IOTROUTER

Edge Computing Gateway

EG&EV Series

Quick Start Instructions

Contents

Ⅰ. Preparation

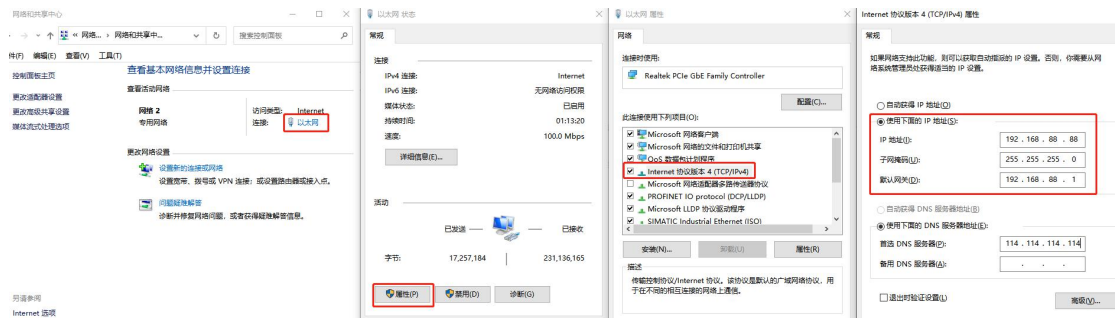
1. Indicator Lights

Marks	Function	Status	Explain
POW	Power Indicator	Always Off	Abnormal power supply
		Always On	Normal power supply
SYS/RUN	Operating Status	Always Off	Internal program not running
		600ms On/600ms Off	Program is running, but not connected to the Internet(external network address is the configured detection address)
		100ms On/2800ms Off	Program is running and connected to the Internet
4G/NET	Module Status	200ms On/1800ms Off	Network searching
		1800ms On/200ms Off	Standby status
		125ms On/125ms Off	Data transmission mode
WIFI	STATION	Always Off	Disabled STATION mode
		Always On	Enabled STATION mode,connected to an external hotspot
		Flashing	Enabled STATION mode,not connected to an external hotspot
LED1-2	User-defined	Always Off	Mode 0
		Always On	Mode 1
		Slow Flashing	Mode 2
		Quick Flashing	Mode 3
TX/RX	LoRa Transmit	TX Flashing	Data sending ⋆ EG2000 Only
		RX Flashing	Data receiving ⋆ EG2000Only
GPS	GPS Status	Always Off	Location acquisition failed ⋆ EG8200 Only
		Flashing	Location acquisition successful ⋆ EG8200 Only
TX1-8	485 Data Transmit	Always Off	No data sending ⋆ EG8208 Only
		Flashing	Data sending ⋆ EG8208 Only
RX1-8	485 Data Receive	Always Off	No data receiving ⋆ EG8208 Only
		Flashing	Data receiving ⋆ EG8208 Only

2. Connecting to the Gateway

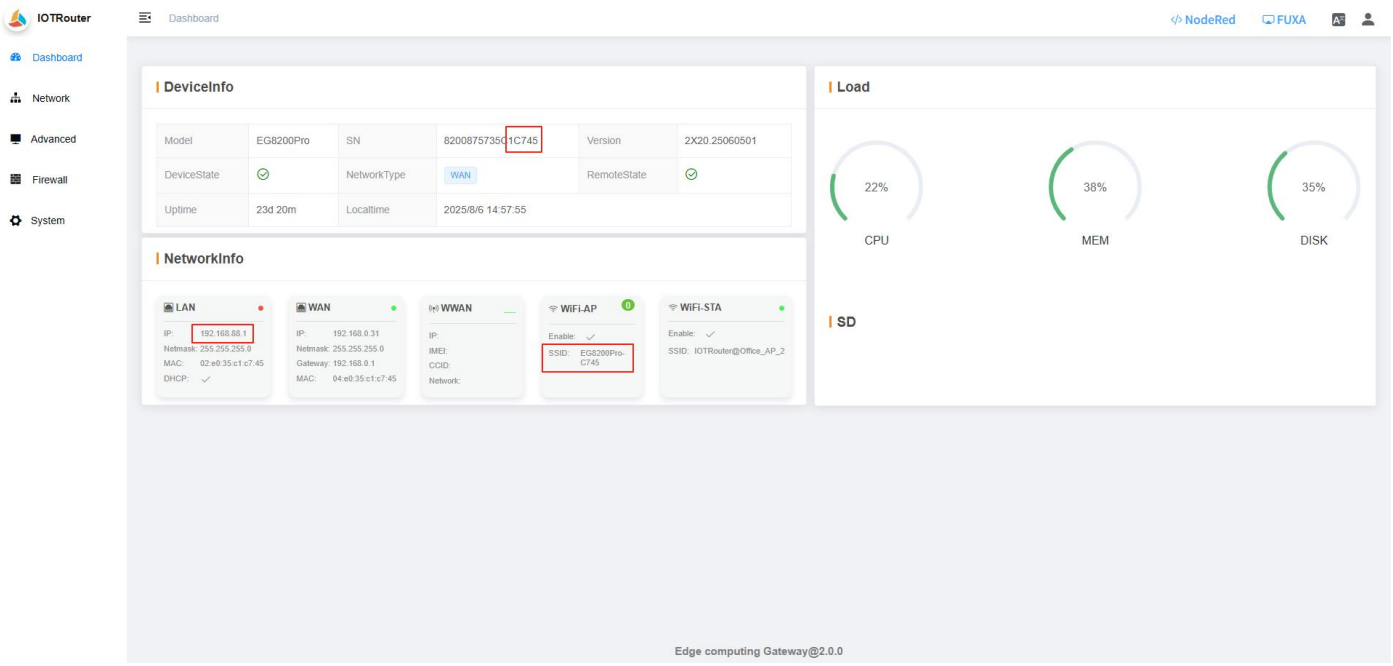
Method 1:

Connect your computer's Ethernet port to the gateway's LAN port using a network cable. The default IP address of the gateway's LAN port is 192.168.88.1. Set your computer's IP address to the same network segment. Otherwise, the computer and gateway will not be able to communicate. As the image below:



Method 2:

Connect your computer to the gateway's hotspot via WiFi. The WiFi name is: (gateway model-the last 4 digits of the SN number), and the password is: EG12345678. After the connection well, the gateway will assign an IP address in the 192.168.88.X network segment to the computer, as shown in the figure:



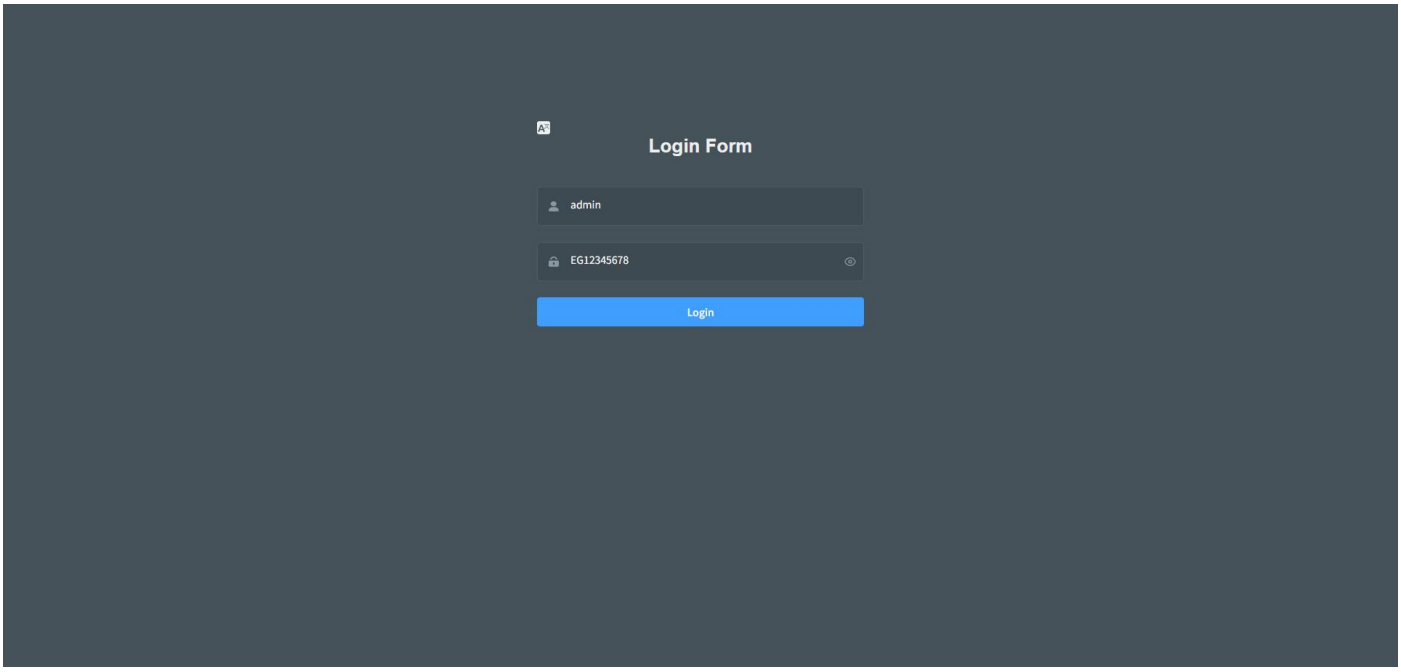
Note: Only some gateways can be accessed locally via WiFi

(Available Models: EG8200Mini/EG8200/EG8200Pro)

Ⅱ. Basic Use

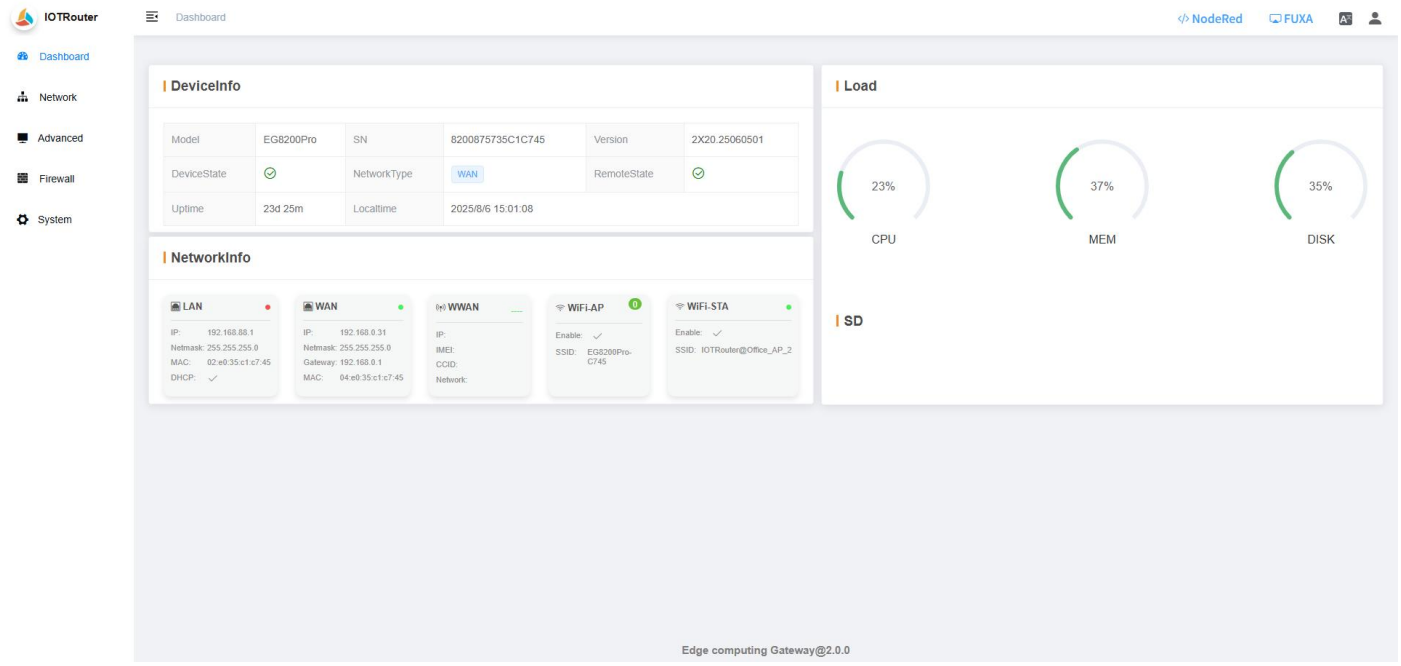
1. Login

Open a browser and enter 192.168.88.1 in the address bar to access the login interface. Default administrative password: EG12345678 (can be changed after logging in).



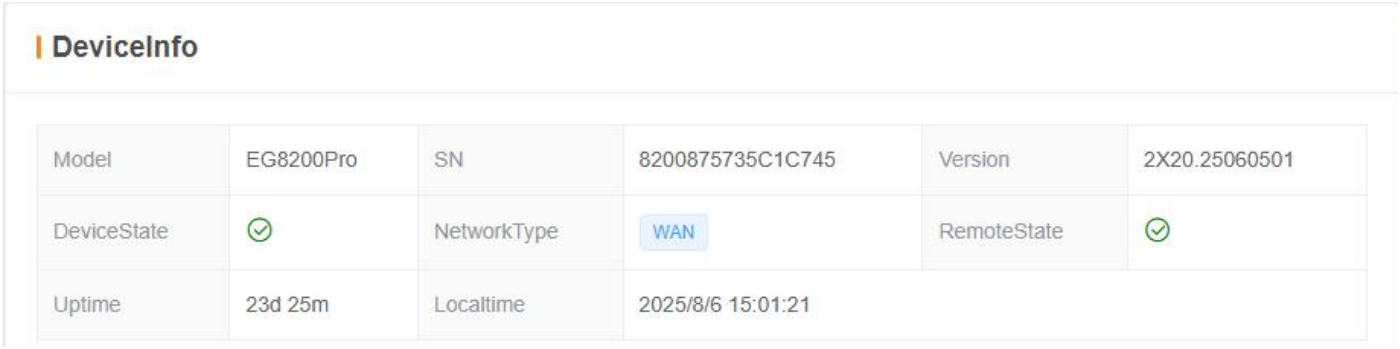
2. Home Page

Displays basic gateway information, network information, load status, and SD card usage.



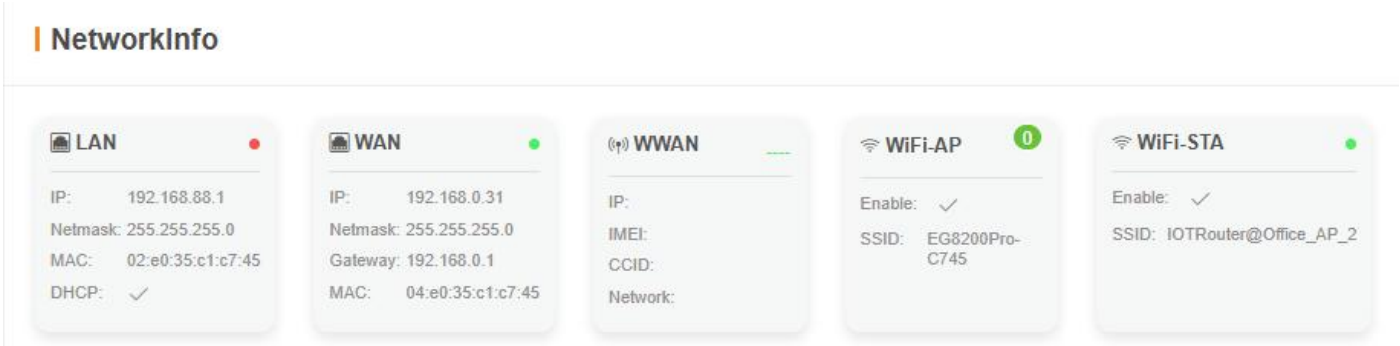
Note: There are slight differences in parameters between different models, please refer to the actual ones.

2.1. Device Information



- Model: Displays the specific model of the gateway.
- SN: Gateway's serial number, a globally unique number, typically used as a unique device identifier.
- Firmware Version: Current gateway version. The actual version displayed is subject to change.
- Device Status: Current operating status.
- Network Type: Current network connection method. "Unknown" indicates no network connection.
- Remote Status: Whether the gateway is remotely accessible.
- Uptime: The length of time the gateway has been powered on.
- Local Time: Current time of gateway.

2.2. Network Information



LAN Status Information:

- Status Icon: Green (connected) / Red (disconnected).
- IP: Current IP address of the LAN port.
- Mask: Current subnet mask of the LAN port.
- MAC: MAC address of the LAN port.
- DHCP: DHCP enable status (√Enabled/×Disabled).

WAN Status Information:

- Status Icon: Green (connected)/Red (disconnected).
- IP: Current IP address of the WAN port.
- Mask: Current subnet mask of the WAN port.
- Gateway: Current gateway address of the WAN port.
- MAC: MAC address of the WAN port.

Cellular (4G/5G) Status Information:

- Status Icon: Indicates the current cellular signal strength.
- IP: Current cellular IP address.
- IMEI: International Mobile Equipment Identity of the cellular module.
- Card Number: The number of the currently used SIM card.
- Network: Currently connected network type (e.g., LTE-4G).

WiFi Hotspot Status:

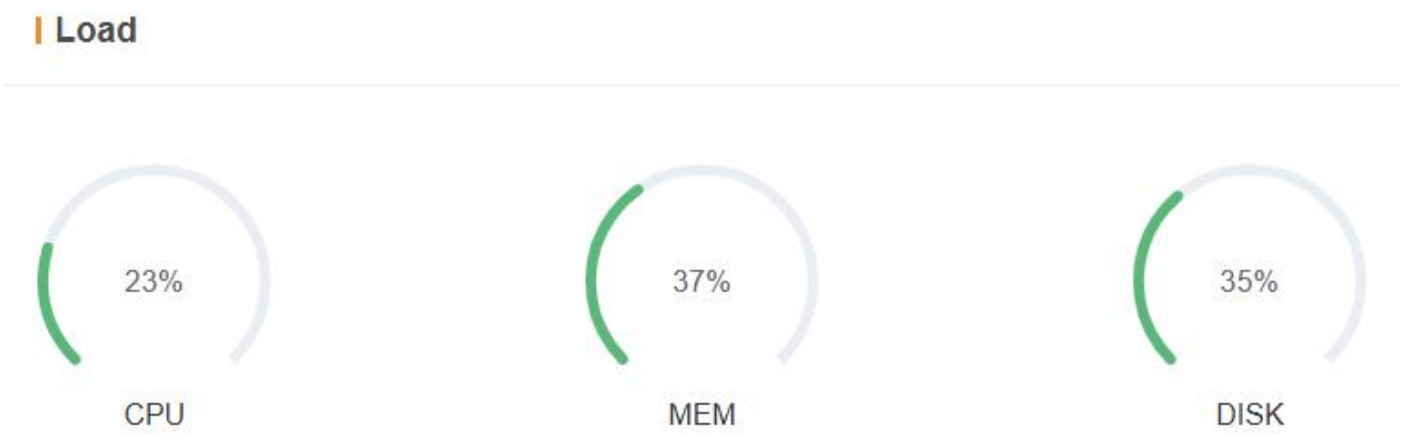
- Status Icon: Number of devices connected to the gateway AP hotspot.
- On: AP mode enabled (√ Enabled / × Disabled).
- Hotspot Name: Name of the gateway AP hotspot.

