G335 Edge Computing Gateway

User Manual

Version: 1.6

Revision History:

No.	Software Version	Description	Date
V1.0	V200R003	First release	May 25, 2020
V1.1	V200R003	Modified the configuration of the Gateway	Jun 30, 2020
V1.2	V200R005	1. Added information about serial ports/ CAN/ GPS/ ZigBee/ system boot 2. Modified 3.5.3 4G/LTE description 3. Added SSH login description 4. Added a chapter for protocol configuration	Jun 1, 2022
V1.3	V200R005	Updated contact information	Jun 15, 2022
V1.4	V200R003	Updated interface description& gateway setup (Gen 7)	Nov. 21, 2022
V1.5	V200R003	Updated protocol portal login and configuration	Feb. 27, 2023
V1.6	V200R004	1. Updated the description of collection configuration, status description, and historical data on the protocol portal based on the program update 2. Updated the quick start and deleted the networking part 3. Added backlist and white list features to the firewall	Sep. 18, 2023

Table of Contents

Foreword

Thank you for purchasing G335 Industrial Gateway ("the Gateway" or "the Product"). 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.

Intended Users

This manual is intended for:

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

Copyright

Disclaimer

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

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

Technical Support and Assistance

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

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

Vantron Technology, Inc.
Address: 48434 Milmont Drive, Fremont, CA 94538
Tel: (650) 422-3128
Email: sales@vantrontech.com

Regulatory Information

The Product is designed to comply with:

- Part 15 of the FCC Rules
- PTCRB

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

Symbology

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

⚠	Caution for latent damage to system or harm to personnel
ℹ	Attention to important information or regulations

General Safety Instructions

For your safety and prevention of damage to the Gateway 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 the USB port or any other 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 power.

⚠ Place the cables properly at places without extrusion hazards.

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

⚠ Cleaning instructions:

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

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

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

⚠ Do not use in combustible and explosive environment:

- Keep away from combustible and explosive environment
- Keep away from all energized circuits
- Unauthorized removal of the enclosure from the 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 HARDWARE DESCRIPTION

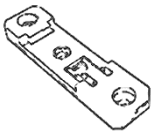
1.1 Product Overview

Vantron G335 edge computing gateway is a flagship gateway launched to meet the needs of Machine-to-Machine (M2M) communication and IIoT applications in various industrial scenarios. The Gateway supports a variety of industrial protocols to allow access by field industrial devices such as PLCs, HMIs, sensors, etc. The edge computing functionality helps to achieve data optimization at IoT edge nodes, which reduces the data volume accumulated in the field and the central console. With standard MQTT protocol, the Gateway provides a broad access to industrial data platforms to facilitate the digital transformation of factories.

The gateway adopts industrial design with guaranteed quality and reliability to offer an ideal solution for your IOT application. It supports a wide range of wireless communication networks, including 3G/4G/LTE cellular, WLAN, GPS, Zigbee, Lora, Bluetooth, and Iridium (9603). Meanwhile it provides access to Vantron BlueSphere cloud platform for unified management to ease the efforts of users by real-time monitoring and tracking, remote maintenance and OTA updates, task assignment and follow-ups.

1.2 Unpacking

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

Standard accessories		Optional accessories	
	1 x G335 gateway		1 x Power adapter
	1 x Wi-Fi antenna		1 x Female DC power connector
	1 x DIN rail mount		2 x 4G LTE antenna
/	/		1 x ZigBee antenna
/	/		1 x GPS antenna

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

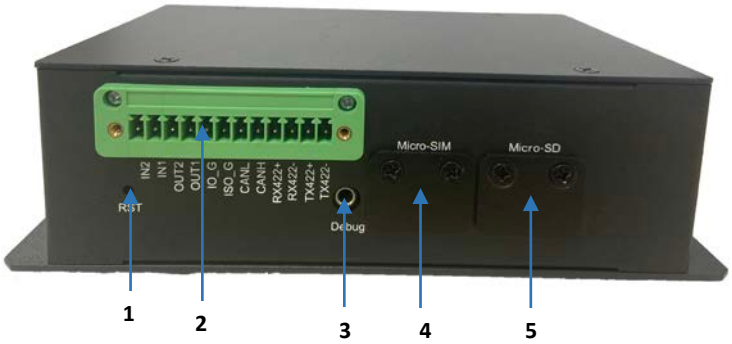
1.3 Specifications

G335			
System	CPU	TI, AM335x, ARM Cortex-A8, 32-Bit, 1GHz	
	Memory	512MB	
	Storage	8GB 1 x Micro SD card	
Communication	Ethernet	2 x Giga Ethernet Port (PoE supported on one port)	
	4G LTE	CAT M/ CAT 4 (Optional)	
	Wi-Fi & Bluetooth	Wi-Fi 802.11 a/b/g/n/ac + BT 5.0	
	Local RF module	ZigBee (Optional)	
	GNSS	GPS (Optional)	
I/Os	Serial port	1 x RS232, for debugging 1 x RS232/RS485 (DB9) 1 x RS232/RS485/RS422 (Reserved on the terminal block)	
	USB	1 x USB Type-A	
	GPIO	2 x Input, 2 x Output, isolated (Optional)	
	Alarm	1 x Buzzer alarm (Optional)	
	RTC	Supported	
	CAN	1 x CAN 2.0b (Reserved on the terminal block)	
System Control	Button	1 x Reset button	1 x Renew button
	LED indicator	1 x Power indicator	1 x Status indicator
Mechanical	Dimensions	155mm x 105mm x 50mm (Enclosure only) 177mm x 105mm x 50mm (With bracket)	
	Enclosure	Metal	
	Installation	DIN rail mount, wall mount	
	IP rating	IP30	
	Heat dissipation	Fanless	
Power	Input	6-36V DC, Over-current protection, Reverse polarity protection	
	Terminal	3-pin 3.81mm power terminal	
	Consumption	1.8W on average (Without considering wireless module consumption)	

Software	OS	VantronOS
	Custom development	SDK available, C/C++/Python/Node-Red/Node JS supported
	Device management platform	Vantron BlueSphere GWM
	Northbound protocol	MQTT
	Edge computing script	JavaScript, MicroPython
	Southbound protocol	Modbus TCP, Modbus RTU, EtherNet/IP, ISO-on-TCP, CC-link, etc.
	IPK import	Supported
	Interface language	Chinese and English (Default) Other languages (Optional)
	Log	Supported
	Configuration mode	Local, remote
	Upgrade	Local, OTA update
Network	NAT	Supported
	Network management	SNMP v1/v2c/v3
	NTP	Supported
	IP application	Ping, Traceroute, Nslookup
	Routing	Static routing
Security & Reliability	Firewall	Supported
	VPN	OpenVPN, L2TP, PPTP, IPSec
	Multi-level permission	Supported
	Link detection	Heartbeat detection, automatic re-connection
	Network reliability	Failover supported, link backup between Ethernet, Wi-Fi and 4G/LTE
Environment Condition	Temperature	Operating: -20℃ ~ +70℃ (Optional: -40℃ ~ +85℃) Storage: -40℃~+85℃
	Humidity	RH 5%-95% (Non-condensing)
	Certification	FCC, PTCRB

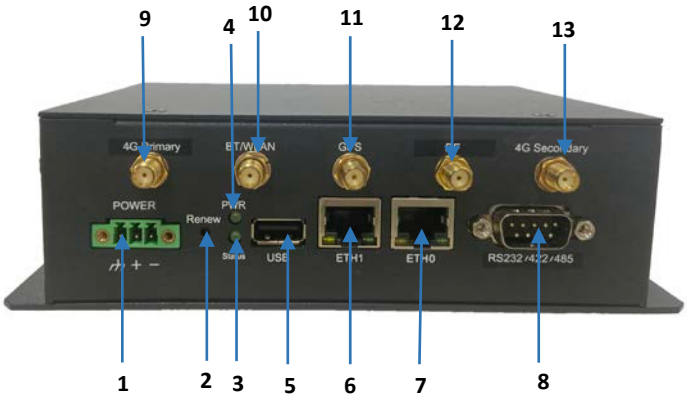
1.4 Definition of Interfaces

1.4.1 Front view



No.	Name	Description
1	RST button	A short press of this button will reset and restart the Gateway
2	Terminal block	Check out the pinout description of the terminal block in **1.5 Serial Port Introduction**
3	Debug port	
4	Micro SIM slot	
5	Micro SD slot	

1.4.2 Rear view

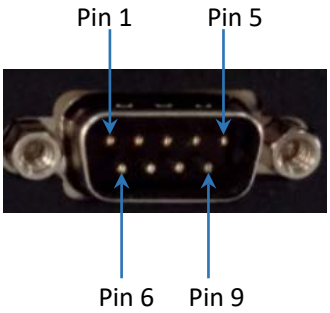


No.	Name	Description
1	Power terminal	12V DC power terminal
2	Renew button	1. If a system upgrade drive is inserted in the SD card slot or USB port, the system will be upgraded upon a short press of the button for 2 seconds, and the buzzer will sound for 3 seconds. 2. The gateway will be factory reset with user data and custom configurations erased when the button is pressed for 3-10 seconds, and the buzzer will sound for 1 second. 3. User partitions will be formatted with user data be cleared when this button is pressed for more than 10 seconds, and the buzzer will sound for 4 seconds at intervals of 200ms.
3	Status indicator	1. The indicator blinks when the Gateway boots up. 2. The indicator will turn solid green when the bootup finishes. 3. The indicator will blink when the system is being upgraded or configurations are cleared.
4	Power indicator	The indicator will light up when the Gateway is powered on.
5	USB 2.0 Type-A	
6	ETH 1 port	Set as ETH1 in VantronOS and works in WAN area by default
7	ETH 0 port	Set as ETH0 in VantronOS and works in LAN area by default
8	Serial port	RS232/RS485 (DB9 connector)
9	4G primary antenna	
10	BT/WLAN antenna	
11	GPS antenna	
12	RF antenna	
13	4G diversity antenna	

1.5 Serial Ports

1.5.1 DB9 connector

The DB9 serial port is multiplexed as RS232 or RS485.



Pinout description:

Pin	Signal	Node	Port	Type	Description
1	RS485-A	/dev/ttyO4	UART1		RS485 A Signal
2	RS485-B / RS232RXD			I	RS485 B Signal / RS232 Receive Signal
3	RS232TXD			O	RS232 Transmit Signal
4	NC				
5	GND			P	GND
6	NC				
7	NC				
8	NC				
9	NC				

To enable RS232 mode on the serial port and open it with a serial port communication program (e.g., microcom):

```
~# gpio set uart1 rs232 save
Or
~# gpio set uart1 rs232
~# gpio get uart1
rs232

~# microcom /dev/ttyO4 -s 115200
```

To enable RS485 mode on the serial port and open it with a serial port communication program (e.g., microcom):

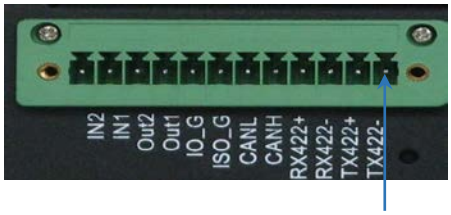
```
~# gpio set uart1 rs485 save

~# microcom /dev/ttyO4 -s 115200
```

*"**Save**" in the above command line is optional. When set as default, the configuration will remain valid after the device reboot.*

1.5.2 Terminal block

Certain pins on the terminal block are multiplexed as RS232, RS485 or RS422.



Pin 1

Pinout description:

Pin	Pin name	Node	Port	Type	Description
1	TX422-	/dev/ttyO1	UART0		
2	TX422+				
3	RX422- / RS485_2_B / SRXD3			Jumper cap configuration	
4	RX422+ / RS485_2_A / STXD3			Jumper cap configuration	
5	CANH				
6	CANL				
7	ISO_GND			P	GND
8	IO_GND			P	GND
9	GPIO_OUT1			IO	
10	GPIO_OUT2			IO	
11	GPIO_IN1			IO	
12	GPIO_IN2			IO	

Jumper connection might vary with the serial port modes.

For RS232 communication, take off the top cover and remove JP2, JP3, and JP4, then open the serial port with the serial port communication program:

```
~# gpio set uart0 rs232 save
Or
~# gpio set uart0 rs232

~# gpio get uart0
rs232

~# microcom /dev/ttyO1 -s 115200
```

For RS485 communication, take off the top cover and remove JP2 with JP3 and JP4 unchanged, then open the serial port with the serial port communication program:

```
~# gpio set uart0 rs485 save

~# microcom /dev/ttyO1 -s 115200
```

For RS422 communication test, take off the top cover and remove JP2, JP3, and JP4, then open the serial port with the serial port communication program:

```
~# gpio set uart0 rs422 save

~# microcom /dev/ttyO1 -s 115200
```

__"Save"__ in the above command line is optional. When set as default, the configuration will remain valid after the device reboot.

1.6 CAN (Optional)

As shown in the pinout description in section 1.5.2, the terminal block offers a CAN bus as an option. The following describes the communication of two G335 gateways via CAN protocol. If you have customized end devices and special data protocols requiring customization from Vantron, please contact your sales representative.

1. Prepare two G335 gateways, and the physical CAN connection shall be as follows:

Gateway A		Gateway B
CANH	<->	CANH
CANL	<->	CANL
Transmit Data	->	Receive Data

2. Run "candump" command on Gateway B and set the Baud rate between 100,000 (100kbps) and 1,000,000 (1000kbps);

```
# ip link set can0 type can bitrate 100000
# ifconfig can0 up
# candump can0
```

3. Transmit data from Gateway A;

```
# ifconfig can0 up
# cansend can0 5A1#11.2233.44556677.88
```

4. The data will be printed on Gateway B.

1.7 GPIO (Optional)

As shown in the pinout description in section 1.5.2, the terminal block offers GPIO interfaces as an option. Please refer to the following instructions to enable the GPIO interfaces.

Name	Pin #
"gpio_in1" (gpio0_22)	22
"gpio_in2" (gpio0_26)	26
"gpio_out1" (gpio0_28)	60
"gpio_out2" (gpio0_8)	104

1. Write a GPIO pin number to “/sys/class/gpio/export” to export the pin. For instance, to export pin 22:

```
~# echo 22 > /sys/class/gpio/export
```

2. Once the pin is exported, set its direction as input or output by writing "in" or "out" to the command. For instance, to set pin 22 as an output pin;

```
~# echo out > /sys/class/gpio/gpio22/direction
```

3. If you have configured the pin as an output pin in the prior step, now you can set its value to 0 or 1, which corresponds to low or high, respectively:

```
~# echo 0 > /sys/class/gpio/gpio22/value        [set it low], or
~# echo 1 > /sys/class/gpio/gpio22/value        [set it high]
```

4. Read the GPIO value;

```
~# cat /sys/class/gpio/gpio22/value
```

5. When you finish using the pin, just unexport it. To do this, write the pin number to the unexport file:

```
~# echo 22 > /sys/class/gpio/unexport
```

1.8 Bluetooth

1. Open and initialize HCI device;

```
~# hciconfig hci0 up
```

2. Scan for the Bluetooth devices (the MAC addresses of the Bluetooth devices will be listed below the command line);

```
~# hcitool scan
```

3. Browse all the services available on the target device discovered after the Bluetooth scan and figure out the channel of service "OBEX Object Push";

   For instance, the Bluetooth device with MAC address 3C:CD:5D:36:9F:A6 is running the following services and the channel of service "OBEX Object Push" is 12.

```
# sdptool browse 3C:CD:5D:36:9F:A6
Browsing 3C:CD:5D:36:9F:A6 ...
Service RecHandle: 0x10000
Service Class ID List:
  "Generic Attribute" (0x1801)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 31
……………………………………………………………….
……………………………………………………………….
Browsing 3C:CD:5D:36:9F:A6 ...
Service Name: OBEX Phonebook Access Server
Service RecHandle: 0x1000a
Service Class ID List:
  "Phonebook Access - PSE" (0x112f)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 19
  "OBEX" (0x0008)
Profile Descriptor List:
  "Phonebook Access" (0x1130)
    Version: 0x0101



Service Name: OBEX Object Push
Service RecHandle: 0x1000b
Service Class ID List:
```

```
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 12
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0102
……………………………………………………………….
……………………………………………………………….
```

If the Gateway does not support service “OBEX Object Push”, please input the command line below:

```
~# sdptool add --channel = 12 OPUSH
```

4. Use “obex_test” command to send a test file to the Bluetooth device, i.e., obex_test -b <MAC address of the Bluetooth device > <channel>;

   For instance, to send the test file to the aforementioned Bluetooth device:

```
# obex_test -b 3C:CD:5D:36:9F:A6 12
> c
[Note: to connect to the device]

…………..
Connect OK!
[Note: the Bluetooth device is connected to the gateway.]

Version: 0x10. Flags: 0x00
> p /etc/usb-mode.json
[Note: The arguments following “p” is the path of the test file to be sent.]

PUT file (local)> name=send.txt, size=9
PUT remote filename (default: send.txt)>
Going to send 9 bytes
…………..
PUT successful!
[Note: The test file is sent to the Bluetooth device]

> q
[Note: to exit obex_test]
```

5. Exit “obex_test”, and enable page and search scan so that the target Bluetooth device is discoverable;

```
~# hciconfig hci0 piscan
```

6. Run obexd service to receive the test file, i.e., obexd -a -n -r <path for saving the file>;

   For instance, the test file is stored in “ /tmp”:

```
~# export
DBUS_SESSION_BUS_ADDRESS="unix:path=/var/run/dbus/system_bus_socket"
~# obexd -a -n -r /tmp/
```

7. After the file transfer, disable page and search scan and the device will not be discoverable.

```
~# hciconfig hci0 noscan
```

After you go through the steps above, the function test finishes.

If you need shut down the HCI device, input the command line below:

```
~# hciconfig hci0 down
```

To rename the HCI device, “Bluez 5.21 test” for instance, input the command line below:

```
~# hciconfig hci0 name “Bluez 5.21 test”
~# hciconfig hci0 down
~# hciconfig hci0 up
```

1.9 GPS (Optional)

The Gateway is optionally equipped with a GPS module.

1. To power on the GPS module:

```
~# gpio set gps on
```

2. To acquire GPS data:

```
# gps 9600 /dev/ttyS0
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
GPGGA,,,,,,0,00,99.99,,,,,,*48
GPGSA,A,1,,,,,,,,,,,,,99.99,99.99,99.99*30
GPGLL,,,,,,V,N*64
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
GPGGA,,,,,,0,00,99.99,,,,,,*48
GPGSA,A,1,,,,,,,,,,,,,99.99,99.99,99.99*30
GPGLL,,,,,,V,N*64
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
GPGGA,,,,,,0,00,99.99,,,,,,*48
GPGSA,A,1,,,,,,,,,,,,,99.99,99.99,99.99*30
GPGLL,,,,,,V,N*64
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
GPGGA,,,,,,0,00,99.99,,,,,,*48
GPGSA,A,1,,,,,,,,,,,,,99.99,99.99,99.99*30
GPGLL,,,,,,V,N*64
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
```

3. To power off the GPS module:

```
~# gpio set gps off
```

1.10 ZigBee (Optional)

1.10.1 ZigBee MGM12P module

1. To power on the ZigBee module:

```
~# gpio set zigbee3 on
```

2. Since there are two module versions, command lines for running the application are different based on the version, **Z3GatewayHost -p /dev/ttyO3 -f x -b 115200** for module V2.6 and **Z3Gateway610 -p /dev/ttyO3 -f x -b 115200** for module Silabe3.0 ZigBee (YEM001R077), respectively. Gateways with module V2.6 have the following serial numbers: PO110221-04-001, PO110221-04-002, PO110221-04-003, PO081321-23-MA-001, PO081321-23-MA-002, V5106-202110010-001. Therefore, gateways with serial numbers other than those listed above run the application like below:

```
~# Z3Gateway610 -p /dev/ttyO3 -f x -b 115200
Reset info: 11 (SOFTWARE)
ezspSetupSerialPort: bps:115200 stopBits:1 rtsCts:0
ezspSetupSerialPort: bps match 115200(8)<->115200
ezspSetupSerialPort: serialPort:/dev/ttyO3
ezspSetupSerialPort:SUCCESS
ezsp ver 0x08 stack type 0x02 stack ver. [6.10.3 GA build 297]
Ezsp Config: set address table size to 0x0002:Success: set
Ezsp Config: set TC addr cache to 0x0002:Success: set
Ezsp Config: set MAC indirect TX timeout to 0x1E00:Success: set
Ezsp Config: set max hops to 0x001E:Success: set
Ezsp Config: set tx power mode to 0x8000:Success: set
Ezsp Config: set supported networks to 0x0001:Success: set
Ezsp Config: set stack profile to 0x0002:Success: set
Ezsp Config: set security level to 0x0005:Success: set
Ezsp Value : set end device keep alive support mode to 0x00000003:Success: set
Ezsp Policy: set binding modify to "allow for valid endpoints & clusters
only":Success: set
Ezsp Policy: set message content in msgSent to "return":Success: set
Ezsp Value : set maximum incoming transfer size to 0x00000052:Success: set
Ezsp Value : set maximum outgoing transfer size to 0x00000052:Success: set
Ezsp Config: set binding table size to 0x0010:Success: set
Ezsp Config: set key table size to 0x0004:Success: set
Ezsp Config: set max end device children to 0x0020:Success: set
Ezsp Config: set aps unicast message count to 0x000A:Success: set
Ezsp Config: set broadcast table size to 0x000F:Success: set
Ezsp Config: set neighbor table size to 0x0010:Success: set
```

```
NCP supports maxing out packet buffers
Ezsp Config: set packet buffers to 72
Ezsp Config: set end device poll timeout to 0x0008:Success: set
Ezsp Config: set zll group addresses to 0x0000:Success: set
Ezsp Config: set zll rssi threshold to 0xFFD8:Success: set
Ezsp Config: set transient key timeout to 0x00B4:Success: set
Ezsp Endpoint 1 added, profile 0x0104, in clusters: 8, out clusters 19
Ezsp Endpoint 242 added, profile 0xA1E0, in clusters: 0, out clusters 1
HA Gateweay EUI64 = BC33ACFFFE71A457
MQTT Client Init
MQTT Client ID = gwBC33ACFFFE71A457
Found 0 files

MQTT not connected, message not sent: gw/BC33ACFFFE71A457/settings - {"ncpStackVersion":"6.10.3-297","networkUp":false}
MQTT not connected, message not sent: gw/BC33ACFFFE71A457/relays - {"relays":[]}
MQTT not connected, message not sent: gw/BC33ACFFFE71A457/devices - {"devices":[]}
Attempting to reconnect to broker
Z3Gateway610>MQTT connected to broker
MQTT connected, starting gateway heartbeat and command processing
Subscribing to topic "gw/BC33ACFFFE71A457/commands" using QoS2
Subscribing to topic "gw/BC33ACFFFE71A457/publishstate" using QoS2
Subscribing to topic "gw/BC33ACFFFE71A457/updatesettings" using QoS2

Z3Gateway610>
Z3Gateway610> network leave
# Command explanation: to clear all the networks
Z3Gateway610> plugin network-creator start 1
# Command explanation: to create a network
Z3Gateway610> plugin network-creator-security open-network
# Command explanation: to allow devices to join network
Z3Gateway610> network change-channel 25
# Command explanation: to set the channel to 25
Z3Gateway610> info
# Command explanation: to check the configurations of the existing channel
```

3. To power off the ZigBee module:

```
~# gpio set zigbee3 off
```

1.10.2 ZigBee Digi XB24C (XBee) module

Two gateways are needed to finish the communication. XBee module can set up ZigBee network automatically and assign the address accordingly.

1. To power on the module:

```
~# gpio set zigbee on
```

2. Attach the module to "/dev/ttyO3" to write the AT commands into the tty device (refer to the datasheet of Digi XBee S2C for the details of the AT commands);

3. Set one device as the coordinator (route is the default mode), and input the string "Hello world":

```
~# at 9600 /dev/ttyO3
+++OK
atce 1
atnd
..... (the route information is displayed; an error message will be displayed if it fails to join the network)
atdh 0
OK
atdl ffff
OK
atcn
OK
Hello world!
```

4. The other device is in route mode, and the string "Hello world" will be displayed:

```
~# at 9600 /dev/ttyO3
+++OK
atnd
..... (the route information is displayed; an error message will be displayed if it fails to join the network)
atdh 0
OK
atdl ffff
OK
atcn
OK
Hello world!
```

ZigBee AT Commands used in the above example:

AT Command	Description
+++	Switch to AT command mode
atmy	Response to network address
atce 1	Set to coordinator (1 for coordinator, 0 for route)
atdh 0	Set destination high address as 0x00000000
atdl ffff	Set destination low address as 0x0000ffff
atnd	Response to the route tables
atcn	Exit AT command mode

5. To power off the ZigBee module:

```
~# gpio set zigbee off
```

1.11 3.5mm Debug Port

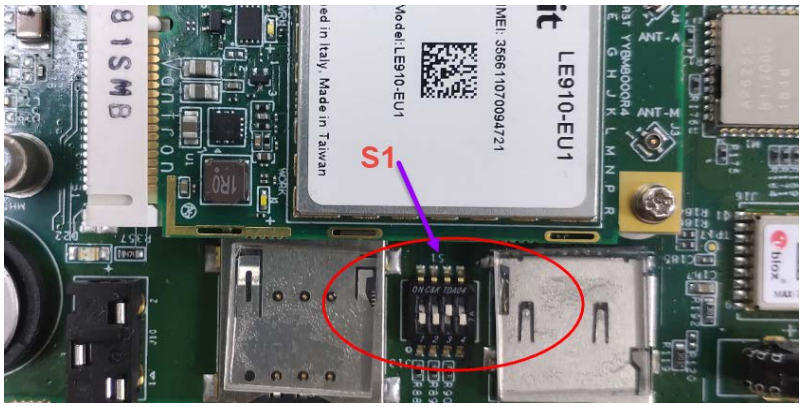
Pin	Description
Pin 1	GND
Pin 2	TXD (RS232)
Pin 3	RXD (RS232)

1.12 System Boot

The system boots up from eMMC by default.

1.12.1 System boot and eMMC flashing from an SD card

1. Open the Gateway box;
2. Set DIP switch S1 to off:off:on:off as shown below;



3. Make a bootable SD card/USB drive;
   1) Insert the SD card/USB drive into a Linux host and input a dmesg command to get the path of the SD card/USB drive (for instance, /dev/sdb);
   2) Input the following command line to unzip the release package sent from Vantron;

      unzip XOS_sd2mmc_VT-M2M-G335S_Vxxxx.zip //replace the name with the package name you received

   3) You will probably get the files as explained below:

      ├── build.date //Image built date

      ├── sd2emmc.sh //Script for SD card bootup

      ├── XOS_sd2mmc_VT-M2M-G335_Vxxx.Fxxx-xxx.img //Bootup image

      ├── XOS_sd2mmc&sdAutoUpgrade_VT-M2M-G335_Vxxx.Fxxx-xxx.sha256sum //sha256sum file

      └── XOS_sdAutoUpgrade_VT-M2M-G335_VxxxRxxx.Fxxx-xxx.img.gz //Upgrade image

   4) Run the following command with root account to make a bootable SD card:

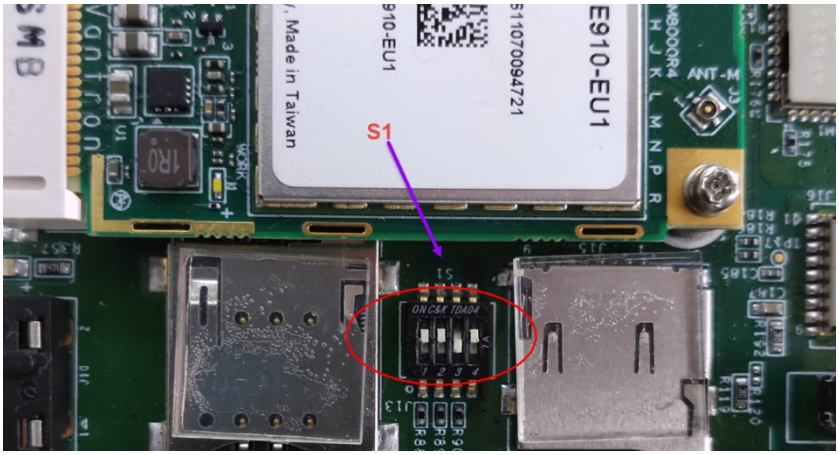
      sudo ./sd2emmc.sh /dev/sdb

- *Replace **/dev/sdb** with the correct SD card path.*
- *Removal of the SD card before a completion message pops up will cause the process to fail.*
- *Remove the SD card and run the command again in case the process fails.*

4. Insert the SD card to the slot;
5. Power the Gateway on. After the system boots up, the buzzer will sound for 10 seconds at intervals of 200ms and eMMC flashing finishes.

1.12.2 System boot from eMMC flash

1. Open the Gateway box;
2. Set DIP switch S1 to on:on:off:on as shown below;



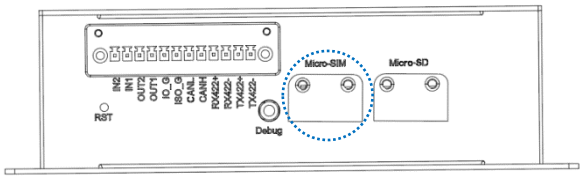
3. Power the Gateway on. After the system boots up from eMMC, the buzzer will sound for 1 second.

CHAPTER 2 GETTING STARTED

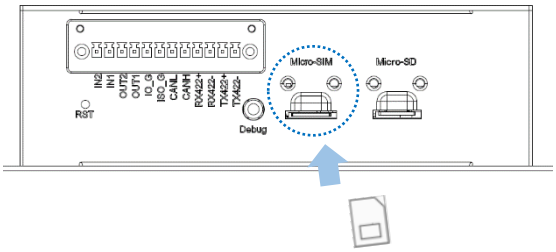
2.1 Setting up the Gateway

Before you proceed with the configuration of the Gateway, follow the steps below to finish hardware connection.

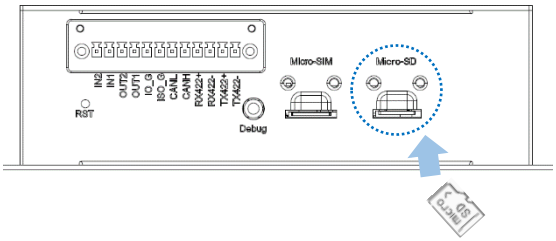
1. Use the mounting bracket and screws to install the Gateway to a secure place;
2. Use a screwdriver to unscrew the SIM card door;



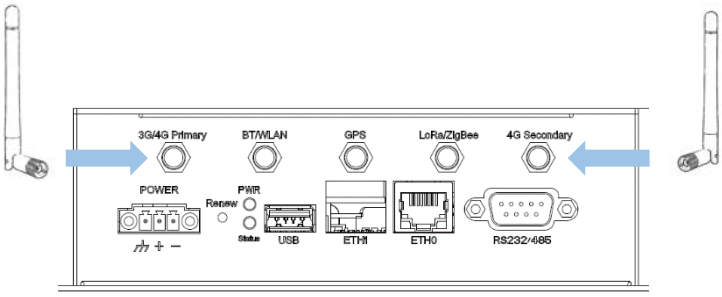
3. Insert an activated Micro SIM card into the slot with the gold-colored contacts facing down;



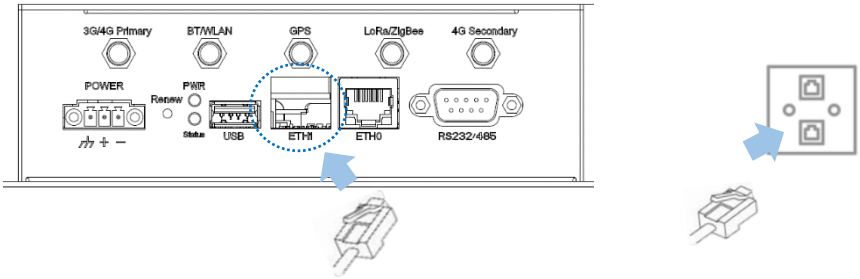
4. Push the Micro SIM card until it clicks into place;
5. Place the SIM card door back and tighten it with the screwdriver;
6. Unscrew the SD card door likewise;
7. Insert a Micro SD card, if any, with the gold-colored pins facing down, then place the door back and tighten it likewise;



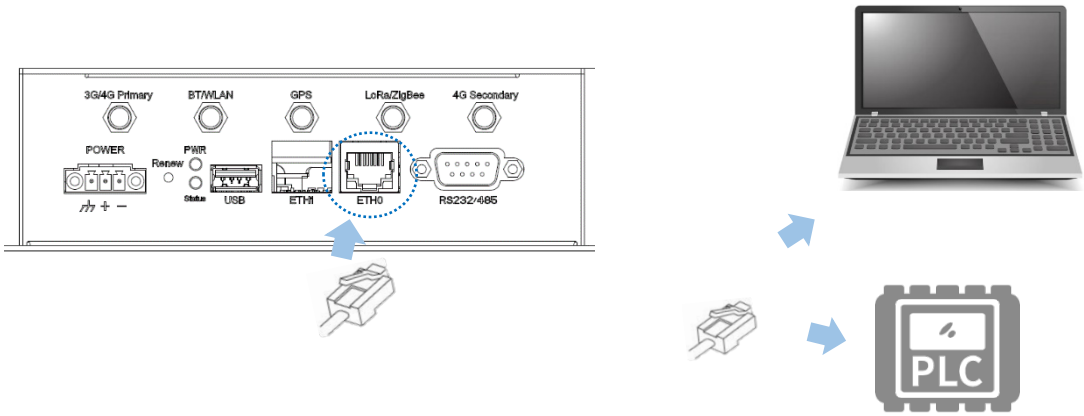
8. Install the antennas to the antenna connectors and tighten the connectors;



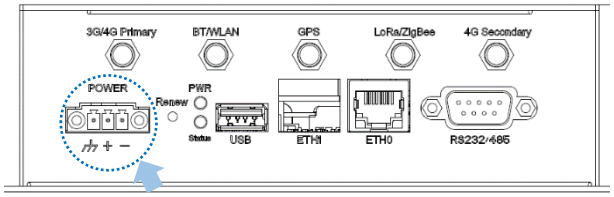
9. Connect one end of an Ethernet cable to ETH1 (WAN port) of the Gateway and the other to a live Ethernet port;

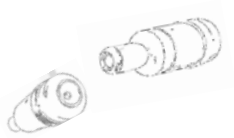


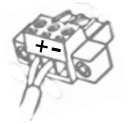
10. Connect one end of an Ethernet cable to ETH0 (LAN port) of the Gateway and the other to a host computer or client device depending on your use. In some cases, the ports on the Gateway are marked as ETH1 and ETH2, functioning the same as ETH1 and ETH0, respectively;



11. Connect the terminal end of the female DC power connector to the power terminal of the Gateway and the round end to the adapter;







If you are using the power connector supplied by Vantron:
Red wire: PWR (+)
Black wire: GND (-)

12. Plug the adapter to a DC power outlet that meets the supply voltage requirement (6V to 36V) to turn on the Gateway;
13. There will be a beep, and the power and status indicators will turn solid green upon power application.

Skip steps 9 & 10 if you choose wireless network connection.

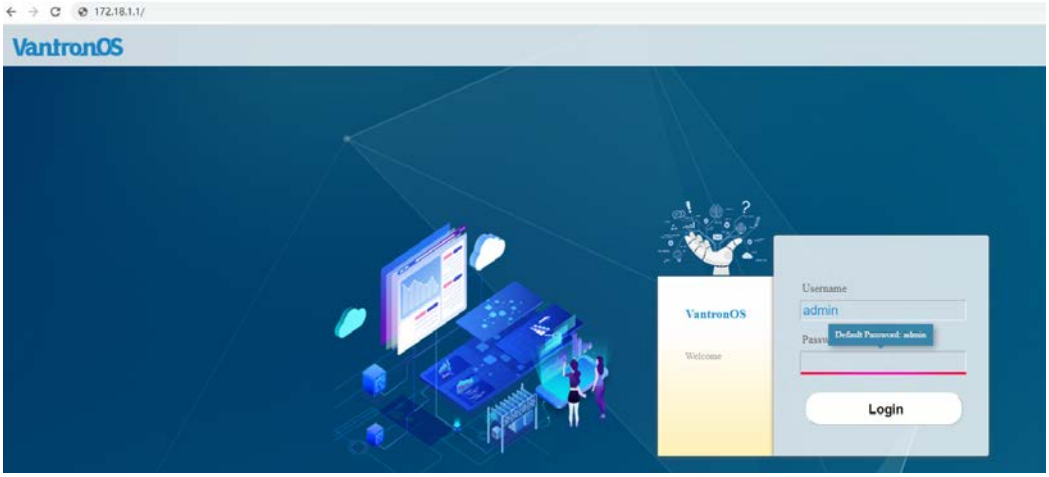
The antennas might be different from what used for illustration here. Should you have any trouble installing the antennas, please contact the sales executive for solution.

