DHCS Quick Start Guide (Tenancy Mode)

1. Basic Concepts

Name	Description
Platform	Refers to the cloud server instance hosting the DHCS system.
Tenant	Refers to your team or company's independent resources and workspace within the cloud platform, where all data and resources are isolated and managed within the tenant.
Platform Administrator	The 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.
Technical Support	Technical Support is responsible for assisting tenants in resolving cloud operation and maintenance issues. By default, they only have business menu permissions without data permissions. When a user grants technical support permission to a network, they can view and operate devices under that network.
Tenant Administrator	The creator of the tenant; the first person to register an account for the organization automatically becomes the administrator, responsible for managing each tenant member, device, and permissions.
Tenant Member	Team members invited by the tenant administrator to join, using platform resources within the permissions assigned by the administrator.
Network	A logical project created by a tenant on the DHCS platform for segmenting and managing their exclusive network resources. A tenant can create multiple networks, e.g., representing different subnets or branch office networks within the company.
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 of a single management entity.

Name	Description
Tenant Mode	Each tenant is an independent organization. For example: different branch offices, customers, or project groups can be set up as independent tenants. Data between tenants (such as devices, configurations, alarms) is completely isolated, enabling secure and independent operation of multiple customers or departments on the same platform.

▲*Table 1 Basic Concepts*

2. Quick Start Preparation

2.1. Preparation Checklist

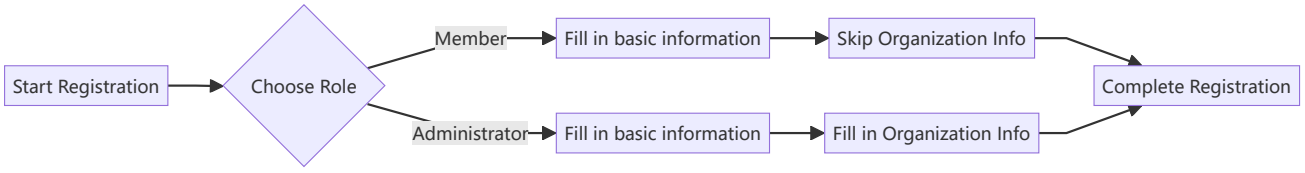
Preparation Content	Requirement	Remarks
Cloud Platform	Installation completed and email service configured	Ensure the mail server can send emails to the target address.
Tenant Member Account	Registered and joined the tenant	Ensure permissions such as "Network Creation" and "Device Management" are available.
Platform Administrator Account		superadmin account
Test Device	A functional device	Network configured.
Network Planning	Device must be able to access the cloud platform service address	Ensure no firewall blockage from the device to the cloud platform.

▲*Table 2 Preparation Checklist*

2.2. Create a Tenant Team

2.2.1. Account Registration

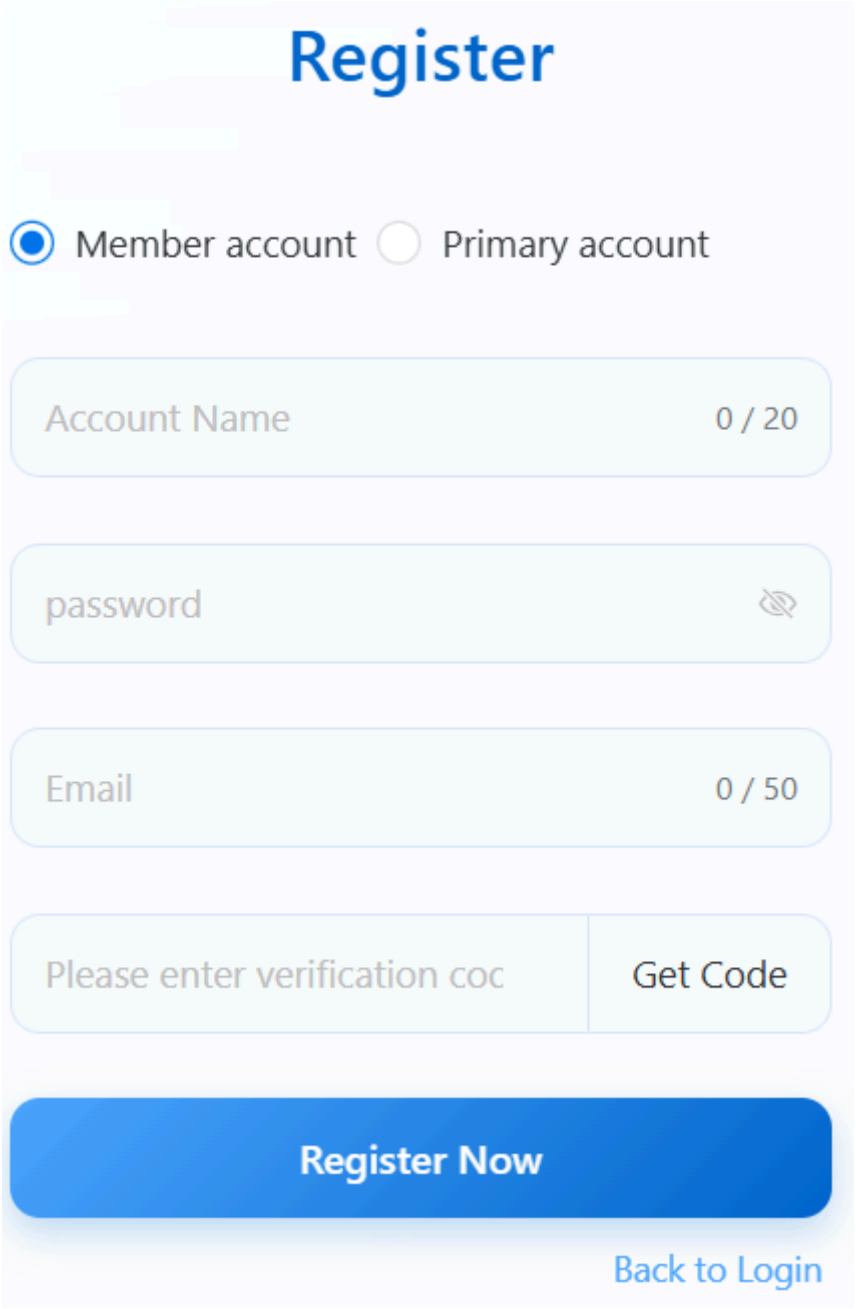
- Registration Process



▲*Figure 1 Account Registration Flowchart*

- Registration

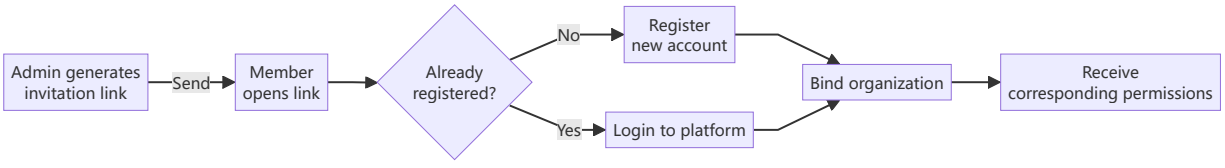
On the login page, click "Register Account" to go to the Register page. Select the required user type and fill in the registration information to register. The tenant is created when the administrator registers.



▲*Figure 2 Account Registration Page*

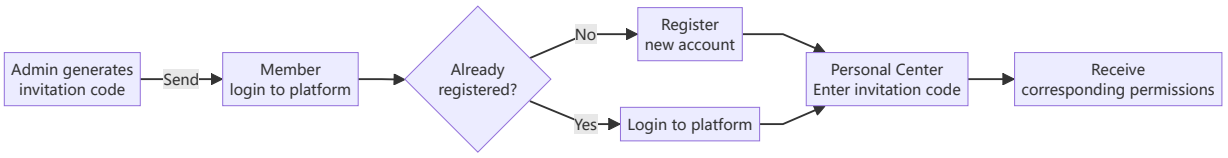
2.2.2. Tenant Member Invitation

- Invitation Link Process



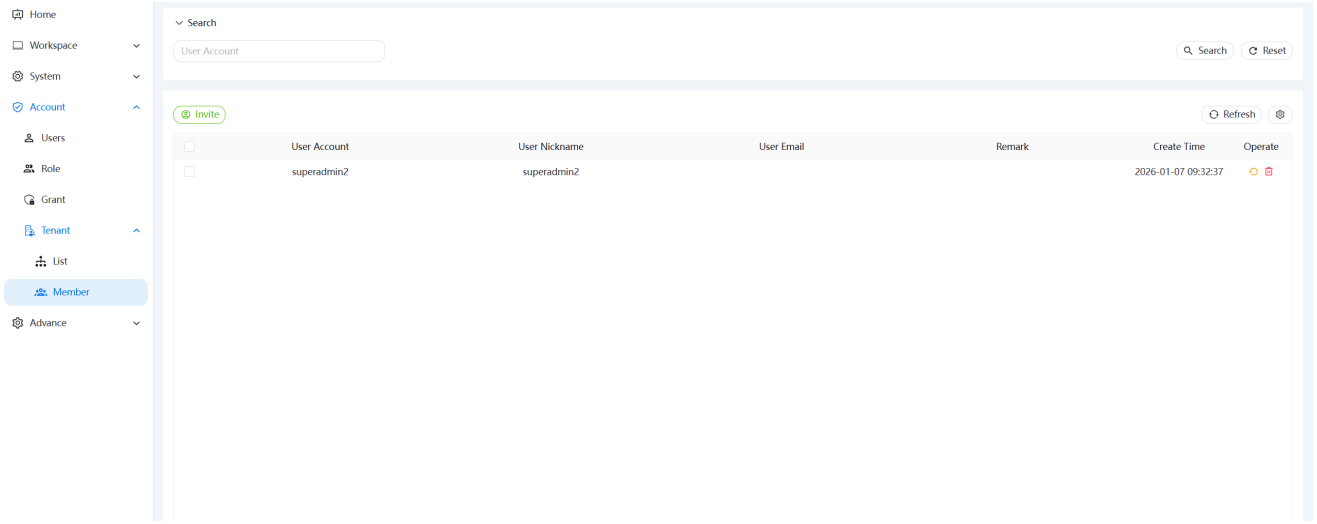
▲*Figure 3 Invitation Link Join Flowchart*

- Invitation Code Process



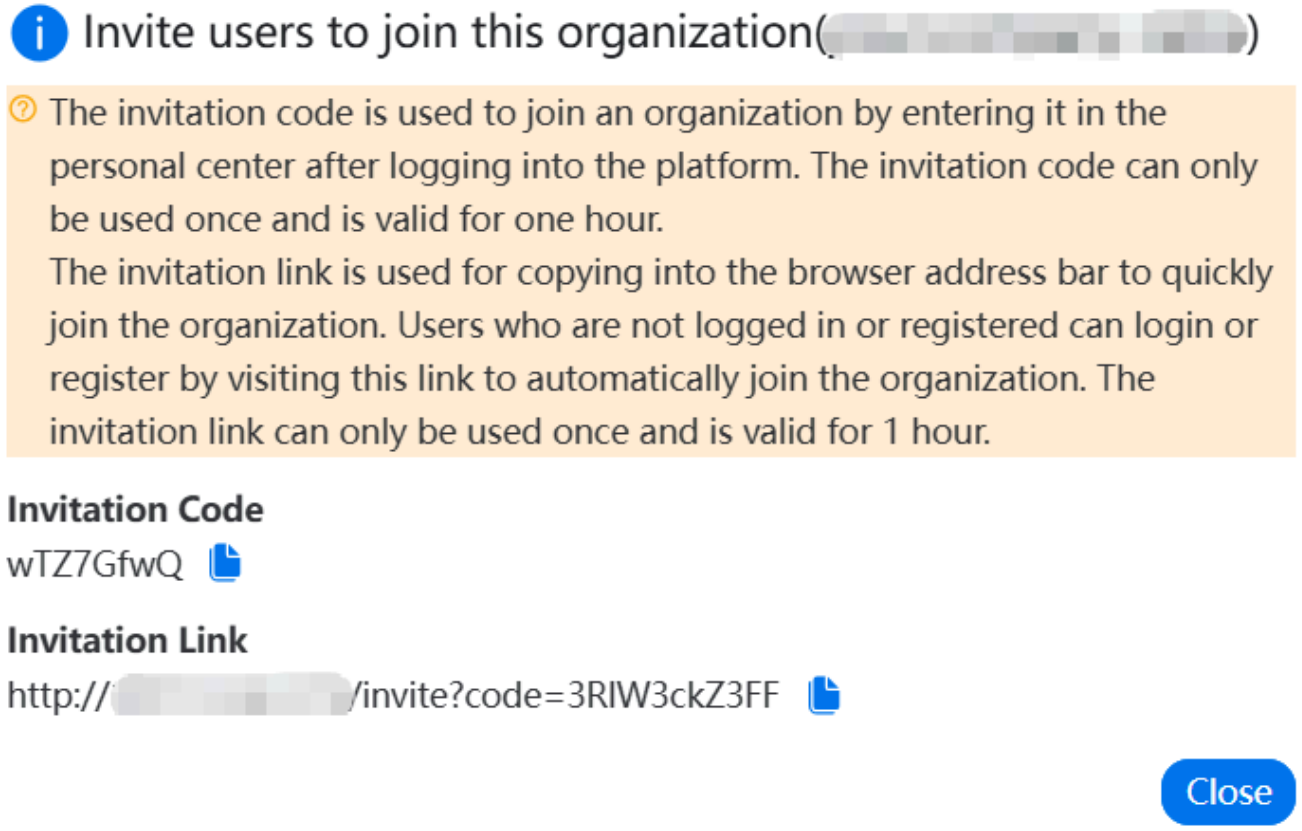
▲*Figure 4 Invitation Code Join Flowchart*

- Generate Invitation Information
  Go to Tenant Management -> Tenant Members menu and click the "Invite" button, as shown:



▲*Figure 5 Tenant Member Management Page*

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



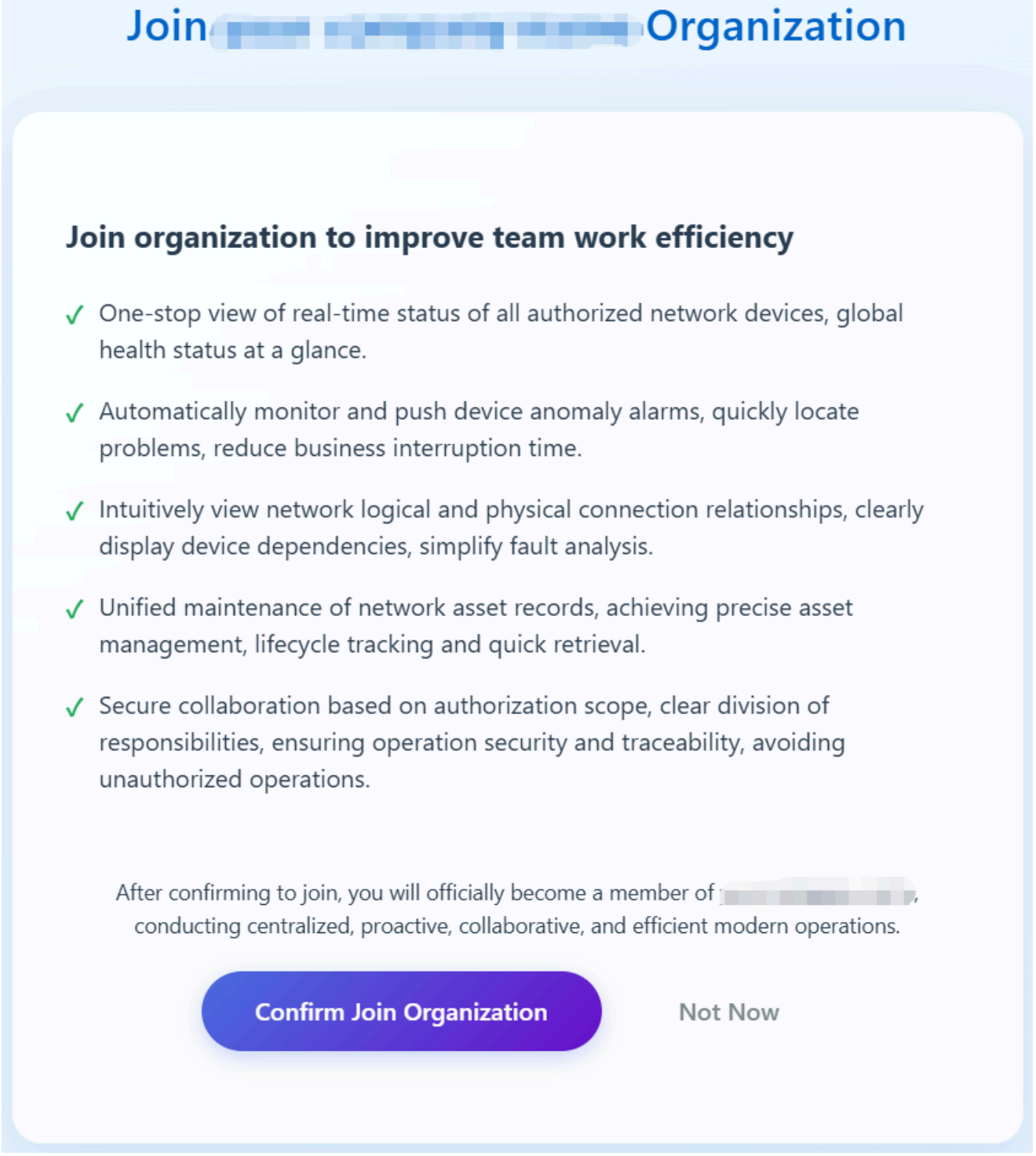
▲*Figure 6 Invitation Information Generation Dialog*

Send the invitation code or invitation link to the user you wish to invite to join the organization.

