HAP202 Wi-Fi HaLow Unit

User Manual

Version: 1.3

Revision History:

No.	Description	Date
V1.0	First release.	Oct. 20, 2025
V1.1	Modified LED definition	Nov. 13, 2025
V1.2	Updated 1.3 Terminologies and Acronyms	Dec. 5, 2025
V1.3	Deleted the Edge Computing section as the current HW version does not include the serial port.	Jan. 22, 2026

Table of Contents

Foreword

Thank you for purchasing HAP202 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/5GHz Wi-Fi, and ***HaLow*** refers to Wi-Fi HaLow.

Intended Users

This manual is intended for:

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

Copyright

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

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

Disclaimer

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

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

Technical Support and Assistance

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

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

Vantron Technology, Inc.

Address: 48434 Milmont Drive, Fremont, CA 94538

Tel: (650) 422-3128

Email: sales@vantrontech.com

Regulatory Information

The Product is designed to comply with:

- Part 15 of the FCC Rules
- ISED

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

Symbology

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

Note: Calls attention to critical operational or safety information.

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

General Safety Instructions

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

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

Precautions for Power Cables and Accessories

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

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

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

⚠ Cleaning instructions:

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

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

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

⚠ Do not use in combustible and explosive environment:

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

CHAPTER 1 DEVICE INTRODUCTION

1.1 Product Overview

Powered by Morse Micro's MM6108 Wi-Fi HaLow chipset, Vantron HAP202 features a new configuration with dual Ethernet ports. This design provides more flexible and convenient access to the device management portal, eliminating the need to manually switch between LAN and WAN connections when the 2.4GHz/5GHz Wi-Fi is operating in client mode. In addition, it is designed to maximize the chipset's throughput to ensure reliable and efficient data transfer.

Operating in both sub-1GHz (IEEE 802.11ah) and 2.4GHz/5GHz (802.11 b/g/n/ac) bands, the device provides long-range connectivity up to 1km at 32.5Mbps and short-range speeds up to 867Mbps, respectively, ensuring reliable performance. It is equipped with DIP switches for quick configuration of HaLow base and nodes in either standard or mesh setups, while also allowing for user-specific customization. The DPP (Wi-Fi Easy Connect) handles secure, effortless device pairing, and the optional IP54 waterproof kit enables reliable outdoor deployment.

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

1.2 Unpacking

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

Standard accessories:

- HAP202 Wi-Fi HaLow unit
- 2 x 2.4GHz Wi-Fi antenna
- 1 x Wi-Fi HaLow antenna
- 1 x DC power connector

Optional accessories:

- 1 x 12V/1A power adapter
- 1 x Power cord
- 1 x RS485 terminal connector
- 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 or directly allocates IP addresses to the STAs.
HaLow Mesh mode	A HaLow Mesh network involves multiple interconnected nodes, which communicate with each other (multi-hop communication) to automatically determine the most efficient path for data transmission, helping to extend network range and improve reliability.
Base	A HaLow unit that allocates or relays IP addresses to all paired Nodes in a HaLow network. There will always be only one Base in a network. In a standard HaLow network, the HaLow AP is the Base. In a HaLow Mesh network, the Base that relays IP addresses is an MP, while a Base that directly allocates IP addresses is an MPP. (MP and MPP are explained below)
Node	A HaLow unit that connects to the Base—or to other Nodes in the mesh configuration—to obtain an IP from the Base or the upstream network via the Base or to relay data to extend the network coverage. In a standard HaLow network, a HaLow STA is a Node.

Table 1-1 (continued)

Glossary	Description
Mesh Portal (MPP)	In a HaLow mesh network, when a Node is configured as a Mesh Portal (MPP), it allocates IP addresses to other nodes. Otherwise, the upstream router will act as the DHCP server for IP assignment.
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™ that streamlines device onboarding. In this document, the term specifically denotes quick device provisioning via basic hardware/software setup for Standard HaLow pairing (“**DPP Pairing**”). For Mesh networking, the combination of DIP switches and Pair button enables mesh configuration, rather than quick pairing.
VantronOS	Web management portal for Vantron IoT communication devices. Its latest available version is VantronOS 25.
DCS	**Dynamic Channel Selection**. Once enabled, the device will automatically select the channel with the strongest signal within the selected bandwidth for optimal performance.

To better understand the device roles, refer to the topologies in section 2.1.

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

1.4 Specifications

HAP202			
System	CPU	MediaTek Dual-core MIPS®1004Kc CPU, 880MHz	
	Wi-Fi HaLow chipset	Morse Micro MM6108	
	Memory	256MB	
	Storage	64MB	
WLAN Features	2.4GHz/5GHz Wi-Fi	Standard: IEE 802.11 b/g/n/ac	
		Frequency range: 2.412GHz~2.462GHz; 5.15GHz~5.25GHz , 5.25GHz~5.35GHz, 5.47GHz~5.725GHz, 5.725GHz~5.85GHz	
		Channel bandwidth: 20/40/80MHz	
		Data rate: up to 867Mbps	
		Security: AES-CCMP	
		Working mode: Access point (AP), station (STA)	
	Wi-Fi HaLow	Standard: IEE 802.11 ah	
		Frequency range: 903.5MHz~926.5MHz (US)	
		Channel bandwidth: 1/2/4/8MHz, dynamic channel selection (DCS) supported	
		Transmit power: 23dBm	
		Data rate: up to 32.5Mbps@8MHz or 15Mbps@4MHz	
		Fast pairing: DPP Easy Connect via hardware/software setup	
		Security: AES, WPA3	
		Working mode: Access point (AP), station (STA), Mesh	
I/O	Fast Ethernet	2 x RJ45, 10/100Mbps (1 x WAN (default)/LAN, 1 x LAN)	
	Antenna	1 x Wi-Fi HaLow antenna	2 x 2.4GHz/5GHz Wi-Fi antenna
System Control	LED indicators	1 x System indicator	1 x HaLow activity indicator
		1 x WLAN activity indicator	3 x HaLow signal strength indicator
		1 x WAN/LAN link indicator	1 x LAN link indicator
	Button	1 x Pair button for DIP-selected mode	1 x Reset pinhole button
	DIP switch	3 x DIP switch (Standard/Mesh, Base/Node, user defined)	
Mechanical	Dimensions	IP40 version (with wall mount): 130mm x 82.9mm x 42mm	
		IP54 version (with wall mount and water proof kit): 130mm x 127.9mm x 44mm	
	Casing material	Black plastics, UL94, SP6 compliant (Optional: White casing)	
	Installation	Flat mount, wall mount	
	IP rating	IP40 (Optional: IP54, independent waterproof kit)	
Power	Input	9V ~ 40V DC	
	Port	3-pin terminal (Over-current protection, reverse polarity protection)	

HAP202			
Software	Operating system	VantronOS	
	Device management	Vantron BlueSphere GWM	
	Upgrade	Local upgrade, OTA upgrade	
	Network protocol	IPV4, HTTPS, TCP & 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/5GHz Wi-Fi	AES-CCMP	
	Wi-Fi HaLow	AES, WPA3	
	Firewall	Stateful	
	Access control	MAC address, IP address, URL	
Environmental	Temperature	Operating: -20℃ ~ +70℃	Storage: -40℃ ~ +85℃
	Humidity	5% ~ 95%RH (Non-condensing)	
	Certification	FCC, ISED	

1.5 Interfaces and Indicators

1.5.1 Front view

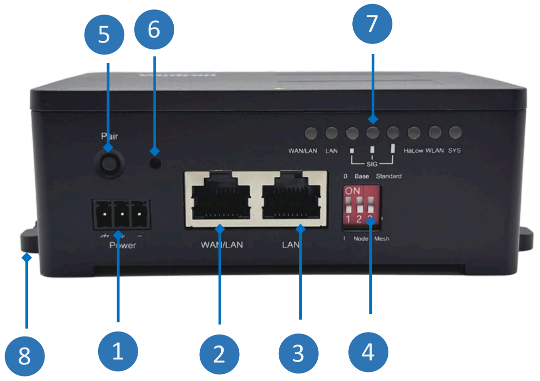


Table 1-2

Indicator/ Interface	Description	
1	Power terminal, supporting 9V~40V DC input	
2	WAN/LAN (100Mbps), configured as a WAN port by default	
3	LAN (100Mbps), mainly for device login	
4	DIP Switches	3 x 2 DIP switch. Refer to section 1.6 for details.
5	Pair button	Activates the device for the DPP-selected mode. Refer to section 1.7 for details.
6	Reset pinhole button	Reset button for device reboot or restart. Refer to section 1.8 for details.
7	LED indicators (Refer to section 1.9)	2 x Ethernet link LED (WAN/LAN)
		3 x HaLow signal strength LED
		1 x HaLow activity LED
		1 x WLAN activity LED
		1 x System status LED
8	Mounting bracket (screws recommended: M3 x 8mm/ST2.9 depending on the mounting surface)	

1.5.2 Back view

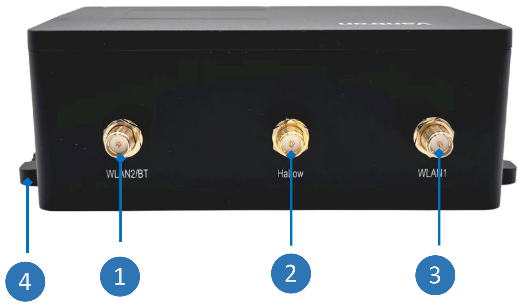


Table 1-3

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

1.6 DIP Switches

HAP202 offers three DIP Switches (3 x 2) that can be configured to different modes as detailed below.

Table 1-4

Switch	Position	Description
Switch 1	0/1	Reserved for user customization.
Switch 2	Base	A HaLow unit that assigns or relays IP addresses to all paired Nodes.
	Node	A HaLow unit that connects to the Base—or to other Nodes in the mesh configuration—to obtain an IP from the upstream network via the Base or to relay data to extend the network coverage.
Switch 3	Standard	Standard HaLow mode.
	Mesh	HaLow mesh mode.

The switch setting alone does **NOT** indicate the current working mode of the device. They are designed to use in combination with the Pair button after power up.

1.7 Pair Button

The Pair button is designed for use in combination with the DIP switches to confirm the switch setup for quick HaLow pairing.

Table 1-5

DPP Setup	Button Action	Description
DIP switches ready	Short press (<1s)	The device enters the DPP pairing state.
	Long press [5s, 10s)	The device cycles through HaLow working modes in sequence: **STA** → **AP** → **Mesh** → **STA**. The selected mode is confirmed when the button is released. The HaLow LED will indicate the current working mode of the device (refer to section 1.9).
DPP pairing in progress	Short press (<1s)	The device exits the DPP pairing process.

1.8 Reset Button

The reset button allows the device to restart or factory reset as defined below:

Table 1-6

Button Hold	LED Status	Description
[2s, 6s)	SYS LED: Red/green alternating (0.5Hz) > solid red > blinking green (3Hz) > solid red > red/green alternating (2Hz) > solid green	Device reboot in progress.
[6s, 12s)	SYS LED: Red/green alternating (0.5Hz) > solid green > red/green alternating (2Hz) > solid green	Device configuration is cleared. You can re-log in to the device with your password and follow the setup wizard to finish the first-time configuration.
[12s, 20s)	1. All LEDs blink at 3Hz. 2. SYS LED: Red/green alternating (3Hz) > solid red > red/green alternating (2Hz) > blinking green (3Hz) > red/green alternating (3Hz) > solid green	The device is factory reset with all configurations, user data, and apps cleared. You must re-log in to the device via the debug port (contact Technical Support).
[20s, +∞)	All LEDs restore to initial status	No device action triggered.

1.9 LED Indicators

1.9.1 Ethernet LEDs

Table 1-7

LED	LED Status	Description
WAN/LAN LAN	ON	The link is up.
	OFF	The link is not reachable.

1.9.2 HaLow Signal Strength LEDs

Table 1-8

LED Status	LED Color	Signal Strength	RSSI Range
ON (HaLow network established)	Left LED: Red	Weak	RSSI (<-70) dBm
	Left LED: Green	Fair	RSSI (-50, -70) dBm
	Left & Mid LEDs: Green	Good	RSSI (-30, -50) dBm
	All three LEDs: Green	Excellent	RSSI (0, -30) dBm

1.9.3 HaLow Activity LED

Table 1-9

Mode	Color	LED Status	Description
HaLow STA	Blue	OFF	Wi-Fi HaLow link is down.
		Blinking at 1Hz	Not connected to a HaLow AP.
		Blinking at 3Hz	DPP pairing initiated via hardware or software configurations.
		Solid on	Connected to a HaLow AP.

Table 1-10

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

1.9.4 WLAN (Wi-Fi) Activity LED

Table 1-11

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

1.9.5 System Status LED

Table 1-12

LED Status	Description
OFF	No power input.
Red	System not running/system fault.
Yellow	Device failure detected (associated with BlueSphere GWM alarm IDs).
Green	Device working properly.
Red/green alternating	Device booting/upgrading/resetting in progress.

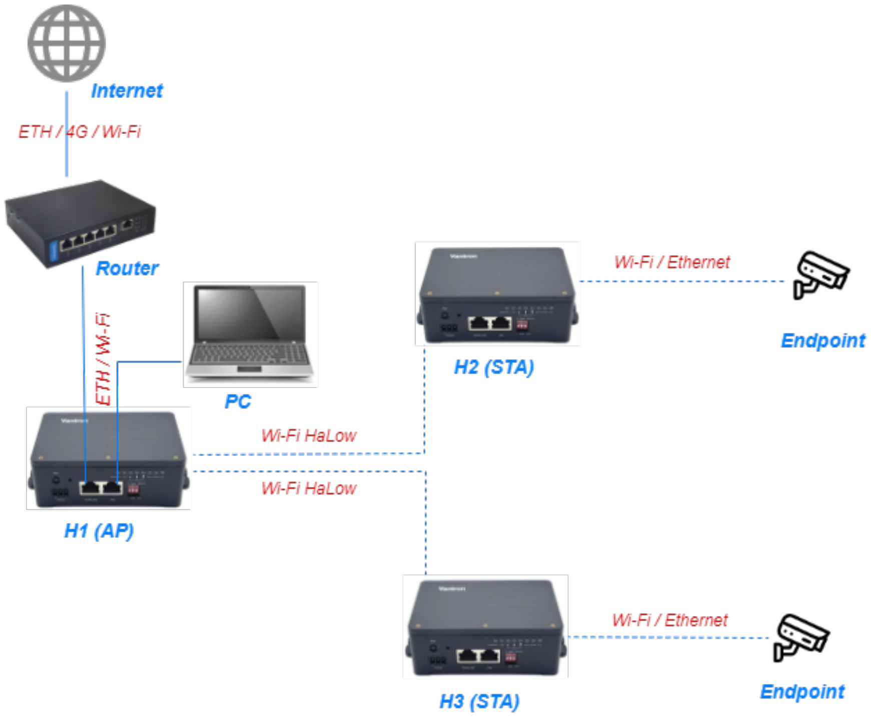
CHAPTER 2 GETTING STARTED

2.1 Network Architecture

HAP202 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 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.

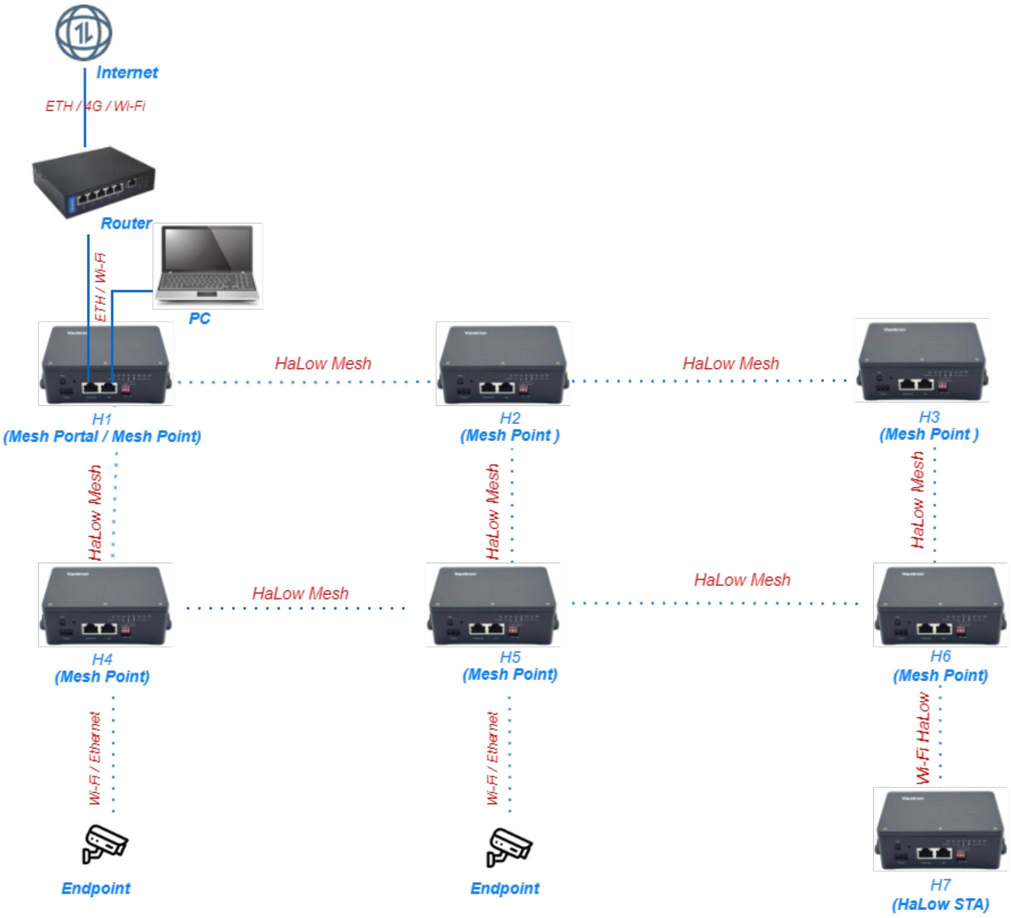


In this topology:

- H1 is the Base that relays/allocates IP addresses.

2.1.2 HaLow Mesh Network

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



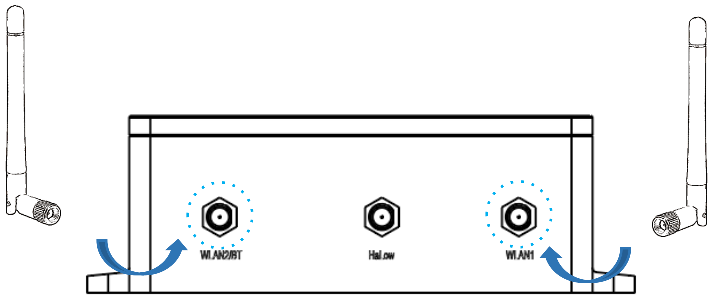
In this topology:

- H1 is the Base that relays/allocates IP addresses.
- 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**.

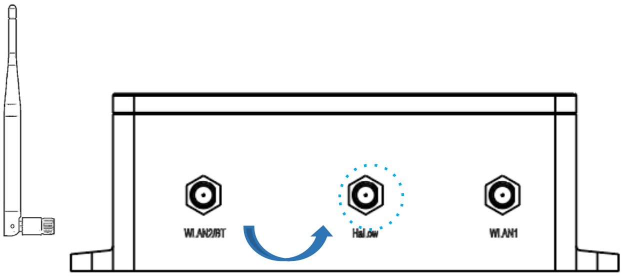
2.2 Setting up the Device

When mounting HAP202 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.

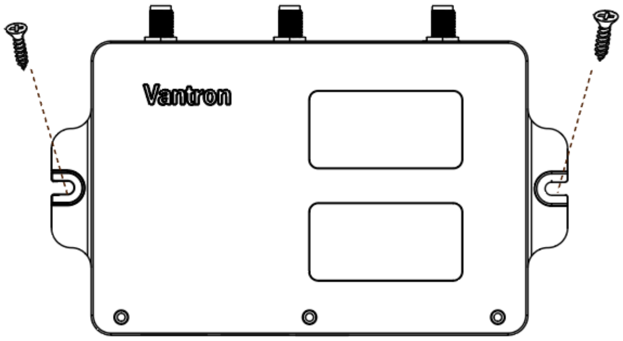
1. Install the shorter antennas to the WLAN antenna connectors (*labelled as WLAN1 and WLAN2/BT*).

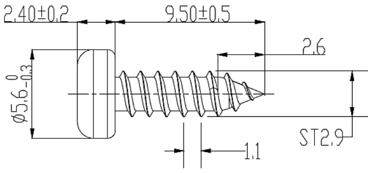


2. Install the longer antenna to the Wi-Fi HaLow antenna connector (*labelled as HaLow*).

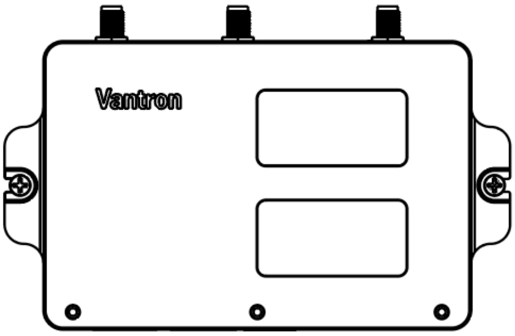


3. Depending on the material of the mounting surface, use two ST2.9 self-tapping screws (for mounting surfaces without provided screws) or two M3 x 8mm screws (for mounting surfaces with provided screws) to fix the device on the mounting surface.

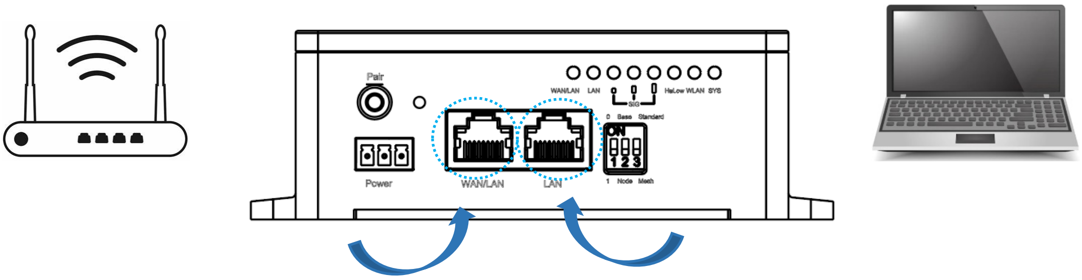




4. Tighten the screws and gently swing the device to make sure it is fastened.



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



2.3 Powering up the Device

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

2.4 Quick Access to the Device

2.4.1 Host PC Login

On power-up, the device can be accessed through either Ethernet or 2.4GHz/5GHz Wi-Fi. Make sure the HAP202 and the host PC are on the same network for device login.

Login Steps:

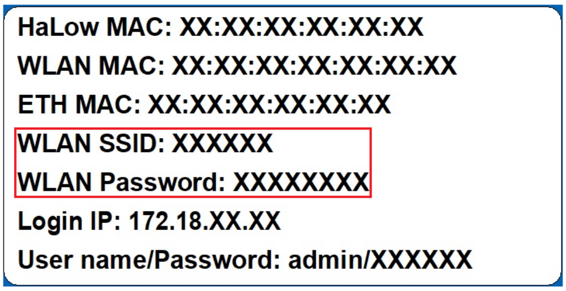
1. Connect the host PC:

   - Via Ethernet

   Connect the host PC directly to the HAP202's LAN port using a standard Ethernet cable.

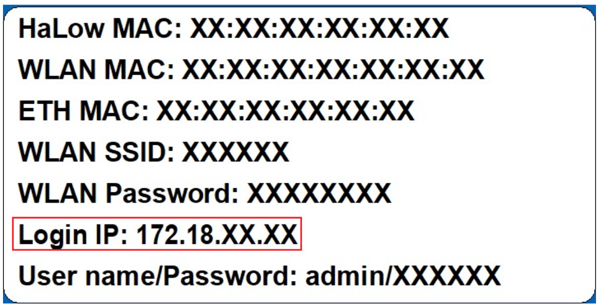
   - Via Wi-Fi

   Connect the host PC to the Wi-Fi AP of the HAP202 using the default SSID and password provided on the device label.



