Ruijie Reyee RG-NBR Series Routers
RGOS 11.9(6)B16

Web-based Configuration Guide

Document Version: V1.0
Date: April 11, 2023

Copyright

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.

The content of this document will be updated from time to time due to product version upgrades or other reasons. 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

- The official website of Reyee: https://www.ireyee.com/
- Technical Support Website: https://www.ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Choose **System** > **Time**.

2. Signs

The signs used in this document are described as follows:

Danger

An alert that calls attention to safety operation instructions that if not understood or followed when operating the device can result in physical injury.

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

This manual introduces the features of the product and offers guidance on configuration and testing.

1 Product Overview

RG-NBR-E series enterprise-class routers are multi-service integrated routers tailored by Ruijie Reyee for integrated scenarios such as office, hotel, restaurant, entertainment, and scenic spot. RG-NBR-E series enterprise-class routers support many functions such as service acceleration channel, precise flow control, network access behavior management, VPN total-division interconnection, and intelligent routing, and support connection to Ruijie cloud platform (MACC free cloud platform) for remote cloud O&M and central management, which can well meet the integrated network needs of scenarios such as office, hotel, restaurant, entertainment, and scenic spot.

RG-NBR-E series enterprise-class routers support the web management GUI. The web management system can be used to configure and manage the common functions of the devices.

2 Device for Login

You can access the management IP address of the NBR-E enterprise-class device through the client (PC or mobile terminal device) for access to the web management system for device configuration and management.

2.1 Configuration Environment Requirements

The client (PC or mobile terminal) used for login to the web management system must meet the following environmental requirements:

- Browsers: Google Chrome, Internet Explorer 9.0, Internet Explorer 10.0, Internet Explorer 11.0, and some Google/Internet Explorer kernel-based browsers (for example, 360 Security Browser (recommended mode: Extreme)) are supported. If you log in to the web management system using other browsers, exceptions such as garbled characters or formatting errors may occur.
- Resolution: The recommended resolution specifications are 1024 x 768, 1280 x 1024, 1440 x 960, and 1600 x 900. At other resolutions, the fonts and formats may be out of alignment or not aesthetically pleasing.

2.2 Default Configurations

Table 2-1 Default web configurations

Function Item	Default Value
Device IP	● After initial configuration or restoration to factory settings, the default web management address is http://192.168.1.1. ● If HTTPS is used, the initial management address is https://192.168.1.1:4430.
User name/Password	admin/admin
Port	Gi0/0 port for connecting the PC to the device in router mode.

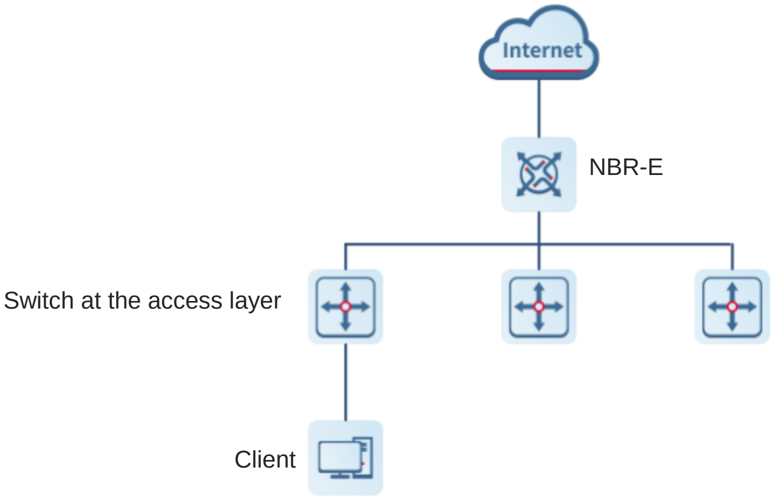
2.3 Login to the Web Management System Using a PC

2.3.1 Device Connection

To access the management page for router configuration, establish a network connection between the management client and the device.

Figure 2-1shows the connection between the device and the client.

Figure 2-1 Connection diagram



2.3.2 Management Client IP Address Configuration

Configure an IP address for the management client that is in the same network segment as the default IP address of the device (default IP address of the device: 192.168.1.1; subnet mask: 255.255.255.0) so that the management client can access the device. For example, set the IP address of the management client to 192.168.1.200.

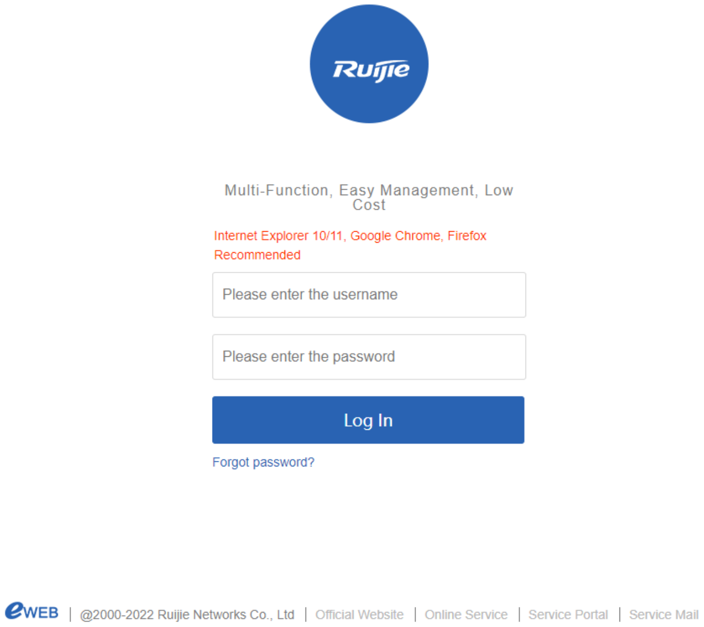
2.3.3 Login to the Web Management System

Prerequisites

Both the web management upgrade package of the NBR series device (the **web.gz** package exists on the device) and the NGX environment for web operation have been verified for web management. Otherwise, the web management page is not displayed. The files and environment have been installed by default on the device. If they are not installed, perform installation according to the methods mentioned in the user guide.

Procedure

(1) Open a browser, enter the IP address of the device (192.168.1.1 by default) in the address box, and press Enter. The login page is displayed.



Multi-Function, Easy Management, Low Cost

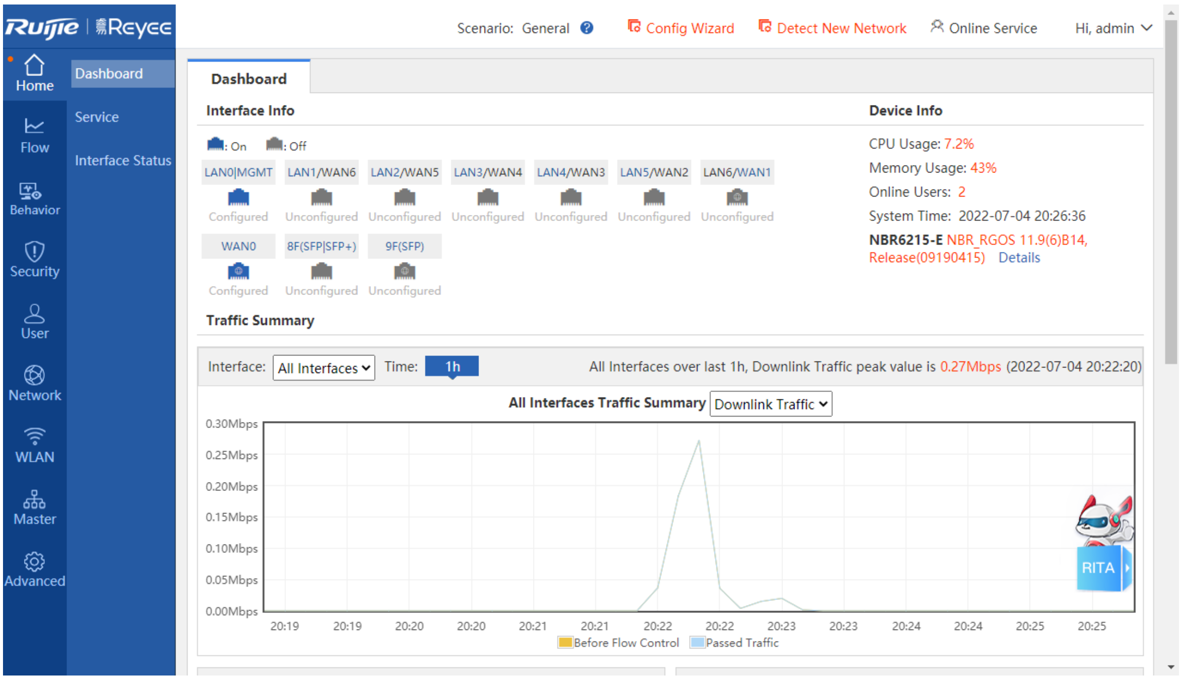
Internet Explorer 10/11, Google Chrome, Firefox Recommended

@2000-2022 Ruijie Networks Co., Ltd

On the login page:

- If you forget your user name or password, click **Forgot password?**
- If customer service assistance is required, click **Online Service** at the bottom of the page to contact our customer service online.

(2) Enter the user name and password and click Log In. The home page of the web management system is displayed.



Scenario: General

Interface Info: LAN0|MGMT Configured; LAN1/WAN6 Unconfigured; LAN2/WAN5 Unconfigured; LAN3/WAN4 Unconfigured; LAN4/WAN3 Unconfigured; LAN5/WAN2 Unconfigured; LAN6/WAN1 Unconfigured; WAN0 Configured; 8F(SFP|SFP+) Unconfigured; 9F(SFP) Unconfigured

Device Info

CPU Usage: 7.2%

Memory Usage: 43%

Online Users: 2

System Time: 2022-07-04 20:26:36

NBR6215-E NBR_RGOS 11.9(6)B14, Release(09190415) Details

Interface: All Interfaces Time: 1h

All Interfaces over last 1h, Downlink Traffic peak value is 0.27Mbps (2022-07-04 20:22:20)

All Interfaces Traffic Summary: Downlink Traffic

Follow-up Procedure

- For device security, you are recommended to change the default password upon your first login to the web management system.
- If you forget the IP address or password, you can press and hold the reset button on the device panel for more than 5s when the device is powered on to restore the device to factory settings. You can use the default

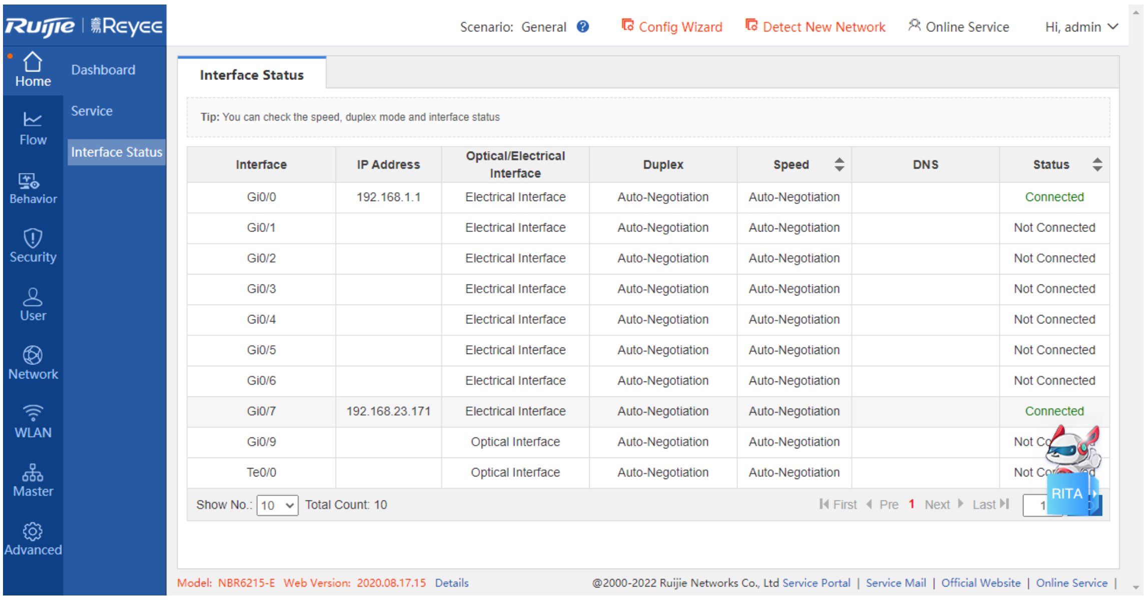
IP address and password for login after restoration.

Caution

Exercise with caution. If restoration to factory settings is performed, the existing configurations will be deleted, and you need to re-configure information next time you log in to the device.

2.4 Main Page of the Web Management System

The following figure shows the main page of the web management system.



Tip: You can check the speed, duplex mode and interface status

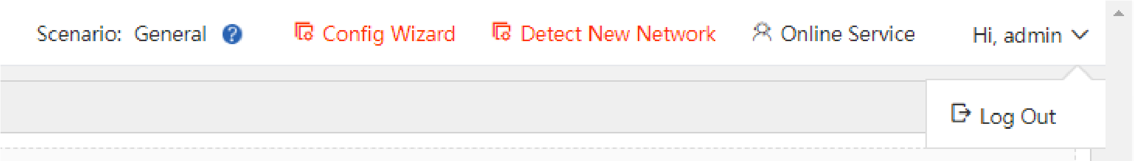
Interface	IP Address	Optical/Electrical Interface	Duplex	Speed	DNS	Status
Gi0/0	192.168.1.1	Electrical Interface	Auto-Negotiation	Auto-Negotiation		Connected
Gi0/1		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/2		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/3		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/4		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/5		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/6		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/7	192.168.23.171	Electrical Interface	Auto-Negotiation	Auto-Negotiation		Connected
Gi0/9		Optical Interface	Auto-Negotiation	Auto-Negotiation		Not Co
Te0/0		Optical Interface	Auto-Negotiation	Auto-Negotiation		Not Co

Show No.: 10 Total Count: 10 First Pre 1 Next Last 1

Model: NBR6215-E Web Version: 2020.08.17.15 Details @2000-2022 Ruijie Networks Co., Ltd Service Portal | Service Mail | Official Website | Online Service |

2.4.1 Title Area

This area provides links to some commonly used functions for you to quickly access the corresponding setup pages, including **Config Wizard**, **Detect New Network**, **Online Service**, and **Log Out**.



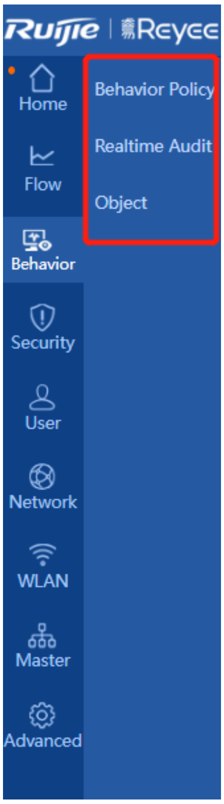
Function Item	Description	Reference Chapter/Section
Config Wizard	Wizard-based configurations are provided. You can click it for quick device access to the network.	3.1 Quick Configuration
Detect New Network	You can click it to complete integrated configuration when a new device is connected to the networking environment.	3.2 Reyee Integrated Configuration

Function Item	Description	Reference Chapter/Section
Online Service	You can click it to contact our online customer service for consultation in case of problems during use.	N/A
Log Out	After completing related operations, you can click it to exit the current page. The login page is displayed.	N/A

2.4.2 Menu Navigation Area

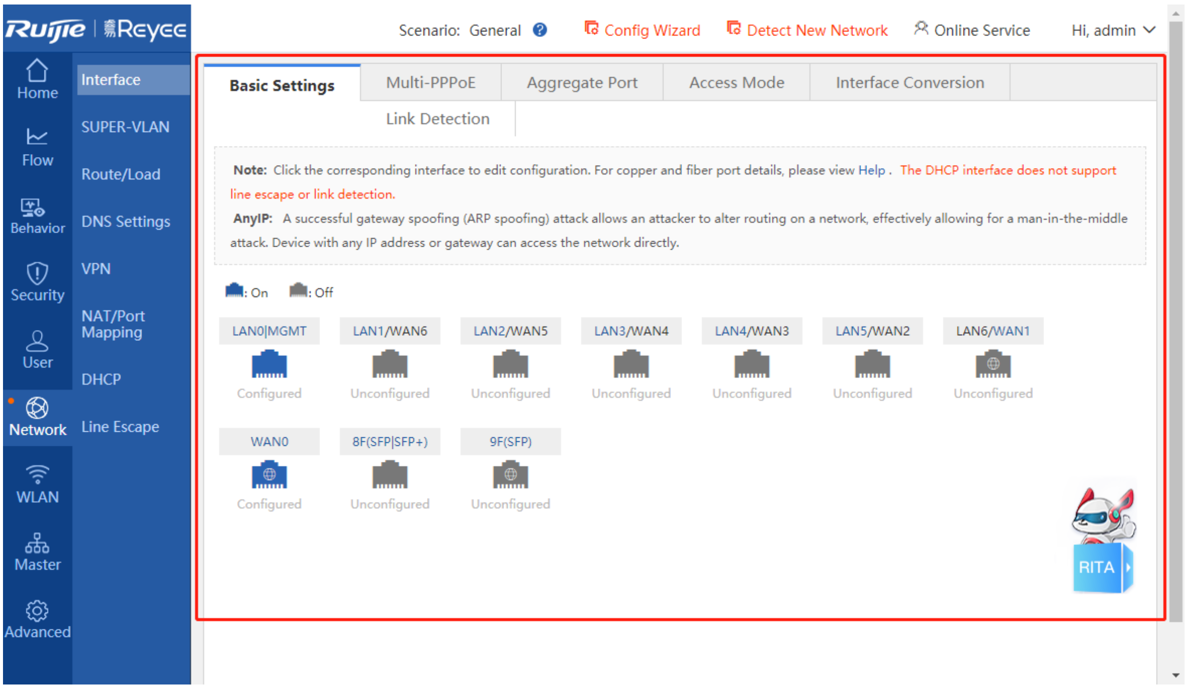
The NBR menu navigation area is displayed on the left of the main page of the web management system, where all NBR function menu items are listed. After you choose a menu item in the navigation tree on the left, the detailed setup page is displayed in the main operating area.

The system uses a two-level menu structure. After you choose a function menu item in the navigation tree, the corresponding sub-item menu is displayed. For example, after you choose **Behavior** in the navigation tree, the sub-item menu corresponding to the function category is displayed, as shown in the following figure.



2.4.3 Main Operating Area

You can complete NBR function configurations in this area. After you choose a menu item in the navigation tree on the left or click a shortcut function item on the top, the corresponding detailed setup page is displayed in the main operating area.



Ruijie | Reyee

Home, Flow, Behavior, Security, User, Network, WLAN, Master, Advanced

Interface, SUPER-VLAN, Route/Load, DNS Settings, VPN, NAT/Port Mapping, DHCP, Line Escape

Scenario: General ? | Config Wizard | Detect New Network | Online Service | Hi, admin

Basic Settings | Multi-PPPoE | Aggregate Port | Access Mode | Interface Conversion | Link Detection

Note: Click the corresponding interface to edit configuration. For copper and fiber port details, please view Help . The DHCP interface does not support line escape or link detection.

AnyIP: A successful gateway spoofing (ARP spoofing) attack allows an attacker to alter routing on a network, effectively allowing for a man-in-the-middle attack. Device with any IP address or gateway can access the network directly.

: On : Off

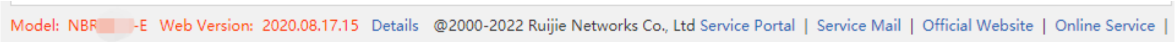
LAN0|MGMT	LAN1/WAN6	LAN2/WAN5	LAN3/WAN4	LAN4/WAN3	LAN5/WAN2	LAN6/WAN1
Configured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Unconfigured

WAN0	8F(SFP|SFP+)	9F(SFP)
Configured	Unconfigured	Unconfigured

RITA

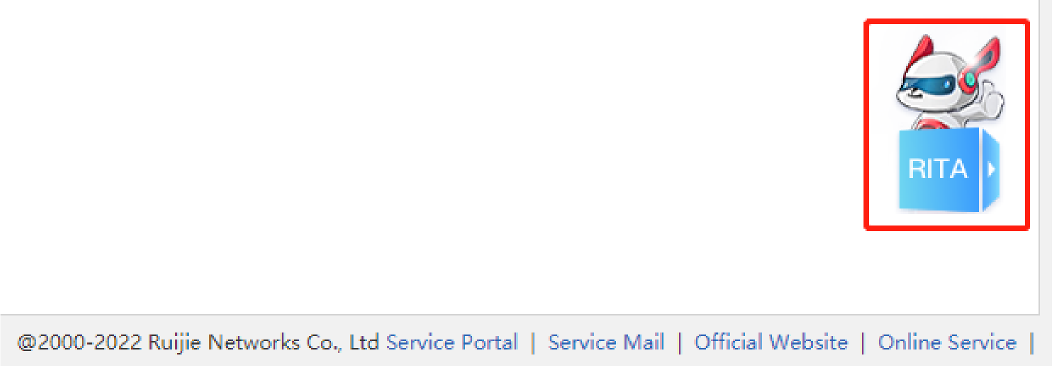
2.4.4 Status Area

In this area, the device model and version are displayed on the left, and the technical forum website link and technical support contact information are displayed on the right. You can contact our customer service for assistance in case of problems during use through the two contact channels.



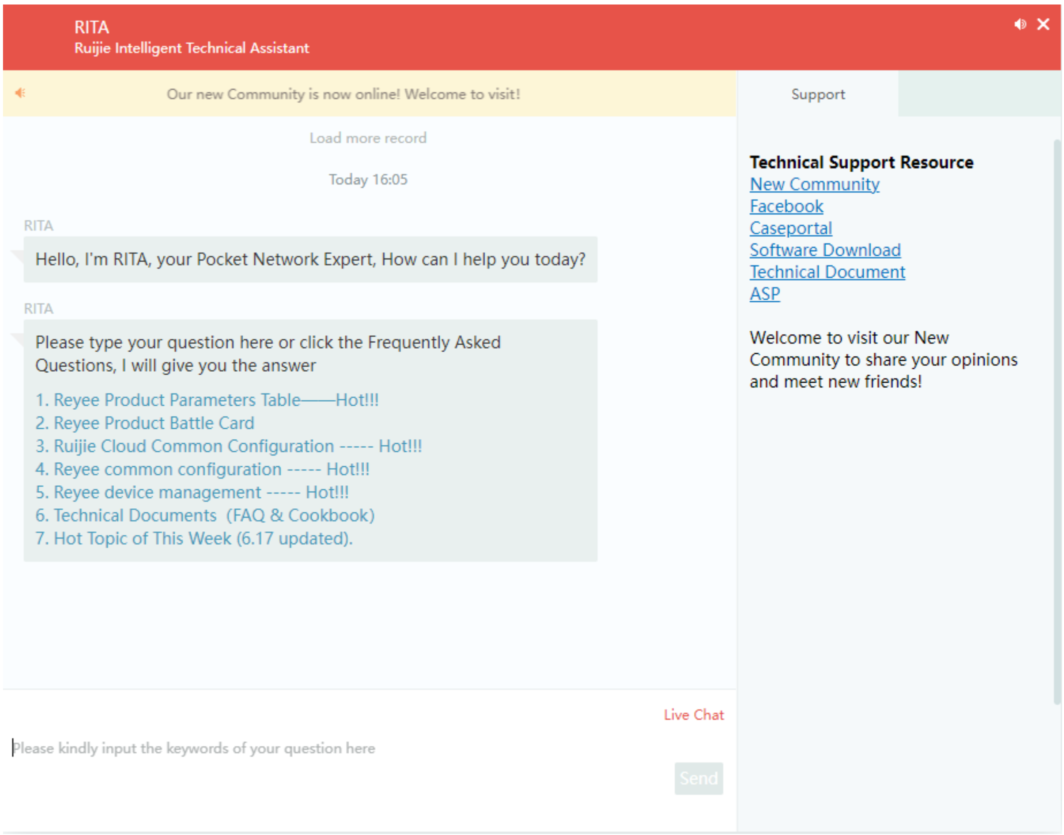
Model: NBR[redacted]-E Web Version: 2020.08.17.15 Details @2000-2022 Ruijie Networks Co., Ltd Service Portal | Service Mail | Official Website | Online Service |

You can click the RITA icon added in the lower right corner for consultation.



RITA

@2000-2022 Ruijie Networks Co., Ltd Service Portal | Service Mail | Official Website | Online Service |



RITA
Ruijie Intelligent Technical Assistant

Our new Community is now online! Welcome to visit!

Load more record

Today 16:05

RITA

Hello, I'm RITA, your Pocket Network Expert, How can I help you today?

RITA

Please type your question here or click the Frequently Asked Questions, I will give you the answer

1. Reyee Product Parameters Table——Hot!!!
2. Reyee Product Battle Card
3. Ruijie Cloud Common Configuration ----- Hot!!!
4. Reyee common configuration ----- Hot!!!
5. Reyee device management ----- Hot!!!
6. Technical Documents (FAQ & Cookbook)
7. Hot Topic of This Week (6.17 updated).

Support

Technical Support Resource
New Community
Facebook
Caseportal
Software Download
Technical Document
ASP

Welcome to visit our New Community to share your opinions and meet new friends!

3 Quick Configuration

3.1 Quick Configuration

Application Scenario

The device is in the empty configuration state upon your first login to the web management page. To simplify configuration, you are recommended to set the common functions of the device according to the corresponding wizard.

Note

- If this function is not required, click **Exit** to directly access the web management page. In this case, the device is in the empty configuration state. (Not recommended; Quick configuration is required. Otherwise, function exceptions such as flow control and default routing may occur even for the device to be upgraded to this version from an old version.)
- You can also click **Config Wizard** in the upper right corner of the main page of the web management system for quick configuration.

Prerequisites

- This function is supported only in router mode.
- The device has been connected to the power supply, and the WAN port of the device has been connected to the upper-level device with a network cable, or directly connected to the home network cable.
- The network access mode has been configured according to the requirements of the local network carrier.

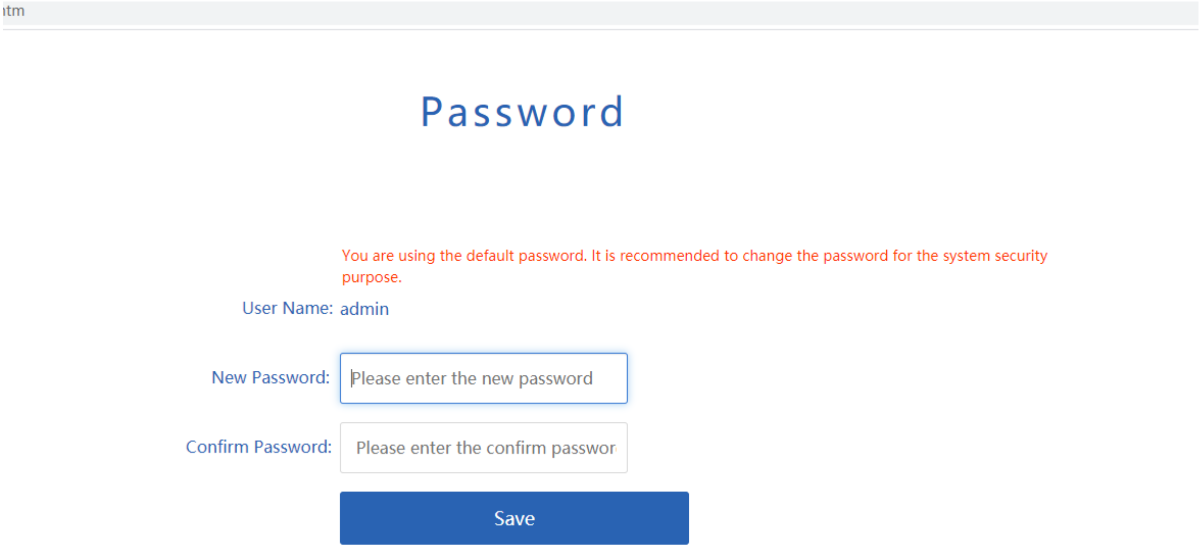
Otherwise, the setup may fail, resulting in network access failure. You are recommended to contact the local network carrier to verify the network access method (dynamic IP address/PPPoE(ADSL)/static IP address).

- If PPPoE(ADSL) is used, the corresponding broadband account and password are required.
- If the static IP address method is used, the corresponding IP address, subnet mask, router, and DNS are required.

Procedure

Complete related configurations according to the wizard.

(1) Reset the administrator password.



Password

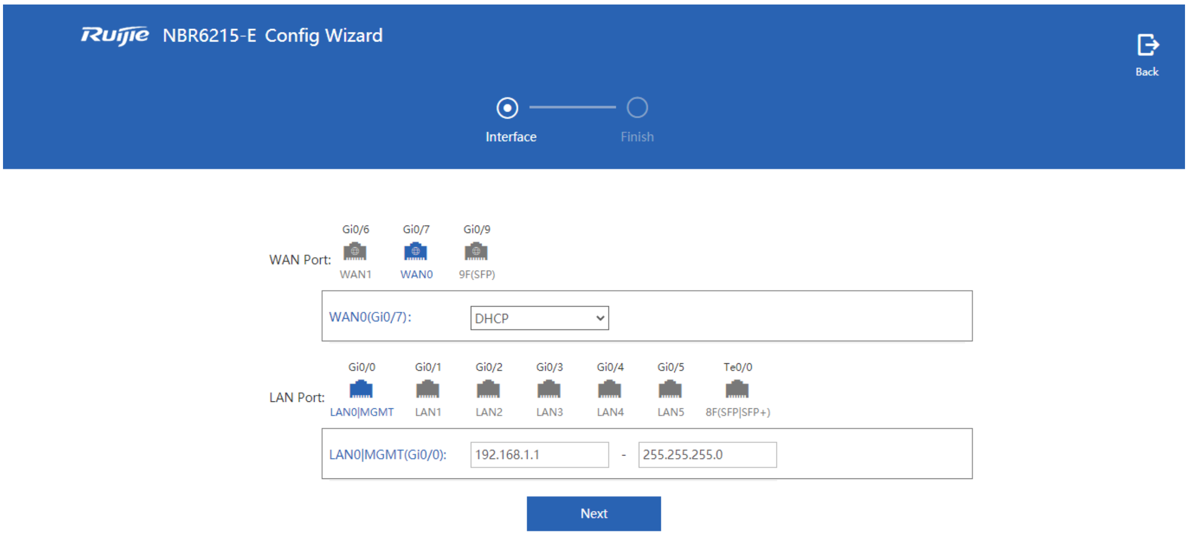
You are using the default password. It is recommended to change the password for the system security purpose.

User Name: admin

New Password: Please enter the new password

Confirm Password: Please enter the confirm passwor

(2) Configure the interface and click **Next**.



NBR6215-E Config Wizard

WAN Port: Gi0/6 WAN1, Gi0/7 WAN0, Gi0/9 9F(SFP)

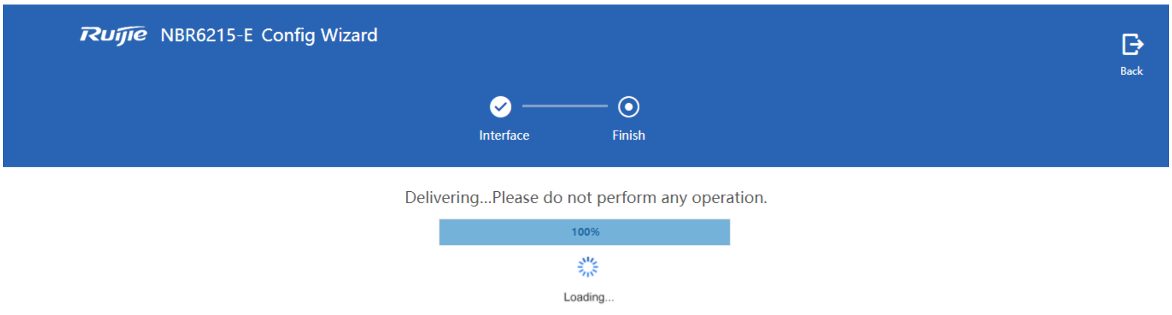
WAN0(Gi0/7): DHCP

LAN Port: Gi0/0 LAN0|MGMT, Gi0/1 LAN1, Gi0/2 LAN2, Gi0/3 LAN3, Gi0/4 LAN4, Gi0/5 LAN5, Te0/0 8F(SFP|SFP+)

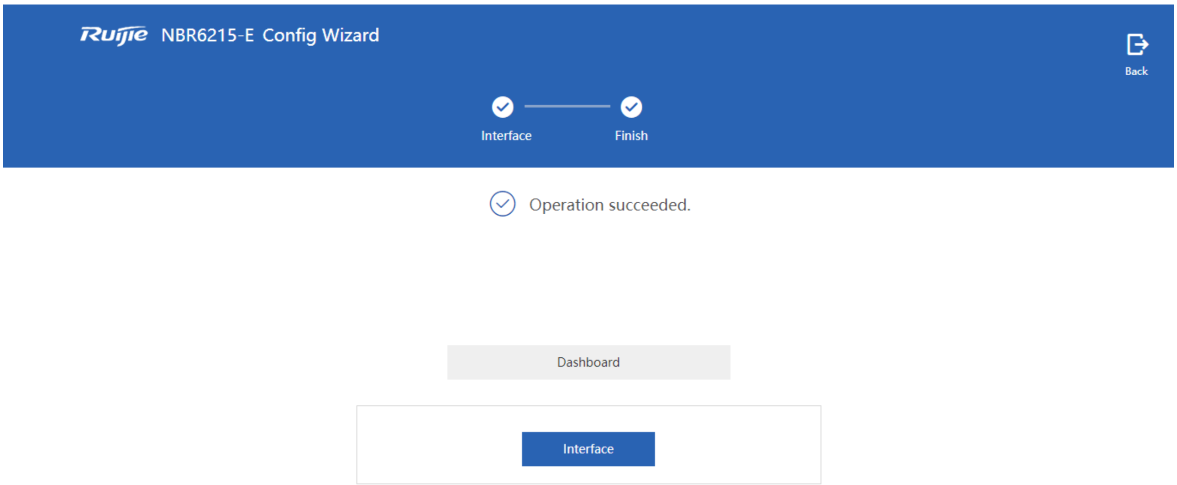
LAN0|MGMT(Gi0/0): 192.168.1.1 - 255.255.255.0

(3) Wait for the system to automatically deliver the configurations.

The system automatically delivers the configurations.



Delivering...Please do not perform any operation.



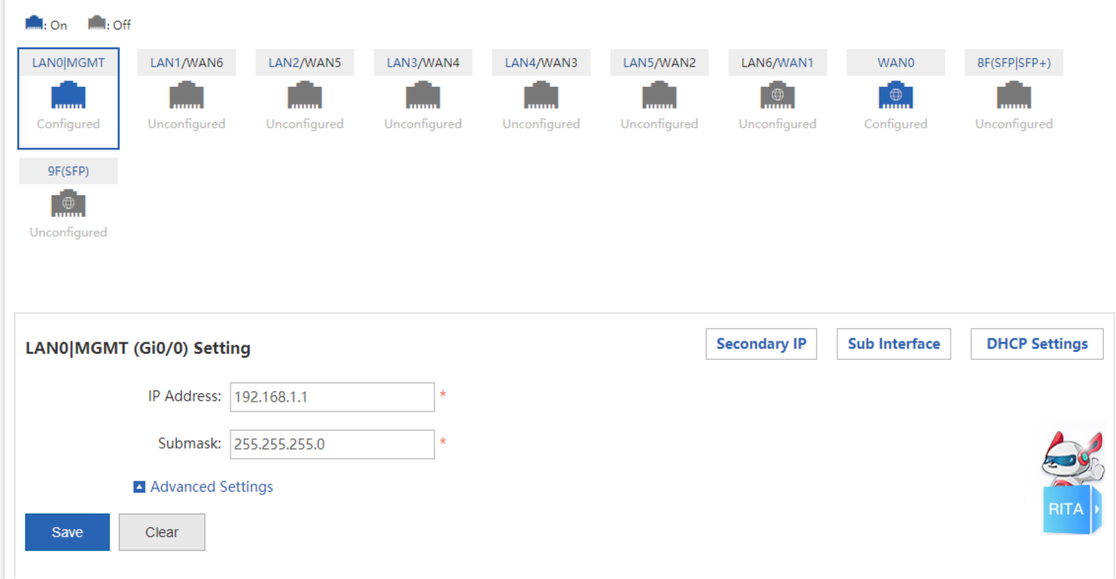
Operation succeeded.

Follow-up Procedure

(1) Click **Interface** for interface configuration.

Interface configuration is the key configuration for intranet access. Correct port information configuration ensures normal intranet access.

- Intranet port configuration: Select the intranet port to be configured, and set **IP Address** and **Submask** in the area below.

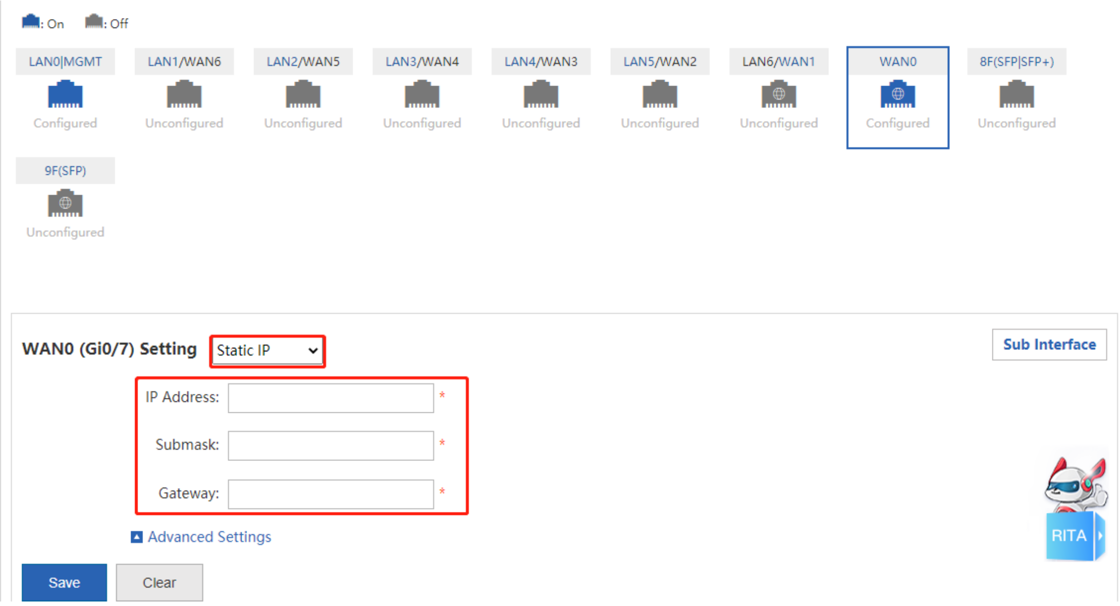


LAN0|MGMT (Gi0/0) Setting

IP Address: 192.168.1.1 *

Submask: 255.255.255.0 *

- Extranet port configuration: select the extranet port to be configured, and set the client IP address allocation method, bandwidth information, line type, and other information in sequence.
  - If you set the client network access method to **Static IP**, set the IP address of the carrier/intranet, subnet mask, and router, as shown in the following figure.



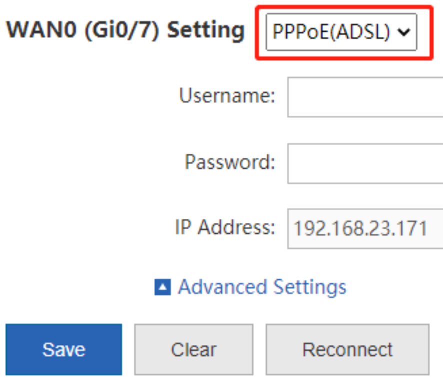
WAN0 (Gi0/7) Setting: Static IP

IP Address: *

Submask: *

Gateway: *

  - Set the client network access method to **PPPoE(ADSL)** if an ADSL line is applied for from the carrier, and configure related information, as shown in the following figure.



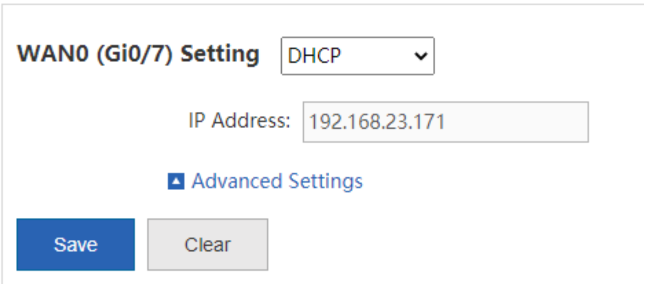
WAN0 (Gi0/7) Setting: PPPoE(ADSL)

Username: *

Password: *

IP Address: 192.168.23.171

  - If you set the client network access method to DHCP, no additional configuration is required.



WAN0 (Gi0/7) Setting: DHCP

IP Address: 192.168.23.171

Note

You can click **Advanced Settings** to set the upstream/downstream bandwidth of the line. Be sure to set bandwidth information correctly according to the actual bandwidth applied for from the carrier so that the device can manage the bandwidth for you in a better and more intelligent way.

(2) Click Save. In this case, you can manage the network operation status on the web management page.

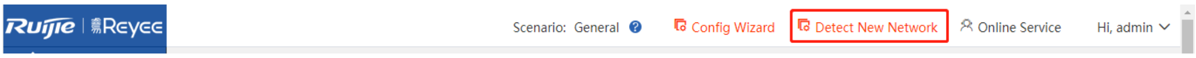
3.2 Reyee Integrated Configuration

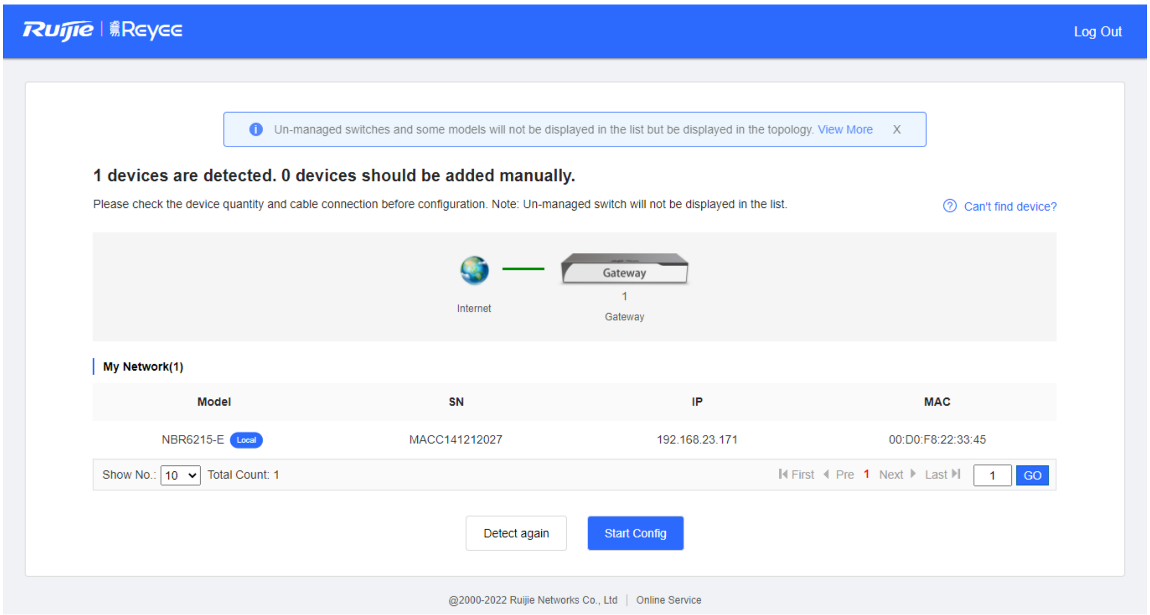
Application Scenario

You can click **Detect New Network** to complete integrated configuration when a new device is connected to the networking environment.

Procedure

(1) Click **Detect New Network** on the top of the page. The current networking information is displayed on the displayed page.





Un-managed switches and some models will not be displayed in the list but be displayed in the topology. View More X

1 devices are detected. 0 devices should be added manually.

Please check the device quantity and cable connection before configuration. Note: Un-managed switch will not be displayed in the list.

Can't find device?

My Network(1)

Model	SN	IP	MAC
NBR6215-E Local	MACC141212027	192.168.23.171	00:D0:F8:22:33:45

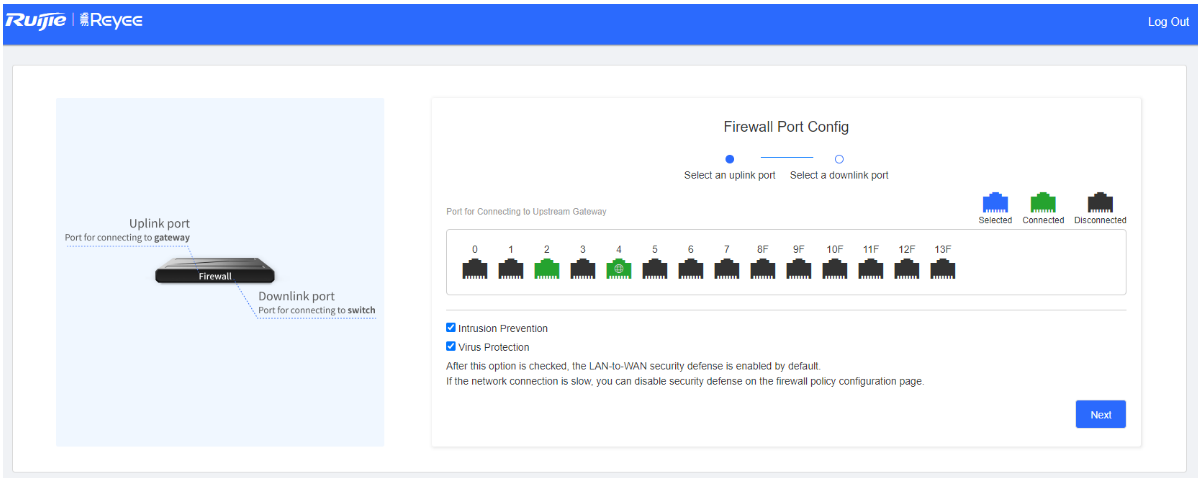
Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 GO

Detect again Start Config

@2000-2022 Ruijie Networks Co., Ltd | Online Service

(2) Click **Start Config**. If a firewall exists on the live network, configure the uplink and downlink ports based on actual networking.

(3)



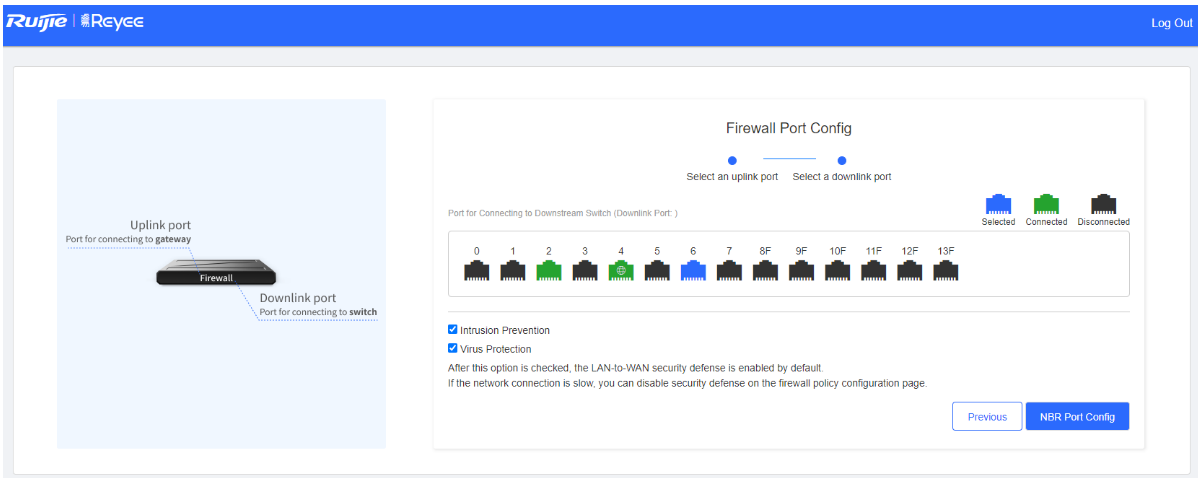
Firewall Port Config

Port for Connecting to Upstream Gateway

☑ Intrusion Prevention

☑ Virus Protection

After this option is checked, the LAN-to-WAN security defense is enabled by default.
If the network connection is slow, you can disable security defense on the firewall policy configuration page.

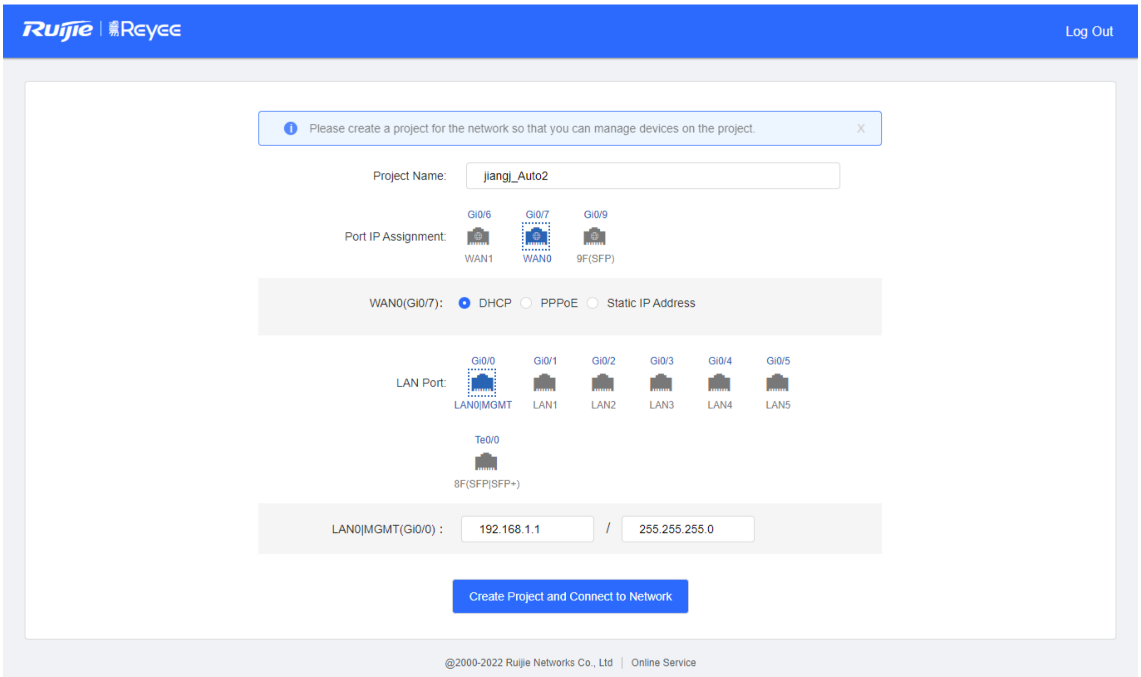


☑ Intrusion Prevention

☑ Virus Protection

After this option is checked, the LAN-to-WAN security defense is enabled by default.
If the network connection is slow, you can disable security defense on the firewall policy configuration page.

(4) Click **NBR Port Config** and configure port information as prompted.



Please create a project for the network so that you can manage devices on the project. X

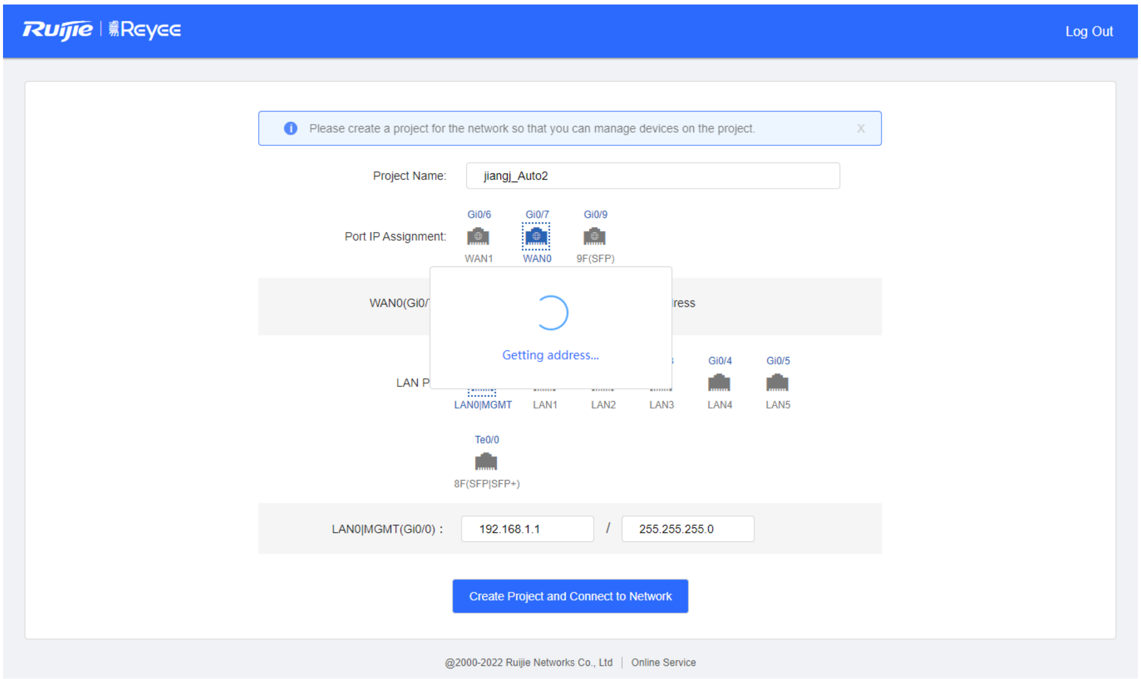
Project Name: jiangj_Auto2

Port IP Assignment:

WAN0(Gi0/7): ● DHCP ○ PPPoE ○ Static IP Address

LAN0|MGMT(Gi0/0) : 192.168.1.1 / 255.255.255.0

(5) Click **Create Project and Connect to Network**. The system delivers configuration information.



Please create a project for the network so that you can manage devices on the project.

Project Name: jiangj_Auto2

Port IP Assignment:

WAN0(Gi0/ ... ress

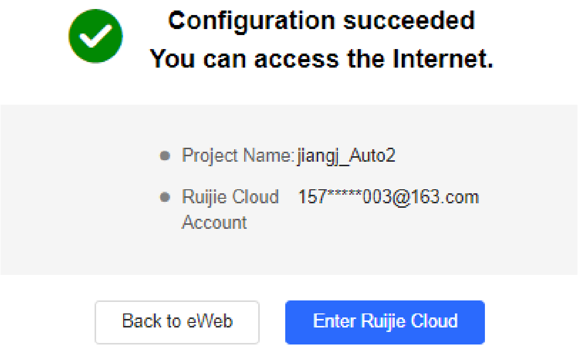
Getting address...

LAN P

LAN0|MGMT(Gi0/0) : 192.168.1.1 / 255.255.255.0

Create Project and Connect to Network

(6) Check the system prompt. A prompt indicating successful configuration is displayed after the configurations are completed.



Configuration succeeded
You can access the Internet.

- Project Name: jiangj_Auto2
- Ruijie Cloud Account 157*****003@163.com

Back to eWeb | Enter Ruijie Cloud

Note

If you change the IP address of the interface, you need to re-enter the new IP address in the address box of the browser for access to the web management system.

4 Home

4.1 Dashboard

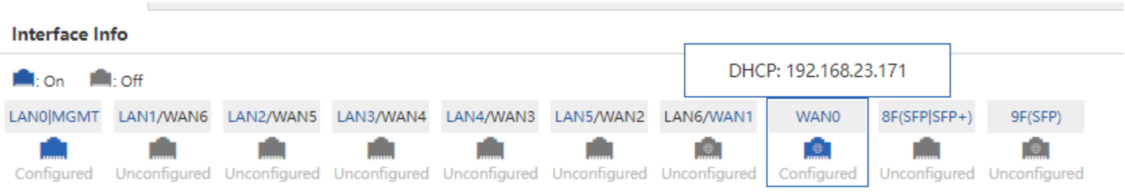
The **Dashboard** page is automatically displayed upon login to the web management page or after you choose

in the menu area.

It is easy for you to view the device CPU, memory, and hard disk usage, number of online users, system version, current system time, and other information on this page. By analyzing the traffic trend, and bandwidth usage of the top 10 applications by traffic, top 10 applications by traffic, top 10 users by traffic, and top 10 users by number of sessions of the current day, you can view the current status of intranet traffic in an all-round way, and troubleshoot common network problems on this page and solve them quickly.

4.1.1 Interface Info

On the top of the **Dashboard** page, interface information is displayed. Click an interface. The basic information about the interface, including the interface type and IP address, is displayed.



Interface Info

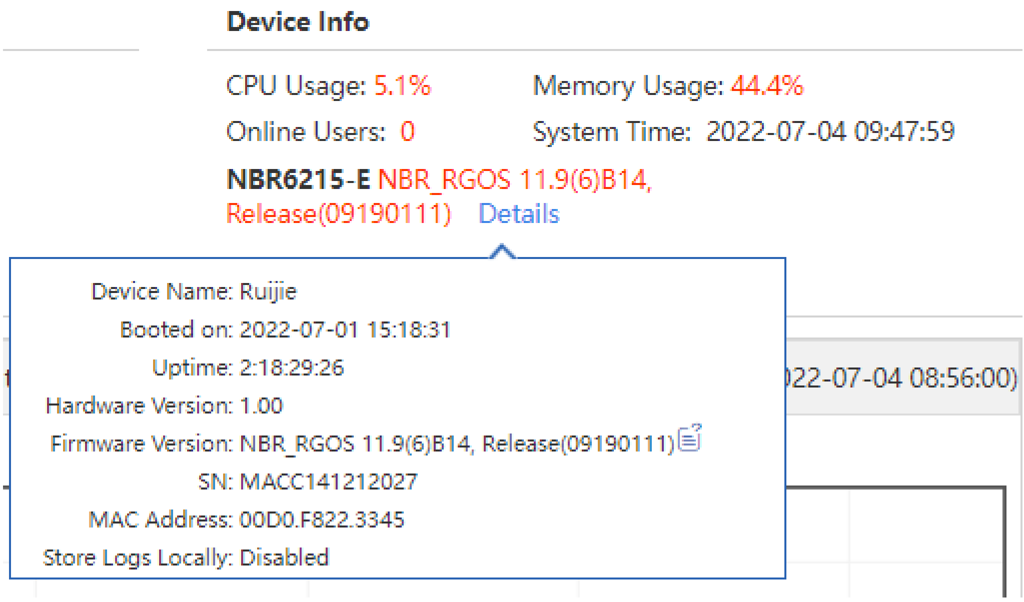
●: On ●: Off

DHCP: 192.168.23.171

LAN0|MGMT	LAN1/WAN6	LAN2/WAN5	LAN3/WAN4	LAN4/WAN3	LAN5/WAN2	LAN6/WAN1	WAN0	8F(SFP|SFP+)	9F(SFP)
Configured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Configured	Unconfigured	Unconfigured

4.1.2 Device Info

On the top of the **Dashboard** page, the current device memory/CPU usage, number of online users, system version, system time, and other information are displayed.



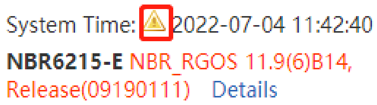
Device Info

CPU Usage: 5.1% Memory Usage: 44.4%

Online Users: 0 System Time: 2022-07-04 09:47:59

NBR6215-E NBR_RGOS 11.9(6)B14, Release(09190111) Details

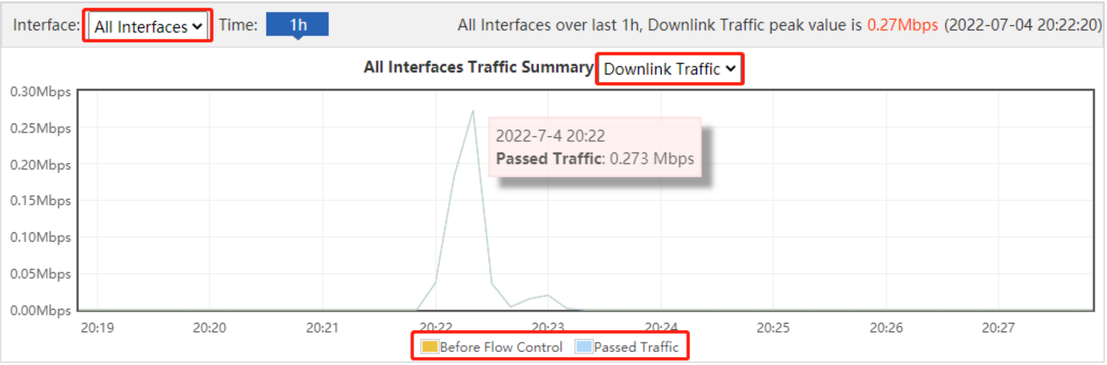
Device Name: Ruijie
Booted on: 2022-07-01 15:18:31
Uptime: 2:18:29:26
Hardware Version: 1.00
Firmware Version: NBR_RGOS 11.9(6)B14, Release(09190111)
SN: MACC141212027
MAC Address: 00D0.F822.3345
Store Logs Locally: Disabled

Parameter	Description
CPU Usage	CPU usage of the current device, where it is easy for you to find out the operation status of the device.
Memory Usage	Memory usage of the current device, where it is convenient for you to find out the device memory usage.
Online Users	Total number of online users of the current device.
System Time	Current system time. ● If the current system time is incorrect or time resetting is required, you can choose **Advanced**>**System**>**System Time** for resetting. ● When the difference between the device time and the management PC time is 1 hour, an alarm icon is displayed next to **System Time**. You can click this icon to access the system time configuration page.  System Time: ⚠2022-07-04 11:42:40 **NBR6215-E** NBR_RGOS 11.9(6)B14, Release(09190111) Details
Details	Click it to view the system startup time, running time, hardware version, software version, and other information.

4.1.3 Bandwidth Status

The system bandwidth status is displayed on the **Dashboard** page, where it is easy for you to view the current device's traffic trend graph for the last hour, and bandwidth usage of the top 10 applications by traffic, top 10 applications by traffic, top 10 users by traffic, and top 10 users by number of sessions of the current day.

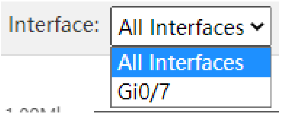
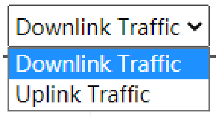
- Traffic trend graph for the last hour



Interface: All Interfaces Time: 1h All Interfaces over last 1h, Downlink Traffic peak value is 0.27Mbps (2022-07-04 20:22:20)

All Interfaces Traffic Summary Downlink Traffic

2022-7-4 20:22
Passed Traffic: 0.273 Mbps

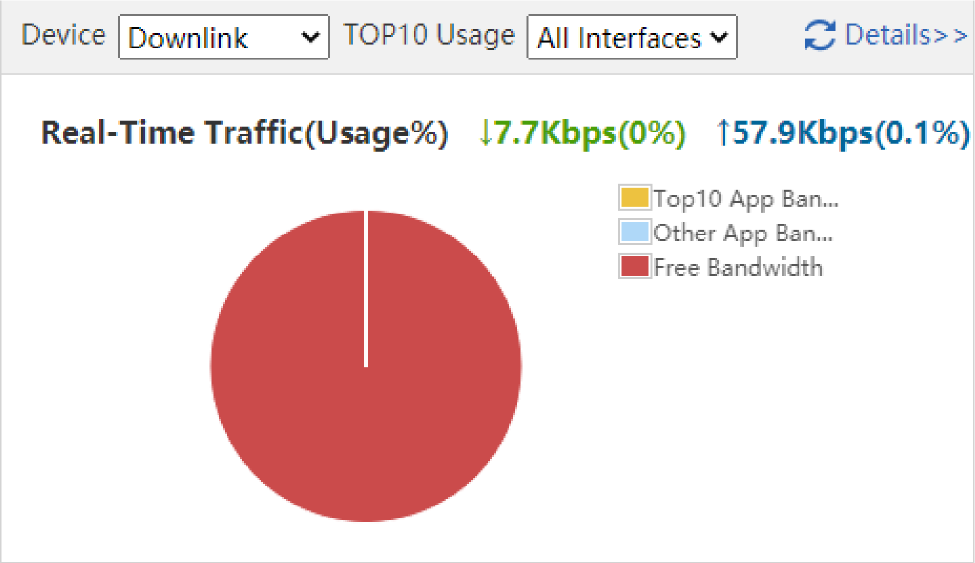
  - In the traffic trend graph, the yellow curve indicates the trend of "traffic before flow control/suppression" and the blue curve indicates the trend of the actual passed traffic after flow control/suppression.
  - You can set  and  to view the upstream/downstream traffic trend of all interfaces.

  - Mouse over a point on the traffic trend curve to view "traffic before flow control/suppression" and "passed traffic".

- You can click 🟨Before Flow Control to hide the curve for the trend of "traffic before flow control/suppression" and click 🟦Passed Traffic to hide that for the trend of "passed traffic".

- Bandwidth usage of the top 10 applications by traffic

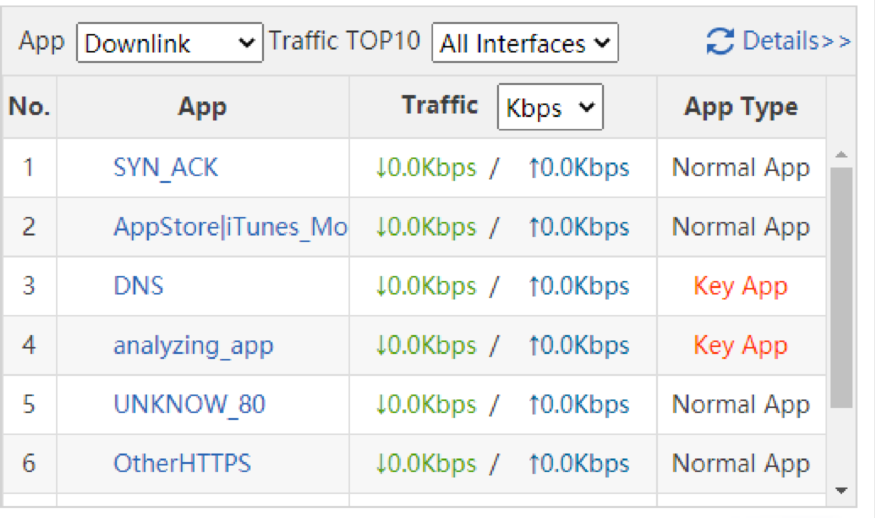
  The ratio of the top 10 applications by real-time traffic to the total bandwidth is shown in a graph.



Device Downlink TOP10 Usage All Interfaces Details>>

Real-Time Traffic(Usage%) ↓7.7Kbps(0%) ↑57.9Kbps(0.1%)

- Top 10 applications by traffic of the current day

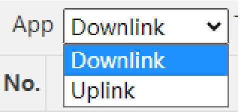


App Downlink Traffic TOP10 All Interfaces Details>>

No.	App	Traffic Kbps	App Type
1	SYN_ACK	↓0.0Kbps / ↑0.0Kbps	Normal App
2	AppStore|iTunes_Mo	↓0.0Kbps / ↑0.0Kbps	Normal App
3	DNS	↓0.0Kbps / ↑0.0Kbps	Key App
4	analyzing_app	↓0.0Kbps / ↑0.0Kbps	Key App
5	UNKNOW_80	↓0.0Kbps / ↑0.0Kbps	Normal App
6	OtherHTTPS	↓0.0Kbps / ↑0.0Kbps	Normal App

- The top 10 applications by traffic are displayed in the table. You can click Details to view the application traffic details.

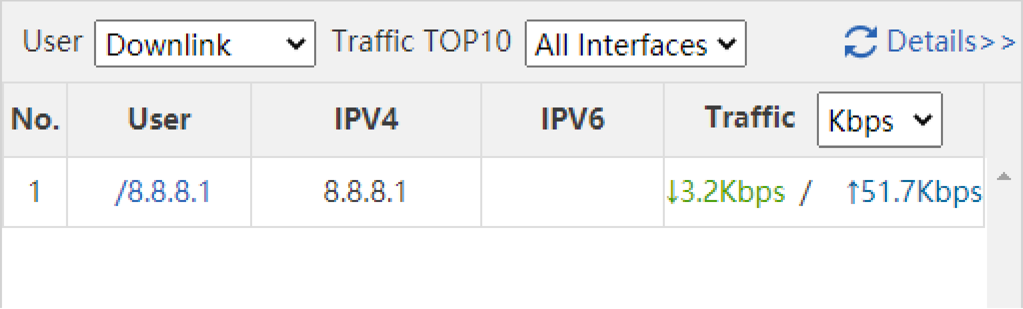
- You can set App Downlink to view the top 10 applications by upstream/downstream traffic for the last 10 minutes.



- You can set All Interfaces to view the top 10 applications by traffic of specified interfaces.

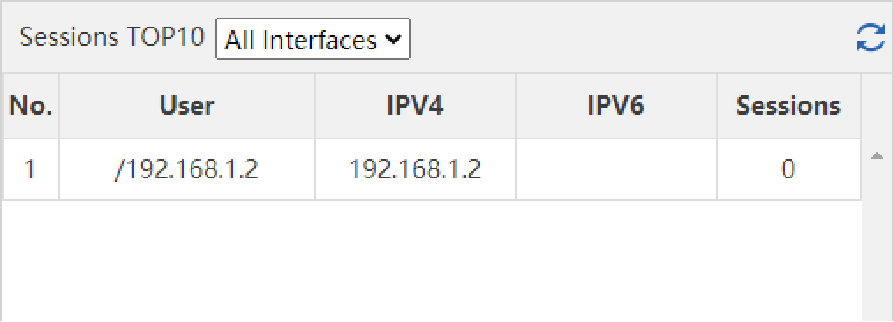
- Top 10 users by traffic

The table shows the top 10 users by traffic.



No.	User	IPV4	IPV6	Traffic Kbps
1	/8.8.8.1	8.8.8.1		↓3.2Kbps / ↑51.7Kbps

- Top 10 users by number of sessions of the current day



No.	User	IPV4	IPV6	Sessions
1	/192.168.1.2	192.168.1.2		0

  - The top 10 users by number of sessions are displayed in the table shown in the preceding figure.
  - You can set All Interfaces to view the top 10 applications by number of sessions of specified interfaces.

4.2 Service

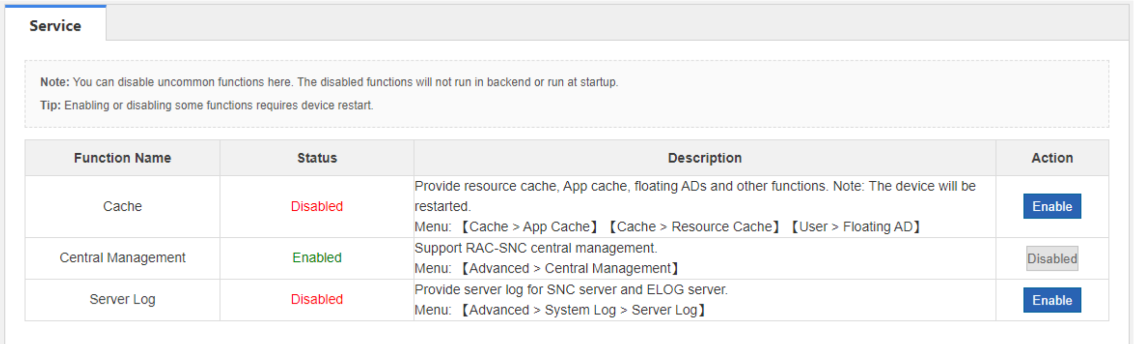
Application Scenario

You can disable the functions that are not used frequently on this page.

A disabled function will not run in the background or be automatically started upon system startup. The corresponding web page will not be displayed.

Procedure

(1) Choose **Home**>**Service**.



Note: You can disable uncommon functions here. The disabled functions will not run in backend or run at startup.

Tip: Enabling or disabling some functions requires device restart.

Function Name	Status	Description	Action
Cache	Disabled	Provide resource cache, App cache, floating ADs and other functions. Note: The device will be restarted. Menu: 【Cache > App Cache】【Cache > Resource Cache】【User > Floating AD】	Enable
Central Management	Enabled	Support RAC-SNC central management. Menu: 【Advanced > Central Management】	Disabled
Server Log	Disabled	Provide server log for SNC server and ELOG server. Menu: 【Advanced > System Log > Server Log】	Enable

(2) Click **Disable** in the **Action** column corresponding to the function to be disabled.

(3) In the window where a prompt is displayed, click **OK**.

Follow-up Procedure

Click **Enable** to re-enable the corresponding function.

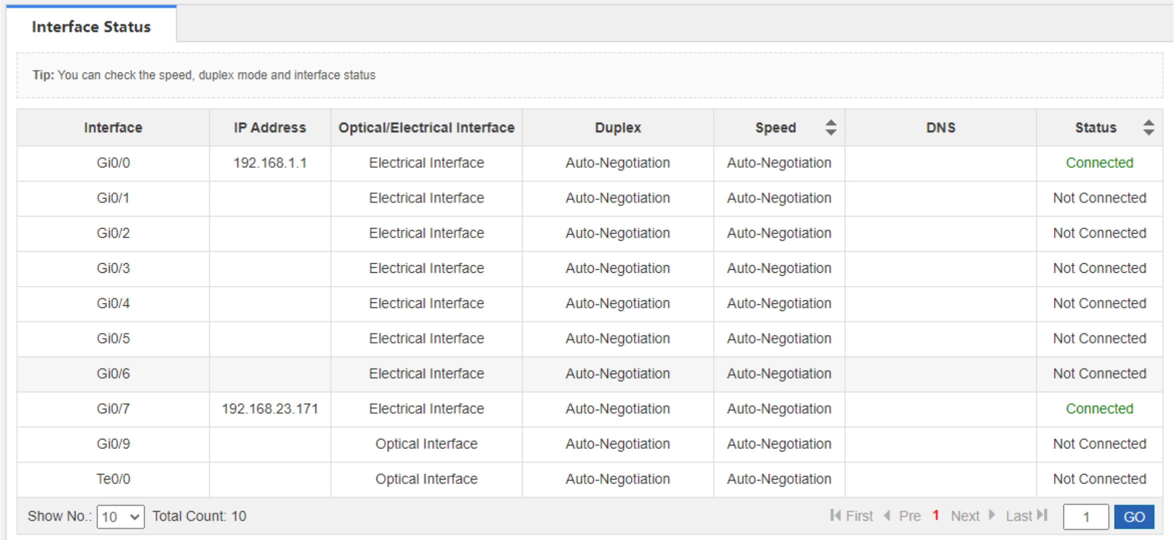
4.3 Interface Status

Procedure

Choose **Home**>**Interface Status** to view the status information about each interface, including the IP address, rate, DNS, and connection status.

Note

If an interface does not support IPv6, its IPv6-related information is not displayed.



Tip: You can check the speed, duplex mode and interface status

Interface	IP Address	Optical/Electrical Interface	Duplex	Speed	DNS	Status
Gi0/0	192.168.1.1	Electrical Interface	Auto-Negotiation	Auto-Negotiation		Connected
Gi0/1		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/2		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/3		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/4		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/5		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/6		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/7	192.168.23.171	Electrical Interface	Auto-Negotiation	Auto-Negotiation		Connected
Gi0/9		Optical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Te0/0		Optical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected

Show No.: 10 Total Count: 10

5 Behavior Management

5.1 Traffic Monitoring

5.1.1 Introduction

The **Traffic Monitoring** module is used to view the current network traffic usage and perform intelligent analysis on specific applications.

5.1.2 Real-Time Traffic

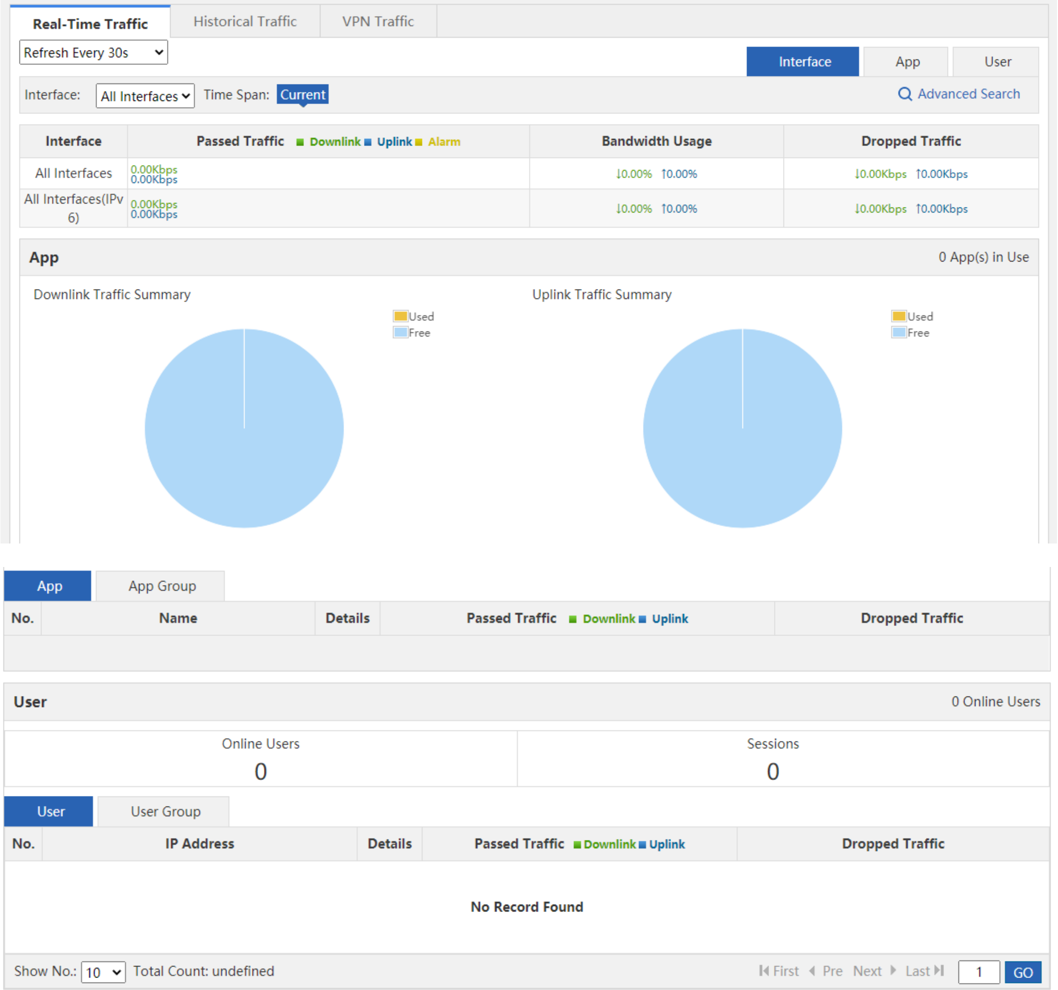
1. Overview

Application Scenario

You can perform this operation to view the real-time monitoring data.

Procedure

(1) Choose Flow > Traffic Monitoring > Real-Time Traffic.



Real-Time Traffic | Historical Traffic | VPN Traffic

Refresh Every 30s

Interface | App | User

Interface: All Interfaces Time Span: Current

Advanced Search

Interface	Passed Traffic ■ Downlink ■ Uplink ■ Alarm	Bandwidth Usage	Dropped Traffic
All Interfaces	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps
All Interfaces(IPv6)	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps

App 0 App(s) in Use

App | App Group

No.	Name	Details	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic

User 0 Online Users

Online Users	Sessions
0	0

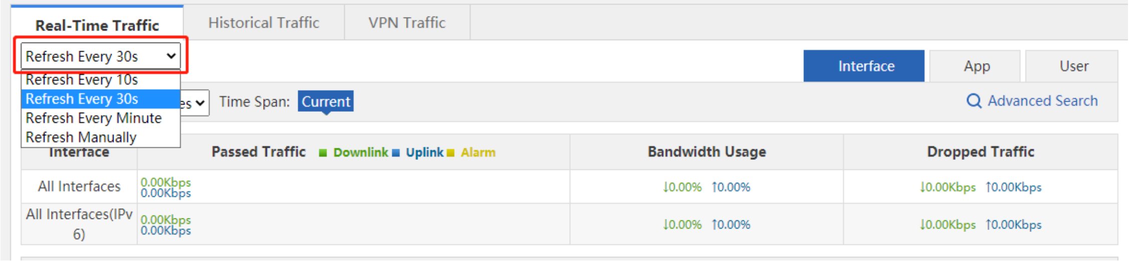
User | User Group

No.	IP Address	Details	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic
		No Record Found		

Show No.: 10 Total Count: undefined First Pre Next Last 1 GO

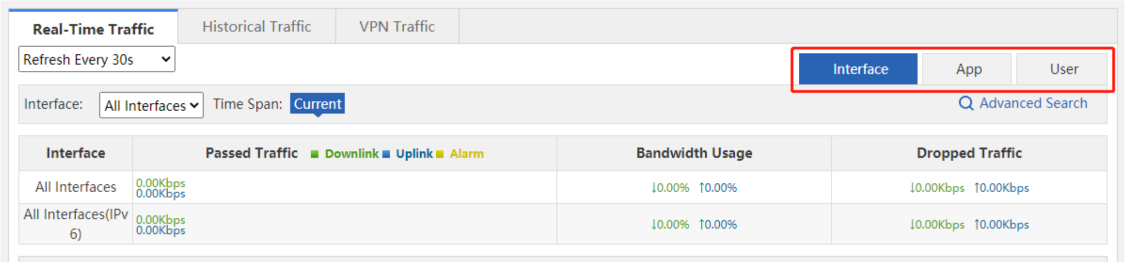
(2) Select a data refreshing frequency.

You can select to refresh the current device traffic information once every 10s, 30s, or every minute, or manually refresh the information.



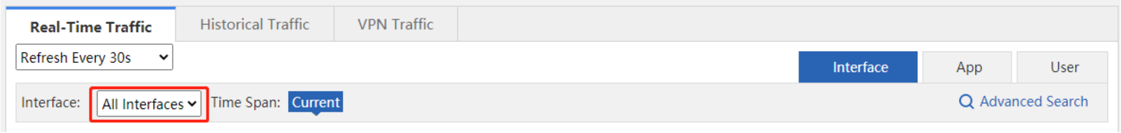
Interface	Passed Traffic ■ Downlink ■ Uplink ■ Alarm	Bandwidth Usage	Dropped Traffic
All Interfaces	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps
All Interfaces(IPv6)	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps

(3) You can switch among tabs Interface App User to view device traffic statistics by interface, application, or user.



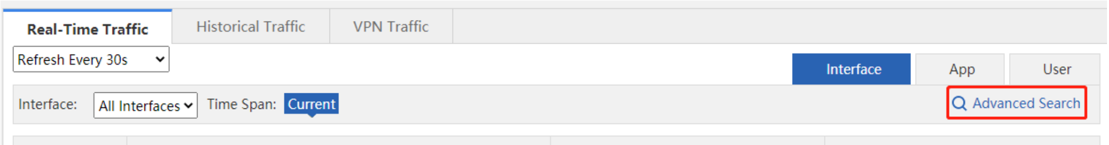
Interface	Passed Traffic ■ Downlink ■ Uplink ■ Alarm	Bandwidth Usage	Dropped Traffic
All Interfaces	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps
All Interfaces(IPv6)	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps

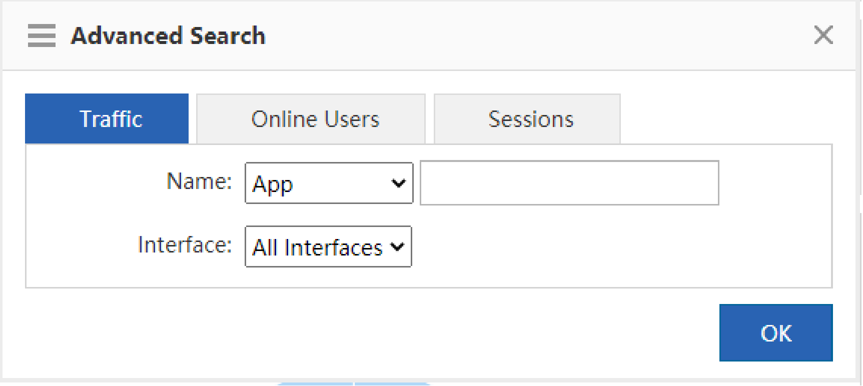
(4) You can select an interface from the drop-down list All Interfaces to view the traffic information of a specific interface, or select **All Interfaces** to view the total traffic of all interfaces.



(5) **Time Span** indicates the statistical time period of the displayed traffic information. Current means that the current traffic information is displayed.

(6) Click Advanced Search to access the **Advanced Search** window, in which you can view the traffic, number of online users, and number of sessions.



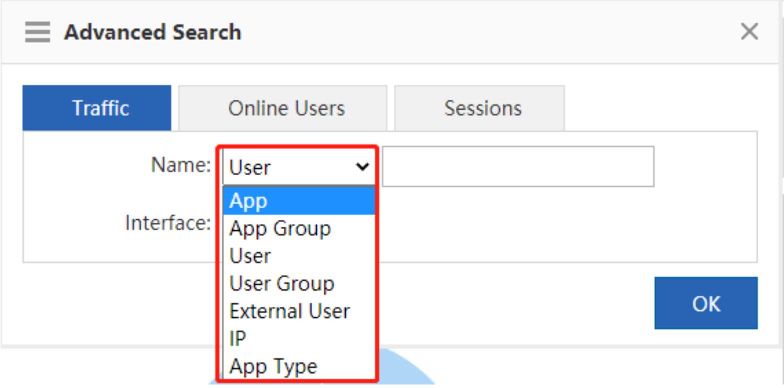


Name: App

Interface: All Interfaces

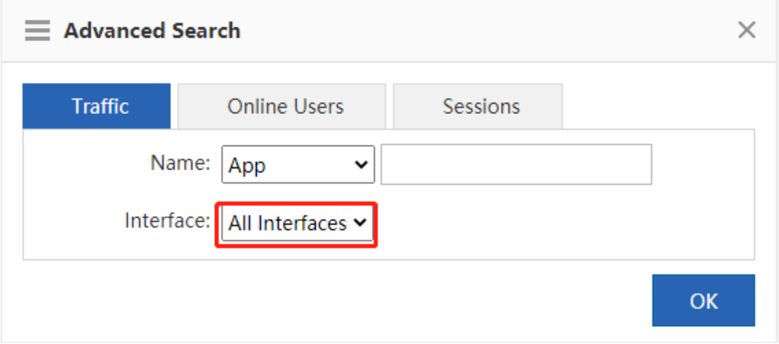
- View traffic details: You can view the current traffic or the traffic within a time span of an interface by user, IP address, or application.

a Select **Traffic**, and then select a query filter from the drop-down list of **Name**. Then, in the text box on the right, select the app scope or user scope you want to query from the displayed app tree or user tree.



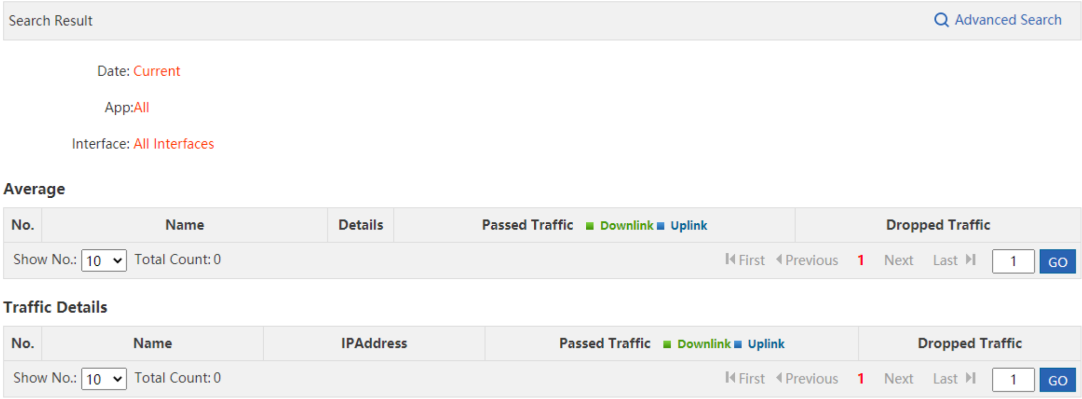
Name: User

b Select an option from the drop-down list of **Interface** and click OK. The query results are displayed.



Name: App

Interface: All Interfaces



Search Result Advanced Search

Date: Current

App:All

Interface: All Interfaces

Average

No.	Name	Details	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

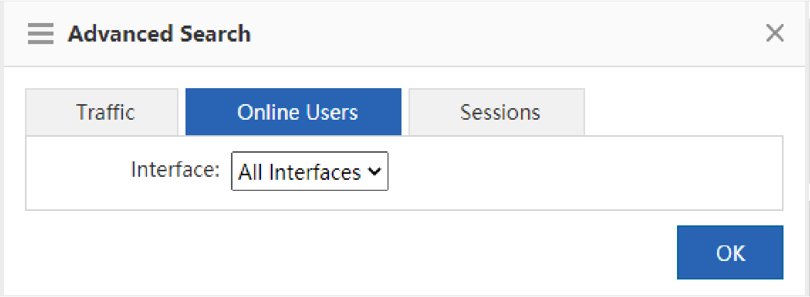
Traffic Details

No.	Name	IPAddress	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

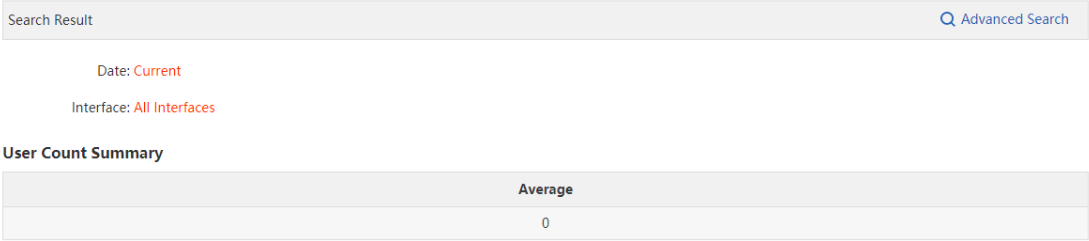
- View details of online users: You can view the number of currently online users or online users within a time span of an interface.

a Select **Online Users** and then select the interface you want to query.



Interface: All Interfaces

c Click OK. The following query results are displayed.



Search Result Advanced Search

Date: Current

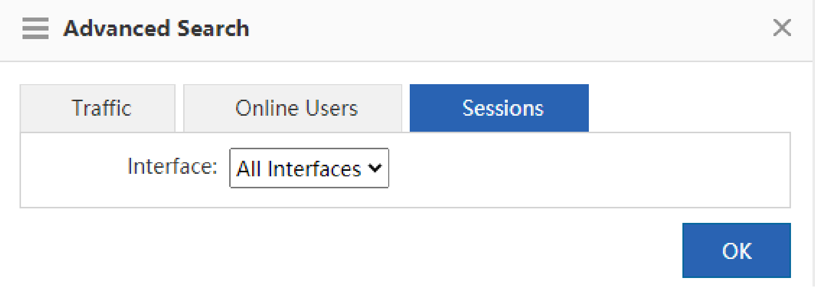
Interface: All Interfaces

User Count Summary

Average
0

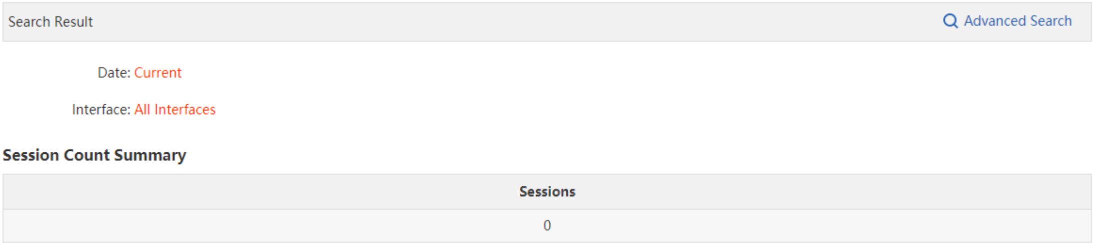
- View details of sessions: You can view the number of current sessions or sessions within a time span of an interface.

a Select **Sessions** and then select the interface you want to query.



Interface: All Interfaces

d Click OK. The following query results are displayed.



Search Result

Date: Current

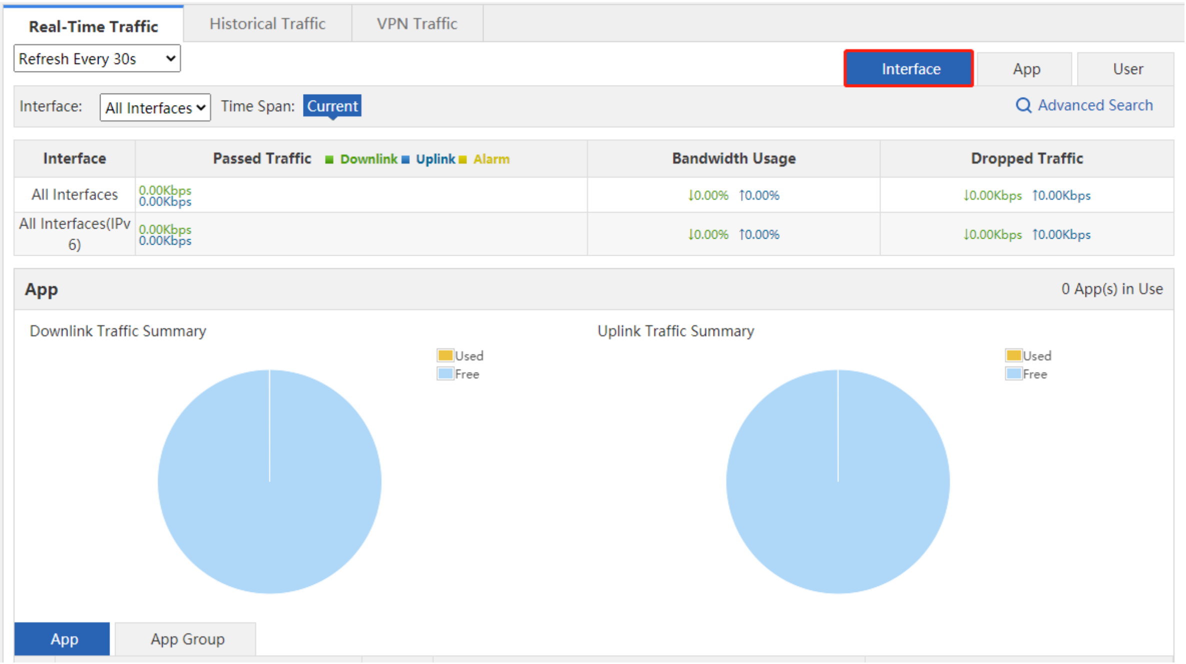
Interface: All Interfaces

Session Count Summary

Sessions
0

2. Interface Traffic Analysis

This function allows you to make statistics on, control, and analyze bandwidth usage by interface to improve the traffic usage values. Click Interface on the Real-Time Traffic tab page. The following information is displayed:



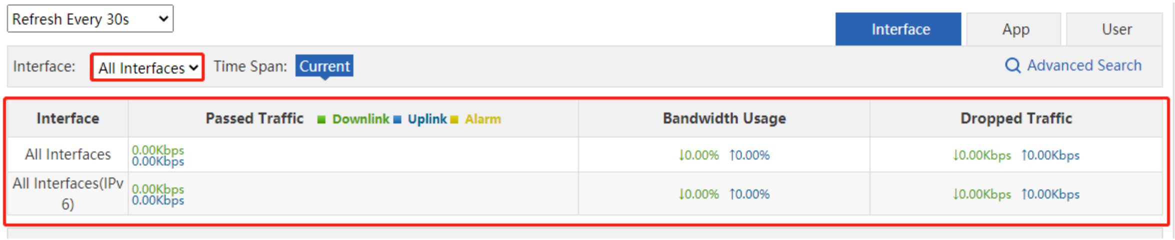
Interface: All Interfaces Time Span: Current

Interface	Passed Traffic ■ Downlink ■ Uplink ■ Alarm	Bandwidth Usage	Dropped Traffic
All Interfaces	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps
All Interfaces(IPv6)	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps

App 0 App(s) in Use

Interface Traffic Information Overview

The first part of the page displays the traffic information of a specified interface. When **All Interfaces** is selected, the total traffic of all interface and the traffic of each interface are displayed.



Interface: All Interfaces Time Span: Current

Interface	Passed Traffic ■ Downlink ■ Uplink ■ Alarm	Bandwidth Usage	Dropped Traffic
All Interfaces	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps
All Interfaces(IPv6)	0.00Kbps 0.00Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps

According to the traffic information displayed in the figure above, you can check whether the current traffic is normal (whether any alarm occurs). If the traffic is too high, a yellow alarm 🟨 Alarm occurs, which helps you quickly locate the bandwidth problem.

Note

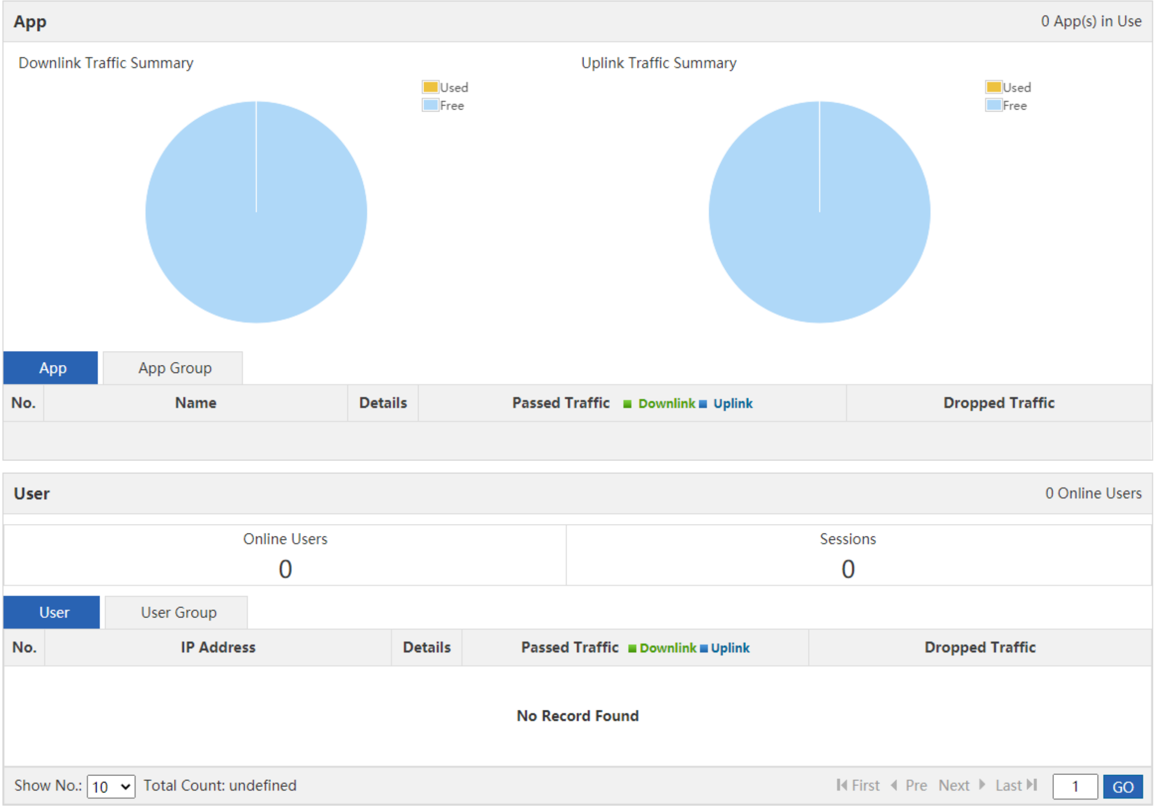
Condition for triggering the yellow alarm: When the total traffic is over 95% of the interface bandwidth (the bandwidth that a user purchases from China Telecom or other carriers).

Solution for the yellow alarm:

- When a yellow alarm occurs and the traffic of the **Key App** group is equivalent to the total traffic, choose **Flow** > **Flow Control Policy** or choose **Flow** > **Object** > **Custom App** to check whether all the selected applications are those whose traffic you want to guarantee. If yes, the current bandwidth is insufficient. In this case, you want to apply for more bandwidth from your carrier to ensure sufficient bandwidth.
- When a yellow alarm occurs and the bandwidth used by the Rate-Limited App group is large, reduce the traffic used by the Rate-Limited App group.
- When an alarm occurs and the traffic of the Normal App group is equivalent to that of the Rate-Limited App group, reduce the traffic used by the Rate-Limited App group and the Normal App group in turn.

Application Traffic Information of an Interface

The middle part of the page displays the application traffic information of a specified interface, including the ratio of bandwidth occupied by different types of applications (key/guaranteed applications, normal/other applications, and rate-limited applications), the total number of applications that are using the traffic, the specific applications, and the traffic usage of each application, and the traffic dropped by the rate limiting policy.



App

0 App(s) in Use

No.	Name	Details	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic

User

0 Online Users

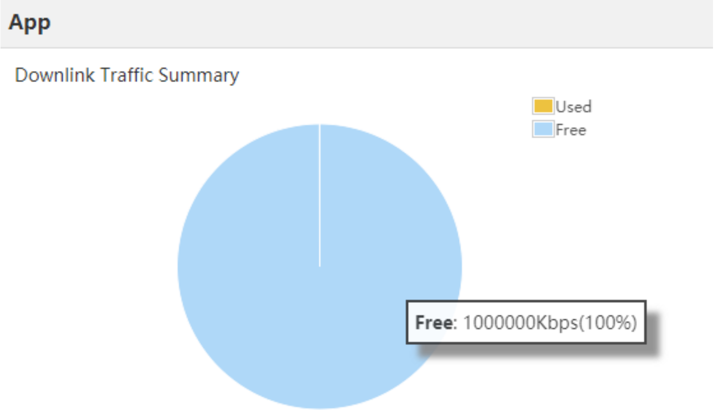
Online Users: 0

Sessions: 0

No.	IP Address	Details	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic
No Record Found				

Show No.: 10 Total Count: undefined

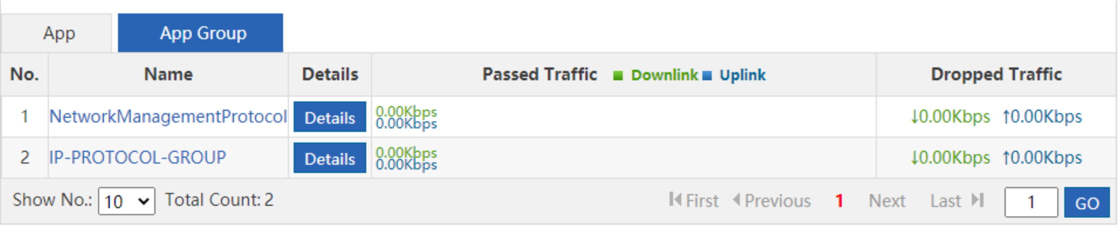
- The two pie charts at the top of this area display the uplink and downlink traffic occupied by different types of applications on the selected interface. You can move the pointer onto the pie charts to view the uplink or downlink traffic not used by applications on the selected interface.



- ○ Key/guaranteed applications: Display the total uplink or downlink traffic used by key/guaranteed applications on the selected interface, and the percentage of used traffic in the total uplink or downlink traffic of the selected interface.
- ○ Normal/other applications: Display the total uplink or downlink traffic used by normal/other applications on the selected interface, and the percentage of used traffic in the total uplink or downlink traffic of the selected interface.
- ○ Rate-limited applications: Display the total uplink or downlink traffic used by rate-limited applications on the selected interface, and the percentage of used traffic in the total uplink or downlink traffic of the selected interface.
- ○ Not used: Display the uplink or downlink traffic not used by applications on the selected interface, and the percentage of not used traffic in the total uplink or downlink traffic of the selected interface.

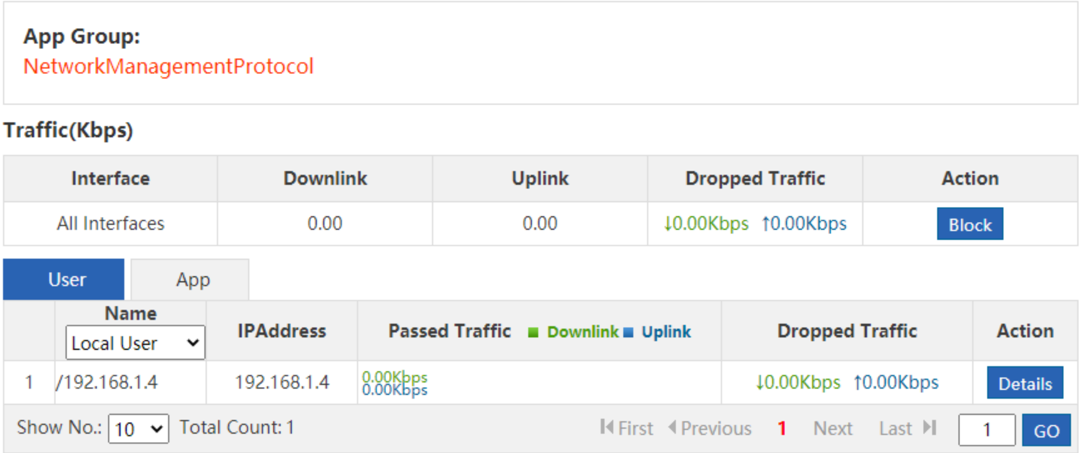
- Tables in the lower part of this area display the current traffic usage of specific applications on the selected interface, including the uplink/downlink traffic occupied by each application and the traffic dropped by the rate limiting policy.

In the navigation menu in the upper-left corner of the tables, select App Group, and the system displays the traffic of the current application group on the selected interface.



No.	Name	Details	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic
1	NetworkManagementProtocol	Details	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps
2	IP-PROTOCOL-GROUP	Details	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps

Click Details and the following window is displayed:



App Group:
NetworkManagementProtocol

Traffic(Kbps)

Interface	Downlink	Uplink	Dropped Traffic	Action
All Interfaces	0.00	0.00	↓0.00Kbps ↑0.00Kbps	Block

User | App

	Name Local User	IPAddress	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic	Action
1	/192.168.1.4	192.168.1.4	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps	Details

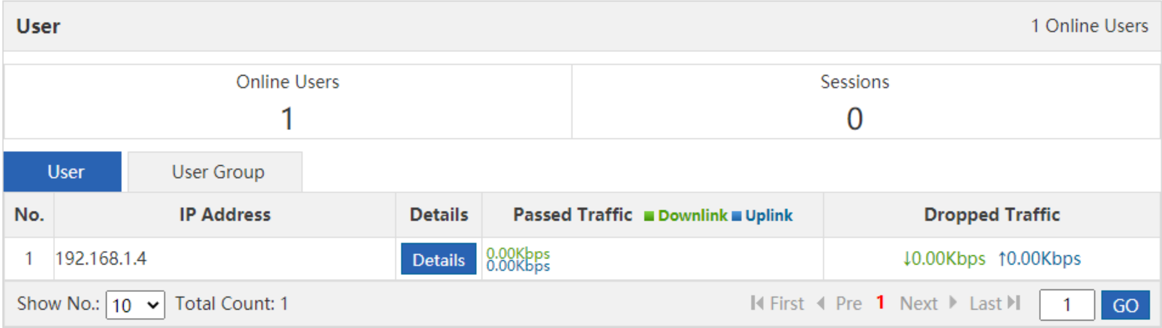
Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

This window displays the application group and type of the selected application, the uplink/downlink traffic occupied by the selected interface, the traffic dropped by the rate limiting policy, and the traffic of the user that runs this application.

You can click Block to block the traffic of the current application. After blocking, the subsequent traffic of this application is completely dropped by the selected interface.

User Traffic Information of an Interface

The lower part of the page displays the traffic usage of users on the current interface, including the number of online users and sessions on the selected interface, and the traffic of users using this interface.



User 1 Online Users

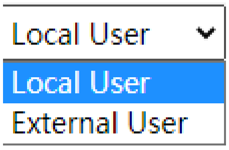
Online Users	Sessions
1	0

User | User Group

No.	IP Address	Details	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic
1	192.168.1.4	Details	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 GO

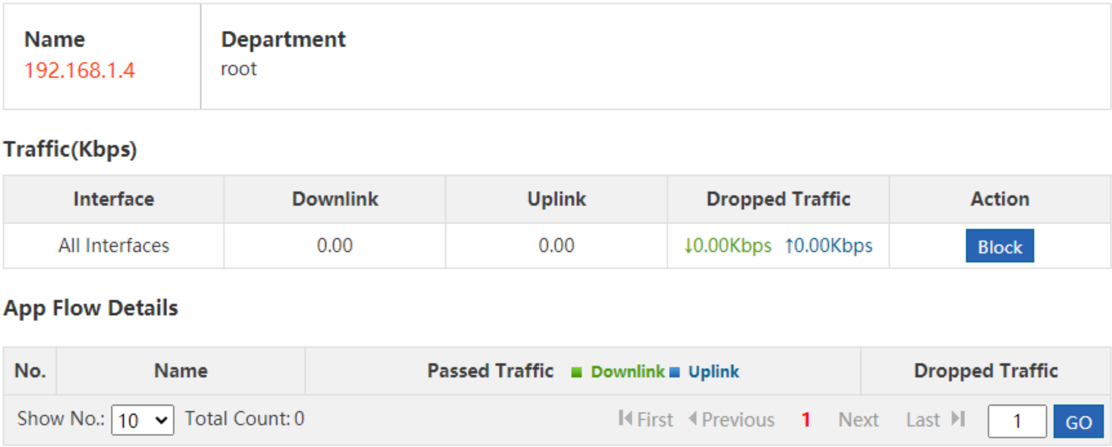
You can choose to view the traffic of a local user or an external user through the drop-down list



Local User
Local User
External User

.

Click Details . The following window appears, which displays the traffic usage of the selected user on the selected interface, details of applications run by the selected user, and the traffic usage of each application.



