# R105 Industrial Router

# User Manual

Version: 1.2

## Revision History:

| No. | Software Version | Description | Date |
|---|---|---|---|
| V1.0 | V200R003 | First release | Jun. 2, 2023 |
| V1.1 | V200R003 | 1. Deleted Firewall zone related description as per design change;<br>2. Added blacklist and whitelist description to the Firewall section. | Apr. 4, 2023 |
| V1.2 | V200R004 | 1. Modified Overview menu description;<br>2. Deleted Quick Start for networking;<br>3. Modified Auto routing description;<br>4. Updated 4G/LTE description;<br>5. Added Diagnostic description;<br>6. Added IPSec setup description. | Jul. 11, 2023 |

# Table of Contents

# Foreword

Thank you for purchasing R105 Industrial Router ("the Router" 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
- 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
- IC
- PTCRB

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

## Symbology

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

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

## General Safety Instructions

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

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

## Precautions for Power Cables and Accessories

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

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

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

⚠ Cleaning instructions:

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

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

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

⚠ Do not use in combustible and explosive environment:

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

# CHAPTER 1 HARDWARE DESCRIPTION

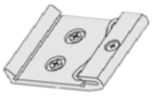
## 1.1 Product Overview

Vantron R105 industrial router offers different options for industrial IoT connectivity, including cellular, Wi-Fi, Ethernet, and virtual private network (VPN) to meet diversified networking requirements. It offers mid- and high-speed CAT 4 cellular networks with major carriers supported. It implements 5 gigabit Ethernet jacks, including one LAN port that offers the PoE option to supply up to 30W of power to client devices. With Wi-Fi IEEE 802.11 b/g/n/ac supported, R105 offers IEEE 802.11ax (Wi-Fi 6) as an option to customers to meet higher communication needs.

R105 industrial router supports multi-channel failover to maintain secure and stable network access. With BlueSphere GWM, a web-based cloud platform for centralized management of mass routers and gateways, you can further configure and manage the router remotely. R105 is very suitable for application in industrial automation, smart home, smart city, etc.

## 1.2 Unpackaging

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

| Standard accessories | | Optional accessories | |
|---|---|---|---|
| | 1 x R105 router | | 1 x 12V DC Power adapter & power cord |
| | 2 x 4G LTE antenna<br>(rubber stick) | | 1 x DC power connector |
| | 2 x Wi-Fi antenna<br>(rubber stick) | | 2 x 4G LTE antenna<br>(magnetic sucker) |
|  | 1 x DIN rail mounting bracket (attached) | / | / |

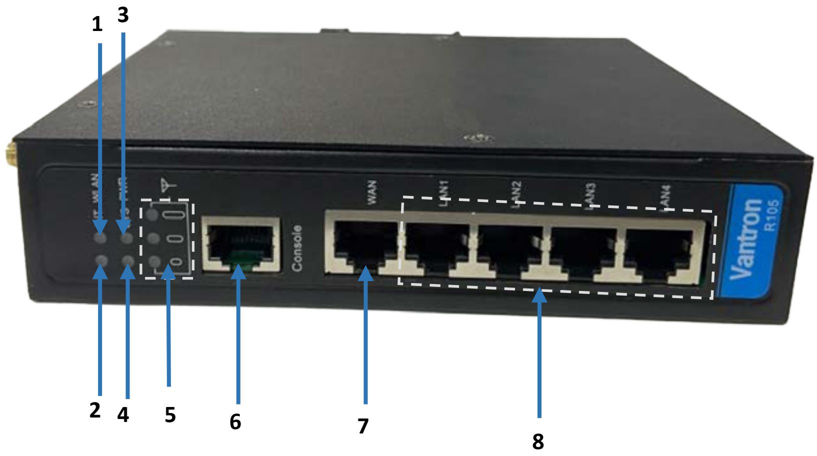
*Actual accessories might vary slightly from the list above as the customer order might be different from the standard configuration options.*

## 1.3 Specifications

| R105 | | | |
|---|---|---|---|
| **Communication** | Ethernet | 5 x RJ45, 10/100/1000Mbps<br>(1 x WAN & 4 x LAN, PoE optional, 30W output) | |
| | Wi-Fi | 2.4GHz & 5GHz, IEEE 802.11 b/g/n/ac, AP & Client<br>Optional: Wi-Fi 6, IEEE 802.11 b/g/n/ac/ax | |
| | 4G LTE | LTE CAT 4, multi-carrier supported | |
| | WAN protocol | PPP, DHCP | |
| **I/Os** | Console | 1 x Console for local configuration | |
| | Serial port | 1 x RS485, isolated<br>1 x RS232, isolated | |
| | SIM slot | 2 x SIM slot | |
| | Antenna (SMA conn.) | 2 x LTE antenna | 2 x Wi-Fi antenna |
| | Grounding | Enclosure & PCB | |
| | Power in | 1 x 3.81mm Phoenix terminal block | |
| **System Control** | LED indicator | 3 x Cellular signal strength indicator<br>1 x Power indicator<br>1 x System indicator | 1 x Internet indicator<br>1 x WLAN indicator |
| | Button | 1 x Pinhole reset button | |
| **Mechanical** | Dimensions | 150mm x 115mm x 35mm | |
| | Enclosure | Metal | |
| | Installation | DIN rail mounting, panel mounting, wall mounting | |
| | IP rating | IP30 | |
| | Drop test | 6 ft. drop test | |
| | Cooling mode | Fanless | |
| **Power** | Input | 9-36V DC, over-current protection, reverse polarity protection | |
| **Software** | OS | VantronOS | |
| | Network management | SNMP v2c/v3 | |
| | Networking protocol | IPV4, HTTPS, TCP & UPD, NTP client and server, ARP, TLS | |
| | VLAN | Supported | |
| | Device management platform | BlueSphere GWM | |
| | Link detection | Heartbeat detection, automatic re-connection | |
| | Device log | Retrievable | |
| | Network reliability | Multi-channel failover, backup between Ethernet, Wi-Fi, 4G LTE | |
| | Dual SIM | Dual SIM failover, automatic switch | |
| | IP application | Ping, Traceroute, DHCP Server/Client, DDNS | |
| | IP Routing | Static routing, dynamic routing | |
| | NAT | Supported | |
| **Security** | Firewall | Supported (Stateful) | |
| | Access control | MAC address, IP address | |
| | Data security | PPTP, L2TP, GRE, IPSec, OpenVPN | |
| | Wi-Fi security | 64/128-bit WEP, TKIP, WPA, WPA2, WPA3, AES, WPS | |
| **Environment Condition** | Temperature | Operating: -20℃~+60℃ | Storage: -40℃~+70℃ |
| | Humidity | Storage: RH 5%~95% (non-condensing) | |
| | Certification | FCC, IC, PTCRB, AT & T, Verizon, T-Mobile | |

# 1.4 Definition of Interfaces

## 1.4.1 Front view



| Indicator/Interface | Description |
|---|---|
| 1 | Wi-Fi status indicator |
| 2 | Network connectivity indicator |
| 3 | Power indicator |
| 4 | System status indicator |
| 5 | 4G LTE signal strength indicator |
| 6 | Console port for debugging the device (baud rate: 57600) |
| 7 | WAN port, mapped as **eth0.2** in VantronOS, working in the WAN area by default |
| 8 | 4 x LAN port, mapped as **eth0.1** in VanrteonOS, working in the LAN area by default |

### Description of the LED indicators

1. Wi-Fi status indicator

| Wi-Fi status | Description |
|---|---|
| The Wi-Fi module is turned on | The indicator turns solid green |
| There is Wi-Fi connectivity | The indicator blinks |
| The Wi-Fi module is turned off | The indicator is off |

2. Network connectivity indicator

| Network connectivity of the Router | Description |
|---|---|
| There is no internet access through any of the available connectivity routes | The indicator is off |
| The router has internet access from any of the routes | The indicator blinks at an interval of 1 second |

3. Power indicator

   When the Router is powered on, the power indicator will turn solid green.

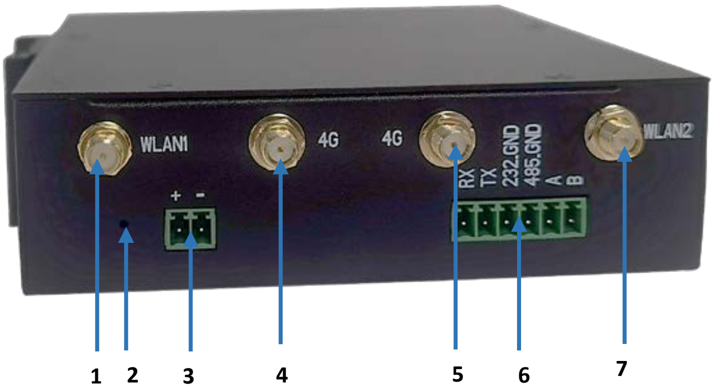
4. System status indicator

| System action | Description |
|---|---|
| System bootup in process | The indicator is off |
| System running properly | The indicator blinks at an interval of 1 second |
| System reboot, upgrade or factory reset | The indicator blinks quickly at an interval of 0.3 seconds |

5. 4G LTE signal strength indicator

| Signal strength | Description |
|---|---|
| >67% | The three indicators turn solid green |
| Between 38% and 67% | The bottom two indicators turn solid green |
| <38% | The bottom indicator blinks |

### 1.4.2 Left side view

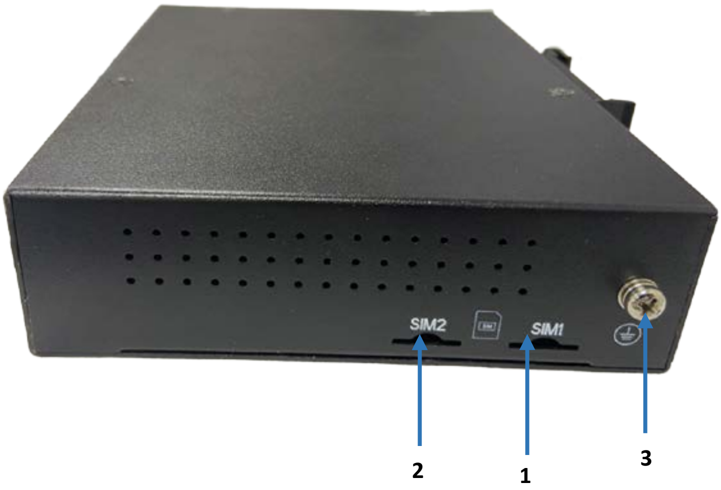


| Interface | Description |
|---|---|
| 1 | Wi-Fi antenna connector 1 |
| 2 | Pinhole RESET button |
| 3 | Power terminal (9V-36V DC) |
| 4 | Secondary 4G LTE antenna connector |
| 5 | Primary 4G LTE antenna connector |
| 6 | RS232 & RS485 serial connectors |
| 7 | Wi-Fi antenna connector 2 |

#### Description of the RESET button

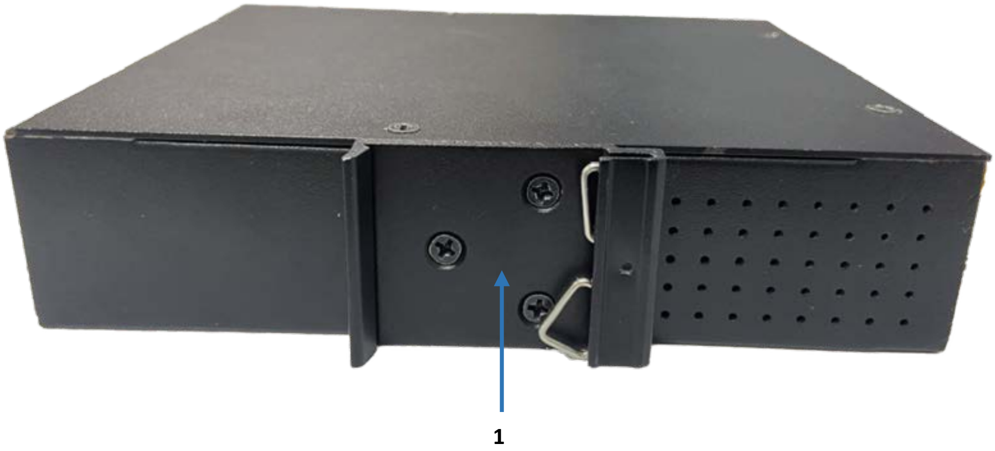
1. A short press of the button for 0 ~ 2 seconds will restart the Router.
2. A long press of the button for 3 ~ 6 seconds will factory reset the Router.
3. A long press of the button for 6 ~ 10 seconds will factory reset the Router with all user data cleared.

### 1.4.3 Right side view



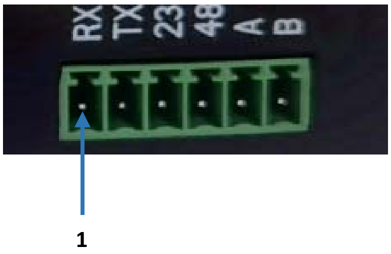
| Interface | Description |
|---|---|
| 1 | Micro SIM slot 1 |
| 2 | Micro SIM slot 2 |
| 3 | Grounding screw |

### 1.4.4 Back view



| Interface | Description |
|---|---|
| 1 | DIN rail bracket |

## 1.5 Serial Port Description



The terminal block incorporates an RS232 port and an RS485 port with pinout description as follows:

| No. | Signal | Device name | Port | Type | Description |
|---|---|---|---|---|---|
| 1 | RX | /dev/ttyS1 | COM1 | I | RS232 receive signal |
| 2 | TX | | | O | RS232 transmit signal |
| 3 | 232. GND | | | NC | RS232 isolated ground |
| 4 | 485. GND | /dev/ttyS2 | COM2 | NC | RS485 isolated ground |
| 5 | A | | | I/O | RS485 A signal |
| 6 | B | | | I/O | RS485 B signal |

For RS232 port connection: RX-TX, TX-RX, GND-GND

For RS485 port connection: A-A, B-B, GND-GND

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

COM1:

```
~# microcom /dev/ttyS1 -s 115200
```

COM2:

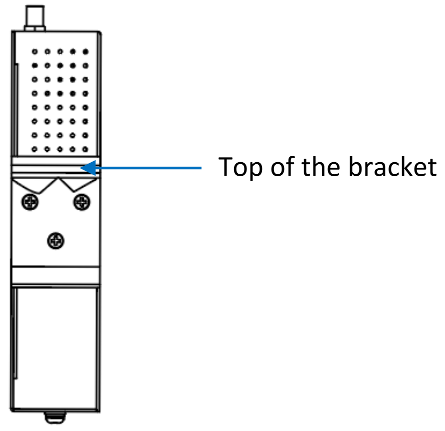
```
~# microcom /dev/ttyS2 -s 115200
```

# CHAPTER 2 GETTING STARTED

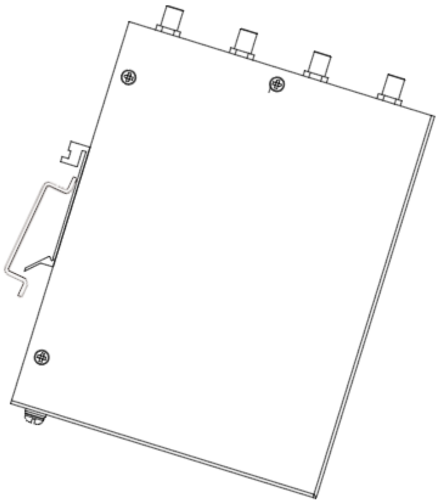
## 2.1 Setting up the Router

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

1. Hold the Router uprightly;

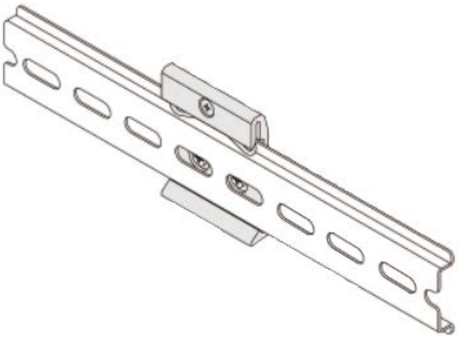


2. Place the Router on the DIN rail at an angle;
3. Fit one side of the DIN rail to the clip at the top of the DIN rail bracket, behind the triangle fixer;

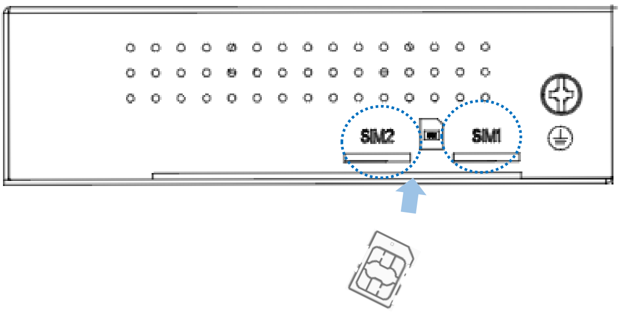


4. Push the Router down to compress the bracket;

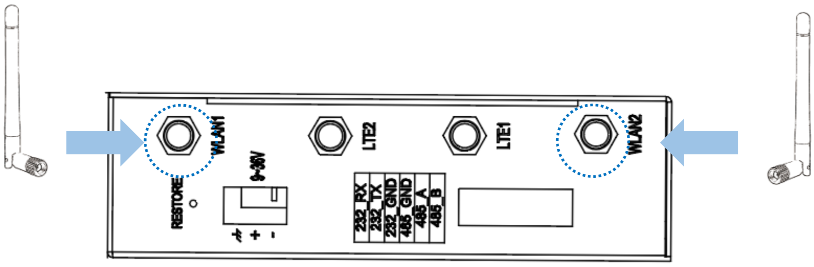
5. Release the Router when there is enough space for the other side of the DIN rail to fit in the downside of the DIN rail bracket;



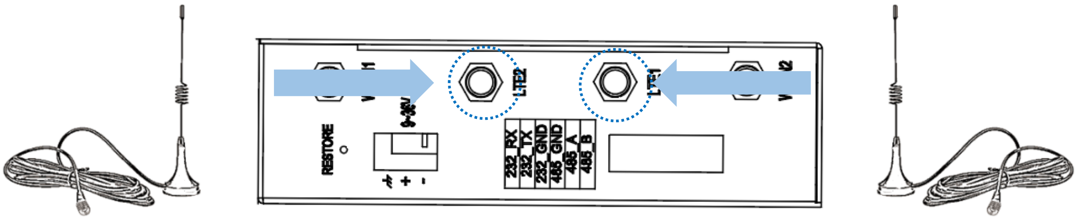
6. Gently swing the Router to make sure the it is fastened on the DIN rail;
7. Insert an activated Micro SIM card into either of the SIM slots with the gold-colored contacts facing up and the clipped side inward;



8. Push the Micro SIM card in to secure it;
9. Install the Wi-Fi antennas (rubber stick) to the WLAN antenna connectors;

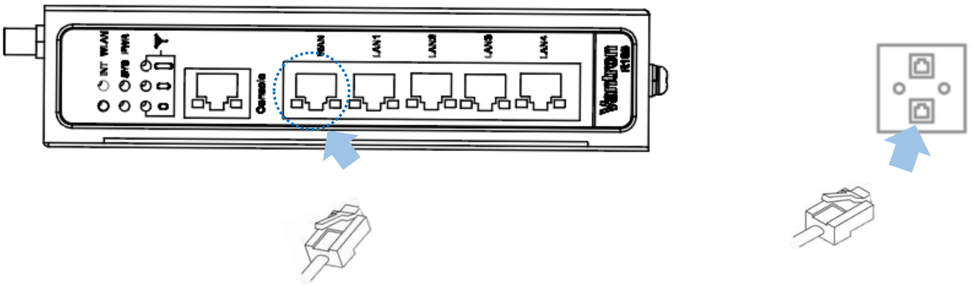


10. Install the LTE antennas (rubber stick /magnetic sucker) to the LTE antenna connectors (if only one antenna is shipped, install to the LTE 1 connector);



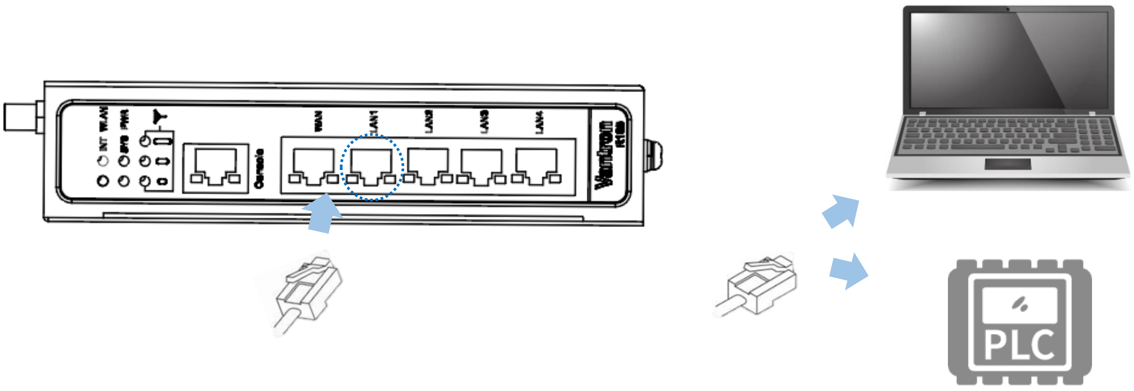
11. Tighten the rotating heads to secure the antennas in proper position;

12. Connect one end of an Ethernet cable to the WAN port of the Router and the other to a live Ethernet port;

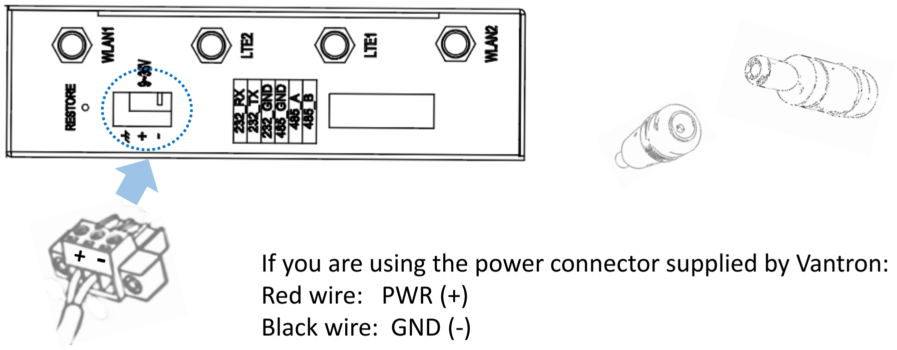


*Skip this step if you choose wireless network connection.*

13. Connect one end of another Ethernet cable to a LAN port of the Router and the other to a host computer or client device depending on your use;



14. Connect the terminal end of the DC power connector to the power terminal of the Router and the round end to the adapter;



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

15. Plug the adapter to a DC power outlet that meets the supply voltage requirement (9V to 36V) to turn on the Router；

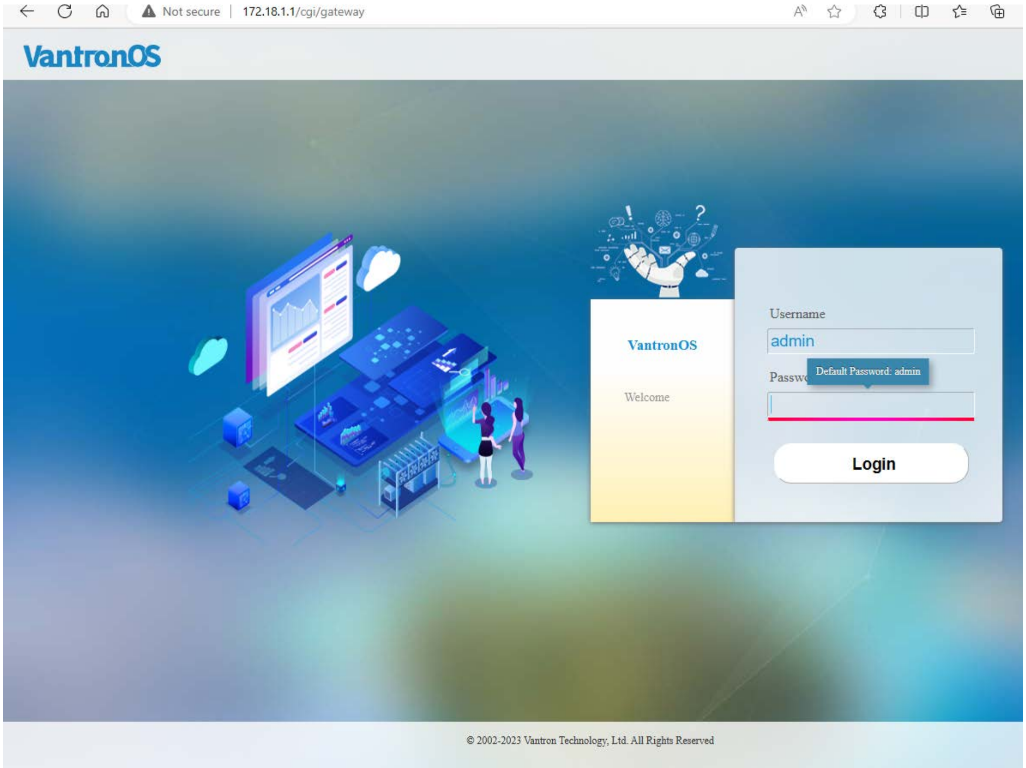
16. The power indicator will turn solid green upon power application.

*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.*

## 2.2 Router Login

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

1. Input the LAN port IP address of the Router 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**



Not secure | 172.18.1.1/cgi/gateway

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

*The web login address coincides with the LAN port IP address of the Router, so 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.*

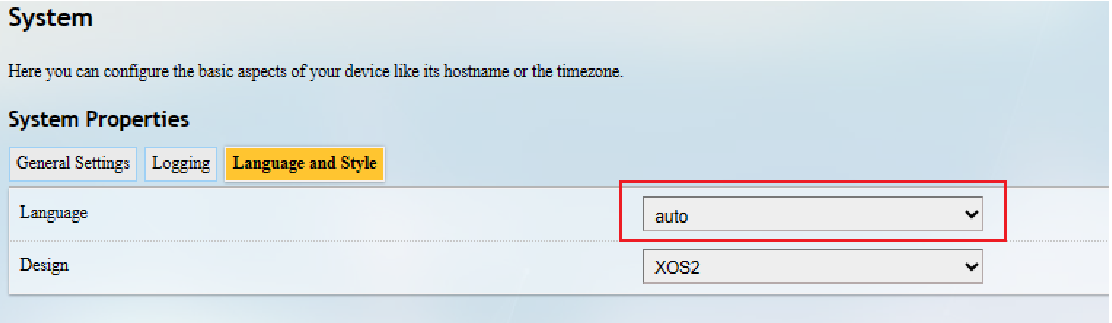
## 2.3 Password Change

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**.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Language: auto

Design: XOS2

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 ROUTER SETUP VIA VANTRONOS

## 3.1 Introduction to VantronOS

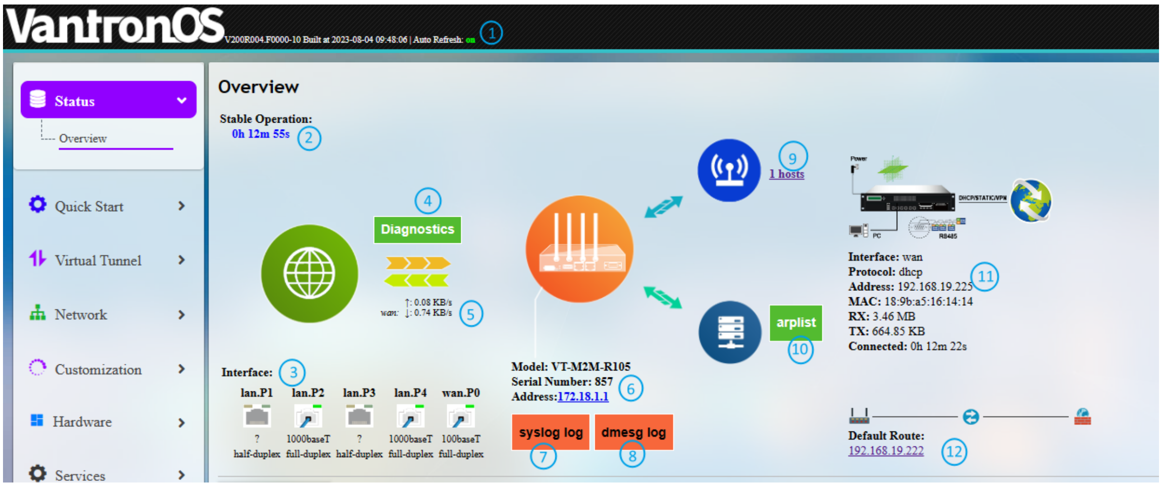
VantronOS is an intelligent operating system developed by the Vantron team, featuring independent system and function development. It is built upon the Linux system and optimized for embedded hardware. The operating system follows a modular design and plug-in expansion approach, utilizing the Linux kernel 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 Router, including stable operation duration, number of devices connected to the Router via wireless or Ethernet connection, default routing, hardware information, traffic statistics, etc.



V200R004.F0000-10 Built at 2023-08-04 09:48:06 | Auto Refresh: on

Overview

Stable Operation:
0h 12m 55s

wan: ↑: 0.08 KB/s
↓: 0.74 KB/s

Interface:

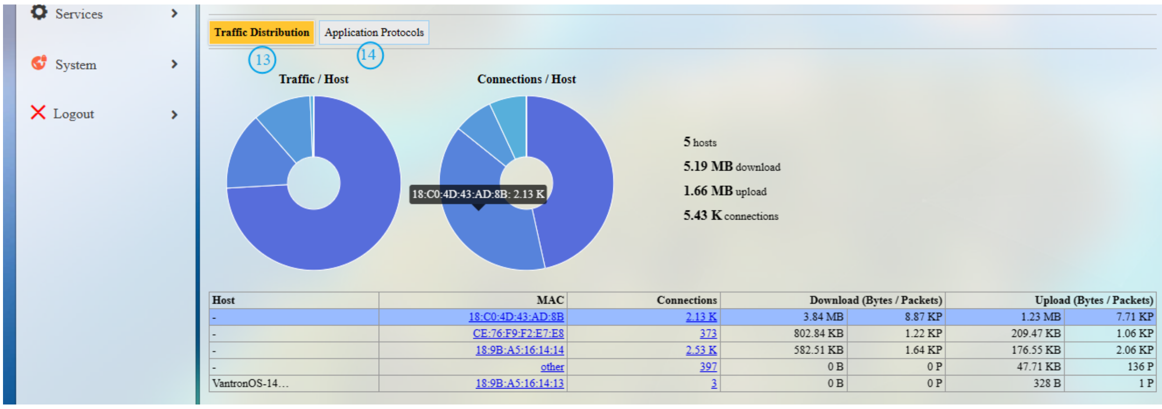
| lan.P1 | lan.P2 | lan.P3 | lan.P4 | wan.P0 |
|---|---|---|---|---|
| ?<br>half-duplex | 1000baseT<br>full-duplex | ?<br>half-duplex | 1000baseT<br>full-duplex | 100baseT<br>full-duplex |

Model: VT-M2M-R105
Serial Number: 857
Address:172.18.1.1

syslog log | dmesg log

Interface: wan
Protocol: dhcp
Address: 192.168.19.225
MAC: 18:9b:a5:16:14:14
RX: 3.46 MB
TX: 664.85 KB
Connected: 0h 12m 22s

Default Route:
192.168.19.222



5 hosts
5.19 MB download
1.66 MB upload
5.43 K connections

| Host | MAC | Connections | Download (Bytes / Packets) | | Upload (Bytes / Packets) | |
|---|---|---|---|---|---|---|
| - | 18:C0:4D:43:AD:8B | 2.13 K | 3.84 MB | 8.87 KP | 1.23 MB | 7.71 KP |
| - | CE:76:F9:F2:E7:E8 | 373 | 802.84 KB | 1.22 KP | 209.47 KB | 1.06 KP |
| - | 18:9B:A5:16:14:14 | 2.53 K | 582.51 KB | 1.64 KP | 176.55 KB | 2.06 KP |
| - | other | 397 | 0 B | 0 P | 47.71 KB | 136 P |
| VantronOS-14… | 18:9B:A5:16:14:13 | 3 | 0 B | 0 P | 328 B | 1 P |

Description of the numbered areas

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

   *(LAN2, LAN4, and the WAN port are connected in this case)*

4. A collection of the network diagnostic tools (refer to 3.7 for details)

5. Instant outbound traffic

6. The model, serial number, and management address of the router in use

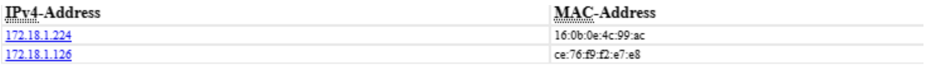
7. System log information

8. Kernel log information

9. Number of clients connected to the Router via Wi-Fi

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

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



| IPv4-Address | MAC-Address |
|---|---|
| 172.18.1.224 | 16:0b:0e:4c:99:ac |
| 172.18.1.126 | ce:76:f9:f2:e7:e8 |

11. Details of the router connectivity

*The illustrative image varies with the communication module on the Router.*

12. Default route currently used by the Router

13. Traffic distribution of clients connected to the Router 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.*

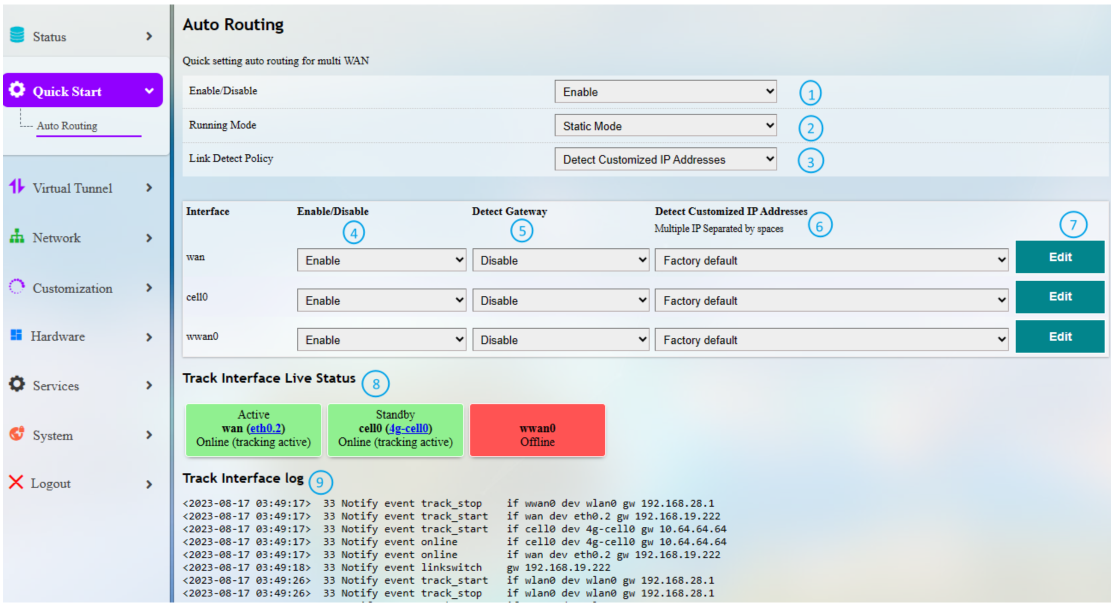
14. Traffic of application layer protocols

*HTTPS, HTTP, and QUIC 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 Router 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.