WiFi Terminal Status Information:

- Status Icon: Green indicates connected to Wi-Fi, Red indicates disconnected.
- On: Station mode is enabled (√ Enabled / × Disabled).

- Hotspot Name: The name of the currently connected Wi-Fi.

2.3. Equipment Load



- CPU: The percentage of the gateway's CPU usage.

- Memory: The percentage of the gateway's memory usage.

- Disk: The percentage of the gateway's disk usage.

2.4. SD

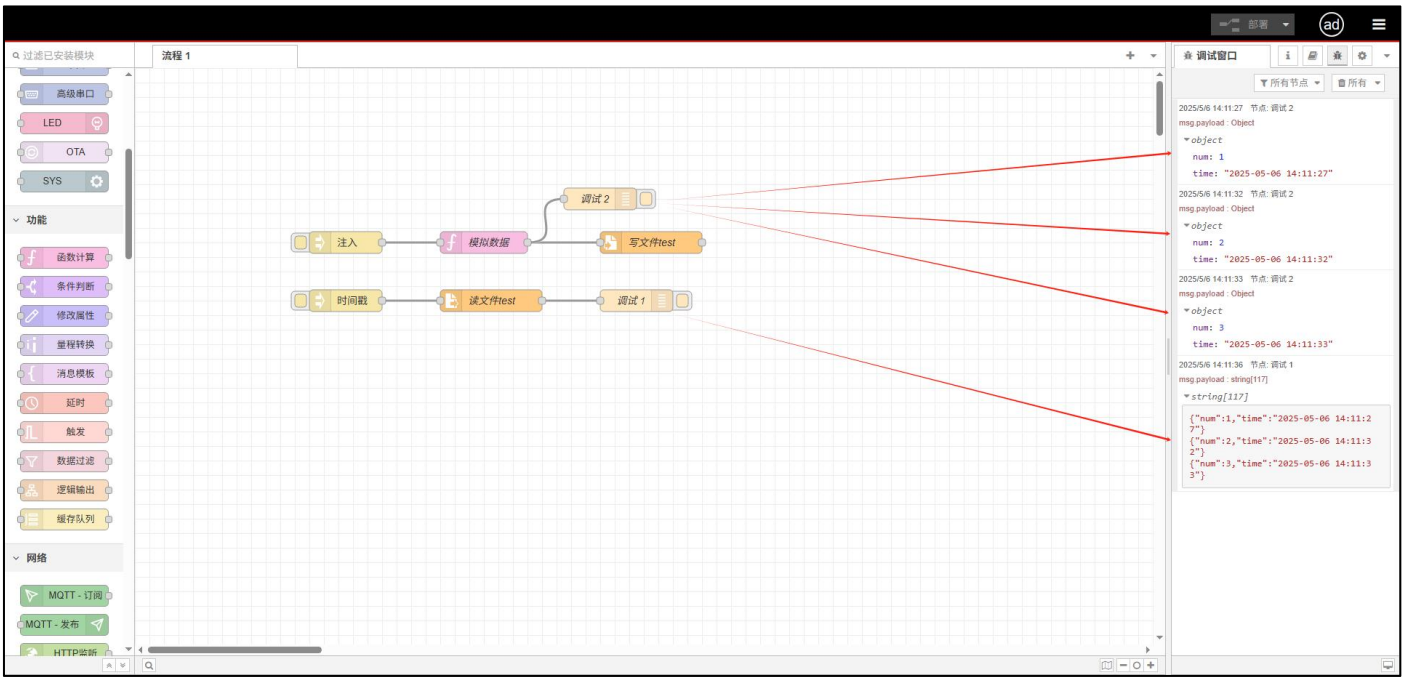
- SD Card Storage: Percentage of storage space used.

- Format SD: Formats the SD card. After the format is successful, restart the gateway.

- Browse Files: Allows you to browse data files stored on the SD card and download them to your local computer for viewing.

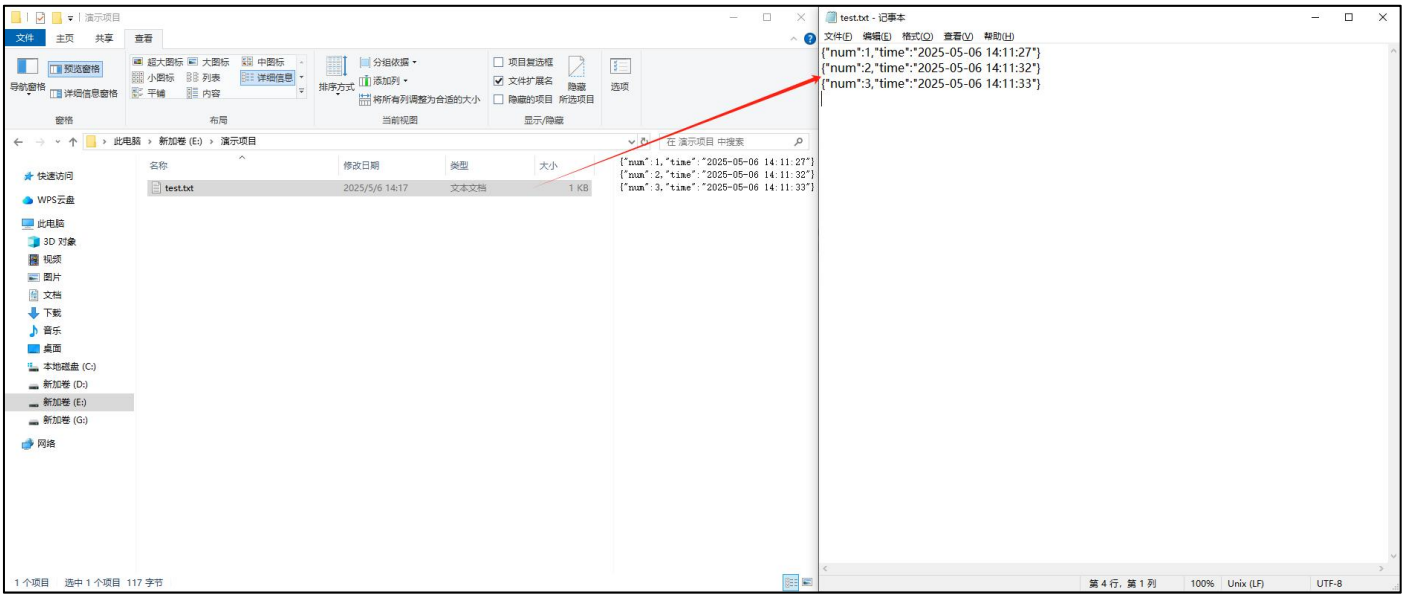
Example:

Step 1: In the visual programming environment, confirm that a file named *test* has been created and 3 data records have been successfully stored.



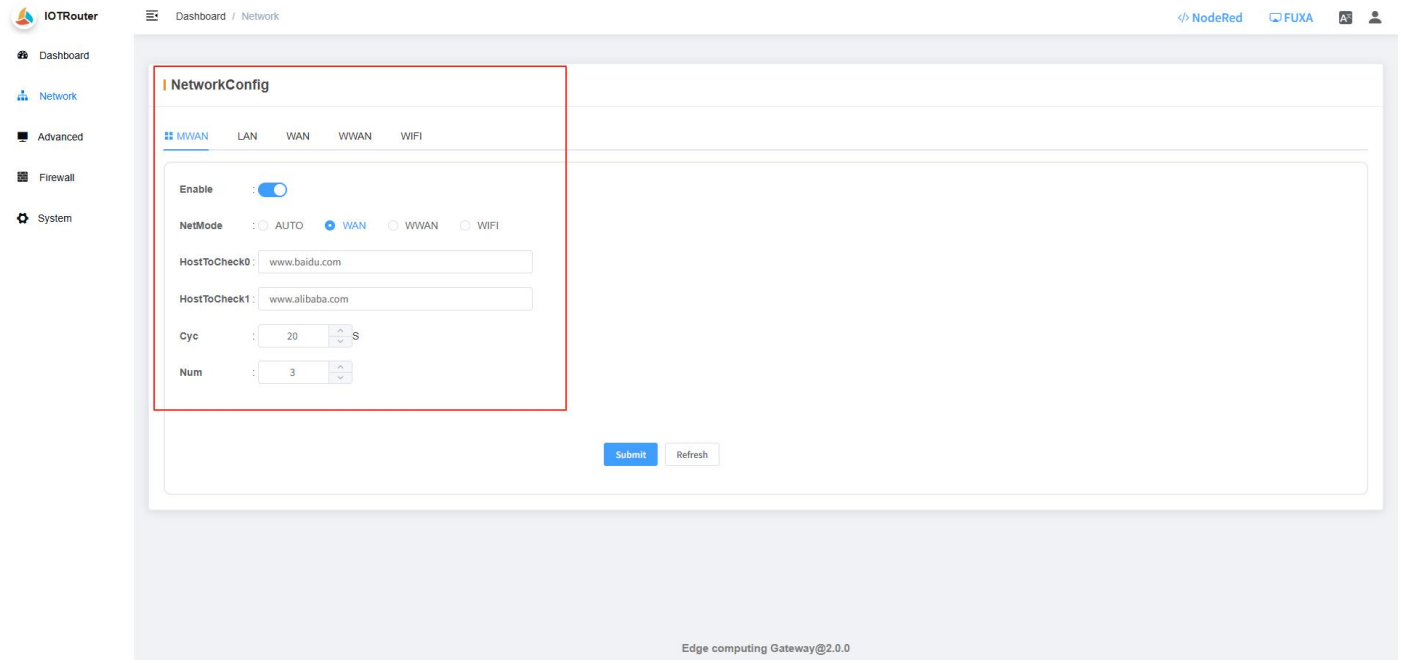
Step 2: Navigate to the SD card part on the home page and click *Browse Files*. Find the target file *test* in the list, verify the name, and click *Download* to complete the file download.

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

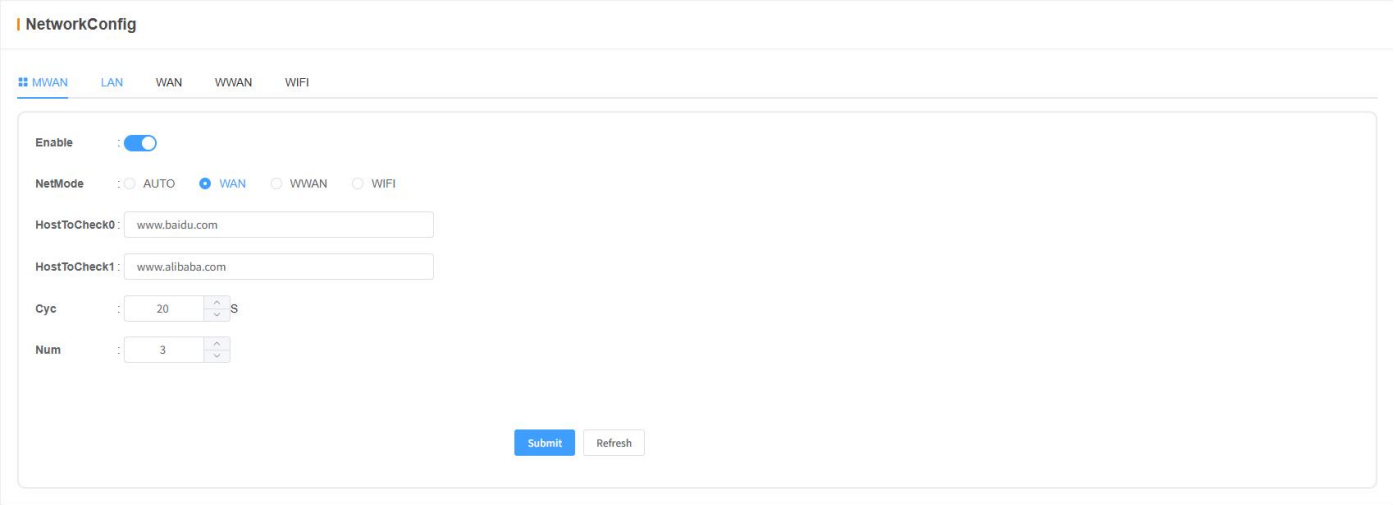


3. Network

Configure the gateway network parameters.



3.1. MWAN Configuration



- On: Enabled by default, please do not disable.

- Network Mode: Defaults to AUTO, which automatically switches the connection mode based on network status. If network anomalies occur, the network switches in the order of WAN/WiFi/WWAN (4G) until a successful connection is established. Other options allow you to set a fixed connection mode.

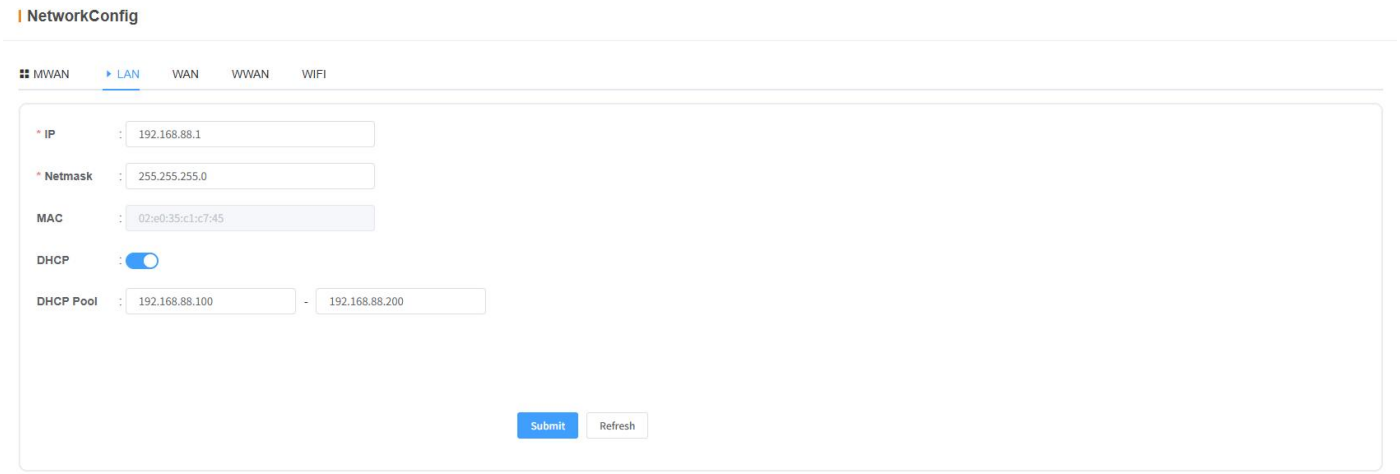
(Note: Gateways without WAN or WiFi capabilities default to 4G Internet access and therefore do not have a network mode configuration option.)

- Detection Function: Pings the host address at a set interval (the address and interval can be modified based on network conditions) to determine the current network status and automatically switch the connection mode (AUTO). If the fixed connection mode is selected, the sniffing function will be replay reconnection.

(Note: If the gateway is only used for LAN communication, it is recommended to change the detection address to an address that can be pinged within the LAN.)

(Note: After setting, click Submit and reboot to take effect.)

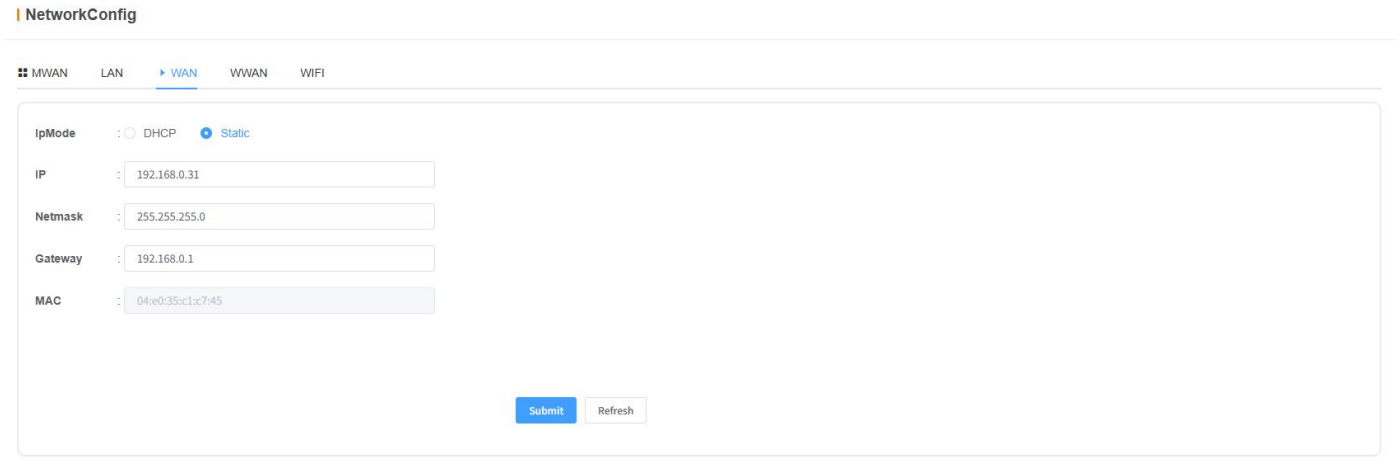
3.2. LAN Configuration



- IP: Default: 192.168.88.1 (can be changed after logging in).
- Netmask: Default: 255.255.255.0.
- MAC: LAN port MAC address.
- DHCP: can set a DHCP pool for external networks (shared between WiFi and LAN).

(Note: After setting, click Submit and reboot to take effect.)

3.3. WAN Configuration



- IP Mode: Default DHCP.
- IP: Automatically obtain a static IP address in DHCP mode; manually configure a static IP address in static mode.

