HAP101 Wi-Fi HaLow Access Point

User Manual

Version: 3.1

Revision History:

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

V3.0	Regenerated chapters 2 & 3 based on the current **VantronOS-25** system UI, including device login, startup wizard, DPP pairing, device setup, etc.	Oct. 25, 2025
V3.1	1. Removed the description of automatic Ethernet mode change upon short press of the Pair button (Section 2.5) based on the new design. 2. Updated Sections 1.6 &1.7 on the button and LED definitions. 3. Updated Section 3.1 as per UI change. 4. Deleted Section 3.3.1.1 Uplink Interface, 3.3.1.2 IP Configuration Mode, 3.3.1.3 Downlink Interfaces, 3.1.4 DHCP Service & DHCP Reservation, 3.3.1.5 Ethernet Port Mode Modification, 3.3.1.6 Interface Bridging as per UI change. 5. Added Section 3.3.1.1 WAN, 3.3.1.2 LAN, and 3.3.1.3 IPv6 Settings as per UI change; included DHCP Service & DHCP Reservation in 3.3.1.2. 6. Modified Sections 3.3.2&3.4.1 Wi-Fi & HaLow settings and added Section 3.4.4 Mesh Settings. 7. Added Section 3.7 CLI.	Mar. 12, 2026

Table of Contents

Foreword

Thank you for purchasing HAP101 Wi-Fi HaLow Access Point ("the Product" or "the device"). This manual intends to provide guidance and assistance necessary on setting up, operating or maintaining the Product. Please read this manual and make sure you understand the structure and functionality of the Product before putting it into use.

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

Intended Users

This manual is intended for:

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

Copyright

Disclaimer

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

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

Technical Support and Assistance

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

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

Vantron Technology, Inc.

Address: 48434 Milmont Drive, Fremont, CA 94538

Tel: (650) 422-3128

Email: sales@vantrontech.com

Regulatory Information

The Product is designed to comply with:

- Part 15 of the FCC Rules
- ISED

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

Symbology

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

Note: Calls attention to critical operational or safety information.

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

General Safety Instructions

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

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

Precautions for Power Cables and Accessories

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

⚠ Place the power cable properly at places without extrusion hazards.

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

⚠ Cleaning instructions:

- Power off before cleaning the Product
- Do not use caustic or aggressive liquids, vapor, or spray
- Clean with a damp cloth
- Do not try to clean exposed electronic components unless with a dust collector

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

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

⚠ Do not use in combustible and explosive environment:

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

CHAPTER 1 DEVICE INTRODUCTION

1.1 Product Overview

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

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

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

1.2 Unpacking

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

Standard accessories:

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

Optional accessories:

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

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

1.3 Terminologies and Acronyms

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

Table 1-1

Glossary	Description
AP	**HaLow access point**. An AP broadcasts the HaLow network to multiple HaLow stations (STA). It typically connects to an internet router, distributing internet connectivity to all paired STAs. In a standard HaLow network, there will always be **only one** HaLow AP.
STA	**HaLow station**. An STA is a client device that connects to a HaLow AP for a Standard HaLow connection. These devices typically access external networks through the HaLow AP.
Standard HaLow mode	Standard HaLow mode refers to a basic HaLow network architecture where Stations (STAs) communicate directly with an Access Point (AP). This AP is typically connected to an internet router to provide connectivity.
HaLow Mesh mode	In a HaLow Mesh configuration, all devices communicate with each other to automatically determine the most efficient path for data transmission, helping to extend network range and improve reliability.
Mesh Portal (MPP)	A Mesh Portal serves as a DHCP server in a mesh network for internal IP assignment. There is at most one Mesh Portal in a mesh network.
Mesh Point (MP)	A Mesh Point operates as an intermediate HaLow node that extends the network coverage through multi-hop communication. In the absence of an MPP in a mesh network, there must be an MP connected to an external network to relay IP addresses from an upstream DHCP server.
DPP	**Device Provisioning Protocol.** Defined by Wi-Fi Alliance for **Wi-Fi Easy Connect™**. In this document, it refers specifically to the fast provisioning of devices via simple hardware/software setup for a Standard HaLow pairing ("**DPP Pairing**").
VantronOS	Web management portal for Vantron IoT communication devices.
DCS	**Dynamic Channel Selection**. Once enabled, the device will automatically select the channel with the strongest signal within the selected bandwidth for optimal performance.

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

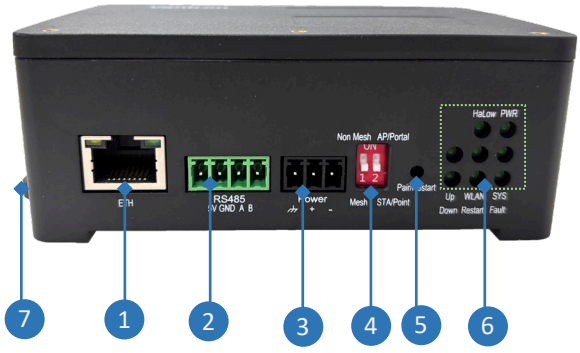
1.4 Specifications

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

HAP101			
Software	Operating system	VantronOS	
	Device management	Vantron BlueSphere GWM (Optional)	
	Upgrade	Local upgrade, OTA upgrade	
	VPN	OpenVPN	
	Network protocol	IPV4, HTTPS, TCP & UPD, NTP client and server, ARP, TLS	
	Link detection	Heartbeat detection, auto reconnection	
	Network reliability	Multi-channel failover, backup between Ethernet, Wi-Fi, HaLow	
	IP application	Ping, Traceroute, DHCP Server/Client	
	IP routing	Static routing, dynamic routing	
Security	2.4GHz Wi-Fi	TKIP, WPA, WPA2, AES, WPS	
	Wi-Fi HaLow	WPA3	
	Firewall	Stateful	
	Access control	MAC address, IP address, URL	
Environmental	Temperature	Operating: -20℃ ~ +70℃	Storage: -40℃ ~ +85℃
	Humidity	≤ 95% RH (non-condensing)	
	Certification	FCC, ISED	

1.5 Interfaces and Indicators

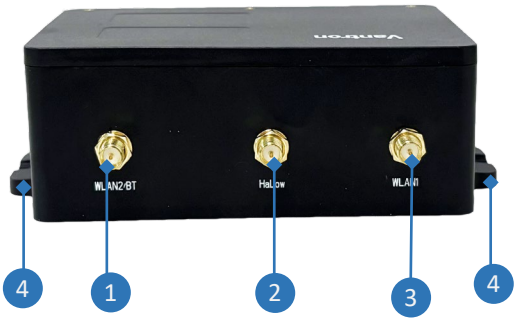
1.5.1 Front view



Description:

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

1.5.2 Back view



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

1.6 DIP Switches

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

Table 1-2

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

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

1.7 Pair/Restart Button

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

Table 1-3

Button Hold	Description
<1s	Confirms the DIP switch setup, and: • Enters DPP pairing state (Standard profile); **OR** • Starts scanning for a HaLow Mesh network with the same settings (Mesh profile).
[2s, 6s)	Initiates a device reboot.
[6s, 12s)	Device configuration is cleared. You can re-log in to the device using the credentials provided on the device label and follow the setup wizard to finish the first-time configuration.
[12s, 20s)	The device is factory reset with all configurations, user data, and user apps cleared. You can re-log in to the device using the credentials provided on the device label and follow the setup wizard to finish the first-time configuration.
[20s, +∞)	No device action triggered.

1.7.1 Button Action for DPP, Mesh & Device Reset

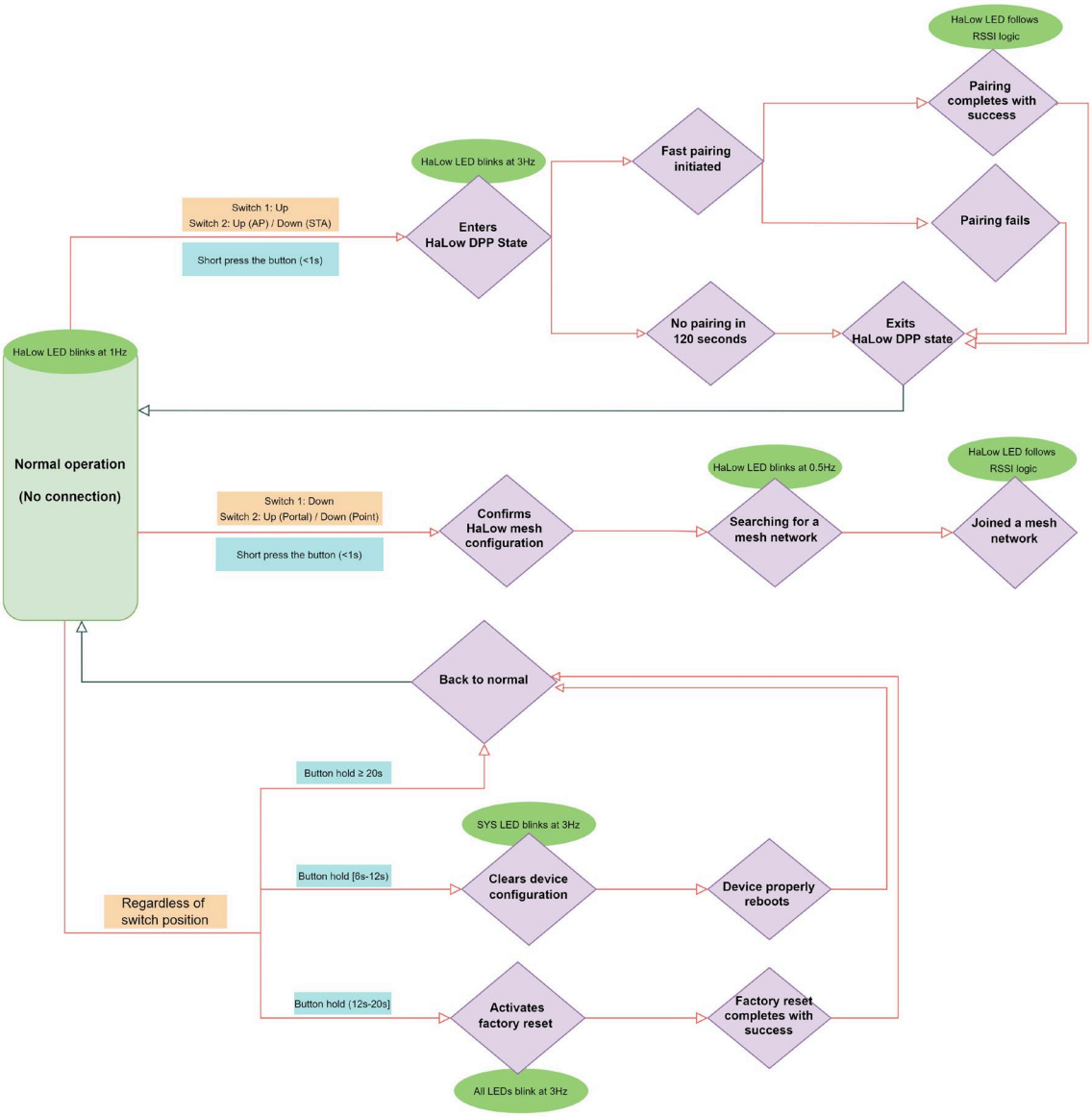
Table 1-4

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

1.7.2 Button Action & HaLow LED Diagram

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

Figure 1-1:



1.8 LED Indicators

1.8.1 WLAN LED

Mode	LED status	Description
Wi-Fi Client	OFF	2.4GHz Wi-Fi module is not working.
	Blinking at 1Hz	Searching for available Wi-Fi AP.
	Solid green	Connection established with a Wi-Fi AP.
Wi-Fi AP	OFF	2.4GHz Wi-Fi module is not working.
	Blinking at 1Hz	2.4GHz Wi-Fi is not connected.
	Blinking at 3Hz	WPS is initiated via hardware or software configurations. (back to normal upon finish)
	Solid green	A Wi-Fi client is connected.

Factory Reset Status:

- Factory reset initiated and in progress: Blinking at 3Hz.

1.8.2 HaLow LED

Mode	LED status	Description
HaLow Station	OFF	Wi-Fi HaLow module is not working.
	Blinking at 1Hz	Searching for available HaLow AP.
	Blinking at 3Hz	A DPP pairing is initiated via hardware or software configurations. (blinking at 1Hz after 3s upon a timeout; following the RSSI configuration logic upon a successful pairing)
	Following the RSSI logic*	Connection established with a HaLow AP.

Mode	LED status	Description
HaLow AP	OFF	Wi-Fi HaLow module is not working.
	Blinking at 1Hz	A standard Wi-Fi HaLow connection is not established.
	Blinking at 3Hz	A DPP pairing is initiated via hardware or software configurations. (blinking at 1Hz after 3s upon a timeout; following the RSSI configuration logic upon a successful pairing)
	Following the RSSI logic*	A HaLow station is connected.
Mesh (Including Mesh + AP)	OFF	Wi-Fi HaLow module is not working.
	Blinking at 0.5Hz	Searching for available HaLow Mesh network.
	Following the RSSI logic*	Joined a HaLow mesh network.

*** HaLow RSSI Configuration Logic:**

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

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

In the HaLow AP mode:

Connection Status	HaLow LED Status
No Connection	OFF
Single station connection	Following the HaLow indicator definitions.
Multiple station connection	Following the RSSI logic based on the STA with the weakest signal strength.

In the HaLow STA mode:

Connection Status	HaLow LED Status
No Connection	OFF
Connected	Following the RSSI logic.

In the HaLow Mesh mode:

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

Factory Reset Status:

Factory reset initiated and in progress: Blinking at 3Hz.

1.8.3 Up & Down LEDs

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

Factory Reset Status:

Factory reset initiated and in progress: Blinking at 3Hz.

1.8.4 Restart LED

- Device not powered on or improperly powered: OFF.
- Factory reset initiated and in progress: Blinking at 3Hz.

1.8.5 Power LED

- Device properly powered on: Solid green.
- Device not powered on or improperly powered: OFF.
- Factory reset initiated and in progress: Blinking at 3Hz; upon successful factory reset: Transitioning to solid green.

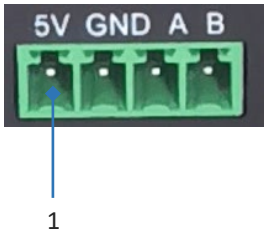
1.8.6 System LED

- Device not powered on or improperly powered: OFF.
- System failure/abnormality detected: Red.
- Device working properly: Solid green.
- Device boot/firmware upgrade in progress/factory reset: Blinking at 3Hz; upon successful factory reset: Transitioning to solid green.

1.8.7 Error LED

- Device working properly: OFF
- System failure/abnormality detected: ON
- Factory reset initiated and in progress: Blinking at 3Hz.

1.9 Serial Port



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

Table 1-4

No.	Signal	Device name	Port	Type	Description
1	VCC	/dev/ttyS0	COM0	P	5V output
2	GND			P	Ground
3	A			I/O	RS485 A signal
4	B			I/O	RS485 B signal

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

Input the following command to open the port with a serial port communication program (e.g., microcom) for serial communication:

```
~# microcom /dev/ttyS0 -s 9600
```

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

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

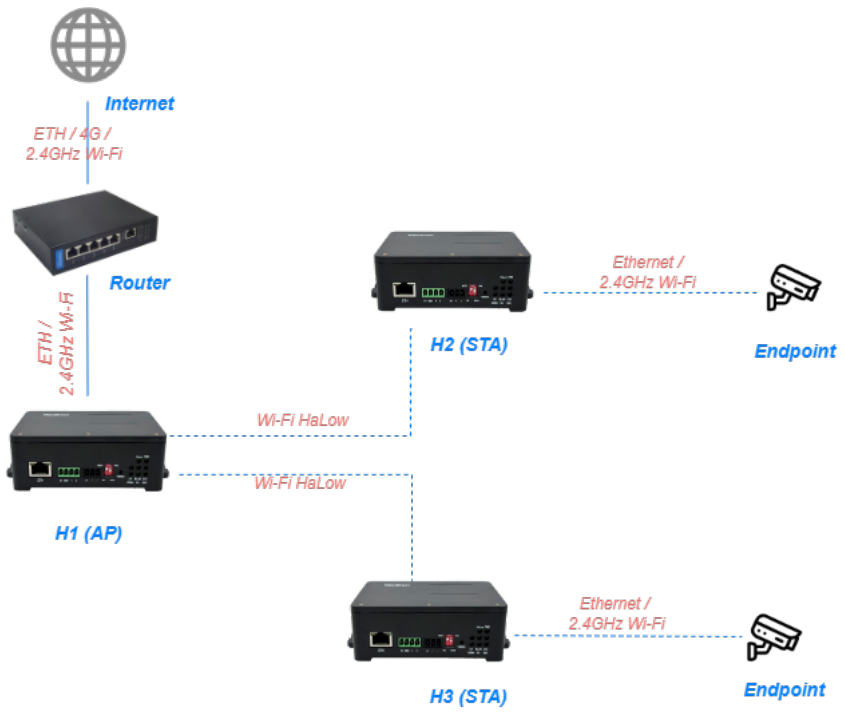
CHAPTER 2 GETTING STARTED

2.1 Network Architecture

HAP101 can operate as either an AP or STA in a Standard HaLow network, or a Portal or Point in a HaLow Mesh network. This flexibility allows the HaLow unit to be installed in a variety of environments and layouts.

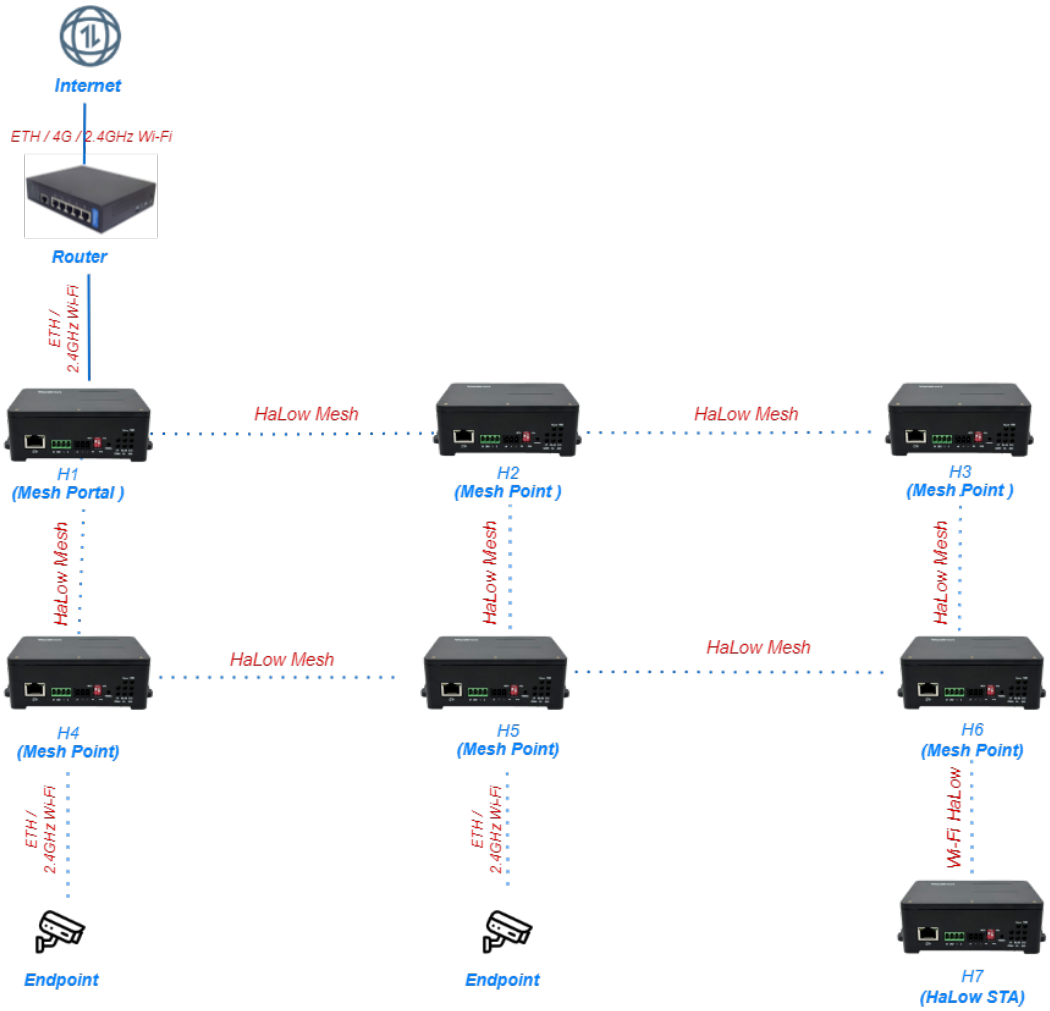
2.1.1 Standard HaLow Network

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



2.1.2 HaLow Mesh Network

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



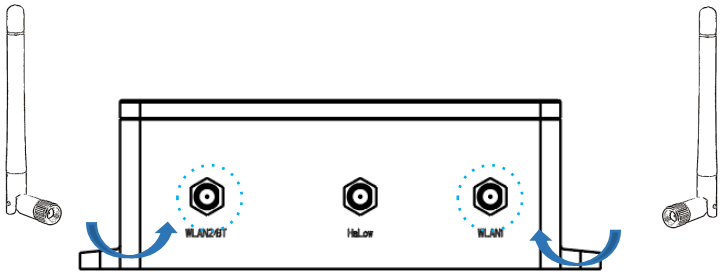
In this topology:

- If H1 itself offers the DHCP service, it is referred to as a **Mesh Portal**.
- If the upstream router offers the DHCP service, H1 is referred to as a **Mesh Point**.

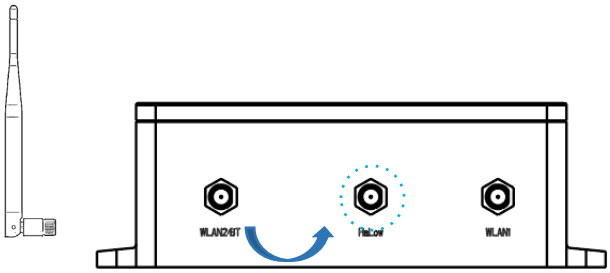
2.2 Setting up the Device

When mounting HAP101 on a vertical surface, please ensure that the device is oriented with the LED indicators pointing down. This positioning allows the LEDs to be visible to the user on the ground. For outdoor installations, it's highly recommended to use the waterproof kit to protect the electronics of the device.