Auto Routing

Quick setting auto routing for multi WAN

| | |
|---|---|
| Enable/Disable | Enable |
| Running Mode | Static Mode |
| Link Detect Policy | Detect Customized IP Addresses |

| Interface | Enable/Disable | Detect Gateway | Detect Customized IP Addresses<br>Multiple IP Separated by spaces |
|---|---|---|---|
| wan | Enable | Disable | Factory default |
| cell0 | Enable | Disable | Factory default |
| wwan0 | Enable | Disable | Factory default |

Track Interface Live Status

| | | |
|---|---|---|
| Active<br>**wan** (eth0.2)<br>Online (tracking active) | Standby<br>**cell0** (4g-cell0)<br>Online (tracking active) | **wwan0**<br>Offline |

Track Interface log

```
<2023-08-17 03:49:17>  33 Notify event track_stop    if wwan0 dev wlan0 gw 192.168.28.1
<2023-08-17 03:49:17>  33 Notify event track_start   if wan dev eth0.2 gw 192.168.19.222
<2023-08-17 03:49:17>  33 Notify event track_start   if cell0 dev 4g-cell0 gw 10.64.64.64
<2023-08-17 03:49:17>  33 Notify event online        if cell0 dev 4g-cell0 gw 10.64.64.64
<2023-08-17 03:49:17>  33 Notify event online        if wan dev eth0.2 gw 192.168.19.222
<2023-08-17 03:49:18>  33 Notify event linkswitch    gw 192.168.19.222
<2023-08-17 03:49:26>  33 Notify event track_start   if wlan0 dev wlan0 gw 192.168.28.1
<2023-08-17 03:49:26>  33 Notify event track_stop    if wlan0 dev wlan0 gw 192.168.28.1
```

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<br>(Default) | 1. The user-designated link priority takes precedence;<br>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;<br>2. The user-designated link priority will be disabled.<br>This is not recommended when special applications are installed on the Router that rely on the designated link priority. |

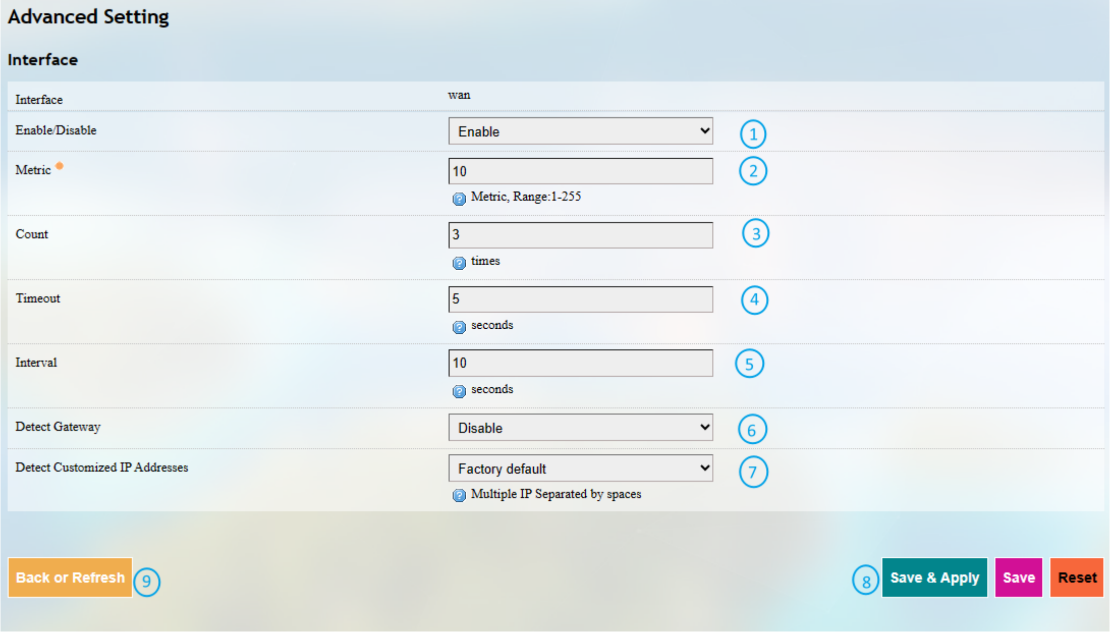
Automatic link detection policy

| Policy | Description |
|---|---|
| Detect customized IP addresses<br>(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”;<br>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.<br>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 an interface will direct you to the rule editing page as follows.



Advanced Setting

Interface

| | |
|---|---|
| Interface | wan |
| Enable/Disable | Enable |
| Metric | 10<br>Metric, Range:1-255 |
| Count | 3<br>times |
| Timeout | 5<br>seconds |
| Interval | 10<br>seconds |
| Detect Gateway | Disable |
| Detect Customized IP Addresses | Factory default<br>Multiple IP Separated by spaces |

Description of the numbered areas

1. Enable/Disable the route tracking on this interface
2. Gateway metric (The smaller the number, the higher the priority)
3. The count of total messages sent in case of a detection timeout (3 by default)
4. The timeout for a single tracking (5s by default)
5. Tracking interval, defined as from the completion of one tracking to the initiation of the next tracking (10s by default)
6. Enable/disable gateway detection
7. Select the default IP addresses (‘factory default’) or customized IP addresses (‘custom’) for IP detection
8. **Save & Apply** the settings
9. Go back to the automatic routing page

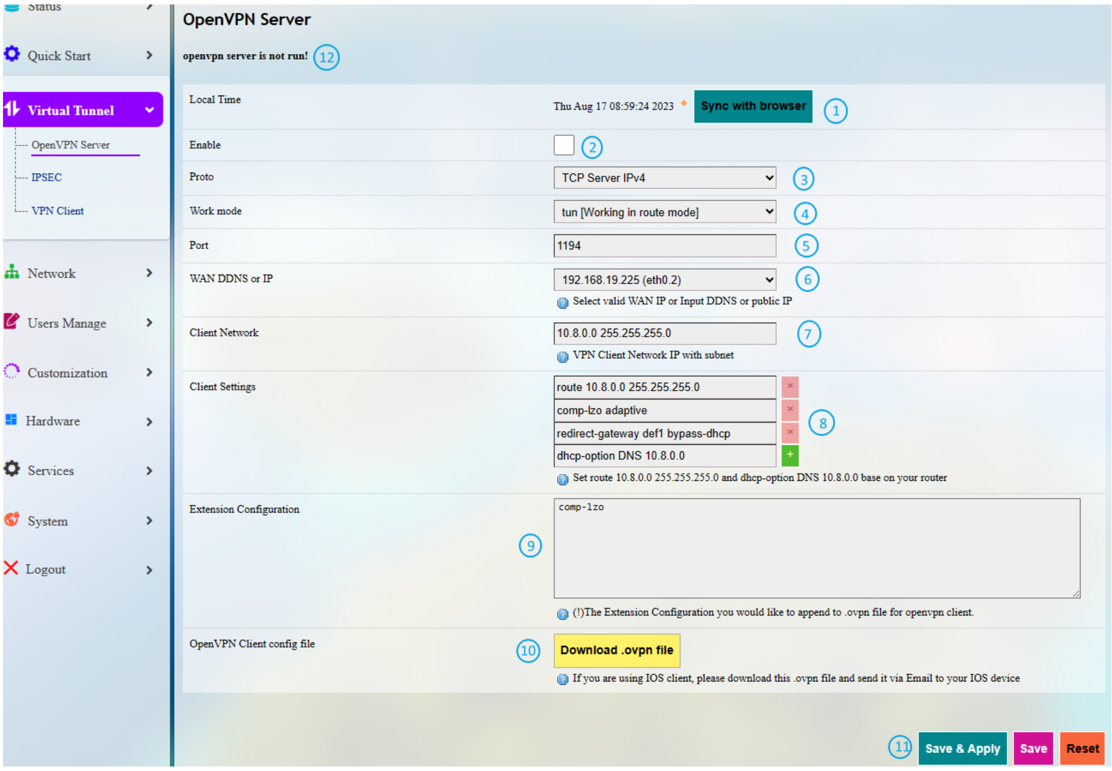
# 3.4 Virtual Tunnel

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

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

## 3.4.1 OpenVPN Server

This page provides virtual private network based on SSL connection and transmission, which features simple and flexible configurations, better security, and no interference.



OpenVPN Server

openvpn server is not run! (12)

Local Time: Thu Aug 17 08:59:24 2023 (1)

Enable: □ (2)

Proto: TCP Server IPv4 (3)

Work mode: tun [Working in route mode] (4)

Port: 1194 (5)

WAN DDNS or IP: 192.168.19.225 (eth0.2) (6)
Select valid WAN IP or Input DDNS or public IP

Client Network: 10.8.0.0 255.255.255.0 (7)
VPN Client Network IP with subnet

Client Settings: (8)
route 10.8.0.0 255.255.255.0
comp-lzo adaptive
redirect-gateway def1 bypass-dhcp
dhcp-option DNS 10.8.0.0
Set route 10.8.0.0 255.255.255.0 and dhcp-option DNS 10.8.0.0 base on your router

Extension Configuration: (9)
```
comp-lzo
```
(!)The Extension Configuration you would like to append to .ovpn file for openvpn client.

OpenVPN Client config file: (10) Download .ovpn file
If you are using IOS client, please download this .ovpn file and send it via Email to your IOS device

(11)

Follow the steps below to build an OpenVPN server:

1. Synchronize the Router time with the browser (local) time;

2. Enable the server or not after the server is built;

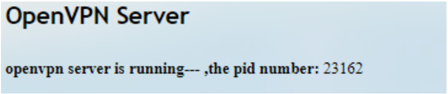
3. Select a protocol (TCP by default);

*TCP provides an ordered delivery of data from the 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 & Apply** the settings;
12. Status of the OpenVPN server after the setup.



OpenVPN Server

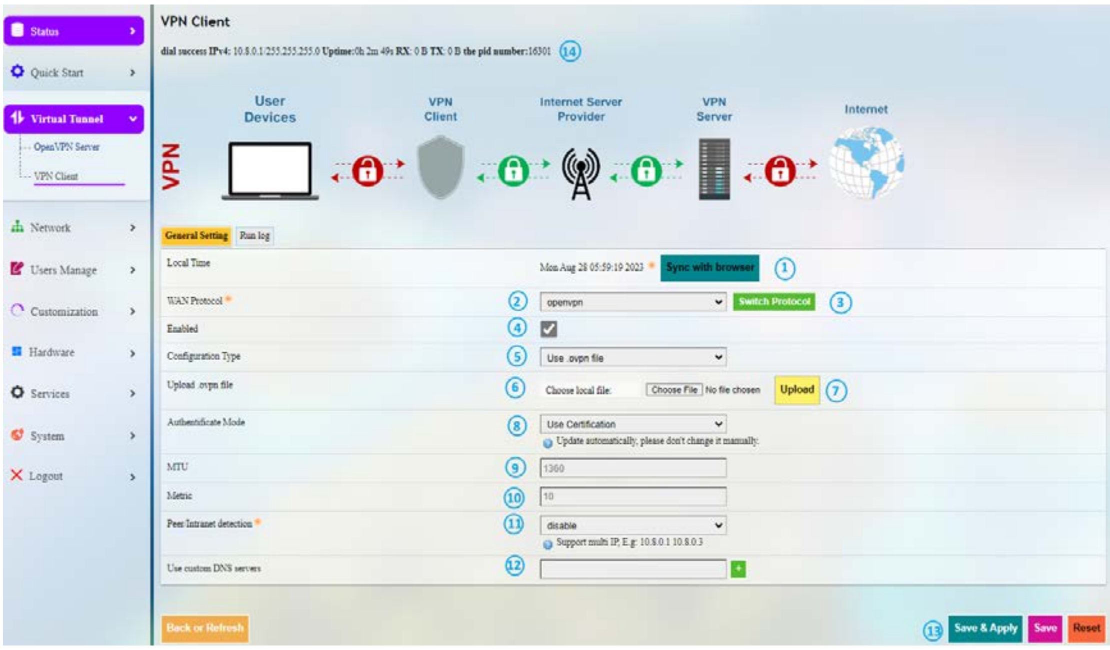
openvpn server is running--- ,the pid number: 23162

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



VPN Client

dial success IPv4: 10.8.0.1/255.255.255.0 Uptime:0h 2m 49s RX: 0 B TX: 0 B the pid number:16301

Local Time: Mon Aug 28 05:59:19 2023

WAN Protocol *: openvpn

Enabled: ☑

Configuration Type: Use .ovpn file

Upload .ovpn file: Choose local file: No file chosen

Authentificate Mode: Use Certification
Update automatically, please don't change it manually.

MTU: 1360

Metric: 10

Peer Intranet detection *: disable
Support multi IP, E.g: 10.8.0.1 10.8.0.3

Use custom DNS servers:

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 file
8. Select to use a certificate 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.*

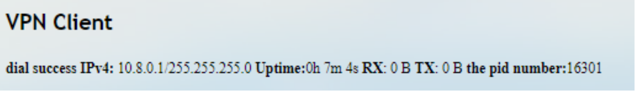
11. Disable/Enable heartbeat detection

*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



VPN Client

**dial success IPv4:** 10.8.0.1/255.255.255.0 **Uptime:**0h 7m 4s **RX:** 0 B **TX:** 0 B **the pid number:**16301

## 3.5 IPSec Connection

### 3.5.1 Prerequisites

- An R105 industrial router (‘G1’ for short)
- A supporting device (gateway/router) that runs on VantronOS and supports IPSec (‘G2’ for short)
- Certificates for the router 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

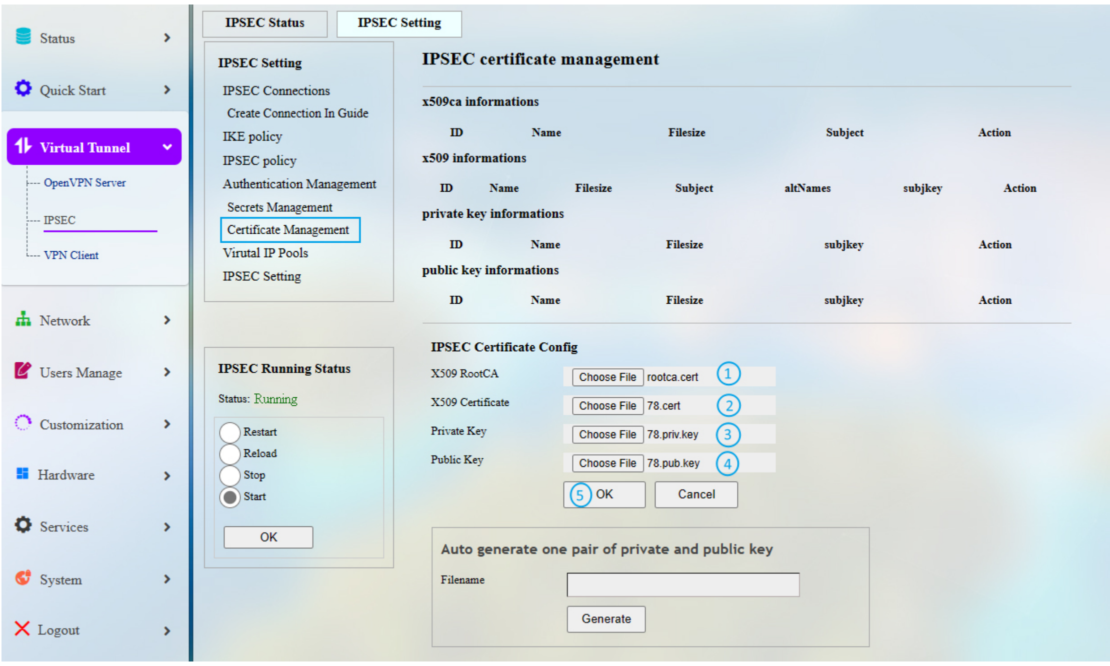
X509 certificate: 82.cert

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):



Status: Running

○ Restart
○ Reload
○ Stop
● Start

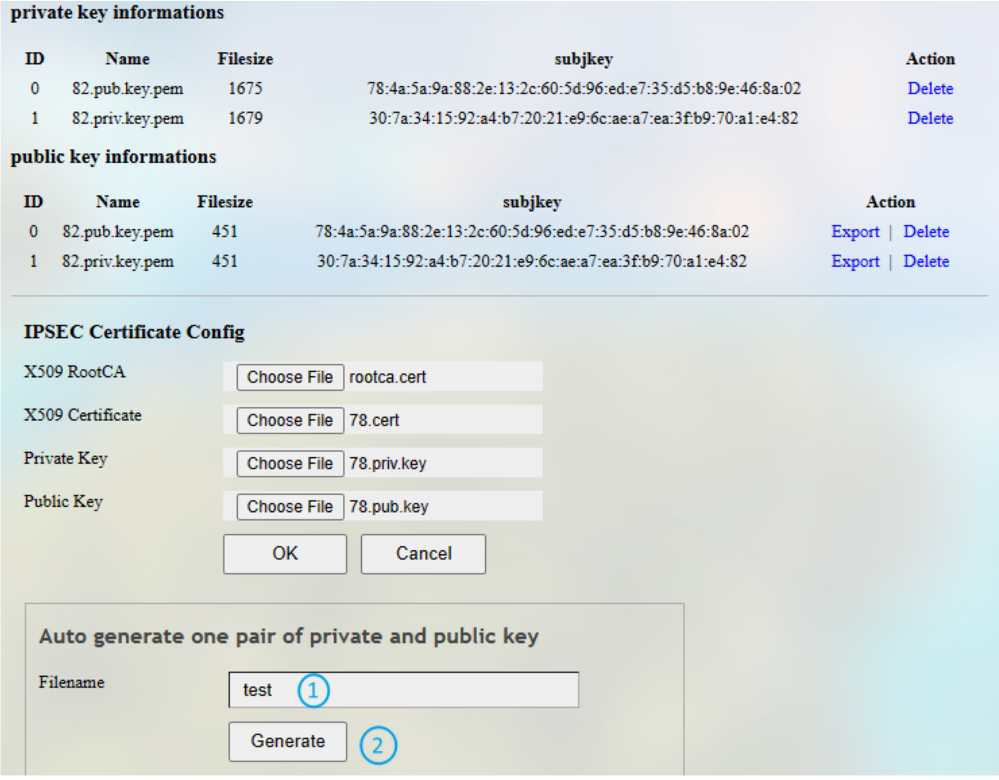
X509 RootCA: rootca.cert
X509 Certificate: 78.cert
Private Key: 78.priv.key
Public Key: 78.pub.key

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.



**private key informations**

| ID | Name | Filesize | subjkey | Action |
|---|---|---|---|---|
| 0 | 82.pub.key.pem | 1675 | 78:4a:5a:9a:88:2e:13:2c:60:5d:96:ed:e7:35:d5:b8:9e:46:8a:02 | Delete |
| 1 | 82.priv.key.pem | 1679 | 30:7a:34:15:92:a4:b7:20:21:e9:6c:ae:a7:ea:3f:b9:70:a1:e4:82 | Delete |

**public key informations**

| ID | Name | Filesize | subjkey | Action |
|---|---|---|---|---|
| 0 | 82.pub.key.pem | 451 | 78:4a:5a:9a:88:2e:13:2c:60:5d:96:ed:e7:35:d5:b8:9e:46:8a:02 | Export \| Delete |
| 1 | 82.priv.key.pem | 451 | 30:7a:34:15:92:a4:b7:20:21:e9:6c:ae:a7:ea:3f:b9:70:a1:e4:82 | Export \| Delete |

**IPSEC Certificate Config**

X509 RootCA: Choose File rootca.cert

X509 Certificate: Choose File 78.cert

Private Key: Choose File 78.priv.key

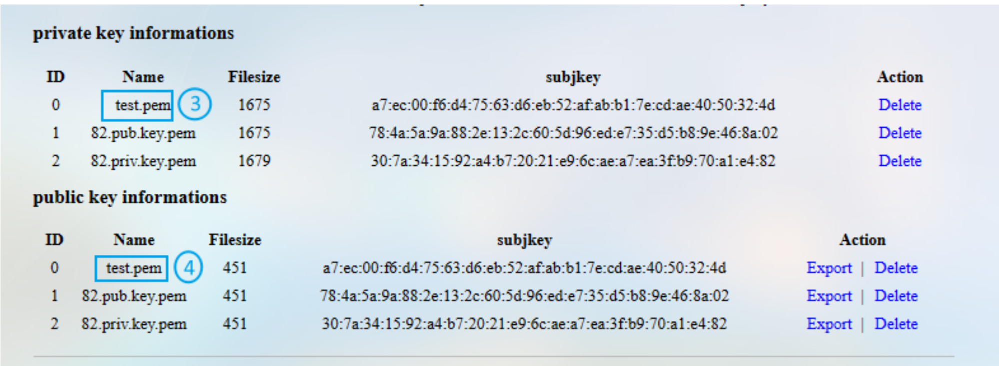
Public Key: Choose File 78.pub.key

OK Cancel

**Auto generate one pair of private and public key**

Filename: test

Generate



**private key informations**

| ID | Name | Filesize | subjkey | Action |
|---|---|---|---|---|
| 0 | test.pem | 1675 | a7:ec:00:f6:d4:75:63:d6:eb:52:af:ab:b1:7e:cd:ae:40:50:32:4d | Delete |
| 1 | 82.pub.key.pem | 1675 | 78:4a:5a:9a:88:2e:13:2c:60:5d:96:ed:e7:35:d5:b8:9e:46:8a:02 | Delete |
| 2 | 82.priv.key.pem | 1679 | 30:7a:34:15:92:a4:b7:20:21:e9:6c:ae:a7:ea:3f:b9:70:a1:e4:82 | Delete |

**public key informations**

| ID | Name | Filesize | subjkey | Action |
|---|---|---|---|---|
| 0 | test.pem | 451 | a7:ec:00:f6:d4:75:63:d6:eb:52:af:ab:b1:7e:cd:ae:40:50:32:4d | Export \| Delete |
| 1 | 82.pub.key.pem | 451 | 78:4a:5a:9a:88:2e:13:2c:60:5d:96:ed:e7:35:d5:b8:9e:46:8a:02 | Export \| Delete |
| 2 | 82.priv.key.pem | 451 | 30:7a:34:15:92:a4:b7:20:21:e9:6c:ae:a7:ea:3f:b9:70:a1:e4:82 | Export \| Delete |

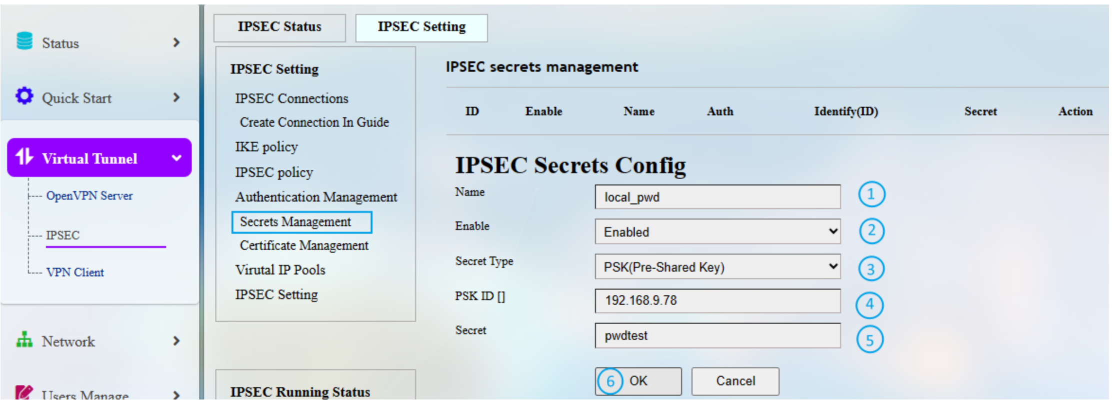
Description of the numbered areas

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):



IPSEC Secrets Config

Name: local_pwd

Enable: Enabled

Secret Type: PSK(Pre-Shared Key)

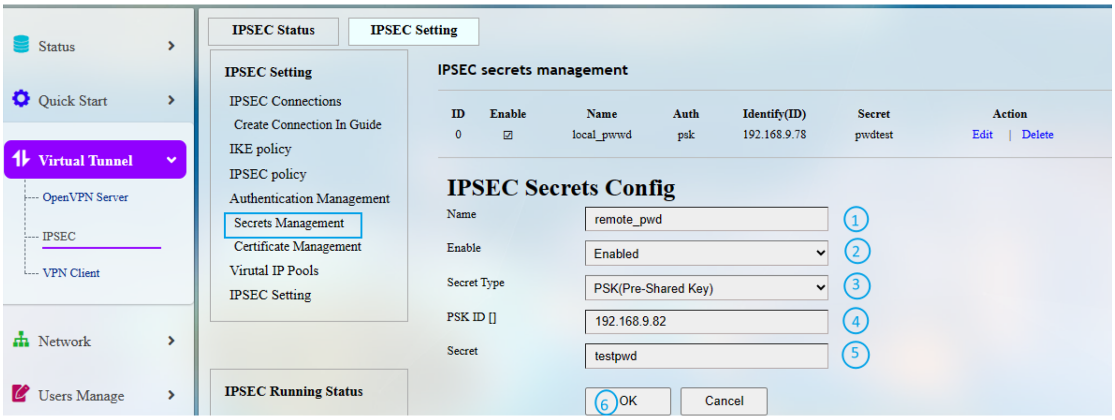
PSK ID []: 192.168.9.78

Secret: pwdtest

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):



IPSEC secrets management

| ID | Enable | Name | Auth | Identify(ID) | Secret | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | local_pwwd | psk | 192.168.9.78 | pwdtest | Edit \| Delete |

IPSEC Secrets Config

Name: remote_pwd ①

Enable: Enabled ②

Secret Type: PSK(Pre-Shared Key) ③

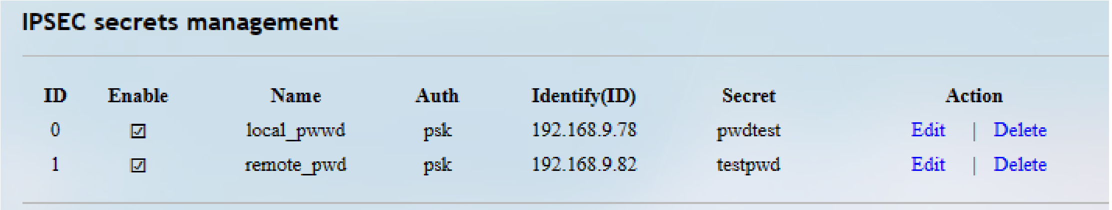
PSK ID []: 192.168.9.82 ④

Secret: testpwd ⑤

⑥ OK

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.

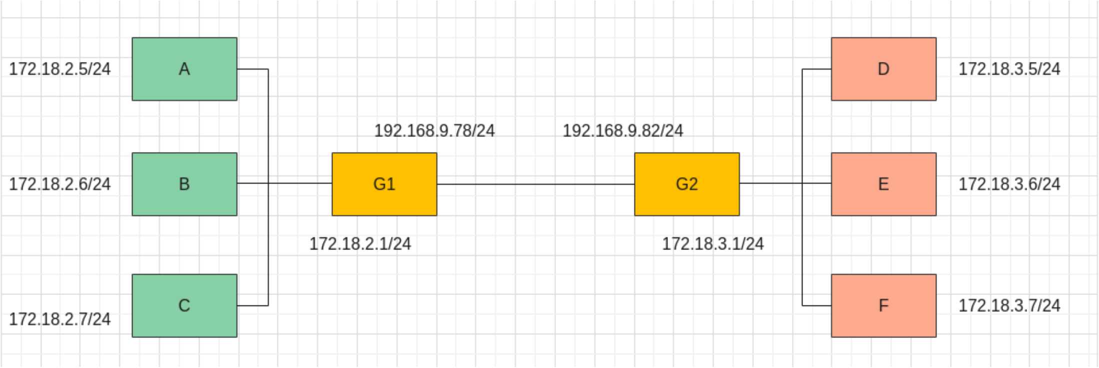


IPSEC secrets management

| ID | Enable | Name | Auth | Identify(ID) | Secret | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | local_pwwd | psk | 192.168.9.78 | pwdtest | Edit \| Delete |
| 1 | ☑ | remote_pwd | psk | 192.168.9.82 | testpwd | Edit \| Delete |

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.

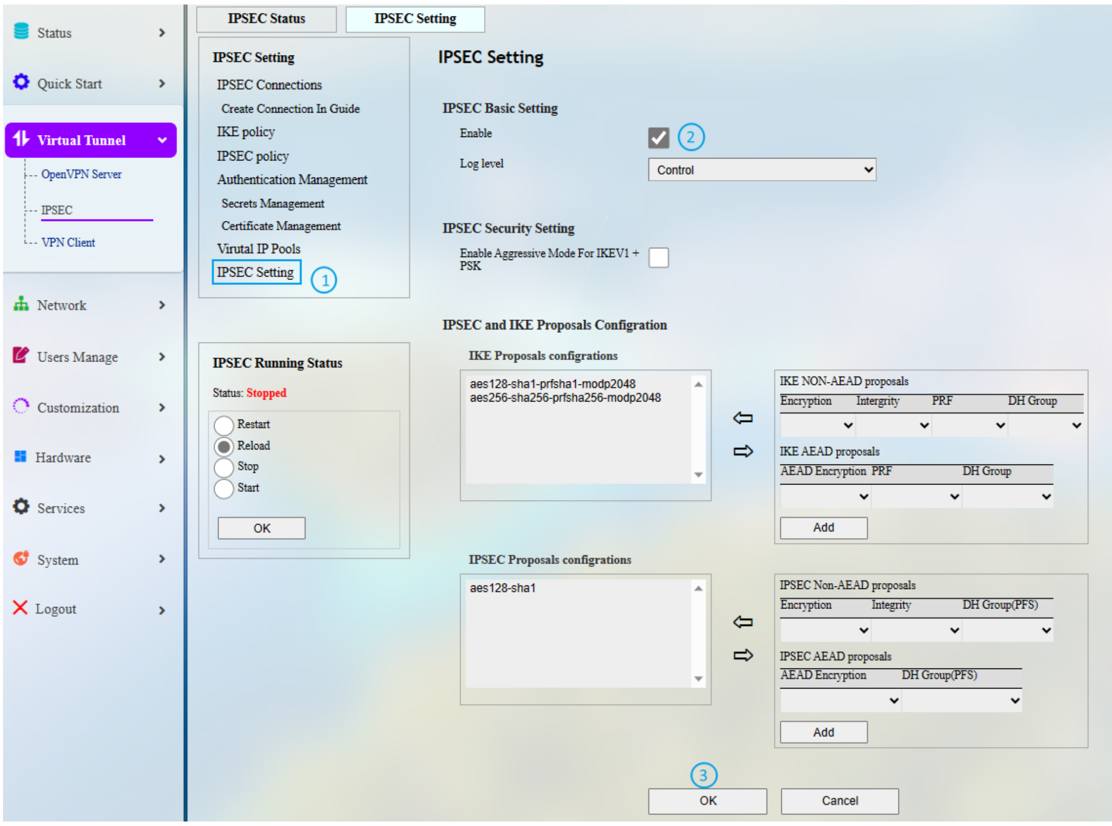
### 3.5.4 IPSec Connection Setup



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



IPSEC Running Status

Status: Stopped

○ Restart
● Reload
○ Stop
○ Start

OK

IPSEC Setting

IPSEC Basic Setting

Enable ☑

Log level: Control

IPSEC Security Setting

Enable Aggressive Mode For IKEV1 + PSK □

IPSEC and IKE Proposals Configration

IKE Proposals configrations

aes128-sha1-prfsha1-modp2048
aes256-sha256-prfsha256-modp2048

IKE NON-AEAD proposals: Encryption | Intergrity | PRF | DH Group

IKE AEAD proposals: AEAD Encryption | PRF | DH Group

IPSEC Proposals configrations

aes128-sha1

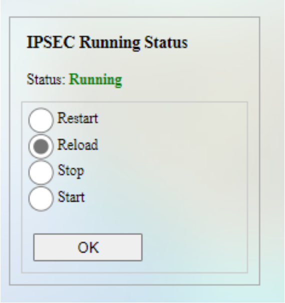
IPSEC Non-AEAD proposals: Encryption | Integrity | DH Group(PFS)

IPSEC AEAD proposals: AEAD Encryption | DH Group(PFS)

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.



