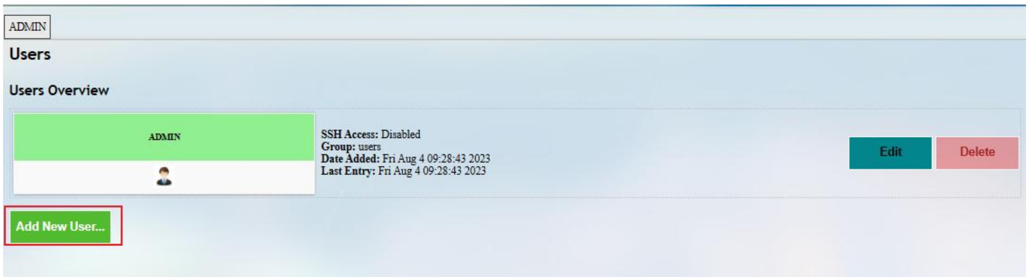
3.9 User Management

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.

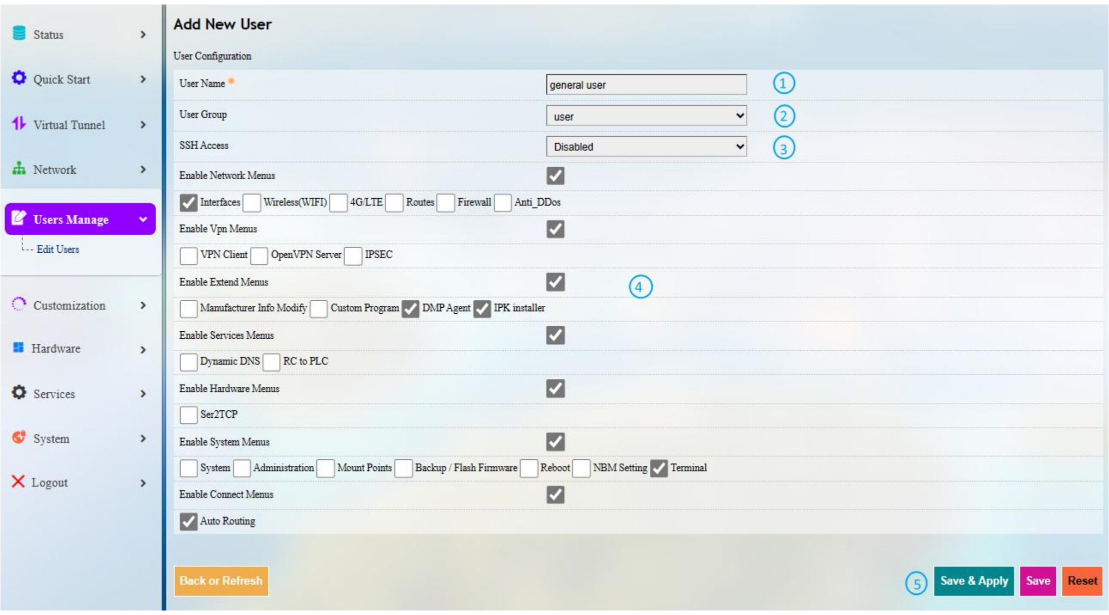
User management allows you to add new users or edit the existing users to assign different permissions to different roles.

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



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.



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

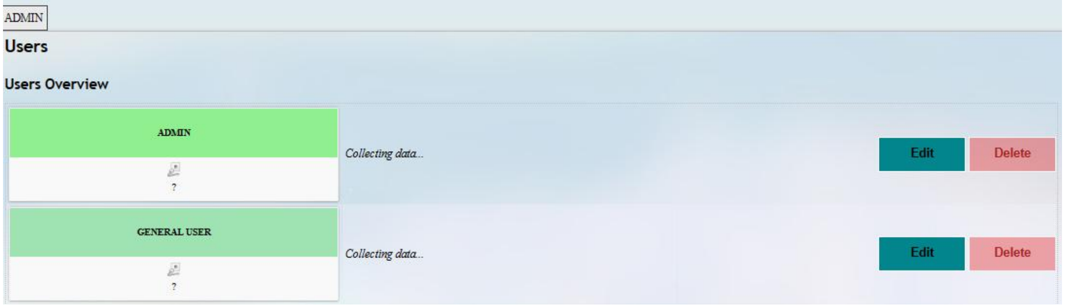
Enable Connect Menus ☑

☑ 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.

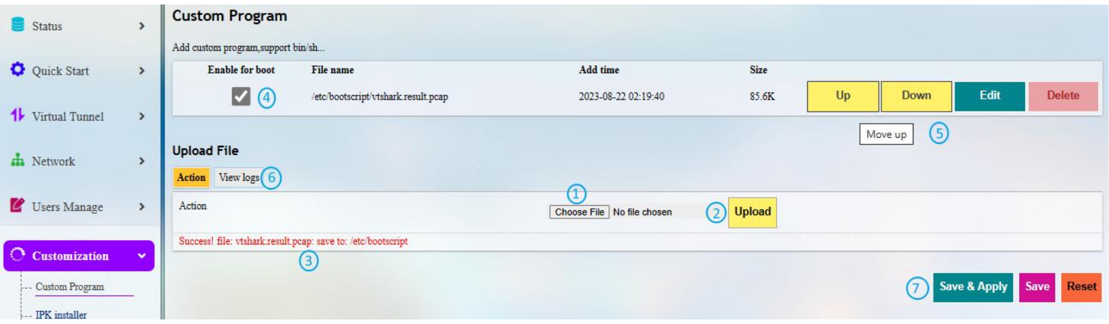


3.10 Customization

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.



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

Action: No file chosen

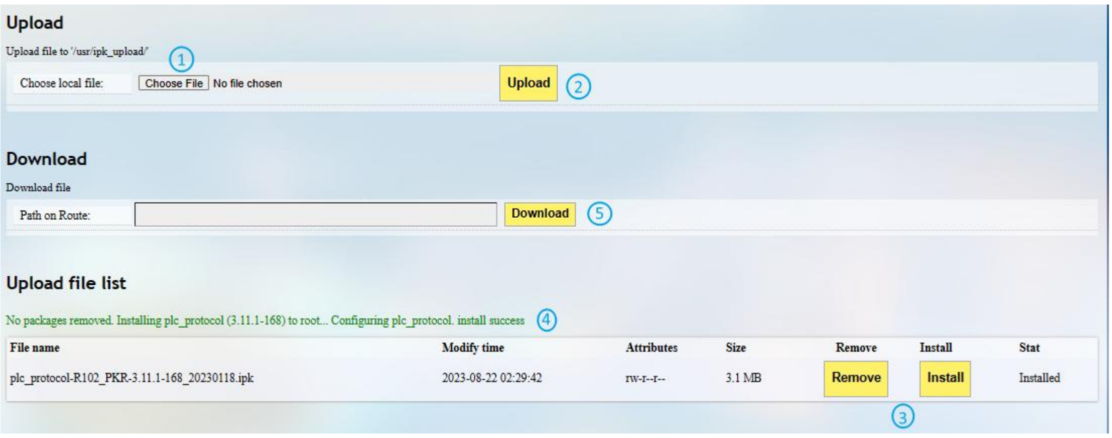
Success! file: vtshark.result.pcap: save to: /etc/bootscript

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: Choose 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