Name	Department
192.168.1.4	root

Traffic(Kbps)

Interface	Downlink	Uplink	Dropped Traffic	Action
All Interfaces	0.00	0.00	↓0.00Kbps ↑0.00Kbps	Block

App Flow Details

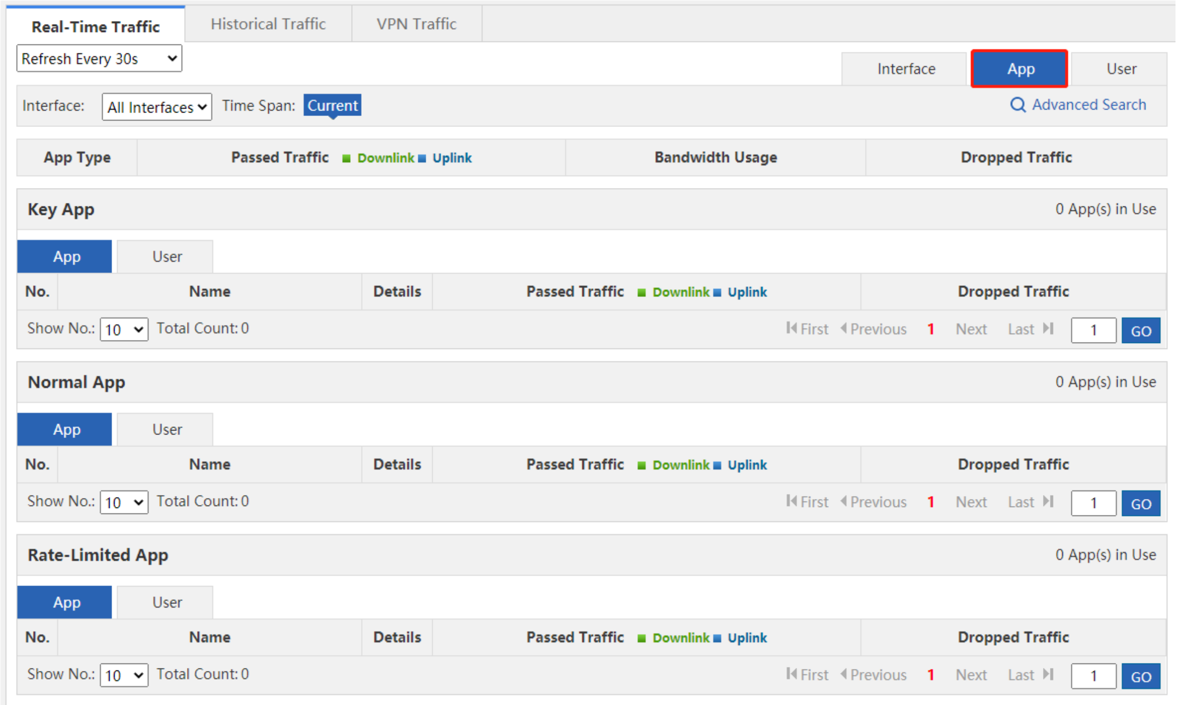
No.	Name	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

You can click Block to block the traffic of the current user. After blocking, the subsequent traffic of this user is completely dropped by the selected interface.

3. Application Traffic Analysis

This function allows you to make statistics on the bandwidth usage of different applications to control and analyze application traffic, so as to improve the traffic usage values. Click App on the Real-Time Traffic tab page. The following information is displayed:



Real-Time Traffic | Historical Traffic | VPN Traffic

Refresh Every 30s

Interface | App | User

Interface: All Interfaces Time Span: Current

Advanced Search

App Type	Passed Traffic 🟩 Downlink 🟦 Uplink	Bandwidth Usage	Dropped Traffic

Key App 0 App(s) in Use

App | User

No.	Name	Details	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

Normal App 0 App(s) in Use

App | User

No.	Name	Details	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

Rate-Limited App 0 App(s) in Use

App | User

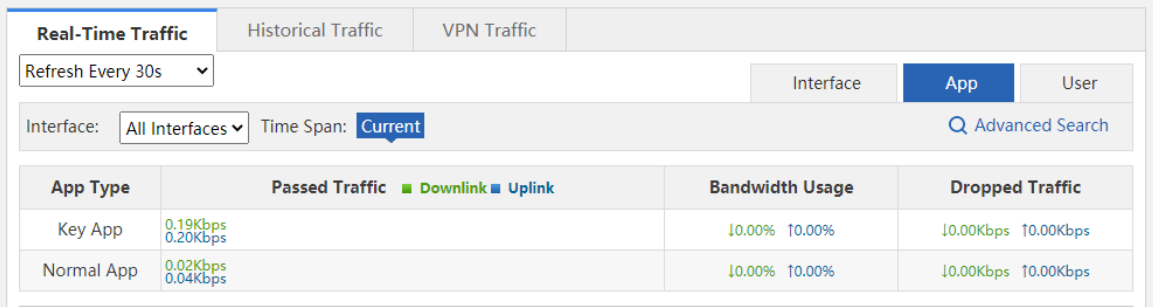
No.	Name	Details	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

The page displays the system application traffic usage overview, and the traffic usage of key/guaranteed applications, normal/other applications, and rate-limited applications.

- Application traffic usage overview

This part displays the used traffic and bandwidth usage of key/guaranteed applications, normal/other applications, and rate-limited applications on the selected interface, and the traffic dropped by the rate limiting policy.

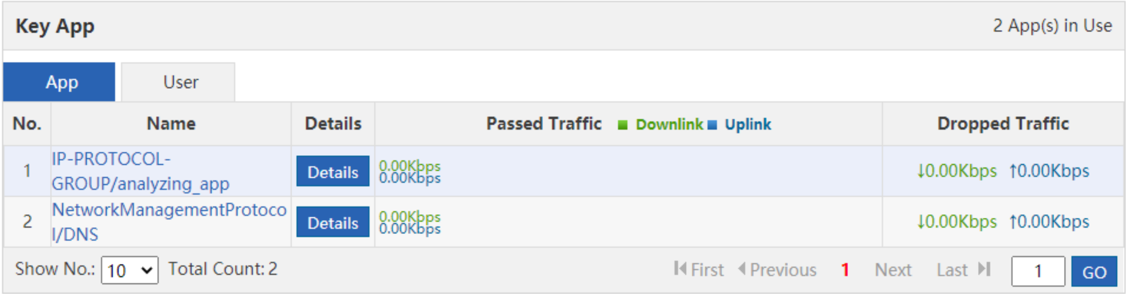


Refresh Every 30s

Interface: All Interfaces Time Span: Current

App Type	Passed Traffic 🟩 Downlink 🟦 Uplink	Bandwidth Usage	Dropped Traffic
Key App	0.19Kbps 0.20Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps
Normal App	0.02Kbps 0.04Kbps	↓0.00% ↑0.00%	↓0.00Kbps ↑0.00Kbps

- Traffic analysis of key/guaranteed applications: Display the details of key/guaranteed applications on the selected interface, the traffic usage of each application, details of users running the key/guaranteed applications, and the traffic usage of each user.

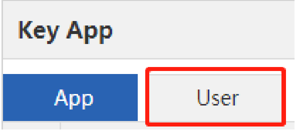


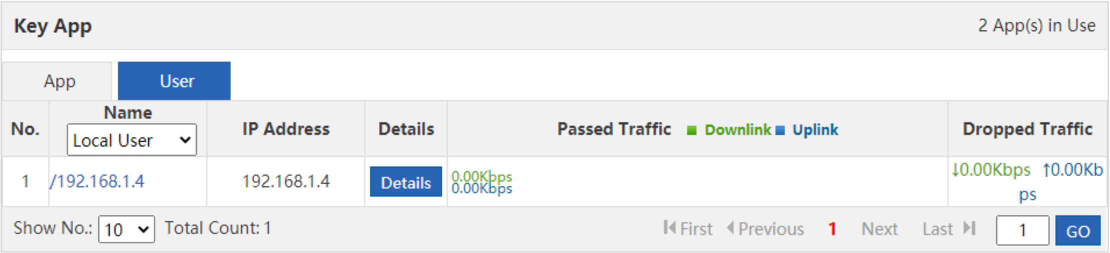
No.	Name	Details	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic
1	IP-PROTOCOL-GROUP/analyzing_app	Details	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps
2	NetworkManagementProtocol/DNS	Details	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps

Show No.: 10 Total Count: 2

Click Details, and the application traffic details window is displayed. For details, see the application traffic details window description in the section Interface Traffic Analysis.

The above figure displays the traffic usage of key/guaranteed applications. You can click User in to display the traffic usage of users running the key/guaranteed applications on the current interface:



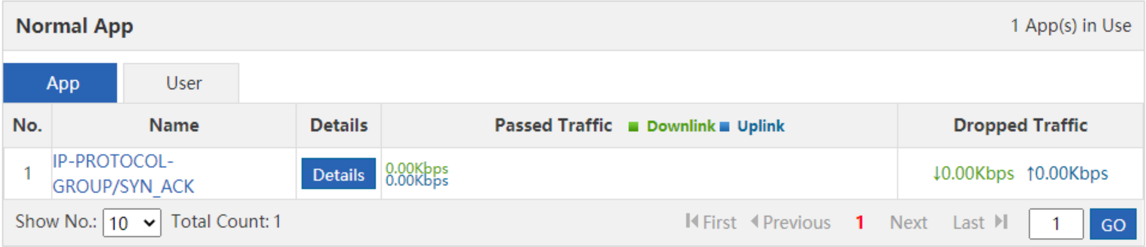


No.	Name Local User	IP Address	Details	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic
1	/192.168.1.4	192.168.1.4	Details	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps

Show No.: 10 Total Count: 1

Click Details, and the user traffic details window is displayed. For details, see the user traffic details window description in the section Interface Traffic Analysis.

- Traffic analysis of normal/other applications: Display the details of normal/other applications on the selected interface, the traffic usage of each application, details of users running the normal/other applications, and the traffic usage of each user.



Normal App 1 App(s) in Use

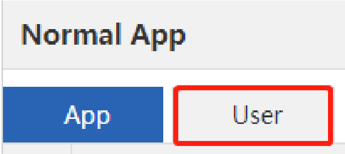
App | User

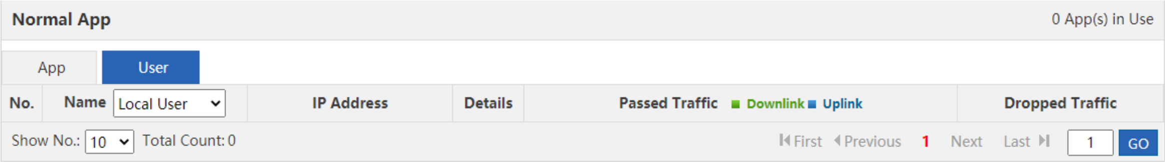
No.	Name	Details	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic
1	IP-PROTOCOL-GROUP/SYN_ACK	Details	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

Click Details, and the application traffic details window is displayed. For details, see the application traffic details window description in the section Interface Traffic Analysis.

The above figure displays the traffic usage of normal/other applications. You can click User in to display the traffic usage of users running the normal/other applications on the current interface:





Normal App 0 App(s) in Use

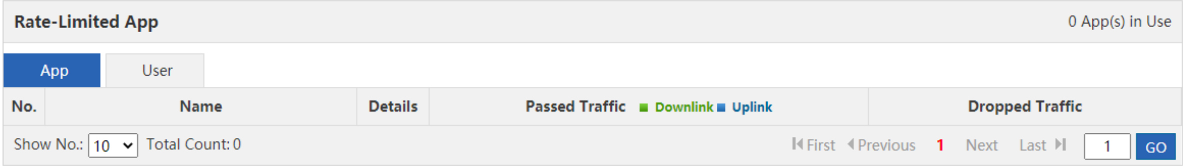
App | User

No.	Name Local User	IP Address	Details	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

Click Details, and the user traffic details window is displayed. For details, see the user traffic details window description in the section Interface Traffic Analysis.

- Traffic analysis of rate-limited applications: Display the details of rate-limited applications on the selected interface, the traffic usage of each application, details of users running the rate-limited applications, and the traffic usage of each user.



Rate-Limited App 0 App(s) in Use

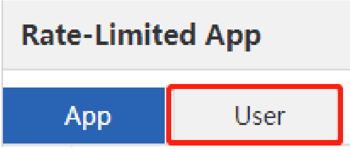
App | User

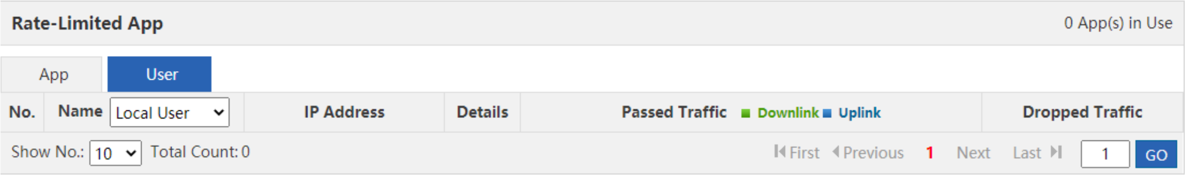
No.	Name	Details	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

Click Details, and the application traffic details window is displayed. For details, see the application traffic details window description in the section Interface Traffic Analysis.

The above figure displays the traffic usage of rate-limited applications. You can click User in to display the traffic usage of users running the rate-limited applications on the current interface:





Rate-Limited App 0 App(s) in Use

App User

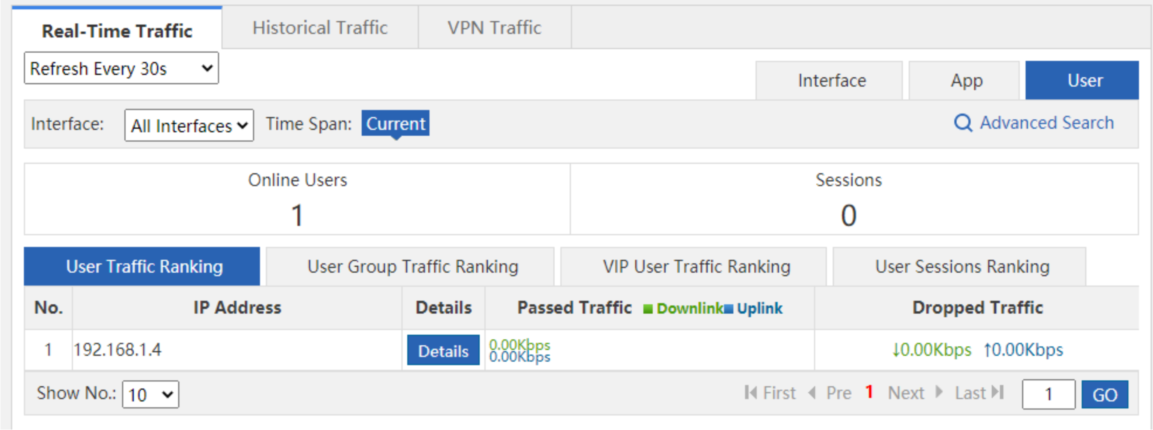
No.	Name Local User	IP Address	Details	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

Click Details, and the user traffic details window is displayed. For details, see the user traffic details window description in the section Interface Traffic Analysis.

4. User Traffic Analysis

This function allows you to analyze users' traffic usage by interface and monitor users' current traffic usage and details of applications in real time, so that you can easily adjust the user traffic usage to rapidly limit users with excessive traffic usage. If your network has many users, you can filter users by user name or IP address. Click User on the Real-Time Traffic tab page. The following information is displayed:



Real-Time Traffic Historical Traffic VPN Traffic

Refresh Every 30s Interface App User

Interface: All Interfaces Time Span: Current Advanced Search

Online Users 1

Sessions 0

User Traffic Ranking User Group Traffic Ranking VIP User Traffic Ranking User Sessions Ranking

No.	IP Address	Details	Passed Traffic 🟩 Downlink 🟦 Uplink	Dropped Traffic
1	192.168.1.4	Details	0.00Kbps 0.00Kbps	↓0.00Kbps ↑0.00Kbps

Show No.: 10 First Pre 1 Next Last 1 GO

This page displays the number of online users and sessions on the selected interface, user traffic ranking, user group traffic ranking, VIP user traffic ranking, and user sessions ranking.

Click Details, and the user traffic details window is displayed. For details, see the user traffic details window description in the section Interface Traffic Analysis.

Users are divided into multiple groups by class, department, or floor. NBR can view and manage the traffic based on the user groups.

Note

To configure a user group, choose **User** > **User** > **Common User** > **User Structure**.

5.1.3 Historical Interface Traffic

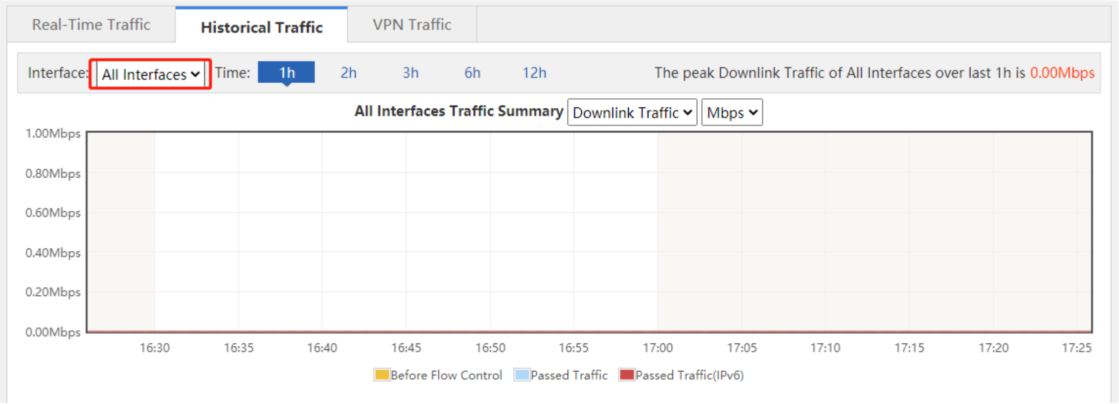
Application Scenario

This function allows you to view the interface traffic in real time and the real-time curve within a unit time. You can view the real-time traffic monitoring curve within a day.

Procedure

(1) Choose **Flow** > **Traffic Monitoring** > **Historical Traffic**.

(2) Select the interface you want to monitor.

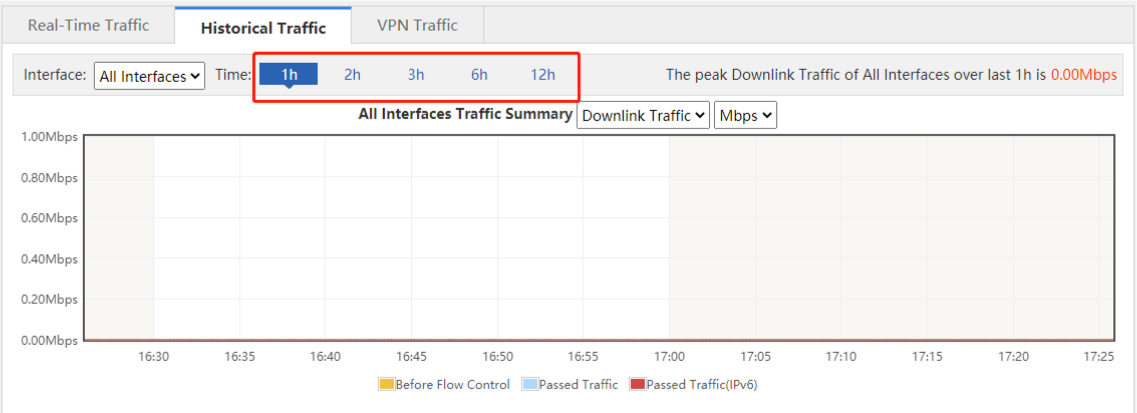


Real-Time Traffic | Historical Traffic | VPN Traffic

Interface: All Interfaces | Time: 1h 2h 3h 6h 12h | The peak Downlink Traffic of All Interfaces over last 1h is 0.00Mbps

All Interfaces Traffic Summary | Downlink Traffic | Mbps

(3) Select the time period you want to monitor.



Real-Time Traffic | Historical Traffic | VPN Traffic

Interface: All Interfaces | Time: 1h 2h 3h 6h 12h | The peak Downlink Traffic of All Interfaces over last 1h is 0.00Mbps

All Interfaces Traffic Summary | Downlink Traffic | Mbps

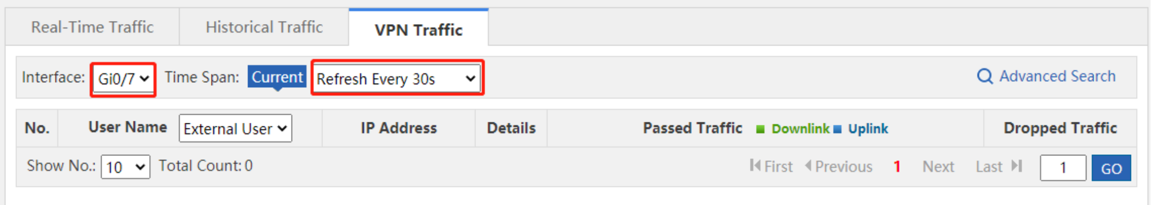
5.1.4 VPN Traffic

Application Scenario

On this tab page, you can view the details of users who access the network through VPN dial-up on an interface and the traffic usage of each VPN user.

Procedure

(1) Choose **Flow** > **Traffic Monitoring** > **VPN Traffic**.



Real-Time Traffic | Historical Traffic | VPN Traffic

Interface: Gi0/7 | Time Span: Current | Refresh Every 30s | Advanced Search

No.	User Name External User	IP Address	Details	Passed Traffic ■ Downlink ■ Uplink	Dropped Traffic

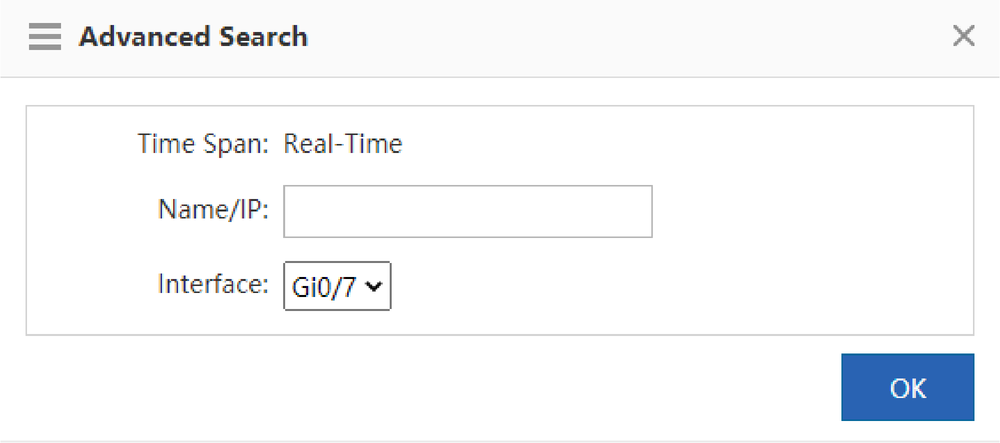
Show No.: 10 | Total Count: 0 | First | Previous | 1 | Next | Last | 1 | GO

(2) Set a query filter.

- Select an interface from Interface: Gi0/7 to view the VPN traffic usage on this interface.
- Select an option from Refresh Every 30s to refresh the current VPN traffic usage of the device

once every 10s, 30s, or every minute, or manually refresh the information.

Click Advanced Search. You can view the traffic usage of a VPN user on an interface. Input the name or IP address, select an interface, and click OK.



Advanced Search

Time Span: Real-Time

Name/IP:

Interface: Gi0/7

5.2 Flow Control Policy

5.2.1 Smart Flow Control

Application Scenario

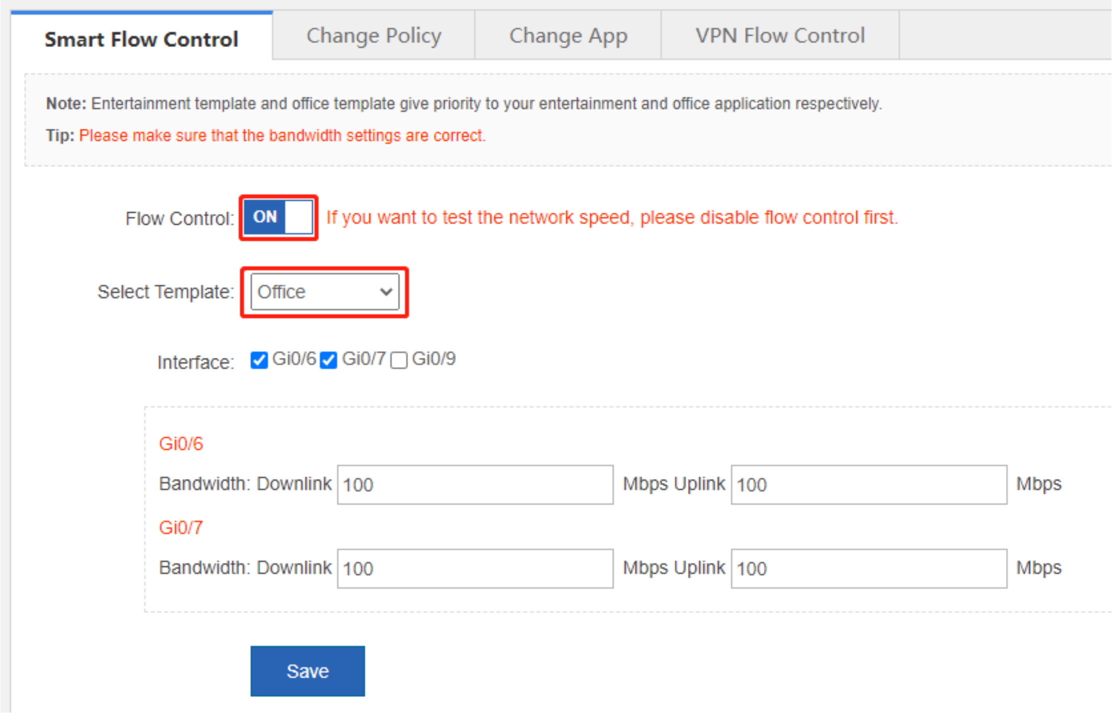
On this tab page, you can enable smart flow control for applications in one click. You can use the entertainment template or office template to provide traffic to your entertainment or office applications first.

Procedure

(1) Choose **Flow** > **Flow Control Policy** > **Smart Flow Control**.

(2) Set the flow control switch to **ON**.

(3) Add an associated application template.



Note: Entertainment template and office template give priority to your entertainment and office application respectively.

Tip: Please make sure that the bandwidth settings are correct.

Flow Control: ON If you want to test the network speed, please disable flow control first.

Select Template: Office

Interface: ☑ Gi0/6 ☑ Gi0/7 □ Gi0/9

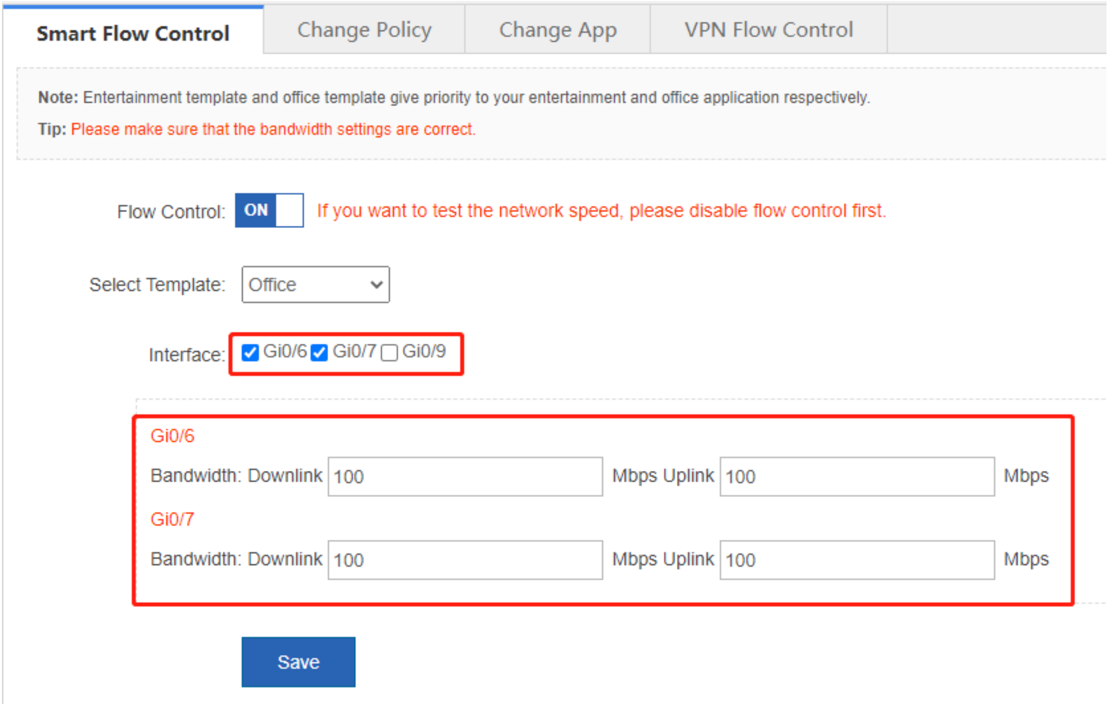
Gi0/6

Bandwidth: Downlink 100 Mbps Uplink 100 Mbps

Gi0/7

Bandwidth: Downlink 100 Mbps Uplink 100 Mbps

(4) Select an interface and set the bandwidth.



Note: Entertainment template and office template give priority to your entertainment and office application respectively.

Tip: Please make sure that the bandwidth settings are correct.

Flow Control: ON If you want to test the network speed, please disable flow control first.

Select Template: Office

Interface: ☑ Gi0/6 ☑ Gi0/7 □ Gi0/9

Gi0/6

Bandwidth: Downlink 100 Mbps Uplink 100 Mbps

Gi0/7

Bandwidth: Downlink 100 Mbps Uplink 100 Mbps

(5) Click **Save**.

5.2.2 Change Policy

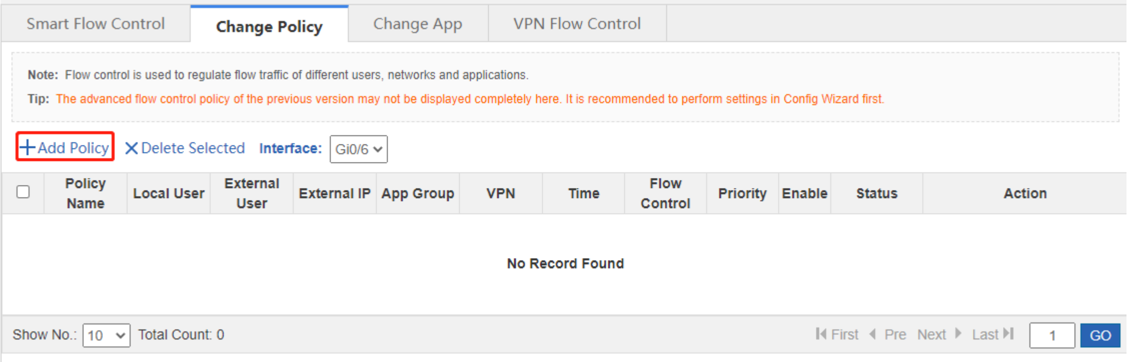
Application Scenario

You can plan and manage your company's internal network or any user or application based on the network condition and company demands.

Procedure

1. Add Policy

(1) Click +Add Policy. The **Add Policy** window is displayed.



Smart Flow Control | Change Policy | Change App | VPN Flow Control

Note: Flow control is used to regulate flow traffic of different users, networks and applications.

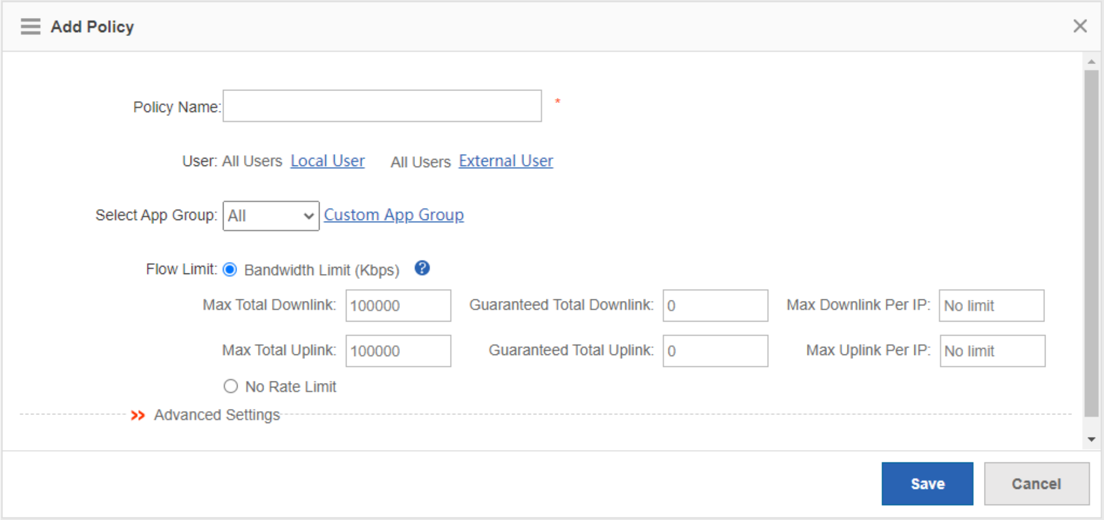
Tip: The advanced flow control policy of the previous version may not be displayed completely here. It is recommended to perform settings in Config Wizard first.

+Add Policy ✕Delete Selected **Interface:** Gi0/6

□	Policy Name	Local User	External User	External IP	App Group	VPN	Time	Flow Control	Priority	Enable	Status	Action

No Record Found

Show No.: 10 Total Count: 0 First Pre Next Last 1 GO



Add Policy

Policy Name: *

User: All Users Local User All Users External User

Select App Group: All Custom App Group

Flow Limit: ● Bandwidth Limit (Kbps)

Max Total Downlink: 100000 Guaranteed Total Downlink: 0 Max Downlink Per IP: No limit

Max Total Uplink: 100000 Guaranteed Total Uplink: 0 Max Uplink Per IP: No limit

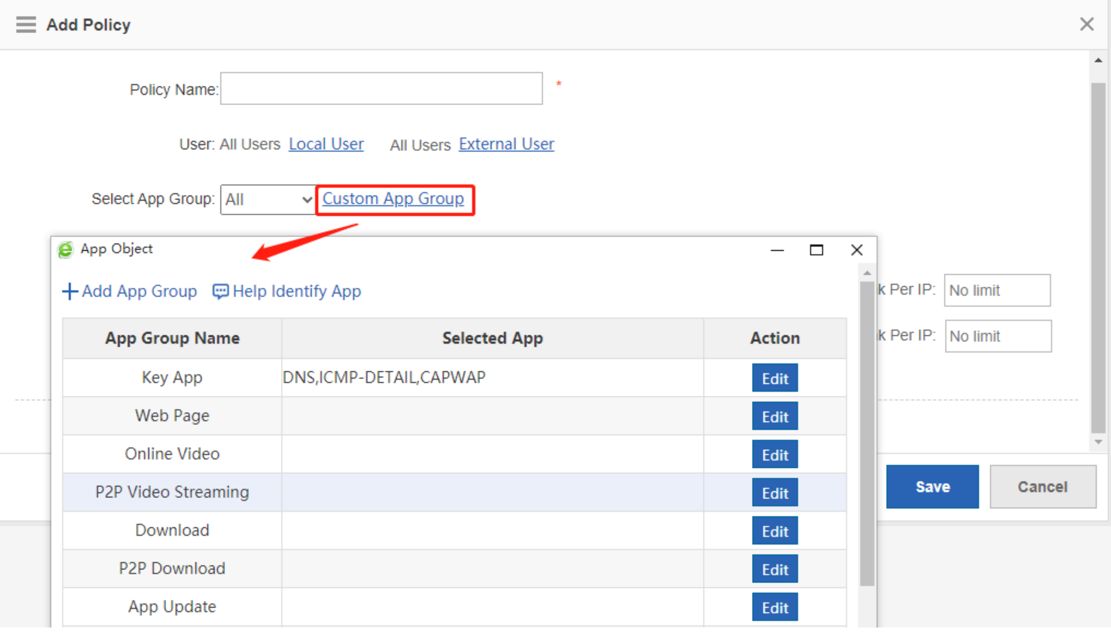
○ No Rate Limit

>> Advanced Settings

Save Cancel

(2) Set policy configuration items.

- Policy Name: In the Policy Name field, input a name for the policy that can indicate the policy purpose or usage.
- User: Select at least one user.
- Select App Group: Select an existing application group from the drop-down list. If the existing application groups do not meet your requirements, you can click Custom App Group to customize an application group.



Add Policy

Policy Name: *

User: All Users Local User All Users External User

Select App Group: All Custom App Group

App Object

+Add App Group Help Identify App

App Group Name	Selected App	Action
Key App	DNS,ICMP-DETAIL,CAPWAP	Edit
Web Page		Edit
Online Video		Edit
P2P Video Streaming		Edit
Download		Edit
P2P Download		Edit
App Update		Edit

k Per IP: No limit

k Per IP: No limit

- **Flow Limit**: You can control the traffic separately. If you select **No Rate Limit**, all applications share the bandwidth. The guaranteed speed and maximum speed are the minimum and maximum speeds at which all users share at the current interface. Maximum Uplink/Download per IP indicates the maximum bandwidth for each user.

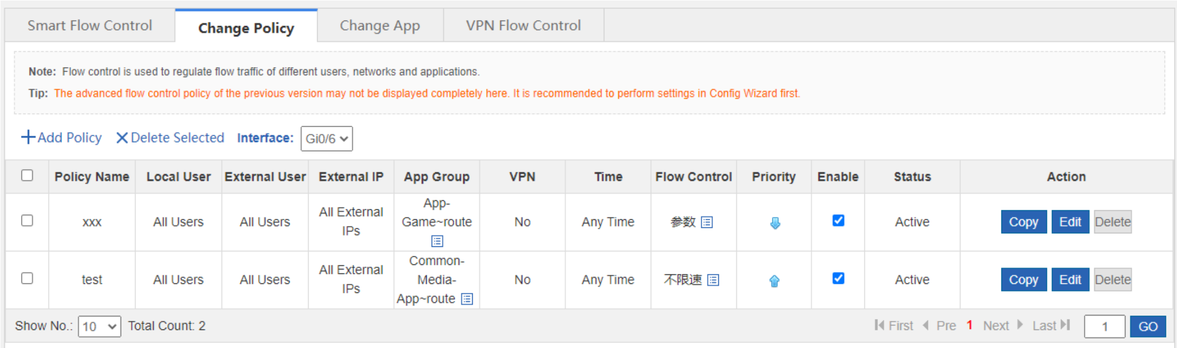
  You can click >> Advanced Settings to make more advanced settings.

- **External IP Group**: Click Select IP Group to select an IP group.
- **Active Time**: Select an active time available from the drop-down list. You can also click Time Management to configure an active time.

(3) Click **Save**.

2. View Policy

After a policy is added, all flow control policies configured for the device are listed in a table on the page. You can modify or delete existing policies, as shown below:



Note: Flow control is used to regulate flow traffic of different users, networks and applications.

Tip: The advanced flow control policy of the previous version may not be displayed completely here. It is recommended to perform settings in Config Wizard first.

+Add Policy ✕Delete Selected **Interface:** Gi0/6

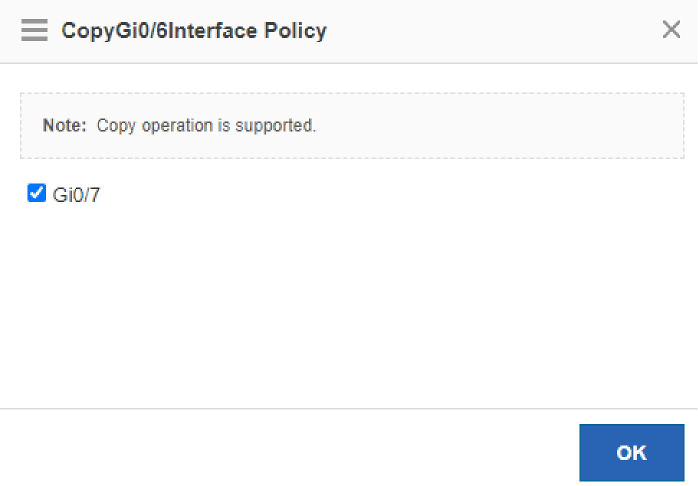
□	Policy Name	Local User	External User	External IP	App Group	VPN	Time	Flow Control	Priority	Enable	Status	Action
□	xxx	All Users	All Users	All External IPs	App-Game~route ☰	No	Any Time	参数 ☰	⬇	☑	Active	Copy Edit Delete
□	test	All Users	All Users	All External IPs	Common-Media-App~route ☰	No	Any Time	不限速 ☰	⬆	☑	Active	Copy Edit Delete

Show No.: 10 Total Count: 2 First Pre 1 Next Last 1 GO

- Click ☰ in the **App Group** column to view applications of an application group.
- **Enable**: You can enable or disable a single policy or all policies. After enabling or disabling, the status

displayed in the **Status** column changes to **Active** or **Inactive**.

- **Status**: Options are **Active** and **Inactive**. When the current time is not the **Active Time** or a policy is disabled, the policy status is **Inactive**.
- **Priority**: The flow control policies come into effect in descending order of configuration time. The first policy is displayed at the top of the table. You can click ⇧ or ⇩ to adjust the priority of existing policies.
- Click Edit. In the dialog box displayed, you can edit or modify a policy.
- Click Delete to delete a policy.
- Click Copy to copy the flow control policies of an interface to another interface.



CopyGi0/6Interface Policy

Note: Copy operation is supported.

☑ Gi0/7

5.2.3 Change Application

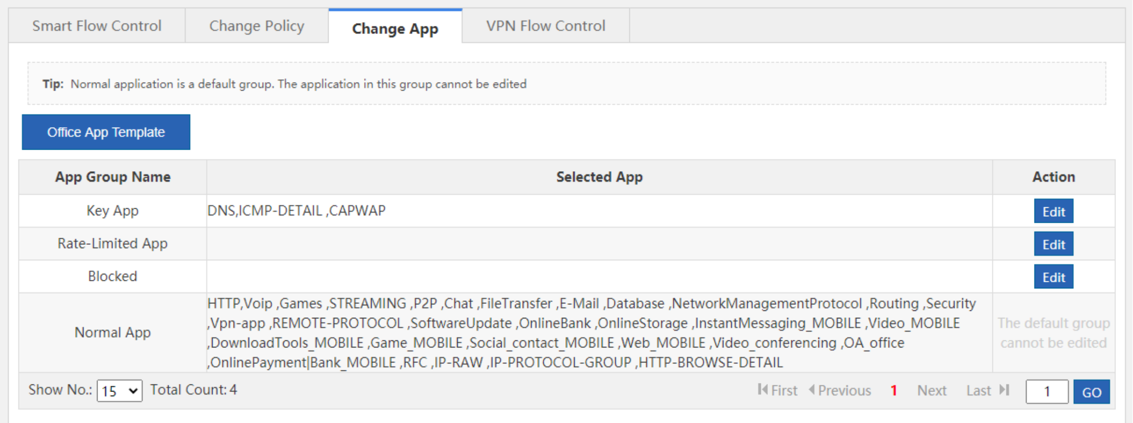
Application Scenario

This function allows you to adjust the application classification.

Procedure

(1) Choose **Flow** > **Flow Control Policy** > **Change App**.

(2) Select the application you want to modify and click **Edit**.



Tip: Normal application is a default group. The application in this group cannot be edited

App Group Name	Selected App	Action
Key App	DNS,ICMP-DETAIL ,CAPWAP	Edit
Rate-Limited App		Edit
Blocked		Edit
Normal App	HTTP,Voip ,Games ,STREAMING ,P2P ,Chat ,FileTransfer ,E-Mail ,Database ,NetworkManagementProtocol ,Routing ,Security ,Vpn-app ,REMOTE-PROTOCOL ,SoftwareUpdate ,OnlineBank ,OnlineStorage ,InstantMessaging_MOBILE ,Video_MOBILE ,DownloadTools_MOBILE ,Game_MOBILE ,Social_contact_MOBILE ,Web_MOBILE ,Video_conferencing ,OA_office ,OnlinePayment|Bank_MOBILE ,RFC ,IP-RAW ,IP-PROTOCOL-GROUP ,HTTP-BROWSE-DETAIL	The default group cannot be edited

Show No.: 15 Total Count: 4

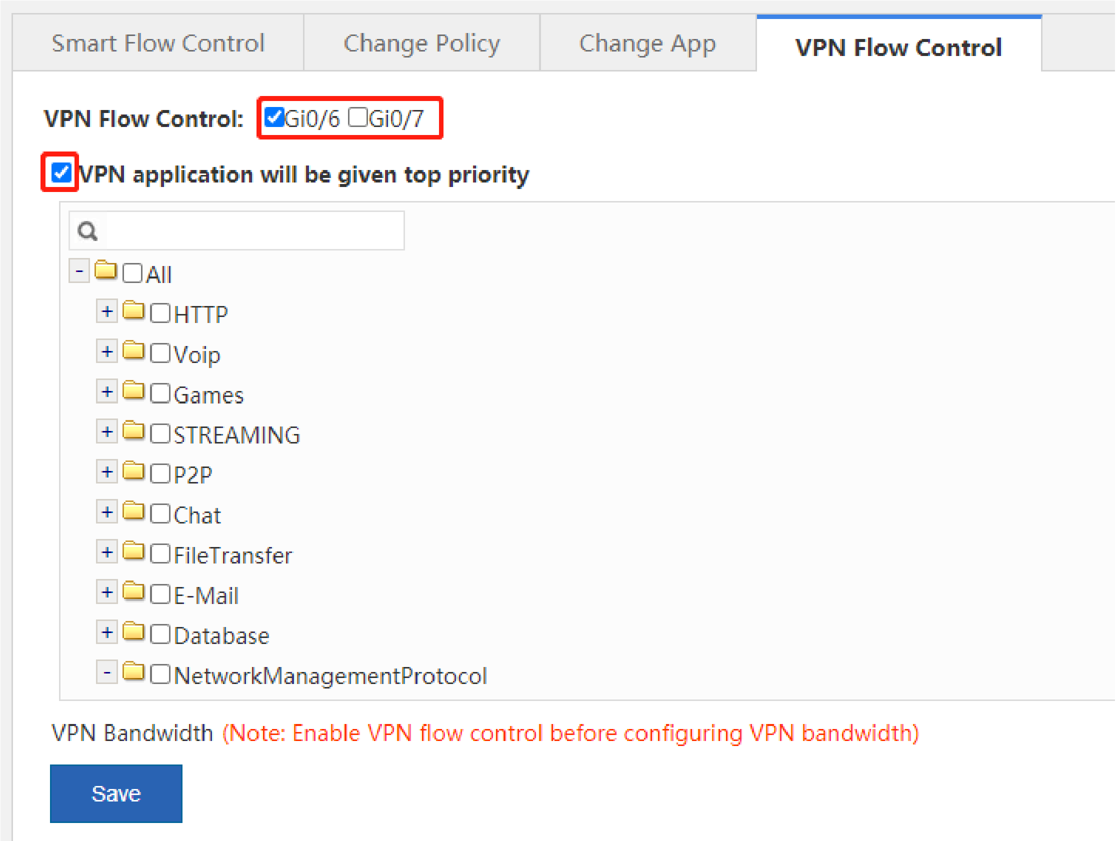
5.2.4 VPN Flow Control

Application Scenario

This function allows you to enable VPN flow control for an interface.

Procedure

(1) Choose **Flow** > **Flow Control Policy** > **VPN Flow Control**.



VPN Flow Control: ☑Gi0/6 □Gi0/7

☑VPN application will be given top priority

- □All
  - □HTTP
  - □Voip
  - □Games
  - □STREAMING
  - □P2P
  - □Chat
  - □FileTransfer
  - □E-Mail
  - □Database
  - □NetworkManagementProtocol

VPN Bandwidth (Note: Enable VPN flow control before configuring VPN bandwidth)

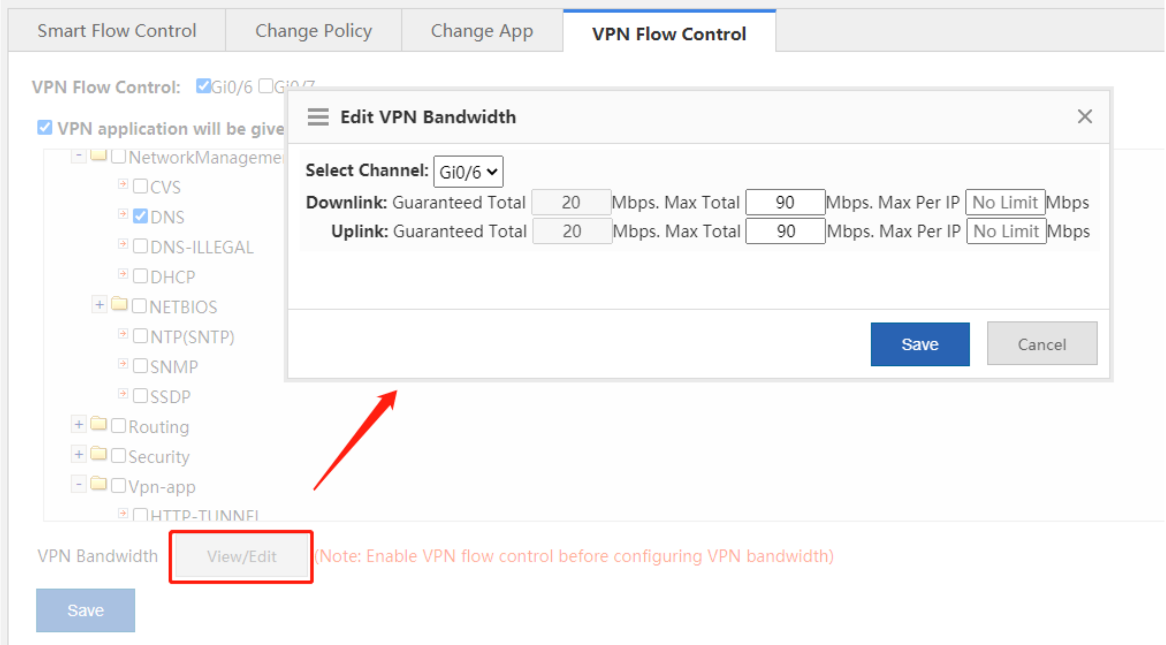
(2) Select the interface for which you want to enable VPN flow control.

(3) Select a key application.

(4) Click **Save**.

Follow-up Procedure

After configuring the interface, click **View/Edit** to configure the available bandwidth for key VPN applications on the current channel.



Select Channel: Gi0/6

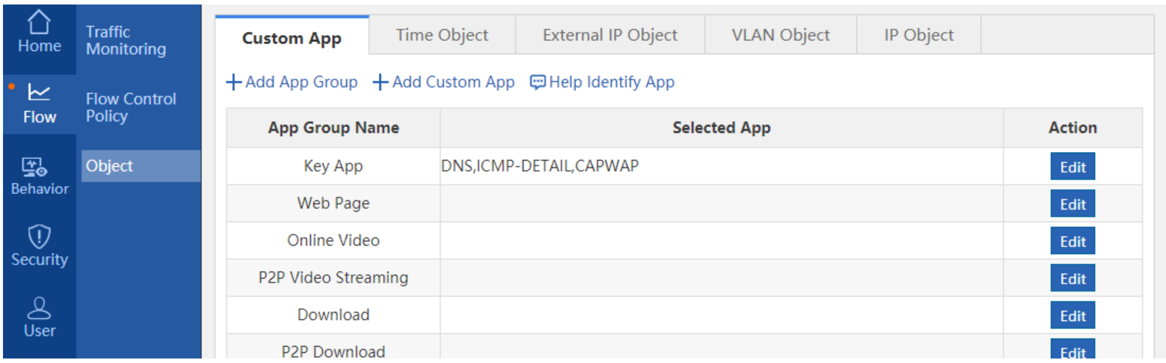
Downlink: Guaranteed Total	20	Mbps. Max Total	90	Mbps. Max Per IP	No Limit	Mbps
Uplink: Guaranteed Total	20	Mbps. Max Total	90	Mbps. Max Per IP	No Limit	Mbps

(Note: Enable VPN flow control before configuring VPN bandwidth)

5.3 Object Definition

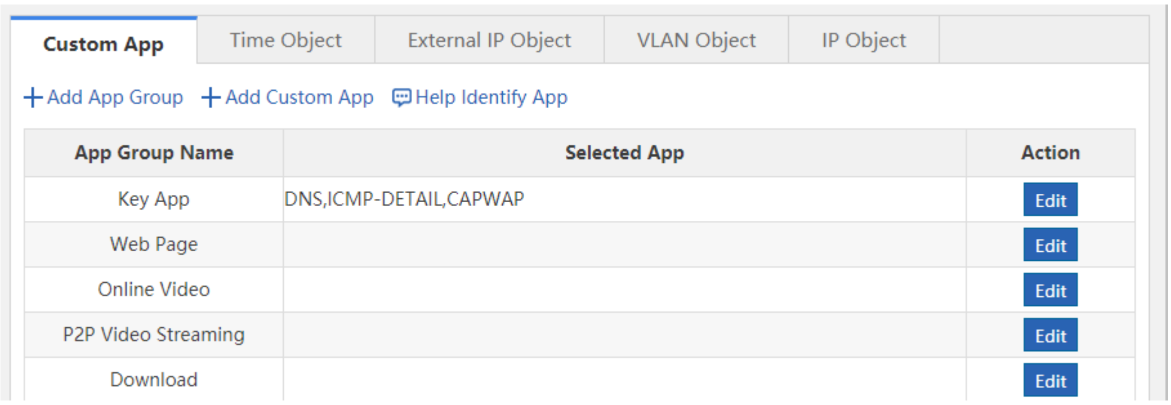
5.3.1 Introduction

For management convenience, the system allows you to abstract some common configuration items into objects, such as time objects, application group objects, and VLAN objects. The following figure shows objects supported by the system:



App Group Name	Selected App	Action
Key App	DNS,ICMP-DETAIL,CAPWAP	Edit
Web Page		Edit
Online Video		Edit
P2P Video Streaming		Edit
Download		Edit
P2P Download		Edit

5.3.2 Custom App Group



App Group Name	Selected App	Action
Key App	DNS,ICMP-DETAIL,CAPWAP	Edit
Web Page		Edit
Online Video		Edit
P2P Video Streaming		Edit
Download		Edit

This page displays all application groups available in the current system and applications of each application group. Key App, Rate-Limited App, Blocked, Normal App, Web Page, Online Video, P2P Video Streaming, Download, P2P Download, App Update, and Upload are application groups available in the system, and others are application groups defined by users.

1. App Group

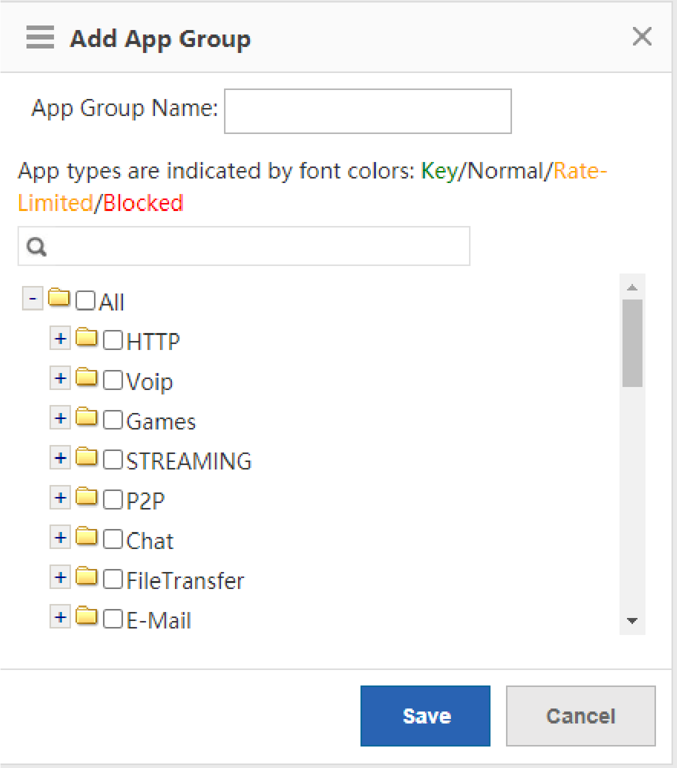
Application Scenario

You can set application groups to manage usage of a company's internal protocol in a unified manner and ensure that the company's internal network can be accessed smoothly and the bandwidth is not wasted.

Procedure

(1) Choose **Flow** > **Object** > **Custom App**.

(2) Click + Add App Group to customize an application group.



App types are indicated by font colors: Key/Normal/Rate-Limited/Blocked

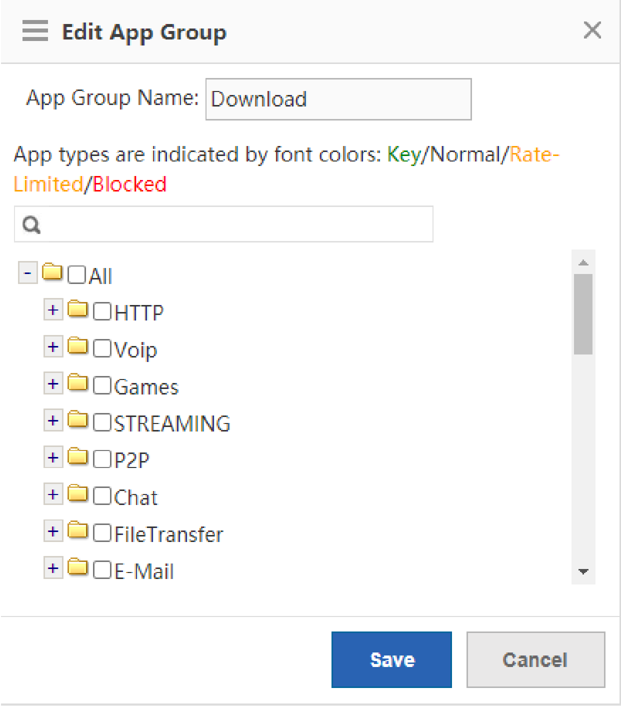
(3) In the **App Group Name** field, input a name for the application group, and select applications that you want to join this application group.

(4) Click Save to save the configuration of the custom application group. The information of the configured application group is displayed in the table on the **Custom App** page.

Follow-up Procedure

- Edit an application group:

  In the table on the **Custom App** page, click Edit to reallocate applications to an application group.



App Group Name: Download

App types are indicated by font colors: Key/Normal/Rate-Limited/Blocked

- ☐All
  - ☐HTTP
  - ☐Voip
  - ☐Games
  - ☐STREAMING
  - ☐P2P
  - ☐Chat
  - ☐FileTransfer
  - ☐E-Mail

Applications displayed in green are already in the key/guaranteed application group. Applications displayed in orange are already in the rate-limited application group. Applications in red are already in the blocked application group. Applications in black are already in normal/other application group or applications not added to any group.

Applications already added to the key/guaranteed application group, rate-limited application group, or blocked application group cannot be added to any other groups.

To modify a rate-limited application to a key/guaranteed application, you must first delete the target application from the rate-limited application group, and then add this application to the key/guaranteed application group.

- Delete an application group:

  In the table on the **Custom App** page, click Delete to delete a custom application group. You cannot delete system application groups, that is, the key/guaranteed application group, the rate-limited application group, the blocked application group, and the normal/other application group.

2. Custom App

Application Scenario

In addition to built-in network application protocols of the system, you can also customize other network applications, such as applications based on a port or a destination server. Like built-in protocols of the system, custom protocols can also be used for policy-based network application control and bandwidth management, as well as real-time network application monitoring.

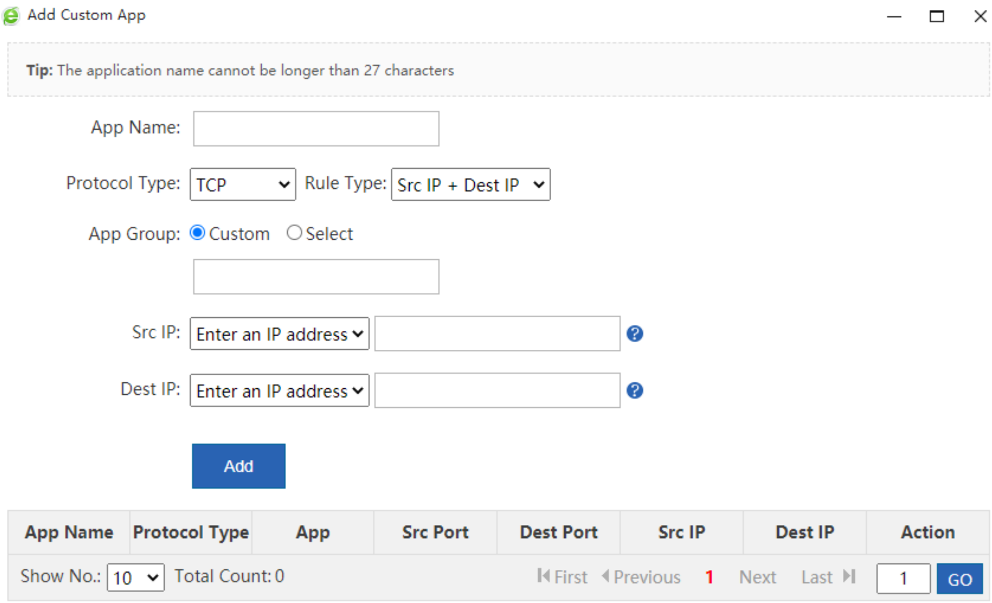
Note

Custom protocols have the highest priority. When a custom protocol conflicts with a built-in protocol of the system (for example, their port IDs are the same), the custom protocol is applied.

Procedure

(1) Choose **Flow** > **Object** > **Custom App**.

(2) On the **Custom App** page, click + Add Custom App. The following **Add Custom App** window is displayed:



Add Custom App

Tip: The application name cannot be longer than 27 characters

App Name:

Protocol Type: TCP Rule Type: Src IP + Dest IP

App Group: ● Custom ○ Select

Src IP: Enter an IP address

Dest IP: Enter an IP address

Add

App Name	Protocol Type	App	Src Port	Dest Port	Src IP	Dest IP	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

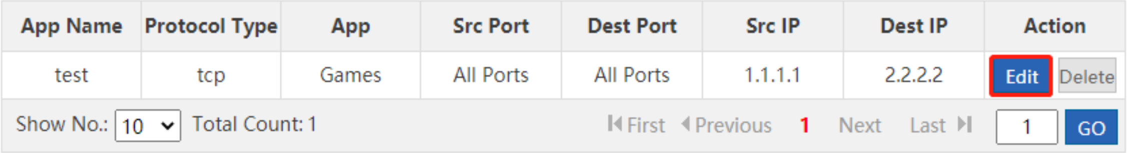
(3) Set configuration items for the custom application.

Input a name for the custom application, select the protocol type, select the rule type, select the application group (you can customize an application group or select among built-in application groups), and input the source or destination port ID or IP address based on the selected rule type.

(4) Click Add. The configuration is successful.

Follow-up Procedure

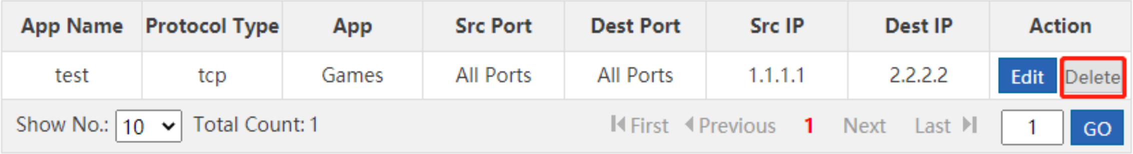
- **Edit a custom application**: Select the application you want to modify and then click Edit.



App Name	Protocol Type	App	Src Port	Dest Port	Src IP	Dest IP	Action
test	tcp	Games	All Ports	All Ports	1.1.1.1	2.2.2.2	Edit Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

- **Delete a custom application**: Select the application you want to delete and then click Delete.



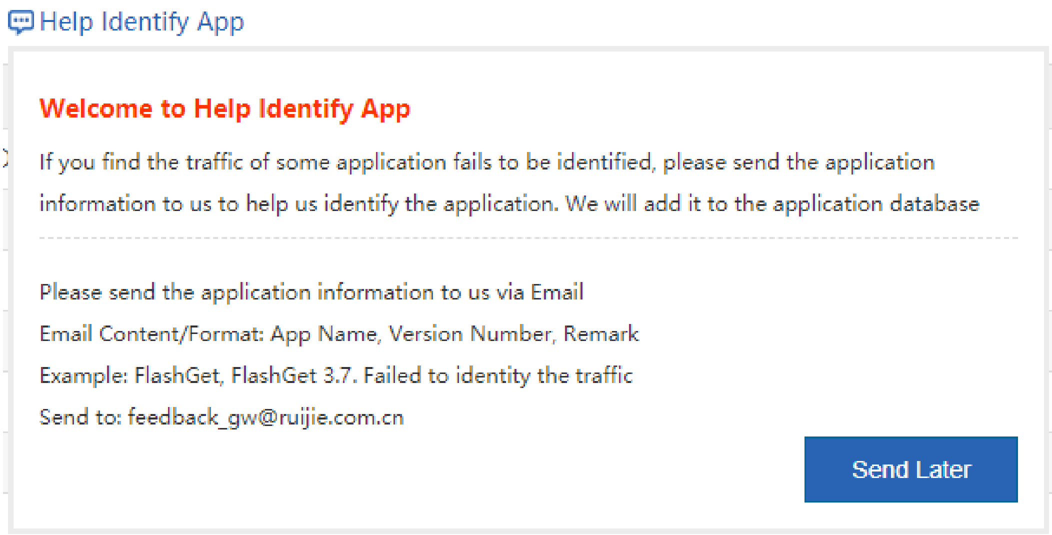
App Name	Protocol Type	App	Src Port	Dest Port	Src IP	Dest IP	Action
test	tcp	Games	All Ports	All Ports	1.1.1.1	2.2.2.2	Edit Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

3. Feed Back Applications that Failed to be Identified

Application Scenario

When the traffic of a network application cannot be identified by the current device and thus you cannot effectively control this application, you can click Help Identify App. In the window displayed, report the event to Ruijie Cloud Center and we will analyze the application you report and add it to the feature library to meet your requirements.



Help Identify App

Welcome to Help Identify App

If you find the traffic of some application fails to be identified, please send the application information to us to help us identify the application. We will add it to the application database

Please send the application information to us via Email

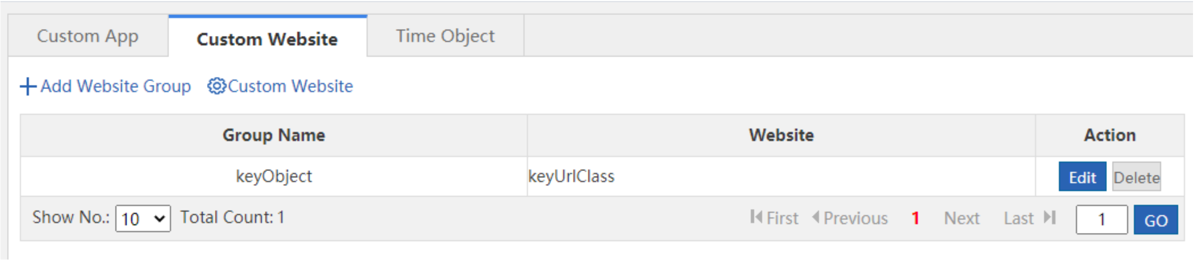
Email Content/Format: App Name, Version Number, Remark

Example: FlashGet, FlashGet 3.7. Failed to identity the traffic

Send to: feedback_gw@ruijie.com.cn

5.3.3 Custom Website Group

The following figure shows the **Custom Website** page, which displays all application groups available in the current system and applications of each application group.



Group Name	Website	Action
keyObject	keyUrlClass	Edit Delete

Show No.: 10 Total Count: 1

1. Website Group

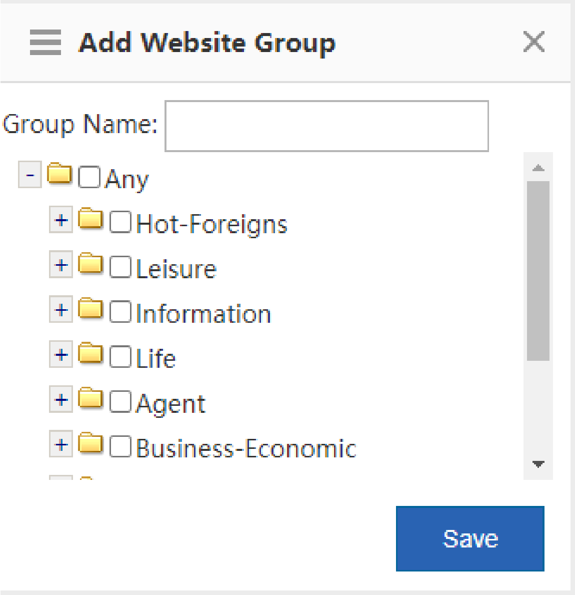
Application Scenario

You can set website groups to manage websites accessed by internal employees of the company in a unified manner and ensure that the company's internal network can be accessed smoothly and the bandwidth is not wasted on work-unrelated networks.

Procedure

(1) Choose **Behavior** > **Object** > **Custom Website.**

(2) Click + Add Website Group to customize a website group.



Add Website Group

Group Name:

- □ Any
  - □ Hot-Foreigns
  - □ Leisure
  - □ Information
  - □ Life
  - □ Agent
  - □ Business-Economic

Save

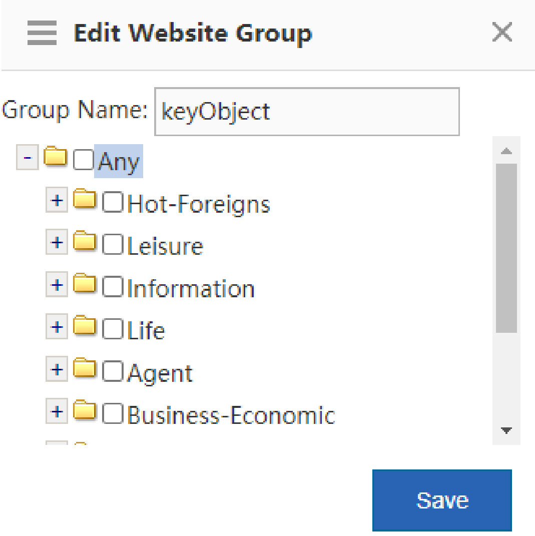
(3) Input a name for the website group and select the websites for this website group.

(4) Click Save. Then, a new website group is created.

Follow-up Procedure

- Edit a website group:

  In the table on the Custom Website page, click Edit to reallocate websites to a website group:



Edit Website Group

Group Name: keyObject

- □ Any
  - □ Hot-Foreigns
  - □ Leisure
  - □ Information
  - □ Life
  - □ Agent
  - □ Business-Economic

Save

  Select the desired websites, deselect the undesired websites, and then click Save.

- Delete a website group:

  In the table on the **Custom Website** page, click Delete to delete the selected website group.

2. Custom Website

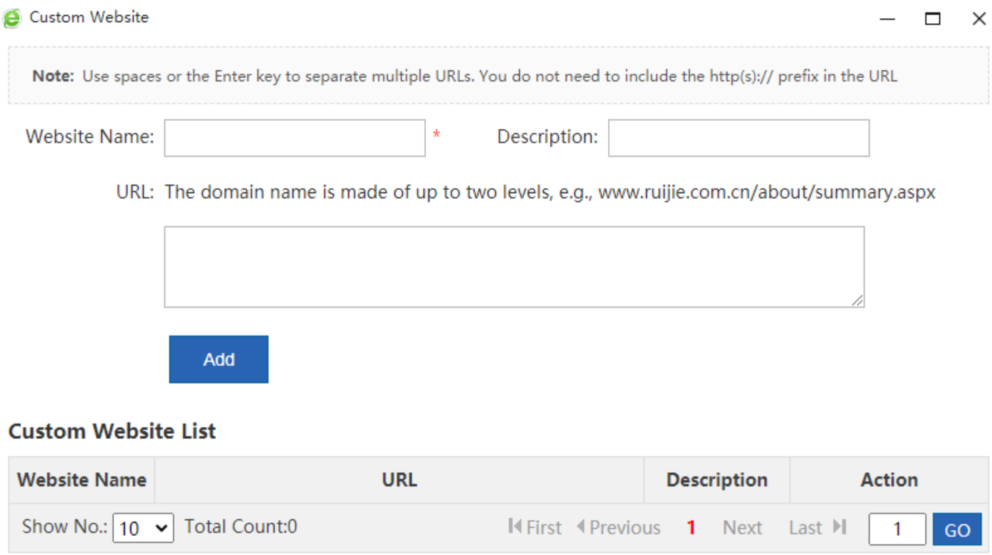
Application Scenario

In addition to built-in website types of the system, you can custom other websites. For example, you can allocate several similar websites to a website group. Like built-in websites of the system, action policies can also be applied to custom websites.

Procedure

(1) Choose **Behavior** > **Object** > **Custom Website**.

(2) On the **Custom Website** page, click ⚙Custom Website. The following **Custom Website** window is displayed:



Custom Website

Note: Use spaces or the Enter key to separate multiple URLs. You do not need to include the http(s):// prefix in the URL

Website Name: * Description:

URL: The domain name is made of up to two levels, e.g., www.ruijie.com.cn/about/summary.aspx

Add

Custom Website List

Website Name	URL	Description	Action

Show No.: 10 Total Count:0 First Previous 1 Next Last 1 GO

(3) Set website configuration items.

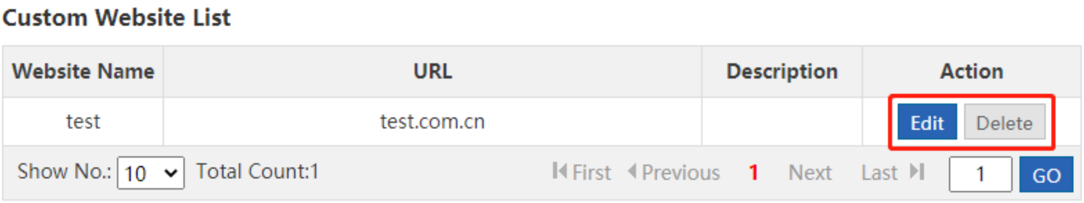
Create a custom website: Input a name that can clearly indicate the intention or user of this website for the custom website, and input the domain names of the website (separate multiple domain names by commas (,)).

(4) Click Add. The configuration is successful.

The system allows you to configure up to 100 custom websites.

Follow-up Procedure

- Edit a custom website: Select the website you want to modify and then click Edit.



Custom Website List

Website Name	URL	Description	Action
test	test.com.cn		Edit Delete

Show No.: 10 Total Count:1 First Previous 1 Next Last 1 GO

- Delete a custom website: Select the website you want to delete and then click Delete.

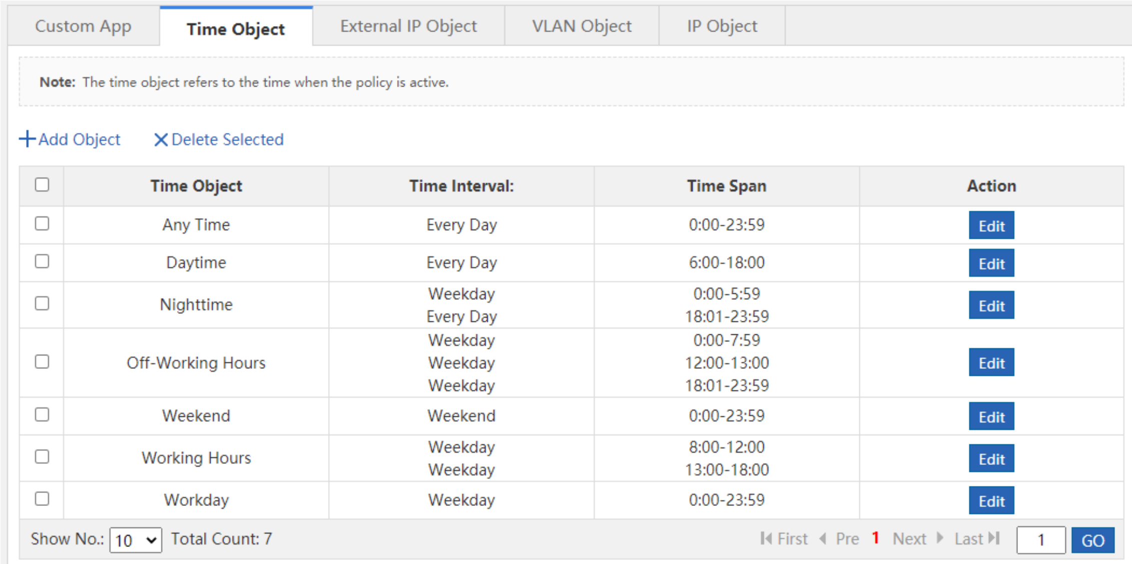
5.3.4 Time Object

Application Scenario

This function allows you to define a time object which is used during policy setting.

Procedure

(1) Choose **Flow** > **Object** > **Time Object**.



Note: The time object refers to the time when the policy is active.

+Add Object ✕Delete Selected

□	Time Object	Time Interval:	Time Span	Action
□	Any Time	Every Day	0:00-23:59	Edit
□	Daytime	Every Day	6:00-18:00	Edit
□	Nighttime	Weekday Every Day	0:00-5:59 18:01-23:59	Edit
□	Off-Working Hours	Weekday Weekday Weekday	0:00-7:59 12:00-13:00 18:01-23:59	Edit
□	Weekend	Weekend	0:00-23:59	Edit
□	Working Hours	Weekday Weekday	8:00-12:00 13:00-18:00	Edit
□	Workday	Weekday	0:00-23:59	Edit

Show No.: 10 Total Count: 7

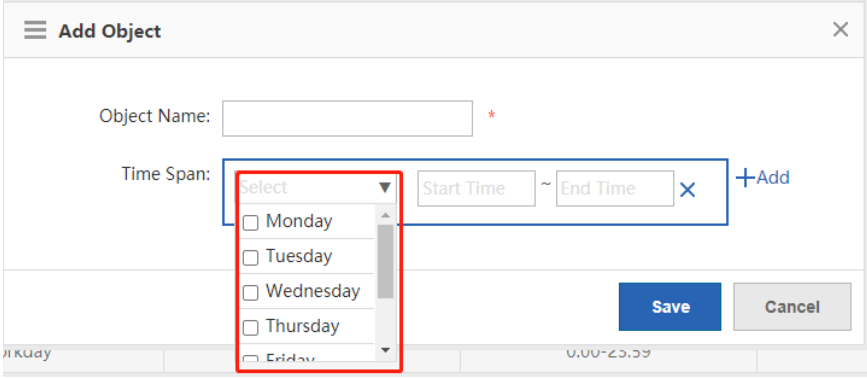
(2) Click +Add Object.

(3) In the window displayed, input a name for the object and select one or more time spans.

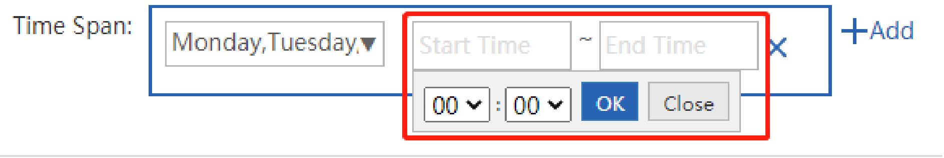
The following describes how to create a weekday time object:

a In the **Object Name** field, input a name for the time object.

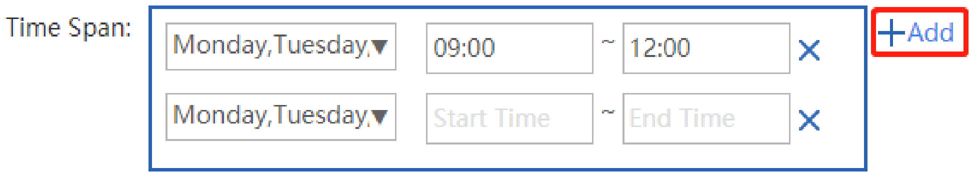
b From the drop-down list of **Time Span**, select a time interval, that is, select a week starting from Monday to Friday.



c From the drop-down list of **Time Span**, select a time span.



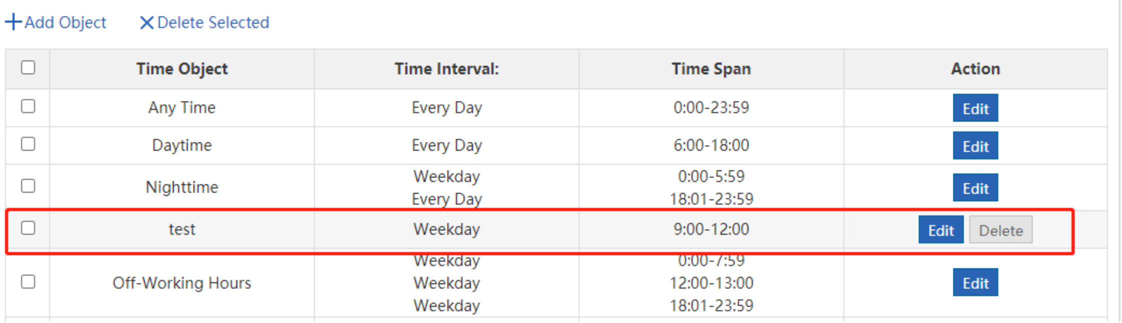
d You can click **Add** to add another time span.



Time Span: Monday,Tuesday,▼ 09:00 ~ 12:00 ×

Monday,Tuesday,▼ Start Time ~ End Time ×

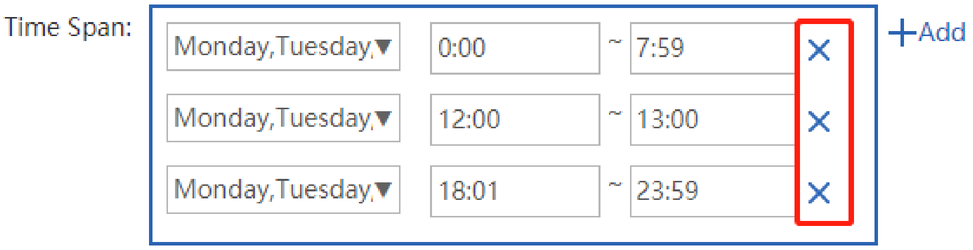
(4) Then, click Save. A time object is generated.



□	Time Object	Time Interval:	Time Span	Action
□	Any Time	Every Day	0:00-23:59	Edit
□	Daytime	Every Day	6:00-18:00	Edit
□	Nighttime	Weekday Every Day	0:00-5:59 18:01-23:59	Edit
□	test	Weekday	9:00-12:00	Edit Delete
□	Off-Working Hours	Weekday Weekday Weekday	0:00-7:59 12:00-13:00 18:01-23:59	Edit

Follow-up Procedure

- Edit a time object: Select the time object you want to edit, and click Edit. In the window displayed, you can delete or modify the time object or add a time object.
- Delete a time object: Select a time object in the list and then click Delete to delete it.
- Delete a time span: To delete a time span of a time object, select a time object in the list. In the window displayed, select the time span you want to delete, and then click × .



Time Span: Monday,Tuesday,▼ 0:00 ~ 7:59 ×

Monday,Tuesday,▼ 12:00 ~ 13:00 ×

Monday,Tuesday,▼ 18:01 ~ 23:59 ×

5.3.5 External IP Object

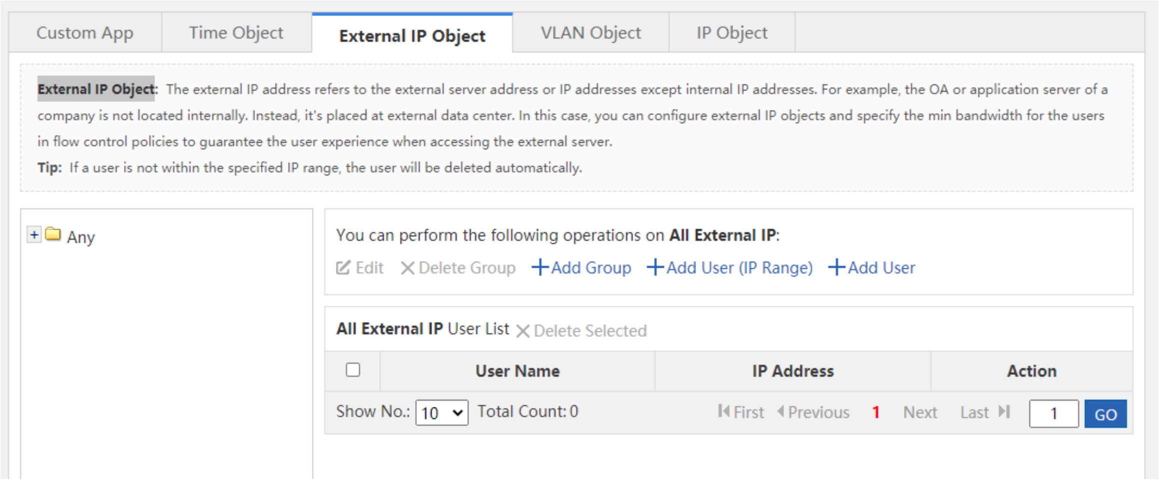
Application Scenario

An external IP object is an external server address or other IP address except for your internal IP address. For example, the server of your company's OA or service system is not deployed in your company, but in the computer room of China Telecom or a hosting center. To ensure that your internal network users can access this server, you can configure the address of this server as an external IP object and specify the minimum bandwidth for users in flow control policies.

The system has a default object "/". When L2 or L3 classification recognition is enabled, the destination IP address in the packets matches the default object "/" when it does not match any other network object.

Procedure

(1) Choose **Flow** > **Object** > **External IP Object**.



External IP Object: The external IP address refers to the external server address or IP addresses except internal IP addresses. For example, the OA or application server of a company is not located internally. Instead, it's placed at external data center. In this case, you can configure external IP objects and specify the min bandwidth for the users in flow control policies to guarantee the user experience when accessing the external server.

Tip: If a user is not within the specified IP range, the user will be deleted automatically.

You can perform the following operations on **All External IP**:

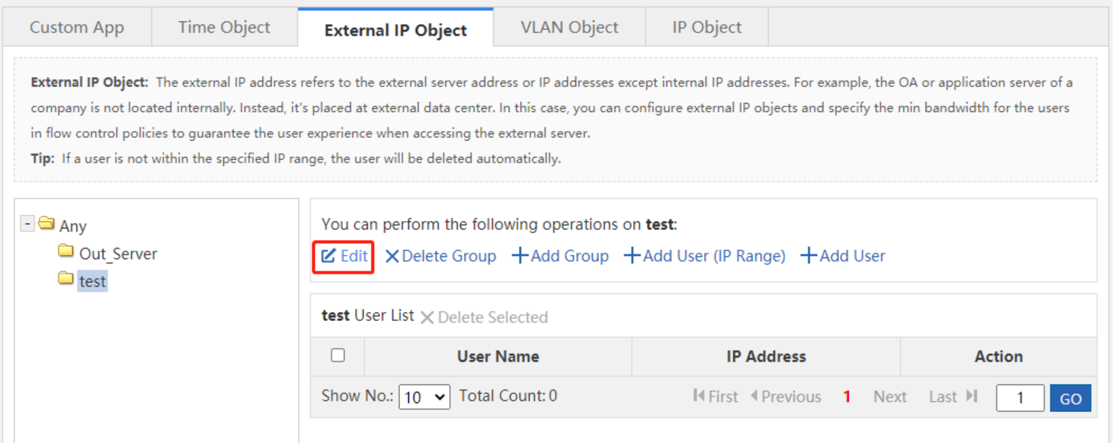
All External IP User List ✕ Delete Selected

□	User Name	IP Address	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

(2) The tree on the left shows the structure of current external IP objects. After you select an external IP object, the object information is displayed on the right. You can edit or modify the object information.

- Click Edit to modify the name of selected external user group or external IP group.



External IP Object: The external IP address refers to the external server address or IP addresses except internal IP addresses. For example, the OA or application server of a company is not located internally. Instead, it's placed at external data center. In this case, you can configure external IP objects and specify the min bandwidth for the users in flow control policies to guarantee the user experience when accessing the external server.

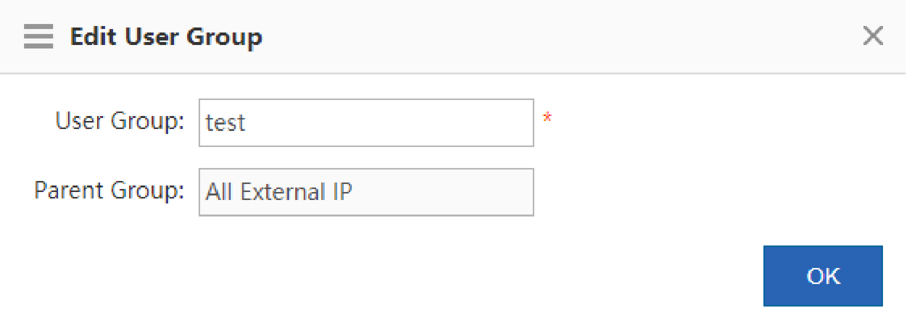
Tip: If a user is not within the specified IP range, the user will be deleted automatically.

You can perform the following operations on **test**:

test User List ✕ Delete Selected

□	User Name	IP Address	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

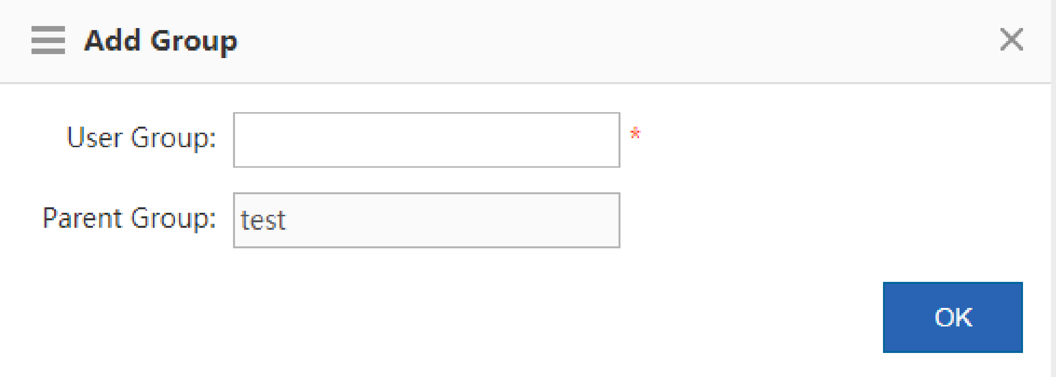


Edit User Group

User Group: test *

Parent Group: All External IP

- Click ✕Delete Group to delete the selected external user group or external IP group from the tree of external IP objects.
- Click +Add Group to add an external user sub-group to the selected external user group.



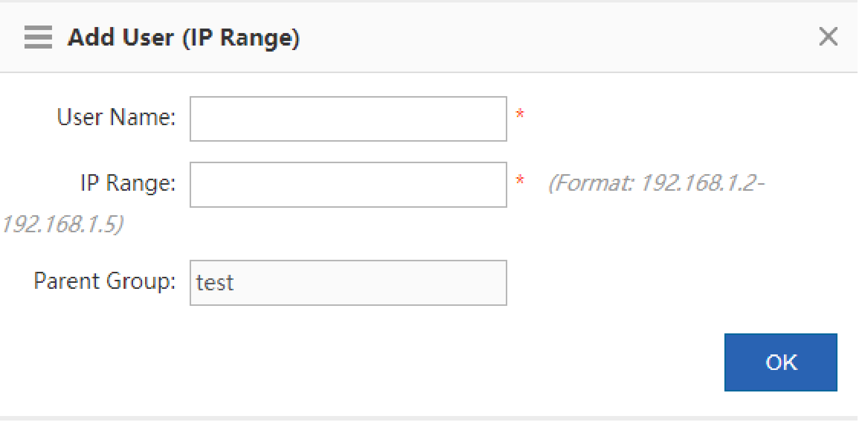
Add Group

User Group: *

Parent Group: test

OK

- Click +Add User (IP Range) to add an IP group to the selected external user group.



Add User (IP Range)

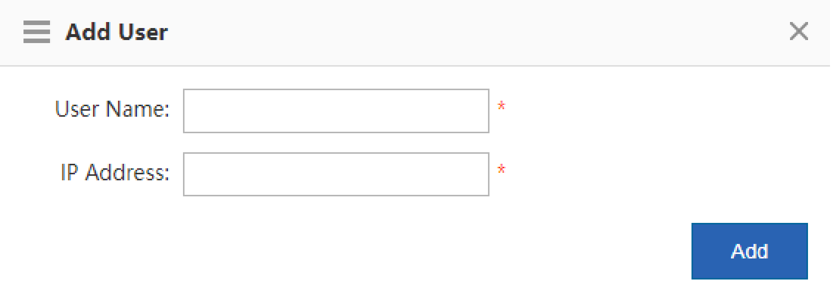
User Name: *

IP Range: * *(Format: 192.168.1.2-192.168.1.5)*

Parent Group: test

OK

- Click +Add User to add a user member to the selected external user group or external IP group.



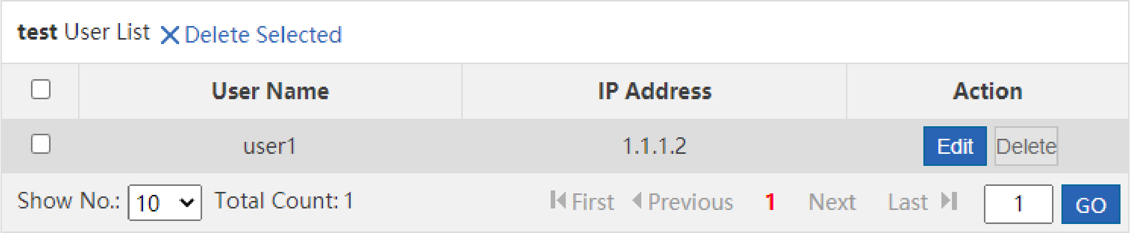
Add User

User Name: *

IP Address: *

Add

User list of external user group or external IP group:



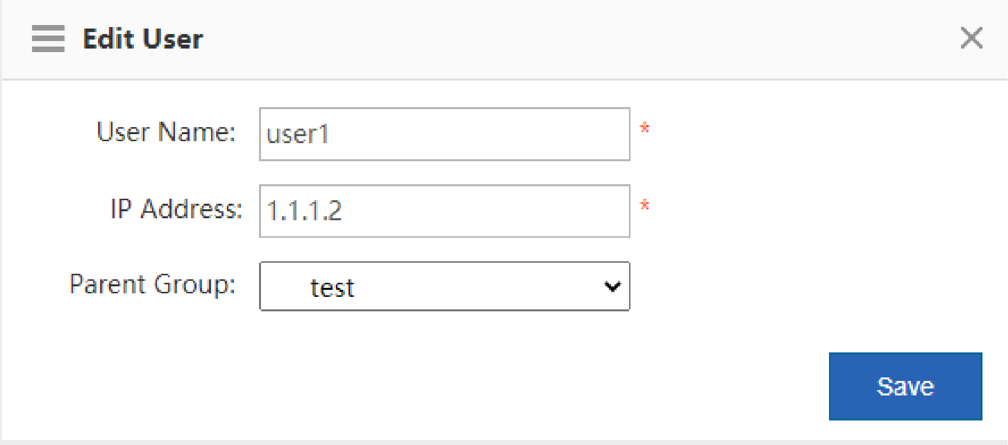
test User List ✕ Delete Selected

□	User Name	IP Address	Action
□	user1	1.1.1.2	Edit Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

The table above shows all the users of the external user group or external IP group you have selected from the left tree. You can edit or delete users.

Click Edit. In the **Edit User** dialog box displayed, you can modify the user name, IP address, and parent group (move a user to another external user group).



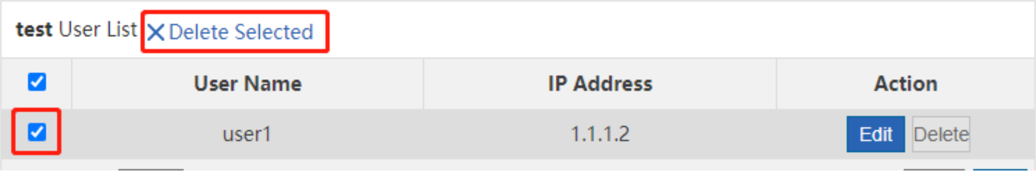
Edit User

User Name: user1 *

IP Address: 1.1.1.2 *

Parent Group: test

- Click Delete to delete a user from the selected external user group or external IP group. You can also select multiple users and then click ✕ Delete Selected to delete them.

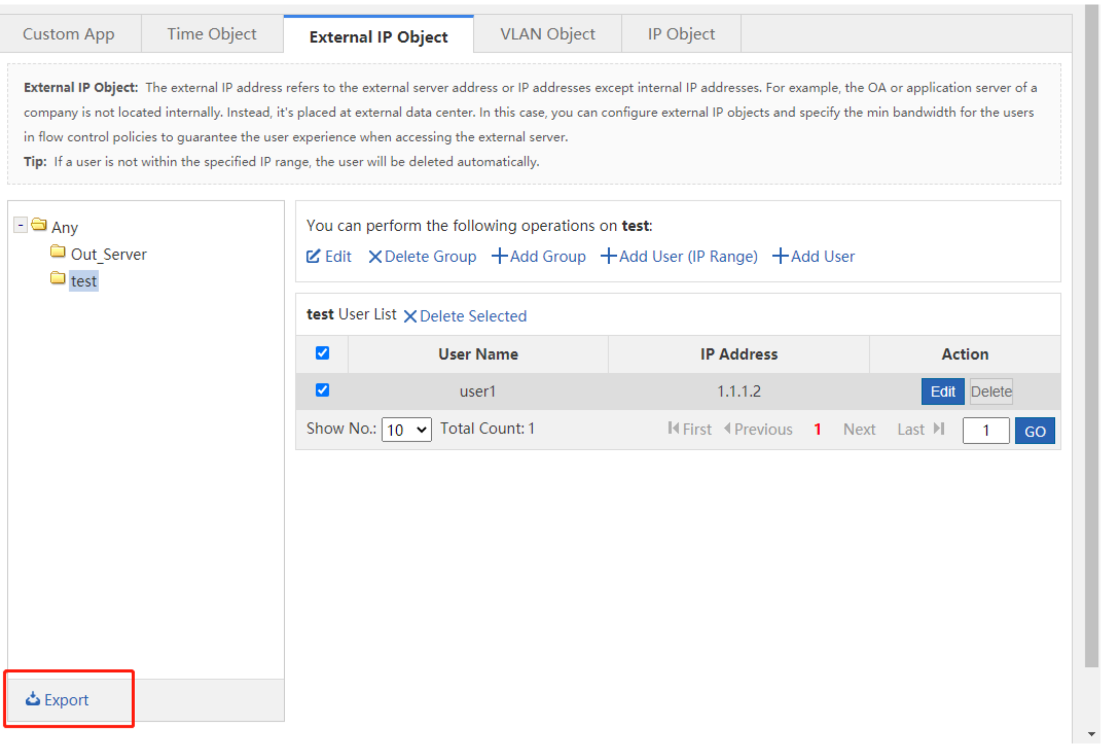


test User List ✕ Delete Selected

☑	User Name	IP Address	Action
☑	user1	1.1.1.2	Edit Delete

(3) Import/export.

- You can also import or export external IP addresses from or to a file. Click Export and the following window is displayed.



External IP Object: The external IP address refers to the external server address or IP addresses except internal IP addresses. For example, the OA or application server of a company is not located internally. Instead, it's placed at external data center. In this case, you can configure external IP objects and specify the min bandwidth for the users in flow control policies to guarantee the user experience when accessing the external server.

Tip: If a user is not within the specified IP range, the user will be deleted automatically.

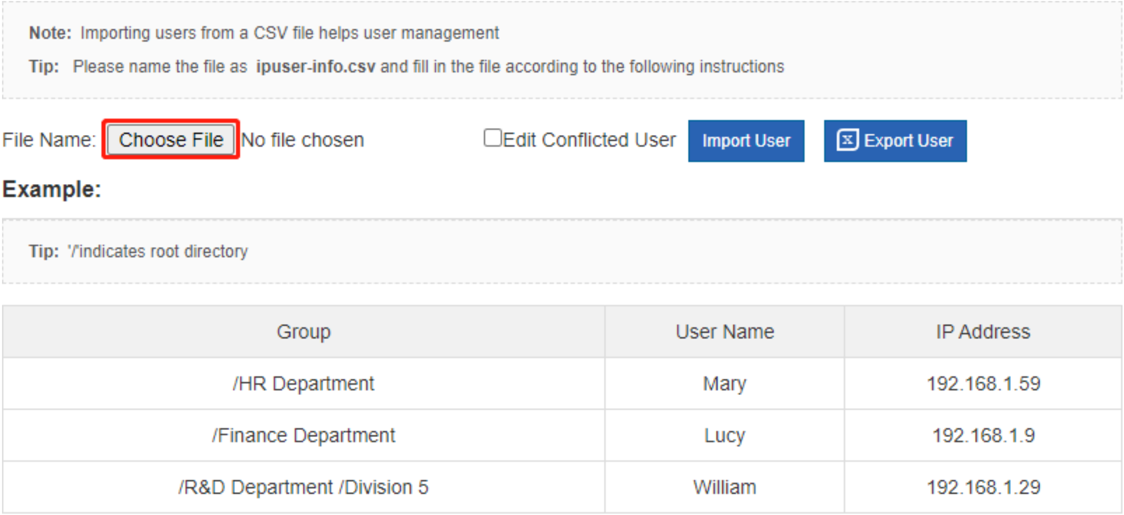
You can perform the following operations on **test**:

Edit ✕Delete Group +Add Group +Add User (IP Range) +Add User

test User List ✕Delete Selected

☑	User Name	IP Address	Action
☑	user1	1.1.1.2	Edit Delete

Show No.: 10 Total Count: 1



Note: Importing users from a CSV file helps user management

Tip: Please name the file as **ipuser-info.csv** and fill in the file according to the following instructions

File Name: Choose File No file chosen ☐Edit Conflicted User Import User Export User

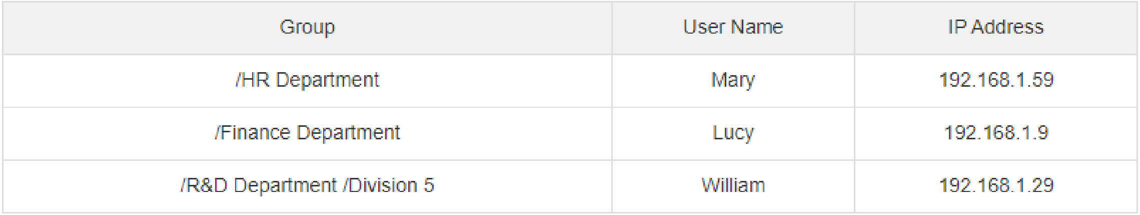
Example:

Tip: '/'indicates root directory

Group	User Name	IP Address
/HR Department	Mary	192.168.1.59
/Finance Department	Lucy	192.168.1.9
/R&D Department /Division 5	William	192.168.1.29

- **Import external IP addresses**: This function allows you to import external IP addresses from a file to help the administrator edit external IP addresses in one click.

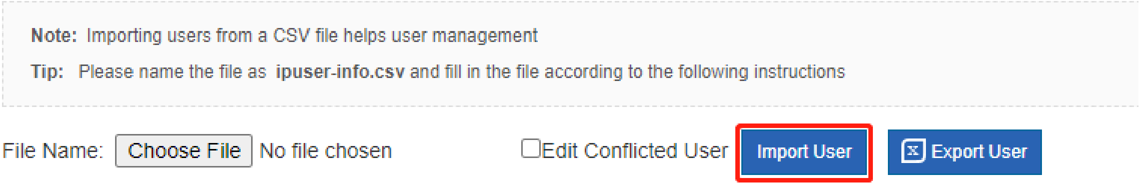
a Create a table named **ipuser-info.csv** on a local PC, and input the external IP address information according to the following format in the table:



Group	User Name	IP Address
/HR Department	Mary	192.168.1.59
/Finance Department	Lucy	192.168.1.9
/R&D Department /Division 5	William	192.168.1.29

b Click **Browse** and find the file **ipuser-info.csv**.

c Click Import User. An import progress bar is displayed. When the progress bar is loaded completely, the file is uploaded.



Note: Importing users from a CSV file helps user management

Tip: Please name the file as **ipuser-info.csv** and fill in the file according to the following instructions

File Name: Choose File No file chosen ☐Edit Conflicted User Import User Export User

- **Export external IP addresses**: Click Export User, select a save path, and then click **Save**.

5.3.6 VLAN Object

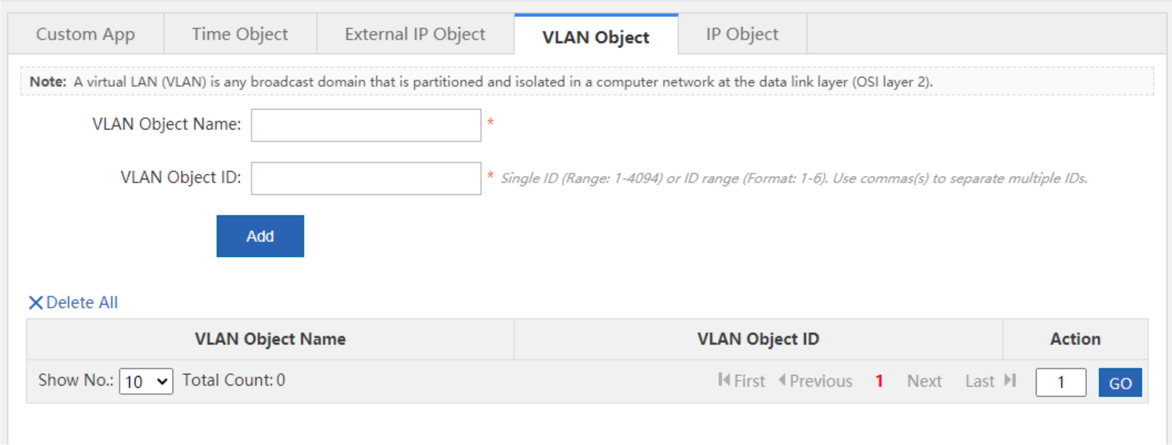
Application Scenario

Multiple VLAN objects cannot have the same VLAN ID and multiple VLAN IDs must be separated by commas (,). To configure several continuous VLAN IDs for the same VLAN object, separate the start VLAN ID and end VLAN ID by "-".

The system has a default VLAN object "any". When L2 or L3 classification recognition is enabled, in router mode, all data streams match the default object "any" by default. In bridge mode, all data streams match the VLAN object corresponding to the native VLAN in the bridge by default. If no VLAN object is set for the bridge native VLAN, the data streams match the default object "any".

Procedure

(1) Choose **Flow** > **Object** > **VLAN Object**.



Note: A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

VLAN Object Name: *

VLAN Object ID: * *Single ID (Range: 1-4094) or ID range (Format: 1-6). Use commas(s) to separate multiple IDs.*

VLAN Object Name	VLAN Object ID	Action

Show No.: 10 Total Count: 0

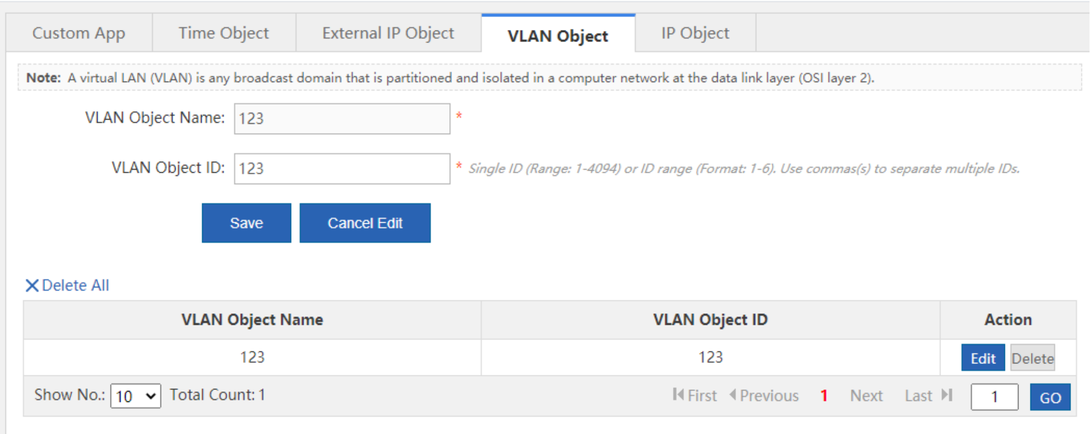
(2) Input a name and ID in the **VLAN Object Name** and **VLAN Object ID** fields respectively.

(3) Click Add.

Follow-up Procedure

- **Edit a VLAN object**: Select the VLAN object you want to edit and then click Edit.

  For example, to edit the object vlan1, click Edit, modify its name or ID, and then click Save.



Note: A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

VLAN Object Name: 123 *

VLAN Object ID: 123 * *Single ID (Range: 1-4094) or ID range (Format: 1-6). Use commas(s) to separate multiple IDs.*

VLAN Object Name	VLAN Object ID	Action
123	123	Edit Delete

Show No.: 10 Total Count: 1

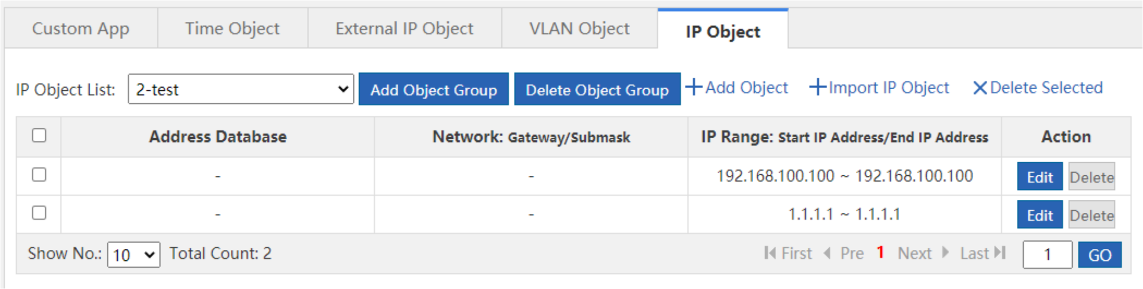
- **Delete a VLAN object**: Select the VLAN object you want to delete and then click Delete.

