8.2 Digital Input (DI)	17
1.8.3 Digital Output (DO).....	17
1.8.4 Analog Input (AI)	18
1.8.5 Analog Output (AO).....	18
1.8.6 RS-232/485/422	18
1.9 LED Indicators.....	20
1.9.1 Power LED.....	20
1.9.2 SYS LED	20
1.9.3 WLAN (Wi-Fi) LED	20
1.9.4 Cellular Signal Strength LED	21
1.10 Button.....	21
1.10.1 Reset Button	21
1.10.2 WPS Button	22
1.10.3 DPP Button	22
1.11 Console Port	22
1.12 SIM Slot	22
1.13 USB Type-A	22
CHAPTER 2 GETTING STARTED	23
2.1 Device Installation	24
2.2 Hardware Connection	25
2.3 Web Login.....	29
2.3.1 Login Wizard.....	31
2.3.2 Log Out	37
2.4 SSH Login	37
2.5 Debugging the Device (via Console Port)	39
2.6 Wireless Quick Pairing.....	41
2.6.1 Wi-Fi WPS Connection.....	41
2.6.2 HaLow DPP Pairing	42
CHAPTER 3 DEVICE SETUP VIA VANTRONOS.....	43
3.1 Introduction to VantronOS	44
3.1.1 Web Overview	44

3.1.2	Language Change	45
3.2	Dashboard	46
3.3	Network.....	47
3.3.1	WAN Interface.....	47
3.3.1.1	Basic IP Configuration.....	47
3.3.1.2	Interface Bridging.....	49
3.3.1.3	Link Priority	50
3.3.1.4	Link Diagnosis	51
3.3.2	LAN Interface.....	52
3.3.2.1	Subnet Conflict	52
3.3.2.2	DHCP Service & DHCP Reservation	53
3.3.3	IPv6 Settings	54
3.3.4	Cellular	55
3.3.4.1	Basic Settings.....	56
3.3.4.2	Advanced Settings	57
3.3.5	Wi-Fi	59
3.3.5.1	AP-Mode Basic Settings.....	59
3.3.5.2	AP-Mode Advanced Settings	60
3.3.5.3	STA-Mode Basic Settings	61
3.3.5.4	STA-Mode Advanced Settings.....	62
3.3.6	VPN	63
3.3.6.1	OpenVPN Server-Client Network Settings.....	63
3.3.6.2	OpenVPN Server Setup.....	65
3.3.6.3	OpenVPN Client Setup.....	67
3.3.6.4	Application Scenario Topology.....	69
3.3.7	QoS Bandwidth Control.....	71
3.3.8	Static Route	72
3.3.9	Porting Mapping.....	74
3.3.10	Network Security.....	76
3.3.10.1	Basic SSH Access Setup	76
3.3.10.2	ACL Access Control.....	77
3.4	HaLow.....	80
3.4.1	Overview	80
3.4.2	DDP Pairing via Software Setup.....	81
3.4.3	Mesh Networking.....	82
3.5	Terminals	82
3.6	System	82
3.6.1	Device Settings	82
3.6.1.1	Modifying Device Name	83
3.6.1.2	System Time	84
3.6.2	User Management.....	85
3.6.3	Diagnostics	85
3.6.3.1	Network Diagnostics.....	86

3.6.3.2 Web Terminal	87
3.6.3.3 Logs	88
3.6.3.4 Log Capture	88
3.6.4 System Maintenance	90
3.6.4.1 BlueSphere	90
3.6.4.2 Device Maintenance	91
3.7 Edge Computing	92
3.7.1 Serial to TCP.....	93
3.7.1.1 Server Mode Rule Setup.....	94
3.7.1.2 Client Mode Rule Setup.....	95
3.7.2 PLC	96
CHAPTER 4 INDUSTRIAL PROTOCOLPORTAL	97
4.1 Overview	98
4.2 I/O Configuration.....	98
4.2.1 DI/DO Configuration.....	98
4.2.2 AI/AO Configuration	100
4.3 Portal Login.....	101
CHAPTER 5 DISPOSAL AND WARRANTY	102
5.1 Disposal	103
5.2 Warranty.....	104
Appendix Regulatory Compliance Statement	105

Foreword

Thank you for purchasing RAH305 Wi-Fi HaLow Router (“the Product” or “the router”). This manual intends to provide guidance and assistance necessary on setting up, operating and maintaining the Product. Please read this manual and make sure you understand the structure and functionality of the Product before putting it into use.

Unless otherwise stated, Wi-Fi in this manual refers to the device’s 2.4GHz/5GHz Wi-Fi (Wi-Fi 6), and HaLow refers to Wi-Fi HaLow.

Intended Users

This manual is intended for:

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

Copyright

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

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

Disclaimer

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

It is our practice to change part numbers when published ratings or features are changed, or when significant structure changes are made. However, some specifications of the Product may be changed without notice.

Technical Support and Assistance

Should you have any question about the Product that is not covered in this manual, contact your sales representative for solution. Please include the following information in your question:

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

Vantron Technology, Inc.

Address: 48434 Milmont Drive, Fremont, CA 94538

Tel: (650) 422-3128

Email: sales@vantrontech.com

Regulatory Information

The Product is designed to comply with:

- FCC
- ISED
- CE

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.

	Caution for latent damage to system or human injury
	Attention to important information or regulations

General Safety Instructions

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

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

Precautions for Power Cables and Accessories

-  Use proper power source only. Make sure the supply voltage falls within the specified range. The Product is designed to use 9-36V DC. Always check whether the Product is DC powered before applying power.
-  Place the cables properly at places without extrusion hazards.
-  Use only approved antenna(s). Non-approved antenna(s) may produce spurious or excessive RF transmitting power which may violate FCC limits.
-  Cleaning instructions:
 - Power off the Product before cleaning
 - Do not use spray detergent
 - Clean with a damp cloth
 - Do not try to clean exposed electronic components unless with a dust collector
-  Power off and contact Vantron technical support engineer in case of the following faults:
 - The Product is damaged
 - The temperature is excessively high
 - Fault is still not solved after troubleshooting according to this manual
-  Do not use in combustible and explosive environment:
 - Keep away from combustible and explosive environment
 - Keep away from all energized circuits
 - Unauthorized removal of the enclosure from the Product is not allowed
 - Do not change components unless the power cable is unplugged
 - In some cases, the Product may still have residual voltage even if the power cable is unplugged. Therefore, it is a must to remove and fully discharge the Product before replacement of the components.

CHAPTER 1 HARDWARE DESCRIPTION

1.1 Overview

Powered by the advanced MM6108 Wi-Fi HaLow chipset, Vantron RAH305 redefines the long-range connectivity. Complying with the IEEE 802.11ah (Wi-Fi HaLow) standard and the latest WPA3 security protocol, it delivers exceptional kilometer-range wireless coverage with superior penetration through obstacles. This enables secure, massive connectivity for thousands of IoT devices across vast areas. It also supports traditional Wi-Fi 6, providing unparalleled deployment flexibility for large-scale industrial, agricultural, and smart city applications.

The RAH305 ensures always-on connectivity with integrated LTE CAT 4 backup, precise GNSS location tracking, and Bluetooth 5.3 support. Its wired connectivity includes five Gigabit Ethernet ports—one configurable WAN/LAN and four LAN—delivering robust network infrastructure. A comprehensive suite of industrial interfaces, including a USB 2.0 port, a DB9 serial port (configurable for RS232/422/485), and 4 x DI/DO and 4 x AI/AO channels, allows for seamless integration with a wide array of machinery, sensors, and legacy systems.

The RAH305 features WPS and DPP buttons for quick Wi-Fi 6 and Wi-Fi HaLow pairing. It supports AP mode for both Wi-Fi 6 and Wi-Fi HaLow, with the latter also supporting Mesh functionalities, facilitating resilient, scalable, and future-proof IoT network deployment.

1.2 Features

- Dual wireless integration: Wi-Fi 6 + Wi-Fi HaLow
- 4 x LAN, 1 x WAN, LTE CAT 4, BT 5.3, GNSS
- Rich industrial interfaces: AI/AO, DI/DO, USB, RS-232/485/422
- Supports sub-1 GHz low-frequency communication
- Long-distance transmission, coverage up to 1 km
- Better penetration through walls and obstacles
- Supports 1/2/4/8 MHz channel bandwidths with dynamic channel selection (DCS)
- Optional BlueSphere GWM support for remote control
- Industrial extended input voltage operation
- Wi-Fi HaLow DPP fast pairing supported

1.3 Unpacking

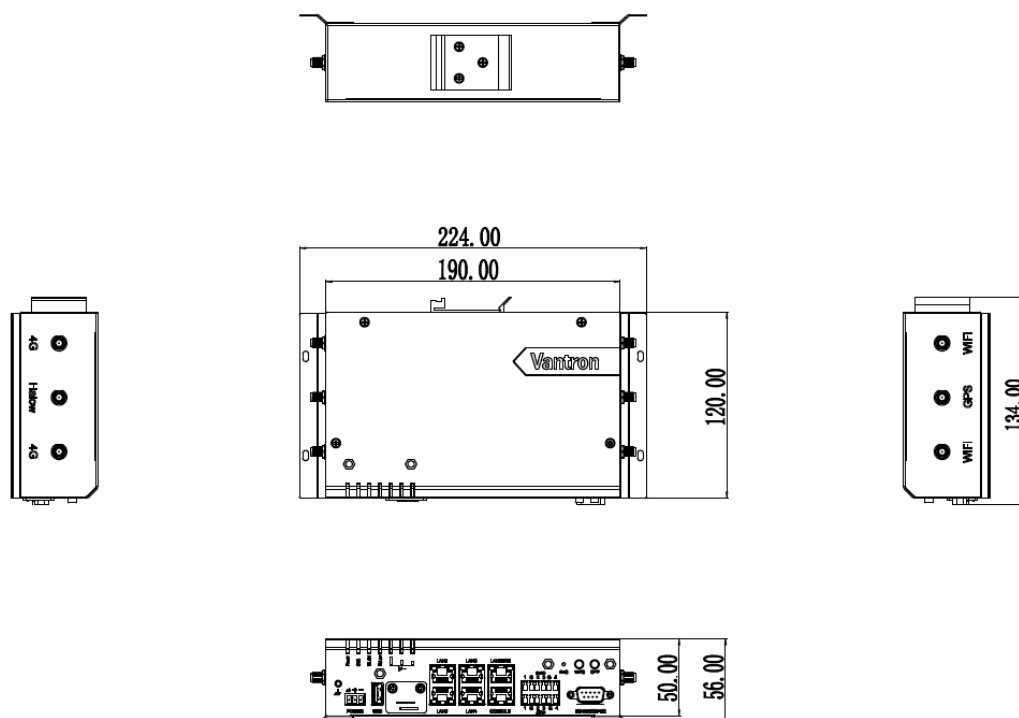
The Product has been carefully packed with special attention to quality. However, should you find anything damaged or missing, please contact your sales representative in due time.

Standard Accessories

- 1 x RAH305 Wi-Fi HaLow router
- 1 x Wi-Fi HaLow antenna
- 2 x 2.4GHz/5GHz Wi-Fi antenna
- 1 x GNSS magnetic mount antenna
- 2 x 4G LTE magnetic mount antenna
- 2 x 3.81mm x 6-pin terminal connector for DI, DO, AI, AO
- 1 x 12V 2A DC Power adapter
- 1 x DC power connector

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

1.4 Mechanical Outline



1.5 Terminologies and Acronyms

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

Glossary	Description
AP	HaLow access point. An 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.
STA	HaLow station. An STA is a client device that connects to a HaLow AP for a Standard HaLow connection. These devices typically access external networks through the HaLow AP.
Standard HaLow mode	Standard HaLow mode refers to a basic HaLow network architecture where Stations (STAs) communicate directly with an Access Point (AP). This AP is typically connected to an internet router to provide connectivity.
HaLow Mesh mode	In a HaLow Mesh configuration, all devices communicate with each other to automatically determine the most efficient path for data transmission, helping to extend network range and improve reliability.
Mesh Portal (MPP)	A Mesh Portal serves as a DHCP server in a mesh network for internal IP assignment. There is at most one Mesh Portal in a mesh network.
Mesh Point (MP)	A Mesh Point operates as an intermediate HaLow node that extends the network coverage through multi-hop communication. In the absence of an MPP in a mesh network, there must be an MP connected to an external network to relay IP addresses from an upstream DHCP server.
WPS	Wi-Fi Protected Setup (WPS), an official Wi-Fi Alliance standard designed to simplify secure wireless pairing between a router/gateway and Wi-Fi-enabled end devices (sensors, industrial panels, PLCs, handheld terminals). This operation eliminates the need to manually input a password.

Glossary	Description
DPP	Device Provisioning Protocol. 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.
DCS	Dynamic Channel Selection. Once enabled, the device will automatically select the channel with the strongest signal within the selected bandwidth for optimal performance.

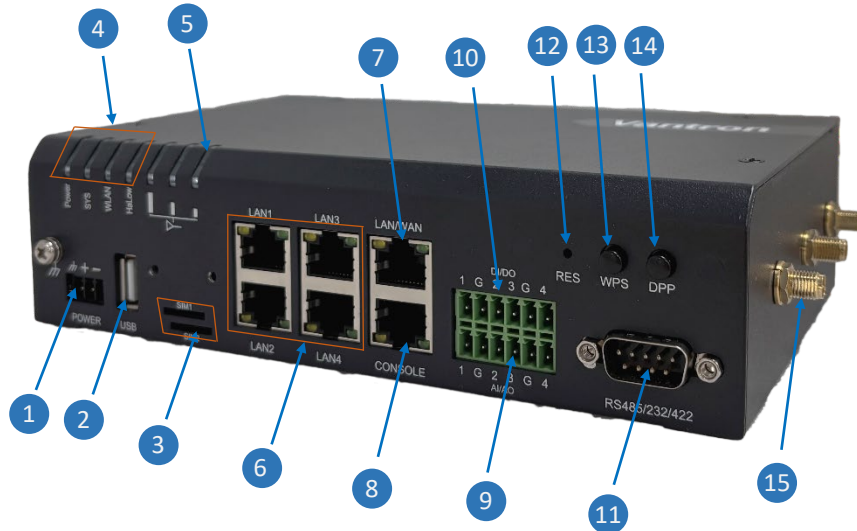
Unless otherwise stated, *Wi-Fi* in this manual refers to the device's 2.4GHz/5GHz Wi-Fi (Wi-Fi 6), and *HaLow* refers to Wi-Fi HaLow.

1.6 Specifications

RAH305		
HARDWARE		
System	CPU	Ti AM64 64-bit Arm® Cortex®-A53 microprocessor, up to 1GHz
	Wi-Fi HaLow SoC	Morse Micro MM6108
	Memory	1GB DDR4
	Storage	8GB eMMC
WLAN	Wi-Fi 6	Standard: IEEE 802.11ax/ac/a/b/g/n
		Frequency range: 2.400GHz~2.835GHz, 5.150GHz~5.850GHz (Subject to local regulations)
		Channel bandwidth: 20/40/80MHz
		Data rate: up to 1200Mbps @80MHz
		Quick pairing: WPS quick pairing supported
		Working mode: AP
	Wi-Fi HaLow	Standard: IEEE 802.11 ah
		Frequency range: 903.5MHz~926.5MHz (US)
		Channel bandwidth: 1/2/4/8MHz, dynamic channel selection (DCS) supported
		Transmit power: 23dBm
		Data rate: up to 32.5 Mbps @8MHz or 15 Mbps @4MHz
		Application mode: Mesh, BridgeWAN
		Quick pairing: DPP quick pairing supported
		Working mode: AP, Mesh
Bluetooth*	Version	BT 5.3
Cellular	Category	LTE CAT 4
	Frequency Band	LTE-FDD: B1, B2, B3, B4, B5, B7, B8, B12, B13, B18, B19, B20, B25, B26, B28, B66 LTE-TDD: B34, B38, B39, B40, B41
	Data Rate	Theoretical: 150 Mbps (DL) / 50 Mbps (UL)
GNSS*	Satellite Support	GPS, Beidou, GLONASS, GALILEO, QZSS (A-GNSS supported)
	Positioning Precision	2.5m (CEP50)
I/O	Ethernet	5 x RJ45, 10/100/1000Mbps (1 x WAN/LAN, 4 x LAN)
	Console	1 x RS232-to-RJ45 port
	USB	1 x USB 2.0 Type-A
	Serial Port	1 x RS485/232/422 (DB9, baud rate: 115200)
	DI/DO	4 x DI/DO (Software switchable, measurement: DI: 0-VIN, DO: 0-VIN)
	AI/AO	4 x AI/AO (Software switchable, measurement: AI: 0-10V, AO: 4-20mA)
	SIM slot	2 x Micro SIM slot
	Antenna	1 x Wi-Fi HaLow antenna
		2 x Wi-Fi (6) antenna
		2 x 4G LTE antenna
		1 x GNSS antenna

RAH305					
System Control	LED indicators	1 x Power indicator		1 x Wi-Fi HaLow activity indicator	
		1 x System indicator		1 x WLAN (Wi-Fi 6) activity indicator	
		3 x LTE signal strength indicator			
	Button	1 x Restore button (pinhole)			
		1 x WPS button (Wi-Fi quick pairing)		1 x DPP button (HaLow quick pairing)	
Miscellaneous	RTC	Supported			
	WDT	Supported			
Mechanical	Casing material	SGCC (Steel Galvanized Cold Commercial)			
	Dimensions	224mm x 134mm x 56mm			
	Installation	Wall mounting, DIN rail mounting			
Power	Input	9V ~ 36V DC			
	Port	3-Pin x 3.81mm terminal (Over-current protection, reverse polarity protection)			
Environmental	Temperature	Operating: -20°C~+60°C		Storage: -40°C~+70°C	
	Humidity	Storage: 5%~95% RH (Non-condensing)			
Certification	Compliance	CE, FCC, ISED, PTCRB (In progress)			
	Carrier certification	AT&T, Verizon, T-Mobile			
SOFTWARE					
Device Management	Operating system	Web-based VantronOS			
	Configuration	VantronOS, SSH, console, cloud-based BlueSphere GWM (Optional)			
	Remote management	BlueSphere GWM (Optional)			
Routing & Network Reliability	Network protocol	IPv4, HTTPS, TCP & UDP, NTP client and server, ARP, TLS			
	Link detection & report	Address: IP, URL		Protocol: ICMP, TCP, HTTP	
	Failover	Auto routing		Network priority: Ethernet > Wi-Fi client > LTE/5G (Def.)	
	Dual SIM	Dual SIM failover, automatic switch			
	NAT	Network address translation Supported			
	WAN protocol	DHCP client, PPPoE, Static IP			
	IP application	Ping, Traceroute, DHCP Server/Client, DDNS			
	IP routing	Static routing			
	Network Diagnostics	Statistics	Traffic data and up time at Ethernet WAN, Wi-Fi client WAN, cellular WAN Cellular and Wi-Fi signal strength; SIM card switch frequency		
Health check		Usage of CPU, memory, disk; service running status Alarm on Ethernet/Wi-Fi/cellular hardware abnormality			
Log		System log, diagnostic log; log export supported			
Security	Firewall	Stateful, whitelist control, ingress/egress filtering			
	Access control	MAC address filtering, IP address filtering			
	VPN	PPTP*, L2TP*, GRE*, IPSec, OpenVPN			
	Firmware validation	SHA256 checksum			

1.7 Product Layout



Description:

Item	Description
1	9~36V power terminal (1: GND, 2: V+, 3: V-)
2	USB 2.0 Type-A
3	2 x Micro SIM slot
4	4 x LED indicator (Power, System, WLAN, HaLow). Refer to Section 1.9 for the definition.
5	4G LTE signal strength LED. Refer to Section 1.9 for the definition.
6	4 x LAN, connects local devices for data communication or device management.
7	WAN (switchable to LAN), connects to an external network to provide internet access to the local network.
8	Console port, provides out-of-band management access to the device shell (Baud rate: 115200).
9	AI/AO 1~4, software switchable. AI: 0~10V input (12-bit res.); 4~20mA output (12-bit res.)
10	DI/DO 1~4, software switchable. DO output voltage follows device supply voltage. DI: 0~12V, max. 200mA, pulse counter supported (max. frequency <25Hz).
11	RS-232/485/422 (uart0), mode switchable via the VantronOS web portal (default parameters: 9600, 8N1).

Item	Description
12	Reset pinhole button ([2s, 6s): Device restart; [6, 12s): Configuration clear; [12, 20s): Factory reset; [20s,+∞): Normal operation)
13	WPS quick pairing button. Supports one-touch Wi-Fi quick connection.
14	DPP quick pairing button. Supports one-touch Wi-Fi HaLow quick pairing.
15	3 x Antenna connector (Far → Near: Wi-Fi (6) antenna, GNSS antenna, Wi-Fi (6) antenna)

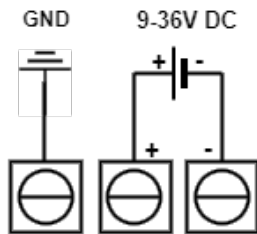


Description:

Item	Description
1	DIN rail mount
2	3 x Antenna connector (Far → Near: 4G LTE antenna, Wi-Fi HaLow antenna, 4G LTE antenna)

1.8 Wiring Instructions

1.8.1 Power Input



Power terminal: 1 x 3 x 3.81mm, 12V/2A DC recommended.

1.8.2 Digital Input (DI)

Each digital input channel supports software-configurable dry/wet contact mode.

Wiring:

DIx → External switch or sensor signal wire

GND → Signal ground

DI input range: 0–12V, max input current 200mA. Pulse counting function supported (frequency <25Hz).

1.8.3 Digital Output (DO)

The RAH305 provides four analog input channels for 0~10V voltage measurement.

Wiring:

DOx → Positive terminal of external load (indicator light, small relay)

GND → Negative terminal of external load

DO output voltage is consistent with the device supply voltage, max 200mA per channel output.

1.8.4 Analog Input (AI)

The RAH305 provides four analog input channels for 0-10V voltage measurement.

Wiring:

AIx → Switch/sensor V+

GND → Switch/sensor V-

1.8.5 Analog Output (AO)

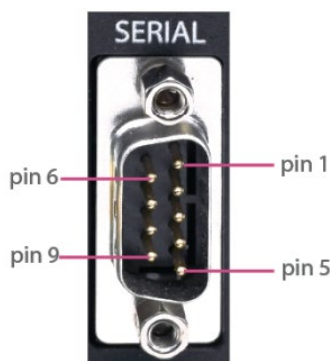
The RAH305 provides four analog output channels for 4-20mA current control. Testing AO requires an external load. Shell commands are used to write raw DAC values to the sysfs nodes to adjust the AO output current.

Wiring:

AOx → Load +

GND → Load –

1.8.6 RS-232/485/422

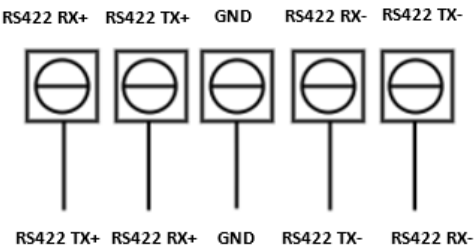
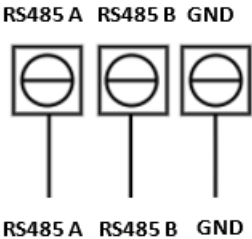
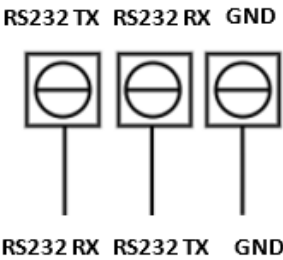


The RAH305 provides an RS-232/RS-485/RS-422 multiplexer for local data transfer. The multiplexer defaults to the RS-422 mode and can be modified via the **Edit** menu on the **Edge Computing > Serial-to-TCP** page. Refer to Section [3.7.1](#) for details.