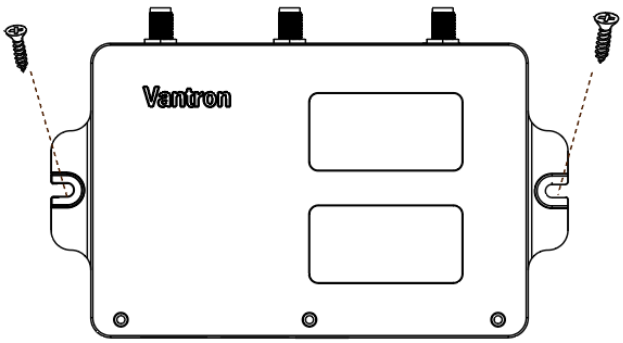
1. Install the shorter antennas to the WLAN antenna connectors (*labelled as WLAN1 and WLAN2/BT*).

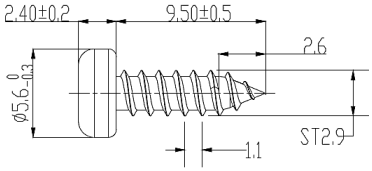


2. Install the longer antenna to the Wi-Fi HaLow antenna connector (*labelled as HaLow*).

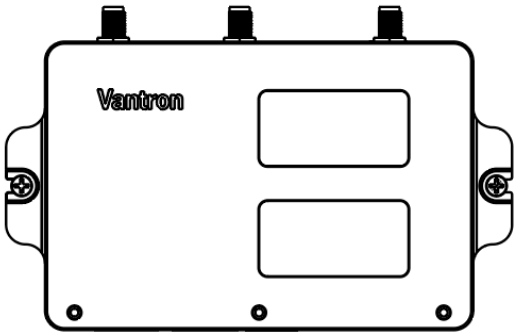


3. Depending on the material of the mounting surface, use two ST2.9 self-tapping screws (for mounting surfaces without provided screws) or two M3 x 8mm screws (for mounting surfaces with provided screws) to fix the device on the mounting surface.

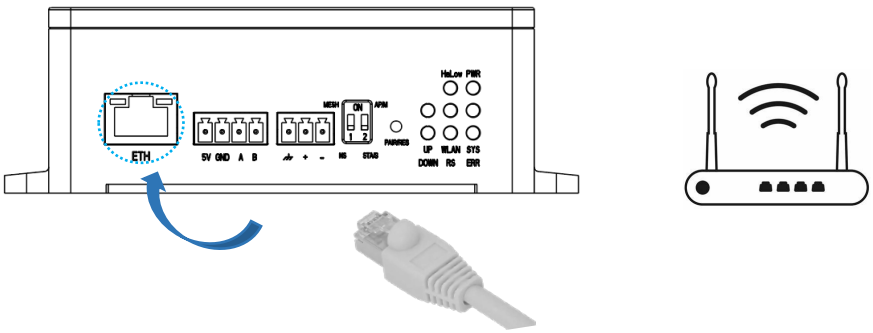




4. Tighten the screws and gently swing the device to make sure it is fastened.



5. When needed, connect the WAN port of HAP101 to a router using an Ethernet cable.



2.3 Powering up the Device

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

2.4 Quick Access to the Device

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

2.4.1 Host PC Login

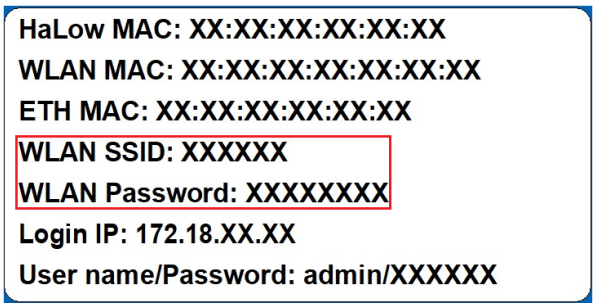
You can configure the network settings and manage the device on the web-based management portal (VantronOS) using a **Windows** host PC.

Follow the steps below to access the device through web portal login.

1. Connect the host PC:
   - Via Ethernet

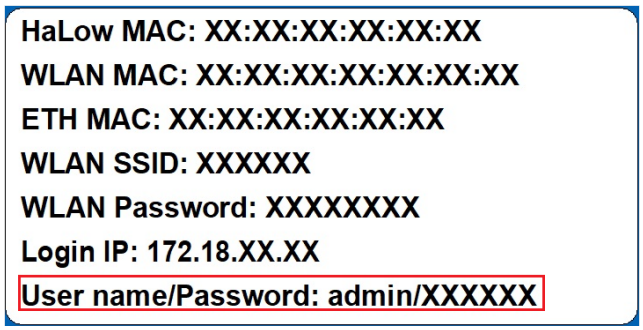
     Connect the host PC directly to the HAP101's Ethernet port using a standard Ethernet cable.
   - Via Wi-Fi

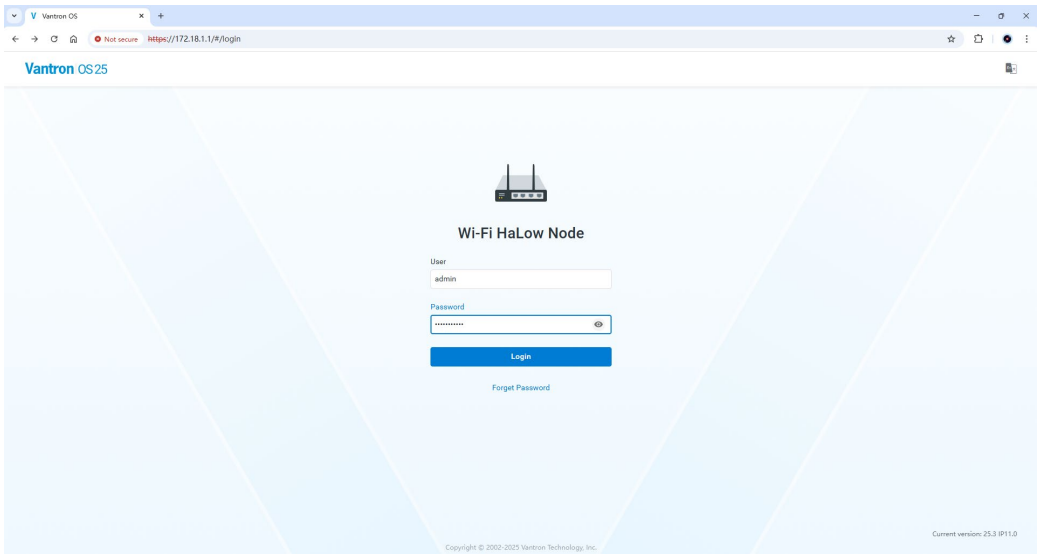
     Connect the host PC to the 2.4GHz Wi-Fi of the HAP101 using the default SSID and password provided on the device label.

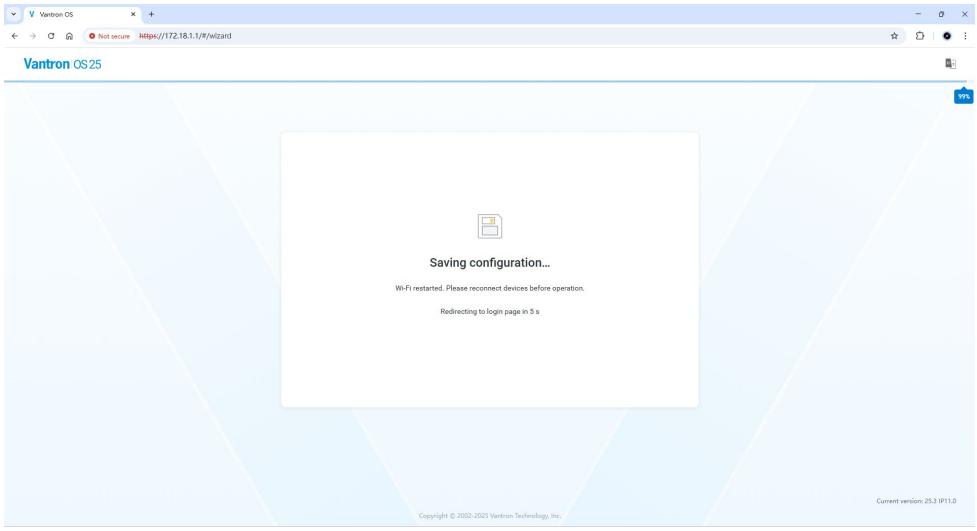
2. Enter the login IP in the browser of the host PC for device login.

   *If the address is blocked, please click **Advanced** to proceed.*
3. Log in to the management portal using the username and password on the device label.



4. Upon **first** login, the system will automatically launch a setup wizard that will guide you through configuring essential settings, including:
   - 2.4 GHz Wi-Fi AP (SSID, encryption, and password)
   - User password (you can click **Next** and choose “set up later” to change the password on the **System** page after login)
   - Time zone
5. Modify the settings as needed and wait about 20 seconds for new configurations to take effect.



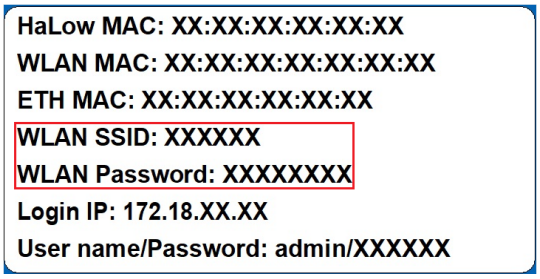
6. After the wizard finishes, the HAP101 will restart its Wi-Fi radio. If you have previously connected the host PC to the device via 2.4GHz Wi-Fi, you will need to reconnect the host PC to the device's network.
7. On the reloaded login page, enter the new password (if you changed it during the setup) to access the web portal.

2.4.2 Mobile Setup

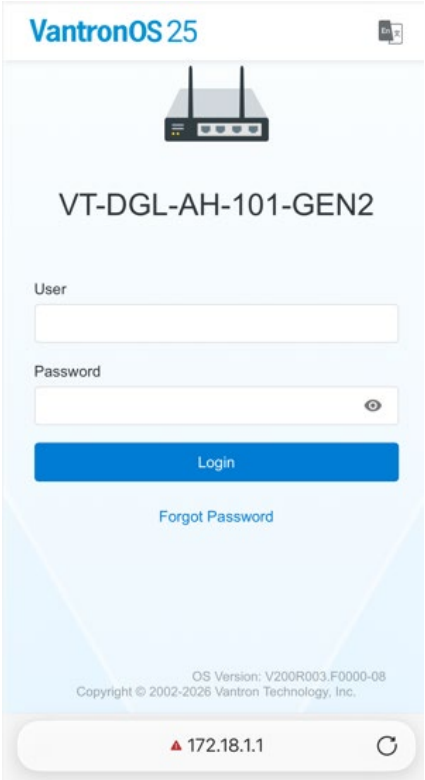
Mobile Web Tool is a quick-configuration utility for HAP101, designed for phones, tablets, and other mobile devices. It provides network diagnostics, mesh-node RSSI-threshold settings, and other essential functions.

Login Steps:

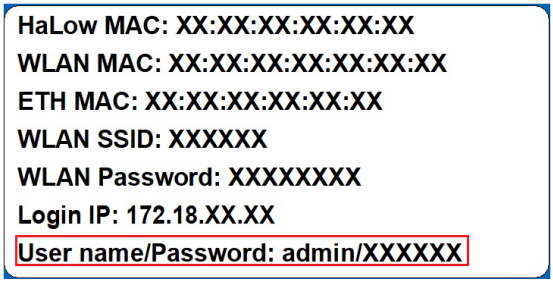
1. Make sure HAP101's 2.4 GHz Wi-Fi operates in AP mode.
2. Connect your phone, tablet or other mobile device to the 2.4GHz Wi-Fi using the provided SSID and password.



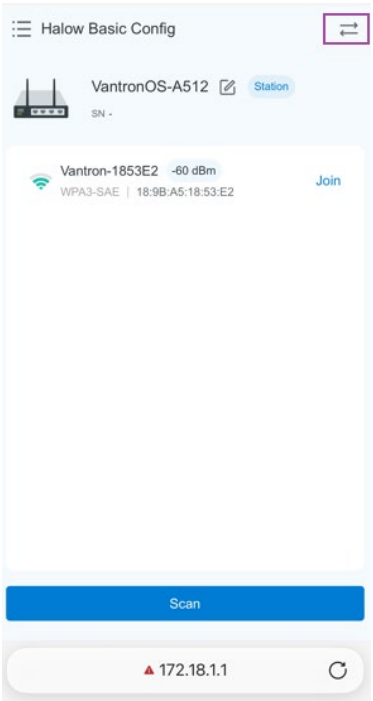
3. Open a browser, enter the HAP101's IP address, and the Mobile Web tool will load.

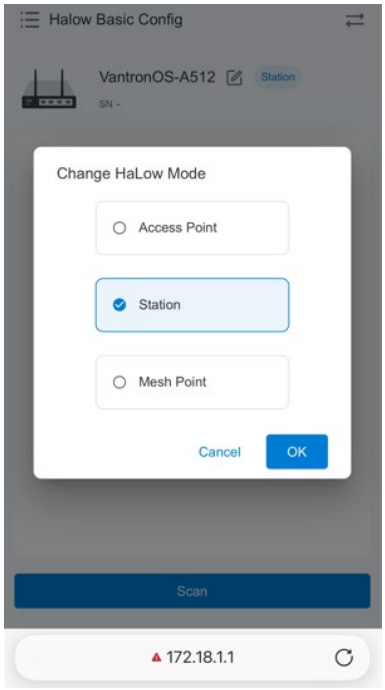


4. Log in to the management portal using the username and password on the device label.



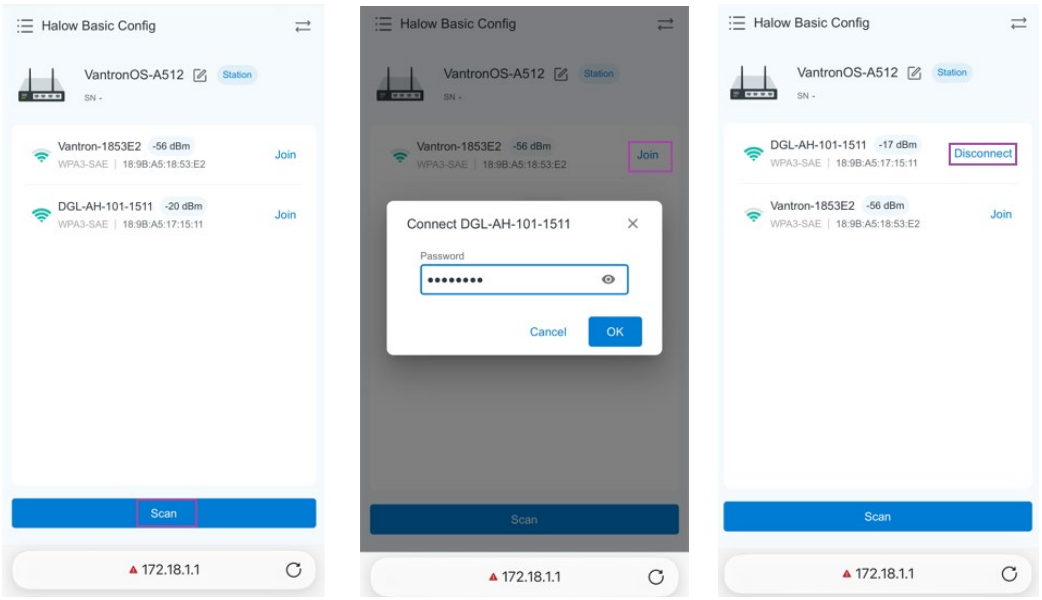
5. Once logged in, you can click the Swap icon in the top-right corner to change the HaLow operation mode.



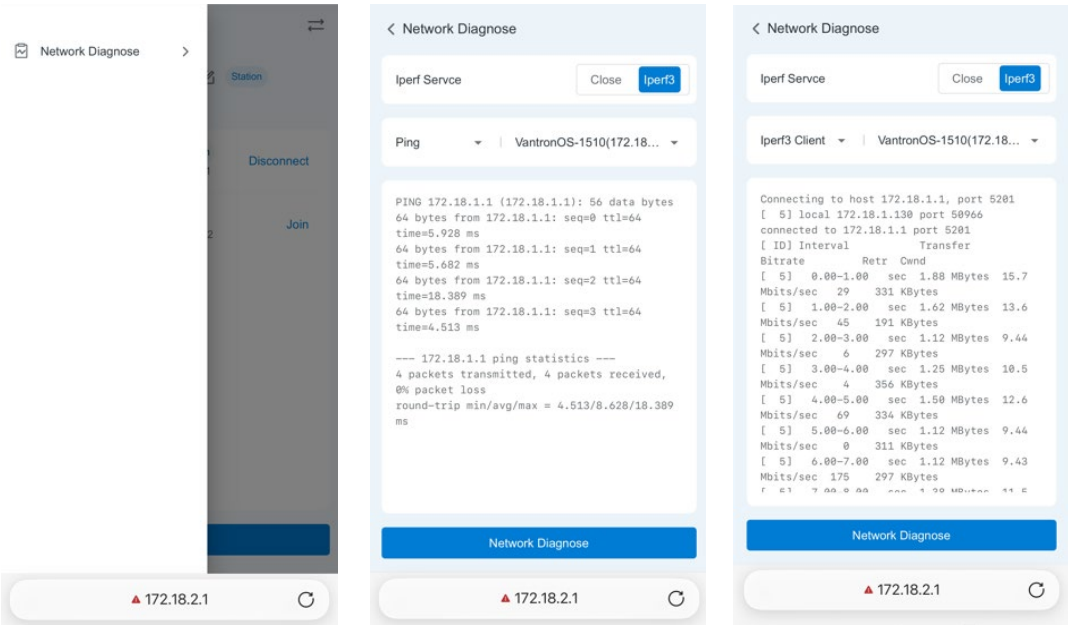


Available STA-Mode Configurations:

- Scan for nearby HaLow APs and establish a direct connection, streamlining the pairing process.



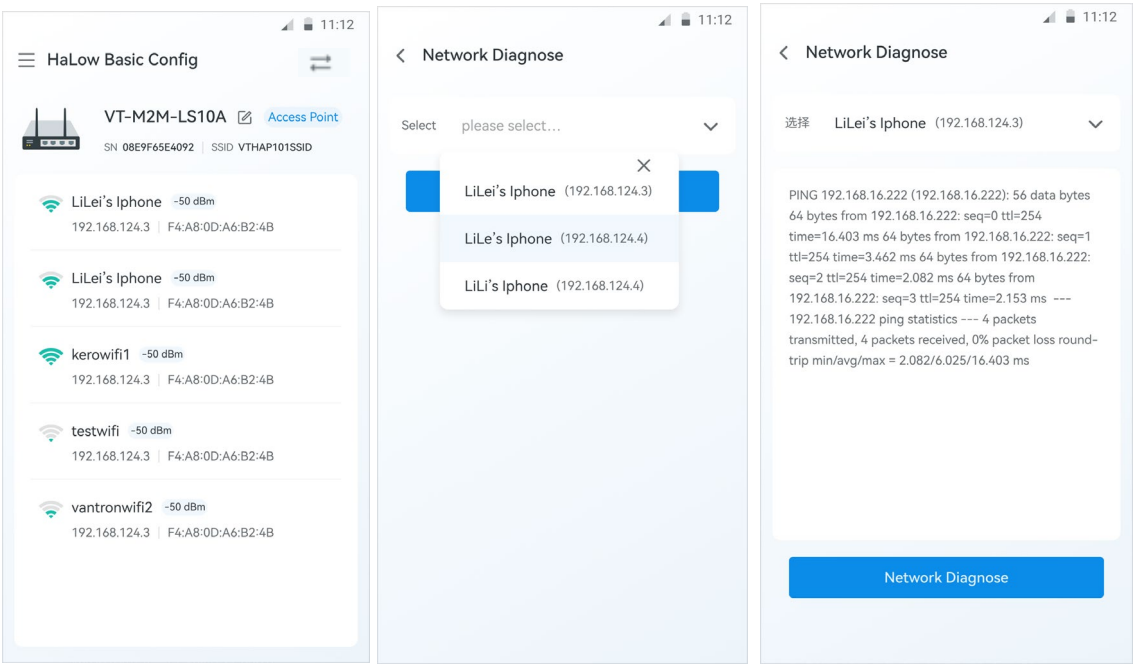
- Use ping/iperf3 for quick HaLow connectivity diagnostics; round-trip time and packet loss will be displayed.



To avoid IP conflicts, make sure the two HaLow units have different LAN IP addresses before testing.

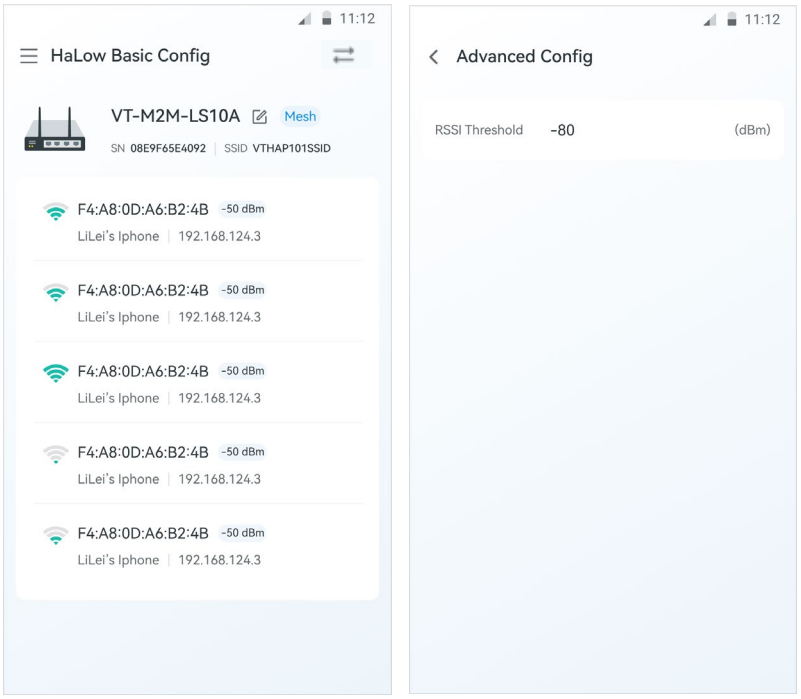
Available AP-Mode HaLow Configurations:

- List the stations connected to the current HaLow AP, displaying related information such as SS RSSI, MAC, and IP.
- Display quick network diagnostics tools, allowing users to evaluate the round-trip time and packet loss.



Available Mesh-Mode Configurations:

- View the neighboring nodes' info in the mesh topology, including SS RSSI, MAC, and IP.
- Configure the RSSI threshold of the current mesh-mode device for connecting to the nearest node. This can be used for optimizing the multi-hop use case as well.