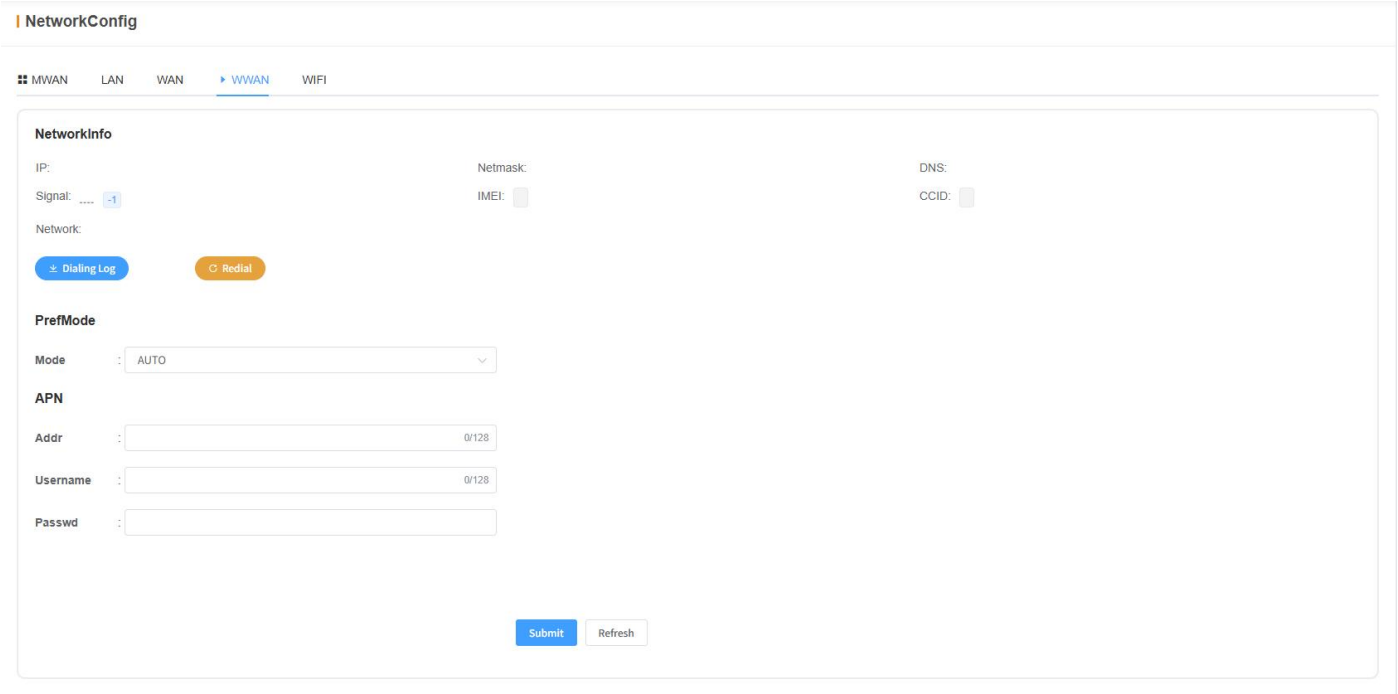
- Netmask: Automatically obtain a default IP address in DHCP mode; manually configure a default IP mask in static mode.

- Gateway: Automatically obtain a default IP address in DHCP mode; manually configure a default gateway in static mode.

- MAC: WAN port MAC address.

(Note: After setting, click Submit and reboot to take effect.)

3.4. Cellular



- IP: Current cellular network IP address.

- Mask: Current cellular network mask.

- DNS: Current cellular network DNS.

- Signal: Current cellular network signal strength (range: 0-100, with higher values indicating stronger signals).

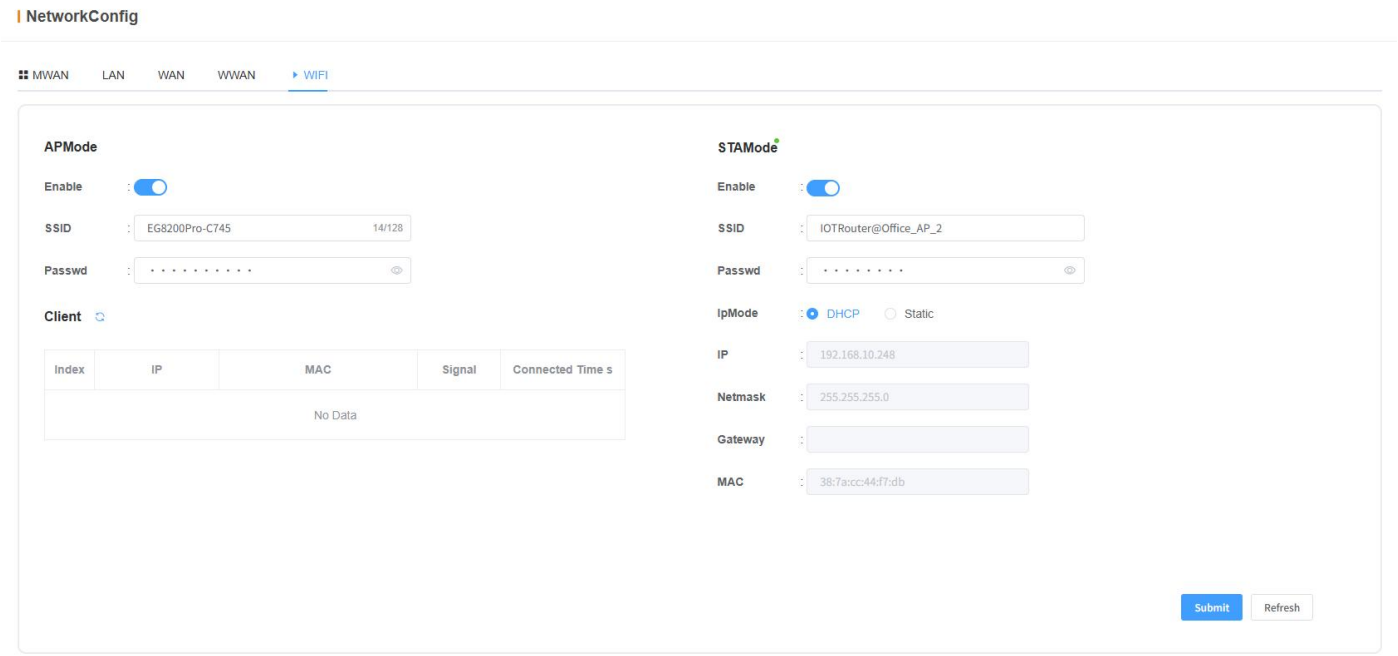
- IMEI: cellular module IMEI number.

- Card number: SIM card number.

- Dial log: Download the most recent 4G module dial log for debugging purposes.
- Manual Redial: Allows you to redial the number immediately.
- APN: Configures APN parameters.

(Note: After setting, click Submit and the system will reboot to take effect.)

3.5. WiFi Configuration



- Mode: AP mode creates a Wi-Fi hotspot, allowing other devices to connect to it.

STA mode allows the gateway to connect to the on-site Wi-Fi network.

(Note: Only EG8200Pro support dual-band 5GHz/2.4GHz, other Wi-Fi-enabled gateways only support the 2.4GHz band.)

AP Mode Configuration Information:

- On: AP mode is enabled (enabled by default).
- Hotspot Name: AP - Wi-Fi hotspot name. Default value is *Gateway Model-Last 4 Digits of SN* (a combination of numbers, letters, and symbols, up to 32 characters).
- Password: AP - Wi-Fi password. Default value is EG12345678 (a combination of numbers, letters, and symbols, at least 8 characters).

- Client: Information about devices connected to the gateway's Wi-Fi.

STA Mode Configuration:

- On: STA mode is disabled by default and can be enabled manually.

- Hotspot Name: The name of the Wi-Fi hotspot you want to connect to. Can automatically search for the hotspot name or manually enter the name of the hotspot you want to connect to.

- Password: Manually enter the password of the hotspot you want to connect to.

- IP Mode: DHCP by default, manually set to static.

- IP: Automatically obtain an IP address in DHCP mode. manually configure a fixed IP address in static mode.

- Netmask: Automatically obtain an IP address in DHCP mode. manually configure a netmask in static mode.

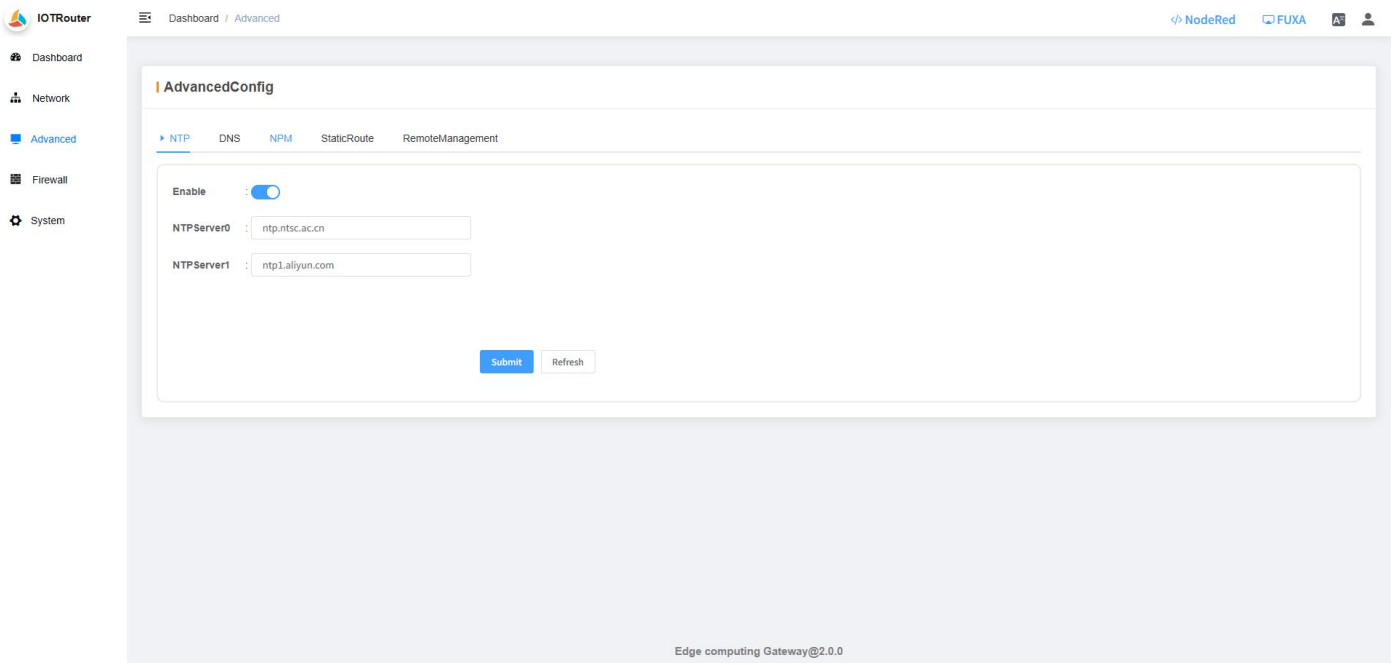
- Gateway: Automatically obtain an IP address in DHCP mode. manually configure a default gateway in static mode.

- MAC: MAC address of the Wi-Fi in STA mode. (After completing the settings, click Submit and reboot to take effect.)

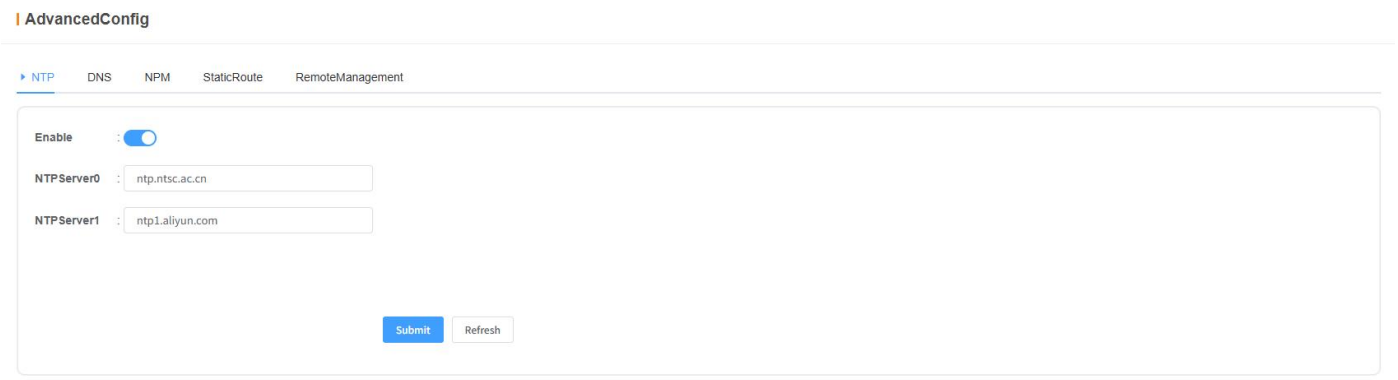
(Note: After setting, click Submit and reboot to take effect.)

4. Advanced

Configure advanced gateway parameters



4.1. NTP

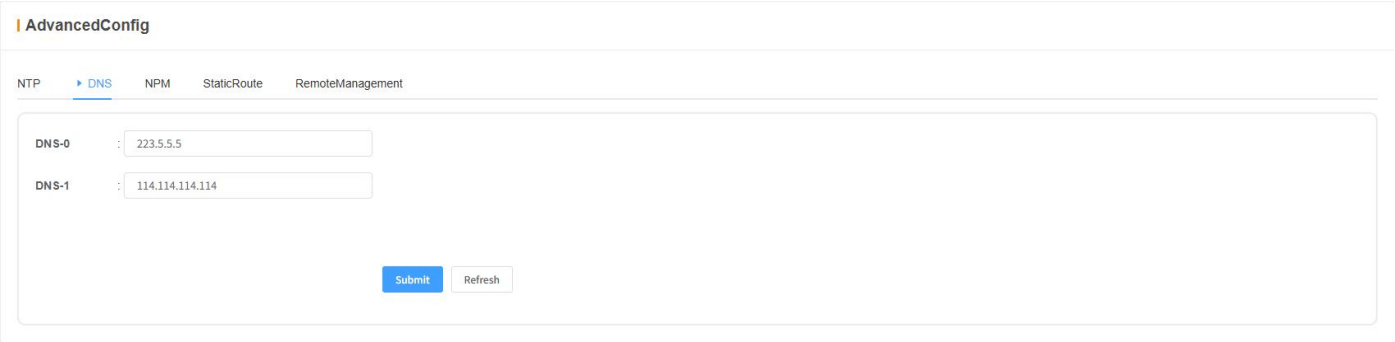


- Enabled : Enabled by default

- NTP Server: NTP server address. For private or intranet networks, you must modify the NTP server address.

(Note: After setting, click Submit and reboot to take effect.)

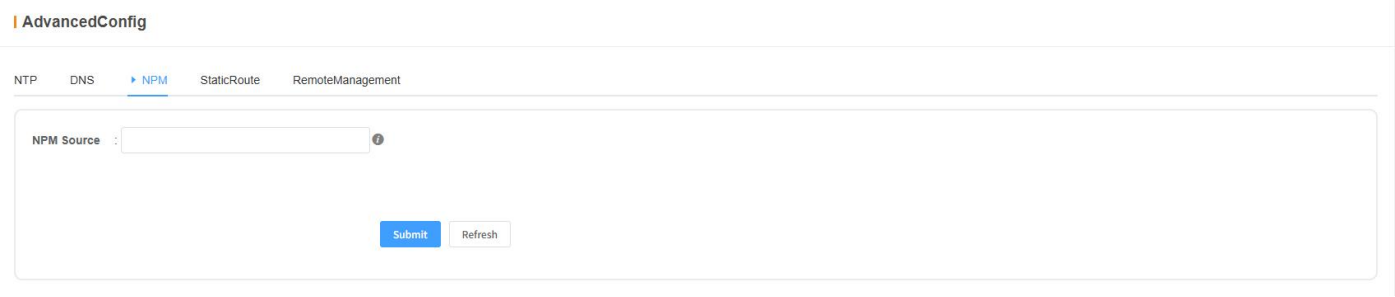
4.2. DNS



- DNS: DNS service affects domain name resolution. Users should configure or modify DNS server settings according to their needs.

(Note: After setting, click Submit and reboot to take effect.)

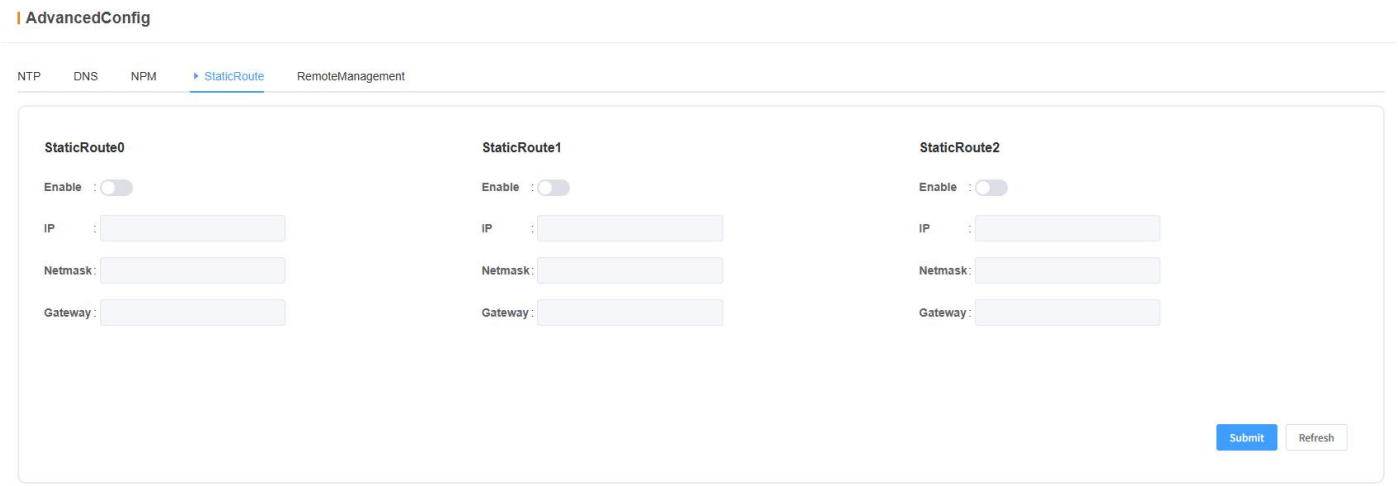
4.3. NPM



- NPM: Configure the NPM source address. Users can specify the Node-Red node installation source.