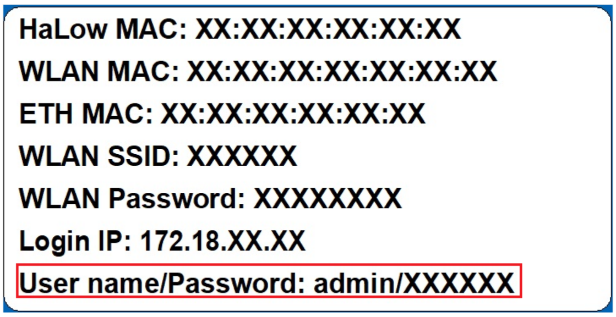
HaLow MAC: XX:XX:XX:XX:XX:XX
WLAN MAC: XX:XX:XX:XX:XX:XX:XX
ETH MAC: XX:XX:XX:XX:XX:XX
WLAN SSID: XXXXXX
WLAN Password: XXXXXXX
Login IP: 172.18.XX.XX
User name/Password: admin/XXXXXX

2. Enter the login IP (HAP202’s IP address) in the browser of the host PC for device login.

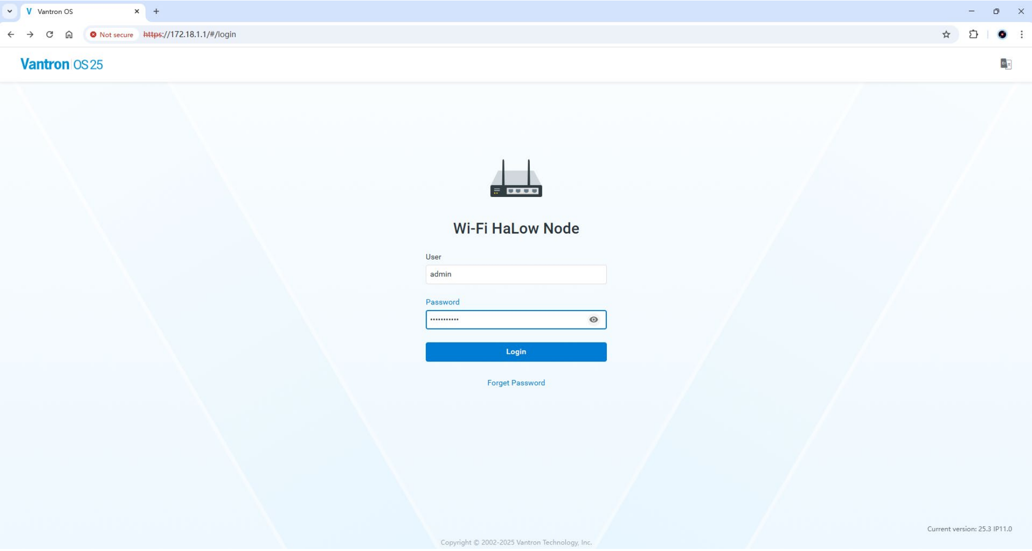


HaLow MAC: XX:XX:XX:XX:XX:XX
WLAN MAC: XX:XX:XX:XX:XX:XX:XX
ETH MAC: XX:XX:XX:XX:XX:XX
WLAN SSID: XXXXXX
WLAN Password: XXXXXXXX
Login IP: 172.18.XX.XX
User name/Password: admin/XXXXXX

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



HaLow MAC: XX:XX:XX:XX:XX:XX
WLAN MAC: XX:XX:XX:XX:XX:XX:XX
ETH MAC: XX:XX:XX:XX:XX:XX
WLAN SSID: XXXXXX
WLAN Password: XXXXXXXX
Login IP: 172.18.XX.XX
User name/Password: admin/XXXXXX


Vantron OS
Not secure
https://172.18.1.1/#/login
Vantron OS 25

Wi-Fi HaLow Node

User
admin

Password
•••••••••••

Login

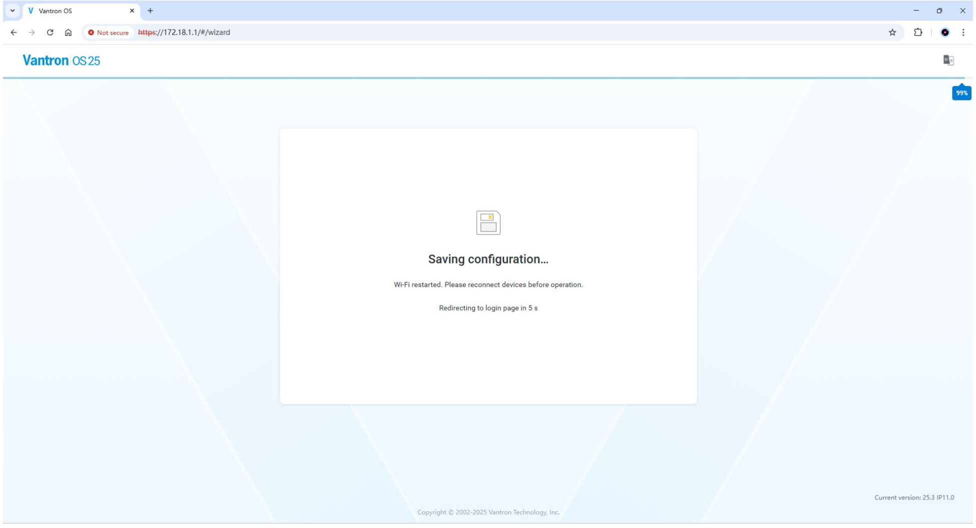
Forget Password

Copyright © 2002-2025 Vantron Technology, Inc.
Current version: 25.3 IP11.0

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

- 2.4GHz/5GHz 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** tab after login)
- Time zone

5. Modify the settings as needed and wait about 20 seconds for new configurations to take effect.


Vantron OS
Not secure
https://172.18.1.1/#/wizard
Vantron OS 25
99%

Saving configuration...

Wi-Fi restarted. Please reconnect devices before operation.

Redirecting to login page in 5 s

Copyright © 2002-2025 Vantron Technology, Inc.
Current version: 25.3 IP11.0

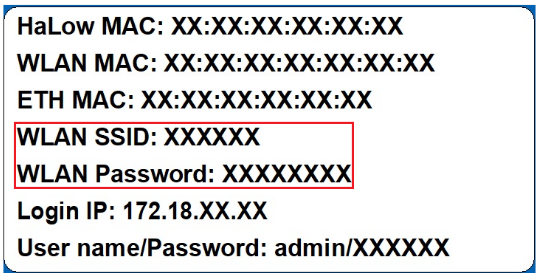
6. After the wizard finishes, HAP202 will restart its wireless radio. If you have previously connected the host PC to the device via 2.4GHz/5GHz Wi-Fi, you will need to reconnect the host PC to the device's network.
7. On the reloaded login page, enter the new password (if you changed it during the setup) to access the web portal.

2.4.2 Mobile Setup

Mobile Web Tool is a quick-configuration utility for the HAP202, designed for phones, tablets, and other mobile devices. It provides network diagnostics, mesh-node RSSI-threshold settings, and other essential functions. Make sure the HAP202 and the mobile device are on the same network for device login.

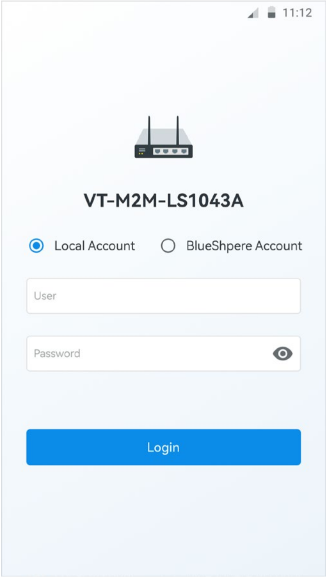
Login Steps:

1. Make sure HAP202's 2.4GHz/5GHz Wi-Fi operates in AP mode.
2. Connect your phone, tablet or other mobile device to the Wi-Fi AP using the provided SSID and password.

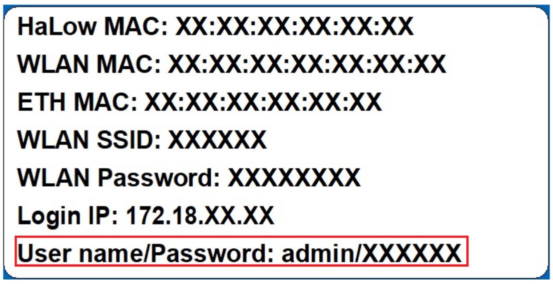


HaLow MAC: XX:XX:XX:XX:XX:XX
WLAN MAC: XX:XX:XX:XX:XX:XX:XX
ETH MAC: XX:XX:XX:XX:XX:XX
WLAN SSID: XXXXXX
WLAN Password: XXXXXXXX
Login IP: 172.18.XX.XX
User name/Password: admin/XXXXXX

3. Open a browser, enter the login IP (HAP202's IP address), and Mobile Web Tool will load.

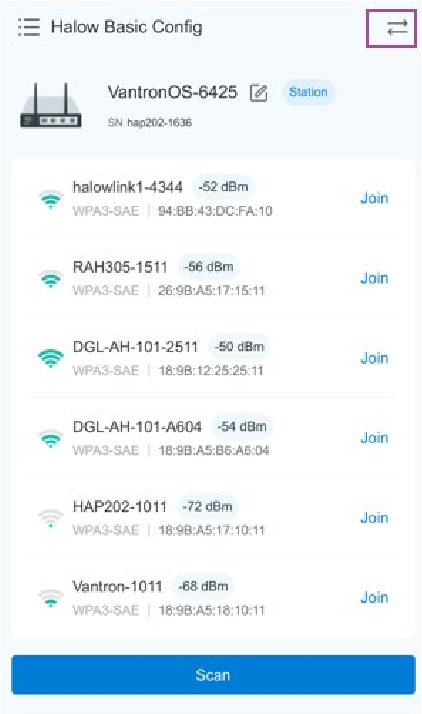


4. Log in to the management portal using the username and password on the device label.



HaLow MAC: XX:XX:XX:XX:XX:XX
WLAN MAC: XX:XX:XX:XX:XX:XX:XX
ETH MAC: XX:XX:XX:XX:XX:XX
WLAN SSID: XXXXXX
WLAN Password: XXXXXXXX
Login IP: 172.18.XX.XX
User name/Password: admin/XXXXXX

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



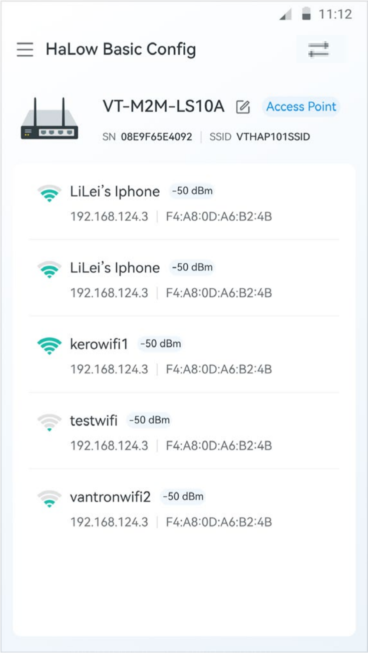
Halow Basic Config

VantronOS-6425 Station
SN hap202-1636

halowlink1-4344 -52 dBm	WPA3-SAE | 94:BB:43:DC:FA:10	Join
RAH305-1511 -56 dBm	WPA3-SAE | 26:9B:A5:17:15:11	Join
DGL-AH-101-2511 -50 dBm	WPA3-SAE | 18:9B:12:25:25:11	Join
DGL-AH-101-A604 -54 dBm	WPA3-SAE | 18:9B:A5:B6:A6:04	Join
HAP202-1011 -72 dBm	WPA3-SAE | 18:9B:A5:17:10:11	Join
Vantron-1011 -68 dBm	WPA3-SAE | 18:9B:A5:18:10:11	Join

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.



11:12

HaLow Basic Config

VT-M2M-LS10A Access Point

SN 08E9F65E4092 | SSID VTHAP101SSID

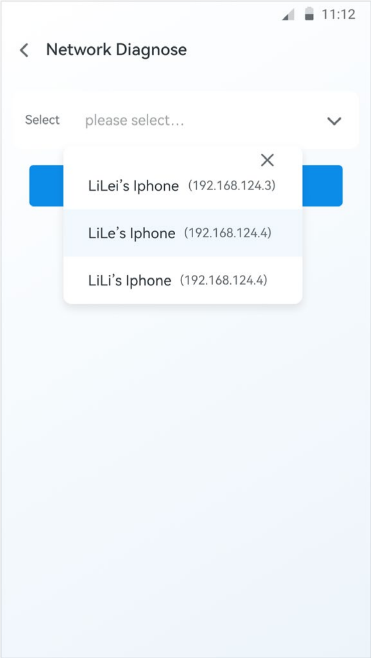
LiLei's Iphone -50 dBm
192.168.124.3 | F4:A8:0D:A6:B2:4B

LiLei's Iphone -50 dBm
192.168.124.3 | F4:A8:0D:A6:B2:4B

kerowifi1 -50 dBm
192.168.124.3 | F4:A8:0D:A6:B2:4B

testwifi -50 dBm
192.168.124.3 | F4:A8:0D:A6:B2:4B

vantronwifi2 -50 dBm
192.168.124.3 | F4:A8:0D:A6:B2:4B

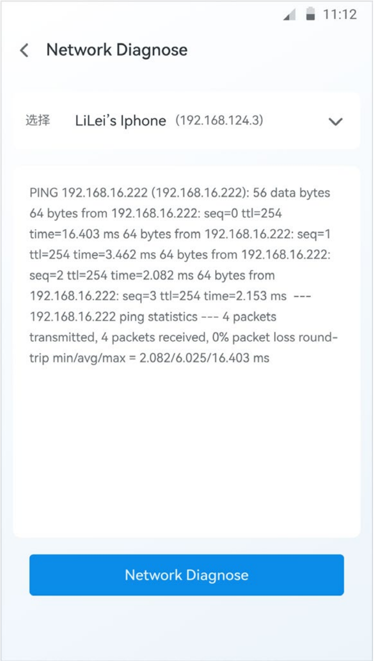


11:12

Network Diagnose

Select please select...

LiLei's Iphone (192.168.124.3)
LiLe's Iphone (192.168.124.4)
LiLi's Iphone (192.168.124.4)



11:12

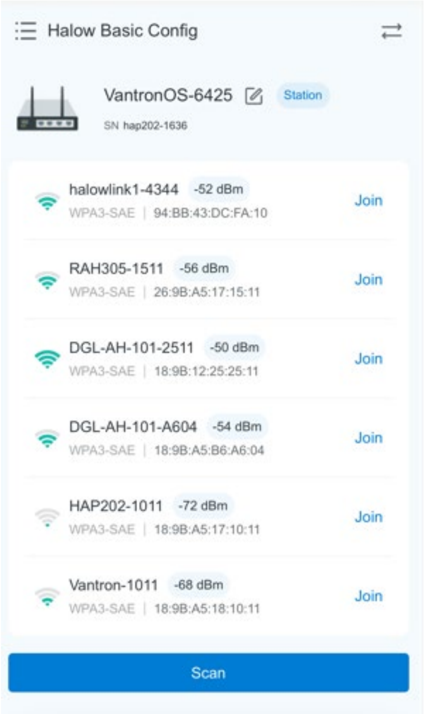
Network Diagnose

选择 LiLei's Iphone (192.168.124.3)

```
PING 192.168.16.222 (192.168.16.222): 56 data bytes
64 bytes from 192.168.16.222: seq=0 ttl=254
time=16.403 ms 64 bytes from 192.168.16.222: seq=1
ttl=254 time=3.462 ms 64 bytes from 192.168.16.222:
seq=2 ttl=254 time=2.082 ms 64 bytes from
192.168.16.222: seq=3 ttl=254 time=2.153 ms ---
192.168.16.222 ping statistics --- 4 packets
transmitted, 4 packets received, 0% packet loss round-
trip min/avg/max = 2.082/6.025/16.403 ms
```

Available STA-Mode Configurations:

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



Halow Basic Config

VantronOS-6425 Station

SN hap202-1636

halowlink1-4344 -52 dBm
WPA3-SAE | 94:BB:43:DC:FA:10 Join

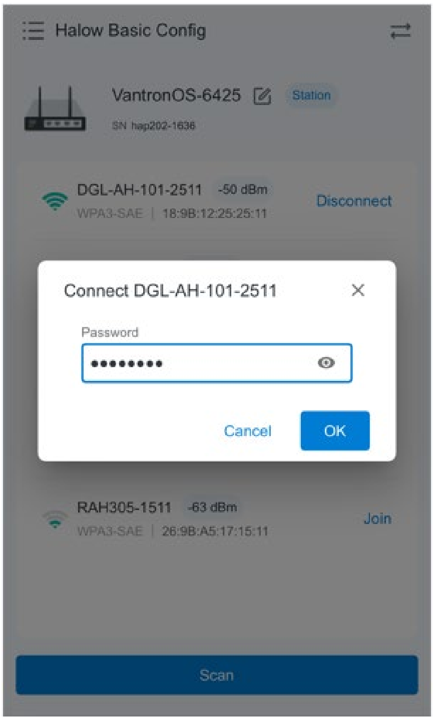
RAH305-1511 -56 dBm
WPA3-SAE | 26:9B:A5:17:15:11 Join

DGL-AH-101-2511 -50 dBm
WPA3-SAE | 18:9B:12:25:25:11 Join

DGL-AH-101-A604 -54 dBm
WPA3-SAE | 18:9B:A5:B6:A6:04 Join

HAP202-1011 -72 dBm
WPA3-SAE | 18:9B:A5:17:10:11 Join

Vantron-1011 -68 dBm
WPA3-SAE | 18:9B:A5:18:10:11 Join



Halow Basic Config

VantronOS-6425 Station

SN hap202-1636

DGL-AH-101-2511 -50 dBm
WPA3-SAE | 18:9B:12:25:25:11 Disconnect

Connect DGL-AH-101-2511

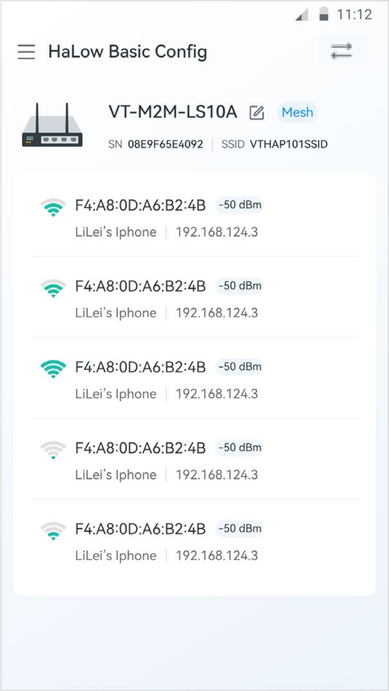
Password: ●●●●●●●●●

Cancel OK

RAH305-1511 -63 dBm
WPA3-SAE | 26:9B:A5:17:15:11 Join

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.



11:12

HaLow Basic Config

VT-M2M-LS10A Mesh

SN 08E9F65E4092 | SSID VTHAP101SSID

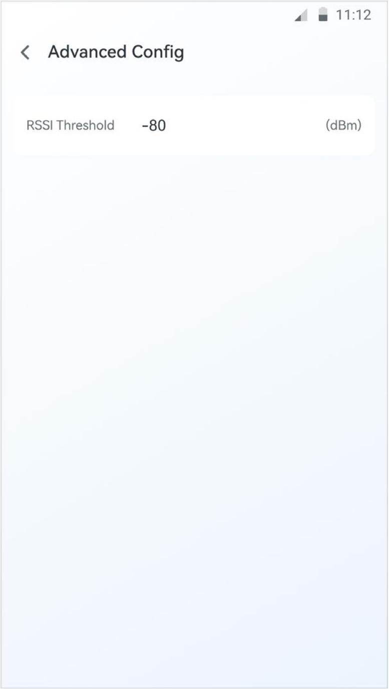
F4:A8:0D:A6:B2:4B -50 dBm
LiLei's Iphone | 192.168.124.3

F4:A8:0D:A6:B2:4B -50 dBm
LiLei's Iphone | 192.168.124.3

F4:A8:0D:A6:B2:4B -50 dBm
LiLei's Iphone | 192.168.124.3

F4:A8:0D:A6:B2:4B -50 dBm
LiLei's Iphone | 192.168.124.3

F4:A8:0D:A6:B2:4B -50 dBm
LiLei's Iphone | 192.168.124.3



11:12

Advanced Config

RSSI Threshold -80 (dBm)

2.5 Default Network Interface Status

Table 2-1

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

2.6 DPP Pairing

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

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, please refer to sections 1.6, 1.7, and 1.9 for description on the DIP switches, the Pair button, and corresponding LED status, respectively.

Note:

There will always be only **one** HaLow AP (Base) 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 Pair button activates DPP mode, which remains valid for a maximum of **120** seconds.

Table 2-2 DIP Switch Setup for DPP Pairing

Device	Switch 2	Switch 3	Result
H1	Base	Standard	HaLow DPP state in the HaLow AP mode
H2	Node	Standard	HaLow DPP state in the HaLow STA mode
Hn	Node	Standard	HaLow DPP state in the HaLow STA mode

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

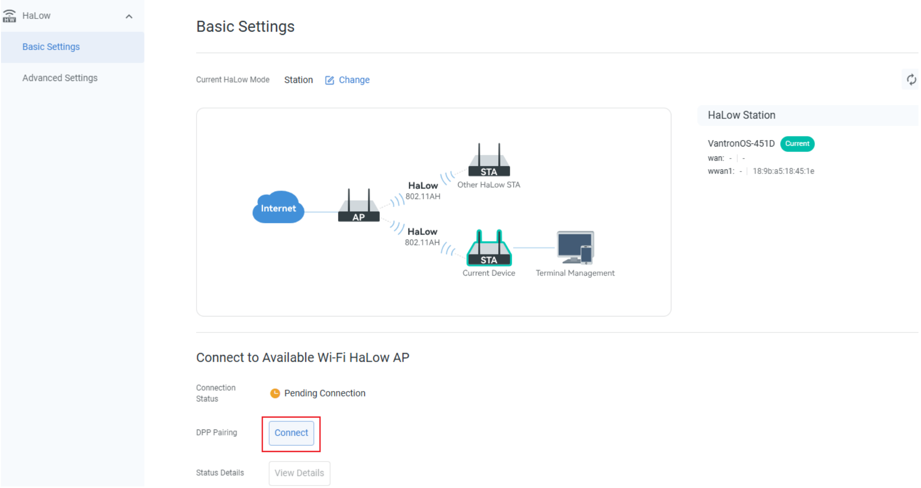
1. Make sure both HAP202 units are powered on and next to each other.
2. Short press (< 1s) the Pair button on both devices to activate the **pairing state**. Make sure the time interval between button actions on both devices is within 120 seconds.
3. Upon successful connection, the devices will exit the HaLow DPP mode.
4. Enable the DPP mode on the AP and repeat above steps for the remaining STAs, if any.
5. Move the devices to the desired locations after pairing.

2.6.2 DPP Pairing via Software Setup

The software setup is completed via the VantronOS web management portal. Given that the device is factory-set to HaLow STA mode, you may need to switch it to AP mode within VantronOS as described in section 3.5.1.1.

1. Prepare two HAP202 units, one in AP mode and one in STA mode.
2. Make sure both HAP202 units are powered on and 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 the **Connect** button.