IPSEC Running Status

Status: Running

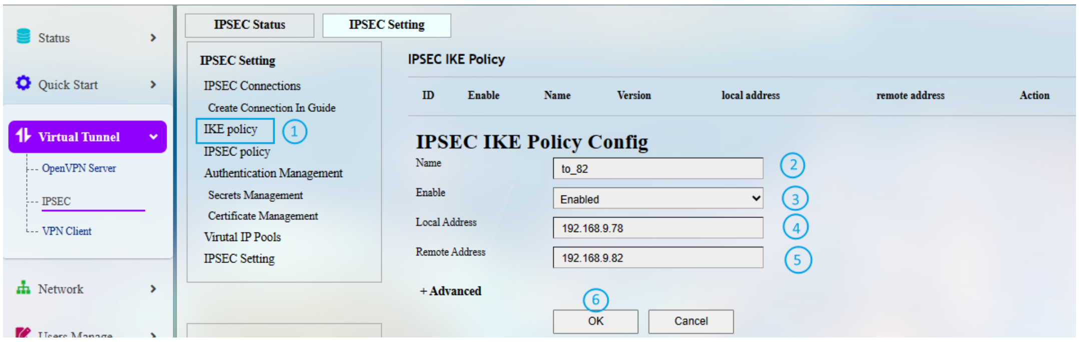
○ Restart
● Reload
○ Stop
○ Start

OK

**STEP 2: IKE policy configuration**

Configurations for scenarios 1 and 2:

G1 setup



IPSEC IKE Policy

| ID | Enable | Name | Version | local address | remote address | Action |
|---|---|---|---|---|---|---|

IPSEC IKE Policy Config

Name: to_82

Enable: Enabled

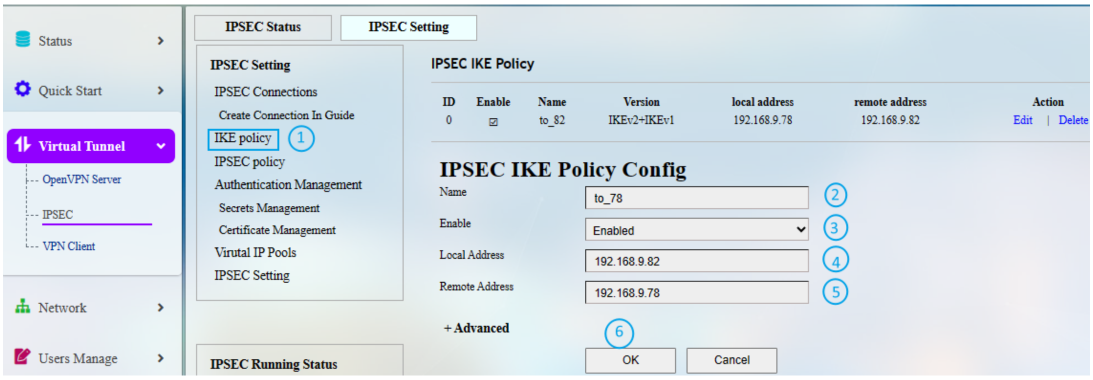
Local Address: 192.168.9.78

Remote Address: 192.168.9.82

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



IPSEC IKE Policy

| ID | Enable | Name | Version | local address | remote address | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | to_82 | IKEv2+IKEv1 | 192.168.9.78 | 192.168.9.82 | Edit \| Delete |

IPSEC IKE Policy Config

Name: to_78

Enable: Enabled

Local Address: 192.168.9.82

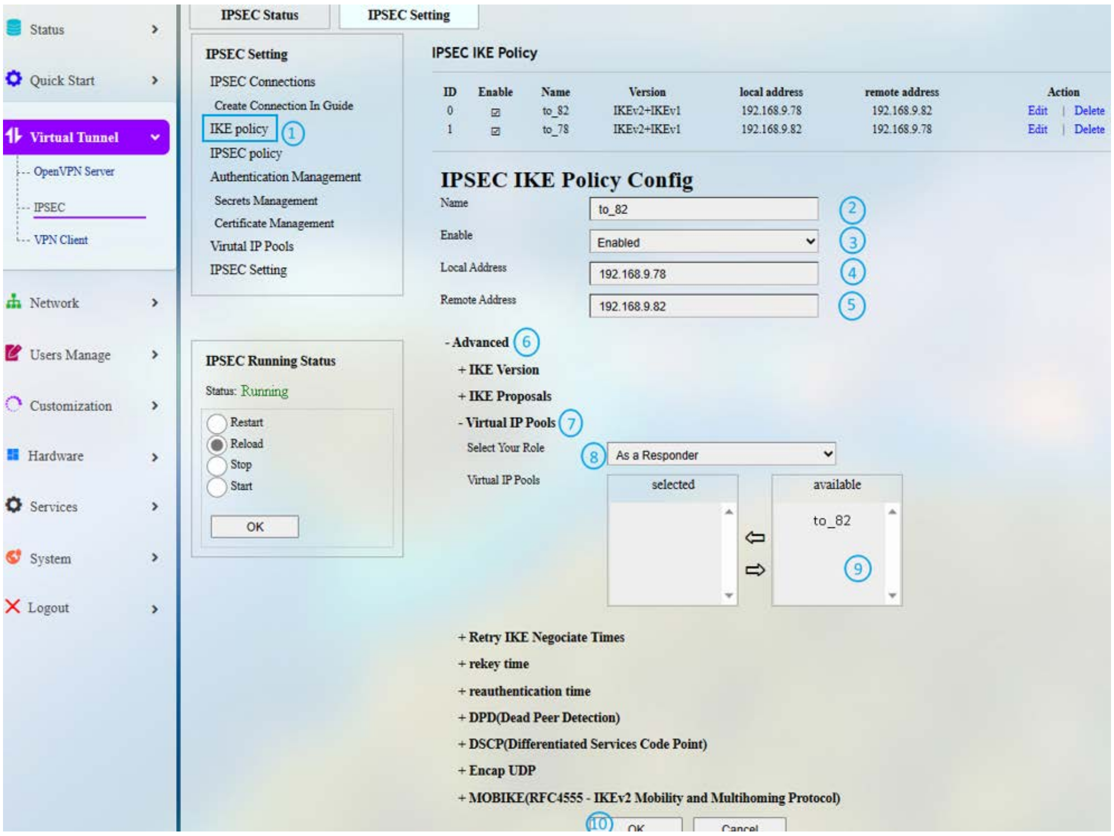
Remote Address: 192.168.9.78

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



| ID | Enable | Name | Version | local address | remote address | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | to_82 | IKEv2+IKEv1 | 192.168.9.78 | 192.168.9.82 | Edit \| Delete |
| 1 | ☑ | to_78 | IKEv2+IKEv1 | 192.168.9.82 | 192.168.9.78 | Edit \| Delete |

Name: to_82

Enable: Enabled

Local Address: 192.168.9.78

Remote Address: 192.168.9.82

Select Your Role: As a Responder

Virtual IP Pools: selected: ; available: to_82

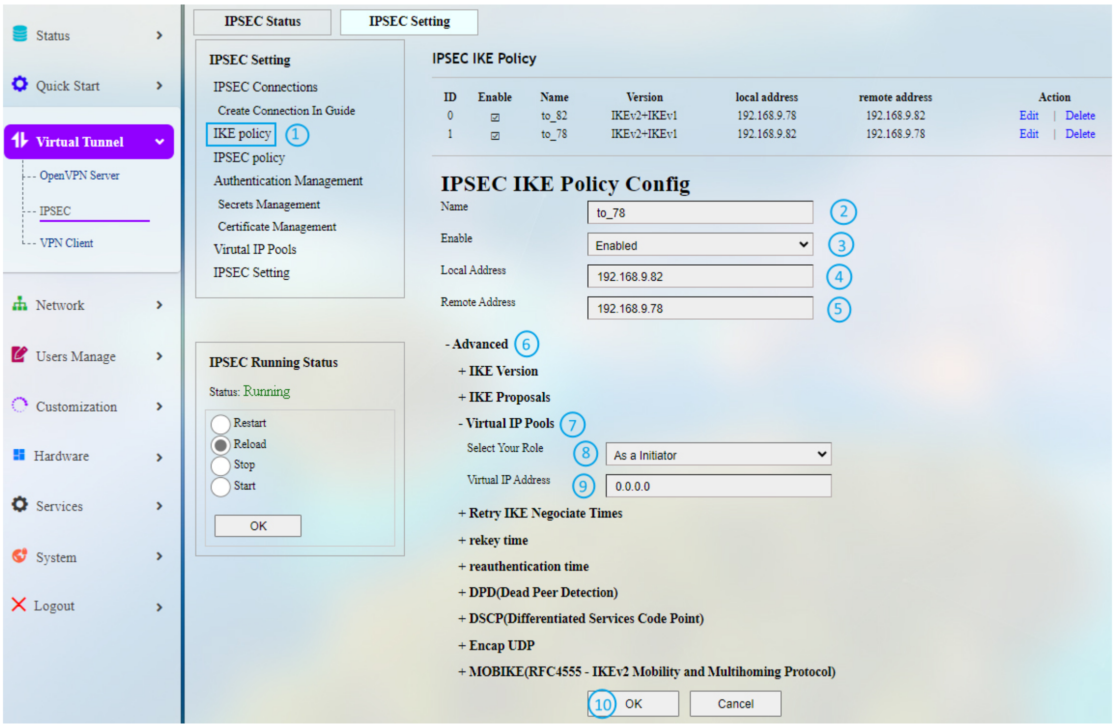
Status: Running

○ Restart
● Reload
○ Stop
○ Start

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



Status: Running

IPSEC IKE Policy

| ID | Enable | Name | Version | local address | remote address | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | to_82 | IKEv2+IKEv1 | 192.168.9.78 | 192.168.9.82 | Edit \| Delete |
| 1 | ☑ | to_78 | IKEv2+IKEv1 | 192.168.9.82 | 192.168.9.78 | Edit \| Delete |

IPSEC IKE Policy Config

Name: to_78

Enable: Enabled

Local Address: 192.168.9.82

Remote Address: 192.168.9.78

- Advanced

+ IKE Version

+ IKE Proposals

- Virtual IP Pools

Select Your Role: As a Initiator

Virtual IP Address: 0.0.0.0

+ Retry IKE Negociate Times

+ rekey time

+ reauthentication time

+ DPD(Dead Peer Detection)

+ DSCP(Differentiated Services Code Point)

+ Encap UDP

+ MOBIKE(RFC4555 - IKEv2 Mobility and Multihoming Protocol)

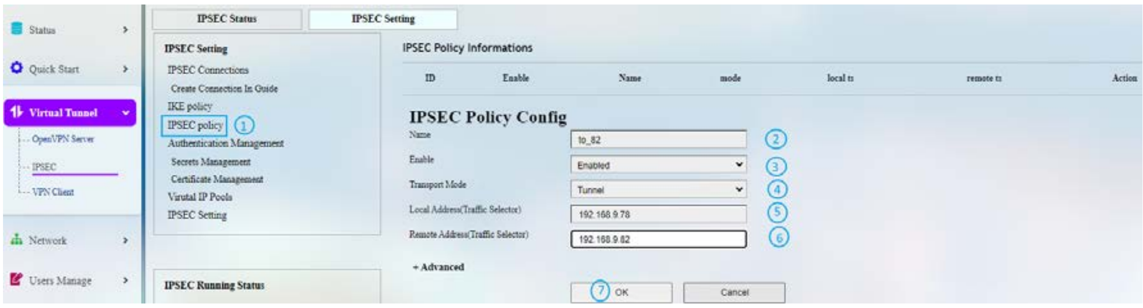
Description of the numbered areas

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



IPSEC Policy Config

Name: to_82

Enable: Enabled

Transport Mode: Tunnel

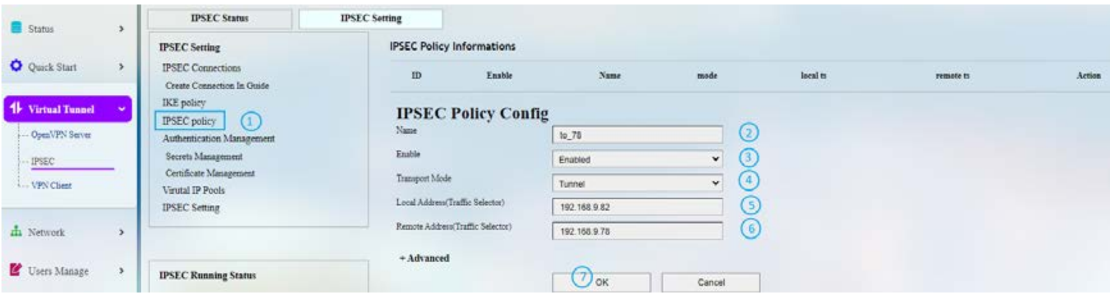
Local Address(Traffic Selector): 192.168.9.78

Remote Address(Traffic Selector): 192.168.9.82

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



IPSEC Policy Config

Name: to_78

Enable: Enabled

Transport Mode: Tunnel

Local Address(Traffic Selector): 192.168.9.82

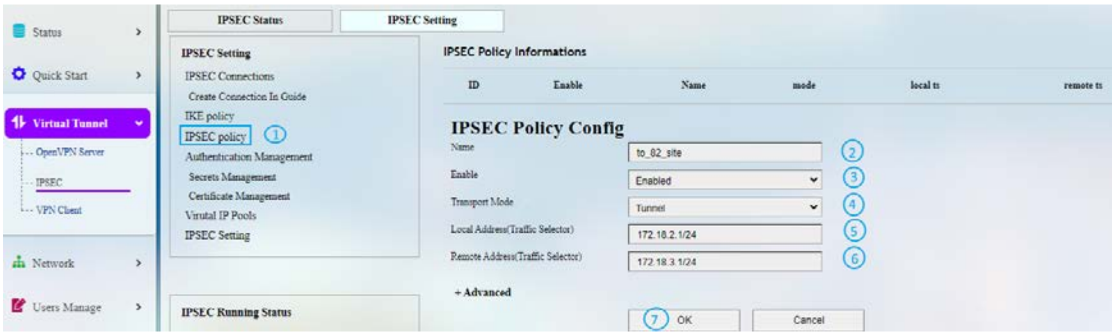
Remote Address(Traffic Selector): 192.168.9.78

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



Name: to_82_site

Enable: Enabled

Transport Mode: Tunnel

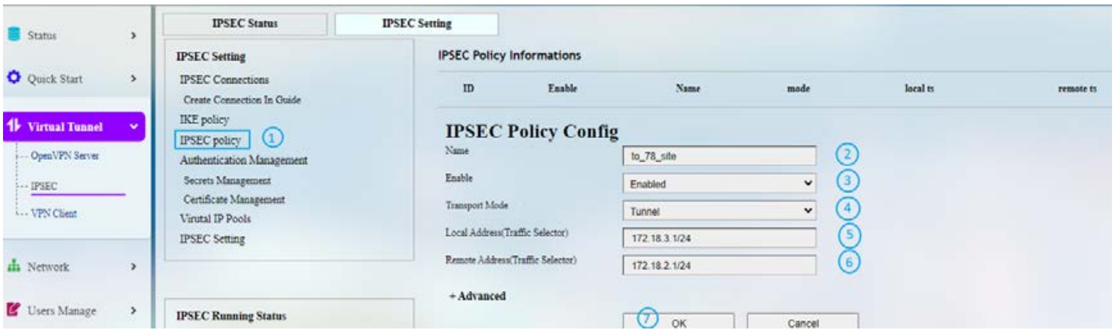
Local Address(Traffic Selector): 172.18.2.1/24

Remote Address(Traffic Selector): 172.18.3.1/24

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



Name: to_78_site

Enable: Enabled

Transport Mode: Tunnel

Local Address(Traffic Selector): 172.18.3.1/24

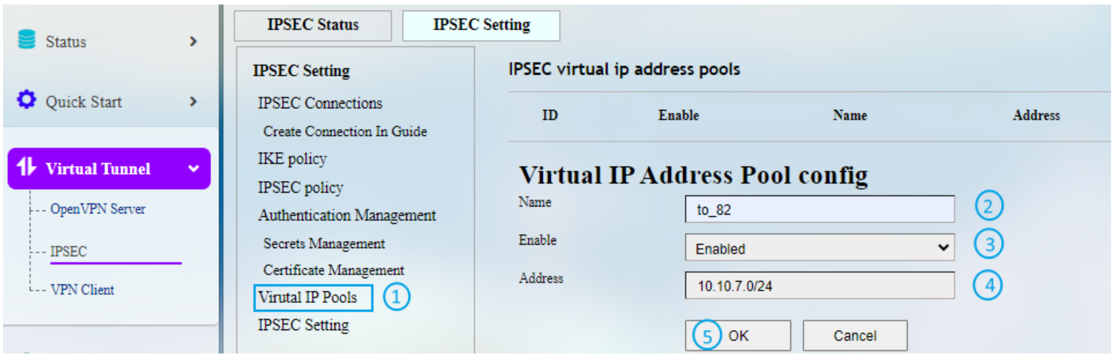
Remote Address(Traffic Selector): 172.18.2.1/24

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



IPSEC virtual ip address pools

| ID | Enable | Name | Address |
|---|---|---|---|

Virtual IP Address Pool config

Name: to_82

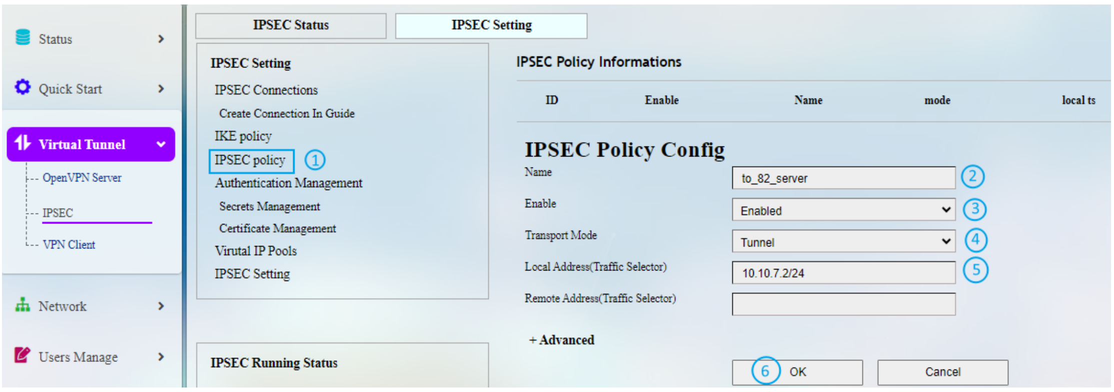
Enable: Enabled

Address: 10.10.7.0/24

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



IPSEC Policy Informations

| ID | Enable | Name | mode | local ts |
|---|---|---|---|---|

IPSEC Policy Config

Name: to_82_server

Enable: Enabled

Transport Mode: Tunnel

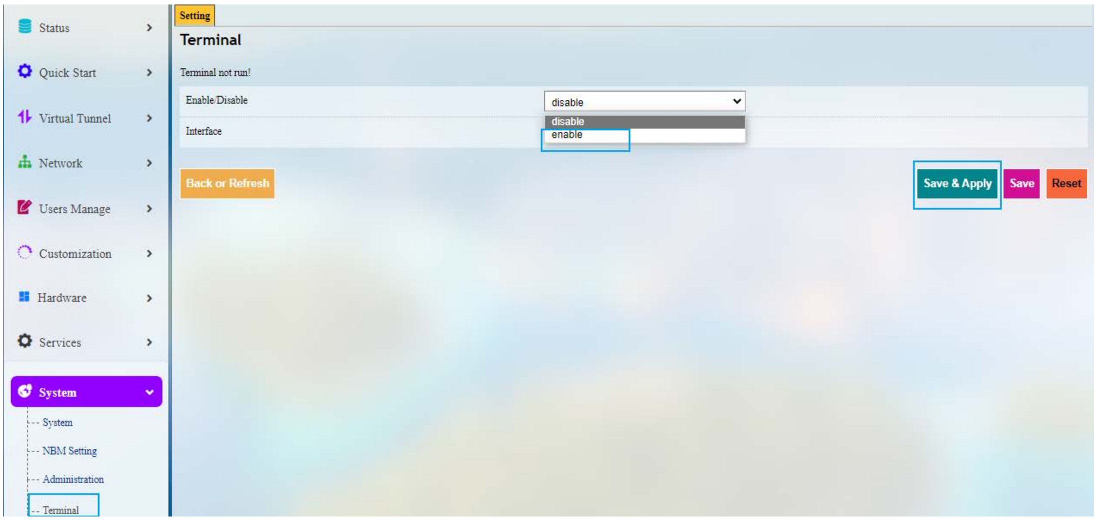
Local Address(Traffic Selector): 10.10.7.2/24

Remote Address(Traffic Selector):

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.



Terminal

Terminal not run!

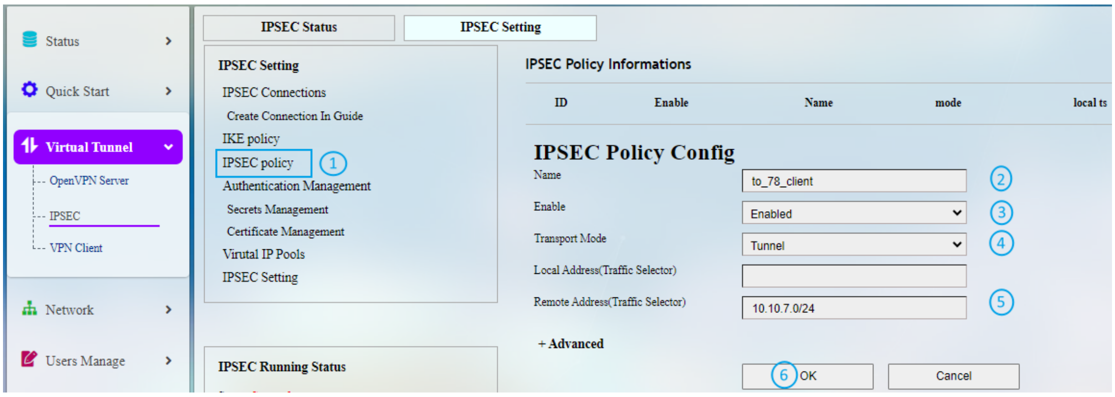
Enable/Disable: disable (disable / enable)

Interface

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



IPSEC Policy Informations

| ID | Enable | Name | mode | local ts |
|---|---|---|---|---|

IPSEC Policy Config

Name: to_78_client

Enable: Enabled

Transport Mode: Tunnel

Local Address(Traffic Selector):

Remote Address(Traffic Selector): 10.10.7.0/24

Description of the numbered areas

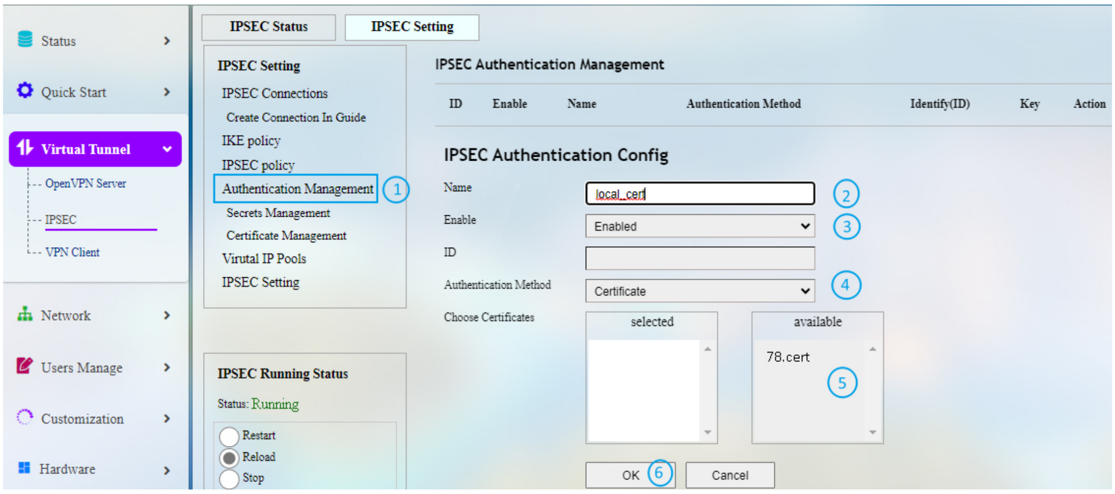
1. Navigate to **Virtual Tunnel > IPSEC > IPSEC Setting > IPSEC policy**
2. Assign a name to the policy (to_78_client)
3. Select **Enabled** from the dropdown list to enable the policy
4. Select **Tunnel** as the transport mode
5. Input the remote address: 10.10.7.0/24
6. Click **OK** to save the settings

### STEP 4: Authentication management

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

Certificate authentication

Configurations of G1 for local authentication



Name: local_cert

Enable: Enabled

ID:

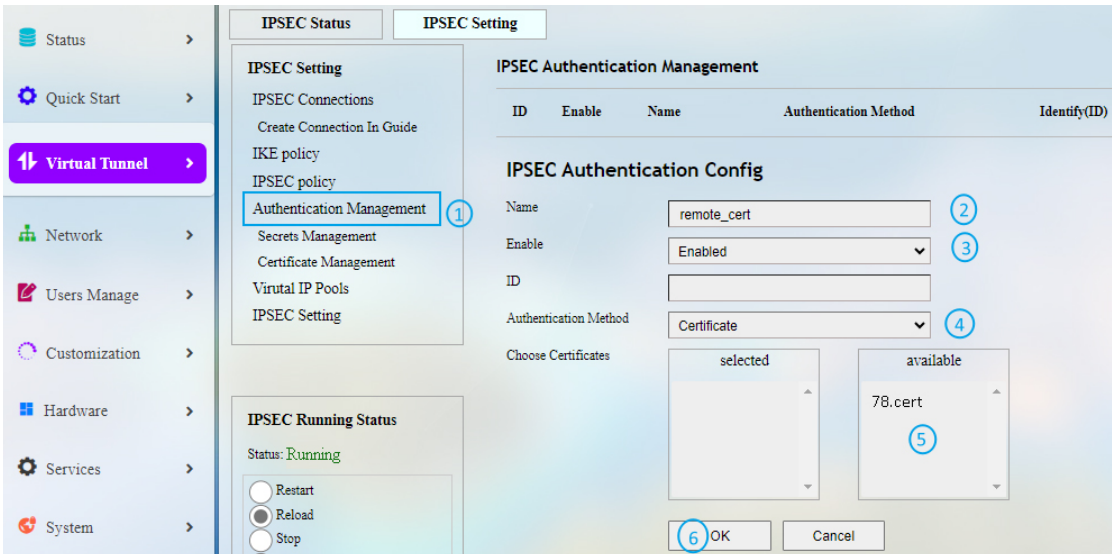
Authentication Method: Certificate

Choose Certificates: available: 78.cert

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



IPSEC Authentication Management

| ID | Enable | Name | Authentication Method | Identify(ID) |
|---|---|---|---|---|

IPSEC Authentication Config

| | |
|---|---|
| Name | remote_cert |
| Enable | Enabled |
| ID | |
| Authentication Method | Certificate |
| Choose Certificates | selected: <br> available: 78.cert |

IPSEC Running Status

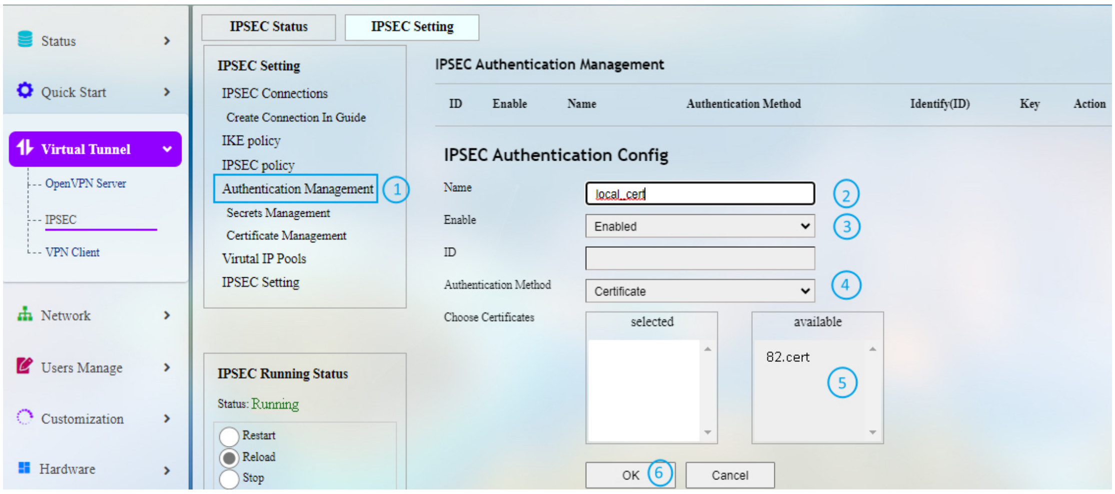
Status: Running

○ Restart
● Reload
○ Stop

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



IPSEC Running Status

Status: Running

○ Restart
● Reload
○ Stop

IPSEC Authentication Config

Name: local_cert

Enable: Enabled

ID:

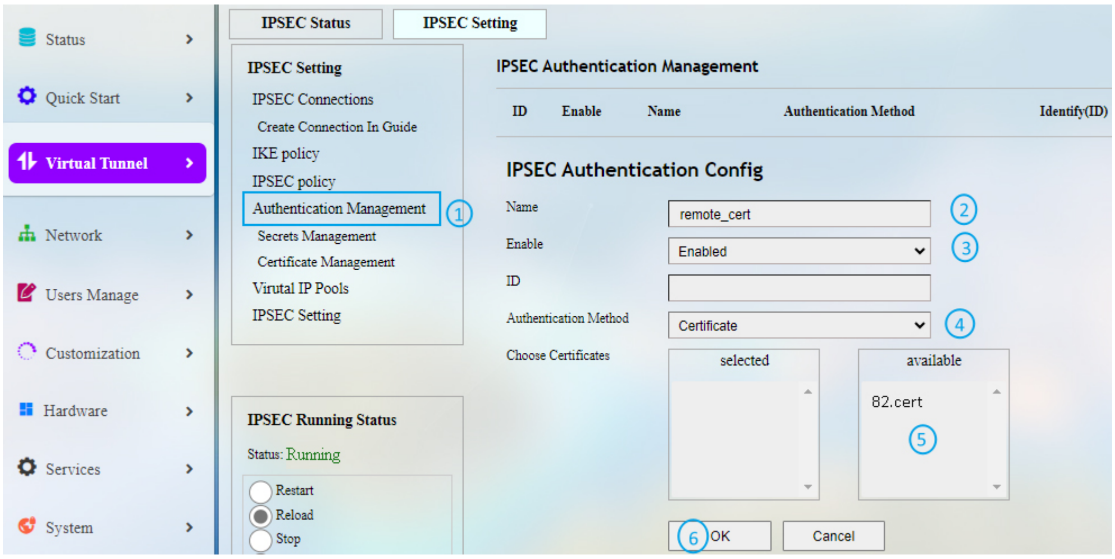
Authentication Method: Certificate

Choose Certificates: selected / available: 82.cert

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



Status: Running

○ Restart
● Reload
○ Stop

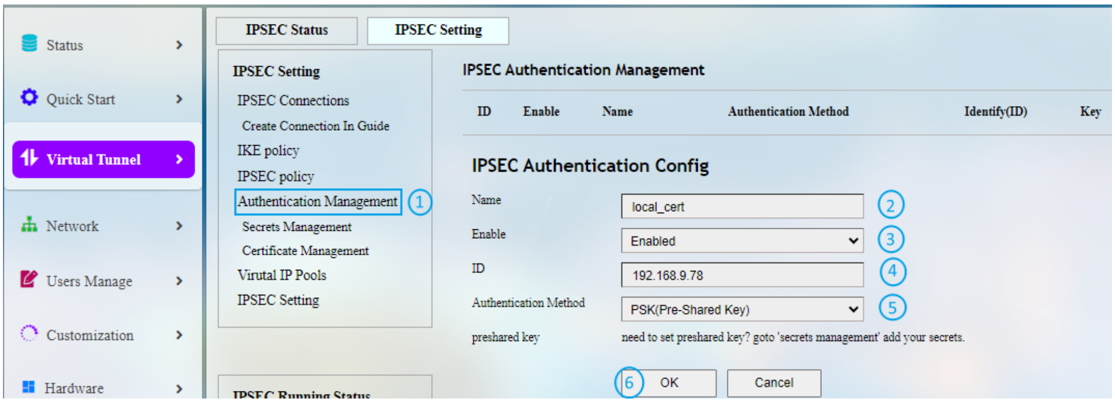
| | |
|---|---|
| Name | remote_cert |
| Enable | Enabled |
| ID | |
| Authentication Method | Certificate |
| Choose Certificates | selected: <br> available: 82.cert |

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



IPSEC Authentication Config

Name: local_cert

Enable: Enabled

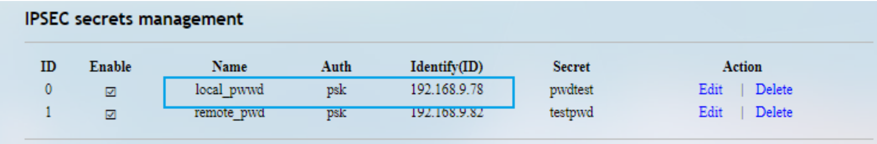
ID: 192.168.9.78

Authentication Method: PSK(Pre-Shared Key)

preshared key: need to set preshared key? goto 'secrets management' add your secrets.

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)

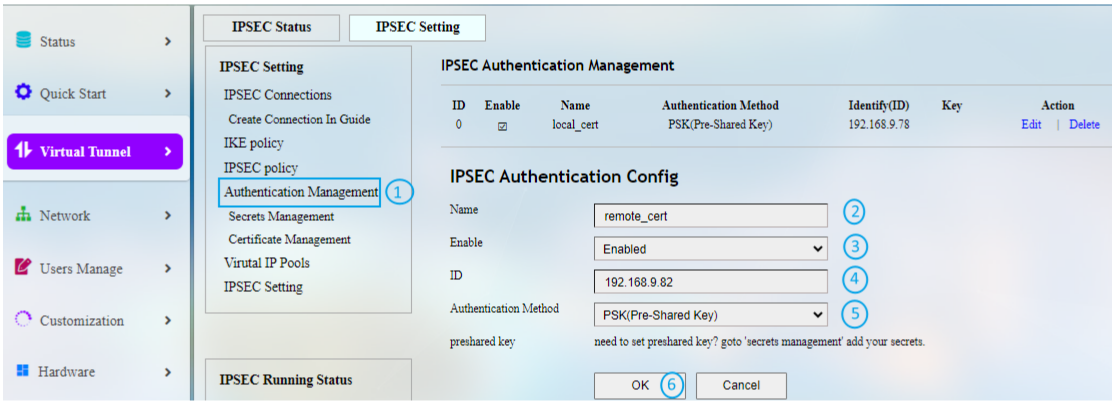


IPSEC secrets management

| ID | Enable | Name | Auth | Identify(ID) | Secret | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | local_pwwd | psk | 192.168.9.78 | pwdtest | Edit \| Delete |
| 1 | ☑ | remote_pwd | psk | 192.168.9.82 | testpwd | Edit \| Delete |

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



IPSEC Authentication Management

| ID | Enable | Name | Authentication Method | Identify(ID) | Key | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | local_cert | PSK(Pre-Shared Key) | 192.168.9.78 | | Edit \| Delete |

IPSEC Authentication Config

Name: remote_cert ②

Enable: Enabled ③

ID: 192.168.9.82 ④

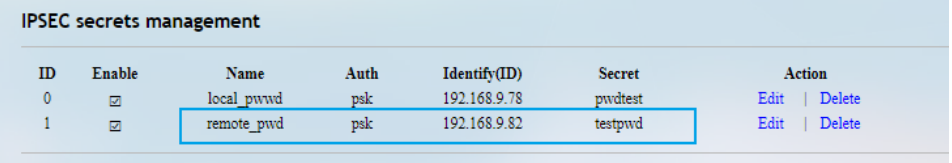
Authentication Method: PSK(Pre-Shared Key) ⑤

preshared key: need to set preshared key? goto 'secrets management' add your secrets.

OK ⑥ Cancel

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)

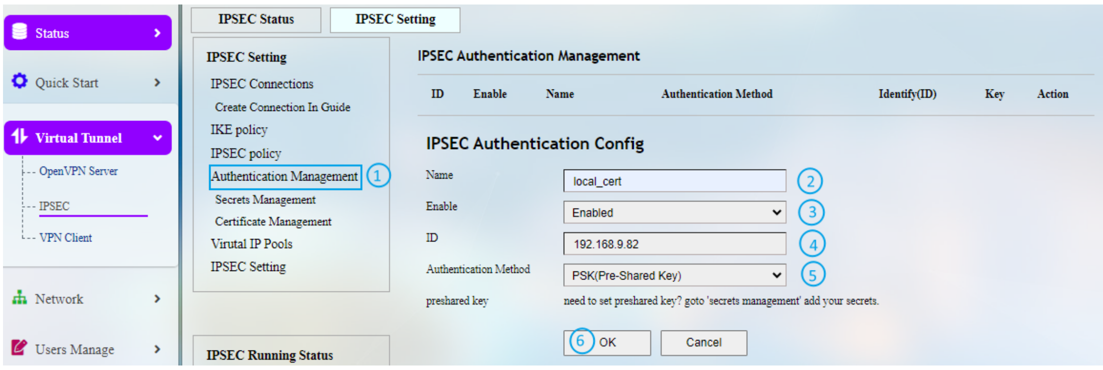


IPSEC secrets management

| ID | Enable | Name | Auth | Identify(ID) | Secret | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | local_pwwd | psk | 192.168.9.78 | pwdtest | Edit \| Delete |
| 1 | ☑ | remote_pwd | psk | 192.168.9.82 | testpwd | Edit \| Delete |

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

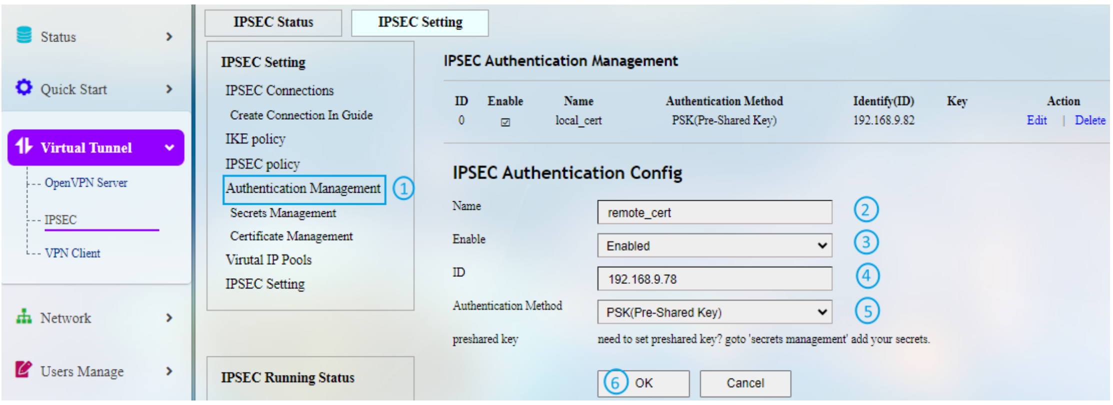


Name: local_cert
Enable: Enabled
ID: 192.168.9.82
Authentication Method: PSK(Pre-Shared Key)
preshared key: need to set preshared key? goto 'secrets management' add your secrets.