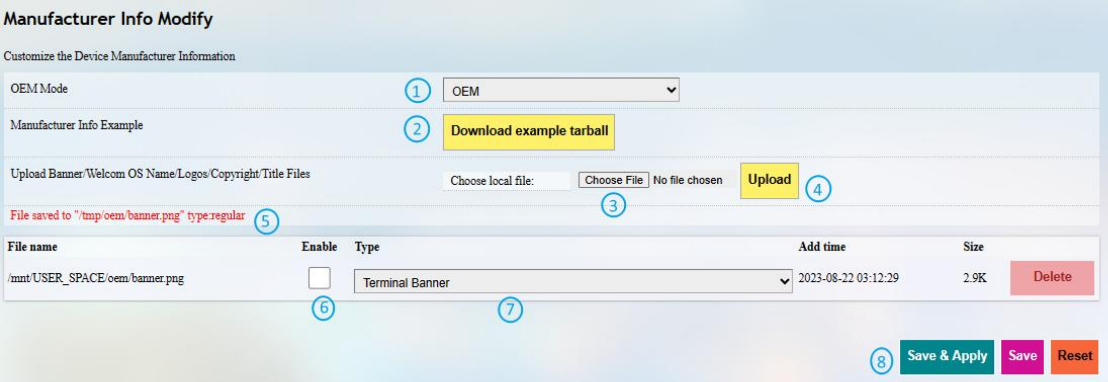
File name	Modify time	Attributes	Size	Remove	Install	Stat
plc_protocol-R102_PKR-3.11.1-168_20230118.ipk	2023-08-22 02:29:42	rw-r--r--	3.1 MB	Remove	Install	Installed

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

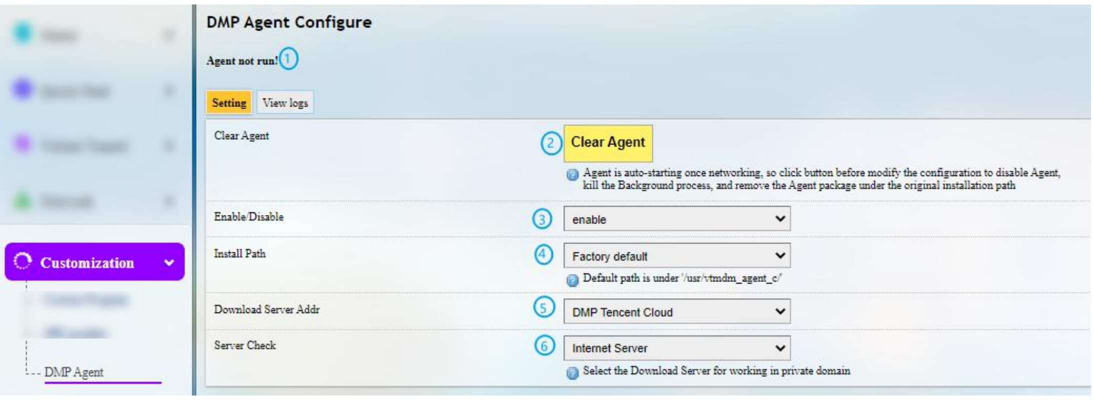
1. Select the **OEM** mode
2. Download the illustrative .tar file to the local directory
3. Select the target file from the local directory
4. Upload the file to the Router
5. The path of the file on the device will be displayed here
6. Choose to enable the file or not for next startup
7. Select the 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!

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: enable

Install Path: Factory default — Default path is under '/usr/vtmdm_agent_c/'

Download Server Addr: DMP Tencent Cloud

Server Check: 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.

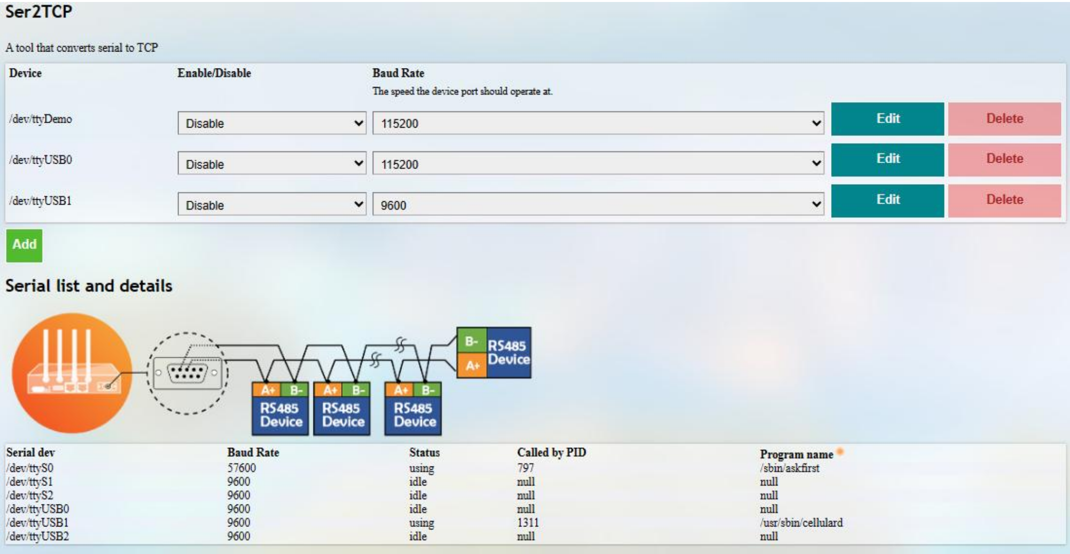
3. Enable/Disable the Agent
4. You can customize the installation path of the Agent here (default path: '/usr/vtmdm_agent_c/')
5. Set up the download address of the Agent server (better to keep the default setting)
6. Internet server for public domain and download server for private domain

*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 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

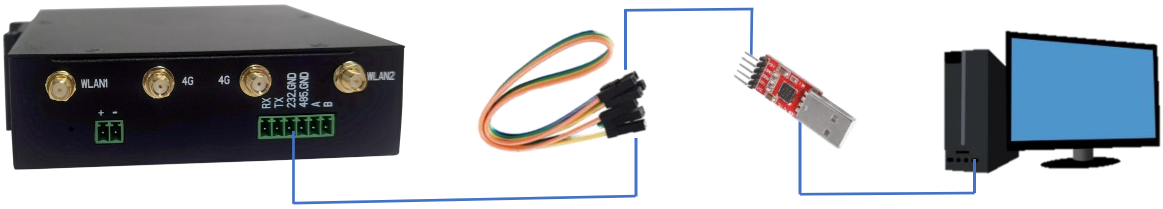
Add

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

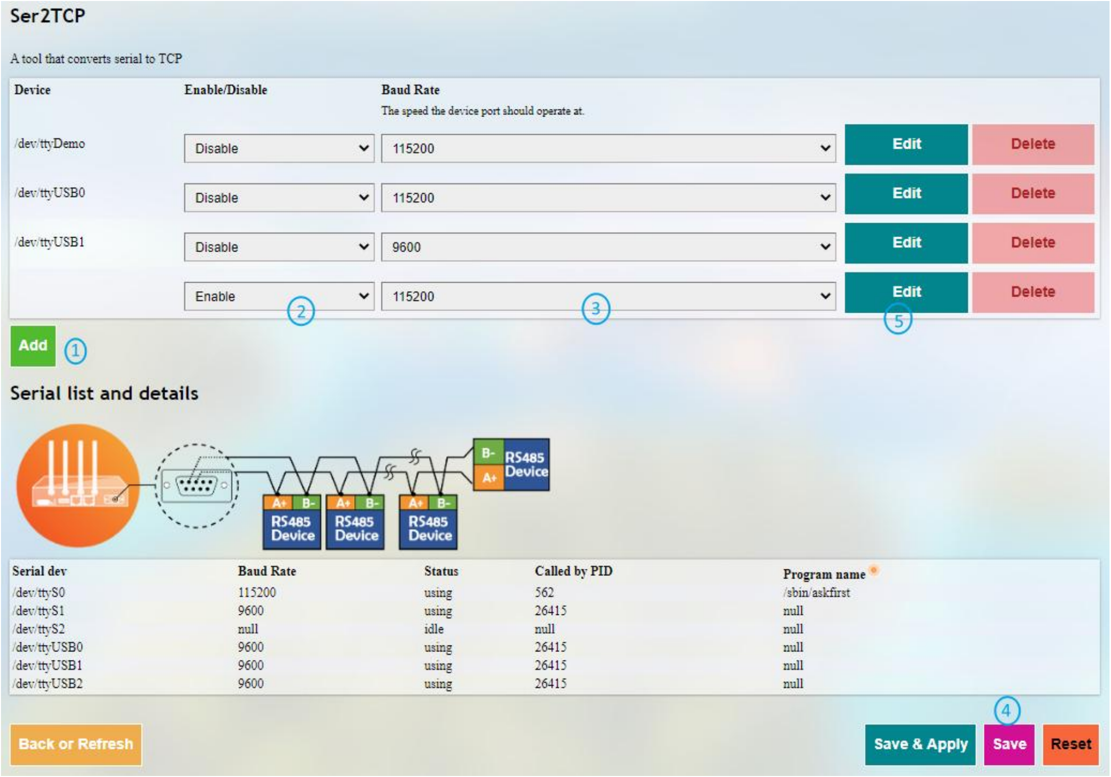
3.11.2 Ser2net Environment Setup and Verification