Pinout description:

Item	RS-232	RS-485	RS-422
1			
2	RXD	A	TX+
3	TXD		RX+
4			
5	GND		GND
6		B	TX-
7			
8			
9			RX-

Wiring:



1.9 LED Indicators

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

Individual LEDs are defined as follows.

1.9.1 Power LED

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

1.9.2 SYS LED

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

1.9.3 WLAN (Wi-Fi) LED

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

1.9.4 Cellular Signal Strength LED

Signal Strength	Description
>67%	All three LEDs turn solid green.
Between 38% and 67%	The middle and right LEDs turn solid green.
<38%	The right LED blinks.

1.10 Button

1.10.1 Reset Button

The RAH305 offers a **Reset** (RST) pinhole button that allows the device to restart or reset as defined below:

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

1.10.2 WPS Button

The RAH305 supports Wi-Fi Protected Setup (WPS). It removes the need to manually input Wi-Fi SSIDs and passwords, enabling fast, secure Wi-Fi connections between the Wi-Fi AP and client.

Refer to Section [2.6.1](#) for the steps of WPS connection.

1.10.3 DPP Button

The RAH305 also supports Device Provisioning Protocol (DPP), enabling fast provisioning of two HaLow devices for a Standard HaLow connection.

Refer to Section [2.6.2](#) for the steps of DPP pairing.

1.11 Console Port

The RAH305 offers a console port as a dedicated serial management interface, providing out-of-band access to the device's command-line interface (CLI).

To access the device shell, connect the RAH305's console port to a host PC using an USB-to-RJ45 Console cable.

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

Refer to Section [2.5](#) for the specific debugging steps.

1.12 SIM Slot

The RAH305 is equipped with two Micro SIM slots. With dual SIMs installed, the device automatically switches to the line with the stronger signal whenever the current cellular connection becomes unstable.

1.13 USB Type-A

The RAH305 offers a USB 2.0 Type-A port. Users can plug in a USB storage drive to export device running logs or complete offline firmware updates on-site.

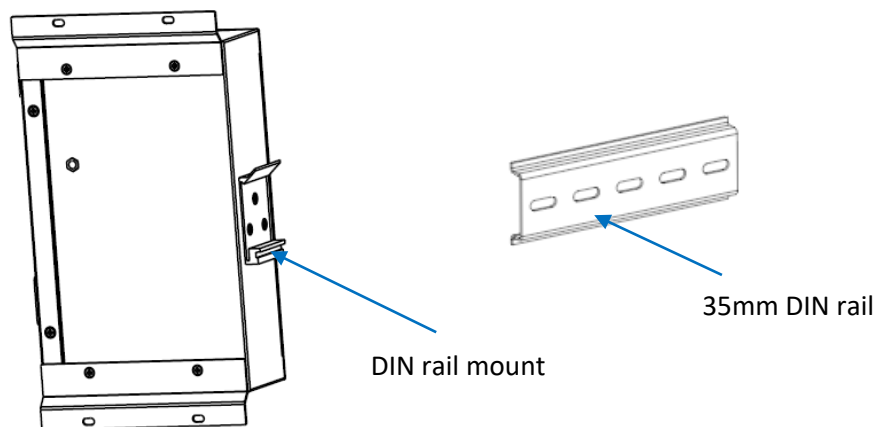
CHAPTER 2 GETTING STARTED

2.1 Device Installation

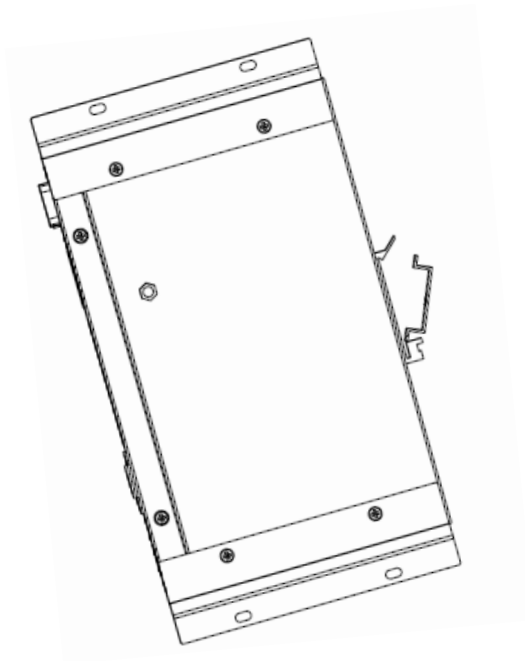
When mounting the RAH305 on a vertical surface, please ensure that the device is oriented with the LED indicators facing down. This positioning allows the LEDs to be visible to the user on the ground.

The following steps detail DIN rail mounting procedures.

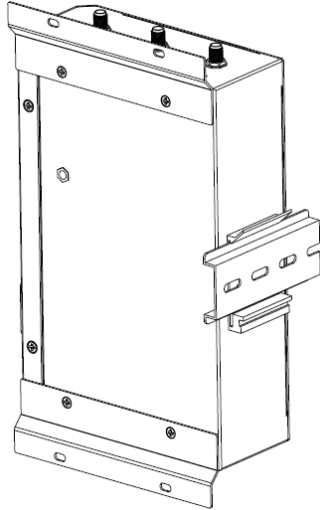
1. Hold the router vertically, and align the DIN rail mount of the device to the 35mm DIN rail.



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



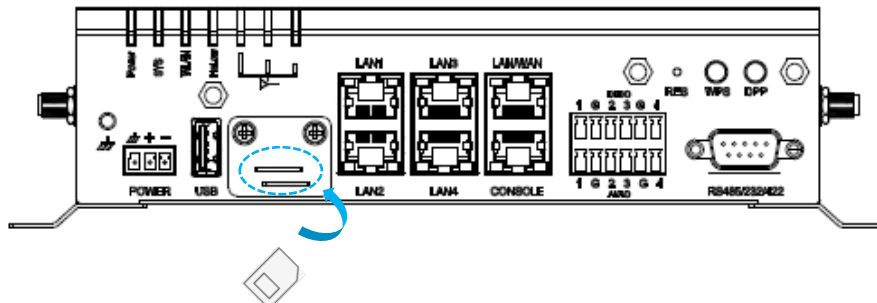
3. Push the router toward the DIN rail until it snaps securely into place.
4. Gently swing the device to make sure it is fixed on the DIN rail.



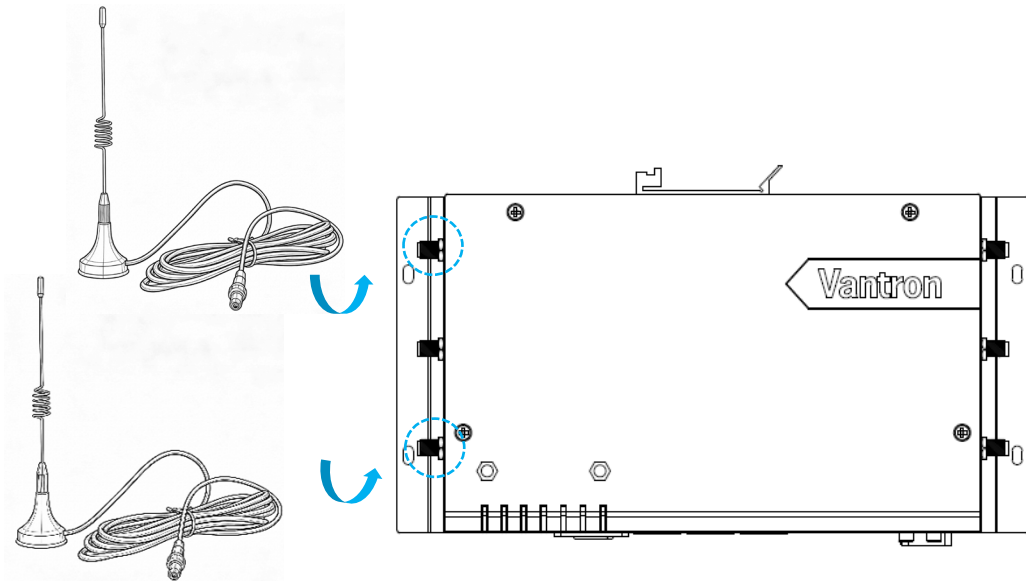
2.2 Hardware Connection

After installation, complete the hardware connections below **as needed** for smooth operation of the RAH305.

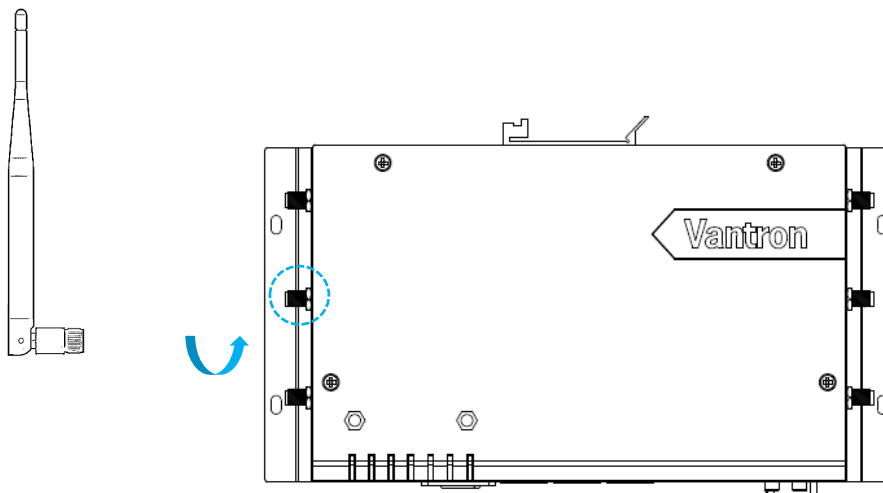
1. Based on your actual situation, insert an activated Micro SIM card into the desired slot and push the card in until it clicks.
 - For SIM 1: gold contacts facing **down**;
 - For SIM 2: gold contacts facing **up**.



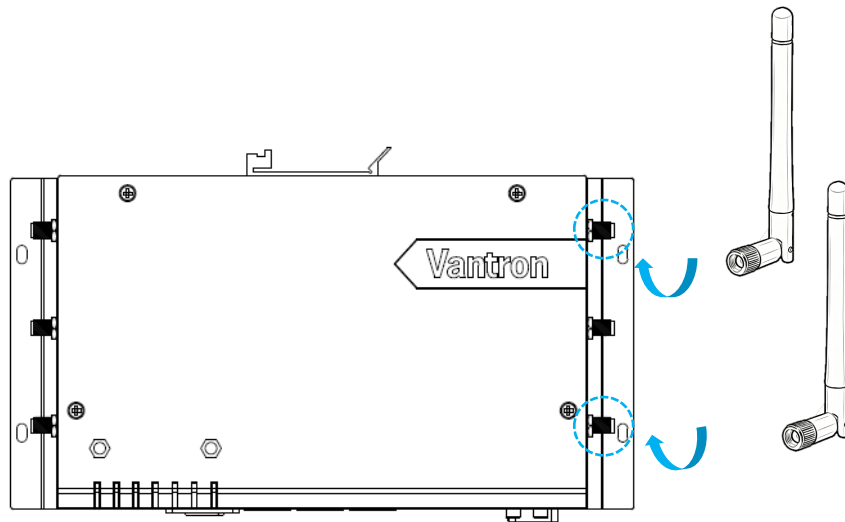
2. For cellular connectivity, install cellular antennas (magnetic mount) onto their matching connectors on the device's left side.



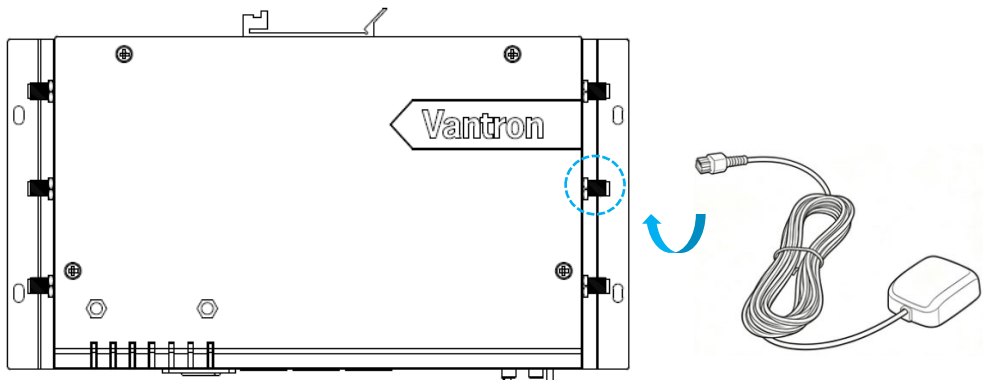
3. Attach the HaLow antenna (with longer tip) to the middle connector on the left side.



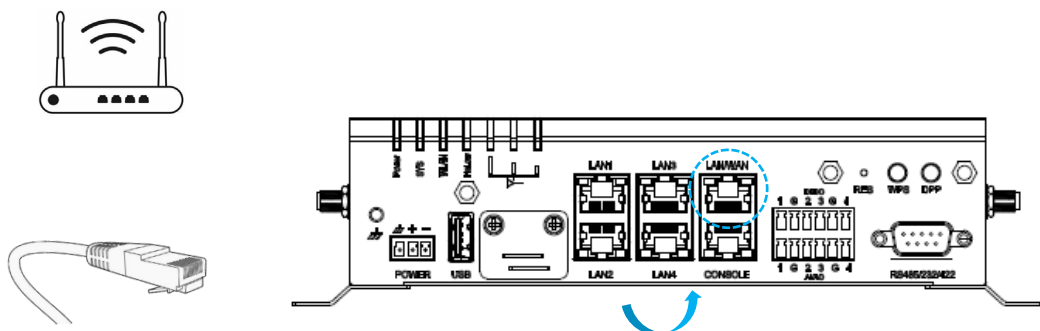
4. Install the Wi-Fi antennas onto their matching connectors on the device's right side.



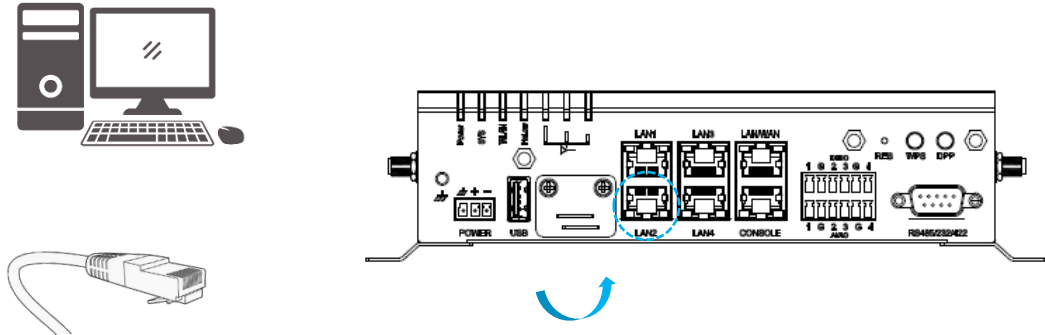
5. Install the GNSS antenna (magnetic mount) to the middle connector on the left side.



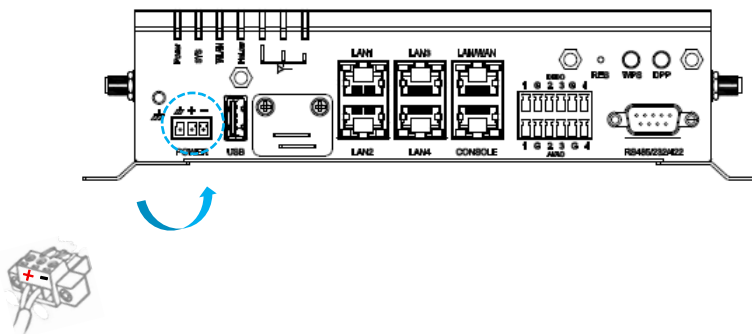
6. Connect the router's WAN port to the upstream network (e.g. an Ethernet switch).



7. Connect a PC or other network devices to the router's LAN port (LAN 1~LAN 4) using an Ethernet cable for local management or Internet access.



8. For wiring of the AI/DI/DO channels, refer to the wiring instructions in Section [1.8](#).
9. Insert the terminal block of the DC power connector into the router's power terminal and connect the other end to the power cord.



10. Plug the power adapter into a DC outlet that meets the device's operating voltage requirement (9V~36V DC) to power on the router.
11. After power-on, the Power and SYS LEDs turn solid green to indicate the device is working properly.

2.3 Web Login

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

There are two login options to access VantronOS for the RAH305, depending on how the host PC is connected to it.

Method	Host PC Connection	Login Address
Option 1	Host connected to the device's LAN network (via Ethernet or Wi-Fi).	RAH305's LAN IP
Option 2	Host's WAN interface on the same IP subnet as RAH305's WAN interface (e.g., both connected to the same Ethernet switch or upstream Wi-Fi).	RAH305's WAN IP

We recommend initially logging into VantronOS using Option 1. Afterwards, you may establish additional connections between RAH305 and your host PC, and switch to the other login option as needed by referring to the device's IP addresses listed under the **Network** tab in VantronOS.

Steps:

1. Connect the host PC:

- Via Ethernet

Connect the host PC directly to the RAH305's LAN port using a standard Ethernet cable.

- Via Wi-Fi

Connect the host PC to RAH305's Wi-Fi using the default SSID and password provided on the device label.

Vantron	Embedded in your success Embedded in your better life
IMEI No.: XXXXXXXXXXXXXXXX HaLow MAC: XX:XX:XX:XX:XX:XX LAN MAC: XX:XX:XX:XX:XX:XX LAN/WAN MAC: XX:XX:XX:XX:XX:XX WLAN MAC: XX:XX:XX:XX:XX:XX Bluetooth MAC: XX:XX:XX:XX:XX:XX Login IP: 172.18.1.1 User name/Password: admin/XXXXXX WLAN SSID: XXXXXX WLAN Password: XXXXXXXX	

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

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

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

Vantron	Embedded in your success Embedded in your better life
IMEI No.: XXXXXXXXXXXXXXXX	
HaLow MAC: XX:XX:XX:XX:XX:XX	
LAN MAC: XX:XX:XX:XX:XX:XX	
LAN/WAN MAC: XX:XX:XX:XX:XX:XX	
WLAN MAC: XX:XX:XX:XX:XX:XX	
Bluetooth MAC: XX:XX:XX:XX:XX:XX	
Login IP: 172.18.1.1	
User name/Password: admin/XXXXXX	
WLAN SSID: XXXXXX	
WLAN Password: XXXXXXXX	

← → ↻ https://172.18.1.1/#/login

VantronOS 25



VT-M2M-RAH305

User

Password

Login

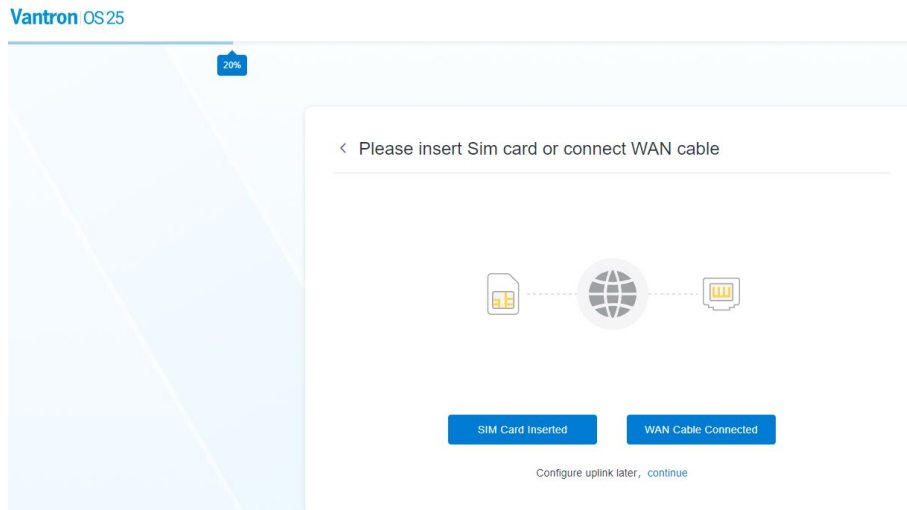
[Forgot Password](#)

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

2.3.1 Login Wizard

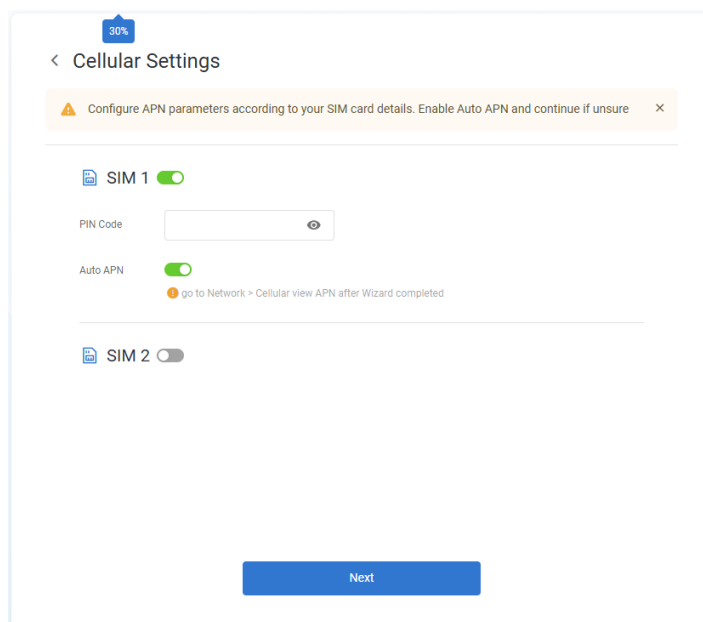
For first-time login or login after a device reset, the setup wizard will guide you through the initial setup process for quick setup.

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



- **Setup with Active Cellular Network (SIM Card Inserted)**

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



PIN: Carrier-defined, optional.

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

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

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

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

< Cellular Traffic Control 40%

Traffic Control ☒

SIM 1

Total flow 600 (mb) Used threshold 80 (%)

After exceeding the threshold Uplink Rate Limiting Limited speed 60 (kb/s)

SIM 2

Total flow 600 (mb) Used threshold 80 (%)

After exceeding the threshold Uplink Rate Limiting Limited speed 60 (kb/s)

Next

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

VantronOS 25

< Configure Wi-Fi SSID and Password

50%

Wi-Fi AP

Frequency Band: 2.4GHz Wi-Fi AP 5GHz Wi-Fi AP Currently, only one Wi-Fi frequency band is supported.

