RAH305 Wi-Fi HaLow Router



User Manual

Version: 1.4

© Vantron Technology, Inc. All rights reserved.

Revision History

No.	Firmware Version	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
V1.4	VantronOS 25 - V200R003.F0000-04 (OS: 26.3.1, App: 26.3.2)	1. Updated the definition of MPP and MP in Section 1.5. 2. Updated cover image and product layout markup in Section 1.7. 3. Added the HaLow LED definition in Section 1.9.4. 4. Updated cellular LED definition in Section 1.9.5. 5. Updated the description on WAN login in Section 2.3. 6. Added Notes to Sections 2.6.1 & 2.6.2. 7. Updated Section 3.3.4 on cellular configurations to reflect UI changes. 8. Added description on network access control in Section 3.3.10, and updated Section 3.3.11 to align with UI changes. 9. Added GNSS-related settings to Section 3.6.1.3. 10. Added Sections 3.6.3.1, 3.6.5 & 3.6.6 to reflect the new features.	Nov. 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 HaLow Activity LED (HaLow) 21
1.9.5 Cellular Signal Strength LED 21
1.10 Button 22
1.10.1 Reset Button 22
1.10.2 WPS Button 22
1.10.3 DPP Button 22
1.11 Console Port 23
1.12 SIM Slot 23
1.13 USB Type-A 23
CHAPTER 2 GETTING STARTED 24
2.1 Device Installation 25
2.2 Hardware Connection 26
2.3 Web Login 30
2.3.1 Login Wizard 31
2.3.2 Log Out 38
2.4 Debugging the Device (via Console Port) 38
2.5 SSH Login 41
2.6 Wireless Quick Pairing 43
2.6.1 Wi-Fi WPS Connection 43

2.6.2 HaLow DPP Pairing 44
CHAPTER 3 DEVICE SETUP VIA VANTRONOS 45
3.1 Introduction to VantronOS 46
3.1.1 Web Overview 46
3.1.2 Log Out 47
3.2 Dashboard 48
3.3 Network 49
3.3.1 WAN Interface 49
3.3.1.1 Basic IP Configuration 49
3.3.1.2 Interface Bridging 51
3.3.1.3 Link Priority 52
3.3.1.4 Link Diagnosis 53
3.3.2 LAN Interface 54
3.3.2.1 Subnet Conflict 54
3.3.2.2 DHCP Service & DHCP Reservation 54
3.3.3 IPv6 Settings 56
3.3.4 Cellular 57
3.3.4.1 Basic Settings 57
3.3.4.2 Advanced Settings 58
3.3.5 Wi-Fi 60
3.3.5.1 AP-Mode Basic Settings 60
3.3.5.2 AP-Mode Advanced Settings 61
3.3.5.3 STA-Mode Basic Settings 62
3.3.5.4 STA-Mode Advanced Settings 63
3.3.6 VPN 64
3.3.6.1 OpenVPN Server-Client Network Settings 64
3.3.6.2 OpenVPN Server Setup 65
3.3.6.3 OpenVPN Client Setup 67
3.3.6.4 Application Scenario Topology 70
3.3.7 QoS Bandwidth Control 72
3.3.8 Static Route 73
3.3.9 Porting Mapping 75
3.3.10 Network Security 77
3.3.11 ACL Access Control 79
3.3.11.1 No-Rule Access Policy 79
3.3.11.2 ACL Rules 79
3.4 HaLow 81
3.4.1 AP-Mode Settings 82
3.4.2 Mesh Networking 84
3.5 Terminals 85
3.6 System 85

3.6.1 Device Settings 85
3.6.1.1 Modifying Device Name....85
3.6.1.2 System Time 86
3.6.1.3 GNSS Information 87
3.6.2 User Management 89
3.6.3 Diagnostics 90
3.6.3.1 Packet Capture....90
3.6.3.2 Network Diagnostics....91
3.6.3.3 Web Terminal 92
3.6.3.4 Logs 93
3.6.3.5 Log Capture 93
3.6.4 System Maintenance 95
3.6.4.1 BlueSphere 95
3.6.4.2 Device Maintenance....96
3.6.5 Performance Indicators....98
3.6.6 USB Management 100
3.7 Edge Computing.... 101
3.7.1 Serial to TCP 101
3.7.1.1 Server Mode Rule Setup 103
3.7.1.2 Client Mode Rule Setup 104
3.7.2 PLC 105
CHAPTER 4 INDUSTRIAL PROTOCOLPORTAL.... 106
4.1 Overview.... 107
4.2 I/O Configuration 107
4.2.1 DI/DO Configuration.... 107
4.2.2 AI/AO Configuration.... 109
4.3 Portal Login 110
CHAPTER 5 DISPOSAL AND WARRANTY 111
5.1 Disposal 112
5.2 Warranty 113
Appendix Regulatory Compliance Statement.... 114

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
ℹ	Attention to important information or regulations

General Safety Instructions

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

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

Precautions for Power Cables and Accessories

⚠ Use proper power source only. Make sure the supply voltage falls within the specified range. The Product is designed to use 9-36V DC. Always check whether the Product is DC powered before applying power.

⚠ Place the cables properly at places without extrusion hazards.

⚠ Use only approved antenna(s). Non-approved antenna(s) may produce spurious or excessive RF transmitting power which may violate FCC limits.

⚠ Cleaning instructions:

- Power off the Product before cleaning
- Do not use spray detergent
- Clean with a damp cloth
- Do not try to clean exposed electronic components unless with a dust collector

⚠ Power off and contact Vantron technical support engineer in case of the following faults:

- The Product is damaged
- The temperature is excessively high
- Fault is still not solved after troubleshooting according to this manual

⚠ Do not use in combustible and explosive environment:

- Keep away from combustible and explosive environment
- Keep away from all energized circuits
- Unauthorized removal of the enclosure from the Product is not allowed
- Do not change components unless the power cable is unplugged
- In some cases, the Product may still have residual voltage even if the power cable is unplugged. Therefore, it is a must to remove and fully discharge the Product before replacement of the components.

CHAPTER 1 HARDWARE DESCRIPTION

1.1 Overview

Powered by the advanced MM8108 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 cellular 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 × DI/DO and 4 × 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 × LAN, 1 × WAN, 4G/5G, BT 5.3, GNSS
- Rich industrial interfaces: AI/AO, DI/DO, USB, RS-232/485/422
- Sub-1 GHz HaLow operating bands
- Long-distance transmission, coverage up to 1 km
- Improved penetration through walls and obstacles
- Supports 1/2/4/8 MHz channel bandwidths with dynamic channel selection (DCS)
- WPS & DPP support for quick Wi-Fi 6 & HaLow pairing
- Static routing, port mapping, QoS, and ACL support
- Optional BlueSphere GWM support for remote control
- Industrial extended input voltage operation

1.3 Unpacking

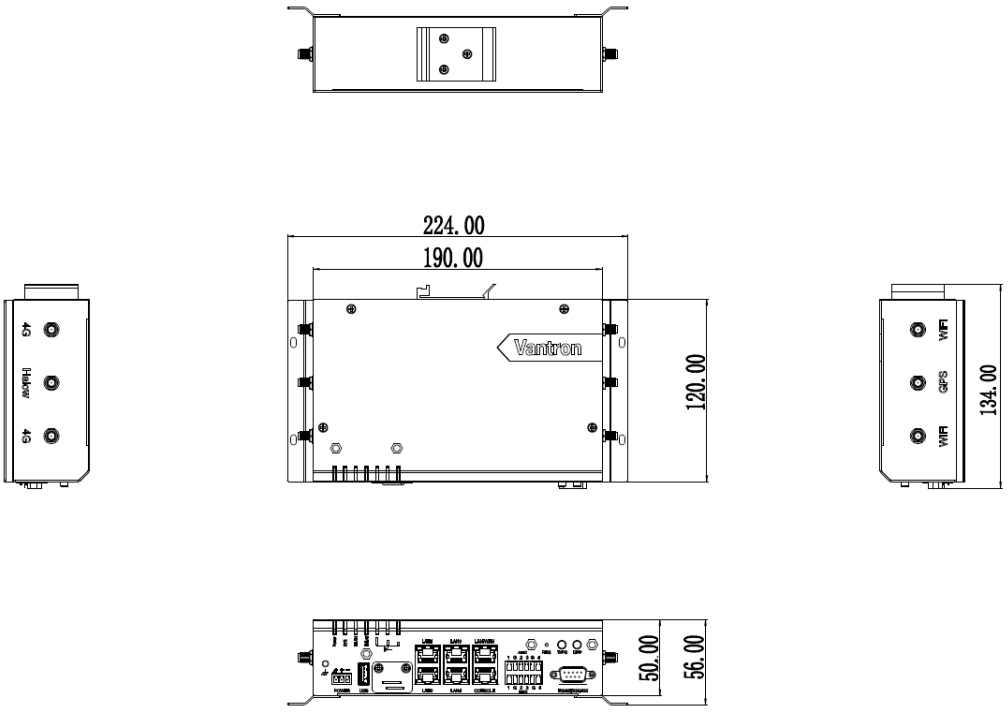
The Product has been carefully packed with special attention to quality. However, should you find anything damaged or missing, please contact your sales representative in due time.

Standard Accessories

- 1 × RAH305 Wi-Fi HaLow router
- 1 × Wi-Fi HaLow antenna
- 2 × 2.4GHz/5GHz Wi-Fi antenna
- 1 × GNSS magnetic mount antenna
- 2 × Cellular magnetic mount antenna
- 2 × 6-pin × 3.81mm terminal connector for DI, DO, AI, AO
- 1 × 12V 2A DC Power adapter
- 1 × 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
Access Point (AP)	A HaLow access point (AP) broadcasts the HaLow network to multiple HaLow stations (STA). It typically connects to an internet router, distributing internet connectivity to all paired STAs. In a standard HaLow network, there will always be **only one** HaLow AP.
Station (STA)	An STA is a client device that connects to a HaLow AP for a standard HaLow networking. It normally accesses external networks through the HaLow AP.
Standard HaLow network	Standard HaLow network describes the basic star-shaped HaLow network architecture. In this topology, all STAs associate with a central AP, and traffic between endpoints is relayed through the AP.
HaLow Mesh network	A HaLow Mesh network extends network range and improves reliability through multi-hop communication between interconnected nodes, which automatically determine the most efficient path for data transmission.
Mesh Portal (MPP)	A Mesh Portal (MPP) serves as the DHCP server in a mesh network. When a HaLow AP enables mesh settings, it takes on a combined AP+MPP role. Mesh nodes gain internet access when the MPP connects to an upstream network device.
Mesh Point (MP)	A Mesh Point (MP) operates as an intermediate HaLow node that forwards data between other mesh nodes via multi-hop relaying. These nodes retain their original HaLow IP addresses as mesh IP addresses.
Wi-Fi Protected Setup (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
Device Provisioning Protocol (DPP)	Defined by Wi-Fi Alliance for **Wi-Fi Easy Connect™**. In this document, it refers specifically to the fast provisioning of devices via simple hardware/software setup for a standard HaLow pairing ("**DPP Pairing**").
VantronOS	Web management portal for Vantron IoT communication devices.
Dynamic Channel Selection (DCS)	DCS is a mechanism that automatically evaluates channel conditions and selects a suitable operating channel for the radio. It avoids interference from other wireless signals and improves link stability.

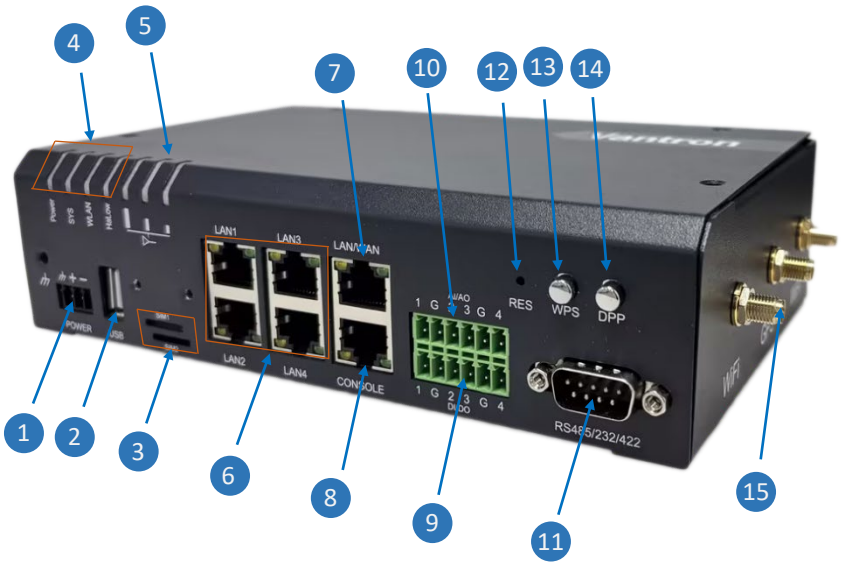
Unless otherwise stated, *Wi-Fi* in this manual refers to the device's 2.4GHz/5GHz Wi-Fi (Wi-Fi 6), and *HaLow* refers to Wi-Fi HaLow.

1.6 Specifications

RAH305			
HARDWARE			
System	CPU	TI AM64 64-bit Arm® Cortex®-A53 microprocessor, up to 1GHz	
	Wi-Fi HaLow SoC	Morse Micro MM8108	
	Memory	512MB DDR4	
	Storage	8GB eMMC	
WLAN	Wi-Fi 6	Standard: IEEE 802.11ax/ac/b/g/n	
		Frequency range: 2.400GHz~2.4835GHz, 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, STA**	
	Wi-Fi HaLow	Standard: IEEE 802.11 ah	
		Frequency range: 903.5MHz~926.5MHz (US)	
		Channel bandwidth: 1/2/4/8MHz, dynamic channel selection (DCS) supported	
		Max. transmit power: 28.5 dBm (700 mW)	
		Data rate: up to 43.3 Mbps @8 MHz bandwidth	
		Application mode: Mesh, Bridge WAN	
		Quick pairing: DPP quick pairing supported	
		Working mode: **AP, Mesh**	
Bluetooth	Version	BT 5.3	
Cellular	Modem	4G/5G	
GNSS	Satellite Support	GPS, BeiDou, GLONASS, GALILEO, QZSS (A-GNSS supported)	
	Positioning Precision	2.5m (CEP50)	
I/O	Ethernet	5 × RJ45, 10/100/1000Mbps (1 × WAN/LAN, 4 × LAN)	
	Console	1 × RS232-to-RJ45 port	
	USB	1 × USB 2.0 Type-A	
	Serial Port	1 × RS485/232/422 (DB9)	
	DI/DO	4 × DI/DO (Software switchable, DI: 0-12V, DO: Follows device supply voltage)	
	AI/AO	4 × AI/AO (Software switchable, AI: 0-10V, AO: 4-20mA)	
	SIM Slot	2 × Micro SIM slot	
	Antenna	1 × Wi-Fi HaLow antenna	2 × Wi-Fi (6) antenna
		2 × Cellular antenna	1 × GNSS antenna

RAH305			
System Control	LED indicators	1 × Power indicator	1 × Wi-Fi HaLow activity indicator
		1 × System indicator	1 × WLAN (Wi-Fi 6) activity indicator
		3 × Cellular signal strength indicator	
	Button	1 × Restore button (pinhole)	
		1 × WPS button (For Wi-Fi quick pairing)	1 × DPP button (For HaLow quick pairing)
Miscellaneous	RTC	Supported	
	WDT	Supported	
Mechanical	Enclosure Material	SGCC (Steel Galvanized Cold Commercial)	
	Dimensions	224mm × 134mm × 56mm	
	Installation	Wall mounting, DIN rail mounting	
Power	Input	9V ~ 36V DC	
	Port	3-Pin × 3.81mm terminal (Over-current protection, reverse polarity protection)	
Environmental Conditions	Temperature	Operating: -20℃~+60℃	Storage: -40℃~+70℃
	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 & UPD, 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 > Cellular (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	OpenVPN, PPTP*, L2TP*, GRE*, IPSec*	
	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 × Micro SIM slot
4	4 × 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 × 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	DI/DO 1-4, software switchable. DO output voltage follows device supply voltage. DI: 0~12V, max. 200mA, pulse counter supported (max. frequency <25Hz).
10	AI/AO 1-4, software switchable. AI: 0~10V input (12-bit res.); 4~20mA output (12-bit res.)
11	RS-232/485/422 (uart0), mode switchable via the VanrtonOS 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 × Antenna connector (Far → Near: Wi-Fi (6) antenna, GNSS antenna, Wi-Fi (6) antenna)

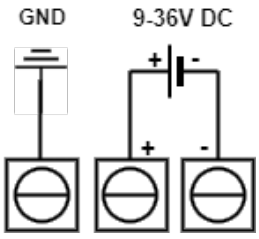


Description:

Item	Description
1	DIN rail mount
2	3 × 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 × 3 × 3.81mm, 12V/2A DC recommended.

1.8.2 Digital Input (DI)

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

Wiring:

DIx → External switch or sensor signal wire

GND → Signal ground

1.8.3 Digital Output (DO)

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

Wiring:

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

GND → Negative terminal of external load

1.8.4 Analog Input (AI)

Wiring:

AIx → Switch/sensor V+

GND → Switch/sensor V-

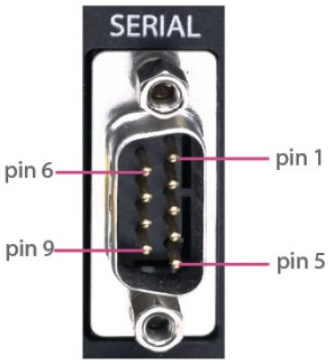
1.8.5 Analog Output (AO)

Wiring:

AOx → Load +

GND → Load –

1.8.6 RS-232/485/422

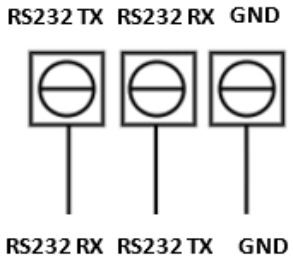


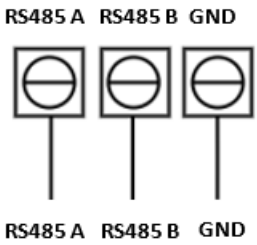
The RAH305 provides an RS-232/RS-485/RS-422 multiplexer for local data transfer. The multiplexer defaults to the RS-422 mode and can be modified via the **Edit** menu on the **Edge Computing > Serial-to-TCP** page. Refer to Section 3.7.1 for details.

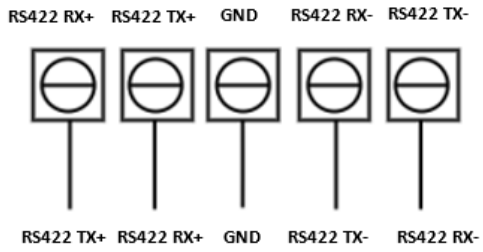
Pinout description:

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 boot failure/system anomaly.

1.9.3 WLAN (Wi-Fi) LED

Mode	LED Status	Description
Wi-Fi Client	OFF	Wi-Fi link is down.
	Blinking at 1Hz	Not connected to a Wi-Fi AP yet.
	Solid green	Connected to a Wi-Fi AP.
Wi-Fi AP	OFF	Wi-Fi link is down.
	Blinking at 1Hz	Not connected to a Wi-Fi AP yet.
	Blinking at 3Hz	WPS (quick pairing) initiated. Back to solid green after the process finishes.
	Solid green	At least one Wi-Fi client connected.

1.9.4 HaLow Activity LED (HaLow)

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

The RAH305 supports HaLow AP and Mesh operations modes.

1.9.5 Cellular Signal Strength LED

LED Status	Description
OFF	No SIM card inserted / Cellular module not functioning.
Blinking in a loop (1-2-3-1-2-3… 0.5s per LED)	SIM card inserted and module operational. Transitions to solid on state after dial-up completes.
Blinking at 0.5Hz (All three LEDs)	Cellular connection unavailable.
Solid on	Cellular connection active, indicating signal strength: • Excellent: ≥ 93% (LED 1, LED 2, LED 3 solid on) • Good: 67% ~ 92% (LED 1 & LED 2 solid on) • Fair: 39% ~ 66% (LED 1 solid on) • Weak: ≤ 38% (LED 1 blinking)

In the table above, LED 1 refers to the one located on the right, 2 in the middle, and 3 on the left.

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 2.4 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.

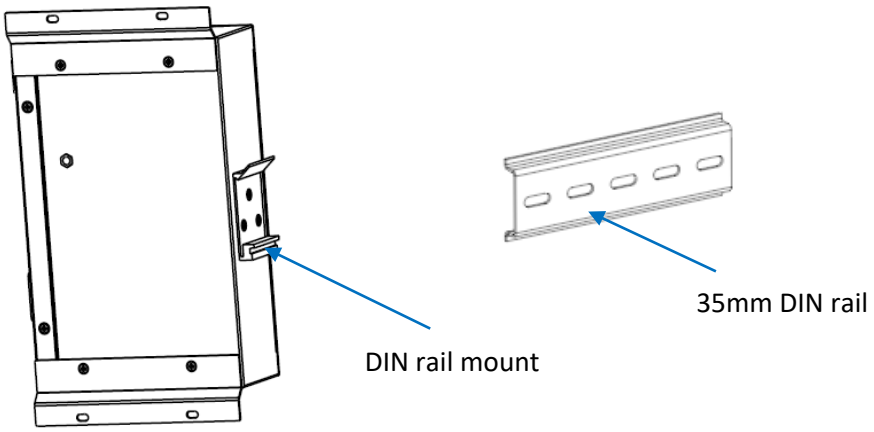
CHAPTER 2 GETTING STARTED

2.1 Device Installation

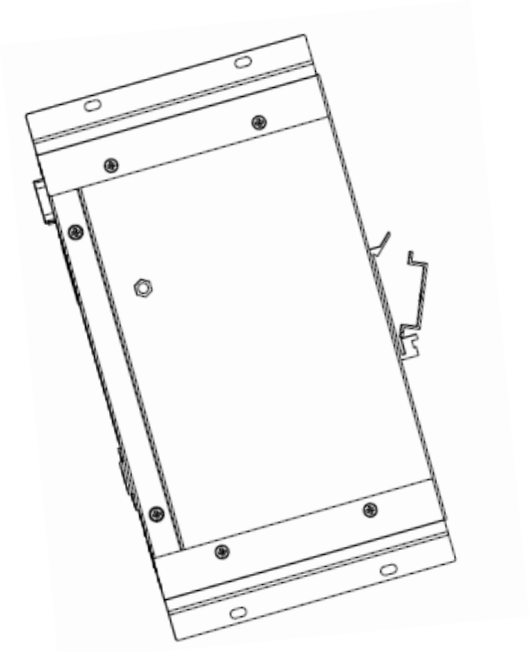
When mounting the RAH305 on a vertical surface, ensure the device is positioned so that the LED indicators are visible from ground level.

The following steps detail the DIN rail mounting procedure.

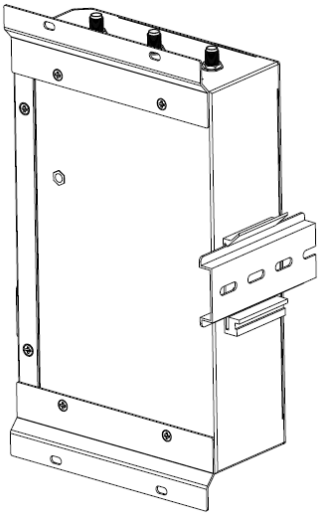
1. Hold the router vertically, and align the DIN rail mount of the device to the 35mm DIN rail.



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.



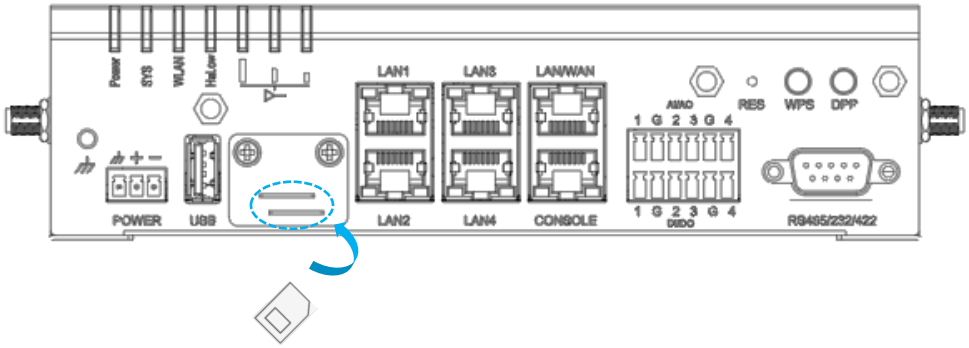
3. Push the router toward the DIN rail until it snaps securely into place.
4. Gently swing the device to make sure it is fixed on the DIN rail.



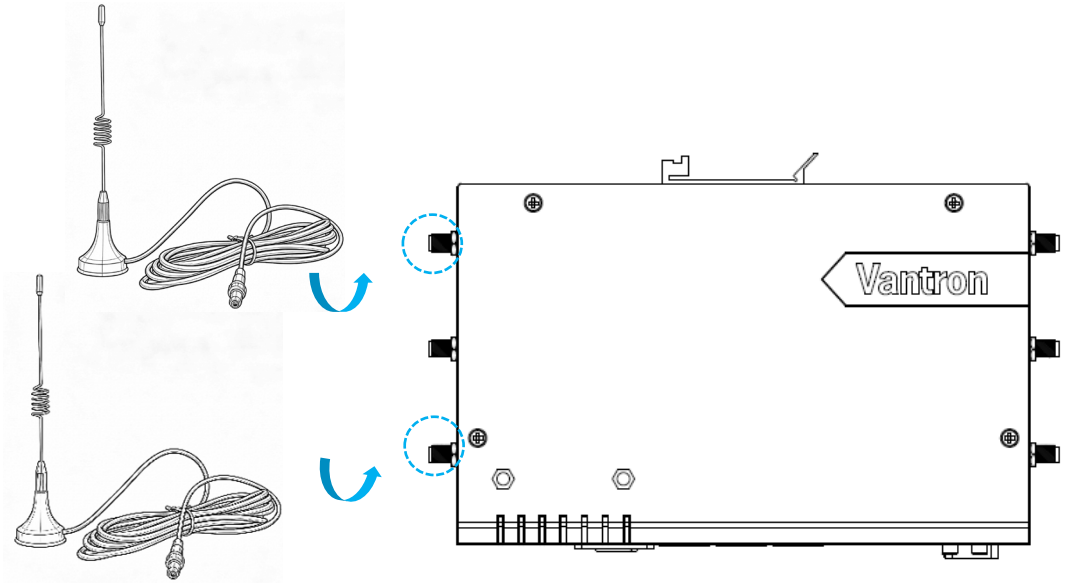
2.2 Hardware Connection

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

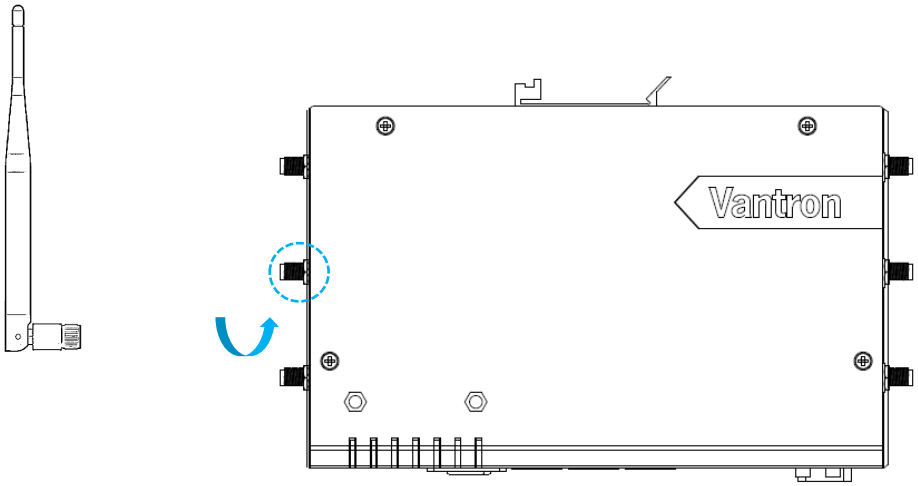
1. Based on your networking requirements, insert an activated Micro SIM card into either slot and push the card in until it clicks into place.
   - For SIM 1: Gold contacts facing **down**;
   - For SIM 2: Gold contacts facing **up**.