(Note: After setting, click Submit and reboot to take effect.)

4.4. Static Routing



- Static Routing: Defines the exact path for data packets to reach a specific network or host (primarily applicable for cross-segment communication scenarios and when forwarding data through a designated gateway is required).

- Enabled: Supports three static routing rules, disabled by default.

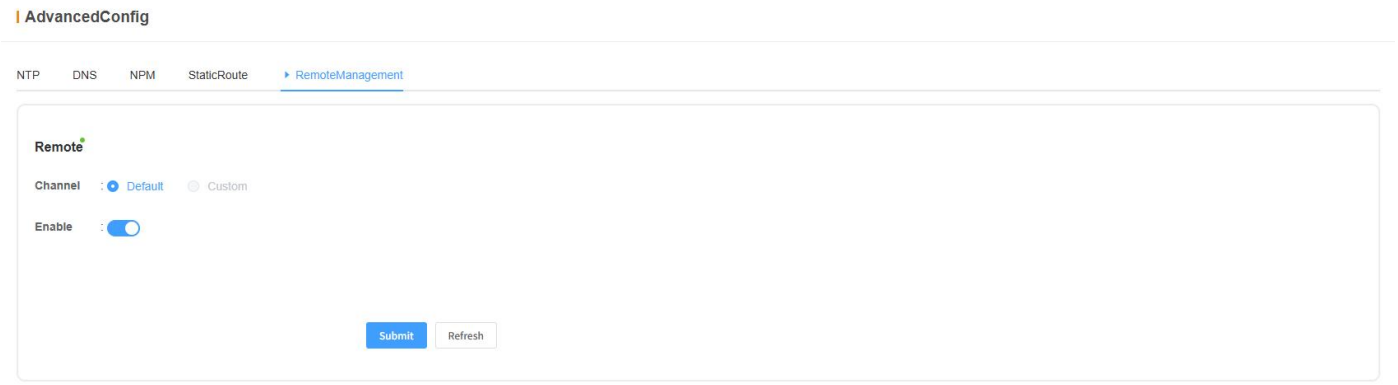
- IP: Enter the target IP address or IP network segment to be accessed.

- Mask: Enter 255.255.255.255 for accessing a specific IP address, or 255.255.255.0 for accessing a specific network segment.

- Gateway: Enter the gateway address for data transfer. (For more information, see the https://iotrouter.yuque.com/r/organizations/homepage.)

(Note: After setting, click Submit and reboot to take effect.)

4.5. Remote Management

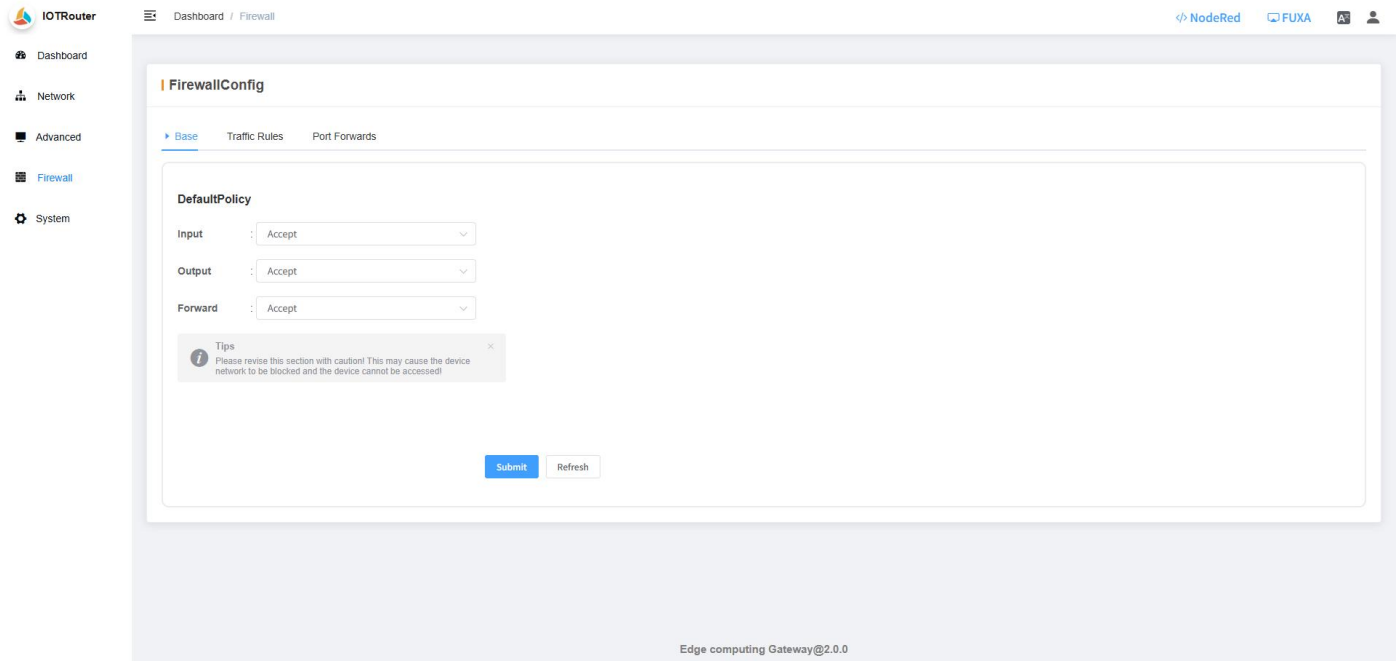


- Remote Management: Once enabled, you can use our remote service to remotely access and configure the gateway. You can disable it for special needs. (Note: Disabling remote management will prevent remote configuration, and you will be solely responsible for any consequences.)

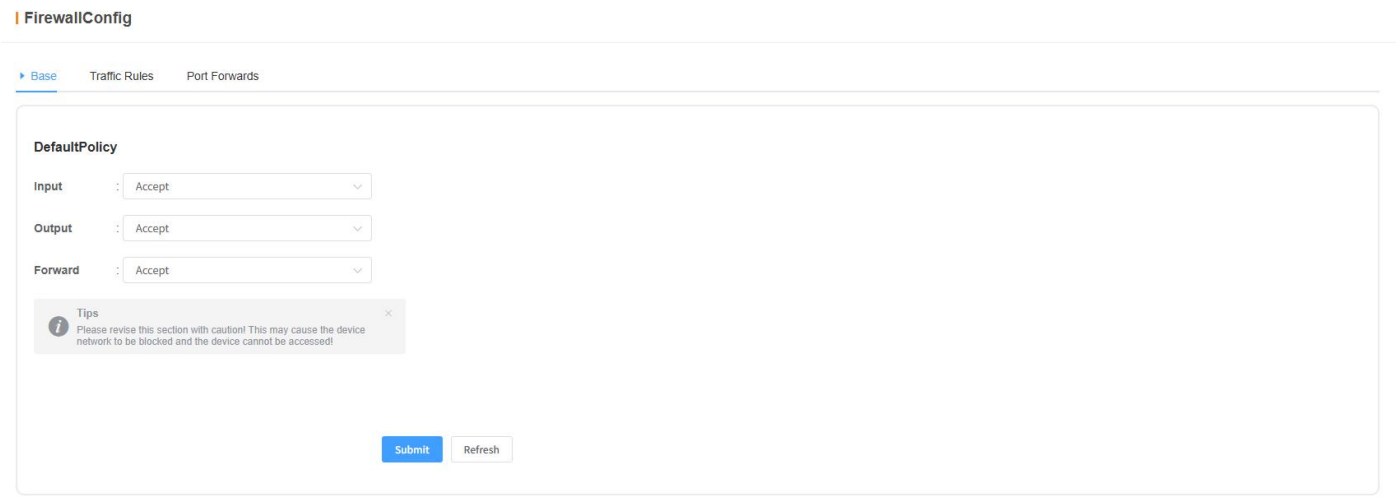
(Note: After setting, click Submit and reboot to take effect.)

5. Firewall

Configure gateway firewall rules and policies



5.1. Basic



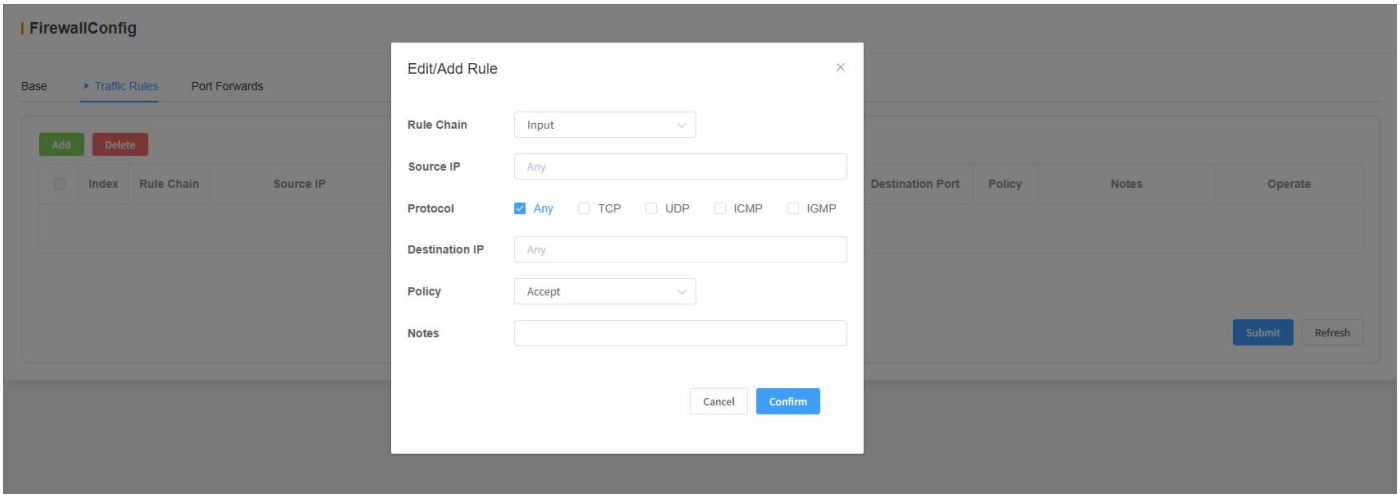
- Inbound: Determines the default handling of packets from external networks to the gateway. If set to *Accept*, all packets not explicitly denied by other rules are allowed in; if set to *Reject*, only packets matching the specified rules are allowed through.

- Outbound: Controls the default behavior for packets sent from the gateway to external networks. Similarly, *Accept* allows all outgoing packets by default, while *Reject* blocks all packets not specifically allowed from leaving the gateway.

- Forward: Applies to situations where the gateway acts as a router, determining whether packets are allowed to be forwarded from one network to another through the gateway.

(Note: Be careful when modifying this section! It may result in the gateway network being blocked and unable to access the gateway.)

5.2. Communication Rules



- Rule Chain: Select whether this rule is inbound, outbound, or forwarding.

- Source IP: Enter the source IP address for traffic to allow or deny. Leaving this field blank means any IP address will be matched.

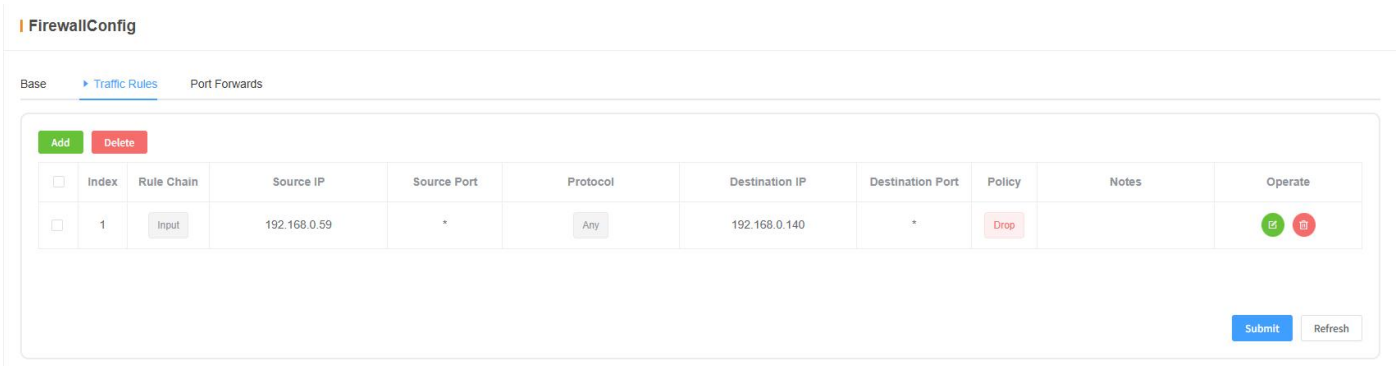
- Protocol: Select a protocol based on your needs. If unsure, select *Any* to match all protocols.

- Destination IP: Enter the destination IP address for the packet. Leaving this field blank means any IP address will be matched.

- Policy: Select how the packet should be handled. You can choose between *Accept* (allow) and *Drop* (block).

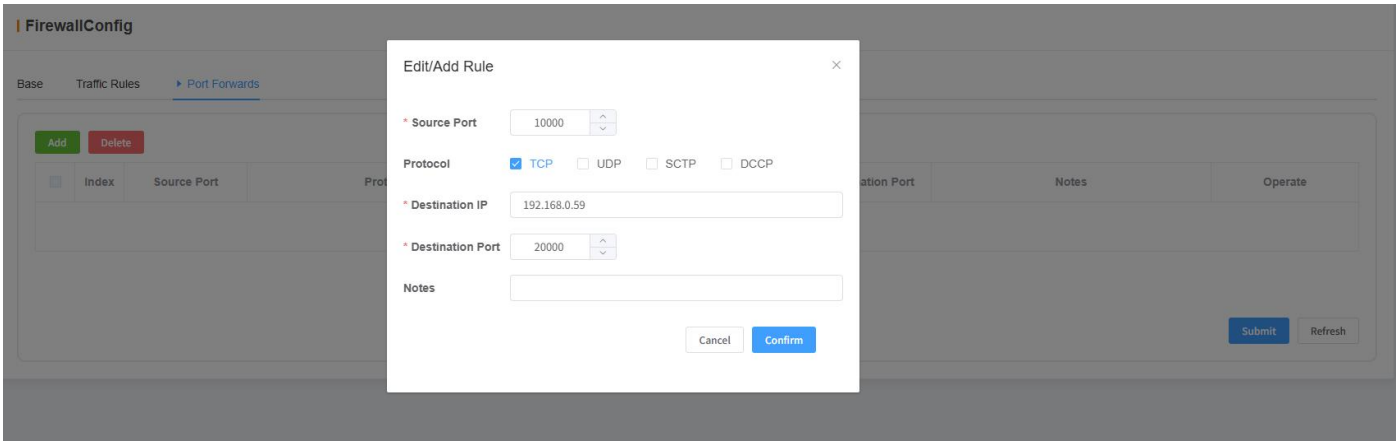
- Notes: Enter any notes.

- Save Rules. Click *OK* to add the rule, then click *Submit* for it to take effect.



As shown in the figure above, this rule prevents the device with IP address 192.168.0.59 from sending any type of data packets to the gateway with IP address 192.168.0.140.

5.3. Port Forwarding

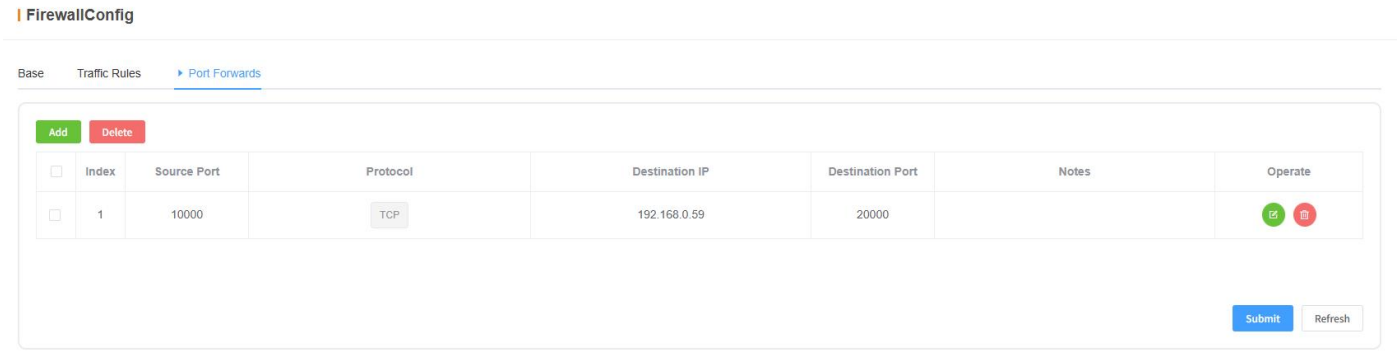


- Source Port: Enter the source port to be forwarded.

- Protocol: Select the protocol type to use, such as TCP, UDP, SCTP, or DCCP. Choose based on your needs. For example, HTTP services typically use TCP.

- Destination IP: Enter the IP address of the target device on the internal network. This is the device to which the packets will ultimately arrive.