> **Note**
>
> 1. The validity period for invitation codes and links is 1 hour.
> 2. If a tenant member is not bound to any tenant, logging into the platform will automatically redirect them to the Personal Center.

- Join via Invitation Link

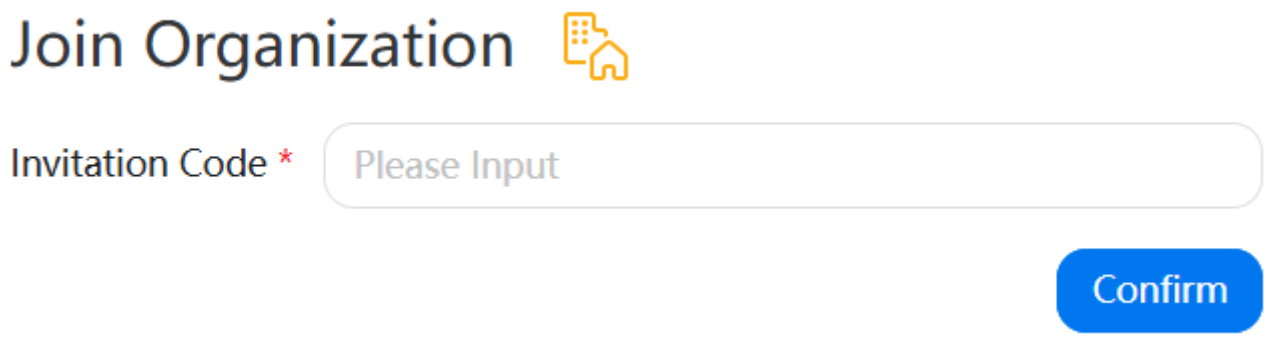
After logging in, the invitee opens the invitation link and clicks "Confirm to join the organization" to complete joining the tenant, as shown:



▲*Figure 7 Invitation Link Join Confirmation Page*

- Join via Invitation Code

After logging in, the invitee clicks on the account in the top right corner -> Personal Center. In the "Join Organization" section of the Personal Center, enter the invitation code and click "Confirm" to complete joining the organization, as shown:

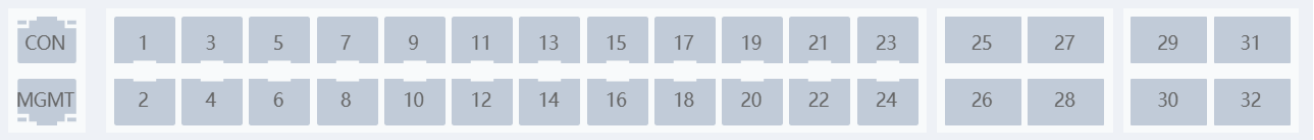


▲*Figure 8 Personal Center Enter Invitation Code Page*

2.3. Device Side Preparation

2.3.1. Managed Ports Introduction

Device ports are categorized into three types: Serial Port, Management Port, and VLAN 1. Serial Ports and Management Ports are identified on the device panel as "CON" and "MGMT," respectively. VLAN 1 refers to all other service ports except CON and MGMT. As shown in the figure, ports 1 through 32 are VLAN 1 ports.

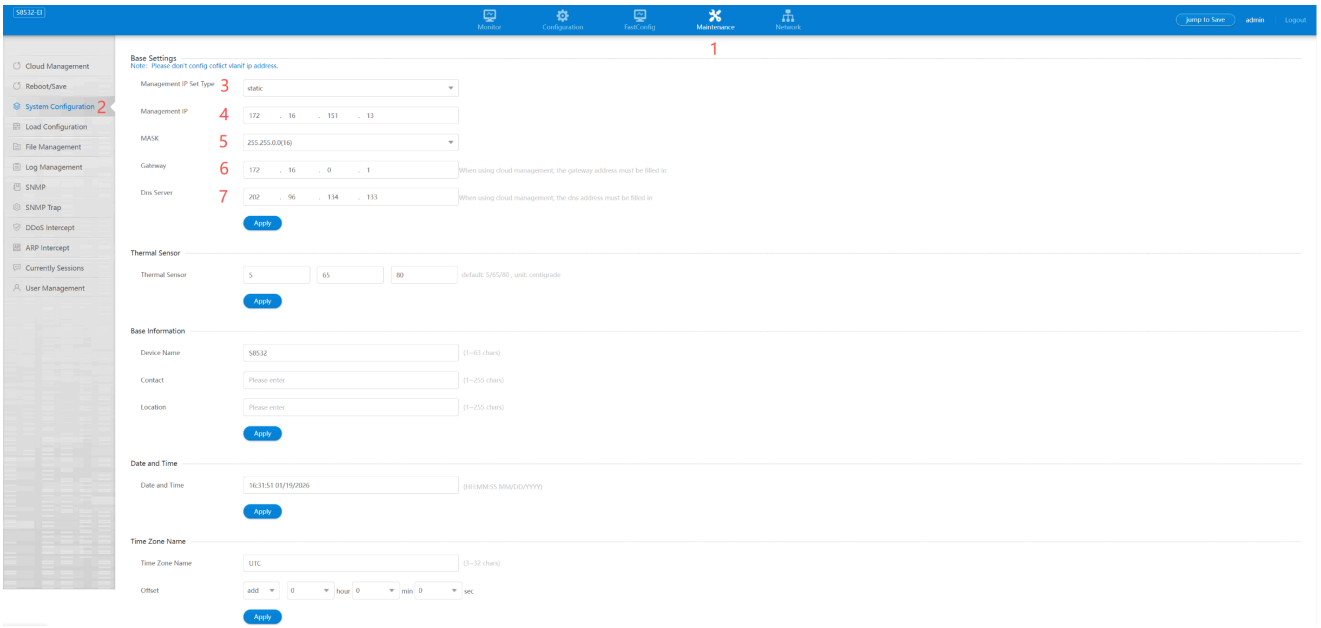


▲*Figure 9 Device Ports Diagram*

2.3.2. Device IP Address Configuration

Devices can access the management network via MGMT or VLAN1. The corresponding IP address descriptions are as follows:

- MGMT access: The default IP address is 192.168.1.1. If the default IP cannot access DHCS, please manually configure. As shown in the image below, after logging into the device's web interface, users should modify the Management IP, Gateway, and other settings in the system configuration as required.

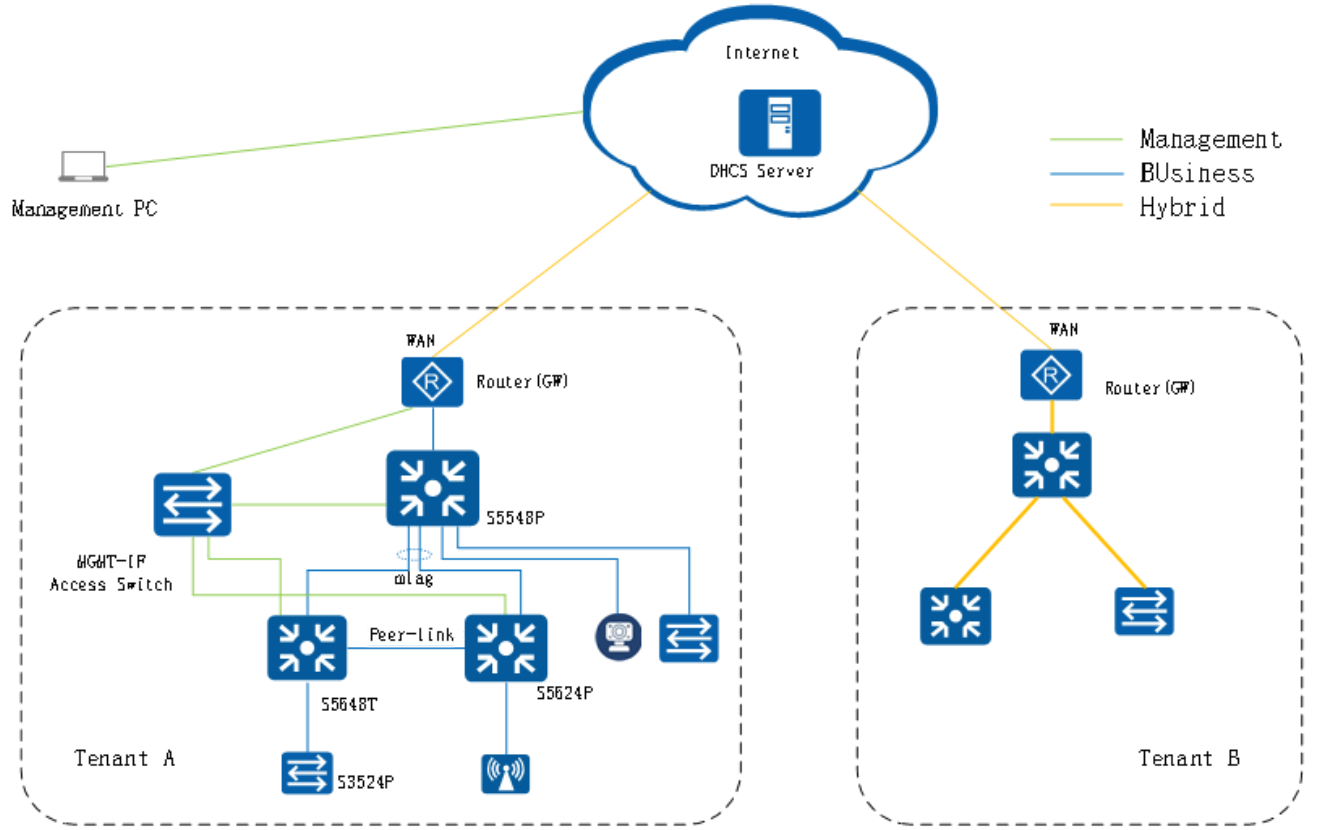


▲*Figure 10 Device Management IP Configuration Page*

- VLAN1 access: Devices have DHCP enabled by default out of the box and will automatically obtain an IP address after connecting to the network. Users can also manually configure a static IP.

2.4. Network Planning

The plan is to deploy the DHCS platform in the cloud, connecting two tenants, A and B. Their respective internal network topologies are shown in the following figure:



▲*Figure 11 Multi-Tenant Network Planning Topology*

Tenant A: Its network devices access the cloud platform via a dedicated out-of-band management port.
Tenant B: Its network devices access the cloud platform directly via the service port over the public internet.
This document will guide users in minimally managing one device on the cloud platform, such as Tenant B's network in the diagram.

3. Device Operation and Maintenance (Tenant)

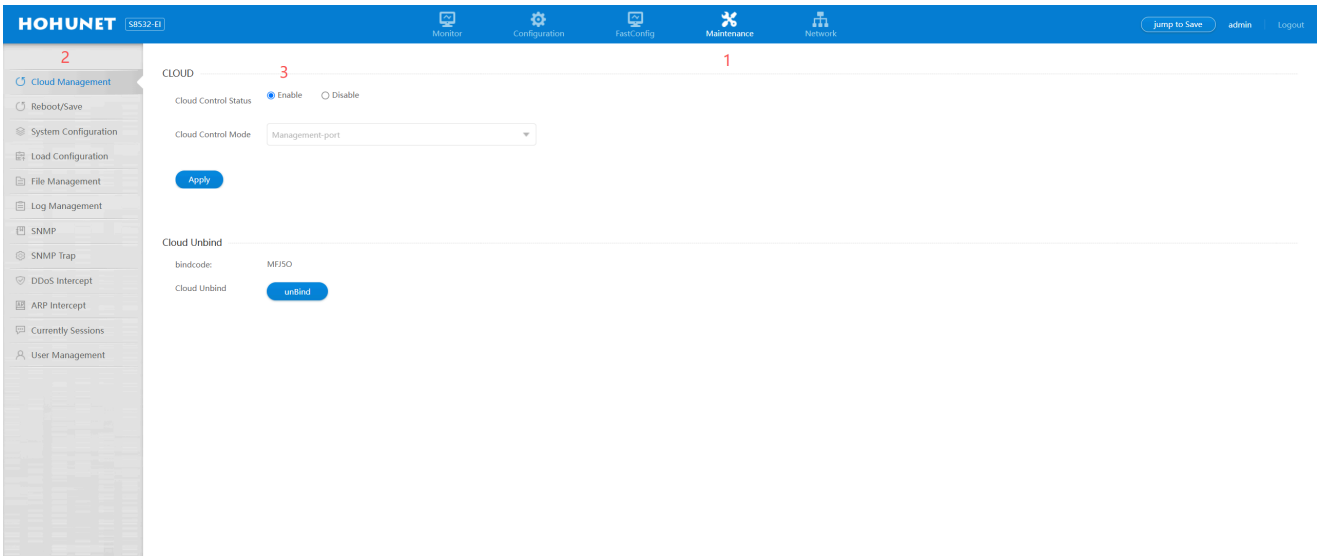
3.1. Onboarding the First Device

3.1.1. Enabling Cloud Management Service

Users can directly configure the management command on the switch via CLI. The steps are as follows:

```
#1. Login to the switch and enter the admin username and password.

#2. Enter configuration mode (must)
configure terminal

#3. Configure the cloud management mode: DHCS (must)
cloud control version dhcs

#4. Configure the cloud management platform port and the domain name or
IP address of the platform (must)
cloud control domain-port 883 domain-name 10.78.1.34

#5. Select the management interface. Choose one that matches the actual
physical connection (must)
  # VLAN1 connects to the cloud management platform
  cloud control enable
  # MGMT connects to the cloud management platform
  cloud control mgmt-if enable

#6. Save the configuration (must)
  write
```

Login to the device's web interface and confirm according to steps 1, 2, and 3 in the figure below. As shown, the Cloud Management Enable status should be "Enabled".



▲*Figure 12 Device Cloud Management Service Configuration Page*

> **Note**
> The type of managed port selected for the cloud management connection mode must be consistent with the port actually connected to the cloud platform.

3.1.2. Obtaining the Binding Code

There are two ways to obtain the binding code:

- **Obtaining the Binding Code via the Web Page**

Login to the device web interface, navigate to Maintenance -> Cloud Management Service to view the binding code obtained after enabling the service. Refer to the 【Cloud Management Configuration】interface.

