



Ruijie RG-CS86 Series Switches

CS86_RGOS 12.6(2)B0103

Web-based Configuration Guide

Document Version: V1.0

Date: May 09th, 2023

Copyright © 2023 Ruijie Networks

Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerpt, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Trademark  and  are owned by Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- Technical Support Website: <https://ruijienetworks.com/support>
- Case Portal: <https://caseportal.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: [service_rj@ruijienetworks.com](https://www.ruijienetworks.com)

Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords are in bold font .
<i>Italic font</i>	Arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
&<1-n>	The argument before the sign (&) can be input for consecutive 1- n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

 **Caution**

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

 **Note**

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

 **Specification**

An alert that contains a description of product or version support.

3. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

1 RG-INC-EMB User Guide

1.1 Overview

This document describes how to use the eWeb management system. You can use the eWeb management system to configure common settings for switches.

You can access the eWeb management system through a browser (such as Google Chrome) to manage switches.

Note

This document only applies to the eWeb management system of the CS86 series, and is compatible with the RG-INC-EMB_1.22 version.

1.2 Typical Applications

Typical Application	Description
Managing Switches Through the eWeb Management System	After switches are properly configured, you can access the eWeb management system through a browser to manage these switches.

1.2.1 Managing Switches Through the eWeb Management System

Configuration Environment Requirements

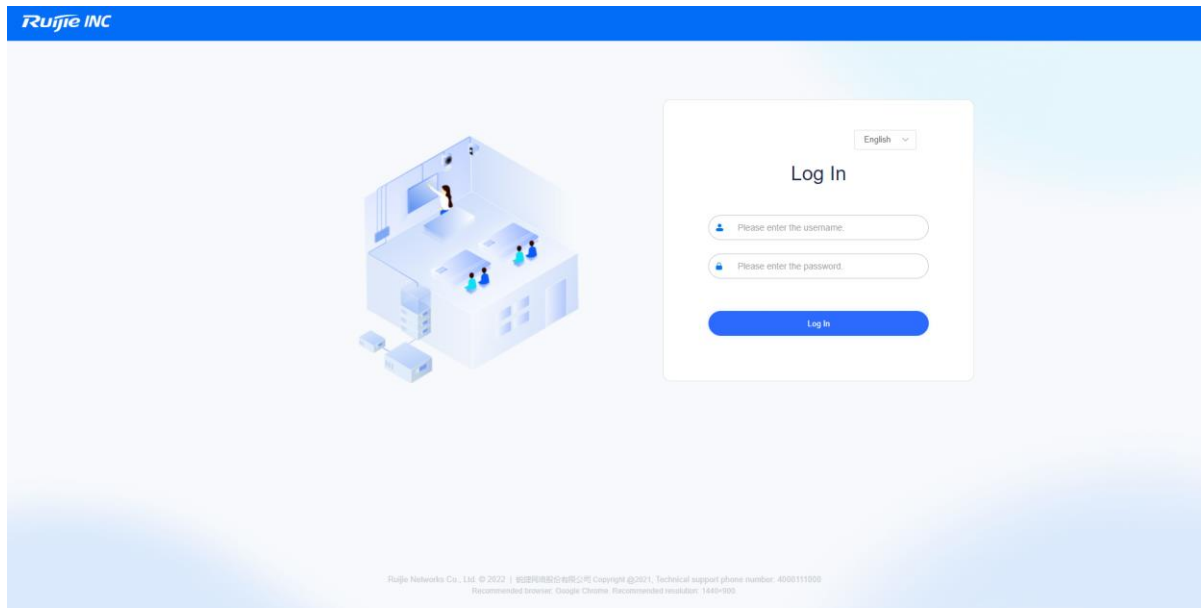
Client requirements:

1. Client: A client refers to a PC or a mobile terminal such as a laptop. A network administrator can log in to the eWeb graphical user interface (GUI) of a switch from the client's browser to manage switches.
2. Browser: Google Chrome is recommended. Exceptions such as garbled characters or formatting errors may occur if an unsupported browser is used. If an exception occurs due to the use of an old version of Google Chrome, you are advised to upgrade it to the latest version.
3. Resolution: You are advised to set the resolution to 1600 x 900 or 1920 x 1080. If other resolutions are used, font and formatting issues may occur.

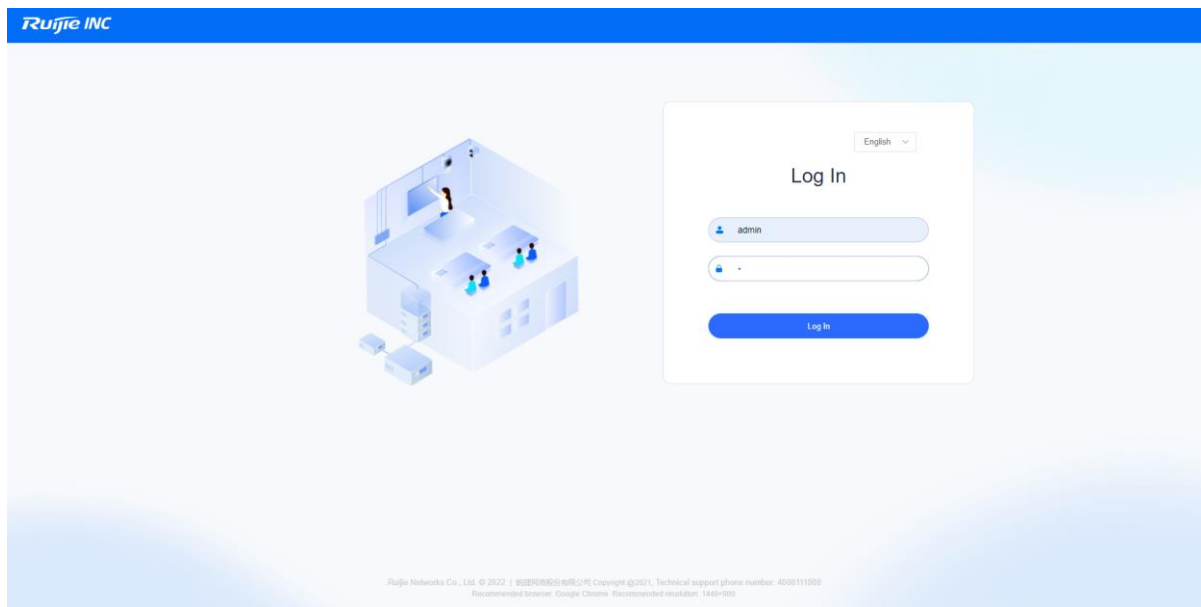
1.3 eWeb Management System

1.3.1 Logging In

Enter the switch IP address in your browser's address bar. Make sure that the IP address is reachable. The login page is displayed.



1. Enter the username and password and click **Log In**. The main interface of the eWeb management system is displayed.
2. If you cannot remember your username or password, click **Forgot Password?**
3. If you need customer service assistance, contact local technical support.
4. To prevent login through brute-force cracking, your account will be locked for 10 minutes after 5 failed attempts. You cannot log in during the locking period.

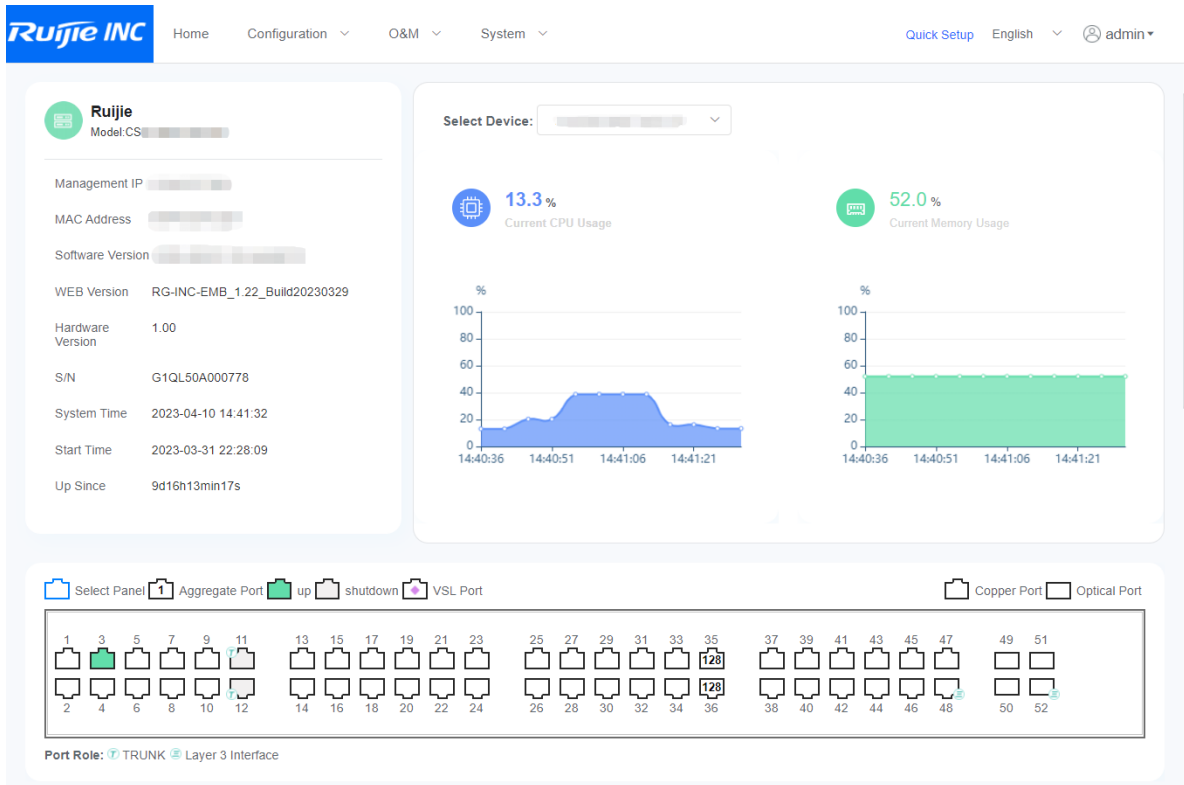


i Note

To use the eWeb management system, ensure that the rg-web component has been installed on the switch and the web service has been enabled (if the web service is not enabled, run the enable service web-server command in config mode to enable it). Otherwise, the login page is not displayed. In most situations, the rg-web component is integrated in the rgos.bin system by default. However, if it is not installed, you can install it by installing the upgrade file mentioned in this release note of the eWeb management system.

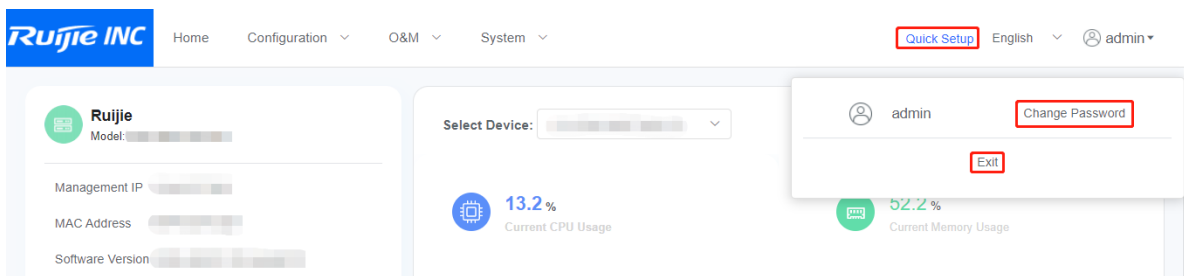
1.3.2 Main Interface

The main interface of the eWeb management system is displayed.



1. Header

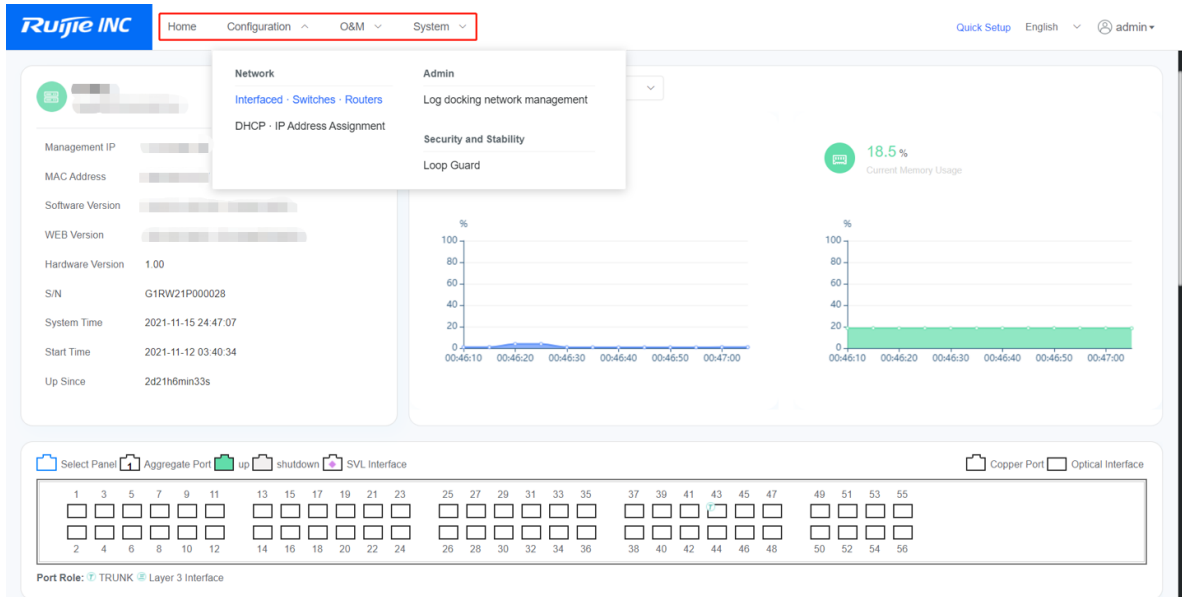
This area displays the links to common functions, including Quick Setup, Change Password, and Exit. You can click these links to switch to specific configuration pages.



- **Change Password:** After you click **Change Password**, the **Change Password** page is displayed. You can enter the old password and the new password to reset the password.
- **Exit:** When device management is complete, you can click **Exit** to exit the main interface and return to the login page.

2. Navigation Menu

This area displays main tabs of the eWeb management system.



3. Main Operation Area

In this area, you can perform configurations on the eWeb management system. When you click the shortcut menu at the top of the page, the detailed configuration page is displayed.

1.3.3 Quick Setup

The switch is not configured when you log in to the eWeb management system for the first time. To simplify the configuration, you can use the **Quick Setup** wizard to configure common settings for the switch.

Note

You can click **Quick Setup** in the upper-right corner of the main interface of the eWeb management system to open the **Quick Setup** wizard.

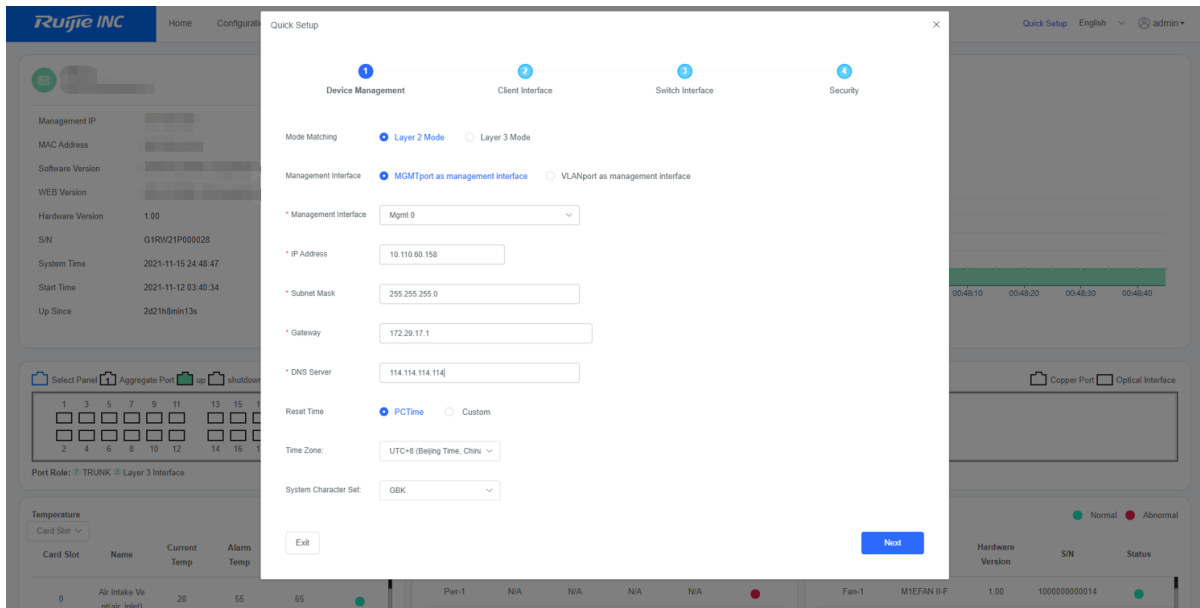
1. Quick Setup

Layer 2 Mode

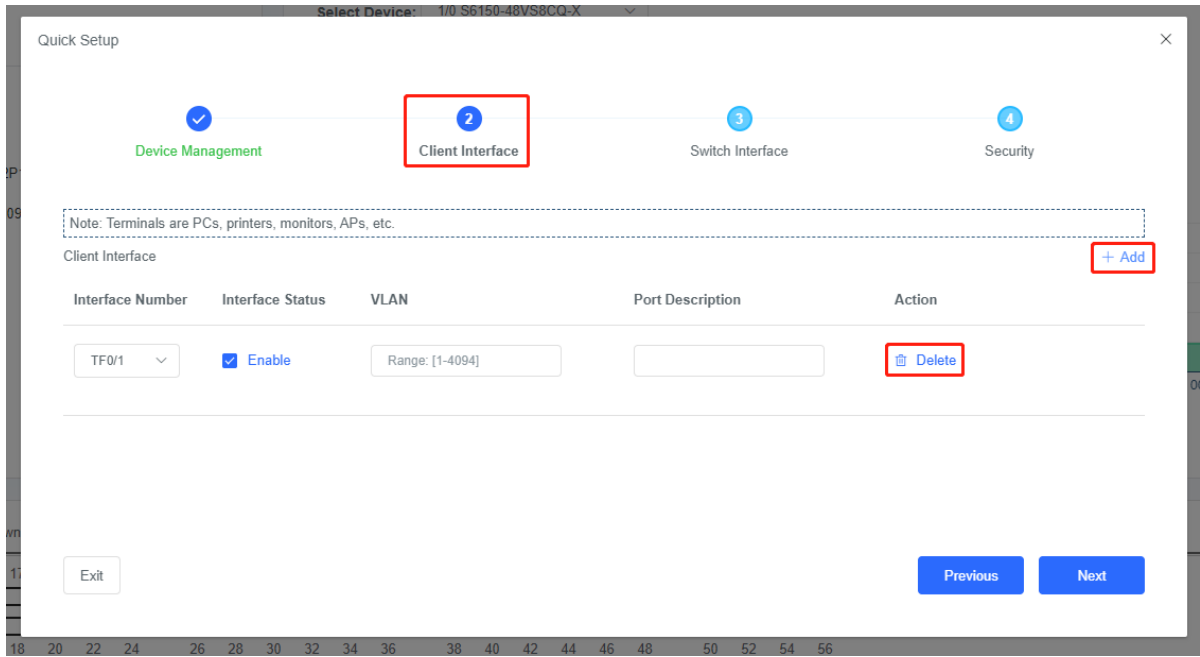
There are four steps in this mode.

(1) Device Management

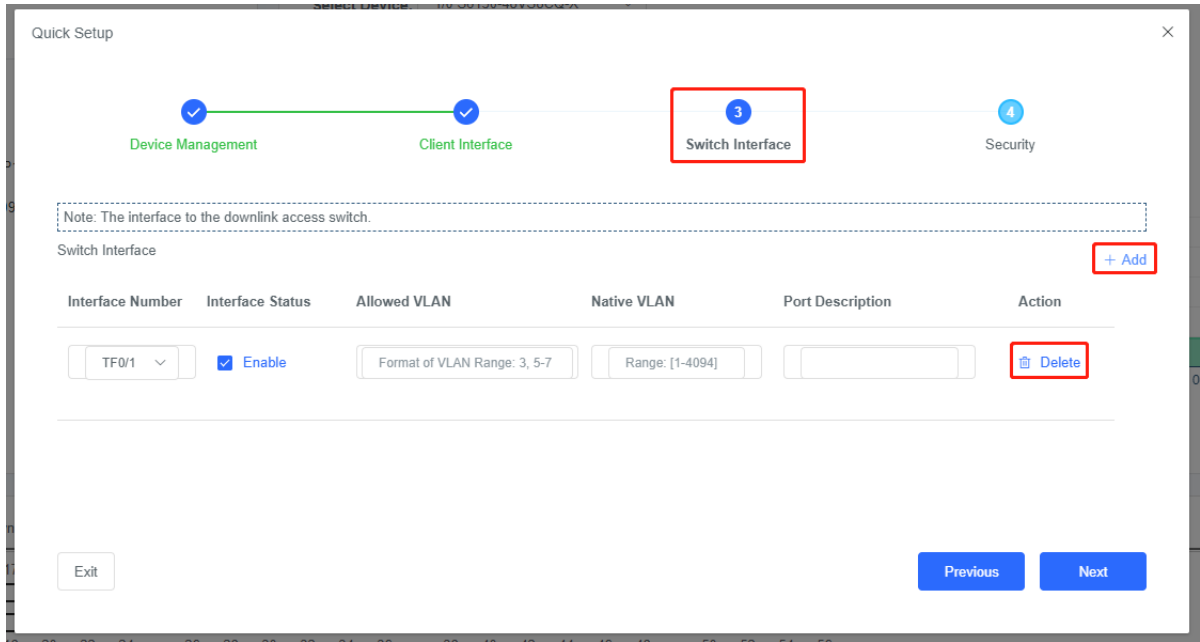
Web-based Configuration Guide



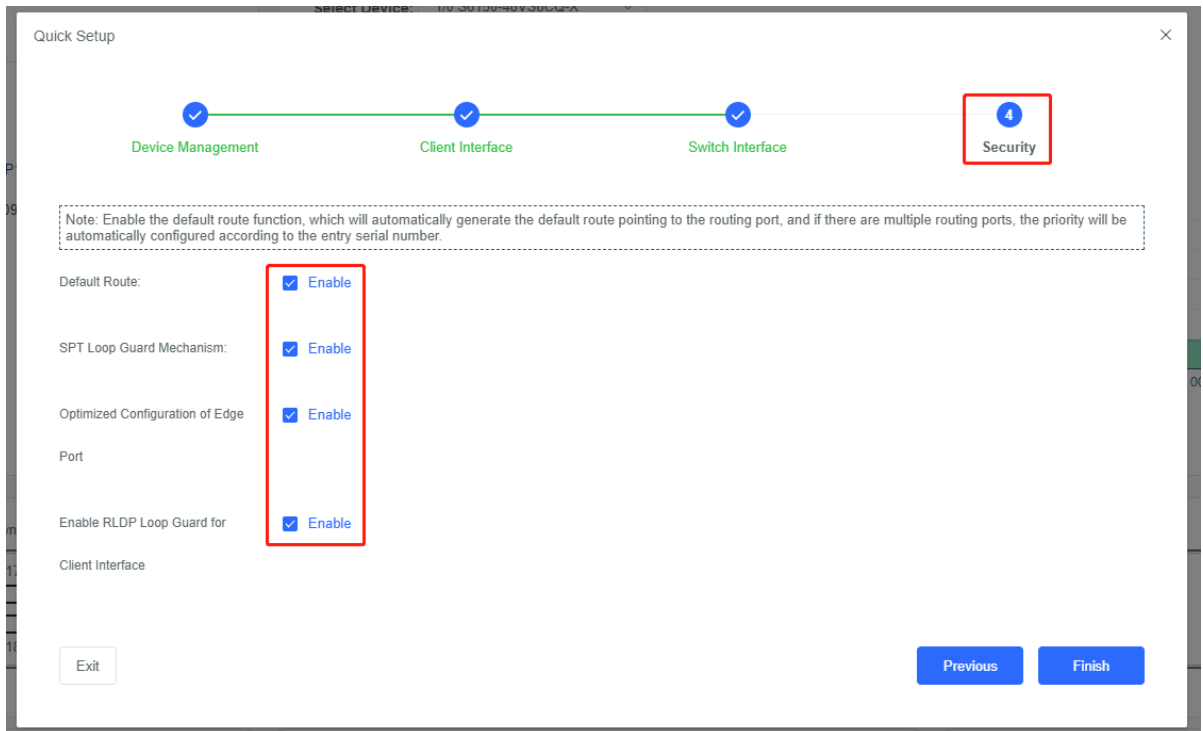
(2) Client Interface



(3) Switch Interface



(4) Security

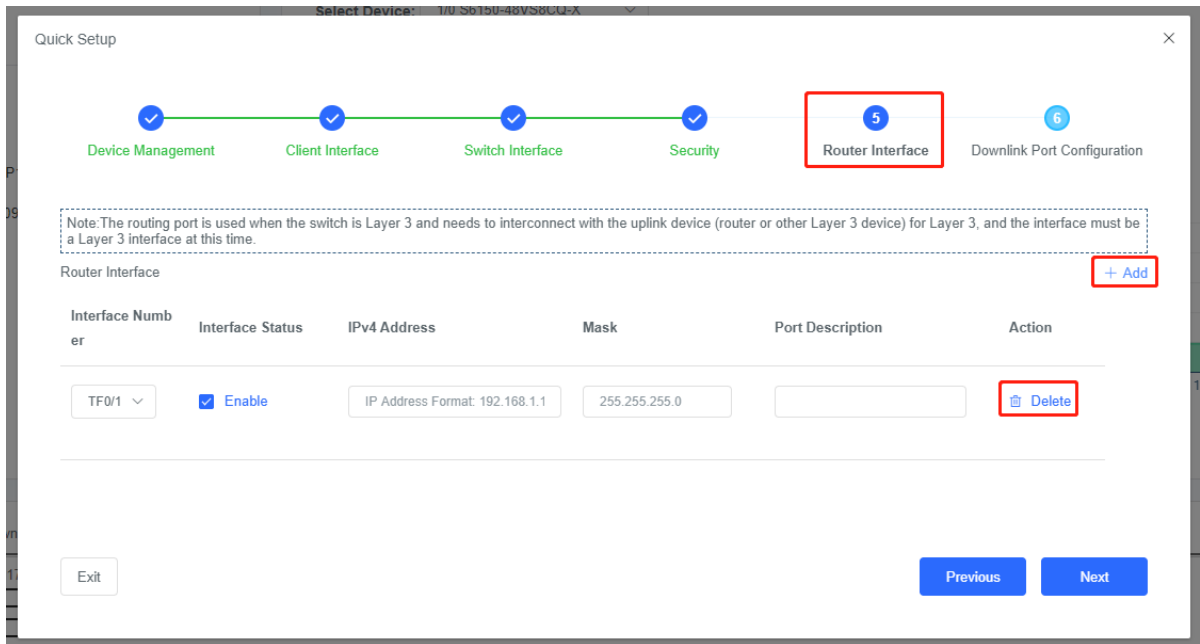


Layer 3 Mode

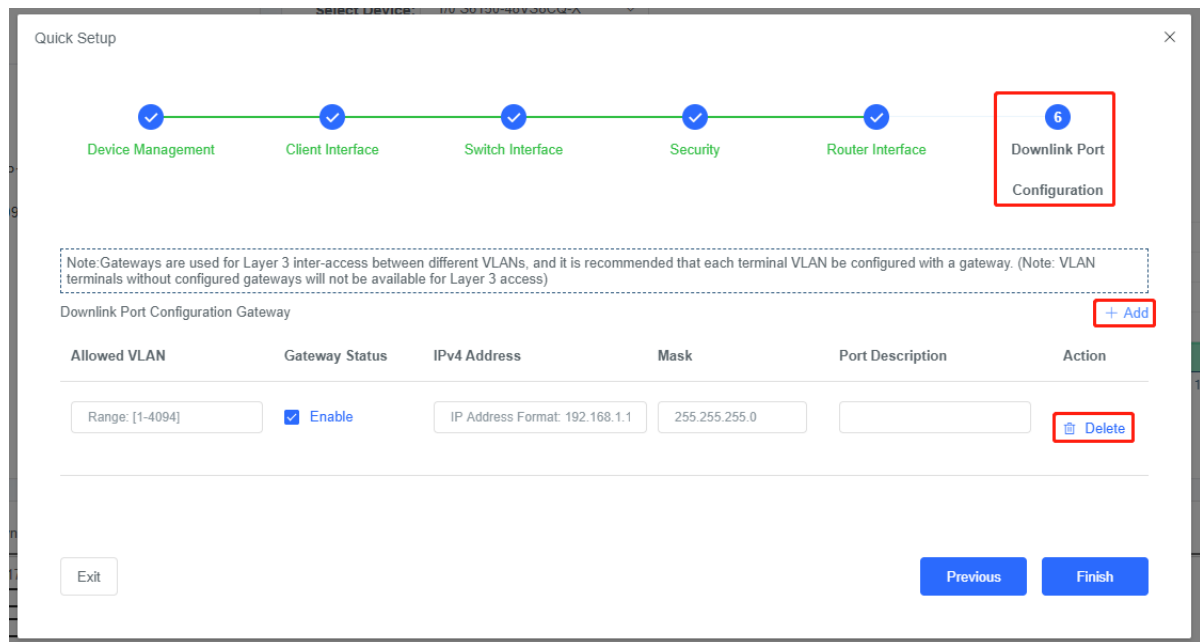
There are six steps in this mode.

The first four steps are the same as those in Layer 2 mode, so only the last two steps are described here.

(1) Router Interface (Layer 3 Mode)



(2) Downlink Port Configuration (Layer 3 Mode)



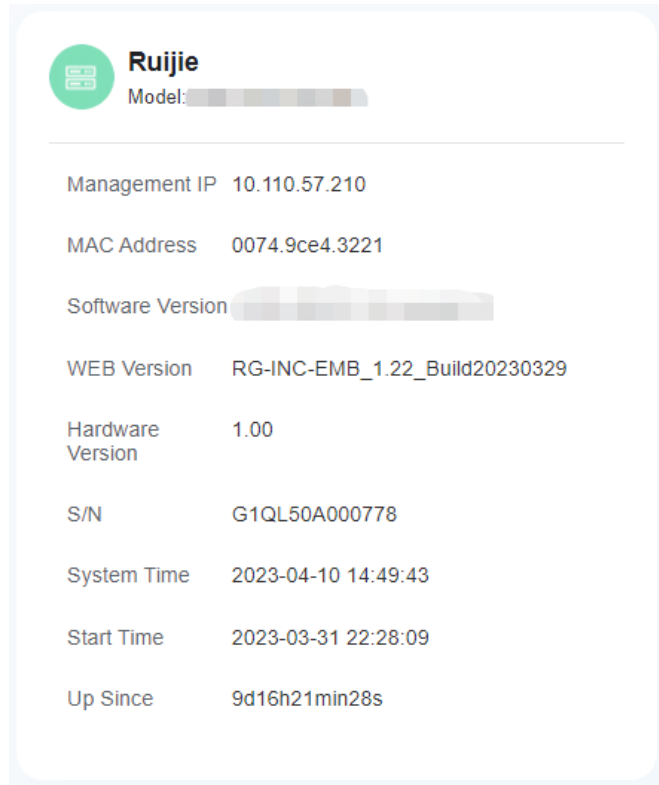
1.3.4 Home Page

After you log in to the eWeb management system, you will be automatically redirected to the home page. Or, you can click **Home** in the navigation menu to switch to the home page.

On this page, you can view the CPU, memory usage, system version, current system time, and other information of the switch. By analyzing the trend of Top 5 interface traffic, you can identify common network problems on this page and quickly resolve these problems.

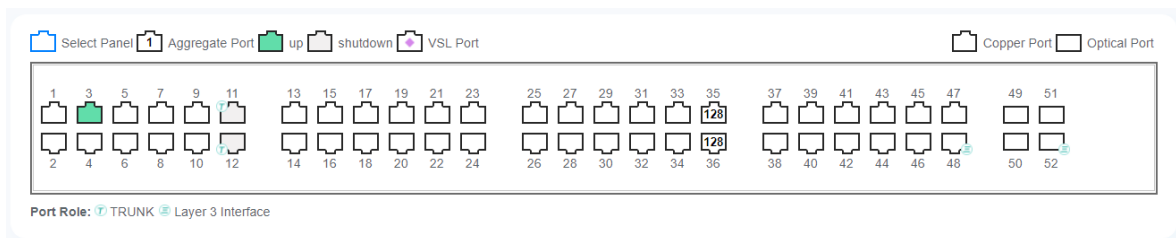
1. Switch Overview

At the top of the home page, you can view the switch name, model, management IP address, MAC address, software version, hardware version, serial number, system time, startup time, and uptime. You can reset the system time on the **System Time** page by choosing **O&M > Basic Configuration > System Time**.



2. Interfaces

In the upper part of the home page is the interface panel where interface information is displayed. The panel shows the basic interface configurations, such as interface type, state, aggregated interface, and virtual switching link (SVL) interface.

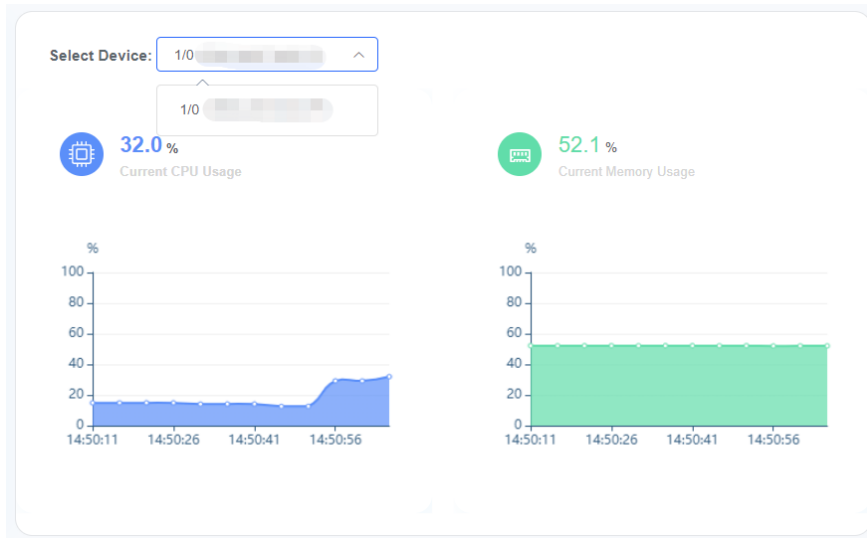


3. CPU/Memory Usage

The CPU and memory usage of the switch is displayed at the top of the home page.

