DHCS Quick Start Guide (Private Mode)

DHCS Quick Start Guide (Private)

release v1.0.0

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. All data and resources are isolated and managed within the tenant.
Platform Administrator	The administrator is primarily responsible for configuring system runtime parameters to ensure the platform operates normally, including the platform license, platform name, IP, operating mode, etc.
Technical Support	Technical support is responsible for assisting tenants in resolving cloud management issues. By default, they have only business menu permissions but no data permissions. When a user grants technical support access to a specific network, they can view and operate devices within that network.
Regular User	Created by the platform administrator, regular users are granted default permissions to use the platform.
Network	A logical project created by a tenant on the DHCS platform for dividing and managing their exclusive network resources. A tenant can create multiple networks, representing different internal subnets or branch office networks.
Private Mode	The entire platform operates under a single private organization. All resources, data, and users are centrally managed within this organization. Suitable for internal network operation and maintenance scenarios of a single management entity.
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 for multiple customers or departments on the same platform.

▲*Table 1: Basic Concepts*

2. Quick Start Preparation

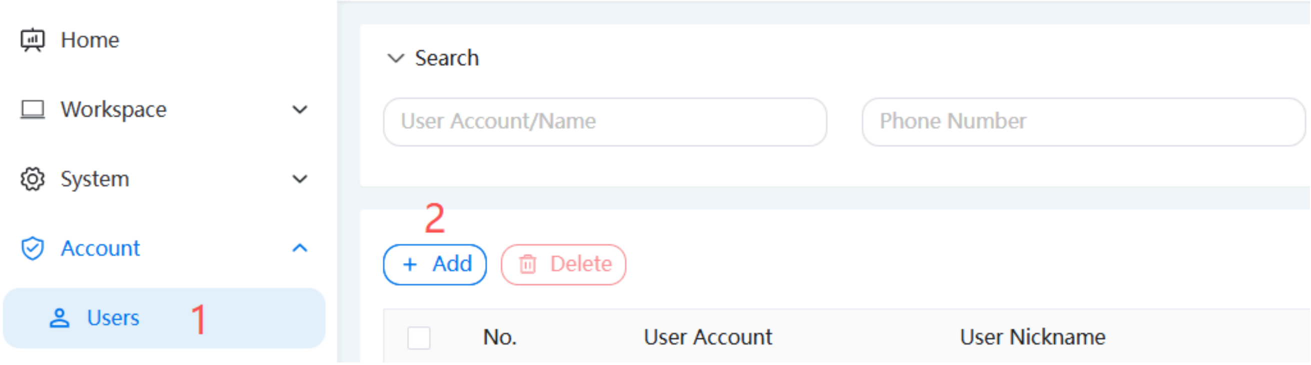
2.1. Preparation Checklist

Preparation Item	Requirement	Remarks
Cloud Platform	Installation completed, email service configured	If the cloud platform is installed on an internal network, ensure the mail server can send emails to target addresses.
Regular User Account	Regular user added	Ensure permissions like "Network Creation", "Device Management" are granted.
Platform Administrator Account		superadmin account
Test Device	An operational device	Network configured.
Network Planning	Device must be able to access the cloud platform service address	Ensure no firewall blockage between the device and the cloud platform.

▲Table 2: Preparation Checklist

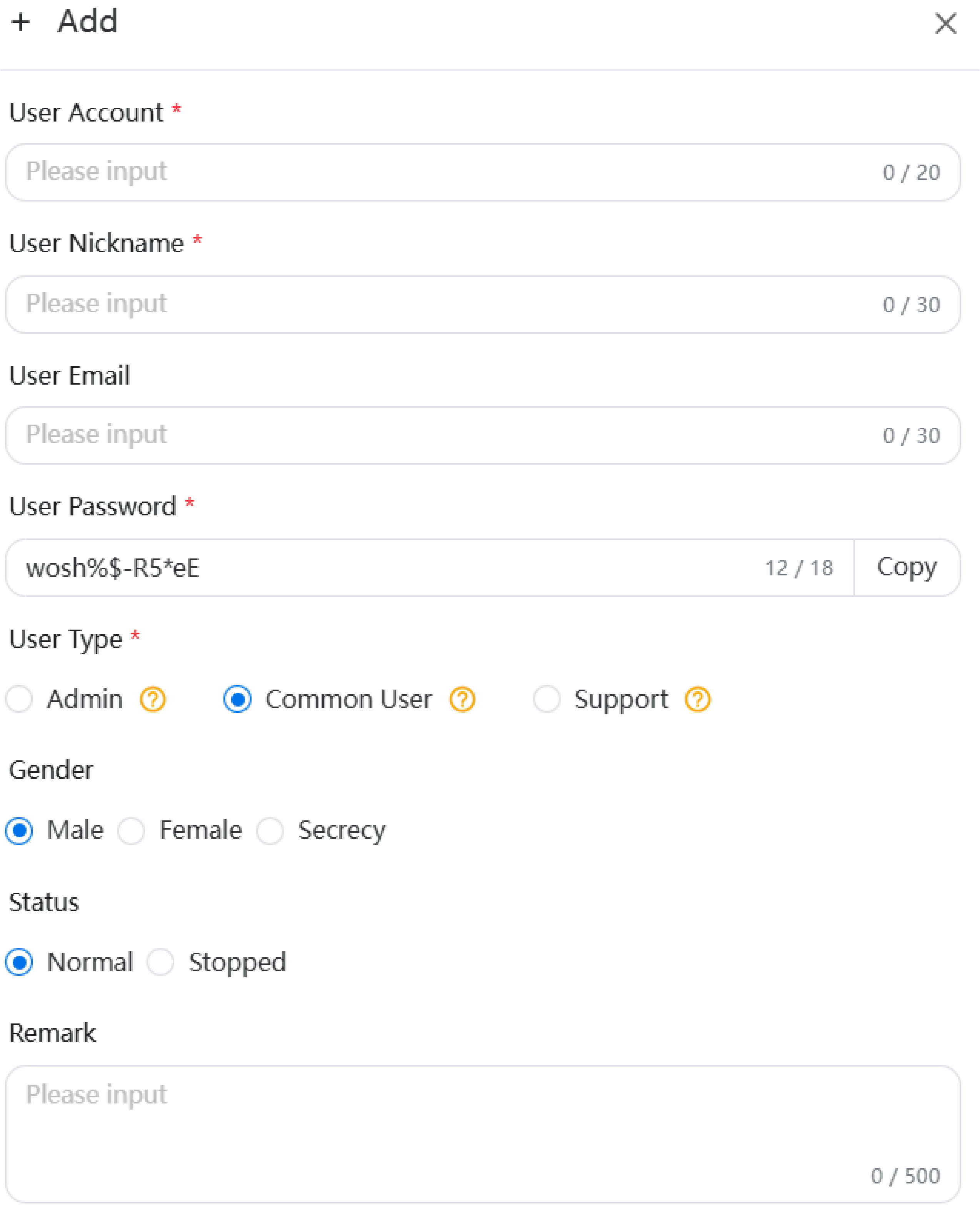
2.2. Adding a Regular User

Add a regular user to be responsible for the daily maintenance of the network. Click "Account Permissions -> User Management" to enter the user management page, then click the "Add" button.



▲Figure 1: User Management Page

Fill in the new user information in the pop-up page. Here we select "User Type" as "Regular User". The default "Regular User" has all permissions for network management, Then click "Confirm" to submit.



+ Add ×

User Account *

Please input 0 / 20

User Nickname *

Please input 0 / 30

User Email

Please input 0 / 30

User Password *

wosh%$-R5*eE 12 / 18 Copy

User Type *

○ Admin ● Common User ○ Support

Gender

● Male ○ Female ○ Secrecy

Status

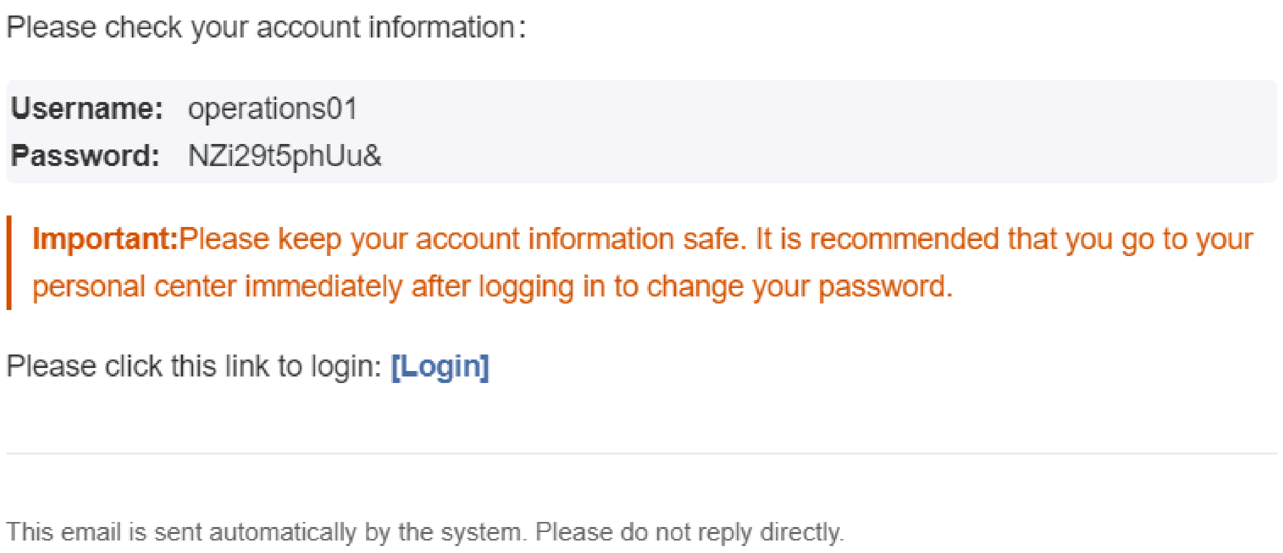
● Normal ○ Stopped

Remark

Please input 0 / 500

▲*Figure 2: Add User Information Page*

After successfully adding the user, the registered email will receive an automatically generated email from the system. 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]**

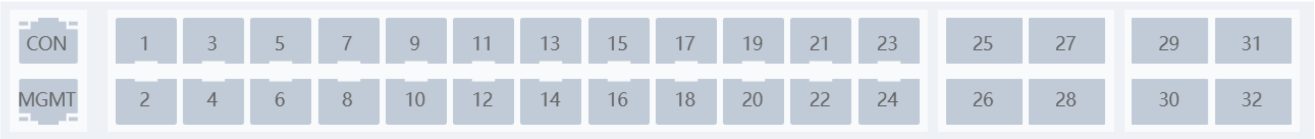
This email is sent automatically by the system. Please do not reply directly.

▲Email notification

2.3. Device-Side Preparation

2.3.1. Introduction to Managed Ports

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.

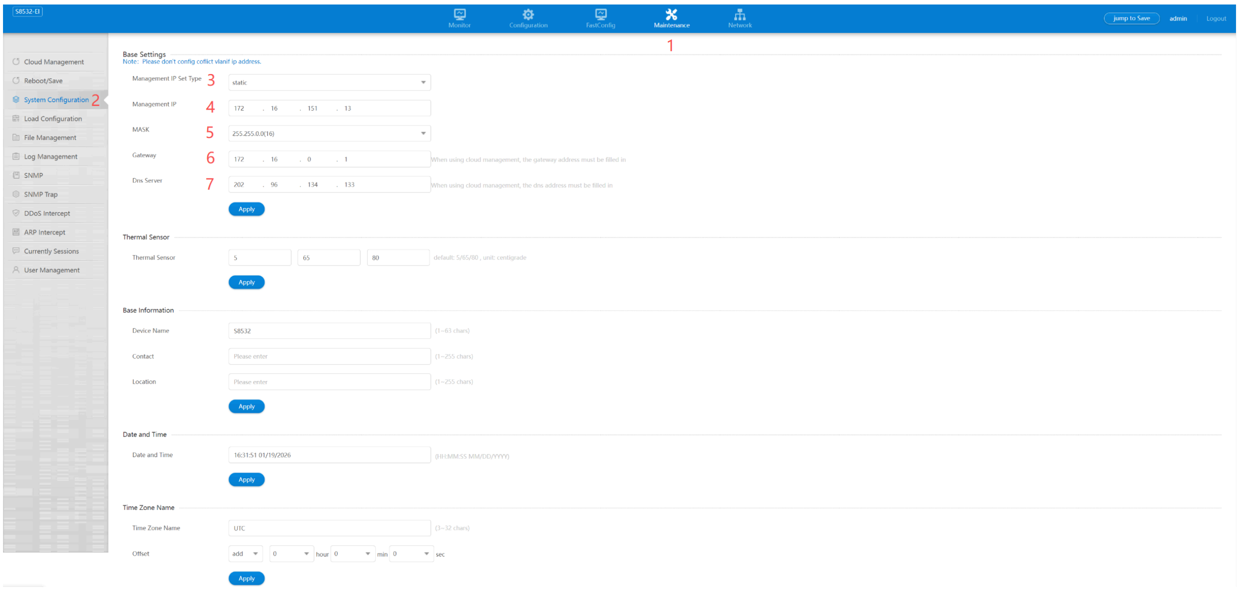


▲Figure 3: Device Port Diagram

2.3.2. Device IP Configuration

Devices can be connected to the management network via MGMT and VLAN1. The corresponding IP address descriptions are as follows:

- **MGMT Connection**: The default IP is 192.168.1.1. If the default IP is not accessible to DHCS, set the IP manually. Users can login to the device WEB and modify the Management IP, Gateway, etc., as needed in the system configuration. As shown:



Base Settings
Note: Please don't config coflict vlanif ip address.

Management IP Set Type: static
Management IP: 172 . 16 . 151 . 13
MASK: 255.255.0.0(16)
Gateway: 172 . 16 . 0 . 1 When using cloud management, the gateway address must be filled in
Dns Server: 202 . 96 . 134 . 133 When using cloud management, the dns address must be filled in

Thermal Sensor
Thermal Sensor: 5 65 80 default: 5/65/80 , unit: centigrade

Base Information
Device Name: S8532 (1~63 chars)
Contact: Please enter (1~255 chars)
Location: Please enter (1~255 chars)

Date and Time
Date and Time: 16:31:51 01/19/2026 (HH:MM:SS MM/DD/YYYY)

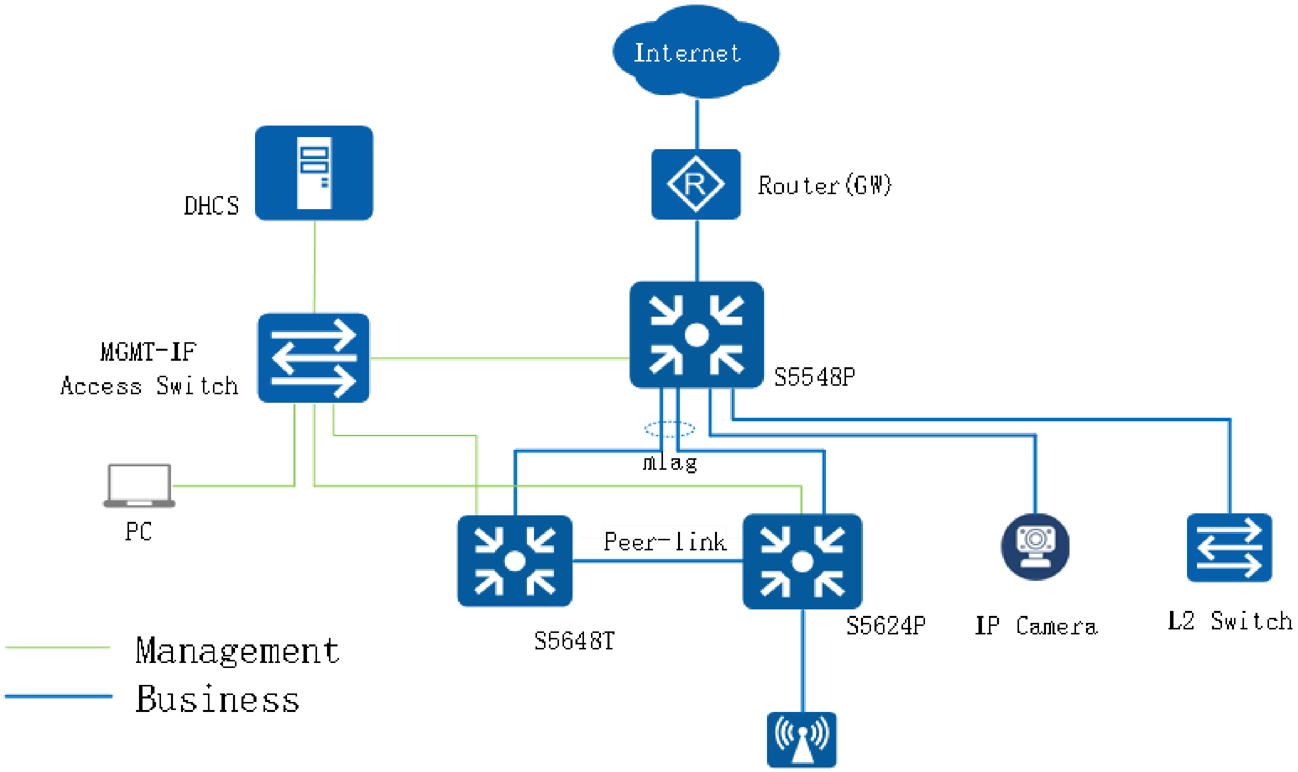
Time Zone Name
Time Zone Name: UTC (3~32 chars)
Offset: add 0 hour 0 min 0 sec

▲*Figure 4: Device Management IP Configuration Page*

- **VLAN1 Connection**: The device has DHCP enabled by default out of the factory. It 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 uses a private cloud server for centralized management of devices within the network. Each switch connects via an out-of-band management port (mgmt-if) to a dedicated switch, which then communicates with the DHCP server. The cloud platform is deployed in a private mode on the internal network for unified network management and operation. As shown:



▲*Figure 5: Network Planning Topology Diagram*

New users can login to the DHCS cloud platform using the username and password provided in the email.

