# Ruijie RG-EG Series Gateways

# Web-Based Configuration Guide, Release 11.9(1)B11S1

## Copyright Statement



## Exemption Statement

## Preface

Thank you for using our products.

## Audience

This manual is intended for:

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

## Obtaining Technical Assistance

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: http://caseportal.ruijienetworks.com
- Community: http://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: service_rj@ruijienetworks.com

## Related Documents

| Documents | Description |
| --- | --- |
| Command Reference | Describes the related configuration commands, including command modes, parameter descriptions, usage guides, and related examples. |
| Hardware Installation and Reference Guide | Describes the functional and physical features and provides the device installation steps, hardware troubleshooting, module technical specifications, and specifications and usage guidelines for cables and connectors. |

## Conventions

This manual uses the following conventions:

| Convention | Description |
| --- | --- |
| **boldface** font | Commands, command options, and keywords are in **boldface**. |
| *italic* font | Arguments for which you supply values are in *italics*. |
| [ ] | Elements in square brackets are optional. |
| { x \| y \| z } | Alternative keywords are grouped in braces and separated by vertical bars. |
| [ x \| y \| z ] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |

## Symbols

Means reader take note. Notes contain helpful suggestions or references.

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

# 1 Web-Based Configuration

## 1.1 Overview

This document describes how to use the Web management system. You can use the Web management system to manage the common functions of the EasyGate (EG) routers.

You can access the Web management system from a browser such as the Internet Explorer (IE) to manage EG gateways.

Currently, this document is applicable only to the EG gateway series.

## 1.2 Applications

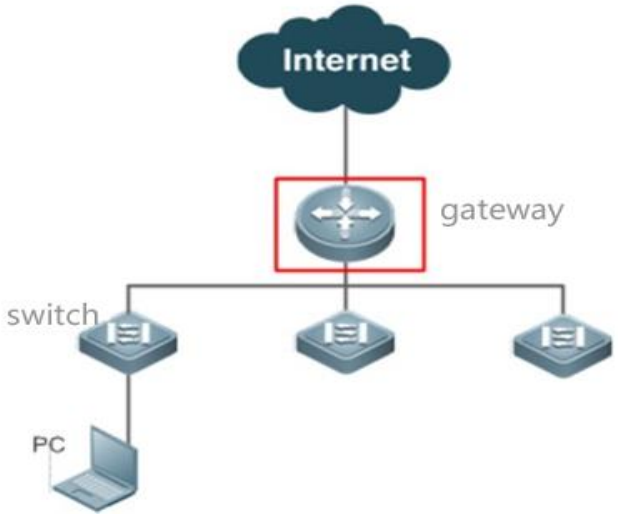
| Application | Description |
|---|---|
| Managing Devices via Web Management System | After EG devices are configured, you can access the Web management system from a browser. |

### 1.2.1 Managing Devices via Web Management System

#### Scenario

As shown in Figure 1-1, you can access the Web management system of the EG device from a PC browser to manage and configure the EG device.

Figure 1-1




| Remarks | The device enclosed in the red rectangle in the figure above is the EG gateway. Ensure that the EG gateway can be pinged successfully from the PC. Then, you can access the Web management system of the EG gateway. |
|---|---|

## Deployment

### Configuration Environment Requirements

Client requirements:

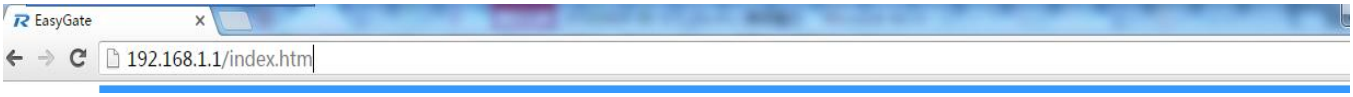
1. Network administrators can log in to the Web management UI from the browser of the Web management system client, to manage the EG gateway. Clients refer to PCs or other mobile terminals such as laptops.
2. Google Chrome, Firefox, IE8.0 and later versions, and some IE kernel-based browsers are supported. If you log in to the Web management system from an unsupported browser, exceptions such as garble and format error may occur.
3. It is recommended to set the resolution to 1024 x 768, 1280 x 1024, 1440 x 960, or 1600 x 900. If other resolutions are used, the page fonts and formats may not be aligned, the UI may not be artistic, or other exceptions may occur.

# 1.3 Web Management System

This section describes how to use the Web management UI. You can use the Web management UI to manage the common functions of the EG egress gateway.

## 1.3.1 Access to Web Management UI

Step 1: Enter the IP address of the LAN interface, WAN interface, or management interface of the EG router in the address bar of the browser. The IP address of your PC must be in the same network segment as the IP address of the EG device.




The default Web management address is http://192.168.1.1 when the device is reset or is used initially.

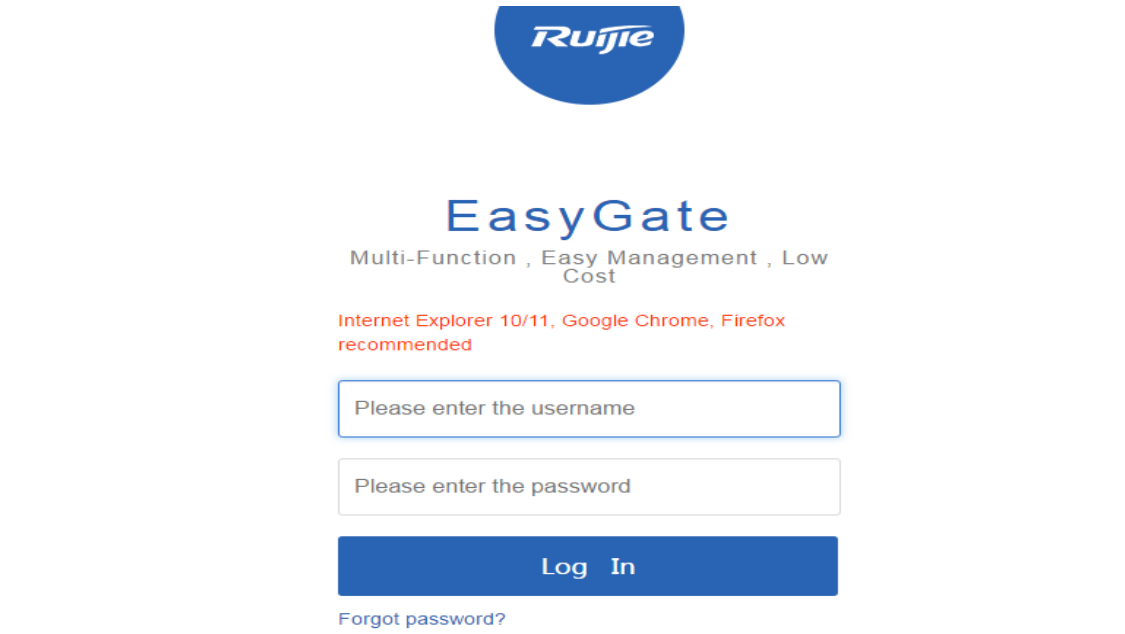
If the Hypertext Transfer Protocol Secure (HTTPS) protocol is used, the initial management address is https://192.168.1.1:4430.

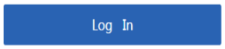
The default username and password are both **admin** when the device is reset or is used initially.

In gateway mode, the PC is connected to Port Gi0/0 of the device.

If a network failure (such as network cable disconnection or network interruption) occurs during login, the UI may be stuck for 1 or 2 minutes. The error cause is displayed about 2 minutes later.

Step 2: Access the system login UI, as shown in the figure below.



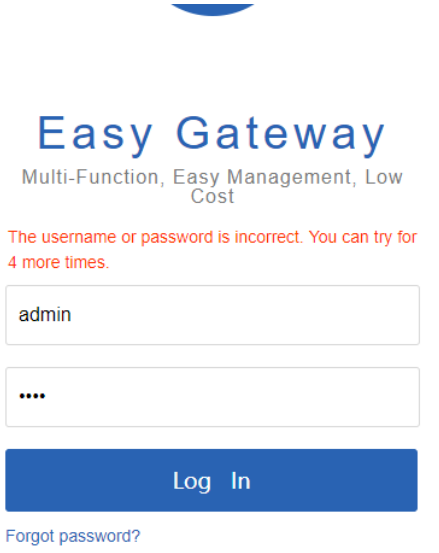

1. Enter the username and password and click 

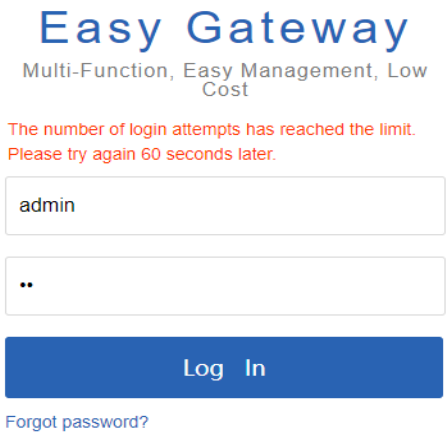
to access the main UI for device management.

2. If you forget the username or password, click Forgot password? .

3. If you need assistance from customer service personnel, click Online Service to contact a customer service representative online.

4. If you enter the wrong username or password for five consecutive times, your account will be locked for one minute.

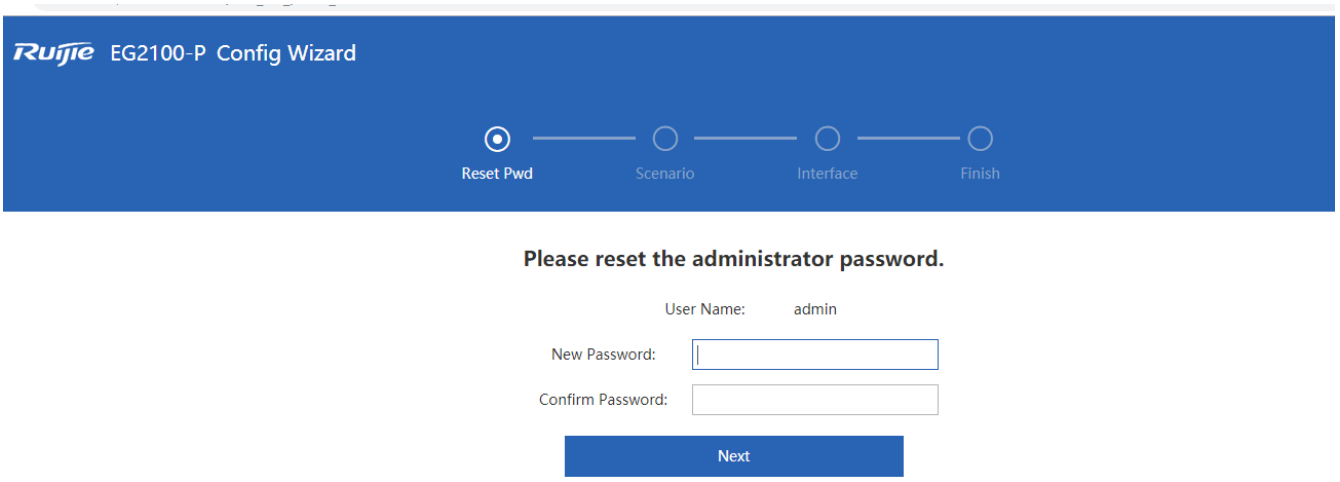



Before using the Web management system, you must check that the Web page upgrade package (the **web.gz** file) exists in the flash memory of the EG device. Otherwise, the management UI shown in the figure above will not be displayed. The file is installed on the device by default. If it is not installed, install it according to the upgrade file installation described in the manual.

### 1.3.2 Config Wizard

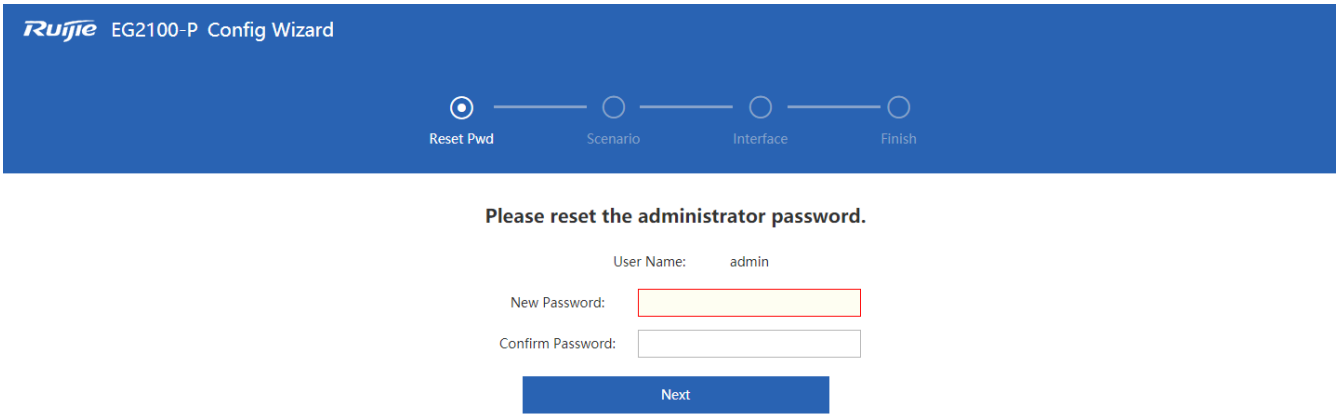
The EG device is not configured when you log in to the Web management UI for the first time. You will enter **Config Wizard** to reset the administrator password, select the scenario, enable smart flow control and configure WiFi.



