IOTROUTER

Industrial IoT | Empowering the Edge

FlowPLC ®

EM Series

Quick Start Guide

Chengdu Zongheng Intelligence Control Technology Co., Ltd.

1 Power Supply and Connection

1.1 Power and Indicator Status

Connect a 12 VDC power supply to the gateway power terminal. After power-on, the power indicator remains steadily lit when the supply is normal.

Mark	Function	Status	Description
PWR	Power	Off	Abnormal power supply
PWR	Power	Steady on	Power supply normal
RUN	Operating status	600 ms on / 600 ms off	Abnormal status
RUN	Operating status	100 ms on / 2700 ms off	Operating normally
WiFi	STA status	Off	STA mode disabled
WiFi	STA status	Steady on	STA mode enabled and connected to an external hotspot
WiFi	STA status	Flashing	STA mode enabled but not connected
NET	Cellular status	Off	Cellular network disabled
NET	Cellular status	600 ms on / 600 ms off	Cellular enabled; module detection in progress
NET	Cellular status	200 ms on / 200 ms off	Dial-up in progress
NET	Cellular status	Steady on	Dial-up successful
LED1 / LED2	User-defined	User-defined	User-defined

Mark	Function	Status	Description
P	Power	Off	Abnormal power supply
P	Power	Steady on	Normal power supply
E	Exception status	Off	No slave status
E	Exception status	Steady on	Addressing error
E	Exception status	1000 ms on / 1000 ms off	Configuration error
E	Exception status	200 ms on / 200 ms off	Slave offline
TX1-4	RS485 transmit	Off / steady on	No data sent / data activity
RX1-4	RS485 receive	Off / steady on	No data received / data received
DI	Digital input	Off / steady on	No input / input active
DO	Digital output	Off / steady on	Output off / output active

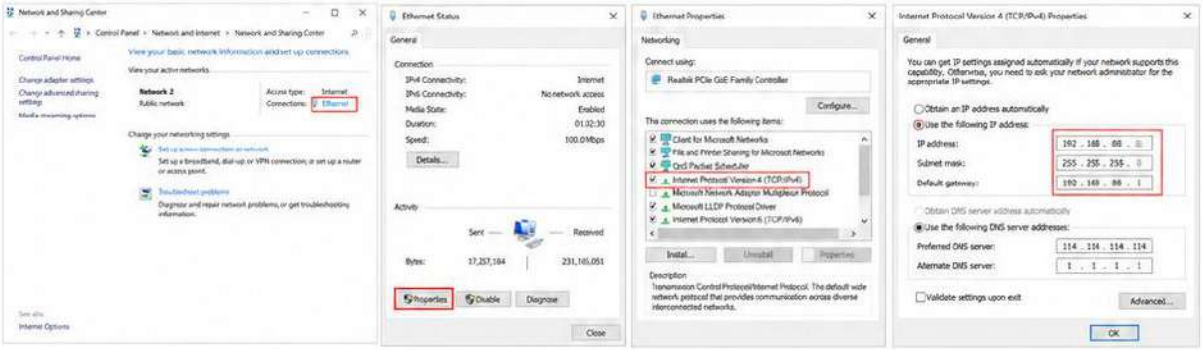
Indicator	Function	Status	Status Description
PWR	Power Indicator	Off	Power supply abnormal
		On	Power supply normal
RUN	Operation Status Indicator	600ms On/600ms Off	Status abnormal
		100ms On/2700ms Off	Operation normal
WiFi	STA Status Indicator	Off	STA mode disabled
		On	STA mode enabled, connected to external hotspot
		Blinking	STA mode enabled, not connected to external hotspot
NET	Cellular Network Status	Off	Cellular network not enabled
		600ms On/600ms Off	Cellular network enabled and module under detection
		200ms On/200ms Off	Dialing
		On	Dial successful
LED1	User-defined	User-defined	User-defined
LED2	User-defined	User-defined	User-defined

Indicator	Function	Status	Status Description
P	Power Indicator	Off	Power supply abnormal
		On	Power supply normal
E	Exception Indicator	Off	No station status
		On	Address conflict
		1000ms On/1000ms Off	Configuration error
		200ms On/200ms Off	Off-station
TX1–4	485 Data Transmit Indicator	Off	No data transmission
		On	Data transmission
RX1–4	485 Data Receive Indicator	Off	No data reception
		On	Data reception

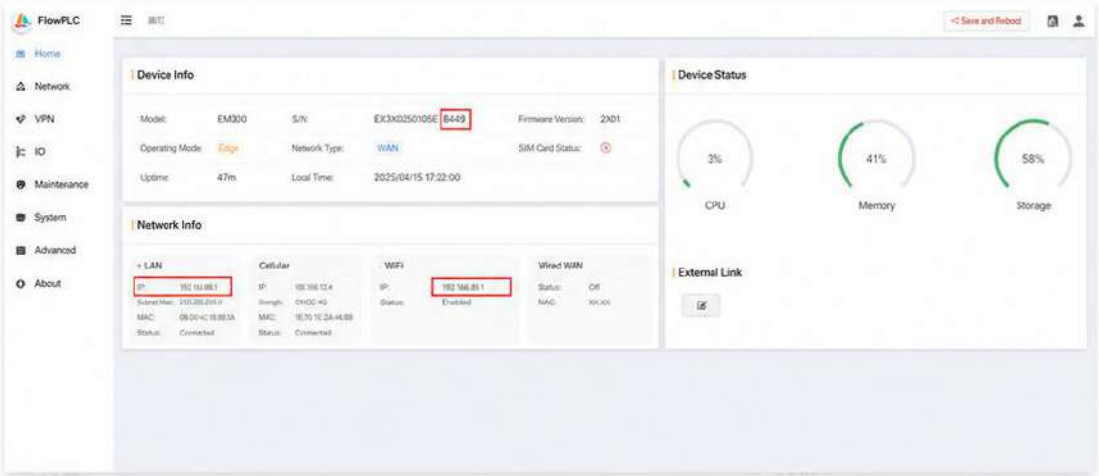
DI	Digital Input State	Normally Off	No Signal Input
		Normally On	Signal Input Present
DO	Digital Output State	Normally Off	No Output
		Normally On	Output Present

2. Connecting the Device

Method 1: Connect the computer's Ethernet port to the device's LAN port. The device's LAN is set to static IP 192.168.88.1 by default, so you need to set the computer's IP address to the same subnet (e.g., 192.168.88.x), as shown below:



Method 2: Connect to the WiFi hotspot broadcast by the device. WiFi name: (SX-series serial number last 4 digits), password: EM12345678. The WiFi default IP is 192.168.88.1 (in the same subnet as the LAN IP), as shown below:



Basic Usage

4

1.2 Connect to the Device

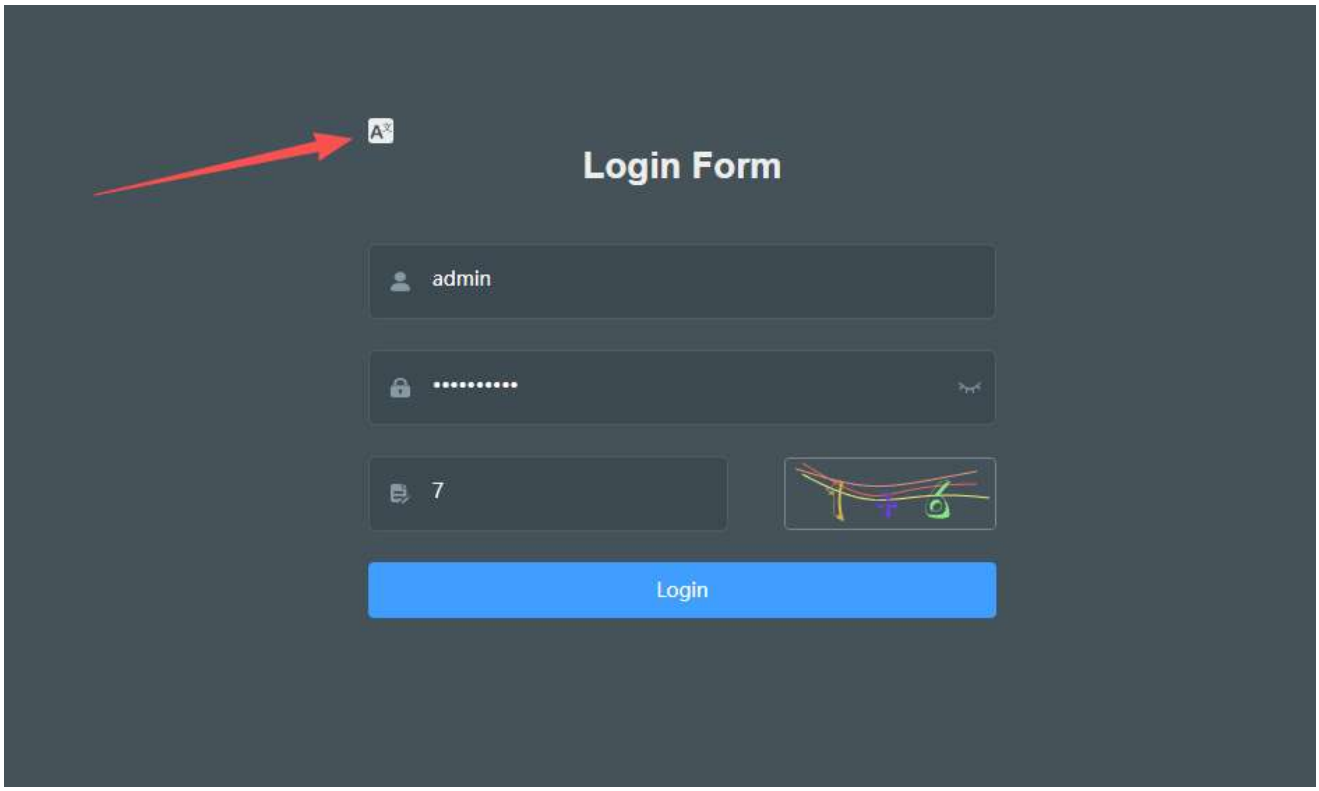
Method 1 Connect the computer Ethernet port to a device LAN port. Because the default LAN IP address is 192.168.88.1, set the computer to the same subnet, for example 192.168.88.x.

Method 2 Connect the computer to the gateway Wi-Fi hotspot. The default SSID is the gateway model followed by the last four digits of the serial number. The default password is EM12345678. The default Wi-Fi IP address is 192.168.88.1 and is synchronized with the LAN IP address.

2 Basic Operation

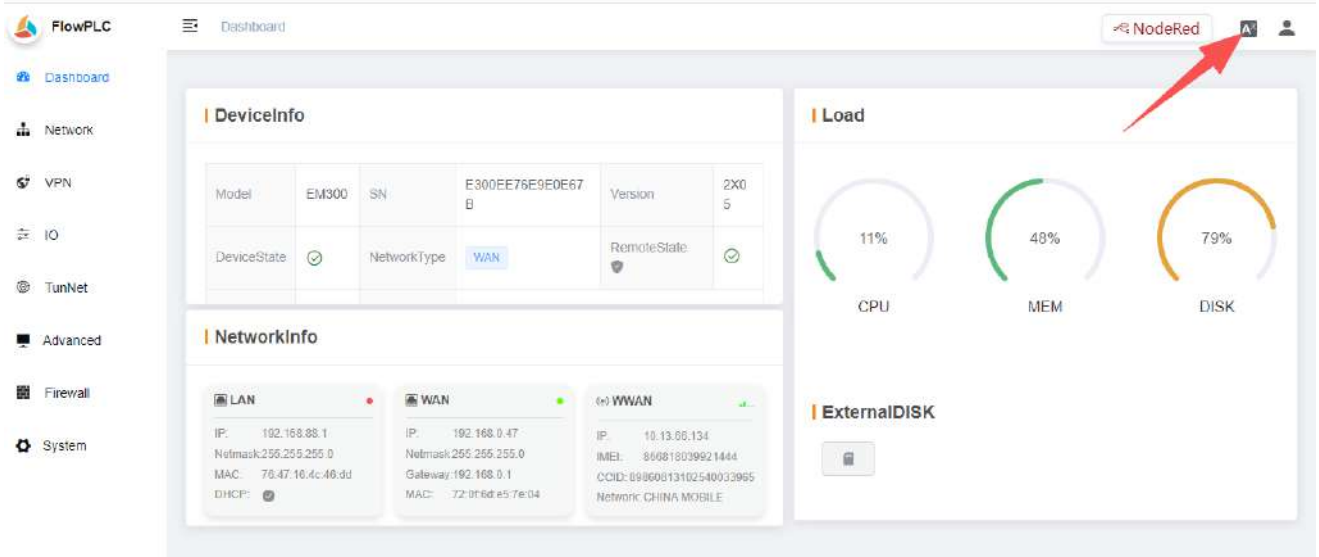
2.1 Login

Open a browser and enter 192.168.88.1 in the address bar. The default administrator password is EM12345678. You can change it after logging in.

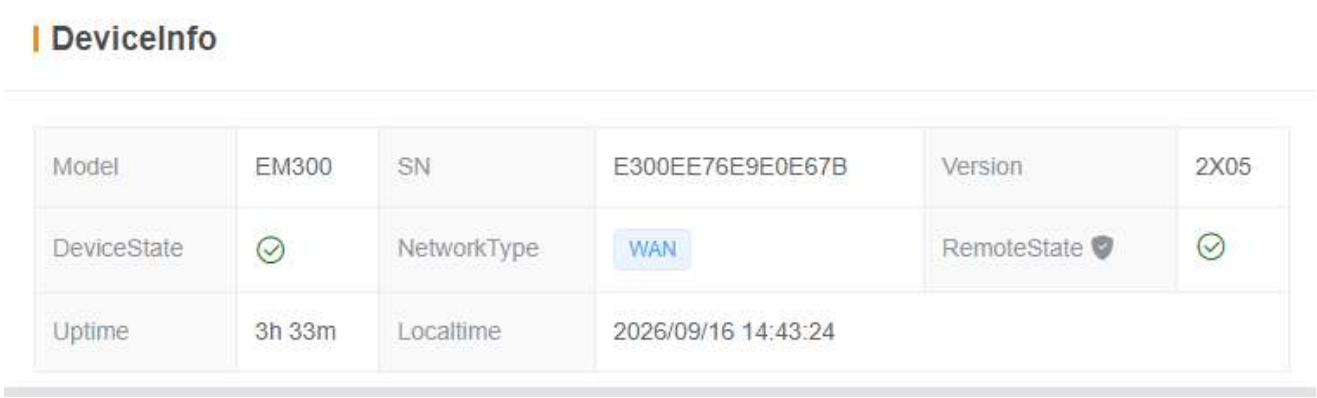


2.2 Home Page

The Home page displays basic device information, network information, system load, and external disk management.