3. Device Operation and Maintenance (Regular User)

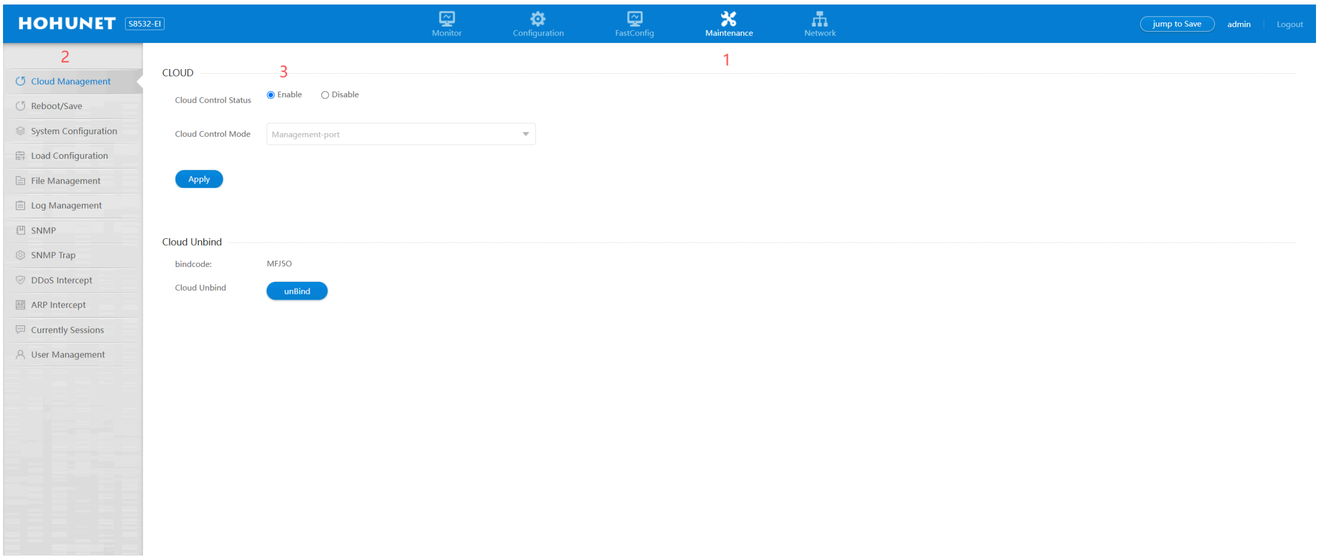
3.1. Onboarding the First Device

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".



CLOUD

Cloud Control Status ● Enable ○ Disable

Cloud Control Mode Management-port

Cloud Unbind

bindcode: MFJ5O

Cloud Unbind

▲*Figure 6: 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.