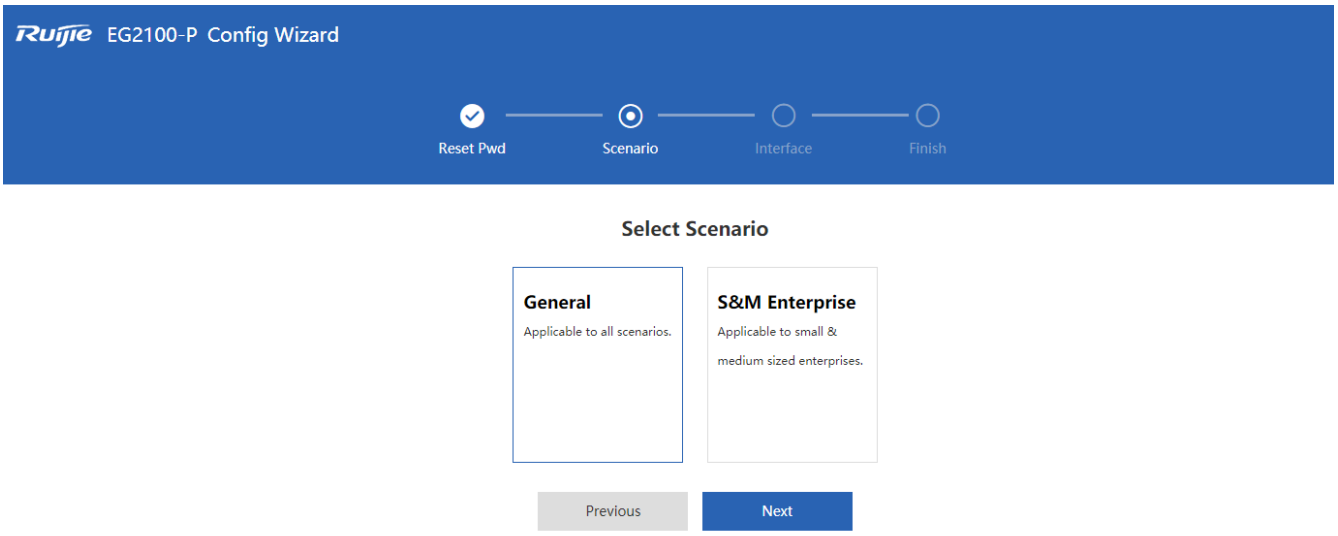

### 1.3.2.1 Quick Settings

The figure below shows the main UI of the config wizard in gateway mode.

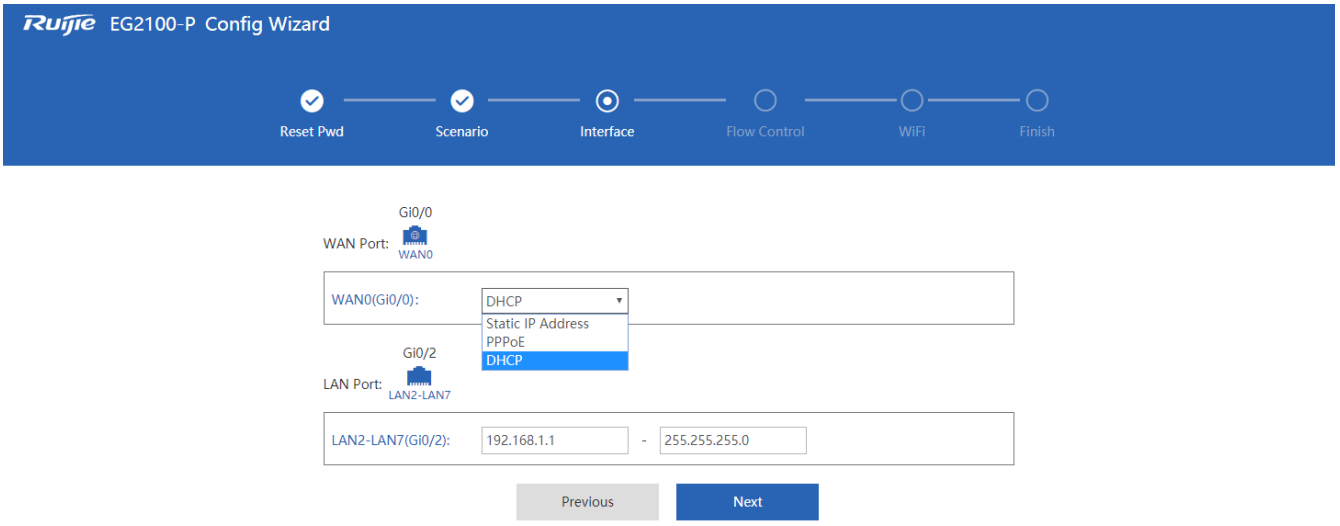
(1) Reset Password



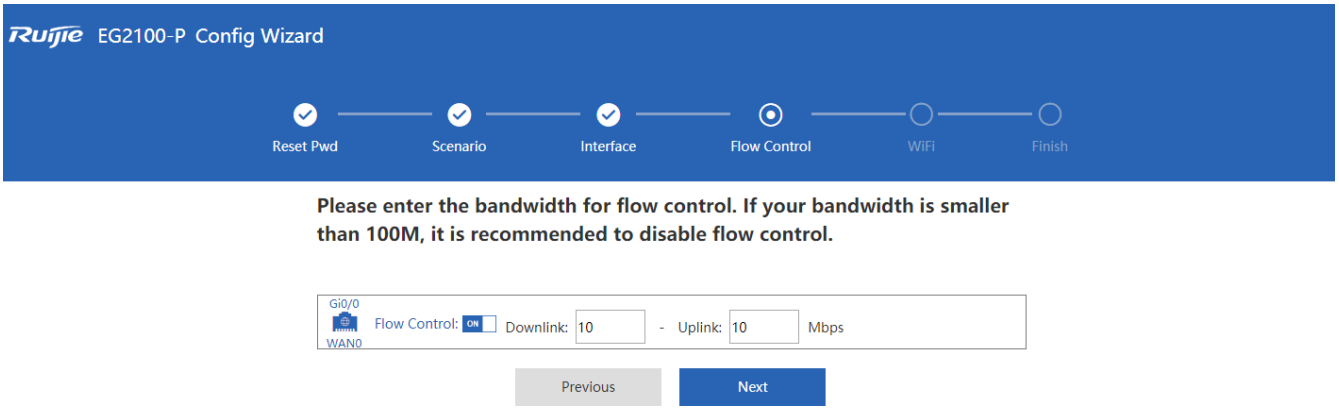

(2) Select Scenario



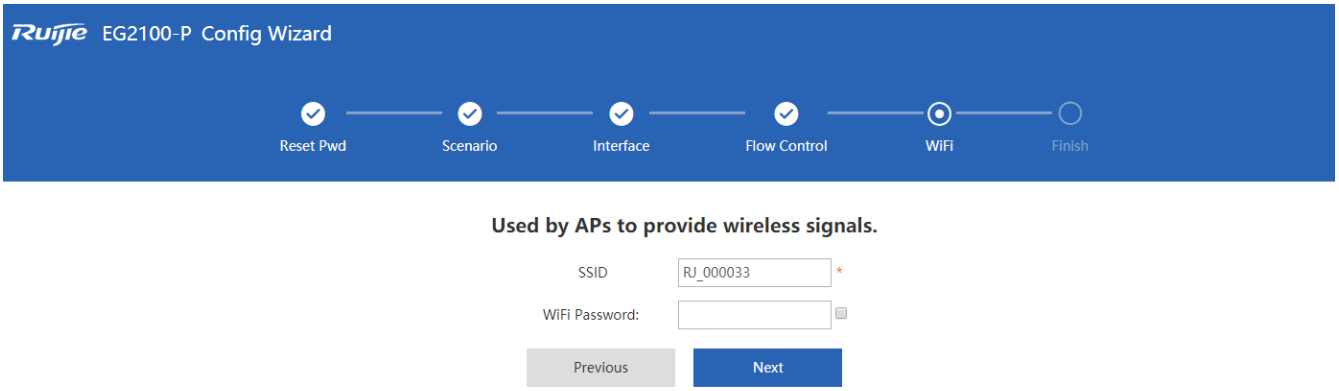

(3) Configure Interface



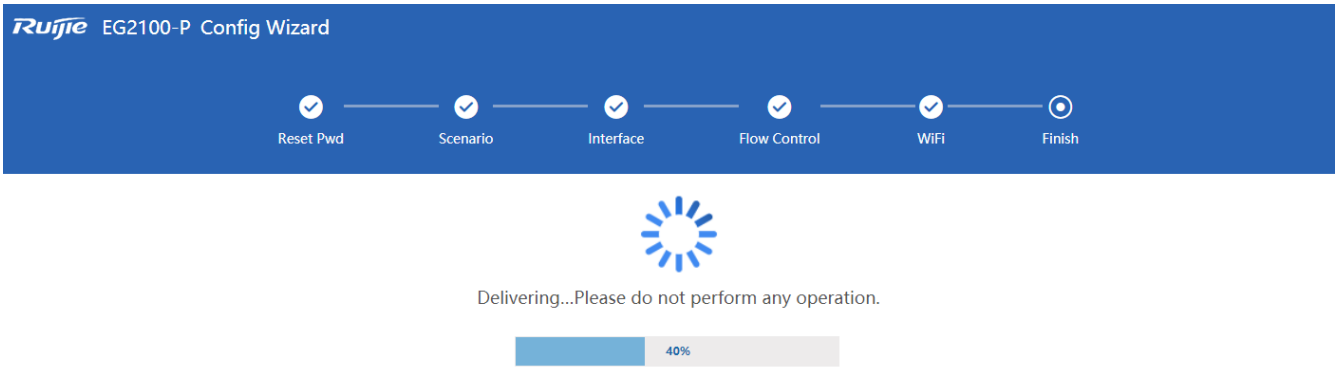

(4) Enable Smart Flow Control

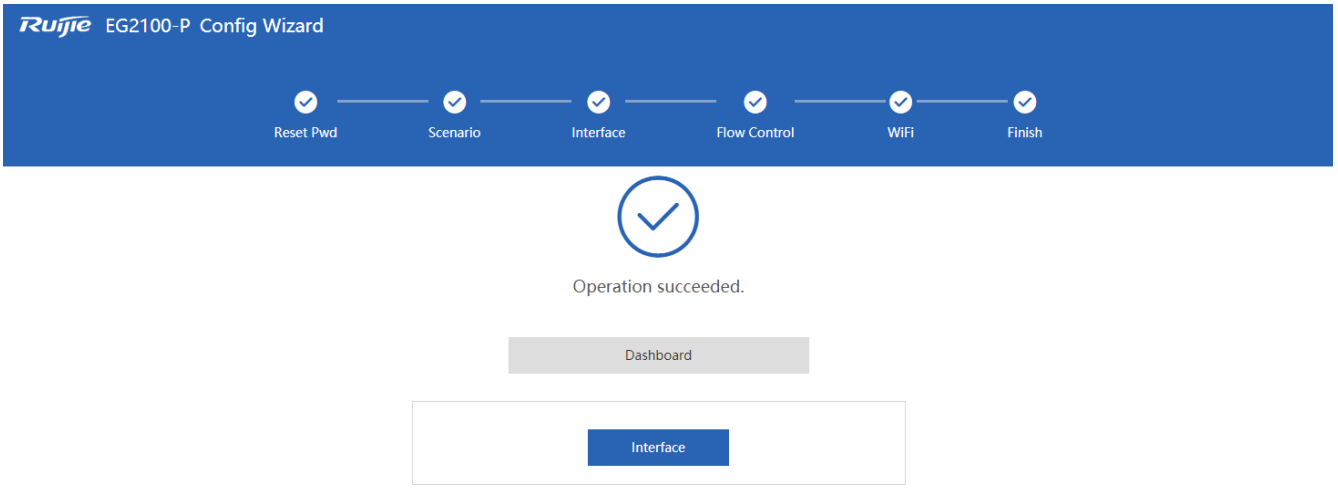



(5) Configure WiFi




(6) Save Configuration

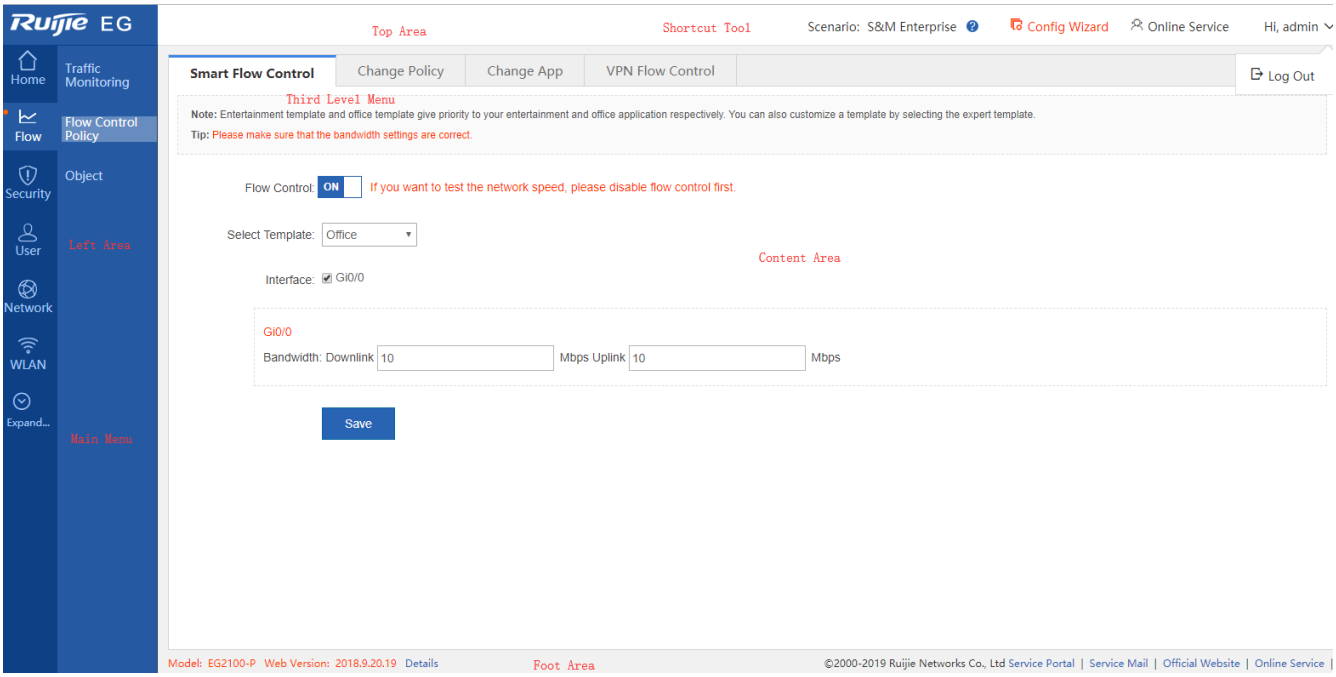



WiFi settings will be displayed only if the device supports WiFi.