Basic Settings

Current HaLow Mode Station Change

HaLow Station

VantronOS-451D Current
wan: - | -
wwan1: - | 18:9b:a5:18:45:1e

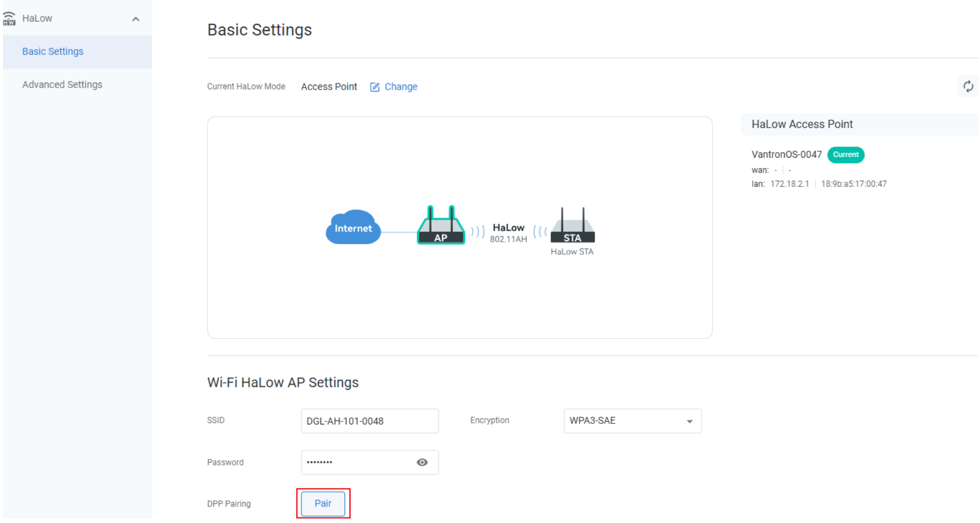
Connect to Available Wi-Fi HaLow AP

Connection Status: Pending Connection

DPP Pairing: Connect

Status Details: View Details

6. For the **AP**: In the **Wi-Fi HaLow AP Settings** section, click the **Pair** button.



Basic Settings

Current HaLow Mode Access Point Change

HaLow Access Point

VantronOS-0047 Current
wan: - | -
lan: 172.18.2.1 | 18:9b:a5:17:00:47

Wi-Fi HaLow AP Settings

SSID: DGL-AH-101-0048

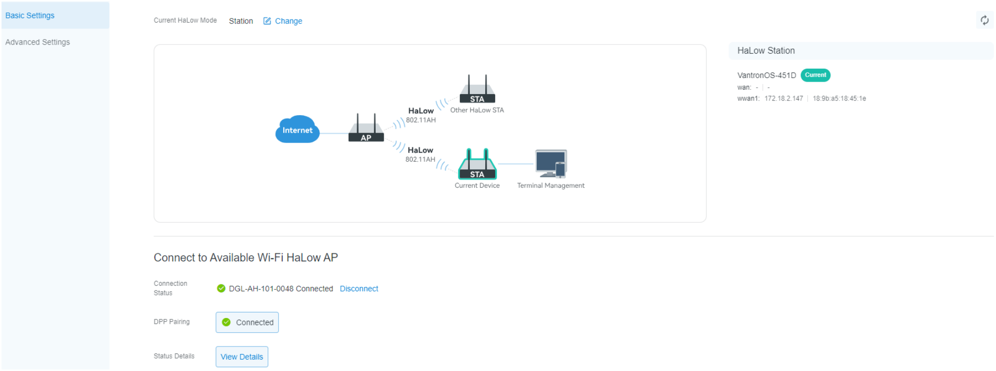
Encryption: WPA3-SAE

Password: ••••••••

DPP Pairing: Pair

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

STA-side connection:



Current HaLow Mode Station Change

HaLow Station

VantronOS-451D Current
wan: - | -
wwan1: 172.18.2.147 | 18:9b:a5:18:45:1e

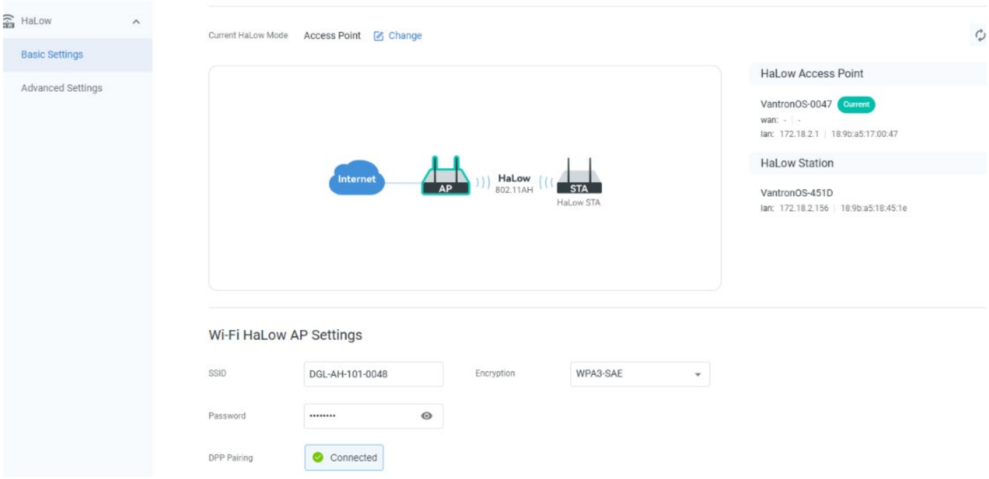
Connect to Available Wi-Fi HaLow AP

Connection Status: DGL-AH-101-0048 Connected Disconnect

DPP Pairing: Connected

Status Details: View Details

AP-side connection:



Current HaLow Mode Access Point

HaLow Access Point

VantronOS-0047
wan: - | -
lan: 172.18.2.1 | 18:9b:a5:17:00:47

HaLow Station

VantronOS-451D
lan: 172.18.2.156 | 18:9b:a5:18:45:1e

Wi-Fi HaLow AP Settings

SSID DGL-AH-101-0048

Encryption WPA3-SAE

Password ••••••••

DPP Pairing Connected

- For the STA: You can access the connection details by clicking **View Details**.
- For the AP: You can access the connection details in the **Network Topology** Page.

8. Brief connection information will display next to the topology.
9. Enable the DPP mode on the AP and repeat above steps for the remaining STAs, if any.
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. A HaLow connection is successfully established.

b. The Pair button is pressed after the device enters the pairing mode.

c. The target device fails to enable the pairing mode within **120 seconds** after the first device does.

d. The HaLow connection between both devices fails.

2.7 Quick Mesh Networking

By default, HAP202 units are pre-configured with common Mesh settings. With Mesh configuration enabled, a 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 3.5.1.3.

Table 2-3 DIP Switch Setup for Quick Mesh Networking

Device	Switch 2	Switch 3	Result
H1	Base*	Mesh	Quick Mesh configuration as a HaLow Base
H2	Node	Mesh	Quick Mesh configuration as a HaLow Node
Hn	Node	Mesh	Quick Mesh configuration as a HaLow Node

* A Base in a Mesh network is either a **Mesh Portal (MPP)** that allocates the IP addresses or a **Mesh Point (MP)** that relays the IP addresses from the upstream network.

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

1. Power on these units.
2. Short press (< 1s) the Pair button of the device to enable the **Mesh configuration**.
3. If no Mesh Portal (MPP) is present, connect a designated Mesh Point (MP) to an external router via Wi-Fi or Ethernet WAN for IP assignment.
4. Additional MPs can be added to the network at any time by repeating this procedure.

Note:

There will always be only **one** Base in a Mesh network. Additional Nodes can be dynamically configured to join the Mesh network at any time after the network is established.

2.8 SSH Login

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

Table 2-4 SSH Login Options

Method	Host PC Connection	Login Address
Option 1	Host connects to the device's Ethernet LAN port or 2.4GHz/5GHz Wi-Fi.	Use HAP202's LAN IP
Option 2	Host's WAN interface on the same IP subnet as HAP202's WAN interface	Use HAP202's WAN port IP
Option 3	HAP202's debug port connection (serial session rather than SSH)	Use the debug port parameters (57600, 8N1)

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

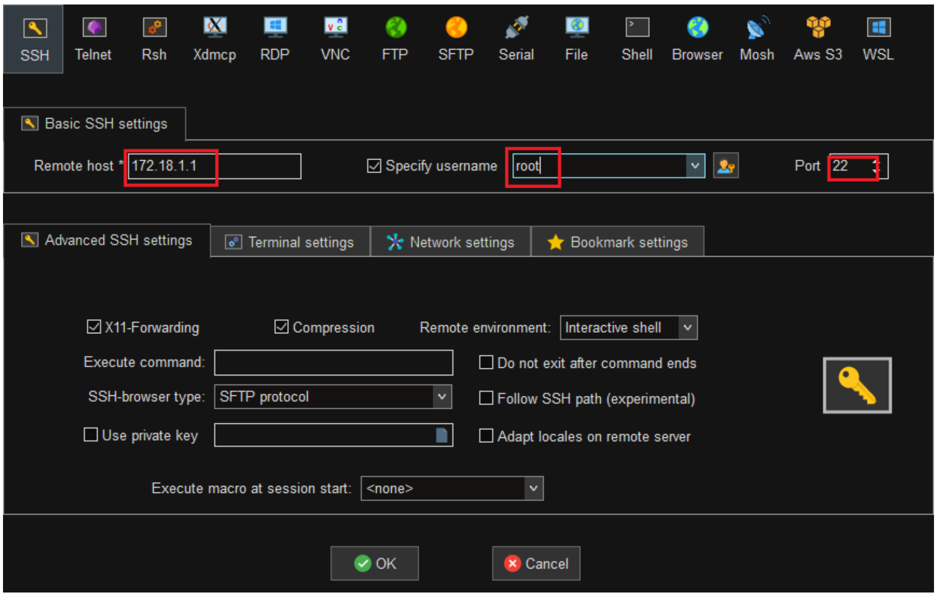
Option 1 is used in most cases.

For option 2, read the device's WAN IP from the 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.

SSH login via LAN IP:

1. Connect a Windows host PC to HAP202's LAN port via Ethernet or 2.4GHz/5GHz Wi-Fi.
2. Open a serial debug program (PuTTY or MobaXterm recommended) on the host PC.
3. Select **SSH** session.
4. Enter HAP202's LAN IP, keep the default SSH port No. (22) unchanged, and use "root" as the username.



Remote host * 172.18.1.1

☑ Specify username root

Port 22

☑ X11-Forwarding ☑ Compression Remote environment: Interactive shell

Execute command:

☐ Do not exit after command ends

SSH-browser type: SFTP protocol

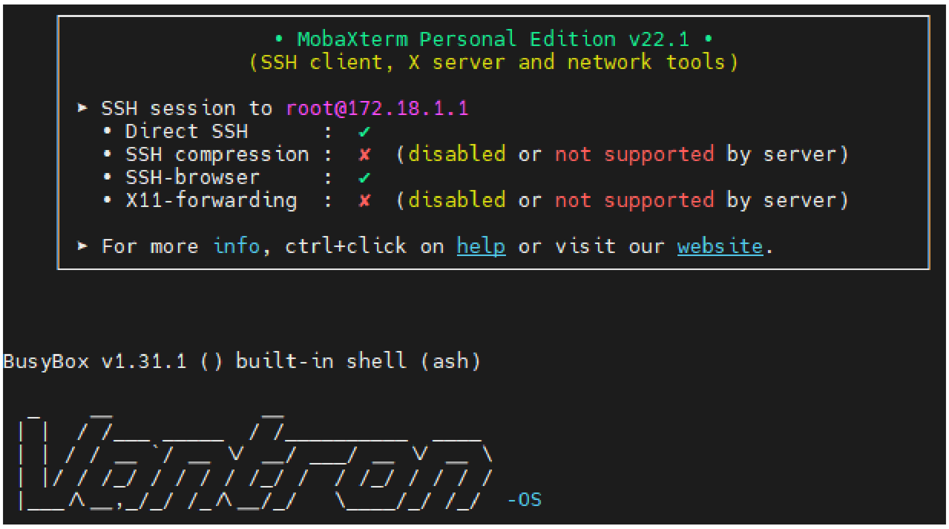
☐ Follow SSH path (experimental)

☐ Use private key

☐ Adapt locales on remote server

Execute macro at session start: <none>

5. Click **OK** to open the session.



```
                 • MobaXterm Personal Edition v22.1 •
               (SSH client, X server and network tools)

   ➤ SSH session to root@172.18.1.1
     • Direct SSH      :  ✓
     • SSH compression :  ✘  (disabled or not supported by server)
     • SSH-browser     :  ✓
     • X11-forwarding  :  ✘  (disabled or not supported by server)

   ➤ For more info, ctrl+click on help or visit our website.


BusyBox v1.31.1 () built-in shell (ash)

  _    __            __
 | |  / /___ _____  / /__________  ____
 | | / / __ `/ __ \/ __/ ___/ __ \/ __ \
 | |/ / /_/ / / / / /_/ /  / /_/ / / / /
 |___/\__,_/_/ /_/\__/_/   \____/_/ /_/  -OS
```

SSH login requires root privileges. The root password is unique to each device due to security concern. Please contact the Vantron FAE team to obtain 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 the HAP202, ensure you are an authorized BlueSphere GWM user with a valid customer ID. Refer to section 3.7.4.1 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/5GHz 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** button (refer to section 1.8 for details on the duration).
2. Release the button.
3. The SYS LED reacts as described in section 1.8.
4. Wait about 10 minutes before the process completes.

2.10.2 Software Reset

1. Log in to VantronOS by referring to section 2.4.1.
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. Click the **Reset** button under **Device Maintenance**.
5. The progress bar will display the reset status. The process takes approximately 10 minutes to complete.

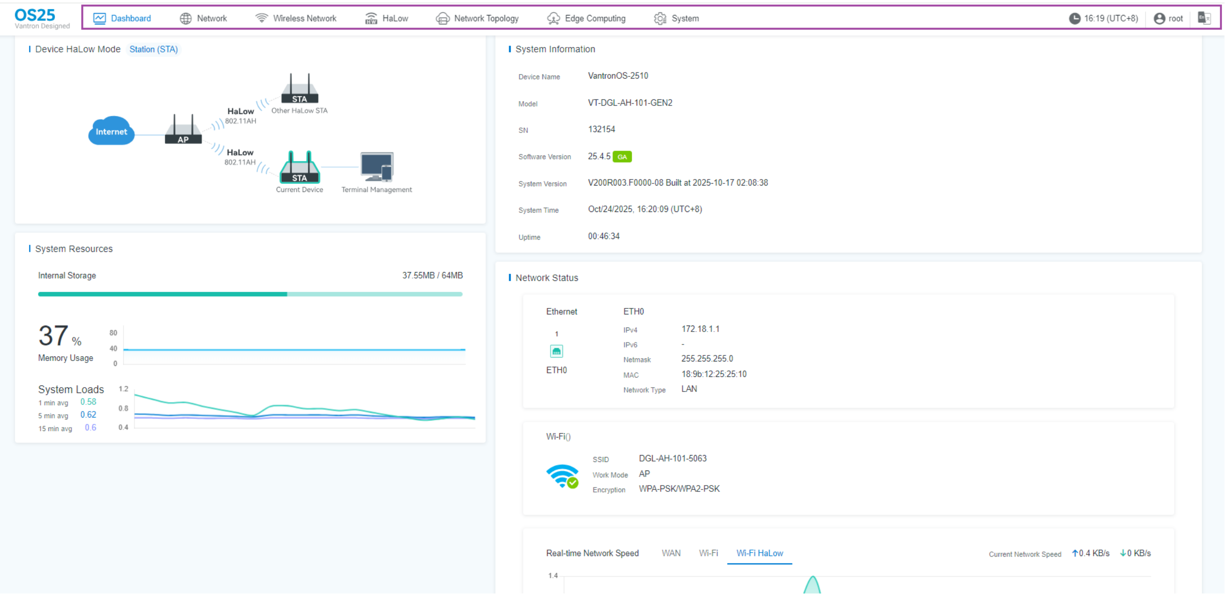
CHAPTER 3 DEVICE SETUP IN VANTRONOS

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



Device HaLow Mode Station (STA)

System Resources

Internal Storage 37.55MB / 64MB

37 %
Memory Usage

System Loads
1 min avg 0.58
5 min avg 0.62
15 min avg 0.6

System Information

Device Name	VantronOS-2510
Model	VT-DGL-AH-101-GEN2
SN	132154
Software Version	25.4.5 GA
System Version	V200R003.F0000-08 Built at 2025-10-17 02:08:38
System Time	Oct/24/2025, 16:20:09 (UTC+8)
Uptime	00:46:34

Network Status

Ethernet
1
ETH0

ETH0

IPv4	172.18.1.1
IPv6	-
Netmask	255.255.255.0
MAC	18:9b:12:25:25:10
Network Type	LAN

Wi-Fi()

SSID	DGL-AH-101-5063
Work Mode	AP
Encryption	WPA-PSK/WPA2-PSK

Real-time Network Speed

Current Network Speed ↑0.4 KB/s ↓0 KB/s

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

Dashboard: Displays general device information and dynamic status updates.

Network: Manages network settings, including interface setup, link management, and security configurations.

Wireless Network: Configures device settings for Wi-Fi connectivity.

Network Topology: Provides information of connected devices (downlink devices). Devices connected via a bridged interface will be invisible.

Edge Computing: Configures the device for field endpoint connection and data processing.

System: Displays device information, system settings, network diagnostics, connection with BlueSphere GWM.

Time Settings:

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

Refer to section 3.8.1.2 for modifying the time settings.

User Avatar: For log out selection upon a click.

Language Toggle: English ⇄ Chinese.

3.1.2 Log Out

To sign out:

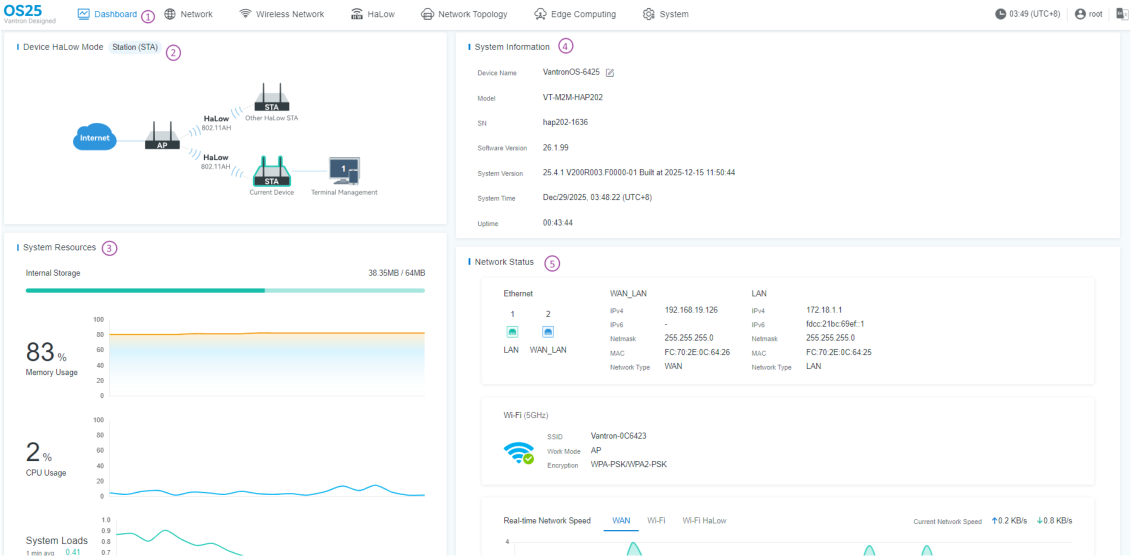
1. Click the user avatar in the upper right corner.
2. Select **Logout**.
3. Confirm the action by clicking **Logout** again.

3.1.3 Language Change

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

3.2 Dashboard

This page provides the overall information of HAP202, including a network topology, the system information, device resource usage, interface connection status, traffic statistics, etc.



Internal Storage 38.35MB / 64MB

83 % Memory Usage

2 % CPU Usage

System Loads 1 min avg 0.41

Device Name VantronOS-6425
Model VT-M2M-HAP202
SN hap202-1636
Software Version 26.1.99
System Version 25.4.1 V200R003.F0000-01 Built at 2025-12-15 11:50:44
System Time Dec/29/2025, 03:48:22 (UTC+8)
Uptime 00:43:44

	WAN_LAN		LAN
IPv4	192.168.19.126	IPv4	172.18.1.1
IPv6	-	IPv6	fdcc:21bc:69ef::1
Netmask	255.255.255.0	Netmask	255.255.255.0
MAC	FC:70:2E:0C:64:26	MAC	FC:70:2E:0C:64:25
Network Type	WAN	Network Type	LAN

Wi-Fi (5GHz)
SSID Vantron-0C6423
Work Mode AP
Encryption WPA-PSK/WPA2-PSK

Current Network Speed ↑0.2 KB/s ↓0.8 KB/s

Description of the numbered areas

1. **Menu Tabs**—highlighting the active menu in blue.
2. **Device HaLow Mode**—presenting the device's HaLow mode in a network topology, with the "Current Device" indicating the role of your unit. To manage the downlink device, click the "Terminal Management" icon to access the **Network Topology** page.
3. **System Resources**—indicating the device's performance, mainly including: storage space (used/total), memory usage, and system loads (1-, 5-, 15-minute averages).
4. **System Information**—including: device name, model, serial number, software version, firmware version, current host time, and uptime.
5. **Network Status**—live status and throughput for each interface.
   - Ethernet: LAN and WAN/LAN port IP addresses, subnet masks, MAC addresses, and network types.

     Clicking the Ethernet port icon will direct you to corresponding interface settings.
   - Wi-Fi: 2.4GHz/5GHz Wi-Fi (operation mode and corresponding information).
   - Real-time network speeds: Uplink WAN/Wi-Fi (client)/Wi-Fi HaLow (STA) speeds.

3.3 Network

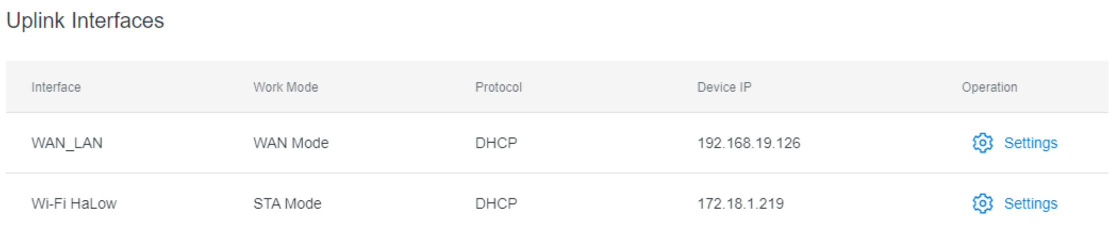
The **Network** menu centralizes critical network management functions, including interface settings, link redundancy, static routing, and more. These features enable precise control over connectivity, ensuring optimal performance and high availability. By integrating these tools, the system reduces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

3.3.1 Interface Settings

Interfaces are categorized into uplink and downlink domains.

On HAP202, uplink interfaces include Wi-Fi client, HaLow STA, HaLow Mesh Point, and Ethernet WAN; downlink interfaces consist of Wi-Fi AP, HaLow AP, HaLow Mesh Portal, and Ethernet LAN.

3.3.1.1 Uplink Interfaces



Uplink Interfaces

Interface	Work Mode	Protocol	Device IP	Operation
WAN_LAN	WAN Mode	DHCP	192.168.19.126	Settings
Wi-Fi HaLow	STA Mode	DHCP	172.18.1.219	Settings

The above screenshot is for illustration only. In a typical deployment, individual HaLow stations would not be connected as standalone units to an external network. Instead, it is the HaLow AP that typically connects to the external network.

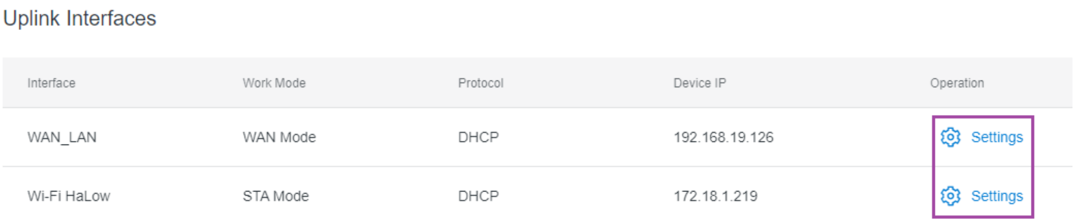
Clicking the **Settings** icon next to an uplink interface allows you to select an IP configuration mode for the interface.

3.3.1.2 IP Configuration Mode

There are different IP configuration modes for uplink interfaces.

To select the IP configuration mode:

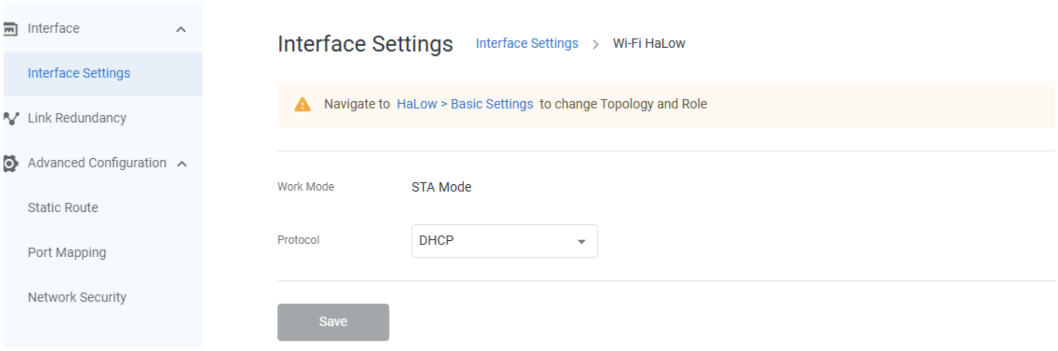
Click the **Settings** icon next to an uplink interface.