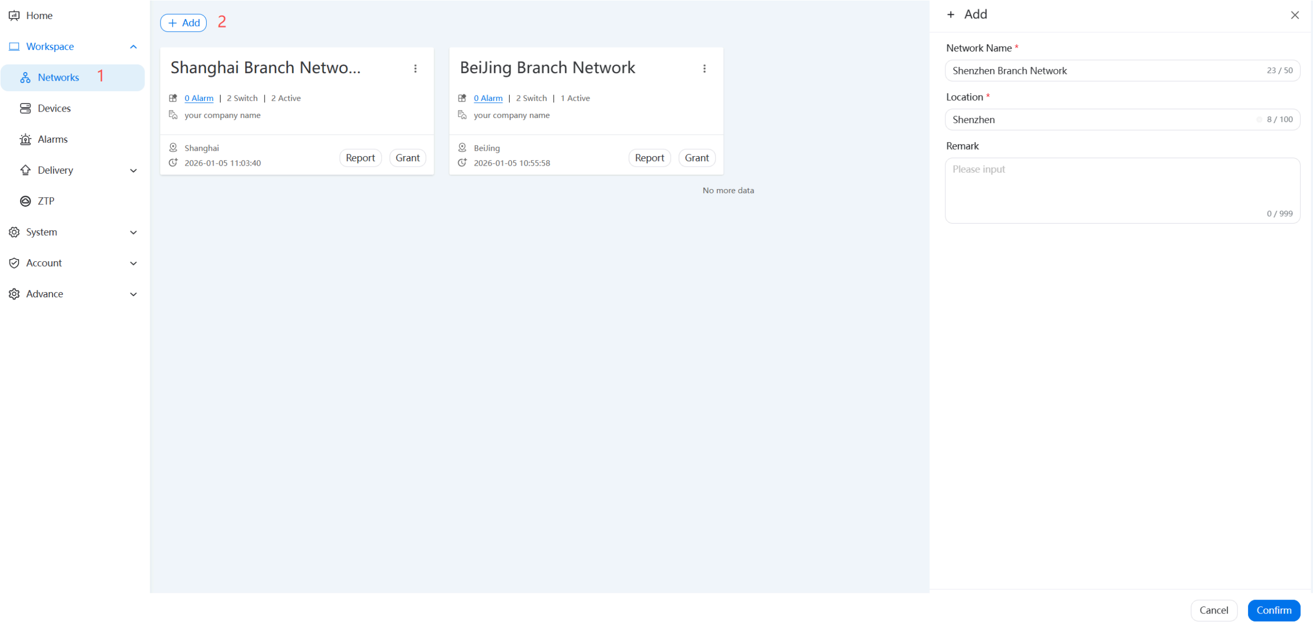
- Obtaining the Binding Code via CLI Command
  Login to the device, enter the command `show cloud-management state` to view it.

```
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:



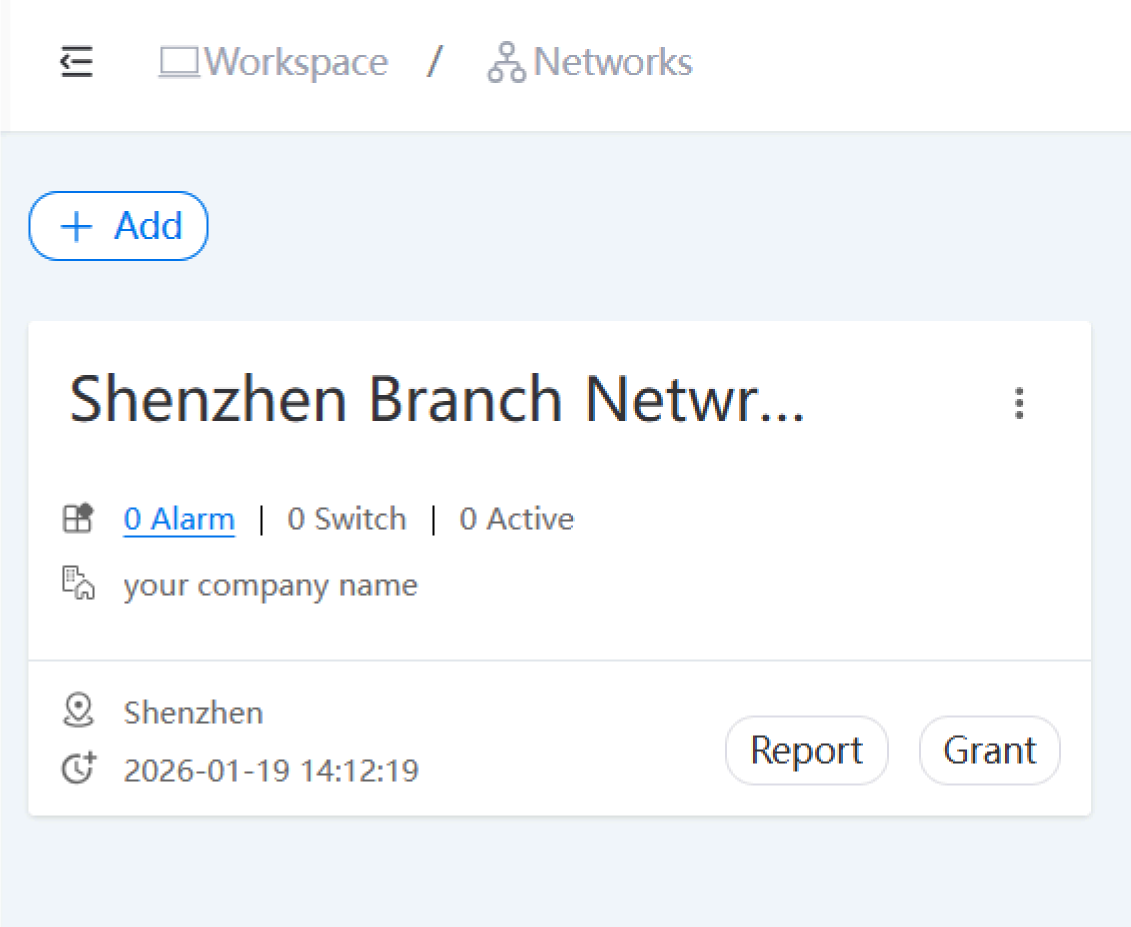
Shanghai Branch Netwo...
0 Alarm | 2 Switch | 2 Active
your company name
Shanghai
2026-01-05 11:03:40

BeiJing Branch Network
0 Alarm | 2 Switch | 1 Active
your company name
BeiJing
2026-01-05 10:55:58

Network Name *: Shenzhen Branch Network 23 / 50
Location *: Shenzhen 8 / 100
Remark: Please input 0 / 999

▲*Figure 7: 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.



Shenzhen Branch Netwr...

0 Alarm | 0 Switch | 0 Active

your company name

Shenzhen

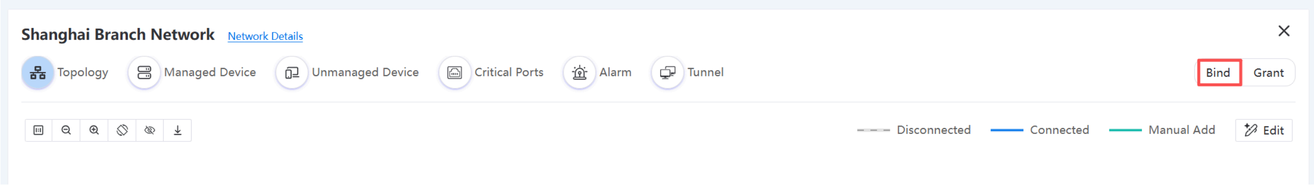
2026-01-19 14:12:19

▲Figure 8: Created Network List Page

3.1.4. Cloud Platform Binding

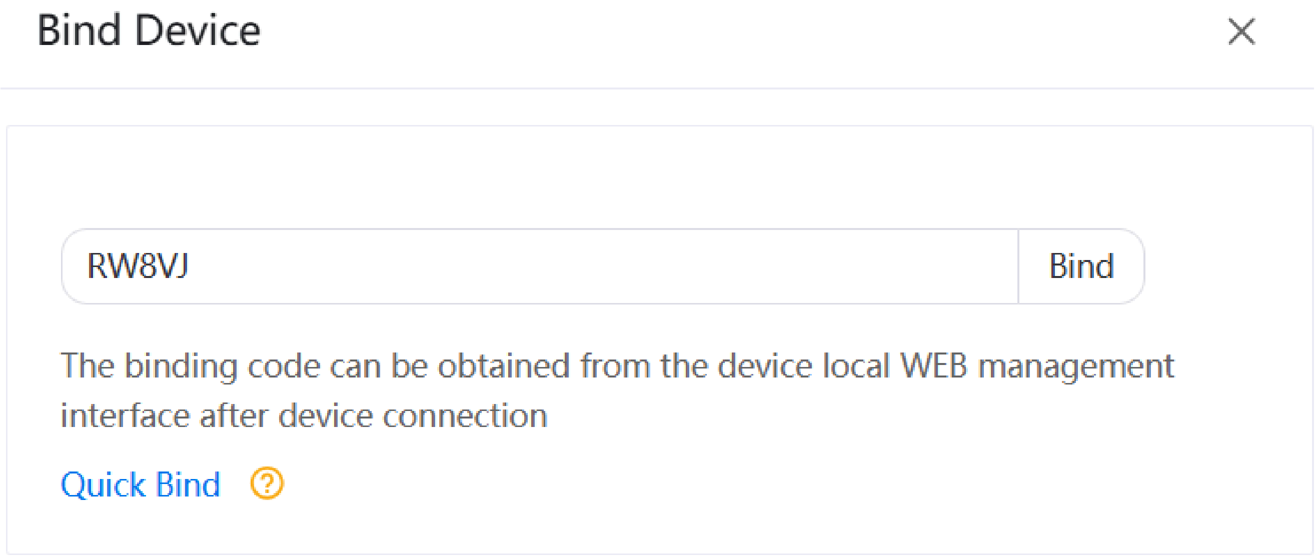
- **Bind via Binding Code**

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 9: 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).



Bind Device

RW8VJ

The binding code can be obtained from the device local WEB management interface after device connection

▲*Figure 10: Input 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.

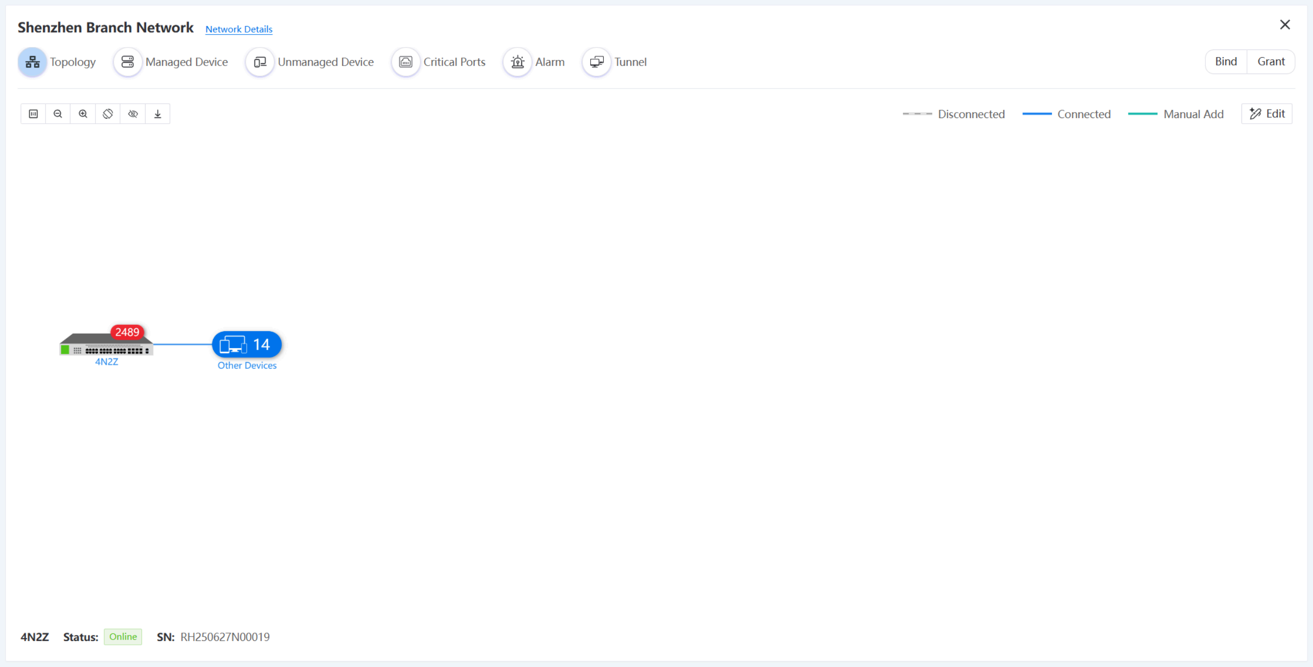
Thus, device onboarding is complete. DHCS also supports onboarding via ZTP, CLI, DHCP auto-discovery protocol, and other methods. Please refer to the DHCS user manual for details.

3.1.5. How to Confirm Successful Onboarding

After device binding, you can confirm whether onboarding was successful using any of the following methods:

- **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.

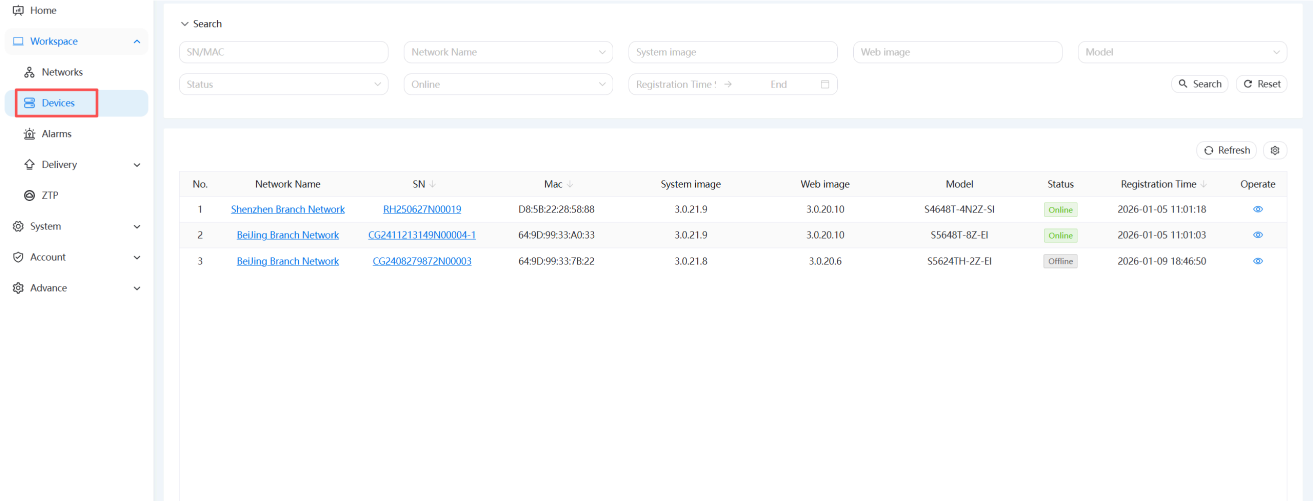


4N2Z Status: Online SN: RH250627N00019

▲*Figure 11: 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.

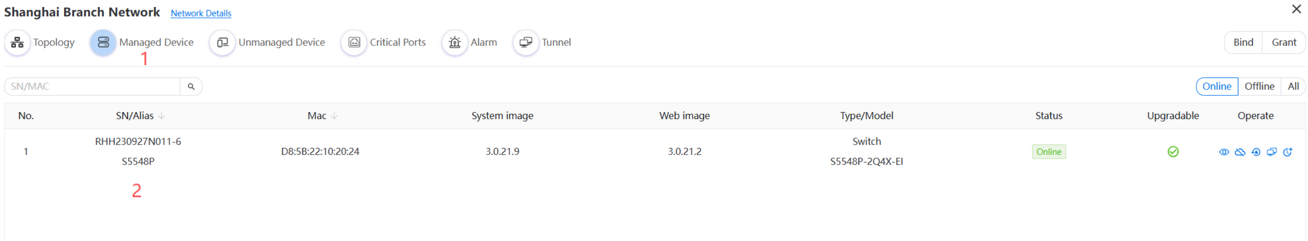


No.	Network Name	SN	Mac	System image	Web image	Model	Status	Registration Time	Operate
1	Shenzhen Branch Network	RH250627N00019	D8:5B:22:28:58:88	3.0.21.9	3.0.20.10	S4648T-4N2Z-SI	Online	2026-01-05 11:01:18	👁
2	BeiJing Branch Network	CG2411213149N00004-1	64:9D:99:33:A0:33	3.0.21.9	3.0.20.10	S5648T-8Z-EI	Online	2026-01-05 11:01:03	👁
3	BeiJing Branch Network	CG2408279872N00003	64:9D:99:33:7B:22	3.0.21.8	3.0.20.6	S5624TH-2Z-EI	Offline	2026-01-09 18:46:50	👁

▲*Figure 12: Device Management Page Showing 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:



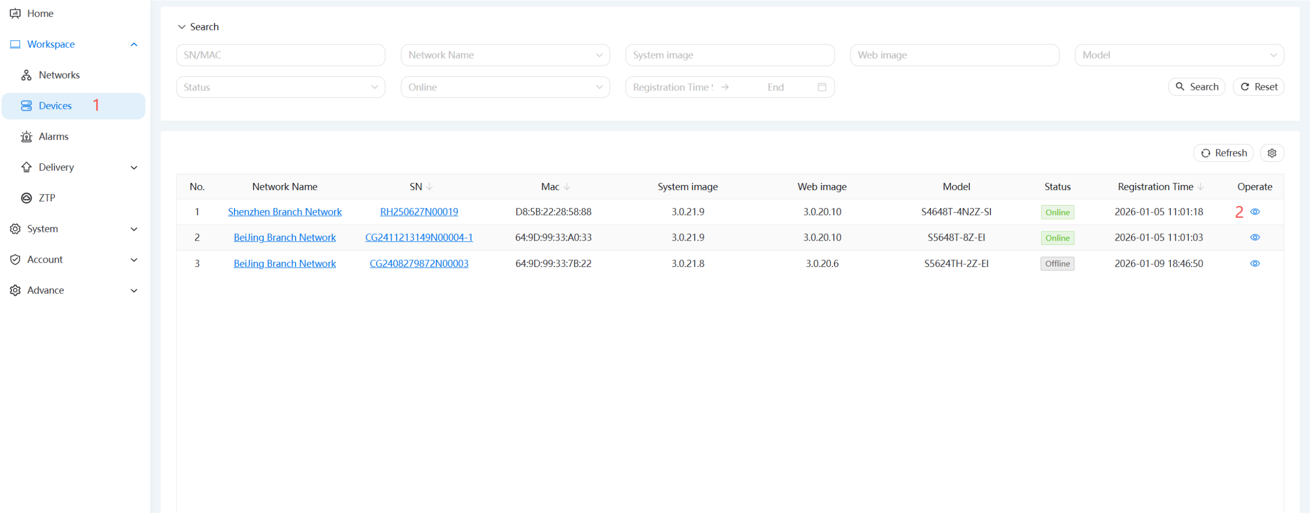
No.	SN/Alias	Mac	System image	Web image	Type/Model	Status	Upgradable	Operate
1	RHH230927N011-6 S5548P	D8:5B:22:10:20:24	3.0.21.9	3.0.21.2	Switch S5548P-2Q4X-EI	Online	✓	

▲*Figure 13: Cloud-Managed Device List within a Network*

3.2. Device Management

3.2.1. Device Overview

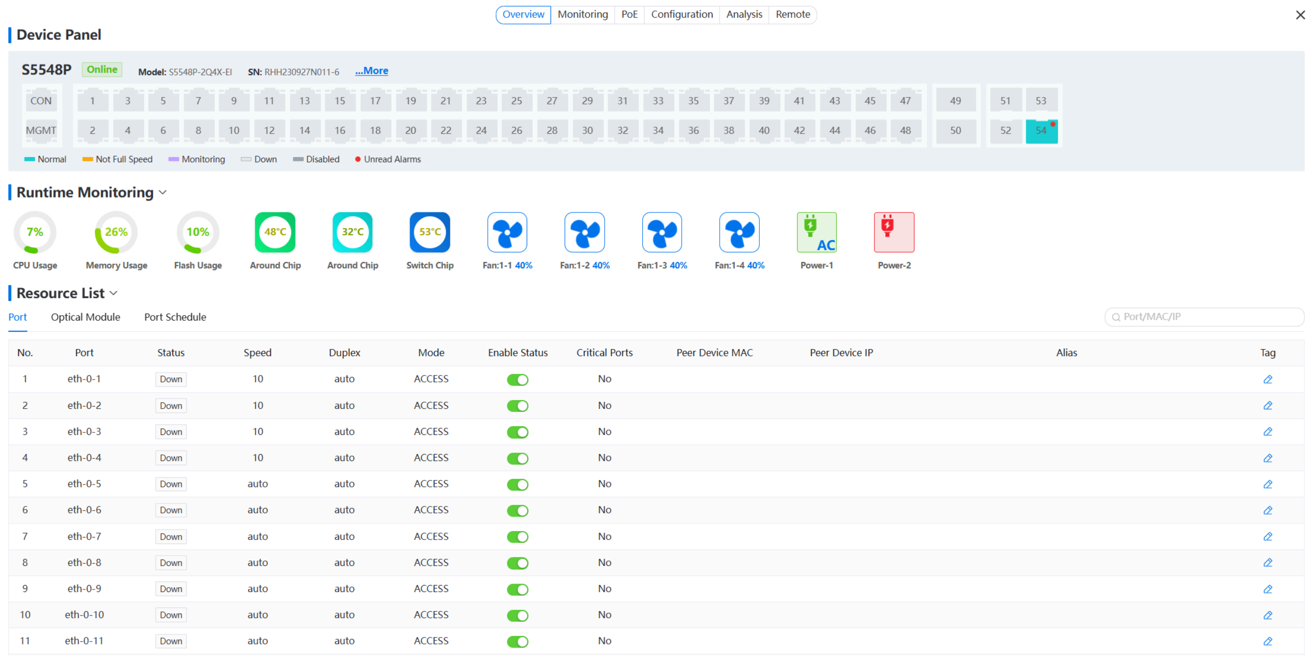
Go to Workspace -> Networks -> Cloud-Managed Devices or Workspace -> Device Management to view managed devices. Click the "View" button in the operation column to enter the device details page.



No.	Network Name	SN	Mac	System image	Web image	Model	Status	Registration Time	Operate
1	Shenzhen Branch Network	RH250627N00019	D8:5B:22:28:58:88	3.0.21.9	3.0.20.10	S4648T-4N2Z-SI	Online	2026-01-05 11:01:18	
2	BeiJing Branch Network	CG2411213149N00004-1	64:9D:99:33:A0:33	3.0.21.9	3.0.20.10	S5648T-8Z-EI	Online	2026-01-05 11:01:03	
3	BeiJing Branch Network	CG2408279872N00003	64:9D:99:33:7B:22	3.0.21.8	3.0.20.6	S5624TH-2Z-EI	Offline	2026-01-09 18:46:50	

▲*Figure 14: View Button in Device List Operation Column*

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



Device Panel

S5548P Online Model: S5548P-2Q4X-EI SN: RHH230927N011-6 ...More

🟦 Normal 🟧 Not Full Speed 🟪 Monitoring ⬜ Down ⬛ Disabled 🔴 Unread Alarms

Runtime Monitoring

7% CPU Usage
26% Memory Usage
10% Flash Usage
48°C Around Chip
32°C Around Chip
53°C Switch Chip
Fan:1-1 40%
Fan:1-2 40%
Fan:1-3 40%
Fan:1-4 40%
Power-1
Power-2

Resource List

Port Optical Module Port Schedule

No.	Port	Status	Speed	Duplex	Mode	Enable Status	Critical Ports	Peer Device MAC	Peer Device IP	Alias	Tag