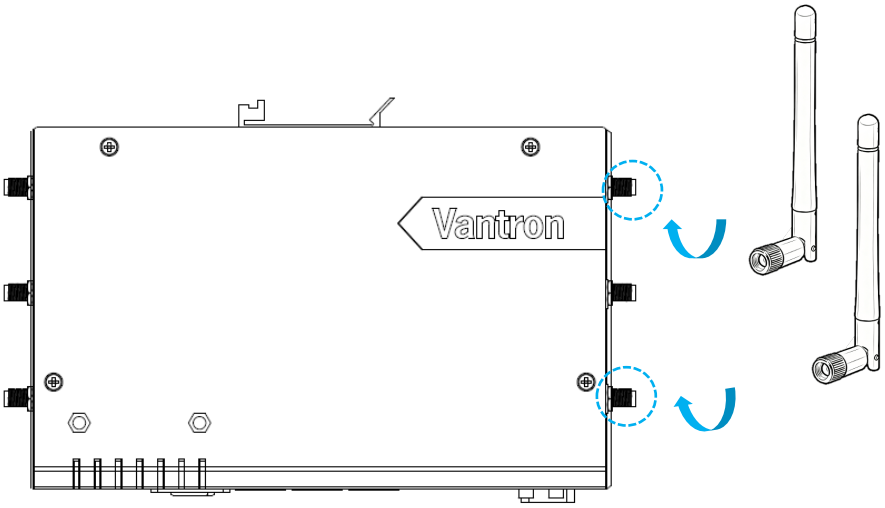
2. For cellular connectivity, install cellular antennas (magnetic mount) to their matching connectors on the left panel of the device.



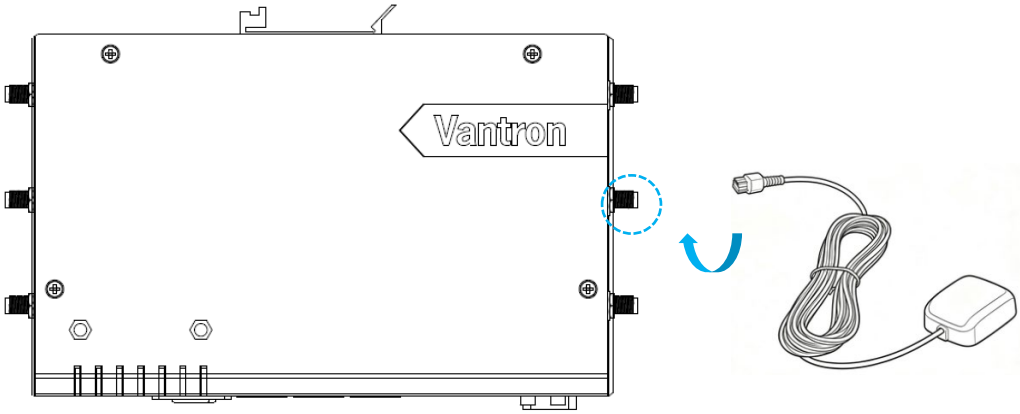
3. Attach the HaLow antenna (one with longer tip) to the middle connector on the left panel.



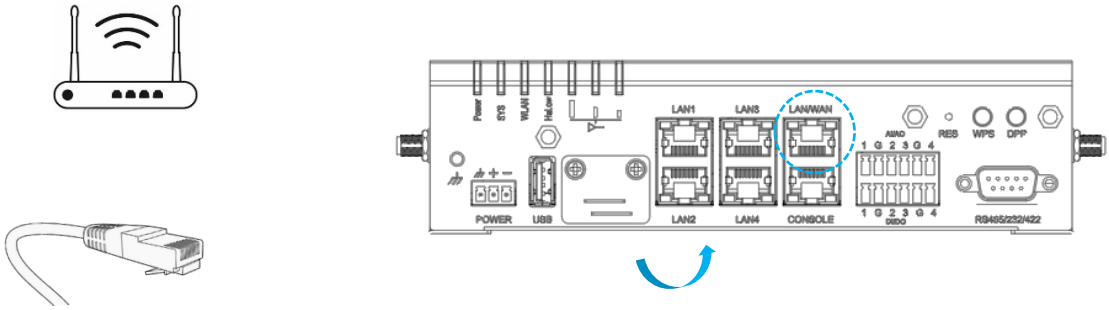
4. Install the Wi-Fi antennas to the matching connectors on the right panel of the device.



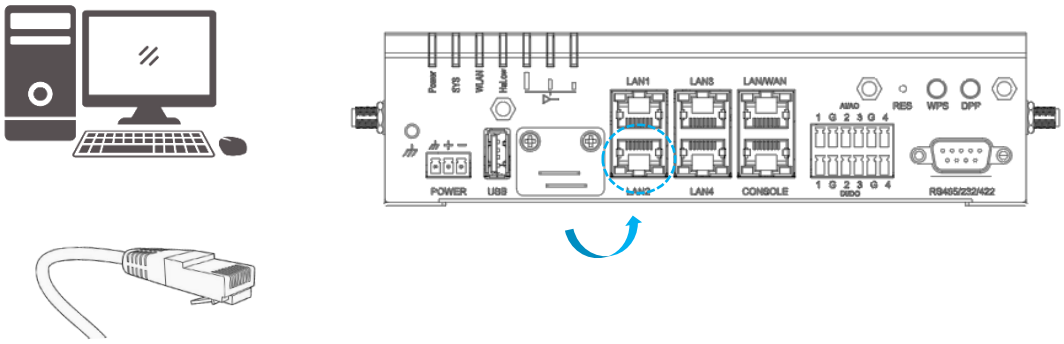
5. Install the GNSS antenna (magnetic mount) to the middle connector on the right panel.



6. To enable internet access, connect the WAN/LAN port to an upstream network device.

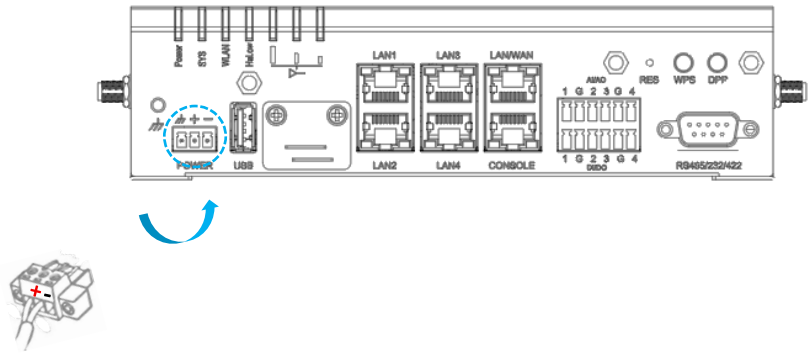


7. Connect a PC or other network devices to any of the LAN ports (LAN 1~LAN 4) using an Ethernet cable for local management or Internet access.



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 device's power terminal and connect the other end to the power cord.



10. Plug the power adapter into a DC power source 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

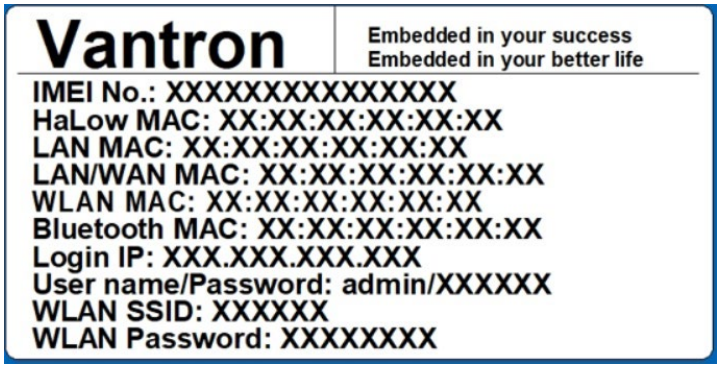
You can configure the network settings and manage the device via the web-based management portal (VantronOS) using a **Windows** PC.

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

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

* Option 2 is factory disabled for security concerns. To enable it, log in using Option 1 first, then modify the settings on the **Network > Network Security** page.

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



To establish quick LAN access for device management, follow the procedure below:

1. Connect the Windows PC:
   - Via Ethernet

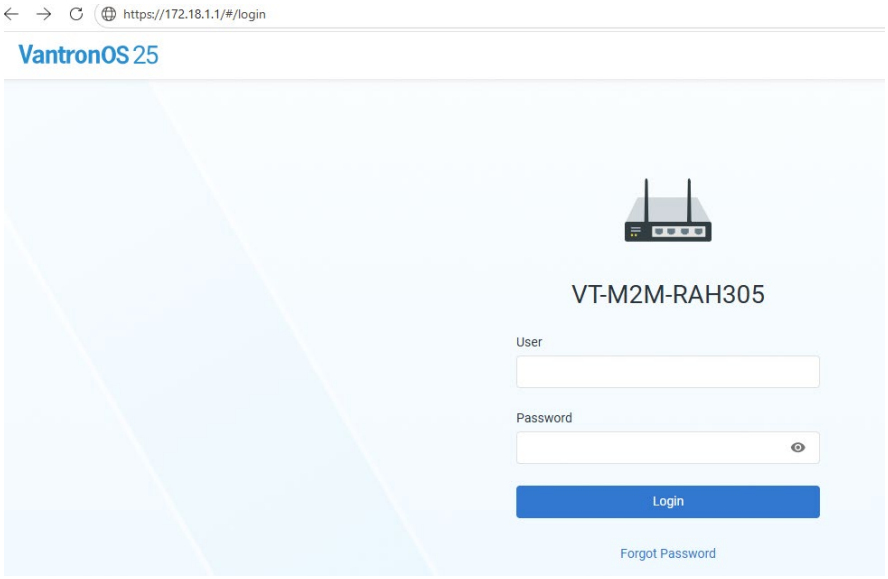
     Connect the Windows PC directly to any of the RAH305's LAN ports using a standard Ethernet cable.
   - Via Wi-Fi

     Connect the PC to the Wi-Fi AP of the RAH305 using the default WLAN SSID and password provided on the device label.

2. Enter the login IP in the browser for device login.

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

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

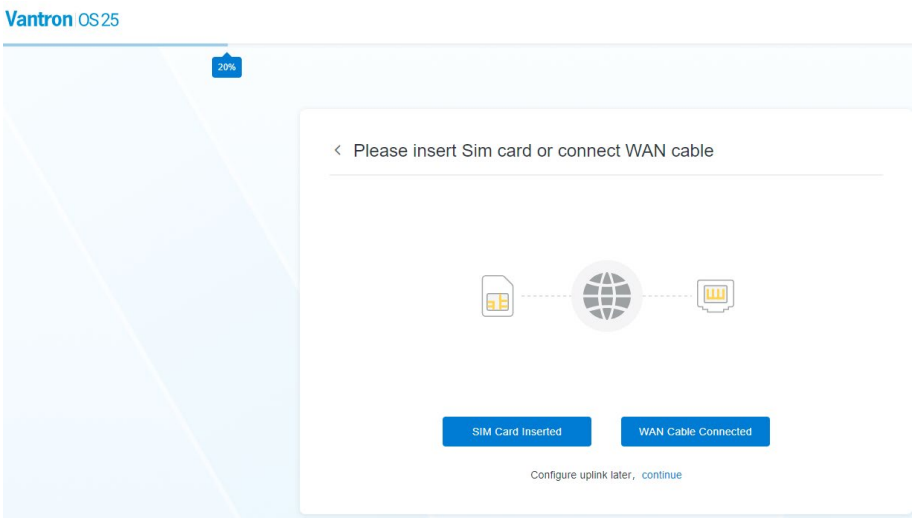


4. Upon **first** login, the system will automatically launch a setup wizard that will guide you through configuring essential settings.

2.3.1 Login Wizard

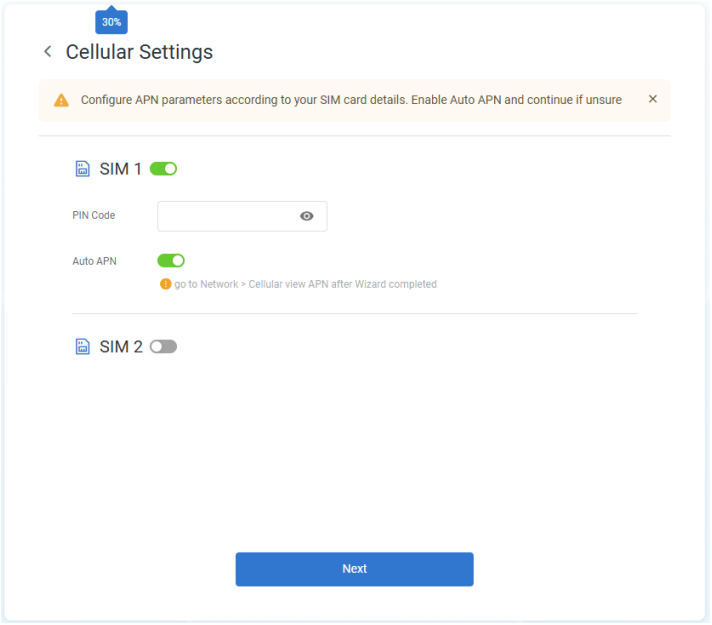
For first-time login or login after a device reset, the setup wizard will guide you through the initial setup process for quick setup.

Connect to an upstream network device 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.



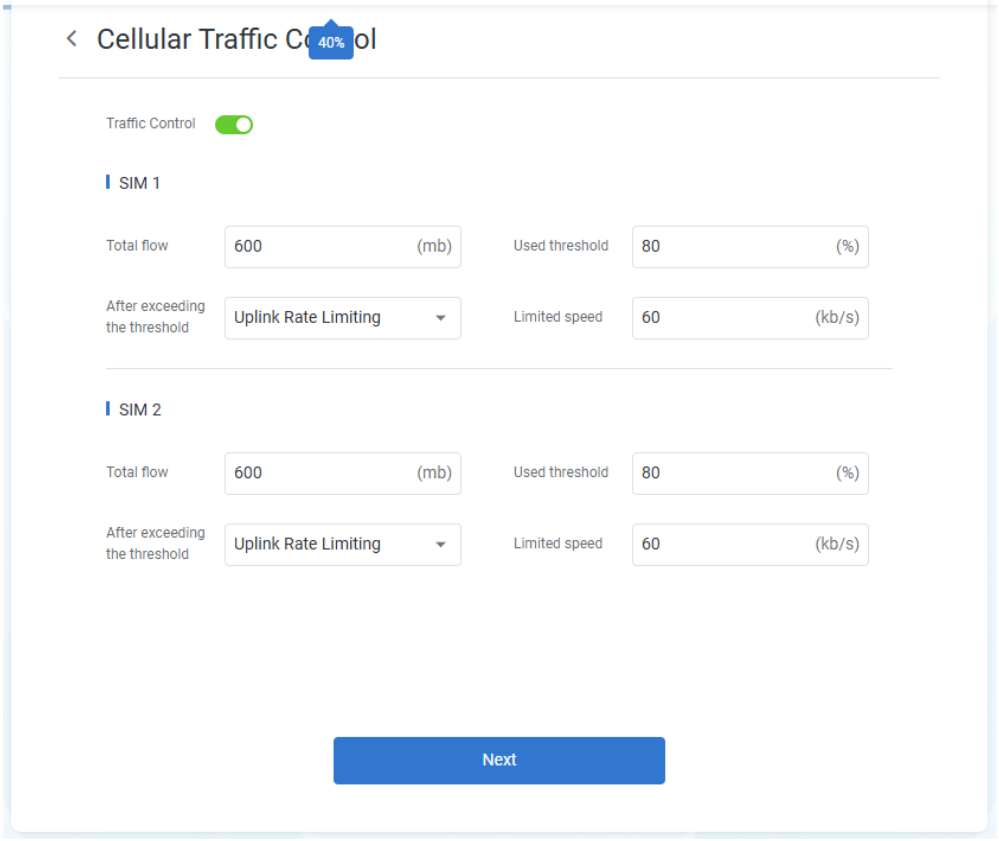
PIN Code: Carrier-defined, optional.

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

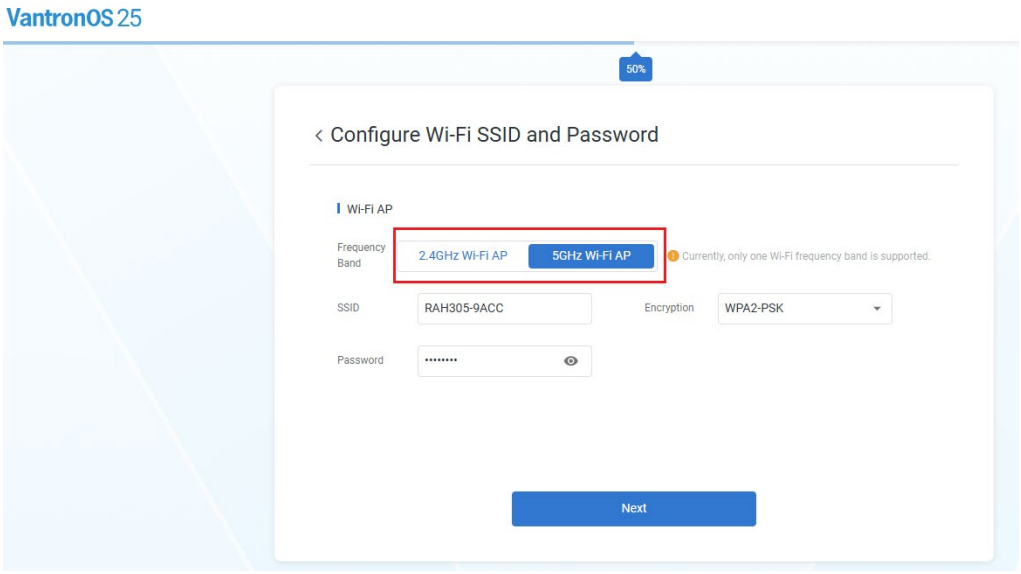
Authentication Type (None / PAP / CHAP): Carrier-defined; required when **Auto APN** is disabled.

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

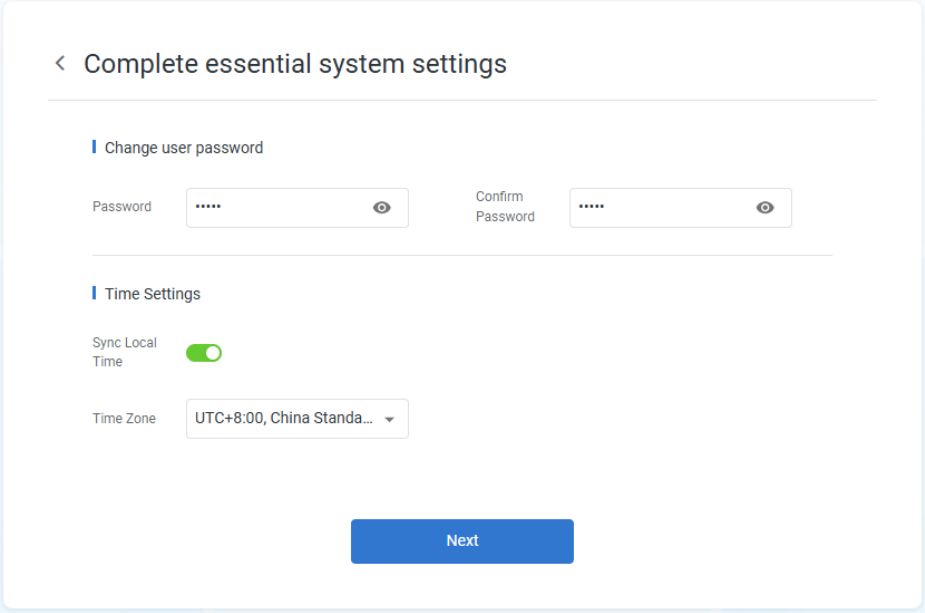
2. To manage data usage, enable **Traffic Control** and configure the relevant parameters as needed.



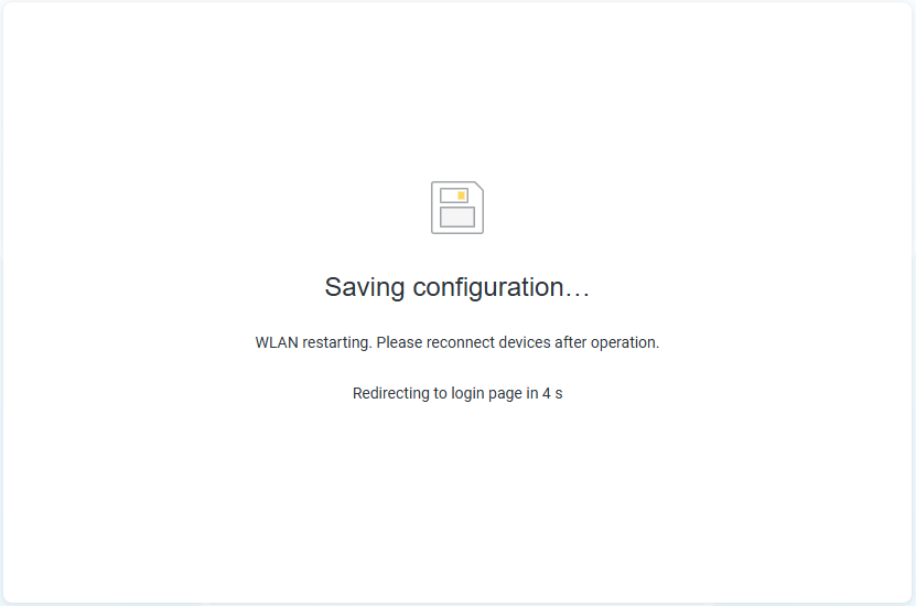
3. Configure the device's Wi-Fi AP settings for the 2.4GHz or 5GHz band (both can be configured, but **only one** is active at a time).



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



5. Wait approximately 10 seconds to allow the changes to apply. Once the countdown finishes, you will be redirected to the login page.

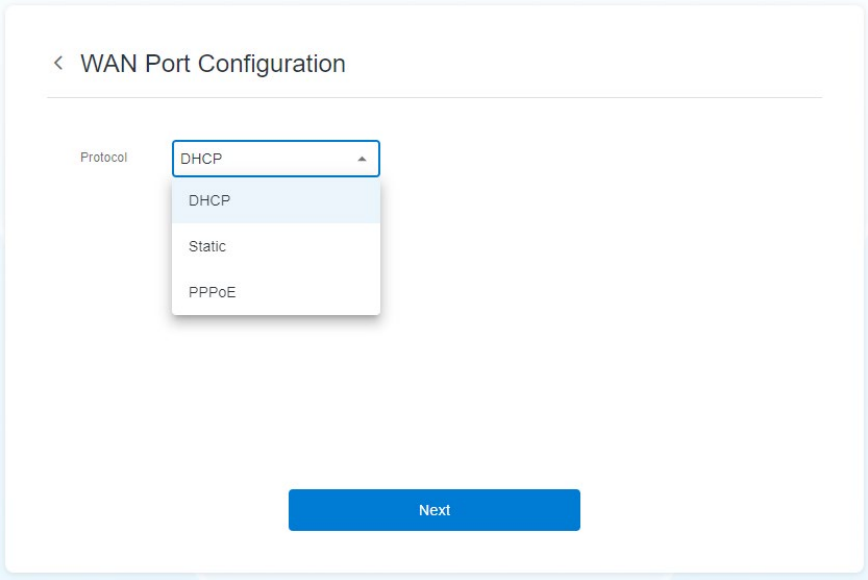


6. Log back in to the web portal using the new password.

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

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

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

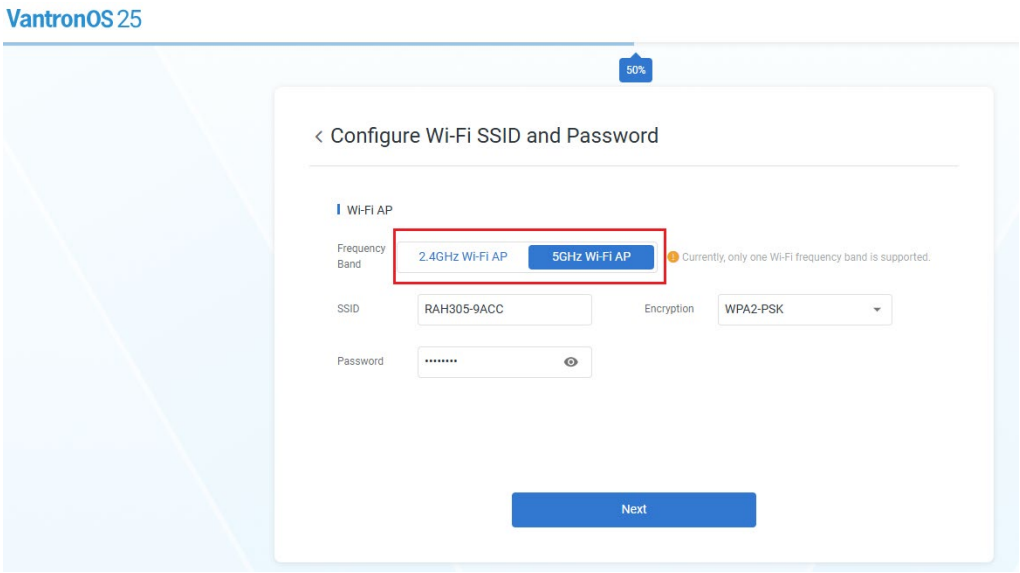


DHCP (Dynamic Host Configuration Protocol): A DHCP server **automatically** assigns IP addresses and network configuration (subnet, gateway, DNS) to the device.

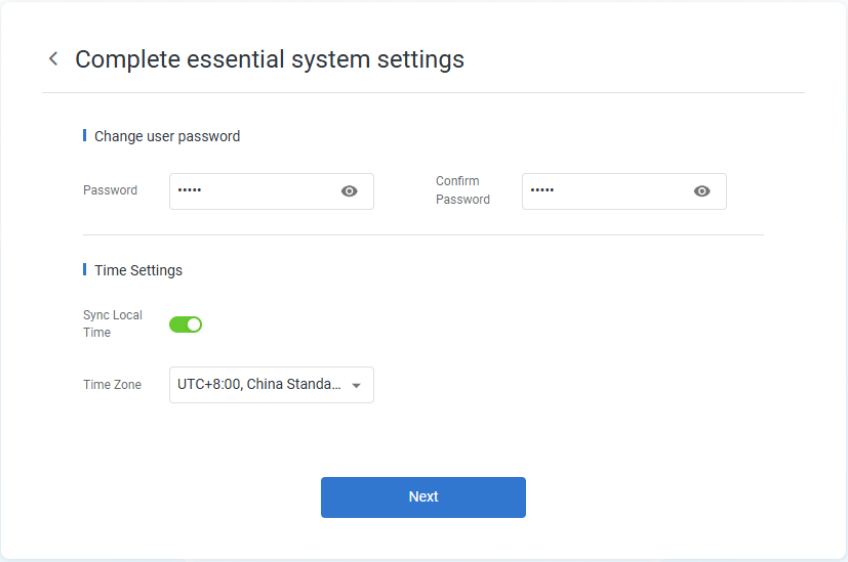
Static: IP settings are **manually** entered into the device and remain fixed until changed.

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).