Uplink Interfaces

Interface	Work Mode	Protocol	Device IP	Operation
WAN_LAN	WAN Mode	DHCP	192.168.19.126	⚙ Settings
Wi-Fi HaLow	STA Mode	DHCP	172.18.1.219	⚙ Settings

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



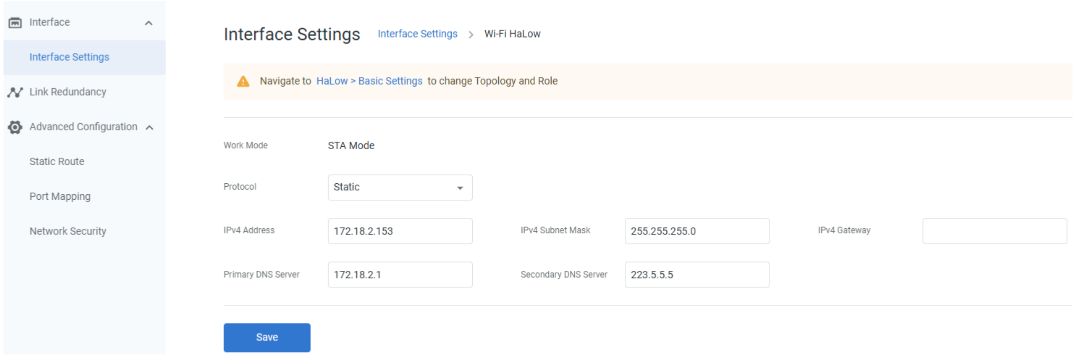
Interface Settings   Interface Settings > Wi-Fi HaLow

Navigate to HaLow > Basic Settings to change Topology and Role

Work Mode: STA Mode

Protocol: DHCP

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



Interface Settings   Interface Settings > Wi-Fi HaLow

Navigate to HaLow > Basic Settings to change Topology and Role

Work Mode: STA Mode

Protocol: Static

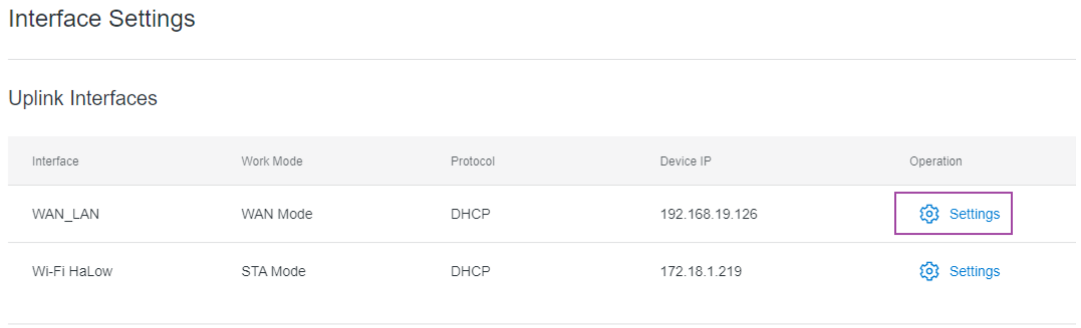
IPv4 Address: 172.18.2.153   IPv4 Subnet Mask: 255.255.255.0   IPv4 Gateway:

Primary DNS Server: 172.18.2.1   Secondary DNS Server: 223.5.5.5

3.3.1.3 WAN/LAN Mode Change

The WAN/LAN port defaults to WAN mode. When necessary, you can modify it to the LAN mode:

1. Click the **Settings** icon next to the WAN_LAN port.

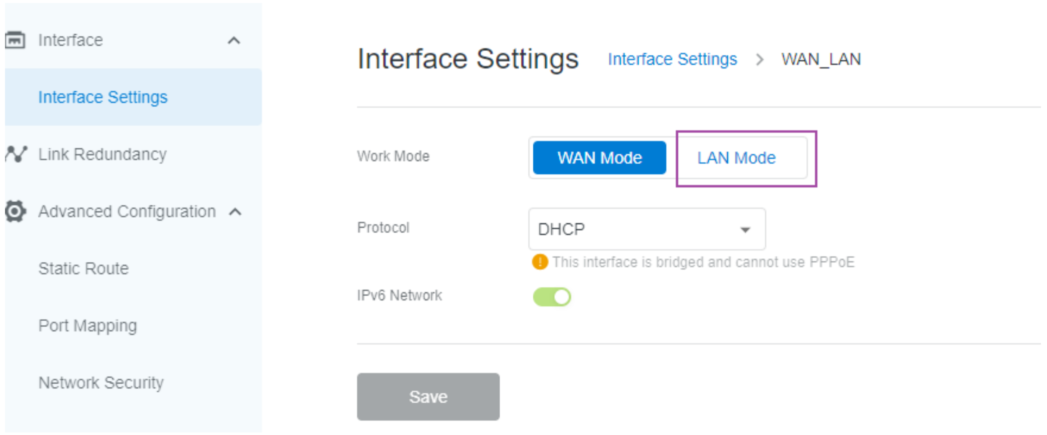


Interface Settings

Uplink Interfaces

Interface	Work Mode	Protocol	Device IP	Operation
WAN_LAN	WAN Mode	DHCP	192.168.19.126	Settings
Wi-Fi HaLow	STA Mode	DHCP	172.18.1.219	Settings

2. Click **LAN** to change to this work mode.



Work Mode: WAN Mode | LAN Mode

Protocol: DHCP

This interface is bridged and cannot use PPPoE

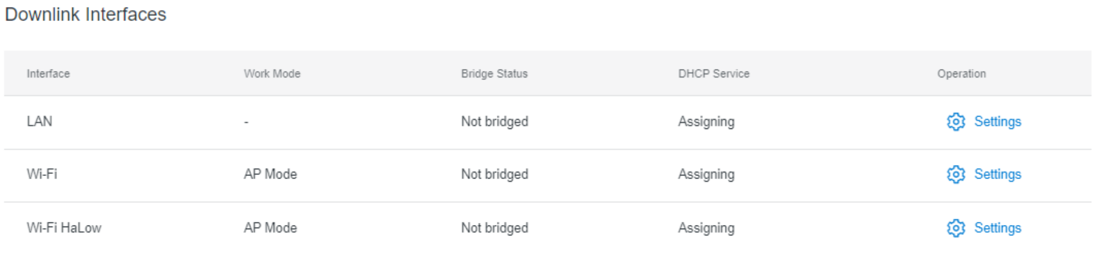
IPv6 Network

3. Click **Confirm** to validate the modification.

If you are currently using the WAN port for internet access or device management, please ensure that you have switched to an alternative connection method.

To switch back to WAN mode, navigate to the **Settings** icon next to the port in the **Downlink Interfaces** section and complete the mode change.

3.3.1.4 Downlink Interfaces

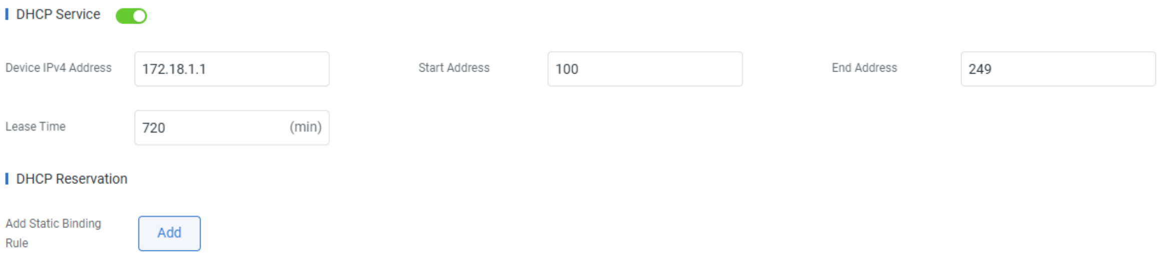


Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
LAN	-	Not bridged	Assigning	⚙ Settings
Wi-Fi	AP Mode	Not bridged	Assigning	⚙ Settings
Wi-Fi HaLow	AP Mode	Not bridged	Assigning	⚙ Settings

Clicking the **Settings** icon for a downlink interface that offers DHCP service allows you to choose whether to bridge the interface to an uplink interface that connects to a DHCP server. If enabled, client devices connected to the HAP202 through this link will receive an IP from the DHCP server. Refer to section 3.3.1.6 for the configurations.

3.3.1.5 DHCP Service & DHCP Reservation



DHCP Service ●

Device IPv4 Address	172.18.1.1	Start Address	100	End Address	249
Lease Time	720 (min)				

DHCP Reservation

Add Static Binding Rule: Add

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

Editable fields under **DHCP Service**:

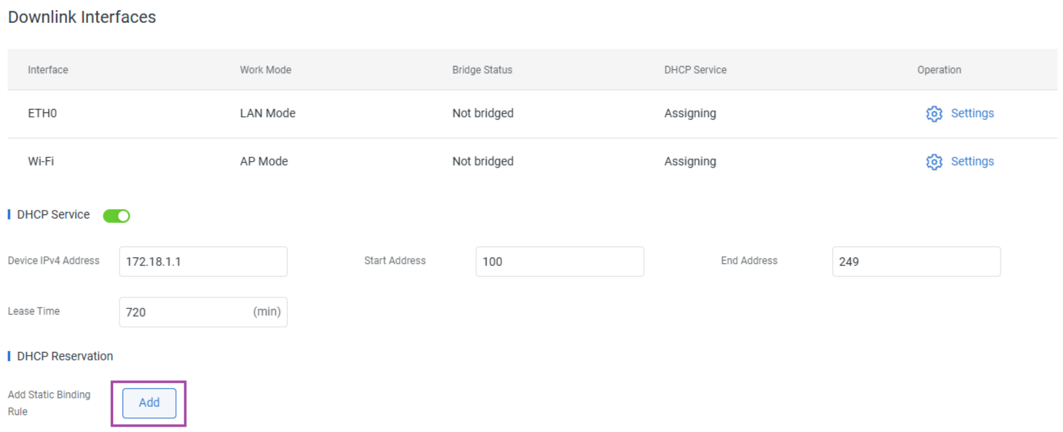
- Device IPv4 address: HAP202's own IP address on the downlink domain.
- Start & End addresses: The pool from which addresses are leased to clients.
- Lease Time: The valid duration for which HAP202, as the DHCP server, assigns an IP address to a client. Before expiry of the lease time, the client will send a renew request to HAP202 to extend the lease. If the renewal fails and the lease expires, the client must release this IP address and initiate a new DHCP discovery.

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

By adding a DHCP reservation rule to HAP202, 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**.



Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
ETH0	LAN Mode	Not bridged	Assigning	Settings
Wi-Fi	AP Mode	Not bridged	Assigning	Settings

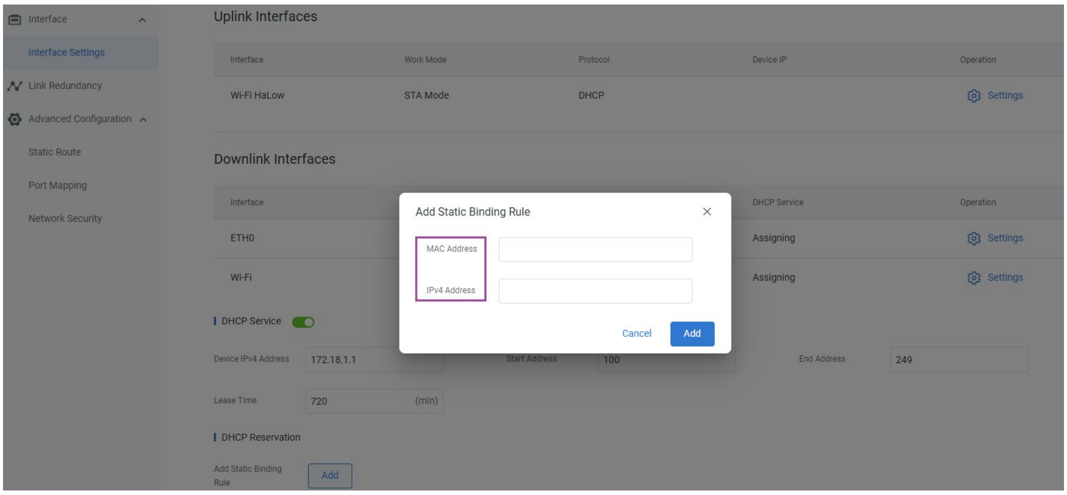
DHCP Service

Device IPv4 Address: 172.18.1.1
Start Address: 100
End Address: 249
Lease Time: 720 (min)

DHCP Reservation

Add Static Binding Rule: Add

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



Uplink Interfaces

Interface	Work Mode	Protocol	Device IP	Operation
Wi-Fi HaLow	STA Mode	DHCP		Settings

Downlink Interfaces

Interface	DHCP Service	Operation
ETH0	Assigning	Settings
Wi-Fi	Assigning	Settings

DHCP Service

Device IPv4 Address: 172.18.1.1 Start Address: 100 End Address: 249

Lease Time: 720 (min)

DHCP Reservation

Add Static Binding Rule: Add

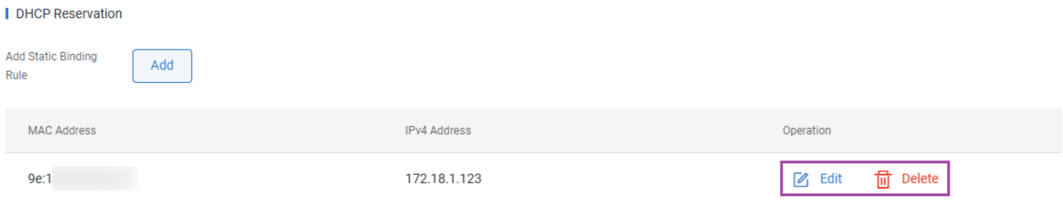
Add Static Binding Rule

MAC Address:

IPv4 Address:

Cancel Add

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

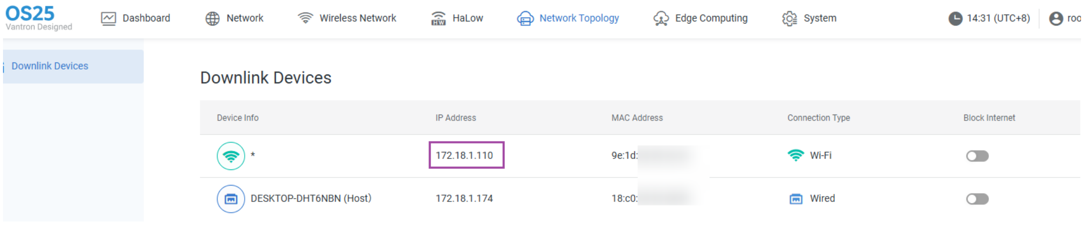


DHCP Reservation

Add Static Binding Rule: Add

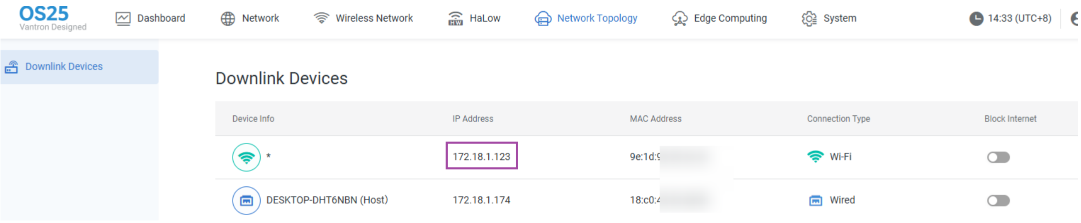
MAC Address	IPv4 Address	Operation
9e:1[redacted]	172.18.1.123	Edit Delete

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



Downlink Devices

Device Info	IP Address	MAC Address	Connection Type	Block Internet
*	172.18.1.110	9e:1d:[redacted]	Wi-Fi	
DESKTOP-DHT6NBN (Host)	172.18.1.174	18:c0:[redacted]	Wired	



Downlink Devices

Device Info	IP Address	MAC Address	Connection Type	Block Internet
*	172.18.1.123	9e:1d:[redacted]	Wi-Fi	
DESKTOP-DHT6NBN (Host)	172.18.1.174	18:c0:[redacted]	Wired	

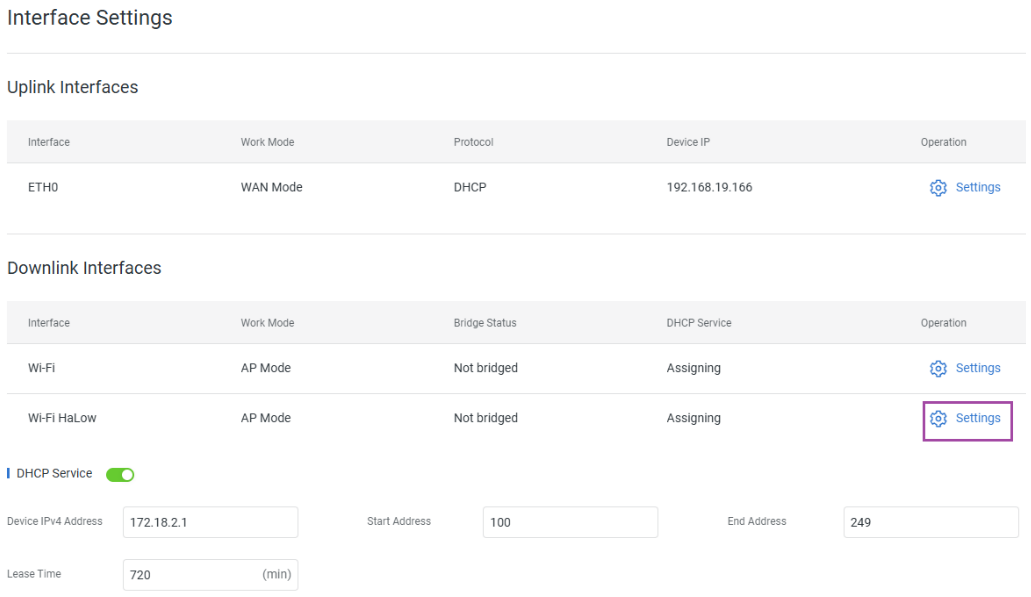
3.3.1.6 Interface Bridging

By enabling the bridge mode for a downlink interface (Ethernet LAN/Wi-Fi AP/HaLow AP), both the bridged interface and uplink interface will be added to the same Layer 2 bridge, sharing the same broadcast domain:

- Any device connected to the bridged interface is placed on the upstream network.
- HAP202 stops providing NAT or DHCP for that LAN/Wi-Fi/HaLow interface. Instead, the upstream (WAN-side) DHCP server handles the client addressing.

To enable bridge mode on a downlink interface (HaLow AP for instance):

1. Navigate to **Network > Interface > Interface Settings.**
2. Locate the target downlink interface, and click the **Settings** icon.



Interface Settings

Uplink Interfaces

Interface	Work Mode	Protocol	Device IP	Operation
ETH0	WAN Mode	DHCP	192.168.19.166	Settings

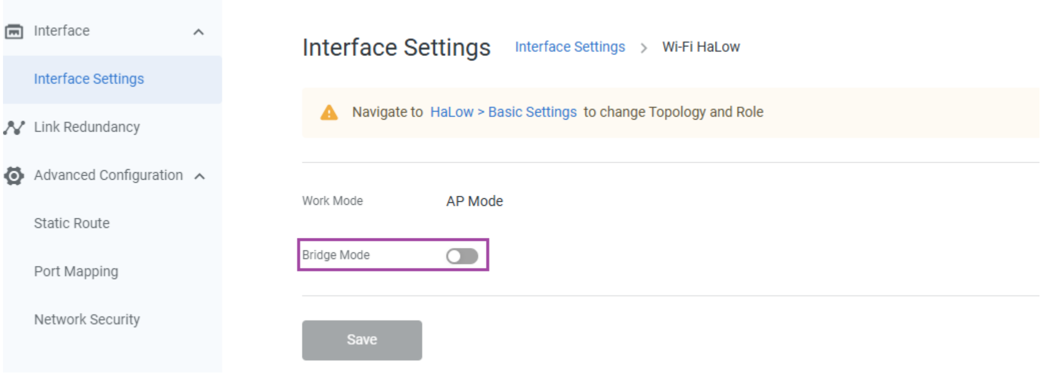
Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
Wi-Fi	AP Mode	Not bridged	Assigning	Settings
Wi-Fi HaLow	AP Mode	Not bridged	Assigning	Settings

DHCP Service

Device IPv4 Address: 172.18.2.1
Start Address: 100
End Address: 249
Lease Time: 720 (min)

3. Toggle on **Bridge Mode**.



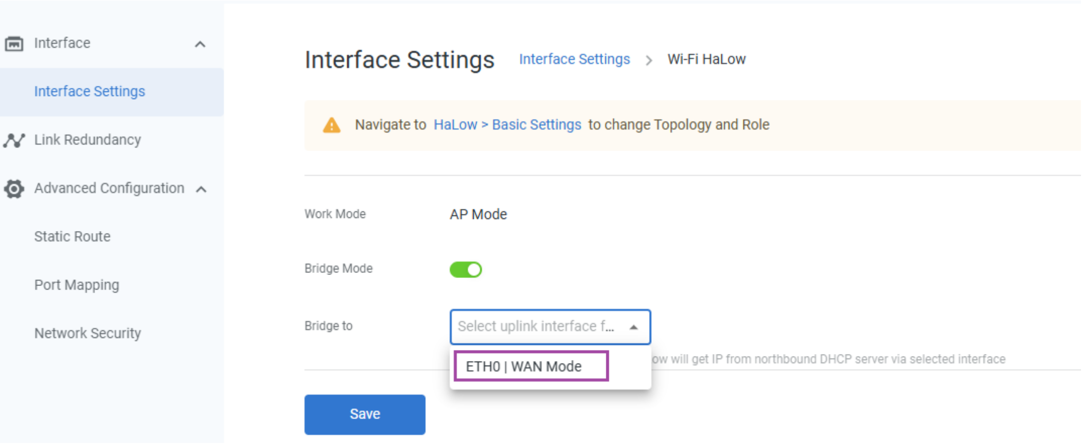
Interface Settings   Interface Settings > Wi-Fi HaLow

Navigate to HaLow > Basic Settings to change Topology and Role

Work Mode: AP Mode

Bridge Mode

4. Select the uplink interface (for instance, Ethernet WAN) to bridge to, and click **Save**.



Navigate to HaLow > Basic Settings to change Topology and Role

Work Mode AP Mode

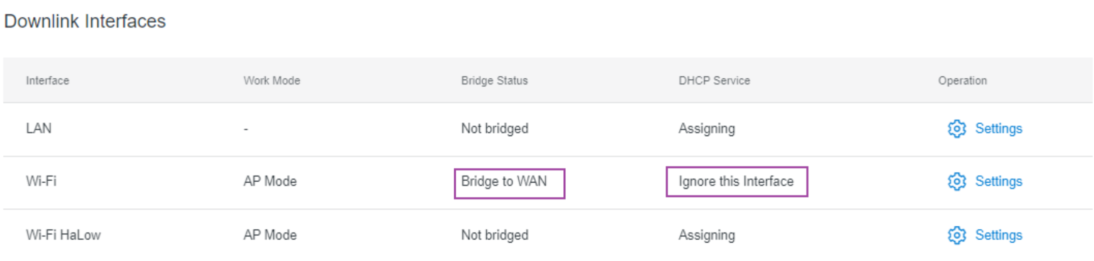
Bridge Mode

Bridge to Select uplink interface f...

ETH0 | WAN Mode

ow will get IP from northbound DHCP server via selected interface

5. When the **DHCP Service** column under **Downlink Interfaces** is displaying **Ignore this Interface**, the bridged uplink interface acts as the DHCP server for IP allocation.

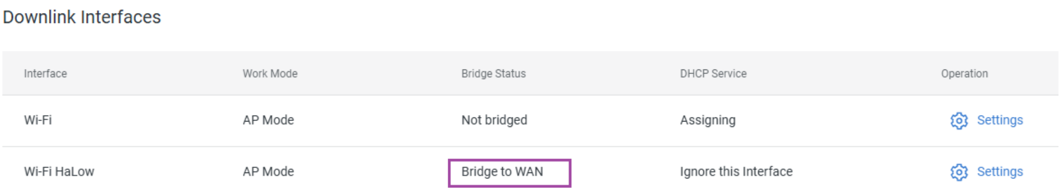


Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
LAN	-	Not bridged	Assigning	Settings
Wi-Fi	AP Mode	Bridge to WAN	Ignore this Interface	Settings
Wi-Fi HaLow	AP Mode	Not bridged	Assigning	Settings

6. Once bridged, DHCP service will **not** take effect on this interface. For a HaLow AP interface that is bridged, HaLow stations connected to this interface will obtain IP addresses directly from the upstream network's DHCP server.