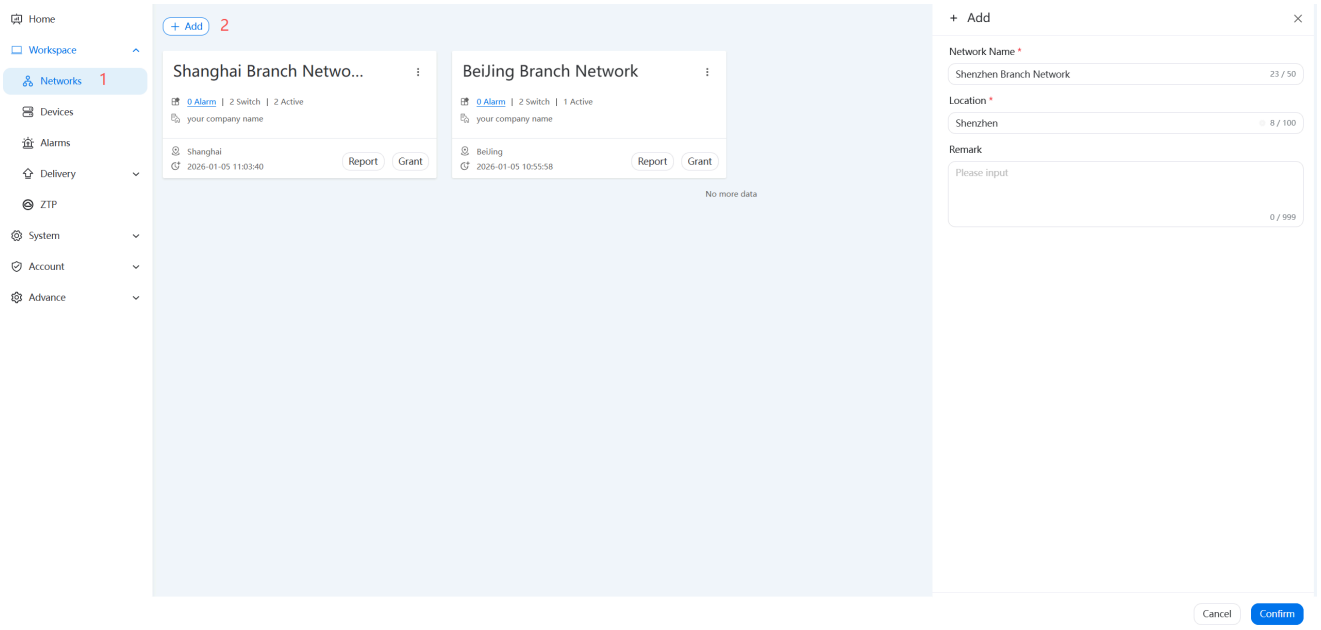
- **Obtaining the Binding Code via CLI Command**
  Login to the device, enter the command `show cloud-management state` to view it. If the binding code has already been obtained via the web interface, this step is not necessary.

```
S5624P# show cloud-management state
Current Global status:
============================================================
Cloud control state           : Enable
Cloud control mode            : Management-port
Current Cloud Root status:
============================================================
Root server host              : 192.168.200.112
Root server port              : 883
Root server connected at      : 2025-12-25T19:55:01.646
Current Cloud Sub status:
============================================================
```

```
Sub server address              : 192.168.200.112:883
Sub server connection state     : Connected
Sub bind state                  : bind
Sub bind code                   : RW8VJ
```

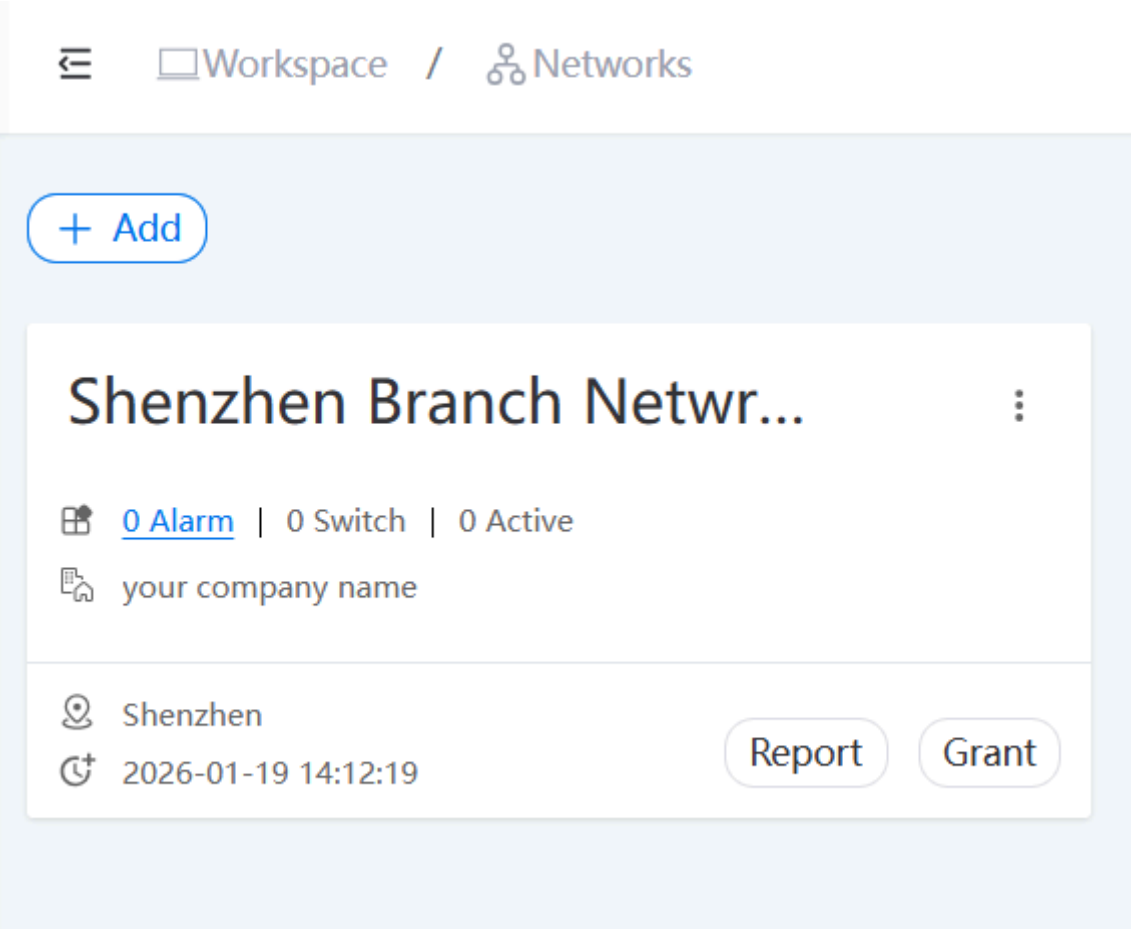
3.1.3. Create a Network

A network must be created in the Network module before binding a device. Users can create one in the Workspace -> Networks. Click the "Add" button, and fill in the basic information for the network to be created: "Network Name" and "Location", etc., as shown:



▲*Figure 13 Create Network Page*

Then, you can see that a network named "Shenzhen Branch Network" has been created. At this point, the number of devices and alarms under this network are both 0.

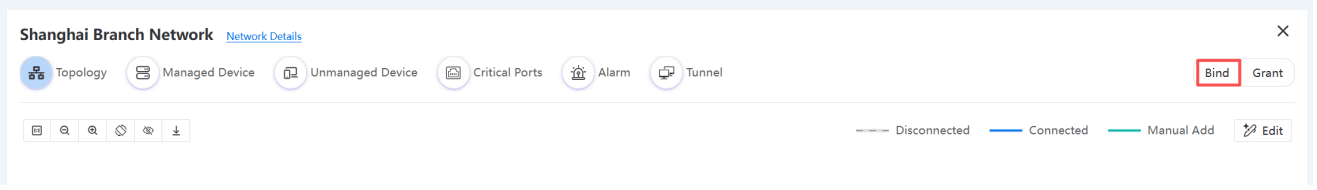


▲*Figure 14 Created Network List Page*

3.1.4. Cloud Platform Binding

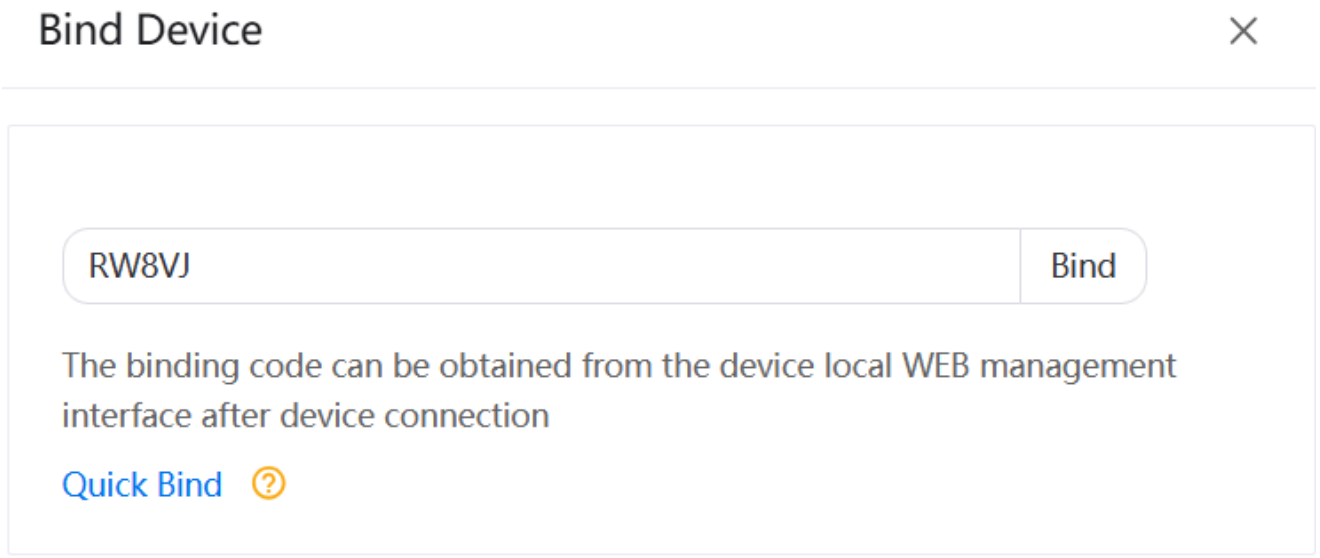
- **Bind via Binding Code**

Login to the cloud platform, enter the network where you want to bind the device, click the "Bind Device" button in the top right corner, and enter the binding code to bind, as shown:



▲*Figure 15 Device Binding Entry in Network Details Page*

In the new dialog box, enter the BindCode from the switch (case-sensitive) and click the "Bind" button (a prompt will appear upon successful binding).



▲*Figure 16 Enter Binding Code Dialog*

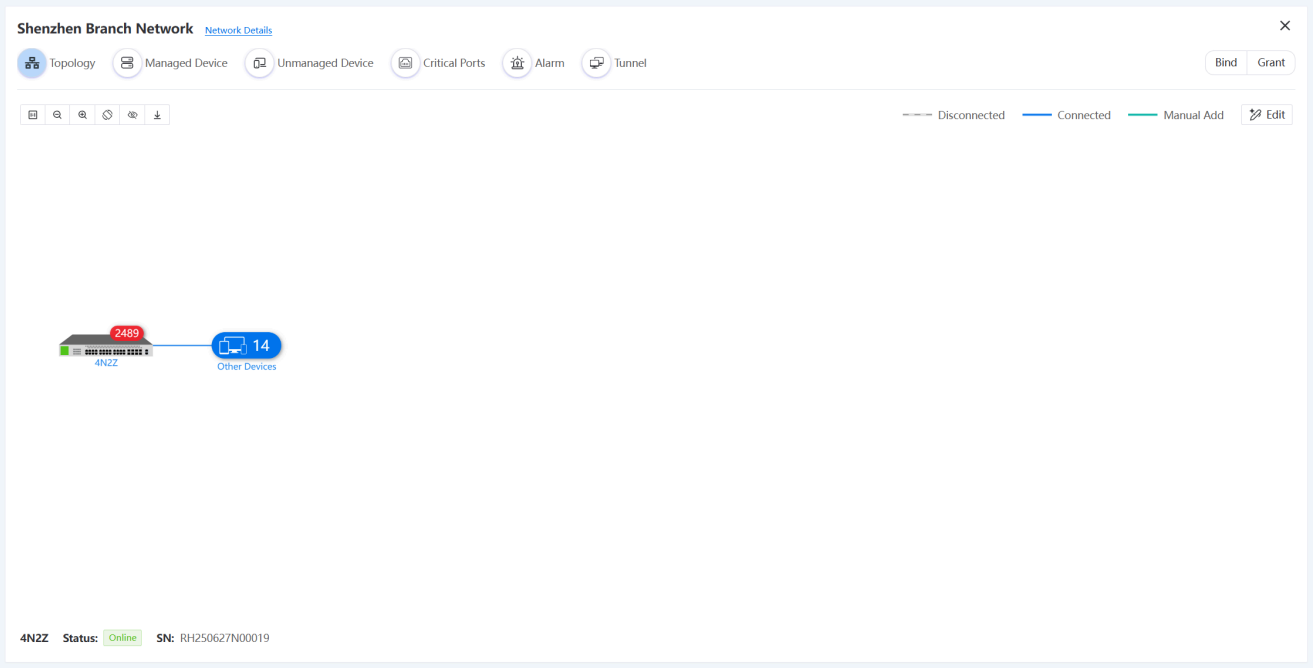
> **Note**
>
> - The device must be online to be bound from the cloud platform side.
> - A device can only be bound to one network.

At this point, device onboarding is complete. DHCS also supports onboarding via ZTP, CLI, DHCP auto-discovery protocol, and other methods. Please refer to the "How to Onboard Devices" chapter in the user manual for details.

3.1.5. How to Confirm Onboarding

- **View in Topology Map**

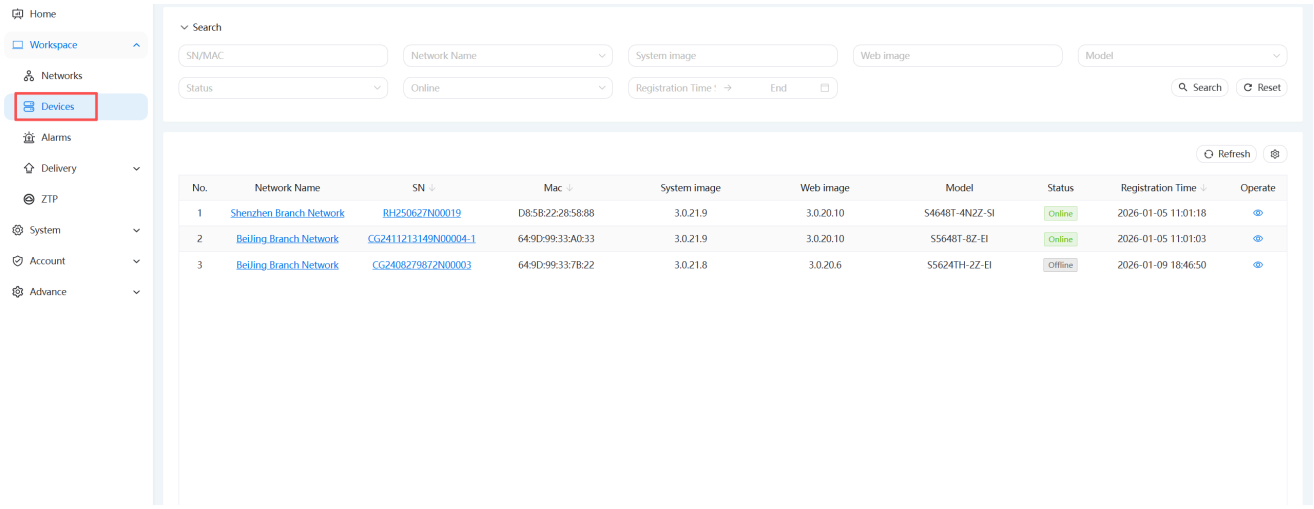
After successful binding, the device will be visible on the Network Topology page. If the device is connected to other devices, they will also be displayed in the topology map.



▲*Figure 17 Network Topology Showing Managed Device*

- **View in Device Management**

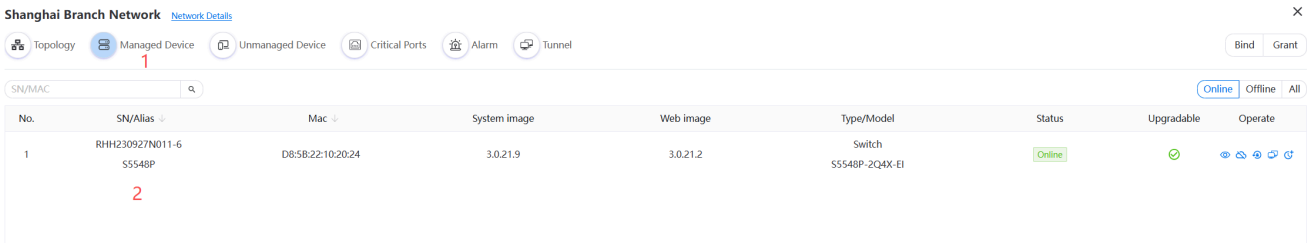
In Workspace -> Device Management, search for onboarded devices using criteria like serial number or MAC address. If the "Network" field in the search results displays the bound network name, it indicates successful onboarding. If empty, it means these devices are connected to the platform but not bound to a network.