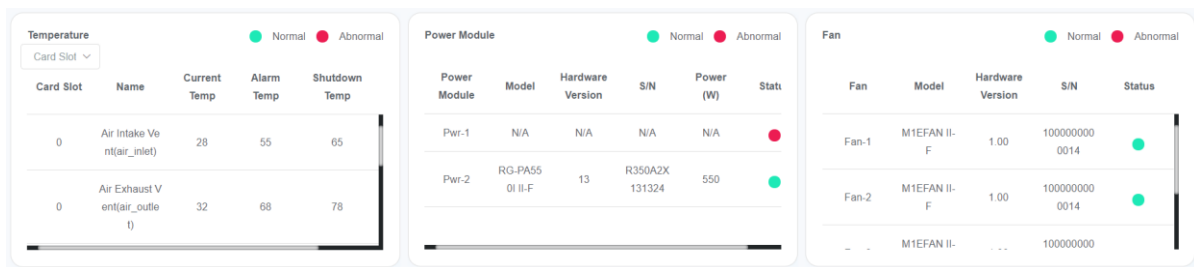
CPU: indicates the CPU usage of the switch service module.

Memory: indicates the memory usage of the switch service module.



4. Temperature/Power Module/Fan

The middle part of the home page displays the temperature, power module status, fan status of the switch at different positions.



In the **Temperature** panel, you can view the temperature of a card slot by selecting a card slot from the **Card Slot** drop-down list box.

5. Bandwidth



You can click **More** in the **Top 5 Interface Bandwidth Utilization** panel to query more details about interface bandwidth utilization.

<input type="checkbox"/>	Name	Inbound Bandwidth Usage	Outbound Bandwidth Usage	Port bandwidth	Packet not complete/too large	CRC/FCS error packets	Number of Conflicts
<input type="checkbox"/>	G/3/21	0.01%	0.01%	1000M	0/0	0/0	0
<input type="checkbox"/>	G/3/23	0.01%	0.01%	1000M	0/0	0/0	0
<input type="checkbox"/>	G/3/24	0.02%	0.01%	1000M	0/0	0/0	0

Total: 3

Back: returns to the home page.

Refresh: re-queries the interface bandwidth utilization.

Clear: deletes statistics about a selected interface, such as the number of error packets and conflicting count.

Clear All: deletes statistics about all interfaces, such as the number of error packets and conflicting count.

1.3.5 Configuration

1. Port Management

Port Configuration

Port

- Network
 - Interfaced - Switches - Routers
 - DHCP - IP Address Assignment
- Admin
 - Log docking network management
 - Security and Stability
 - Loop Guard

Layer 3 Interface

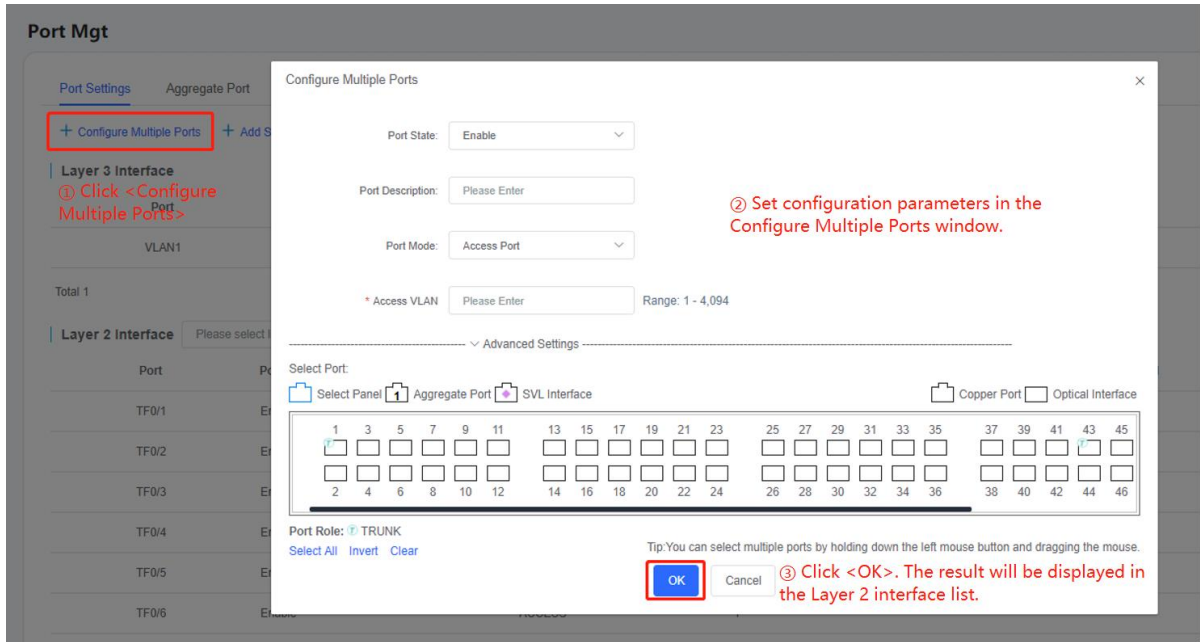
Port	Port State	IP Address	Subnet Mask	IPv6 Address	Port Description	Action
VLAN1	Enable					Edit Delete

Total 1

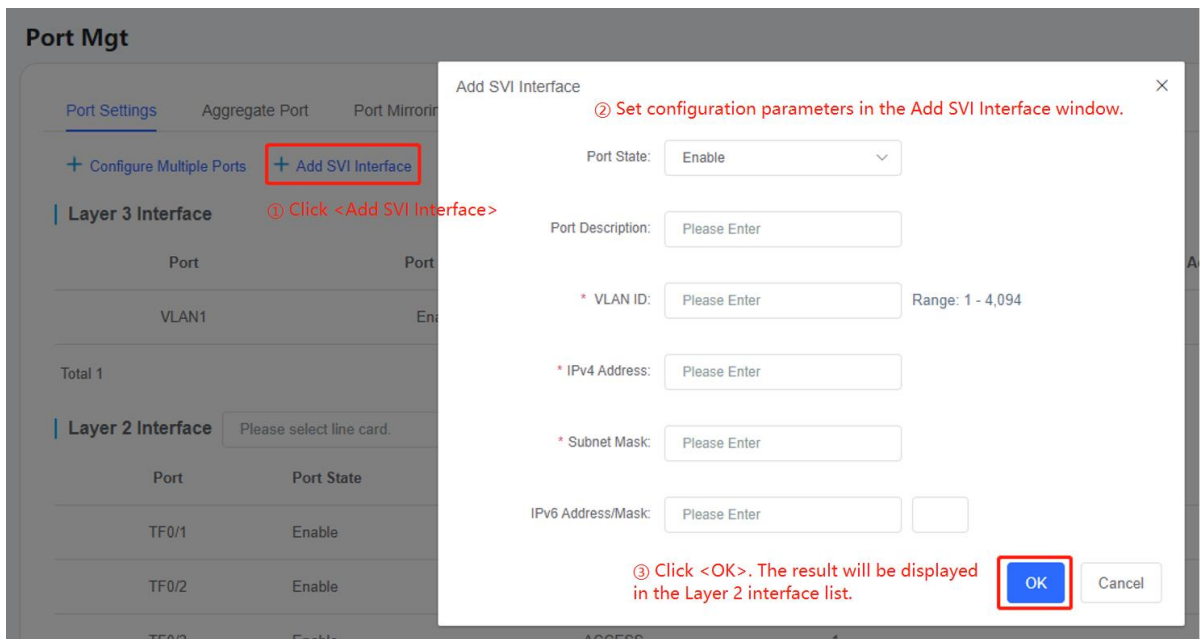
Layer 2 Interface Please select line card.

Port	Port State	Port Type	Access VLAN	Native VLAN	Permit VLAN	Port Description	Action
TF0/1	Enable	TRUNK		1	3		Edit Details
TF0/2	Enable	ACCESS	1				Edit Details
TF0/3	Enable	ACCESS	1				Edit Details
TF0/4	Enable	ACCESS	1				Edit Details
TF0/5	Enable	ACCESS	1				Edit Details
TF0/6	Enable	ACCESS	1				Edit Details

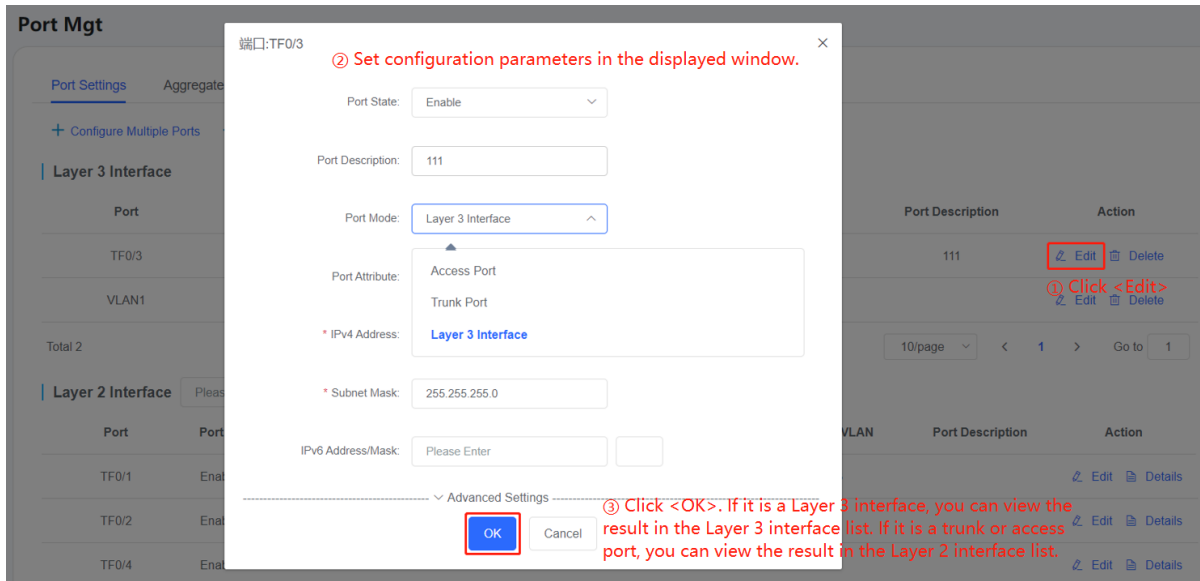
- **Configuring multiple ports**



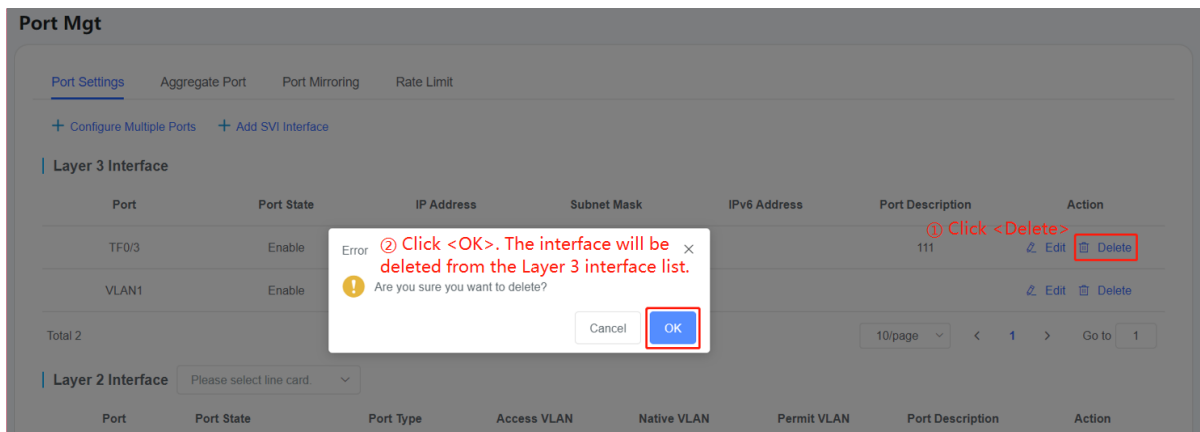
- Adding an SVI



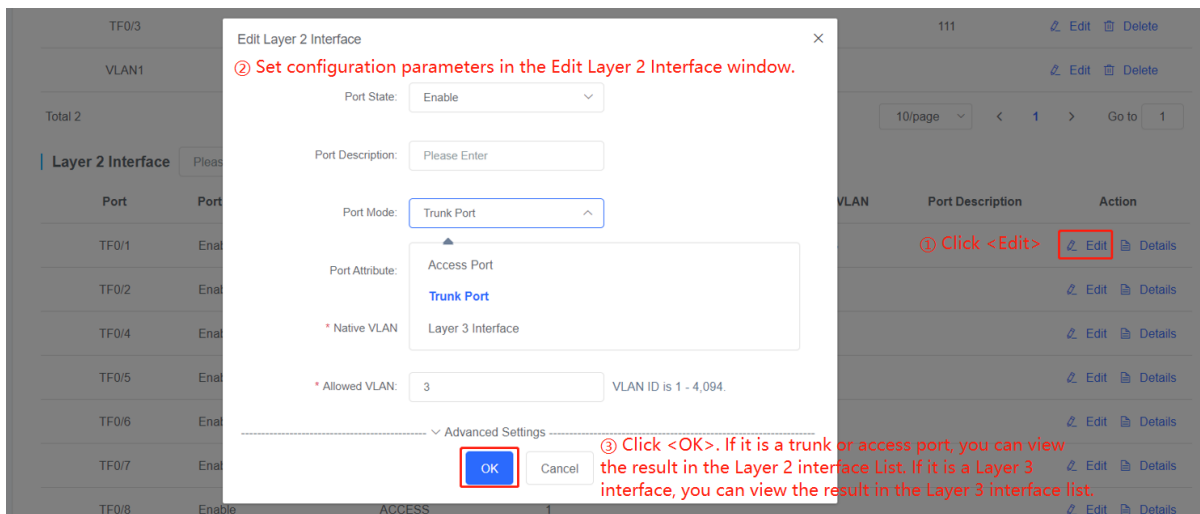
- Editing a Layer 3 interface



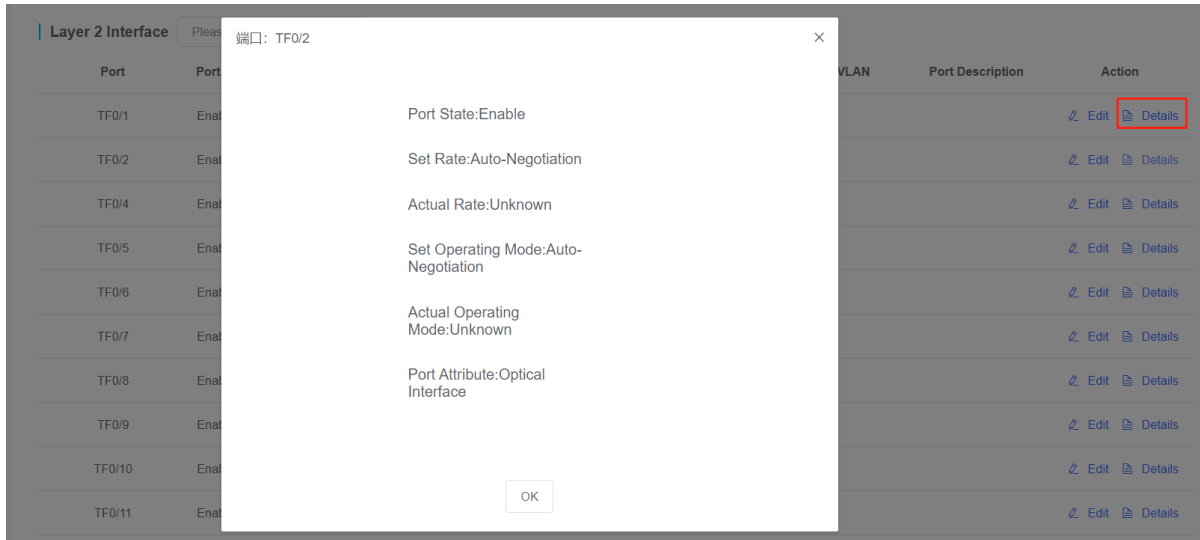
● Deleting a Layer 3 interface



● Editing a Layer 2 interface



● A Layer 2 interface details



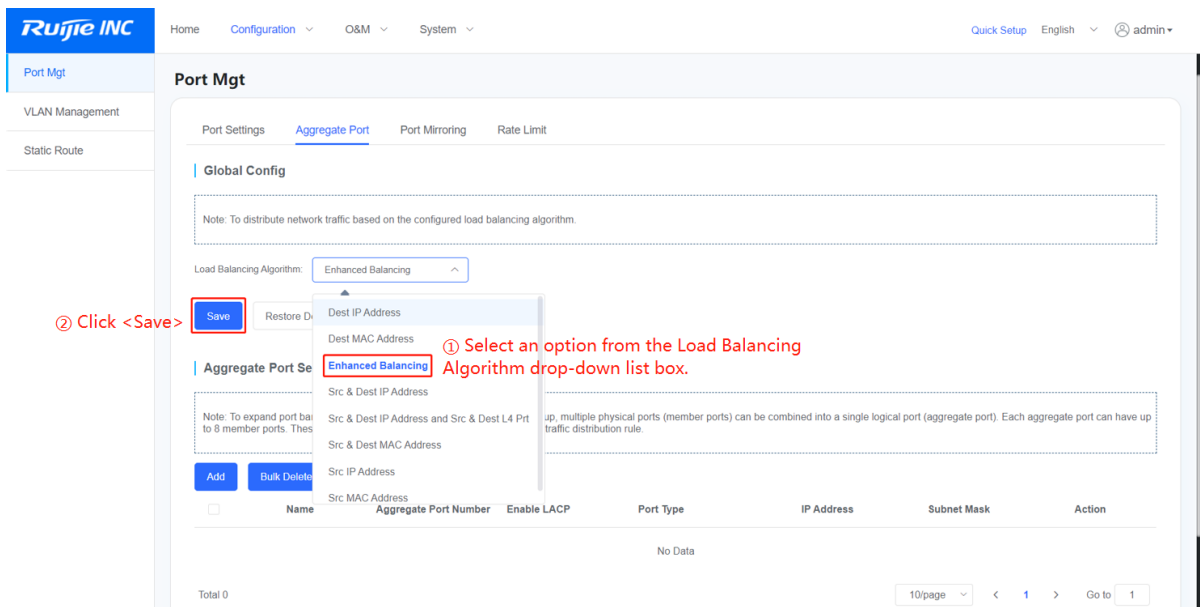
Click **Details**. You can view detailed information about a selected port.

Port Aggregation

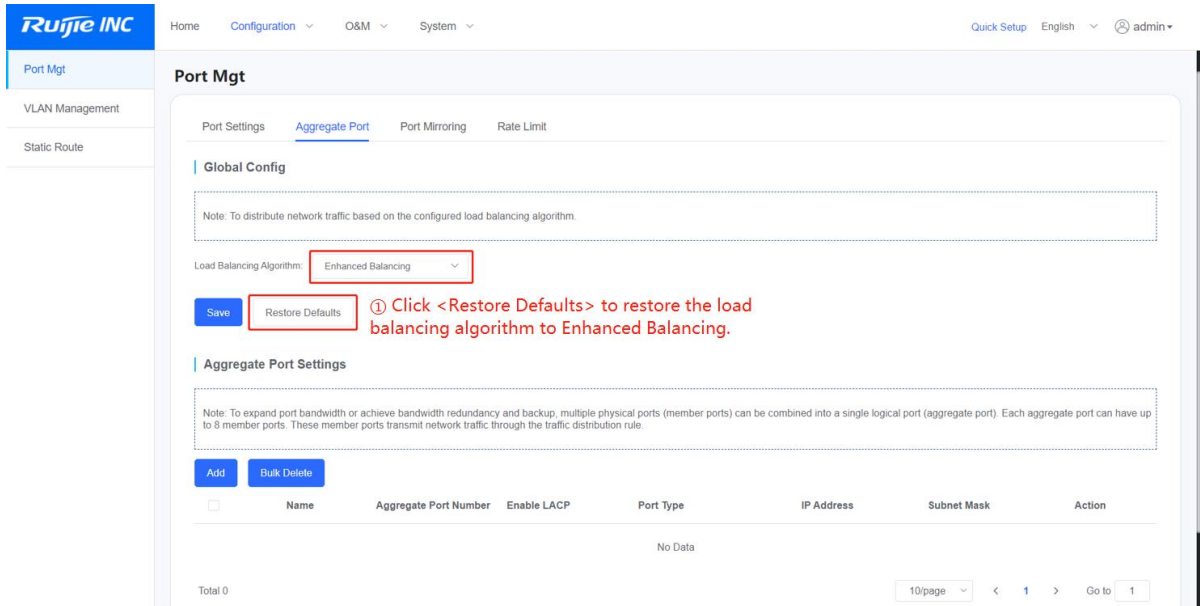
Note

To increase bandwidth or provide redundancy, multiple physical ports (member ports) can be combined into a single logical port (aggregated port). Each aggregated port can have up to 8 member ports. These member ports transmit network traffic based on traffic distribution rules.