2.5 Network Interface Status

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

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

When you change the 2.4GHz Wi-Fi to Client mode, ensure the Ethernet port remains in **LAN** mode for smooth device login.

Table 2-1 Network Interface Status in **HaLow Mesh Mode**

Network Interface	Working Mode	Description
Ethernet	WAN	Allows connection to an external router for: • External network access (MPP+MPs); **OR** • IP assignment & external network access (MPs only).
Wi-Fi HaLow	Bridged	The device operates as an MP.
	Not bridged	The device operates as an MPP.

Refer to Sections 3.4.4.1 for information about device login.

2.6 DPP Pairing

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

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

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

Note:

There will always be only one HaLow AP in a network. Each pairing process enrolls exactly one Access Point (AP) with one Station (STA). To add more STAs to the network, simply repeat the DPP pairing steps between the same AP and each new STA individually.

2.6.1 DPP Pairing via Hardware Setup

With the DIP switches in the correct position, pressing the button enables the DPP mode, which remains active for a maximum of **120** seconds.

Table 2-4 DIP Switch Setup for DPP Pairing

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

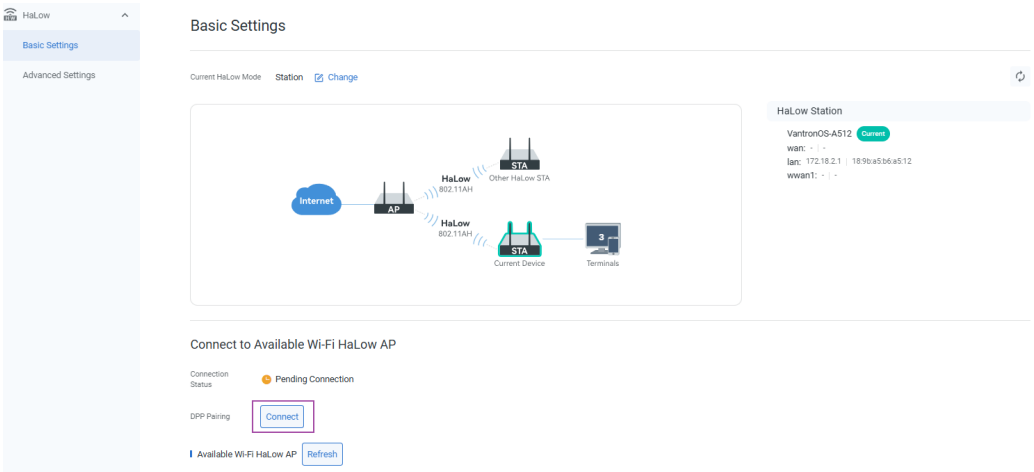
After setting up the DIP switches for both the AP and STA, proceed with the following HaLow DPP pairing procedure:

1. Make sure both HAP101 units are powered on and placed next to each other.
2. Short press (< 1s) the Pair/Restart button on one device to enable the pairing mode.
3. Repeat step 2 on the other device. Make sure the time interval between button actions on both devices is within 120 seconds.
4. Upon successful connection, both devices will exit the HaLow DPP mode, and the HaLow LED blinks regularly.
5. Repeat above steps for the same AP and each new STA, if applicable.
6. Move the devices to the desired locations after pairing.

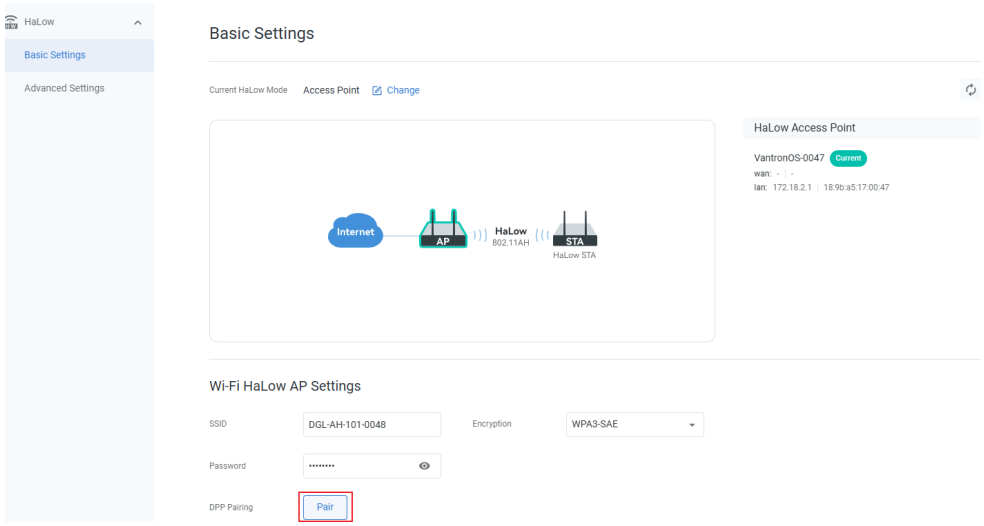
2.6.2 DPP Pairing via Software Setup

The software setup is performed through the VantronOS web management portal. Given that the device is factory-set to HaLow STA mode, you may need to switch one unit to HaLow AP mode within VantronOS as described in Section 3.4.2. Then proceed with the following steps:

1. Prepare two HAP101 units, one in AP mode and one in STA mode.
2. Make sure both units are powered on and placed next to each other.
3. Refer to Section 2.4.1 to log in to the VantronOS web portal on two separate PCs.
4. On both PCs, navigate to the **HaLow** menu tab in VantronOS.
5. For the **STA**: In the **Connect to Available Wi-Fi HaLow AP** section, click **Connect** next to **DPP Pairing**.

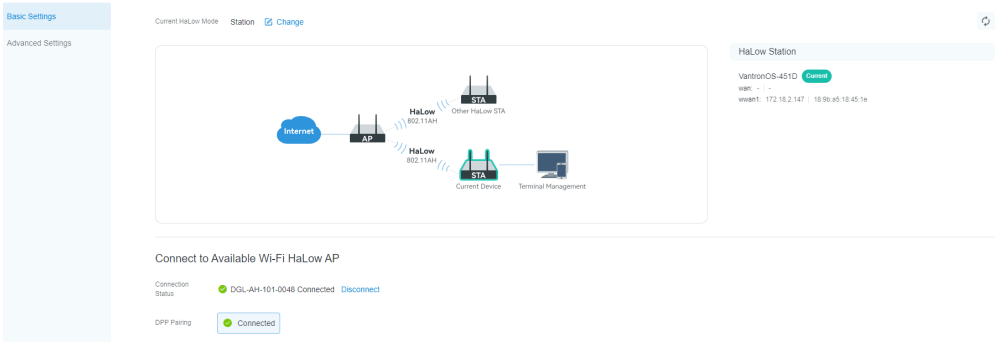


6. For the **AP**: In the **Wi-Fi HaLow AP Settings** section, click **Pair** next to **DPP Pairing**.

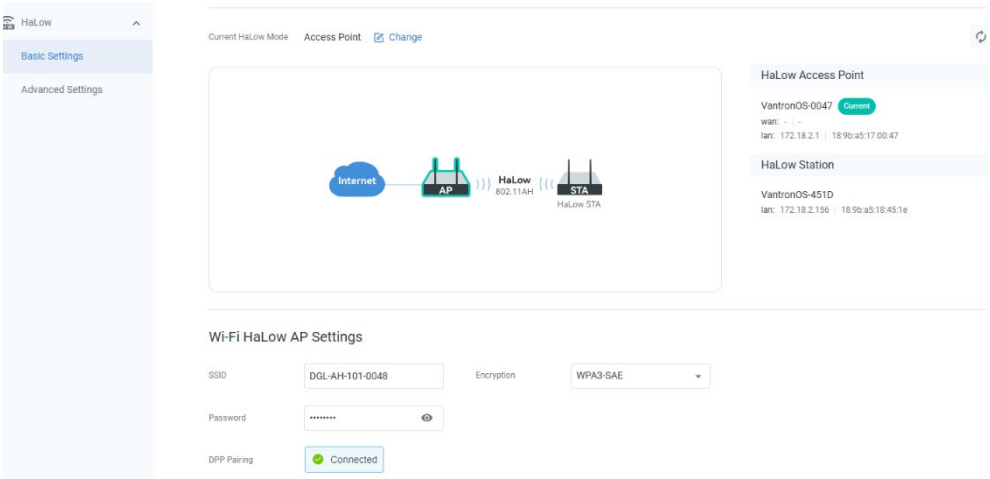


7. Ensure the interval between clicking the buttons is **less than 120 seconds**. A **Connected** status will confirm the pairing.

   STA-side connection:



   AP-side connection:



8. Brief connection information will display next to the connection topology.
9. Repeat above steps for the same AP and each new STA, if applicable.
10. Move the devices to the desired locations after pairing.

2.6.3 Exiting DPP Pairing Mode

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

- A HaLow connection is successfully established.
- The target device fails to enable the pairing mode within **120 seconds** after the first device does.
- The HaLow connection between both devices fails.

2.7 Quick Mesh Networking

By default, HAP101 units are pre-configured with common Mesh settings. Once the Mesh mode is enabled, the unit will automatically form or join a HaLow Mesh network with the same settings, **regardless of** the time elapsed.

To modify the Mesh settings of a unit, refer to the description in Section 3.5.4.

Table 2-5 DIP Switch Setup for Quick Mesh Networking

Device	Switch 1	Switch 2	Result
H1	Mesh	AP/Portal*	Quick HaLow Mesh configuration in the MPP mode
H2	Mesh	STA/Point	Quick HaLow Mesh configuration in the MP mode
Hn	Mesh	STA/Point	Quick HaLow Mesh configuration in the MP mode

* Based on your network deployment, refer to Section 3.5.4.1 to determine if the Mesh network requires an MPP.

After setting up the DIP switches on the target units, proceed with the following procedure:

1. Power on the units.
2. Short press (< 1s) the Pair/Restart button both these units to activate the **Mesh configuration**.
3. If no MPP is present, connect a designated MP to an external router for IP assignment.
4. Additional MPs can be added to the network at any time by repeating this procedure.

2.8 SSH and Serial Console Access

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

Table 2-6 Access Options

Method	Host PC Connection	Login Address/Parameters
Option 1 (SSH)	Host connected to the device's LAN network (via Ethernet or 2.4GHz Wi-Fi).	HAP101's LAN IP
Option 2 (SSH)	Host's WAN interface on the same IP subnet as HAP101's WAN interface (Ethernet or 2.4GHz Wi-Fi client)	HAP101's WAN IP
Option 3 (Serial console)	Host connected to HAP101's debug UART	57600, 8N1

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

Option 1 applies in most cases.

Option 2 applies when the device's Ethernet port is configured as a WAN interface or the 2.4GHz Wi-Fi is in client mode, and both the device and the host PC are connected to the same upstream DHCP server.

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

Example: SSH login via **LAN IP**

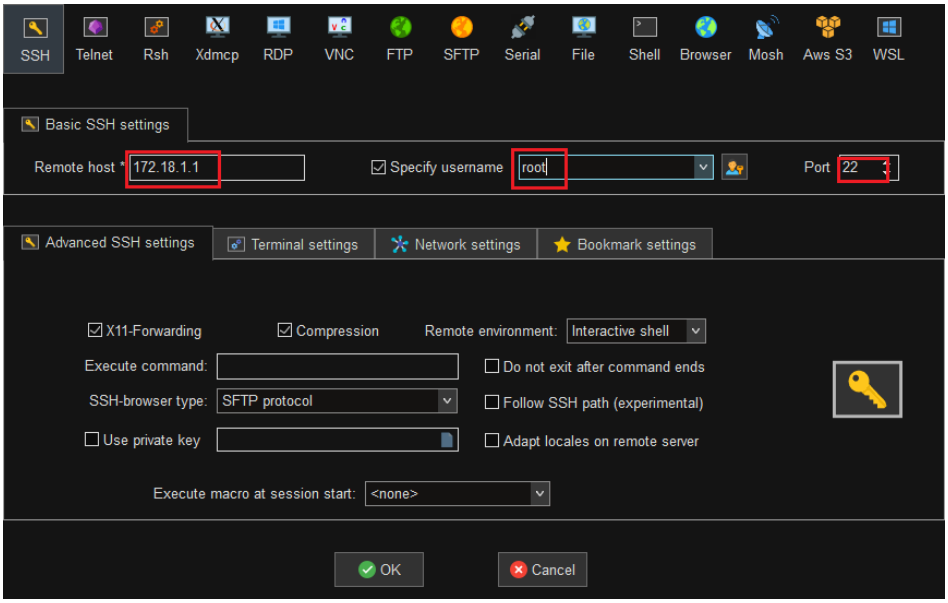
1. Connect the host PC to HAP101's LAN network via Ethernet or 2.4GHz Wi-Fi.
2. Install SSH client if it is not available.
   - **Windows host**:
     - PuTTY
     - Tera Term
     - MobaXterm

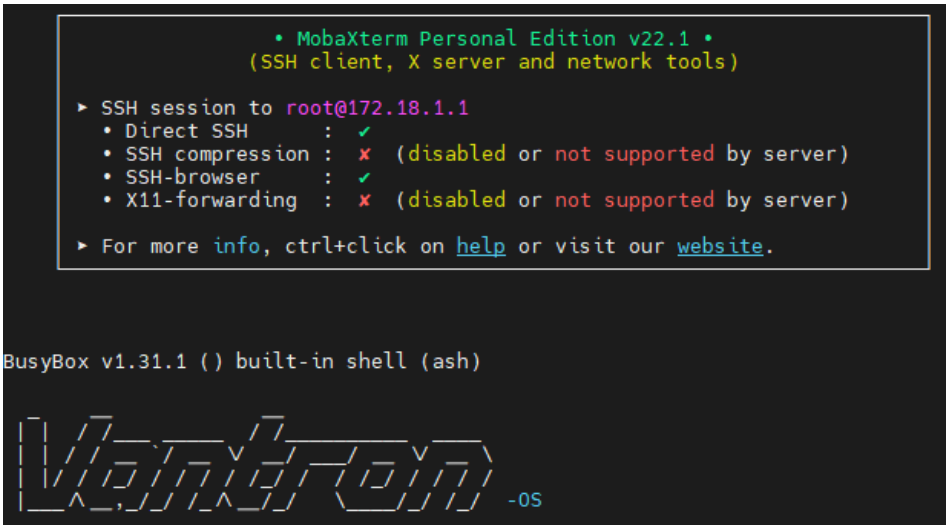
- **Linux host**:

```
$ sudo apt-get update

$ sudo apt-get install ssh
```

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





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

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

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

2.9 Interfacing with Vantron Gateway Manager

BlueSphere Gateway Manager (hereinafter referred to as "GWM") is a cloud-based management portal that empowers organizations to seamlessly provision, monitor, and manage Vantron IoT communication devices, including gateways, routers, and DTUs. By leveraging BlueSphere GWM, organizations can streamline device setup, ensure real-time visibility into device performance, and effortlessly control device configurations. This contributes to enhanced operational efficiency and improved decision-making.

To use BlueSphere GWM for remote management of HAP101, ensure you are an authorized BlueSphere GWM user with a valid customer ID. Refer to Section 3.6.4.1 for instructions of adding your device to BlueSphere GWM for centralized management.

2.10 Factory Reset

There are two options to factory reset the device, one from the hardware perspective and the other from the software perspective. Once factory reset, device configurations, user data, and user-installed applications will be cleared and the device will restore to Wi-Fi HaLow STA mode and 2.4GHz Wi-Fi AP mode by default.

Please exercise caution when performing a factory reset, as you will need to re-log in to the device via the debug port afterward.

2.10.1 Hardware Reset

1. Long press (12-20s) the Pair/Restart button.
2. Release the button.
3. LED indicators will start flashing. If not, go back to step 1 again.
4. Wait about 10 minutes before the process completes.

2.10.2 Software Reset

1. Log in to VantronOS by referring to Section 2.4.
2. Navigate to **System > System Maintenance > Device Maintenance**.
3. Under **Configuration Management**, click the **Download Backup** button to save a backup of the current device configurations.
4. Move the cursor up and click the **Reset** button.
5. The progress bar will display the reset status. The process takes approximately 10 minutes to complete.

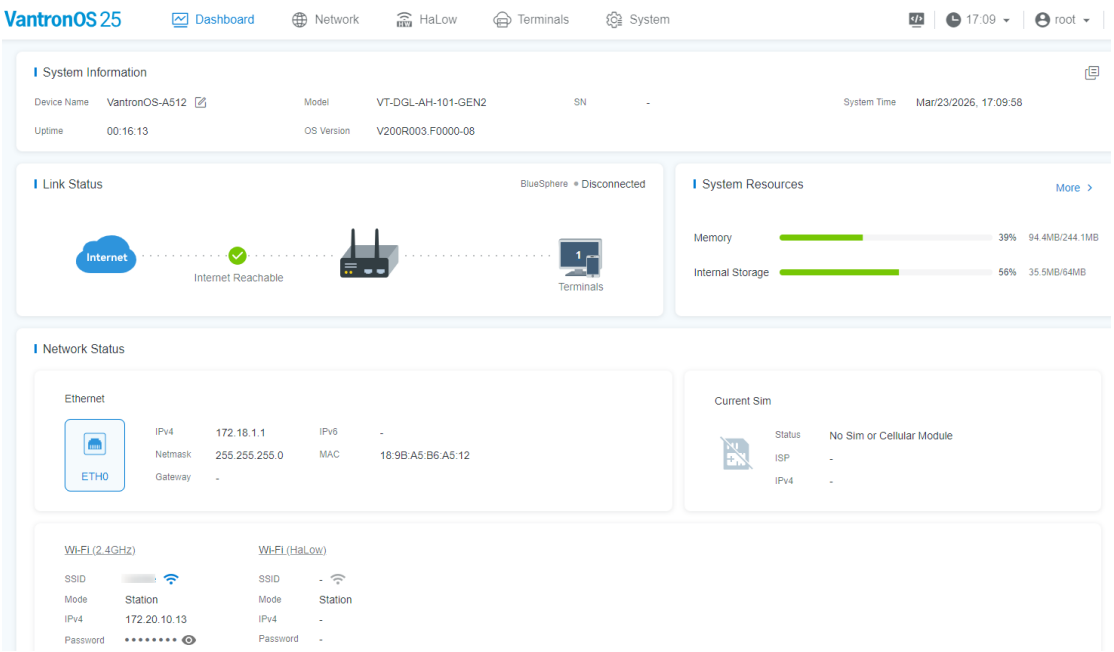
CHAPTER 3 DEVICE SETUP IN VANTRONOS

3.1 Introduction to VantronOS

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

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

3.1.1 Web Overview



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

Dashboard: Displays general device information and dynamic status updates.

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

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

Terminals: Provides information of connected end nodes.

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

Terminal: Provides command-line access to the device shell for debugging.

Time Settings:

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

Refer to Section 3.6.1.2 for modifying the time settings.

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

- Toggle Edge Computing functionality
- Log out

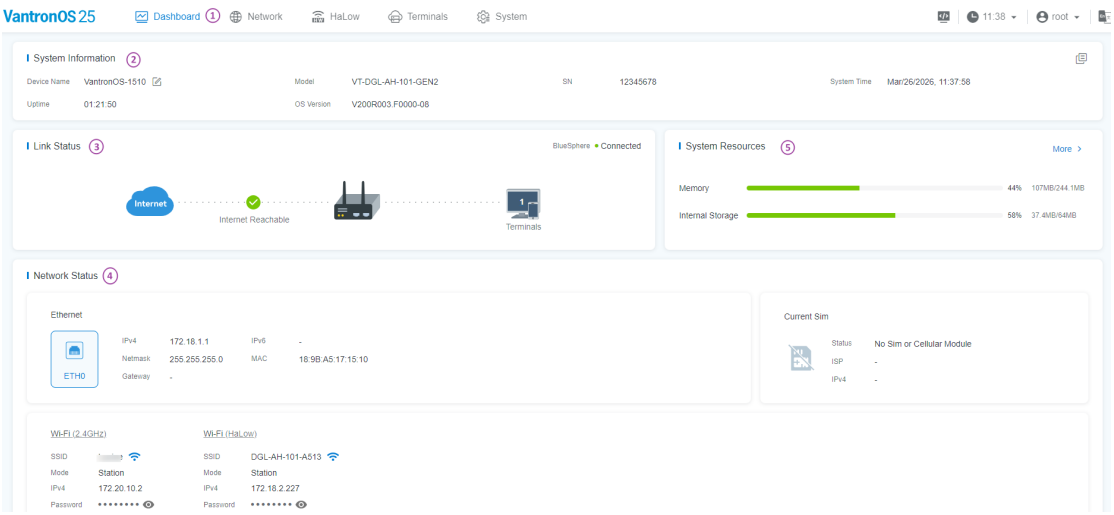
Language Toggle: English ⇄ Chinese.

3.1.2 Language Change

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

3.2 Dashboard

The **Dashboard** provides an overall information of the HAP101, including the system information, network topology, device resource usage, interface connection status.



Description:

1. **Menu Tabs**—Highlights the active menu in blue.
2. **System Information**—Includes the device name, model, SN, current system time, link uptime, and OS version.

   - Clicking the pencil icon next to the device name allows you to modify the device name as needed.
   - Clicking the copy icon in the upper right corner copies all system information.

3. **Link Status**—Shows a simplified network topology of the current device.

   - Clicking the connected terminal count navigates to the end node page, where detailed end node information is displayed.

4. **Network Status**—Displays the live status for each network interface.

   - Ethernet (LAN default): IPv4 and IPv6 addresses, subnet mask, and MAC address.
   - 2.4GHz Wi-Fi/Wi-Fi HaLow: Operation mode (e.g., AP or STA) and associated network details.
   - Cellular: Mobile network information, if supported.

5. **System Resources**—Shows device performance metrics, including memory usage (used/total) 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, 2.4GHz 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.

3.3.1 Interface Settings

Interfaces on the HAP101 are categorized as either WAN or LAN.

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

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

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

Changing an interface's operating mode (e.g., LAN to WAN) may alter its IP address or disable its local network access. In such cases, you may need to **reconnect** your host PC to an active LAN interface (e.g., switch connection from Ethernet to Wi-Fi AP) to restore access to the device.

Ensure that you unplug the Ethernet cable whenever you switch the Ethernet mode.