1	eth-0-1	Down	10	auto	ACCESS	●	No				✎
2	eth-0-2	Down	10	auto	ACCESS	●	No				✎
3	eth-0-3	Down	10	auto	ACCESS	●	No				✎
4	eth-0-4	Down	10	auto	ACCESS	●	No				✎
5	eth-0-5	Down	auto	auto	ACCESS	●	No				✎
6	eth-0-6	Down	auto	auto	ACCESS	●	No				✎
7	eth-0-7	Down	auto	auto	ACCESS	●	No				✎
8	eth-0-8	Down	auto	auto	ACCESS	●	No				✎
9	eth-0-9	Down	auto	auto	ACCESS	●	No				✎
10	eth-0-10	Down	auto	auto	ACCESS	●	No				✎
11	eth-0-11	Down	auto	auto	ACCESS	●	No				✎

▲*Figure 15: 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 Explanation*

> **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	CON	Serial Port
2	MGMT	Management Port

▲*Table 4: Serial and Management Port Legend*

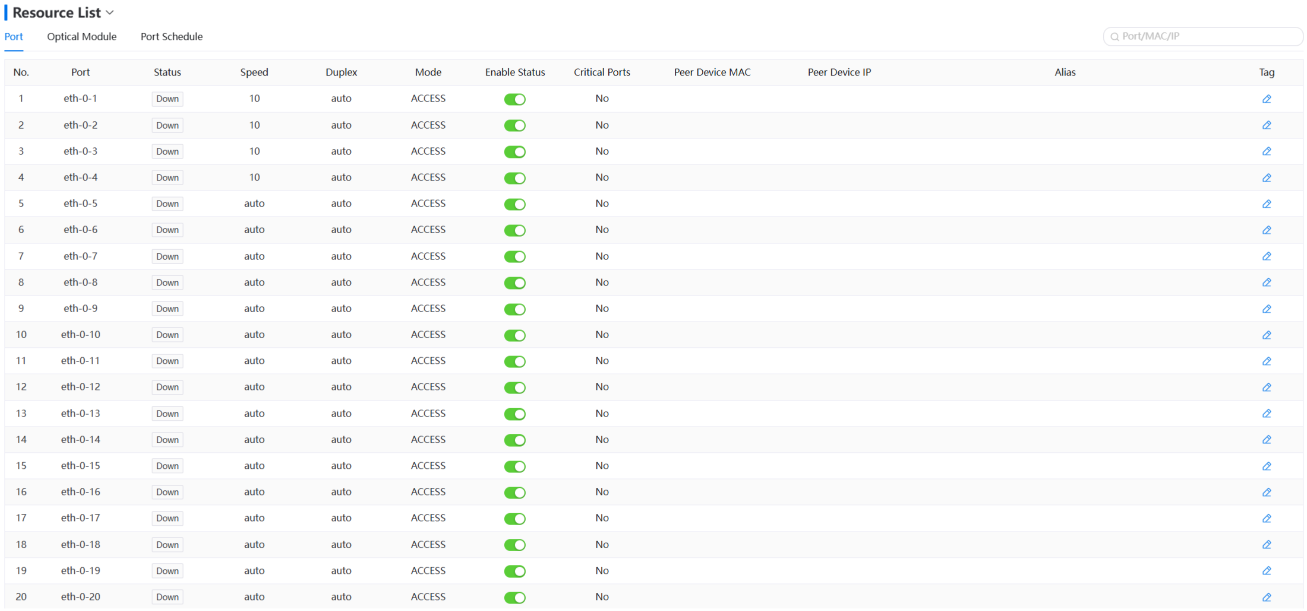
- **Running Monitoring**

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:



Resource List ⌄

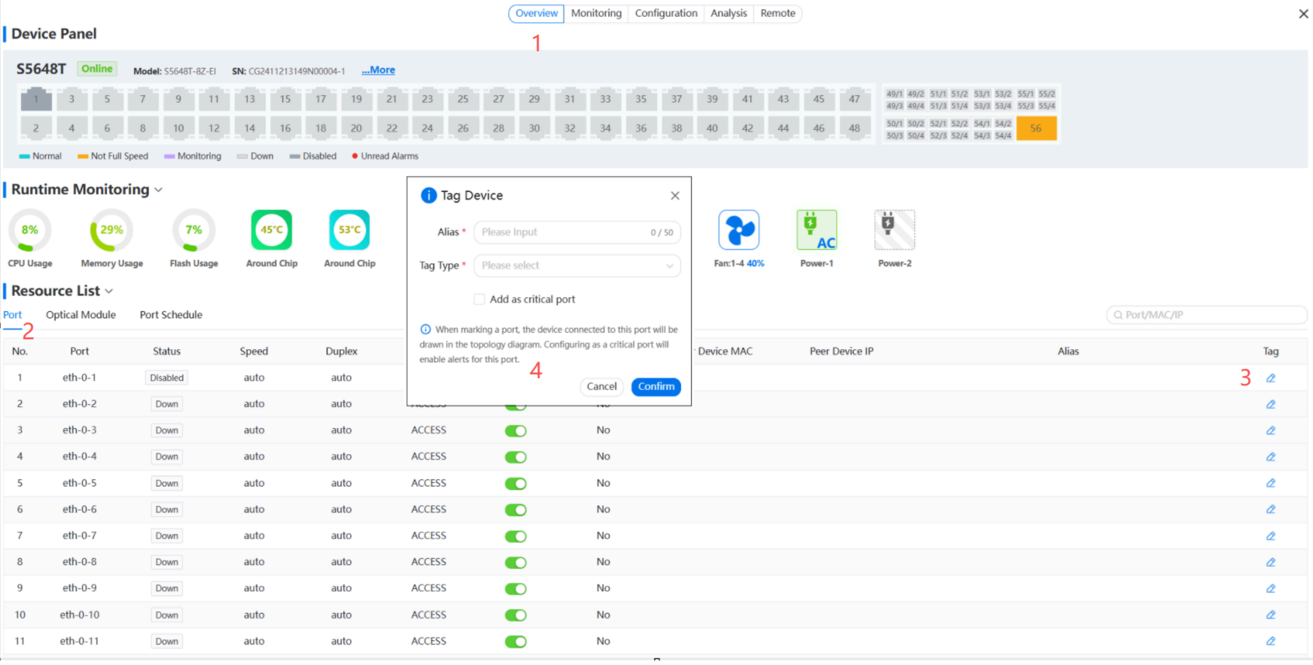
Port | Optical Module | Port Schedule | Port/MAC/IP

No.	Port	Status	Speed	Duplex	Mode	Enable Status	Critical Ports	Peer Device MAC	Peer Device IP	Alias	Tag
1	eth-0-1	Down	10	auto	ACCESS	●	No				✎
2	eth-0-2	Down	10	auto	ACCESS	●	No				✎
3	eth-0-3	Down	10	auto	ACCESS	●	No				✎
4	eth-0-4	Down	10	auto	ACCESS	●	No				✎
5	eth-0-5	Down	auto	auto	ACCESS	●	No				✎
6	eth-0-6	Down	auto	auto	ACCESS	●	No				✎
7	eth-0-7	Down	auto	auto	ACCESS	●	No				✎
8	eth-0-8	Down	auto	auto	ACCESS	●	No				✎
9	eth-0-9	Down	auto	auto	ACCESS	●	No				✎
10	eth-0-10	Down	auto	auto	ACCESS	●	No				✎
11	eth-0-11	Down	auto	auto	ACCESS	●	No				✎
12	eth-0-12	Down	auto	auto	ACCESS	●	No				✎
13	eth-0-13	Down	auto	auto	ACCESS	●	No				✎
14	eth-0-14	Down	auto	auto	ACCESS	●	No				✎
15	eth-0-15	Down	auto	auto	ACCESS	●	No				✎
16	eth-0-16	Down	auto	auto	ACCESS	●	No				✎
17	eth-0-17	Down	auto	auto	ACCESS	●	No				✎
18	eth-0-18	Down	auto	auto	ACCESS	●	No				✎
19	eth-0-19	Down	auto	auto	ACCESS	●	No				✎
20	eth-0-20	Down	auto	auto	ACCESS	●	No				✎

▲*Figure 16: 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.



Device Panel

S5648T Online Model: S5648T-8Z-EI SN: CG2411213149N00004-1 ...More

Runtime Monitoring ⌄

Tag Device

Alias * Please Input 0 / 50

Tag Type * Please select

□ Add as critical port

When marking a port, the device connected to this port will be drawn in the topology diagram. Configuring as a critical port will enable alerts for this port.

Cancel | Confirm

Resource List ⌄

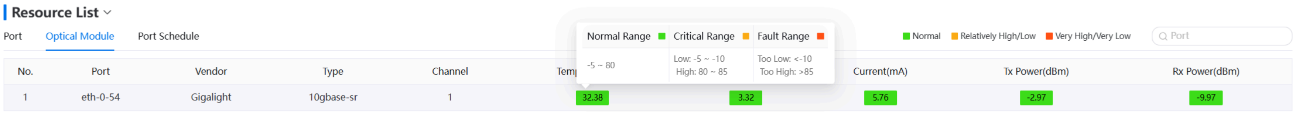
Port | Optical Module | Port Schedule | Port/MAC/IP

No.	Port	Status	Speed	Duplex				Device MAC	Peer Device IP	Alias	Tag
1	eth-0-1	Disabled	auto	auto							✎
2	eth-0-2	Down	auto	auto							✎
3	eth-0-3	Down	auto	auto	ACCESS	●	No				✎
4	eth-0-4	Down	auto	auto	ACCESS	●	No				✎
5	eth-0-5	Down	auto	auto	ACCESS	●	No				✎
6	eth-0-6	Down	auto	auto	ACCESS	●	No				✎
7	eth-0-7	Down	auto	auto	ACCESS	●	No				✎
8	eth-0-8	Down	auto	auto	ACCESS	●	No				✎
9	eth-0-9	Down	auto	auto	ACCESS	●	No				✎
10	eth-0-10	Down	auto	auto	ACCESS	●	No				✎
11	eth-0-11	Down	auto	auto	ACCESS	●	No				✎

▲*Figure 17: 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:



Resource List ⌄

Port | Optical Module | Port Schedule

🟩 Normal 🟧 Relatively High/Low 🟥 Very High/Very Low

Port

Normal Range 🟩	Critical Range 🟧	Fault Range 🟥
-5 ~ 80	Low: -5 ~ -10 High: 80 ~ 85	Too Low: <-10 Too High: >85

No.	Port	Vendor	Type	Channel	Temp		Current(mA)	Tx Power(dBm)	Rx Power(dBm)
1	eth-0-54	Gigalight	10gbase-sr	1	32.38	3.32	5.76	-2.97	-9.97

▲*Figure 18: Optical Module List and Metric Display*

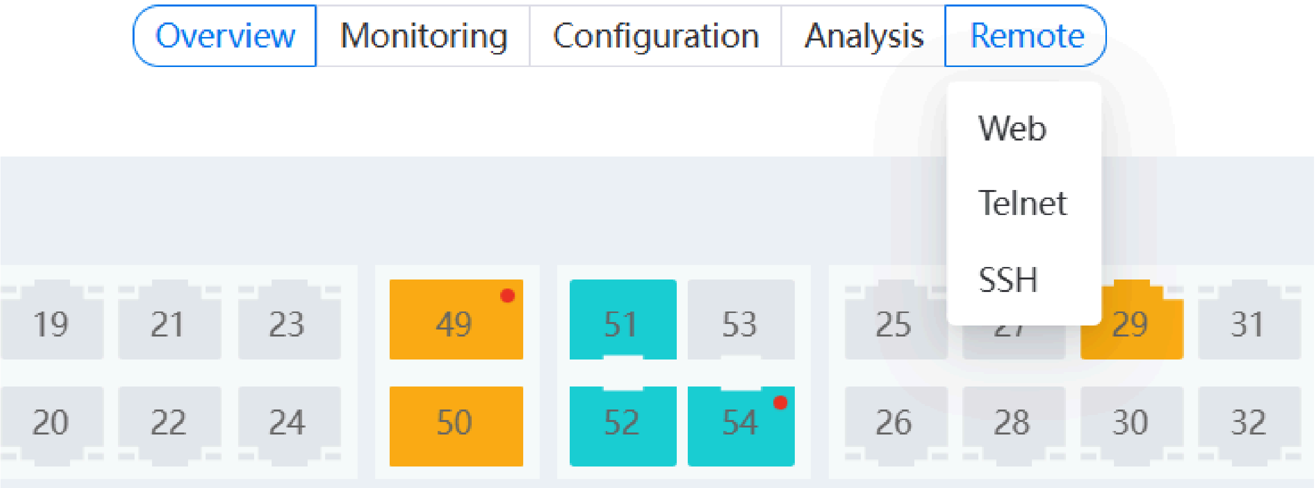
Hovering the mouse over a specific metric shows its corresponding range. The platform uses green, orange, and red to indicate the status of operational metrics. The specific meanings are as follows:

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

▲*Table 5: Optical Module Metric Color Explanation*

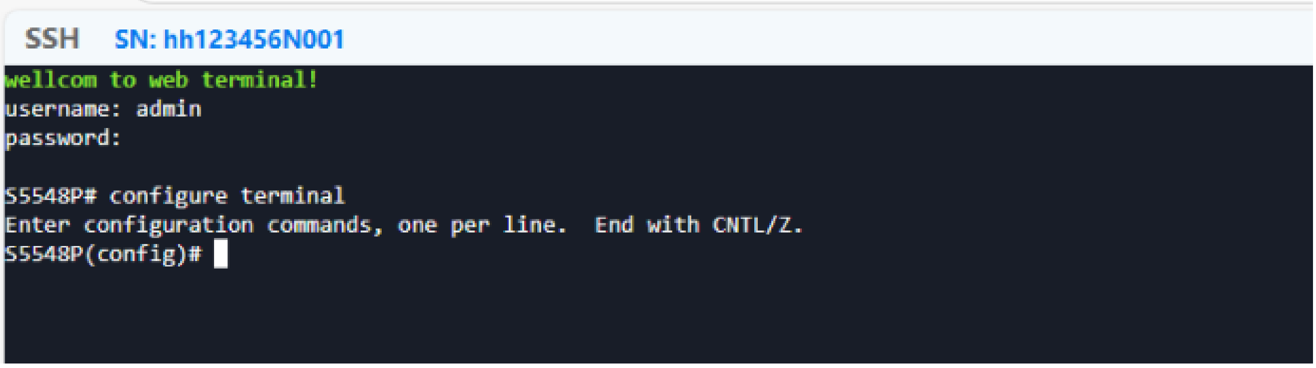
3.2.2. Remote Maintenance

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 19: Remote O&M Service Type Selection*

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

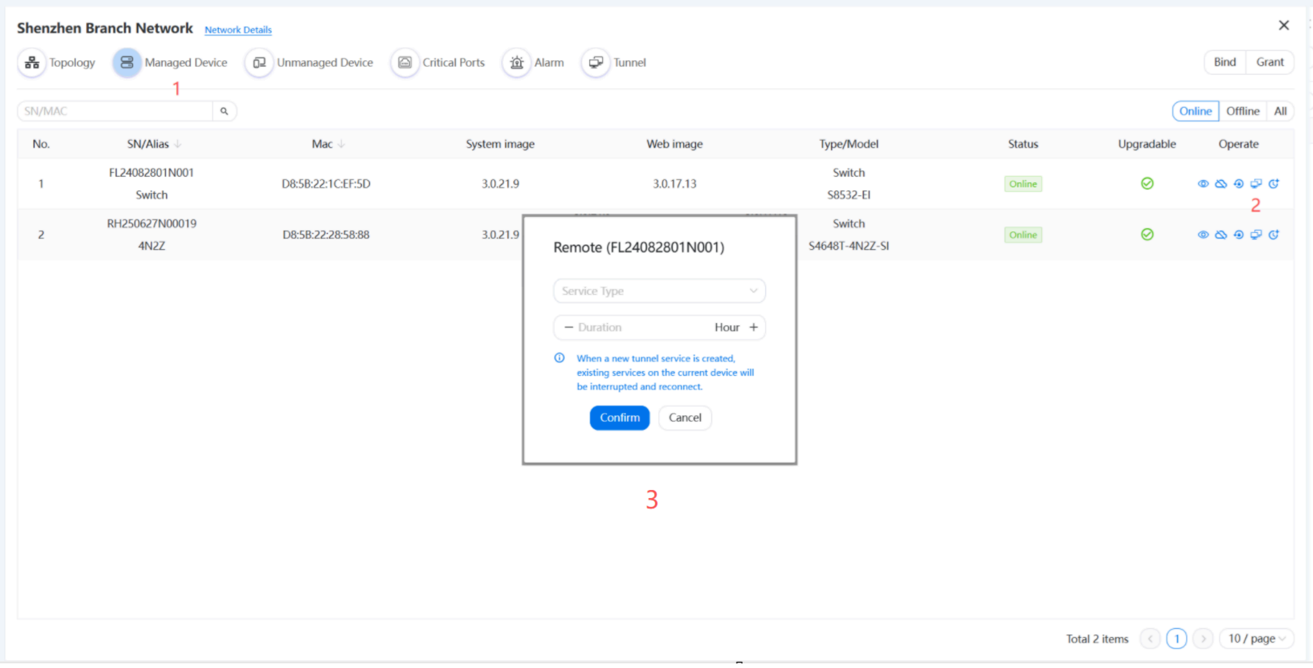


SSH SN: hh123456N001