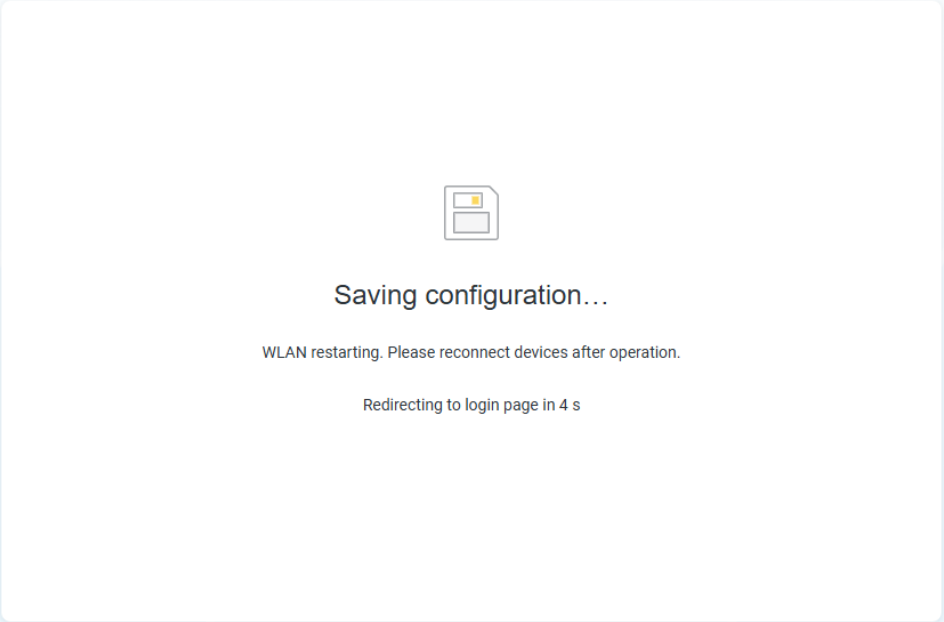
2. Configure the device's Wi-Fi AP settings for the 2.4GHz or 5GHz band (both can be configured, but only one is active at a time).



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



4. Wait approximately 10 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, the setup wizard will be relaunched. A configuration clear requires your user-defined password, while a factory reset requires the credentials on the device label.

2.3.2 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.

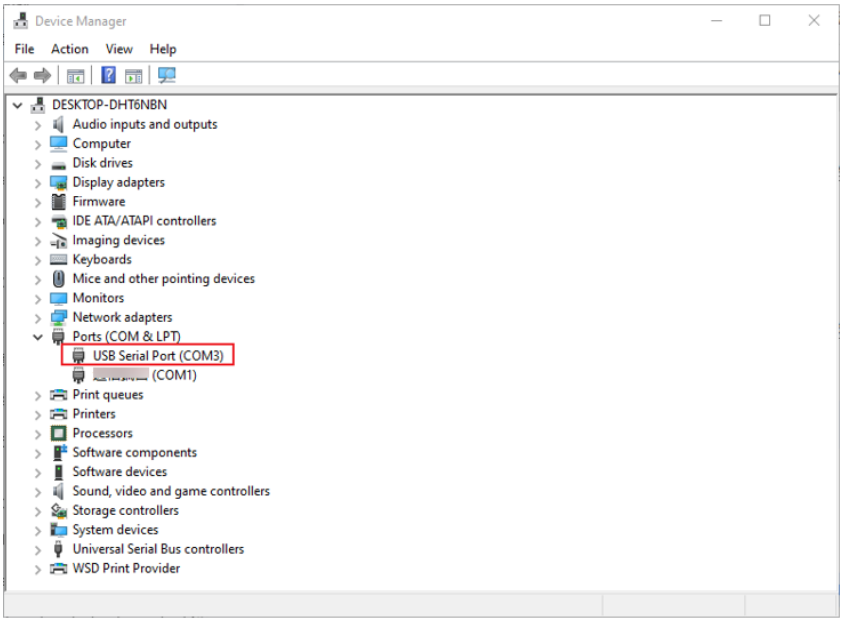
2.4 Debugging the Device (via Console Port)

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

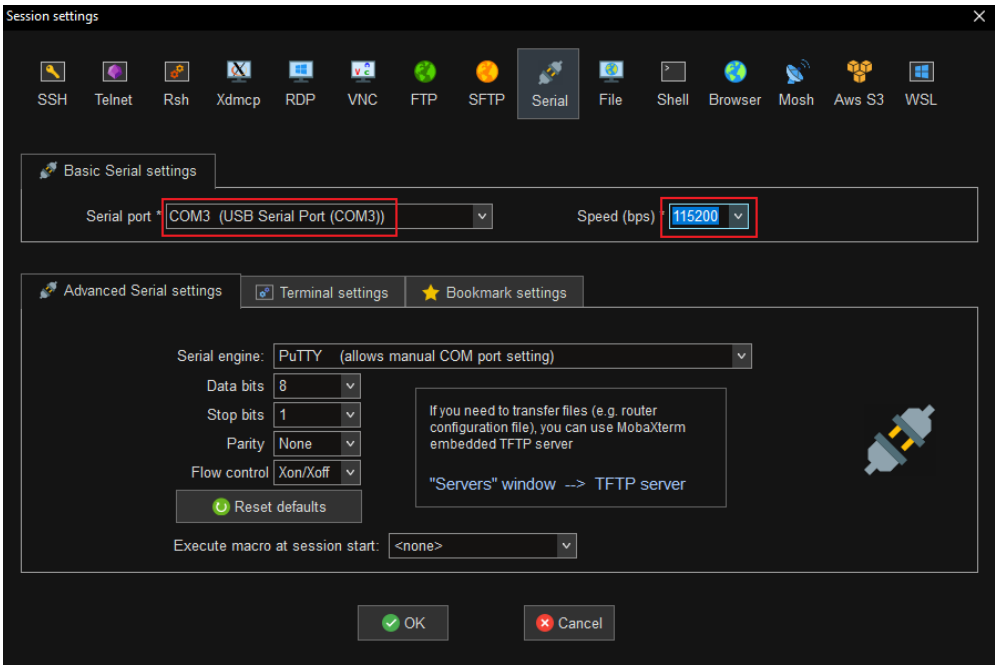
1. Connect the RAH305 to a Windows PC using a USB-to-RJ45 Console cable.



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** and enter the login password in the subsequent window to start the session.

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

2.5 SSH Login

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

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

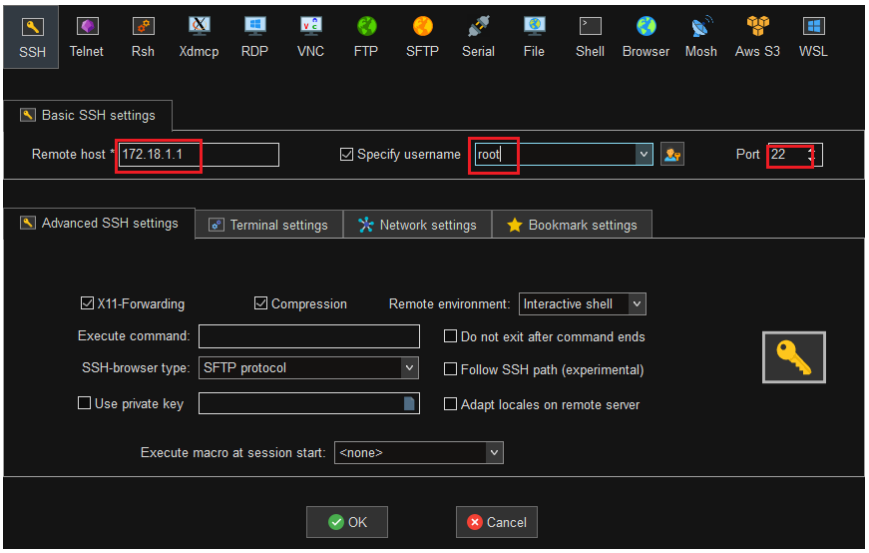
* This option requires WAN-side access, which is disabled by default, as mentioned in Section 2.3.

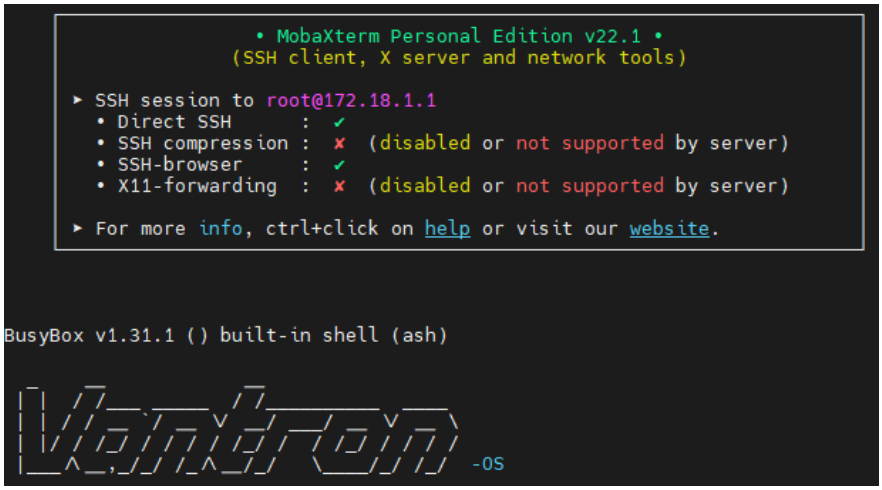
Example: SSH login via **LAN IP**

1. Connect the PC to RAH305's LAN network via Ethernet or Wi-Fi.
2. Install an SSH client if it is not available.
   - **Windows PC**:
     - PuTTY
     - Tera Term
     - MobaXterm
   - **Linux PC**:

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

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





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

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

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

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 procedure:

1. Prepare two RAH305 routers and place them within a suitable short range for pairing.

   *Ensure there is **no** IP conflict between the two units, as Vantron communication devices use **172.18.1.1** as the default LAN IP address.*

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

2. Short press (< 1s) the WPS button on one device to activate WPS connection mode. The WLAN LED blinks at 3Hz when the mode is activated.
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 operates as the **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.

   *Ensure there is **no** IP conflict between the two units, as Vantron communication devices use **172.18.1.1** as the default LAN IP address.*

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

2. Short press (< 1s) the DPP button on the RAH305 to activate DPP pairing mode. The HaLow LED blinks at 3Hz when the mode is activated.
3. Repeat step 2 on the HaLow STA. 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.

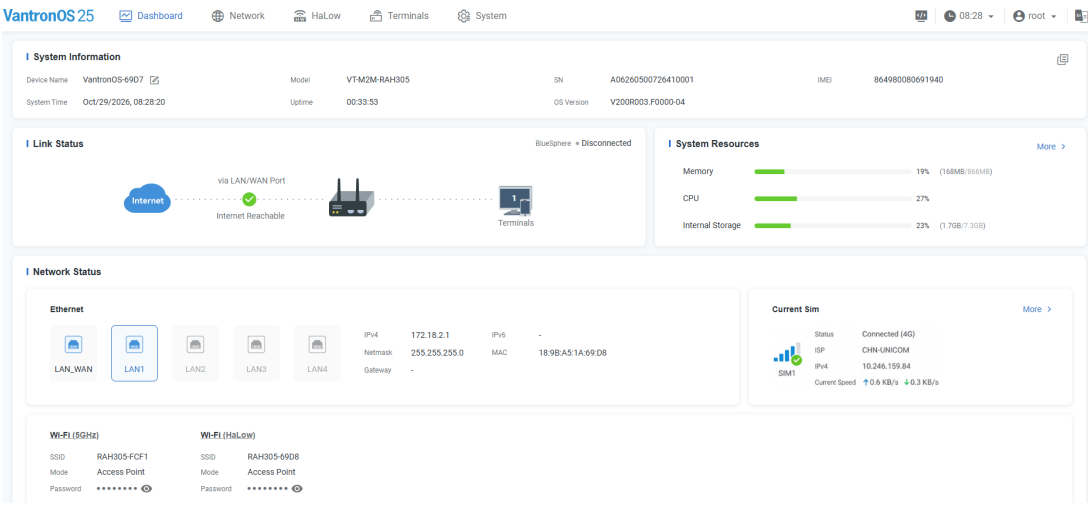
CHAPTER 3 DEVICE SETUP VIA VANTRONOS

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.

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

Terminals: Provides information of connected end nodes.

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

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

Time Settings:

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

Refer to Section 3.6.1.2 for modifying the time settings.

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

- Toggle Edge Computing functionality
- Log out

Language Toggle: English ⇄ Chinese.

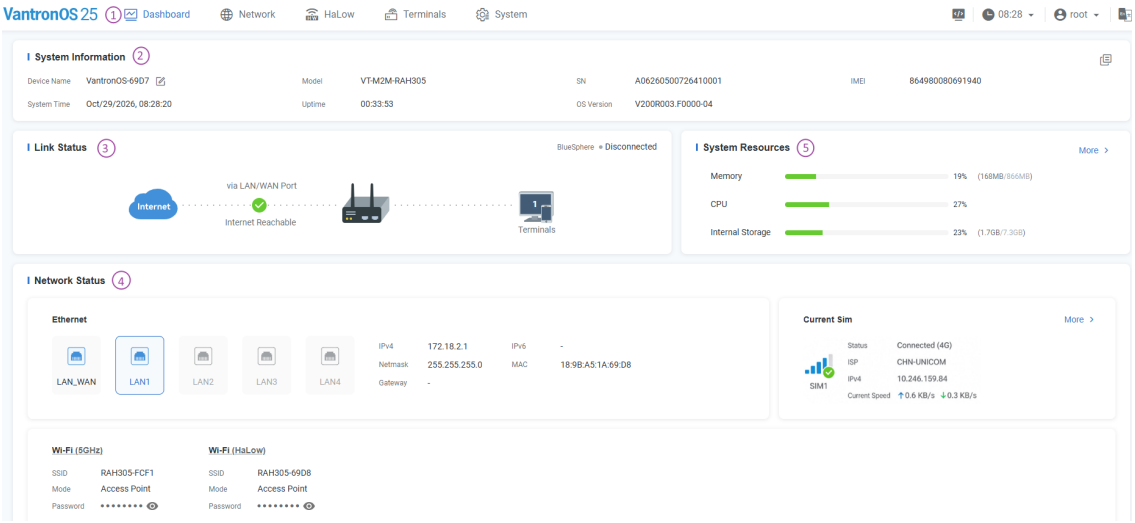
3.1.2 Log Out

To sign out:

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

3.2 Dashboard

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



Description:

1. **Menu Tabs** — Highlights the active menu in blue.
2. **System Information** — Includes the device name, model, SN, IMEI, current system time, system uptime, and OS version.
   - Clicking the pencil icon next to the device name enables device name modification.
   - Clicking the copy icon in the upper-right corner copies all system information.
   - Pressing Ctrl + F12 switches between the baseline OS version and the specific build version.
3. **Link Status** — Shows a simplified network topology of the current device.
   - If the device has Internet connectivity, its access path will be shown (e.g. via WAN).
   - Clicking the count of connected terminals navigates to the end node page, where detailed end node information is displayed.
4. **Network Status** — Displays the live status for each network interface.
   - Ethernet: Active ports are highlighted in blue, with IPv4 and IPv6 addresses, subnet mask, gateway, and MAC address displayed for the selected port.
   - 2.4GHz/5GHz Wi-Fi / Wi-Fi HaLow: Displays device 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 WAN/LAN interface settings, 2.4 GHz Wi-Fi settings, static routing, and more. These features enable precise control over connectivity, ensuring optimal performance and high availability. By integrating these tools, the system reduces administrative overhead and enhances operational efficiency, allowing you to build a resilient, secure, and fully customized network fabric.

Interfaces on the 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

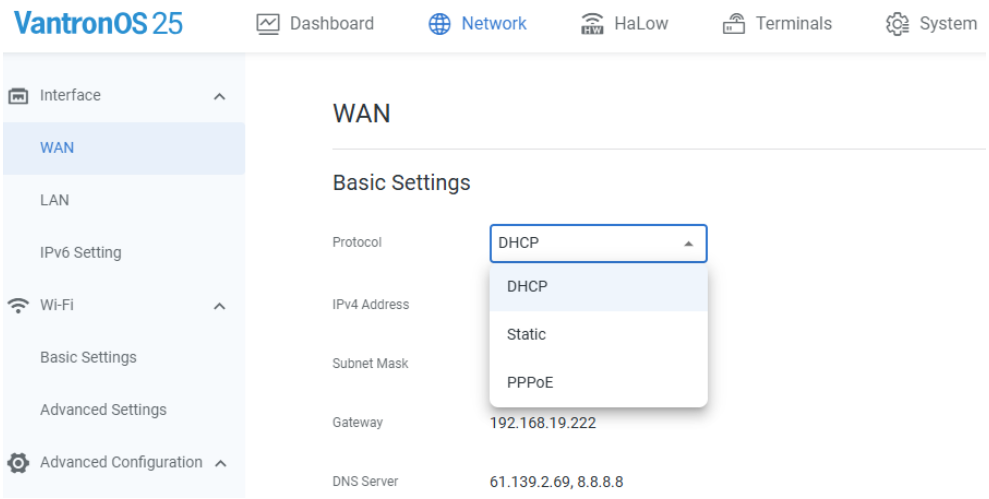
The WAN interface page includes the following three functionalities:

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

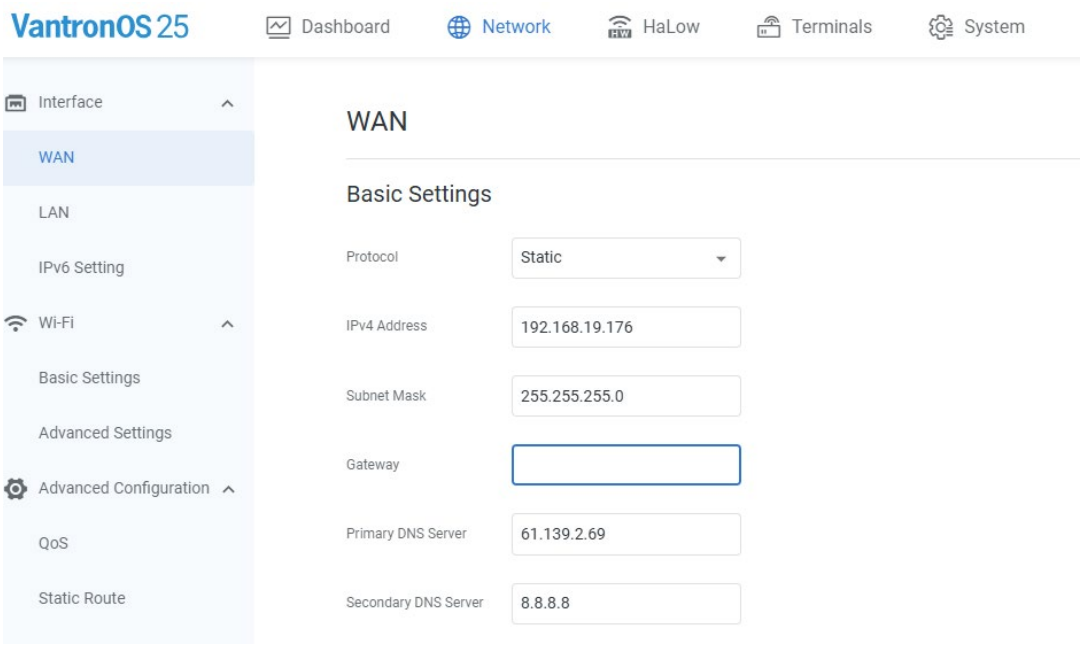
Whenever you make a change, always ensure the host PC and the RAH305 are on the same subnet for smooth VantronOS login.

3.3.1.1 Basic IP Configuration

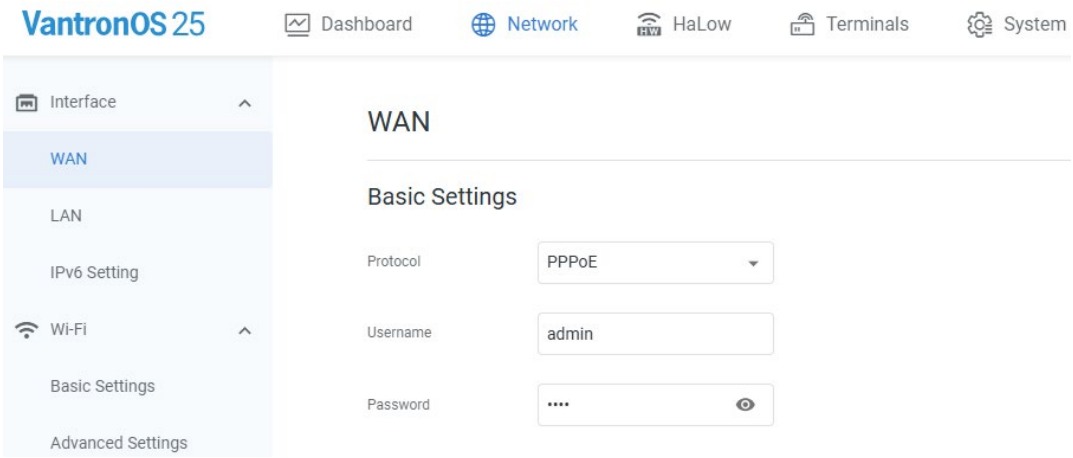
DHCP: The WAN interface obtains its IP address **automatically** from an upstream DHCP server.



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



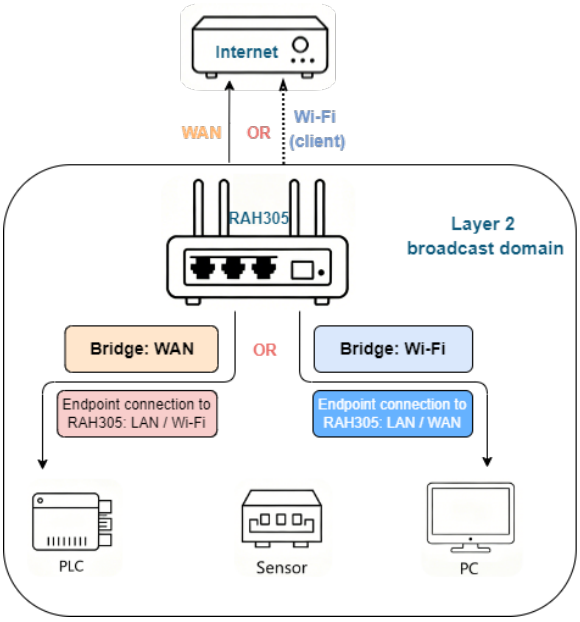
PPPoE (Point-to-Point Protocol over Ethernet): The device initiates a dial-up connection to the ISP using a username and password encapsulated in PPP over Ethernet. The ISP then provides dynamic or static IP configuration.



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

3.3.1.2 Interface Bridging

Interface bridging on the RAH305 removes WAN/LAN zone separation, placing all interfaces into the same Layer 2 bridge for transparent forwarding. After bridging, IP addressing is centrally managed by an accessible upstream DHCP server. You may select either the Wi-Fi STA interface or the Ethernet WAN interface for bridging; the selected interface acts as the uplink to reach the DHCP server.



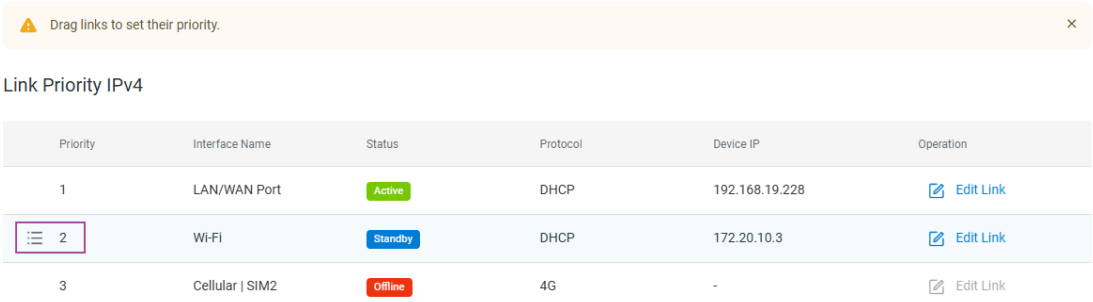
- After bridging is enabled, LAN interfaces **no longer** provide NAT and DHCP services to connected endpoints.
- When you bridge either the Ethernet WAN or Wi-Fi STA interface, the selected interface becomes the uplink. All other interfaces are moved into the same Layer 2 bridge, leaving the device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

3.3.1.3 Link Priority

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

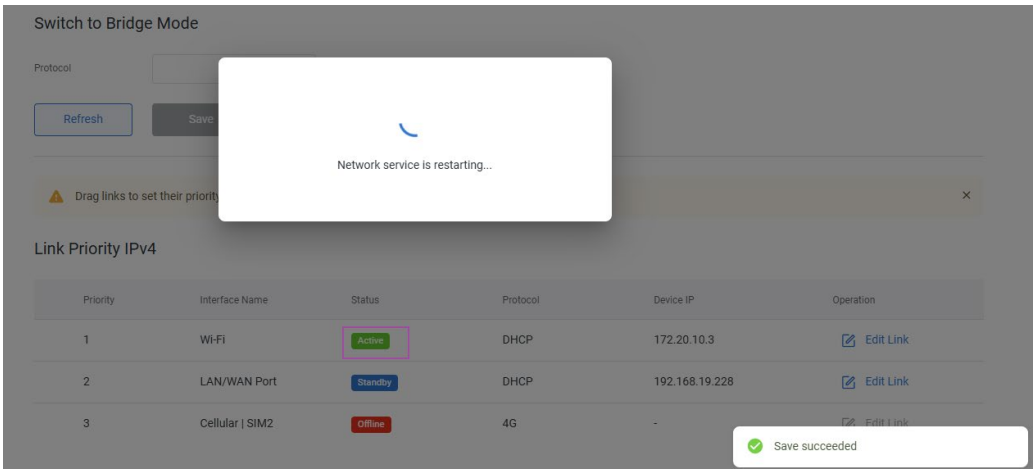
To manually set the network priority:

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



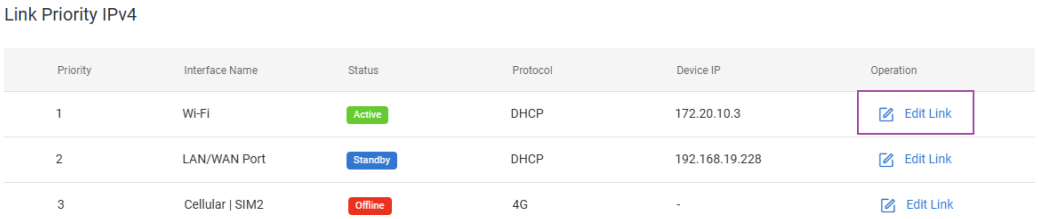
*If the Cellular link is shown **Offline** after SIM card insertion, verify that the matching SIM card profile is **enabled** on the cellular configuration page.*

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



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

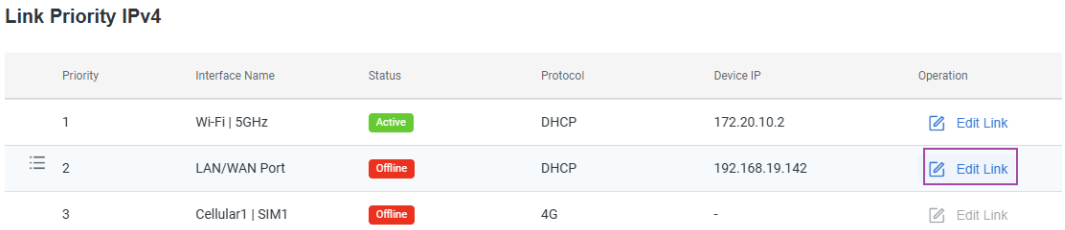
3. Use the **Edit Link** option to modify the probe settings for the link as needed.