3.3.1.1 WAN

The WAN interface page includes the following three functionalities:

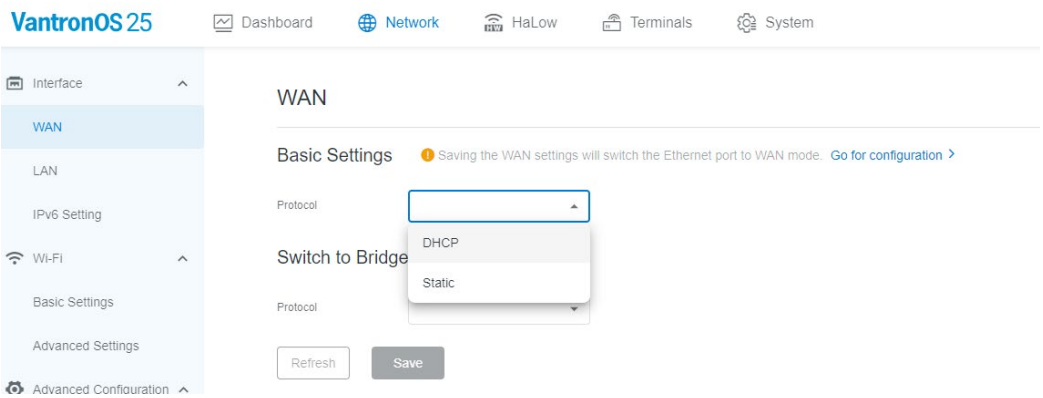
1. **Basic IP configuration** – Sets the interface to DHCP or Static mode.
2. **Interface bridging**–Converts the bridged interface to a WAN interface and places it on the same network level as other LAN interfaces, thereby causing it to lose its local management capability.
3. **Link priority IPv4**–Displays all upstream links and the Ethernet port status, lets you change their priority.

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

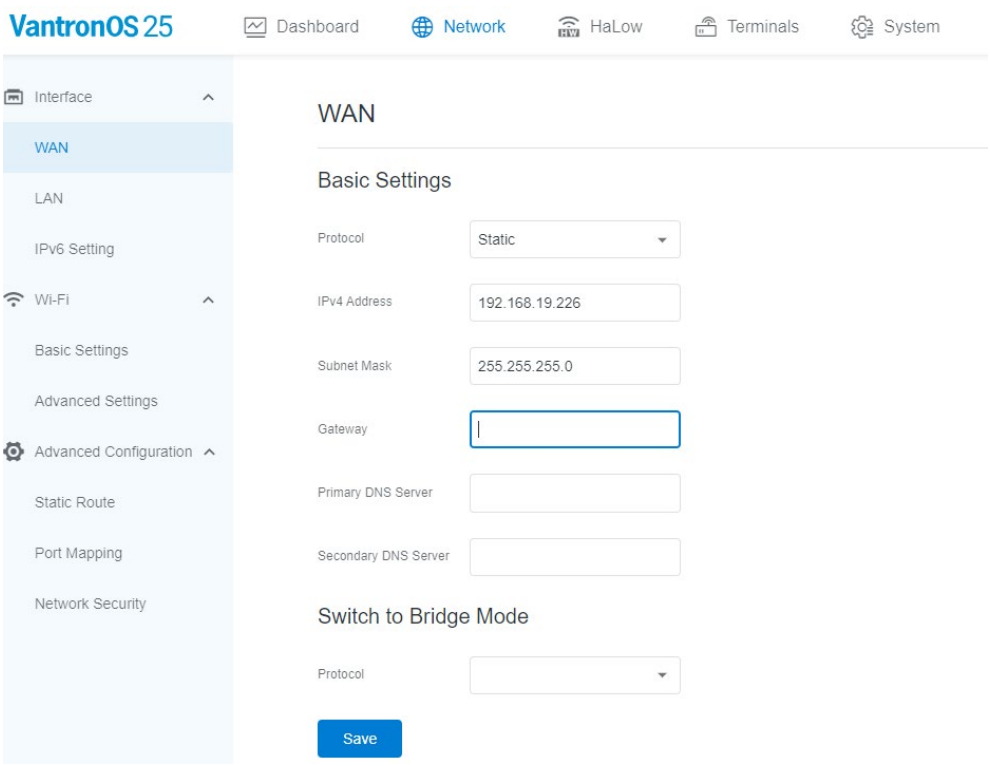
The above settings apply to WAN interfaces only. Saving a WAN configuration switches the Ethernet port to WAN mode. Therefore, it is recommended that you use the 2.4GHz Wi-Fi AP for device management.

- **Basic IP Configuration**

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



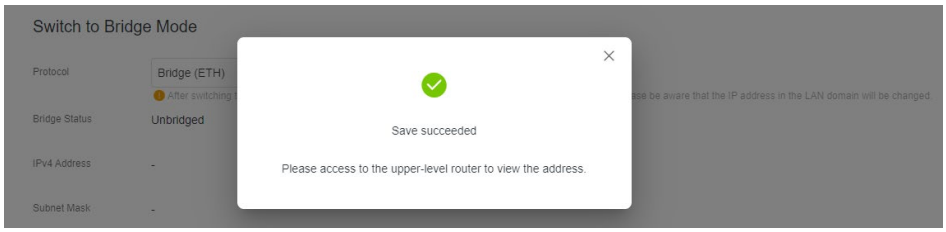
Static: You need **manually** configure the IP address for the interface, inducing the IP address, subnet, gateway, and DNS.



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

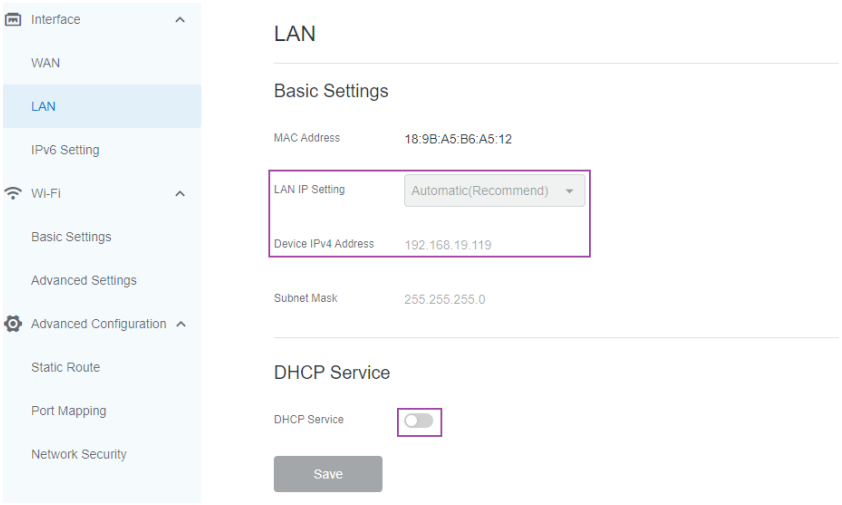
- **Interface Bridging**

You can choose to bridge the 2.4GHz Wi-Fi/Ethernet/HaLow mesh interface. When an interface is bridged, it is switched to WAN mode and placed on the same network level as other LAN interfaces, thereby losing its local management capability. **Bridging an interface other than the Ethernet port also automatically switches the Ethernet port to WAN mode, allowing connection to an upstream router via Ethernet.**



After bridging:

- The bridged interface and Ethernet port switch to WAN mode, while the LAN interfaces **stop** providing NAT and DHCP services to connected devices.
- The bridged interface obtains IP address from the upstream DHCP server, just like other LAN interfaces, leaving the device with only **one** effective LAN IP.



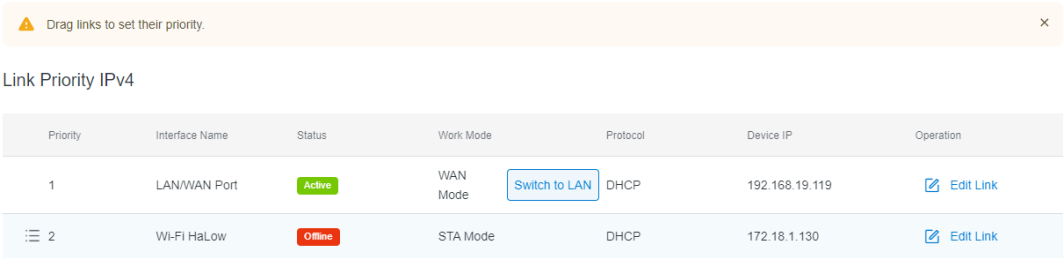
- Devices connected to the LAN interface of the HAP101 will obtain IP addresses from the upstream DHCP server. Consequently, to manage the device, you must retrieve its IP address from the upstream DHCP server.
- If you connect the device's Ethernet WAN port to an upstream router before the bridging, the IP address assigned by the router will be displayed in seconds.
- To **cancel interface bridging**, unplug the Ethernet cable first, then enable the **DHCP service** or switch the Ethernet port to LAN mode from the **Link Priority** section.

- **Link Priority**

The default link detection and data forwarding are prioritized based on the following rule: Ethernet (WAN) > Wi-Fi HaLow (STA) > 2.4GHz Wi-Fi (Client).

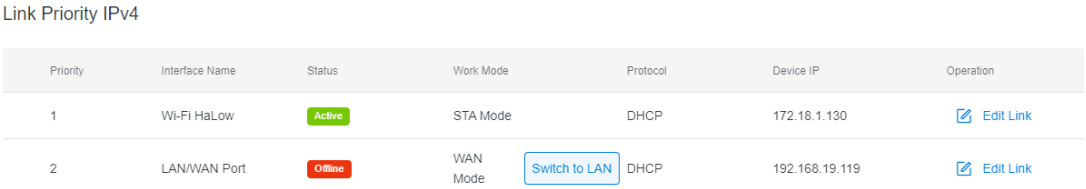
To manually set the network priority:

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

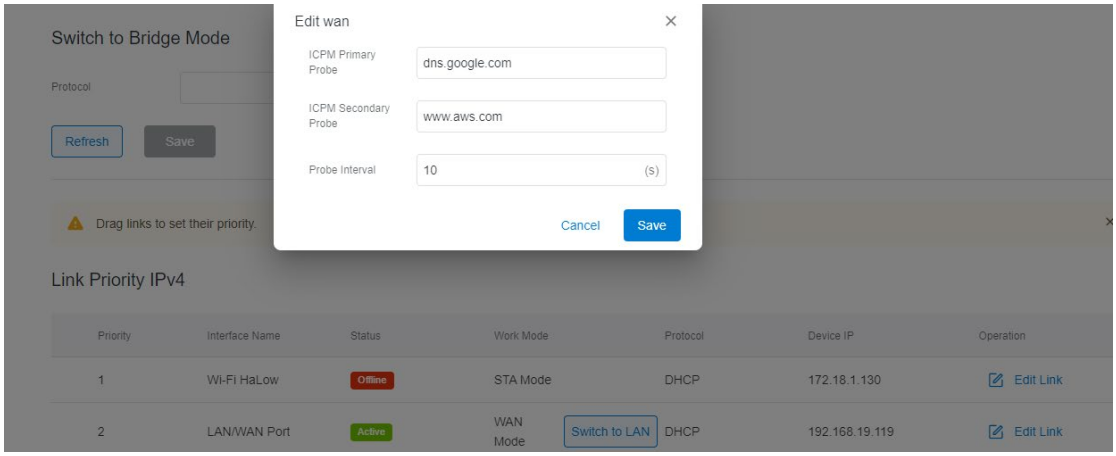


The screenshot is for illustration only. In a typical deployment, individual HaLow stations would not be connected as standalone units to an external network.

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



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

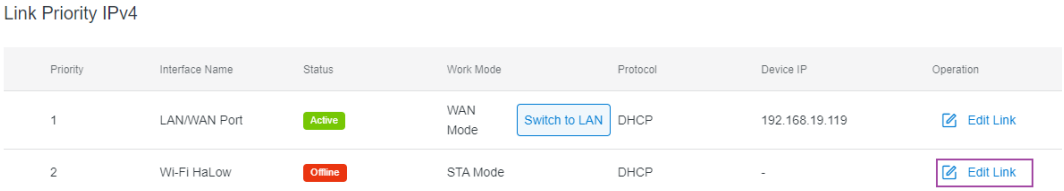


Editable fields include: primary & secondary probe addresses, and probe interval.

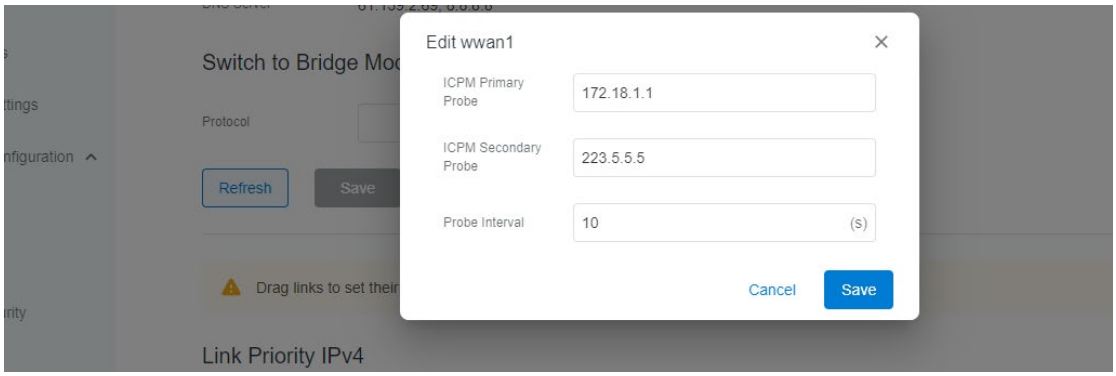
- **Link Diagnosis**

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

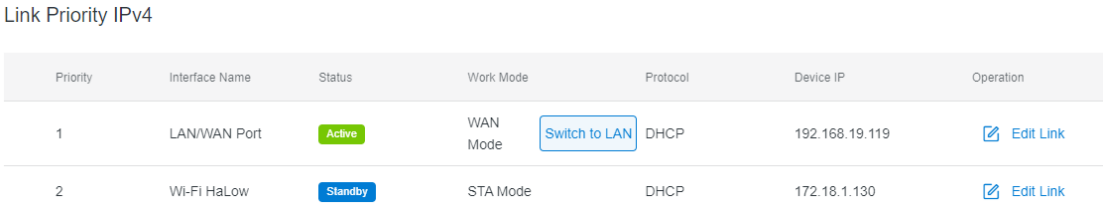
1. Locate the target link, and click **Edit Link**.



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

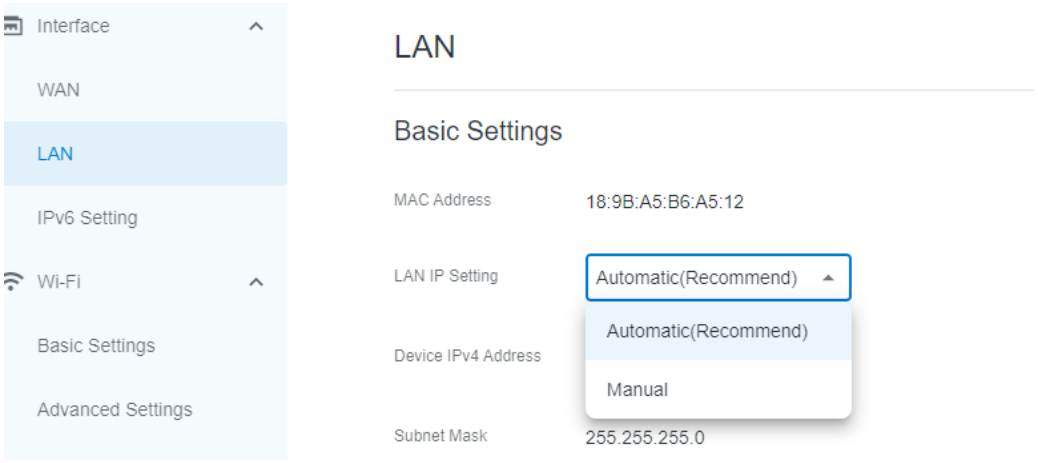


3. Check the link status to verify if it becomes reachable.



3.3.1.2 LAN

The HAP101 defaults to the 172.18.1.1 subnet for IP assignment.



- **Subnet Conflict**

A subnet conflict may occur when a Vantron communication device (router/gateway/HaLow AP) acts as a DHCP server for the HAP101's uplink interface and its factory LAN address (172.18.1.1) overlaps with the HAP101's default LAN subnet.

As a best practice, we recommend reconfiguring the HAP101's LAN IP address to a different subnet when connecting to a Vantron communication device to avoid IP conflicts.

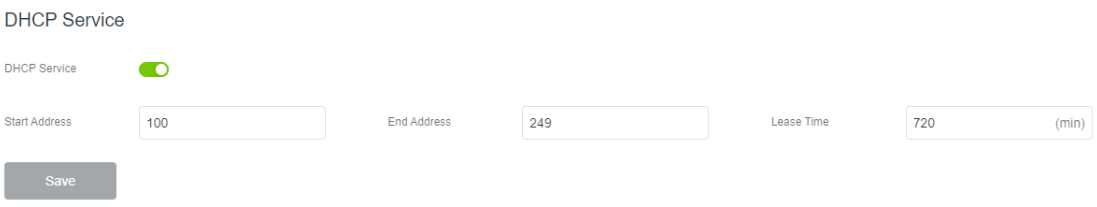
Manual IPv4 address configuration requires entering an IPv4 address and the subnet mask. If you modify the device's LAN IP address, reconnect the host PC to the device to maintain access.

- **DHCP Service & DHCP Reservation**

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

Editable fields under **DHCP Service**:

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

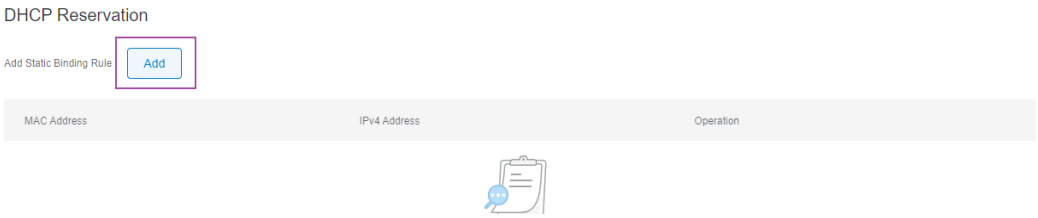


DHCP Reservation allows a DHCP server to reserve a specific IP address for a particular device (client) based on its MAC address. When enabled, the server will always assign the same IP address to that device whenever it connects to the network, optimizing the network's IP address space and enhancing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

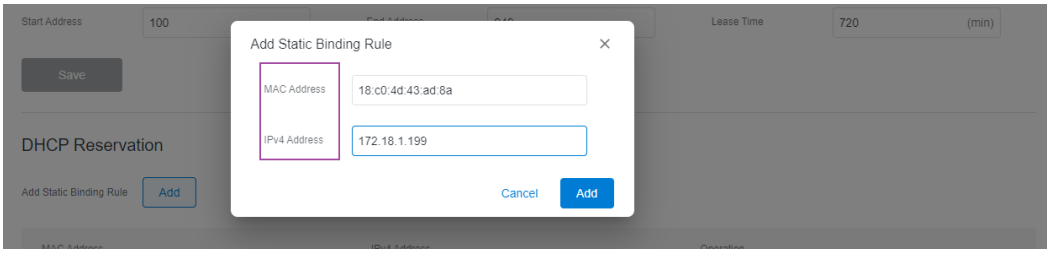
By adding a DHCP reservation rule to the HAP101, the specified client device will maintain the allocated IP address to reduce configuration errors.

Steps of adding a DHCP reservation rule:

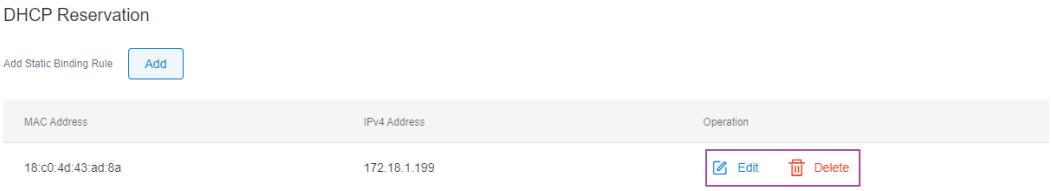
1. Click **Add** under **DHCP Reservation**.



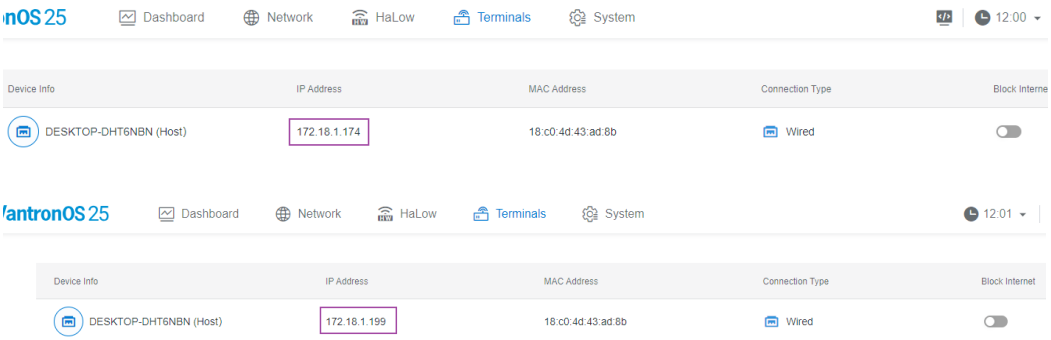
2. Enter the client's MAC address and allocate an IP between the start and end addresses specified under **DHCP Service**.



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



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



3.3.1.3 IPv6 Settings

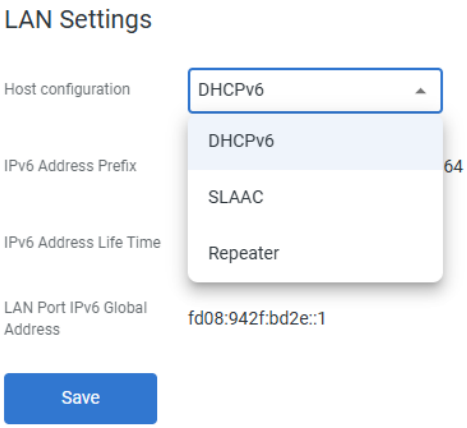
IPv6 (Internet Protocol version 6) is an advanced network layer protocol succeeding IPv4. It is designed to solve IPv4 address exhaustion and support enhanced networking features. It provides 128-bit addresses, eliminating the need for NAT and enabling end-to-end connectivity.