```
wellcom to web terminal!
username: admin
password:

S5548P# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S5548P(config)# 
```

▲*Figure 20: SSH Tunnel Interface*

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.



No.	SN/Alias	Mac	System image	Web image	Type/Model	Status	Upgradable	Operate
1	FL24082801N001 Switch	D8:5B:22:1C:EF:5D	3.0.21.9	3.0.17.13	Switch S8532-EI	Online	✓	
2	RH250627N00019 4N2Z	D8:5B:22:28:58:88	3.0.21.9		Switch S4648T-4N2Z-SI	Online	✓	

Remote (FL24082801N001)

Service Type

− Duration Hour +

When a new tunnel service is created, existing services on the current device will be interrupted and reconnect.

Confirm Cancel

▲*Figure 21: 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.

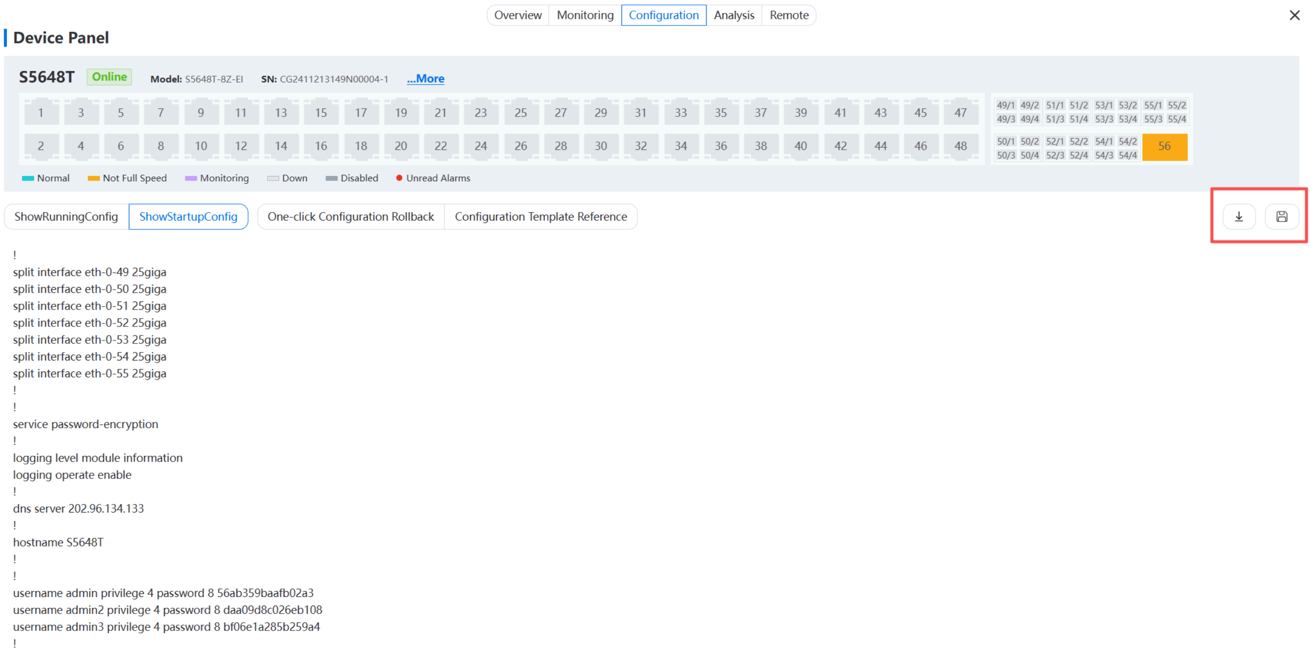
3.2.3. Configuration Management

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.

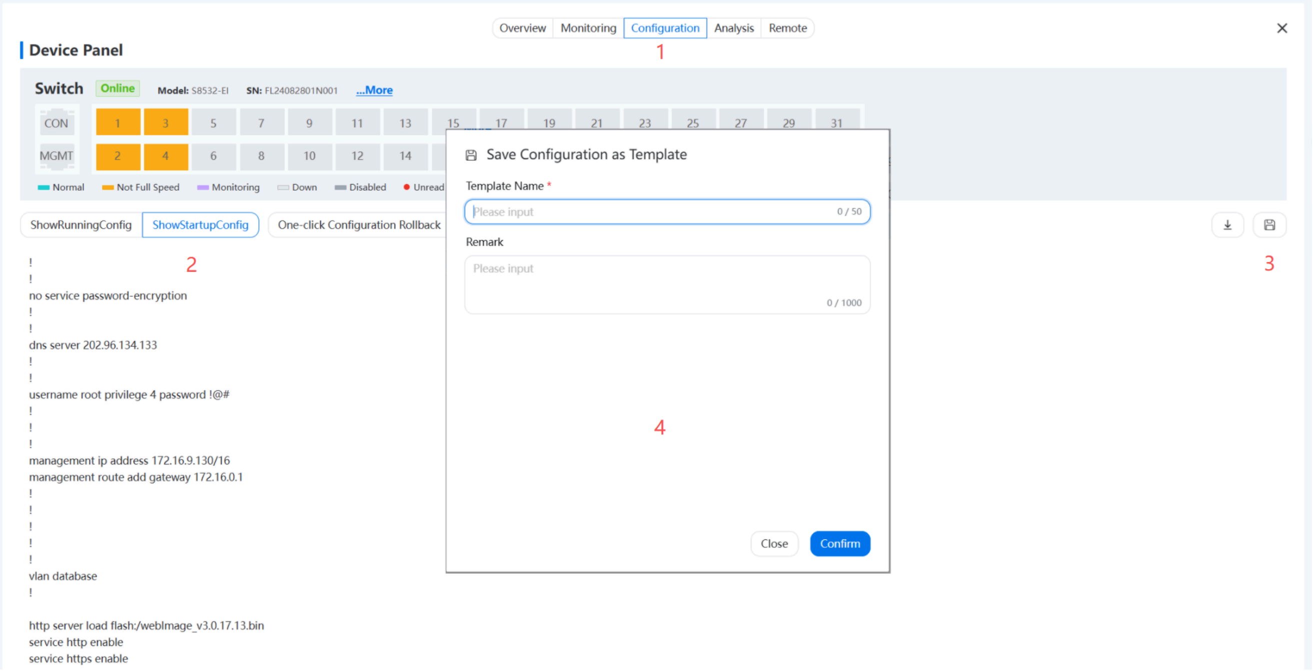


```
!
split interface eth-0-49 25giga
split interface eth-0-50 25giga
split interface eth-0-51 25giga
split interface eth-0-52 25giga
split interface eth-0-53 25giga
split interface eth-0-54 25giga
split interface eth-0-55 25giga
!
!
service password-encryption
!
logging level module information
logging operate enable
!
dns server 202.96.134.133
!
hostname S5648T
!
!
username admin privilege 4 password 8 56ab359baafb02a3
username admin2 privilege 4 password 8 daa09d8c026eb108
username admin3 privilege 4 password 8 bf06e1a285b259a4
!
```

▲*Figure 22: 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:



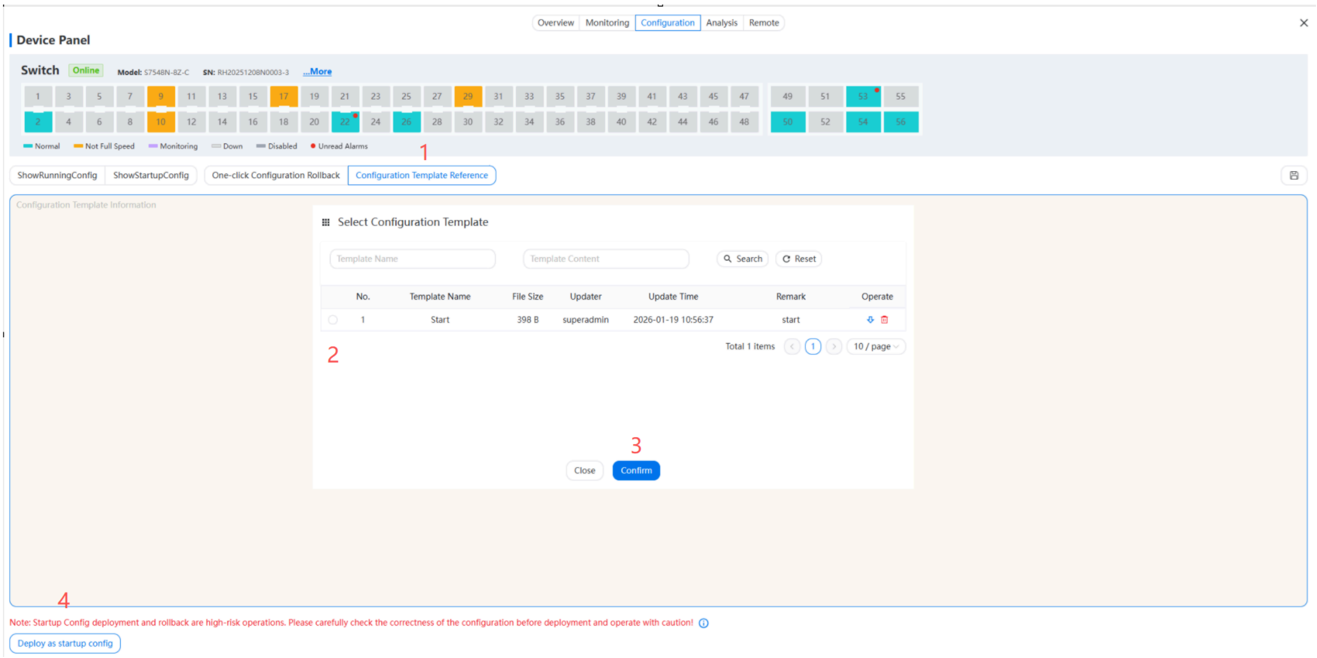
```
!
!
no service password-encryption
!
!
dns server 202.96.134.133
!
!
username root privilege 4 password !@#
!
!
!
management ip address 172.16.9.130/16
management route add gateway 172.16.0.1
!
!
!
!
!
vlan database
!

http server load flash:/webImage_v3.0.17.13.bin
service http enable
service https enable
```

▲*Figure 23: 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:



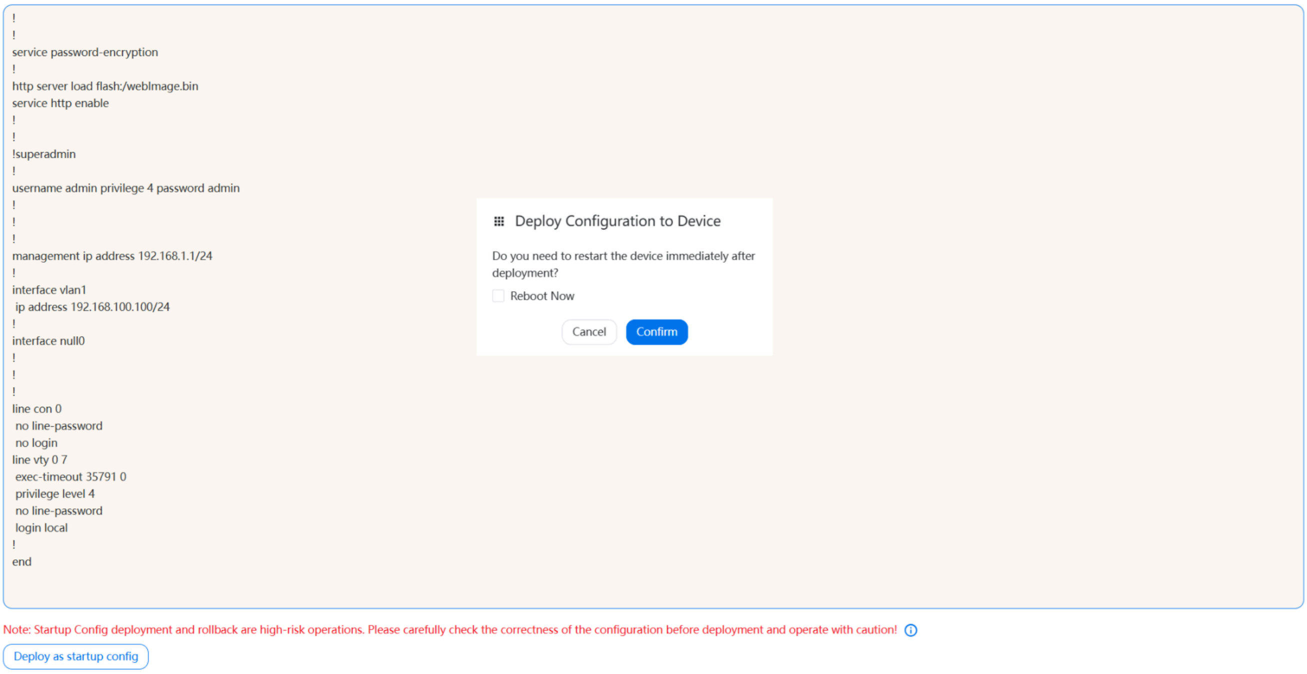
Model: S7548N-8Z-C SN: RH20251208N0003-3

	No.	Template Name	File Size	Updater	Update Time	Remark	Operate
○	1	Start	398 B	superadmin	2026-01-19 10:56:37	start	

Note: Startup Config deployment and rollback are high-risk operations. Please carefully check the correctness of the configuration before deployment and operate with caution!

▲*Figure 24: Configuration Template Reference 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:



```
!
!
service password-encryption
!
http server load flash:/webImage.bin
service http enable
!
!
!superadmin
!
username admin privilege 4 password admin
!
!
!
management ip address 192.168.1.1/24
!
interface vlan1
 ip address 192.168.100.100/24
!
interface null0
!
!
!
line con 0
 no line-password
 no login
line vty 0 7
 exec-timeout 35791 0
 privilege level 4
 no line-password
 login local
!
end
```

Deploy Configuration to Device

Do you need to restart the device immediately after deployment?

□ Reboot Now

Note: Startup Config deployment and rollback are high-risk operations. Please carefully check the correctness of the configuration before deployment and operate with caution!

▲*Figure 25: Configuration Preview and Apply Interface*

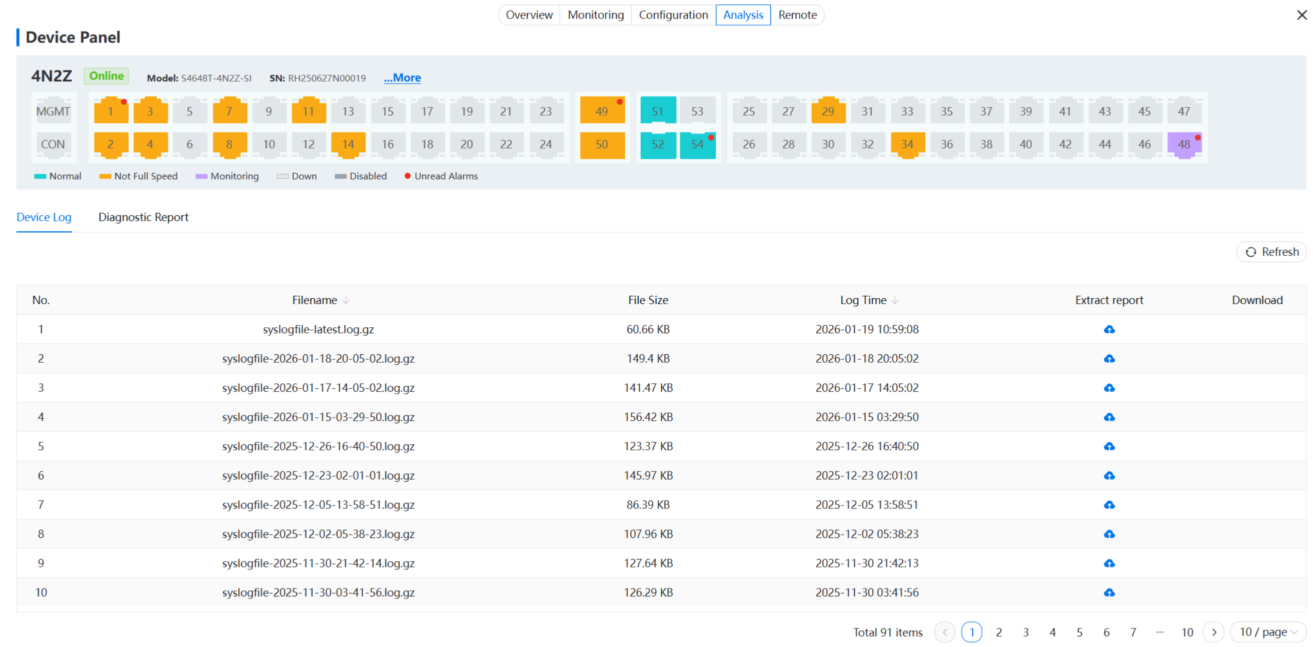
If there are multiple switches of the same model in the network with similar configurations, you can select an already saved configuration template, modify it, and then apply it.

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.



Device Panel

4N2Z Online **Model:** S4648T-4N2Z-SI **SN:** RH250627N00019 ...More

🟦 Normal 🟧 Not Full Speed 🟪 Monitoring □ Down ▬ Disabled ● Unread Alarms

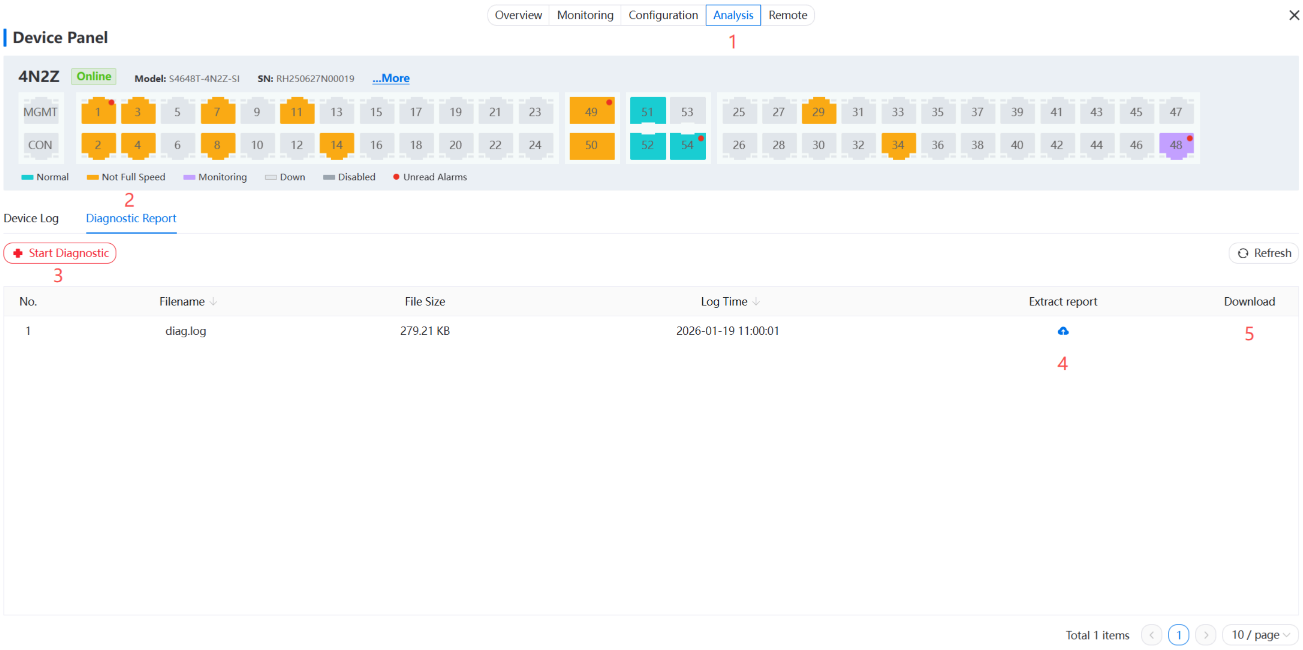
No.	Filename	File Size	Log Time	Extract report	Download
1	syslogfile-latest.log.gz	60.66 KB	2026-01-19 10:59:08	☁	
2	syslogfile-2026-01-18-20-05-02.log.gz	149.4 KB	2026-01-18 20:05:02	☁	
3	syslogfile-2026-01-17-14-05-02.log.gz	141.47 KB	2026-01-17 14:05:02	☁	
4	syslogfile-2026-01-15-03-29-50.log.gz	156.42 KB	2026-01-15 03:29:50	☁	
5	syslogfile-2025-12-26-16-40-50.log.gz	123.37 KB	2025-12-26 16:40:50	☁	
6	syslogfile-2025-12-23-02-01-01.log.gz	145.97 KB	2025-12-23 02:01:01	☁	
7	syslogfile-2025-12-05-13-58-51.log.gz	86.39 KB	2025-12-05 13:58:51	☁	
8	syslogfile-2025-12-02-05-38-23.log.gz	107.96 KB	2025-12-02 05:38:23	☁	
9	syslogfile-2025-11-30-21-42-14.log.gz	127.64 KB	2025-11-30 21:42:13	☁	
10	syslogfile-2025-11-30-03-41-56.log.gz	126.29 KB	2025-11-30 03:41:56	☁	

Total 91 items < 1 2 3 4 5 6 7 ··· 10 > 10 / page

▲*Figure 26: Operation Log Retrieval 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.



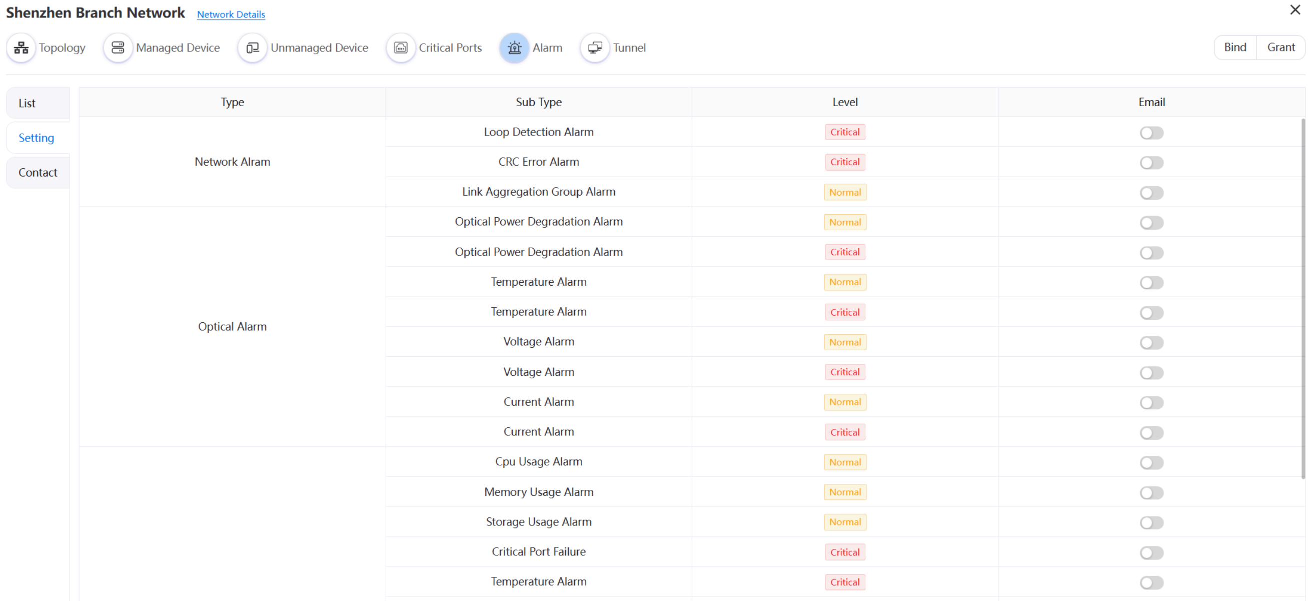
No.	Filename	File Size	Log Time	Extract report	Download
1	diag.log	279.21 KB	2026-01-19 11:00:01		

▲*Figure 27: Diagnostic Report Retrieval 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.

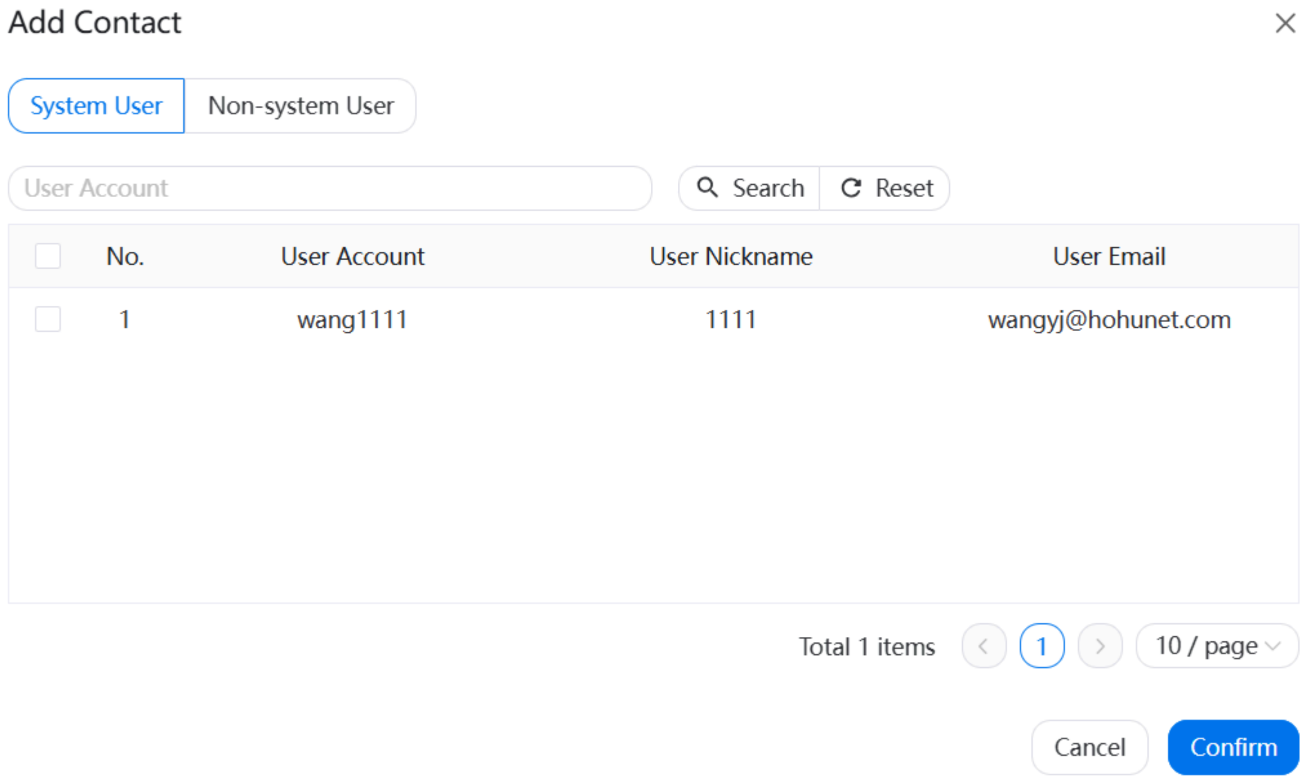


Type	Sub Type	Level	Email
Network Alram	Loop Detection Alarm	Critical	○
	CRC Error Alarm	Critical	○
	Link Aggregation Group Alarm	Normal	○
Optical Alarm	Optical Power Degradation Alarm	Normal	○
	Optical Power Degradation Alarm	Critical	○
	Temperature Alarm	Normal	○
	Temperature Alarm	Critical	○
	Voltage Alarm	Normal	○
	Voltage Alarm	Critical	○
	Current Alarm	Normal	○
	Current Alarm	Critical	○
	Cpu Usage Alarm	Normal	○