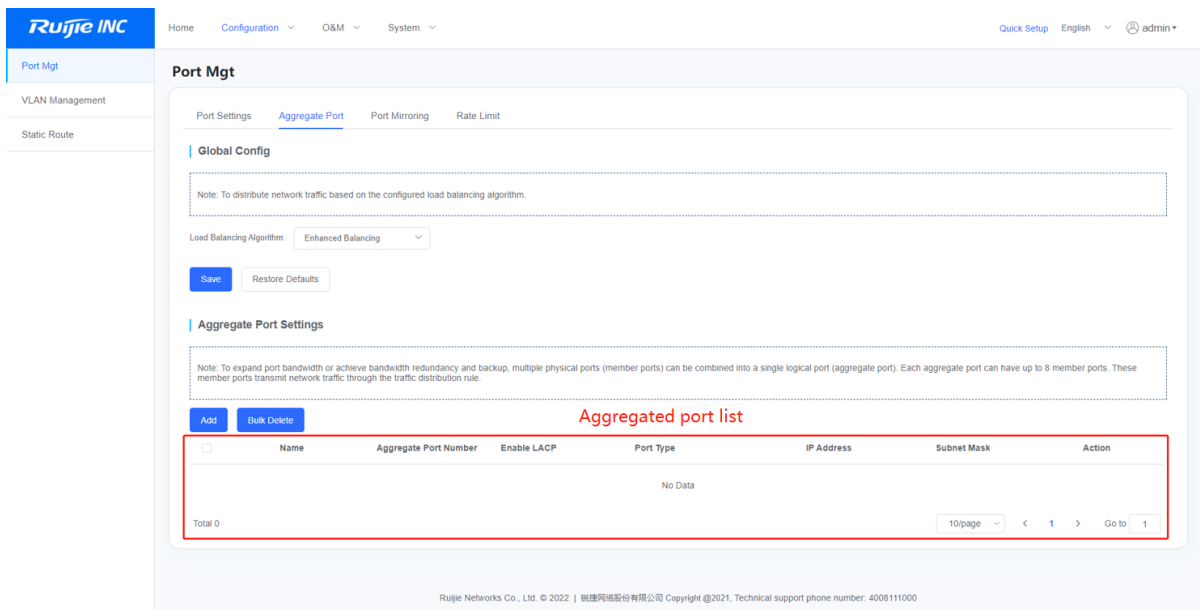
● Saving configurations



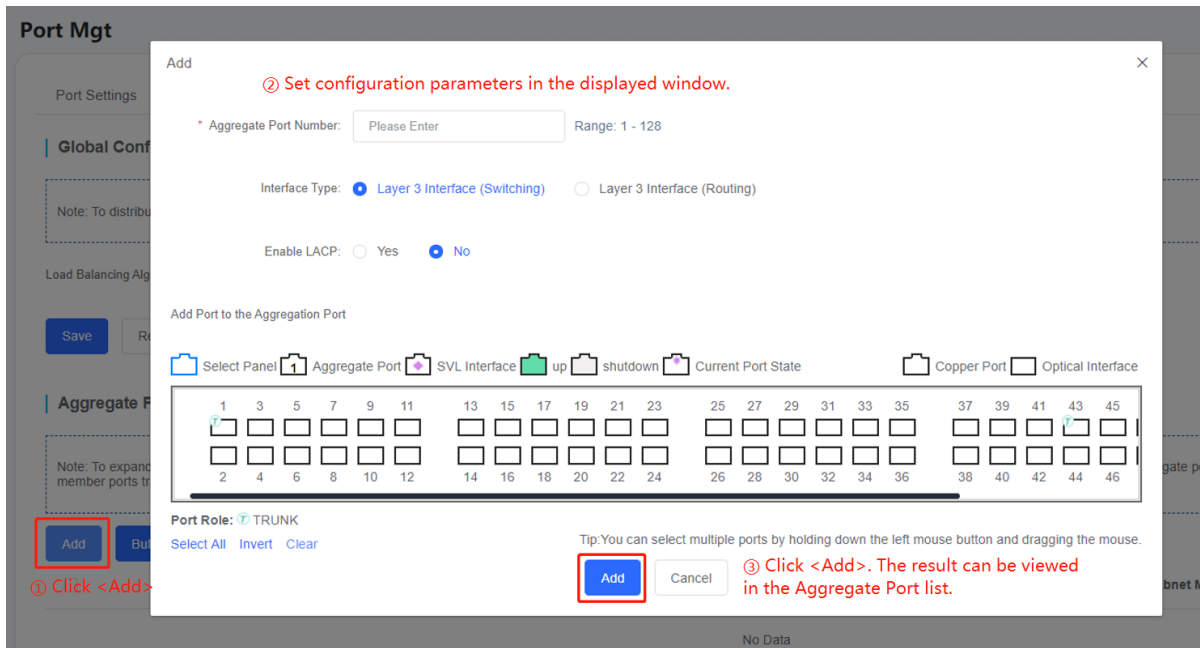
● Restoring default settings



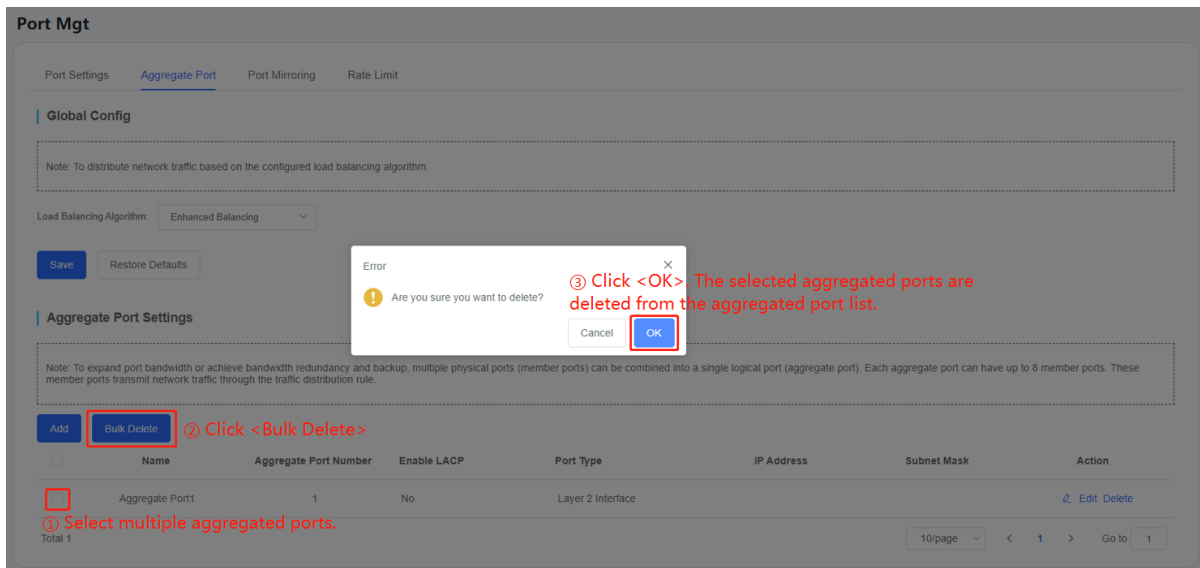
● Querying the aggregated port list



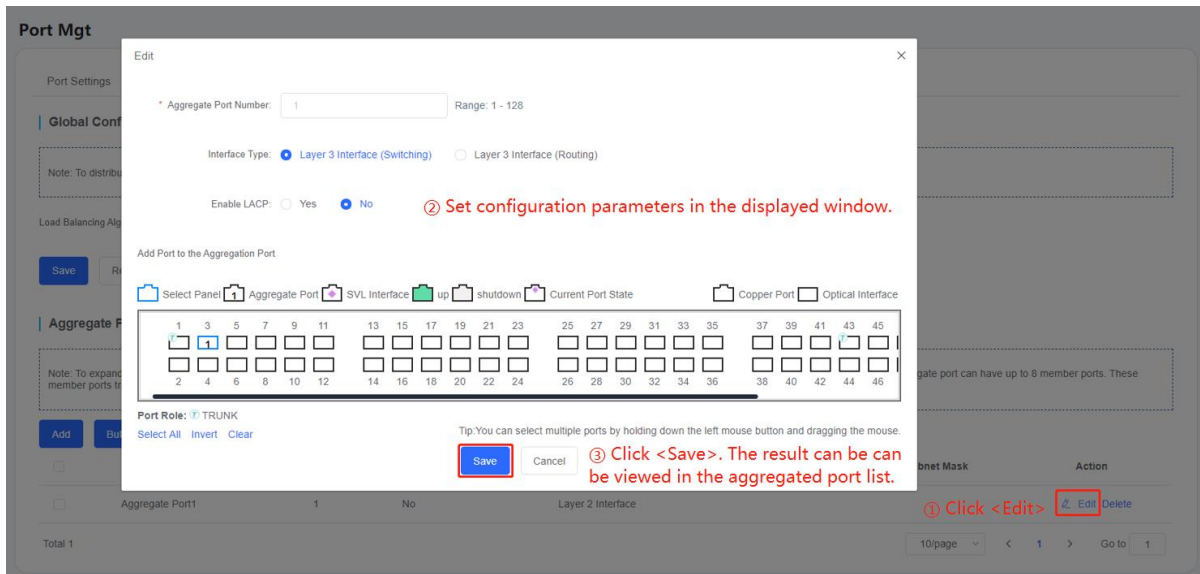
● Adding an aggregated port



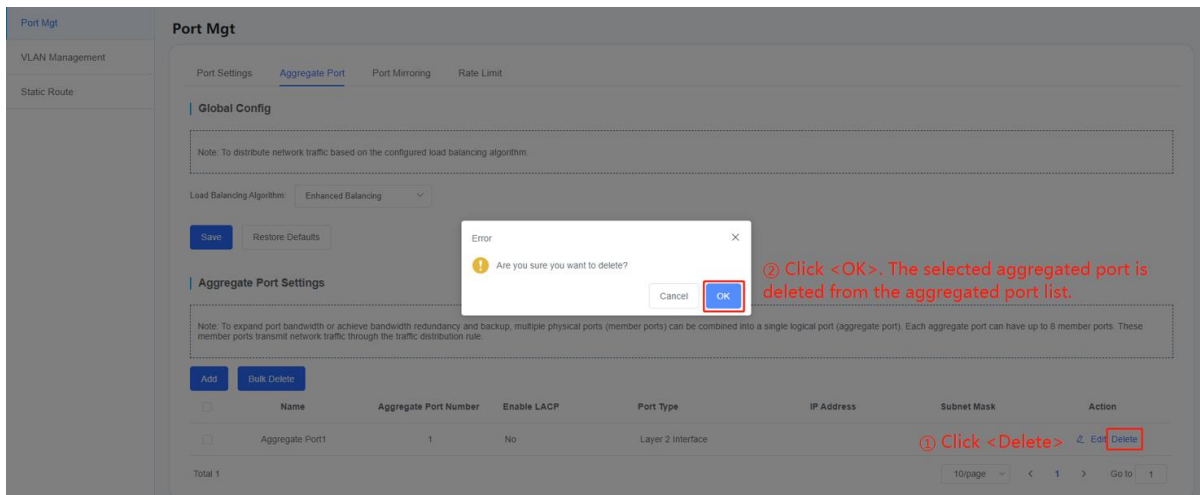
● Deleting multiple aggregated ports



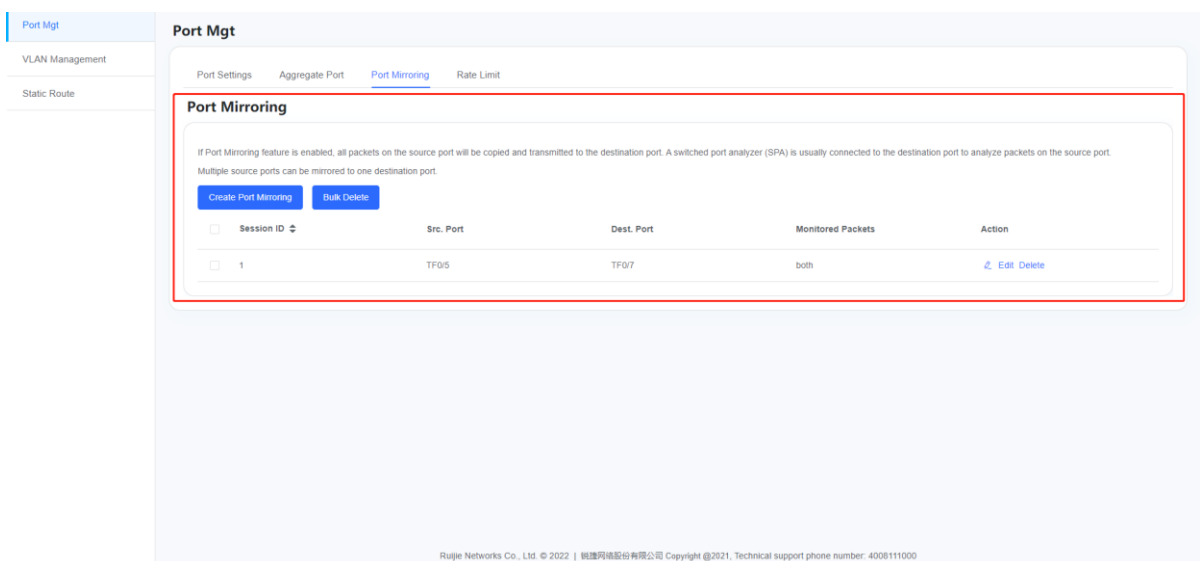
● Editing an aggregated port



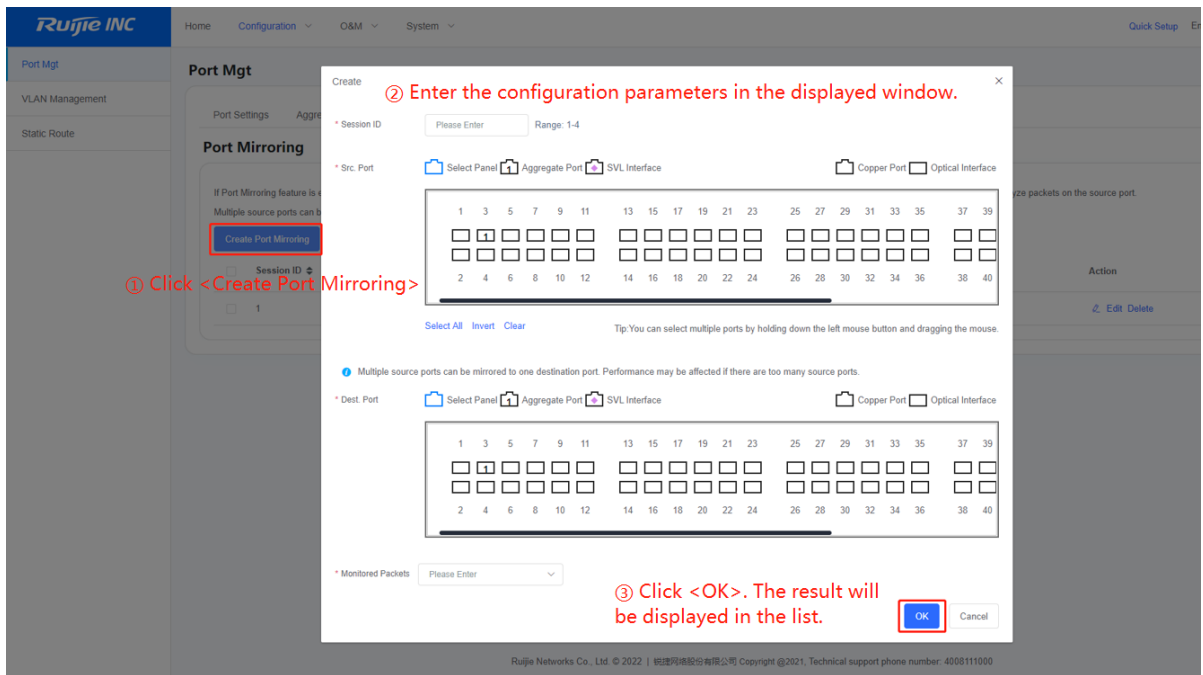
● Deleting an aggregated port



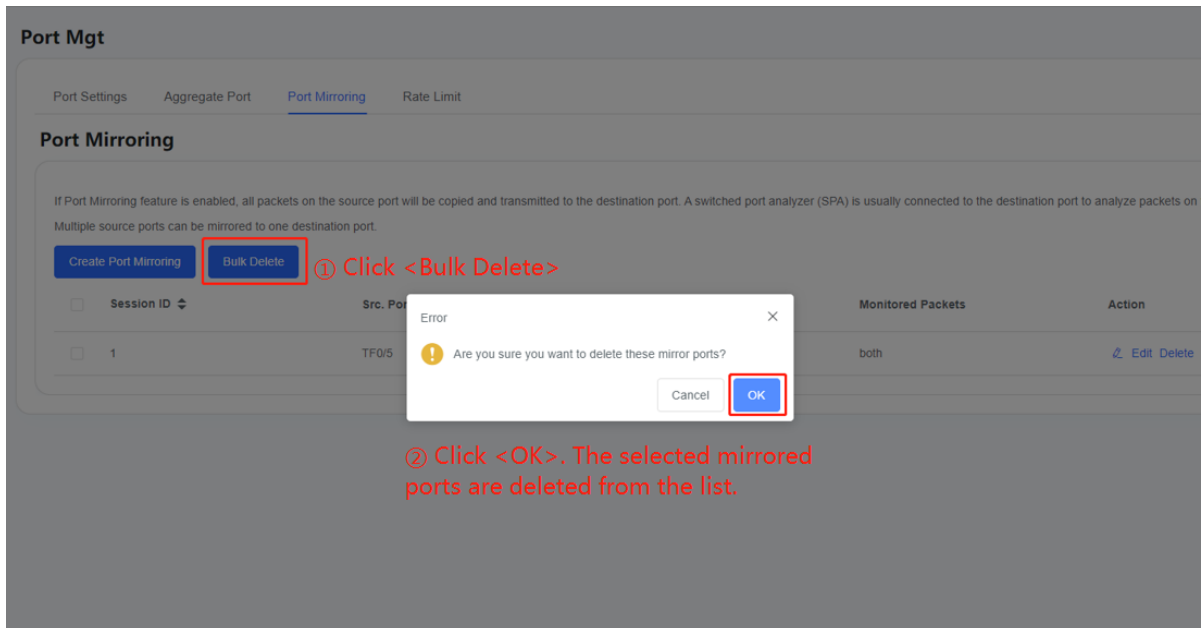
Port Mirroring



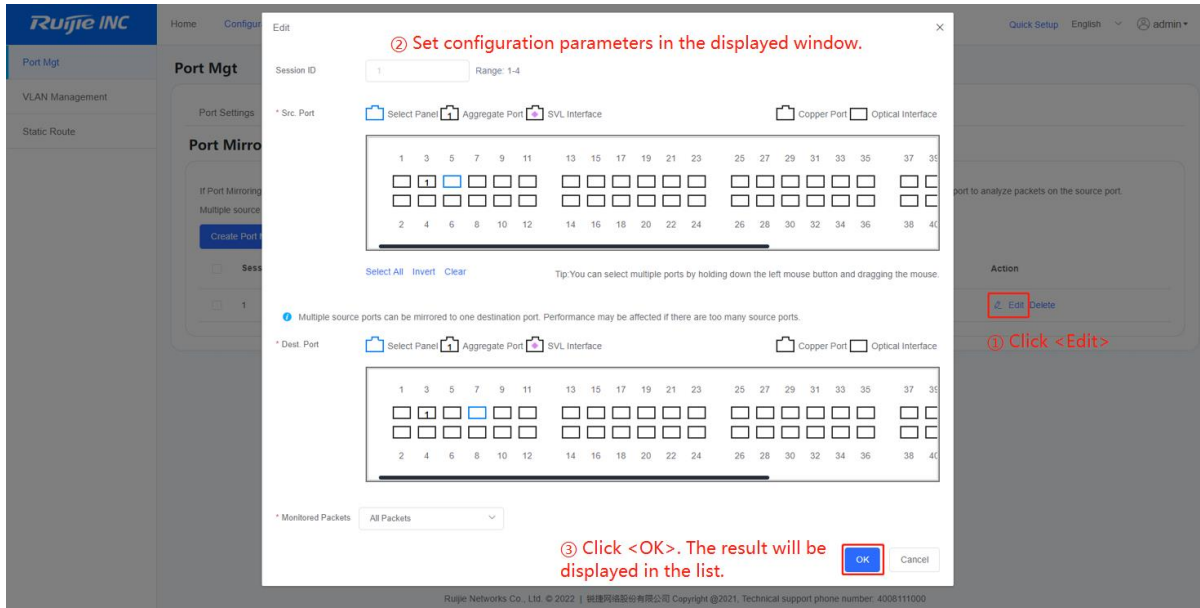
● **Creating port mirroring**



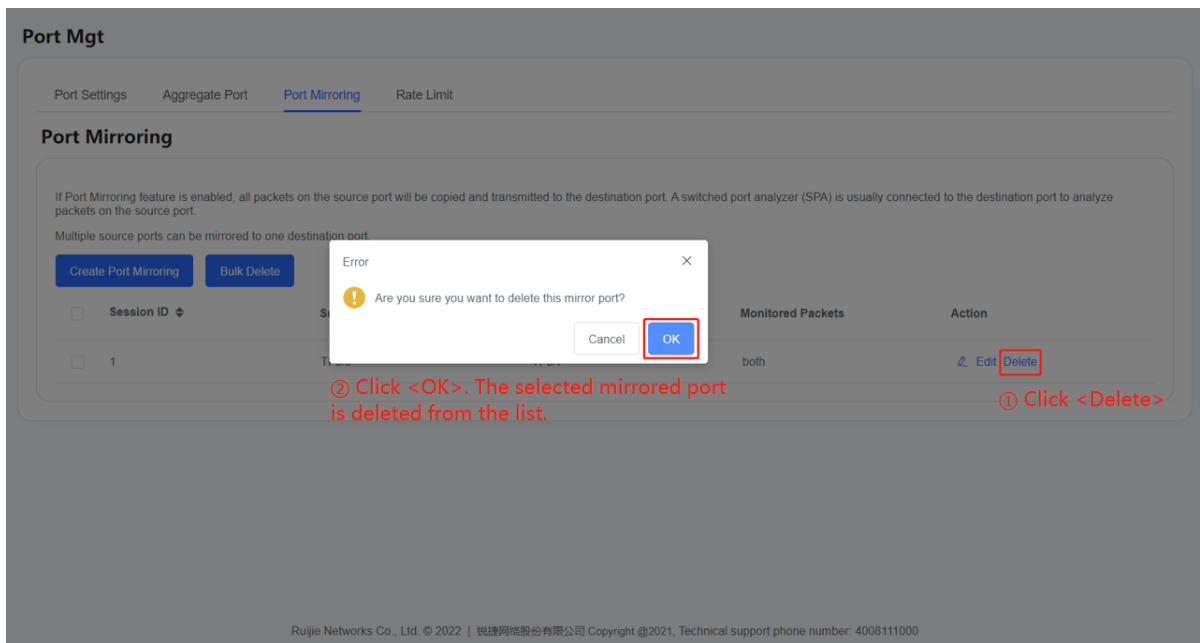
● **Deleting multiple mirrored ports**



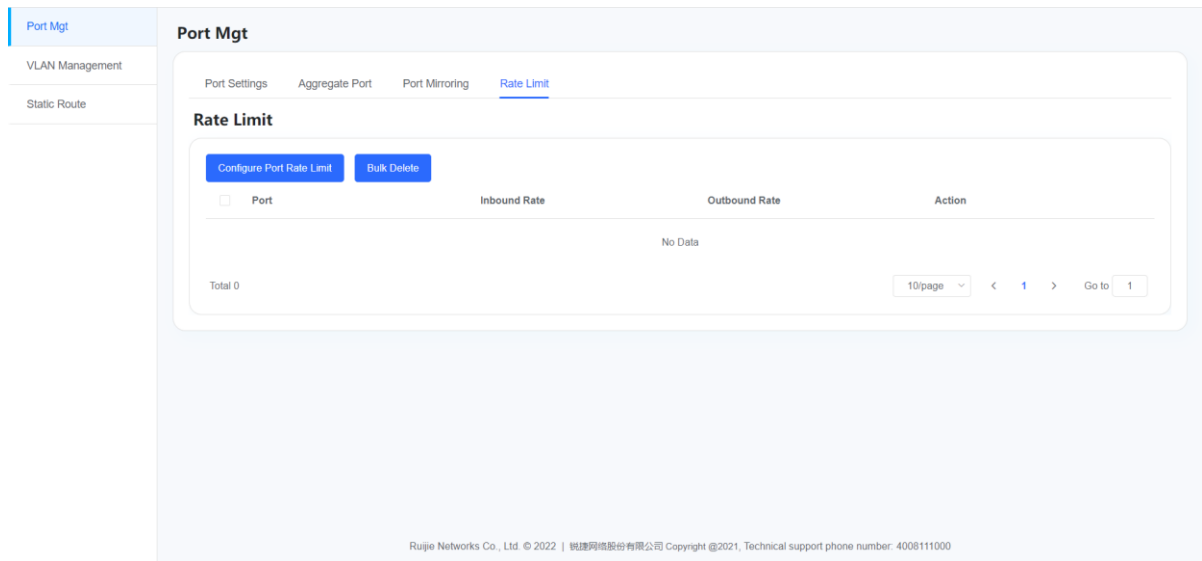
● **Editing a mirrored port**



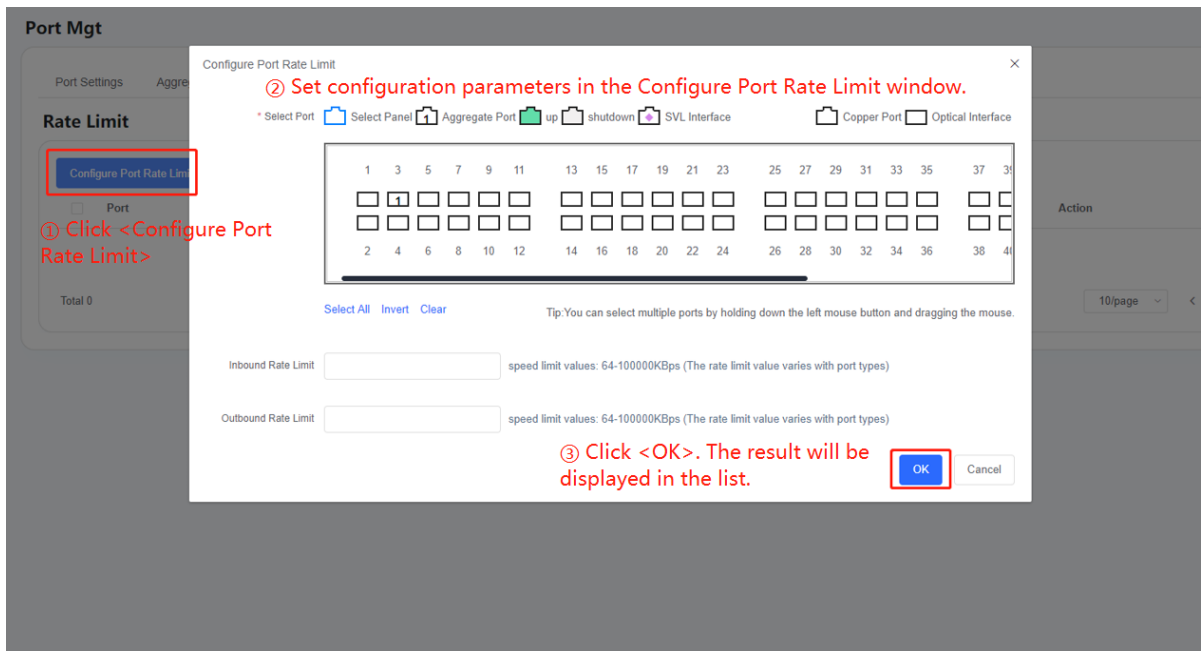
● Deleting a mirrored port



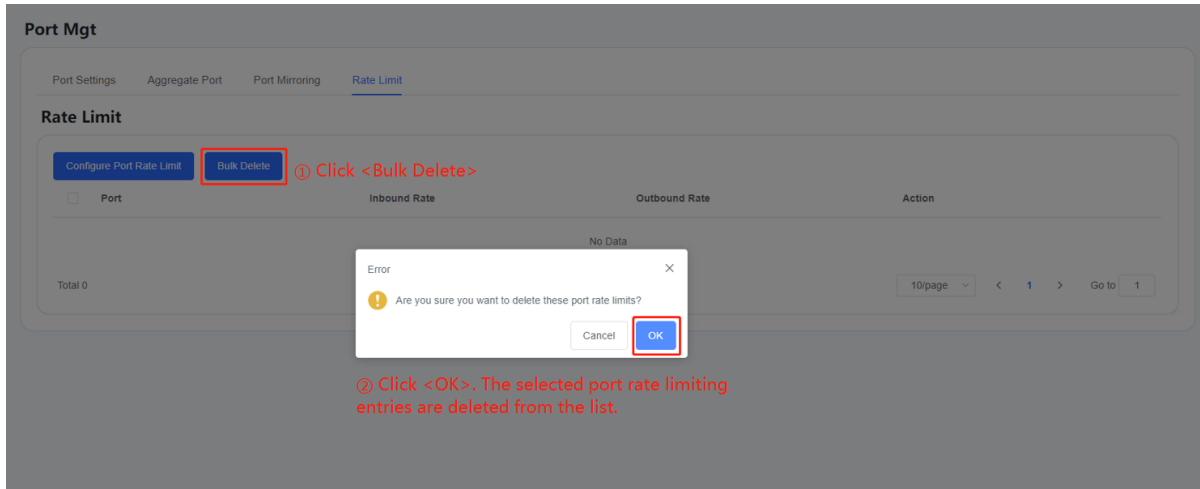
Rate Limiting



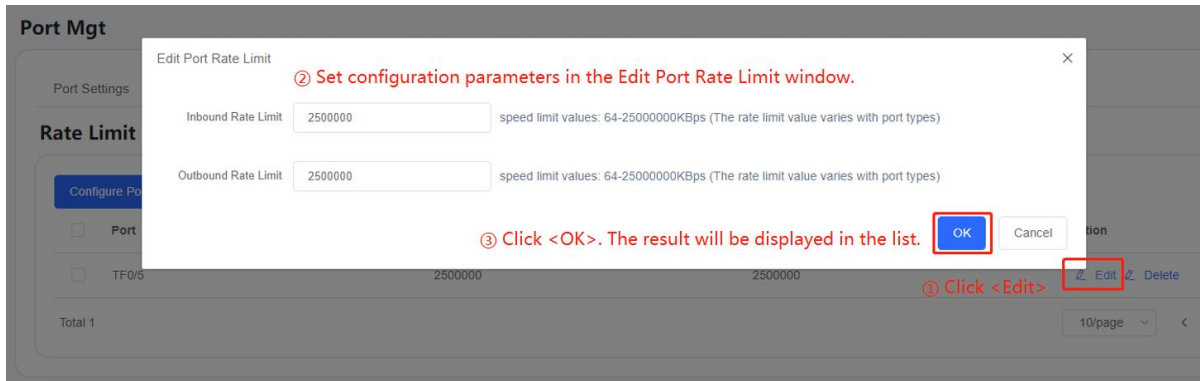
- **Configuring port rate limiting**



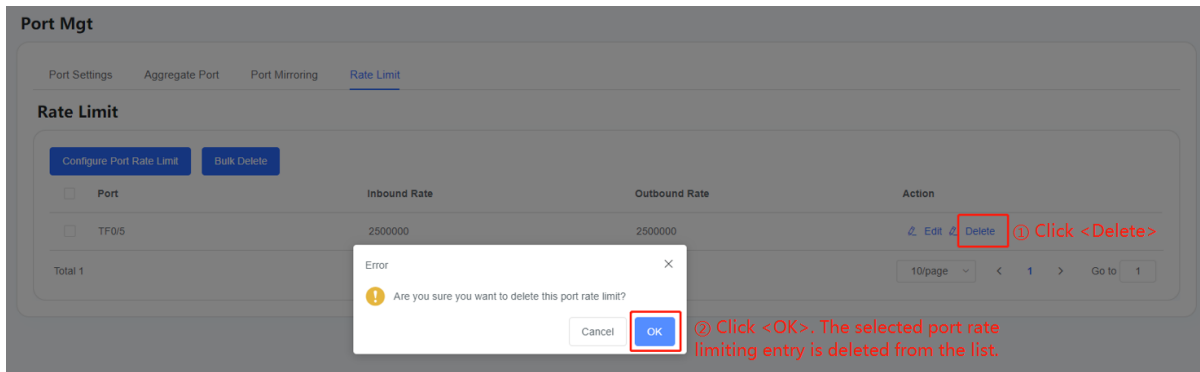
- **Deleting multiple rate limiting entries**



● Editing a port rate limiting entry



● Deleting a port rate limiting entry



2. VLAN Management

VLAN Management

① Click <Bulk Add> ② Click <Add>

③ Click <Delete Selected VLAN>

④ Click <Edit>

⑤ Click <Delete> to delete a single VLAN.

⑥ Jump to a certain page

VLAN ID	VLAN Name	VLAN Status	Port	Action
1	VLAN0001	STATIC	TF0/2,TF0/4,TF0/6-12,TF0/14-48,HundredG10/49-56,Ag1	Edit
2	222	STATIC	TF0/5,TF0/43,HundredG0/55	Edit Delete
3	333	STATIC	TF0/1,TF0/13,TF0/43,HundredG0/55	Edit Delete

Total 3

10/page < 1 > Go to 1

Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright ©2021, Technical support phone number: 4008111000

- Adding multiple VLANs

To add multiple VLANs, click **Bulk Add** and the **Bulk Add** window is displayed. Enter the VLAN ID and click **Done**.

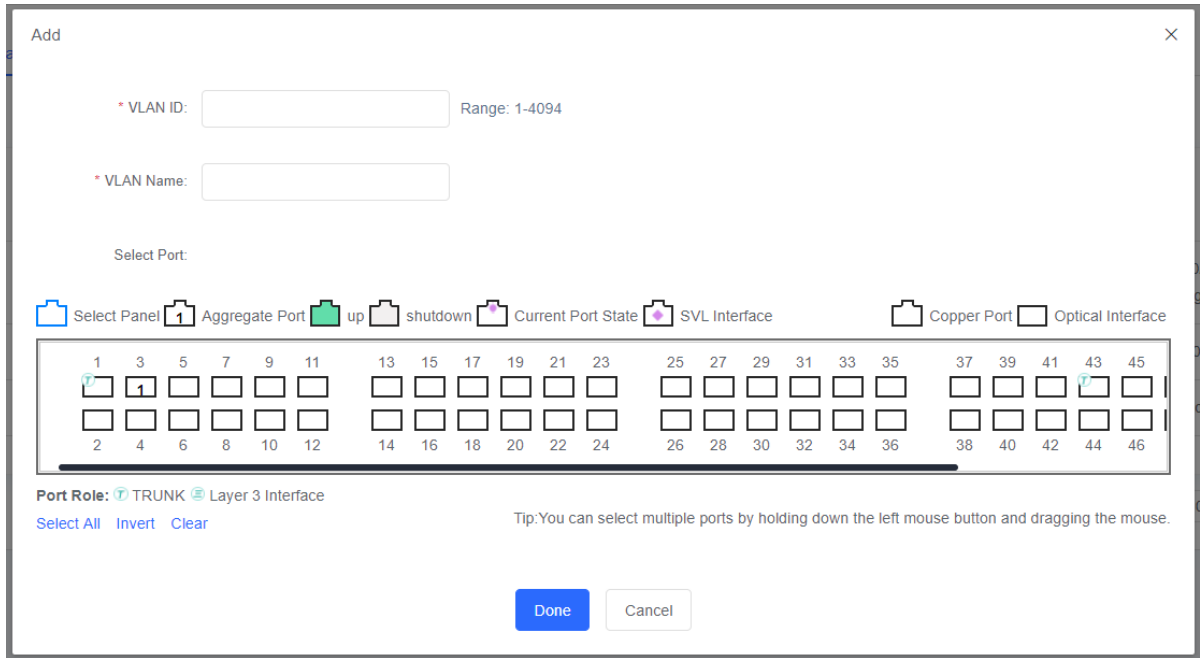
Bulk Add

* VLAN ID: Range: 1-4094; Format: (3-5,200)

Done Cancel

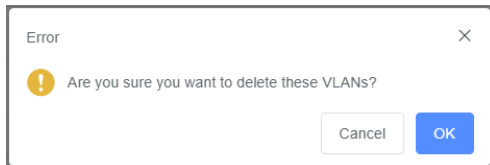
- Adding a single VLAN

To add a single VLAN, click **Add** and the **Add** window is displayed. Set configuration parameters and click **Done**.



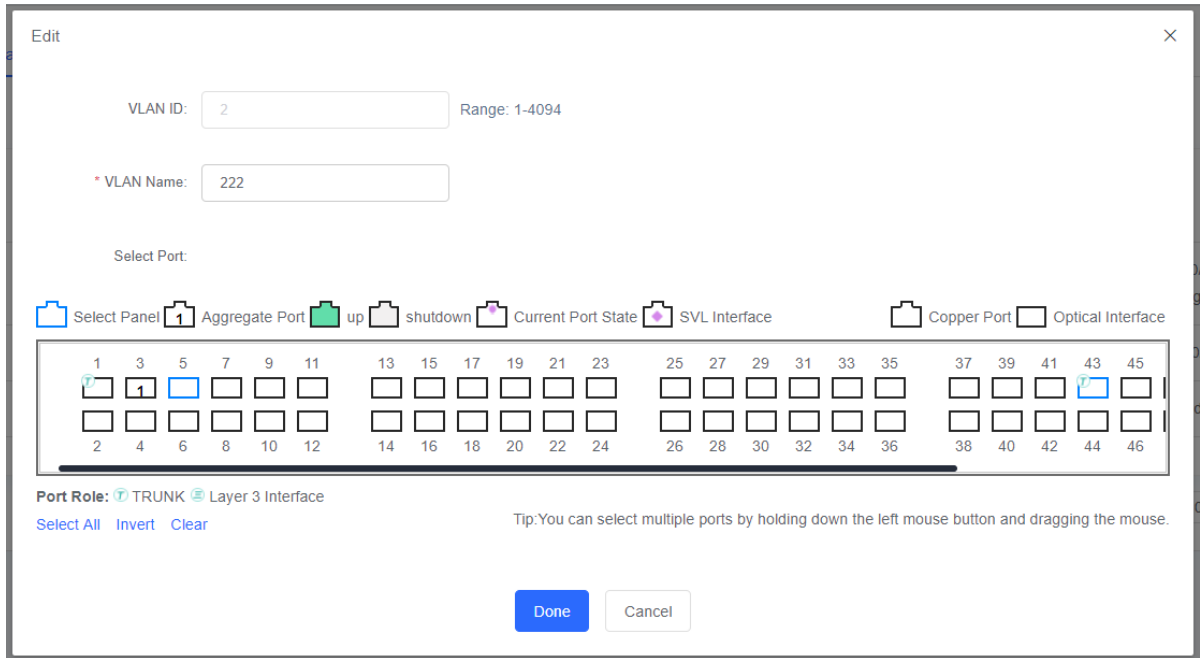
● **Deleting multiple VLANs**

To delete the selected VLANs, click before each VLAN to select multiple VLANs, then click . The error message is displayed. Click .



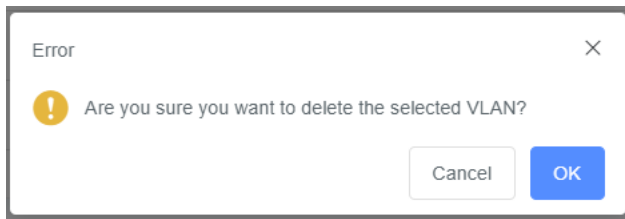
● **Editing a VLAN**

To edit a VLAN, click , and the **Edit** window is displayed. Set configuration parameters and click .

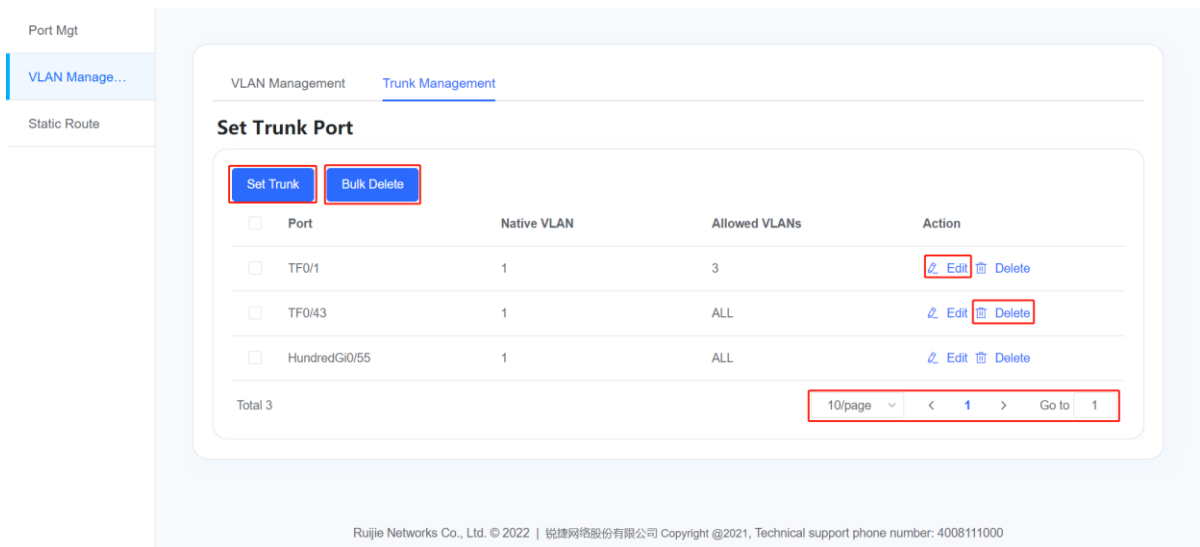


● **Deleting a VLAN**

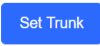

To delete a VLAN, click **Delete**. The **Error** dialog box is displayed. Click **OK**.

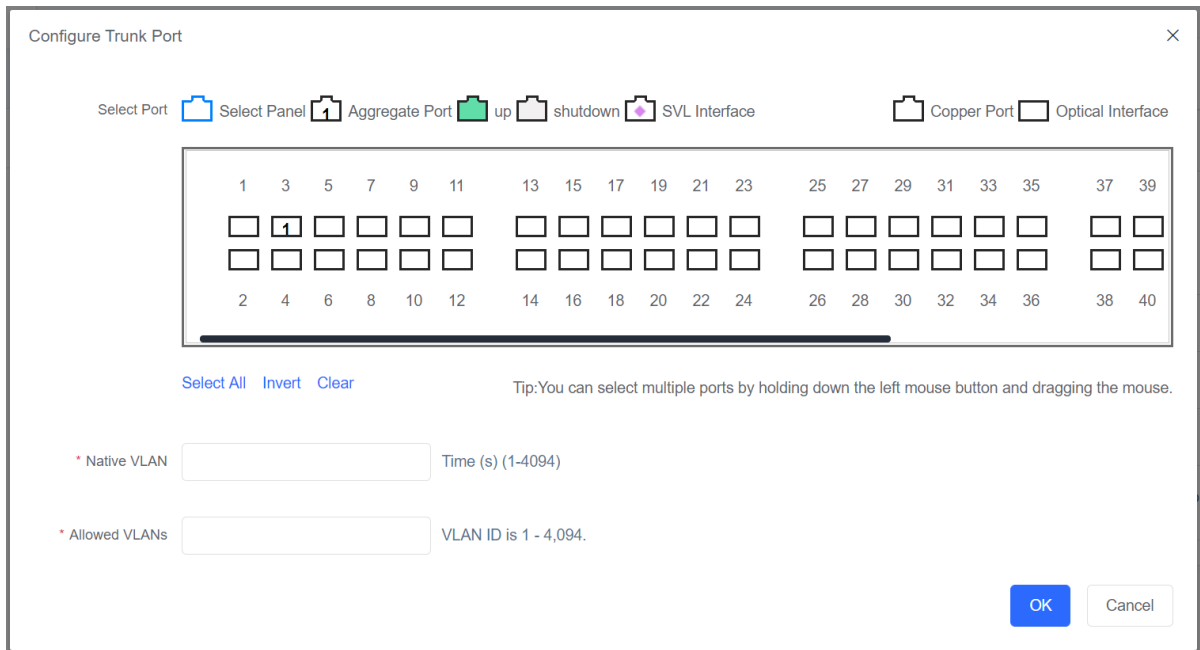


Trunk Management





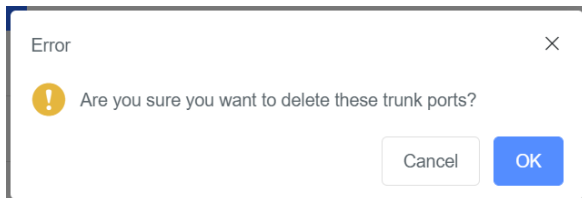
● **Setting a Trunk port**

To set a trunk port, click . The **Configure Trunk Port** window is displayed. Set configuration parameters and click .





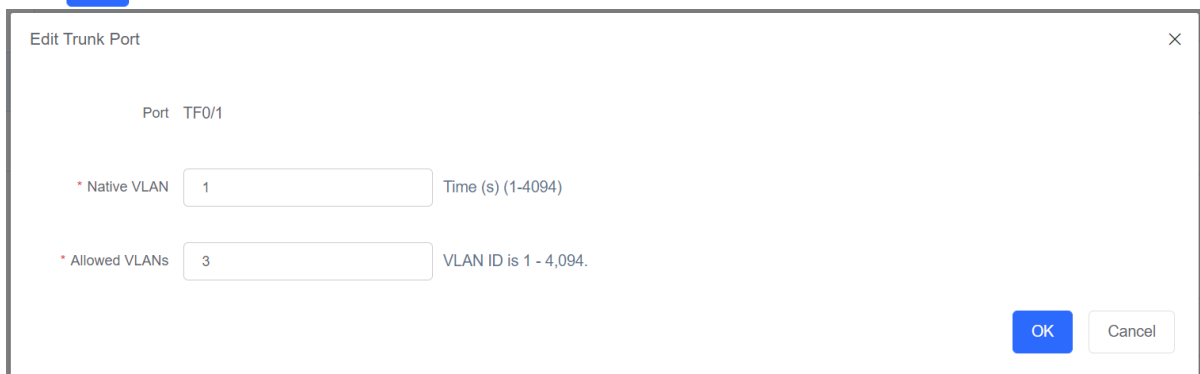
● **Deleting multiple trunk ports**

To delete multiple trunk ports, click next to each trunk port to select multiple trunk ports, and then click . The **Error** dialog box is displayed. Click .





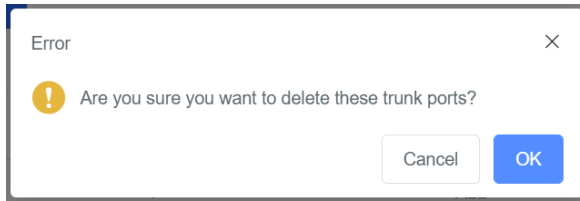
● **Editing a trunk port**

To edit a Trunk port, click  **Edit**. The **Edit Trunk Port** window is displayed. Set configuration parameters and click .



- **Deleting a trunk port**

To delete a selected trunk port, click  **Delete**. The **Error** dialog box is displayed. Click .





3. Static Route

Packets destined for a specified destination network are routed along a pre-determined path when a static route is configured. The routing priority is source in source out > forward DNS proxy > policy-based routing > user-defined routing and app-based routing > static route > auto routing > multi-link load balancing and default route.

 **Note**

The system supports up to 32 equal-cost routes to the same destination subnet. If over 32 equal-cost routes are configured, only the 32 equal-cost routes that are configured first will take effect.

The screenshot shows the 'Static Route' configuration page. On the left is a navigation menu with 'Port Mgt', 'VLAN Manage...', and 'Static Route' (selected). The main content area includes a title 'Static Route' and a description: 'Static Route: By adding a static route, packets destined for a specified destination network are routed along a predetermined path.' Below this is a breadcrumb trail: 'Routing Preferences: Source In Source Out > Forward DNS Proxy > Policy Routing > User Routing and Application Routing > Static Routing > Address Base Auto Routing > Multi-Link Load Balancing and Default Routing'. There are three buttons: 'Add Static Route', 'Add Default Route', and 'Delete Selected Route'. A note states: 'Note: The system supports configuring 32 equal-cost routes to the same destination network segment. If the number of equal-cost routes is greater than 32, only the first 32 equal-cost routes take effect.' A table lists the configured routes:

<input type="checkbox"/>	Dest. Segment	Dest. Mask	Next Hop IP	Router Outbound Interface	Administrative Distance	Type	Action
<input type="checkbox"/>	0.0.0.0	0.0.0.0	10.110.60.1		1	Default Route	 

At the bottom, it shows 'Total 1' and a pagination control: '10/page', '<', '1', '>', 'Go to 1'. The footer contains: 'Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright ©2021, Technical support phone number: 4008111000'.

- **Adding a static route**

To add a static route, click **Add Static Route**. The **Add Static Route** window is displayed. Set configuration parameters and click .

Add Static Route

IP Type: IPv4 IPv6

* Dest. Segment: Example: 172.29.1.0

* Dest. Segment Mask: Example: 255.255.255.0 Here, an IPv4 address is configured.