▲*Figure 18 Device Management Page Viewing Onboarding Status*

- **View in Cloud-Managed Devices**

Check in Workspace -> Networks -> Cloud-Managed Devices to see if there are any managed devices. If present, it indicates successful onboarding. As shown:

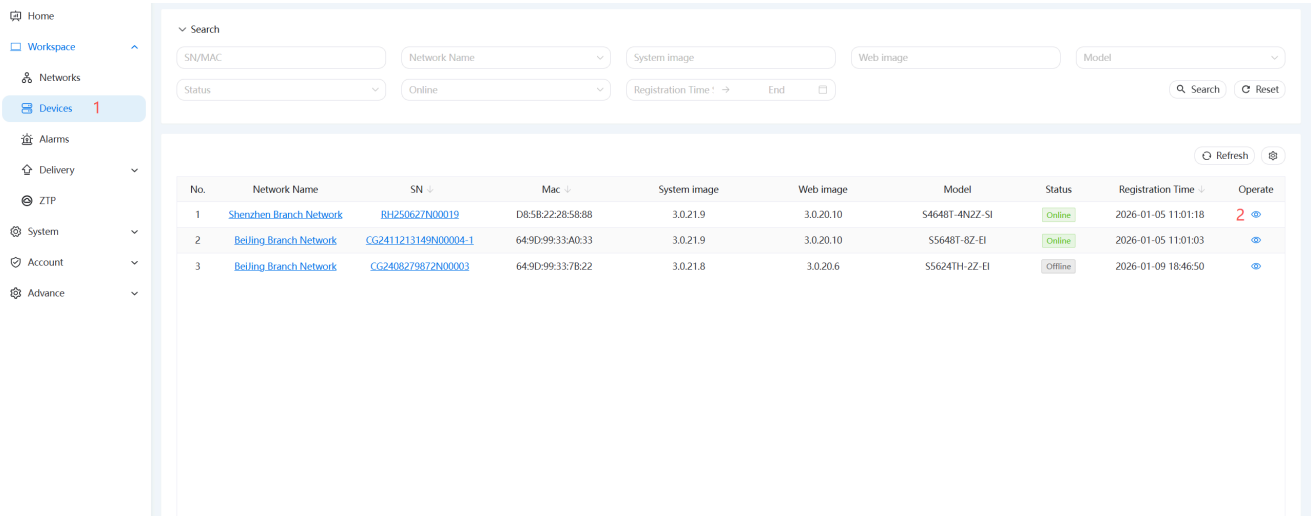


▲*Figure 19 Cloud-Managed Device List within Network*

3.2. Device Management

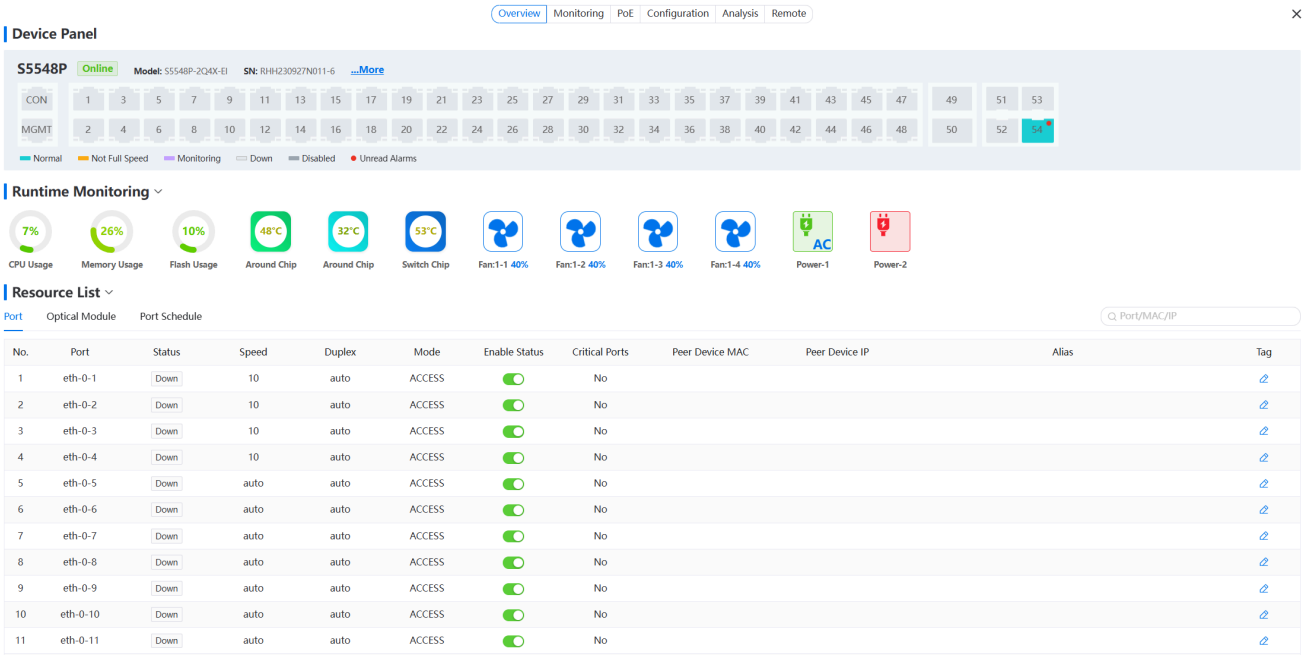
3.2.1. Device Overview

Go to Workspace -> Networks -> Cloud-Managed Devices or Workspace -> Device Management to view managed devices. Click the "View" button in the operation column to enter the device details page.



▲*Figure 20 View Button in Device List Operation Column*

The device overview is divided into three areas: Device Panel, Running Monitoring, and Resource List.



▲*Figure 21 Device Overview Page Layout*

- **Device Panel**

The Device Panel presents a simulated device port layout to the user, along with basic information such as device online status, model, serial number, port status, etc., in this area. Real-time information is displayed when the device is online; the last known information is shown when offline. The color meanings for device port states are shown in the table below:

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

▲*Table 3 Port Status Description*

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

Serial and management ports are identified with CON and MGMT labels on the Device Panel, as shown:

No.	Example	Description
1		Serial Port
2		Management Port

▲*Table 4 Serial and Management Port Examples*

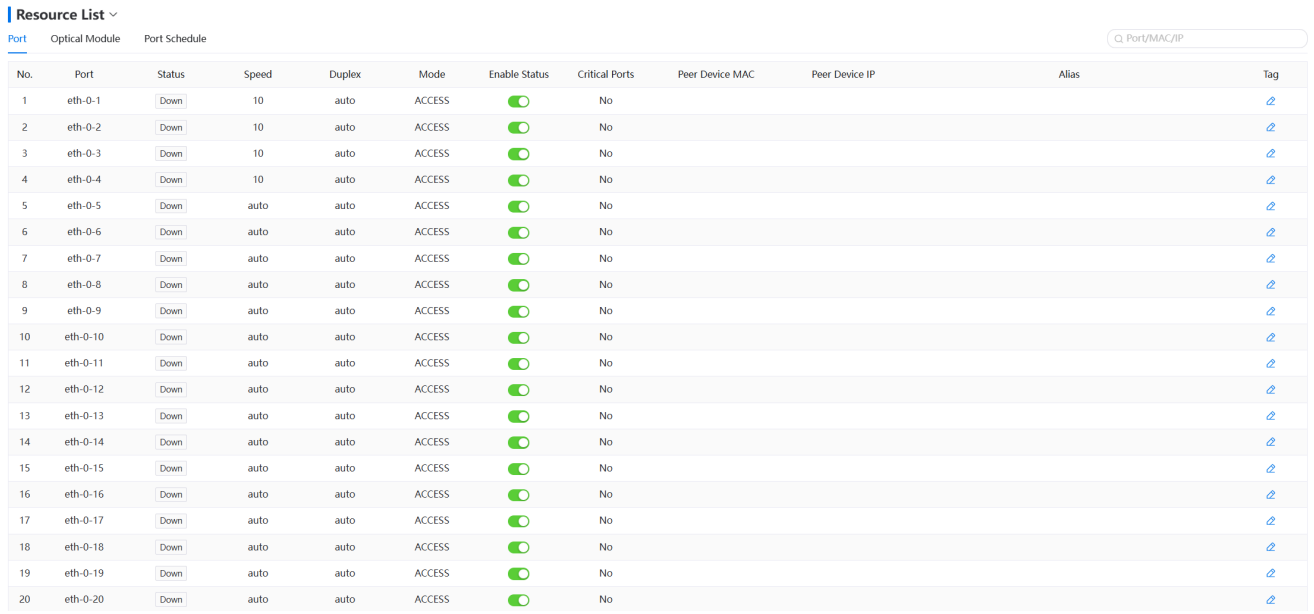
- **Running Monitoring**

  Running Monitoring integrates rich monitoring metrics:

  - CPU, Memory, Flash, Temperature: The higher the metric, the darker the icon color.
  - Fan: The faster the speed, the faster the animation. If a fan is not spinning, it can indicate it's not installed or faulty.
  - Power Supply: Three colors represent power supply status: Green (Normal), Red (Power supply present but not powered), Gray (Power supply not present).

- **Port List**

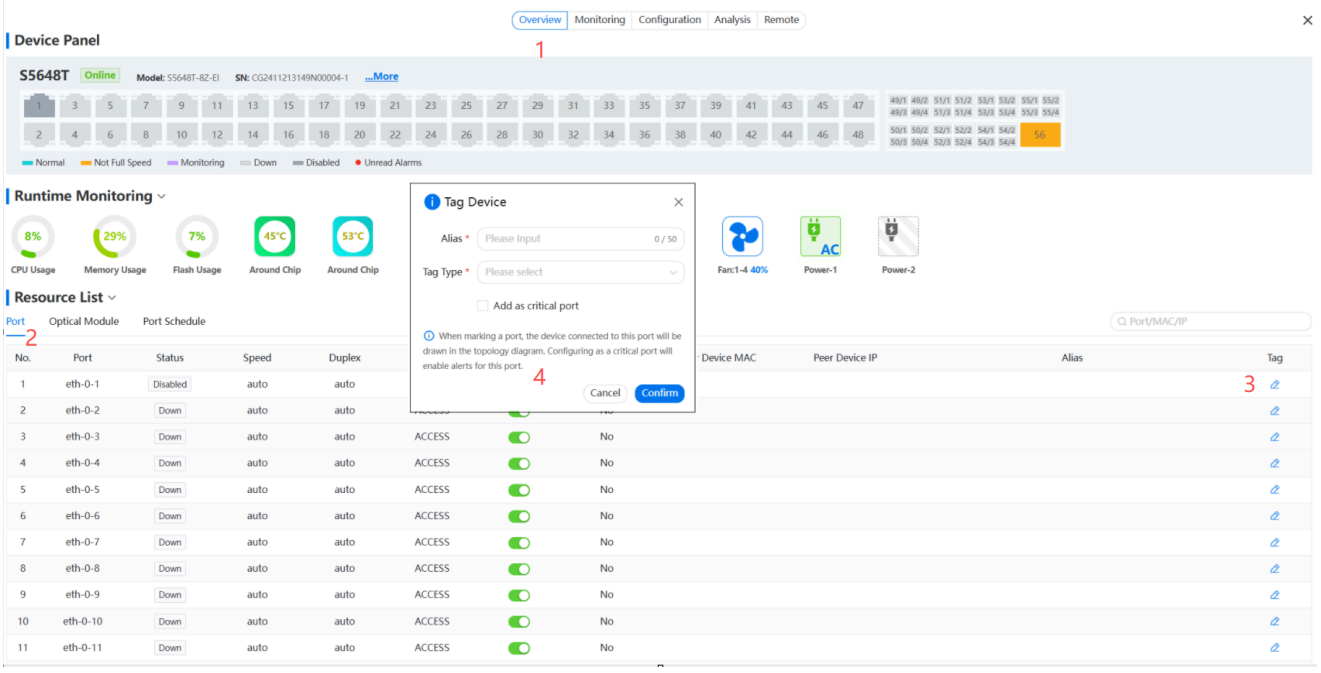
The Port List displays the operational information of all ports on the device, including the peer device's IP and MAC, allowing users to have a comprehensive understanding of port status. Users can manually control **Port Enable State** in the Port List, as shown:



▲*Figure 22 Port List and Port Enable Control*

- **Port Tagging**

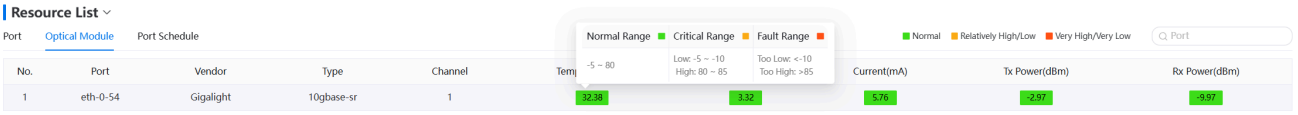
In the operation column of the Port List, you can mark the port with an alias or as a critical port for easy identification. Marking a device will automatically draw the port on the topology map with its marked type.



▲*Figure 23 Port Tagging Operation Interface*

- **Optical Module List**

The Optical Module List displays the operational data of all optical modules on the device, including module name, vendor, type, channel, temperature, voltage, current, transmit power, and receive power. This provides an intuitive view of optical module performance indicators, as shown:



▲*Figure 24 Optical Module List and Indicator Display*

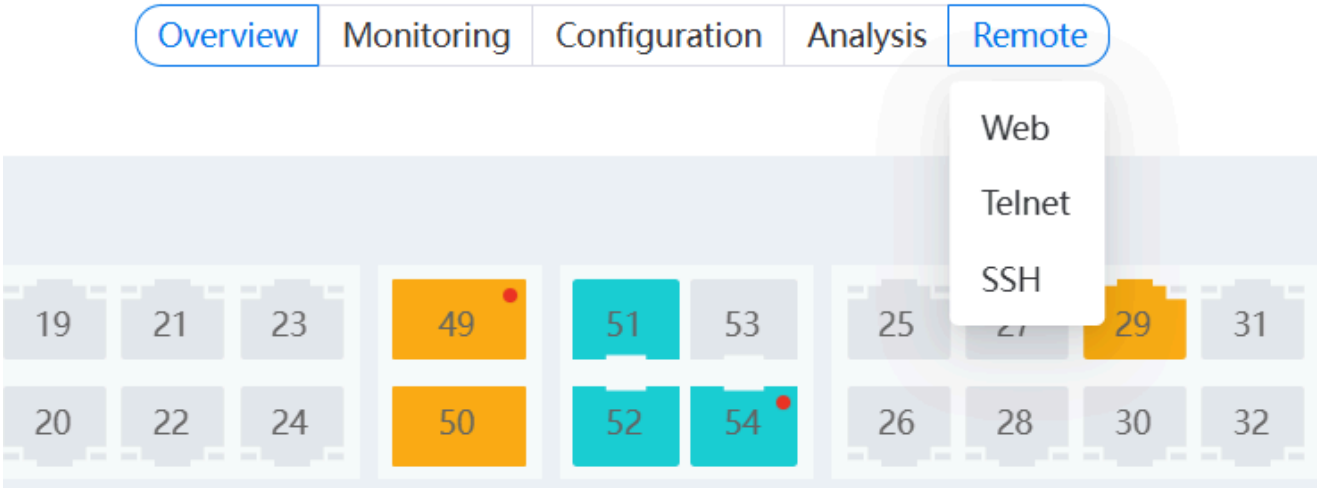
Hovering the mouse over a specific metric shows its corresponding range. The platform uses green, orange, and red to indicate the status of operational metrics. The specific meanings are as follows:

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

▲*Table 5 Optical Module Indicator Color Explanation*

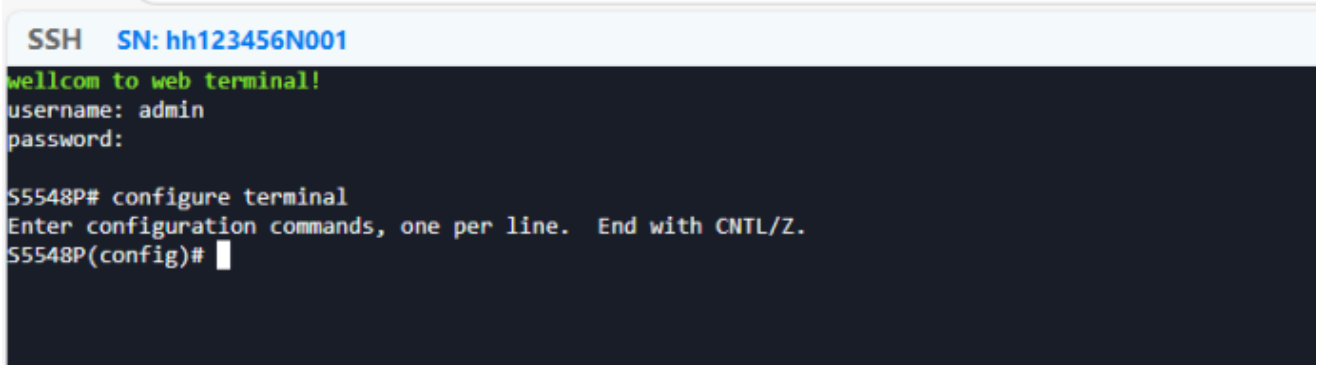
3.2.2. Remote Maintenance

Maintenance personnel can directly connect to devices through DHCS's remote operation and maintenance features, facilitating device debugging, configuration changes, or other operations. Available service types include web, SSH, and Telnet.



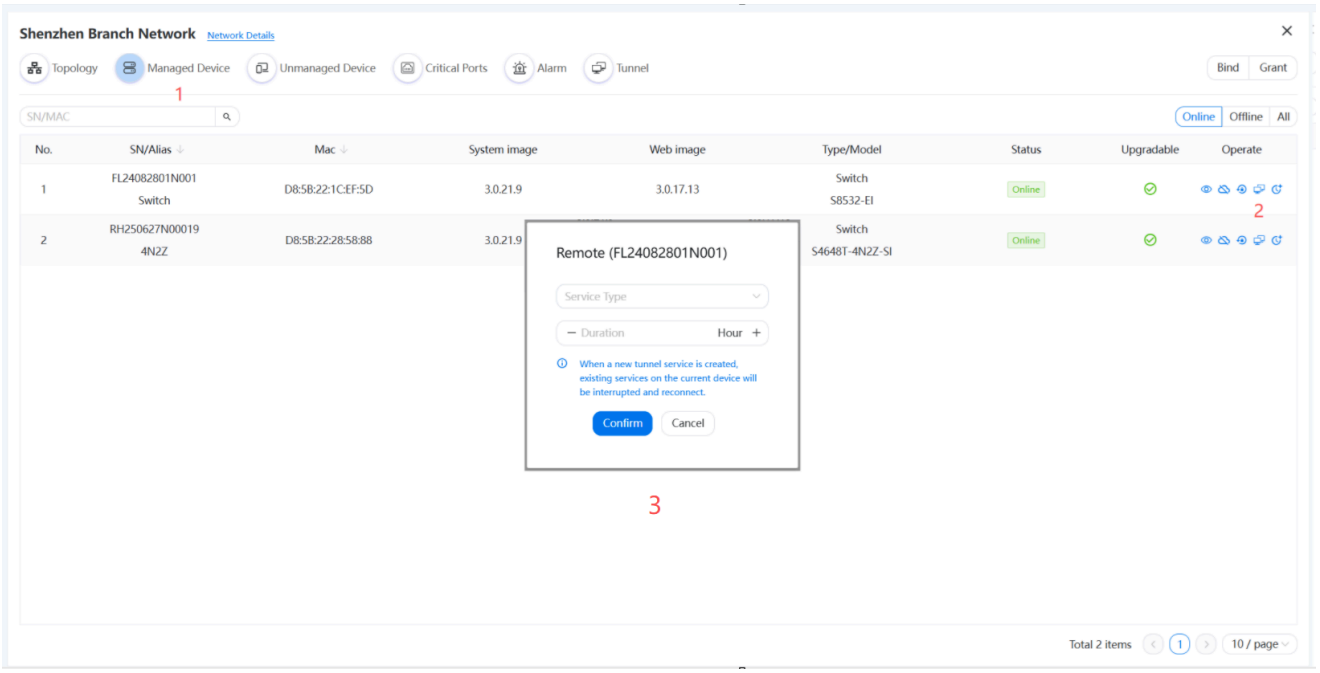
▲*Figure 25 Remote O&M Service Type Selection*

SSH and Telnet tunnels are automatically closed and released after being idle for half an hour by default.