### 1.3.3 Main UI of Web Management System

The main UI of the Web management system is displayed in the figure below.




### 1.3.3.1 Top Area

This area provides links to some common functions, so that you can easily access the corresponding setting pages. The functions include Config Wizard, Customer Service, and Log Out.

#### Config Wizad

Click 

, and the **Config Wizard** page will be displayed. You can reset the administrator password, select the scenario, enable smart flow control and configure WiFi.

#### Customer Service

When you click 

, the online customer service window is displayed. You can consult customer service personnel after entering your information.

#### Log Out

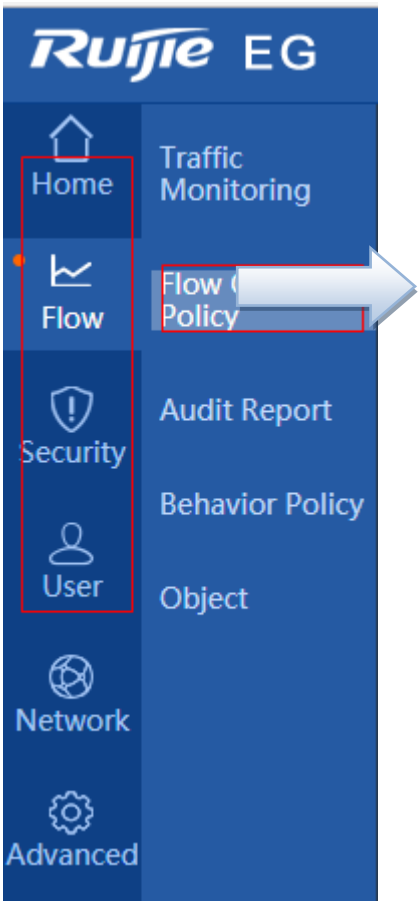
After you complete device management, click 

to exit the main UI of the Web management system of the EG device and return to the login page.

### 1.3.3.2 Left Area

This area lists all function menus of the EG device. After you click a menu, the detailed setting page is displayed.

The menus in the menu navigation area are organized in two levels. When you click a function category, relevant submenus are displayed. For example, if you click **Flow**, the submenus of this category are displayed, as shown in the figure below.




### 1.3.3.3 Content Area

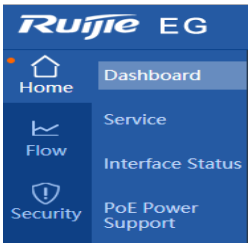
The Content allows you to complete function settings for the EG device. After you click a navigation menu on the left side or a shortcut menu on the top, the detailed setting page is displayed in the main action area.

### 1.3.3.4 Foot Area

The Foot area displays the device model and version on the left side and technical forum website and contact information for technical support on the right side. You can find them for help.

## 1.3.4 Home

### 1.3.4.1 Dashboard

After you log in to the Web management UI, the system home page is automatically displayed. You can also click 

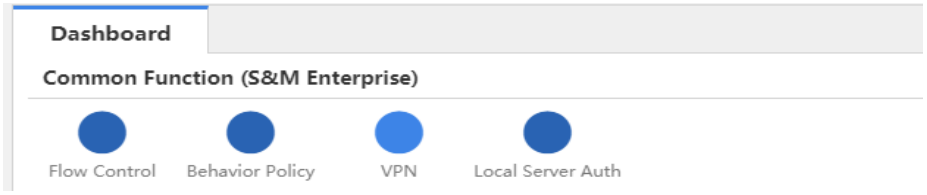
in the left area to redirect to the system Dashboard page.

The **Dashboard** page displays common functions, interface information, the device CPU, memory usage, disk space, online users, system version, and system time. By analyzing the traffic trend, TOP10 applications in traffic, and TOP10 users in traffic on the current day, you can comprehensively learn about the current status of LAN traffic, find out and locate common network faults, and correct the faults rapidly.

#### 1.3.4.1.1 Dashboard

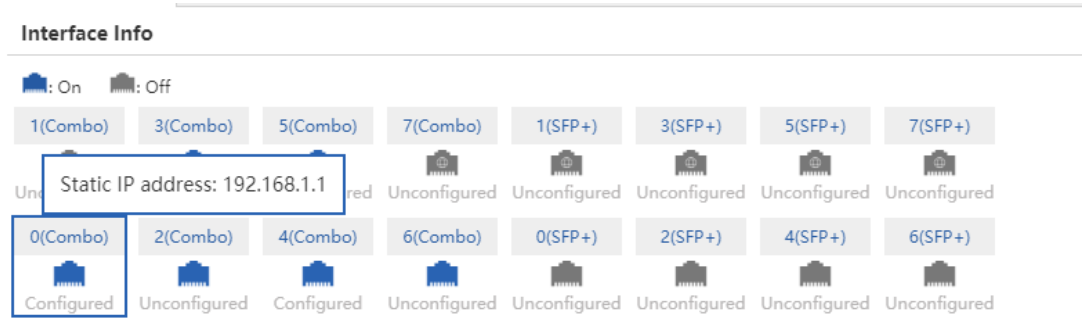
The home page displays the CPU, memory usage, disk space, online users, system version, and system time about the current device on the top.

#### 1.3.4.1.2 Common Function

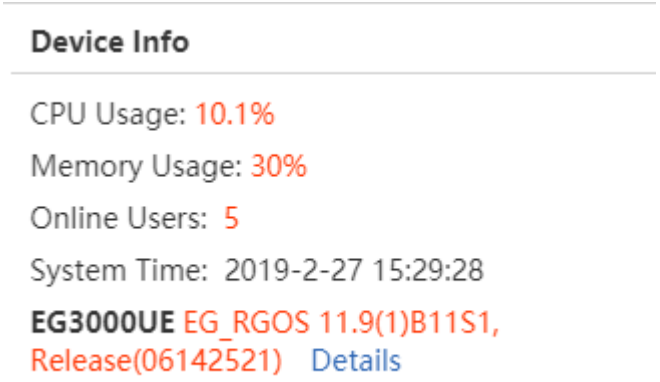



#### 1.3.4.1.3 Interface Info

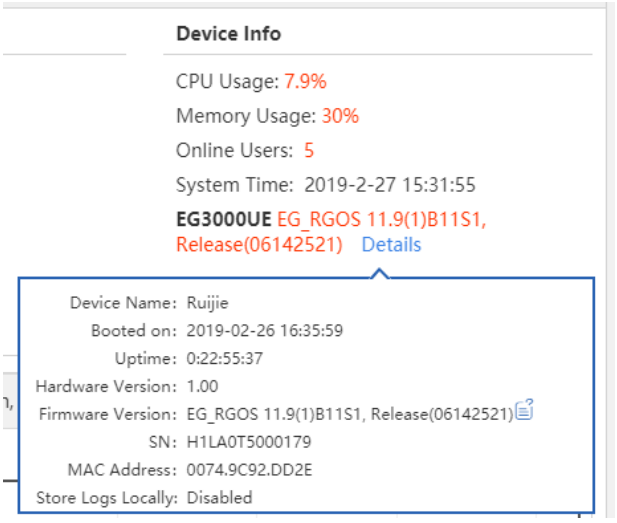
Place the mouse cursor over the interface, the interface information will be displayed, including interface type, IP address and account.



### 1.3.4.1.4 Device Info



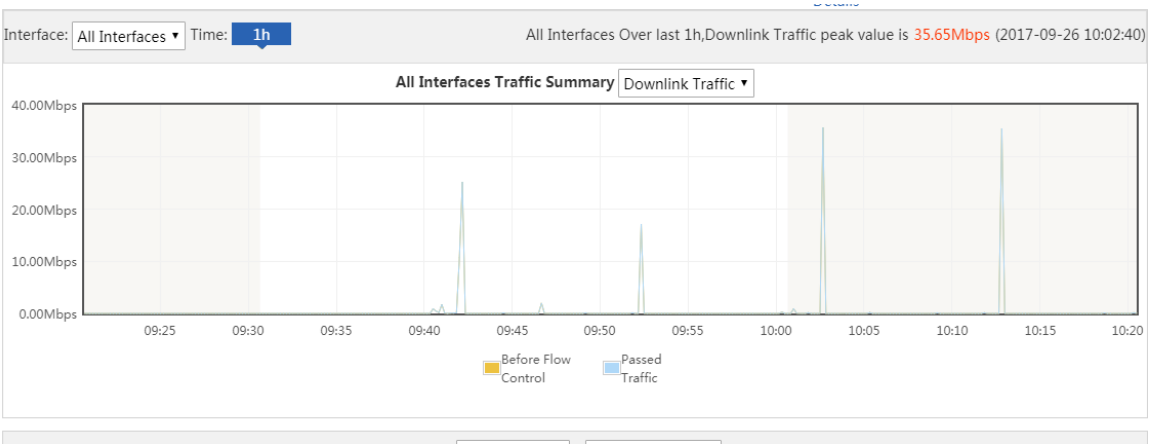

1. **CPU**: Displays the CPU usage of the current device. You can easily know the running status of the device. When you move the cursor over the CPU display area, more specific information and description will be displayed.
2. **Memory Usage**: Displays the memory usage of the current device. You can easily know the memory usage of the device. When you move the cursor over the memory display area, the total memory, used memory, and free memory of the current device are displayed.
3. **Disk Space**: Displays the disk usage of the current device. You can easily know the disk usage of the device. When you move the cursor over the disk display area, the total disk size, used disk size, and free disk size of the current device as well as a precaution (Do not power off the device when the SATA LED is blinking.) are displayed.
4. **Online Users**: Displays the number of online users of the current device. When you move the cursor over the online users display area, the number of online users in each line (interface) of the current device is displayed.
5. **System Time**: Displays the current system time. If the current system time is incorrect or the system time needs to be set as required, choose **Advanced** > **System** and click **System Time** to set the system time.
6. **Details**: Place the mouse cursor over **Details**, and the device information will be displayed.



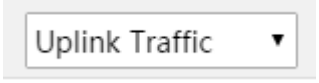
### 1.3.4.1.5 Bandwidth

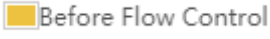
The system home page displays the system bandwidth status. On this page, you can view the device's traffic trend on the current day, TOP10 applications in traffic on the current day, and TOP10 users in traffic on the current day.

- **Interface**




1. As shown in the figure above, the curve in yellow shows the traffic trend before flow control is implemented while the curve in blue shows the trend of actually passed traffic after flow control is implemented.
2. Change the values in 

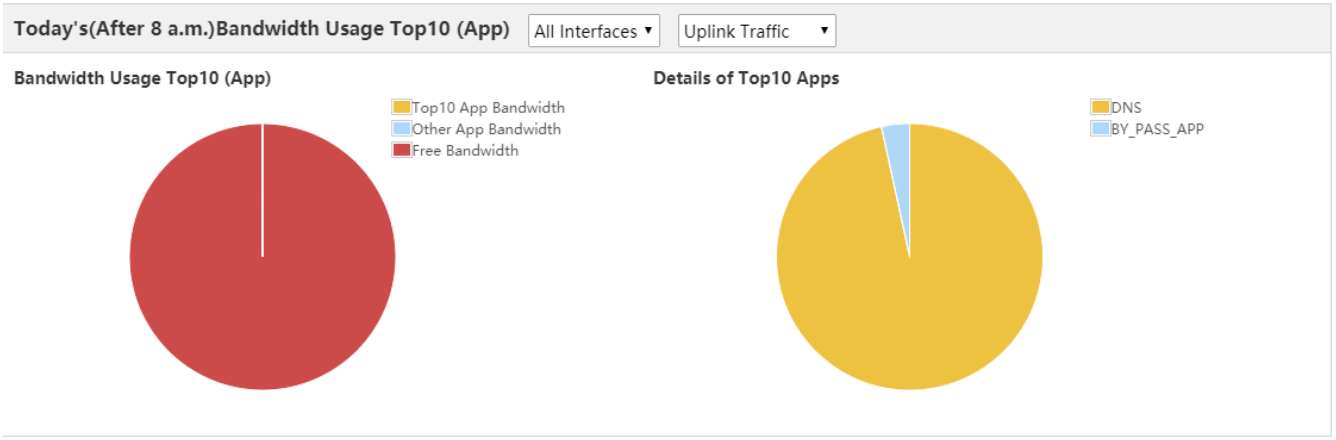
and 

to display the traffic trend of each interface on the current day.
3. When you move the cursor over a point on the curve, the traffic prior to flow control and the passed traffic at this point are displayed.
4. Click 

to hide the trend curve of the traffic prior to flow control and click 

to hide the trend curve of passed traffic.

- **Today's (After 8 a.m.) Bandwidth Usage Top10 (App)**



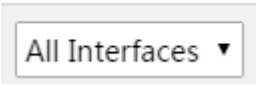

1. As shown in the figure above, the pie chart on the left shows the bandwidth proportions of Top 10 applications. You can move the cursor over the pie chart to display bandwidth occupation details.

   (1) **Top10 App Bandwidth**: It displays the percentage of the total uplink/downlink bandwidth of a selected interface occupied by Top 10 bandwidth applications to the total uplink/downlink bandwidth of the selected interface.

   (2) **Other App Bandwidth**: It displays the percentage of the total uplink/downlink bandwidth of a selected interface occupied by applications (except Top 10 applications) to the total uplink/downlink bandwidth of the selected interface.

   (3) **Free bandwidth**: It displays the percentage of the total free uplink/downlink bandwidth of a selected interface to the total uplink/downlink bandwidth of the selected interface.