  For example, to delete the object vlan1, click Delete next to vlan1. To delete all VLAN objects, click ✕Delete All.

5.3.7 IP Object

Procedure

(1) Choose **Flow** > **Object** > **IP Object**.



IP Object List: 2-test

☐	Address Database	Network: Gateway/Submask	IP Range: Start IP Address/End IP Address	Action
☐	-	-	192.168.100.100 ~ 192.168.100.100	Edit Delete
☐	-	-	1.1.1.1 ~ 1.1.1.1	Edit Delete

Show No.: 10 Total Count: 2 First Pre 1 Next Last 1 GO

(2) Perform required operations as follows:

- Click **Import IP Object** to add multiple IP objects in batch through the configuration file.
- Add an IP object group: Click **Add Object Group**. In the window displayed, input the group ID and object group description, and object IP address, and then click OK.
- Delete an IP object group: Click Delete Object Group to directly delete the object group selected from the IP object list.
- Add an IP object: Click +Add Object to add an IP object to the IP group.
- Delete the selected IP object: Click ✕Delete Selected to delete the IP object selected in the table.
- Edit an IP object: Click Edit to edit the IP object.
- Delete an IP object: Click Delete to delete the IP object.

5.4 Behavior Policy

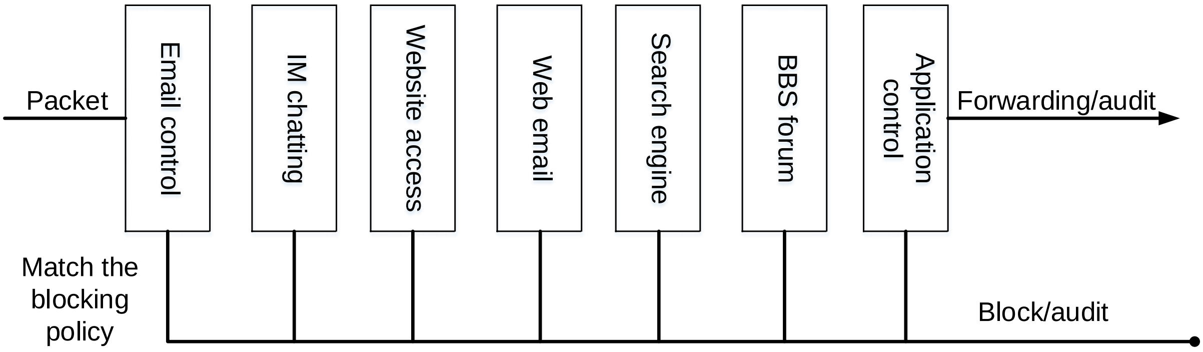
5.4.1 Introduction

The behavior policy module allows you to perform access audit, monitoring, and policy configuration for user behaviors. It can provide access audit information for users and allow the administrator to manage user behaviors, which can guide users to perform correct network behaviors and allocate the access time and block impact of bad information on users.

The policies for behavior management are matched in a certain order.

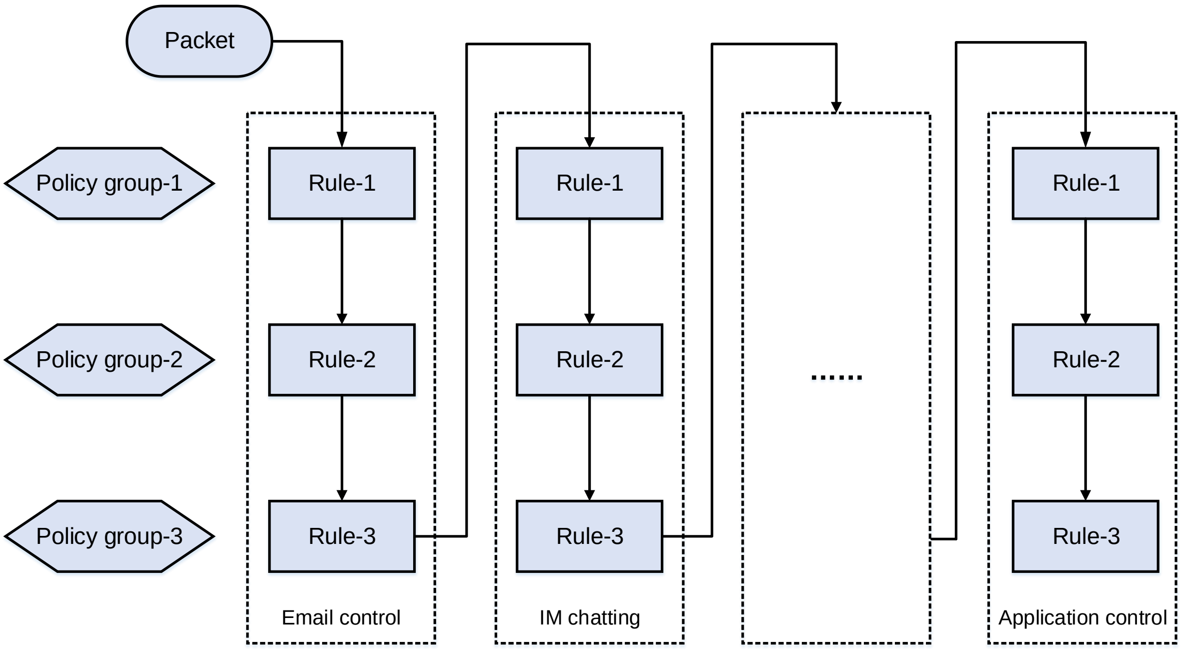
If the first type of behavior management service does not block the packets, the packets will be processed by the next behavior management service. If a packet is blocked by a behavior management service, the packet will not be processed by the next behavior management service. The following figure shows the processing sequence of behavior management services:

Figure 5-1 Processing sequence of behavior management services



The behavior policies are matched according to the priorities of the policy groups and rules.

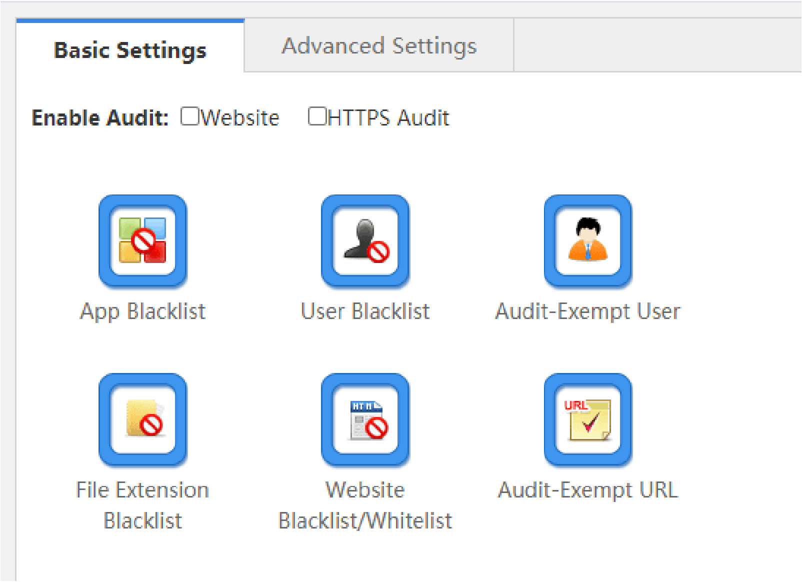
Figure 5-2 Priority-based policy and rule matching sequence



5.4.2 Basic Settings

Application Scenario

On the **Basic Settings** page, you can enable or disable the default audit function for website access, email sending/receiving, IM chatting, forum posting, and search engines. You can also perform special operations, such as direct filtering or audit exemption, for specific users, applications, websites, or file extensions.



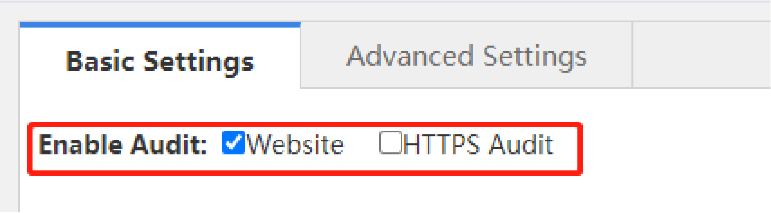
Enable Audit: □Website □HTTPS Audit

Procedure

(1) Choose **Behavior** > **Behavior Policy** > **Basic Settings**.

(2) Enable the default audit function.

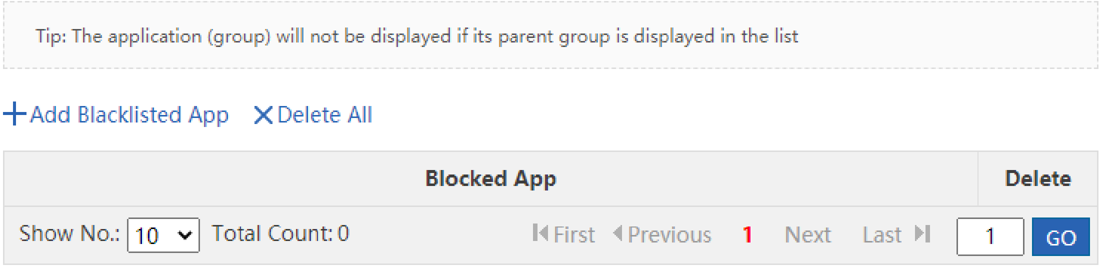
After the default audit function is enabled for a function, the device audits all network access records of this type.



Enable Audit: ☑Website □HTTPS Audit

(3) Application blacklist

Click App Blacklist and the following window is displayed, in which you can view which applications are blacklisted and blacklist an application or remove a blacklisted application from the blacklist.

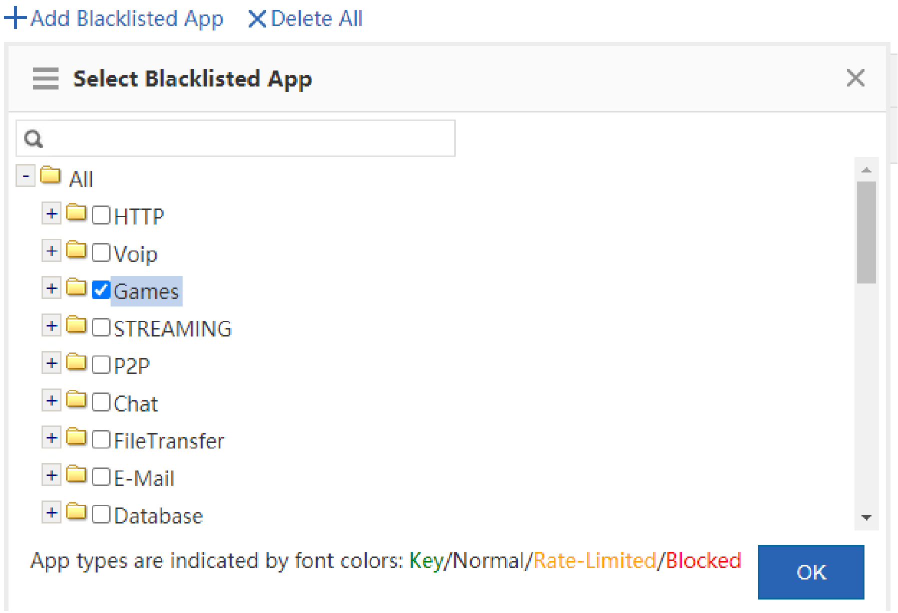


Tip: The application (group) will not be displayed if its parent group is displayed in the list

Blocked App	Delete

Show No.: 10 Total Count: 0

- Click +Add Blacklisted App . The following window is displayed:



+Add Blacklisted App ✕Delete All

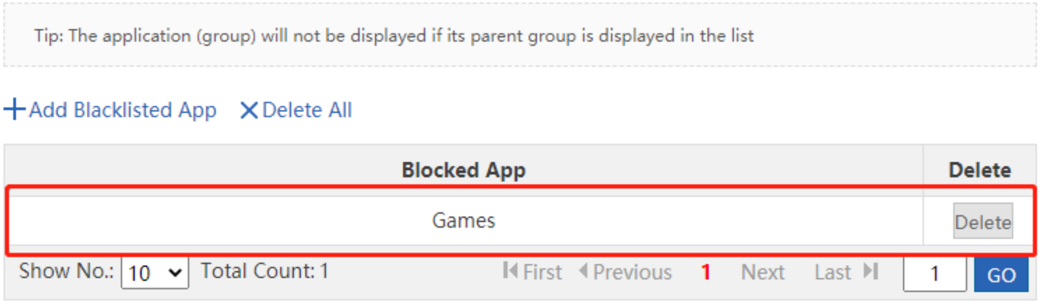
Select Blacklisted App ✕

- All
  - + □HTTP
  - + □Voip
  - + ☑Games
  - + □STREAMING
  - + □P2P
  - + □Chat
  - + □FileTransfer
  - + □E-Mail
  - + □Database

App types are indicated by font colors: Key/Normal/Rate-Limited/Blocked

OK

Select the application you want to blacklist, for example, Games, and then click OK. The selected application is blacklisted.



Tip: The application (group) will not be displayed if its parent group is displayed in the list

+Add Blacklisted App ✕Delete All

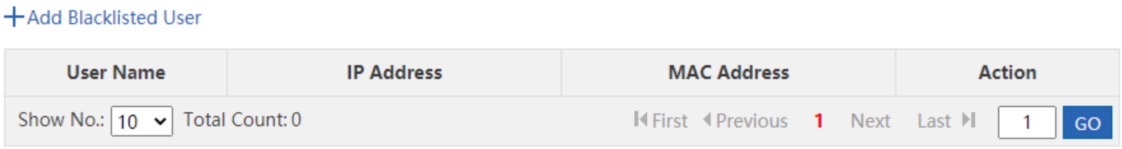
Blocked App	Delete
Games	Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

- Click Delete to remove a blacklisted application from the blacklist.
- Click ✕Delete All to remove all blacklisted applications from the blacklist.
- When an application blacklist is enabled, the device prohibits users from running applications in the blacklist.

(4) User blacklist

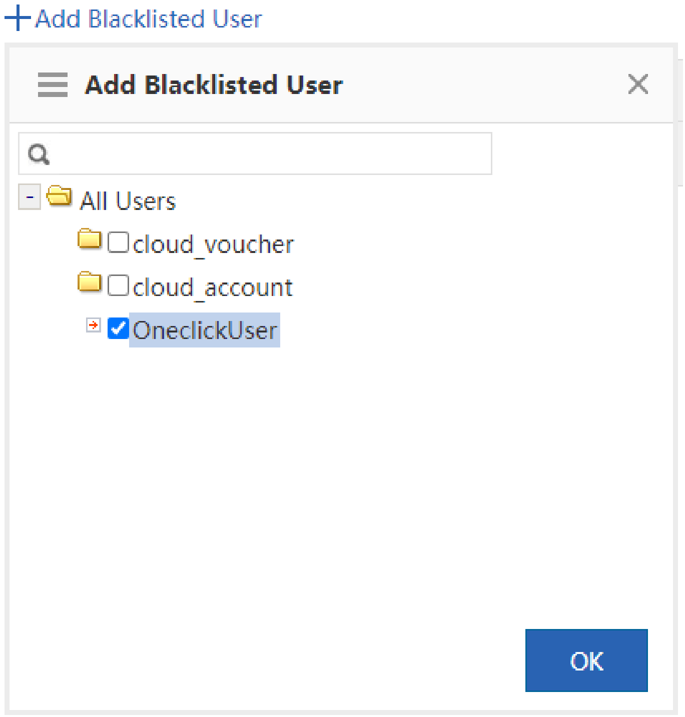
Click User Blacklist and the following window is displayed, in which you can view which users are blacklisted and blacklist a user or remove a blacklisted user from the blacklist.



+Add Blacklisted User

User Name	IP Address	MAC Address	Action
Show No.: 10 Total Count: 0			First Previous 1 Next Last 1 GO

- Click +Add Blacklisted User and the following window is displayed:



+Add Blacklisted User

Add Blacklisted User

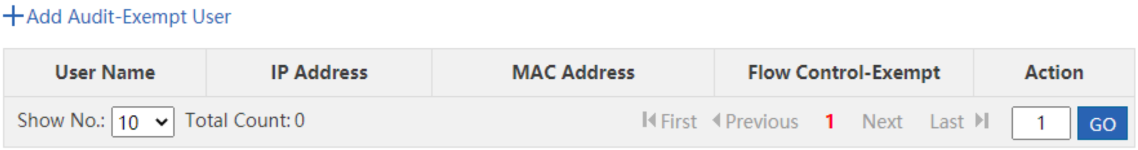
- All Users
  - ☐ cloud_voucher
  - ☐ cloud_account
  - ☑ OneclickUser

Select the user you want to blacklist and click OK. The selected user is added to the user blacklist.

- Click Delete to remove a user from the user blacklist.
- When a user blacklist is enabled, the device blocks the network access behaviors of users in the user blacklist.

(5) Configure an audit-exempt user.

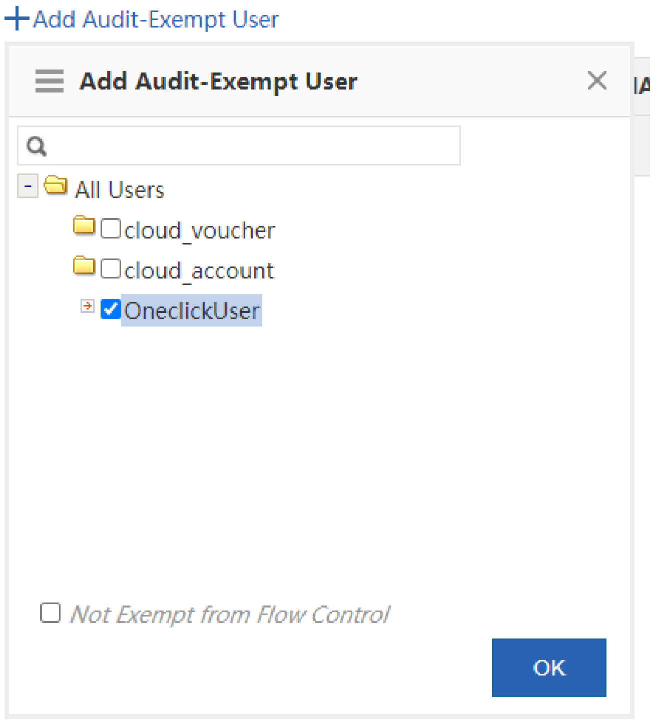
Click Audit-Exempt User and the following window is displayed, in which you can view which user devices are exempted from audit and add or delete an audit-exempt user.



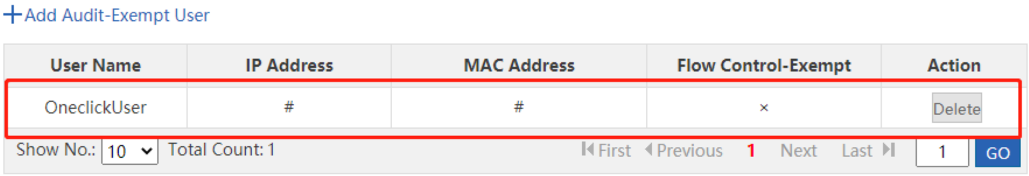
+Add Audit-Exempt User

User Name	IP Address	MAC Address	Flow Control-Exempt	Action
Show No.: 10 Total Count: 0				First Previous 1 Next Last 1 GO

- Click +Add Audit-Exempt User and the following window is displayed:



- Select a user that you want to exempt from audit. Flow control is not enabled for audit-exempt users by default. To enable flow control for all users, select ☑ *Not Exempt from Flow Control* and then click OK to add the user to the flow-control-exempt list.



+Add Audit-Exempt User

User Name	IP Address	MAC Address	Flow Control-Exempt	Action
OneclickUser	#	#	×	Delete

In the **Flow Control-Exempt** column, √ indicates that the user is exempted from flow control and × indicates that flow control is enabled for this user.

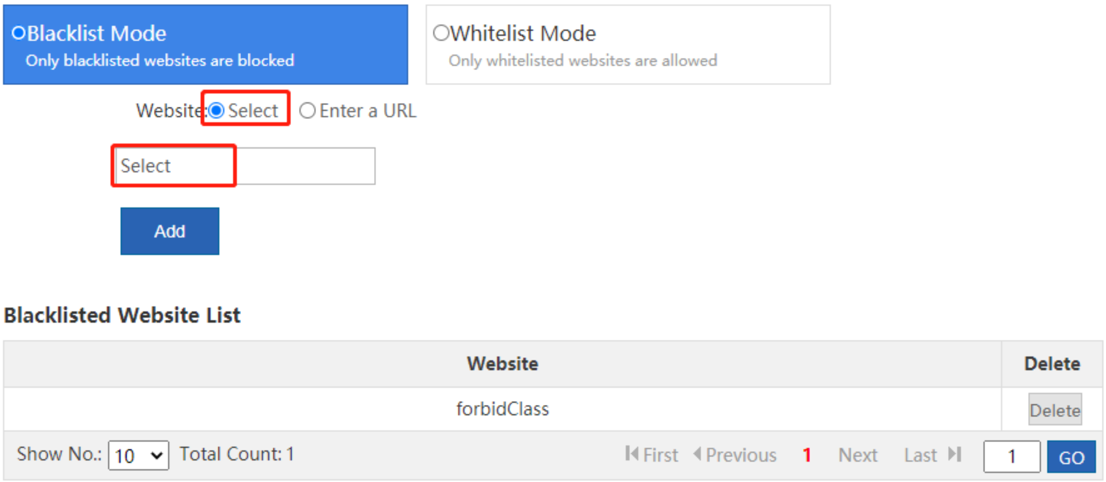
- Click Delete to remove a user from the flow-control-exempt list.
- The device does not audit the network access records of audit-exempt users. If **Not Exempt from Flow Control** is selected, the rate limiting rules in the flow control policy still apply to the audit-exempt users.

(6) Set a website blacklist.

Click Website Blacklist/Whitelist and the **Website Blacklist/Whitelist** window is displayed, in which you can view which websites are blacklisted and blacklist a website or remove a blacklisted website from the blacklist.

This function supports the blacklist mode and whitelist mode.

- Blacklist mode: Only websites in the blacklist are blocked by the device. Other websites are allowed to access.



○Blacklist Mode
Only blacklisted websites are blocked

○Whitelist Mode
Only whitelisted websites are allowed

Website: ● Select ○ Enter a URL

Select

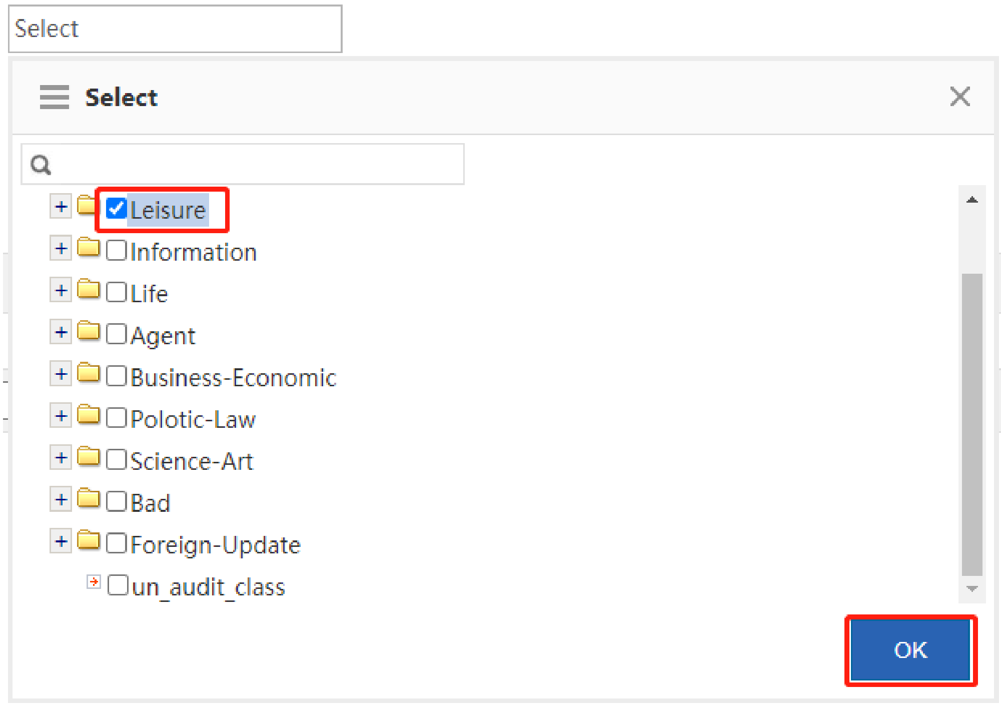
Blacklisted Website List

Website	Delete
forbidClass	Delete

Show No.: 10 Total Count: 1

- Add a website to the blacklist: You can select a URL from the available URLs or directly input a URL.

Select from available URLs: As shown in the figure above, check **Select** and then click in the text box. The following window is displayed, in which you need to select the URLs you want to blacklist, click OK, and then click Add.



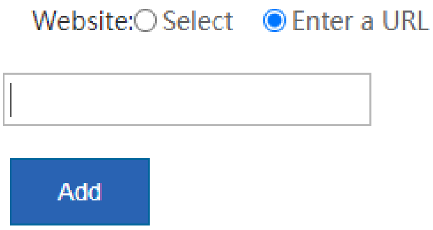
Select

☰ Select ✕

☑ Leisure
□ Information
□ Life
□ Agent
□ Business-Economic
□ Polotic-Law
□ Science-Art
□ Bad
□ Foreign-Update
□ un_audit_class

OK

Input a URL: As shown in the figure below, in the **Enter a URL** field, input a URL you want to blacklist and then click Add.

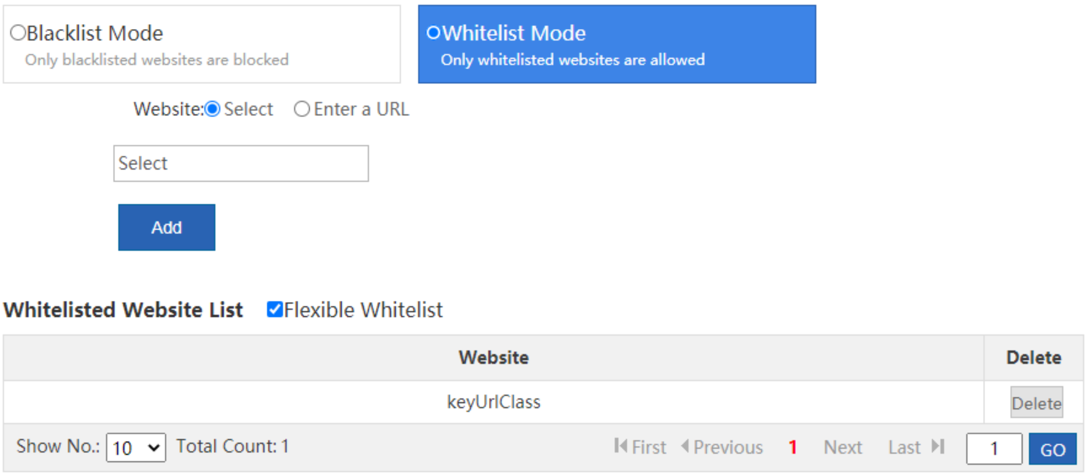


Website:○ Select ● Enter a URL

Add

- ○ Remove a website from the blacklist: Select the website you want to remove from the blacklist and then click Delete.

- Whitelist mode: Only websites in the whitelist can be accessed. Other websites are blocked by the device.



○Blacklist Mode
Only blacklisted websites are blocked

○Whitelist Mode
Only whitelisted websites are allowed

Website:● Select ○ Enter a URL

Select

Add

Whitelisted Website List ☑Flexible Whitelist

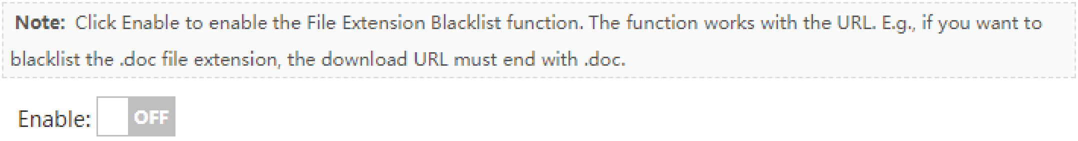
Website	Delete
keyUrlClass	Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

- Add a website to the whitelist: You can select a URL from the available URLs or directly input a URL. The operation is the same as that of adding a website to the blacklist and is omitted here.
- Remove a website from the whitelist: Select the website you want to remove from the whitelist and then click Delete .
- Flexible whitelist: Select ☑Flexible Whitelist . All URL requests initiated by whitelisted websites are allowed. For example, if www.ruijie.com.cn is a whitelisted website, all links on this website are allowed to access.

(7) Blacklisted file extensions.

Click File Extension Blacklist and the following window is displayed, in which you can view which file extensions are blocked by the device and blacklist a file extension or remove a blacklisted file extension from the blacklist.

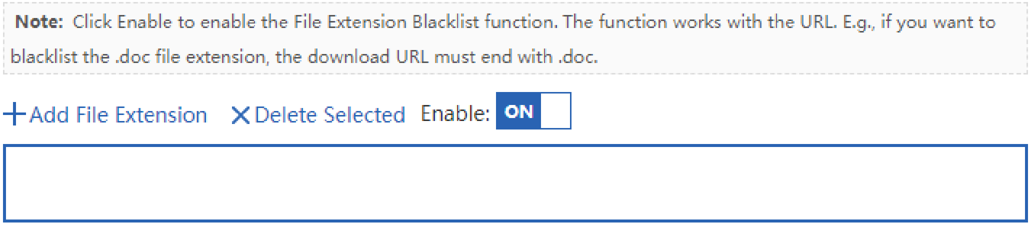


Note: Click Enable to enable the File Extension Blacklist function. The function works with the URL. E.g., if you want to blacklist the .doc file extension, the download URL must end with .doc.

Enable: OFF

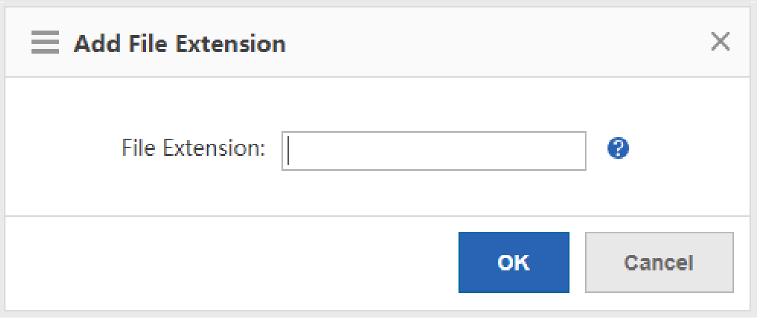
- Click Enable: OFF to enable the file extension blacklist function.

When this function is enabled, the device does not allow you to upload or download files of the blacklisted extension.



Note: Click Enable to enable the File Extension Blacklist function. The function works with the URL. E.g., if you want to blacklist the .doc file extension, the download URL must end with .doc.

- Click +Add File Extension to add the file extension names you want to blacklist. Separate multiple extension names by commas (,).

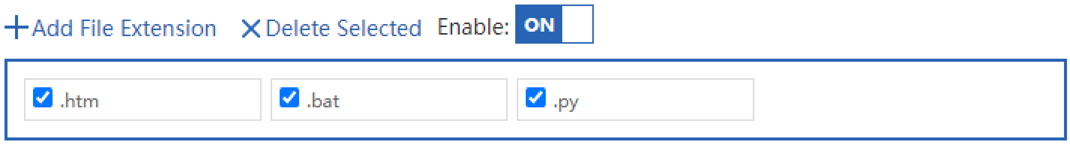


Add File Extension

File Extension: [ ]

OK Cancel

Input the file extension name you want to blacklist and click OK. The file extension name is added to the blacklist.



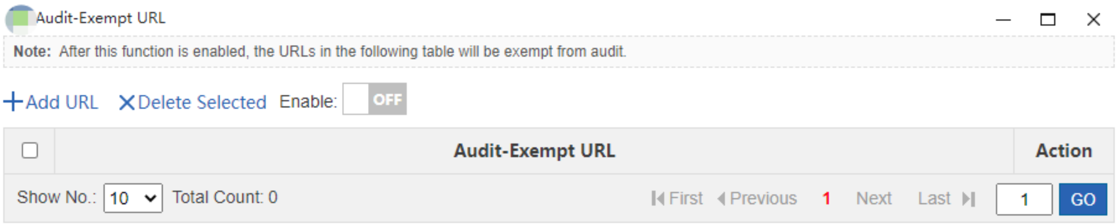
+Add File Extension ✕Delete Selected Enable: ON

☑ .htm ☑ .bat ☑ .py

- Click ✕ Delete Selected to remove the deselected file extensions from the blacklist.

(8) Audit-exempt URL

Click Audit-Exempt URL and the following window is displayed, in which you can view which URLs are exempted from audit and add or delete an audit-exempt URL.



Audit-Exempt URL

Note: After this function is enabled, the URLs in the following table will be exempt from audit.

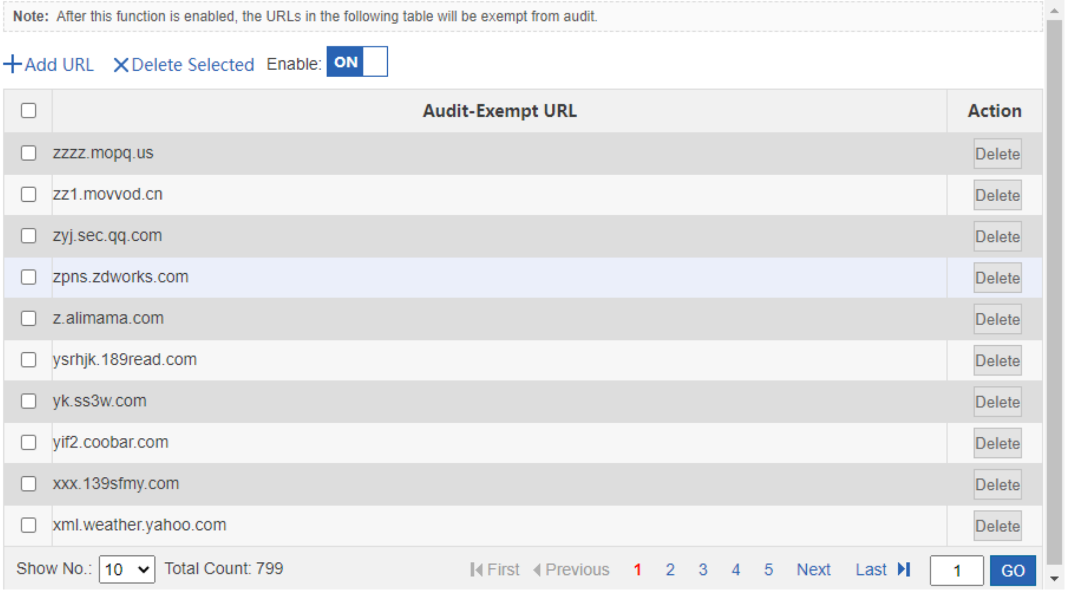
+Add URL ✕Delete Selected Enable: OFF

□	Audit-Exempt URL	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

- Select Enable: ON to enable the audit-exempt URL function:

  After this function is enabled, accesses to these URLs are neither audited nor blocked by the device.



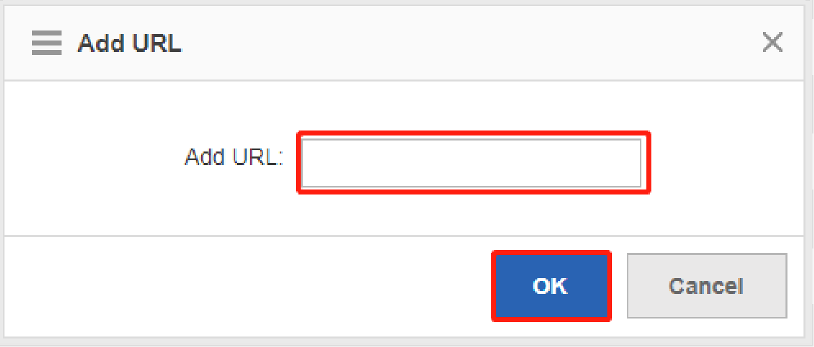
Note: After this function is enabled, the URLs in the following table will be exempt from audit.

+Add URL ✕Delete Selected Enable: ON

□	Audit-Exempt URL	Action
□	zzzz.mopq.us	Delete
□	zz1.movvod.cn	Delete
□	zyj.sec.qq.com	Delete
□	zpns.zdworks.com	Delete
□	z.alimama.com	Delete
□	ysrhjk.189read.com	Delete
□	yk.ss3w.com	Delete
□	yif2.coobar.com	Delete
□	xxx.139sfmy.com	Delete
□	xml.weather.yahoo.com	Delete

Show No.: 10 Total Count: 799 First Previous 1 2 3 4 5 Next Last 1 GO

- Click +Add URL. In the window displayed, input a URL you want to exempt from audit, and click **OK**. The URL is added to the audit-exempt URL list.



Add URL

Add URL:

OK Cancel

- Click Delete to delete a URL from the audit-exempt URL list.
- Click ✕Delete Selected to delete URLs in batch from the audit-exempt URL list.

5.4.3 Advanced Settings

Application Scenario

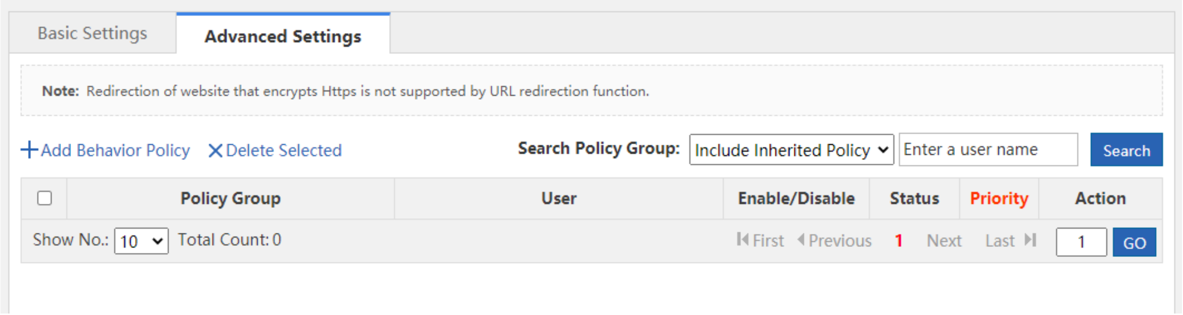
Internet-based information transmission has been a key application for enterprises and institutions. However, problems such as information confidentiality, health, and political correctness must be concerned.

Ruijie NBRs provide brand-new refined information sending/receiving monitoring and audit functions, helping you effectively control the transmission scope of key information and avoid possible legal risks.

Ruijie NBRs allow you to monitor information transmission channels, such as email, webmail, BBS, IM, Web-SEARCH, FTP, Telnet, and web pages. For example, you can audit content of emails, chatting, and posts.

Procedure

(1) Choose **Behavior** > **Behavior Policy** > **Advanced Settings**.



Note: Redirection of website that encrypts Https is not supported by URL redirection function.

Search Policy Group: Include Inherited Policy | Enter a user name

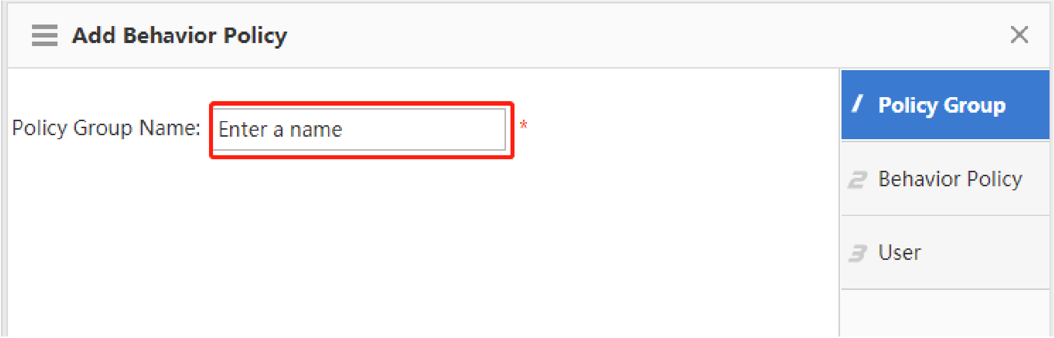
☐	Policy Group	User	Enable/Disable	Status	Priority	Action

Show No.: 10 Total Count: 0

On this page, you can manage and configure application control policies and website access policies.

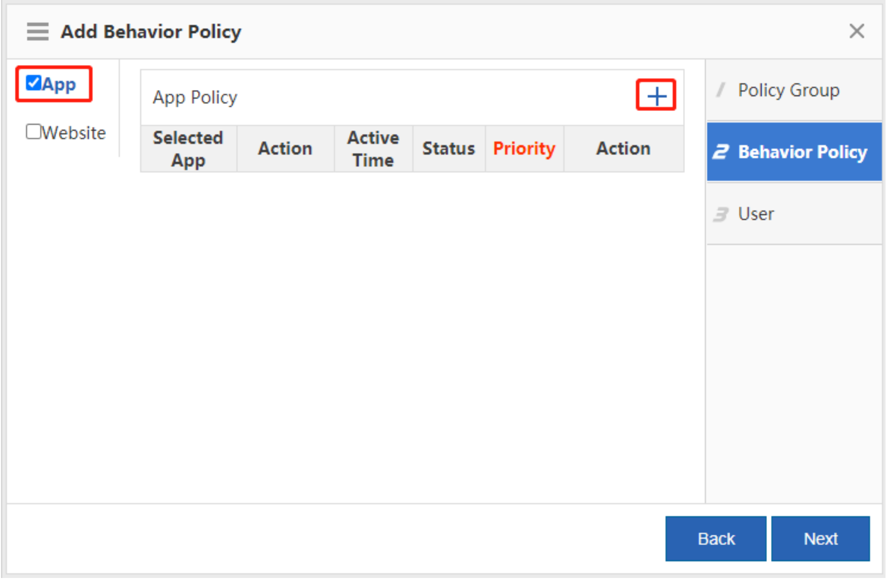
(2) Click +Add Behavior Policy and the **Add Behavior Policy** window is displayed.

a Policy group name: In the **Policy Group Name** field, input a name for the policy that can clearly indicate the policy rules or usage, and then click **Next**.



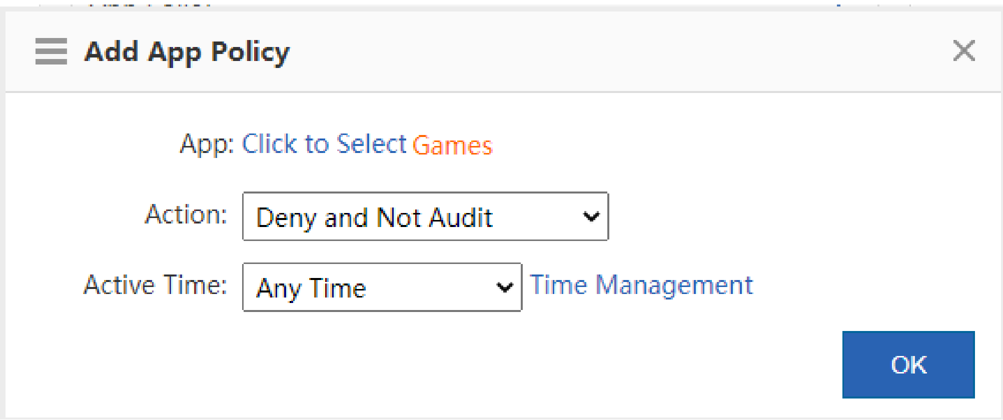
Policy Group Name: Enter a name *

b Behavior control: Select behavior rules you want to apply to this policy. You can select multiple behavior rules at a time. The page is as follows:



Selected App	Action	Active Time	Status	Priority	Action

Click a rule name on the left to view all rules under this policy. To edit a rule, select the check box ☑App before the policy and then edit, delete, or add rules. Then, click **Next**. For the addition page of each type, see the sections below.



Add App Policy

App: Click to Select Games

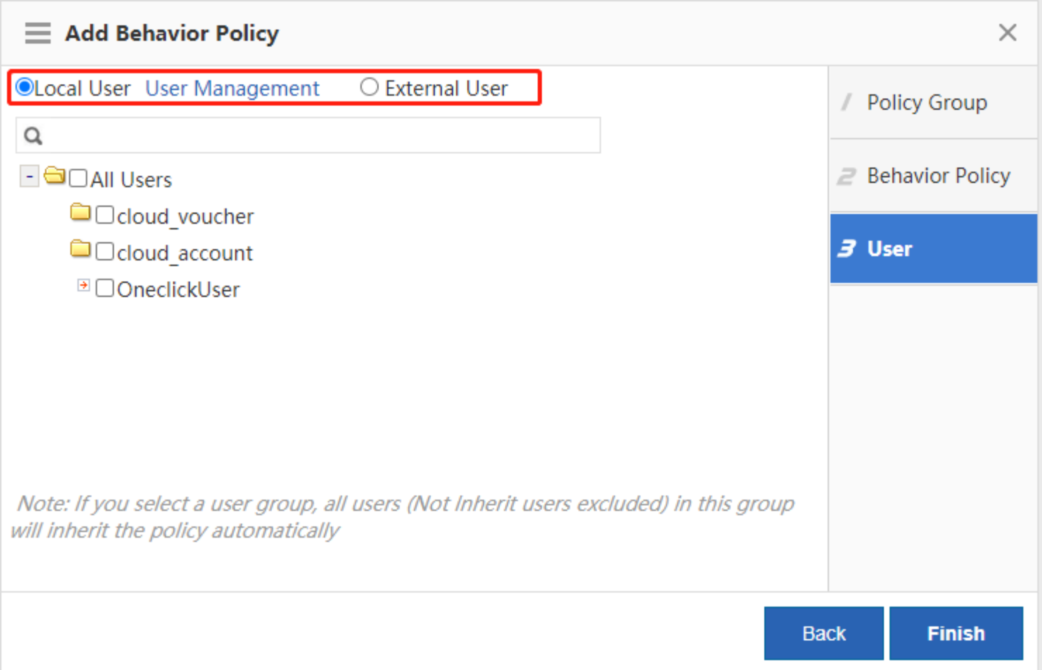
Action: Deny and Not Audit

Active Time: Any Time

Control rule description:

- **Allow and Audit**: The device does not block network access behaviors of the selected user but will record the network access information.
- **Allow and Not Audit**: The device neither blocks network access behaviors of the selected user nor records the network access information.
- **Deny and Audit**: The device blocks network access behaviors of the selected user and records the blocked access request information.
- **Deny and Not Audit**: The device blocks network access behaviors of the selected user but does not record the blocked access request information.
- **Active Time**: Specify the active time for the rule. The rule is active only within the active time.

c Associated user: Select users (either local or external) to which the policy is applied. An external user is a user that passes third-party login authentication, such as an authenticated VPN user or web user.



Add Behavior Policy

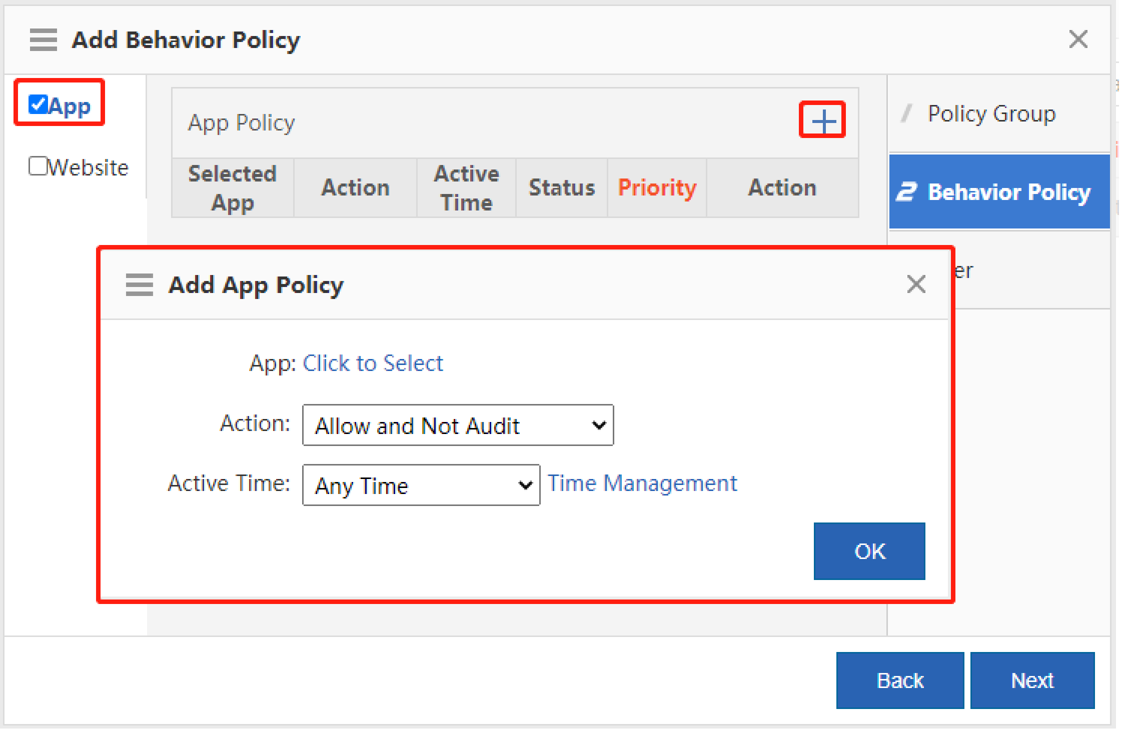
● Local User User Management ○ External User

□ All Users
□ cloud_voucher
□ cloud_account
□ OneclickUser

Note: If you select a user group, all users (Not Inherit users excluded) in this group will inherit the policy automatically

(3) Application control.

This function allows you to monitor the network behaviors of applications, release or block data streams of relevant applications as needed, and audit the control behaviors. You can create an application control policy as follows:



Add Behavior Policy

☑App

□Website

App Policy

Selected App	Action	Active Time	Status	Priority	Action

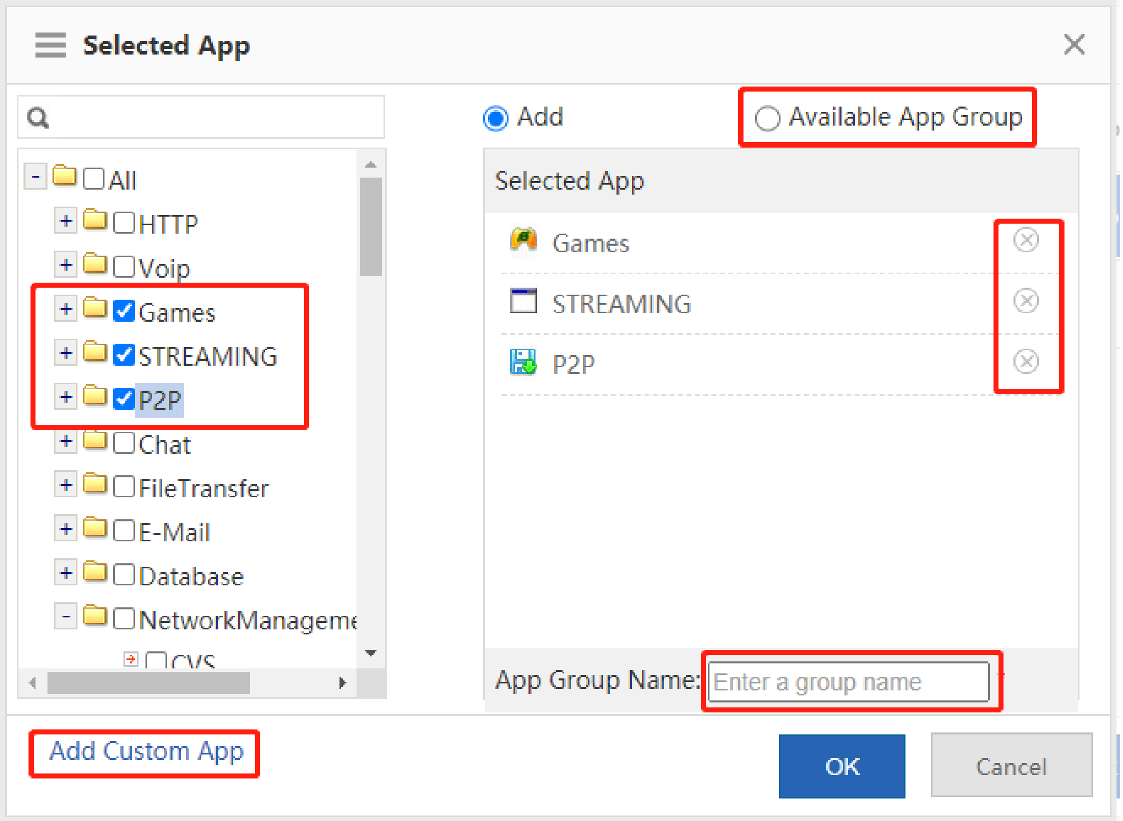
Add App Policy

App: Click to Select

Action: Allow and Not Audit

Active Time: Any Time Time Management

Click **Click to Select** and the following page is displayed:



Selected App

□All
□HTTP
□Voip
☑Games
☑STREAMING
☑P2P
□Chat
□FileTransfer
□E-Mail
□Database
□NetworkManageme
□CVS

● Add ○ Available App Group

Selected App

Games
STREAMING
P2P

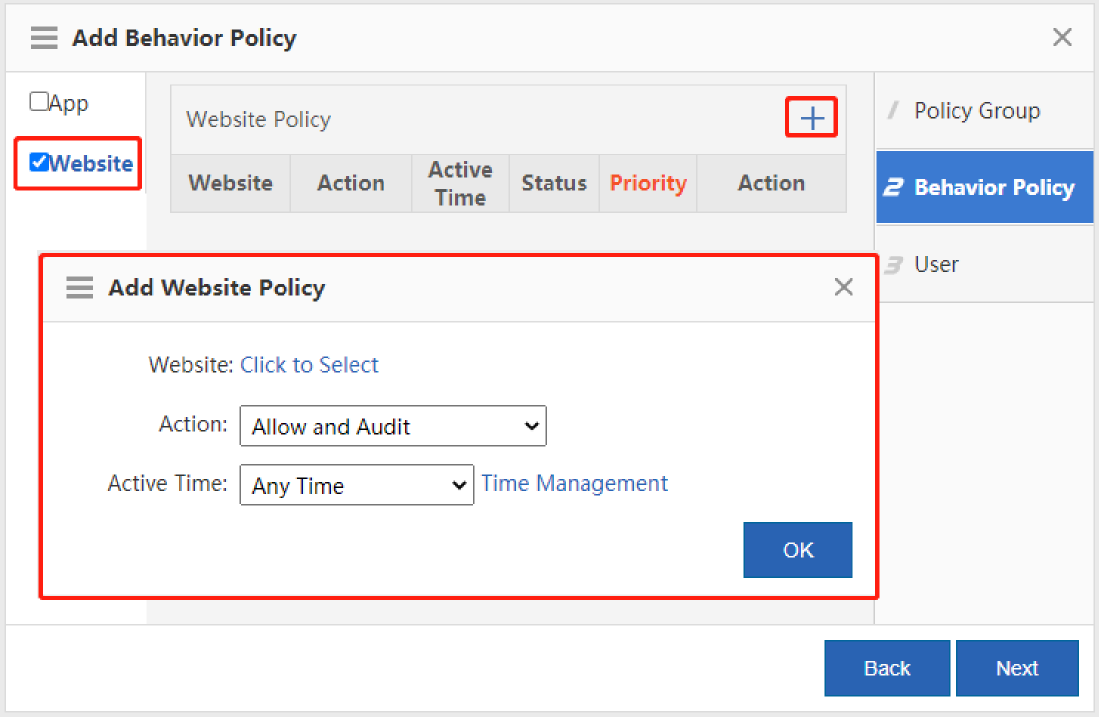
App Group Name: Enter a group name

From the left application list, select the applications you want to control or click Add Custom App to customize applications. You can create an application group or click ○ Available App Group to select one from available application groups. To create an application group, select applications you want to control, input a name for the group in the **App Group Name** field, and then click **OK**.

Click ⊗ to delete a selected application.

(4) Website access policy.

This function allows you to monitor accesses to URLs, classify and audit all URL access requests initiated by the internal network, and block or release the URL access requests as needed. The configuration page is as follows:



Add Behavior Policy

☐App

☑Website

Website Policy

Website	Action	Active Time	Status	Priority	Action

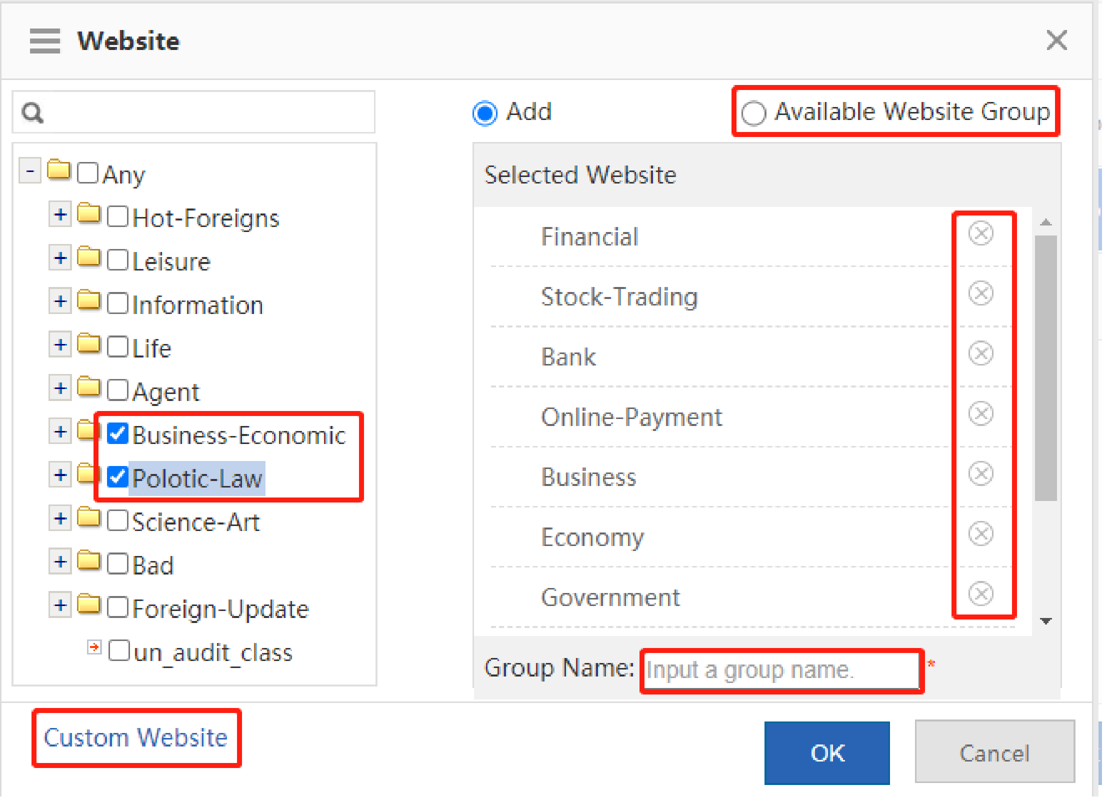
Add Website Policy

Website: Click to Select

Action: Allow and Audit

Active Time: Any Time Time Management

Click **Click to Select** and the following page is displayed:



The tree on the left shows the structure of URL categories of the current system. You can select a URL category from the tree as the monitoring object. If no URL is selected, all URLs are used by default.

Click Custom Website to customize a website. You can create a website group or click ○ Available Website Group to select one from available website groups. To create a website group, select the websites you want to control, input a name for the group in the **Group Name** field, and then click **OK**.

Click ⊗ to delete a selected website.

5.5 Realtime Audit

Application Scenario

This page allows you to make statistics on the audit records of user traffic.

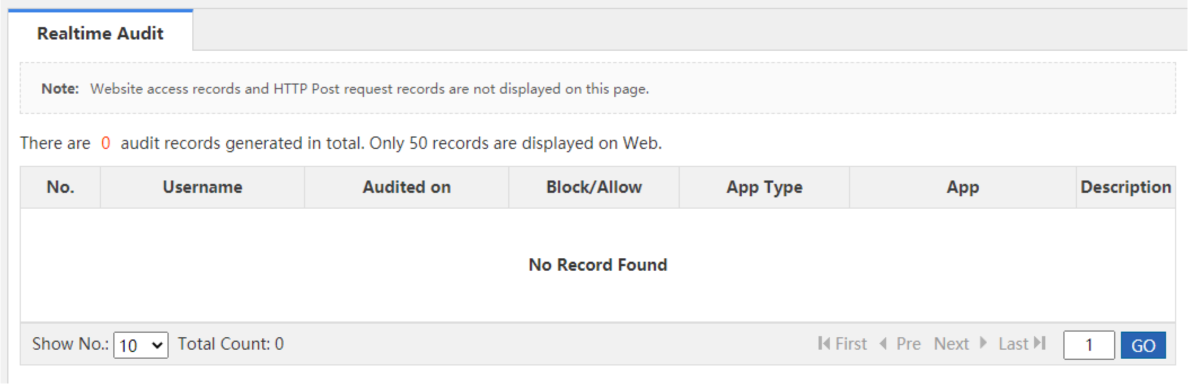
Note

Considering the large number of website access records and external transmission records, the page does not display these two audit records.

Procedure

(1) Choose **Behavior** > **Realtime Audit**.

(2) View detailed audit records.



Note: Website access records and HTTP Post request records are not displayed on this page.

There are 0 audit records generated in total. Only 50 records are displayed on Web.

No.	Username	Audited on	Block/Allow	App Type	App	Description
No Record Found						

Show No.: 10 Total Count: 0

6 Security Authentication

6.1 User Organization

6.1.1 User management

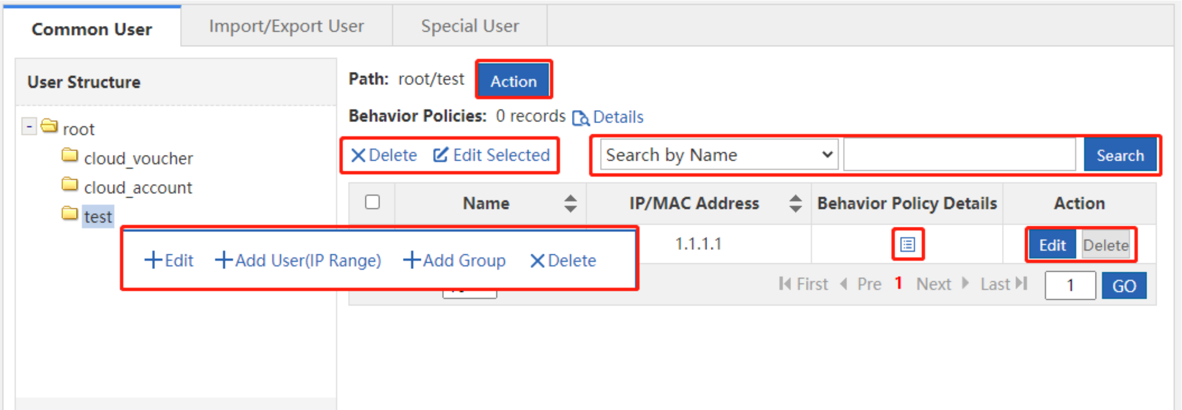
Application Scenario

Users on the device can be either internal users or authenticated web users or VPN users.

One user can log in to a VPN and be used for web authentication. For example, a user named Lisan is configured under the financial department. VPN and web authentication is enabled for this user and the computer IP address assigned for Lisan is bound to his account. In this way, Lisan's network behaviors can be audited and controlled no matter Lisan logs in to his account from the company's network or from a web or VPN. VPN here refers to PPTP, L2TP, or SSLVPN.

Procedure

(1) Choose **User** > **User** > **Common User**.



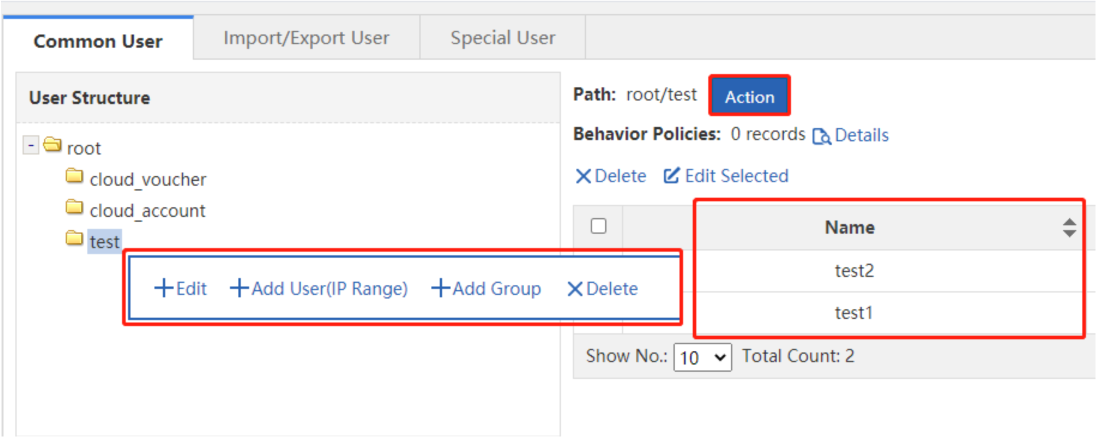
Path: root/test

Behavior Policies: 0 records

□	Name	IP/MAC Address	Behavior Policy Details	Action
		1.1.1.1		Edit Delete

(2) The tree on the left is the structure of all users of the current system. After you select a user group, information about this object is displayed on the right. You can edit or modify the object information.

To modify a user or user group, click the corresponding user group. The following page is displayed.



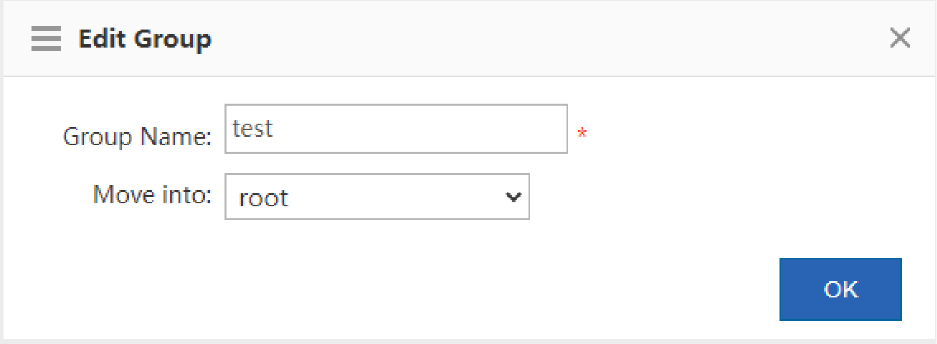
Path: root/test

Behavior Policies: 0 records

□	Name
	test2
	test1

Show No.: 10 Total Count: 2

- Click +Edit to edit the selected user group, as shown below:



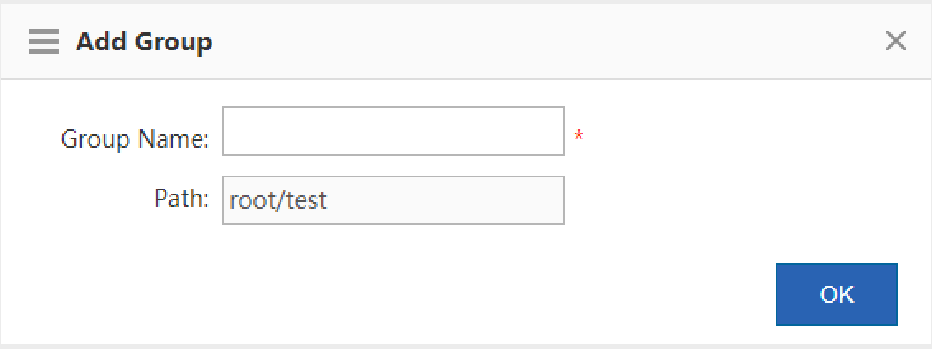
Edit Group

Group Name: test *

Move into: root

You can modify the user group name and move a user to another user group.

- Click +Add Group to add a user sub-group to the selected user group, as shown below:



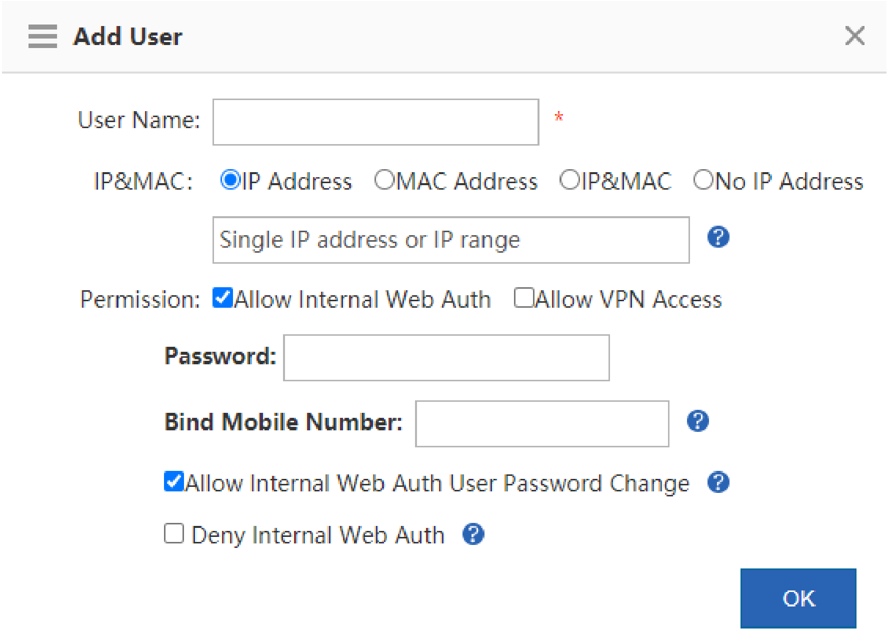
Add Group

Group Name: *

Path: root/test

The user group name can contain up to 31 English characters. One Chinese character equals two English characters.

- Click ✕Delete to delete the selected user group from the user tree. All users in this user group are also deleted.
- Click +Add User(IP Range) to create a user or IP range under the selected user group.



Add User ✕

User Name: ______ *

IP&MAC: ● IP Address ○ MAC Address ○ IP&MAC ○ No IP Address

Single IP address or IP range ?

Permission: ☑ Allow Internal Web Auth □ Allow VPN Access

Password: ______

Bind Mobile Number: ______ ?

☑ Allow Internal Web Auth User Password Change ?

□ Deny Internal Web Auth ?

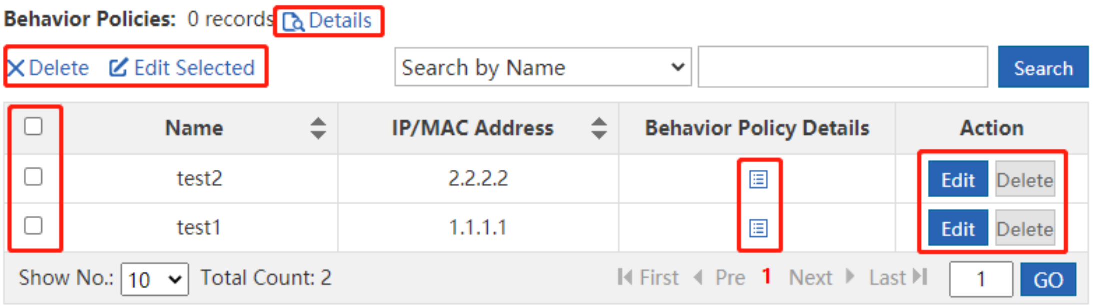
OK

- **User Name**: The name of this user, which is used for VPN login or web authentication.
- **Permission**: Indicate whether this user name and password can be used for web authentication or VPN login. If yes, you must set a password; otherwise, login may fail.
- **Password**: The password used for web authentication or VPN login.
- **Allow Internal Web Auth User Password Change**: This item is displayed only after you select **Allow Internal Web Auth**. It indicates whether to allow users to modify the password after web authentication is passed.
- **Deny Internal Web Auth**: This item is displayed only after selecting **Allow Internal Web Auth**. In this mode, users can only access internal network resources and cannot access external networks even after web authentication is passed.
- **IP Address and MAC Address**: The IP address or MAC address of the user. You can configure an IP address range or configure both an IP address and a MAC address. To configure an IP address range, separate IP addresses by "-".
- **Auth Mode**: Options are **Single Direction Bind** and **Dual Direction Bind**. This item is available only after selecting **Allow Internal Web Auth**. **Dual Direction Bind** means that, in real time authentication mode, the user name can only use the specified address to access networks and the specified address can only be used by this user. **Single Direction Bind** means that, in real-time authentication mode, the user name can only use the specified address to access networks but the specified address can be used by other users.

Note

You can also click Action to add or delete a user group or add a user.

(3) You can perform operations in the following figure on the user list of a user group.



Behavior Policies: 0 records Details

Delete Edit Selected

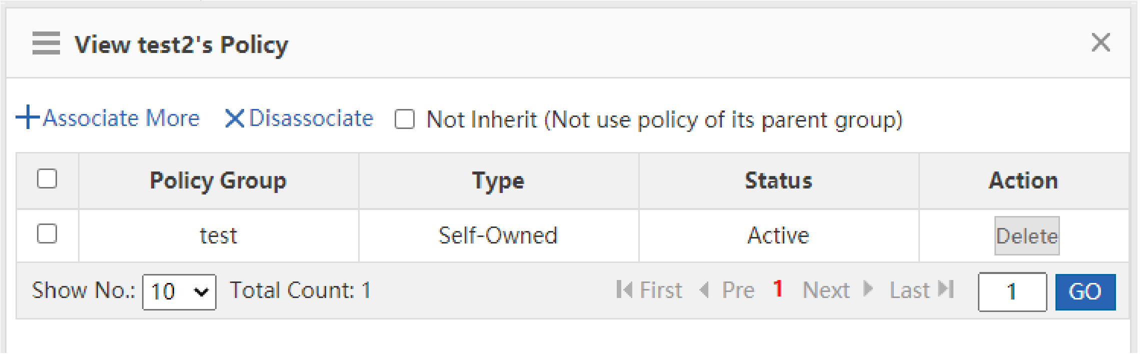
Search by Name Search

□	Name	IP/MAC Address	Behavior Policy Details	Action
□	test2	2.2.2.2	☰	Edit Delete
□	test1	1.1.1.1	☰	Edit Delete

Show No.: 10 Total Count: 2 First Pre 1 Next Last 1 GO

The table above shows all the users of the user group you have selected from the left tree. You can edit or delete users.

- Click ☰ or Details . The action policy associated with the user or user group is displayed, as shown below:



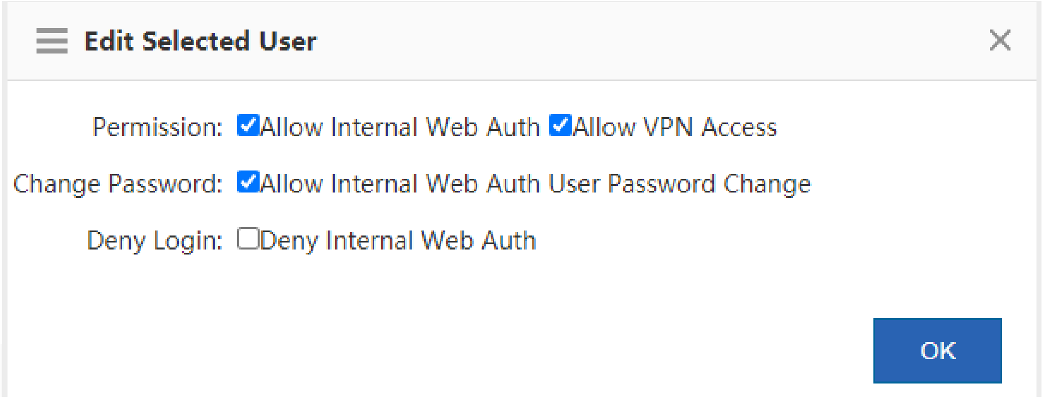
View test2's Policy

+Associate More Disassociate □ Not Inherit (Not use policy of its parent group)

□	Policy Group	Type	Status	Action
□	test	Self-Owned	Active	Delete

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 GO

- The device allows you to edit users in batch: Select users you want to edit and then click Delete Edit Selected to delete or edit users in batch. The edition page is shown below:



Edit Selected User

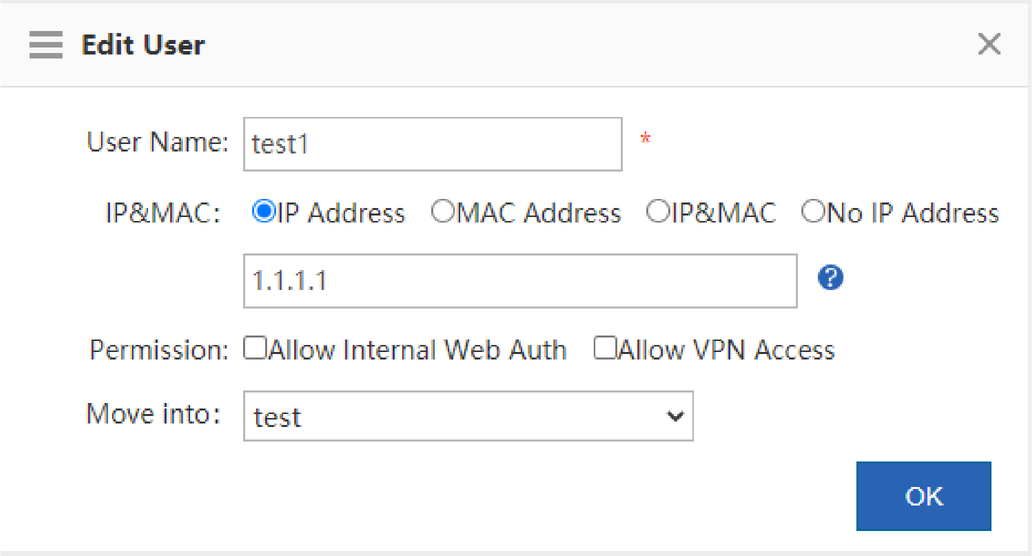
Permission: ☑Allow Internal Web Auth ☑Allow VPN Access

Change Password: ☑Allow Internal Web Auth User Password Change

Deny Login: □Deny Internal Web Auth

OK

- Click Edit to edit user parameters. For the function of each parameter, see the section **Add User**.



Edit User

User Name: test1 *

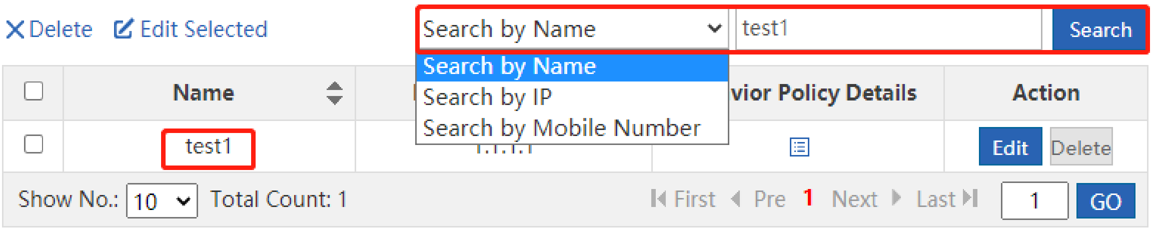
IP&MAC: ● IP Address ○ MAC Address ○ IP&MAC ○ No IP Address

1.1.1.1

Permission: □ Allow Internal Web Auth □ Allow VPN Access

Move into: test

- In the search box, input user name or IP address. The query results are displayed in the table below.



Search by Name: test1

□	Name		vior Policy Details	Action
□	test1	1.1.1.1	☰	Edit Delete

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 GO

6.1.2 Import and Export Users

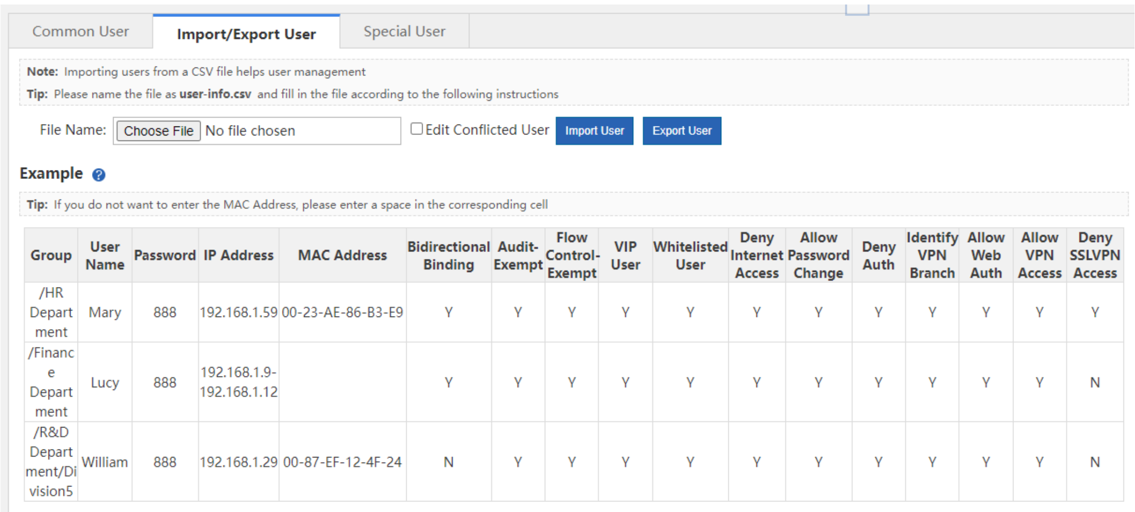
Application Scenario

This function allows you to:

- Export user configurations existing in the system.
- Import user configurations in batch based on a template.

Procedure

(1) Choose **User** > **User** > **Import/Export User**.



Note: Importing users from a CSV file helps user management

Tip: Please name the file as **user-info.csv** and fill in the file according to the following instructions

File Name: Choose File No file chosen ☐Edit Conflicted User Import User Export User

Example

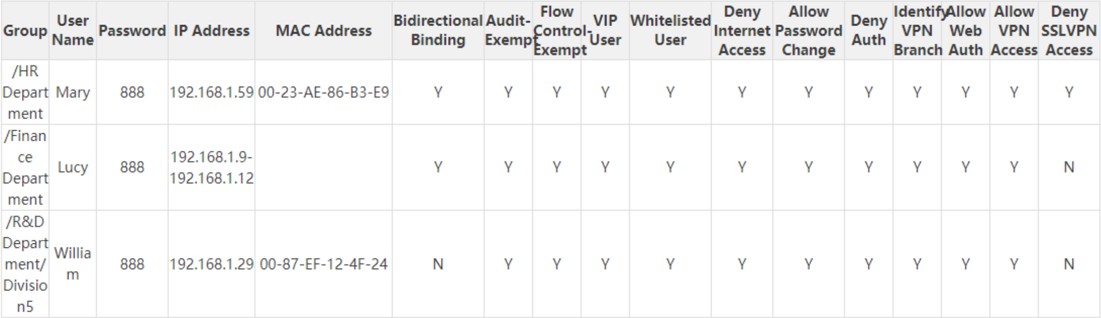
Tip: If you do not want to enter the MAC Address, please enter a space in the corresponding cell

Group	User Name	Password	IP Address	MAC Address	Bidirectional Binding	Audit-Exempt	Flow Control-Exempt	VIP User	Whitelisted User	Deny Internet Access	Allow Password Change	Deny Auth	Identify VPN Branch	Allow Web Auth	Allow VPN Access	Deny SSLVPN Access
/HR Department	Mary	888	192.168.1.59	00-23-AE-86-B3-E9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
/Finance Department	Lucy	888	192.168.1.9-192.168.1.12		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
/R&D Department/Division5	William	888	192.168.1.29	00-87-EF-12-4F-24	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N

(2) Import users.

You can import users from a file to help the administrator edit users in one click.

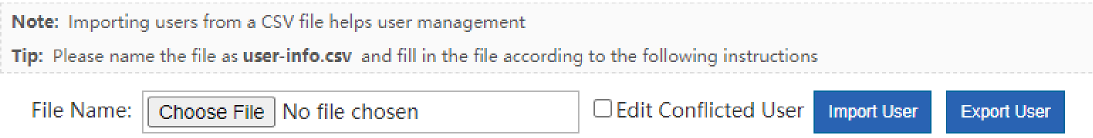
a Create a table named **user-info.csv** on a local PC, and input the user information according to the following format in the table:



Group	User Name	Password	IP Address	MAC Address	Bidirectional Binding	Audit-Exempt	Flow Control-Exempt	VIP User	Whitelisted User	Deny Internet Access	Allow Password Change	Deny Auth	Identify VPN Branch	Allow Web Auth	Allow VPN Access	Deny SSLVPN Access
/HR Department	Mary	888	192.168.1.59	00-23-AE-86-B3-E9	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
/Finance Department	Lucy	888	192.168.1.9-192.168.1.12		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
/R&D Department/Division5	William	888	192.168.1.29	00-87-EF-12-4F-24	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N

b Click Choose File and import the file **user-info.csv**.

c Click Import User. An import progress bar is displayed. When the progress bar is loaded completely, the file is uploaded.



Note: Importing users from a CSV file helps user management

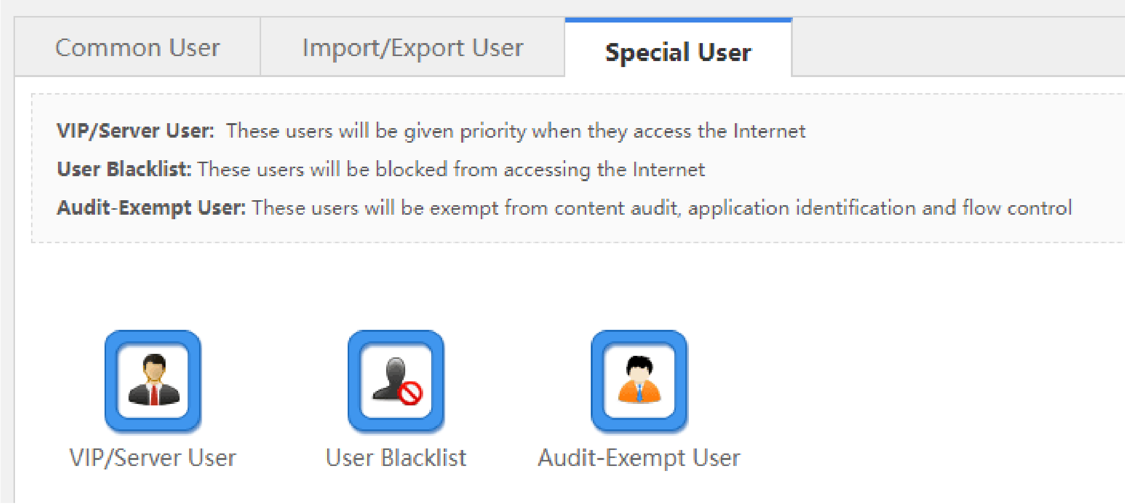
Tip: Please name the file as **user-info.csv** and fill in the file according to the following instructions

File Name: Choose File No file chosen ☐Edit Conflicted User Import User Export User

(3) Export users. Click Export User. In the **Save** dialog box displayed, save the file **user-info.csv** to a local PC.

6.1.3 Special User Management

Special users include VIP/server users, blacklisted users, and audit-exempt users.

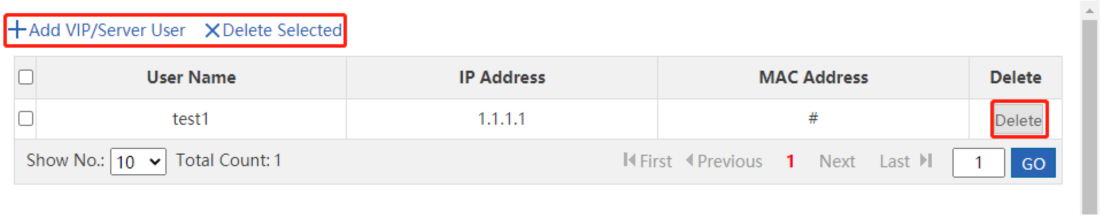


VIP/Server User: These users will be given priority when they access the Internet

User Blacklist: These users will be blocked from accessing the Internet

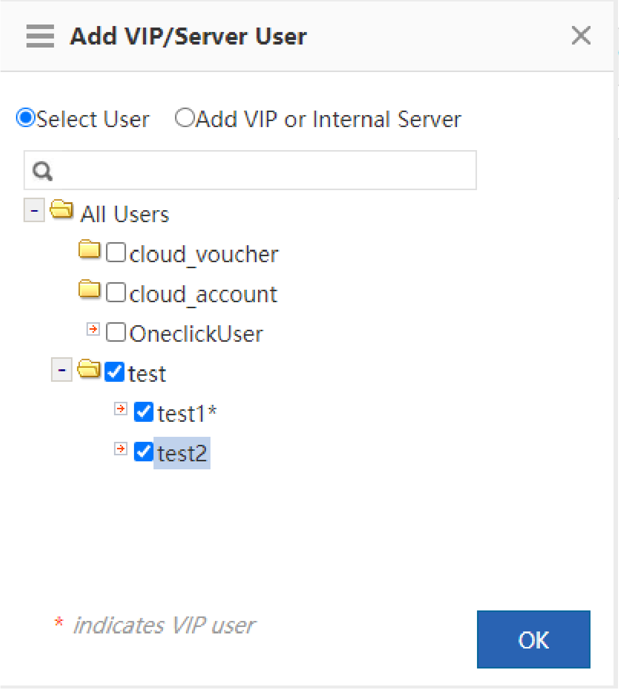
Audit-Exempt User: These users will be exempt from content audit, application identification and flow control

- **VIP/Server User**: These users are key users or internal network servers that need to be protected. These users will be given priority when they access the network. Click VIP/Server User . The VIP/server user configuration window is displayed, in which you can add or delete a VIP/server user.



□	User Name	IP Address	MAC Address	Delete
□	test1	1.1.1.1	#	Delete

  - Click +Add VIP/Server User to add a VIP/server user. You can also check **Select User** and select users in the tree, or select **Add VIP or Internal Server**, and then manually input the user name and IP address.



Add VIP/Server User

● Select User ○ Add VIP or Internal Server

- All Users
  - □ cloud_voucher
  - □ cloud_account
  - □ OneclickUser
  - ☑ test
    - ☑ test1*
    - ☑ test2

* indicates VIP user

- **User Blacklist:** These users are blacklisted. To block all network access behaviors of a user, you can add this user to the blacklist. Click User Blacklist and the user blacklist configuration window is displayed, in which you can add or remove a user to or from the blacklist. For details, see the section 5.4.2 (4) User blacklist.
- **Audit-Exempt User**: These users are users exempted from traffic audit or flow control. For example, a boss does not want his/her network access behaviors audited, and then you can set this boss as an audit-exempt user. Click Audit-Exempt User and the audit-exempt user configuration window is displayed, in which you can add or delete an audit-exempt user. For details, see the section 5.4.2 (5) Configure an audit-exempt user.

6.1.4 Block Internet Access

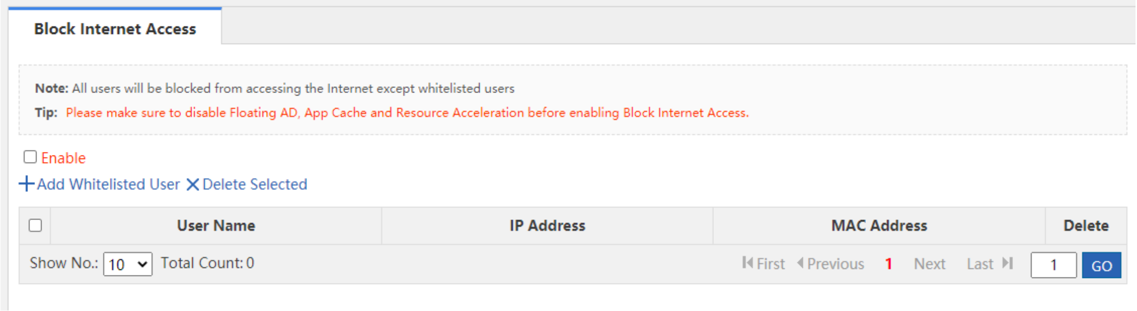
Application Scenario

After **Block Internet Access** is enabled, all users of an internal network cannot access the Internet.

You can add a user to a whitelist so that this user can access the Internet.

Procedure

(1) Choose **User** > **Block Internet Access**.



Block Internet Access

Note: All users will be blocked from accessing the Internet except whitelisted users

Tip: Please make sure to disable Floating AD, App Cache and Resource Acceleration before enabling Block Internet Access.

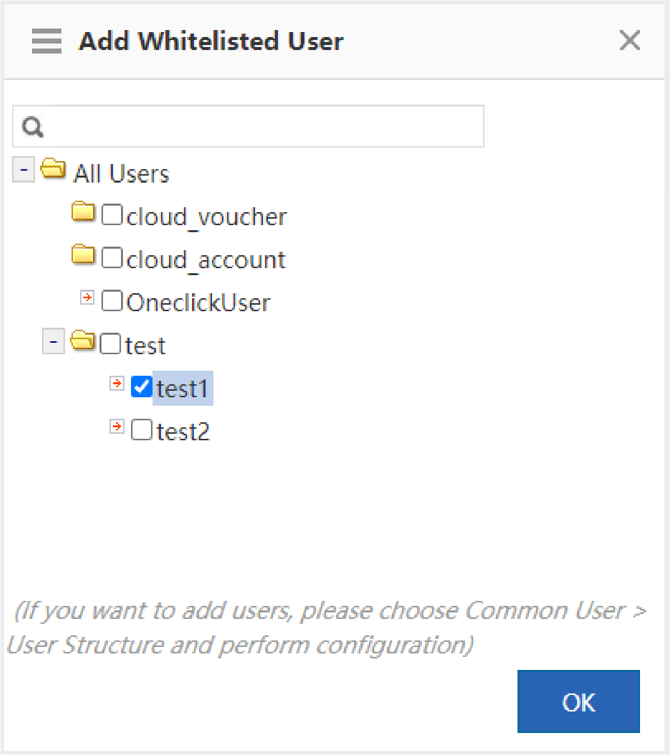
☐ Enable

+Add Whitelisted User ✕Delete Selected

☐	User Name	IP Address	MAC Address	Delete

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

(2) Click +Add Whitelisted User to add at least one user to a whitelist and select ☐ Enable to enable **Block Internet Access**.



Add Whitelisted User

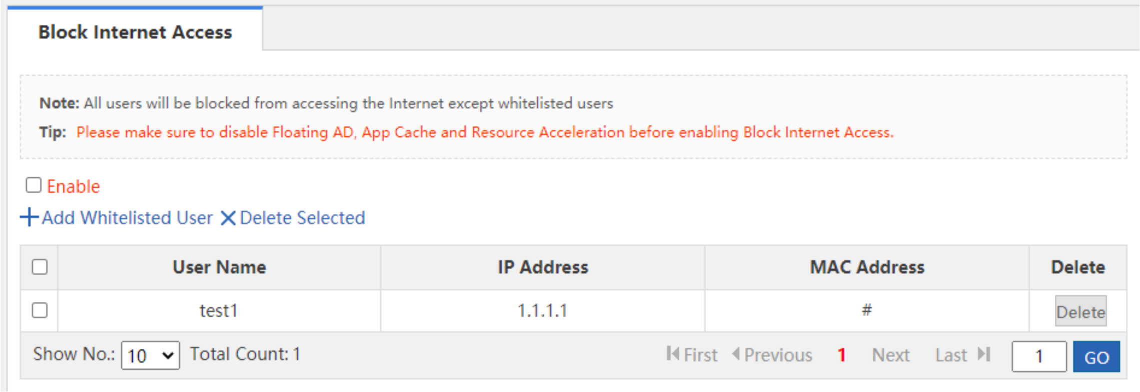
- All Users
  - ☐cloud_voucher
  - ☐cloud_account
  - ☐OneclickUser
  - ☐test
    - ☑test1
    - ☐test2

(If you want to add users, please choose Common User > User Structure and perform configuration)

OK

(3) Select users you want to add to the whitelist.

(4) Click OK.



Block Internet Access

Note: All users will be blocked from accessing the Internet except whitelisted users

Tip: Please make sure to disable Floating AD, App Cache and Resource Acceleration before enabling Block Internet Access.

□ Enable

+Add Whitelisted User ✕Delete Selected

□	User Name	IP Address	MAC Address	Delete
□	test1	1.1.1.1	#	Delete

Show No.: 10 Total Count: 1

Follow-up Procedure

- Click Delete in the **Delete** column to delete a single whitelisted user.
- Click ✕ Delete Selected to delete multiple selected whitelisted users.

6.2 Web Authentication

The system provides web authentication and web authentication exemption functions.

6.2.1 Web Authentication

Application Scenario

Web authentication is also known as user authentication.

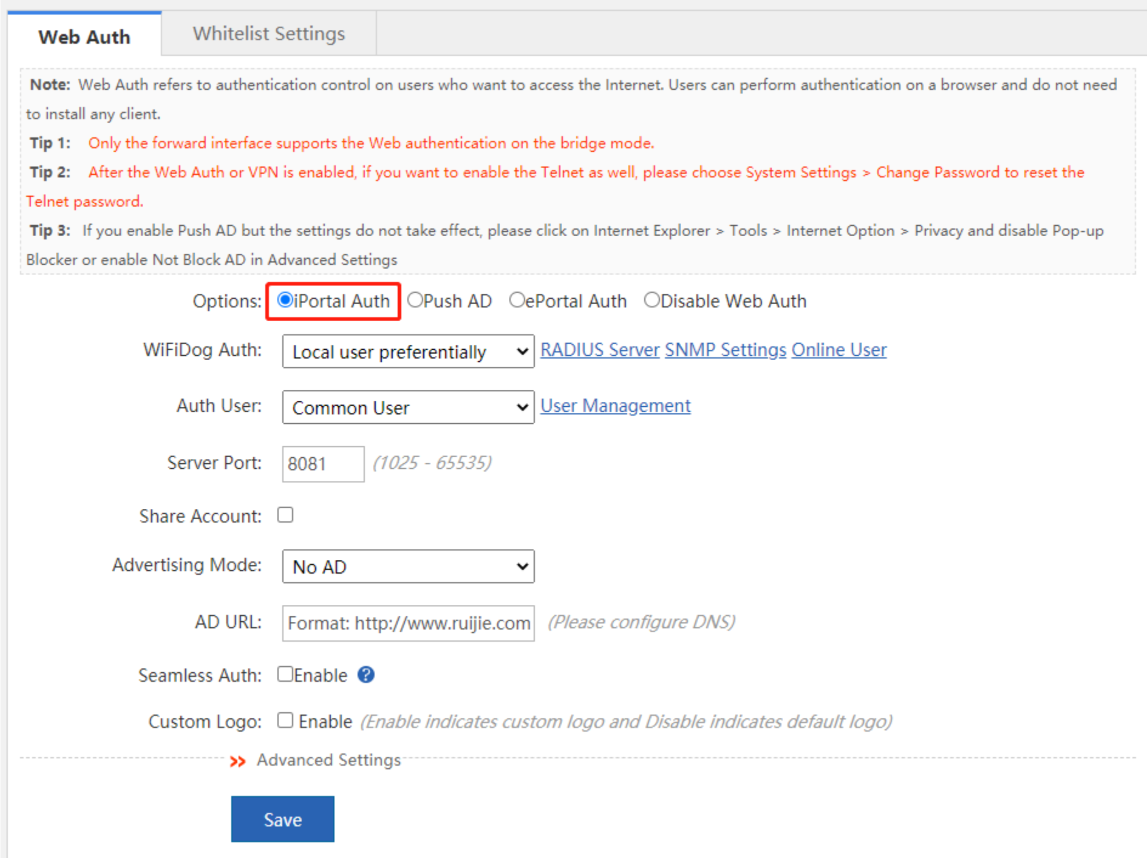
User authentication is an authentication method used to control users' permission to access a network. You do not need to install a specific client authentication software and can just use a common browser for access authentication. When an external user accesses a network, the authentication device forces the user to log in to the specified site and then the user can access services of the network for free. When the user needs other information on the Internet, the user must be authenticated on the web authentication server and then can use Internet resources. If the user attempts to access other external networks via HTTP, the user is forced to access the web authentication website and thus the web authentication process is started. This method is called forced authentication. Authentication provides users with convenient management functions. Portal websites can provide advertising, community service, and customized services.

The device supports both the built-in authentication server and external authentication server. When the built-in authentication server is used, the device already provides relevant service functions and thus you do not need to use an external server. When an external authentication server is used, you must deploy an ePortal server and Radius server first.

Procedure

(1) Choose **User** > **Web Auth** > **Web Auth**.

(2) Set the built-in authentication server.



Note: Web Auth refers to authentication control on users who want to access the Internet. Users can perform authentication on a browser and do not need to install any client.

Tip 1: Only the forward interface supports the Web authentication on the bridge mode.

Tip 2: After the Web Auth or VPN is enabled, if you want to enable the Telnet as well, please choose System Settings > Change Password to reset the Telnet password.

Tip 3: If you enable Push AD but the settings do not take effect, please click on Internet Explorer > Tools > Internet Option > Privacy and disable Pop-up Blocker or enable Not Block AD in Advanced Settings

Options: ● iPortal Auth ○ Push AD ○ ePortal Auth ○ Disable Web Auth

WiFiDog Auth: Local user preferentially RADIUS Server SNMP Settings Online User

Auth User: Common User User Management

Server Port: 8081 (1025 - 65535)

Share Account: □

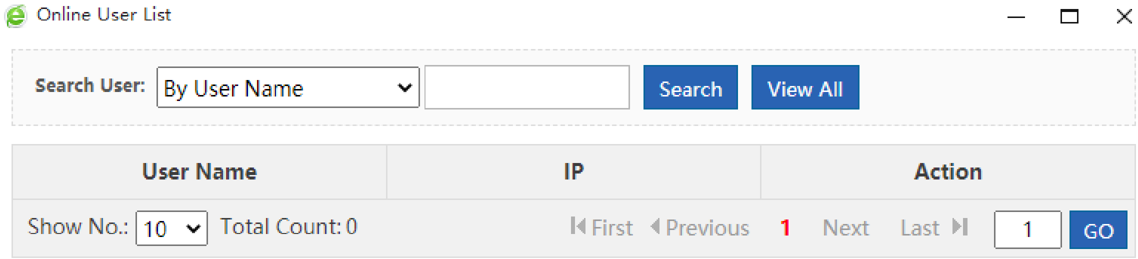
Advertising Mode: No AD

AD URL: Format: http://www.ruijie.com (Please configure DNS)

Seamless Auth: □ Enable

Custom Logo: □ Enable (Enable indicates custom logo and Disable indicates default logo)

Click Online User and the following window is displayed, in which you can view currently authenticated online users. Click **Force Offline** to make the selected user offline. You can also query online users:

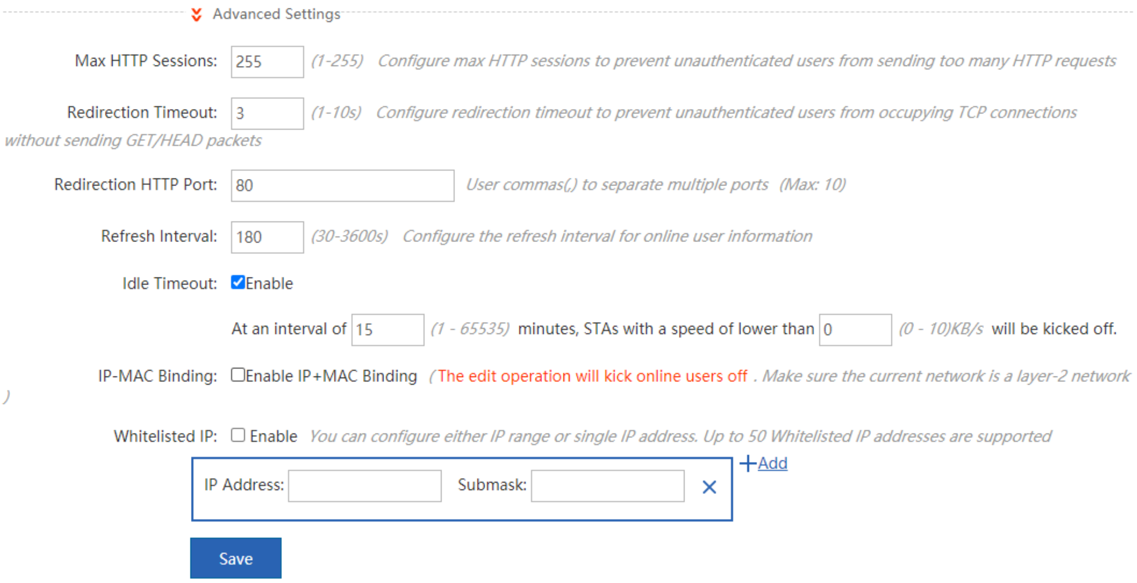


User Name	IP	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

- **WiFiDog Auth**: When the built-in portal server of the device is used for user identity authentication, you can obtain the user information from a local server, from a Radius server, or from both the local and Radius servers. The option **External user preferentially** is recommended but you have to build a Radius server first.
- **Server Port**: The port ID of the built-in portal server, ranging from 1025 to 65535. The default port ID is 8081. You can modify the port.
- **Share Account**: One account can have only one IP address at a time. After **Share Account** is enabled, multiple IP addresses can share one account. After this function is disabled, the account logged in later is valid.
- **SMP User Changes Password**: After this function is enabled, you need to input the URL for password modification, and then SMP users can modify their passwords through this URL.
- **Advertising Mode**: Set the advertising display method. Options are **AD after Auth** or **No AD**.

- **AD URL**: The URL of the advertising page.
- **Seamless Auth**: After this function is enabled, the advertising is pushed without the need of authenticating the user IP address.
- **Custom Logo**: When this function is enabled, the custom logo is displayed. When this function is disabled, the system default logo is displayed. You can customize authentication logos.
- **Advanced Settings**: Click >> Advanced Settings to configure more parameters, as shown below. For details, see the section 6.2.3 Advanced Settings for User Authentication.



Advanced Settings

Max HTTP Sessions: 255 (1-255) Configure max HTTP sessions to prevent unauthenticated users from sending too many HTTP requests

Redirection Timeout: 3 (1-10s) Configure redirection timeout to prevent unauthenticated users from occupying TCP connections without sending GET/HEAD packets

Redirection HTTP Port: 80 User commas(,) to separate multiple ports (Max: 10)

Refresh Interval: 180 (30-3600s) Configure the refresh interval for online user information

Idle Timeout: ☑Enable

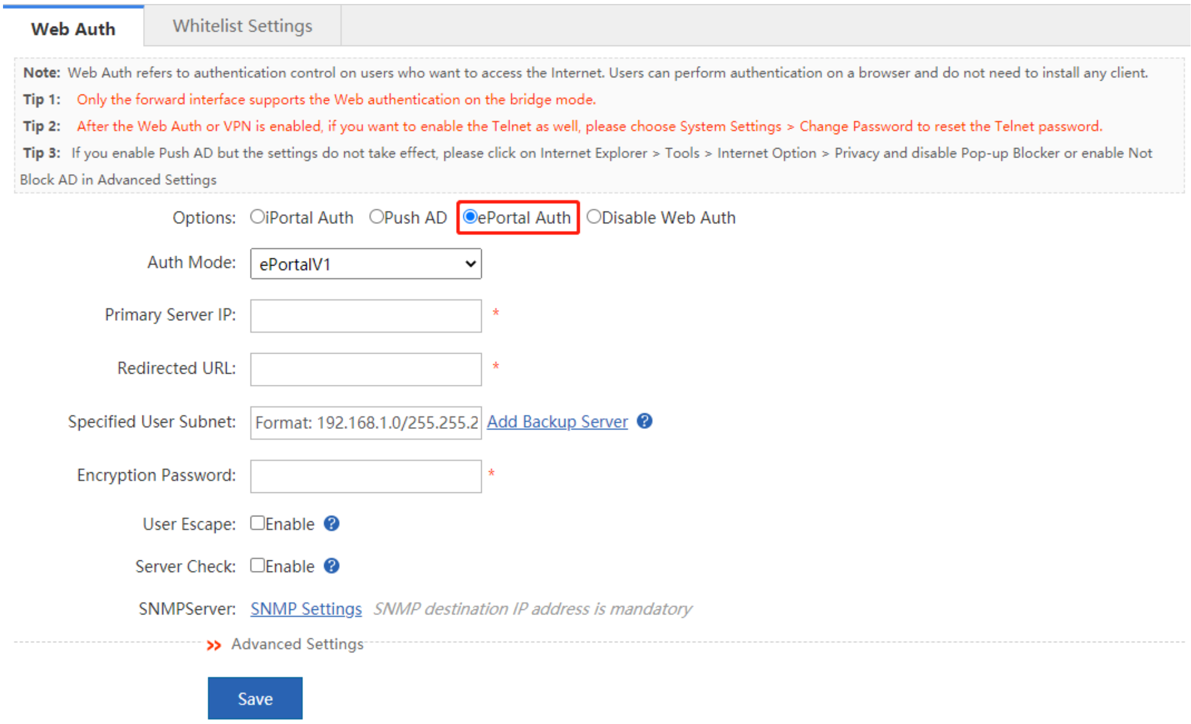
At an interval of 15 (1 - 65535) minutes, STAs with a speed of lower than 0 (0 - 10)KB/s will be kicked off.

IP-MAC Binding: □Enable IP+MAC Binding (The edit operation will kick online users off . Make sure the current network is a layer-2 network)

Whitelisted IP: □ Enable You can configure either IP range or single IP address. Up to 50 Whitelisted IP addresses are supported

IP Address: Submask: ×

(3) Set the external authentication server.



Note: Web Auth refers to authentication control on users who want to access the Internet. Users can perform authentication on a browser and do not need to install any client.