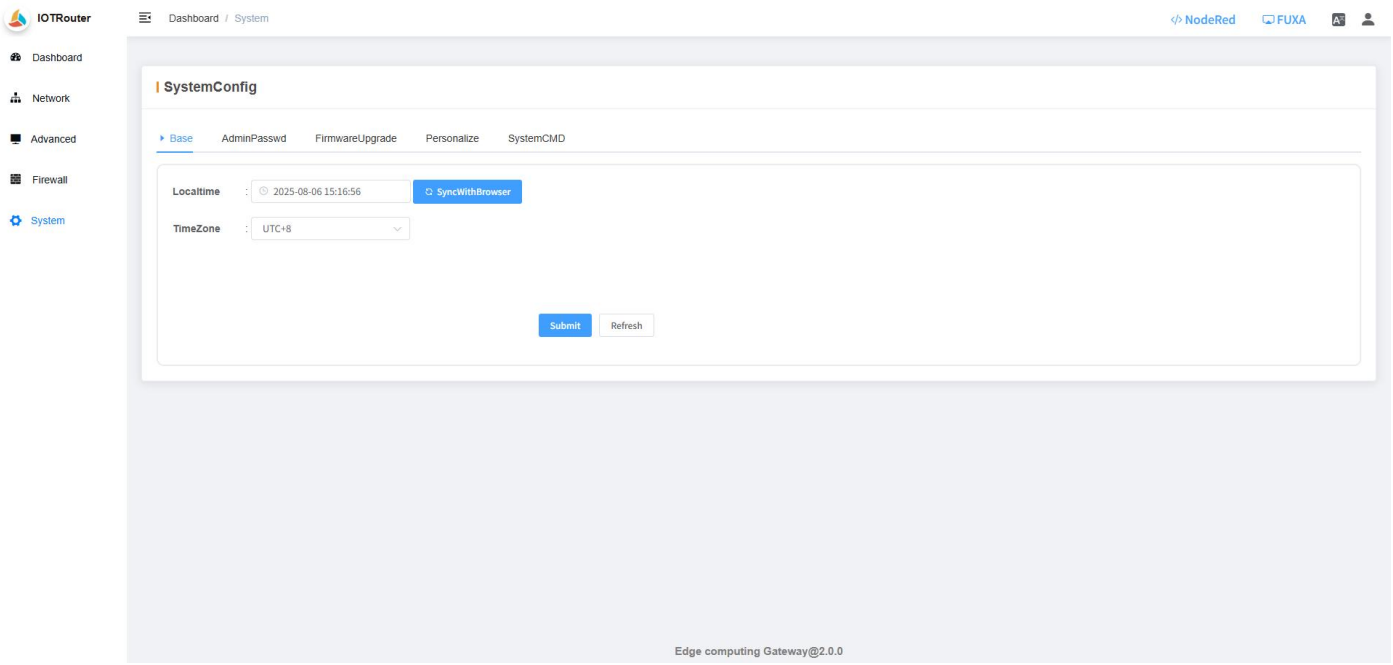
- Destination Port: Enter the port on the target device where the application is listening.



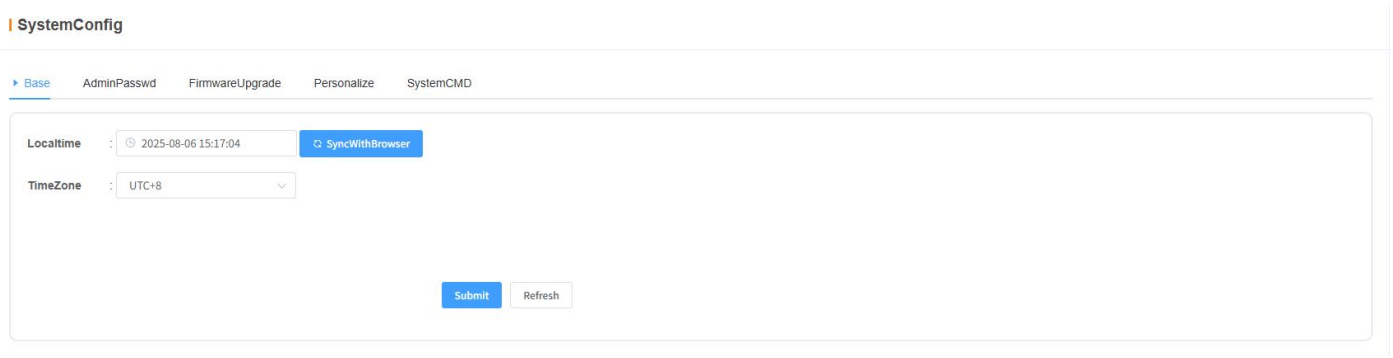
As shown in the figure above, this rule redirects external TCP traffic from the public port 10000 to port 20000 of the device with the IP address 192.168.0.59 on the internal network.

6. System

Configure gateway system parameters.



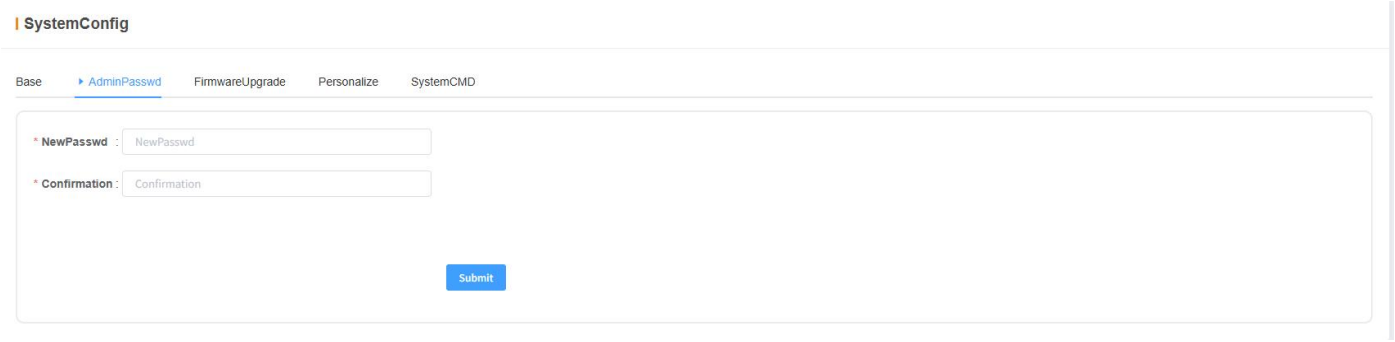
6.1. Basic



- Local Time: Real-time clock (RTC). Network-connected time automatically synchronizes with the network's NTP time. Users can click the *Sync with Browser* button to instantly sync.

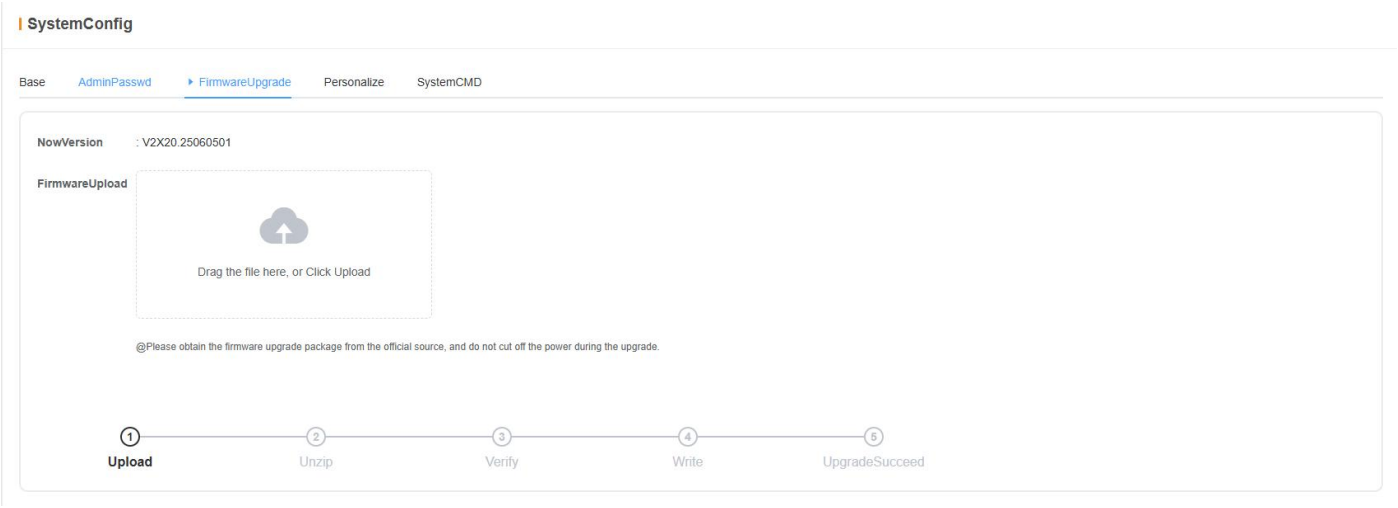
- Time Zone: Displays and allows users to change the gateway's time zone. Correctly setting the time zone ensures that the time (including the RTC time and the time synchronized with the network) is consistent with the local time.

6.2. Manage Passwords



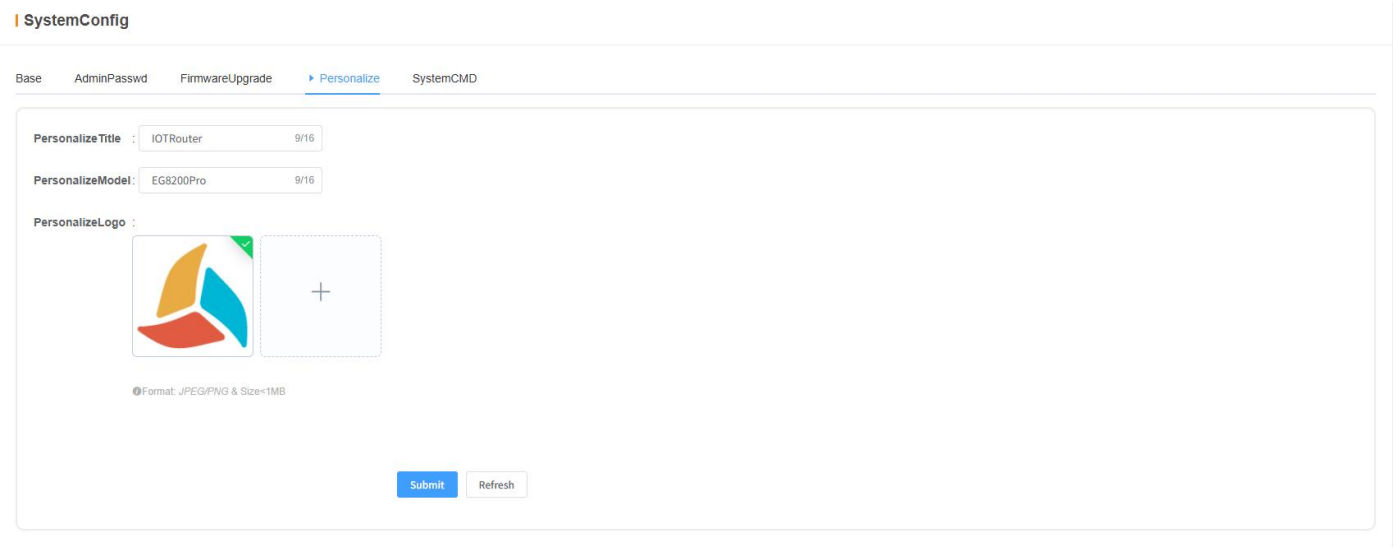
- Admin Password: Change the gateway login password. The password for the configuration page and the visual programming interface must be the same.

6.3. Firmware Upgrade



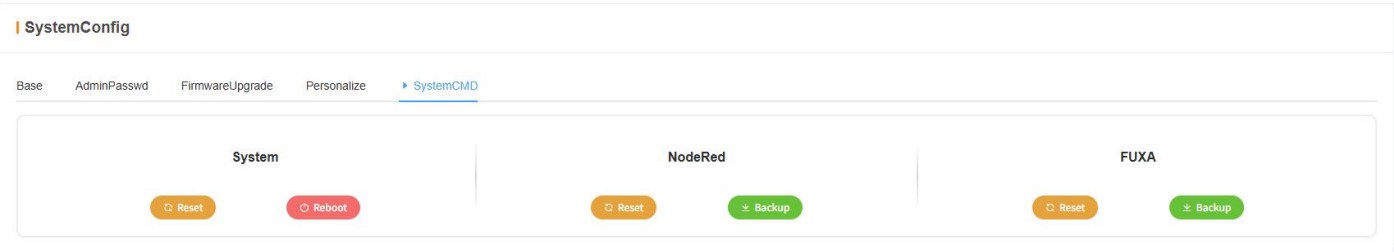
- Firmware Upgrade: Update the gateway's firmware version.

6.4. User-defined



- User-defined: Supports custom modification of gateway title, model and LOGO icon (please upload the icon file in the specified format).

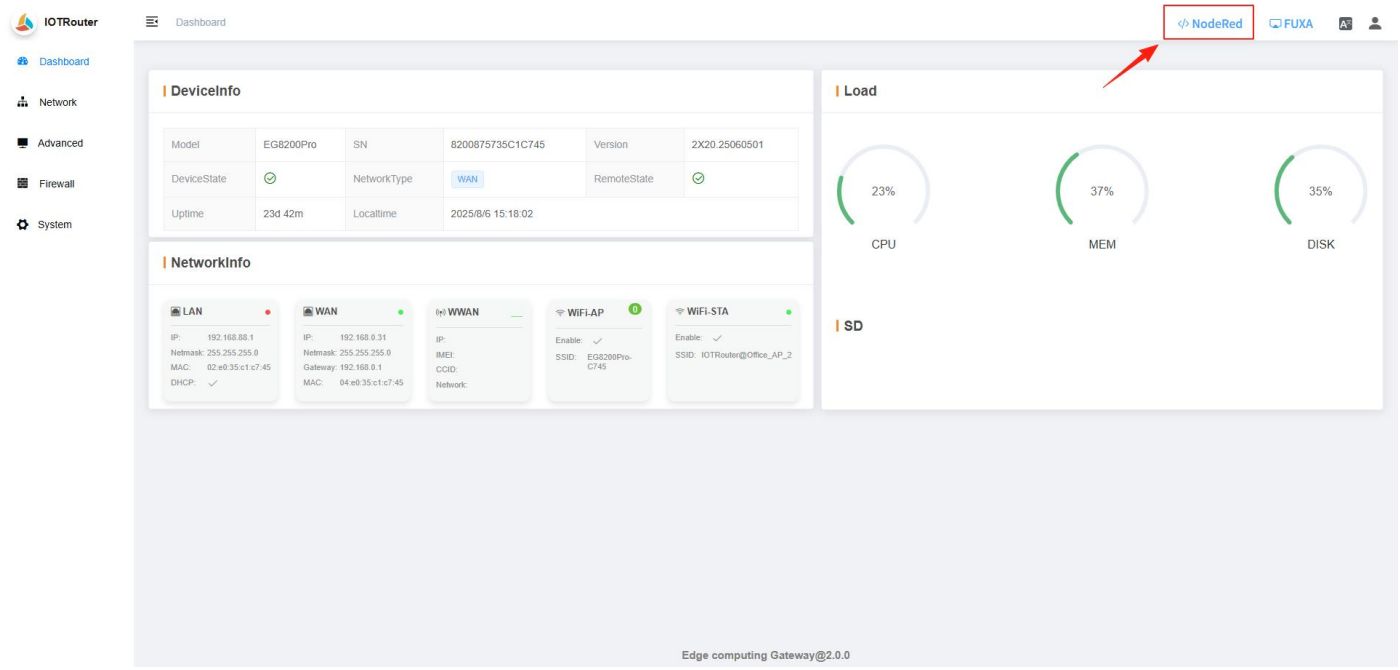
6.5. System Commands

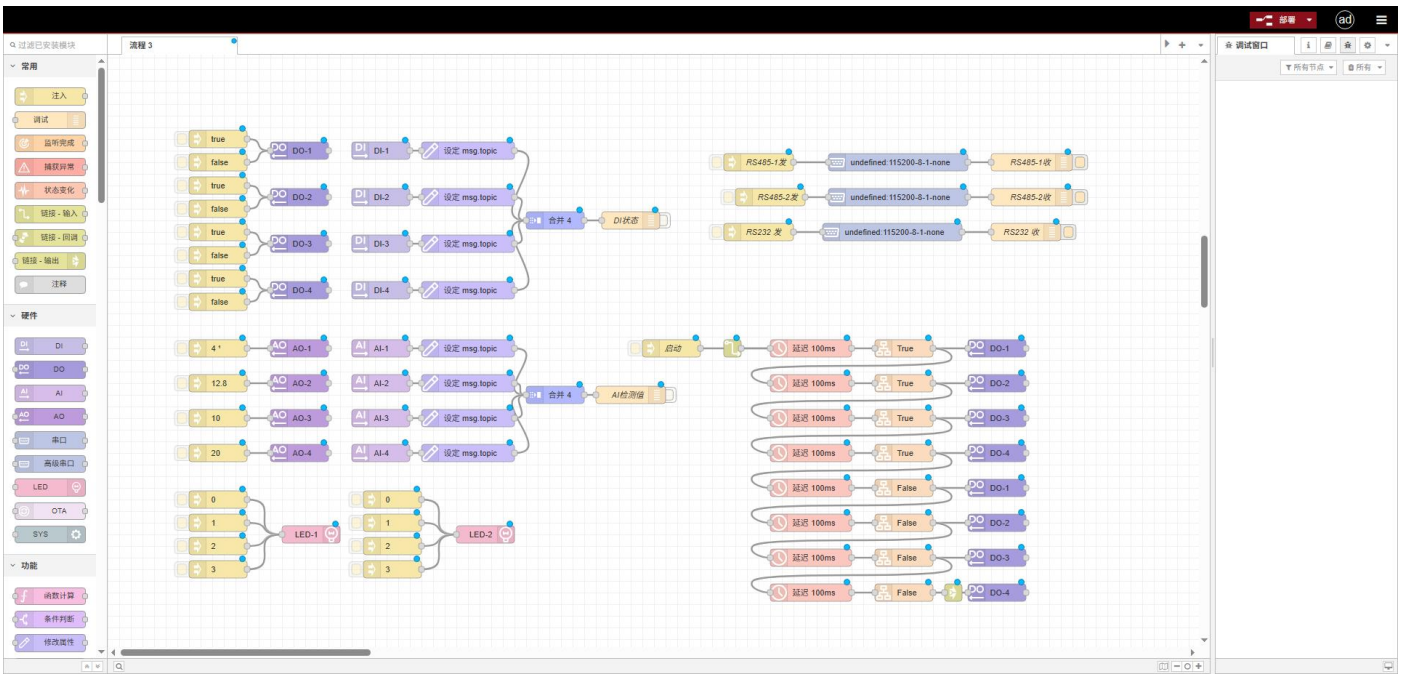


- System Reset: Restores the entire gateway to factory settings.
- System Restart: Restarts the gateway.
- Visual Programming Reset: Restores only the visual programming interface to factory settings.
- Visual Programming Backup: Exports the current visual programming configuration.
- Web Configuration Reset: Restores only the web configuration to factory settings.
- Web Configuration Backup: Exports the current web configuration project.

(Note: Only the EG8200Pro and EV8010 support web configuration.)

7. Visual Programming

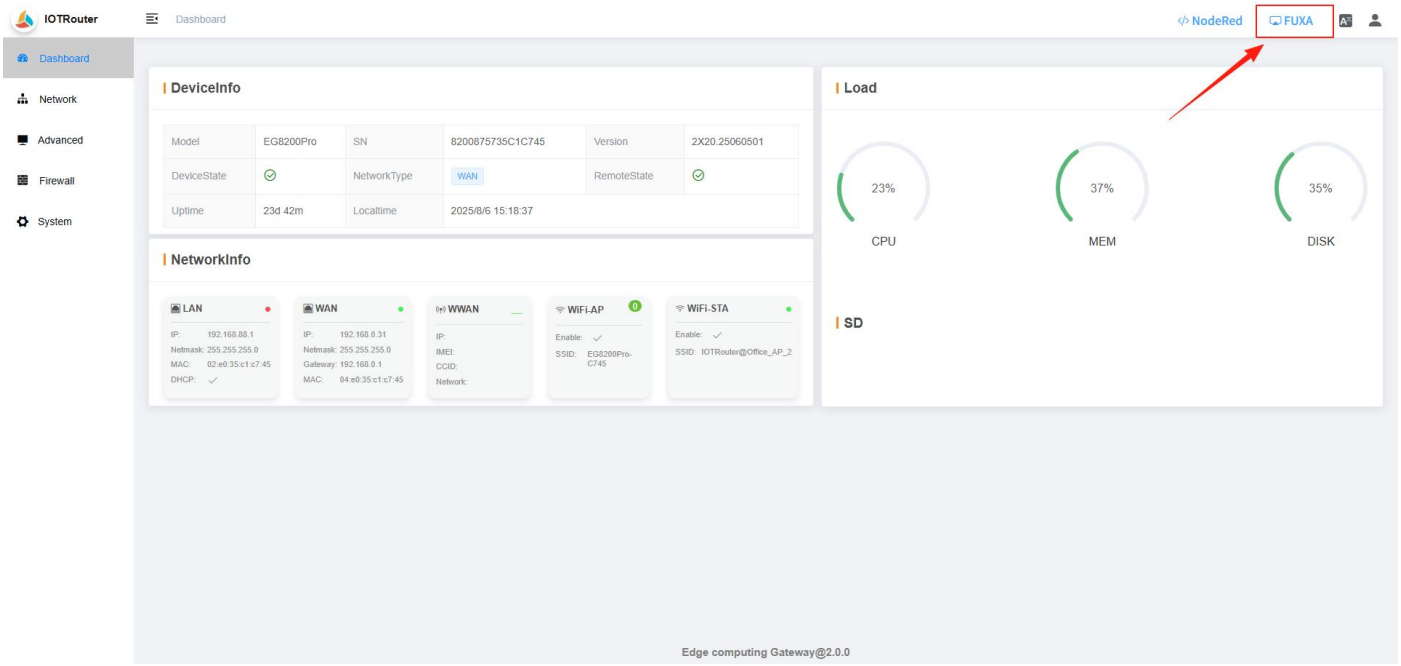


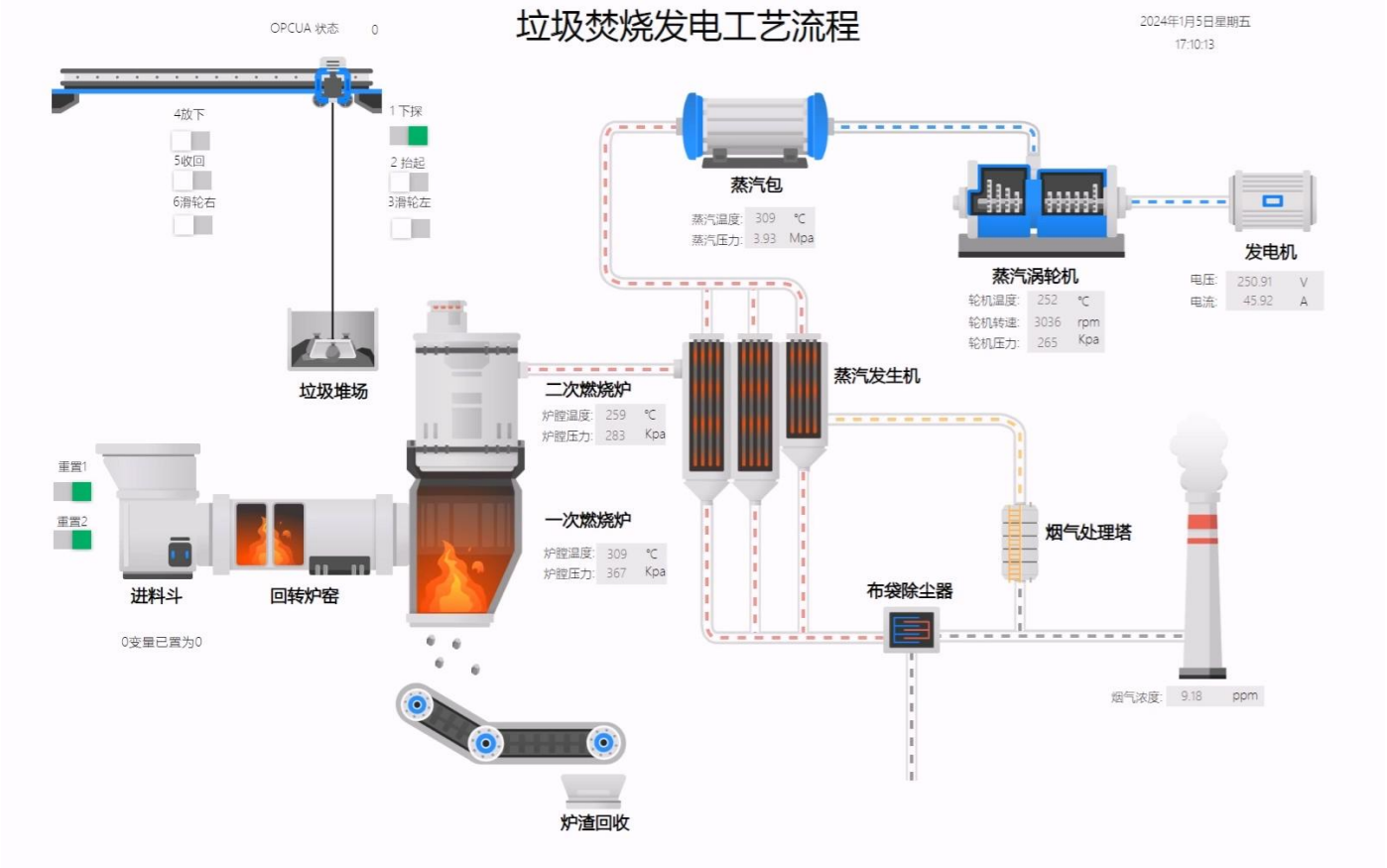


This product integrates a Node-RED-based visual programming environment, providing a graphical, drag-and-drop workflow development approach, greatly simplifying the development of data acquisition and edge computing logic for industrial equipment. The system includes a rich set of built-in protocol nodes, including PLC-specific and CNC protocols, Modbus TCP, Modbus RTU, and other common industrial communication protocols; TCP, UDP, HTTP, MQTT, and other common network communication protocols; and IEC104, DL/T645, CJ188, and HJ212. Data acquisition and logic processing are supported via network, serial, and local I/O ports. Users can configure data parsing, format conversion, edge

computing, and business logic orchestration, and upload processed data to various cloud platforms or third-party servers. Complex control logic can also be implemented locally on the gateway, meeting the requirements of edge intelligence and real-time control. For detailed instructions on using the visualization, please refer to:
https://iotrouter.yuque.com/r/organizations/homepage

8. WEB Configuration





This product features a powerful ***web configuration editor***, allowing users to build online data visualization interfaces for industrial sites via a browser. Configuration features include a rich set of graphical components, allowing users to flexibly configure dashboards, graphs, status indicators, and other elements for real-time display and historical review of collected data. The interface supports multi-level page navigation and dynamic binding, adapting to monitoring needs in diverse scenarios. All configuration screens are directly accessible via the web, eliminating the need for additional client installation. This facilitates remote operation and maintenance and centralized management, significantly improving visibility and ease of operation for device operating status. For detailed instructions on using web configuration, please refer to https://iotrouter.yuque.com/r/organizations/homepage

Note: The [WEB Configuration] feature is only supported on the EG8200Pro/EV8010.

III. Remote Management (IOTClient User Manual)

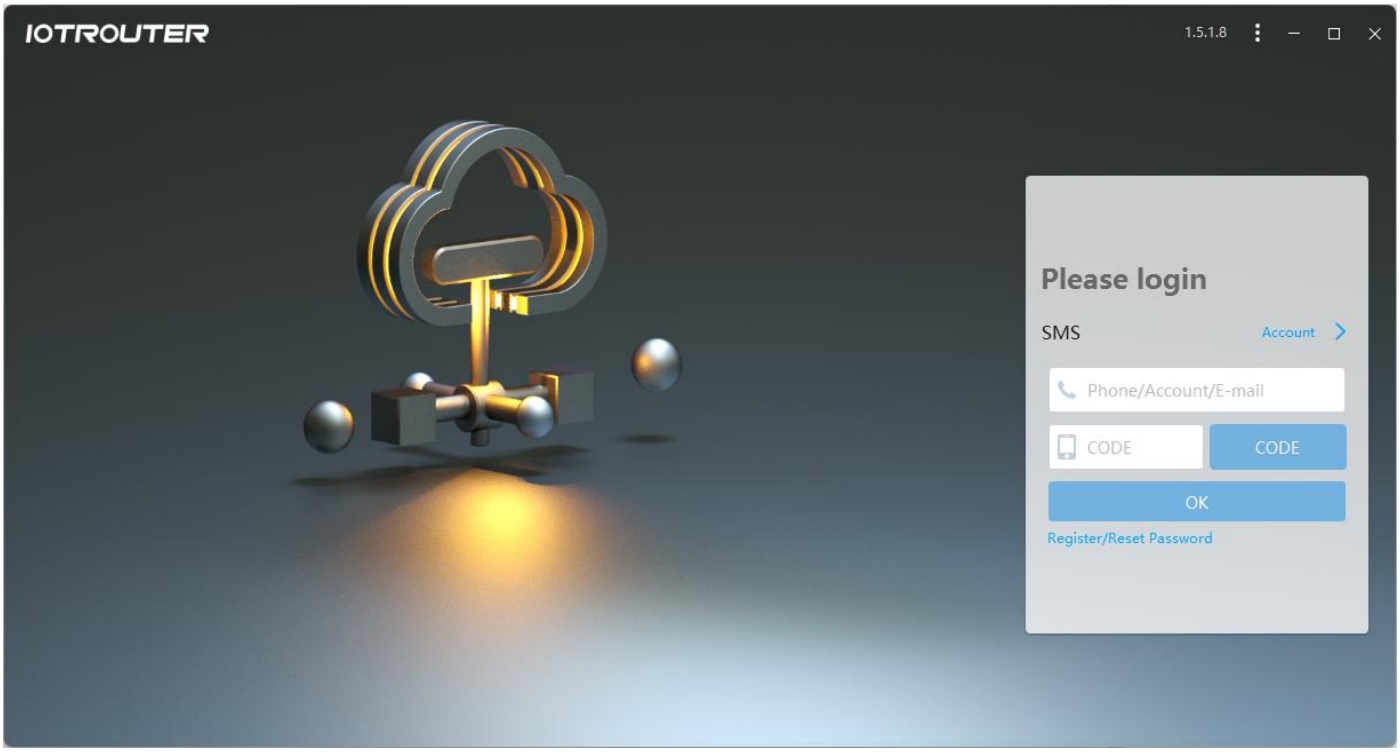
1. Software Download

View https://www.iotrouter.com/product/ click ***Downloads*** to access the download page. You can download

the EG/EV series remote management software.

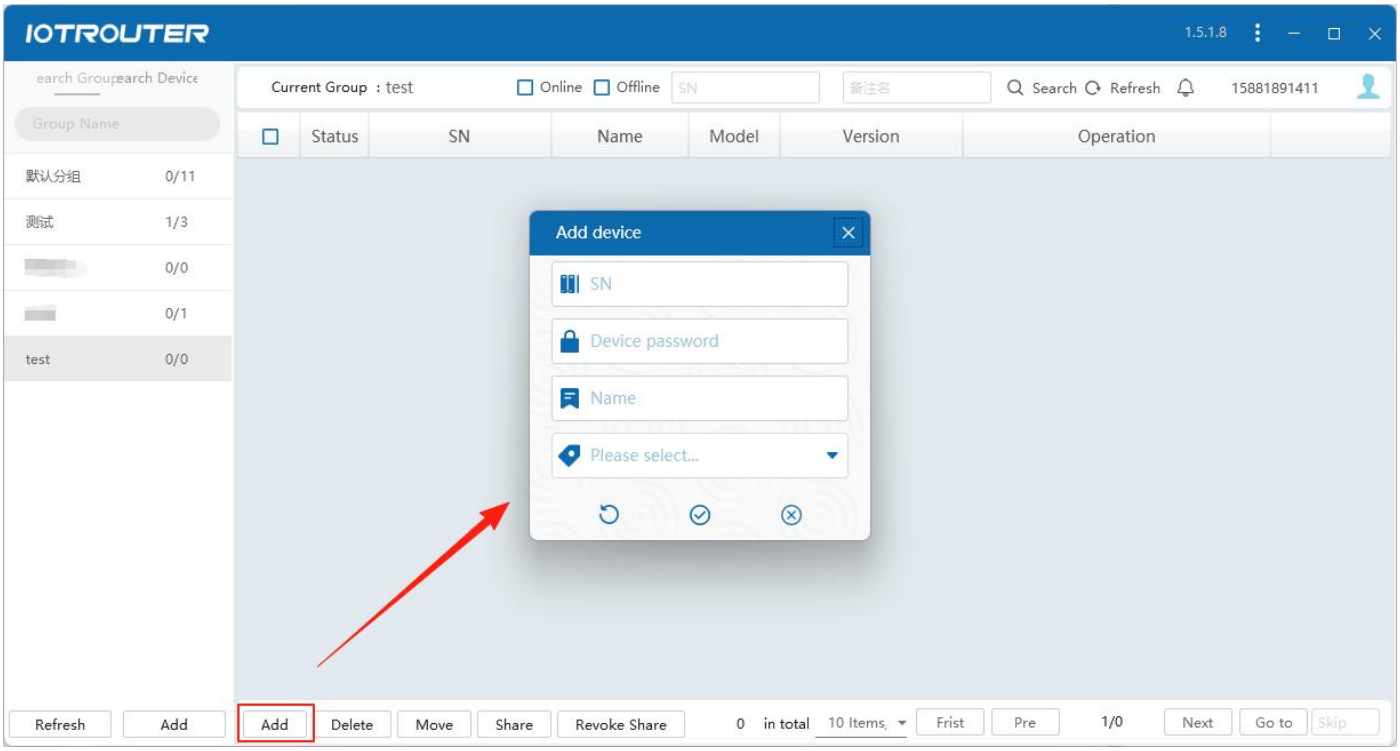
2. Account Login

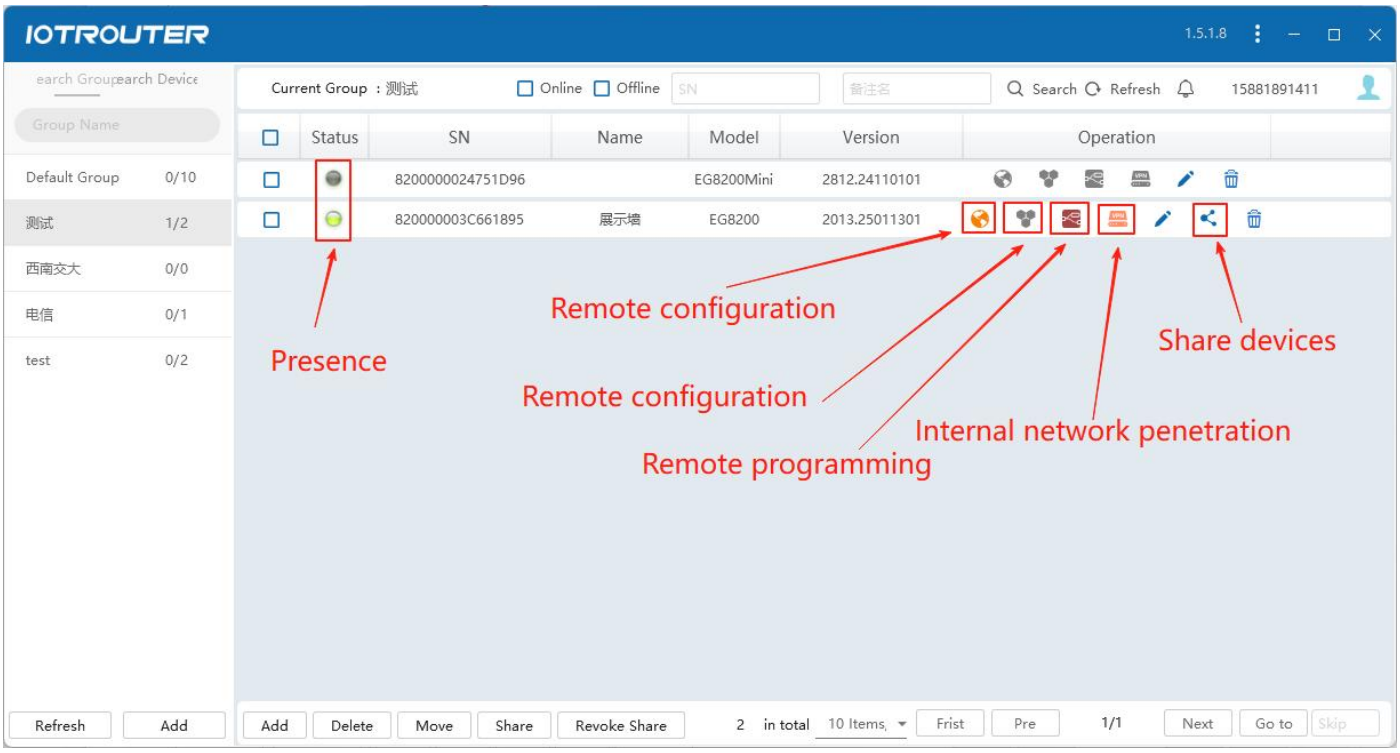
Open the remote software and log in using your account and password.



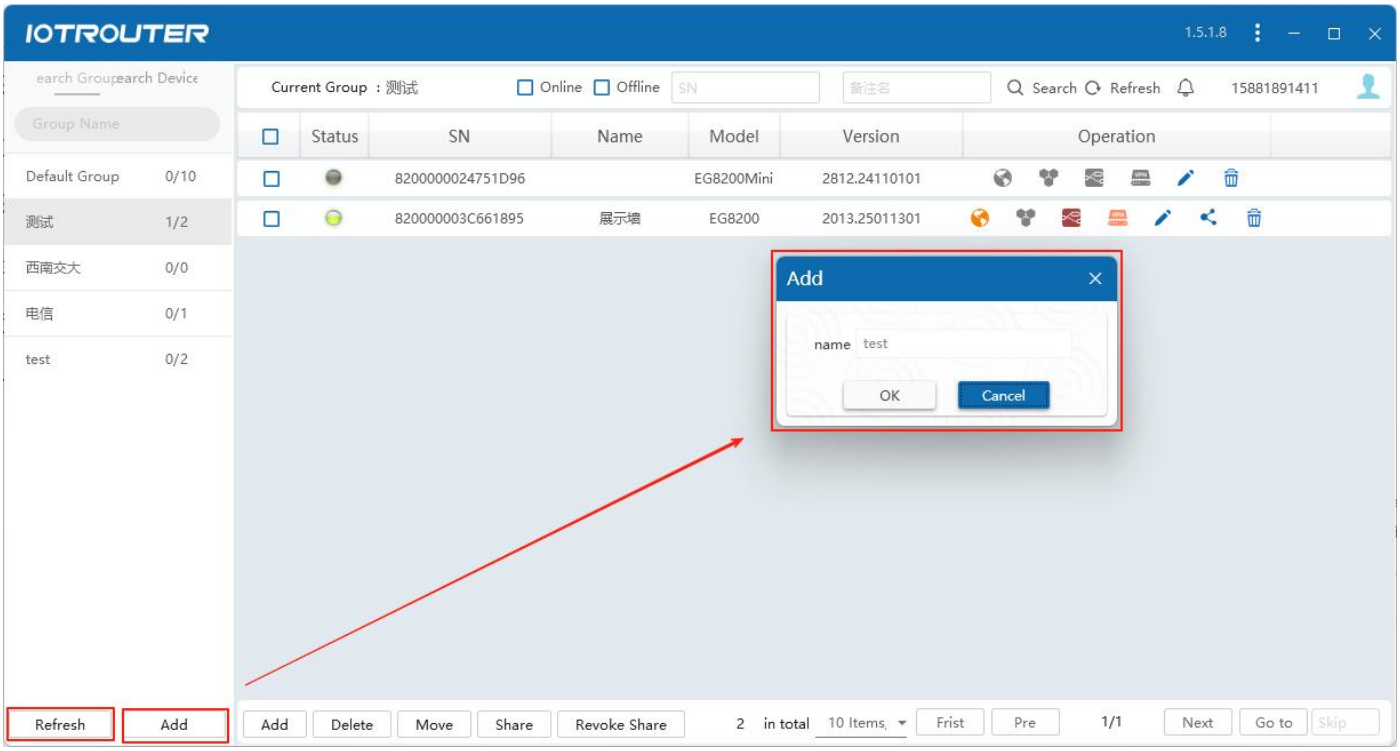
3. Add a device

After logging in, click Add Gateway in the lower left corner. Enter the SN for the gateway's unique serial number, the password for the web login password, and the name as Custom for easy memorization. Once you're finished, click Done. (Each gateway has a unique SN and password. Once a gateway is bound, no one else can bind it again unless the owner deletes the gateway from their account.)



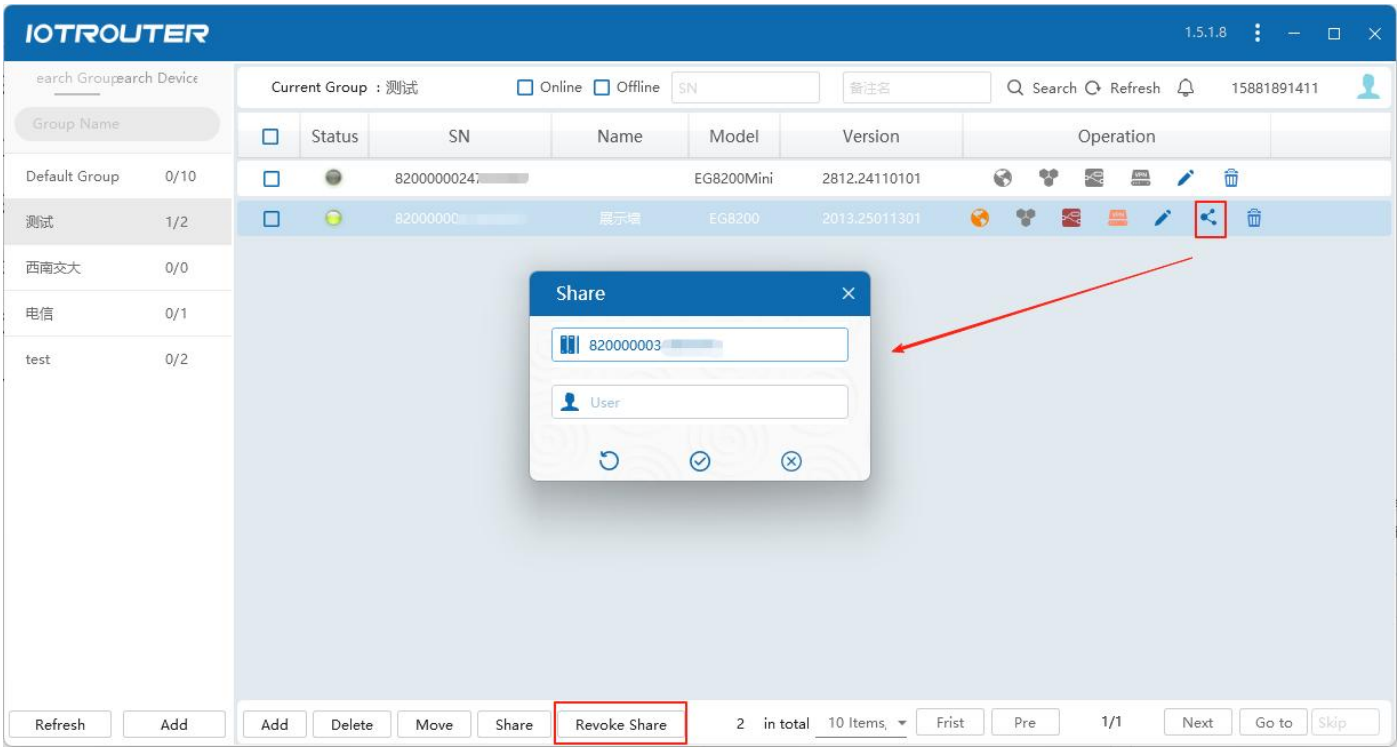


4. Group management



- Can create multiple groups to manage your gateways. If the corresponding group doesn't appear on the left after creating a new group, click Refresh Group.

5. Device Sharing

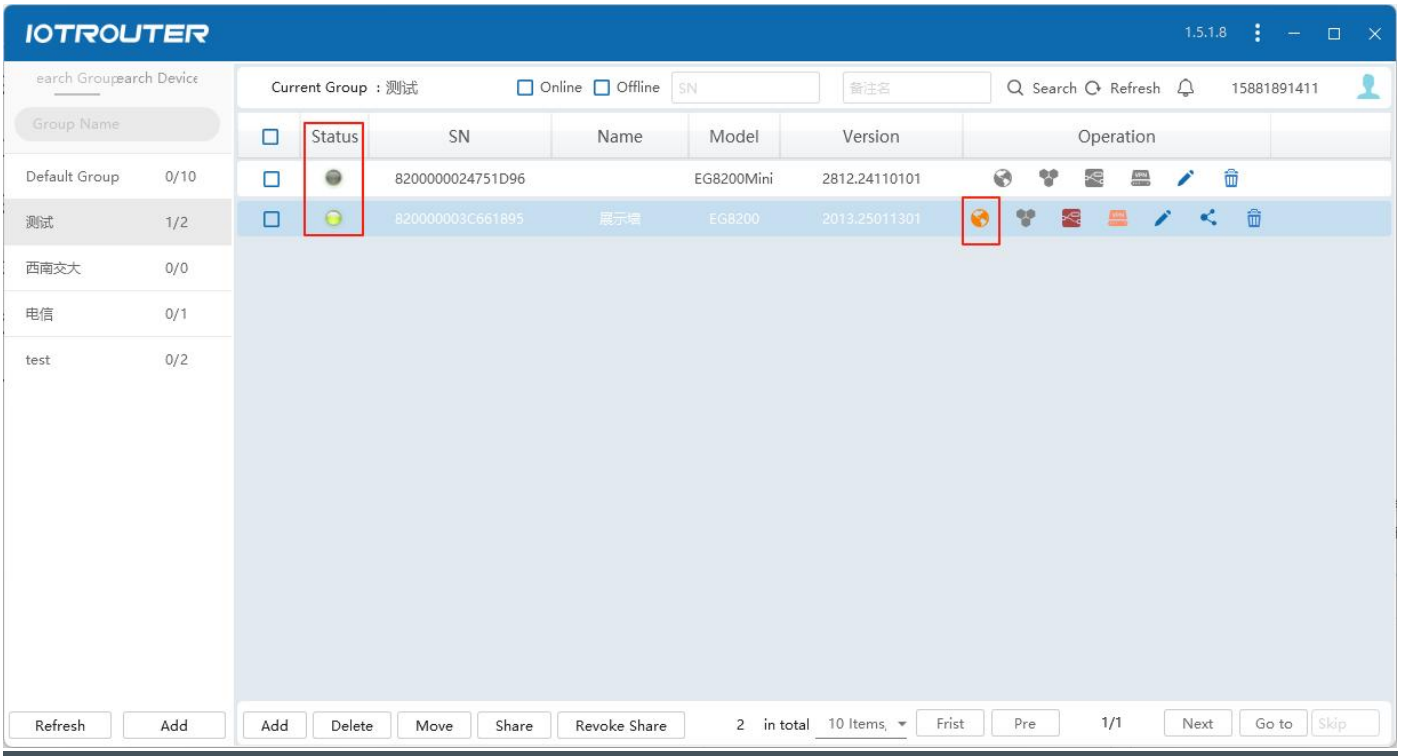


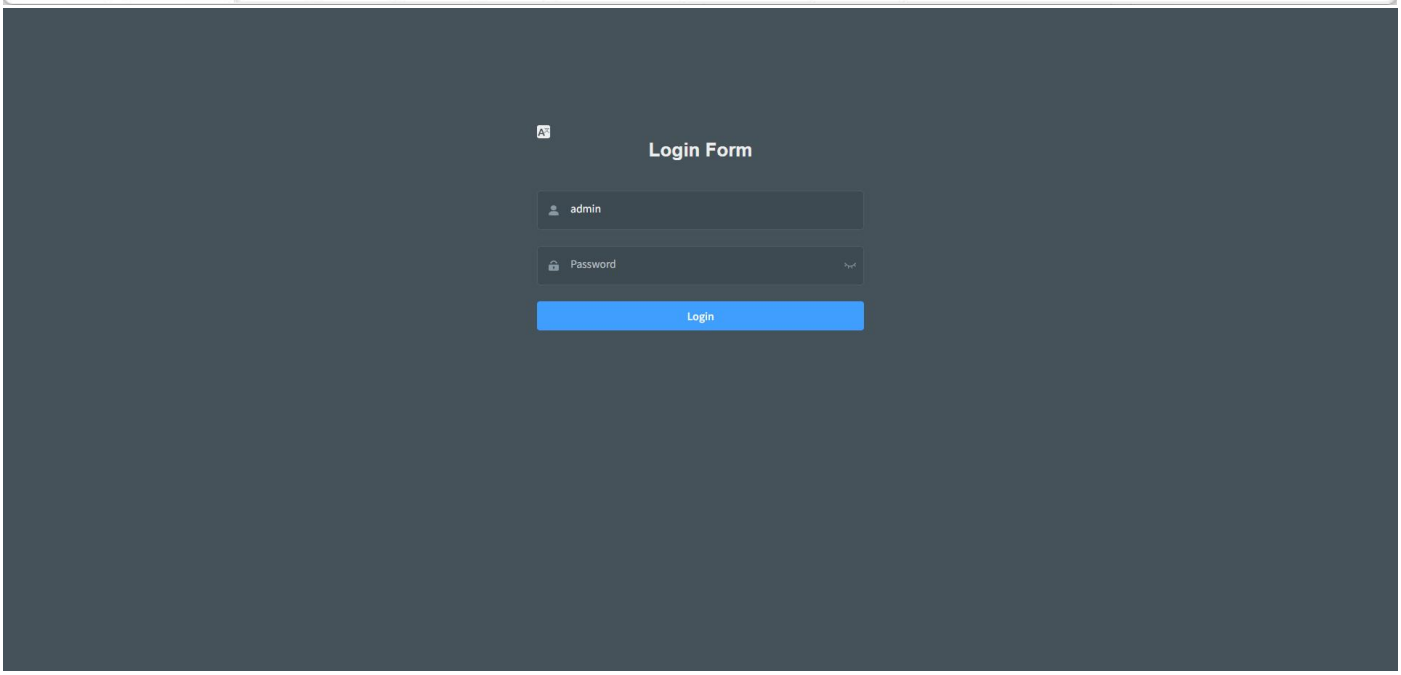
- Sharing Devices: Can share a gateway added to your primary account with a sub-account (a gateway can only be shared with one sub-account).

The sub-account can then remotely configure and program the gateway.

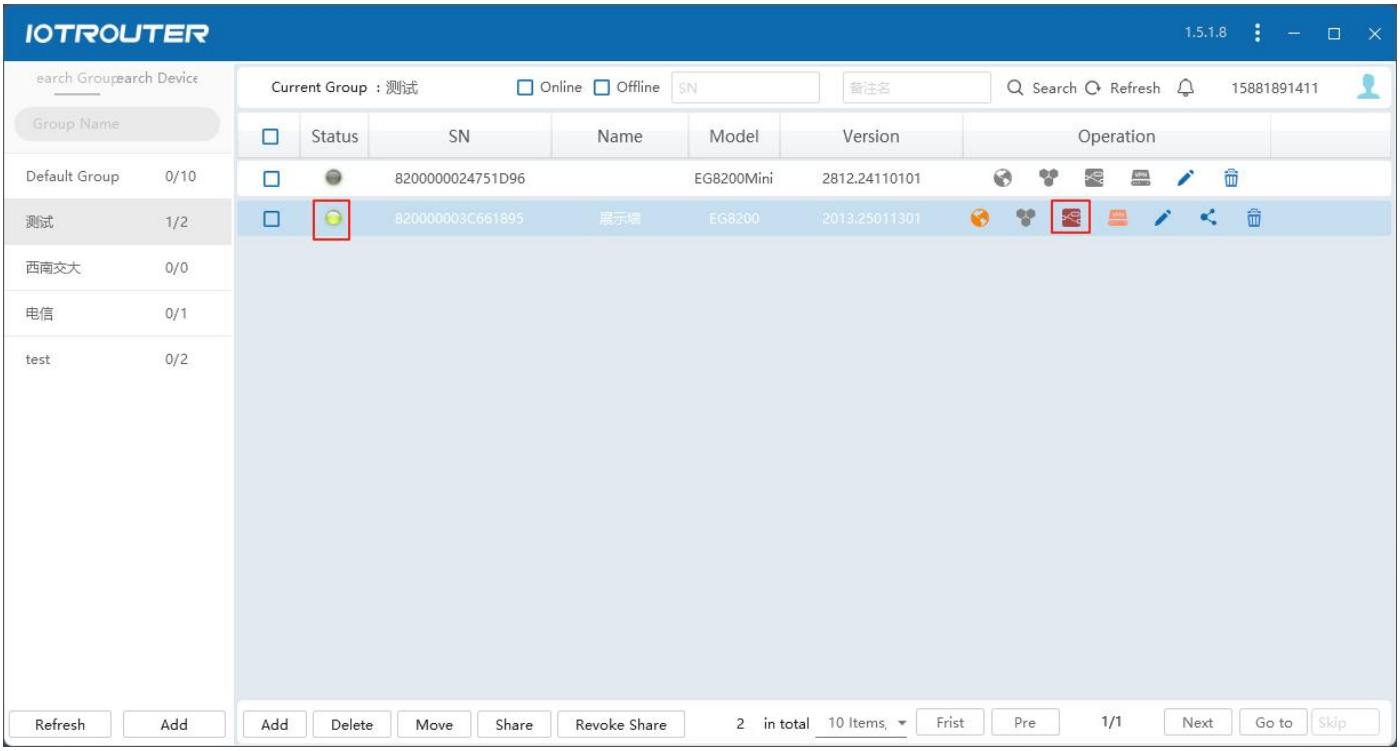
6. Remote Configuration and Programming

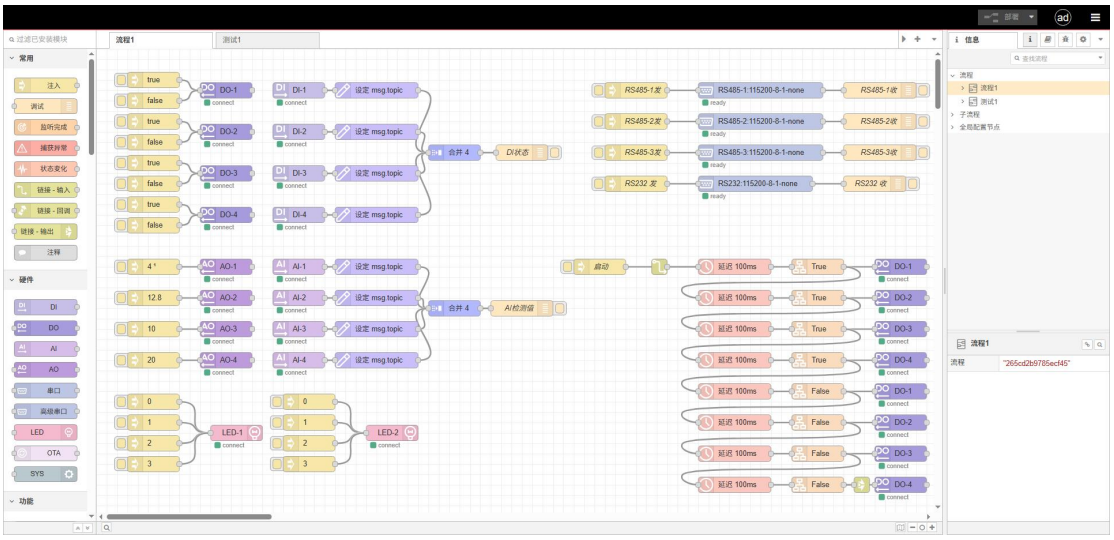
- Remote Configuration: Ensure the gateway is online and the status is green. Clicking the remote configuration button will automatically open a browser and redirect to the gateway's configuration interface.





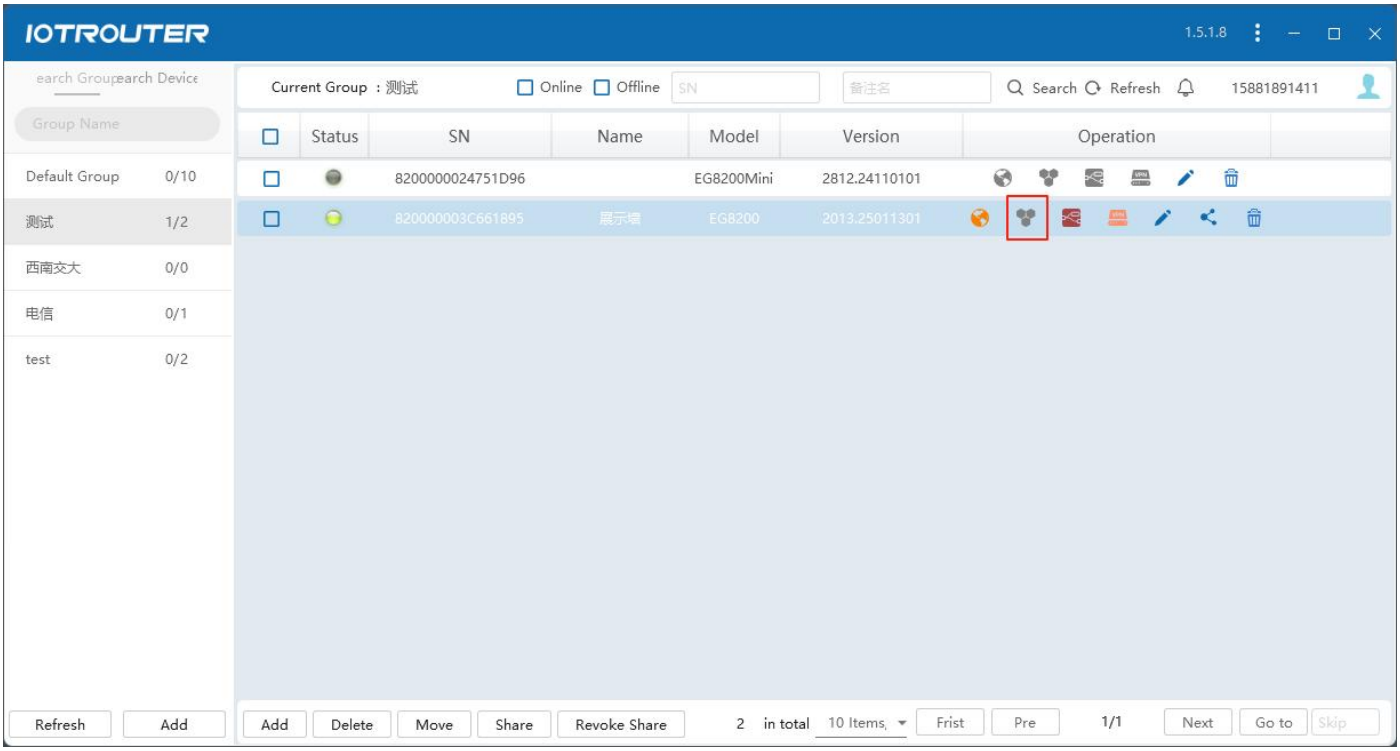
- Remote programming: Click the remote programming button to automatically open the browser and jump to the programming interface of the gateway.

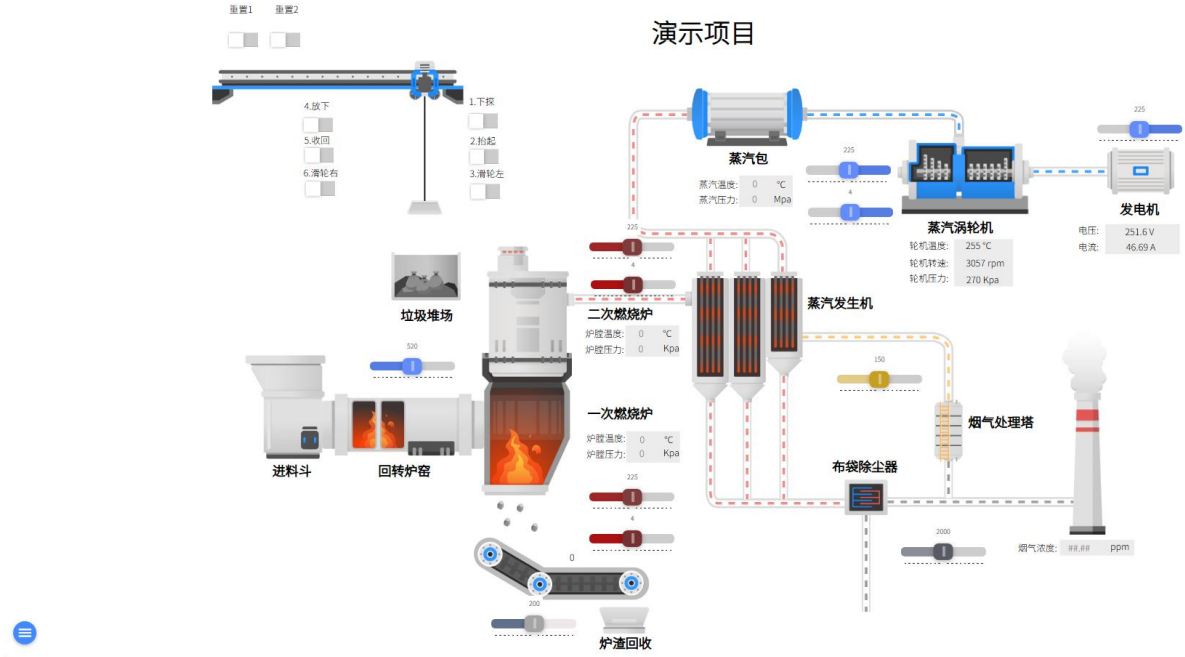




- Remote Configuration: Clicking the Remote Configuration button will automatically open a browser and redirect to the gateway's web configuration interface.

(Note: This feature is only available for gateways that support WEB configuration.)

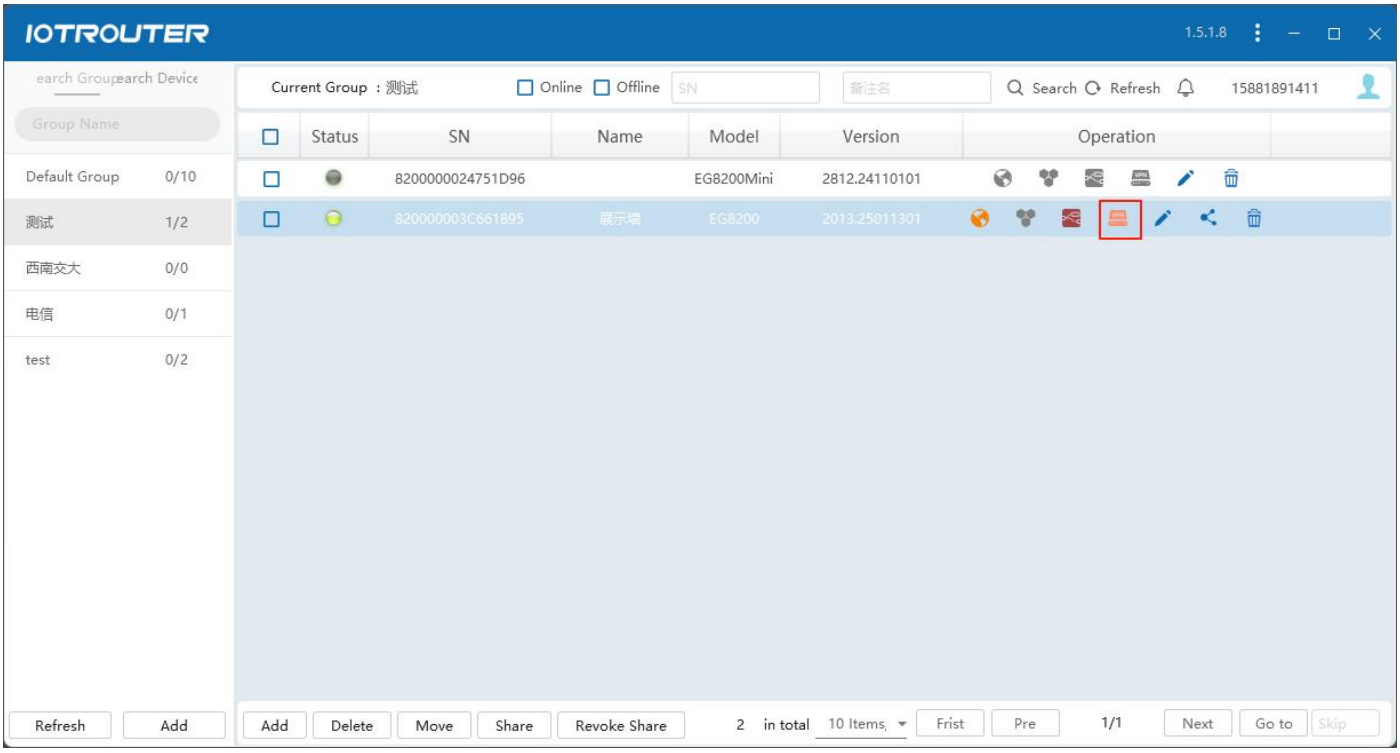


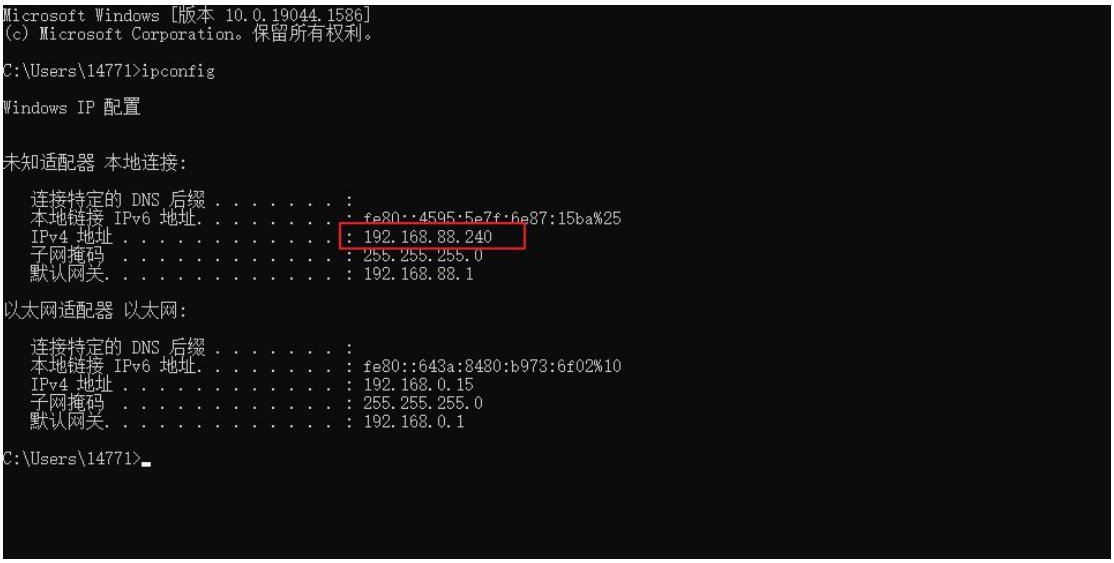


7. Intranet Traversal

Click Remote LAN to enable intranet traceback. The software will automatically install a virtual network card on your local computer, and the gateway will assign an IP address to this computer. The network segment of the assigned IP address is the same as the gateway's LAN port (the LAN port IP address can be

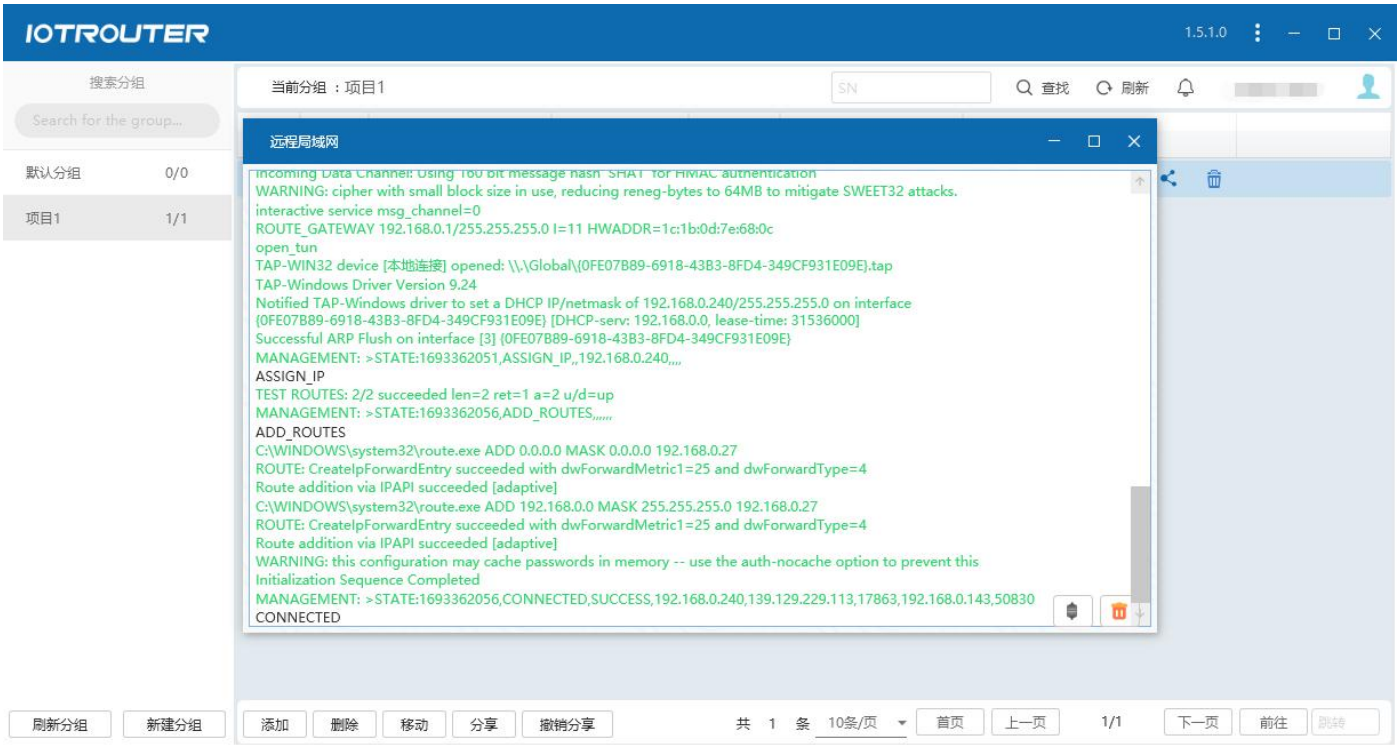
changed).





The IP is assigned successfully, and the local machine can directly access the LAN where the gateway is located.

Note: The network segment used by the computer cannot be the same as the gateway network segment, otherwise it may cause the remote LAN to fail. the interface opened by the remote software cannot be closed. After closing it, the intranet penetration will be disabled.


IOTROUTER
1.5.1.0
搜索分组
Search for the group...
默认分组 0/0
项目1 1/1
当前分组 ：项目1
SN
查找
刷新
远程局域网
Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
WARNING: cipher with small block size in use, reducing reneg-bytes to 64MB to mitigate SWEET32 attacks.
interactive service msg_channel=0
ROUTE_GATEWAY 192.168.0.1/255.255.255.0 I=11 HWADDR=1c:1b:0d:7e:68:0c
open_tun
TAP-WIN32 device [本地连接] opened: \\.\Global\{0FE07B89-6918-43B3-8FD4-349CF931E09E}.tap
TAP-Windows Driver Version 9.24
Notified TAP-Windows driver to set a DHCP IP/netmask of 192.168.0.240/255.255.255.0 on interface
{0FE07B89-6918-43B3-8FD4-349CF931E09E} [DHCP-serv: 192.168.0.0, lease-time: 31536000]
Successful ARP Flush on interface [3] {0FE07B89-6918-43B3-8FD4-349CF931E09E}
MANAGEMENT: >STATE:1693362051,ASSIGN_IP,,192.168.0.240,,,,
ASSIGN_IP
TEST ROUTES: 2/2 succeeded len=2 ret=1 a=2 u/d=up
MANAGEMENT: >STATE:1693362056,ADD_ROUTES,,,,,,
ADD_ROUTES
C:\WINDOWS\system32\route.exe ADD 0.0.0.0 MASK 0.0.0.0 192.168.0.27
ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=25 and dwForwardType=4
Route addition via IPAPI succeeded [adaptive]
C:\WINDOWS\system32\route.exe ADD 192.168.0.0 MASK 255.255.255.0 192.168.0.27
ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=25 and dwForwardType=4
Route addition via IPAPI succeeded [adaptive]
WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Initialization Sequence Completed
MANAGEMENT: >STATE:1693362056,CONNECTED,SUCCESS,192.168.0.240,139.129.229.113,17863,192.168.0.143,50830
CONNECTED
刷新分组
新建分组
添加
删除
移动
分享
撤销分享
共 1 条
10条/页
首页
上一页
1/1
下一页
前往

Version: 1.0

Leading Provider of IO and OT Integrated Products

Sales & Support :

7-Mars Technology Co., LTD.

66/1270 Moo. 2 Khu Fang Nuea, Nong Chok District, Bangkok, Thailand 10530

Support： +66 096 4501250

Web： www.7-mars.com

Email： info@7-mars.com

ใช้คิวอาร์โค้ดหรือลิงก์เพื่อให้ผู้ใช้คนอื่นเพิ่มคุณเป็นเพื่อน