Device Information

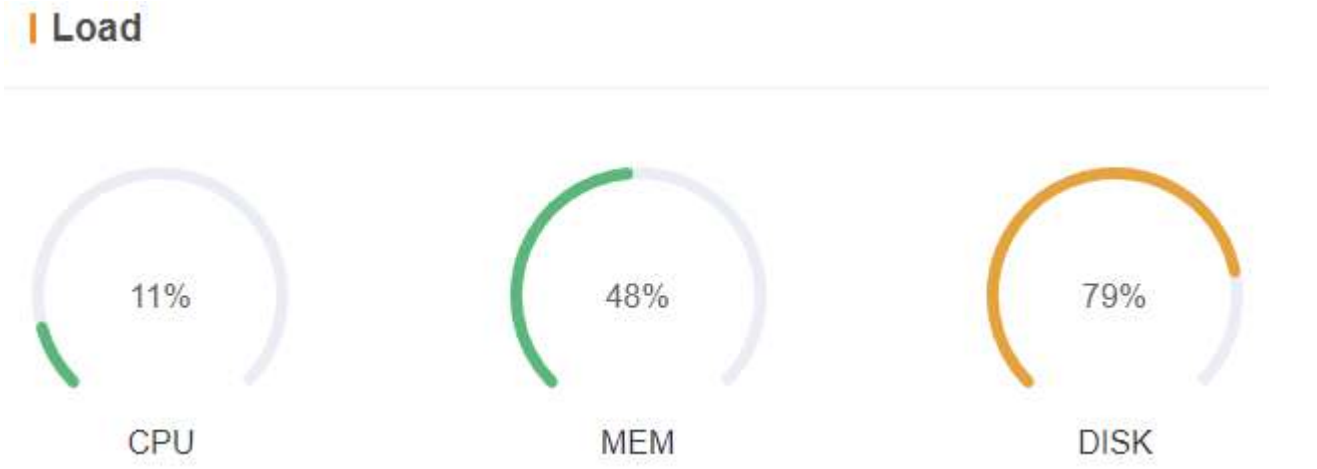


- Model: exact gateway model.
- SN: globally unique serial number, normally used as the device identifier.
- Firmware Version: currently installed version.
- Device Status: current operating status.
- Network Type: current uplink method (Unknown means no active WAN, cellular, or Wi-Fi connection)
- Remote Status: √ means remote connected, / means disconnected.
- Uptime: time since the gateway was powered on.
- Local Time: current device time.

Network Information

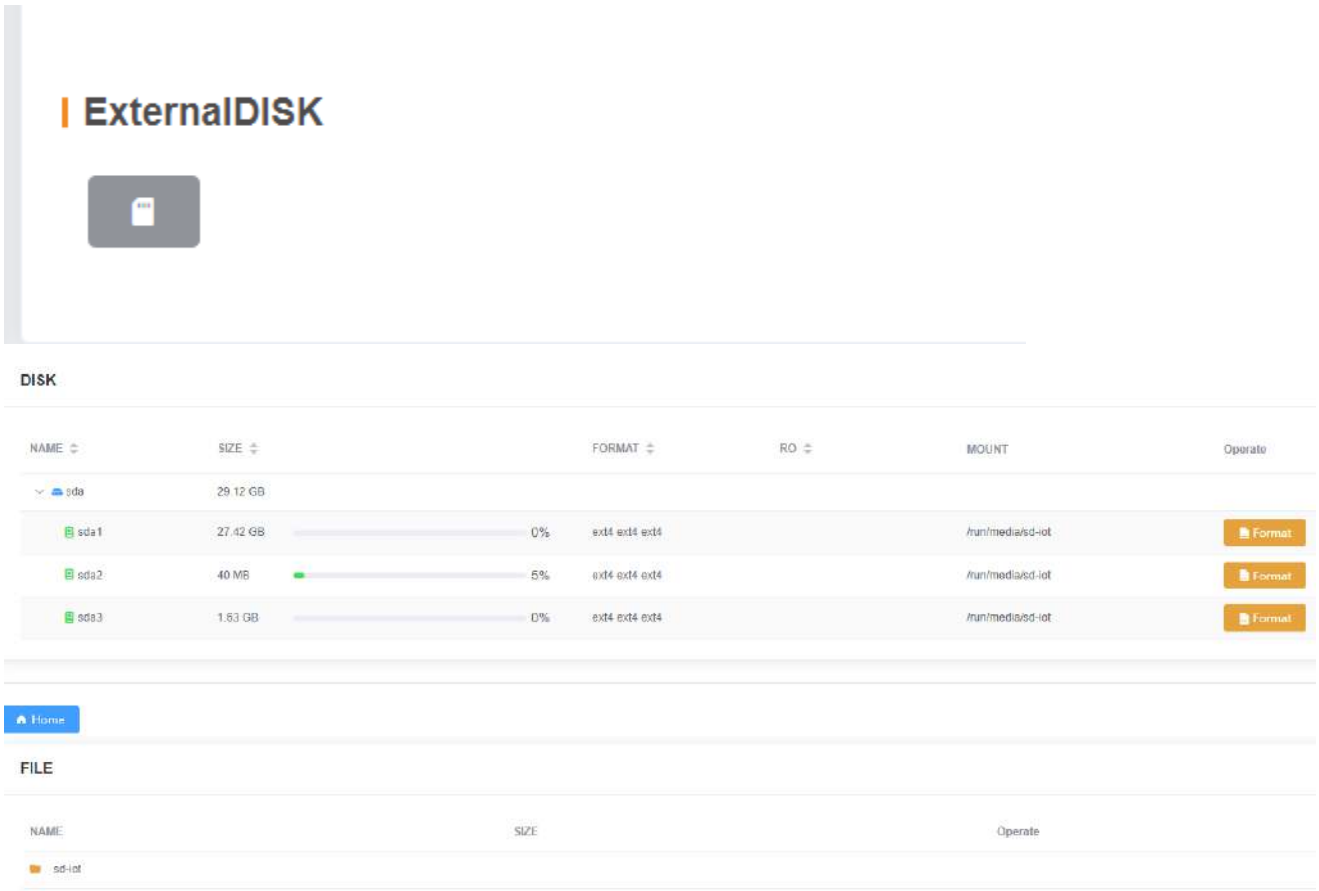
- LAN: link icon, IP address, subnet mask, MAC address, and DHCP status.
- WAN: link icon, IP address, subnet mask, gateway address, and MAC address.
- Cellular 4G or 5G: signal level, current IP address, module IMEI, SIM card number, and network type.
- Wi-Fi AP: number of clients, AP enable status, and hotspot name.
- Wi-Fi STA: connection icon, STA enable status, and connected hotspot name.

Device Load



Displays CPU utilization, memory utilization, and disk utilization as percentages.

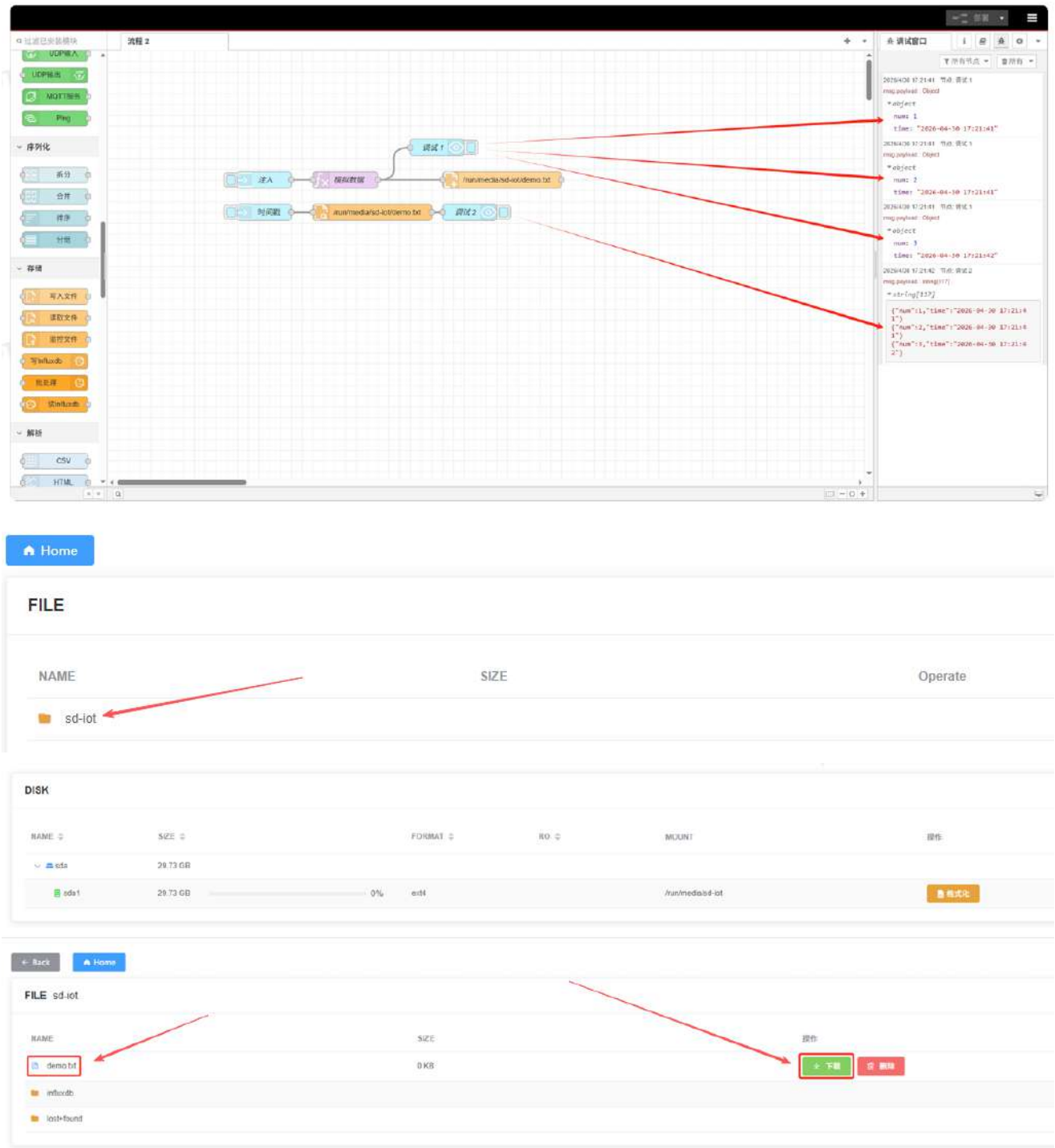
External Disk



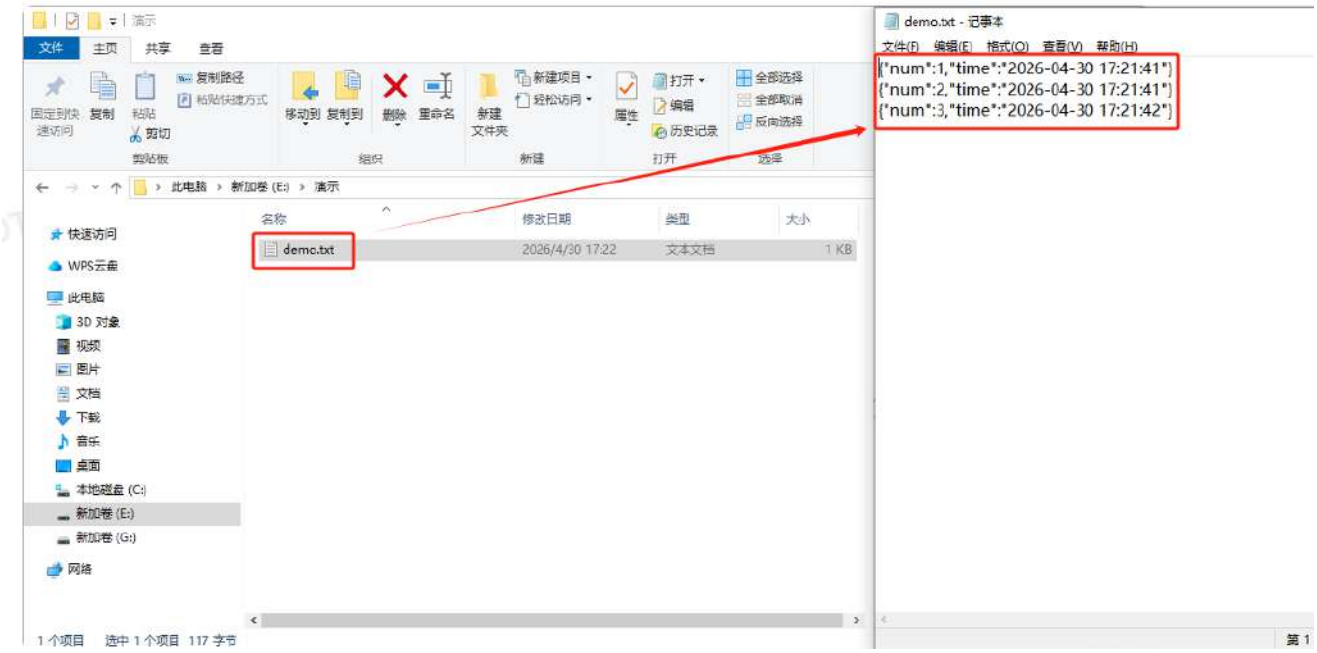
Displays external storage capacity, partitions, and files. Formatting and file download are supported. This function is commonly used for log management with a TF card or USB storage device.

Step 1: Configure the "Write File" node in the visual programming environment based on the mount path of the external storage device (e.g., /run/media/sd-iot). By specifying the target path and filename (e.g., demo), collected data can be written directly to the `demo` file, enabling automatic file creation and data storage.

Step 2: Enter the mount directory (e.g., sd-iot), locate the target file, and click Download to export the stored data file to your local system.