- 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 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 ②	115200 ③	Edit ⑤	Delete

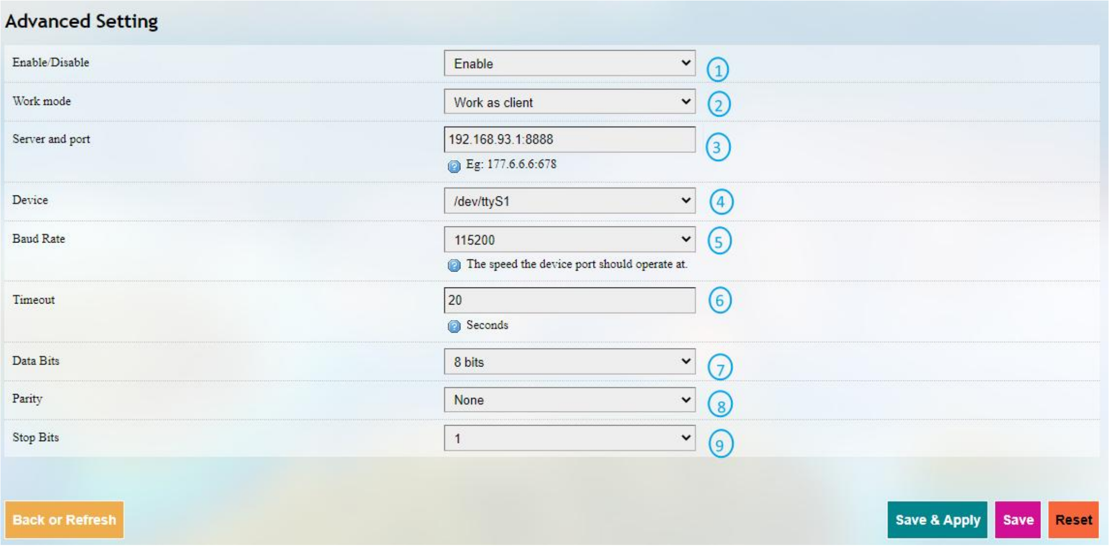
Add ①

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 client ②
Server and port	192.168.93.1:8888 ③ Eg: 177.6.6.6:678
Device	/dev/ttyS1 ④
Baud Rate	115200 ⑤ The speed the device port should operate at.
Timeout	20 ⑥ Seconds
Data Bits	8 bits ⑦
Parity	None ⑧
Stop Bits	1 ⑨

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)

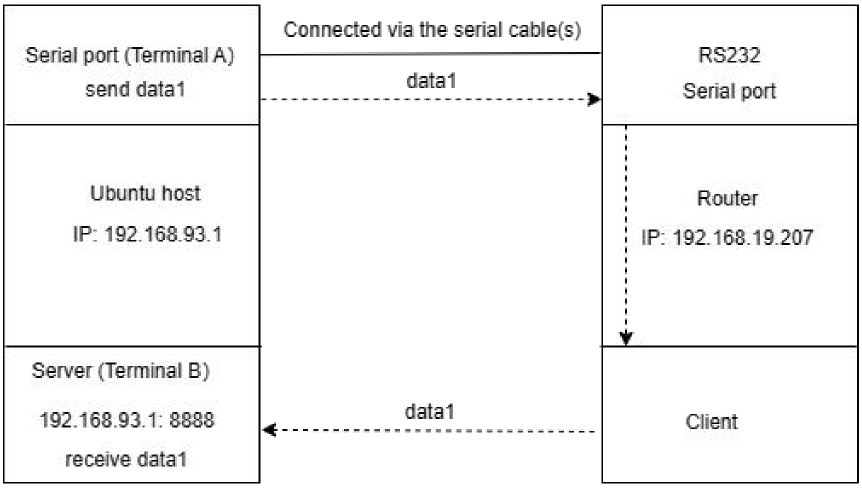
```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

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

-

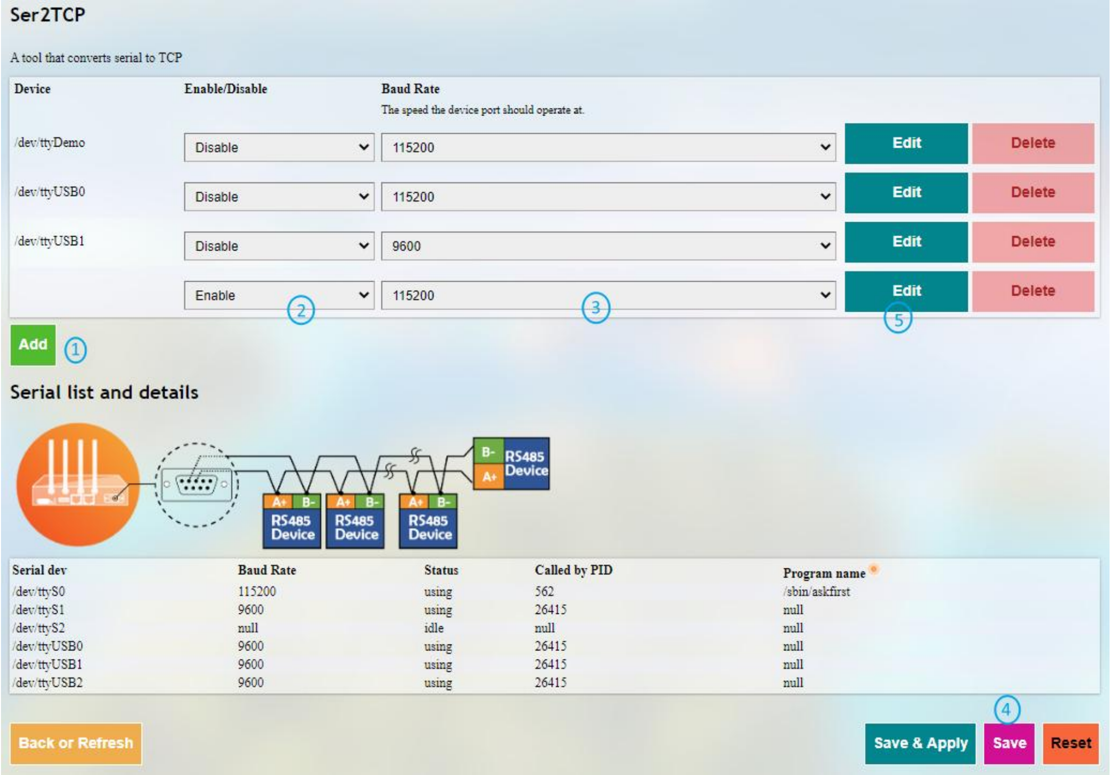
```
tcpudp_test tcp server:tcpudp_test -p 8888
```

ut 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

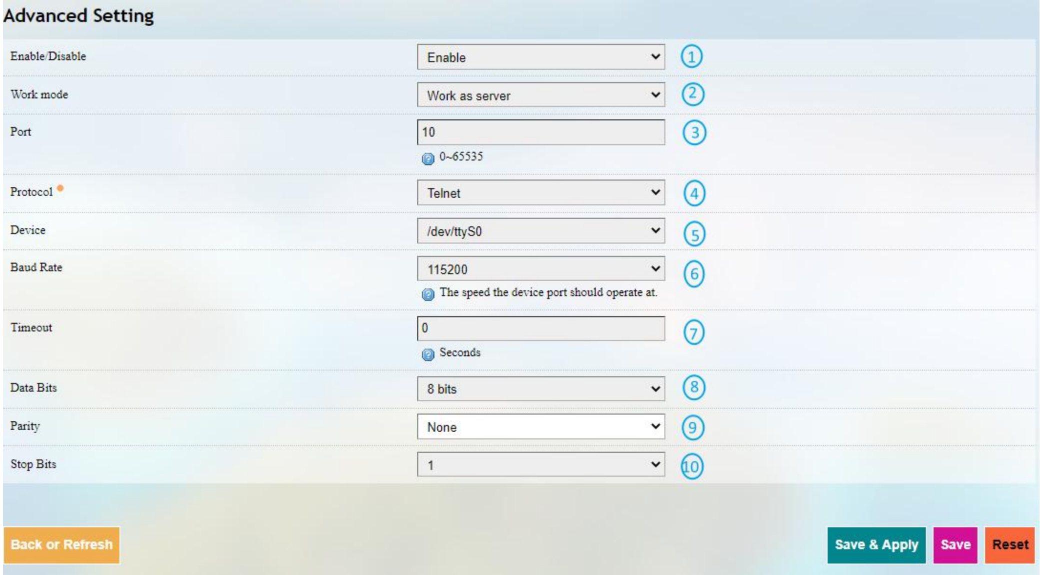
Device	Enable/Disable	Baud Rate The speed the device port should operate at.		
/dev/ttyDemo	Disable	115200	Edit	Delete
/dev/ttyUSB0	Disable	115200	Edit	Delete
/dev/ttyUSB1	Disable	9600	Edit	Delete
	Enable	115200	Edit	Delete

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 0~65535	3
Protocol	Telnet	4
Device	/dev/ttyS0	5
Baud Rate	115200 The speed the device port should operate at.	6
Timeout	0 Seconds	7
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)

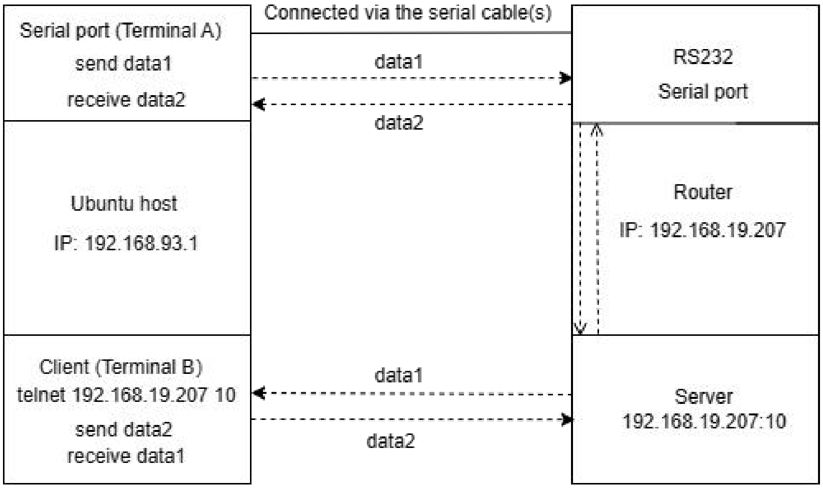
```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