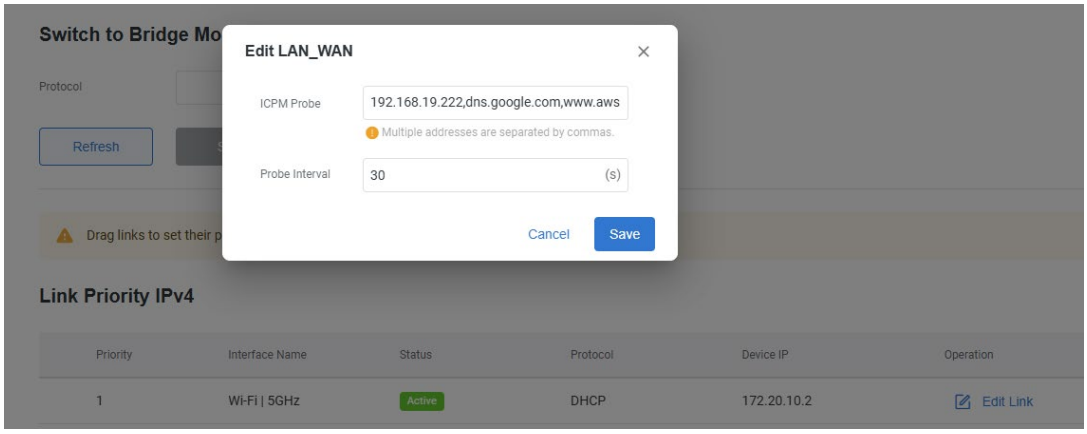
3.3.1.4 Link Diagnosis

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

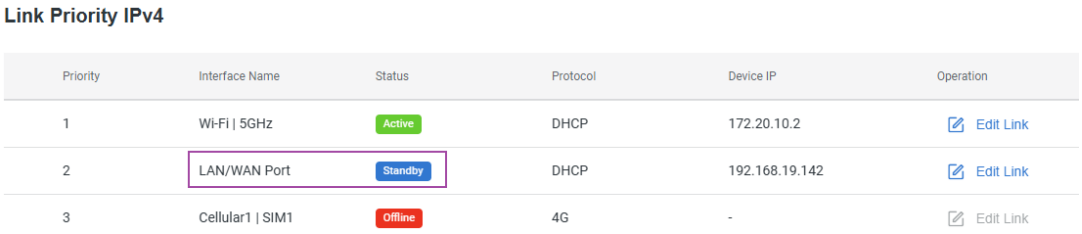
1. Locate the target link, and click **Edit Link**.



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

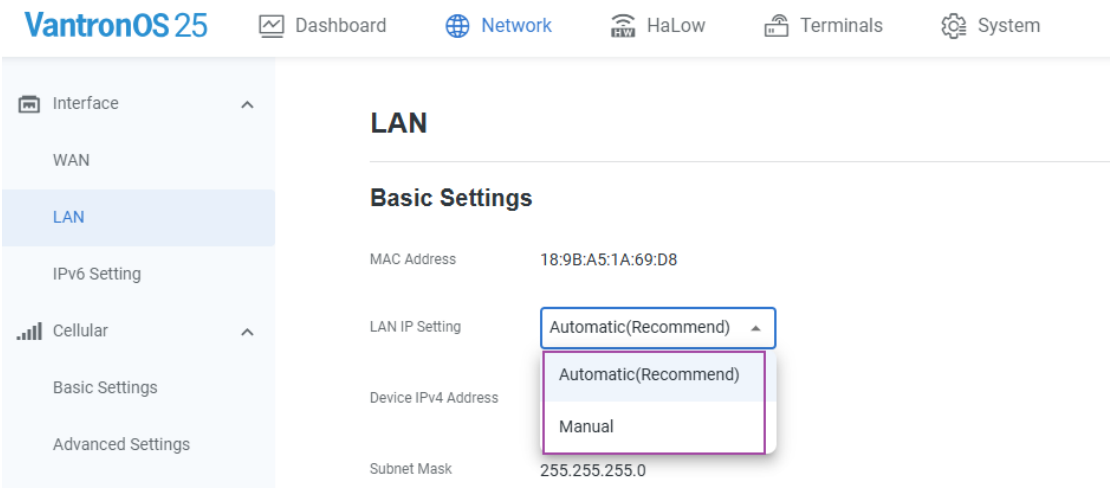


3. Check the link status to verify if it becomes reachable.



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) 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. Enabling or disabling DHCP Service takes effect after the changes are saved.

Editable fields under **DHCP Service**:

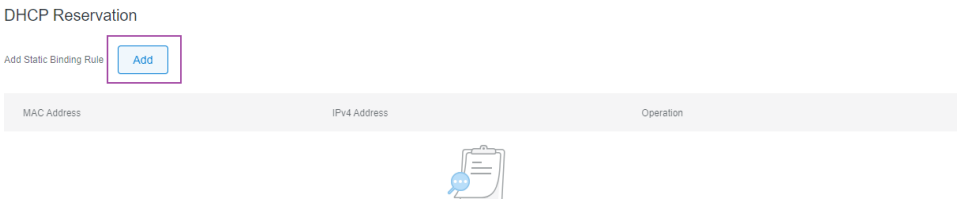
- Start & End addresses: IP addresses within this range are leased to clients.
- Lease Time: The valid duration for which the RAH305, as the DHCP server, assigns an IP address to a client. Before expiry of the lease time, the client will send a renew request to the RAH305 to extend the lease. If the renewal fails and the lease expires, the client must release this IP address and initiate a new DHCP discovery.

DHCP 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.

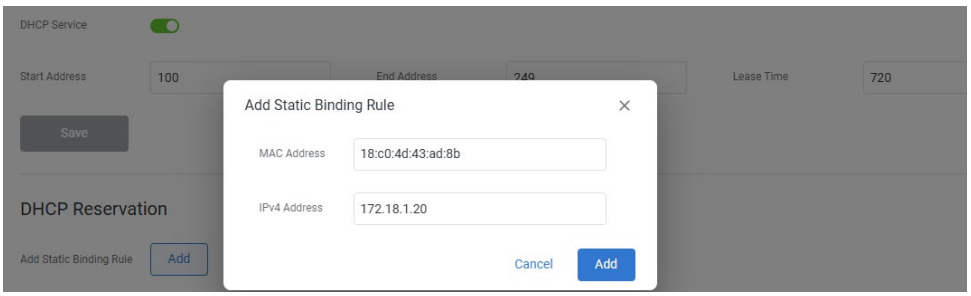
By adding a DHCP reservation rule to the RAH305, the specified client device will maintain the allocated IP address to reduce configuration errors.

Steps of adding a DHCP reservation rule:

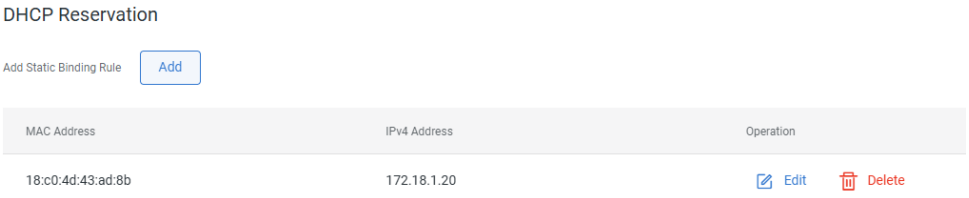
1. Click **Add** under **DHCP Reservation**.



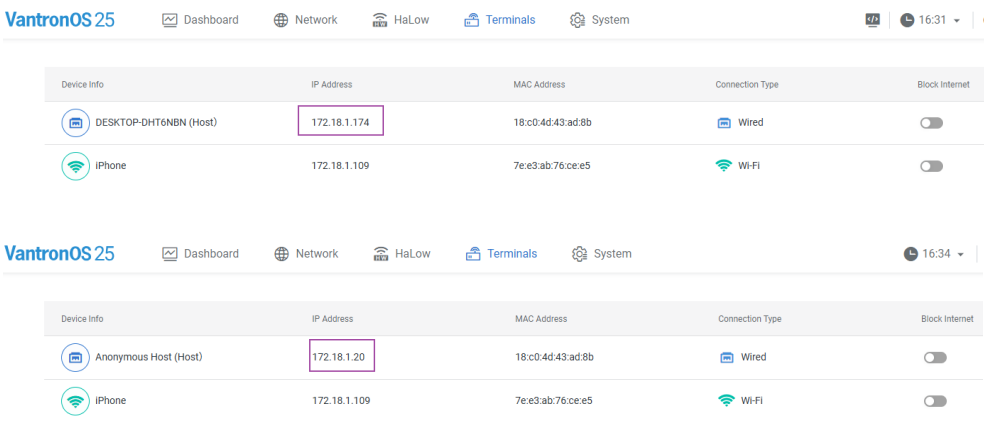
2. Enter the client's MAC address and allocate an IP on the same subnet as the RAH305.



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



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



3.3.3 IPv6 Settings

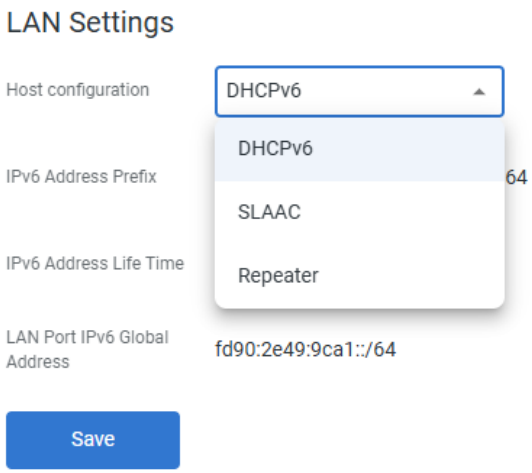
IPv6 (Internet Protocol version 6) is an advanced network layer protocol succeeding IPv4. It is designed to solve IPv4 address exhaustion and support enhanced networking features. It provides 128-bit addresses, eliminating the need for NAT and enabling end-to-end connectivity.

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

When IPv6 is enabled:

- The **WAN** interface defaults to DHCPv6 to automatically obtain an IPv6 address from the upstream network, requiring no manual input.
- The **LAN** interface defaults to DHCPv6 for address assignment, using a default IPv6 prefix and address lifetime that can be customized as needed.

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



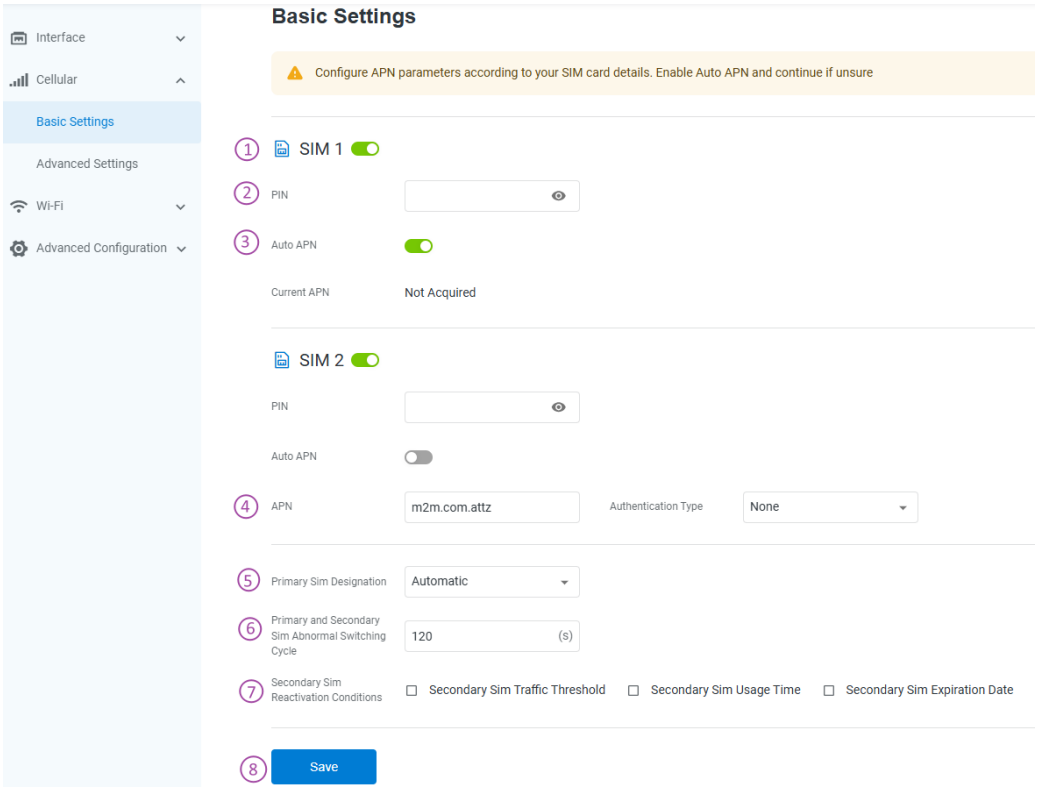
- **DHCPv6**: The RAH305 acts as a stateful DHCPv6 server, assigning full IPv6 addresses to LAN devices with configurable prefix and lease time.
- **SLAAC:** The RAH305 advertises an IPv6 prefix via RA messages. LAN devices automatically generate their own addresses for plug-and-play use.
- **Repeater:** 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.



Description:

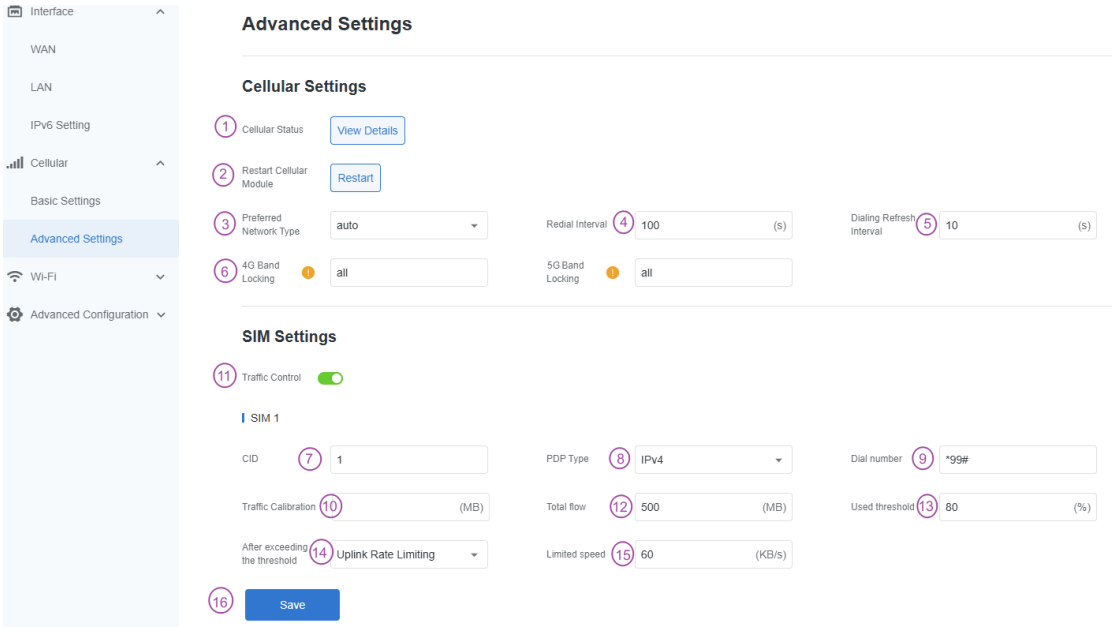
1. Before configuration, insert an activated SIM card into a Micro SIM slot and enable the corresponding SIM.
2. Leave the PIN code blank unless your carrier enables PIN verification after activation.
3. The APN and authentication type are provided by the carrier; if you are unsure about them, enable **Auto APN**.
4. Alternatively, you can enter the carrier parameters manually.

When two SIM cards are inserted, the following options are available:

5. Designate the primary SIM card. If **Automatic** is selected, the card with stronger signal will be used as the primary.

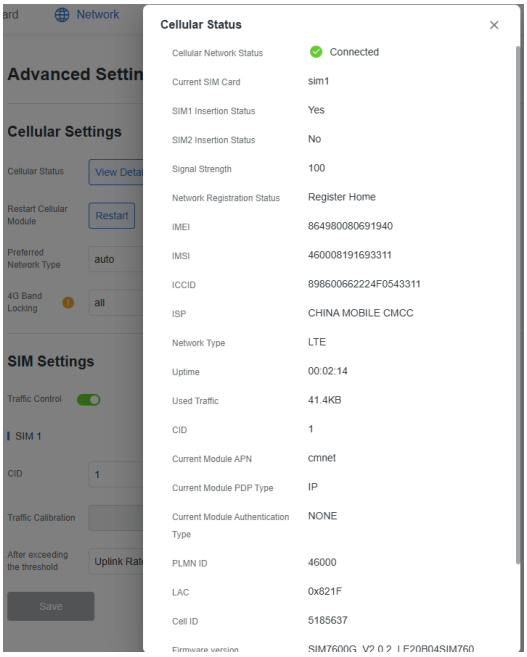
6. Enter a time interval for SIM failover when an anomaly is detected on the current SIM card.
7. Set the thresholds (e.g., traffic or time) that trigger a switch back from the secondary SIM to the primary SIM.
8. Save the changes to apply them.

3.3.4.2 Advanced Settings



Description:

1. Cellular status — Clicking **View Details** displays the detailed cellular information of the device, including network status, active SIM card, uptime, data usage, signal strength, module information, etc.



2. Cellular module restart — Manually restarts the cellular module.
3. Preferred network type — Selects a preferred network type for the module.
   - Auto: The module automatically selects the best available network.
   - LTE: Forces the module to register only on 4G LTE networks.
4. Redial interval — The module redials at the specified interval in case of a connection failure (in seconds).
5. Dialing refresh interval — Specifies the interval (in seconds) to refresh the last dial-up status.
6. 4G/5G Band Locking — Specifies the 4G/5G bands for the module to use. Keep the default "all" to retain all available bands.

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

7. CID value — Cell identity.
8. PDP type — Packet data protocol type.
9. Dial number — *99# for general use.
10. Traffic Calibration — After dial-up, enter a valid value (in MB) as the starting traffic for calculating data consumption on the selected SIM. The **Used Traffic** field under **Cellular Status** shows this calibrated reading.
11. Traffic Control — Enable this feature to manage data consumption for the selected SIM, then configure its parameters in the subsequent fields.
12. Total flow — Sets the maximum data usage (in MB) for the selected SIM.
13. Used threshold — Defines a data usage percentage (in %) that triggers a restriction action when exceeded.
14. Restriction action — Choose to either restrict data speed or cut off the link when exceeding the limit.
15. If uplink rate limit is selected, enter a speed limit (in KB/s) to control data rate.
16. If you have made any changes, click **Save** to apply.

    Leave the field as-is if not applicable or unsure. In the screenshot example, upon reaching 80% of the preset total flow (500MB), the system will limit the data rate to 60 KB/s.

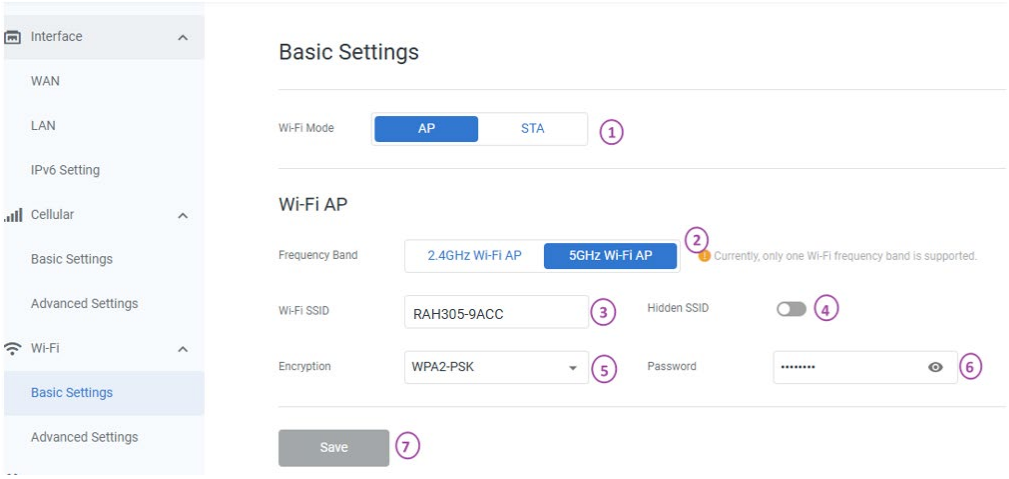
3.3.5 Wi-Fi

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 them 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 on the **Basic Settings** page.

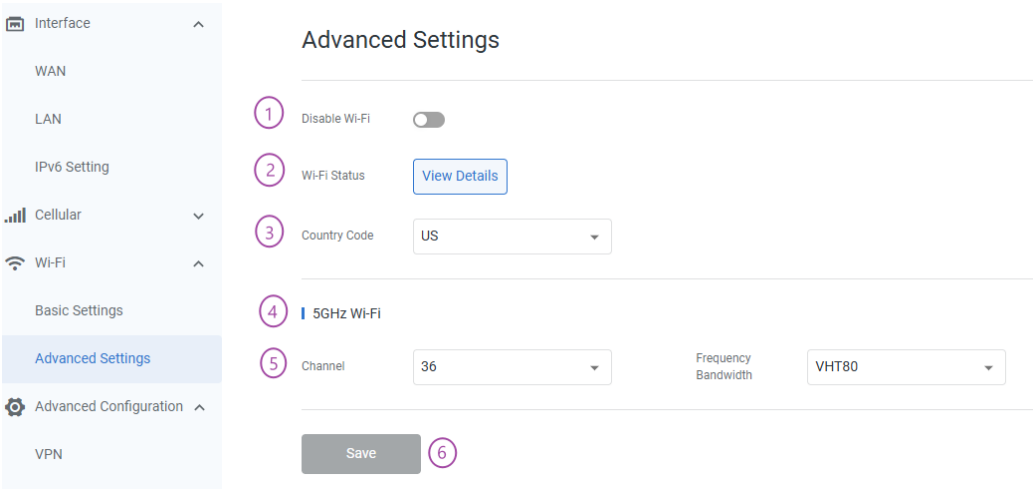
3.3.5.1 AP-Mode Basic Settings



Description:

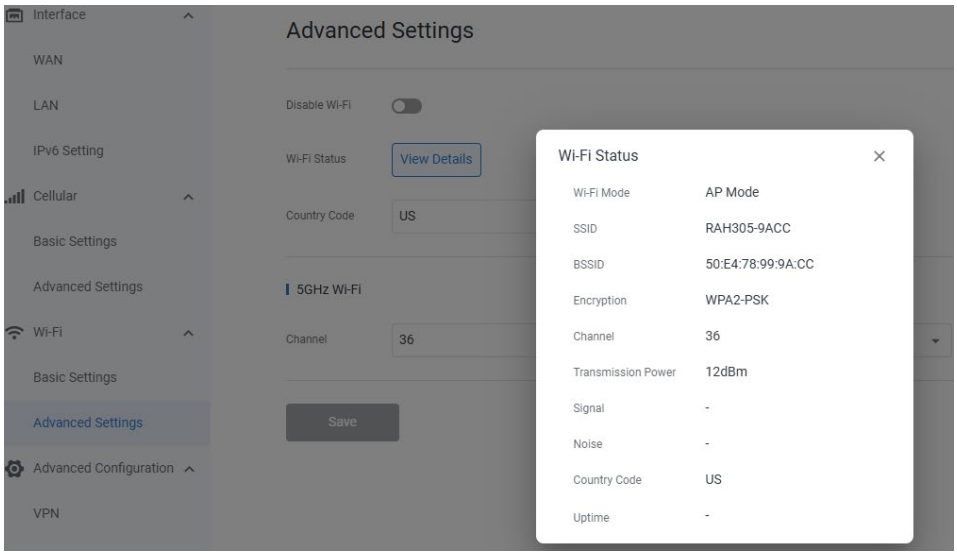
1. The device is factory set to operate in **AP** mode, and you can switch the mode here.
2. The RAH305 supports dual-band Wi-Fi operation. Both bands are configurable, but only the selected band will be active. You are recommended to select the device's Wi-Fi operating band according to on-site deployment requirements.
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 — The password for connecting the device's Wi-Fi.
7. Click **Save** to allow changes to take effect.

3.3.5.2 AP-Mode Advanced Settings



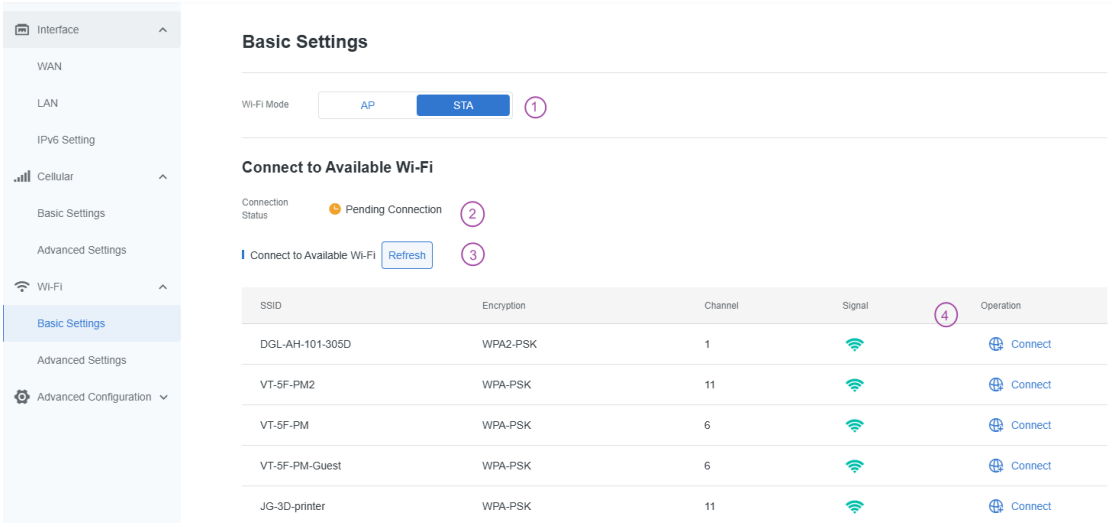
Description:

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



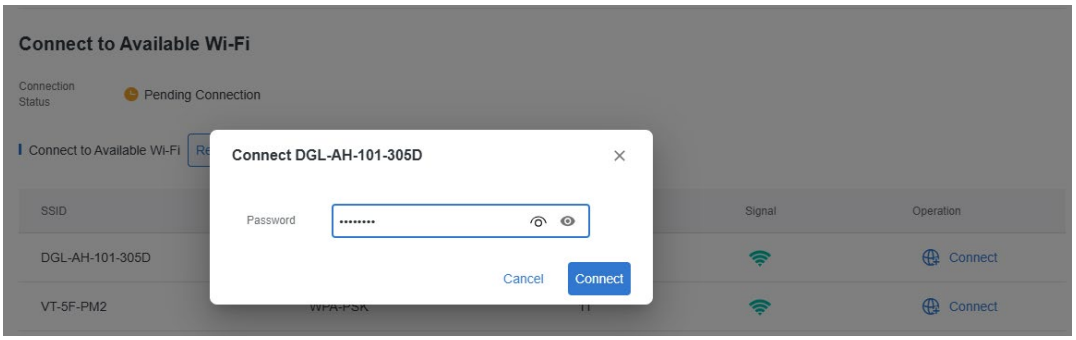
3. Country code (only ‘US’ supported).
4. The currently active band matches the selection made on the **Basic Settings** page.
5. Channel options (configurable) and default frequency bandwidth.
6. Click **Save** to allow changes to take effect.