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



| ID | Enable | Name | Authentication Method | Identify(ID) | Key | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | local_cert | PSK(Pre-Shared Key) | 192.168.9.82 | | Edit \| Delete |

Name: remote_cert
Enable: Enabled
ID: 192.168.9.78
Authentication Method: PSK(Pre-Shared Key)
preshared key: need to set preshared key? goto 'secrets management' add your secrets.

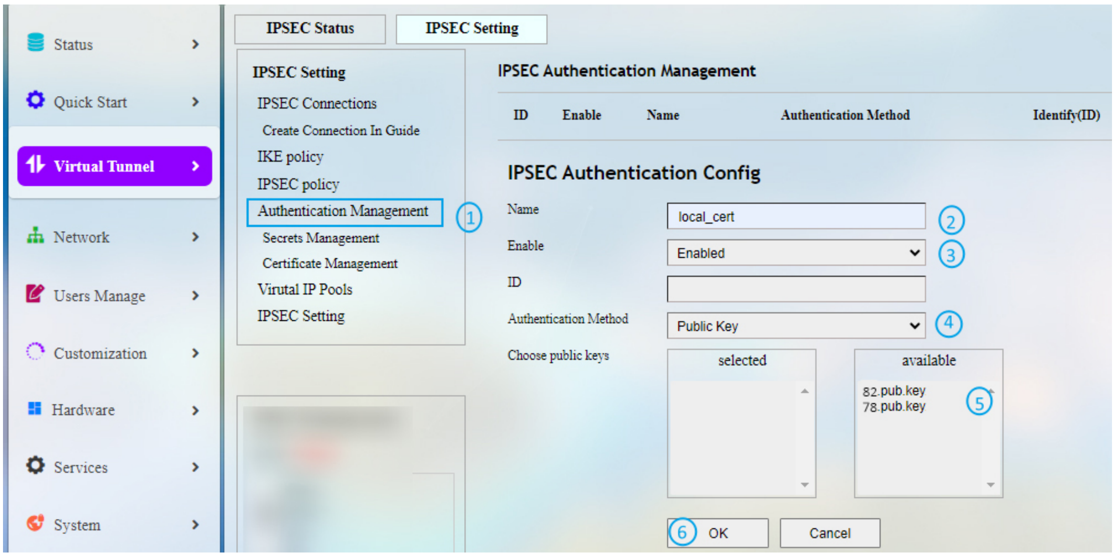
Description of the numbered areas

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



IPSEC Authentication Management

| ID | Enable | Name | Authentication Method | Identify(ID) |
|---|---|---|---|---|

IPSEC Authentication Config

Name: local_cert

Enable: Enabled

ID:

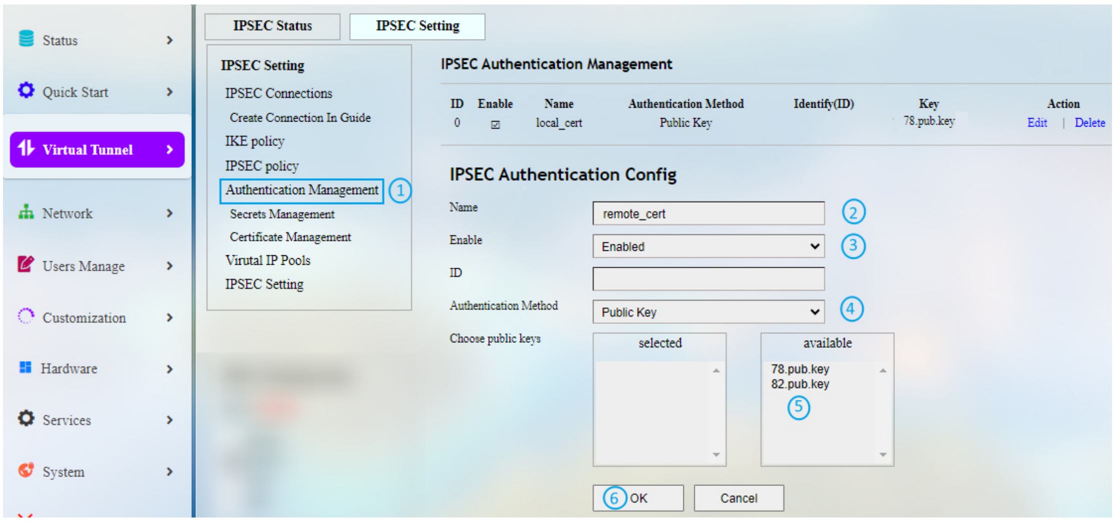
Authentication Method: Public Key

Choose public keys: selected | available: 82.pub.key, 78.pub.key

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



IPSEC Authentication Management

| ID | Enable | Name | Authentication Method | Identify(ID) | Key | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | local_cert | Public Key | | 78.pub.key | Edit \| Delete |

IPSEC Authentication Config

Name: remote_cert ②

Enable: Enabled ③

ID:

Authentication Method: Public Key ④

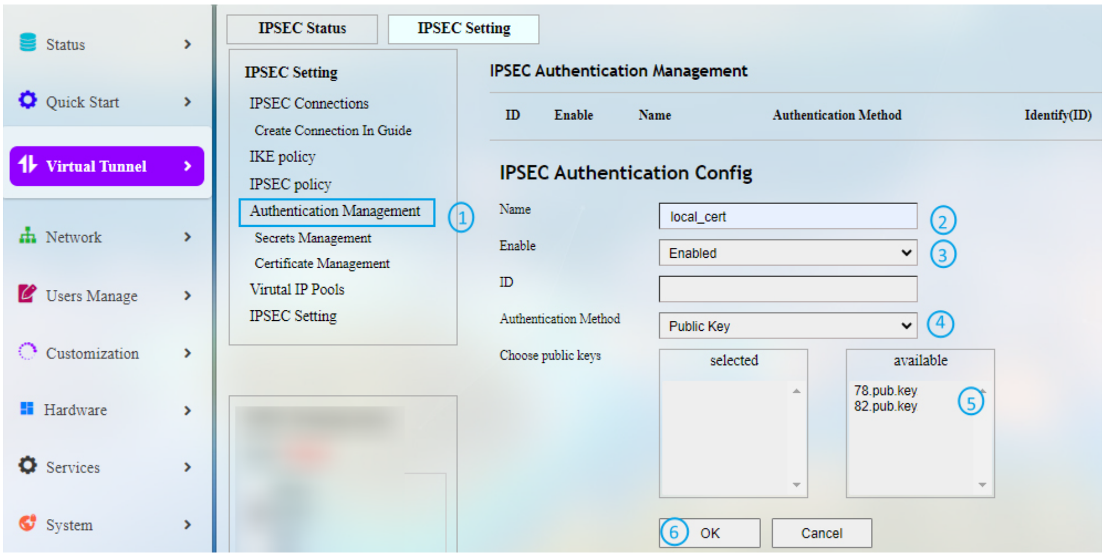
Choose public keys: selected / available: 78.pub.key, 82.pub.key ⑤

⑥ OK   Cancel

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



IPSEC Authentication Management

| ID | Enable | Name | Authentication Method | Identify(ID) |
|---|---|---|---|---|

IPSEC Authentication Config

Name: local_cert

Enable: Enabled

ID:

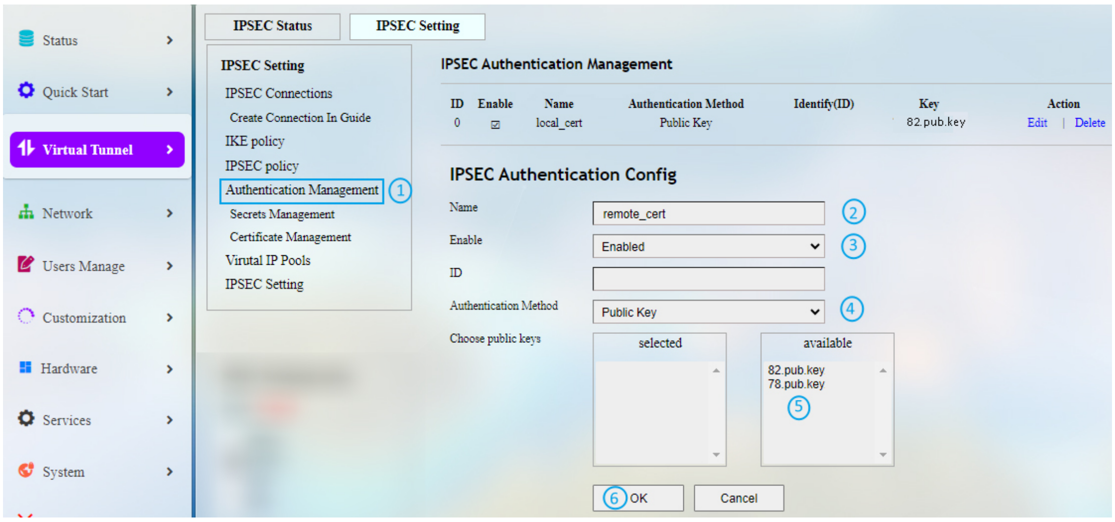
Authentication Method: Public Key

Choose public keys: selected | available: 78.pub.key, 82.pub.key

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



IPSEC Authentication Management

| ID | Enable | Name | Authentication Method | Identify(ID) | Key | Action |
|---|---|---|---|---|---|---|
| 0 | ☑ | local_cert | Public Key | | 82.pub.key | Edit \| Delete |

IPSEC Authentication Config

Name: remote_cert

Enable: Enabled

ID:

Authentication Method: Public Key

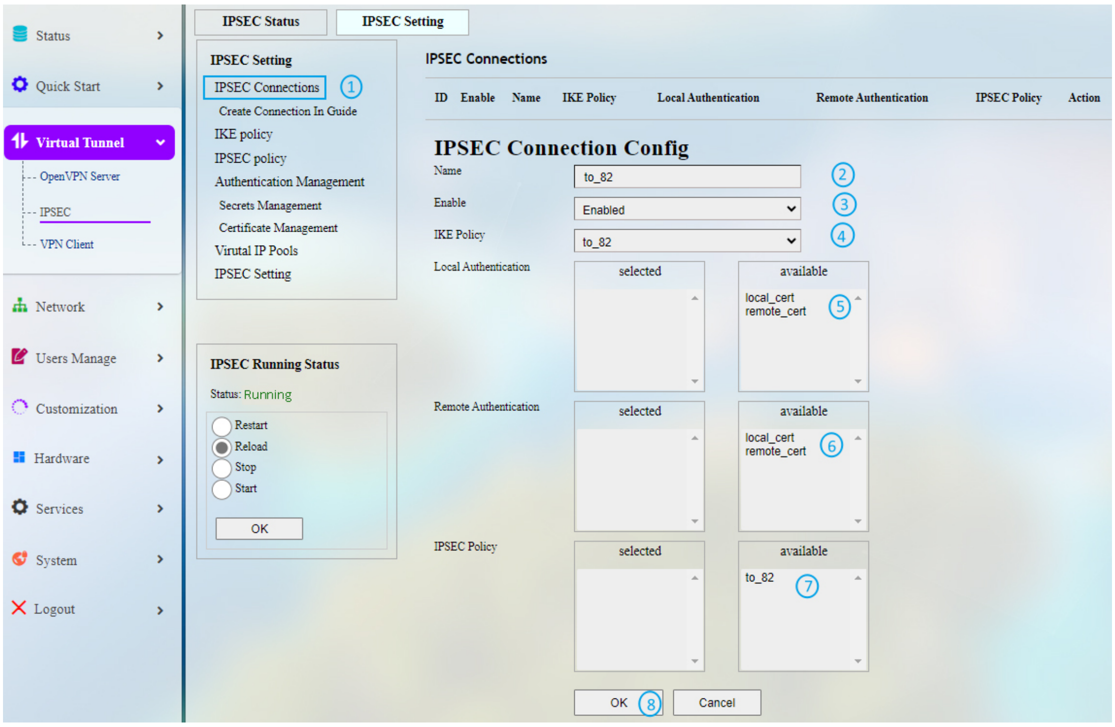
Choose public keys: selected / available: 82.pub.key, 78.pub.key

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



IPSEC Connection Config

Name: to_82

Enable: Enabled

IKE Policy: to_82

Local Authentication: selected / available: local_cert, remote_cert

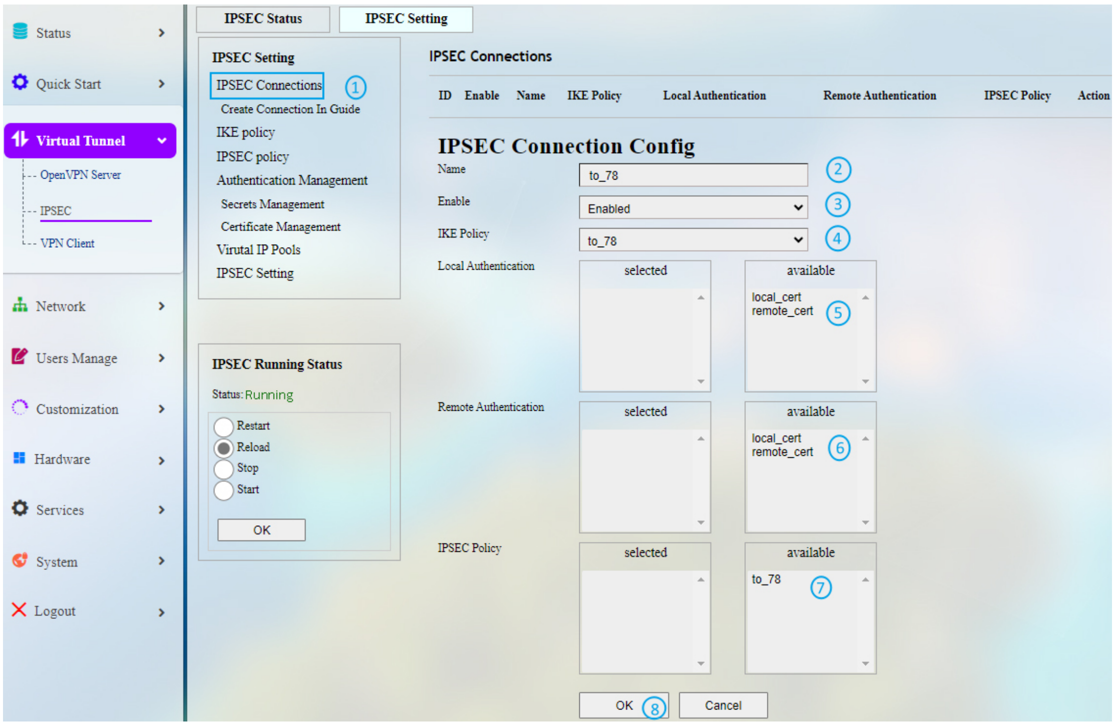
Remote Authentication: selected / available: local_cert, remote_cert

IPSEC Policy: selected / available: to_82

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



Name: to_78

Enable: Enabled

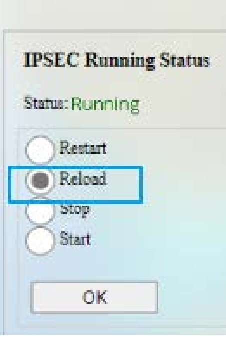
IKE Policy: to_78

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.



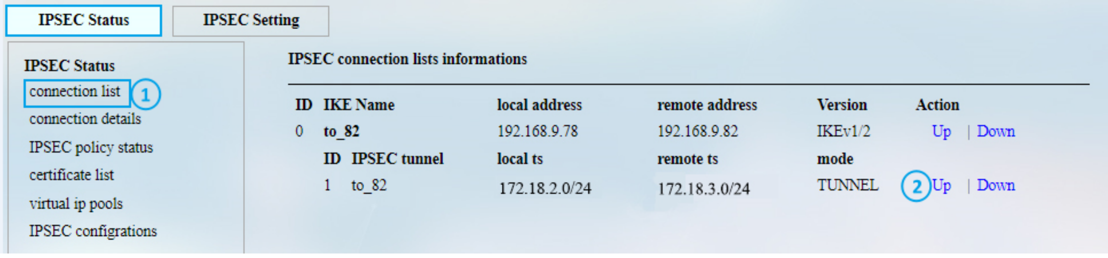
IPSEC Running Status

Status: Running

○ Restart
● Reload
○ Stop
○ Start

OK

### STEP 7: IPSec connection



IPSEC Status | IPSEC Setting

IPSEC Status
- connection list 1
- connection details
- IPSEC policy status
- certificate list
- virtual ip pools
- IPSEC configrations

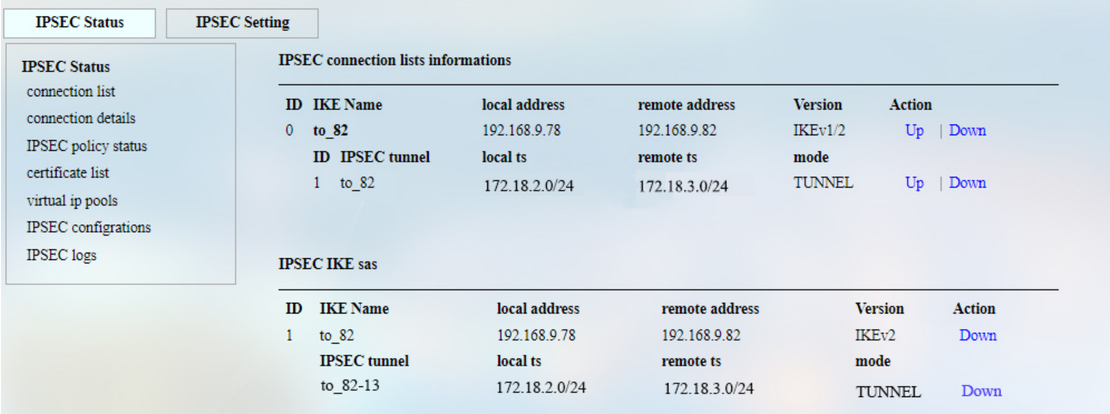
IPSEC connection lists informations

| ID | IKE Name | local address | remote address | Version | Action |
|---|---|---|---|---|---|
| 0 | to_82 | 192.168.9.78 | 192.168.9.82 | IKEv1/2 | Up \| Down |
| ID | IPSEC tunnel | local ts | remote ts | mode | |
| 1 | to_82 | 172.18.2.0/24 | 172.18.3.0/24 | TUNNEL | 2 Up \| Down |

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.



IPSEC Status | IPSEC Setting

IPSEC Status
- connection list
- connection details
- IPSEC policy status
- certificate list
- virtual ip pools
- IPSEC configrations
- IPSEC logs

IPSEC connection lists informations

| ID | IKE Name | local address | remote address | Version | Action |
|---|---|---|---|---|---|
| 0 | to_82 | 192.168.9.78 | 192.168.9.82 | IKEv1/2 | Up \| Down |
| ID | IPSEC tunnel | local ts | remote ts | mode | |
| 1 | to_82 | 172.18.2.0/24 | 172.18.3.0/24 | TUNNEL | Up \| Down |

IPSEC IKE sas

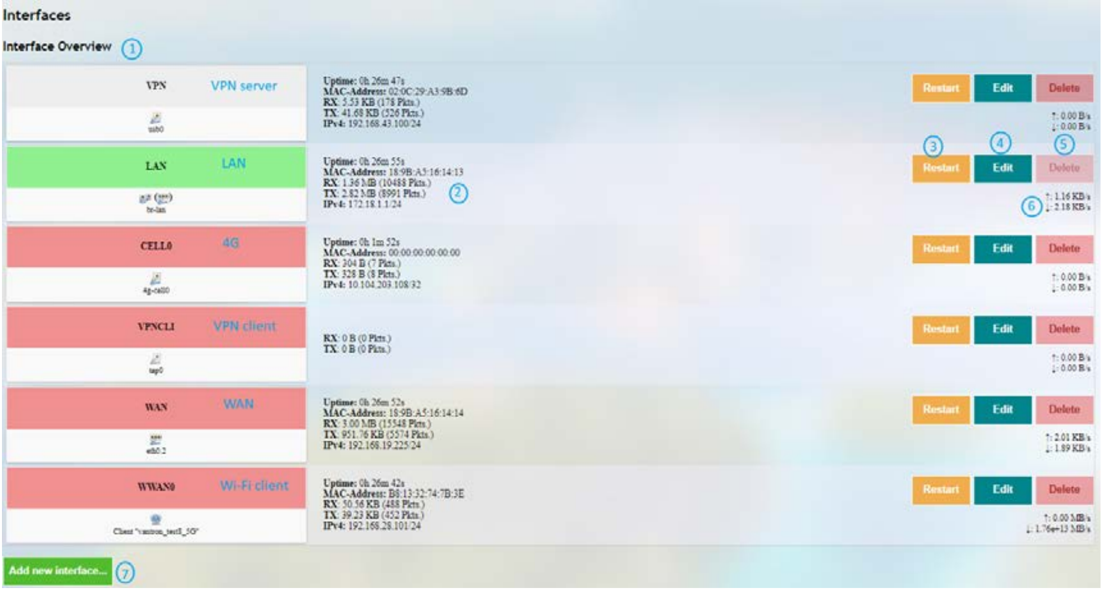
| ID | IKE Name | local address | remote address | Version | Action |
|---|---|---|---|---|---|
| 1 | to_82 | 192.168.9.78 | 192.168.9.82 | IKEv2 | Down |
| | IPSEC tunnel | local ts | remote ts | mode | |
| | to_82-13 | 172.18.2.0/24 | 172.18.3.0/24 | TUNNEL | Down |

# 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**.



VPN
Uptime: 0h 26m 47s
MAC-Address: 02:0C:29:A3:9B:6D
RX: 5.53 KB (178 Pkts.)
TX: 41.68 KB (526 Pkts.)
IPv4: 192.168.43.100/24
↑: 0.00 B/s
↓: 0.00 B/s

LAN
Uptime: 0h 26m 55s
MAC-Address: 18:9B:A5:16:14:13
RX: 1.36 MB (10488 Pkts.)
TX: 2.82 MB (8991 Pkts.)
IPv4: 172.18.1.1/24
↑: 1.16 KB/s
↓: 2.18 KB/s

CELL0
Uptime: 0h 1m 52s
MAC-Address: 00:00:00:00:00:00
RX: 304 B (7 Pkts.)
TX: 328 B (8 Pkts.)
IPv4: 10.104.203.108/32
↑: 0.00 B/s
↓: 0.00 B/s

VPNCLI
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
↑: 0.00 B/s
↓: 0.00 B/s

WAN
Uptime: 0h 26m 52s
MAC-Address: 18:9B:A5:16:14:14
RX: 3.00 MB (15548 Pkts.)
TX: 951.76 KB (5574 Pkts.)
IPv4: 192.168.19.225/24
↑: 2.01 KB/s
↓: 1.89 KB/s

WWAN0
Uptime: 0h 26m 42s
MAC-Address: B8:13:32:74:7B:3E
RX: 50.56 KB (488 Pkts.)
TX: 39.23 KB (452 Pkts.)
IPv4: 192.168.28.101/24
↑: 0.00 MB/s
↓: 1.76e+13 MB/s

Take the LAN port for example, the numbered areas are as follows:

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)

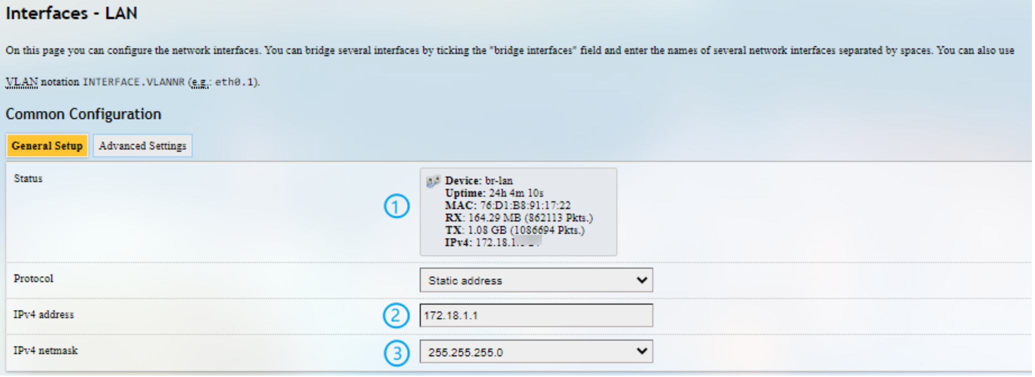
*The interfaces may differ from what is shown above as certain interfaces are related to your prior settings and the communication modules available on the device.*

The following section illustrates on how to edit the LAN port and WAN port settings of the Router.

### 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.



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status ①
Device: br-lan
Uptime: 24h 4m 10s
MAC: 76:D1:B8:91:17:22
RX: 164.29 MB (862113 Pkts.)
TX: 1.08 GB (1086694 Pkts.)
IPv4: 172.18.1.[redacted]

Protocol: Static address

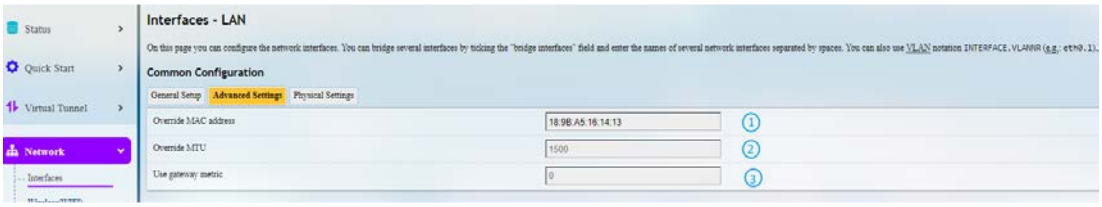
IPv4 address ②: 172.18.1.1

IPv4 netmask ③: 255.255.255.0

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:



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Override MAC address: 18:9B:A5:16:14:13 ①

Override MTU: 1500 ②

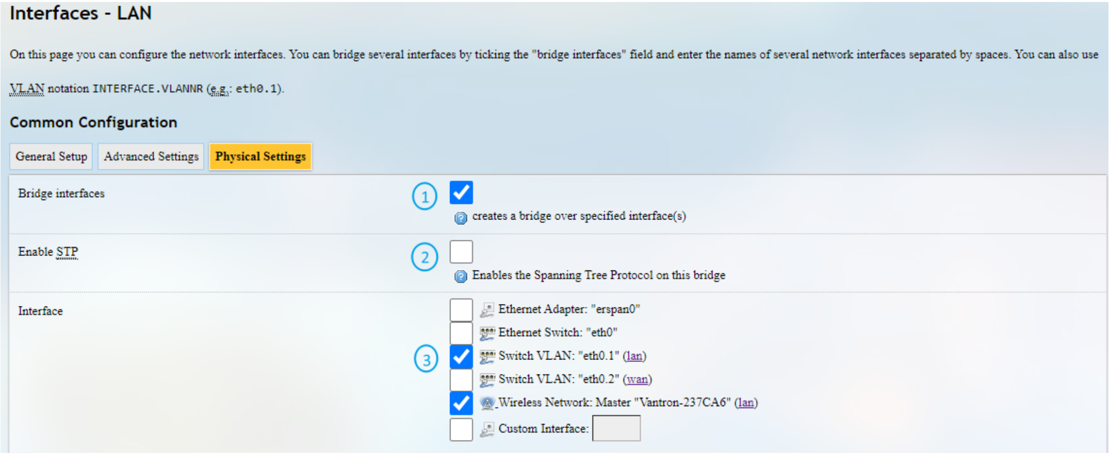
Use gateway metric: 0 ③

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.



### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

**Common Configuration**

Bridge interfaces ① ☑ creates a bridge over specified interface(s)

Enable STP ② □ Enables the Spanning Tree Protocol on this bridge

Interface ③
- □ Ethernet Adapter: "erspan0"
- □ Ethernet Switch: "eth0"
- ☑ Switch VLAN: "eth0.1" (lan)
- □ Switch VLAN: "eth0.2" (wan)
- ☑ Wireless Network: Master "Vantron-237CA6" (lan)
- □ Custom Interface:

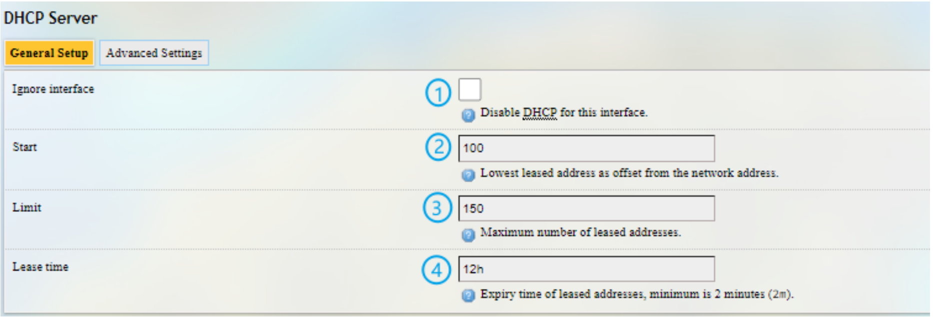
Description of the numbered areas

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



| | | | |
|---|---|---|---|
| Ignore interface | ① | □ | Disable DHCP for this interface. |
| Start | ② | 100 | Lowest leased address as offset from the network address. |
| Limit | ③ | 150 | Maximum number of leased addresses. |
| Lease time | ④ | 12h | Expiry time of leased addresses, minimum is 2 minutes (2m). |

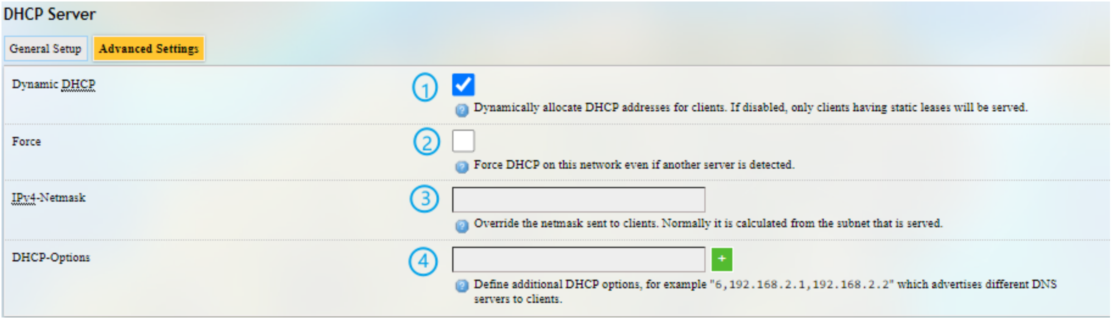
Description of the numbered areas

1. Disable the DHCP service

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

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:



| | | | |
|---|---|---|---|
| Dynamic DHCP | ① | ☑ | Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served. |
| Force | ② | □ | Force DHCP on this network even if another server is detected. |
| IPv4-Netmask | ③ | | Override the netmask sent to clients. Normally it is calculated from the subnet that is served. |
| DHCP-Options | ④ | | Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients. |

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.*

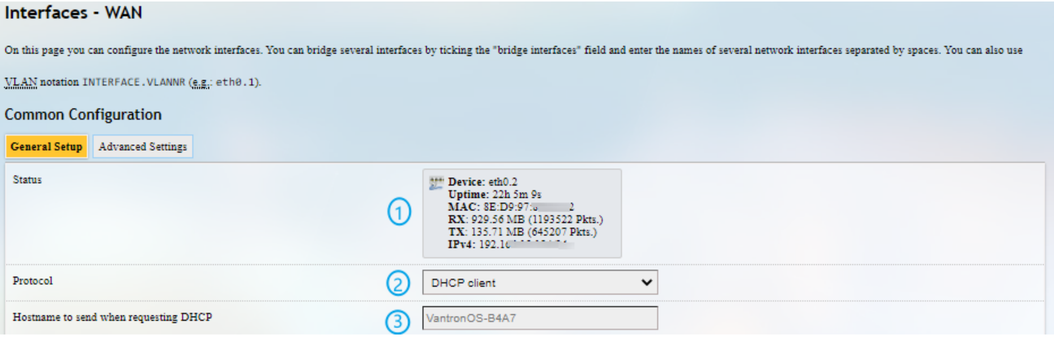
4. Add different DNS servers for client devices

*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.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup | Advanced Settings

Status ① 
**Device:** eth0.2
**Uptime:** 22h 5m 9s
**MAC:** 8E:D9:97:[redacted]
**RX:** 929.56 MB (1193522 Pkts.)
**TX:** 135.71 MB (645207 Pkts.)
**IPv4:** 192.1[redacted]

Protocol ② DHCP client

Hostname to send when requesting DHCP ③ VantronOS-B4A7

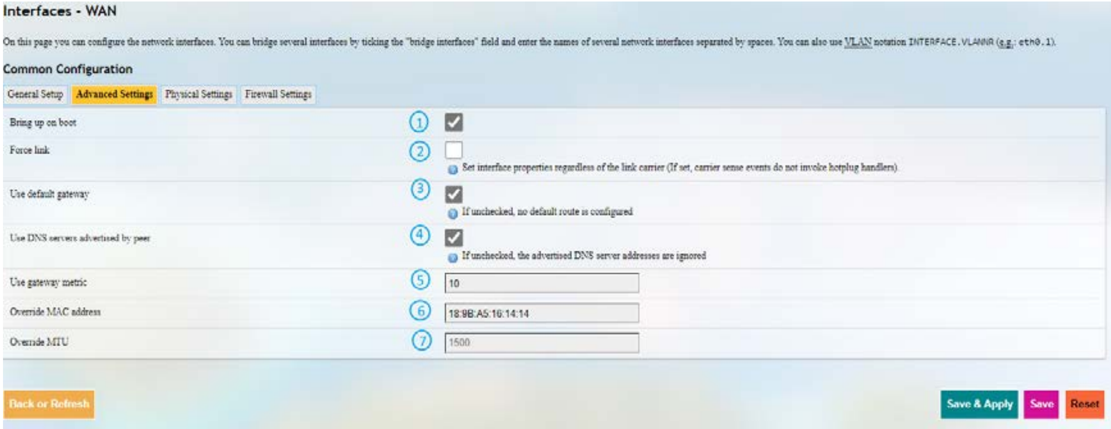
Description of the numbered areas

1. Status of the WAN port
2. Select a WAN protocol (DHCP client by default)
3. Input a hostname of the Router for 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.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

| | | |
|---|---|---|
| Bring up on boot | ① | ☑ |
| Force link | ② | ☐<br>Set interface properties regardless of the link carrier (If set, carrier sense events do not invoke hotplug handlers). |
| Use default gateway | ③ | ☑<br>If unchecked, no default route is configured |
| Use DNS servers advertised by peer | ④ | ☑<br>If unchecked, the advertised DNS server addresses are ignored |
| Use gateway metric | ⑤ | 10 |
| Override MAC address | ⑥ | 18:9B:A5:16:14:14 |
| Override MTU | ⑦ | 1500 |