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

-

```
telnet 192.168.19.207 10
```

minals 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.

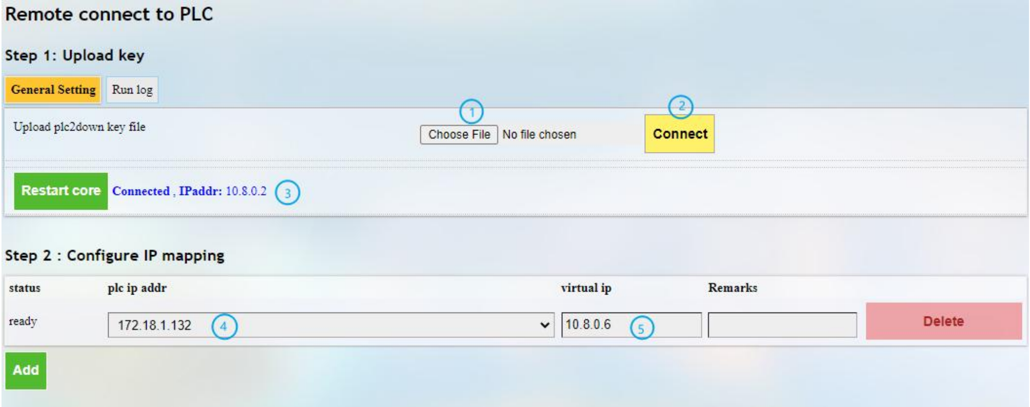
3.12.2 RC to PLC

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 — No file chosen

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)

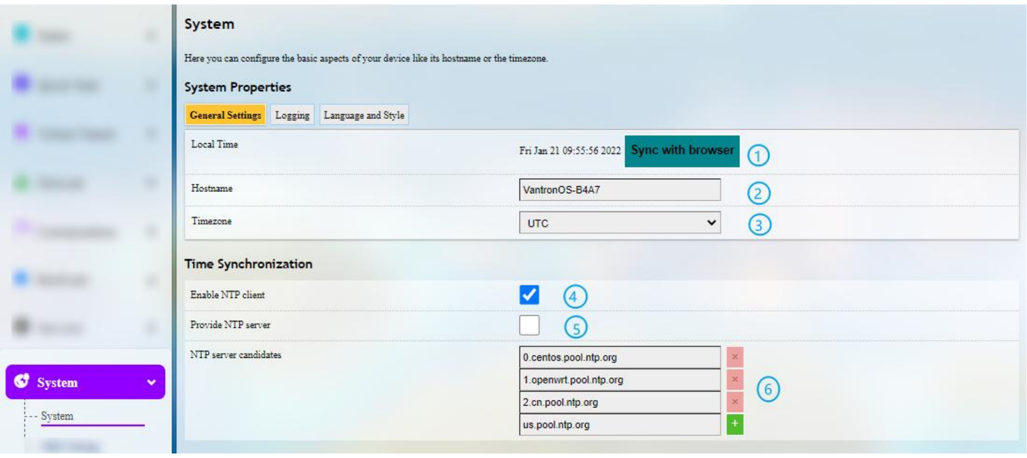
5. Input a virtual IP for the PLC (on the same IP network as the one assigned by the OpenVPN server and not occupied by other clients)