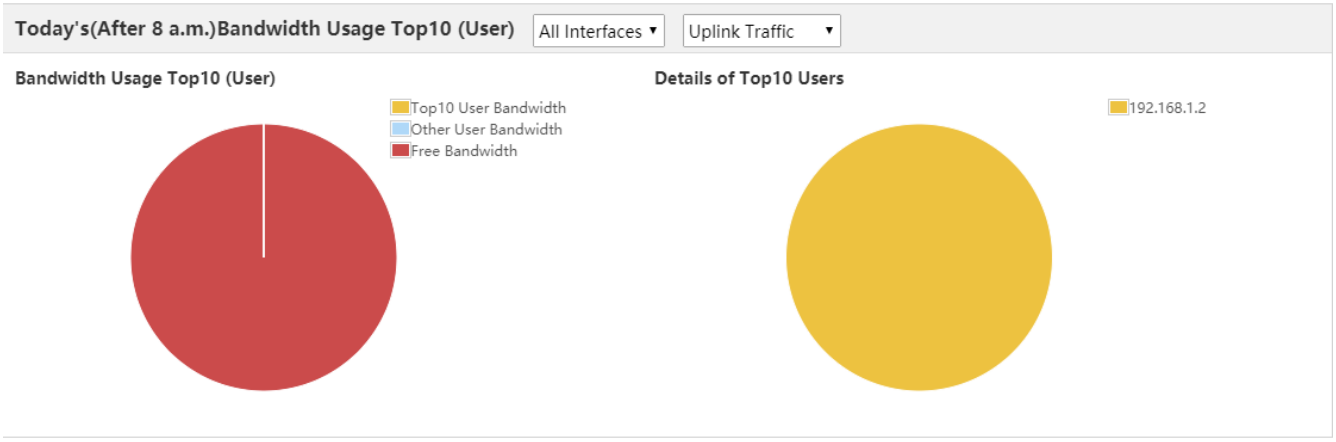
2. The pie chart on the right displays details about the Top 10 applications that occupy the most bandwidth in the uplink/downlink bandwidth of a selected interface, and the percentages of the bandwidth occupied by these applications. You can move the cursor over the pie chart to display the bandwidth occupied by an application.

3. You can change the values of 

and 

to display Top 10 applications in terms of uplink/downlink traffic of different interfaces.

- **Today's (After 8 a.m.) Bandwidth Usage Top10 (User)**



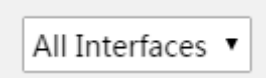
1. As shown in the figure above, the pie chart on the left shows the bandwidth proportions of Top 10 users. You can move the cursor over the pie chart to display bandwidth occupation details.

   (1) **Top10 User Bandwidth**: It displays the percentage of the total uplink/downlink bandwidth of a selected interface occupied by Top 10 bandwidth users to the total uplink/downlink bandwidth of the selected interface.

   (2) **Other User Bandwidth**: It displays the percentage of the total uplink/downlink bandwidth of a selected interface occupied by users (except Top 10 users) to the total uplink/downlink bandwidth of the selected interface.

   (3) **Free Bandwidth**: It displays the percentage of the total free uplink/downlink bandwidth of a selected interface to the total uplink/downlink bandwidth of the selected interface.

2. The pie chart on the right side displays details about the Top 10 users who occupy the most bandwidth in the uplink/downlink bandwidth of a selected interface, and the percentages of the bandwidth occupied by these users. You can move the cursor over the pie chart to display the bandwidth occupied by a user.

3. You can change the values of 

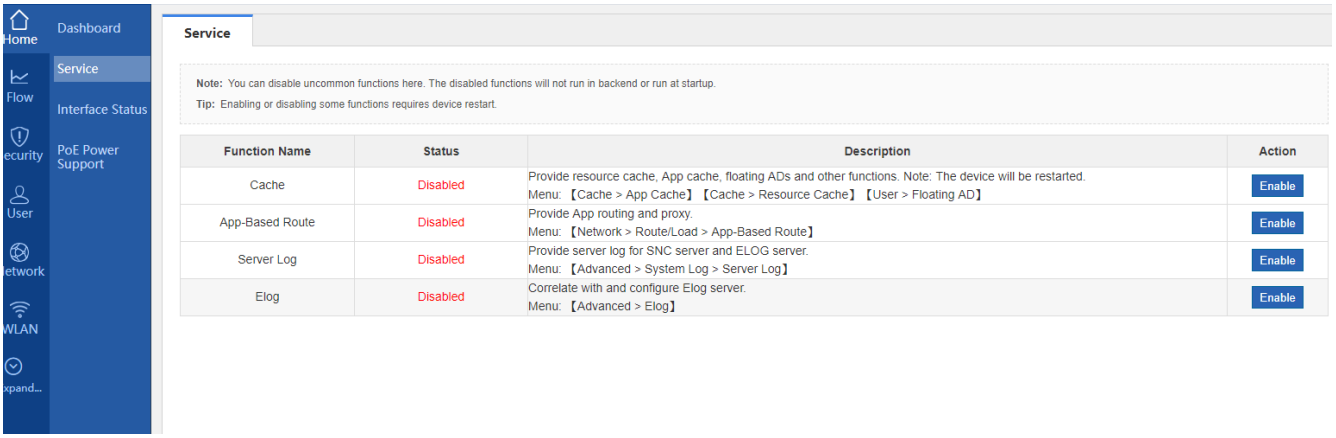
and 

to display Top 10 users in terms of uplink/downlink traffic of different interfaces.

## 1.3.5 Service

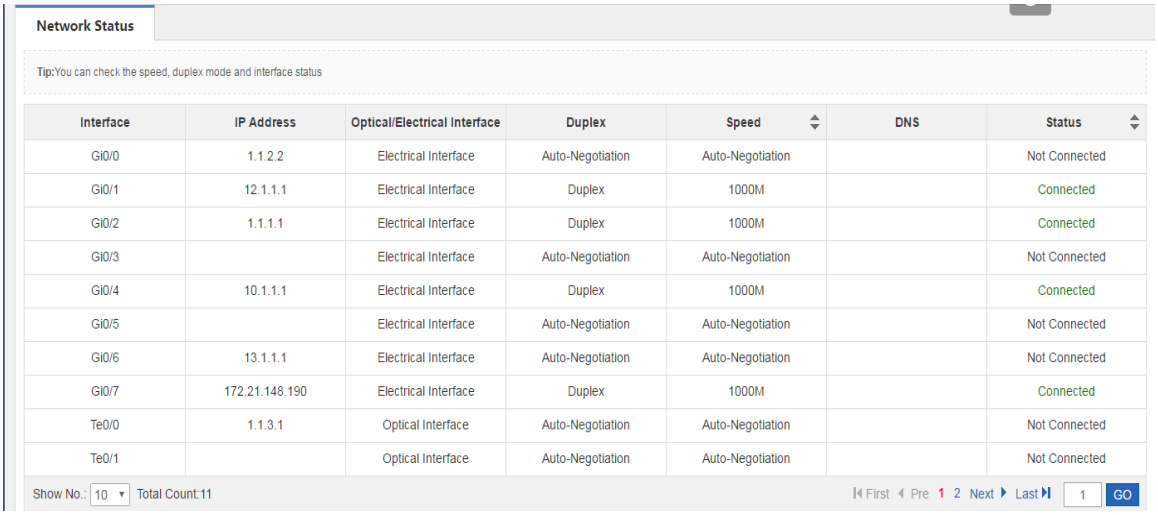
Default services vary with different devices. If you want to enable a specific service, click 

in the **Action** column.



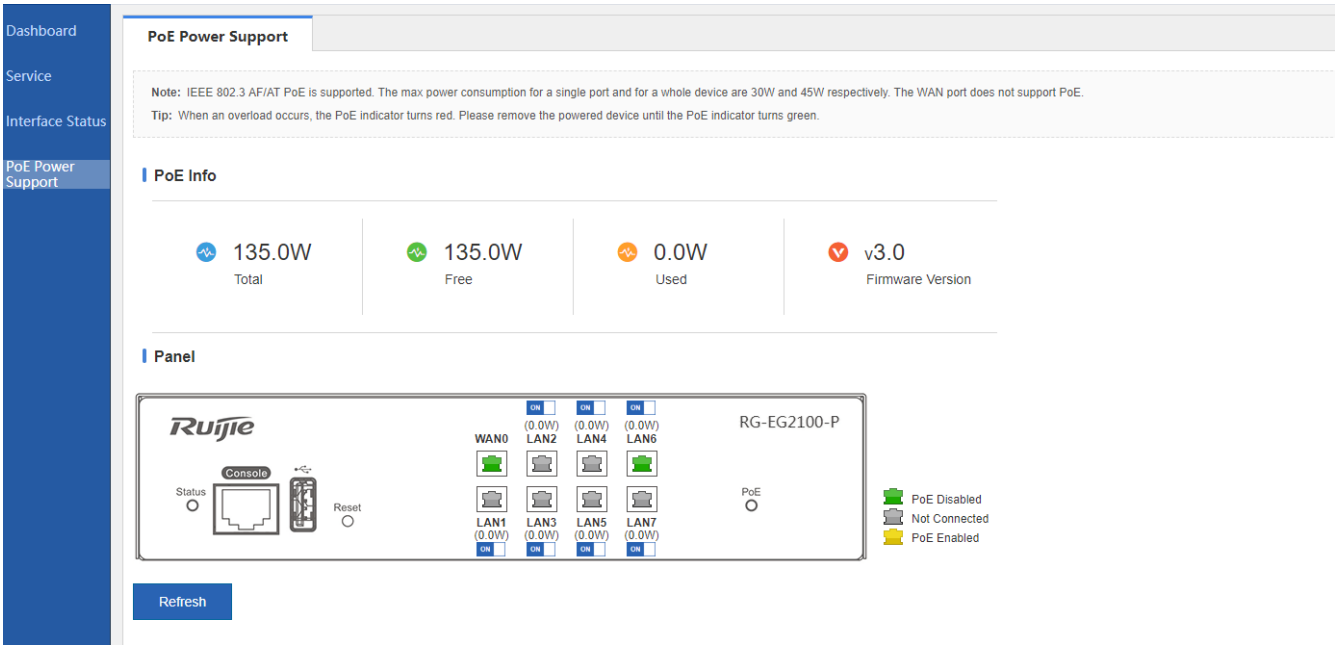

## 1.3.6 Interface Status

The **Interface Status** page displays information about the status of each interface, including the IP address, optical/electrical interface, duplex, speed, DNS, and connection status.




## 1.3.7 PoE Power Support

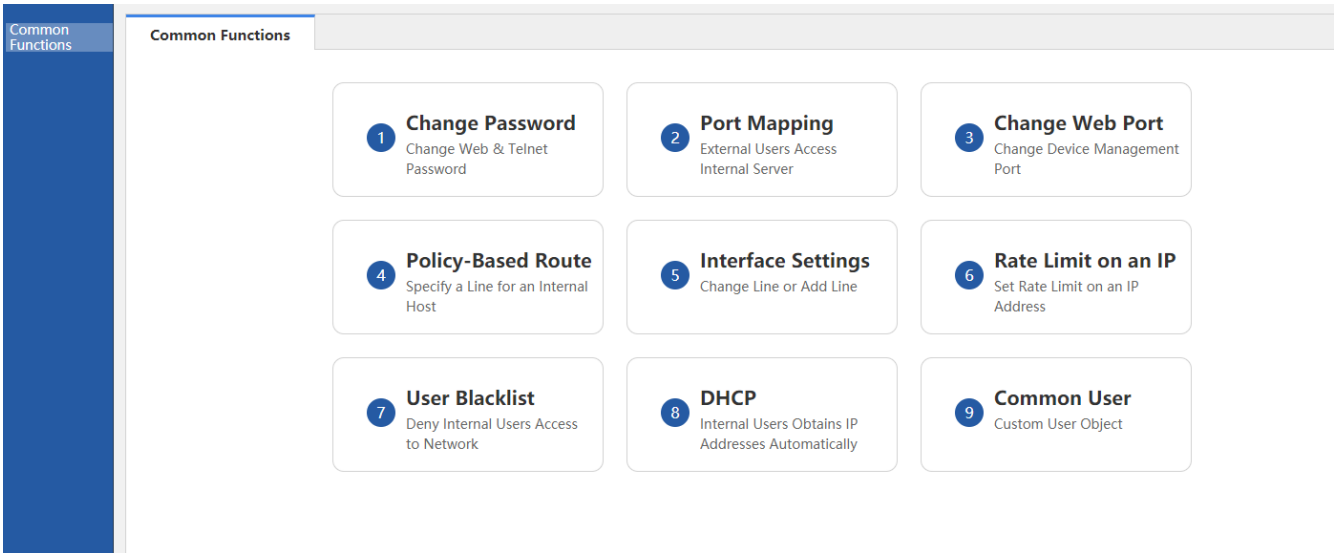
PoE power is supported by only EG2100-P.