Tip 1: Only the forward interface supports the Web authentication on the bridge mode.

Tip 2: After the Web Auth or VPN is enabled, if you want to enable the Telnet as well, please choose System Settings > Change Password to reset the Telnet password.

Tip 3: If you enable Push AD but the settings do not take effect, please click on Internet Explorer > Tools > Internet Option > Privacy and disable Pop-up Blocker or enable Not Block AD in Advanced Settings

Options: ○iPortal Auth ○Push AD ●ePortal Auth ○Disable Web Auth

Auth Mode: ePortalV1

Primary Server IP: *

Redirected URL: *

Specified User Subnet: Format: 192.168.1.0/255.255.2 Add Backup Server

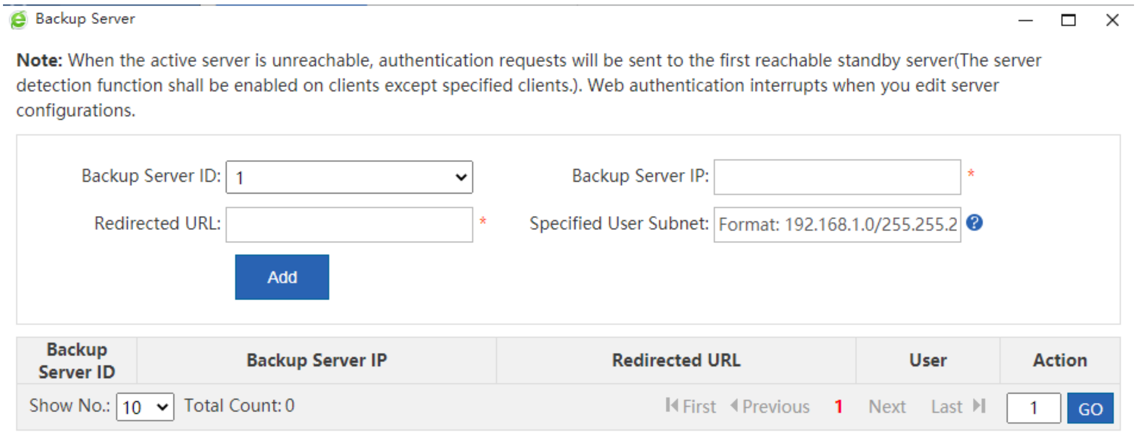
Encryption Password: *

User Escape: □Enable

Server Check: □Enable

SNMPServer: SNMP Settings SNMP destination IP address is mandatory

- **Server IP**: Input the IP address for the external ePortal server you have built. Generally, the authentication page is provided by the authentication ePortal server.
- **Redirected URL**: Input the URL of the authentication page in this field. When an unauthenticated user accesses network resources, the system redirects to this page automatically and remains on this page after the user is authenticated.
- **Specified User Subnet**: The network segment in which IP addresses must be authenticated by the ePortal server. IP addresses not in this network segment do not need to be authenticated.
- **Add Backup Server**: When the active server communication fails, the system automatically switches to the backup server. Web authentication service is interrupted when you edit the server configurations. As shown below, the web allows you to add up to 4 backup portal servers:



Backup Server

Note: When the active server is unreachable, authentication requests will be sent to the first reachable standby server(The server detection function shall be enabled on clients except specified clients.). Web authentication interrupts when you edit server configurations.

Backup Server ID: 1 Backup Server IP: *

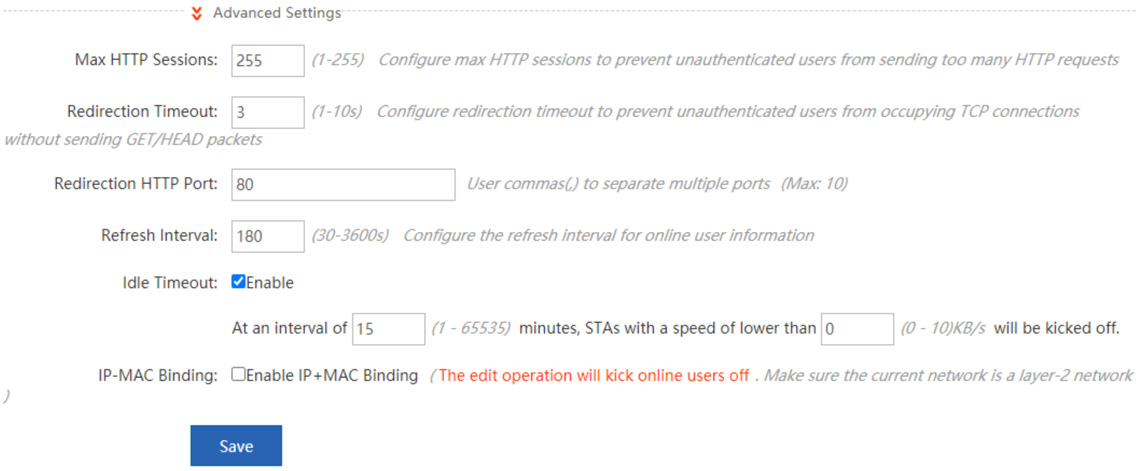
Redirected URL: * Specified User Subnet: Format: 192.168.1.0/255.255.2

Add

Backup Server ID	Backup Server IP	Redirected URL	User	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

- **Encryption Password**: Set the password for communication between the device and the authentication server. This password must be consistent with the communication password of the authentication server; otherwise, it does not come into effect.
- **SNMP Dest Host**: The host address of the authentication server.
- SNMP can be configured only when an external authentication server is used. To enable authentication by an external server, you must set the NIC parameters for SNMP communication between the authentication device and the authentication server, including **SNMP Password** and **SNMP Dest Host**.
- **Advanced Settings**: Click >> Advanced Settings to configure more parameters, as shown below. For details, see the section 6.2.3 Advanced Settings for User Authentication.



Advanced Settings

Max HTTP Sessions: 255 (1-255) Configure max HTTP sessions to prevent unauthenticated users from sending too many HTTP requests

Redirection Timeout: 3 (1-10s) Configure redirection timeout to prevent unauthenticated users from occupying TCP connections without sending GET/HEAD packets

Redirection HTTP Port: 80 User commas(,) to separate multiple ports (Max: 10)

Refresh Interval: 180 (30-3600s) Configure the refresh interval for online user information

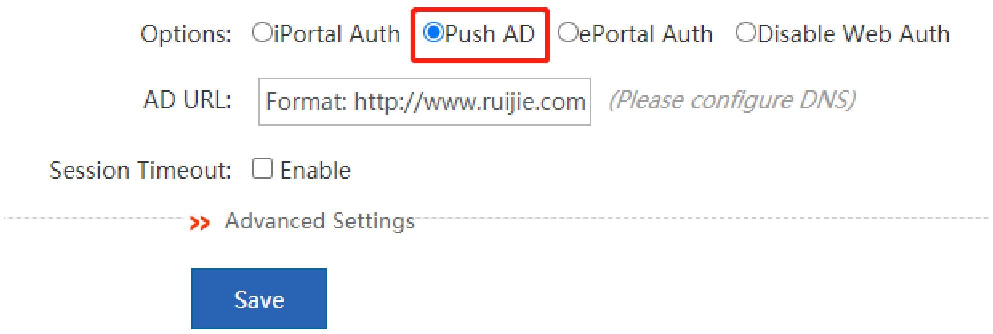
Idle Timeout: ☑Enable

At an interval of 15 (1 - 65535) minutes, STAs with a speed of lower than 0 (0 - 10)KB/s will be kicked off.

IP-MAC Binding: ☐Enable IP+MAC Binding （The edit operation will kick online users off . Make sure the current network is a layer-2 network ）

Save

(4) Set the advertising push service.



Options: ○iPortal Auth ●Push AD ○ePortal Auth ○Disable Web Auth

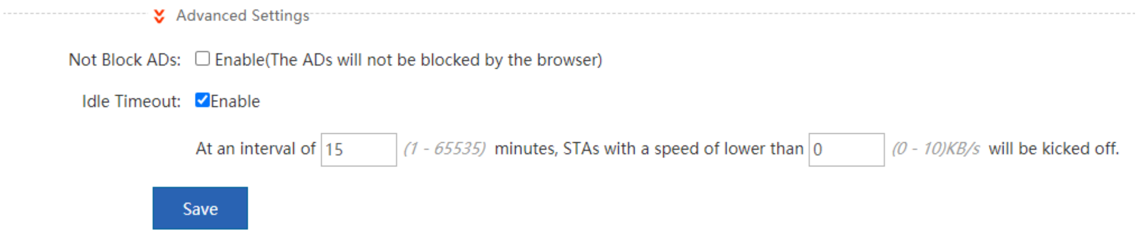
AD URL: Format: http://www.ruijie.com *(Please configure DNS)*

Session Timeout: □ Enable

» Advanced Settings

Save

- Input the advertising URL.
- **Advanced Settings**: Click » Advanced Settings to configure more parameters, as shown below.



Advanced Settings

Not Block ADs: □ Enable(The ADs will not be blocked by the browser)

Idle Timeout: ☑Enable

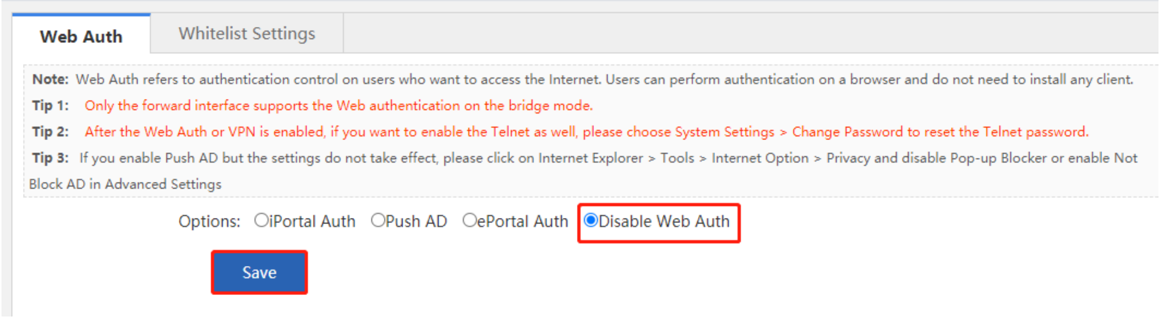
At an interval of 15 *(1 - 65535)* minutes, STAs with a speed of lower than 0 *(0 - 10)KB/s* will be kicked off.

Save

After the advertising push service configuration is saved, the advertising page pops up when the advertising push user accesses the network for the first time. After **Push AD** is enabled, if the advertising page does not pop up, choose **Internet options** > **Privacy** and unselect **Enable pop-up blocker**, or enable **Not Block ADs** Not Block ADs: ☑ Enable(The ADs will not be blocked by the browser) in Advanced Settings.

Follow-up Procedure

If user authentication is no longer required, select ●Disable Web Auth and then click Save to disable the function.



Web Auth | Whitelist Settings

Note: Web Auth refers to authentication control on users who want to access the Internet. Users can perform authentication on a browser and do not need to install any client.

Tip 1: Only the forward interface supports the Web authentication on the bridge mode.

Tip 2: After the Web Auth or VPN is enabled, if you want to enable the Telnet as well, please choose System Settings > Change Password to reset the Telnet password.

Tip 3: If you enable Push AD but the settings do not take effect, please click on Internet Explorer > Tools > Internet Option > Privacy and disable Pop-up Blocker or enable Not Block AD in Advanced Settings

Options: ○iPortal Auth ○Push AD ○ePortal Auth ●Disable Web Auth

Save

6.2.2 Web Authentication Exemption

Application Scenario

- **Whitelisted Network**: Input the IP address of the network server. Then all users, including unauthenticated users, can access this IP address. You can set up to 1,000 rules.

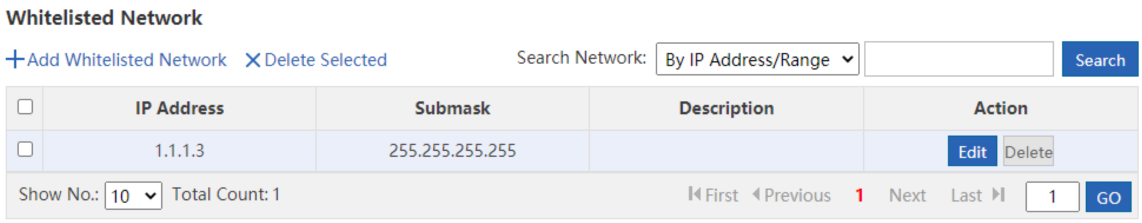
- **IP/MAC of Whitelisted User**: This user can directly access the network and no advertising will be pushed to this user. You can set up to 1,000 rules.

Procedure

(1) Choose **User** > **Web Auth** > **Whitelist Settings**.

(2) Set the whitelisted networks.

- **Whitelisted Network**: After **Web Auth** is enabled, unauthenticated users must pass web authentication first before they can access networks. To allow unauthenticated users to access some whitelisted networks, you can use this item to set whitelisted networks. After a website is set as a whitelisted network, all users, including unauthenticated users, can access this website. By default, unauthenticated users cannot access non-whitelisted networks. (Note: You can configure a single IP address or an IP address range (in the format of IP address + mask, such as 192.168..1.0 255.255.255.0). The IP address range is a whitelisted network.)



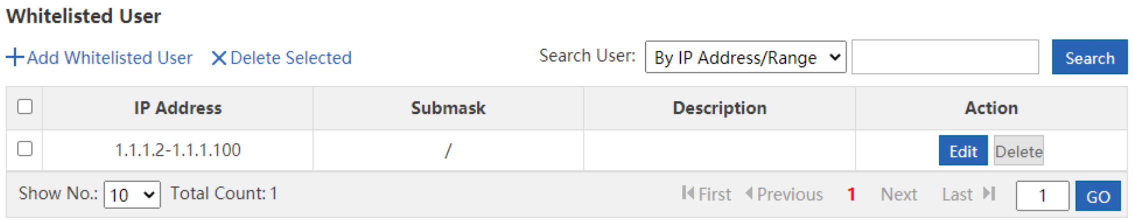
Whitelisted Network

+Add Whitelisted Network ✕Delete Selected Search Network: By IP Address/Range Search

□	IP Address	Submask	Description	Action
□	1.1.1.3	255.255.255.255		Edit Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

- **Whitelisted User**: If the IP address of a user is whitelisted, the user can directly access all reachable networks without needing to pass the web authentication. No whitelisted user is configured by default. All users must pass the web authentication before they can access networks. (Note: You can configure a single IP address or an IP address range (in the format of IP address + mask, such as 192.168..1.0 255.255.255.0). The IP address range is a whitelisted network.)



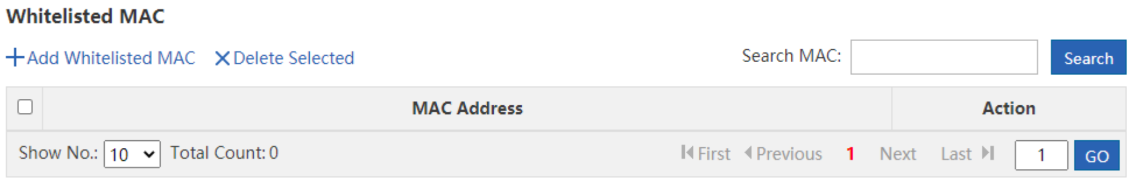
Whitelisted User

+Add Whitelisted User ✕Delete Selected Search User: By IP Address/Range Search

□	IP Address	Submask	Description	Action
□	1.1.1.2-1.1.1.100	/		Edit Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

- **Whitelisted MAC**: You can query, add, delete, or modify the user MAC addresses.



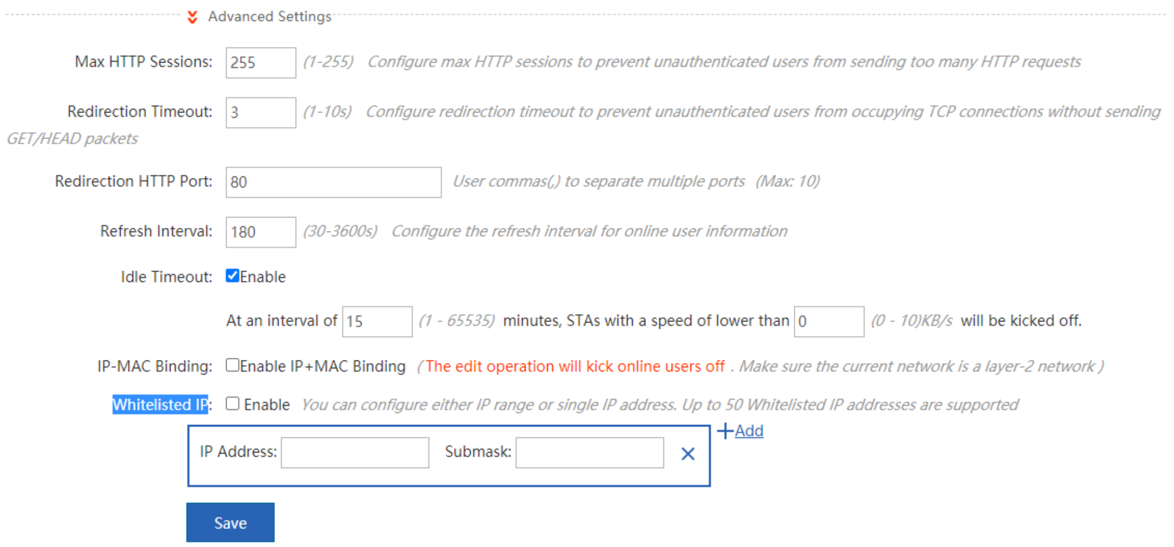
Whitelisted MAC

+Add Whitelisted MAC ✕Delete Selected Search MAC: Search

□	MAC Address	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

6.2.3 Advanced Settings for User Authentication



Advanced Settings

Max HTTP Sessions: 255 *(1-255) Configure max HTTP sessions to prevent unauthenticated users from sending too many HTTP requests*

Redirection Timeout: 3 *(1-10s) Configure redirection timeout to prevent unauthenticated users from occupying TCP connections without sending GET/HEAD packets*

Redirection HTTP Port: 80 *User commas(,) to separate multiple ports (Max: 10)*

Refresh Interval: 180 *(30-3600s) Configure the refresh interval for online user information*

Idle Timeout: ☑Enable

At an interval of 15 *(1 - 65535)* minutes, STAs with a speed of lower than 0 *(0 - 10)KB/s* will be kicked off.

IP-MAC Binding: □Enable IP+MAC Binding (The edit operation will kick online users off . *Make sure the current network is a layer-2 network)*

Whitelisted IP: □ Enable *You can configure either IP range or single IP address. Up to 50 Whitelisted IP addresses are supported*

- **Max HTTP Sessions:** You can set a maximum number of HTTP sessions for each authenticated user. When an unauthenticated user accesses a network, the user PC sends an HTTP session connection request. The device blocks the HTTP packet and requires the user to pass the web authentication through a redirection request. To prevent an unauthenticated user from sending too many HTTP connection requests to save the device resources, you need to set a maximum number of HTTP sessions for the unauthenticated user on the authentication device. One HTTP session is occupied for user authentication, while other applications of the user may occupy HTTP sessions. Therefore, do not set the maximum number of HTTP sessions of unauthenticated users to 1. By default, the maximum number of HTTP sessions of unauthenticated users is 255.
- **Redirection Timeout:** You can set a redirection timeout time. When an unauthenticated user accesses a network via HTTP, the user's TCP connection requests will be blocked and a TCP connection is established with the authentication device. After the connection is established, the authentication device waits for the HTTP GET/HEAD packet from the user, returns an HTTP redirection packet, and then closes the connection. The redirection timeout time can prevent the problem that the user does not send the GET/HEAD packet and occupies the TCP connection for a long time. By default, the redirection timeout time is 3s.
- **Redirection HTTP Port**: You can set up to 10 destination port IDs. When a user accesses a network (such as accessing the Internet through a browser), the user will send an HTTP packet, and the authentication device blocks this HTTP packet and judges whether the user is accessing a network. When the authentication device detects that an unauthenticated user is accessing a network, the device blocks the user's network access request and displays the authentication page. By default, the authentication device blocks HTTP packets sent from the port 80 to check whether the user is accessing a network.
- **Refresh Interval**: You can set an interval for refreshing online user information. The authentication device maintains online user information and needs to update such information periodically, including the online duration. In this way, the device can monitor the network resources used by online users. When the online duration of a user is greater than or equal to the online limit, the user is disabled from using the network again. By default, the refresh interval is 60s.
- **Idle Timeout**: You can set a traffic-based user offline detection mode. For example, if the user traffic does not increase within 15 minutes, the device judges that the user has been offline. This command is used to check whether a user is offline, but some detection errors may occur. The system supports two user offline

detection modes: a. The user has clicked the **Offline** button on the authentication page. b. The traffic-based user offline detection mode is used. When user traffic does not increase within 15 minutes, the device judges that the user has been offline. Both modes are enabled by default.

- **IP-MAC Binding**: Set the IP-MAC binding mode to IP+MAC. In an L2 network, you can bind a user name to both the MAC address and IP address.
- **Whitelisted IP**: Advertising is pushed to users whose IP addresses are whitelisted without the need to authenticate such users.

6.3 Local Server Authentication

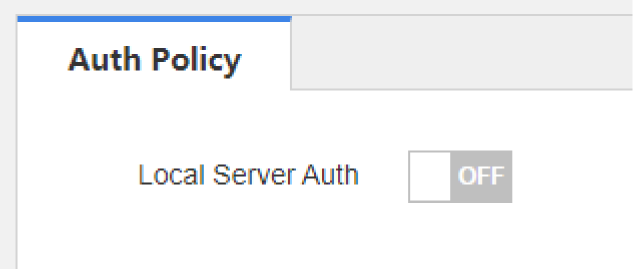
6.3.1 Authentication Policy

Procedure

(1) Choose **User** > **Local Auth** > **Auth Policy**.

(2) Set **Local Server Auth** to ON.

If **Local Server Auth** is set to **OFF**, only **Auth Policy** is available in the **Local Server Auth** sub-menu.

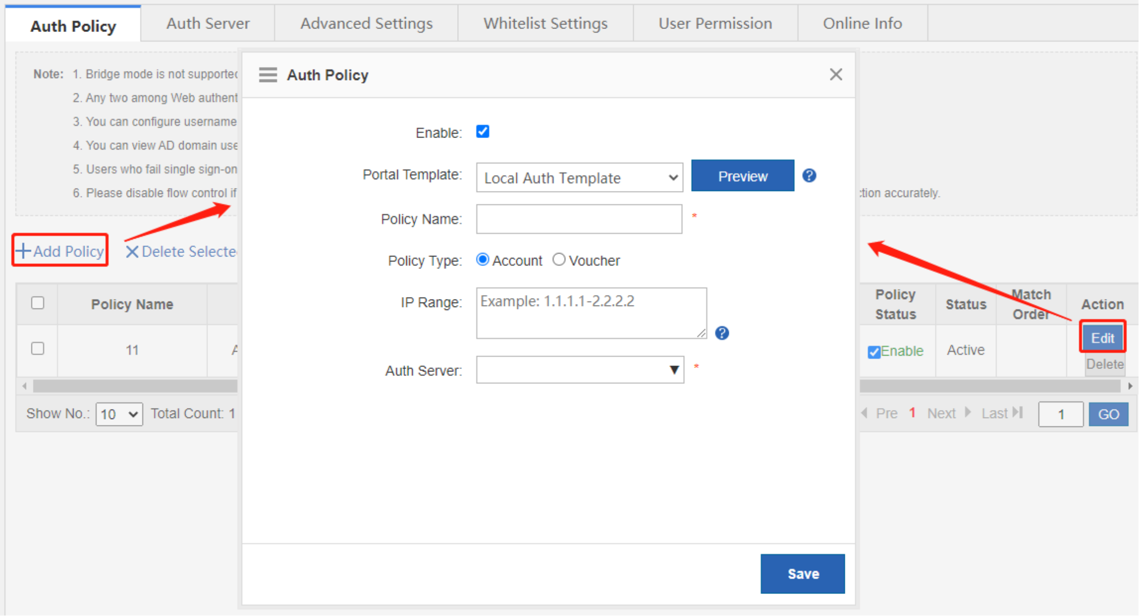


Local Server Auth OFF

(3) Add or edit an authentication policy

Click **Add Policy** or **Edit** to configure an authentication policy.

You can edit the policy only after selecting **Enable**. The authentication server obtains relevant requests through the **Auth Server** interface.


Auth Policy
Auth Server
Advanced Settings
Whitelist Settings
User Permission
Online Info
Note: 1. Bridge mode is not supportec
2. Any two among Web authent
3. You can configure username
4. You can view AD domain use
5. Users who fail single sign-on
6. Please disable flow control if
:tion accurately.
+Add Policy
✕Delete Selecte
Preview
Save
Edit
Delete
Pre 1 Next Last
GO

Auth Policy

Enable: ☑

Portal Template: Local Auth Template

Policy Name: *

Policy Type: ● Account ○ Voucher

IP Range: Example: 1.1.1.1-2.2.2.2

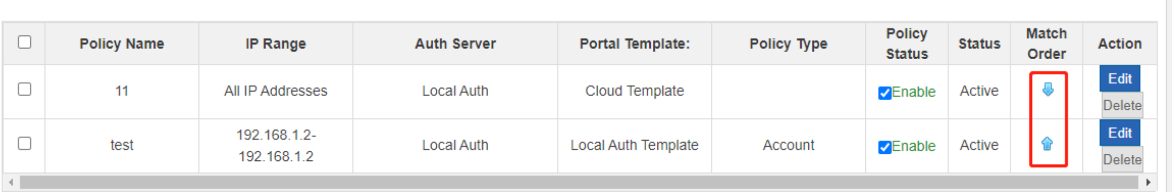
Auth Server: *

□	Policy Name	Policy Status	Status	Match Order	Action
□	11	☑Enable	Active		Edit Delete

Show No.: 10 Total Count: 1

(4) Adjust the priority of an authentication policy

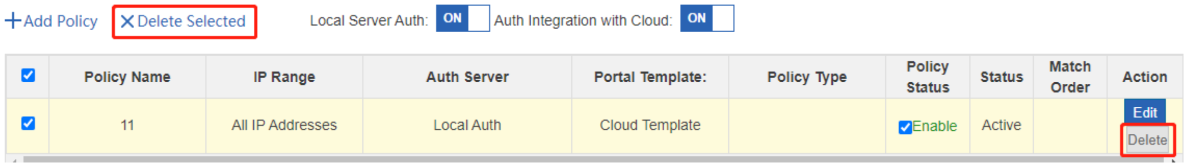
Click the arrows in the **Match Order** column to switch the priorities of authentication policies.



☐	Policy Name	IP Range	Auth Server	Portal Template:	Policy Type	Policy Status	Status	Match Order	Action
☐	11	All IP Addresses	Local Auth	Cloud Template		☑Enable	Active	↓	Edit Delete
☐	test	192.168.1.2- 192.168.1.2	Local Auth	Local Auth Template	Account	☑Enable	Active	↑	Edit Delete

Follow-up Procedure

Click Delete or ✕ Delete Selected to delete authentication policies.



+Add Policy ✕Delete Selected Local Server Auth: ON Auth Integration with Cloud: ON

☑	Policy Name	IP Range	Auth Server	Portal Template:	Policy Type	Policy Status	Status	Match Order	Action
☑	11	All IP Addresses	Local Auth	Cloud Template		☑Enable	Active		Edit Delete

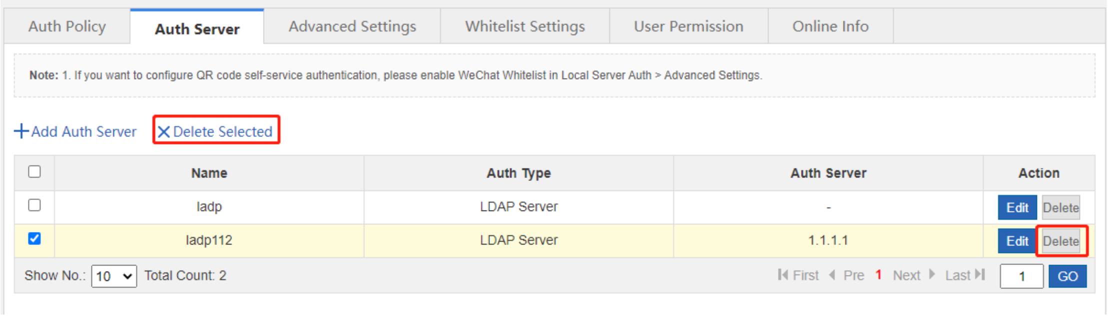
6.3.2 Authentication Server

Procedure

(1) Choose **User** > **Local Auth** > **Auth Server**.

(2) Delete the authentication server

Click Delete or ✕ Delete Selected to delete the authentication server.



Auth Policy | Auth Server | Advanced Settings | Whitelist Settings | User Permission | Online Info

Note: 1. If you want to configure QR code self-service authentication, please enable WeChat Whitelist in Local Server Auth > Advanced Settings.

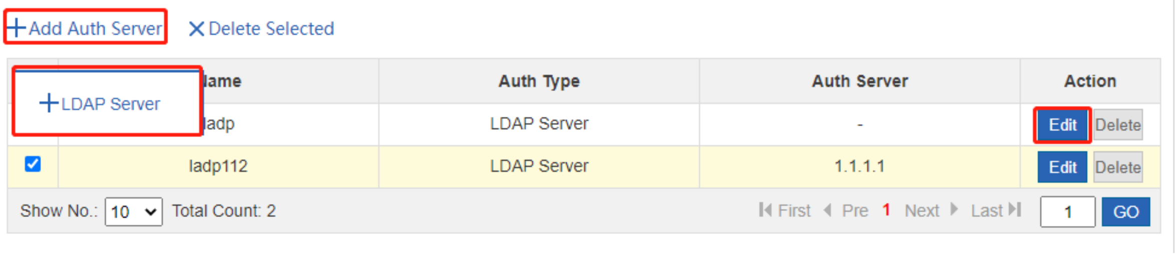
+Add Auth Server ✕Delete Selected

☐	Name	Auth Type	Auth Server	Action
☐	ladp	LDAP Server	-	Edit Delete
☑	ladp112	LDAP Server	1.1.1.1	Edit Delete

Show No.: 10 Total Count: 2 First Pre 1 Next Last 1 GO

(3) Add or edit an LDAP server.

Click **Add Auth Server** or **Edit** to configure an LDAP server.

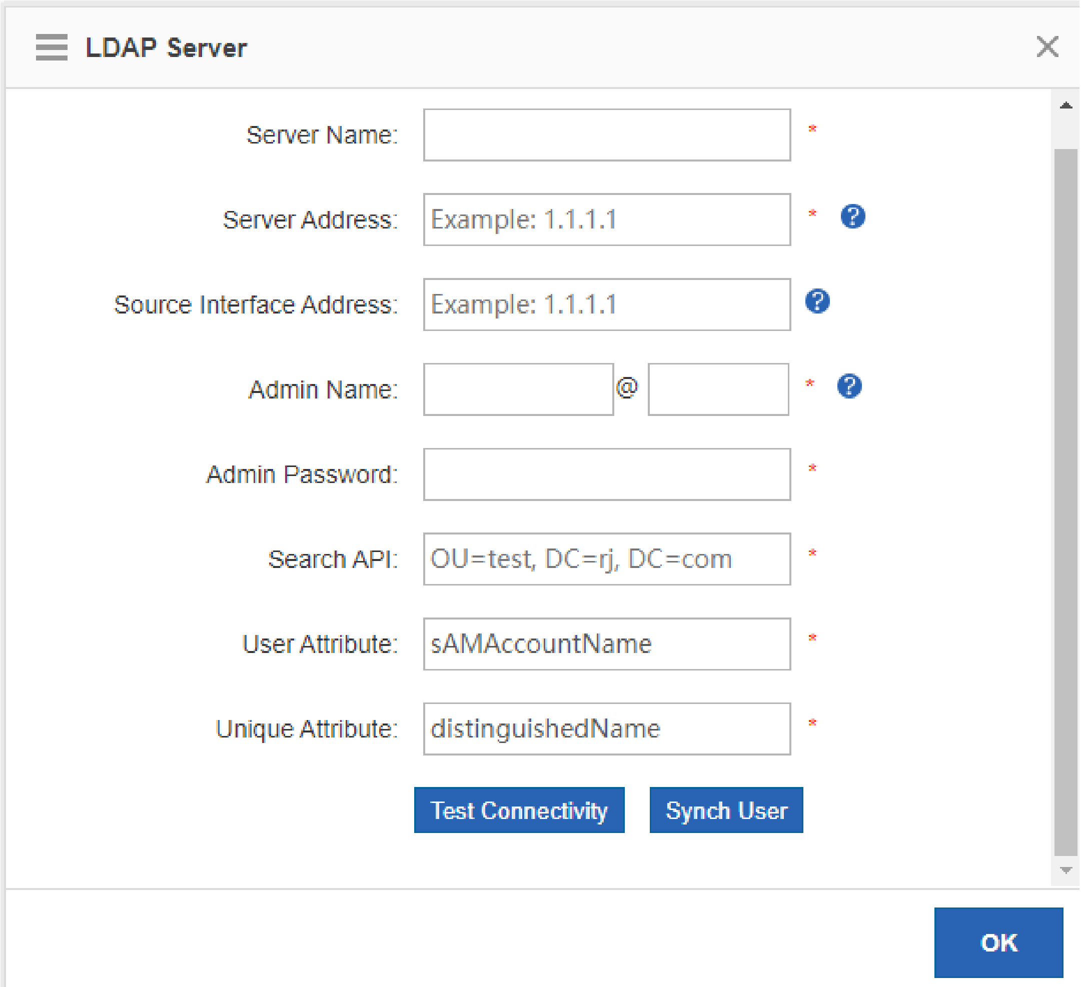


+Add Auth Server ✕Delete Selected

+LDAP Server

	ame	Auth Type	Auth Server	Action
	adp	LDAP Server	-	Edit Delete
☑	ladp112	LDAP Server	1.1.1.1	Edit Delete

Show No.: 10 Total Count: 2 First Pre 1 Next Last 1 GO



LDAP Server

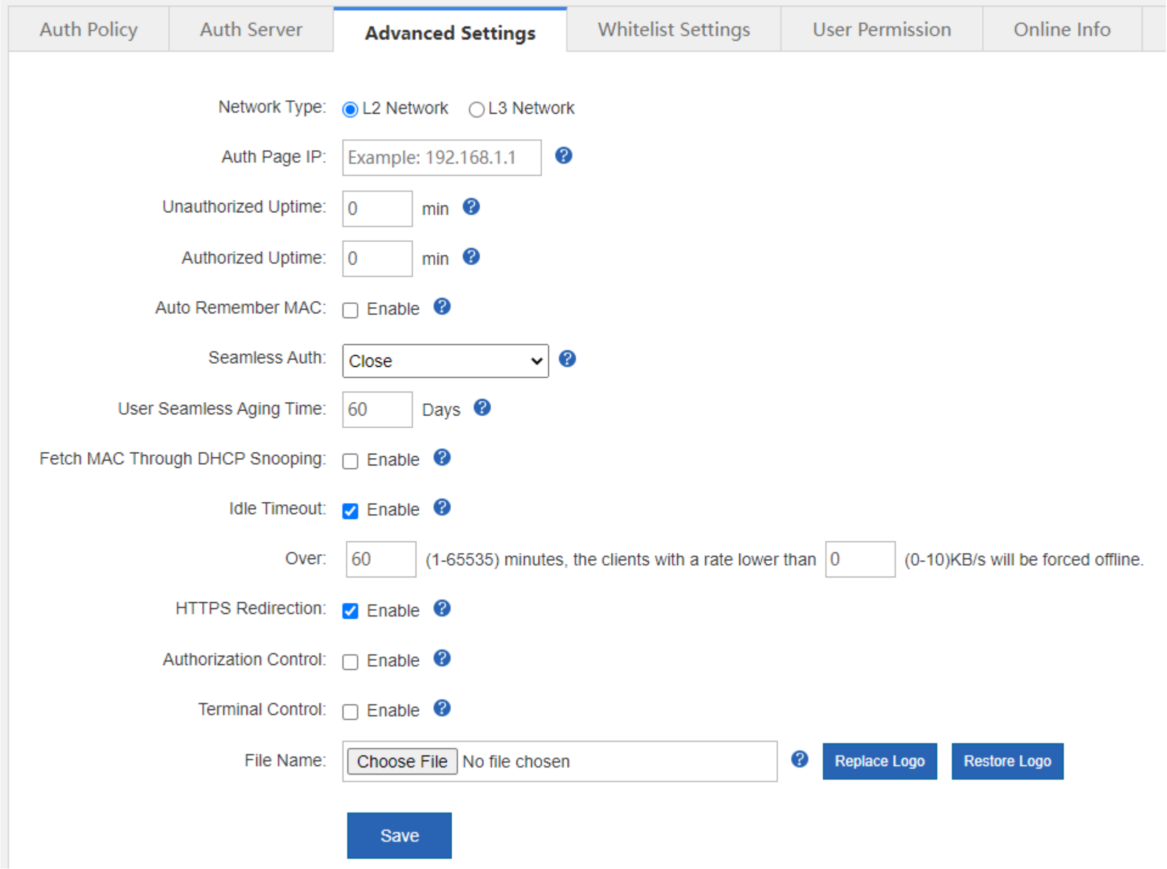
Server Name:	*
Server Address:	Example: 1.1.1.1 *
Source Interface Address:	Example: 1.1.1.1
Admin Name:	@ *
Admin Password:	*
Search API:	OU=test, DC=rj, DC=com *
User Attribute:	sAMAccountName *
Unique Attribute:	distinguishedName *

Field	Note
Server Name	The name of the authentication server
Server Address	The IP address of the server
Source Interface Address	The source interface address, which can be left blank
Admin Name	The administrator name
Admin Password	The administrator password
Search API	The search API
User Attribute	The user attribute
Unique Attribute	The user unique attribute

6.3.3 Advanced Settings

Procedure

(1) Choose **User** > **Local Auth** > **Advanced Settings**.



Network Type: ● L2 Network ○ L3 Network

Auth Page IP: Example: 192.168.1.1

Unauthorized Uptime: 0 min

Authorized Uptime: 0 min

Auto Remember MAC: □ Enable

Seamless Auth: Close

User Seamless Aging Time: 60 Days

Fetch MAC Through DHCP Snooping: □ Enable

Idle Timeout: ☑ Enable

Over: 60 (1-65535) minutes, the clients with a rate lower than 0 (0-10)KB/s will be forced offline.

HTTPS Redirection: ☑ Enable

Authorization Control: □ Enable

Terminal Control: □ Enable

File Name: Choose File No file chosen

(2) Set advanced configuration items.

Field	Note
Network Type	The network type ● L2 Network ● L3 Network
Unauthorized Uptime	The online duration of an unauthorized user
Authorized Uptime	The online duration of an authorized user
Auto Remember MAC	Whether to automatically record the account's MAC address
MAC Address Limit	The maximum number of MAC addresses recorded for each account
Seamless Auth	0: Close

Field	Note
	1: Seamless MAC bypass 2: Seamless Web Popup
User Seamless Aging Time	The idle aging time of the account
Fetch MAC Through DHCP Snooping	Whether to obtain the MAC address through DHCP Snooping
Idle Timeout	Whether to enable offline detection when there is no traffic
Over x minutes	The duration
the clients with a rate lower than x KB/s will be forced offline.	The traffic below which the user's traffic is will the user be forced offline
HTTPS Redirection	Whether to enable HTTPS redirection
Authorization Control	Whether to enable authorization control
Authorization Times for Unprivileged Users	The number of authorization times for an authorized user
Terminal Control	When Internet access from PCs or mobile terminals is disabled, terminal control can be enabled.
Deny PC Access	Whether accesses from PCs are denied
Exceptional Time	The exceptional time for **Deny PC Access** You must set an exceptional time of **None**.
Deny Mobile Terminal Access	Whether accesses from mobile terminals are denied
Exceptional Time	The exceptional time for Deny Mobile Terminal Access You must set an exceptional time of **None**.

(3) Click **Save**.

6.3.4 Whitelisted Settings

Application Scenario

After IP addresses or MAC addresses are configured for whitelisted users, they can directly access the Internet without passing authentication. Traffic from all the users in the blacklist is blocked.

Whitelisted User: This user is allowed to access the Internet without authentication. No AD will be pushed to this user.

Whitelisted External IP: All users are allowed to access this external IP address.

Whitelisted URL: All users are allowed to access this URL.

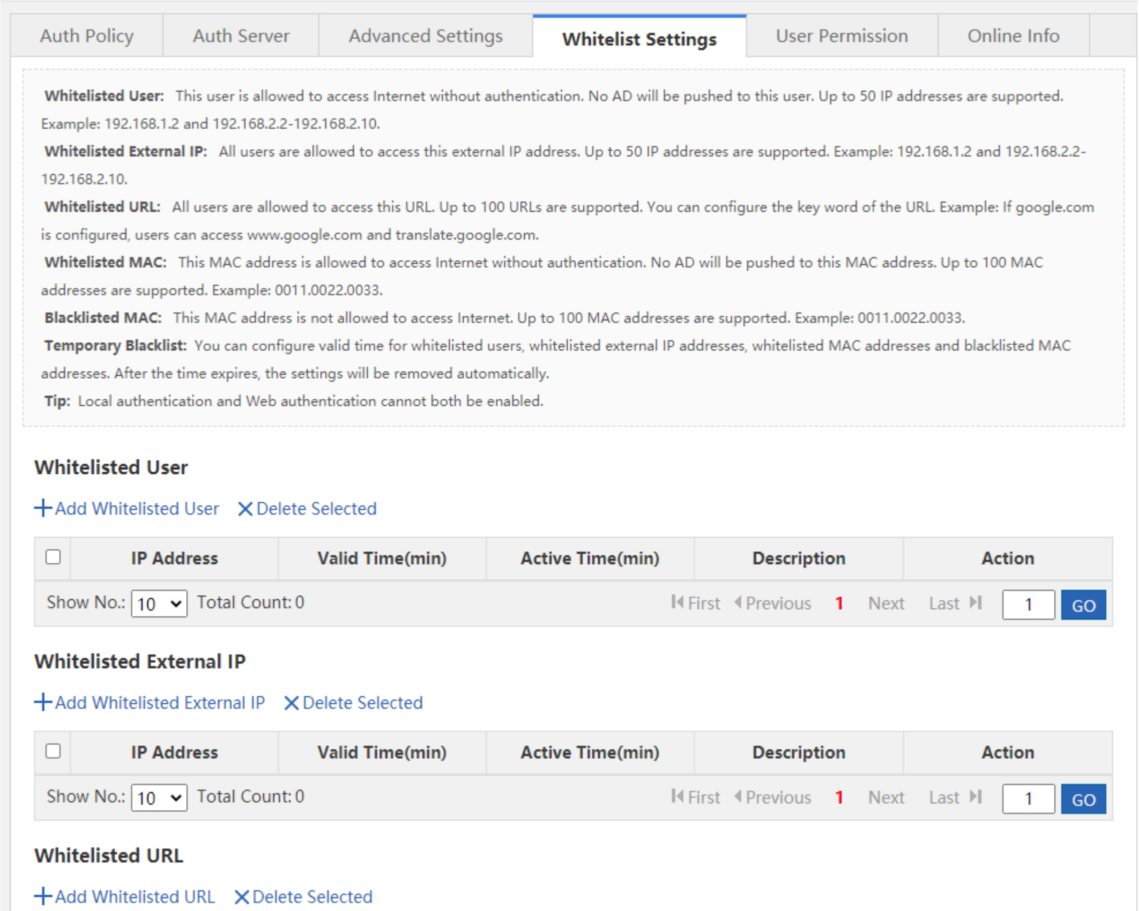
Whitelisted MAC: This MAC address is allowed to access the Internet without authentication. No AD will be pushed to this MAC address.

Blacklisted MAC: This MAC address is not allowed to access Internet.

Temporary Blacklist: You can configure a valid time for whitelisted users, whitelisted external IP addresses, whitelisted MAC addresses, and blacklisted MAC addresses. After the time expires, the settings will be removed automatically.

Procedure

(1) Choose **User** > **Local Auth** > **Whitelist Settings**.



Whitelisted User: This user is allowed to access Internet without authentication. No AD will be pushed to this user. Up to 50 IP addresses are supported. Example: 192.168.1.2 and 192.168.2.2-192.168.2.10.

Whitelisted External IP: All users are allowed to access this external IP address. Up to 50 IP addresses are supported. Example: 192.168.1.2 and 192.168.2.2-192.168.2.10.

Whitelisted URL: All users are allowed to access this URL. Up to 100 URLs are supported. You can configure the key word of the URL. Example: If google.com is configured, users can access www.google.com and translate.google.com.

Whitelisted MAC: This MAC address is allowed to access Internet without authentication. No AD will be pushed to this MAC address. Up to 100 MAC addresses are supported. Example: 0011.0022.0033.

Blacklisted MAC: This MAC address is not allowed to access Internet. Up to 100 MAC addresses are supported. Example: 0011.0022.0033.

Temporary Blacklist: You can configure valid time for whitelisted users, whitelisted external IP addresses, whitelisted MAC addresses and blacklisted MAC addresses. After the time expires, the settings will be removed automatically.

Tip: Local authentication and Web authentication cannot both be enabled.

Whitelisted User

□	IP Address	Valid Time(min)	Active Time(min)	Description	Action

Show No.: 10 Total Count: 0

Whitelisted External IP

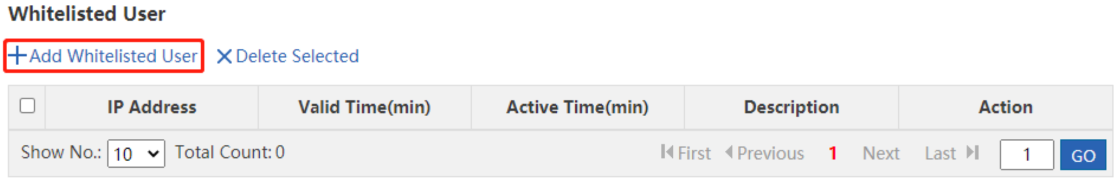
□	IP Address	Valid Time(min)	Active Time(min)	Description	Action

Show No.: 10 Total Count: 0

Whitelisted URL

(2) Set whitelisted users.

Click +Add Whitelisted User to set the IP address range and valid time for the whitelisted users. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254).

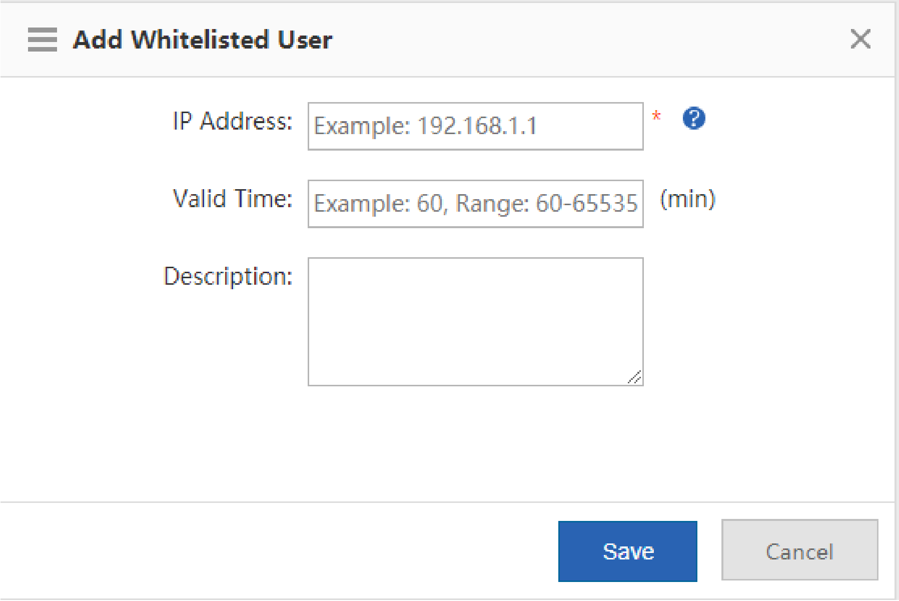


Whitelisted User

+Add Whitelisted User ✕Delete Selected

□	IP Address	Valid Time(min)	Active Time(min)	Description	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO



Add Whitelisted User ✕

IP Address: Example: 192.168.1.1 *

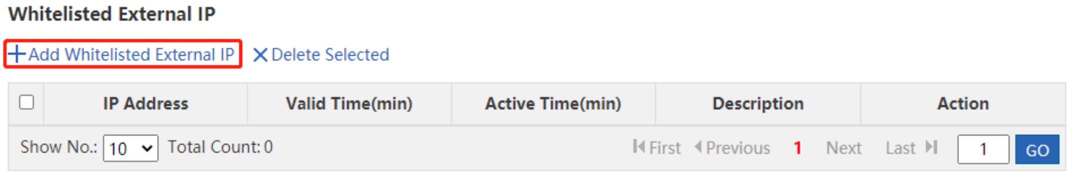
Valid Time: Example: 60, Range: 60-65535 (min)

Description:

Save Cancel

(3) Set whitelisted external IP addresses.

Click +Add Whitelisted External IP , input external IP addresses that can be accessed by users without authentication and input the valid time, and then click Save.

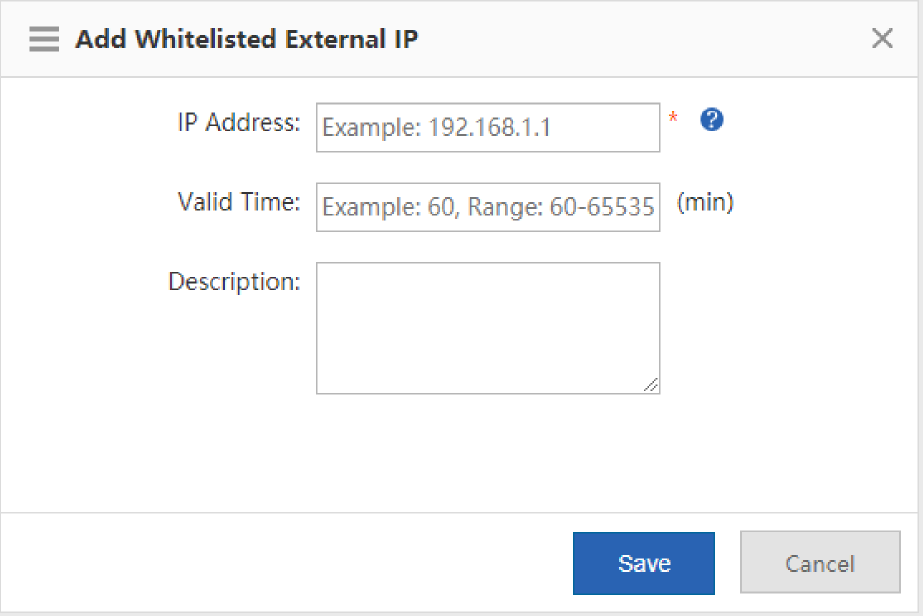


Whitelisted External IP

+Add Whitelisted External IP ✕Delete Selected

□	IP Address	Valid Time(min)	Active Time(min)	Description	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO


Add Whitelisted External IP

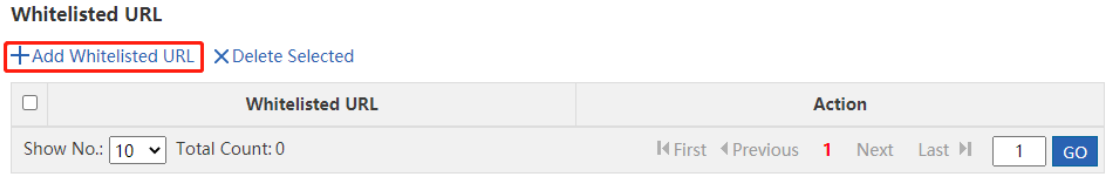
IP Address: Example: 192.168.1.1 *

Valid Time: Example: 60, Range: 60-65535 (min)

Description:

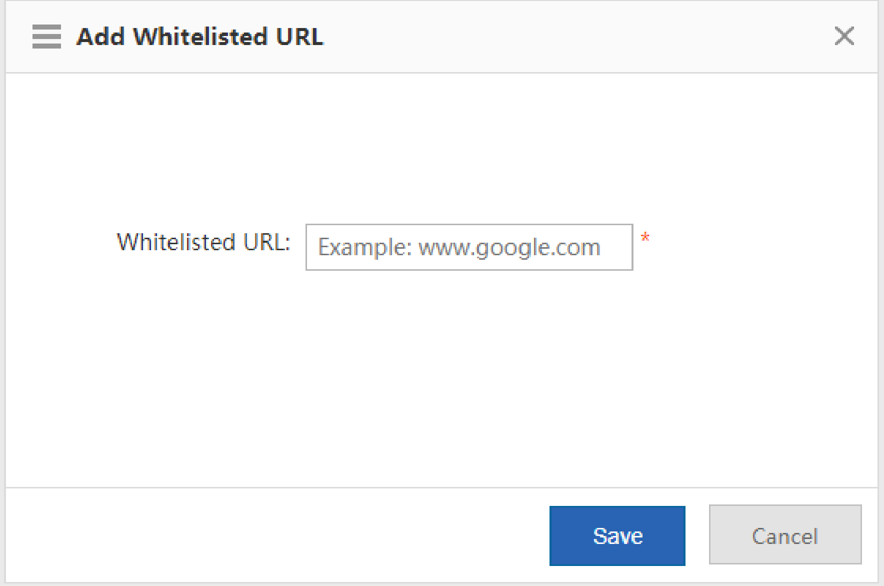
(4) Set a URL whitelist.

Click +Add Whitelisted URL , input the whitelisted URLs, and click Save. When the destination URL of the user is in the URL whitelist, traffic from the user will be permitted directly, regardless of whether the user passes authentication.


Whitelisted URL

□	Whitelisted URL	Action

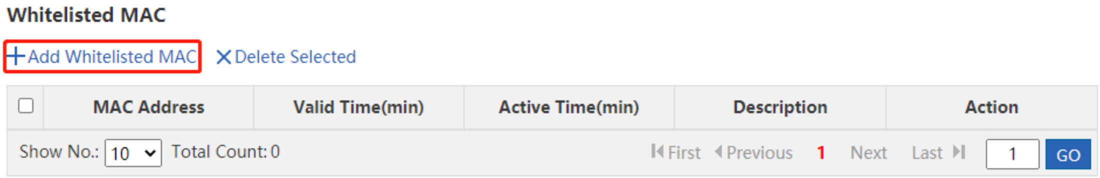
Show No.: 10 Total Count: 0


Add Whitelisted URL

Whitelisted URL: Example: www.google.com *

(5) Set a user MAC whitelist.

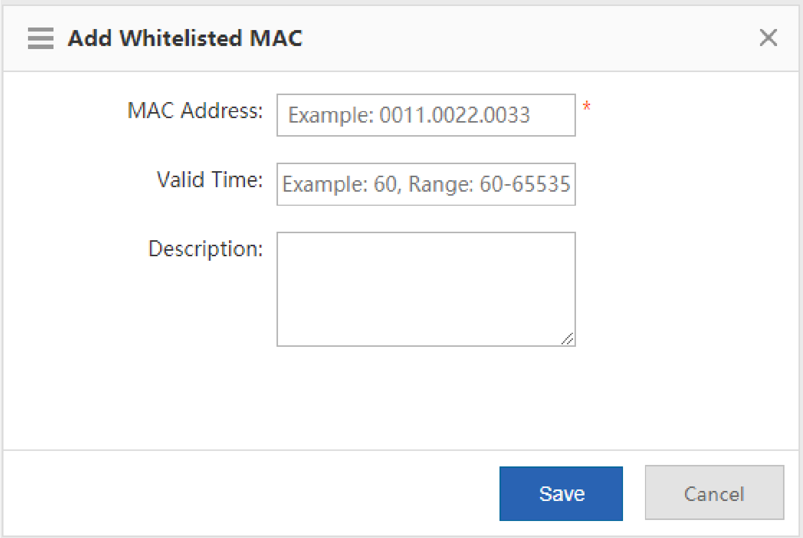
Click +Add Whitelisted MAC, input the MAC addresses of whitelisted users and the valid time, and then click Save.



Whitelisted MAC

□	MAC Address	Valid Time(min)	Active Time(min)	Description	Action

Show No.: 10 Total Count: 0



Add Whitelisted MAC

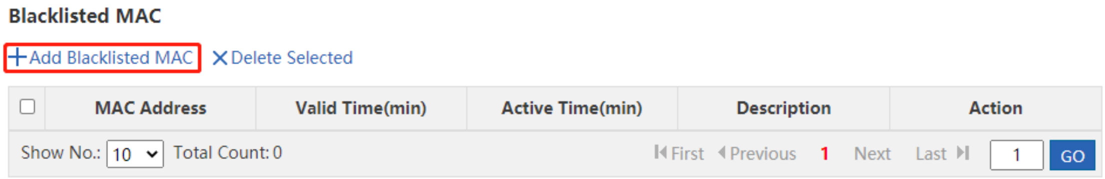
MAC Address: Example: 0011.0022.0033 *

Valid Time: Example: 60, Range: 60-65535

Description:

(6) Set a user MAC blacklist.

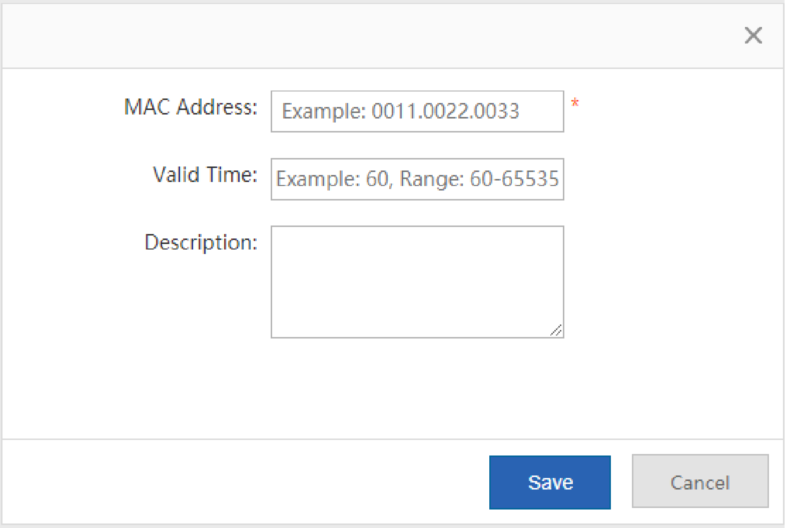
Click +Add Blacklisted MAC, input the MAC addresses of blacklisted users and the limit time, and then click Save.



Blacklisted MAC

□	MAC Address	Valid Time(min)	Active Time(min)	Description	Action

Show No.: 10 Total Count: 0

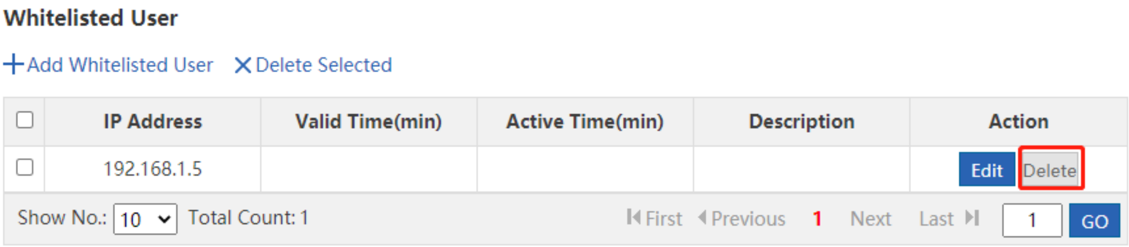


MAC Address: Example: 0011.0022.0033 *

Valid Time: Example: 60, Range: 60-65535

Description:

(7) To delete the whitelist configuration, click Delete in the **Action** column.



Whitelisted User

□	IP Address	Valid Time(min)	Active Time(min)	Description	Action
□	192.168.1.5				Edit Delete

Show No.: 10 Total Count: 1

6.3.5 User Permissions

Application Scenario

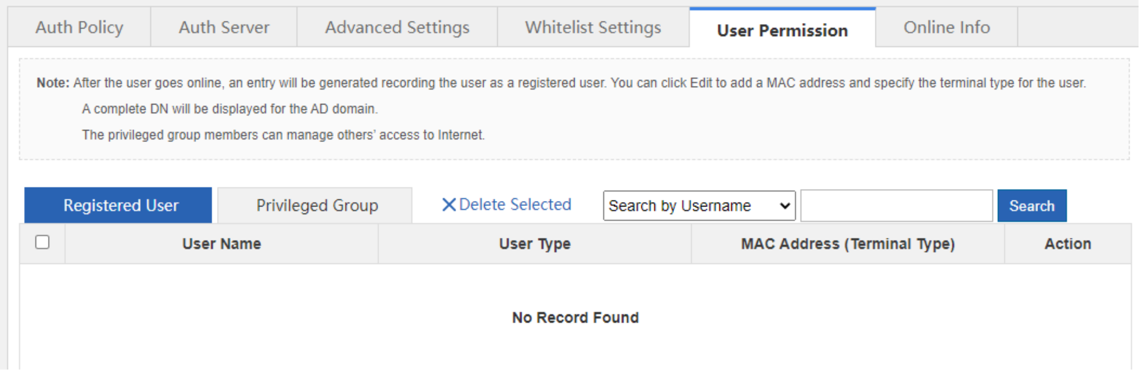
Set user permissions and specify a user that can grant access permissions to visitors.

Procedure

(1) Choose **User** > **Local Auth** > **User Permission**.

(2) The system displays information about registered users and users in the privileged group.

Registered users are entries generated after a user goes online. After a user is generated, click Edit to add a MAC address and specify the terminal type under this account.



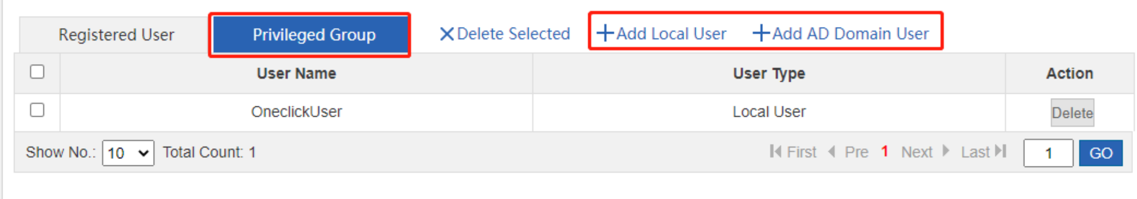
Note: After the user goes online, an entry will be generated recording the user as a registered user. You can click Edit to add a MAC address and specify the terminal type for the user.
A complete DN will be displayed for the AD domain.
The privileged group members can manage others' access to Internet.

□	User Name	User Type	MAC Address (Terminal Type)	Action

No Record Found

(3) Set users in a privileged group.

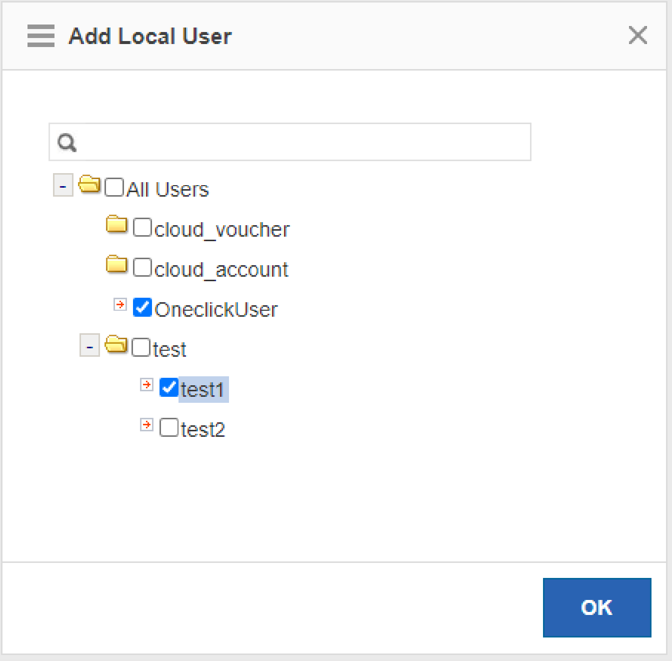
You can set users in a privileged group. Users in this group can grant access permissions to other users. Privileged groups are divided into the local user privileged group and AD domain user privileged group.



□	User Name	User Type	Action
□	OneclickUser	Local User	Delete

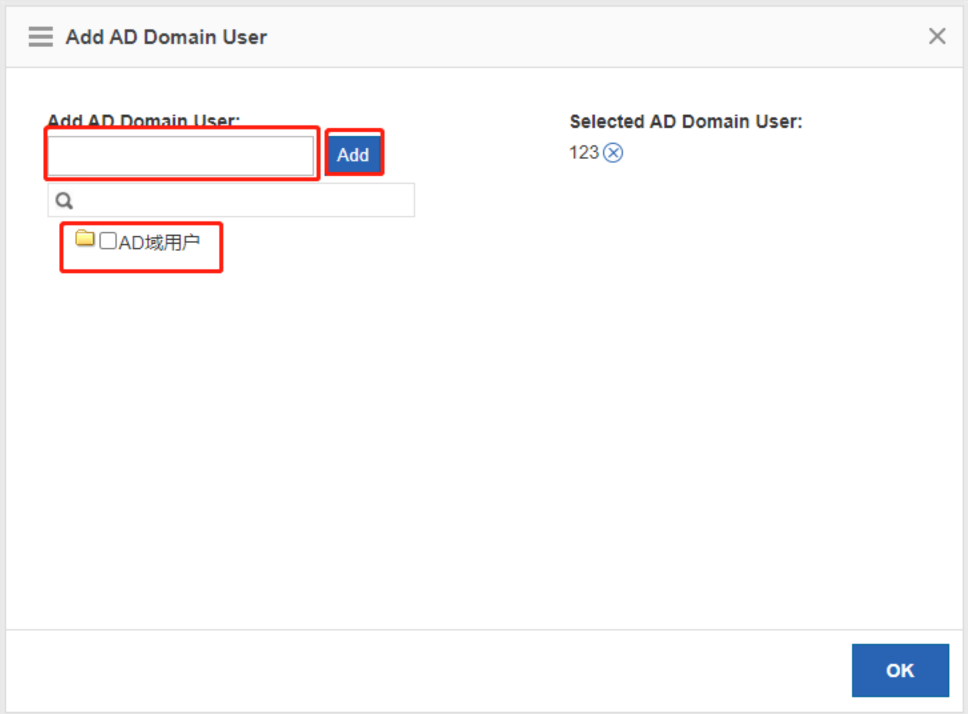
Show No.: 10 Total Count: 1

a Edit a local user privileged group: Click +Add Local User, select local users you want to add to the privileged group, and then click OK.



- □ All Users
  - □ cloud_voucher
  - □ cloud_account
  - ☑ OneclickUser
  - □ test
    - ☑ test1
    - □ test2

b Edit an AD domain user privileged group: Click +Add AD Domain User, select AD domain users from the tree that you want to add to the privileged group, or input user names in the text box, and then click Add. Finally, click OK.



6.3.6 Online Information

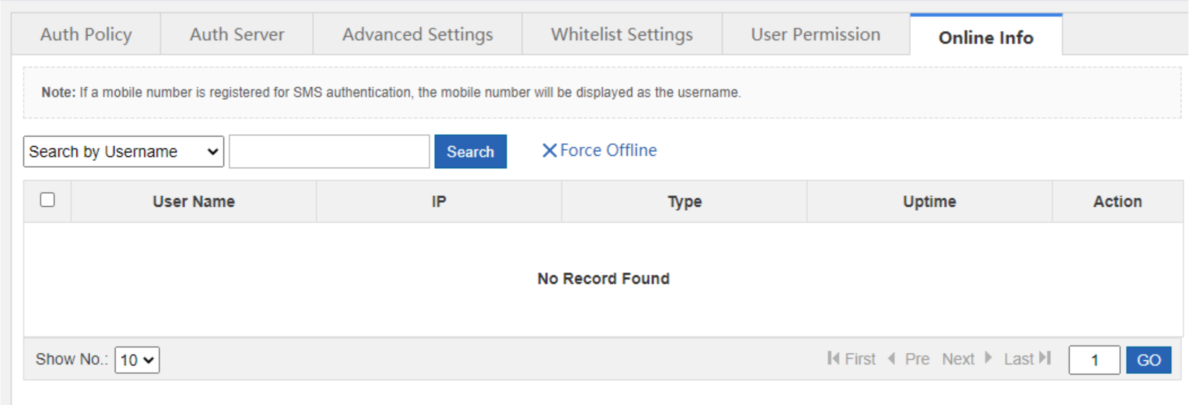
Application Scenario

This function allows you to get details of online users.

Procedure

(1) Choose **User** > **Local Auth** > **Online Info**.

(2) The system displays information of online users. You can query details of a specific online user by user name or IP address. You can click ✕Force Offline to force an online user offline.



Note: If a mobile number is registered for SMS authentication, the mobile number will be displayed as the username.

□	User Name	IP	Type	Uptime	Action
			No Record Found		

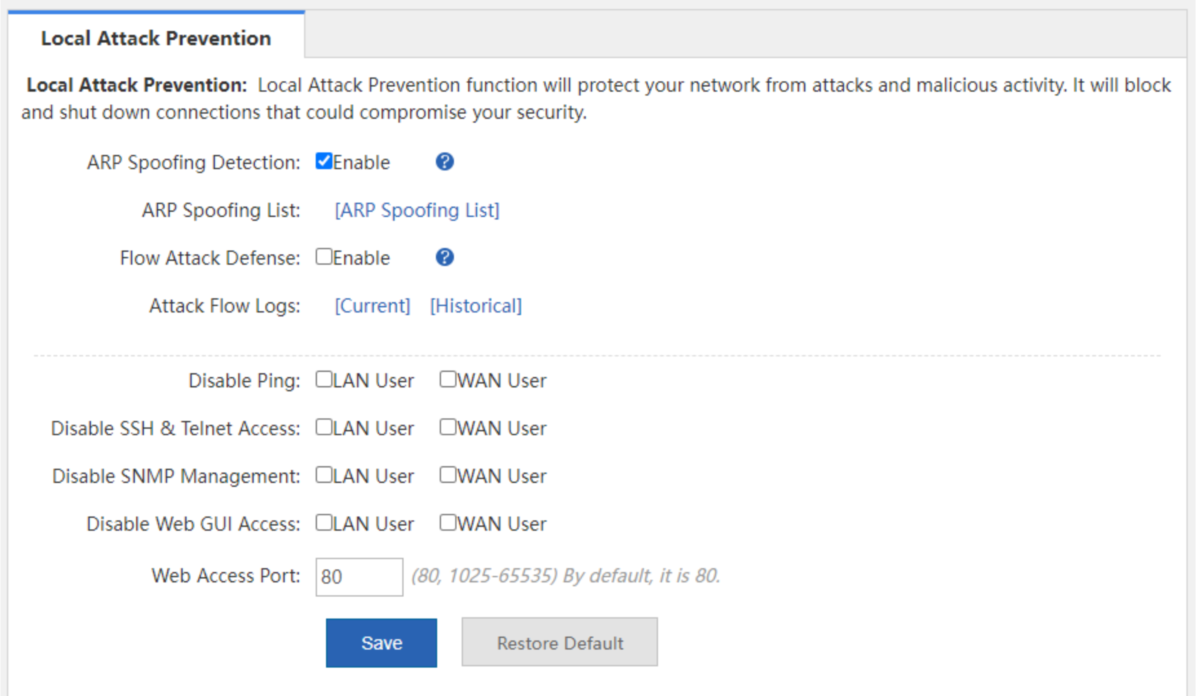
6.4 Local Attack Prevention

Application Scenario

The Local Attack Prevention function allows you to classify, filter, and limit the rate of data packets to be processed at the control layer. It can prevent attacks and protect key resources at the control layer.

Procedure

(1) Choose **Security** > **Local Attack Prevention**.



Local Attack Prevention: Local Attack Prevention function will protect your network from attacks and malicious activity. It will block and shut down connections that could compromise your security.

ARP Spoofing Detection: ☑Enable

ARP Spoofing List: [ARP Spoofing List]

Flow Attack Defense: □Enable

Attack Flow Logs: [Current] [Historical]

Disable Ping: □LAN User □WAN User

Disable SSH & Telnet Access: □LAN User □WAN User

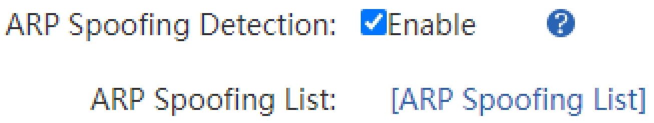
Disable SNMP Management: □LAN User □WAN User

Disable Web GUI Access: □LAN User □WAN User

Web Access Port: 80 *(80, 1025-65535) By default, it is 80.*

(2) Set an policy.

ARP attacks are targeted at Ethernet Address Resolution Protocol (ARP). Such attacks help attackers obtain or even tamper with data packets in a LAN and make a specific computer or all computers on the network unable to be connected.



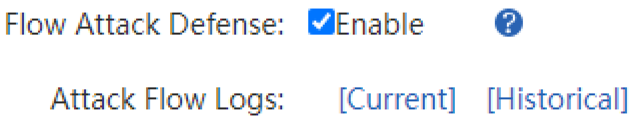
ARP Spoofing Detection: ☑Enable

ARP Spoofing List: [ARP Spoofing List]

- ARP spoofing detection: You can enable ARP Spoofing Detection: ☑Enable to prevent hackers from eavesdropping on all IP or MAC addresses in the network and pretending to be a PC in the network for ARP spoofing.

- View the ARP spoofing list: You can click [ARP Spoofing List] to view the list of hosts suspected of ARP spoofing in the current system.

(3) Set a flow attack defense policy.



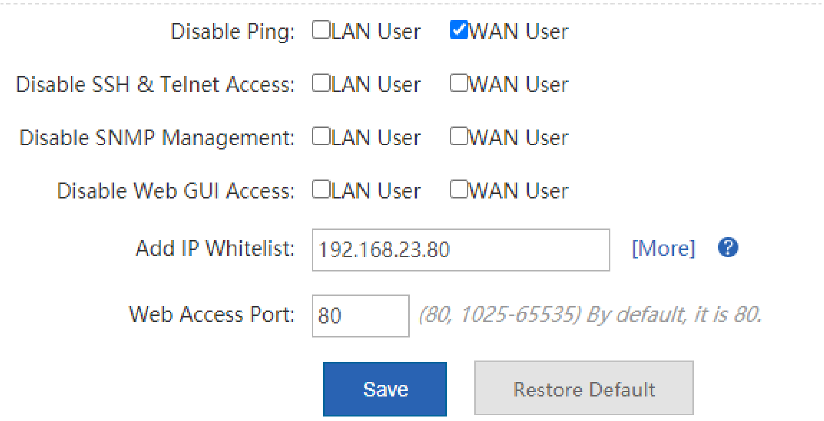
Flow Attack Defense: ☑Enable

Attack Flow Logs: [Current] [Historical]

Flow Attack Defense: Enable Flow Attack Defense: ☑Enable . If the packets of the process exceed the threshold, the packets will be discarded. The threshold is 200 packets per second on average. 300 packets can be sent per second in emergency cases.

Attack Flow Logs: Click [Current] to view the logs of current attacks of the system or click [Historical] to view the logs of historical attacks of the system.

(4) Set other anti-attack policies.



Disable Ping: □LAN User ☑WAN User

Disable SSH & Telnet Access: □LAN User □WAN User

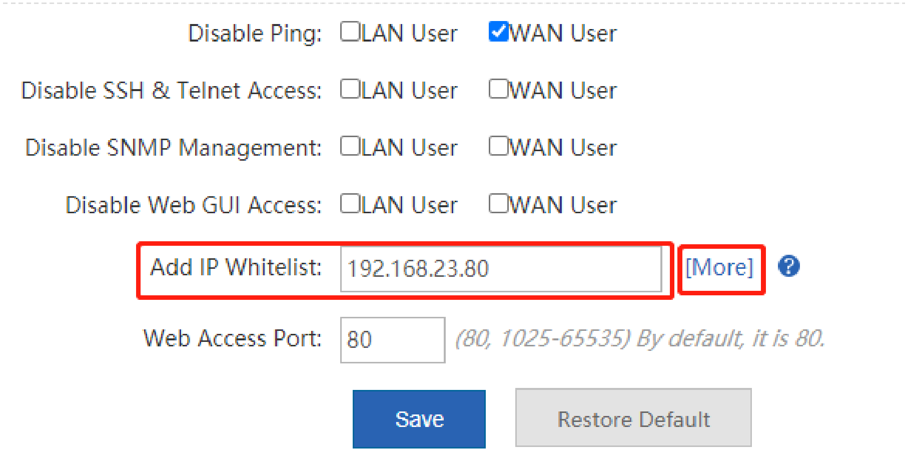
Disable SNMP Management: □LAN User □WAN User

Disable Web GUI Access: □LAN User □WAN User

Add IP Whitelist: 192.168.23.80 [More] ?

Web Access Port: 80 *(80, 1025-65535) By default, it is 80.*

- **Disable Web GUI Access**: After Disable Web GUI Access: □LAN User is enabled, internal network users cannot log into the web system of this device. After ☑WAN User is enabled, external network users cannot log into the web system of this device.
- **Add IP Whitelist**: The IP address input here must be the IP address of the administrator which is not affected by the rate limiting policy. This can improve the device management efficiency of the administrator. You can click [More] to view and manage more information:



Disable Ping: □LAN User ☑WAN User

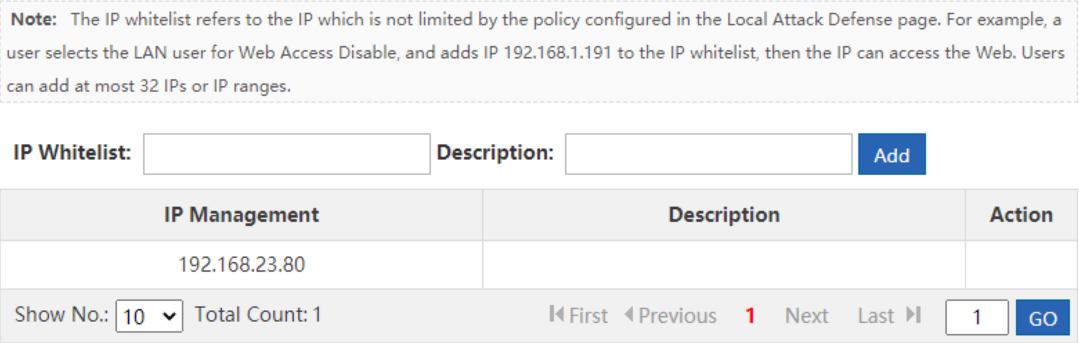
Disable SSH & Telnet Access: □LAN User □WAN User

Disable SNMP Management: □LAN User □WAN User

Disable Web GUI Access: □LAN User □WAN User

Add IP Whitelist: 192.168.23.80 [More] ?

Web Access Port: 80 *(80, 1025-65535) By default, it is 80.*



Note: The IP whitelist refers to the IP which is not limited by the policy configured in the Local Attack Defense page. For example, a user selects the LAN user for Web Access Disable, and adds IP 192.168.1.191 to the IP whitelist, then the IP can access the Web. Users can add at most 32 IPs or IP ranges.

IP Whitelist: **Description:**

IP Management	Description	Action
192.168.23.80		

- **Disable Ping**: You can select Disable Ping: ☑LAN User and ☑WAN User to prevent internal network users or external network users from pinging the same device. This function can filter out some malicious packets because some packets will no longer intrude on the system when they find that the system cannot be pinged.
- **Web Access Port**: The default port is 80. If you have modified the port ID, you must add the port ID in the address bar and then you can access the device via the URL http://IP address: access port ID.

(5) Click Save.

6.5 Interface Access Control

Application Scenario

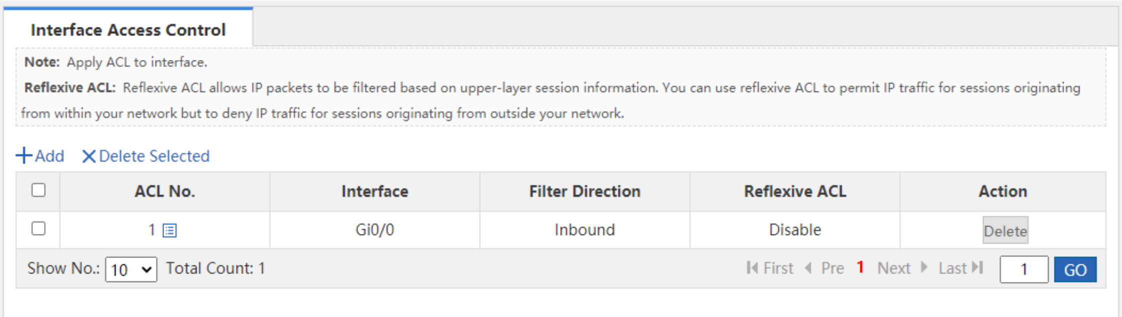
You can apply an ACL to a device interface to control inbound and outbound packets of the interface, so as to improve the network device security.

Prerequisites

You can configure an ACL. For details, see 6.7 ACL.

Procedure

(1) Choose **Security** > **Interface**.



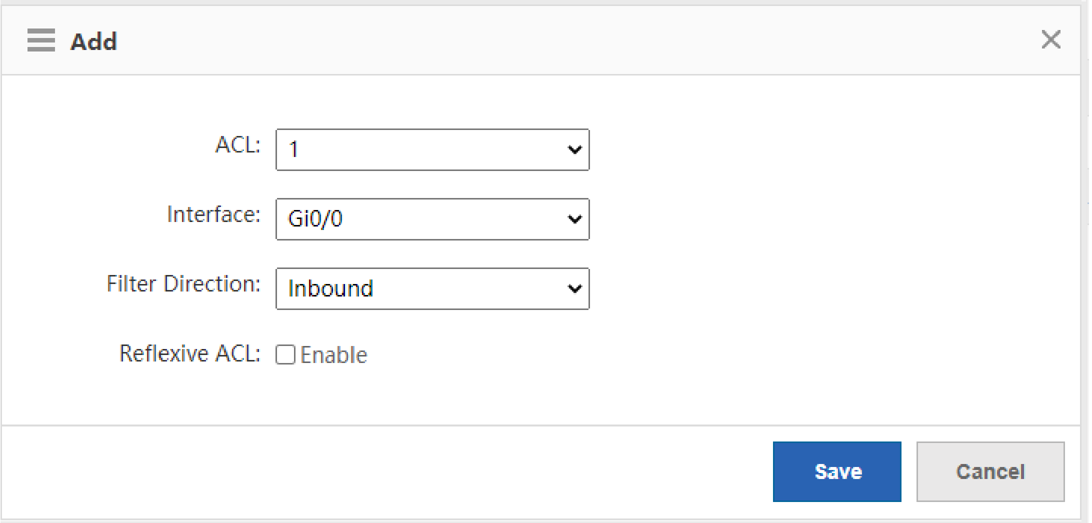
Interface Access Control

Note: Apply ACL to interface.

Reflexive ACL: Reflexive ACL allows IP packets to be filtered based on upper-layer session information. You can use reflexive ACL to permit IP traffic for sessions originating from within your network but to deny IP traffic for sessions originating from outside your network.

□	ACL No.	Interface	Filter Direction	Reflexive ACL	Action
□	1	Gi0/0	Inbound	Disable	Delete

(2) Click +Add to add an interface access control rule.



ACL: 1

Interface: Gi0/0

Filter Direction: Inbound

Reflexive ACL: □ Enable

a Select the number of the ACL you want to apply and the matching interface.

b Set a packet filter direction. Options are Inbound and Outbound.

c Click **Save**. Then, the access control rule is applied to the interface and serves as a firewall.

The firewall supports ACLs based on status tracing. After Reflexive ACL: ☑ Enable is selected, you can trace network disconnections and allow reflexive traffic to enter the network again.

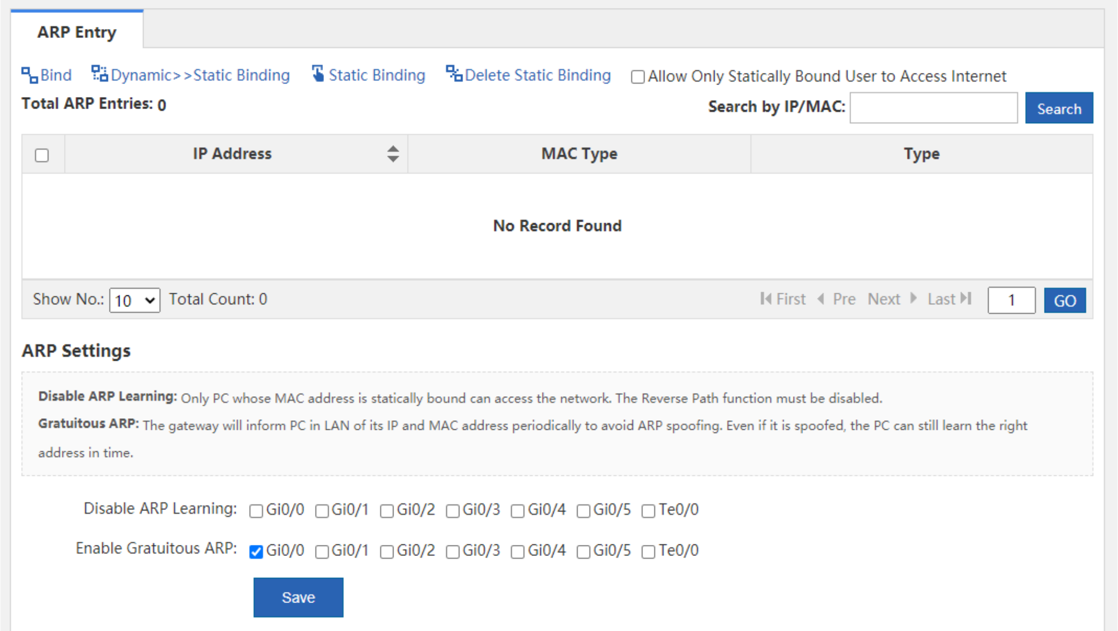
6.6 ARP Entries

Application Scenario

The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. You can bind ARP mapping entries and enable gratuitous ARP to restrict Internet access of LAN hosts, prevent ARP spoofing, and improve network security.

Procedure

(1) Choose **Security** > **ARP**.



ARP Entry

Bind   Dynamic>>Static Binding   Static Binding   Delete Static Binding   □ Allow Only Statically Bound User to Access Internet

Total ARP Entries: 0   Search by IP/MAC: [ ] Search

□	IP Address	MAC Type	Type
No Record Found			

Show No.: 10   Total Count: 0   First Pre Next Last 1 GO

ARP Settings

Disable ARP Learning: Only PC whose MAC address is statically bound can access the network. The Reverse Path function must be disabled.
Gratuitous ARP: The gateway will inform PC in LAN of its IP and MAC address periodically to avoid ARP spoofing. Even if it is spoofed, the PC can still learn the right address in time.

Disable ARP Learning: □Gi0/0 □Gi0/1 □Gi0/2 □Gi0/3 □Gi0/4 □Gi0/5 □Te0/0

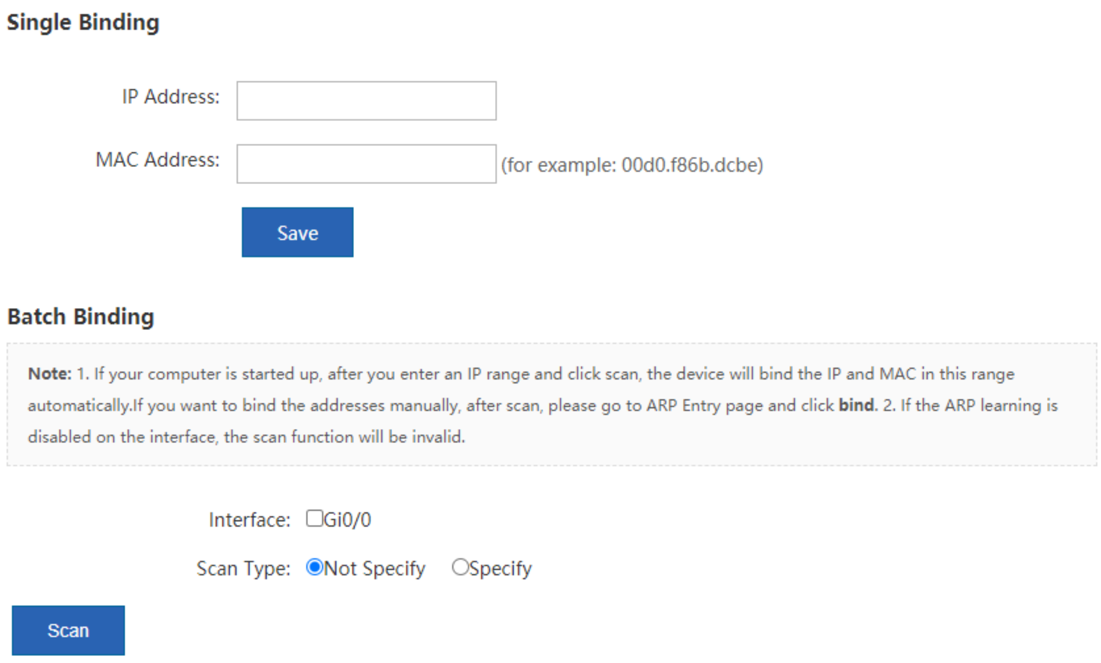
Enable Gratuitous ARP: ☑Gi0/0 □Gi0/1 □Gi0/2 □Gi0/3 □Gi0/4 □Gi0/5 □Te0/0

Save

(2) Bind static IP addresses/MAC addresses.

You can manually bind static IP addresses/MAC addresses one by one or bind addresses in batch by scanning.

- Click Static Binding and the following window is displayed:



Single Binding

IP Address: [ ]

MAC Address: [ ] (for example: 00d0.f86b.dcbe)

Save

Batch Binding

Note: 1. If your computer is started up, after you enter an IP range and click scan, the device will bind the IP and MAC in this range automatically.If you want to bind the addresses manually, after scan, please go to ARP Entry page and click **bind**. 2. If the ARP learning is disabled on the interface, the scan function will be invalid.

Interface: □Gi0/0

Scan Type: ●Not Specify ○Specify

Scan

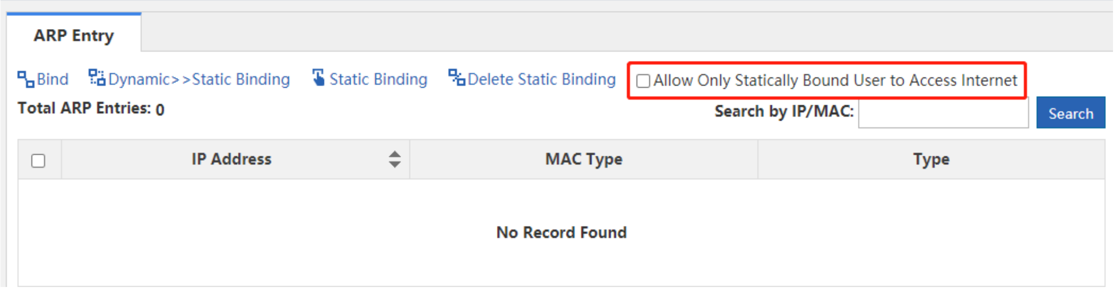
Single Binding: You just need to input the IP address and MAC address and then click Save.

Batch Binding: Select the external interface you want to scan, specify the address range to be scanned (if no address range is specified, the addresses of all computers in the network are scanned), and then click

Scan. The device automatically binds IP addresses and MAC addresses within the specified range. If ARP learning is disabled for the interface, the scanning function is invalid.

(3) Enable **Allow Only Statically Bound User to Access Internet**.

After this function is selected, the device only permits traffic of statically bound IP addresses and MAC addresses.



ARP Entry

Bind | Dynamic>>Static Binding | Static Binding | Delete Static Binding | □ Allow Only Statically Bound User to Access Internet

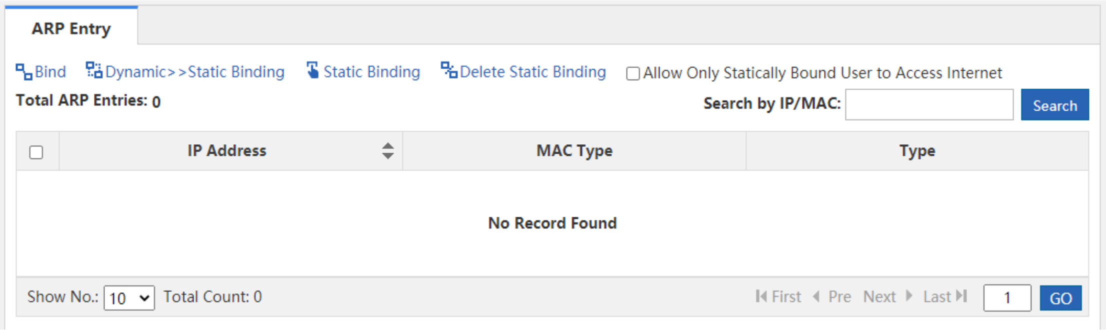
Total ARP Entries: 0

Search by IP/MAC: Search

□	IP Address	MAC Type	Type
	No Record Found		

Follow-up Procedure

- The ARP entry table displays the IP addresses and MAC addresses statically bound by a user or dynamically bound by the system.



ARP Entry

Bind | Dynamic>>Static Binding | Static Binding | Delete Static Binding | □ Allow Only Statically Bound User to Access Internet

Total ARP Entries: 0

Search by IP/MAC: Search

□	IP Address	MAC Type	Type
	No Record Found		

Show No.: 10 Total Count: 0 First Pre Next Last 1 GO

- Delete a statically bound address

  In the ARP entry table, select the statically bound IP address or MAC address you want to delete, and then click Delete Static Binding.

- Convert dynamic binding to static binding

  In the ARP entry table, select the dynamically bound IP address or MAC address you want to change, and then click Dynamic>>Static Binding.

- ARP function setting
  - **Disable ARP Learning**: Select the interface for which you want to disable ARP learning. Then PCs dynamically bound to this interface cannot access the Internet. Only PCs statically bound to this interface can access the Internet.
  - **Enable Gratuitous ARP**: When a network interface of the device serves as the router for downstream devices but a downstream device acts as a router, if gratuitous ARP is enabled, you can set a gratuitous ARP request periodically from this interface to advertise this interface is the real router.

6.7 ACL

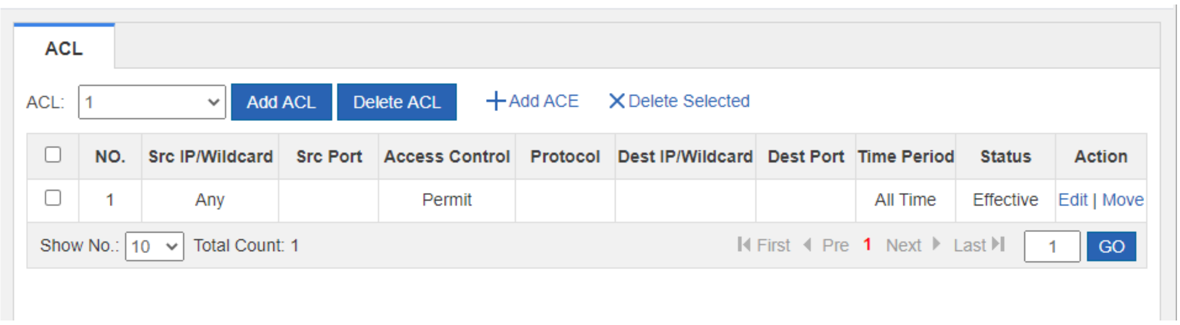
Application Scenario

An Access Control List (ACL) defines a series of **Permit** or **Deny** rules and applies these rules to a device interface to control inbound and outbound packets of the interface, so as to improve the network device security.

You can configure ACLs to ensure network security, reliability, and stability, prevent packet attacks, and control **network accesses.**

Procedure

(1) Choose **Security** > **ACL**.



□	NO.	Src IP/Wildcard	Src Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
□	1	Any		Permit				All Time	Effective	Edit | Move

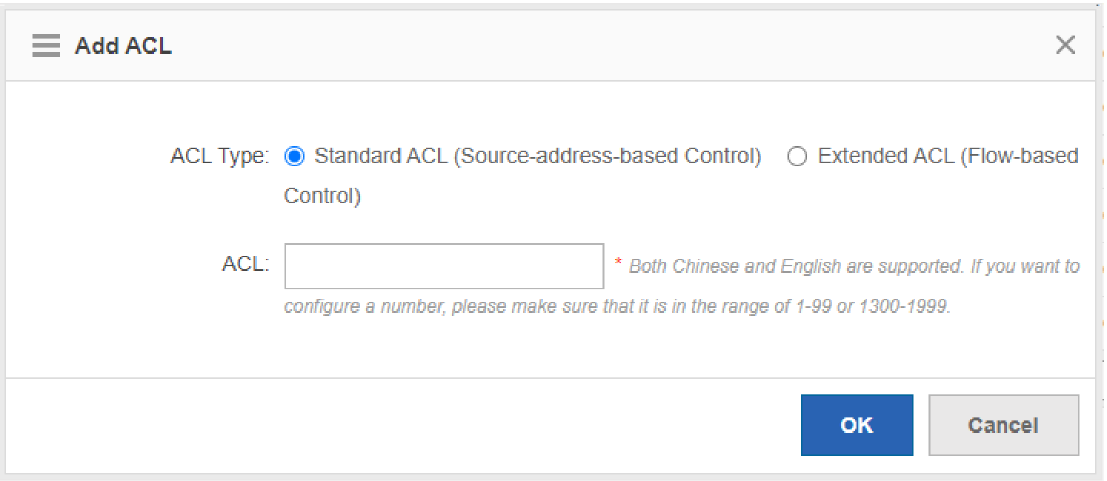
Show No.: 10 Total Count: 1

(2) Click Add ACL to add an ACL.

a Select the ACL type. Options are Standard ACL (Source-address-based Control) and **Extended ACL (Flow-based Control).**

b Input a name for the ACL.

c Click **OK**.

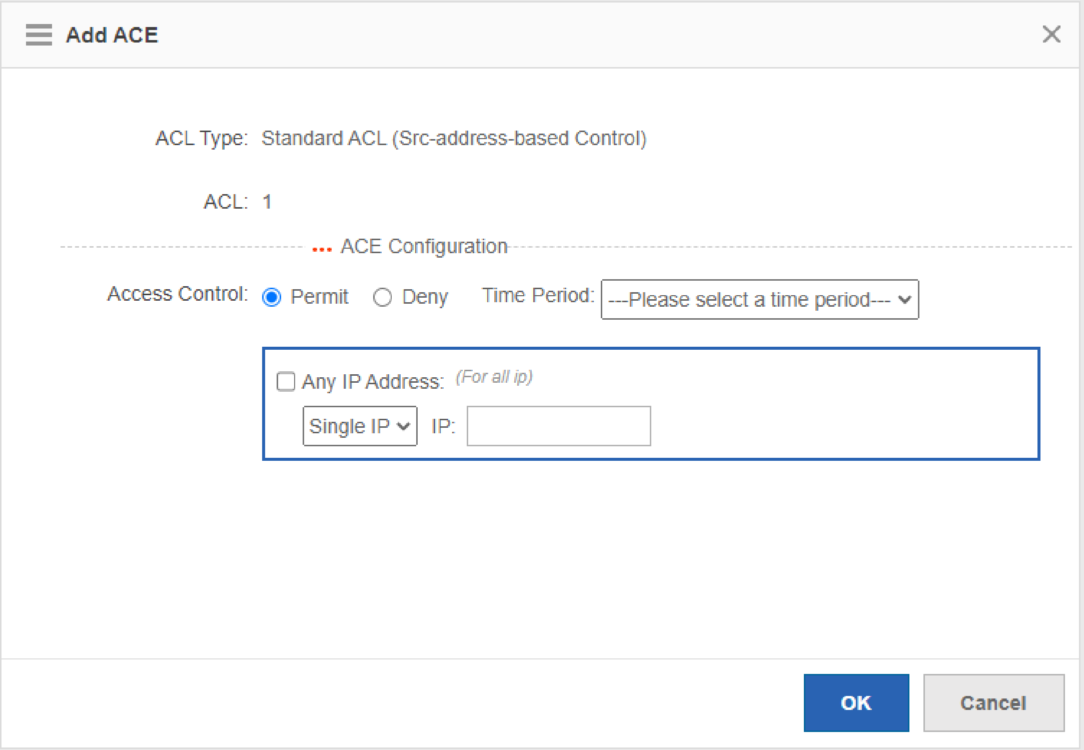


ACL Type: ● Standard ACL (Source-address-based Control) ○ Extended ACL (Flow-based Control)

ACL: * *Both Chinese and English are supported. If you want to configure a number, please make sure that it is in the range of 1-99 or 1300-1999.*

(3) Click +Add ACE. In the window displayed, set access control rules.

- **Standard ACL (Source-address-based Control)**: Select the access control action and time period, input the IP address, and then click OK. A standard ACL is then generated.



ACL Type: Standard ACL (Src-address-based Control)

ACL: 1

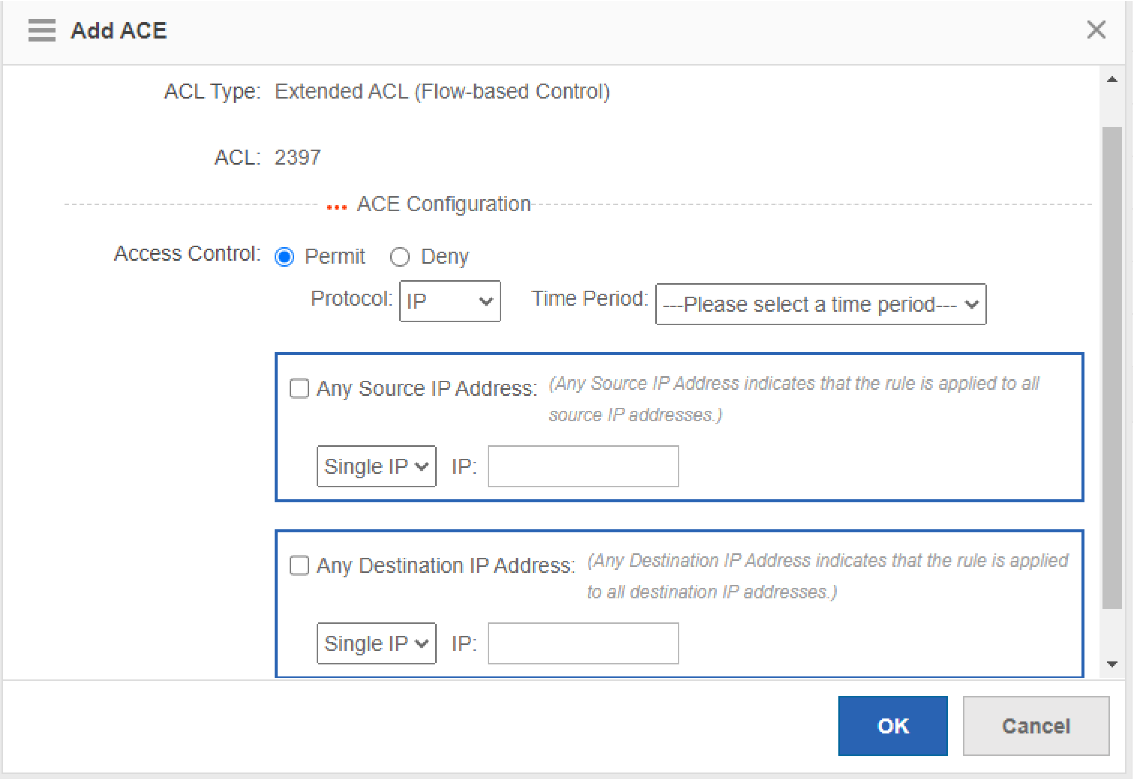
ACE Configuration

Access Control: ● Permit ○ Deny Time Period: ---Please select a time period---

□ Any IP Address: (For all ip)

Single IP IP:

- **Extended ACL (Flow-based Control**: Select the access control action, protocol type, and time period, configure the corresponding source and destination IP addresses and source and destination ports, and then click OK. An extended ACL is then generated.



ACL Type: Extended ACL (Flow-based Control)

ACL: 2397

ACE Configuration

Access Control: ● Permit ○ Deny

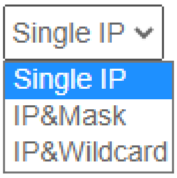
Protocol: IP Time Period: ---Please select a time period---

□ Any Source IP Address: (Any Source IP Address indicates that the rule is applied to all source IP addresses.)

Single IP IP:

□ Any Destination IP Address: (Any Destination IP Address indicates that the rule is applied to all destination IP addresses.)

Single IP IP:

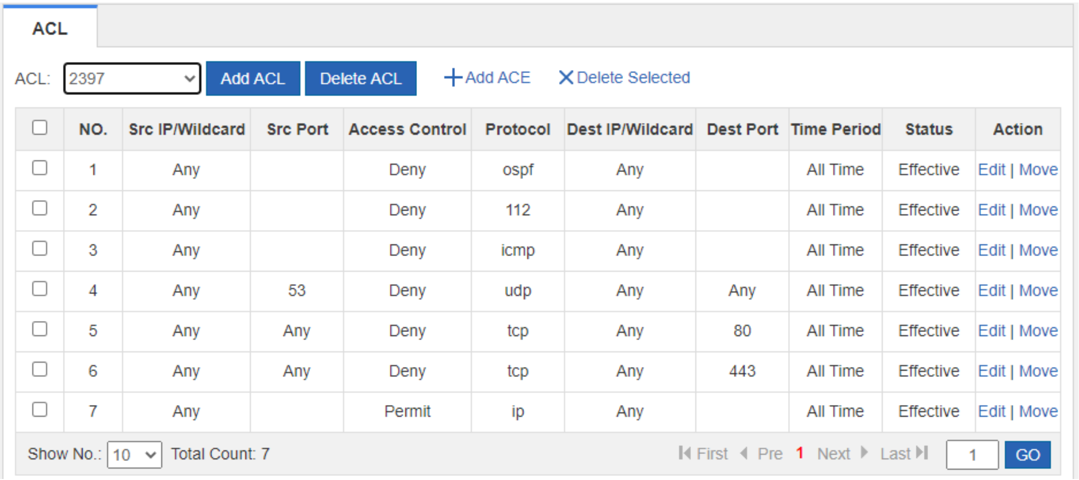
- You can select the source and destination IP address type from the drop-down list :
- **Single IP**: Input a single source or destination IP address.
- **IP&Mask**: Input the source or destination IP address ranges in the format of masks.
- **IP&Wildcard**: Input the source or destination IP address ranges in the format of wildcards.

Note

- You can set any source or destination IP addresses and source or destination ports.
- The wildcard masks specify which bits of an IP address will be ignored when this IP address is compared with other IP addresses. 1 in the wildcard masks indicates ignoring the corresponding bit in the IP address and 0 indicates retaining this bit. If the wildcard mask is omitted, 0.0.0.0 will be considered the default mask.

Follow-up Procedure

The system generates ACLs.



ACL

ACL: 2397 Add ACL Delete ACL +Add ACE ✕Delete Selected

□	NO.	Src IP/Wildcard	Src Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
□	1	Any		Deny	ospf	Any		All Time	Effective	Edit | Move
□	2	Any		Deny	112	Any		All Time	Effective	Edit | Move
□	3	Any		Deny	icmp	Any		All Time	Effective	Edit | Move
□	4	Any	53	Deny	udp	Any	Any	All Time	Effective	Edit | Move
□	5	Any	Any	Deny	tcp	Any	80	All Time	Effective	Edit | Move
□	6	Any	Any	Deny	tcp	Any	443	All Time	Effective	Edit | Move
□	7	Any		Permit	ip	Any		All Time	Effective	Edit | Move

Show No.: 10 Total Count: 7 First Pre 1 Next Last 1 GO

- Click Move to adjust the sequence of an ACL.
- Click Edit to edit the selected ACL.
- To delete an ACL, select the ACL you want to delete and then click ✕Delete Selected.

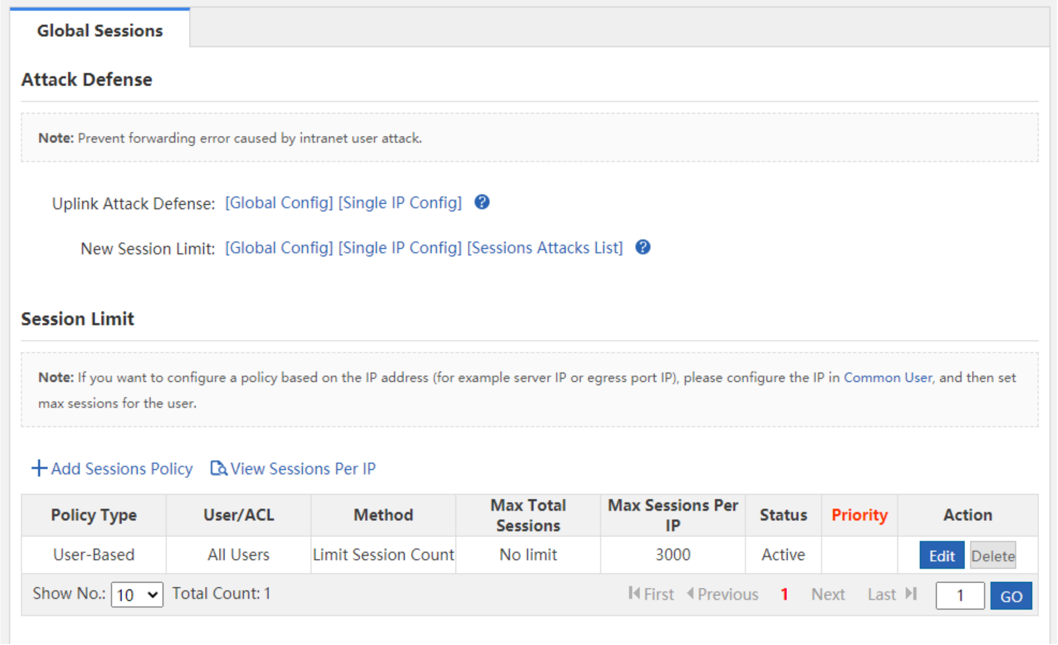
6.8 Limiting the Number of Connections

Application Scenario

This function allows you to limit the total number of sessions of the device, to avoid network lag because a user consumes excessive created connections while other users cannot connect to the network.