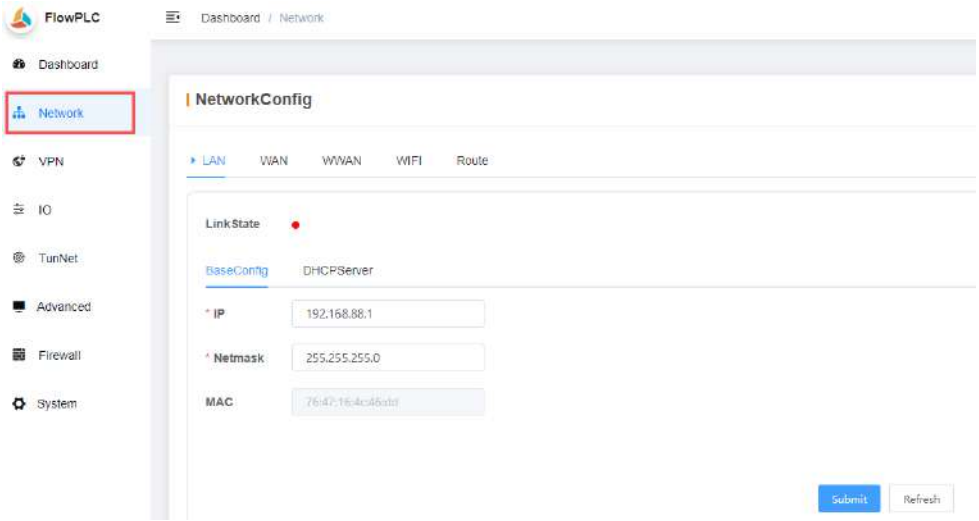


Step 3: Open the downloaded file locally to view it.



3 Network

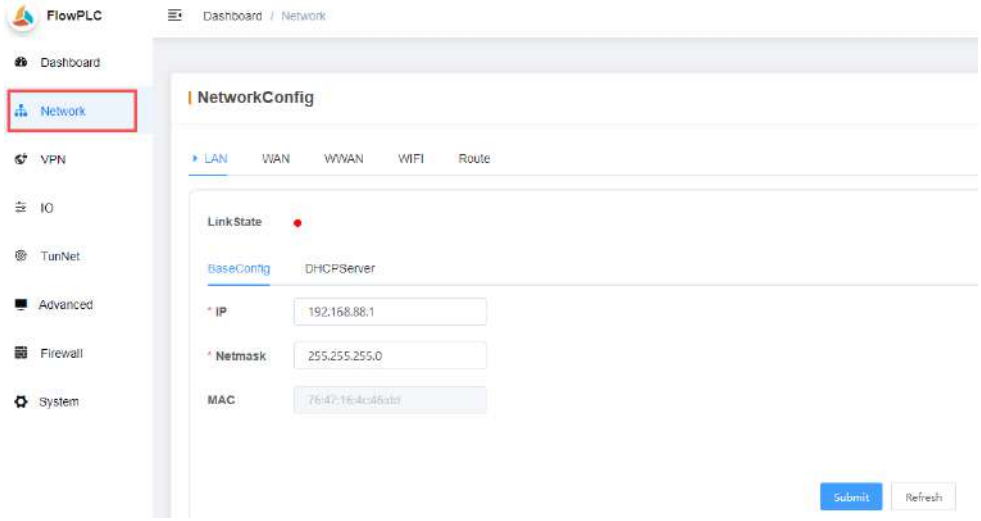
Use this section to configure network parameters.



Note Available connection methods depend on the product model.

3.1 LAN

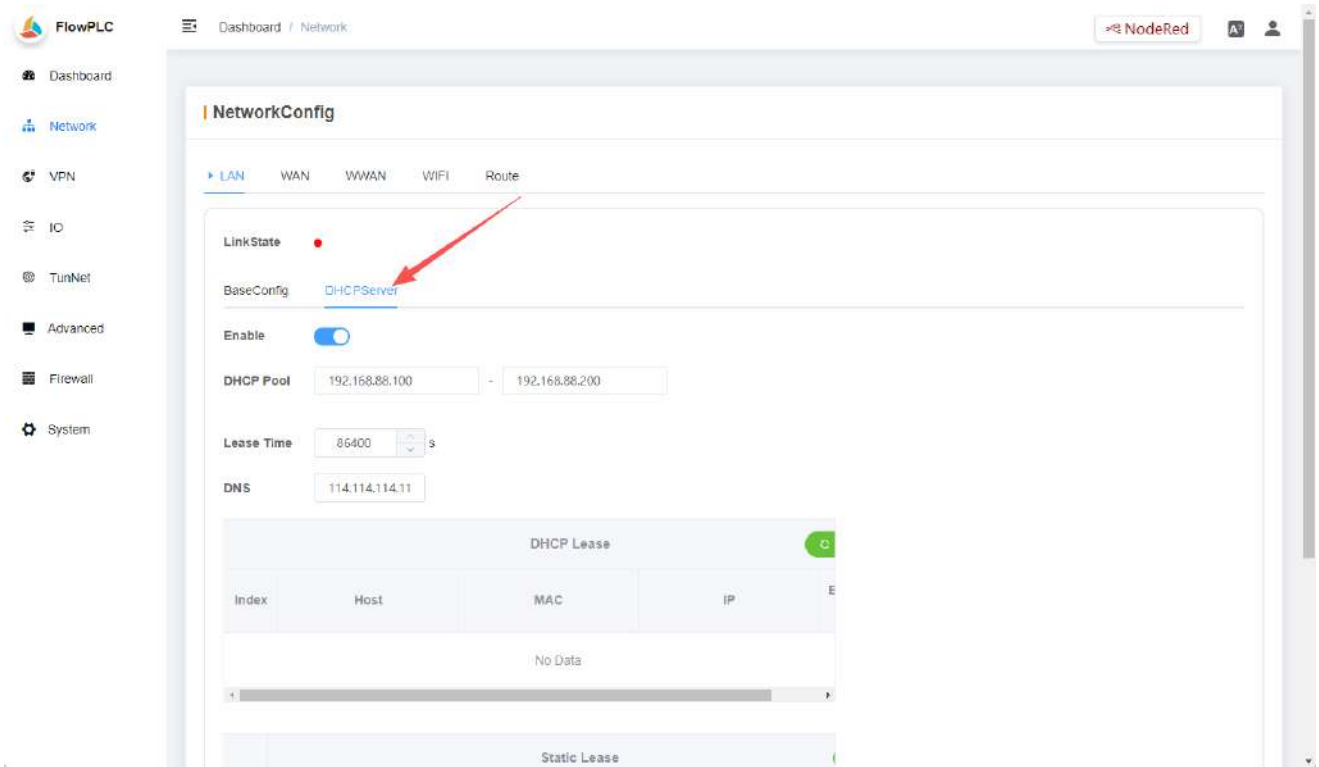
Basic Configuration



- Connection Status: LAN link state; green indicates connected and red indicates disconnected.
- IP: default 192.168.88.1; editable after login.
- Subnet Mask: default 255.255.255.0.
- MAC: LAN port MAC address.

DHCP Server

The Wi-Fi AP and LAN share one DHCP pool.

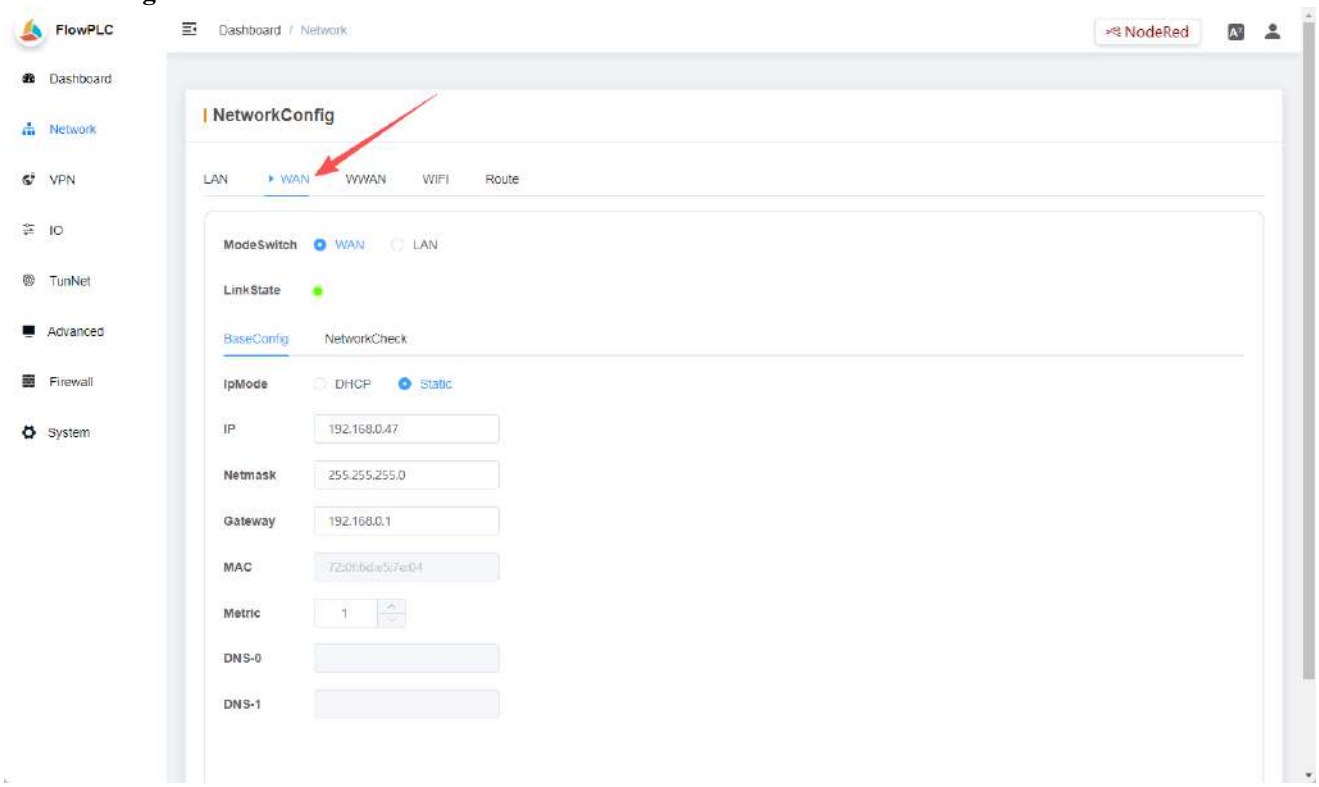


- Enable: enabled by default.
- DHCP Pool: client address range automatically assigned by the gateway; default 192.168.88.100-200.
- Lease Time: validity period of an assigned address; default 86400 seconds.
- DNS: resolver address assigned to clients; default 114.114.114.114.
- DHCP Leases: list of devices that have obtained addresses; refresh is supported.
- Static Lease: assigns a fixed IP address to a specified MAC address, independent of the pool range.

Note After changing settings, click Submit and restart the gateway for the changes to take effect.

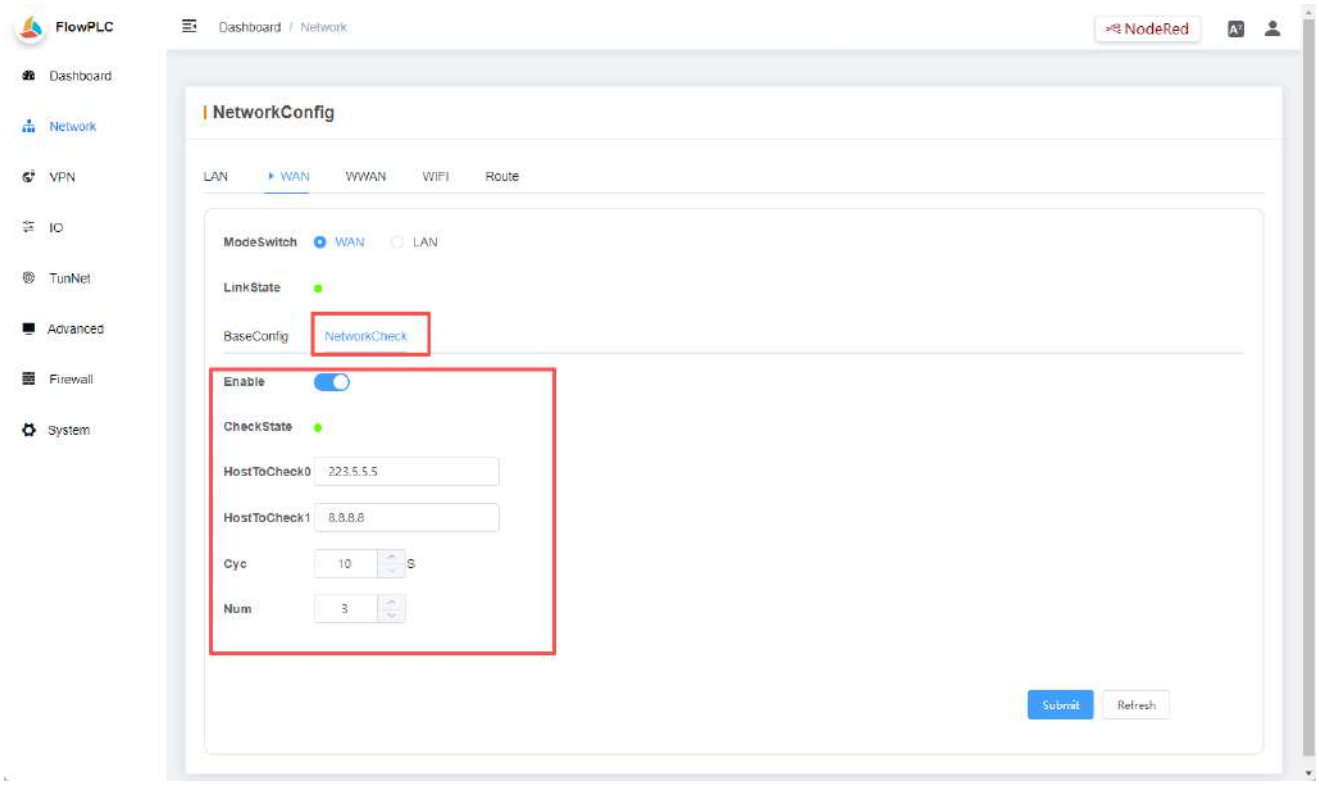
3.2 WAN

Basic Configuration



- Mode: WAN by default; can be switched to LAN mode.
- Connection Status: green when connected and red when disconnected.
- IP Mode: DHCP by default.
- IP, Subnet Mask, and Gateway: obtained automatically in DHCP mode or entered manually in Static mode.
- MAC: WAN port MAC address.
- Metric: route priority; a lower value has higher priority. The default order is WAN, Wi-Fi, then cellular.
- DNS-0 and DNS-1: DNS addresses assigned by the upstream router.