SSID: RAH305-9ACC Encryption: WPA2-PSK

Password:

Next

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

< Complete essential system settings

Change user password

Password: Confirm Password:

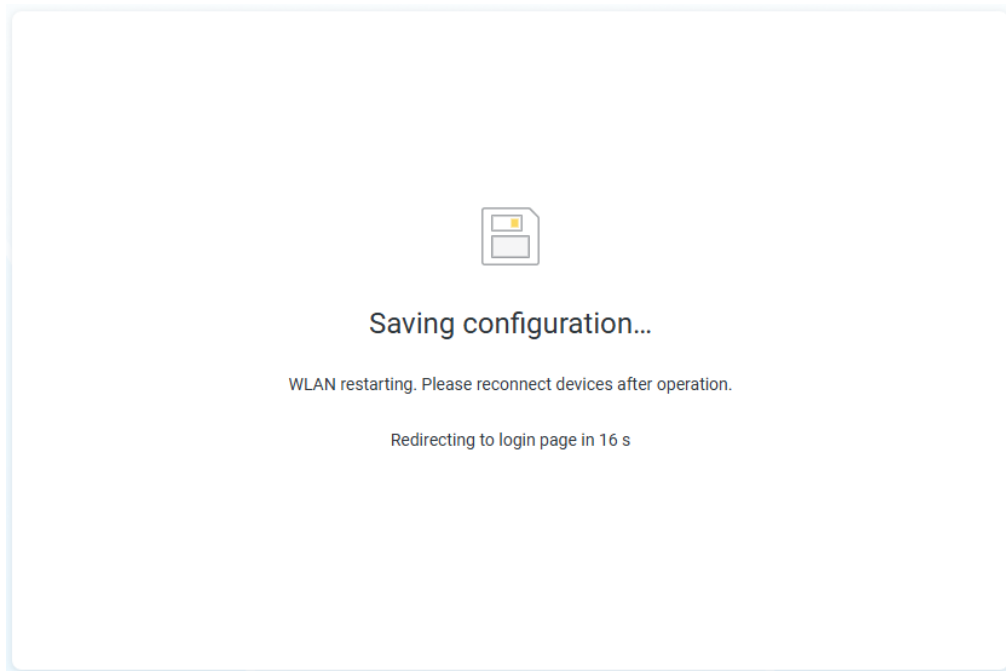
Time Settings

Sync Local Time: ☒

Time Zone: UTC+8:00, China Stand...

Next

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

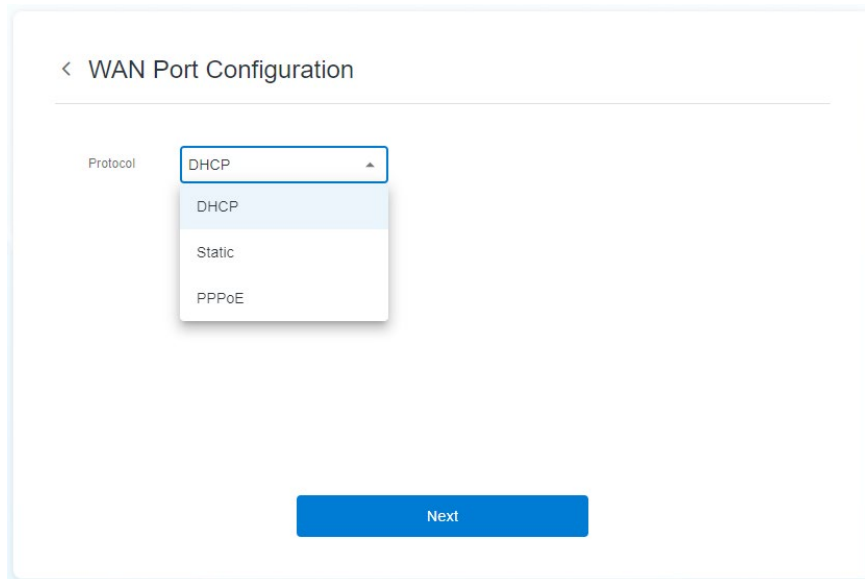


6. Log back in to the web portal using the new password.

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

- **Setup with WAN Port Connected (WAN Cable Connected)**

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



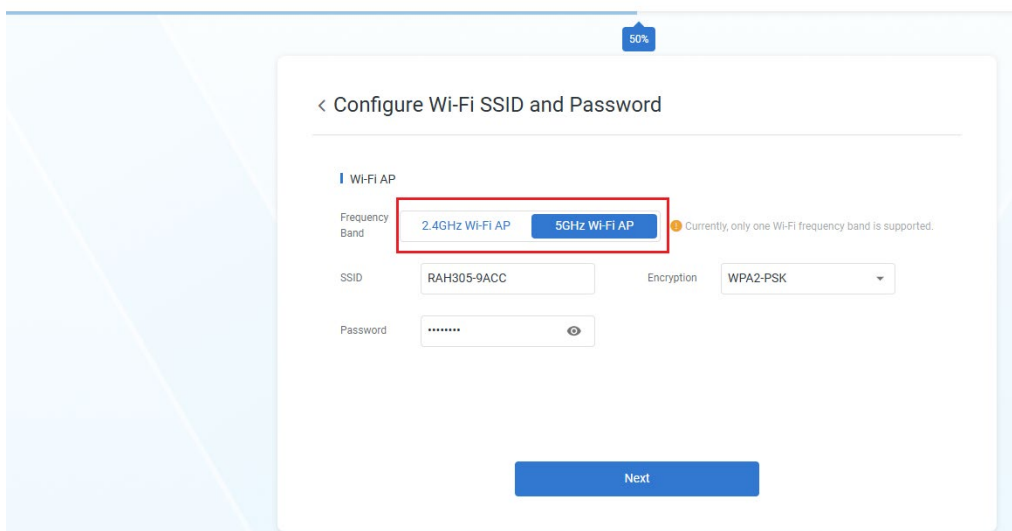
DHCP (Dynamic Host Configuration Protocol): A DHCP server **automatically** assigns IP addresses and network configuration (subnet, gateway, DNS) to the device.

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

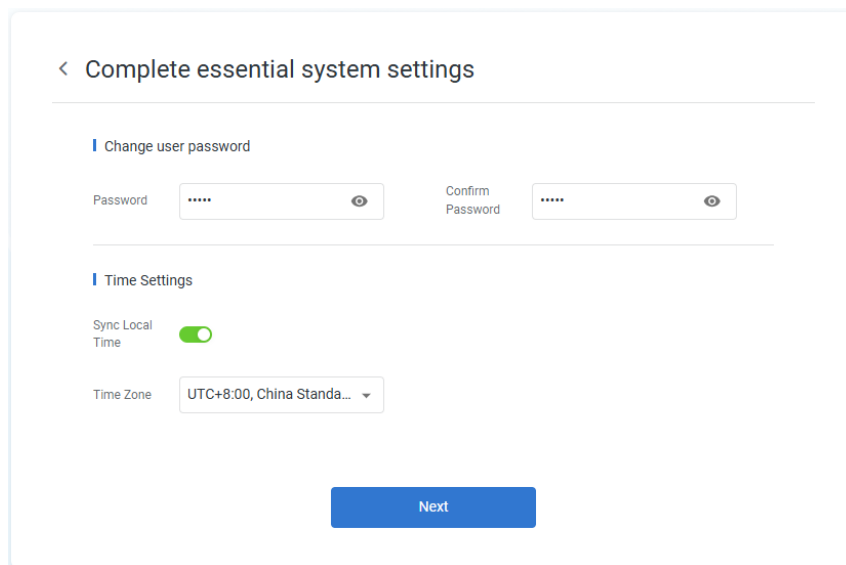
PPPoE (Point-to-Point Protocol over Ethernet): The device **dial-ups** an ISP using a username and password encapsulated in PPP over Ethernet; the ISP then assigns IP settings dynamically (or sometimes fixed).

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

VantronOS 25



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

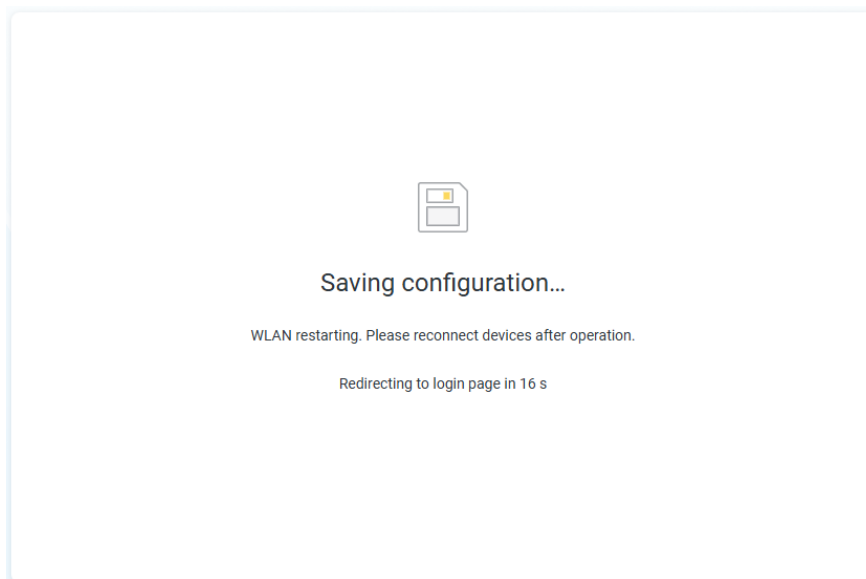


The screenshot shows a web interface titled "Complete essential system settings". It has two main sections: "Change user password" and "Time Settings".

- Change user password:** Contains two input fields labeled "Password" and "Confirm Password", both with masked characters (dots) and toggle icons for visibility.
- Time Settings:** Contains a "Sync Local Time" toggle switch that is currently turned on (green), and a "Time Zone" dropdown menu showing "UTC+8:00, China Stand...".

A blue "Next" button is located at the bottom center of the form.

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



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

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

2.3.2 Log Out

To sign out:

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

2.4 SSH Login

SSH is enabled on the RAH305 by default. Prior to establishing an SSH connection, make sure the Windows host PC (client) can reach RAH305's (server) IP.

Method	Host PC Connection	Login Address
Option 1	Host connected to the device's LAN network (via Ethernet or Wi-Fi).	RAH305's LAN IP
Option 2	Host's WAN interface on the same IP subnet as RAH305's WAN interface (e.g., both connected to the same router or upstream Wi-Fi).	RAH305's WAN IP

Example: SSH login via **LAN IP**

1. Connect the host PC to RAH305's LAN network via Ethernet or Wi-Fi.
2. Install SSH client if it is not available.

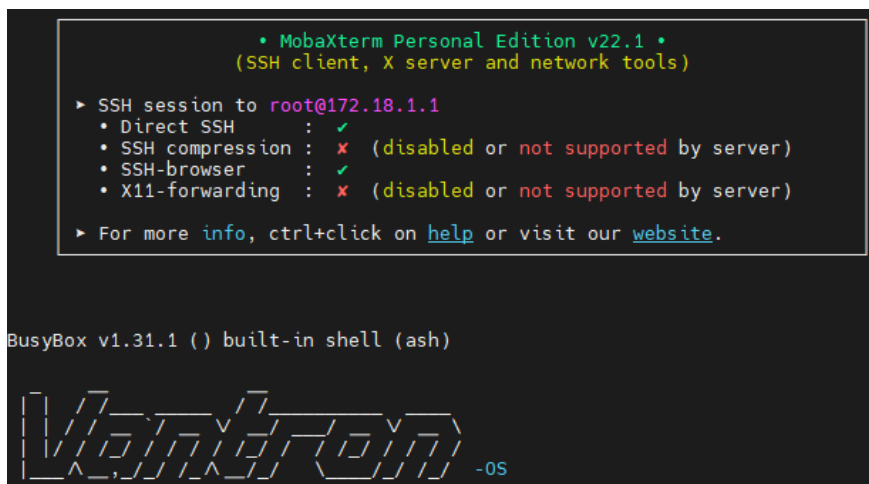
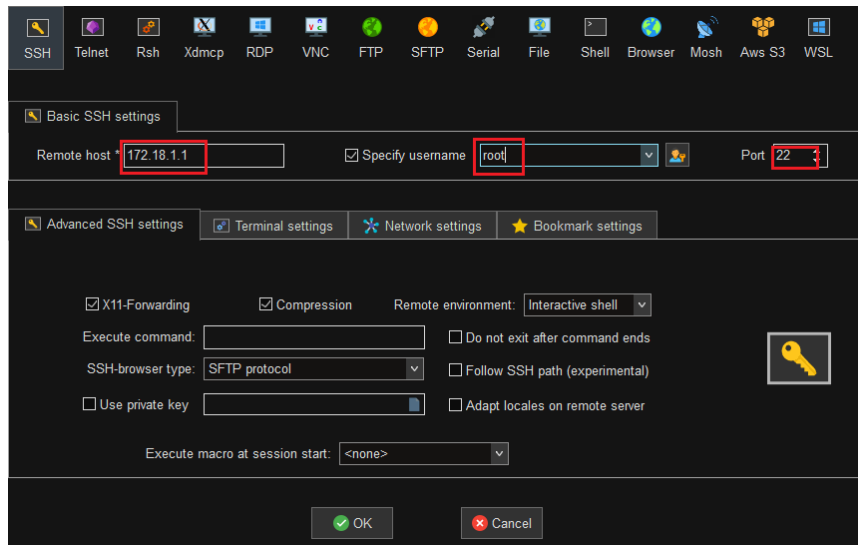
- **Windows host:**

- [PuTTY](#)
- [Tera Term](#)
- [MobaXterm](#)

- **Linux host:**

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

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



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

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

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

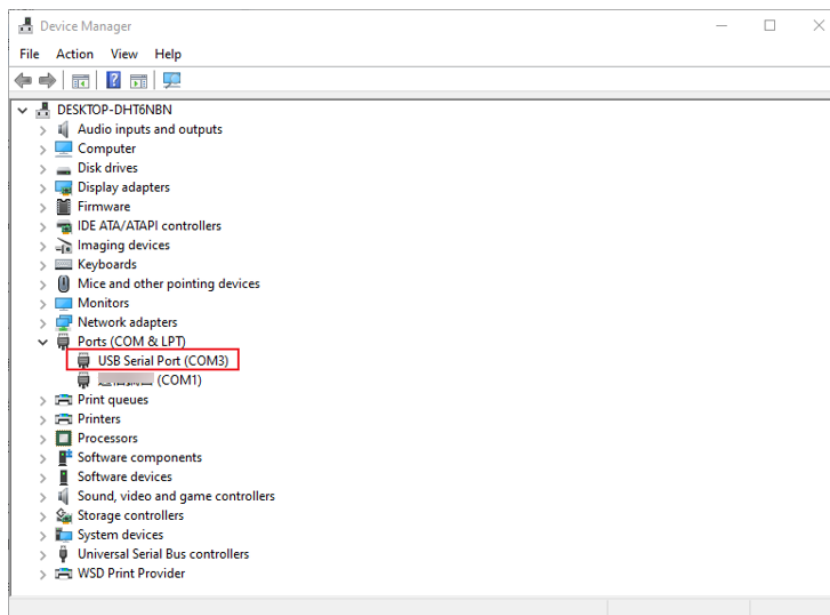
2.5 Debugging the Device (via Console Port)

The RAH305 provides an RS232 Console port (RJ45 connector) for low-level debugging. This port provides direct access to the device as long as the hardware is intact—even if the network is misconfigured, the IP address is lost, network interfaces are down, or the VantronOS web portal is inaccessible. All you need is a USB-to-RJ45 Console cable.

1. Connect the RAH305 to a **Windows** PC using a USB-to-RJ45 Console cable.



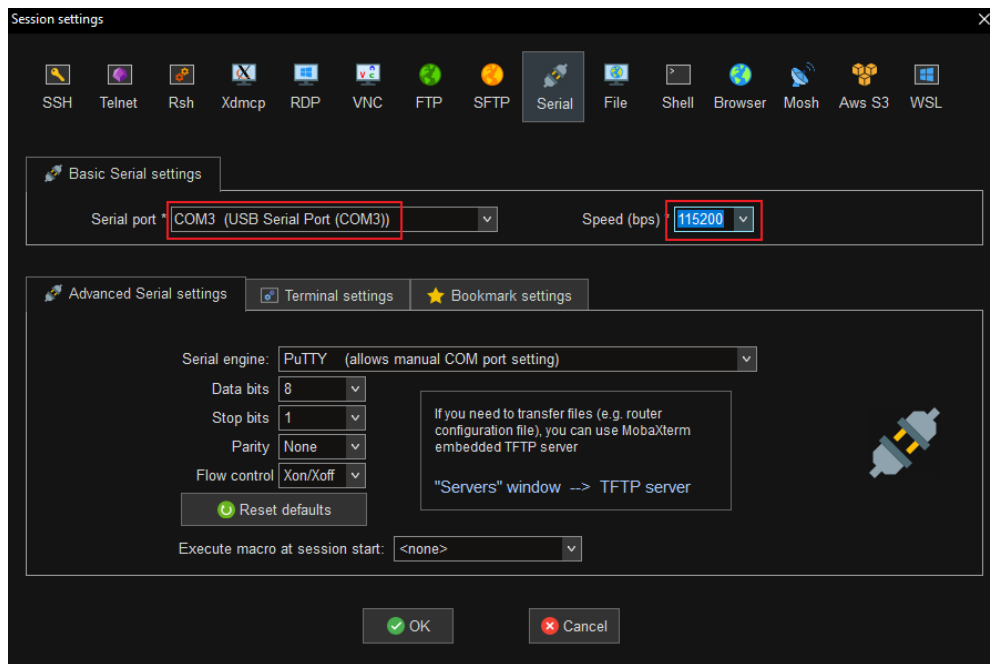
2. Install the Console cable's driver on the PC depending on its model.
3. Check **Device Manager** for the COM port number assigned to the cable.



4. Launch a serial terminal on the host PC.

- [PuTTY](#)
- [Tera Term](#)
- [MobaXterm](#)

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



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

2.6 Wireless Quick Pairing

This section describes the methods for quick device pairing via hardware setup.

2.6.1 Wi-Fi WPS Connection

Prerequisites:

- Both target devices support the Wi-Fi WPS feature.
- Both target devices operate on the same Wi-Fi band, as WPS handshake does not support cross-band communication. While the RAH305 supports dual-band Wi-Fi, only one band is active at a time. The default band is set in the initial setup wizard.
- The target devices are pre-configured with one in Wi-Fi AP mode, and the other in Wi-Fi client mode.

Example procedures:

1. Prepare two RAH305 routers and place them close to each other.
2. Short press (< 1s) the WPS button on one device to activate WPS connection mode.
3. Repeat step 2 on the other device. Make sure the time interval between button actions on both devices is within **30** seconds.
4. Upon successful connection, the WLAN LED turns solid green and both devices exit the WPS mode.
5. Repeat above steps for the same Wi-Fi AP and each new client, if applicable.
6. Place the devices at target deployment sites.

2.6.2 HaLow DPP Pairing

Prerequisites:

- Both target devices support the HaLow DPP feature.
- The RAH305 acts as **HaLow AP** while the peer device works in HaLow STA mode.

Example procedures:

1. Prepare an RAH305 (AP) and a HaLow node (STA) and place them close to each other.
2. Short press (< 1s) the DPP button on one device to activate DPP pairing mode.
3. Repeat step 2 on the other device. Make sure the time interval between button actions on both devices is within **120** seconds.
4. Upon successful connection, the HaLow LED on the RAH305 turns solid green and both devices exit the DPP mode.
5. Repeat above steps to pair additional new STAs with the current RAH305, if applicable.
6. Place the devices at target deployment sites.

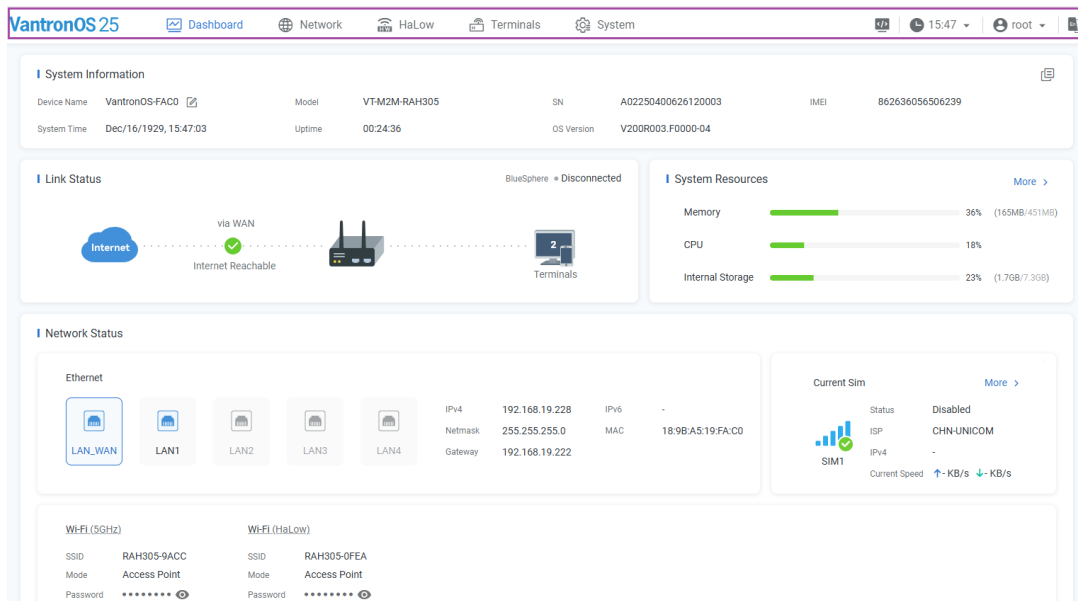
CHAPTER 3 DEVICE SETUP VIA VANTRONOS

3.1 Introduction to VantronOS

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

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

3.1.1 Web Overview



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

Dashboard: Displays general device information and dynamic status updates.

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

Terminals: Provides information of connected end nodes.

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

Command Line Interface: Allows users to access the device's shell for debugging.

Time Settings:

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

Refer to Section [3.6.1.2](#) for modifying the time settings.

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

- Toggle Edge Computing functionality
- Log out

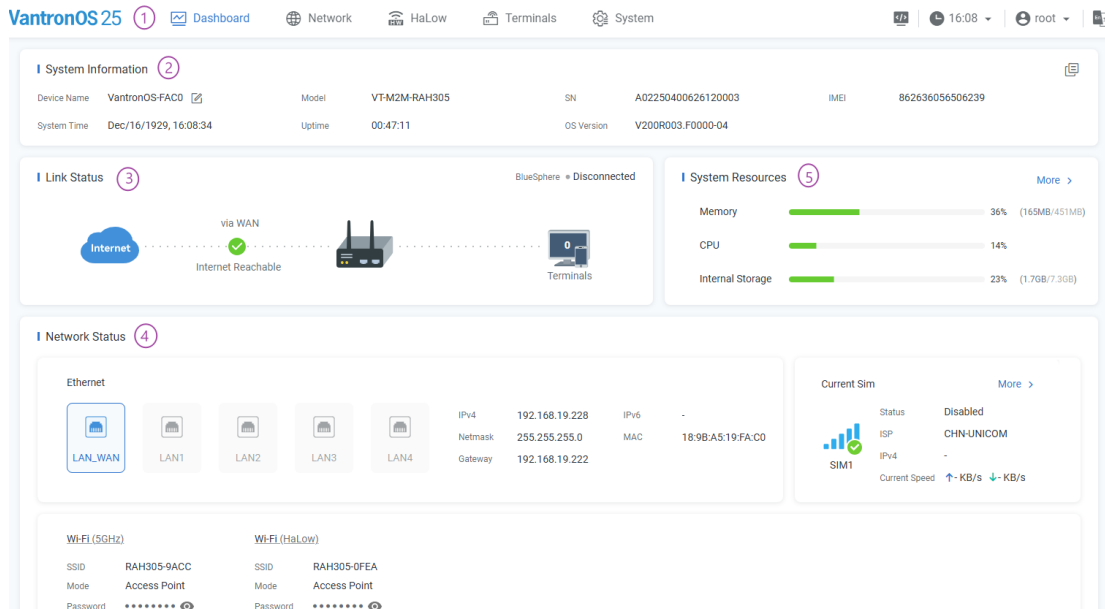
Language Toggle: English ⇄ Chinese.

3.1.2 Language Change

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

3.2 Dashboard

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



Description:

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

3.3 Network

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

Interfaces on the RAH305 are categorized as either WAN or LAN.