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**

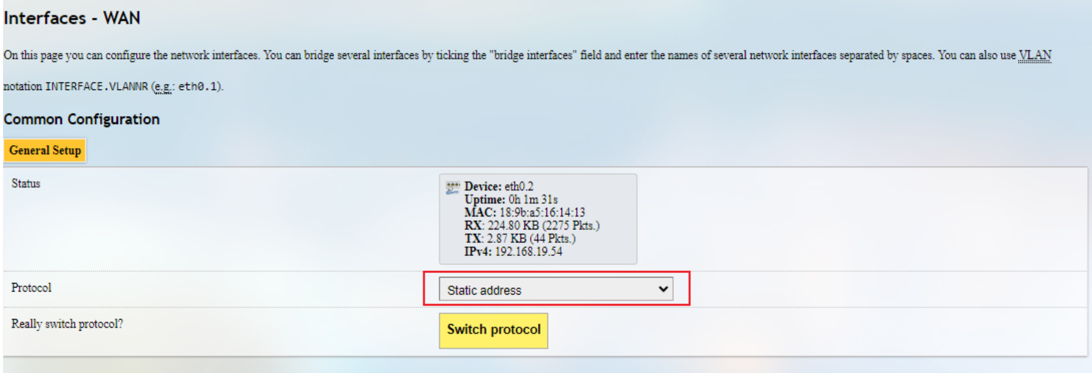
*If this option is disabled, you will need to define a DNS server.*

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 protocol drop-down list under **General Setup** of the WAN port and click **Switch protocol**.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

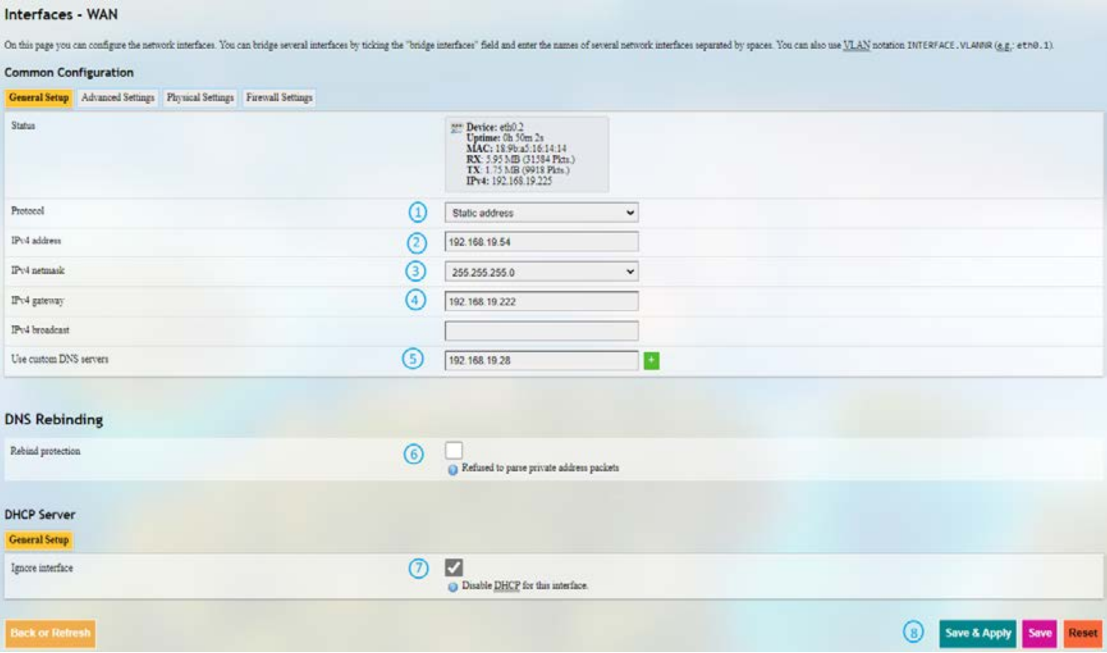
General Setup

Status: Device: eth0.2<br>Uptime: 0h 1m 31s<br>MAC: 18:9b:a5:16:14:13<br>RX: 224.80 KB (2275 Pkts.)<br>TX: 2.87 KB (44 Pkts.)<br>IPv4: 192.168.19.54

Protocol: Static address

Really switch protocol? Switch protocol

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



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Status: Device: eth0.2<br>Uptime: 0h 50m 2s<br>MAC: 18:9b:a5:16:14:14<br>RX: 5.95 MB (31584 Pkts.)<br>TX: 1.75 MB (9918 Pkts.)<br>IPv4: 192.168.19.225

Protocol ① Static address

IPv4 address ② 192.168.19.54

IPv4 netmask ③ 255.255.255.0

IPv4 gateway ④ 192.168.19.222

IPv4 broadcast

Use custom DNS servers ⑤ 192.168.19.28

DNS Rebinding

Rebind protection ⑥ □ Refused to parse private address packets

DHCP Server

General Setup

Ignore interface ⑦ ☑ Disable DHCP for this interface.

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.*

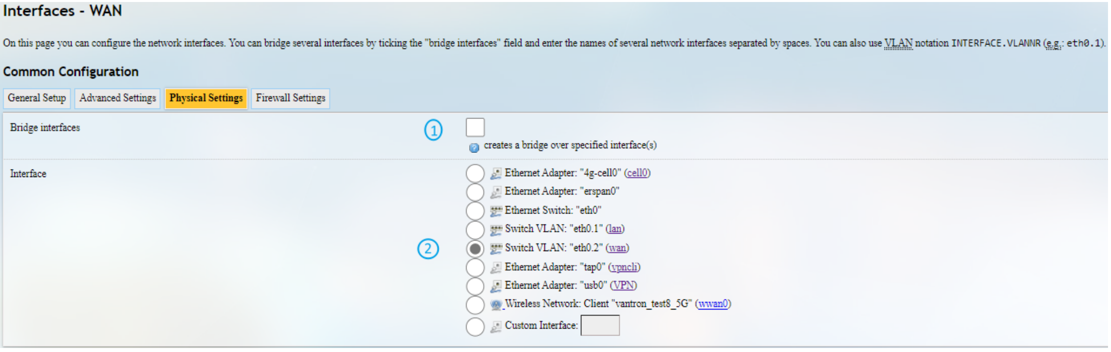
*When static address protocol is selected, DHCP server will be automatically disabled.*

*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.



**Interfaces - WAN**

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

**Common Configuration**

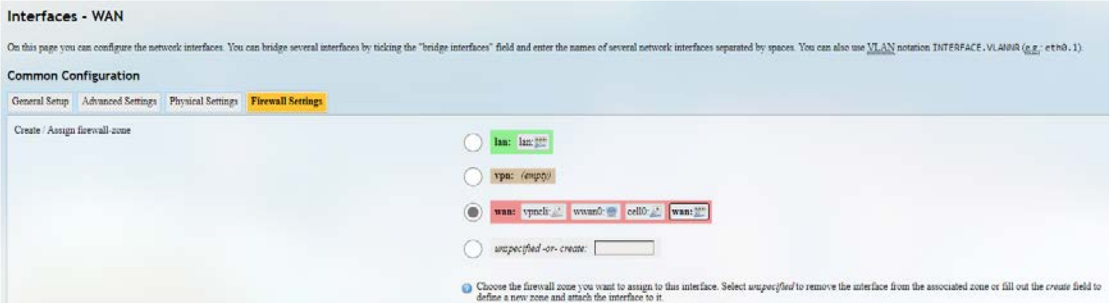
Bridge interfaces ☐
creates a bridge over specified interface(s)

Interface
○ Ethernet Adapter: "4g-cell0" (cell0)
○ Ethernet Adapter: "erspan0"
○ Ethernet Switch: "eth0"
○ Switch VLAN: "eth0.1" (lan)
● Switch VLAN: "eth0.2" (wan)
○ Ethernet Adapter: "tap0" (vpncli)
○ Ethernet Adapter: "usb0" (VPN)
○ Wireless Network: Client "vantron_test8_5G" (wwan0)
○ Custom Interface:

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.



**Interfaces - WAN**

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

**Common Configuration**

Create / Assign firewall-zone
○ lan: lan:
○ vpn: (empty)
● wan: vpncli: wwan0: cell0: wan:
○ unspecified -or- create:

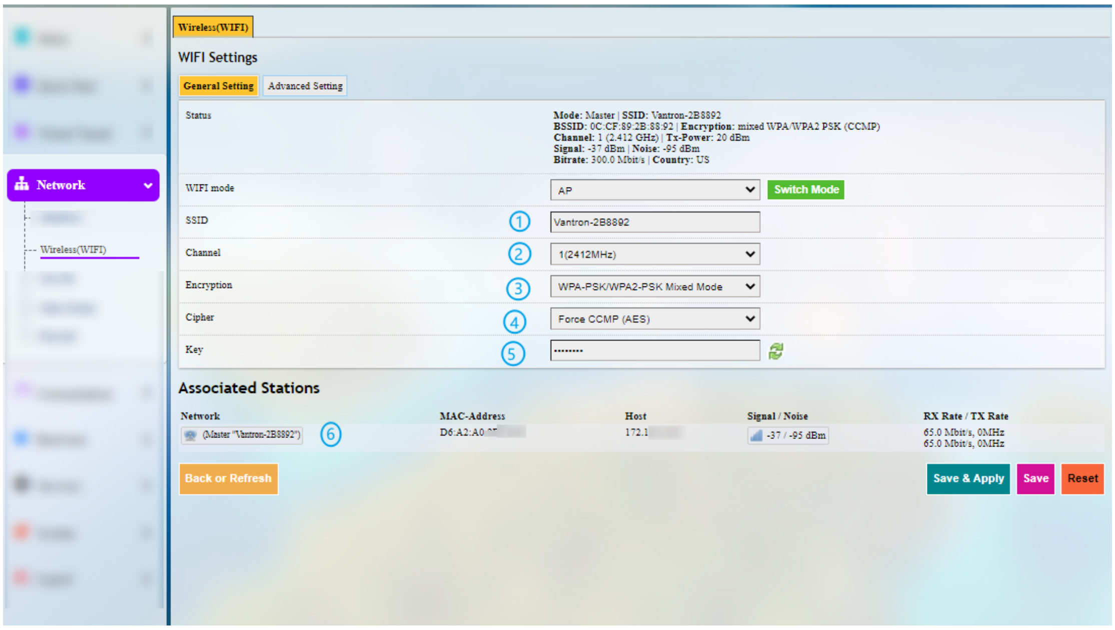
Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

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.

### 3.6.2.1 Wi-Fi – AP Mode (General settings)



WIFI Settings

| | |
|---|---|
| Status | **Mode:** Master \| **SSID:** Vantron-2B8892<br>**BSSID:** 0C:CF:89:2B:88:92 \| **Encryption:** mixed WPA/WPA2 PSK (CCMP)<br>**Channel:** 1 (2.412 GHz) \| **Tx-Power:** 20 dBm<br>**Signal:** -37 dBm \| **Noise:** -95 dBm<br>**Bitrate:** 300.0 Mbit/s \| **Country:** US |
| WIFI mode | AP |
| SSID | Vantron-2B8892 |
| Channel | 1(2412MHz) |
| Encryption | WPA-PSK/WPA2-PSK Mixed Mode |
| Cipher | Force CCMP (AES) |
| Key | •••••••• |

Associated Stations

| Network | MAC-Address | Host | Signal / Noise | RX Rate / TX Rate |
|---|---|---|---|---|
| (Master "Vantron-2B8892") | D6:A2:A0[redacted] | 172.1[redacted] | -37 / -95 dBm | 65.0 Mbit/s, 0MHz<br>65.0 Mbit/s, 0MHz |

Description of the numbered areas

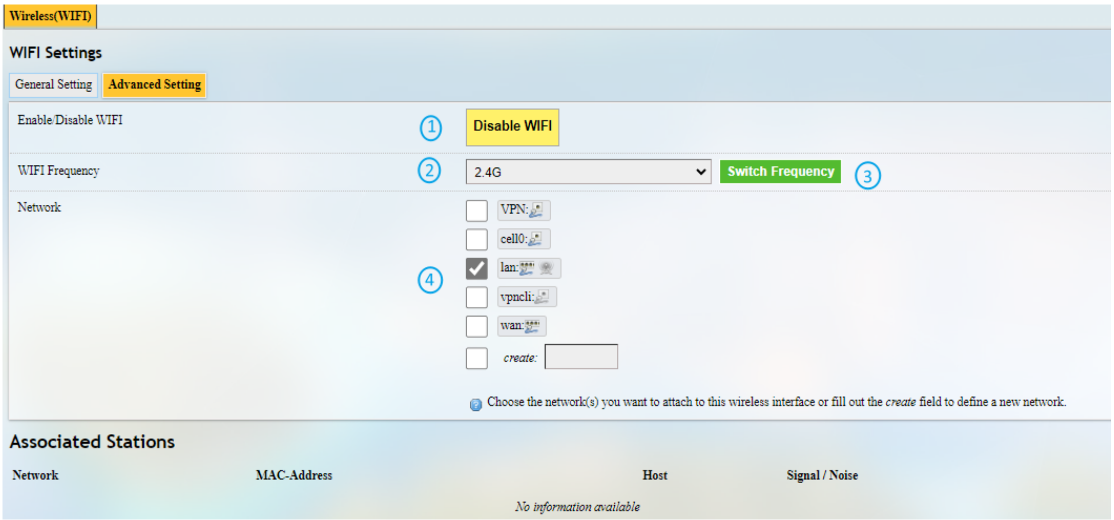
1. Set an SSID for the Router

*The ID name shall not contain special 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)



Wireless(WIFI)

WIFI Settings

General Setting | Advanced Setting

Enable/Disable WIFI ① Disable WIFI

WIFI Frequency ② 2.4G Switch Frequency ③

Network ④
☐ VPN:
☐ cell0:
☑ lan:
☐ vpncli:
☐ wan:
☐ *create:*

Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Associated Stations

| Network | MAC-Address | Host | Signal / Noise |
|---|---|---|---|
| *No information available* | | | |

Description of the numbered areas

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

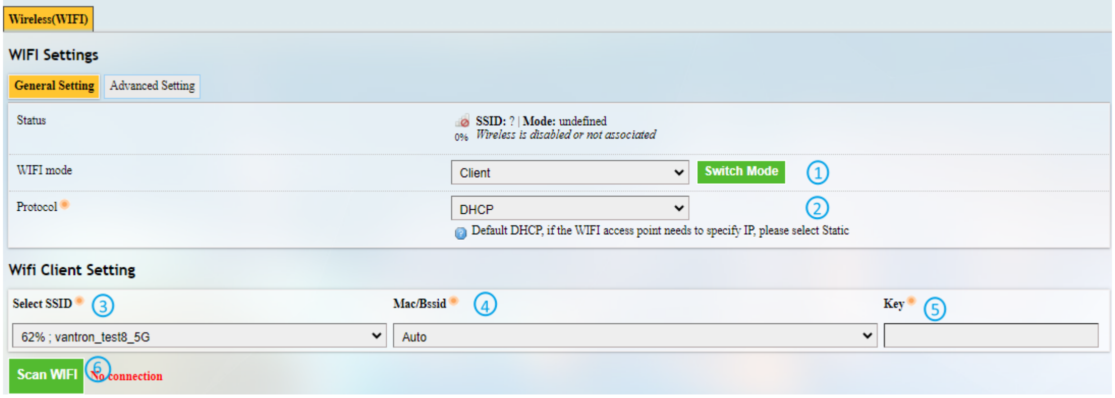
*As modification of field 2 will have impact on the Wi-Fi signal, the web interface will return to the general settings page upon a click of the switch button.*

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

### 3.6.2.3 Wi-Fi – Client Mode

When the Router 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.*



Status: SSID: ? | Mode: undefined
0% *Wireless is disabled or not associated*

WIFI mode: Client

Protocol *: DHCP
Default DHCP, if the WIFI access point needs to specify IP, please select Static

Select SSID *: 62% ; vantron_test8_5G
Mac/Bssid *: Auto
Key *:

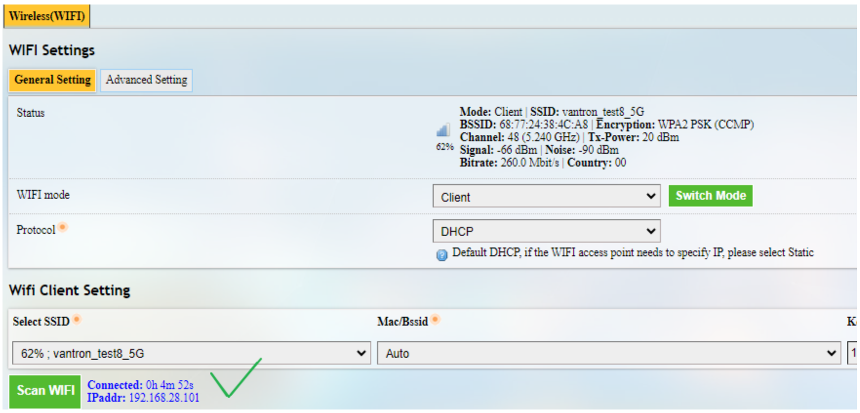
No connection

Description of the numbered areas

1. Switch to **Client mode**
2. Select DHCP protocol to automatically get an IP or Static protocol to specify an IP for the Router
3. Select a wireless network for internet access
4. Select the MAC address of the access point or leave it to 'Auto' if not sure
5. Input the password of the Wi-Fi
6. Click **Scan WIFI** to refresh the Wi-Fi list if the target SSID is not identified

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

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



Status: 62%
**Mode:** Client | **SSID:** vantron_test8_5G
**BSSID:** 68:77:24:38:4C:A8 | **Encryption:** WPA2 PSK (CCMP)
**Channel:** 48 (5.240 GHz) | **Tx-Power:** 20 dBm
**Signal:** -66 dBm | **Noise:** -90 dBm
**Bitrate:** 260.0 Mbit/s | **Country:** 00

WIFI mode: Client

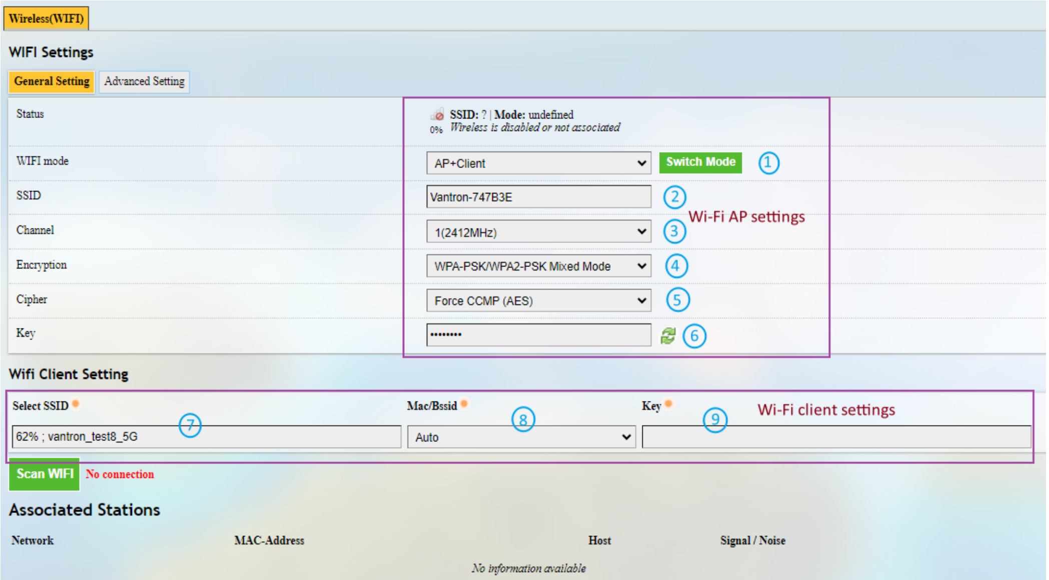
Protocol *: DHCP
Default DHCP, if the WIFI access point needs to specify IP, please select Static

Select SSID *: 62% ; vantron_test8_5G
Mac/Bssid *: Auto
K

**Connected:** 0h 4m 52s
**IPaddr:** 192.168.28.101

### 3.6.2.4 Wi-Fi – AP + Client Mode

This mode enables you to use the Router as an AP to allow client devices to join after it connects a Wi-Fi AP as a client.



Wireless(WIFI)

WIFI Settings

General Setting | Advanced Setting

Status: SSID: ? | Mode: undefined
0% Wireless is disabled or not associated

WIFI mode: AP+Client — Switch Mode ①

SSID: Vantron-747B3E ②

Channel: 1(2412MHz) ③

Encryption: WPA-PSK/WPA2-PSK Mixed Mode ④

Cipher: Force CCMP (AES) ⑤

Key: •••••••• ⑥

Wi-Fi AP settings

Wifi Client Setting

Select SSID: 62% ; vantron_test8_5G ⑦

Mac/Bssid: Auto ⑧

Key: ⑨

Wi-Fi client settings

Scan WIFI — No connection

Associated Stations

| Network | MAC-Address | Host | Signal / Noise |
|---|---|---|---|
| *No information available* | | | |

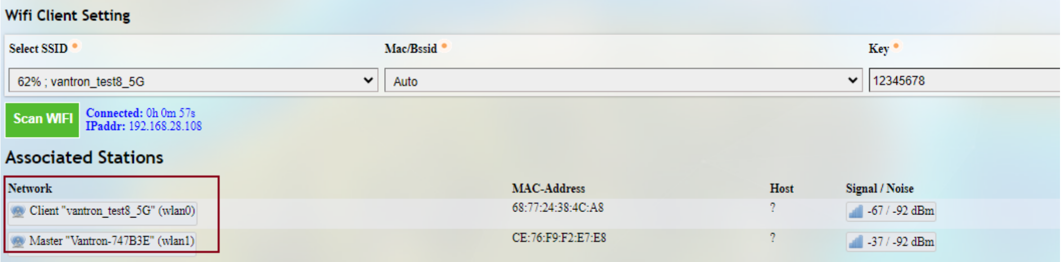
Description of the numbered areas

1. Switch to **AP + Client mode**
2. Set an SSID for the Router
3. Select a Wi-Fi channel
4. Select an encryption method (the following options vary with the encryption method)
5. Select an encryption algorithm
6. Assign a Wi-Fi password (no less than 8 characters)
7. Select a wireless network for internet access
8. Select the MAC address of the access point or leave it to 'Auto' if not sure
9. Input the password of the Wi-Fi

*Click **Scan WIFI** to refresh the Wi-Fi list if the target SSID is not identified.*

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

Status of the connectivity is as follows when the settings take effect.



Wifi Client Setting

Select SSID: 62% ; vantron_test8_5G

Mac/Bssid: Auto

Key: 12345678

Scan WIFI — Connected: 0h 0m 57s
IPaddr: 192.168.28.108

Associated Stations

| Network | MAC-Address | Host | Signal / Noise |
|---|---|---|---|
| Client "vantron_test8_5G" (wlan0) | 68:77:24:38:4C:A8 | ? | -67 / -92 dBm |
| Master "Vantron-747B3E" (wlan1) | CE:76:F9:F2:E7:E8 | ? | -37 / -92 dBm |

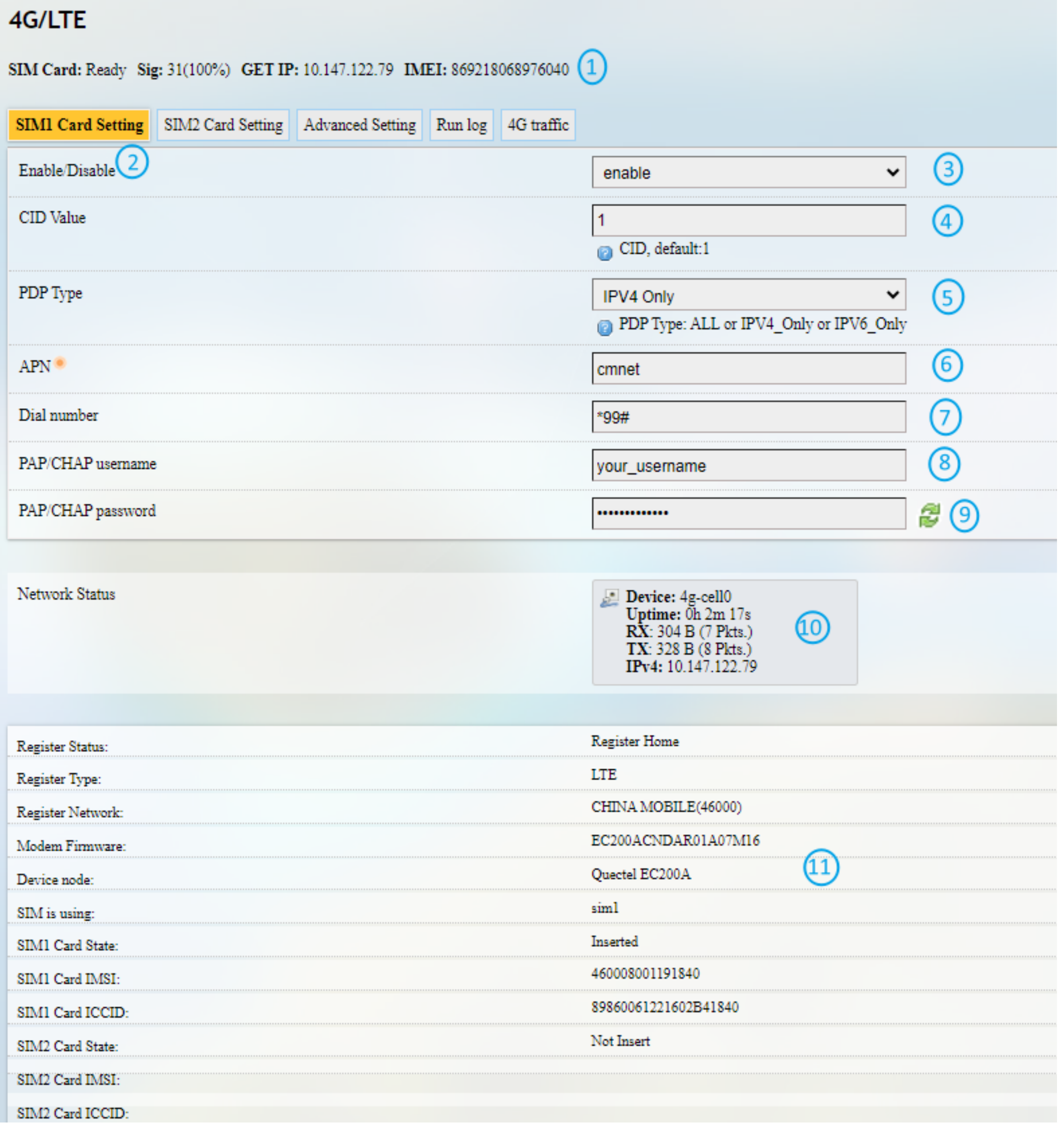
### 3.6.3 4G/LTE

Before you configure for 4G/LTE, be sure to install the activated SIM card and the LET antennas following the steps set out in 2.1.

Confirm with your sales executive whether the 4G module is AT&T or 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**.

After installation, the 4G signal indicators on the Router will light up to indicate the signal strength. Navigate to **Network > 4G/LTE** for more settings.



4G/LTE

**SIM Card:** Ready **Sig:** 31(100%) **GET IP:** 10.147.122.79 **IMEI:** 869218068976040

| | |
|---|---|
| Enable/Disable | enable |
| CID Value | 1<br>CID, default:1 |
| PDP Type | IPV4 Only<br>PDP Type: ALL or IPV4_Only or IPV6_Only |
| APN * | cmnet |
| Dial number | *99# |
| PAP/CHAP username | your_username |
| PAP/CHAP password | ••••••••••••• |
| Network Status | **Device:** 4g-cell0<br>**Uptime:** 0h 2m 17s<br>**RX:** 304 B (7 Pkts.)<br>**TX:** 328 B (8 Pkts.)<br>**IPv4:** 10.147.122.79 |

| | |
|---|---|
| Register Status: | Register Home |
| Register Type: | LTE |
| Register Network: | CHINA MOBILE(46000) |
| Modem Firmware: | EC200ACNDAR01A07M16 |
| Device node: | Quectel EC200A |
| SIM is using: | sim1 |
| SIM1 Card State: | Inserted |
| SIM1 Card IMSI: | 460008001191840 |
| SIM1 Card ICCID: | 89860061221602B41840 |
| SIM2 Card State: | Not Insert |
| SIM2 Card IMSI: | |
| SIM2 Card ICCID: | |

Description of the numbered areas

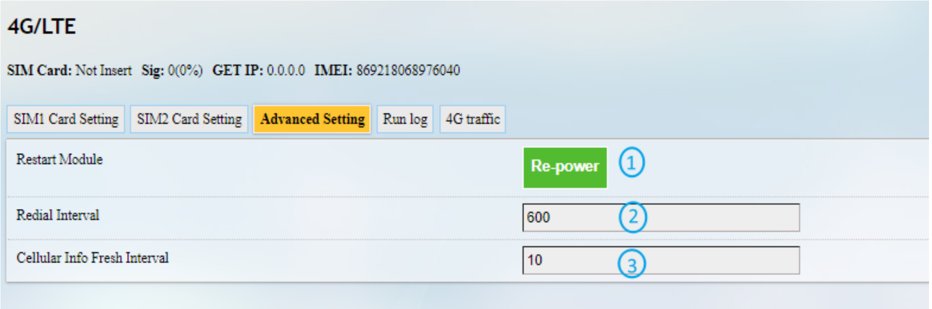
1. Connection status information (including SIM card status, signal strength, IP, and IMEI)
2. Set up SIM card 1/2
3. Enable/Disable the SIM card
4. Input the CID value
5. Select a PDP type
6. Input the APN provided by the carrier
7. Input ***99***1#** for SIM cards from AT&T and ***99***3#** for SIM cards from Verizon
8. Enter the username provided by the carrier for PAP/CHAP authentication
9. Enter the password provided by the carrier for PAP/CHAP authentication
10. Current network interface status
11. Detailed information of the SIM cards

*Leave the field as is if not applicable or if you are not sure.*

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

*If you have inserted a SIM card into SIM slot 2, you can click the **SIM2 Card Setting** tab for more settings.*

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



4G/LTE

**SIM Card:** Not Insert **Sig:** 0(0%) **GET IP:** 0.0.0.0 **IMEI:** 869218068976040

Restart Module

Redial Interval: 600

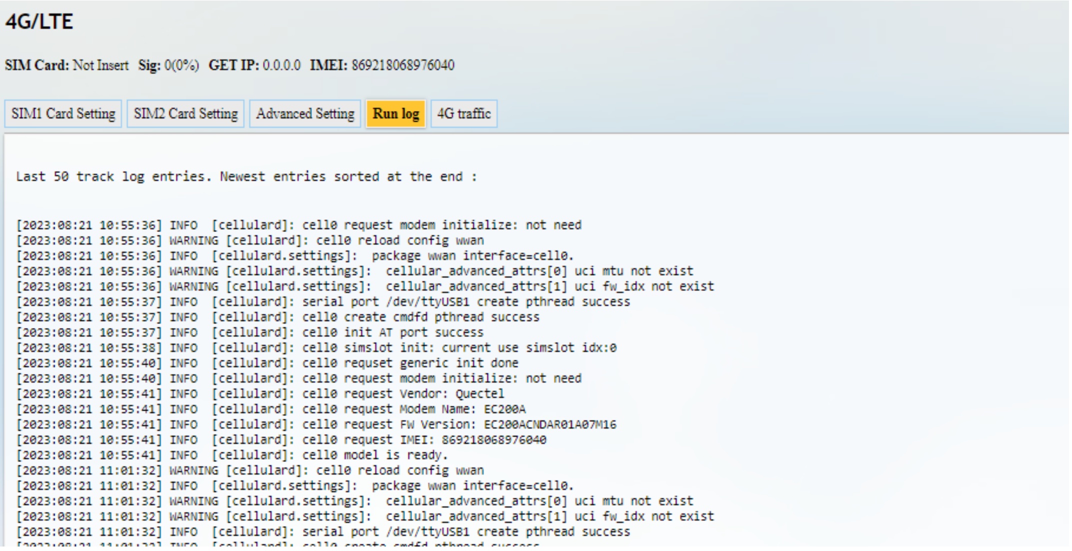
Cellular Info Fresh Interval: 10

Description of the numbered areas

1. Click to restart the 4G module
2. Time interval for automatic restart of the 4G module when it is offline
3. Time interval for auto refresh of the cellular information

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

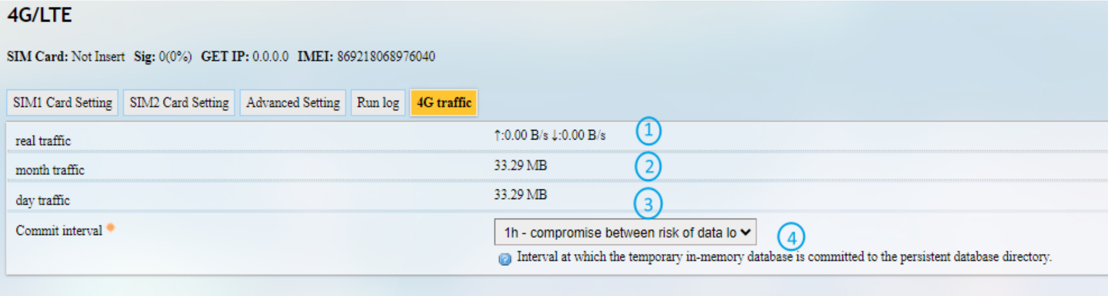
The **Run Log** tab next to the **Advanced Setting** tab displays the last 50 log entries of the module.