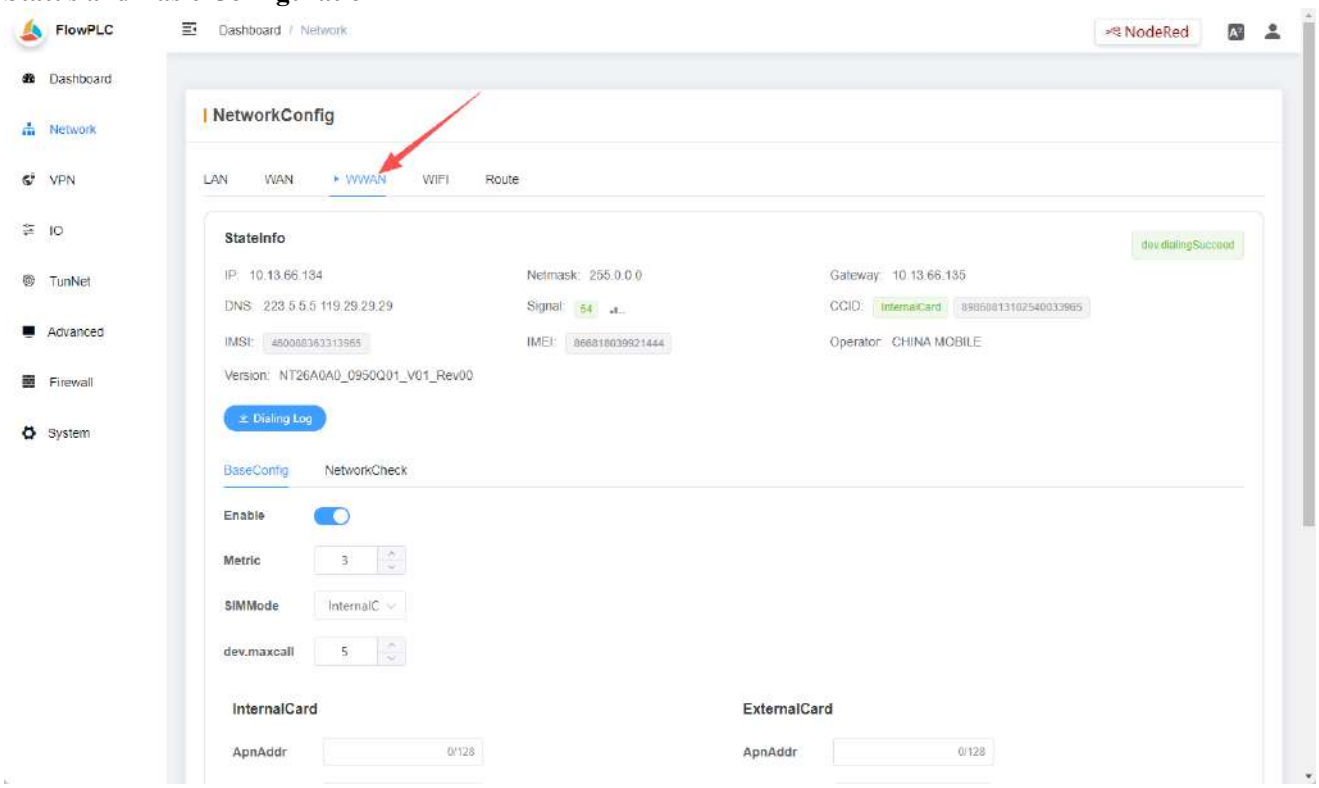
Network Detection



- Enable: turns on WAN connectivity detection.
- Detection Status: green indicates normal operation.
- Detection Host 0 and 1: target IP addresses; defaults are 223.5.5.5 and 8.8.8.8.
- Interval: test interval in seconds; default 10 seconds.
- Failure Count: consecutive failure threshold. When reached, the interface metric is increased.

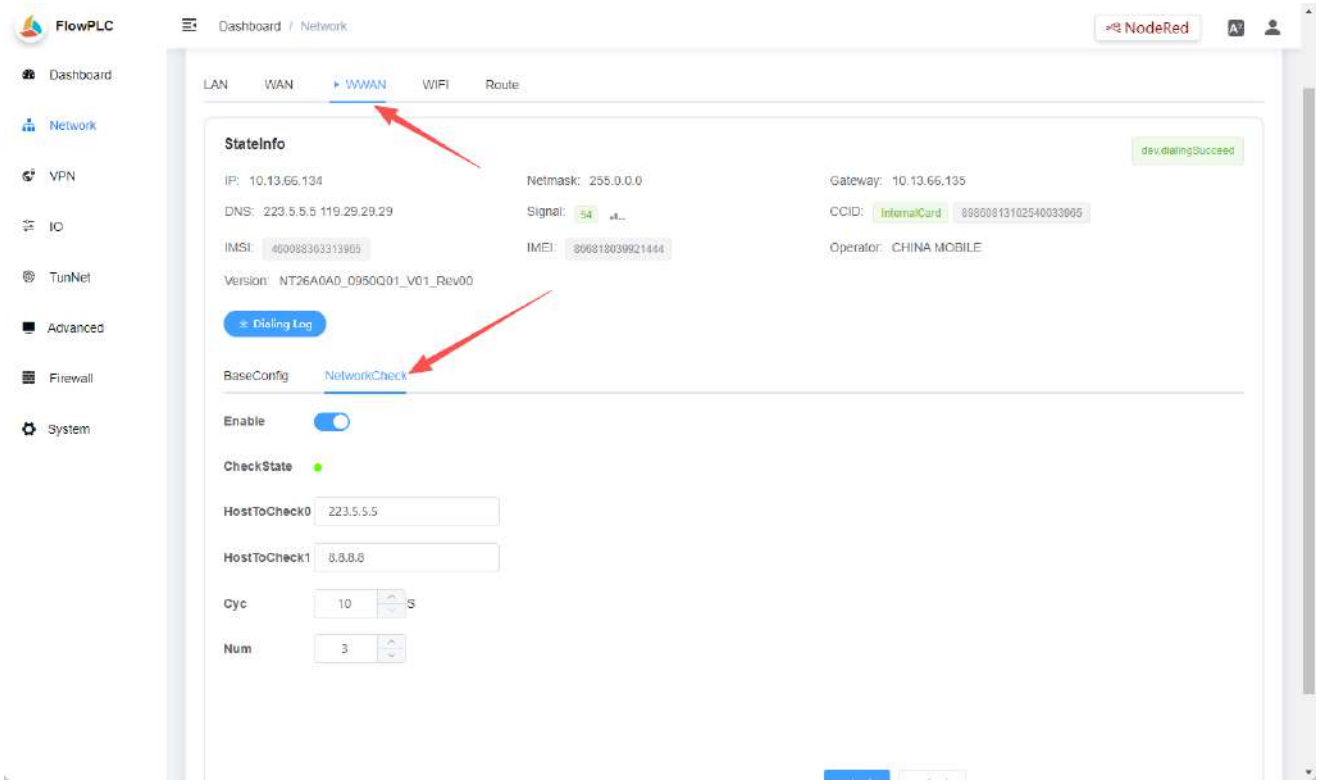
3.3 Cellular

Status and Basic Configuration



- IP, Subnet Mask, Gateway, and DNS: current cellular network parameters.
- Signal: current strength from 0 to 100; a higher value indicates a stronger signal and maps linearly to the module value 0-31.
- SIM Number: active SIM card number.
- IMEI: cellular module identifier.
- Operator: registered carrier, for example CHINA MOBILE.
- Firmware Version: cellular module firmware.
- Dial Log: downloads the most recent module dial-up log for troubleshooting.
- Manual Redial: immediately starts a new dial-up attempt.
- Enable: turns cellular dialing on or off.
- Metric: route priority; lower values have higher priority.
- SIM Mode: preferred SIM type and failover strategy.
- Maximum Dial Attempts: retry threshold; the module restarts after the threshold is reached.
- Internal or External SIM APN: APN parameters for the selected SIM.

Network Detection



Enable: Activates the network probing function to monitor cellular network connectivity.

Probe Status: Displays the current status of the probing task; green indicates normal operation.

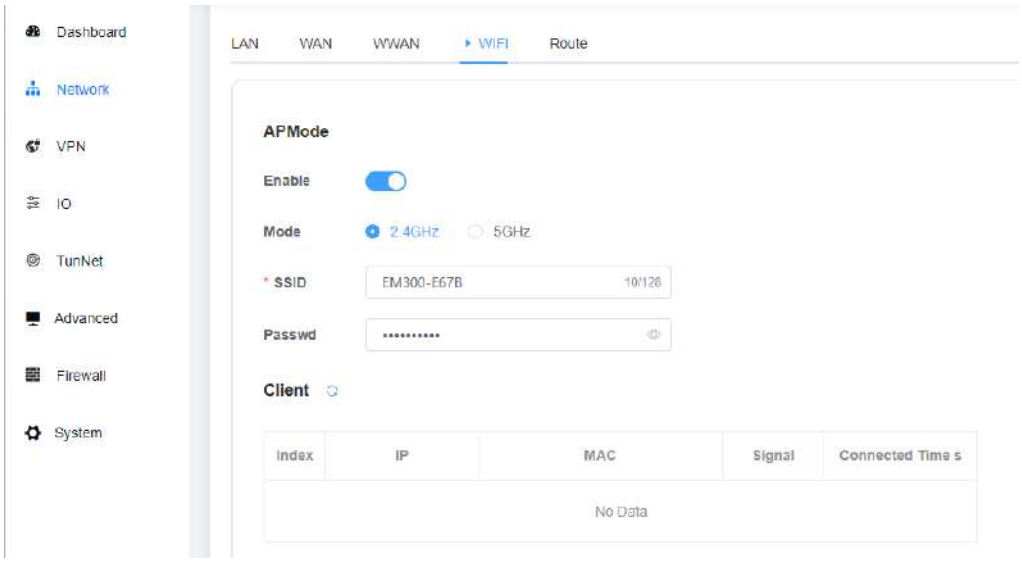
Probe Host 0/1: Sets the target IP addresses for probing; defaults are 223.5.5.5 and 8.8.8.8.

Interval: The time interval between probe attempts (in seconds); default is 10 seconds.

Count: The threshold for consecutive probe failures; upon reaching this limit, the interface metric is increased, and a redial is attempted.

After Settings are complete. Click Submit and restart to take effect.

3.4 Wi-Fi



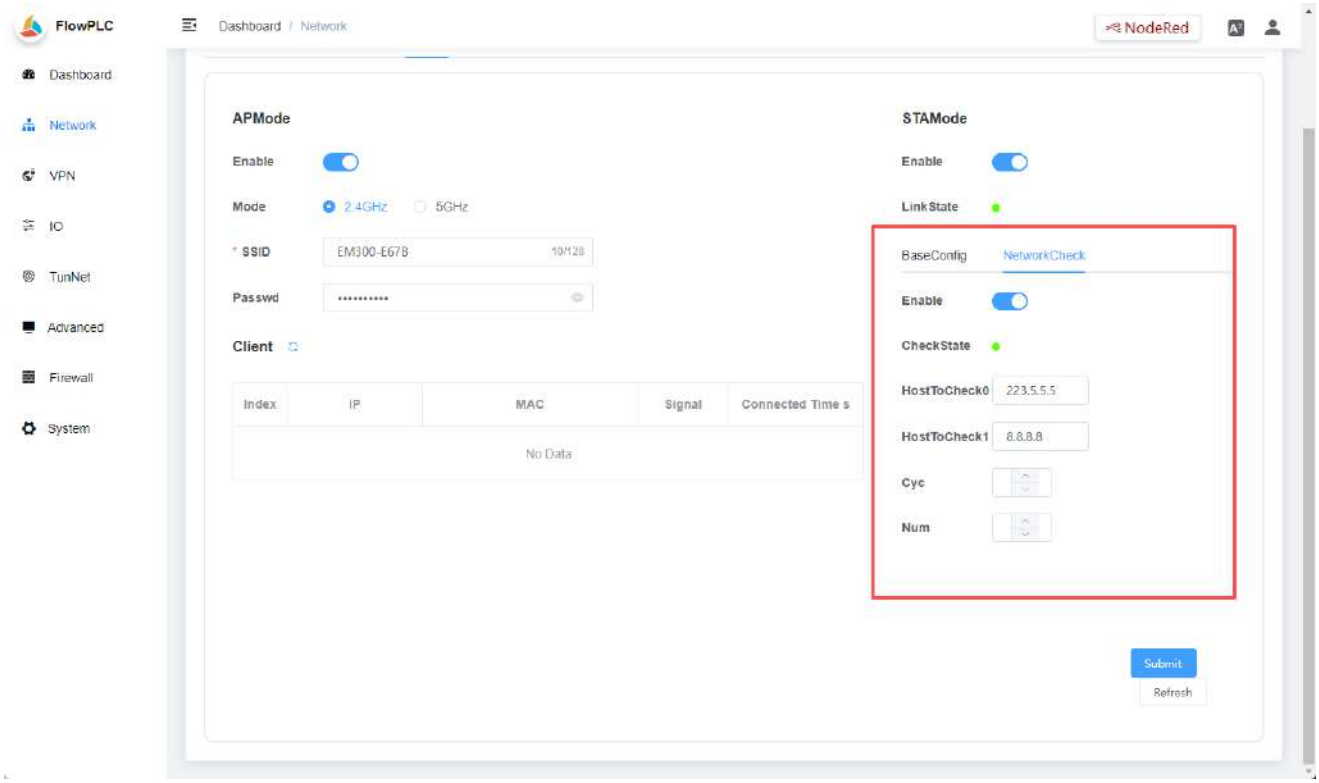
AP Mode

- Enable: provides a hotspot for other Wi-Fi devices.
- SSID: default is the device model plus the last four digits of the SN; up to 32 letters, numbers, or symbols.
- Password: default EM12345678.
- Clients: information about connected devices.

STA Mode

- Enable: connects the gateway to an on-site Wi-Fi network.
- Connection Status: connection to the external Wi-Fi network.
- SSID and Password: select by automatic scan or enter manually.
- IP Mode: DHCP by default; Static configuration is also supported.
- IP, Subnet Mask, and Gateway: automatic in DHCP mode or manual in Static mode.
- MAC: STA interface MAC address.
- Metric: route priority; lower values have higher priority.
- DNS-0 and DNS-1: DNS addresses assigned by the upstream router.