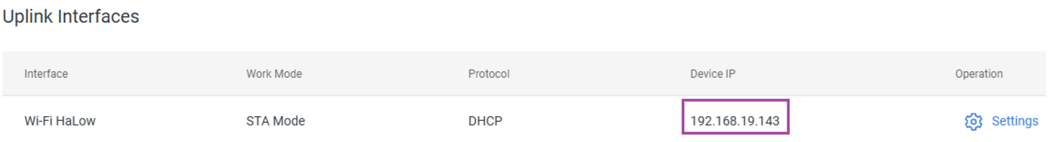
AP side:



Downlink Interfaces

Interface	Work Mode	Bridge Status	DHCP Service	Operation
Wi-Fi	AP Mode	Not bridged	Assigning	Settings
Wi-Fi HaLow	AP Mode	Bridge to WAN	Ignore this Interface	Settings

STA side:



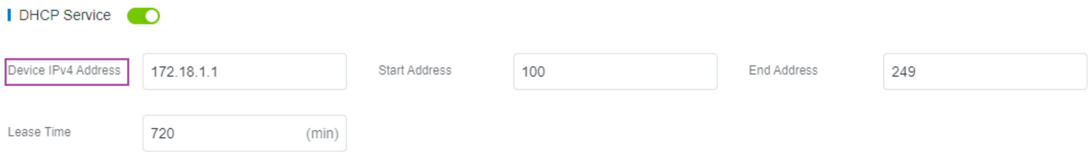
Uplink Interfaces

Interface	Work Mode	Protocol	Device IP	Operation
Wi-Fi HaLow	STA Mode	DHCP	192.168.19.143	Settings

3.3.1.7 Subnet Conflict

A subnet conflict prompt for local interfaces may appear when a Vantron router or HaLow AP is used as a DHCP server for the HAP202's uplink interface, as its factory LAN address (172.18.1.1) overlaps with the HAP202's default downlink subnet.

To avoid this, you can modify the **Device IPv4 Address** of the HAP202.



DHCP Service

Device IPv4 Address	172.18.1.1	Start Address	100	End Address	249
Lease Time	720 (min)				

3.3.2 Link Redundancy

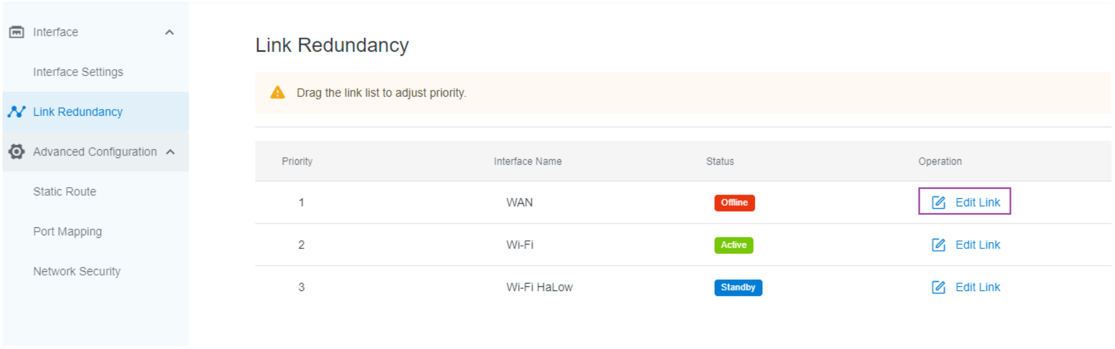
Link redundancy ensures network reliability by running multiple connections in parallel. If the primary link fails, traffic is instantly switched to a backup path, minimizing downtime and protecting critical environments from single points of failure.

Link redundancy takes effect when there are **at least two** upstream links.

3.3.2.1 Link Diagnosis

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

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

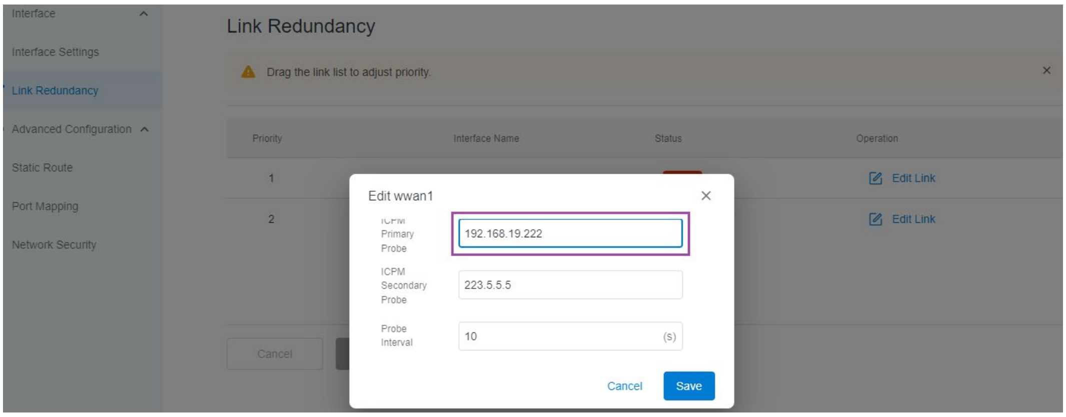


Link Redundancy

Drag the link list to adjust priority.

Priority	Interface Name	Status	Operation
1	WAN	Offline	Edit Link
2	Wi-Fi	Active	Edit Link
3	Wi-Fi HaLow	Standby	Edit Link

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

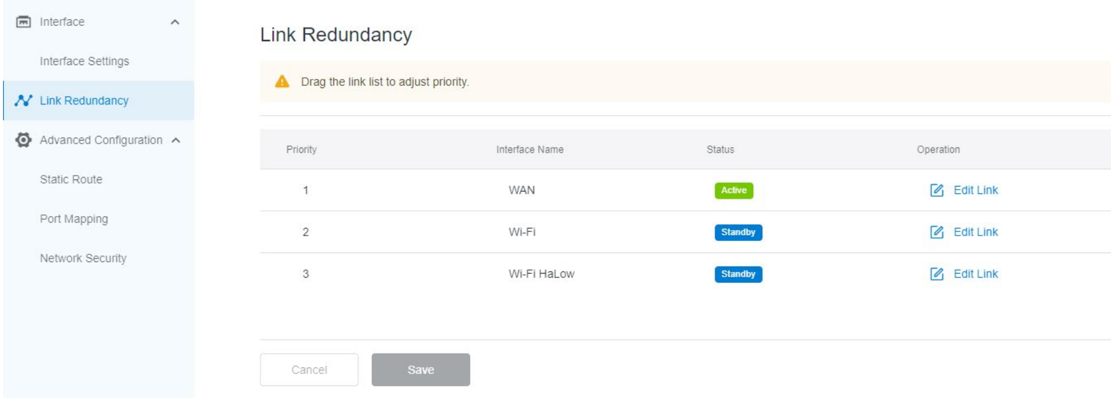


Edit wwan1

ICPM Primary Probe	192.168.19.222
ICPM Secondary Probe	223.5.5.5
Probe Interval	10 (s)

Cancel Save

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



Link Redundancy

Drag the link list to adjust priority.

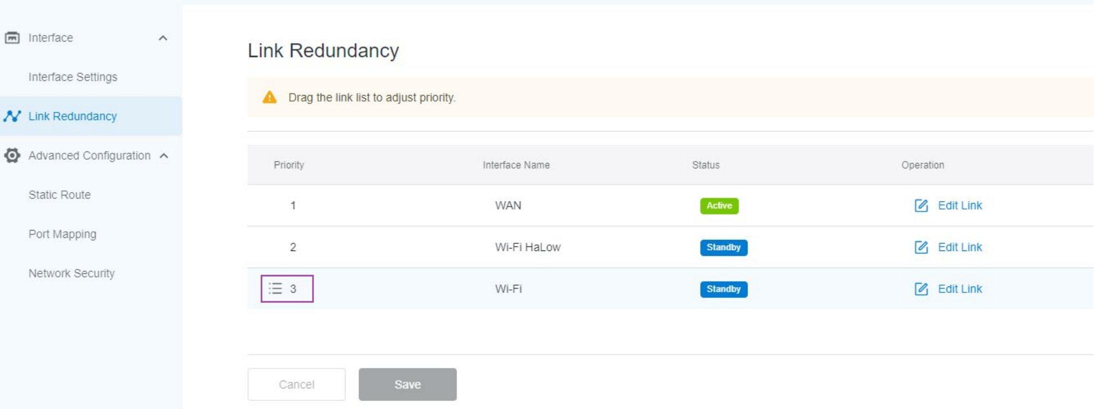
Priority	Interface Name	Status	Operation
1	WAN	Active	Edit Link
2	Wi-Fi	Standby	Edit Link
3	Wi-Fi HaLow	Standby	Edit Link

3.3.2.2 Link Priority

The default link detection and data forwarding are prioritized based on the following rule: Ethernet (WAN) > Wi-Fi HaLow (STA) > 2.4GHz/5GHz Wi-Fi (Client).

To manually set the network priority:

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

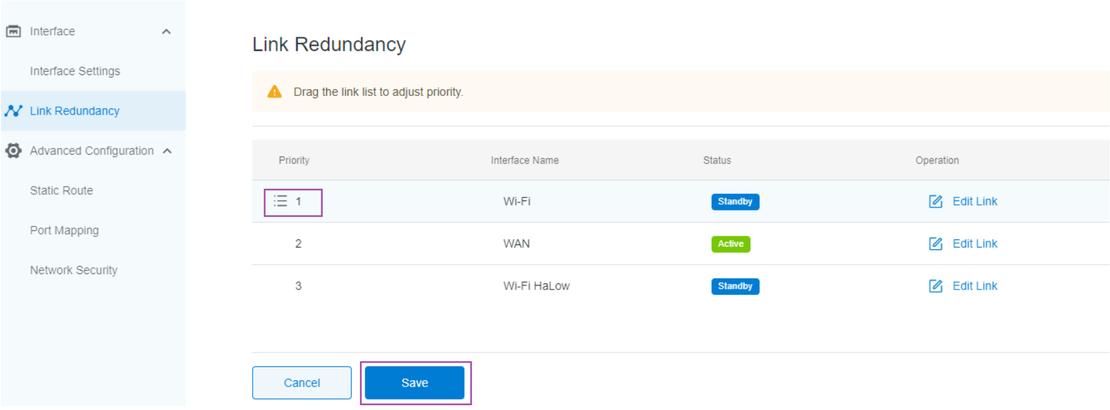


Link Redundancy

Drag the link list to adjust priority.

Priority	Interface Name	Status	Operation
1	WAN	Active	Edit Link
2	Wi-Fi HaLow	Standby	Edit Link
3	Wi-Fi	Standby	Edit Link

2. Drag the link up or down to the desired position, then click **Save**.



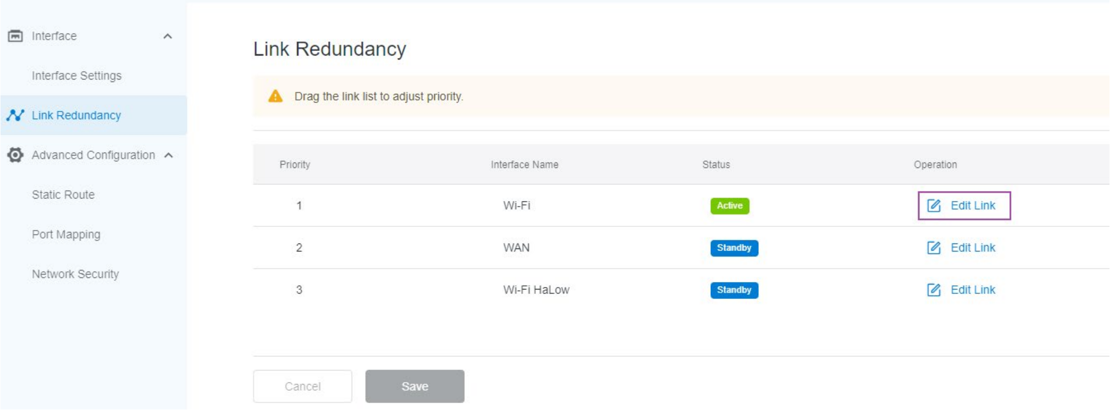
Link Redundancy

Drag the link list to adjust priority.

Priority	Interface Name	Status	Operation
1	Wi-Fi	Standby	Edit Link
2	WAN	Active	Edit Link
3	Wi-Fi HaLow	Standby	Edit Link

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

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



Link Redundancy

Drag the link list to adjust priority.

Priority	Interface Name	Status	Operation
1	Wi-Fi	Active	Edit Link
2	WAN	Standby	Edit Link
3	Wi-Fi HaLow	Standby	Edit Link

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

3.3.3 Static Route

Static routing is a manual network configuration method where administrators explicitly define paths for traffic through specific network interfaces. This provides precise control over routing behavior, particularly useful for: multi-WAN load balancing, traffic segregation, or backup link configuration.

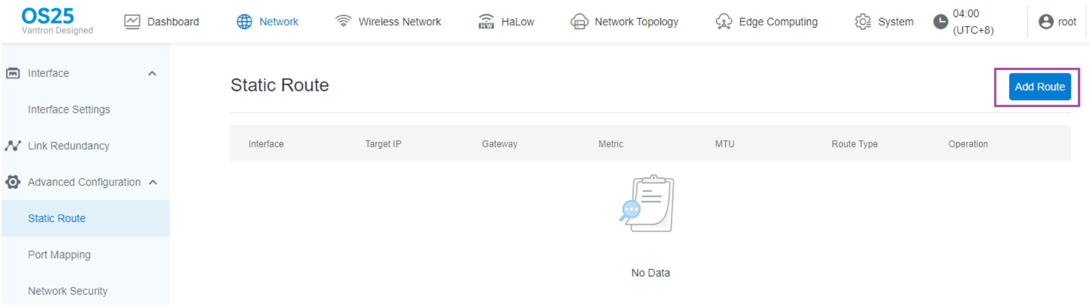
Example:

Goal: Allow HaLow stations connected to the HaLow AP interface that is bridged to Ethernet WAN to access the internal network (192.168.0.0 - 192.168.255.255).

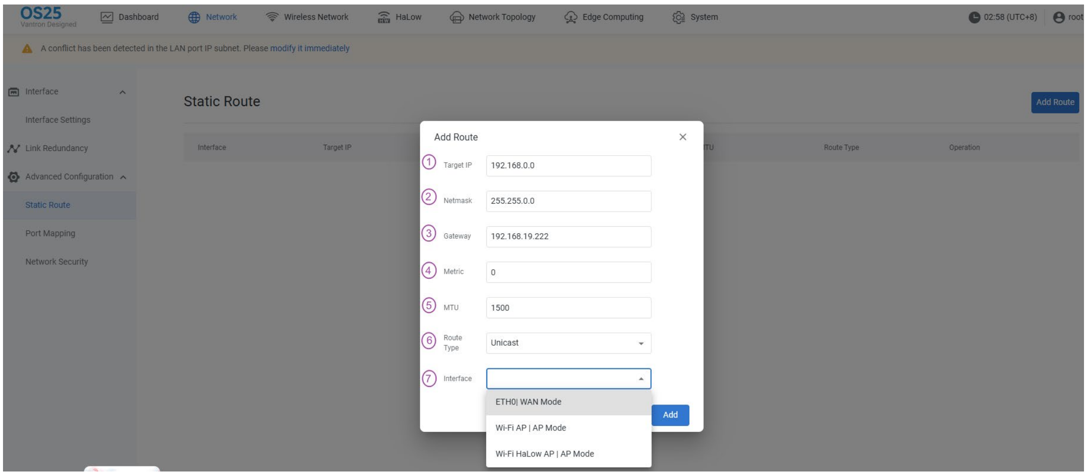
Topology: HaLow Stations -> HaLow AP (bridged to WAN) -> upstream router -> internal network server (192.168.0.0/16)

Steps:

1. Refer to section 3.3.1.6 for instructions on how to bridge an interface.
2. Navigate to **Network > Advanced Configuration > Static Route**.
3. Click **Add Route** to create a routing rule.



4. Configure the rules for the route:



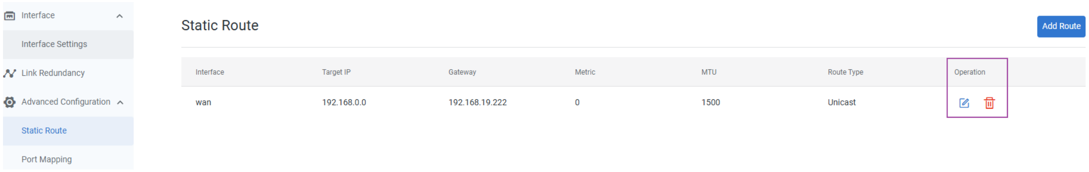
A conflict has been detected in the LAN port IP subnet. Please modify it immediately

1 Target IP: 192.168.0.0
2 Netmask: 255.255.0.0
3 Gateway: 192.168.19.222
4 Metric: 0
5 MTU: 1500
6 Route Type: Unicast
7 Interface: ETH0| WAN Mode / Wi-Fi AP | AP Mode / Wi-Fi HaLow AP | AP Mode

Description of the numbered areas

1) Input the destination IP address (192.168.0.0).
2) Input the subnet mask (255.255.0.0).
3) Input the address of the upstream router (e.g., 192.168.19.222).
4) Gateway metric (**The smaller the number, the higher the priority**).
5) Set the MTU.
6) Select a route type (refer to the details in the table below).
7) Select an outbound interface for the route (the interface that leads to the gateway, ETH0 WAN in this case).

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



Static Route

Interface	Target IP	Gateway	Metric	MTU	Route Type	Operation
wan	192.168.0.0	192.168.19.222	0	1500	Unicast	✎ 🗑

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:

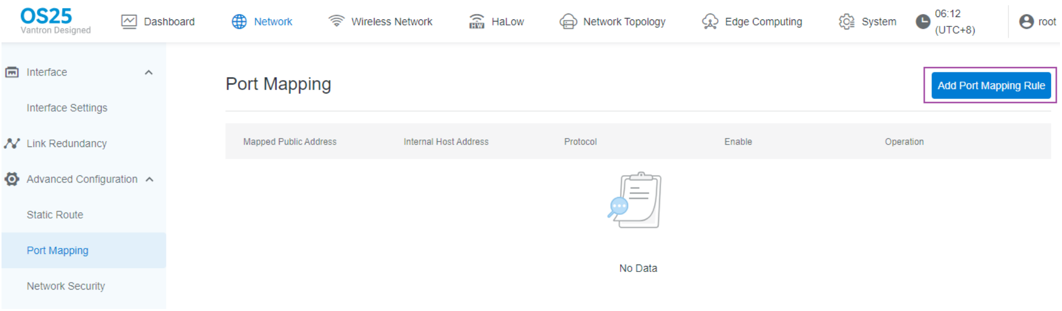
Scenario:

- HAP202 has both an internal zone (e.g., HaLow AP) and an external WAN zone (e.g., Ethernet WAN) configured, with NAT enabled from internal to external.
- Port mapping (Destination NAT) operates based on this NAT boundary.

Goal:

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

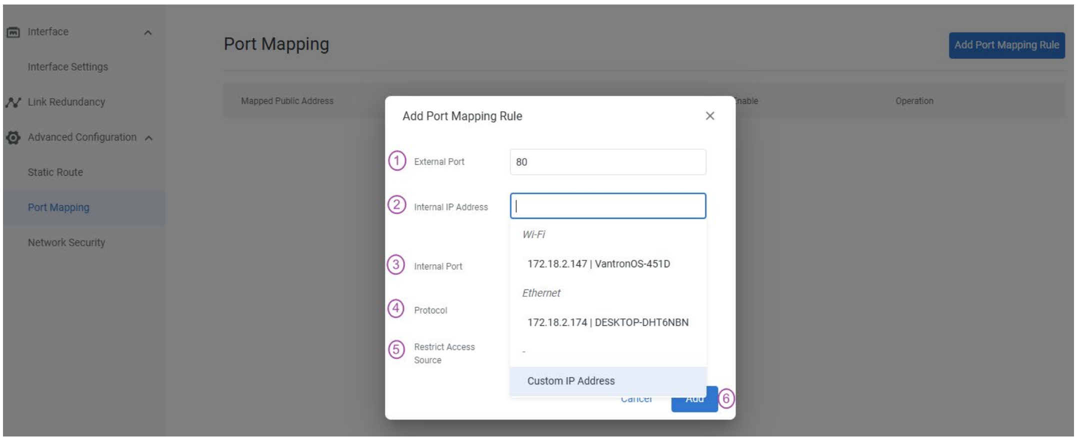
1. Click **Add Port Mapping Rule** in the upper right side.



Mapped Public Address	Internal Host Address	Protocol	Enable	Operation

No Data

2. Fill in the rule information.



1 External Port: 80

2 Internal IP Address:

Wi-Fi
172.18.2.147 | VantronOS-451D
Ethernet
172.18.2.174 | DESKTOP-DHT6NBN
-
Custom IP Address

3 Internal Port

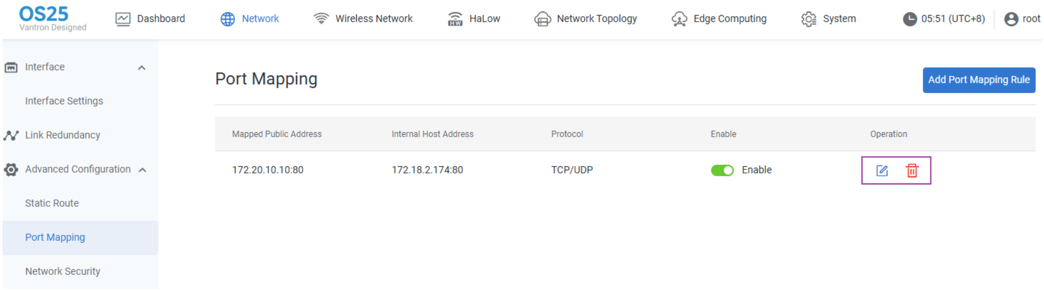
4 Protocol

5 Restrict Access Source

Description of the numbered areas

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.



Port Mapping

Mapped Public Address	Internal Host Address	Protocol	Enable	Operation
172.20.10.10:80	172.18.2.174:80	TCP/UDP	Enable	

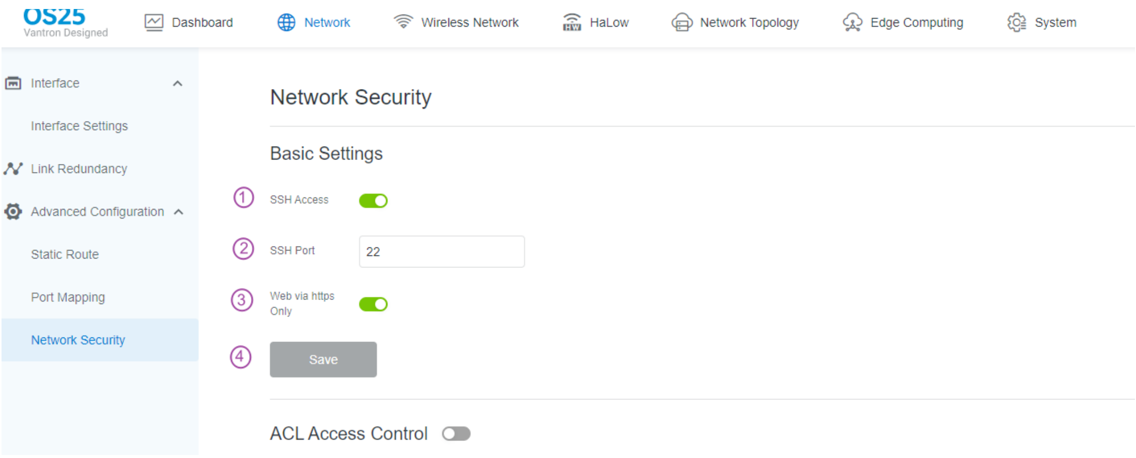
Note: *The mapped public address is determined by your WAN connection and may change.*

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



Network Security

Basic Settings

SSH Access ●

SSH Port 22

Web via https Only ●

ACL Access Control ○

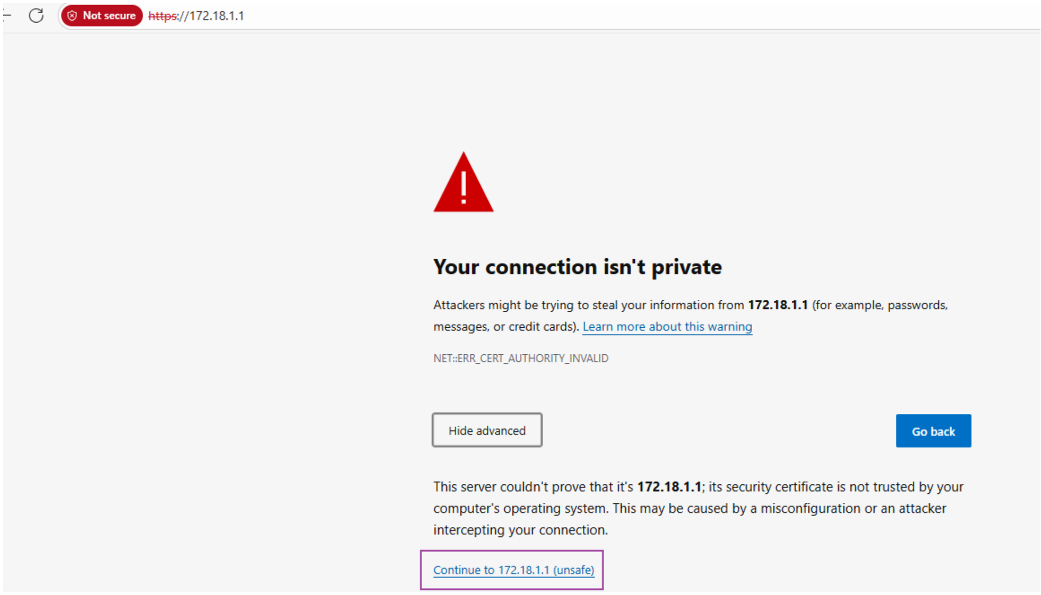
Description of the numbered areas

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.