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

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

3.3.1 WAN Interface

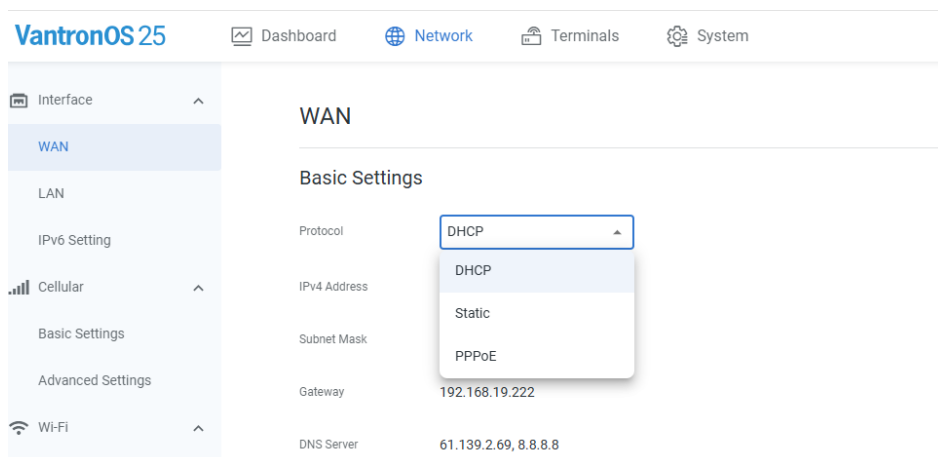
The WAN interface page includes the following three functionalities:

1. **Basic IP configuration** — Selects the WAN interface IP protocol (e.g., DHCP, Static IP, PPPoE).
2. **Interface bridging** — Designates either the physical WAN port or Wi-Fi Client as the Layer 2 egress path to the upstream network. The RAH305 and all LAN-side terminals obtain IP address from the upstream DHCP server, while local NAT and DHCP are disabled.
3. **Link priority IPv4** — Displays all upstream links and the port status, letting you change their priority.

Whenever you make a change, always ensure the host PC and the RAH305 are on the same subnet for smooth VantronOS login.

3.3.1.1 Basic IP Configuration

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



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

The screenshot shows the VantronOS 25 web interface. The top navigation bar includes 'Dashboard', 'Network' (selected), 'Terminals', and 'System'. On the left, the 'Interface' menu is expanded, showing 'WAN' (selected), 'LAN', and 'IPv6 Setting'. Under 'Cellular' and 'Wi-Fi', there are 'Basic Settings' and 'Advanced Settings' options. The main content area is titled 'WAN' and 'Basic Settings'. It contains the following fields: 'Protocol' (set to 'Static'), 'IPv4 Address' (192.168.19.109), 'Subnet Mask' (255.255.255.0), 'Gateway' (empty), 'Primary DNS Server' (empty), and 'Secondary DNS Server' (empty).

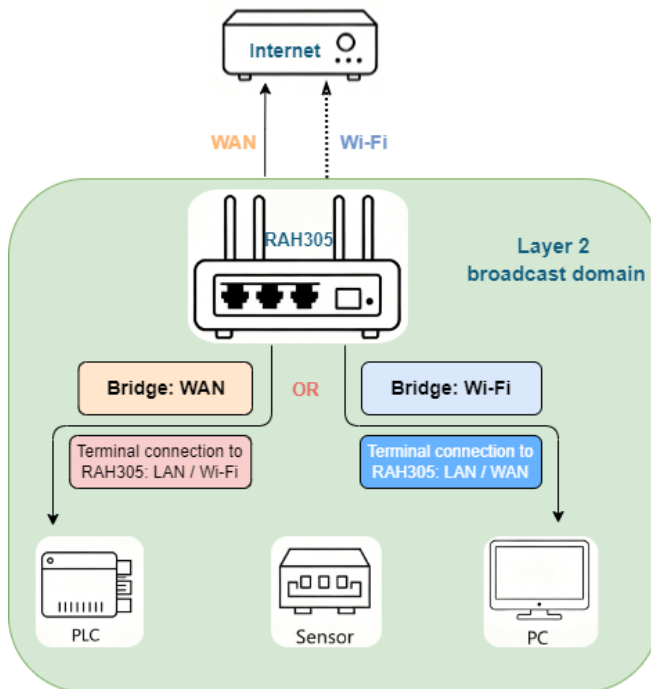
PPPoE (Point-to-Point Protocol over Ethernet): The device **dials** an ISP using a username and password encapsulated in PPP over Ethernet; the ISP then assigns IP settings dynamically (or sometimes fixed).

The screenshot shows the VantronOS 25 web interface with the same navigation structure as the previous image. In the 'WAN' 'Basic Settings' section, the 'Protocol' is set to 'PPPoE'. The 'Username' field is filled with 'admin', and the 'Password' field is filled with six dots, with an eye icon to its right for toggling visibility.

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

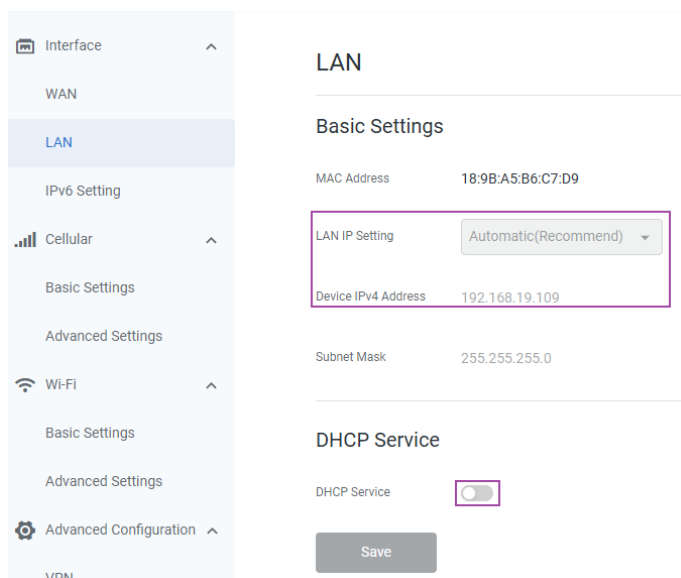
3.3.1.2 Interface Bridging

Bridging connects two or more network segments such that they operate as a single Layer 2 broadcast domain. **Bridge (ETH)** uses the physical WAN port as the upstream link, while **Bridge (Wi-Fi)** adopts Wi-Fi STA for upstream access. The two modes cannot be enabled simultaneously. Selecting Wi-Fi for bridging automatically switches the radio to **Wi-Fi STA** mode.



After bridging:

- The LAN interfaces **no longer** provide NAT and DHCP services to connected terminals.
- The bridged interface obtains an IP address from the upstream DHCP server, leaving the device with only **one** effective LAN IP.



- Terminals connected to the RAH305 will obtain IP addresses from the upstream DHCP server. Consequently, to manage the router, you need retrieve its IP address from the DHCP server.
- If you connect the device's Ethernet WAN port to an upstream network before enabling the bridge mode, the IP address assigned to the RAH305 will be displayed in seconds for local management.
- If you choose to bridge the Wi-Fi interface, it will switch to the STA mode automatically, with available SSIDs displayed for quick connection.
- To **cancel interface bridging**, enable the **DHCP service** on the **Interface > WAN** page.

3.3.1.3 Link Priority

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

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

To manually set the network priority:

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

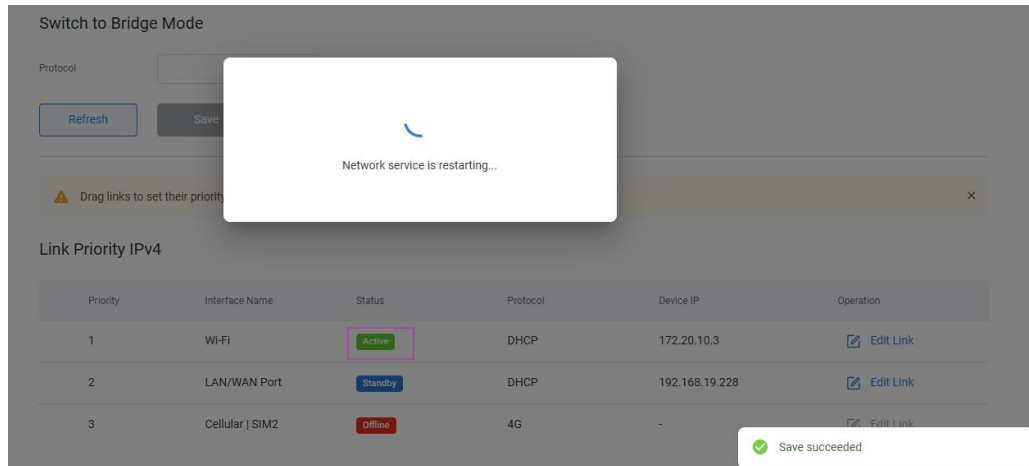
 Drag links to set their priority. ×

Link Priority IPv4

Priority	Interface Name	Status	Protocol	Device IP	Operation
1	LAN/WAN Port	Active	DHCP	192.168.19.228	 Edit Link
2	Wi-Fi	Standby	DHCP	172.20.10.3	 Edit Link
3	Cellular SIM2	Offline	4G	-	 Edit Link

*If the Cellular link is shown **Offline** after SIM card insertion, verify that the matching SIM card profile is **enabled** on the cellular configuration page.*

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



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

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

Link Priority IPv4

Priority	Interface Name	Status	Protocol	Device IP	Operation
1	Wi-Fi	Active	DHCP	172.20.10.3	Edit Link
2	LAN/WAN Port	Standby	DHCP	192.168.19.228	Edit Link
3	Cellular SIM2	Offline	4G	-	Edit Link

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

3.3.1.4 Link Diagnosis

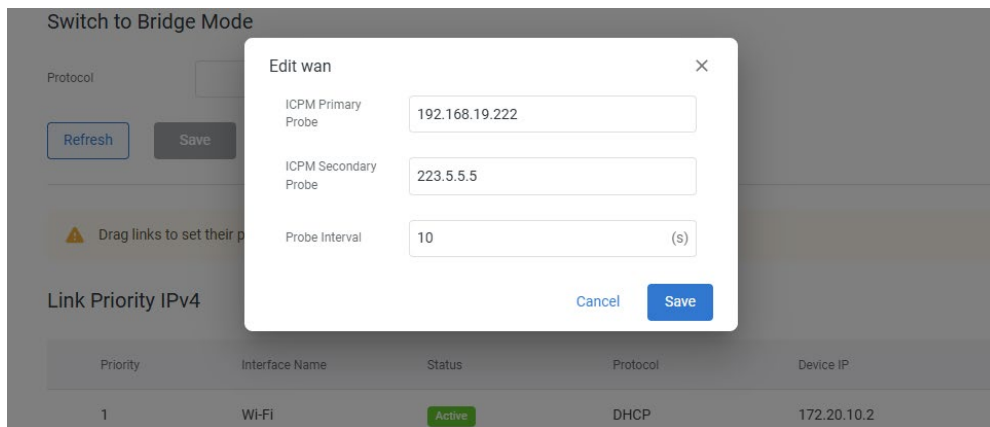
When a link is shown as **Offline**, first make sure the interface is connected to the upstream network. Once verified, you can run a reachability test by setting ICMP probe's destination address to the desired target (e.g., the gateway IP) on that link.

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

Link Priority IPv4

Priority	Interface Name	Status	Protocol	Device IP	Operation
1	Wi-Fi	Active	DHCP	172.20.10.2	Edit Link
2	WAN Port	Offline	DHCP	192.168.19.109	Edit Link
3	Cellular SIM1	Offline	4G	-	Edit Link

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



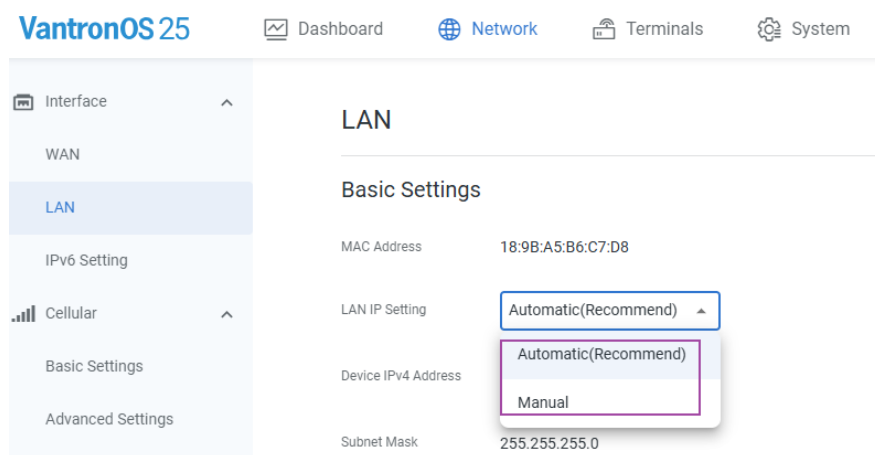
3. Check the link status to verify if it becomes reachable.

Link Priority IPv4

Priority	Interface Name	Status	Protocol	Device IP	Operation
1	Wi-Fi	Active	DHCP	172.20.10.2	Edit Link
2	WAN Port	Standby	DHCP	192.168.19.109	Edit Link
3	Cellular SIM1	Offline	4G	-	Edit Link

3.3.2 LAN Interface

The RAH305 defaults to the 172.18.1.1 subnet for IP assignment.



3.3.2.1 Subnet Conflict

A subnet conflict may occur when a Vantron communication device (router/gateway/HaLow AP) acts as a DHCP server for the RAH305's uplink interface and its factory LAN address (172.18.1.1) overlaps with the RAH305's default LAN subnet.

As a best practice, we recommend reconfiguring the RAH305's LAN IP address to a different subnet when connecting to a Vantron communication device to avoid IP conflicts.

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

3.3.2.2 DHCP Service & DHCP Reservation

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

Editable fields under **DHCP Service**:

- **Start & End addresses:** IP addresses within this range are leased to clients.
- **Lease Time:** The valid duration for which the RAH305, 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 RAH305 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 Service

DHCP Service



Start Address

100

End Address

249

Lease Time

720

(min)

Save

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 RAH305, the specified client device will maintain the allocated IP address to reduce configuration errors.

Steps of adding a DHCP reservation rule:

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

DHCP Reservation

Add Static Binding Rule

Add

MAC Address

IPv4 Address

Operation



No Data

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

The screenshot shows the 'DHCP Service' configuration page. A modal window 'Add Static Binding Rule' is displayed in the center. It contains two input fields: 'MAC Address' with the value '18:c0:4d:43:ad:8b' and 'IPv4 Address' with the value '172.18.1.20'. There are 'Cancel' and 'Add' buttons at the bottom of the modal. In the background, the 'DHCP Service' settings are visible, including a toggle for 'DHCP Service' (turned on), 'Start Address' (100), 'End Address' (249), and 'Lease Time' (720). There is also a 'Save' button and a 'DHCP Reservation' section with an 'Add Static Binding Rule' button.

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

DHCP Reservation

Add Static Binding Rule Add

MAC Address	IPv4 Address	Operation
18:c0:4d:43:ad:8b	172.18.1.20	Edit Delete

4. If you have reserved a different IP for a connected device, reconnect the device to the RAH305, and its IP will update accordingly as shown under **Terminals**.

VantronOS 25 [Dashboard](#) [Network](#) [HaLow](#) [Terminals](#) [System](#) 16:31

Device Info	IP Address	MAC Address	Connection Type	Block Internet
DESKTOP-DHT6NBN (Host)	172.18.1.174	18:c0:4d:43:ad:8b	Wired	☐
iPhone	172.18.1.109	7e:e3:ab:76:ce:e5	Wi-Fi	☐

VantronOS 25 [Dashboard](#) [Network](#) [HaLow](#) [Terminals](#) [System](#) 16:34

Device Info	IP Address	MAC Address	Connection Type	Block Internet
Anonymous Host (Host)	172.18.1.20	18:c0:4d:43:ad:8b	Wired	☐
iPhone	172.18.1.109	7e:e3:ab:76:ce:e5	Wi-Fi	☐

3.3.3 IPv6 Settings

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

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

When IPv6 is enabled:

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

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

LAN Settings

Host configuration: DHCPv6

IPv6 Address Prefix: 64

IPv6 Address Life Time:

LAN Port IPv6 Global Address: fd90:2e49:9ca1::/64

Save

- **DHCPv6:** The RAH305 acts as a stateful DHCPv6 server, assigning full IPv6 addresses to LAN devices with configurable prefix and lease time.
- **SLAAC:** The RAH305 advertises an IPv6 prefix via RA messages. LAN devices automatically generate their own addresses for plug-and-play use.
- **Repeater:** The RAH305 relays upstream IPv6 configurations transparently. LAN devices obtain addresses directly from the upstream network, with no local address assignment.

3.3.4 Cellular

The RAH305 supports dual-SIM communication. Default cellular configurations from the initial setup wizard are retained if available. To modify settings for a SIM card, ensure it is enabled first.

3.3.4.1 Basic Settings

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

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

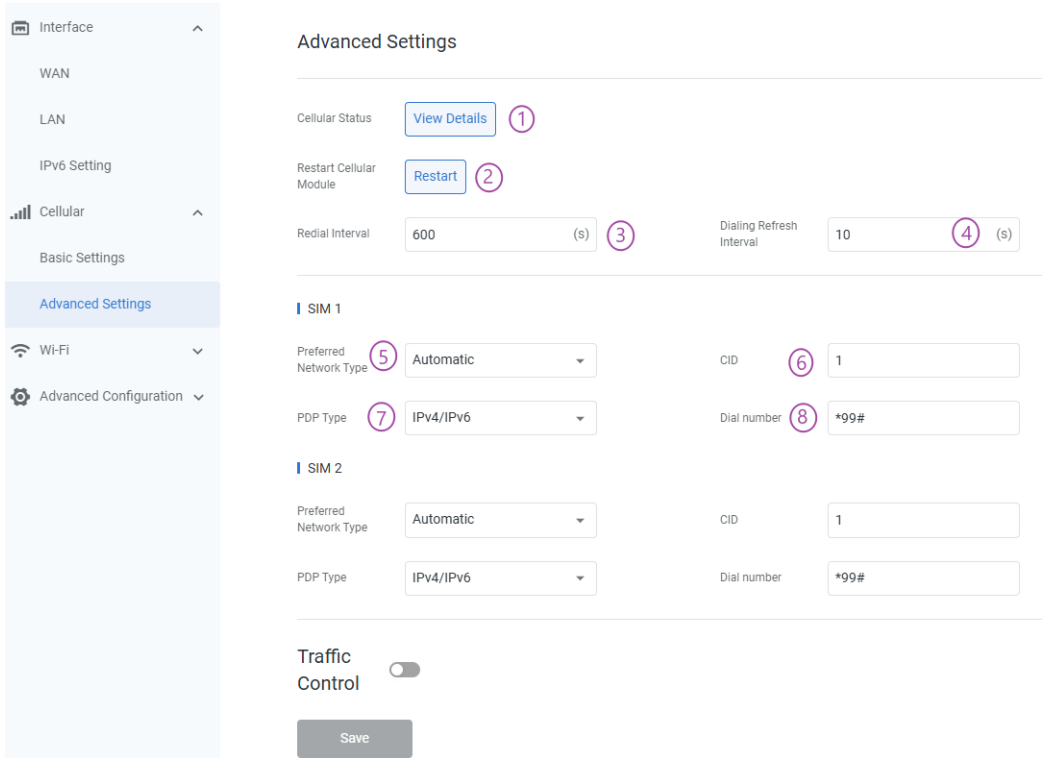
The screenshot shows the 'Basic Settings' page for cellular configuration. On the left is a sidebar menu with options: Interface (WAN, LAN, IPv6 Setting), Cellular (Basic Settings, Advanced Settings), Wi-Fi, and Advanced Configuration. The main area is titled 'Basic Settings' and contains a yellow warning banner: 'Configure APN parameters according to your SIM card details. Enable Auto APN and continue if unsure'. Below this, there are two SIM card sections. SIM 1 is enabled (toggle on) and has a PIN field (with an eye icon for visibility), an enabled Auto APN toggle, and a 'Current APN' status of 'Not Acquired'. SIM 2 is also enabled (toggle on) and has a PIN field. Below SIM 2, there is an APN field containing 'm2m.com.attz' and an 'Authentication Type' dropdown menu set to 'None'. A blue 'Save' button is at the bottom. Numbered callouts 1 through 5 point to: 1. SIM 1 toggle, 2. PIN field for SIM 1, 3. Auto APN toggle for SIM 1, 4. APN field for SIM 2, and 5. Save button.

Description:

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

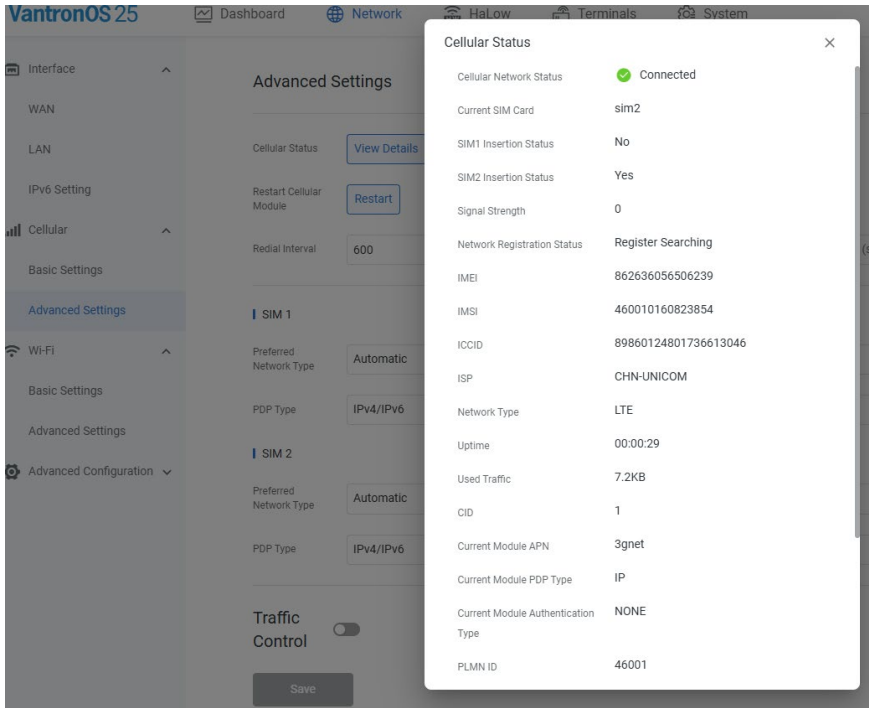
3.3.4.2

 Advanced Settings



Description:

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



2. Manually restart the cellular module.

3. Redial interval — Redials at the specified interval in case of a connection failure (in seconds).
4. Dialing refresh interval — Specifies the interval (in seconds) to refresh the last dal-up status.

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

5. Preferred network type — Currently only 'Automatic' is supported.
6. CID value — Cell identity.
7. PDP type — Packet data protocol type.
8. Dial number — *99# is for general use.

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

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

Traffic Control ☒

SIM 1

Total flow **9** 500 (mb) Used threshold **10** 80 (%)

After exceeding the threshold **11** Uplink Rate Limiting Limited speed **12** 60 (kb/s)

SIM 2

Total flow 500 (mb) Used threshold 80 (%)

After exceeding the threshold Uplink Rate Limiting Limited speed 60 (kb/s)

Save **13**

9. Total flow — Sets the maximum data usage (in MB) available for the RAH305.
10. Used threshold — Defines a data usage percentage (in %) that triggers a restriction action when exceeded.
11. You can select to either: Restrict data speed or cut off the link when exceeding the limit.
12. If uplink rate limit is selected, enter a speed limit (in KB/s) to control data rate.
13. If you have made any changes, click **Save** to apply.