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

When IPv6 is enabled:

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

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



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

3.3.2 Wi-Fi

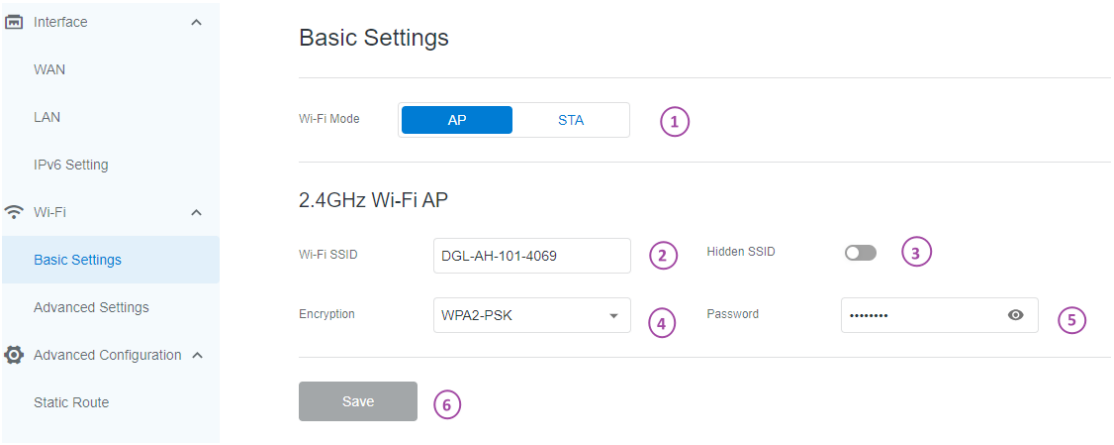
During the initial login wizard, the device's 2.4 GHz Wi-Fi is pre-configured as an access point (AP). You can modify these settings as needed.

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

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

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

3.3.2.1 AP-Mode Basic Settings

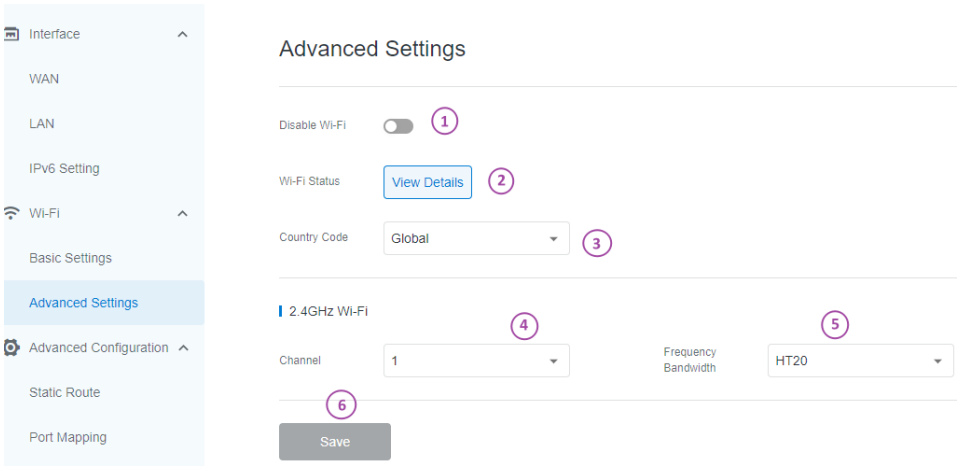


Description:

1. Click **AP** and confirm the action in the pop-up to enable the AP mode.
2. Wi-Fi SSID—The Wi-Fi AP's name.
3. Hide SSID—Once hidden, clients cannot scan the device's SSID and must manually enter the exact SSID and password to connect.
4. Encryption—The basic protocols for establishing secure communication. (None, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK)
5. Password—Credential for connecting the device's Wi-Fi.
6. Click **Save** to allow changes to tack effect.

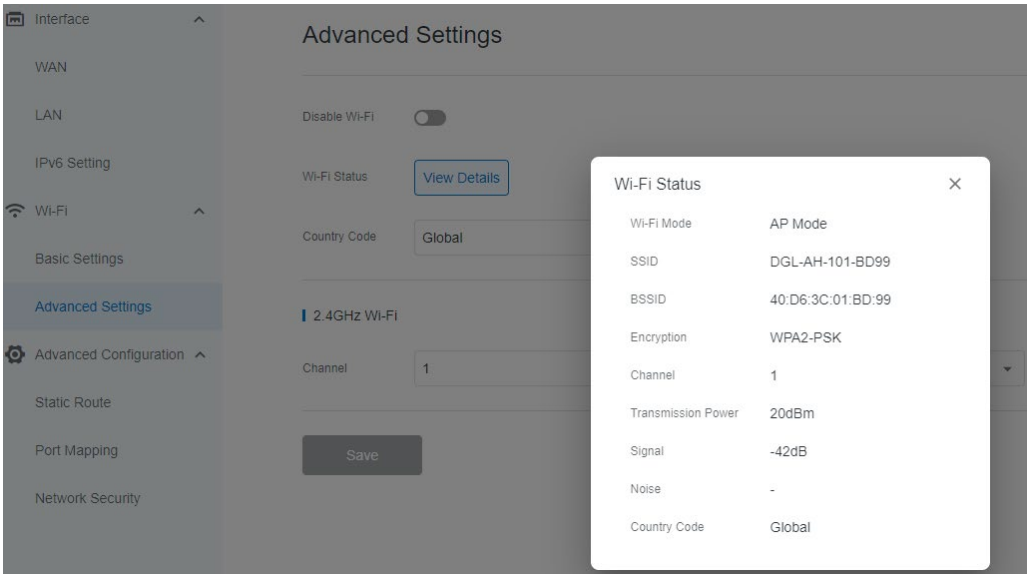
3.3.2.2 AP-Mode Advanced Settings

Before you proceed, ensure 2.4GHz Wi-Fi is set to AP mode in **Basic Settings**.



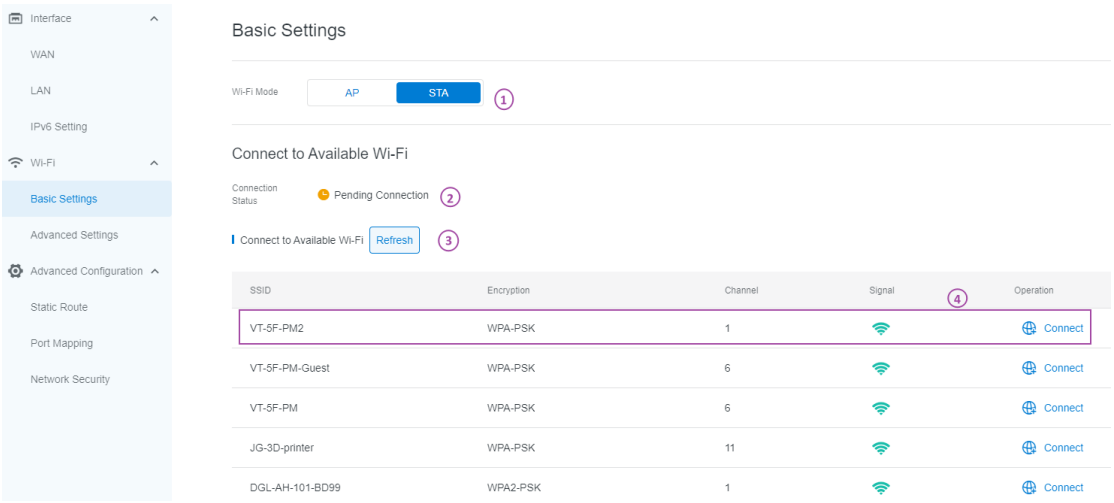
Description:

1. Toggle off the 2.4GHz Wi-Fi.
2. Wi-Fi Status—Clicking **View Details** will display the detailed Wi-Fi settings of the device, including Wi-Fi mode, SSID, encryption, channel, transmit power.



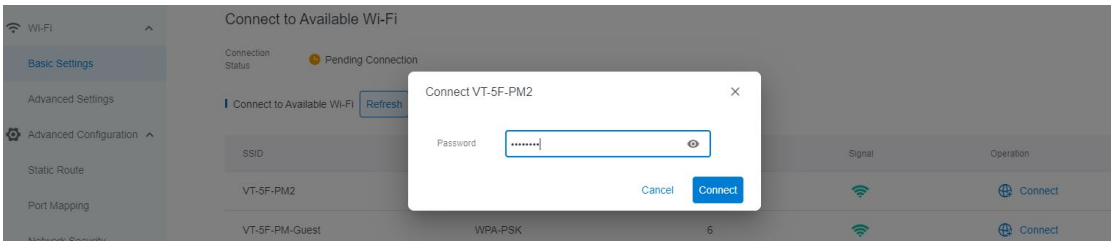
3. Country code (‘global’ by default)
4. Channel options
5. Frequency bandwidth (‘HT20’ by default)
6. If you have modified the parameters, click **Save** to apply.

3.3.2.3 Client-Mode Basic Settings

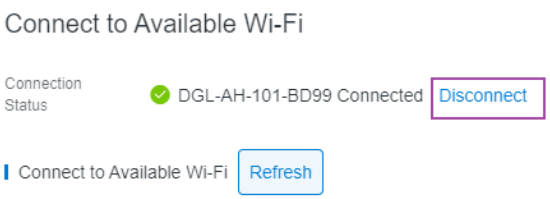


Description:

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

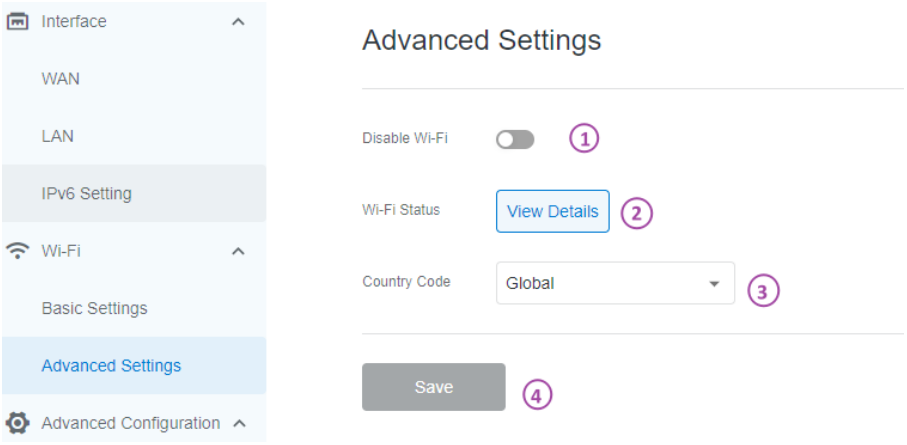


*When the device successfully establishes a connection to the target AP, **Disconnect** becomes available, next to the connected SSID.*



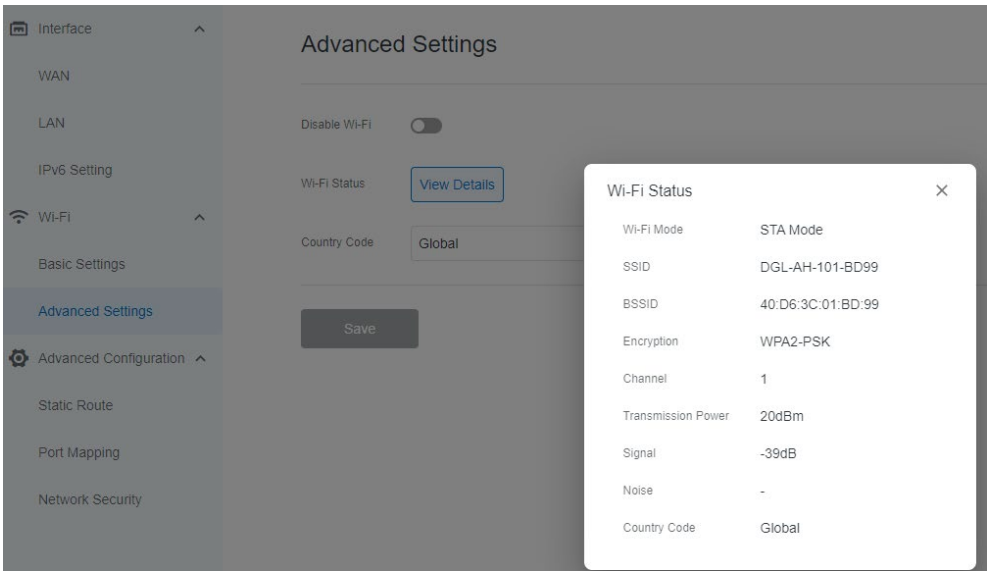
3.3.2.4 Client-Mode Advanced Settings

Before you proceed, ensure 2.4GHz Wi-Fi is set to STA mode in **Basic Settings**.



Description:

1. Toggle off the 2.4GHz Wi-Fi.
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, channel, transmit power, etc.



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

3.3.3 Static Route

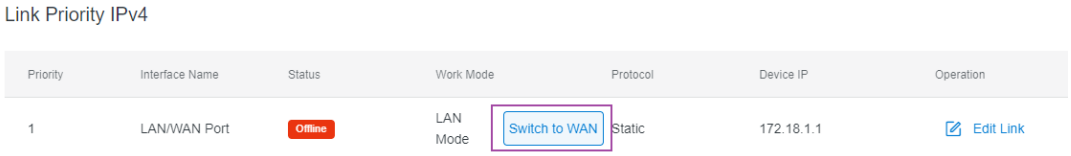
Static routing is a manual network configuration method that uses explicitly defined paths to direct traffic through specific interfaces. This provides precise control over routing behavior and is particularly useful for multi-WAN load balancing, traffic segregation, and backup link configuration.

Example:

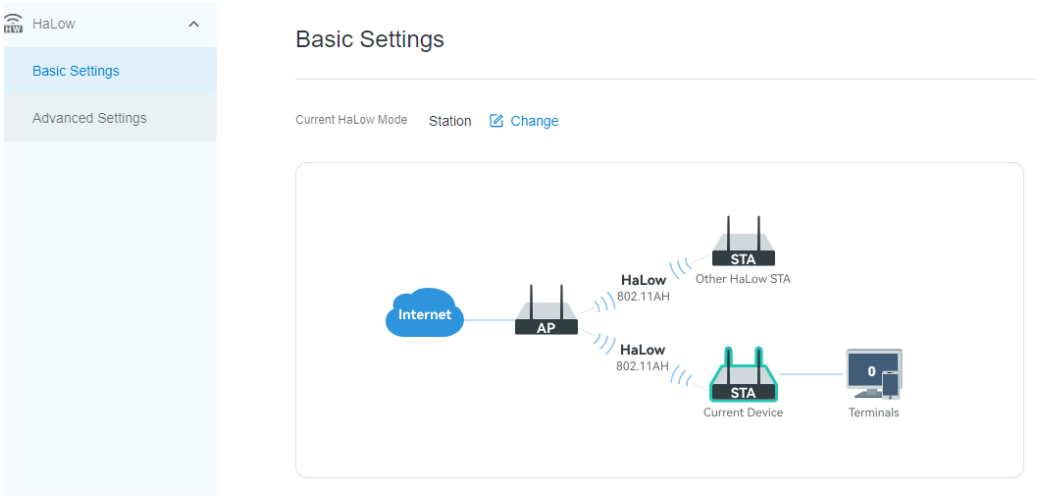
Goal: The device obtains internet access via the Ethernet WAN interface, while HaLow-based data transmission (to a specific remote network or device) is carried out through the HaLow STA interface.

Steps:

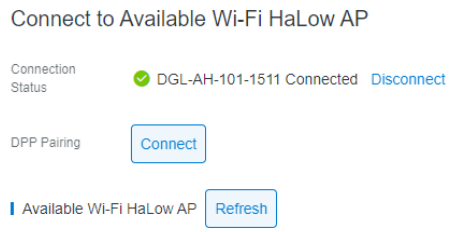
1. Ensure your host PC is connected to the device via 2.4GHz Wi-Fi AP for local access.
2. Navigate to **Network > Interface > WAN**.
3. In the **Link Priority** section, switch the Ethernet port to WAN mode.



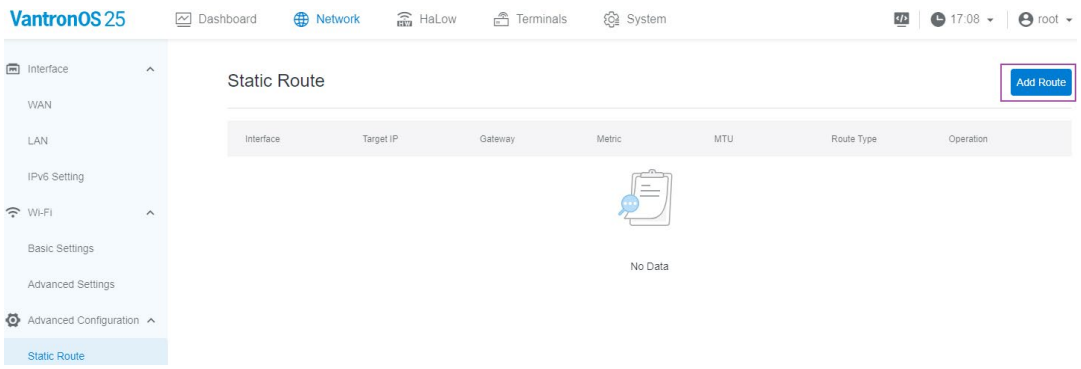
4. Navigate to HaLow > Basic Settings, and ensure the device operates in the HaLow STA mode.



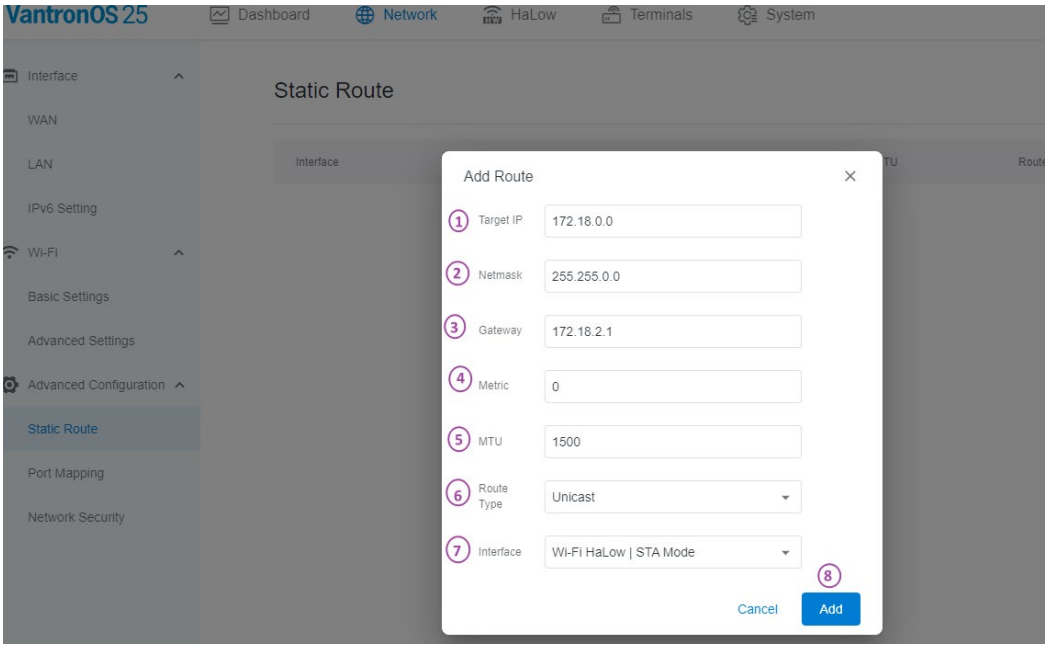
5. Connect the Ethernet port to an external router (primary WAN uplink).
6. Also connect the device to an AP-mode HaLow unit (HaLow uplink).



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



8. Configure the static route with the following parameters:



Description:

1) Target IP address: The destination network you want to reach via HaLow.
2) Netmask: Subnet mask of the destination network.

3) The upstream HaLow AP on the HaLow network.
4) Gateway metric: The smaller the number, the higher the priority.
5) MTU: 1500 by default.
6) Route type (refer to the details in the table below).
7) Select an outbound interface for the route (the interface that leads to the gateway, HaLow STA in this case).
8) Click **Add** to create the rule.

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

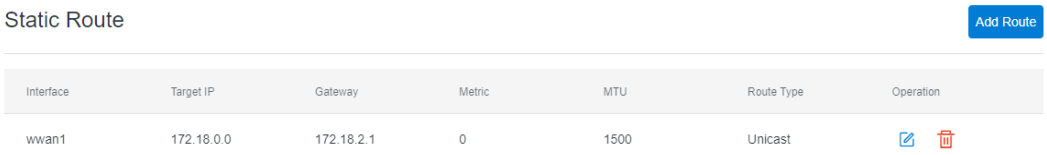


Table 3-1 Description of the route type:

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

3.3.4 Porting Mapping

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

Example:

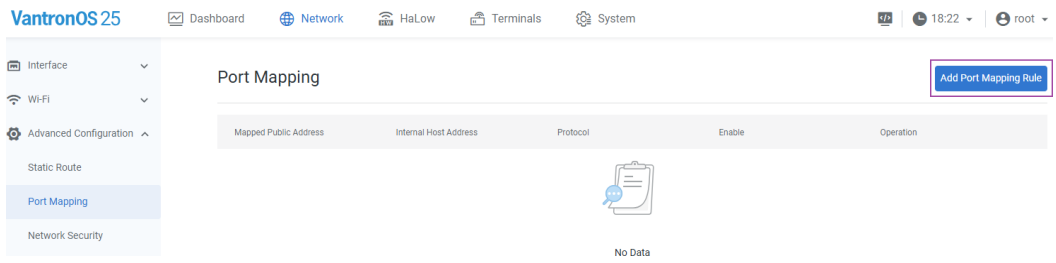
Scenario:

- HAP101 has both an internal zone (e.g., HaLow AP) and an external WAN zone (e.g., Ethernet WAN) configured, with NAT enabled from internal to external.
- Port mapping (Destination NAT) operates based on this NAT boundary.