Procedure

(1) Choose **Security** > **Max Sessions**.



Global Sessions

Attack Defense

Note: Prevent forwarding error caused by intranet user attack.

Uplink Attack Defense: [Global Config] [Single IP Config]

New Session Limit: [Global Config] [Single IP Config] [Sessions Attacks List]

Session Limit

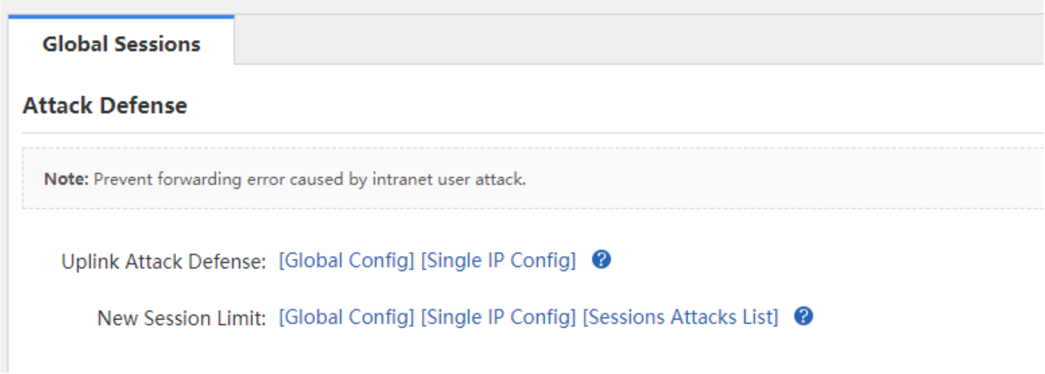
Note: If you want to configure a policy based on the IP address (for example server IP or egress port IP), please configure the IP in Common User, and then set max sessions for the user.

+Add Sessions Policy View Sessions Per IP

Policy Type	User/ACL	Method	Max Total Sessions	Max Sessions Per IP	Status	Priority	Action
User-Based	All Users	Limit Session Count	No limit	3000	Active		Edit Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

(2) Configure attack defense for the device.



Global Sessions

Attack Defense

Note: Prevent forwarding error caused by intranet user attack.

Uplink Attack Defense: [Global Config] [Single IP Config]

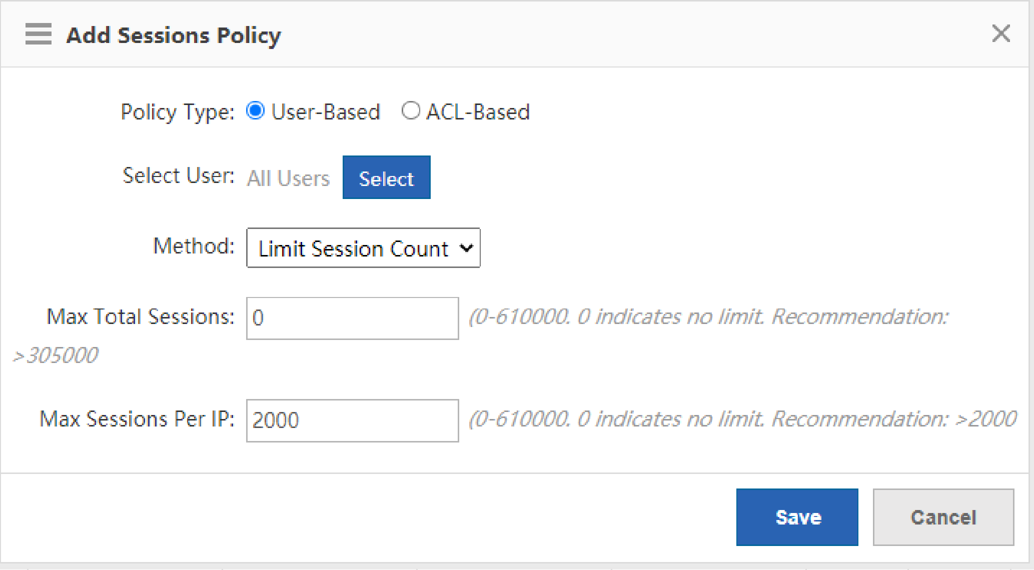
New Session Limit: [Global Config] [Single IP Config] [Sessions Attacks List]

- **Uplink Attack Defense**: Limit the packet uplink rate per second for internal network users to prevent uplink attacks against the internal network. You can limit the rate for all users or for a single user.
- **New Session Limit**: Limit the number of new sessions created per second for internal network users to avoid sessions attack. You can limit the rate for all users or for a single user. Click [Sessions Attacks List] to view the list of hosts suspected of making sessions attack.

(3) Create a sessions limiting policy.

Click +Add Sessions Policy to create a sessions limiting policy. You can limit the number of sessions based on user or based on ACL.

- User-based sessions limiting policy:



Add Sessions Policy

Policy Type: ● User-Based ○ ACL-Based

Select User: All Users Select

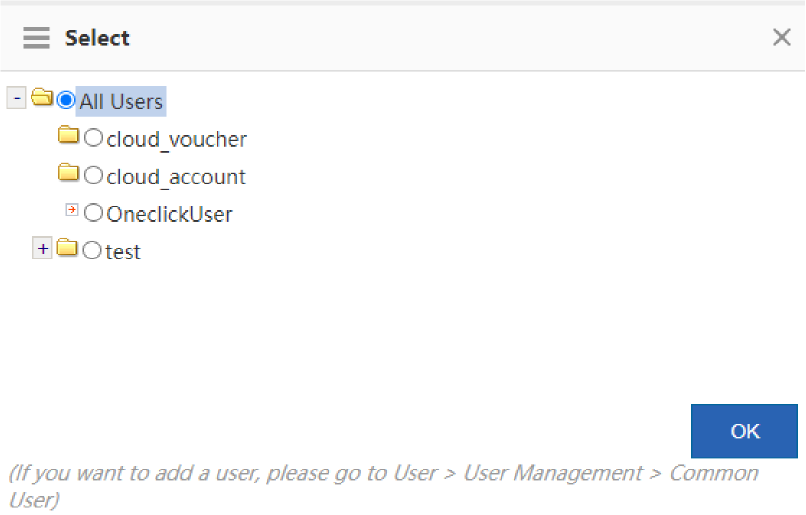
Method: Limit Session Count

Max Total Sessions: 0 *(0-610000. 0 indicates no limit. Recommendation: >305000*

Max Sessions Per IP: 2000 *(0-610000. 0 indicates no limit. Recommendation: >2000*

Save Cancel

a **Select User**: Click Select . In the **Select** window displayed, select users for which you want to limit the number of sessions, and then click OK.

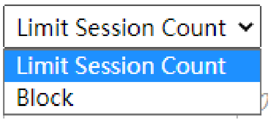


Select

- ● All Users
  - ○ cloud_voucher
  - ○ cloud_account
  - ○ OneclickUser
  - + ○ test

OK

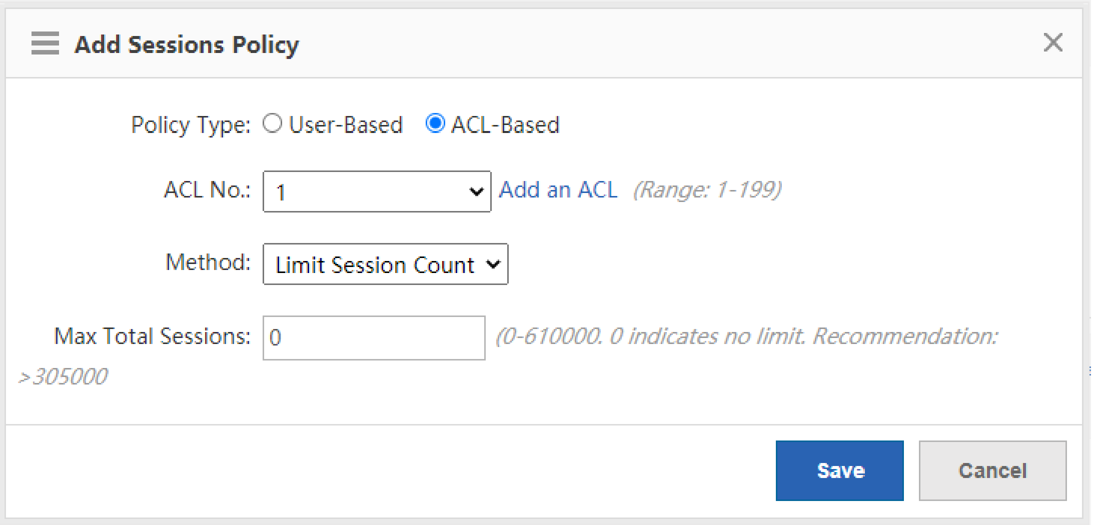
(If you want to add a user, please go to User > User Management > Common User)



b **Method**: Select a control method from the drop-down list . If **Block** is selected, selected users cannot access the Internet. If **Limit Session Count** is selected, you need to set the maximum number of sessions of all IP addresses and the maximum number of sessions of each IP address. The range is 1 to 200000, which depends on the specific product model.

c Click **Save**.

- User-ACL sessions limiting policy:



Add Sessions Policy

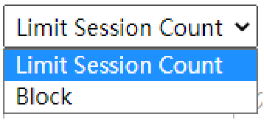
Policy Type: ○ User-Based ● ACL-Based

ACL No.: 1 Add an ACL *(Range: 1-199)*

Method: Limit Session Count

Max Total Sessions: 0 *(0-610000. 0 indicates no limit. Recommendation: >305000*

b **ACL No.**: Select an ACL No. available in the system from the drop-down list ACL No.: 1 . Or, you can click Add an ACL to create an ACL and configure it. For how to create an ACL, see 6.8 ACL.

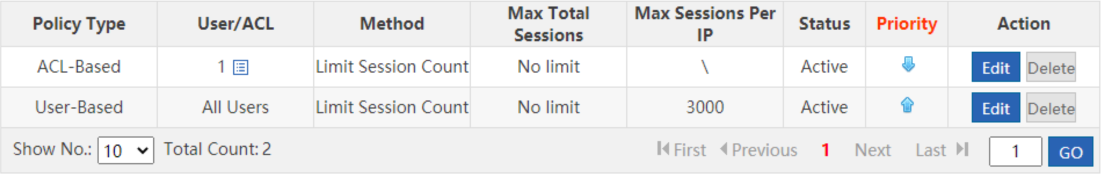


d **Method**: Select a control method from the drop-down list . If **Block** is selected, users to which the selected ACL is applied cannot access the Internet. If **Limit Session Count** is selected, you need to set the maximum number of sessions. The range is 1 to 200000, which depends on the specific product model.

e Click **Save**.

Follow-up Procedure

- The following figure lists sessions limiting policies.



Policy Type	User/ACL	Method	Max Total Sessions	Max Sessions Per IP	Status	Priority	Action
ACL-Based	1	Limit Session Count	No limit	\	Active	⇩	Edit Delete
User-Based	All Users	Limit Session Count	No limit	3000	Active	⇧	Edit Delete

Show No.: 10 Total Count: 2 First Previous 1 Next Last 1 GO

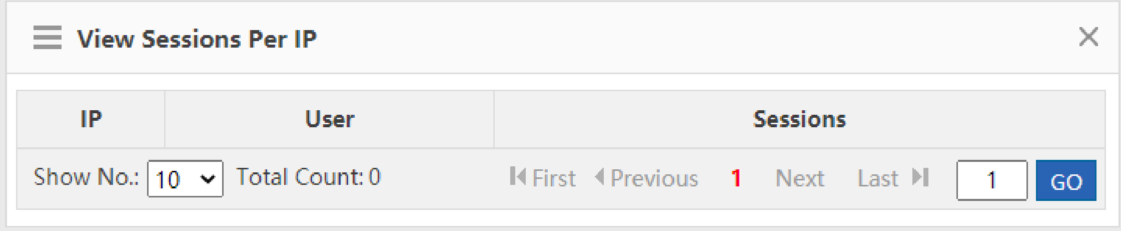
  - **Policy Type**: Indicate that the policy is based on ACL or user.
  - **Status**: Indicate whether the current policy is active.

The sessions limiting policies come into effect in descending order of configuration time. You can click ⇩ or ⇧ in the **Priority** column to adjust the priority of existing policies.

Click Edit to modify the policy and click Delete to delete the policy.

- View sessions per IP address

Click View Sessions Per IP to view the number of sessions per IP address when sessions limiting per IP address is enabled for the device.



View Sessions Per IP

IP	User	Sessions

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

6.9 Account Sharing Prevention

6.9.1 One-click Account Sharing Prevention

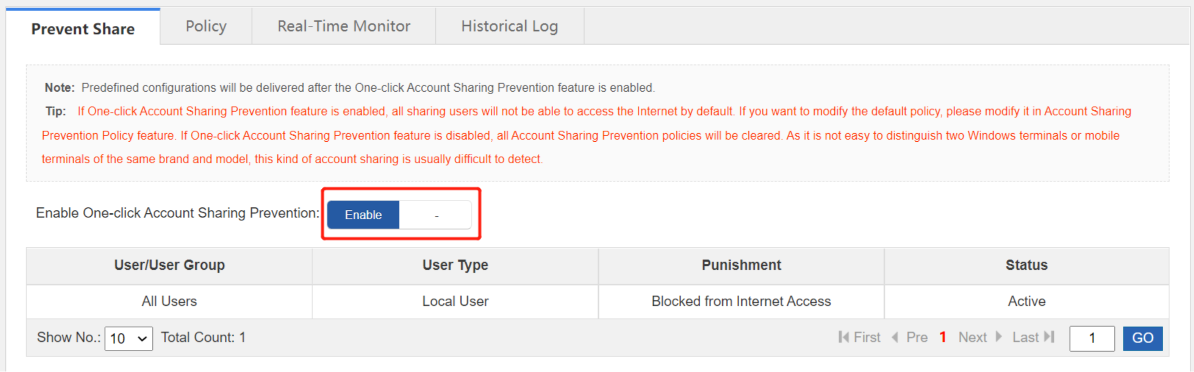
The device will deliver the configurations based on the predefined policy after the one-click account sharing prevention feature is enabled. You can add or modify the account sharing prevention policy on the **Policy** page.

If the one-click account sharing prevention is enabled, the device will only detect sharing users but not block Internet access, or block Internet access or limit Internet speed for the sharing users according to the punishment method configured in the policies. If this feature is disabled, all account sharing prevention policies will be cleared.

Procedure

(1) Choose **Security** > **Prevent Share** > **Prevent Share**.

(2) Turn on **Enable One-click Account Sharing Prevention**.



Note: Predefined configurations will be delivered after the One-click Account Sharing Prevention feature is enabled.

Tip: If One-click Account Sharing Prevention feature is enabled, all sharing users will not be able to access the Internet by default. If you want to modify the default policy, please modify it in Account Sharing Prevention Policy feature. If One-click Account Sharing Prevention feature is disabled, all Account Sharing Prevention policies will be cleared. As it is not easy to distinguish two Windows terminals or mobile terminals of the same brand and model, this kind of account sharing is usually difficult to detect.

Enable One-click Account Sharing Prevention: Enable

User/User Group	User Type	Punishment	Status
All Users	Local User	Blocked from Internet Access	Active

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 GO

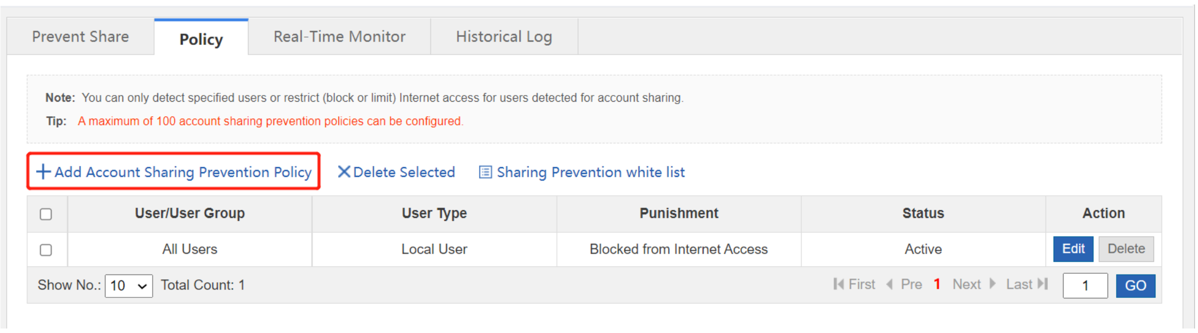
6.9.2 Account Sharing Prevention Policy

Through the account sharing prevention policy, you can detect specified users. You can also choose to only detect users but not block Internet access, or block Internet access or limit Internet speed for those sharing users.

Procedure

(1) Choose **Security** > **Prevent Share** > **Policy**.

(2) Click **Add Account Sharing Prevention Policy** to access the **Add Account Sharing Prevention Policy** page.



Prevent Share | **Policy** | Real-Time Monitor | Historical Log

Note: You can only detect specified users or restrict (block or limit) Internet access for users detected for account sharing.

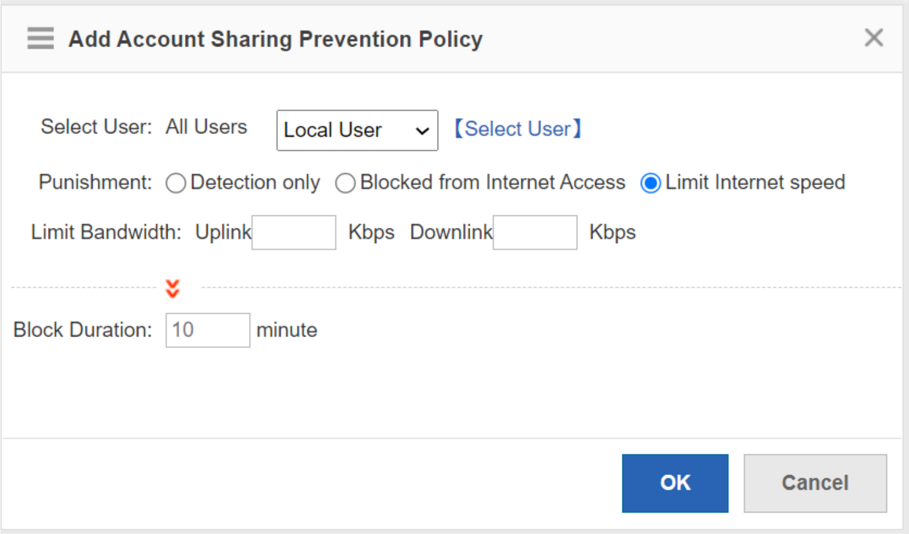
Tip: A maximum of 100 account sharing prevention policies can be configured.

+Add Account Sharing Prevention Policy ✕Delete Selected Sharing Prevention white list

□	User/User Group	User Type	Punishment	Status	Action
□	All Users	Local User	Blocked from Internet Access	Active	Edit Delete

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 GO

(3) Select the user and the punishment mode. Select **Detection only** to only detect whether the user accesses the Internet through account sharing. Select **Blocked from Internet Access** to block sharing users from Internet access. Select **Limit Internet speed** to limit Internet speed of sharing users.



Add Account Sharing Prevention Policy

Select User: All Users Local User 【Select User】

Punishment: ○ Detection only ○ Blocked from Internet Access ● Limit Internet speed

Limit Bandwidth: Uplink Kbps Downlink Kbps

Block Duration: 10 minute

OK Cancel

(4) Click **OK**.

(5) (Optional) Click **Sharing Prevention white list** to add users exempted from detection to the whitelist. The device will not detect the users in the whitelist.

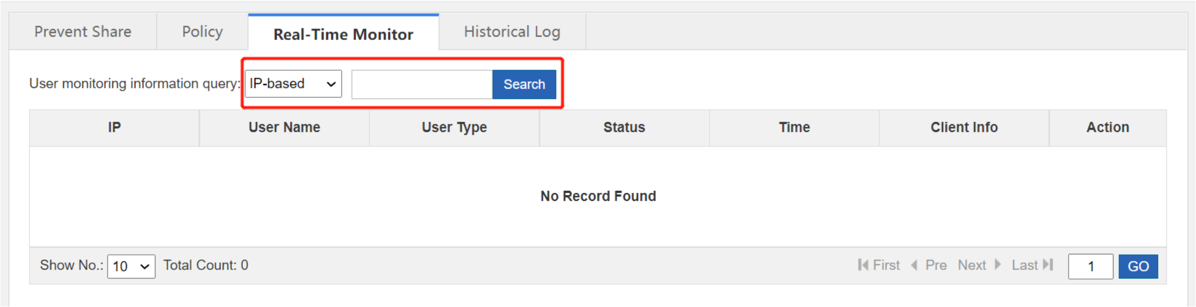
6.9.3 Real-Time Monitoring

The function is used to display the monitoring results and query the monitoring information based on the IP address, the user name, the user type, the user status, time, client information and the action.

Procedure

(1) Choose **Security** > **Prevent Share** > **Real-Time Monitor**.

(2) Select the query criterion from the drop-down list box and click **Search** to display the monitoring results.



Prevent Share | Policy | **Real-Time Monitor** | Historical Log

User monitoring information query: IP-based Search

IP	User Name	User Type	Status	Time	Client Info	Action
No Record Found						

Show No.: 10 Total Count: 0 First Pre Next Last 1 GO

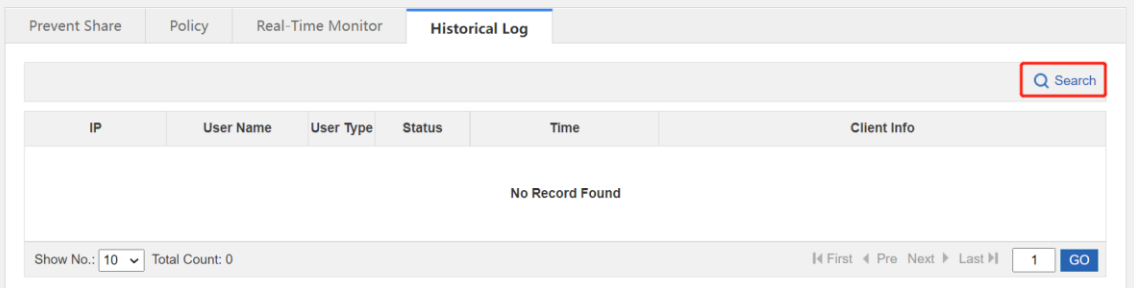
6.9.4 Historical Log

The function is used to display the historical logs.

Procedure

(1) Choose **Security** > **Prevent Share** > **Historical Log**.

(2) Click **Search** to configure filtering conditions for historical logs.

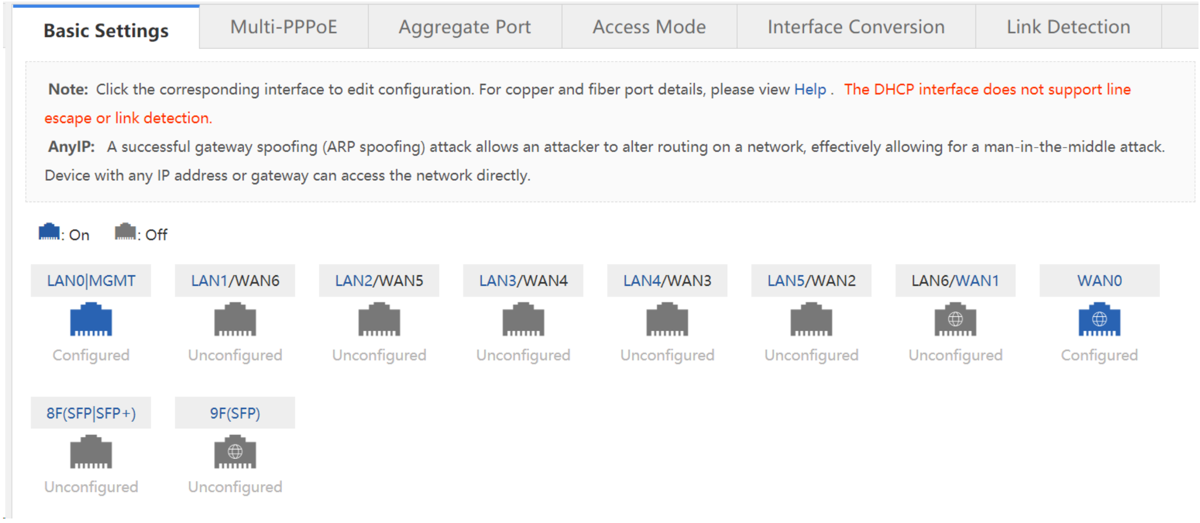


IP	User Name	User Type	Status	Time	Client Info
No Record Found					

7 Network

7.1 Interface Configuration

Interface configuration is the key configuration for intranet access, and its correctness is related to normal intranet access. The following figure shows the interface configuration page.



Basic Settings | Multi-PPPoE | Aggregate Port | Access Mode | Interface Conversion | Link Detection

Note: Click the corresponding interface to edit configuration. For copper and fiber port details, please view Help . The DHCP interface does not support line escape or link detection.

AnyIP: A successful gateway spoofing (ARP spoofing) attack allows an attacker to alter routing on a network, effectively allowing for a man-in-the-middle attack. Device with any IP address or gateway can access the network directly.

■: On □: Off

LAN0|MGMT	LAN1/WAN6	LAN2/WAN5	LAN3/WAN4	LAN4/WAN3	LAN5/WAN2	LAN6/WAN1	WAN0
Configured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Configured

8F(SFP|SFP+)	9F(SFP)
Unconfigured	Unconfigured

If the icon corresponding to an interface is highlighted in blue like this ( ), the interface is powered on (the network cable is connected). A grayscale icon ( ) indicates that the corresponding interface is not powered on. If the icon has a small globe, the corresponding interface is an extranet port. Otherwise, it is an intranet port.

Interface configuration varies with the mode (router or bridge), which will be described separately below.

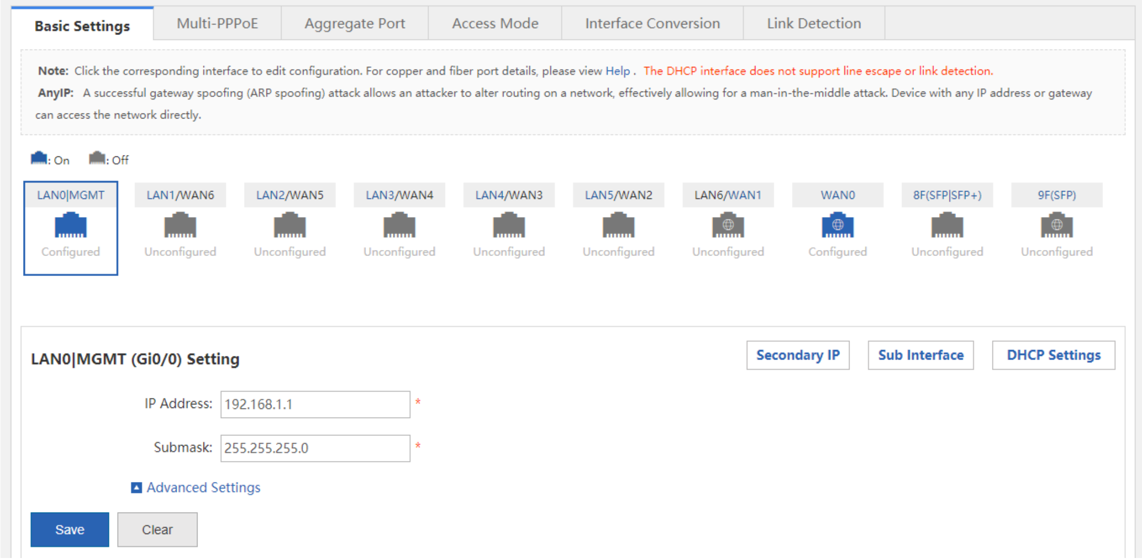
7.1.1 Basic Settings

Application Scenario

This operation allows you to configure various interfaces of the device.

Procedure

(1) Choose **Network** > **Interface** > **Basics Settings**.



Note: Click the corresponding interface to edit configuration. For copper and fiber port details, please view Help . The DHCP interface does not support line escape or link detection.

AnyIP: A successful gateway spoofing (ARP spoofing) attack allows an attacker to alter routing on a network, effectively allowing for a man-in-the-middle attack. Device with any IP address or gateway can access the network directly.

■: On ■: Off

LAN0|MGMT	LAN1/WAN6	LAN2/WAN5	LAN3/WAN4	LAN4/WAN3	LAN5/WAN2	LAN6/WAN1	WAN0	8F(SFP|SFP+)	9F(SFP)
Configured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Unconfigured	Configured	Unconfigured	Unconfigured

LAN0|MGMT (Gi0/0) Setting

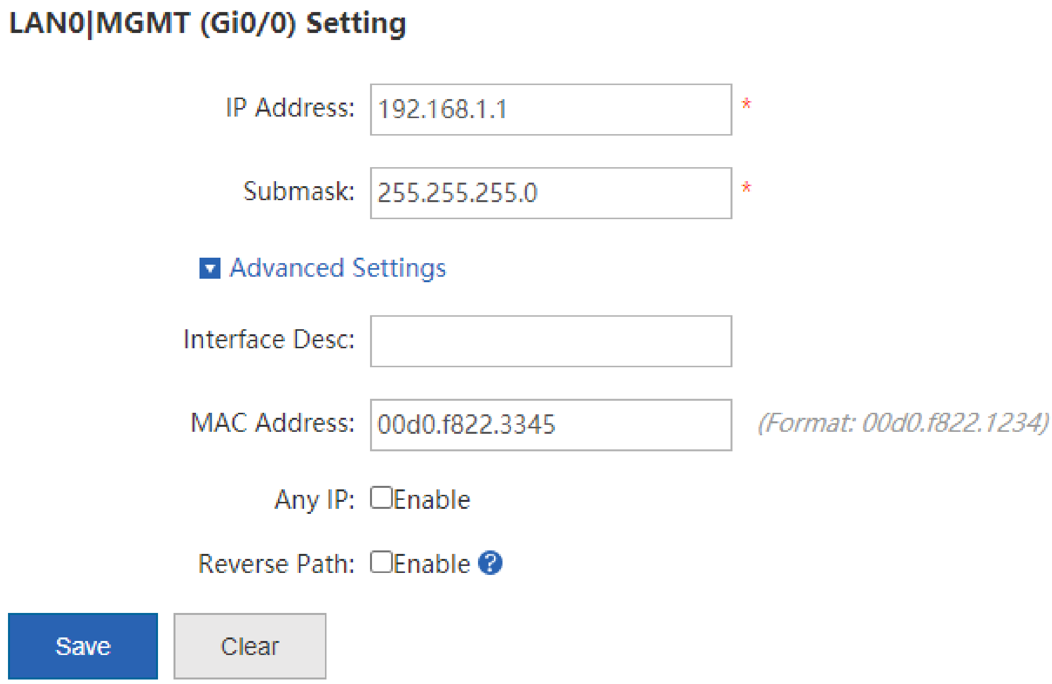
IP Address: 192.168.1.1 *

Submask: 255.255.255.0 *

Advanced Settings

(2) Configure an intranet port.

a Click the icon (for example, ▆) corresponding to the intranet port to be configured.



LAN0|MGMT (Gi0/0) Setting

IP Address: 192.168.1.1 *

Submask: 255.255.255.0 *

▼ Advanced Settings

Interface Desc:

MAC Address: 00d0.f822.3345 *(Format: 00d0.f822.1234)*

Any IP: □Enable

Reverse Path: □Enable ?

b Set the IP address and subnet mask.

IP Address: IP address of the intranet port, which is the router IP address in the planned network segment of the intranet.

Submask: mask corresponding to the network segment.

c Expand **Advanced Settings** and set other configuration items corresponding to the LAN port.

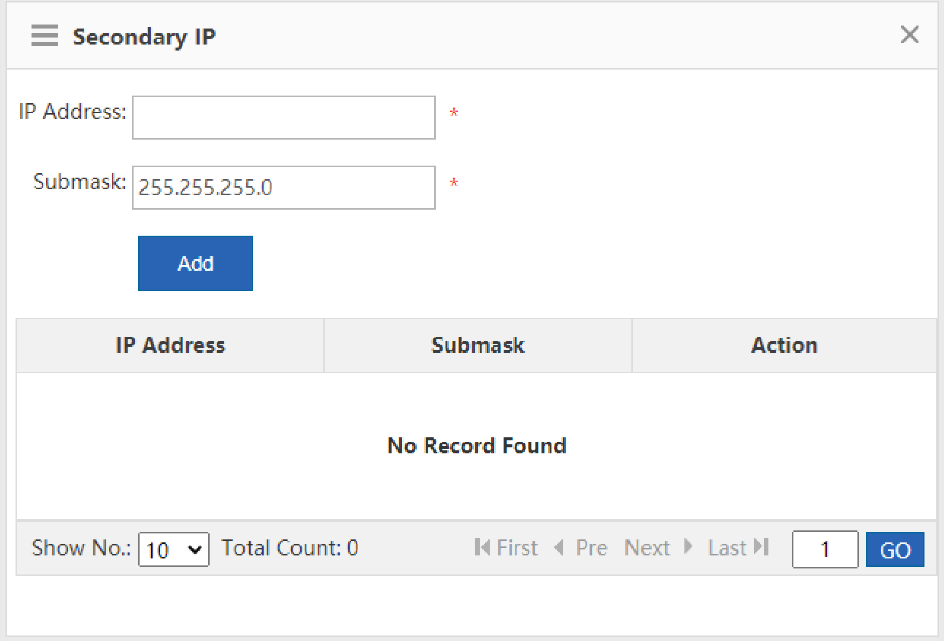
MAC Address: physical address of the interface, which is mainly used to prevent internal physical addresses from conflicting with each other. Generally, it can be left unset.

Any IP: If this function is enabled, normal network access is available with random IP address configuration or without IP address configuration for the intranet PC. That is, this function allows normal network access for some PCs when the IP addresses are incorrectly set.

Reverse Path: If this function is enabled, the incoming packets from the CERNET interface still go out through the CERNET interface, and the routing table will not be queried when response packets are sent. This prevents the scenario where it is found by routing table query during response packet sending that, for example, the incoming DNS request packets of China Telecom users from the CERNET interface shall go out from the Telecom interface, while the carrier will take corresponding measures to prevent the failure of packet loss resolution in this case.

d Set the parameters in the **Secondary IP** and **Sub Interface** windows.

Secondary IP: The Ethernet interface supports multiple IP addresses, and the secondary IP address is an IP address other than the one configured for the first time. Click Secondary IP to check and manage the secondary IP address corresponding to the selected interface.



Secondary IP

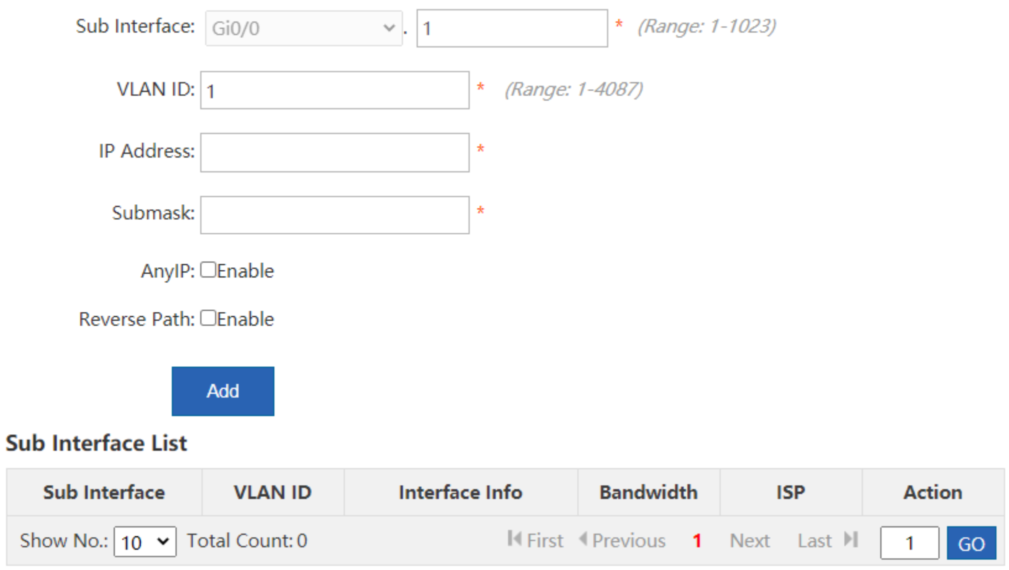
IP Address: *

Submask: 255.255.255.0 *

IP Address	Submask	Action
No Record Found		

Show No.: 10 Total Count: 0

Sub Interface: Sub interfaces are multiple logical interfaces derived from one physical interface. This means that multiple logical interfaces are associated with one physical interface, and several logical interfaces belonging to the same physical interface share the physical configuration parameters of the physical interface when they work, but have separate link layer and network layer configuration parameters. Click Sub Interface to check and manage the sub interface derived from the selected interface.



Sub Interface: Gi0/0 . 1 * (Range: 1-1023)

VLAN ID: 1 * (Range: 1-4087)

IP Address: *

Submask: *

AnyIP: □Enable

Reverse Path: □Enable

Add

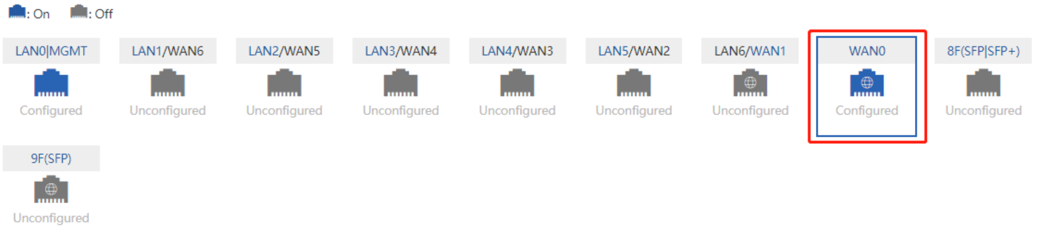
Sub Interface List

Sub Interface	VLAN ID	Interface Info	Bandwidth	ISP	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

(3) Configure an extranet port.

Properly connect the extranet line you applied for to the extranet port of the device and select the extranet port to be configured. The configuration page is displayed, as shown in the following figure.



: On : Off

LAN0|MGMT Configured

LAN1/WAN6 Unconfigured

LAN2/WAN5 Unconfigured

LAN3/WAN4 Unconfigured

LAN4/WAN3 Unconfigured

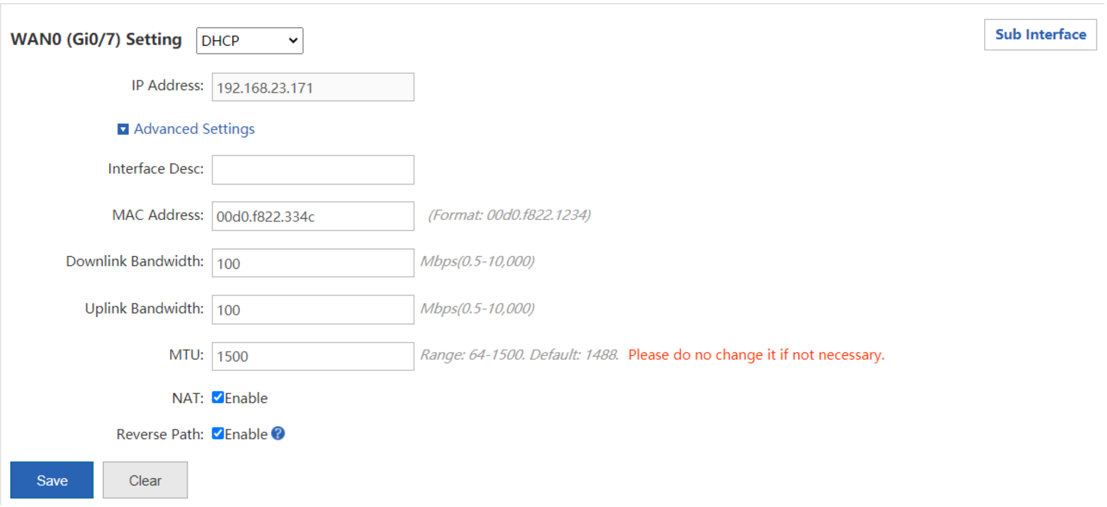
LAN5/WAN2 Unconfigured

LAN6/WAN1 Unconfigured

WAN0 Configured

8F(SFP|SFP+) Unconfigured

9F(SFP) Unconfigured



WAN0 (Gi0/7) Setting DHCP Sub Interface

IP Address: 192.168.23.171

Advanced Settings

Interface Desc:

MAC Address: 00d0.f822.334c (Format: 00d0.f822.1234)

Downlink Bandwidth: 100 Mbps(0.5-10,000)

Uplink Bandwidth: 100 Mbps(0.5-10,000)

MTU: 1500 Range: 64-1500. Default: 1488. Please do no change it if not necessary.

NAT: ☑Enable

Reverse Path: ☑Enable

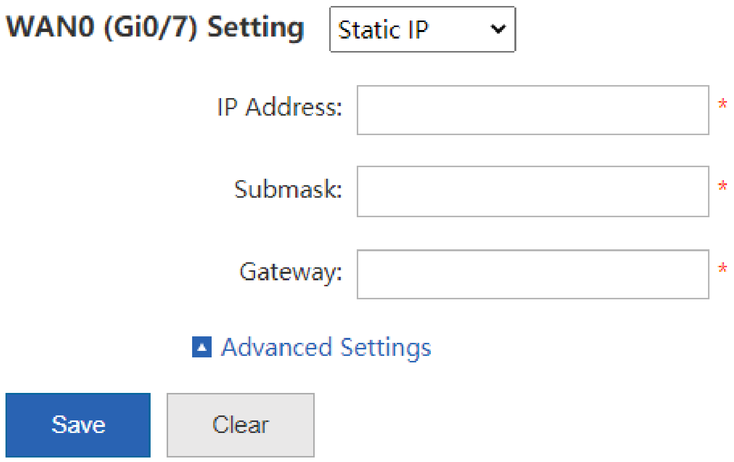
Save Clear

a Set the line type.

The options for extranet port configuration are **Static IP**, **DHCP**, and **PPPoE(ADSL)**.

- **Static IP:**

If you select it, set the IP address assigned to you by the operator, subnet mask, and next hop address (also router).



WAN0 (Gi0/7) Setting Static IP

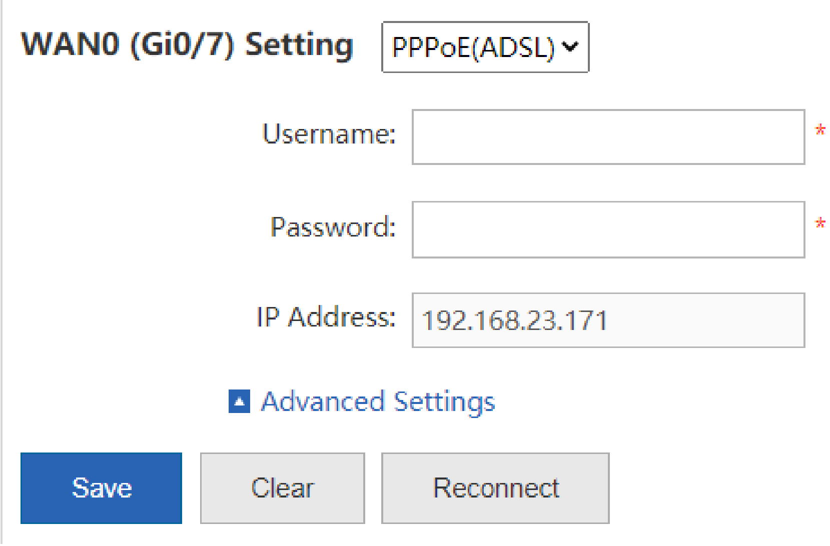
IP Address: *

Submask: *

Gateway: *

- ○ **PPPoE(ADSL):**

Select it if you apply for an ADSL line from the carrier. You need to set the dial-up account and password you applied for from the network carrier.



WAN0 (Gi0/7) Setting PPPoE(ADSL)

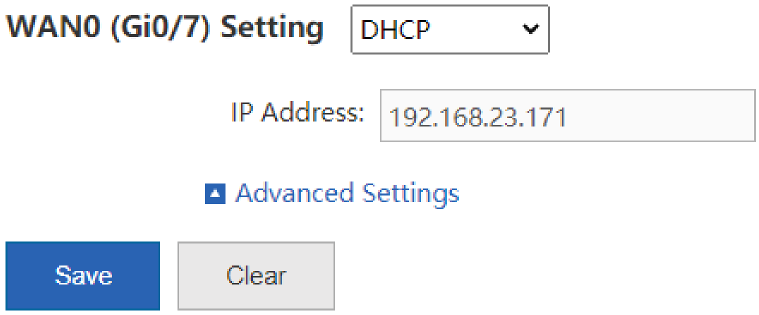
Username: *

Password: *

IP Address: 192.168.23.171

- ○ **DHCP:**

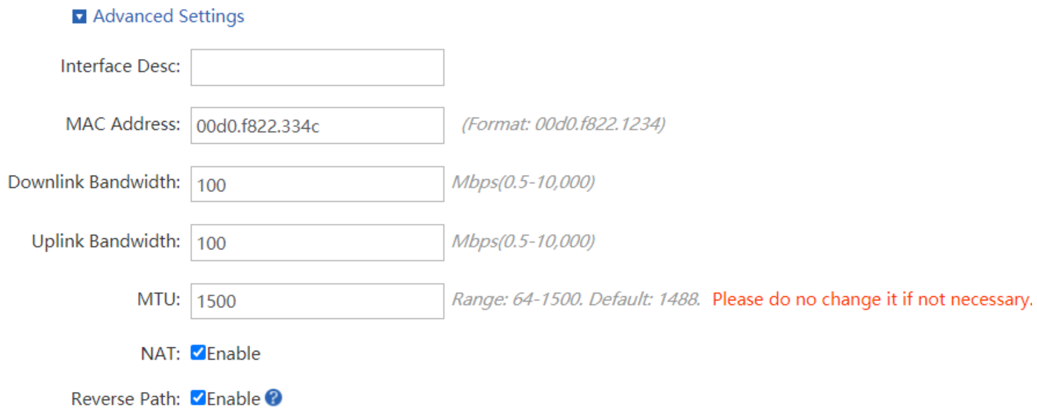
If you select it, the system will obtain the IP address dynamically.



WAN0 (Gi0/7) Setting DHCP

IP Address: 192.168.23.171

b Expand **Advanced Settings** and set other configuration information about the extranet port.



Advanced Settings

Interface Desc:

MAC Address: 00d0.f822.334c (Format: 00d0.f822.1234)

Downlink Bandwidth: 100 Mbps(0.5-10,000)

Uplink Bandwidth: 100 Mbps(0.5-10,000)

MTU: 1500 Range: 64-1500. Default: 1488. Please do no change it if not necessary.

NAT: ☑Enable

Reverse Path: ☑Enable

- **Interface Desc**: describes interface information. Set it when **Static IP** is selected, which is optional.
- **Uplink Bandwidth**/**Downlink Bandwidth**: maximum bandwidth allowed by the interface. Set it according to the actual bandwidth you applied for from the carrier. The bandwidth ranges from 0.5 Mbps to 1000 Mbps.

(4) Click **Save**.

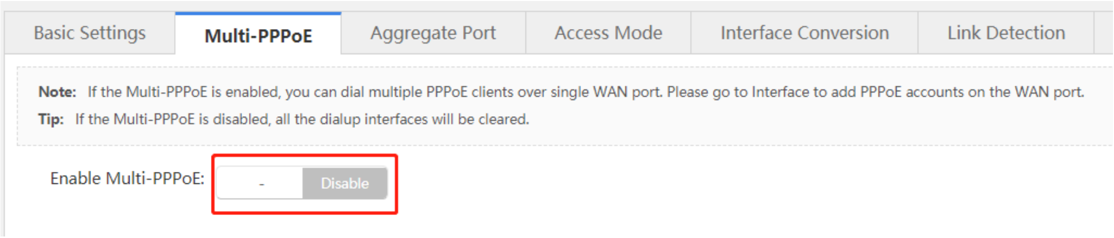
7.1.2 Multi-PPPoE

Application Scenario

This function allows dialer line adding for the corresponding interface.

Procedure

(1) Choose **Network** > **Interface** > **Multi-PPPoE**.



Note: If the Multi-PPPoE is enabled, you can dial multiple PPPoE clients over single WAN port. Please go to Interface to add PPPoE accounts on the WAN port.

Tip: If the Multi-PPPoE is disabled, all the dialup interfaces will be cleared.

Enable Multi-PPPoE: Disable

(2) Enable this function.

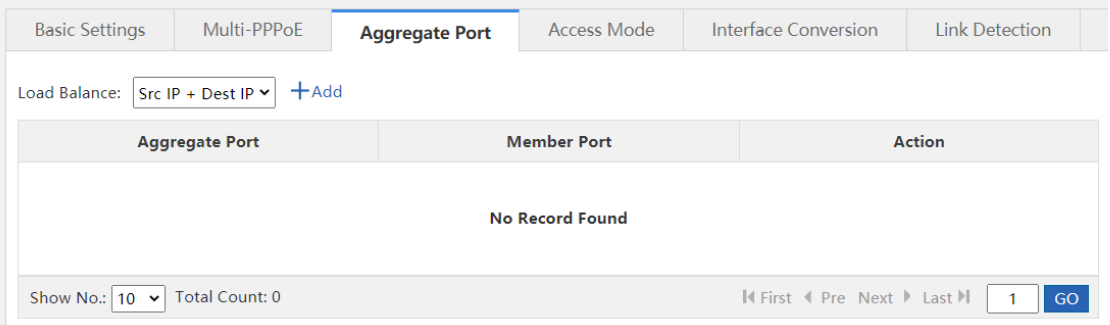
7.1.3 Multi-link Aggregation

Application Scenario

An Aggregate Port (AP) can bind multiple physical links together to form a logical link for link bandwidth expansion, which provides higher connection reliability. You can set link aggregation if link bandwidth expansion is required.

Procedure

(1) Choose **Network** > **Interface** > **Aggregate Port**.

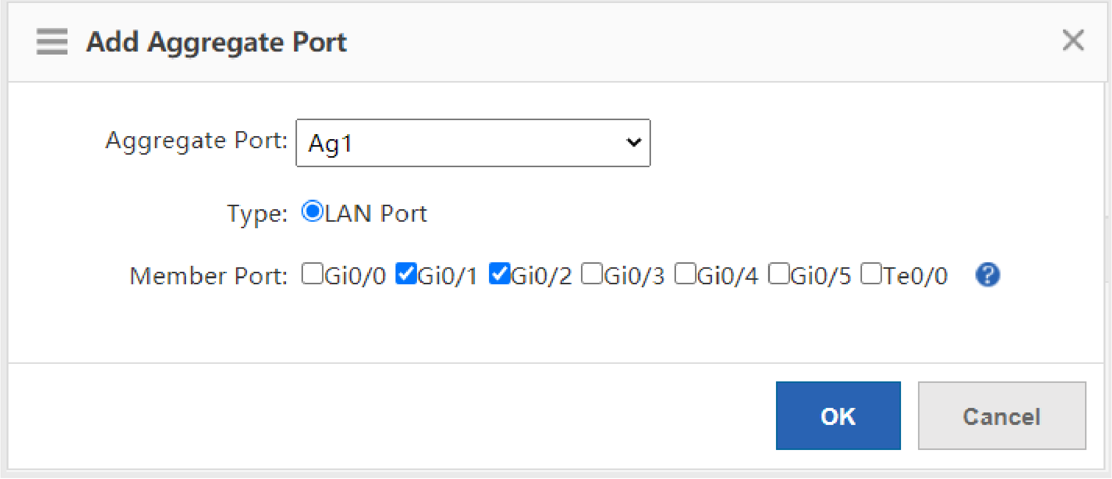


Load Balance: Src IP + Dest IP

Aggregate Port	Member Port	Action
No Record Found		

Show No.: 10 Total Count: 0 1

(2) Click +Add.



Aggregate Port: Ag1

Type: ● LAN Port

Member Port: □ Gi0/0 ☑ Gi0/1 ☑ Gi0/2 □ Gi0/3 □ Gi0/4 □ Gi0/5 □ Te0/0

(3) Set the configuration items related to intranet multi-link aggregation, that is, set **Aggregate Port**, **Type**, and **Member Port**.

(4) Click OK.

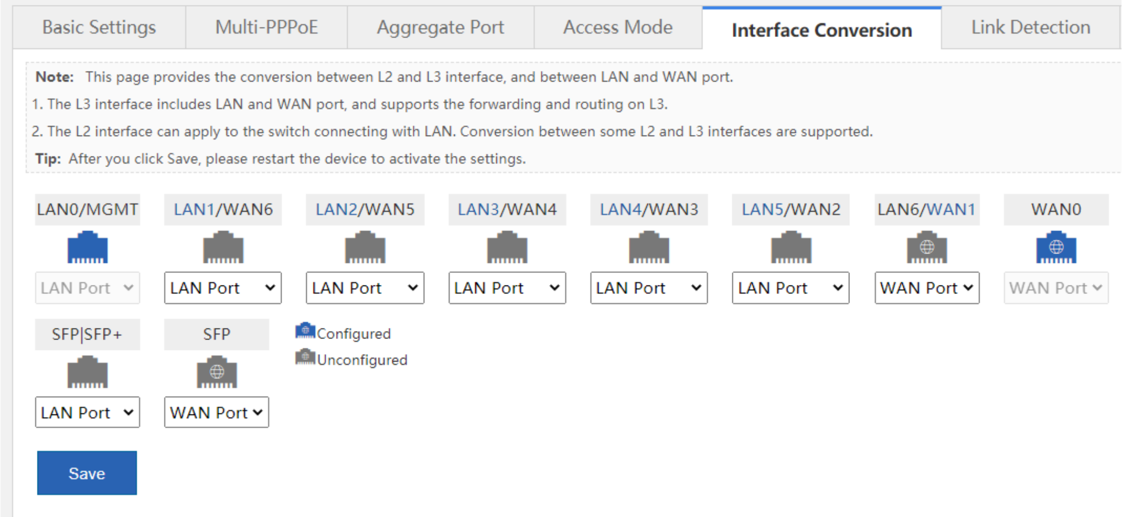
7.1.4 Interface Conversion

Application Scenario

Except for the fixed LAN ports and WAN ports, all other interfaces support switching between intranet ports and extranet ports. You can perform the switching on this page.

Procedure

(1) Choose **Network** > **Interface** > **Interface Conversion**.



Note: This page provides the conversion between L2 and L3 interface, and between LAN and WAN port.

1. The L3 interface includes LAN and WAN port, and supports the forwarding and routing on L3.
2. The L2 interface can apply to the switch connecting with LAN. Conversion between some L2 and L3 interfaces are supported.

Tip: After you click Save, please restart the device to activate the settings.

LAN0/MGMT	LAN1/WAN6	LAN2/WAN5	LAN3/WAN4	LAN4/WAN3	LAN5/WAN2	LAN6/WAN1	WAN0
LAN Port	LAN Port	LAN Port	LAN Port	LAN Port	LAN Port	WAN Port	WAN Port

SFP|SFP+	SFP
LAN Port	WAN Port

(2) Click the icon corresponding to the interface for conversion, and select **LAN Port** or **WAN Port** from the drop-down list for conversion.

(3) Click Save and restart the device for the interface mode to take effect.

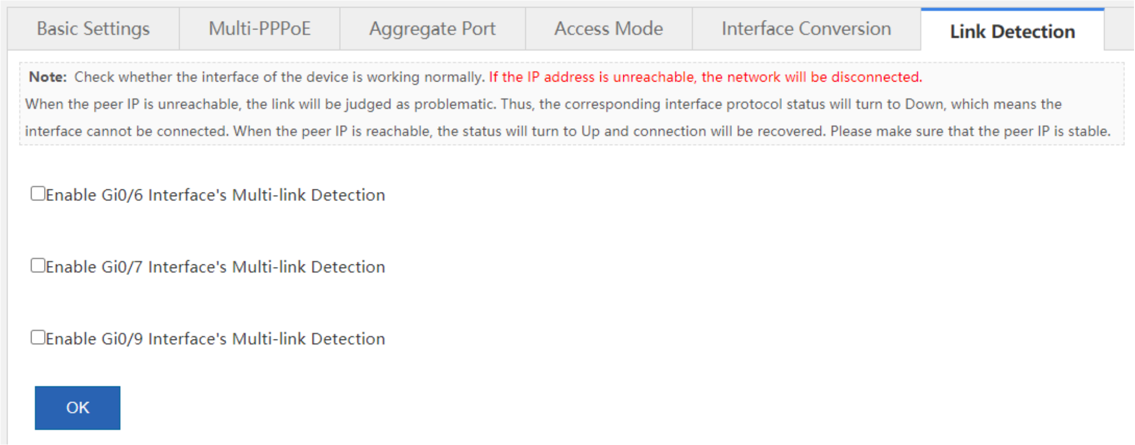
7.1.5 Link Detection

Application Scenario

This operation allows you to check whether the extranet port of the device is working properly.

Procedure

(1) Choose **Network** > **Interface** > **Link Detection**.



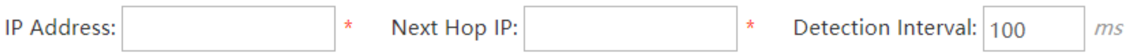
Note: Check whether the interface of the device is working normally. If the IP address is unreachable, the network will be disconnected.
When the peer IP is unreachable, the link will be judged as problematic. Thus, the corresponding interface protocol status will turn to Down, which means the interface cannot be connected. When the peer IP is reachable, the status will turn to Up and connection will be recovered. Please make sure that the peer IP is stable.

□Enable Gi0/6 Interface's Multi-link Detection

□Enable Gi0/7 Interface's Multi-link Detection

□Enable Gi0/9 Interface's Multi-link Detection

(2) Enable link detection for the corresponding interface, for example, select ☑Enable Gi0/7 Interface's Multi-link Detection. The link detection configuration items for the Gi0/7 interface are displayed.



IP Address: * Next Hop IP: * Detection Interval: 100 ms

- To check whether an interface can be connected, enter a pingable IP address, for example,

183.79.250.251 (yahoo.co.jp).

⚠ Caution

Please do not enter an IP address that cannot be pinged even when the interface works properly. Otherwise the network may be down. When the peer IP is unreachable, the link will be judged as problematic. Thus, the corresponding interface protocol status will turn to **Down**, which means the interface cannot be connected.

- Set **Next Hop IP**. Set it to the router IP address for an intranet device.
- Set **Detection Interval**. The default interval is 100 ms.

(3) Click OK. If the interface complies with the preceding configurations and can be pinged, a prompt indicating good network connection is displayed in the system. Otherwise, a prompt is displayed, indicating that the network is disconnected.

7.2 SUPER-VLAN

7.2.1 Introduction

SUPER-VLAN: implements the one-armed routing function, which allows the traffic of each VLAN to be routed to and from a specified intranet port without sub interface configuration.

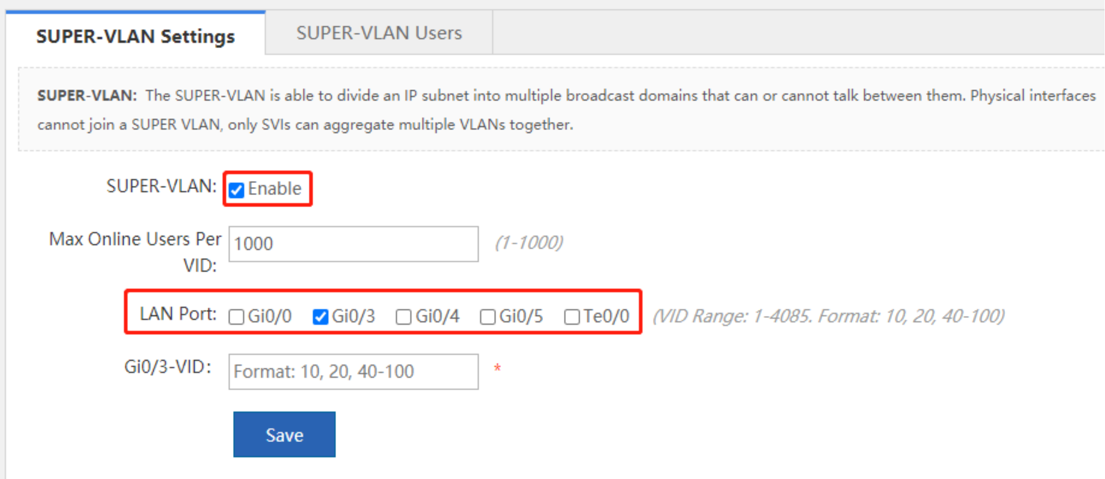
7.2.2 SUPER-VLAN Settings

Application Scenario

You can enable and configure the SUPER-VLAN function on this page.

Procedure

(1) Choose **Network** > **SUPER-VLAN** > **SUPER-VLAN Settings**.



SUPER-VLAN: The SUPER-VLAN is able to divide an IP subnet into multiple broadcast domains that can or cannot talk between them. Physical interfaces cannot join a SUPER VLAN, only SVIs can aggregate multiple VLANs together.

SUPER-VLAN: ☑ Enable

Max Online Users Per VID: 1000 (1-1000)

LAN Port: □ Gi0/0 ☑ Gi0/3 □ Gi0/4 □ Gi0/5 □ Te0/0 (VID Range: 1-4085. Format: 10, 20, 40-100)

Gi0/3-VID: Format: 10, 20, 40-100 *

(2) Select **Enable**.

(3) Set **Max Online Users Per VID**.

Max Online Users Per VID: maximum number of online users allowed by a VLAN, which ranges from 1 to 1000.

(4) Set the VID for the intranet port.

Select the intranet port to be configured. The corresponding configuration item is displayed below. The VID ranges from 1 to 4085. The VIDs for two interfaces cannot overlap. For example, if a VID of 1–1000 is configured for one port, only a VID out of the range of 1–1000 can be configured for the other port (for example, a VID of 500–600 cannot be configured).

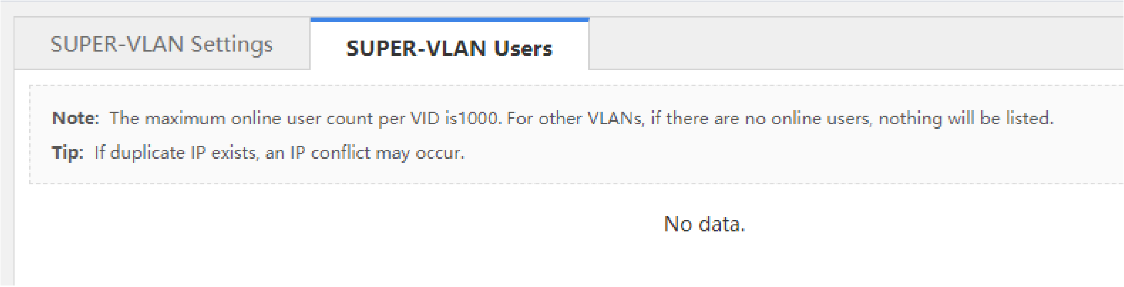
(5) Click Save.

7.2.3 SUPER-VLAN Users

Procedure

(1) Choose **Network** > **SUPER-VLAN** > **SUPER-VLAN Users**.

(2) Check the current information on this page, as shown in the following figure.



Note: The maximum online user count per VID is1000. For other VLANs, if there are no online users, nothing will be listed.

Tip: If duplicate IP exists, an IP conflict may occur.

No data.

7.3 Route/Load

7.3.1 Introduction

- Routes are classified into policy-based routes and common IP-based routes, which can be used as the basis for packet forwarding. When the policies exist simultaneously, the priority levels are in descending order for the policy-based route, static route, and default route.
- Load balancing: Generally, a network egress interface is connected to two or more carrier links. For example, a campus network egress interface is generally connected to CERNET and China Telecom/CNC lines, and a government extranet egress interface is generally connected to China Telecom and CNC lines. Multiple carrier links share traffic or function as backups according to certain policies, which is known as multi-link load balancing.

7.3.2 Policy-Based Route

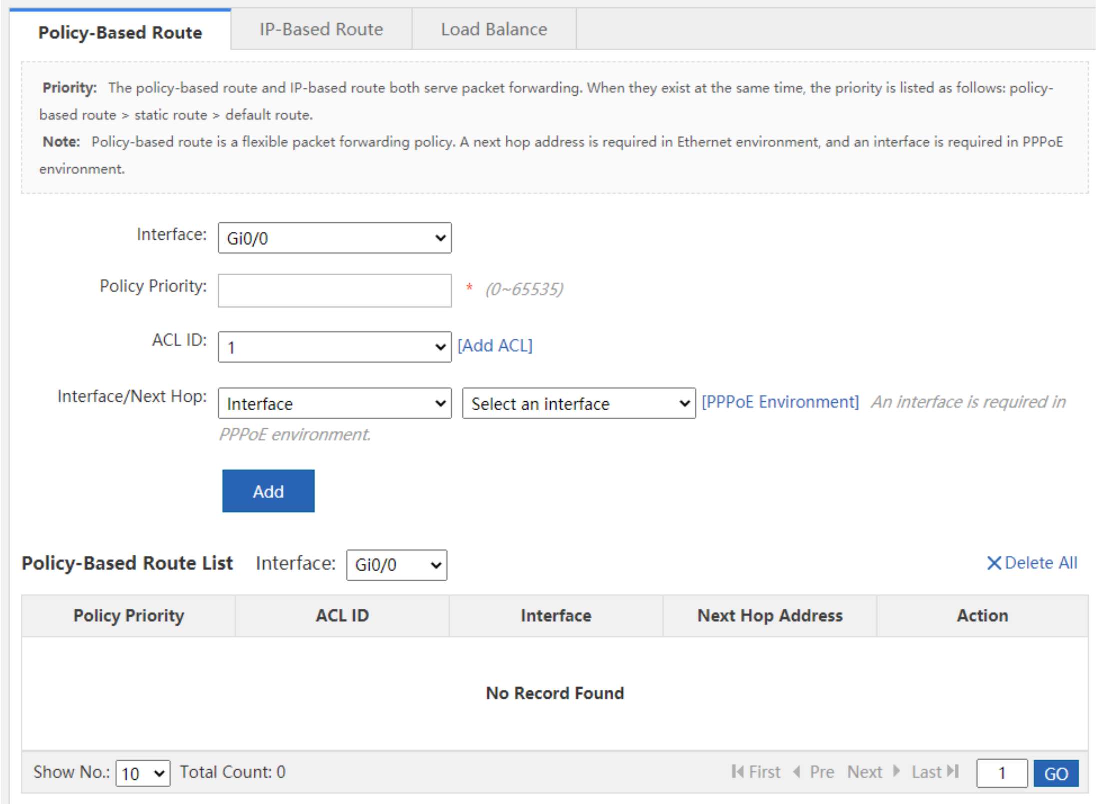
Application Scenario

Policy-based routing is a data packet routing and forwarding mechanism, which is more flexible than destination network–based routing. When policy-based routing is applied, the device will determine how to process packets to be routed according to a route diagram, which determines the next hop forwarding device for packets.

To apply policy-based routing, you must specify the route diagram to be used for policy-based routing and create the route diagram. A route diagram consists of many policies, each of which defines one or more matching rules and corresponding operations. After policy-based routing is applied to an interface, all packets received by the interface will be checked. Packets that do not conform to any policy in the route diagram will be processed according to the common routing and forwarding mechanism, and packets that conform to a policy in the route diagram will be processed according to the operations defined in the policy.

Procedure

(1) Choose **Network** > **Route/Load** > **Policy-Based Route**.



Priority: The policy-based route and IP-based route both serve packet forwarding. When they exist at the same time, the priority is listed as follows: policy-based route > static route > default route.

Note: Policy-based route is a flexible packet forwarding policy. A next hop address is required in Ethernet environment, and an interface is required in PPPoE environment.

Interface: Gi0/0

Policy Priority: * (0~65535)

ACL ID: 1 [Add ACL]

Interface/Next Hop: Interface | Select an interface [PPPoE Environment] *An interface is required in PPPoE environment.*

Add

Policy-Based Route List Interface: Gi0/0 ✕Delete All

Policy Priority	ACL ID	Interface	Next Hop Address	Action
No Record Found				

Show No.: 10 Total Count: 0 First Pre Next Last 1 GO

(2) Set related configuration items.

a Select the interface that requires a policy.

b Set **Policy Priority**.

c Set **ACL ID** (the ACL is used to specify the data stream matched by the policy-based route). You can click [Add ACL] for ACL adding. For detailed operation, see 6.7 ACL.

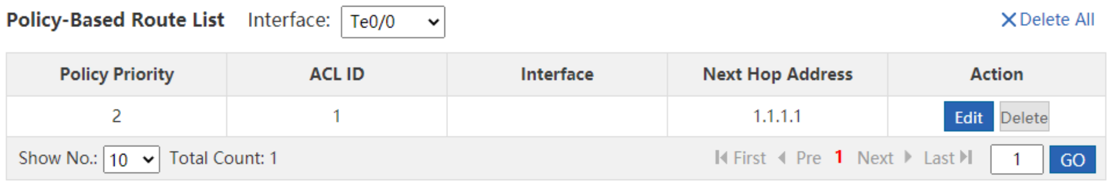
d Set the next hop address.

If you select **Interface** and select an interface from the drop-down list, the router address of this interface is used as the next hop address for routing. If you select **Next Hop Address**, be sure to enter an IP address in the text box.

e Click Add.

Follow-up Procedure

- Select the interface and view the generated policy-based route under **Policy-Based Route List**.



Policy-Based Route List Interface: Te0/0 ✕Delete All

Policy Priority	ACL ID	Interface	Next Hop Address	Action
2	1		1.1.1.1	Edit Delete

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 GO

- Editing: Click Edit in the policy-based route list and modify the corresponding policy-based route.
- Deletion: Click Delete in the policy-based route list to delete the corresponding item. You can click ✕Delete All in the upper right corner of the configuration page to delete all policy-based routes from the corresponding group.

7.3.3 IP-Based Route

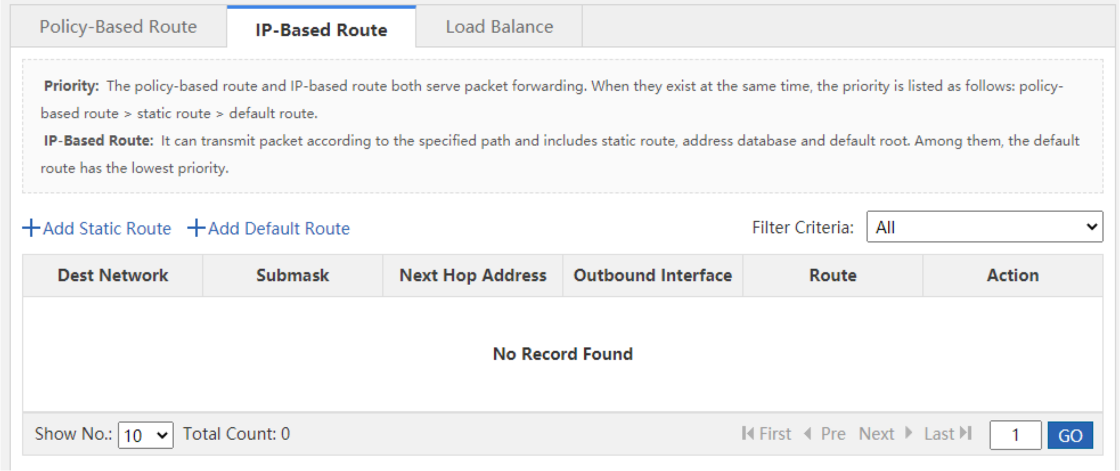
Application Scenario

Common IP-based routing enables transmission of packets to the specified destination network according to the predetermined path. When Ruijie's products cannot learn the routes of some destination networks, it is important to configure a static route. It is common practice to configure a default route for all packets that do not have an exact route.

Common IP-based routes include static routes, and default routes, where default routes have the lowest priority.

Procedure

(1) Choose **Network** > **Route/Load** > **IP-Based Route**.



Priority: The policy-based route and IP-based route both serve packet forwarding. When they exist at the same time, the priority is listed as follows: policy-based route > static route > default route.

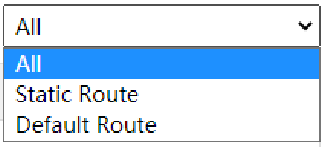
IP-Based Route: It can transmit packet according to the specified path and includes static route, address database and default root. Among them, the default route has the lowest priority.

+Add Static Route +Add Default Route Filter Criteria: All

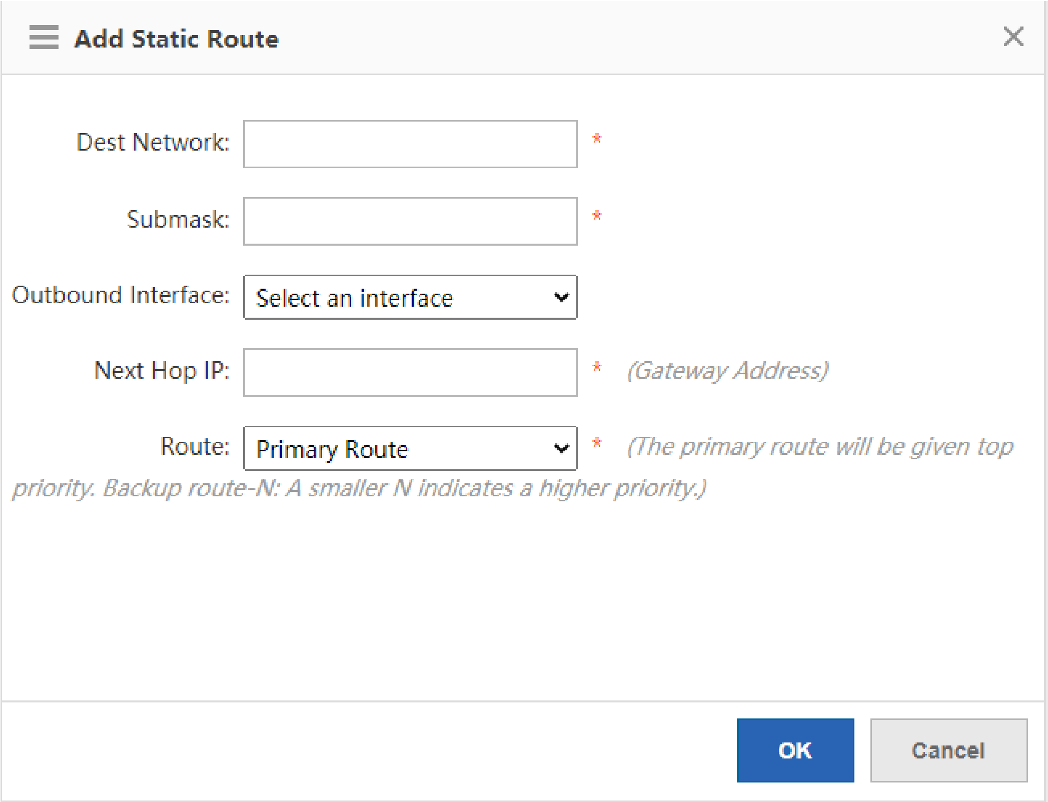
Dest Network	Submask	Next Hop Address	Outbound Interface	Route	Action
No Record Found					

Show No.: 10 Total Count: 0 First Pre Next Last 1 GO

The table in the preceding figure lists the static routes and default routes configured in the system. You can set to filter out the static routes or default routes only.



(2) Click +Add Static Route.



Add Static Route

Dest Network: *

Submask: *

Outbound Interface: Select an interface

Next Hop IP: * (Gateway Address)

Route: Primary Route * (The primary route will be given top priority. Backup route-N: A smaller N indicates a higher priority.)

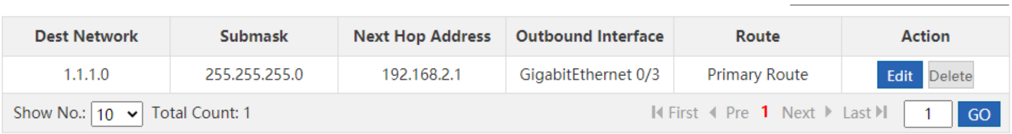
(3) Set configuration items related to the static route.

- **Dest Network**: destination network segment of the route.
- **Submask**: mask of the destination network segment.
- **Outbound Interface**: egress interface of the route.
- **Next Hop IP**: ingress interface address of the next route (router).
- **Route**: specifies the routing priority. If it is set to **Primary Route**, the primary route is given the top priority. If it is set to **Backup Route-***N*, a smaller *N* value indicates higher priority.

(4) Click OK.

Follow-up Procedure

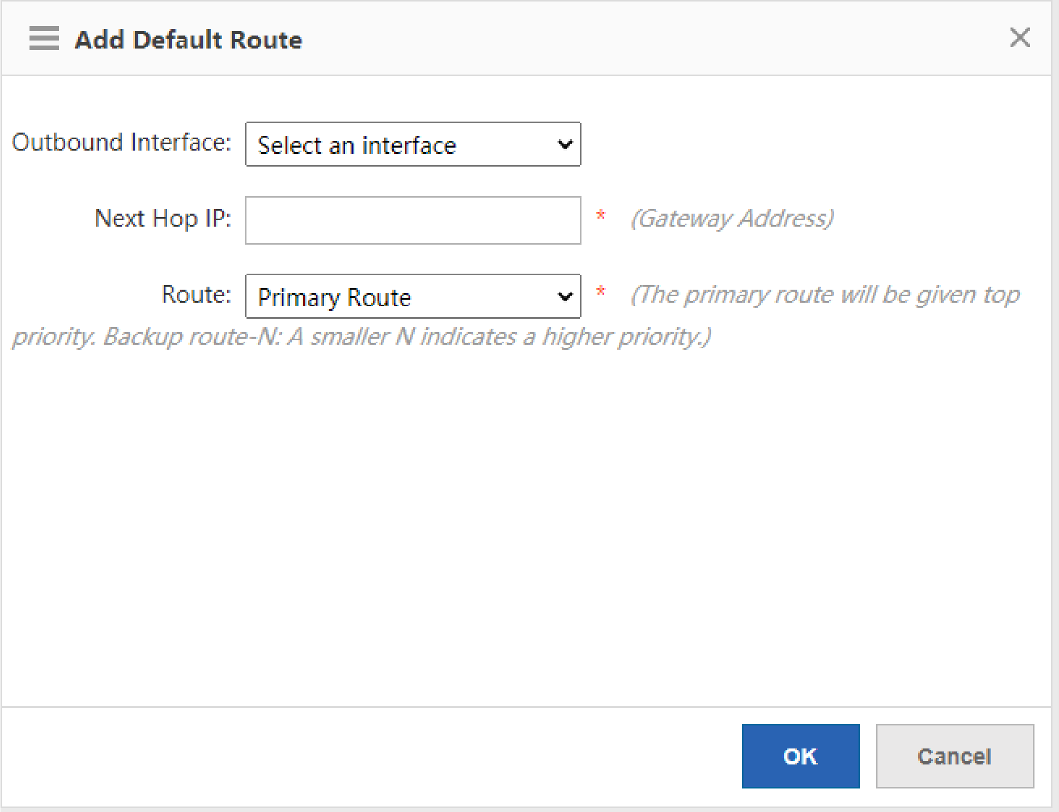
- View the generated common route.



Dest Network	Submask	Next Hop Address	Outbound Interface	Route	Action
1.1.1.0	255.255.255.0	192.168.2.1	GigabitEthernet 0/3	Primary Route	Edit Delete

Show No.: 10 Total Count: 1

- Click Delete to delete a static route.
- Click +Add Default Route . The window shown in the following figure is displayed.

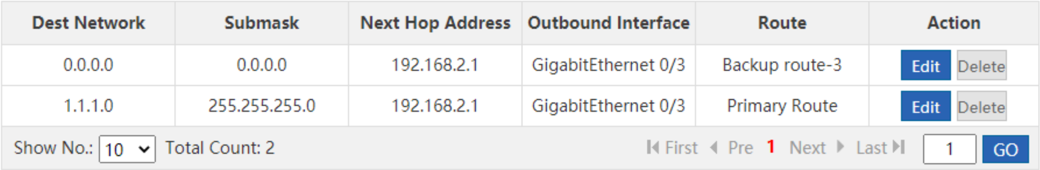


Outbound Interface: Select an interface

Next Hop IP: * *(Gateway Address)*

Route: Primary Route * *(The primary route will be given top priority. Backup route-N: A smaller N indicates a higher priority.)*

Set **Outbound Interface**, **Next Hop Address**, and **Route**, and click OK to configure a default route.



Dest Network	Submask	Next Hop Address	Outbound Interface	Route	Action
0.0.0.0	0.0.0.0	192.168.2.1	GigabitEthernet 0/3	Backup route-3	Edit Delete
1.1.1.0	255.255.255.0	192.168.2.1	GigabitEthernet 0/3	Primary Route	Edit Delete

Click Delete to delete a default route.

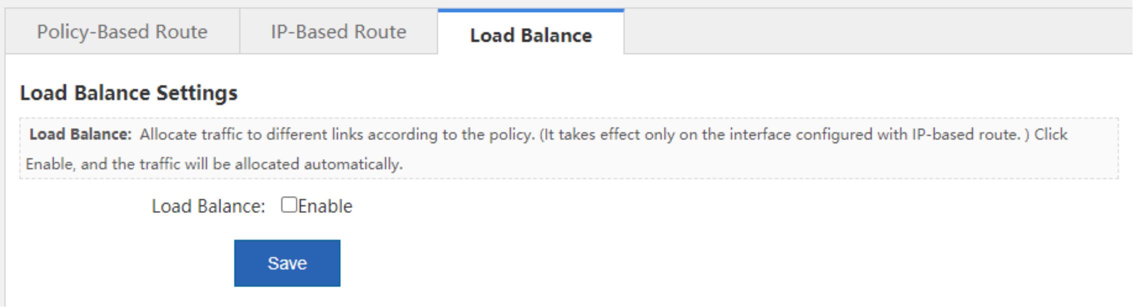
7.3.4 Multi-link Load Balancing

Application Scenario

This function allows appropriate traffic distribution on multiple links according to certain policies, improving the efficiency of link resource utilization.

Procedure

(1) Choose **Network** > **Route/Load** > **Load Balance**.



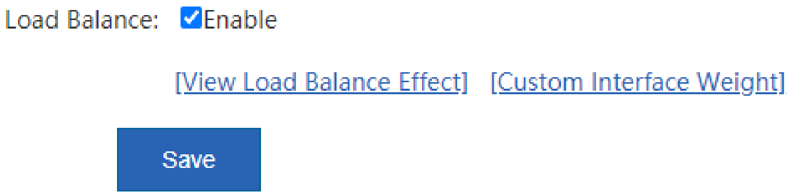
Load Balance Settings

Load Balance: Allocate traffic to different links according to the policy. (It takes effect only on the interface configured with IP-based route.) Click Enable, and the traffic will be allocated automatically.

Load Balance: □Enable

Save

(2) Select **Enable**.



Load Balance: ☑Enable

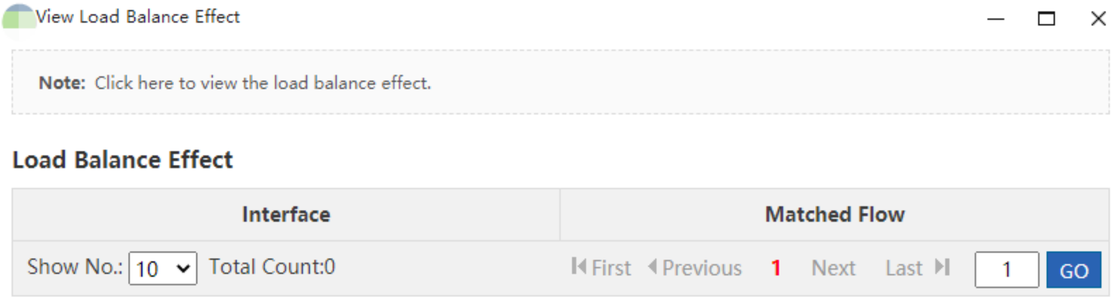
[View Load Balance Effect] [Custom Interface Weight]

Save

(3) Click **Save**.

Follow-up Procedure

Click [View Load Balance Effect] to view the effect of load balancing.



View Load Balance Effect

Note: Click here to view the load balance effect.

Load Balance Effect

Interface	Matched Flow
Show No.: 10 Total Count:0	First Previous 1 Next Last 1 GO

7.4 DNS Configuration

7.4.1 Introduction

The Domain Name System (DNS), a distributed database on the Internet that provides mutual mapping between domain names and IP addresses, makes it easier for users to access the Internet without having to memorize IP strings that can be directly read by machines. Domain name resolution (or host name resolution) is a process where the IP address corresponding to a given host name is finally obtained.

DNS configuration includes DNS server configuration and DNS proxy configuration.

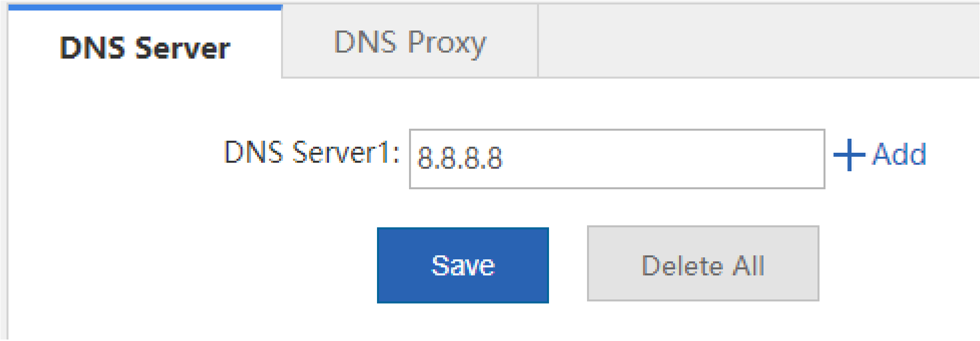
7.4.2 DNS Server

Application Scenario

This function allows the configuration of the DNS server address of the device, similar to the preferred DNS server address of the PC.

Procedure

(1) Choose **Network** > **DNS Settings** > **DNS Server**.



DNS Server1: 8.8.8.8

(2) Set the IP address of DNS server 1.

(3) (Optional) Click +Add to set the IP address of DNS server 2 if you need to configure multiple servers.

(4) Click Save.

Configuration Verification

Pinging www.google.com is used as an example to illustrate the effect of DNS server configuration.

- When the DNS server address is not configured, www.google.com cannot be pinged using the device because the device cannot resolve the domain name www.google.com.
- www.google.com can be pinged only when an available DNS server address is configured.

7.4.3 DNS Proxy

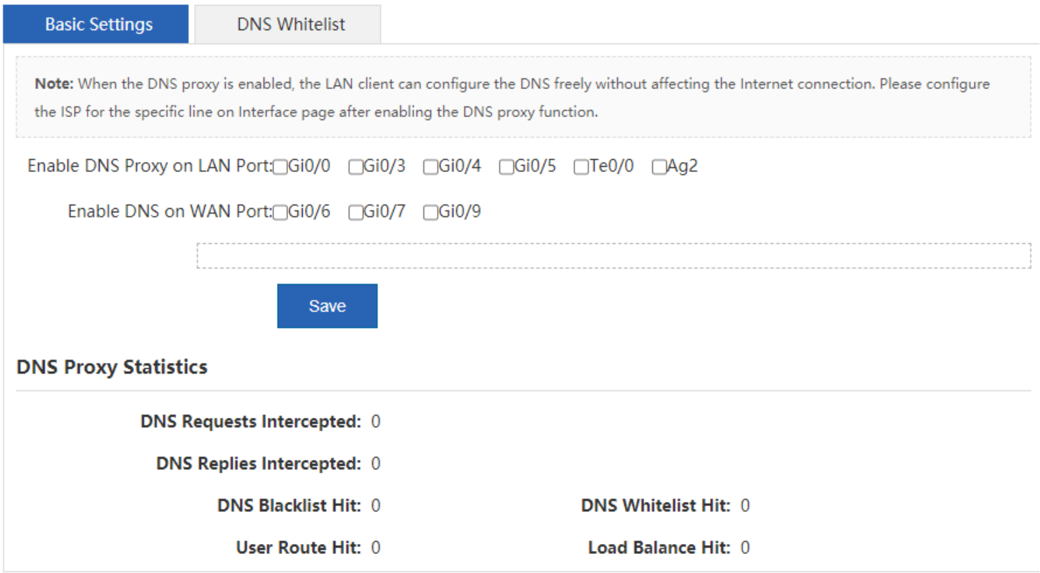
Application Scenario

A DNS proxy is typically deployed between the DNS server and the user's PC, functioning as a proxy for the DNS server to process the user's domain name resolution requests.

Procedure

(1) Choose **Network** > **DNS Settings** > **DNS Proxy**.

(2) Click the **Basic Settings** tab and set related configuration items.



Note: When the DNS proxy is enabled, the LAN client can configure the DNS freely without affecting the Internet connection. Please configure the ISP for the specific line on Interface page after enabling the DNS proxy function.

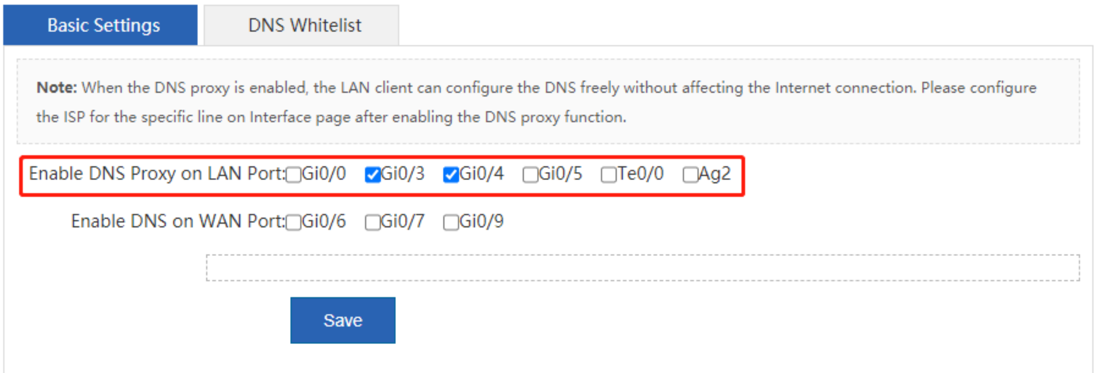
Enable DNS Proxy on LAN Port: □Gi0/0 □Gi0/3 □Gi0/4 □Gi0/5 □Te0/0 □Ag2

Enable DNS on WAN Port: □Gi0/6 □Gi0/7 □Gi0/9

DNS Proxy Statistics

DNS Requests Intercepted:	0		
DNS Replies Intercepted:	0		
DNS Blacklist Hit:	0	**DNS Whitelist Hit:**	0
User Route Hit:	0	**Load Balance Hit:**	0

a Select the intranet ports for which the DNS proxy function needs to be enabled.

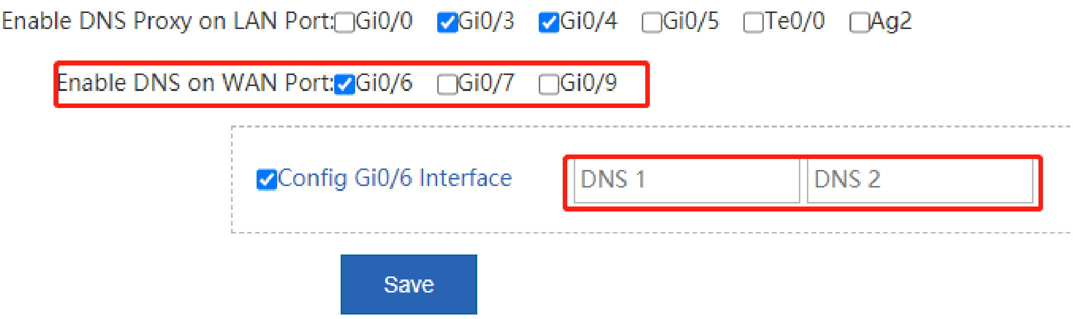


Note: When the DNS proxy is enabled, the LAN client can configure the DNS freely without affecting the Internet connection. Please configure the ISP for the specific line on Interface page after enabling the DNS proxy function.

Enable DNS Proxy on LAN Port: □Gi0/0 ☑Gi0/3 ☑Gi0/4 □Gi0/5 □Te0/0 □Ag2

Enable DNS on WAN Port: □Gi0/6 □Gi0/7 □Gi0/9

b Select the extranet port to be connected to the DNS server and set the DNS server address for the corresponding line.

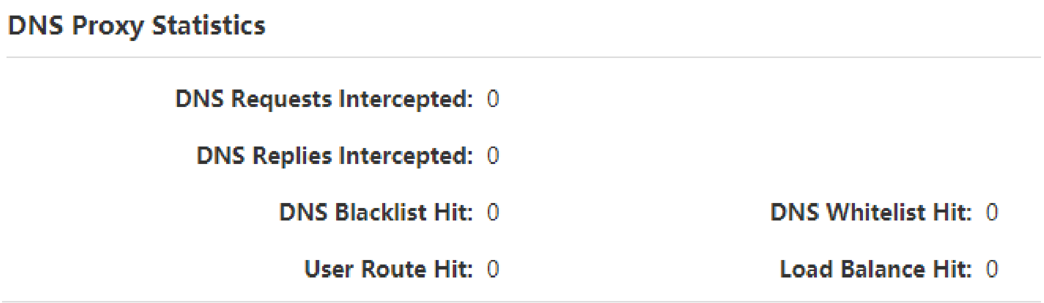

Enable DNS Proxy on LAN Port: □Gi0/0 ☑Gi0/3 ☑Gi0/4 □Gi0/5 □Te0/0 □Ag2

Enable DNS on WAN Port: ☑Gi0/6 □Gi0/7 □Gi0/9

☑Config Gi0/6 Interface DNS 1 DNS 2

c Click Save.

d View the DNS proxy statistics below.



DNS Proxy Statistics

DNS Requests Intercepted: 0

DNS Replies Intercepted: 0

DNS Blacklist Hit: 0 DNS Whitelist Hit: 0

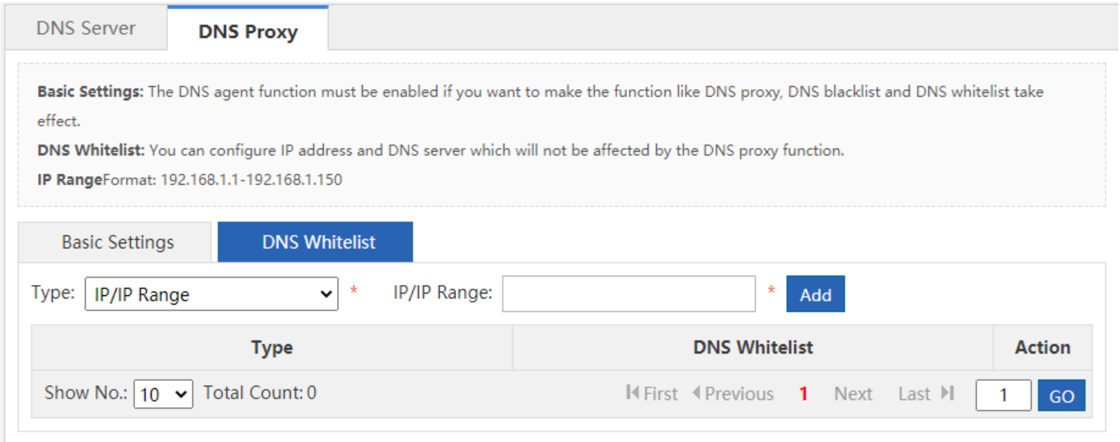
User Route Hit: 0 Load Balance Hit: 0

(3) Click the **DNS Whitelist** tab and set the configuration items related to DNS proxy exclusion.

This function is used to set some special resources (including the IP address and DNS server) that do not need to be affected by the DNS proxy function.

Set **Type** to **IP/IP Range** or **DNS Server**, enter the corresponding IP address in the text box, and click Add.

The configurations will be displayed in the table below.



Basic Settings: The DNS agent function must be enabled if you want to make the function like DNS proxy, DNS blacklist and DNS whitelist take effect.

DNS Whitelist: You can configure IP address and DNS server which will not be affected by the DNS proxy function.

IP Range Format: 192.168.1.1-192.168.1.150

Type: IP/IP Range * IP/IP Range: * Add

Type	DNS Whitelist	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

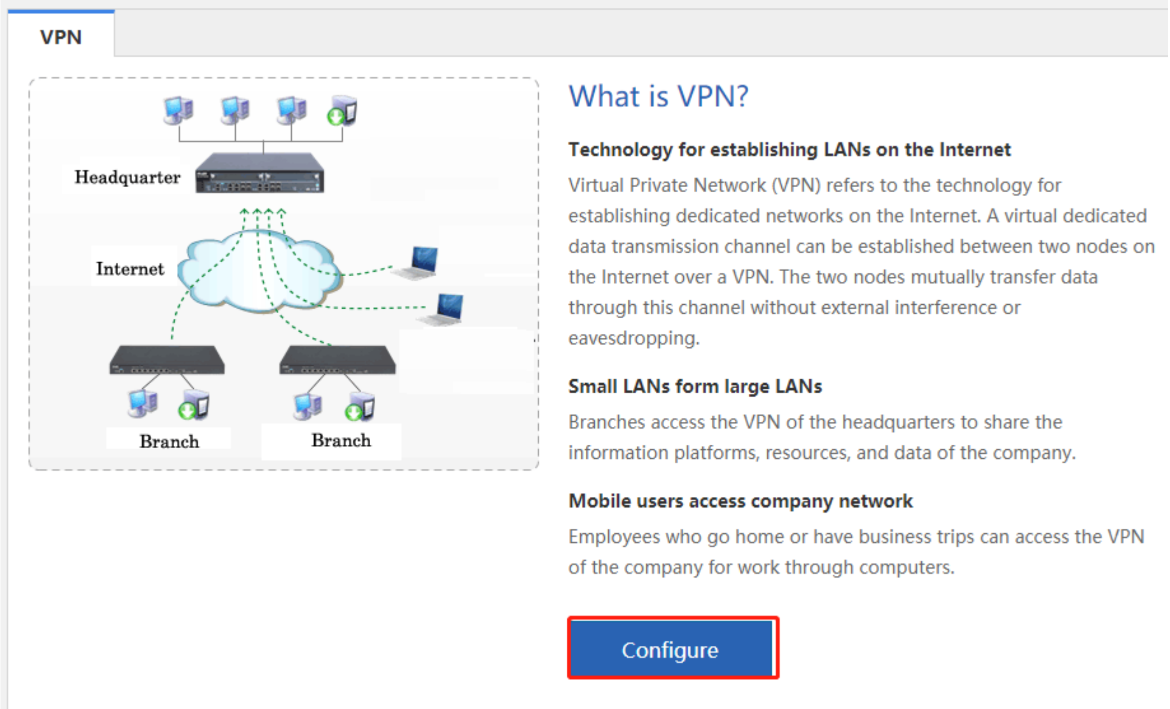
7.5 VPN Configuration

7.5.1 Introduction

A Virtual Private Network (VPN) is not a real physical link, but a virtual line simulated through technical means. Through a VPN, a virtual private data transmission channel can be established between two nodes on the Internet, where the information transmitted to each other will not be interfered with or eavesdropped.

7.5.2 VPN Server (Headquarters) Configuration

The following figure shows the configuration page for the first VPN configuration.



What is VPN?

Technology for establishing LANs on the Internet

Virtual Private Network (VPN) refers to the technology for establishing dedicated networks on the Internet. A virtual dedicated data transmission channel can be established between two nodes on the Internet over a VPN. The two nodes mutually transfer data through this channel without external interference or eavesdropping.

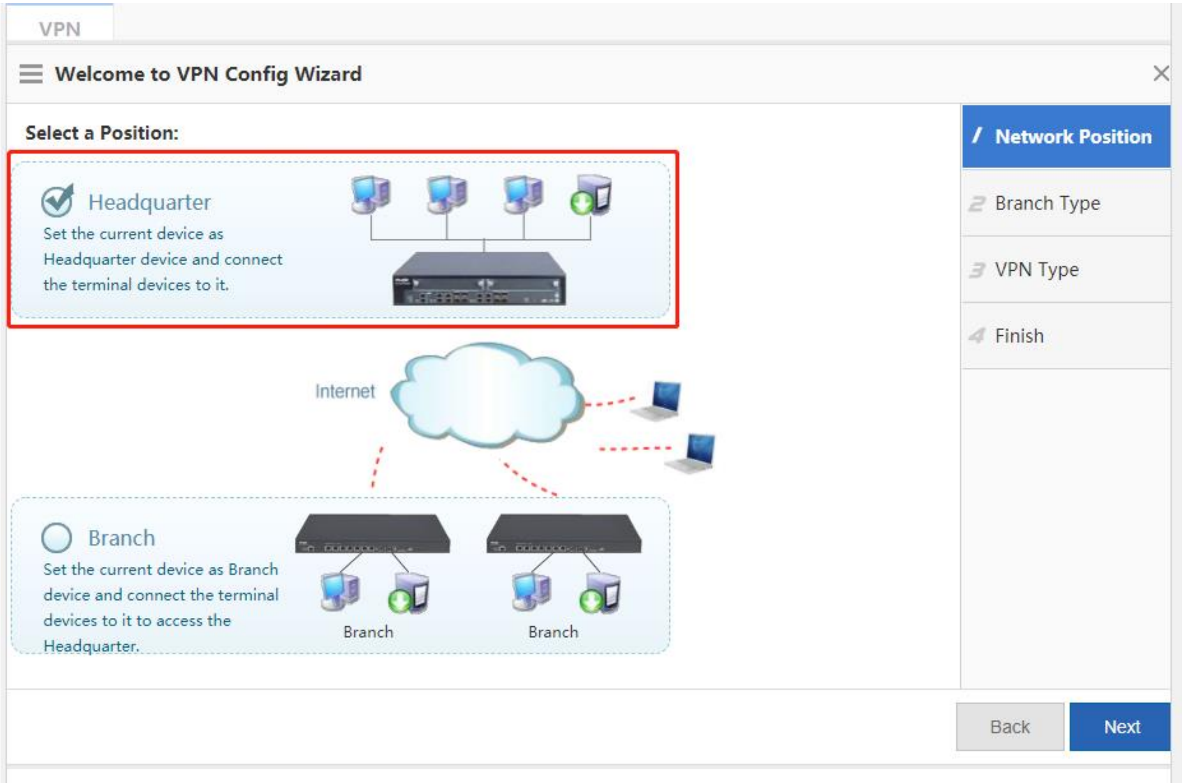
Small LANs form large LANs

Branches access the VPN of the headquarters to share the information platforms, resources, and data of the company.

Mobile users access company network

Employees who go home or have business trips can access the VPN of the company for work through computers.

(1) Click **Configure** on the right. In the window shown in the following figure, select **Headquarter** and click **Next**.

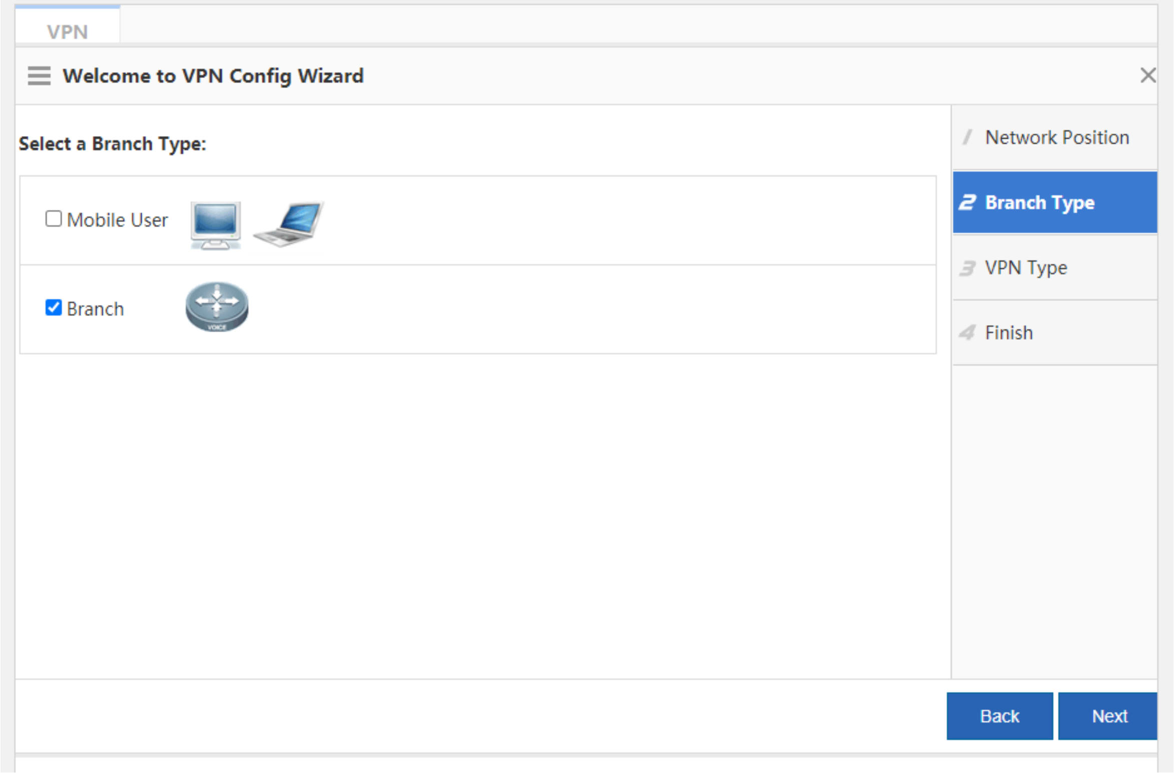


Select a Position:

☑ Headquarter
Set the current device as Headquarter device and connect the terminal devices to it.

○ Branch
Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.

(2) Select a branch type according to the access terminal type. Select **Mobile User** for a mobile terminal of an individual user, and **Branch** for an egress router of a branch. Click **Next**.



VPN

Welcome to VPN Config Wizard

Select a Branch Type:

□ Mobile User

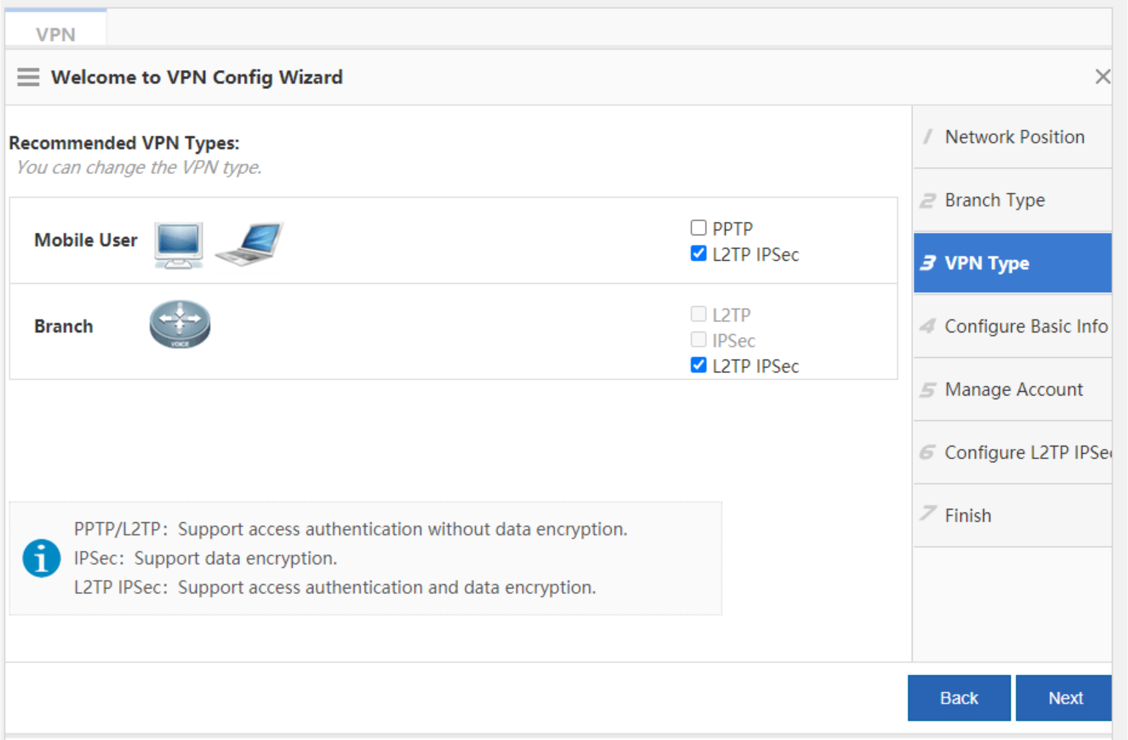
☑ Branch

(3) Set the VPN type as required. Configuration steps vary with the VPN types. Click **Next**. The next configuration page is displayed. In the following content, the **L2TP IPSec** type is used as an example.

PPTP/L2TP: supports access authentication without data encryption.

IPSec: support data encryption.

L2TP IPSec: supports access authentication and data encryption.



VPN

Welcome to VPN Config Wizard

Recommended VPN Types:

You can change the VPN type.