Your connection isn't private

Attackers might be trying to steal your information from **172.18.1.1** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **172.18.1.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Continue to 172.18.1.1 (unsafe)

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

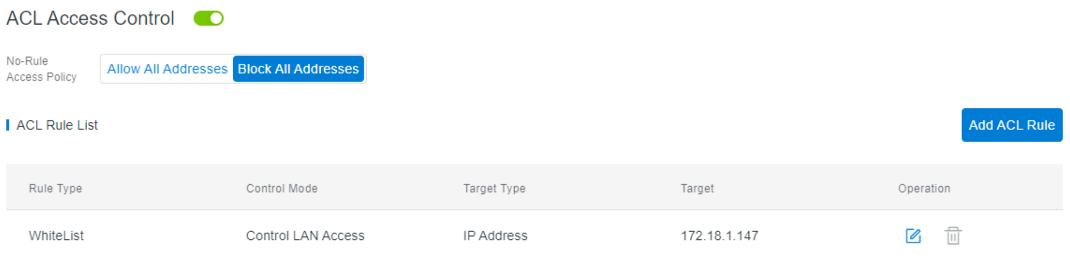
3.3.5.2 ACL Access Control

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

- **No-Rule Access Policy**

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

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



ACL Access Control

No-Rule Access Policy: Allow All Addresses | **Block All Addresses**

ACL Rule List

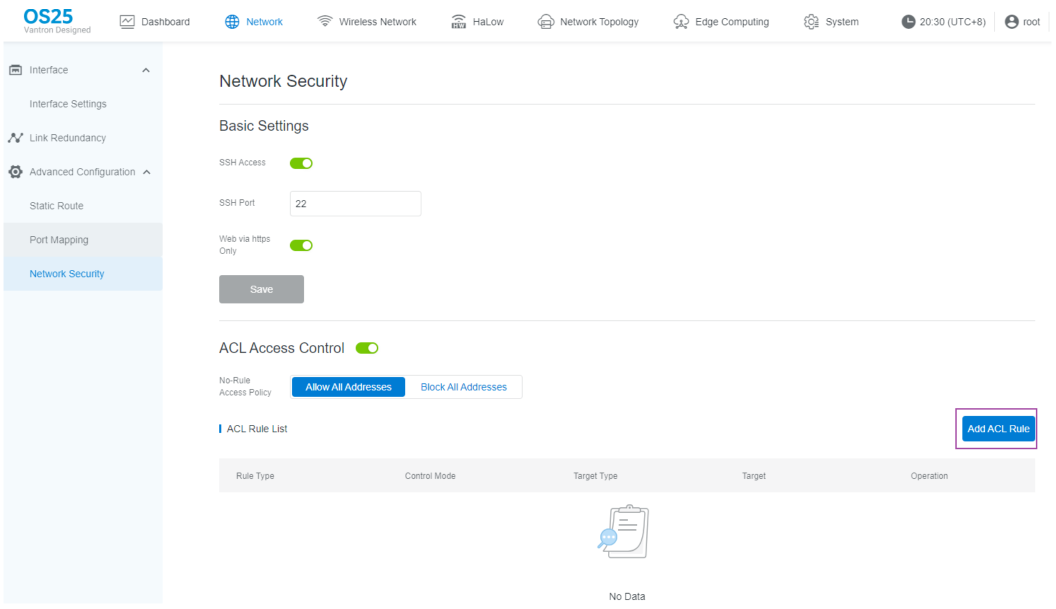
Add ACL Rule

Rule Type	Control Mode	Target Type	Target	Operation
WhiteList	Control LAN Access	IP Address	172.18.1.147	

- **ACL Rule List**

To add an ACL rule:

1. Navigate to **Network > Network Security**, and click **Add ACL Rule**.



Network Security

Basic Settings

SSH Access

SSH Port: 22

Web via https Only

Save

ACL Access Control

No-Rule Access Policy: **Allow All Addresses** | Block All Addresses

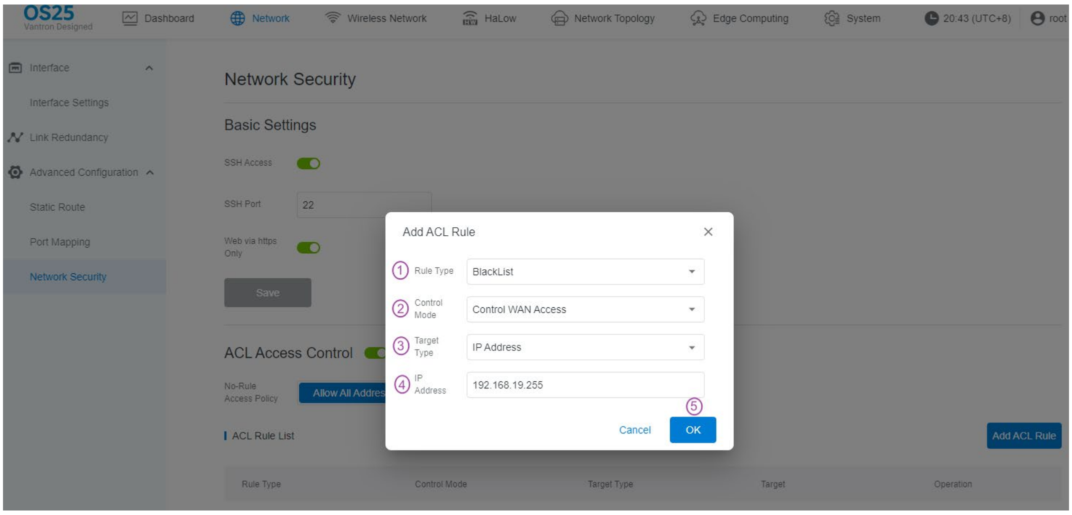
ACL Rule List

Add ACL Rule

Rule Type	Control Mode	Target Type	Target	Operation

No Data

2. Configure the rule in the pop-up.



Network Security

Basic Settings

SSH Access

SSH Port 22

Web via https Only

ACL Access Control

No-Rule Access Policy

ACL Rule List

Add ACL Rule

① Rule Type: BlackList

② Control Mode: Control WAN Access

③ Target Type: IP Address

④ IP Address: 192.168.19.255

⑤ OK

Description of the numbered areas

1) Select a rule type:

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

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

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

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

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

5) Click **OK** to complete.

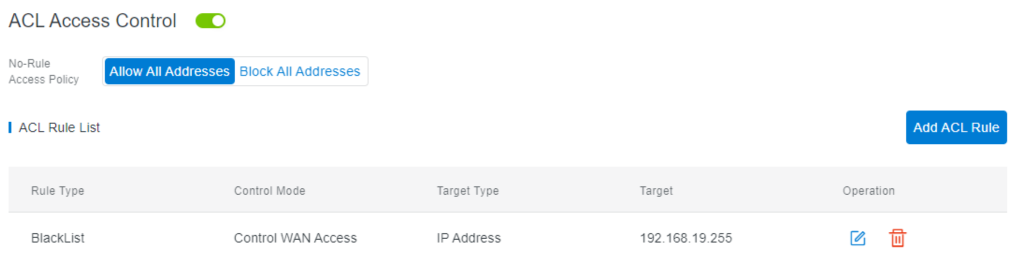
Description for the rule settings:

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

Rule Type	Control Mode	Target Type	Result
Blacklist	WAN	IP address (Source)	The designated WAN IP is blocked from accessing HAP202 or its LAN devices.
		Destination IP/ URL/URL keyword	HAP202 or its LAN devices has no access to the designated WAN IP/URL/URL keyword.
	LAN	IP/MAC/OUI	The designated LAN devices are blocked from accessing the WAN domain.

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

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



ACL Access Control

No-Rule Access Policy: Allow All Addresses | Block All Addresses

ACL Rule List

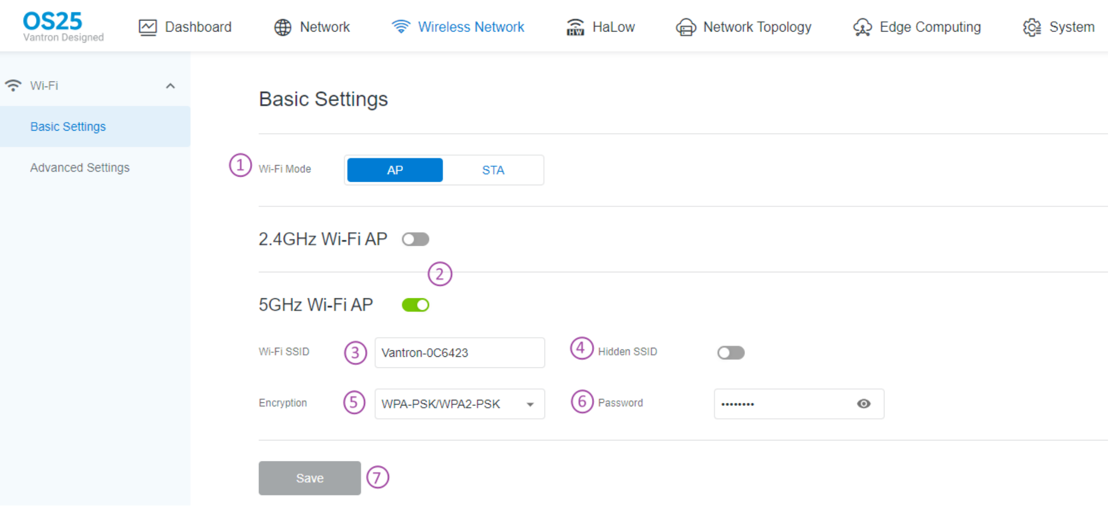
Rule Type	Control Mode	Target Type	Target	Operation
BlackList	Control WAN Access	IP Address	192.168.19.255	

3.4 Wireless Network

2.4GHz/5GHz Wi-Fi related settings are configured on the **Wireless Network** page.

During the initial login wizard, the device's 2.4GHz Wi-Fi/5GHz is pre-configured as an access point (AP). Users can modify the configurations as needed.

3.4.1 AP-Mode Basic Settings



Basic Settings

Wi-Fi Mode: [✓ AP] STA

2.4GHz Wi-Fi AP: ○

5GHz Wi-Fi AP: ●

Wi-Fi SSID: Vantron-0C6423

Hidden SSID: ○

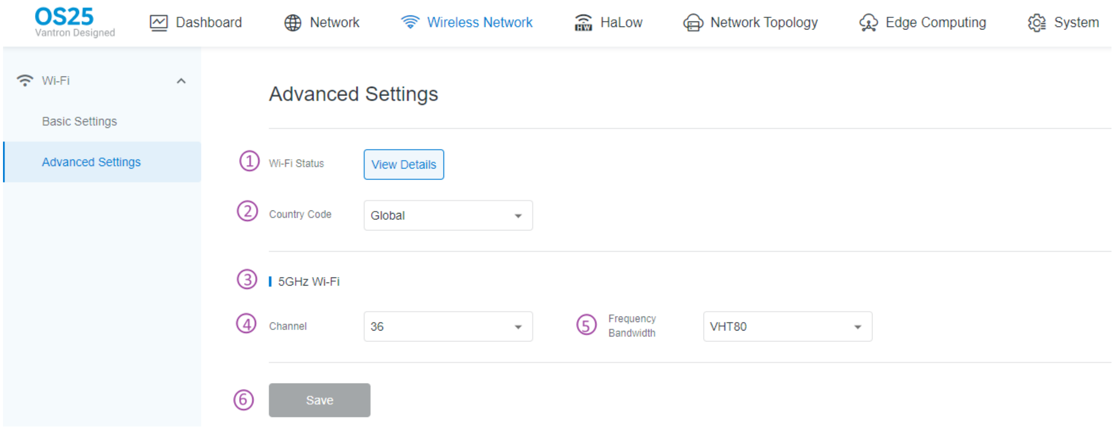
Encryption: WPA-PSK/WPA2-PSK

Password: ••••••••

Description of the numbered areas

1. Current Wi-Fi mode is displayed in dark blue.
2. The HAP202 supports dual-band Wi-Fi and the 5GHz Wi-Fi is enabled by default. The editable fields for both bands are the same, and you can modify the configurations after enabling the target band.
3. Wi-Fi SSID—The Wi-Fi AP's name.
4. Hide SSID: Once hidden, clients cannot scan the device's SSID and must manually enter the exact SSID and password to connect.
5. Encryption—The basic protocols for establishing secure communication. (None, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK)
6. Password—Credential for connecting the device's Wi-Fi.
7. If you have modified the parameters, click **Save** to apply.

3.4.2 AP-Mode Advanced Settings



Advanced Settings

① Wi-Fi Status: View Details

② Country Code: Global

③ 5GHz Wi-Fi

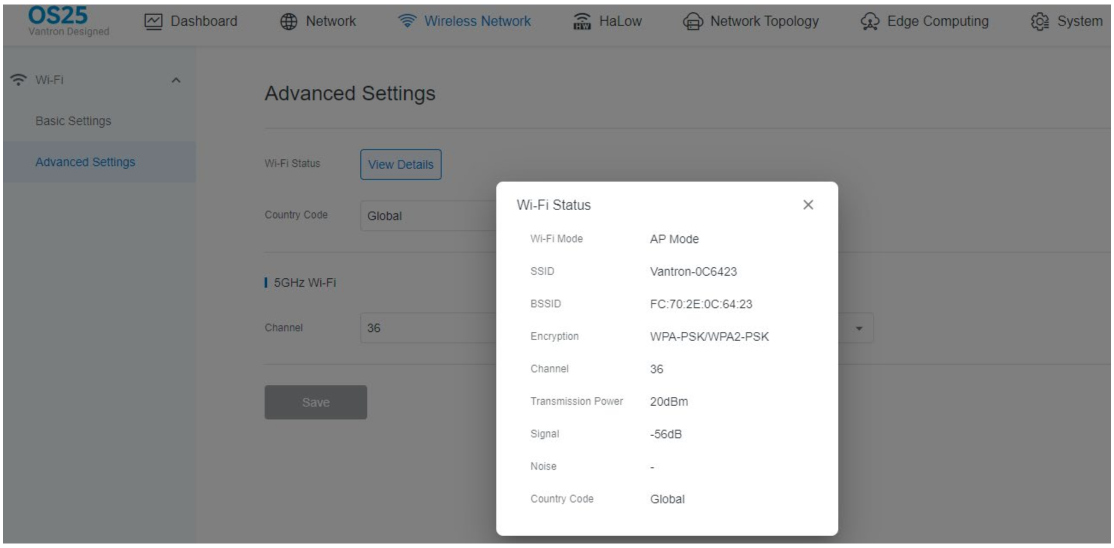
④ Channel: 36

⑤ Frequency Bandwidth: VHT80

⑥ Save

Description of the numbered areas

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

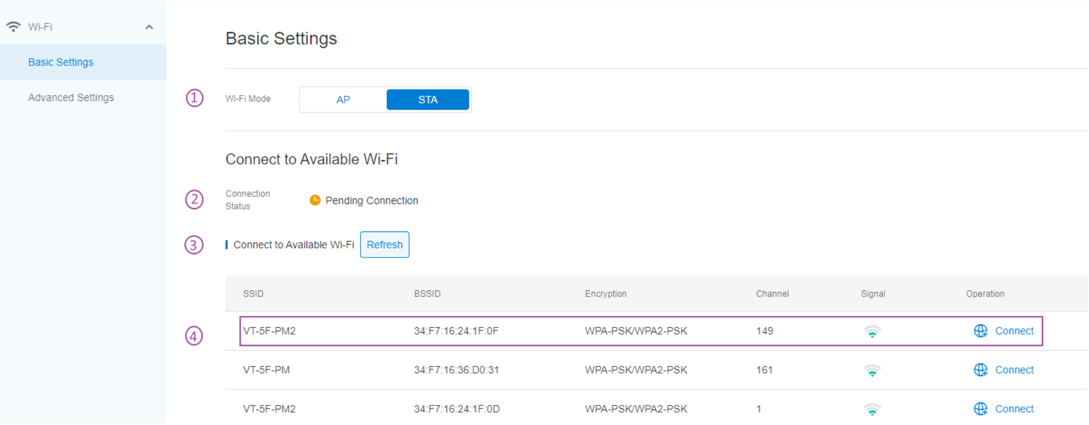


Wi-Fi Status

Wi-Fi Mode	AP Mode
SSID	Vantron-0C6423
BSSID	FC:70:2E:0C:64:23
Encryption	WPA-PSK/WPA2-PSK
Channel	36
Transmission Power	20dBm
Signal	-56dB
Noise	-
Country Code	Global

2. Country code (‘global’ by default)
3. Wi-Fi band (depends on your selection in **Basic Settings**)
4. Channel options
5. Frequency bandwidth (‘VHT80’ for 5GHz, ‘HT20’ for 0.4GHz by default)
6. If you have modified the parameters, click **Save** to apply.

3.4.3 Client-Mode Basic Settings



Basic Settings

Wi-Fi Mode: AP | STA

Connect to Available Wi-Fi

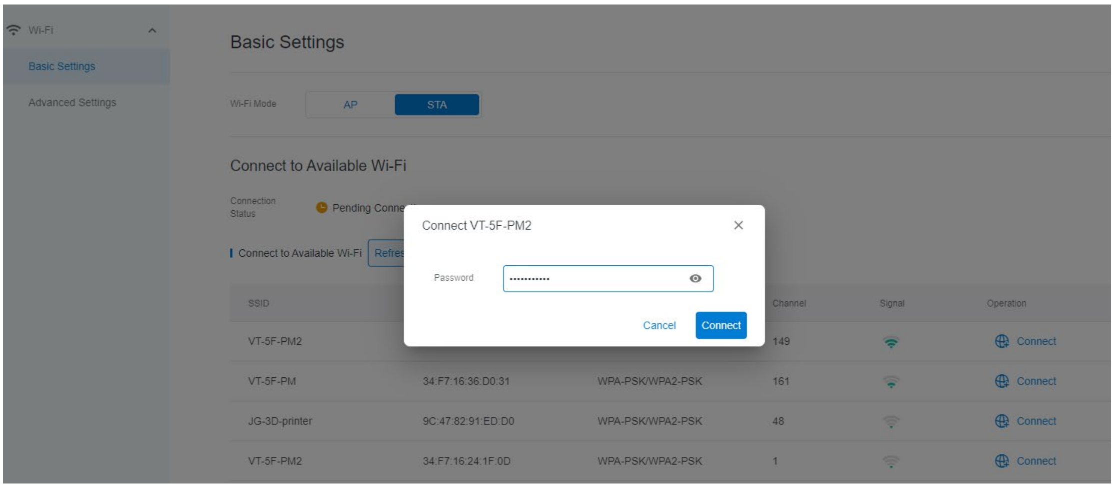
Connection Status: Pending Connection

Connect to Available Wi-Fi Refresh

SSID	BSSID	Encryption	Channel	Signal	Operation
VT-5F-PM2	34:F7:16:24:1F:0F	WPA-PSK/WPA2-PSK	149		Connect
VT-5F-PM	34:F7:16:36:D0:31	WPA-PSK/WPA2-PSK	161		Connect
VT-5F-PM2	34:F7:16:24:1F:0D	WPA-PSK/WPA2-PSK	1		Connect

Description of the numbered areas

1. Current Wi-Fi mode is displayed in dark blue.
2. Current Wi-Fi connection status.
3. If the target SSID is not included in the list, click the **Refresh** 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.



Basic Settings

Wi-Fi Mode: AP | STA

Connect to Available Wi-Fi

Connection Status: Pending Conne

Connect to Available Wi-Fi Refres

Connect VT-5F-PM2 ×

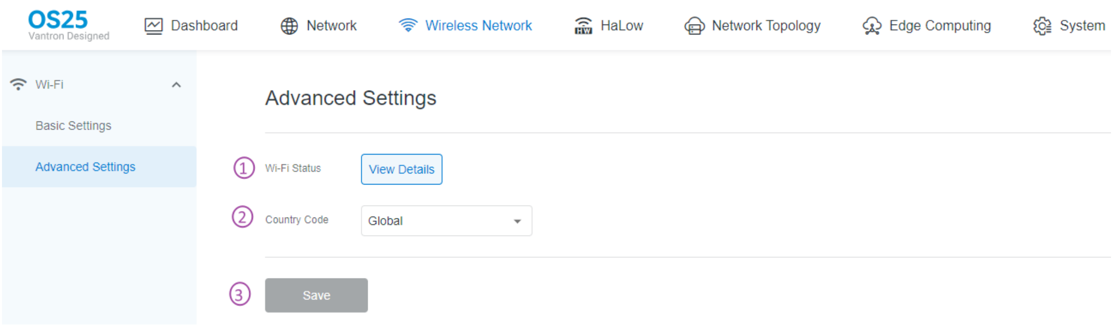
Password: ···········

Cancel Connect

SSID			Channel	Signal	Operation
VT-5F-PM2			149		Connect
VT-5F-PM	34:F7:16:36:D0:31	WPA-PSK/WPA2-PSK	161		Connect
JG-3D-printer	9C:47:82:91:ED:D0	WPA-PSK/WPA2-PSK	48		Connect
VT-5F-PM2	34:F7:16:24:1F:0D	WPA-PSK/WPA2-PSK	1		Connect

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

3.4.4 Client-Mode Advanced Settings

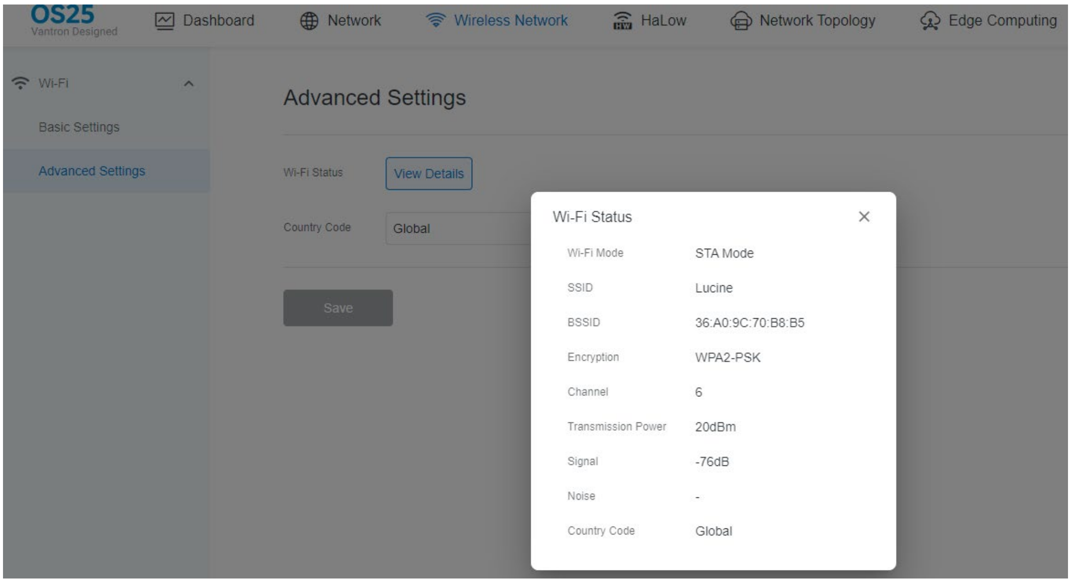


Wi-Fi Status: View Details

Country Code: Global

Description of the numbered areas

1. 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.