## 1.3.8 Common

### 1.3.8.1 Common Functions

The following common functions are available: Change Password, Port Mapping, Change Web Port, Policy-Based Route, Interface Settings, Rate Limit on an IP, User Blacklist, DHCP, and Common User

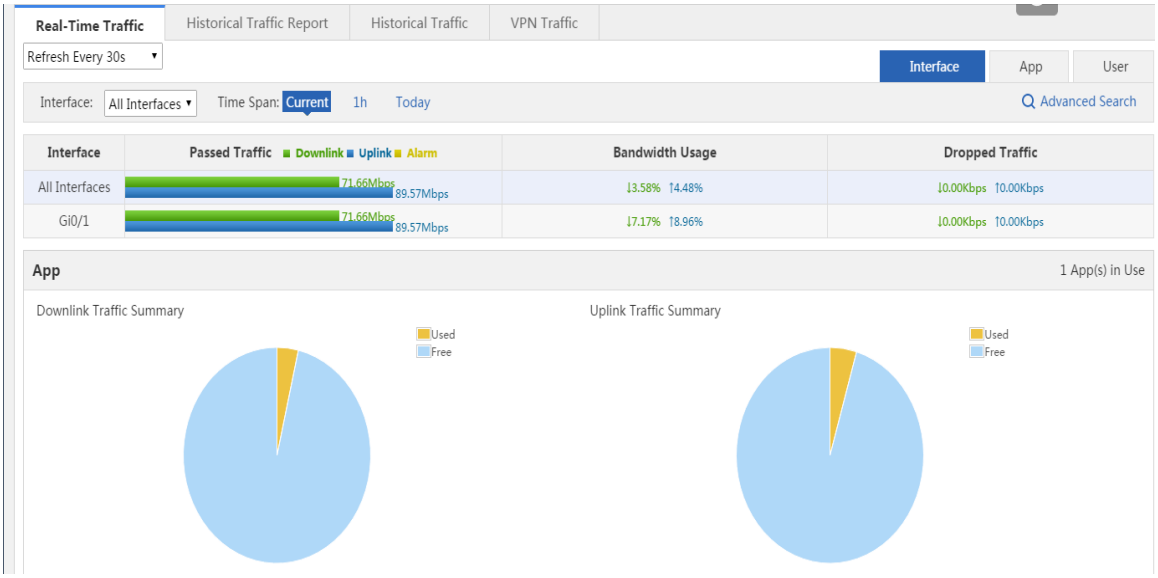



## 1.3.9 Flow Control

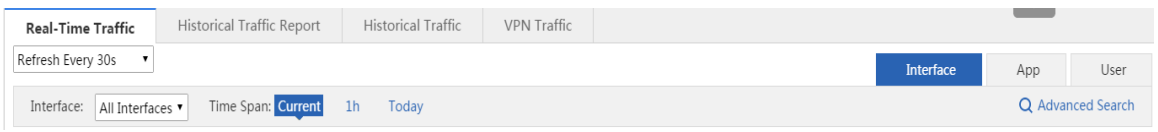
### 1.3.9.1 Traffic Monitoring

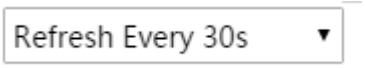
Choose **Flow** > **Traffic Monitoring** to display the traffic usage of the current network and enable the device to intelligently analyze specific applications.

#### 1.3.9.1.1 Real-time Traffic




1. The **Real-Time Traffic** page displays the real-time traffic navigation menus in the upper part.



(1) Select 10 seconds, 30 seconds, or 1 minute from 

to automatically update the information about the current traffic of the device or manually update the information about the current traffic of the device.

(2) Click 

to display information about the device traffic by interface, application, or user.

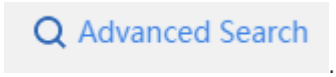
(3) Select a line from 

to display traffic information of the line or select **All Interfaces** to display information about the total traffic of all lines.

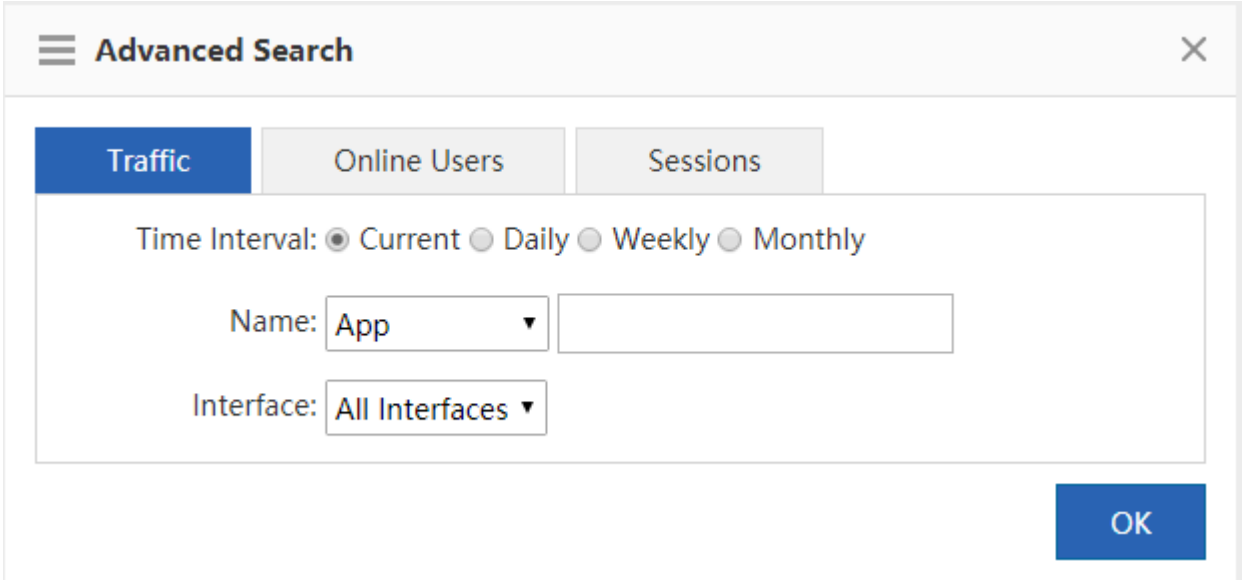
(4) Click 

to display information about the current traffic, or information about the overall traffic trend in the last one hour or on the current day. 

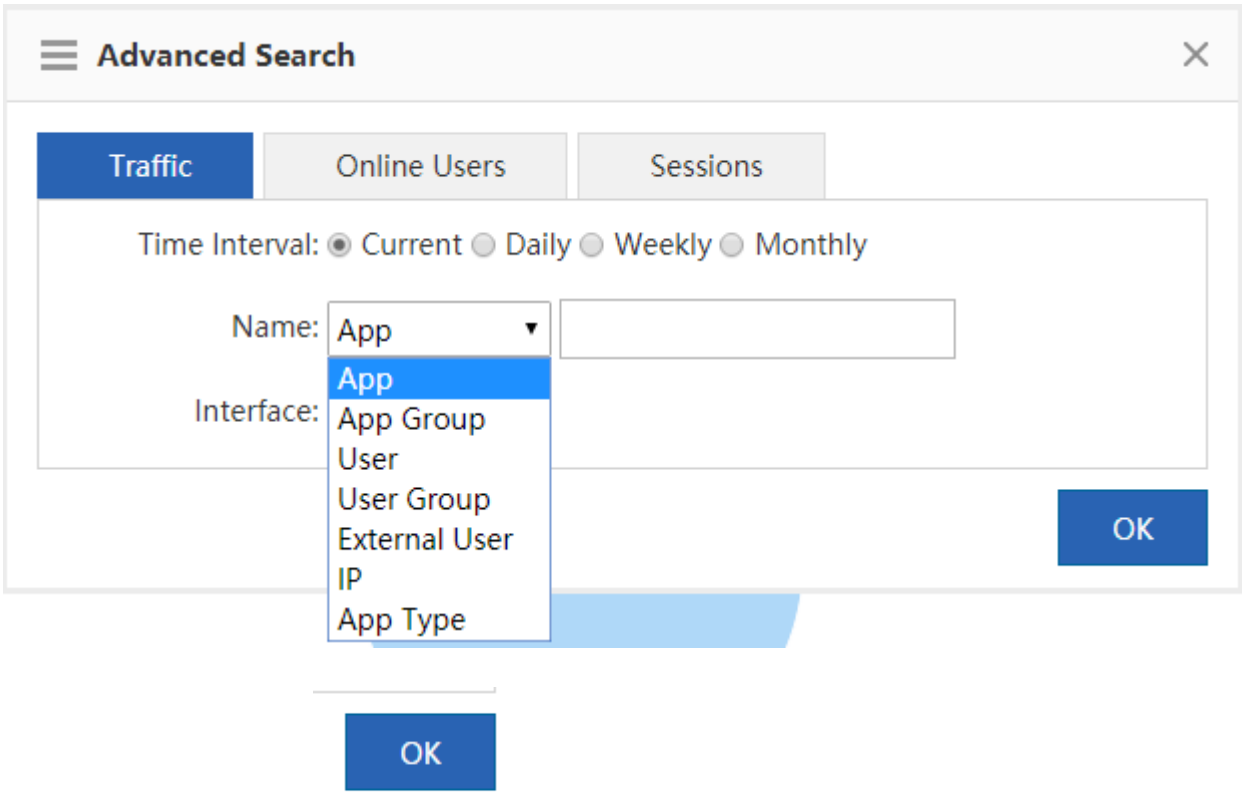
Indicates that information about the current traffic is displayed.

(5) Click 

. A dialog box shown in the figure below is displayed. You can query details about the traffic, online users, and sessions.



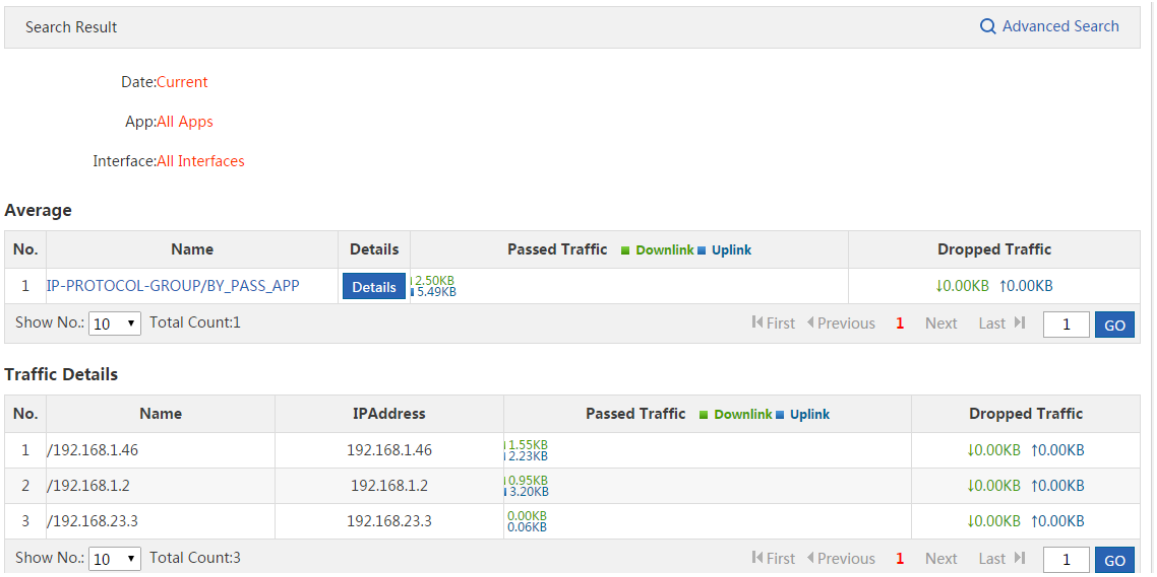

**Traffic**: You can query information about the current traffic of an interface or about traffic in a time range by user, IP address, or application. As shown in the figure below, select the required type from click the drop-down list next to **Name**, and click the input box to select the required application range or user range from the displayed applications or users.



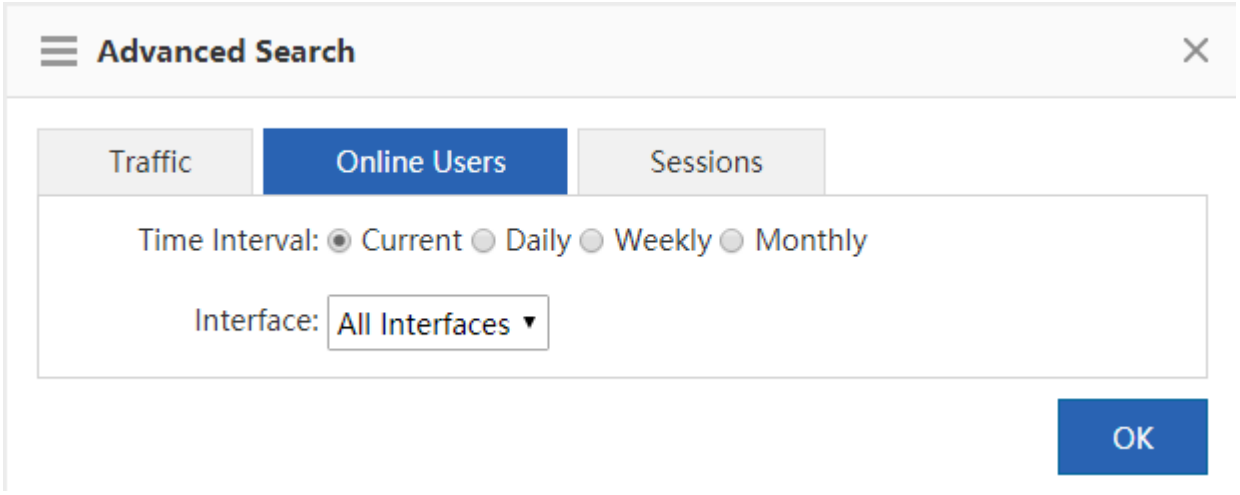




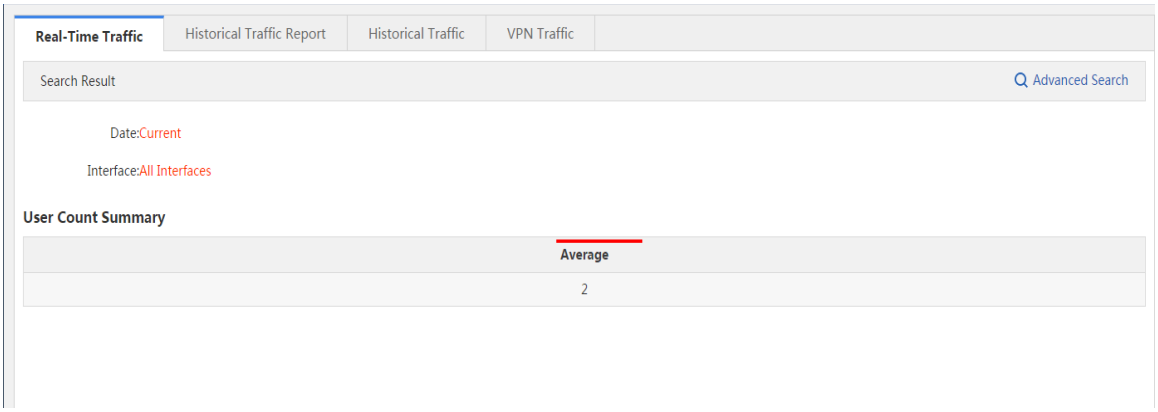
Select an interface and click . The search result shown in the figure below is displayed.