▲*Figure 26 SSH/Telnet Tunnel Duration Explanation*

Alternatively, in the "Cloud-Managed Devices" list, select the "Remote O&M" icon in the "Operations" column, or select the desired device from the device list. A dialog box will pop up to choose the service type and duration.



▲*Figure 27 Initiating Remote O&M from Device List*

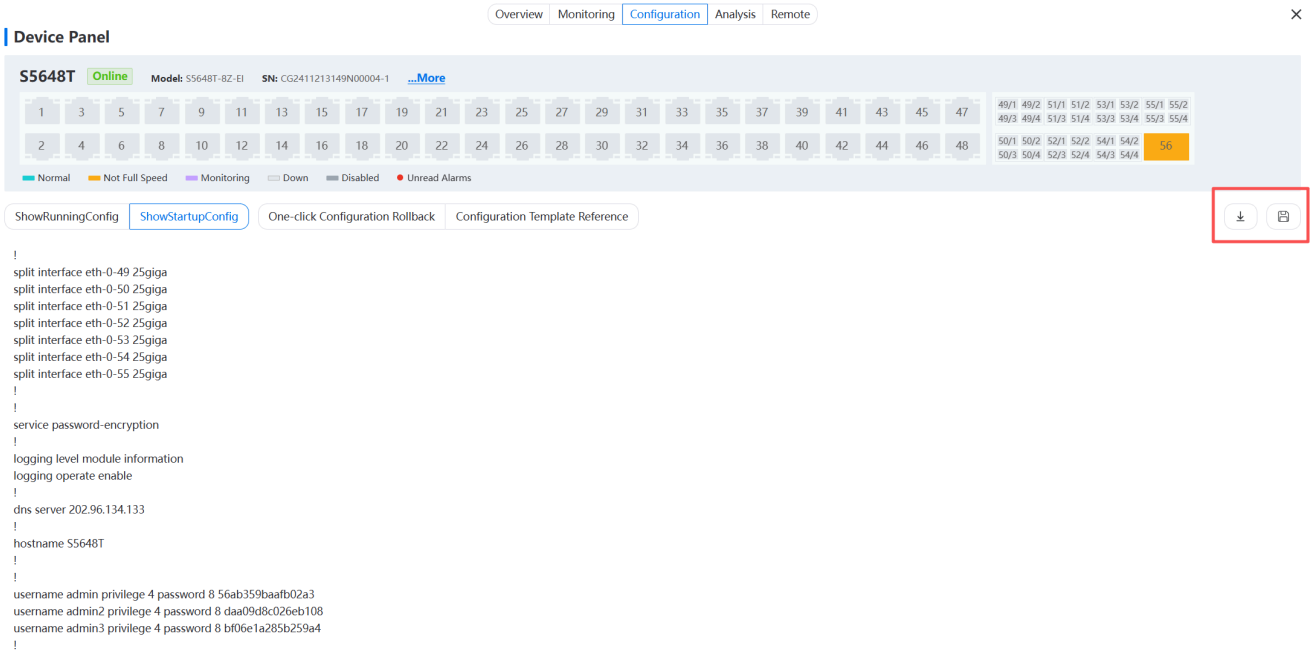
> **Note**
>
> - Remote access still requires knowledge of the login username and password.
> - After logging into the switch via remote O&M, first confirm the normal communication between the device and the cloud platform's communication port. Unless necessary, avoid misconfigurations during subsequent configuration changes that could interrupt communication between the switch and the cloud platform, causing the switch to fall out of cloud management.

3.2.3. Configuration Management

Configuration Management provides users with basic functions for viewing configuration, downloading configuration, one-click configuration rollback, saving configuration templates, and applying configuration templates.

- View and Download Configuration

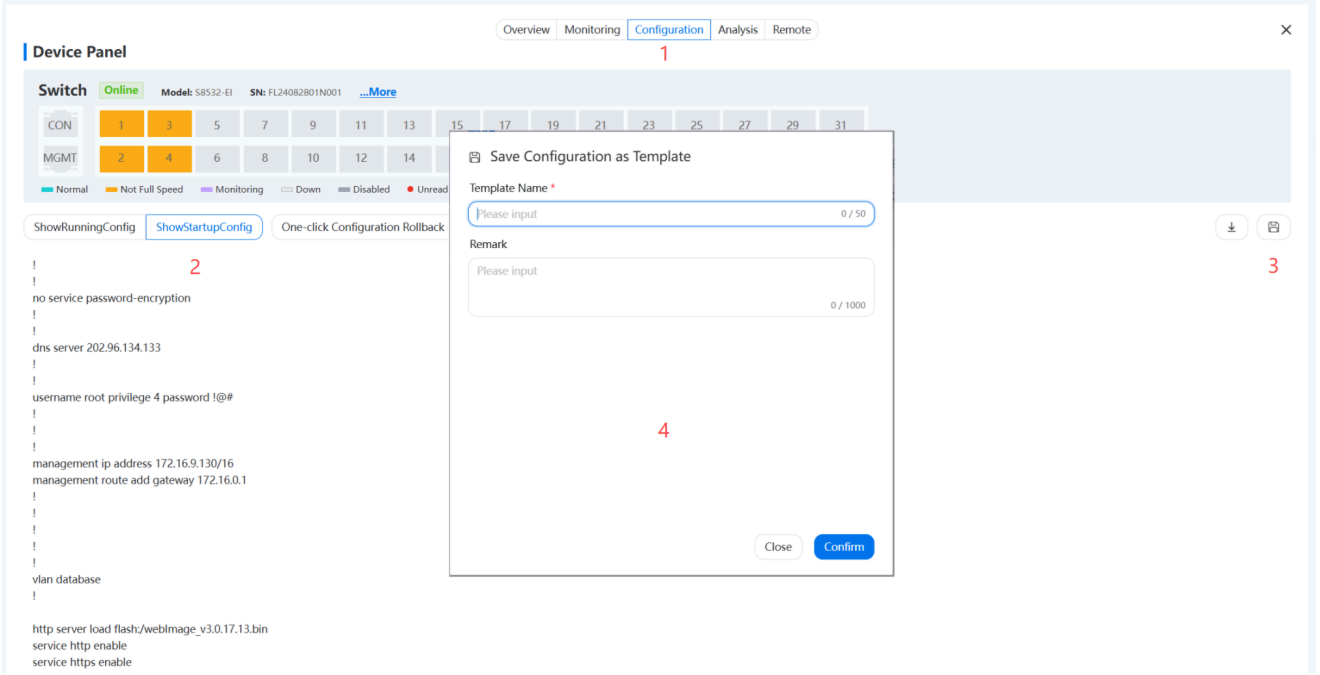
Click "ShowRunningConfig" to display the device's currently running configuration. Click the download button on the right to download the current running configuration to the user's host.
Click "ShowStartConfig" to display the device's startup configuration. Click the download button on the right to download the startup configuration to the user's host.



▲*Figure 28 Configuration View and Download Interface*

- Save Configuration Template

When switching to "show startup config", the platform provides the function to save the displayed content to the configuration template library. Click the save button as shown:

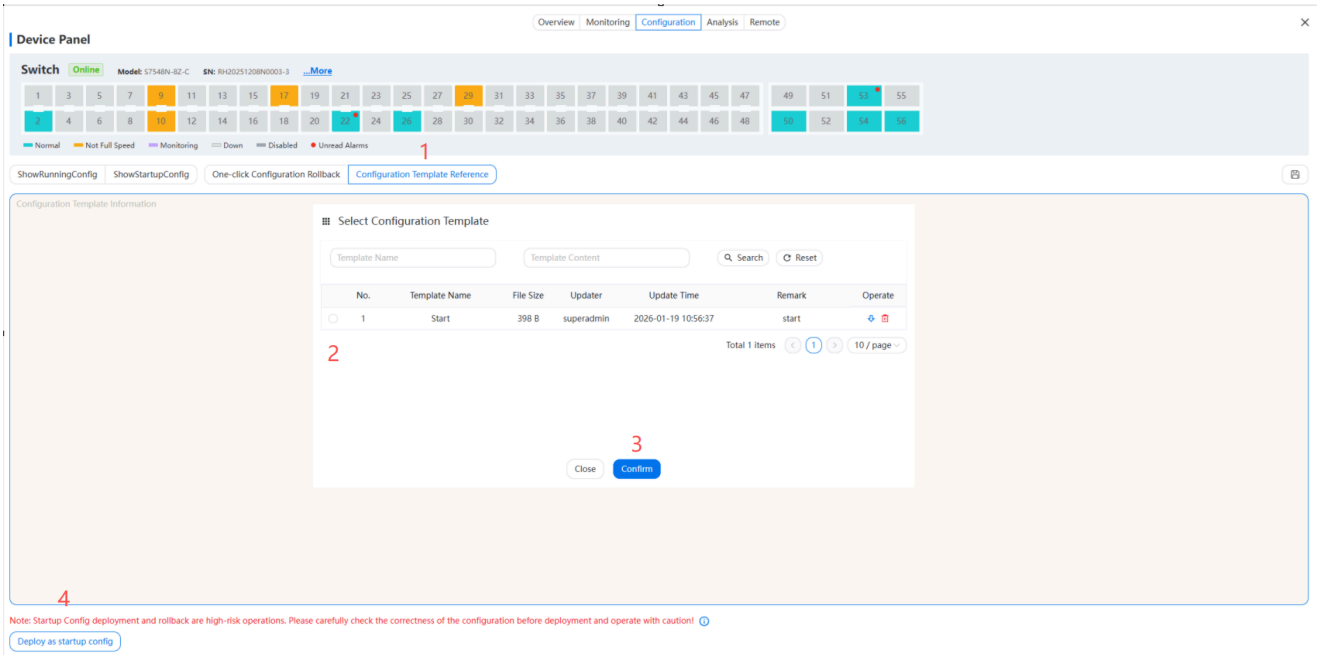


▲*Figure 29 Save Configuration Template Dialog*

After saving as a template, it can be referenced later.

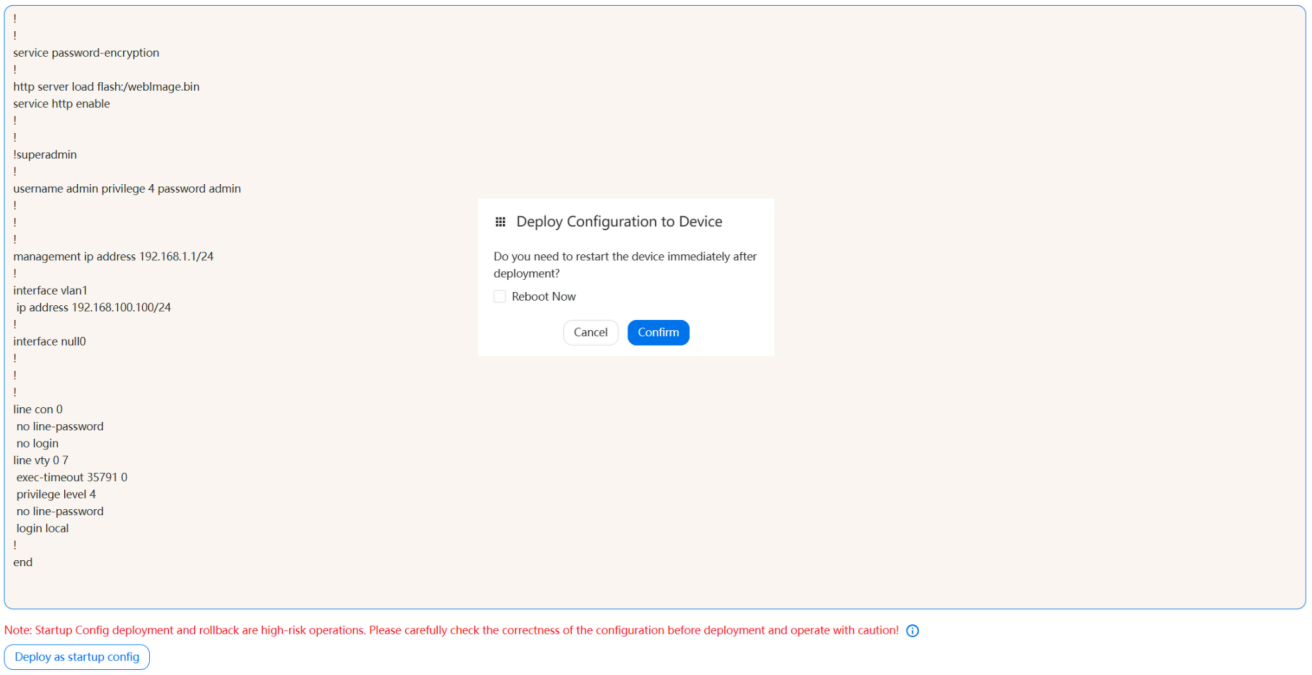
- Configuration Template Reference

Saved configuration templates can be used for later configuration restoration on the same device. Click the "Reference Configuration Template" button, select the correct configuration template, and import the configuration to this switch, as shown below:



▲*Figure 30 Reference Configuration Template Dialog*

After clicking the "Confirm" button, the complete configuration will be displayed on the page. Please carefully confirm that this is the configuration you need and that it is applicable to the current model. After confirmation, click the "Apply as startup config" button at the bottom of the configuration information. The current device's startup configuration will be replaced, and after a reboot, the applied configuration will be used:



▲*Figure 31 Configuration Preview and Application Interface*

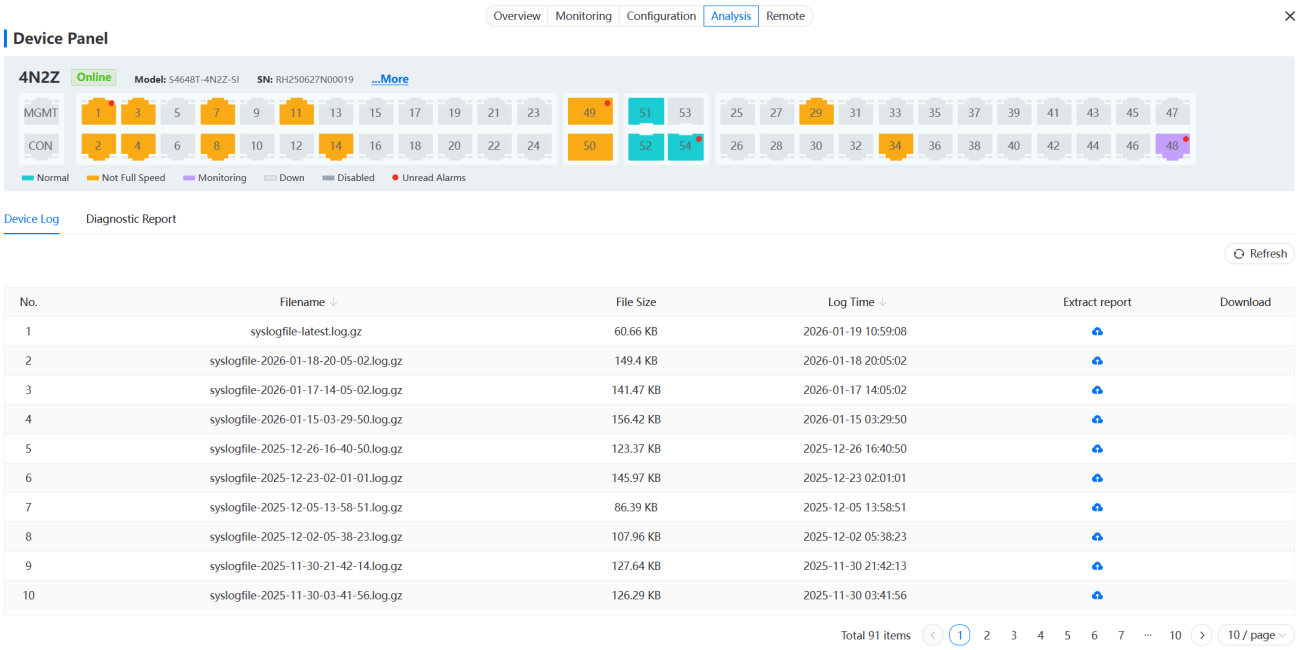
If there are multiple switches of the same model in the network with similar configurations, you can select an already saved configuration template, modify it, and then apply it.