Wi-Fi Status

Wi-Fi Mode	STA Mode
SSID	Lucine
BSSID	36:A0:9C:70:B8:B5
Encryption	WPA2-PSK
Channel	6
Transmission Power	20dBm
Signal	-76dB
Noise	-
Country Code	Global

2. Country code (‘global’ by default).

3. If you have modified the parameters, click **Save** to apply.

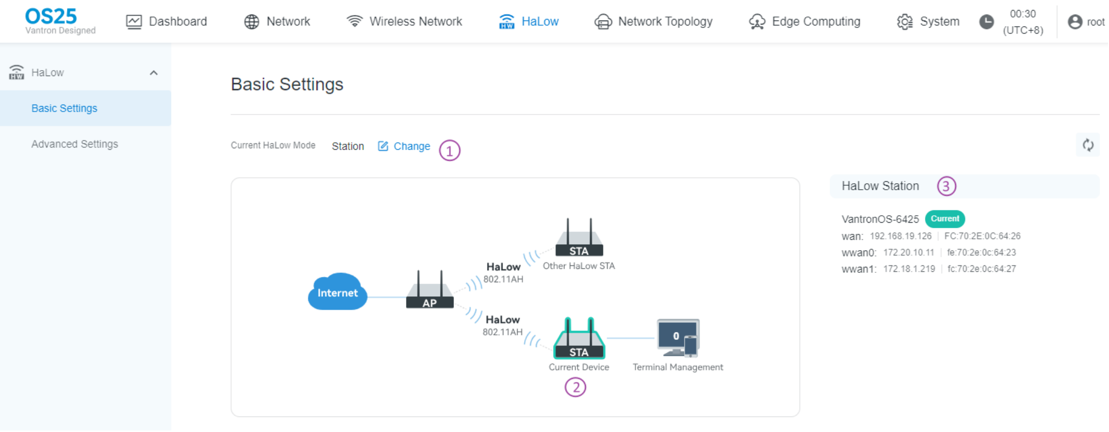
3.5 HaLow

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.

3.5.1 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.



Basic Settings

Current HaLow Mode Station

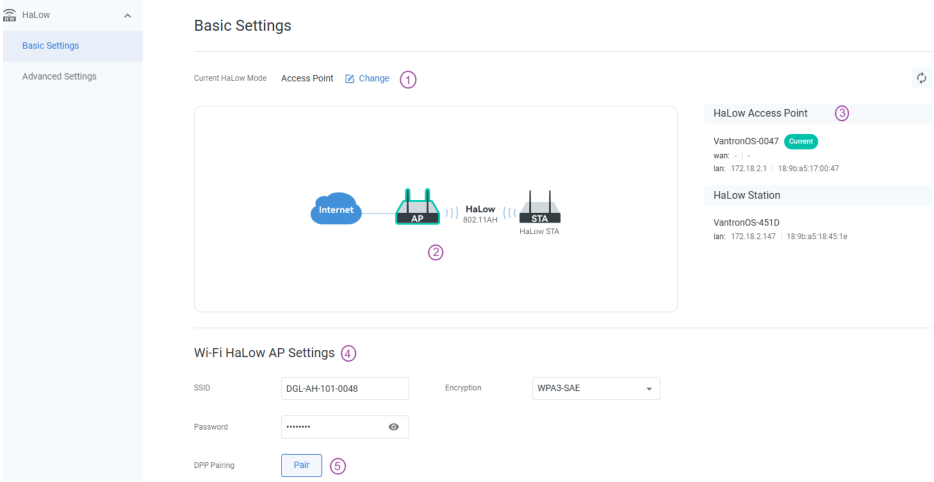
HaLow Station

VantronOS-6425
wan: 192.168.19.126 | FC:70:2E:0C:64:26
wwan0: 172.20.10.11 | fe:70:2e:0c:64:23
wwan1: 172.18.1.219 | fc:70:2e:0c:64:27

Description of the numbered areas

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.
3. Device Information: Shows brief connection information for the current device in the topology. Clicking the sync button refreshes the device information.
    - wan: WAN domain IP
    - lan: LAN domain IP
    - wwan0: Wi-Fi STA IP
    - wwan1: HaLow STA IP

3.5.1.1 AP-Mode Settings



Basic Settings

Current HaLow Mode Access Point

HaLow Access Point

VantronOS-0047 Current
wan: - | -
lan: 172.18.2.1 | 18:9b:a5:17:00:47

HaLow Station

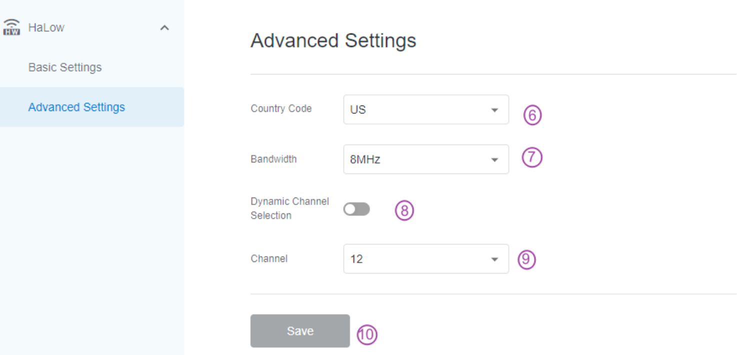
VantronOS-451D
lan: 172.18.2.147 | 18:9b:a5:18:45:1e

Wi-Fi HaLow AP Settings

SSID: DGL-AH-101-0048
Encryption: WPA3-SAE
Password: ••••••••
DPP Pairing: Pair

Description of the numbered areas

1. Click to change HaLow operation mode (Access Point/Station/Mesh Point).
2. Network topology for the current mode. The local device is highlighted with a **cyan** outline.
3. Brief device connection information: **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. DPP 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.

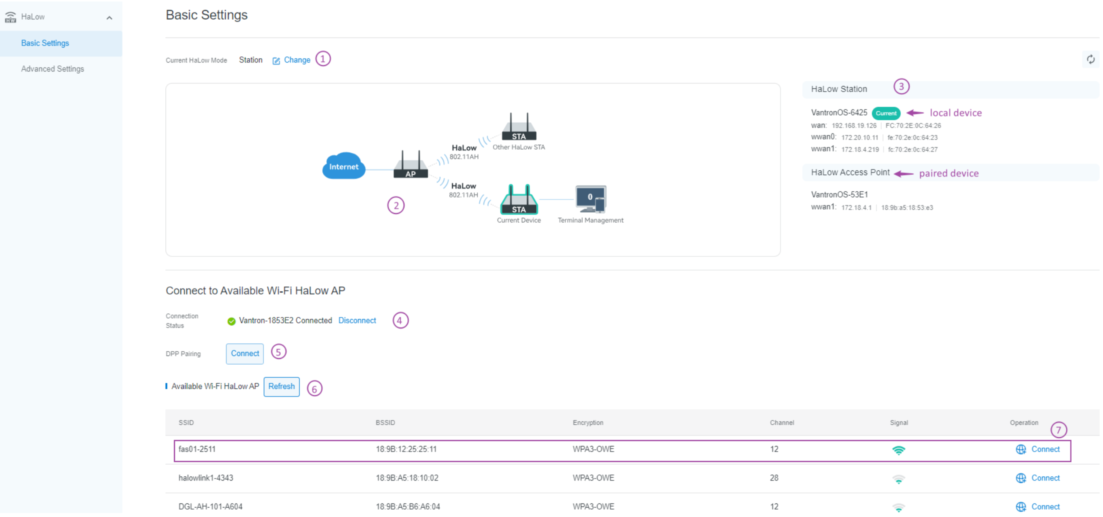


Advanced Settings

Country Code: US
Bandwidth: 8MHz
Dynamic Channel Selection: ○
Channel: 12

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

3.5.1.2 STA-Mode Settings



Basic Settings

Current HaLow Mode Station

HaLow Station

VantronOS-6425 Current
wan: 192.168.19.126 | FC:70:2E:0C:64:26
wwan0: 172.20.10.11 | fe:70:2e:0c:64:23
wwan1: 172.18.4.219 | fc:70:2e:0c:64:27

HaLow Access Point

VantronOS-53E1
wwan1: 172.18.4.1 | 18:9b:a5:18:53:e3

Connect to Available Wi-Fi HaLow AP

Connection Status: Vantron-1853E2 Connected

DPP Pairing

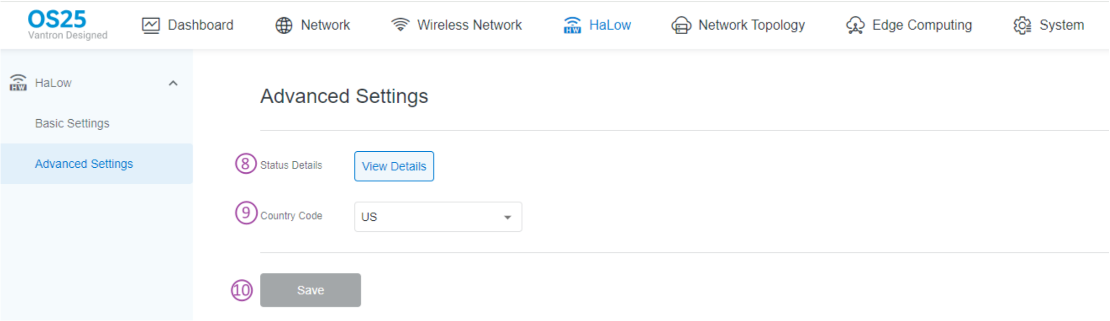
Available Wi-Fi HaLow AP

SSID	BSSID	Encryption	Channel	Signal	Operation
fas01-2511	18:9B:12:25:25:11	WPA3-OWE	12		Connect
halowlink1-4343	18:9B:A5:18:10:02	WPA3-OWE	28		Connect
DGL-AH-101-A604	18:9B:A5:B6:A6:04	WPA3-OWE	12		Connect

Description of the numbered areas

1. Click to change HaLow operation mode (Access Point/Station/Mesh Point).
2. Network topology for the current mode. The local device is highlighted with a **cyan** outline.
3. Brief device connection information: 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: 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.

*When the HAP202 connects to a HaLow AP, the AP information labeled **3** in the screenshot displays the device name, while the AP information labeled **4** in the screenshot shows the SSID.*



Advanced Settings

8 Status Details: View Details

9 Country Code: US

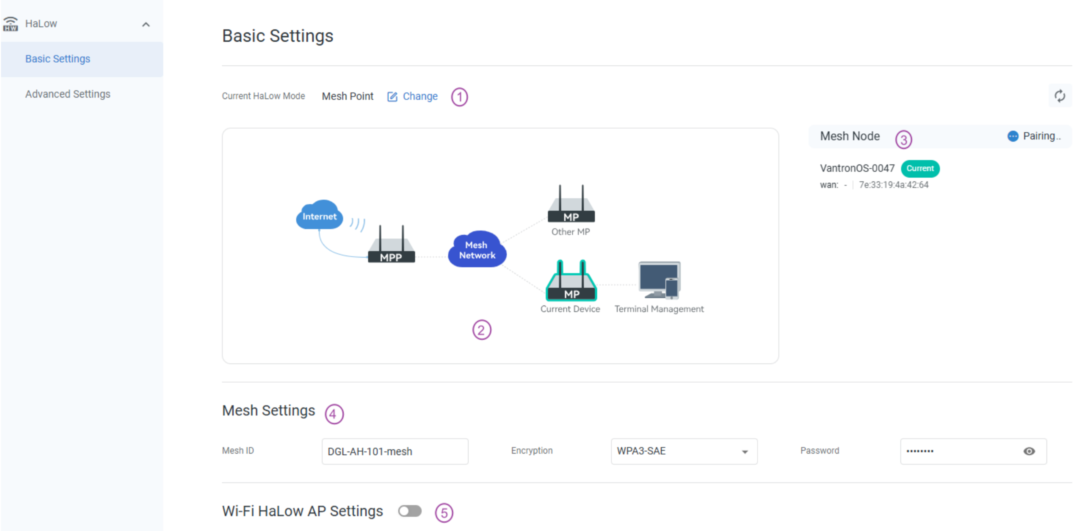
10 Save

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**.

3.5.1.3 Mesh-Point Settings



Basic Settings

Current HaLow Mode: Mesh Point — Change (1)

Mesh Node (3) — Pairing..

VantronOS-0047 Current
wan: - | 7e:33:19:4a:42:64

Mesh Settings (4)

Mesh ID: DGL-AH-101-mesh
Encryption: WPA3-SAE
Password: ••••••••

Wi-Fi HaLow AP Settings (5)

Description of the numbered areas

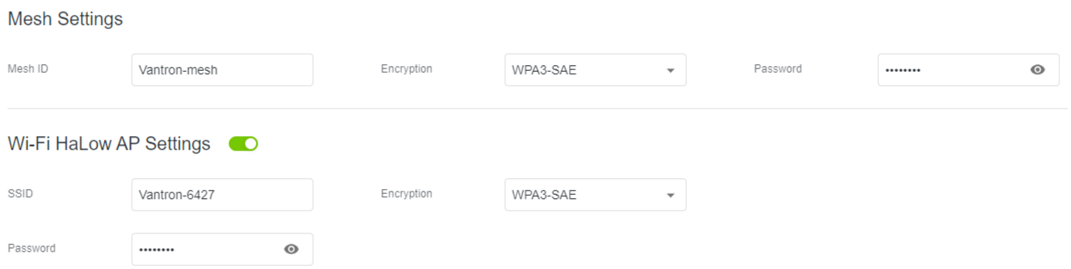
1. Click to change HaLow operation mode (Access Point/Station/Mesh Point).

2. Network topology for the current mode. The local device is highlighted with a **cyan** outline.

3. Brief device connection information: Clicking the sync icon refreshes the information. In the **Mesh Point** mode, the device continuously scans for and joins peers with the **same** Mesh settings.

4. Mesh Settings: Devices with the same Mesh parameters automatically establish a Mesh network. As all HAP202 units share the same default settings, you can modify these parameters to create separate, isolated mesh networks. Editable fields include: Mesh ID, Encryption, and Password.

5. HaLow AP Settings: Once enabled, the device broadcasts standard HaLow network and allows HaLow STAs to pair.



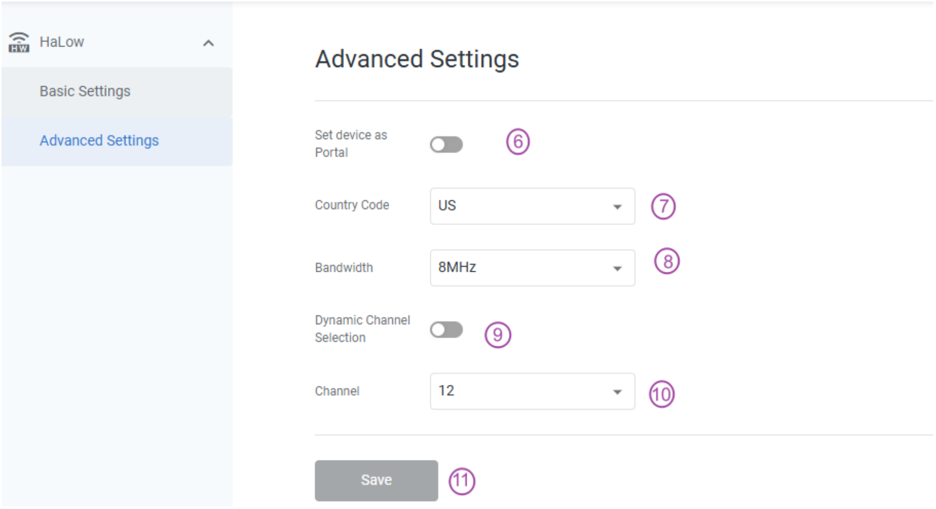
Mesh Settings

Mesh ID: Vantron-mesh
Encryption: WPA3-SAE
Password: ••••••••

Wi-Fi HaLow AP Settings

SSID: Vantron-6427
Encryption: WPA3-SAE
Password: ••••••••

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



Advanced Settings

Set device as Portal ⑥
Country Code: US ⑦
Bandwidth: 8MHz ⑧
Dynamic Channel Selection ⑨
Channel: 12 ⑩

6. When a Mesh Point is set as a **Portal**, its role in the topology changes to **MPP**, providing DHCP service to the entire Mesh network.

   In the absence of an MPP, a designated Mesh Point must be connected to an upstream router to relay DHCP service for the Mesh network. Refer to Table 3-1 for details.

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**.

Table 3-1 Role difference between a Mesh Point (MP) and Mesh Portal (MPP):

Role in a Mesh Network	DHCP Service Provider	External Network Access
Mesh Portal (MPP)	MPP	MPP NATs mesh traffic to its upstream IP
Mesh Point (MP)	Upstream router (DHCP relay via the router-connected MP)	The upstream router provides internet access

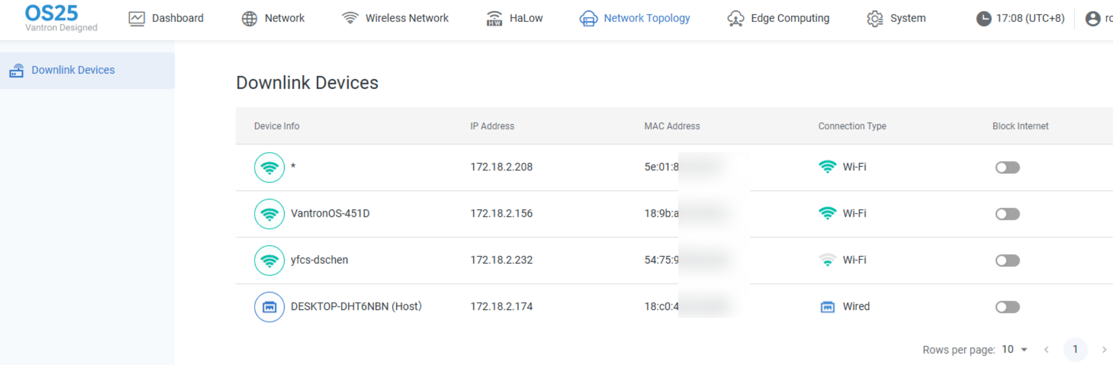
3.6 Network Topology

Network topology displays the information of connected clients in the LAN domain, including the device name, IP address, MAC address, and connection type.

2.4GHz/5GHz Wi-Fi and Wi-Fi HaLow connections are both classified to the **Wi-Fi** Connection Type. Client devices connected to a bridged interface will **NOT** be displayed here.

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 3.3.1.4 for details on DHCP reservation.



Downlink Devices

Device Info	IP Address	MAC Address	Connection Type	Block Internet
*	172.18.2.208	5e:01:8[redacted]	Wi-Fi	○
VantronOS-451D	172.18.2.156	18:9b:a[redacted]	Wi-Fi	○
yfcs-dschen	172.18.2.232	54:75:9[redacted]	Wi-Fi	○
DESKTOP-DHT6NBN (Host)	172.18.2.174	18:c0:4[redacted]	Wired	○

Rows per page: 10 ‹ 1 ›

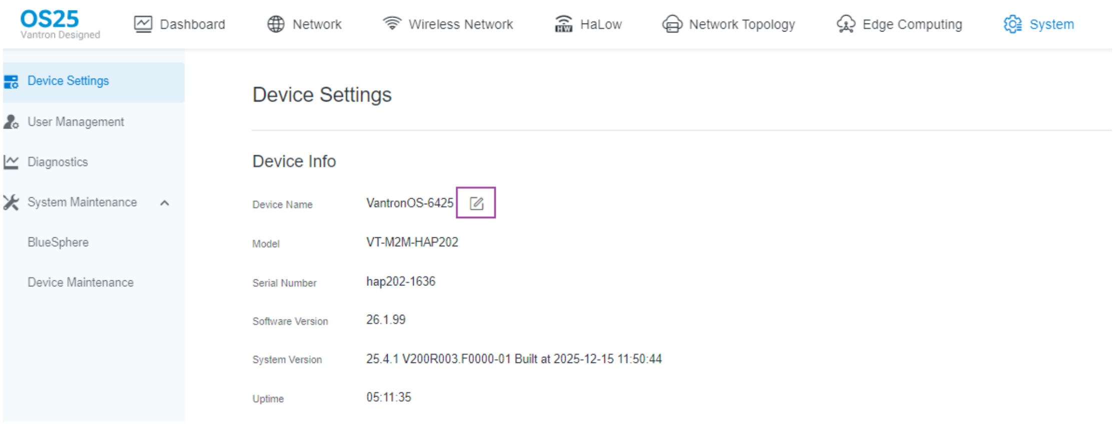
3.7 System

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

3.7.1 Device Settings

3.7.1.1 Modifying Device Name

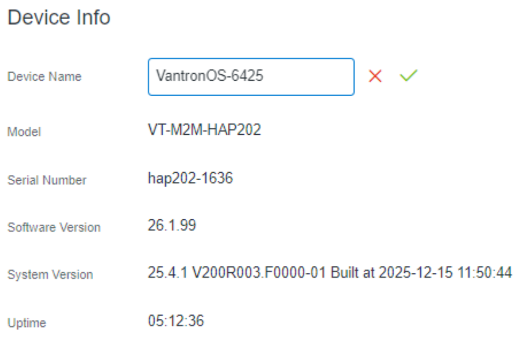
Device Info display core information—device name, model, serial number, software and system versions, and uptime.



Device Settings

Device Info

Device Name	VantronOS-6425
Model	VT-M2M-HAP202
Serial Number	hap202-1636
Software Version	26.1.99
System Version	25.4.1 V200R003.F0000-01 Built at 2025-12-15 11:50:44
Uptime	05:11:35



Device Info

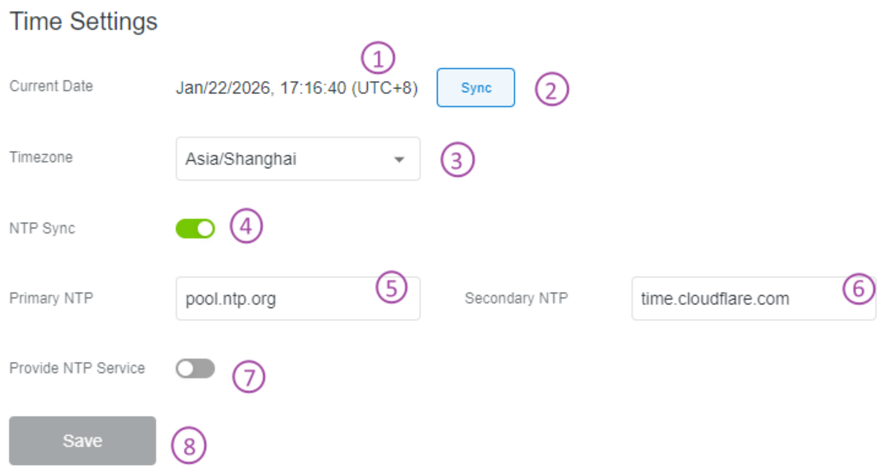
Device Name	VantronOS-6425 ✕ ✓
Model	VT-M2M-HAP202
Serial Number	hap202-1636
Software Version	26.1.99
System Version	25.4.1 V200R003.F0000-01 Built at 2025-12-15 11:50:44
Uptime	05:12:36

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.

3.7.1.2 System Time

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



Time Settings

Current Date: Jan/22/2026, 17:16:40 (UTC+8) [Sync]

Timezone: Asia/Shanghai

NTP Sync: ●

Primary NTP: pool.ntp.org

Secondary NTP: time.cloudflare.com

Provide NTP Service: ○

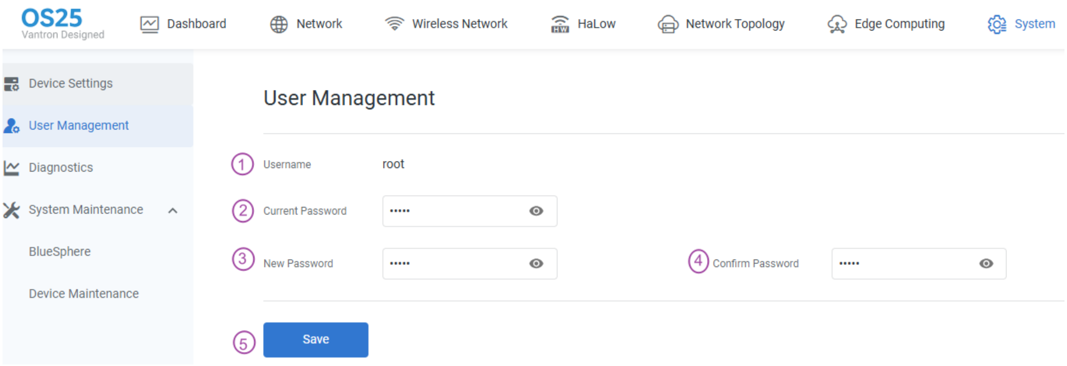
[Save]

Description of the numbered areas

1. Current Date—Displays today’s date for the selected time zone.
2. Sync—Triggers a one-time NTP update immediately. The date resets after every power cycle because HAP202 lacks an RTC.
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.
5. Primary NTP—Preferred NTP server.
6. Secondary NTP—Backup NTP server.
7. Use the current device as the NTP service provider, so that clients can synchronize their time to its system clock.
8. If you have made any changes, click **Save** to apply.