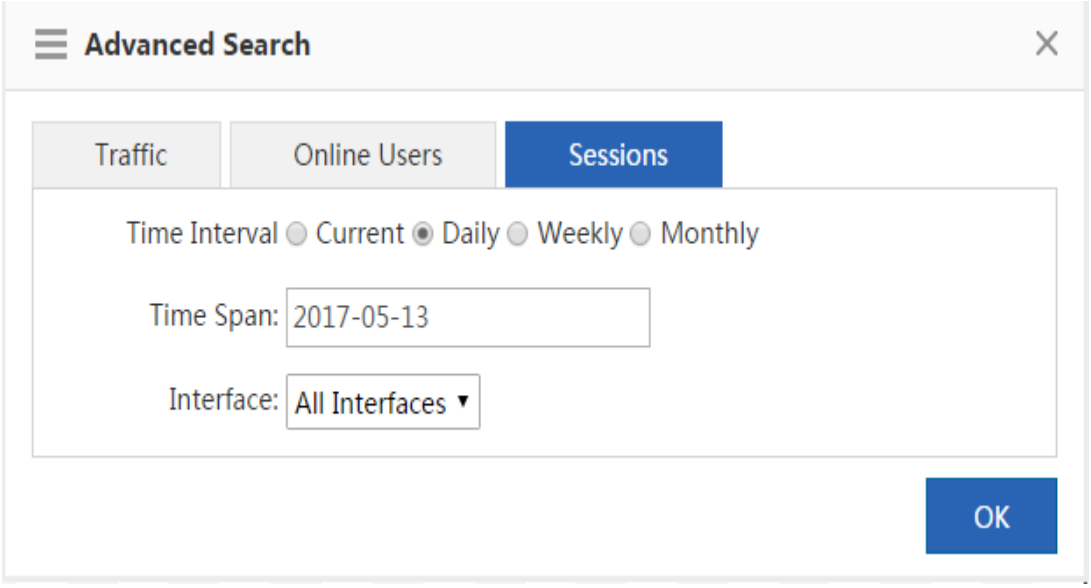

**Online Users**: You can query the number of current online users of an interface or the number of online users within a time range.



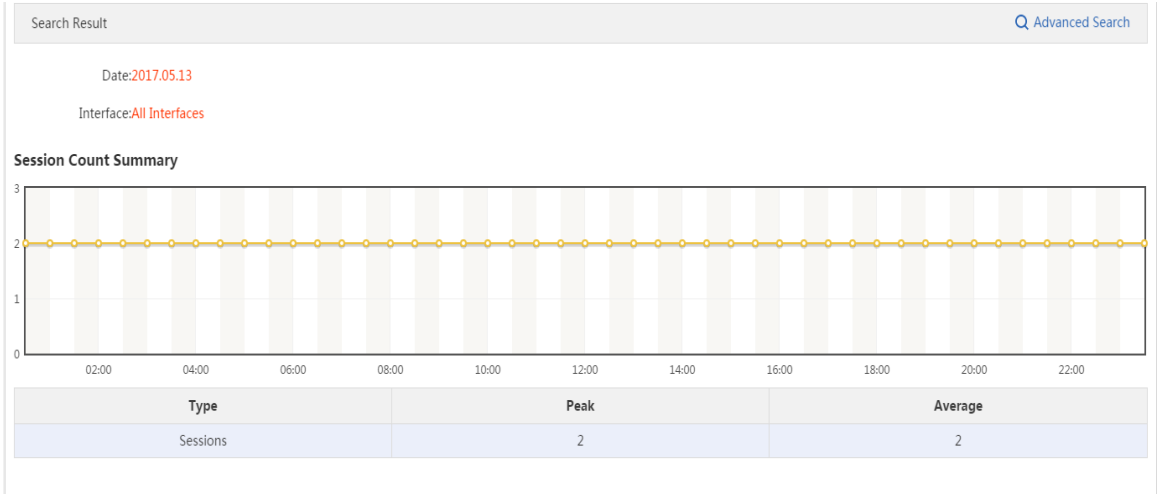

Click OK. The search result shown in the figures below is displayed.




**Sessions**: You can query the number of current sessions of an interface or the number of sessions within a time range, as shown in the figure below.

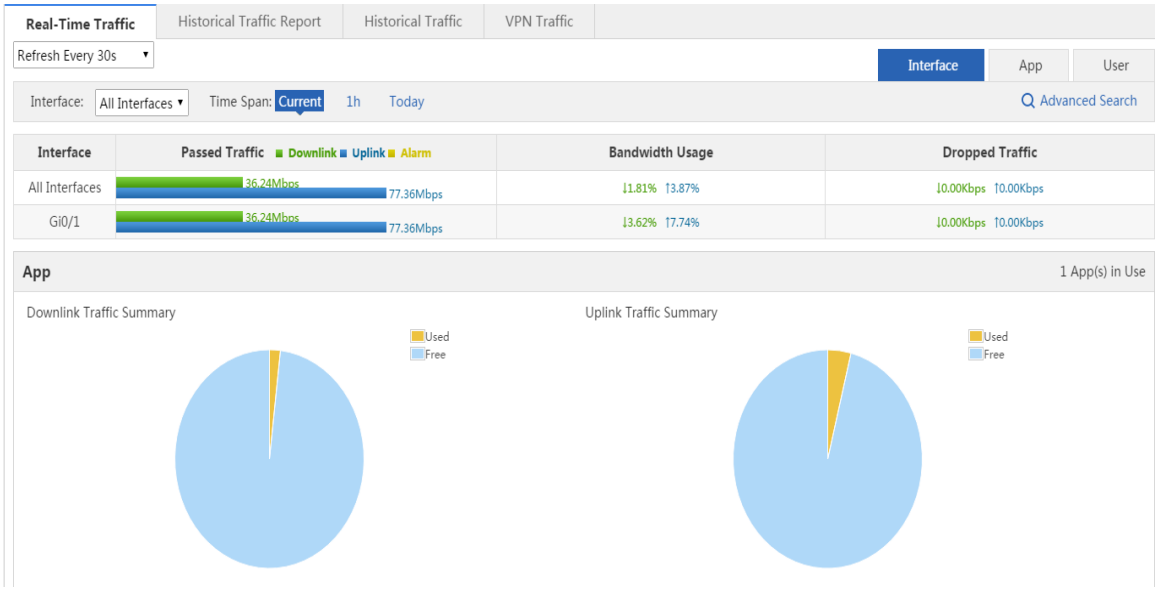



Click OK. The search result shown in the figure below is displayed.



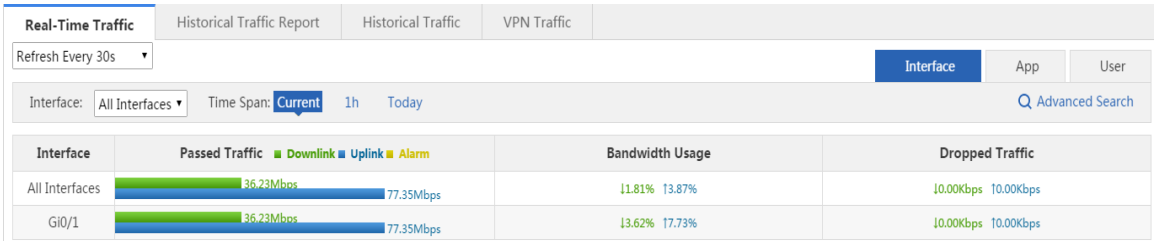

- **Interface Traffic Analysis**

The interface traffic analysis function collects statistics on the bandwidth usage of different interfaces. You can control and analyze the traffic of an interface to improve the traffic utilization rate. Click Interface on the **Real-Time Traffic** page. A page shown in the figure below is displayed.




- **Overview**

Overview: Traffic information of an interface is displayed. If you select **All Interfaces** from the **Interface** drop-down list, information about the total traffic of all interfaces as well as the traffic of each interface are displayed.




Current traffic: The figure above shows information about the current traffic of interfaces. You can check whether the current traffic is normal (whether an alarm is generated). If the traffic is too heavy, a yellow alarm icon 

is displayed so that you can pinpoint the bandwidth problem rapidly.

Q: When is an alarm prompted?

An alarm is prompted when the total traffic is higher than 95% of the line bandwidth (bandwidth purchased from an ISP).

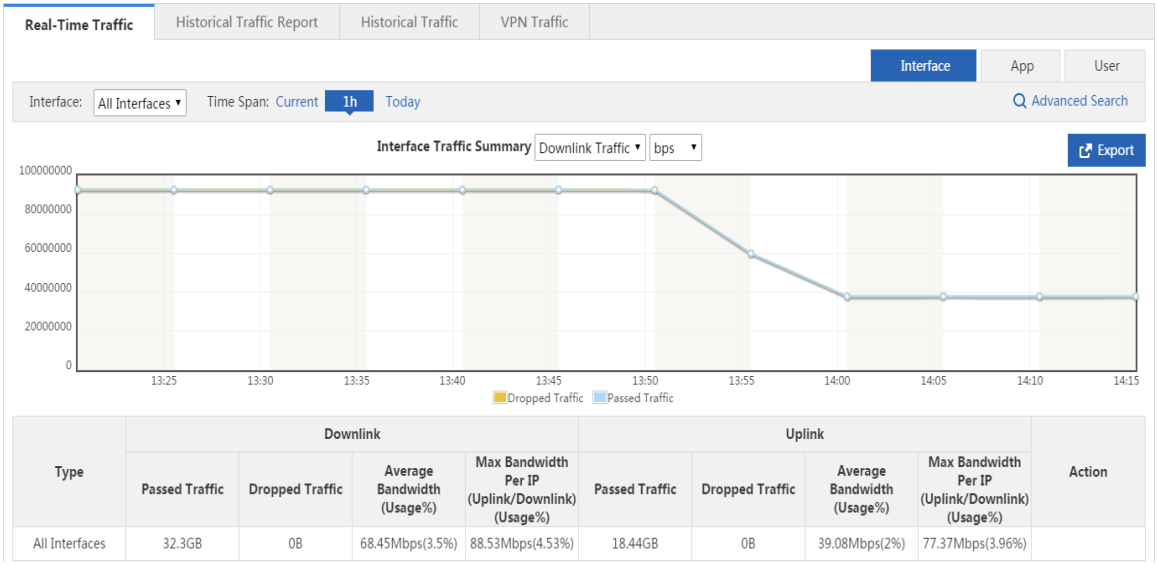
Q: How to clear a yellow alarm?

When only a yellow alarm about the total traffic is generated and the traffic of the key application group is equivalent to the total traffic, access the **Flow Control Policy** or **Custom App** page to check whether the selected applications are applications to be guaranteed with sufficient bandwidth. If the applications need to be guaranteed, the bandwidth is insufficient. Apply to your ISP for more bandwidth to ensure smooth office work.

When a yellow alarm about the total traffic is generated and the bandwidth occupied by the rate-limited application group is high, limit the traffic of the rate-limited application group to prevent heavy traffic.

When an alarm about the total traffic is generated and the traffic of the normal application group is equivalent to that of the rate-limited application group, limit the traffic of the rate-limited application group and normal application group to prevent heavy traffic.

(2) Traffic trend in the last one hour




| Type | Downlink | | | | Uplink | | | | Action |
|---|---|---|---|---|---|---|---|---|---|
| | Passed Traffic | Dropped Traffic | Average Bandwidth (Usage%) | Max Bandwidth Per IP (Uplink/Downlink) (Usage%) | Passed Traffic | Dropped Traffic | Average Bandwidth (Usage%) | Max Bandwidth Per IP (Uplink/Downlink) (Usage%) | |
| All Interfaces | 32.3GB | 0B | 68.45Mbps(3.5%) | 88.53Mbps(4.53%) | 18.44GB | 0B | 39.08Mbps(2%) | 77.37Mbps(3.96%) | |

The curve in the figure above shows the traffic trend of the selected interface in the last one hour. For details about the curve, see "Current App" in 1.3.4.1.2 "Bandwidth."

Click 

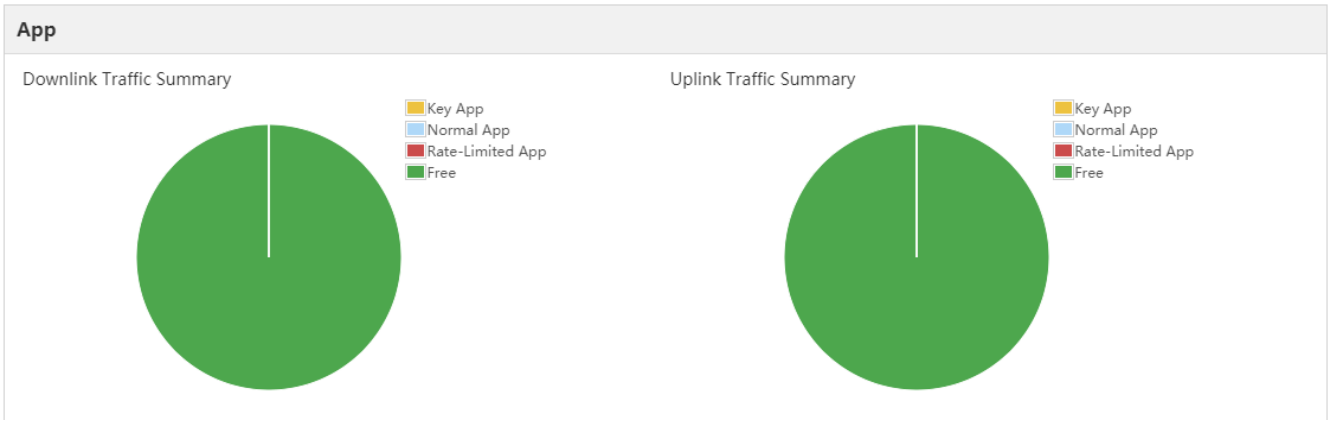
to export the traffic trend report to the local PC.

The table in the lower part lists the passed uplink/downlink traffic of the selected interface in the last one hour, dropped traffic due to flow control, average bandwidth, and maximum bandwidth per IP in the last one hour.

(3) Traffic trend on the current day: The interface traffic trend UI is the same as that for traffic in the last one hour except for the time range.