Network Detection



Enable: Activates the network probing function to monitor cellular network connectivity.

Probe Status: Displays the current status of the probing task; green indicates normal operation.

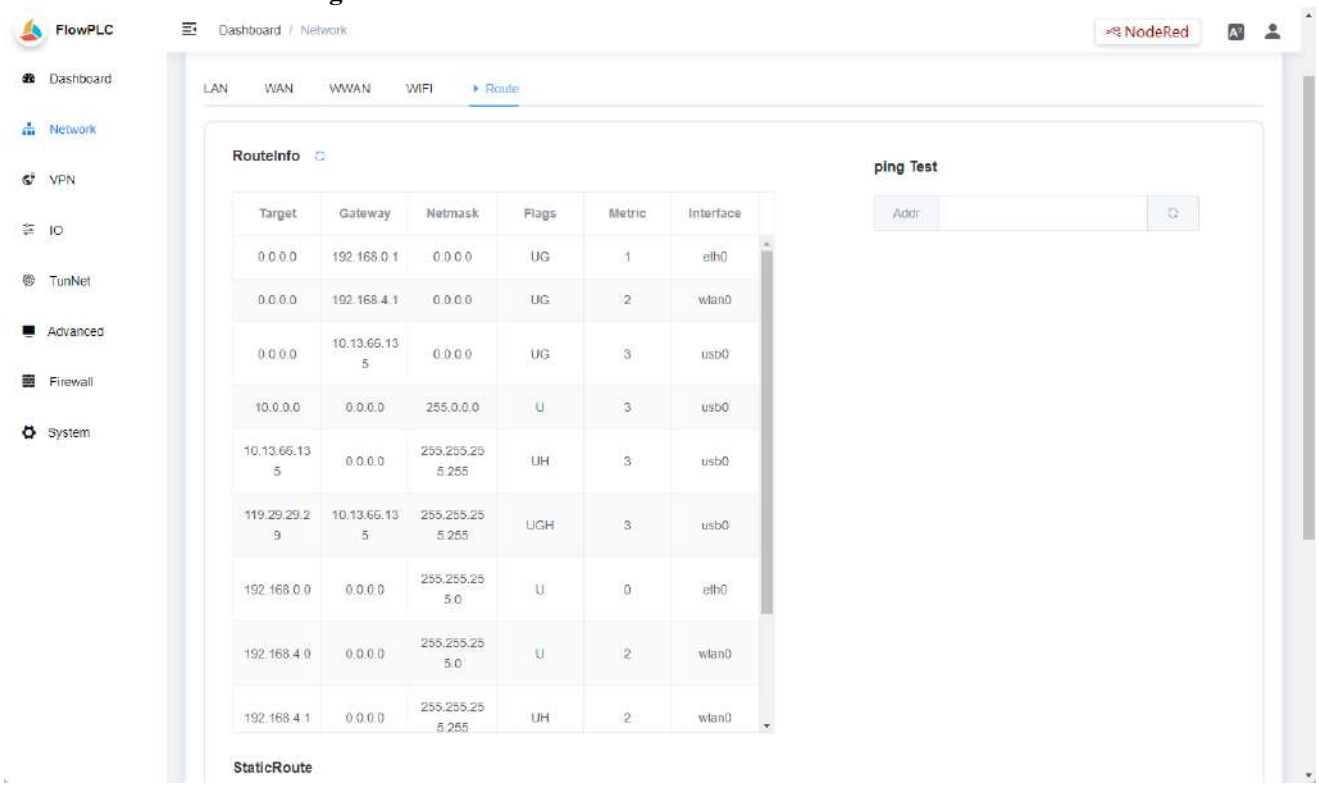
Probe Host 0/1: Sets the target IP addresses for probing; defaults are 223.5.5.5 and 8.8.8.8.

Interval: The time interval between probe attempts (in seconds); default is 10 seconds.

Count: The threshold for consecutive probe failures; upon reaching this limit, the interface metric is increased, and a redial is attempted.

3.5 Routing

Route Information and Ping Test



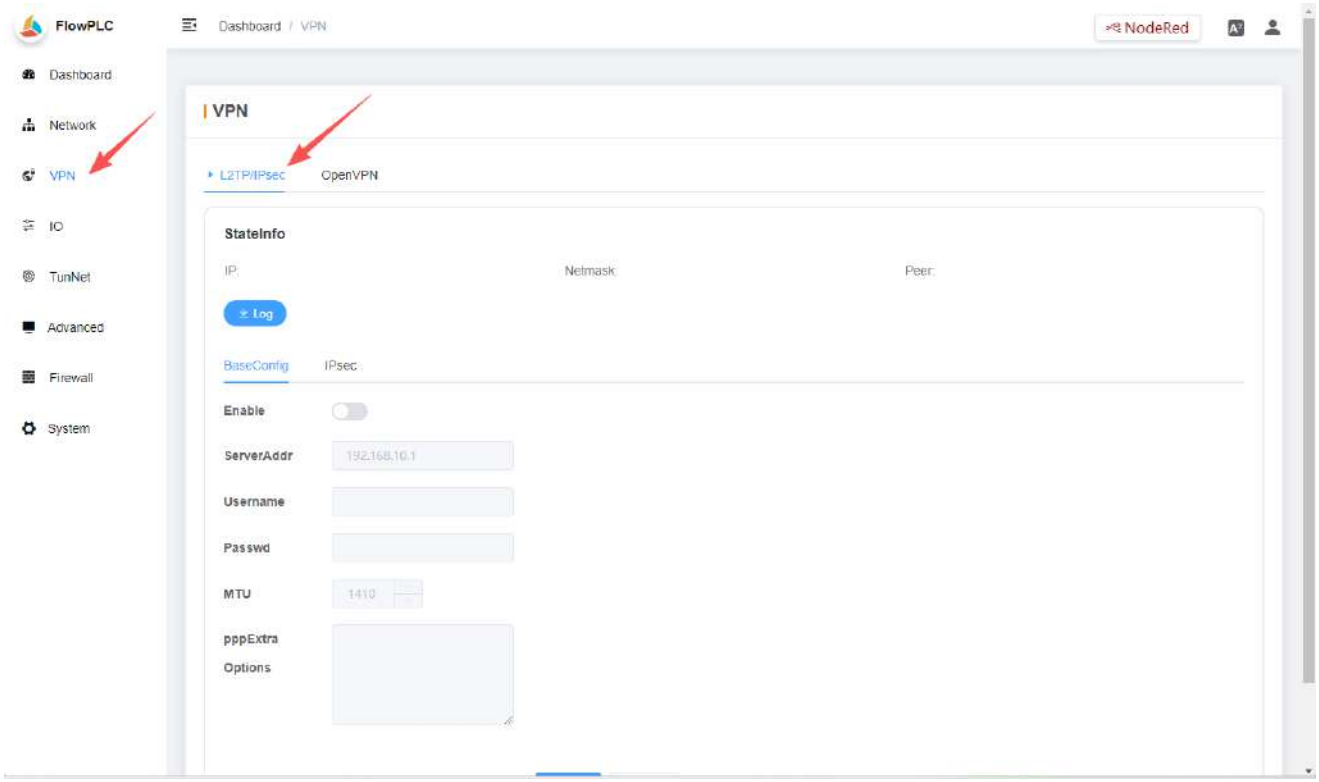
Route Information displays the current routing table, including destination network, gateway, subnet mask, metric, and interface. Enter a target address in Ping Test to check network reachability.

Static Route

A static route defines the exact path used to reach a specific host or network. It is mainly used for communication across subnets or when traffic must pass through a specified gateway.

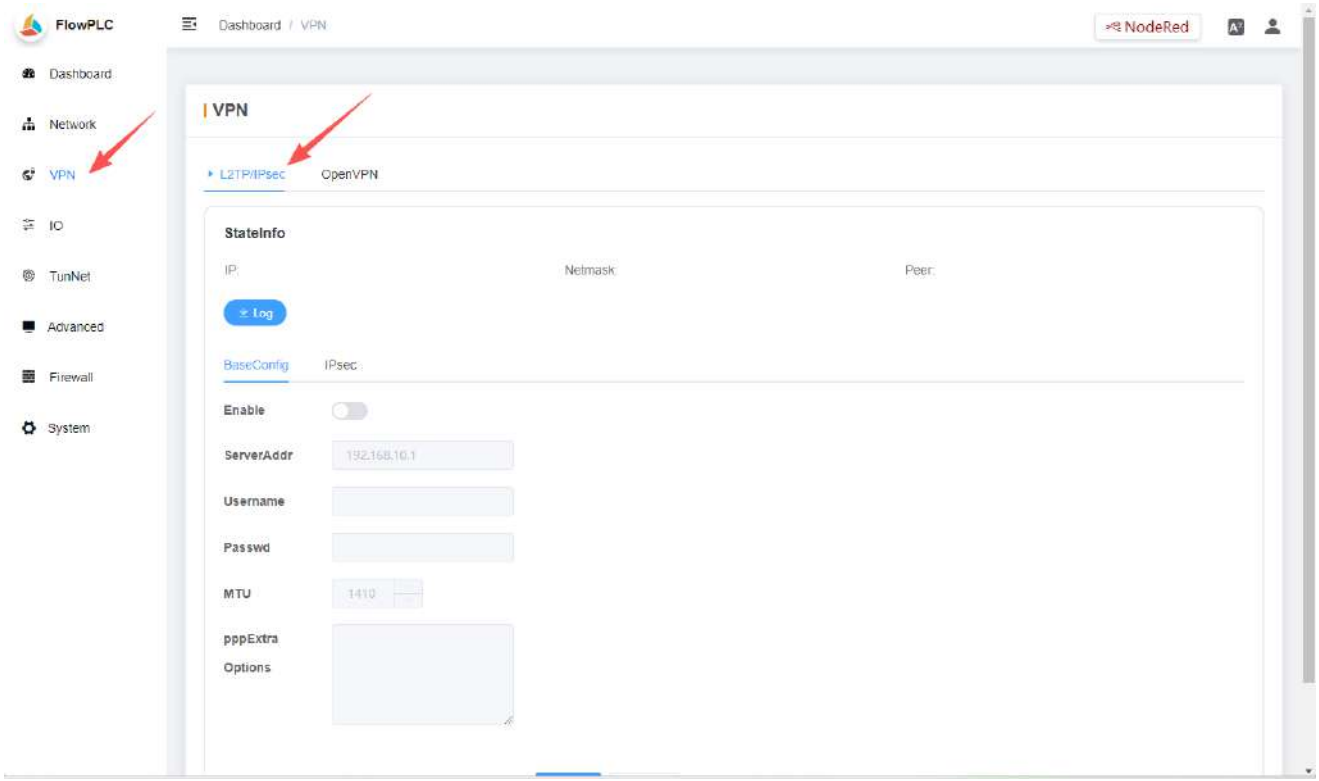
- Destination IP: target host address or target network.
- Subnet Mask: use 255.255.255.255 for one host or 255.255.255.0 for a typical /24 subnet.
- Gateway: address of the router that forwards the traffic.

4 VPN

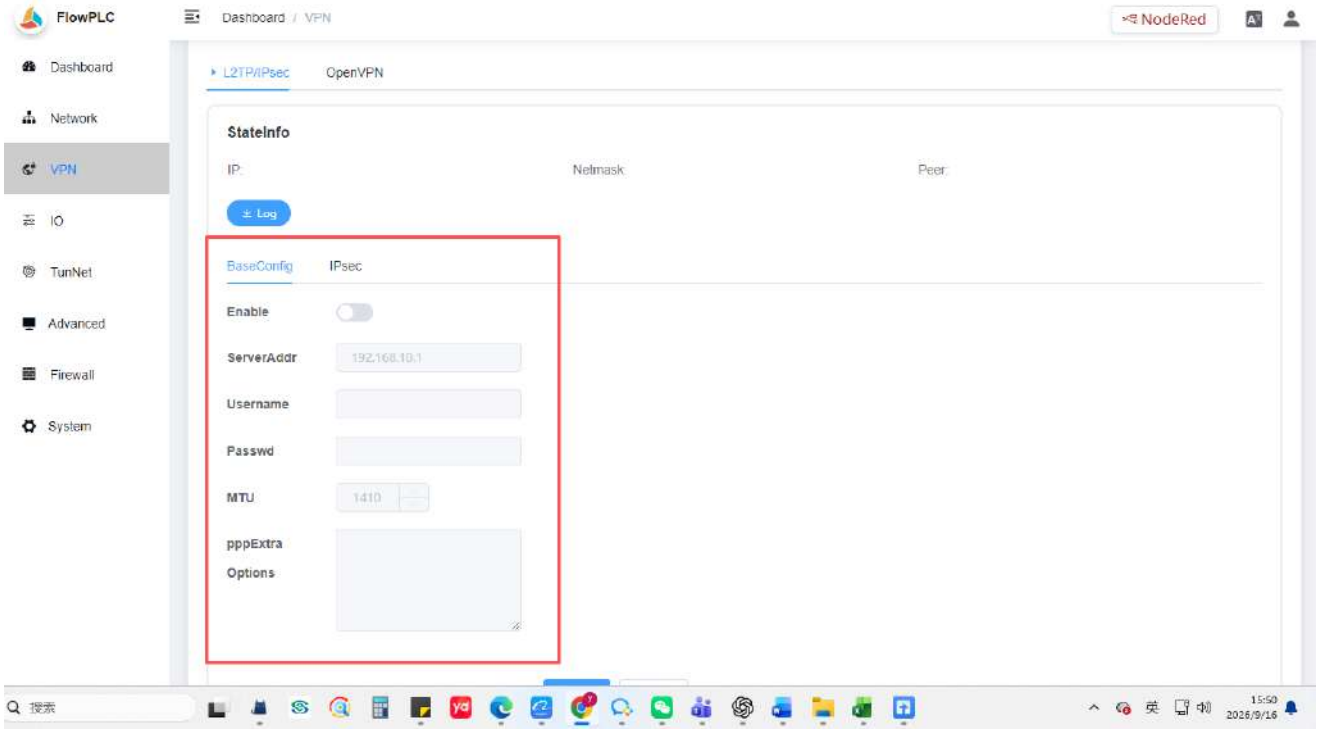


4.1 L2TP over IPsec

The gateway acts as an encrypted VPN client. L2TP establishes a UDP tunnel and IPsec encrypts the traffic, allowing secure access to a remote private network over the public Internet. After connection, the Status area shows the assigned VPN IP address, subnet mask, and peer server address. Connection logs can be downloaded.