* Administrative Distance: Time (s) (1-255)

* Next Hop IP: Example: 172.29.13.1

Outbound Interface: Please Select

Done Cancel

- **Adding a default route**

To add a default route, click **Add Default Route**. The **Add Default Route** window is displayed. Set configuration parameters and click **Done**.

Add Default Route

IP Type: IPv4 IPv6

* Administrative Distance: Time (s) (1-255)

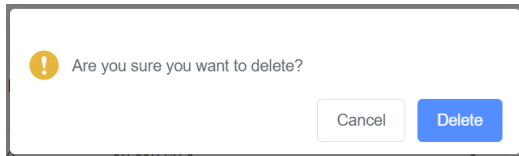
* Next Hop IP: Example: 172.29.13.1

Outbound Interface: Please Select



Done Cancel

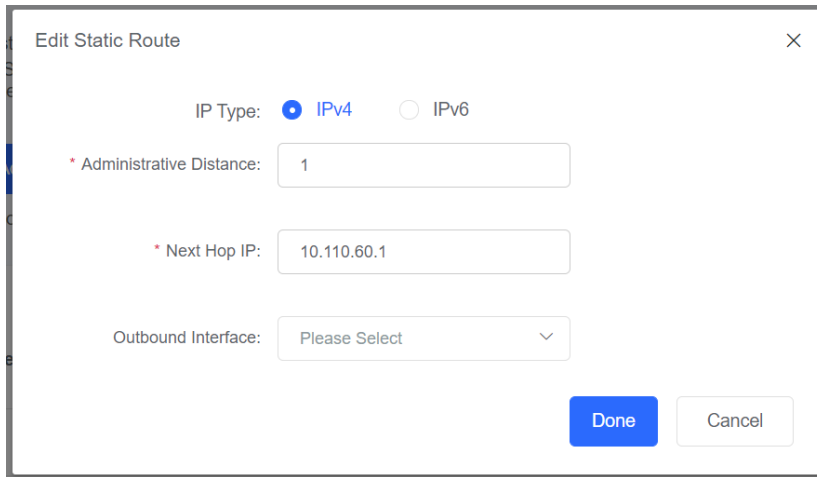
- **Deleting the selected routes**

To delete the selected routes, click next to each route to select multiple routes, and then click **Delete Selected Route**. A dialog box is displayed. Click **Delete**.



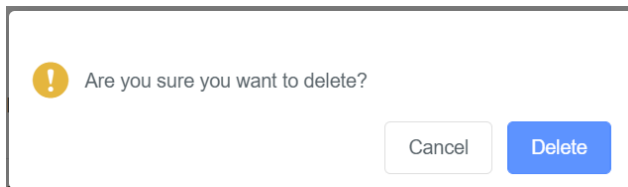
- **Editing a static route**

To edit a route, click  **Edit**. The **Edit Static Route** window is displayed. Set configuration parameters and click .



- **Deleting a static route**

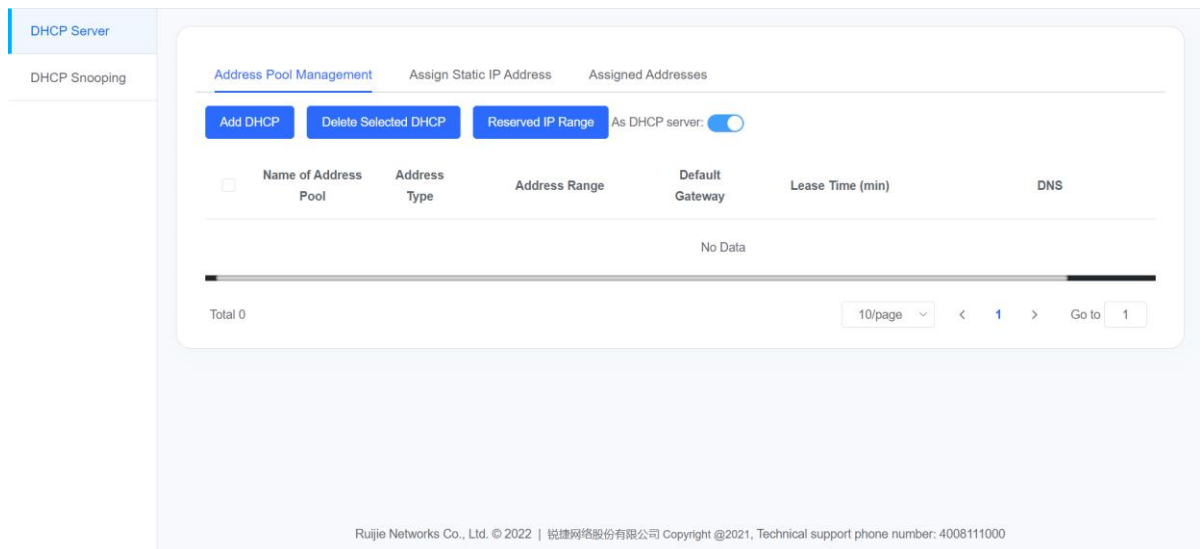
To delete a static route, click  **Delete**. A dialog box is displayed. Click .



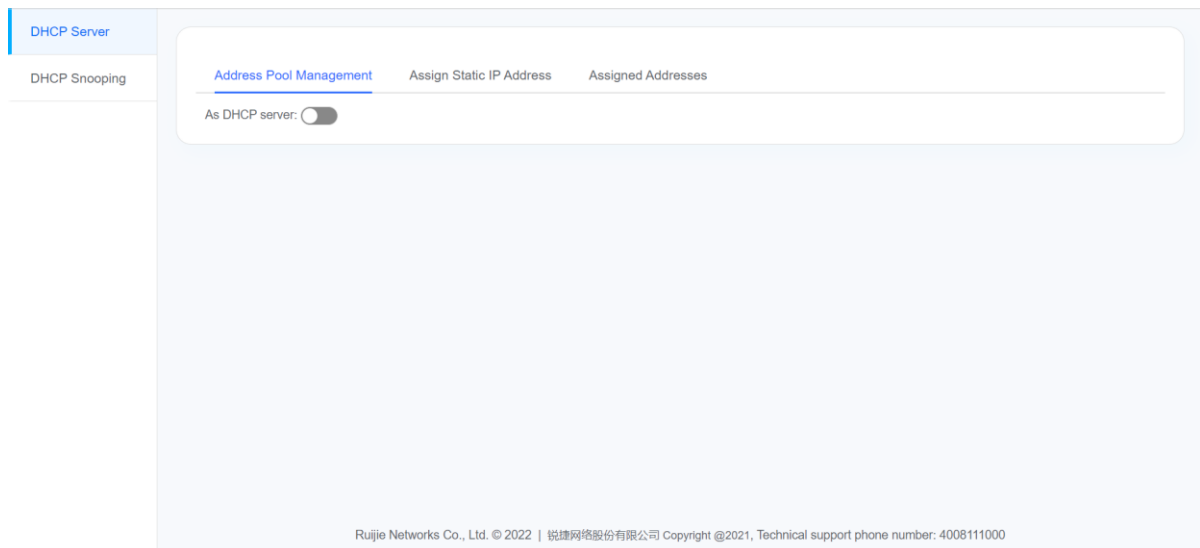
4. DHCP Server

DHCP Address Pool Management

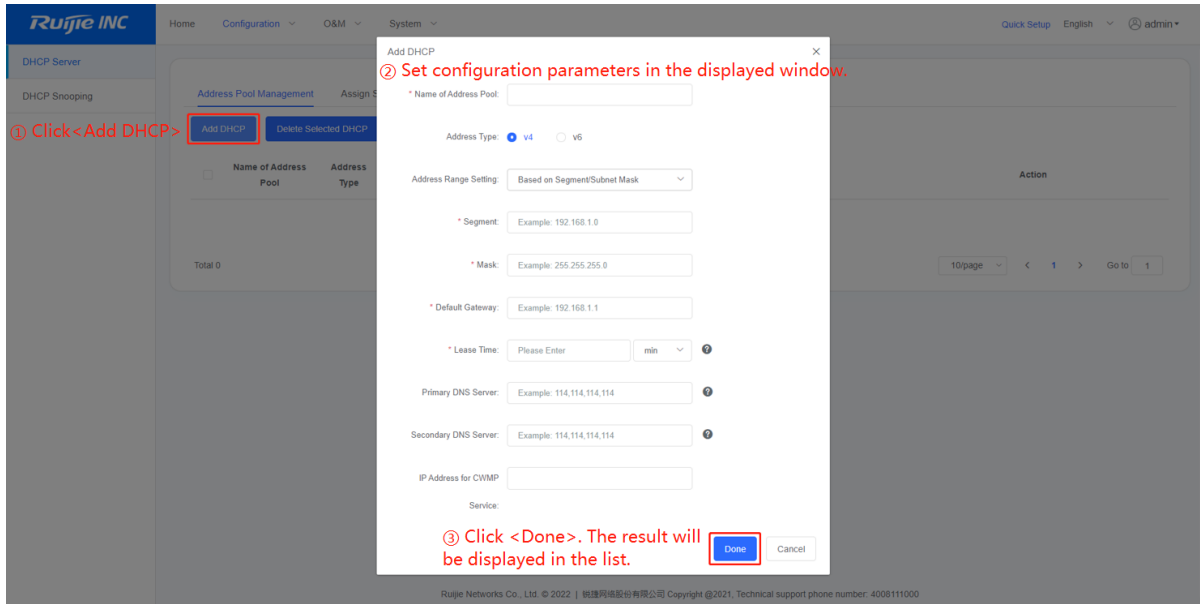
- **Enabling the DHCP server**



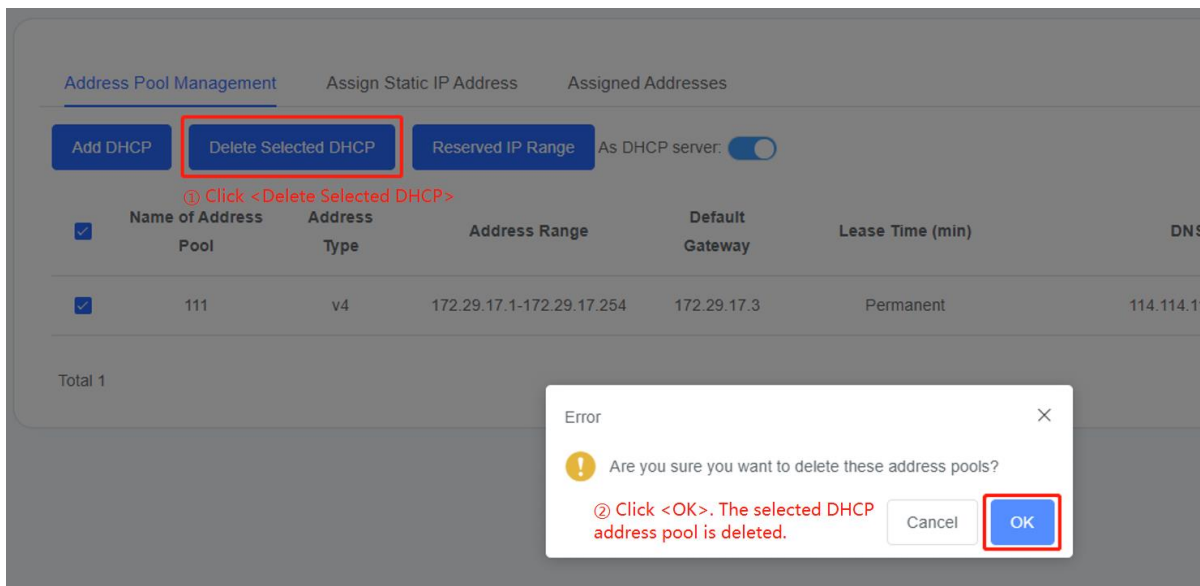
- **Disabling the DHCP server**



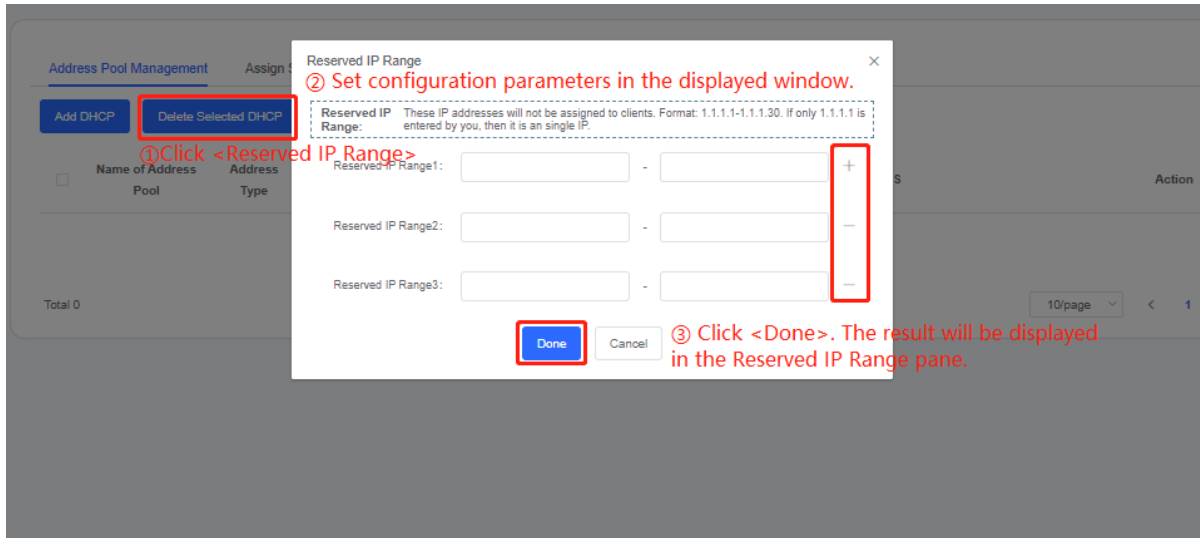
- **Adding a DHCP address pool**



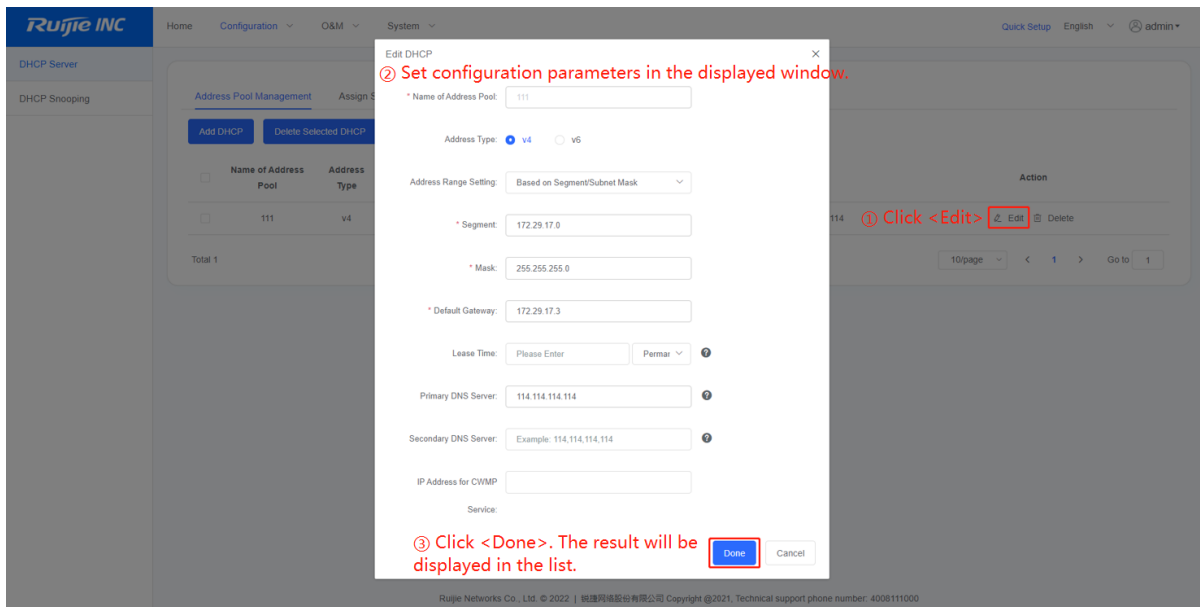
● **Deleting the selected DHCP address pool**



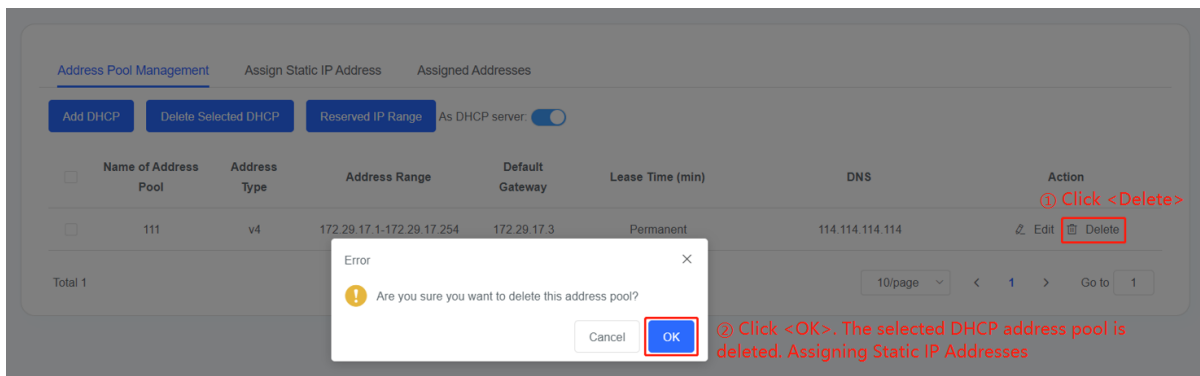
● **Configuring the reserved IP range**



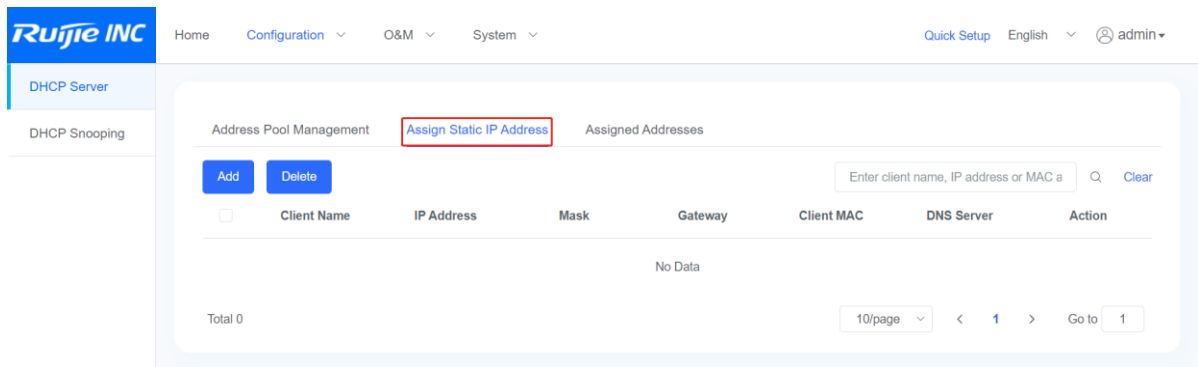
● Editing a DHCP address pool



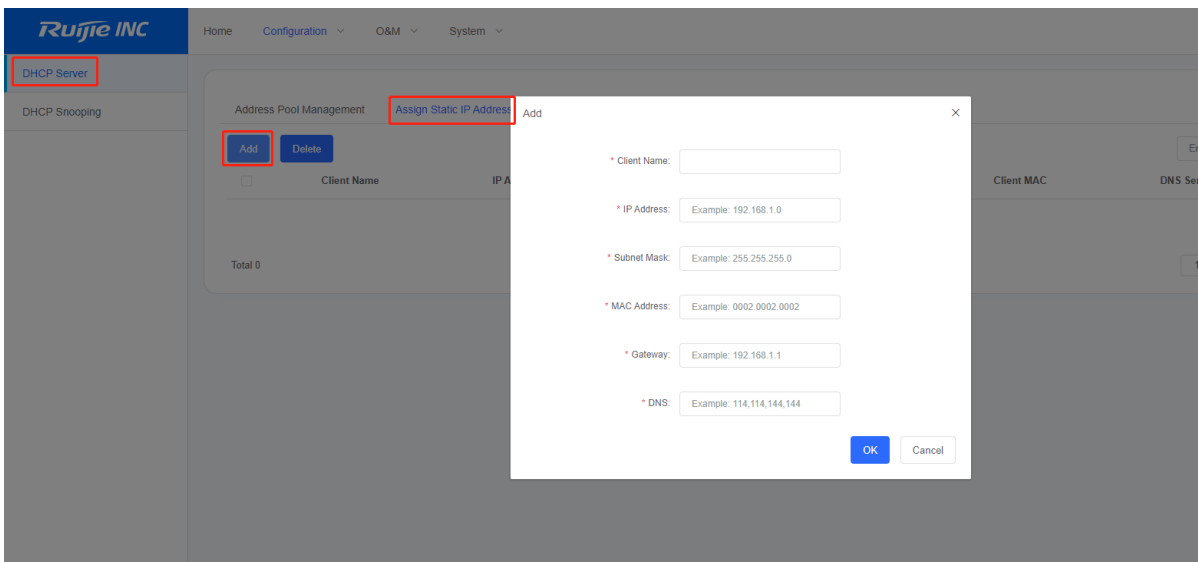
● Deleting a DHCP address pool



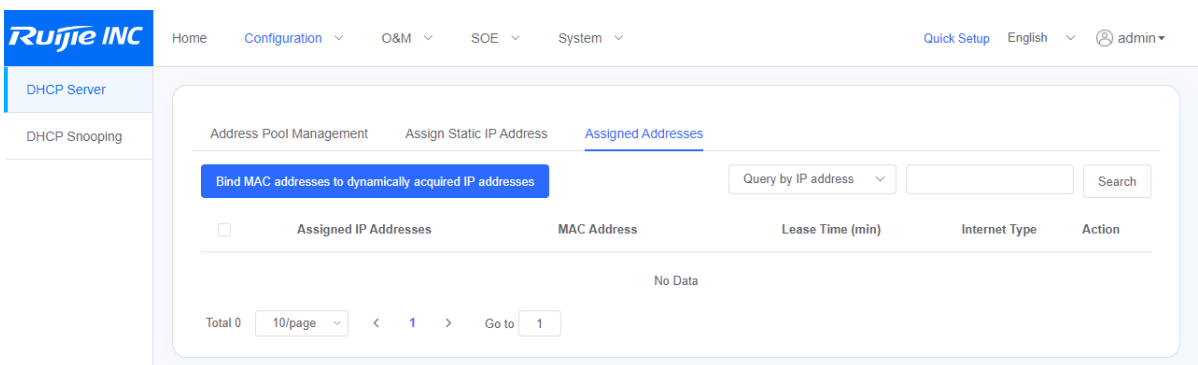
Assigning Static IP Addresses



- Choose **DHCP Server > Assign Static IP Address > Add** to access the **Add static IP address** page and add a static IP address.



The Assigned IP Addresses Page



5. Configuring DHCP Snooping

DHCP Snooping

DHCP listening function can listen to DHCP messages in the network, the correct client IP, MAC, Vlan, interface and other information recorded to the legitimate client library (software table). In conjunction with IP Source Guard, ARP Inspection and other features, ARP spoofing and IP source address spoofing can be prevented in dynamic IP address environments.

In addition, by dividing interfaces into trusted interfaces and untrusted interfaces, only trusted DHCP servers are allowed, and illegal DHCP servers are blocked to prevent DHCP server spoofing.

You are advised to enable this function on access switches.

Note: If this feature is enabled, WEB MAB authentication, obtaining MAC addresses through commercial marketing authentication, and obtaining MAC addresses through local server authentication will fail.

DHCP Snooping Enabled **1 Enable or disable DHCP snooping.**

Configure Trusted Interface

Please select the interface (usually an uplink interface) that connects to a valid DHCP server as a trusted interface. Any unselected interface is an untrusted interface.

The system will only forward DHCP reply messages from trusted interfaces. Requests from DHCP client will be forwarded only to trusted interfaces.

If the DHCP service is enabled on the local device, you do not need to configure the trust interface.

If the DHCP service is not enabled on the local device, you must correctly configure the trust interface. Otherwise, the client will not be able to get the MAC address.

2 Configure the interface connected to the DHCP server as a trusted interface.

Select Panel Aggregate Port up shutdown Current Port State Copper Port Optical Interface

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56

Current Trusted interface: Select All Invert Clear

3 Save the configuration.

Tip: You can select multiple ports by holding down the left mouse button and dragging the mouse.

6. Logs

Configuring the Log Server

Log Server

Syslog Upload

Syslog Upload Enabled

* IP of Upload Dest. Server:

* Port:

The port number is 514 by default. Please use a port with a port number between 1024 and 65,535. Make sure that the port is not used by other UDP packets.

Logging Level:

Logging level: 0 indicates a critical error, 1 indicates an error that needs to be corrected immediately, 2 indicates a critical error, 3 indicates an error that needs attention but is not critical, 4 indicates a warning that may exist, 5 indicates the information that needs attention, 6 indicates the general information, and 7 indicates the debugging information. The smaller the number, the more urgent and important the log is.

Logging through management

interface

Save

Configuring SNMP or the Trap Function

The Simple Network Management Protocol (SNMP) enables a network administrator to easily monitor and manage nodes on a network.

- **SNMP Version:** indicates the SNMP version supported by the switch, which can be SNMPv2 or SNMPv3.
- **Location:** indicates the location the switch.
- **SNMP Community String:** is used by the management host to connect to a switch.
- **Trap Community String:** is used to connect to the management host. When an alarm is generated on a

switch, the switch can send the alarm to the management host.

- **Trap receiver:** refers to the management host that receives alarms from a switch. A maximum of 10 trap receivers can be configured.

SNMPv3 is more secure than SNMPv2. The encryption password and authentication password of SNMP users need to be configured.

Only one SNMP version can be configured, that is, SNMP V2 or SNMP V3.

SNMP Version: V2 V3

Location:

* SNMP Community String:

Trap Community String: *Trap Community String must be the same as SNMP Community String.*

* Trap receiver: *A maximum of 10 Trap receivers can be configured. Multiple IP addresses must be separated by comma (,) or CRLF (\n).*

Only one SNMP version can be configured, that is, SNMP V2 or SNMP V3.

SNMP Version: V2 V3

Location:

* SNMP Community String:

Trap Community String: *Trap Community String must be the same as SNMP Community String.*

Encryption Key: *At least 8 characters long.*

Authentication Key: *At least 8 characters long.*

* Trap receiver: *A maximum of 10 Trap receivers can be configured. Multiple IP addresses must be separated by comma (,) or CRLF (\n).*

SNMP V2: Select V2 . Set configuration parameters and click to submit the configuration.

SNMP V3: Select V3 . Set configuration parameters and click to submit the configuration.

Clear: Click to clear the SNMPv2 or SNMPv3 configuration.

Configuring Telnet or SSH

i You can remotely connect, manage and configure this device through Telnet or SSH.

Telnet Service

SSH Service

Username: admin

* New Password: **i**

* Confirm Password:

Save

Telnet/SSH: Click **Telnet Service** to enable or disable the Telnet service, and click **SSH Service** to enable or disable the SSH service. The default user name is **admin**. Set configuration parameters and click **Save** to submit Telnet or SSH configurations. When both the Telnet service and SSH service are disabled, you do not need to set a password.

i You can remotely connect, manage and configure this device through Telnet or SSH.

Telnet Service

SSH Service

When configuring a switch through Telnet, you must log in with this password.

i **Note**

Remember the new password for login next time.

7. STP Loop Guard

Global Settings

The purpose of SPT Loop Guard feature is to discover and start an optimal tree topology of LAN to ensure stability of the network.
 SPT protocol: a protocol used to avoid broadcast storms caused by link loops and to provide redundant backup of links.

Enable STP Loop Guard

Priority: <input type="text" value="8"/> <small>Range: 0-</small>	Handshake Time: <input type="text" value="2"/> <small>Time (s): 1-</small>
<small>15. Default: 8</small>	<small>10. Default: 2</small>
Aging Time: <input type="text" value="20"/> <small>Time (s): 6-40.</small>	Forward Delay: <input type="text" value="15"/> <small>Time (s): 4-</small>
<small>Default: 20</small>	<small>30. Default: 15</small>
SPT Mode: <input type="text" value="MSTP"/> <small>▼</small>	
MST Name: <input type="text"/> <small>No more than 32 characters.</small>	MST Version: <input type="text" value="0"/> <small>Range: 0-65535. Default: 0</small>

Enable or disable STP Loop Guard: Click **Enable STP Loop Guard** to enable or disable STP loop guard.

Global Settings: Enable **STP Loop Guard** and set configuration parameters. There are three STP modes, which are STP, RSTP, and MSTP. Click to submit the global settings.

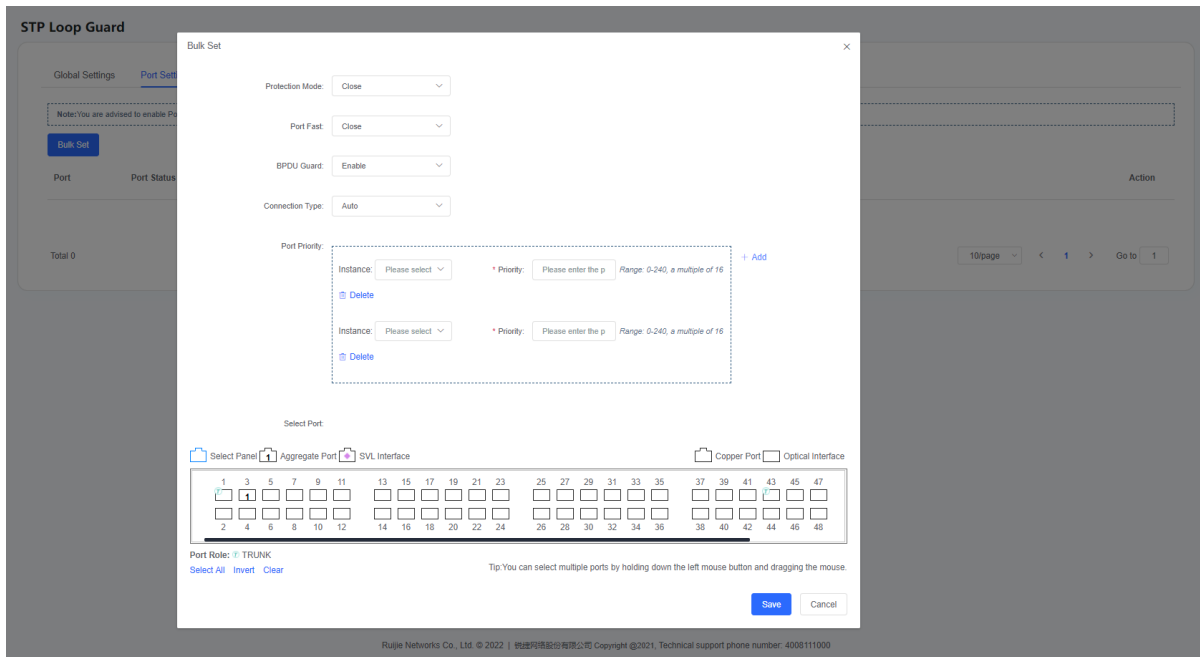
Port Settings

Note





You are advised to enable **Port Fast** on the port directly connected to a PC.

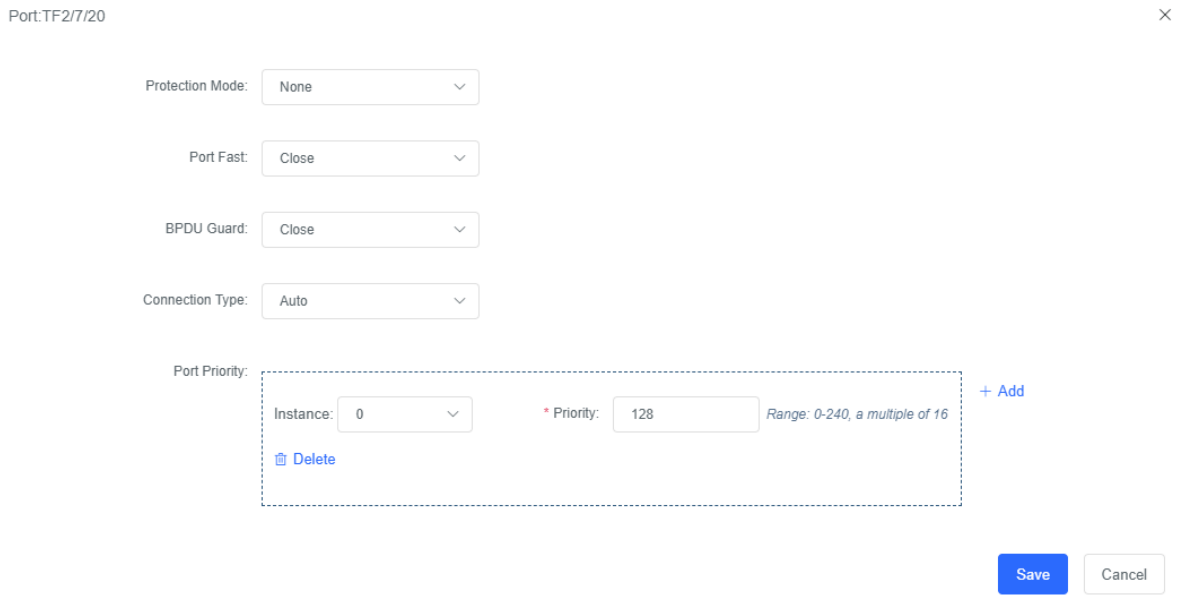
1. Setting the STP loop guard function for multiple ports

Click . The **Bulk Set** window is displayed. Set configuration parameters. Add or delete the port priority by clicking **+ Add** or **Delete**. Select multiple ports, and click to submit the configuration. Then the result will be displayed in the list.



2. Editing the STP loop guard function for a single port

Click  **Edit** in the **Action** column. A window is displayed. Set configuration parameters. Add or delete the port priority by clicking  **+ Add** or  **Delete**. Click  **Save** to submit the configuration. Then the result will be displayed in the list.



STP State

STP Loop Guard

Global Settings Port Settings **SPT State**

SPT State: Enable Configuring Spanning Tree

SPT Mode: MSTP

Root Bridge Status: Root Bridge

Instance:

Select Panel Port:

Select Panel
 Aggregate Port
 up
 shutdown
 Current Port State
 Copper Port
 Optical Interface

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56

Port Role: TRUNK
 Layer 3 Interface
 Root Port
 Designated Port
 All Port
 Master Port
 STP Port State: STP Enabled and Forwarding
 STP Enabled and Blocking
 STP Enabled
 Edge Port Enabled

Disable Edge Port: Select the Up port and click . The icon of Port 23 is changed to .