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

3.3.5 Wi-Fi

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

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

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

3.3.5.1 AP-Mode Basic Settings

The screenshot displays the 'Basic Settings' page for the RAH305 device's Wi-Fi AP mode. On the left is a sidebar menu with options: Interface, WAN, LAN, IPv6 Setting, Cellular, Basic Settings (selected), Advanced Settings, Wi-Fi, and another Advanced Settings. The main content area is titled 'Basic Settings' and contains the following fields:

- Wi-Fi Mode:** Two buttons, 'AP' (selected) and 'STA'. A circled '1' is next to the 'AP' button.
- Wi-Fi AP:** A section header.
- Frequency Band:** Two buttons, '2.4GHz Wi-Fi AP' and '5GHz Wi-Fi AP' (selected). A circled '2' is next to the '5GHz Wi-Fi AP' button. A note below says 'Currently, only one Wi-Fi frequency band is supported.'
- Wi-Fi SSID:** A text field containing 'RAH305-9ACC'. A circled '3' is next to the field.
- Hidden SSID:** A toggle switch. A circled '4' is next to the switch.
- Encryption:** A dropdown menu showing 'WPA2-PSK'. A circled '5' is next to the dropdown.
- Password:** A text field with masked characters and an eye icon to toggle visibility. A circled '6' is next to the field.
- Save:** A button at the bottom. A circled '7' is next to the button.

Description:

1. Click **AP** and confirm the action in the pop-up to enable the AP mode.
2. The RAH305 supports dual-band Wi-Fi operation. Both bands are configurable, but only the selected band will be active.
3. Wi-Fi SSID — The Wi-Fi AP's name.
4. Hide SSID — Once hidden, clients cannot scan the device's SSID and must manually enter the exact SSID and password to connect.
5. Encryption mode — The basic protocols for establishing secure communication. (None, WPA-PSK, WPA2-PSK)
6. Password — Credential for connecting the device's Wi-Fi.
7. Click **Save** to allow changes to take effect.

3.3.5.2 AP-Mode Advanced Settings

Interface

WAN

LAN

IPv6 Setting

Cellular

Wi-Fi

Basic Settings

Advanced Settings

Advanced Configuration

VPN

Advanced Settings

1 Disable Wi-Fi

2 Wi-Fi Status View Details

3 Country Code US

4 5GHz Wi-Fi

5 Channel 36 Frequency Bandwidth VHT80

6 Save

Description:

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

Advanced Settings

Disable Wi-Fi

Wi-Fi Status View Details

Country Code US

5GHz Wi-Fi

Channel 36 Frequency Bandwidth VHT80

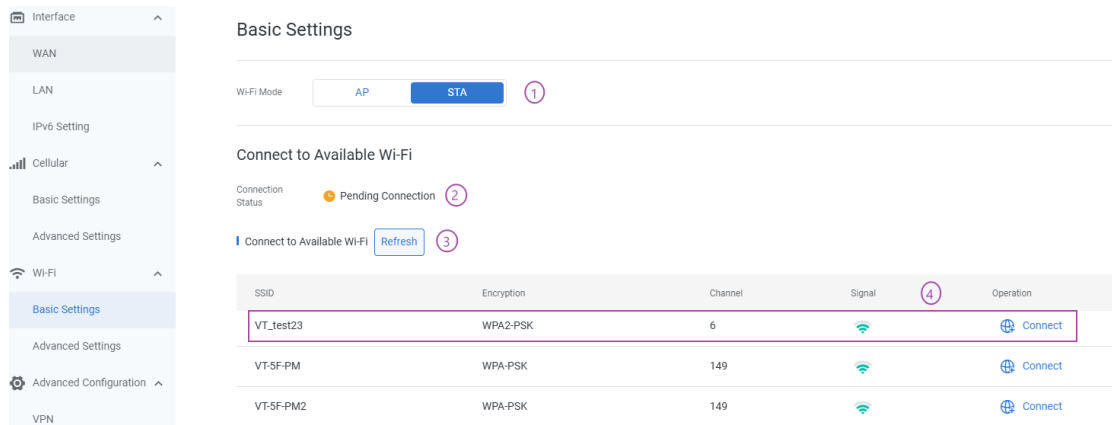
Save

Wi-Fi Status

Wi-Fi Mode	AP Mode
SSID	RAH305-9ACC
BSSID	50:E4:78:99:9A:CC
Encryption	WPA2-PSK
Channel	36
Transmission Power	12dBm
Signal	-
Noise	-
Country Code	US
Uptime	-

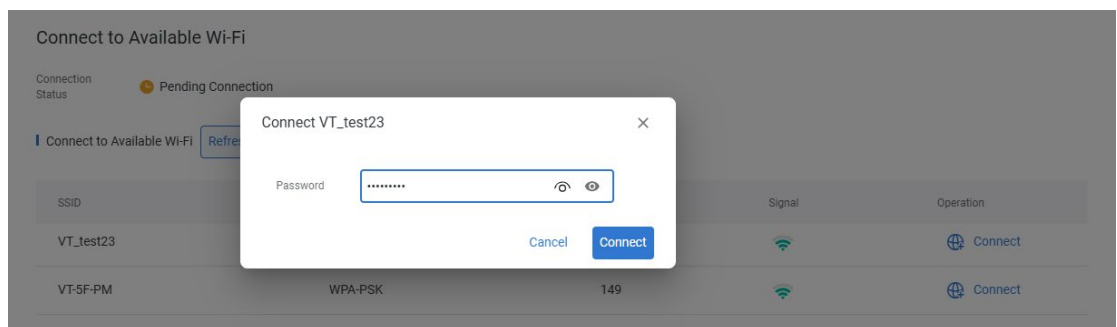
3. Country code ('US' by default).
4. The currently active band matches the selection made in the basic settings.
5. Channel options (configurable) and default frequency bandwidth.
6. If you have modified the parameters, click **Save** to apply.

3.3.5.3 STA-Mode Basic Settings

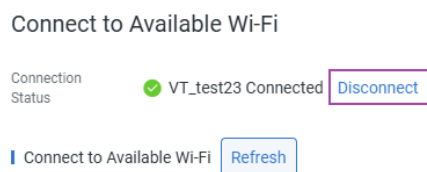


Description:

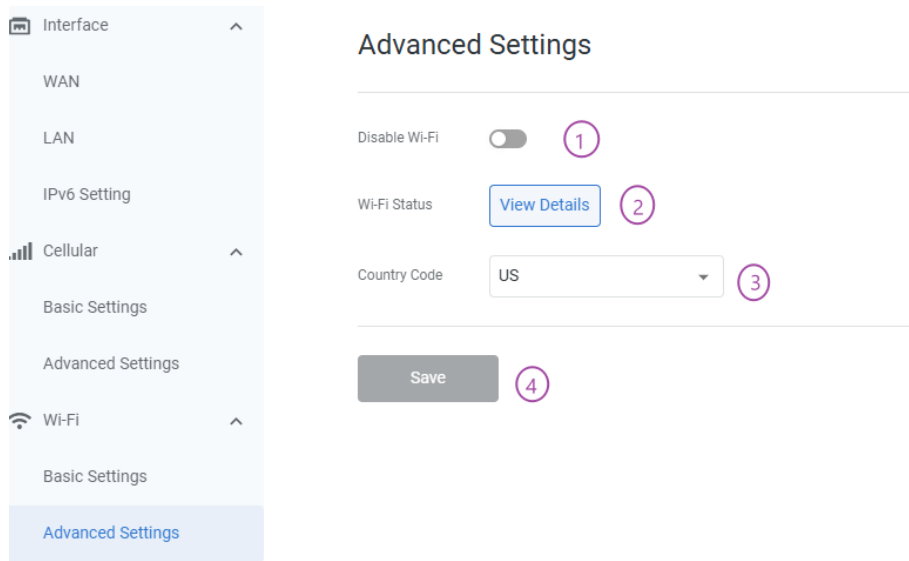
1. Click **STA** and confirm the action in the pop-up to enable the **Station** mode.
2. Current Wi-Fi connection status.
3. If the target SSID is not included in the list, click the button to refresh the list.
4. Information of available Wi-Fi APs is displayed. Click **Connect** and enter the password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



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

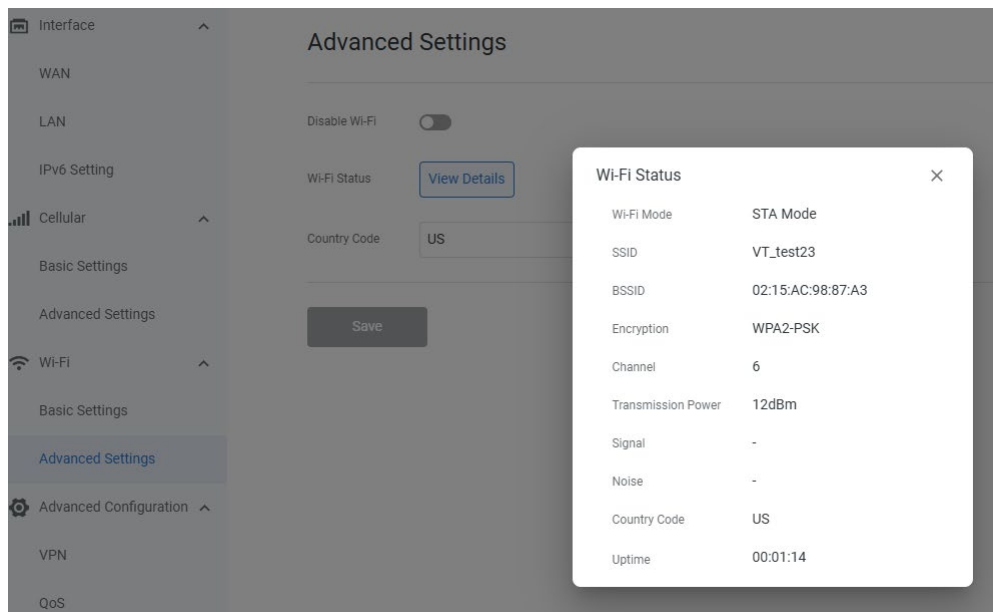


3.3.5.4 STA-Mode Advanced Settings



Description:

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



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

3.3.6 VPN

A virtual private network (VPN) lets you use the Internet to securely access your network remotely. The RAH305 supports PPTP, L2TP, GRE, IPSec, and OpenVPN protocols to ensure data confidentiality and undisturbedness.

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

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

3.3.6.1 OpenVPN Server-Client Network Settings

Scenario	Description
Server has a public IP (or DDNS); Client connects over the Internet	Standard deployment across public networks. Server is directly accessible from the Internet. (Mostly used)
Port forwarding (NAT)	Server sits behind NAT; UDP/1194 (or a self-defined port) has been forwarded to the server's LAN IP.
Local area network communication	Server and client are on the same LAN. (Local testing)

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

Client configurations:

The IP/domain for the **remote** field in the configuration file for an OpenVPN client is as follows:

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

If you are using two RAH305 routers for the connection, make sure there is no IP address conflict when they are in the same LAN.

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

Server configurations:

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

TUN mode

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

TAP mode

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

In a VPN network:

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

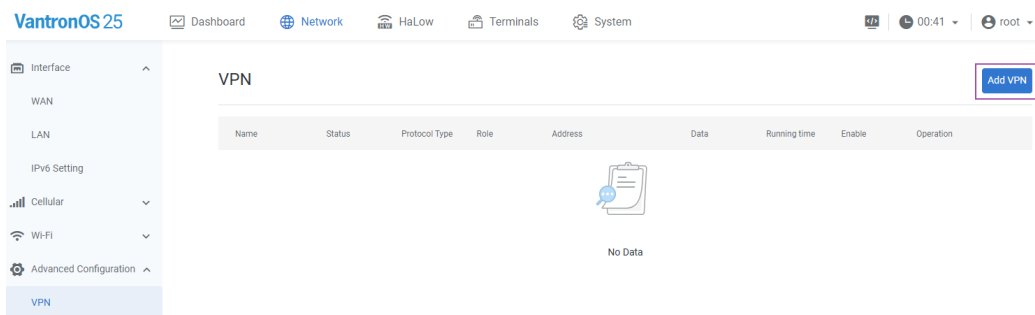
TUN mode works at Layer 3, handling only IP packets (both IPv4 and IPv6) while creating a separate routed network for VPN clients. **TUN** is the **preferred choice** for general-purpose VPN use cases like remote work, secure web browsing, and cloud access, offering better performance and simpler configuration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

3.3.6.2 OpenVPN Server Setup

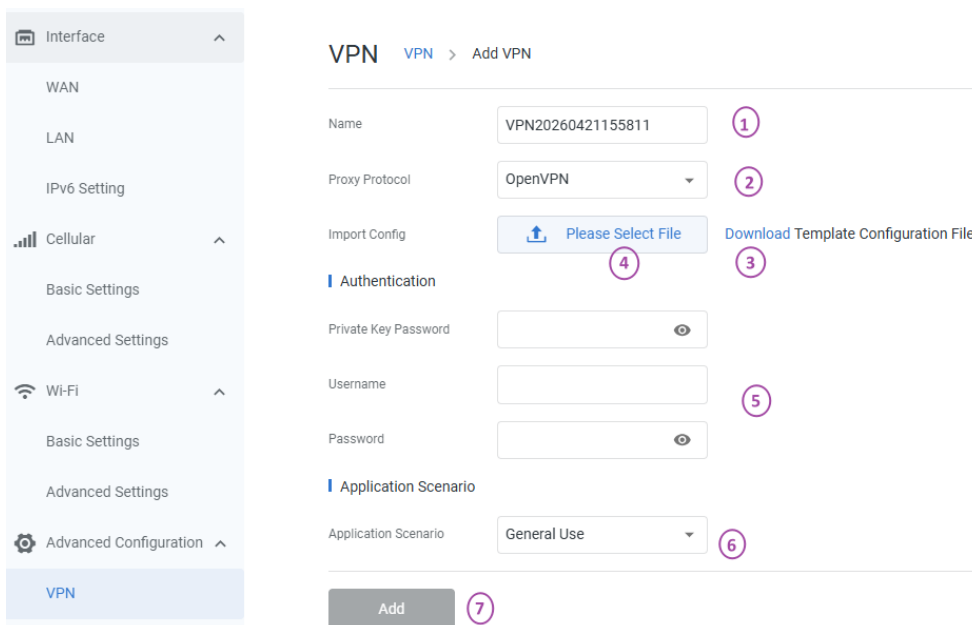
Please note that the configuration templates provided here are for test only. You are recommended to modify the certificates and keys in the configuration file to your own.

To add an OpenVPN **server** rule for the current RAH305:

1. Synchronize both the RAH305 (server) and the client to the same NTP server (for certificate validation).
2. Navigate to **Network > Advanced Configuration > VPN**, and click **Add VPN**.



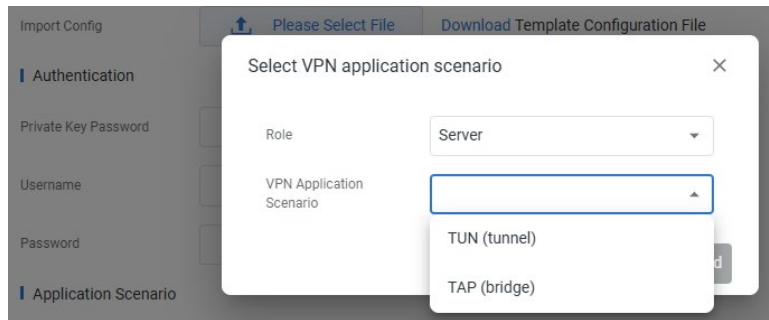
3. In the configuration page, set up the OpenVPN server:



Description:

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

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

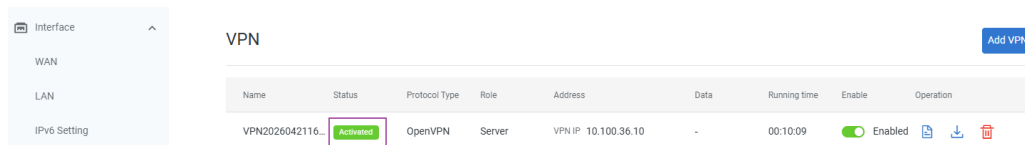


Refer to Section [3.3.6.1](#) for the configuration instructions.

- 4) Click **Select File** to import the pre-configured file or the modified template file.
- 5) Set the authentication credentials, if necessary.
- 6) Select an application scenario.

Refer to Section [3.3.6.4](#) for details on the application scenarios.

- 7) Click **Add** to complete the rule setup.
4. The newly created rule is enabled by default and shows an **Initializing** or **Disconnected** status during device configuration.
 5. When the status changes to **Activated**, the device's role as an OpenVPN server is enabled.



If the status remains unchanged, verify your configuration and check for conflicts with other existing rules. Recreate the rule if the issue persists.

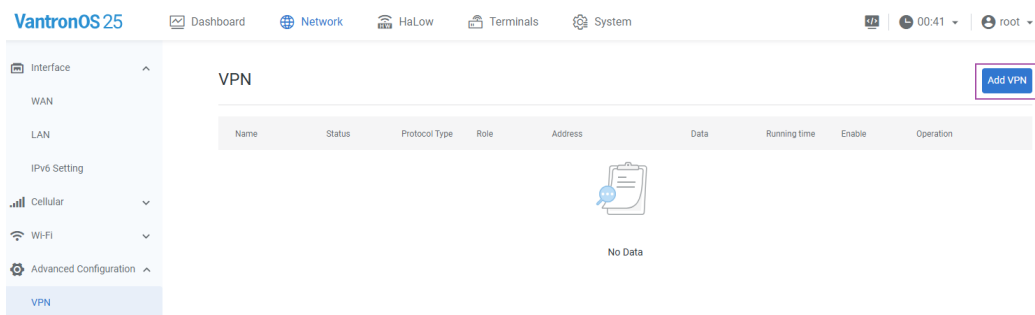
After the setup, you can enable/disable the rule, view its logs (useful for troubleshooting if the rule fails to activate), download the configuration file, or delete it.

3.3.6.3 OpenVPN Client Setup

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

To add an OpenVPN **Client** rule for the current RAH305 and connect it to an OpenVPN server:

1. Synchronize both the RAH305 (client) and the server to the same NTP server (for certificate validation).
2. Navigate to **Network > Advanced Configuration > VPN**, and click **Add VPN**.

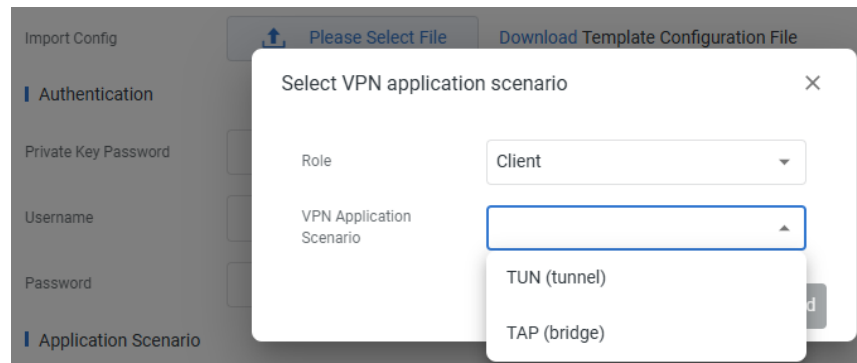


3. On the configuration page, set up the OpenVPN client:

Description:

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

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

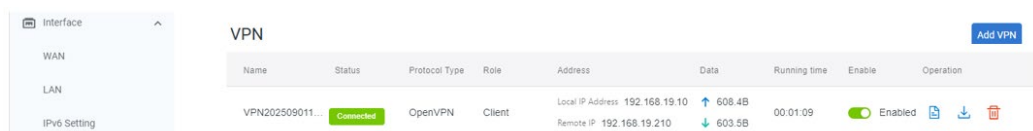


Refer to Section [3.3.6.1](#) for the configuration instructions.

- 4) Click **Select File** to import the pre-configured file or the modified template file.
- 5) Set the authentication credentials, if necessary.
- 6) Select an application scenario.

Refer to Section [3.3.6.4](#) for details on the application scenarios.

- 7) Click **Add** to complete the rule setup.
4. The newly created rule is enabled by default and shows an **Initializing** or **Disconnected** status during device configuration.
 5. When the status changes to **Activated**, the device successfully establishes a connection with a server.



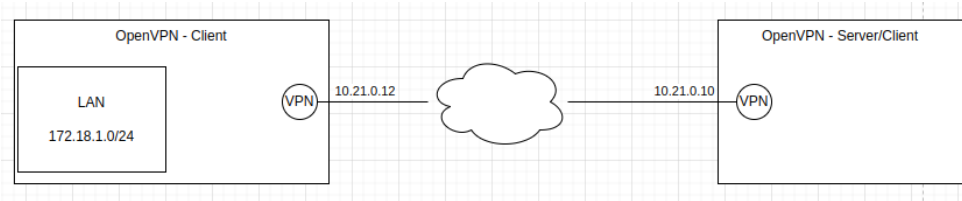
Name	Status	Protocol Type	Role	Address	Data	Running time	Enable	Operation
VPN202509011...	Connected	OpenVPN	Client	Local IP Address 192.168.19.10 Remote IP 192.168.19.210	↑ 608.4B ↓ 603.5B	00:01:09	Enabled	

If the status remains unchanged, verify your configuration and check for conflicts with other existing rules. Recreate the rule if the issue persists.

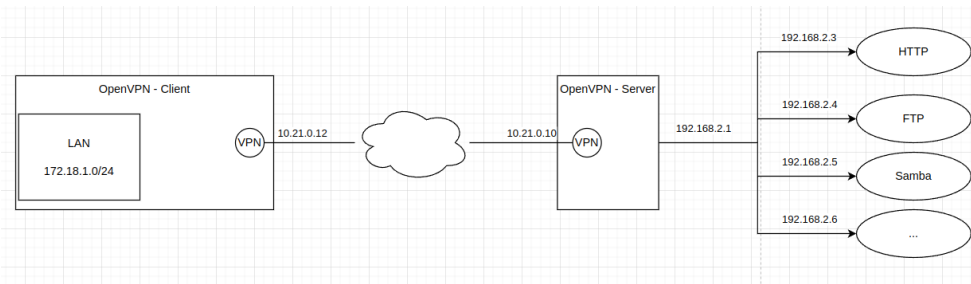
After setup, you can enable/disable the rule, view its logs (useful for troubleshooting if the rule fails to activate), download the configuration file, or delete it.