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

Local Time: Fri Jan 21 09:55:56 2022

Hostname: VantronOS-B4A7

Timezone: UTC

Time Synchronization

Enable NTP client ☑

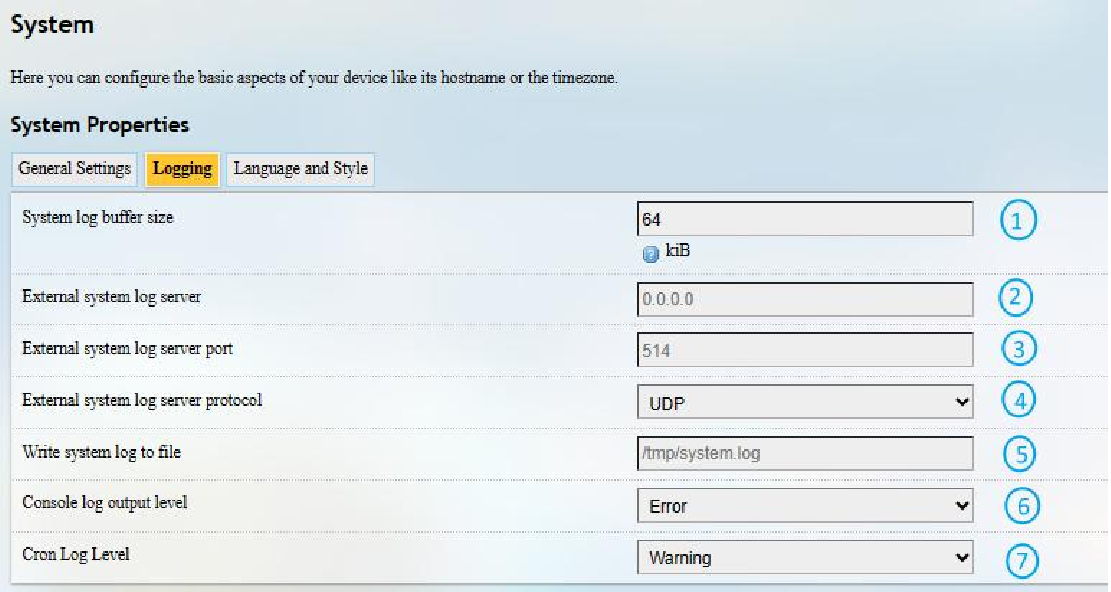
Provide NTP server □

NTP server candidates: 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

System log buffer size: 64 kiB

External system log server: 0.0.0.0

External system log server port: 514

External system log server protocol: UDP

Write system log to file: /tmp/system.log

Console log output level: Error

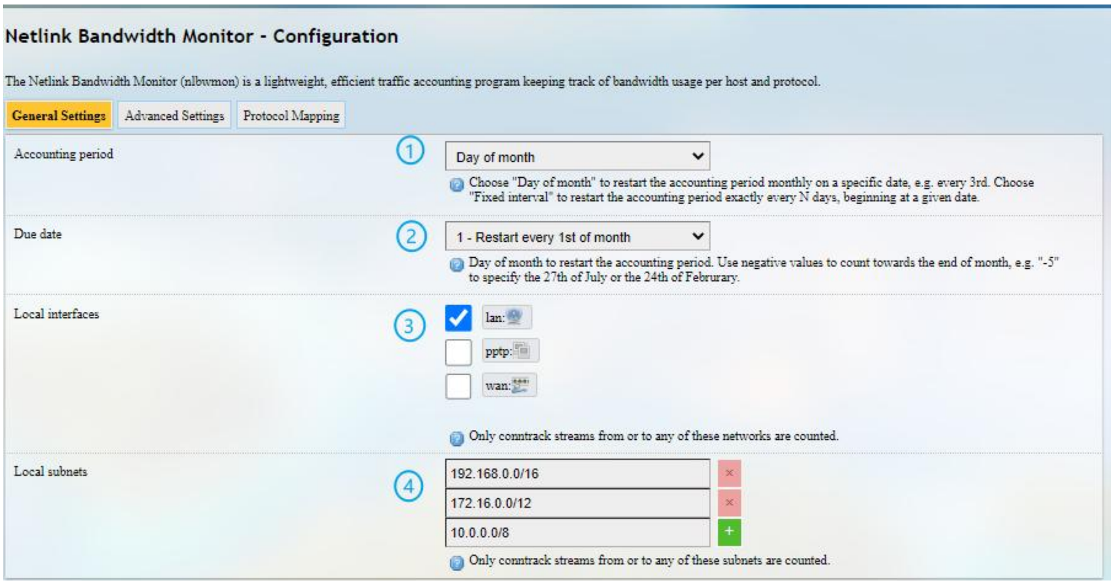
Cron Log Level: Warning

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 ① 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 ② 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 ③
☑ lan:
□ pptp:
□ wan:
Only conntrack streams from or to any of these networks are counted.

Local subnets ④
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.

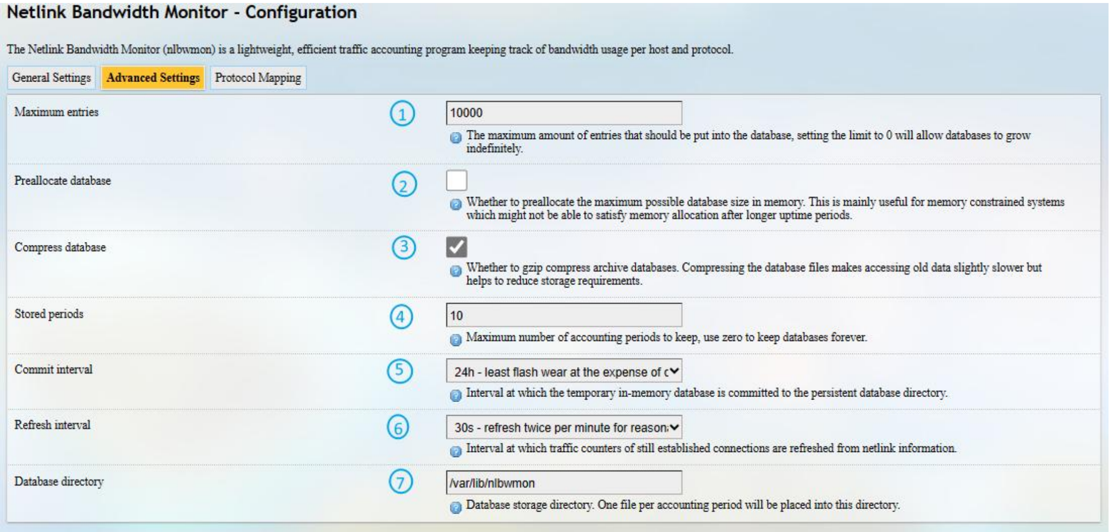
Description of the numbered areas

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.

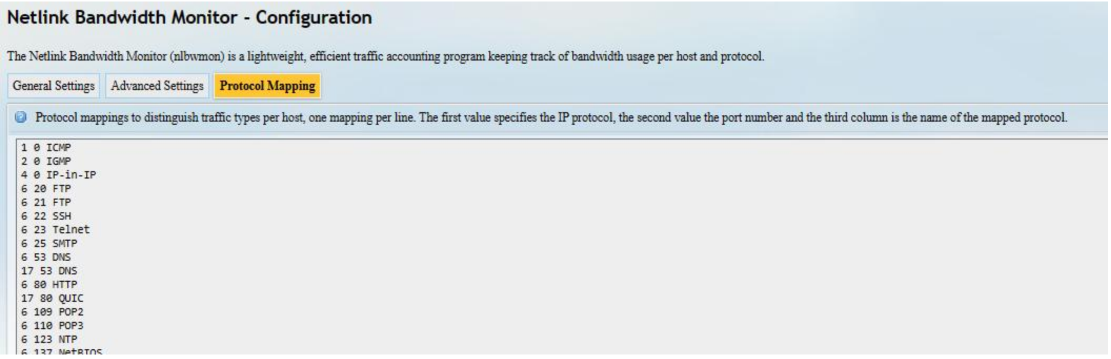
Refresh interval: 30s - refresh twice per minute for reason
Interval at which traffic counters of still established connections are refreshed from netlink information.

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.