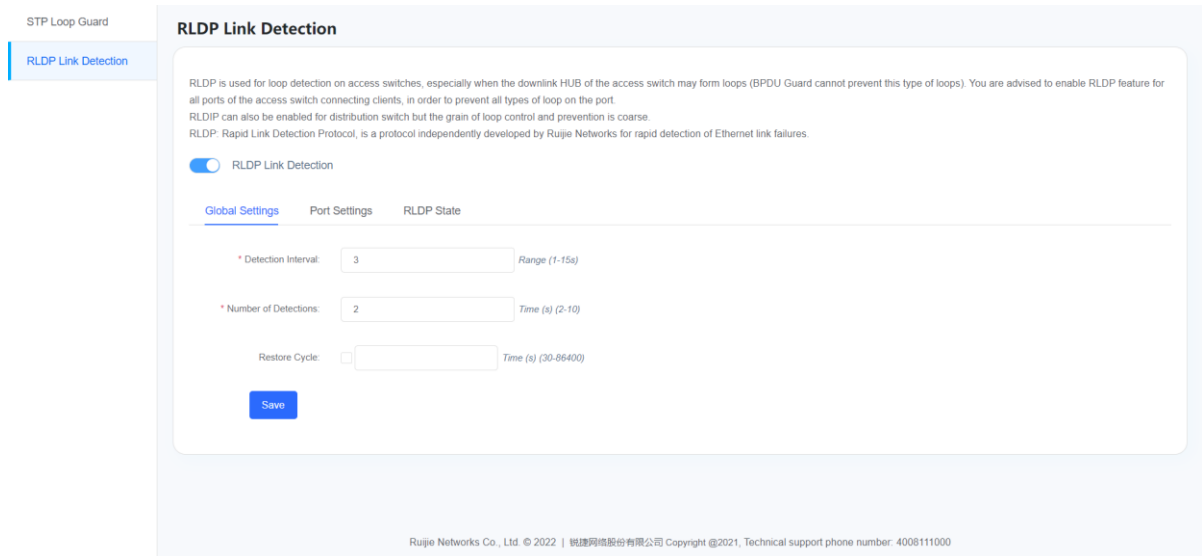
Enable Edge Port: Select the Up port and click . The icon of Port 23 is changed to .


8. RLDP Link Detection

The Rapid Link Detection Protocol (RLDP) is independently developed by Ruijie Networks for rapid detection of Ethernet link failures. It is used for loop detection on access switches in a specific situation where a loop occurs on the downstream hub of the access switch (BPDU guard cannot prevent this type of loops). You are advised to enable RLDP on all ports of the access switch connecting to clients, in order to prevent all types of loops on these ports.

RLDP can also be enabled for distribution switches, but the loop guard performance is coarse-grained.

Global Settings



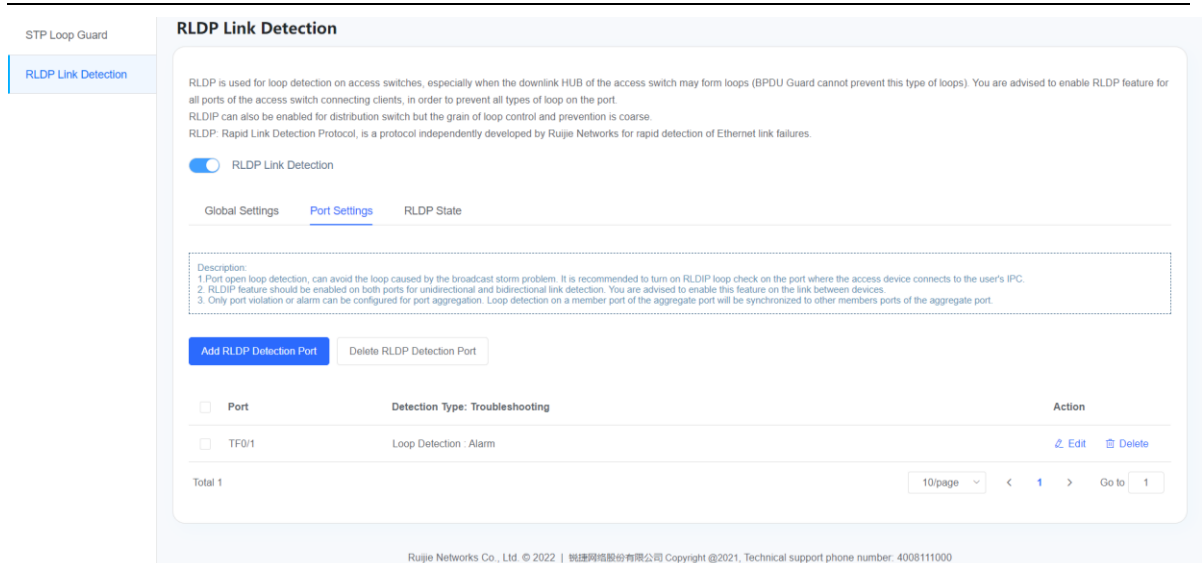
1. **Save:** After you have entered the detection interval, number of detections, and restoration cycle (optional), click  to save the global settings.

2. **RLDP Link Detection:** Click  to enable or disable RLDP.

Port Configuration

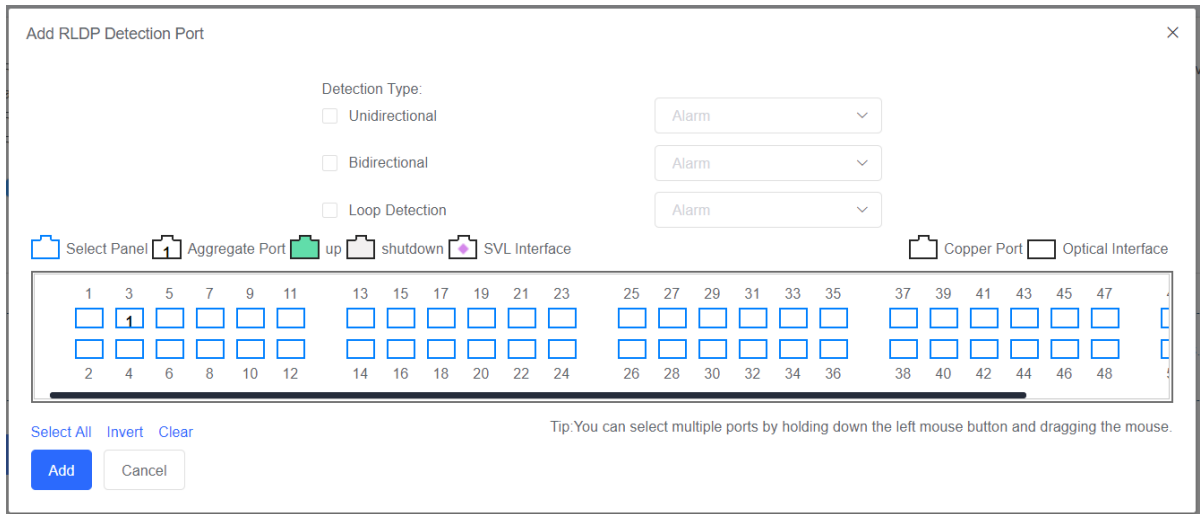
Note

- (1) Enabling loop detection on a port can prevent broadcast storm caused by loops. You are advised to enable loop detection on ports of the access switch connecting to a client.
- (2) RLDP must be enabled on both ports for unidirectional and bidirectional link detection. You are advised to enable RLDP on the link between switches.
- (3) Only port violation or alarm detection types can be configured for aggregated ports. Loop detection on a member port of the aggregated port will be synchronized to other member ports of the aggregated port.



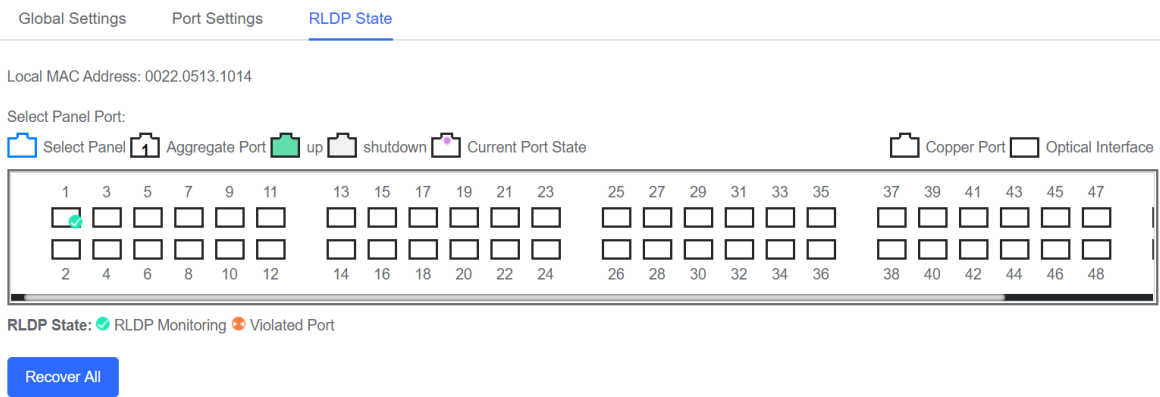
1. Adding an RLDP-enabled port

Click **Add RLDP Detection Port**. The **Add RLDP Detection Port** window is displayed.



RLDP involves unidirectional link detection, bidirectional link detection, and loop detection. Options in the drop-down list boxes corresponding to these three types include **Alarm**, **Disable port learning and forwarding**, **Port violation**, and **Disable SVI**. You can select multiple ports one by one, or using the **Select All** **Invert** **Clear** button. Click **Add** to submit the configuration. The result will be displayed in the list.

RLDP State



RLDP State: You can select RLDP Monitoring or Violated Port.

Restore All: You can click **Recover All** to recover all violated ports.

1.3.6 O&M

1. Ping or Tracert

Performing a Ping Test

The screenshot shows the Ruijie O&M web interface for performing a Ping Test. The interface includes a navigation menu with 'Home', 'Configuration', 'O&M', and 'System'. The 'O&M' menu is expanded, showing 'Ping Test' and 'Traceroute Test'. The 'Ping Test' configuration page has the following fields:


- Ping Mode:** Non-Management Interface (dropdown)
- * Dest. IP Address or Domain Name:** 192.168.1.1
- * Timeout Period:** 2
- * Number of Retries:** 5
- * Packet Size:** 100
- * Allow Fragmentation:** Yes No


There are 'Start' and 'Stop' buttons. Below the configuration fields is a terminal window showing the following output:

```

Sending 5, 100-byte ICMP Echoes to 192.168.1.1, timeout is 2 seconds:
 < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5).
    
```

At the bottom of the page, there is a footer: 'Ruijie Networks Co., Ltd. © 2022 | 锐捷网络股份有限公司 Copyright ©2021, Technical support phone number: 4008111000'.

1. **Start:** Select **Non-Management Interface** from the **Ping Mode** drop-down list box to select the ping mode. You can select **Non-Management Interface** and **Management Interface**, and there may be multiple management interfaces. Enter the destination IP address or domain name, timeout period, number of attempts, and packet size. The **Allow Fragmentation** item is displayed only when **Ping Mode** is set to **Non-Management Interface**. After setting configuration parameters, click  to run the ping test. After the ping test is complete, the test results will be displayed.

2. **Stop:** Click  to stop the current ping test.

Performing a Tracert Test

The screenshot shows the Ruijie O&M web interface for performing a Tracert Test. The interface includes a navigation menu with 'Home', 'Configuration', 'O&M', and 'System'. The 'O&M' menu is expanded, showing 'Ping Test' and 'Traceroute Test'. The 'Traceroute Test' configuration page has the following fields:


- Tracert Mode:** Non-Management Interface (dropdown)
- * Dest. IP Address or Domain Name:** 192.168.1.1
- * Timeout Period:** 2

There are 'Start' and 'Stop' buttons. Below the configuration fields is a terminal window showing the following output:

```

< press Ctrl+C to break >
Tracing the route to 192.168.1.1
 0  *  *  *
 1  *  *  *
 2  *  *
    
```

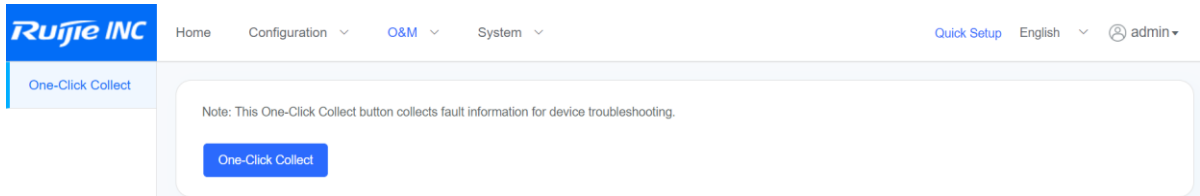
1. **Start:** Select **Non-Management Interface** from the **Tracert Mode** drop-down list box to select the tracert mode. You can select **Non-Management Interface** and **Management Interface**, and there may be multiple

management interfaces. Enter the destination IP address or domain name and timeout period. Click  to run the tracer test. After the tracer test is complete, the test results will be displayed.

2. **Stop:** Click  to stop the current tracer test.

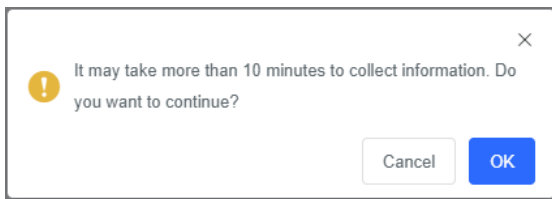
2. Performing One-Click Collection


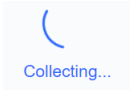
You can use the **One-Click Collect** function to collect switch fault information for troubleshooting.

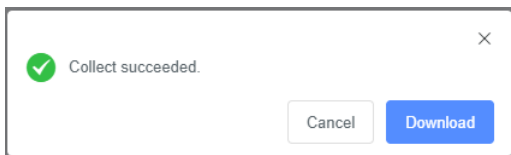



Collecting fault information may take about 10 minutes. After the collection is complete, you can download the collected fault information to a file named **tech_vsd0_20210716142650.tar.gz**.

One-Click Collect: Click . The **Error** dialog box is displayed.



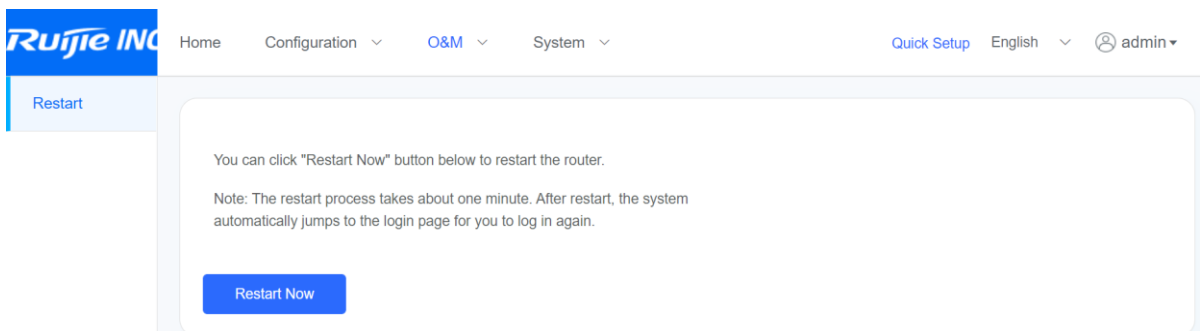
Click . The collecting process starts, and  is displayed. After the collection process is complete, the **Error** dialog box is displayed.



Click  to download the collected information in a **tar.gz** compressed file.

3. Restarting the Switch

Click **Restart Now** to restart a switch. The restart process takes about 1 minute. Do not perform any operation during this period. After the switch is successfully restarted, the current page will be refreshed automatically.



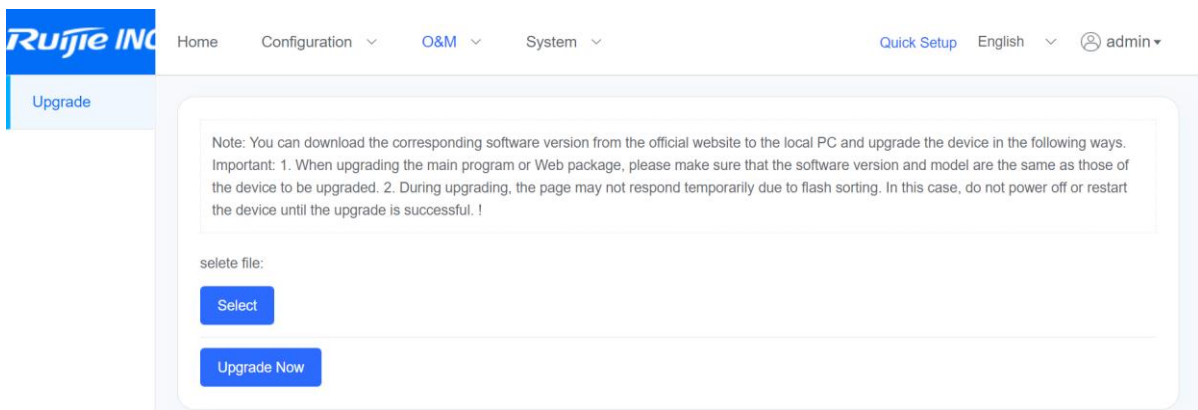
4. Upgrading the Switch

Note

You can download the required software version file from Ruijie Networks's official website to the local PC and upgrade the switch using the downloaded file.

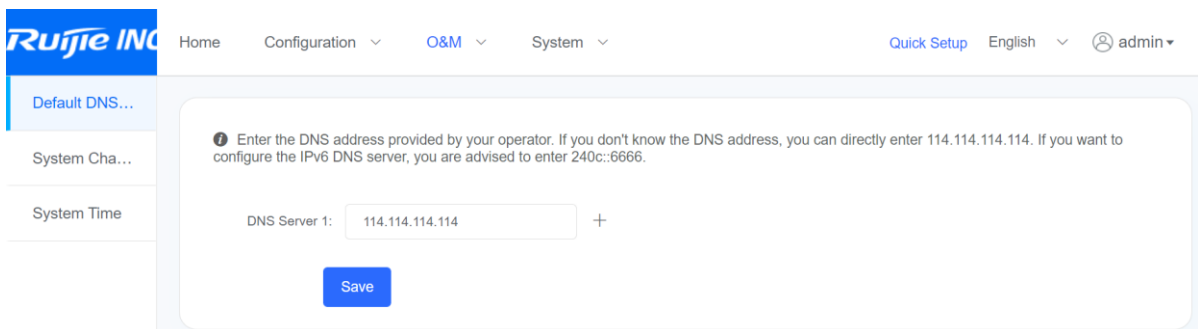
Caution




1. When upgrading the main program or the web package, ensure that the version and model are the same as those of the current switch.
2. During upgrading, there may be no response temporarily due to flash loading. In this case, do not power off or restart the switch until the upgrade is successful.



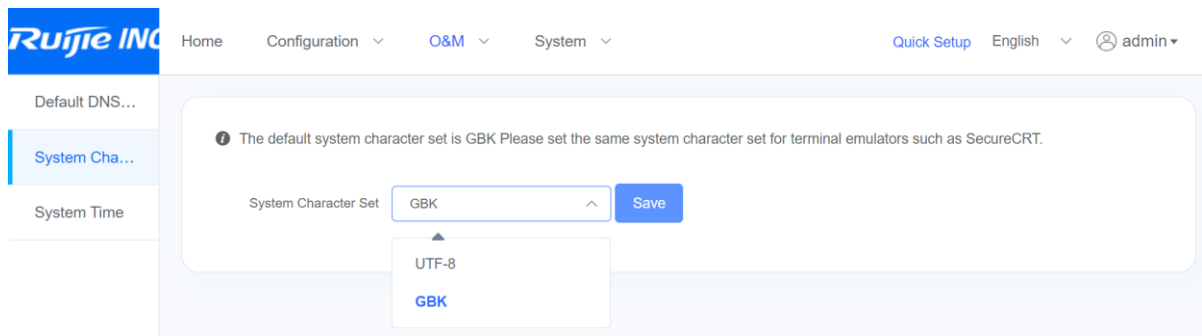
5. Basic Configurations


Default DNS Server



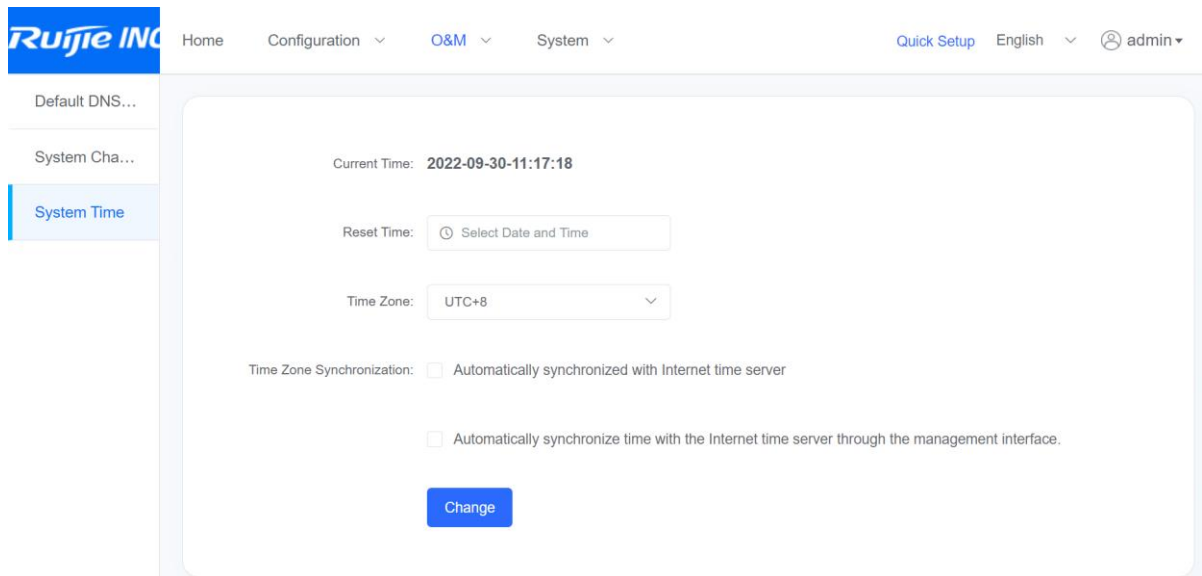
1. You can click  to add a DNS server, click  to delete a DNS server, or click  to submit the configuration.

System Character Set



System character set: There are two options in the **System Character Set** drop-down list box, which are **UTF-8** and **GBK**. The default value is **UTF-8**. After a character set is selected, click  to save the configuration.

System Time

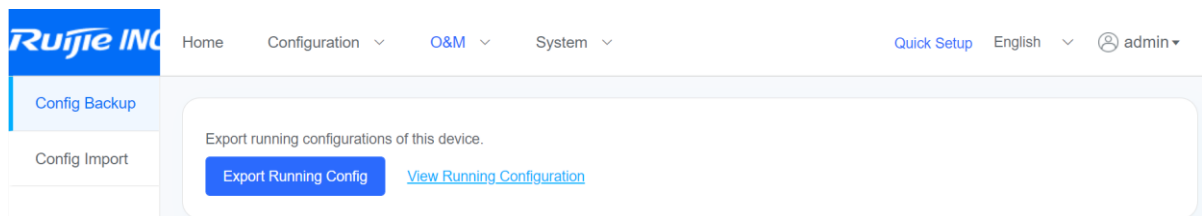


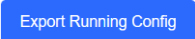
You can manually select the system time or select **Time Zone Synchronization** to automatically synchronize the switch system time with the Internet time server.

6. Configuration Management

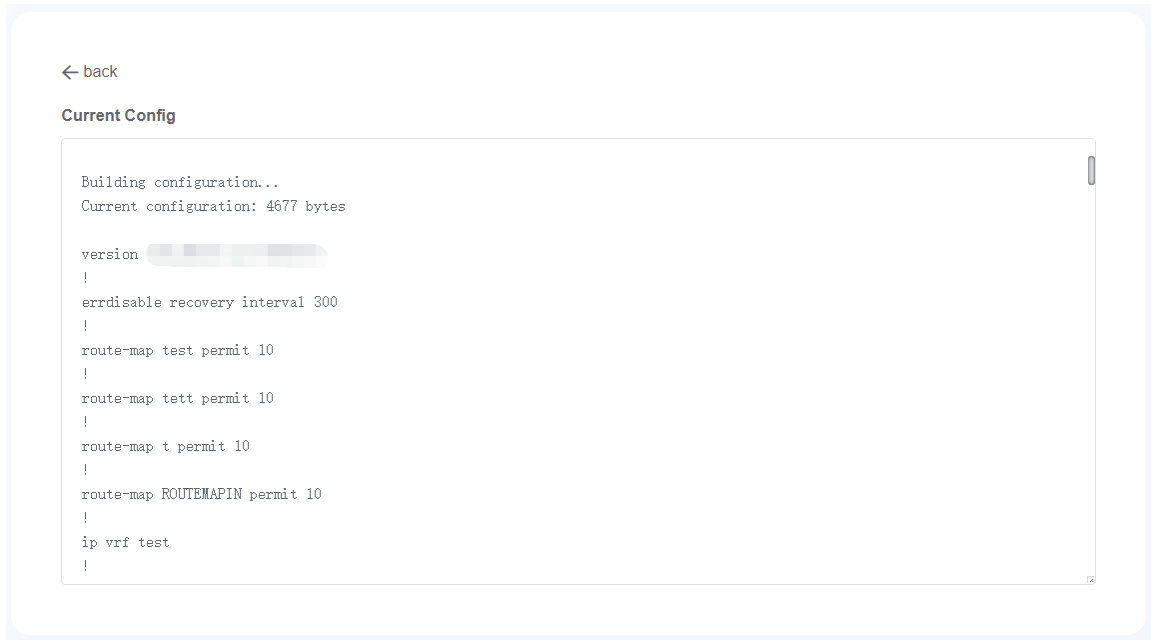
Performing Configuration Backup

The configuration backup function enables you to import or view the running configuration of the switch.

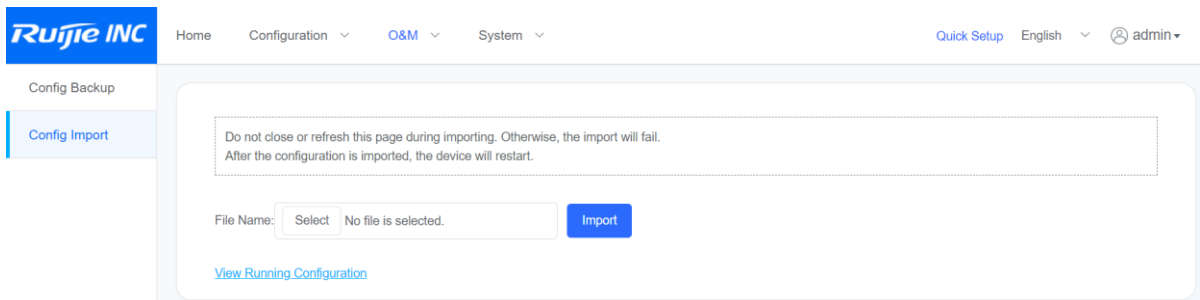


1. **Export running configuration:** You can click  to generate the **config.text** text file.

2. **View running configuration:** You can click [View Running Configuration](#) to switch to the **Current Config** page.



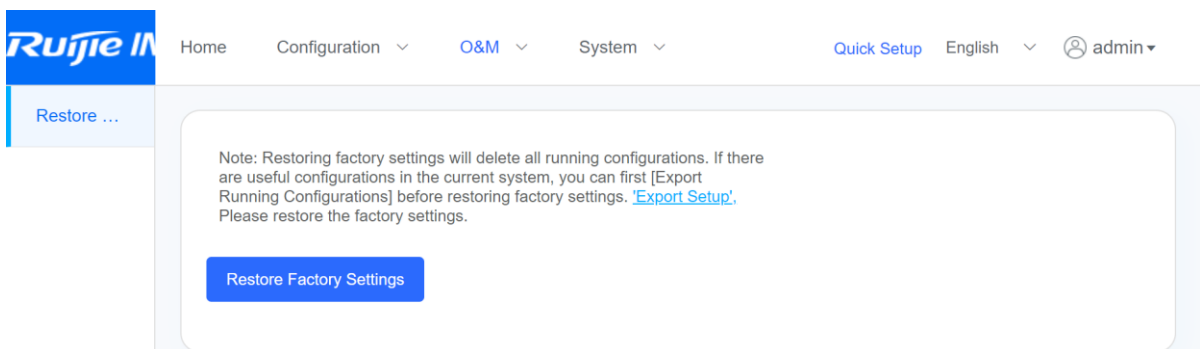
Importing Configurations



- 1. Import configurations:** You can click to select the configuration file to be imported, and then click to import the configuration file.
- 2. View running configuration:** You can click [View Running Configuration](#) to switch to the **Current Config** page.

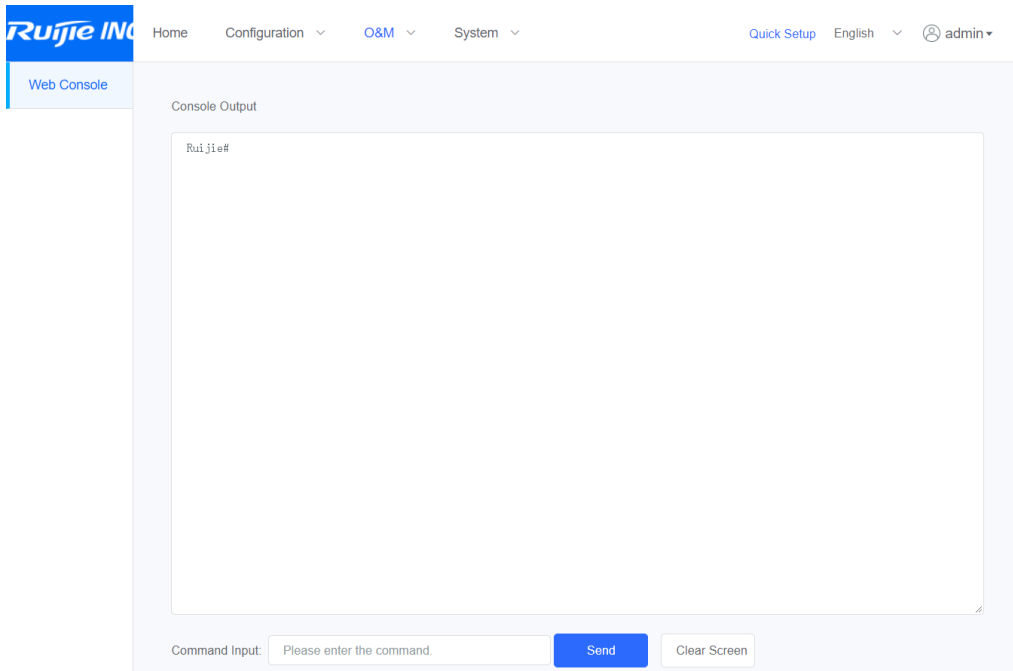
7. Restoring Factory Settings

You can click **Restore Factory Settings** to delete all the configurations of the switch, and restore the switch to factory settings. To save the current configuration, you are advised to export the current configuration by clicking **Export Setup**.



8. Web Console

The web console simulates the connection of a client connection tool such as xshell, rt, mobaxterm to the controller of the switch.

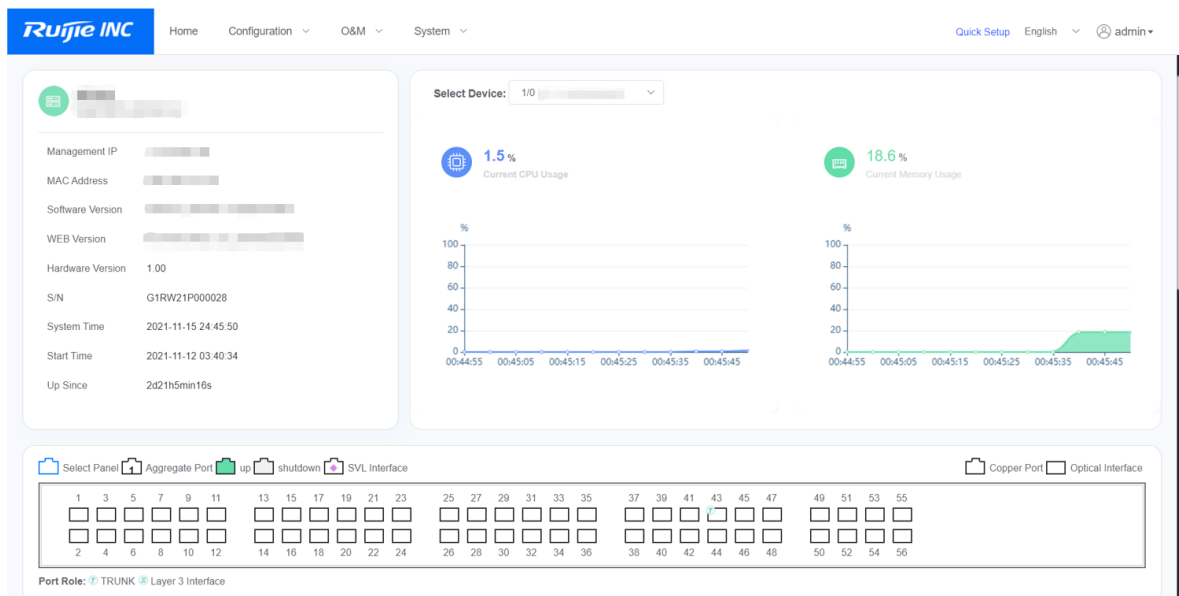


1. Enter a command in and click . The command execution result will be displayed in the console.

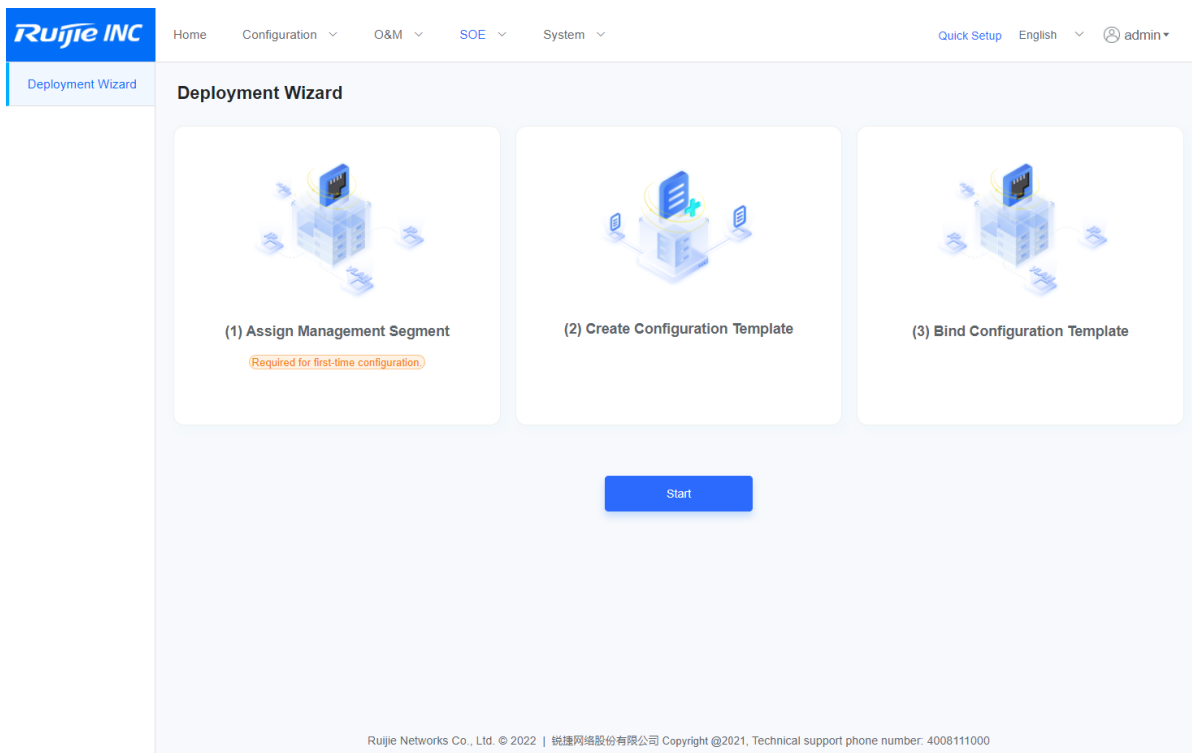
2. Click to clear the output result.