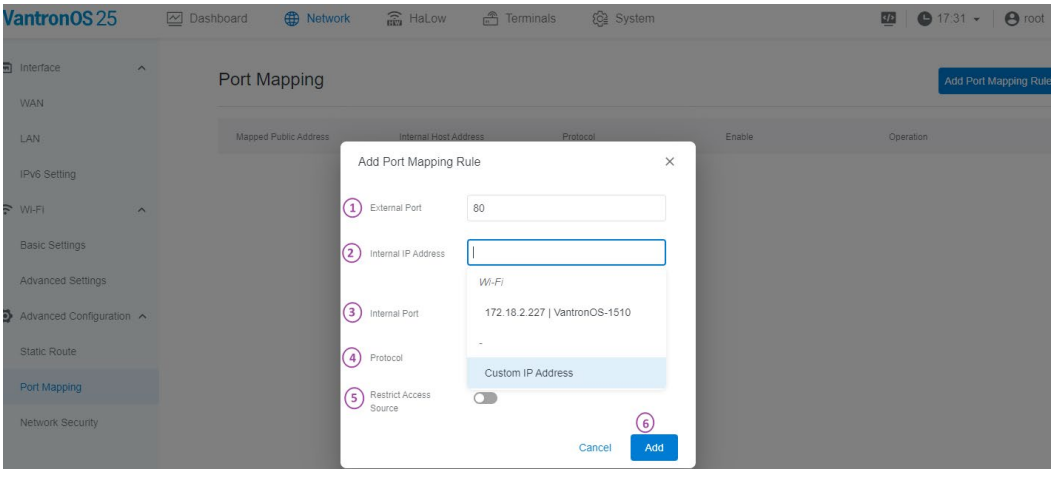
Goal:

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

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



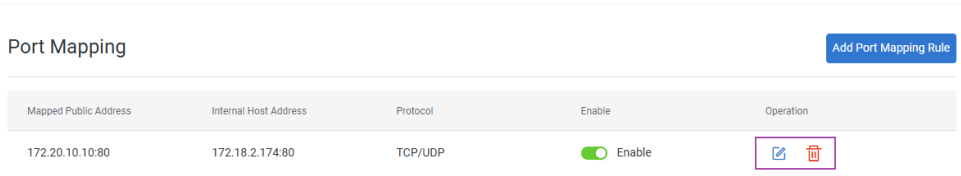
2. Fill in the rule information.



Description:

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

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



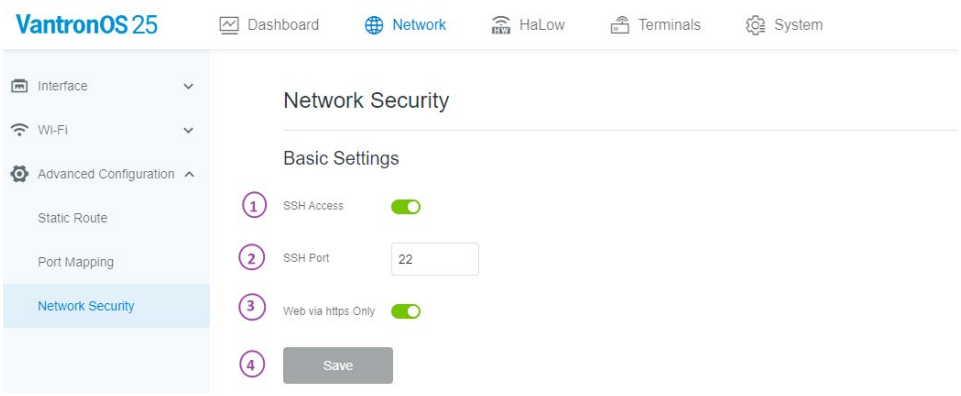
Note: *The mapped public address is determined by your WAN connection and may change.*

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

3.3.5 Network Security

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

3.3.5.1 Basic SSH Access Setup



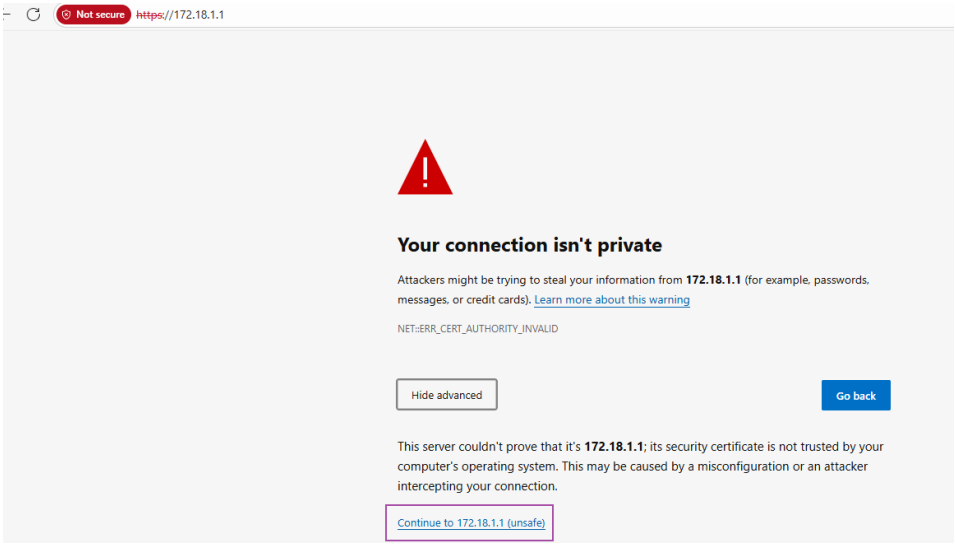
Description:

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

   Refer to 2.8 for the login method.

2. Default SSH port is 22.

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



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

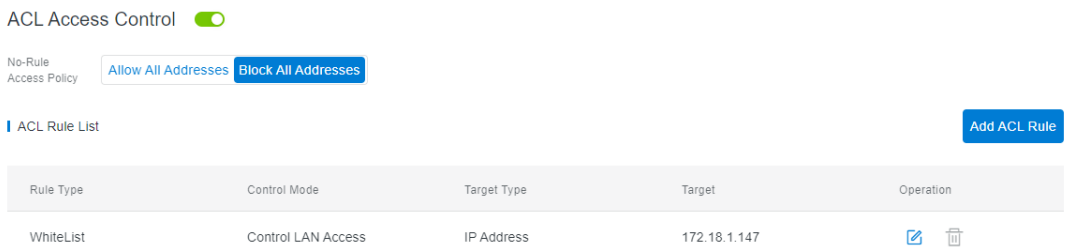
3.3.5.2 ACL Access Control

The device's access control consists of no-rule access policies and ACL rules.

- **No-Rule Access Policies**

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

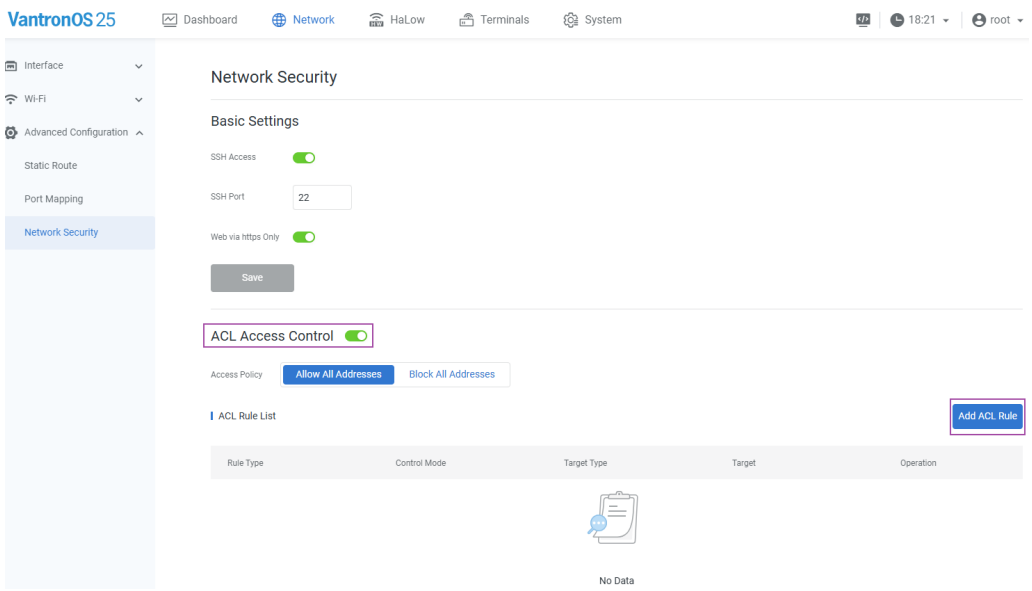
Block all addresses: When enabled, this policy **denies all WAN-side access**—only whitelisted IPs can reach the device—and **prevents** LAN-side devices from using it to **reach the WAN**. If no whitelist rules exist at activation, the device automatically adds the host PC's **current IP** to prevent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



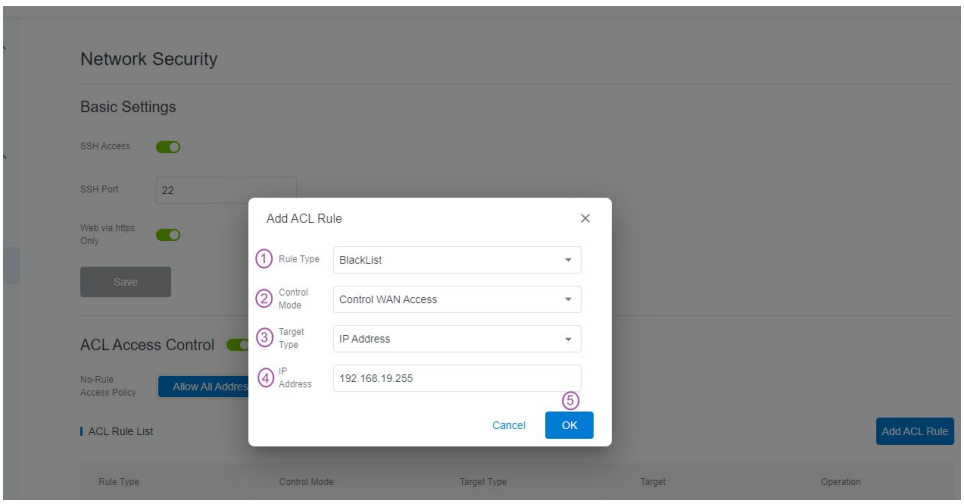
- **ACL Rules**

To add an ACL rule:

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



3. Configure the rule in the pop-up.



Description:

1) Select a rule type:

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

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

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

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

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

5) Click **OK** to complete.

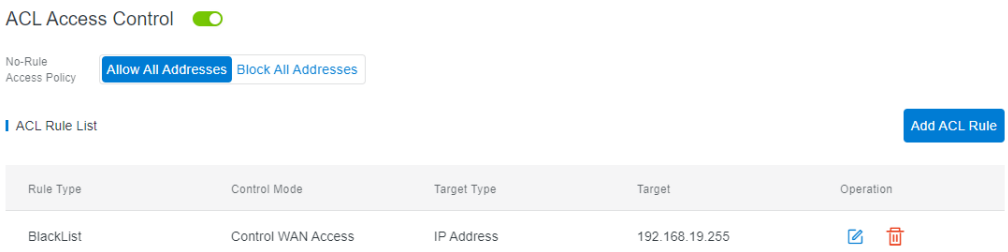
Description for the rule settings:

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

Rule Type	Control Mode	Target Type	Result
Blacklist	WAN	IP address (Source)	The designated WAN IP is blocked from accessing HAP101 or its LAN devices.
		Destination IP/ URL/URL keyword	HAP101 or its LAN devices has no access to the designated WAN IP/URL/URL keyword.
	LAN	IP/MAC/OUI	The designated LAN devices are blocked from accessing the WAN domain.

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

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



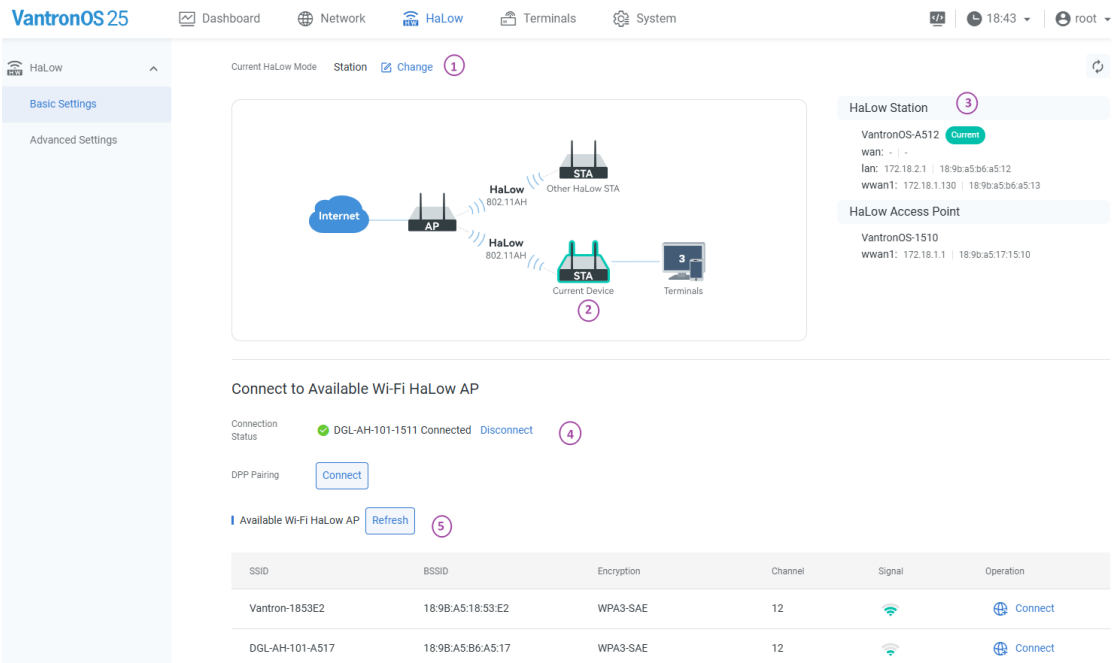
3.4 HaLow

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

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

3.4.1 Overview

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

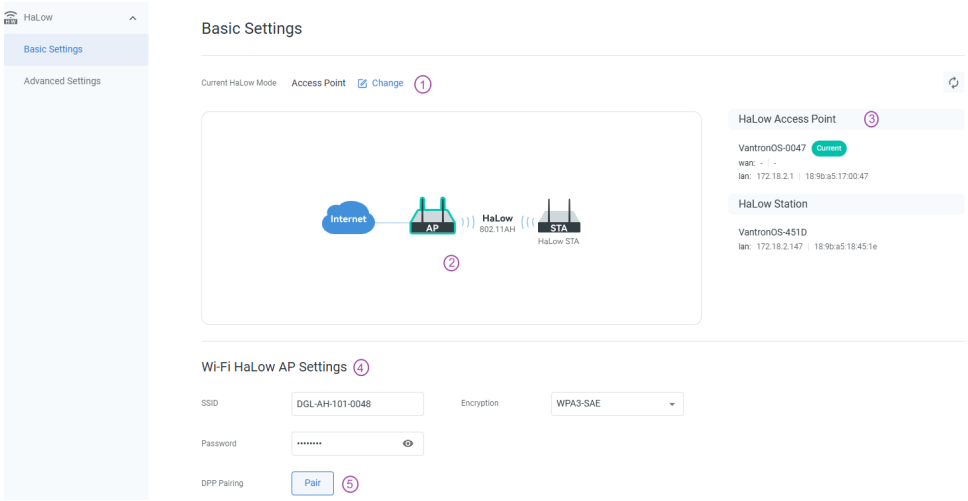


Description:

1. Click to change HaLow operation mode.
   - Access Point (AP): Broadcasts the HaLow network for stations to connect to.
   - Station (STA): Connects to an existing Wi-Fi HaLow AP.
   - Mesh Point: Forms or extends a mesh network with other devices sharing the same Mesh ID via multi-hop communication.
2. Network topology: Displays the layout of the current HaLow network connections. The local device is highlighted with a **cyan** outline. Number of end nodes connected to this device is displayed next to the **Terminals** icon.

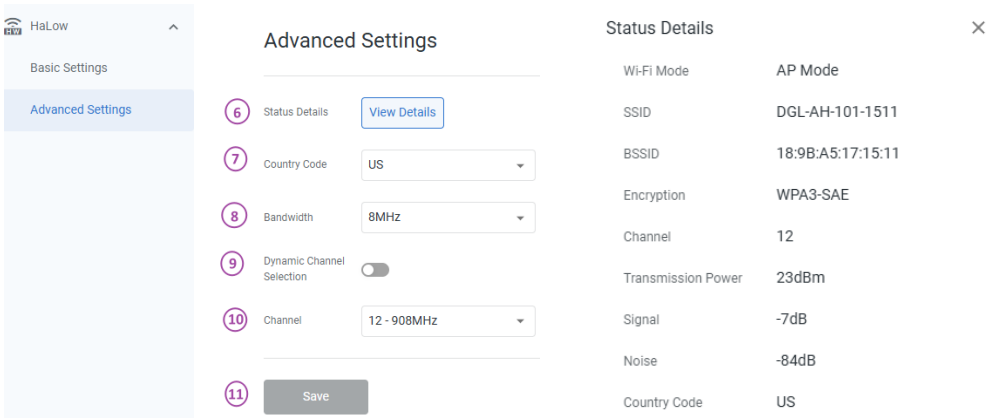
3. Device Information: Shows brief connection information about the current device within the network topology.
    - Clicking the sync button updates the connection status.
    - Device name followed by the **Current** label indicates the local device and its current role.
    - Once a HaLow network is established, associated devices in the network are displayed along with their respective IP and MAC addresses.

3.4.2 AP-Mode Settings



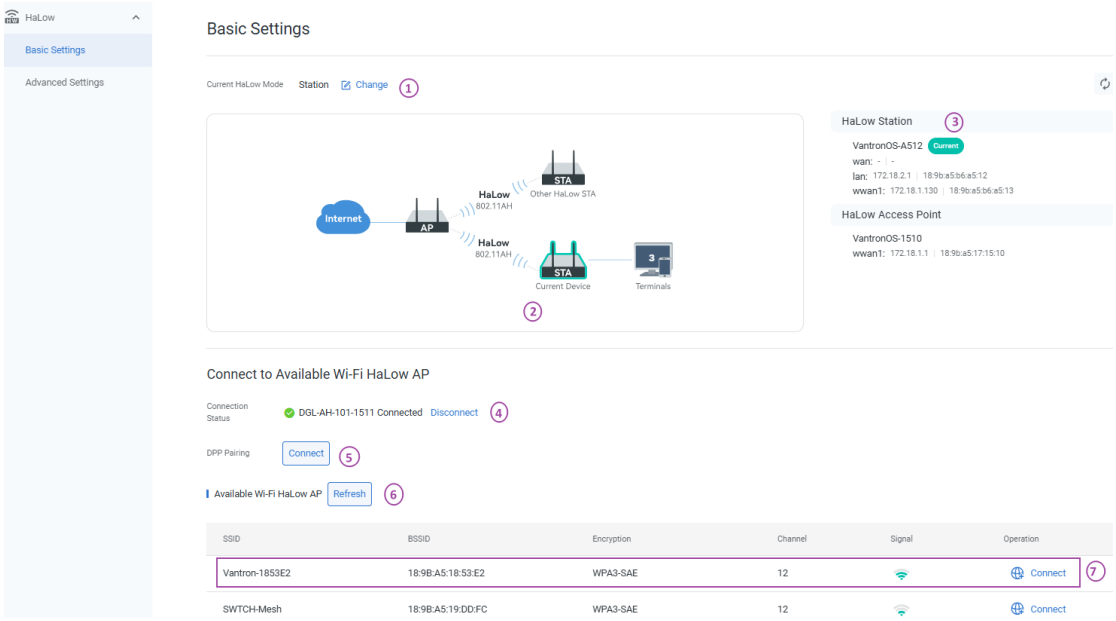
Description:

1. Click **Change** to select **Access Point** as the HaLow operation mode.
2. Network topology for the current mode. The local device is highlighted with a **cyan** outline.
3. Brief device connection info: **Current** indicates the local device. Clicking the sync button refreshes the information.
4. AP settings: SSID, encryption, and password. You can modify these parameters as needed.
5. DDP pairing: Initiates a quick HaLow connection upon clicking the **Pair** button. The target STA shall press the button within 120 seconds for a successful connection. Refer to Section 2.6.2 for the pairing instructions.



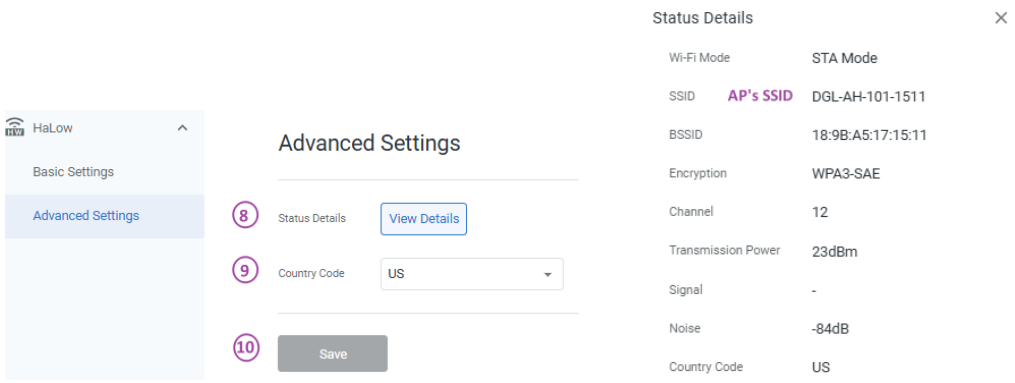
6. Status details: Clicking **View Details** will display the detailed HaLow settings of the device, including HaLow mode, SSID, encryption, channel, transmit power.
7. Country code: Ensure the device meets the local radio frequency regulations.
8. Channel bandwidth: A wider bandwidth typically offers higher throughput.
9. DCS: Once enabled, the device will automatically select the channel with the strongest signal within the selected bandwidth for optimal performance.
10. Available operating channels are 12 and 28.
11. Apply the changes by clicking **Save**.

3.4.3 STA-Mode Settings



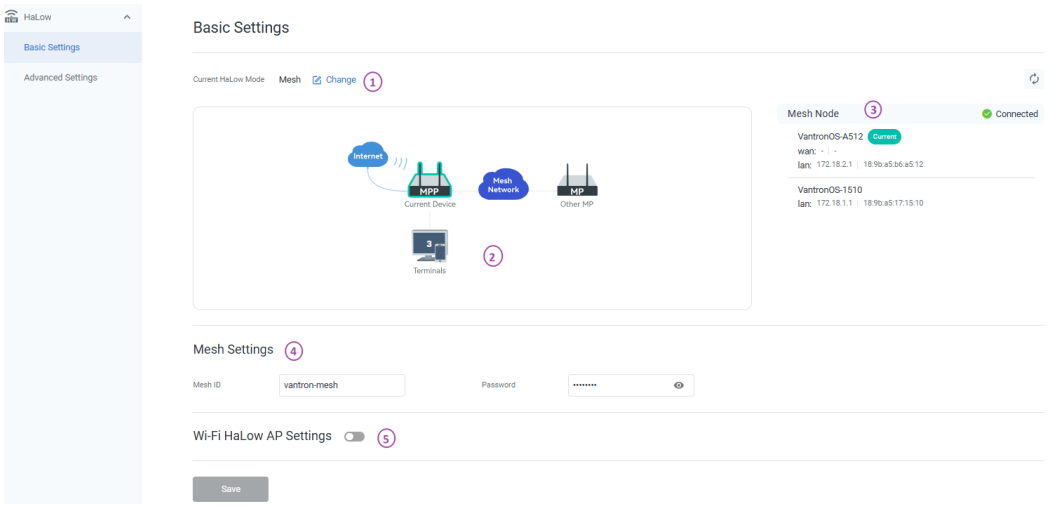
Description:

1. Click **Change** to select **Station** as the HaLow operation mode.
2. Network topology for the current mode. The local device is highlighted with a **cyan** outline. Number of end nodes connected to this device is displayed next to the **Terminals** icon.
3. Brief device connection info: Clicking the sync icon refreshes the information.
4. Connection status:
   - Pending Connection: Not connected to an AP.
   - xxx Disconnect: Having connected to the indicated SSID. Clicking **Disconnect** will cut off the link.
   - Connection Failed: Failed to connect to the target AP.
5. DPP pairing: Initiates a quick HaLow connection upon clicking the **Connect** button. The target AP shall press the button within 120 seconds for a successful connection. Refer to Section 2.6.2 for the pairing instructions.
6. Available Wi-Fi HaLow AP list: Displays available HaLow SSIDs. Clicking the button refreshes the list.
7. To connect/switch connection to a target AP: Click **Connect** next to the target SSID and enter the password in the pop-up.