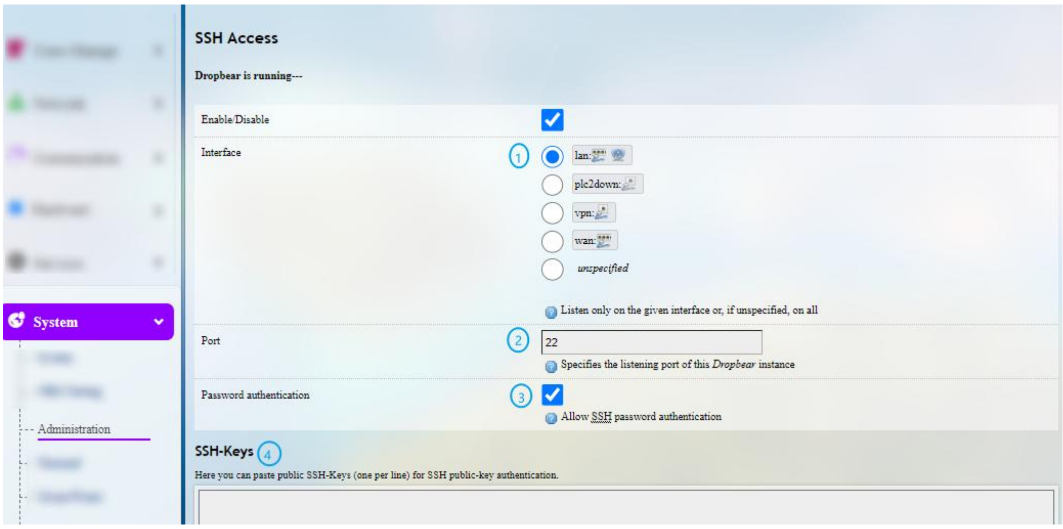
SSH Access

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)

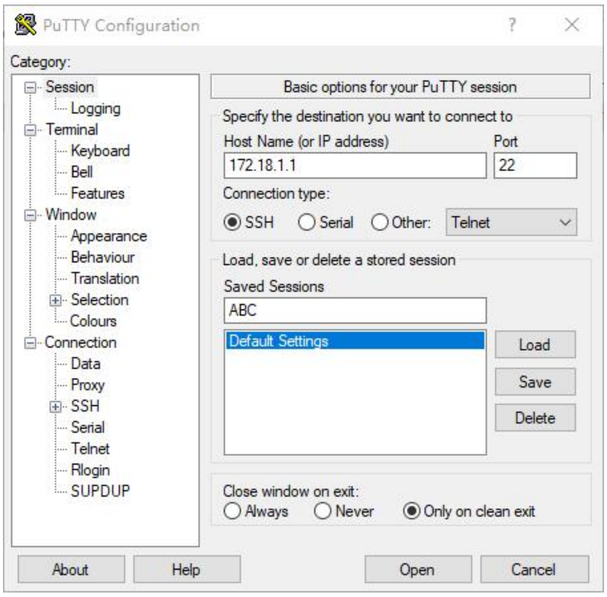
When “unspecified” is selected, all the ports will be monitored.