1.3.7 SOE (paid service)

SOE is a paid service and is available only when an RG-INC-EMB-SW-AMAIN license is imported.



Page layout before an RG-INC-EMB-SW-AMAIN license is imported



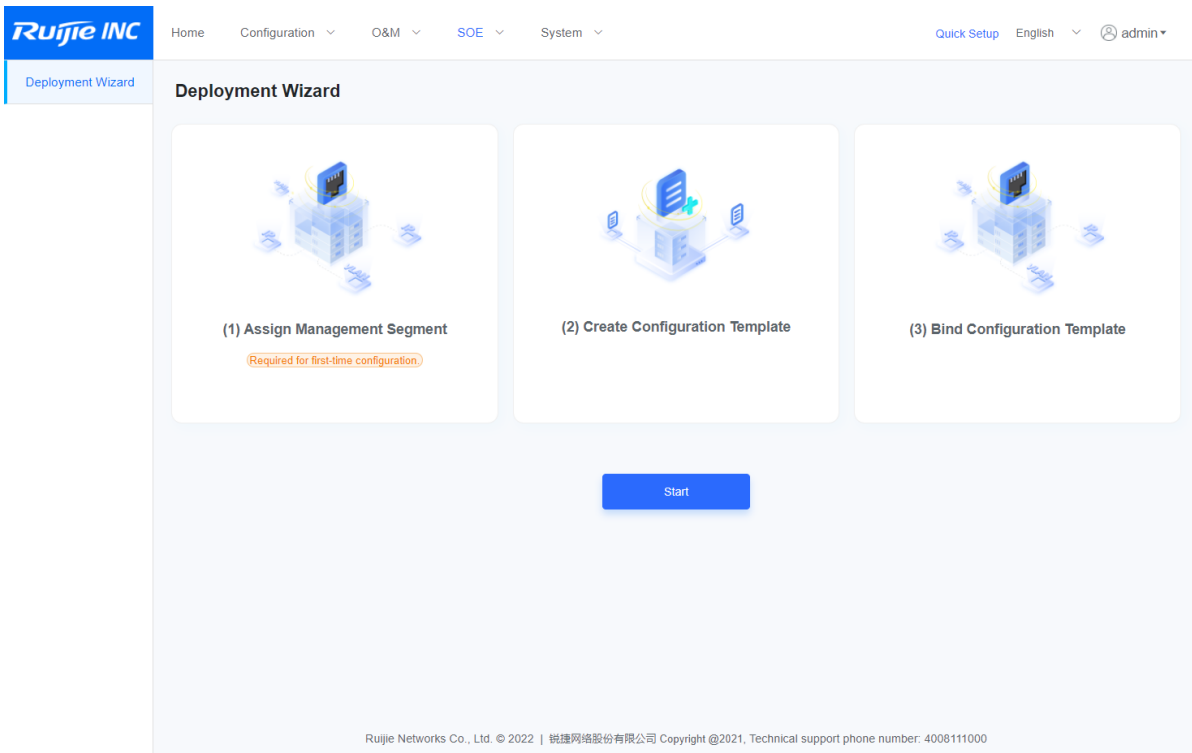
Page layout after an RG-INC-EMB-SW-AMAIN license is imported

1. Deployment Wizard

Step 1: Assign a management subnet.

Step 2: Create a configuration template.

Step 3: Bind a configuration template.



Assigning a Management Subnet

Assigning a management subnet refers to configuring the default management VLAN and management subnet, and user-defined management VLAN and management subnet. When a management subnet is assigned for the first time, the user-defined management VLAN and management subnet are optional. The user-defined management VLAN and management subnet cannot be removed when being assigned.

A switch going online through the zero-touch provisioning (ZTP) process will be assigned with an IP address based on the default management VLAN and management subnet. If a user-defined management VLAN is configured, the switch will be assigned with an IP address based on the user-defined management VLAN and management subnet.

The screenshot shows a configuration page with three steps: 1. Assign Management Segment, 2. Create Configuration Template, and 3. Bind Configuration Template. The current step is 'Assign Management Segment'. It contains two sections: 'Default Management VLAN and Segment' and 'Custom Management VLAN and Segment'. Each section has five input fields: Management VLAN, Management Gateway, Management Segment/Subnet Mask, IP of SOE Components, and Excluded Addresses. A 'Save and Next' button is highlighted with a red box at the bottom of the form.

Field	Default Management VLAN and Segment	Custom Management VLAN and Segment
* Management VLAN	1	30
* Management Gateway	10.110.60.1	10.110.70.1
* Management Segment/Subnet Mask	10.110.60.0/24	10.110.70.0/24
* IP of SOE Components	10.110.60.158	
Excluded Addresses	10.110.60.1-10.110.60.200	10.110.70.1-10.110.70.200

Configure User-Defined Management VLAN and Management Subnet.

The default management VLAN and management subnet must not be on the same subnet. Click [Save and Next](#) to save the configuration and switch to **Create Configuration Template**.

Creating a Configuration Template

1 Assign Management Segment 2 Create Configuration Template 3 Bind Configuration Template

① Create a template

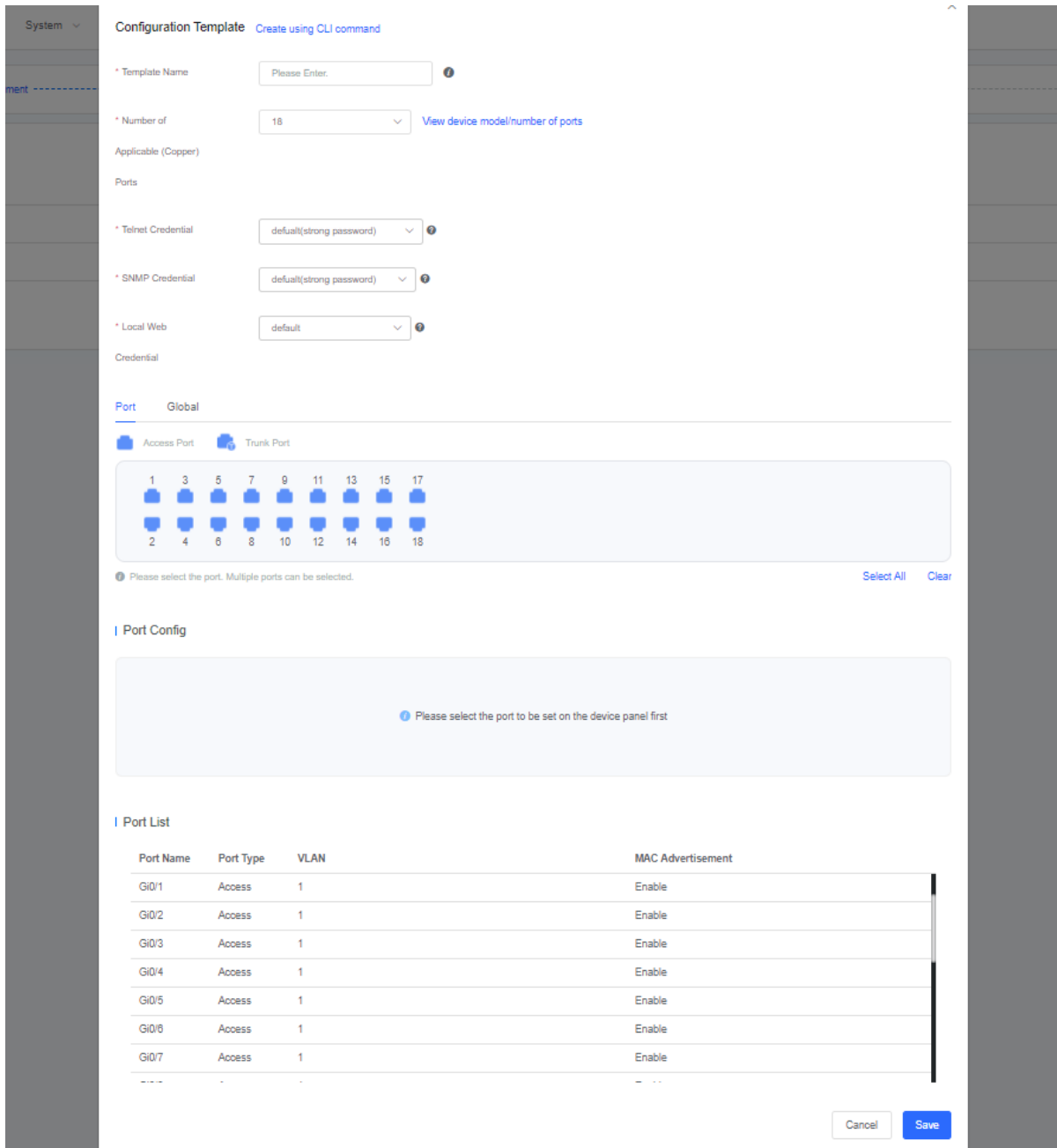
[Create Template](#)


⑦ Search a configuration template by entering the template name here and pressing Enter.

Template Name	Number of Applicable Ports	Number of Associated Devices	Action
first	18	2	Edit ③ Edit a template
second	18	0	④ Delete a template. The template associated with devices cannot be deleted. Edit Delete
third	4	0	Edit Delete

⑤ Return to the [Assign Management Subnet] page. [Previous](#) [Next](#) ⑥ Switch to the [Bind Configuration Template] page.

You will be redirected to the same **Configuration Template** page when you click <Create Template> and <Edit>.



Configuring a template: Set configuration parameters in the displayed window. In the **Port Config** panel, select a ports, set configuration parameters in the displayed window and click **OK**. Click . The results can be viewed in the **Port List** panel. The port configuration or preview is displayed.

Web-based Configuration Guide

Port Global

Access Port Trunk Port

1	3	5	7	9	11	13	15	17
2	4	6	8	10	12	14	16	18

You can select one or more ports.

Please select the port. Multiple ports can be selected.

You can click <Select All> or <Clear> to quickly select or delete one or more ports.

Select All Clear

Port Config Selected: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

* Port Type: Access

* VLAN ID: 1

Advanced Settings

OK Confirm your operation

Port Config Selected: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18

* Port Type: Access

* VLAN ID: 1

Advanced Settings Expand Advanced Settings.

MAC Advertisement Enable

Loop Guard: Enable

Storm Control Unicast Multicast Broadcast

Port Isolation Enable

PoE: Enable

PoE Priority: Low

OK Confirm your operation Click <OK> to save the configuration.

| Port List

Port Name	Port Type	VLAN	MAC Advertisement
Gi0/1	Access	1	Enable
Gi0/2	Access	1	Enable
Gi0/3	Access	1	Enable
Gi0/4	Access	1	Enable
Gi0/5	Access	1	Enable
Gi0/6	Access	1	Enable
Gi0/7	Access	1	Enable
Gi0/8	Access	1	Enable

Preview: You can click [Create using CLI command](#) to switch to the **Configuration Template (Using CLI Command)** page. On the **Custom CLI Commands** pane, enter the customized CLI command and click to save it. You can view the parameters of the current configuration template in the **Preview** pane on the right. You can click or to switch to the **Configuration Template** page.

← Configuration Template (Using CLI Command) ×

1. Do not use custom CLI commands for features that are supported by the visual interface.
2. Please make sure that each custom command is correct. **Please make sure that all custom commands are correct.** The device Do not use custom CLI commands for features that are supported by the visual interface
3. 2920U Series will ignore this configuration (including SF2920U, MF2920U, IF2920U, PF2920U series)

Preview

```
username sfadmin password ruijie@123
line vty 0 35
 login local
 privilege level 15
!
interface GigabitEthernet 0/1
 no ip dhcp snooping trust
 switchport mode access
 switchport access vlan 1
 no switchport protected
 snmp trap mac-notification added
 snmp trap mac-notification removed
 poe enable
 poe priority low
 no auto-power-down enable
 no storm-control broadcast
 no storm-control multicast
 no storm-control unicast
 rldp port loop-detect shutdown-port
!
interface GigabitEthernet 0/2
 no ip dhcp snooping trust
 switchport mode access
 switchport access vlan 1
 no switchport protected
 snmp trap mac-notification added
 snmp trap mac-notification removed
 poe enable
 poe priority low
 no auto-power-down enable
 no storm-control broadcast
 no storm-control multicast
 no storm-control unicast
 rldp port loop-detect shutdown-port
!
interface GigabitEthernet 0/2
```



Custom CLI Commands

Please enter CLI commands here. You are advised to use a text editor to edit and then paste the content here.

Cancel Confirm and Preview

Configuring the Associated Device

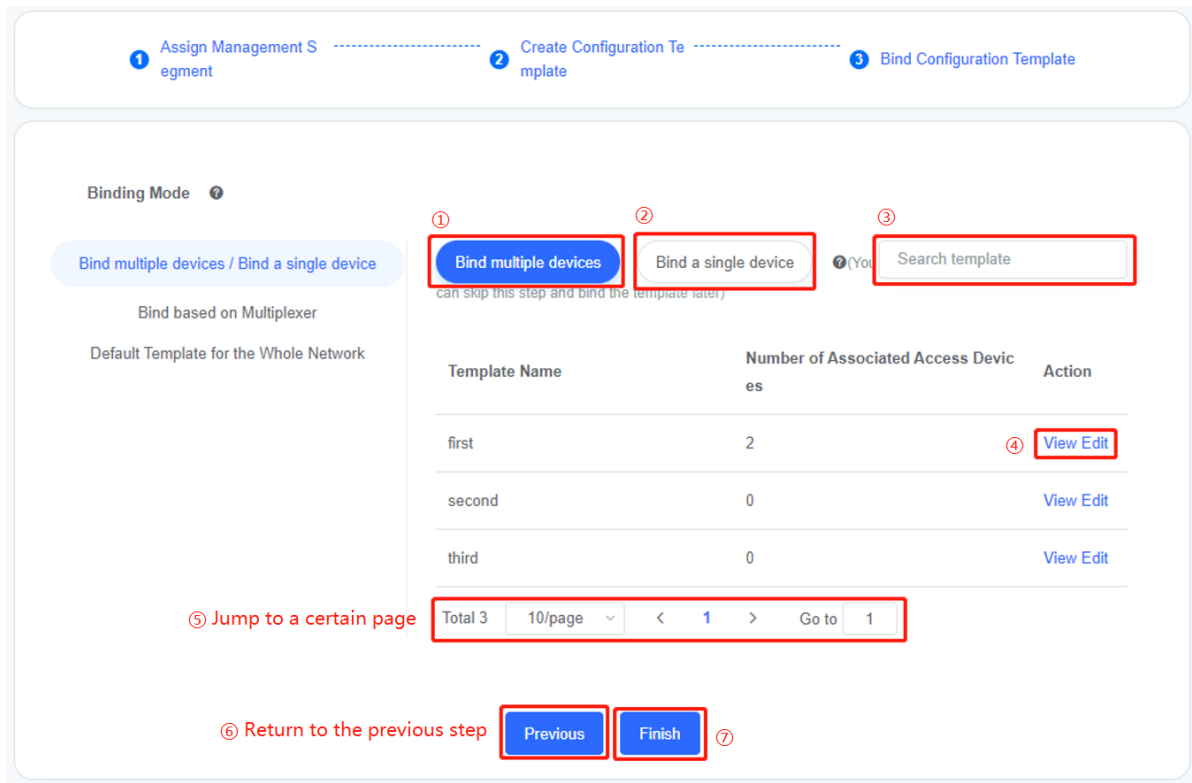
The screenshot shows a web interface titled "Associated Device". At the top right, there is a search box containing the text "SN | Please | Location", with a red circle and arrow pointing to it labeled "2 Search box". Below the search box is a table with the following columns: Status, Device IP, Device SN, Model, Name, Area Name, Location, and Action. The table contains one row with the following data: Status: Not Managed, Device IP: (empty), Device SN: MACC942570009, Model: (empty), Name: 1, Area Name: defaultAre..., Location: (empty), and Action: Edit (with a pencil icon) and Delete (with a trash icon). A red circle and arrow points to the "Edit" button labeled "3 Edit an associated device". At the bottom left, there is a pagination control showing "Total 1", "10/page" (with a dropdown arrow), navigation arrows, "1" (with a dropdown arrow), and "Go to 1". A red circle and arrow points to this control labeled "1 Jump to a certain page".

On the **Associated Device** page, click  **Edit**. The **Bind a single device** page is displayed. After setting configuration parameters, click  to bind one switch.

The screenshot shows a form titled "Bind a single device". It contains the following fields: "Device SN" with the value "MACC942570009"; "Bound Configuration Template" with a dropdown menu showing "first"; "Area Name" with the value "defaultArea"; "Location" with the placeholder text "Please enter. Example: Room 3001." and a question mark icon; and "Name" with the value "1" and a question mark icon. At the bottom right, there are two buttons: "Cancel" and "Bind".

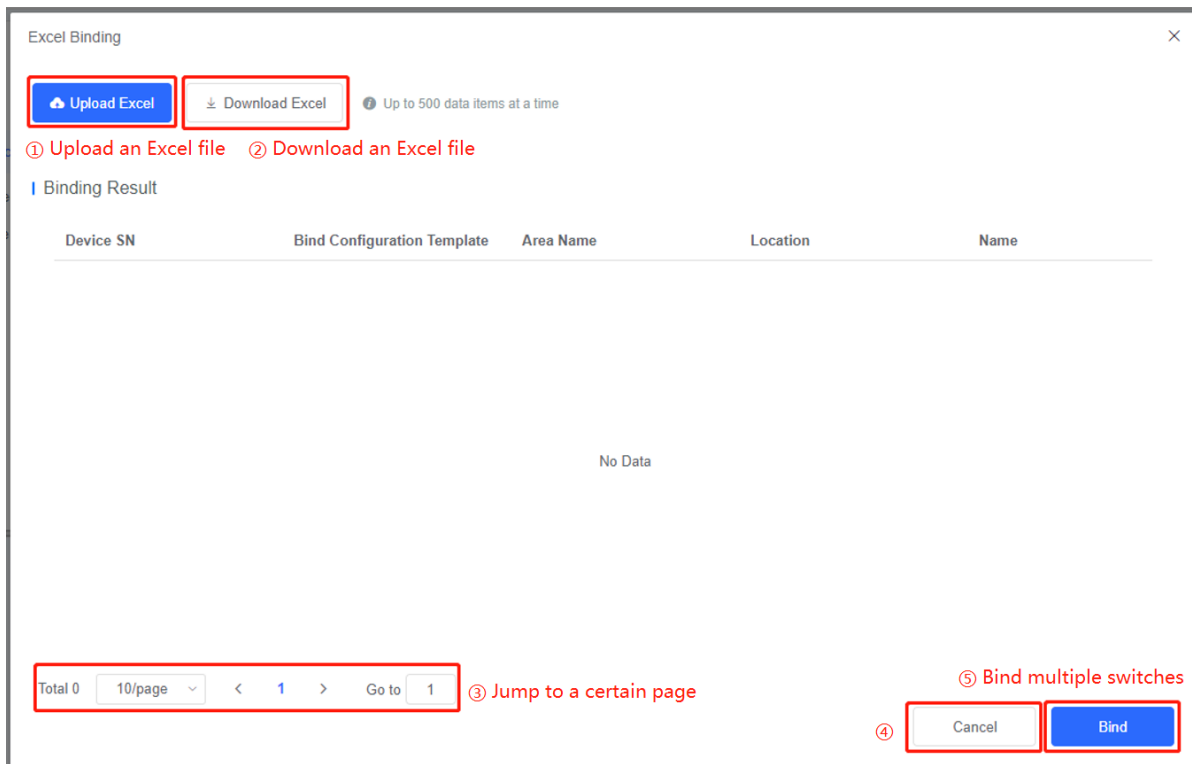
Binding a Configuration Template

Binding One or More Switches

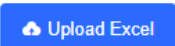


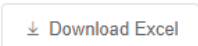
(1) Binding multiple switches

On the **Bind multiple devices** or **Bind a single device** page, click [Bind multiple devices](#). The **Excel Binding** page is displayed.

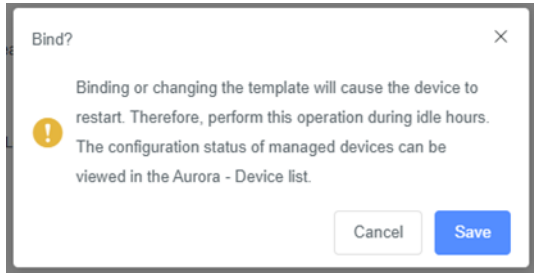



On the **Excel Binding** page, you can perform the following operations:

(1) Upload an Excel file: You can click  to upload the switches to be bound. The binding results will be displayed in the **Binding Result** pane.

(2) Click  to download an Excel binding template.

(3) Click . A dialog box is displayed.



Click . The bound devices will be displayed in the refreshed window.

Binding Based on the Aggregation Layer

① Add a distribution layer-based binding policy

② New access devices connected to the aggregation switch will be automatically matched to a template.



③ Add

④ Search a binding policy

Policy Name	Multiplexer	Template name	Action
first	172.29.17.4	first	② Edit a binding policy ③ Delete a binding policy

⑤ Jump to a certain page

(1) Adding or editing a binding policy based on the aggregation layer

You can click  to switch to the **Add** page. On the **Add** page that is displayed, set configuration parameters and click  to save the configured policy.

Add ✕

? One multiplexer can be bound to multiple templates. An access device from the distribution layer can be automatically matched to a template based on the number of ports.

* Policy Name ?

* Multiplexer ?

* Bound Configuration Template ▼

Note

Device IP: Run the `sh lldp local-information` command on the aggregation switch to check the switch's IP address.

Bound Configuration Template: The number of ports in the configuration template must be different so that the switch can be automatically matched to a template based on the number of ports in the configuration template.

(2) Deleting a binding policy

Click **Delete**. A dialog box is displayed.

✕

Are you sure you want to delete this template?

Click . The selected policy is deleted.

2. Deployment Log

The **Deployment Result** page shows the switch deployment results. You can filter and view the deployment results on this page. This page also contains the [Device List](#) link.

Deployment Result After the deployment finishes, you can modify the configuration of a single device in the Device List. [Device List](#) Modify the configuration of a single device

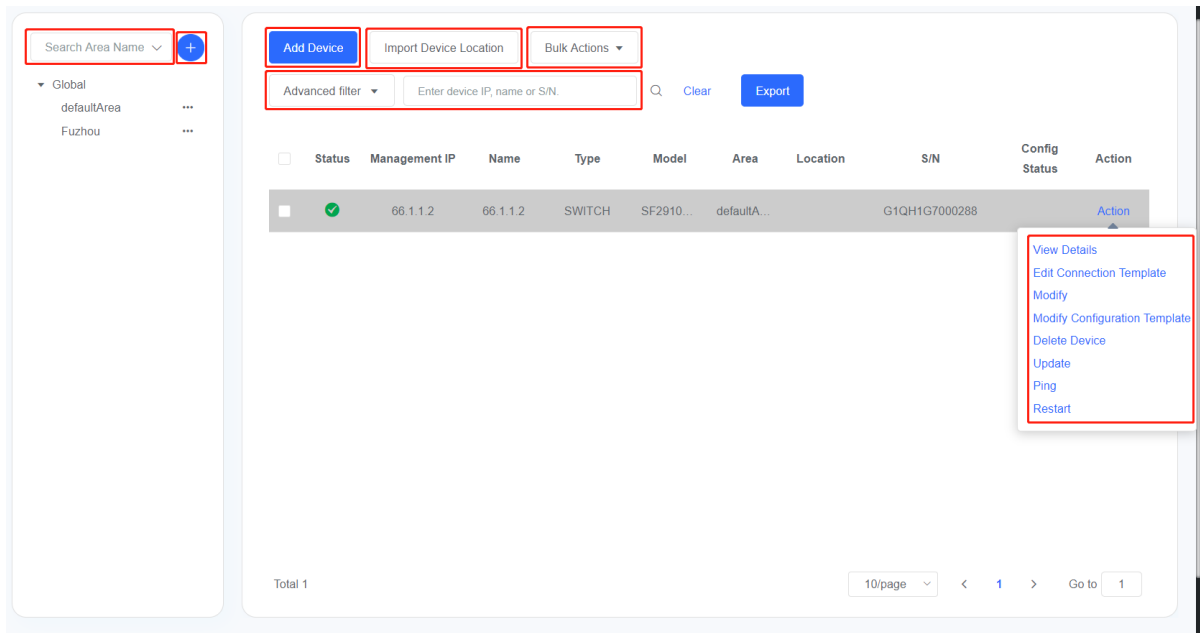
Last 7 days
 Only show failures
Device SN | Device IP

Device IP	Device SN	Name	Area	Location	Management Status	Description	Model	Template Name	Template Source	Updated at	Action
66.1.1.2	G1QH1G7000288	66.1.1.2	defaultArea		Managed	Success. (Replace)	SF2910-4GT2XS-P	Custom Template	Custom Template	2022-10-09 17:11:56	

Total 1 10/page < 1 > Go to 1

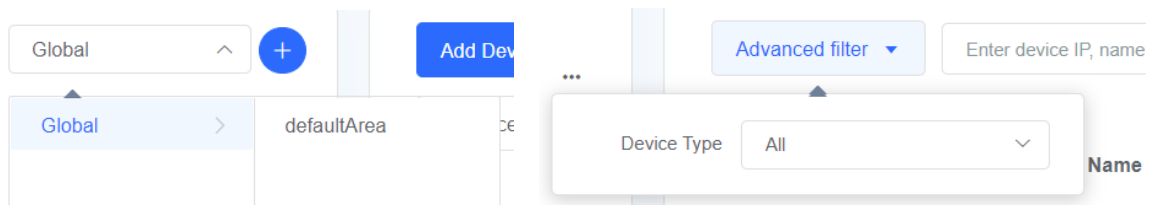
3. Device List

Adding or Editing a Switch



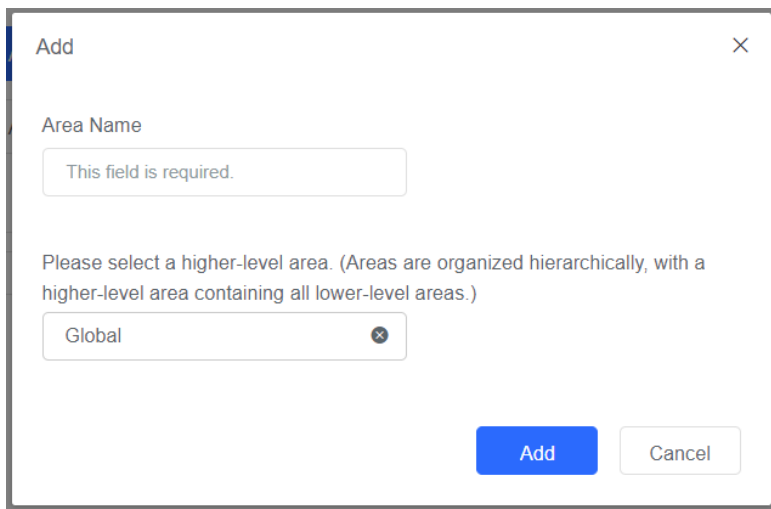
● **Querying a switch**

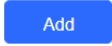
You can query a switch by area or device type, or entering the switch's management IP address, name or SN in the search box.



● **Adding an area**

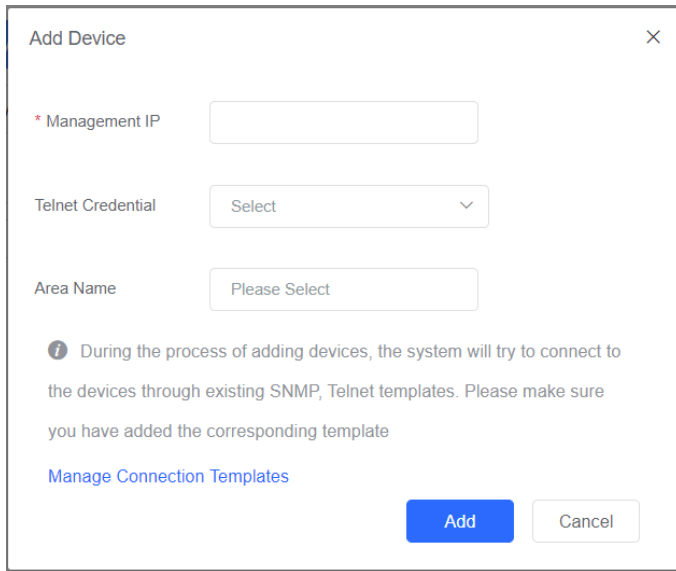
To add an area, click  in the **Area** pane. The **Add** window is displayed.




On the **Add** window, enter the area name, select a higher-level area, and click  .


● **Adding a single switch**

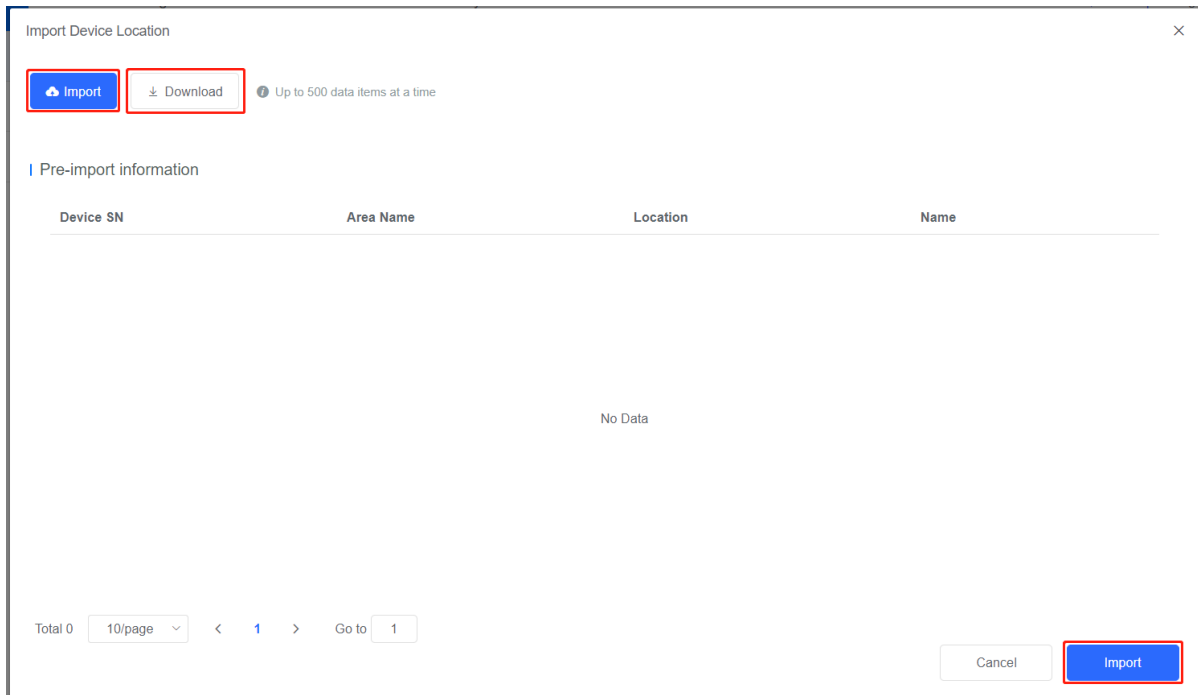
To add a single switch, click . The **Add Device** window is displayed.



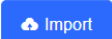
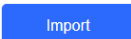
Enter the switch's management IP address, select the area name, and click . If the switch's IP address already exists or the switch is not reachable, the switch cannot be added.

- **Importing the switch location**


To import the location of a switch, you can click . The **Import Device Location** window is displayed.

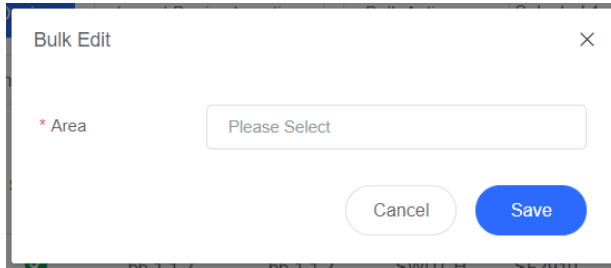



Click  to download the template (an Excel file). Set configuration parameters in the template.

Click  to import the completed Excel file, and click  to import the switch location data.

- **Editing multiple areas**

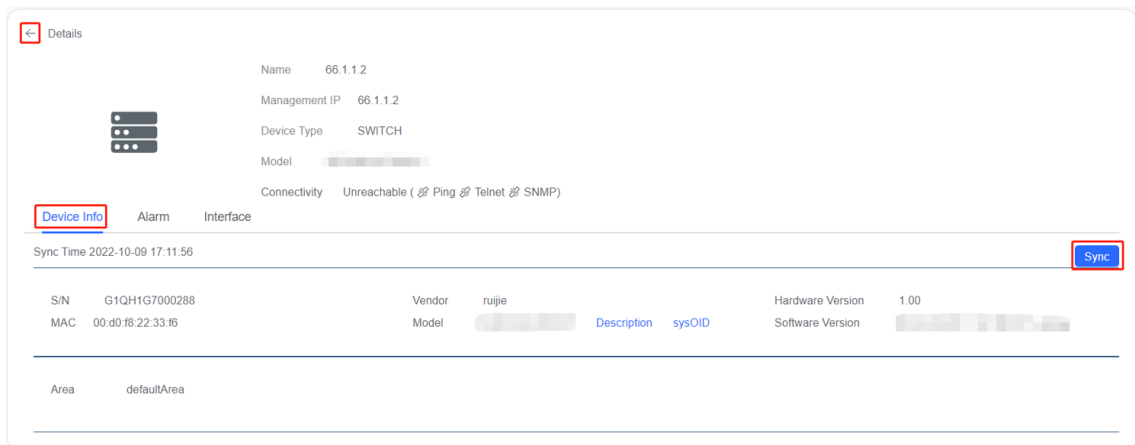
Click  next to **Device List**, select **Bulk Edit** from the **Bulk Actions** drop-down list box. The **Bulk Edit** window is displayed.

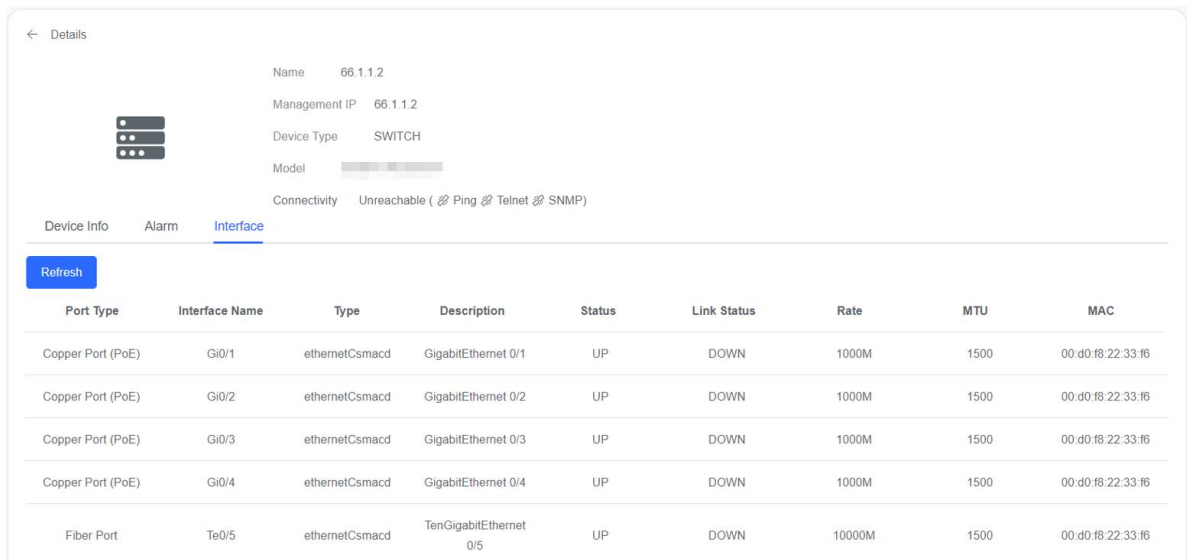


Select an area in the window, and click .

- **Querying switch details**

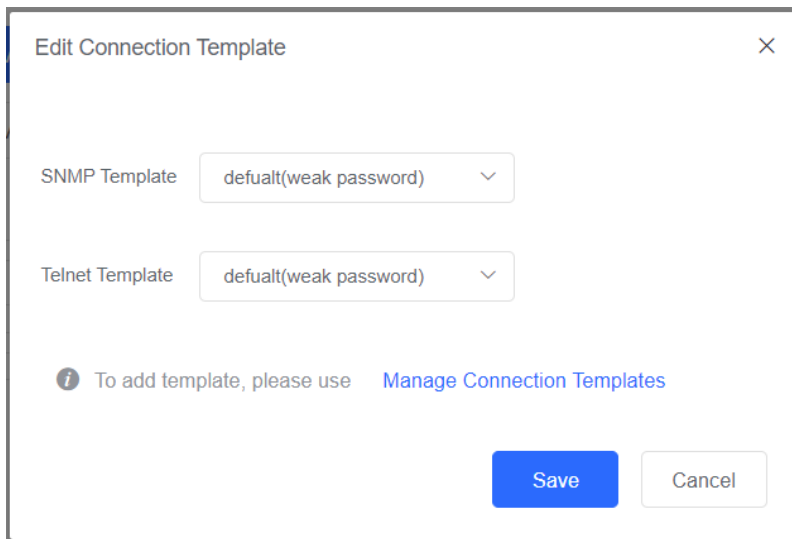
To query switch details, click the **Action** column of the **Device List**, and then click [View Details](#) to switch to the **Details** page. On the **Device Info** page, you can view basic information about a switch, and synchronize the switch by clicking **Sync**. On the **Alarm** page, you can query and set alarm details. On the **Interface** page, you can query the switch's interface data.





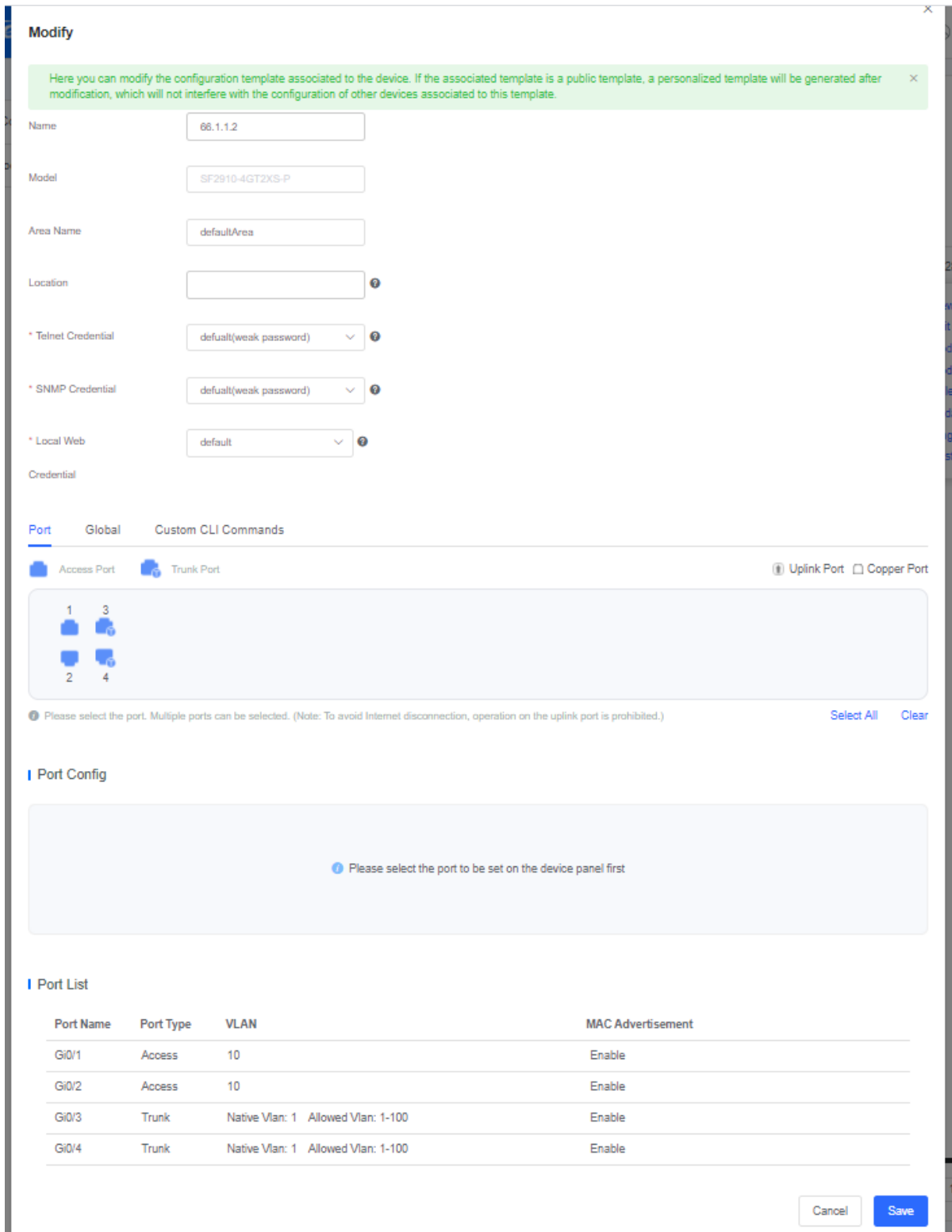
● **Editing a connection template**

To edit a connection template, click the **Action** column of **Device List**, and then click [Edit Connection Template](#). The **Edit Connection Template** window is displayed. Select the SNMP and/or Telnet template, and click [Save](#).



● **Editing the configuration (for switches that go online through the ZTP process only)**

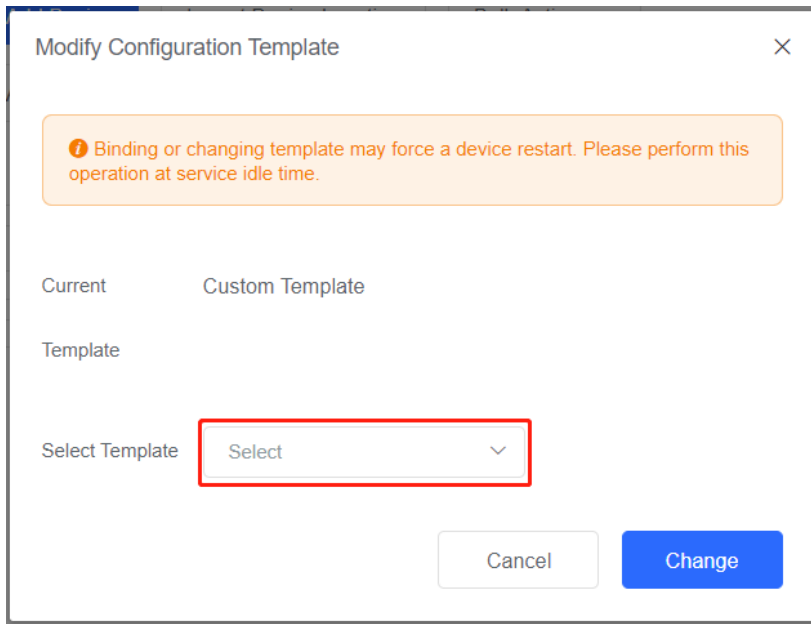
To edit the configuration of a switch, click the **Action** column of **Device List**, and then click [Modify](#). The **Modify** window is displayed. Set configuration parameters. If you change the value of **Telnet Credential** of the switch, the system displays the message “After this configuration is saved, the configuration will be delivered to this switch. This operation may force a switch restart. Please perform this operation at service idle time.” If you do not change it, the Telnet configuration will be delivered to the switch.



- **Modifying a configuration template (for switches that go online through the ZTP process only)**

Click the **Action** column of **Device List**, and then click [Modify Configuration Template](#). The **Modify**

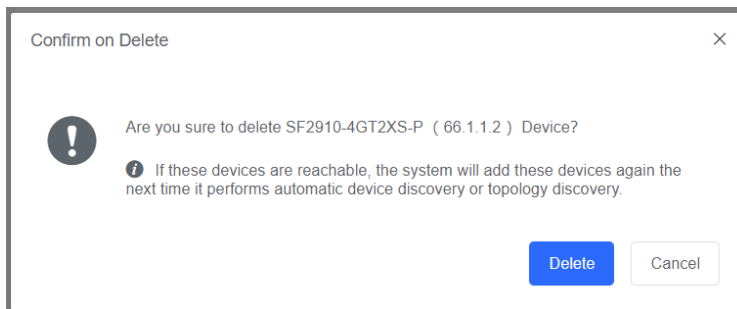
Configuration Template window is displayed. After selecting a template, click [Change](#). The switch will start the login process again.



- **Deleting a switch**

To delete a switch, you can click the **Action** column of **Device List**, and then click [Delete Device](#). The

Confirm on Delete dialog box is displayed. Click [Delete](#).



- **Updating switch details**

To update basic information about and interfaces of a switch, you can click the **Action** column of **Device List**, and then click [Update](#).

- **Ping a switch**

To ping a switch, click the **Action** column of **Device List**, and then click [Ping](#). After the ping test is successfully executed, the system displays the message "[XXX. XXX. XXX. XXX] is reachable" or "[XXX. XXX. XXX] is not reachable."

- **Restarting a switch**

To restart a switch, you can click the **Action** column of **Device List**, and then click [Restart](#). A dialog box is displayed.

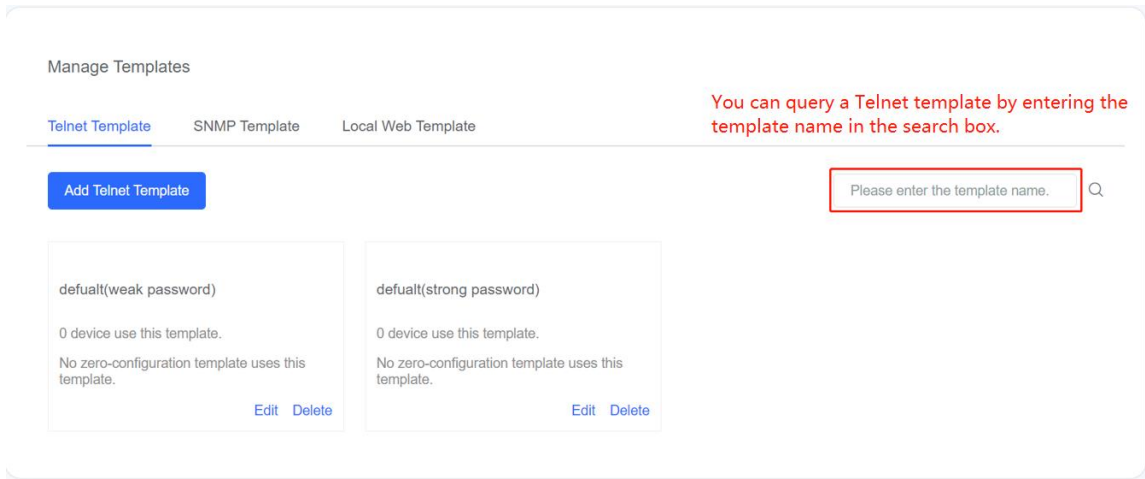


Click **OK**. The switch will restart successfully after 2 to 3 minutes.

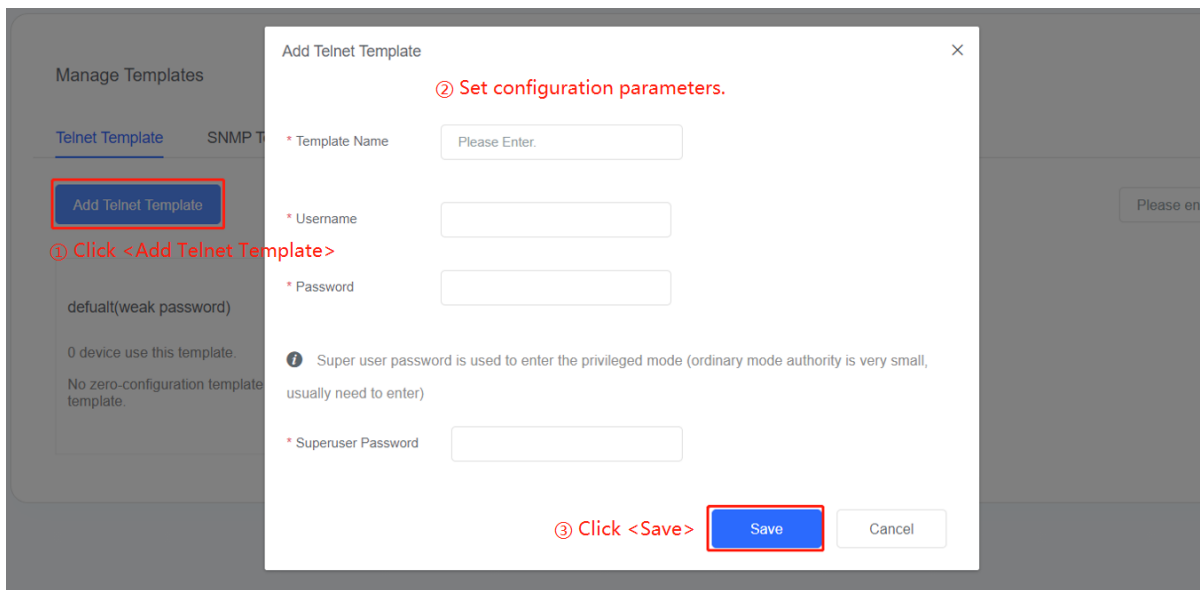
Managing Connection Templates of a Switch

(1) Telnet Templates

- **Querying a Telnet template**

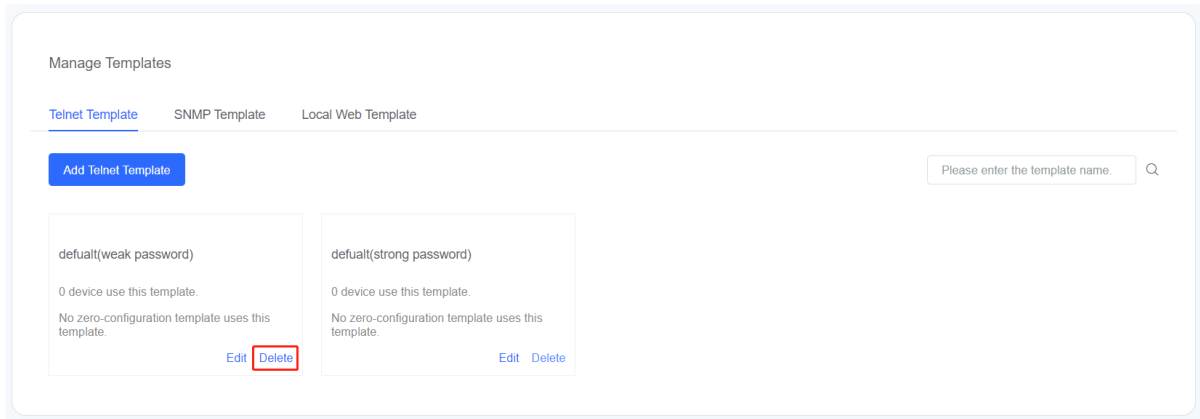


- **Adding a Telnet template (similar to editing a Telnet template)**



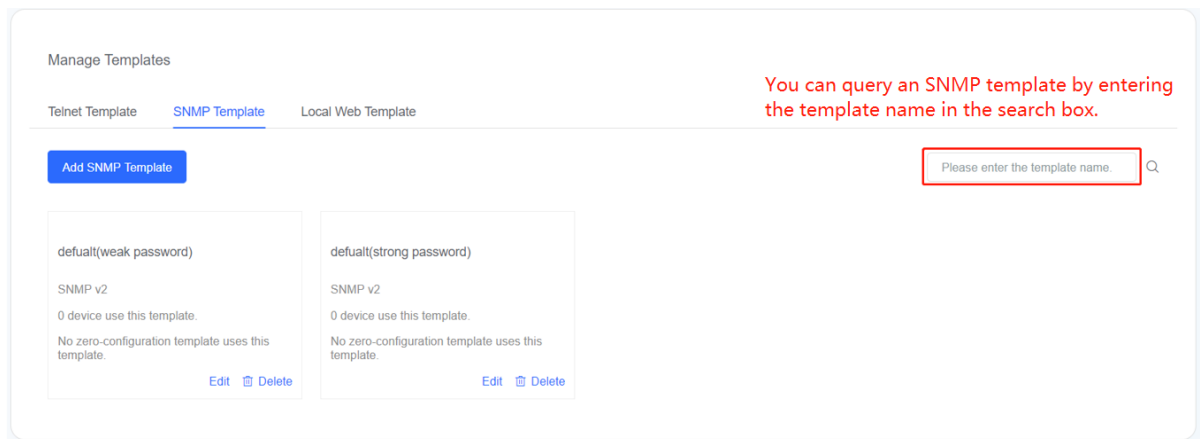
- **Deleting a Telnet template**

A referenced Telnet template cannot be deleted. You can only delete a Telnet template after you have successfully disassociated switches from the Telnet template.

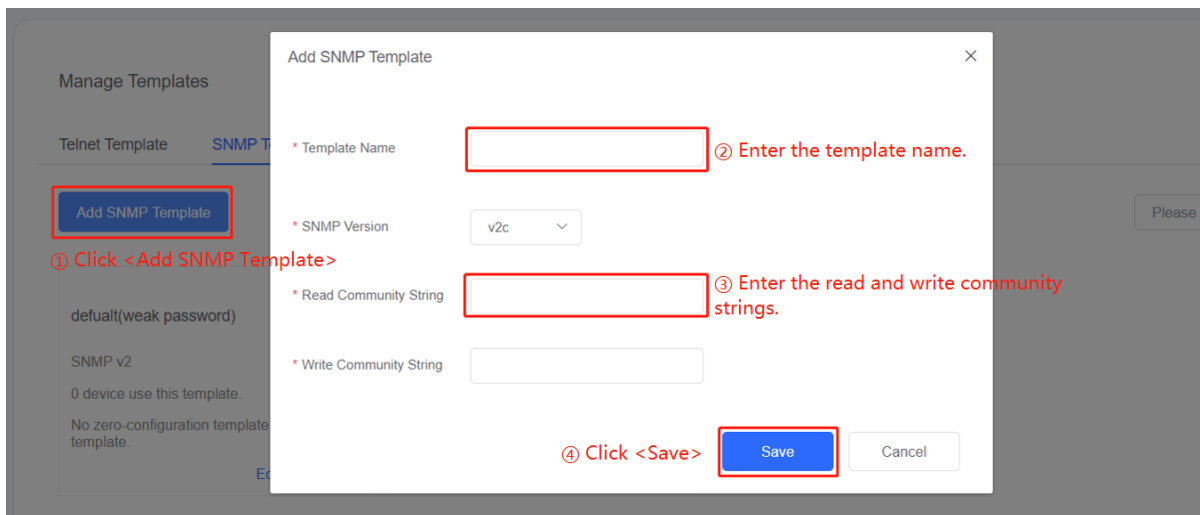


(2) SNMP Templates

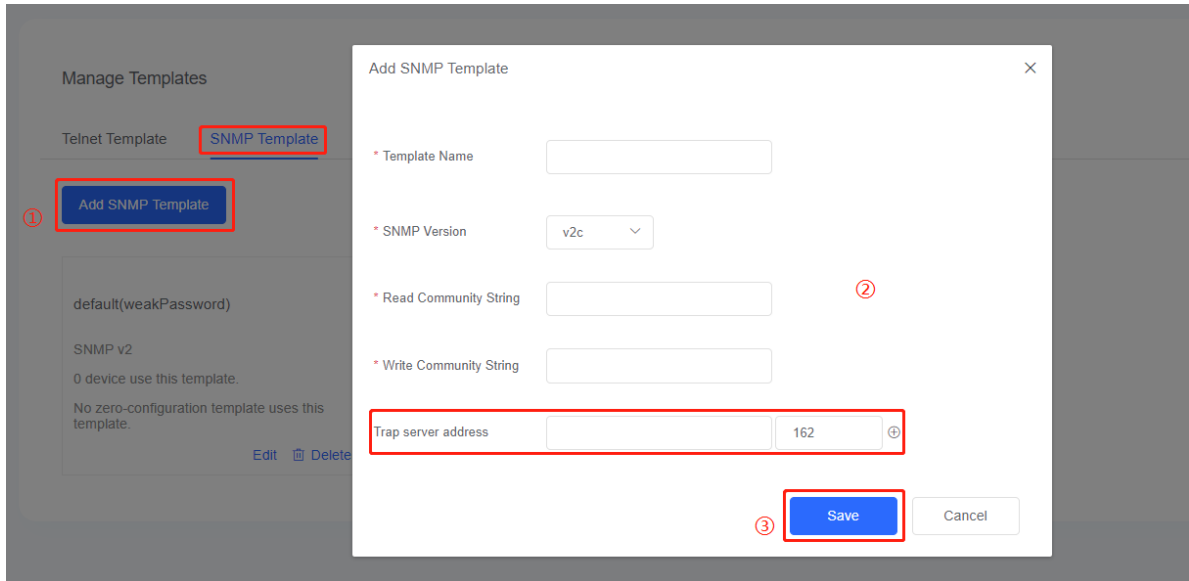
● Querying an SNMP template



● Adding an SNMP template (similar to editing an SNMP template)

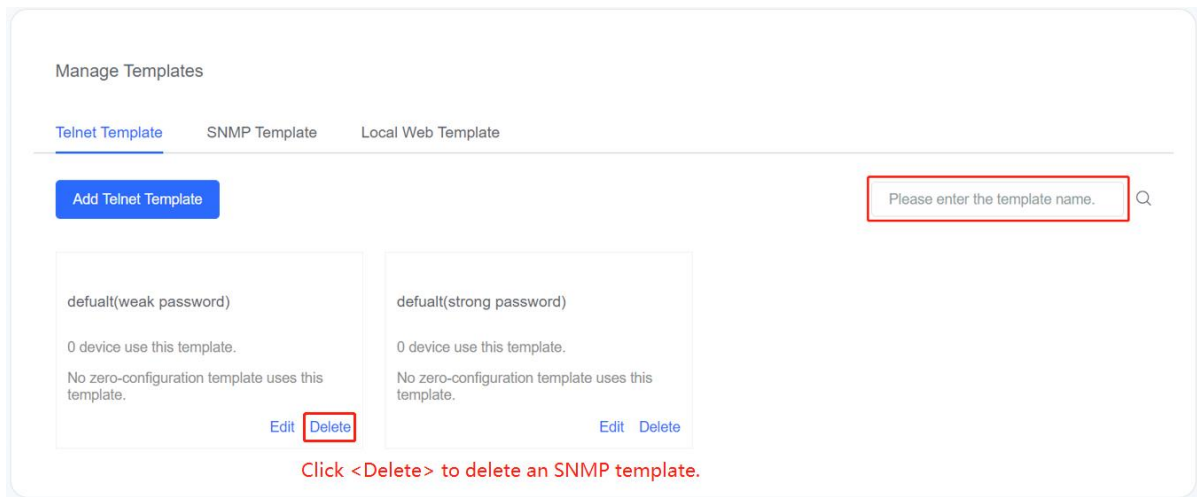


● Configuring a Trap Server Address in the SNMP Template



● Deleting an SNMP Template

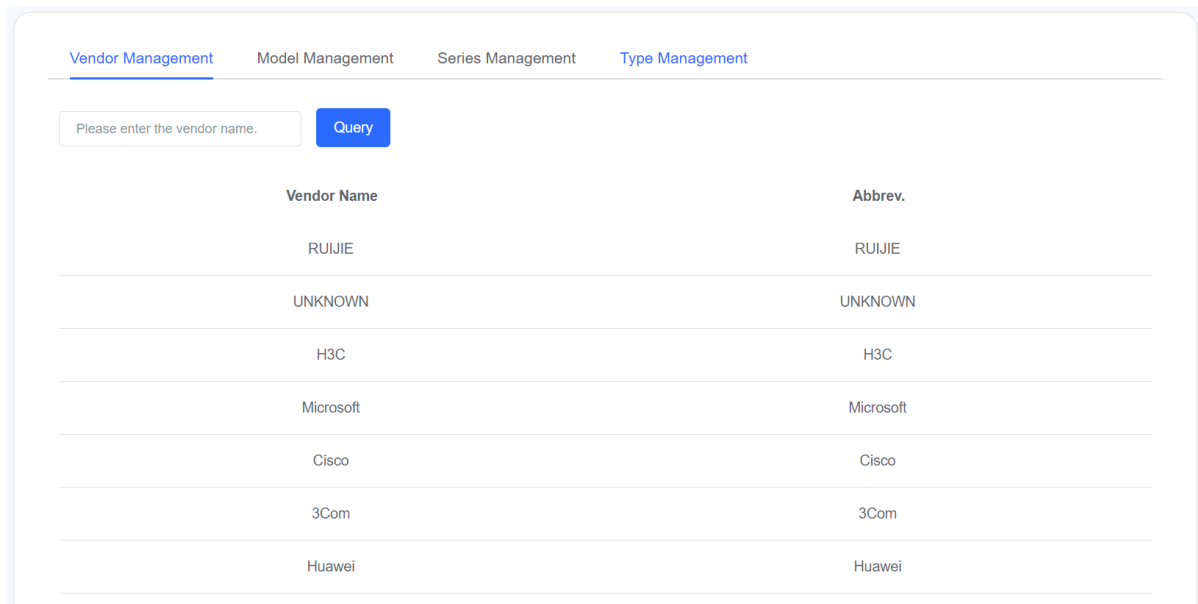
The SNMP template that is associated with a switch or is a default template cannot be deleted.



Managing the Switch Model Library

(1) Managing Switch Vendors

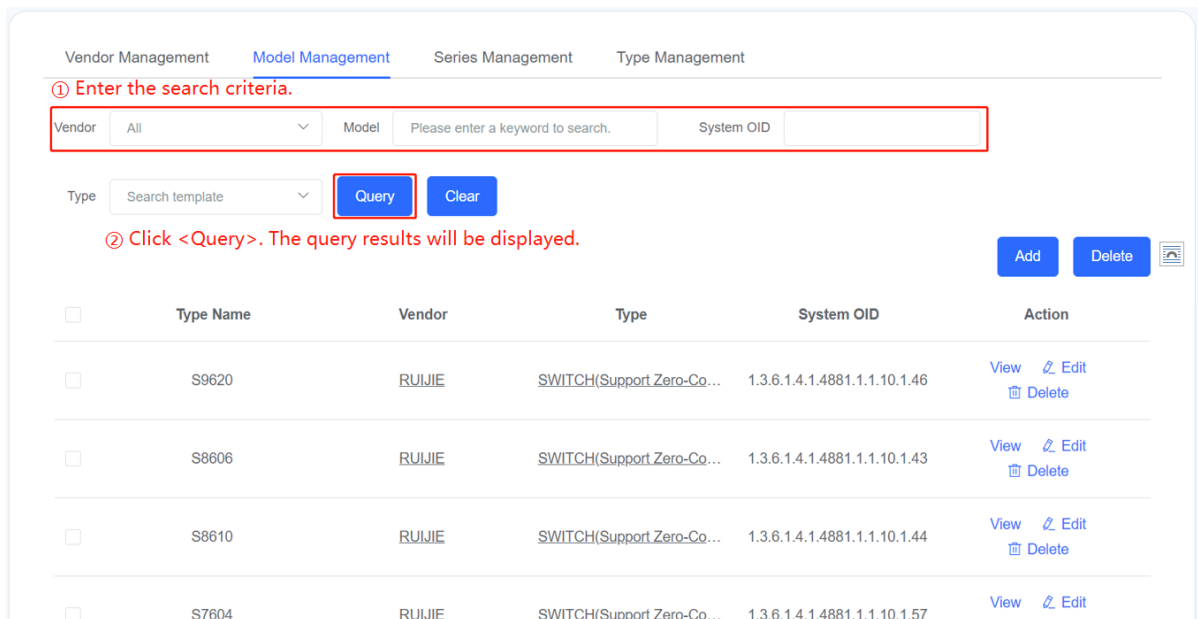
On the **Vendor Management** page, you can view vendors and their abbreviations supported in the model library supported by the system.



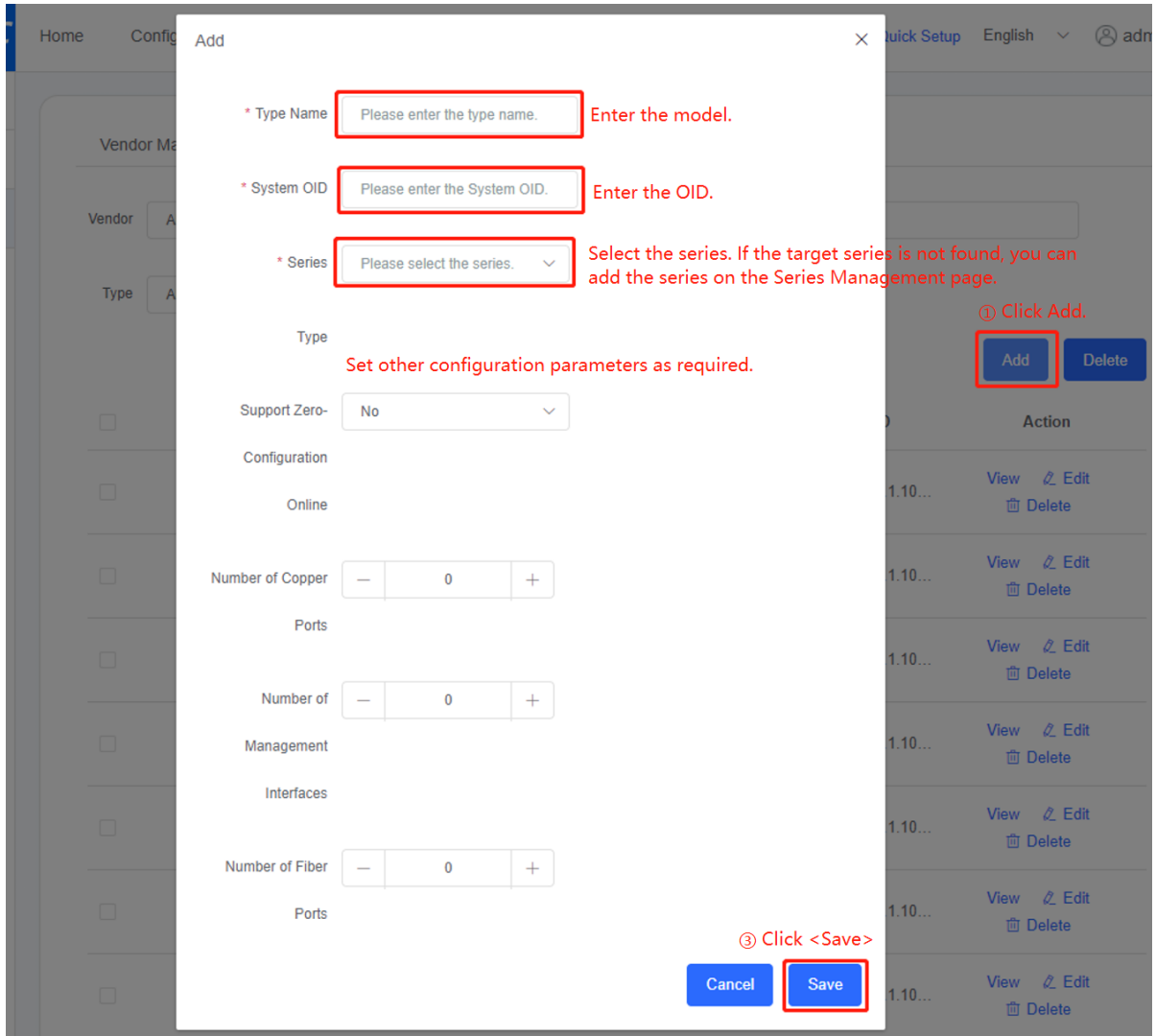
(2) Managing Switch Models

On the **Model Management** page, you can view the model library supported by the system. You can also add, delete, and edit switch models.

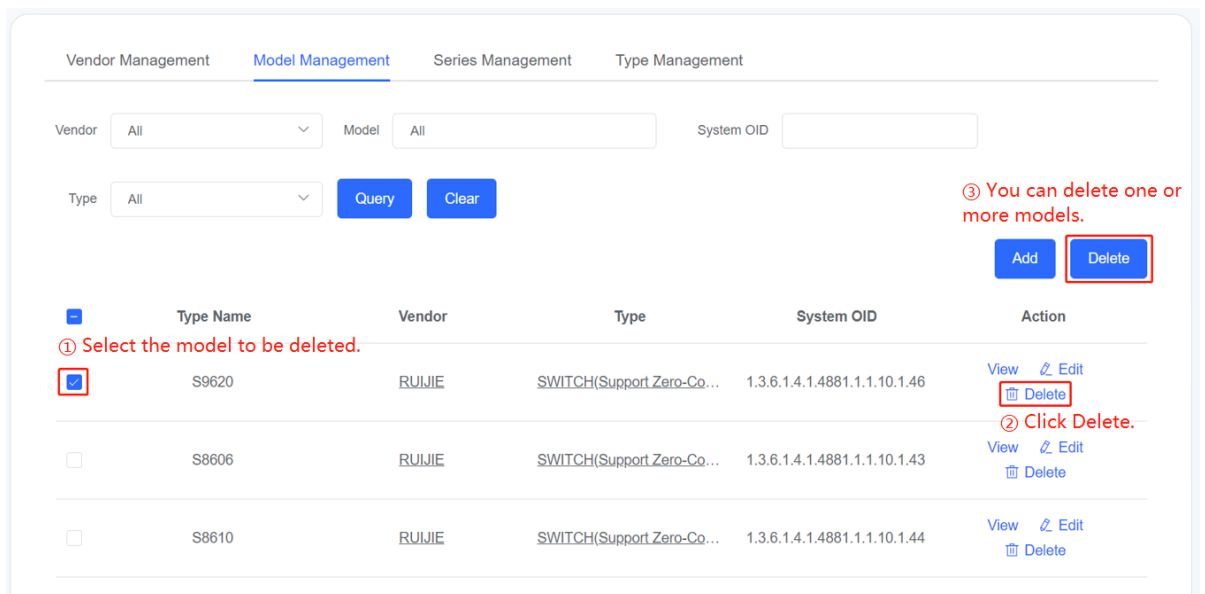
● **Querying a switch model**



● **Adding a switch model**



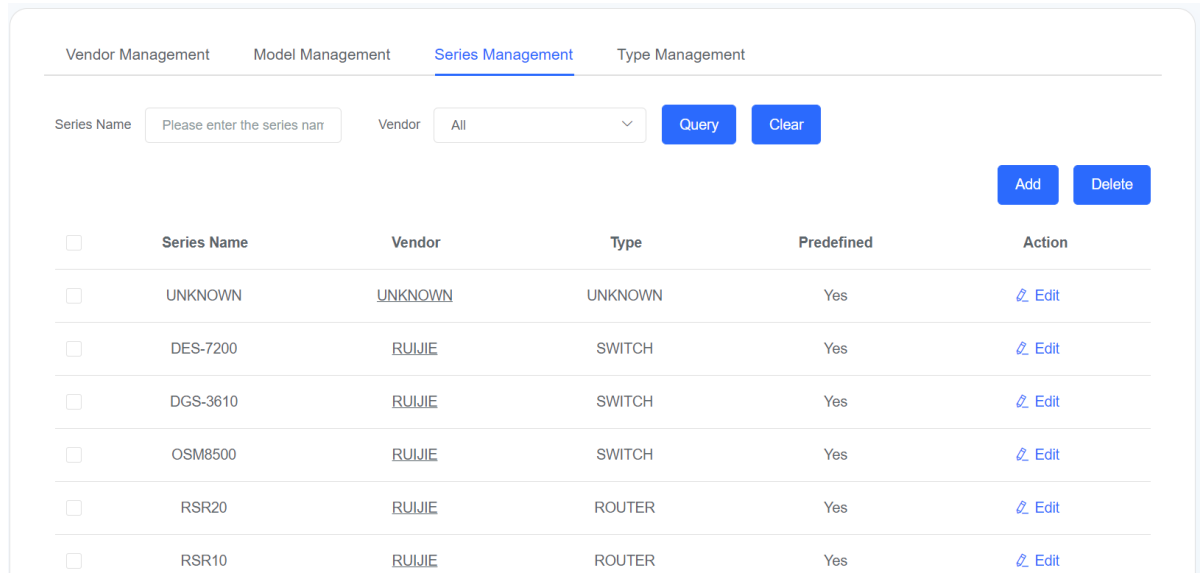
● **Deleting a switch model**



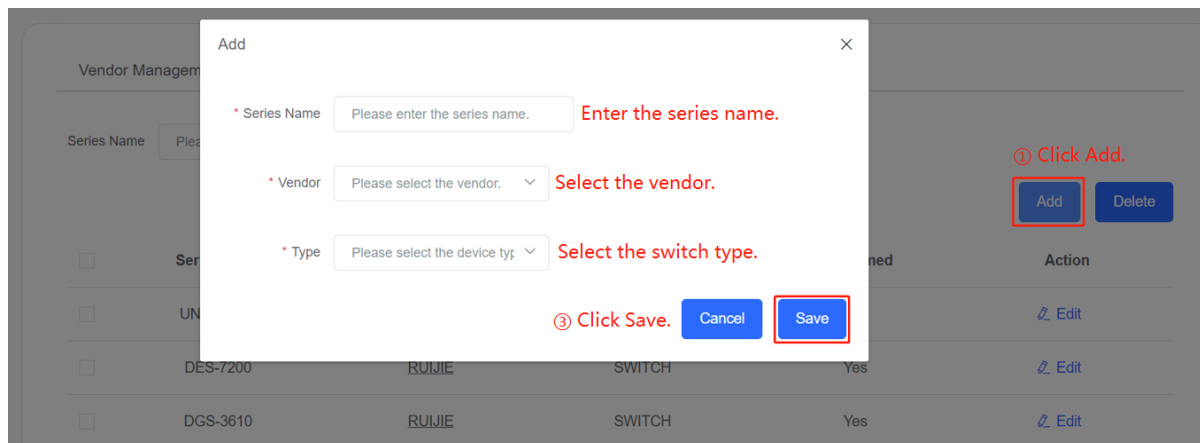
Managing Switch Series

On the **Series Management** page, you can manage switch series, including querying, deleting, or adding a switch series.

- **Querying a switch series**

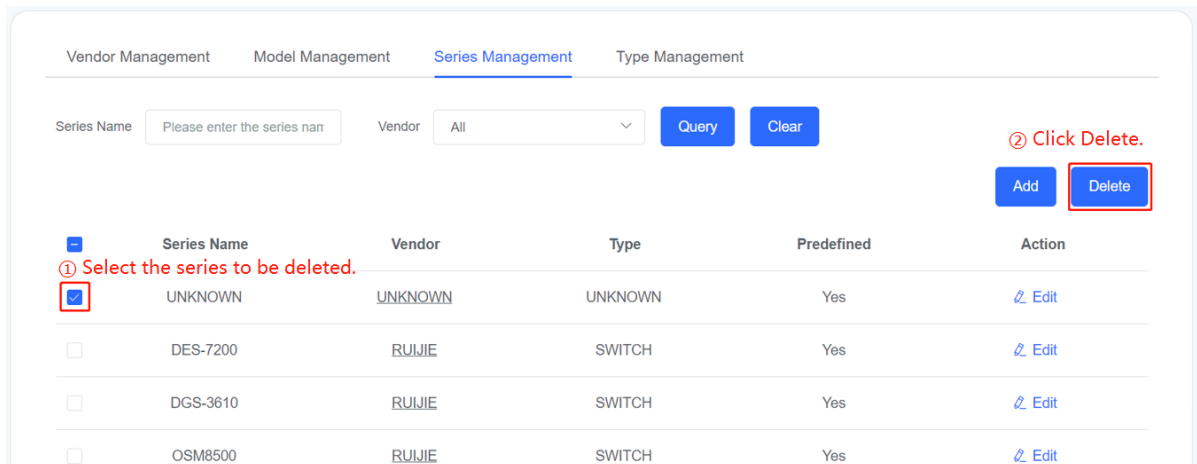


- **Adding a switch series**



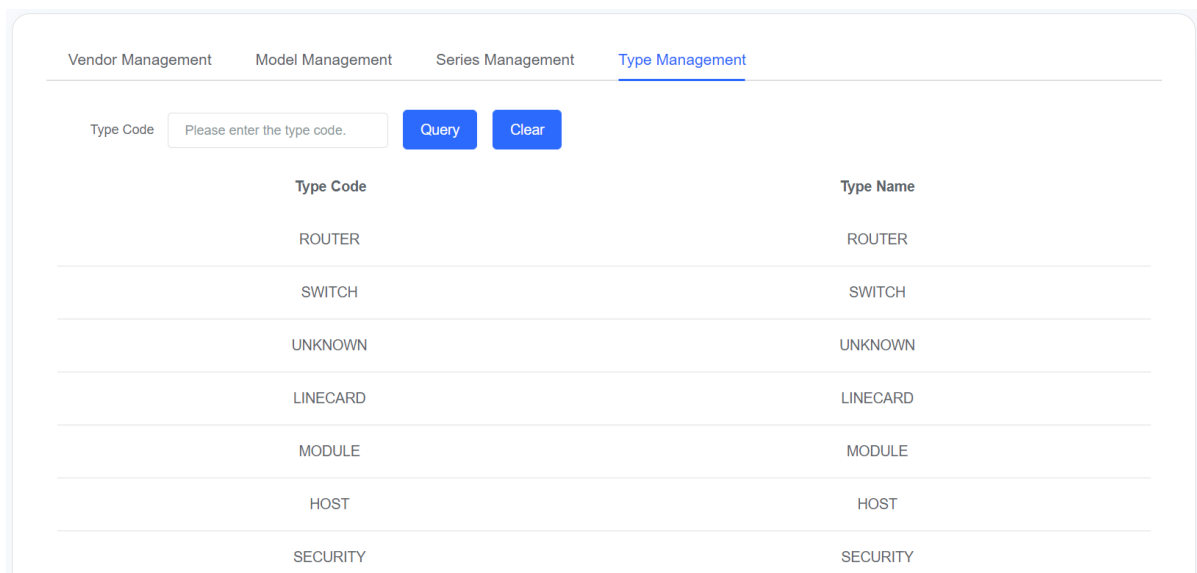
- **Deleting a switch series**

A referenced series cannot be deleted.



Managing Switch Types

On the **Type Management** page, you can query switch types supported by the system.



4. Upgrading a Switch

Upgrading the Switch Software

You can upgrade the bin file of the managed switches by clicking **Bulk Update**.

- Query the switch to be upgraded by entering the search criteria, and select the switch (only switches of the same model can be upgraded in a batch).

Filter Model Please enter a keyword to search. Hardware Version All Software Version All Clear

You can query a switch by entering the search criteria.

More

You can also query a switch by entering the switch's management IP address or name.

Please enter the device management IP or name. Bulk Update

② Click <Bulk Update>

<input type="checkbox"/>	Management IP	Name	Vendor	Model	Hardware Version	Software Version	Area	Action
No Data								

① Select the switches to be upgraded.

Total 0 10/page < 1 > Go to 1

- Upload the bin file and start upgrade. This operation has potential risks. Proceed with caution.

Device List:

Management IP	Name	Model	Area	Hardware Version	Software Version	Connectivity
66.1.1.2	66.1.1.2	SF2910-4GT2XS-P	defaultArea	1.00	SF29_RGOS 11.4(1)B...	Telnet

Choose an upgrade package:

Select Upgrade Package ① Select the bin file.

② The upgrade can succeed only when the Telnet connectivity is normal.

③ Click <Delivered to 1 devices> Delivered to 1 devices Cancel

- Wait for the upgrade process to finish. If you exit the page and open the upgrade page again, you can still view the upgrade progress.

5. Performing Backup

Performing Backup and Recovery

With configuration backup and recovery, you can manage the configurations of the managed switches.

Due to the limited storage space of the switch, the system allows a maximum of five records for a single switch.

Area Global

66.1.1.2 ① Select the switch you want to back up or view.

Total 1 < 1 >

Management IP:66.1.1.2 Manufacturer:ruijie

Current Config Manually Back Up

Reading configuration...Please wait.

② Click <Manually Back Up> if you want to back up the configuration.

The actual configuration of the selected switch is displayed here in real time.

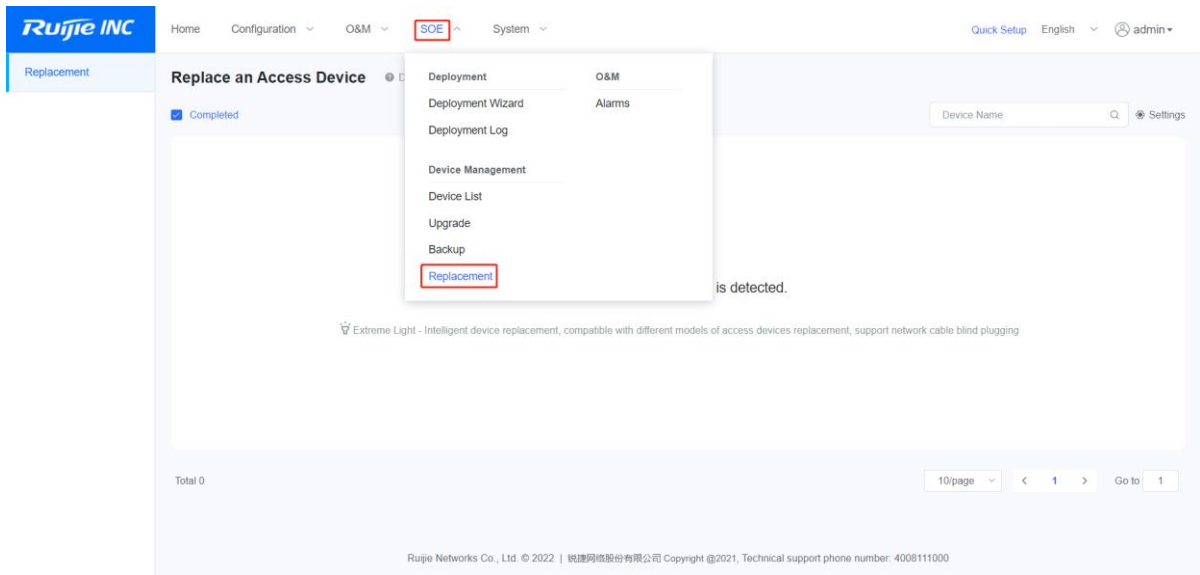
Backup configuration Restore This Backup

③ You can select and view configuration backup in a given period of time.

No Backup ④ Click <Restore This Backup> to restore the configuration.

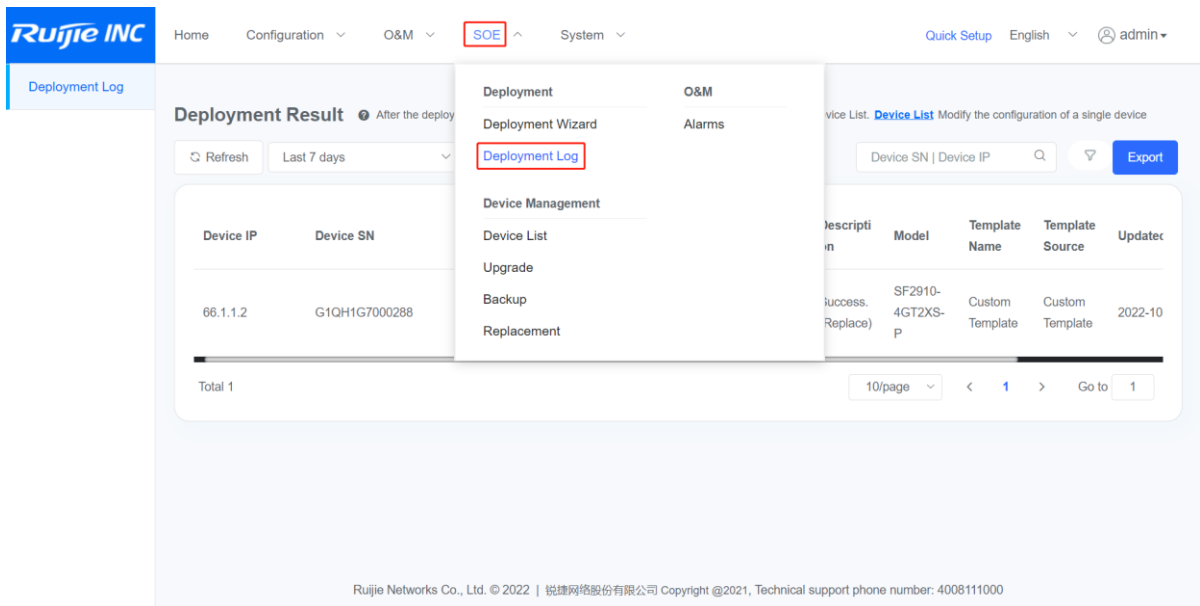
6. Replacing a Switch

Choose **SOE > Replacement**. The **Replacement** page is displayed.



If a switch fails, an O&M engineer can replace the faulty switch with a new one by installing the optical fiber or network cable connected to the faulty switch into the new switch.

Choose **SOE > Deployment Log**. The **Deployment Log** page is displayed.



You can view the replacement results on the **Deployment Log** page.

Deployment Result After the deployment finishes, you can modify the configuration of a single device in the Device List. [Device List](#) Modify the configuration of a single device

Last 7 days
 Only show failures
 Device SN | Device IP

Device IP	Device SN	Name	Area	Location	Management Status	Description	Model	Template Name	Template Source	Updated
66.1.1.2	G1QH1G7000288	66.1.1.2	defaultArea		Managed	Success. (Replace)	SF2910-4GT2XS-P	Custom Template	Custom Template	2022-10

Total 1 10/page < 1 > Go to

7. Configuring the Alarm Module

You can view, export, and handle alarms of the switches managed by the system in **Alarm Module**, and set the alarm storage time and expiration time.

1. Viewing alarms

Alarm Alarm Settings

Alarm Level All Major Moderate Minor
Query alarms by the switch's IP address.
Advanced filter

Filter alarms by the alarm severity. Select one or more items from the <Advanced filter drop-down> list box.

Last Alarm Time	Alarm Level	Number of Re	Name	Device IP	Device ID	Alarm Event	Description	Status	Action
2022-08-29 08:54:36	Major	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	The optica...	Expired	View Details
2022-08-29 08:49:36	Moderate	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	接口【Te0...	Expired	View Details
2022-08-28 23:27:53	Major	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	The optica...	Expired	View Details
2022-08-28 23:22:45	Moderate	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	接口【Te0...	Expired	View Details
2022-08-27 23:37:07	Major	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	The optica...	Expired	View Details
2022-08-27 23:31:07	Moderate	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	接口【Te0...	Expired	View Details

2. Exporting alarms

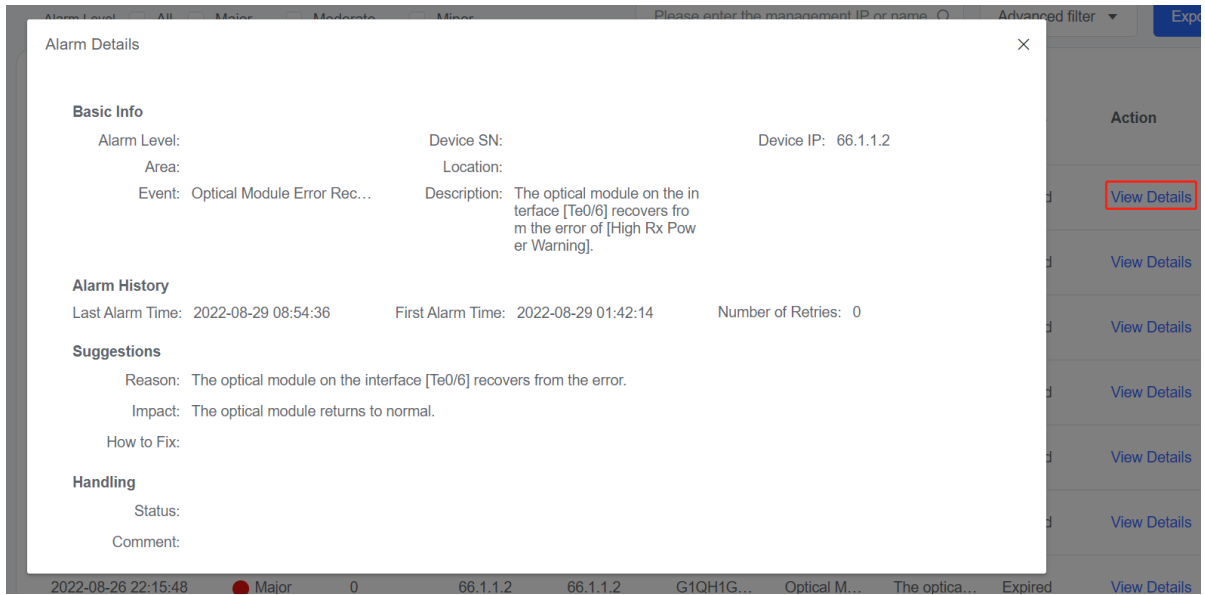
Alarm Alarm Settings

Alarm Level All Major Moderate Minor
Please enter the management IP or name
Advanced filter

Download alarms into an Excel file.

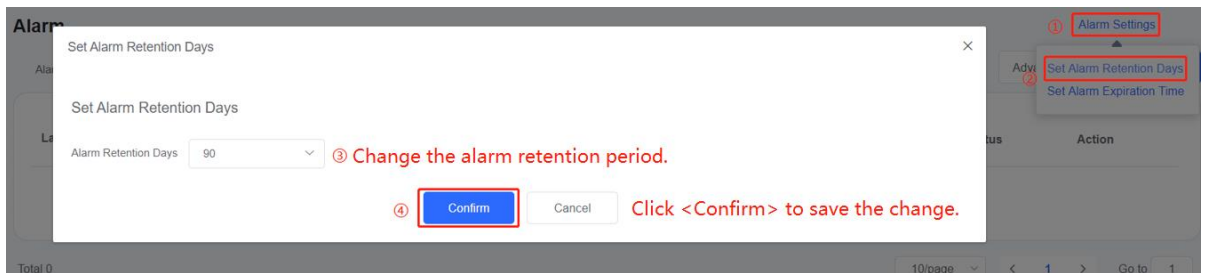
Last Alarm Time	Alarm Level	Number of Re	Name	Device IP	Device ID	Alarm Event	Description	Status	Action
2022-08-29 08:54:36	Major	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	The optica...	Expired	View Details
2022-08-29 08:49:36	Moderate	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	接口【Te0...	Expired	View Details
2022-08-28 23:27:53	Major	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	The optica...	Expired	View Details
2022-08-28 23:22:45	Moderate	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	接口【Te0...	Expired	View Details
2022-08-27 23:37:07	Major	0	66.1.1.2	66.1.1.2	G1QH1G...	Optical M...	The optica...	Expired	View Details

3. Viewing and handling alarms

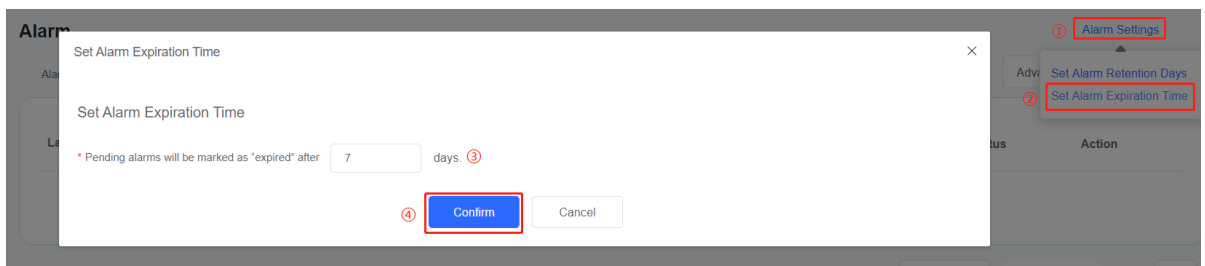


4. Setting the alarm retention period

To save the switch's storage space, set a proper alarm retention period.



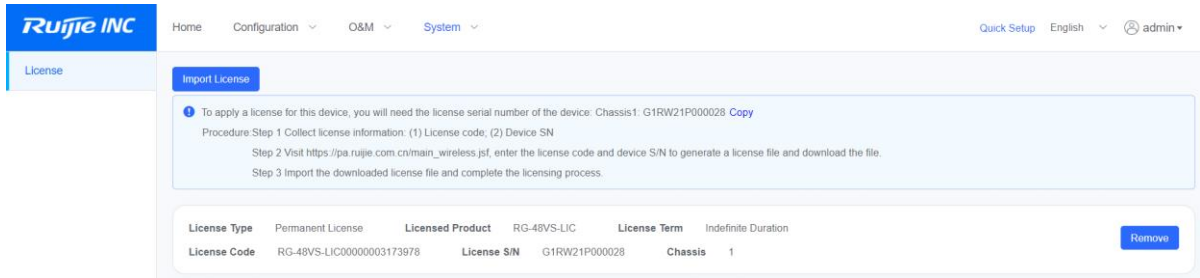
5. Setting the alarm expiration time



1.3.8 System

1. License

- Sample License



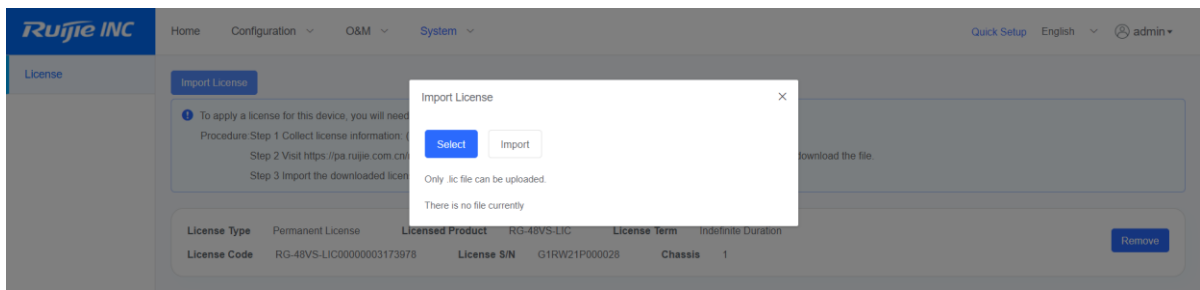
- Importing a license

Procedure:

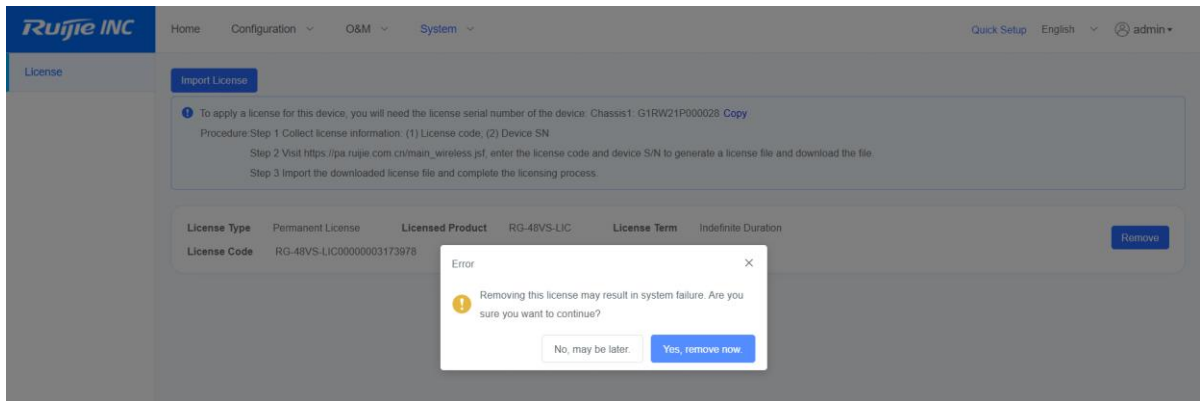
Step 1: Collect the license information, including the license code and license SN.

Step 2: Visit https://pa.ruijie.com.cn/main_wireless.jsf. Enter the license code and license SN to generate a license file, and download the license file.

Step 3: Import the downloaded license file.



- Removing a license



2. Admin Account

In addition to the admin account that comes with the eWeb management system, you can also create and maintain other accounts (only the network administrator has this privilege).

1. Adding an account

Web-based Configuration Guide

Add

① Click <Add>

2 Enter the username.

* Account: You are advised to use your phone number as login account which is easy to remember.

3 Change the password.

* New Password: IR52glrm

A random password has been generated for you. You can change this password if necessary.

④ Click <Confirm> **Confirm** Cancel

2. Changing the password

Edit

Edit admin

* Old Password: **2 Enter the old password.**

* New Password: **3 Enter a new password.**

④ Click <Confirm> **Confirm** Cancel

3. Deleting an account (the admin account cannot be deleted)

	Username	Role	Action
<input type="checkbox"/>	admin	Super Administrator	Edit Delete

Total 1 10/page < 1 > Go to 1

1 Click <Delete>

Confirm on Delete

Are you sure you want to delete the account ?

2 Click <OK> Cancel **OK**

3. Certificates and Registration

Upload Certificate

Certificate file: (. crt format file)

Certificate private key: (. key format file)

Issued by: OU=localhostC=CN

Expiry Time: 2018-02-01~2028-01-30

ICP License Management

ICP License Number:

4. Operation Log

The operation log records users' key operations. You can query the operation log based on the search criteria.

Operation Log

Time to Username Login IP Type

Log Details

Time	Username	Login IP	Module	Type	Log Details
2022-09-30 10:39:07		172.26.1.107		Login	Operation succeeded.
2022-09-30 08:50:45		172.26.1.107		Login	Operation succeeded.
2022-09-30 08:50:22		172.26.1.107		Login	The username or password is incorrect.
2022-09-30 08:50:11		172.26.1.107		Login	The username or password is incorrect.
2022-09-30 08:49:44		172.26.1.107		Login	The username or password is incorrect.
2022-09-29 18:30:30		172.26.1.107		Login	Operation succeeded.
2022-09-29 16:33:13		172.26.1.107		Login	Operation succeeded.
2022-09-22 09:30:48		10.104.23.41		Login	Operation succeeded.
2022-09-06 19:34:25		10.104.23.41		Login	Operation succeeded.

Total 9

10/page < 1 > Go to 1

5. Performing Data Backup and Import

- Performing data backup

You can click **Export** to download the database file with the suffix **.db**.

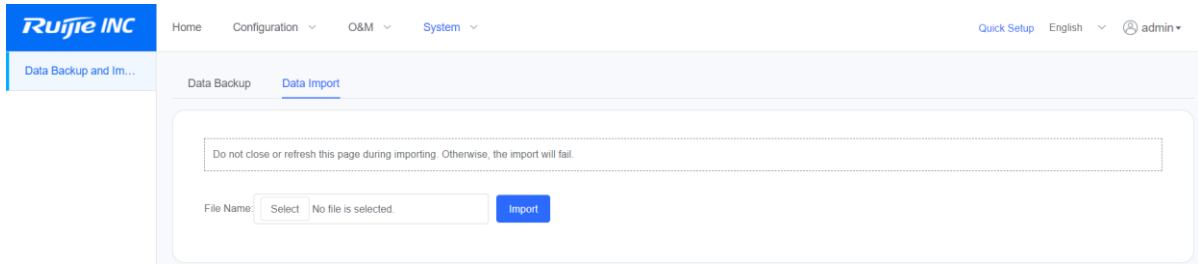
Ruijie INC Home Configuration O&M System Quick Setup English admin

Data Backup and Im... **Data Backup** Data Import

Export this Service's Current Data

- Importing data

The suffix of the imported database file must be .db, and the imported file version be the same as or earlier than the current database version.



1.4 Appendixes

1. About the INC-EMB License

Difference Between the INC-EMB License and the INC-STD License

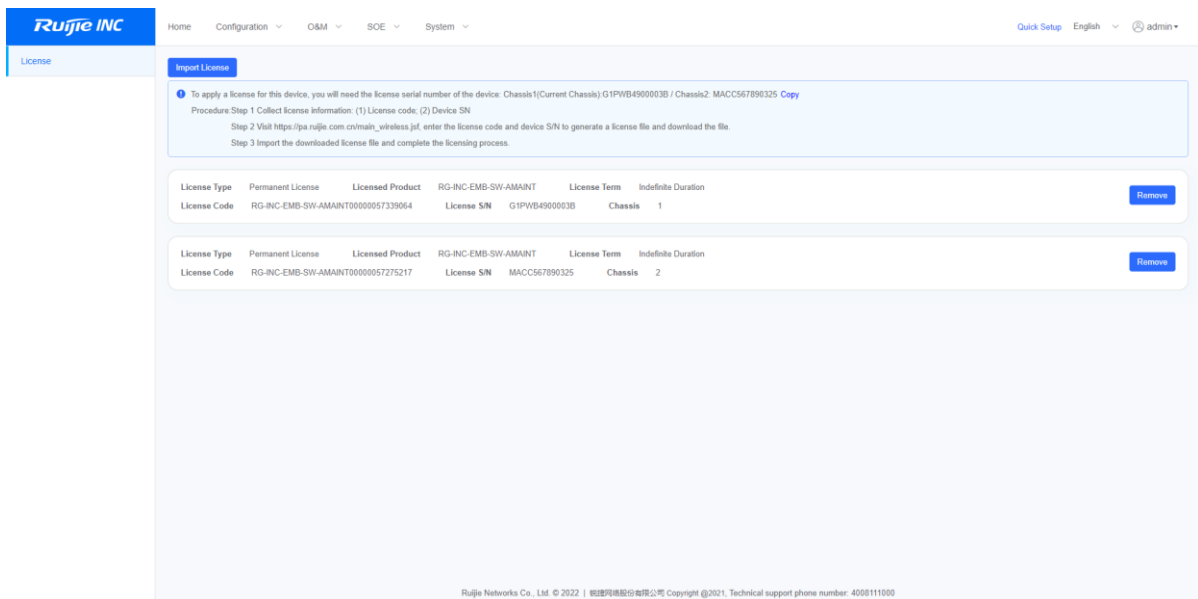
The INC-EMB license runs on the switch and is a device license, while the INC-STD license is an application software license.

Information on the License

- **Device SN**
- **License code**

Licensing Procedure

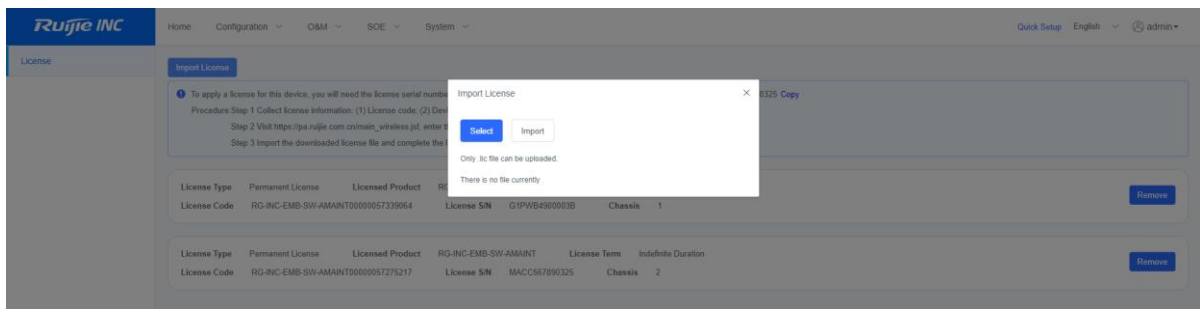
- You will be given a license code after purchasing a license.
- You must obtain the device SN on the switch by choosing **System > License**.



- Visit https://pa.ruijie.com.cn/main_wireless.jsf (Ruijie Networks's PA system), and enter the license code and switch SN on the PA system to generate a license file.



- Enter the license SN and license code, and click **Finish** to download the license file.
- Choose **System > License**, click **Select** to select the downloaded license file with the suffix *.lic from your local PC, and click **Import**.



- You can view or remove the imported license on the **License** page in the eWeb management system. You can view or remove other licenses in addition to the INC-EMB licenses on the **License** page.