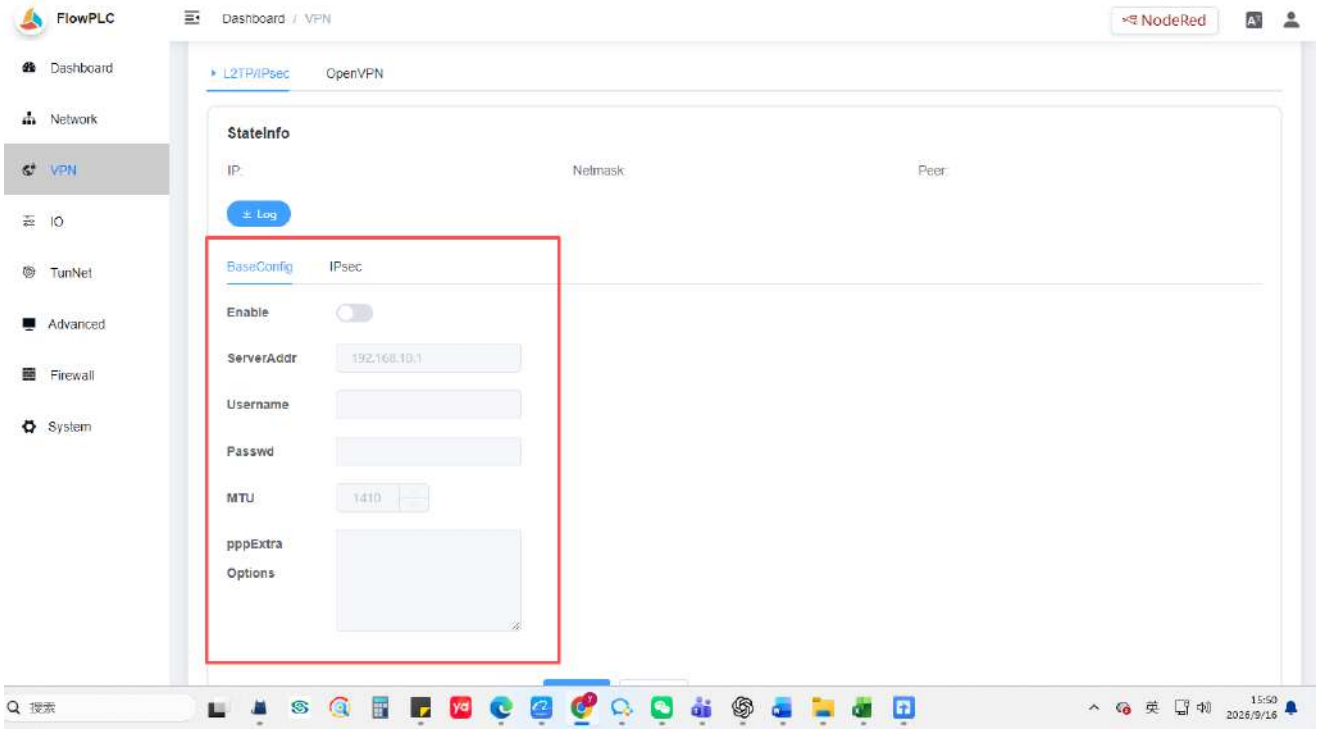


Basic Configuration



- Enable: enables or disables the L2TP VPN client.
- Server Address: public IP address or domain name of the L2TP server.
- Username and Password: VPN credentials.
- MTU: maximum transmission unit; default 1410.
- Additional PPP Options: extended PPP parameters.

IPsec Configuration

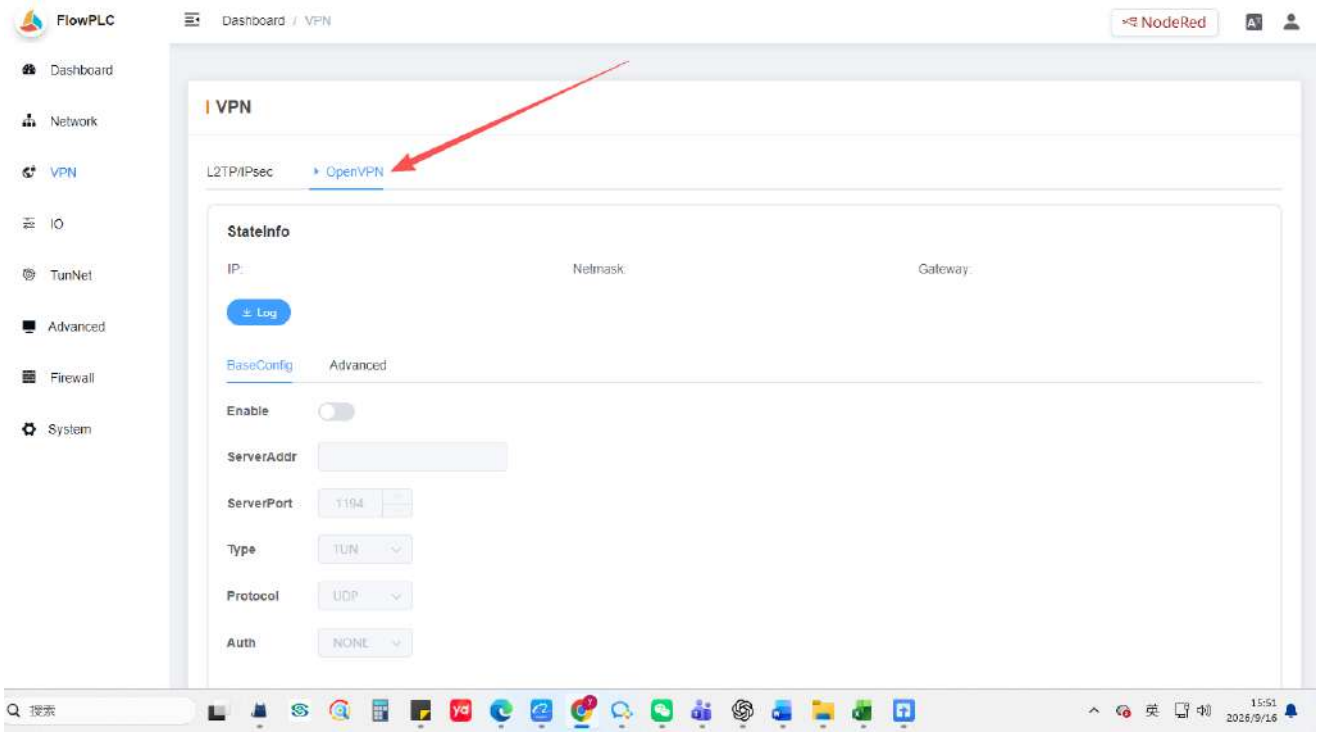


- Enable: enables IPsec encryption; use together with L2TP.
- Connection Status: current VPN state.
- IKE Version: ikev1 by default.
- IKE Encryption: aes128 by default.
- IKE Authentication: sha1 by default.
- IKE DH Group: modp1024 by default.
- ESP Encryption: aes128 by default.

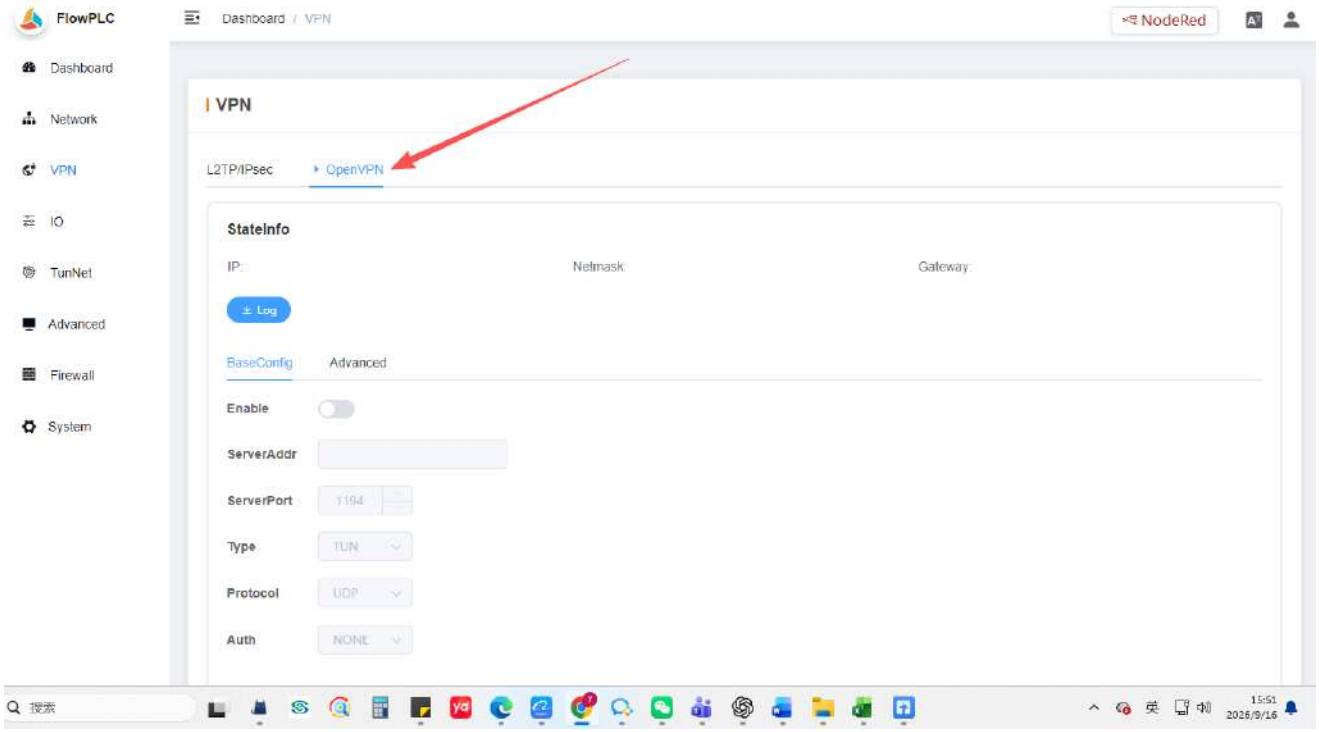
- ESP Authentication: sha1 by default.
- Pre-shared Key: must exactly match the server setting.
- Additional Options: extended IPsec parameters, such as NAT traversal.

4.2 OpenVPN

OpenVPN creates an encrypted virtual private network tunnel for secure remote access, data protection, unified device management, and cross-region network connectivity. After connection, the Status area shows the virtual IP address, subnet mask, and tunnel gateway assigned by the server. Connection logs can be downloaded.



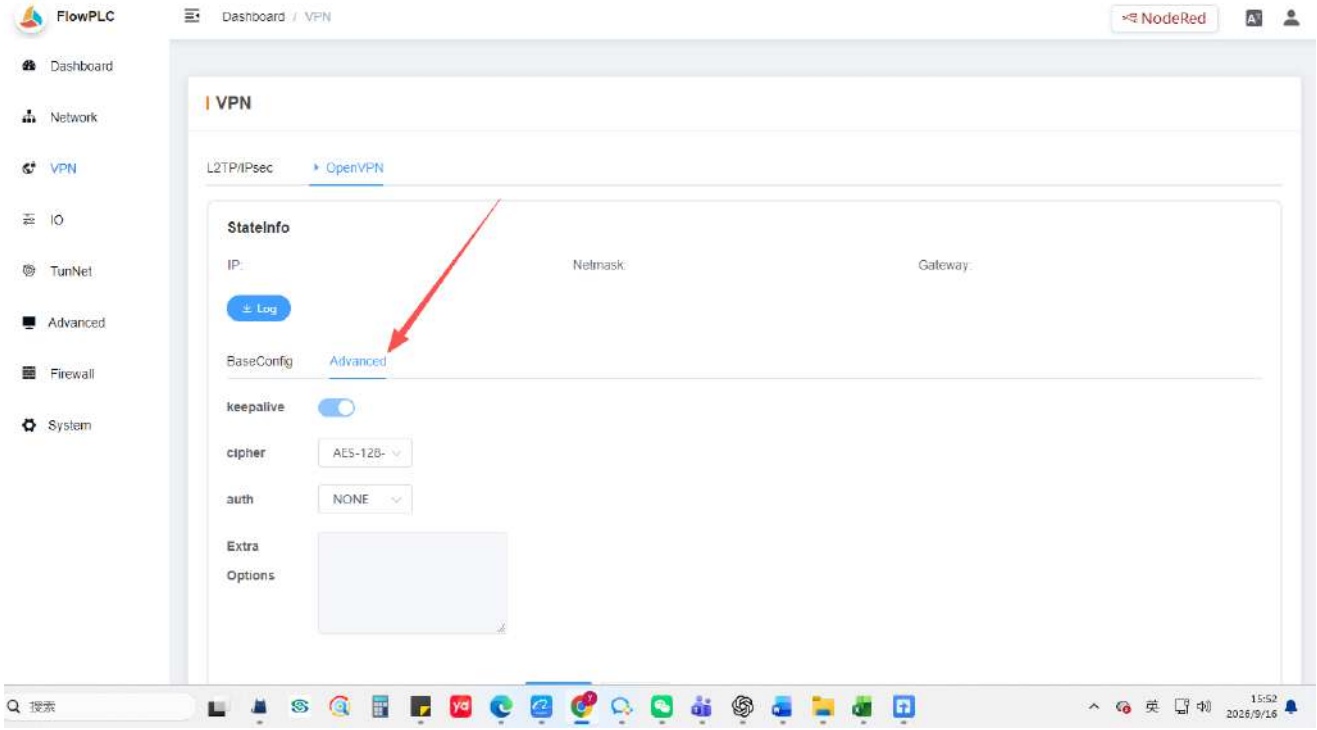
Basic Configuration



- Enable: enables or disables the OpenVPN client.
- Server Address: public IP address or domain name.
- Server Port: 1194 by default; must match the server.
- Type: TUN for Layer 3 routing, commonly used in industrial deployments, or TAP for Layer 2 bridging.
- Protocol: UDP for lower latency or TCP for reliable delivery.