3.7.2 User Management

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



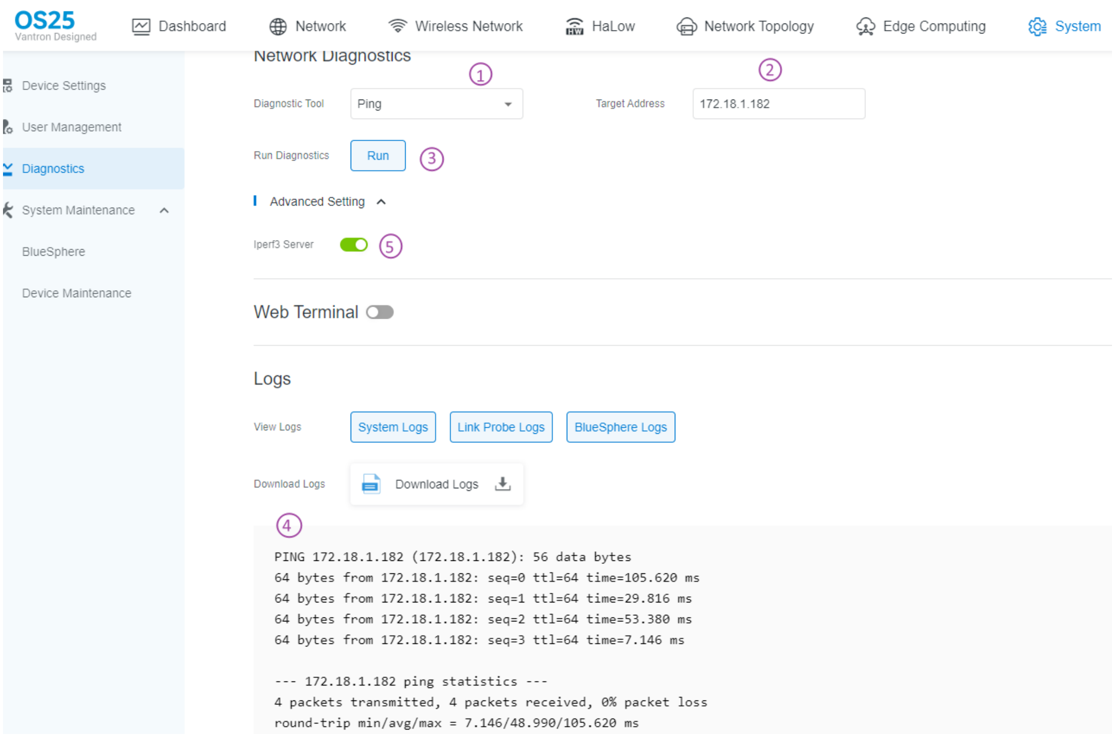
Description of the numbered areas

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

3.7.3 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.

3.7.3.1 Network Diagnostics



Diagnostic Tool: Ping

Target Address: 172.18.1.182

Iperf3 Server: on

```
PING 172.18.1.182 (172.18.1.182): 56 data bytes
64 bytes from 172.18.1.182: seq=0 ttl=64 time=105.620 ms
64 bytes from 172.18.1.182: seq=1 ttl=64 time=29.816 ms
64 bytes from 172.18.1.182: seq=2 ttl=64 time=53.380 ms
64 bytes from 172.18.1.182: seq=3 ttl=64 time=7.146 ms

--- 172.18.1.182 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 7.146/48.990/105.620 ms
```

Description of the numbered areas

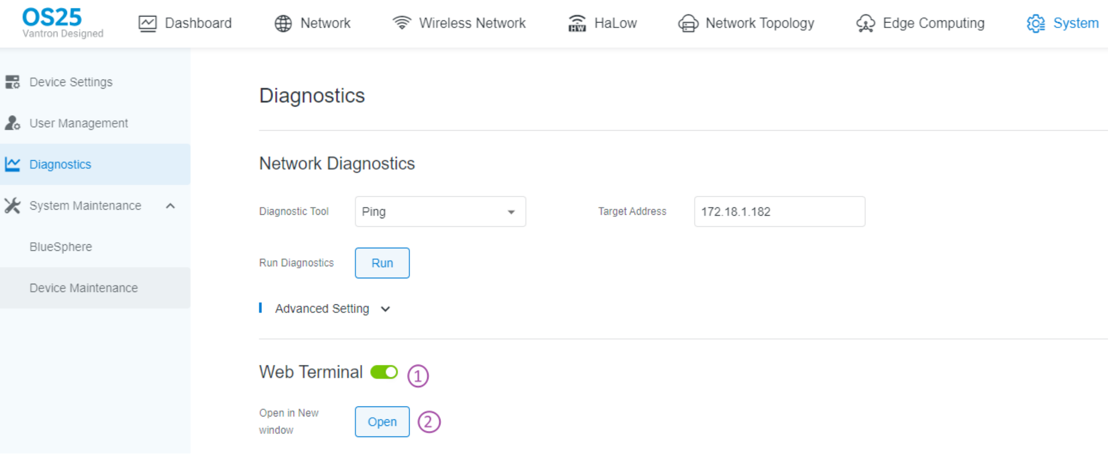
1. Select a diagnostic tool from the drop-down list (ping, traceroute, nsloopup, iPerf3).

   After selecting iPerf3 Client as the diagnostic tool, you need enable the iPerf3 server on the paired device.

2. Enter the destination IP address or domain name for the test.
3. Initiate a diagnostic test.
4. The test results are displayed correspondingly.
5. Under **Advanced Settings**, toggle the iPerf3 server on/off. (Enabling the iPerf3 server allows an iPerf3 client to test the link throughput.)

3.7.3.2 Web Terminal

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



Diagnostics

Network Diagnostics

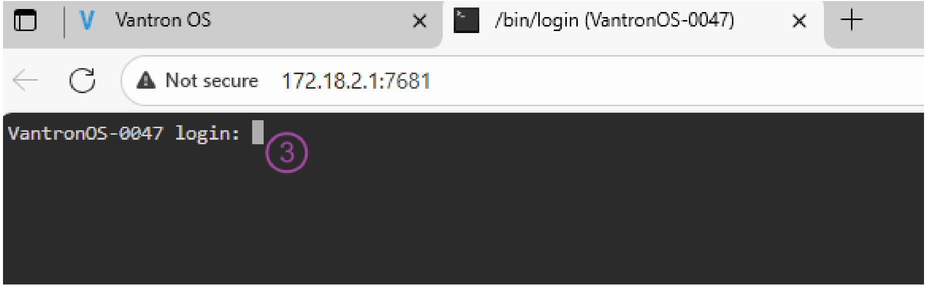
Diagnostic Tool: Ping

Target Address: 172.18.1.182

Run Diagnostics

Web Terminal

Open in New window



```
VantronOS-0047 login: 
```

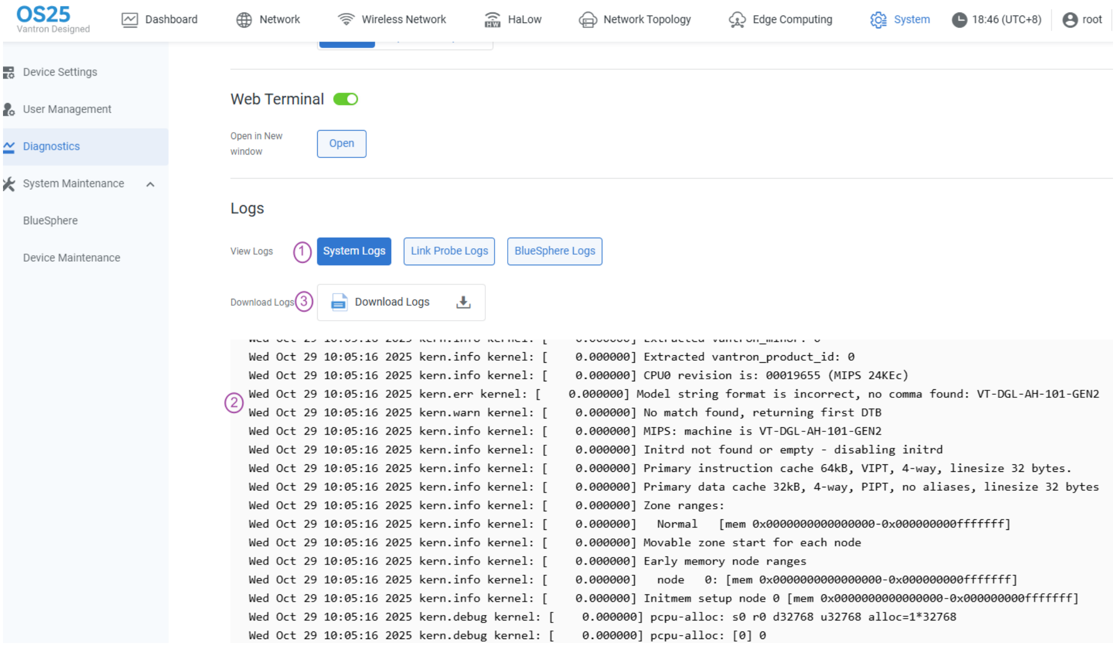
Description of the numbered areas

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

Web terminal login requires root privileges. The root password is unique to each device due to security concern. Please contact the Vantron FAE team to obtain it.

3.7.3.3 Logs

The system offers different device logs for maintenance or troubleshooting.



```
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] Extracted vantron_minor: 0
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] Extracted vantron_product_id: 0
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] CPU0 revision is: 00019655 (MIPS 24KEc)
Wed Oct 29 10:05:16 2025 kern.err kernel: [    0.000000] Model string format is incorrect, no comma found: VT-DGL-AH-101-GEN2
Wed Oct 29 10:05:16 2025 kern.warn kernel: [    0.000000] No match found, returning first DTB
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] MIPS: machine is VT-DGL-AH-101-GEN2
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] Initrd not found or empty - disabling initrd
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] Primary instruction cache 64kB, VIPT, 4-way, linesize 32 bytes.
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] Primary data cache 32kB, 4-way, PIPT, no aliases, linesize 32 bytes
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] Zone ranges:
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000]   Normal   [mem 0x0000000000000000-0x000000000fffffff]
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] Movable zone start for each node
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] Early memory node ranges
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000]   node   0: [mem 0x0000000000000000-0x000000000fffffff]
Wed Oct 29 10:05:16 2025 kern.info kernel: [    0.000000] Initmem setup node 0 [mem 0x0000000000000000-0x000000000fffffff]
Wed Oct 29 10:05:16 2025 kern.debug kernel: [    0.000000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
Wed Oct 29 10:05:16 2025 kern.debug kernel: [    0.000000] pcpu-alloc: [0] 0
```

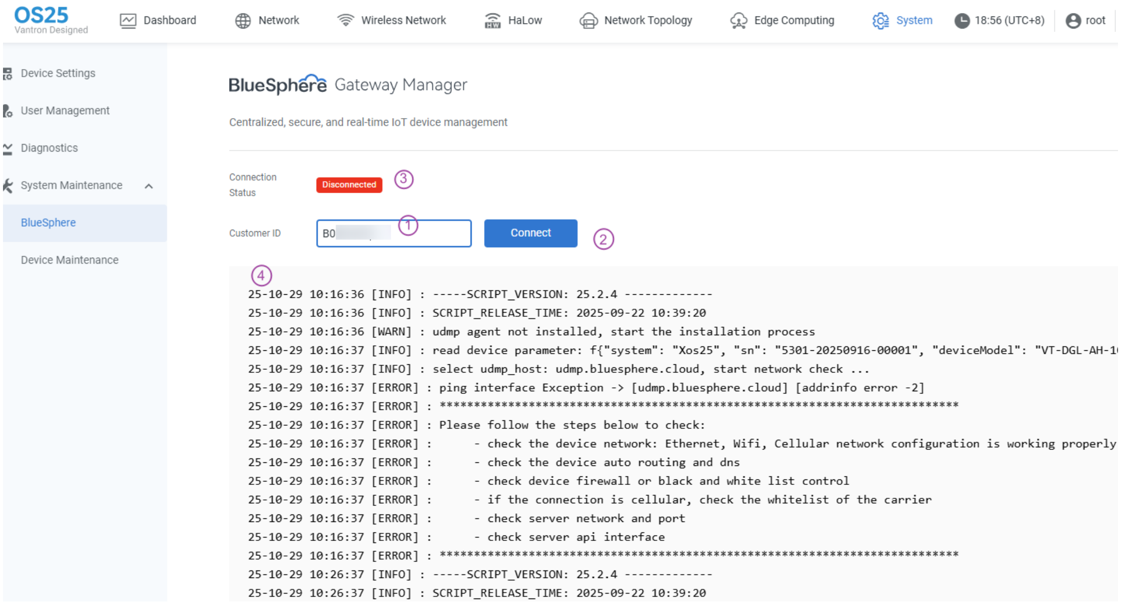
Description of the numbered areas

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

3.7.4 System Maintenance

3.7.4.1 BlueSphere

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



Connection Status: Disconnected

Customer ID: B0[redacted]

```
25-10-29 10:16:36 [INFO] : -----SCRIPT_VERSION: 25.2.4 -------------
25-10-29 10:16:36 [INFO] : SCRIPT_RELEASE_TIME: 2025-09-22 10:39:20
25-10-29 10:16:36 [WARN] : udmp agent not installed, start the installation process
25-10-29 10:16:37 [INFO] : read device parameter: f{"system": "Xos25", "sn": "5301-20250916-00001", "deviceModel": "VT-DGL-AH-1
25-10-29 10:16:37 [INFO] : select udmp_host: udmp.bluesphere.cloud, start network check ...
25-10-29 10:16:37 [ERROR] : ping interface Exception -> [udmp.bluesphere.cloud] [addrinfo error -2]
25-10-29 10:16:37 [ERROR] : *****************************************************************************
25-10-29 10:16:37 [ERROR] : Please follow the steps below to check:
25-10-29 10:16:37 [ERROR] :      - check the device network: Ethernet, Wifi, Cellular network configuration is working properly
25-10-29 10:16:37 [ERROR] :      - check the device auto routing and dns
25-10-29 10:16:37 [ERROR] :      - check device firewall or black and white list control
25-10-29 10:16:37 [ERROR] :      - if the connection is cellular, check the whitelist of the carrier
25-10-29 10:16:37 [ERROR] :      - check server network and port
25-10-29 10:16:37 [ERROR] :      - check server api interface
25-10-29 10:16:37 [ERROR] : *****************************************************************************
25-10-29 10:26:37 [INFO] : -----SCRIPT_VERSION: 25.2.4 -------------
25-10-29 10:26:37 [INFO] : SCRIPT_RELEASE_TIME: 2025-09-22 10:39:20
```

Prerequisites:

HAP202 must have internet access.

You have an authorized BlueSphere GWM user account.

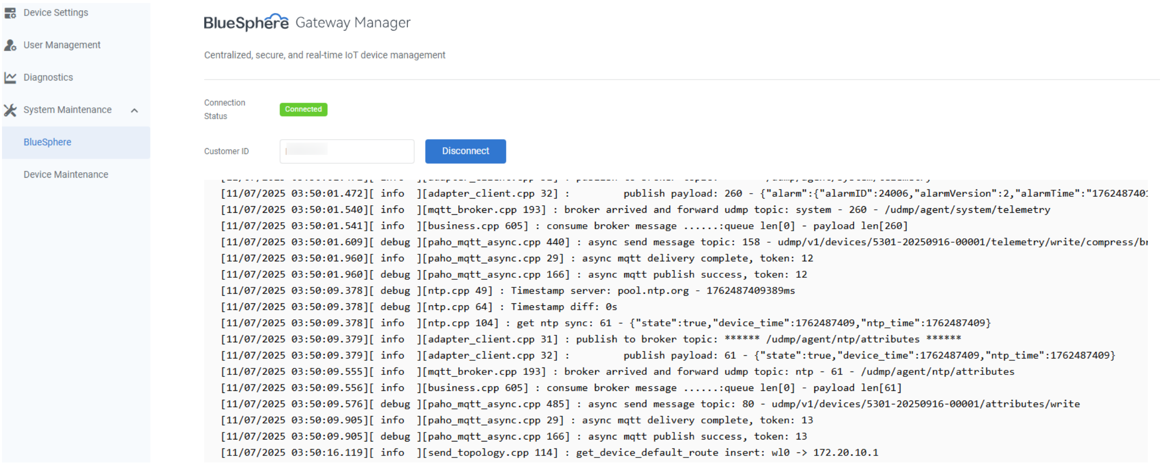
Description of the numbered areas

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.

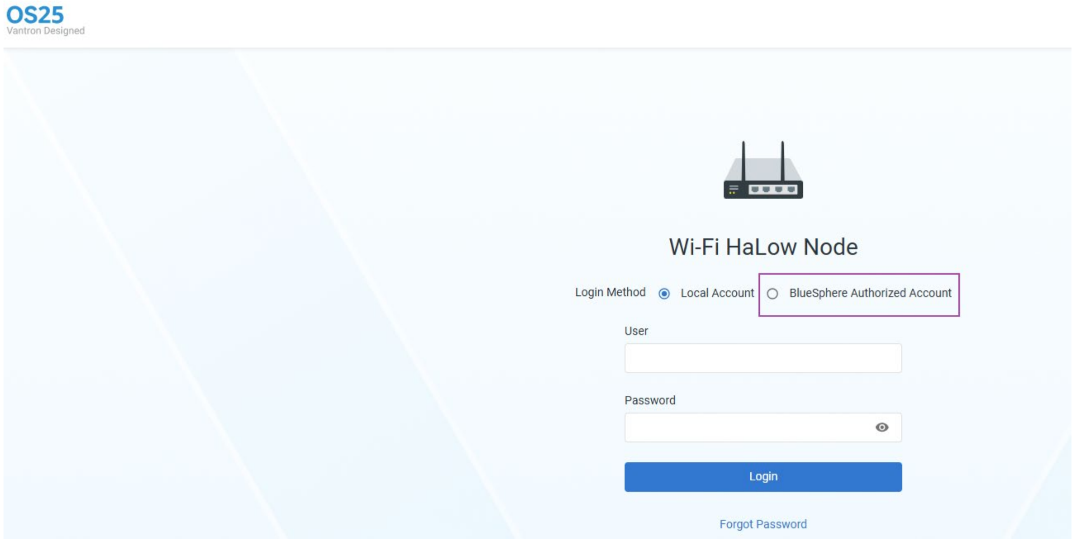


Connection Status: Connected

Customer ID: [redacted]

```
[11/07/2025 03:50:01.472][ info  ][adapter_client.cpp 32] :         publish payload: 260 - {"alarm":{"alarmID":24006,"alarmVersion":2,"alarmTime":"176248740
[11/07/2025 03:50:01.540][ info  ][mqtt_broker.cpp 193] : broker arrived and forward udmp topic: system - 260 - /udmp/agent/system/telemetry
[11/07/2025 03:50:01.541][ info  ][business.cpp 605] : consume broker message ......:queue len[0] - payload len[260]
[11/07/2025 03:50:01.609][ debug ][paho_mqtt_async.cpp 440] : async send message topic: 158 - udmp/v1/devices/5301-20250916-00001/telemetry/write/compress/b
[11/07/2025 03:50:01.960][ info  ][paho_mqtt_async.cpp 29] : async mqtt delivery complete, token: 12
[11/07/2025 03:50:01.960][ debug ][paho_mqtt_async.cpp 166] : async mqtt publish success, token: 12
[11/07/2025 03:50:09.378][ debug ][ntp.cpp 49] : Timestamp server: pool.ntp.org - 1762487409389ms
[11/07/2025 03:50:09.378][ debug ][ntp.cpp 64] : Timestamp diff: 0s
[11/07/2025 03:50:09.378][ info  ][ntp.cpp 104] : get ntp sync: 61 - {"state":true,"device_time":1762487409,"ntp_time":1762487409}
[11/07/2025 03:50:09.379][ info  ][adapter_client.cpp 31] : publish to broker topic: ****** /udmp/agent/ntp/attributes ******
[11/07/2025 03:50:09.379][ info  ][adapter_client.cpp 32] :         publish payload: 61 - {"state":true,"device_time":1762487409,"ntp_time":1762487409}
[11/07/2025 03:50:09.555][ info  ][mqtt_broker.cpp 193] : broker arrived and forward udmp topic: ntp - 61 - /udmp/agent/ntp/attributes
[11/07/2025 03:50:09.556][ info  ][business.cpp 605] : consume broker message ......:queue len[0] - payload len[61]
[11/07/2025 03:50:09.576][ debug ][paho_mqtt_async.cpp 485] : async send message topic: 80 - udmp/v1/devices/5301-20250916-00001/attributes/write
[11/07/2025 03:50:09.905][ info  ][paho_mqtt_async.cpp 29] : async mqtt delivery complete, token: 13
[11/07/2025 03:50:09.905][ debug ][paho_mqtt_async.cpp 166] : async mqtt publish success, token: 13
[11/07/2025 03:50:16.119][ info  ][send_topology.cpp 114] : get_device_default_route insert: wl0 -> 172.20.10.1
```

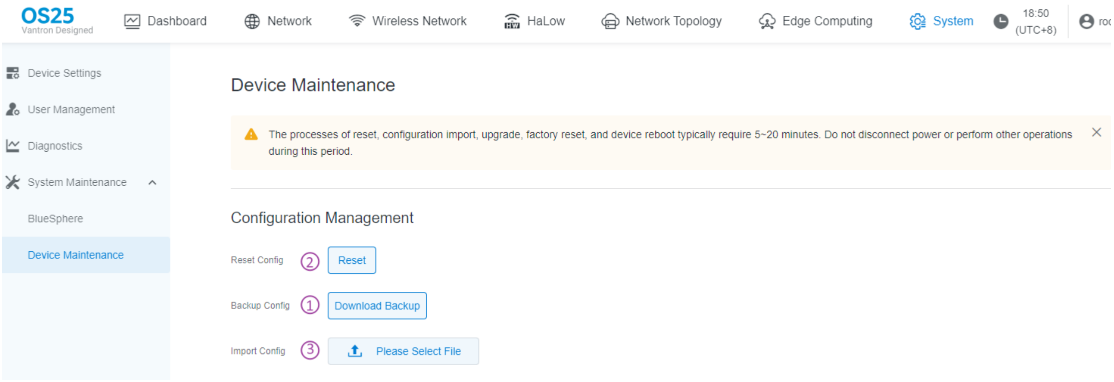
If you log out the portal now, you will find two login methods available. You can sign back in with either your local credentials or your authorized GWM account.



3.7.4.2 Device Maintenance

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

- Configuration Management



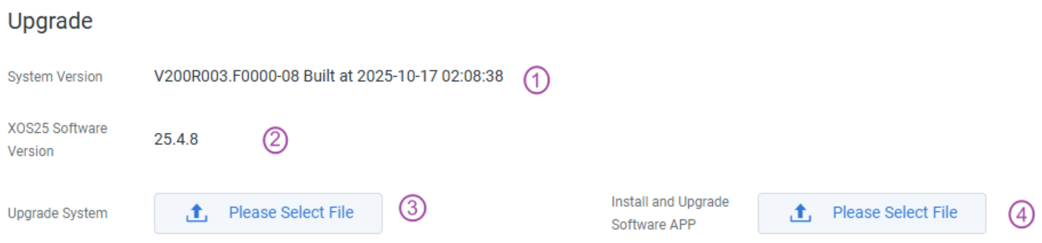
The processes of reset, configuration import, upgrade, factory reset, and device reboot typically require 5~20 minutes. Do not disconnect power or perform other operations during this period.

Description of the numbered areas

1. If needed, download current device configuration as a backup.
2. Reset the device configuration (this action clears user configuration).
3. If needed, import a configuration file after the device reset (only configuration files for the same device model are supported).

After the configuration reset, you can re-log in to the device **with your password** and follow the setup wizard to finish the first-time configuration.

- Upgrade



Upgrade

System Version: V200R003.F0000-08 Built at 2025-10-17 02:08:38

XOS25 Software Version: 25.4.8

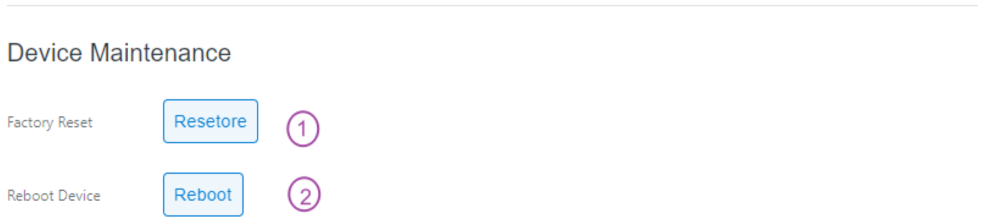
Description of the numbered areas

1. Current firmware version.
2. Current VantronOS version.
3. Upgrade the firmware manually from a local directory.

   Upgrades are allowed only from an older to a higher version.
4. Install new apps or upgrade existing ones from a local directory.

   Upgrades are allowed only from an older to a higher version.

- Device Maintenance



Device Maintenance

Description of the numbered areas

1. Factory reset the device with device configuration, user data and apps cleared.
2. Manually restart the device.

After factory reset the device, you must re-log in to the device **via the debug port** (contact Technical Support).

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

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.