	Memory Usage Alarm	Normal	○
	Storage Usage Alarm	Normal	○
	Critical Port Failure	Critical	○
	Temperature Alarm	Critical	○

▲*Figure 28: Alarm Notification Settings Page*

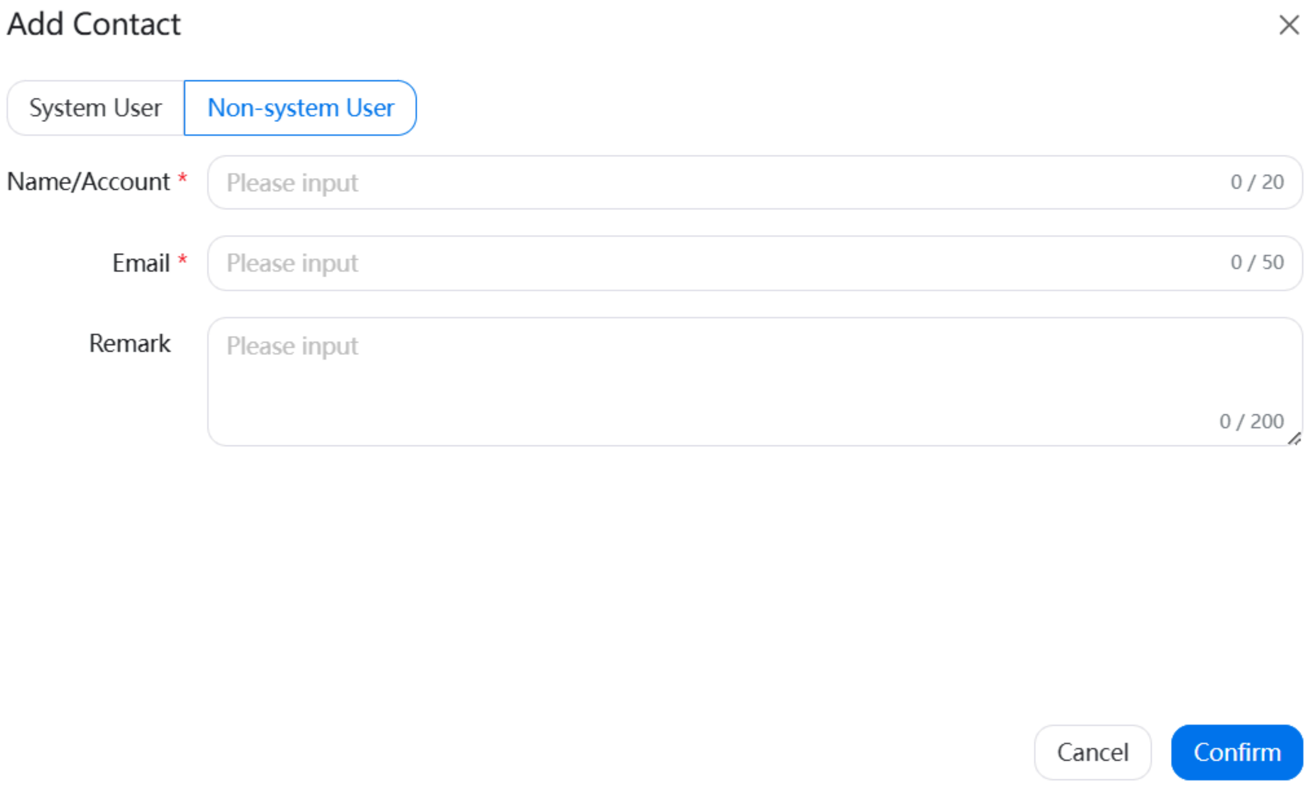
- Contact Settings

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:



□	No.	User Account	User Nickname	User Email
□	1	wang1111	1111	wangyj@hohunet.com

▲*Figure 29: Alarm Contacts Page (System Contacts)*



Name/Account * Please input 0 / 20

Email * Please input 0 / 50

Remark Please input 0 / 200

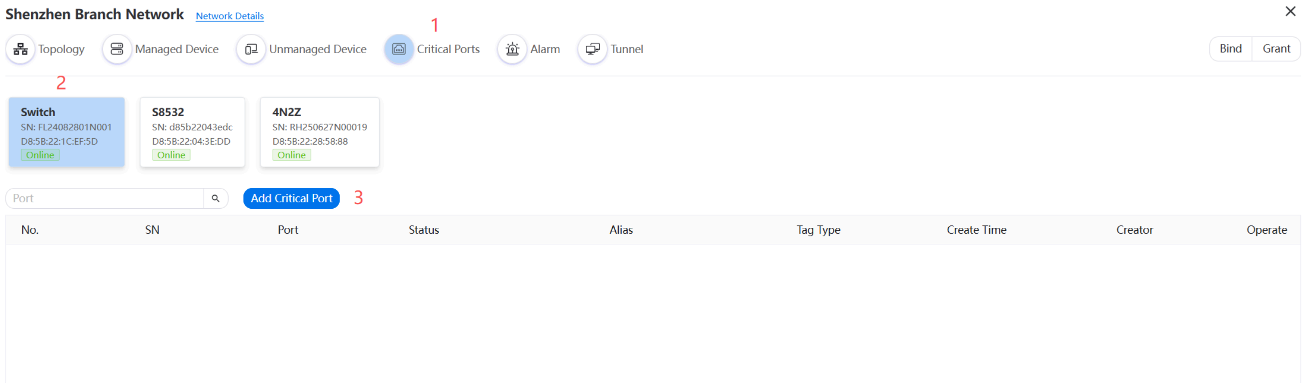
▲*Figure 30: Alarm Contacts Page (Non-System Contacts)*

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.

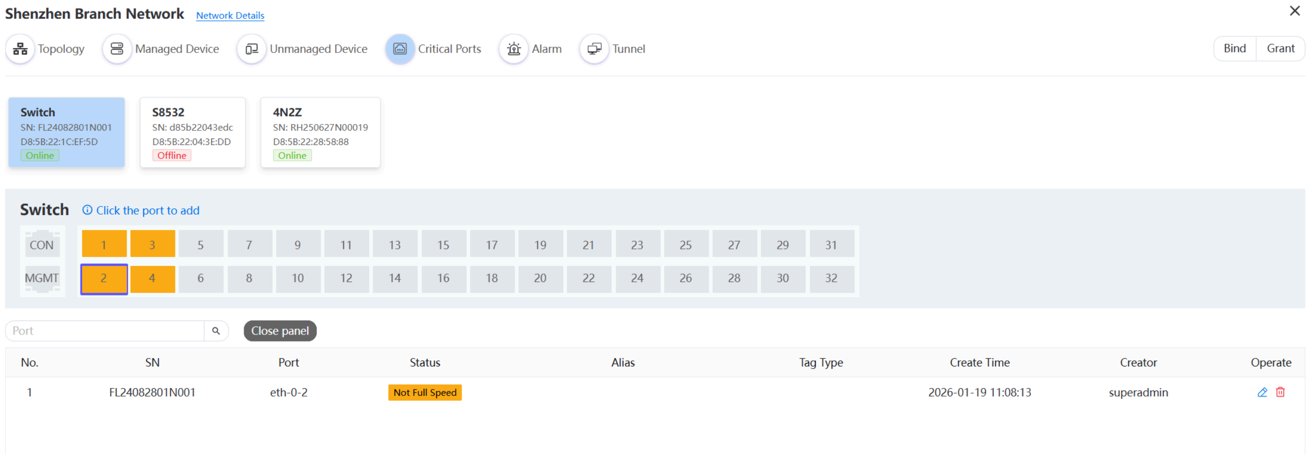
We can define these ports as "Critical Ports" and enable the corresponding alarm function to notify maintenance personnel promptly when port status becomes abnormal.



No.	SN	Port	Status	Alias	Tag Type	Create Time	Creator	Operate

▲*Figure 31: 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:



No.	SN	Port	Status	Alias	Tag Type	Create Time	Creator	Operate
1	FL24082801N001	eth-0-2	Not Full Speed			2026-01-19 11:08:13	superadmin	

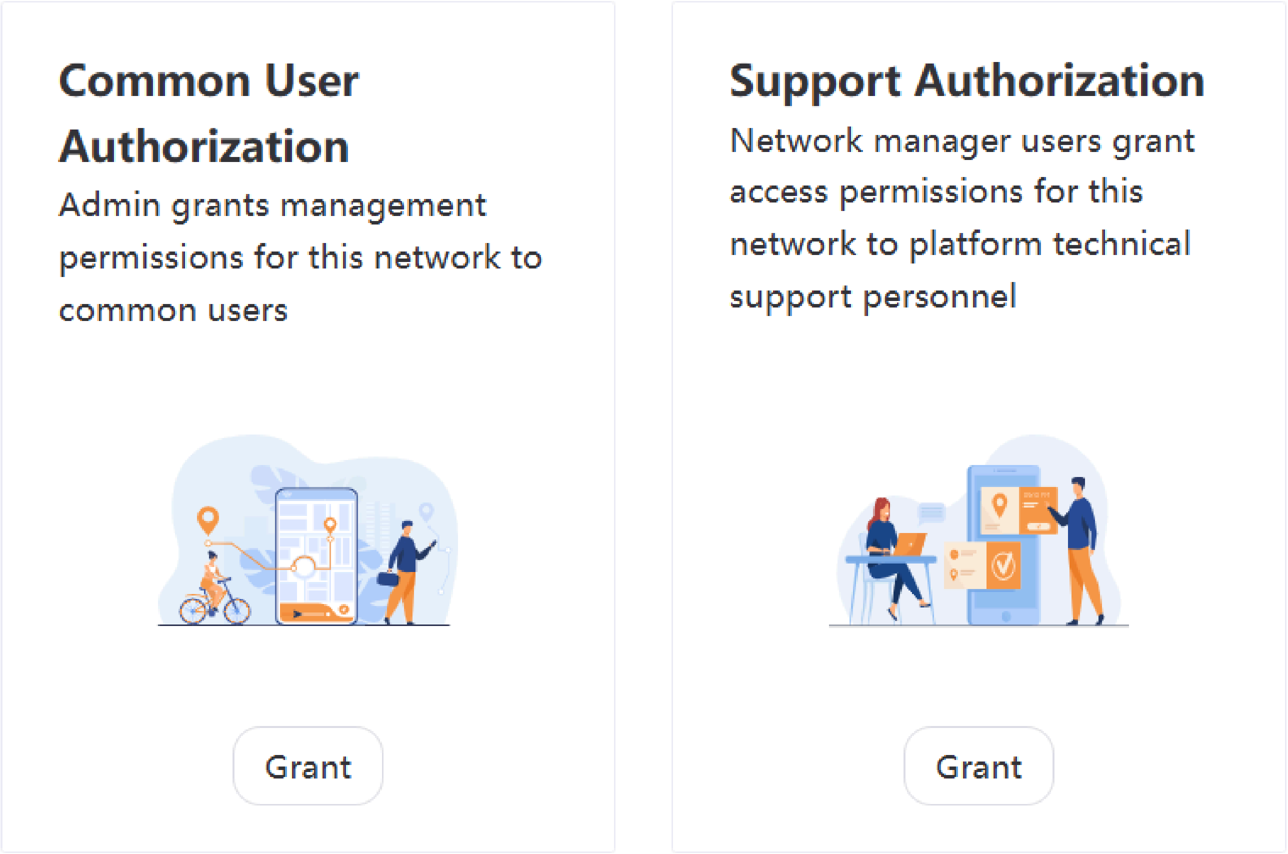
▲*Figure 32: Marking Critical Ports on Device Panel*

- 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. Also, check the email address you set in 'Alarm Contacts'; you should receive an alarm notification email for 'Critical Port Exception'.

3.3. Request Technical Support

If a user encounters network issues they cannot handle and need assistance from platform technical support, they can authorize platform technical support. Click "Platform Support Authorization" in Network Authorization.



Common User Authorization

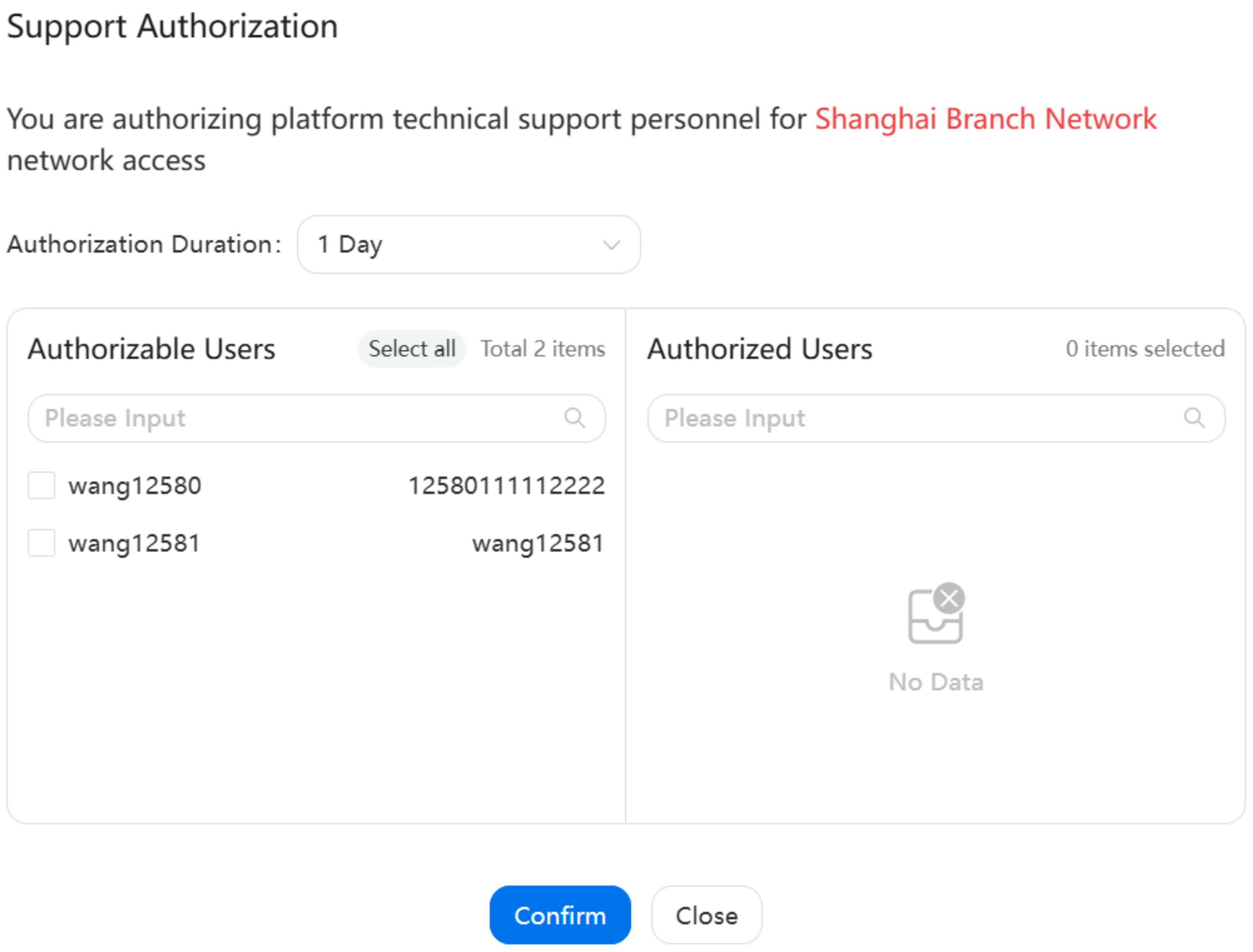
Admin grants management permissions for this network to common users

Support Authorization

Network manager users grant access permissions for this network to platform technical support personnel

▲*Figure 33: 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 read-only or partial operational permissions for the authorized network and devices within a specified time (default 24 hours). Permissions are automatically revoked after expiration.



Support Authorization

You are authorizing platform technical support personnel for Shanghai Branch Network network access

Authorization Duration: 1 Day

□ wang12580 12580111112222

□ wang12581 wang12581

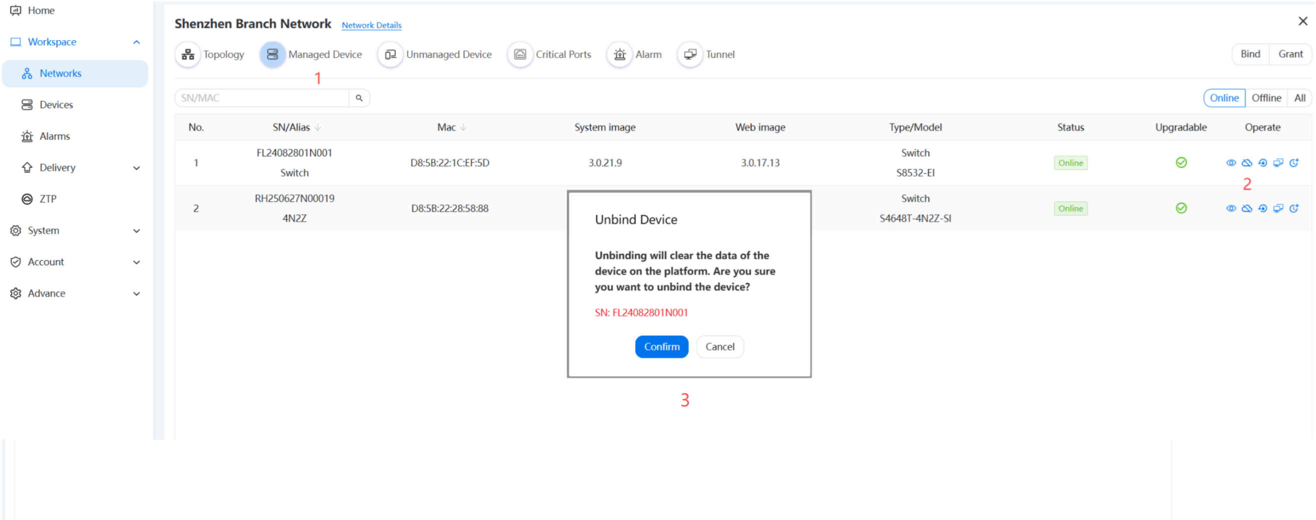
▲*Figure 34: Platform Technical Support Authorization Dialog*

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.



No.	SN/Alias	Mac	System image	Web image	Type/Model	Status	Upgradable	Operate
1	FL24082801N001 Switch	D8:5B:22:1C:EF:5D	3.0.21.9	3.0.17.13	Switch S8532-EI	Online	✓	
2	RH250627N00019 4N2Z	D8:5B:22:28:58:88			Switch S4648T-4N2Z-SI	Online	✓	

Unbind Device