8. Status Details—Clicking **View Details** will display the detailed connection information of the device, including HaLow mode, and—if connected—the SSID of the target HaLow AP, encryption, channel, transmit power, etc.
9. Select the country code based on local radio frequency regulations.
10. Apply the changes by clicking **Save**.

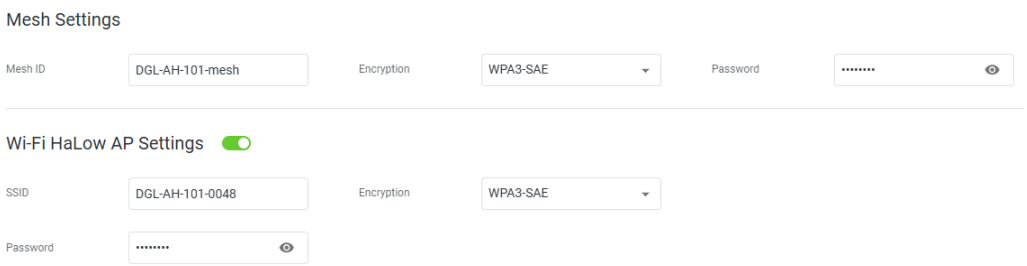
3.4.4 Mesh Settings



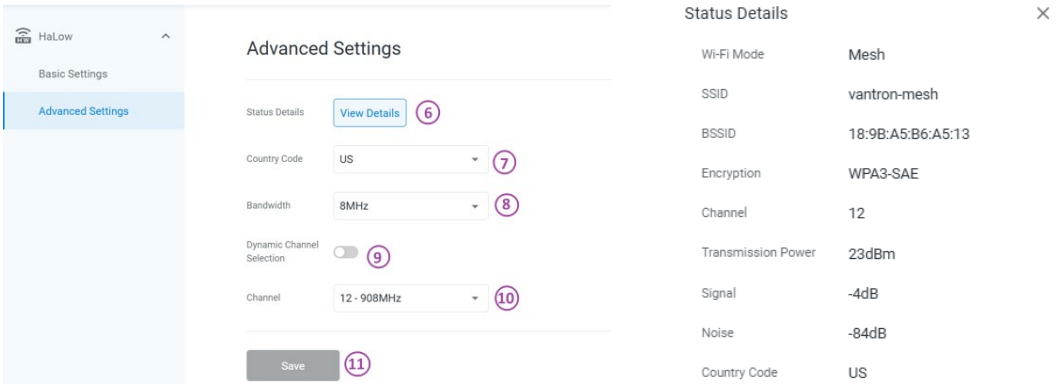
Description:

1. Click **Change** to select **Mesh** as the HaLow operation mode.
2. Network topology for the current mode. The local device is highlighted with a **cyan** outline.

   When an HAP101 is set to Mesh mode via VantronOS, it defaults to **MPP** and acts as the **DHCP server** for the mesh network. Only **one** MPP (or **no devices** in a router-dominated MP topology) requires this mode change to provide DHCP service for the entire mesh network.
3. Brief device connection info: Clicking the sync icon refreshes the information. In the Mesh mode, the device continuously scans for and joins peers with the **same** Mesh settings. Detailed connection information is retrievable in the **Terminals** menu tab.
4. Mesh settings: Nodes with the same mesh parameters automatically join the Mesh network with IP addresses assigned by the MPP (only one MPP exists in a mesh network). Since all HAP101 units share the same default configuration, you can modify these parameters to create separate, isolated mesh networks.
5. HaLow AP settings in Mesh mode: When operating within a mesh network, enabling this feature allows the device to broadcast a standard HaLow network and allow HaLow STAs to pair (separate from the mesh backhaul).



In **Advanced Settings**, available configurations are as follows:



6. Details of the Mesh mode.
7. Country code: Ensures the device meets the local radio frequency regulations.
8. Select a channel bandwidth: A wider bandwidth typically offers higher throughput.
9. DCS: Once enabled, the device will automatically select the channel with the strongest signal within the selected bandwidth for optimal performance.
10. Available operating channels are 12 and 28.
11. Apply the changes by clicking **Save**.

3.4.4.1 DHCP Service in a Mesh Network

In a mesh network, the DHCP server configuration differs based on the network setup:

- **One MPP + Multiple MPs**: The only Mesh Portal (MPP) acts as the DHCP server for the entire mesh network. If the MPP is connected to an upstream router, it NATs the mesh traffic to its upstream IP; if not, the mesh supports only internal communication between nodes.
- **Multiple MPs**: The upstream router acts as the DHCP server. The Mesh Point (MP) connected to this router relays external network access to the entire mesh.

Table 3-1 DHCP Service in a Mesh Network:

Network Setup	DHCP Service Provider	External Network Access	Device Login IP
One MPP + Multiple MPs	MPP	WAN DHCP enabled (connected to an upstream router via Ethernet): Provides external network access to the entire mesh network.	MPP: Device's Ethernet IP from the router or its 2.4GHz Wi-Fi IP. MP: Device's IP assigned by the MPP
		LAN DHCP only (no upstream connection): Internal communication only.	MPP: Ethernet or 2.4GHz Wi-Fi IP MP: Device's IP assigned by the MPP
Multiple MPs	Upstream router (DHCP relay via the router-connected MP)	The upstream router provides external access to the entire mesh network.	MP: Device's IP assigned by the router

With the same Mesh ID and password set, a mesh network can be established using either of the following methods:

- **Via DIP switches and Pair button**: No software configuration is required; the mesh network is established automatically.
- **Via software configuration:** If you configure the mesh network via VantronOS, follow the steps in the following sections.

Software configuration involves interface bridging and WAN DHCP service enablement, as needed. Both operations apply exclusively to WAN interfaces. Saving a related configuration switches the Ethernet port to **WAN** mode. Always make sure the host PC and the device are on the same subnet for smooth device login.

3.4.4.2 MPP to Provide DHCP Service

In a mesh network setup with one MPP and multiple MPs (with or without an upstream router), the MPP provides the DHCP service. Ensure the following:

- The MPP's DHCP service is enabled.
- All MPs have their HaLow Mesh interface bridged.

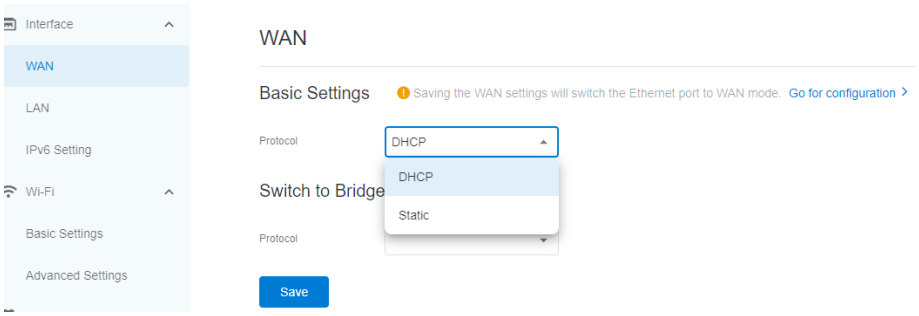
MPP setup:

1. Ensure the device operates in HaLow mesh mode.

   *For local mesh networking, no additional device configuration is required. To enable **external network access** for the entire mesh network, complete the following steps.*

2. Navigate to **Network > Interface > WAN**.

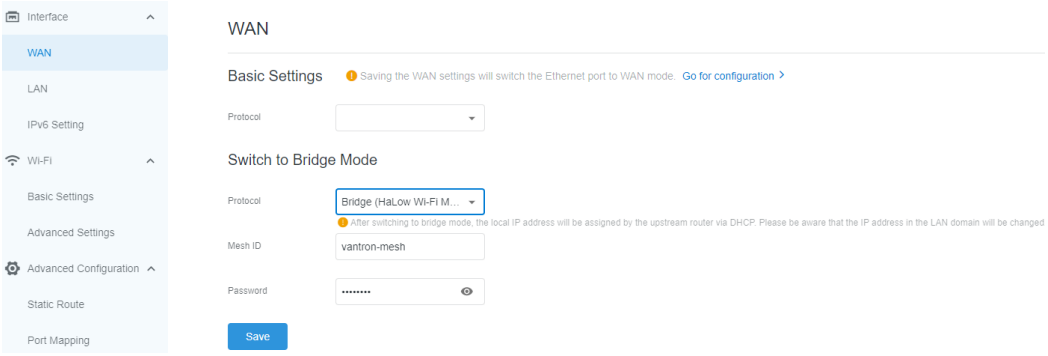
3. Enable the WAN DHCP protocol in the **Basic Settings** section.



4. Connect the MPP to an upstream router.

MP setup:

1. Ensure the device operates in HaLow mesh mode.
2. Navigate to **Network > Interface > WAN**.
3. Select the interface to bridge – HaLow Wi-Fi Mesh.



   Configuration parameters including Mesh ID and password are editable here.

4. Once bridged:

   - The MP automatically joins a HaLow mesh network with the same parameters.
   - Each MP obtains an IP address from the MPP. To log back into the device, use this IP address over a 2.4GHz Wi-Fi/ETH connection.
   - The HaLow mode and corresponding parameters are not configurable on the HaLow **Basic Settings** page.

- To exit mesh mode, enable the device's WAN DHCP, log back using its LAN IP (for Ethernet connection, switch the Ethernet port to LAN mode first), then modify the HaLow mode.

3.4.4.3 DHCP Relay via Router-Connected MP

In a mesh network setup with all MPs and an upstream router. The upstream router provides the DHCP service via the MP connected to the router. Ensure the following:

- All MPs have their HaLow Mesh interfaces bridged.
- One MP is connected to the upstream router.

MP setup:

The MP configuration procedure is **identical** to that outlined in the prior section.

1. Refer to the **MP Setup** description in Section 3.4.4.2 to configure all MPs.
2. Connect one MP to an upstream router.
3. Once bridged:
   - The MP automatically joins a HaLow mesh network with the same parameters.
   - Each MP obtains an IP address from the upstream router. To log back to any MP, use this IP address while keeping the host PC connected to the same router.
   - The HaLow mode and corresponding parameters are not configurable on the HaLow **Basic Settings** page.
   - To exit mesh mode, enable the device's WAN DHCP, log back using its LAN IP (for Ethernet connection, switch the Ethernet port to LAN mode first), then modify the HaLow mode.

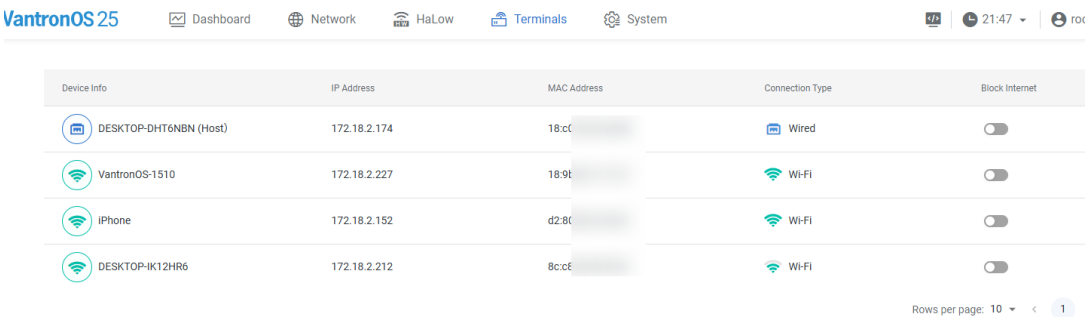
3.5 Terminals

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

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

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

DHCP reserved for a specified device using its MAC addresses is also displayed here. Refer to Section 3.3.1.2 for details on DHCP reservation.


VantronOS 25
Dashboard
Network
HaLow
Terminals
System
21:47
Device Info
IP Address
MAC Address
Connection Type
Block Internet
DESKTOP-DHT6NBN (Host)
172.18.2.174
Wired
VantronOS-1510
172.18.2.227
Wi-Fi
iPhone
172.18.2.152
Wi-Fi
DESKTOP-IK12HR6
172.18.2.212
Wi-Fi
Rows per page: 10
1

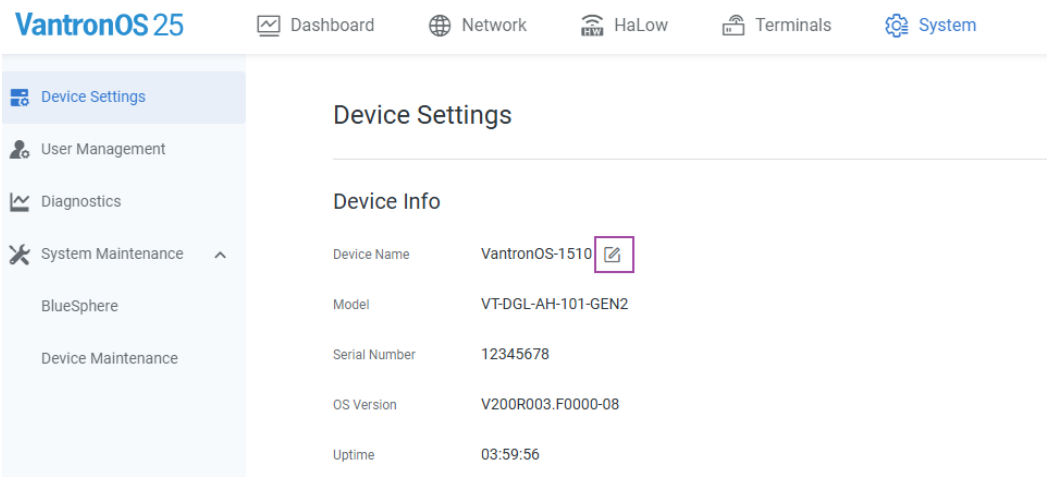
3.6 System

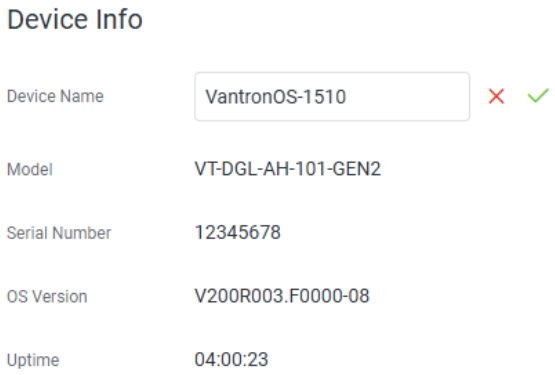
Under **System**, users can view and edit all system-level settings.

3.6.1 Device Settings

3.6.1.1 Modifying Device Name

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



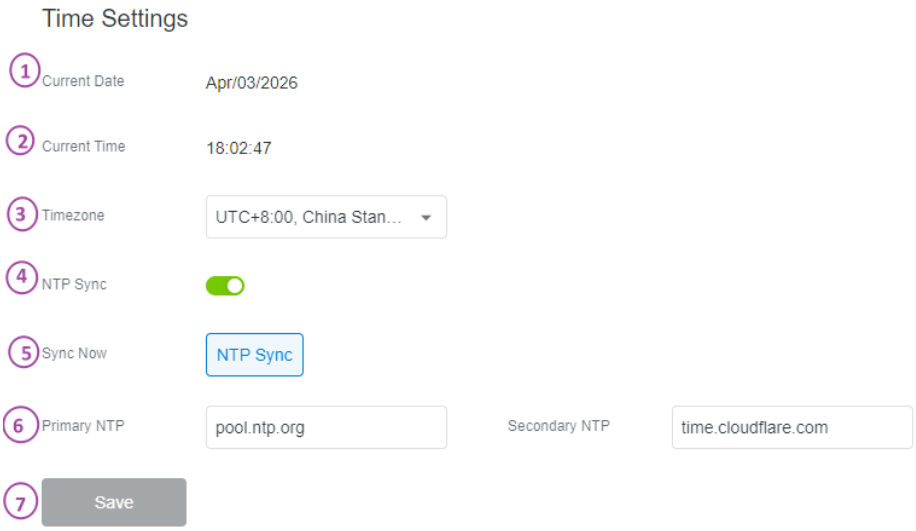


To modify the device name:

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

3.6.1.2 System Time

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

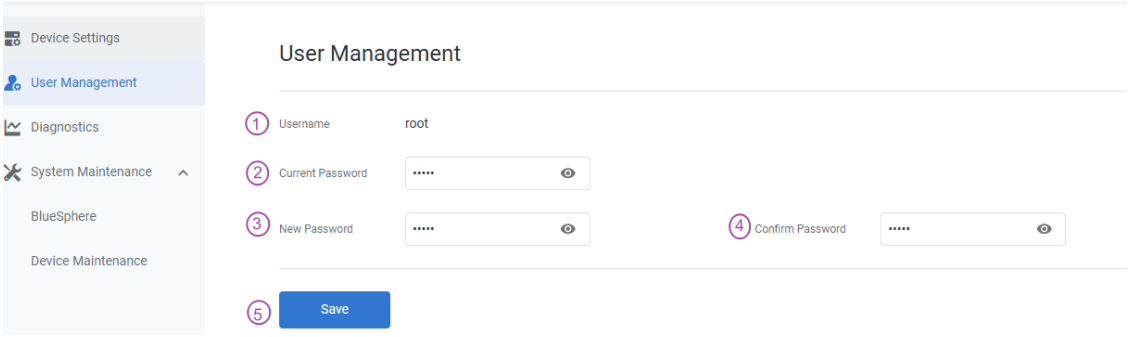


Description:

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—Toggle automatic time synchronization with NTP servers. The following options can be configured only when this feature is enabled.
5. Sync Now—Triggers a one-time NTP update immediately. The date resets after every power cycle because HAP101 lacks an RTC.
6. Primary NTP—Preferred NTP server. Secondary NTP—Backup NTP server.
7. If you have made any changes, click **Save** to apply.

3.6.2 User Management

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



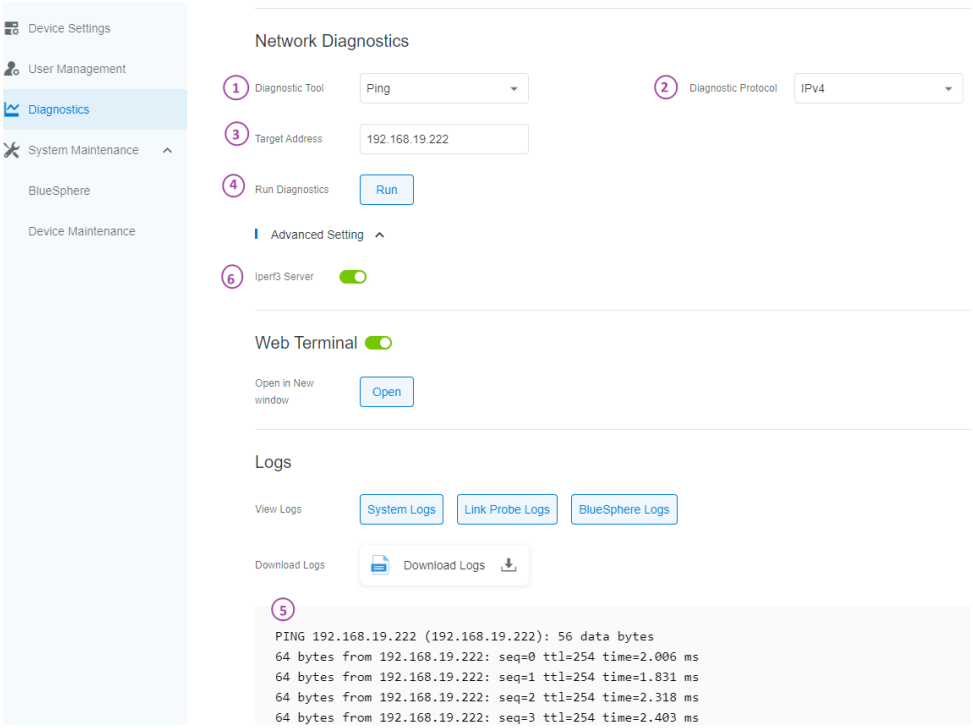
Steps to reset the login password:

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

3.6.3 Diagnostics

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

3.6.3.1 Network Diagnostics

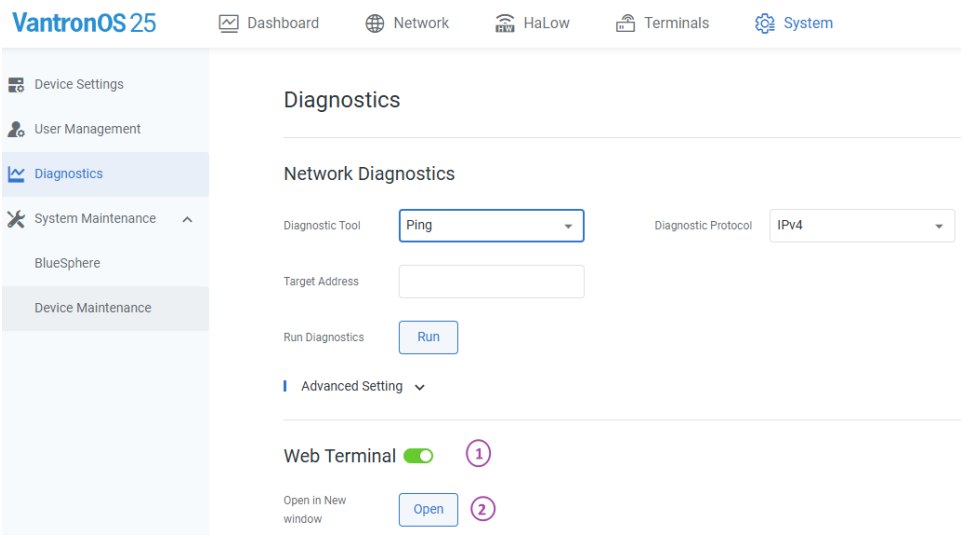


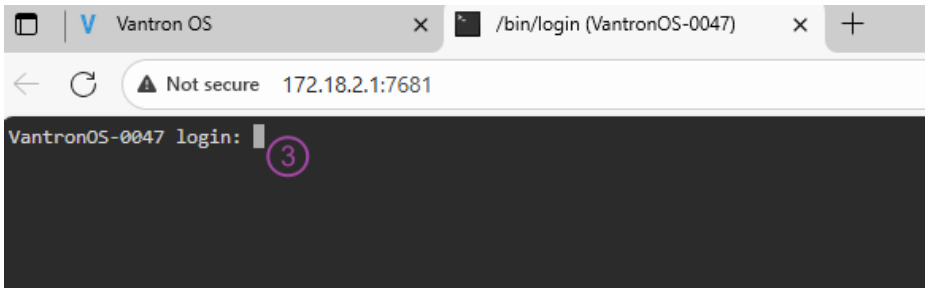
Description:

1. Select a diagnostic tool from the drop-down list (**ping, traceroute, nsloopup, iPerf3 client**).
2. Enter the destination IP address or domain name for the test.
3. Initiate a diagnostic test.
4. Run the test.
5. The test results are displayed correspondingly.
6. The HAP101's iPerf3 server is enabled by default, allowing remote clients to start a HaLow throughput test immediately without manual activation.