Customers have the option for a 4G/LTE module that is AT&T and Verizon pre-certified. Before you use a SIM card to provide wireless network access for the Gateway, make sure the SIM card is activated with data plans (refer to 3.6.3 4G/LTE for the application of the SIM card from the carriers if the module is pre-certified).

2.2 VantronOS Login

The Gateway is designed to allow network connectivity with minimal configuration. That said, you can configure the network settings and customize the Gateway from VantronOS interface.

1. Input the LAN port IP of the Gateway in your browser to log in the VantronOS web interface (default: http://172.18.1.1/):
   - Default user: **admin** / Super user: **root**
   - Default password: **admin** / Super user password: **rootpassword**



2. For SSH login, use the LAN port IP address (default: http://172.18.1.1/).
   - Port: **22**
   - Account: **root**
   - Password: **rootpassword**

Since The web login address coincides with the LAN port IP address of the Gateway, you might have to change the login address when you reset the IP address.

*SSH login is disabled by default, refer to **SSH Access** included in 3.13.3 for more details.*

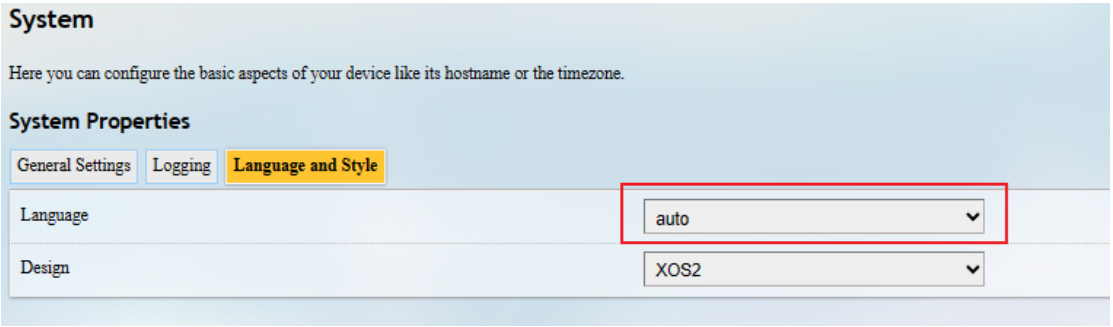
2.3 Password Change

It is up to you to decide whether you would like to change the login password after logging in VantronOS.

1. Navigate to **System > Administration**;
2. Input the original password for the current user;
3. Input a new password and confirm the password;
4. Save the settings and apply;
5. The system will log out automatically;
6. Log in with the new password.

2.4 Language Change

Currently the system supports simplified Chinese and English. The system language is set to automatically follow your browser language by default. You can change the system language by navigating to **System > System > Language and Style**.



Auto: System language based on the browser language (default)

English: English interface

Simplified Chinese: Simplified Chinese interface

2.5 Interfacing with Vantron Gateway Management Platform

BlueSphere Gateway Management Platform ("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.

Before you can use the BlueSphere GWM for remote management of Vantron IoT devices, please make sure the following prerequisites are met:

- You have obtained a license for login to the BlueSphere GWM
- The DMP agent is installed on the device for remote management
- The DMP agent is “enabled” (Refer to 3.10.4 DMP Agent for the configuration)
- The serial number of the device is added to the BlueSphere GWM

CHAPTER 3 GATEWAY SETUP VIA VANTRONOS

3.1 Introduction to VantronOS

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

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

In the following sections, should you find any features not displayed in the VantronOS interface as an 'admin' user, please log in with the root account.

Make sure to save all settings and changes before exit to let them take effect.

3.2 Status

This page provides the overall information of the Gateway, including stable operation duration, number of devices connected to the Gateway via wireless or Ethernet connection, default routing, hardware information, traffic statistics, etc.

Description of the numbered areas

1. Firmware version and auto refresh on/off (click to switch the mode)
2. Stable running duration of the Gateway since network connection
3. Current working status of Ethernet ports

   (LAN and WAN ports are connected in this case)
4. A collection of network diagnostic tools (refer to 3.7 for details)
5. Instant outbound traffic

6. The model, serial number, and IP address of the gateway in use
7. System log information
8. Kernel log information
9. Number of clients connected to the Gateway via Wi-Fi

You will access Wi-Fi settings upon a click of the number.

10. Address information of clients connected to the Gateway via Ethernet

IPv4 地址	MAC 地址
172.18.1.174	18:c0:4d:43:ad:8b

11. Details of the gateway connectivity

The image illustration varies when the Gateway has cellular connection.

12. Default route currently used by the Gateway
13. Select a period for the data to display
14. Traffic distribution of clients connected to the Gateway displayed by MAC addresses

Clicking on each MAC address in the table at the page bottom will get the detailed traffic information of the clients.

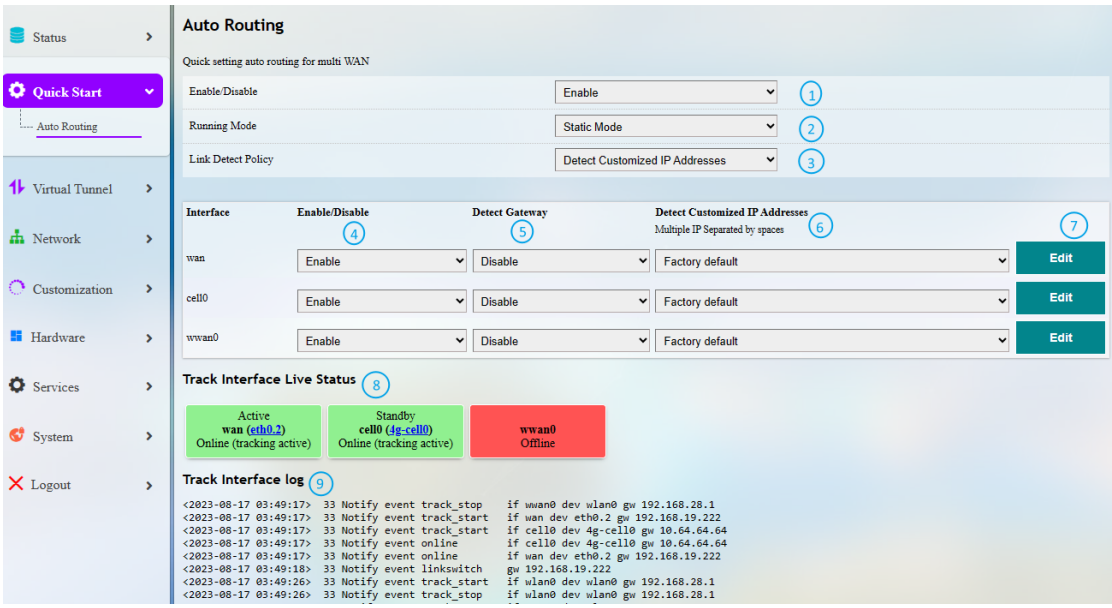
15. Traffic of application layer protocols

HTTPS, HTTP, and POP3S represent the top 3 protocols for data download and upload. HTTPS, HTTP and DNS represent the top 3 protocols for device connection.

3.3 Quick Start— Auto Routing

Automatic routing ensures that the Gateway maintains Internet access when multiple links are available. It features automatic link detection, automatic route switching, and recovery.

The default link detection and data forwarding are prioritized based on the following rule: Ethernet > Wi-Fi > LTE > others.



Description of the numbered areas

1. Enable/Disable route tracking
2. Mode of the automatic routing (refer to the details below)
3. Automatic link detection policy (refer to the details below)
4. Enable/Disable link detection for a specific network interface

   In the screenshot above, wan stands for Ethernet connection, cell0 for cellular connection, and wwan0 for Wi-Fi connection.

5. Enable/Disable gateway detection
6. Customized IP address detection (heartbeat or gateway address)
7. Edit the auto routing rule of a specific network interface (refer to the details below)
8. Link status
9. Link detection log and service running log

Mode of the automatic routing

Mode	Description
Static mode (Default)	1. The user-designated link priority takes precedence; 2. If the user does not designate the link priority, the default rule will apply.
Dynamic mode	1. The default rule governs the entire routing policy; 2. The user-designated link priority will be disabled. This is not recommended when special applications are installed on the Router that rely on the designated link priority.

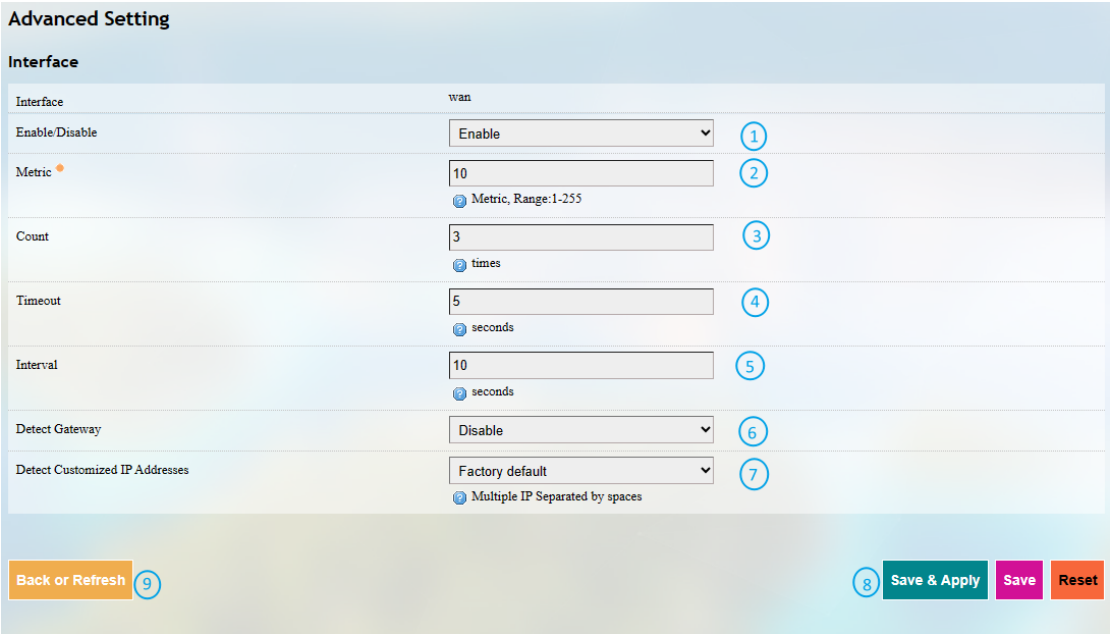
Automatic link detection policy

Policy	Description
Detect customized IP addresses (Default)	1. You can set IP addresses for a specific network interface. If these IP addresses have packets received and transmitted, the interface is active and set "Online"; 2. If the Router is located at a place without access to external network, please change the policy to "Detect gateway" or add some IP addresses that the Router can detect.
Detect gateway	This policy is to identify the IP address of the gateway on the current network. You are recommended not to apply this policy for P2P/PPP connection scenarios, in which circumstance, verifying the public network IP address (such as 8.8.8.8) is recommended.

Note:

1. Please choose an appropriate policy based on the device's network position and the network access protocol used by the network interface.
2. If you have configured for both "Detect customized IP addresses" and "Detect gateway", the gateway detection will take precedence.
3. If you have selected "Detect customized IP addresses" but have not provided any IP address, it will automatically switch to gateway detection.
4. Refer to the next page on editing the routing rules for more details.

Clicking on the **Edit** button behind the interface will direct you to the rule editing page as follows.



Description of the numbered areas

1. Enable/Disable route tracking
2. Select the interface for route tracking
3. Metric settings (The smaller the number, the higher the priority)
4. The maximum retry number for a single tracking failure
5. The maximum timeout for a single tracking failure
6. Number of online interfaces

If a tracking is confirmed successful, the interface will be considered online.

7. Number of offline interfaces

If a tracking is confirmed failed and the confirmation number reaches/exceeds the pre-set value, the interface will be considered offline.

8. Tracking interval, defined as from the completion of one tracking to the initiation of the next tracking
9. Traceable IP (heartbeat server)

Use spaces to separate multiple IP addresses. If you do not have internet access or private network, set the traceable IP to that of the upper layer gateway.

10. **Save & Apply** the settings

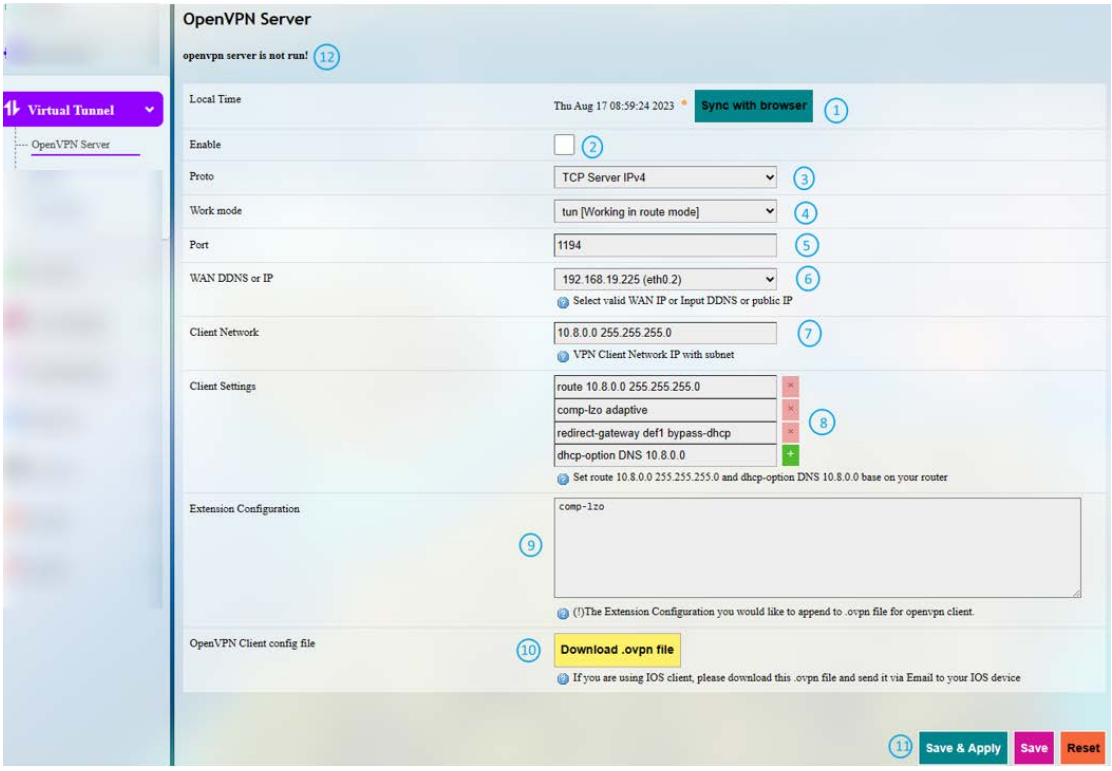
3.4 Virtual Tunnel

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

You can configure the Gateway either as an OpenVPN server or an OpenVPN client based on needs.

3.4.1 OpenVPN Server

Basic and advanced settings for OpenVPN server are accessible on this page.



Follow the steps below to build an OpenVPN Server:

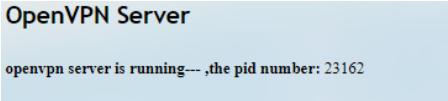
1. Synchronize the Gateway time with the browser (local) time;
2. Enable the server or not after the server is built;
3. Select a protocol (TCP by default);

TCP provides an ordered delivery of data from user to server (and vice versa), whereas UDP is not dedicated to end-to-end communications, nor does it check the readiness of the receiver.

4. Select a working mode between **tap** and **tun** (tun by default);

> ***Tap*** *bridges two ethernet segments at different locations, so use* ***tap*** *if you need to connect to remote network (remote desktops, PLCs, controllers, etc.). If you only need network connection, then use* ***tun****.*

5. Set a port that the server is to monitor;
6. Choose the WAN port IP or DDNS or public IP that the server is to monitor;
7. Assign a virtual IP network for the clients;
8. The basic configurations sent to the clients (not applicable to the tap working mode);
9. The extension configurations sent to the clients;
10. Download the configuration file for client connection (not necessary for server setup);
11. Save the above settings and apply;
12. Status of the OpenVPN server after the setup.



Advanced Setting allows you to set the authentication method, certificate authentication options, and renew the system certificate.

Run Log displays the details after the server setup.

3.4.2 VPN Client

To connect the Gateway to a VPN server and use it as a client, navigate to **Virtual Tunnel > VPN Client** for specific settings.

Description of the numbered areas

1. Synchronize your VPN time with the browser (local) time
2. Select a WAN protocol for the virtual line (OPENVPN & PPTP available)
3. Click to switch to the protocol
4. Check or uncheck the box to enable/disable the protocol

Only when the protocol is enabled will subsequent options be displayed. The subsequent options correspond to the type of WAN protocol selected.

5. If you select OpenVPN as the WAN protocol, you'll have to continue with the configuration using a .ovpn file

If you select PPTP as the WAN protocol, you shall input the PPTP server IP, user name and password as indicated.

6. Select the .ovpn file from the local directory for configuration
7. Upload the local profile
8. Select to use a certification or username & password for the authentication

The mode will update automatically, leave it as is.

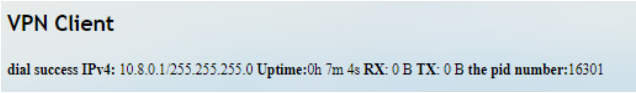
9. Set the MTU
10. Set the gateway metric (between 1 and 255)

The smaller the number, the higher the priority.

11. Disable/Enable heartbeat detection

*Select **custom** and enter the IP address for heartbeat detection to enable the mechanism.*

12. Enter a custom DNS Server
13. **Save & Apply** the settings
14. Status of the VPN client after the setup



3.5 IPSec Connection

3.5.1 Prerequisites

- A G335 edge computing gateway ('G1' for short)
- A supporting device (gateway/router) that runs on VantronOS and supports IPSec ('G2' for short)
- Certificates for G335 and the supporting device:

1. Assume that the IP addresses of the G1 and G2 are as follows:

   G1— LAN IP: 172.18.2.1, WAN IP: 192.168.9.78

   G2— LAN IP: 172.18.3.1, WAN IP: 192.168.9.82

2. Assume the certificates of the two devices are as follows:

   G1—

   X509 root certificate: rootca.cert

   X509 certificate: 78.cert

   Private key: 78.priv.key

   Public key: 78.pub.key

   G2—

   X509 root certificate: rootca.cert

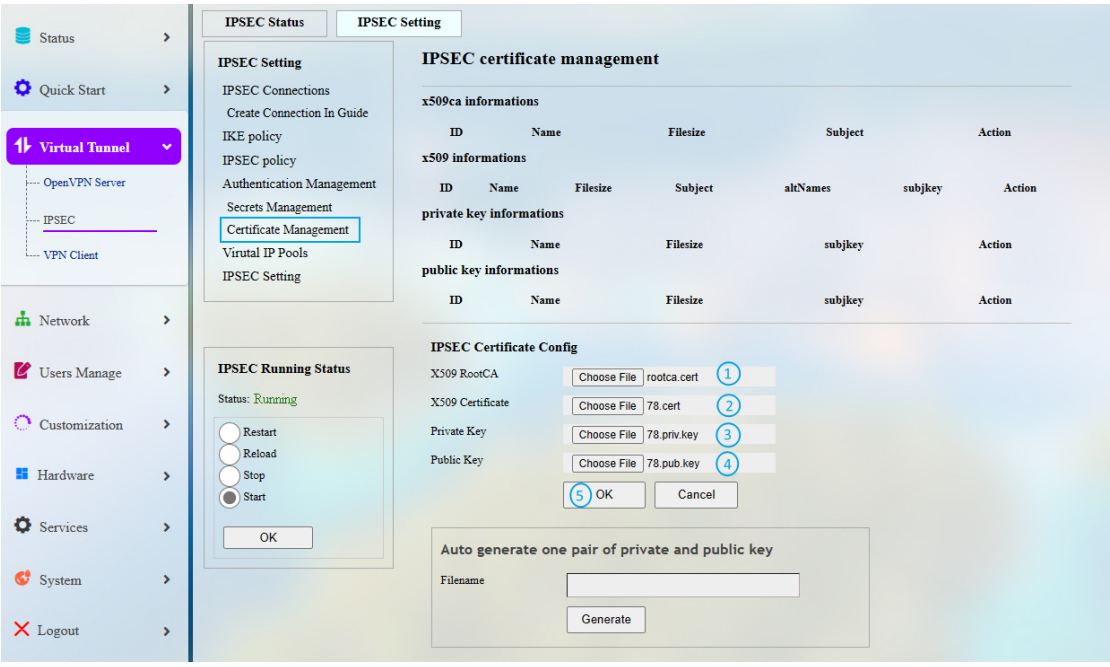
   X509 certificate: 82.cert

   Private key: 82.priv.key

   Public key: 82.pub.key

3.5.2 Certificate Setup

- Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Certificate Management** to upload the certificates (take G1 as an example):

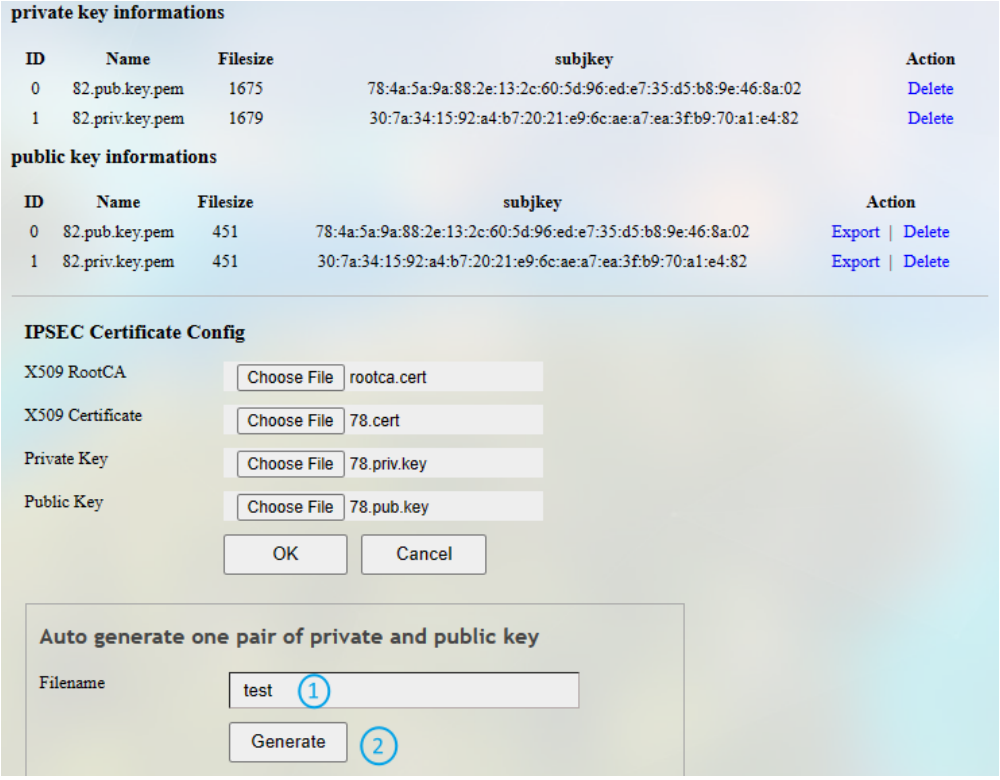


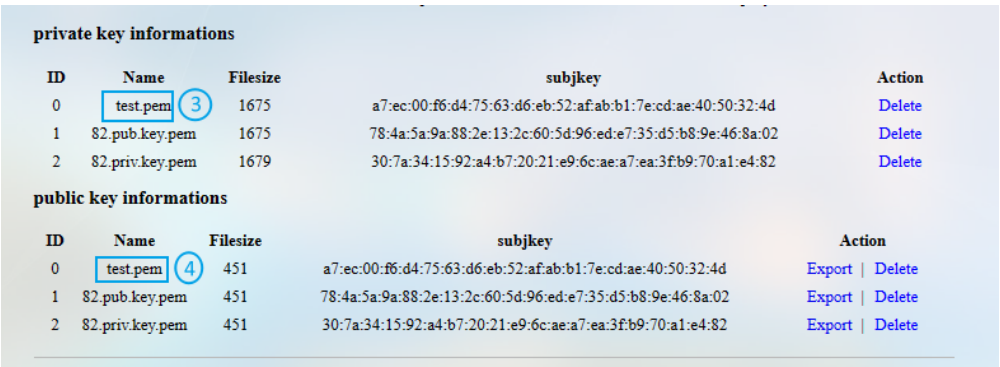
Follow the steps below to upload the certificates.

1. Select the X509 root certificate;
2. Select the X509 certificate;
3. Select the private key;
4. Select the public key;
5. Click **OK** to upload the certificates for G1.

The above screenshot only illustrates how to upload the certificates for G1. Please follow the same way to upload the certificates for G2.

You can use the tool located at the bottom of the page to generate a pair of private and public keys, which, however, can only be used as public key authentication.





Description of the numbered areas

1. Input a file name for the keys
2. Click **Generate** to generate the keys
3. Newly generated private key
4. Newly generated public key

3.5.3 Secret Setup

This configuration only applies when pre-shared key (PSK) is selected as the secret type.

- Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Secretes Management** to configure a local secret (take G1 as an example):

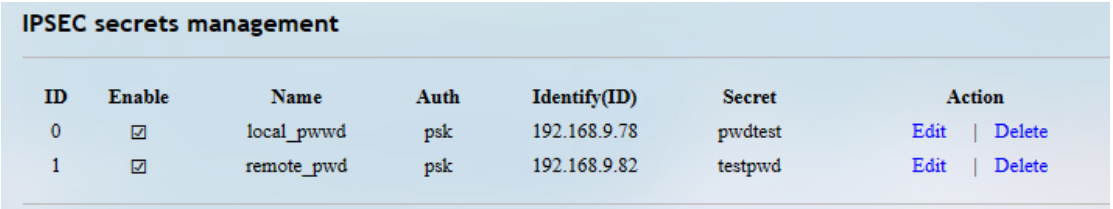
Follow the steps below to set a local secret**.**

1. Assign a name for the secrete;
2. Select **Enabled** from the dropdown list to enable the secret;
3. Select **PSK** as the secret type;
4. Input the PSK ID: 192.168.9.78 (WAN IP of G1);
5. Input a password;
6. Click **OK** to save the secret.

- Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Secretes Management** to configure a remote secret (take G1 as an example):

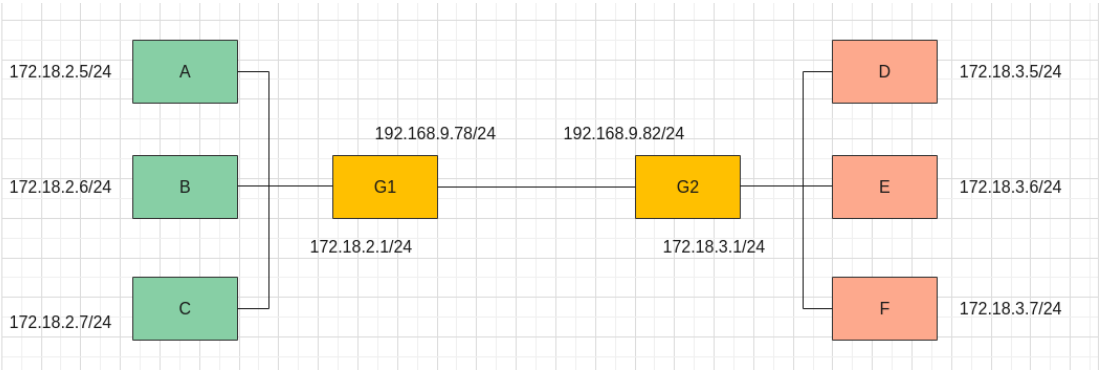
Follow the steps below to set a remote secret**.**

1. Assign a name for the secrete;
2. Select **Enabled** from the dropdown list to enable the secret;
3. Select **PSK** as the secret type;
4. Input the PSK ID: 192.168.9.82 (WAN IP of G2);
5. Input a password;
6. Click **OK** to save the secret.



The local secret of G1 acts as the remote secret of G2, and the remote secret of G1 acts as the local secret of G2.

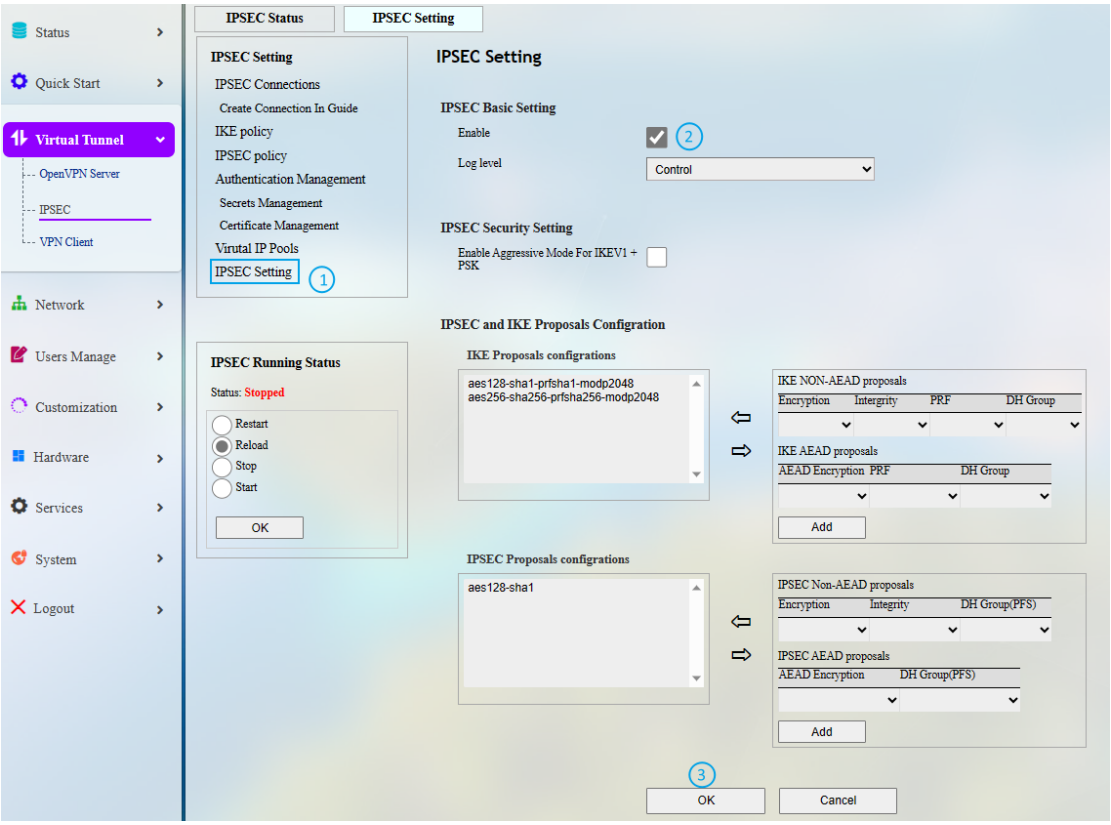
3.5.4 IPSec Connection Setup



Introduction to the above scenarios

- Scenario 1: Host-to-Host, G1 connects with G2 via IPSec, and subnets are not connected
- Scenario 2: Site-to-Site, G1 connects with G2 via IPSec, and subnets are connected
- Scenario 3: Remote access (Server), D connects to G1 via IPSec with access to subnets of G1
- Scenario 4: Remote access (Client), A connects to G2 via IPSec with access to subnets of G2

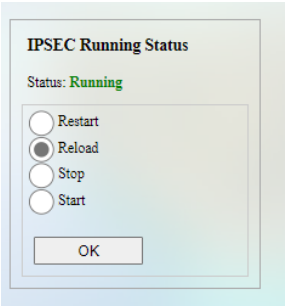
STEP 1: Enabling IPSec



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC Setting**
2. Enable IPSec settings
3. Click **OK** to save the setting

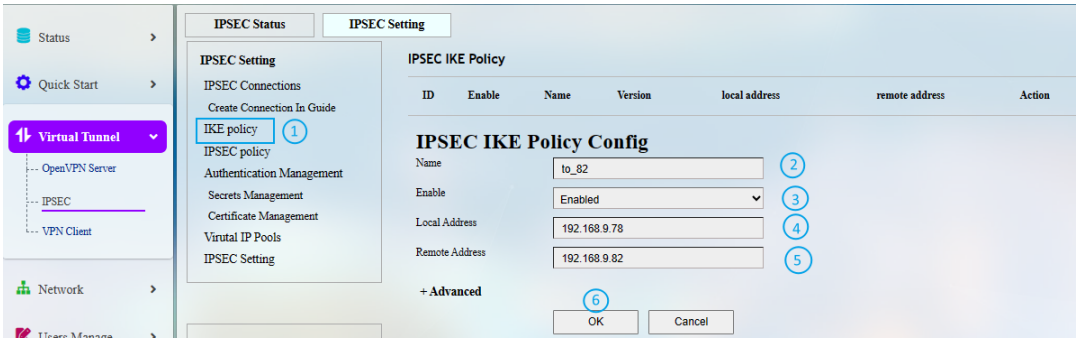
After the settings are loaded, the status of IPSec will change to 'running' as follows.