**SIM Card:** Not Insert **Sig:** 0(0%) **GET IP:** 0.0.0.0 **IMEI:** 869218068976040

```
Last 50 track log entries. Newest entries sorted at the end :


[2023:08:21 10:55:36] INFO  [cellulard]: cell0 request modem initialize: not need
[2023:08:21 10:55:36] WARNING [cellulard]: cell0 reload config wwan
[2023:08:21 10:55:36] INFO  [cellulard.settings]:  package wwan interface=cell0.
[2023:08:21 10:55:36] WARNING [cellulard.settings]:  cellular_advanced_attrs[0] uci mtu not exist
[2023:08:21 10:55:36] WARNING [cellulard.settings]:  cellular_advanced_attrs[1] uci fw_idx not exist
[2023:08:21 10:55:37] INFO  [cellulard]: serial port /dev/ttyUSB1 create pthread success
[2023:08:21 10:55:37] INFO  [cellulard]: cell0 create cmdfd pthread success
[2023:08:21 10:55:37] INFO  [cellulard]: cell0 init AT port success
[2023:08:21 10:55:38] INFO  [cellulard]: cell0 simslot init: current use simslot idx:0
[2023:08:21 10:55:40] INFO  [cellulard]: cell0 requset generic init done
[2023:08:21 10:55:40] INFO  [cellulard]: cell0 request modem initialize: not need
[2023:08:21 10:55:41] INFO  [cellulard]: cell0 request Vendor: Quectel
[2023:08:21 10:55:41] INFO  [cellulard]: cell0 request Modem Name: EC200A
[2023:08:21 10:55:41] INFO  [cellulard]: cell0 request FW Version: EC200ACNDAR01A07M16
[2023:08:21 10:55:41] INFO  [cellulard]: cell0 request IMEI: 869218068976040
[2023:08:21 10:55:41] INFO  [cellulard]: cell0 model is ready.
[2023:08:21 11:01:32] WARNING [cellulard]: cell0 reload config wwan
[2023:08:21 11:01:32] INFO  [cellulard.settings]:  package wwan interface=cell0.
[2023:08:21 11:01:32] WARNING [cellulard.settings]:  cellular_advanced_attrs[0] uci mtu not exist
[2023:08:21 11:01:32] WARNING [cellulard.settings]:  cellular_advanced_attrs[1] uci fw_idx not exist
[2023:08:21 11:01:32] INFO  [cellulard]: serial port /dev/ttyUSB1 create pthread success
[2023:08:21 11:01:32] INFO  [cellulard]: cell0 create cmdfd pthread success
```

Under the **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.



**SIM Card:** Not Insert **Sig:** 0(0%) **GET IP:** 0.0.0.0 **IMEI:** 869218068976040

| | |
|---|---|
| real traffic | ↑:0.00 B/s ↓:0.00 B/s |
| month traffic | 33.29 MB |
| day traffic | 33.29 MB |
| Commit interval * | 1h - compromise between risk of data lo<br>Interval at which the temporary in-memory database is committed to the persistent database directory. |

Description of the numbered areas

1. Real-time traffic
2. Data used in the current month
3. Data used in the day
4. Time interval for submitting the temporary database to the persistent database

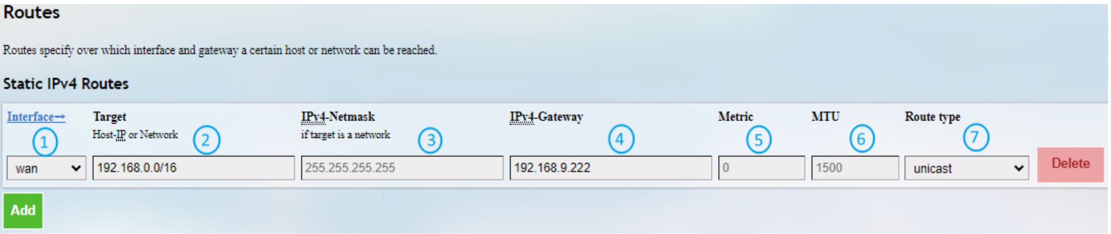
### 3.6.4 Static Routes

This is an advanced function allowing you to specify interface rules for route access.

Example:

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

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



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

| Interface | Target<br>Host-IP or Network | IPv4-Netmask<br>if target is a network | IPv4-Gateway | Metric | MTU | Route type |
|---|---|---|---|---|---|---|
| wan | 192.168.0.0/16 | 255.255.255.255 | 192.168.9.222 | 0 | 1500 | unicast |

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. |
| 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

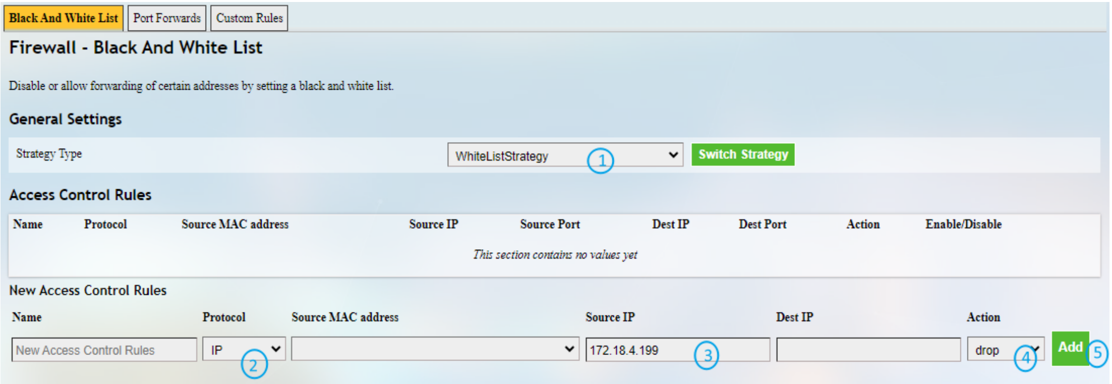
- **Black List and White List**

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



Firewall - Black And White List

Disable or allow forwarding of certain addresses by setting a black and white list.

General Settings

Strategy Type: WhiteListStrategy

Access Control Rules

| Name | Protocol | Source MAC address | Source IP | Source Port | Dest IP | Dest Port | Action | Enable/Disable |
|---|---|---|---|---|---|---|---|---|
| This section contains no values yet | | | | | | | | |

New Access Control Rules

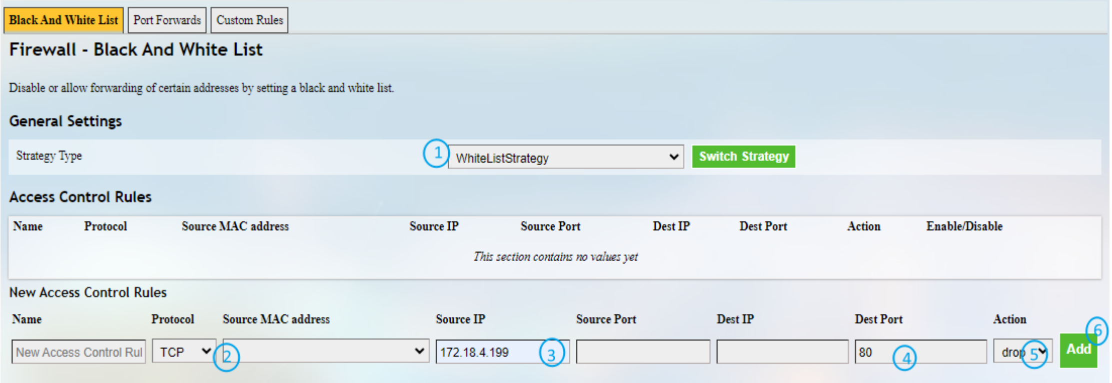
| Name | Protocol | Source MAC address | Source IP | Dest IP | Action |
|---|---|---|---|---|---|
| New Access Control Rules | IP | | 172.18.4.199 | | drop |

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



Firewall - Black And White List

Disable or allow forwarding of certain addresses by setting a black and white list.

General Settings

Strategy Type: WhiteListStrategy

Access Control Rules

| Name | Protocol | Source MAC address | Source IP | Source Port | Dest IP | Dest Port | Action | Enable/Disable |
|---|---|---|---|---|---|---|---|---|

*This section contains no values yet*

New Access Control Rules

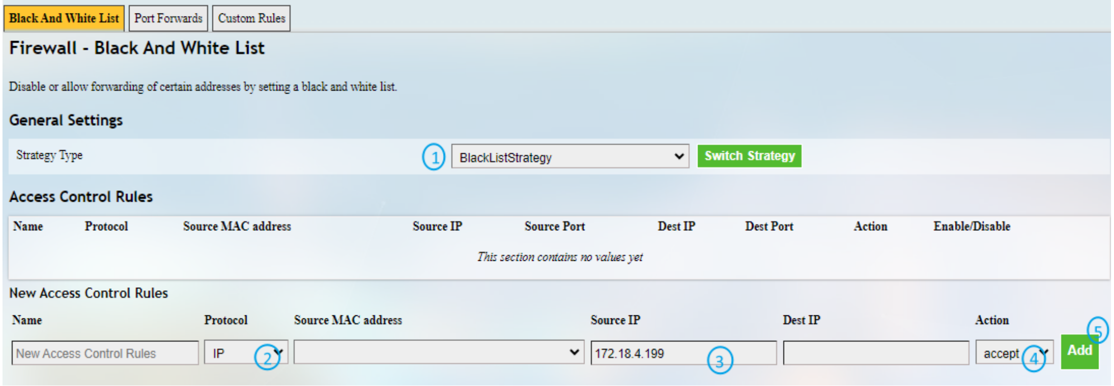
| Name | Protocol | Source MAC address | Source IP | Source Port | Dest IP | Dest Port | Action |
|---|---|---|---|---|---|---|---|
| New Access Control Rul | TCP | | 172.18.4.199 | | | 80 | drop |

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



Firewall - Black And White List

Disable or allow forwarding of certain addresses by setting a black and white list.

General Settings

Strategy Type: BlackListStrategy

Access Control Rules

| Name | Protocol | Source MAC address | Source IP | Source Port | Dest IP | Dest Port | Action | Enable/Disable |
|---|---|---|---|---|---|---|---|---|

*This section contains no values yet*

New Access Control Rules

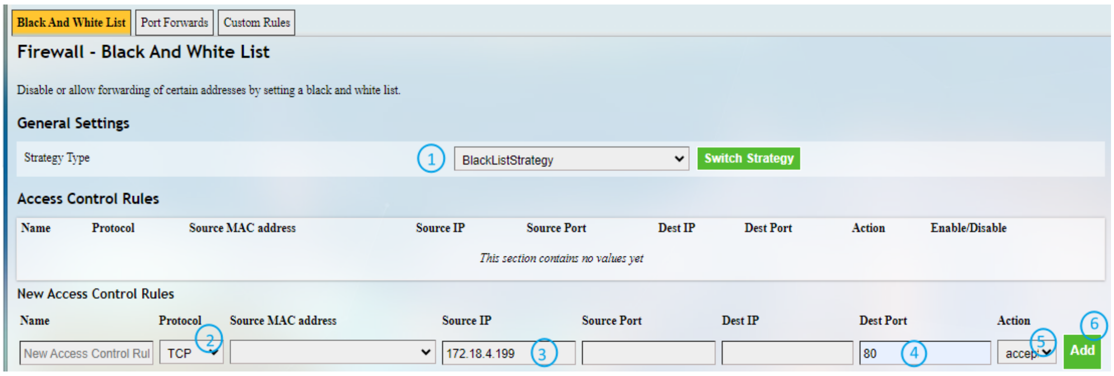
| Name | Protocol | Source MAC address | Source IP | Dest IP | Action |
|---|---|---|---|---|---|
| New Access Control Rules | IP | | 172.18.4.199 | | accept |

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



Firewall - Black And White List

Disable or allow forwarding of certain addresses by setting a black and white list.

General Settings

Strategy Type: BlackListStrategy — Switch Strategy

Access Control Rules

| Name | Protocol | Source MAC address | Source IP | Source Port | Dest IP | Dest Port | Action | Enable/Disable |
|---|---|---|---|---|---|---|---|---|

*This section contains no values yet*

New Access Control Rules

| Name | Protocol | Source MAC address | Source IP | Source Port | Dest IP | Dest Port | Action | |
|---|---|---|---|---|---|---|---|---|
| New Access Control Rul | TCP | | 172.18.4.199 | | | 80 | accept | Add |

Description of the numbered areas

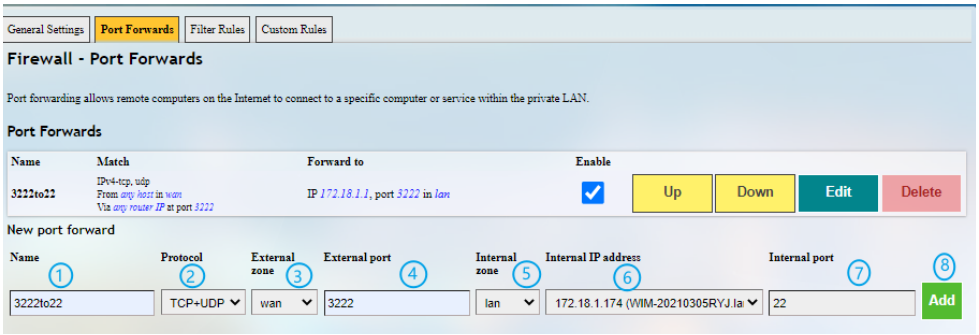
1. Select the black list strategy and click the button behind to switch to the strategy
2. Select the TCP protocol
3. Input the source IP
4. Input the destination port
5. Select ‘accept’ as the action for the target IP and port
6. Click **Add** to release the IP and port from the access control list

*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):



Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

| Name | Match | Forward to | Enable |
|---|---|---|---|
| 3222to22 | IPv4-tcp, udp<br>From any host in wan<br>Via any router IP at port 3222 | IP 172.18.1.1, port 3222 in lan | ☑ |

New port forward

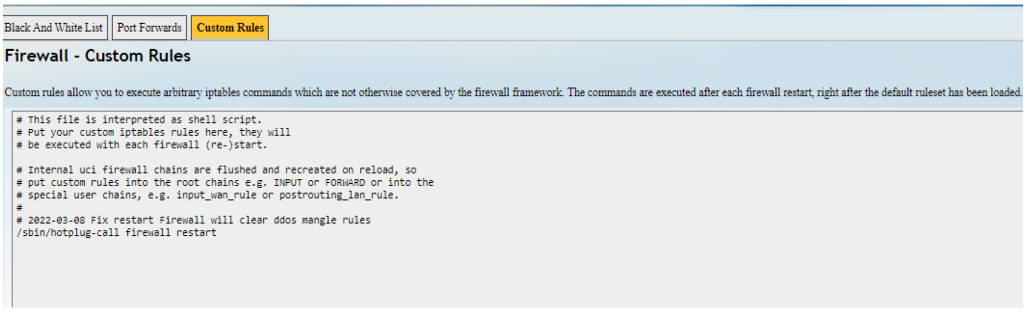
| Name | Protocol | External zone | External port | Internal zone | Internal IP address | Internal port |
|---|---|---|---|---|---|---|
| 3222to22 | TCP+UDP | wan | 3222 | lan | 172.18.1.174 (WIM-20210305RYJ.la | 22 |

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.



Firewall - 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 ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
#
# 2022-03-08 Fix restart Firewall will clear ddos mangle rules
/sbin/hotplug-call firewall restart
```

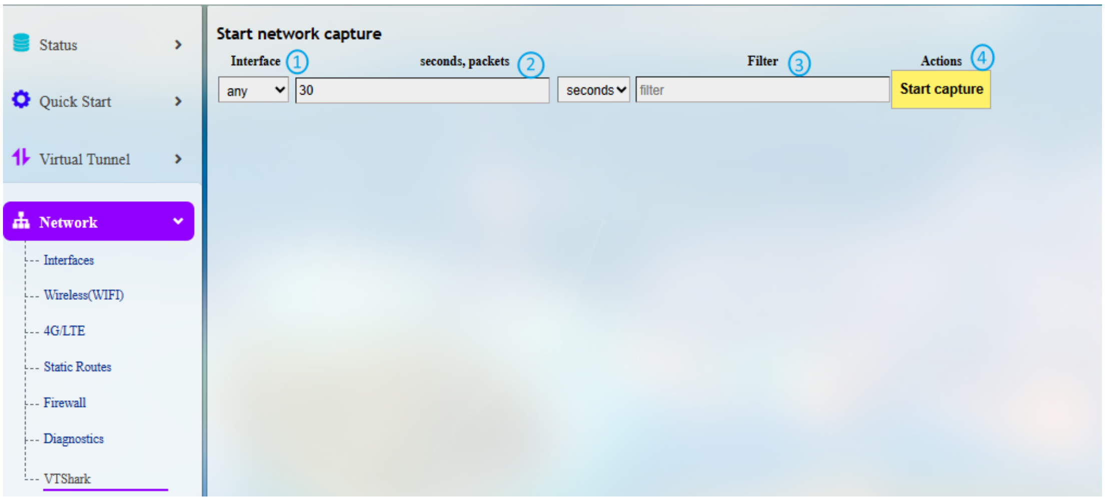
## 3.7 Diagnostics

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.



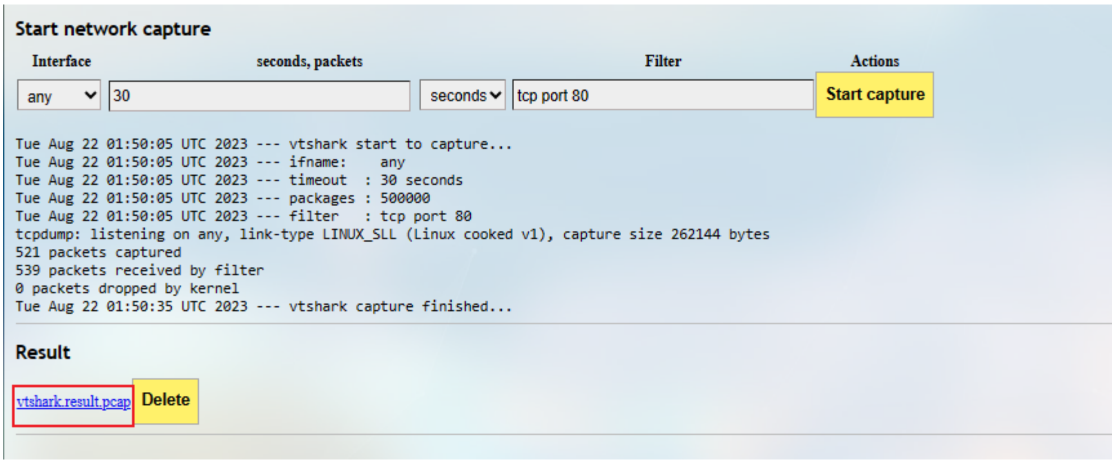
Description of the numbered areas

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.<br>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.<br>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.



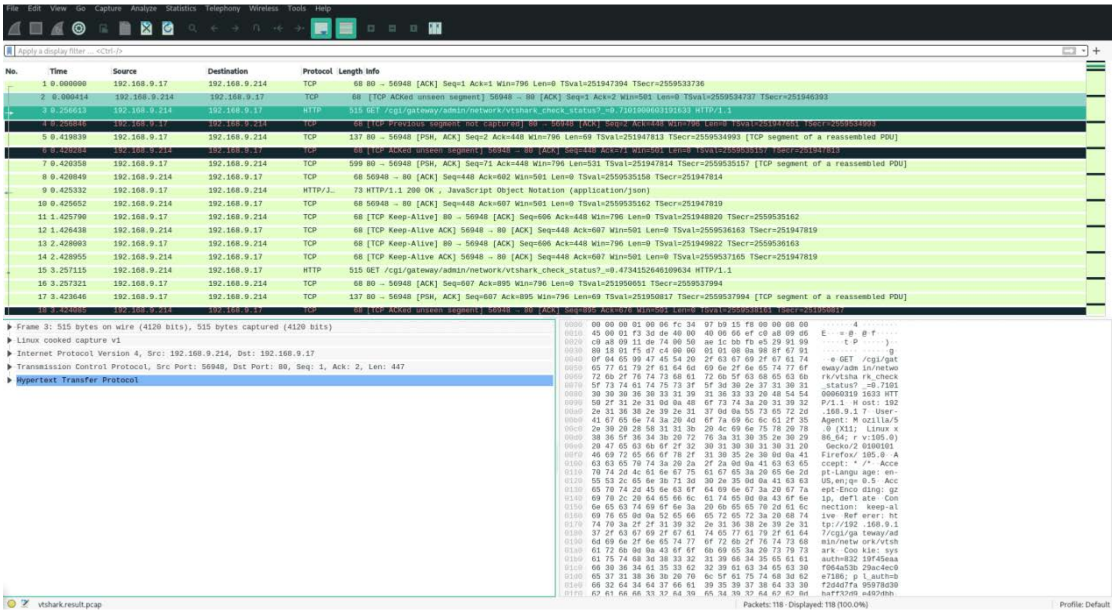
**Start network capture**

| Interface | seconds, packets | | Filter | Actions |
|---|---|---|---|---|
| any | 30 | seconds | tcp port 80 | Start capture |

```
Tue Aug 22 01:50:05 UTC 2023 --- vtshark start to capture...
Tue Aug 22 01:50:05 UTC 2023 --- ifname:    any
Tue Aug 22 01:50:05 UTC 2023 --- timeout  : 30 seconds
Tue Aug 22 01:50:05 UTC 2023 --- packages : 500000
Tue Aug 22 01:50:05 UTC 2023 --- filter   : tcp port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
521 packets captured
539 packets received by filter
0 packets dropped by kernel
Tue Aug 22 01:50:35 UTC 2023 --- vtshark capture finished...
```

**Result**

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



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source          Destination     Protocol  Length Info
   1 0.000000   192.168.9.17    192.168.9.214   TCP        68 80 → 56948 [ACK] Seq=1 Ack=1 Win=796 Len=0 TSval=251947394 TSecr=2559533736
   2 0.000414   192.168.9.214   192.168.9.17    TCP        68 [TCP ACKed unseen segment] 56948 → 80 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=2559534737 TSecr=251946393
   3 0.256613   192.168.9.214   192.168.9.17    HTTP      515 GET /cgi/gateway/admin/network/vtshark_check_status?_=0.7101000603191633 HTTP/1.1
   4 0.256846   192.168.9.17    192.168.9.214   TCP        68 [TCP Previous segment not captured] 80 → 56948 [ACK] Seq=2 Ack=448 Win=796 Len=0 TSval=251947651 TSecr=2559534993
   5 0.419839   192.168.9.17    192.168.9.214   TCP       137 80 → 56948 [PSH, ACK] Seq=2 Ack=448 Win=796 Len=69 TSval=251947813 TSecr=2559534993 [TCP segment of a reassembled PDU]
   6 0.420284   192.168.9.214   192.168.9.17    TCP        68 [TCP ACKed unseen segment] 56948 → 80 [ACK] Seq=448 Ack=71 Win=501 Len=0 TSval=2559535157 TSecr=251947813
   7 0.420358   192.168.9.17    192.168.9.214   TCP       599 80 → 56948 [PSH, ACK] Seq=71 Ack=448 Win=796 Len=531 TSval=251947814 TSecr=2559535157 [TCP segment of a reassembled PDU]
   8 0.420849   192.168.9.214   192.168.9.17    TCP        68 56948 → 80 [ACK] Seq=448 Ack=602 Win=501 Len=0 TSval=2559535158 TSecr=251947814
   9 0.425332   192.168.9.17    192.168.9.214   HTTP/J…    73 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  10 0.425652   192.168.9.214   192.168.9.17    TCP        68 56948 → 80 [ACK] Seq=448 Ack=607 Win=501 Len=0 TSval=2559535162 TSecr=251947819
  11 1.425790   192.168.9.17    192.168.9.214   TCP        68 [TCP Keep-Alive] 80 → 56948 [ACK] Seq=606 Ack=448 Win=796 Len=0 TSval=251948820 TSecr=2559535162
  12 1.426438   192.168.9.214   192.168.9.17    TCP        68 [TCP Keep-Alive ACK] 56948 → 80 [ACK] Seq=448 Ack=607 Win=501 Len=0 TSval=2559536163 TSecr=251947819
  13 2.428003   192.168.9.17    192.168.9.214   TCP        68 [TCP Keep-Alive] 80 → 56948 [ACK] Seq=606 Ack=448 Win=796 Len=0 TSval=251949822 TSecr=2559536163
  14 2.428955   192.168.9.214   192.168.9.17    TCP        68 [TCP Keep-Alive ACK] 56948 → 80 [ACK] Seq=448 Ack=607 Win=501 Len=0 TSval=2559537165 TSecr=251947819
  15 3.257115   192.168.9.214   192.168.9.17    HTTP      515 GET /cgi/gateway/admin/network/vtshark_check_status?_=0.4734152646109634 HTTP/1.1
  16 3.257321   192.168.9.17    192.168.9.214   TCP        68 80 → 56948 [ACK] Seq=607 Ack=895 Win=796 Len=0 TSval=251950651 TSecr=2559537994
  17 3.423646   192.168.9.17    192.168.9.214   TCP       137 80 → 56948 [PSH, ACK] Seq=607 Ack=895 Win=796 Len=69 TSval=251950817 TSecr=2559537994 [TCP segment of a reassembled PDU]
  18 3.424085   192.168.9.214   192.168.9.17    TCP        68 [TCP ACKed unseen segment] 56948 → 80 [ACK] Seq=895 Ack=676 Win=501 Len=0 TSval=2559538161 TSecr=251950817
```

```
▶ Frame 3: 515 bytes on wire (4120 bits), 515 bytes captured (4120 bits)
▶ Linux cooked capture v1
▶ Internet Protocol Version 4, Src: 192.168.9.214, Dst: 192.168.9.17
▶ Transmission Control Protocol, Src Port: 56948, Dst Port: 80, Seq: 1, Ack: 2, Len: 447
▶ Hypertext Transfer Protocol
```

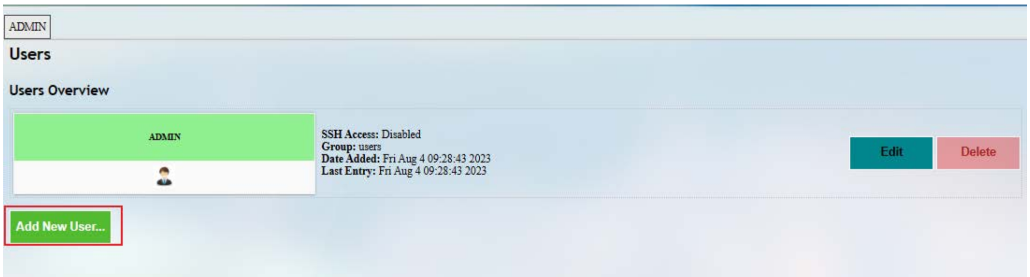
```
0000  00 00 00 01 00 06 fc 34  97 b9 15 f8 00 00 08 00   ·······4 ········
0010  45 00 01 f3 3d de 40 00  40 06 66 ef c0 a8 09 d6   E···=·@· @·f·····
0020  c0 a8 09 11 de 74 00 50  ae 1c bb fb e5 29 91 99   ·····t·P ·····)··
0030  80 18 01 f5 d7 c4 00 00  01 01 08 0a 98 8f 67 91   ········ ······g·
0040  0f 04 65 99 47 45 54 20  2f 63 67 69 2f 67 61 74   ··e·GET  /cgi/gat
0050  65 77 61 79 2f 61 64 6d  69 6e 2f 6e 65 74 77 6f   eway/adm in/netwo
0060  72 6b 2f 76 74 73 68 61  72 6b 5f 63 68 65 63 6b   rk/vtsha rk_check
0070  5f 73 74 61 74 75 73 3f  5f 3d 30 2e 37 31 30 31   _status? _=0.7101
0080  30 30 30 36 30 33 31 39  31 36 33 33 20 48 54 54   00060319 1633 HTT
0090  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 31 39 32   P/1.1··H ost: 192
00a0  2e 31 36 38 2e 39 2e 31  37 0d 0a 55 73 65 72 2d   .168.9.1 7··User-
00b0  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 35   Agent: M ozilla/5
00c0  2e 30 20 28 58 31 31 3b  20 4c 69 6e 75 78 20 78   .0 (X11;  Linux x
00d0  38 36 5f 36 34 3b 20 72  76 3a 31 30 35 2e 30 29   86_64; r v:105.0)
00e0  20 47 65 63 6b 6f 2f 32  30 31 30 30 31 30 31 20    Gecko/2 0100101 
00f0  46 69 72 65 66 6f 78 2f  31 30 35 2e 30 0d 0a 41   Firefox/ 105.0··A
0100  63 63 65 70 74 3a 20 2a  2f 2a 0d 0a 41 63 63 65   ccept: * /*··Acce
0110  70 74 2d 4c 61 6e 67 75  61 67 65 3a 20 65 6e 2d   pt-Langu age: en-
0120  55 53 2c 65 6e 3b 71 3d  30 2e 35 0d 0a 41 63 63   US,en;q= 0.5··Acc
0130  65 70 74 2d 45 6e 63 6f  64 69 6e 67 3a 20 67 7a   ept-Enco ding: gz
0140  69 70 2c 20 64 65 66 6c  61 74 65 0d 0a 43 6f 6e   ip, defl ate··Con
0150  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0160  69 76 65 0d 0a 52 65 66  65 72 65 72 3a 20 68 74   ive··Ref erer: ht
0170  74 70 3a 2f 2f 31 39 32  2e 31 36 38 2e 39 2e 31   tp://192 .168.9.1
0180  37 2f 63 67 69 2f 67 61  74 65 77 61 79 2f 61 64   7/cgi/ga teway/ad
0190  6d 69 6e 2f 6e 65 74 77  6f 72 6b 2f 76 74 73 68   min/netw ork/vtsh
01a0  61 72 6b 0d 0a 43 6f 6f  6b 69 65 3a 20 73 79 73   ark··Coo kie: sys
01b0  61 75 74 68 3d 38 33 32  31 39 66 34 35 65 61 61   auth=832 19f45eaa
01c0  66 30 36 34 61 35 33 62  32 39 61 63 34 65 63 30   f064a53b 29ac4ec0
01d0  65 37 31 38 36 3b 20 70  6c 5f 61 75 74 68 3d 62   e7186; p l_auth=b
01e0  66 32 64 34 64 37 66 61  39 35 39 37 38 64 33 30   f2d4d7fa 95978d30
01f0  62 61 66 66 33 32 64 39  65 34 39 32 64 62 62 0d   baff32d9 e492dbb·
```

## 3.9 User Management

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

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.



ADMIN

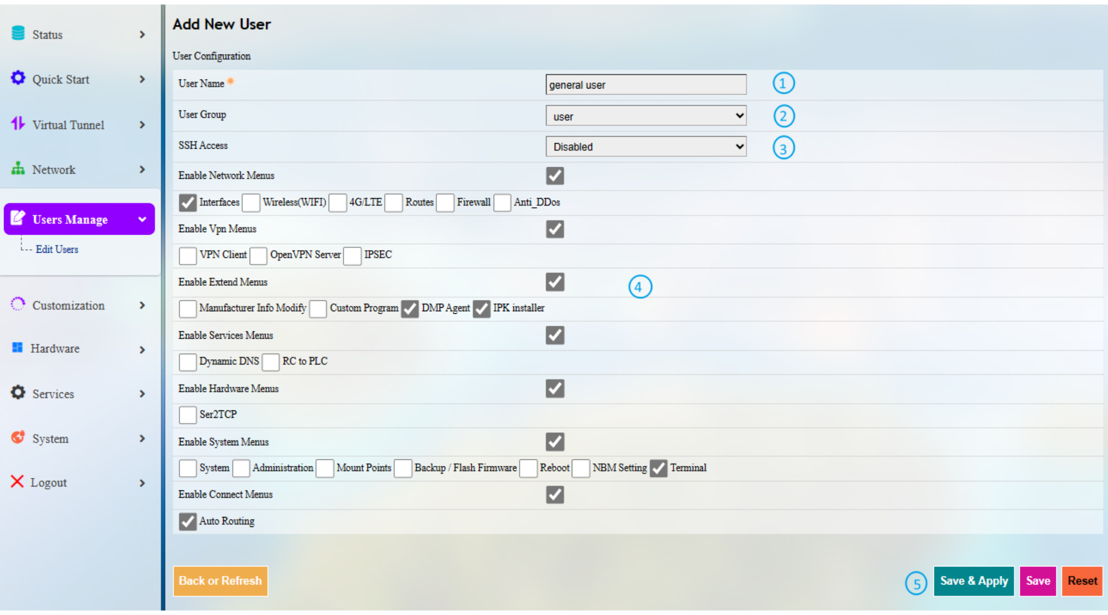
Users

Users Overview

ADMIN

**SSH Access:** Disabled
**Group:** users
**Date Added:** Fri Aug 4 09:28:43 2023
**Last Entry:** Fri Aug 4 09:28:43 2023

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



Add New User

User Configuration

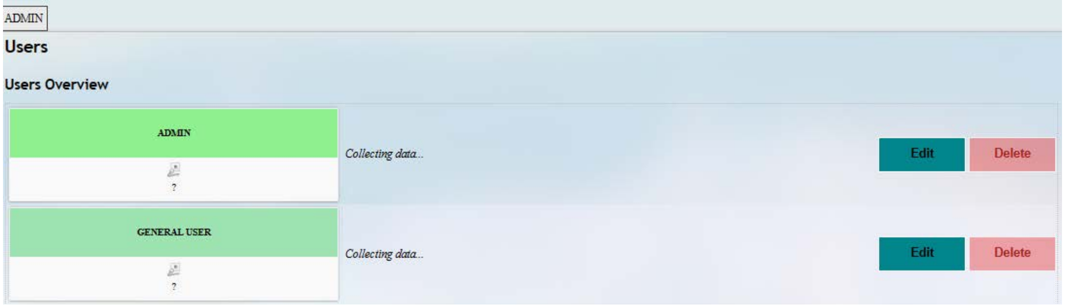
User Name * general user
User Group user
SSH Access Disabled

Enable Network Menus ☑
☑ Interfaces ☐ Wireless(WIFI) ☐ 4G/LTE ☐ Routes ☐ Firewall ☐ Anti_DDos
Enable Vpn Menus ☑
☐ VPN Client ☐ OpenVPN Server ☐ IPSEC
Enable Extend Menus ☑
☐ Manufacturer Info Modify ☐ Custom Program ☑ DMP Agent ☑ IPK installer
Enable Services Menus ☑
☐ Dynamic DNS ☐ RC to PLC
Enable Hardware Menus ☑
☐ Ser2TCP
Enable System Menus ☑
☐ System ☐ Administration ☐ Mount Points ☐ Backup / Flash Firmware ☐ Reboot ☐ NBM Setting ☑ Terminal
Enable Connect Menus ☑
☑ Auto Routing

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.

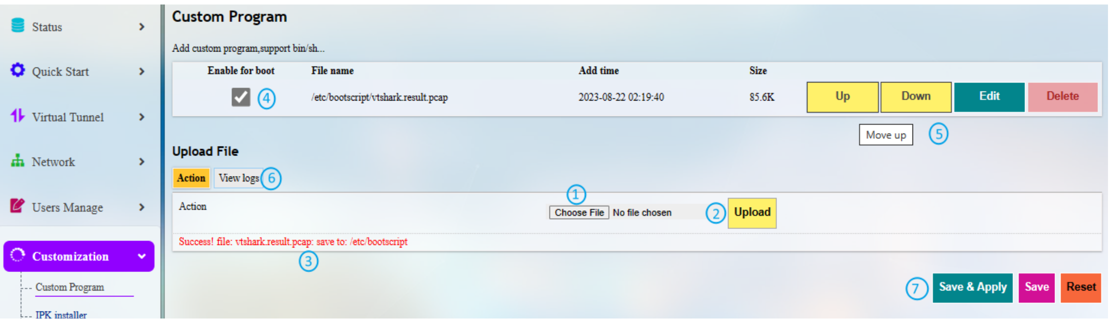


## 3.10 Customization

As certain features in 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 features.