3.3.6.4 Application Scenario Topology

- General Use (point-to-point)

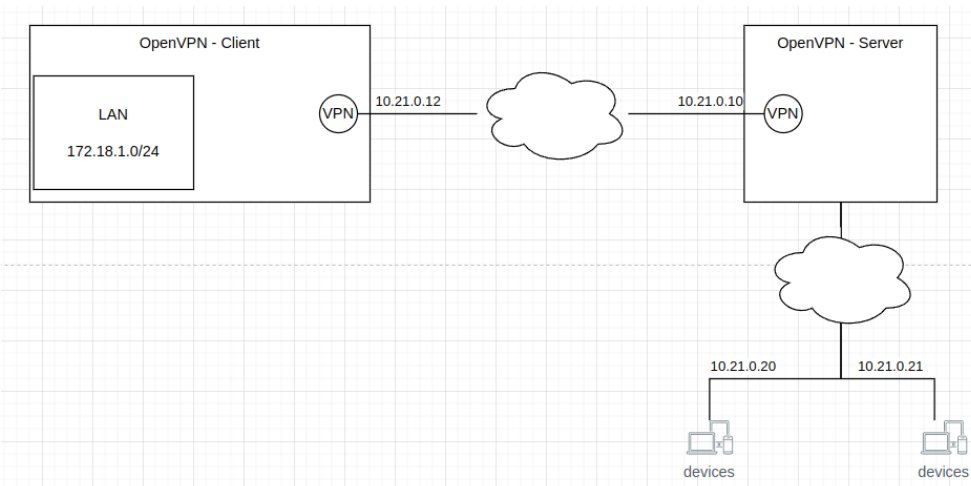


- Routing Mode (client-to-network)



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

- DNAT Port Forwarding (client-to-clients)

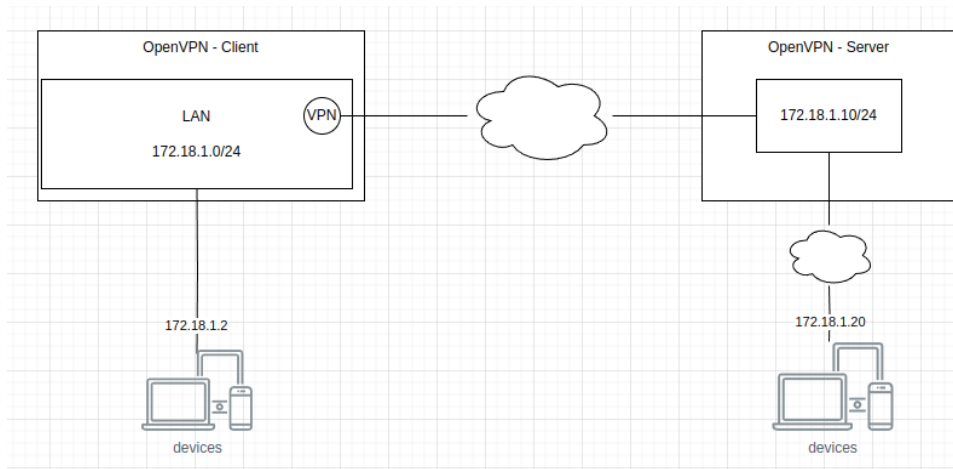


In this scenario, the OpenVPN client is assigned an IP: 10.21.0.12, on the same subnet as the remote devices (10.21.0.20 & 10.21.0.21). So, they can communicate with each other.

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

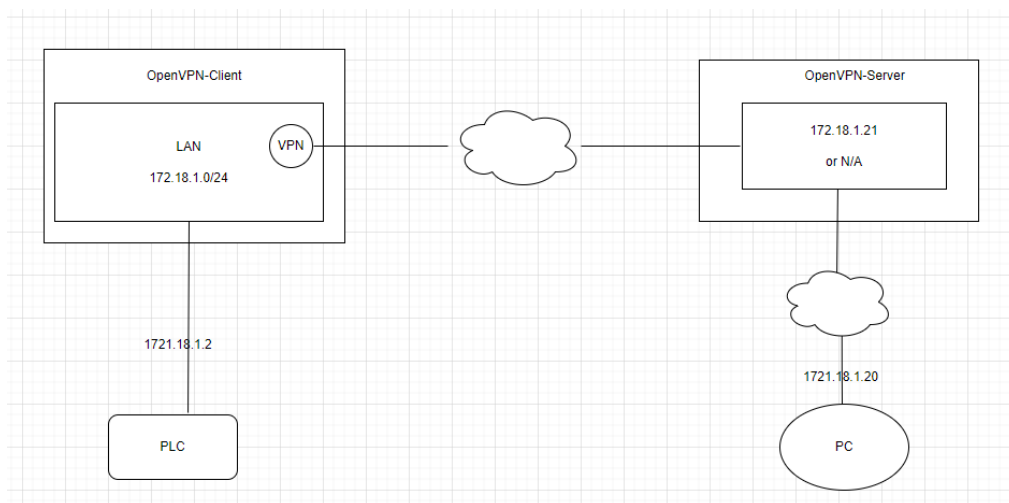
- Bridging Mode (clients-to-clients)

Option 1: IP addresses are assigned by the OpenVPN server



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

Option 2: IP addresses are assigned by the OpenVPN client



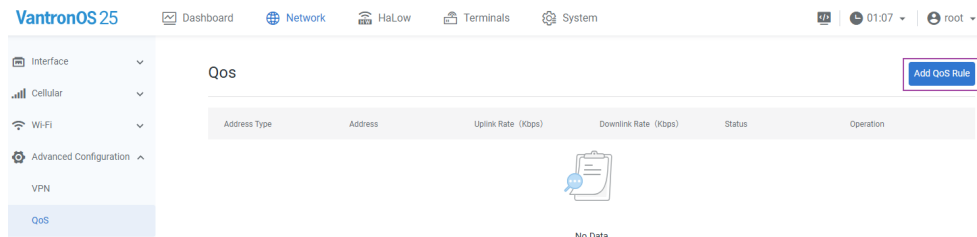
In this scenario, (a) OpenVPN client is customized; (b) DHCP should be started after VPN connection is established or a static IP is added to the VPN interface after the connection is established.

3.3.7 QoS Bandwidth Control

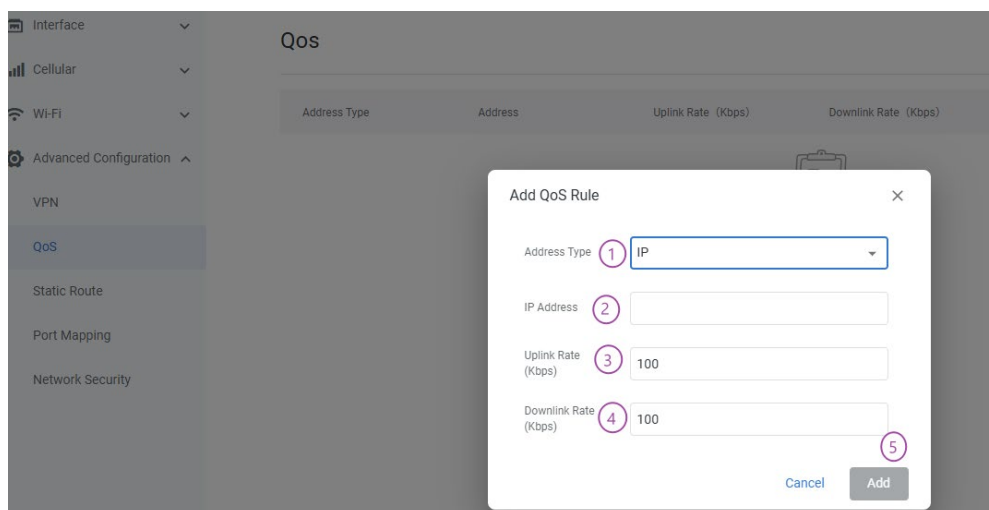
The QoS feature provides fine-grained bandwidth shaping rules to limit uplink and downlink traffic of designated terminals, preventing bandwidth preemption and stabilizing industrial communication quality.

Follow the steps below to create a QoS rule:

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



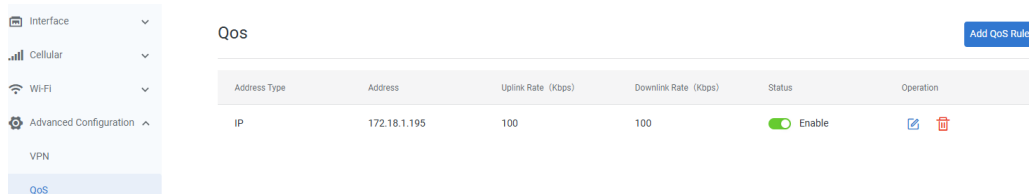
2. On the configuration page, set up the rule:



Description:

- 1) Select the address type (IP, IP range, MAC).
- 2) Fill in the corresponding parameter.
 - **IP:** Apply rate limits to a single specified IPv4 device. Ideal for precise bandwidth control of key equipment such as PLCs and industrial controllers.
 - **IP Range:** Restrict traffic for a continuous segment of IP subnet, enabling batch bandwidth control for groups of sensors or surveillance cameras.
 - **MAC:** Restrict device traffic via physical 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.



Address Type	Address	Uplink Rate (Kbps)	Downlink Rate (Kbps)	Status	Operation
IP	172.18.1.195	100	100	Enable	

3.3.8 Static Route

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

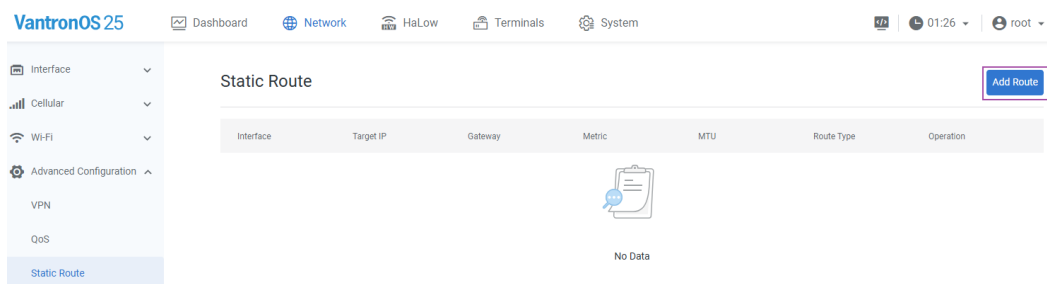
Example:

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

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

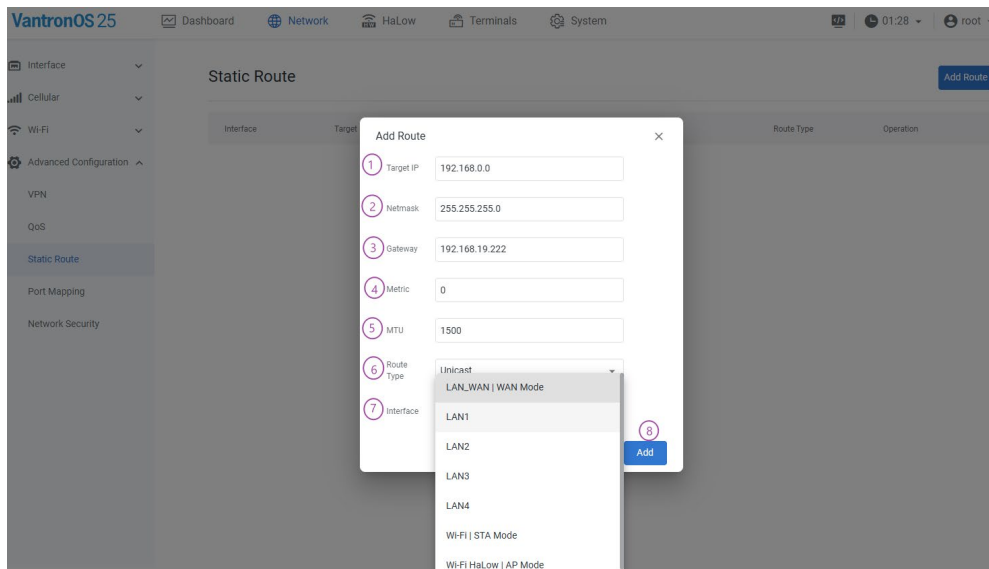
Steps:

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



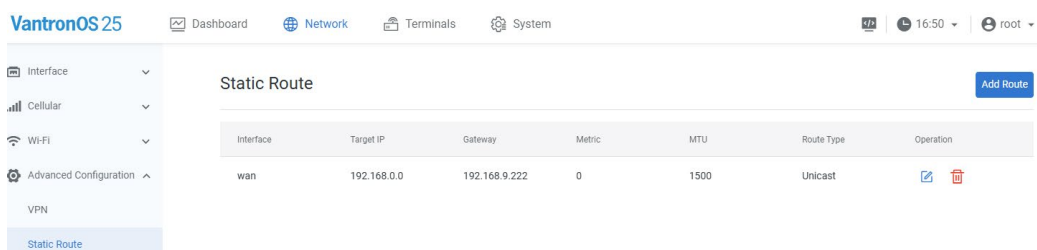
Interface	Target IP	Gateway	Metric	MTU	Route Type	Operation
No Data						

2. Configure the routing rule.



Description:

- 1) Input the destination IP address.
 - 2) Input the subnet mask (e.g., 255.255.255.0 = /24 = 192.168.0.0 - 192.168.0.255).
 - 3) Input the address of the upstream router.
 - 4) Gateway metric (**The smaller the number, the higher the priority**).
 - 5) Set the MTU.
 - 6) Select a route type (refer to the details in the table below).
 - 7) Select an outbound interface for the route (the interface that leads to the router, WAN in this case).
3. After creation, you can edit or delete this rule as needed.



Description of the route type:

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

3.3.9 Porting Mapping

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

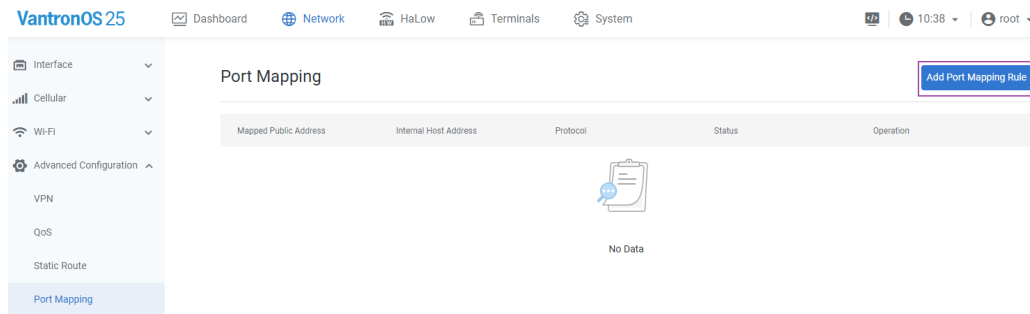
Example:

Scenario:

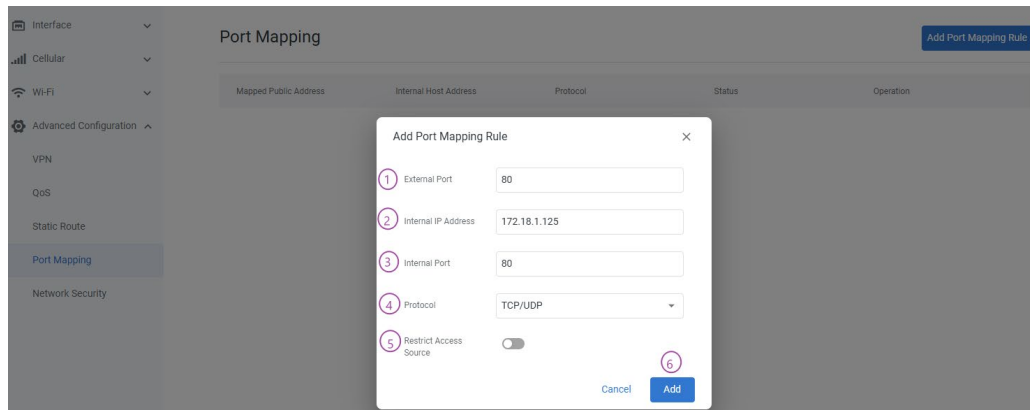
- The RAH305 has both an internal zone (e.g., Wi-Fi AP) and an external WAN zone (e.g., Ethernet WAN) configured, with NAT enabled from internal to external.
- Port mapping (Destination NAT) operates based on this NAT boundary.

Goal:

- Allow external users to access the internal service (on port 80) by connecting to the WAN IP (on port 80).
1. Navigate to **Network > Advanced Configuration > Static Route**, and click **Add Port Mapping Rule**.



2. Fill in the rule information.



Description:

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

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

Port Mapping					Add Port Mapping Rule
Mapped Public Address	Internal Host Address	Protocol	Enable	Operation	
Device IP:80	172.18.1.25:80	TCP/UDP	☒ Enable	✎	✖

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

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

3.3.10 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.

3.3.10.1 Basic SSH Access Setup

VantronOS 25

[Dashboard](#) [Network](#) [HaLow](#) [Terminals](#) [System](#)

Interface

Cellular

Wi-Fi

Advanced Configuration

VPN

QoS

Static Route

Port Mapping

Network Security

Network Security

Basic Settings

1

SSH Access ☒

2

SSH Port

3

Web via https Only ☒

4

Save

ACL Access Control ☐

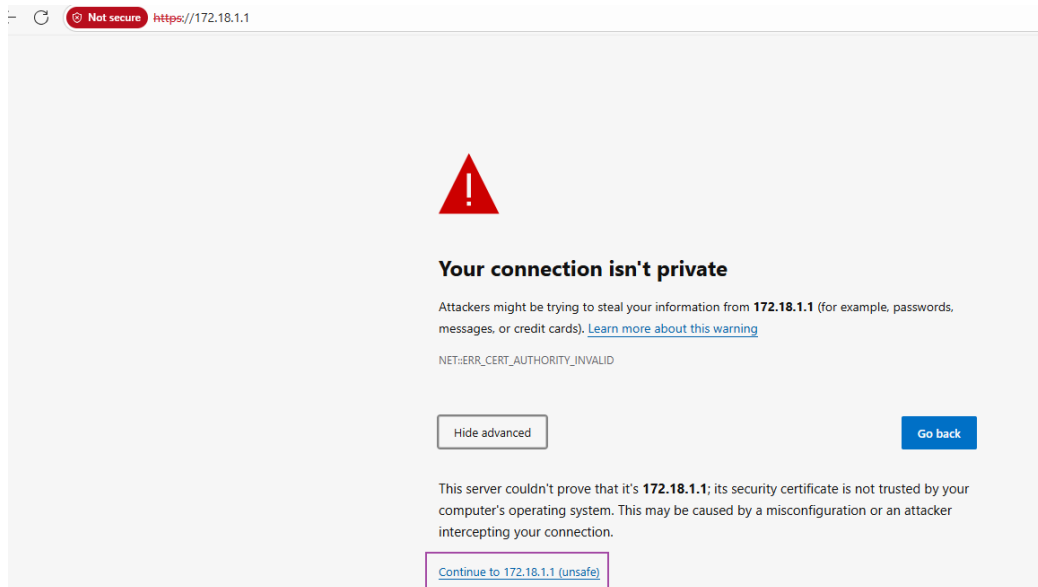
Description:

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

Refer to [2.3](#) for the login method.

- Default SSH port is 22.

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



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

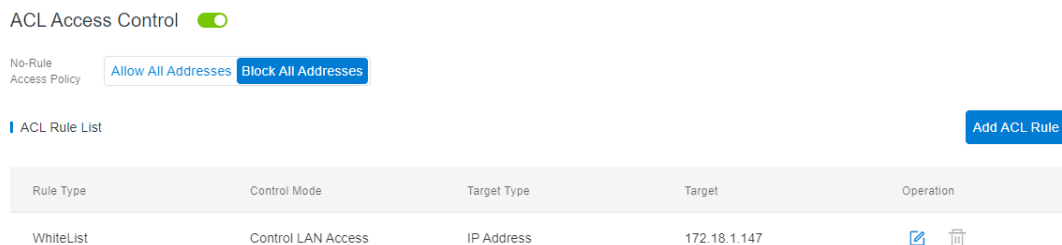
3.3.10.2 ACL Access Control

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

- **No-Rule Access Policy**

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

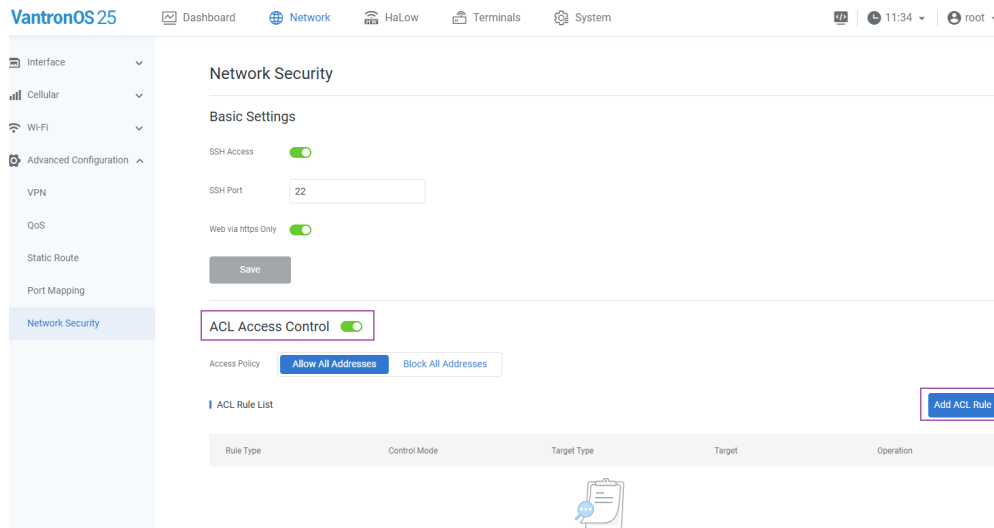
Block all addresses: When enabled, this policy **denies all WAN-side access** — only whitelisted IPs can reach the device — and **prevents** LAN-side devices from using it to **reach the WAN**. If no whitelist rules exist at activation, the device automatically adds the host PC's current IP to prevent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



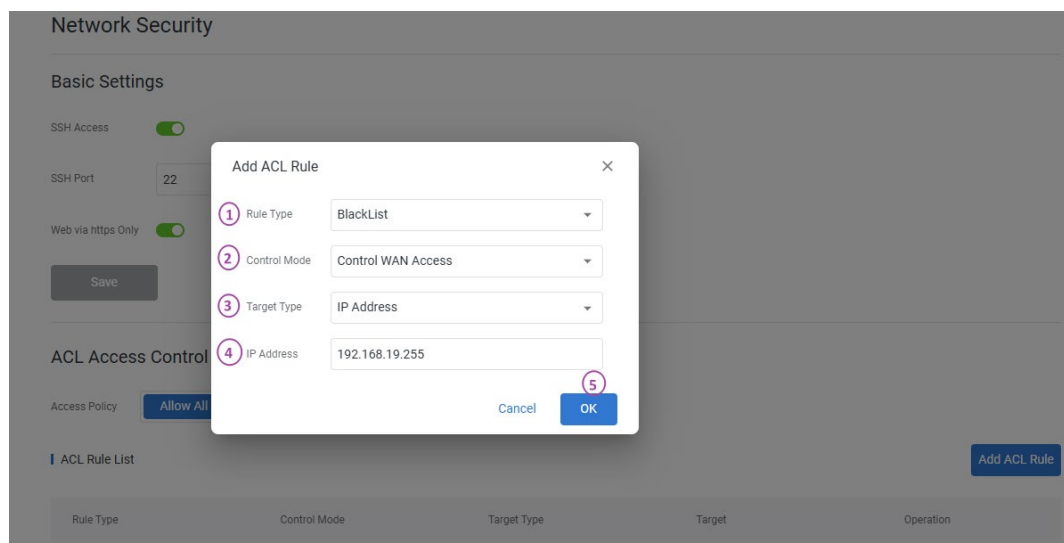
- **ACL Rule List**

To add an ACL rule:

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



3. Configure the rule in the pop-up.



Description:

- 1) Select a rule type:

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

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

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

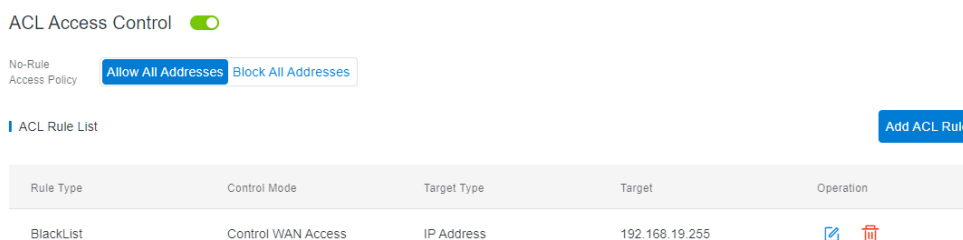
- 3) Target type (changes with the domain selected).
- 4) Target: the specific content corresponding to the target type.
- 5) Click **OK** to complete configuration.