3.3.5.3 STA-Mode Basic Settings

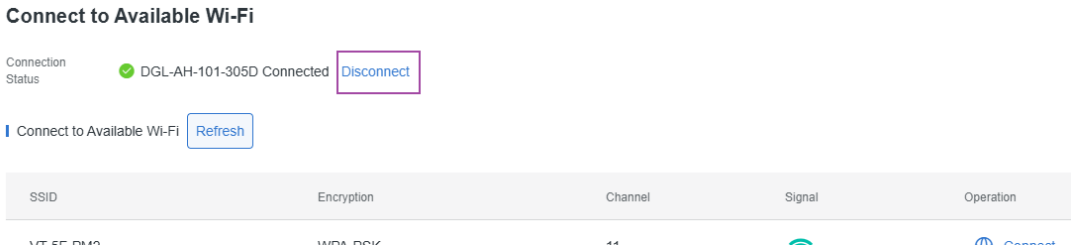


Description:

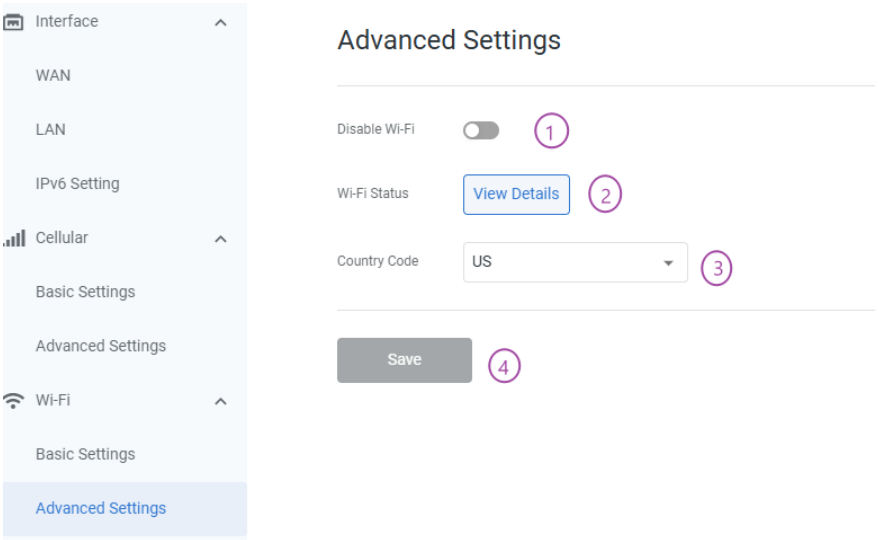
1. Click **STA** and confirm the action in the pop-up to enable the Client mode.
2. Current Wi-Fi connection status.
3. If the target SSID is not included in the list, click the button to refresh the list.
4. Information of available Wi-Fi APs is displayed. Click **Connect** and enter the password to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



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

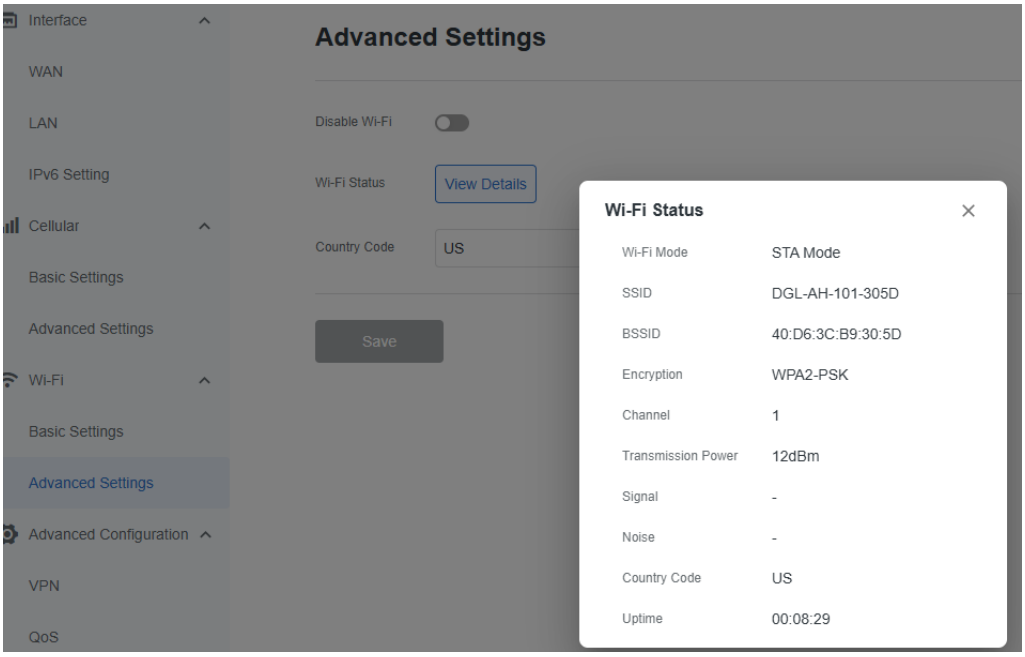


3.3.5.4 STA-Mode Advanced Settings



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. Click **Save** to allow changes to take effect.

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 your actual deployment scenario. If you are using two Vantron communication devices for the connection, make sure there is no IP address conflict when they are on the same LAN.

When preparing OpenVPN configuration files, you can download the templates from the VantronOS and modify them as needed.

3.3.6.2 OpenVPN Server Setup

In a server-side VPN deployment, clients access the internal network through the RAH305, which functions as the VPN server. Modify the following directives in the OpenVPN server configuration file.

TUN mode

- **port:** Specifies the server's listening port (e.g., 1194).
- **dev tun:** Enables a Layer 3 routed tunnel.
- **push "route…":** Specifies the internal network subnet to be pushed to VPN clients.
- **push "dhcp-option DNS…":** Specifies the internal DNS server IP address.
- **server:** Defines the virtual IP address pool for VPN clients.

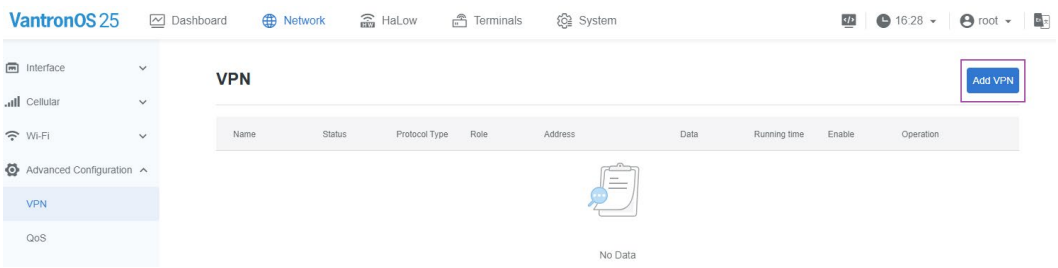
TAP mode

- **port:** Specifies the server listening port (e.g., 1194).
- **dev tap**: Enables a Layer 2 Ethernet bridge tunnel.
- **ifconfig:** Specifies the virtual IP address and subnet mask for the server TAP endpoint.
- **ifconfig-pool:** Defines the start and end virtual IP range for client assignment.

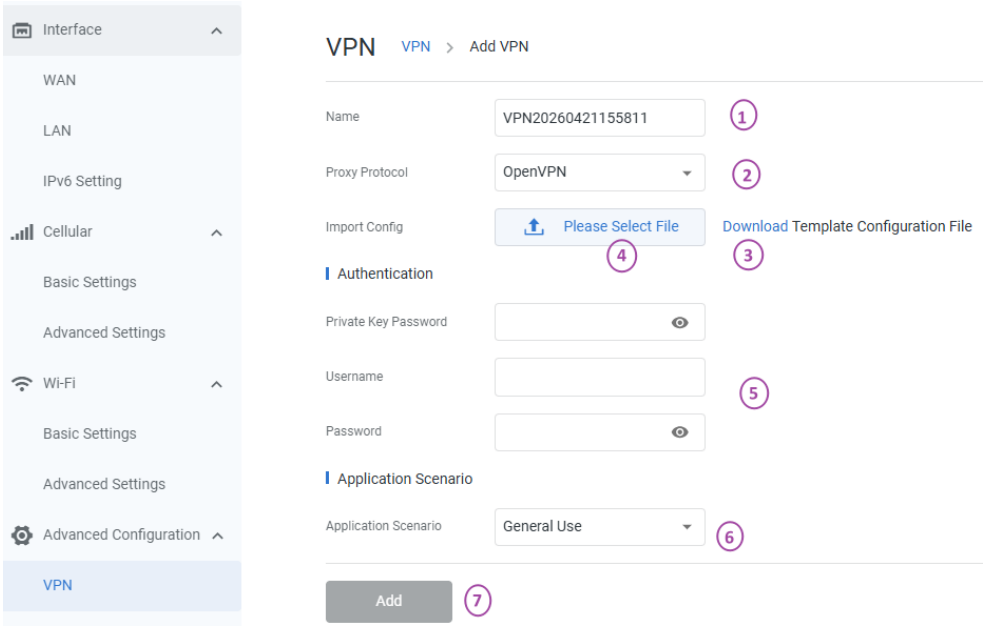
Note: The provided configuration templates are for testing only. We recommend that you replace the certificates and keys in the configuration file with your own.

To add an OpenVPN **Server** rule for the RAH305:

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



3. Configure the OpenVPN server parameters on the configuration page:

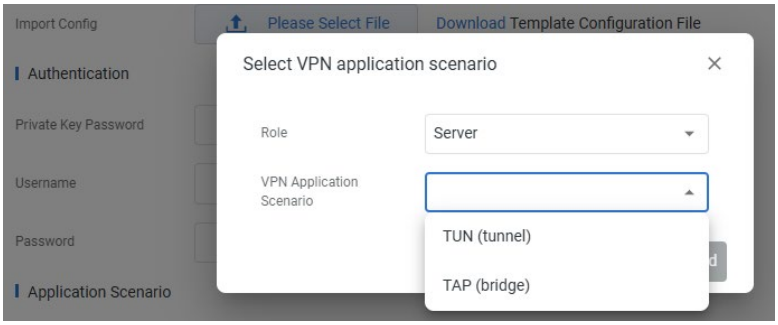


Description:

1) Enter a VPN rule name (the 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)



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

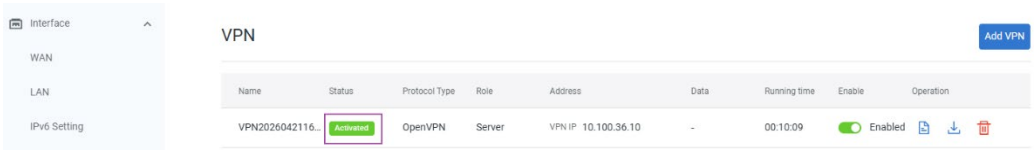
5) Set the authentication credentials, if necessary.

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 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

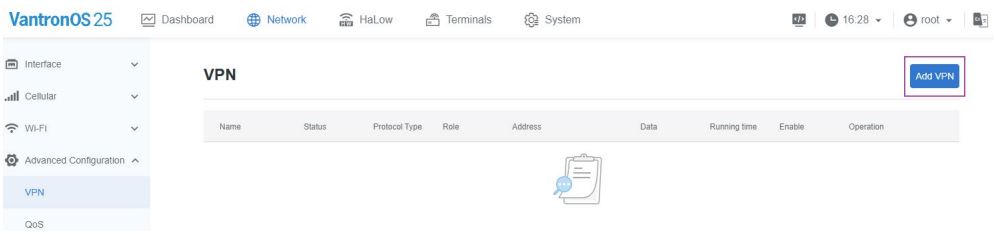
In a client-side VPN deployment, the RAH305 acts as the VPN client and connects to a remote OpenVPN server to access the remote internal network. Its configuration must match the server's connection parameters. In particular:

- **dev**: Must match the server's tunnel mode (tun or tap).
- **proto**: Must match the server's protocol (tcp-client for tcp-server, udp for udp).
- **remote:** The server's address, set as follows:
  - If the server has a public IP address: Use the server's public IP.
  - If the server uses DDNS: Use the DDNS domain name (e.g., vpn.example.com).
  - If the server is behind NAT (port forwarding): Use the public IP or DDNS of the front-end gateway.
  - If both the server and client are on the same LAN: Use the server's local LAN IP address.
- **port:** Must match the server's listening port.

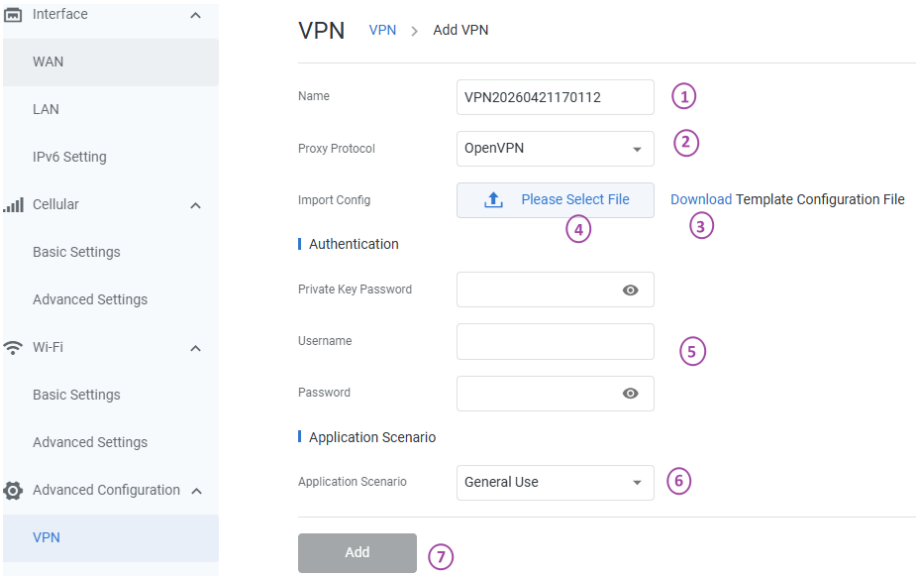
Note: The provided configuration templates are for testing only. We recommend that you replace the certificates and keys in the configuration file with your own.

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

1. Synchronize 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**.

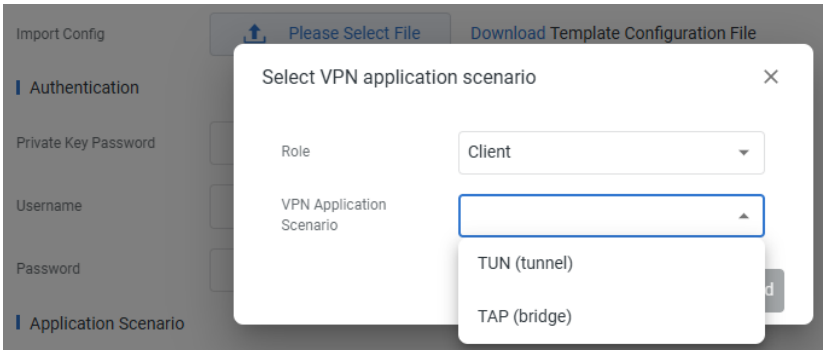


3. Configure the OpenVPN client parameters on the configuration page:



Description:

1) Enter a VPN rule name (the 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)



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

5) Set the authentication credentials, if necessary.

6) Select an application scenario.

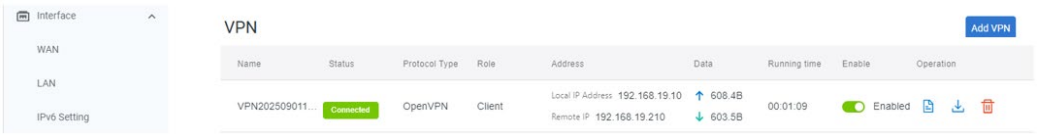
Refer to Section 3.3.6.4 for details on the application scenarios.

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

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

*If the status shows **Disconnected**, verify your configuration and resolve conflicts with other rules; recreate the rule if necessary.*

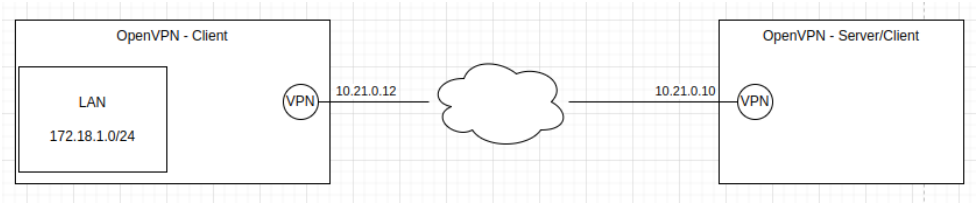
5. When the status changes to **Connected**, the device successfully establishes a connection with a server.



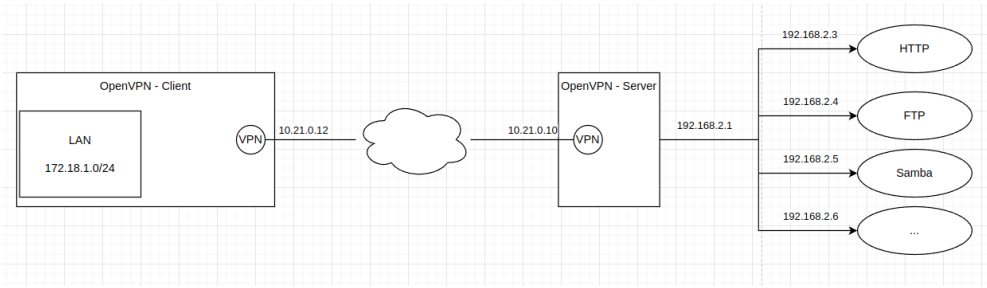
After setup, you can enable/disable the rule, view its logs (useful for troubleshooting if the rule fails to activate), download the configuration file, or delete it.

3.3.6.4 Application Scenario Topology

- General Use (point-to-point)

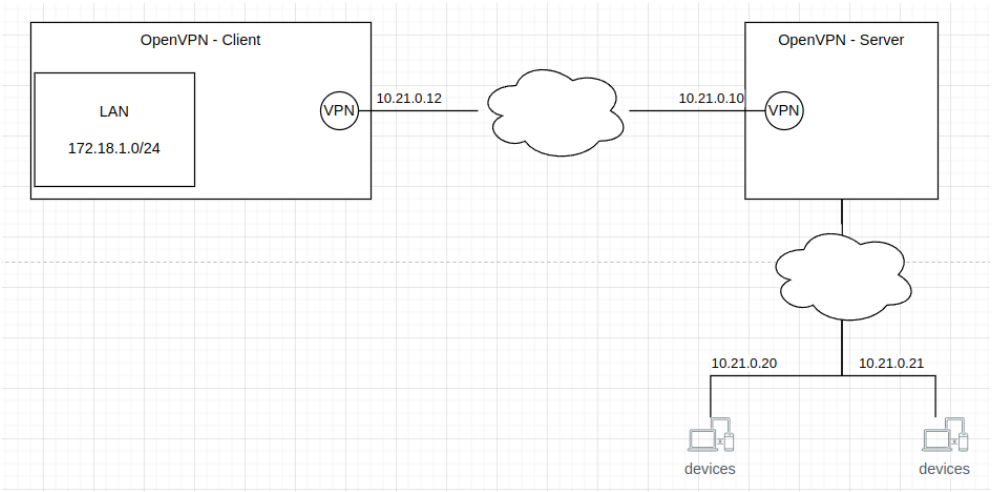


- Routing Mode (client-to-network)



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

- DNAT Port Forwarding (client-to-clients)

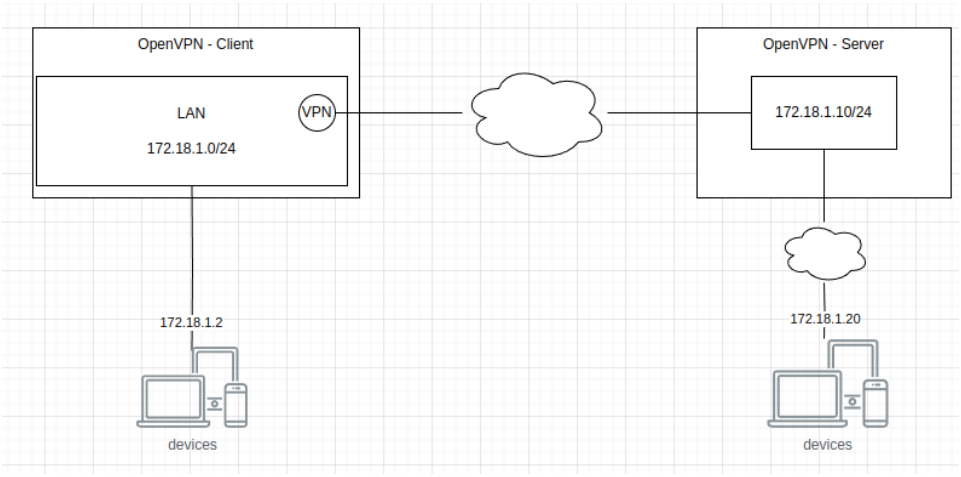


In this scenario, the OpenVPN client is assigned an IP: 10.21.0.12, on the same subnet as the remote devices (10.21.0.20 & 10.21.0.21). So, they can communicate with each other.

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

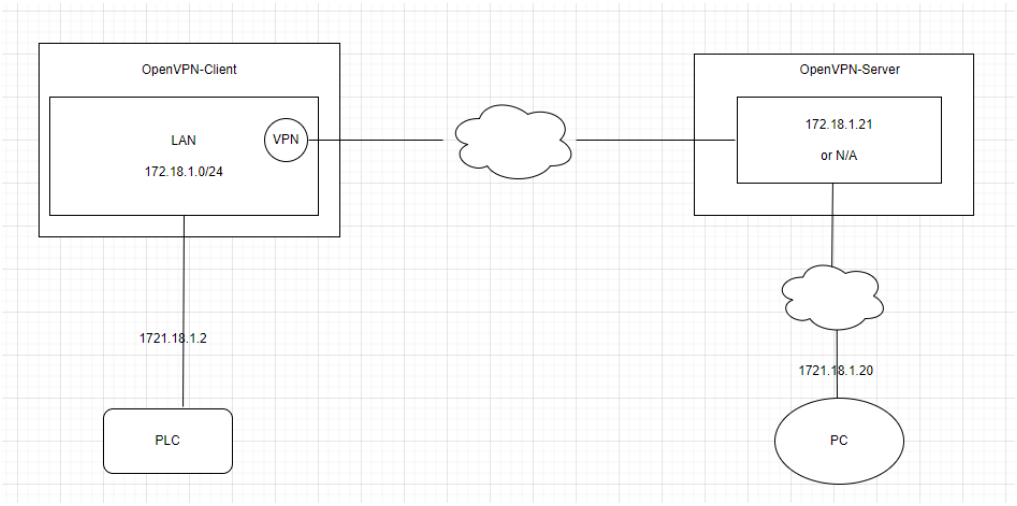
- Bridging Mode (clients-to-clients)

Option 1: IP addresses are assigned by the OpenVPN server



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

Option 2: IP addresses are assigned by the OpenVPN client



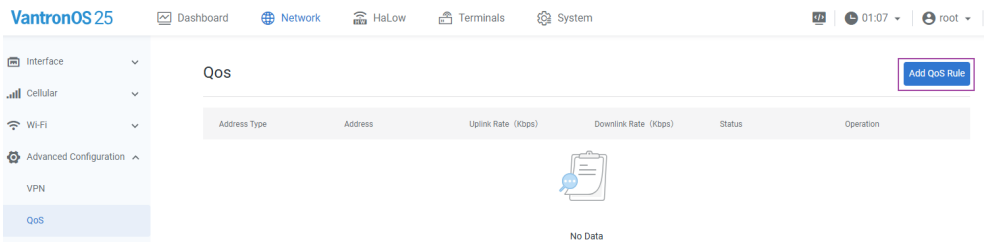
In this scenario, (a) OpenVPN client is customized; (b) DHCP should be started after VPN connection is established or a static IP is added to the VPN interface after the connection is established.

3.3.7 QoS Bandwidth Control

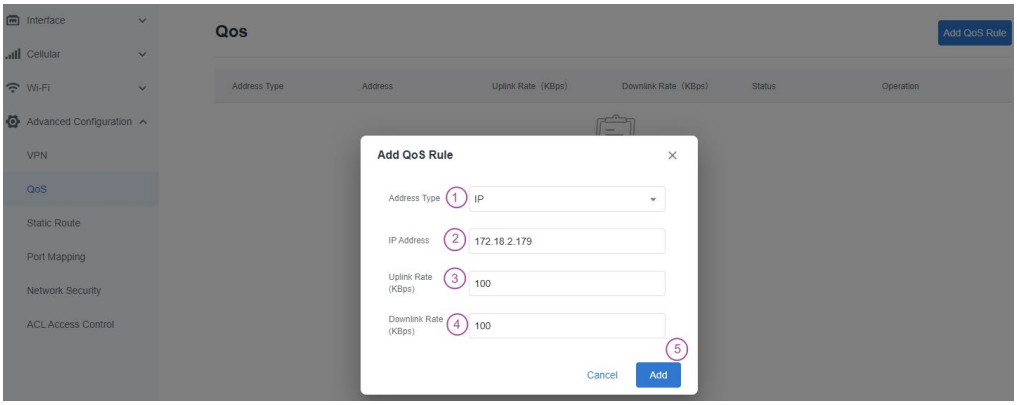
The QoS feature provides fine-grained bandwidth shaping rules to limit uplink and downlink traffic of designated terminals, preventing bandwidth preemption and stabilizing industrial communication quality.

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.

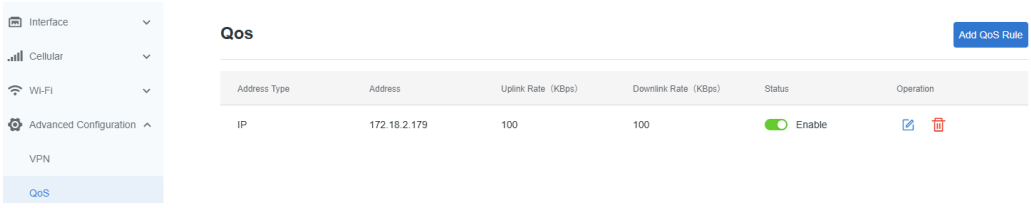
- **IP:** Apply rate limits to a single specified IPv4 device. Ideal for precise bandwidth control of key equipment such as PLCs and industrial controllers.
- **IP Range:** Restrict traffic for a continuous segment of IP subnet, enabling batch bandwidth control for groups of sensors or surveillance cameras.
- **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.



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.

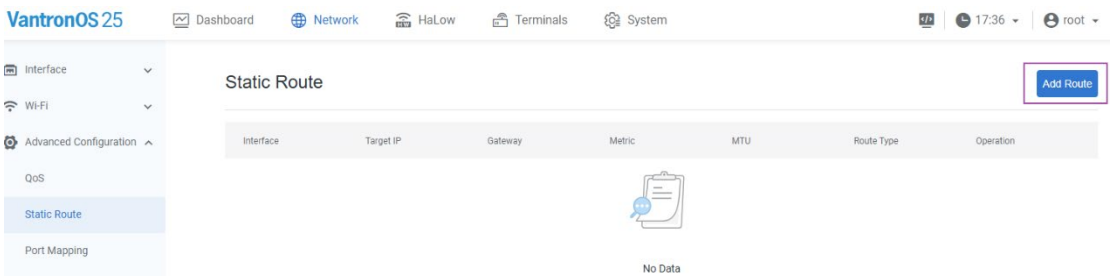
Example:

Goal: Allow HaLow stations on the RAH305's LAN side (172.18.1.0/24) to reach an internal server (192.168.0.0/16) located behind the upstream router.

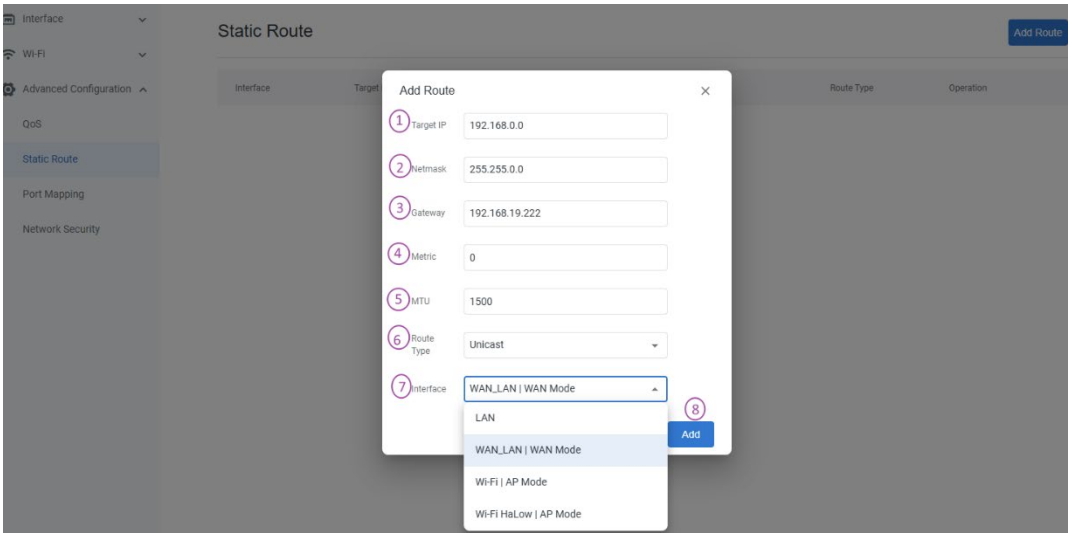
Topology: HaLow Stations (172.18.1.x) -> HaLow AP (LAN: 172.18.1.1, WAN: 192.168.19.176) -> Upstream router (Gateway: 192.168.19.222) -> internal network server (192.168.0.0/16).