### 3.10.1 Custom Program

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



Custom Program

Add custom program,support bin/sh...

| Enable for boot | File name | Add time | Size |
|---|---|---|---|
| ☑ | /etc/bootscript/vtshark.result.pcap | 2023-08-22 02:19:40 | 85.6K |

Upload File

Action

No file chosen

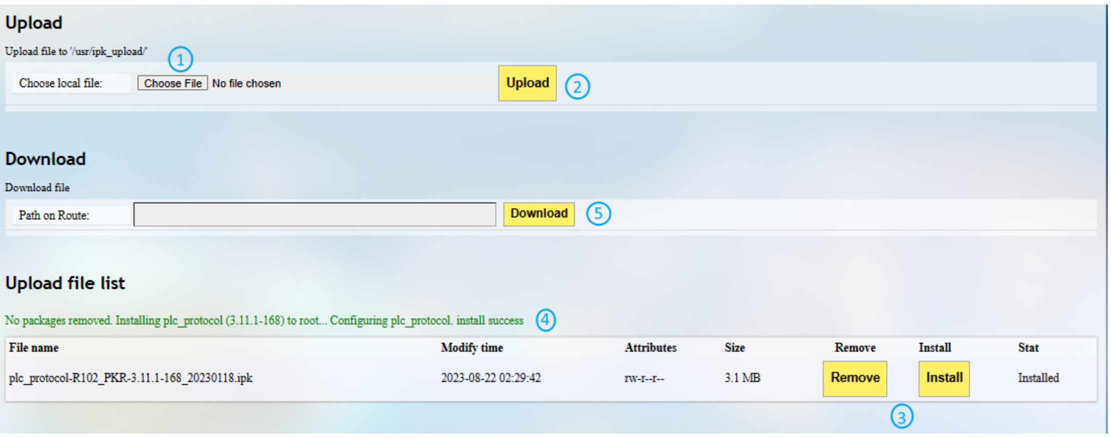
Success! file: vtshark.result.pcap: save to: /etc/bootscript

Description of the numbered areas

1. Select a script to upload
2. Upload the script to the Router
3. When the script is uploaded successfully, the file name and file directory will be displayed here
4. Enable the script, and it will run automatically next time when the router starts up
5. 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 scripts
6. Check the script log
7. **Save & Apply** the settings

## 3.10.2 IPK Installer

With IPK Installer, customers can install self-compiled IPK packages to the Router. Vantron industrial protocol packages are also uploaded from here.



Upload

Upload file to '/usr/ipk_upload/'

Choose local file: No file chosen

Download

Download file

Path on Route:

Upload file list

No packages removed. Installing plc_protocol (3.11.1-168) to root... Configuring plc_protocol. install success

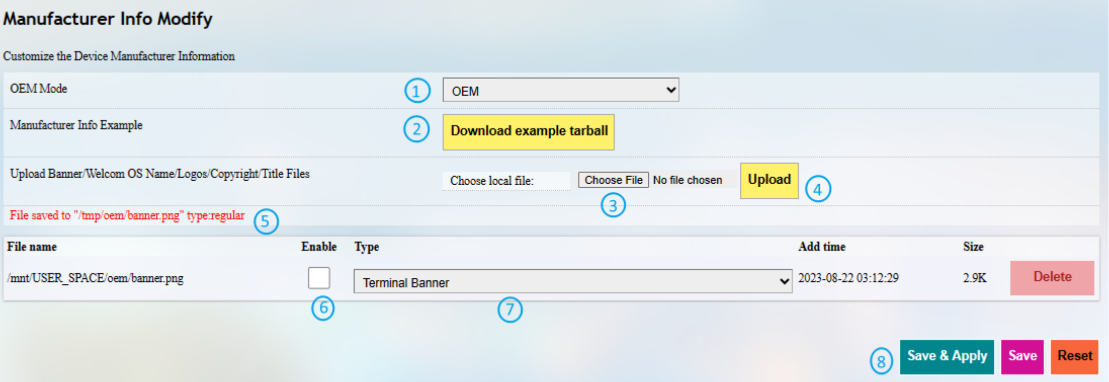
| File name | Modify time | Attributes | Size | Remove | Install | Stat |
|---|---|---|---|---|---|---|
| plc_protocol-R102_PKR-3.11.1-168_20230118.ipk | 2023-08-22 02:29:42 | rw-r--r-- | 3.1 MB | Remove | Install | Installed |

Description of the numbered areas

1. Select an .ipk file from the local directory
2. Click **Upload** to upload the file to the device
3. You can delete or install the file after the .ipk file is uploaded
4. Install the file and wait a moment, there will be a prompt for the installation status
5. You can also input a file path on the device to download the specific file

### 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 select **OEM** from the **OEM Mode** drop-down list.



Manufacturer Info Modify

Customize the Device Manufacturer Information

OEM Mode: OEM

Manufacturer Info Example

Upload Banner/Welcom OS Name/Logos/Copyright/Title Files

Choose local file: No file chosen

File saved to "/tmp/oem/banner.png" type:regular

| File name | Enable | Type | Add time | Size |  |
|---|---|---|---|---|---|
| /mnt/USER_SPACE/oem/banner.png | □ | Terminal Banner | 2023-08-22 03:12:29 | 2.9K | Delete |

Description of the numbered areas

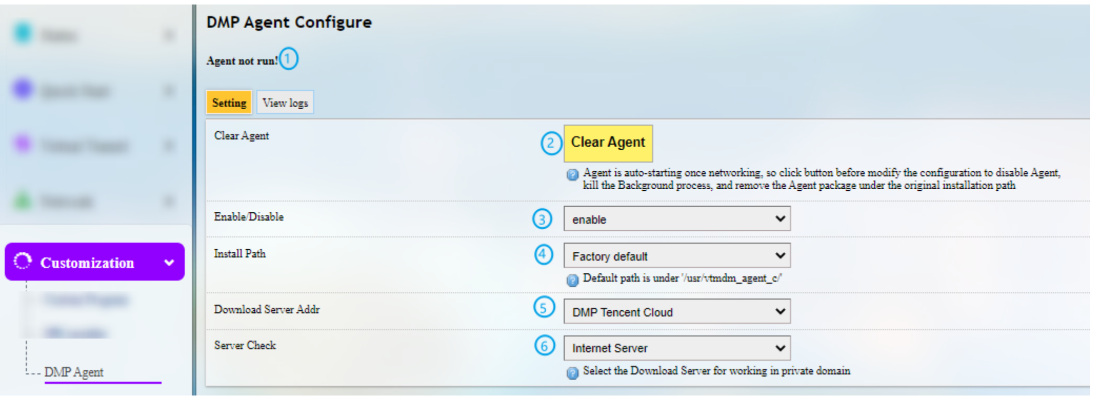
1. Select the **OEM** mode
2. Download the illustrative .tar file to the local directory and replace the files with your own as necessary
3. Select the target file from the local directory
4. Upload the file to the Router
5. The path of the file will be displayed here
6. Choose to enable the file or 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.



DMP Agent Configure

Agent not run! (1)

Clear Agent: (2) Clear Agent
Agent is auto-starting once networking, so click button before modify the configuration to disable Agent, kill the Background process, and remove the Agent package under the original installation path

Enable/Disable: (3) enable

Install Path: (4) Factory default
Default path is under '/usr/vtmdm_agent_c/'

Download Server Addr: (5) DMP Tencent Cloud

Server Check: (6) Internet Server
Select the Download Server for working in private domain

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.*

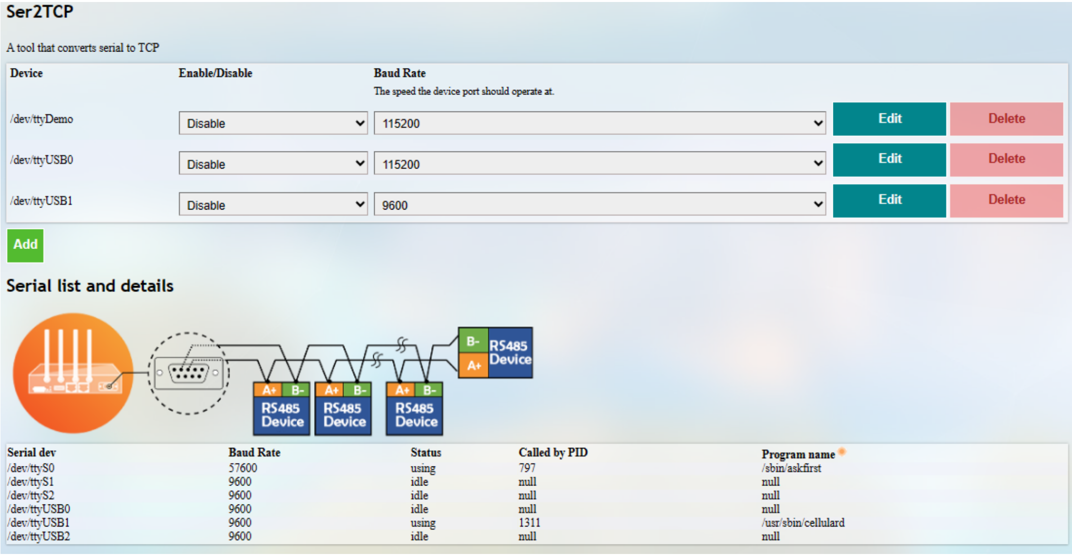
3. Enable/Disable the Agent
4. You can customize the installation path of the Agent here (default path: '/usr/vtmdm_agent_c/')
5. Set up the download address of the Agent server (better to keep the default setting)
6. Internet server for public domain and download server for private domain

*Factory reset of the Router 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.



Ser2TCP

A tool that converts serial to TCP

| Device | Enable/Disable | Baud Rate<br>The speed the device port should operate at. | | |
|---|---|---|---|---|
| /dev/ttyDemo | Disable | 115200 | Edit | Delete |
| /dev/ttyUSB0 | Disable | 115200 | Edit | Delete |
| /dev/ttyUSB1 | Disable | 9600 | Edit | Delete |

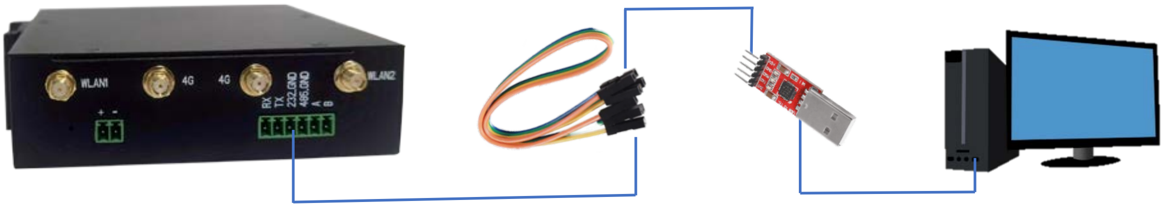
Add

Serial list and details

| Serial dev | Baud Rate | Status | Called by PID | Program name |
|---|---|---|---|---|
| /dev/ttyS0 | 57600 | using | 797 | /sbin/askfirst |
| /dev/ttyS1 | 9600 | idle | null | null |
| /dev/ttyS2 | 9600 | idle | null | null |
| /dev/ttyUSB0 | 9600 | idle | null | null |
| /dev/ttyUSB1 | 9600 | using | 1311 | /usr/sbin/cellulard |
| /dev/ttyUSB2 | 9600 | idle | null | null |

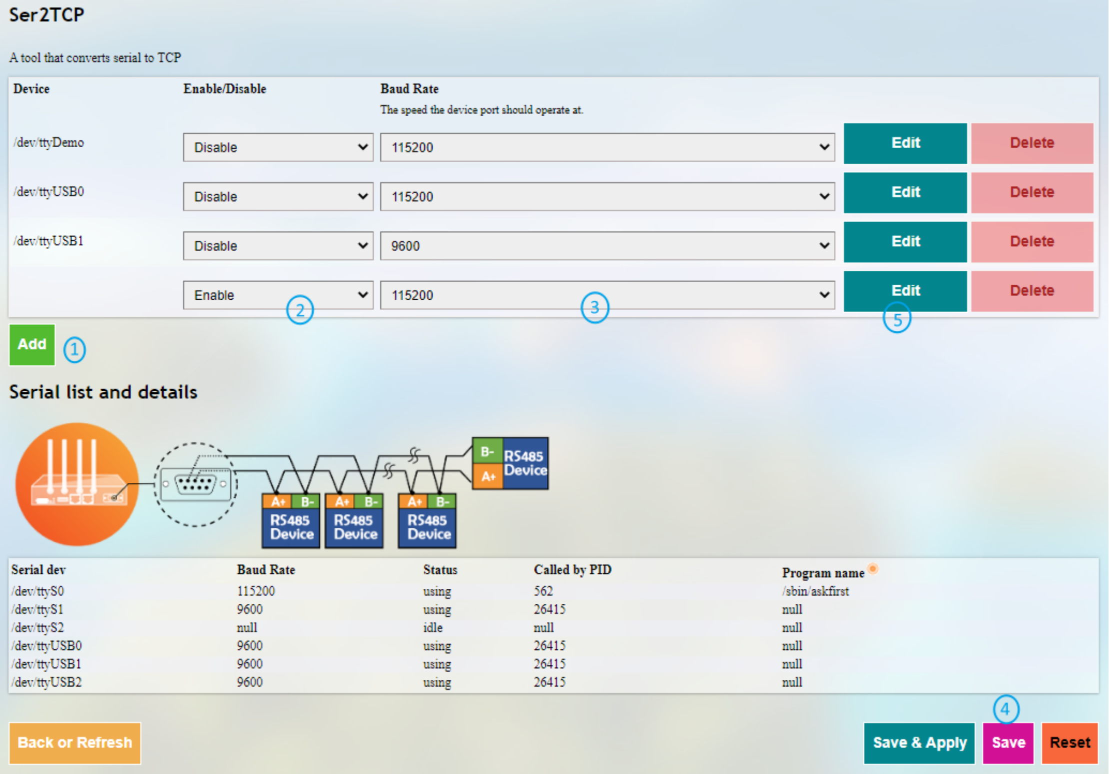
## 3.11.2 Ser2net Environment Setup and Verification

- Prerequisites
  - An R105 router
  - A Linux host computer (Ubuntu for demonstration here)
  - A USB to TTL serial adapter
  - A DuPont cable
  - Connect the serial port of the Router to the host computer as follows (refer to 1.5 for the connection, RS232 mode for demonstration here)



- Client mode

(1) Settings on VantronOS web interface



Ser2TCP

A tool that converts serial to TCP

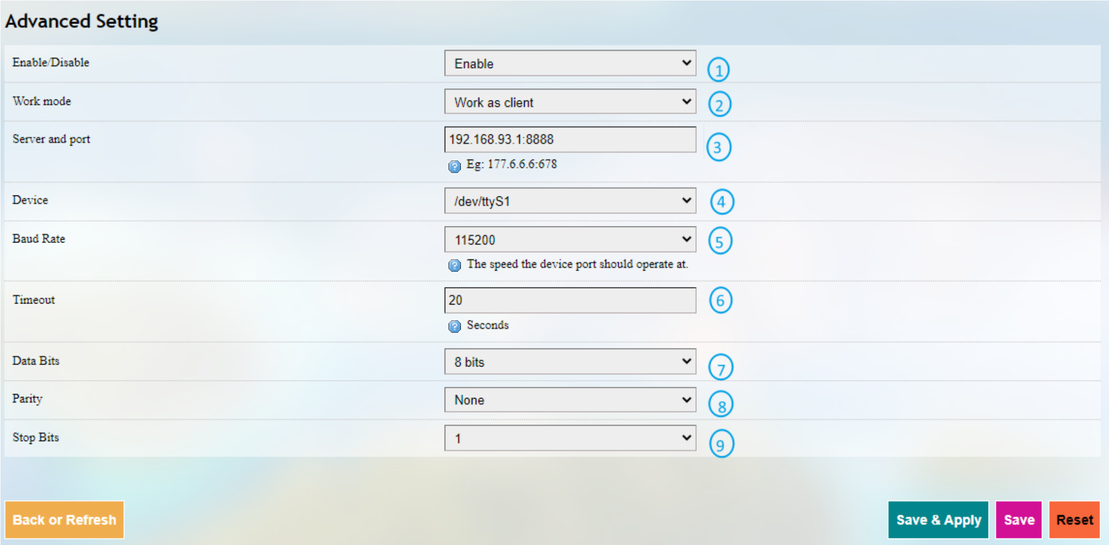
| Device | Enable/Disable | Baud Rate<br>The speed the device port should operate at. |
|---|---|---|
| /dev/ttyDemo | Disable | 115200 |
| /dev/ttyUSB0 | Disable | 115200 |
| /dev/ttyUSB1 | Disable | 9600 |
|  | Enable | 115200 |

Serial list and details

| Serial dev | Baud Rate | Status | Called by PID | Program name |
|---|---|---|---|---|
| /dev/ttyS0 | 115200 | using | 562 | /sbin/askfirst |
| /dev/ttyS1 | 9600 | using | 26415 | null |
| /dev/ttyS2 | null | idle | null | null |
| /dev/ttyUSB0 | 9600 | using | 26415 | null |
| /dev/ttyUSB1 | 9600 | using | 26415 | null |
| /dev/ttyUSB2 | 9600 | using | 26415 | null |

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 access the advanced settings page



Advanced Setting

| | |
|---|---|
| Enable/Disable | Enable |
| Work mode | Work as client |
| Server and port | 192.168.93.1:8888<br>Eg: 177.6.6.6:678 |
| Device | /dev/ttyS1 |
| Baud Rate | 115200<br>The speed the device port should operate at. |
| Timeout | 20<br>Seconds |
| Data Bits | 8 bits |
| Parity | None |
| Stop Bits | 1 |

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 RS232 port is /dev/ttyS1 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/ttyS1 -b 115200 -a 8 -r none -s 1 -o 20
```

(3) Settings on the Ubuntu host

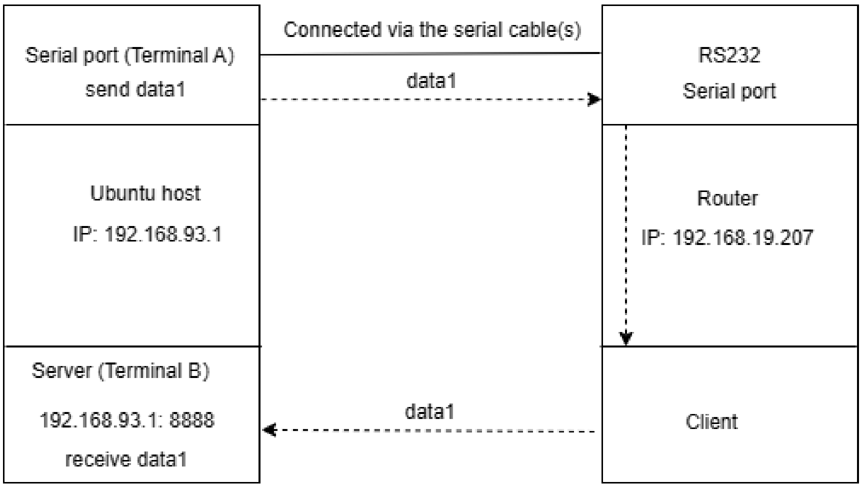
- Use microcom to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

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

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

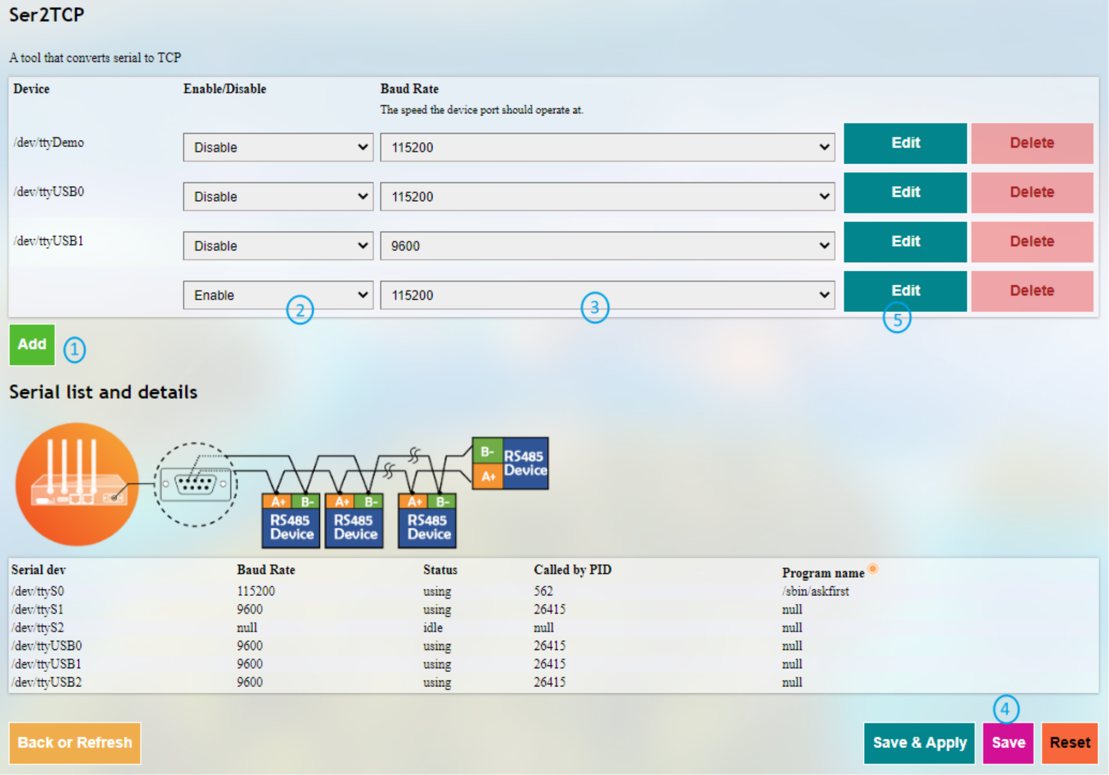
```
tcpudp_test tcp server:tcpudp_test -p 8888
```

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



- Server mode

(1) Settings on VantronOS web interface



Ser2TCP

A tool that converts serial to TCP

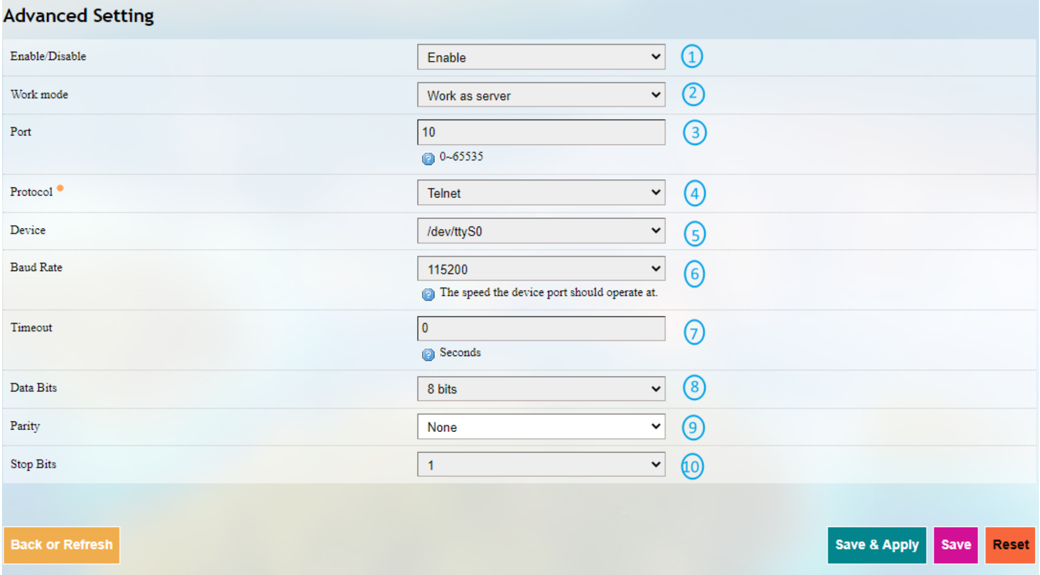
| Device | Enable/Disable | Baud Rate<br>The speed the device port should operate at. | | |
|---|---|---|---|---|
| /dev/ttyDemo | Disable | 115200 | Edit | Delete |
| /dev/ttyUSB0 | Disable | 115200 | Edit | Delete |
| /dev/ttyUSB1 | Disable | 9600 | Edit | Delete |
| | Enable | 115200 | Edit | Delete |

Serial list and details

| Serial dev | Baud Rate | Status | Called by PID | Program name |
|---|---|---|---|---|
| /dev/ttyS0 | 115200 | using | 562 | /sbin/askfirst |
| /dev/ttyS1 | 9600 | using | 26415 | null |
| /dev/ttyS2 | null | idle | null | null |
| /dev/ttyUSB0 | 9600 | using | 26415 | null |
| /dev/ttyUSB1 | 9600 | using | 26415 | null |
| /dev/ttyUSB2 | 9600 | using | 26415 | null |

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 access the advanced settings page



Advanced Setting

| | |
|---|---|
| Enable/Disable | Enable ① |
| Work mode | Work as server ② |
| Port | 10 ③<br>0~65535 |
| Protocol | Telnet ④ |
| Device | /dev/ttyS0 ⑤ |
| Baud Rate | 115200 ⑥<br>The speed the device port should operate at. |
| Timeout | 0 ⑦<br>Seconds |
| Data Bits | 8 bits ⑧ |
| Parity | None ⑨ |
| Stop Bits | 1 ⑩ |

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 RS232 port is /dev/ttyS1 as described in 1.5)
6. Select 115200 as the baud rate (the default value will be 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

*Be sure to save above settings before you exit.*

(2) The Ser2net process is running as follows:

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

(3) Settings on the Ubuntu host

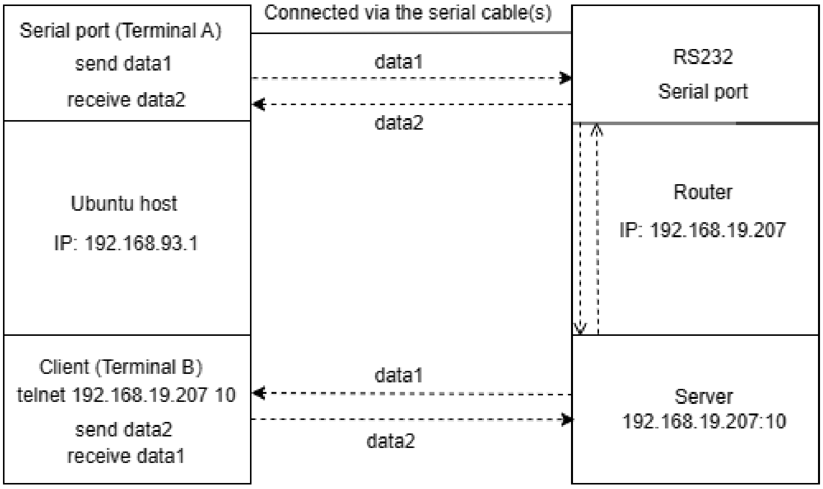
- Use microcom to access the serial port in terminal A (assume that the device name for the USB to TTL serial adapter is identified as /dev/ttyUSB1)

```
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.

# 3.12 Services

## 3.12.1 Dynamic DNS

Dynamic DNS is a technology in domain name system (DNS) that automatically updates the content of Name Server, often in real time, with the active DDNS configuration of its configured hostnames, addresses or other information.

Input a name of the subdomain or root domain and click **Add** button, and you will be directed to the setup page of the dynamic DNS. Then you can edit the service as needed.

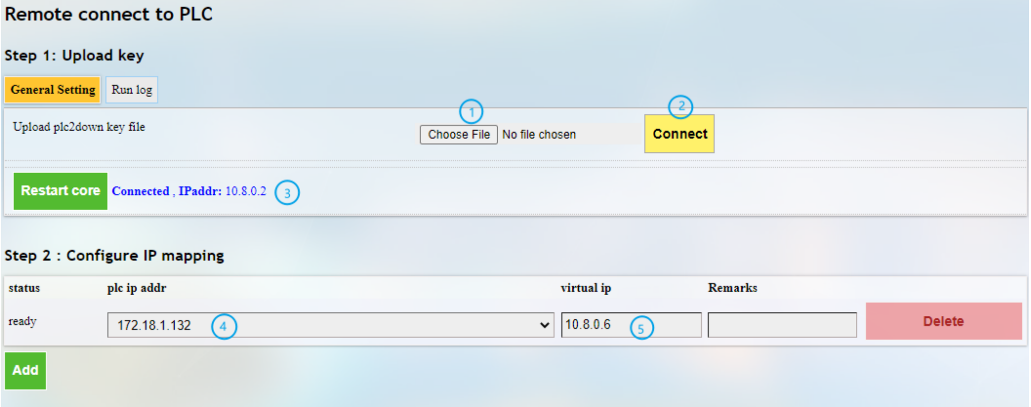
## 3.12.2 RC to PLC

For remote access and control of PLC devices via OpenVPN protocol, you will need two R105 routers and a Windows host computer ('Windows PC') that are on the same network. One router ('R1') is for building an OpenVPN server, and the other ('R2') is for connecting the OpenVPN server built by R1.

Prerequisites:

1. Prepare the R1, R2, Windows PC, and PLC device
2. Connect R1 and R2 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 R1 and download the .ovpn file
5. Connect the Windows PC to the OpenVPN server built by R1 via the OpenVPN client program
6. Connect R2 to the OpenVPN server built by R1 (see below)
7. Connect the PLC device to a LAN port of R2 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 R2 to R1 and configuring the PLC and R2. For other settings, please download the related software program and finish the setup.



Remote connect to PLC

Step 1: Upload key

Upload plc2down key file

Connected , IPaddr: 10.8.0.2

Step 2 : Configure IP mapping

| status | plc ip addr | virtual ip | Remarks |
|---|---|---|---|
| ready | 172.18.1.132 | 10.8.0.6 | |

Description of the numbered areas

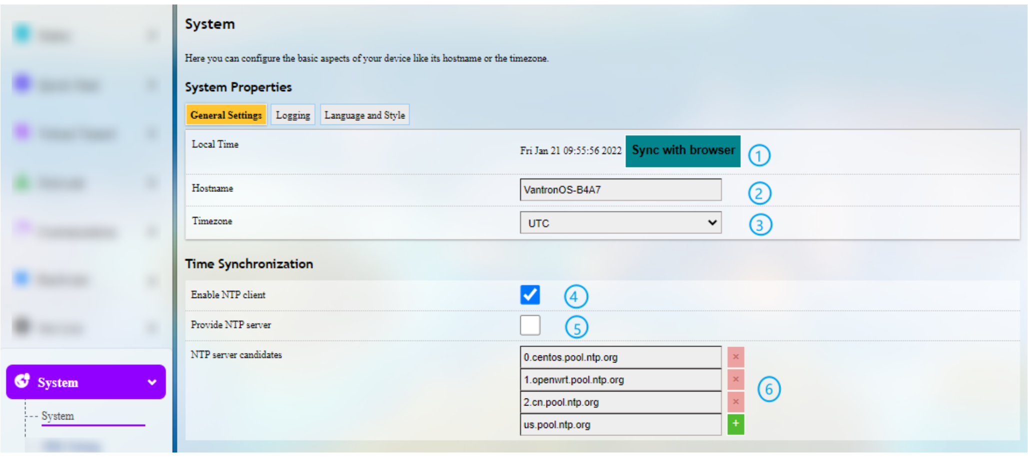
1. Download and save the .ovpn file after setting up the OpenVPN server on R1, then click this button to open the directory of the file
2. Click **Connect** to connect R2 to the OpenVPN server built by R1
3. After connection, an IP address assigned by the OpenVPN server will be displayed here
4. Input a static IP address for the PLC (on the same IP network as the LAN port of R2)
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.*

# 3.13 System

## 3.13.1 System

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



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings | Logging | Language and Style

Local Time: Fri Jan 21 09:55:56 2022 Sync with browser ①

Hostname: VantronOS-B4A7 ②

Timezone: UTC ③

Time Synchronization

Enable NTP client ☑ ④

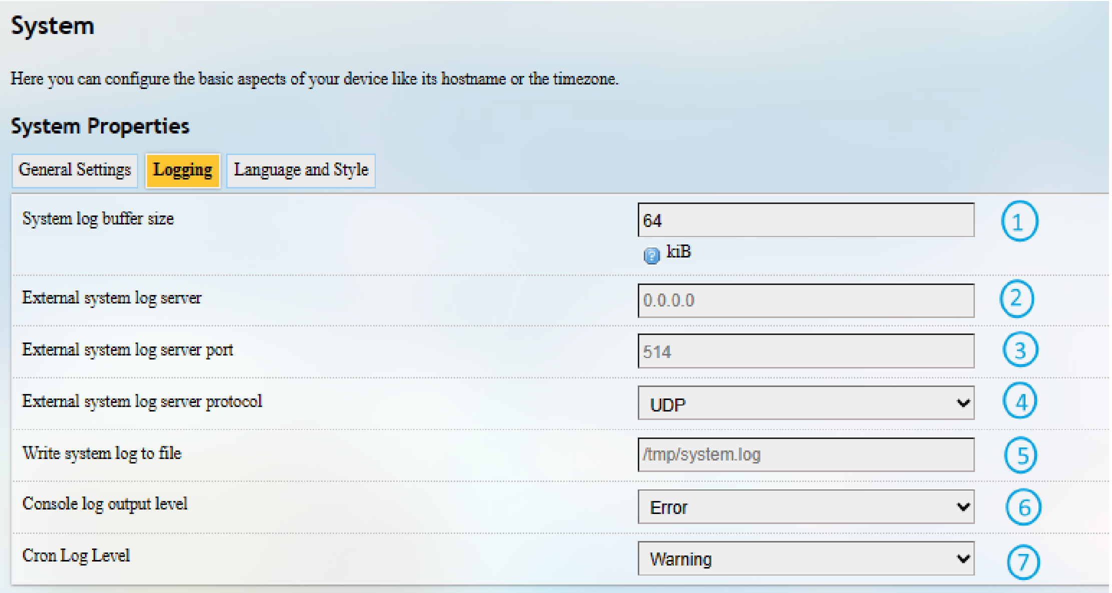
Provide NTP server □ ⑤

NTP server candidates: ⑥
0.centos.pool.ntp.org
1.openwrt.pool.ntp.org
2.cn.pool.ntp.org
us.pool.ntp.org

Description of the numbered areas

1. Synchronize the router time with the browser (local) time
2. Change the name of the host
3. Select a time zone
4. Enable NTP online time adjustment
5. Start the NTP server (the Router is used as the NTP server)
6. NTP online time server

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



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings | Logging | Language and Style

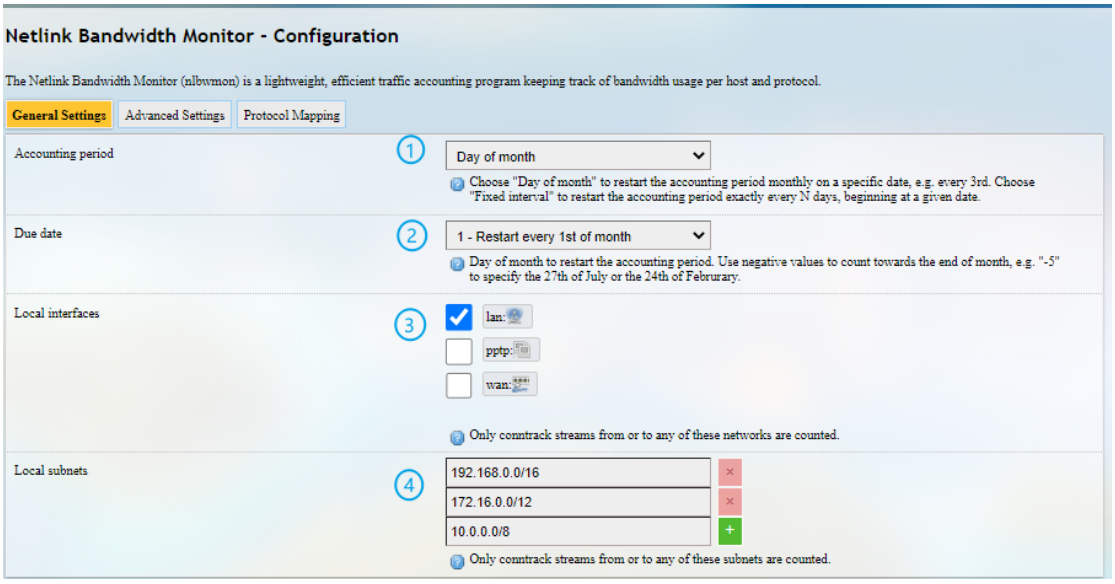
| | | |
|---|---|---|
| System log buffer size | 64<br>kiB | 1 |
| External system log server | 0.0.0.0 | 2 |
| External system log server port | 514 | 3 |
| External system log server protocol | UDP | 4 |
| Write system log to file | /tmp/system.log | 5 |
| Console log output level | Error | 6 |
| Cron Log Level | Warning | 7 |

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**



**Netlink Bandwidth Monitor - Configuration**

The Netlink Bandwidth Monitor (nlbwmon) is a lightweight, efficient traffic accounting program keeping track of bandwidth usage per host and protocol.