- App

Application: The application area displays the bandwidth usage proportions of different types (key, normal, rate-limited and free) of applications on the selected interface, the number of running applications, specific applications, traffic occupied by each application, and traffic dropped due to the rate limit policy.




(1) The two pie charts in the upper part of the area respectively display information about the uplink traffic and downlink traffic occupied by each type of applications on the selected interface. When you move the cursor over a pie chart, the size of the free uplink/downlink traffic on the selected interface is displayed.

Key App: Displays the percentage of uplink/downlink traffic occupied by all key applications on the selected interface to the total uplink/downlink traffic of the selected interface.

Normal App: Displays the percentage of uplink/downlink traffic occupied by all normal applications on the selected interface to the total uplink/downlink traffic of the selected interface.

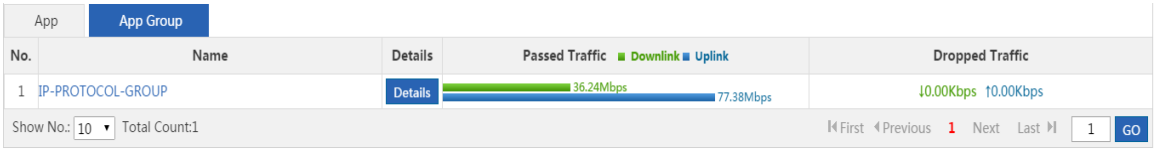
Rate-limited App: Displays the percentage of uplink/downlink traffic occupied by all rate-limited applications on the selected interface to the total uplink/downlink traffic of the selected interface.

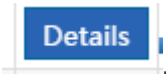
Free: Displays the percentage of free uplink/downlink traffic of the selected interface to the total uplink/downlink traffic of the selected interface.

(2) The table in the lower part of the area displays information about the traffic of running applications on the selected interface, including the uplink/downlink traffic occupied by each application and traffic dropped due to the rate limit policy.

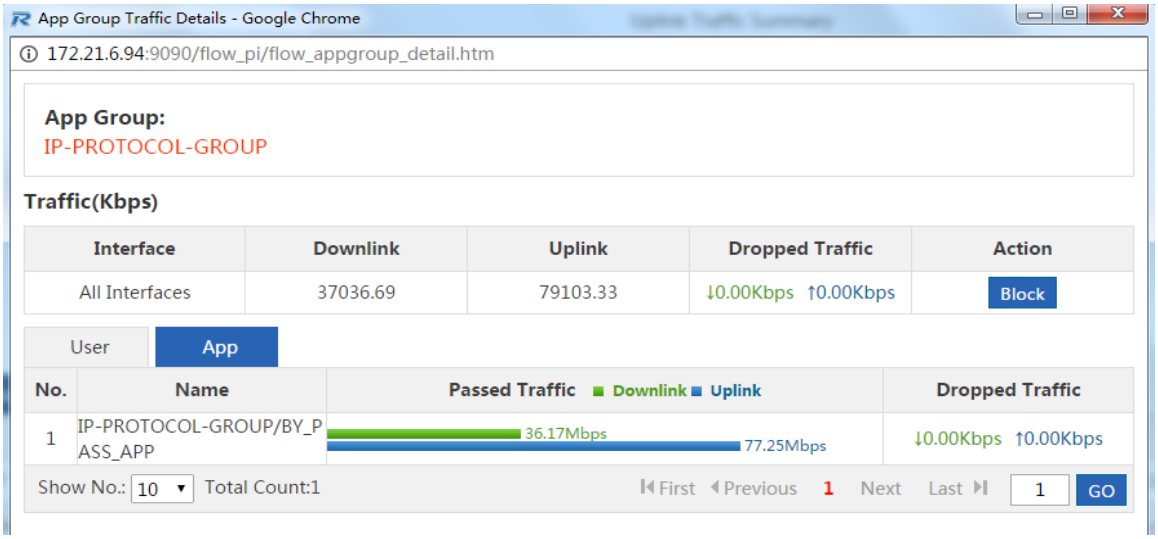
Click 

above the table. Information about the traffic of a running application group on the selected interface is displayed.




Click 

. A window shown in the figure below is displayed.



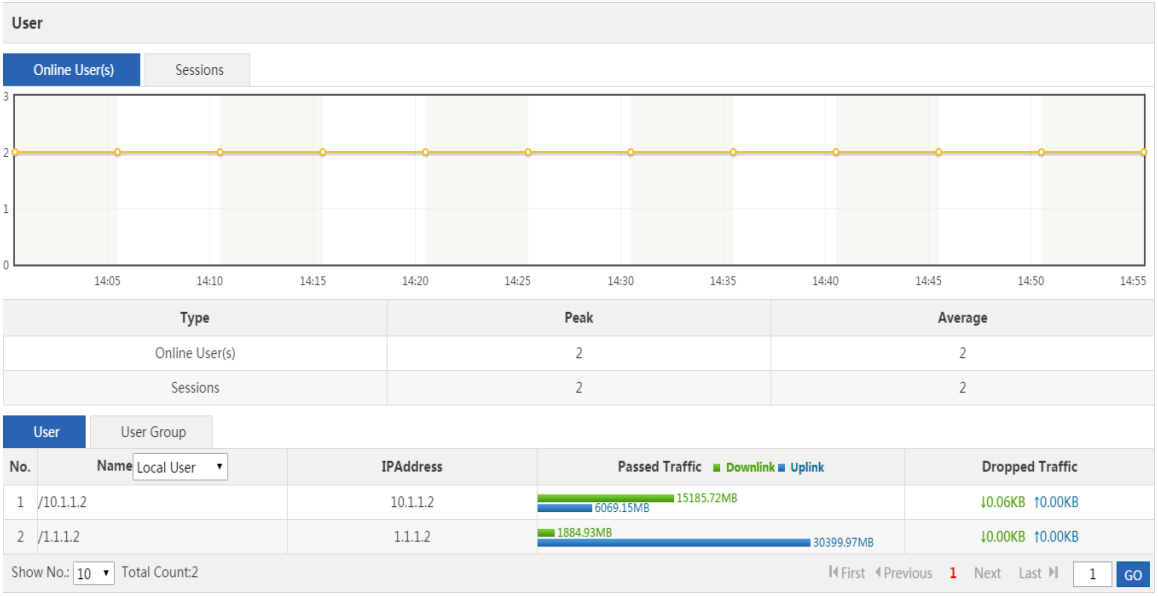

The window displays the application group to which the selected application belongs, type of the application, uplink/downlink traffic occupied by the application on the selected interface, and traffic dropped due to the rate limit policy, and traffic of users who are using the application.

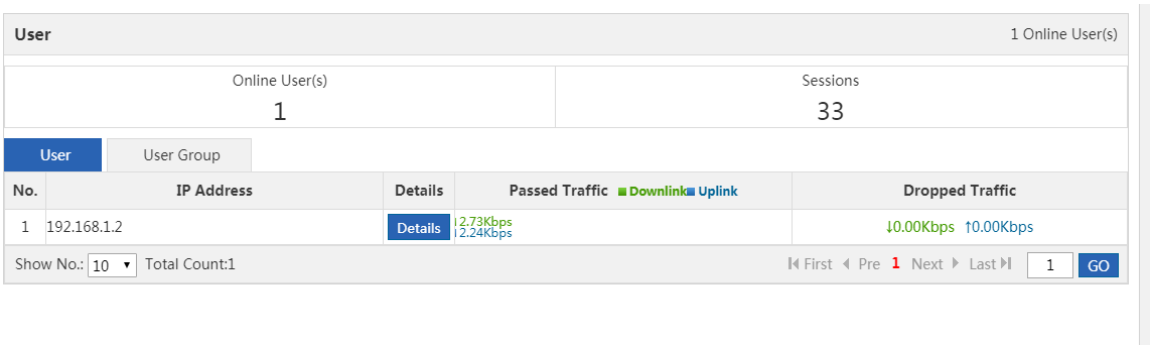
Click 

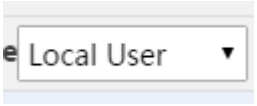
to block the traffic of the current application. After blocking, the subsequent traffic of the application will be thoroughly dropped by the interface.

(3) User

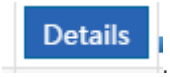
The user area displays the number of online users, number of sessions, and information about the traffic of users who are using the interface.



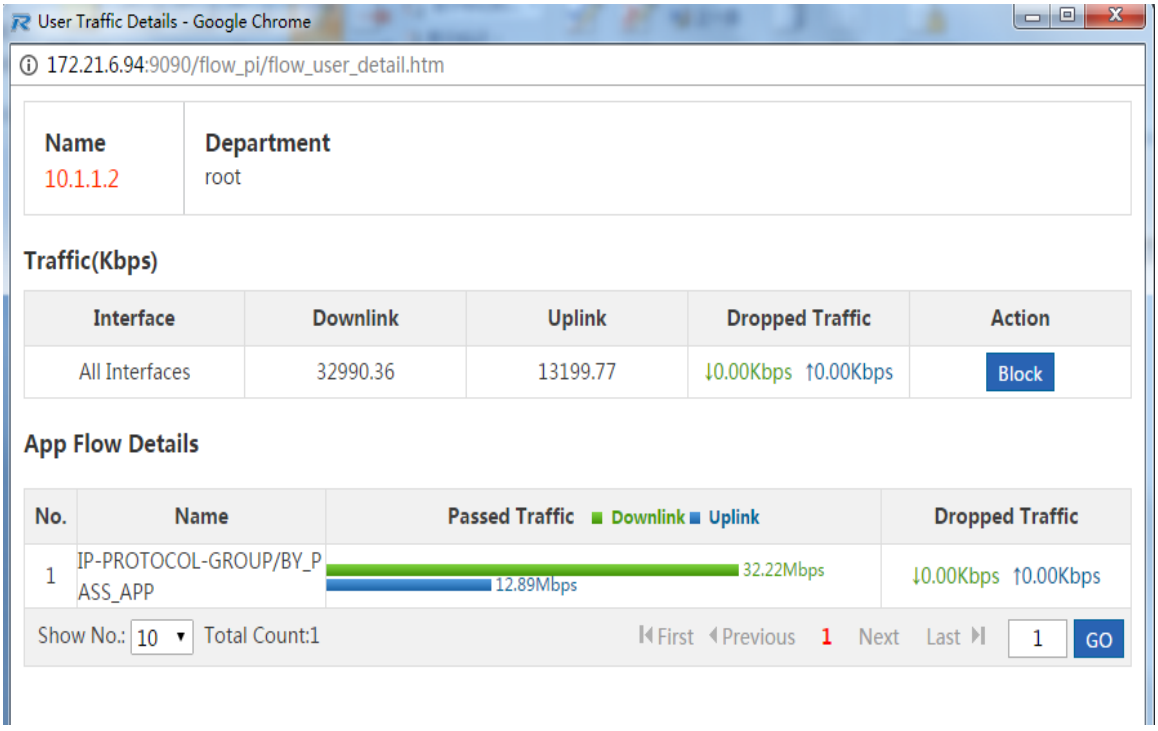



Select a value from the 

drop-down list to display information about the traffic of local users or authenticated users.

Click 

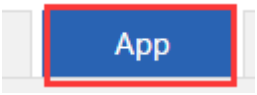
. A window shown in the figure below is displayed, and the traffic usage of the selected user, details about applications used by the selected user, and information about the traffic of each application are displayed.



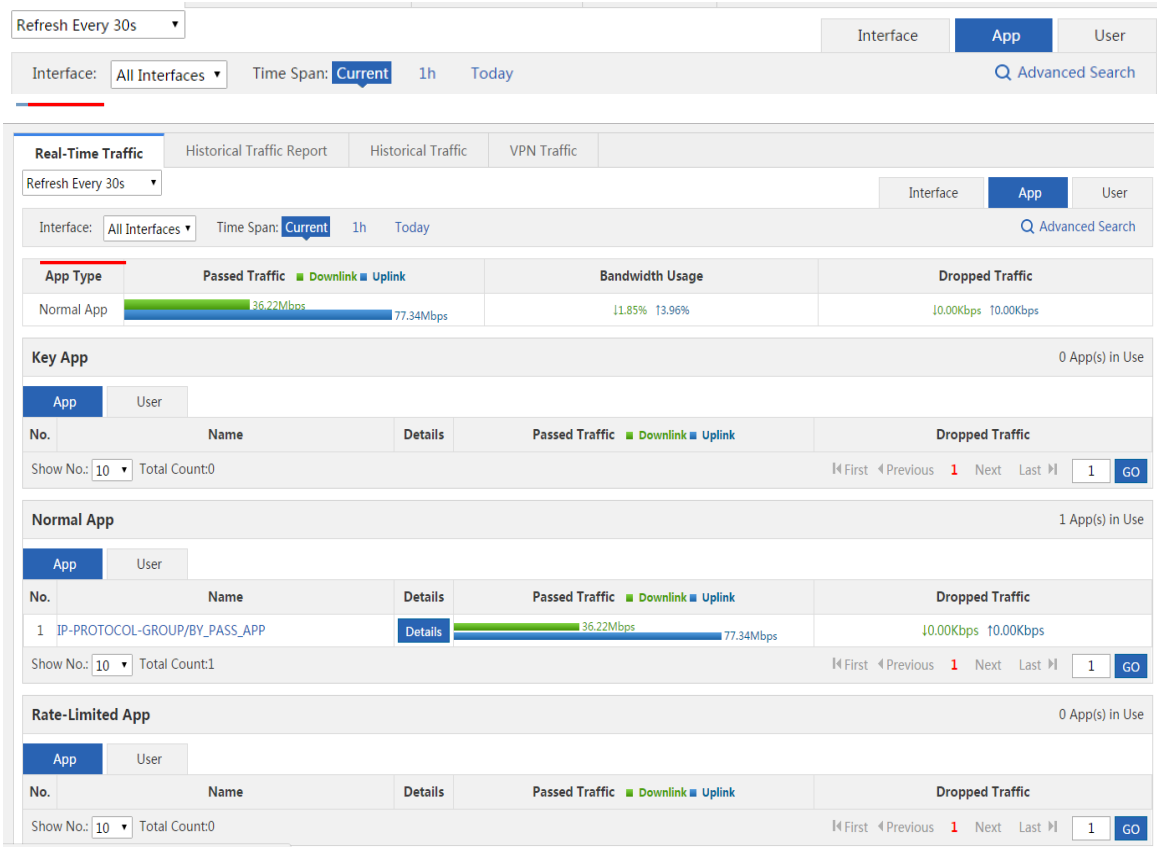

Click 

to block the traffic of the current user. After blocking, the subsequent traffic of the user will be thoroughly dropped by the interface.