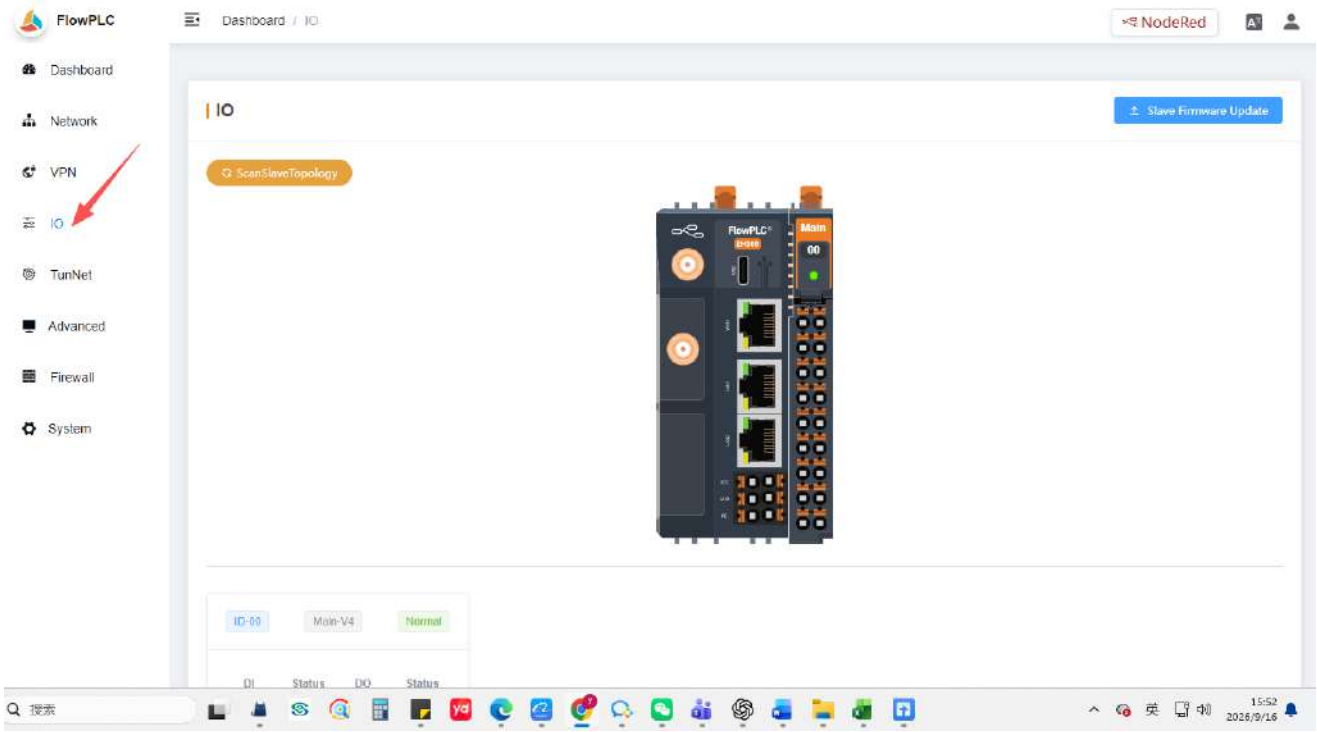
- Authentication: NONE, SSL, User/Password, or another supported mode.

Advanced Configuration



- keepalive: tunnel keepalive mechanism.
- cipher: data encryption algorithm; AES-128-GCM by default.
- auth: data-integrity authentication algorithm; NONE by default.
- Additional Options: custom OpenVPN configuration parameters.

5 IO



Scan Slave Topology: Rescan the slave topology architecture.

Module Display: The upper section of the page displays a schematic of the device and its cascaded expansion modules, providing a visual overview of all currently connected I/O modules.

Module ID: The lower section lists information for each subsequent module, organized by Module ID (e.g., ID-00, ID-01) according to the cascade sequence.

DI (Digital Input) Status:

Displays the real-time status of each input channel:

Gray: Not triggered / Low level

Green: Triggered / High level

DO (Digital Output) Control

Displays and allows control of the status of each output channel:

Gray switch: Output off

Blue switch: Output on

Supports direct clicking of the switch to control the on/off state of the DO channel.

AI (Analog Input) Status

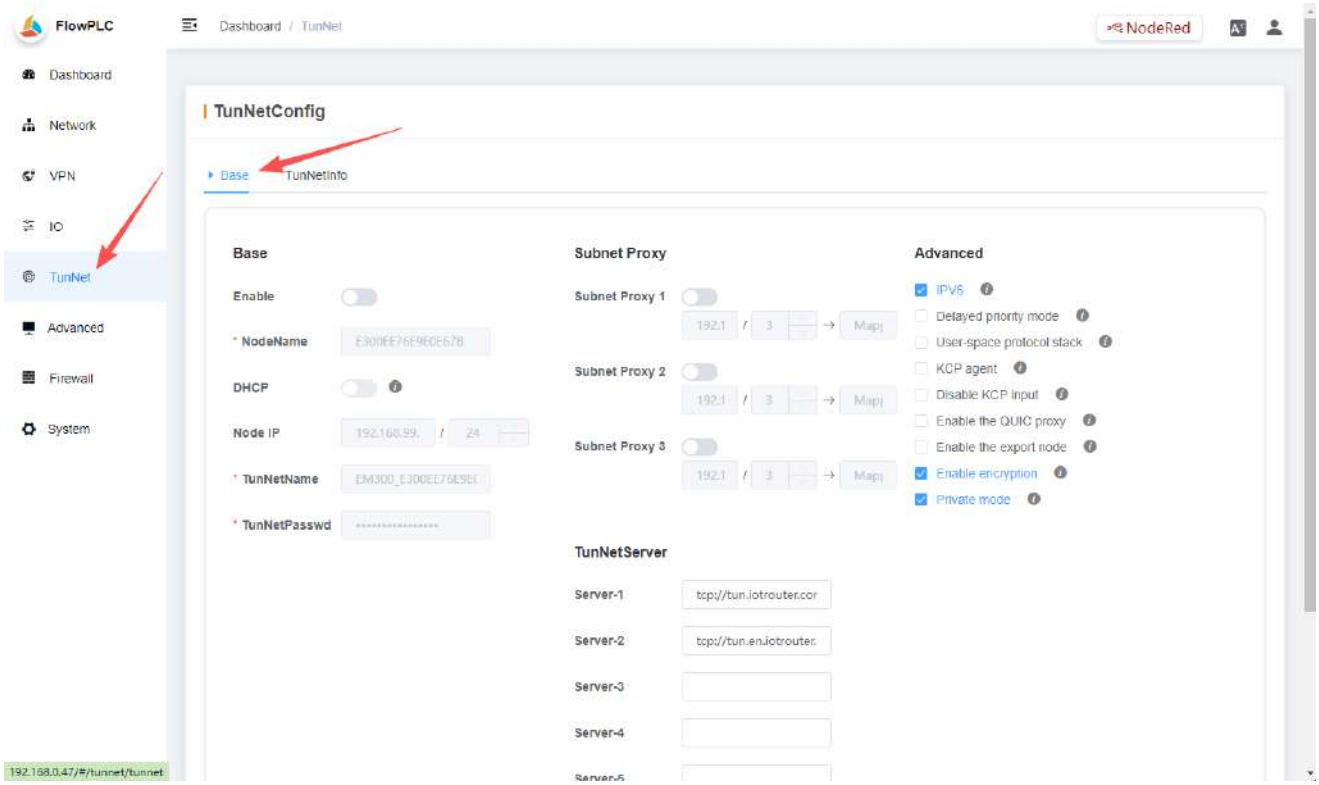
Displays the status of each input channel:

AO (Analog Output) Control

Displays and allows control of the status of each output channel

6 Virtual Networking

Use this section to configure virtual networking. For the detailed feature guide, see:
https://iotrouter.yuque.com/zn3vdn/bk/cgpmguz63va2lnvc?view=doc_embed



6.1 Basic Settings

- Enable: turns virtual networking on or off.
- Node Name: identifies the device; each node name must be unique in the same network.
- DHCP: automatically assigns a virtual IP address. A static virtual IP address is recommended.
- Node IP: gateway virtual IP address.
- Network Name: custom name shared by all nodes in the same network; 6-127 characters.
- Network Password: custom password shared by all nodes in the same network; 6-127 characters.

Subnet Proxy

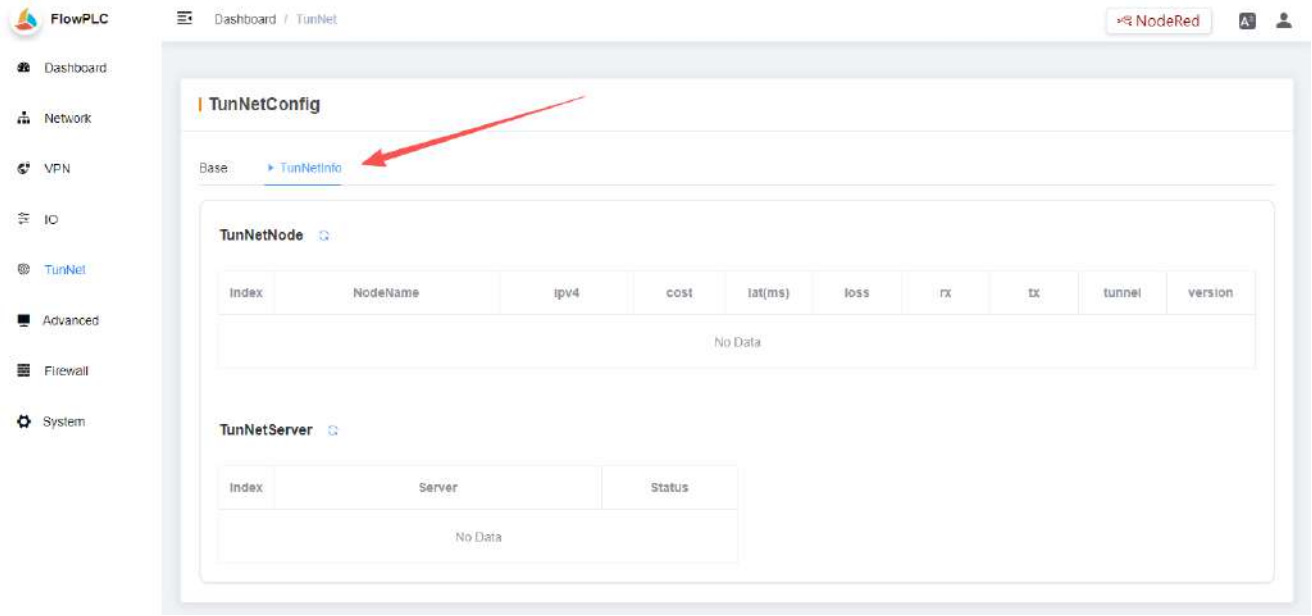
Subnet proxy allows remote access to devices on the LAN connected to this gateway. Up to three proxy rules are supported.

- Single device example: to access 192.168.0.55, configure 192.168.0.55/32 and leave Mapped IP blank.
- Entire subnet example: to access 192.168.0.x, configure 192.168.0.0/24 and leave Mapped IP blank.

Networking Servers and Advanced Options

- Networking Server: one or more server addresses that the device can connect to.
- IPv6: when disabled, only IPv4 is used.
- Latency-first Mode: selects the path with the lowest total latency regardless of relay hops.
- User-space Network Stack: uses a user-space TCP/IP stack to avoid operating-system firewall issues affecting subnet or KCP proxying.
- KCP Proxy: converts TCP traffic to KCP to reduce latency and improve throughput.
- Disable KCP Input: blocks inbound KCP traffic; other KCP-enabled nodes still connect to this node over TCP.
- QUIC Proxy: converts TCP traffic to QUIC to reduce latency and improve throughput.
- Exit Node: allows this node to act as an exit node.
- Encryption: if disabled, the setting must match peer nodes.
- Private Mode: permits only nodes with a matching network name and password.

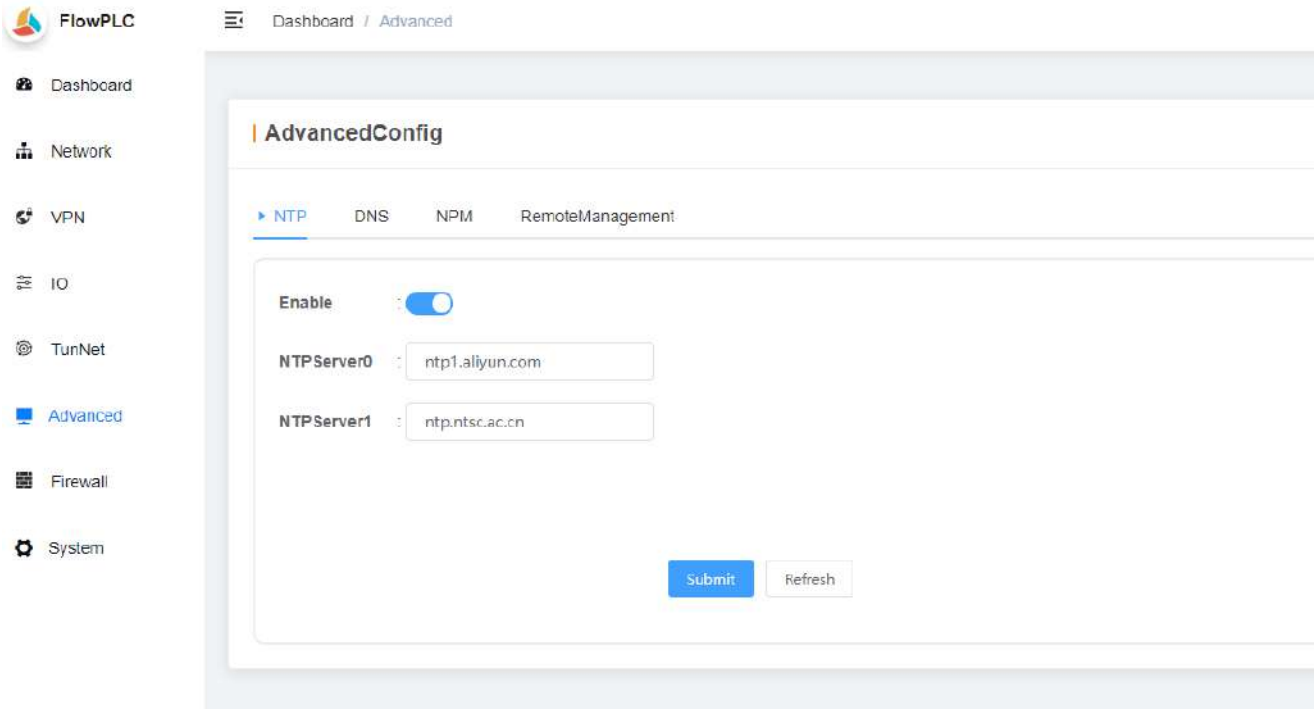
6.2 Network Information



- Network Nodes: names, virtual IP addresses, and other information for nodes in the current network.
- Networking Servers: connection status of the configured servers.