STEP 2: IKE policy configuration

Configurations for scenarios 1 and 2:

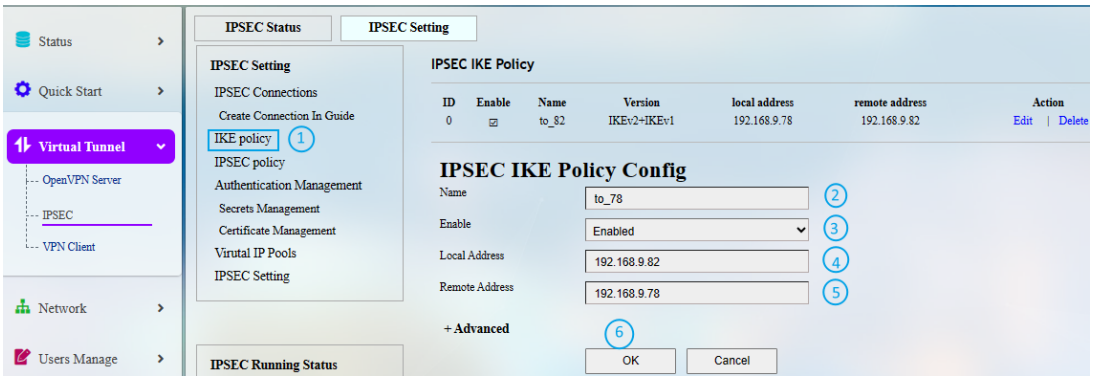
G1 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.78
5. Input the remote address: 192.168.9.82
6. Click **OK** to save the settings

G2 setup

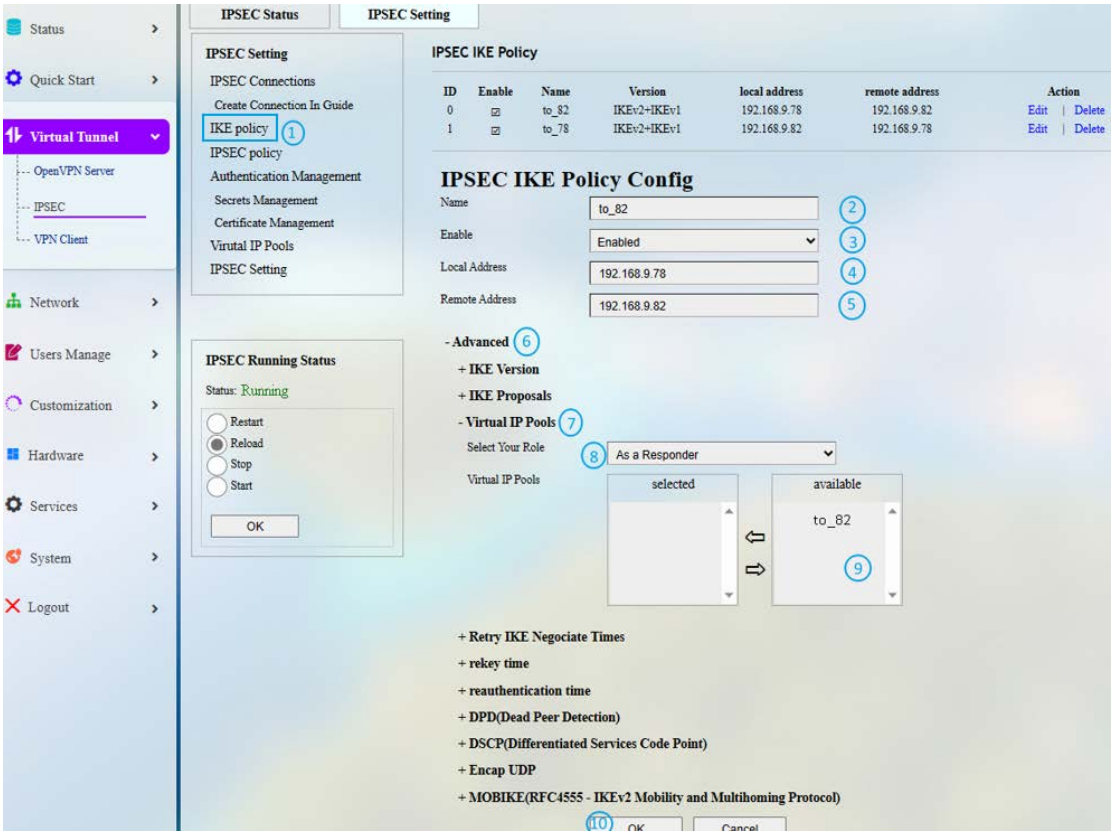


Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.82
5. Input the remote address: 192.168.9.78
6. Click **OK** to save the settings

Configurations for scenario 3 (swapping the configurations of G1 and G2 will get you the configurations for scenario 4):

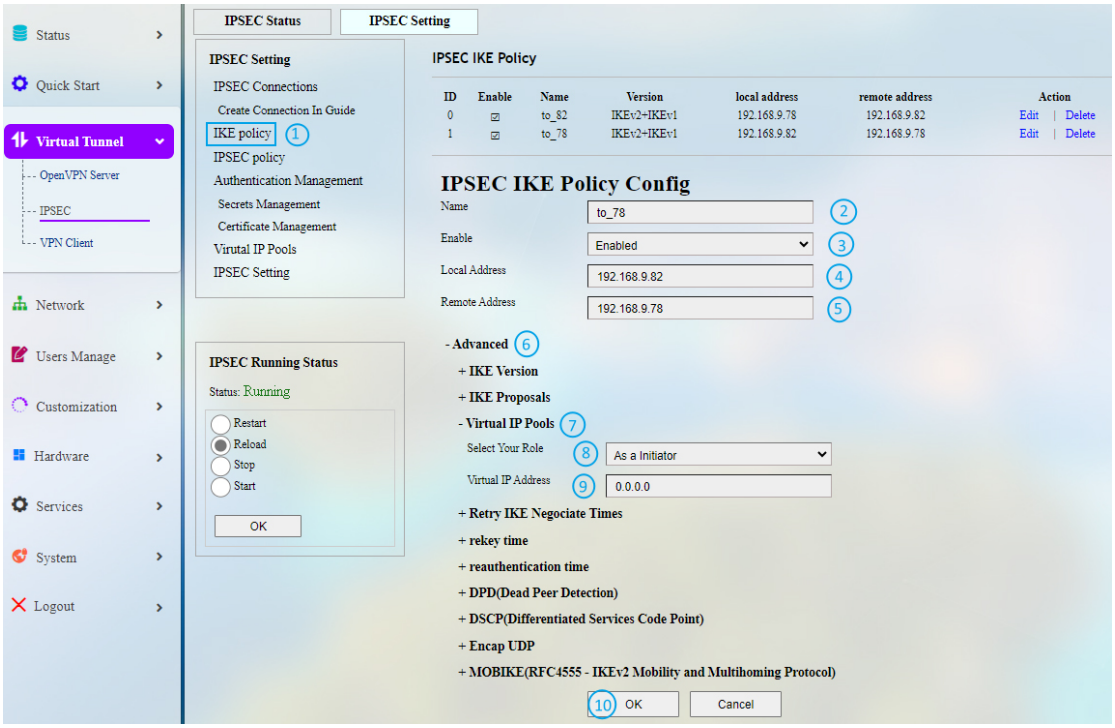
G1 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy (to_82)
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.78
5. Input the remote address: 192.168.9.82
6. Click **Advanced** to access the advanced settings
7. Click **Virtual IP Pools**
8. Select 'Responder' as the role of G1
9. Double click the available 'to_82' IP to select it
10. Click **OK** to save the settings

G2 setup



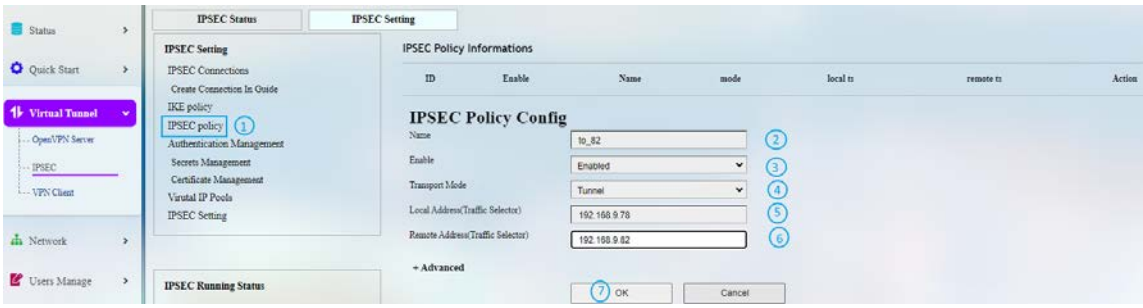
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IKE policy**
2. Assign a name to the policy (to_78)
3. Select **Enabled** from the dropdown list to enable the policy
4. Input the local address: 192.168.9.82
5. Input the remote address: 192.168.9.78
6. Click **Advanced** to access the advanced settings
7. Click **Virtual IP Pools**
8. Select 'Initiator' as the role of G2
9. Input a virtual IP (0.0.0.0)
10. Click **OK** to save the settings

STEP 3: IPSec policy configuration

Configurations for scenario 1:

G1 setup



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_82)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 192.168.9.78
6. Input the remote address: 192.168.9.82
7. Click **OK** to save the settings

G2 setup

Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_78)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 192.168.9.82
6. Input the remote address: 192.168.9.78
7. Click **OK** to save the settings

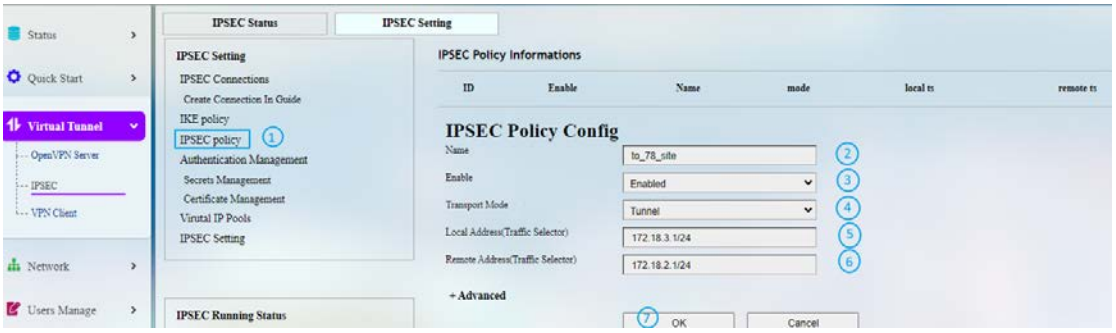
Configurations for scenario 2:

G1 setup

Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_82_site)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 172.18.2.1/24 (LAN IP of G1)
6. Input the remote address: 172.18.3.1/24 (LAN IP of G2)
7. Click **OK** to save the settings

G2 setup

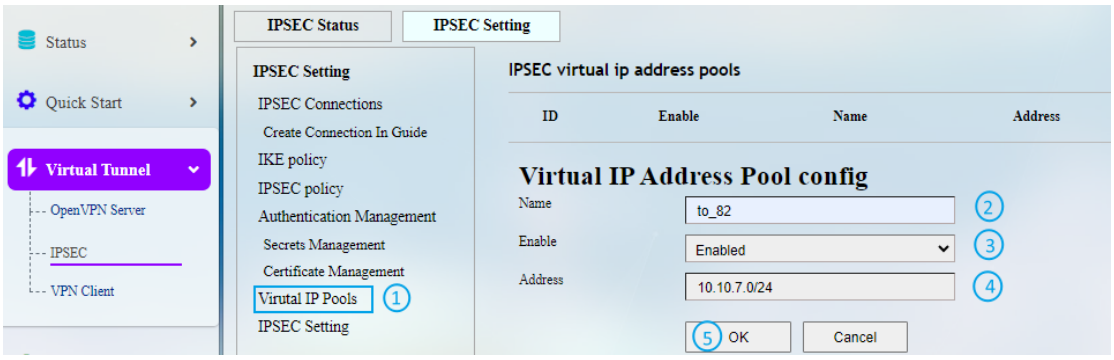


Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_78_site)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 172.18.3.1/24 (LAN IP of G2)
6. Input the remote address: 172.18.2.1/24 (LAN IP of G1)
7. Click **OK** to save the settings

Configurations for scenario 3 (swapping the configurations of G1 and G2 will get you the configurations for scenario 4):

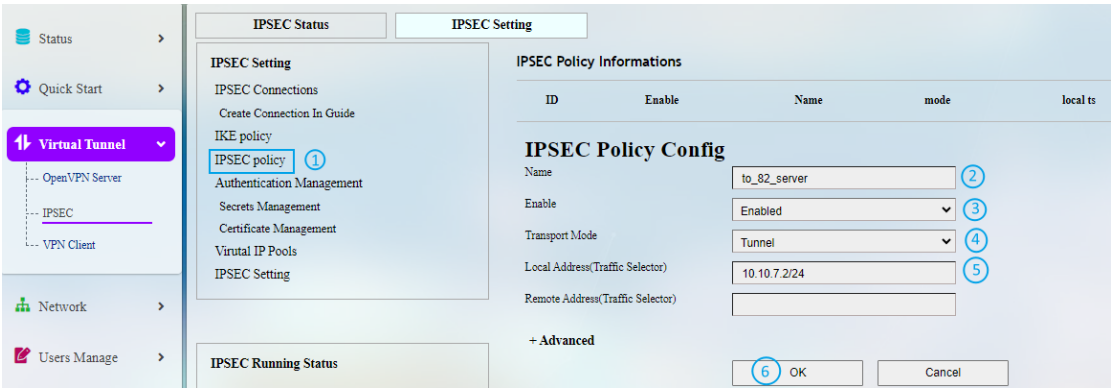
Virtual IP setup of G1



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Virtual IP Pools**
2. Assign a name to the policy (to_82)
3. Select **Enabled** from the dropdown list to enable the policy
4. Input a virtual address: 10.10.7.0/24
5. Click **OK** to save the settings

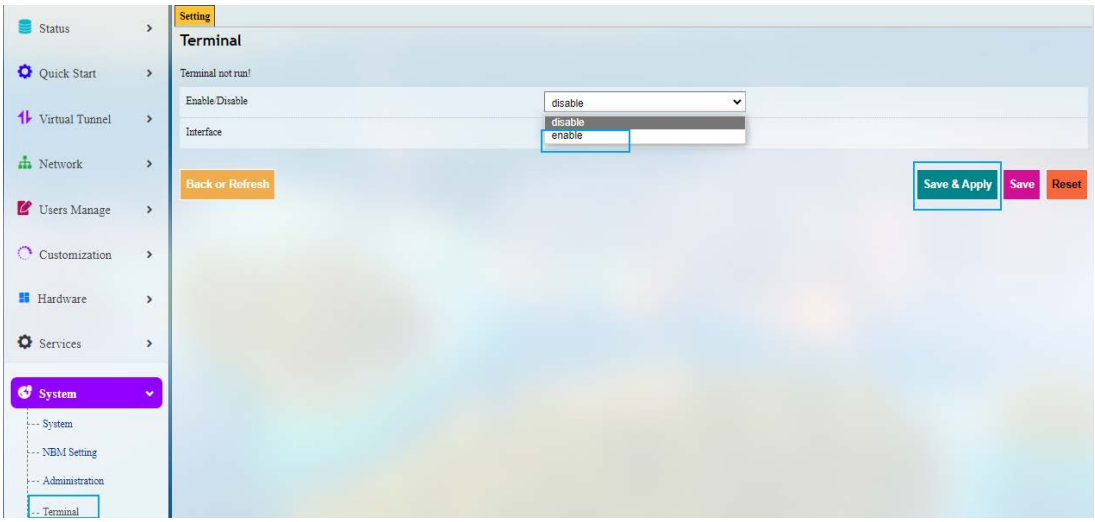
IPSec policy of G1



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSec policy**
2. Assign a name to the policy (to_82_server)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the local address: 10.10.7.0/24
6. Click **OK** to save the settings

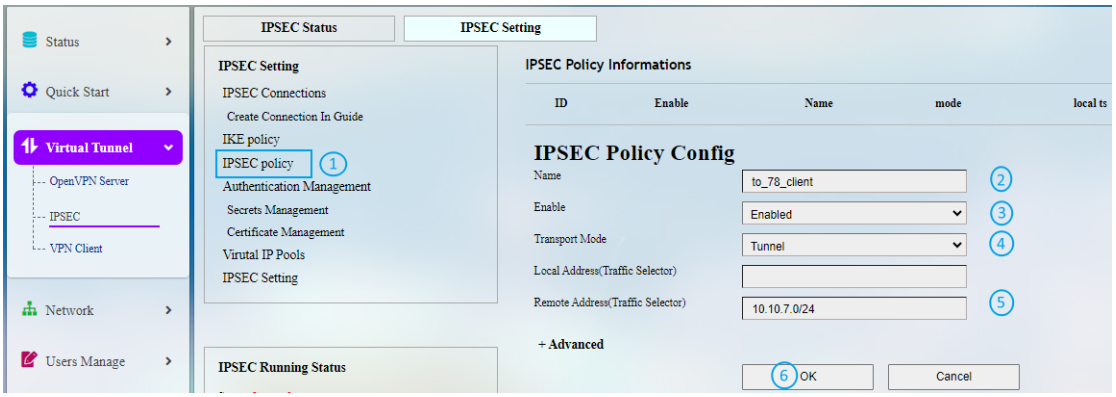
Navigate to **System > Terminal > Settings** to enable the terminal.



Log in with root account (default password: rootpassword), and input the following command to add the IP to G1.

```
ip address add 10.10.7.2/24 dev eth0
```

IPSec policy of G2



Description of the numbered areas

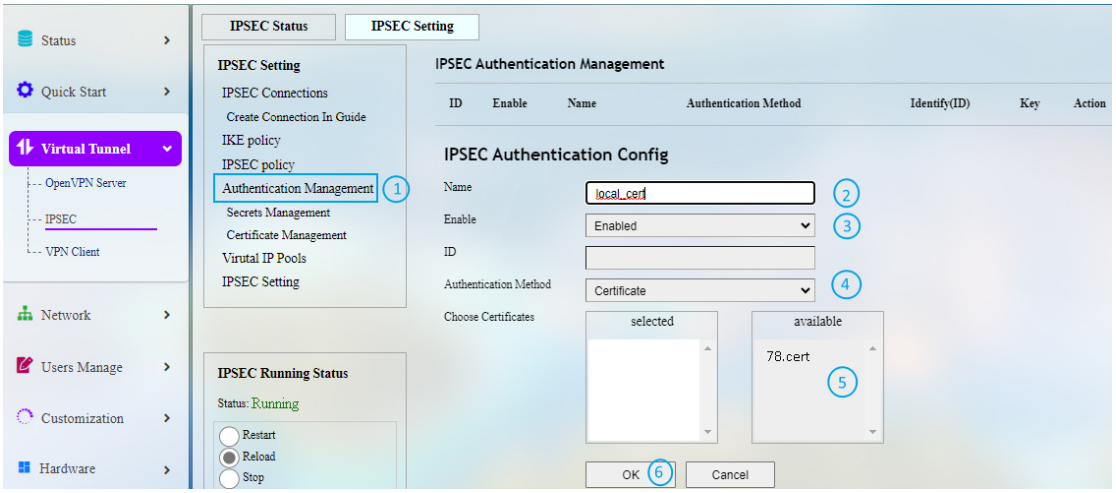
1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC policy**
2. Assign a name to the policy (to_78_client)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the remote address: 10.10.7.0/24
6. Click **OK** to save the settings

STEP 4: Authentication management

Three ways are available for the authentication: certificate, PSK, and public key.

Certificate authentication

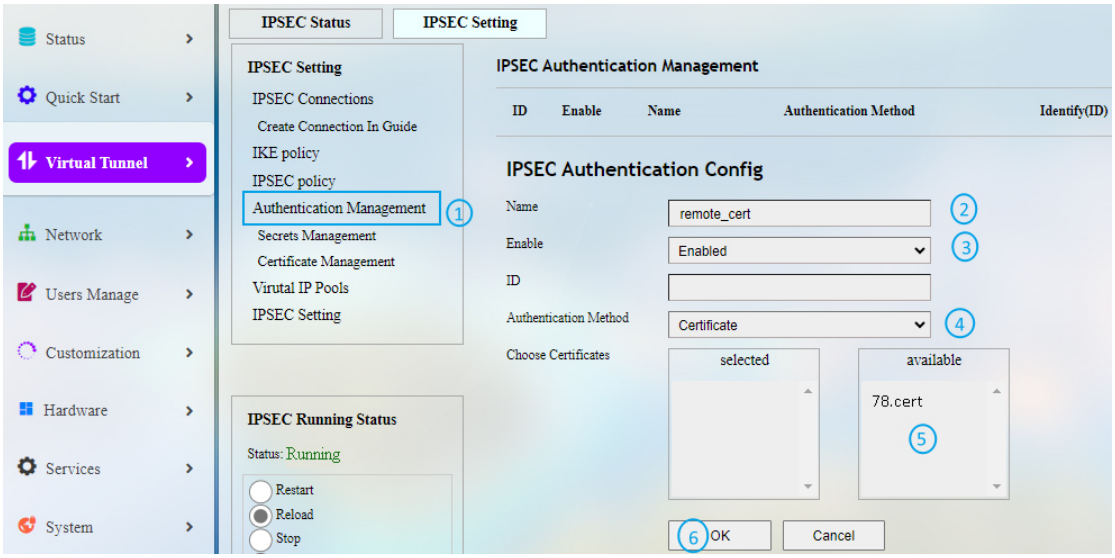
Configurations of G1 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available '78.cert' certificate to select it
6. Click **OK** to save the settings

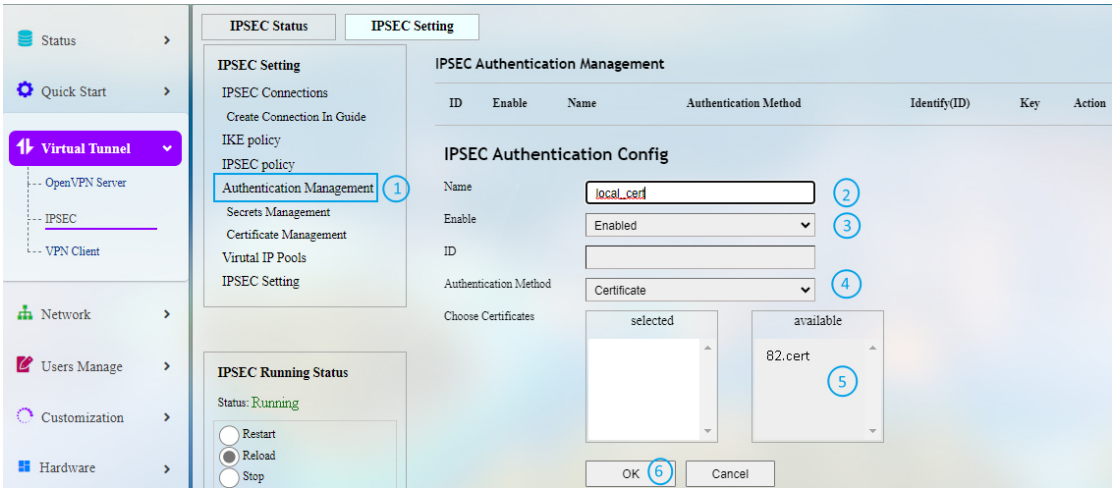
Configurations of G1 for remote authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available '78.cert' certificate to select it
6. Click **OK** to save the settings

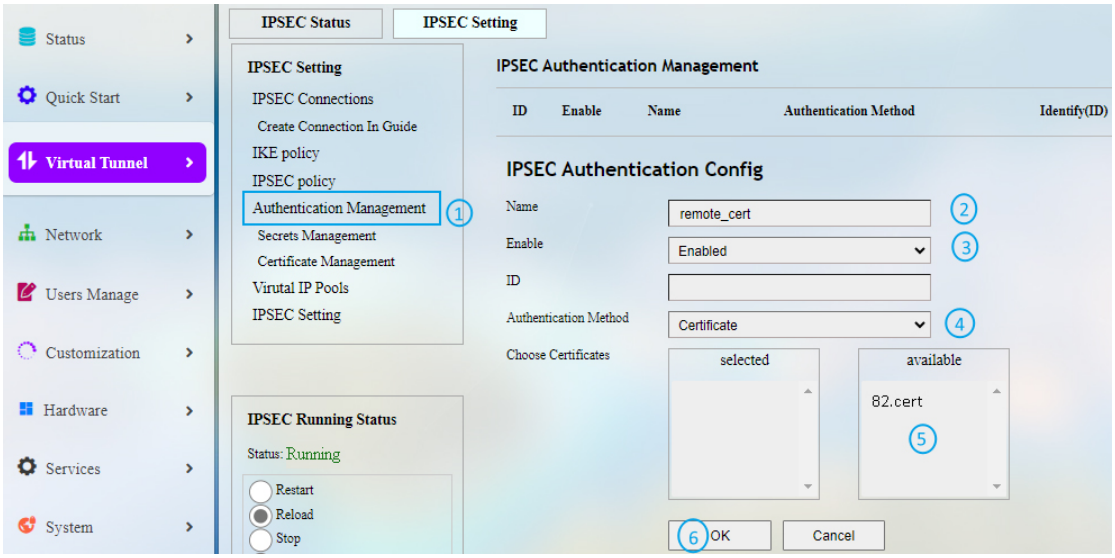
Configurations of G2 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available '82.cert' certificate to select it
6. Click **OK** to save the settings

Configurations of G2 for remote authentication

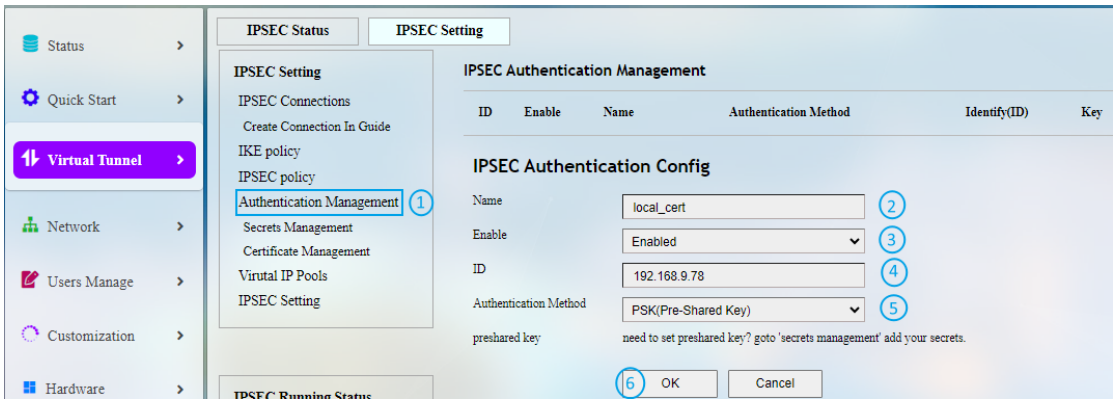


Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. **Certificate** is the default authentication method
5. Double click the available '82.cert' certificate to select it
6. Click **OK** to save the settings

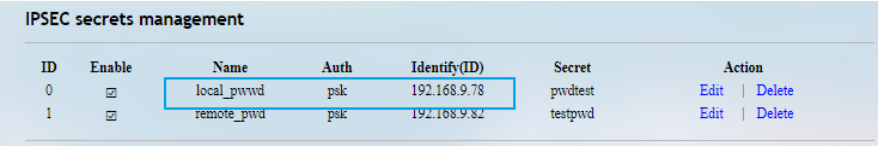
PSK authentication

Configurations of G1 for local authentication



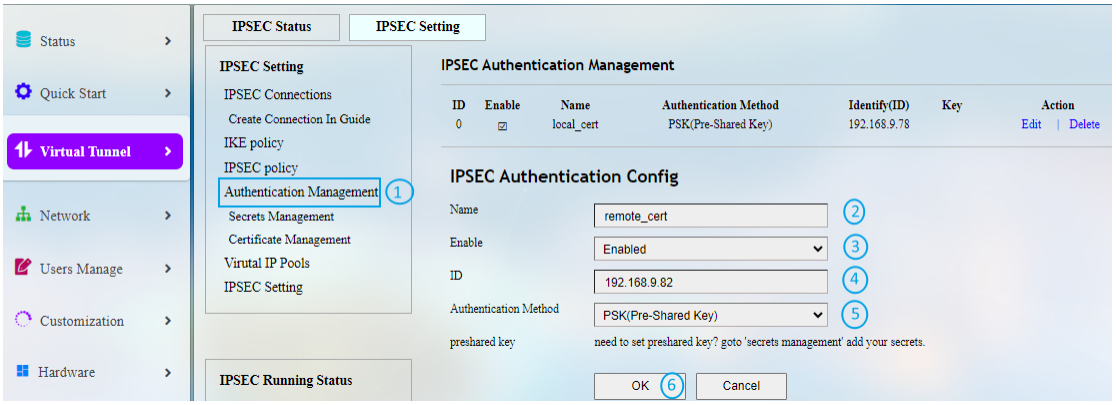
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.78)



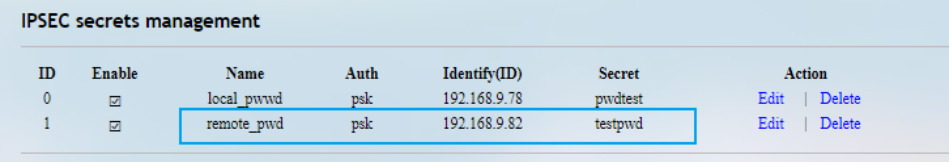
5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

Configurations of G1 for remote authentication



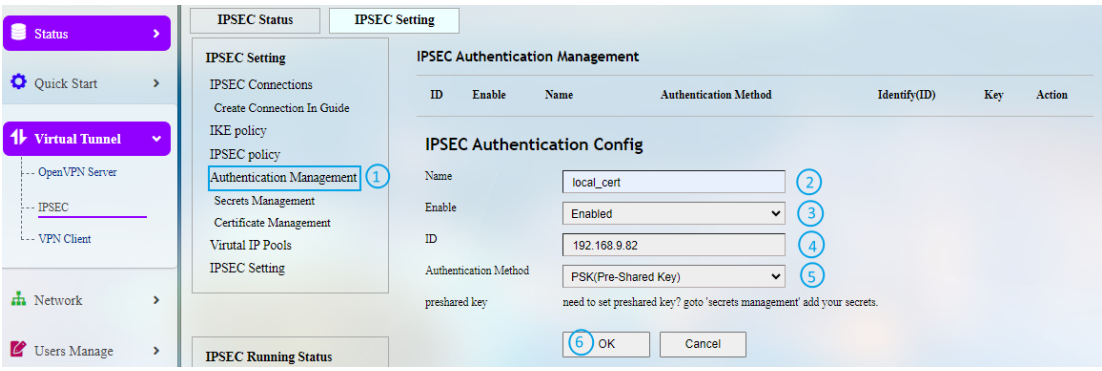
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.82)



5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

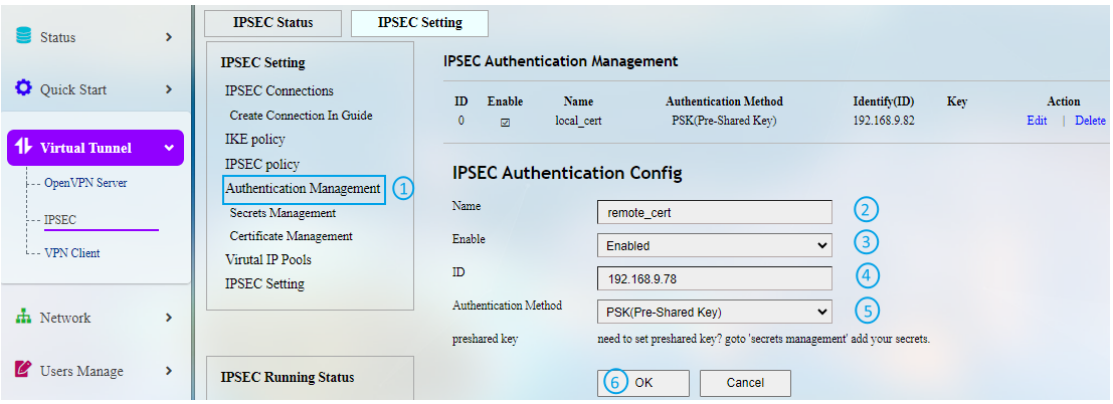
Configurations of G2 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.82)
5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

Configurations of G2 for remote authentication



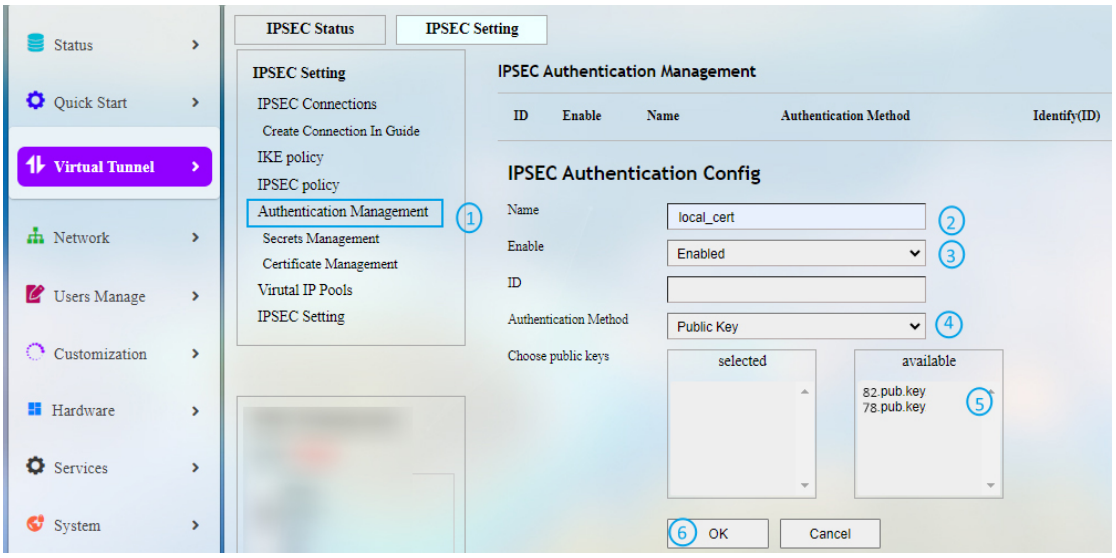
Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Input the ID same as that set in **Secret Management** (192.168.9.78)
5. Select **PSK (Pre-shared key)** from the drop-down list as the authentication method
6. Click **OK** to save the settings

Public key authentication

This authentication requires to upload the public key of G1 (78.pub.key) to G2 and upload the public key of G2 (82.pub.key) to G1.

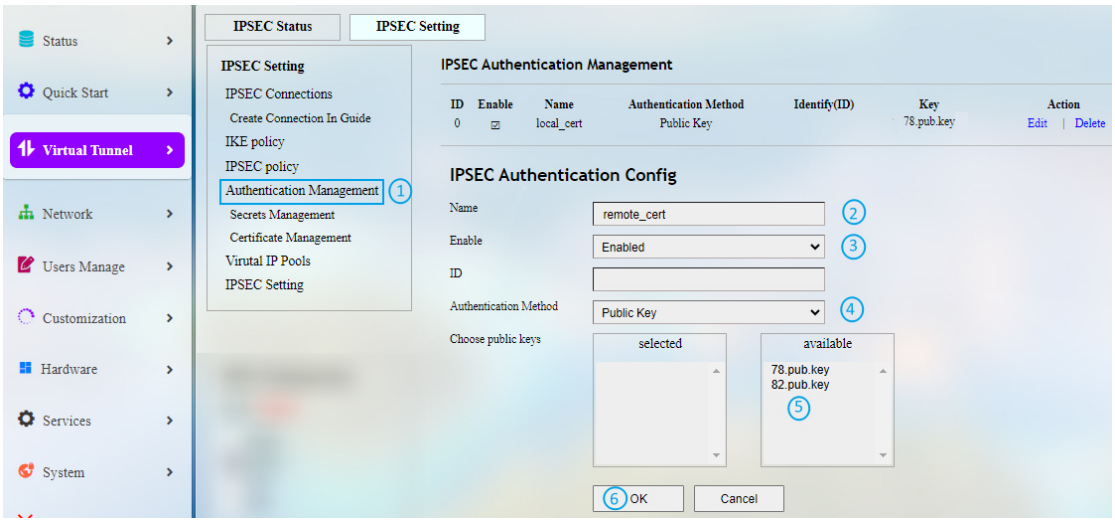
Configurations of G1 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select '78.pub.key'
6. Click **OK** to save the settings

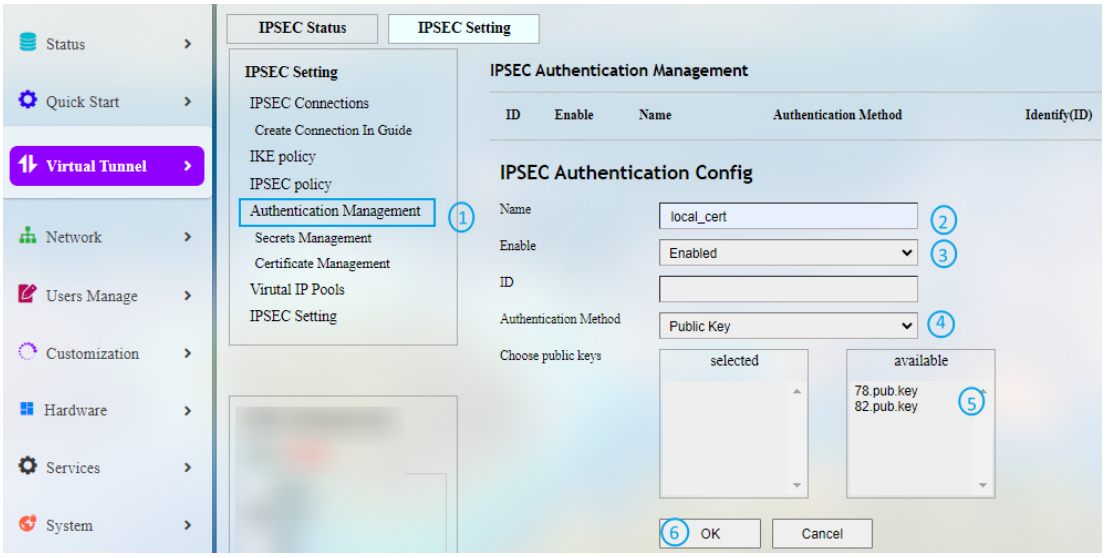
Configurations of G1 for remote authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select '82.pub.key'
6. Click **OK** to save the settings

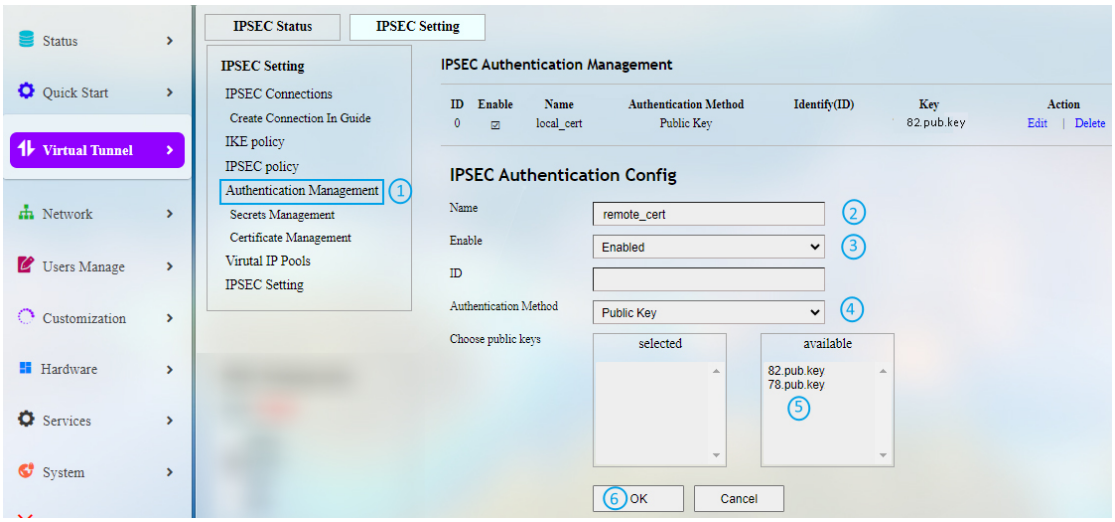
Configurations of G2 for local authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (local_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select '82.pub.key'
6. Click **OK** to save the settings

Configurations of G2 for remote authentication



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > Authentication Management**
2. Assign a name for the certificate (remote_cert)
3. The certificate is **Enabled** by default
4. Select **Public key** from the drop-down list as the authentication method
5. Double click to select '78.pub.key'
6. Click **OK** to save the settings

STEP 5: Configurations for IPSec connection

G1 setup

Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC Connection**
2. Assign a name for the connection (to_82)
3. The certificate is **Enabled** by default
4. Select a previously created IKE policy ('to_82' in this case) from the drop-down list
5. Double click a previously created local authentication policy ('local_cert' in this case) to select the policy
6. Double click a previously created remote authentication policy ('remote_cert' in this case) to select the policy
7. Double click a previously created IPSec policy ('to_82' in this case) to select the policy
8. Click **OK** to save the settings

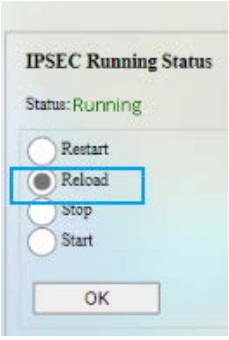
G2 setup

Description of the numbered areas

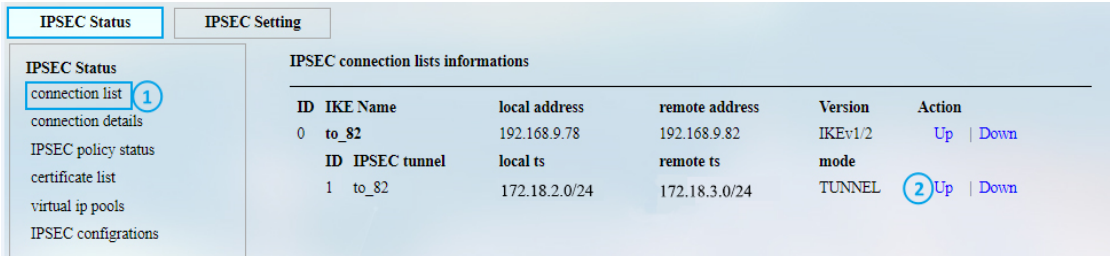
1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC Connection**
2. Assign a name for the connection (to_78)
3. The certificate is **Enabled** by default
4. Select a previously created IKE policy ('to_78' in this case) from the drop-down list
5. Double click a previously created local authentication policy ('local_cert' in this case) to select the policy
6. Double click a previously created remote authentication policy ('remote_cert' in this case) to select the policy
7. Double click a previously created IPSec policy ('to_78' in this case) to select the policy
8. Click **OK** to save the settings

STEP 6: Reloading the IPSec program

Click the radio button before **Reload** and then **OK** to reload the program.