3.6.3.2 Web Terminal

The **Web Terminal** allows users to toggle the web shell and access the device's shell for debugging.





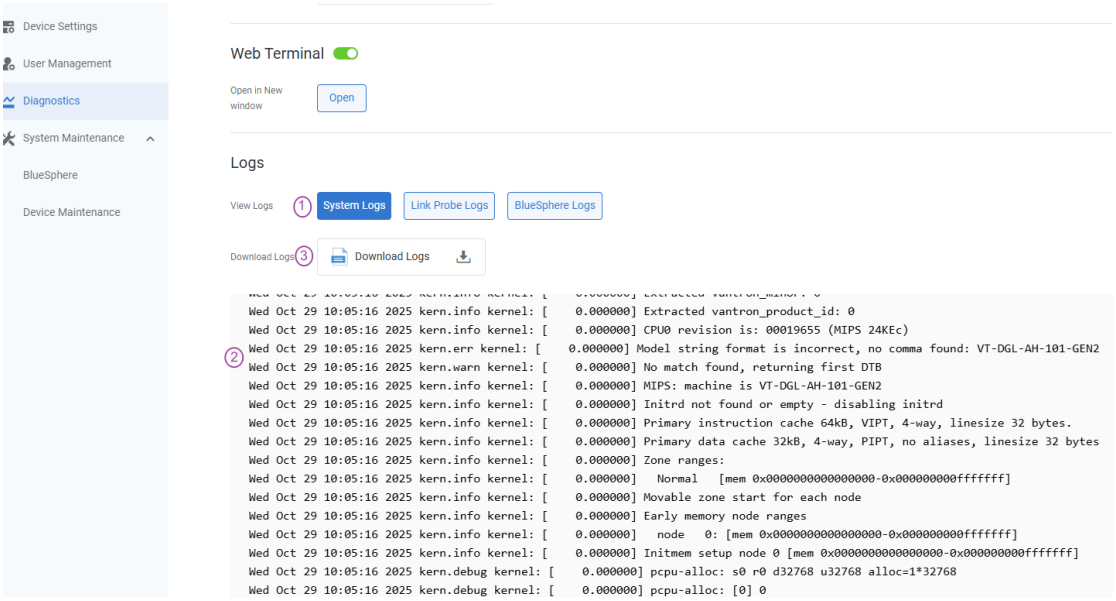
Description:

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

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

3.6.3.3 Logs

The system offers different device logs for maintenance or troubleshooting.



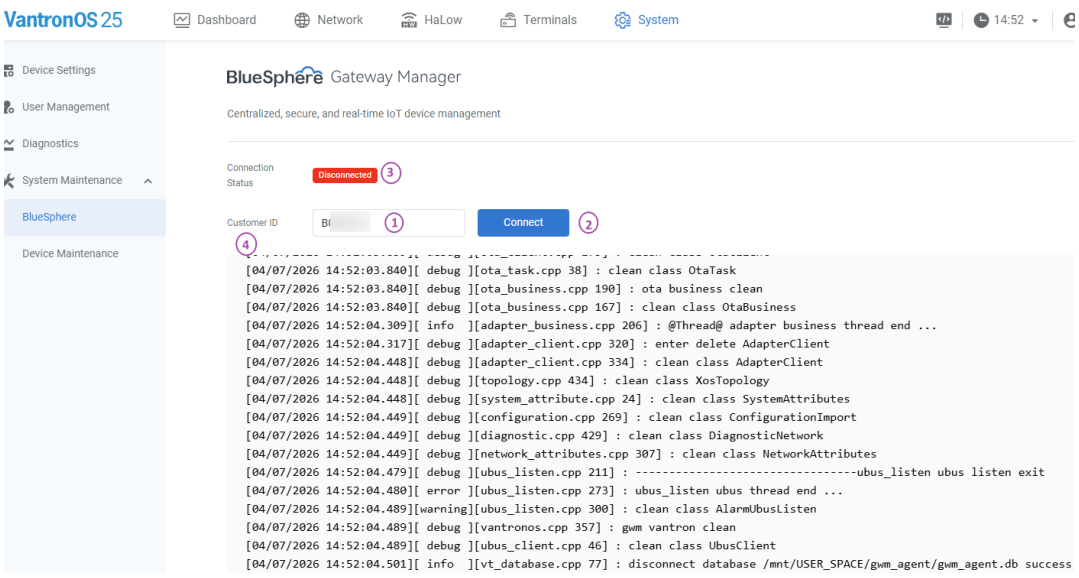
Description:

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

3.6.4 System Maintenance

3.6.4.1 BlueSphere

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



Prerequisites:

- **The HAP101 has internet access.**
- **You have an authorized BlueSphere GWM user account.**

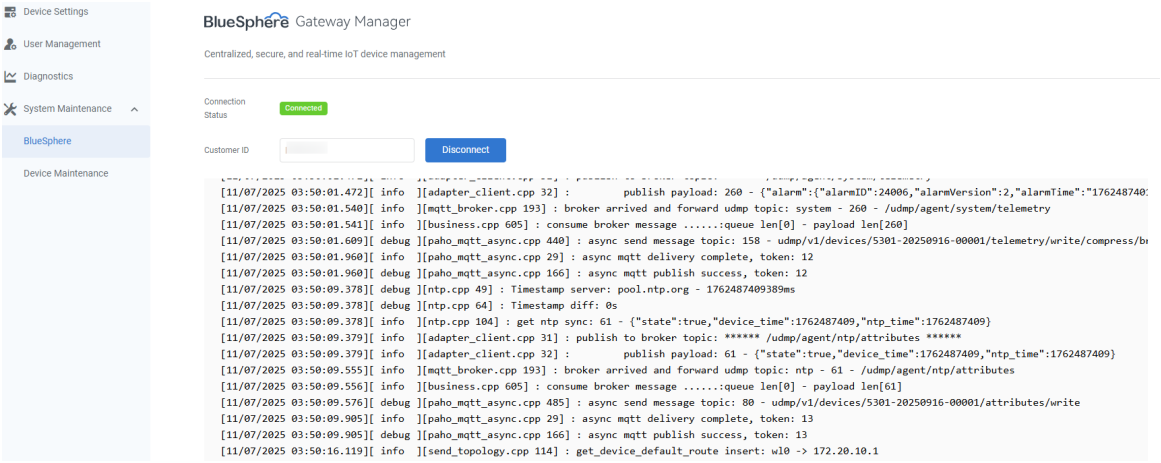
Description:

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

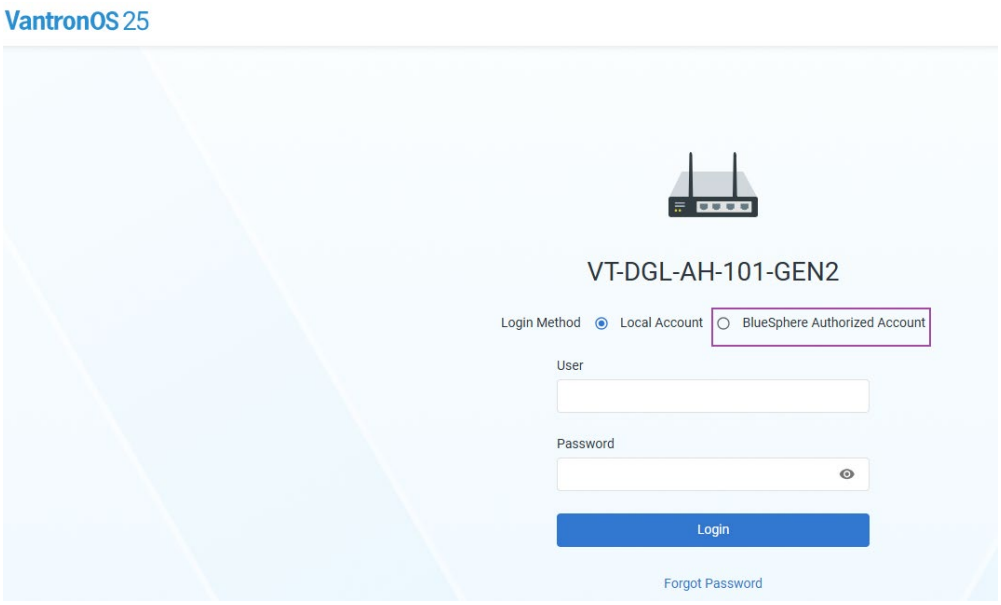
   *If a customer ID is pre-filled, you can click **Disconnect** first and fill in your own.*

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

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



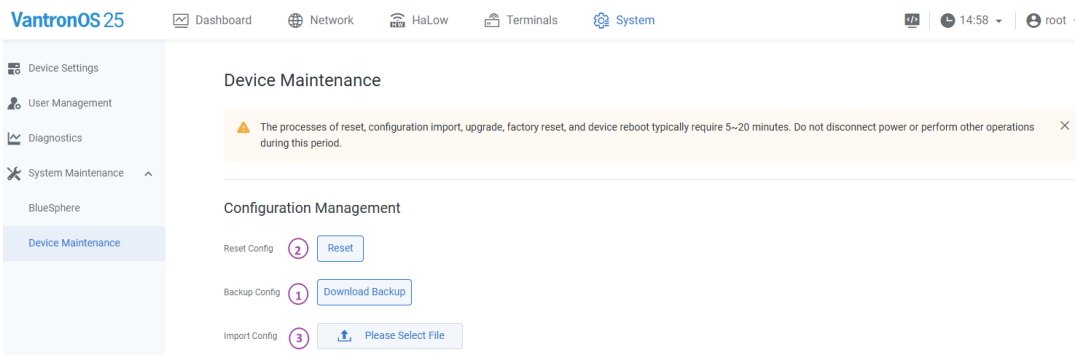
If you log out the portal now, you will find two login methods available. You can sign back in with either your local credentials or your authorized GWM account.



3.6.4.2 Device Maintenance

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

- Configuration Reset

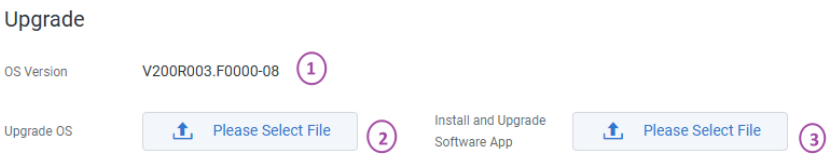


Description:

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

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

- Upgrade

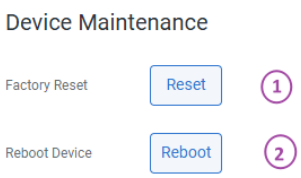


Description:

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

   VantronOS 25 consists of the operating system and VantronOS25 applications, which can be upgraded separately by following step 2 or 3 above. Upgrades are allowed only from an older to a higher version.

- Device Maintenance



Description:

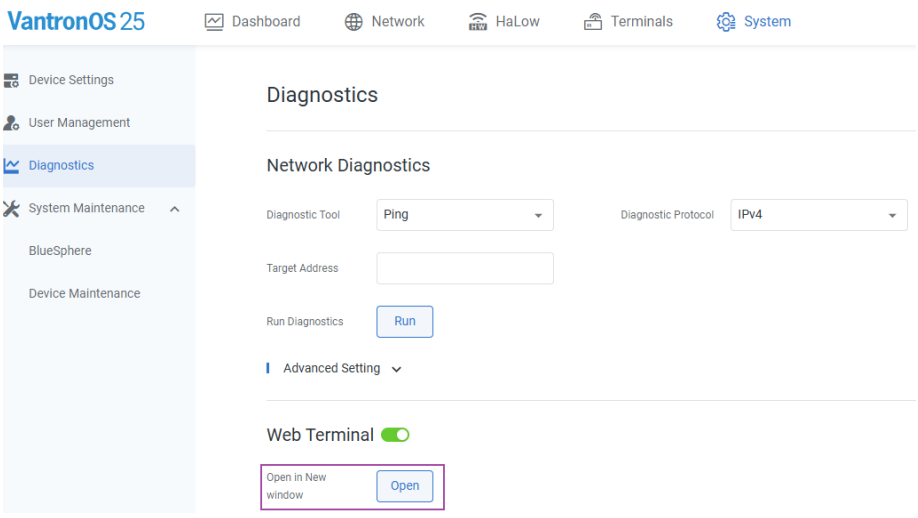
1. Factory reset the device with device configuration, user data and custom applications (including VantronOS 25 APP) cleared.
2. Manually restart the device.

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

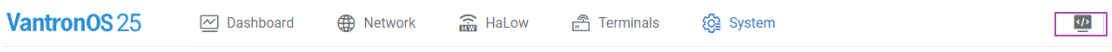
3.7 Command Line Interface

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

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

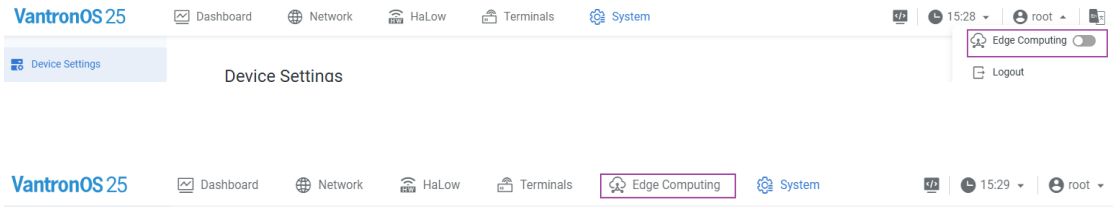


- Click the CLI icon on the menu tab.



3.8 Edge Computing

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



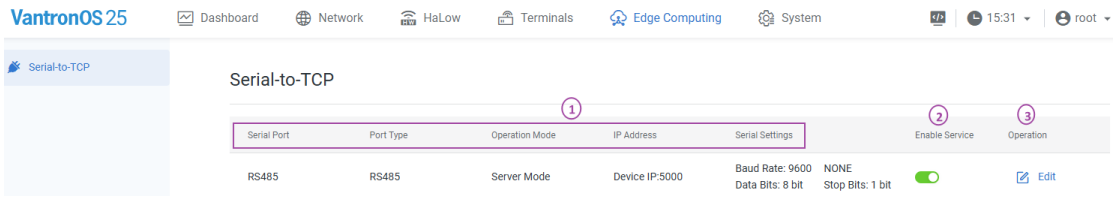
3.8.1 Serial to TCP

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

- The serial parameters (baud rate, data bits, parity, stop bits) on both the serial peripheral and the HAP101 shall match.
- The server's listening port matches the client's target port.
- Both ends use the same protocol (TCP).
- Server and client are mutually IP-reachable.

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

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

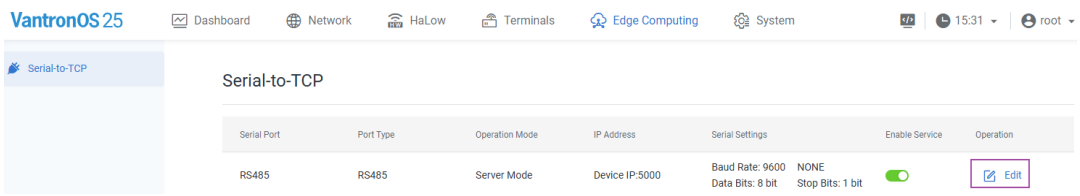


Description:

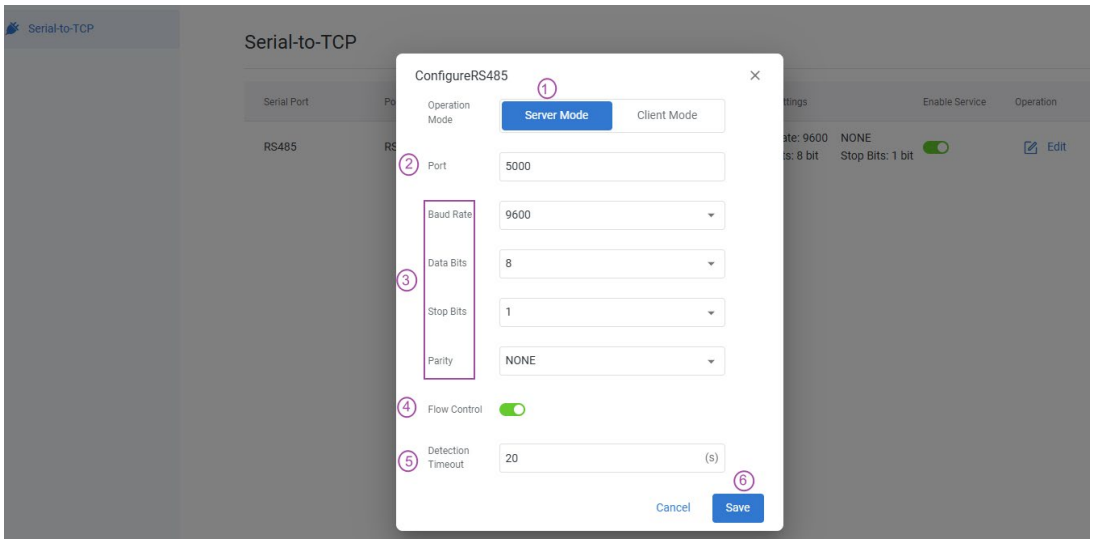
1. Details of the conversion rule, including the serial port name and type, current operation mode, IP address of the device + port, and serial parameters.
2. Enable/disable the rule
3. Edit the rule

3.8.1.1 Server Mode Rule Setup

1. Click the edit icon next to the rule.



2. Modify the parameters, ensuring consistency between the server and client on the network, and between the serial peripheral and the HAP101 on the serial link.



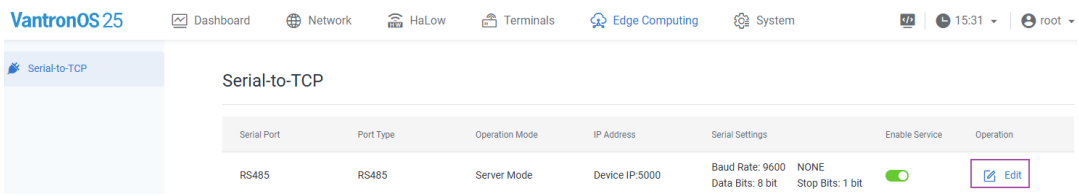
Description:

1) Select **Server Mode.**
2) Designate a TCP port to listen to (0~65535). Make sure the port on both the server and client are the same.
3) Make sure the serial parameters on both HAP101 and the serial peripheral are set the same.
4) Enable/Disable software flow control to prevent packet loss (but this reduces throughput).
5) Set the timeout to automatically drop the connection if no data is received (0=disabled).
6) Save the changes to let them take effect.

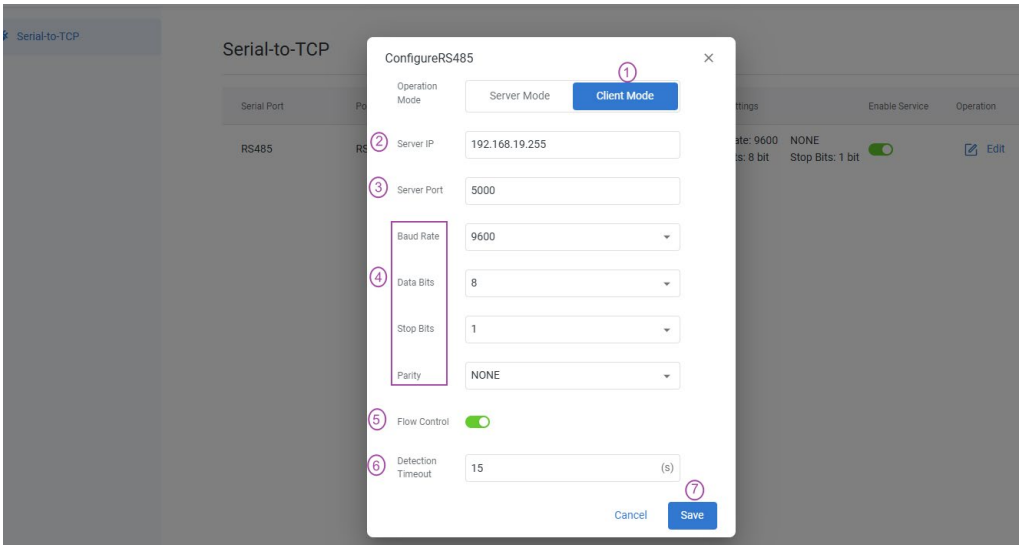
3. Enable the conversion rule.
4. Make sure both the client and server are on the same reachable IP network.
5. Verify the data transmission between the devices.

3.8.1.2 Client Mode Rule Setup

1. Click the edit icon after the rule.



2. Modify the parameters, ensuring consistency between the server and client on the network, and between the serial peripheral and the HAP101 on the serial link.



Description:

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

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

CHAPTER 4 DISPOSAL AND PRODUCT WARRANTY

4.1 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.

4.2 Warranty

Product warranty

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

Out-of-Warranty Repair

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

Returned Products

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

Appendix Regulatory Compliance Statement

FCC Compliance Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

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

Exposure to radio frequency energy:

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

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

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

IC Statement

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

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

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

Exposure to radio frequency energy:

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

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

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

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

L'exposition à l'énergie radiofréquence:

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