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

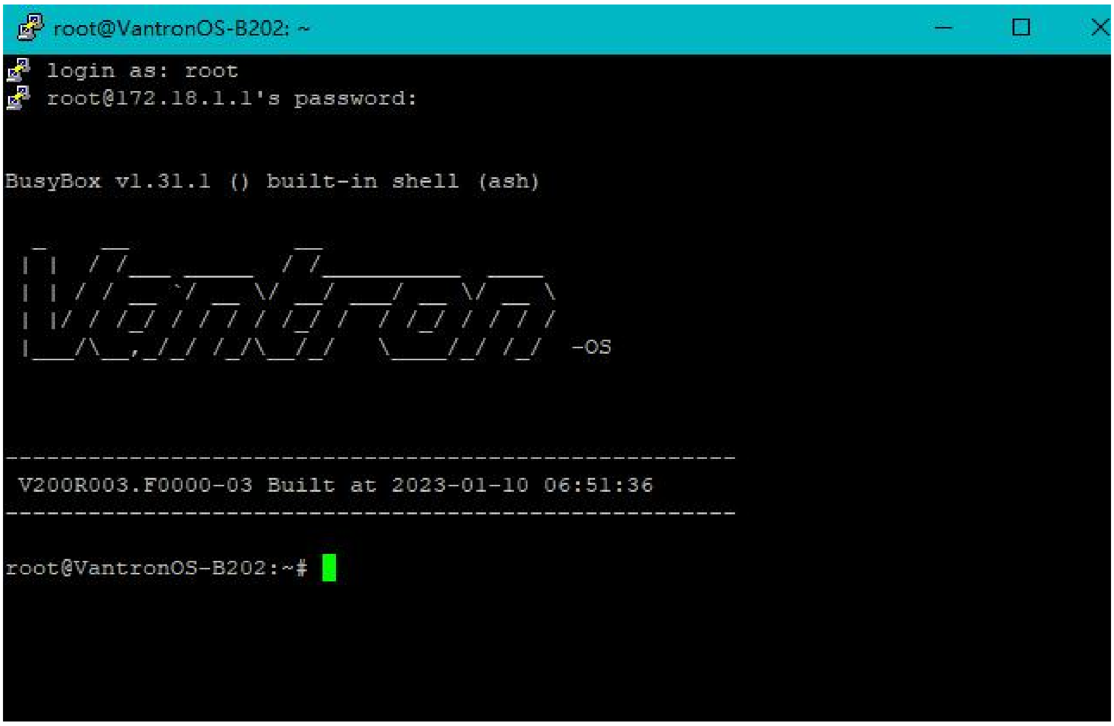
Load, save or delete a stored session

Saved Sessions: ABC

Default Settings

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

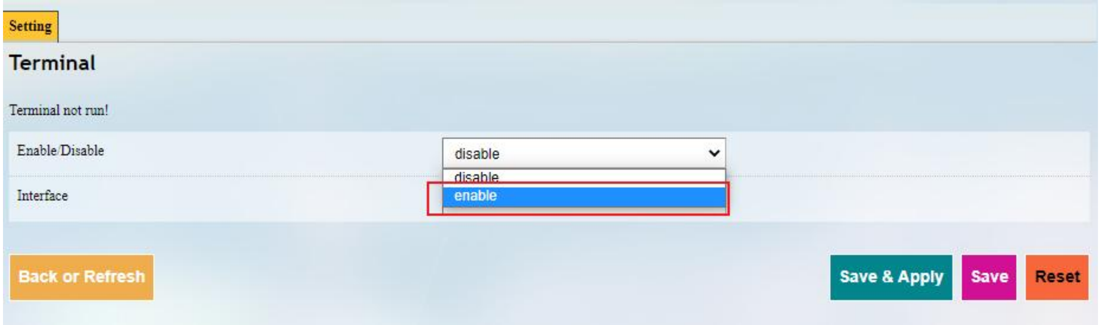
Step 7: Log in with the root account and password (same as those in the prior step), and start an SSH remote session.



```
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

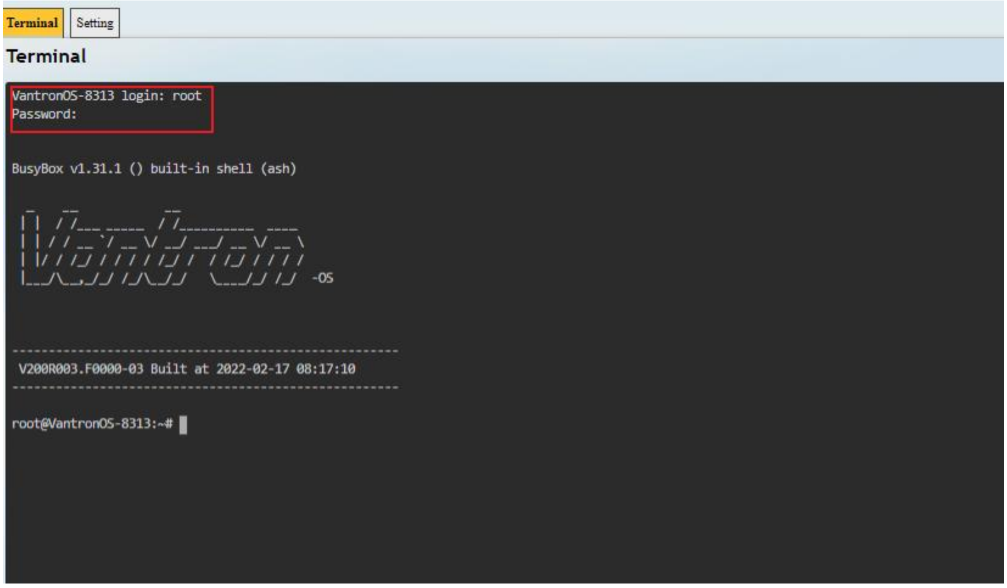
After navigating to **System > Terminal**, users can click **enable** from the drop-down box under the **Setting** tab and **Save & Apply** the setting to enable the web terminal for router debugging.



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

Login name: root

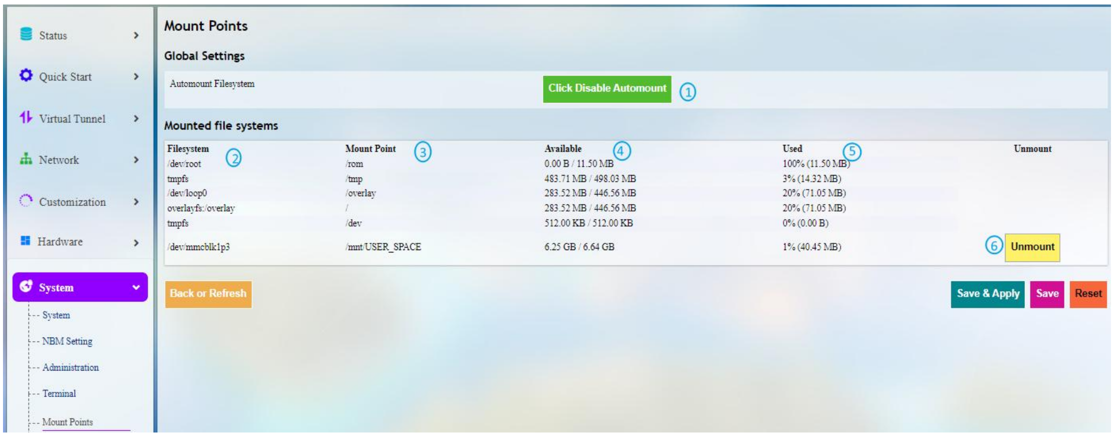
Login password: rootpassword (invisible while typing)



```
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 — Click Disable Automount

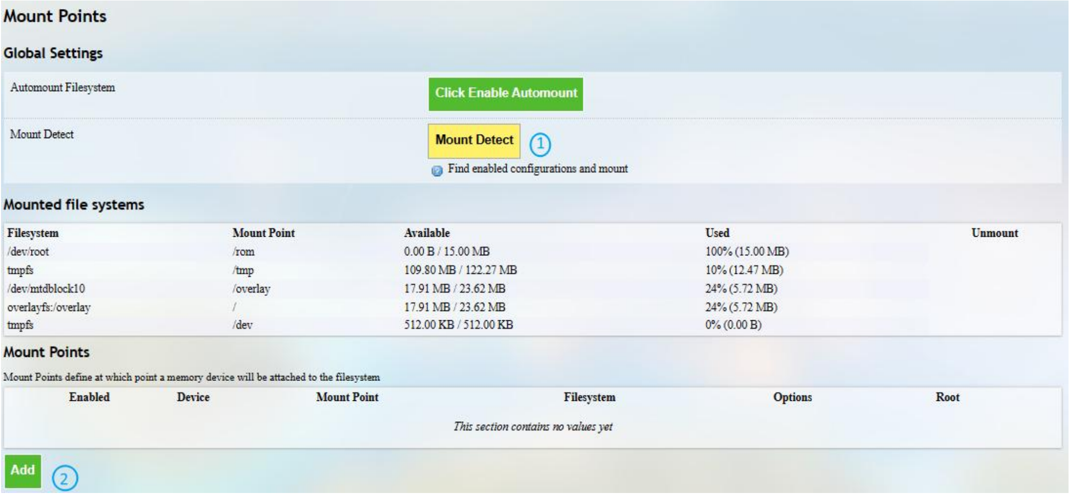
Mounted file systems

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

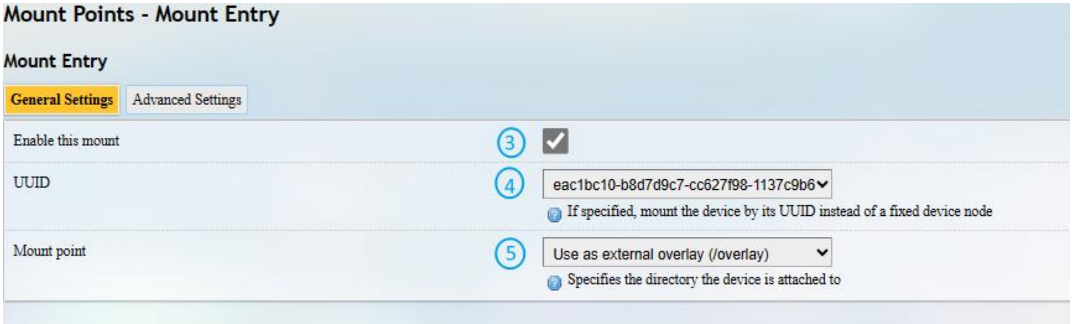
Enabled	Device	Mount Point	Filesystem	Options	Root

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

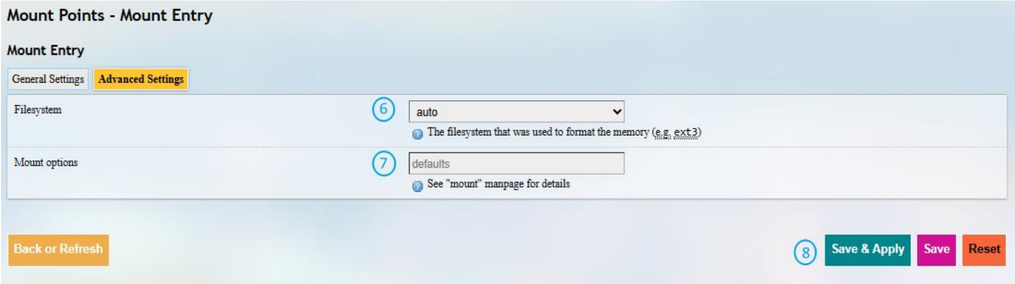
Enable this mount ③ ☑

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

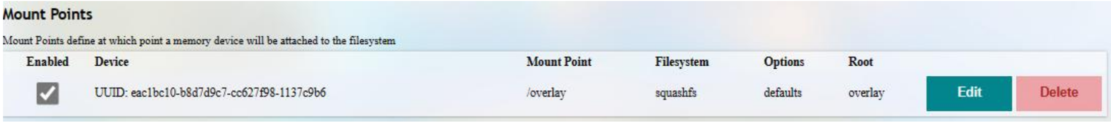
Mount Entry

General Settings | Advanced Settings

Filesystem (6) auto
The filesystem that was used to format the memory (e.g. ext3)