Description for the rule settings:

Rule Type	Control Mode	Target Type	Result
Whitelist	WAN	IP address (Source)	The designated WAN IP has access to RAH305 or its LAN devices.
		Destination IP/ URL/URL keyword	RAH305 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 RAH305 or its LAN devices.
		Destination IP/ URL/URL keyword	RAH305 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.



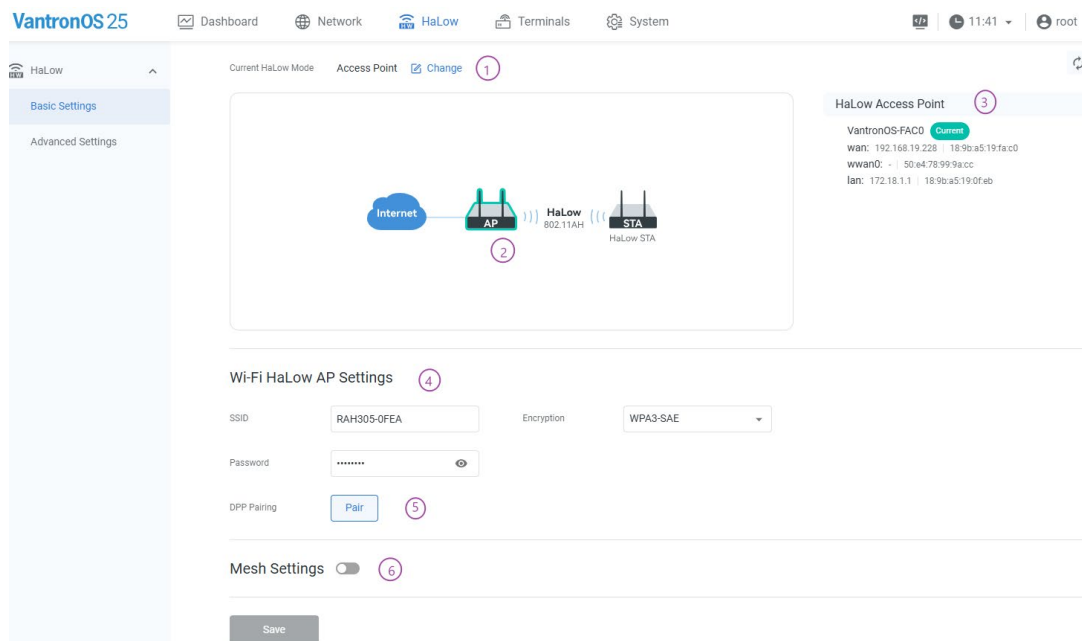
3.4 HaLow

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

The RAH305 runs in **HaLow AP** mode by default. Once **Mesh Settings** are enabled, the router supports two concurrent working modes: HaLow AP for standard point-to-point HaLow connections, and HaLow Mesh mode for large-scale multi-node mesh networking.

3.4.1 Overview

In the **Basic Settings** section, 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. Only **Access Point (AP)** role is supported. This option allows you to switch the HaLow working mode from Mesh back to AP when Mesh mode is enabled.
2. Network topology: Displays the layout of the current HaLow network connections. The local device is highlighted with a **cyan** outline.
3. Device Information: Shows brief connection information about the current device within the network topology.
 - Clicking the sync button updates the connection status.
 - Device name followed by the **Current** label indicates the local device and its current role.

- Once a HaLow network is established, associated devices in the network are displayed along with their respective IP and MAC addresses.
4. Wi-Fi HaLow AP settings: SSID, encryption, and password. You can modify these parameters as needed. HaLow STAs adopt these credentials to establish a standard HaLow connection.
 5. DDP pairing: Initiates a quick HaLow connection upon clicking the **Pair** button. The target STA shall press the button within 120 seconds for a successful connection.
 6. Enable/Disable Mesh Settings. Nodes with the same mesh parameters automatically join the Mesh network, where IP addresses are allocated by the MPP (only one MPP exists in a mesh network). All RAH305 routers ship with identical default mesh configurations. Modify the mesh parameters if you need to build independent, isolated mesh networks.

Enabling Mesh Settings allows the router to work in both AP and Mesh modes and the router automatically acts as the MPP to assign IP addresses to the nodes within the HaLow network. Switching the HaLow operating mode back to AP will disable the Mesh functionality.

3.4.2 DDP Pairing via Software Setup

As introduced in Section [2.6.2](#), the RAH305 supports hardware DPP pairing with individual HaLow STAs. This section covers the procedures for HaLow fast DPP pairing via the VantronOS web management interface.

1. Prepare one RAH305 (working as HaLow AP) and one DPP-capable HaLow STA node, then position the two devices in close proximity.
2. Log in to the RAH305's web portal, navigate to **HaLow**, and click **Pair** next to **DPP Pairing** (within **Wi-Fi HaLow AP Settings**) to activate the DPP pairing mode.
3. Briefly press the physical DPP button on the STA, or log in to its web portal and click the on-screen **Pair** button. Make sure the time window between the two device operations is within **120** seconds.
4. Upon successful connection, the HaLow LED on the RAH305 turns solid green and both devices will automatically exit the DPP mode.
5. Repeat above steps to pair additional new STAs with the current RAH305, if applicable.
6. Place the devices at target deployment sites.

3.4.3 Mesh Networking

By default, HAP305 routers are pre-configured with common Mesh settings. Once the Mesh Settings are enabled, the router will automatically form or join a HaLow Mesh network with the same settings, **regardless of** the time elapsed.

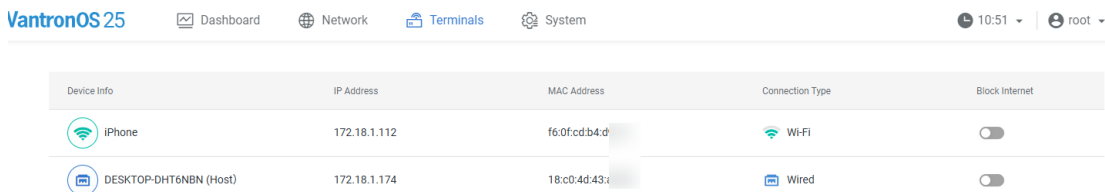
3.5 Terminals

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

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

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

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



The screenshot shows the VantronOS 25 interface with the 'Terminals' tab selected. The table lists two connected devices: an iPhone and a desktop host. Each row includes columns for Device Info, IP Address, MAC Address, Connection Type, and a Block Internet toggle switch.

Device Info	IP Address	MAC Address	Connection Type	Block Internet
 iPhone	172.18.1.112	f6:0f:cd:b4:d	 Wi-Fi	☐
 DESKTOP-DHT6NBN (Host)	172.18.1.174	18:c0:4d:43:c	 Wired	☐

3.6 System

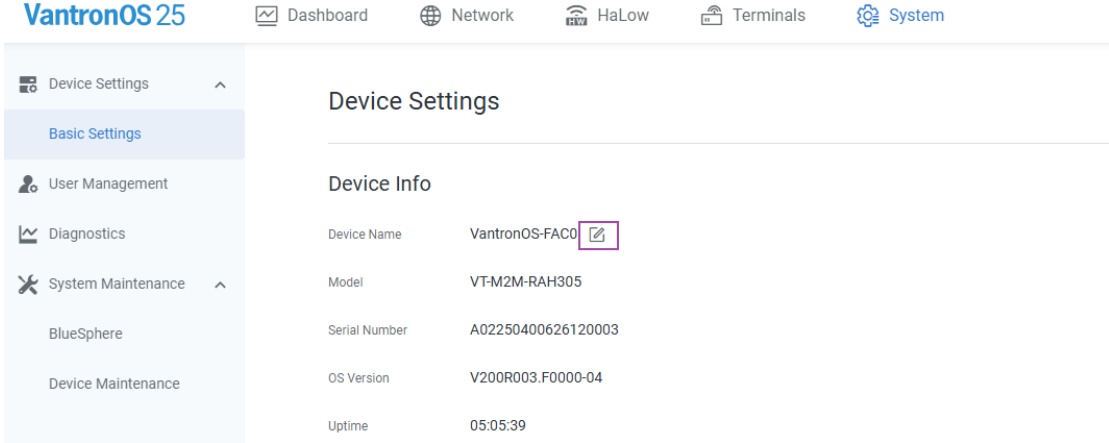
Under **System**, users can view and edit all system-level settings.

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.



The screenshot shows the VantronOS 25 interface. At the top, there's a navigation bar with 'VantronOS 25' and icons for Dashboard, Network, HaLow, Terminals, and System. A left sidebar contains 'Device Settings' (expanded) with sub-items: Basic Settings, User Management, Diagnostics, and System Maintenance. The main area is titled 'Device Settings' and contains a 'Device Info' section. This section lists: Device Name (VantronOS-FAC0 with a pencil icon), Model (VT-M2M-RAH305), Serial Number (A02250400626120003), OS Version (V200R003.F0000-04), and Uptime (05:05:39).

Device Info

Device Name	VantronOS-305-2L	✕	✓
Model	VT-M2M-RAH305		
Serial Number	A02250400626120003		
OS Version	V200R003.F0000-04		
Uptime	05:06:35		

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.

Time Settings

- 1 Current Date Apr/22/2026
- 2 Current Time 11:18:47
- 3 Timezone UTC+8:00, China Standa... ▼
- 4 NTP Sync ☒
- 5 Sync Now NTP Sync
- 6 Primary NTP pool.ntp.org Secondary NTP time.cloudflare.com
- 7 Provide NTP Service ☐
- 8 Save

Description:

1. Current Date — Displays today's date for the selected time zone or the host PC's local time after time synchronization.
2. Current Time — Displays the current time.
3. Time Zone — Users can choose the desired time zone from the drop-down list.
4. NTP Sync — Toggles automatic time synchronization with NTP servers. The date resets after every power cycle because the RAH305 lacks an RTC.
5. Sync Now — Triggers a one-time NTP update immediately.
6. Primary NTP — Preferred NTP server. Secondary NTP—Backup NTP server.
7. Provide NTP Service — Enables/Disables the RAH305 to act as an NTP server for LAN devices.
8. If you have made any changes, click **Save** to apply.

3.6.2 User Management

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

The screenshot shows the 'User Management' interface. On the left is a sidebar menu with options: Device Settings, User Management (selected), Diagnostics, System Maintenance, BlueSphere, and Device Maintenance. The main content area is titled 'User Management' and contains the following fields and controls:

- 1. Username: A text field containing the value 'root'.
- 2. Current Password: A password input field with masked characters (dots) and a toggle icon.
- 3. New Password: A password input field with masked characters (dots) and a toggle icon.
- 4. Confirm Password: A password input field with masked characters (dots) and a toggle icon.
- 5. Save: A blue button to save the changes.

Steps to reset the login password:

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

3.6.3 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

VantronOS 25 Dashboard Network HaLow Terminals System

Device Settings ^

- Basic Settings
- User Management
- Diagnostics**
- System Maintenance ^
 - BlueSphere
 - Device Maintenance

Network Diagnostics

1 Diagnostic Tool: Ping

2 Diagnostic Protocol: IPv4

3 Target Address: 192.168.19.222

4 Run Diagnostics: Run

Advanced Setting ^

6 Iperf3 Server: ☒

Web Terminal ☒

Open in New window: Open

Logs

View Logs: System Logs Link Probe Logs Cellular Logs BlueSphere Logs

Download Logs: Download Logs

5

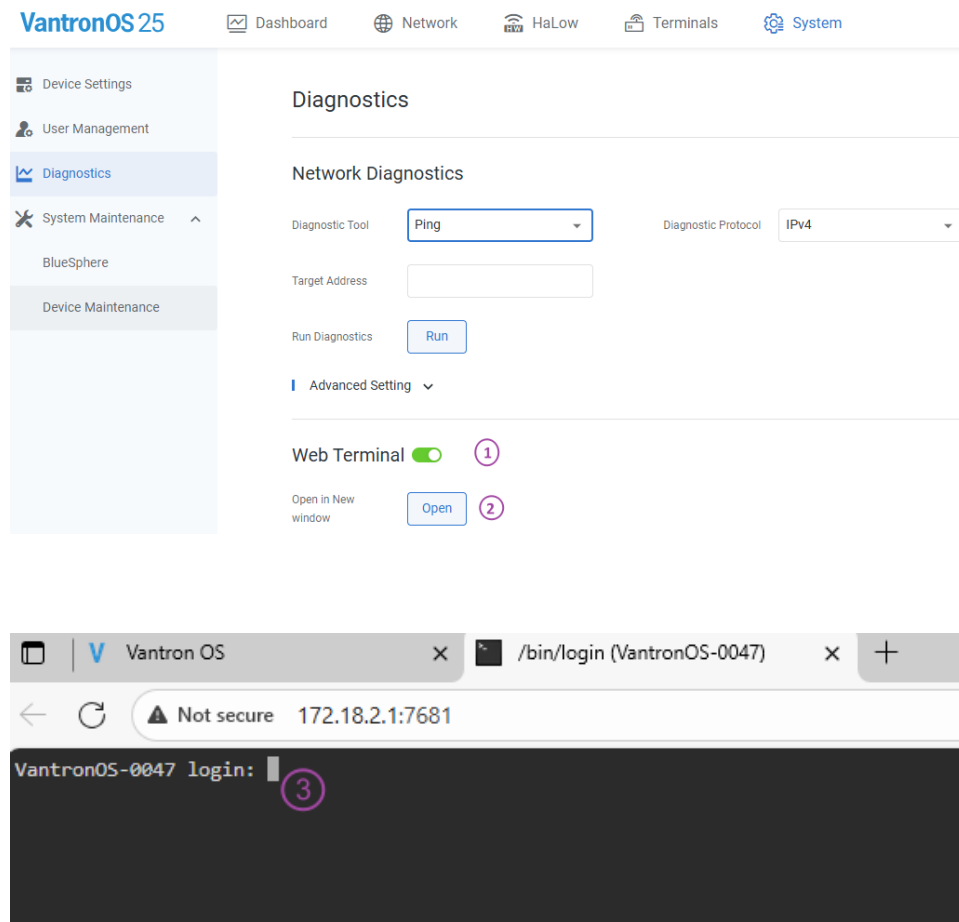
```
PING 192.168.19.222 (192.168.19.222): 56 data bytes
64 bytes from 192.168.19.222: seq=0 ttl=254 time=1.941 ms
64 bytes from 192.168.19.222: seq=1 ttl=254 time=1.713 ms
64 bytes from 192.168.19.222: seq=2 ttl=254 time=1.787 ms
64 bytes from 192.168.19.222: seq=3 ttl=254 time=1.772 ms
```

Description:

1. Select a diagnostic tool from the drop-down list.
2. For the Ping and Traceroute tools, select either IPv4 or IPv6 as the protocol.
3. Enter the target address (IP/Domain address).
4. Run the test.
5. The test results are displayed accordingly.
6. The RAH305's iPerf3 server is enabled by default, allowing remote clients to start a HaLow throughput test immediately without manual activation.

3.6.3.2 Web Terminal

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

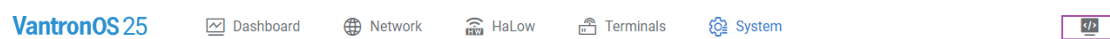


Description:

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

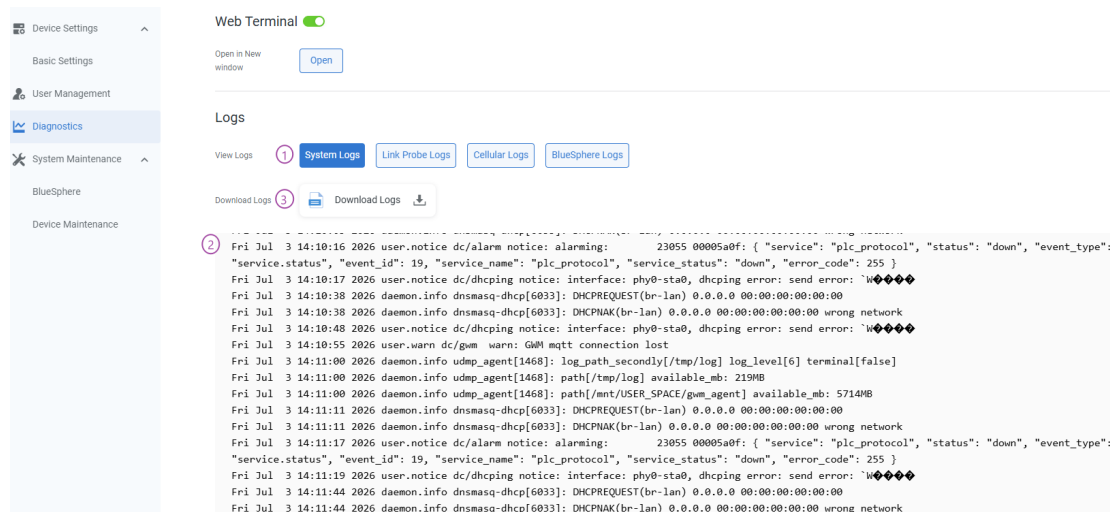
Use the credentials provided on the device label for web terminal login.

When the web terminal is enabled, you can quickly access the command line interface by clicking the icon on the menu tab.



3.6.3.3 Logs

The system offers different device logs for maintenance or troubleshooting.



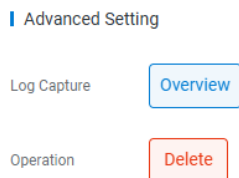
Description:

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

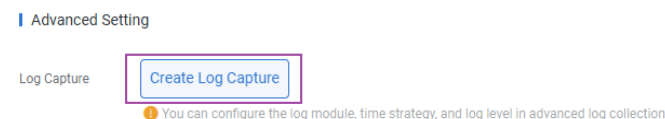
3.6.3.4 Log Capture

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

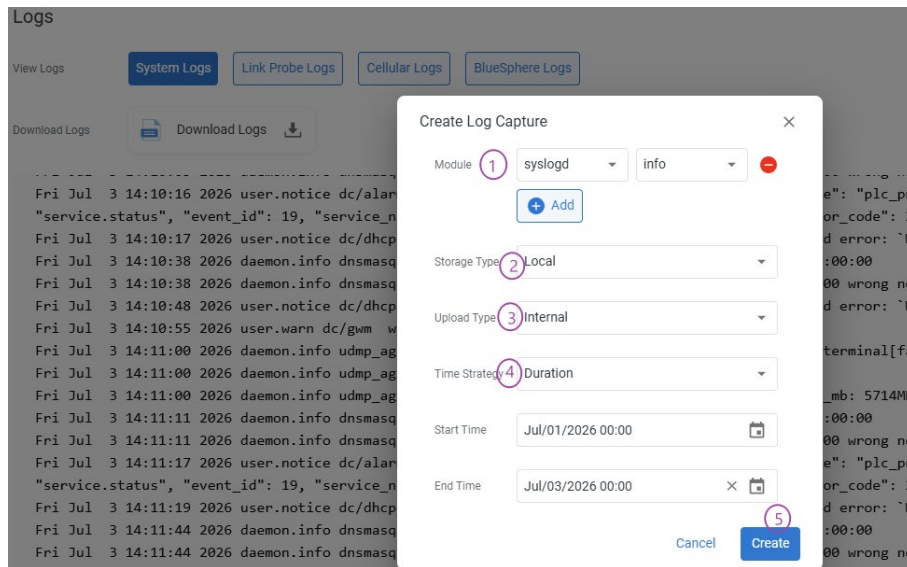
1. Navigate to **System > Diagnostics > Advanced Setting**.
2. View the details of the existing capture rule or delete it, if any. To create a new one, you need delete the existing rule first.