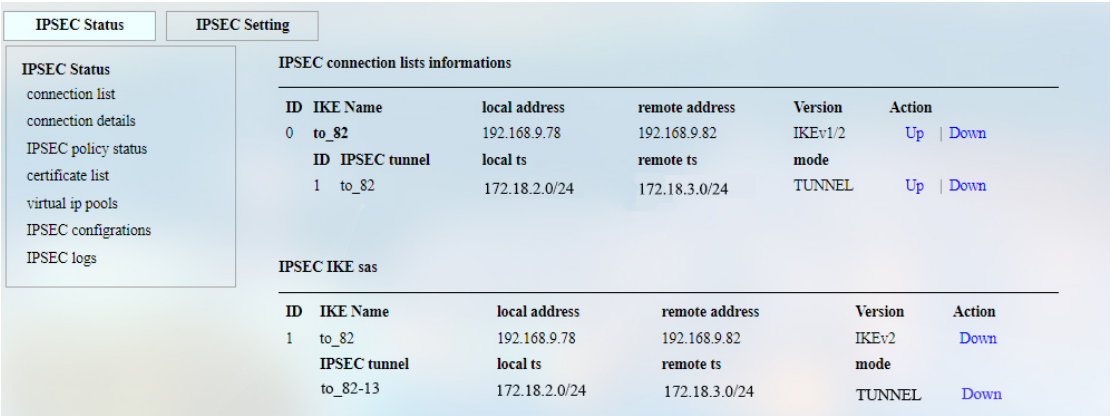
STEP 7: IPSec connection



Description of the numbered areas

1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Status> Connection list**
2. Select the connection setting and click **Up**

When the connection is added to **IPSEC IKE SAS**, the connection is established successfully.



3.6 Network

Users can change the settings related to the available network interfaces in the **Network** page.

3.6.1 Interfaces

All the network interfaces currently available and configurable are displayed under **Network > Interfaces**.

Description of the numbered areas

1. Interface overview
2. Interface traffic details
3. Restart the interface manually
4. Edit the interface settings
5. Delete the interface (available only when you log in as a root user)
6. Instantaneous traffic of the interface
7. Add a new interface (available only when you log in as a root user)

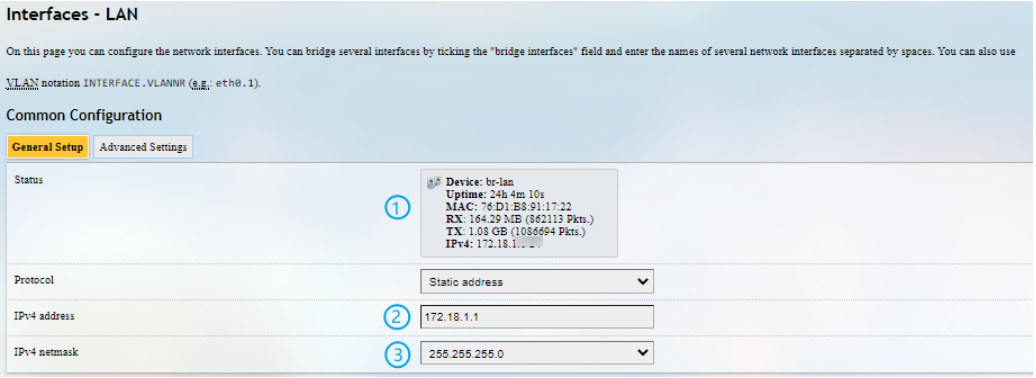
The interfaces may differ from what is shown above as certain interfaces are related to your prior settings and the communication modules available on the device.

The interfaces will be described in detail in the following sections.

3.6.1.1 LAN

- **Common Configurations**

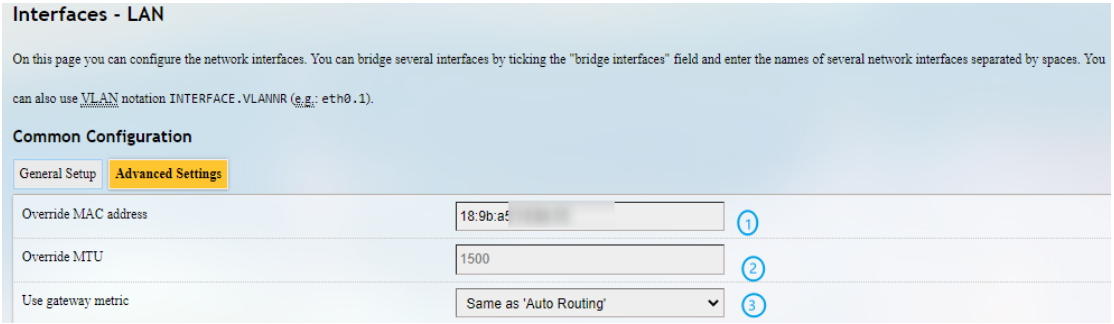
Clicking on the **Edit** button behind the **LAN** port will allow you to access the configurations of the LAN port, and **General Setup** is displayed by default.



Description of the numbered areas

1. Status of the interface
2. The IP address of the LAN port
3. The LAN port subnet mask

In the **Advanced Settings** next to the general setup:

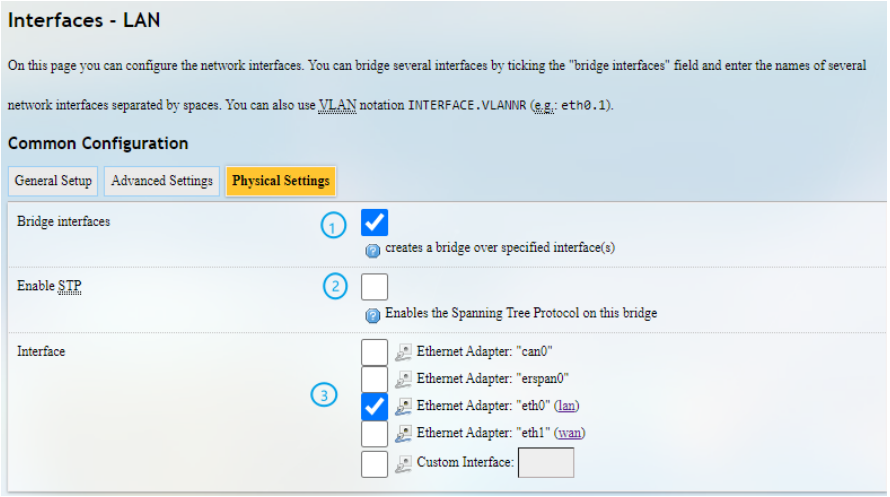


Description of the numbered areas

1. MAC address cloning
2. Set the MTU (keep the default setting)
3. Set a gateway metric (keep the default setting)

Be sure to save the settings before you exit the page.

There is a **Physical Settings** tab next to **Advanced settings** when you log in with the root account, allowing you to configure the LAN port for network bridge.



Description of the numbered areas

1. Enable the interface for network bridge
2. Enable STP protocol
3. Select the interface for bridge connection

Be sure to save the settings before you exit the page.

- **DHCP Server**

In the **General Setup** page of **DHCP Server**, DHCP could be set up with more details:

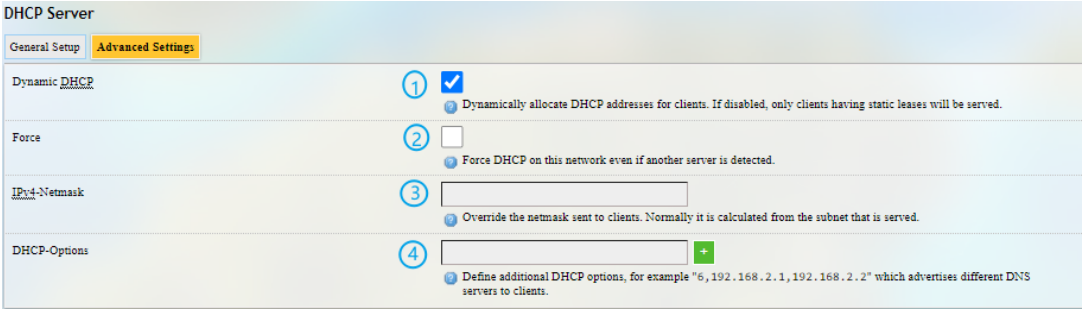
Description of the numbered areas

1. Disable the DHCP service

If disabled, DHCP service will not be available to the client devices connected to the LAN port of the Gateway.

2. DHCP start address
3. Maximum number of leased addresses (up to 150)
4. Expiry time of leased addresses (min. 2m)

Advanced Settings of DHCP Server:



Description of the numbered areas

1. Enable allocation of DHCP addresses for client devices
2. Force enablement of DHCP service (to bypass other servers)
3. Override the netmask sent to clients

Normally it is based on the subnet that is served.

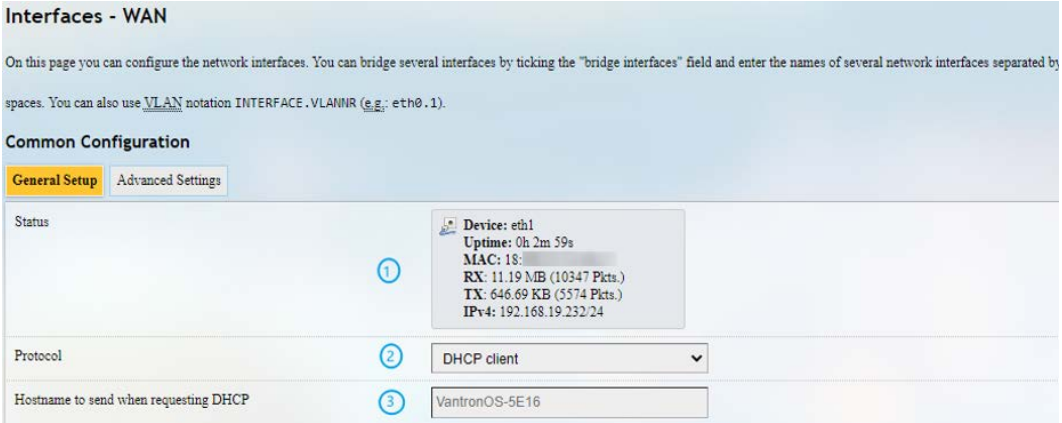
4. Add different DNS servers for client devices

*Be sure to save the settings before you exit the page. Clicking on **Back or Refresh** will get you back to the general information of the network interface.*

3.6.1.2 WAN

- **General DHCP settings**

Clicking on the **Edit** button behind the **WAN** port will allow you to access the configurations of the WAN port, and **General Setup** is displayed by default.



Description of the numbered areas

1. Status of the WAN port
2. Select DHCP client as WAN protocol
3. Hostname to send when requesting DHCP

Be sure to save the settings before you exit the page.

- **Advanced DHCP settings**

If you have selected DHCP client protocol, advanced settings are available after you have finished the setup as mention above.

Description of the numbered areas

1. Check the box to bring up the port upon device boot
2. Force link (once the box is checked, hotplug handlers will not be invoked after a link change)
3. Enable **Use default gateway**
4. Enable **Use DNS server advertised by peer**

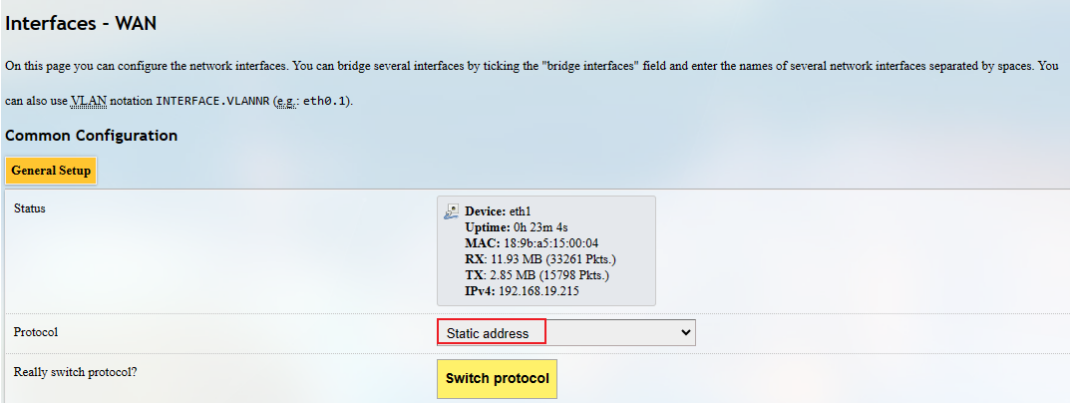
If this option is disabled, you will need to define a DNS server.

5. Set a gateway metric
6. MAC address cloning
7. Set the MTU

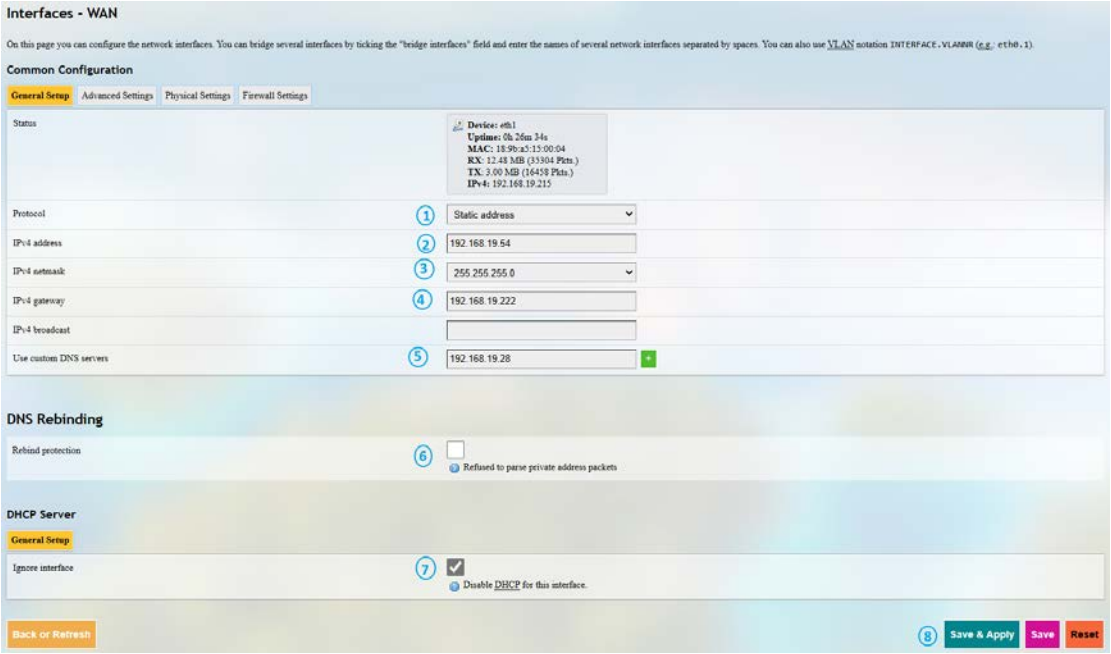
Be sure to save the settings before you exit the page.

- **General Static protocol settings**

To activate static address protocol, select **Static address** from the drop-down list in the **General Setup** page of the WAN port and click **Switch protocol**.



Upon click of **Switch protocol**, you'll need to input the IPv4 address, subnet mask, IPv4 gateway, and the IPv4 broadcast.



Description of the numbered areas

1. Current protocol
2. Input an IPv4 address
3. Input an IPv4 netmask
4. Input the IPv4 gateway
5. Set a custom DNS server (can be provided by the carrier or self-defined)

6. DNS re-binding protection (if enabled, parsing of private IP data will be refused)
7. Disable DHCP service (keep the default settings)
8. Save & apply the settings

Leave the field as is if not applicable.

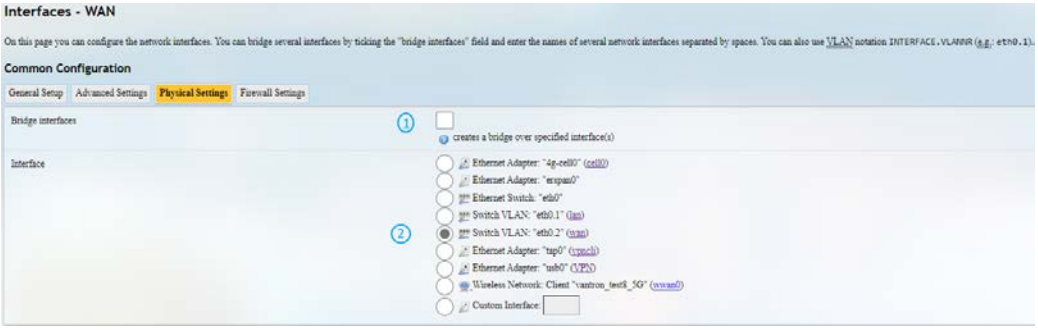
When static address protocol is selected, DHCP server will be automatically disabled.

The advanced settings are basically same as those for DHCP protocol.

Be sure to save the settings before you exit the page.

Other available WAN protocols include PPPoE, GRE tunnel over IPv4, and relay bridge. The settings are dependent on the specific protocols. Clicking on **Back or Refresh** allows you to return to interface settings.

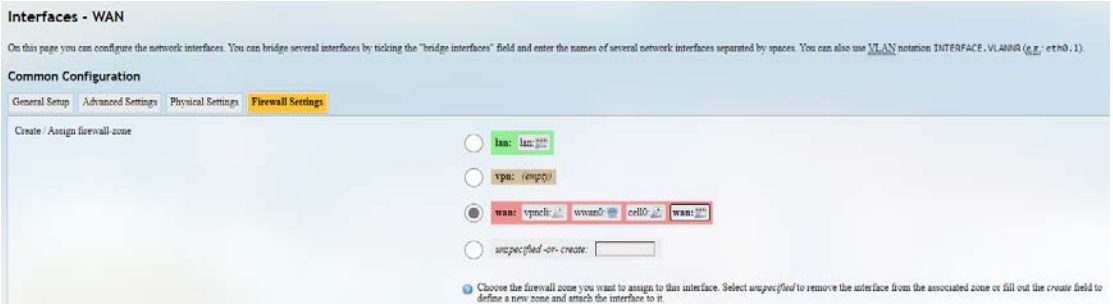
There is a **Physical Settings** tab next to **Advanced settings** when you log in with the root account, allowing you to configure the WAN port for network bridge.



Description of the numbered areas

1. Enable the interface for network bridge
2. Select the interfaces for bridge connection

There is a **Firewall Settings** tab next to the **Physical settings** tab when you log in with the root account, allowing you to create or designate a firewall zone.

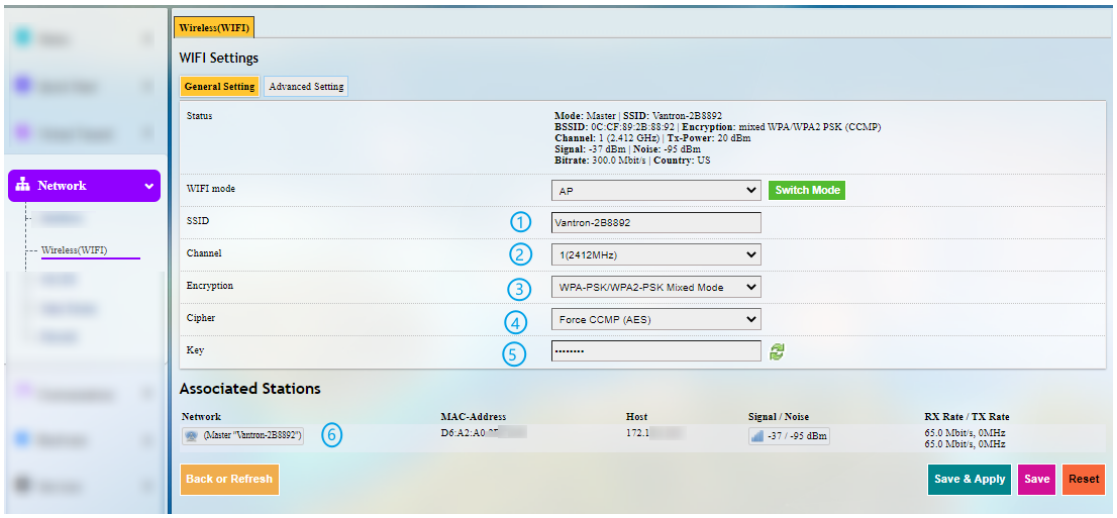


When 'unspecify or create' is selected, you can remove the interface from the associated firewall zone or create a new zone.

3.6.2 Wireless (WIFI)

You can switch between AP and client modes for wireless connection depending on your needs. When you use the Gateway as an AP, make sure it has internet access.

3.6.2.1 Wi-Fi – AP Mode (General setting)



Description of the numbered areas

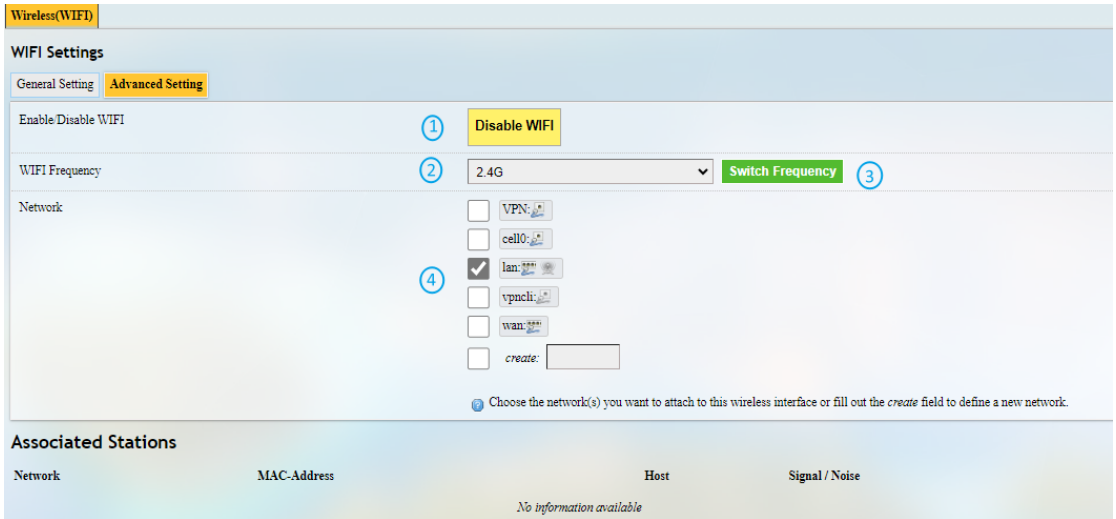
1. Set an SSID for the Gateway

The ID name shall not contain characters including $, `, \.

2. Select a Wi-Fi channel
3. Select an encryption method (the following options vary with the encryption method)
4. Select an encryption algorithm
5. Assign a Wi-Fi password (no less than 8 characters)
6. List of currently connected devices

Be sure to save the settings before you exit the page.

3.6.2.2 Wi-Fi – AP Mode (Advanced setting)



Description of the numbered areas

1. Turn on/off Wi-Fi
2. Set a Wi-Fi frequency (determined by hardware)
3. Click to switch frequency
4. The network interfaces to which Wi-Fi belongs

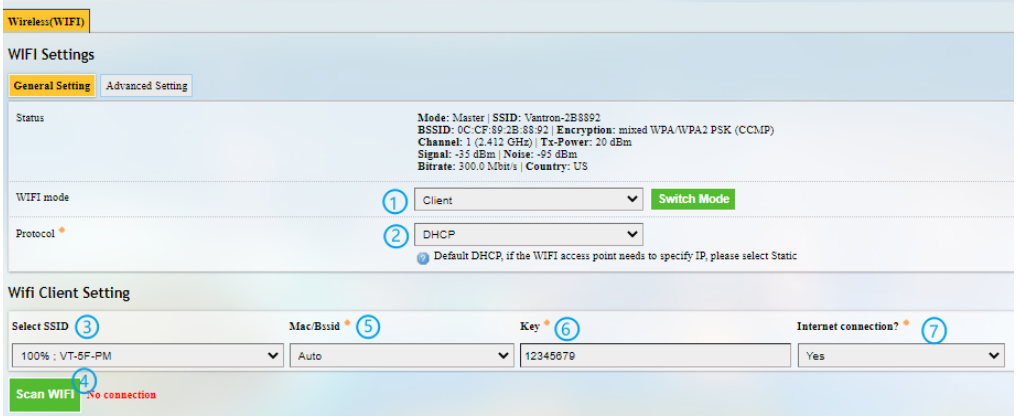
As modification of fields 2 will have impact on the Wi-Fi signal, the web interface will return to the general settings page upon a clicking of the switch button.

Be sure to save the settings before you exit the page.

3.6.2.3 Wi-Fi – Client Mode

When the Gateway is set as a client on a wireless network, the page below allows you to make changes to the network settings.

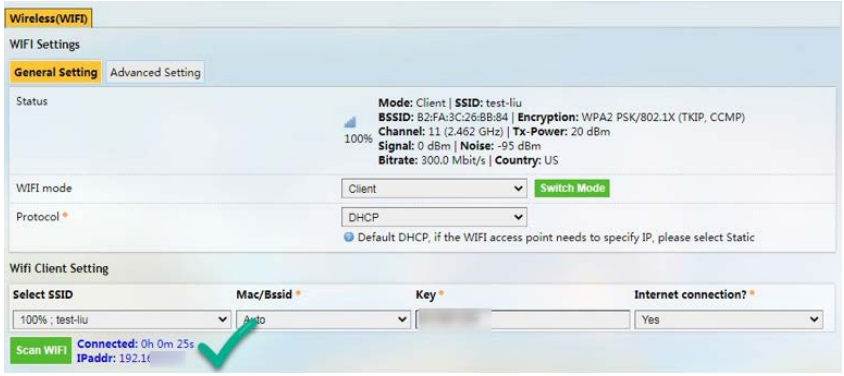
*A wwan0 port will be added (as shown in the **Interface** page) when the Wi-Fi client mode is enabled.*



Description of the numbered areas

1. Switch to **Client mode**
2. Select DHCP protocol to automatically assign an IP to the Gateway or Static protocol to specify an IP for the Gateway
3. Select a wireless network for internet access (previously joined network is shown first)
4. Click **Scan WIFI** to refresh the Wi-Fi list if the target Wi-Fi is not identified
5. Select the MAC address of the Wi-Fi, or leave it to Auto if not clear
6. Input the password of the Wi-Fi
7. Confirm that the target Wi-Fi has internet connection

When the Gateway is successfully connected as a client, there will be the network information next to **Scan WIFI** button.

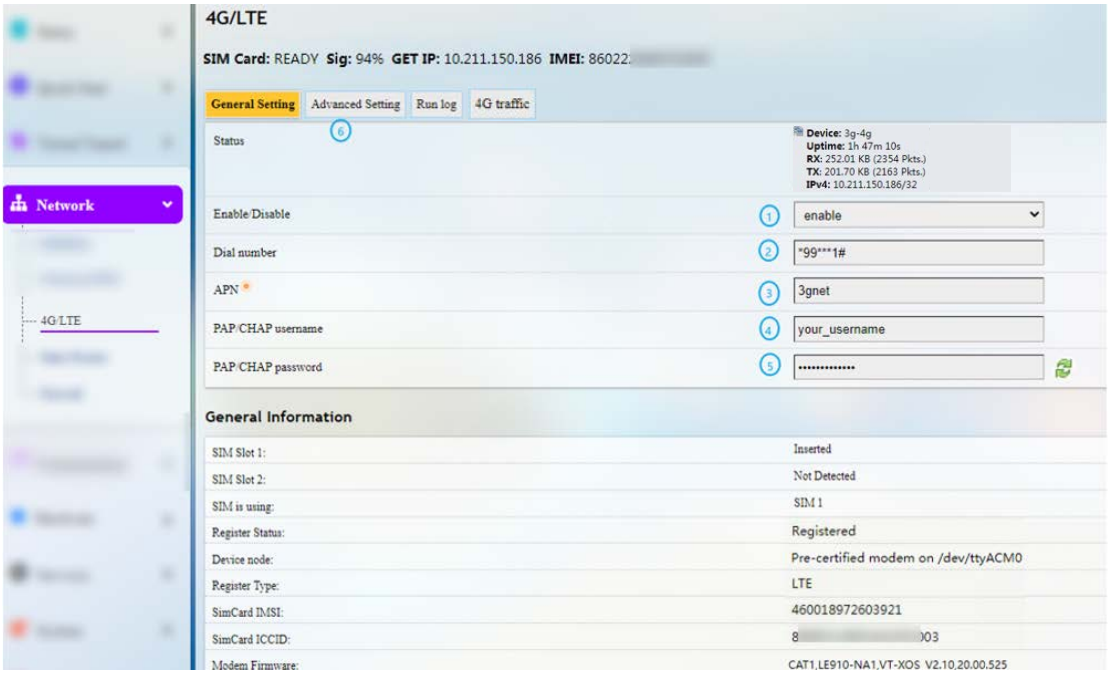


3.6.3 4G/LTE

Before you configure for 4G/LTE, be sure to install the activated SIM card and the LET antennas. After installation, the SIM card information will display on the top of the page, including signal strength, IP, and IMEI. While register status and other general information will display at the bottom of the page.

Confirm (with your sales executive) whether the 4G module is AT&T and Verizon pre-certified. If so, when you apply for SIM cards from the carriers,

- provide Verizon with the pre-certified module name **VT-MOB-CELL-mPCIe**.
- provide AT&T with the pre-certified module name **VT-MOB-MPCIE-4G**.



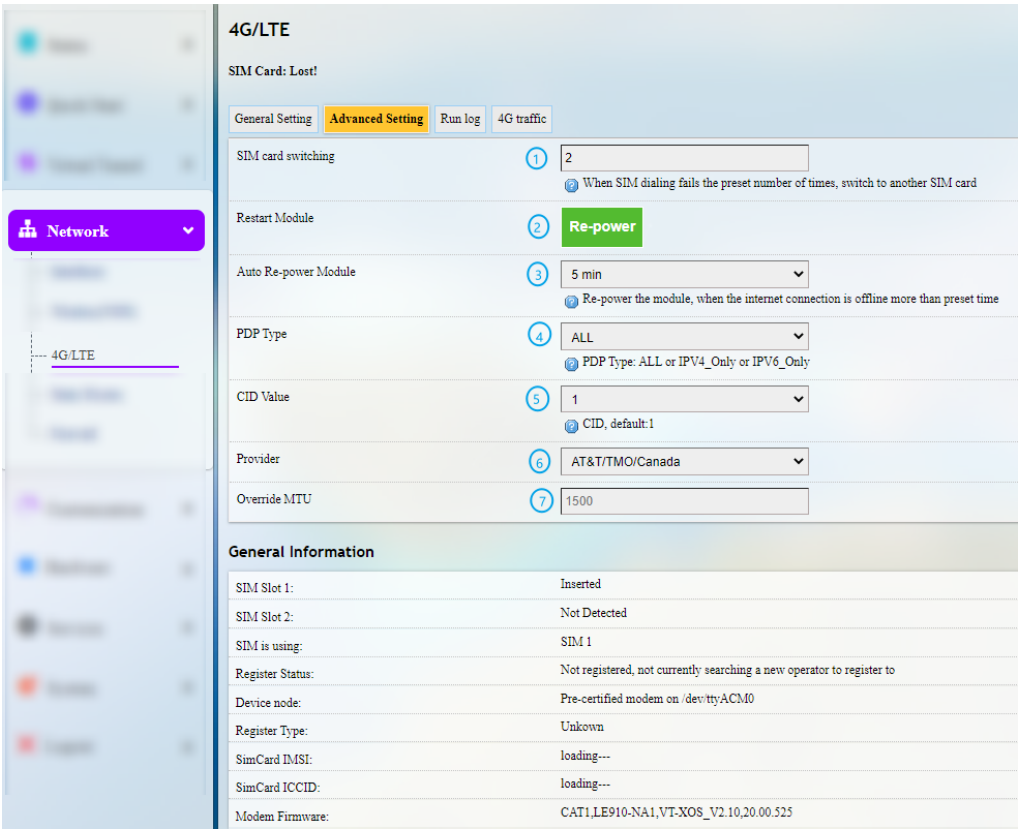
Description of the numbered areas

1. Enable/disable 4G/LTE service
2. Input *99***1# for AT&T SIM cards and *99***3# for Verizon SIM cards
3. Input the APN provided by the carrier
4. Enter the username provided by the carrier for PAP/CHAP authentication
5. Enter the password provided by the carrier for PAP/CHAP authentication
6. Click **Advanced Setting** for more configuration options

Leave the field as is if not applicable.

PAP/CHAP username and password are to be specified only if your carrier has set up APN with user name and password.

In the **Advanced Setting** page, you can further configure the cellular network.



Description of the numbered areas

1. Maximum number of dial failures allowed for current SIM card (only for devices with dual SIM cards, better to leave it as is)
2. Click to restart the 4G module
3. Time scheduled for automatic restart of the 4G module when it is offline
4. Select a PDP type (leave it as is)
5. Select **custom** from the drop-down list, input **1** for AT&T SIM cards and **3** for Verizon SIM cards
6. Select **AT&T/TMO/Canada** or **Verizon** from the drop-down list for AT&T SIM cards and Verizon SIM cards, respectively
7. Default MTU value (1500)

Remember to save the settings to have the configurations take effect.

If the 4G module is not AT&T and Verizon pre-certified, the provider information will not be available in **Advanced Setting**, and the **General Setting** options are the same as those for pre-certified 4G modules. You can keep the default values of the fields unchanged.

The **Run Log** next to the **Advanced Setting** tab displays the last 50 log entries of the module.

Under **4G traffic** tab, traffic information measured in real time or on the monthly and daily basis is available. You can also set the interval for submitting the temporary in-memory database to the persistent database directory.

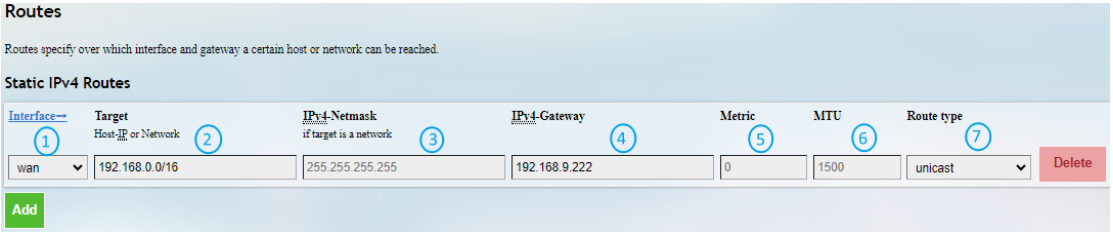
3.6.4 Static Routes

This advanced function allows you to specify interface rules for route access.

Example:

Requirement: When the Gateway has 4G and WAN interfaces, the internal network (192.168.0.0 - 192.168.255.254) is accessed via the WAN interface by the internal server. Other data access is realized via the 4G interface.

Click **Add** to set a new static route.



Description of the numbered areas

1. Select an interface to configure the route
2. Input the IP address of the host
3. Input the subnet mask (255.255.255.255 by default)
4. Input the address of IPv4 gateway
5. Gateway metric (The smaller the number, the higher the priority)
6. Set the MTU
7. Select a route type (refer to the details next page)

Be sure to save the settings before you exit the page.

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.
Type	Description
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.

3.6.5 Firewall

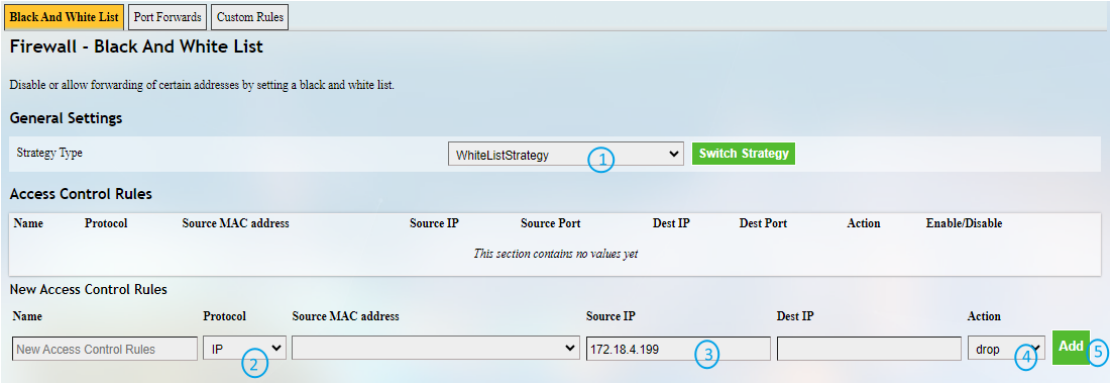
- **Black List and White List**

The black and white list feature allows you to enable/disable the forwarding of specific addresses.

White list policy: All addresses but those added to the **Access Control Rules** have the access

Black list policy: All addresses but those released to the **Access Control Rules** are blocked

Scenario 1: To block the internet access of 172.18.4.199

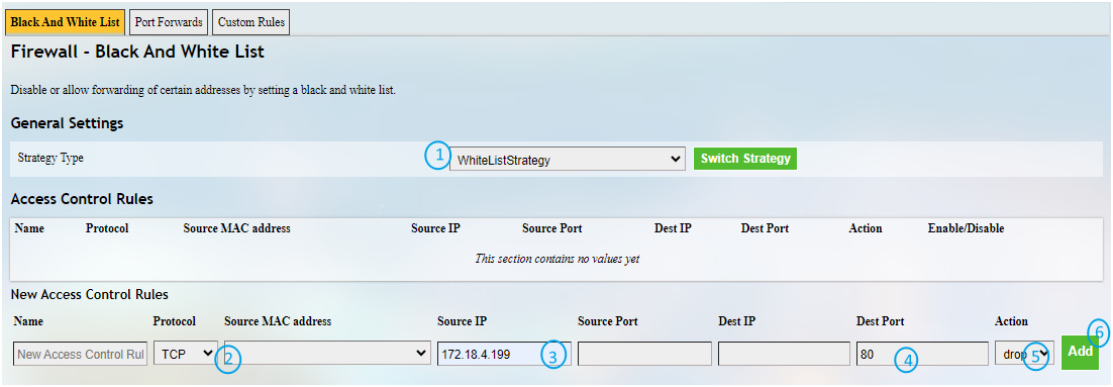


Description of the numbered areas

1. Select the white list strategy and click the button behind to switch to the strategy
2. Select the IP protocol
3. Input the source IP
4. Select 'drop' as the action for the target address
5. Click **Add** to add the address to the access control list

Be sure to save the settings before you exit the page.

Scenario 2: To block the TCP communication between 172.18.4.199 and the external network via port 80

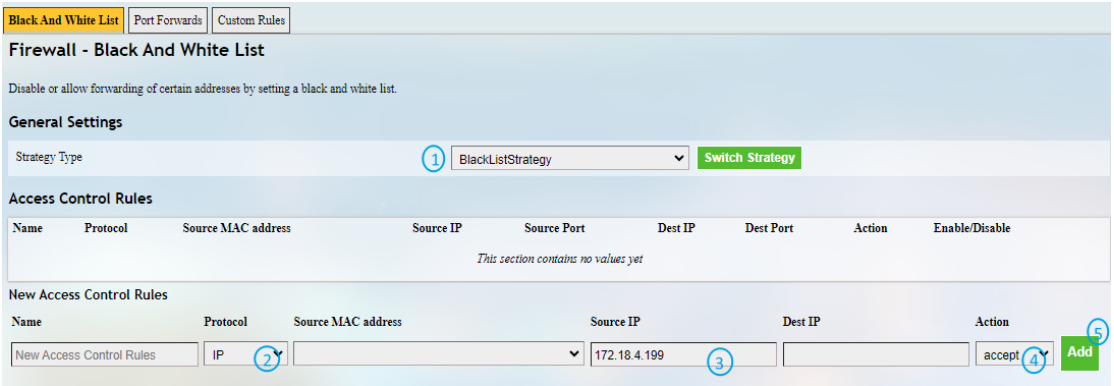


Description of the numbered areas

1. Select the white list strategy and click the button behind to switch to the strategy
2. Select the TCP protocol
3. Input the source IP
4. Input the destination port
5. Select 'drop' as the action for the target IP and port
6. Click **Add** to add the IP and port to the access control list

Be sure to save the settings before you exit the page.

Scenario 3: To release 172.18.4.199 for internet access

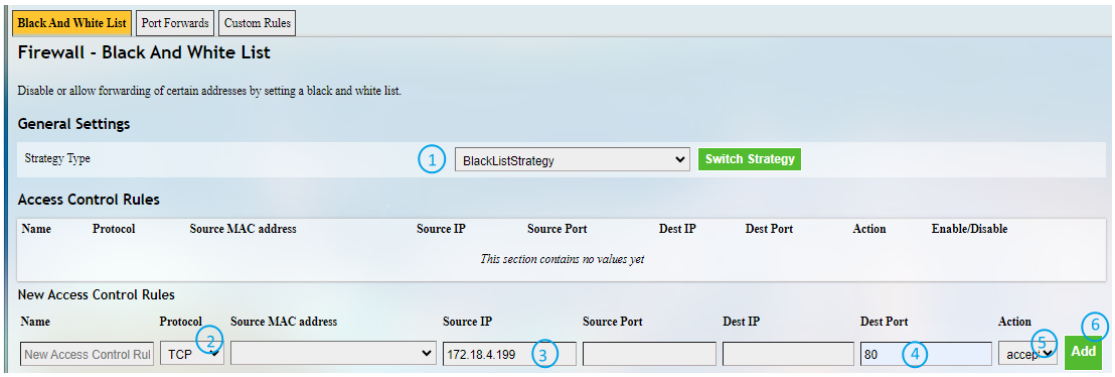


Description of the numbered areas

1. Select the black list strategy and click the button behind to switch to the strategy
2. Select the IP protocol
3. Input the source IP
4. Select 'accept' as the action for the target IP
5. Click **Add** to release the IP from the access control list

Be sure to save the settings before you exit the page.

Scenario 4: To allow the TCP communication between 172.18.4.199 and the external network via port 80



Description of the numbered areas

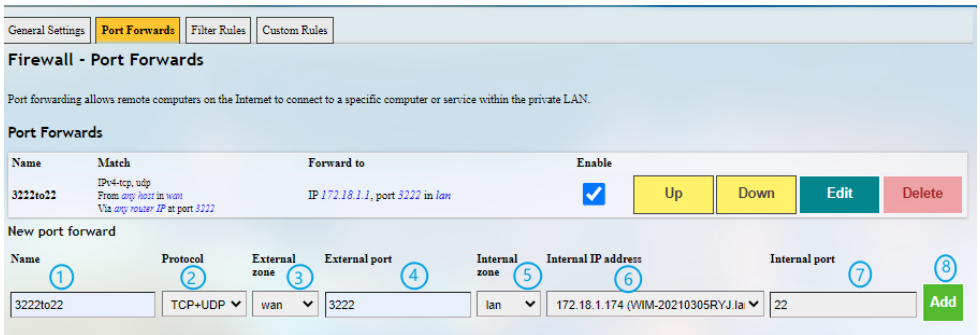
1. Select the black list strategy and click the button behind to switch to the strategy
2. Select the TCP protocol
3. Input the source IP
4. Input the destination port
5. Select 'accept' as the action for the target IP and port
6. Click **Add** to release the IP and port from the access control list

Be sure to save the settings before you exit the page.

- **Port Forwards**

The forwarding controls the traffic between zones and may enable MSS clamping for specific directions. Only one direction is covered by a forwarding rule. To allow bidirectional traffic flows between two zones, two forwarding setups are required with the dest ports reversed.

Example of port forwarding (To forward port 3222 of the WAN port to port 22 of the LAN host 172.18.1.174):

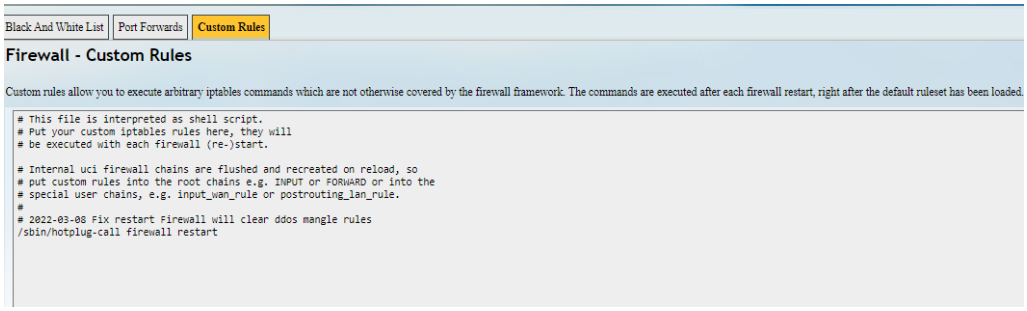


Description of the numbered areas

1. Rule name
2. Protocol (TCP/UDP/TCP + UDP are supported)
3. External zone: WAN
4. External port: 3222
5. Internal zone: LAN
6. LAN host: 172.18.1.174
7. Port number of the target host in the internal zone: 22
8. Add the rule (mandatory)

- **Custom Rules**

Custom rules allow you to execute arbitrary **iptables** commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default rule settings have been loaded.



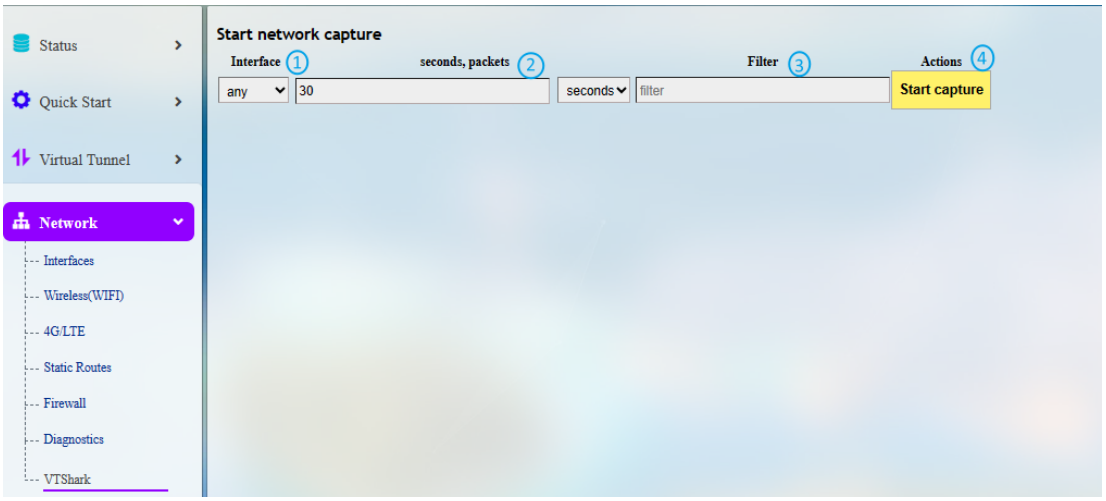
3.7 Diagnostics

Tools available in **Diagnostics** are explained below:

Tool	Description
Ping	To test the connectivity and measure the response time between the router and external IP addresses on the internet
Traceroute	To access information about the path that network traffic follows, including the number of hops and the response time of each hop
Nslookup	To query the Domain Name System (DNS) to obtain information about domain names, IP addresses, and DNS records

3.8 VTShark

The **VTShark** feature provides a flexible way to follow up and verify network issues. You can use wireshark to open and check the packets captured.



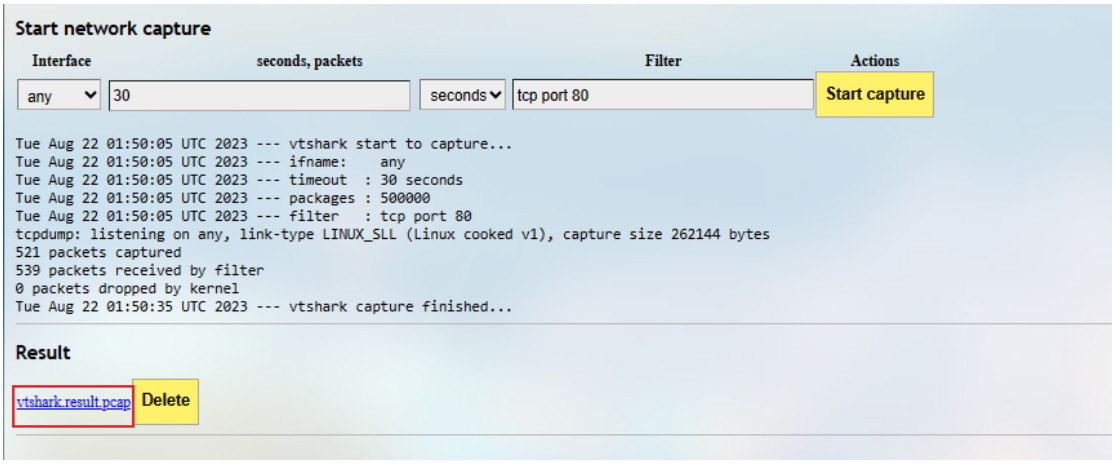
Description of the numbered areas

1. The interface from which the packets are captured (all interfaces are selected by default)
2. The measurement by which the data packets are captured (by seconds or by packet counts as explained below)
3. The filter for capturing the designated packets (more details are available at https://www.tcpdump.org/manpages/pcap-filter.7.html for advanced filtering)
4. Start the data capturing

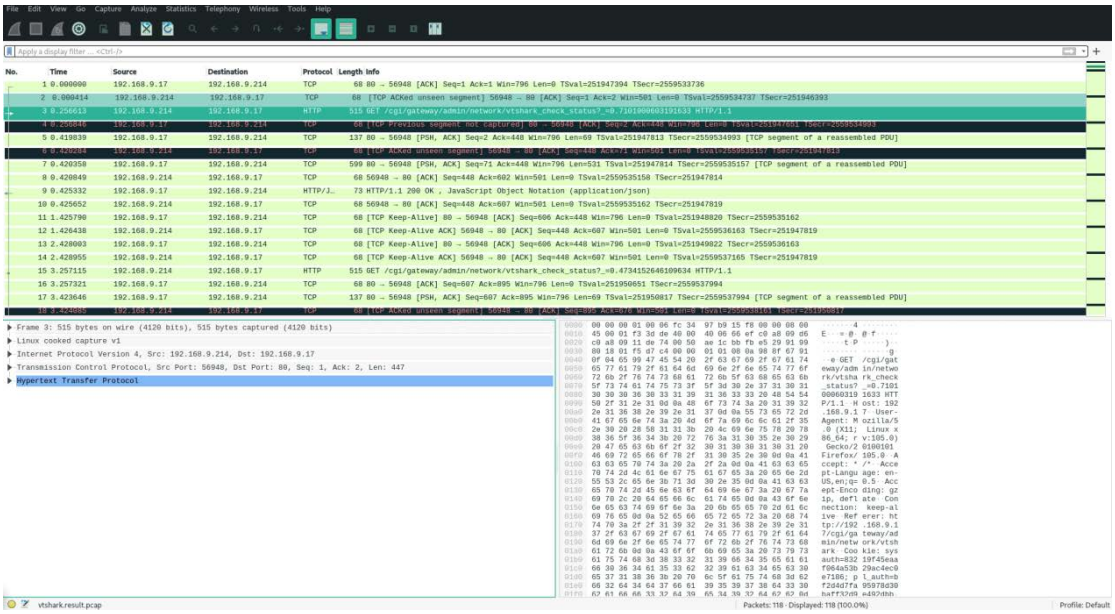
Packets capturing by seconds and by packet counts:

Measurement	Description
Seconds	To specify a time duration for data capturing. For instance, you can input '10/20/30…' for the data capturing, which indicates that the capture will stop in 10/20/30 seconds.
	The system supports up to 500,000 packets for the time-based data capturing. The capture stops after reaching this limit, even if it has not reached the preset time duration.
Packets	To specify the count of packets for data capturing. For instance, you can input '100/200/500…' for the data capturing, which indicates that the capture will stop when 100/200/500 packets have been captured.
	The system supports up to 10 minutes (600 seconds) for the packet-based data capturing. The capture stops after reaching this limit, even if it has not reached the preset packet counts.

In the following scenario, the capture targets at all interfaces for the http packets from 'tcp port 80' for 30 seconds.



Clicking the result will download it to the local directory and you can open it with wireshark.



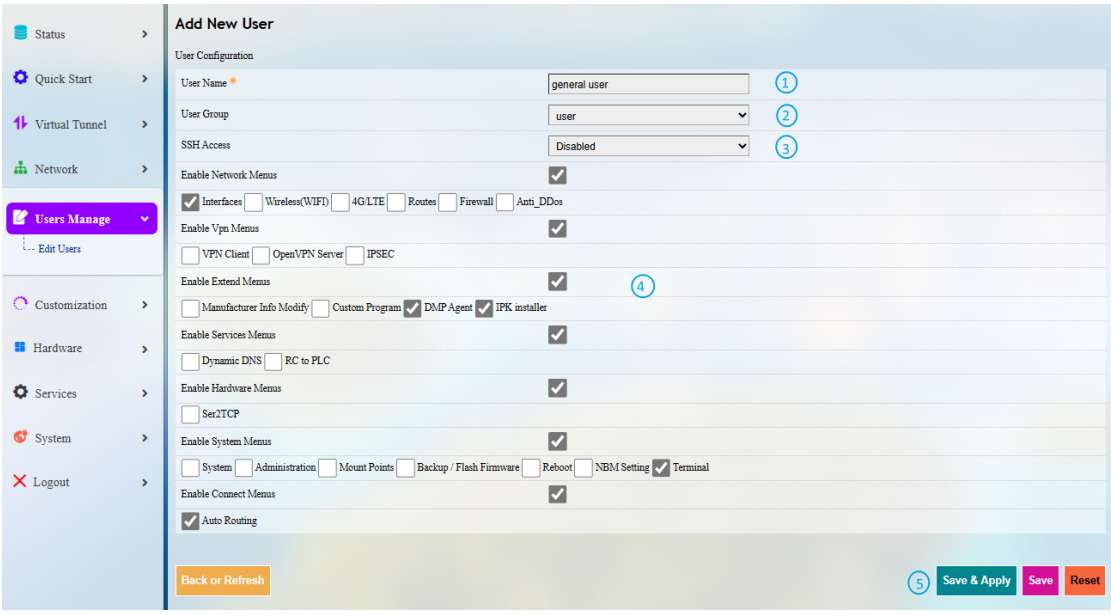
3.9 User Management

As this function may change system settings, you need log in with the root account (Refer to 2.2 for the username and password) to enable the function.

User management allows you to add new users or edit the existing users to assign different permissions to different roles.

To add a new user, click the button below the existing user information.

In the new page, you can create the user and enable certain features for the user.



Description of the numbered areas

1. Input a username
2. Select a group for the new user
3. Enable SSH access or not for the new user
4. Expand the menus to enable specific functions for the new user
5. Save the settings before you exit

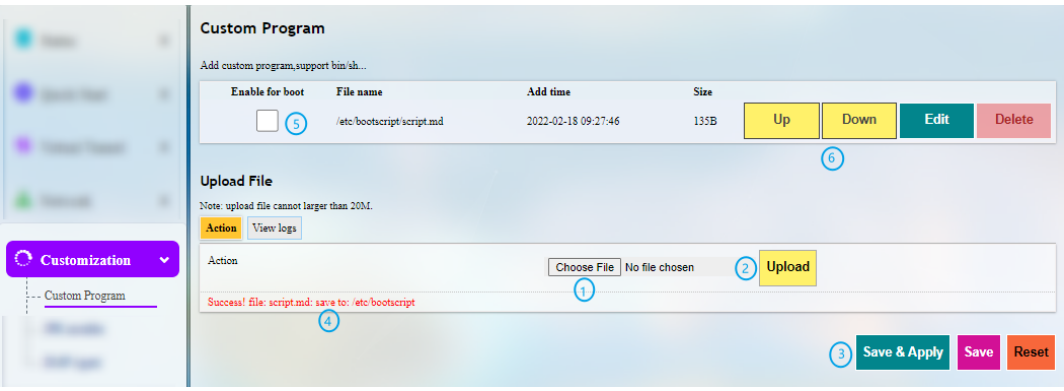
After creating the user, it will be added to the user list. The **Edit** and **Delete** buttons behind a user allow you to enable/disable certain functions for this user or delete this user.

3.10 Customization

As certain functions under this menu may change the system settings, you need log in with the root account (Refer to 2.2 for the username and password) to enable the function.

3.10.1 Custom Program

Custom program allows users to upload scripts or programs (sh/bin) to the Gateway and run them at the startup.



Description of the numbered areas

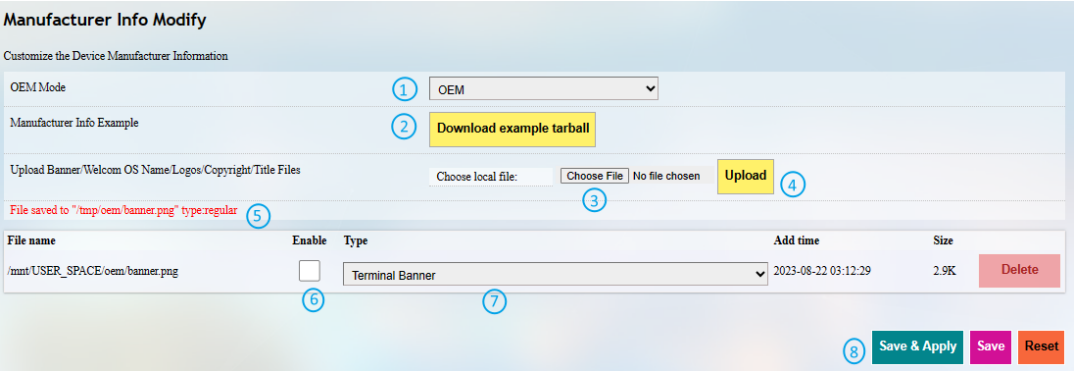
1. Select a script to upload
2. Upload the script to the Gateway
3. **Save & Apply** the settings
4. When the script is uploaded successfully, the file name and file directory will be displayed
5. Enable the script, and it will run next time when the Gateway starts up
6. If more than one script is uploaded, you can move any of them up or down to rearrange the script order, and edit/delete the script

3.10.2 IPK Installer

With IPK Installer, customers can install self-compiled IPK packages to the Gateway. Vantron industrial protocol packages are also uploaded from here. Refer to 4.2 Protocol Configuration and Application for uploading an IPK for Industrial Protocols.

3.10.3 Manufacturer Info Customization

Once you need to customize the manufacturer information for logging in the system, navigate to **Customization > Manufacturer Info Modify**, and follow the steps below.



Description of the numbered areas

1. Select the **OEM** mode
2. Download the illustrative .tar file to the local directory and replace the files with your own as necessary
3. Select the target file from the local directory
4. Upload the file to the Gateway
5. The path of the file will be displayed here
6. Choose to enable the file or not for next startup
7. Select the type of the file
8. **Save & Apply** the settings

The three modes that customers can choose from the drop-down list based on needs are explained as follows.

Mode	Description
Vantron	All the information displayed in VantronOS will be Vantron-related.
Standard	Some of the information displayed in VantronOS will be “Gateway” by default, and some information like the copyright will be left blank.
OEM	All the information displayed will be user tailored.

3.10.4 DMP Agent

Gateways/routers are interfacing with BlueSphere GWM via DMP Agent. You can modify the settings of the DMP agent here.

Description of the numbered areas

1. Status of DMP Agent
2. Click **Clear Agent** before changing any configurations

Provided that the remaining prerequisites (refer to [2.5 Interfacing with Vantron Gateway Management Platform]) are met, the DMP Agent, once enabled, will run automatically when there is internet access. Clicking this button will disable DMP Agent, kill all the processes running at the background, and remove the Agent package from the original installation directory.

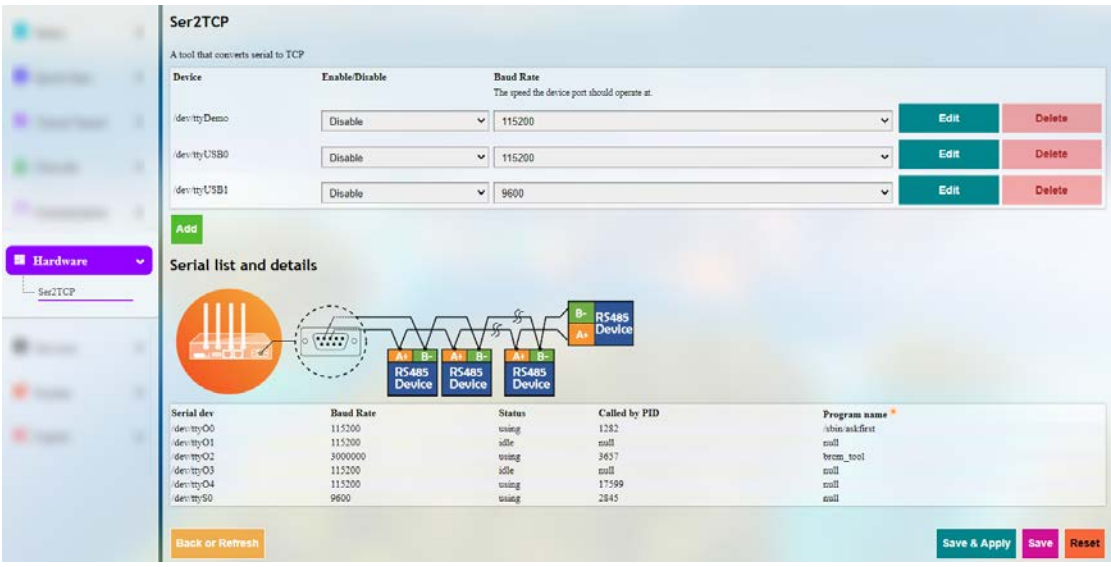
3. Enable/Disable the Agent
4. You can customize the installation path of the Agent here (default path: '/usr/vtmdm_agent_c/')
5. Set up the download address of the Agent server
6. Internet server for public domain and download server for private domain

*Factory reset of the Gateway will deactivate the device on the BlueSphere GWM platform. If you wish to activate it again on the GWM, please click **Clear Agent** in the VantronOS portal, then **enable** the agent and wait a moment to allow the device to come online on the BlueSphere GWM platform.*

3.11 Hardware

3.11.1 Ser2TCP

Serial to TCP provides an easy way to convert local serial data into Ethernet data and enables two-way communication with remote devices. Each conversion rule can be independently configured to server-side or client-side mode. You can also add, edit or delete a conversion rule on this page.

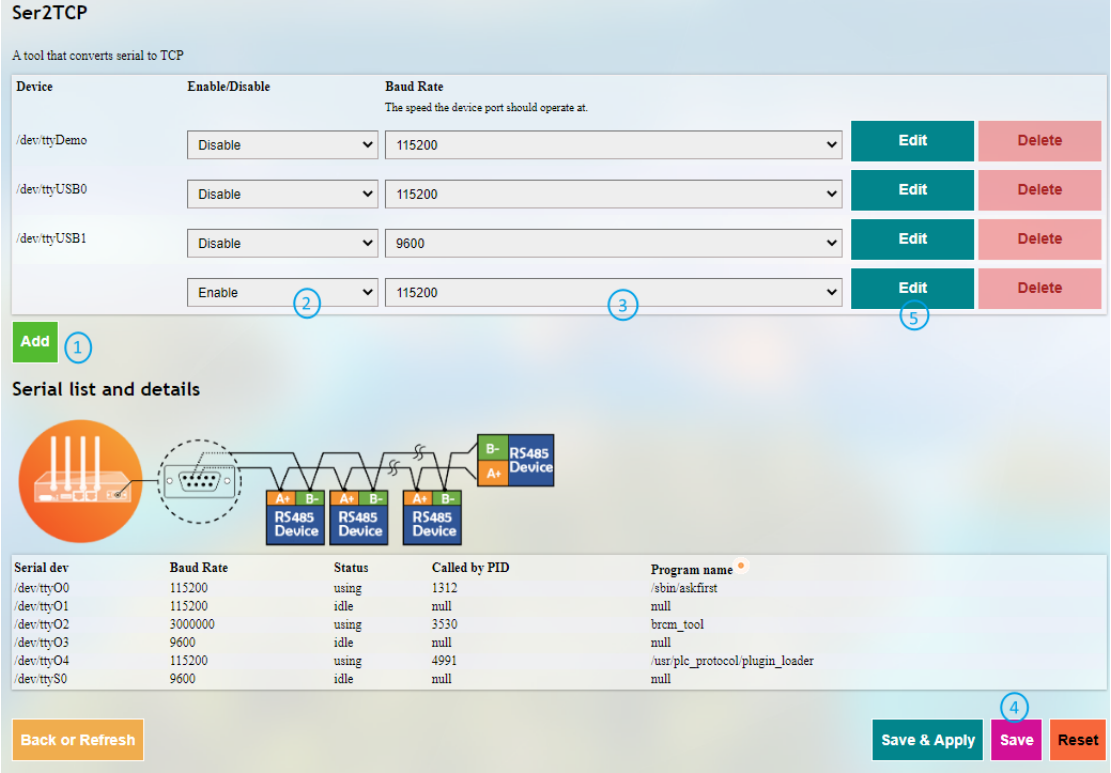


3.11.2 Ser2net environment setup and verification

- Prerequisites
  - A G335 gateway
  - A Linux host computer (Ubuntu for demonstration here)
  - An F/F DB9 serial cable
  - An RS232 to USB serial cable
  - Connect the serial port (e.g., DB9) of the gateway to the host as follows

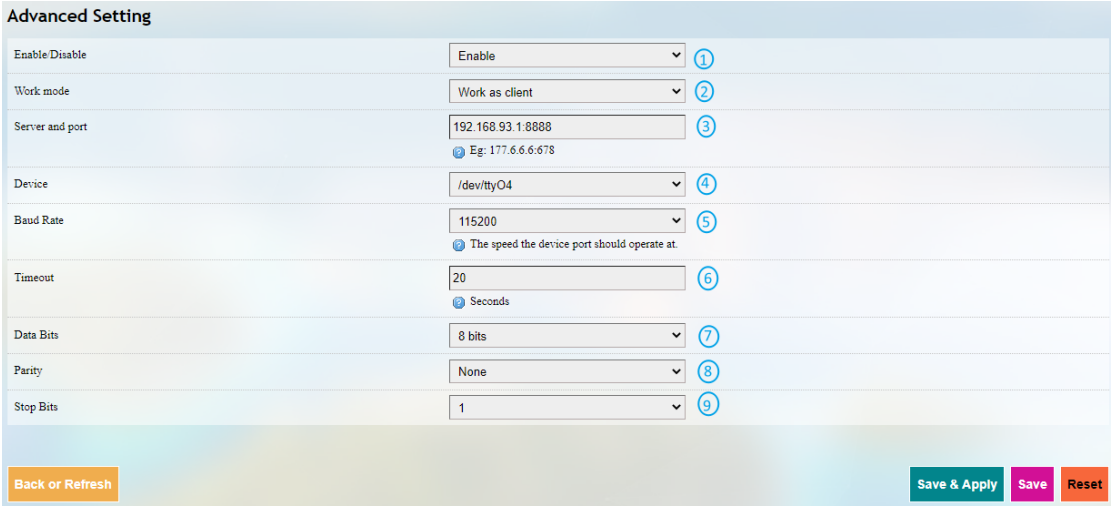
- Client mode

(1) Settings on VantronOS web interface



Description of the numbered areas

1. Click **Add** to add a conversion rule
2. Select **Enable** from the drop-down
3. Set the Baud rate to 115200
4. Save the settings
5. Click **Edit** after the rule to enter the advanced settings page



Description of the numbered areas

1. **Enable** the rule
2. Select the **Work as client** mode
3. Input the server address and port number (Ubuntu host shall be the server, and port number is user-defined)
4. Select the serial device from the drop-down list (software node for the DB9 connector is /dev/ttyO4 as described in 1.5)
5. Select 115200 as the baud rate (the default value will be the one selected when setting up the rule)
6. Set a timeout value
7. Select “8 bits” for the data bit
8. Select “None” for parity
9. Select “1” as the stop bit

Save and Apply *above settings before you exit.*

(2) The Ser2net process is running as follows:

```
uart2net -c -d 192.168.93.1 -p 8888 -t /dev/ttyO4 -b 115200 -a 8 -r none -s 1 -o 20
```

(3) Settings on the Ubuntu host

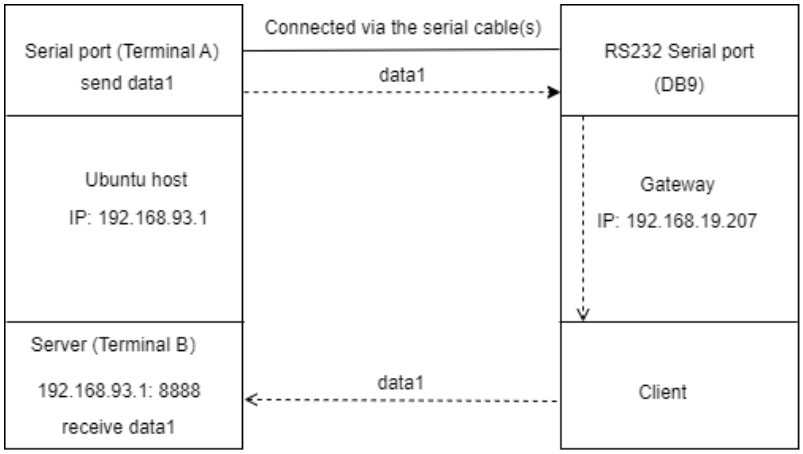
- Use microcom to access the serial port in terminal A (assume that the device name for the RS232 to USB serial adapter is identified as /dev/ttyUSB1)

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- Monitor the designated port (8888 as assigned in prior steps)

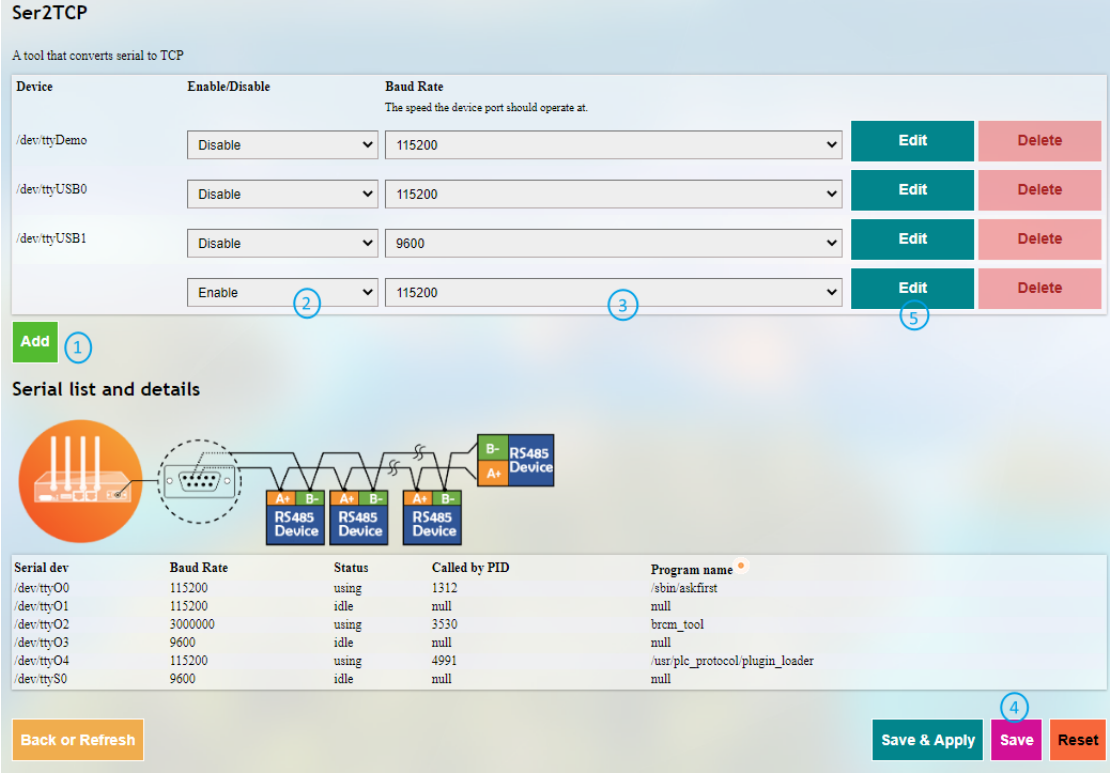
```
tcpudp_test tcp server:tcpudp_test -p 8888
```

- Input data in terminal A and receive in terminal B (the topology is as follows)



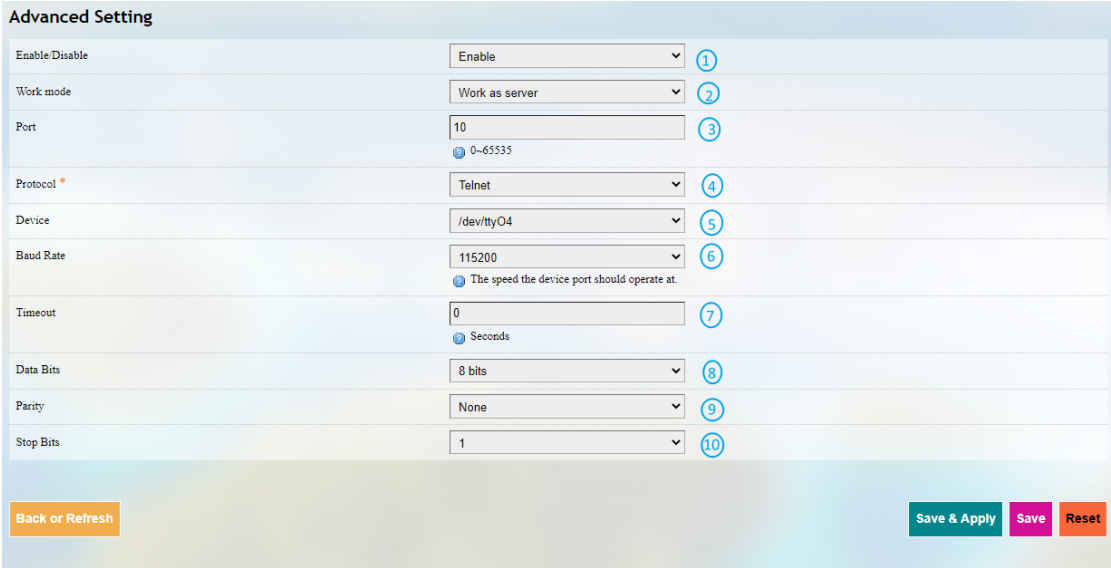
- Server mode

(1) Settings on VantronOS web interface



Description of the numbered areas

1. Click **Add** to add a conversion rule
2. Select **Enable** from the drop-down
3. Set the Baud rate to 115200
4. Save the settings
5. Click **Edit** after the rule to enter the advanced settings page



Description of the numbered areas

1. **Enable** the rule
2. Select the **Work as server** mode
3. Input the port number (user-defined)
4. Select a protocol from the drop-down (**Telnet** for instance, see 3.11.3 for the difference between the protocols)
5. Select the serial device from the drop-down ((software node of the DB9 connector is /dev/ttyO4 as described in 1.5)
6. Select 115200 as the baud rate (the default value is the one selected when setting up the rule)
7. Set a timeout value
8. Select “8 bits” for the data bit
9. Select “None” for parity
10. Select “1” as the stop bit

Save and Apply *above settings before you exit.*

(2) Ser2net running process is as follows:

```
/usr/sbin/ser2net  -n  -c  /tmp/ser2net.conf
```

(3) Settings on the Ubuntu host

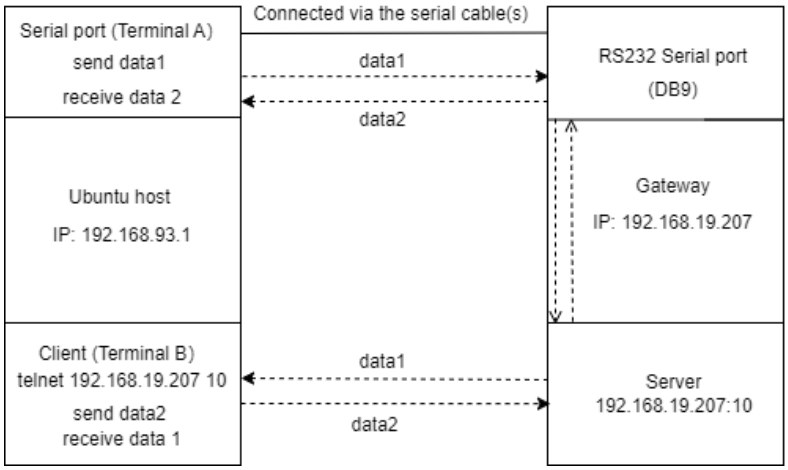
- Use microcom to access the serial port in terminal A (assume that the device name for the RS232 to USB serial adapter is identified as /dev/ttyUSB1)

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- Monitor the designated port (10 as assigned in prior steps) in terminal B using Telnet protocol

```
telnet 192.168.19.207 10
```

- Terminals A and B can send and receive data in both directions (the topology is as follows)



3.11.3 Protocol comparison

Under the server mode, two protocols are available which are differentiated as below:

1) Raw: enables the port and transfers all data as-is between the port and the long integer.

2) Telnet: enables the port and runs the telnet protocol on the port to set up telnet parameters (less used).

3.12 Services

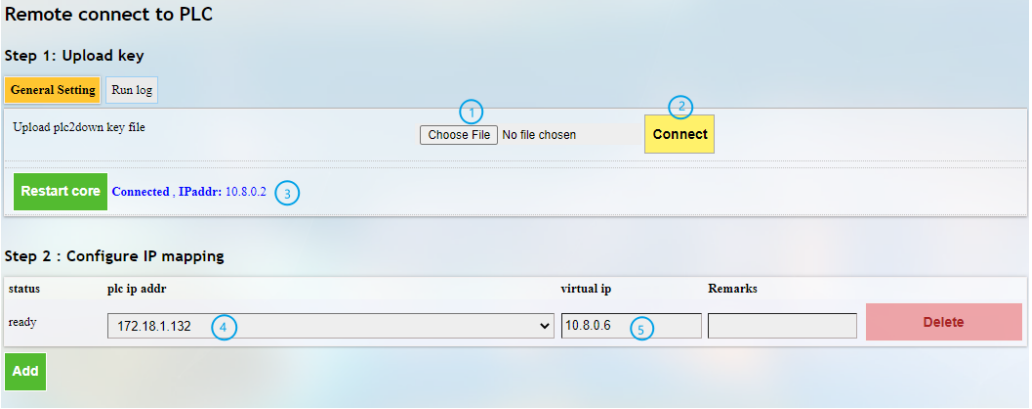
3.12.1 RC to PLC

For remote access and control of PLC devices via OpenVPN protocol, you will need two gateways and a Windows host computer ('Windows PC') that are on the same network. One gateway ('G1') is for building an OpenVPN server, and the other ('G2') is for connecting the OpenVPN server built by G1.

Prerequisites:

1. Prepare the G1, G2, Windows PC, and PLC device
2. Connect G1 and G2 to the same network via Wi-Fi or Ethernet
3. Install an OpenVPN client program (such as OpenVPN-2.5.2-I601-amd64.msi) and a PLC programming software (such as STEP7 depending on the device) on the Windows PC
4. Refer to 3.4.1 OpenVPN Server to build an OpenVPN server in the **tap** working mode on G1 and download the .ovpn file
5. Connect the Windows PC to the OpenVPN server built by G1 via the OpenVPN client program
6. Connect G2 to the OpenVPN server built by G1 (see below)
7. Connect the PLC device to a LAN port of G2 and set a static IP address for the PLC (see details below)
8. Connect the PLC device to the Windows PC via Ethernet and control the PLC with the PLC programming software (STEP7)

VantronOS offers a platform for connecting G2 to G1 and configuring the PLC and G2. For other settings, please download the related software program and finish the setup.



Description of the numbered areas

1. Download and save the .ovpn file after setting up the OpenVPN server on G1, then click this button to open the directory of the file
2. Click **Connect** to connect G2 to the OpenVPN server built by G1
3. After connection, an IP address assigned by the OpenVPN server will be displayed here
4. Input a static IP address for the PLC (on the same IP network as the LAN port of G2)
5. Input a virtual IP for the PLC (on the same IP network as the one assigned by the OpenVPN server and not occupied by other clients)

Be sure to save above settings to allow them to take effect.

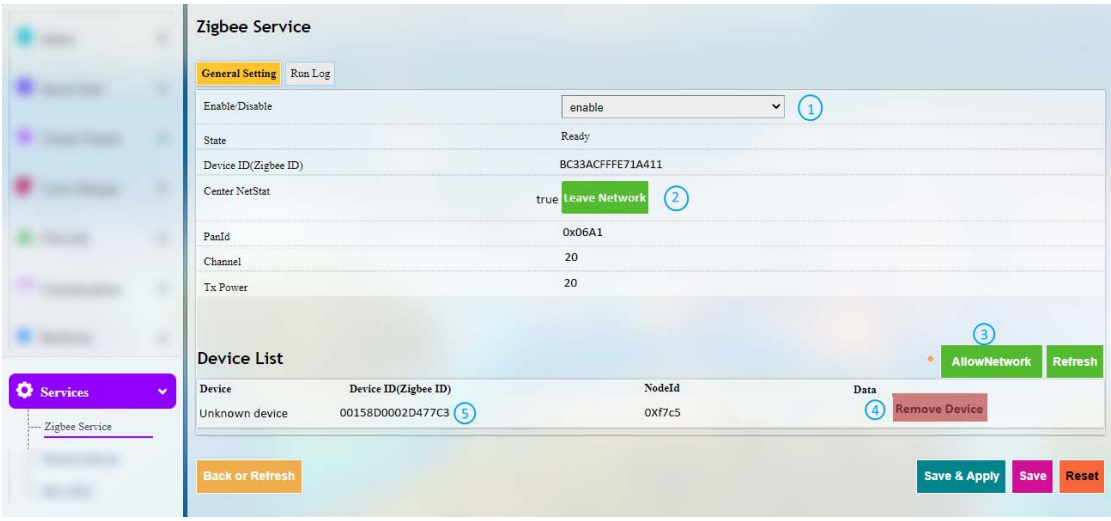
3.12.2 Protocol Service

If a protocol-related .ipk file has been installed on the device, the protocol-related service information will be accessible on VantronOS with root account login, which shall be the same as that displayed on the protocol specific portal.

Please refer to **chapter 4** for the configurations and applications of industrial protocols.

3.12.3 ZigBee Service

If the Gateway has a ZigBee module, you can create a ZigBee network on VantronOS with root account login.



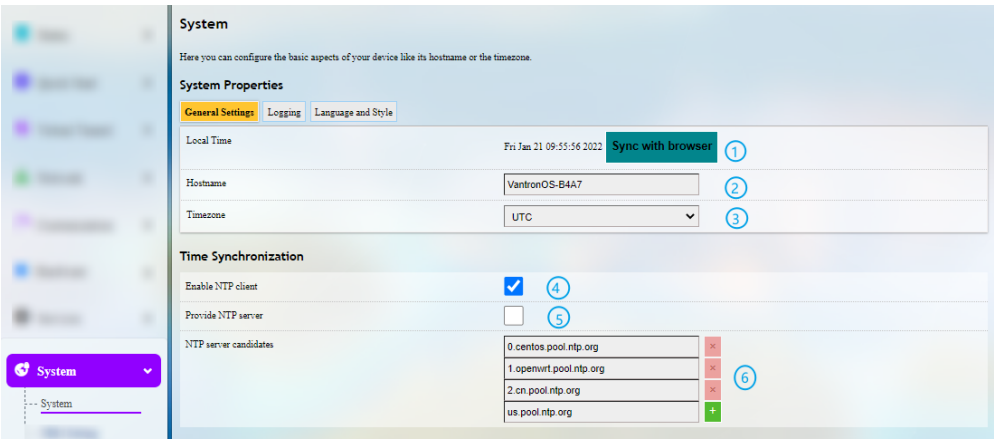
Steps for set up a ZigBee network:

1. Click **enable** from the drop-down box then click **Save & Apply** to apply the change;
2. The Device ID will display as shown above if there is a ZigBee network; if not, click **Add Network** to create one;
3. After creating the ZigBee network, click **Allow Network** to allow client devices to join the network (valid for 180s at the max., expires when a device joins the network)
4. Click **Remove Device** to remove a client device from the ZigBee network;
5. Information of the client device on the network.

3.13 System

3.13.1 System

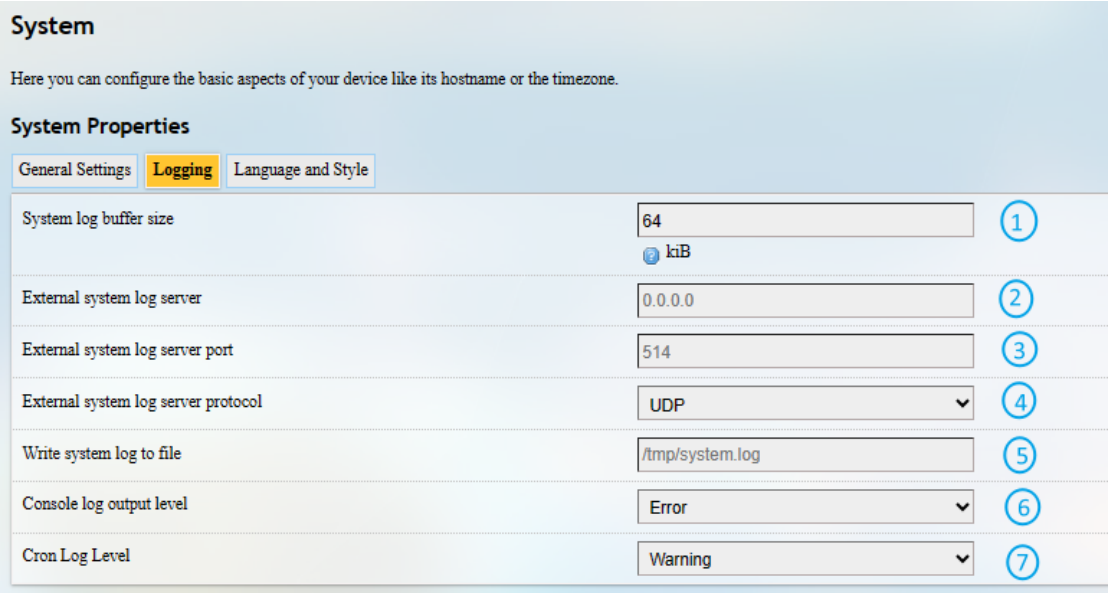
Apart from the device settings you might make in the previous sections, here you can configure your Gateway in more details, including host name, time zone, administrative password and so on.



Description of the numbered areas

1. Synchronize the Gateway time with the browser (local) time
2. Assign a name to the host
3. Select a time zone
4. Enable NTP online time adjustment
5. Start the NTP server (the Gateway is the NTP server)
6. NTP online time server

For log-related settings, click **Logging** tab next to the **General settings** tab.

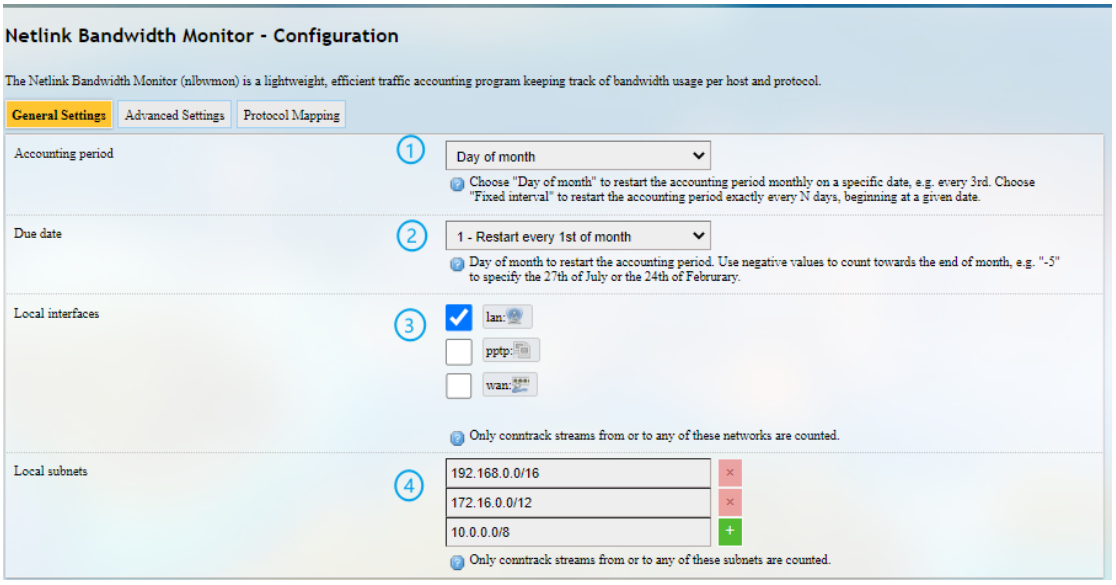


Description of the numbered areas

1. Buffer size of the system log
2. Address of the log server
3. Port of the log server
4. Protocol used by the log server
5. Path of the file for the system log
6. Output level of the console log
7. Cron log level

3.13.2 Netlink Bandwidth Monitor (NBM) Setting

- **General Settings**



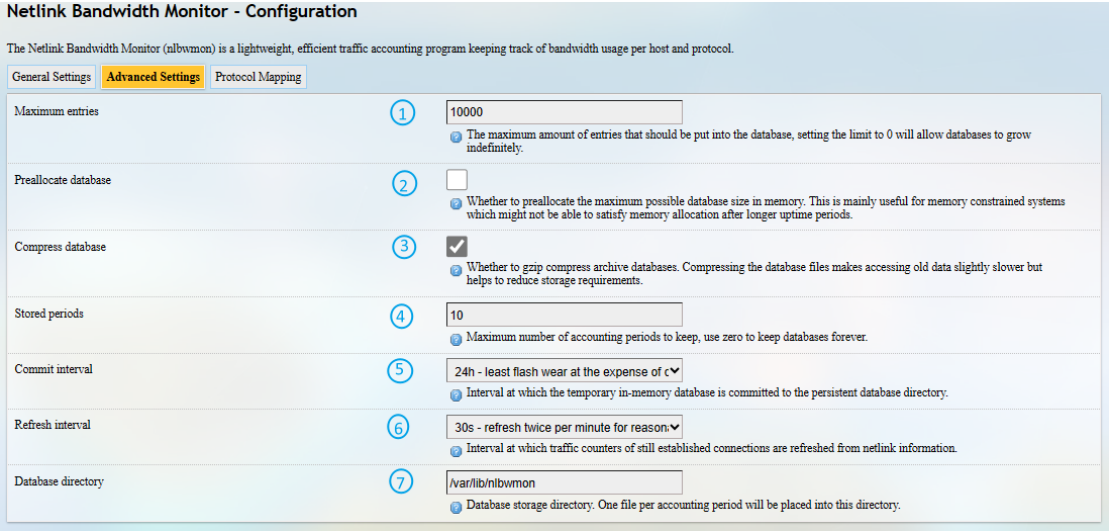
Description of the numbered areas

1. Set how long you would like the monitoring activities to be reported
2. Specify a date in a month for restarting another round of monitoring activities

Applicable when Day of month is selected in 1

3. Select the interfaces to monitor
4. Local subnets

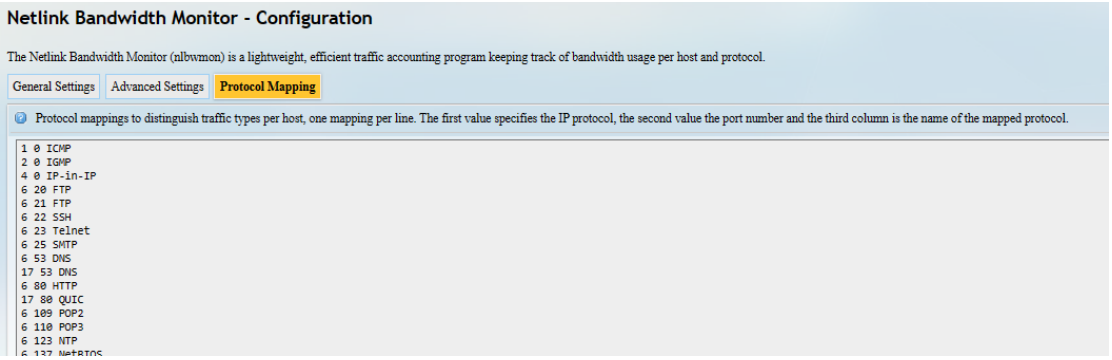
Under **Advanced Settings** tab, you can further set up the monitoring activities.



Description of the numbered areas

1. Set the maximum count of entries to store in the database (‘0’ for no limit)
2. Check the box to pre-allocate a database (more frequently applicable to devices with less memory space)
3. Check the box to compress the database
4. Maximum count of reporting periods to store (‘0’ for no limit)
5. Time interval for submitting the temporary database to the persistent database
6. Time interval for refreshing the traffic counters from the netlink information
7. Directory of the database

Protocol Mapping can be used to distinguish traffic types per host. Each mapping takes one line, with the first value being the IP protocol, the second value being the port number, and the third value being the name of the mapping protocol.



3.13.3 Administration

Under the **Router Password** section, you can reset a password for accessing the Gateway.

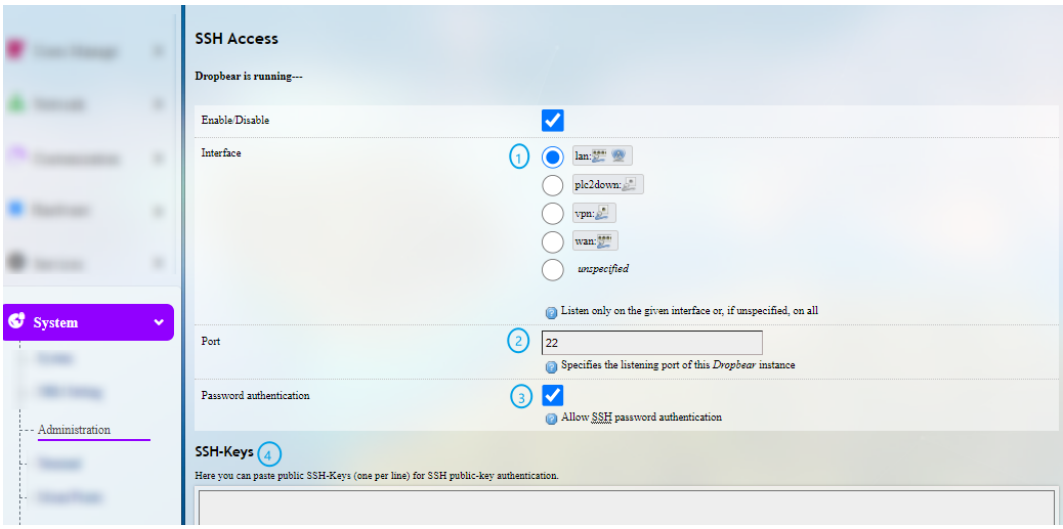
SSH Access

As this function might compromise the security of the network, you have to log in the web interface with a root account.

Step 1: Log out the interface by clicking **Logout** at the left bottom corner;

Step 2: Log in with the root account (root) and password (rootpassword);

Step 3: Navigate to **System > Administration**, and enable dropbear;



Description of the numbered areas

1. Select a port to access (LAN by default)

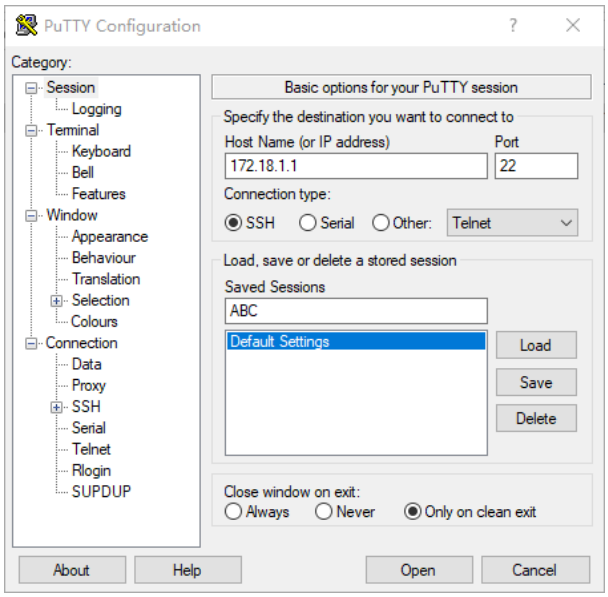
When "unspecified" is selected, all the ports will be monitored.

2. Specify a port for monitoring (port 22 by default)
3. Allow SSH password authentication
4. Add SSH-Keys for public key authentication

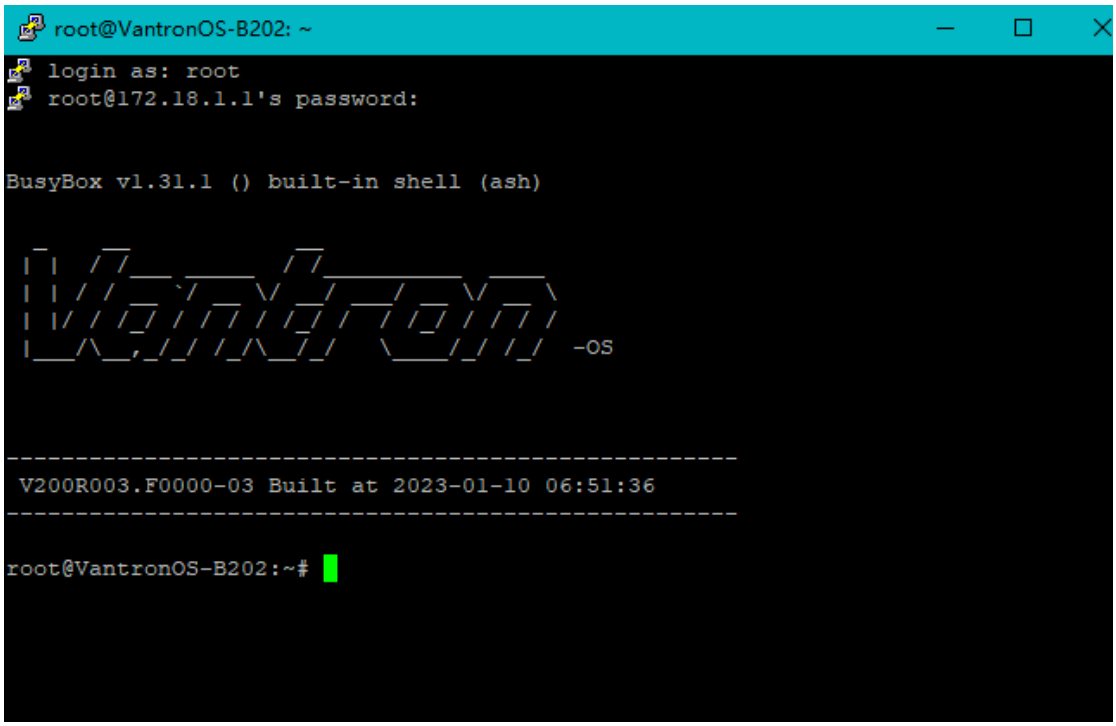
Step 4: Open an SSH client (PuTTY or MobaXterm recommended) in the Windows host;

Step 5: Input the host name or IP address (LAN port address by default: 172.18.1.1), keep the default port No. (22), and select **SSH** for the connection type;

Step 6: Set the session name and **Save**, keep the other settings unchanged, then click **Open**;

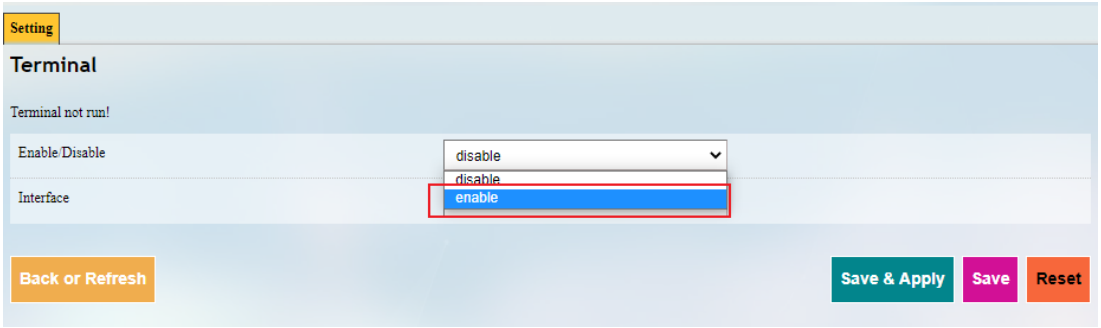


Step 7: Log in to the root account (password same as the gateway login password as shown above), and start an SSH remote session.



3.13.4 Terminal

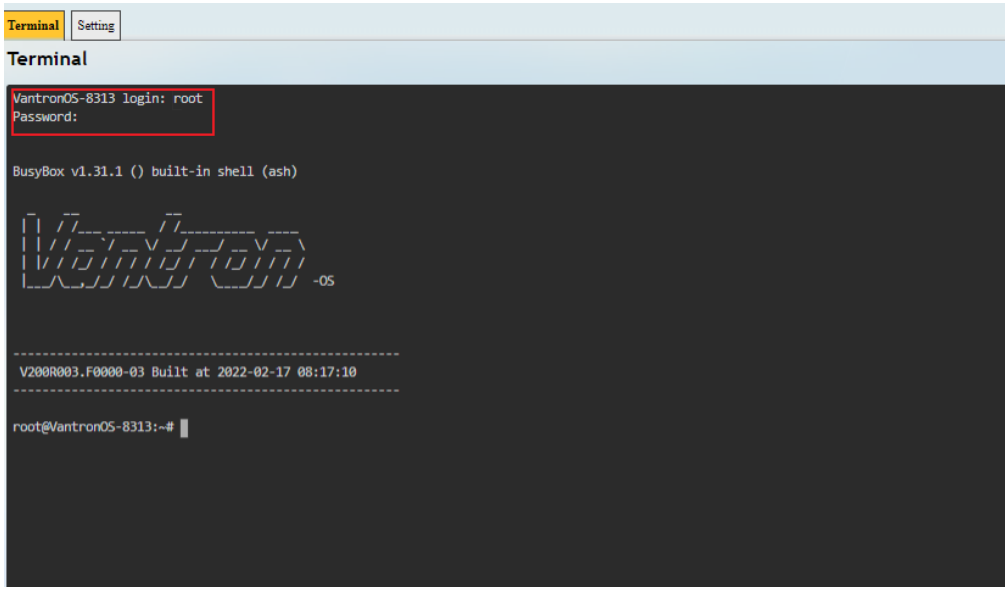
Under the **Setting** tab, users can click **enable** from the drop-down box and **Save & Apply** to enable the web terminal and input command lines here.



After the web Terminal is enabled, the **Terminal** tab will be available next to the **Setting** tab.

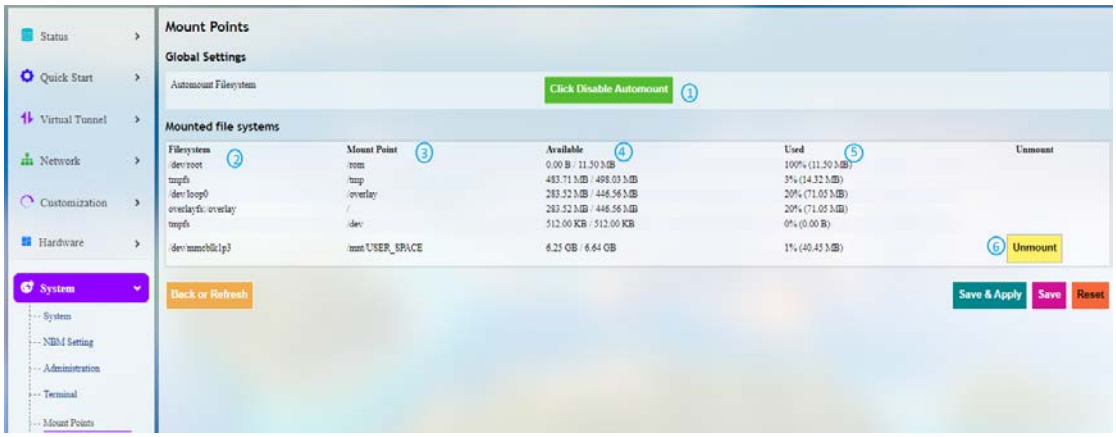
Login name: root

Login password: rootpassword (invisible while typing)



3.13.5 Mount points

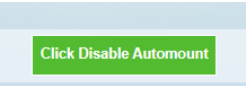
You can enable/disable automount and check the mounting information here.

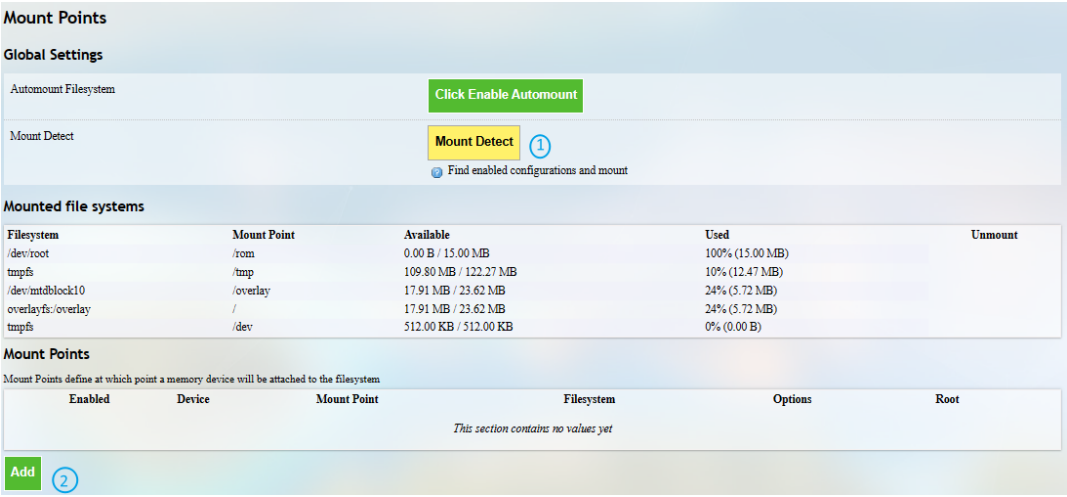


Description of the numbered areas

1. Disable/Enable automatic mount
2. File path on the Router
3. Mount point
4. Available space in the mount point
5. Space used in percentage
6. If you have previously mounted a file to the device, you can manually unmount the file here

To manually mount a file, click the **Click Disable Automount** button first and then proceed with the settings.

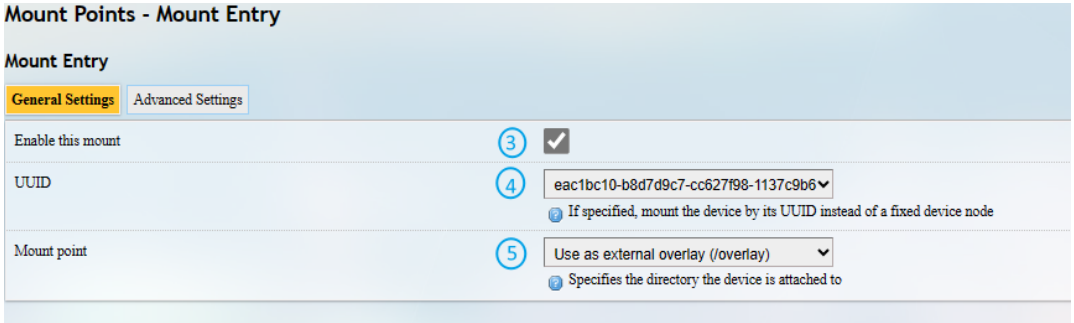




Description of the numbered areas

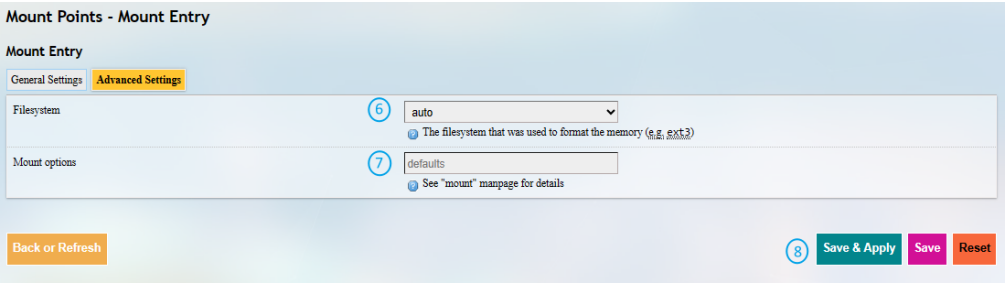
1. Detect the available mount points
2. Click **Add** to add a mount point

Click the **Edit** button behind the newly added mount point for more settings.