Mount options (7) 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

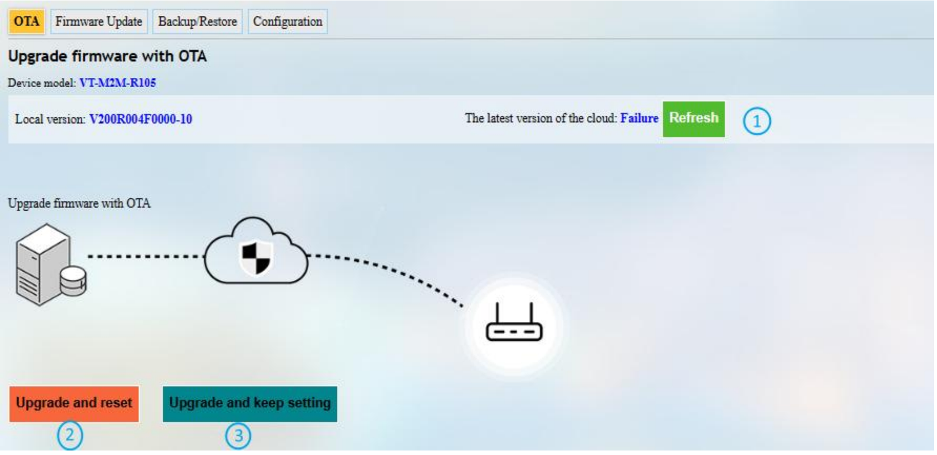
Enabled	Device	Mount Point	Filesystem	Options	Root		
☑	UUID: eac1bc10-b8d7d9c7-cc627f98-1137c9b6	/overlay	squashfs	defaults	overlay	Edit	Delete

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



OTA | Firmware Update | Backup/Restore | Configuration

Upgrade firmware with OTA

Device model: VT-M2M-R105

Local version: V200R004F0000-10

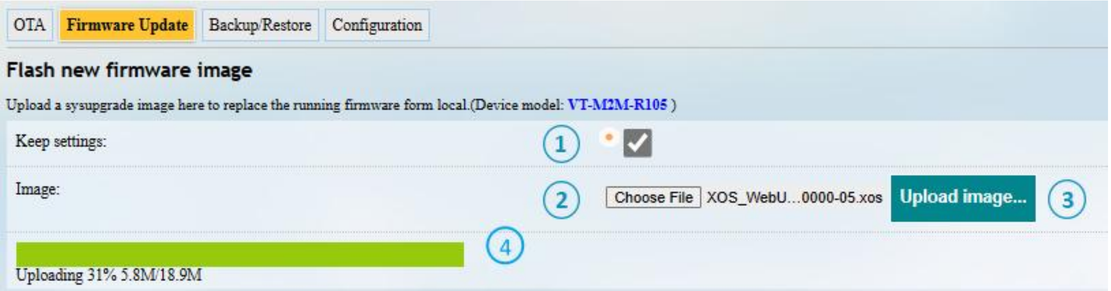
The latest version of the cloud: Failure

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: ☑

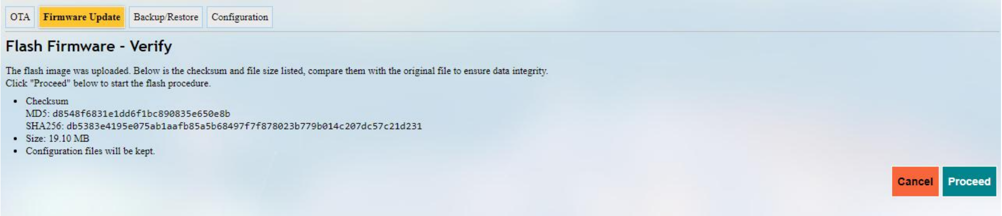
Image:

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;

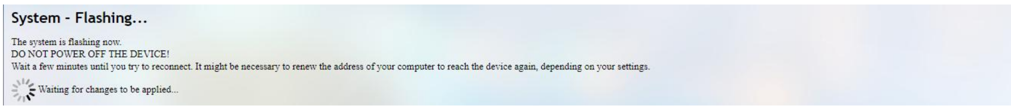


Flash Firmware - Verify

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: d8548f6831e1dd6f1bc890835e650e8b
  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;

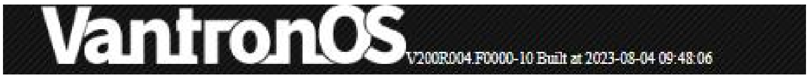


System - Flashing...

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.

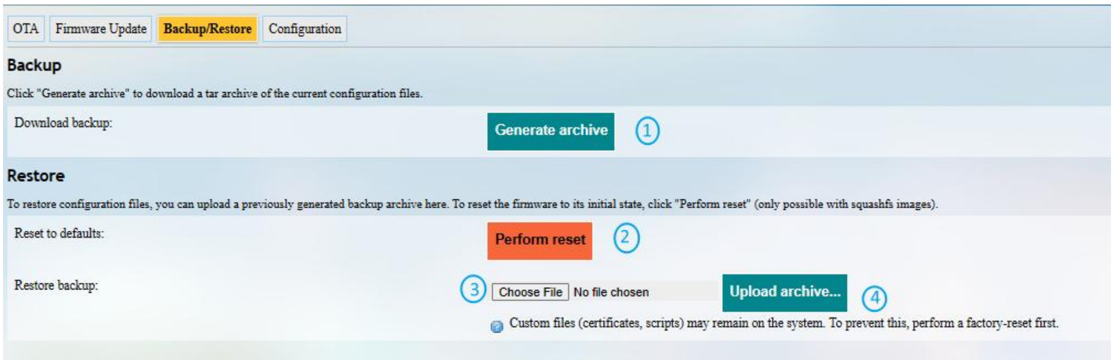
Waiting for changes to be applied...

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



VantronOS 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:

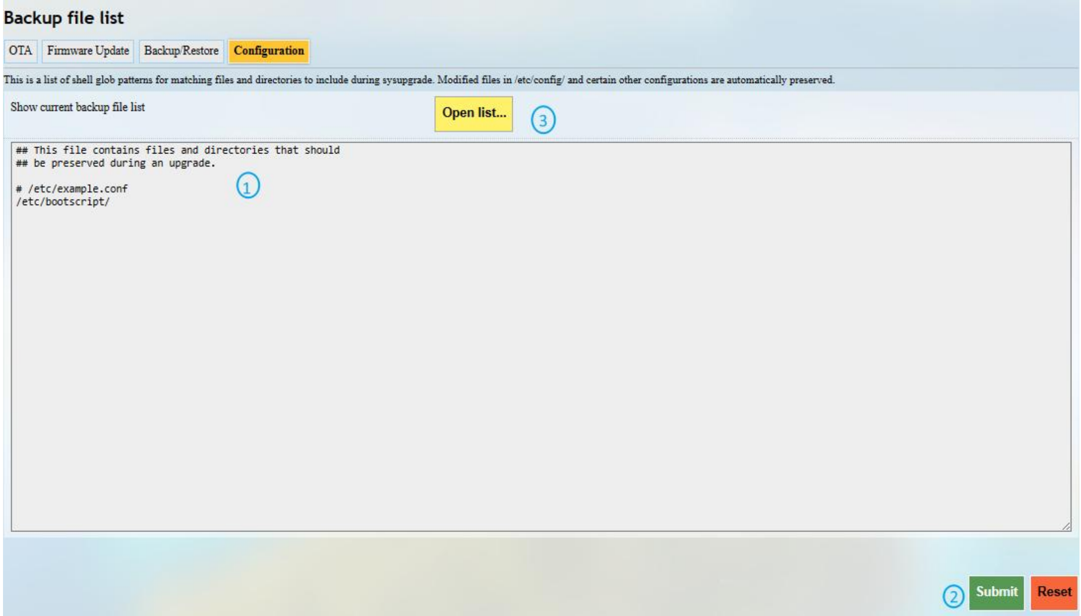
Restore backup:

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.



Backup file list

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.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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.

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

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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.

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

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps.