DHCS User Guide

release v1.0.0

1. Organization & Accounts

1.1. Organization

An Organization is the top-level logical unit within the platform for resource isolation, data isolation, and personnel management.

- In **Tenant Mode**: Each tenant is an independent organization. For example: different branches, customers, or project groups can be set up as separate tenants. Data (such as devices, configurations, alarms) between tenants is completely isolated, enabling secure and independent operation of multiple customers or departments on the same platform.
- In **Private Mode**: The entire platform has only one private organization. All resources, data, and users are centrally managed under this organization, suitable for internal network operation and maintenance scenarios for a single management entity.

1.2. Roles

1.2.1. Built-in Roles

The system pre-configures the following three out-of-the-box role templates for administrators to quickly assign to users:

- **Administrator**: Has full management and operational permissions for all functions within the jurisdiction (platform or tenant).
- **Technical Support**: Has broad menu permissions; requires network authorization to view and operate certain functions.
- **Regular User**: A basic set of permissions, typically related to business processing. Administrators can create custom roles based on this role.

1.2.2. Custom Roles

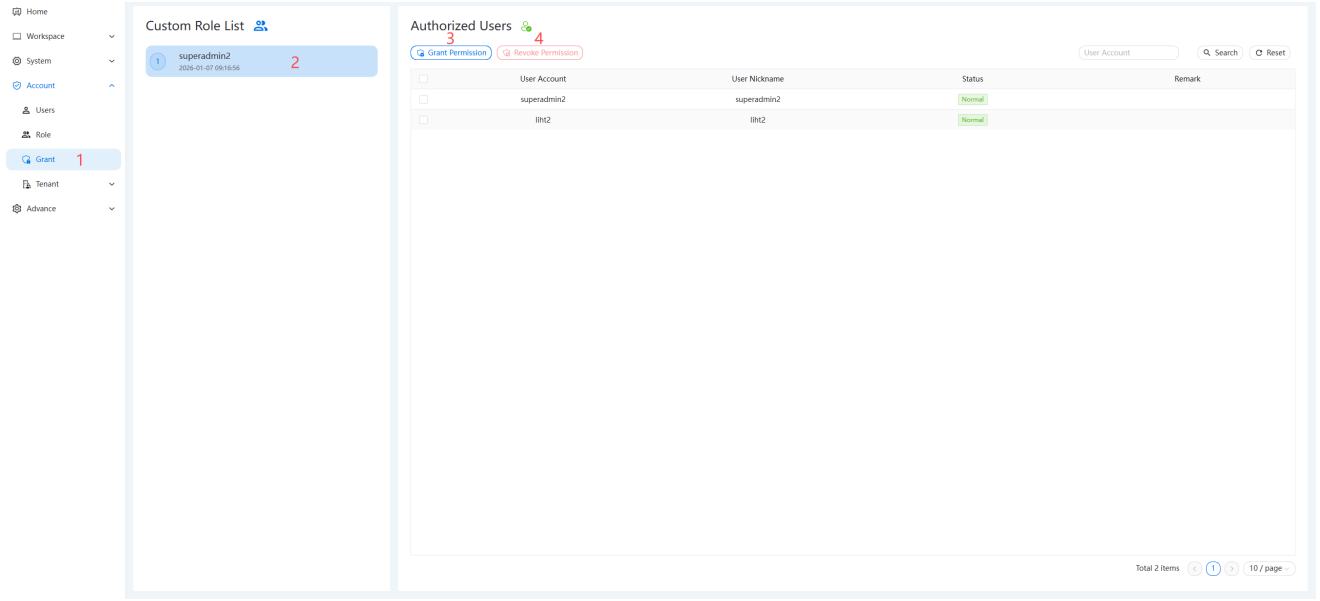
Administrators can create custom roles based on actual operational division of labor. During creation, permissions for various platform functions (e.g., "Device Management - Read-Only", "Configuration Management - Read/Write", "Alarm - Read-Only") can be finely selected or deselected, thus precisely matching the responsibilities of specific positions like "Network Monitor", "Configuration Engineer", etc.

> **Note**

- The authorization relationship with accounts under a role must be removed before deleting that role.
- Only custom roles can be deleted; built-in roles cannot be deleted.

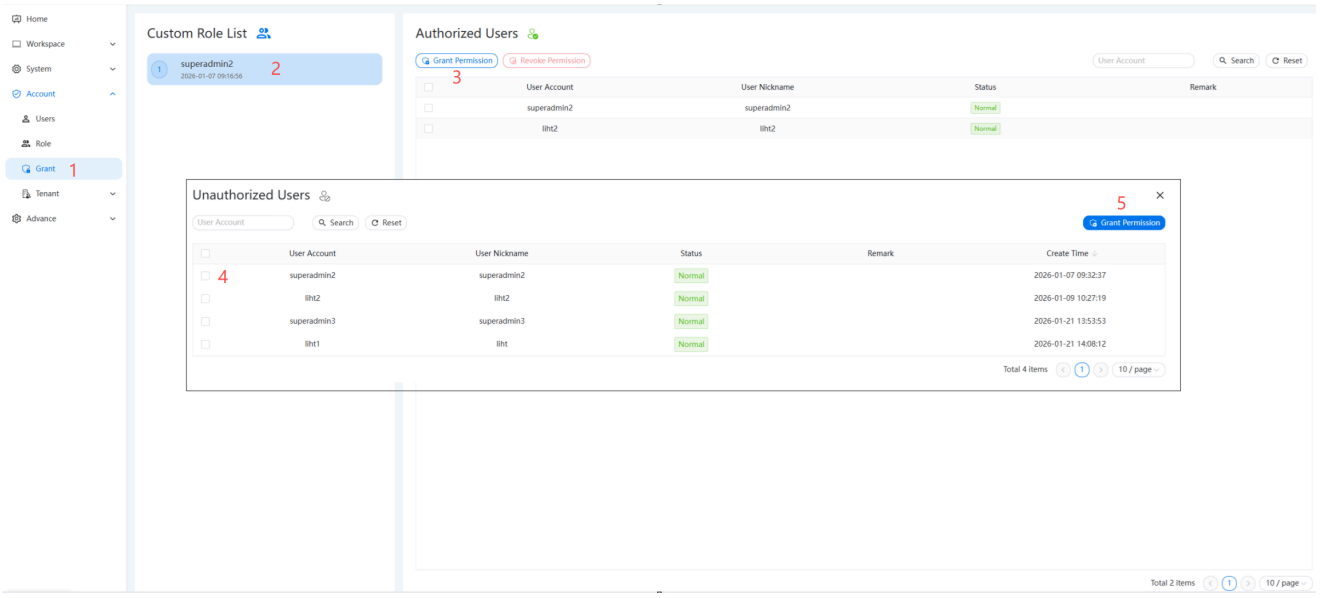
1.2.3. Role Authorization

Custom roles can be authorized to users within the same organization. In the Account Authorization module, select a custom role from the left-hand role list; the list on the right will display accounts already authorized with that selected role. As shown in the figure:



▲*Figure 1: Authorized Accounts*

Click the "Grant Permission" button to pop up the list of unauthorized accounts. Select the relevant accounts to authorize. As shown in the figure:



▲*Figure 2: Unauthorized Accounts*

1.2.4. Permission Revocation

In the Account Authorization module, select a custom role from the left-hand role list; the list on the right will display accounts already authorized with that selected role. Select the account(s) from which permissions need to be revoked and click the "Revoke Authorization" button.

1.3. Accounts

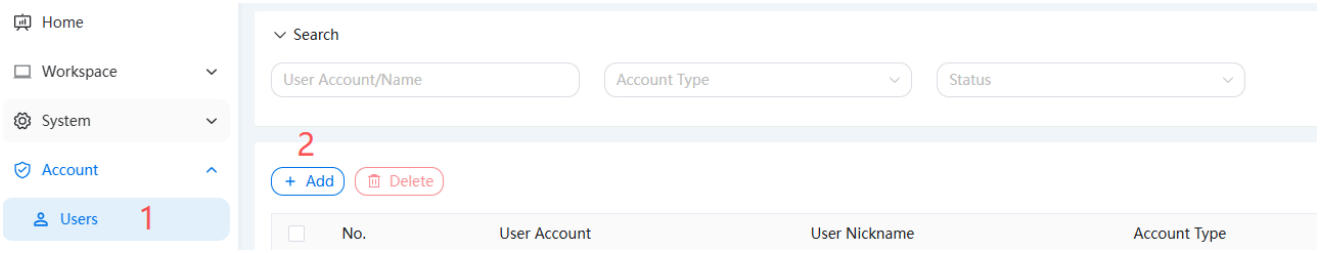
1.3.1. Account Types

Account Type	Description
Platform Administrator	1. In tenant mode, the platform administrator is primarily responsible for configuring system operation parameters to ensure the normal operation of the platform, including platform license, platform name, IP, operation mode, etc. 2. In non-tenant mode, the platform administrator has the highest permissions for all modules and all data.
Tenant Administrator	Responsible for managing members and devices of each tenant. Tenant administrator accounts are opened via registration.
Regular User	Primarily responsible for maintaining devices under the network, monitoring device operation status, device upgrades, initial deployment, configuration command issuance, and other maintenance tasks. In tenant mode, regular users are tenant members invited by the tenant administrator. In non-tenant mode, they are created by the platform administrator.
Technical Support	Technical support by default only has business menu permissions without data permissions. When a user authorizes technical support for a specific network, technical support can view and operate devices under that network.

▲*Table 1: Account Types*

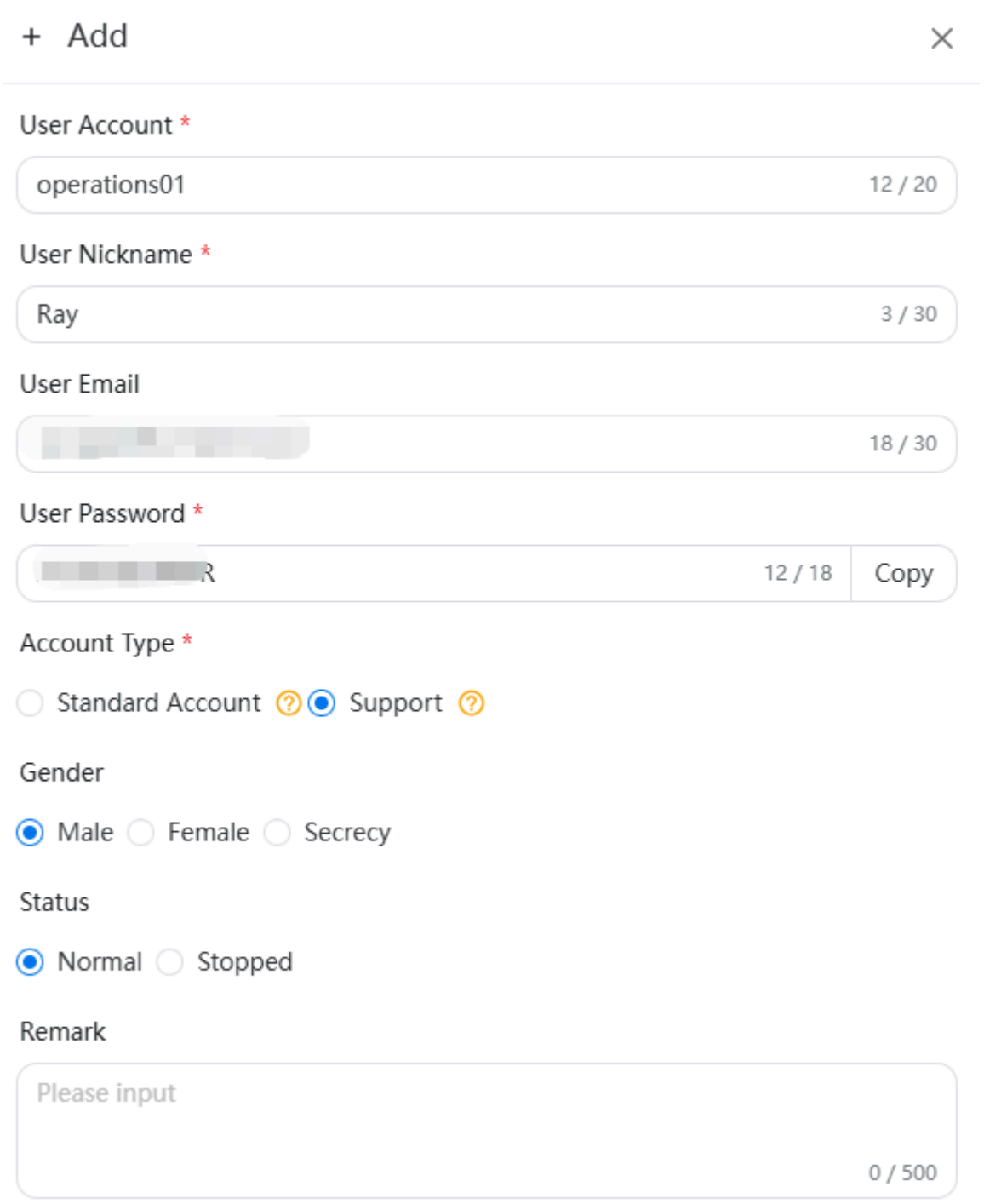
1.3.1. Adding Regular Users

The platform administrator clicks the "Add" button in the User Management module to show the add interface. Navigate to "Account Permissions -> User Management" to enter the User Management page, then click the "Add" button.



▲*Figure 3: User Management*

The system randomly generates an initial password for the account. Enter the user account, name, select the regular user account type, then click the "Confirm" button to complete account creation.



▲*Figure 4: Add User*

After successfully adding the user, the registered email will receive an automatic system notification email. The sender is the email account configured in the system settings.

Please check your account information:

Username: operations01
Password: NZi29t5phUu&

> **Important:**Please keep your account information safe. It is recommended that you go to your personal center immediately after logging in to change your password.

Please click this link to login: **[Login]**

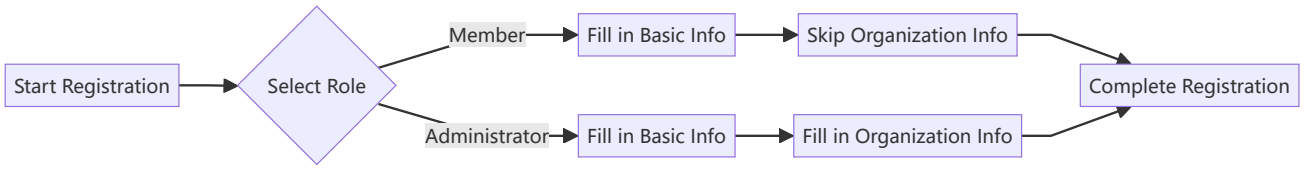
This email is sent automatically by the system. Please do not reply directly.

▲*Figure 5: New User Email Notification*

1.3.2. Creating a Tenant Team

1.3.2.1. Tenant Registration

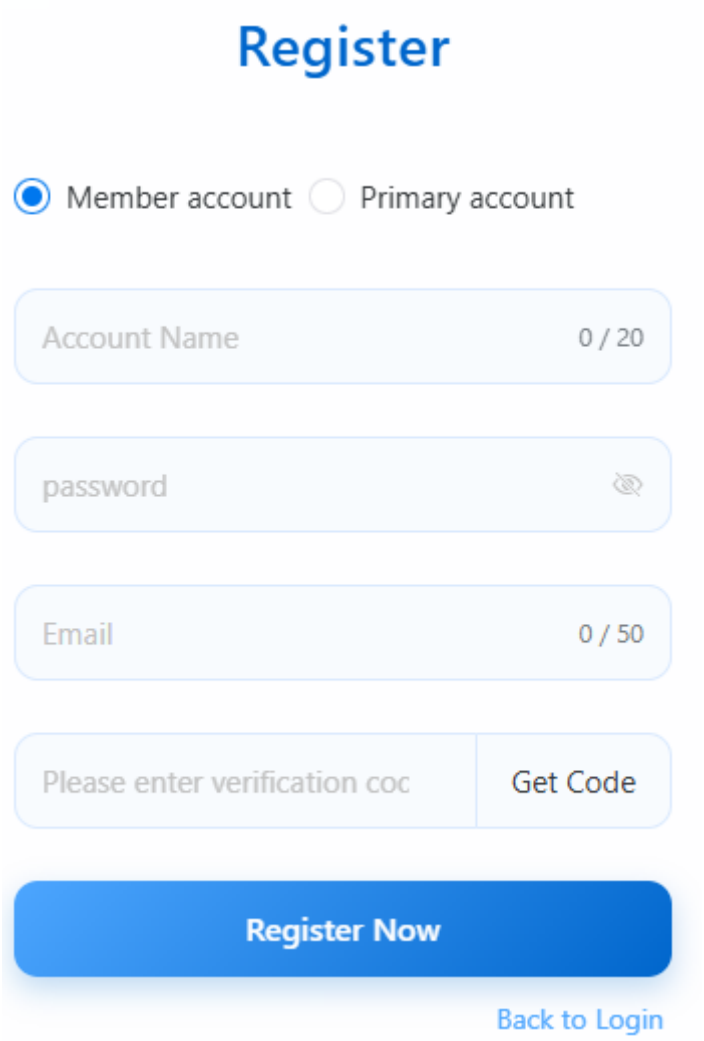
- Registration Process



▲*Figure 6: Registration Flowchart*

- Registration Entry

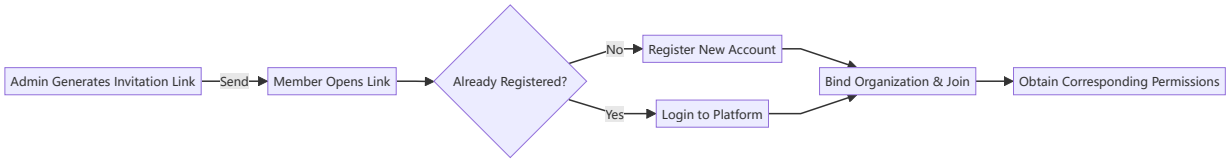
On the login page, click "Register Account" to jump to the Register page. Select the required user type and register with the registration information. The tenant is created when the administrator registers.



▲*Figure 7: Tenant Registration Page*

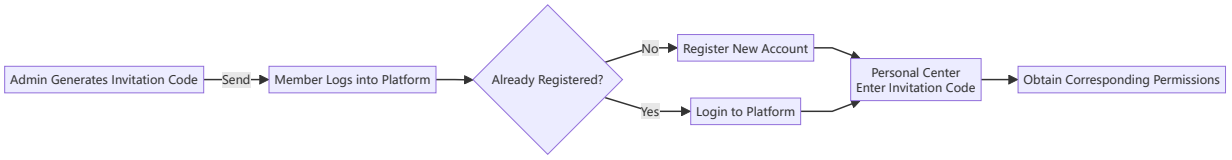
1.3.2.2. Member Joining

- Invitation Link Join Process



▲*Figure 8: Invitation Link Join Flowchart*

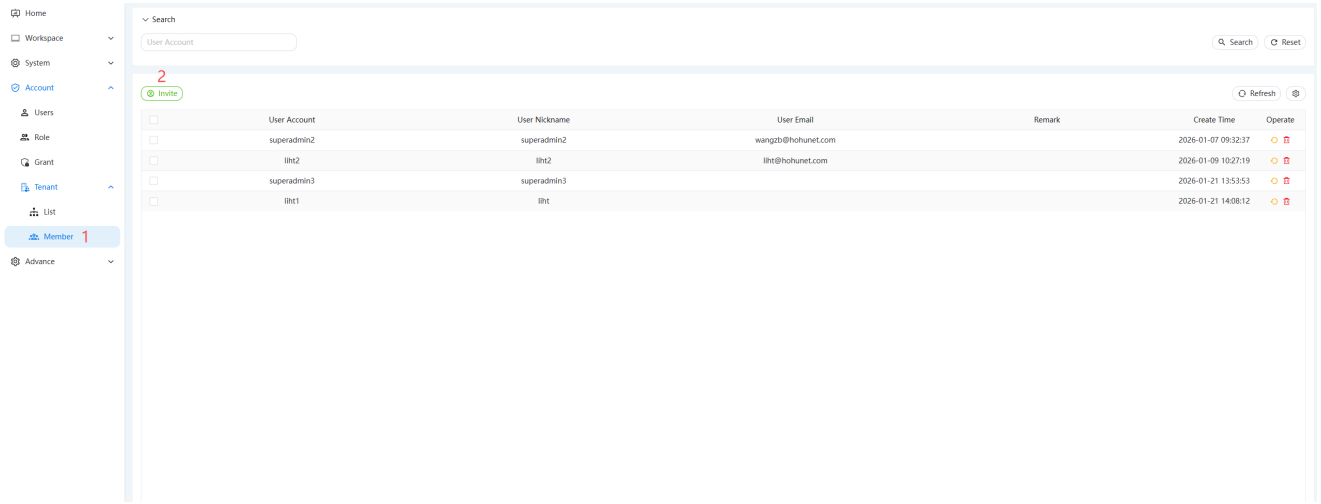
- Invitation Code Join Process



▲*Figure 9: Invitation Code Join Flowchart*

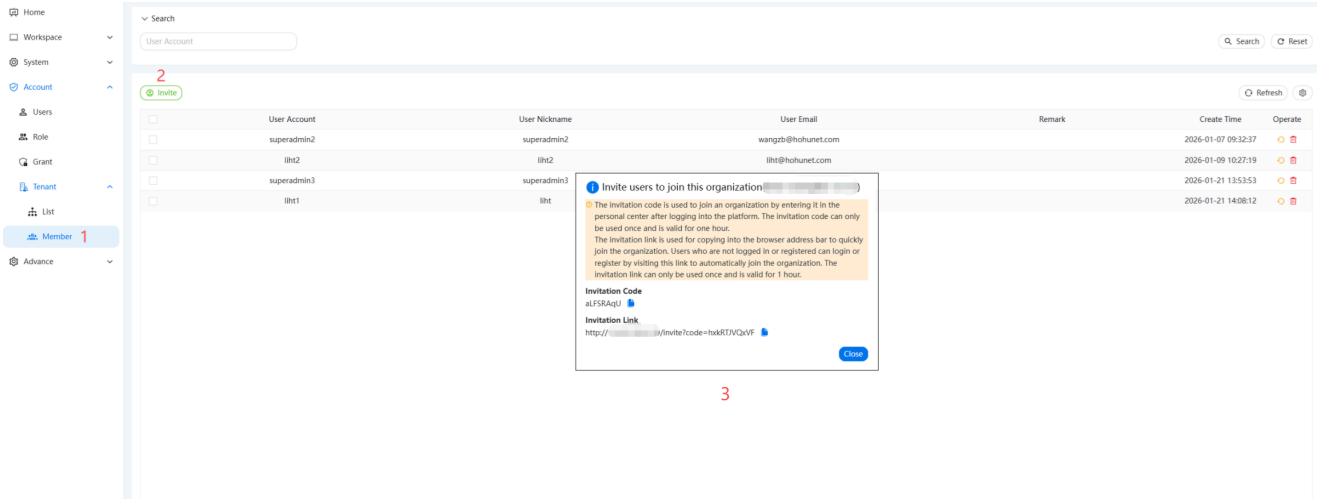
- Generate Invitation Information

Under Tenant Management -> Tenant Members menu, the tenant administrator clicks the "Invite" button, as shown:



▲*Figure 10: Tenant Member Management Page*

The pop-up will display the "Invitation Code" and "Invitation Link". Users can choose freely.



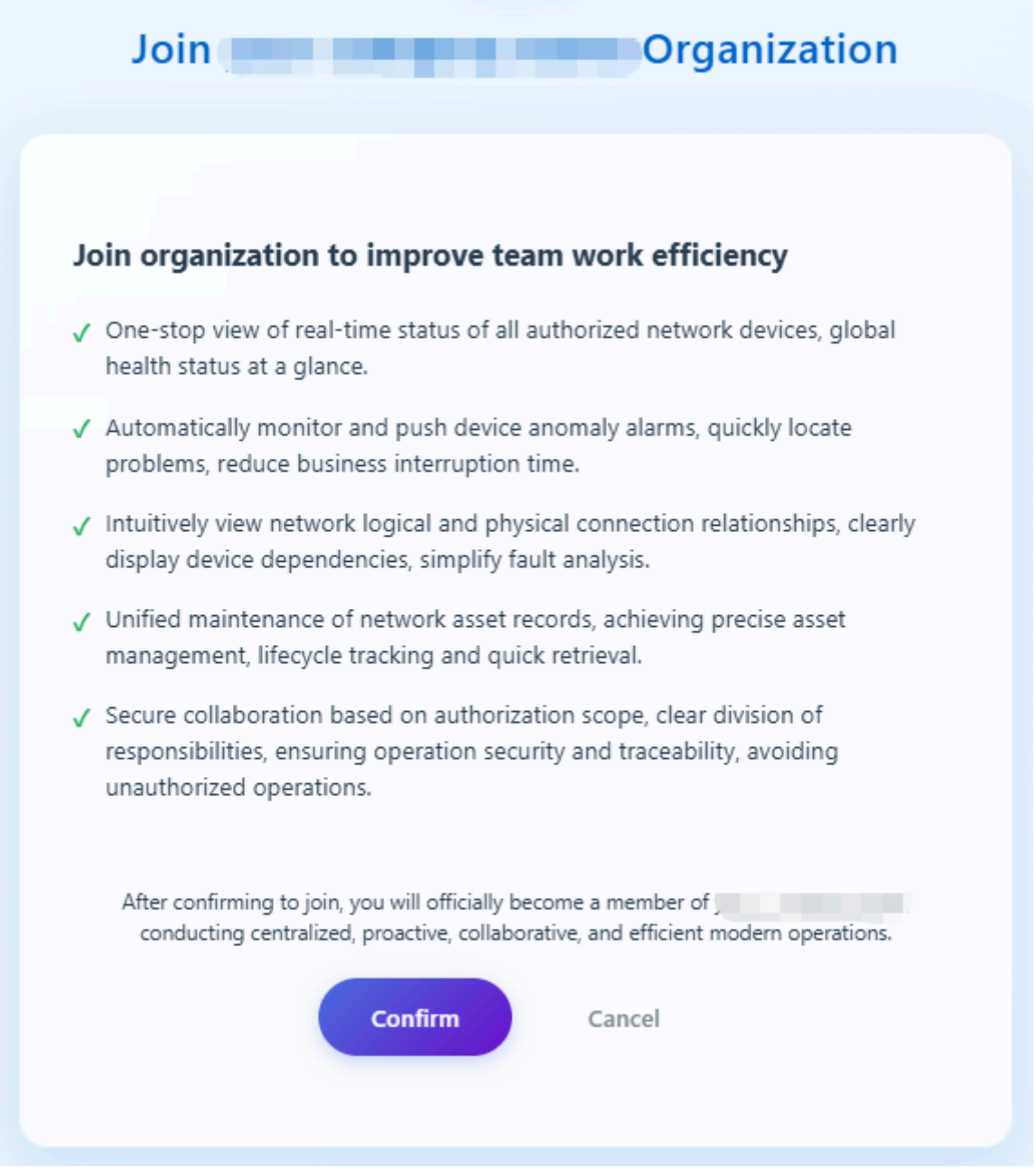
▲*Figure 11: Generate Invitation Link and Code Dialog*

Send the invitation code or link to the user invited to join the organization;

> **Note**
>
> 1. The invitation code and link are valid for 1 hour;
> 2. If a tenant member is not bound to any tenant, logging into the platform will automatically redirect to the Personal Center;

- Joining via Invitation Link

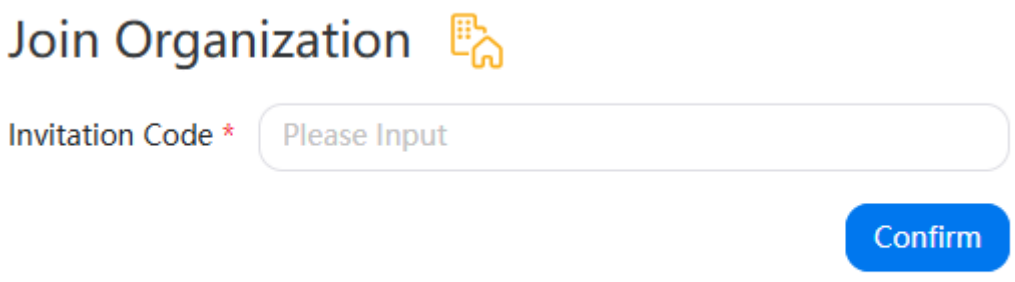
After the invitee logs into the platform and opens the invitation link, click "Confirm to Join Organization" to complete joining the tenant. As shown:



▲*Figure 12: Invitation Link Join Confirmation Page*

- Joining via Invitation Code

After the invitee logs into the platform, click the account icon in the top right -> Personal Center. In the Personal Center's "Join Organization" section, enter the invitation code and click "Confirm" to complete joining the organization. As shown:



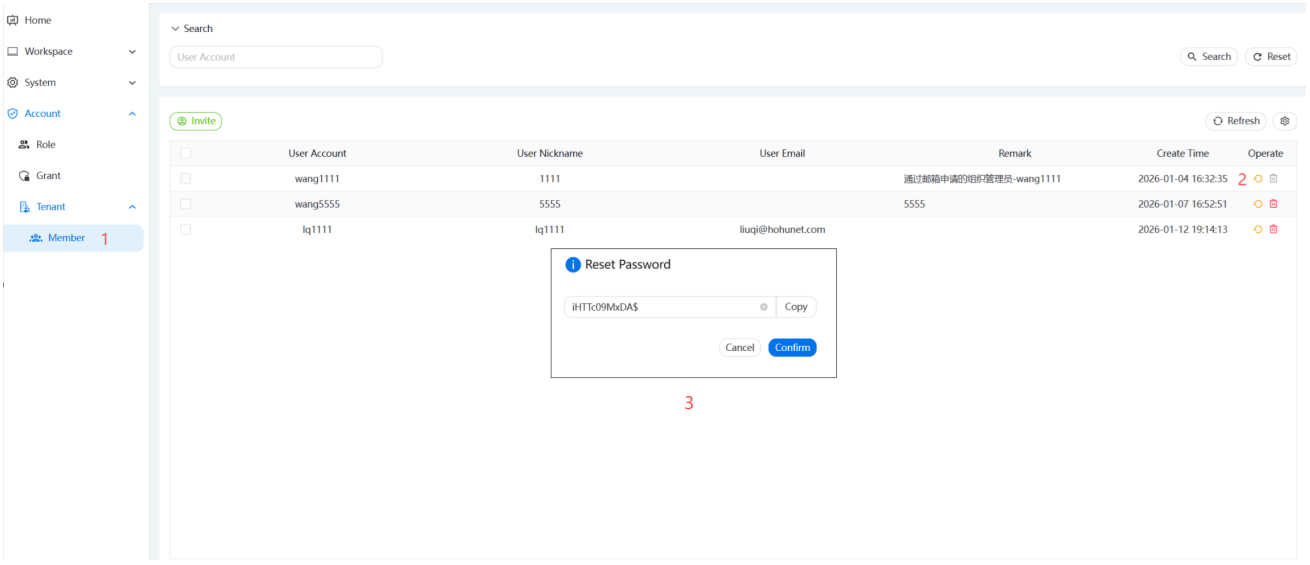
▲*Figure 13: Personal Center Enter Invitation Code Page*

1.3.3. User Account Unlock

In private mode, if a user enters the wrong password 5 times, the account is automatically locked. If you don't want to wait, you can contact the administrator to unlock it. Find the locked account in User Management and click the "Unlock" button in the Actions column to unlock immediately.

1.3.4. Account Password Reset

When a user forgets their password, the administrator can reset it. In tenant mode, the tenant administrator resets it in the Tenant Members module; in private mode, the platform administrator resets it in the User Management module.
Click the "Reset" button in the Actions column of the account list. If the user has not bound an email, a password reset dialog pops up. The system defaults to generating a new password; the administrator can modify and copy it, then click "Confirm" to reset the account password. After resetting, the administrator should send the new password to the user, who should change it promptly after logging in.



▲*Figure 14: Reset Password Dialog*

If the user account is bound to an email, the password modification dialog does not pop up. The system directly generates a random password and sends it to the user's email.

Please check your account information:

Username: superadmin2
Password: Uty9%wRV1qUq

Important: Please keep your account information safe. It is recommended that you go to your personal center immediately after logging in to change your password.

Please click this link to login: **[Login]**

This email is sent automatically by the system. Please do not reply directly.

▲*Figure 15: Reset Password Email Notification*

1.3.5. Default Account Permissions

Function					Private Mode			Tenant Mode			
					Platform Admin	Regular User	Technical Support	Platform Admin	Tenant Admin	Tenant Member	Technical Support
Dashboard					●	●	-	●	●	●	-
Workspace	Network Management	View Permissions	Network List, Network Details, View Topology, Alarm Information, Authorized Members, Authorized Technical Support, Key Port List		●	●	○	●	●	●	○
		Basic Operations	Create/Delete/Edit Network, Set Hostname, Edit Topology, Unmanaged Device Management, Transfer, Transfer Confirmation, Transfer Report, Alarm Deletion		●	●	-	●	●	●	-
		Network Authorization	Regular User Authorization		●	-	-	●	●	-	-
			Technical Support Authorization		●	●	-	●	●	●	-
		Device Binding	Bind, Quick Bind		●	●	-	●	●	●	-
		Alarm Settings	Traffic Alarm		●	●	-	●	●	●	-
			Notification Method		●	●	-	●	●	●	-
			Contact Person		●	●	-	●	●	●	-
		Cloud-managed Devices	Device List		●	●	○	●	●	●	○
			Device Information	Device Panel, Port List, Optical Module List, PoE List, Unmanaged Device List, Port Monitoring (excluding traffic alarm settings), Tunnel Management (excluding reconnection), Log Analysis, Running Config, Startup Config, Config Backup List, Config Download	●	●	○	●	●	●	○
			Configuration Management	Configuration Rollback	●	●	-	●	●	●	-
			Port Management	Port Enable/Disable, Port Schedule, Port Tagging	●	●	-	●	●	●	-
			PoE Management	Alarms, Priority, Enable/Disable Switch, Trend Graph, PoE Schedule	●	●	-	●	●	●	-
			Remote Tunnel	Telnet, SSH, HTTP Remote	●	●	○	●	●	●	○
			Polling Frequency Setting		●	●	-	●	●	●	-
			Unbind Device		●	●	-	●	●	●	-
			Reset Device Password		●	●	-	●	●	●	-
	Device Management				●	●	○	●	●	●	○
	Alarm Center	View Alarms			●	●	○	●	●	●	○
	Upgrade Management	Version Upgrade	List		●	●	-	●	●	●	-
			Push Command		●	●	-	●	●	●	-
		Upgrade File	File List		●	●	○	●	●	●	○
			File Maintenance		●	-	-	●	-	-	-
		Upgrade Task	Task List, Chart		●	●	○	●	●	●	○
			Task Activation		●	●	-	●	●	●	-
			Task Closure		●	●	-	●	●	●	-
			Re-push		●	●	-	●	●	●	-
	零配置开局				●	●	-	●	●	●	-
System Man	System Dashboard				●	-	-	●	-	-	-
	Platform Settings				●	-	-	●	-	-	-
	Operation Log				●	-	-	●	●	-	-
	Product Model				●	-	-	●	-	-	-
	Template Library	Email Template			●	-	-	●	-	-	-
		Configuration Template			●	●	-	●	●	●	-
Account & P	User Management				●	-	-	●	-	-	-
	Role Management				●	-	-	●	●	-	-
	User Authorization				●	-	-	●	●	-	-
	Tenant Management	Tenant List			-	-	-	●	-	-	-
		Tenant Members			-	-	-	●	●	-	-

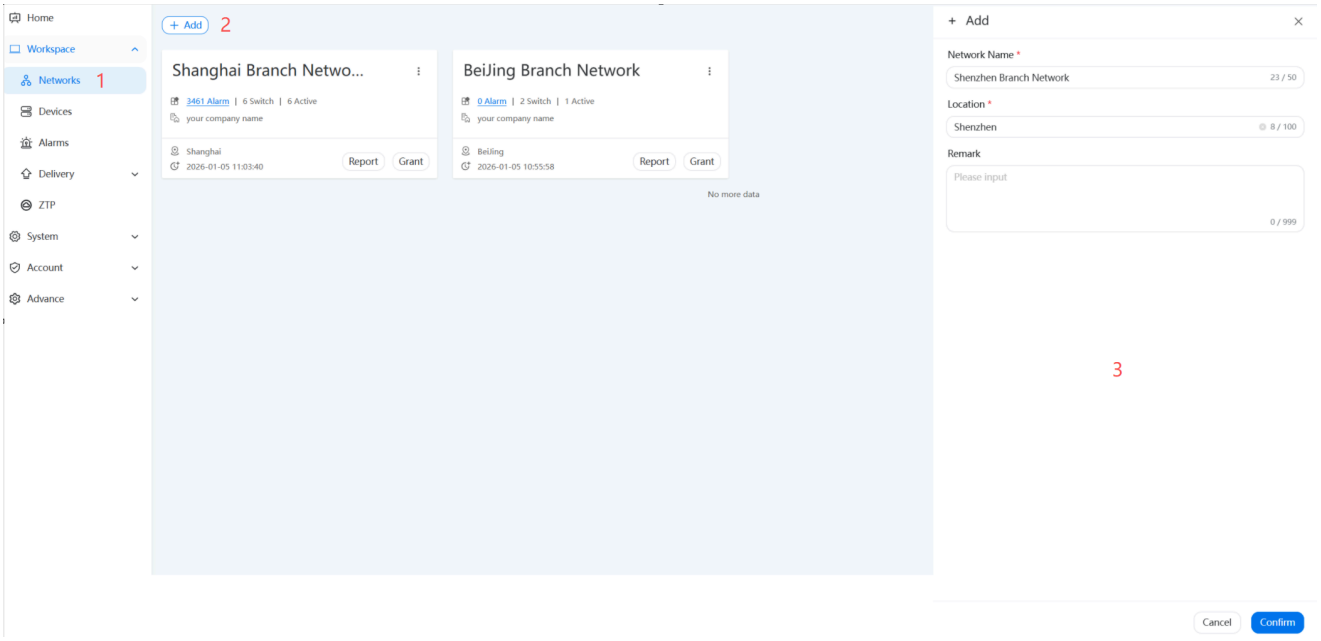
▲*Table 2: Default Account Permissions*

> **Note**
> In the table, ● indicates having permission for that function, ○ indicates only having menu permission for that function, requiring further authorization after being assigned.

2. Creating the First Network

2.1. Add Network

A network must be created in the Network module before devices can be bound to it. Users can create it in the Network module. Click the "Add" button, enter the network name and coverage area location information, and save to complete creation.



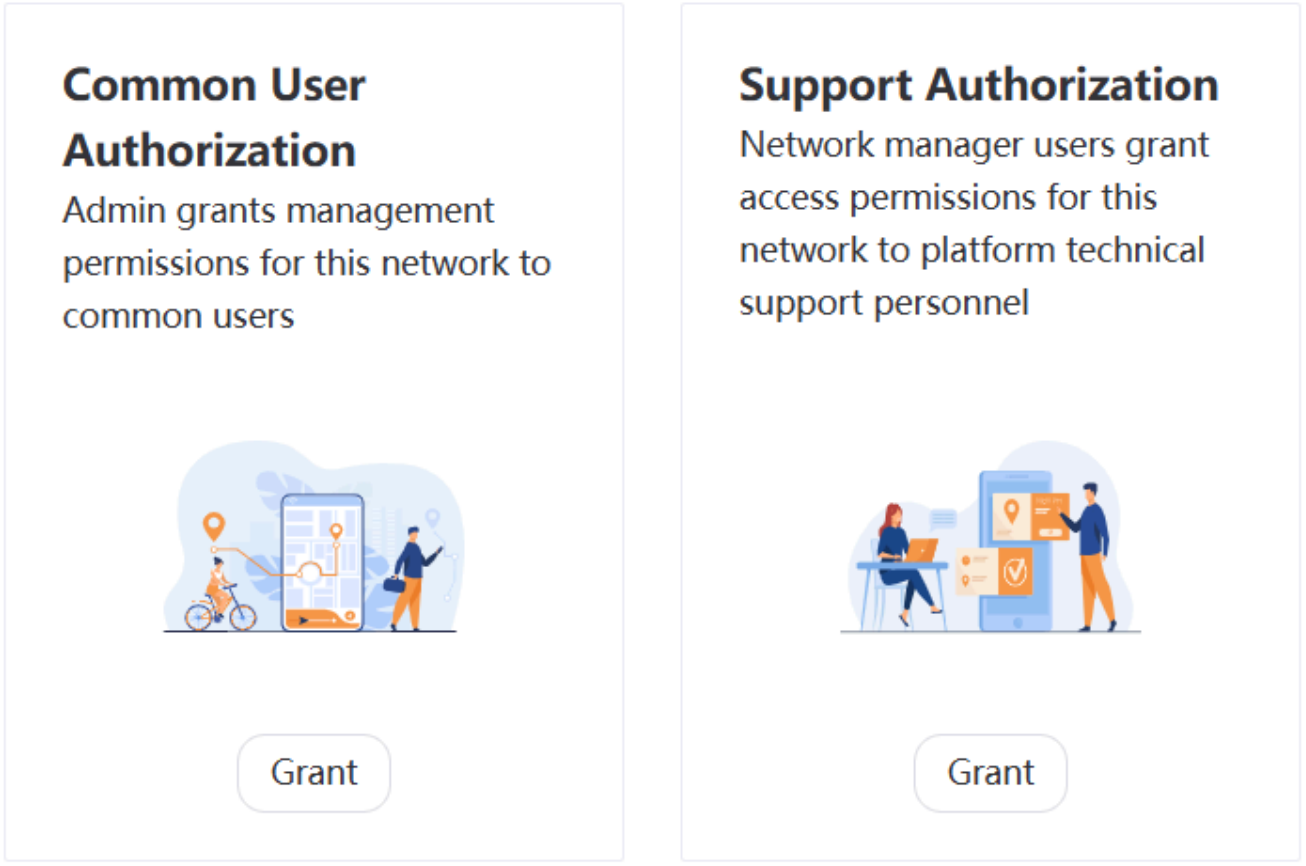
▲*Figure 16: Add Network Page*

To modify or delete a network, click the three dots in the top right corner of the network card. After clicking, "Edit" and "Delete" buttons appear for modifying or deleting the network.

> **Note**
>
> - Before deleting a network, all devices under that network must be unbound first;

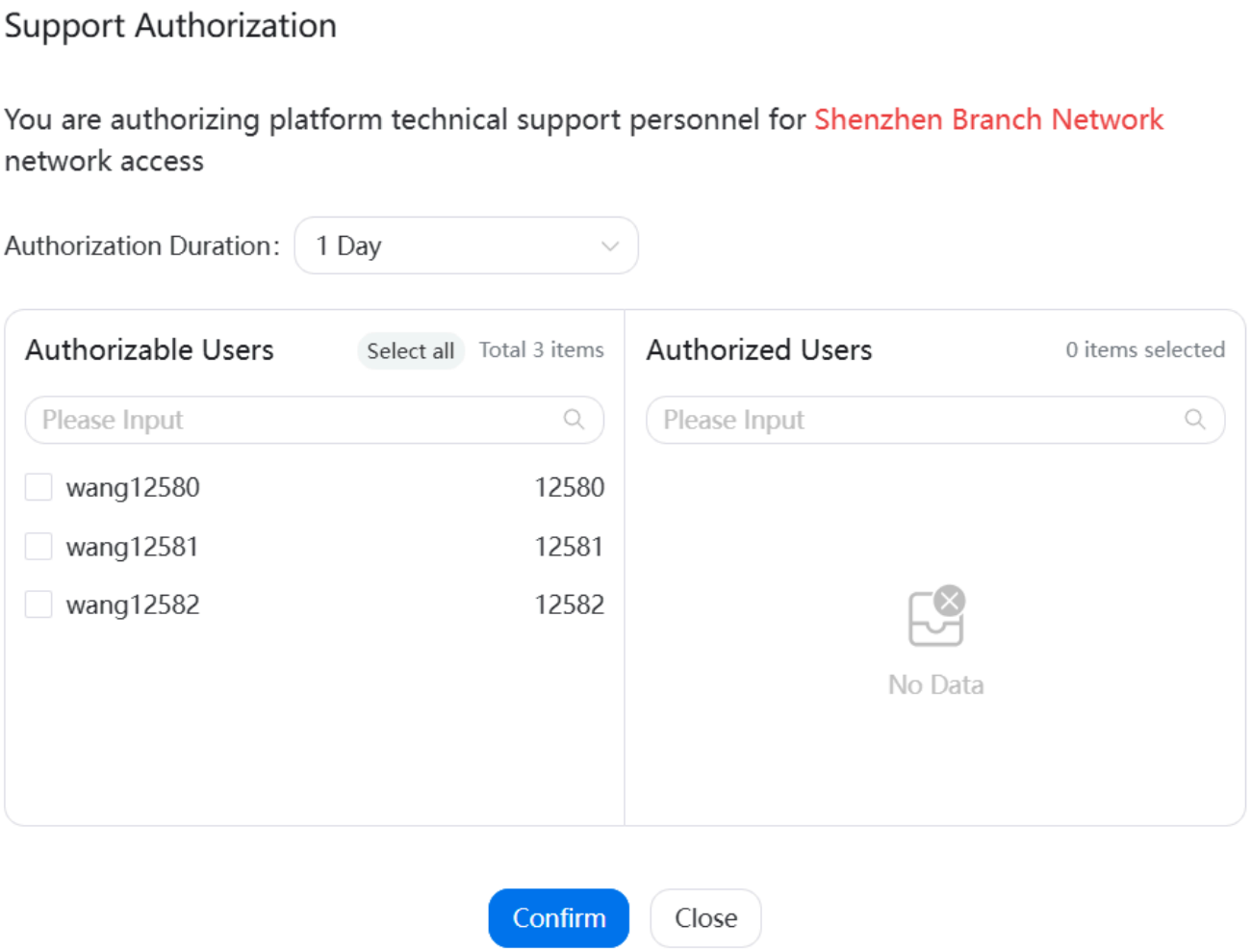
2.2. Network Authorization

Network authorization is divided into Regular User Authorization and Technical Support Authorization based on the authorization target. The main difference is that regular users obtain permissions for a long period, while technical support obtains permissions temporarily, which automatically expire after a set time. Additionally, technical support serves the entire platform users and is not affected by tenants.



▲*Figure 17: Network Authorization Page*

During user authorization, select the personnel to be authorized and click the "Save" button to complete authorization, as shown:



▲*Figure 18: Technical Support Authorization Dialog*

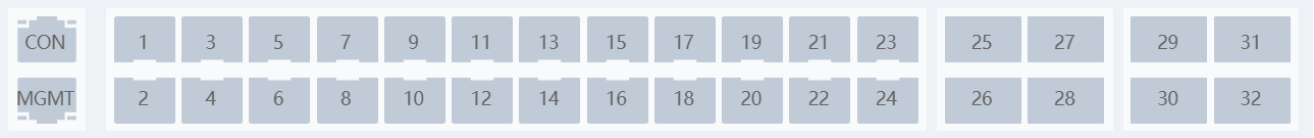
Regular user authorization operates the same as technical support authorization.

3. Device Management & Unbinding

3.1. How to Manage Devices

3.1.1. Introduction to Management Ports

Devices have three types of ports: Serial port, Management port, and VLAN1. Serial and Management ports are labeled CON and MGMT on the device panel. VLAN1 refers to all other business ports besides CON and MGMT, as shown: ports 1-32 are VLAN1 ports.



▲*Figure 19: Device Port Diagram*

3.1.2. Preparation for Management

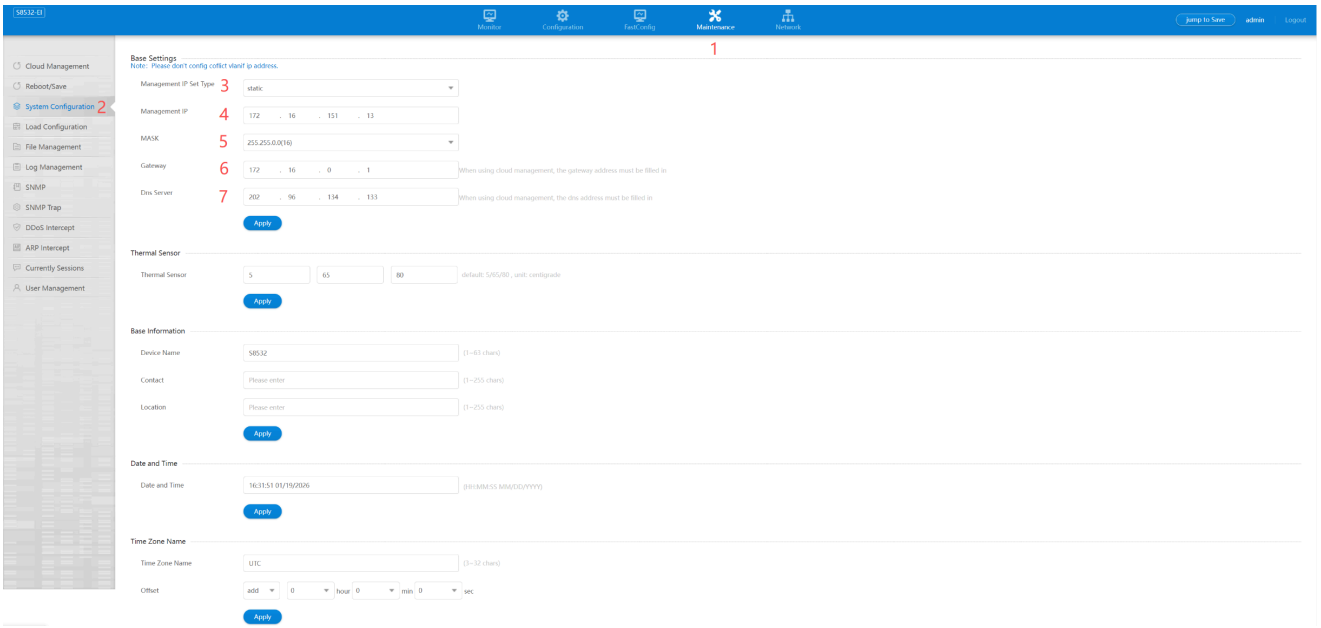
1. **Network Reachability Requirement**

- Ensure the firewall between the device and the cloud platform does not block communication.

2. **Device IP Address Configuration**

Devices can connect to the management network via MGMT or VLAN1. The corresponding IP address instructions are as follows:

- **MGMT Connection**: Default IP is 192.168.1.1. If the default IP cannot access DHCS, manually set the IP. Users can log into the device WEB and modify the Management IP, Gateway, etc., in the System Configuration as needed. As shown:



▲*Figure 20: Device Side Management IP Configuration Page*

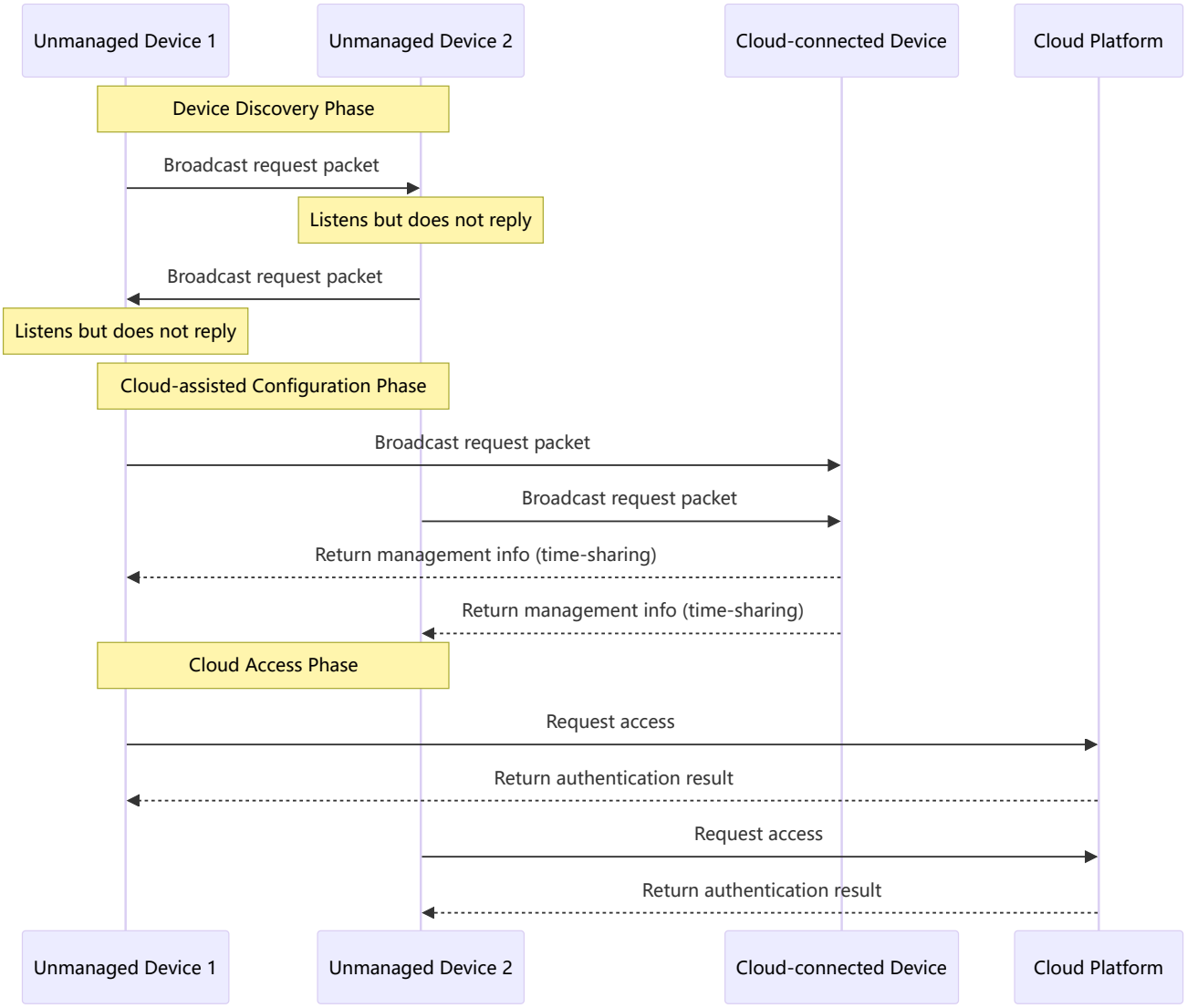
- **VLAN1 Connection**: The device leaves the factory with DHCP enabled by default and will automatically obtain an IP address after connecting to the network. Users can also manually configure a static IP;

3.1.3. Device Registration

3.1.3.1. Private Protocol Registration

Private protocol management is based on a "contagion" method between same-brand devices, where the management configuration is sent via private protocol to other unmanaged devices. The specific process is as follows:

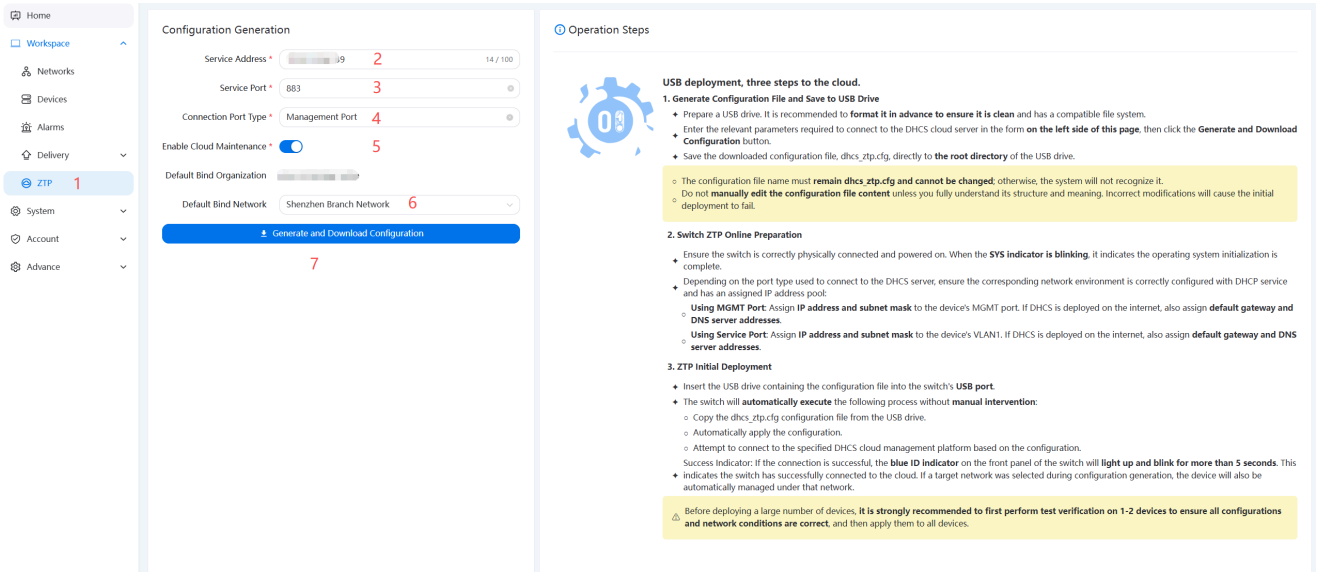
- Unmanaged devices broadcast request packets for management configuration;
- Other unmanaged devices listen to the broadcast request but do not reply;
- A device already connected to the cloud listens to the broadcast request and returns the management configuration. If it hears multiple requests, it replies in a time-sharing manner;
- The unmanaged device obtains the management configuration and actively initiates an access request to the cloud platform, which returns the access result;



▲*Figure 21: Private Protocol Broadcast Management Flowchart*

3.1.3.2. ZTP Registration

- **Generate Configuration File and Save to USB Drive**
  - Prepare a USB drive. It is recommended to **pre-format it** to ensure it is clean and the file system is compatible.
  - Enter the relevant parameters required to connect to the DHCS cloud server in the form on **the left side of this page**, then click the **Generate and Download Config** button, as shown in Figure 22;
  - Save the downloaded configuration file `dhcs_ztp.cfg` directly to the **root directory** of the USB drive.



▲*Figure 22: ZTP Configuration File Generation Page*

> ⚠ **Warning**
>
> - The configuration file **name must remain** `dhcs_ztp.cfg` and cannot be changed, otherwise the system will not recognize it.
> - **Do not manually edit the configuration file content** unless you fully understand its structure and meaning. Incorrect modifications will cause deployment failure.

- **Switch ZTP Online Preparation**
  Ensure the switch is correctly physically connected and powered on. When the **SYS** indicator is **blinking**, it indicates the operating system initialization is complete. Please ensure the corresponding network environment has correctly configured DHCP service and assigned an IP address pool according to the port type you use to connect to the DHCS server:

No.	Connection Method to DHCS	DHCP Server Required Configuration
1	MGMT Port	Allocate **IP address, subnet mask** for the device's MGMT port. If DHCS is deployed on the internet, also allocate **default gateway** and **DNS server** addresses.
2	Business Port	Allocate **IP address, subnet mask** for the device's VLAN1. If DHCS is deployed on the internet, also allocate **default gateway** and **DNS server** addresses.

▲*Table 3: ZTP Online Preparation*

- ZTP Deployment
  - Insert the USB drive containing the configuration file into the switch's **USB port**.

- The switch will **automatically execute** the following process **without manual intervention**:
  - Copy the `dhcs_ztp.cfg` configuration file from the USB drive.
  - Automatically apply the configuration.
  - Attempt to connect to the specified DHCS cloud management platform based on the configuration.
- Success Indicator: If the connection is successful, the **blue ID indicator light** on the front panel of the switch will light up and **blink for over 5 seconds**. This indicates the switch has successfully connected to the cloud. If a network was selected when generating the configuration file, the device will also be automatically managed under that network.

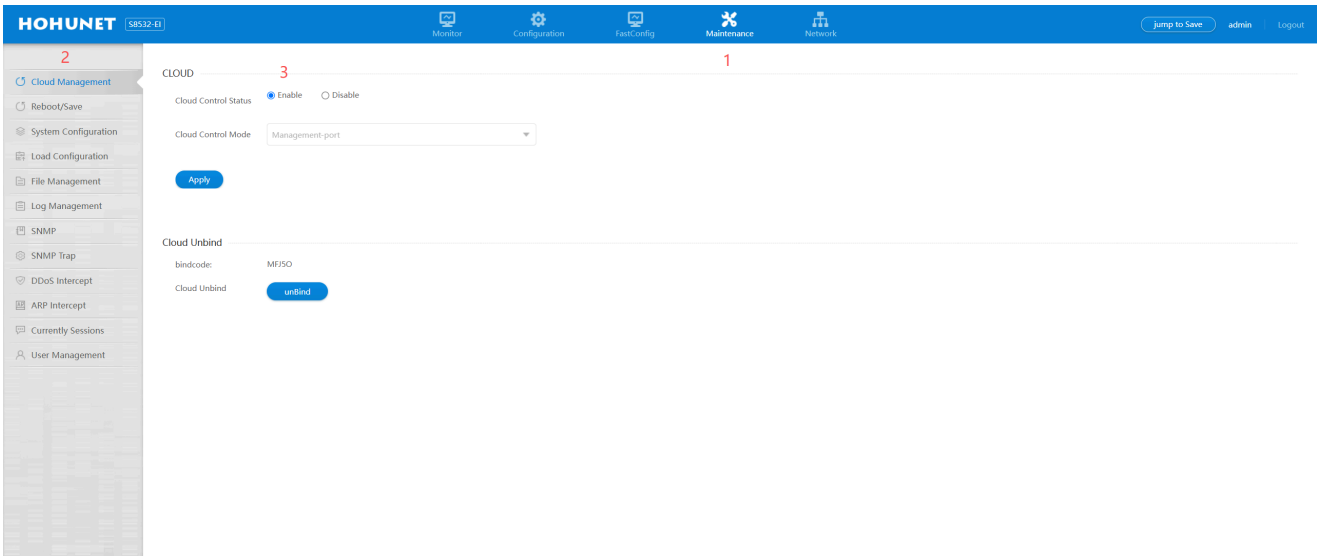
> **Note**
> Before large-scale device deployment, **it is strongly recommended to test and verify on 1-2 devices first** to ensure all configurations and network conditions are correct, then proceed with all devices.

3.1.3.3. CLI Registration

Users can directly configure management commands on the switch via the command line. Steps are as follows:

```
#1. Log into the switch, enter admin username and password

#2 Enter configuration mode (mandatory)
configure terminal

#3. Configure cloud control mode: DHCS (mandatory)
cloud control version dhcs

#4. Configure cloud control platform port and the cloud control
platform's domain name or IP address (mandatory)
cloud control domain-port 883 domain-name 10.45.12.9

#5. Select management interface, choose one matching the actual
connection (mandatory)
  # VLAN1 connected to cloud control platform
  cloud control enable
  # MGMT connected to cloud control platform
  cloud control mgmt-if enable

#6. Save configuration (mandatory)
  write
```

After executing the commands, you can check if it's enabled in the device's web system under Maintenance menu -> Cloud Control Configuration. As shown, the Cloud Control Enable status is "Enabled".



▲*Figure 23: Device Side Cloud Management Service Configuration Page*

> **Note**
>
> - The management port type selected for cloud control connection mode must match the actual port connected to the cloud platform.

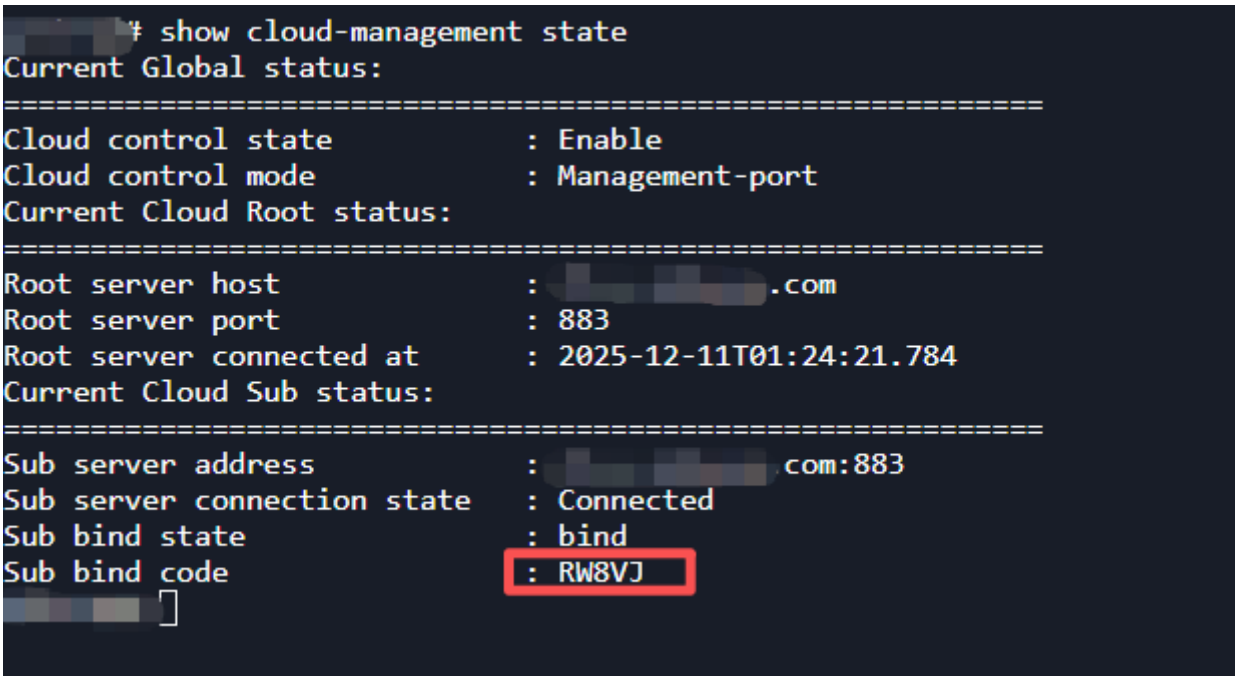
3.1.3. Device Management

After device registration, it can be managed using a binding code.

3.1.3.1. Step 1: Obtain Binding Code

There are two ways to obtain the binding code:

- **Get binding code via CLI command**
  Log into the device, enter the command `show cloud-management state` to view, as shown in the red box in the figure:

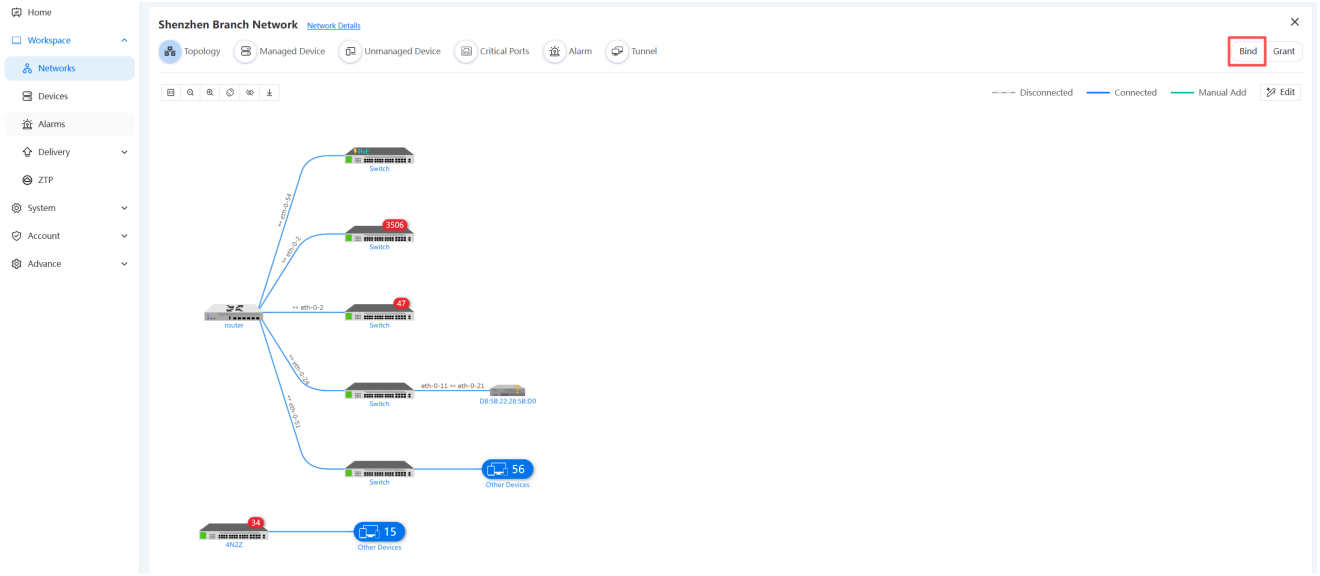


▲*Figure 24: View Binding Code via CLI Command*

- **Get binding code via web page**
  You can log into the device web and view the binding code obtained after enabling the cloud management service in the Maintenance menu -> Cloud Management Service. Refer to the interface in 【Cloud Control Configuration】.

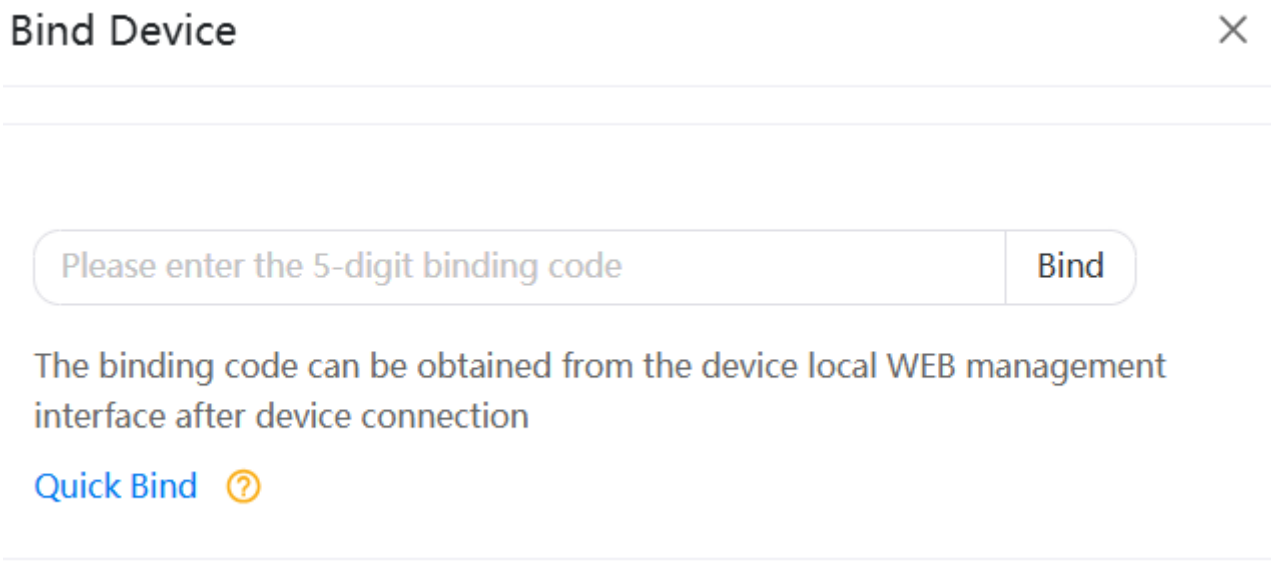
3.1.3.2. Step 2: Cloud Platform Binding

- **Binding via Binding Code**
  Log into the cloud platform, enter the network where the device needs to be bound, click the "Device Binding" button in the top right corner, and enter the binding code to bind, as shown:



▲*Figure 25: Network Details Page Device Binding Entry*

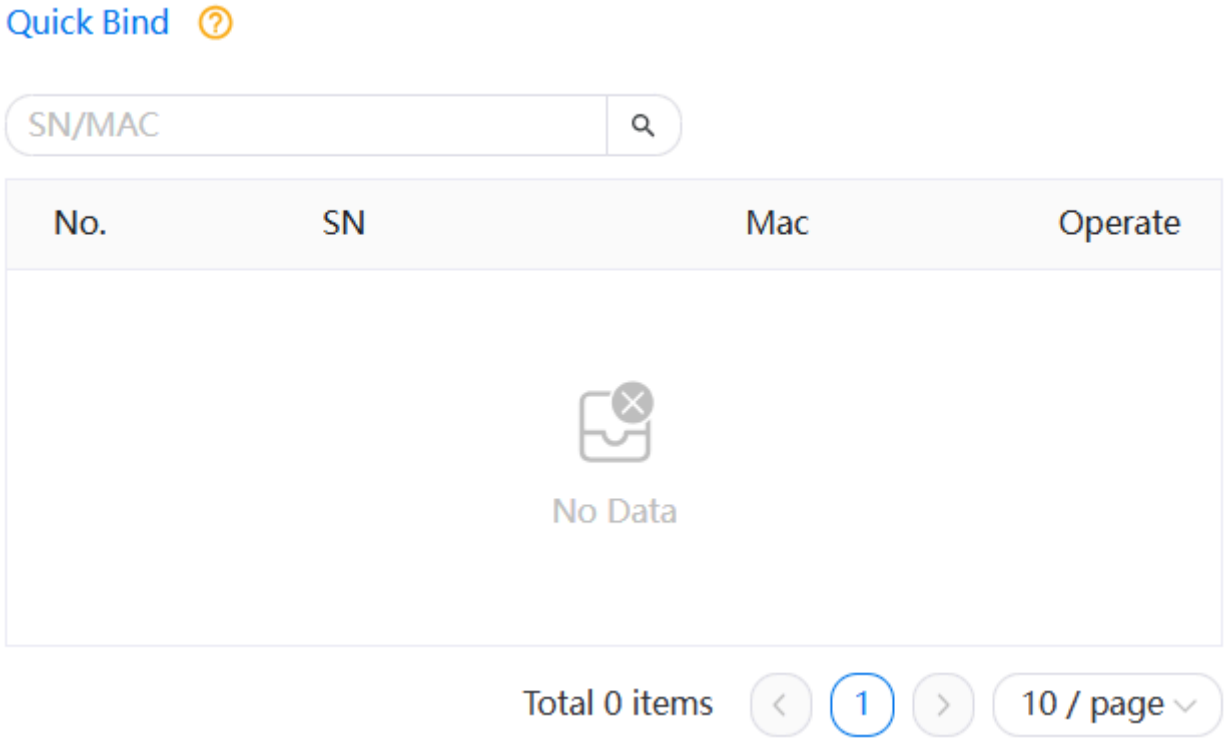
In the new pop-up dialog, enter the `BindCode` from the switch (case-sensitive), click the "Bind" button (a success prompt will appear).



▲*Figure 26: Enter Binding Code Dialog*

> **Note**
>
> - The device must be online to be bound from the cloud platform side;
> - A device can only be bound to one network;

- **Quick Binding**
  When users register to the platform but haven't bound to a network yet, they can use the Quick Bind function to bind in batches without entering binding codes one by one. The prerequisite for Quick Bind is knowing the device can be bound to this network. As shown:



▲*Figure 27: Quick Binding Dialog*

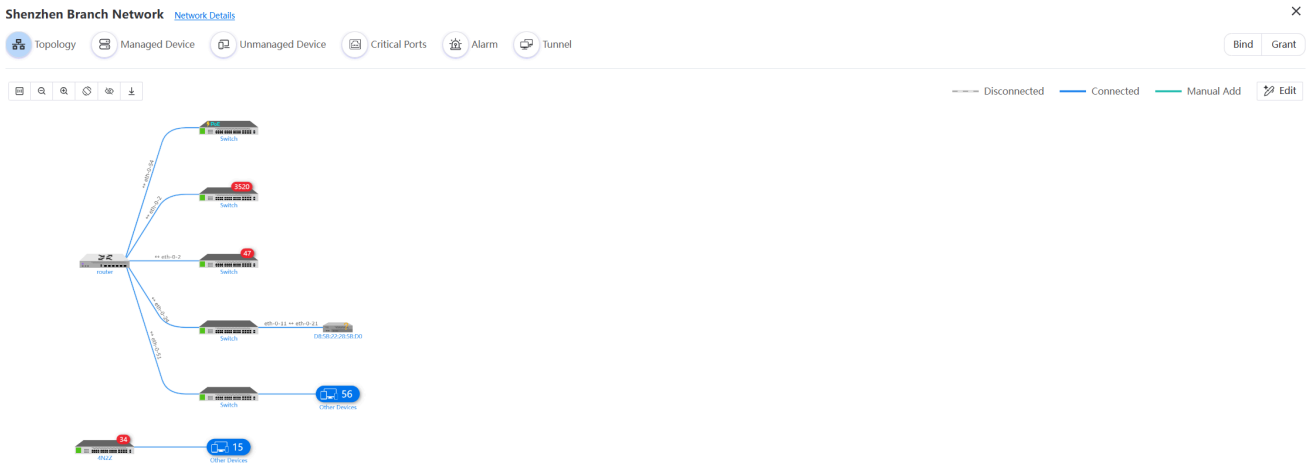
> **Note**

- The device must be online to be bound from the cloud platform side;
- A device can only be bound to one network;

3.2. How to Confirm Device is Managed

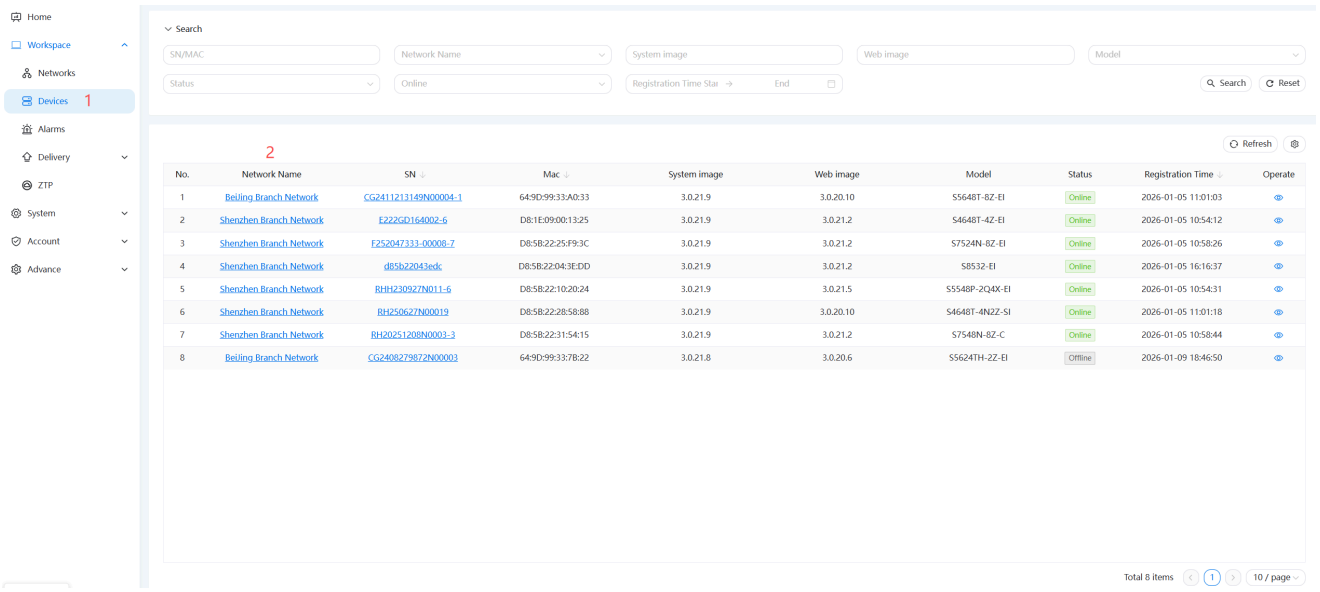
There are two ways to confirm a device is managed: one is to check the Network field content in the device list, the other is to view it in the Cloud Managed Devices section of the network.

- **View in Topology Diagram**
  After successful binding, the device becomes visible on the network topology page. If the device is connected to other devices, they will also be displayed in the topology.



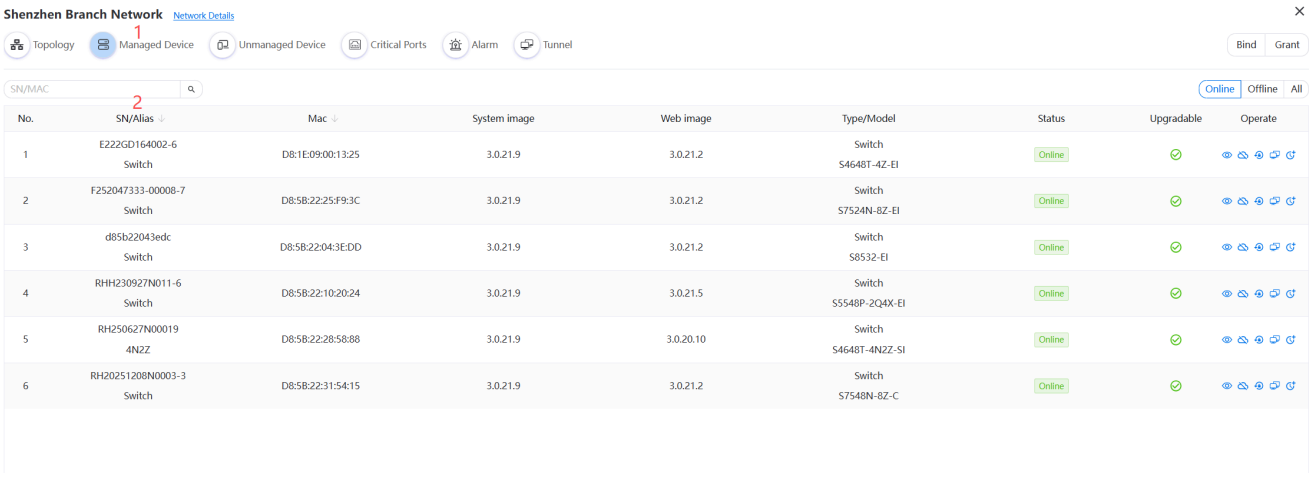
▲*Figure 28: Network Topology Diagram Displaying Managed Devices*

- **View in Device List**
  In Workspace -> Device List, search for managed devices by Serial Number, MAC address. If the Network field in the search results shows the bound network, it is managed; otherwise, it is not.



▲*Figure 29: Device Management Page Viewing Management Status*

- **View in Cloud Managed Devices**
  In Workspace -> Network -> Cloud Managed Devices, check if managed devices exist. If managed devices exist, they are managed. As shown:



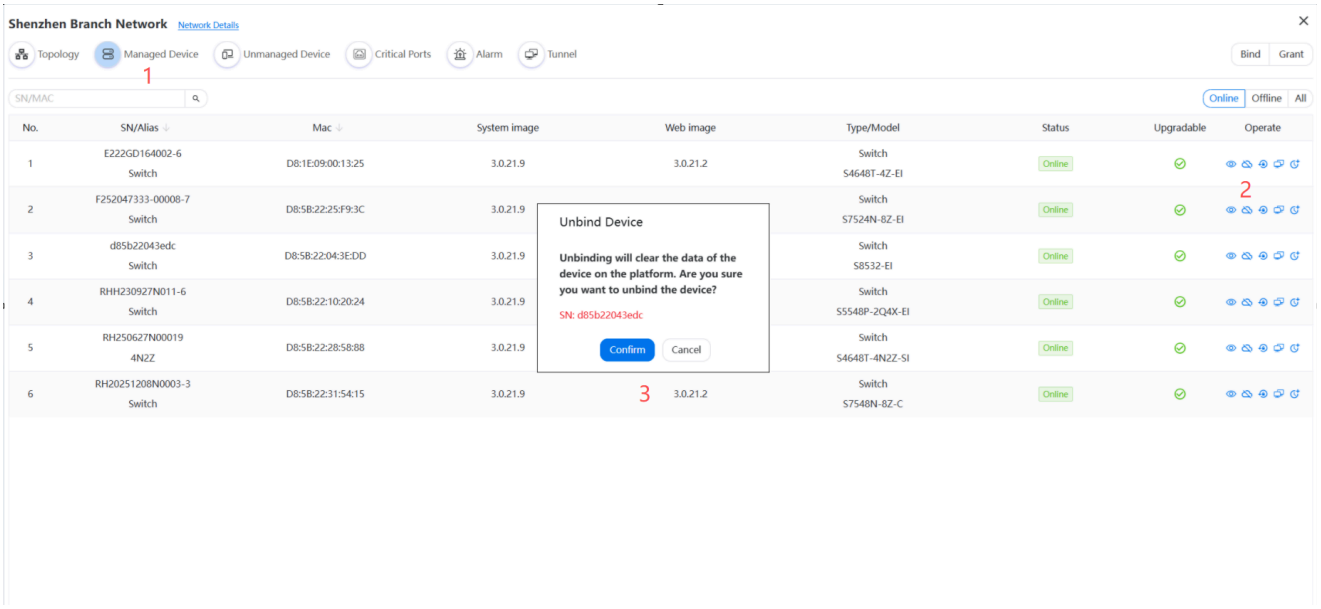
▲*Figure 30: Network Cloud Managed Device List*

3.3. How to Remove Management

There are two ways to unbind a device: one is to unbind it from the cloud platform, the other is to unbind it from the device's WEB system. Both methods support unbinding even when the device is not connected to the cloud platform.

3.3.1. Cloud Platform Unbinding

In Workspace -> Devices, click the "Unbind" button in the Actions column for the device to be unbound. A confirmation dialog pops up; confirm to unbind. If the device is offline during unbinding, the binding relationship will be automatically removed when the device comes back online.



▲*Figure 31: Device Unbind Confirmation Dialog*

3.3.2. Device Side Unbinding

Log into the device's web system, go to Maintenance -> 【Cloud Control Configuration】, find the "Unbind" button and click it to unbind. If the device is offline, the unbind status will be synchronized when the device reconnects to the cloud platform.

> ⚠ **Warning**
> The unbind operation will clear all data of the device on the cloud platform. Please operate with caution.

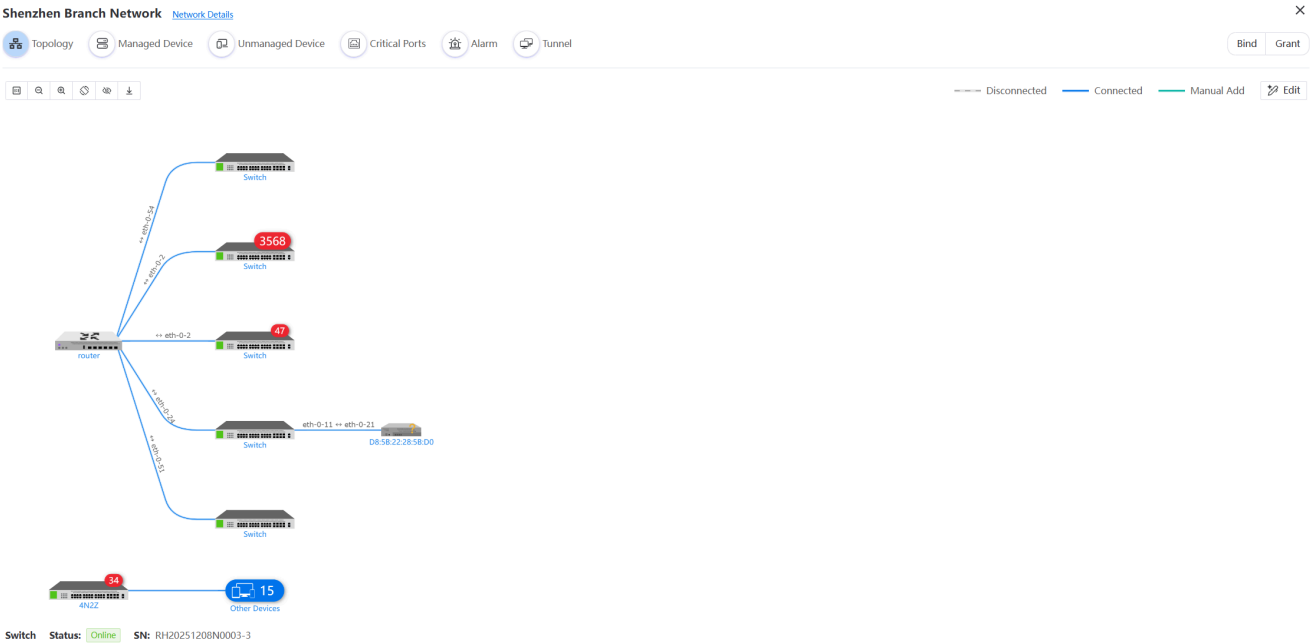
4. Network Management

4.1. Auto Topology Diagram

Auto Topology Discovery is used to automatically identify and visualize network structure. The topology diagram dynamically displays the current network state, reflecting real-time changes like device online status, link failures, etc., helping O&M personnel quickly locate faults and discover new assets.

4.1.1. Basic Functions Introduction

- If managed devices in the topology are online, their indicator lights on the device icon show green; offline shows red. Devices with POE functionality also display "POE" text on the icon.
- When the mouse hovers over a device in the diagram, the bottom left corner of the topology shows the device's name, status, and serial number. If the device has alarms, the alarm count is displayed in the top left corner of the device.
- Users can hold down the right or left mouse button anywhere in the topology diagram to move the entire diagram. Release the mouse button to confirm the move.
- Right-clicking on a managed device icon brings up a context menu, providing options for quick remote access to that device and the ability to modify the device name.



▲*Figure 32: Auto Topology Diagram*

- **Control Buttons**
  The top right corner of the topology diagram has 6 function buttons to control the display, with specific purposes explained in the table below:

No.	Icon	Description
1		Zoom Out Topology Scale
2		Zoom In Topology Scale
3		Reset Topology Scale
4		Rotate Topology Direction
5		Hide Connection Info
6		Download Topology Diagram

▲*Table 4: Topology Icon Description*

- **Topology Connections**

Connections in the topology display communicating port pairs for easy viewing. For some unmanaged devices, users can manually connect two devices in Edit Mode. Manually connected devices are shown in green. If both manual and auto-discovered connections exist for the same devices, the topology diagram only shows the auto-discovered connection; manual connections are only visible in Edit Mode.

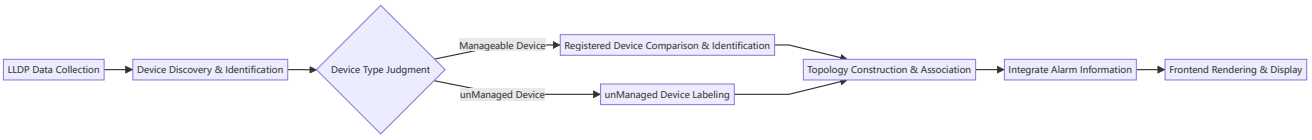
No.	Color	Connection Description
1	Green	Manual Connection (for display only)
2	Blue	Auto Connection (normal communication)

No.	Color	Connection Description
3	Gray	Connection Interrupted (port status abnormal)
4	Orange	Connection Conflict (port conflict)

▲*Table 5: Topology Connection Description*

4.1.2. Auto-Drawing Principle

The platform automatically discovers devices and draws network topology diagrams based on the LLDP protocol. Topology technology principles mainly include: device discovery and identification, binding of unmanaged devices, topology association, and front-end display. The overall flow is shown below:



▲*Figure 33: LLDP-Based Auto Topology Discovery Flowchart*

- Device Discovery and Identification
  The platform automatically discovers devices with LLDP protocol enabled in the network via probe devices and distinguishes between "Manageable Devices" and "unManaged Devices" (devices not managed by the platform).
  - **LLDP Data Collection**
    Probe devices obtain the LLDP neighbor table of neighbor devices with LLDP enabled within the network via CLI, extracting key fields from each LLDP entry: neighbor device's Chassis ID (usually MAC address), Port ID, System Name, etc.
  - **Device Identification Mechanism**
    - **Managed Device Identification**: The platform maintains a list of already managed devices (including MAC address, IP address, model, etc.) and compares the discovered Chassis ID (MAC address) from LLDP with the MAC addresses of managed devices. If matched, it's labeled as a "Managed Device" and associated with its registration info (like device role, management IP). If not matched, it's labeled as a "unManaged Device" (e.g., printers, IP phones, unmanaged switches).
      Example: Suppose the platform manages device A (MAC 00:11:22:33:44:55). When the LLDP message from switch B discovers a neighbor MAC of 00:11:22:33:44:55, the platform identifies it as device A.

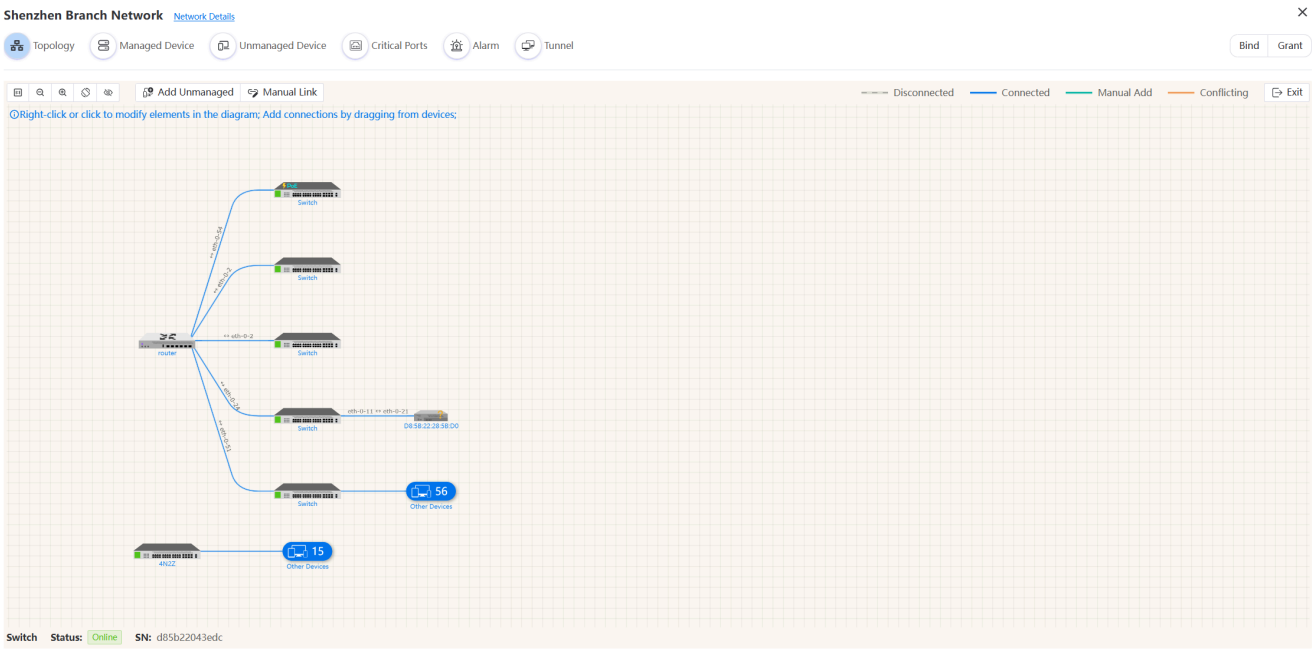
        - **Terminal Device Identification**: When the probe device identifies that an LLDP-discovered MAC address is unique in the MAC table and appears only once, and the LLDP Port ID is in MAC address form, it is identified as a terminal device.

- **unManaged Device Binding**
  For identified unmanaged devices, the platform needs to determine their connection relationships and bind them to specific ports. The platform obtains the Port ID (port information) to which the unmanaged device is connected from the LLDP information. Administrators can manually mark the port where a unmanaged device is connected on the topology diagram. Detailed operations can be found in the unManaged Devices section.
- **Topology Construction and Association**
  LLDP protocol provides direct connection relationships between devices. The platform parses all reported LLDP data to generate a relationship graph: each node represents a device, edges represent physical links between devices.
    - **Associate Devices**: Using the Chassis ID and Port ID from LLDP messages, the platform forms the skeleton of the topology from connection relationships between managed devices. Then, unmanaged devices are manually connected to ports on managed devices to form an end-to-end topology.
    - **Real-time Updates**: The platform polls LLDP data periodically (e.g., every 1 minute), dynamically updating the topology to reflect network changes (like device online/offline, link changes).
- **Integrate Alarms and Status**
  The topology diagram integrates alarm data to improve fault location efficiency.
    - **Device Alarm Information**
      The platform collects alarm events from network element devices (like port errors, CPU overload) and directly displays the number of important alarms on the device icon in the topology, helping O&M personnel quickly identify problematic devices.
    - **Online Status Information**
      The platform monitors MQTT client online status and device heartbeat mechanisms to detect device online status. The device indicator light in the topology shows "Online" or "Offline" status (e.g., green for online, gray for offline).
- **Frontend Display**
    - **Data Processing**: Backend services send topology data (device list, connection relationships, alarms, status) to the frontend via RESTful API or WebSocket. The frontend receives and parses the data.

- **Visualization Rendering**: The frontend uses AntV to draw the topology: devices are displayed as icons, labeled with device type (e.g., switch, router, third-party device). A switch or manually added router serves as the root node. Lines connect devices with port information labeled. Duplicate links and self-loop connections are filtered.

4.1.3. Edit Mode

Edit Mode can be used for topology planning and refining topology content. Before use, relevant nodes need to be added to unManaged Devices. Click the "Edit" button in the top right corner of the topology to enter Edit Mode, as shown below:

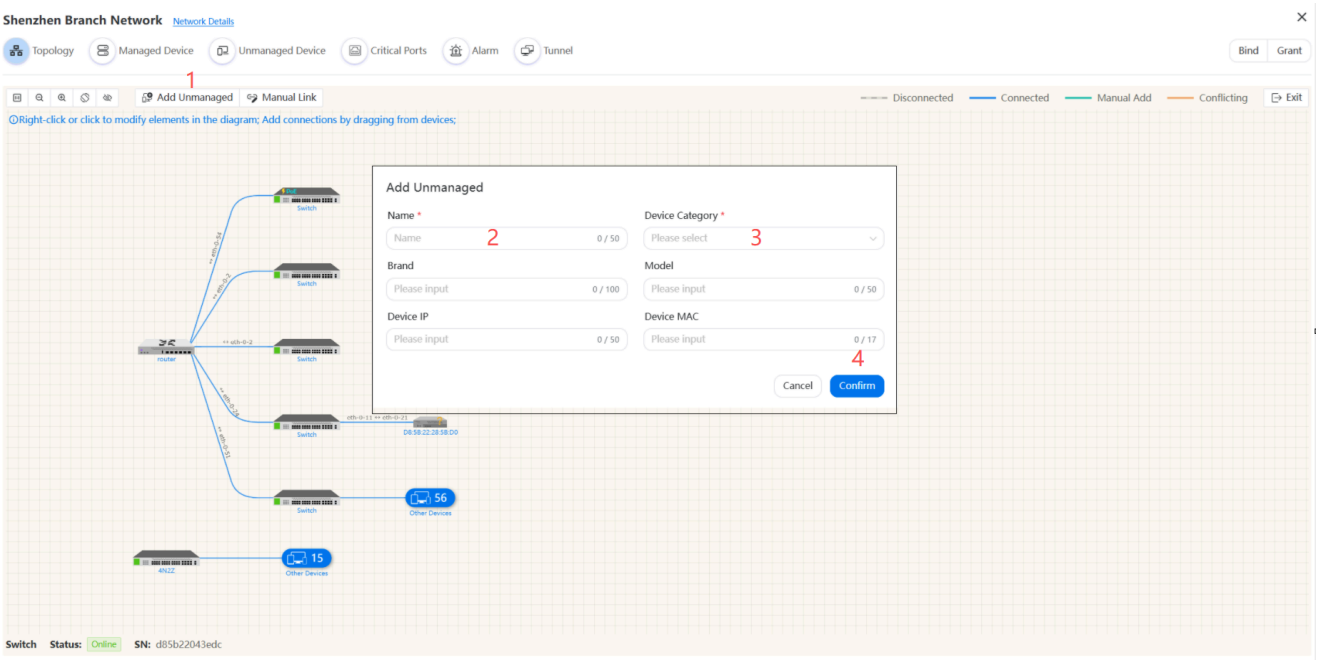


▲*Figure 34: Topology Diagram Edit Mode*

In Edit Mode, you can manually add unmanaged devices under this network and establish connection relationships between devices.

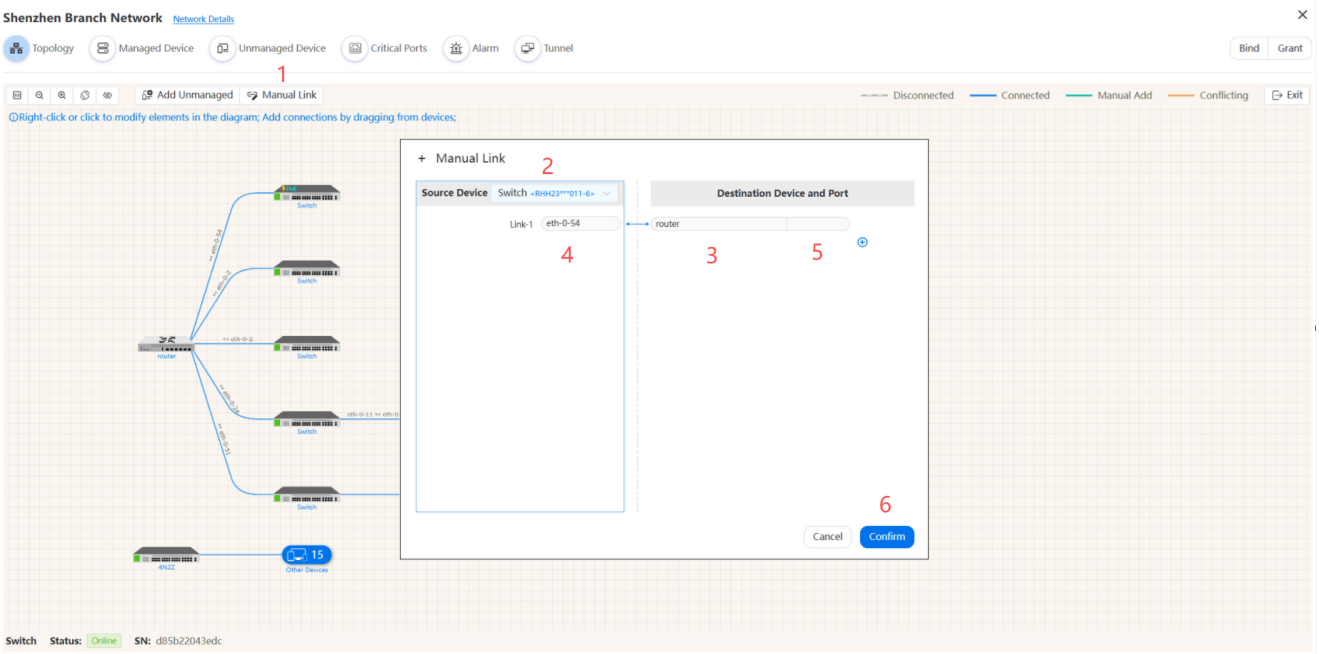
- **Add unManaged Device**

  unmanaged devices are typically devices that need attention but cannot be managed by the cloud platform. Users can manually add them in Edit Mode of the topology.
  In Edit Mode, click the "unManaged Device" button; a pop-up input box appears as shown below. Device Name and Category are required. Brand, Model, IP, and MAC can be entered as needed. Click "Save" to add a unmanaged device entry.



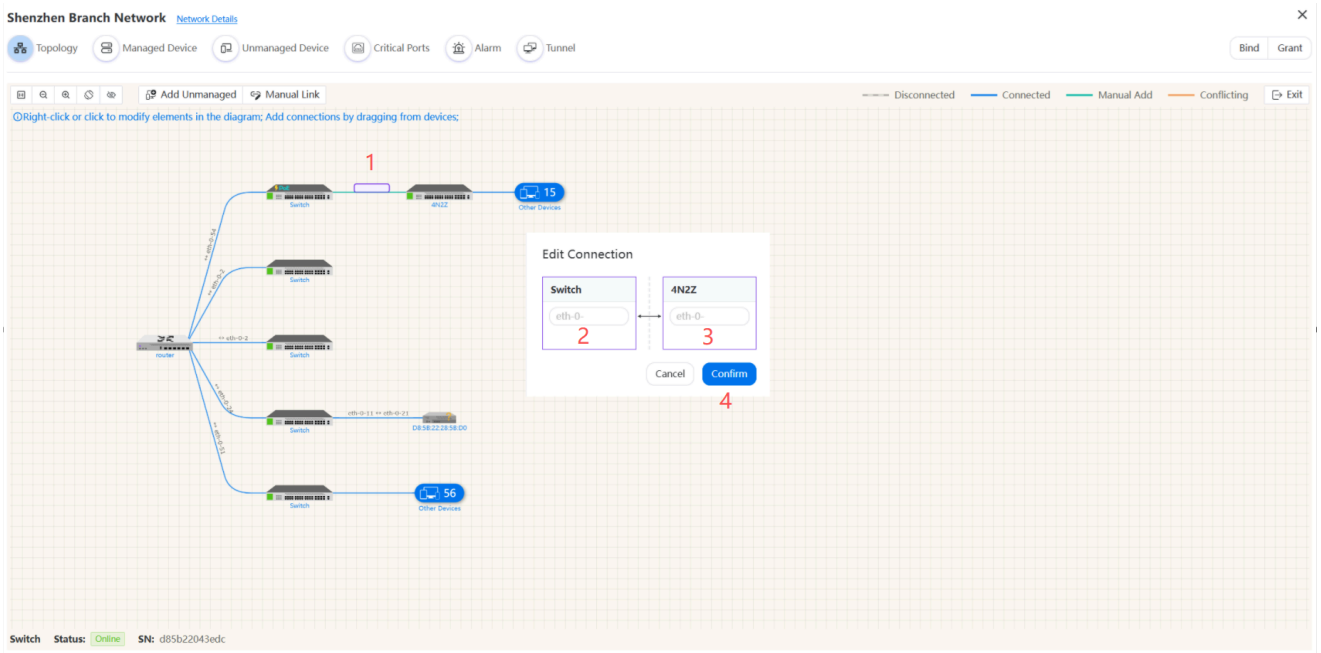
▲*Figure 35: Add unManaged Device Dialog*

- **Adjust Topology Relationships**
  When topology relationships need adjustment, click the "Manual Connection" button in Edit Mode to pop up the dialog below.
  Set the source and destination devices for the connection, and fill in the port names. Multiple connection relationships can be configured in one batch. Click "Confirm" to draw the corresponding connections in the topology.



▲*Figure 36: Manual Connection Dialog*

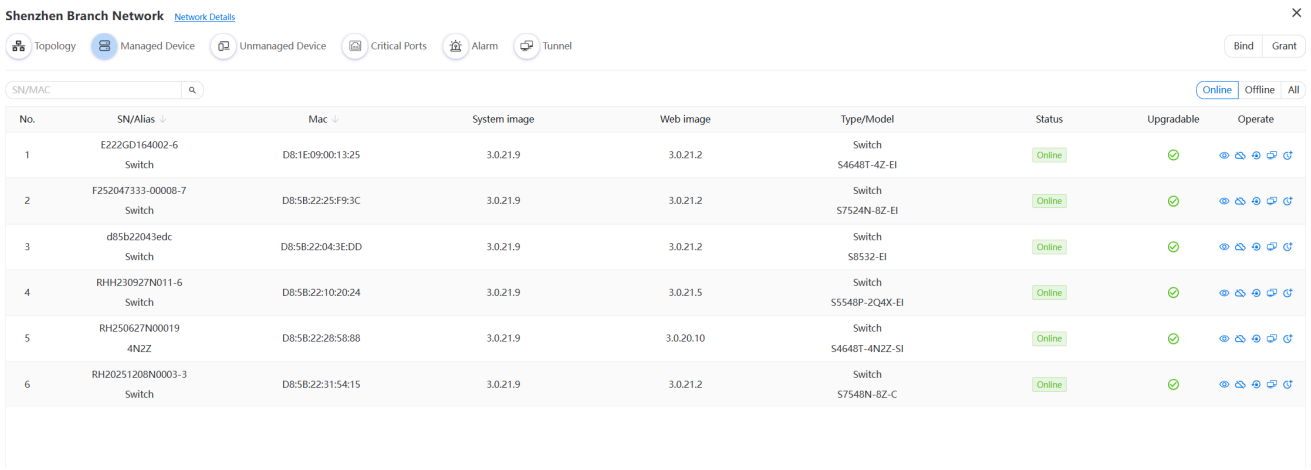
In Edit Mode, the connection ports between two managed devices can be adjusted. Double-click the connection line to pop up an edit box for modifying the ports. As shown:



▲*Figure 37: Edit Connection Dialog*

4.2. Manageable Devices

Under Network -> Cloud Managed Devices, you can see manageable devices, as shown:



▲*Figure 38: Cloud Managed Device List*

Users can search for devices by SN/MAC and filter data directly by clicking the Online/Offline tags. In the Actions column for each record, there are function buttons for **Device Details, Device Unbind, Reset Password, Remote Maintenance, and Reporting Frequency**.

4.2.1. Device Details

Click the "View" button in the Actions column for a device to enter its details page. The Device Details interface defaults to showing the device's monitoring panel, where you can view the device overview, port monitoring status, manage device POE and configurations, analyze device logs, and perform remote maintenance. POE

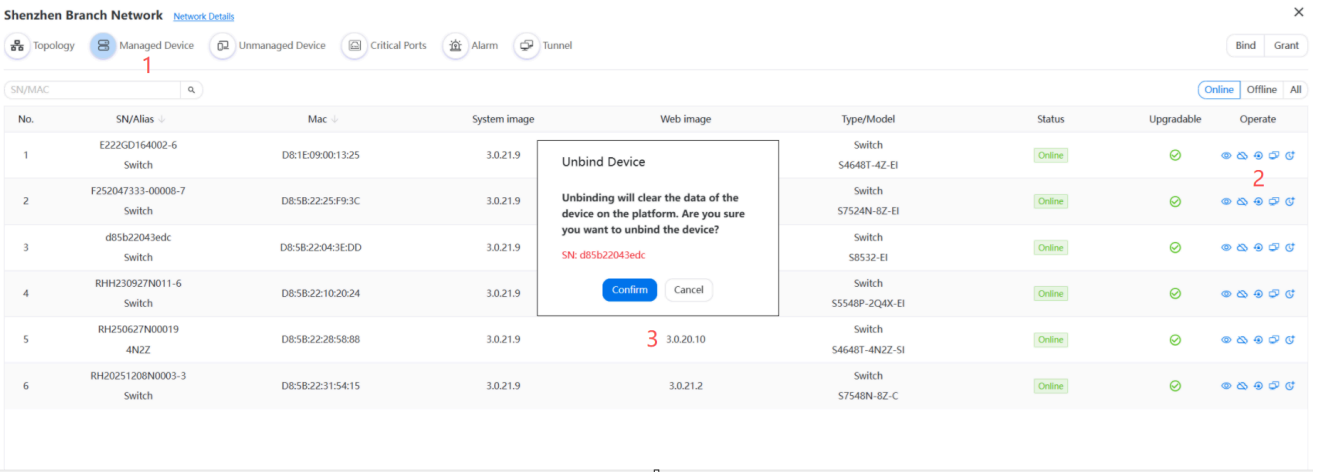
Management is only displayed for devices with POE functionality. Please refer to the Device Management chapter for details.

4.2.2. Device Unbind

Refer to the How to Remove Management chapter for device unbinding.

4.2.3. Reset Password

If the device-side admin password is forgotten, it can be reset. Click the "Reset" button for the device in the Cloud Managed Devices Actions column. A confirmation dialog pops up asking if you want to reset the device's admin password, as shown below:



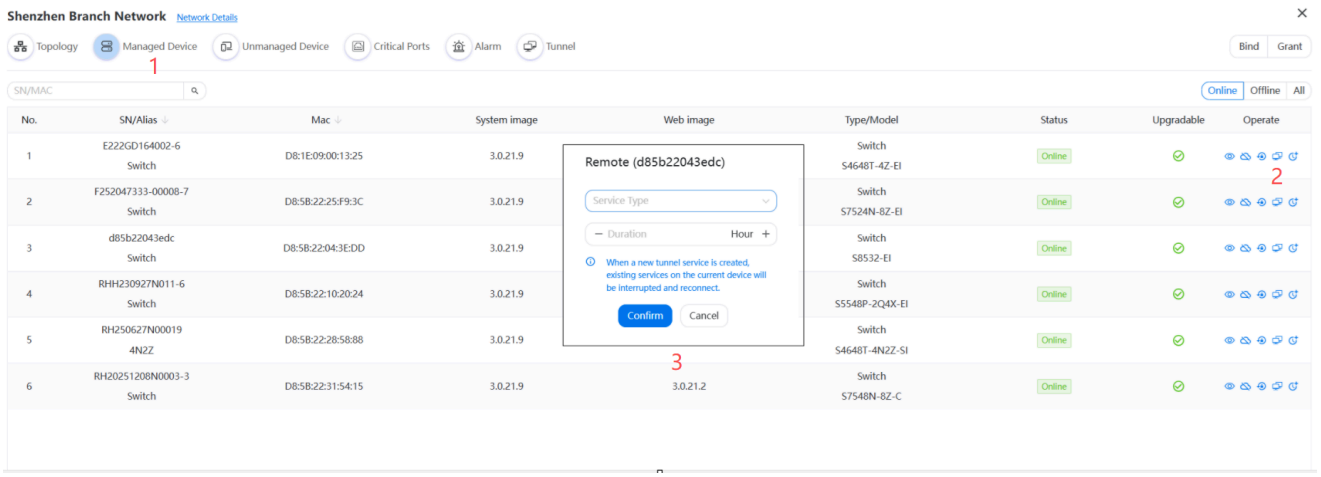
▲*Figure 39: Confirm Reset Device Password Dialog*

After clicking "Confirm", a dialog pops up for identity verification. There are two methods: mobile verification and password verification.

- **Mobile Verification**
  Users need to have a bound mobile number to use this. After binding, the system sends an SMS verification code to the mobile phone. Enter the code to reset the admin password to the factory default.
- **Password Verification**
  Users enter their login password for verification. After passing, the admin password is reset to the factory default.

4.2.4. Remote Maintenance

Maintenance personnel can directly connect to devices via the Remote Maintenance function. Available service types are web, SSH, and Telnet. In the Actions column, click the "Remote Maintenance" button for the target device. A dialog pops up to select the service type and duration, as shown below:



▲*Figure 40: Remote Maintenance Configuration Dialog*

Click the "Confirm" button; the platform establishes a tunnel with the device and directly jumps to the web, SSH, or Telnet maintenance interface. The tunnel automatically closes and releases upon expiration. As shown below:

▲*Figure 41: Web Remote Maintenance Interface*

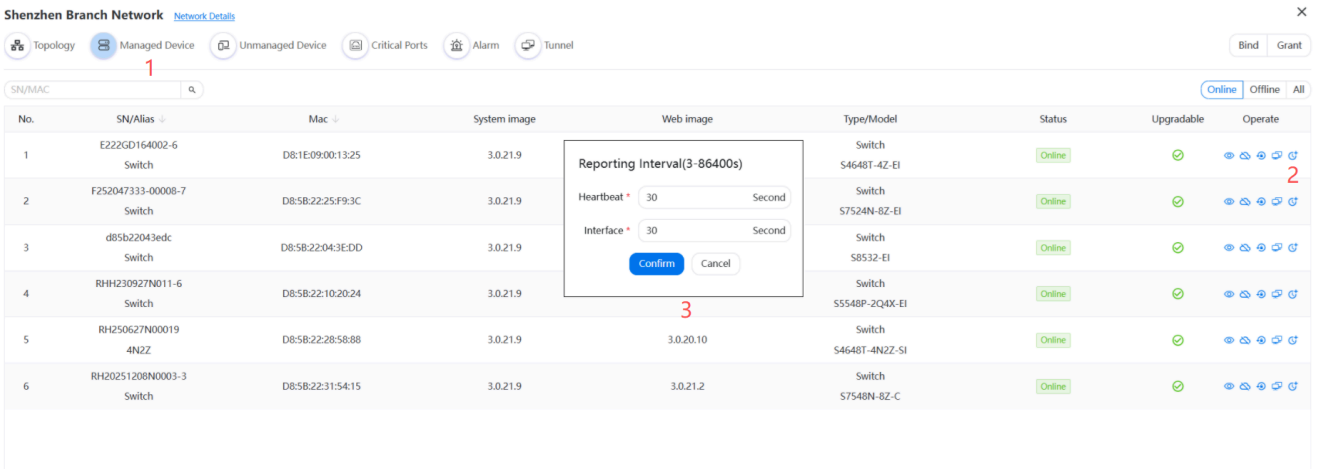
SSH and Telnet tunnels automatically close and release after 30 minutes of inactivity by default.

▲*Figure 42: SSH Remote Maintenance Interface*

▲*Figure 43: Telnet Remote Maintenance Interface*

4.2.5. Reporting Frequency

Maintenance personnel can customize the frequency of device data reporting based on maintenance needs, primarily for heartbeat data and interface data. In the Actions column, click the "Reporting Frequency" button for the target device. A dialog pops up as shown below:



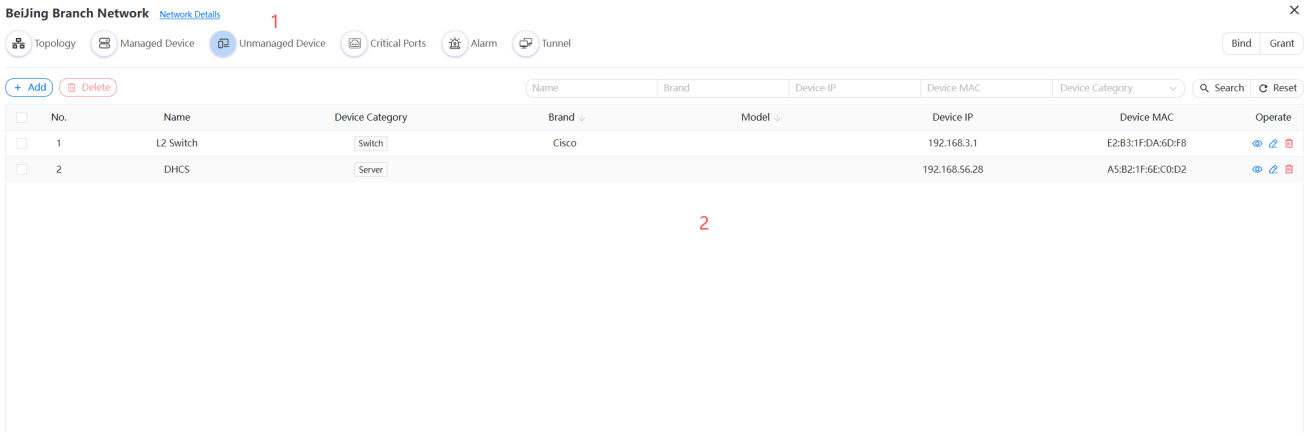
▲*Figure 44: Reporting Frequency Setting Dialog*

> **Note**
> The default reporting frequency is 300 seconds. Users can modify it within the allowed range (30-86400). It is not necessary to adjust this parameter unless required.

4.3. unManaged Devices

4.3.1. unManaged Device List

To provide a more comprehensive and accurate topology display, the platform offers management functions for unmanaged devices. unmanaged devices added in the topology's Edit Mode are centrally managed in this module. The unManaged Device list is shown below:



▲*Figure 45: unManaged Device List*

4.3.2. Add unManaged Device

Users can manually add or label devices not connected to the platform for display on the topology (refer to: Add unManaged Device). Added unmanaged devices are available for selection when adding device nodes in the topology's Edit Mode.

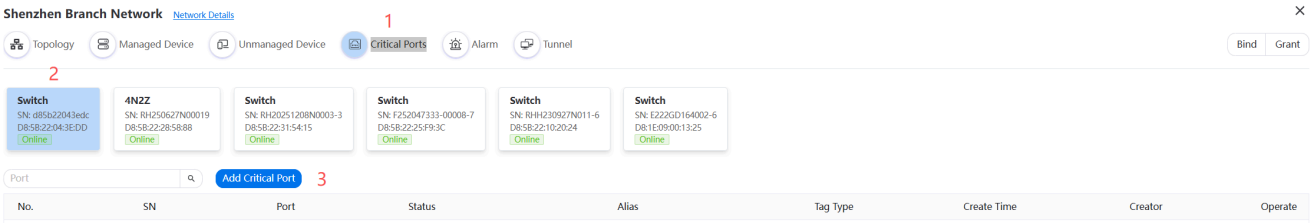
4.4. Critical Ports

4.4.1. Concept

A device port becomes a Critical Port when it connects to a key device. Critical Ports typically require special attention. Once a port is marked as a Critical Port, its UP/DOWN abnormal status will be closely monitored.

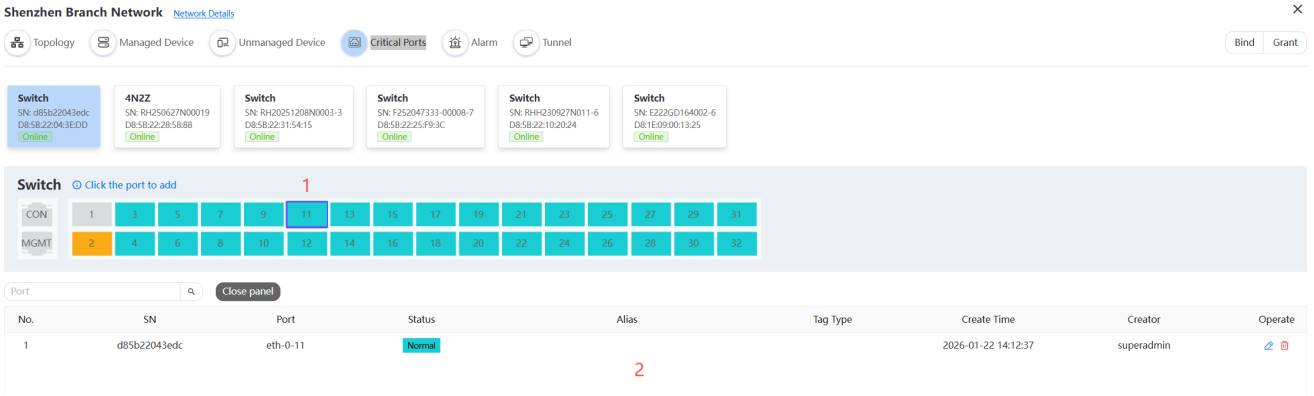
4.4.2. Panel Introduction

The Critical Ports module consists of three parts: Device List, Port Panel (hidden by default), and Port List. Users can select devices by differentiating them via serial number, alias, online status, etc., as shown:



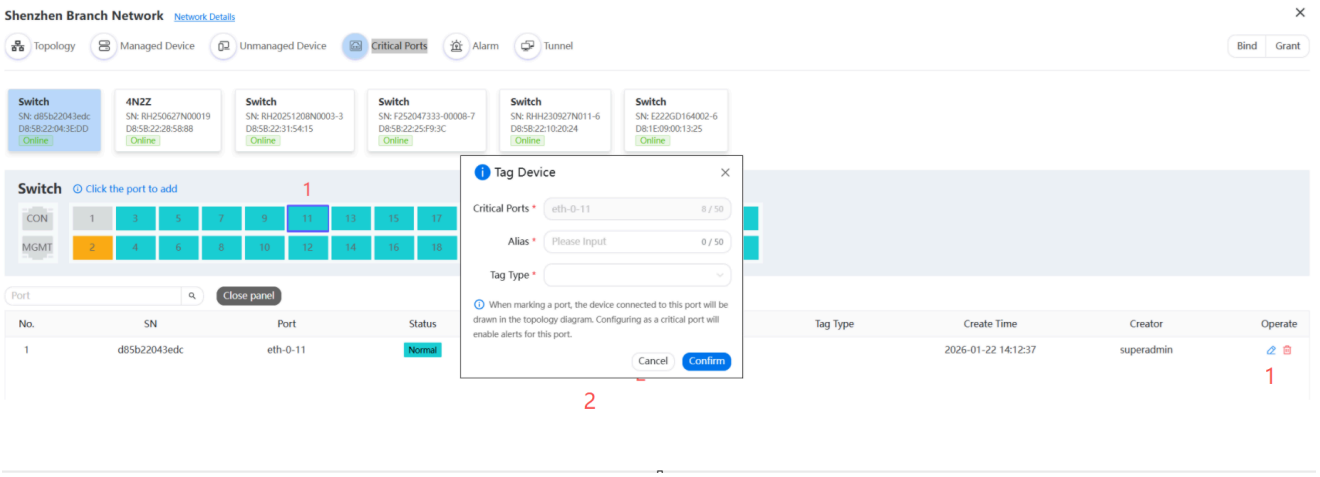
▲*Figure 46: Critical Port Device List*

After selecting a device and clicking the "Add Port" button, the port panel for that device is displayed. The Port List shows already added Critical Ports. Clicking a port on the port panel automatically adds it to the Port List, marking it as a Critical Port.



▲*Figure 47: Critical Port Addition Panel*

After adding a Critical Port, if you need to set the device type for that Critical Port, click the "Edit" button for the Critical Port. A dialog pops up to select the device type connected to that Critical Port.



▲*Figure 48: Set Critical Port Device Type Dialog*

After setting, the corresponding device icon will be displayed in the topology diagram.

4.4.3. Impact

- **Impact 1**
  Setting a Critical Port will monitor its UP/DOWN status and generate alarms;
- **Impact 2**
  After setting a Critical Port, the device connected to it will be displayed on the relevant topology diagram;

4.4.4. Remove Critical Port

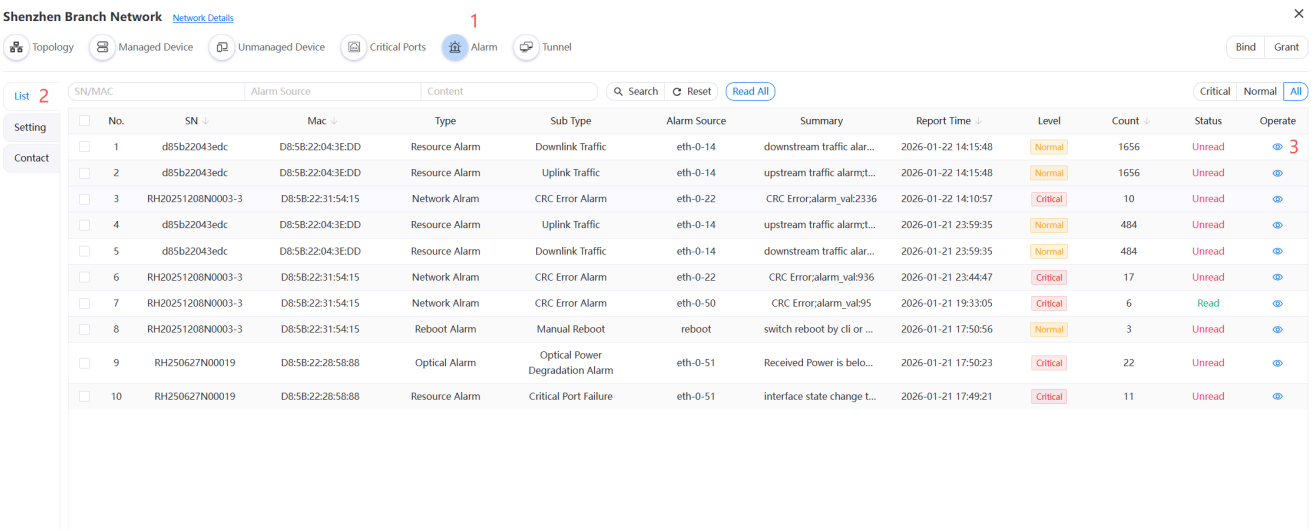
When the device connected to a Critical Port changes, the original Critical Port setting can be removed to avoid misjudgment. Go to the Critical Ports page, find the changed Critical Port, and click the "Delete" button in the Actions column.

4.5. Alarms

Alarm Information aggregates all alarms generated by devices in the current network. It is divided into three parts: Alarm Records, Notification Settings, and Alarm Contacts.

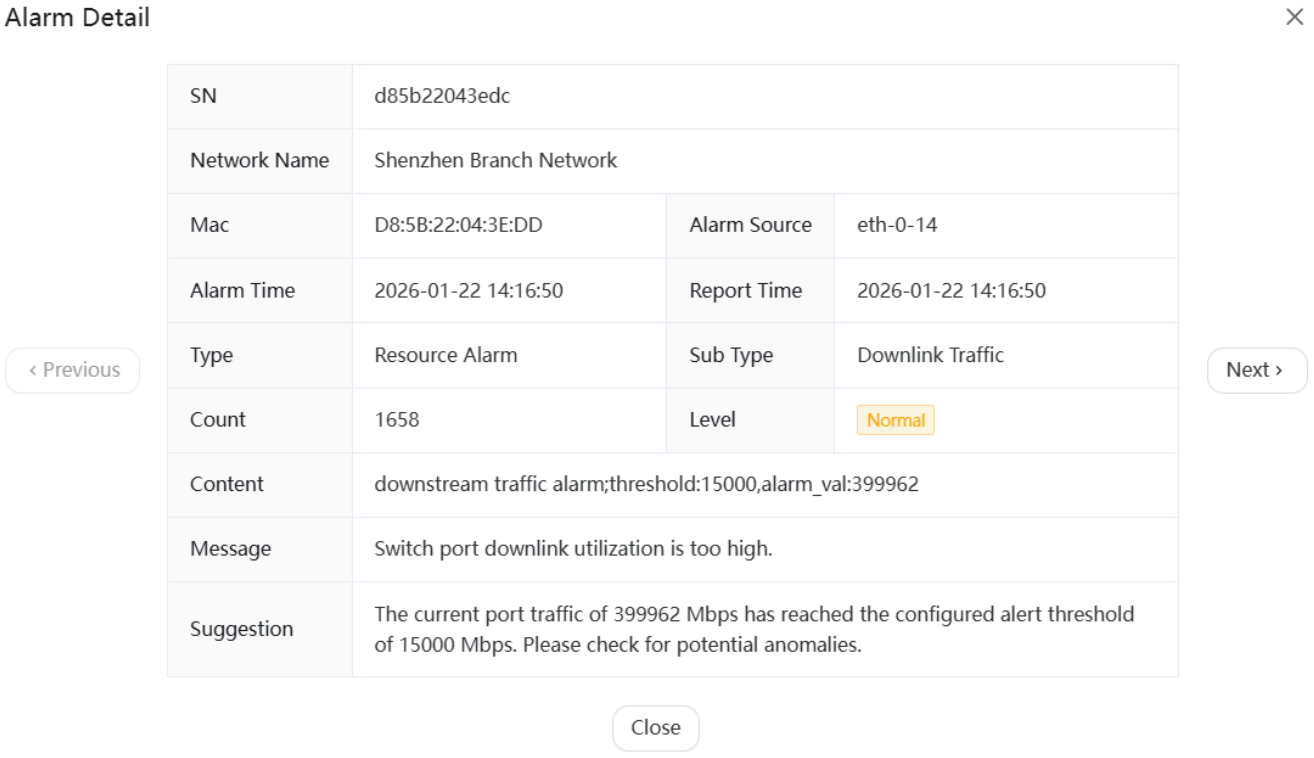
4.5.1. Alarm Records

Alarm Records display alarms from all devices in this network. Identical alarm data is automatically aggregated daily, using the date as the identifier. Aggregated alarms only show the latest data time. The "Mark All as Read" function sets all unread alarms to read status at once. Alarm Records are shown as:



▲*Figure 49: Alarm Records List*

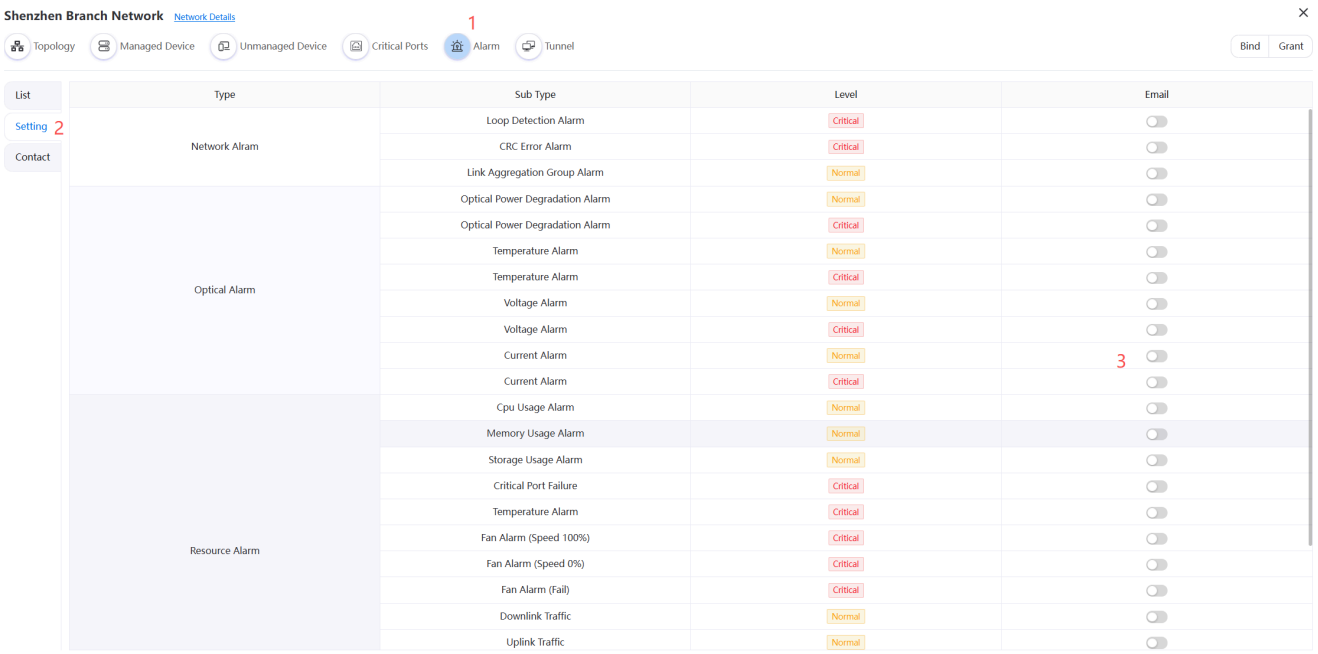
In Alarm Records, click the "View" button for an alarm to see its details, as shown:



▲*Figure 50: Alarm Details*

4.5.2. Notification Settings

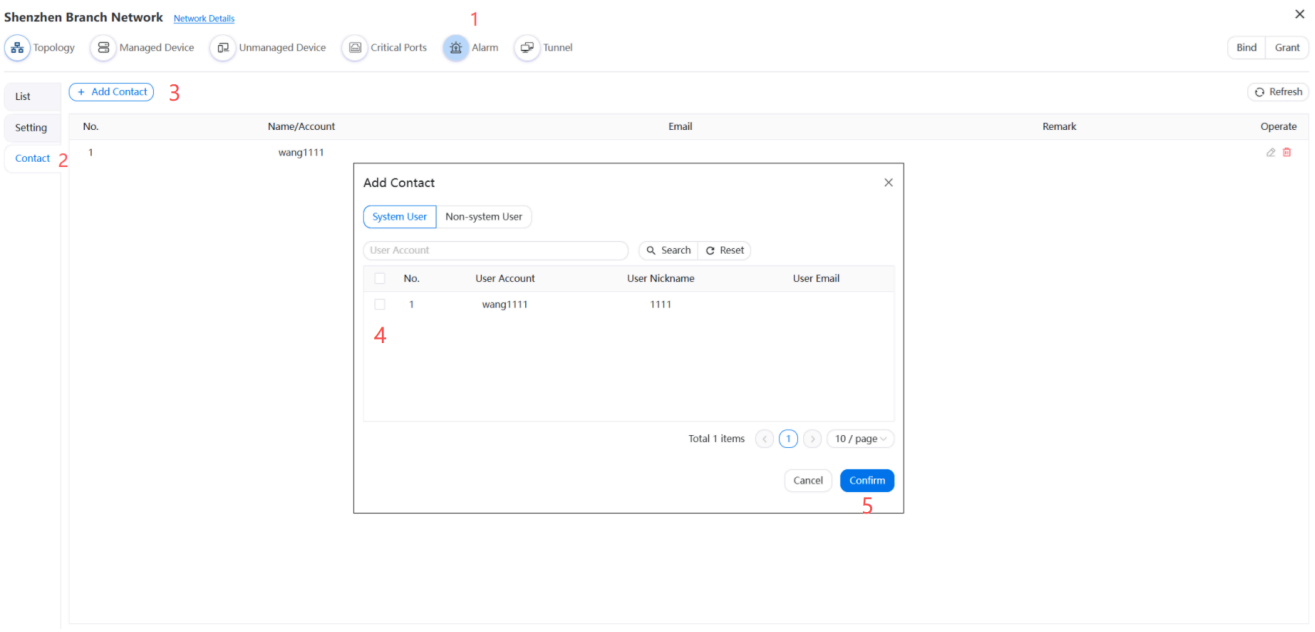
Click on a network to enter the Network Details page, then click "Alarm Information -> Notification Settings" to select and enable the alarm items for which notifications are needed.



▲*Figure 51: Alarm Notification Settings Page*

4.5.3. Alarm Contacts

Alarm Contacts are divided into System Contacts and Non-System Contacts. Contacts not registered in the system can be added as Non-System Contacts. Added alarm contacts automatically receive all enabled alarms from this network. The Alarm Contacts interface is shown as:



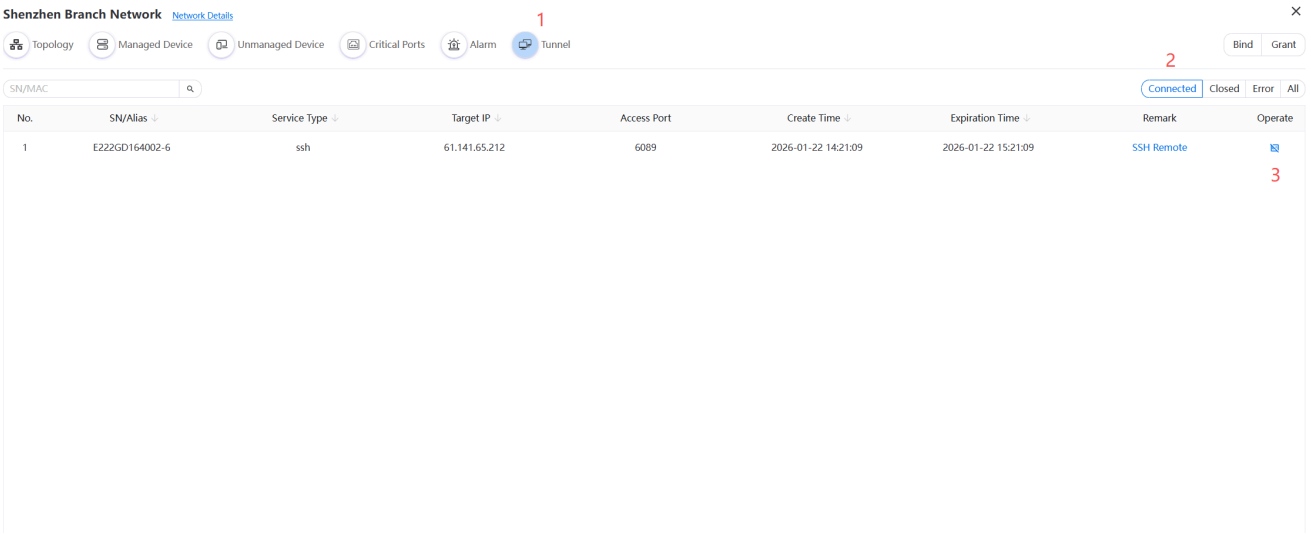
▲*Figure 52: Alarm Contacts Page*

4.6. Maintenance Tunnel Management

Records of Remote Maintenance tunnels created by users can be viewed in Tunnel Management. Tunnel Management allows closing or restoring created tunnels.

4.6.1. Tunnel List

The top right corner of the Tunnel List has tags: Connected, Closed, Abnormal, All. Click these tags to quickly filter tunnel connections of different statuses



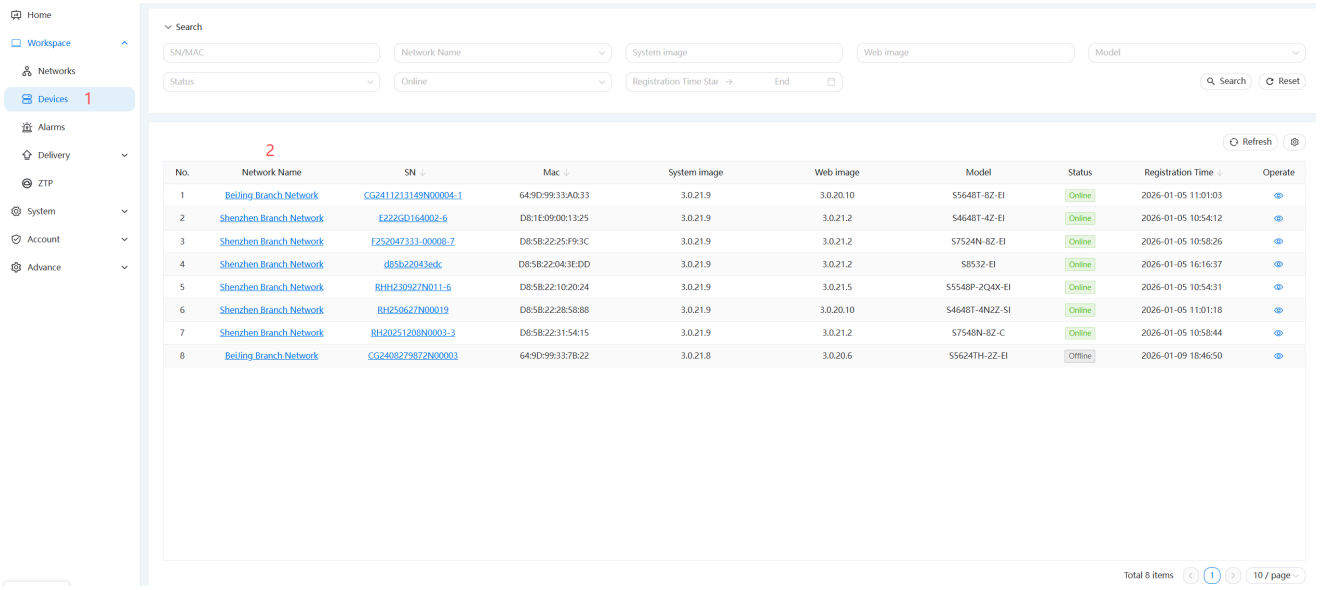
▲*Figure 53: Tunnel Management List*

- **Access Tunnel**
  For tunnels in the "Connected" state, click the link in the Remarks column to access the tunnel. Details can be found in Remote Maintenance.
- **Close Tunnel**
  Tunnels in the "Connected" state can be closed directly via the "Close" button in the Actions column without waiting for timeout expiration.
- **Reconnect Tunnel**
  Tunnels in "Closed" or "Abnormal" states can be reconnected by clicking the "Reconnect" button in the Actions column.

5. Device Management

5.1. Overview

The Device Management module provides a quick overview of the global status of all device assets within your permissions, enabling real-time tracking of performance metrics, identification of bottlenecks, optimization of operational configurations, ensuring effective resource utilization for optimal network performance.

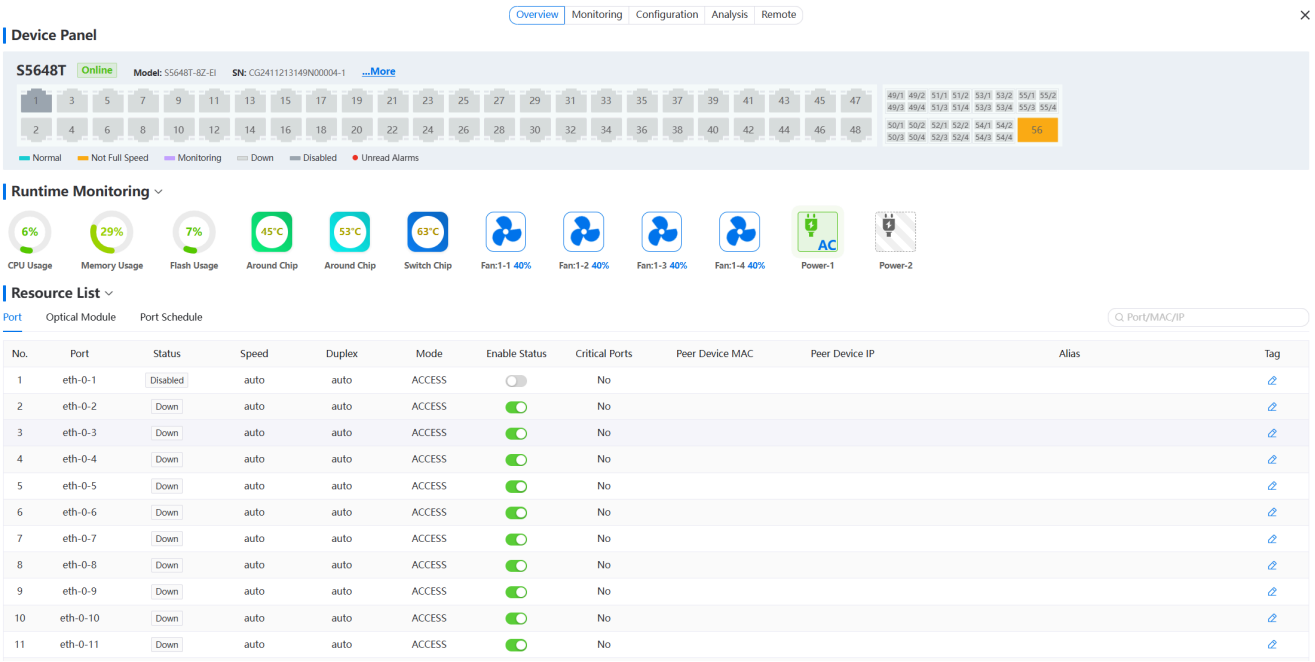


▲*Figure 54: Device Management Page*

> **Note**
> In tenant mode, tenants can only view their own tenant's data; platform administrators cannot view devices. In private mode, platform administrators can view all devices.

5.2. Monitoring Panel

The Device Monitoring Panel is divided into three areas: Device Panel, Runtime Monitoring, and Resource List.



▲*Figure 55: Device Monitoring Panel*

5.2.1. Device Panel

At the top, it presents a simulated device port layout to the user, along with basic device information such as online status, model, serial number, and port status. Real-time information is displayed when the device is online; the last known information is shown when offline. The color meanings for device ports in different states are shown in the table below:

No.	Icon	Port Status
1		Normal
2		Not Full Speed
3		Bypass Monitor
4		No Cable
5		Disabled
6		Unread Alarm (Red dot on port)

▲*Table 6: Port Status Description*

> **Note**
> The cloud platform currently does not support directly viewing bypass monitoring data; it only displays the status. Refer to the device user manual if needed.

Serial and Management ports are identified as CON and MGMT on the device panel, as shown in the table below:

No.	Icon	Description
1		Serial Port (CON)
2		Management Port (MGMT)

▲*Table 7: Serial & Management Port Icons*

5.2.2. RunTime Monitoring

RunTime Monitoring integrates rich monitoring metrics:

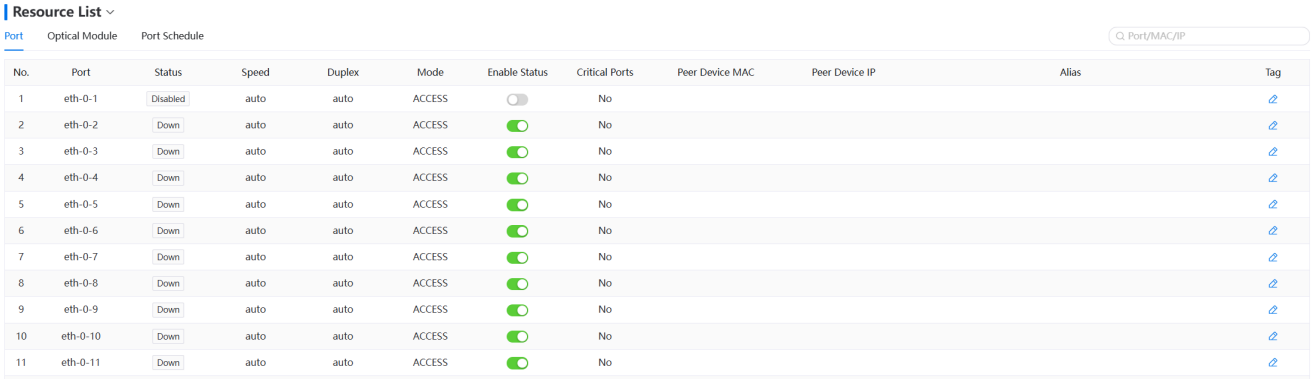
- CPU|Memory|Flash|Temperature
  The higher the CPU, memory, flash utilization, and temperature, the darker the icon color;
- Fans
  Fans animate faster as speed increases. If a fan is not spinning, it can be immediately identified as missing or faulty;
- Power Supply
  The power supply working status has three colors: Green, Red, Gray. Their meanings are as follows:

No.	Color	Description
1	Green	Normal
2	Red	Power supply present but no power
3	Gray	Power supply absent

▲*Table 8: Power Supply Color Description*

5.2.3. Port Control

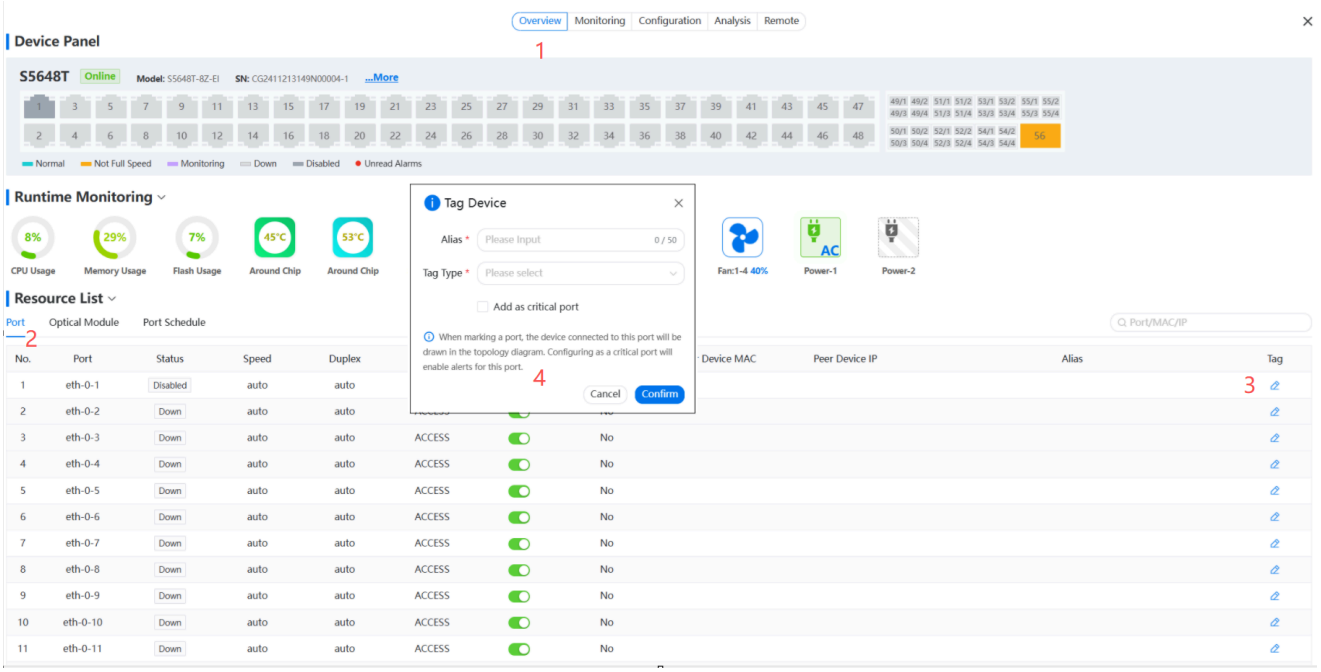
The user can manually control the **Port** by setting it to shutdown or no shutdown., as shown below:



▲*Figure 56: Port List and Port Control*

5.2.4. Port Tagging

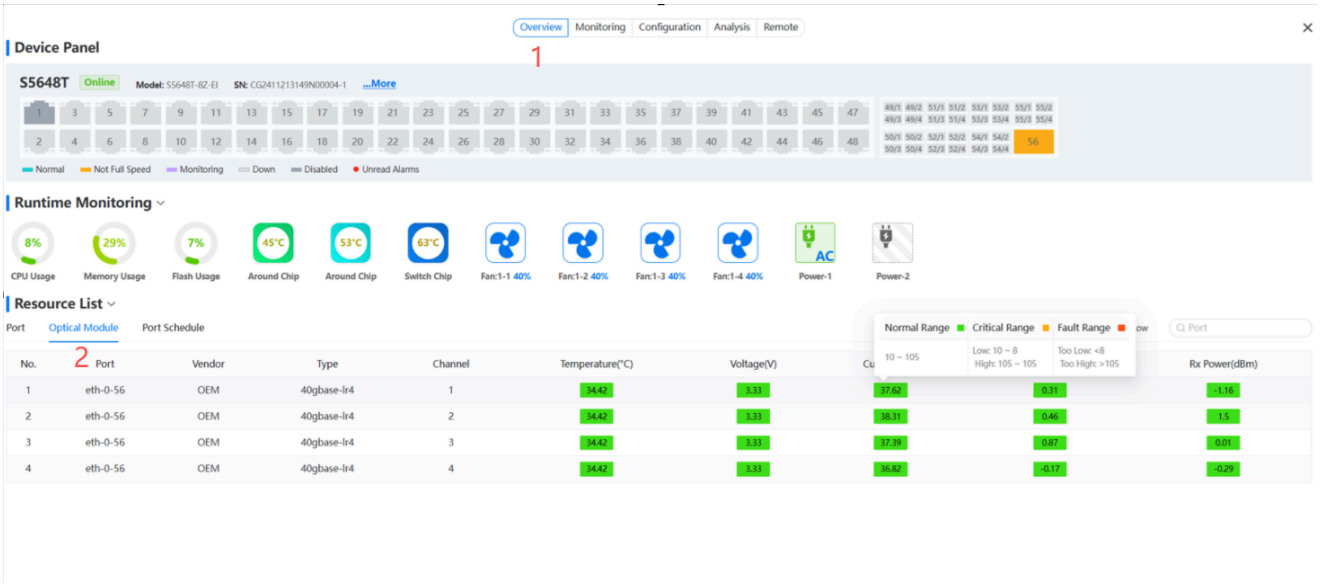
To facilitate port identification, the platform provides port tagging functionality. In the Actions column of the Port List, you can tag a port's alias and whether it is a Critical Port. Tagging a device will automatically draw the device of the tagged type in the topology. If marked as a Critical Port, Critical Port alarms are automatically enabled, as shown:



▲*Figure 57: Port Tagging Operation Interface*

5.2.5. View SFP Module Information

SFP module information can be viewed in the SFP Module List, which displays all SFP module operational data for the device, including module name, vendor, type, channel, temperature, voltage, current, transmit power, and receive power, as shown:



▲*Figure 58: SFP Module List*

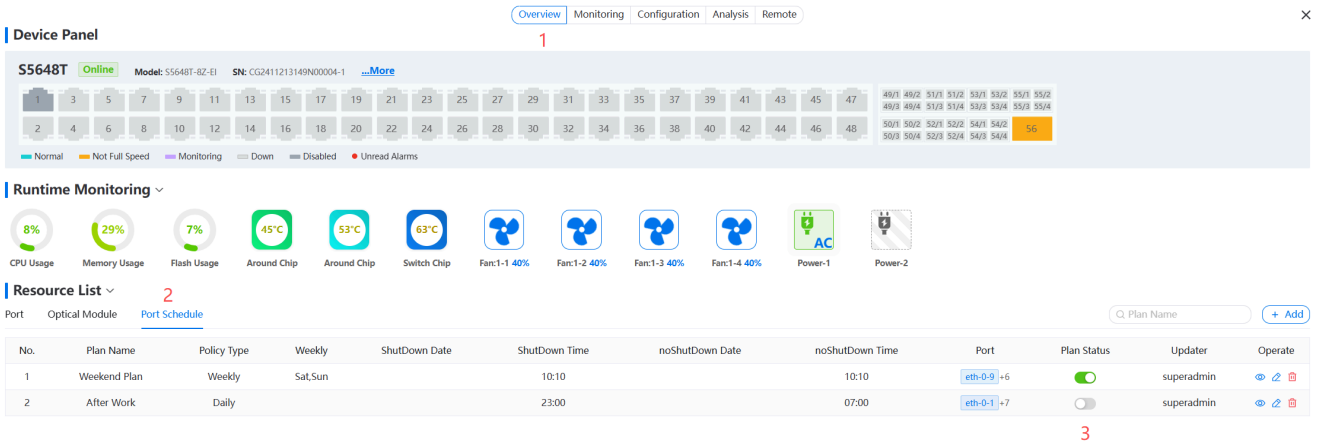
Hovering the mouse over a specific metric shows its normal range. The platform uses green, orange, and red to indicate the status of operational metrics, with specific meanings as follows:

No.	Color	Description
1	Green	Normal
2	Orange	Critical Range
3	Red	Abnormal Range

▲*Table 9: SFP Module Metric Color Description*

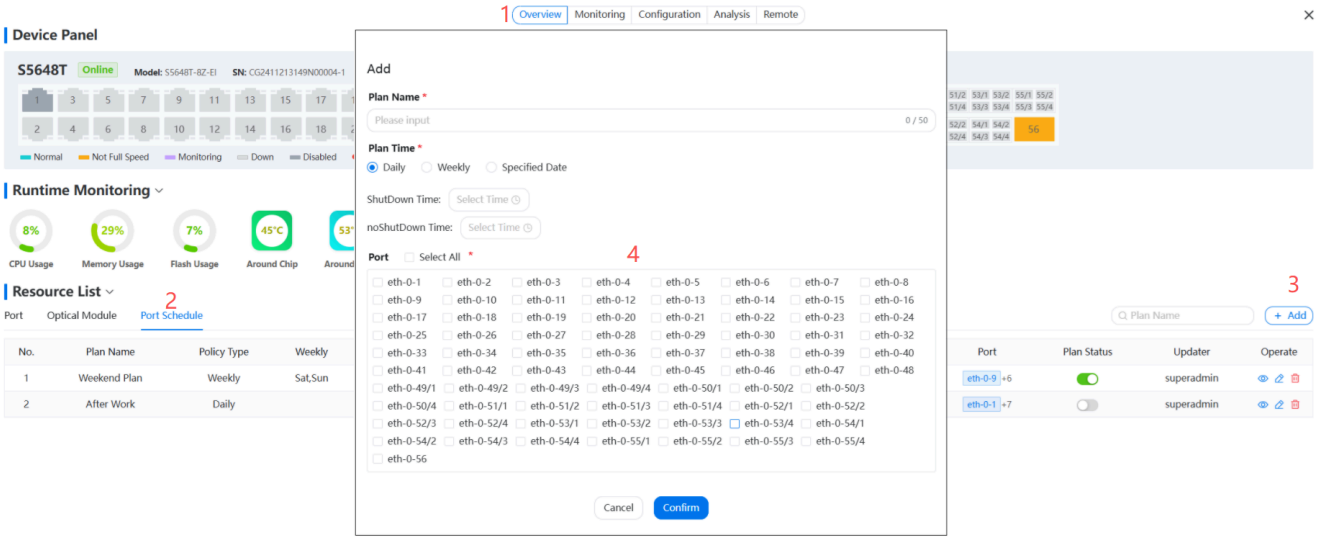
5.2.6. Port Schedule

Users can create schedules for port enable/disable based on usage needs. After creating a port schedule, it is **disabled by default** in the list. If needed, it can be manually enabled. Once the schedule is enabled, the platform will disable the port at the scheduled start time and re-enable it at the scheduled end time.



▲*Figure 59: Port Schedule List*

Click the "Add" button above the list to pop up the Add dialog. Add content includes Schedule Name, Schedule Time, and ports to execute on. Schedule Time can be set to execute daily, weekly, or on specific dates. By default, the port is disabled at the start time and enabled at the end time.



▲*Figure 60: Add Port Schedule Dialog*

> **Note**
> For a single port, daily, weekly, and specific date policies are not allowed to have overlapping time periods.

5.3. Port Monitoring

5.3.1. Port Traffic Graph

Clicking a port on the device panel displays that port's real-time operational data and traffic trend graph. The trend graph shows traffic volume and packet data for the port over the past 7 days, defaulting to 1-hour intervals. The two differently colored "max" icons on the graph indicate the maximum values for upstream and

downstream traffic.

▲*Figure 61: Port Traffic Monitoring*

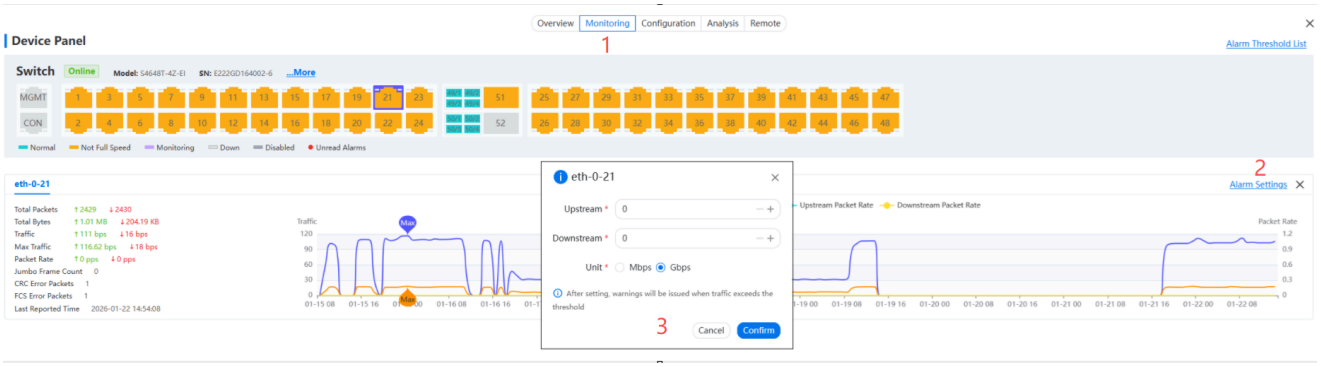
5.3.2. Traffic Graph Zoom

The traffic graph defaults to 1-hour interval data. To view more granular data, move the mouse over the traffic graph, and a vertical dashed line will appear. Hold down the left mouse button and drag the line horizontally (up to a 6-hour range) to view 5-minute interval data within the dragged range. Click the "Reset" button to restore the initial state. As shown:

▲*Figure 62: Traffic Graph Time Region Zoom Operation*

5.3.3. Traffic Alarm Setting

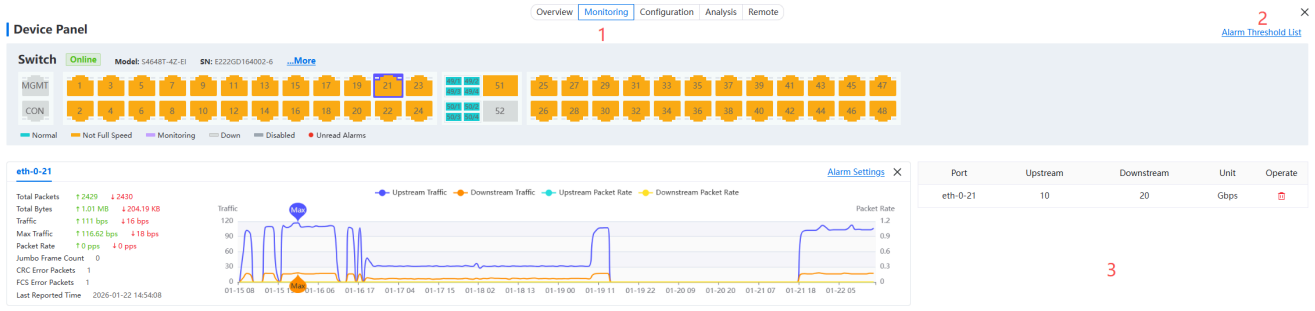
To monitor traffic on a specific port, users can set the traffic alarm threshold for that port. In the top right corner of each port's trend graph, there is an "Alarm Threshold Setting" label (as shown in step 3 in the figure). Clicking it opens the setting interface, as shown below:



▲*Figure 63: Port Traffic Alarm Threshold Setting*

5.3.4. View Alarm Settings

When to view the traffic alarm thresholds for all ports, click the "Alarm Threshold List" label in the top right corner of the device panel. It displays all alarm thresholds for the device's ports, with a delete function in the Actions column.

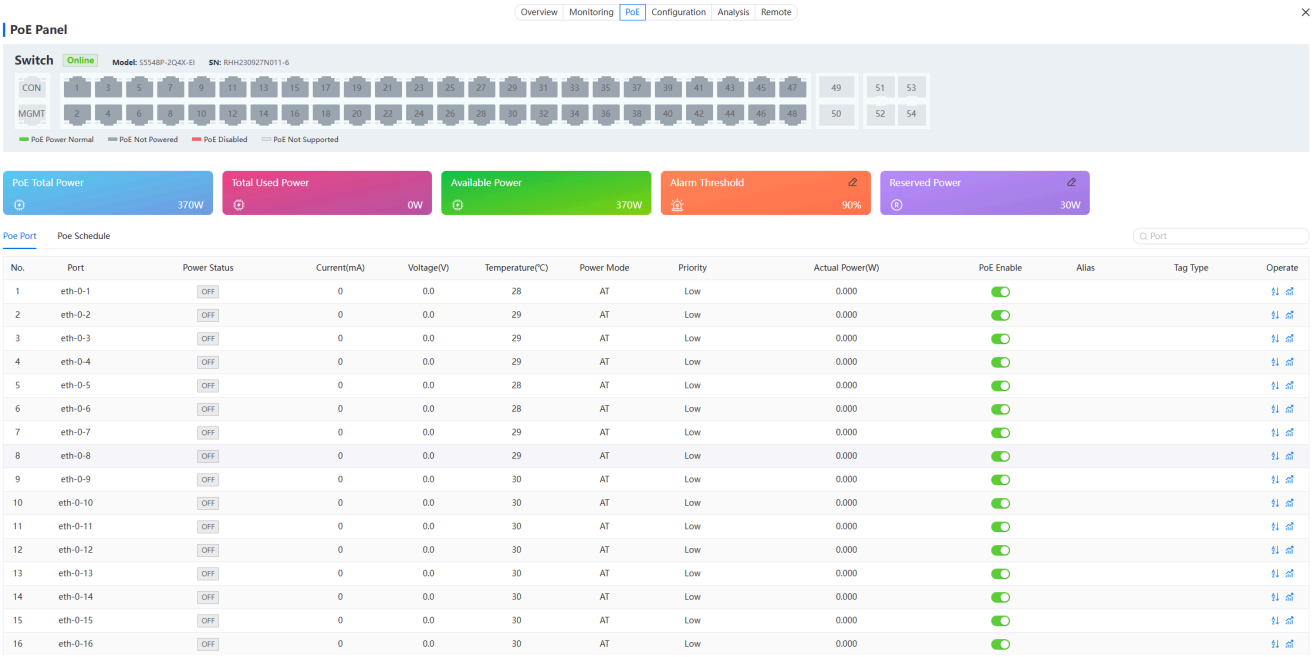


▲*Figure 64: Port Traffic Alarm Threshold List*

5.4. POE Management

5.4.1. POE Panel Introduction

The POE Panel mainly consists of Port Panel, POE Statistics, POE Monitoring List, and POE Schedule. The POE Monitoring List monitors metrics like current, voltage, power, temperature, priority, etc., as shown:



▲*Figure 65: POE Management Panel*

The color meanings for POE port statuses are shown in the table below:

No.	Icon	Port Status
1		POE Power Normal
2		POE No Power (No device connected)
3		POE Disabled
4		Non-POE Port

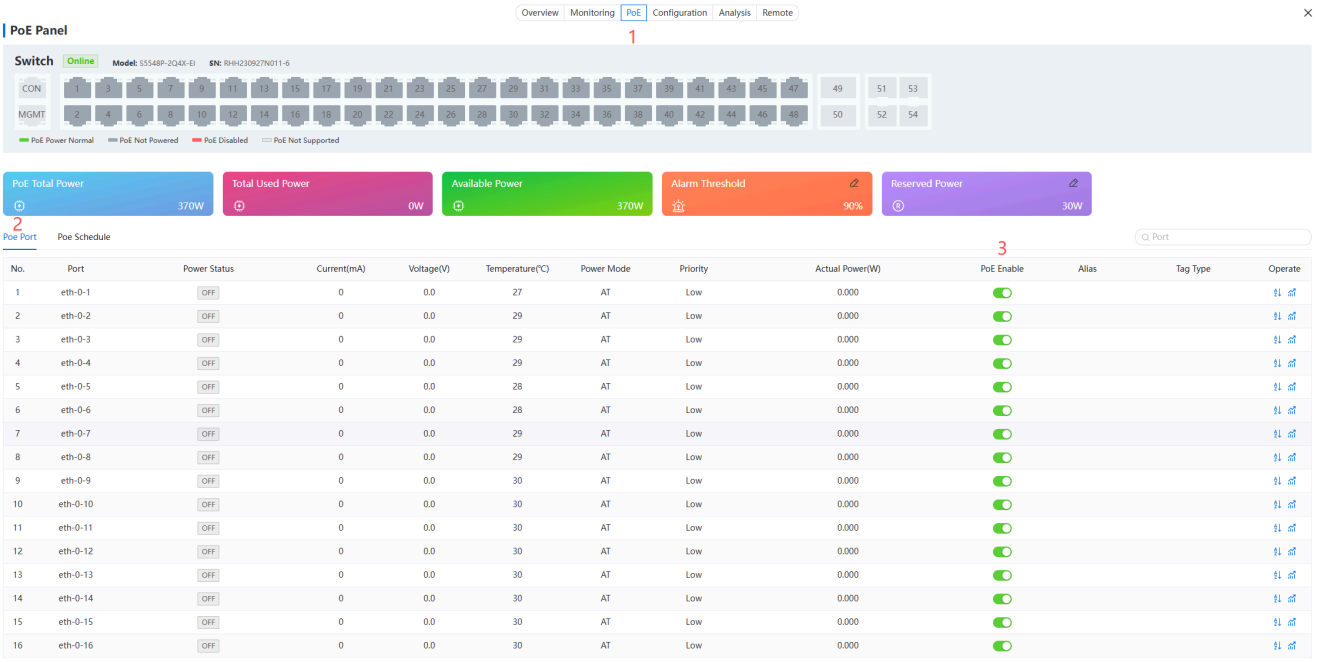
▲*Table 10: POE Port Status Description*

No.	Icon	Button Description
1		POE Priority Setting
2		POE Trend Graph

▲*Table 11: POE Actions Column Icons*

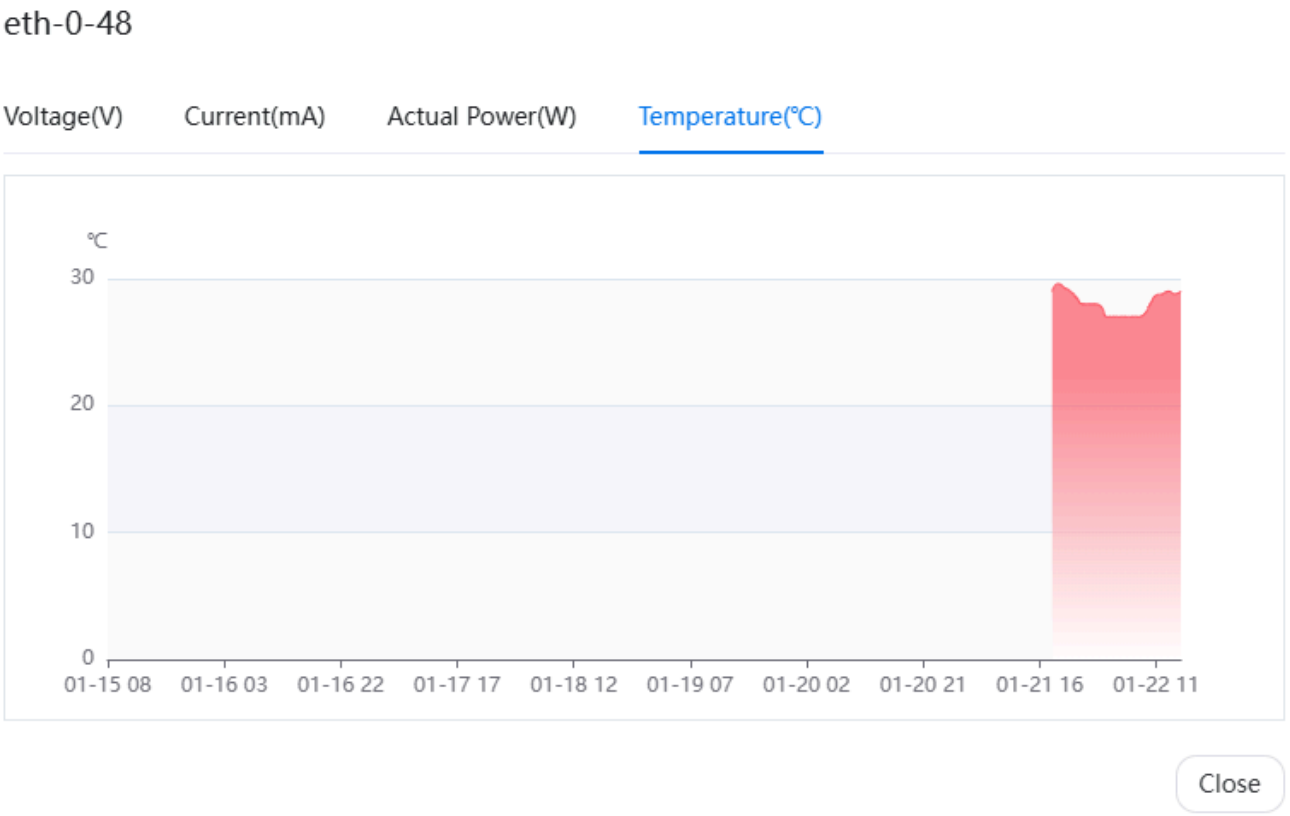
5.4.2. POE Basic Configuration

- POE Port Power On/Off
  Users can manually control the on/off state of each POE port in the POE List based on requirements.



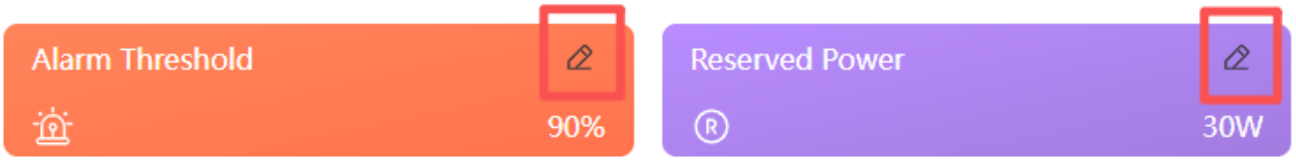
▲*Figure 66: POE Port Power Switch Control*

- POE Historical Power Usage
  Clicking a port on the POE Panel or the history icon for a port in the POE List displays trend graphs for that port's current, voltage, temperature, and power (as shown). To view more detailed data, refer to the Traffic Graph Zoom operation for port traffic.



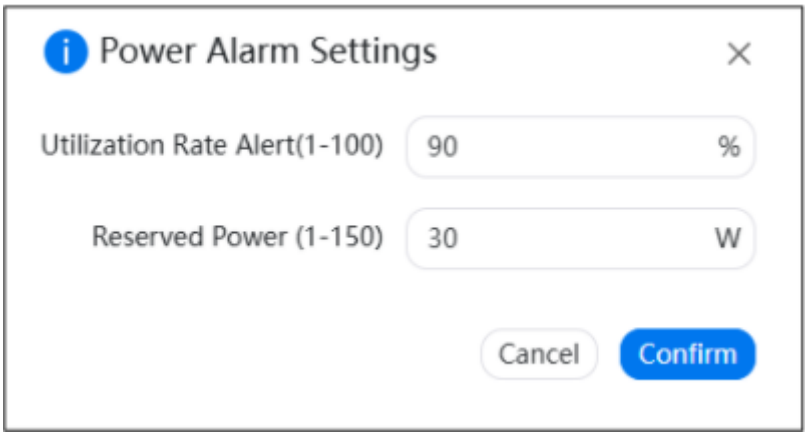
▲*Figure 67: POE Port Monitoring Metric Trend Graph*

- Adjust Power Alarm Settings
  POE Power Alarms include Total Power Utilization Alarm and Reserved Power Alarm metrics, located as shown:



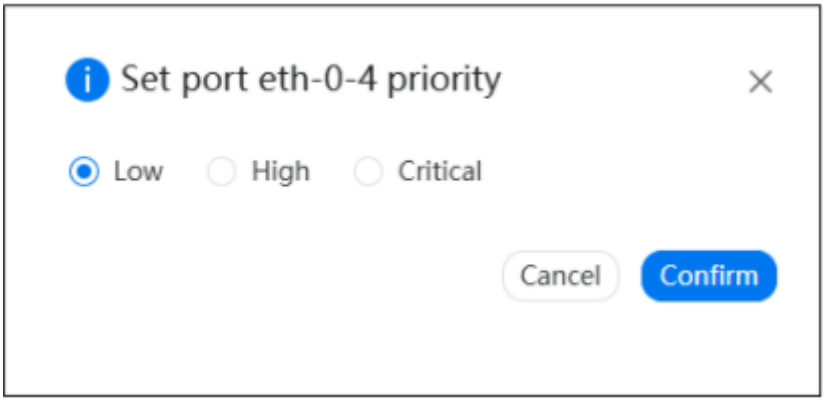
▲*Figure 68: POE Power Alarm Setting Entry*

Click the "Edit" button to configure, including total power utilization and reserved total power. The setting interface is shown below:



▲*Figure 69: POE Total Power Alarm Setting Dialog*

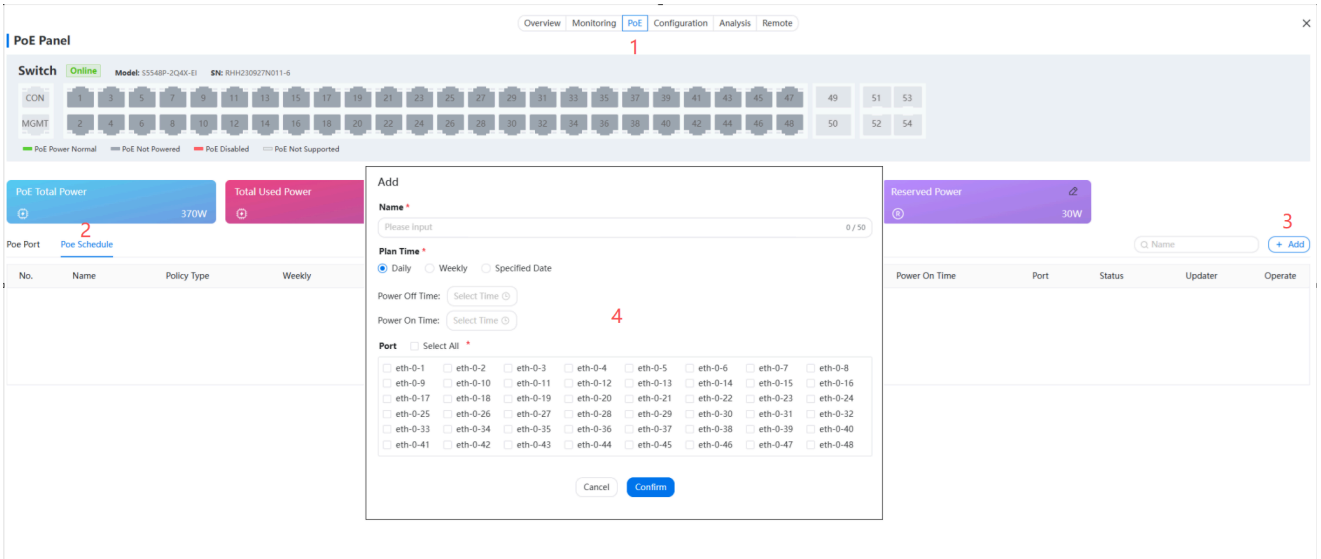
- Priority Setting
  POE Priority is mainly used when the switch's total power supply is insufficient, determining which devices get power first to ensure critical business continuity. The priority for each POE port is set in the Actions column of the POE Port List. Click the priority setting button to pop up a dialog, where you can set Low, Medium, or High priority:



▲*Figure 70: POE Port Priority Setting Dialog*

5.4.2. POE Energy Saving Schedule

POE Energy Saving Schedules, when used appropriately, can significantly save device energy consumption. In the POE Schedule interface, click the "Add" button to pop up the interface for creating a POE schedule, as shown:



▲*Figure 71: Add POE Schedule Dialog*

Step 1: Configure Basic Schedule Information

Schedule Name (required), fill in a custom name in the "Name" input box

Name length limit: maximum 50 characters

Suggested naming convention: Location_Function_Time (e.g., Office_AP_NightMode)

Step 2: Set Power Schedule Strategy

Select the schedule execution cycle type: Daily (repeat daily), Weekly (repeat on specified weekly times), Specific Date (execute once on a specific date)

Input the Stop Power time and Restore Power time

Step 3: Select Application Ports

The port selection area displays all available ports (e.g., eth-0-1 to eth-0-48)

Step 4: Save Configuration

Cancel: Discard current configuration, return to previous interface

Confirm: Save all settings, create a new POE schedule. By default, created schedules are disabled and need to be manually enabled in the POE Schedule list to take effect.

> **Caution**
> When creating a POE schedule, the schedule times for POE ports cannot conflict.

5.4.3. Application Scenarios

The core value of POE Schedules lies in transforming POE power supply from "always on" to "on-demand," primarily serving four goals: energy saving, security, device lifespan management, and automated operations.

- **Energy Saving & Cost Control**
  - Automatic power off after work: Set weekdays 18:00 to next day 8:00 to automatically turn off power to IP phones, wireless APs (key APs can be retained via other means), desktop devices, etc., in office areas.
  - Full-day power off on weekends: Turn off power to non-critical area surveillance cameras, displays, etc., on weekends.
  - Power schedule based on timetable: Supply power to classroom wireless APs, projectors, etc., only during class times (e.g., 8:00-12:00, 14:00-18:00).
  - Holiday mode: Turn off POE power for most floors during holidays like winter/summer breaks.
- **Security & Access Control Enhancement**
  - Access Control Systems: Can be set to cut power to secondary access card readers during non-working hours (e.g., late night) to increase security (ensuring critical access like fire exits remains unaffected).
  - Scenario-based on/off: Cameras inside warehouses can be turned off when no one is working and automatically turned on during security patrols or when alarms are triggered.
  - Misleading shutdown: Intentionally turning off power to cameras in obvious locations as part of a security strategy (use with caution).
- **Device Lifecycle Management**

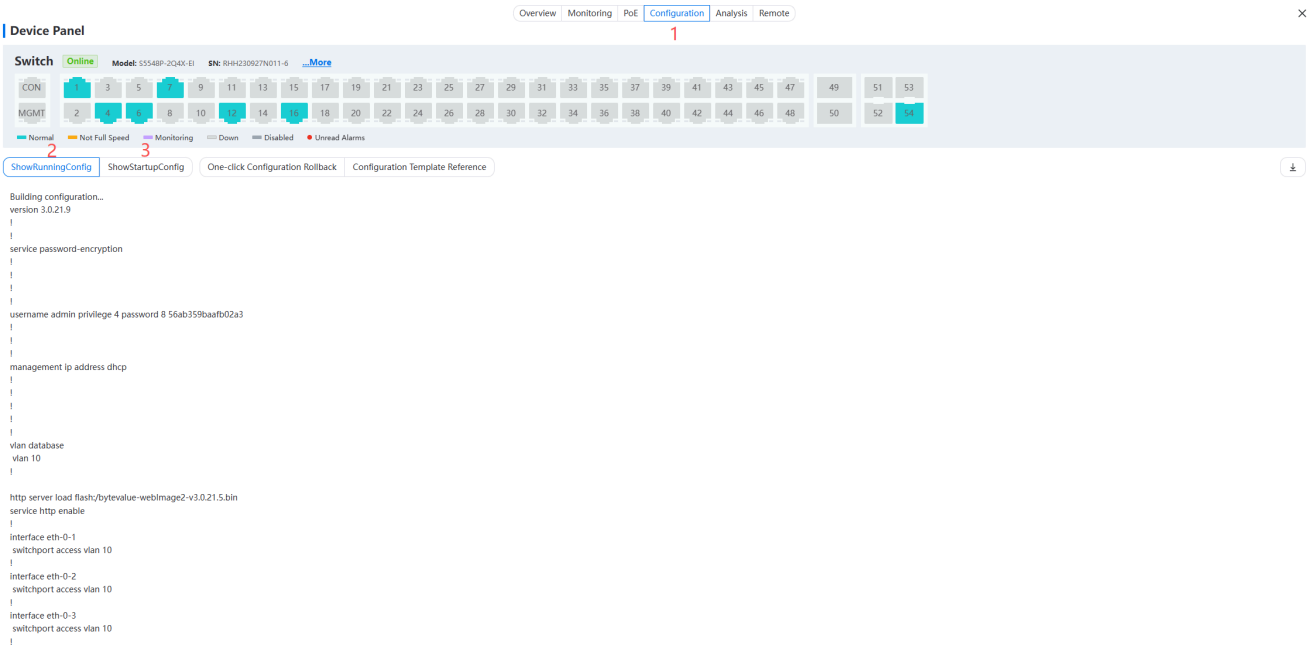
    - Regular reboot/refresh: Set a schedule for devices that may develop dead processes from long-term operation (e.g., certain wireless APs, digital signage) to automatically power off at 3 AM every Sunday, power on 5 minutes later, achieving automated soft reboots to improve system stability and reduce manual intervention.
    - Extend device lifespan: Allow non-24/7 essential devices to rest periodically, reducing continuous operation time, theoretically extending hardware lifespan.
- **Network Policy & Traffic Management**
    - Guest Network Control: Set power schedules for wireless APs dedicated to guest networks, e.g., provide guest network only on weekdays 9:00-17:00.
    - Children's Internet Management: The POE port connecting to network devices in a child's room can be scheduled to power off after 22:00, forcing a network disconnect.

5.5. Device Configuration

The Cloud Management Platform's configuration management mainly includes real-time configuration viewing, one-click configuration rollback, and configuration template library reference.

5.5.1. Real-time Configuration Viewing

Entering the Configuration Template interface defaults to viewing the device's current running configuration (`show running config`). Switch to `show startup config` to view the device's startup configuration, as shown:

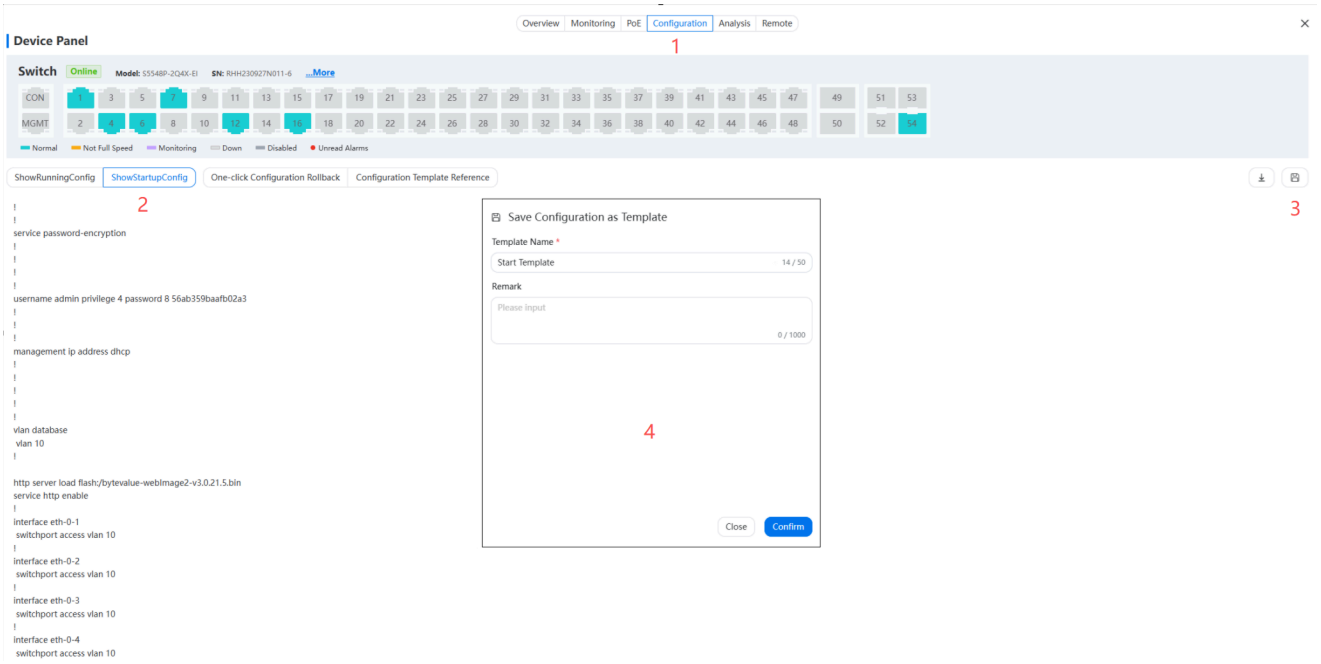


▲*Figure 72: Configuration Viewing Interface*

> **Note**
> Running & Startup Configuration Introduction:
>
> - `show running config`: The currently running configuration, includes unsaved commands entered via CLI;
> - `show startup config`: The startup configuration saved to the configuration file, does not include unsaved commands entered via CLI;

- **Save as Configuration Template**

  When viewing `show running config`, only a download button for the viewed content appears in the top right of the output area. When switched to `show startup config`, the viewed content can be downloaded and saved as a configuration template. Clicking the "Save" button shows:

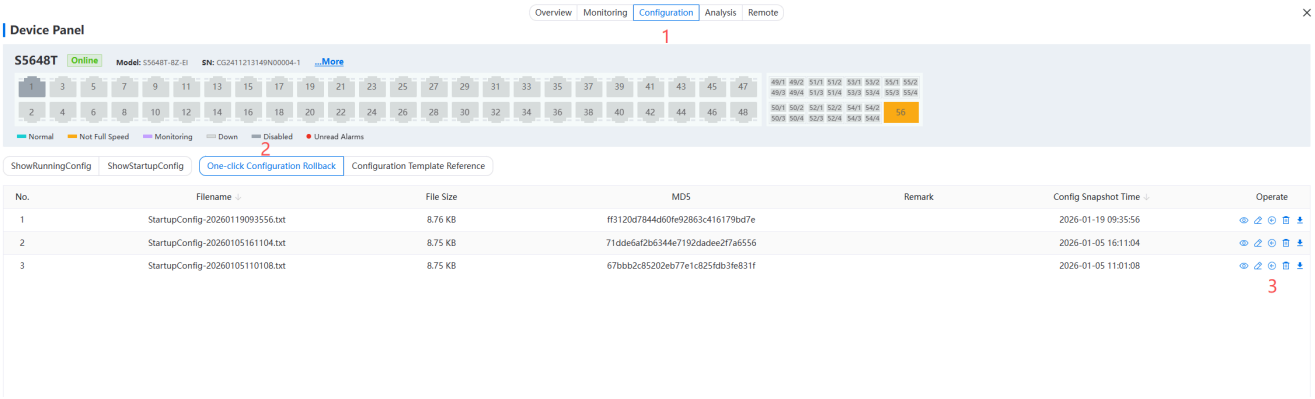


▲*Figure 73: Save as Configuration Template Library Dialog*

Enter the template name and click "Confirm" to save the configuration content as a template in the Configuration Template Library.

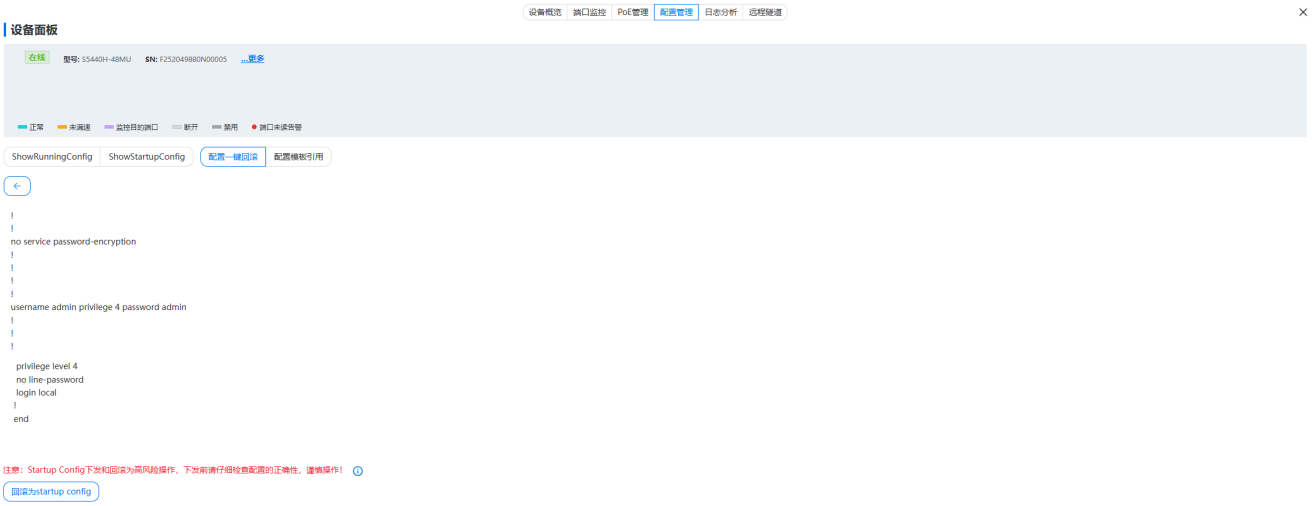
5.5.2. One-Click Configuration Rollback

- **Overview**
  When device configuration changes, the latest configuration file is automatically reported to the cloud platform. Duplicate configuration files on the cloud platform are automatically overwritten. Opening One-Click Rollback is shown in steps 1, 2 below:



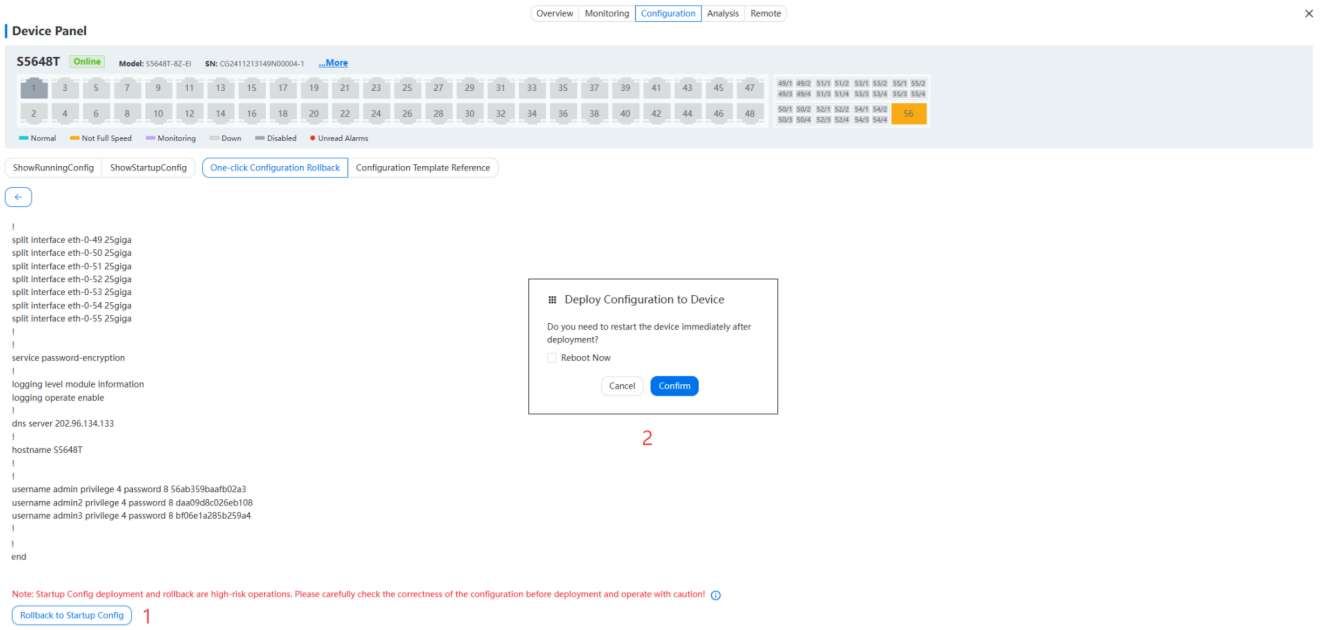
▲*Figure 74: Configuration Backup List*

- **Configuration Rollback**
  Configuration Rollback refers to restoring the device's **startup configuration** to a historical version backed up on the cloud platform. Before rolling back, users can view and download the backed-up configuration file in the Actions column to confirm it meets rollback needs. When a user decides to roll back to a specific configuration file, click the configuration rollback icon to enter the rollback interface, as shown:



▲*Figure 75: Configuration Rollback Interface*

After confirming the configuration content is correct, click the "Rollback to startup config" button. A dialog pops up to confirm whether to reboot the device during configuration deployment. Confirm to deploy the configuration to the device. As shown:



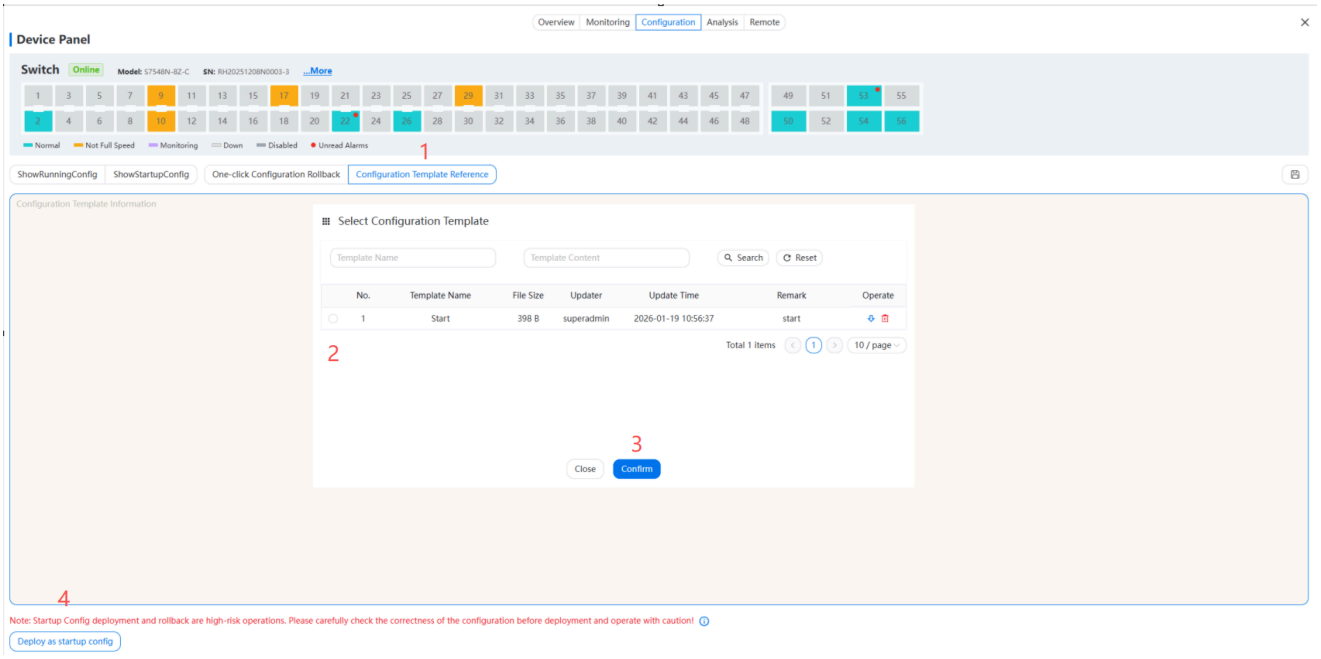
▲*Figure 76: Configuration Rollback Confirmation Dialog*

> **Note**
> If "Reboot immediately" is not selected before deployment, users can manually reboot via the `reboot` command when needed;

5.5.3. Configuration Template Reference

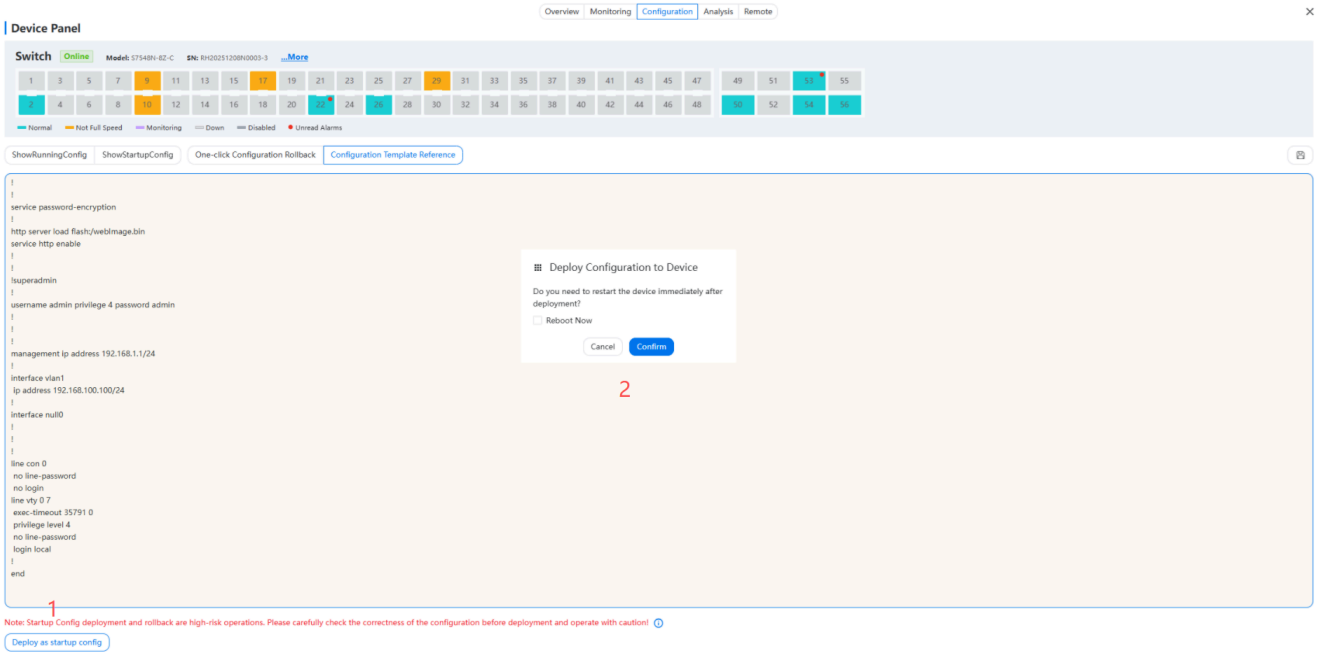
When users need to deploy similar configurations to multiple devices in bulk, they can first save one device's configuration as a configuration template. When deploying configurations to other devices, click the "Reference from Configuration Template Library" button and select that template.

Edit the configuration content and confirm it's correct, then click the "Deploy as startup config" button. A dialog pops up to confirm whether a reboot is needed during configuration deployment, as shown:



▲*Figure 77: Select Configuration Template Dialog*

Confirm to deploy the configuration to the device. If reboot was selected before deployment, it will reboot immediately. The edited result can also be saved as a new template in the Configuration Template Library by clicking the "Save" button in the top right corner.



▲*Figure 78: Edit Configuration and Deploy Interface*

> ⚠ **Warning**
>
> - It is recommended to always confirm if template content needs modification before using a configuration template;
> - The configuration template must include commands to enable the Cloud Management Service; otherwise, the device will be unable to connect to the cloud platform. To enable the cloud management configuration, refer to the following example:
> cloud control domain-port <cloud-server-port> domain-name <cloud-server-ip>
> cloud control version dhcs
> cloud control enable or cloud control mgmt-if enable

5.6. Logs & Diagnostics

Network device log analysis is a core tool for O&M personnel troubleshooting. Users can remotely extract log files stored locally on devices to the cloud platform for download. The Log Analysis function integrates device diagnostic reports and device operation logs.

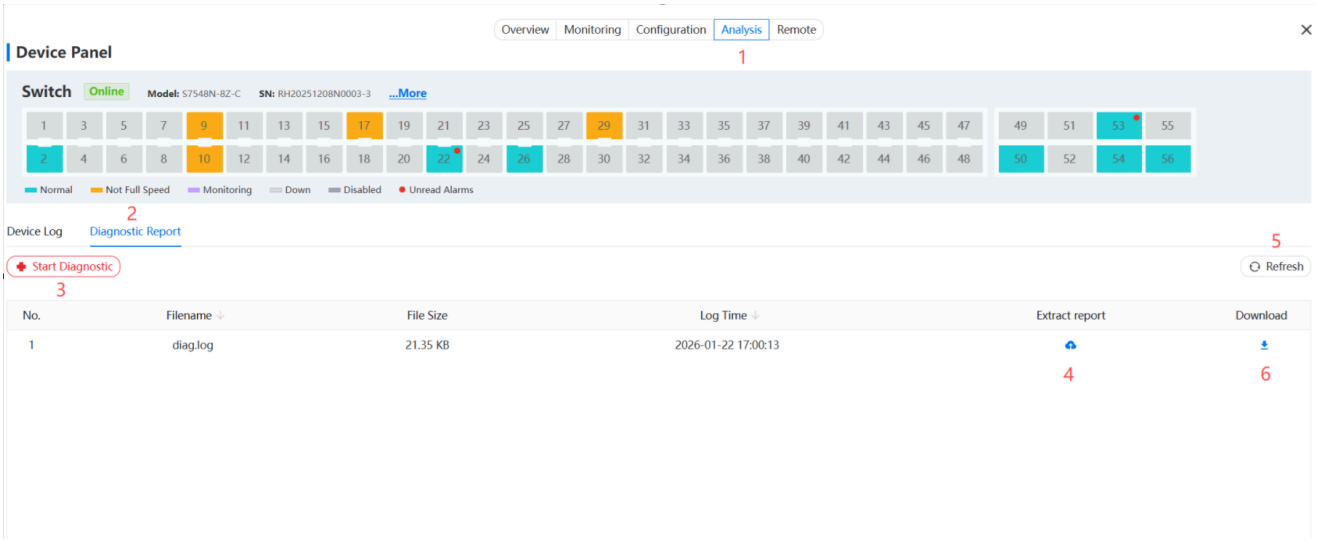
5.6.1. Device Diagnostic Report

The Device Diagnostic Report is a comprehensive diagnostic report, typically used for troubleshooting (network issues, performance degradation), configuration verification, system health checks, performance monitoring, and device status backup. Main content overview:

Report Section	Report Description
System Information	Device model, software version, uptime, serial number, hardware info, etc.
Configuration Information	Running configuration (`running-config`), startup configuration (`startup-config`)
Interface Status	Link status, speed, duplex mode, traffic statistics, error counts for all ports
VLAN Information	VLAN database, interface VLAN assignments
Routing Information	Routing table, ARP table, MAC address table
IP Settings	Management IP, gateway, DNS, static routes
Service Status	HTTP service, LLDP, Cloud Control, SSH/Web login status
Hardware Status	Power supply, fans, temperature sensors, SFP module info
Memory & CPU	Memory usage, CPU usage, process info
Log Information	System logs (syslog), error records, ARP refresh failure records
Diagnostic Commands	Summarized output of multiple `show` commands executed

▲*Table 12: Device Diagnostic Report Content*

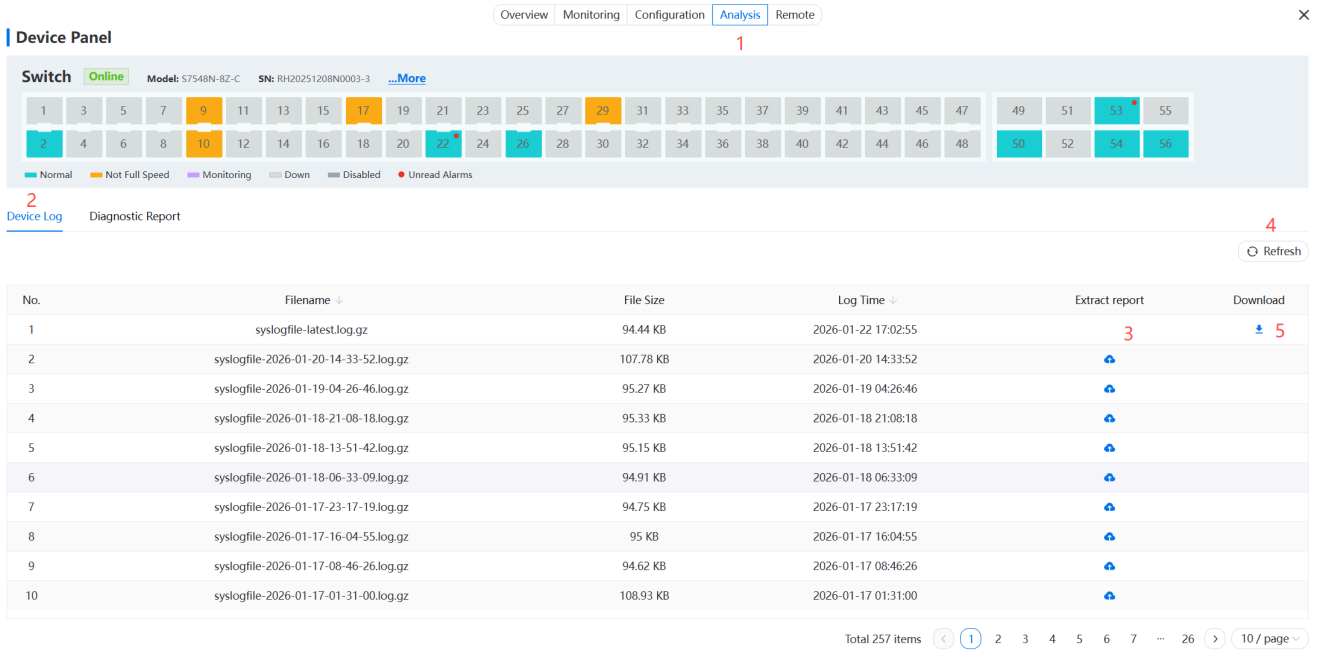
Enter the Diagnostic Report page and click the "Start Diagnosis" button. The platform will notify the device to generate a diagnostic report. Wait approximately 3 minutes for the device to generate the report. Then, click the "Refresh" button on the platform; the latest report record will appear in the Diagnostic Report list. Historical report records are deleted, keeping only the latest one. Click the "Extract" button; the report file is uploaded to the cloud platform, and a download button appears in the report list. Click to download and view. As shown:



▲*Figure 79: Diagnostic Report List*

5.6.2. Device Operation Logs

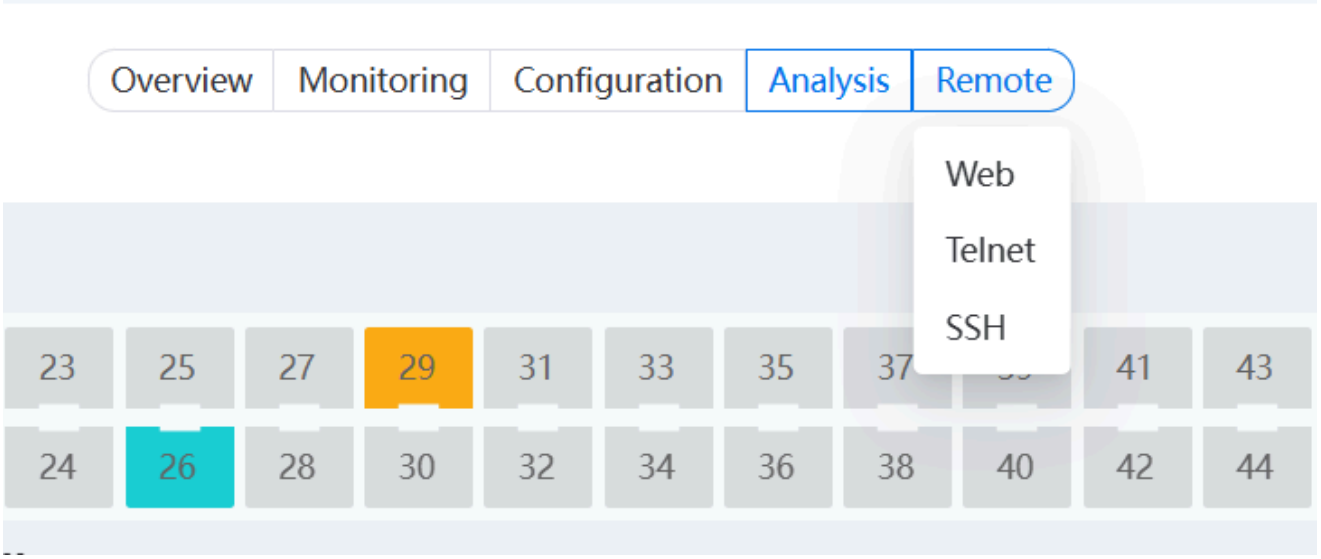
Device Operation Logs record device operation status, management communication behavior, abnormal errors, etc., serving as important evidence for network operation and troubleshooting. By filtering, correlating, and visualizing this log data, users can accurately analyze the root causes of historical faults and propose solutions. Opening the Log Analysis interface defaults to showing the current device's log file list. To view a specific log file, click the "Extract" button corresponding to that file. It will be extracted to the cloud platform, and a download button will appear. Click to download, as shown:



▲*Figure 80: Operation Log File List*

5.7. Remote Maintenance

Device Details provides a quick entry for device remote maintenance. Click the "Remote Maintenance" button to reveal three remote methods: web, Telnet, SSH. The default service duration is 1 hour, no user selection needed. The interface after selecting a remote method is referenced in Remote Maintenance.



▲*Figure 81: Device Details Remote Maintenance Entry*

6. Remote Upgrade

The platform provides centralized remote upgrade capabilities for device system software and built-in Web services. The upgrade operation is divided into two phases:

- Version Push: Push the upgrade command with the specified upgrade package file to the target device.
- Version Activation: Confirm and enable the downloaded new version on the device, completing the final upgrade.

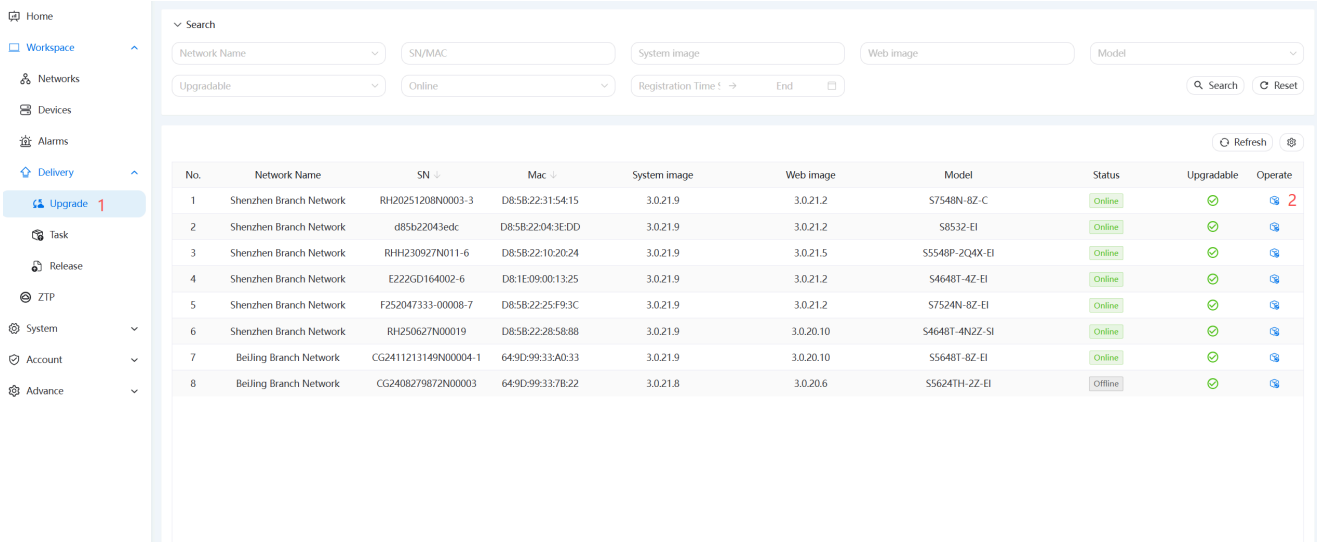
This process ensures controllability and safety of the upgrade, allowing full verification between push and activation.

6.1. Version Push

Version Push is the first step of the upgrade process. Its core task is to select and push the upgrade instruction to online and eligible devices. This function guides administrators through the upgrade instruction deployment operation.

6.1.1. Upgrade Device Selection

In the "Version Push" interface, the system lists all devices and their current upgrade status. Colors intuitively differentiate: green icons indicate upgradeable, gray icons indicate not upgradeable. Administrators can find target devices in this list and click the "Push" button in their Actions column to proceed to the next step.

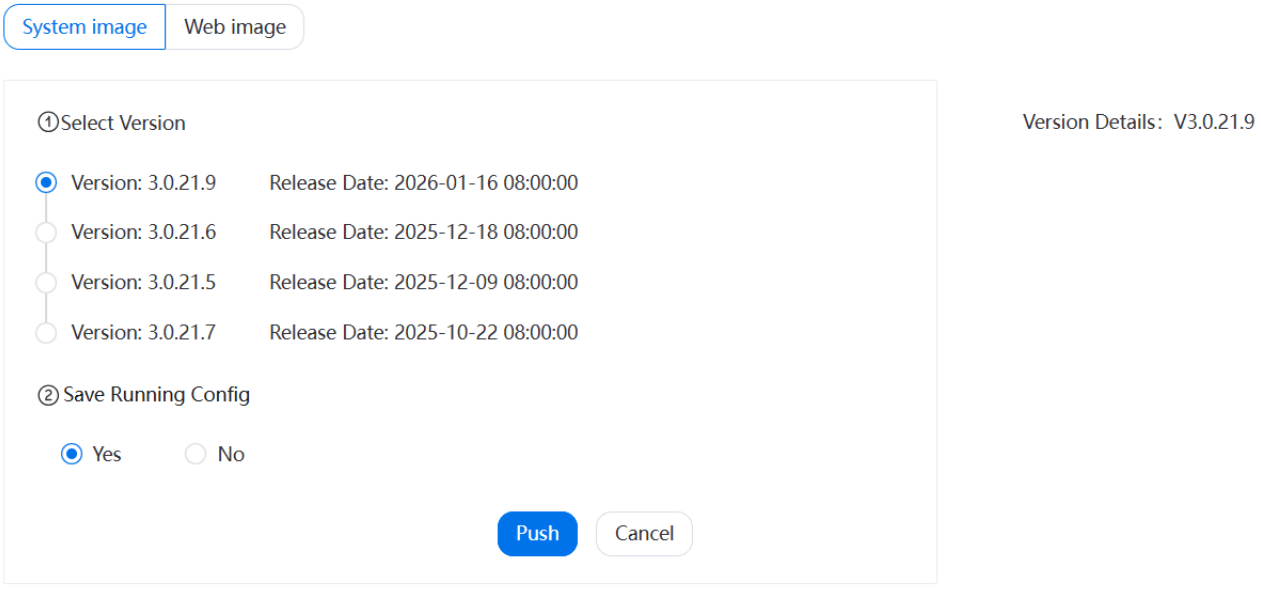


▲*Figure 82: Version Push Device List*

6.1.2. Version Selection & Push

After entering the Push page, you can switch between "System image" and "Web image" types as needed. The page lists all available upgrade versions for that device. Clicking a version's blank area displays its detailed information.

Select the target version and confirm whether to automatically save the device's current running configuration before upgrading (Configuration Introduction). Confirm and click the "Push" button. The platform will then push the download instruction to the device, completing the push operation. The platform creates an upgrade task after pushing the instruction, facilitating user tracking of upgrade progress;



▲*Figure 83: Version Selection and Push Page*

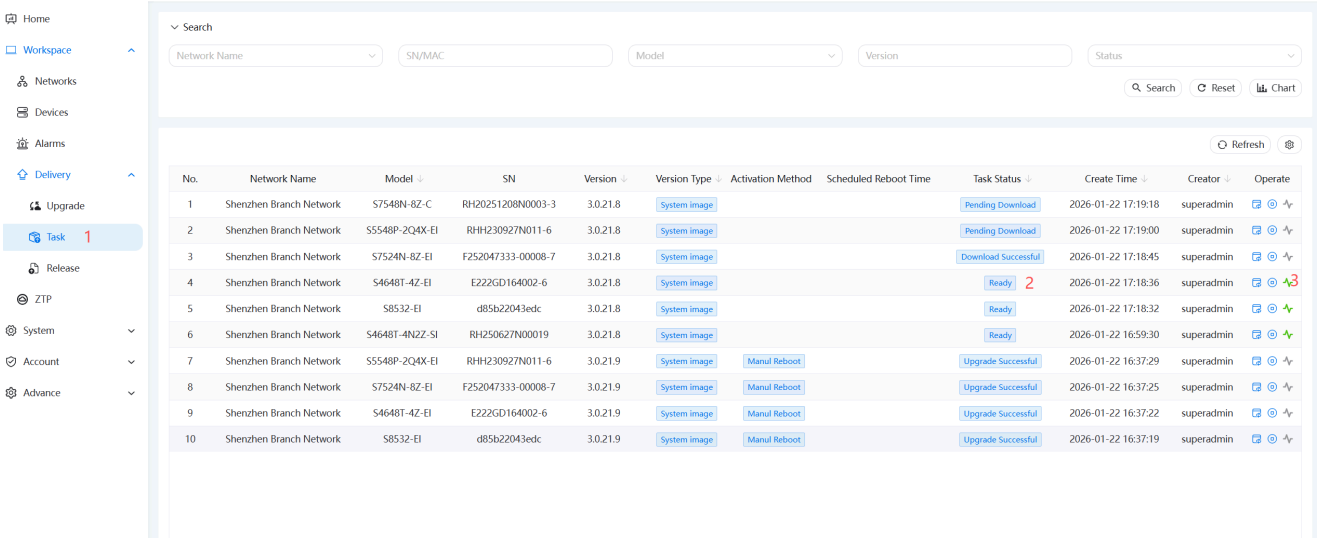
> **Note**
>
> - Only online devices can receive push instructions; offline devices cannot be operated.
> - If a device already has a task with status "Pending Download", "Download Success", "Ready", "Rebooted", or "Activating" in the current upgrade task, a new push cannot be initiated.
> - In tenant mode, only tenant administrators can view their tenant's devices. In private mode, platform administrators can view all devices.

6.2. Activate Version

After Version Push comes the Activation operation. All upgrade task progress, status details version activation and final results are presented in **Upgrade Tasks**, facilitating user tracking.

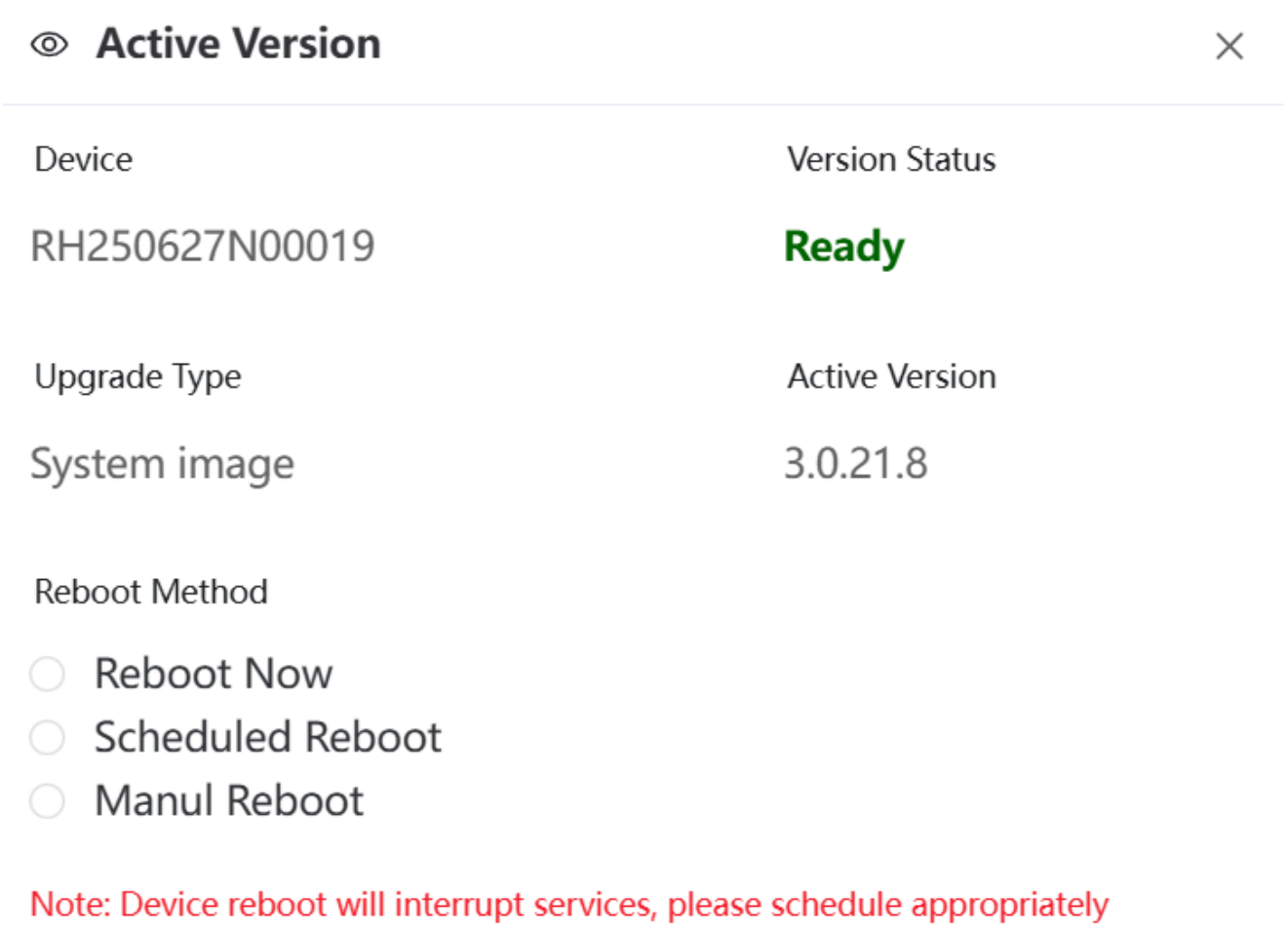
6.2.1. Device Activation

When a device completes upgrade package download and passes verification, the task status changes to "Ready". At this point, click the "Activate" button in the Actions column to enter the final upgrade stage, as shown:



▲*Figure 84: Upgrade Task List (Ready Status)*

- **Activation Instructions**
  Web image can be activated directly, usually without causing a device reboot. System image activation requires choosing a reboot method:
  - Reboot Immediately: Device reboots immediately after activation, upgrade takes effect;
  - Scheduled Reboot: Set a future specific time for automatic reboot, facilitating maintenance window planning;
  - Manual Reboot: Device does not automatically reboot after activation; administrator must manually log into the device to execute reboot later. Activation interface is shown:



▲*Figure 85: Software Activation Dialog*

6.2.2. Task Close

For tasks in "Pending Download", "Download Success", "Ready", "Rebooted", "Activating" etc., if they need to be aborted or cleaned up, they can be directly ended via the "Close" button in the Actions column to avoid affecting subsequent operations.

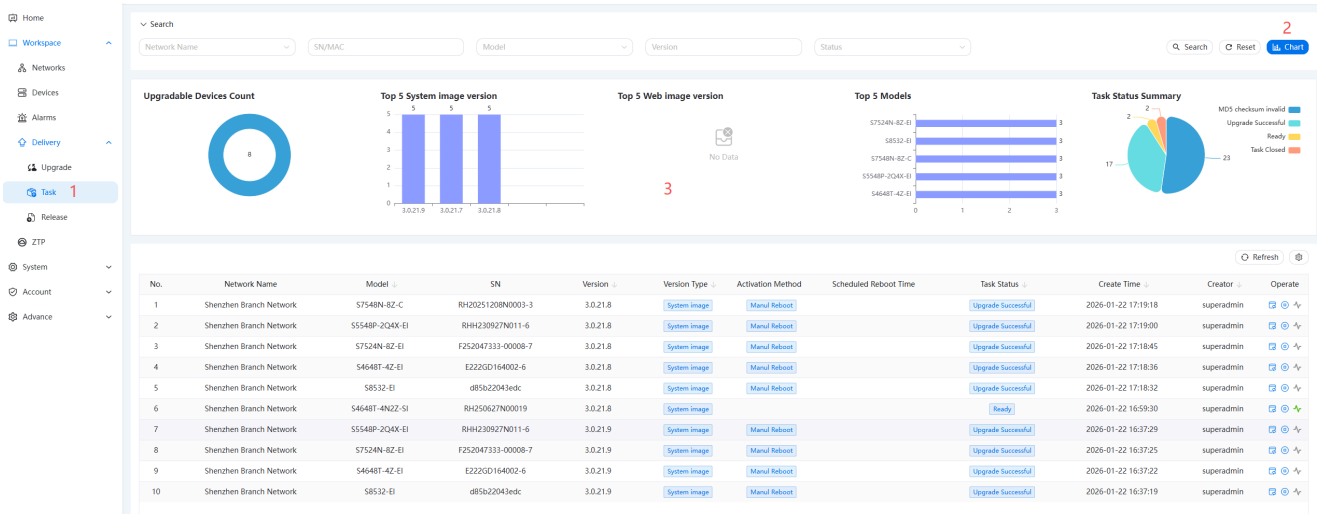
6.2.31. Re-push

If a task fails due to "Download Failed", "File Verification Failed", "Upgrade Failed" etc., or if the status is "Ready" but a version change is needed, use the "Re-push" function to re-initiate the push process.

6.2.4. Task Statistics

In the Upgrade Tasks module, click the "Chart" button to obtain a multi-dimensional global view and analysis of upgrades, including:

- Number of upgradeable devices currently in the platform.
- Top 5 Software versions and Top 5 Web versions being upgraded to.
- Top 5 device models currently undergoing upgrade.
- Status classification statistics for all upgrade tasks.



▲*Figure 86: Upgrade Task Statistics*

6.2.5. Task Statuses

No.	Status	Description
1	Pending Download	Upgrade task created, waiting for device to start downloading upgrade file
2	Download Success	Device successfully downloaded complete upgrade file
3	Download Failed	Device failed during upgrade file download process
4	File Verification Failed	Device local verification of upgrade file's MD5 value failed
5	File Verification Passed	Device local verification of upgrade file passed, upgrade package ready
6	Rebooted	Device has executed reboot operation (for System Image)
7	Pending Reboot	Device activated, waiting for scheduled reboot time
8	Upgrade Success	Device rebooted and new version is running normally, upgrade complete
9	Upgrade Failed	Device rebooted but upgrade not successful, possible version rollback
10	Task Closed	Task manually closed or terminated by administrator

▲*Table 13: Task Status Description*

> ⚠ **Warning**
>
> - **Business Impact Planning**: Upgrading the system image (System Image) causes device reboot, which may interrupt services. Plan ahead, activate devices sequentially and off-peak (e.g., use "Scheduled Reboot" with delays) to avoid large-scale simultaneous reboots.
> - **Network Stability Assurance**: Ensure network reachability from the platform to the device throughout the process. Network interruption during upgrade may cause download failure, activation timeout, or result detection anomalies.
> - **Result Auto-detection**: After activation completes, the platform automatically attempts to detect the device's final upgrade status (success/failure); no manual confirmation needed.
> - **Web Upgrade Non-disruptive**: Upgrading Web Image typically does not involve device reboot, has no impact on services, and requires no special order planning.

6.3. Upgrade Files

6.3.1. Overview

The Upgrade File Management module is dedicated to centralized, standardized, and secure full lifecycle management of various system upgrade files for network devices, including System Images and Web Images. This module is uniformly maintained by the platform administrator, ensuring the purity, reliability, and version consistency of upgrade sources.

- System Image: The device's core operating system file, containing the full feature set and system kernel;
- Web Image: An independent file for the device's Web management interface, typically used to update the graphical management interface;

6.3.2. Upgrade File Description

Upgrade files are provided to customers as a zip archive. The archive contains a .bin file and a release.xml file. When the zip is imported into the platform, it is automatically extracted, and the release.xml content is parsed. The release format is as follows:

```
# File header
<release xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
# File type
<type>web</type>
# Version number
<version>3.0.18.6</version>
```

```
# MD5 of the .bin file
<md5>2627c154d5d1b86ad56ad2b4000496b2</md5>
# Release date
<release.date>2025-10-10</release.date>
# Release details
<remark>WEB-3.0.18.6</remark>
# CRC verification code for the release file
<crc>d31f4cb4</crc>
</release>
```

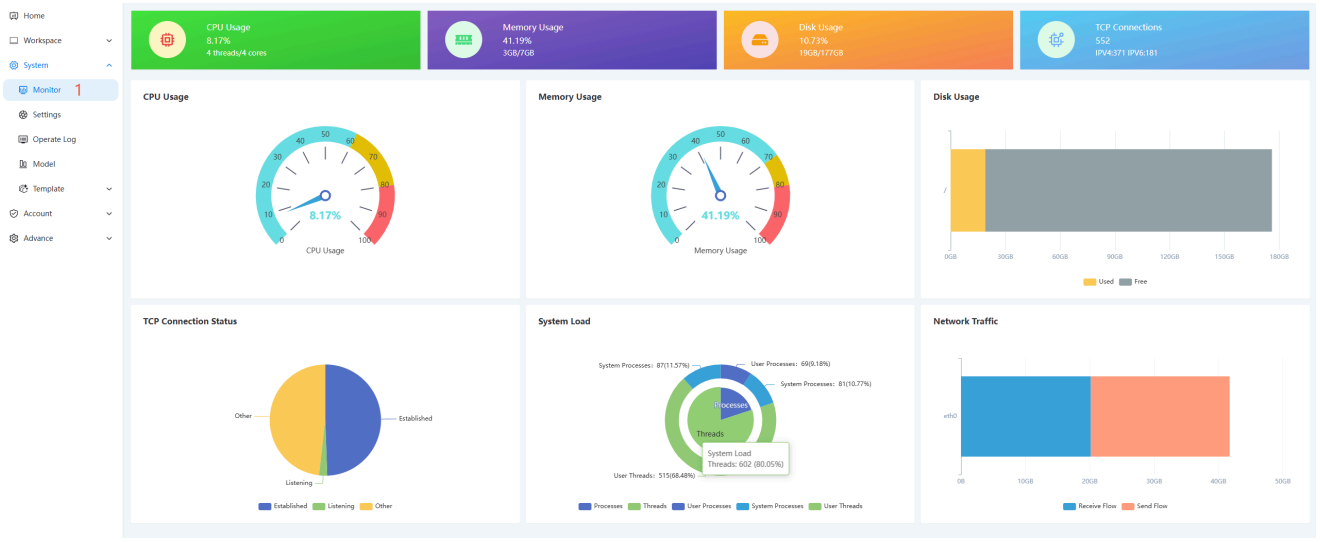
> ⚠ **Warning**
>
> To avoid affecting planned or ongoing upgrade tasks, please do not arbitrarily delete upgrade files unless necessary.

7. System Management

7.1. System Dashboard

The System Dashboard dynamically presents the platform's real-time operational status and core performance metrics in a graphical, visual manner. It aggregates key data such as server resources, system load, and network traffic, providing a clear health overview for platform administrators.

- Resource Utilization: Intuitively displays platform server's CPU usage, memory usage, and disk usage, quickly identifying resource bottlenecks.
- System Load: Monitors system process and user process ratios, reflecting the system's overall processing pressure state.
- Network & Connections: Shows platform management network inbound and outbound traffic, as well as current TCP connection count, monitoring the platform's network communication load and activity.



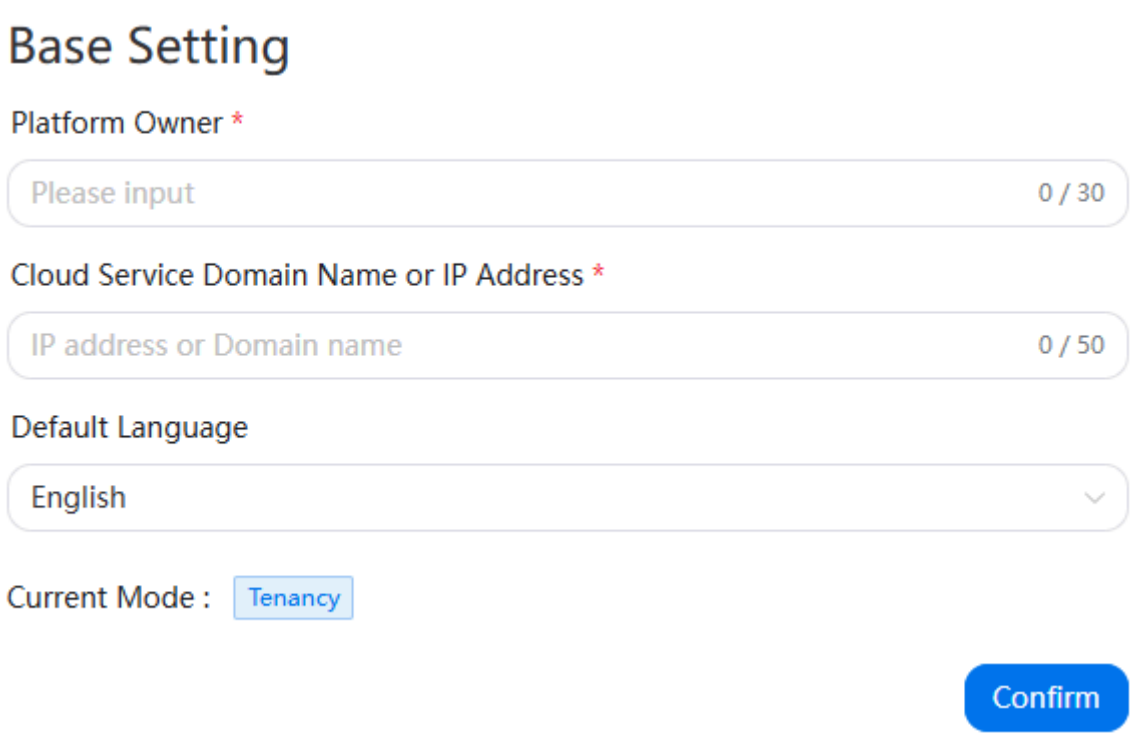
▲*Figure 87: System Dashboard Page*

7.2. Platform Settings

To ensure platform normal operation, some settings need to be configured after installation, including Basic Settings, Customer Custom Settings, Mail Server Settings, SMS Notification Settings, and WeChat Notification Settings.

7.2.1. Basic Settings

Basic Settings primarily configure foundational functions, including platform owner, cloud service IP, system default language, multi-tenant mode status, etc., as shown:

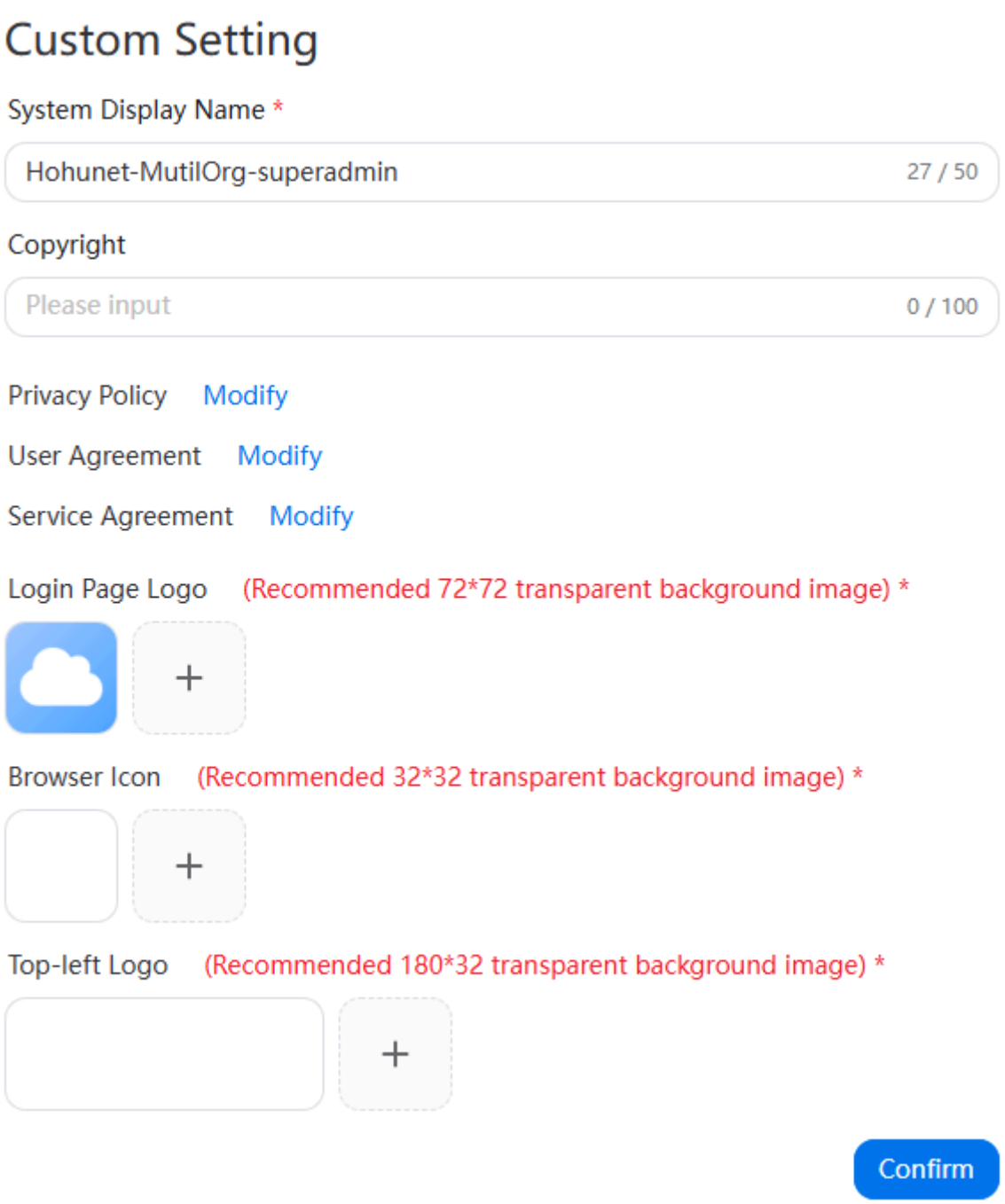


▲*Figure 88: Basic Settings Page*

- Platform owner refers to the platform's proprietor and can be displayed to users where necessary;
- Cloud Service IP is primarily used for device communication interfaces and when establishing tunnel services;
- System Default Language can be switched to default English or Chinese display based on location, reducing frequent switching hassle;
- Multi-tenant mode can only be set during the first configuration after installation and cannot be modified afterward.

7.2.2. Customer Custom Settings

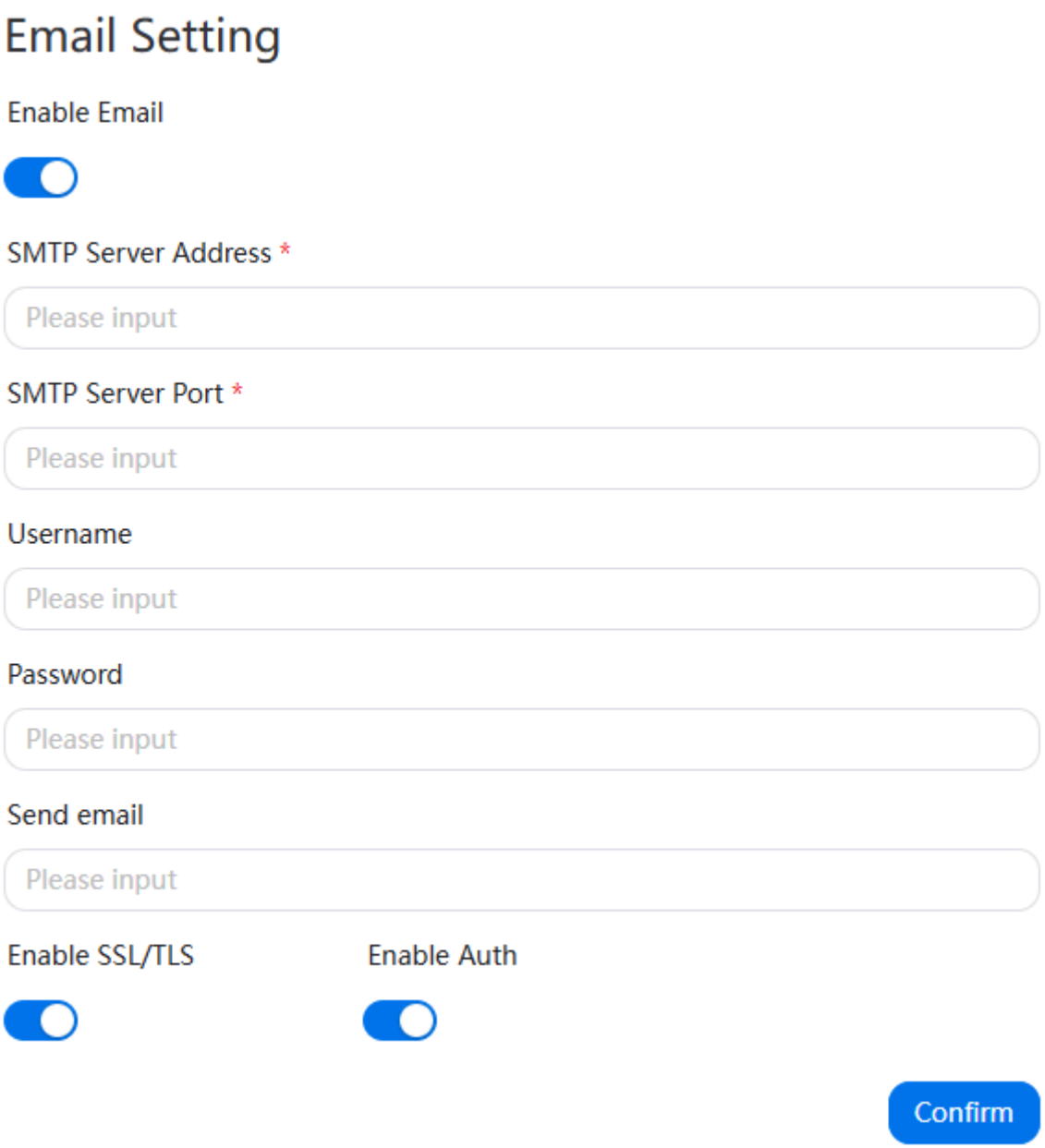
Customers can customize platform name, logo, website filing information, privacy policy, user agreement, service agreement, etc. The system detects content for user agreement, privacy policy, and service agreement, displaying entries on the login page if configured; otherwise, no entries are shown. The Customer Custom Settings interface is shown as:



▲*Figure 89: Customer Custom Settings Page*

7.2.3. Mail Server Settings

The platform's email notification function requires configuration of related mail service information before use. Enabling this function makes the Email login entry appear on the login page. Specific configuration information is shown:

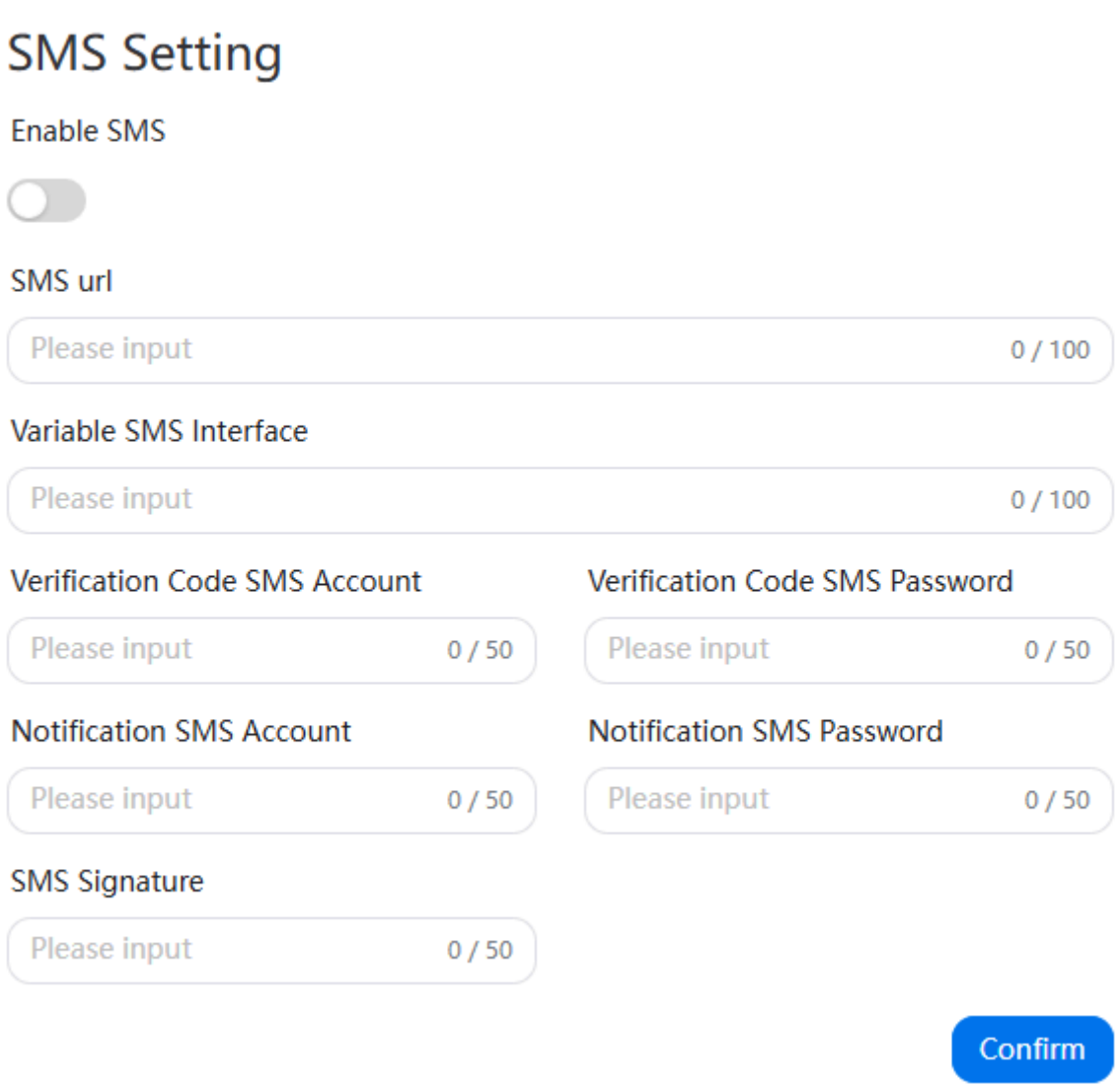


▲*Figure 90: Mail Server Settings Page*

> ⚠ **Warning**
> Email notifications require the corresponding Email Templates to be enabled and used simultaneously.

7.2.4. SMS Notification Settings

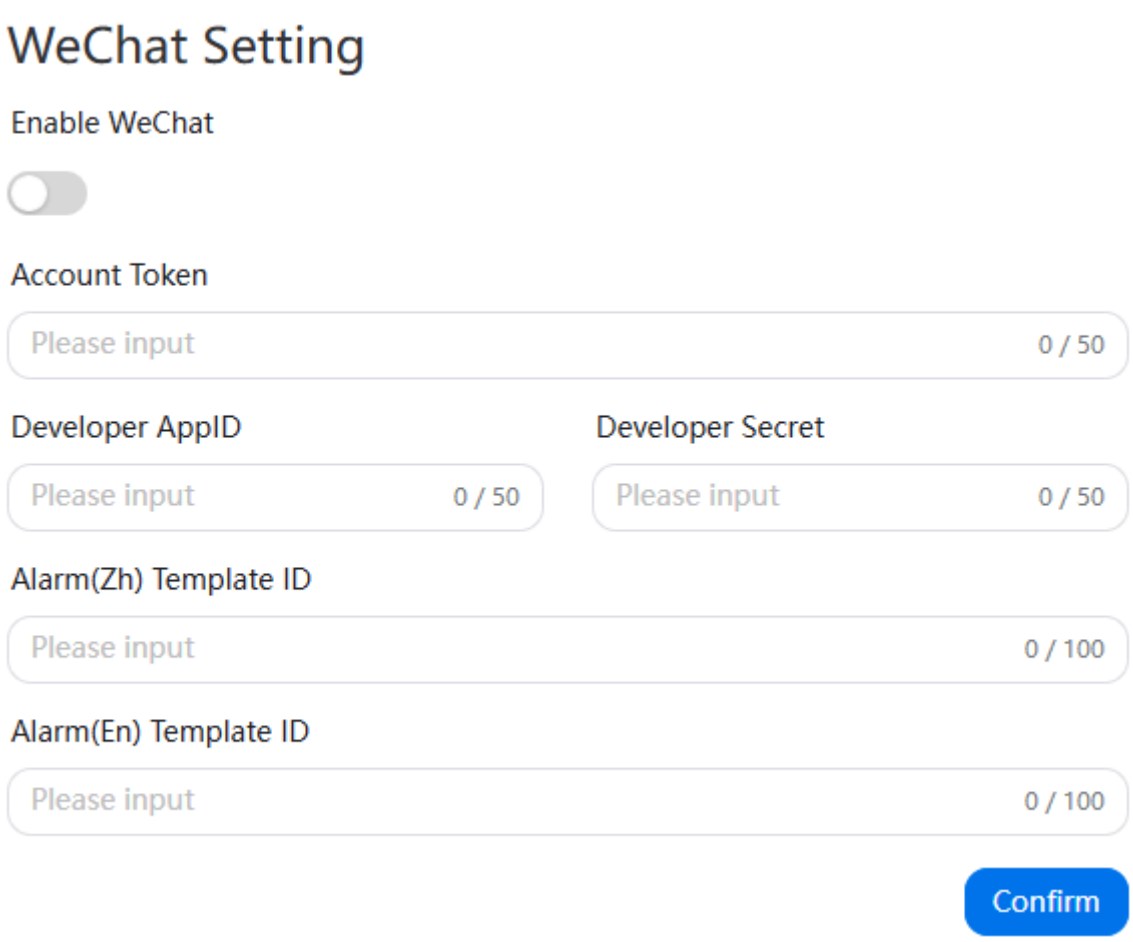
The platform's SMS notification function requires configuration of related SMS interface information before use. Enabling this function makes the SMS login entry appear on the login page. Currently, SMS service only supports mobile numbers from mainland Chinese carriers. Specific configuration information is shown:



▲*Figure 91: SMS Notification Settings Page*

7.2.5. WeChat Notification Settings

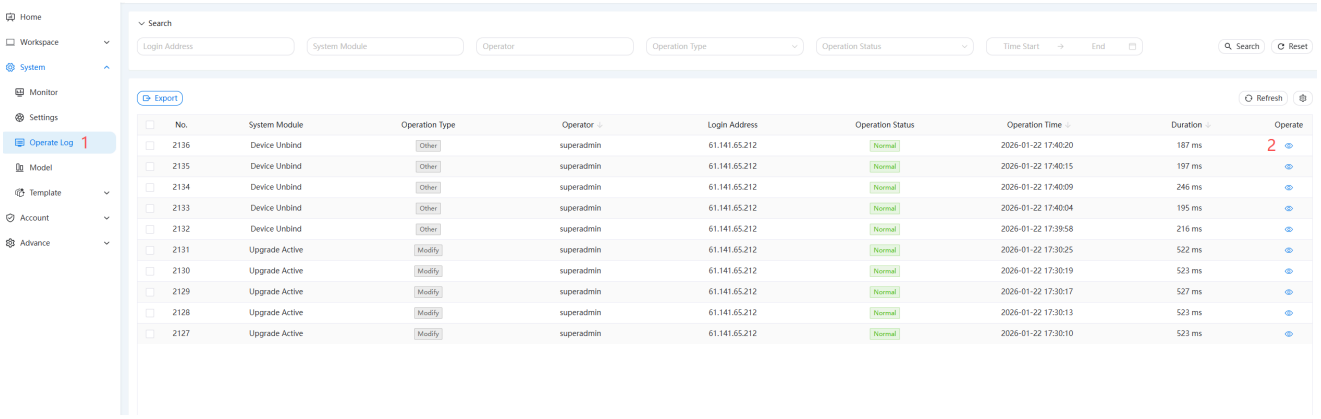
The platform's WeChat notification function requires configuration of related WeChat interface information before use. Enabling this function makes the WeChat login entry appear on the login page. The WeChat notification function requires prior application for a WeChat Official Account. Users need to follow the official account and bind their platform account to their personal WeChat account. Specific configuration information is shown:



▲*Figure 92: WeChat Notification Settings Page*

7.3. Operation Logs

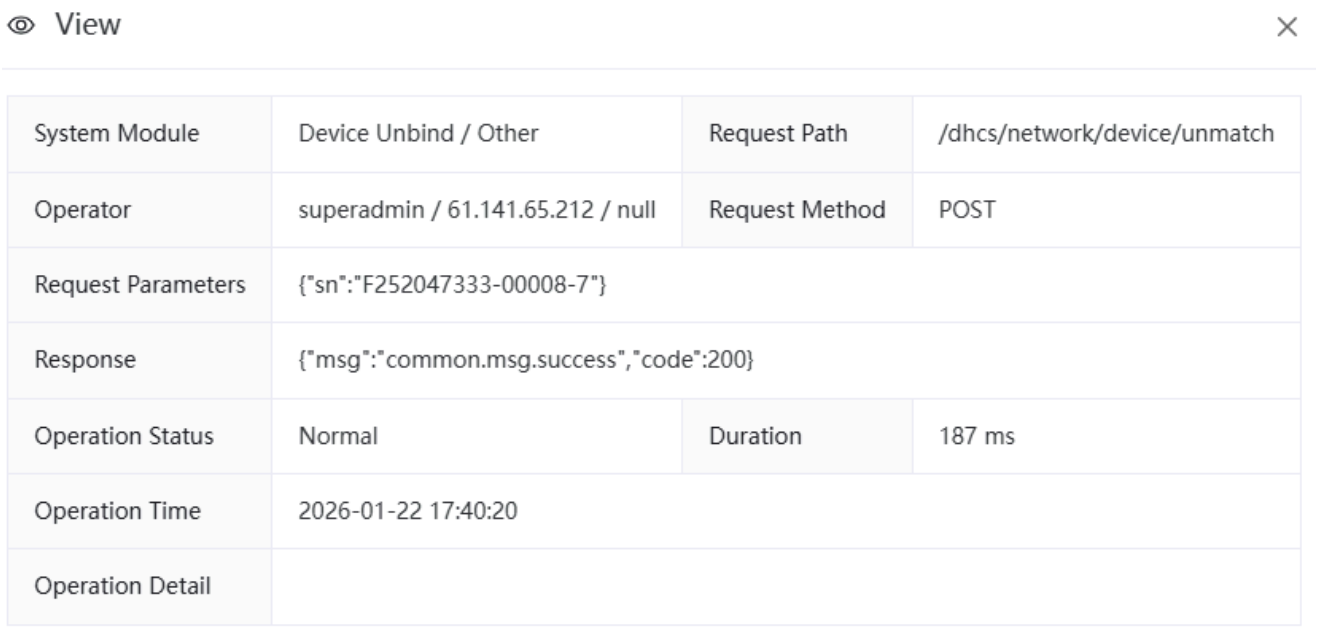
Operation Logs record user operation behaviors, facilitating audit review. In tenant mode, only tenant administrators can see their own tenant's data. In private mode, platform administrators can see all operation logs.



▲*Figure 93: Operation Log List*

- List Query
  Administrators can search operation log records based on module name, operator, operation time, etc.

- Operation Details
  Click the view button in the Actions column to view detailed operation content. Some less important operations only record the behavior, not the content, as shown:

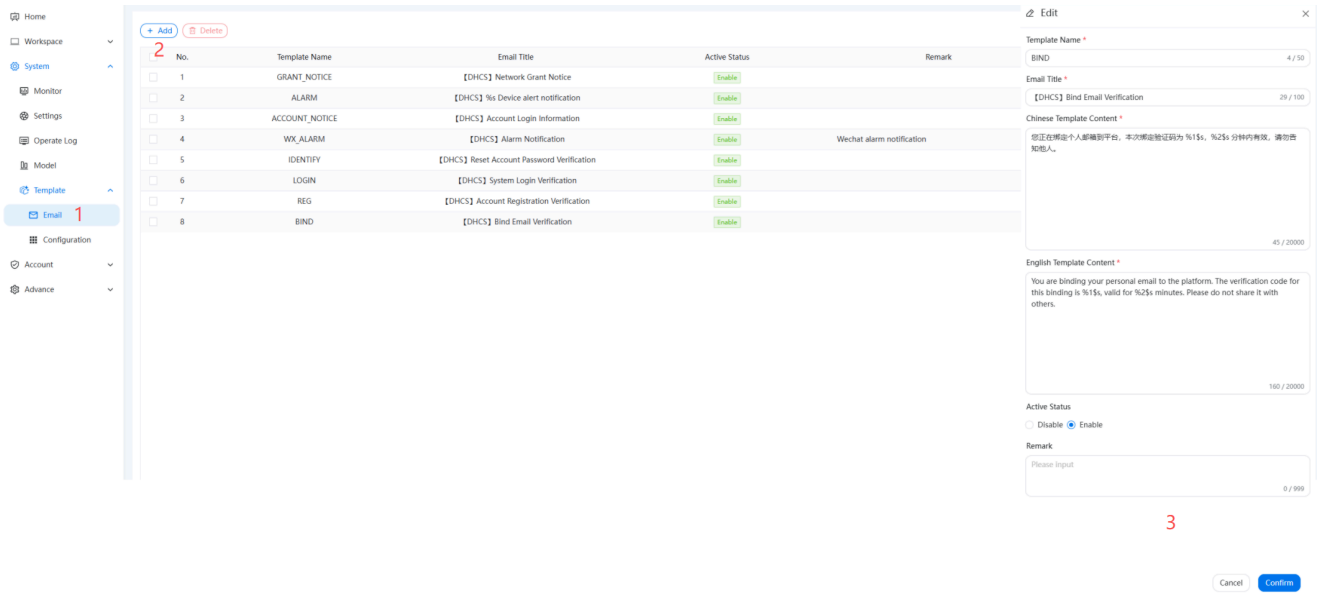


▲*Figure 94: Operation Log Details*

7.4. Templates

7.4.1. Email Templates

The Email Templates function aims to standardize, automate, and personalize the management of system notification emails. Administrators can predefine email formats and content for various business notifications (such as alarms, registration, login). By embedding variables (e.g., `{sn}`, `{alarm_time}`), dynamic filling of key information is achieved. Email templates must be enabled to take effect. As shown:

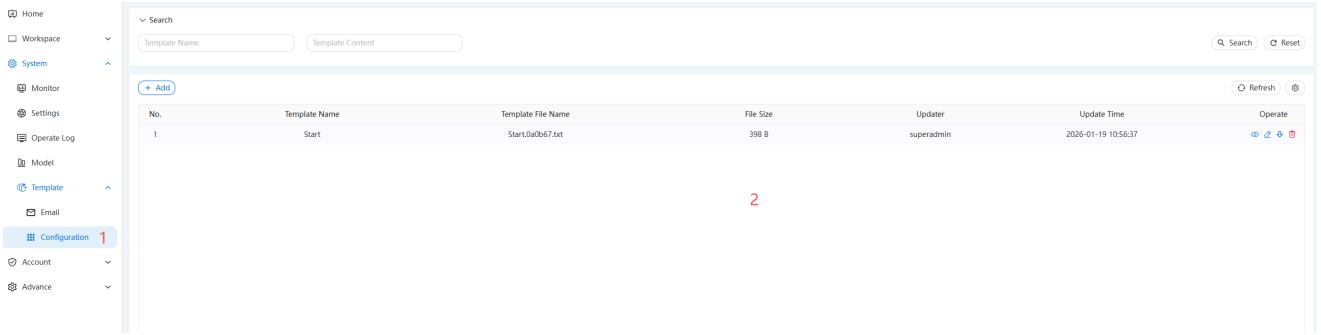


▲*Figure 95: Edit Email Template Page*

> ⚠ **Warning**
> Each email template corresponds to a platform execution action. Deleting it will prevent emails from being sent. Only adjustments to some necessary text in the email content and title are allowed.

7.4.2. Configuration Template Library

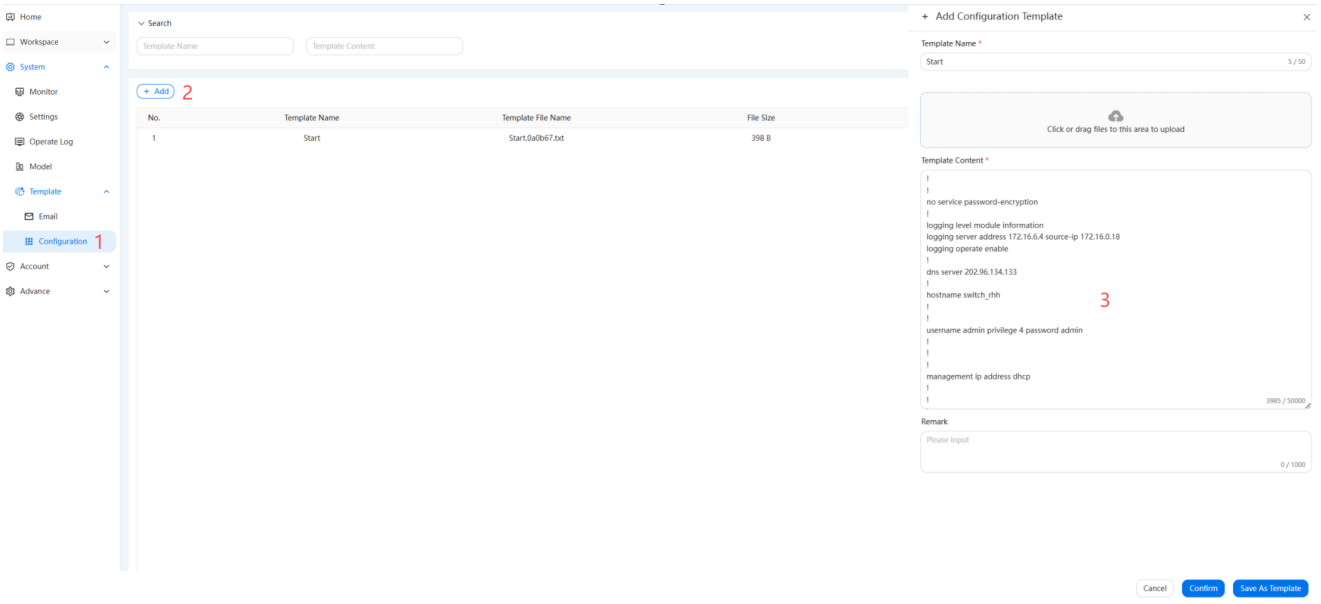
- **Overview**
  The Configuration Template Library is a tool for improving network device deployment and management efficiency. Its core idea is to centrally store and manage verified, standardized device configurations as reusable templates. When initializing new devices (deployment) or performing batch device configuration, administrators can quickly retrieve the appropriate template, make necessary minimal modifications (like replacing IP addresses, device names, etc.) on the template basis, and then rapidly and accurately deploy the configuration to target devices. The Configuration Template List is shown as:



▲*Figure 96: Configuration Template Library List*

> ⓘ **Note**
> In tenant mode, all templates of that tenant are displayed. In private mode, all templates of the entire platform are displayed.

- Add Template
  Click the "Add" button, drag the locally edited template file into the upload area. The platform automatically reads the template content into the edit box where users can make final adjustments. After filling in the template name, click "Save" to complete template creation. As shown:

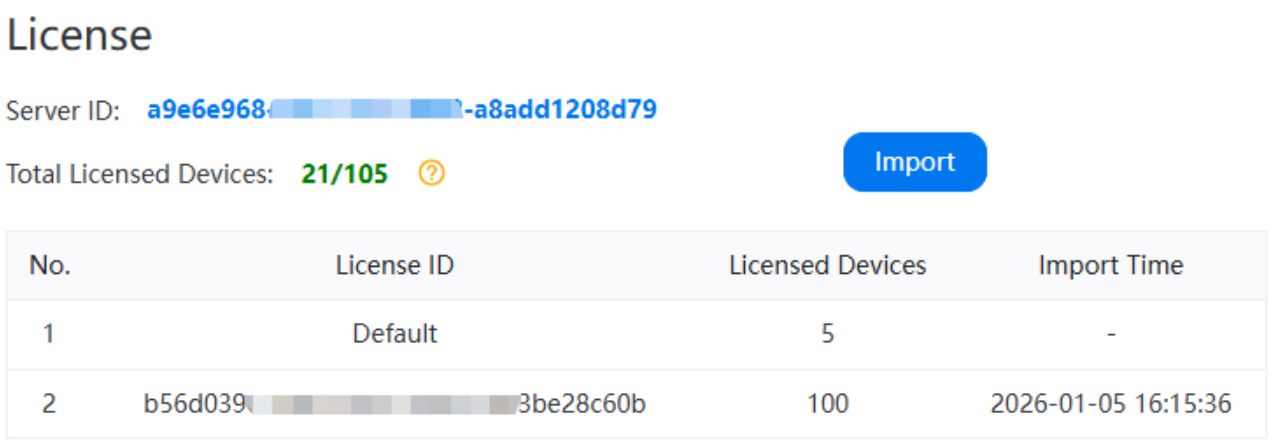


▲*Figure 97: Add Configuration Template Page*

7.5. License Management

7.5.1. Overview

By default, the platform supports free connection for 5 devices. Users needing more can apply for licenses for more devices through sales personnel. Each license permits a certain number of devices to connect to the cloud platform.
Multiple Licenses can be stacked for use. The maximum number of devices the platform can manage is the sum of the device quotas authorized by each License.



▲*Figure 98: License Management List*

7.5.2. Operation Process

License application process is as shown below:

▲*Figure 99: License Application Flowchart*

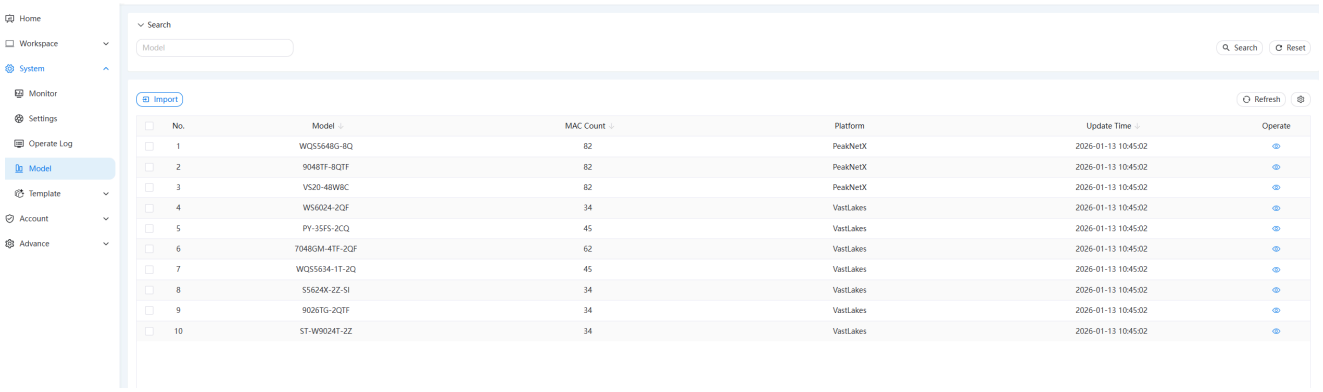
- Obtain ServerID
  Users can obtain the fingerprint information of the current running environment via the "Get ServerID" button in the cloud platform;
- Apply for License
  Submit the ServerID and the requested number of devices to the manufacturer to apply for a License;
- Import License
  Import the applied License in the License module. The interface displays the total number of devices allowed to connect;

> ⚠ **Warning**
> If the cloud platform is reinstalled, the obtained ServerID will change. Any License previously applied for based on the old ServerID will become invalid and must be reapplied for.

8. Basic Information

8.1. Product Models

Product Models refer to the models and panel information of manageable devices and are foundational data for the platform. Without this information, some functions may not work properly. If this occurs, contact the supplier to obtain the relevant data files and import them. As shown:



▲*Figure 100: Product Model List*

8.2. Alarm Types

Alarm Code	Major Category	Minor Category	Severity Level
101	Network Abnormality	Loop Alarm	Minor
102	Network Abnormality	CRC Alarm	Minor
103	Network Abnormality	Link Aggregation Group Alarm	Critical
201	SFP Module Alarm	Optical Power Attenuation Alarm	Critical
202	SFP Module Alarm	Optical Power Attenuation Alarm	Minor
203	SFP Module Alarm	Temperature Alarm	Critical
204	SFP Module Alarm	Temperature Alarm	Minor

Alarm Code	Major Category	Minor Category	Severity Level
205	SFP Module Alarm	Voltage Alarm	Critical
206	SFP Module Alarm	Voltage Alarm	Minor
207	SFP Module Alarm	Current Alarm	Critical
208	SFP Module Alarm	Current Alarm	Minor
301	Resource Alarm	CPU Alarm	Critical
302	Resource Alarm	Memory Alarm	Critical
303	Resource Alarm	Storage Alarm	Critical
304	Resource Alarm	Critical Port Abnormality	Minor
305	Resource Alarm	Temperature Alarm	Minor
306	Resource Alarm	Fan Alarm	Critical
307	Resource Alarm	Fan Alarm	Minor
308	Resource Alarm	Fan Alarm	Minor
309	Resource Alarm	Fan Alarm	Minor
310	Resource Alarm	Uplink Traffic Alarm	Critical
311	Resource Alarm	Downlink Traffic Alarm	Critical
312	Resource Alarm	POE Total Power Alarm	Critical
313	Resource Alarm	POE Total Power Alarm	Critical
401	Reboot Alarm	Manual Reboot	Critical
402	Reboot Alarm	Power Loss Reboot	Critical
403	Reboot Alarm	Overheat Reboot	Minor

▲*Table 14: Alarm Types*