Unbinding will clear the data of the device on the platform. Are you sure you want to unbind the device?

SN: FL24082801N001

Confirm Cancel

▲Figure 35: 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.

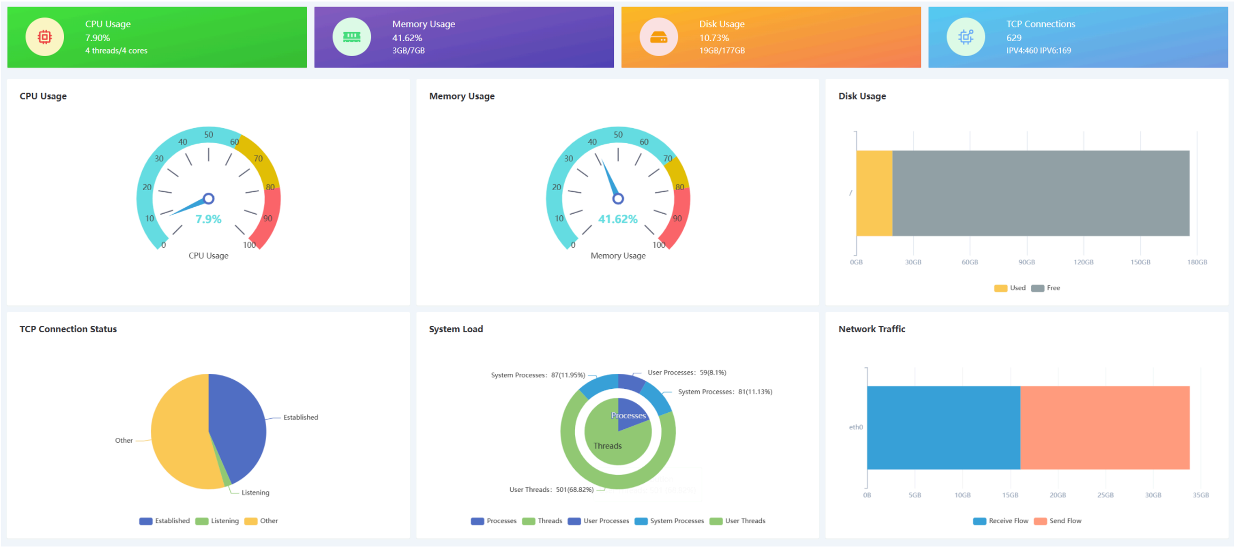
4. System Management (Platform Administrator)

The following are the steps for configuring system parameters by the platform administrator (superadmin). Regular 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.



CPU Usage
7.90%
4 threads/4 cores

Memory Usage
41.62%
3GB/7GB

Disk Usage
10.73%
19GB/177GB

TCP Connections
629
IPV4:460 IPV6:169

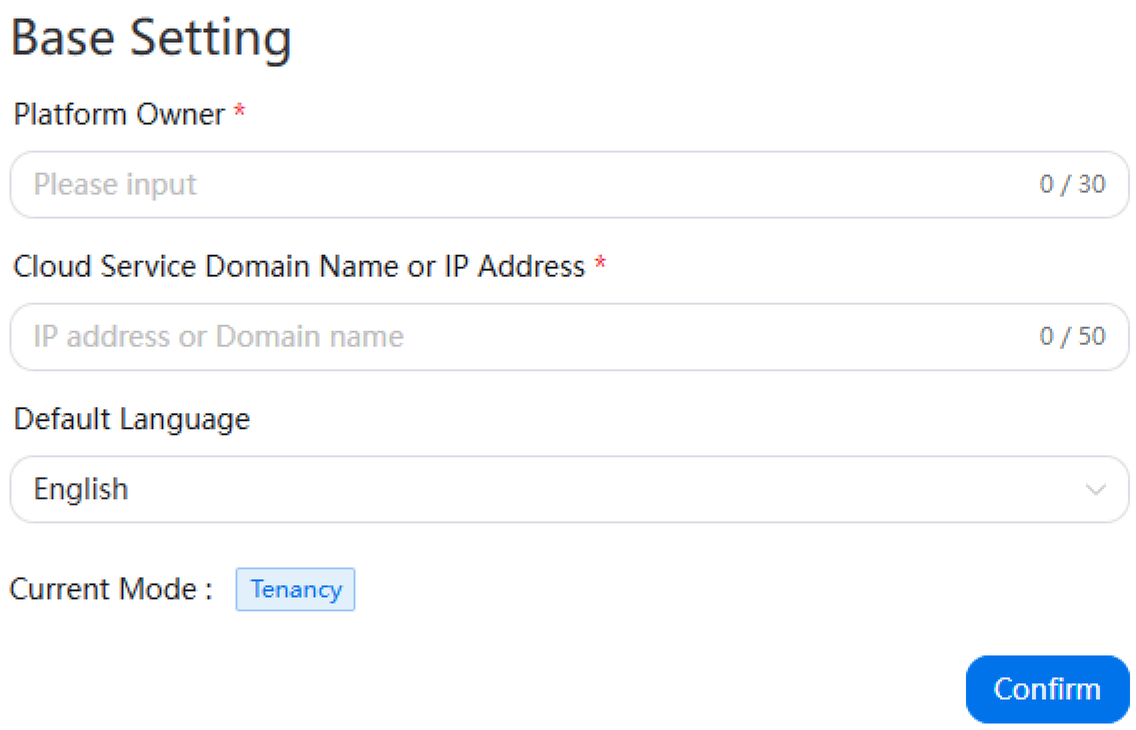
▲*Figure 36: System Dashboard Page*

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, etc.

4.2.1. Basic Settings

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



Base Setting

Platform Owner *

Please input 0 / 30

Cloud Service Domain Name or IP Address *

IP address or Domain name 0 / 50

Default Language

English

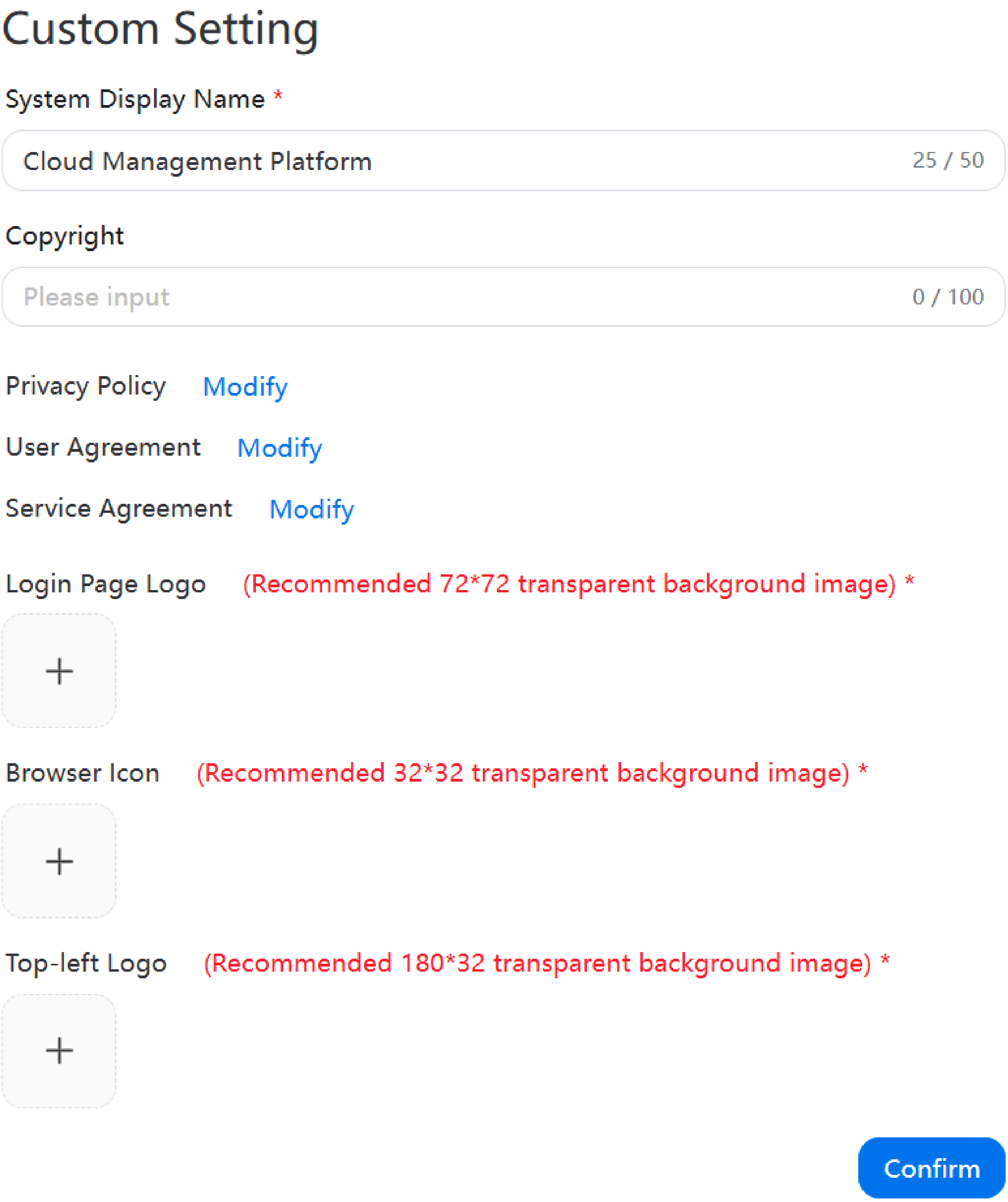
Current Mode : Tenancy

▲*Figure 37: 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:



Custom Setting

System Display Name *

Cloud Management Platform 25 / 50

Copyright

Please input 0 / 100

Privacy Policy Modify

User Agreement Modify

Service Agreement Modify

Login Page Logo (Recommended 72*72 transparent background image) *

+

Browser Icon (Recommended 32*32 transparent background image) *

+

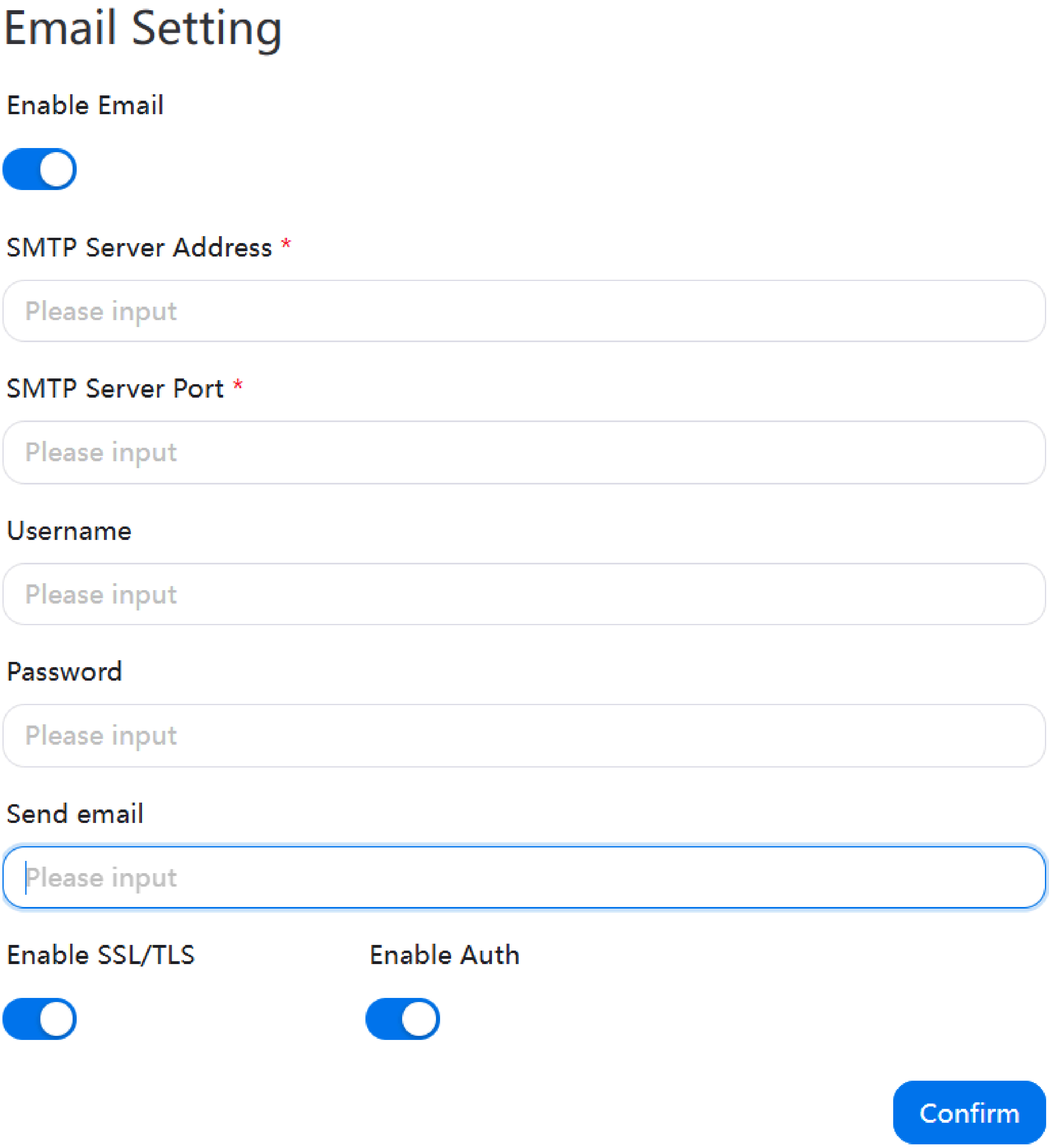
Top-left Logo (Recommended 180*32 transparent background image) *

+

▲*Figure 38: 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:



Email Setting

Enable Email

SMTP Server Address *

Please input

SMTP Server Port *

Please input

Username

Please input

Password

Please input

Send email

Please input

Enable SSL/TLS

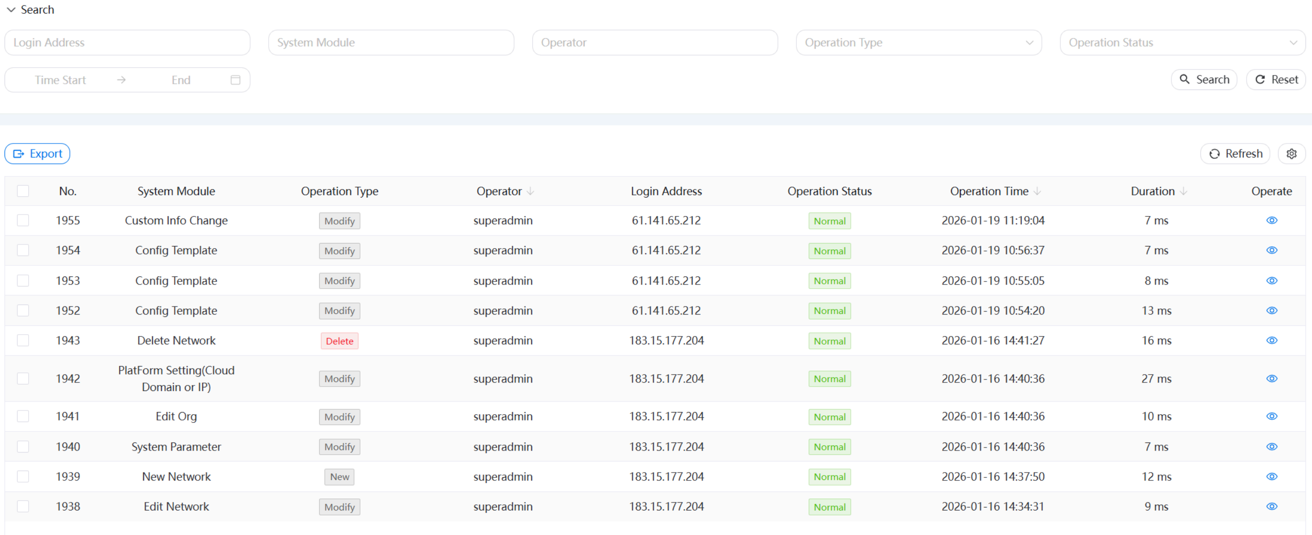
Enable Auth

▲*Figure 39: 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.



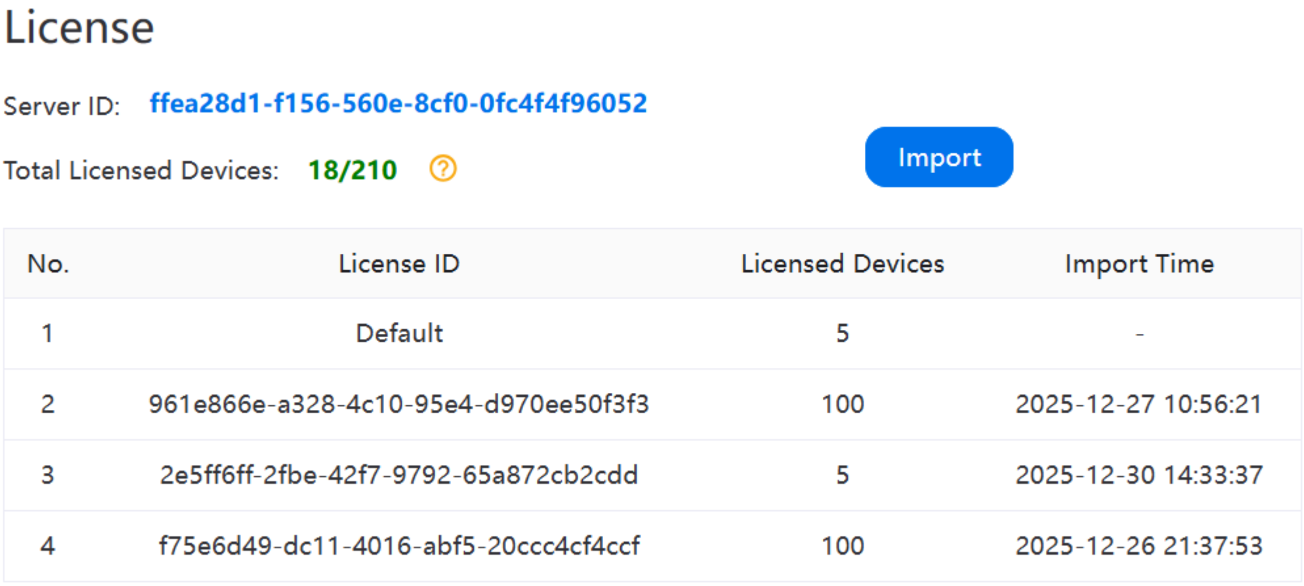
□	No.	System Module	Operation Type	Operator	Login Address	Operation Status	Operation Time	Duration	Operate
□	1955	Custom Info Change	Modify	superadmin	61.141.65.212	Normal	2026-01-19 11:19:04	7 ms	👁
□	1954	Config Template	Modify	superadmin	61.141.65.212	Normal	2026-01-19 10:56:37	7 ms	👁
□	1953	Config 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 40: 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.



Server ID: ffea28d1-f156-560e-8cf0-0fc4f4f96052

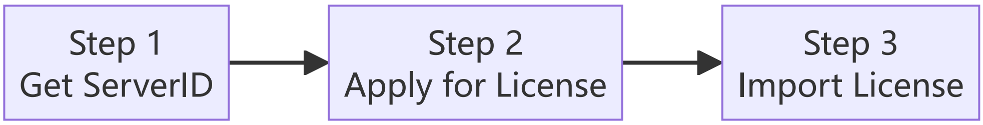
Total Licensed Devices: 18/210

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 41: License Management Page*

4.4.2. Operation Process

The License application process is shown below:



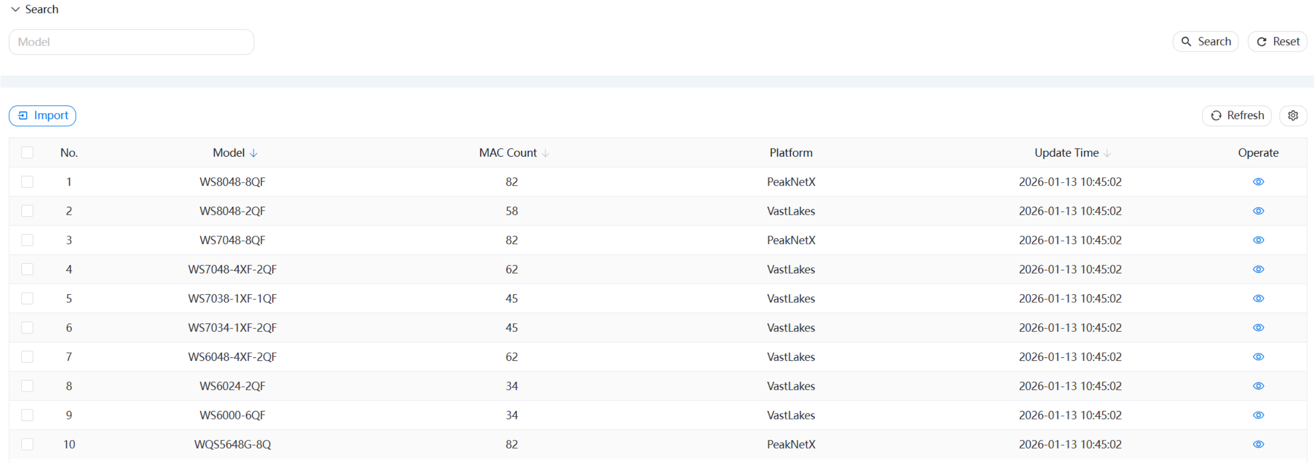
▲*Figure 42: License Application Flow Chart*

- 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 43: Product Models Management Page*