Accounting period: Day of month

Choose "Day of month" to restart the accounting period monthly on a specific date, e.g. every 3rd. Choose "Fixed interval" to restart the accounting period exactly every N days, beginning at a given date.

Due date: 1 - Restart every 1st of month

Day of month to restart the accounting period. Use negative values to count towards the end of month, e.g. "-5" to specify the 27th of July or the 24th of Februrary.

Local interfaces:
☑ lan:
□ pptp:
□ wan:

Only conntrack streams from or to any of these networks are counted.

Local subnets:
192.168.0.0/16
172.16.0.0/12
10.0.0.0/8

Only conntrack streams from or to any of these subnets are counted.

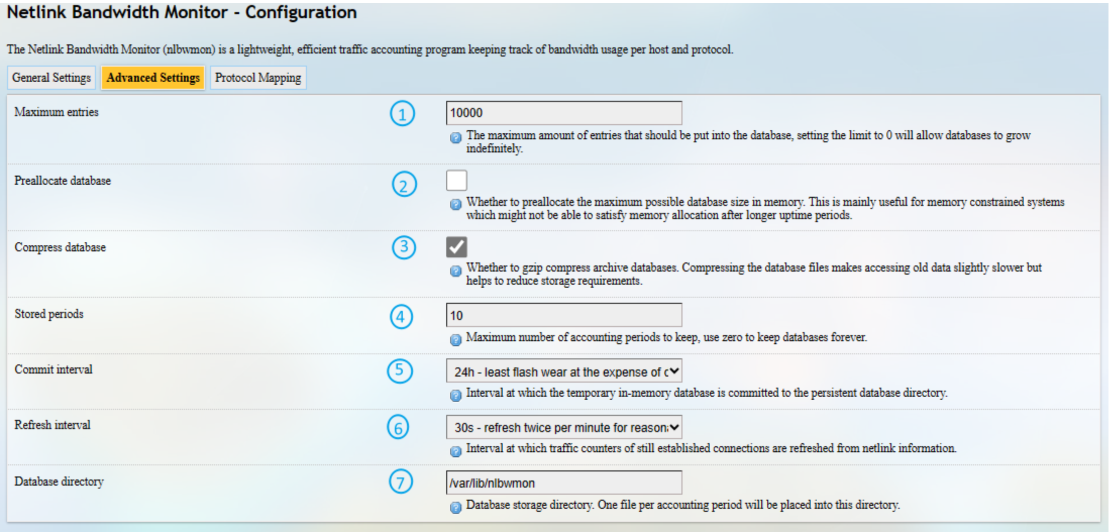
Description of the numbered areas

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.



Netlink Bandwidth Monitor - Configuration

The Netlink Bandwidth Monitor (nlbwmon) is a lightweight, efficient traffic accounting program keeping track of bandwidth usage per host and protocol.

General Settings | **Advanced Settings** | Protocol Mapping

Maximum entries: 10000
The maximum amount of entries that should be put into the database, setting the limit to 0 will allow databases to grow indefinitely.

Preallocate database: □
Whether to preallocate the maximum possible database size in memory. This is mainly useful for memory constrained systems which might not be able to satisfy memory allocation after longer uptime periods.

Compress database: ☑
Whether to gzip compress archive databases. Compressing the database files makes accessing old data slightly slower but helps to reduce storage requirements.

Stored periods: 10
Maximum number of accounting periods to keep, use zero to keep databases forever.

Commit interval: 24h - least flash wear at the expense of c
Interval at which the temporary in-memory database is committed to the persistent database directory.

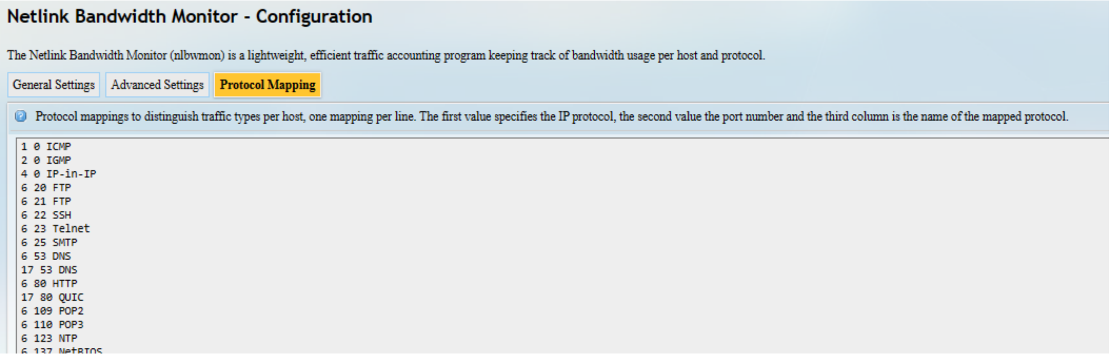
Refresh interval: 30s - refresh twice per minute for reason
Interval at which traffic counters of still established connections are refreshed from netlink information.

Database directory: /var/lib/nlbwmon
Database storage directory. One file per accounting period will be placed into this directory.

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.



Netlink Bandwidth Monitor - Configuration

The Netlink Bandwidth Monitor (nlbwmon) is a lightweight, efficient traffic accounting program keeping track of bandwidth usage per host and protocol.

General Settings | Advanced Settings | **Protocol Mapping**

Protocol mappings to distinguish traffic types per host, one mapping per line. The first value specifies the IP protocol, the second value the port number and the third column is the name of the mapped protocol.

```
1 0 ICMP
2 0 IGMP
4 0 IP-in-IP
6 20 FTP
6 21 FTP
6 22 SSH
6 23 Telnet
6 25 SMTP
6 53 DNS
17 53 DNS
6 80 HTTP
17 80 QUIC
6 109 POP2
6 110 POP3
6 123 NTP
6 137 NetBIOS
```

## 3.13.3 Administration

On this page, you can reset the password for accessing the Router.

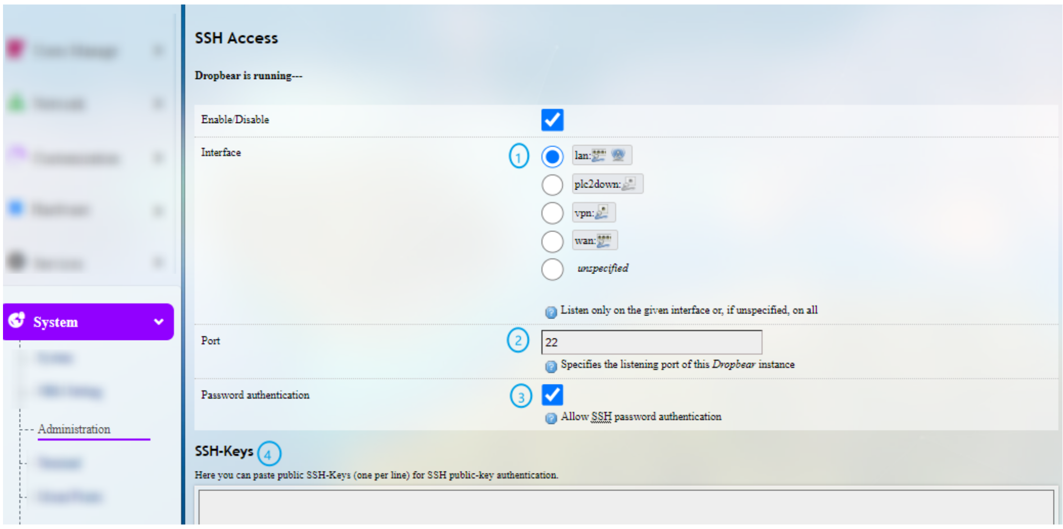
### SSH Access

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;



SSH Access

Dropbear is running---

Enable/Disable ☑

Interface
● lan:
○ plc2down:
○ vpn:
○ wan:
○ *unspecified*

Listen only on the given interface or, if unspecified, on all

Port 22

Specifies the listening port of this *Dropbear* instance

Password authentication ☑

Allow SSH password authentication

SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

Description of the numbered areas

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

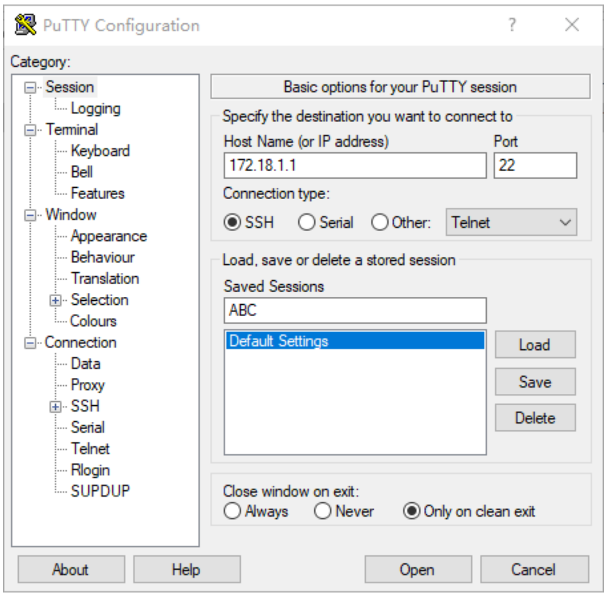
*When “unspecified” is selected, all the ports will be monitored.*

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) unchanged, and select **SSH** for the connection type;

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



Specify the destination you want to connect to

Host Name (or IP address): 172.18.1.1

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

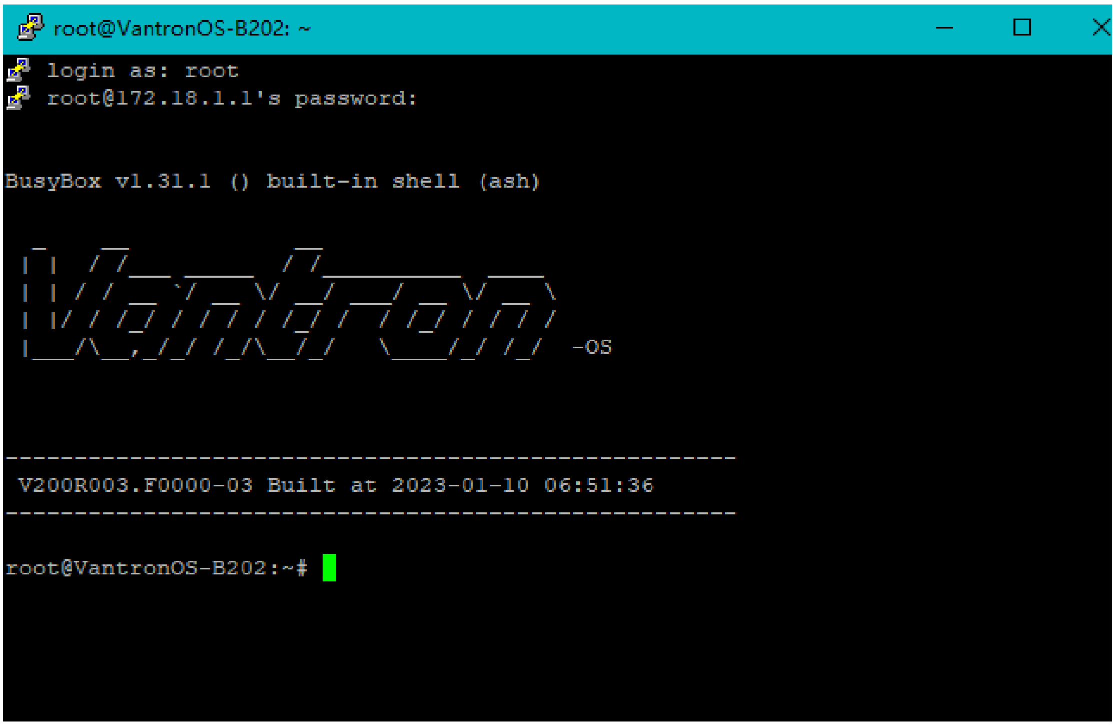
Load, save or delete a stored session

Saved Sessions: ABC

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

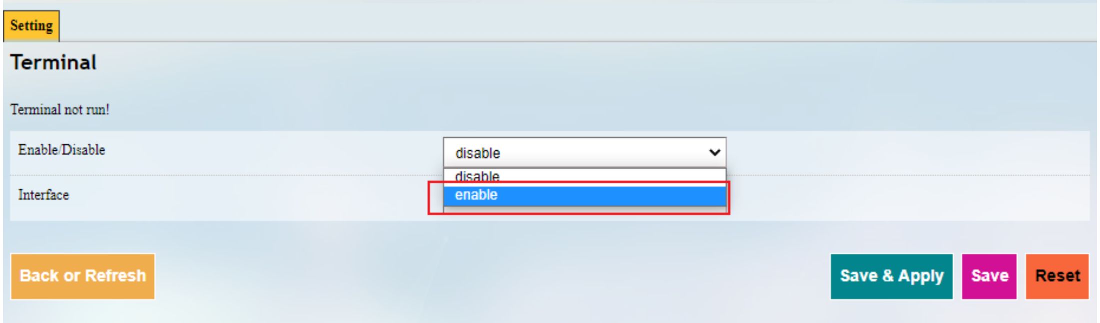
Step 7: Log in with the root account and password (same as those in the prior step), and start an SSH remote session.



```
login as: root
root@172.18.1.1's password:


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

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



-----------------------------------------------------
 V200R003.F0000-03 Built at 2023-01-10 06:51:36
-----------------------------------------------------

root@VantronOS-B202:~#
```

### 3.13.4 Terminal

After navigating to **System > Terminal**, users can click **enable** from the drop-down box under the **Setting** tab and **Save & Apply** the setting to enable the web terminal for router debugging.



Terminal

Terminal not run!

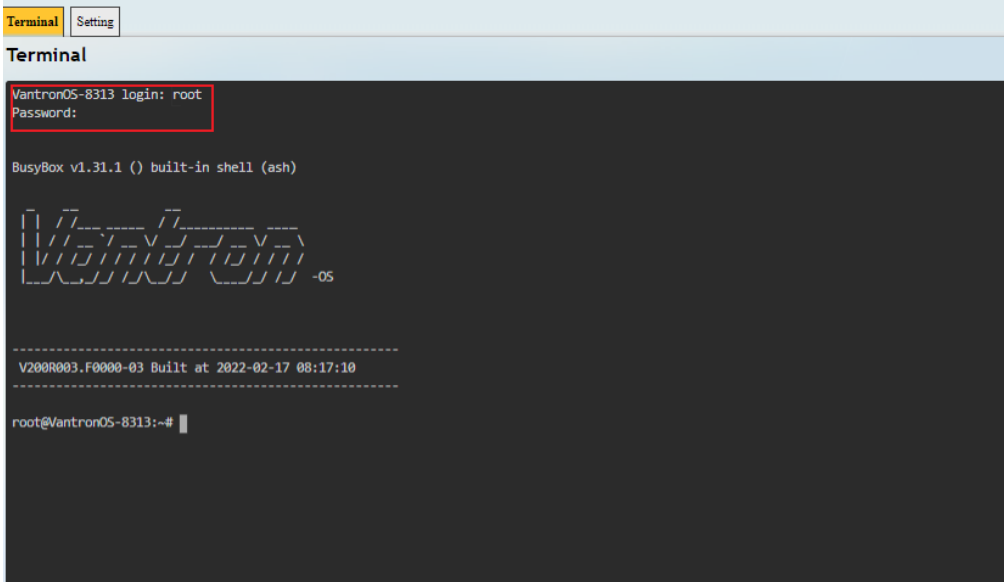
Enable/Disable: disable
- disable
- enable

Interface

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)

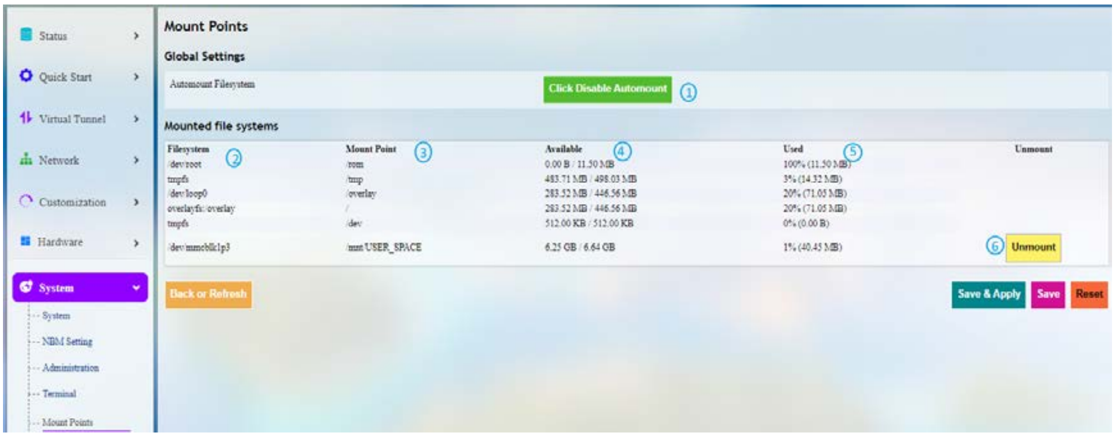


Terminal

```
VantronOS-8313 login: root
Password:


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

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



-----------------------------------------------------
 V200R003.F0000-03 Built at 2022-02-17 08:17:10
-----------------------------------------------------

root@VantronOS-8313:~#
```

### 3.13.5 Mount Points

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



Mount Points

Global Settings

Automount Filesystem

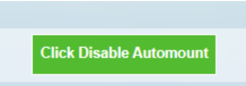
Mounted file systems

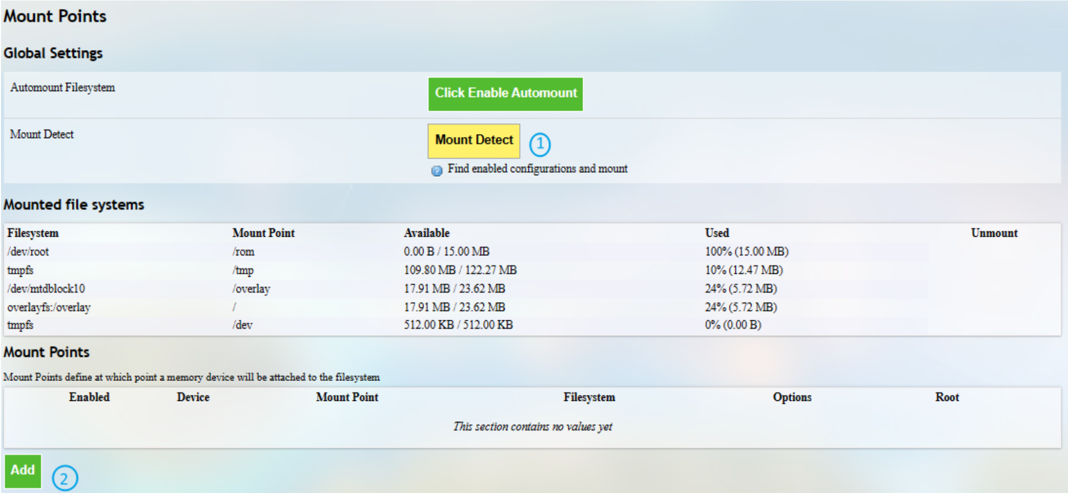
| Filesystem | Mount Point | Available | Used | Unmount |
|---|---|---|---|---|
| /dev/root | /rom | 0.00 B / 11.50 MB | 100% (11.50 MB) | |
| tmpfs | /tmp | 483.71 MB / 498.03 MB | 3% (14.32 MB) | |
| /dev/loop0 | /overlay | 283.52 MB / 446.56 MB | 20% (71.05 MB) | |
| overlayfs:/overlay | / | 283.52 MB / 446.56 MB | 20% (71.05 MB) | |
| tmpfs | /dev | 512.00 KB / 512.00 KB | 0% (0.00 B) | |
| /dev/mmcblk1p3 | /mnt/USER_SPACE | 6.25 GB / 6.64 GB | 1% (40.45 MB) | Unmount |

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.





Mount Points

Global Settings

Automount Filesystem — Click Enable Automount

Mount Detect — Mount Detect ①
Find enabled configurations and mount

Mounted file systems

| Filesystem | Mount Point | Available | Used | Unmount |
|---|---|---|---|---|
| /dev/root | /rom | 0.00 B / 15.00 MB | 100% (15.00 MB) | |
| tmpfs | /tmp | 109.80 MB / 122.27 MB | 10% (12.47 MB) | |
| /dev/mtdblock10 | /overlay | 17.91 MB / 23.62 MB | 24% (5.72 MB) | |
| overlayfs:/overlay | / | 17.91 MB / 23.62 MB | 24% (5.72 MB) | |
| tmpfs | /dev | 512.00 KB / 512.00 KB | 0% (0.00 B) | |

Mount Points

Mount Points define at which point a memory device will be attached to the filesystem

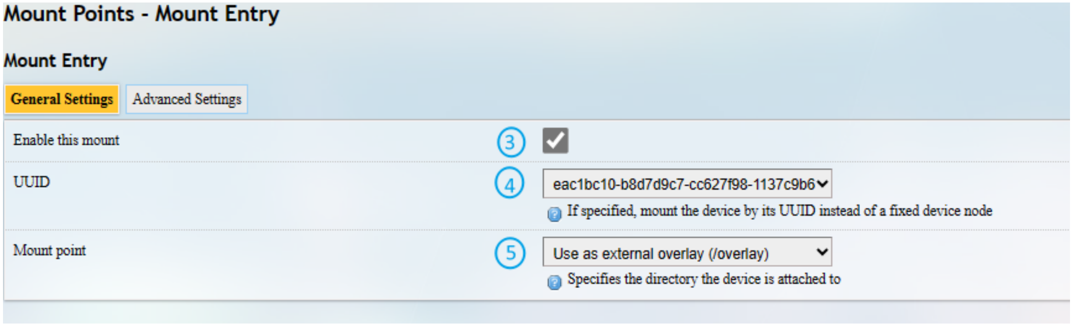
| Enabled | Device | Mount Point | Filesystem | Options | Root |
|---|---|---|---|---|---|
| | | *This section contains no values yet* | | | |

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.



Mount Points - Mount Entry

Mount Entry

Enable this mount ③ ☑

UUID ④ eac1bc10-b8d7d9c7-cc627f98-1137c9b6
If specified, mount the device by its UUID instead of a fixed device node

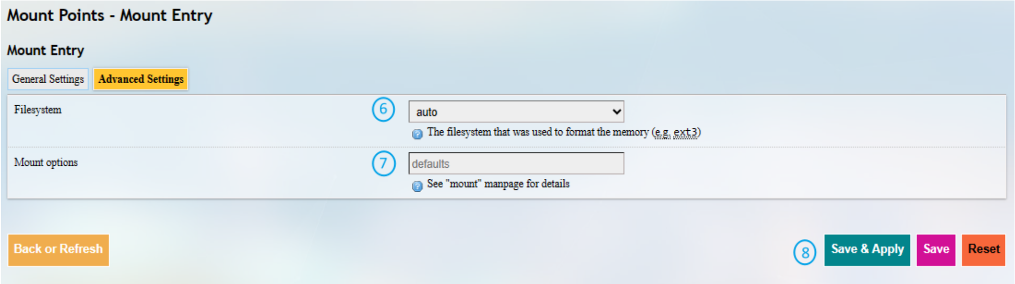
Mount point ⑤ Use as external overlay (/overlay)
Specifies the directory the device is attached to

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.



Mount Points - Mount Entry

Mount Entry

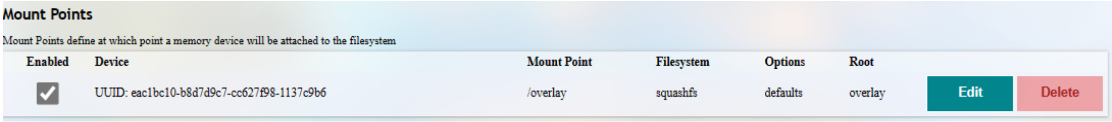
Filesystem: auto

The filesystem that was used to format the memory (e.g. ext3)

Mount options: defaults

See "mount" manpage for details

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



Mount Points

Mount Points define at which point a memory device will be attached to the filesystem

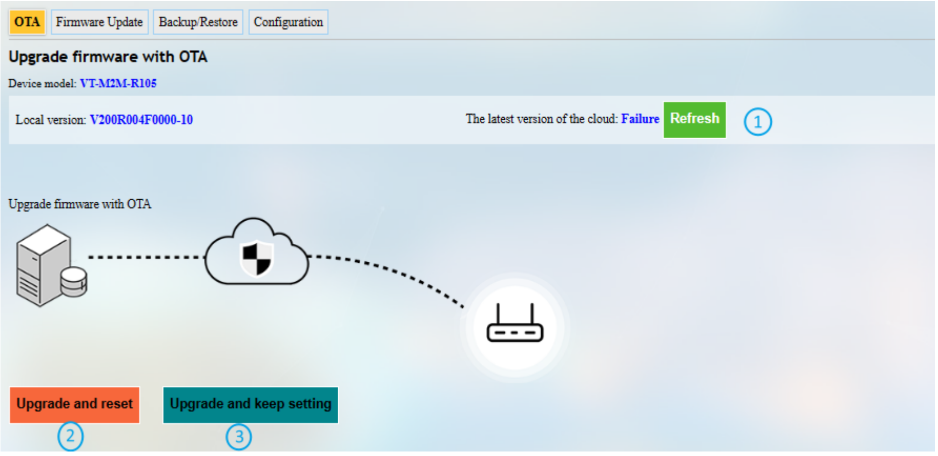
| Enabled | Device | Mount Point | Filesystem | Options | Root | | |
|---|---|---|---|---|---|---|---|
| ☑ | UUID: eac1bc10-b8d7d9c7-cc627f98-1137c9b6 | /overlay | squashfs | defaults | overlay | Edit | Delete |

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



Upgrade firmware with OTA

Device model: VT-M2M-R105

Local version: V200R004F0000-10

The latest version of the cloud: Failure

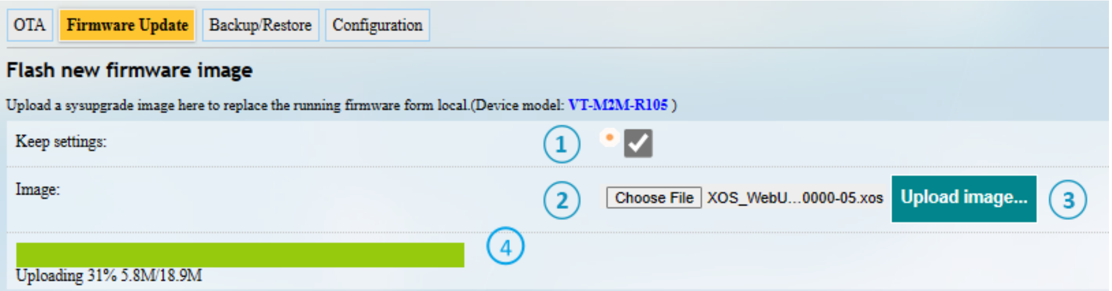
Upgrade firmware with OTA

Description of the numbered areas

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

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

### Firmware Update



Flash new firmware image

Upload a sysupgrade image here to replace the running firmware form local.(Device model: VT-M2M-R105 )

Keep settings: ☑

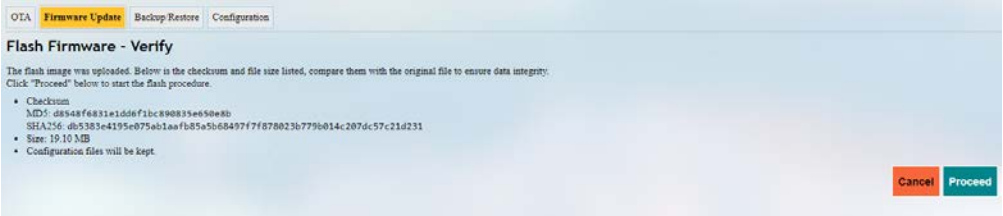
Image: XOS_WebU...0000-05.xos

Uploading 31% 5.8M/18.9M

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;

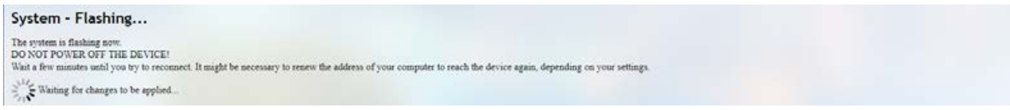


Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

- Checksum
  MD5: d8548f6831e1dd6f1bc898835e650e8b
  SHA256: db5383e4195e075ab1aafb85a5b68497f7f878023b779b014c207dc57c21d231
- Size: 19.10 MB
- Configuration files will be kept

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

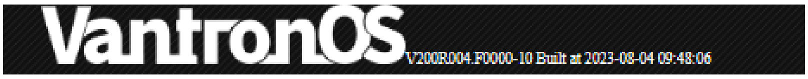


System - Flashing...

The system is flashing now.
DO NOT POWER OFF THE DEVICE!
Wait a few minutes until you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

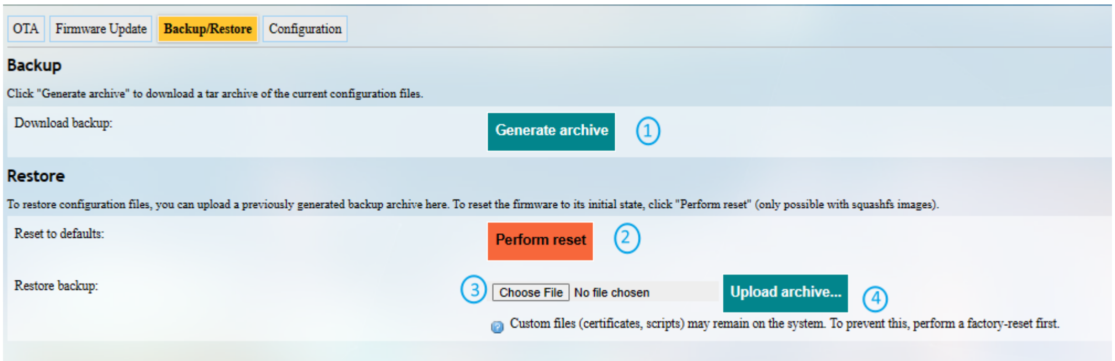
Waiting for changes to be applied...

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



V200R004.F0000-10 Built at 2023-08-04 09:48:06

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.



Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup:

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults:

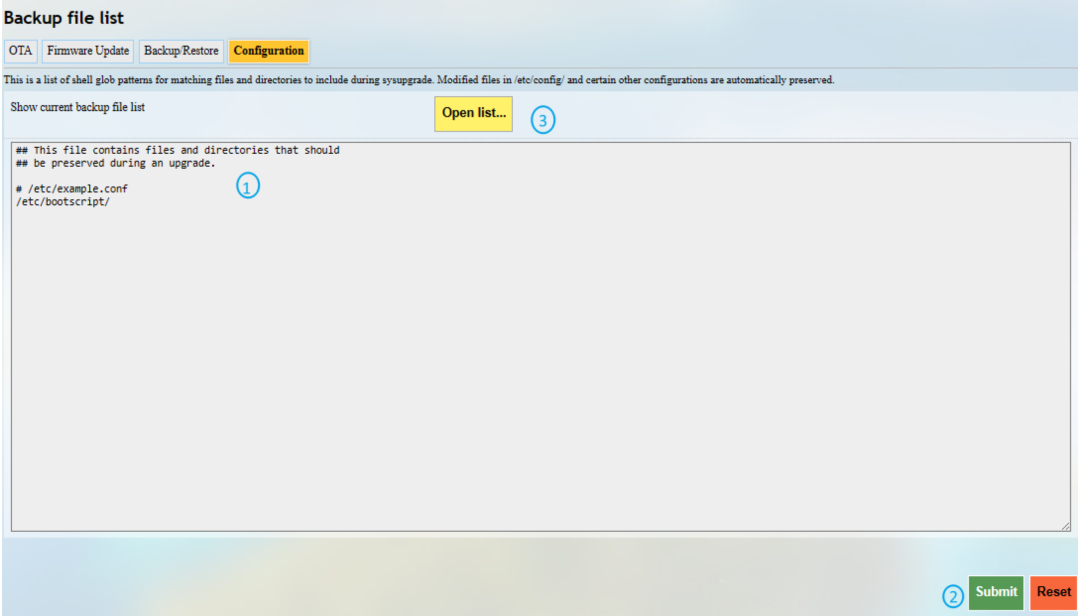
Restore backup: No file chosen

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

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.



This is a list of shell glob patterns for matching files and directories to include during sysupgrade. Modified files in /etc/config/ and certain other configurations are automatically preserved.

Show current backup file list

```
## This file contains files and directories that should
## be preserved during an upgrade.

# /etc/example.conf
/etc/bootscript/
```

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 Router.

## 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**. Make sure you have saved the changes before logout.

# CHAPTER 4 DISPOSAL AND PRODUCT WARRANTY

## 4.1 Disposal

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

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

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

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

## 4.2 Warranty

### Product warranty

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

### Out-of-Warranty Repair

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

### Returned Products

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

# Appendix Regulatory Compliance Statement

## FCC 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.

## IC Statement

This device complies with ISED’s licence-exempt RSSs. 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.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be chosen so that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

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

1. Le dispositif ne doit pas produire de brouillage préjudiciable, et
2. Ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radio électrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.