3.2.4. Log Analysis

The Log Analysis module can retrieve device operation logs and diagnostic reports.

- Get Operation Logs

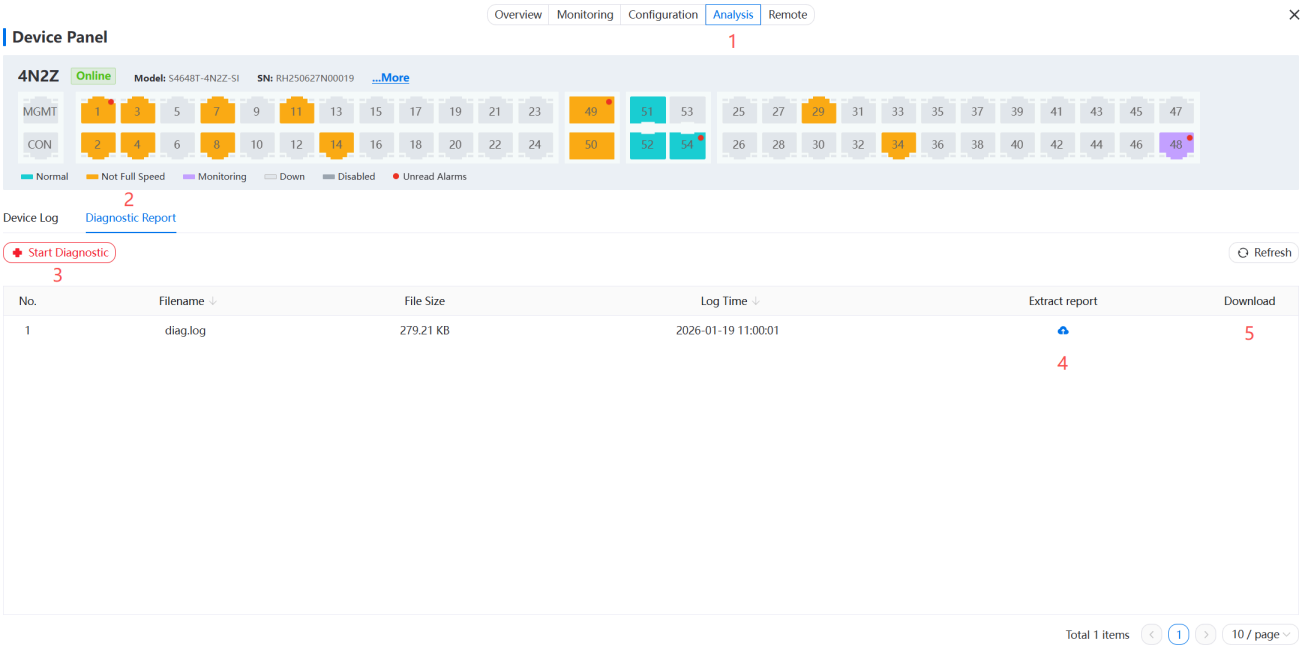
The system logs already present on the switch are listed by default. To obtain a log file, click the "Extract" button to upload the log to the cloud. After refreshing, a download button will appear. Click it to download to the user's host.



▲*Figure 32 Operation Log Acquisition Interface*

- Get Diagnostic Report

Go to 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 will be deleted, keeping only the latest one. Click the "Extract" button to upload the report file to the cloud platform, and a download button will appear in the report list. Click to download and view.

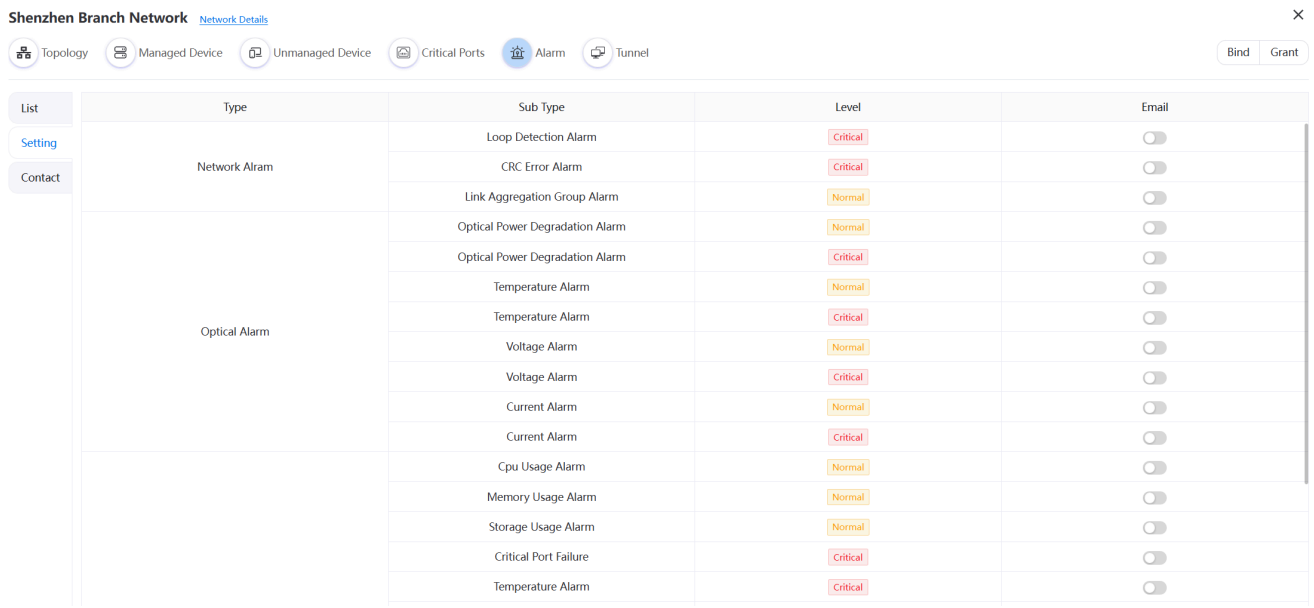


▲*Figure 33 Diagnostic Report Acquisition Interface*

3.2.5. Alarm Settings

- Email Alarm Notification

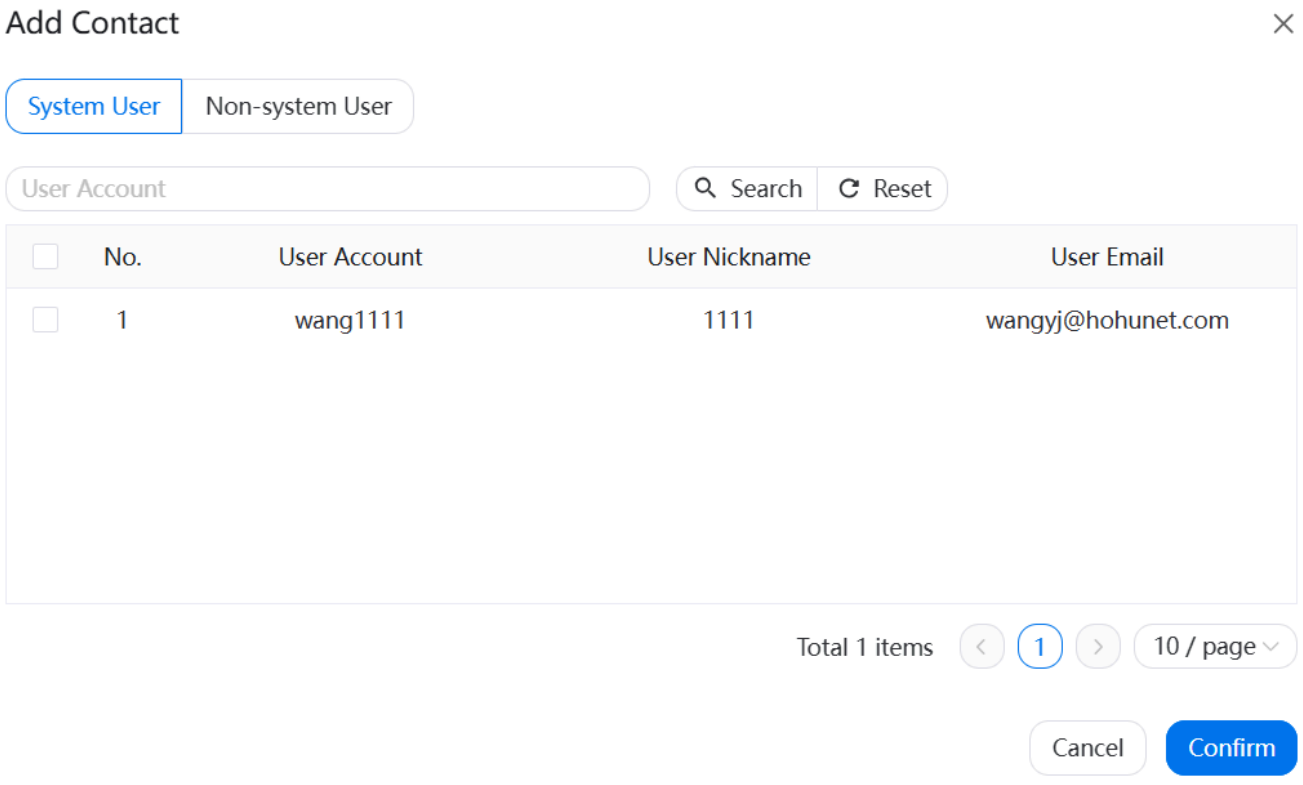
Click on the network to enter the Network Settings page. Then click "Alarm Information -> Notification Settings" and select to enable the alarm items for which notifications are required.



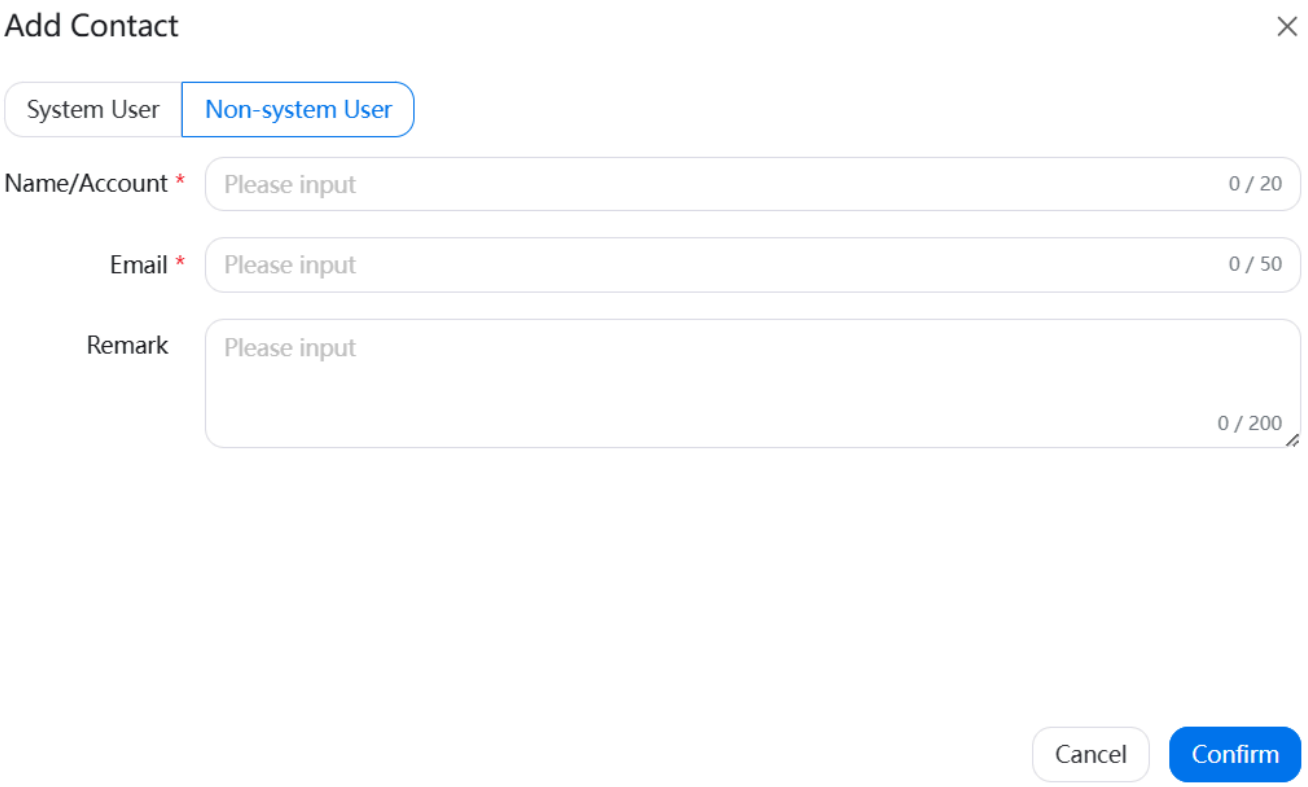
▲*Figure 34 Alarm Notification Settings Page*

- Contact Settings

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 under that network. The Alarm Contacts interface is shown:



▲*Figure 35 Alarm Contacts Page (System Contacts)*

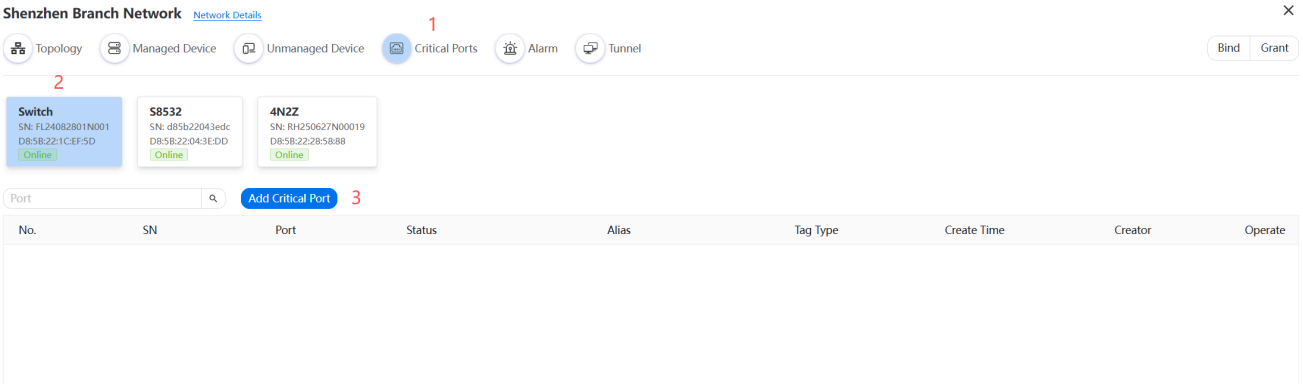


▲*Figure 36 Alarm Contacts Page (Non-System Contacts)*

3.2.6. Alarm Test

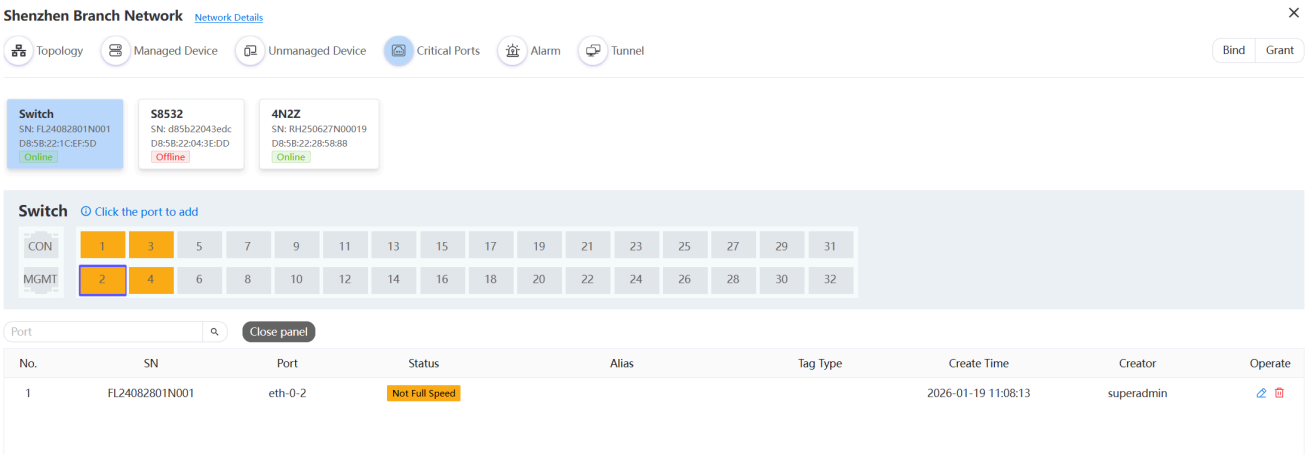
- Step 1: Define Critical Ports

Some ports in the network connect to devices that require special attention, such as ports connecting to critical servers, ports accessing the Internet or interconnecting with other networks, ports connecting to key location monitoring devices, etc. Abnormal changes in the status of these ports require faster awareness and response. We can define these ports as "Critical Ports" and enable the corresponding alarm function to notify maintenance personnel promptly when port status becomes abnormal.