Steps:

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



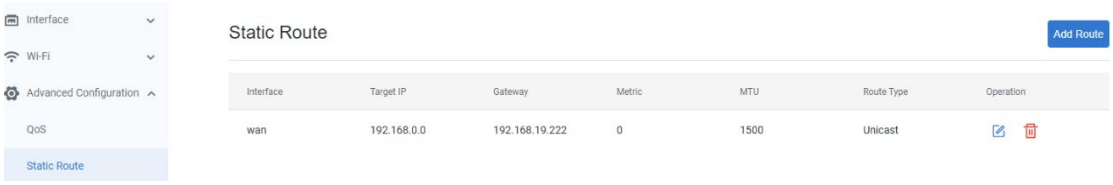
4. Configure the parameters for the route:



Description:

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

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



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

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

Description of the route type:

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

3.3.9 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:

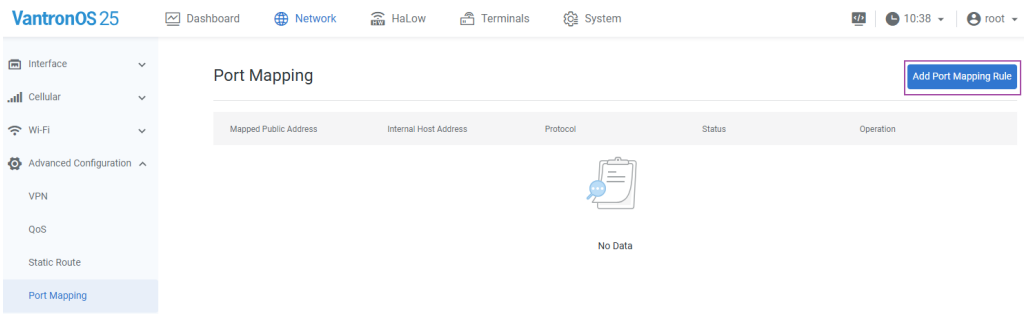
Scenario:

- 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.

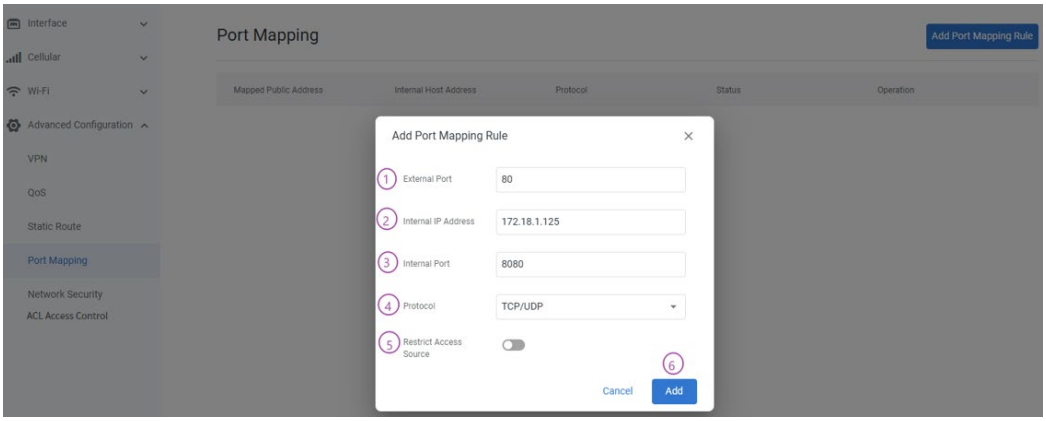
Goal:

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

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



2. Fill in the rule information.



Description:

1) External port — The port number on the WAN side that outsiders will use to connect (e.g., 80).

2) Internal IP — The IP address of the target host (the internal device that provides the actual service).

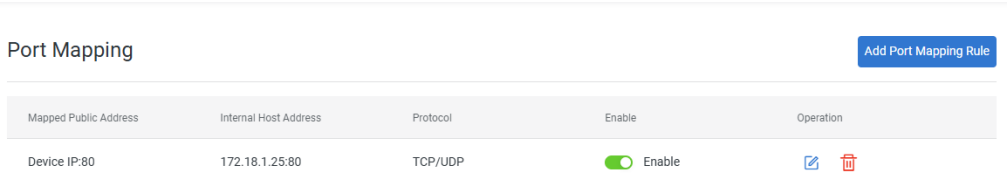
3) Internal port — The port the target host is actually listening for the service (e.g., 8080).

4) Protocol — The protocol used by the service (TCP / UDP / both).

5) When **Restrict Access Source** is enabled, only the source IP with corresponding port and MAC you listed are allowed to reach the forwarded port. If **Restrict Access Source** is disabled, any public IP can access the device's IP and forward it to the internal IP.

6) Click **Add** to finish the configuration.

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

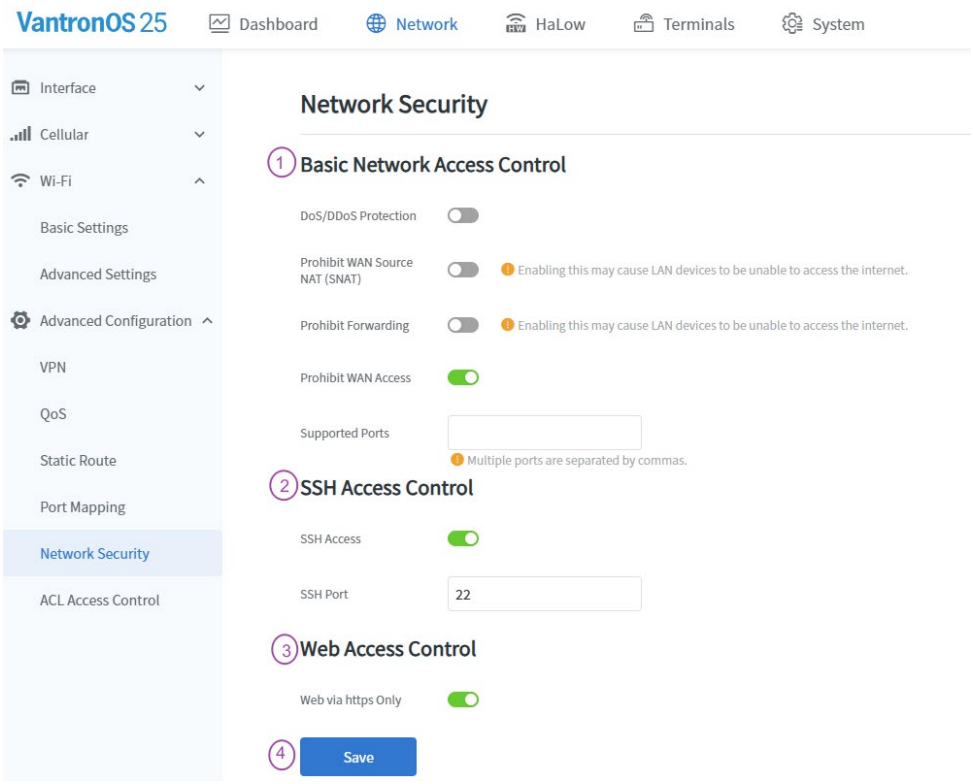


Note: *The mapped public address is determined by your WAN connection and may change.*

7. 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

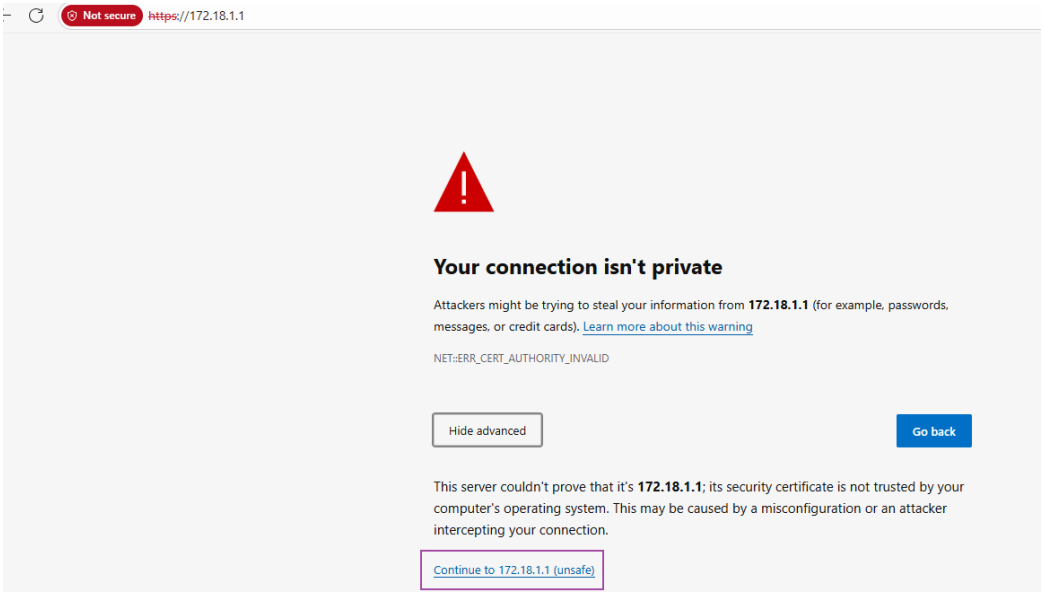
The **Network Security** page provides comprehensive security policy configuration capabilities, enabling granular control over network access behaviors to minimize attack surfaces and enhance overall network protection levels for connected devices.



Description:

1. Basic Network Access Control — Defines the options to control network access.
   - DoS/DDoS Protection: When this option is enabled, it protects the RAH305 and internal devices against DoS and DDoS flood attacks.
   - Prohibit WAN Source NAT (SNAT): When this option is enabled, SNAT for inbound WAN traffic is disabled. This may prevent LAN devices from accessing the internet.
   - Prohibit Forwarding: When this option is enabled, packet forwarding between network interfaces is blocked. This may prevent LAN devices from accessing the internet.
   - Prohibit WAN Access: This option is enabled by default, so users cannot access the gateway's local services from the WAN side. **WAN-side device management is disabled unless this option is turned off.**
   - Supported Ports: You can specify exception ports for WAN access to the device when **Prohibit WAN Access** is enabled. Separate multiple ports with commas.
2. SSH access is enabled by default with 22 as the default SSH port. You can disable it for security concern.

   Refer to Section 2.5 for the login method.
3. Web via HTTPS Only — When this option is enabled, VantronOS accepts logins only over HTTPS. When visiting the HTTPS web UI, a browser privacy warning may pop up. In this case, click **Advanced** → **Continue** to proceed.



4. Click **Save** to allow changes to take effect.

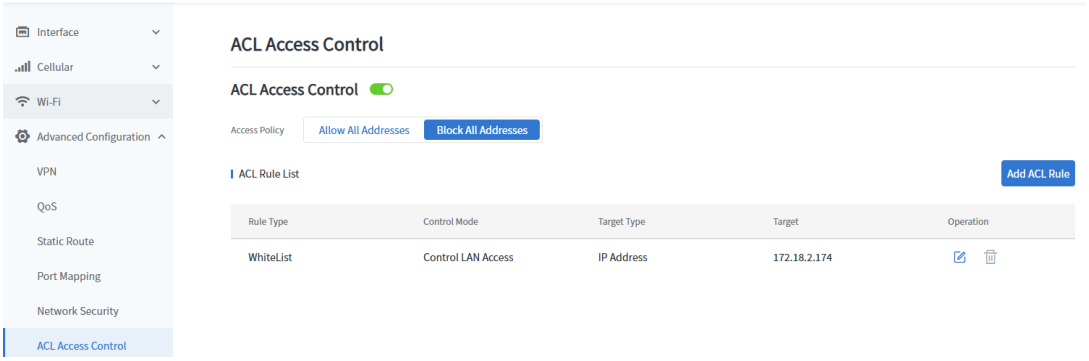
3.3.11 ACL Access Control

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

3.3.11.1 No-Rule Access Policy

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

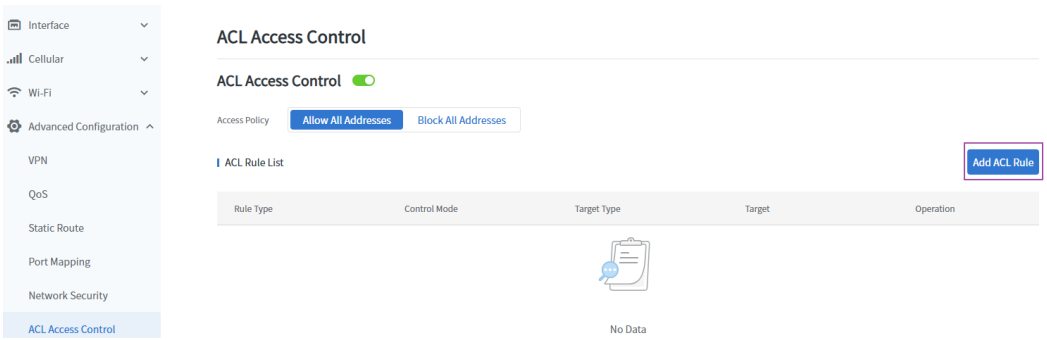
Block all addresses: When enabled, this policy **denies all WAN-side access** — only whitelisted IPs can reach the device — and prevents LAN-side devices from using it to reach the WAN. If no whitelist rules exist at activation, the device automatically adds the host PC's current IP to prevent lock-out.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



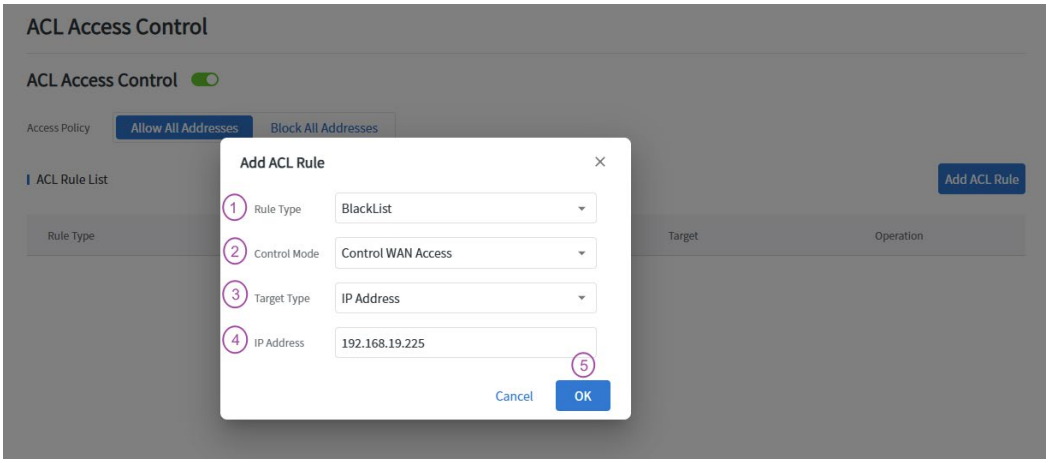
3.3.11.2 ACL Rules

To add an ACL rule:

1. Navigate to **Network > ACL Access Control**, enable the **ACL Access Control** option.
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.

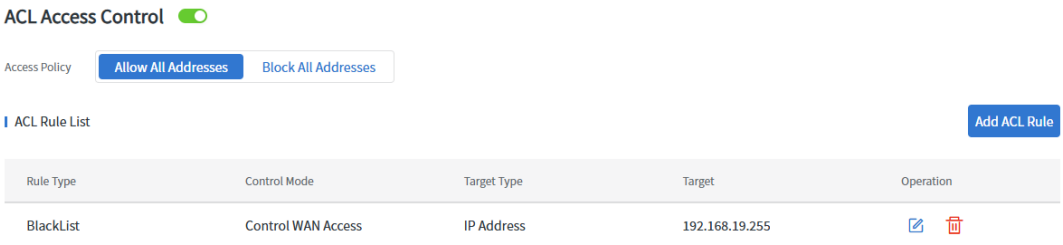
Description for the rule settings:

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.

Rule Type	Control Mode	Target Type	Result
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.



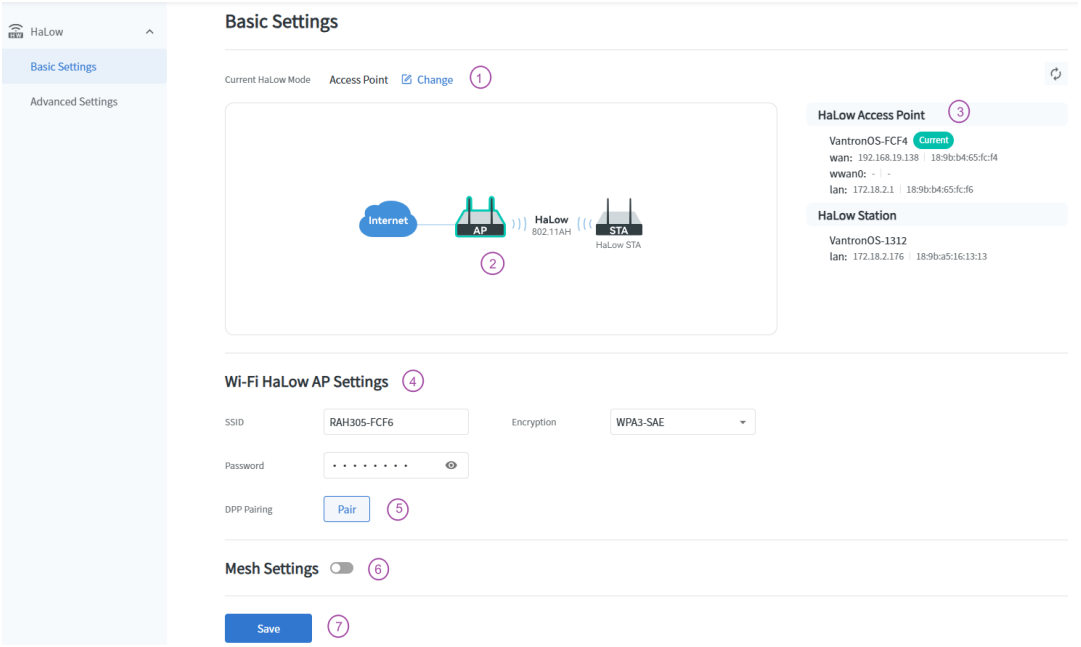
3.4 HaLow

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 AP-Mode Settings

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



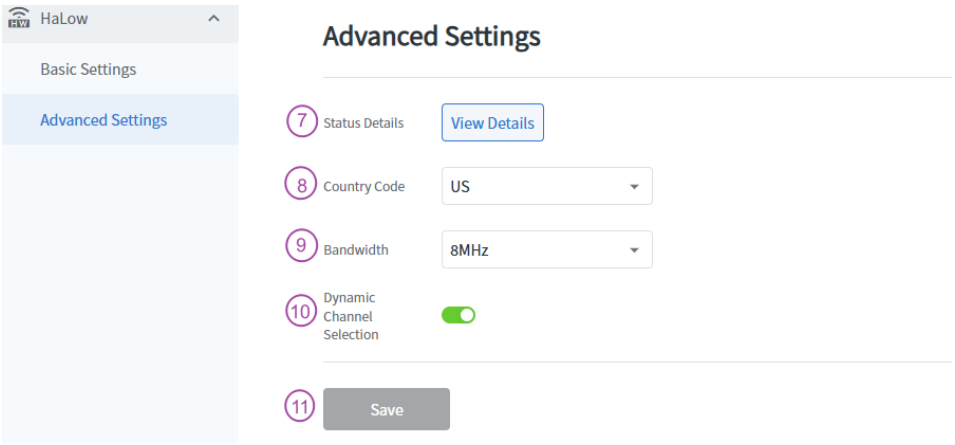
Description:

1. Click to change HaLow operation mode. The RAH305 supports **Access Point (AP)** operation with integrated **Mesh** capability; it cannot operate as a standalone HaLow STA. The **Change** option lets you switch the HaLow working mode back to AP when Mesh mode is active.
2. Network topology — Displays the layout of the current HaLow network connections. The local device is highlighted with a **cyan** outline.
3. Device Information — Shows brief connection information about the current device within the network topology.
   - "Current" indicates the local device.
   - Clicking the sync button refreshes the information.
4. Wi-Fi HaLow AP settings — SSID, encryption mode, and password. You can modify these parameters as needed. HaLow STAs adopt these credentials to establish a standard HaLow connection.
5. DPP pairing — Click **Pair** to initiate a quick HaLow connection. The target HaLow STA shall press the pairing button, either on the web portal or on the device, within the 120-second time window for a successful connection. Refer to Section 2.6.2 for hardware pairing instructions.

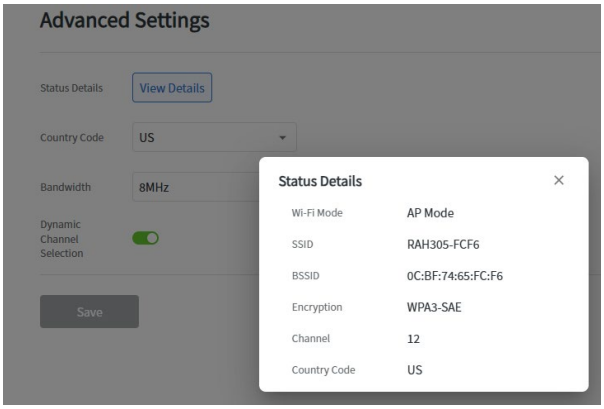
6. Enable/Disable mesh settings. When enabled, the device functions as both a HaLow AP and a Mesh MPP. Connected STAs retain their originally assigned IP when they join the mesh as MPs.

   All mesh nodes share the same parameters. Modifying mesh settings on the MPP automatically update those settings on connected MPs.

   The **Advanced Settings** page lets you view HaLow status details and configure advanced radio parameters such as country code, bandwidth and dynamic channel selection.



7. Status Details — Clicking **View Details** displays the device's detailed connection information (if a standard HaLow connection is established), including HaLow mode, SSID, encryption mode, transmit power, etc.



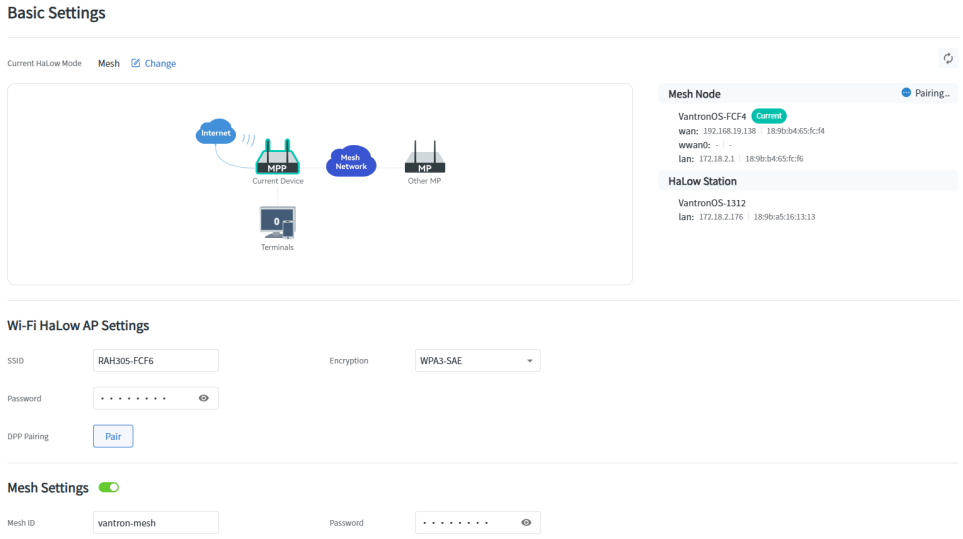
8. Country Code — Select the code based on local radio frequency regulations.
9. Channel bandwidth — A wider bandwidth typically offers higher throughput.
10. DCS — Once enabled, the device will automatically select the channel with the strongest signal within the selected bandwidth for optimal performance.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

When the RAH305 connects to an upstream internet device, all devices on the HaLow link gain internet access.

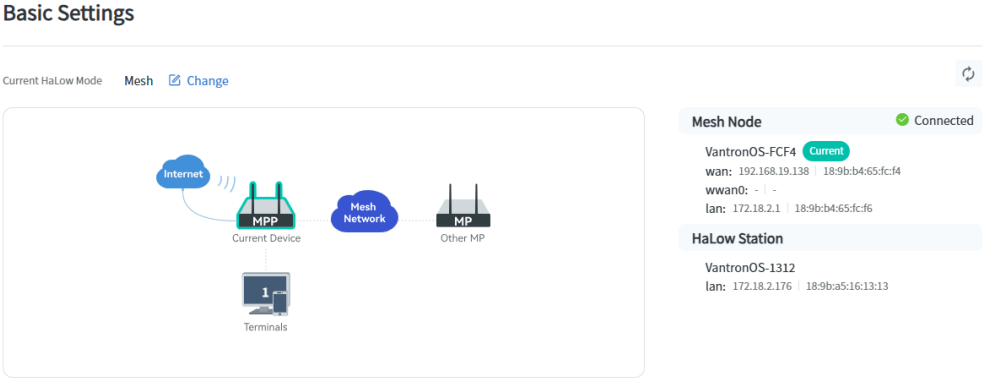
3.4.2 Mesh Networking

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

- As the RAH305 supports operation only in the HaLow AP role:
  - When mesh settings are enabled, this device takes on a combined AP+MPP role under Mesh mode, providing standard HaLow access for regular STAs and mesh networking for MPs.
  - The HaLow AP function handles initial association and DHCP IP assignment for STAs on the HaLow link.
  - Associated HaLow STAs with auto-join mesh enabled automatically join the mesh as MPs, retaining their assigned IP for mesh communication.
  - When the RAH305 connects to an upstream internet device, all devices on the network gain internet access.



(Mesh settings enabled)



(An MP joined the mesh)

*Use the **Change** option to switch back to the AP mode when necessary.*

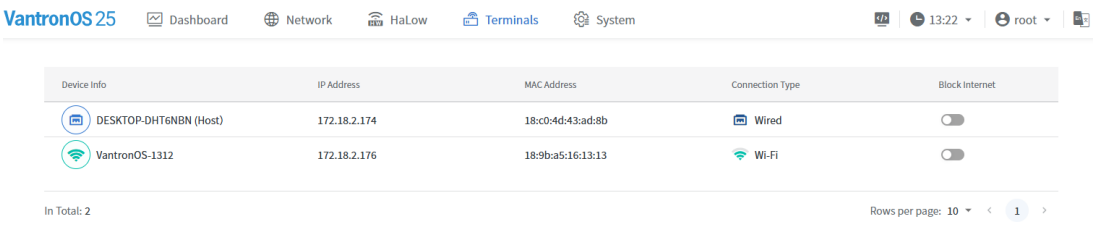
3.5 Terminals

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

2.4 GHz/5 GHz Wi-Fi and Wi-Fi HaLow connections are both classified to the **Wi-Fi** Connection Type, while Ethernet connections fall under the **Wired** Connection type.