Mobile User: □ PPTP ☑ L2TP IPSec

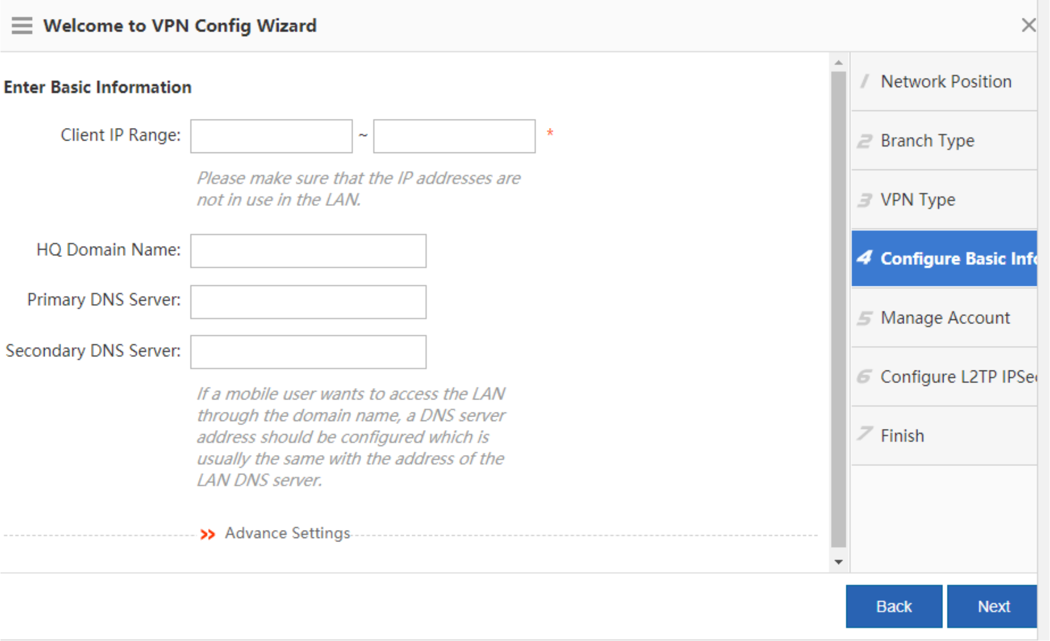
Branch: □ L2TP □ IPSec ☑ L2TP IPSec

PPTP/L2TP：Support access authentication without data encryption.

IPSec：Support data encryption.

L2TP IPSec：Support access authentication and data encryption.

(4) On the page corresponding to **Configure Basic Information**, set basic parameters about the VPN headquarters.



Welcome to VPN Config Wizard

Enter Basic Information

Client IP Range: ~ *

Please make sure that the IP addresses are not in use in the LAN.

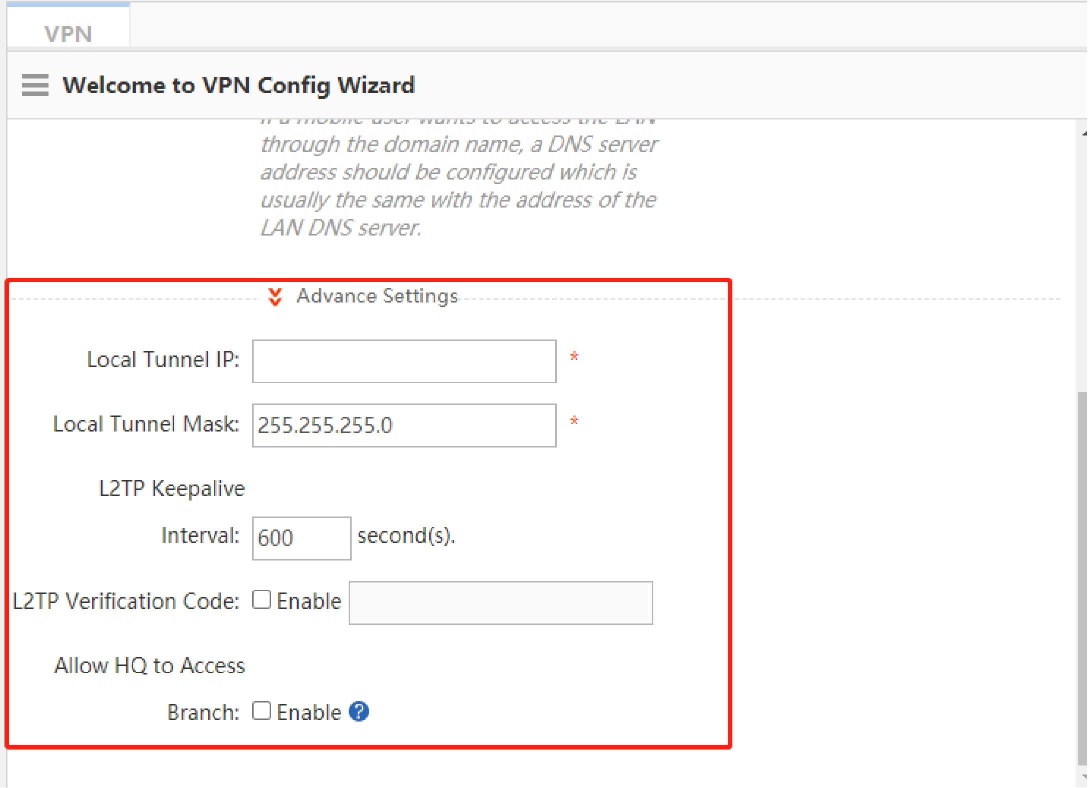
HQ Domain Name:

Primary DNS Server:

Secondary DNS Server:

If a mobile user wants to access the LAN through the domain name, a DNS server address should be configured which is usually the same with the address of the LAN DNS server.

- **Client IP Range**: tunnel IP addresses assigned to the VPN clients. The number of IP addresses determines the number of VPN clients that can be connected.
- **DNS Server**: Set the DNS server address when a VPN client needs to access the LAN through the domain name, which is the same as the address of the LAN DNS server.
- Click >> Advance Settings and set the following configuration items:



VPN

Welcome to VPN Config Wizard

through the domain name, a DNS server address should be configured which is usually the same with the address of the LAN DNS server.

Advance Settings

Local Tunnel IP: *

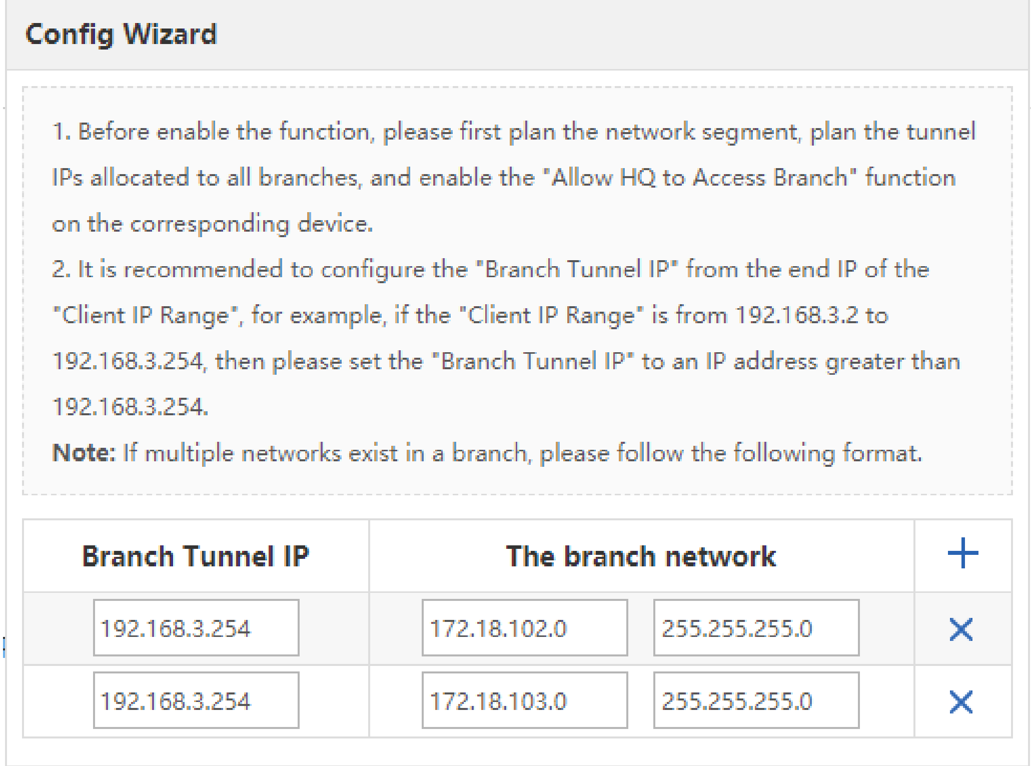
Local Tunnel Mask: 255.255.255.0 *

L2TP Keepalive Interval: 600 second(s).

L2TP Verification Code: □ Enable

Allow HQ to Access Branch: □ Enable

- **Local Tunnel IP**: tunnel IP address used by the local device when a remote client establishes a VPN tunnel with the local device using PPTP or L2TP. The first IP address in the client address range is used by default.
- **PPTP Keepalive Interval**: If you set the interval, the local device will proactively detect the tunnel status if it does not receive any legal packets from the peer end of the tunnel within this interval. The default interval 60s is recommended.
- **L2TP Keepalive Interval**: interval for tunnel control message retransmission. If there is no session within this interval, the tunnel will be automatically cleared. The default interval 600s is recommended.
- **L2TP Verification Code**: Verification is not required for L2TP tunnel establishment by default. If verification is required, both ends of the L2TP tunnel must be configured with the same verification password.
- **Allow HQ to Access Branch**: For headquarters access to the branch intranet, you must plan in advance the tunnel IP address of each branch dialing into the headquarters and the intranet segment of each branch. Click ☑ Enable , hover your mouse over ?, and set basic information in the table in the **Config Wizard** window, as shown in the following figure.



Config Wizard

1. Before enable the function, please first plan the network segment, plan the tunnel IPs allocated to all branches, and enable the "Allow HQ to Access Branch" function on the corresponding device.

2. It is recommended to configure the "Branch Tunnel IP" from the end IP of the "Client IP Range", for example, if the "Client IP Range" is from 192.168.3.2 to 192.168.3.254, then please set the "Branch Tunnel IP" to an IP address greater than 192.168.3.254.

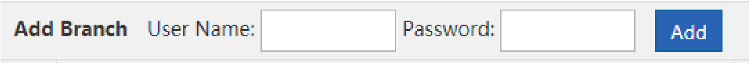
Note: If multiple networks exist in a branch, please follow the following format.

Branch Tunnel IP	The branch network		+
192.168.3.254	172.18.102.0	255.255.255.0	×
192.168.3.254	172.18.103.0	255.255.255.0	×

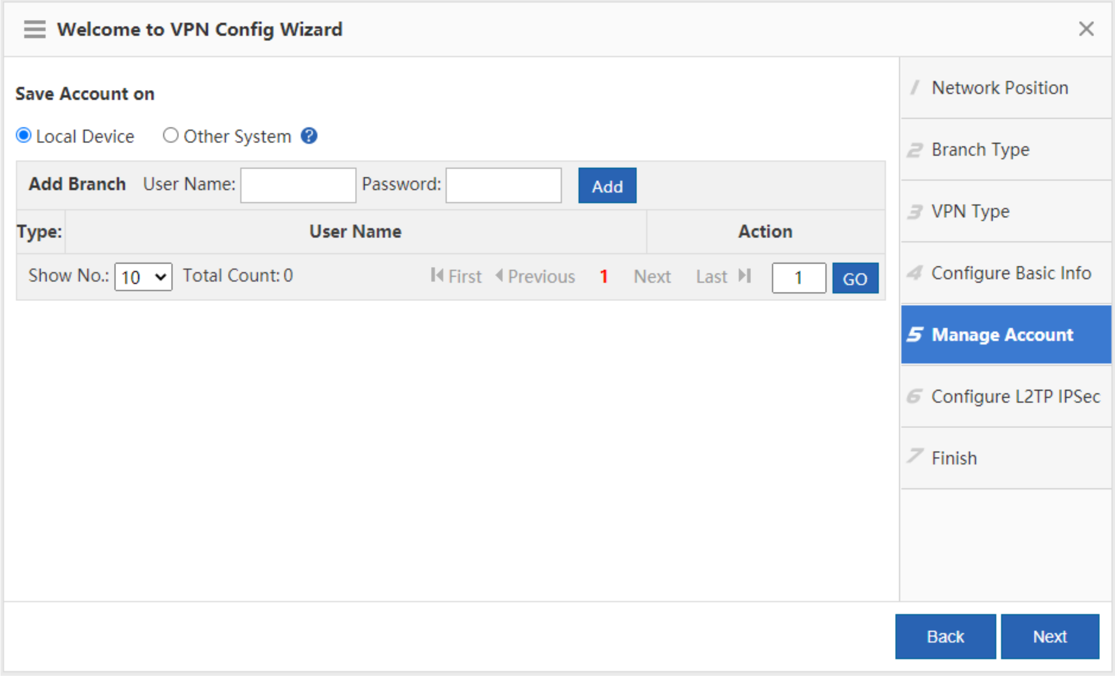
Click **Next**. The next configuration page is displayed.

(5) On the configuration page corresponding to **Manage Account**, configure user information for user authentication of clients attempting remote PPTP or L2TP access to the local device, as shown in the following figure. Select **Local Device** or **Other System** under **Save Account on**.

If you select **Local Device**, the configuration page shown in the following figure is displayed, where the table lists the user name and password information that has been configured on this device. You can click Edit or Delete in the **Action** column for modification or deletion. You can also click for user name and password adding.



Add Branch User Name: Password: Add



Welcome to VPN Config Wizard

Save Account on

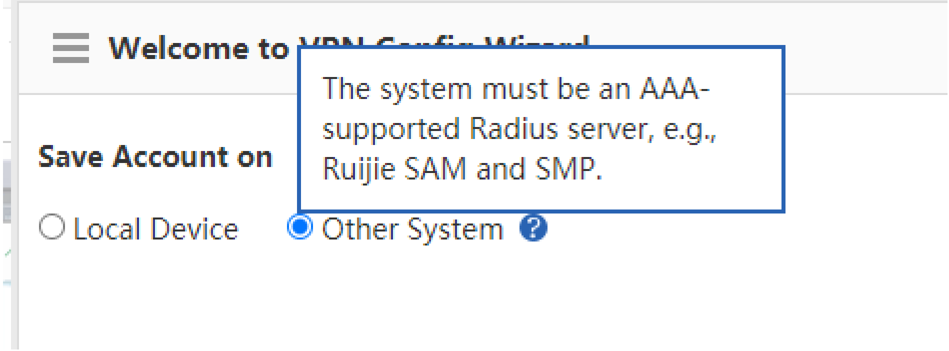
● Local Device ○ Other System

Add Branch User Name: Password: Add

Type:	User Name	Action

Show No.: 10 Total Count: 0 First Previous 1 Next Last 1 GO

If you select **Other System**, you can manage user information through a third-party server.



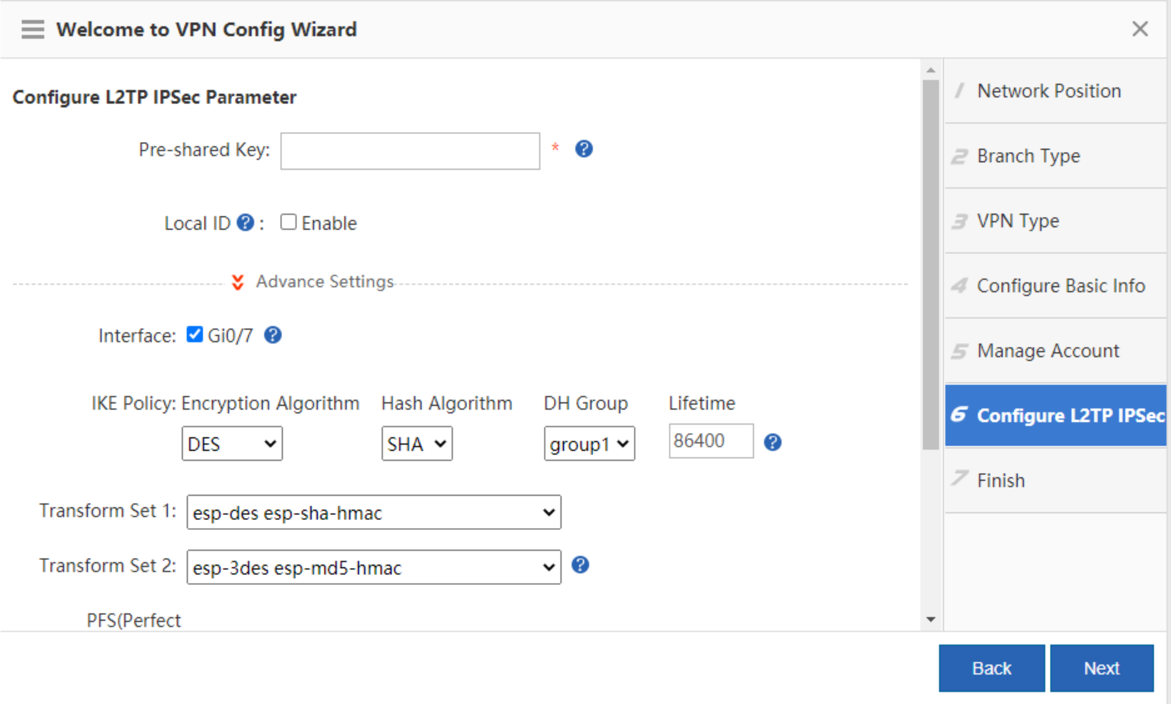
Welcome to VPN Config Wizard

The system must be an AAA-supported Radius server, e.g., Ruijie SAM and SMP.

Save Account on

○ Local Device ● Other System

(6) Set IPSec-related parameters on the configuration page shown in the following figure. (L2TP IPSec is a combination of L2TP and IPSec. If you select **Headquarter** and **L2TP IPSec**, this operation is mandatory in addition to L2TP-related parameter setting on the pages corresponding to **Configure Basic Info** and **Manage Account**.)



Welcome to VPN Config Wizard

Configure L2TP IPSec Parameter

Pre-shared Key: *

Local ID : □ Enable

Advance Settings

Interface: ☑ Gi0/7

IKE Policy: Encryption Algorithm DES; Hash Algorithm SHA; DH Group group1; Lifetime 86400

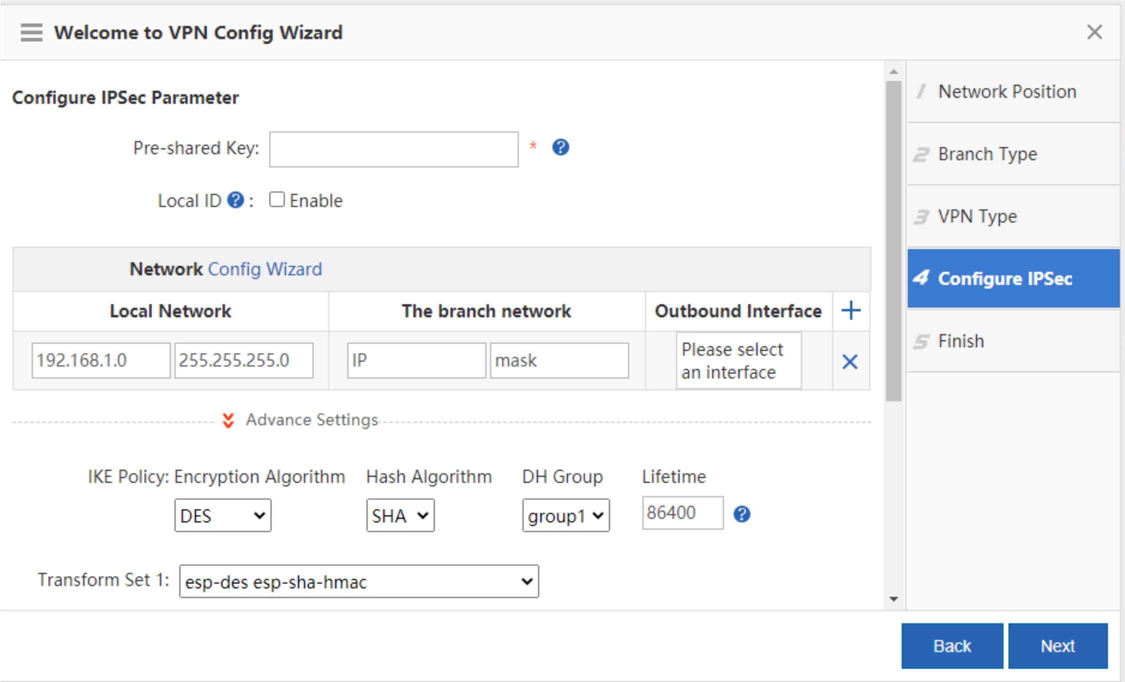
Transform Set 1: esp-des esp-sha-hmac

Transform Set 2: esp-3des esp-md5-hmac

PFS(Perfect

- **Pre-shared Key**: key that must be correctly entered on the mobile user or branch side for successful dial-in.
- **Interface**: For each interface through which IPSec communication will pass, an encrypted mapping set needs to be configured (the set associates the transform sets with data streams, describes the address of the peer end and the required parameters for communication, and completely describes what is required for IPSec communication with the remote peer. Encrypted mapping entries are required for an IPSec security association.) Extranet ports that have been configured for the device are listed, which are selected by default.
- **IKE Policy**: Set **Encryption Algorithm**, **Hash Algorithm**, and **DH Group** for IKE. To ensure successful IKE negotiation, the two parties engaged in IKE negotiation must have at least one set of consistent IKE policy.
- **Transform Set**: combination of specific security protocols and algorithms. During IPSec security association negotiation, the two parties use the same transform set to protect specific data streams.
- **IPSec Lifetime**: When the life cycle of the tunnel establishment ends, the two parties will automatically renegotiate for tunnel establishment, which can effectively prevent the tunnel from being cracked. The default lifetime 1 hour is recommended.

When IPSec VPN headquarters-related parameters are set, the page shown in the following figure is displayed. The basic parameters are generally the same as those on the configuration page shown in the preceding figure (an example for L2TP IPSec), except that the **Network** table is added. You can configure the IP addresses in the specified network segment to be encrypted for mutual access through the IPSec tunnel between the headquarters and the branch in this table.



Welcome to VPN Config Wizard

Configure IPSec Parameter

Pre-shared Key: *

Local ID : □ Enable

Network Config Wizard

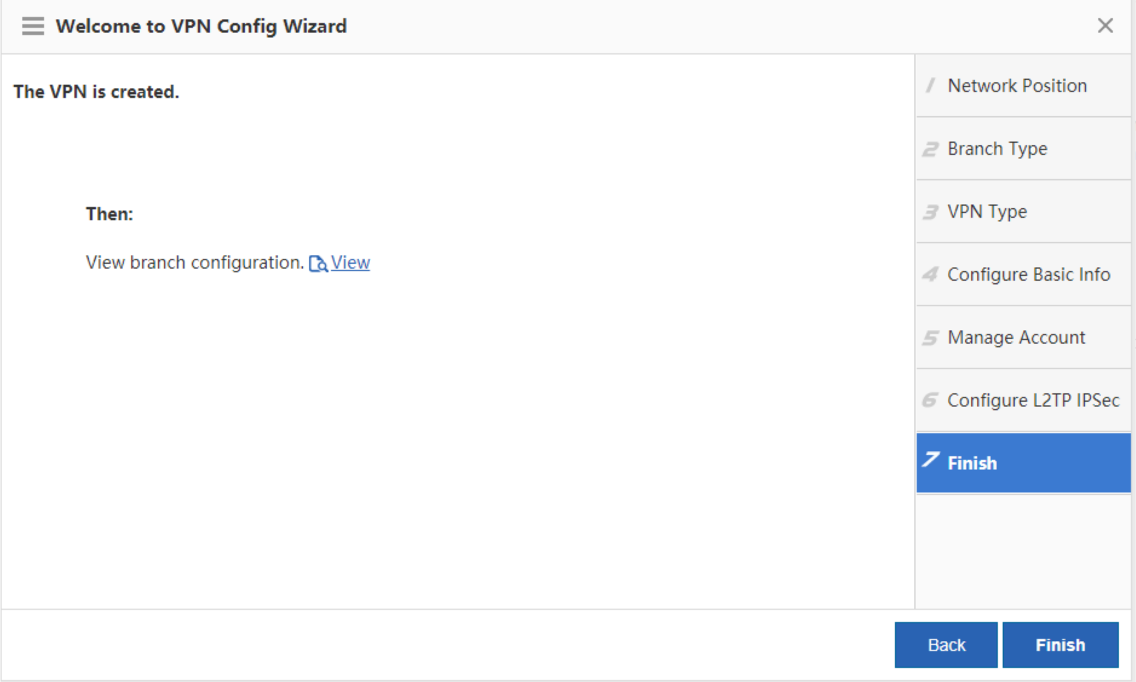
Local Network		The branch network		Outbound Interface
192.168.1.0	255.255.255.0	IP	mask	Please select an interface

Advance Settings

IKE Policy: Encryption Algorithm: DES; Hash Algorithm: SHA; DH Group: group1; Lifetime: 86400

Transform Set 1: esp-des esp-sha-hmac

(7) Click **Next**. The page shown in the following figure is displayed.



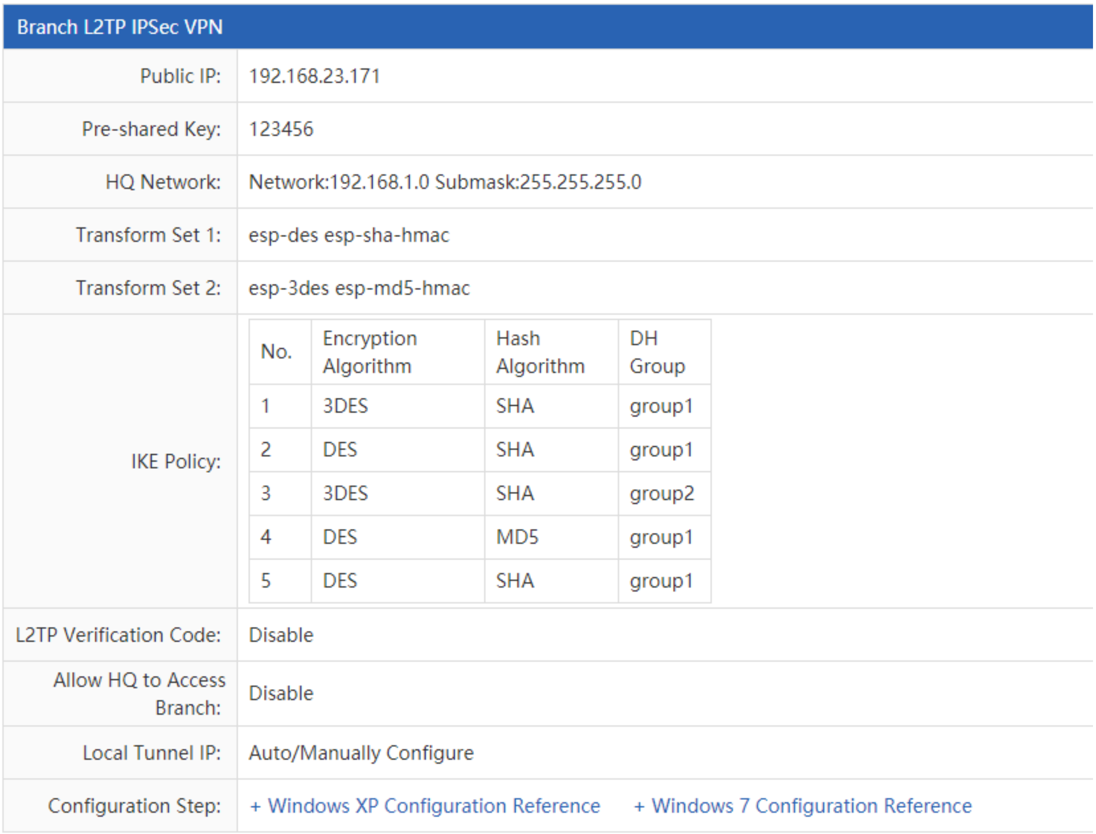
Welcome to VPN Config Wizard

The VPN is created.

Then:

View branch configuration. View

Click **Finish** in the lower right corner to complete VPN configuration for the headquarters. Before clicking **Finish**, click View to check and record the corresponding VPN configurations required for the branch, as shown in the following figure.



Branch L2TP IPSec VPN

Public IP:	192.168.23.171
Pre-shared Key:	123456
HQ Network:	Network:192.168.1.0 Submask:255.255.255.0
Transform Set 1:	esp-des esp-sha-hmac
Transform Set 2:	esp-3des esp-md5-hmac

IKE Policy:

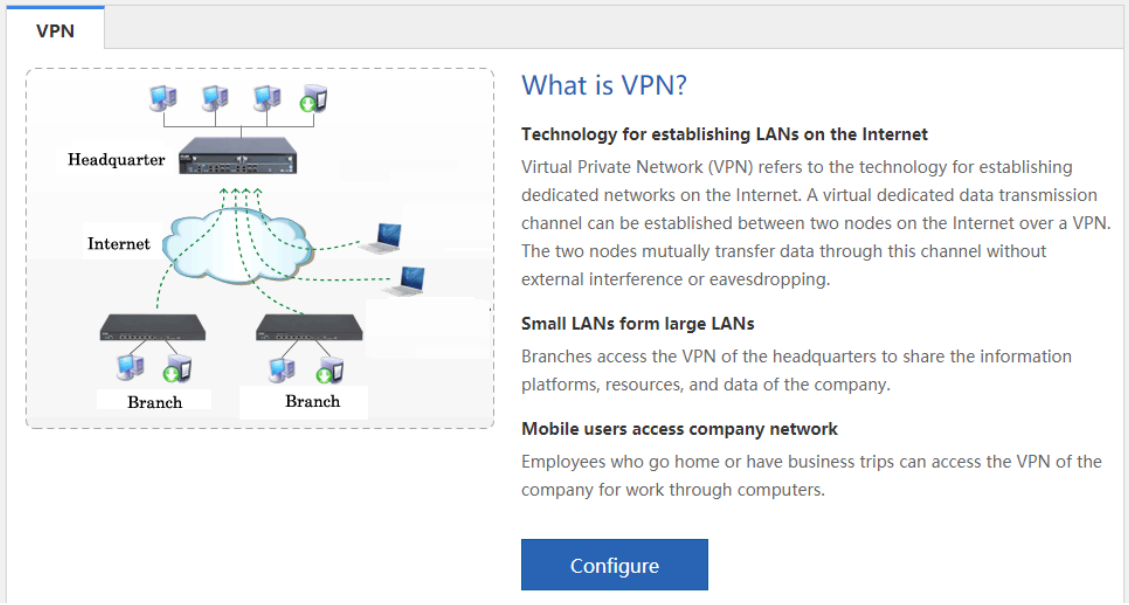
No.	Encryption Algorithm	Hash Algorithm	DH Group
1	3DES	SHA	group1
2	DES	SHA	group1
3	3DES	SHA	group2
4	DES	MD5	group1
5	DES	SHA	group1

L2TP Verification Code:	Disable
Allow HQ to Access Branch:	Disable
Local Tunnel IP:	Auto/Manually Configure
Configuration Step:	+ Windows XP Configuration Reference + Windows 7 Configuration Reference

You can also click the content corresponding to **Configuration Step** for a reference guide on how to connect a mobile user's PC to the VPN server (headquarters).

7.5.3 VPN Client (Branch) Configuration

(1) Click Configure .



What is VPN?

Technology for establishing LANs on the Internet

Virtual Private Network (VPN) refers to the technology for establishing dedicated networks on the Internet. A virtual dedicated data transmission channel can be established between two nodes on the Internet over a VPN. The two nodes mutually transfer data through this channel without external interference or eavesdropping.

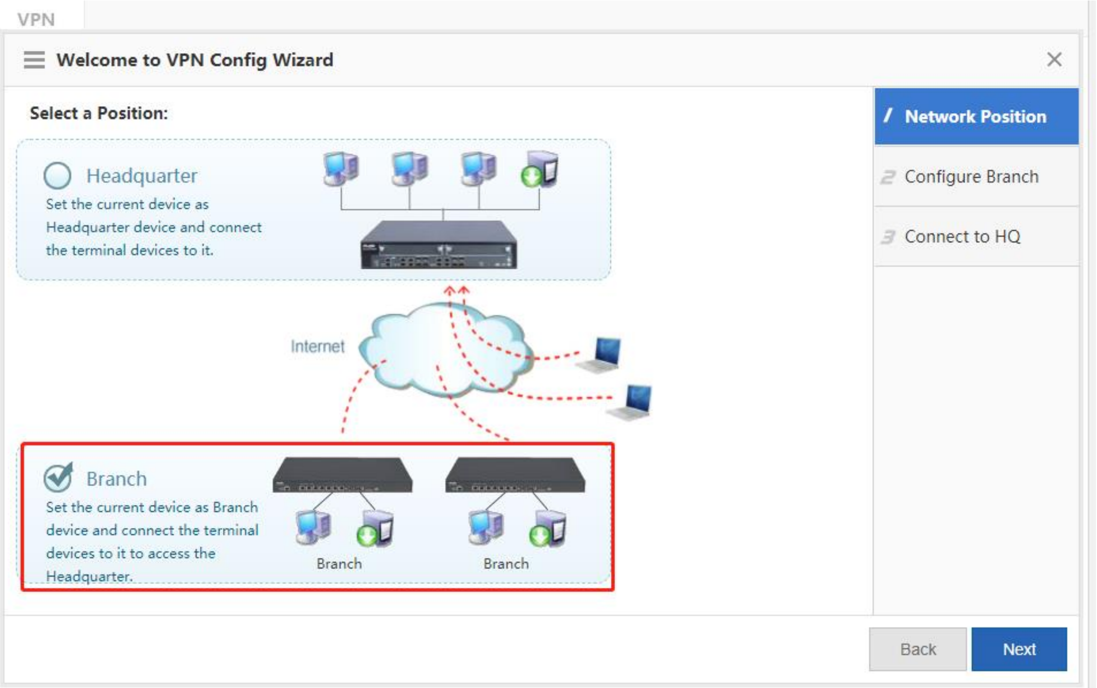
Small LANs form large LANs

Branches access the VPN of the headquarters to share the information platforms, resources, and data of the company.

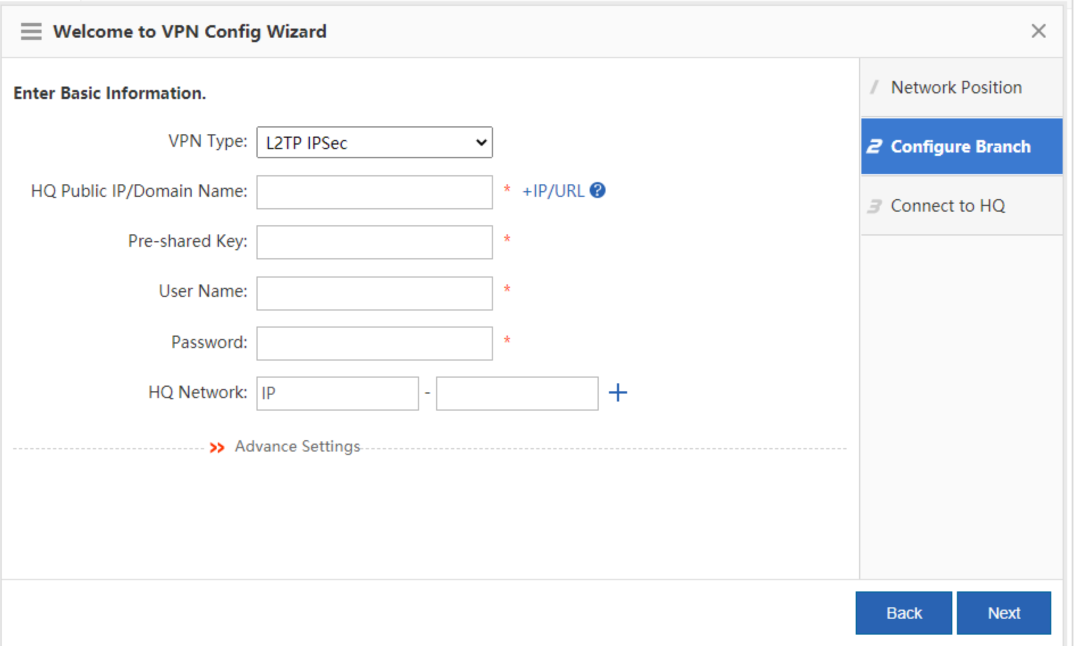
Mobile users access company network

Employees who go home or have business trips can access the VPN of the company for work through computers.

(2) Select **Branch** and click **Next**.


VPN
Welcome to VPN Config Wizard
Select a Position:
Headquarter
Set the current device as Headquarter device and connect the terminal devices to it.
Internet
Branch
Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.
Branch
Branch
1 Network Position
2 Configure Branch
3 Connect to HQ
Back
Next

(3) Set the VPN client parameters.



Enter Basic Information.

VPN Type: L2TP IPSec

HQ Public IP/Domain Name: * +IP/URL

Pre-shared Key: *

User Name: *

Password: *

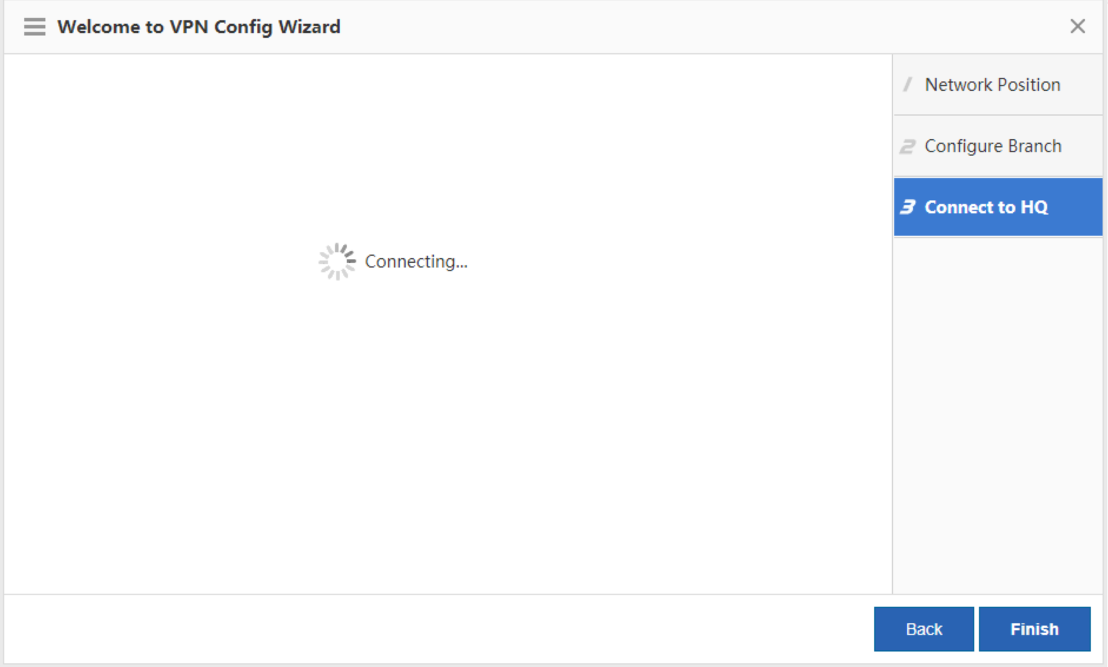
HQ Network: IP -

» Advance Settings

- **VPN Type**: Set it to L2TP IPSec, L2TP, or IPSec.
- **HQ Public IP**: public IP address of the VPN server (headquarters).
- **Pre-shared Key**: the same as that configured for the VPN server (headquarters), which can be obtained from the VPN server (headquarters) administrator.
- **User Name/Password**: user name/password for login to the VPN.
- **HQ Network**: intranet network segment of the headquarters to be accessed.

- ○ **Advanced Settings**: includes **IKE Policy**, **Transform Set**, and **Allow HQ to Access Branch**, which must be set the same as those for the VPN server (headquarters).

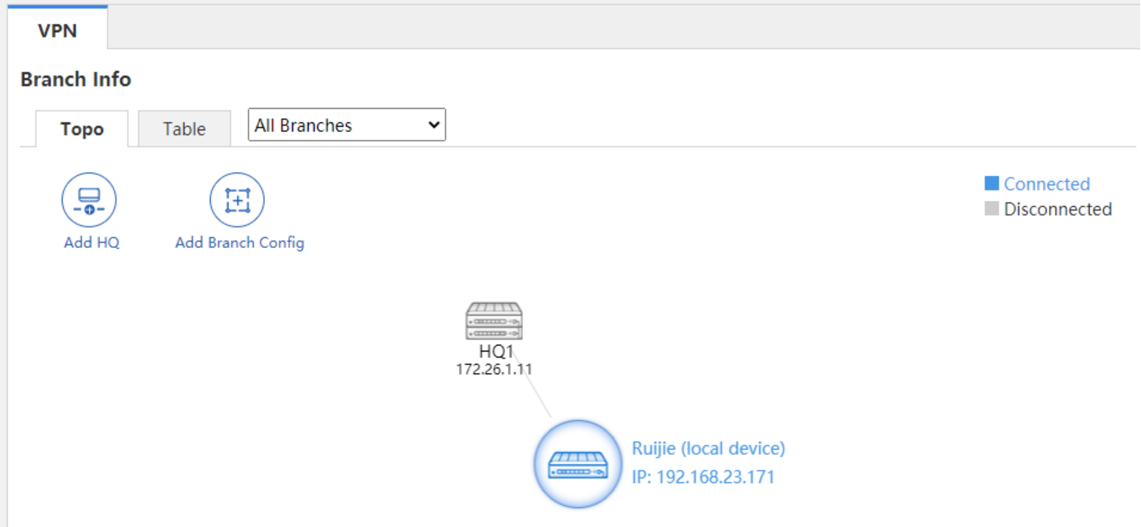
(4) Click **Next**. The page shown in the following figure is displayed. Wait for a period of time. A prompt indicating successful connection or connection failure is displayed. If the connection is successful, click **Finish** in the lower right corner to complete VPN configuration for the branch.



7.5.4 VPN Configuration Management

1. Topo

After VPN configuration, the configuration page shown in the following figure is displayed.



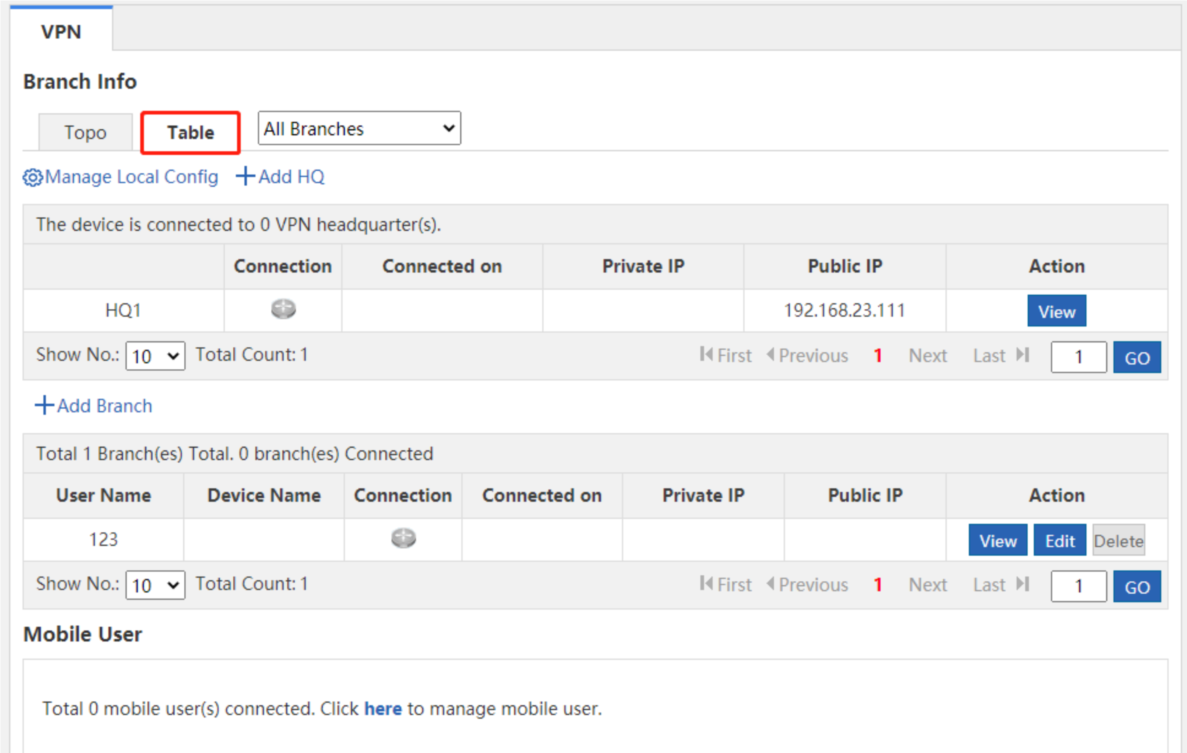
You can view the location of the local device in the topology area, where the device with "(local device)" is the one currently under configuration, as shown by Ruijie (local device) IP: 192.168.23.171 in the preceding figure. You can click this icon to view and modify VPN configuration information about the local device. In the topology, gray devices indicate disconnected users or devices, gray lines indicate VPN channels where connection is not successfully established, and blue devices/lines indicate successfully connected VPN devices/channels.

The device above the local device indicates the headquarters to which the local device is connected when it is used as a VPN branch. Click Add HQ to add the headquarters to which the local device is to be connected when it is used as a VPN branch. You can perform the configuration for multiple times. The local device can be connected to a maximum of nine VPN headquarters. For details about the configuration, see 7.5.3 VPN Client (Branch) Configuration.

The devices below the local device indicate the devices connected to the local device when it is used as the VPN headquarters. If the local device is used as the L2TP or L2TP IPSec VPN headquarters, Add Branch is displayed. You can click it to add an account.

If the current device is only configured as a VPN branch, as shown in the following figure, you can click Add Branch Config to configure the local device as the VPN headquarters. For details, see 7.5.2 VPN Server (Headquarters) Configuration.

2. Table



The device is connected to 0 VPN headquarter(s).

	Connection	Connected on	Private IP	Public IP	Action
HQ1	●			192.168.23.111	View

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

Total 1 Branch(es) Total. 0 branch(es) Connected

User Name	Device Name	Connection	Connected on	Private IP	Public IP	Action
123		●				View Edit Delete

Show No.: 10 Total Count: 1 First Previous 1 Next Last 1 GO

Mobile User

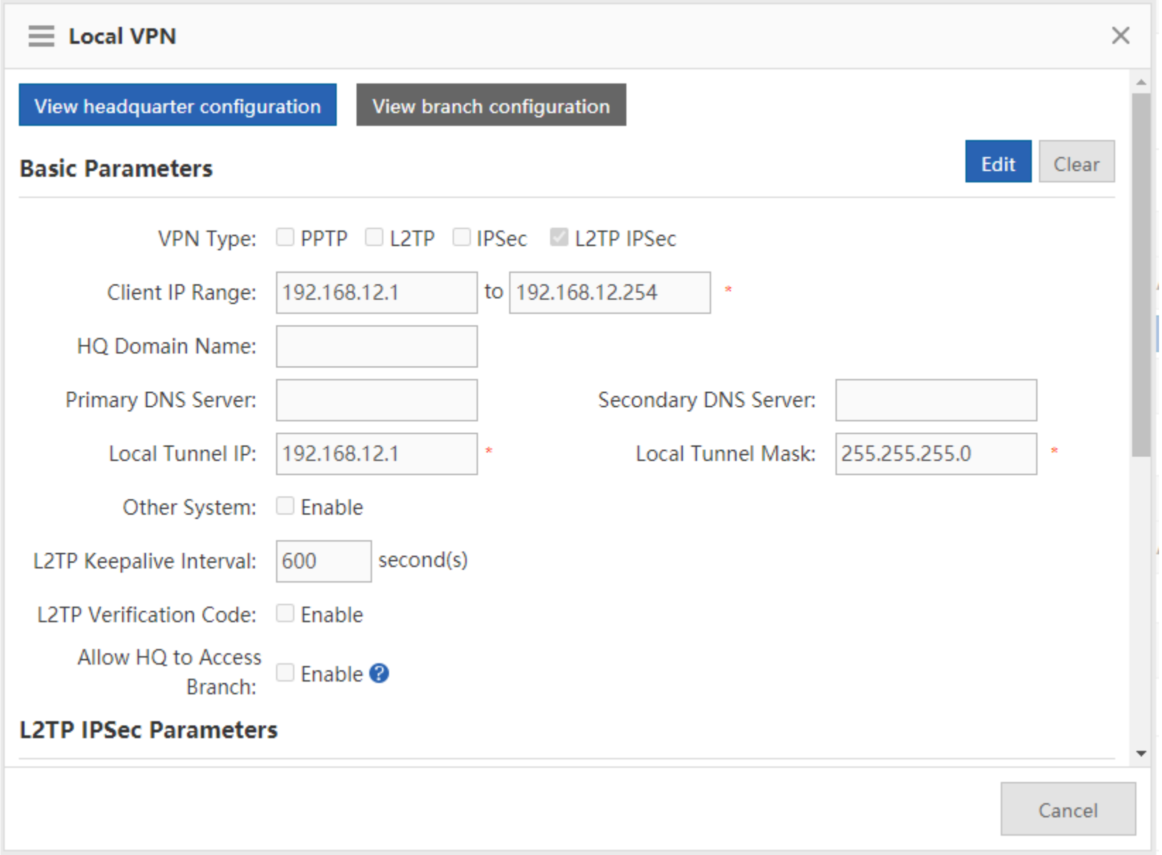
Total 0 mobile user(s) connected. Click here to manage mobile user.

As shown in the preceding figure, the first table lists the information about the headquarters to which the local host is connected when it is used as a VPN branch; the second table lists the information about the branches connected to the local host when it is used as the VPN headquarters.

You can click Manage Local Config to view and modify VPN configuration information about the local device. You can click Add HQ to add multiple headquarters to which the local device is to be connected when it is used as a VPN branch. You can click Add Branch to add user information. You can click the corresponding icon View Edit Delete in the **Action** column of the table to view/modify/delete information about the selected user.

3. View headquarter configuration/View branch configuration

Click the local device icon on the **Topo** tab page or click **Manage Local Config** on the **Table** tab page. The window shown in the following figure is displayed. You can view the VPN configuration information about the local device.



Basic Parameters

VPN Type: □ PPTP □ L2TP □ IPSec ☑ L2TP IPSec

Client IP Range: 192.168.12.1 to 192.168.12.254 *

HQ Domain Name:

Primary DNS Server: Secondary DNS Server:

Local Tunnel IP: 192.168.12.1 * Local Tunnel Mask: 255.255.255.0 *

Other System: □ Enable

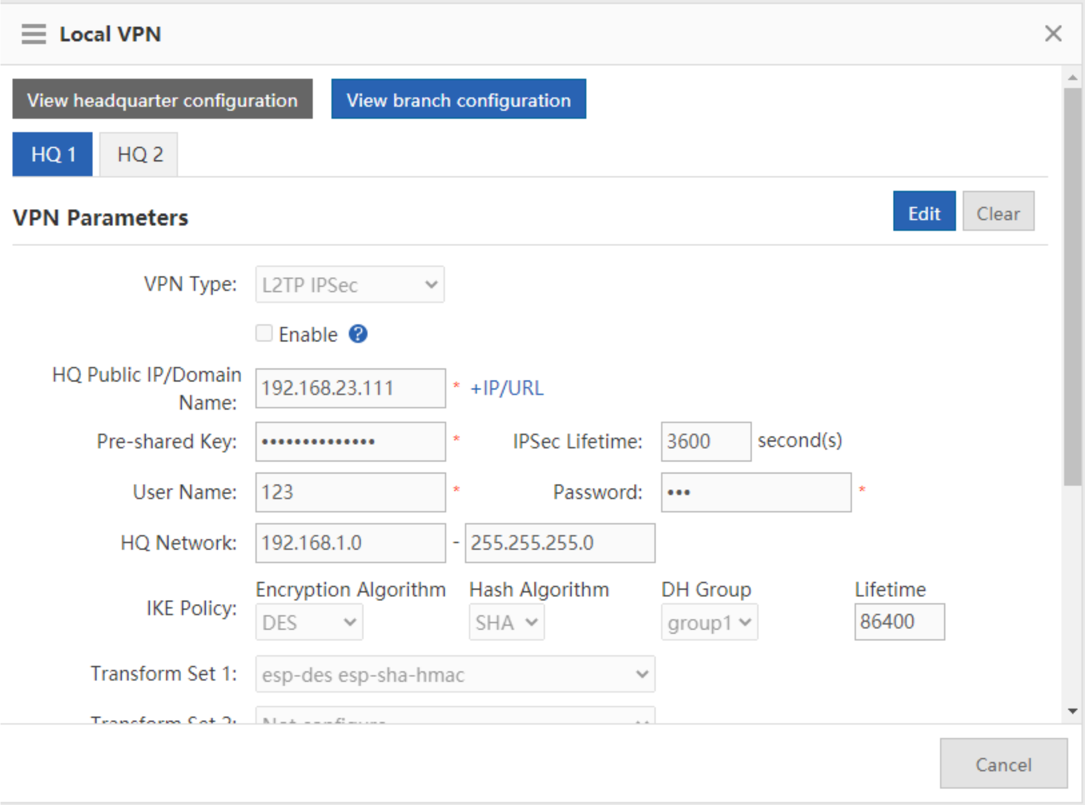
L2TP Keepalive Interval: 600 second(s)

L2TP Verification Code: □ Enable

Allow HQ to Access Branch: □ Enable ?

L2TP IPSec Parameters

If View headquarter configuration is blue, the configuration information about the device that is used as the VPN headquarters is displayed. In this case, click View branch configuration. The configuration information about the device that is used as a VPN branch is displayed, as shown in the following figure.



VPN Parameters

VPN Type: L2TP IPSec

□ Enable

HQ Public IP/Domain Name: 192.168.23.111 * +IP/URL

Pre-shared Key: •••••••••••••• * IPSec Lifetime: 3600 second(s)

User Name: 123 * Password: ••• *

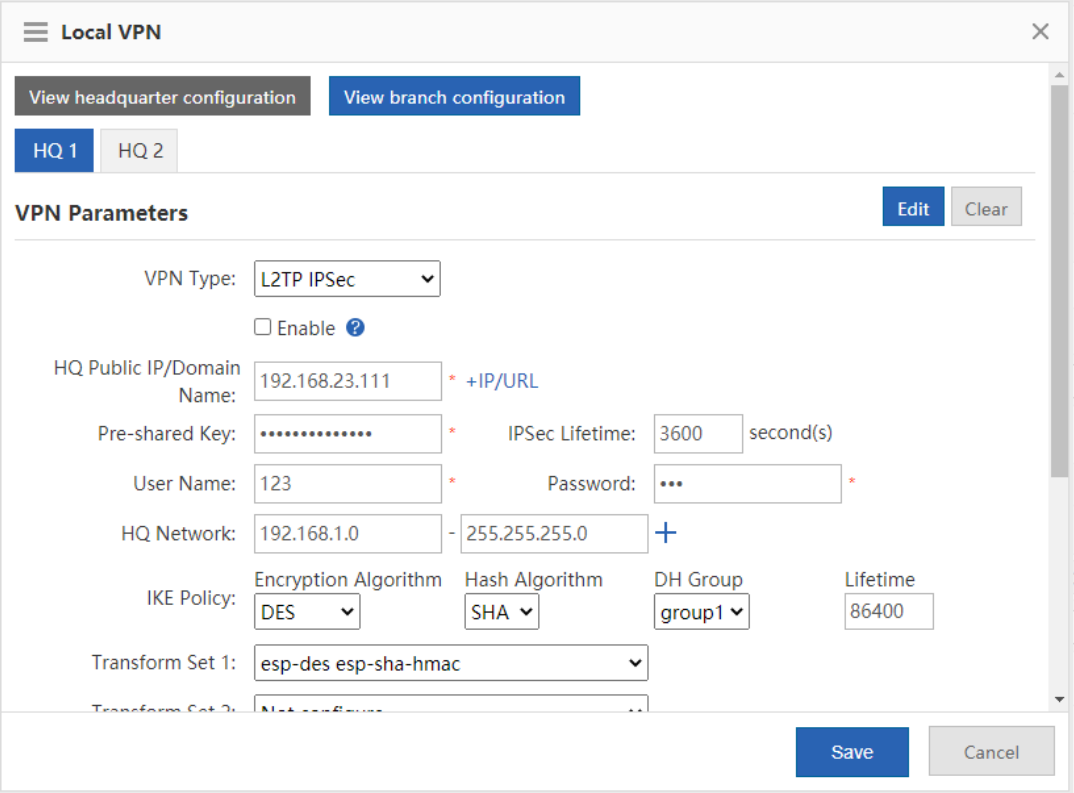
HQ Network: 192.168.1.0 - 255.255.255.0

	Encryption Algorithm	Hash Algorithm	DH Group	Lifetime
IKE Policy:	DES	SHA	group1	86400

Transform Set 1: esp-des esp-sha-hmac

If the local device used as a VPN branch is connected to multiple devices, there are multiple tabs above **VPN Parameters**, as shown by HQ 1 HQ 2. In this case, the VPN configuration about the local device connected to headquarters 1 is displayed. You can click HQ 2. The VPN configuration about the local device connected to headquarters 2 is displayed.

You can click Edit to modify the current VPN configuration information, as shown in the following figure.



VPN Parameters

VPN Type: L2TP IPSec

□ Enable

HQ Public IP/Domain Name: 192.168.23.111 *

Pre-shared Key: •••••••••••••• *

IPSec Lifetime: 3600 second(s)

User Name: 123 *

Password: ••• *

HQ Network: 192.168.1.0 - 255.255.255.0

IKE Policy: Encryption Algorithm DES; Hash Algorithm SHA; DH Group group1; Lifetime 86400

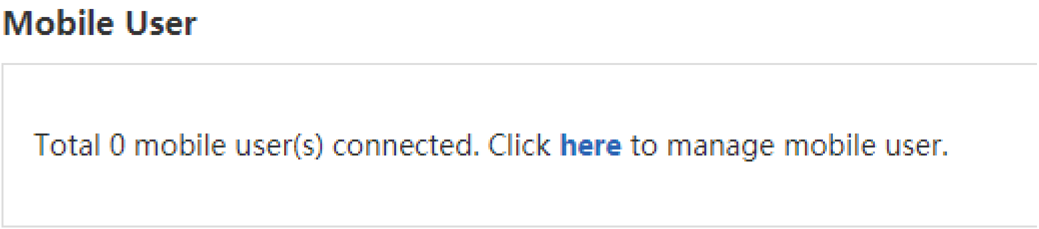
Transform Set 1: esp-des esp-sha-hmac

Click Save.

You can click Cancel to clear the current VPN configuration information. For example, if the **HQ2** tab is clicked, the local device will be disconnected from headquarters 2.

4. Mobile User

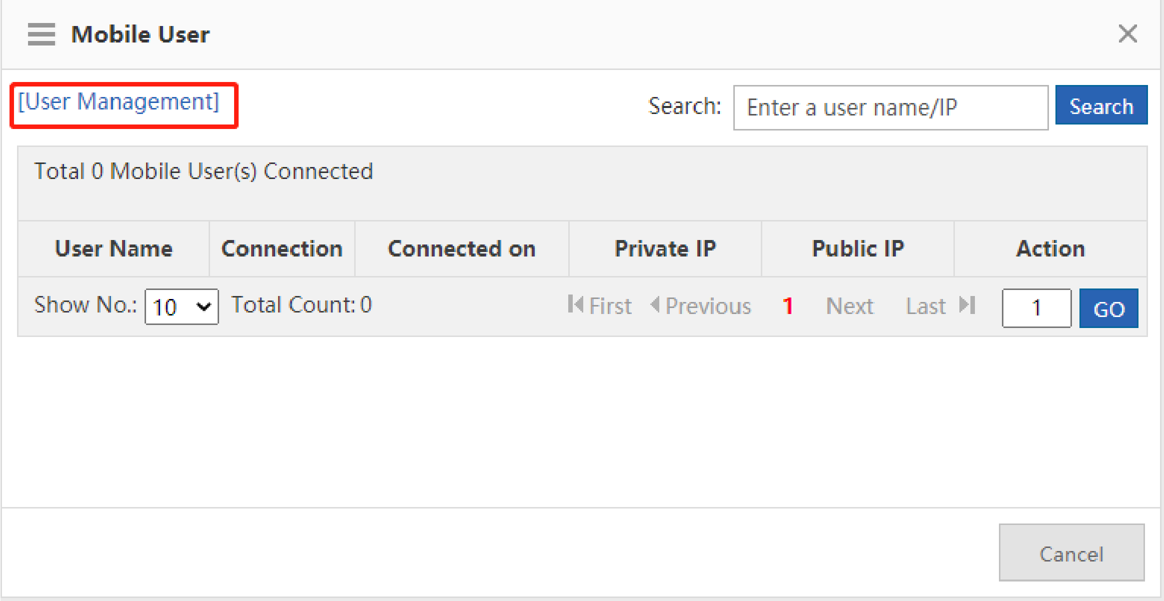
When the local device is configured as the VPN headquarters, you can view the mobile user configuration information on the VPN monitoring page, as shown in the following figure.



Mobile User

Total 0 mobile user(s) connected. Click here to manage mobile user.

Click here. The mobile user management page is displayed, as shown in the following figure. You can view, modify, or delete information about a specific user and click [User Management] for mobile user management.



Total 0 Mobile User(s) Connected

User Name	Connection	Connected on	Private IP	Public IP	Action

Total Count: 0

7.6 NAT/Port Mapping

7.6.1 Introduction

Network Address Translation (NAT) allows an entire organization to appear on the Internet with a common IP address. As the term implies, it is a technology that translates internal private network addresses (IP addresses) into legal network IP addresses.

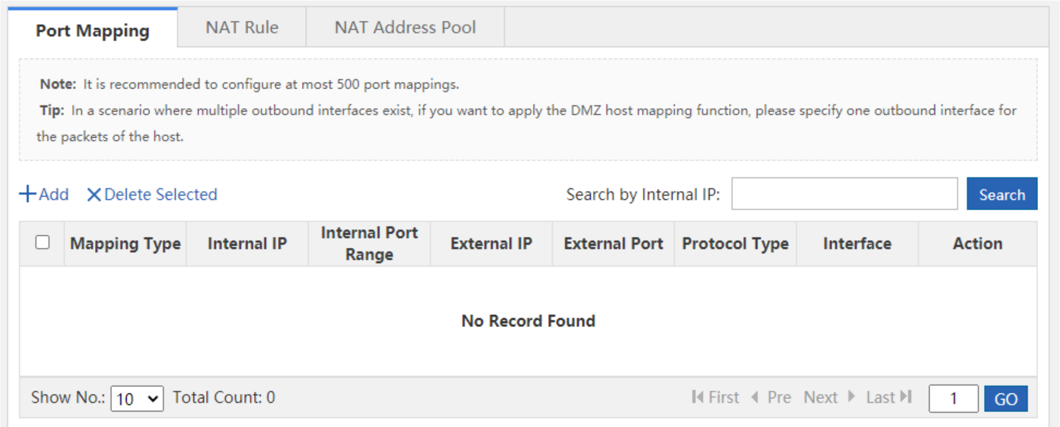
7.6.2 Port Mapping

The following two types of port mapping are available: port mapping and DMZ host mapping.

1. Port Mapping

Procedure

(1) Choose **Network** > **NAT/Port Mapping** > **Port Mapping**.



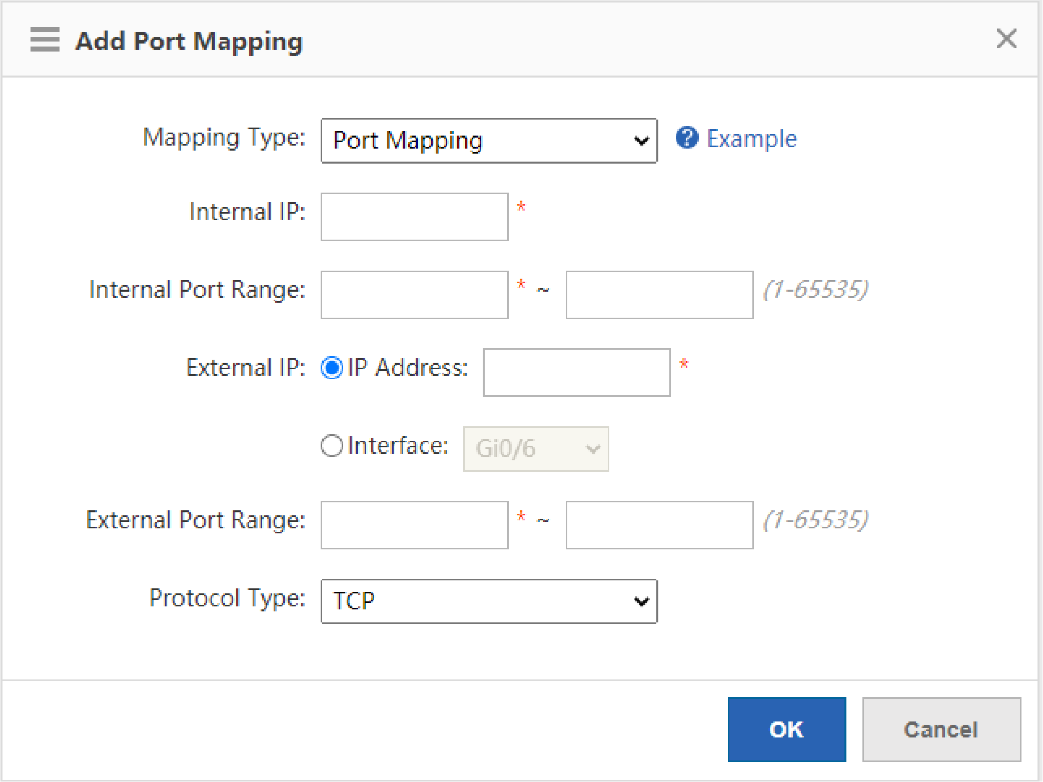
Note: It is recommended to configure at most 500 port mappings.
Tip: In a scenario where multiple outbound interfaces exist, if you want to apply the DMZ host mapping function, please specify one outbound interface for the packets of the host.

□	Mapping Type	Internal IP	Internal Port Range	External IP	External Port	Protocol Type	Interface	Action

No Record Found

Total Count: 0

(2) Click **Add**, set **Mapping Type** to **Port Mapping**, set related configuration items, and click **OK**.



Add Port Mapping

Mapping Type: Port Mapping ❔ Example

Internal IP: *

Internal Port Range: * ~ (1-65535)

External IP: ● IP Address: *

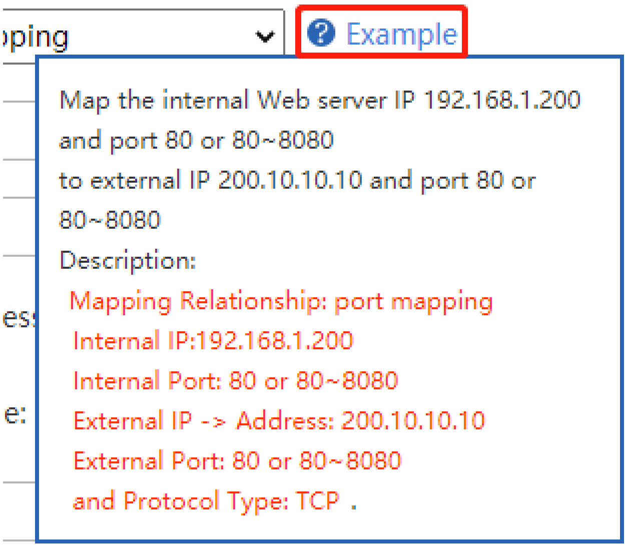
○ Interface: Gi0/6

External Port Range: * ~ (1-65535)

Protocol Type: TCP

- **Internal IP**: intranet IP address to be mapped to the extranet, which is generally the IP address of your server.
- **Internal Port Range**: port(s) to be mapped to the extranet.
- **External IP**: WAN IP address. If **Interface** is set, all IP addresses at the extranet interface will be mapped.
- **External Port Range**: ports on the WAN. The port number ranges from 1 to 65535.
- **Protocol Type**: Select **TCP** or **UDP** as required.

You can click **Example** for configuration according to the example.



Example

Map the internal Web server IP 192.168.1.200 and port 80 or 80~8080 to external IP 200.10.10.10 and port 80 or 80~8080

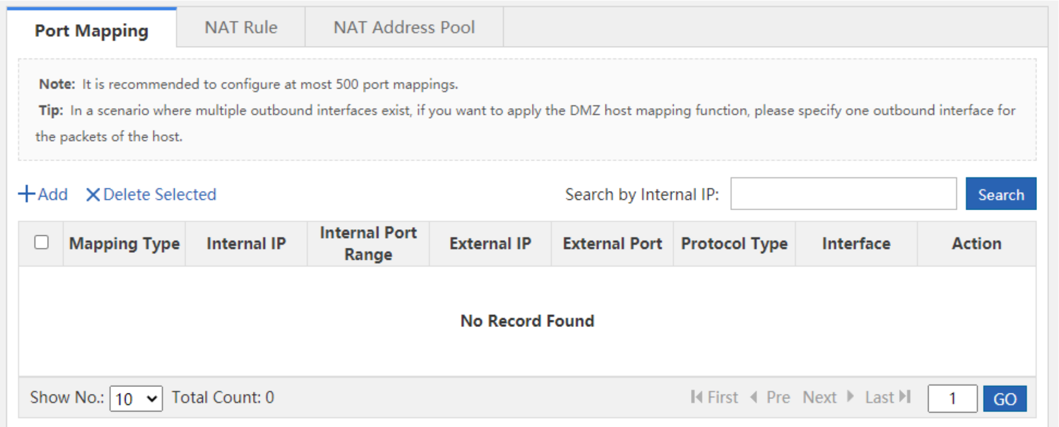
Description:

Mapping Relationship: port mapping
Internal IP:192.168.1.200
Internal Port: 80 or 80~8080
External IP -> Address: 200.10.10.10
External Port: 80 or 80~8080
and Protocol Type: TCP .

2. DMZ Host

Procedure

(1) Choose **Network** > **NAT/Port Mapping** > **Port Mapping**.

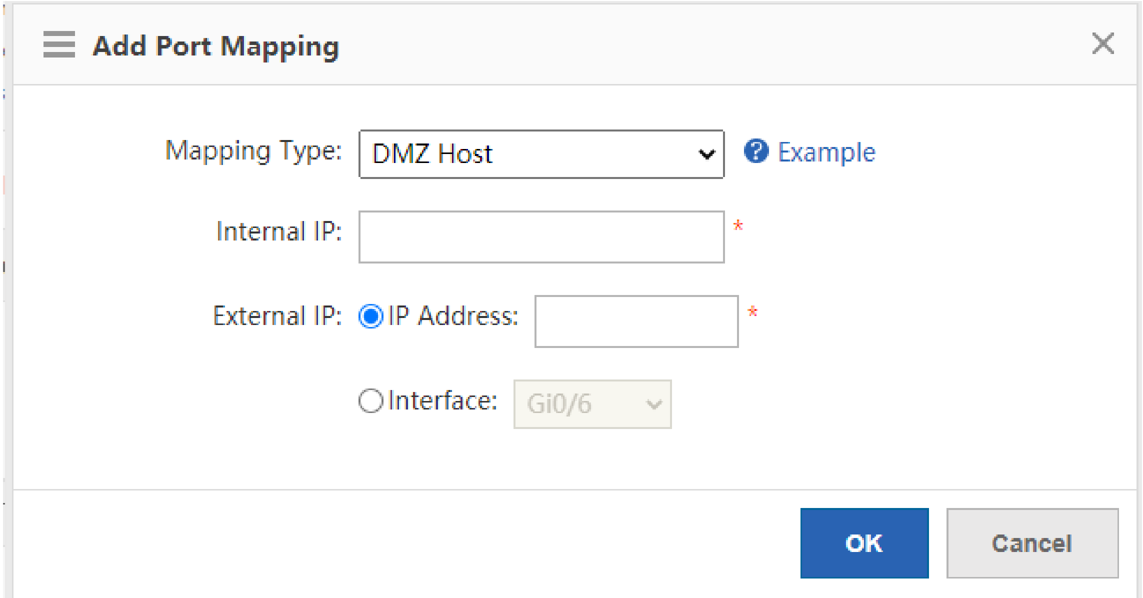


Note: It is recommended to configure at most 500 port mappings.
Tip: In a scenario where multiple outbound interfaces exist, if you want to apply the DMZ host mapping function, please specify one outbound interface for the packets of the host.

□	Mapping Type	Internal IP	Internal Port Range	External IP	External Port	Protocol Type	Interface	Action
No Record Found								

Show No.: 10 Total Count: 0

(2) Click **Add**, set **Mapping Type** to **DMZ Host**, set **Internal IP** and **IP Address/Interface** corresponding to **External IP**, and click **OK**. When an incoming packet does not hit any port mapping rule, the packet is redirected to the intranet server according to the DMZ rule. This indicates that all data packets proactively sent from the Internet to the device are forwarded to the specified DMZ host.



Mapping Type: DMZ Host

Internal IP: *

External IP: ● IP Address: *

○ Interface: Gi0/6

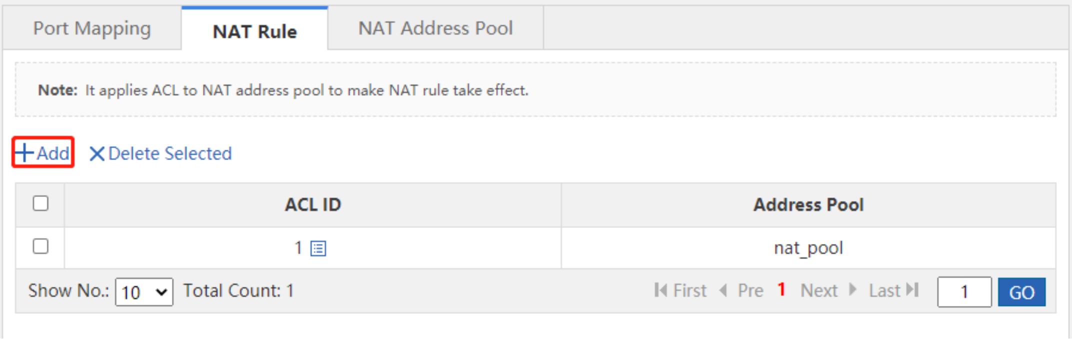
7.6.3 NAT Rule

Application Scenario

The function allows application of an ACL to a NAT address pool. That is, only addresses that match the ACL will be translated.

Procedure

(1) Choose **Network** > **NAT/Port Mapping** > **NAT Rule**.

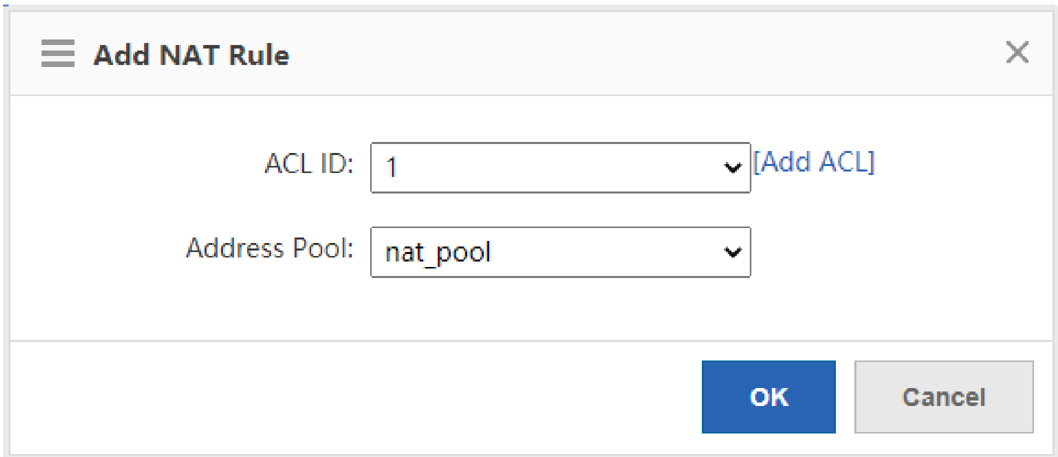


Note: It applies ACL to NAT address pool to make NAT rule take effect.

□	ACL ID	Address Pool
□	1	nat_pool

Show No.: 10 Total Count: 1

(2) Click **Add**.



ACL ID: 1

Address Pool: nat_pool

(2) Set related configuration items.

- **ACL ID**: No. or name of the ACL where this rule is applied.
- **Address Pool**: destination address pool.

(3) Click **OK**.

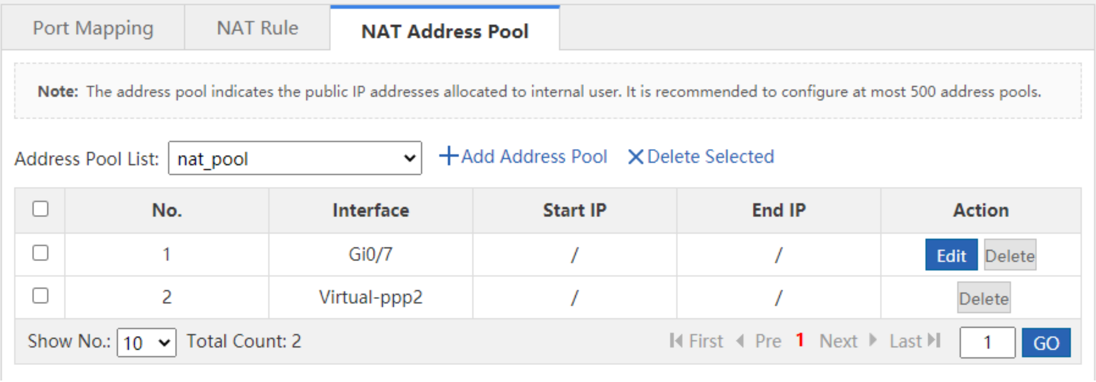
7.6.4 NAT Address Pool

Application Scenario

When there are multiple extranet IP addresses, you can add an address pool for the intranet IP address to automatically select the extranet IP addresses in the address pool for translation.

Procedure

(1) Choose **Network** > **NAT/Port Mapping** > **NAT Address Pool**.



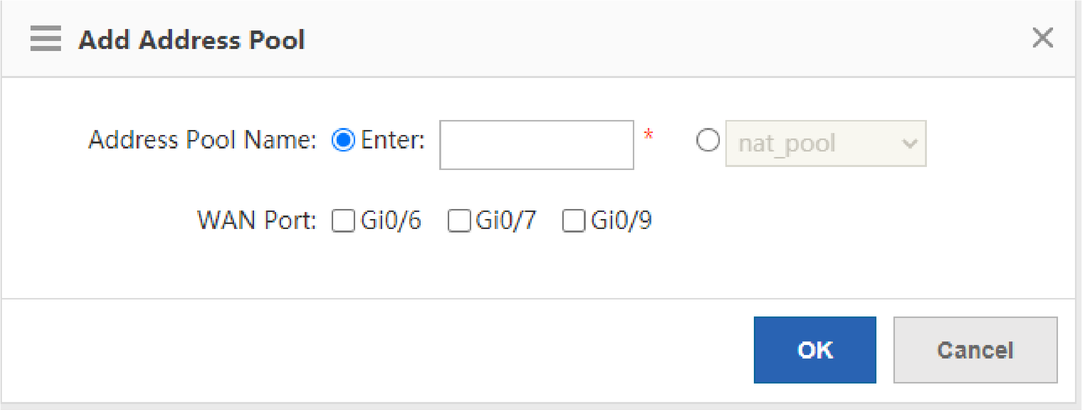
Note: The address pool indicates the public IP addresses allocated to internal user. It is recommended to configure at most 500 address pools.

Address Pool List: nat_pool

□	No.	Interface	Start IP	End IP	Action
□	1	Gi0/7	/	/	Edit Delete
□	2	Virtual-ppp2	/	/	Delete

Show No.: 10 Total Count: 2

(2) Click **Add Address Pool**.



Add Address Pool

Address Pool Name: ● Enter: [ ] * ○ nat_pool

WAN Port: □ Gi0/6 □ Gi0/7 □ Gi0/9

(3) Set related configuration items.

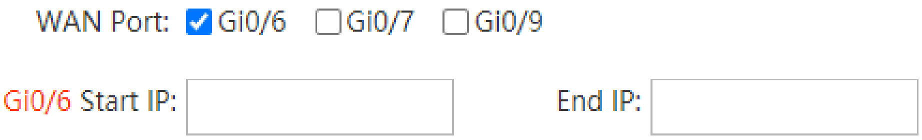
- **Address Pool Name**: name of the address pool.

  For address adding to an existing address pool, select the existing address pool, as shown by

● nat_pool

.

- **WAN Port**: Select the extranet port for address adding. In this case, the configuration items shown in the following figure are displayed below.



WAN Port: ☑ Gi0/6 □ Gi0/7 □ Gi0/9

Gi0/6 Start IP: [ ] End IP: [ ]

Set **Start IP** and **End IP**. If there is only one IP address, set **Start IP** and **End IP** to the same IP address. You can configure multiple network segments for one address pool, which cannot overlap.

(4) Click **OK** to save the configurations.

7.7 DHCP Configuration

7.7.1 Introduction

Dynamic Host Configuration Protocol (DHCP) is a network management protocol applied on the LAN. It works using UDP and is widely used to dynamically allocate network resources that can be reused, such as IP addresses. For smaller networks, DHCP makes subsequent network device adding easy and fast.

Using DHCP enjoys the following benefits:

- Reduced client configuration and maintenance costs

DHCP is easy to configure and deploy. For non-technical users, DHCP can minimize configuration-related operations on the client and reduce remote deployment and maintenance costs.

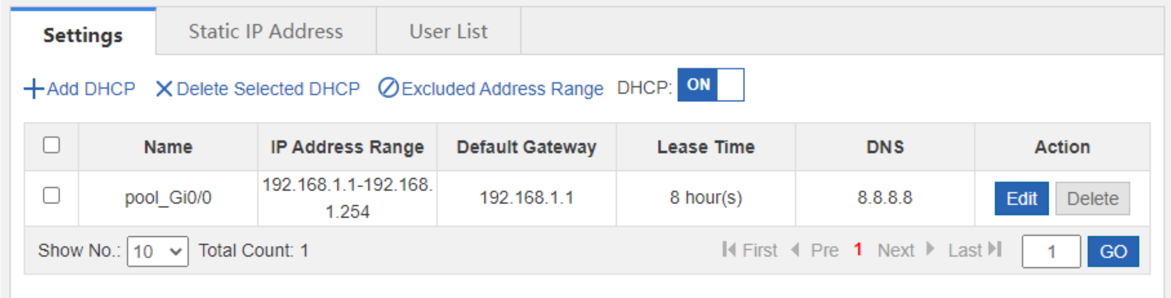
- Central management

The DHCP server can be used to manage the configuration information about multiple network segments. When the configurations of a network segment change, the administrator only needs to update related configurations on the DHCP server.

The NBR series router device can function as a DHCP server to provide IP addresses for intranet users.

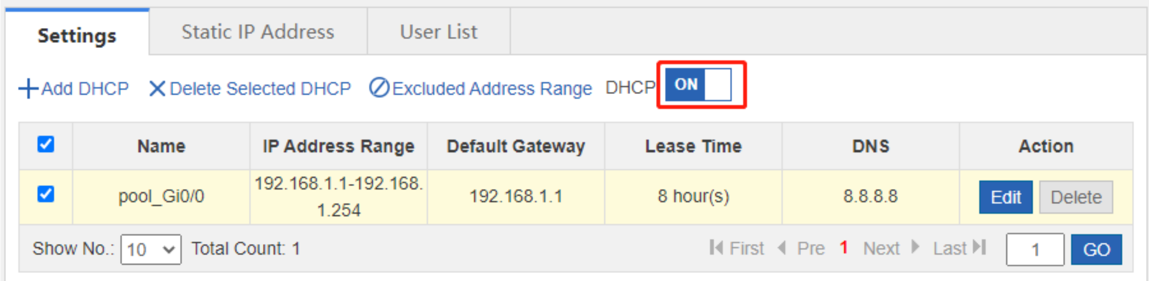
7.7.2 Settings

Choose **Network** > **DHCP** > **Settings**.



☐	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
☐	pool_Gi0/0	192.168.1.1-192.168.1.254	192.168.1.1	8 hour(s)	8.8.8.8	Edit Delete

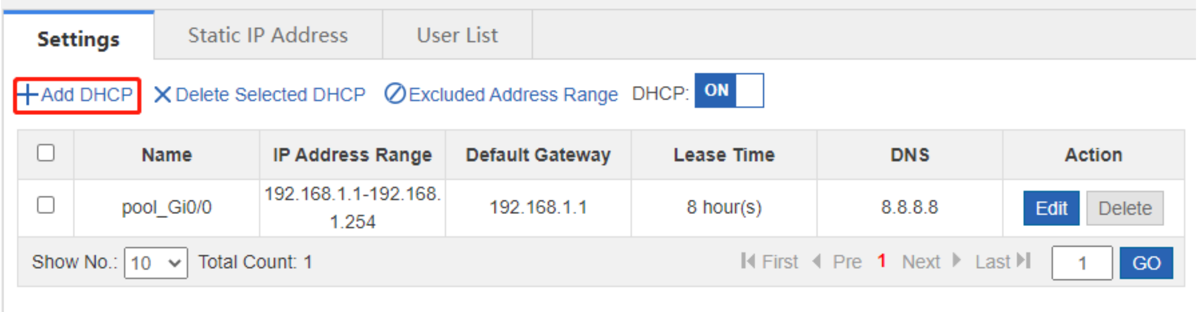
- Set **DHCP** to **ON**.



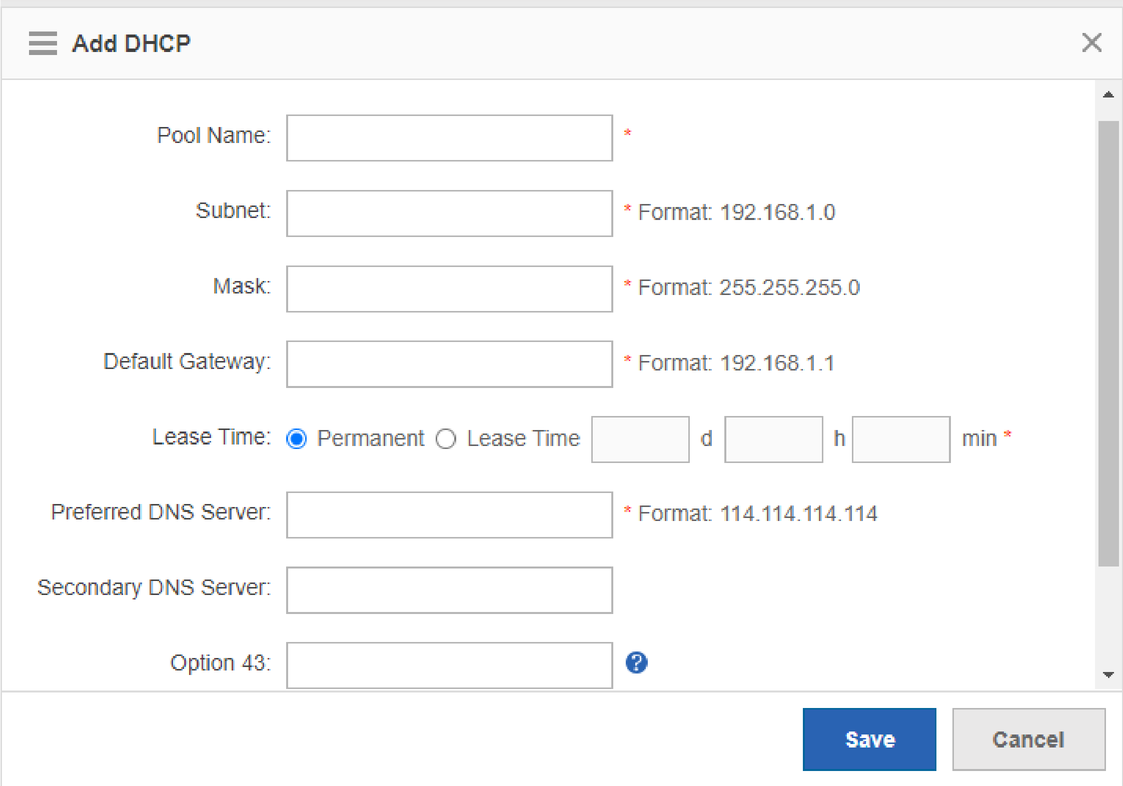
☑	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
☑	pool_Gi0/0	192.168.1.1-192.168.1.254	192.168.1.1	8 hour(s)	8.8.8.8	Edit Delete

- Add a DHCP entry.

Click **Add DHCP** in the upper left corner and set related parameters in the **Add DHCP** window.



☐	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
☐	pool_Gi0/0	192.168.1.1-192.168.1.254	192.168.1.1	8 hour(s)	8.8.8.8	Edit Delete



Add DHCP

Pool Name: *

Subnet: * Format: 192.168.1.0

Mask: * Format: 255.255.255.0

Default Gateway: * Format: 192.168.1.1

Lease Time: ● Permanent ○ Lease Time d h min *

Preferred DNS Server: * Format: 114.114.114.114

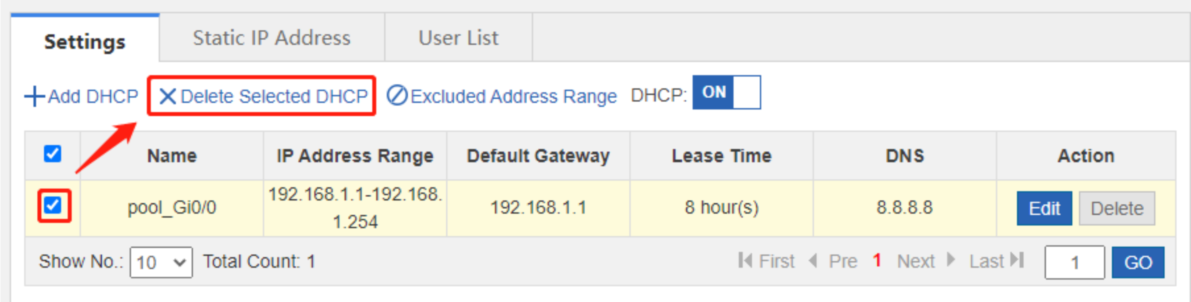
Secondary DNS Server:

Option 43:

- ○ **Pool Name**: address pool name.
- ○ **Subnet**: network segment for assignment.
- ○ **Mask**: subnet mask. The range of IP addresses to be assigned is determined by the values of **Subnet** and this parameter.
- ○ **Default Router**: default router for assignment.
- ○ **Lease Time**: address lease period. After the lease period expires, IP addresses will be reclaimed without renewal.
- ○ **DNS Server**: DNS server address for assignment.
- ○ **Option 43**: When the AC (wireless controller) and the AP are not on the same LAN, the AP cannot detect the AC through broadcast after obtaining an IP address from the DHCP server. To enable the AP to detect the AC, you need to configure Option 43 information carried in the DHCP response packet on the DHCP server.
- ○ **Option 138**: Similar to Option 43, when the AC and AP are not on the same LAN, you can configure Option 138 to enable the downlink AP to obtain the IPv4 address of the AC.

- ● Delete DHCP configuration entries in batches.

Select the DHCP configuration entries to be deleted and click **Delete Selected DHCP**.

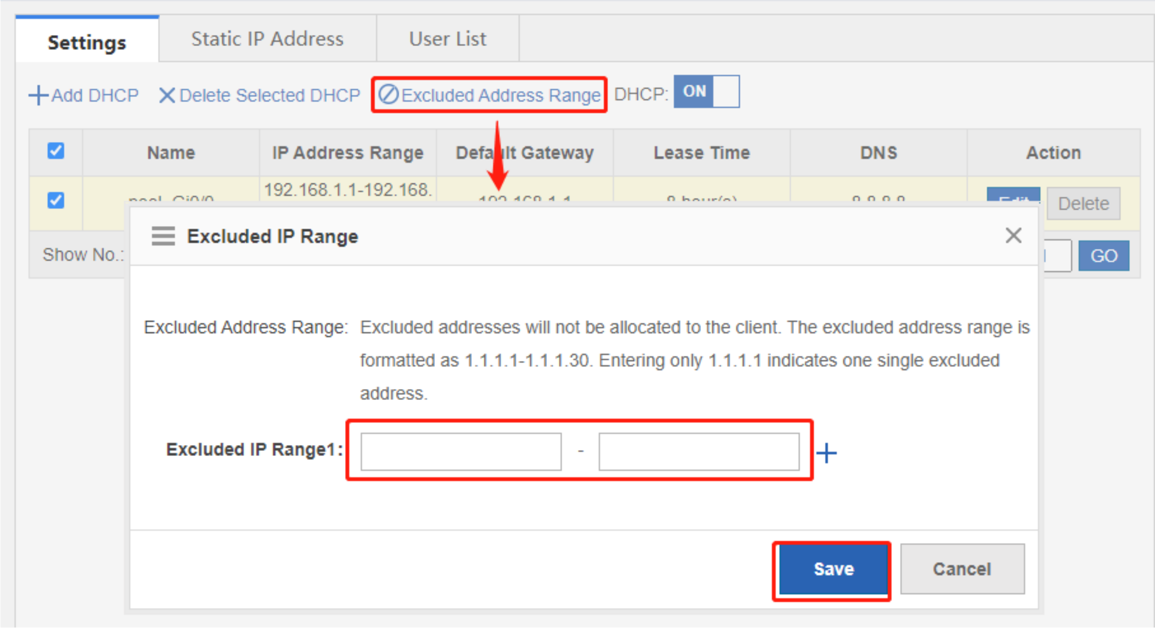


☑	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
☑	pool_Gi0/0	192.168.1.1-192.168.1.254	192.168.1.1	8 hour(s)	8.8.8.8	Edit Delete

Show No.: 10 Total Count: 1

- Configure the network segments excluded from assignment.

Click **Excluded Address Range**, set **Excluded IP Range1**, and click **Save**. You can configure multiple such network segments.



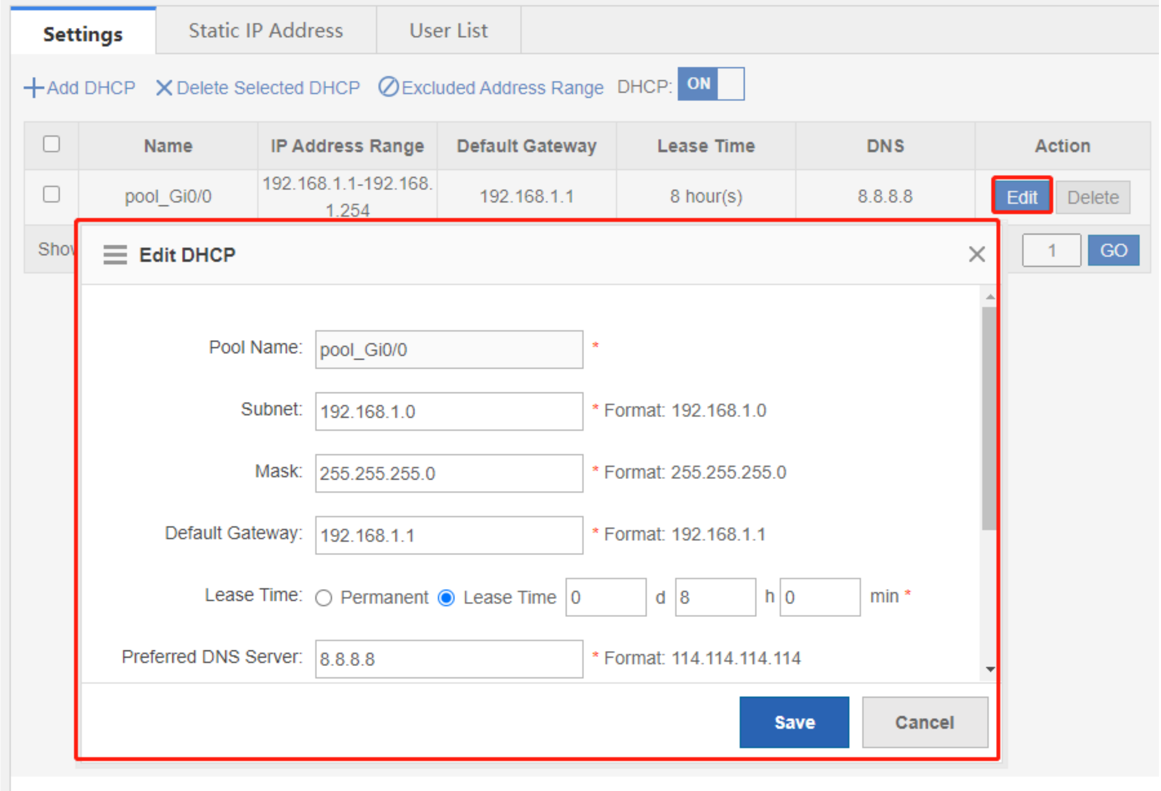
Excluded IP Range

Excluded Address Range: Excluded addresses will not be allocated to the client. The excluded address range is formatted as 1.1.1.1-1.1.1.30. Entering only 1.1.1.1 indicates one single excluded address.

Excluded IP Range1: -

- Modify a DHCP configuration entry.

Click **Edit** corresponding to a DHCP configuration entry. In the window that is displayed, modify related information.



□	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
□	pool_Gi0/0	192.168.1.1-192.168.1.254	192.168.1.1	8 hour(s)	8.8.8.8	Edit Delete

Edit DHCP

Pool Name: pool_Gi0/0 *

Subnet: 192.168.1.0 * Format: 192.168.1.0

Mask: 255.255.255.0 * Format: 255.255.255.0

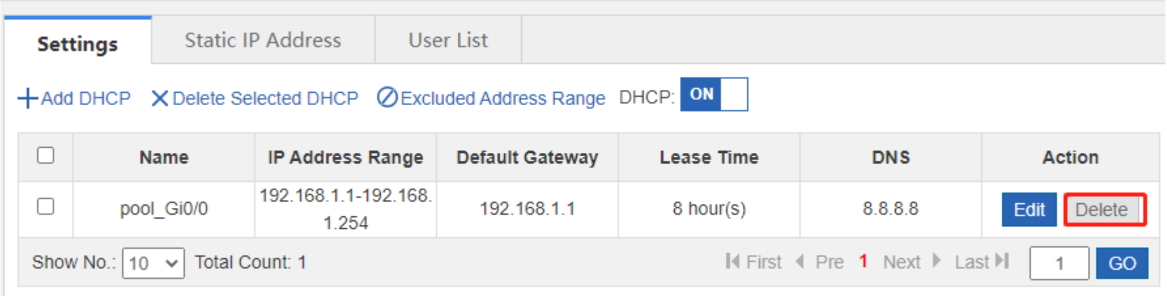
Default Gateway: 192.168.1.1 * Format: 192.168.1.1

Lease Time: ○ Permanent ● Lease Time 0 d 8 h 0 min *

Preferred DNS Server: 8.8.8.8 * Format: 114.114.114.114

- Delete a DCHP configuration entry.

Click **Delete** corresponding to a DHCP configuration entry. In the confirmation window that is displayed, click **OK** for deletion.

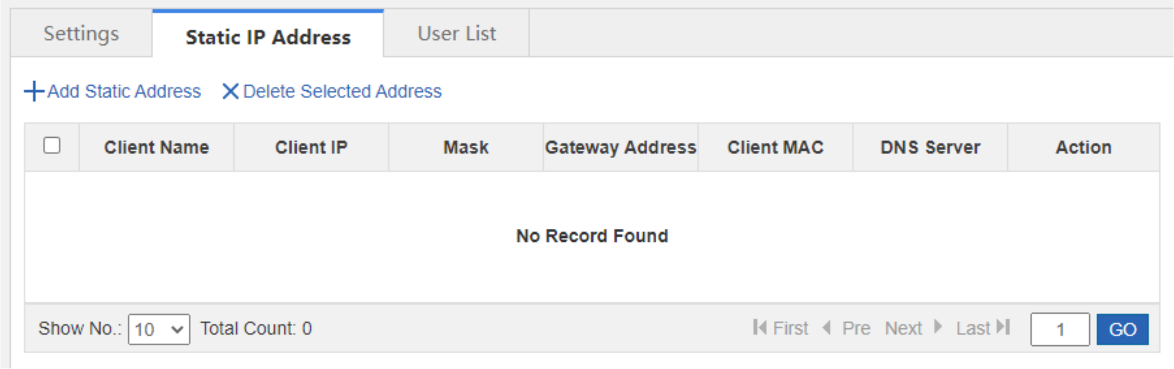


□	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
□	pool_Gi0/0	192.168.1.1-192.168.1.254	192.168.1.1	8 hour(s)	8.8.8.8	Edit Delete

Show No.: 10 Total Count: 1

7.7.3 Static Address

Choose **Network** > **DHCP** > **Static IP Address**.

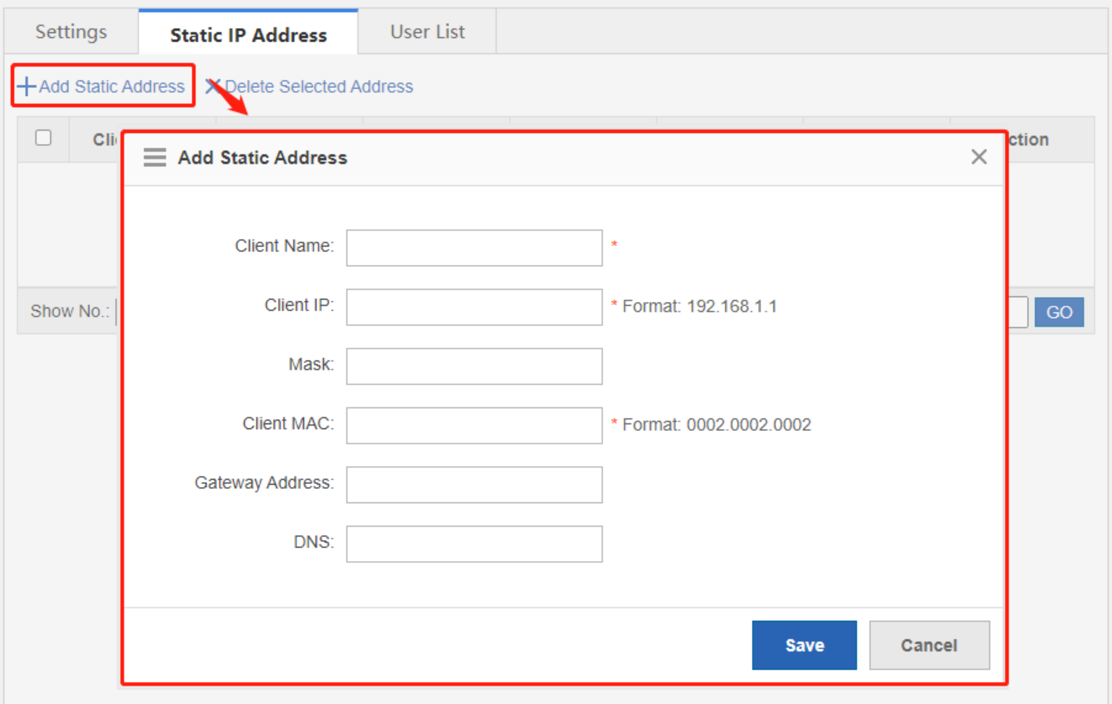


□	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
			No Record Found				

Show No.: 10 Total Count: 0

- Add a static address entry.

Click **Add Static Address** in the upper left corner. In the window that is displayed, add static address bonding to assign a fixed IP address to the specified host.



Add Static Address

Client Name: *

Client IP: * Format: 192.168.1.1

Mask:

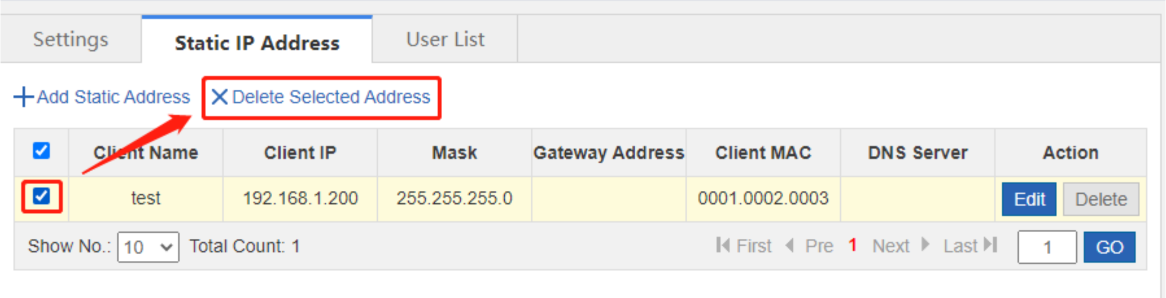
Client MAC: * Format: 0002.0002.0002

Gateway Address:

DNS:

- Delete static address entries in batches.

Select the static addresses to be deleted and click **Delete Selected Address**.

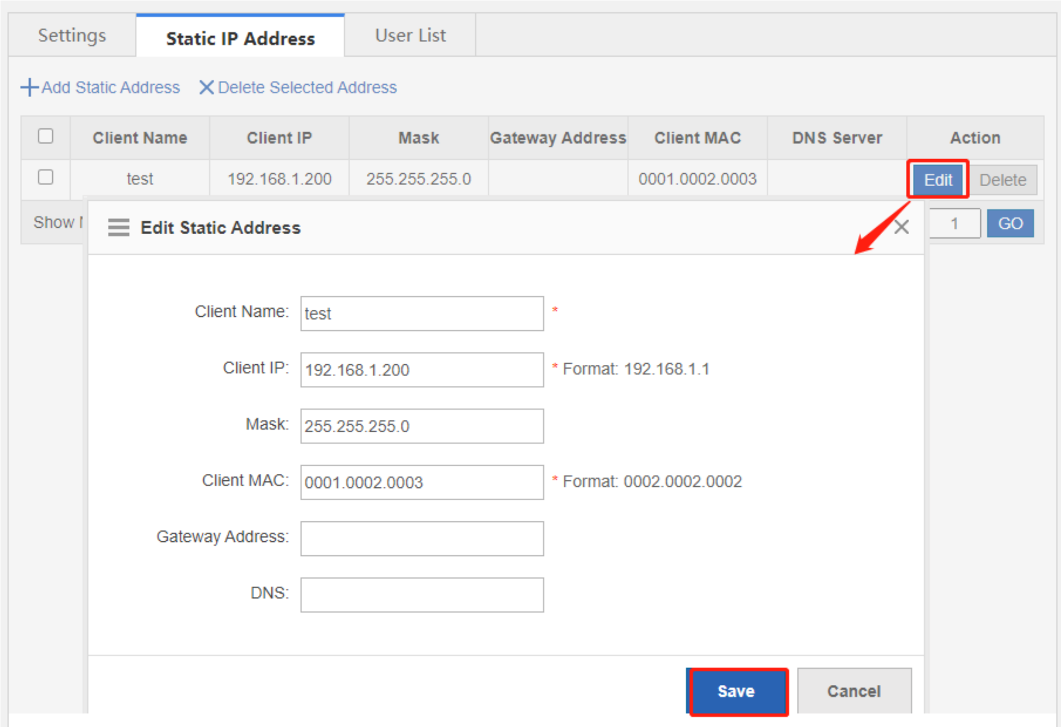


☑	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
☑	test	192.168.1.200	255.255.255.0		0001.0002.0003		Edit Delete

Show No.: 10 Total Count: 1

- Modify a static address entry.

Click **Edit** corresponding to a static IP address entry. In the window that is displayed, modify related information.



□	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
□	test	192.168.1.200	255.255.255.0		0001.0002.0003		Edit Delete

Client Name: test *

Client IP: 192.168.1.200 * Format: 192.168.1.1

Mask: 255.255.255.0

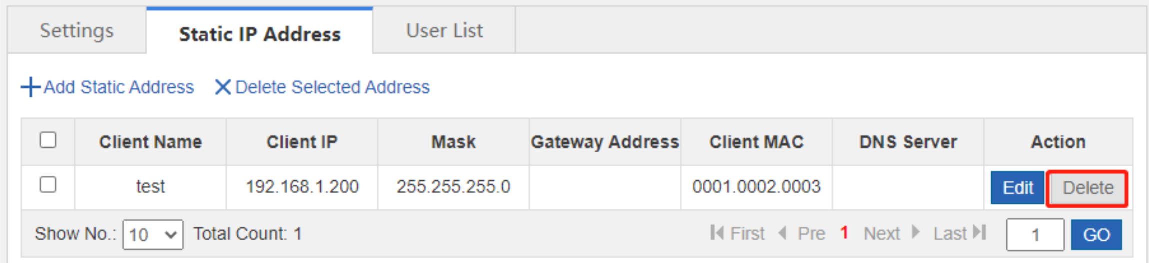
Client MAC: 0001.0002.0003 * Format: 0002.0002.0002

Gateway Address:

DNS:

- Delete a static address entry.

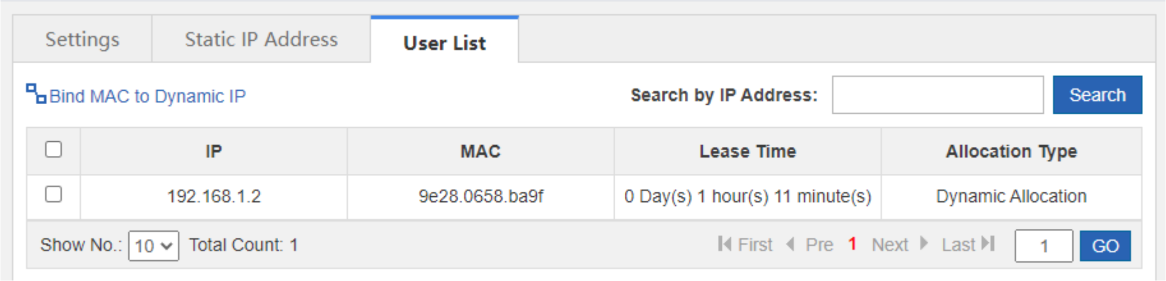
Click **Delete** corresponding to a static IP address entry. In the confirmation window that is displayed, click **OK** for deletion.



□	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
□	test	192.168.1.200	255.255.255.0		0001.0002.0003		Edit Delete

Show No.: 10 Total Count: 1

7.7.4 User List



Search by IP Address:

□	IP	MAC	Lease Time	Allocation Type
□	192.168.1.2	9e28.0658.ba9f	0 Day(s) 1 hour(s) 11 minute(s)	Dynamic Allocation

Show No.: 10 Total Count: 1

- **Bind MAC to Dynamic IP**

In the list, select the entry for bonding, and click **Bind MAC to Dynamic IP**.

- **Search by IP Address**

Enter the IP address to be queried in the text box. Click **Search**. The search result that matches the criterion is displayed in the list.

1.2 Line Escape

7.7.5 Introduction

This function is used to detect whether the line is normal periodically. When an exception occurs, the line is disabled in a timely manner so that the application traffic can go out from normal lines.