▲*Figure 37 Define Critical Ports Guide Interface*

Then, following the prompt information, click on the corresponding port on the panel to add the port to the "Critical Ports" list:



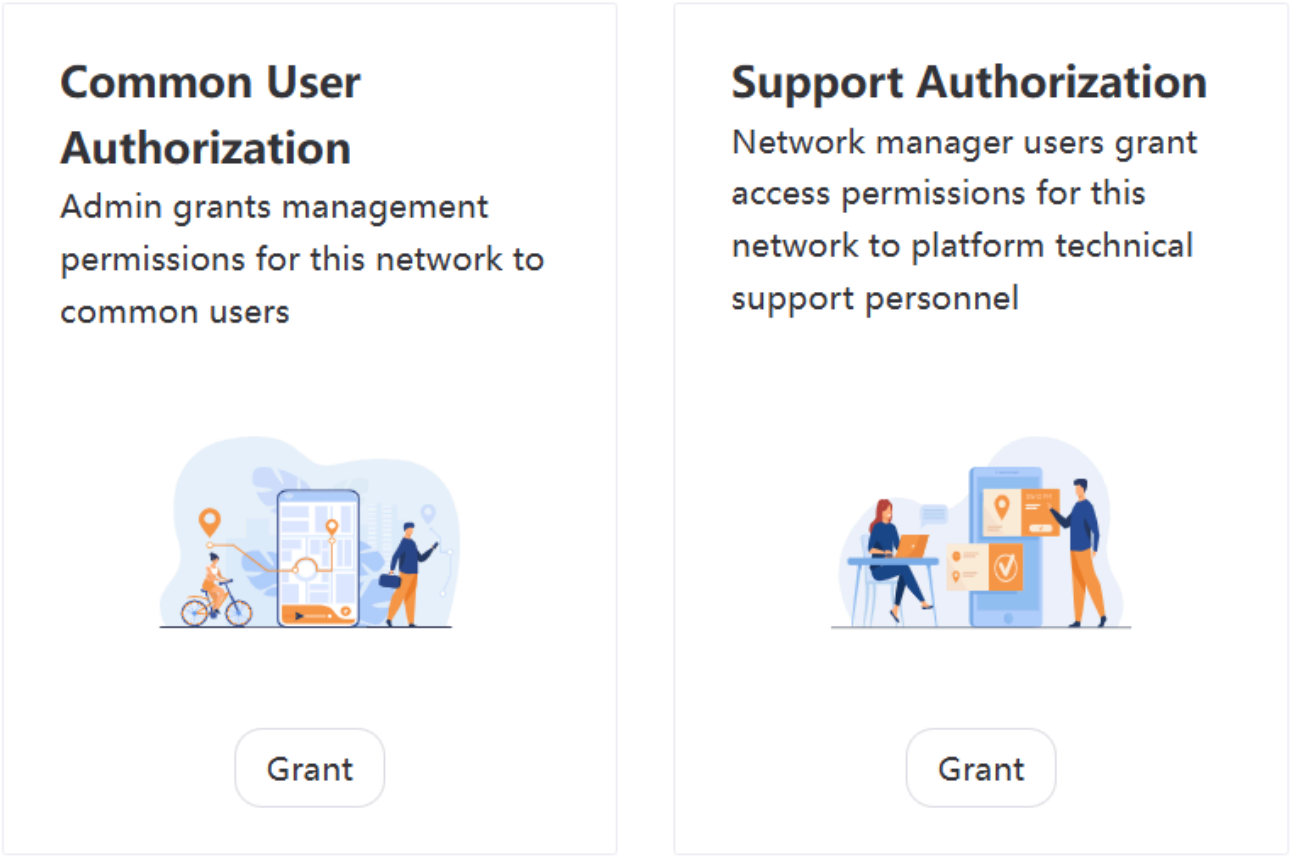
▲*Figure 38 Marking Critical Ports on Device Panel*

- Step 2: Test Email Notification

Briefly disconnect and reconnect the cable for the critical port eth-0-54 on the device, then check the "Alarm Records". A new alarm for "Critical Port Exception" should have been added.

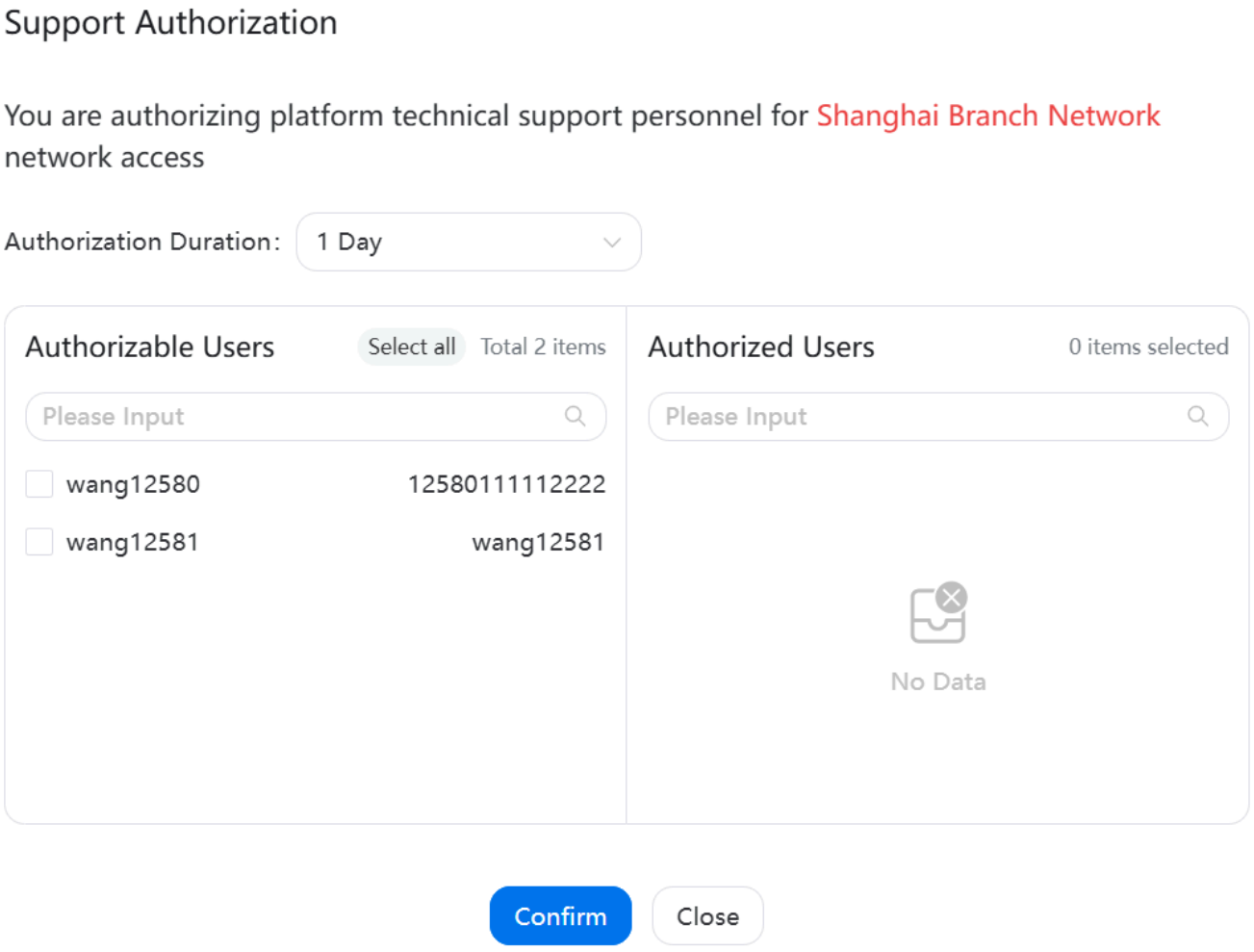
3.3. Request Technical Support

In tenant mode, if a tenant encounters network issues they cannot handle and need platform technical support assistance, they can authorize platform technical support. Click "Platform Support Authorization" in Network Authorization.



▲*Figure 39 Network Authorization Page*

A dialog box will display the DHCS platform's technical support engineer accounts. Select the engineer you want to contact and click "Confirm". The platform will notify the technical support via email. The technical support will have partial operational permissions for the authorized network and devices within a specified time.

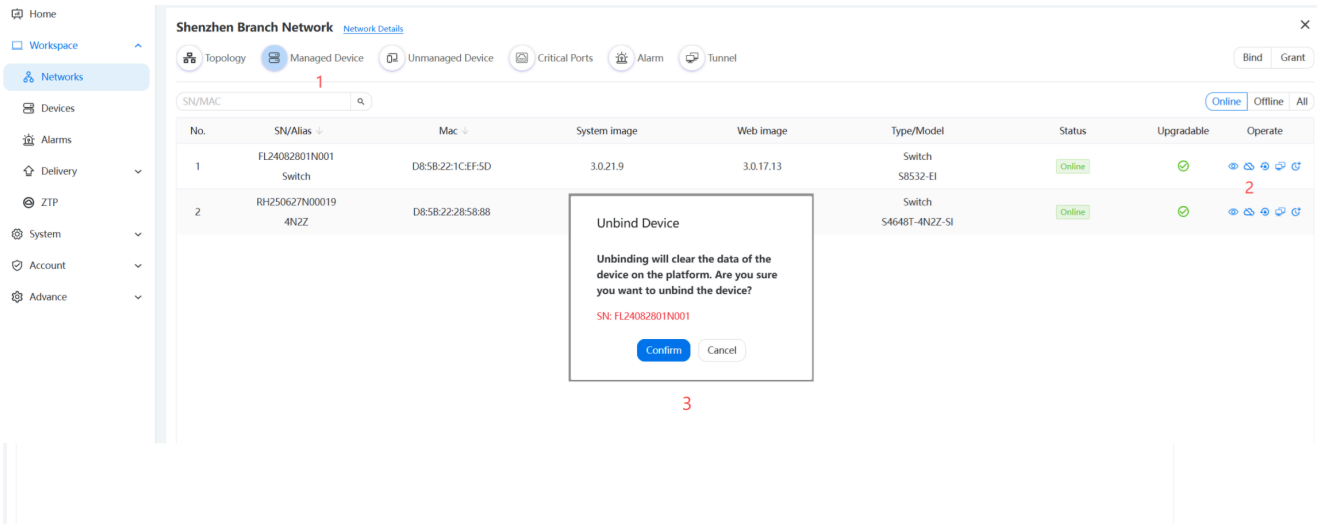


▲*Figure 40 Platform Technical Support Authorization Dialog*

3.4. How to Decommission

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

- **Unbind from Cloud Platform**
  In Workspace -> Device Management, click the "Unbind" button for the device you want to unbind in the operation column. A dialog box will pop up to confirm unbinding. Confirm to proceed. If the device is offline at the time of unbinding, the binding relationship will be automatically removed when the device comes back online.



▲*Figure 41 Device Unbind Operation Dialog*

- **Unbind from Device Side**

Login to the device's web system, go to Maintenance -> 【Cloud-Management Configuration】, find the "Unbind" button and click it. 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.

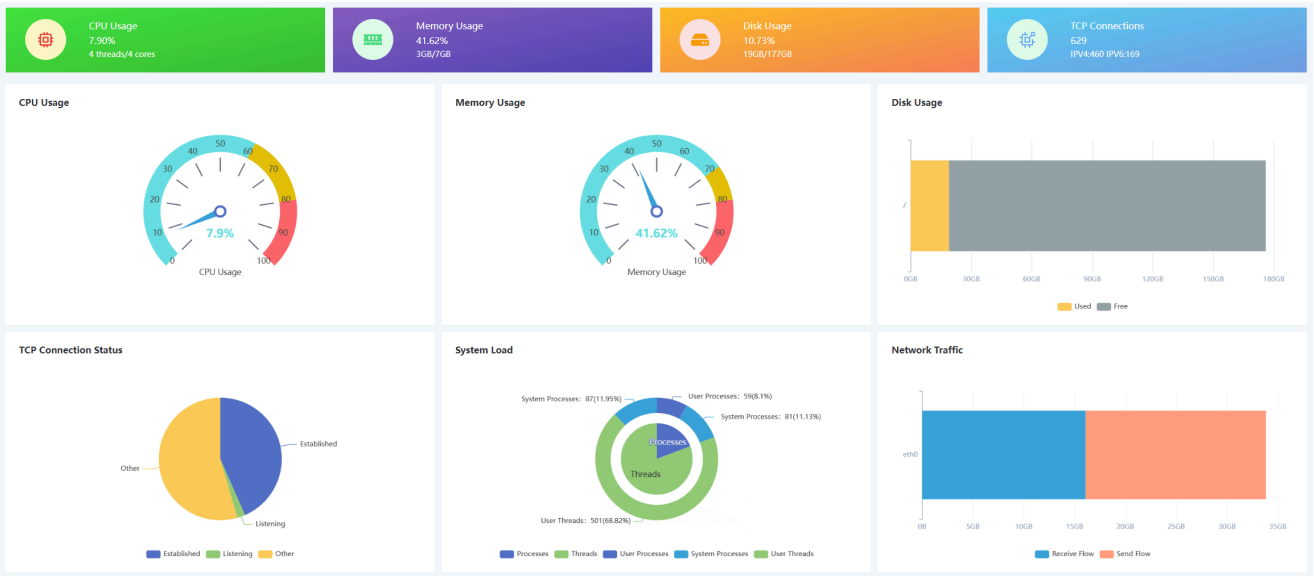
4. System Management (Platform Administrator)

The following are the system configuration steps for the platform administrator (superadmin). Tenant users are not required to perform these operations.

4.1. System Dashboard

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

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



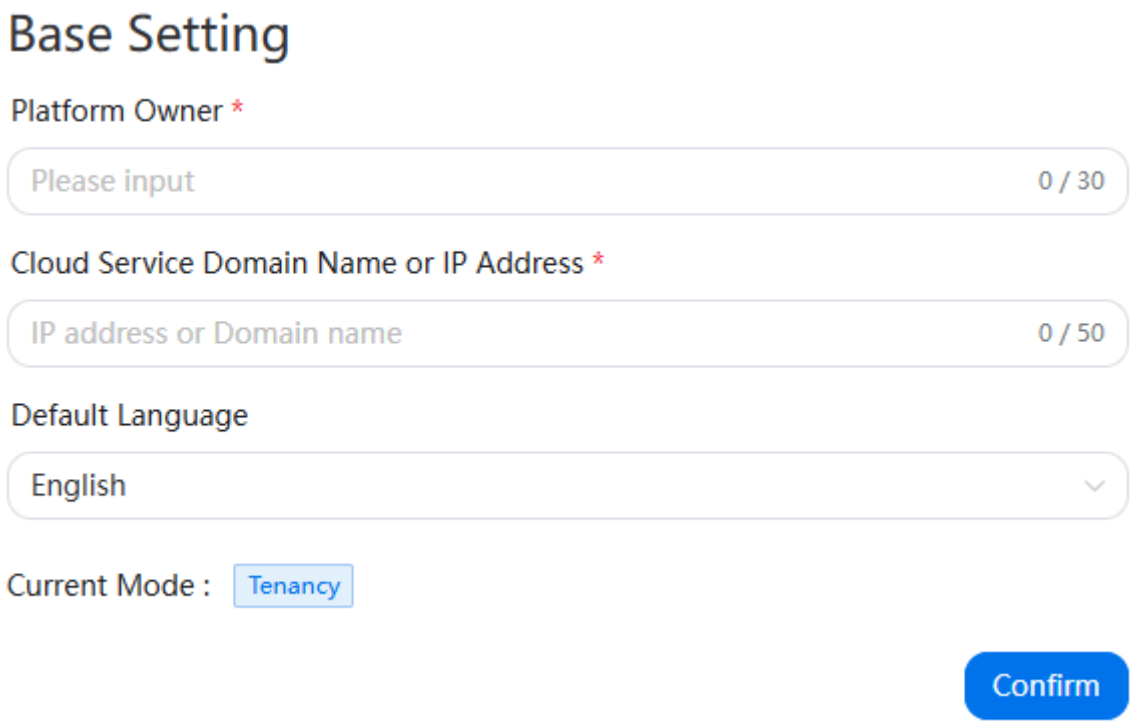
▲*Figure 42 System Dashboard Page*

4.2. Platform Settings

To ensure normal platform operation, some settings need to be configured after platform installation, including Basic Settings, Customer Customization Settings, Mail Server Settings.