Virtual networking configuration reference

7 Advanced Settings



7.1 NTP

- Enable: enabled by default.
- NTP Server: time-server address. For a private network, change it to an accessible internal NTP server.

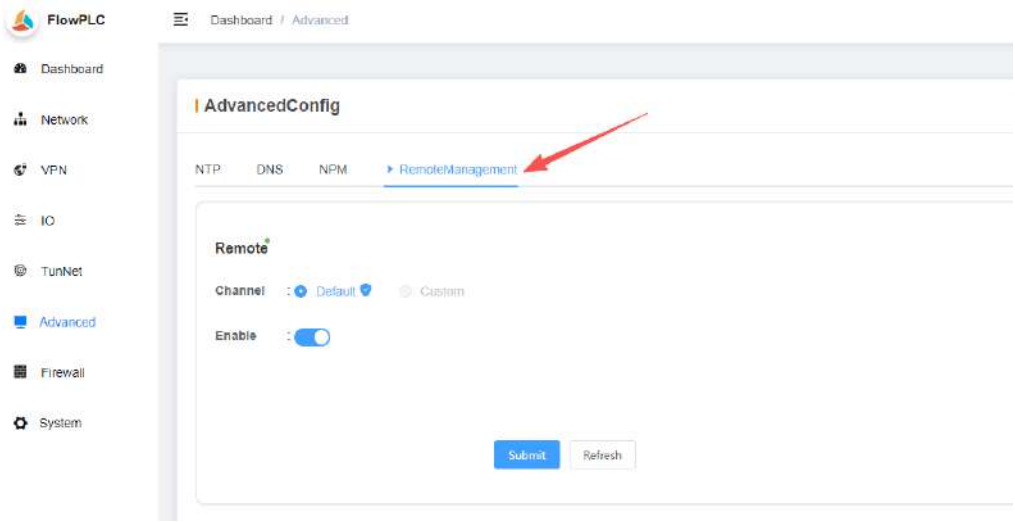
7.2 DNS

DNS affects domain-name resolution. Change the service configuration or DNS server address as required.

7.3 NPM

Sets the NPM registry used to install Node-RED nodes.

7.4 Remote Management

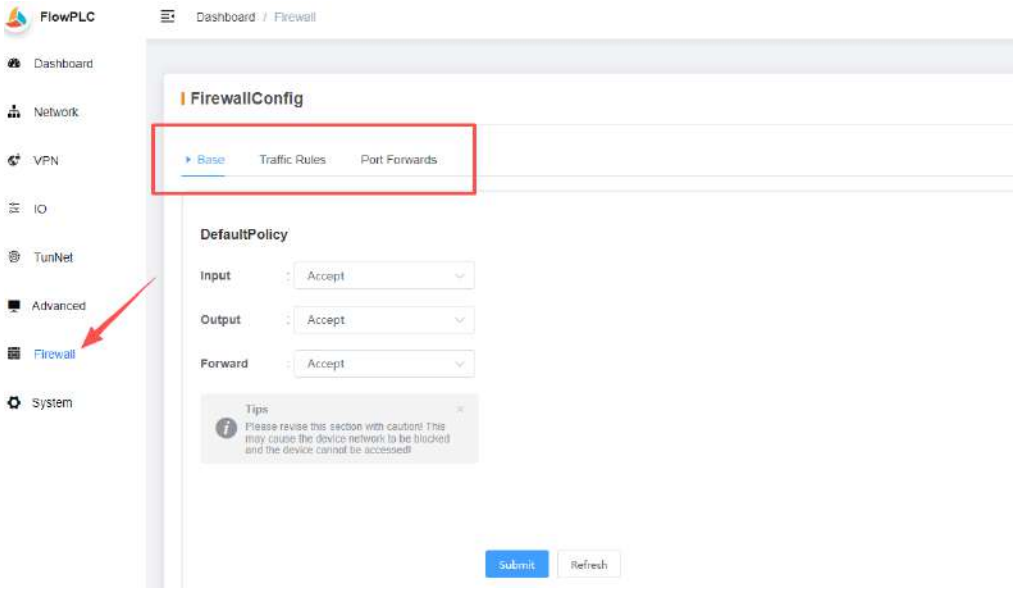


When enabled, the IOTRouter remote service can access and configure the gateway from another location. Disable it only when required. If disabled, remote configuration is unavailable.

Note After changing any setting in this section, click Submit and restart the gateway for the change to take effect.

Advanced settings reference

8 Firewall



Use this section to configure firewall rules and policies.

8.1 Basic Policies

- Input: default treatment of packets from external networks to the device. Accept permits packets not explicitly denied; Reject allows only packets that match an allow rule.
- Output: default treatment of packets sent by the device. Accept permits outbound traffic; Reject blocks traffic that is not explicitly allowed.
- Forward: controls whether the device, when acting as a router, forwards packets between networks.

8.2 Traffic Rules

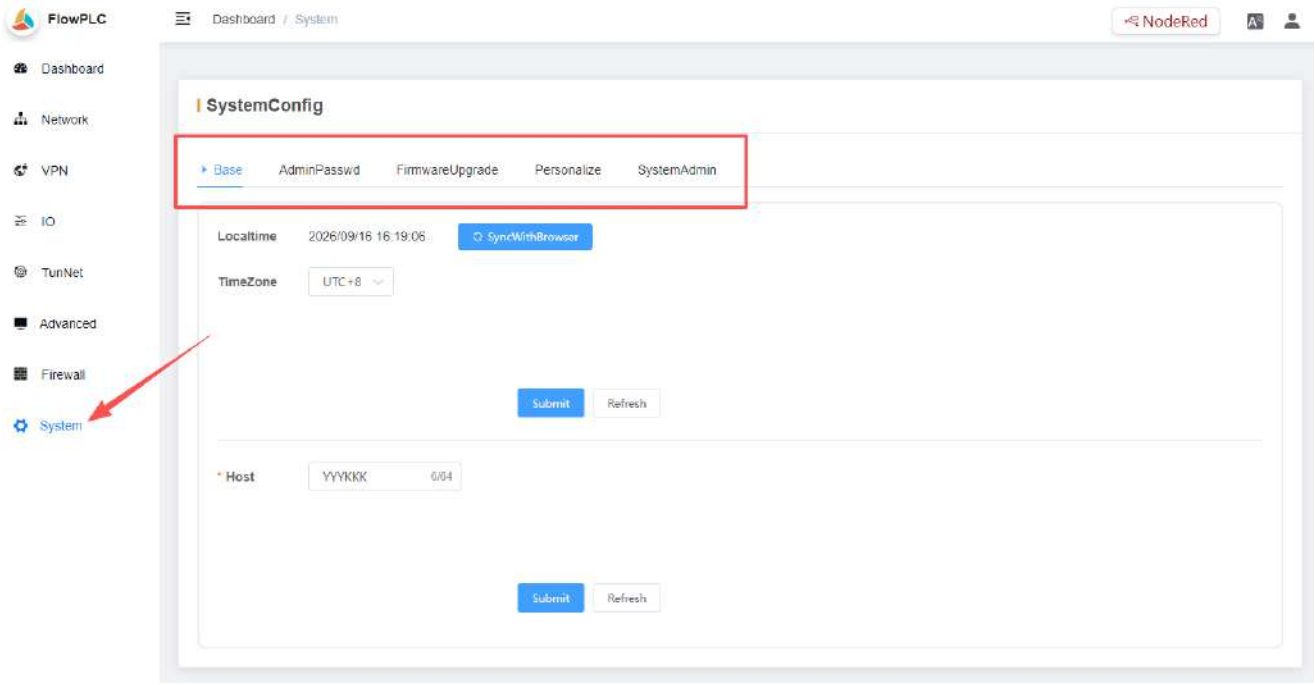
- Chain: Input, Output, or Forward.
- Source IP: address whose traffic is allowed or denied; blank matches any address.
- Protocol: select a protocol or Any when uncertain.
- Destination IP: packet destination; blank matches any address.
- Action: Accept to allow or Drop to block.
- Comment: optional description of the rule.

8.3 Port Forwarding

- Source Port: incoming port to forward.
- Protocol: TCP, UDP, SCTP, or DCCP. For example, HTTP normally uses TCP.
- Destination IP: internal target device.
- Destination Port: port on which the target application listens.
- Comment: optional description.

Note After changing settings, click Submit and restart the gateway for the changes to take effect.

9 System



9.1 Basic

Time Zone displays and allows changes to the device time zone. Set it correctly so device time matches local time.

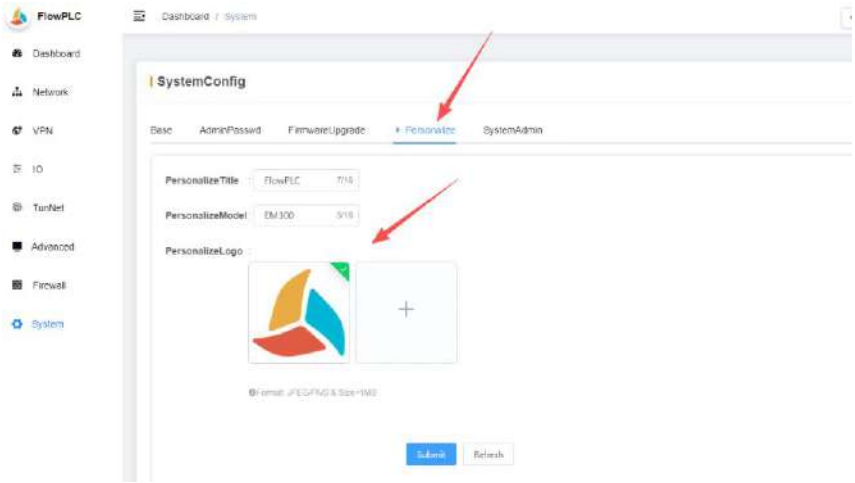
9.2 Administrator Password

Changes the device login password.

9.3 Firmware Upgrade

Updates the device firmware. Here, firmware refers to the device-management web service supplied by IOTRouter.

9.4 Customization



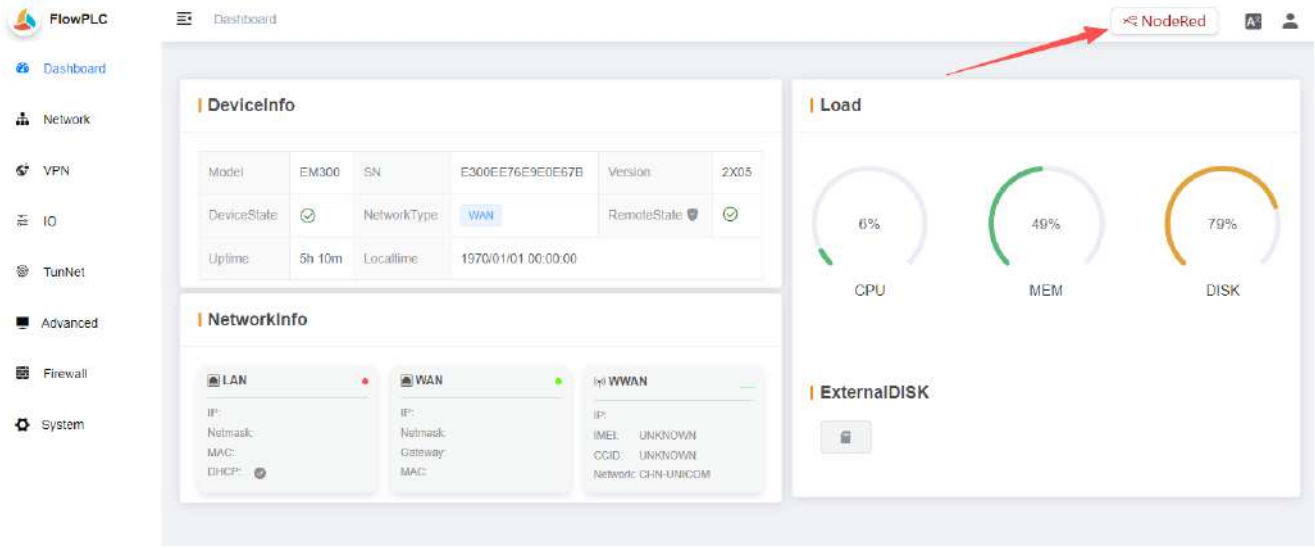
Customizes the gateway title, model name, and logo. Upload the icon file in the required format.

9.5 System Commands

- Factory Reset: restores factory settings.
- Restart: restarts the gateway.
- Scheduled Restart: configures an automatic restart time.
- Visual Programming Reset: restores only the visual programming environment to factory settings.
- Visual Programming Backup: exports the current visual programming configuration.

Note After changing system settings, click Submit and restart the gateway when prompted.

10 Visual Programming



Username: admin

Default password: EM12345678. This is synchronized with the web-management password.

The product includes a Node-RED-based visual programming environment with graphical drag-and-drop flow development. It simplifies industrial data acquisition and edge-logic development.

Built-in nodes cover common industrial and network protocols, including dedicated PLC and CNC protocols, Modbus TCP, Modbus RTU, TCP, UDP, HTTP, MQTT, IEC 60870-5-104, DL/T 645, CJ/T 188, and HJ 212. Data can be acquired through Ethernet, serial ports, and local IO.

Users can configure data parsing, format conversion, edge computing, and business logic, then upload processed data to cloud platforms or third-party servers. Complex local control logic is also supported for edge intelligence and real-time control. Refer to the node and application examples for detailed instructions.

11 Remote Management

EM Series products integrate remote management, remote programming, remote LAN access, and remote upgrades. Using the cloud platform and secure VPN tunneling, engineers can commission devices, update programs, and troubleshoot faults without traveling to the site, reducing travel cost and response time.

The plug-and-play design establishes a connection with minimal setup. Multiple security mechanisms protect data transmission and device access. For detailed instructions, refer to the Remote Management Software User Guide.

Company Information

Item	Details
Company	Chengdu Zongheng Intelligence Control Technology Co Ltd
Address	No. 599, Section 1, Huafu Avenue, Shuangliu District, Chengdu, Sichuan, China
Website	en.iotrouter.com
Email	agnes@iotrouter.com queeney@iotrouter.com
Business Cooperation	+86 189 82006591 +8913890804232