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

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



3.6 System

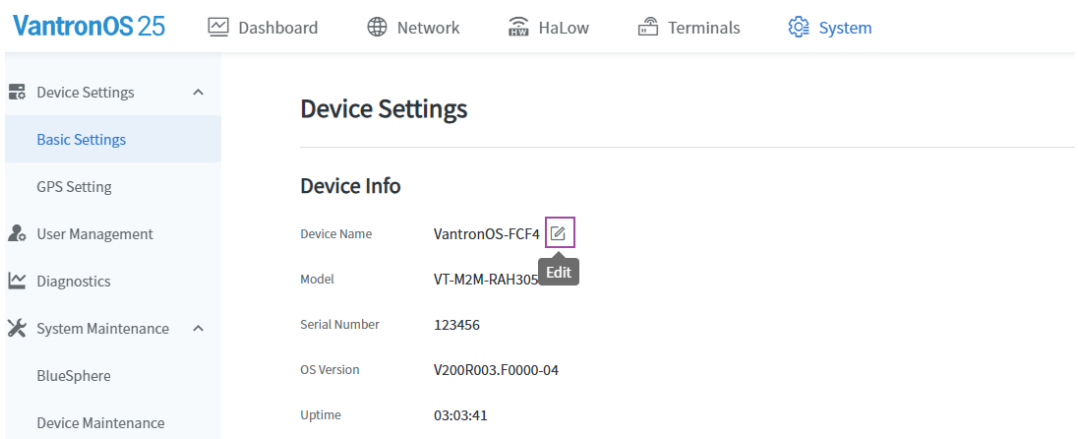
Under **System**, users can view and edit all system-level settings.

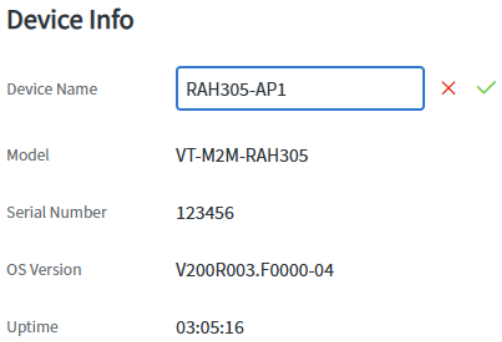
3.6.1 Device Settings

Device settings comprise basic device settings and GNSS feature-related settings.

3.6.1.1 Modifying Device Name

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



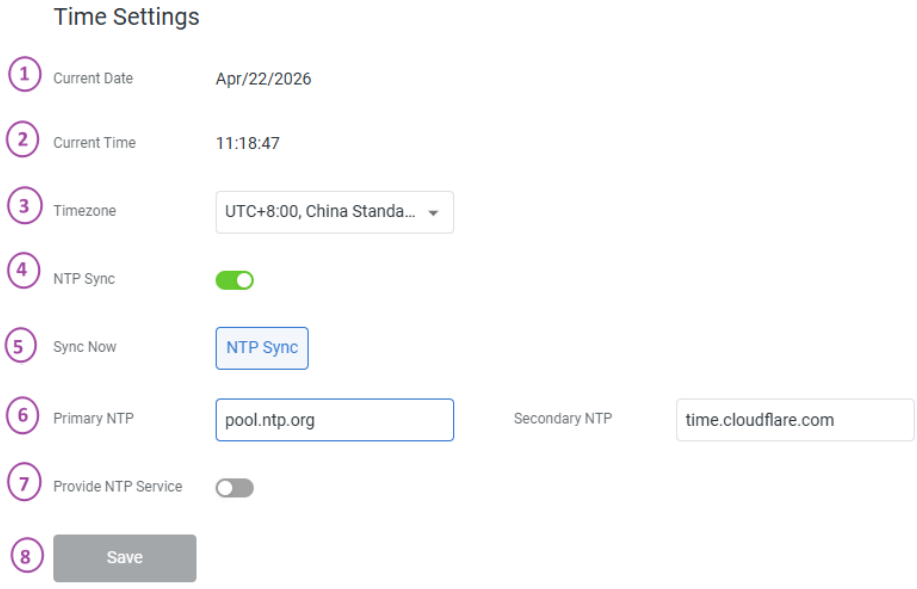


To modify the device name:

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

3.6.1.2 System Time

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



Description:

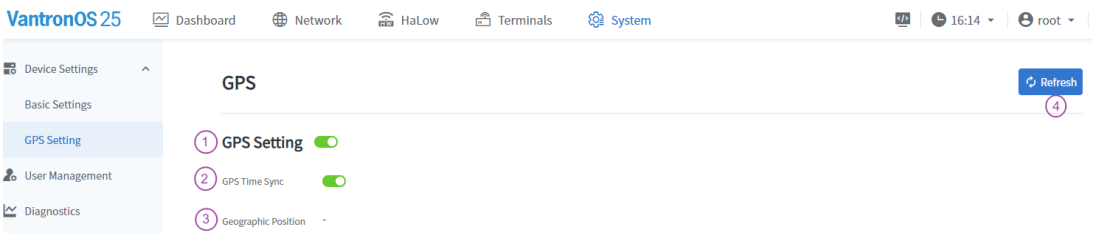
1. Current Date — Displays today's date for the selected time zone.
2. Current Time — Displays the current time.
3. Time Zone — Users can choose the desired time zone from the drop-down list.

4. NTP Sync — Toggles automatic time synchronization with NTP servers. The following options can be configured only when this feature is enabled.
5. Sync Now — Triggers a one-time NTP update immediately.
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.

3.6.1.3 GNSS Information

The RAH305 has a built-in GNSS module that receives satellite positioning signals and forwards the raw NMEA positioning messages it outputs to external devices in real time. This feature is particularly useful at sites without network access, where satellite time provides an accurate device clock for aligning logs and collected data in time.

Ensure the RAH305 is placed outdoors with a clear view of the sky before using the GNSS function.



Description:

1. Enabling **GPS Setting** starts satellite search and positioning, and enables GNSS forwarding.
2. When **GPS Time Sync** is enabled, the device uses GNSS satellite time (UTC) to automatically calibrate the system time, without relying on network NTP.

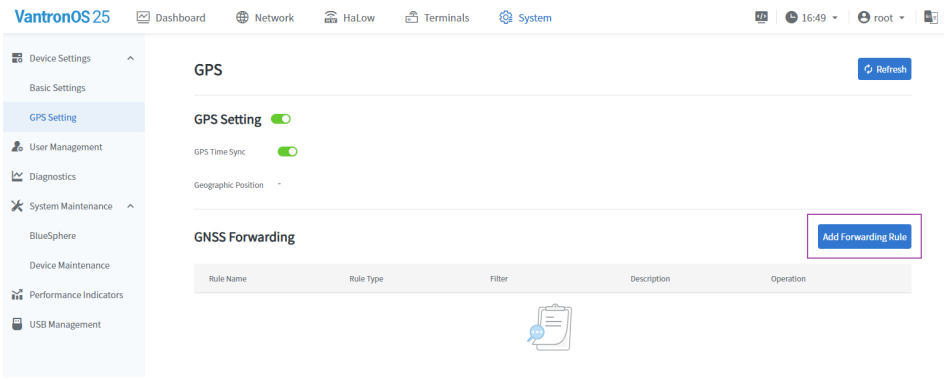
   *Time synchronization requires **a successful positioning first**.*
3. Once the device is outdoors with a clear view of the sky and has obtained a position fix, **Geographic Position** displays the latitude and longitude information currently parsed by the device.
4. Click **Refresh** to reload the current position information from the device and update the page display.

The GNSS module continuously outputs the positioning data. Through forwarding rules, this data stream can be sent to external devices or platforms via:

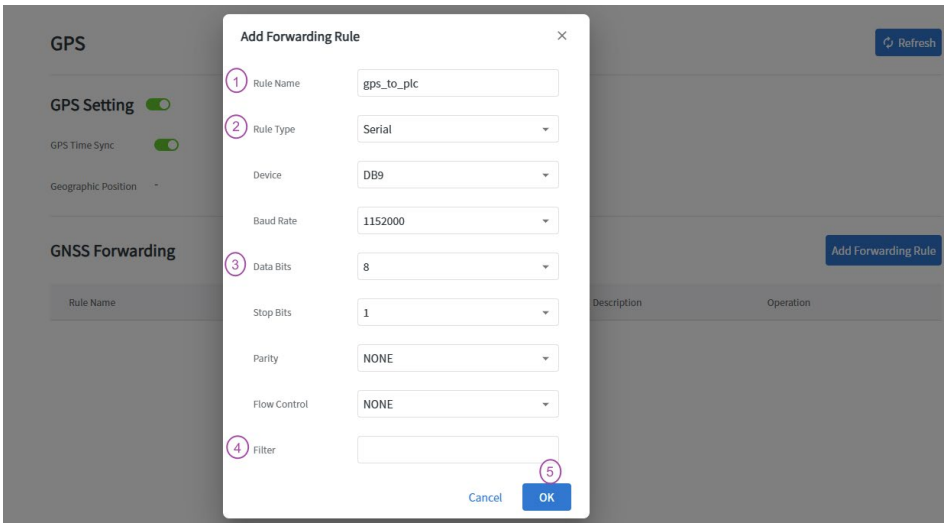
- **Serial:** forwarded to peripherals attached to the local serial port, such as vehicle displays, industrial control boards, microcontrollers, positioning boxes.
- **Network:** forwarded to a remote server or host computer for platform track recording and map display.

Steps to create a forwarding rule:

1. Click **Add Forwarding Rule** on the **GPS Setting** page to open the creation dialog.



2. Set the rule parameters.



Description:

1) Enter a rule name.
2) Select rule type.
3) Fill in corresponding parameters.

   Serial:

   - Device — The serial port in use.
   - Baud rate, data bit, stop bit, parity — Must exactly match the receiving end.
   - Flow control — Configure based on the receiving end's requirements.

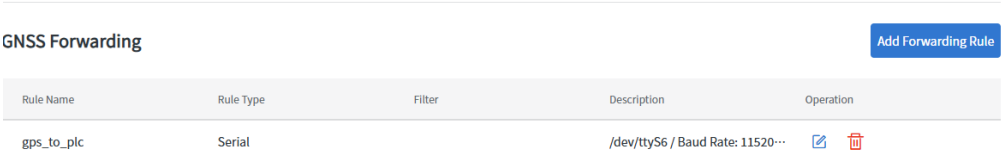
Network:

- Address — Target server IP address or domain name.
- Port — Target server listening port, must match the receiving platform.
- Protocol — Transport protocol, TCP (default, reliable) or UDP (lower latency, connectionless).

4) Filter — Sentence filter; e.g., $GPGGA, $GPRMC; leave blank to forward all.

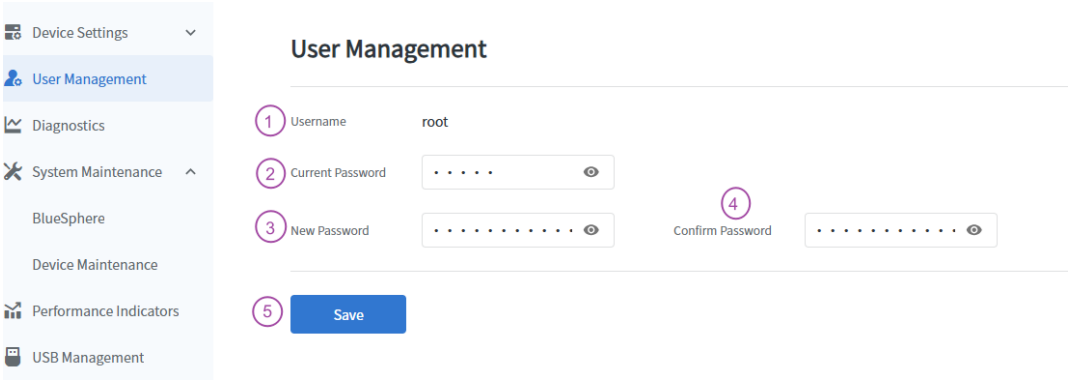
5) Click **OK** to save the rule. The rule immediately appears in the **GNSS Forwarding** list and takes effect.

3. After creating a forwarding rule, you can edit or delete it as necessary via the icons in the **Operation** column.



3.6.2 User Management

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



Steps to reset the login password:

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

3.6.3 Diagnostics

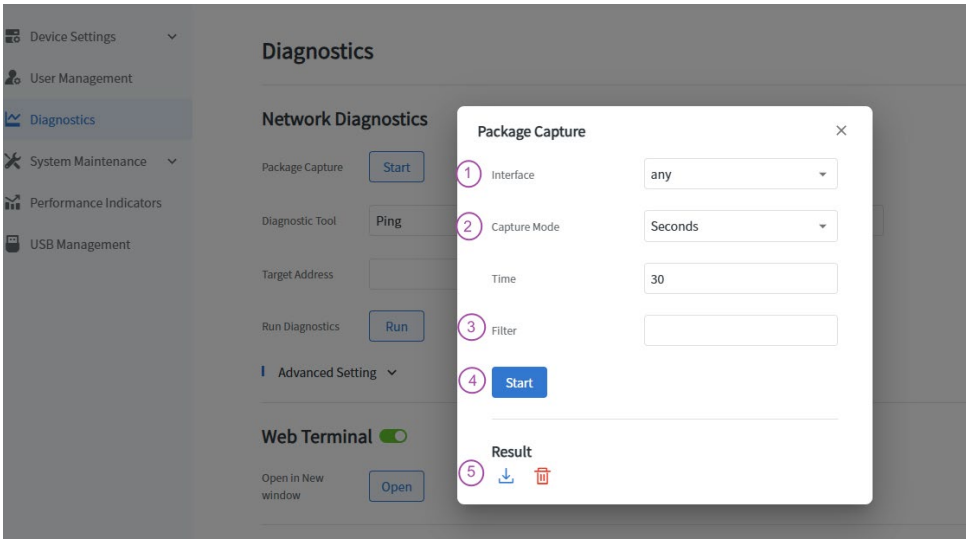
On the **Diagnostics** page, users can run network tests, turn on the web terminal for troubleshooting, and view the device log for maintenance or diagnosis purposes.

3.6.3.1 Packet Capture

The RAH305 supports capturing network packets on a specified network interface for troubleshooting, protocol verification, and traffic analysis. It offers two capture modes: timed capture and packet-count-based capture.

To configure a capture rule:

1. Navigate to **System > Diagnostics > Network Diagnostics**.
2. Click **Start** next to **Packet Capture**.
3. Configure the capture rule in the popup window.

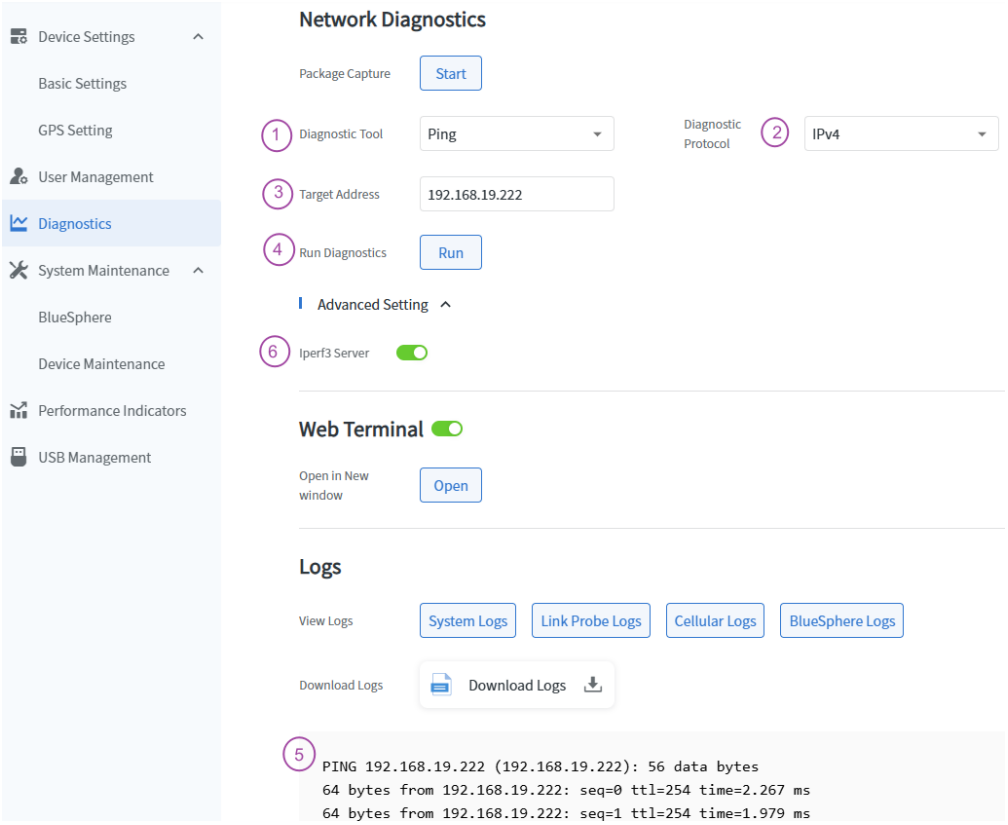


Description:

1) Select the interface for packet capture (defaults to "any" to capture all traffic).
2) Select to capture the packets by time duration (in seconds) or by packet count.
3) Configure the packet filter. You can restrict capture to specific IPs, ports, or protocols to reduce noise.
4) Click **Start** to begin the capture task. You can stop it at any time.
5) Once finished, download the result (a .pcap file) or delete it.

4. Open the file in a packet analyzer such as ‘Wireshark’.

3.6.3.2 Network Diagnostics

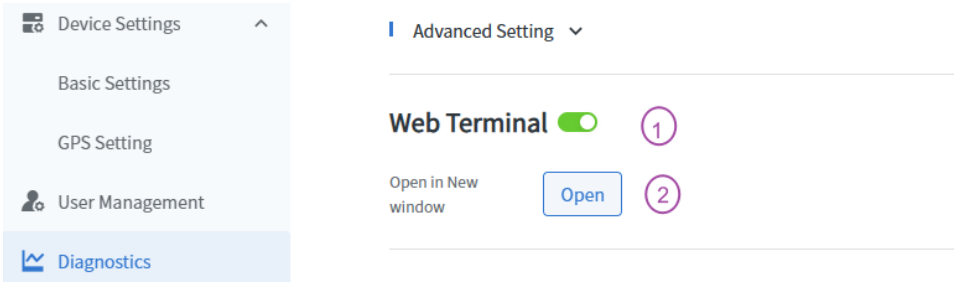


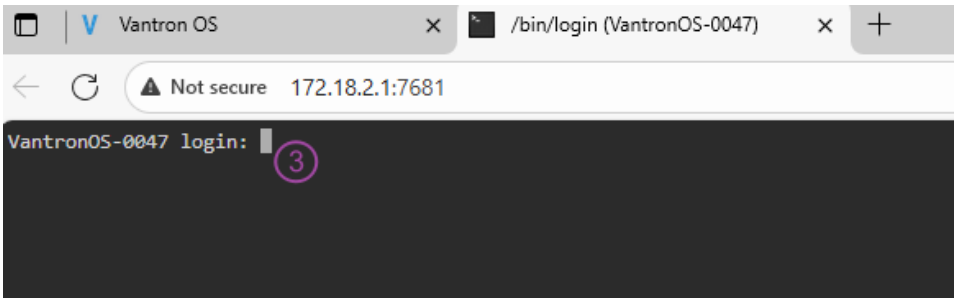
Description:

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

3.6.3.3 Web Terminal

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





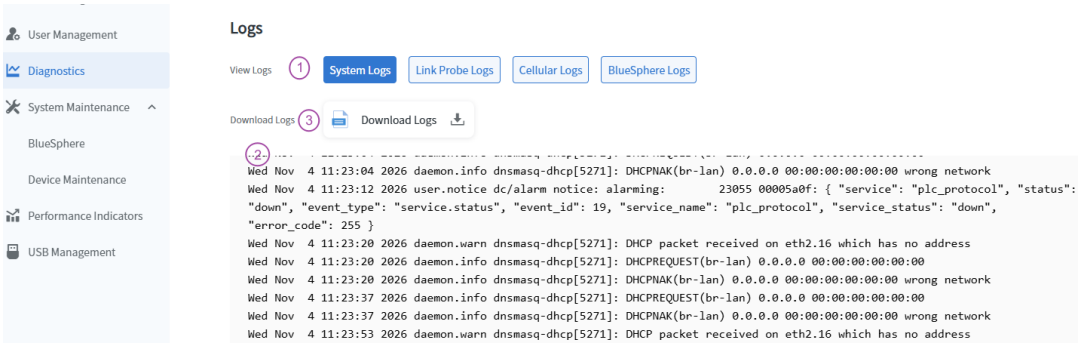
Description:

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.

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

3.6.3.4 Logs

The system offers different device logs for maintenance or troubleshooting.



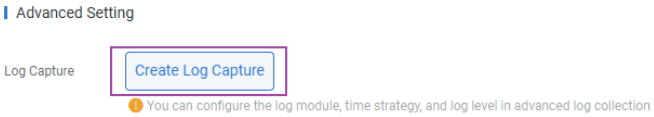
Description:

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.

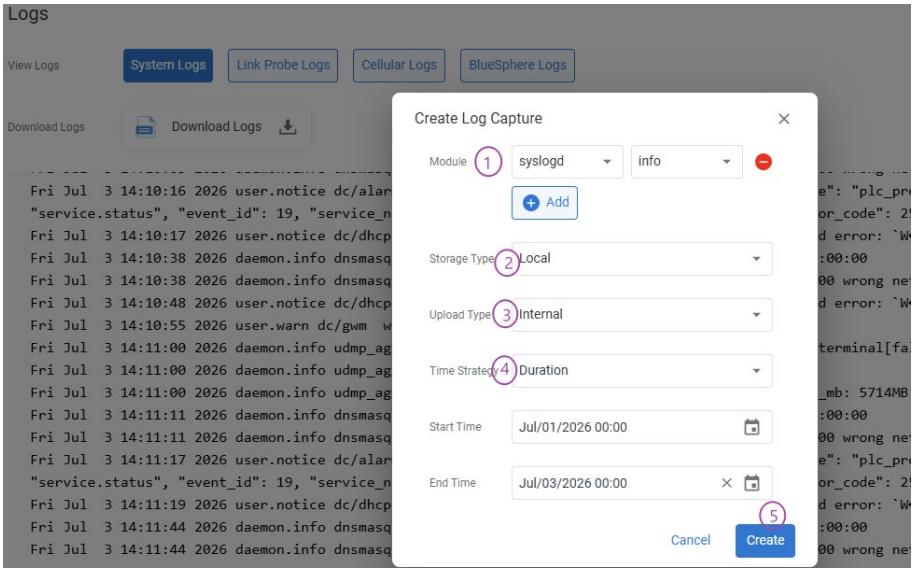
3.6.3.5 Log Capture

In the **Advanced Settings** section under **Network Diagnostics**, 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.
3. Click **Create Log Capture**.



4. Configure the rule.



1) **Module:** Select one or more modules for log generation.

2) **Storage Type:** Specifies where the logs are saved.

3) **Upload type**

- Internal: Logs are saved to the device's **/tmp/log** directory and can be accessed using the `cd` and `cat` commands in the terminal console (**valid until the next device reboot**).

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

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

4) **Time Strategy**

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

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

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

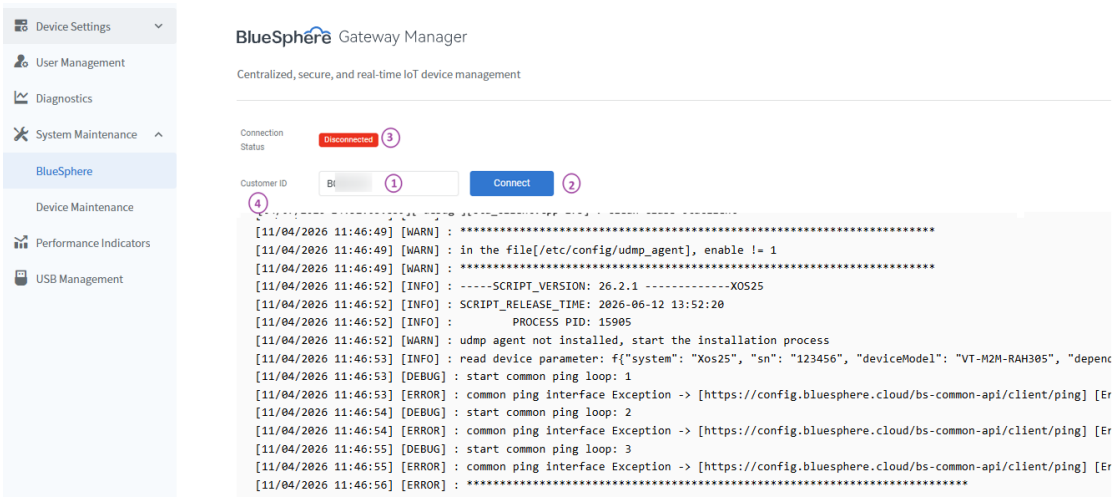
3.6.4 System Maintenance

3.6.4.1 BlueSphere

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

Prerequisite:

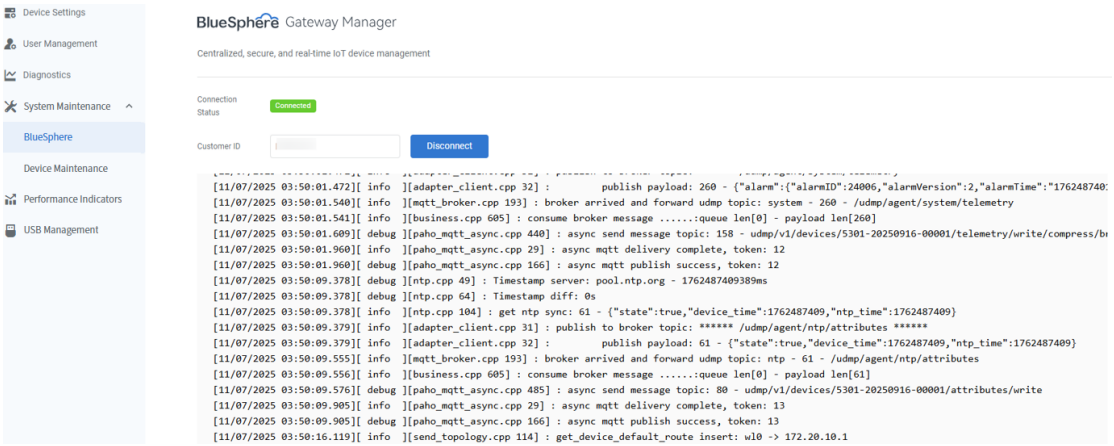
The RAH305 must have internet access.



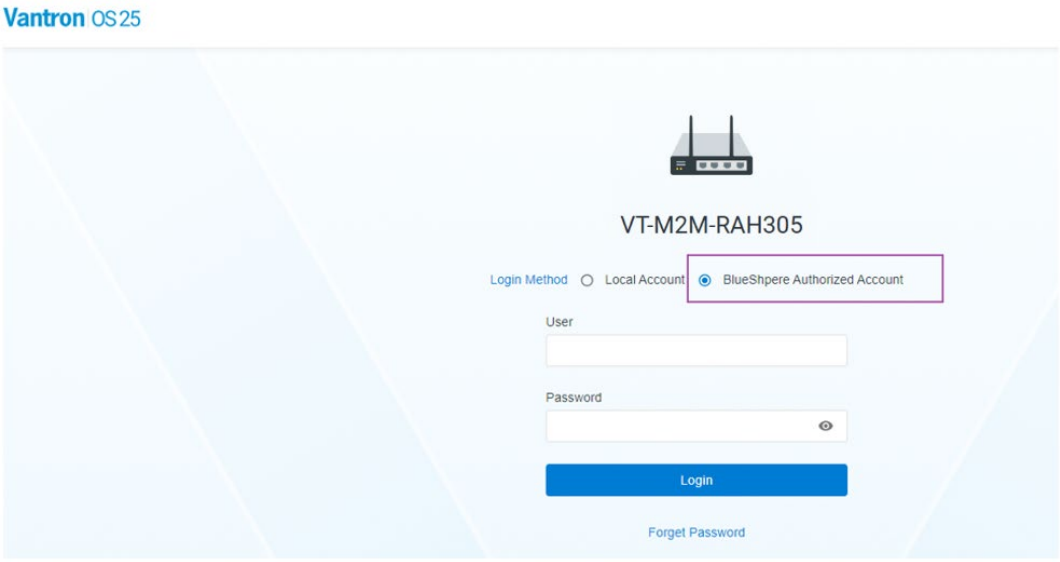
Description:

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.