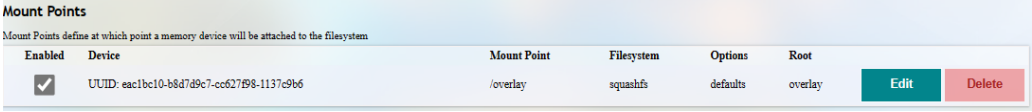


3. Check the box to enable the mount point after creation
4. Select the UUID of the device
5. Select the mount point

Then click the **Advanced Settings** tab to access advanced settings.



6. Select the file system for formatting the memory
7. Input the mount options
8. Save the settings and click the **Back or Refresh** button to return to the general settings

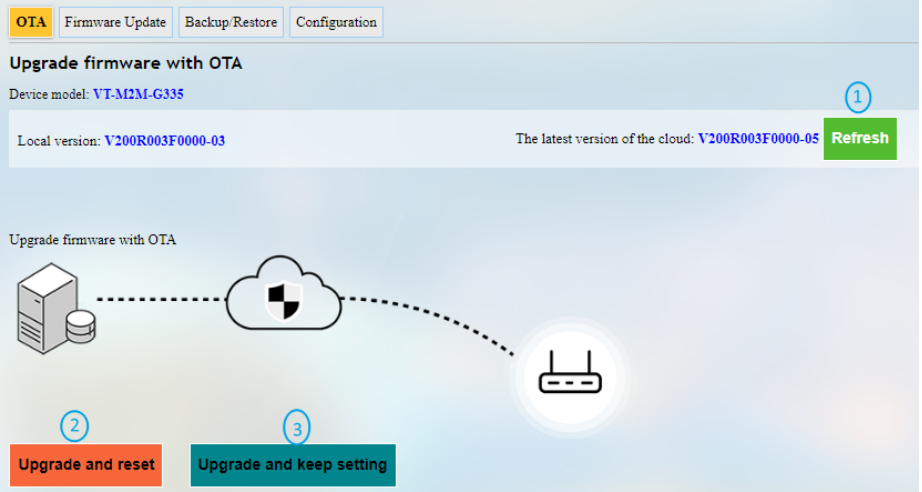


The mount point is created as above.

3.13.6 Backup/Flash firmware

On this page, you can backup/restore parameters, restore factory settings (clear user settings), and update firmware from the local or with OTA.

OTA upgrade

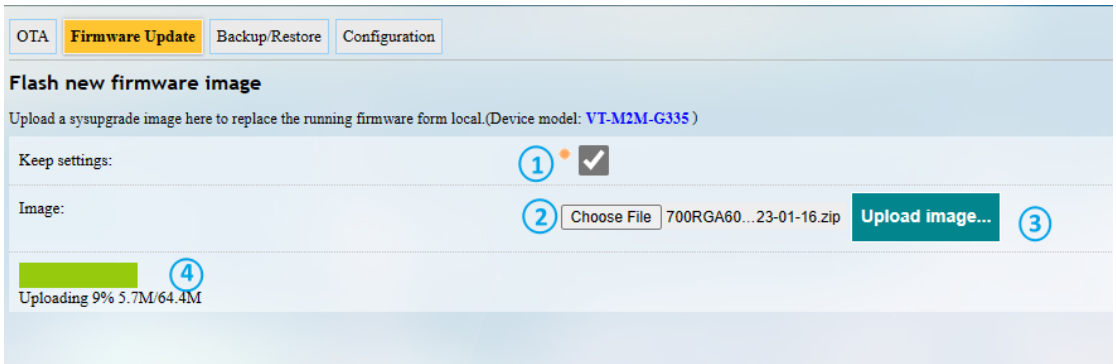


Description of the numbered areas

1. Refresh the cloud version to the latest (internet access required)
2. Upgrade the Gateway and reset to default settings
3. Upgrade the Gateway and keep the existing settings unchanged

*If the version from the cloud is shown **Failure**, please check if the Gateway has internet access.*

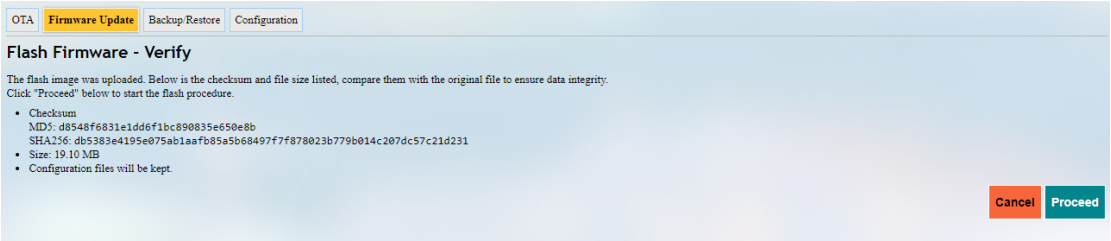
Firmware Update



Description of the numbered areas

1. Check the box to keep the user settings while upgrading the device (not recommended)
2. Select the firmware from the local directory
3. Click the button to upload the firmware
4. Upload progress of the package

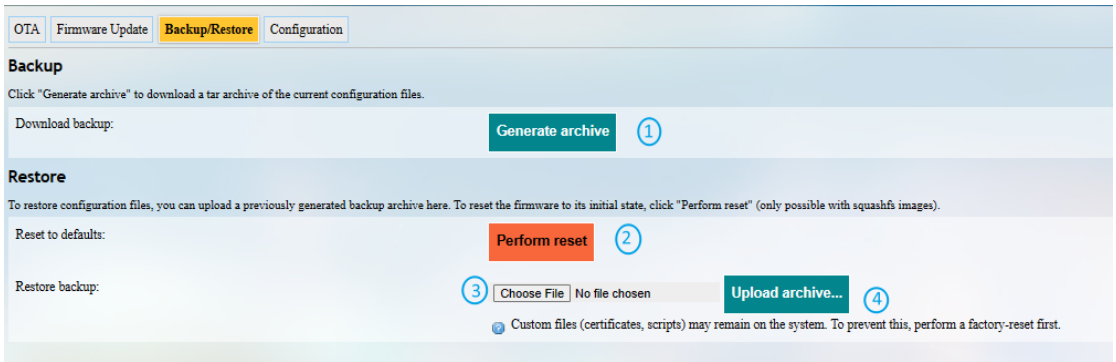
When the detailed information of the firmware is displayed, check if the firmware is correct, then click **Proceed** to start the upgrading. DO NOT power off the Gateway when firmware upgrading is in process. The login page will be refreshed once the upgrading finishes.



It will take some time for the upgrade and DO NOT power off the Router when firmware upgrading is in process;

The login page will be refreshed once the upgrading finishes and you can login to check the firmware version on the homage.

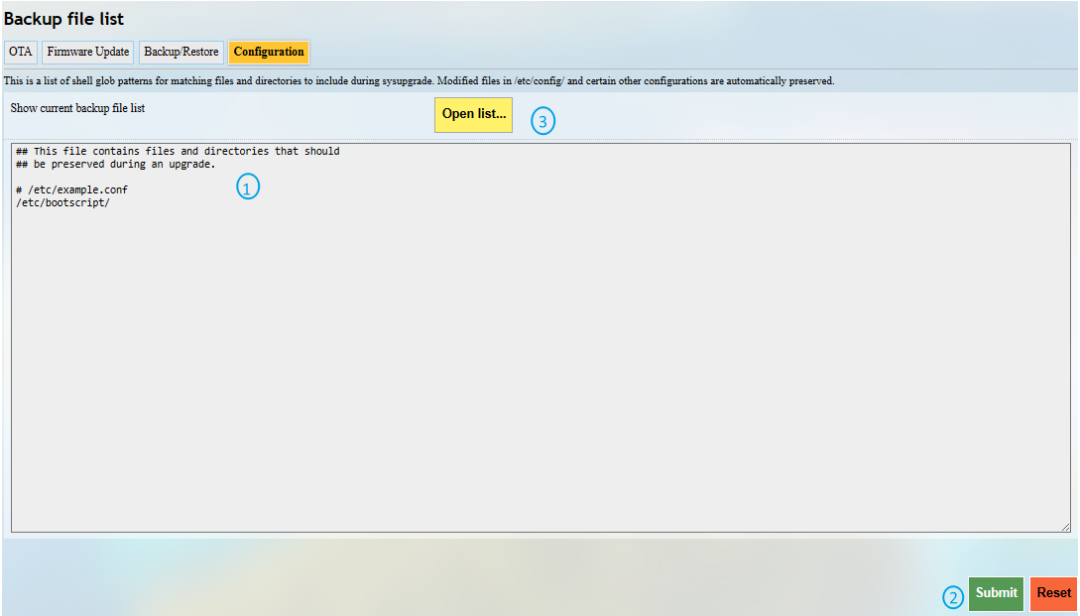
Under the **Backup/Restore** tab, you can download the backup package of your settings, including configuration files and pre-set folders, restore the factory settings of the Router, and upload the backup package saved before.



Description of the numbered areas

1. Click the button to back up the system configurations (include only the configuration files and preset files other than client files or programs)
2. Factory reset the Router (user configurations will be cleared)
3. Select the backup file from the local directory to restore the backup settings
4. Upload the file

Under the **Configuration** tab, you can customize the configuration files or directories to be retained during the upgrade.



Description of the numbered areas

1. Input the configuration file or directory to be retained during the upgrade
2. Click **Submit** to confirm the setting
3. Open the list of configuration files kept during the upgrade

3.13.7 Reboot

Make sure you don't have any ongoing process before rebooting the Gateway.

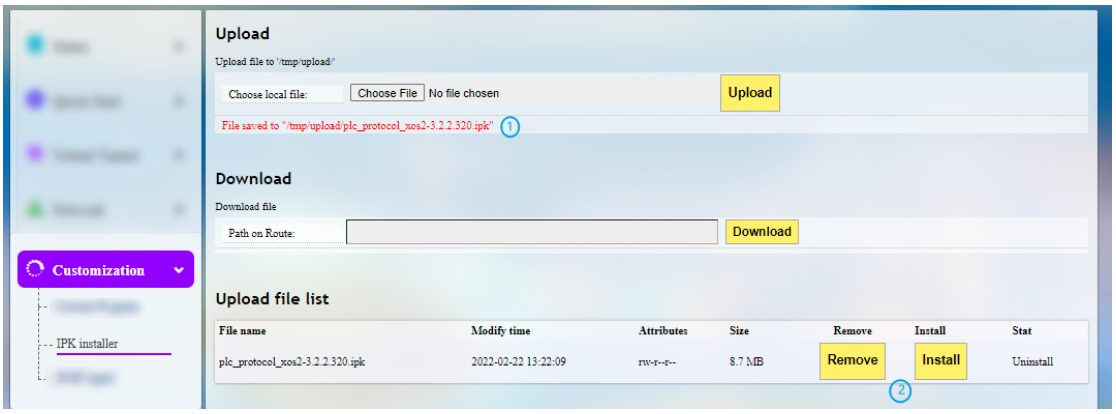
3.14 Logout

You will exit the web interface with a click on the **Logout** tab. If you need make changes to any of your settings, you can log in the web again with default password: **admin**.

CHAPTER 4 INDUSTRIAL PROTOCOL CONFIGURATIONS

4.1 IPK Installation for Industrial Protocols

In VantronOS web interface, navigate to **Customization > IPK installer**, select and upload the .ipk file for industrial protocol configuration.



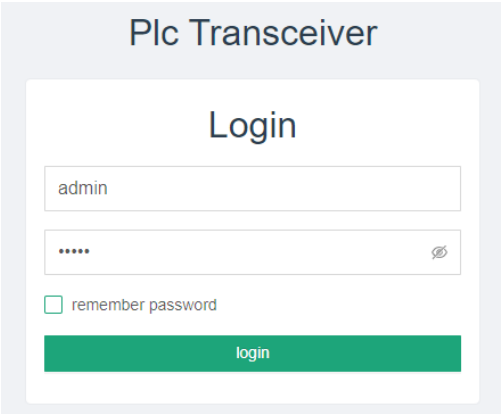
Description of the numbered areas

1. After the .ipk file is uploaded to the Gateway, the directory of the file will be displayed
2. You can remove or install the .ipk thereafter

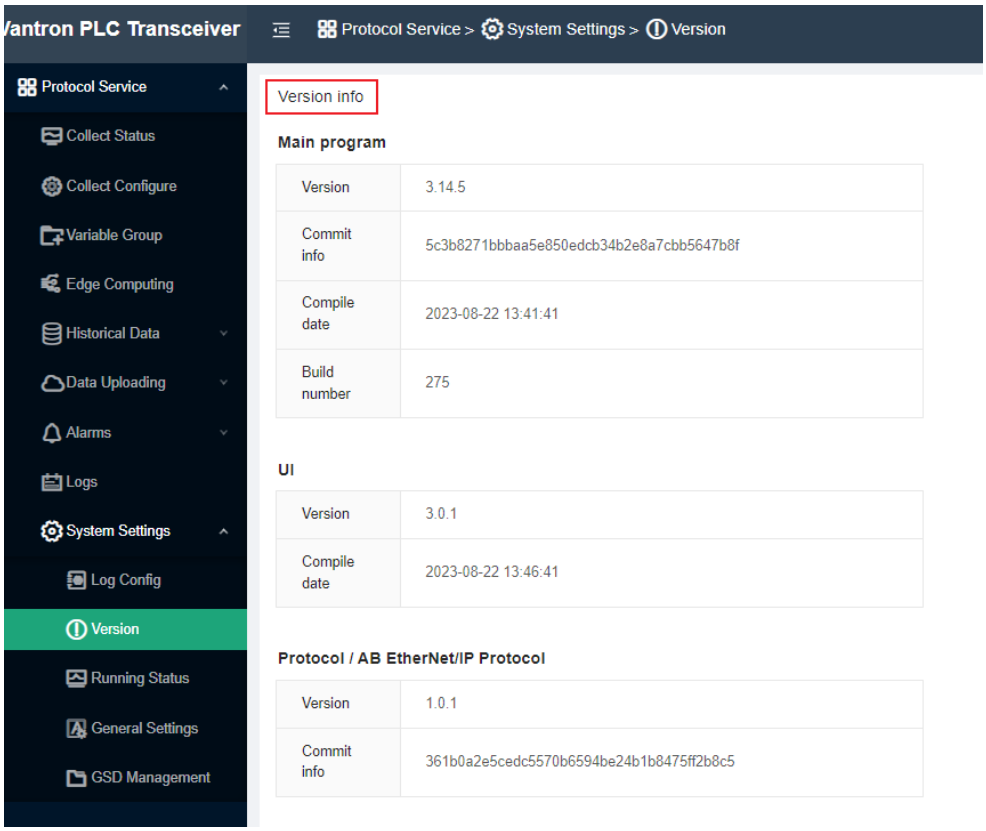
Once the .ipk file is installed, a message will be displayed suggesting the status of the file installation as shown below.

Input the port number (8081) after the LAN port IP of the Gateway in the address bar of a browser (for instance: 172.18.1.1:8081), and input the account and password to login.

- Account: **admin** / **root**
- Password: **admin** / **rootpassword**

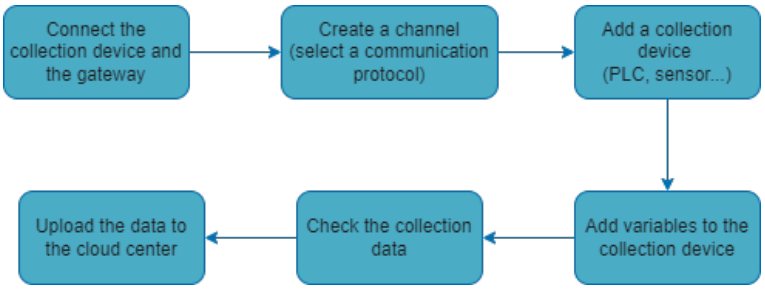


You can check the version information of the protocol package under **System Settings**.



4.2 Protocol Configuration and Application

To use a protocol for data acquisition and edge computing, figure out the device model you are using for data collection and configure the protocol accordingly.

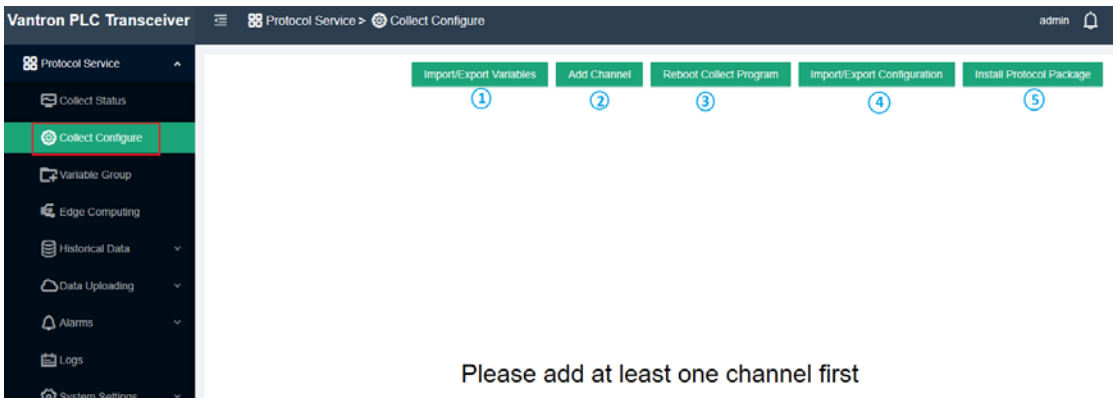


Prerequisites:

- A G335 gateway
- A data collection device
- A serial connection cable/Ethernet cable (depending on the protocol you're using)
- Connect the data collection device to G335 via the serial connection cable/Ethernet cable

4.2.1 Configuration of Collection Channels

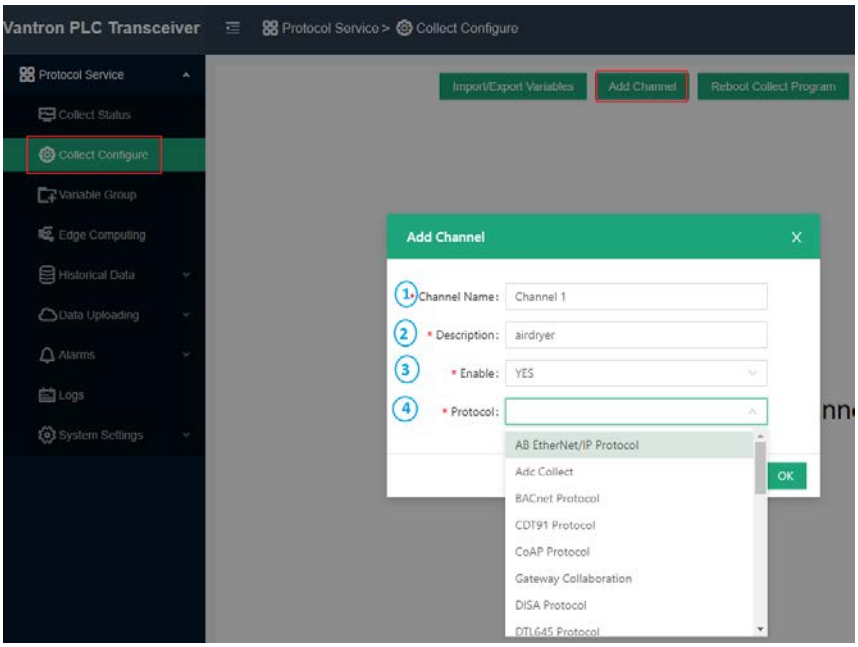
If you are using the portal for the first time, click **Collect Configure** on the menu pane and you will be prompted to add a channel for data collection.



Description of the numbered areas

1. Import the previously saved variables/export the current variables
2. Create a collection channel
3. Restart the collection program (the collection channel and task will be restarted)
4. Import the previously saved configurations/export the current configurations
5. Upload a protocol package (You can upload packages containing additional protocols that are not included in the default collection channels, or updated packages for existing protocols)

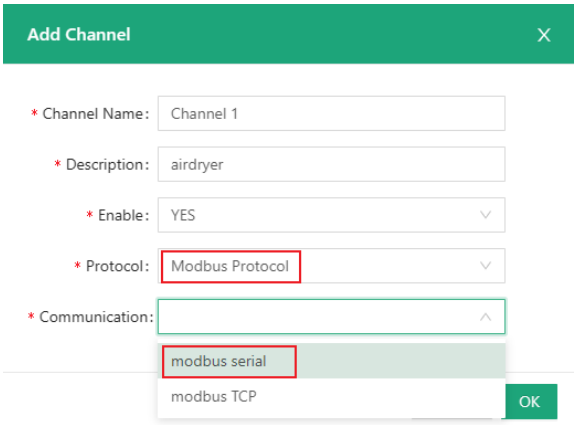
Click the **Add Channel** button (circled as (2) in the above screenshot) to add a channel.

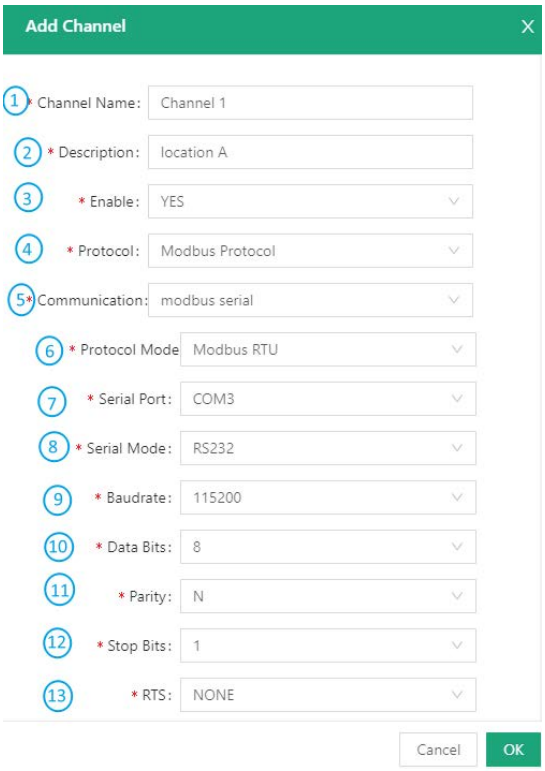


Description of the numbered areas

1. Enter a channel name that shall not be any one of the names in use
2. Describe the channel
3. To enable the channel or not ('Yes' by default)
4. Select a protocol type from the drop-down list based on the model of the data collection device (the protocols are supported by the .ipk file installed)

Certain protocols may require more configuration parameters. For example, if **Modbus RTU** protocol is selected as the communication protocol, you will need to connect the data collection device to the Gateway via the serial ports. When configuring the protocol, make sure to select "Modbus" as the protocol and "Modbus serial" as the communication type to ensure proper communication.

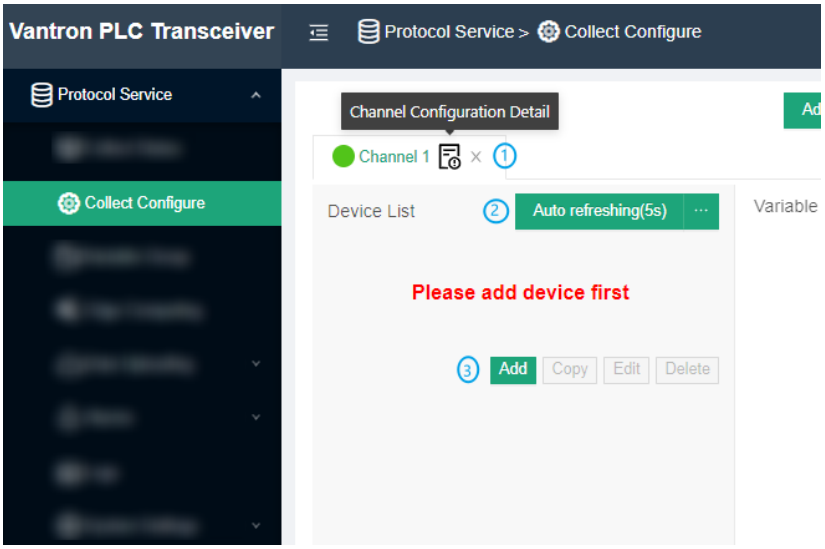




Description of the numbered areas

4. Select Modbus protocol from the drop-down list
5. Choose serial communication as the communication type
6. Select Modbus RTU as the protocol mode
7. After the collection device is connected to the gateway, select the correct serial port from the drop-down list that corresponds to the serial port in use on the gateway
8. Determine the mode of the serial port (the serial mode is determined by the serial port in use)
9. Choose the baud rate of the serial port in use
10. The data bit in communication (8 bits for RTU communication by default)
11. There are three parity bits: even (E), odd (O), and non-parity (N)
12. The stop bit represents the last bit in a single package, and the typical value includes 1, 1.5 and 2
13. Select to enable request to send (RTS) protocol or not

After the configuration of the protocol channel, the channel will be displayed on the interface. You can make subsequent changes to the channel like deletion or edition.

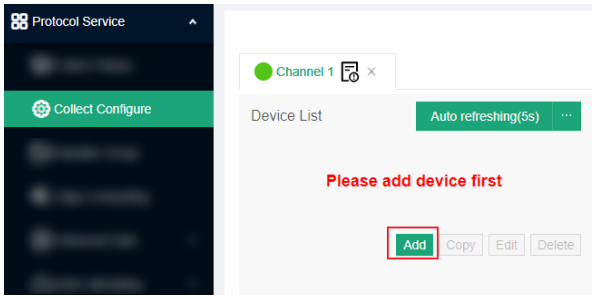


Description of the numbered areas

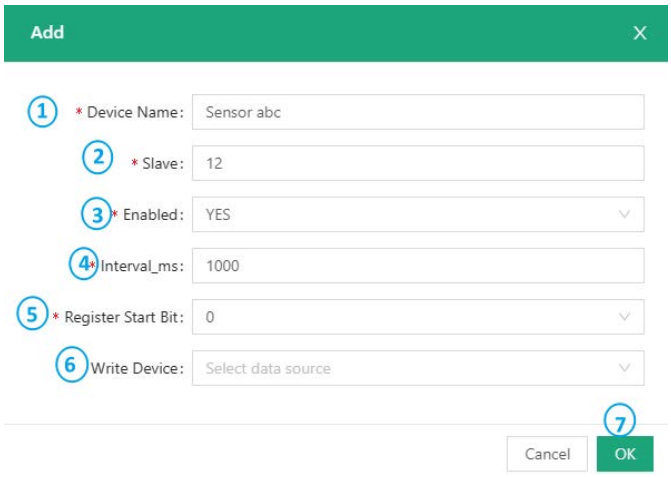
1. Delete the channel (x) or access the detail page ( )of the channel and make changes accordingly, including disabling the channel
2. The channel is set to refresh automatically every 5 seconds, and you can assign an optional value between 1 and 99 for auto refreshing by clicking the (…) button
3. Add a device (e.g., a PLC/sensor) for data collection

4.2.2 Configuration of Collection Devices

After creating a channel, the collection device that connects to the Gateway can be added to the channel. Click the **Add** button under **Device List** and input the device information in the pop-up.



The device information to be input varies with the protocol you added for communication (still take Modbus RTU protocol as example).

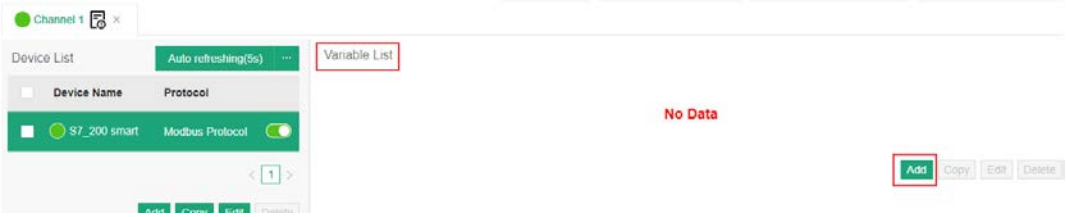


Description of the numbered areas

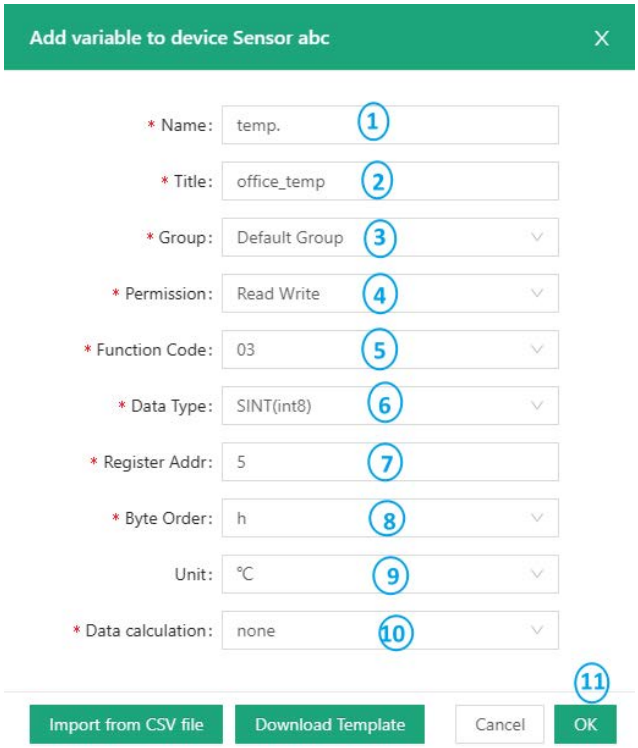
1. Enter a device name
2. Input a slave address between 0 and 255
3. Choose to enable the device or not
4. Set an interval for data collection (better to leave it as is)
5. Set a start bit for the register (better to leave it as is)
6. Select the data source for distribution (unless there is collected data)
7. Click **OK** to complete adding the device

4.2.3 Adding Variables to the Collection Device

After configuration of the data collection devices, click the **Add** button under **Variable List** on the right side of the interface to set the variables for the collection device.



Set the parameters of the variable in the pop-up window.



Description of the numbered areas

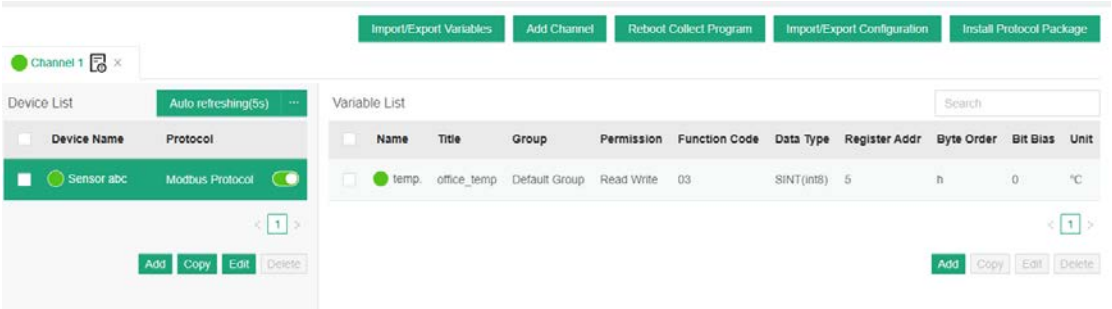
1. Set a variable name that the device collects
2. Enter a title to describe the variable
3. Select a group for the variable (create groups first via the **Variable Group** tab on the left side)
4. Set the access permission of the variable
5. Select a function code
6. Choose the data type (determined by the collection device)

7. Input or adjust the register address from 1 to 65535
8. Set the byte order
9. Select a unit for the variable (determined by the collection device)
10. Set a method for data calculation

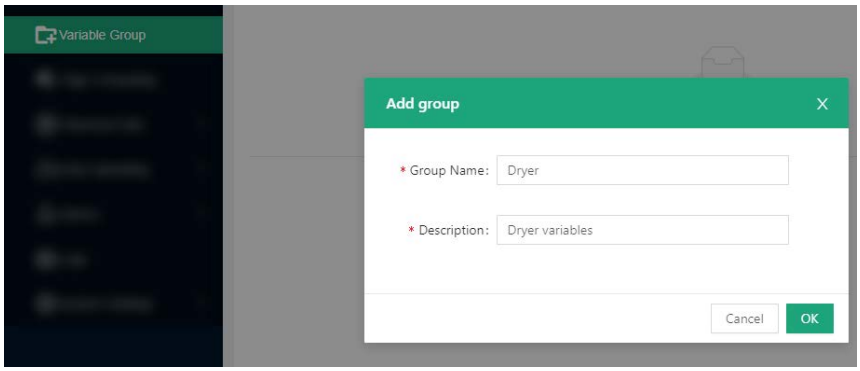
If case you are unsure where to start for the first-time setup, you can download the template as a reference for the required fields when creating a CSV file, then upload the CSV file for bulk setup of the variables.

For fields that require manual input of the information, please avoid using special characters.

After completing the configurations, refresh the portal to check the collection settings or add/copy/edit the variables.

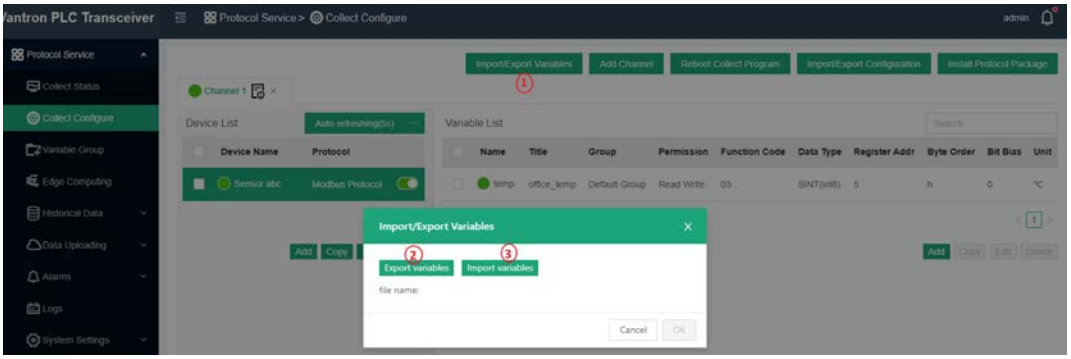


If multiple variables are involved, you can add variable groups for different variables from the **Variable Group** tab on the left side.



4.2.4 Variable Import and Export

To ensure smooth importing of batch variables, it is recommended to export the existing variables to the local directory first. This allows you to review the format and configurations, make any necessary modifications, and upload the file to the portal for bulk variable additions.



Description of the numbered areas

1. Navigate to **Collect Configure > Import/Export Variables**
2. Export the variables (file saved as “all_variables.csv”)

Channel N	Device Na	Name	Title	Group	Permissio	Function (	Data Type	Convert S	Length	Register A	Byte Orde	Bit Bias	Unit	Word base	Data calculation
Channel 1	Sensor ab	temp.	office_ter	default_gr	rw	holding	char		1	5	h	0	℃		
Channel 1	Sensor ab	temp	outdoor_t	default_gr	rw	holding	uint16		1	33	hl	0	℃		
Channel N	Device Na	Name	Title	Group	Permissio	Function (	Data Type	Convert S	Length	Register A	Byte Orde	Bit Bias	Unit	Word base	Data calculation
Channel 2	S7_200 sm	hmdty	warehous	default_gr	rw	holding	uint16		1	7	lh	0	%RH		

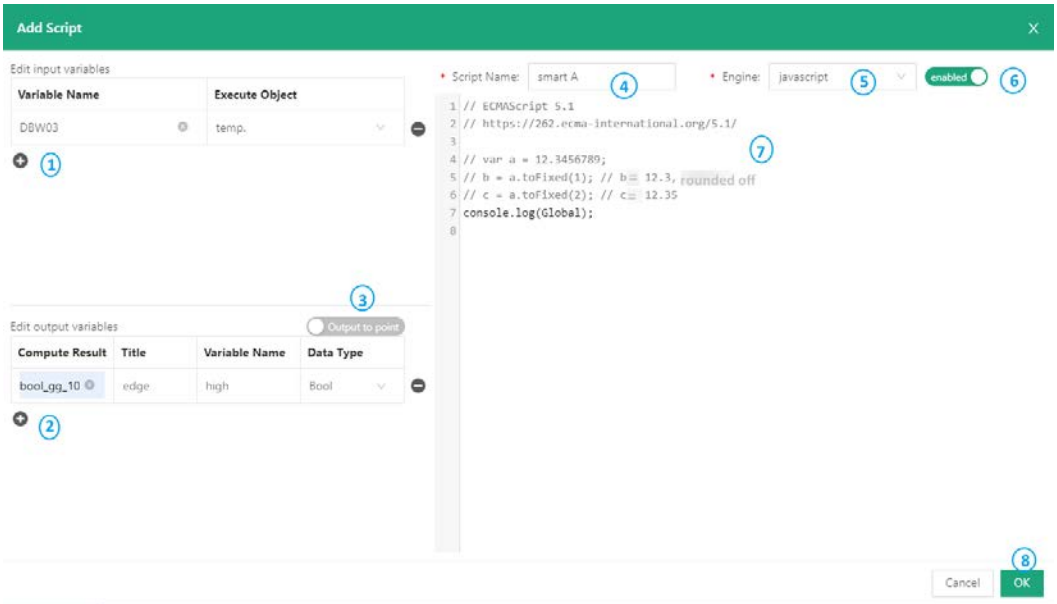
The channel name and device name are unchangeable. You can add variables to the corresponding devices (duplicated names are not allowed).