7.7.6 Line Traffic Escape

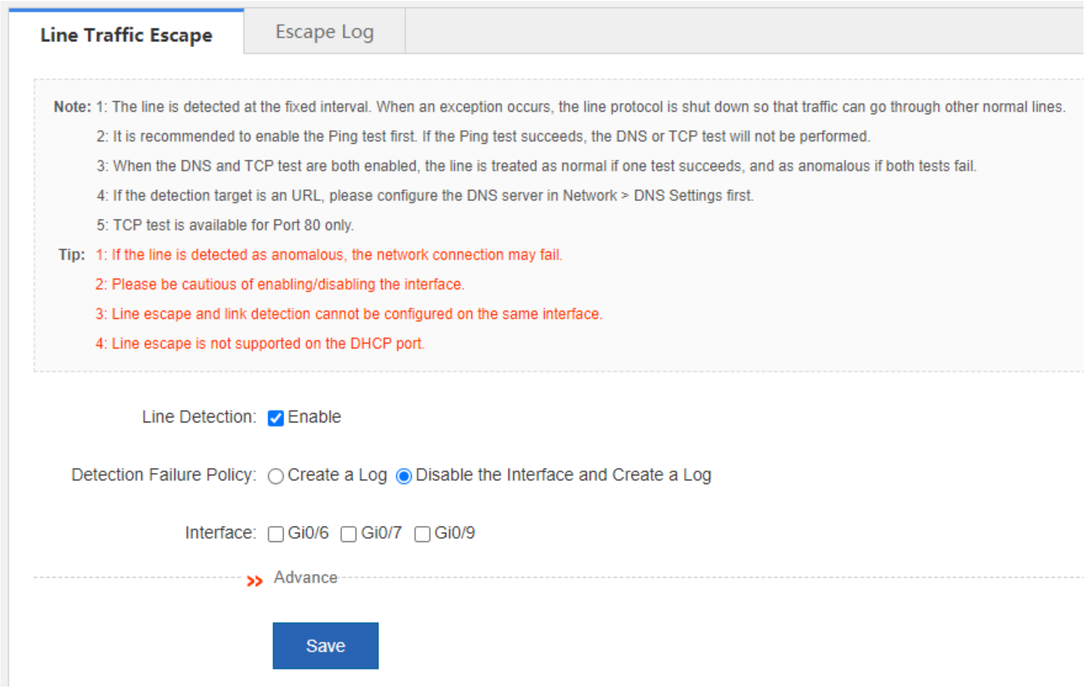
Precautions

- The configuration is at high risk. Whether the line is normal is checked. In case of a line exception, the network connection may fail.
- Interface enabling and disabling is at high risk. Exercise with caution.

Procedure

(1) Choose **Network** > **Line Escape** > **Line Traffic Escape**.

(2) Set **Line Detection** to **Enable** to enable one-click line traffic escape.



Note: 1: The line is detected at the fixed interval. When an exception occurs, the line protocol is shut down so that traffic can go through other normal lines.
2: It is recommended to enable the Ping test first. If the Ping test succeeds, the DNS or TCP test will not be performed.
3: When the DNS and TCP test are both enabled, the line is treated as normal if one test succeeds, and as anomalous if both tests fail.
4: If the detection target is an URL, please configure the DNS server in Network > DNS Settings first.
5: TCP test is available for Port 80 only.

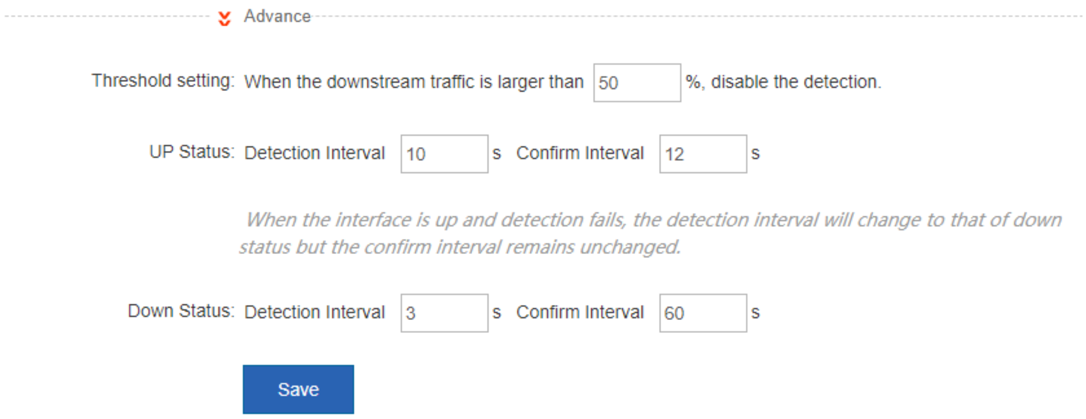
Tip: 1: If the line is detected as anomalous, the network connection may fail.
2: Please be cautious of enabling/disabling the interface.
3: Line escape and link detection cannot be configured on the same interface.
4: Line escape is not supported on the DHCP port.

Line Detection: ☑ Enable

Detection Failure Policy: ○ Create a Log ● Disable the Interface and Create a Log

Interface: □ Gi0/6 □ Gi0/7 □ Gi0/9

(3) Expand **Advance** and set the advanced configuration items.



Threshold setting: When the downstream traffic is larger than 50 %, disable the detection.

UP Status: Detection Interval 10 s Confirm Interval 12 s

When the interface is up and detection fails, the detection interval will change to that of down status but the confirm interval remains unchanged.

Down Status: Detection Interval 3 s Confirm Interval 60 s

(4) Click **Save**.

7.7.7 Escape Log

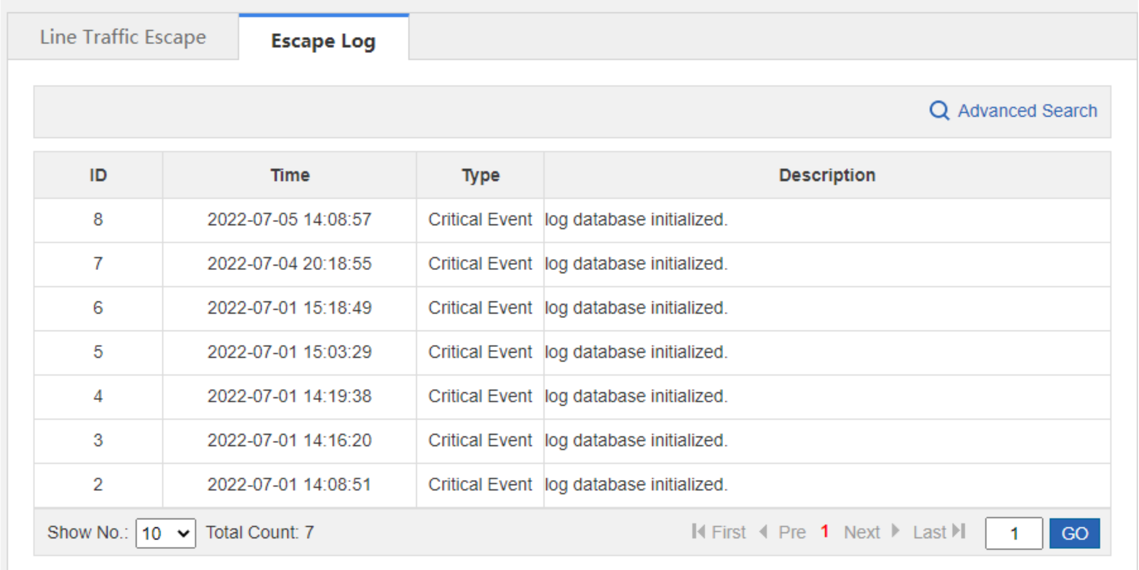
Application Scenario

This operation allows you to view the recent escape logs.

Procedure

(1) Choose **Network** > **Line Escape** > **Escape Log**.

(2) View escape log details, including the ID, time, type, and specific information.



ID	Time	Type	Description
8	2022-07-05 14:08:57	Critical Event	log database initialized.
7	2022-07-04 20:18:55	Critical Event	log database initialized.
6	2022-07-01 15:18:49	Critical Event	log database initialized.
5	2022-07-01 15:03:29	Critical Event	log database initialized.
4	2022-07-01 14:19:38	Critical Event	log database initialized.
3	2022-07-01 14:16:20	Critical Event	log database initialized.
2	2022-07-01 14:08:51	Critical Event	log database initialized.

Show No.: 10 Total Count: 7

8 Firewall

The firewall feature can detect multiple types of network-layer attacks and take measures based on the configured policy to protect the internal network from malicious attacks, thereby ensuring the normal operation of the internal network.

Note

- The NBR6205-E, NBR6210-E and NBR6215-E enterprise-class routers support the firewall feature.
- The NBR6120-E enterprise-class router does not support the firewall feature.

8.1 Attack Defense Configuration

The router is usually deployed on the intranet egress. Both normal service traffic and malicious attack traffic pass through the router. You can enable the attack defense function and configure corresponding policies to detect and block the attack traffic passing through the router, ensuring the safety of the internal network.

Attack defense configuration supports the protocol policy, zone policy, and global defense policy, which are prioritized in a decreasing order.

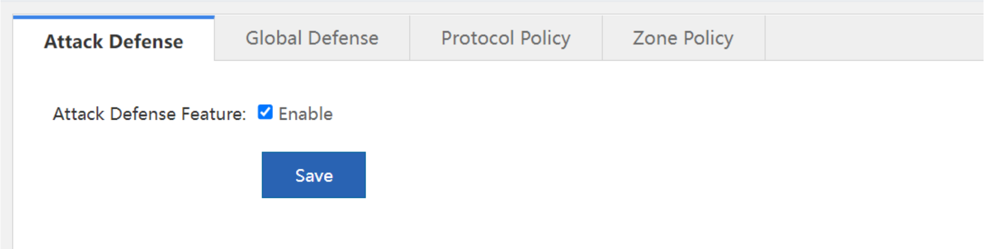
8.1.1 Attack Defense Feature

The attack defense feature is used to display the menu and configure the attack defense. Only when you enable the feature can you view and configure the attack defense feature. If the attack defense is enabled, the device and the internal network will be defended according to the predefined policies. You can add new defense policies as required.

Procedure

(1) Choose **Firewall** > **Attack Defense Config** > **Attack Defense**.

(2) Select **Enable** to enable the attack defense feature and click **Save**.



Attack Defense Feature: ☑ Enable

8.1.2 Global Defense

Global defense is designed to defend the router. The global defense limits the establishment speed of sessions to ensure efficient utilization of router resources. You can enable global defense to prevent resource exhaustion attacks or DoS attacks.

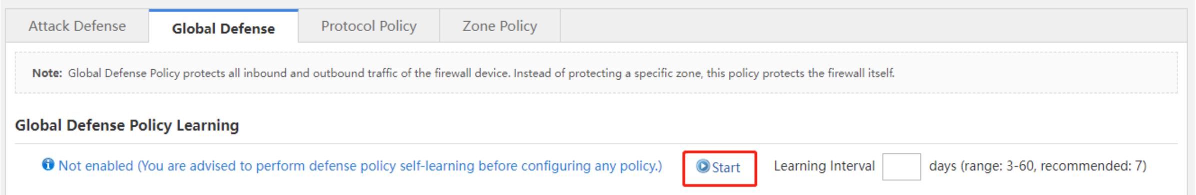
Procedure

(1) Choose **Firewall** > **Attack Defense Config** > **Global Defense**.

(2) Click **Start** and the device will obtain an optimal protection threshold that fits the current network through automatic learning.

Caution

- To guarantee better effects of the learned policy, please ensure that the automatic learning period includes the traffic peak period.
- The default learning period is seven days. You can suspend the learning period or set a new period as required.
- You are advised to make the device relearn and apply new learning results after the network is changed.

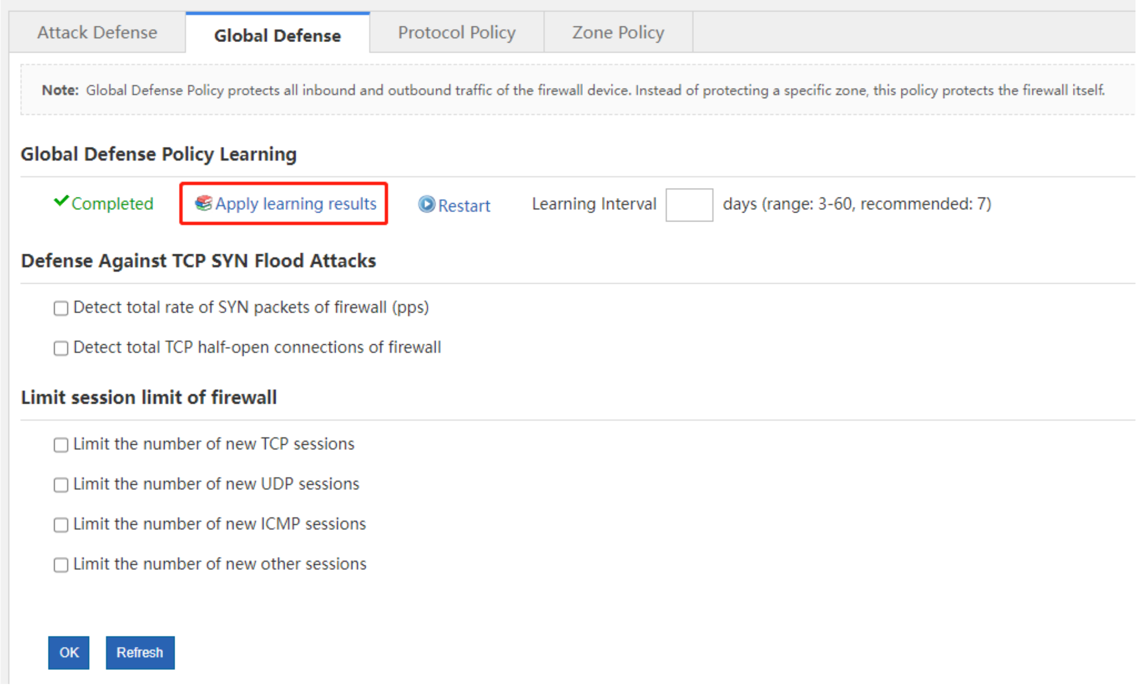


Note: Global Defense Policy protects all inbound and outbound traffic of the firewall device. Instead of protecting a specific zone, this policy protects the firewall itself.

Global Defense Policy Learning

Not enabled (You are advised to perform defense policy self-learning before configuring any policy.) Start Learning Interval [ ] days (range: 3-60, recommended: 7)

(3) After global defense policy learning is completed, click **Apply learning results**. Adjust the threshold based on the network conditions and learning results.



Note: Global Defense Policy protects all inbound and outbound traffic of the firewall device. Instead of protecting a specific zone, this policy protects the firewall itself.

Global Defense Policy Learning

✓ Completed Apply learning results Restart Learning Interval [ ] days (range: 3-60, recommended: 7)

Defense Against TCP SYN Flood Attacks

□ Detect total rate of SYN packets of firewall (pps)

□ Detect total TCP half-open connections of firewall

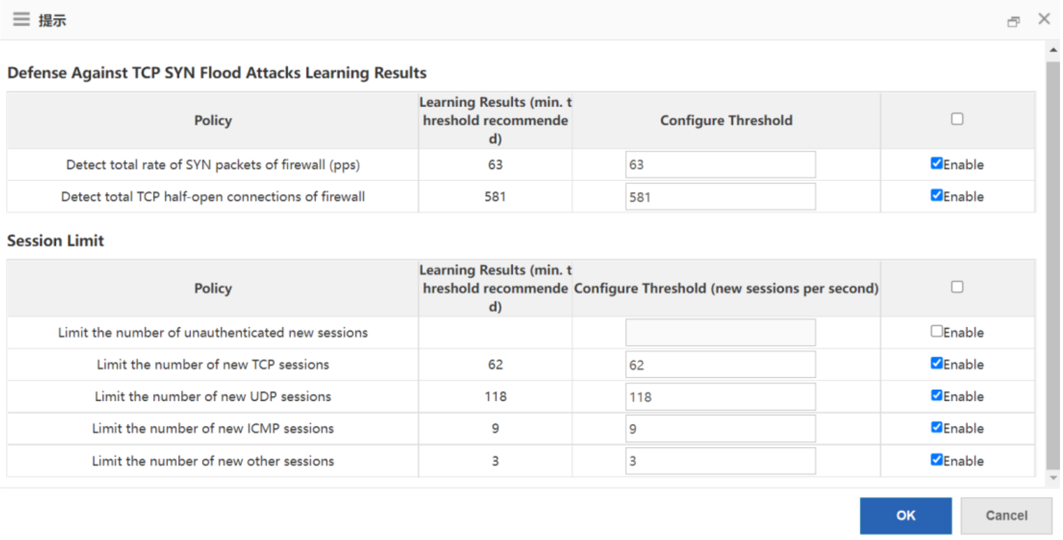
Limit session limit of firewall

□ Limit the number of new TCP sessions

□ Limit the number of new UDP sessions

□ Limit the number of new ICMP sessions

□ Limit the number of new other sessions



提示

Defense Against TCP SYN Flood Attacks Learning Results

Policy	Learning Results (min. threshold recommended)	Configure Threshold	□
Detect total rate of SYN packets of firewall (pps)	63	63	☑Enable
Detect total TCP half-open connections of firewall	581	581	☑Enable

Session Limit

Policy	Learning Results (min. threshold recommended)	Configure Threshold (new sessions per second)	□
Limit the number of unauthenticated new sessions			□Enable
Limit the number of new TCP sessions	62	62	☑Enable
Limit the number of new UDP sessions	118	118	☑Enable
Limit the number of new ICMP sessions	9	9	☑Enable
Limit the number of new other sessions	3	3	☑Enable

OK Cancel

(4) Click **OK** after the configuration is completed.

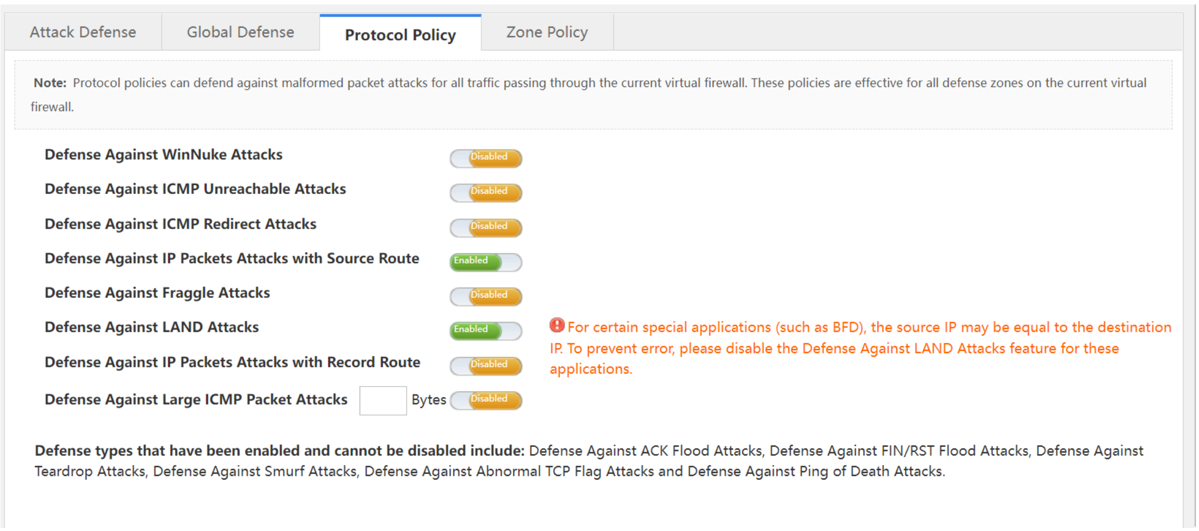
8.1.3 Protocol Policy

Protocol policies can defend against attacks for vulnerabilities of the protocol operating mechanism. The device will filter protocol packets with attack characteristics if the corresponding protocol is enabled.

Procedure

(1) **Choose Firewall** > **Attack Defense Config** > **Protocol Policy**.

(2) Click to enable the defense policy as required to make the specified policy take effect.



Attack Defense | Global Defense | **Protocol Policy** | Zone Policy

Note: Protocol policies can defend against malformed packet attacks for all traffic passing through the current virtual firewall. These policies are effective for all defense zones on the current virtual firewall.

Defense Against WinNuke Attacks	Disabled
Defense Against ICMP Unreachable Attacks	Disabled
Defense Against ICMP Redirect Attacks	Disabled
Defense Against IP Packets Attacks with Source Route	Enabled
Defense Against Fraggle Attacks	Disabled
Defense Against LAND Attacks	Enabled
Defense Against IP Packets Attacks with Record Route	Disabled
Defense Against Large ICMP Packet Attacks ____ Bytes	Disabled

For certain special applications (such as BFD), the source IP may be equal to the destination IP. To prevent error, please disable the Defense Against LAND Attacks feature for these applications.

Defense types that have been enabled and cannot be disabled include: Defense Against ACK Flood Attacks, Defense Against FIN/RST Flood Attacks, Defense Against Teardrop Attacks, Defense Against Smurf Attacks, Defense Against Abnormal TCP Flag Attacks and Defense Against Ping of Death Attacks.

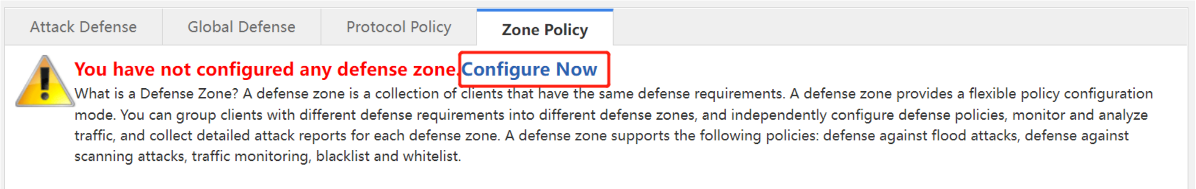
8.1.4 Zone Policy

A defense zone is a collection of clients that have the same defense requirements. You can group clients with different defense requirements into corresponding defense zones to defend the clients based on groups and manage them separately. You can configure defense policies for specified zones respectively to defend the client precisely.

Procedure

(1) Choose **Firewall** > **Attack Defense Config** > **Zone Policy**.

(2) Click **Configure Now** to enter the **Config Wizard for Creating a New Defense Zone** page.



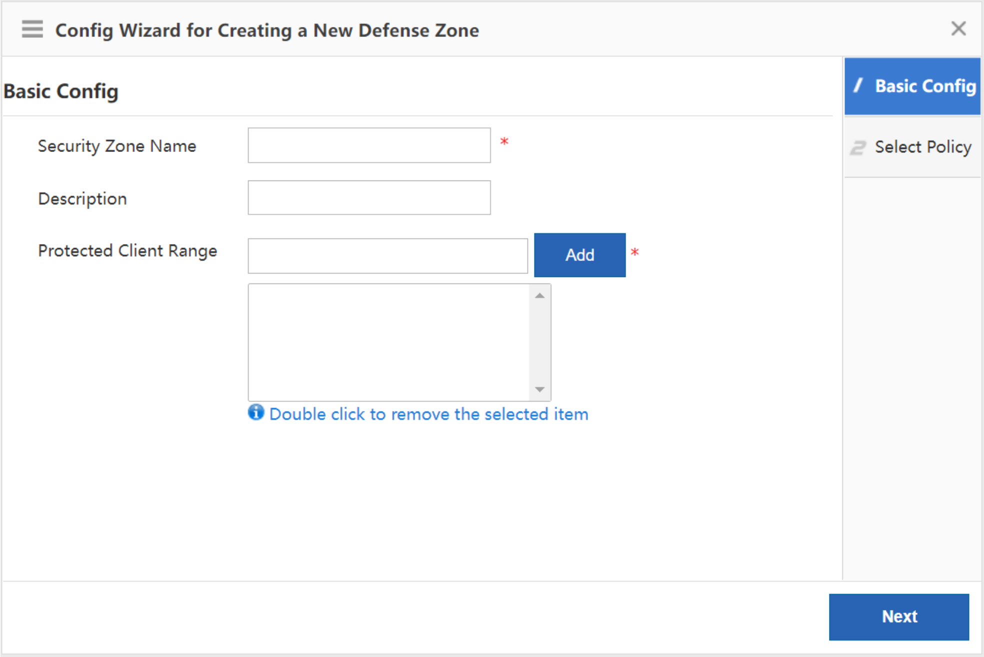
You have not configured any defense zone.Configure Now

What is a Defense Zone? A defense zone is a collection of clients that have the same defense requirements. A defense zone provides a flexible policy configuration mode. You can group clients with different defense requirements into different defense zones, and independently configure defense policies, monitor and analyze traffic, and collect detailed attack reports for each defense zone. A defense zone supports the following policies: defense against flood attacks, defense against scanning attacks, traffic monitoring, blacklist and whitelist.

(3) Enter the security zone name, description and the protected client range, and click **Next**.

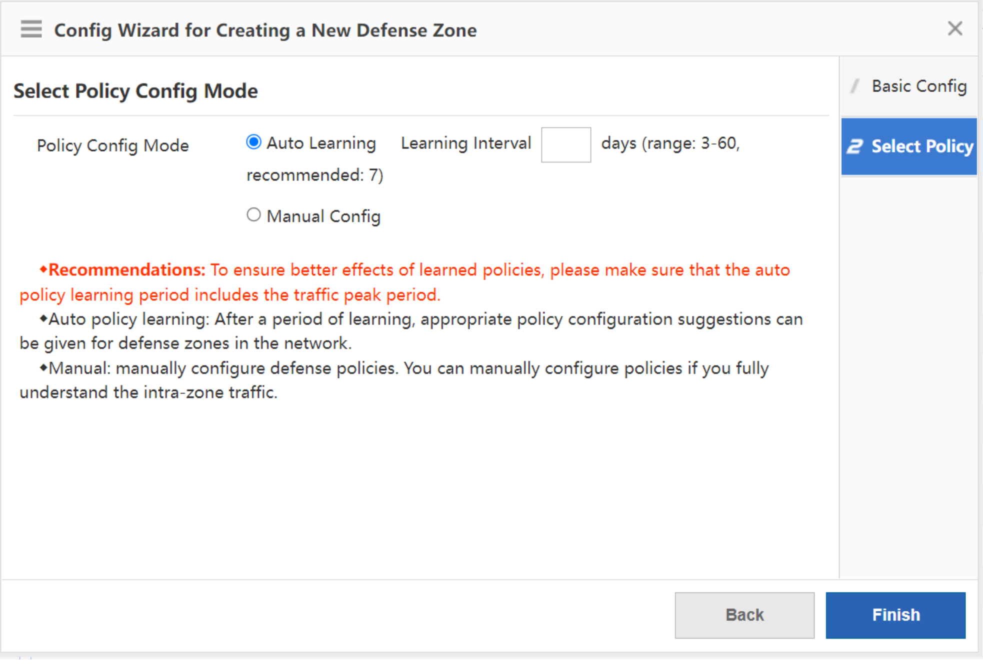
Note

The protected client range supports a single IP address (example: 1.1.1.1), subnet bit length (example: 1.1.1.0/24), or subnet mask (example: 1.1.1.0/255.255.255.0). Enter the protected client range and click **Add** to enter another range.



Double click to remove the selected item

(4) Select policy configuration mode as required and click **Finish**.



Config Wizard for Creating a New Defense Zone ✕

Basic Config

Select Policy

Select Policy Config Mode

Policy Config Mode ● Auto Learning Learning Interval ☐ days (range: 3-60, recommended: 7)

○ Manual Config

⬩**Recommendations:** To ensure better effects of learned policies, please make sure that the auto policy learning period includes the traffic peak period.

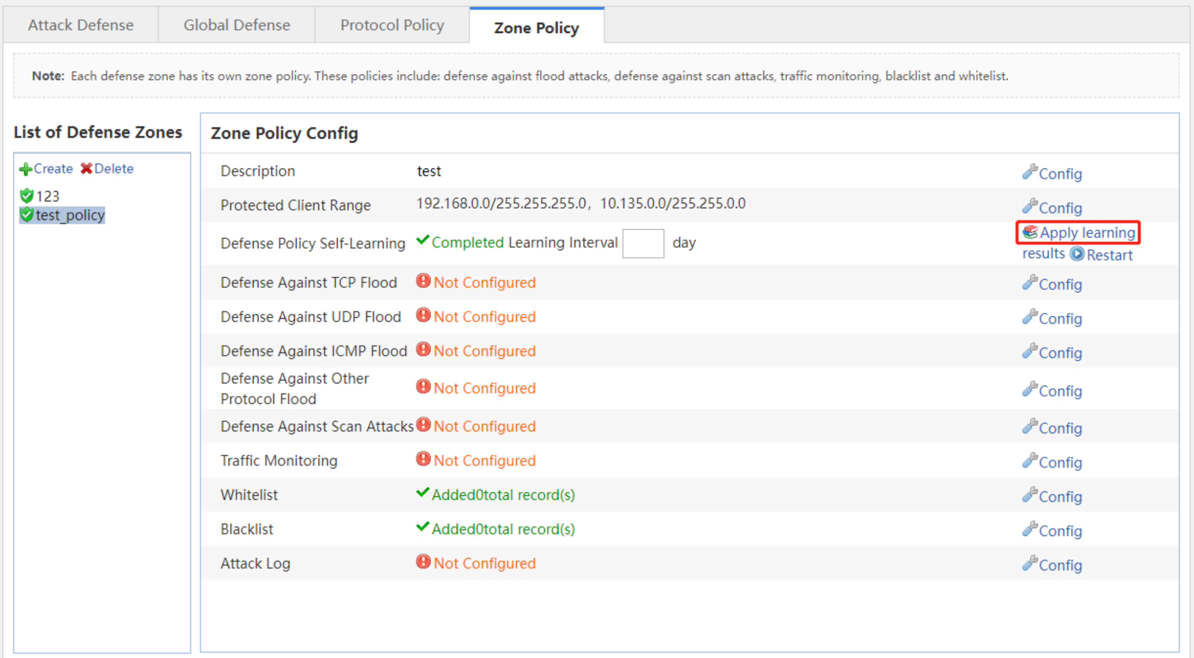
⬩Auto policy learning: After a period of learning, appropriate policy configuration suggestions can be given for defense zones in the network.

⬩Manual: manually configure defense policies. You can manually configure policies if you fully understand the intra-zone traffic.

Back Finish

(5) If you select **Auto Learning** for the policy configuration mode, follow the procedure to configure the policy. If you select **Manual Config**, you can skip the procedure.

a Click Apply learning results after leaning to enter the Apply learning results page.



Attack Defense | Global Defense | Protocol Policy | **Zone Policy**

Note: Each defense zone has its own zone policy. These policies include: defense against flood attacks, defense against scan attacks, traffic monitoring, blacklist and whitelist.

List of Defense Zones

Create Delete

123

test_policy

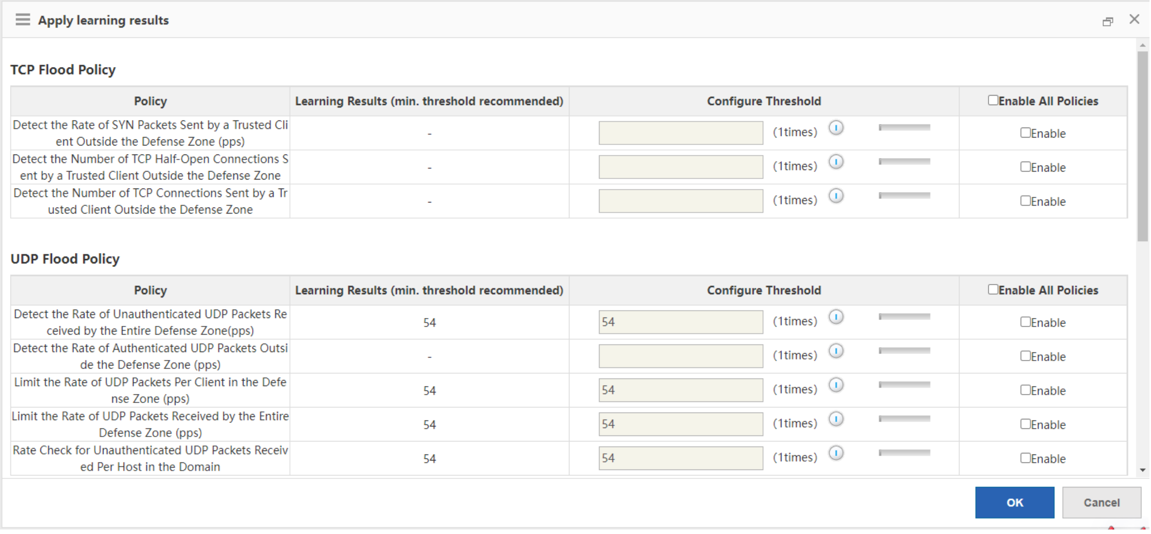
Zone Policy Config

Description	test	Config
Protected Client Range	192.168.0.0/255.255.255.0， 10.135.0.0/255.255.0.0	Config
Defense Policy Self-Learning	✓Completed Learning Interval ☐ day	Apply learning results Restart
Defense Against TCP Flood	Not Configured	Config
Defense Against UDP Flood	Not Configured	Config
Defense Against ICMP Flood	Not Configured	Config
Defense Against Other Protocol Flood	Not Configured	Config
Defense Against Scan Attacks	Not Configured	Config
Traffic Monitoring	Not Configured	Config
Whitelist	✓Added0total record(s)	Config
Blacklist	✓Added0total record(s)	Config
Attack Log	Not Configured	Config

b Configure the threshold based on the learning results and the actual conditions of the defense zone.

Note

As the traffic monitoring function consumes some of device performance. You are advised to disable the traffic monitoring function after the defense zone policy works smoothly to ensure that the device can achieve the maximum service processing capacity.



Apply learning results

TCP Flood Policy

Policy	Learning Results (min. threshold recommended)	Configure Threshold	☐Enable All Policies
Detect the Rate of SYN Packets Sent by a Trusted Client Outside the Defense Zone (pps)	-	(1times)	☐Enable
Detect the Number of TCP Half-Open Connections Sent by a Trusted Client Outside the Defense Zone	-	(1times)	☐Enable
Detect the Number of TCP Connections Sent by a Trusted Client Outside the Defense Zone	-	(1times)	☐Enable

UDP Flood Policy

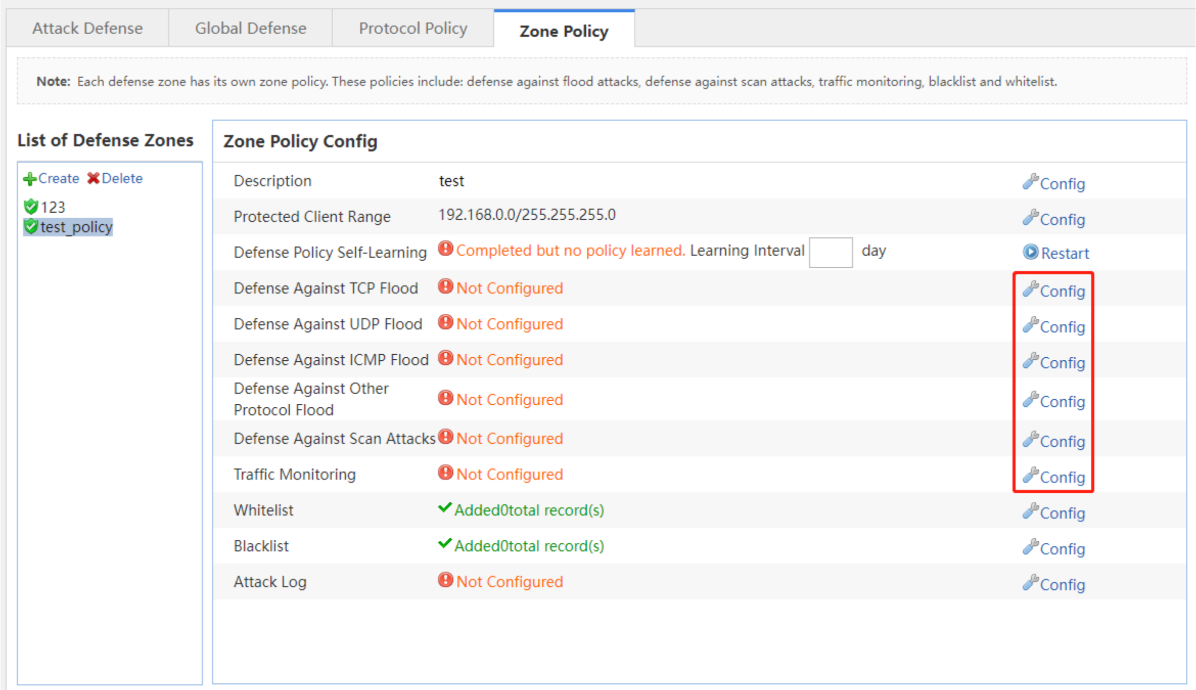
Policy	Learning Results (min. threshold recommended)	Configure Threshold	☐Enable All Policies
Detect the Rate of Unauthenticated UDP Packets Received by the Entire Defense Zone(pps)	54	54 (1times)	☐Enable
Detect the Rate of Authenticated UDP Packets Outside the Defense Zone (pps)	-	(1times)	☐Enable
Limit the Rate of UDP Packets Per Client in the Defense Zone (pps)	54	54 (1times)	☐Enable
Limit the Rate of UDP Packets Received by the Entire Defense Zone (pps)	54	54 (1times)	☐Enable
Rate Check for Unauthenticated UDP Packets Received Per Host in the Domain	54	54 (1times)	☐Enable

c Click **OK** after the configuration is completed.

(6) If you select **Manual Config** for the policy configuration mode, follow the procedure to configure the policy. If you select **Auto Learning**, you can skip the procedure.

Note

As the traffic monitoring function consumes some of device performance. You are advised to disable the traffic monitoring function after the defense zone policy works smoothly to ensure that the device can achieve the maximum service processing capacity.



Note: Each defense zone has its own zone policy. These policies include: defense against flood attacks, defense against scan attacks, traffic monitoring, blacklist and whitelist.

List of Defense Zones

Zone Policy Config

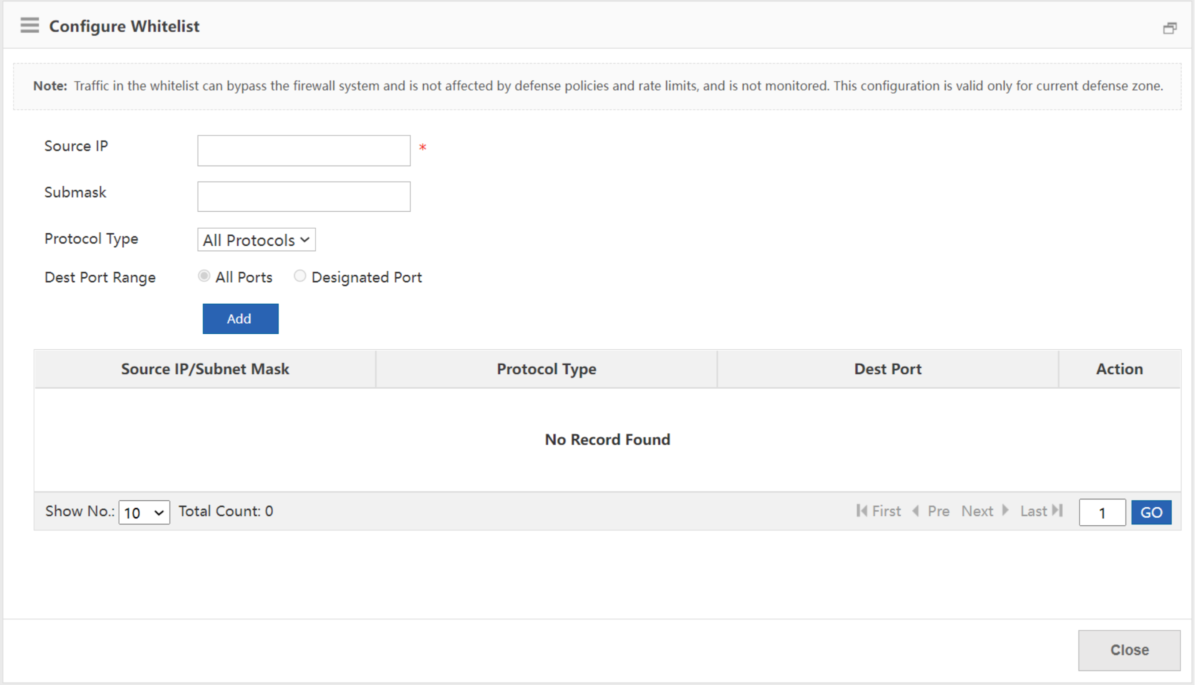
Description	test	Config
Protected Client Range	192.168.0.0/255.255.255.0	Config
Defense Policy Self-Learning	Completed but no policy learned. Learning Interval day	Restart
Defense Against TCP Flood	Not Configured	Config
Defense Against UDP Flood	Not Configured	Config
Defense Against ICMP Flood	Not Configured	Config
Defense Against Other Protocol Flood	Not Configured	Config
Defense Against Scan Attacks	Not Configured	Config
Traffic Monitoring	Not Configured	Config
Whitelist	✓Added0total record(s)	Config
Blacklist	✓Added0total record(s)	Config
Attack Log	Not Configured	Config

(7) (Optional) For a trusted source IP address, you can add it to the whitelist to bypass the detection of the device and the traffic of this source IP will not be affected. Click **Config** of the whitelist to access the **Configure**

Whitelist page, enter the source IP address, the subnet mask, select the protocol type and the designation port range, and click **Add**.

Note

- The whitelist is valid only for this defense zone.
- The whitelist overrides the blacklist. If an IP address is added to a whitelist and a blacklist simultaneously, the whitelist is valid.



Configure Whitelist

Note: Traffic in the whitelist can bypass the firewall system and is not affected by defense policies and rate limits, and is not monitored. This configuration is valid only for current defense zone.

Source IP *

Submask

Protocol Type: All Protocols

Dest Port Range: ● All Ports ○ Designated Port

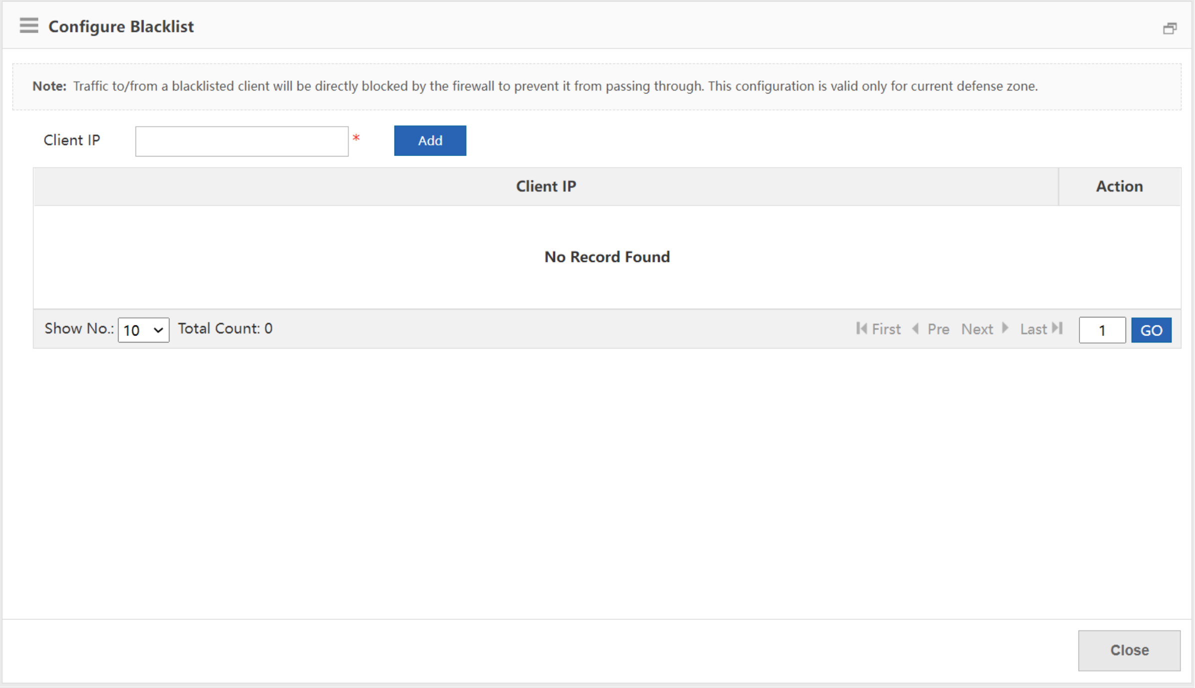
Source IP/Subnet Mask	Protocol Type	Dest Port	Action
No Record Found			

Show No.: 10 Total Count: 0

(8) (Optional) For an untrusted source IP address, you can add it to the blacklist. The traffic to or from the blacklisted client will be blocked by the device. Click **Config** of the blacklist to access the **Configure Blacklist** page, enter the client IP address, and click **Add**.

Note

- The blacklist is valid only for this defense zone.
- The whitelist overrides the blacklist. If an IP address is added to a whitelist and a blacklist simultaneously, the whitelist is valid.



Configure Blacklist

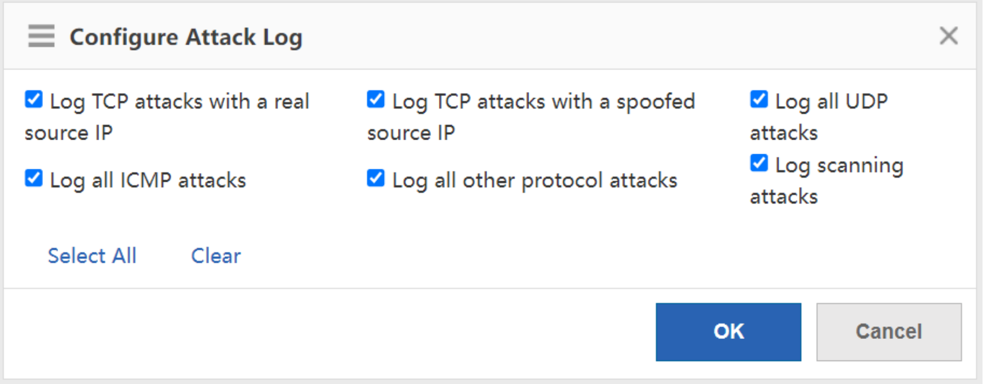
Note: Traffic to/from a blacklisted client will be directly blocked by the firewall to prevent it from passing through. This configuration is valid only for current defense zone.

Client IP * Add

Client IP	Action
No Record Found	

Show No.: 10 Total Count: 0

(9) (Optional) Click **Config** of the attack log to enable logging and printing of the specified type of policy. Select the log types as required, and click **OK**.



Configure Attack Log

☑ Log TCP attacks with a real source IP

☑ Log TCP attacks with a spoofed source IP

☑ Log all UDP attacks

☑ Log all ICMP attacks

☑ Log all other protocol attacks

☑ Log scanning attacks

8.2 Security Zone Configuration

A security zone is a logical concept that the objects in a security zone have same security requirements, security access control, and border control policies. You can group multiple interfaces or IP addresses with the same security requirements on the device into the same security zone to implement hierarchical management of policies and precise protection. For example, the subnet A is connected to the interface 1 of the router device which belongs to the security zone 1, and the subnet B is connected to the interface 2 of the router device which belongs to the security zone 2. You can only configure the access policy between the security zone 1 and the security zone 2 to perform the access control on the subnet A and the subnet B.

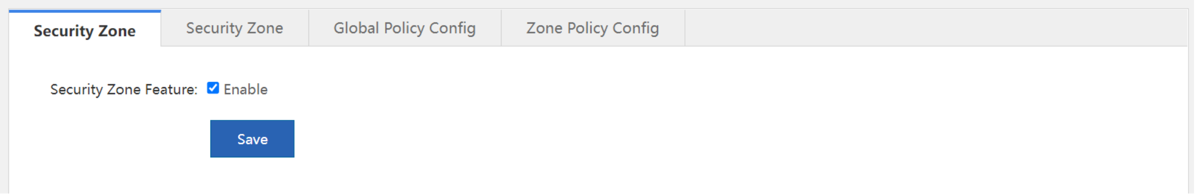
8.2.1 Enabling the Security Zone Feature

The security zone feature is used to display and configure the security zone menu. You can enable this feature to view and configure the security zone and related policies.

Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Security Zone Feature**.

(2) Select the security zone feature and click **Save**.



Security Zone Feature: ☑ Enable

8.2.2 Security Zone

The device supports creating a security zone based on the IP address (IPv4 only) or the device interface. You cannot use the two types of security zones simultaneously. The existing security zone and zone policies will be cleared if you switch the creating mode. An interface-based security zone is created by default.

The default access rules between different security zones are as follows.

- The clients or interfaces in the same security zone cannot access each other.
- The security zone of higher priority can access the security zone of lower priority, but not vice versa.
- The security zones of the same priority cannot access each other.

If the zone policy and the global policy are configured, the device will process the packets based on the access control rule of the zone policy and the global policy. Otherwise, the device will process the packets based on the default access policy.

1. Interface-based Security Zone

After the interfaces are grouped into a security zone, when a packet reaches the device, the device will identify the source interface and the destination interface of the packet, match the interface of the packet with the interface associated with the security zone to determine the source security zone and the destination security zone to which the packet belongs, and then forward or block the packet according to the access policy between security zones or the default access policy.

The default security zone is predefined by the device and cannot be deleted. Interfaces that are not grouped into specified security zones will be assigned to the default security zone.

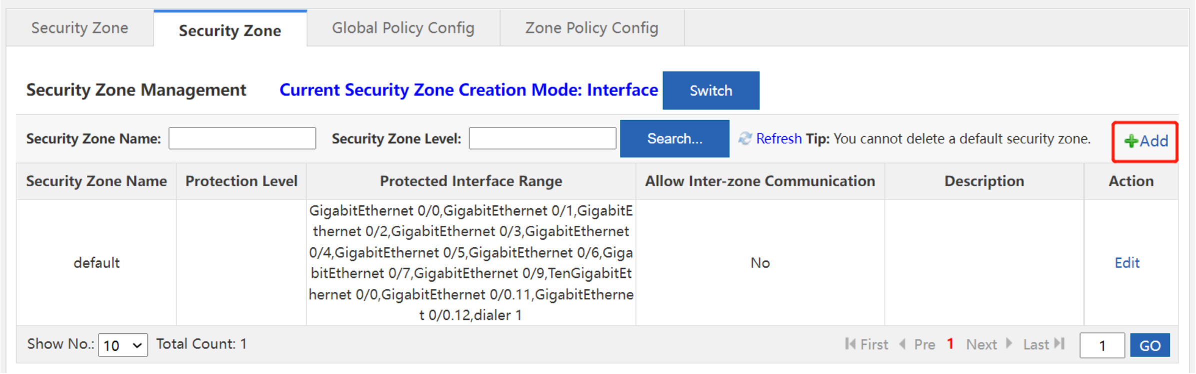
Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Security Zone**.

(2) Click **Add** to access the **Create Interface-based Security Zone** page.

Note

The device will display the page of the interface-based security zone by default. If not, you can click **Switch** to enter the page of the interface-based security zone.



Security Zone Management Current Security Zone Creation Mode: Interface Switch

Security Zone Name: Security Zone Level: Search... Refresh **Tip:** You cannot delete a default security zone. +Add

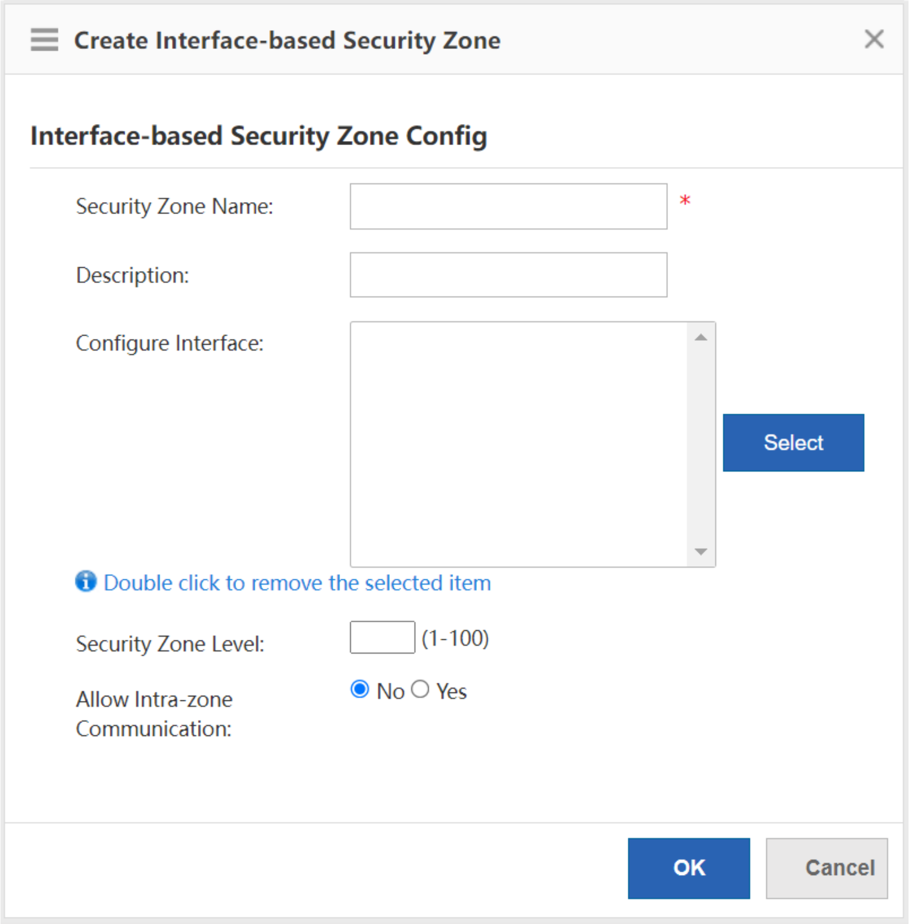
Security Zone Name	Protection Level	Protected Interface Range	Allow Inter-zone Communication	Description	Action
default		GigabitEthernet 0/0,GigabitEthernet 0/1,GigabitEthernet 0/2,GigabitEthernet 0/3,GigabitEthernet 0/4,GigabitEthernet 0/5,GigabitEthernet 0/6,GigabitEthernet 0/7,GigabitEthernet 0/9,TenGigabitEthernet 0/0,GigabitEthernet 0/0.11,GigabitEthernet 0/0.12,dialer 1	No		Edit

Show No.: 10 Total Count: 1

(3) Enter the security zone name and description. Click **Select** to select the interfaces belonging to this security zone. Enter the security zone level, select whether to allow intra-zone communication and click **OK**.

Note

The security zone level is the priority. The higher value indicates higher priority. By default, the security zone with a high priority can access the security zone with a low priority, but not vice versa. The security zones of the same priority cannot access each other.


Create Interface-based Security Zone

Interface-based Security Zone Config

Security Zone Name: *

Description:

Configure Interface:

Double click to remove the selected item

Security Zone Level: (1-100)

Allow Intra-zone Communication: ● No ○ Yes

2. IP-based Security Zone

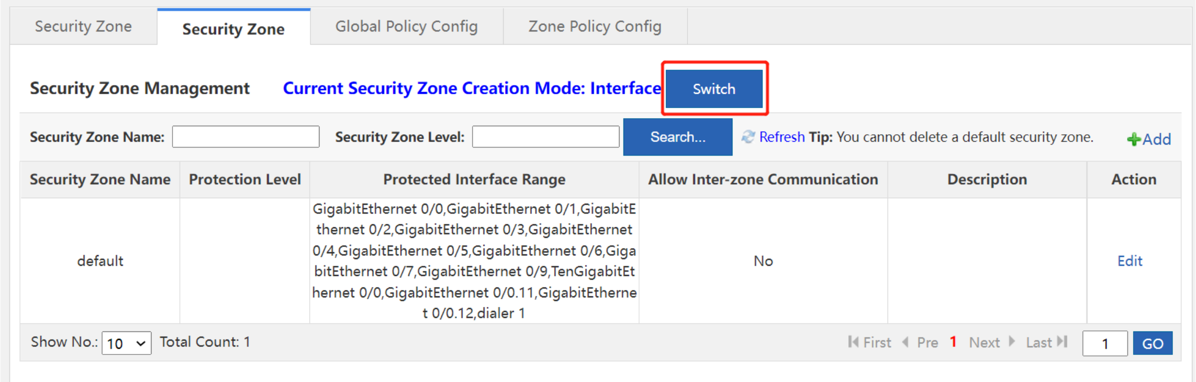
After the IP addresses are grouped into a security zone, when a packet reaches the device, the device will identify the source IP address and the destination IP address of the packet, match the IP address with the ACLs associated with the security zone to determine the source security zone and the designation security zone which the packet belongs to, and then forward or block the packet according to the policy between the security zones or the default access control rule.

The default security zone is predefined by the device and cannot be deleted. IP addresses that are not grouped into specified security zones will be assigned to the default security zone.

Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Security Zone**.

(2) Click **Switch** to access the **Switch Security Zone Creation Mode** page.



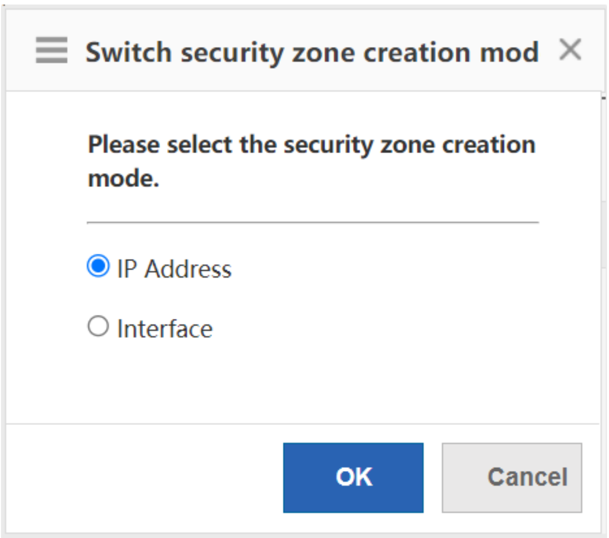
Security Zone Management Current Security Zone Creation Mode: Interface Switch

Security Zone Name: Security Zone Level: Search... Refresh Tip: You cannot delete a default security zone. Add

Security Zone Name	Protection Level	Protected Interface Range	Allow Inter-zone Communication	Description	Action
default		GigabitEthernet 0/0,GigabitEthernet 0/1,GigabitEthernet 0/2,GigabitEthernet 0/3,GigabitEthernet 0/4,GigabitEthernet 0/5,GigabitEthernet 0/6,GigabitEthernet 0/7,GigabitEthernet 0/9,TenGigabitEthernet 0/0,GigabitEthernet 0/0.11,GigabitEthernet 0/0.12,dialer 1	No		Edit

Show No.: 10 Total Count: 1

(3) Select **IP Address** and click **OK**.



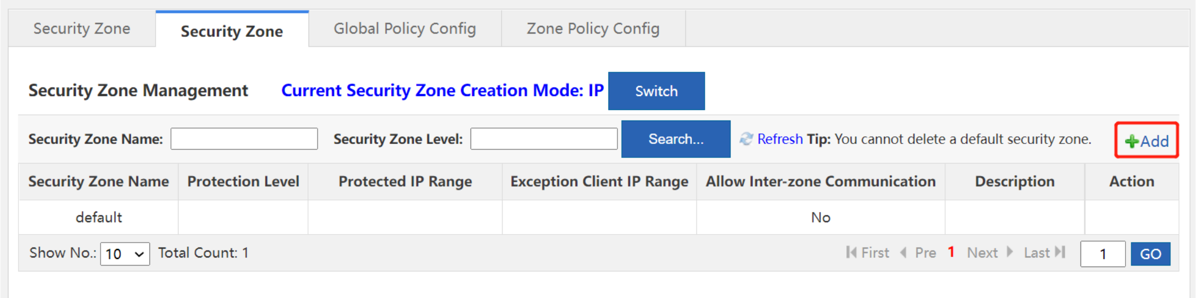
Switch security zone creation mod

Please select the security zone creation mode.

● IP Address

○ Interface

(4) Click **Add** to access the **Create IP-based Security Zone** page.



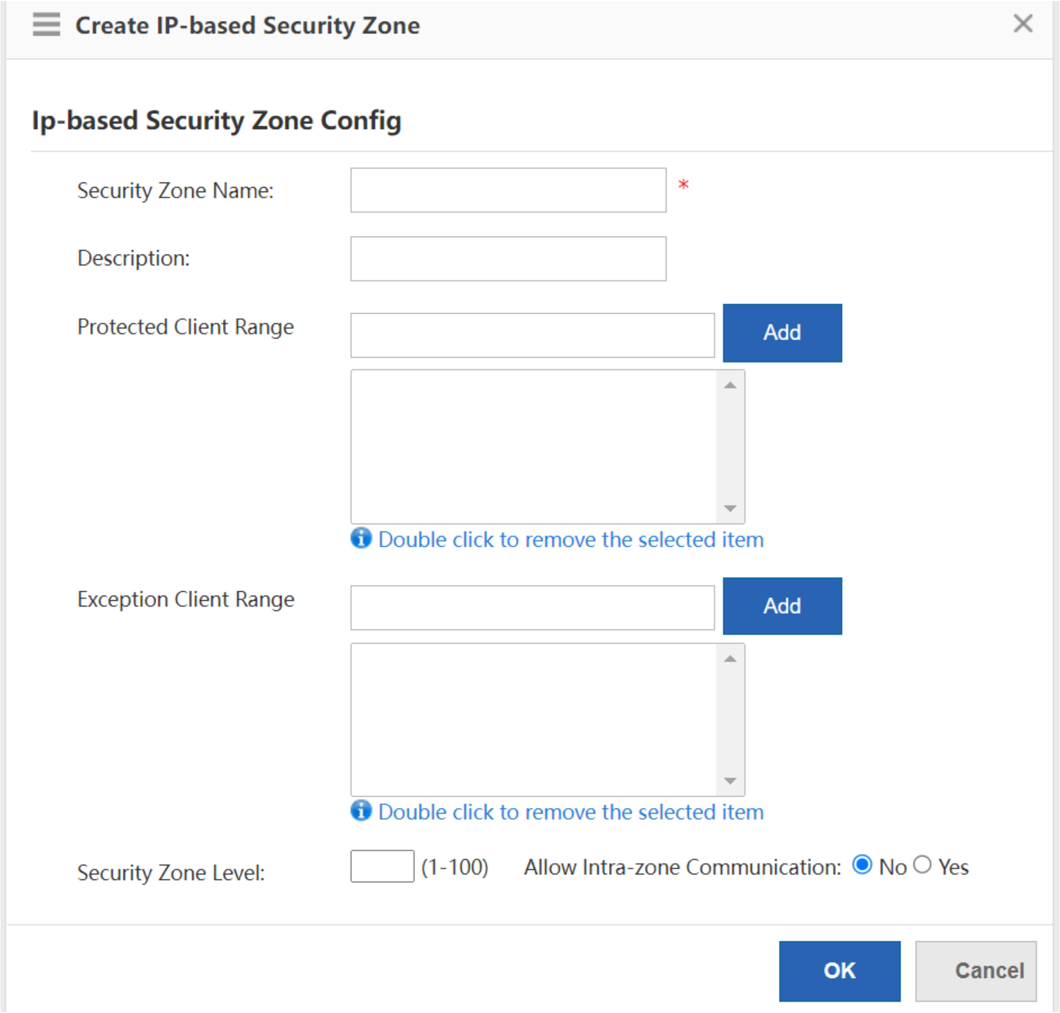
Security Zone Management Current Security Zone Creation Mode: IP Switch

Security Zone Name: Security Zone Level: Search... Refresh **Tip:** You cannot delete a default security zone. Add

Security Zone Name	Protection Level	Protected IP Range	Exception Client IP Range	Allow Inter-zone Communication	Description	Action
default				No		

Show No.: 10 Total Count: 1 First Pre 1 Next Last 1 GO

(5) Enter the parameters of the IP-based security zone and click **OK**.



Create IP-based Security Zone

Ip-based Security Zone Config

Security Zone Name: *

Description:

Protected Client Range Add

Double click to remove the selected item

Exception Client Range Add

Double click to remove the selected item

Security Zone Level: (1-100) Allow Intra-zone Communication: ● No ○ Yes

Parameter	Description
Security Zone Name	The unique identifier of the security zone.
Description	The description of the security zone

Protected Client Range	Indicate the client IP range of the security zone. You can enter a single IP address (example: 1.1.1.1), a subnet or mask length (example: 1.1.1.0/24), a subnet or mask (example: 1.1.1.0/255.255.255.0) or any. Enter a protected client range and click **Add** to enter another range.
Exception Client Range	Indicate the IP address that does not belong to the security zone. For example, add the subnet 1.1.1.0/24 to a security zone, except for the IP address 1.1.1.1 in this subnet. You can add it to the exception client range.
Security Zone Level	The security zone level is the priority. The higher value indicates higher priority. By default, the security zone of higher priority can access the security zone of lower priority, but not vice versa. The security zones of the same priority cannot access each other.
Allow Intra-zone Communication	Select whether the IP addresses in the security zone are allowed for intra-zone communication.

8.2.3 Global Policy Configuration

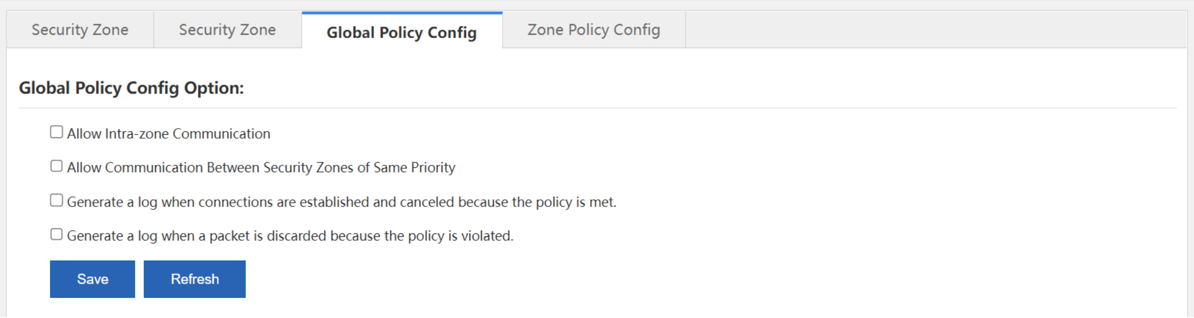
The global access policy is used to control whether to allow the intra-zone communication, whether to allow the communication between security zones of the same priority, whether to generate a log when connections are established and canceled after the security zone policy is matched, and whether to generate a log when the packet is discarded due to the violation of the security zone access policy.

The priority of the global policy is higher than the default access policy.

Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Global Policy Config**.

(2) Select the configuration items as required and click **Save**.



Global Policy Config Option:

☐ Allow Intra-zone Communication

☐ Allow Communication Between Security Zones of Same Priority

☐ Generate a log when connections are established and canceled because the policy is met.

☐ Generate a log when a packet is discarded because the policy is violated.

8.2.4 Zone Policy Configuration

The zone policy function is used to control whether to allow the inter-domain communication.

After the packet reaches the device, the device will identify the source security zone and the destination security zone to which the packet belongs based on the packet characteristics. If the source security zone is not equal to the destination security zone, it is an inter-domain access, and the packet is forwarded according to the zone policy. If the zone policy is not configured, the packet will be processed according to the global policy or the default access policy. If the source security zone is equal to the destination security zone, it is an intra-domain access, and the packet will be processed according to the security zone configuration.

The zone policy varies with the security zone creation mode. That is, if the creation mode is switched from the interface-based mode to the IP-based mode, the zone policy page will also switch to the IP-based security zone policy configuration page and the existing zone policy will be invalid and deleted, and vice versa.

The priority of the zone policy, the global policy and the default access policy is in a decreasing order.

1. Creating an Interface-based security zone policy

The interface-based security zone policy is not configured by default.

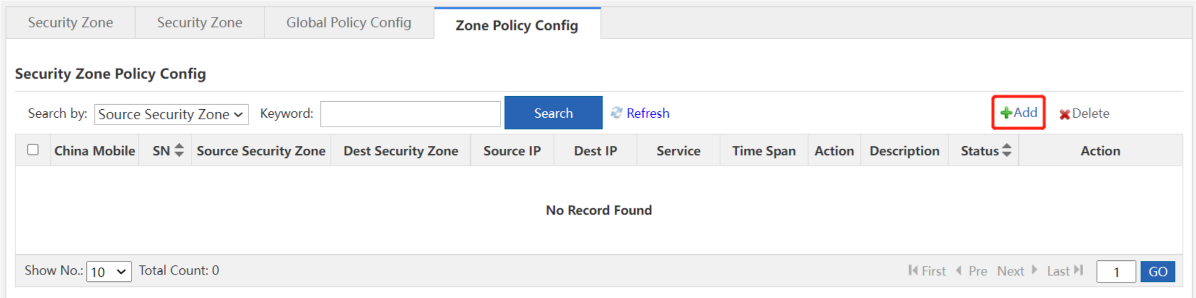
Prerequisite

Select the **Interface** mode for security zone policy configuration.

Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Zone Policy Config**.

(2) Click **Add** to access the **Add Policy** page.



Security Zone Policy Config

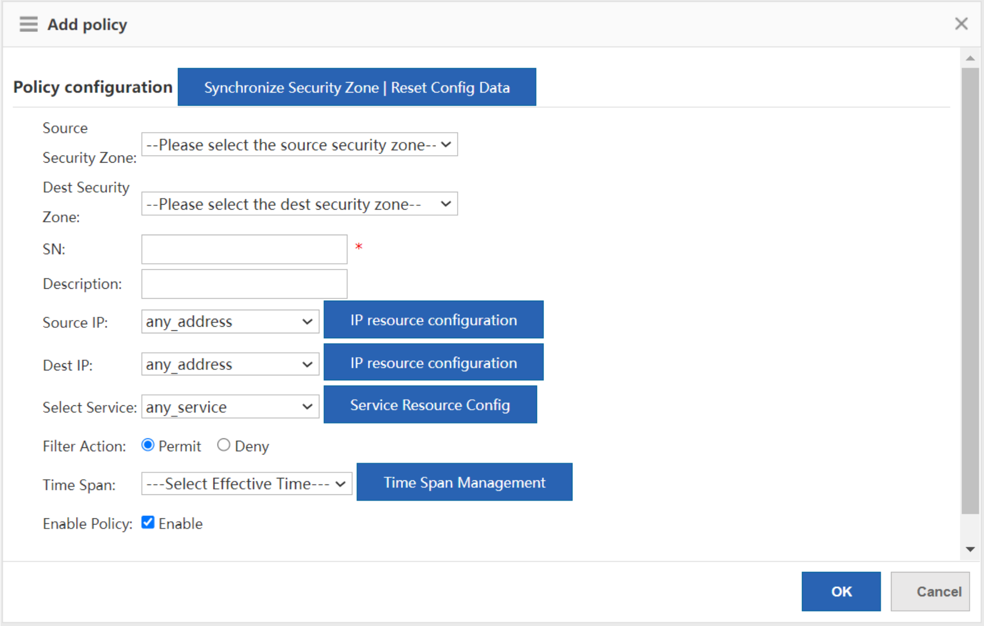
Search by: Source Security Zone Keyword:

☐	China Mobile	SN	Source Security Zone	Dest Security Zone	Source IP	Dest IP	Service	Time Span	Action	Description	Status	Action

No Record Found

Show No.: 10 Total Count: 0 1

(3) Configure the policy parameters according to the following information and click **OK**.


Add policy
Synchronize Security Zone | Reset Config Data
IP resource configuration
IP resource configuration
Service Resource Config
Time Span Management
OK
Cancel

Policy configuration

Source Security Zone: --Please select the source security zone--

Dest Security Zone: --Please select the dest security zone--

SN: *

Description:

Source IP: any_address

Dest IP: any_address

Select Service: any_service

Filter Action: ● Permit ○ Deny

Time Span: ---Select Effective Time---

Enable Policy: ☑ Enable

Configuration Item	Parameter
Source Security Zone	Control the access between the designated source security zone and the destination security zone.
Dest Security Zone	Control the access between the designated source security zone and the destination security zone.
SN	Indicate the policy priority. The lower value indicates the higher priority. The policy of higher priority is matched preferentially if multiple zone policies are configured.
Description	The description of the zone policy.
Source IP	Access control for packets from the designated source IP address. Click **IP Resource Configuration** to add a new IP address object. For details, see 1.4 IP Resource Configuration.
Dest IP	Access control for the packets to the designated destination IP address. Click **IP Resource Configuration** to add a new IP address object. For details, see 1.4 IP Resource Configuration.
Select Service	Access control for the packets from the selected service type. Click **Service Resource Configuration** to add a new service object. For details, see 1.5 Service Resource Configuration.
Filter Action	The action executed on the packets matching with the zone policy.
Time Span	The time span in which the policy takes effect.
Enable Policy	Indicate whether to enable the policy. Only an enabled zone policy will match with the packet.

2. Creating an IP-based Security Zone Policy

The interface-based security zone policy is not configured by default.

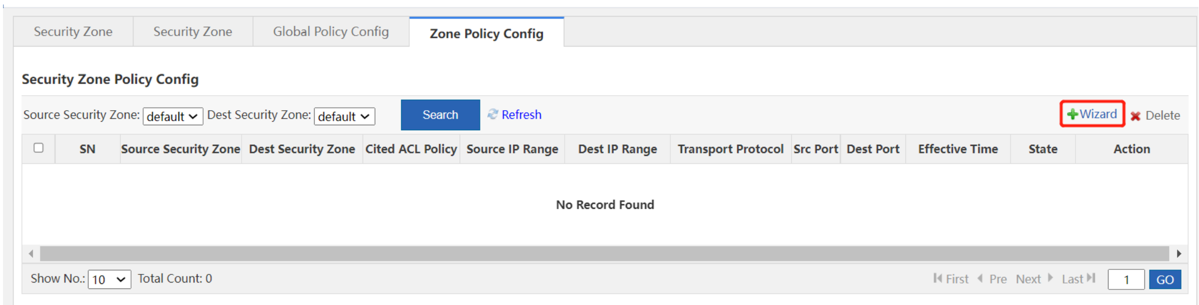
Prerequisite

Select the **IP** mode for security zone policy configuration.

Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Zone Policy Config**.

(2) Click **Wizard** to access the **Create security zone policy** page.



Security Zone Policy Config

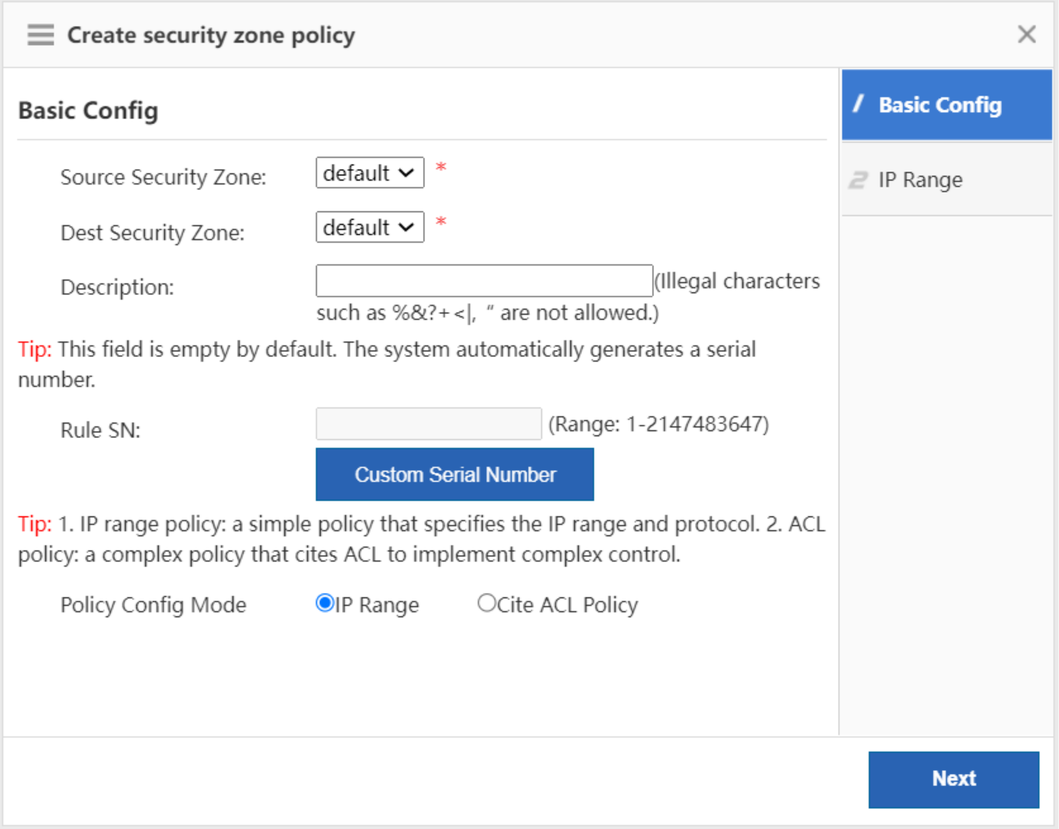
Source Security Zone: default Dest Security Zone: default Search Refresh Wizard Delete

□	SN	Source Security Zone	Dest Security Zone	Cited ACL Policy	Source IP Range	Dest IP Range	Transport Protocol	Src Port	Dest Port	Effective Time	State	Action

No Record Found

Show No.: 10 Total Count: 0 First Pre Next Last 1 GO

(3) Configure the policy parameters according to the following information and click **Next**.



Basic Config

Source Security Zone: default *

Dest Security Zone: default *

Description: (Illegal characters such as %&?+<|, " are not allowed.)

Tip: This field is empty by default. The system automatically generates a serial number.

Rule SN: (Range: 1-2147483647)

Tip: 1. IP range policy: a simple policy that specifies the IP range and protocol. 2. ACL policy: a complex policy that cites ACL to implement complex control.

Policy Config Mode ● IP Range ○ Cite ACL Policy

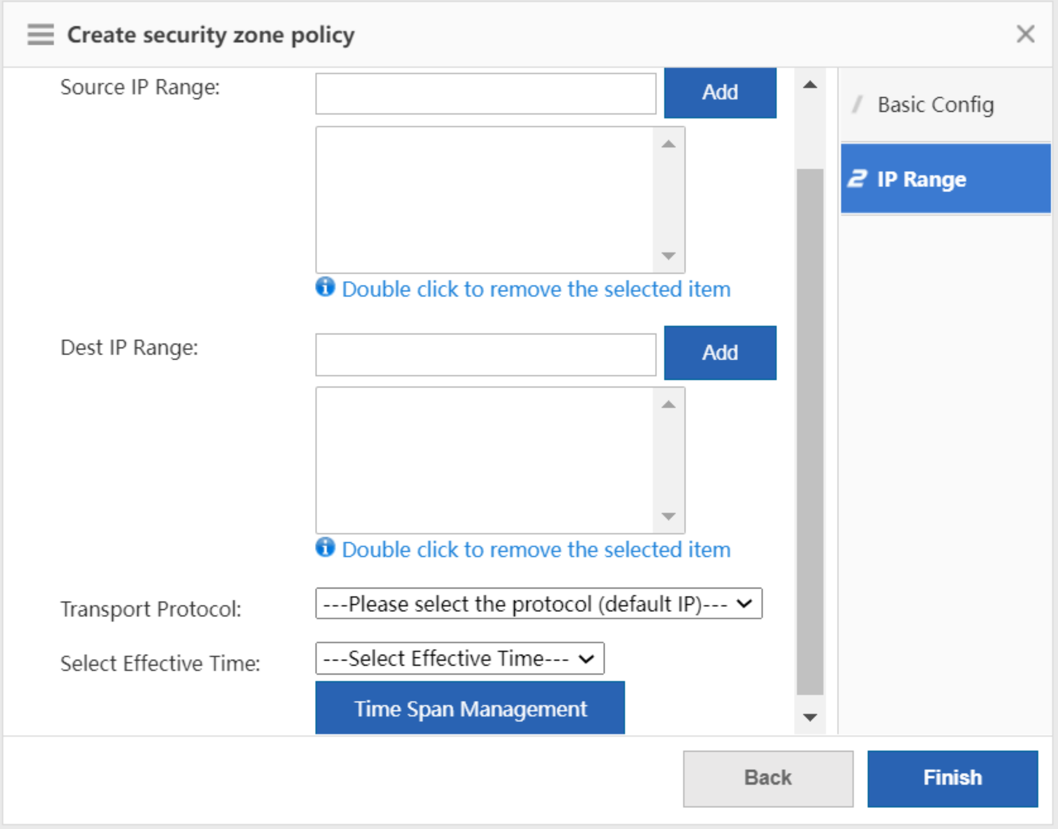
Configuration Item	Parameter
Source Security Zone	Control the access between the designated source security zone and the destination security zone.
Dest Security Zone	Control the access between the designated source security zone and the destination security zone.
Description	The description of the zone policy.
Rule SN	Indicate the policy priority. The lower value stands for the higher priority. The policy of higher priority is matched preferentially if multiple zone policies are configured.

Policy Config Mode	Indicate the mode of matching packets, which supports matching packets based on the IP range or ACL rules.

(4) Configure the IP range according to the following information and click **Finish**. If you select **Cite ACL Policy** for the policy configuration mode, skip this procedure and move on to next step.

Note

After the IP range is configured, the access is allowed or blocked according to the ACL policy with which the IP range matches.

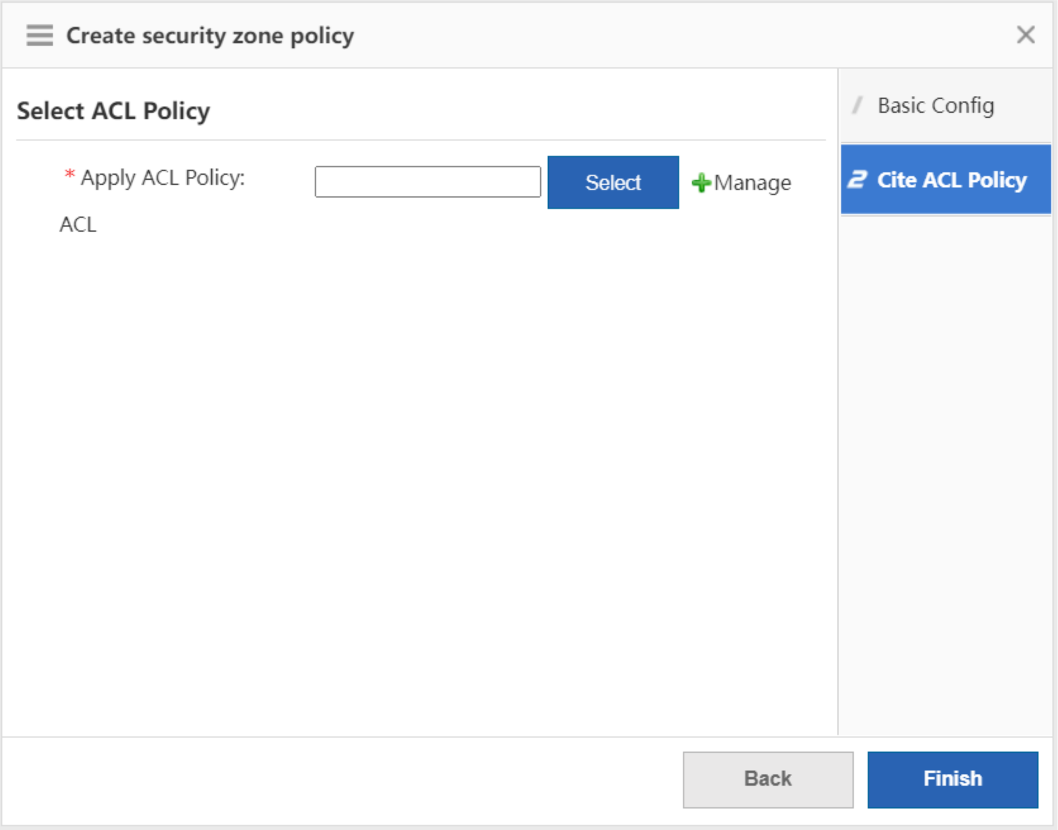

Create security zone policy
Source IP Range:
Add
Double click to remove the selected item
Dest IP Range:
Add
Double click to remove the selected item
Transport Protocol:
---Please select the protocol (default IP)---
Select Effective Time:
---Select Effective Time---
Time Span Management
Basic Config
2 IP Range
Back
Finish

Configuration Item	Parameter
Source IP Range	Access control for the packets from the designated source IP address. You can enter a single IP address (example: 1.1.1.1), a subnet or mask length (example: 1.1.1.0/24), a subnet or mask (example: 1.1.1.0/255.255.255.0) or any. Enter a source IP range and click **Add** to enter another range.

Dest IP Range	Access control for the packets to the designated destination IP address. You can enter a single IP address (example: 1.1.1.1), a subnet or mask length (example: 1.1.1.0/24), a subnet or mask (example: 1.1.1.0/255.255.255.0) or any. Enter a source IP range and click **Add** to enter another range.
Transport Protocol	Access control for the packets of the selected protocol.
Select Effective Time	Indicate the time span in which the policy takes effect. Click **Time Span Management** to select a time span.

(5) Configure the ACL policy according to the following information and click **Finish**. If you select **IP Range** for the policy configuration mode, skip this procedure.

a Click **Select** to select configured ACL policy. If there is no available ACL policy, click **Manage** to create an ACL policy.

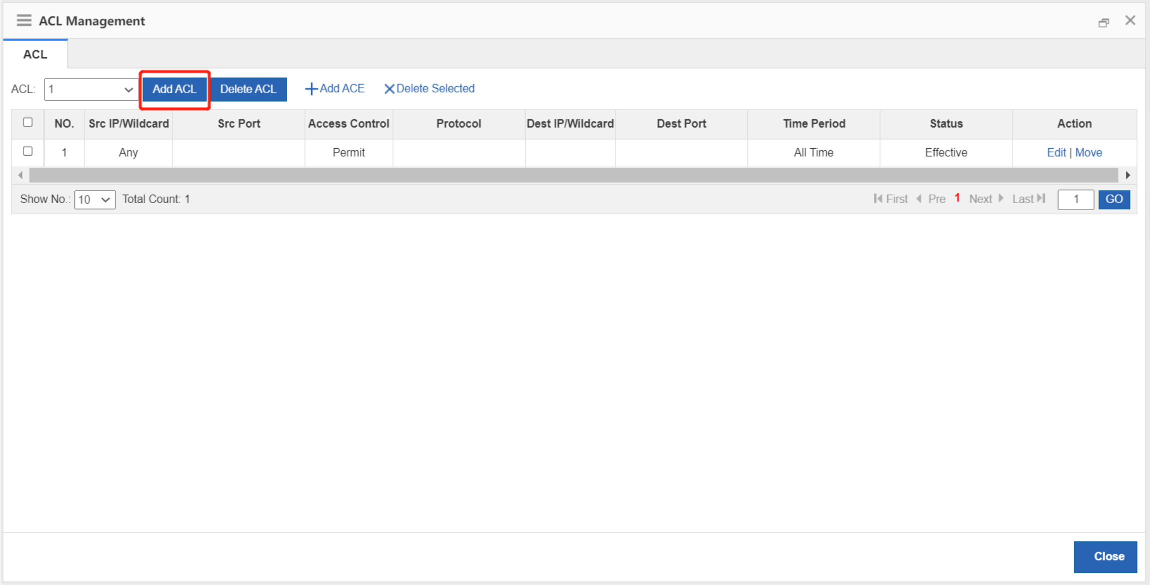


Create security zone policy

Select ACL Policy

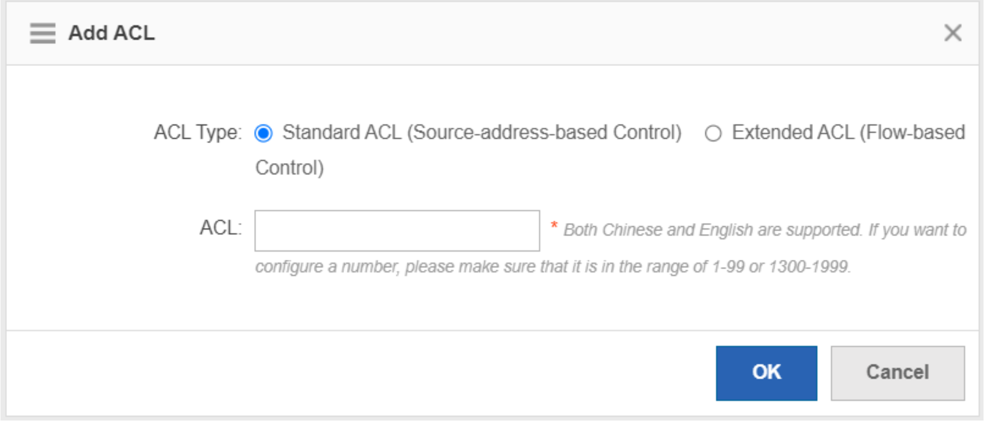
* Apply ACL Policy: ACL

b Click **Add ACL** to access the **Add ACL** page.



□	NO.	Src IP/Wildcard	Src Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action
□	1	Any		Permit				All Time	Effective	Edit | Move

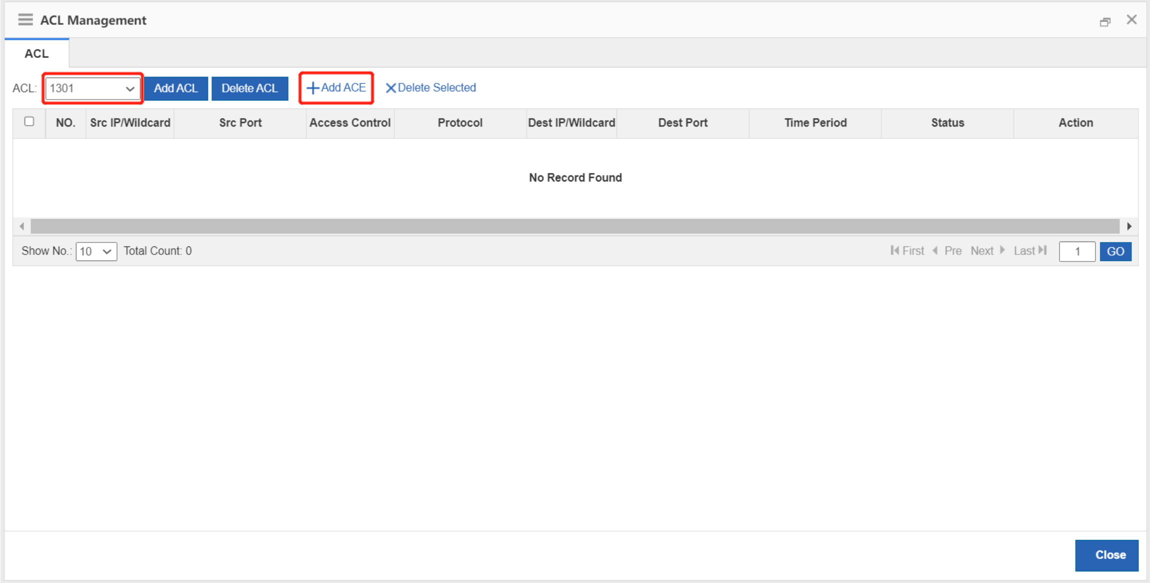
c Select the ACL type, enter the ACL name or the ACL number and click **OK**.



ACL Type: ● Standard ACL (Source-address-based Control) ○ Extended ACL (Flow-based Control)

ACL: * Both Chinese and English are supported. If you want to configure a number, please make sure that it is in the range of 1-99 or 1300-1999.

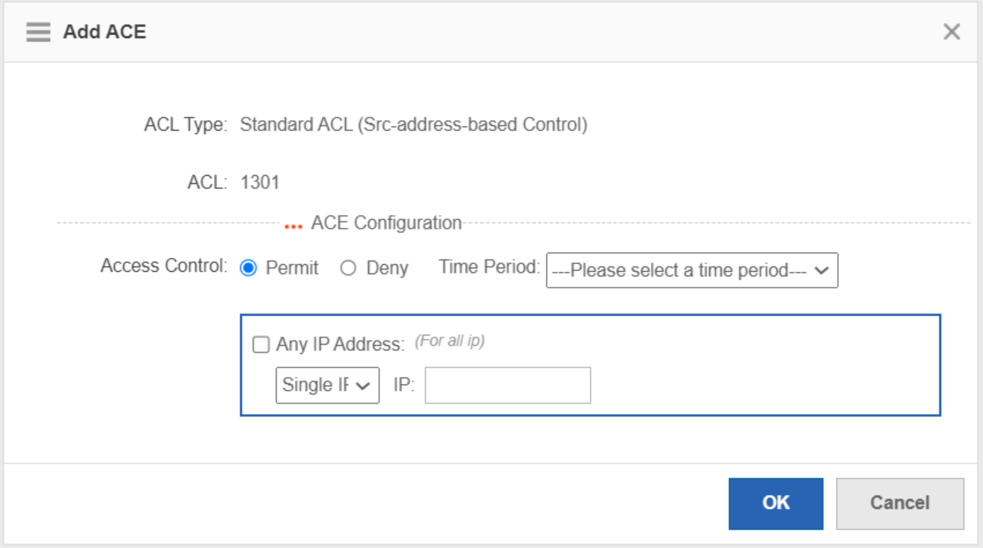
d Select the created ACL and click **Add ACE** to access the **Add ACE** page.



□	NO.	Src IP/Wildcard	Src Port	Access Control	Protocol	Dest IP/Wildcard	Dest Port	Time Period	Status	Action

No Record Found

e Configure the ACE according to the following information and click **OK**.



ACL Type: Standard ACL (Src-address-based Control)

ACL: 1301

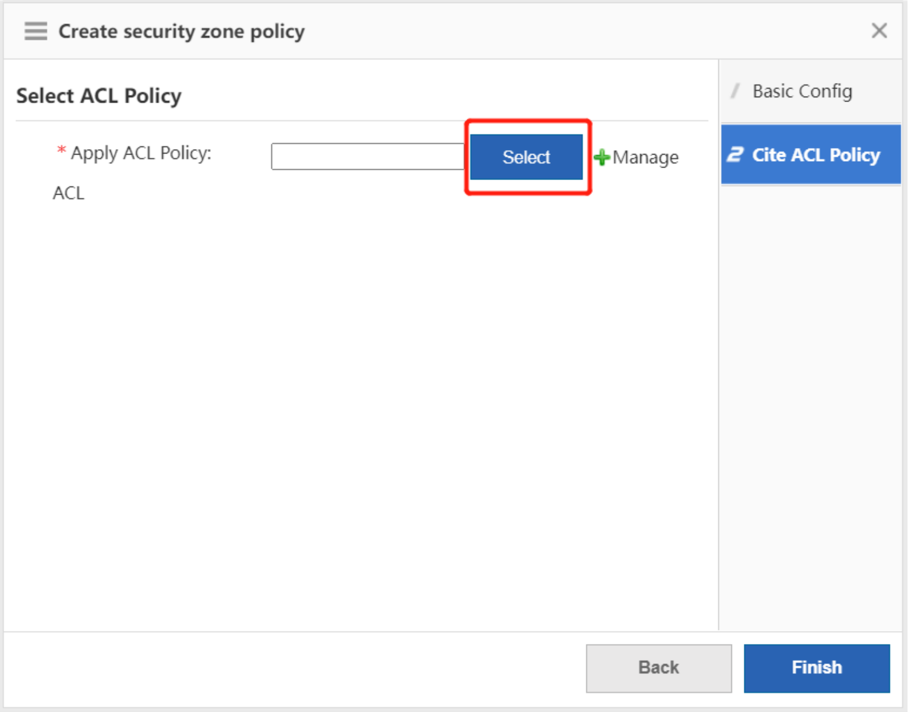
Access Control: ● Permit ○ Deny Time Period: ---Please select a time period---

□ Any IP Address: *(For all ip)*

Single IP IP:

Configuration Item	Parameter
Access Control	Access control for the packets matching the ACE.
Time Period	Indicate the time period in which the ACE takes effect. Click the drop-down list box to select a time period.
IP Address	Access control for the packets from or to the designated IP address. You can enter a single IP address (example: 1.1.1.1), a subnet or mask (example: 1.1.1.0/255.255.255.0) or a wildcard (example: 1.1.1.0/0.0.0.255). If you select **Any IP Address**, the packets from all IP addresses will match the ACE.

f After the ACE is configured, close the **ACL Management** page. Click **Select** on the **Create security zone policy** page to access the **Please select the ACL policy from the table** page.



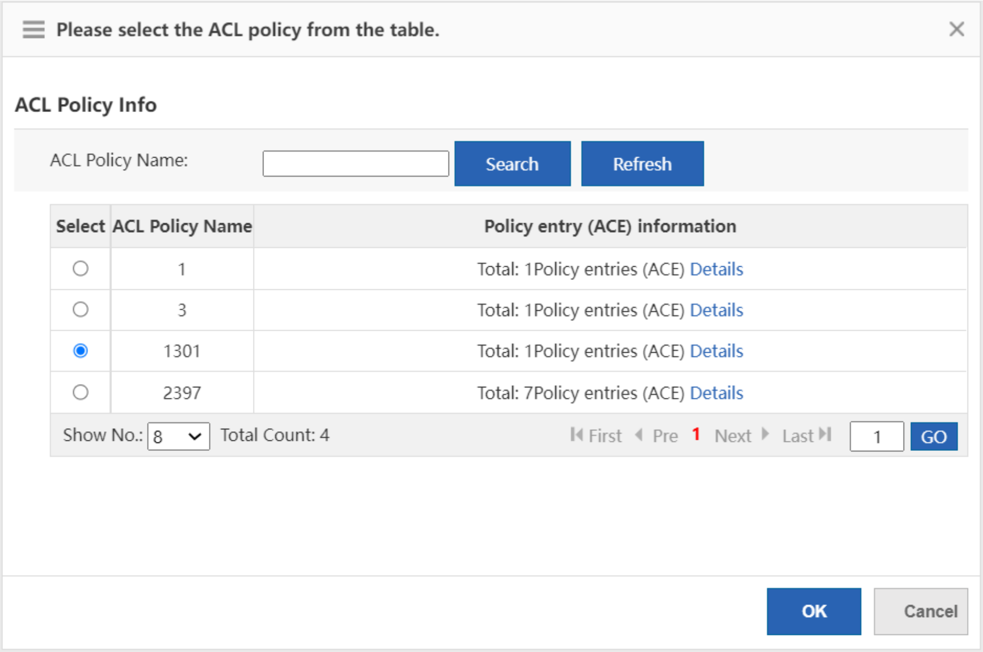
Create security zone policy

Select ACL Policy

* Apply ACL Policy:

ACL

g Click **Refresh**, select the created ACL policy and click **OK**.



Please select the ACL policy from the table.

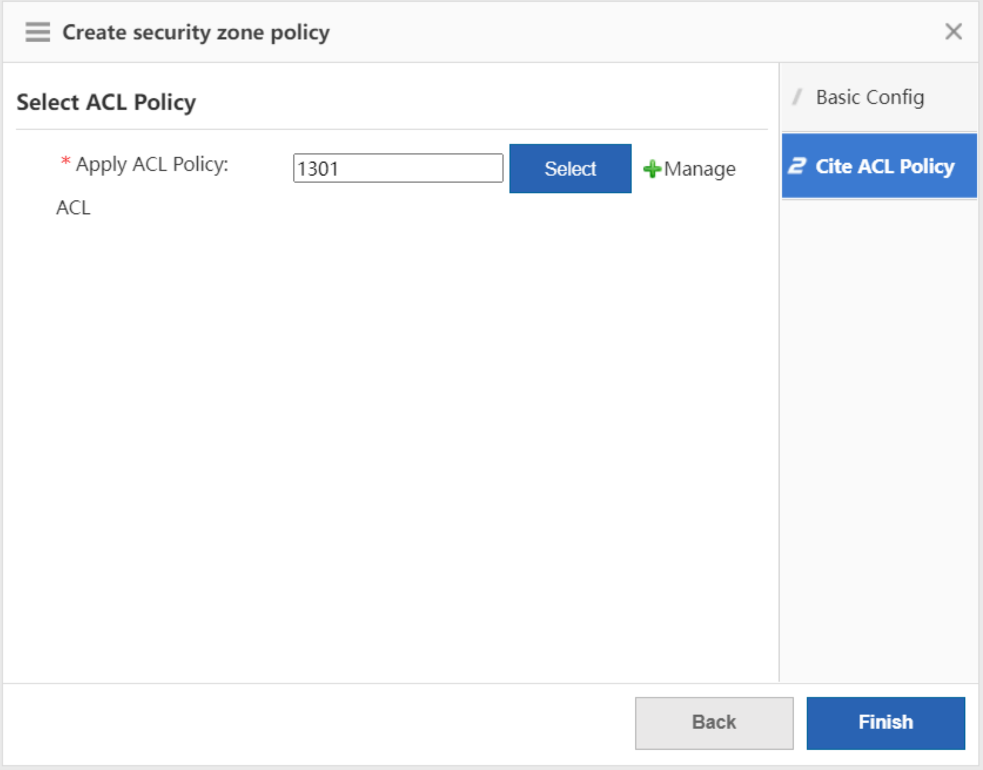
ACL Policy Info

ACL Policy Name:

Select	ACL Policy Name	Policy entry (ACE) information
○	1	Total: 1Policy entries (ACE) Details
○	3	Total: 1Policy entries (ACE) Details
●	1301	Total: 1Policy entries (ACE) Details
○	2397	Total: 7Policy entries (ACE) Details

Show No.: 8 Total Count: 4

h Click **Finish**.



Create security zone policy

Select ACL Policy

* Apply ACL Policy: 1301

ACL

8.3 Defense Zone Monitoring

8.3.1 Zone Running Status

The function is used to display the basic information and traffic statistics of each defense zone.

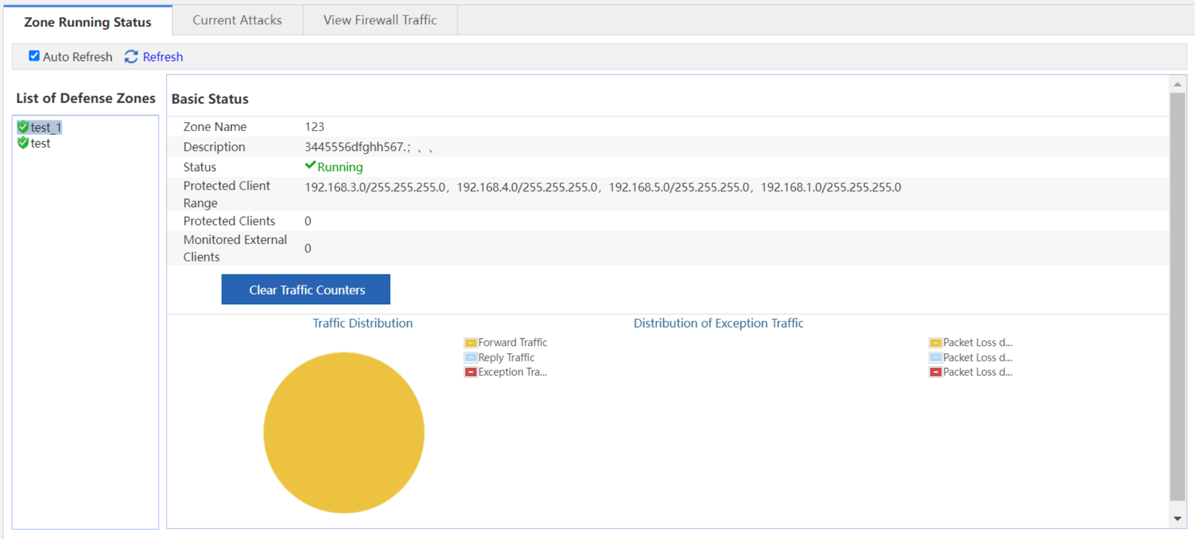
Prerequisite

The defense zone policy is configured. For details, see 1.1.4 Zone Policy.

Procedure

(1) Choose **Firewall** > **Defense Zone Status** > **Zone Running Status**.

(2) Select a defense zone, and its basic information, running status and traffic statistics will be displayed on the right of the page.



Zone Name	123
Description	3445556dfghh567.; 、、
Status	✓Running
Protected Client Range	192.168.3.0/255.255.255.0, 192.168.4.0/255.255.255.0, 192.168.5.0/255.255.255.0, 192.168.1.0/255.255.255.0
Protected Clients	0
Monitored External Clients	0

8.3.2 Current Attacks

The function is used to display the current attacks in each defense zone, and filter the attack information based on attack types or protocol types.

Prerequisite

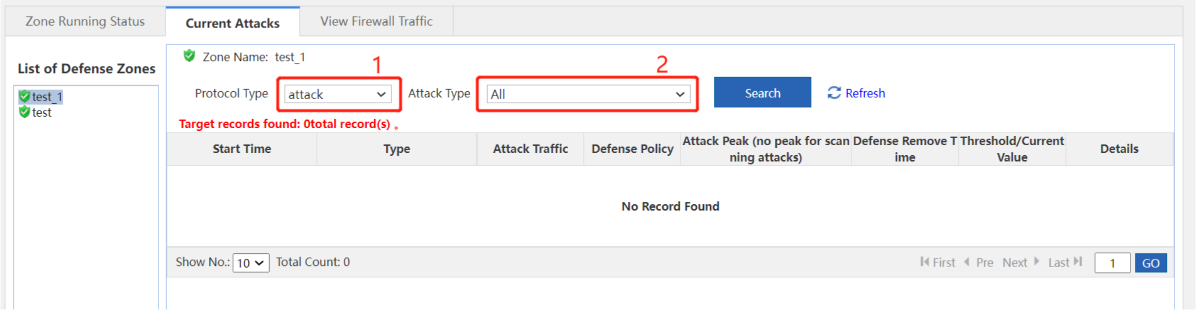
The defense zone policy is configured. For details, see 1.1.4 Zone Policy.

Procedure

(1) Choose **Firewall** > **Defense Zone Status** > **Current Attacks**.

(2) Select a defense zone. By default, the current attacks in the selected defense zone will be displayed by attack types on the right of the page.

(3) (Optional) Click the drop-down list box of **Protocol Type** and select another protocol. Click **Search** to display the attack information based on protocol types.



Zone Name: test_1

Protocol Type: attack

Attack Type: All

Target records found: 0total record(s) 。

Start Time	Type	Attack Traffic	Defense Policy	Attack Peak (no peak for scanning attacks)	Defense Remove Time	Threshold/Current Value	Details
No Record Found							

Show No.: 10 Total Count: 0 1

8.3.3 Viewing Firewall Traffic

The function is used to display global defense information.

Prerequisite

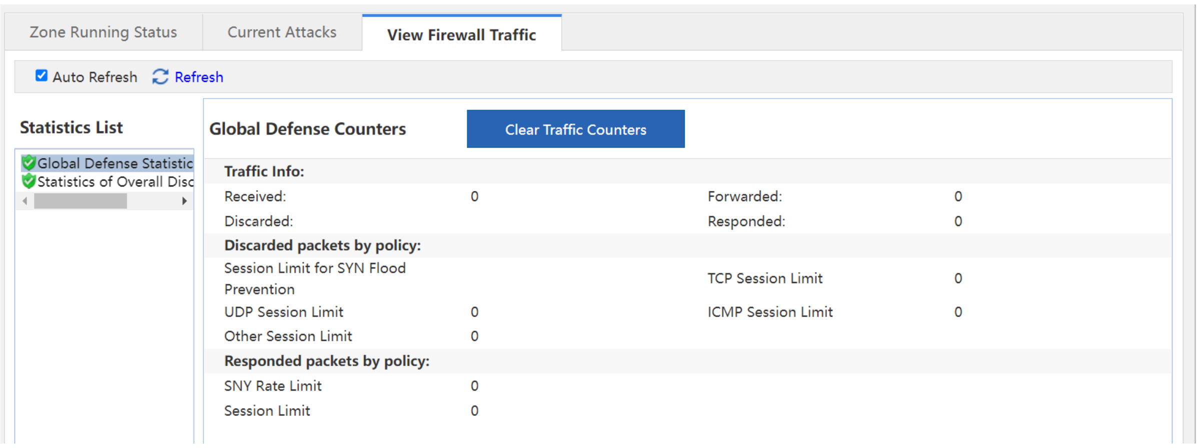
Global defense is configured. For details, see 1.1.2 Global Defense.

Procedure

(1) Choose **Firewall** > **Defense Zone Status** > **View Firewall Traffic**.

(2) Click **Global Defense Statistics** to view defense traffic statistics.

(3) Click **Statistics of Overall Discarded Packets** to view the statistics of the discarded packets based on the defense policy.



Traffic Info:

Received:	0	Forwarded:	0
Discarded:		Responded:	0
Discarded packets by policy:			
Session Limit for SYN Flood Prevention		TCP Session Limit	0
UDP Session Limit	0	ICMP Session Limit	0
Other Session Limit	0		
Responded packets by policy:			
SNY Rate Limit	0		
Session Limit	0		

8.4 IP Resource Configuration

The IP resource function must work with other functions instead of working independently. For example, when configuring the inter-domain policy, you can implement access control on the packets of the designated source IP address in the source security zone.

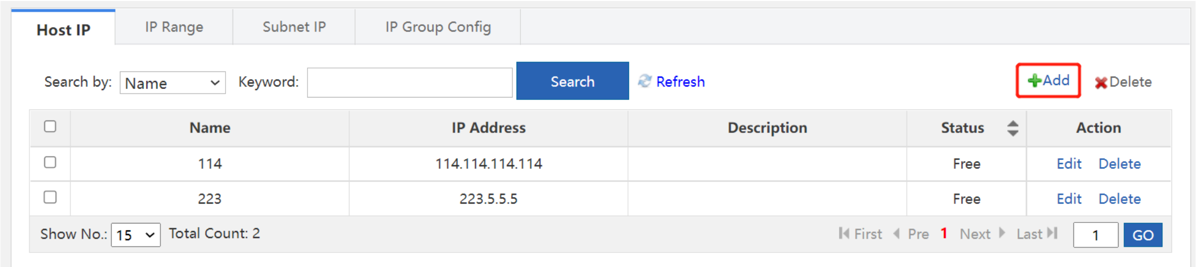
8.4.1 Host IP Address

The host IP address is a single IP address. The administrator can configure a proper name for a single IP address to identify the device with the IP address quickly.

Procedure

(1) Choose **Firewall** > **IP Resource** > **Host IP**.