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@Vantron05-C7D8:/# cd /tmp/log
root@Vantron05-C7D8:/tmp/log# ls
able-startup.log      restapi.log
cellular.log          vt_udmp_agent.log
health.checking.log   vtapp_cmd_result
hotplug.log           vtapp_config_reset.log
lastlog              vtled.log
openvpn-VPN20260422094839.log vtled.log.1
openvpn-VPN20260422094839.status.log wtmp
root@Vantron05-C7D8:/tmp/log# cat health.checking.log
130.704 - info - health checking started---
130.794 - info - add check target for platform VT-M2M-G202
130.800 - notice - add check target - 60 -> service status
130.801 - notice - add check target - 600 -> vtos agent
130.805 - notice - add check target - 300 -> time sync
130.813 - notice - add check target - 120 -> Disk Writable Testing
130.816 - notice - add check target - 120 -> hardware status
130.818 - notice - add check target - 300 -> refresh ARP table
130.824 - notice - add check target - 120 -> IP Address Conflict Detection
130.827 - notice - add check target - 300 -> Local IP Address Conflict Detection
130.834 - notice - add check target - 300 -> Gateway IP Address Conflict Detection
130.841 - notice - add check target - 300 -> Network Address Conflict Detection
```

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

4) **Capture Type**

- Duration: The logs are captured as scheduled. When selected, you need specify a time range for log capture.
- Permanent: The logs are captured continuously without interruption.

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

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

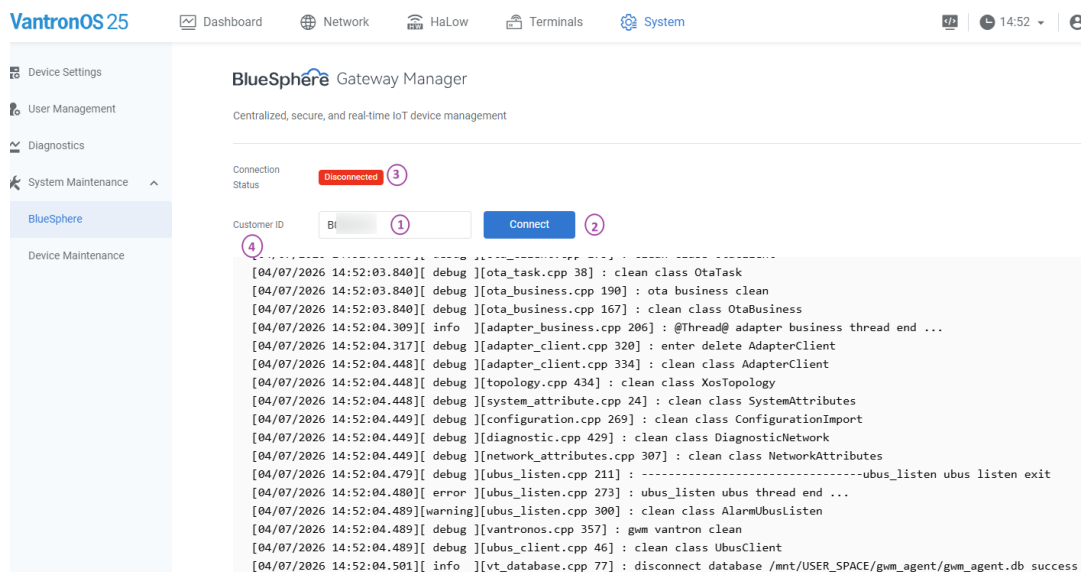
3.6.4 System Maintenance

3.6.4.1 BlueSphere

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

Prerequisite:

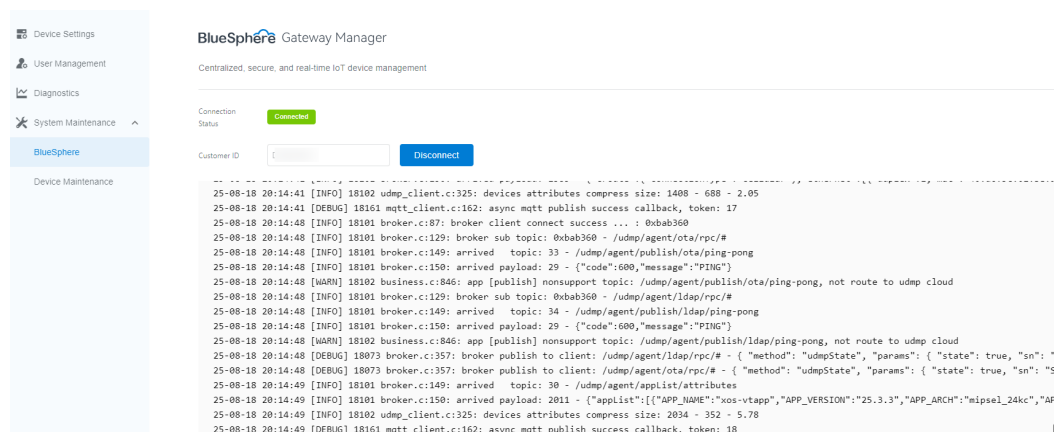
The RAH305 must have internet access.



Description:

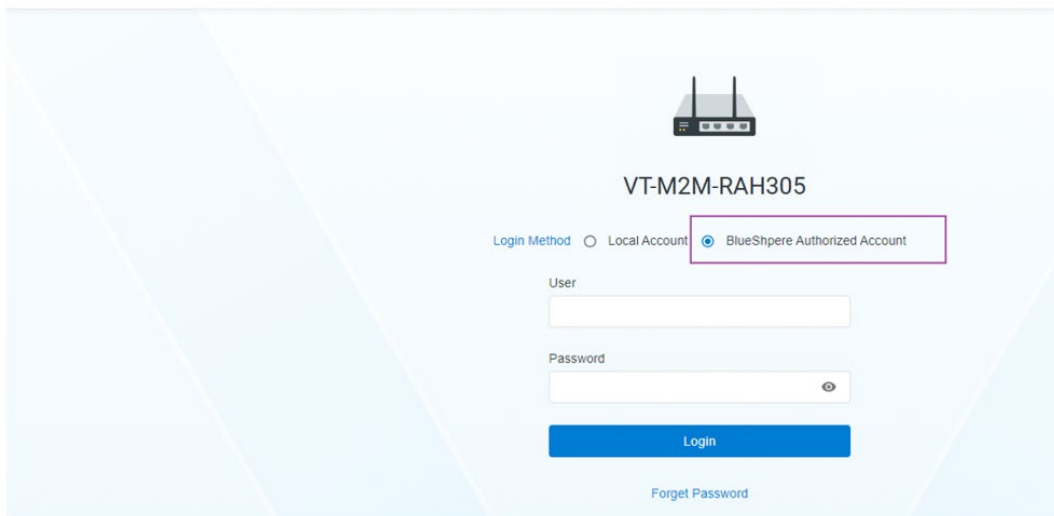
1. Enter the customer ID that is retrievable in the user profile on the GWM portal.
2. Click **Connect** to establish a connection between the device and the GWM portal.
3. When the handshake succeeds, the device status changes to **Connected**.
4. The real-time log will display the whole connection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

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



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

Vantron OS25



VT-M2M-RAH305

Login Method ☐ Local Account ☒ BlueSphere Authorized Account

User

Password

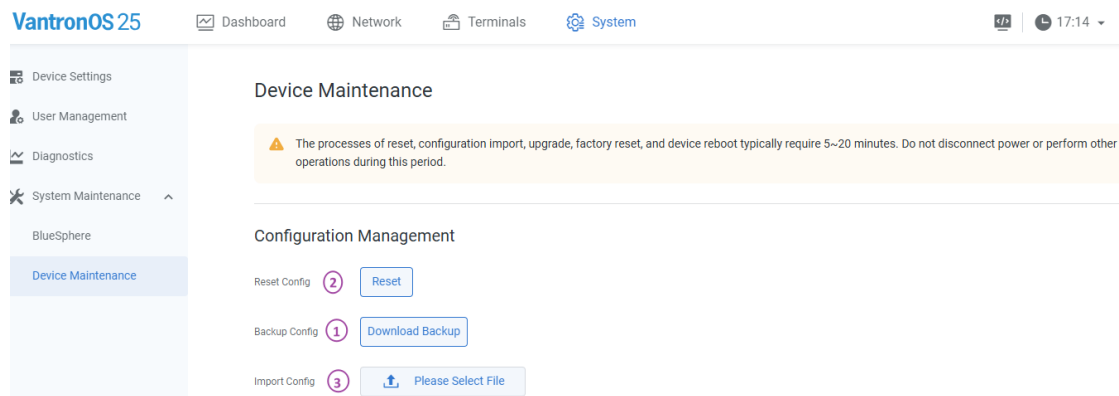
Login

[Forget Password](#)

3.6.4.2 Device Maintenance

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

○ Configuration Management



VantronOS 25

Dashboard Network Terminals System

17:14

Device Settings

User Management

Diagnostics

System Maintenance

BlueSphere

Device Maintenance

Device Maintenance

The processes of reset, configuration import, upgrade, factory reset, and device reboot typically require 5~20 minutes. Do not disconnect power or perform other operations during this period.

Configuration Management

Reset Config 2 Reset

Backup Config 1 Download Backup

Import Config 3 Please Select File

Description:

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

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

○ Upgrade

Upgrade

OS Version	V200R003.F0000-08	1
Upgrade OS	Please Select File	2
Install and Upgrade Software App	Please Select File	3

Description:

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

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

○ Device Maintenance

Device Maintenance

Factory Reset	Reset	1
Reboot Device	Reboot	2

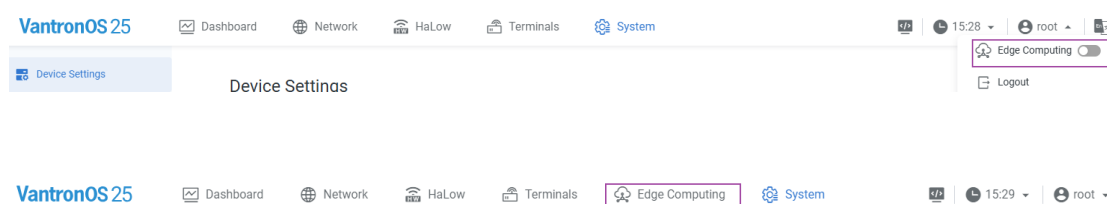
Description

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

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

3.7 Edge Computing

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



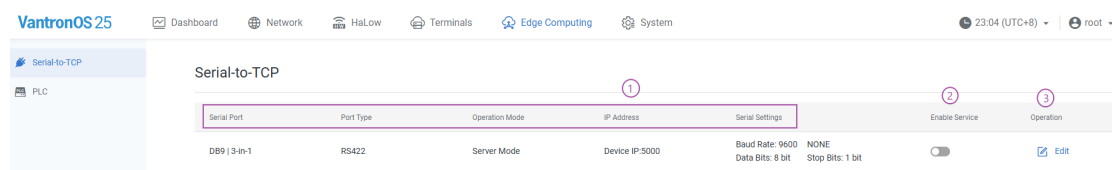
3.7.1 Serial to TCP

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

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

Pre-configured conversion rules for existing serial ports are provided. Users can modify the rule between server and client modes as needed. Adding or deleting a conversion rule is not supported.

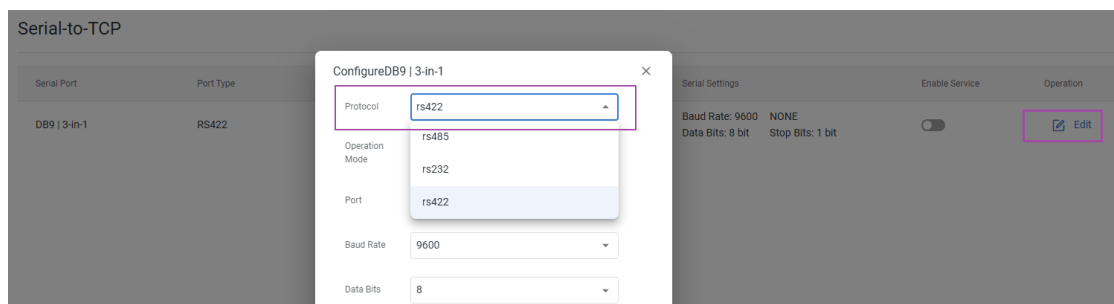
- **Server mode** turns the device's serial port into a TCP listener, allowing remote clients to connect and exchange data.
- **Client mode** makes the device's serial port a TCP client, automatically tunneling all traffic to a specified remote server.



Description:

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

*The serial port is a multiplexed, operating in the RS-422 mode by default and can be modified via the **Edit** menu.*



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

3.7.1.1 Server Mode Rule Setup

1. Click the **Edit** icon to enter the configuration page.

Serial-to-TCP

Serial Port	Port Type	Operation Mode	IP Address	Serial Settings	Enable Service	Operation
DB9 3-in-1	RS422	Server Mode	Device IP:5000	Baud Rate: 9600 Data Bits: 8 bit Stop Bits: 1 bit	☐	Edit

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

Serial-to-TCP

Serial Port	Port Type
DB9 3-in-1	RS422

Configure DB9 | 3-in-1

1 Protocol: rs485

2 Operation Mode: **Server Mode** Client Mode

3 Port: 5000

4 Baud Rate: 9600
Data Bits: 8
Stop Bits: 1
Parity: NONE

5 Flow Control: ☐

6 Detection Timeout: 20 (s)

7 [Save](#)

Serial Settings	Enable Service	Operation
Baud Rate: 9600 Data Bits: 8 bit Stop Bits: 1 bit	☐	Edit

- 1) Select a serial mode for the multiplexer.
 - 2) Select **Server Mode**.
 - 3) Designate a TCP port (0~65535) for the server to listen on. The client must connect to the same port.
 - 4) Make sure the serial parameters on both the peripheral and router are set the same.
 - 5) Enable/Disable software flow control to prevent packet loss (this may reduce throughput).
 - 6) Set the timeout to automatically drop the connection if no data is received (0=disabled).
 - 7) Save the changes to let them take effect.
3. Enable the conversion rule after editing the parameters.
 4. Make sure both the client and server are on the same reachable IP network.
 5. Verify the data transmission between the devices.

3.7.1.2 Client Mode Rule Setup

1. Click the **Edit** icon to enter the configuration page.

Serial-to-TCP

Serial Port	Port Type	Operation Mode	IP Address	Serial Settings	Enable Service	Operation
DB9 3-In-1	RS422	Server Mode	Device IP:5000	Baud Rate: 9600 Data Bits: 8 bit Stop Bits: 1 bit	☐	Edit

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

Serial-to-TCP

Serial Port	Port Type
DB9 3-In-1	RS422

ConfigureDB9 | 3-In-1

1 Protocol: rs485

2 Operation Mode: ☐ Server Mode ☒ **Client Mode**

3 Server IP: 192.168.19.255

4 Server Port: 5000

5 Baud Rate: 9600
Data Bits: 8
Stop Bits: 1
Parity: NONE

6 Flow Control: ☐

7 Detection Timeout: 20 (s)

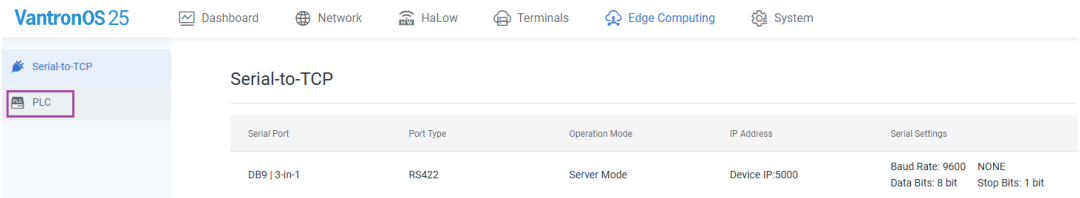
8

- 1) Select a serial mode for the multiplexer.
 - 2) Select **Client Mode**.
 - 3) Enter the server's IP address.
 - 4) Enter the target port and make sure it matches the TCP port on the server.
 - 5) Make sure the serial parameters on both the peripheral and router are set the same.
 - 6) Enable/Disable software flow control to prevent packet loss (this may reduce the throughput).
 - 7) Set the timeout to automatically drop the connection if no data is received (0=disabled).
 - 8) Save the changes to let them take effect.
3. Enable the conversion rule.
 4. Make sure both the client and server are on the same reachable IP network.
 5. Verify the data transmission between the devices.

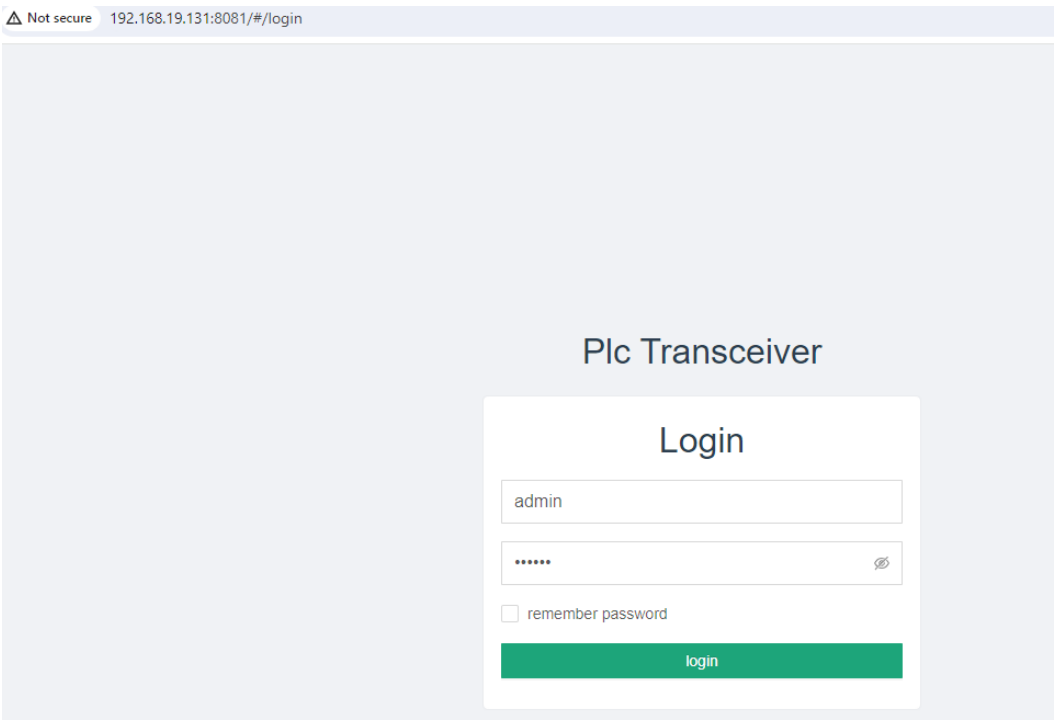
3.7.2 PLC

The RAH305 supports a wide range of edge-computing protocols. Southbound protocols include Modbus TCP, Modbus RTU, EtherNet/IP, ISO-on-TCP, CC-Link, etc. Northbound protocol primarily includes MQTT.

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



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



Refer to Chapter 4 for the detailed information.

CHAPTER 4 INDUSTRIAL PROTOCOLPORTAL

4.1 Overview

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

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

4.2 I/O Configuration

The RAH305 provides 4 digital input/output (DI/DO) channels and 4 analog input/output (AI/AO) channels for edge data transfer.

4.2.1 DI/DO Configuration

Refer to Section 1.8 for interface wiring instructions. The DI/DO channels support software mode switching, and the software node names match the silkscreen labels printed on the device housing.

1. Follow the steps in Section [2.3](#) to log in to the device.
2. Click the **CLI** icon to access the device shell.



3. Configure DI/DO channel working mode:

- Set to DI:

```
# gpio set dido1 di
# gpio set dido2 di
# gpio set dido3 di
# gpio set dido4 di
```

- Set to DO:

```
# gpio set dido1 do  
# gpio set dido2 do  
# gpio set dido3 do  
# gpio set dido4 do
```

4. Query the current working mode of each channel:

```
# gpio get dido1  
# gpio get dido2  
# gpio get dido3  
# gpio get dido4
```

5. Set DO output to high level:

```
# gpio set do1 on  
# gpio set do2 on  
# gpio set do3 on  
# gpio set do4 on
```

6. Set DO output to low level:

```
# gpio set do1 off  
# gpio set do2 off  
# gpio set do3 off  
# gpio set do4 off
```

4.2.2 AI/AO Configuration

Refer to Section 1.8 for interface wiring instructions. The DI/DO channels support software mode switching, and the software node names match the silkscreen labels printed on the device housing.

1. Follow the steps in Section [2.3](#) to log in to the device.
2. Click the **CLI** icon to access the device shell.



3. Configure AI/AO channel working mode:

- Set to AI:

```
# gpio set aiao1 ai
# gpio set aiao2 ai
# gpio set aiao3 ai
# gpio set aiao4 ai
```

- Set to AO:

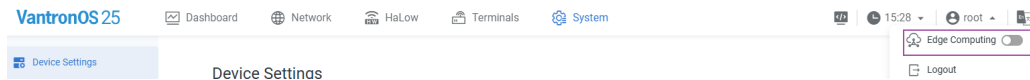
```
# gpio set aiao1 ao
# gpio set aiao1 ao
# gpio set aiao1 ao
# gpio set aiao1 ao
```

4. Query the current working mode of each channel:

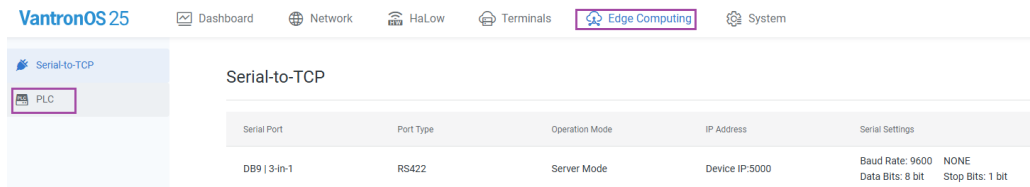
```
# gpio get aiao1
# gpio get aiao2
# gpio get aiao3
# gpio get aiao4
```

4.3 Portal Login

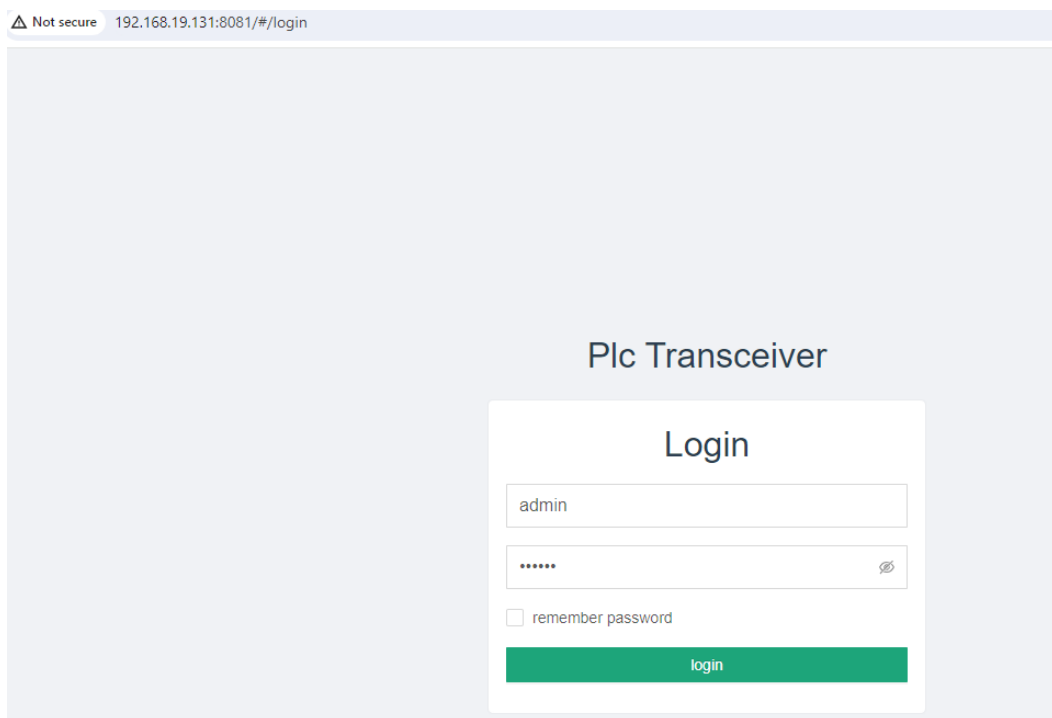
1. Enable the **Edge Computing** feature from the user account drop-down list.



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



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



The device's edge computing feature is currently under development and will be released in the upcoming firmware update.

CHAPTER 5 DISPOSAL AND WARRANTY

5.1 Disposal

When the device comes to end of life, you are suggested to properly dispose of the device for the sake of the environment and safety.

Before you dispose of the device, please back up your data and erase it from the device.

It is recommended that the device is disassembled prior to disposal in conformity with local regulations. Please ensure that the abandoned batteries are disposed of according to local regulations on waste disposal. Do not throw batteries into fire or put in common waste canister as they are explosive. Products or product packages labeled with the sign of “explosive” should not be disposed of like household waste but delivered to specialized electrical & electronic waste recycling/disposal center.

Proper disposal of this sort of waste helps avoid harm and adverse effect upon surroundings and people’s health. Please contact local organizations or recycling/disposal center for more recycling/disposal methods of related products.

5.2 Warranty

Product warranty

VANTRON warrants to its CUSTOMER that the Product manufactured by VANTRON, or its subcontractors will conform strictly to the mutually agreed specifications and be free from defects in workmanship and materials (except that which is furnished by the CUSTOMER) upon shipment from VANTRON. VANTRON's obligation under this warranty is limited to replacing or repairing, at its option, of the Product which shall, within **24 months** after shipment, effective from invoice date, be returned to VANTRON's factory with transportation fee paid by the CUSTOMER and which shall, after examination, be disclosed to VANTRON's reasonable satisfaction to be thus defective. VANTRON shall bear the transportation fee for the shipment of the Product to the CUSTOMER.

Out-of-Warranty Repair

VANTRON will furnish the repair services for the Product which are out-of-warranty at VANTRON's then-prevailing rates for such services. At customer's request, VANTRON will provide components to the CUSTOMER for non-warranty repair. VANTRON will provide this service as long as the components are available in the market; and the CUSTOMER is requested to place a purchase order up front. Parts repaired will have an extended warranty of 3 months.

Returned Products

Any Product found to be defective and covered under warranty pursuant to Clause above, shall be returned to VANTRON only upon the CUSTOMER's receipt of and with reference to a VANTRON supplied Returned Materials Authorization (RMA) number. VANTRON shall supply an RMA, when required within three (3) working days of request by the CUSTOMER. VANTRON shall submit a new invoice to the CUSTOMER upon shipping of the returned products to the CUSTOMER. Prior to the return of any products by the CUSTOMER due to rejection or warranty defect, the CUSTOMER shall afford VANTRON the opportunity to inspect such products at the CUSTOMER's location and no Product so inspected shall be returned to VANTRON unless the cause for the rejection or defect is determined to be the responsibility of VANTRON. VANTRON shall in turn provide the CUSTOMER turnaround shipment on defective Product within **fourteen (14) working days** upon its receipt at VANTRON. If such turnaround cannot be provided by VANTRON due to causes beyond the control of VANTRON, VANTRON shall document such instances and notify the CUSTOMER immediately.

Appendix Regulatory Compliance Statement

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate this equipment.

RF Radiation Exposure Statement:

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

IC Statement

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

- (1) This device may not cause interference, and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

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

Exposure to radio frequency energy:

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

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

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

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

L'exposition à l'énergie radiofréquence:

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