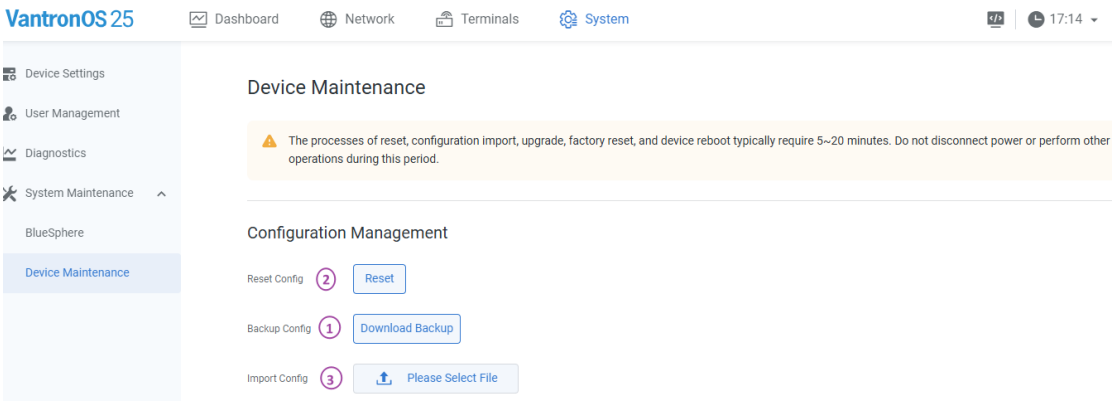
If you log out the portal now, you will find two login methods available. You can sign back in with either your local credentials or an authorized GWM account.



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

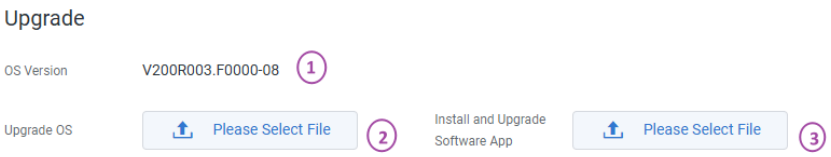


Description:

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

Once the device configuration is cleared, you can re-log in to the device using your existing password and follow the setup wizard to finish the first-time configuration.

- Upgrade

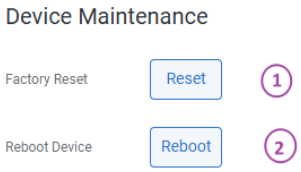


Description:

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

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

- Device Maintenance



Description

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

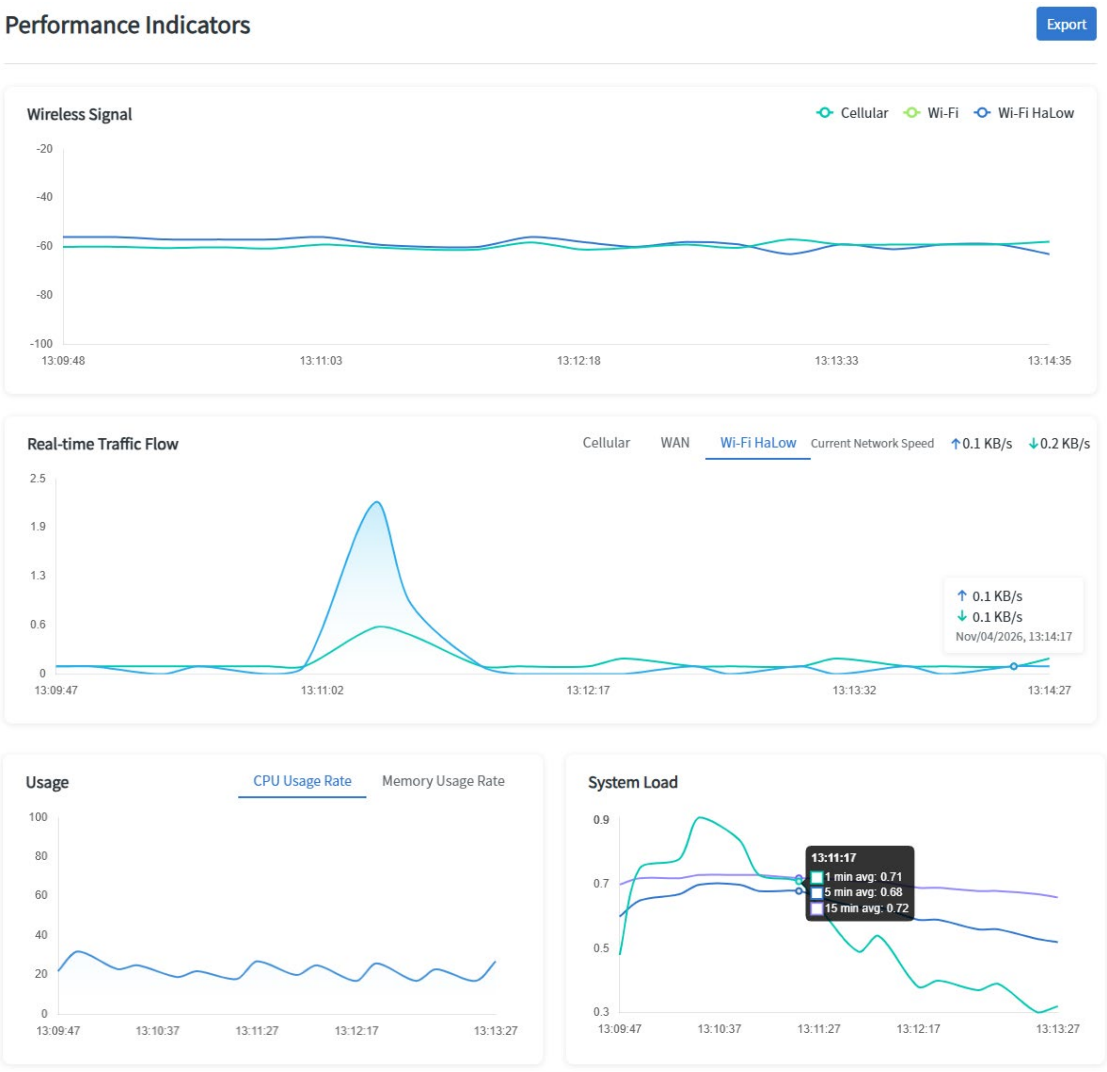
*If needed, back up the existing configuration before factory reset by clicking the **Download Backup** button under **Configuration Management**.*

3.6.5 Performance Indicators

The **Performance Indicators** page presents the device's wireless signal quality, network traffic trends, and system resource usage in real time through visual charts. It allows users to intuitively assess the current operational health of the device and troubleshoot network fluctuations or system overloads.

The **Export** button in the upper right corner allows users to export the monitored data for further analysis.

The page contains four main monitoring sections: wireless signal, real-time traffic flow, resource usage, and system load.

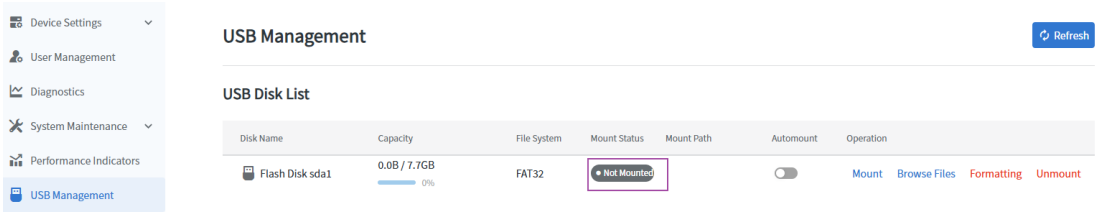


1. **Wireless Signal**
   - Displays the wireless signal strength (RSSI) over time for different wireless network interfaces. Supported interfaces: Cellular, Wi-Fi (STA), HaLow AP+MPP, and HaLow STA / HaLow STA+MP. The HaLow AP interface alone is not supported.
   - Values are displayed once the time axis on the left aligns with the device time, and are then automatically refreshed every 15 seconds.
   - Users can toggle the visibility of specific data lines by clicking the legend.
   - Hovering over a data point displays the signal strength value at a specific time.
2. **Real-time Traffic Flow**
   - Displays the real-time uplink and downlink data transmission rates (KB/s) for the selected network interface.
   - Use the top tabs to switch between interfaces.
   - Hovering over a data point reveals the exact rate at a specific time.
3. **Usage**
   - Monitors the consumption of core hardware resources.
   - CPU Usage Rate: Displays the processor load percentage over time.
   - Memory Usage Rate: Displays the system memory (RAM) consumption percentage.
   - Use the top tabs to switch between the two indices.
   - Hovering over a data point reveals the exact rate at a specific time.
4. **System Load**
   - Displays the device system load average, reflecting the queuing and processing pressure of tasks over specific periods.
   - Metrics: Includes 1 min avg, 5 min avg, and 15 min avg load curves. Hovering over a data point displays the specific load values at that moment.

3.6.6 USB Management

The **USB Management** page allows users to monitor, mount, and manage external USB storage devices connected to the RAH305. It provides a clear overview of connected disks and enables easy access to their file systems.

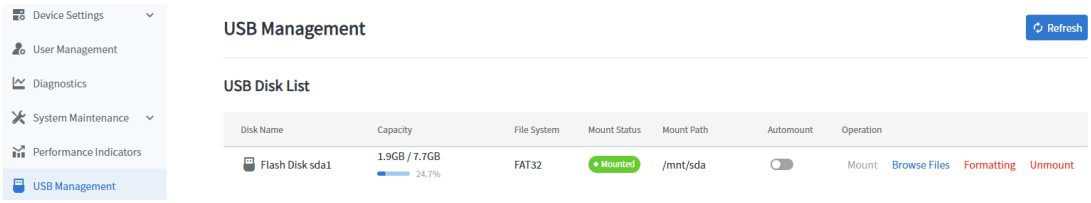
Insert a USB drive into the RAH305 and click **Refresh** to display its information. By default, newly inserted devices are unmounted.



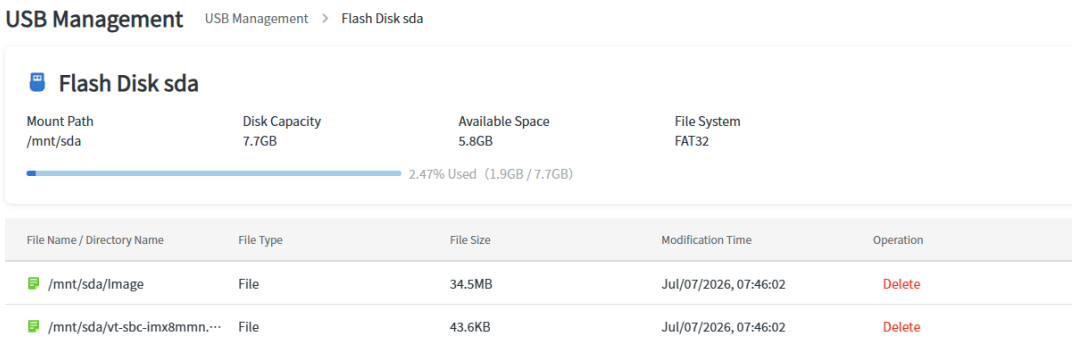
You can mount a USB drive in one of the following two ways:

- **Automount:** Toggle **Automount** on and specify a path under /mnt/. The device will automatically mount to this path the next time it is re-plugged in. Disabling **Automount** keeps the device mounted at its current path, but it will not auto-mount when re-plugged in.
- **Manual Mount:** Select **Mount** to manually enter a path under /mnt/ for a one-time mount. You need to manually close the dialog box after entering the path.

USB Disk List displays all detected USB drives along with key details such as Disk Name, Capacity, File System (e.g., FAT32), and Mount Status. Once a USB drive is mounted, you can view its general information and initiate quick actions to mount, unmount, or format the USB drive.

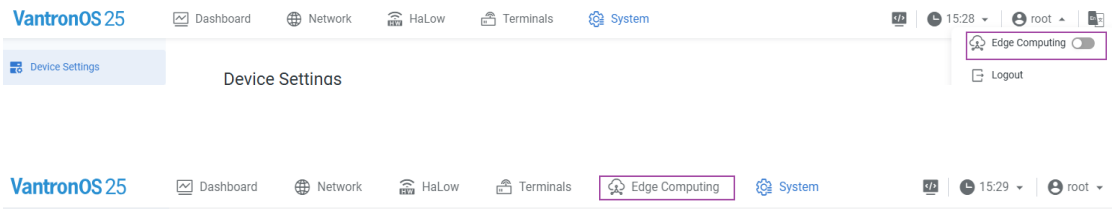


The **Browse Files** option opens a file explorer interface, allowing users to view directory structures, check file sizes, modification times, and delete files directly from the web UI.



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.



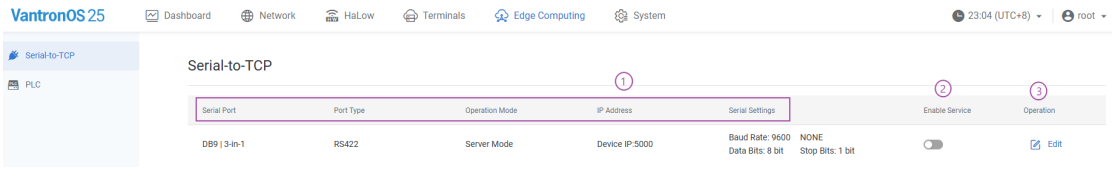
3.7.1 Serial to TCP

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.

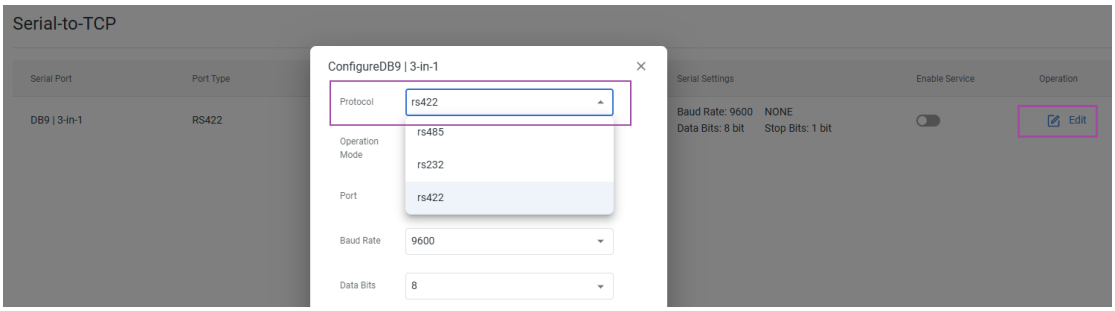
- **Server mode** turns the device's serial port into a TCP listener, allowing remote clients to connect and exchange data.
- **Client mode** makes the device's serial port a TCP client, automatically tunneling all traffic to a specified remote server.



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.

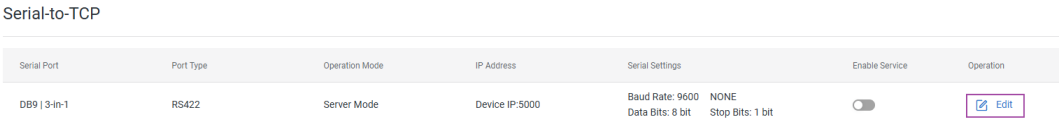
   The serial port is a multiplexed, operating in the RS-422 mode by default and can be modified via the ***Edit*** *menu.*



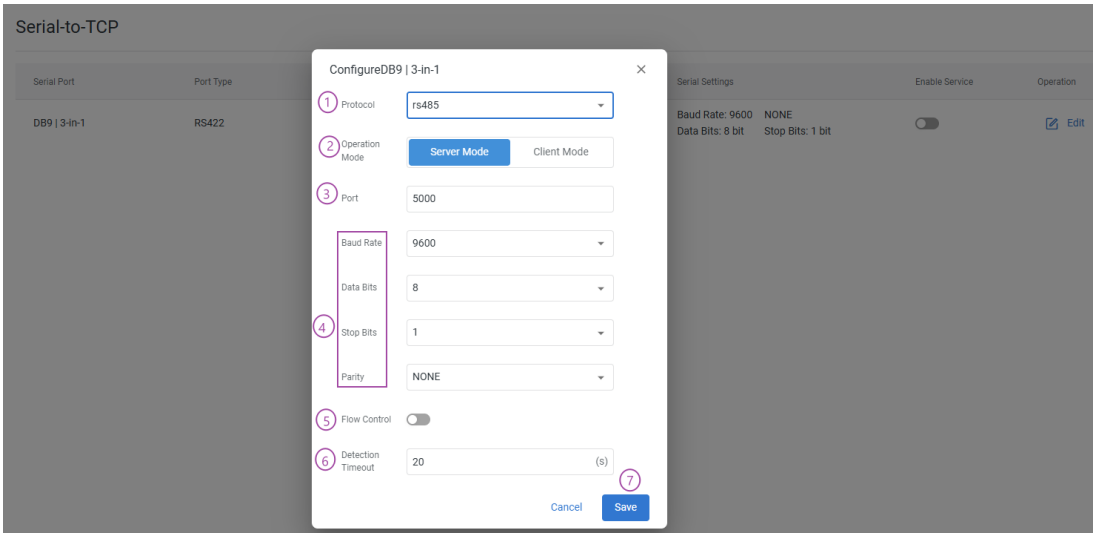
2. Enable/disable the rule.
3. Edit the rule.

3.7.1.1 Server Mode Rule Setup

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



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

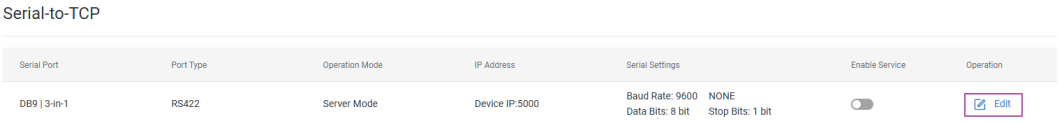


1) Select a serial mode for the multiplexer.
2) Select **Server Mode.**
3) Designate a TCP port (0~65535) for the server to listen on. The client must connect to the same port.
4) Make sure the serial parameters on both the peripheral and router are set the same.
5) Enable/Disable software flow control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

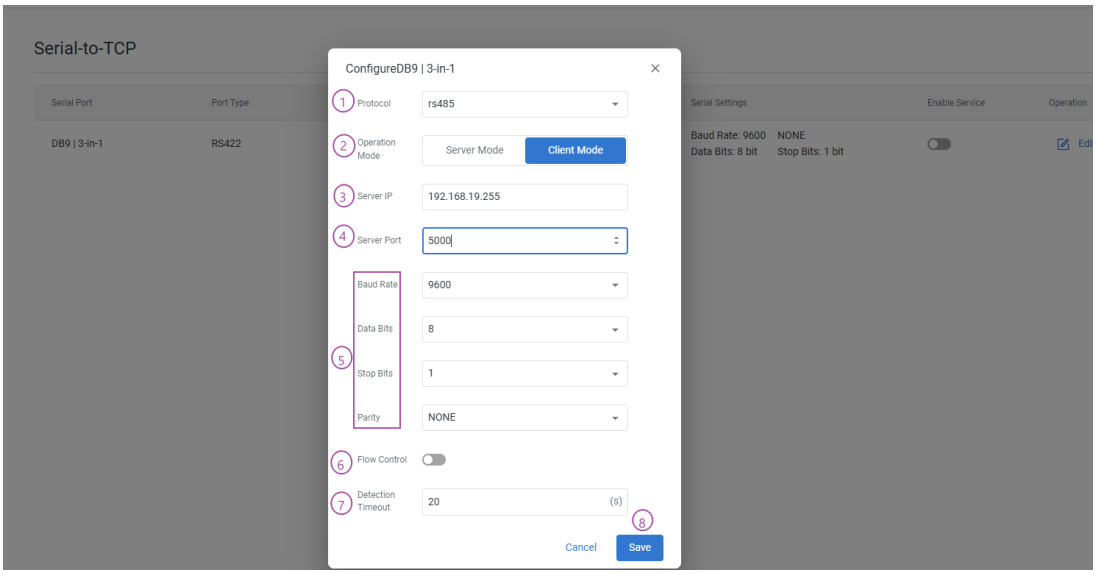
3. Enable the conversion rule after editing the parameters.
4. Make sure both the client and server are on the same reachable IP network.
5. Verify the data transmission between the devices.

3.7.1.2 Client Mode Rule Setup

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



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



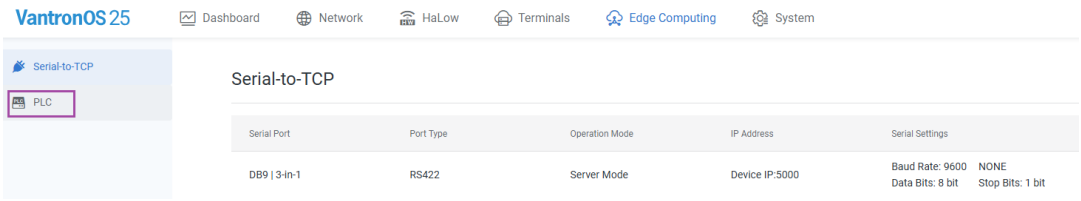
1) Select a serial mode for the multiplexer.
2) Select **Client Mode.**
3) Enter the server's IP address.
4) Enter the target port and make sure it matches the TCP port on the server.
5) Make sure the serial parameters on both the peripheral and router are set the same.
6) Enable/Disable software flow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

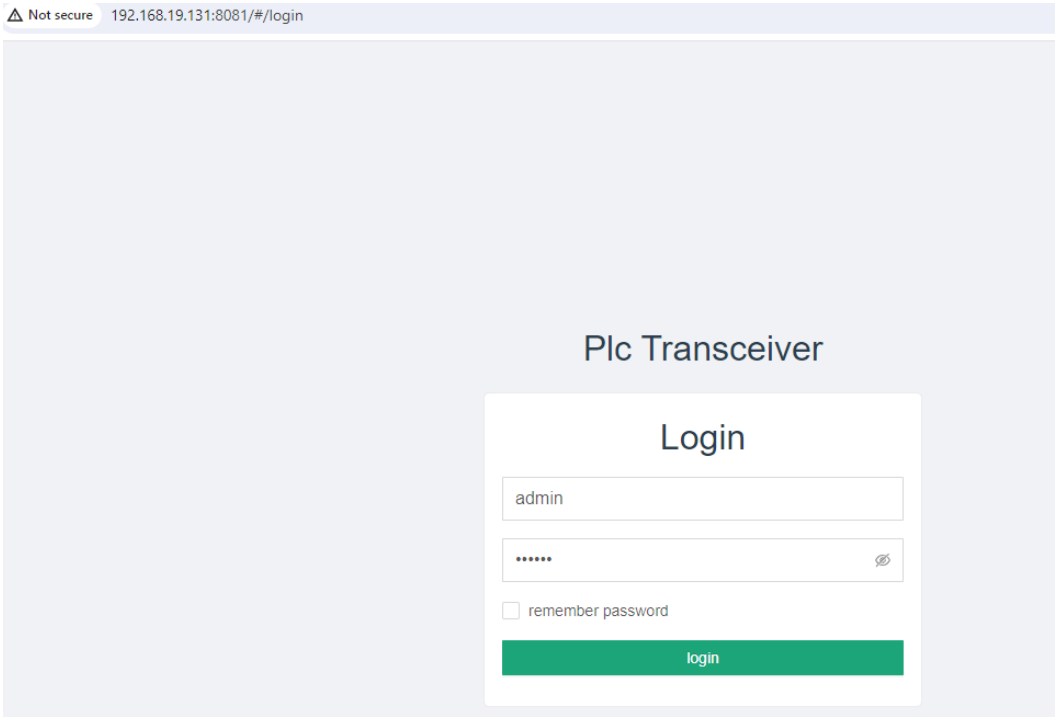
3.7.2 PLC

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.

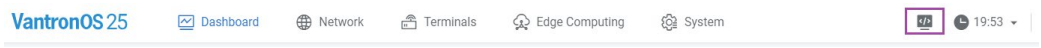
4.2 I/O Configuration

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 AI/AO 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:

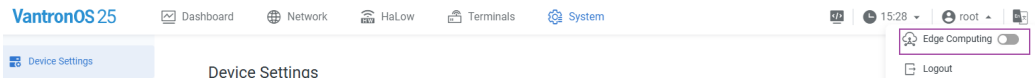
```
# gpio set aiao1 ao
# gpio set aiao1 ao
# gpio set aiao1 ao
# gpio set aiao1 ao
```

4. Query the current working mode of each channel:

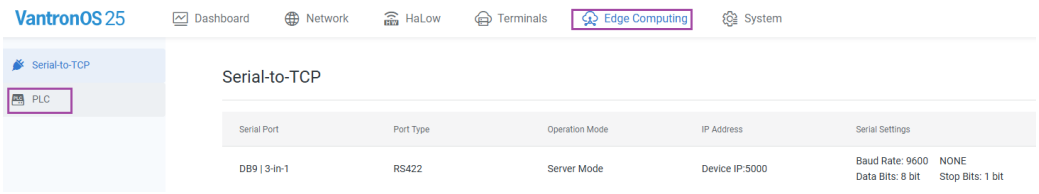
```
# gpio get aiao1
# gpio get aiao2
# gpio get aiao3
# gpio get aiao4
```

4.3 Portal Login

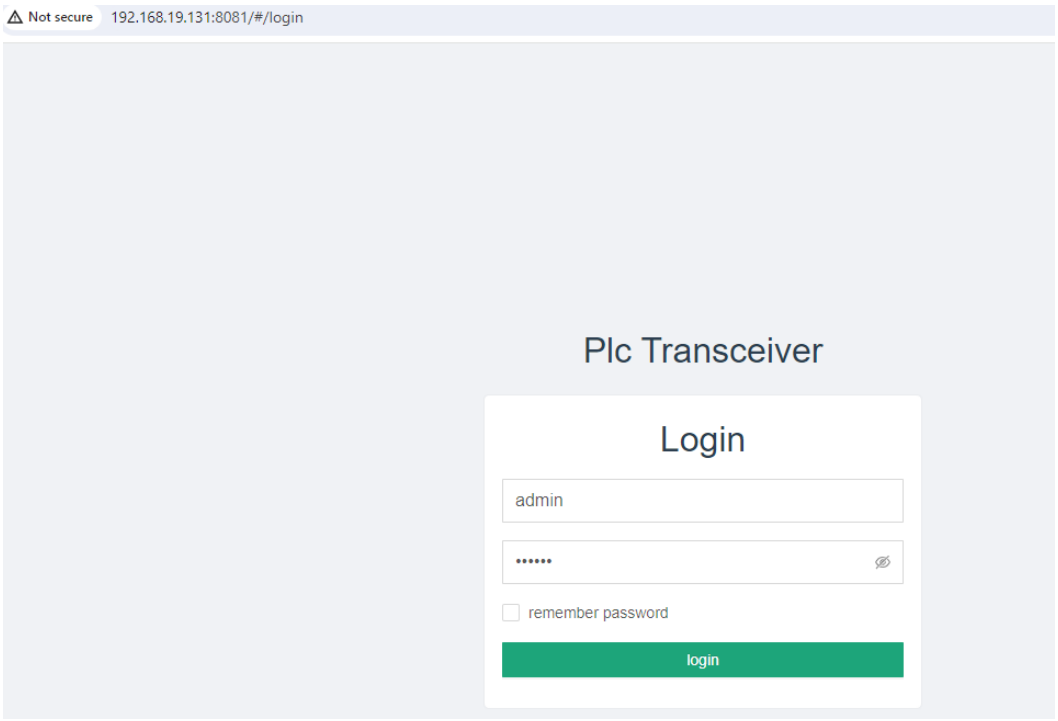
1. Enable the **Edge Computing** feature from the user account drop-down list.



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.