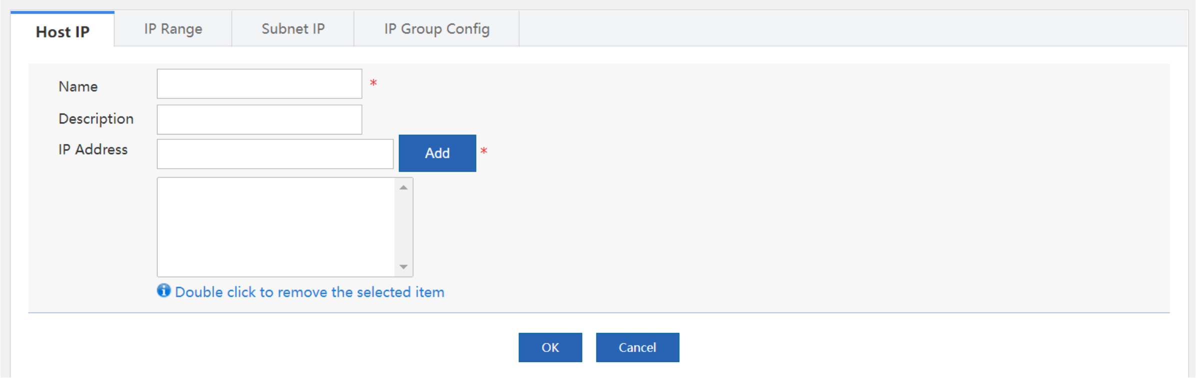
(2) Click **Add**.



☐	Name	IP Address	Description	Status	Action
☐	114	114.114.114.114		Free	Edit Delete
☐	223	223.5.5.5		Free	Edit Delete

Show No.: 15 Total Count: 2 First Pre 1 Next Last 1 GO

(3) Enter the name, description and the IP address, and click **Add**. If you need multiple IP addresses, you can enter other IP addresses and click **Add**.



(4) Click **OK**.

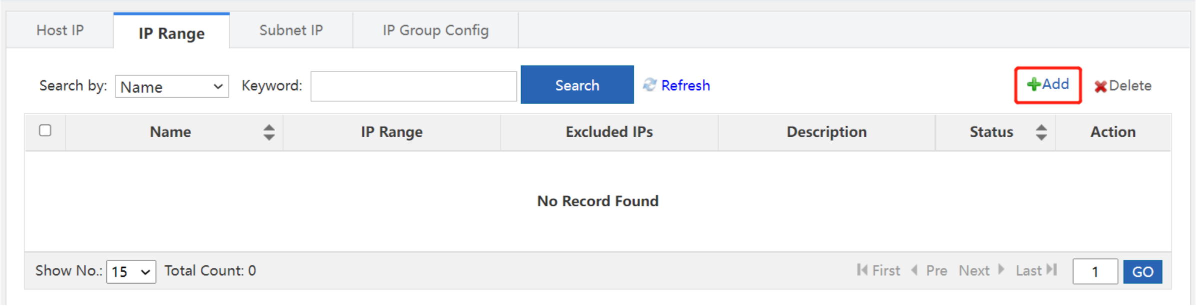
8.4.2 IP Range

IP range indicates a range of multiple IP addresses, such as 1.1.1.1 to 1.1.1.10. The administrator can configure a proper name for an IP range to identify the device with the IP address within the range quickly.

Procedure

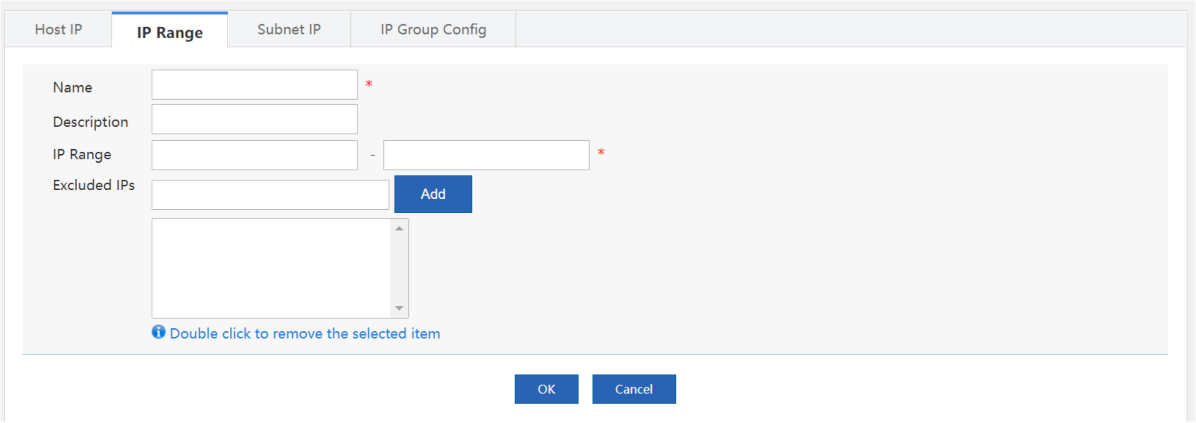
(1) Choose **Firewall** > **IP Resource** > **IP Range**.

(2) Click **Add**.



□	Name	IP Range	Excluded IPs	Description	Status	Action
			No Record Found			

(3) Enter the name, description and the IP range. If there is an excluded IP address, enter the excluded IP address (only a single IP address is supported.) and click **Add**. If you need to add multiple excluded IP addresses, enter other excluded IP addresses and click **Add**.



(4) Click **OK**.

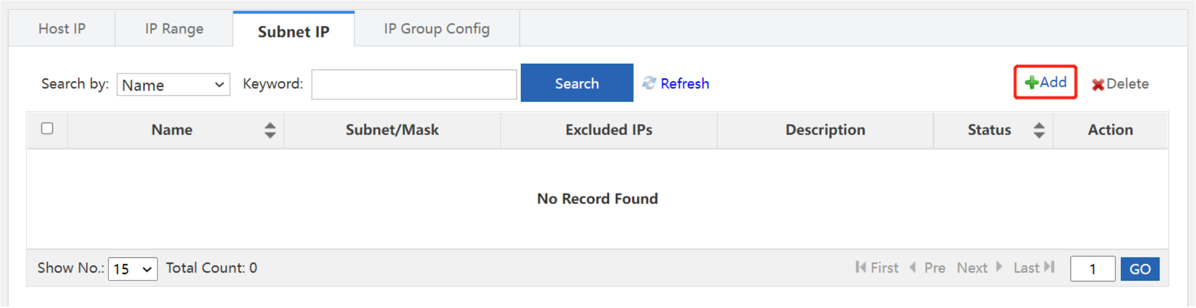
8.4.3 Subnet IP Address

For example, 1.1.1.0/255.255.255.0 is a subnet IP address. The administrator can configure a proper name for a subnet IP address to identify the subnet quickly.

Procedure

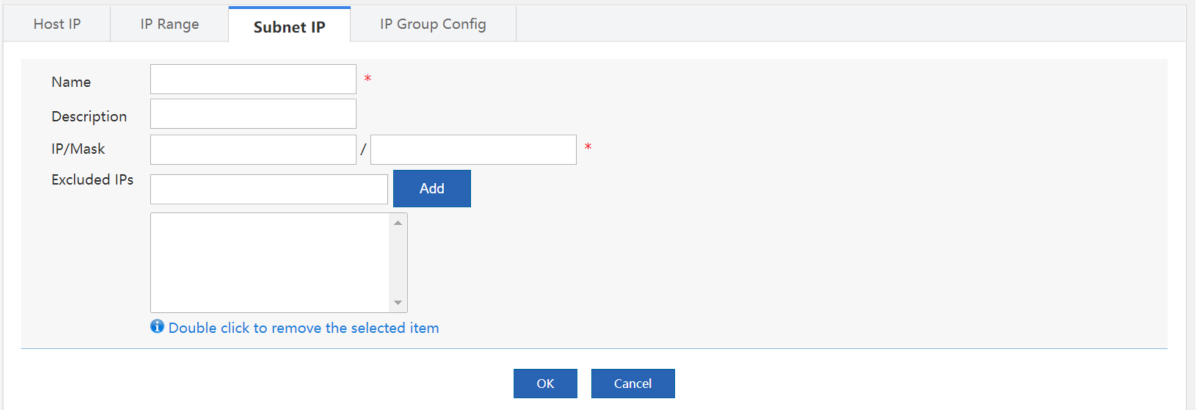
(1) Choose **Firewall** > **IP Resource** > **Subnet IP**.

(2) Click **Add**.



□	Name	Subnet/Mask	Excluded IPs	Description	Status	Action
			No Record Found			

(3) Enter the name, description, the IP address or the mask. If there is an excluded IP address, enter the excluded IP address (only a single IP address is supported.) and click **Add**. If you need to add multiple excluded IP addresses, enter other excluded IP addresses and click **Add**.



(4) Click **OK**.

8.4.4 IP Group Configuration

An IP group is a collection of multiple IP addresses. You can put the host IP address, the IP range or the subnet IP address with the same defense requirements into an IP group for convenient management.

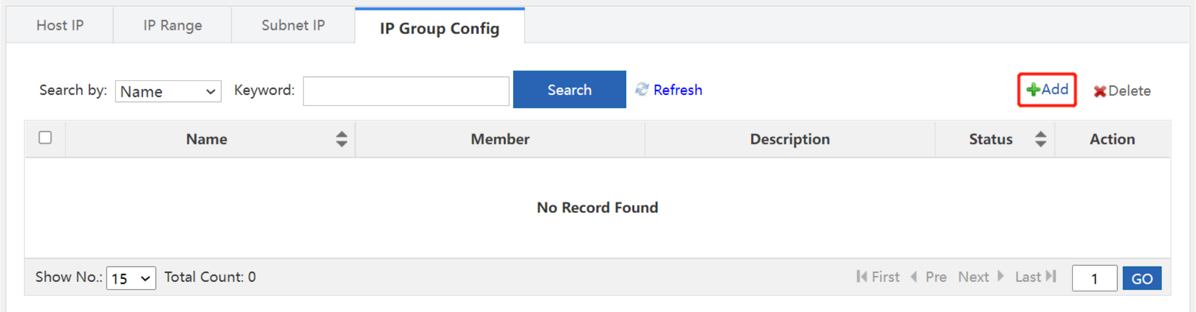
Prerequisite

The host IP address, the IP range or the subnet IP address are configured.

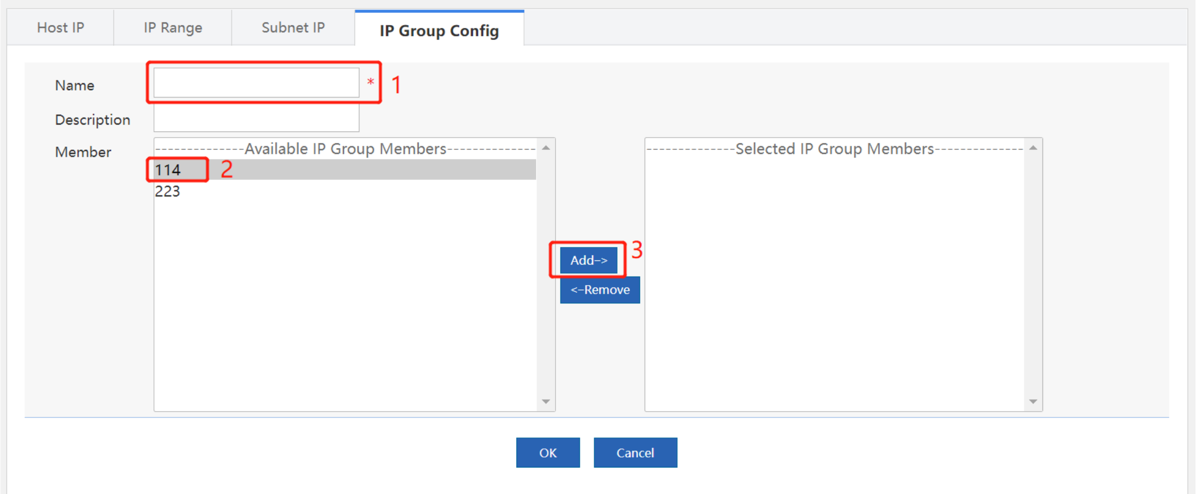
Procedure

(1) Choose **Firewall** > **IP Resource** > **IP Group Config**.

(2) Click **Add**.



(3) Enter the name and description, select the members of the IP group as required, and click **Add**.



(4) Click **OK**.

8.5 Service Resource Configuration

The service resource is represented by protocol types and features. Protocol features are used to match the upper layer protocols carried in the packets, such as the source port and the destination port of TCP and UDP, the ICMP message type or message authentication code.

The service resource does not work independently but works with other functions. For example, you can implement access control on the packets of a specified service when configuring the inter-security zone policies.

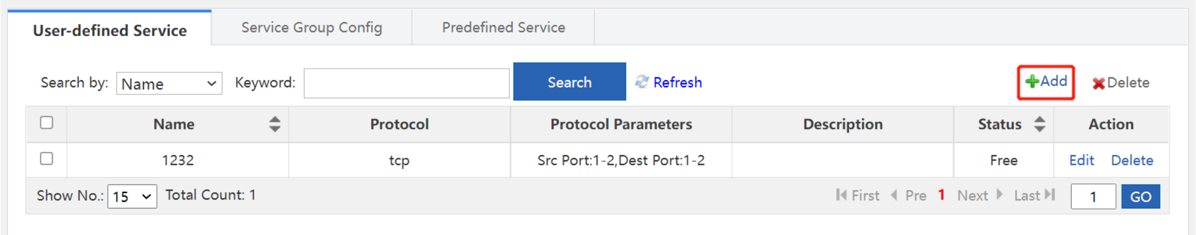
8.5.1 Customer Service

The device predefines common services. You can view the services on the **Predefined Service** page. If the predefined services do not include the required service, you can configure the service resource by yourself.

Procedure

(1) Choose **Firewall** > **Service Resource** > **User-defined Service**.

(2) Click **Add**.



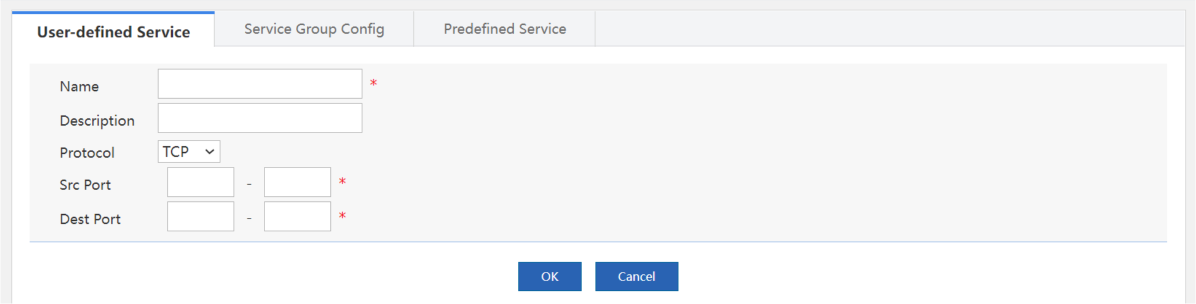
□	Name	Protocol	Protocol Parameters	Description	Status	Action
□	1232	tcp	Src Port:1-2,Dest Port:1-2		Free	Edit Delete

Show No.: 15 Total Count: 1 First Pre 1 Next Last 1 GO

(3) Enter the name and description. Select the protocol, configure the parameters of the protocol and click **OK**.

Note

The parameters may vary with the protocols. The parameters displayed on the webpage prevails.



Name *
Description
Protocol TCP
Src Port - *
Dest Port - *

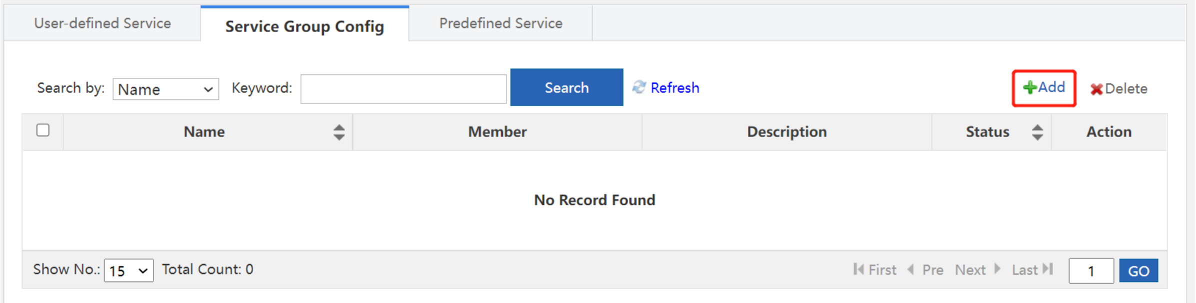
8.5.2 Service Group Configuration

A service group is a collection of multiple services. You can add the custom or predefined services with the same defense requirements to a group for convenient management.

Procedure

(1) Choose **Firewall** > **Service Resource** > **Service Group Config**.

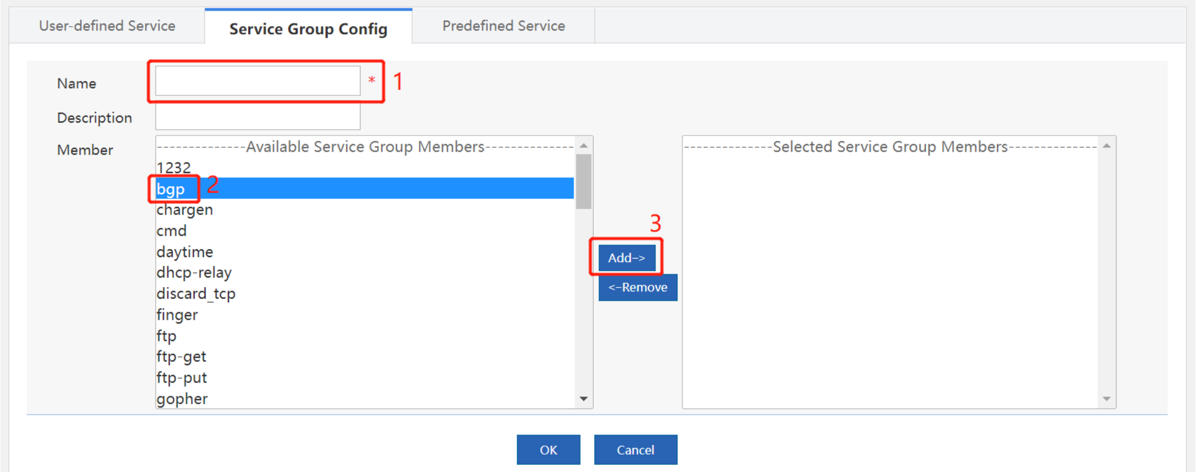
(2) Click **Add**.



□	Name	Member	Description	Status	Action
No Record Found					

Show No.: 15 Total Count: 0 First Pre Next Last 1 GO

(3) Enter the name and description. Select service group members as required and click **Add**.



(4) Click **OK**.

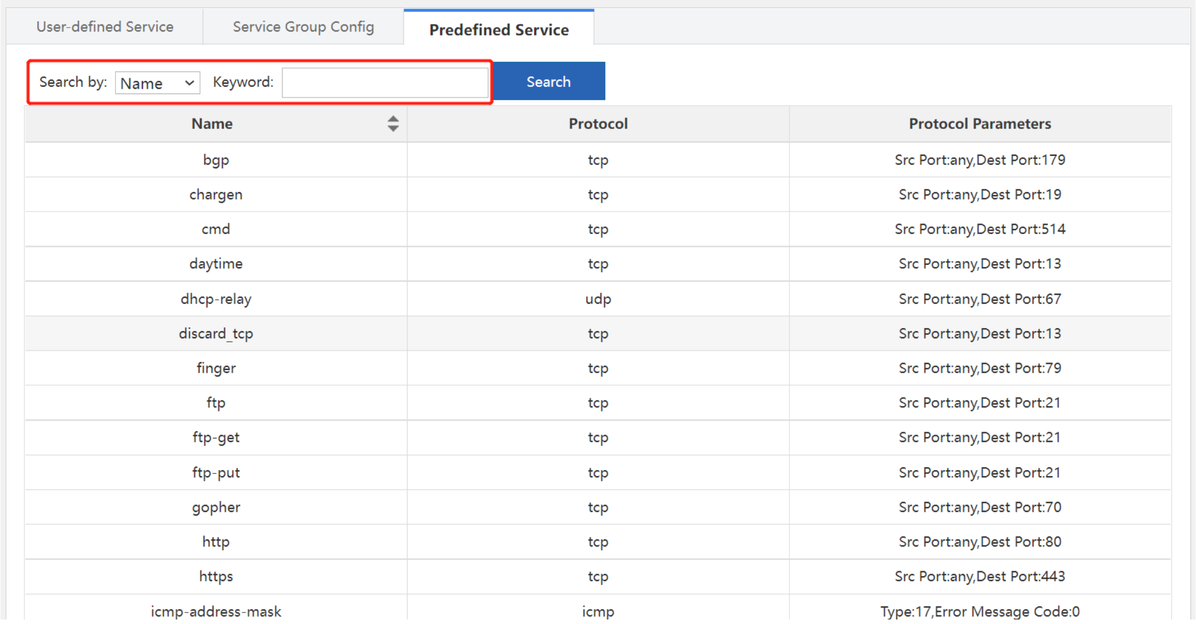
8.5.3 Predefined Service

The function is used to display predefined services.

Procedure

(1) Choose **Firewall** > **Service Resource** > **Predefined Service**.

(2) (Optional) Select a query item or enter a keyword and click **Search** to search for the service information you need.



Name	Protocol	Protocol Parameters
bgp	tcp	Src Port:any,Dest Port:179
chargen	tcp	Src Port:any,Dest Port:19
cmd	tcp	Src Port:any,Dest Port:514
daytime	tcp	Src Port:any,Dest Port:13
dhcp-relay	udp	Src Port:any,Dest Port:67
discard_tcp	tcp	Src Port:any,Dest Port:13
finger	tcp	Src Port:any,Dest Port:79
ftp	tcp	Src Port:any,Dest Port:21
ftp-get	tcp	Src Port:any,Dest Port:21
ftp-put	tcp	Src Port:any,Dest Port:21
gopher	tcp	Src Port:any,Dest Port:70
http	tcp	Src Port:any,Dest Port:80
https	tcp	Src Port:any,Dest Port:443
icmp-address-mask	icmp	Type:17,Error Message Code:0

9 Advanced

9.1 System

9.1.1 Change Password

Web management password: For device configuration on the web page, the password is required for device login. You can change the login password as the **admin** user on this page. After a new web management password is set, the new password is required for re-login.

Telnet password: For device login and configuration using Telnet, the password is required.

⚠ Caution

- Be sure to keep the password after change in mind. Otherwise, login may fail next time.
- Only the **Administrators** group has permission to configure this page, that is, this page is visible only to the **admin** user.

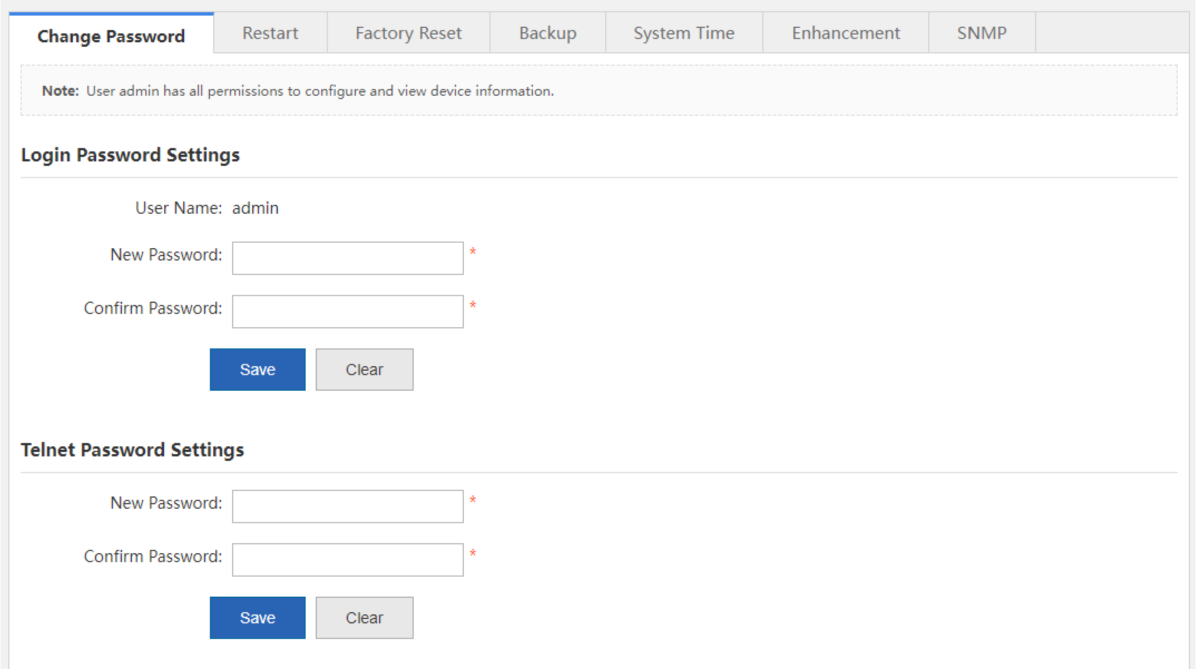
Application Scenario

For device security, you are recommended to change the initial password of the device as soon as possible after your first login.

Procedure

(1) Choose **Advanced** > **System** > **Change Password**.

(2) Enter the web management password or Telnet password based on the actual requirements and click **Save**.



Note: User admin has all permissions to configure and view device information.

Login Password Settings

User Name: admin

New Password: *

Confirm Password: *

Telnet Password Settings

New Password: *

Confirm Password: *

9.1.2 Restart

Device restart takes about 1 minute. Do not perform any other operations during restart. The page will be automatically refreshed after the restart is successful.

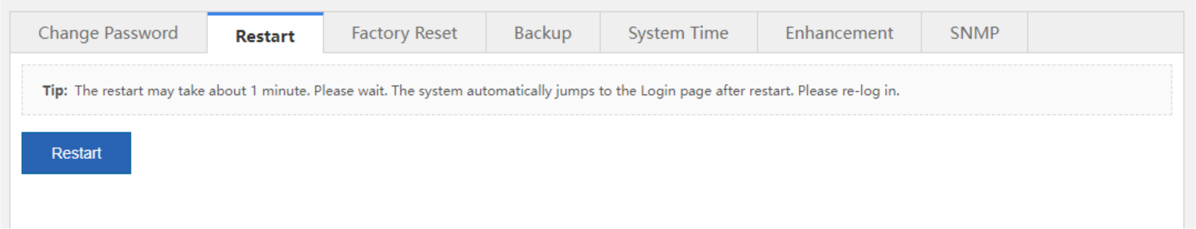
Prerequisites

All configurations have been saved before restart. Otherwise, unsaved configuration information will be lost after restart.

Procedure

(1) Choose **Advanced** > **System** > **Restart**.

(2) Click **Restart**.



Tip: The restart may take about 1 minute. Please wait. The system automatically jumps to the Login page after restart. Please re-log in.

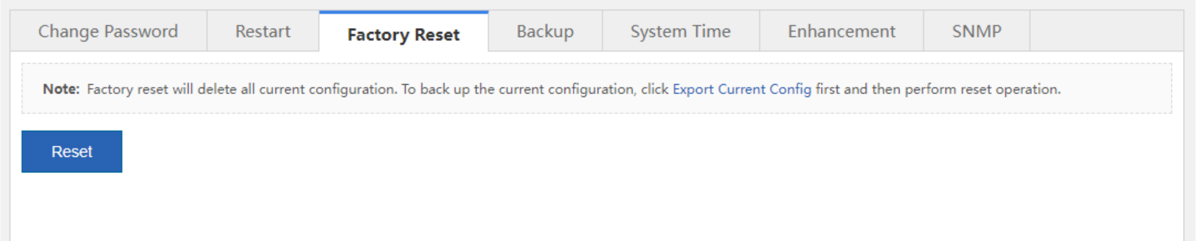
9.1.3 Factory Reset

Factory Reset: clears all the current configurations of the device and restores the device to the default factory settings. To keep your existing configurations, export the current configurations on the **Backup** tab page first.

Procedure

(1) Choose **Advanced** > **System** > **Factory Reset**.

(2) Click **Reset**.



Note: Factory reset will delete all current configuration. To back up the current configuration, click Export Current Config first and then perform reset operation.

9.1.4 Backup

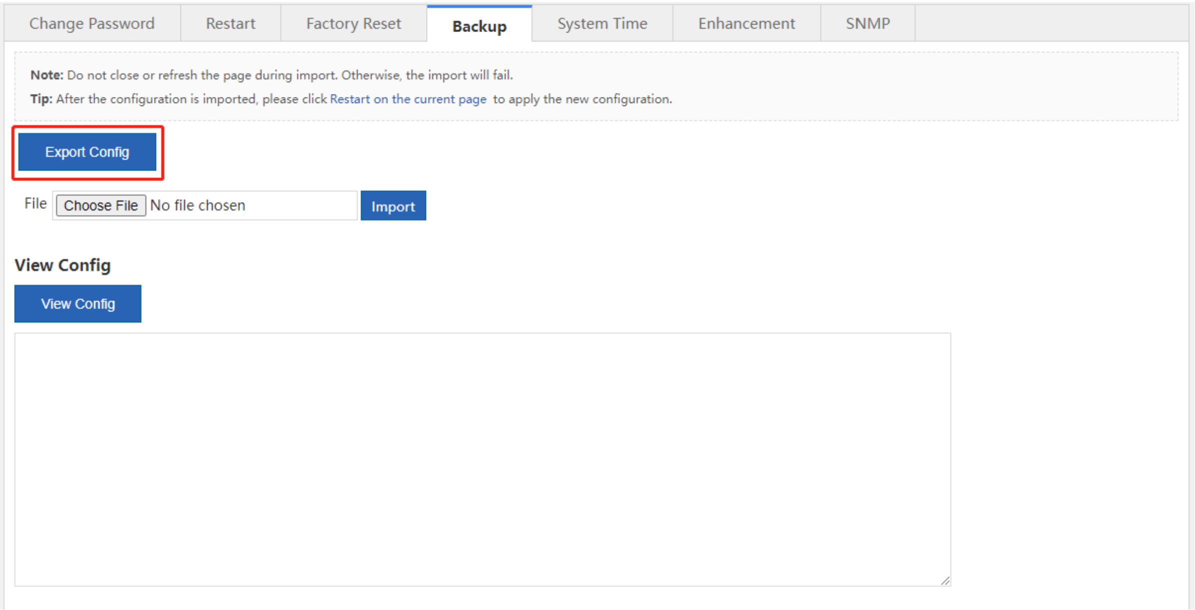
1. Export Config

Export Config: exports the current configurations of the device to a local computer for backup.

Procedure

(1) Choose **Advanced** > **System** > **Backup**.

(2) Click **Export Config**.



Note: Do not close or refresh the page during import. Otherwise, the import will fail.

Tip: After the configuration is imported, please click Restart on the current page to apply the new configuration.

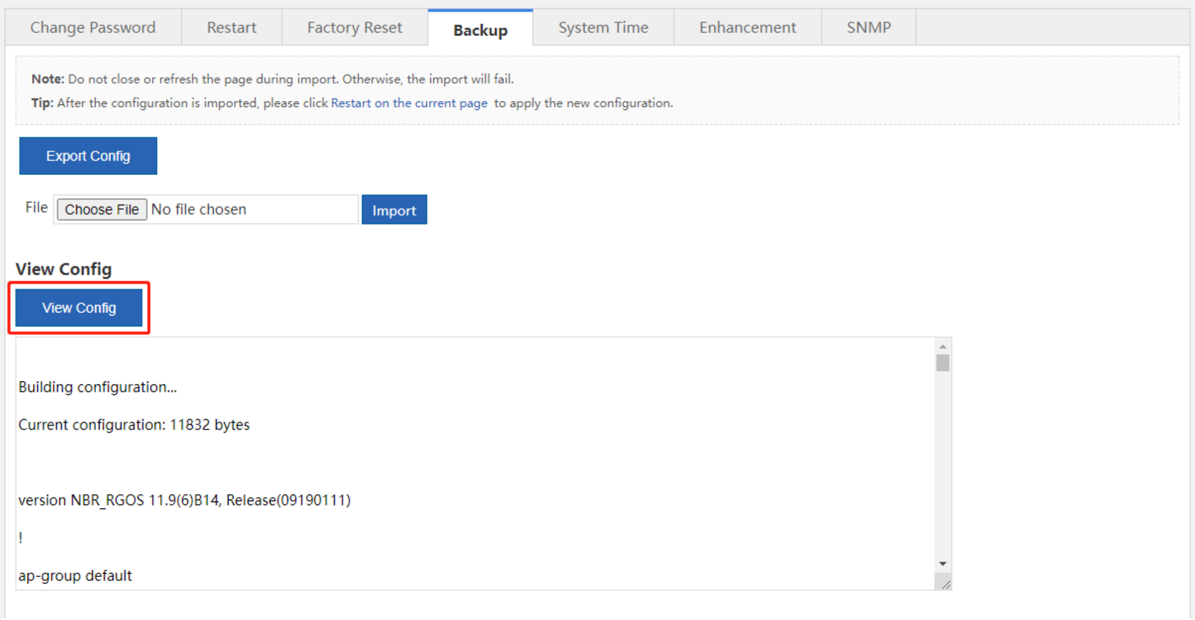
(3) Set the path for storing the configuration file and click **Save**.

2. View Config

View Config: views all configuration commands of the current device.

(1) Choose **Advanced** > **System** > **Backup**.

(2) Click **View Config**.



Note: Do not close or refresh the page during import. Otherwise, the import will fail.

Tip: After the configuration is imported, please click Restart on the current page to apply the new configuration.

```
Building configuration...

Current configuration: 11832 bytes


version NBR_RGOS 11.9(6)B14, Release(09190111)

!

ap-group default
```

9.1.5 System Time

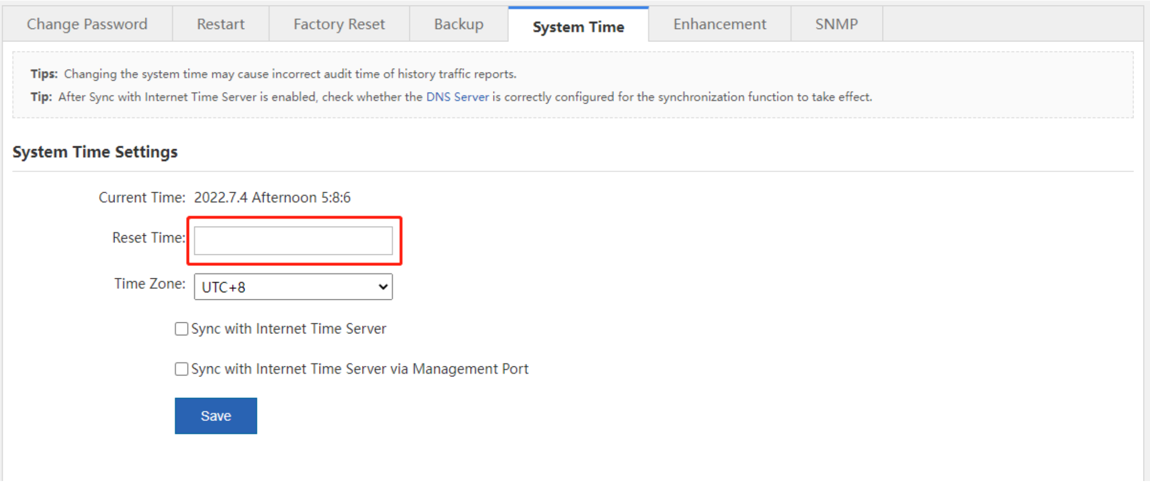
System Time: sets the system time of the device. The device supports the following two system time change methods: manual change and synchronization from the time server. For the latter one, before time synchronization from the Internet time server, choose **Network** > **DNS Settings** and set the DNS server correctly to ensure network connectivity between the device and the time server.

Procedure

(1) Choose **Advanced** > **System** > **System Time**.

(2) Change the system time manually.

a Deselect **Sync with Internet Time Server** and **Sync with Internet Time Server via Management Port**. Click the text box corresponding to **Reset Time** and set the date and time.



Tips: Changing the system time may cause incorrect audit time of history traffic reports.
Tip: After Sync with Internet Time Server is enabled, check whether the DNS Server is correctly configured for the synchronization function to take effect.

System Time Settings

Current Time: 2022.7.4 Afternoon 5:8:6

Reset Time:

Time Zone: UTC+8

□ Sync with Internet Time Server

□ Sync with Internet Time Server via Management Port

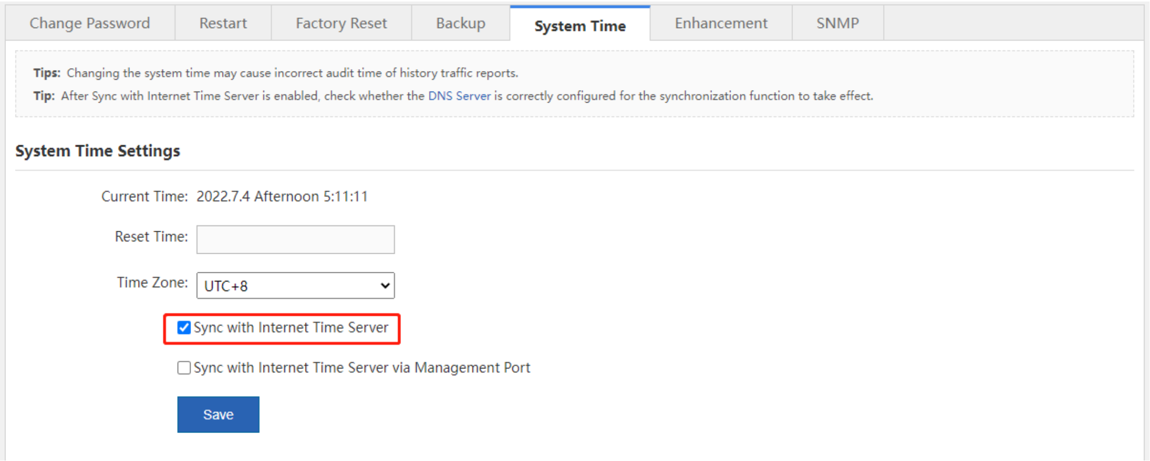
b Set **Time Zone** and click **Save**.

(3) Synchronize the time from the time server.

a Select **Sync with Internet Time Server** or **Sync with Internet Time Server via Management Port**.

Note

- When the device is in bridge or router mode and can be connected to the extranet only through the management port, **Sync with Internet Time Server via Management Port** must be selected.
- When the server that comes with the system is configured as the time server, no additional DNS configuration is required.



Tips: Changing the system time may cause incorrect audit time of history traffic reports.
Tip: After Sync with Internet Time Server is enabled, check whether the DNS Server is correctly configured for the synchronization function to take effect.

System Time Settings

Current Time: 2022.7.4 Afternoon 5:11:11

Reset Time:

Time Zone: UTC+8

☑ Sync with Internet Time Server

□ Sync with Internet Time Server via Management Port

b Set **Time Zone** and click **Save**.

9.1.6 Enhancement

This page provides multiple function configuration entries in a centralized manner, and the individual functions do not affect each other.

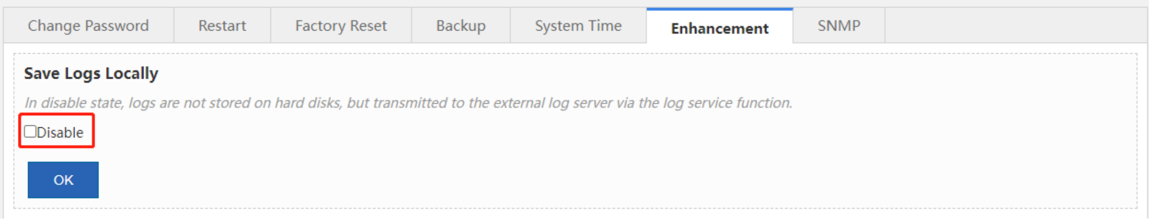
- **Save Logs Locally**: In the disabled state, logs are not stored on hard disks, but transmitted to the external log server via the log service function.
- **Prompt Upon Blocked Access**: sets the prompt displayed when users access a blacklisted website. For example, if you choose **Behavior** > **Behavior Policy** > **Website Blacklist/Whitelist** and specify **www.***xxx***.com** as the blacklisted website, this prompt is displayed when users access this website.
- **Traffic Audit Data Refresh Interval**: sets the period for the device to generate traffic audit data in real time.
- **Web Login Timeout**: sets the login timeout interval. The default timeout interval is 60 minutes, that is, you will be forced to log out of the system if you perform no web operation within 60 minutes upon login.
- **Device Name**: sets the device name. After changing the device name, you can choose **Home** > **Dashboard** and check the updated device name.

Procedure

(1) Choose **Advanced** > **System** > **Enhancement**.

(2) Set one or more of the following functions as required:

- **Save Logs Locally**: Deselect **Disable** and click **OK**. You need to restart the device for the configuration to take effect.

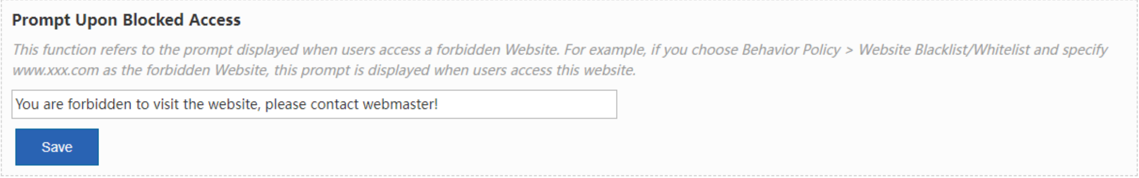


Save Logs Locally

In disable state, logs are not stored on hard disks, but transmitted to the external log server via the log service function.

☐Disable

- **Prompt Upon Blocked Access**: Enter the prompt and click **Save**.

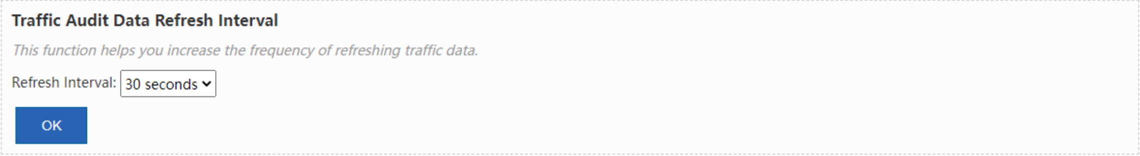


Prompt Upon Blocked Access

This function refers to the prompt displayed when users access a forbidden Website. For example, if you choose Behavior Policy > Website Blacklist/Whitelist and specify www.xxx.com as the forbidden Website, this prompt is displayed when users access this website.

You are forbidden to visit the website, please contact webmaster!

- Traffic Audit Data Refresh Interval: Set Refresh Interval and click OK.

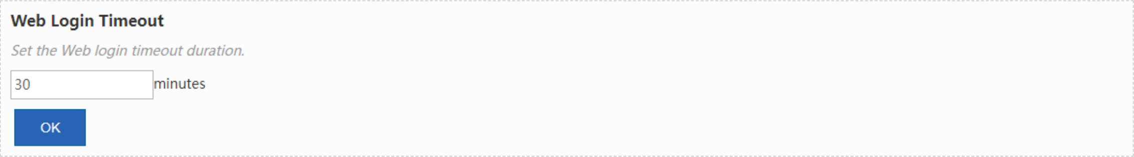


Traffic Audit Data Refresh Interval

This function helps you increase the frequency of refreshing traffic data.

Refresh Interval: 30 seconds

- **Web Login Timeout**: Enter the interval and click **OK**. The configuration takes effect immediately.



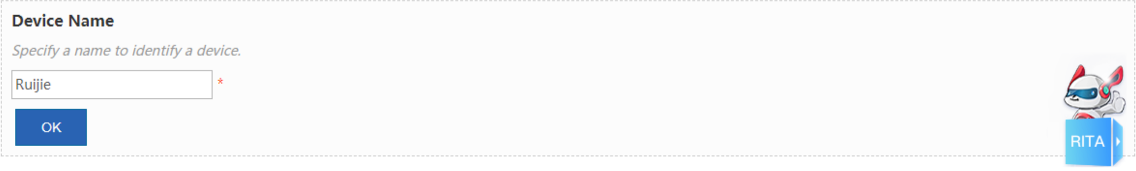
Web Login Timeout

Set the Web login timeout duration.

30 minutes

OK

- **Device Name**: Enter the name and click **OK**. The configuration takes effect immediately.



Device Name

Specify a name to identify a device.

Ruijie *

OK

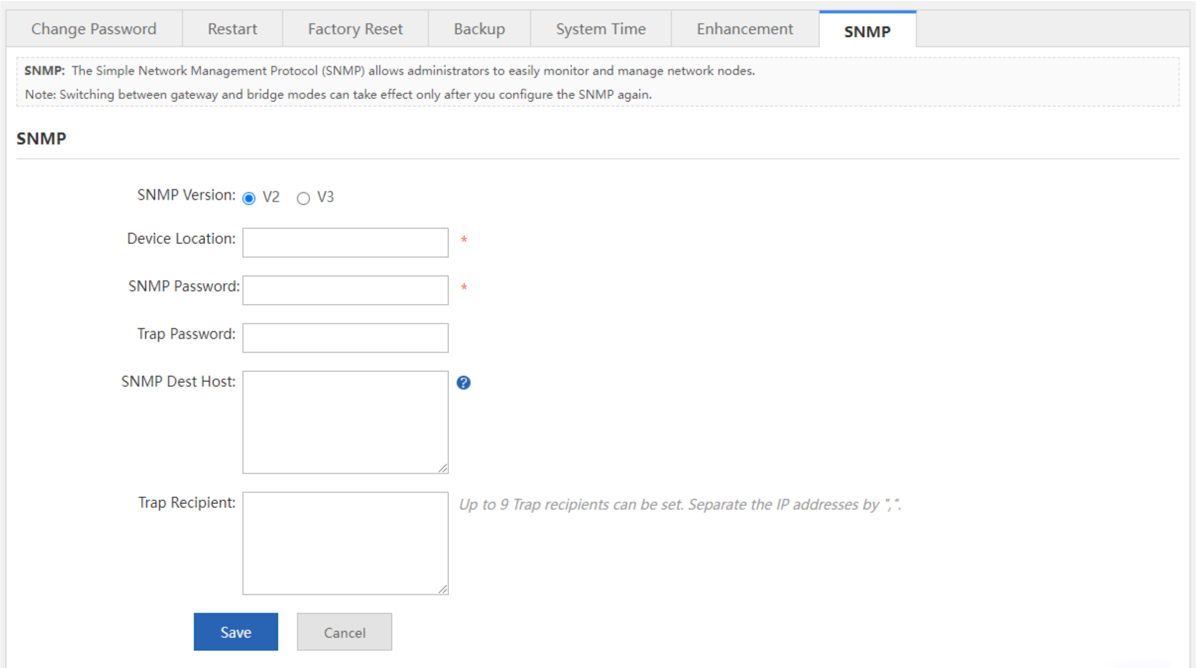
9.1.7 SNMP

Simple Network Management Protocol (SNMP) allows the administrators to perform information query, network configuration, fault locating, and capacity planning for nodes on the network for easy management.

Procedure

(1) Choose **Advanced** > **System** > **SNMP**.

(2) Set the SNMP configuration items and click **Save**.



SNMP: The Simple Network Management Protocol (SNMP) allows administrators to easily monitor and manage network nodes.

Note: Switching between gateway and bridge modes can take effect only after you configure the SNMP again.

SNMP

SNMP Version: ● V2 ○ V3

Device Location: *

SNMP Password: *

Trap Password:

SNMP Dest Host:

Trap Recipient: *Up to 9 Trap recipients can be set. Separate the IP addresses by ",".*

Configuration Item	Description
SNMP Version	Currently, the options are **V2** and **V3**. If it is set to **V3**, the encryption password and authentication password of the SNMP user are required for enhanced security.

Configuration Item	Description
Device Location	Name used to identify your SNMP service.
SNMP Password	Password used by the management host for connection to the current device.
Trap Password	Password for connection to the management host. In case of an alarm, the device will also send alarm information to the management host proactively.
SNMP Dest Host	The inform message of the SNMP destination host requires support from the server. If a Ruijie ePortal server is used during association, enter the IP address of the ePortal server. Use commas (,) to separate multiple IP addresses.
Trap Recipient	IP address of the management host that receives device alarm information. Use commas (,) to separate multiple IP addresses.

9.2 Upgrade

Upgrade: performs upgrade to the new versions of the system software, web package, and signature database. You can update the corresponding version as required. The upgrade takes about 50s. Do not close or refresh this page before a prompt indicating successful upgrade is displayed. Otherwise, the upgrade may fail.

Prerequisites

An available DNS server has been configured before the functions, such as online upgrade and automatic update, are used.

Procedure

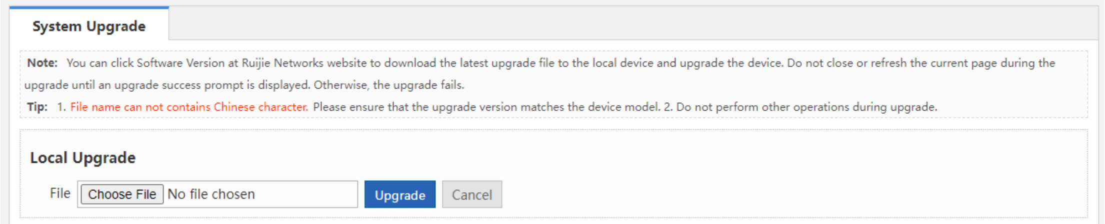
(1) Choose Advanced > Upgrade.

(2) Set one or more of the following items according to the actual requirements:

- **Local Upgrade:**

  You can download the latest upgrade file from the Ruijie Networks official website to the local device for device software version upgrade.

  Click **Choose File**, select the upgrade file, and click **Upgrade**. The upgrade takes about 50s. Do not perform any operations during upgrade. After a prompt indicating successful upgrade is displayed, click **OK**.



System Upgrade

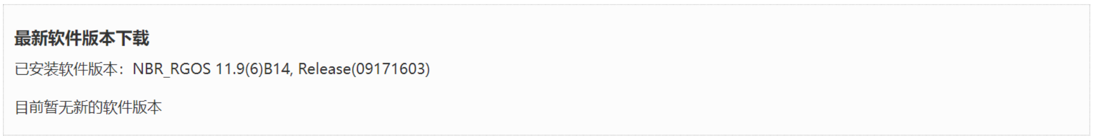
Note: You can click Software Version at Ruijie Networks website to download the latest upgrade file to the local device and upgrade the device. Do not close or refresh the current page during the upgrade until an upgrade success prompt is displayed. Otherwise, the upgrade fails.

Tip: 1. File name can not contains Chinese character. Please ensure that the upgrade version matches the device model. 2. Do not perform other operations during upgrade.

Local Upgrade

File: No file chosen

- **Latest Software Version**: If a new version is available, a message is displayed, prompting you to perform upgrade. In this case, click **Upgrade**.

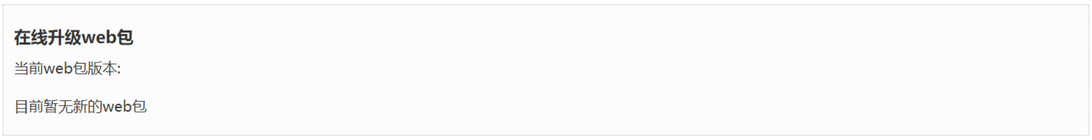


最新软件版本下载

已安装软件版本：NBR_RGOS 11.9(6)B14, Release(09171603)

目前暂无新的软件版本

- **Online Upgrade Web Package**: If a new version is available, a message is displayed, prompting you to perform upgrade. In this case, click **Upgrade**.

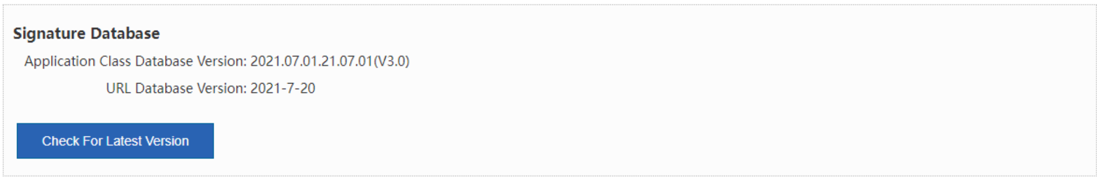


在线升级web包

当前web包版本:

目前暂无新的web包

- **Check For Latest Version**: displays the version of the current device. Click **Check For Latest Version**. The system automatically checks for the latest version released. If the current device is not of the latest version, **Upgrade** is displayed. Click this button. The **Application Class Database Version** and **URL Database Version** files are automatically downloaded to the device for upgrade.



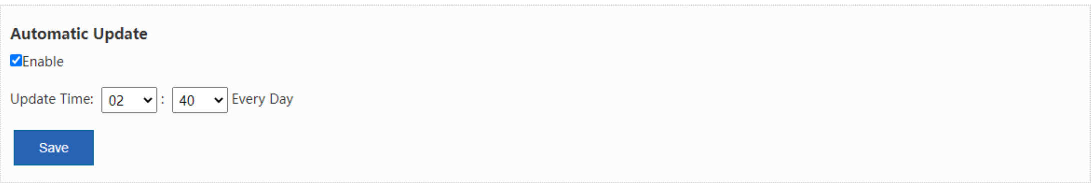
Signature Database

Application Class Database Version: 2021.07.01.21.07.01(V3.0)

URL Database Version: 2021-7-20

- **Automatic Update**: specifies the time for the system to check for the latest software and signature database versions and perform automatic update.

Select **Enable**, set **Update Time**, and click **Save**.



Automatic Update

☑Enable

Update Time: 02 : 40 Every Day

9.3 Administrator

Administrator: used for device administrator adding. You can log in to the device on the web page for daily maintenance or management, but cannot log in to the device using Telnet for command running as the administrator.

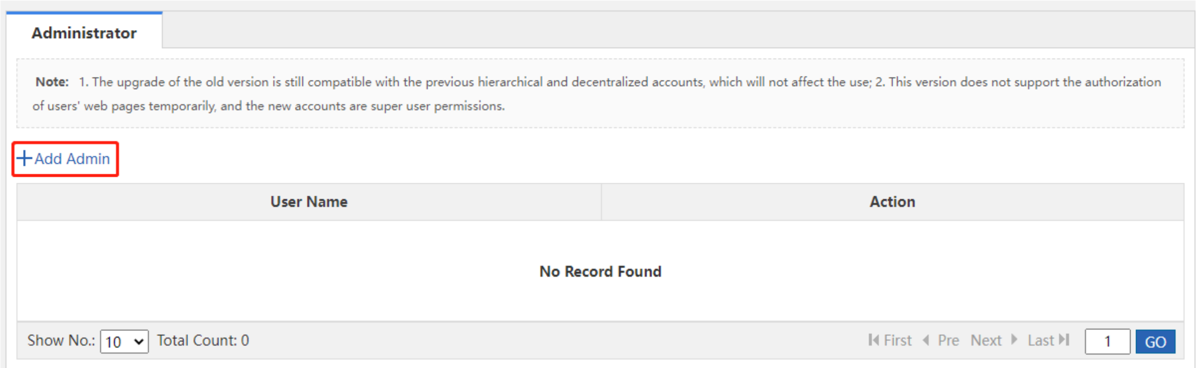
Caution

You can view and edit this page only as the **admin** user.

Procedure

(1) Choose **Advanced** > **Administrator**.

(2) Click **Add Admin**. The **Add Admin** window is displayed.

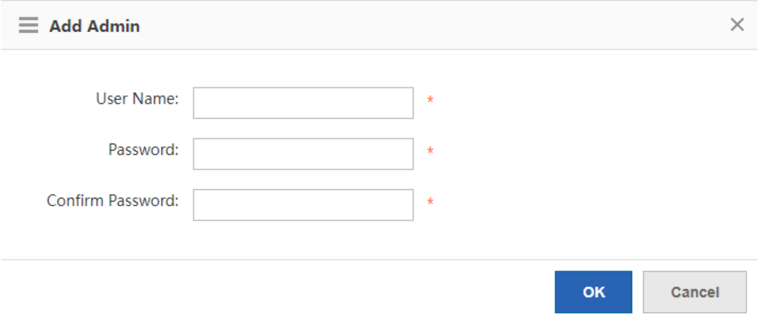


Note: 1. The upgrade of the old version is still compatible with the previous hierarchical and decentralized accounts, which will not affect the use; 2. This version does not support the authorization of users' web pages temporarily, and the new accounts are super user permissions.

User Name	Action
No Record Found	

Show No.: 10 Total Count: 0

(3) Set User Name, Password, and Confirm Password, and click **OK**.



User Name: *

Password: *

Confirm Password: *

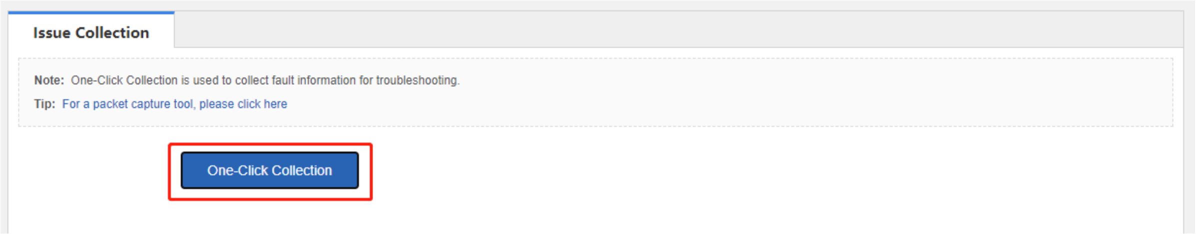
9.4 One-Click Collection

One-Click Collection: collects fault information about the device for troubleshooting.

Procedure

(1) Choose **Advanced** > **Issue Collection**.

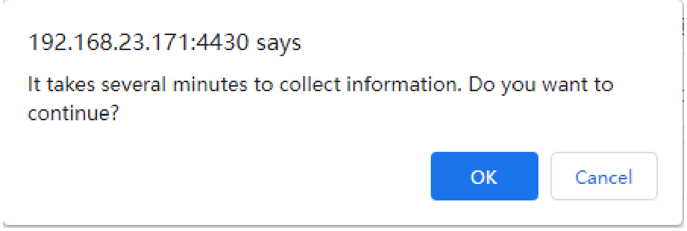
(2) Click **One-Click Collection**.



Note: One-Click Collection is used to collect fault information for troubleshooting.

Tip: For a packet capture tool, please click here

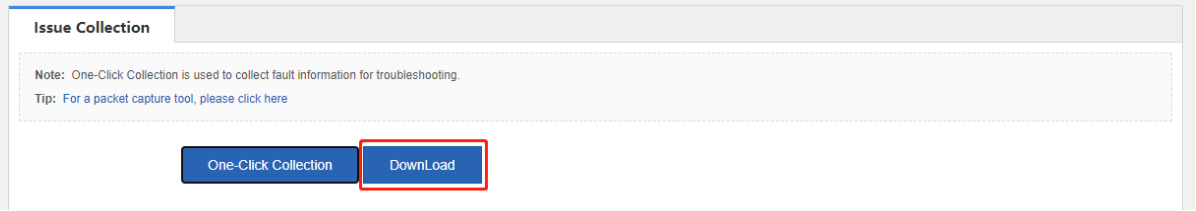
(3) In the displayed prompt window shown in the following figure, click **OK**.



192.168.23.171:4430 says

It takes several minutes to collect information. Do you want to continue?

(4) After the collection is completed, click **Download**. The generated package is downloaded, which facilitates engineers' fault analysis.



Note: One-Click Collection is used to collect fault information for troubleshooting.

Tip: For a packet capture tool, please click here

9.5 Connectivity Detection

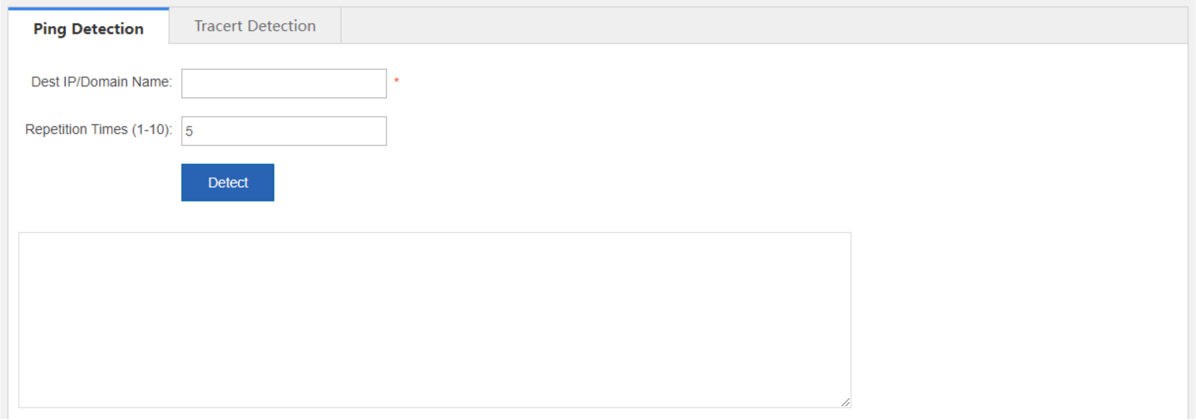
9.5.1 Ping Detection

Ping Detection: tests the network connectivity between the current device and the destination IP address/domain name.

Procedure

(1) Choose **Advanced** > **Connectivity Detection** > **Ping Detection**.

(2) Set **Dest IP/Domain Name** and **Repetition Times (1-10)**, and click **Detect**.



Dest IP/Domain Name: *

Repetition Times (1-10): 5

(3) Check the detection result. After the detection is completed, the detection result is displayed at the bottom of the page.

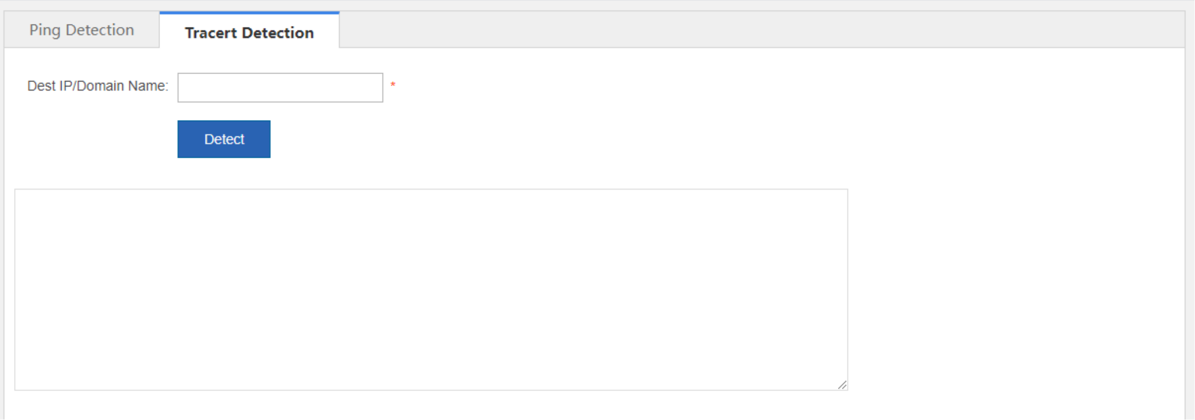
9.5.2 Tracert Detection

Tracert Detection: views the network path traversed by this device to the destination IP address or domain name.

Procedure

(1) Choose **Advanced** > **Connectivity Detection** > **Tracert Detection**.

(2) Set **Dest IP/Domain Name** and click **Detect**.



Dest IP/Domain Name: *

9.6 Central Management

Systems such as Ruijie Remote Auto-management Center (RAC) and Ruijie Cloud can be used to manage NBR series router device in a centralized manner and monitor the device performance, VPN, traffic, and service conditions on a global basis, significantly improving web management efficiency.

Application Scenario

It is applicable to enterprises with headquarters and branches, and chain hotels where simultaneous management of multiple router devices is required.

Prerequisites

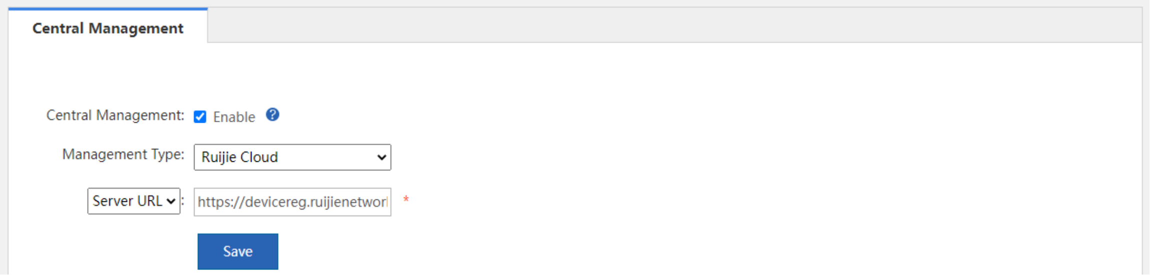
Ruijie RAC or Ruijie Cloud has been deployed, with related configurations completed on Ruijie RAC or Ruijie Cloud platform.

Procedure

(1) Choose **Advanced** > **Central Management**.

(2) Set **Central Management** to **Enable**, set **Management Type**, and set connection parameters.

- When **Management Type** is set to **Ruijie Cloud**, set the parameter shown in the following figure.

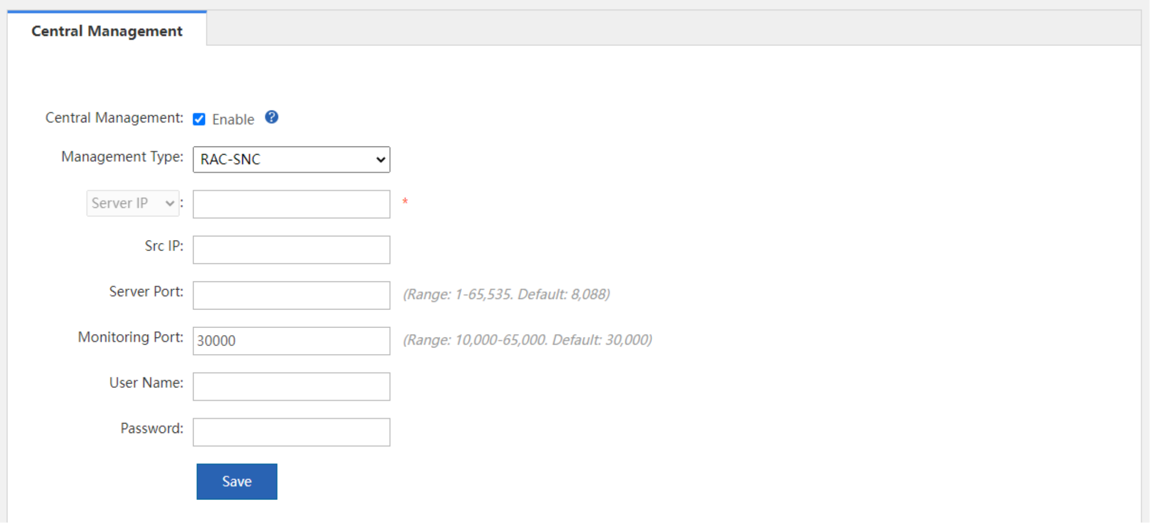


Central Management: ☑ Enable

Management Type: Ruijie Cloud

Server URL: https://devicereg.ruijienetwor *

- When **Management Type** is set to **RAC-SNC**, set the parameters shown in the following figure.



Central Management

Central Management: ☑ Enable

Management Type: RAC-SNC

Server IP: *

Src IP:

Server Port: (Range: 1-65,535. Default: 8,088)

Monitoring Port: 30000 (Range: 10,000-65,000. Default: 30,000)

User Name:

Password:

(3) Click **Save**.

9.7 Screen Mirroring

Note

- The NBR6205-E, NBR6210-E and NBR6215-E enterprise-class routers support the screen mirroring feature.
- The NBR6120-E enterprise-class router does not support the screen mirroring feature.

Screen mirroring allows you to mirror your smartphone to the TV screen. In the hotel industry, almost every room in every hotel is equipped with a TV. Usually, the televisions and clients in a hotel are in the same local area network, which may cause wrong or random casting of the TV screens. The television in the hotel will bring the customer a bad experience if it only serves as a decoration.

The screen mirroring feature supported by RG-NBR series routers can address the above problem. As a mirroring proxy, the router can bind the client to the TV in different LANs through isolating the networks of the client and the TV to implement one-to-one screen mirroring in the hotel.

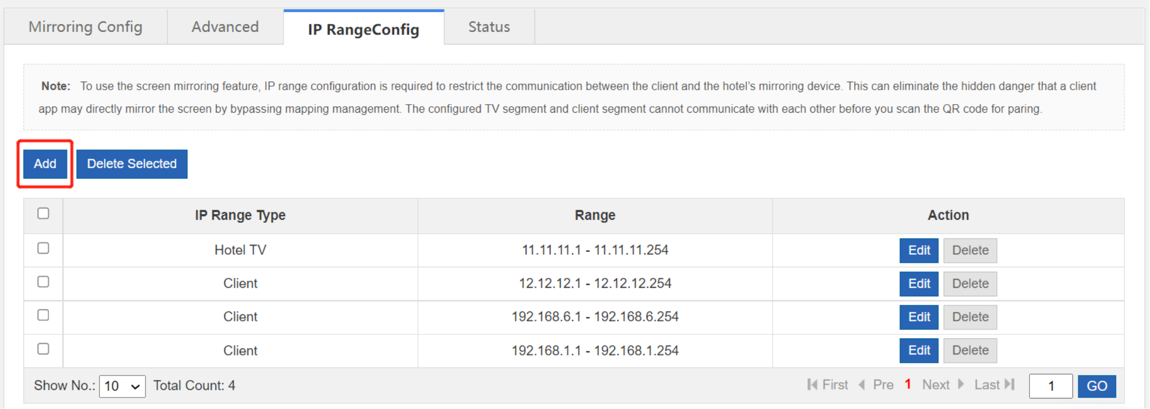
Application Scenario

The screen mirroring feature is designed for the hotel scenario. This feature can work in some simple inter-VLAN topologies.

Procedure

(1) Configure the IP range.

a Choose **Advanced** > **Mirroring Service** > **IP RangeConfig**.

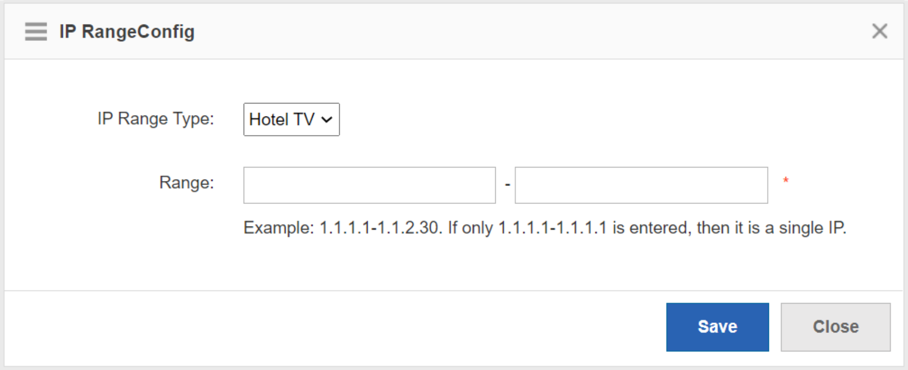


Note: To use the screen mirroring feature, IP range configuration is required to restrict the communication between the client and the hotel's mirroring device. This can eliminate the hidden danger that a client app may directly mirror the screen by bypassing mapping management. The configured TV segment and client segment cannot communicate with each other before you scan the QR code for paring.

□	IP Range Type	Range	Action
□	Hotel TV	11.11.11.1 - 11.11.11.254	Edit Delete
□	Client	12.12.12.1 - 12.12.12.254	Edit Delete
□	Client	192.168.6.1 - 192.168.6.254	Edit Delete
□	Client	192.168.1.1 - 192.168.1.254	Edit Delete

Show No.: 10 Total Count: 4 First Pre 1 Next Last 1 GO

b Click **Add** to configure the isolation segment and set the hotel TV segment.



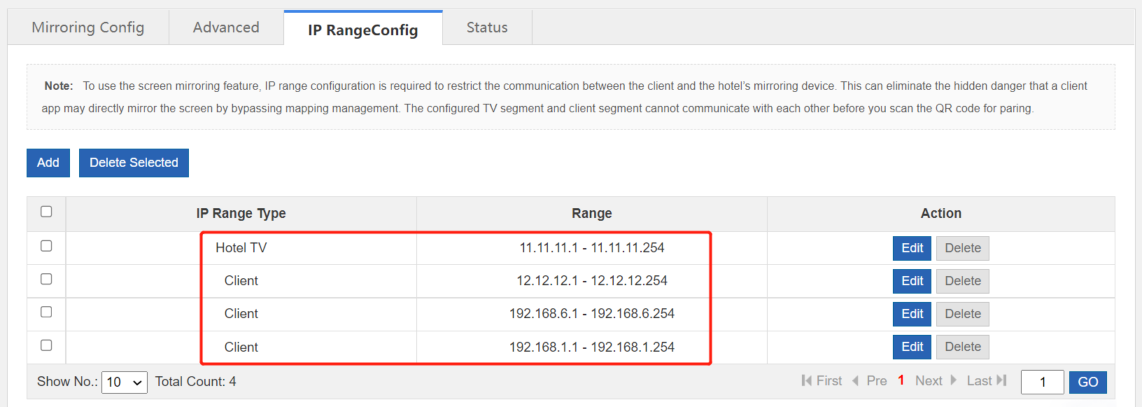
IP Range Type: Hotel TV

Range: ___ - ___ *

Example: 1.1.1.1-1.1.2.30. If only 1.1.1.1-1.1.1.1 is entered, then it is a single IP.

c Click **Save**.

d Set the client segment in the same way. The following page displays the configuration. (The figure is only an example.)



Note: To use the screen mirroring feature, IP range configuration is required to restrict the communication between the client and the hotel's mirroring device. This can eliminate the hidden danger that a client app may directly mirror the screen by bypassing mapping management. The configured TV segment and client segment cannot communicate with each other before you scan the QR code for paring.

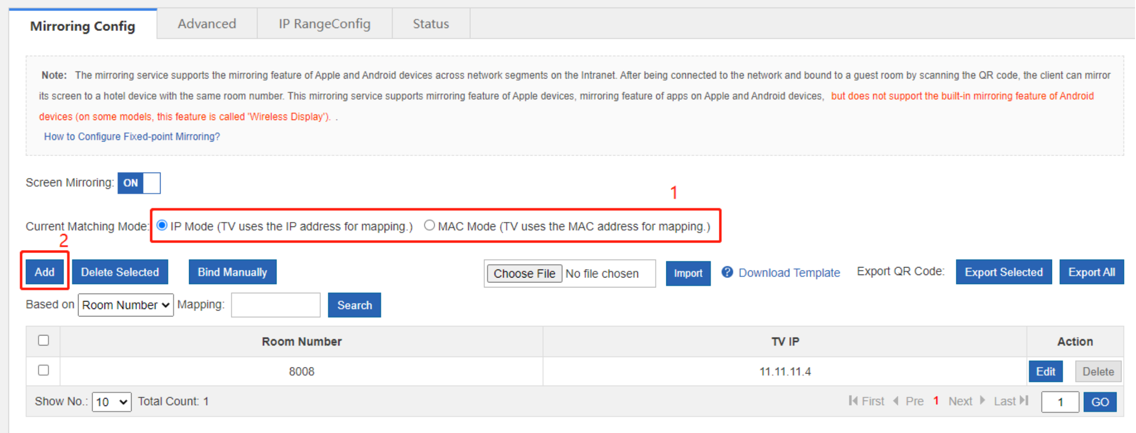
□	IP Range Type	Range	Action
□	Hotel TV	11.11.11.1 - 11.11.11.254	Edit Delete
□	Client	12.12.12.1 - 12.12.12.254	Edit Delete
□	Client	192.168.6.1 - 192.168.6.254	Edit Delete
□	Client	192.168.1.1 - 192.168.1.254	Edit Delete

Show No.: 10 Total Count: 4 First Pre 1 Next Last 1 GO

(2) Configure screen mirroring.

a Choose **Advanced** > **Mirroring Service** > **Mirroring Config**.

b Click to enable the screen mirroring feature and keep it **ON**.



Note: The mirroring service supports the mirroring feature of Apple and Android devices across network segments on the Intranet. After being connected to the network and bound to a guest room by scanning the QR code, the client can mirror its screen to a hotel device with the same room number. This mirroring service supports mirroring feature of Apple devices, mirroring feature of apps on Apple and Android devices, but does not support the built-in mirroring feature of Android devices (on some models, this feature is called 'Wireless Display'). .

How to Configure Fixed-point Mirroring?

Screen Mirroring: ON

Current Matching Mode: ● IP Mode (TV uses the IP address for mapping.) ○ MAC Mode (TV uses the MAC address for mapping.)

No file chosen

Export QR Code:

Based on Room Number Mapping:

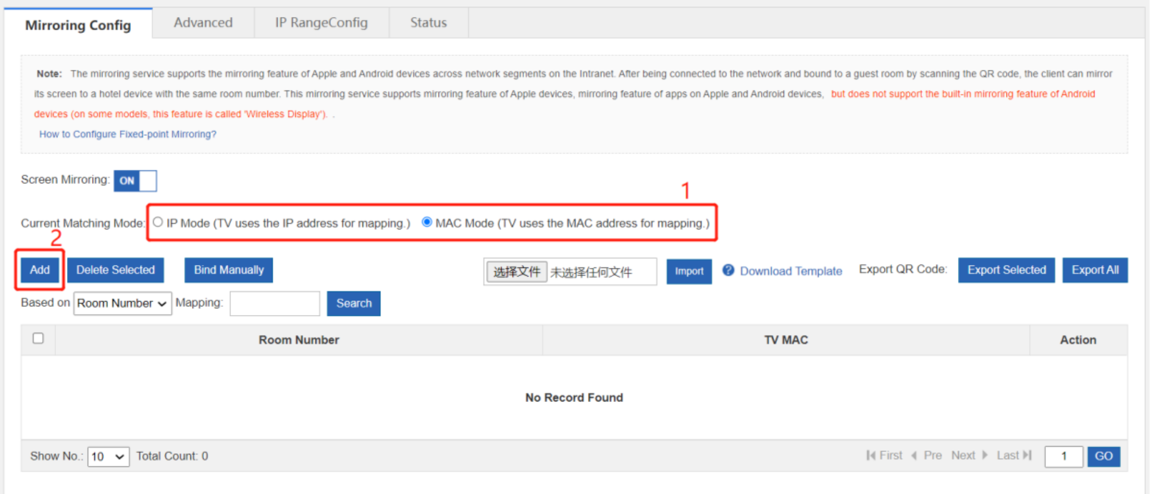
□	Room Number	TV IP	Action
□	8008	11.11.11.4	Edit Delete

Show No.: 10 Total Count: 1 1 1

c Select the matching mode as required. Click **Add** to bind the room number to the TV IP address or MAC address.

Note

- If you switch the matching mode, the existing configuration will be cleared. Please proceed with caution.
- A room number is bound to only one IP address or MAC address.



Note: The mirroring service supports the mirroring feature of Apple and Android devices across network segments on the Intranet. After being connected to the network and bound to a guest room by scanning the QR code, the client can mirror its screen to a hotel device with the same room number. This mirroring service supports mirroring feature of Apple devices, mirroring feature of apps on Apple and Android devices, but does not support the built-in mirroring feature of Android devices (on some models, this feature is called 'Wireless Display'). .

How to Configure Fixed-point Mirroring?

Screen Mirroring: ON

Current Matching Mode: ○ IP Mode (TV uses the IP address for mapping.) ● MAC Mode (TV uses the MAC address for mapping.)

未选择任何文件

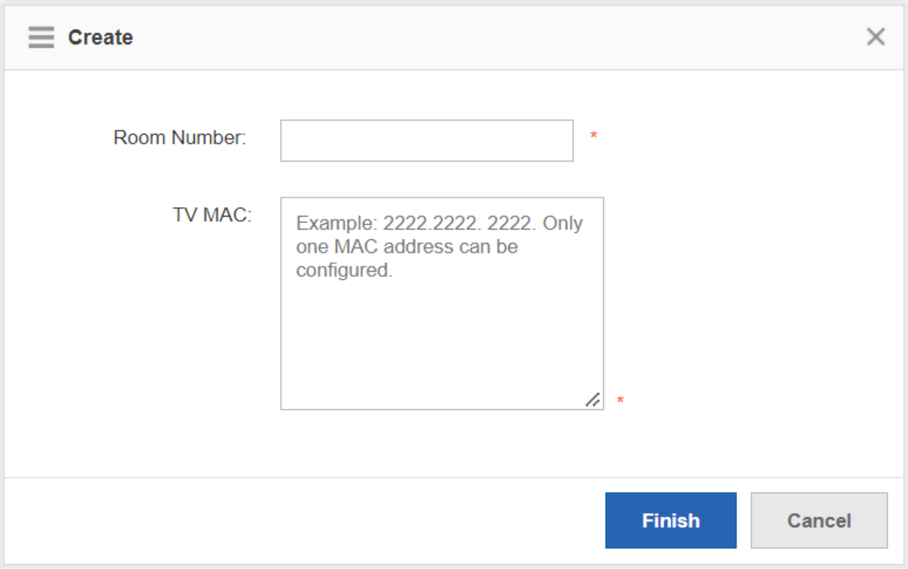
Export QR Code:

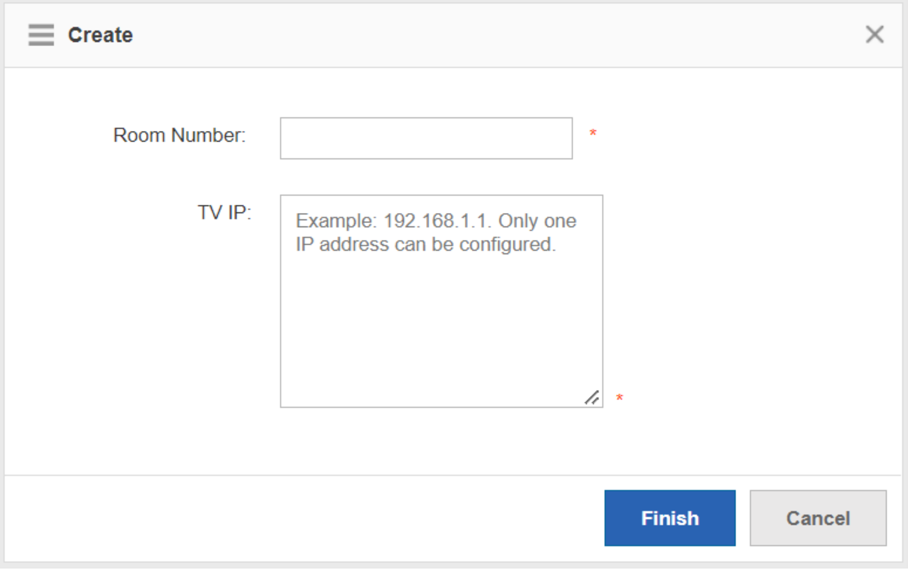
Based on Room Number Mapping:

□	Room Number	TV MAC	Action
No Record Found			

Show No.: 10 Total Count: 0 1

d Click **Finish**.


Create
Room Number: *
TV MAC: *
Example: 2222.2222. 2222. Only one MAC address can be configured.
Finish
Cancel


Create
Room Number: *
TV IP: *
Example: 192.168.1.1. Only one IP address can be configured.
Finish
Cancel

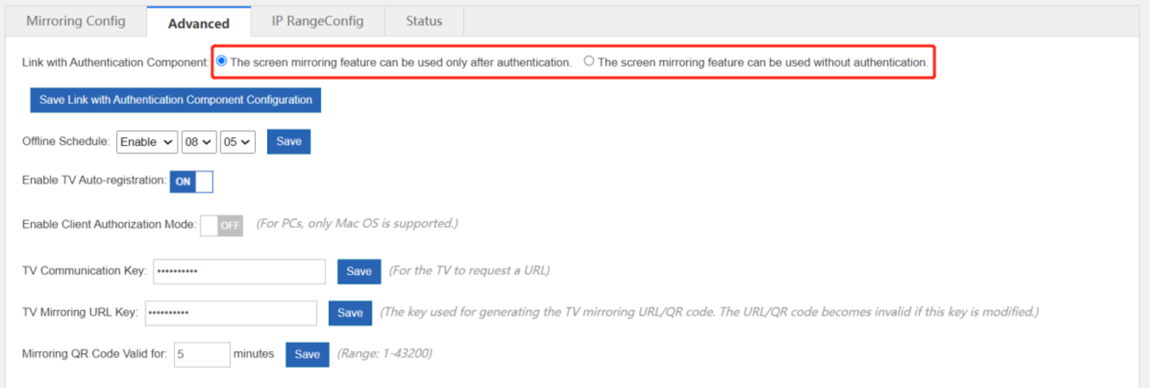
(3) (Optional) Configure advanced settings.

a Choose **Advanced** > **Mirroring Service** > **Advanced**.

b Choose to enable authentication for the screen mirroring feature and to enable other mirroring functions as required.

⚠ Caution

You must click **Save** after configuring each item. Otherwise the configuration will not take effect.



Link with Authentication Component: ● The screen mirroring feature can be used only after authentication. ○ The screen mirroring feature can be used without authentication.

Offline Schedule: Enable 08 05

Enable TV Auto-registration: ON

Enable Client Authorization Mode: OFF *(For PCs, only Mac OS is supported.)*

TV Communication Key: •••••••••• *(For the TV to request a URL)*

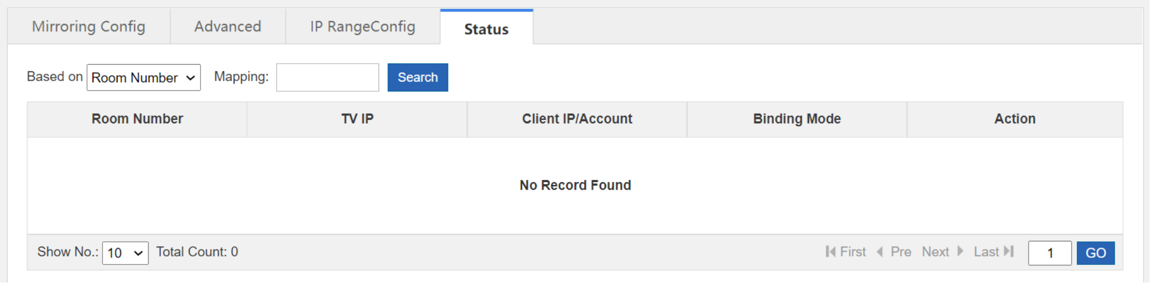
TV Mirroring URL Key: •••••••••• *(The key used for generating the TV mirroring URL/QR code. The URL/QR code becomes invalid if this key is modified.)*

Mirroring QR Code Valid for: 5 minutes *(Range: 1-43200)*

(4) (Optional) Display the mirroring status.

a Choose **Advanced** > **Mirroring Service** > **Status**.

b Display the mirroring status of every room. You can search for the screen mirroring data based on the room number, the TV IP, and the client IP or account.



Based on Room Number Mapping:

Room Number	TV IP	Client IP/Account	Binding Mode	Action
No Record Found				

Show No.: 10 Total Count: 0 1

9.8 VRRP

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant routing protocol. VRRP adds a group of router devices to a backup group called a virtual router, assigns a virtual IP address to the virtual router, and determines the router that functions as the master for forwarding based on the election mechanism. Hosts on the LAN only need to know the virtual IP address of this virtual router and set it as the IP address of the router to communicate with the extranet through this virtual router.

VRRP adopts the active/standby mode. Generally, the master is responsible for packet forwarding. If the master fails, a backup will take over the responsibility to ensure normal service traffic forwarding, which greatly enhances link reliability.

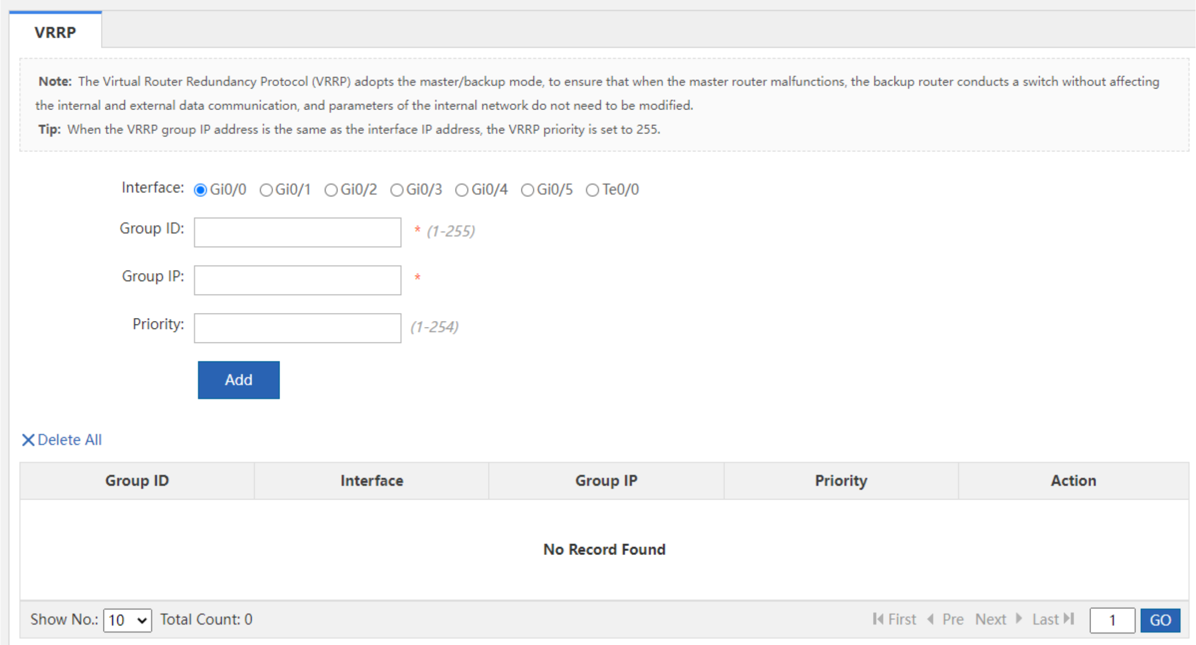
Note

- The NBR6205-E, NBR6210-E and NBR6215-E enterprise-class routers support the VRRP feature.
- The NBR6120-E enterprise-class router does not support the VRRP feature.

Procedure

(1) Choose **Advanced** > **VRRP** > **VRRP**.

(2) Set Group ID, Group IP, and Priority, and click Add.



VRRP

Note: The Virtual Router Redundancy Protocol (VRRP) adopts the master/backup mode, to ensure that when the master router malfunctions, the backup router conducts a switch without affecting the internal and external data communication, and parameters of the internal network do not need to be modified.

Tip: When the VRRP group IP address is the same as the interface IP address, the VRRP priority is set to 255.

Interface: ● Gi0/0 ○ Gi0/1 ○ Gi0/2 ○ Gi0/3 ○ Gi0/4 ○ Gi0/5 ○ Te0/0

Group ID: * (1-255)

Group IP: *

Priority: (1-254)

Group ID	Interface	Group IP	Priority	Action
No Record Found				

Show No.: 10 Total Count: 0

Configuration Item	Description
Interface	Enables VRRP at the specified interface.
Group ID	The value ranges from 1 to 255.
Group IP	IP address of the virtual router, which is used by the hosts on the LAN as the default router.
Priority	A greater value indicates higher priority. The backup group with higher priority will function as the master routing device for packet forwarding. VRRP groups with different priority levels have an active/standby relationship with each other.

(3) (Optional) You can add more VRRP groups as required.

9.9 System Log

9.9.1 Server Log

Server Log: sets Elog log system information. After device connection to the Elog log system, logs of specified types can be sent to the Elog log system.

Prerequisites

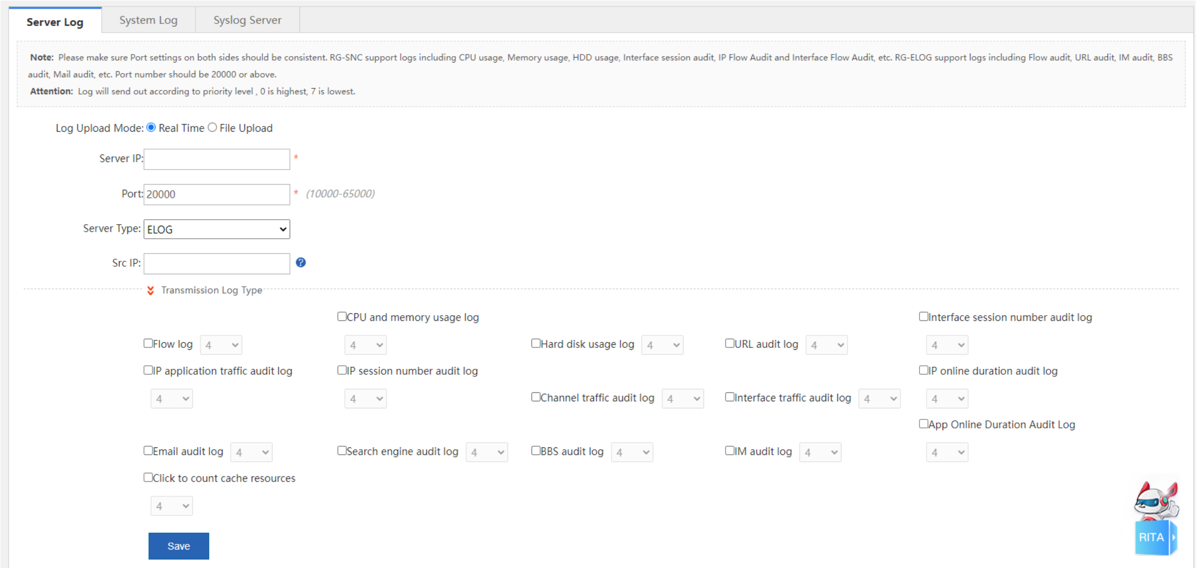
Network connectivity is available between the device and the Elog log system.

Server Log has been enabled on the page under **Home** > **Service**.

Procedure

(1) Choose **Advanced** > **System Log** > **Server Log**.

(2) Set Log Upload Mode, Server IP, and Port, and configure information under Transmission Log Type.



Note: Please make sure Port settings on both sides should be consistent. RG-SNC support logs including CPU usage, Memory usage, HDD usage, Interface session audit, IP Flow Audit and Interface Flow Audit, etc. RG-ELOG support logs including Flow audit, URL audit, IM audit, BBS audit, Mail audit, etc. Port number should be 20000 or above.

Attention: Log will send out according to priority level , 0 is highest, 7 is lowest.

Log Upload Mode: ● Real Time ○ File Upload

Server IP: *

Port: 20000 * (10000-65000)

Server Type: ELOG

Src IP:

Transmission Log Type

□CPU and memory usage log 4

□Interface session number audit log 4

□Flow log 4

□Hard disk usage log 4

□URL audit log 4

□IP application traffic audit log 4

□IP session number audit log 4

□IP online duration audit log 4

□Channel traffic audit log 4

□Interface traffic audit log 4

□App Online Duration Audit Log 4

□Email audit log 4

□Search engine audit log 4

□BBS audit log 4

□IM audit log 4

□Click to count cache resources 4

(3) Click **Save**.

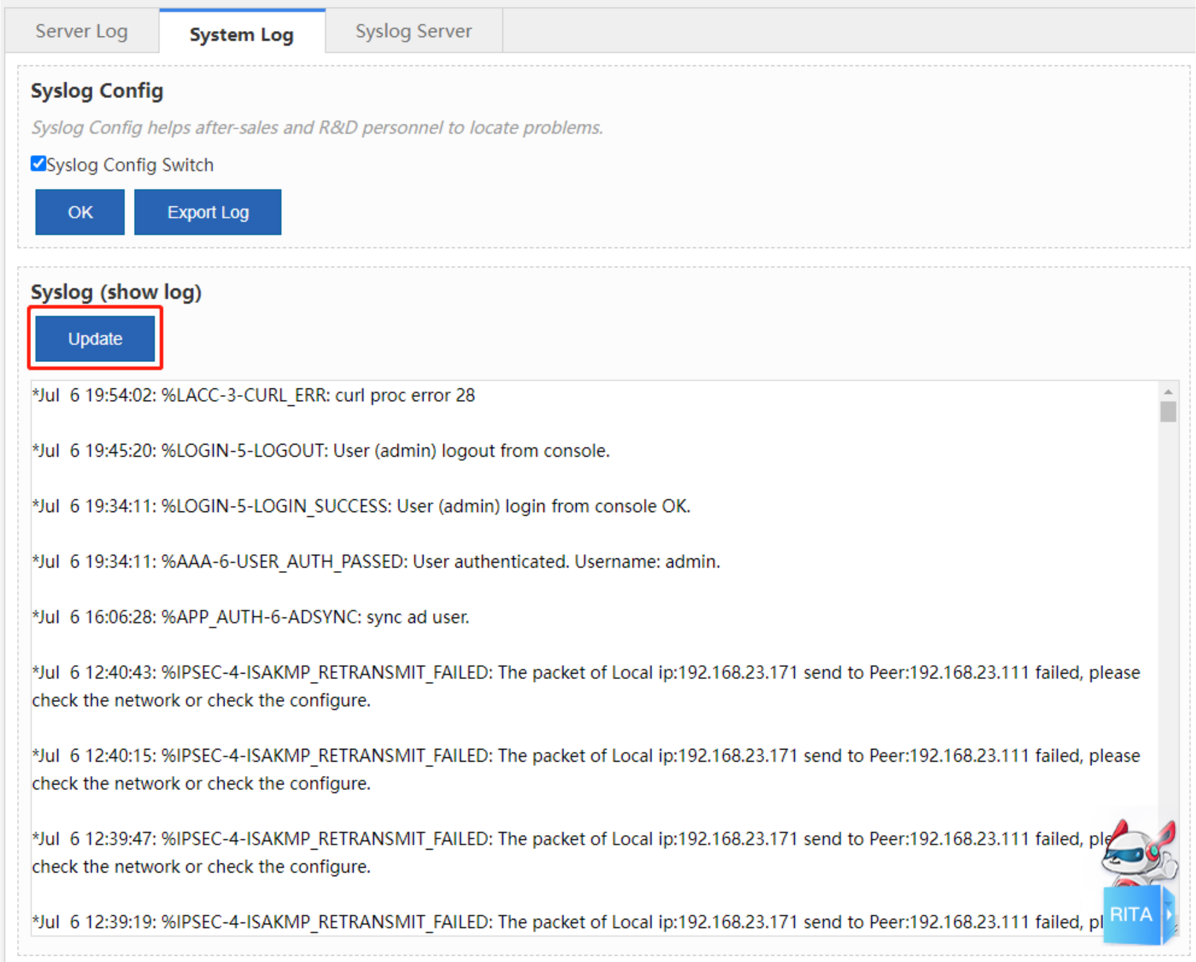
9.9.2 System Log

System Log: views and exports system logs.

Procedure

(1) Choose **Advanced** > **System Log** > **System Log**.

(2) Click **Update** to refresh log information, as shown in the following figure.



Syslog Config

Syslog Config helps after-sales and R&D personnel to locate problems.

☑Syslog Config Switch

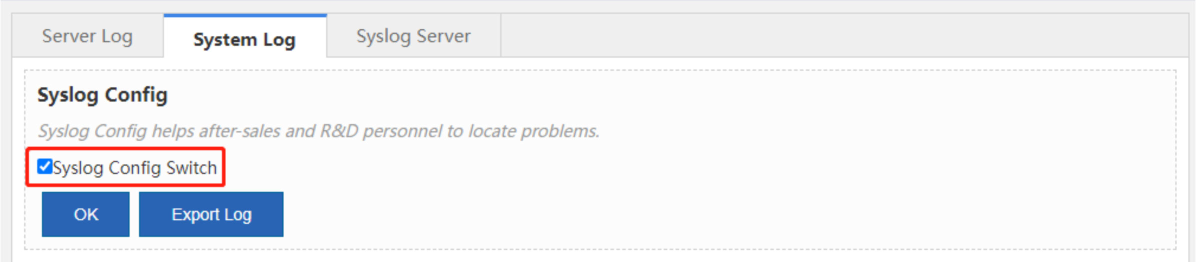
Syslog (show log)

```
*Jul  6 19:54:02: %LACC-3-CURL_ERR: curl proc error 28

*Jul  6 19:45:20: %LOGIN-5-LOGOUT: User (admin) logout from console.

*Jul  6 19:34:11: %LOGIN-5-LOGIN_SUCCESS: User (admin) login from console OK.

*Jul  6 19:34:11: %AAA-6-USER_AUTH_PASSED: User authenticated. Username: admin.

*Jul  6 16:06:28: %APP_AUTH-6-ADSYNC: sync ad user.

*Jul  6 12:40:43: %IPSEC-4-ISAKMP_RETRANSMIT_FAILED: The packet of Local ip:192.168.23.171 send to Peer:192.168.23.111 failed, please
check the network or check the configure.

*Jul  6 12:40:15: %IPSEC-4-ISAKMP_RETRANSMIT_FAILED: The packet of Local ip:192.168.23.171 send to Peer:192.168.23.111 failed, please
check the network or check the configure.

*Jul  6 12:39:47: %IPSEC-4-ISAKMP_RETRANSMIT_FAILED: The packet of Local ip:192.168.23.171 send to Peer:192.168.23.111 failed, ple
check the network or check the configure.

*Jul  6 12:39:19: %IPSEC-4-ISAKMP_RETRANSMIT_FAILED: The packet of Local ip:192.168.23.171 send to Peer:192.168.23.111 failed, pl
```

(3) Select **Syslog Config Switch** and click **OK**. Click **Export Log** to export system logs and download them to the local device.

⚠ Caution

This step is mandatory for log export.



Syslog Config

Syslog Config helps after-sales and R&D personnel to locate problems.

☑Syslog Config Switch

9.9.3 Syslog Server

Syslog Server: enables the device to send logs in Syslog format to the specified server periodically.

Prerequisites

Network connectivity is available between the device and the Syslog log server.

Configurations related to log receiving have been completed on the Syslog server.

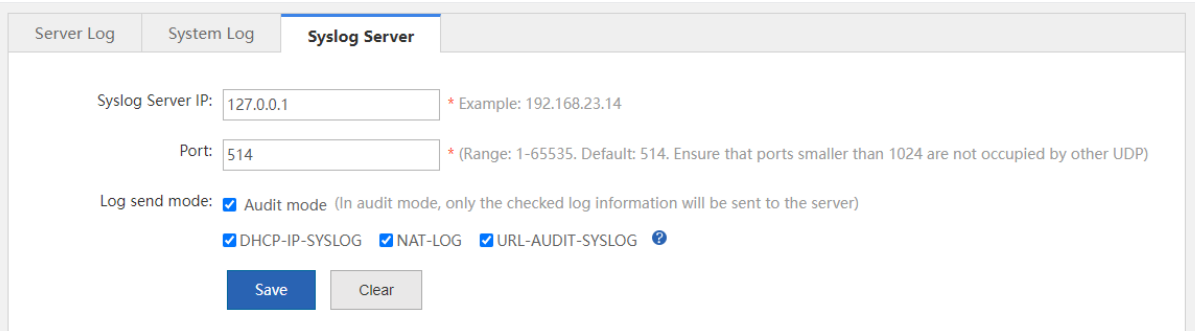
Procedure

(1) Choose **Advanced** > **System Log** > **Syslog Server**.

(2) Set Syslog Server IP, Port, and Log send mode, and click **Save**.

Note

If **Log send mode** is set, only the logs of the selected types are sent to the Syslog server. Otherwise, logs of all types are sent.



Syslog Server IP: 127.0.0.1 * Example: 192.168.23.14

Port: 514 * (Range: 1-65535. Default: 514. Ensure that ports smaller than 1024 are not occupied by other UDP)

Log send mode: ☑ Audit mode (In audit mode, only the checked log information will be sent to the server)

☑ DHCP-IP-SYSLOG ☑ NAT-LOG ☑ URL-AUDIT-SYSLOG

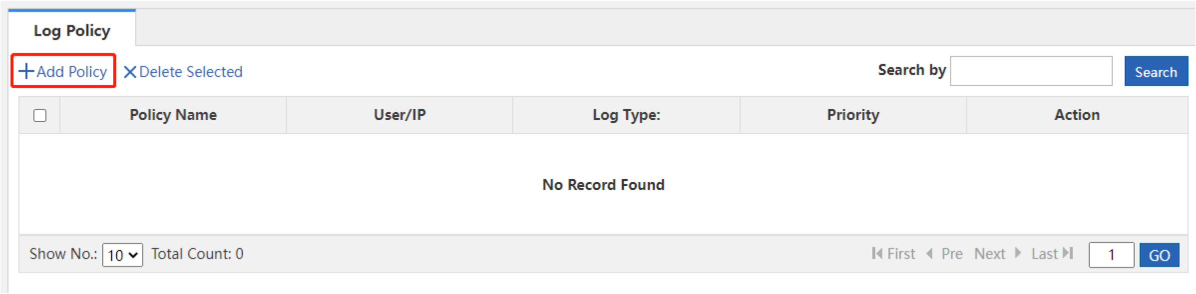
9.10 Log Policy

Log Policy: specifies whether to report the logs about users and IP addresses/IP segments to a third-party server or the Elog log system, and the log types for reporting.

Procedure

(1) Choose **Advanced** > **Log Policy**.

(2) Click **Add Policy**.



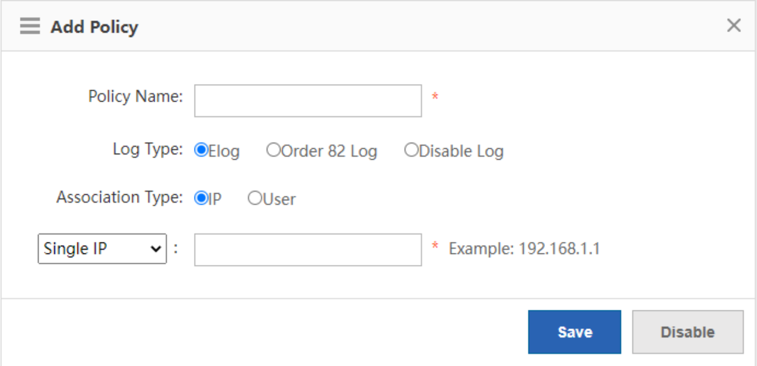
□	Policy Name	User/IP	Log Type:	Priority	Action
			No Record Found		

Show No.: 10 Total Count: 0

(3) In the **Add Policy** window, set **Policy Name**, **Log Type**, and **Associate Type** (options: **User** and **IP**), and corresponding information. Click **Save**.

Caution

- **Server Log** must be enabled on the page under **Home** > **Service** if you want to set **Log Type** to **Order 82 Log** or **Elog**.
- If you set **Log Type** to **Disable Log**, logs about the specified user or IP address are not sent.
- If you set **Log Type** to **Order 82 Log** or **Elog**, the logs of this type are sent to the Elog log system. For configuration about the Elog log system, see 9.9.1 Server Log.



Add Policy

Policy Name: *

Log Type: ● Elog ○ Order 82 Log ○ Disable Log

Association Type: ● IP ○ User

Single IP : * Example: 192.168.1.1

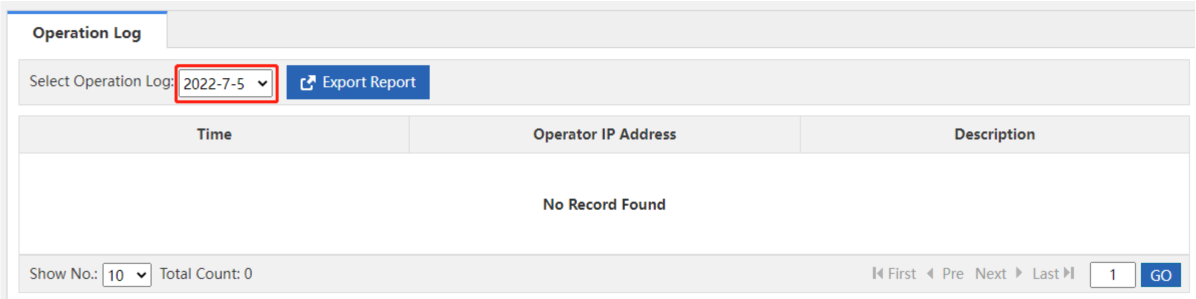
9.11 Operation Log

Operation Log: views device web operation logs. You can also export these logs in reports and view them on the local device.

Procedure

(1) Choose **Advanced** > **Report**.

(2) Set the query date. The web operation records on the specified date are displayed at the bottom of the page.



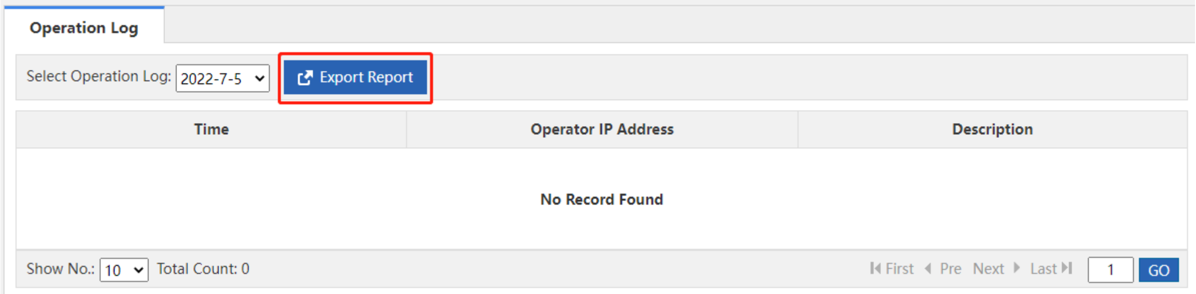
Operation Log

Select Operation Log: 2022-7-5

Time	Operator IP Address	Description
	No Record Found	

Show No.: 10 Total Count: 0

(3) Click **Export Report**. Web operation records are exported in reports and downloaded to the local device.



Operation Log

Select Operation Log: 2022-7-5

Time	Operator IP Address	Description
	No Record Found	

Show No.: 10 Total Count: 0