3. Select the CSV file from the local directory and click **OK** to exit

The import and export of channel configurations are similar as importing and exporting the variables except that the file is in .bin format.

4.2.5 Edge Computing Scripts Setup

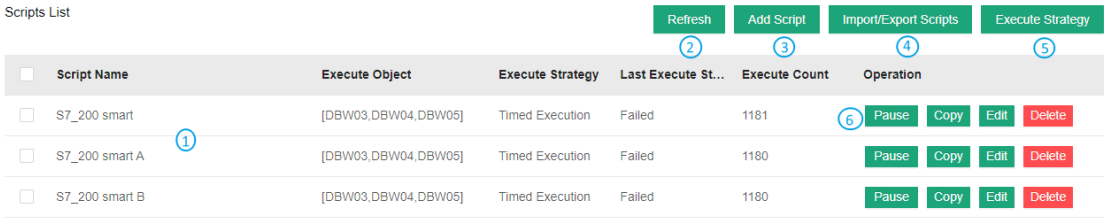
To add a script for edge computing, you need click **Edge Computing** from the navigation pane on the left, then click **Add Script** to input the script information in the pop-up.



Description of the numbered areas

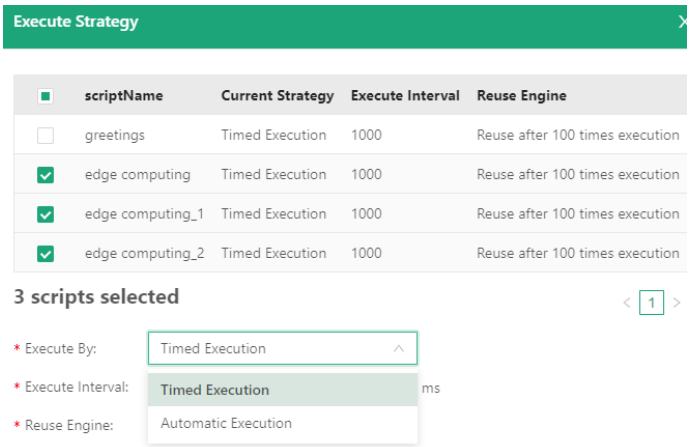
1. Edit the input variables: add a name for the input variable and an object for executing the script (more than one variable could be added)
2. Edit the output variable: add the computation result, title, variable name, and data type
3. Click the toggle button to choose to output the results to the variables or edge nodes
4. Enter a name for the computing script
5. Select the format of the script (JavaScript, Lua and Python supported)
6. Select to enable the script or not
7. Compile the script in the window
8. After compilation, click **OK** to exit

Under **Scripts List**, you can perform a series of actions to the scripts.



Description of the numbered areas

1. Script list and detailed script information
2. Refresh the scripts
3. Add a script
4. Import/export scripts
5. Script execution strategy (you can assign a strategy to multiple scripts upon a click of this button)



The scripts are designed to be executed automatically or at a scheduled time.

Automatic execution: triggered when there is abnormality with the execution object.

Timed execution is supposed to be used together with the **Execution interval:** the system is scheduled to execute the script every 1000ms by default, and you can adjust the interval.

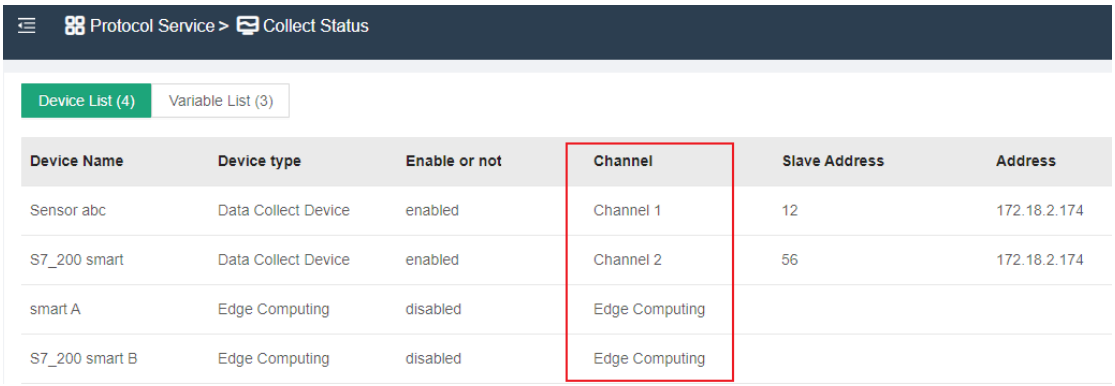
Reuse Context allows you to set a restart mechanism for the scripts

6. Start/pause, copy, edit or delete the script. (You can access the script information and the execution log upon a click of the **Edit** button)

4.2.6 Collection Status

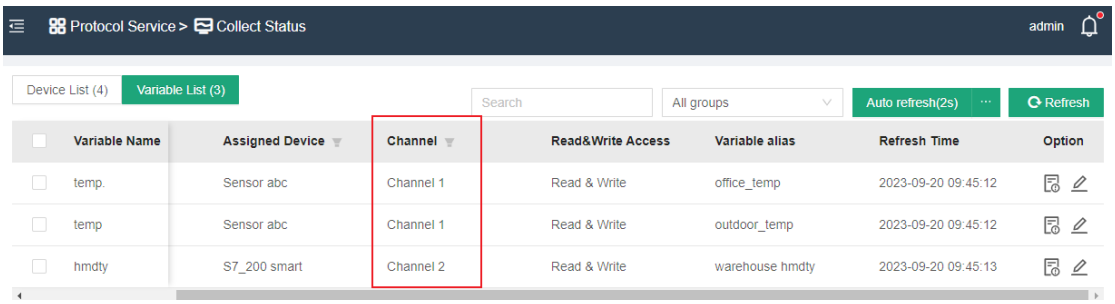
When the setup finishes, you can check the information about the devices and variables by clicking the **Collect Status** tab on the left.

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



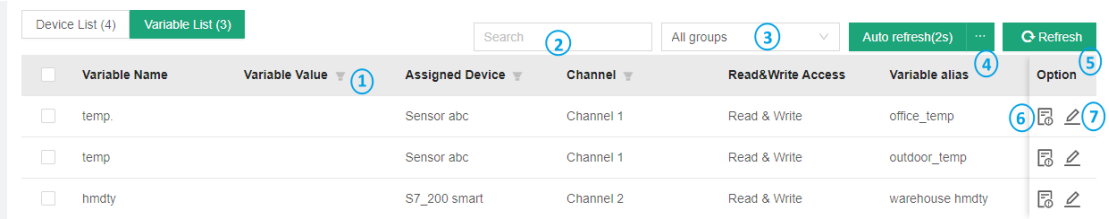
Device Name	Device type	Enable or not	Channel	Slave Address	Address
Sensor abc	Data Collect Device	enabled	Channel 1	12	172.18.2.174
S7_200 smart	Data Collect Device	enabled	Channel 2	56	172.18.2.174
smart A	Edge Computing	disabled	Edge Computing		
S7_200 smart B	Edge Computing	disabled	Edge Computing		

The **Variable List** displays information about the variables, collection devices, user permission to the variables, etc. Users can differentiate the data based on the collection channels.



Variable Name	Assigned Device	Channel	Read&Write Access	Variable alias	Refresh Time	Option
temp.	Sensor abc	Channel 1	Read & Write	office_temp	2023-09-20 09:45:12	
temp	Sensor abc	Channel 1	Read & Write	outdoor_temp	2023-09-20 09:45:12	
hmdty	S7_200 smart	Channel 2	Read & Write	warehouse hmdty	2023-09-20 09:45:13	

The **Variable List** offers the user more feasibility to set or access the variables.

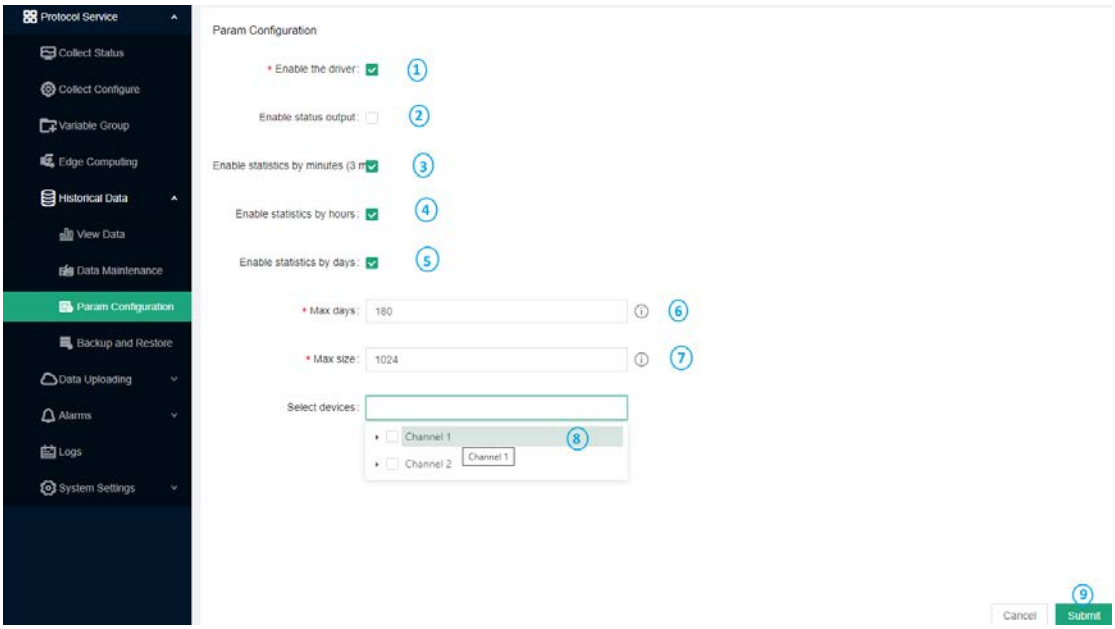


Description of the numbered areas

1. Use the filters to screen out the target information (you can screen variables, collection devices, channels)
2. Fuzzy search for the target variable
3. Select a variable group
4. Click ... to set the Auto refresh interval
5. Manual refresh
6. Variable details
7. Data distribution settings (you can tick the checkboxes before multiple variables to distribute a value to the target device)

4.2.7 Historical Data

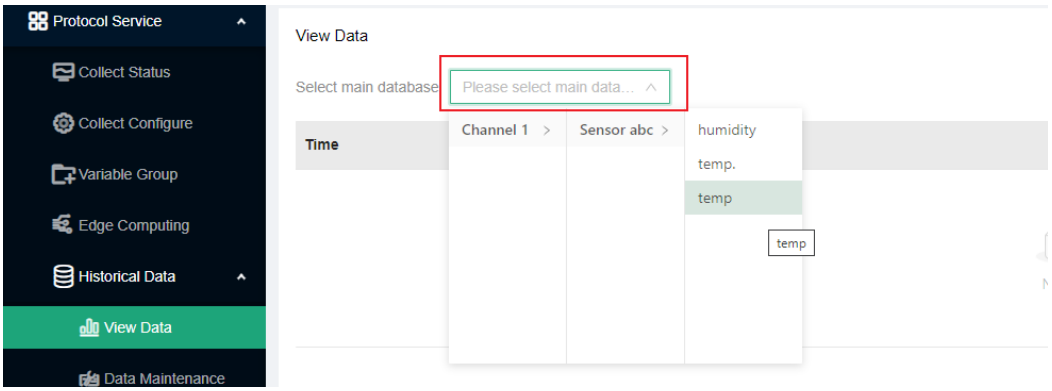
Users can access, delete, or back up historical data from the **Historical Data** tab. Before you proceed with the operations, please navigate to **Param Configuration** to enable the feature and select the configuration channel.



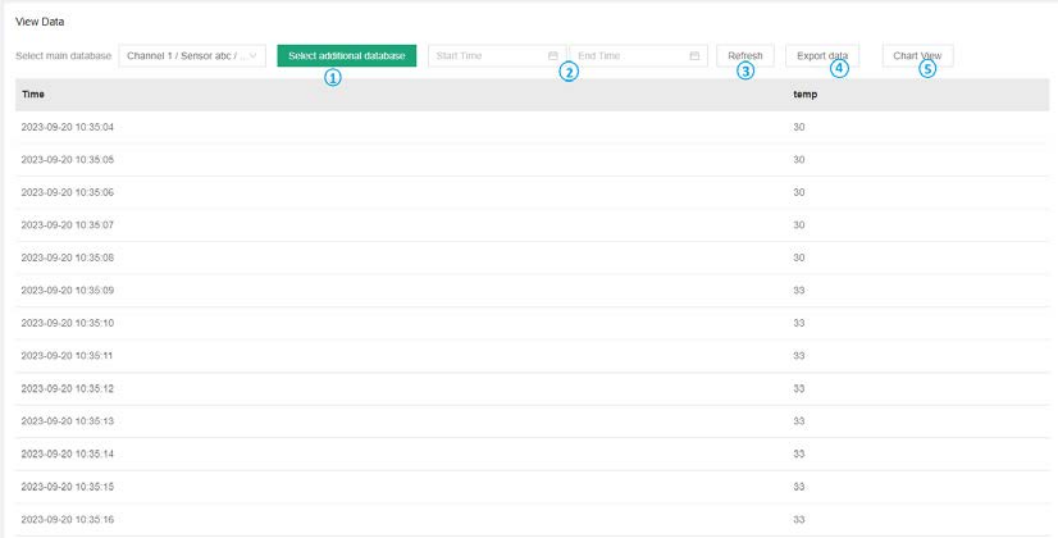
Description of the numbered areas

1. Enable/Disable the historical data feature (only when this feature is enabled can you access the historical data)
2. Enable/Disable status output (you can keep the default setting)
3. Enable/Disable data statistics on a 3-minute basis (you can keep the default setting)
4. Enable/Disable data statistics on a hourly basis (you can keep the default setting)
5. Enable/Disable data statistics on a daily basis (you can keep the default setting)
6. Input the maximum days you would like the data to be stored ('0' means no limit on the days)
7. Input the maximum size you would like to store the data (Unit: M)
8. Select the channel/device you would like to access the historical data
9. Click **Submit** to save and apply the settings

Then, you can navigate to the **View Data** tab and select the channel you have selected with the variable(s) you wish to check.

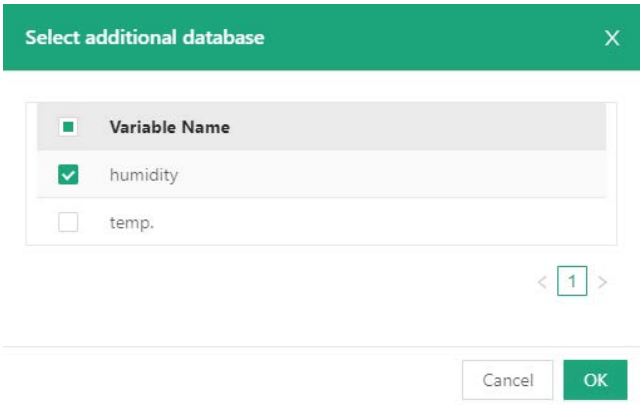


The data will be displayed in a few seconds.

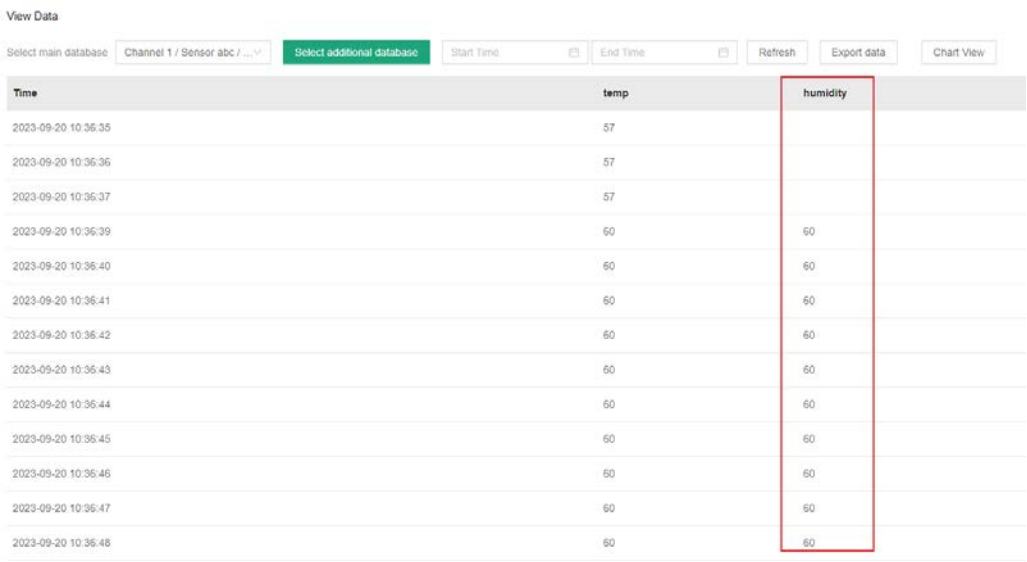


Description of the numbered areas

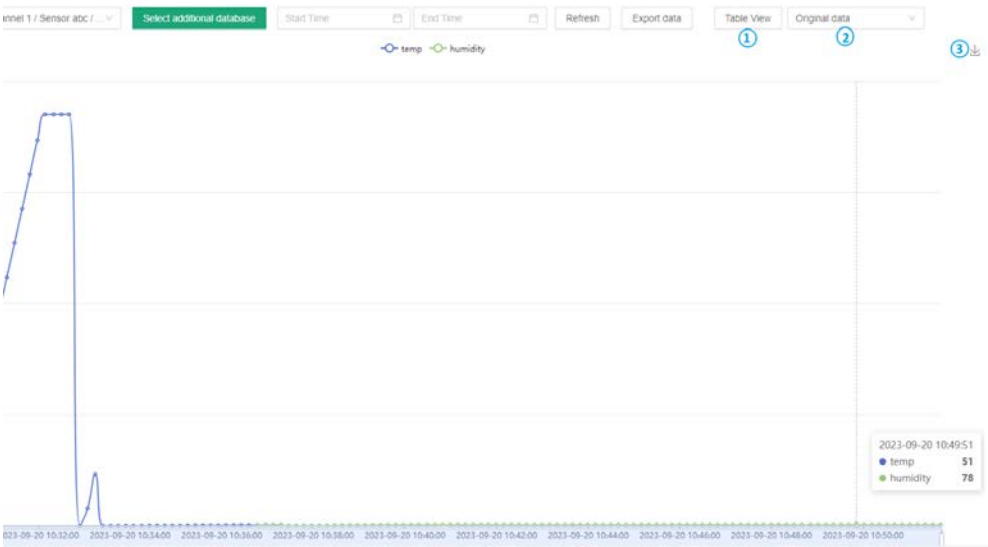
1. If the collection device collects multiple variables, you can click this button to add more variables



After the variable is added, there is another column displaying the target variable.



2. Select a period for displaying the relevant data
3. Manually refresh the data
4. Export the data to the local directory
5. View the data in the chart (click **Table View** to return to the list)



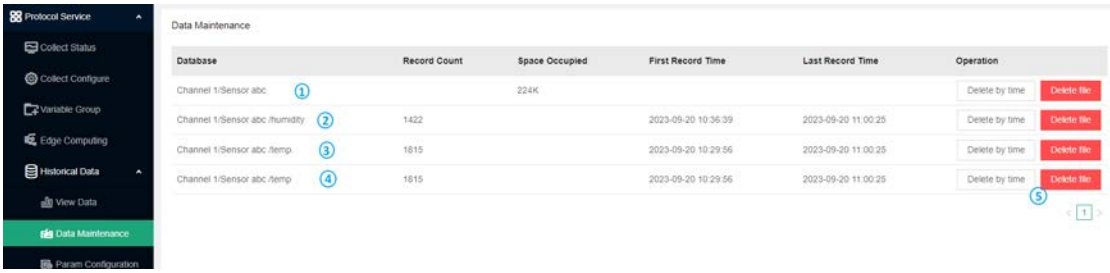
When you view the data in the chart, you can perform the following actions:

(1) Return to the list view

(2) Access the Max./Min./Average data in minutes/hours/days

(3) Export the chart to the local directory in .svg format

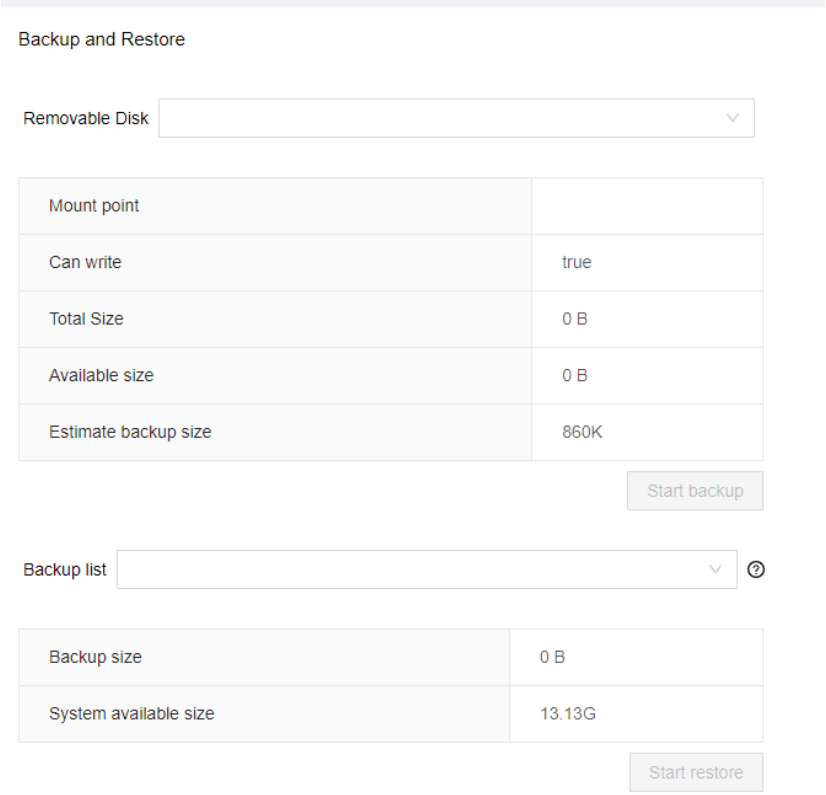
After the historical data is stored for certain time, you can navigate to **Historical Data > Data Maintenance** to delete the data of a specific time or delete the entire data file.



Description of the numbered areas

1. The space occupied by all data in a channel
2. Record count of a single variable in the channel (e.g., humidity)
3. Record count of a single variable in the channel (e.g., temperature)
4. Record count of a single variable in the channel (e.g., temperature)
5. Delete the data file (the buttons behind the channel allow you to delete the data file of the entire channel while the buttons behind a single variable allow you to delete the data associated with the variable)

In the **Historical Data > Backup and Restore** interface, you can back up or restore the historical data.



Before backing up the data, you will need to mount the storage device to the Gateway.

1. Insert the Micro SD card into the corresponsive slot on the Gateway;
2. Login VantronOS and navigate to **System > Mount Points**;
3. The automatic mounting feature is turned on by default, you can check the information here;

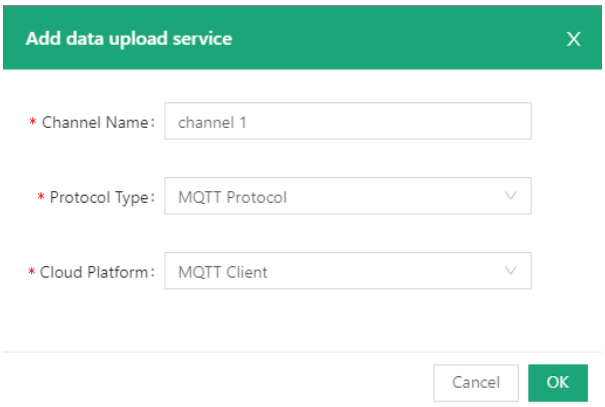
4. Go back to the protocol portal, select the removable disk and start the backup;
5. You can also select the backup data from the list and restore the related data.

4.2.8 Data Upload and Encapsulation

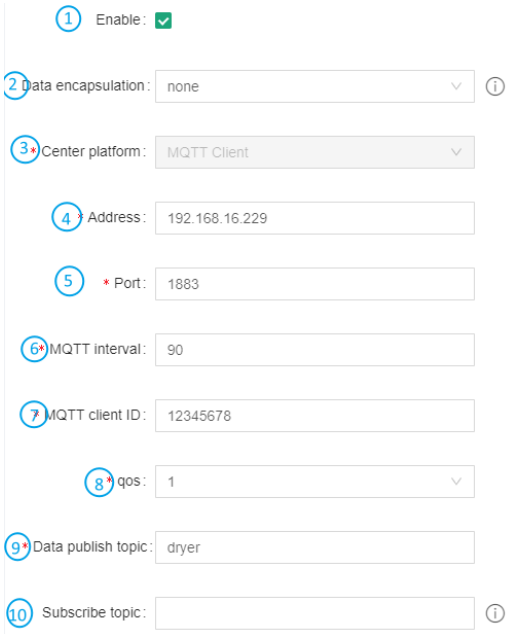
Field data collected will be uploaded to the cloud platform via protocols after edge computing. Take MQTT protocol as an example, follow the steps below for relevant settings.

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

- Create an upload task in the pop-up and click **OK**;



- Configure the MQTT client in the following pop-up.



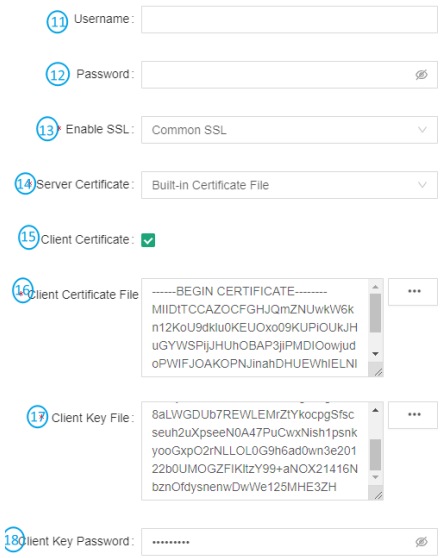
Description of the numbered areas

1. Select to enable data uploading or not after the configuration, and the data collected will be automatically uploaded to the cloud platform if enabled
2. Determine the data encapsulation format (no format by default)
3. The center platform is automatically filled and not changeable
4. Fill in the IP address of the MQTT server
5. The port number is automatically filled (1883)
6. The client will send a message to the server within a heartbeat interval (90 seconds by default and adjustable), otherwise the client network will be disconnected
7. Input the MQTT client ID: a unique identifier, unrepeatable
8. Set the quality of service (QoS) to ensure the reliability of the message

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

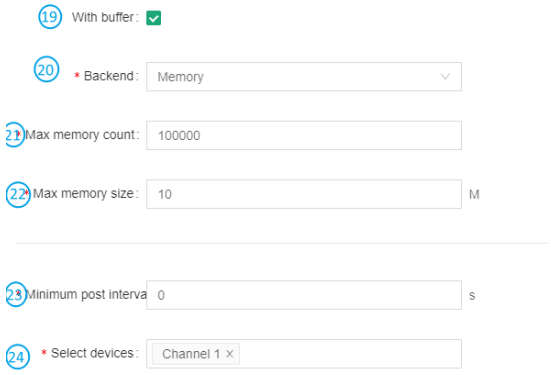
   QoS 1: The message will be sent at least once.

   QoS 2: The message will be sent only once.
9. Data publish topic: used for MQTT messaging to identify which message channel the payload data is supposed to be published
10. Topic for MQTT message subscription which enables the server to send message to a client for the control purpose



11. Input a username (non-compulsory)
12. Input the password (non-compulsory)
13. Select to enable SSL or not (if yes, choose between common SSL and national SSL)
14. If common SSL is enabled, select a certification mode for the server

15. Select to enable client certificate or not
16. If yes, a client certificate file is needed
17. If yes, a client key file is also needed
18. Input a client key password (non-compulsory)



19. Select to enable data caching or not
20. If yes, choose a medium for data caching (caching to memory by default)
21. Determine the maximum memory count
22. Determine the maximum memory size
23. Input a minimum post interval
24. Select the device of the source data

The configurations will take effect after you click **Submit**. Then users can browse the data uploaded to the MQTT platform for data view, statistics, analysis, etc.

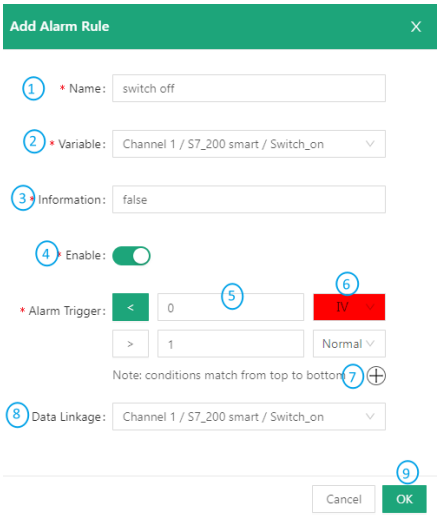
In the Data Encapsulation page, you can upload encapsulated data or configure the encapsulation format of the data.

Description of the numbered areas

1. Description of the built-in data encapsulation format
2. Click to upload. json data for encapsulation

4.2.9 Alarm

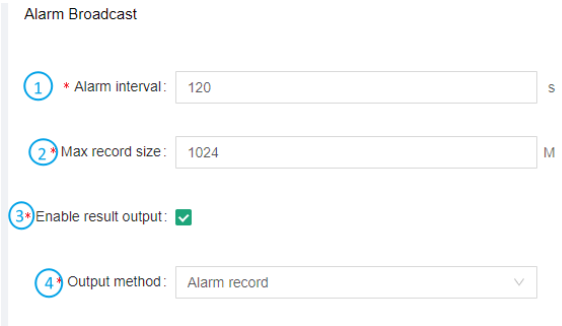
Under **Alarms > Alarm Config**, you can add alarm rules for the variables. The device will alarm when a rule is triggered and the alarm mutes when the condition changes to not meeting the rule.



Description of the numbered areas

1. Set a name for the alarm rule
2. Select the variable for the alarm rule to be applied to
3. Input the alarm message to be display in case of an alarm
4. Select to enable the alarm rule or not
5. Set the thresholds for triggering the alarm (thresholds will be applied from top down)
6. Set an alarm level (under normal level, no alarm will be triggered)
7. Click “+” to add a threshold, click “-” to delete a threshold
8. Select a data linkage
9. Click to save the alarm rule

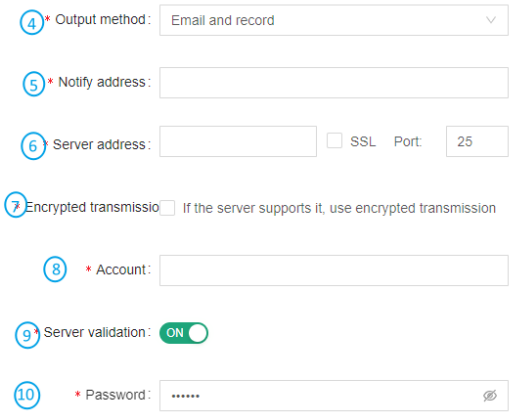
When the alarm rules are created, you can set the parameters for pushing an alarm on the **Alarm Broadcast** page.



Description of the numbered areas

1. Set the interval for an alarm, 120 seconds by default
2. The maximum storage space for the alarm log is 1024M by default
3. Select to enable result output or not
4. Select to output the alarms to the alarm log or alarm log + email

If you choose the latter, please add information about the email.



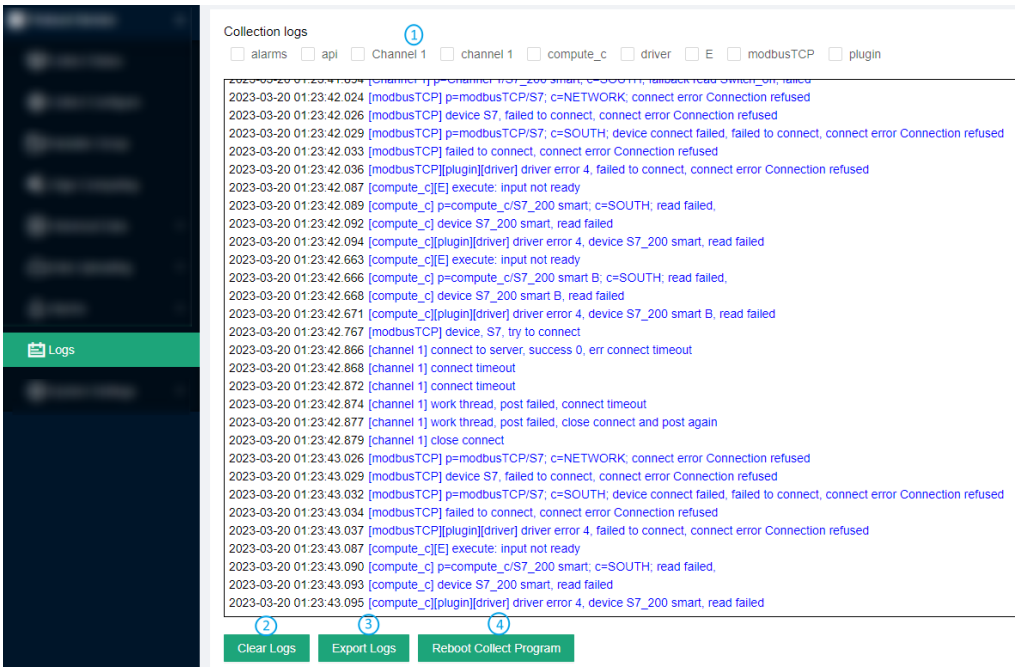
5. Input an email account for receiving the alarm messages
6. Input the outgoing server address (check the settings of the email server in use)
7. Enable encrypted transmission if the server supports
8. Input an email account for sending the alarm messages (could be same as the receiving email)
9. Toggle the server validation or not
10. If server validation is enabled, you need set the password

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

The alarm logs will be displayed on the **Alarm Record** page if any rules are triggered.

4.2.10 Logs

Data collection log and cloud service log are displayed on **Logs** page. You can make changes accordingly.



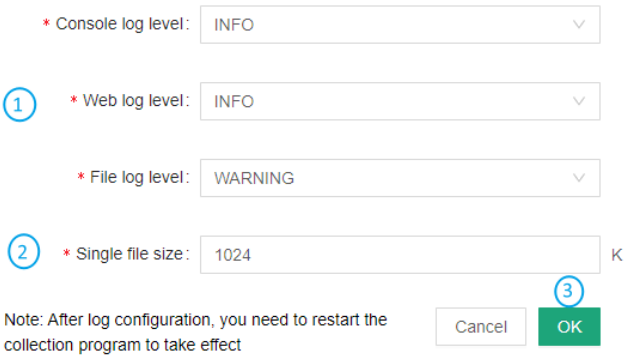
Description of the numbered areas

1. Select one or more checkboxes to screen the data collection logs
2. Clear the logs
3. Export the logs
4. Restart the collection

4.2.11 System Settings

Under **System Settings**, you can configure system parameters and check the system information concerned.

- Log Config.



Description of the numbered areas

1. Select a level for each type of log (including NONE, FATAL, ERROR, WARNING, INFO, DEBUG, TRACE based on the emergency level)
2. Set the size of a single log (1024K by default)
3. Click **OK** to save the settings

If you have changed the settings, be sure to return to **Logs > Reboot Collect Program** to restart the collection to make the settings valid.

- Log Storage

  In the **Log Config > Log Storage** page, users can delete or download a single log/all logs.

- Running Status

  The **Running Status** page displays the system time, and the start point and running duration of the collection program.

- General Settings

  You can change the system language on the **General Settings** page.

- GSD Management

  Users can upload the general station description (GSD) files on the **GSD Management** page for PROFIBUS DP or PROFINET IO communication.

CHAPTER 5 DISPOSAL AND WARRANTY

5.1 Disposal

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

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

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

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

5.2 Warranty

Product warranty

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

Out-of-Warranty Repair

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

Returned Products

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

Appendix A Regulatory Compliance Statement

FCC Statement

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

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

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

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

APPENDIX B Acronyms

Acronym	Description
RXD	Receive data
TXD	Transmit data
GND	Ground
ISO-GND	Isolated ground
NC	No connection