4.2.1. Basic Settings

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

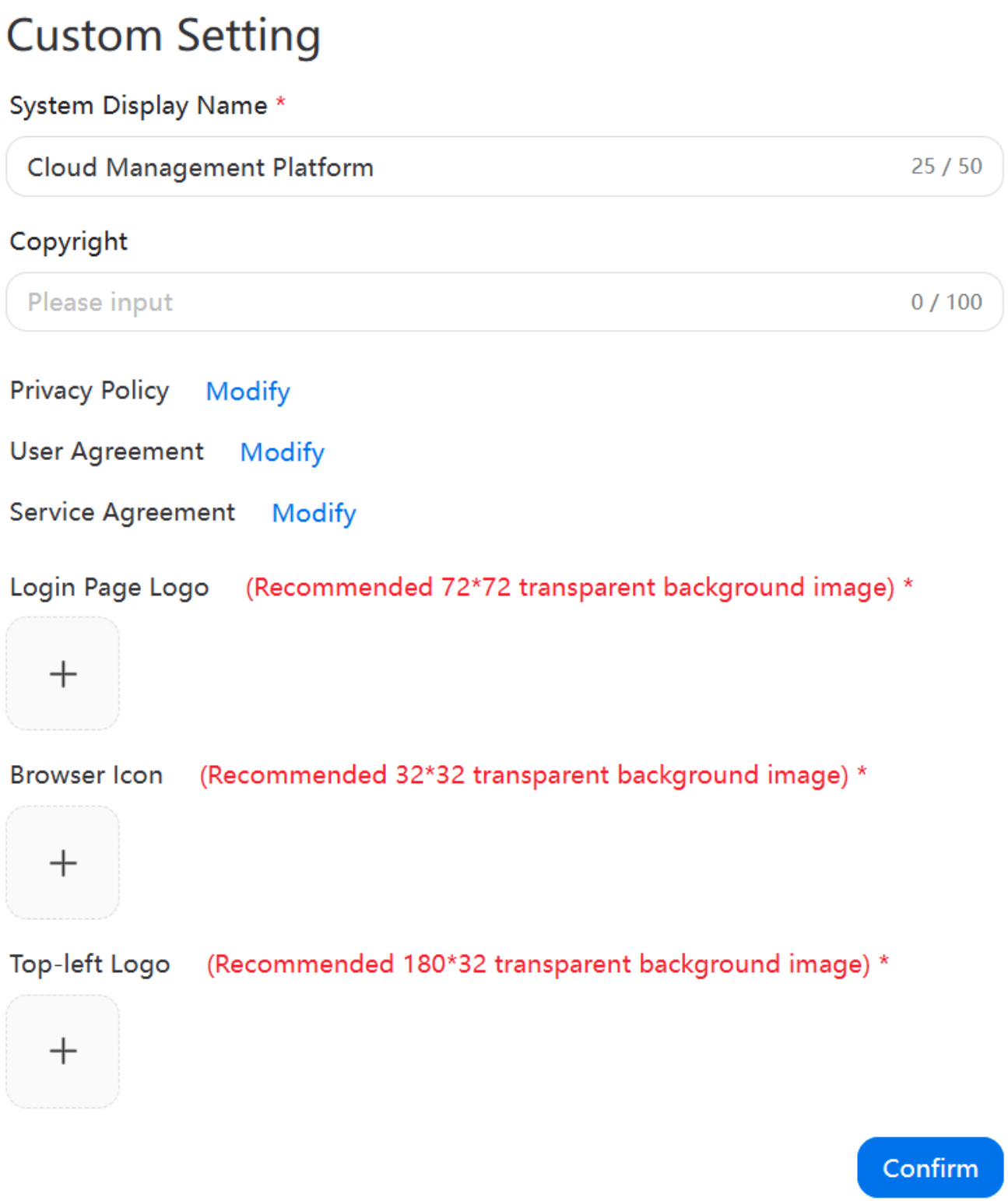


▲*Figure 43 Basic Settings Page*

- Platform Owner: The owner/entity of the platform, can be displayed to users where necessary.
- Cloud Service IP: Mainly used for device communication interfaces and when establishing tunnel services.
- System Default Language: Can be switched to default English or Chinese display based on the local language to reduce frequent switching.
- Multi-Tenancy Mode: Can only be set for the first time after installation and cannot be modified afterward.

4.2.2. Customer Customization Settings

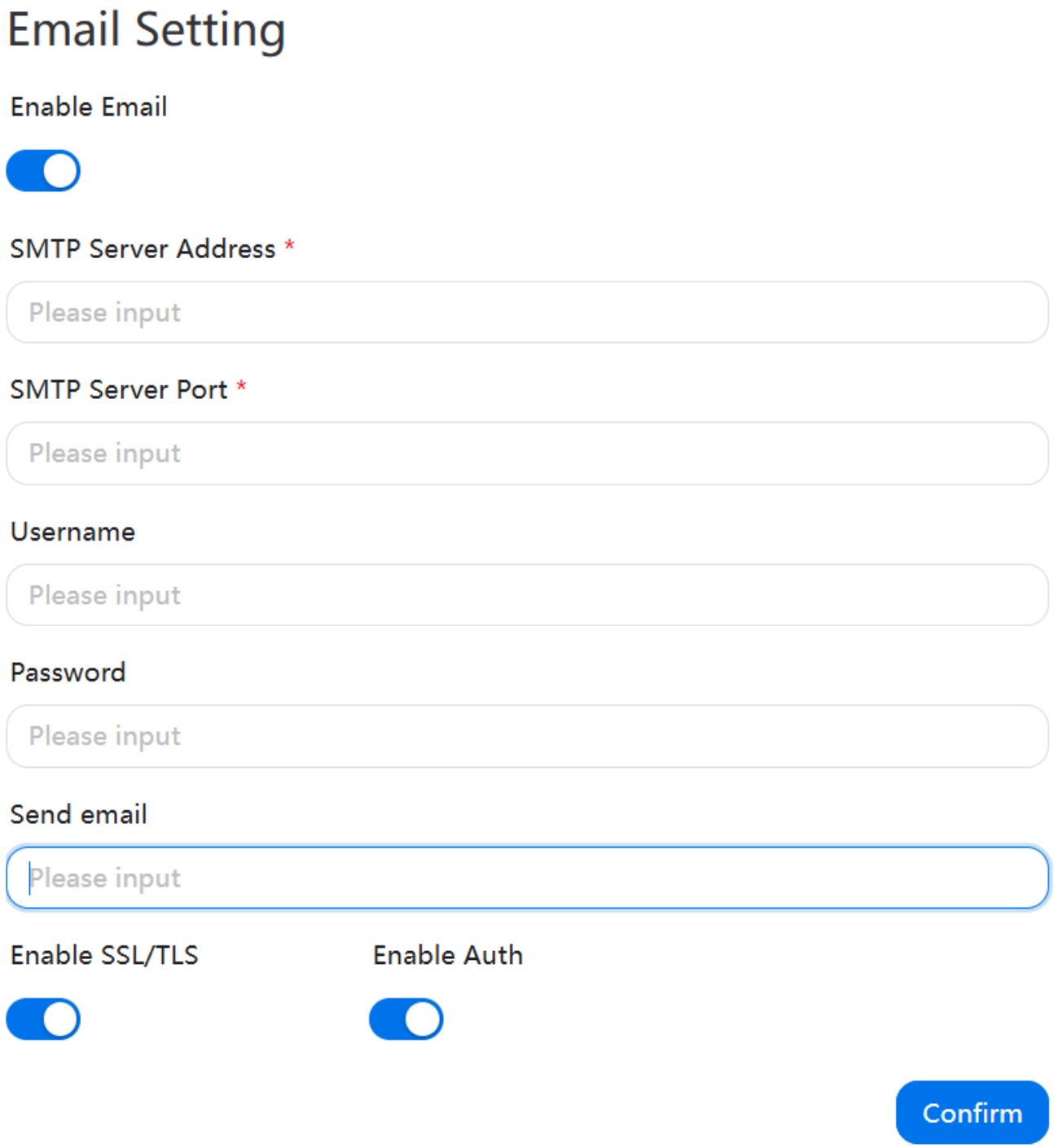
Customers can customize the platform's name, logo, website filing information, privacy policy, user agreement, service agreement, etc. Among these, if the system detects content for the user agreement, privacy policy, and service agreement, it will display an entry point on the login page. If not configured, the entry will not be shown. The Customer Customization Settings interface is shown:



▲*Figure 44 Customer Customization Settings Page*

4.2.3. Mail Server Settings

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

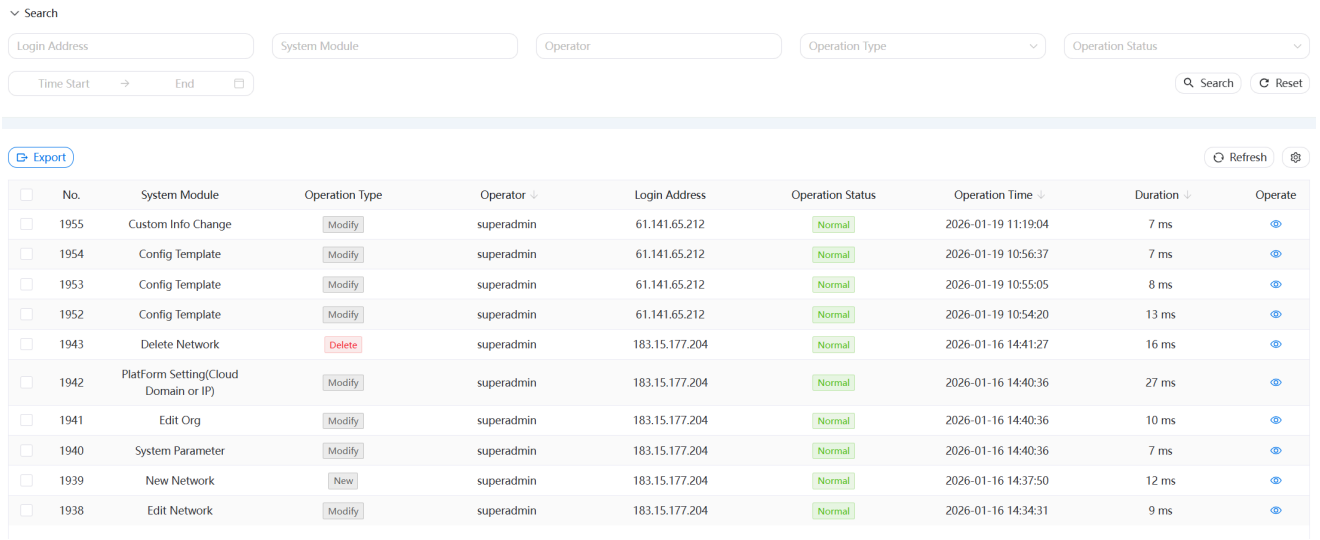


▲*Figure 45 Mail Server Settings Page*

> **Note**
> Email notifications require enabling in conjunction with the email templates.

4.3. Operation Logs

Operation Logs record all user operations on the cloud platform. Platform Administrators can use the search function to quickly retrieve logs they are concerned about. They can also view the detailed content of a log or download specific logs.



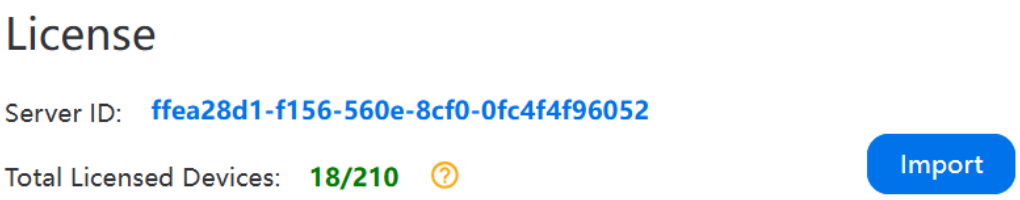
No.	System Module	Operation Type	Operator	Login Address	Operation Status	Operation Time	Duration	Operate
1955	Custom Info Change	Modify	superadmin	61.141.65.212	Normal	2026-01-19 11:19:04	7 ms	
1954	Config Template	Modify	superadmin	61.141.65.212	Normal	2026-01-19 10:56:37	7 ms	
1953	Config Template	Modify	superadmin	61.141.65.212	Normal	2026-01-19 10:55:05	8 ms	
1952	Config Template	Modify	superadmin	61.141.65.212	Normal	2026-01-19 10:54:20	13 ms	
1943	Delete Network	Delete	superadmin	183.15.177.204	Normal	2026-01-16 14:41:27	16 ms	
1942	PlatForm Setting(Cloud Domain or IP)	Modify	superadmin	183.15.177.204	Normal	2026-01-16 14:40:36	27 ms	
1941	Edit Org	Modify	superadmin	183.15.177.204	Normal	2026-01-16 14:40:36	10 ms	
1940	System Parameter	Modify	superadmin	183.15.177.204	Normal	2026-01-16 14:40:36	7 ms	
1939	New Network	New	superadmin	183.15.177.204	Normal	2026-01-16 14:37:50	12 ms	
1938	Edit Network	Modify	superadmin	183.15.177.204	Normal	2026-01-16 14:34:31	9 ms	

▲*Figure 46 Operation Logs Page*

4.4. License Management

4.4.1. Overview

By default, the platform supports free onboarding of 5 devices. If users require more, they can apply for a License for more devices through the business personnel. Each License permits a certain number of devices to be onboarded to the cloud platform. Multiple Licenses can be combined, and the corresponding number of permitted devices will be added together.

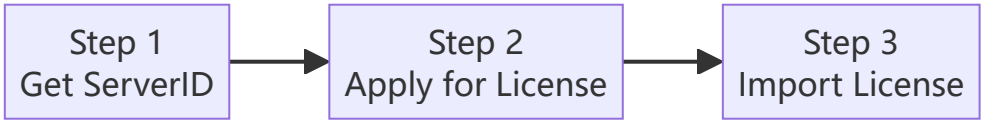


No.	License ID	Licensed Devices	Import Time
1	Default	5	-
2	961e866e-a328-4c10-95e4-d970ee50f3f3	100	2025-12-27 10:56:21
3	2e5ff6ff-2fbe-42f7-9792-65a872cb2cdd	5	2025-12-30 14:33:37
4	f75e6d49-dc11-4016-abf5-20ccc4cf4ccf	100	2025-12-26 21:37:53

▲*Figure 47 License Management Page*

4.4.2. Operation Process

The License application process is shown below:



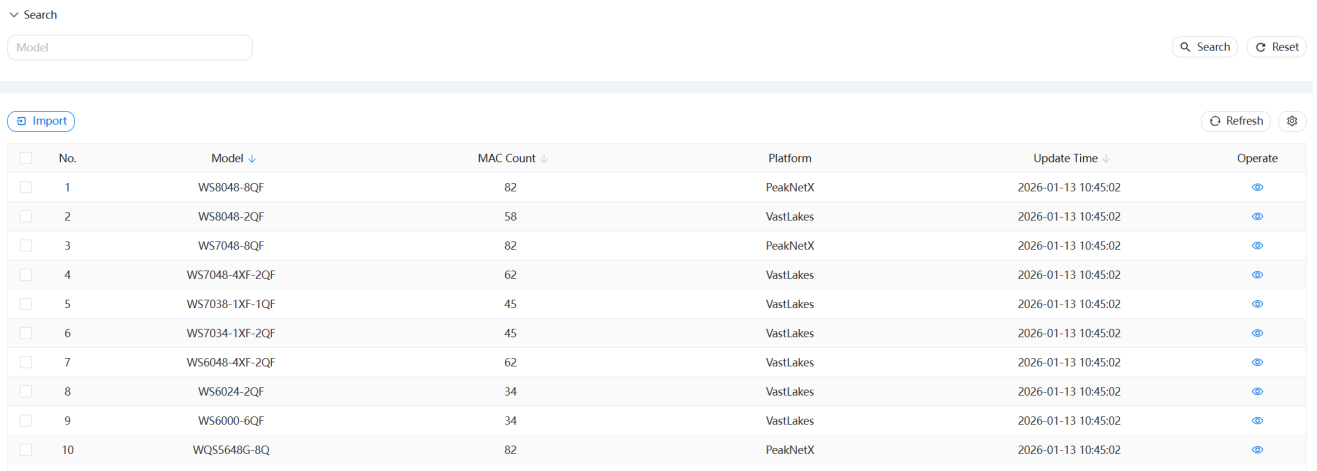
▲*Figure 48 License Application Flowchart*

- Get ServerID
  Users can obtain the fingerprint information of the current running environment via the "Get ServerID" button on the cloud platform.
- Apply for License
  Submit the ServerID and the number of devices for which you are applying to purchase access licenses to the manufacturer to apply for a License.
- Import License
  Import the applied License in the License module. The total number of devices that can be accessed will be displayed on the interface.

> **Note**
> If the cloud platform is reinstalled, the obtained ServerID will change, and you cannot use the old ServerID to apply for a License again.

4.5. Product Models

Product Models refer to the models and key hardware information of manageable devices. They are the platform's foundational data. If this information is missing or certain model information is absent, some functions may not work properly. If this happens, please contact the supplier. After obtaining the relevant data files, import them.



No.	Model	MAC Count	Platform	Update Time	Operate
1	WS8048-8QF	82	PeakNetX	2026-01-13 10:45:02	
2	WS8048-2QF	58	VastLakes	2026-01-13 10:45:02	
3	WS7048-8QF	82	PeakNetX	2026-01-13 10:45:02	
4	WS7048-4XF-2QF	62	VastLakes	2026-01-13 10:45:02	
5	WS7038-1XF-1QF	45	VastLakes	2026-01-13 10:45:02	
6	WS7034-1XF-2QF	45	VastLakes	2026-01-13 10:45:02	
7	WS6048-4XF-2QF	62	VastLakes	2026-01-13 10:45:02	
8	WS6024-2QF	34	VastLakes	2026-01-13 10:45:02	
9	WS6000-6QF	34	VastLakes	2026-01-13 10:45:02	
10	WQS5648G-8Q	82	PeakNetX	2026-01-13 10:45:02	

▲*Figure 49 Product Model Management Page*