- **Application Traffic Analysis**

The application traffic analysis function collects statistics on the bandwidth usage of different applications. You can control and analyze the traffic of an application to improve the traffic utilization rate. Click 

on the **Real-Time Traffic** page. A page shown in the figures below is displayed.

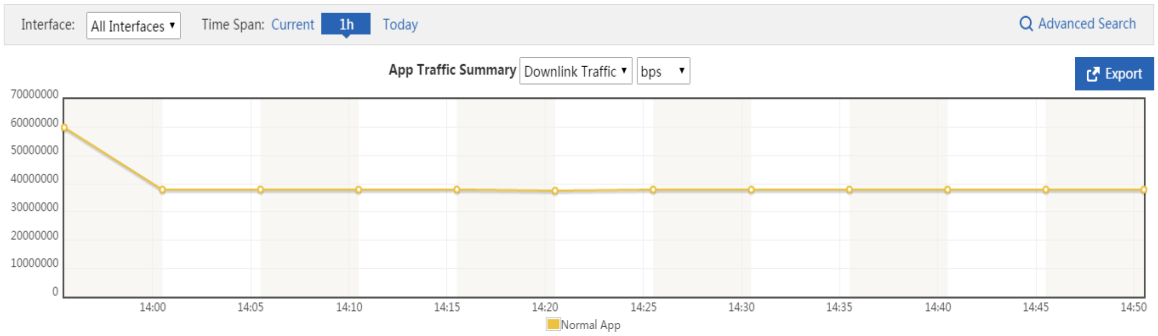



**Overview: The top area of the page displays information about the traffic of all interfaces, traffic of key applications, normal applications, and rate-limited applications.**


(1) Current traffic

As shown in the figure above, the page displays the traffic, bandwidth usage, and traffic dropped due to the rate limit policy for key applications, normal applications, and rate-limited applications on the selected interface.

(2) Traffic trend in the last one hour




| Type | Downlink | | | | Uplink | | | | Action |
|---|---|---|---|---|---|---|---|---|---|
| | Passed Traffic | Dropped Traffic | Average Bandwidth (Usage%) | Max Bandwidth Per IP (Uplink/Downlink) (Usage%) | Passed Traffic | Dropped Traffic | Average Bandwidth (Usage%) | Max Bandwidth Per IP (Uplink/Downlink) (Usage%) | |
| Normal App | 17.9GB | 60B | 37.93Mbps(1.94%) | 57.23Mbps(2.93%) | 35.45GB | 0B | 75.14Mbps(3.85%) | 77.37Mbps(3.96%) | Details |

The curve in the figure above shows the traffic trends of key applications, normal applications, and rate-limited applications in the last one hour on the selected interface. When you move the cursor over a point on the curve, the bandwidths used by applications of the three types at this point are displayed.

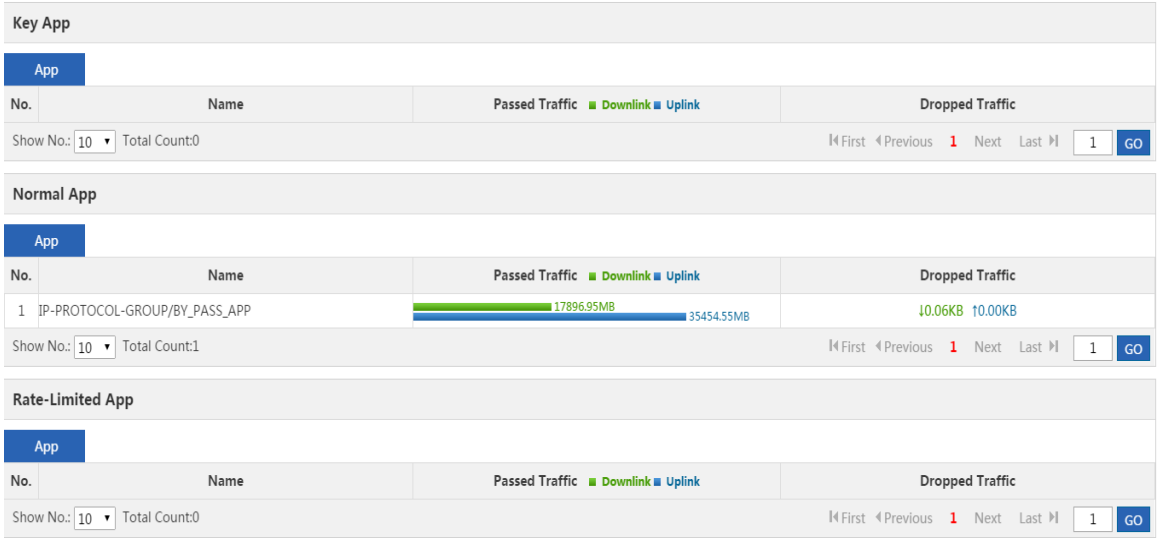
Click 

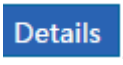
to export the traffic trend report to the local PC.

The table in the lower part lists the passed uplink/downlink traffic of applications of the three types on the selected interface in the last one hour, traffic dropped due to flow control, average bandwidth, and maximum bandwidth in the last one hour.

(3) Traffic trend on the current day: The traffic trend UI is the same as that for traffic in the last one hour except for the time range.

1. Key Applications: The area displays the details about the running key applications on the selected interface, traffic of each application, details about users who are using the key applications, and the traffic of each user.

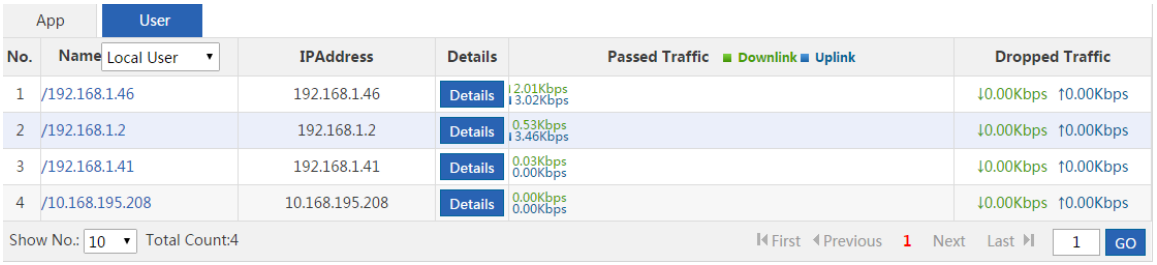


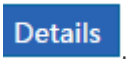

Click 

. The application traffic details window is displayed. For details, see the analysis of the application traffic details window in "Interface Traffic Analysis".

The figure above shows the traffic of key applications. Click **User** in 

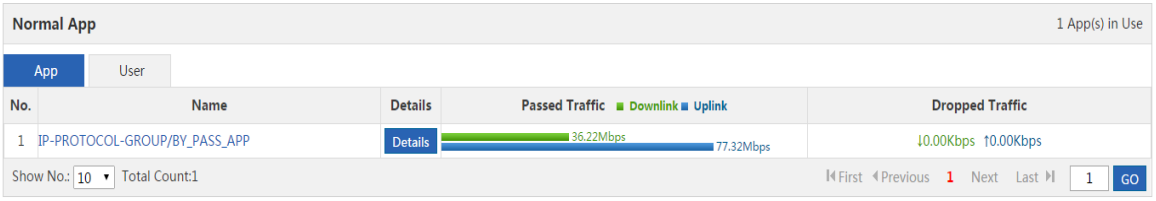
. Then, information about the traffic of users who are using the key applications on the interface is displayed.

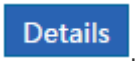



Click 

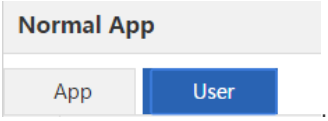
. The user traffic details window is displayed. For details, see the analysis of the user traffic details window in "Interface Traffic Analysis."

2. Normal Applications: The area displays the details about the running normal applications on the selected interface, traffic of each application, details about users who are using the normal applications, and traffic of each user.

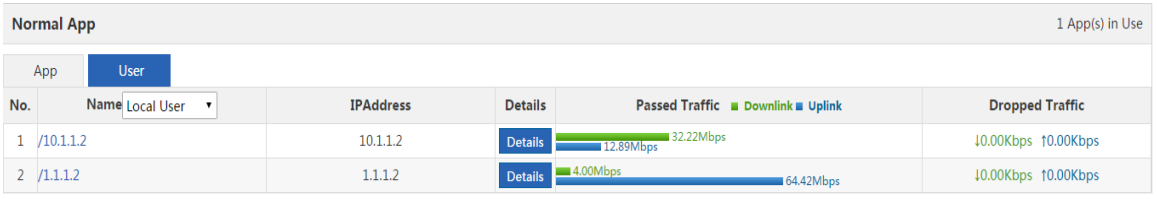


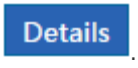

Click 

. The application traffic details window is displayed. For details, see the analysis of the application traffic details window in "Interface Traffic Analysis."

The figure above shows the traffic of normal applications. Click **User** in 

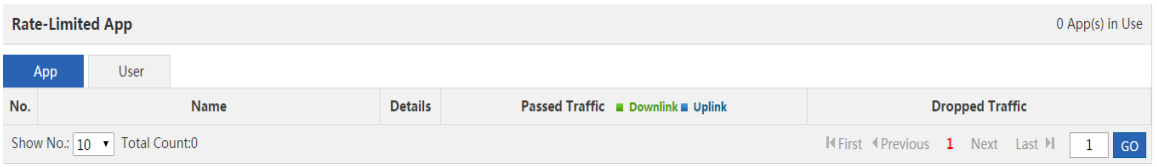
. Then, information about the traffic of users who are using the normal applications is displayed.



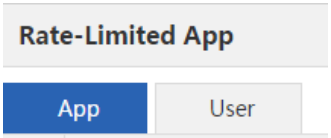

Click 

. The user traffic details window is displayed. For details, see the analysis of the user traffic details window in "Interface Traffic Analysis."

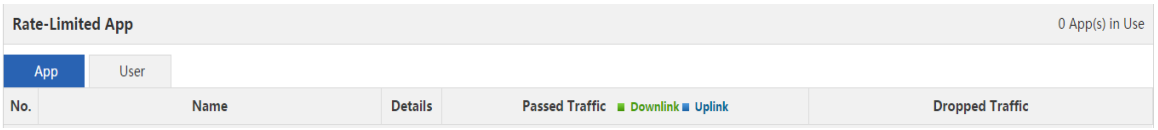
3. Rate-limited Applications: The area displays the details about the running rate-limited applications on the selected interface, traffic of each application, details about users who are using the rate-limited applications, and traffic of each user.




Click Details. The application traffic details window is displayed. For details, see the analysis of the application traffic details window in "Interface Traffic Analysis."

The figure above shows the traffic of rate-limited applications. Click **User** in 

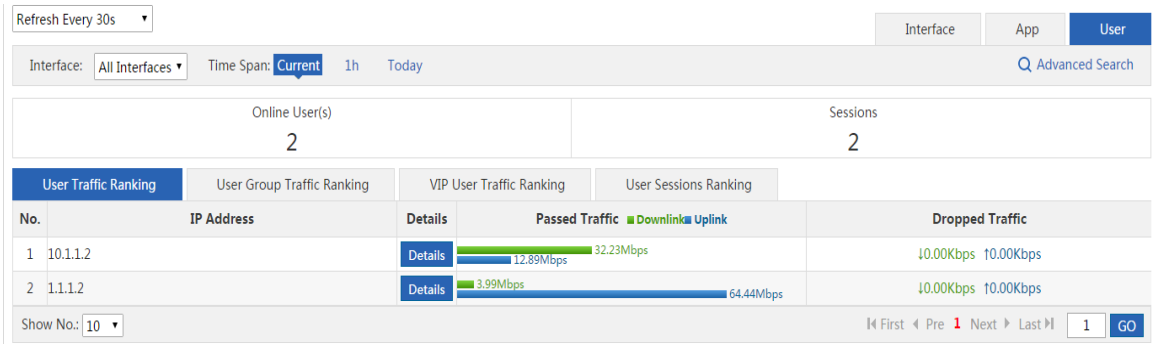
. Then, information about the traffic of users who are using the rate-limited applications is displayed.




Click Details. The user traffic details window is displayed. For details, see the analysis of the user traffic details window in "Interface Traffic Analysis."

- **User Traffic Analysis**

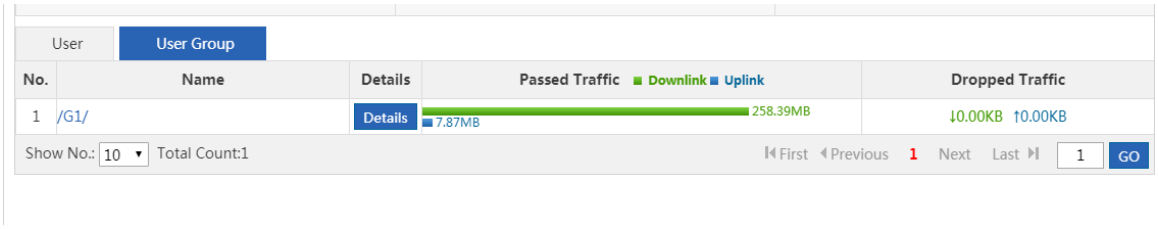
The user traffic analysis function analyzes user traffic by interface, monitors the current traffic of users in real time and details about the used applications, and adjusts user traffic simply, so as to rapidly restrict users with heavy traffic. If there are numerous users in the network, you can filter current users by username or IP address range. Click App User on the **Real-Time Traffic** page. A page shown in the figure below is displayed.



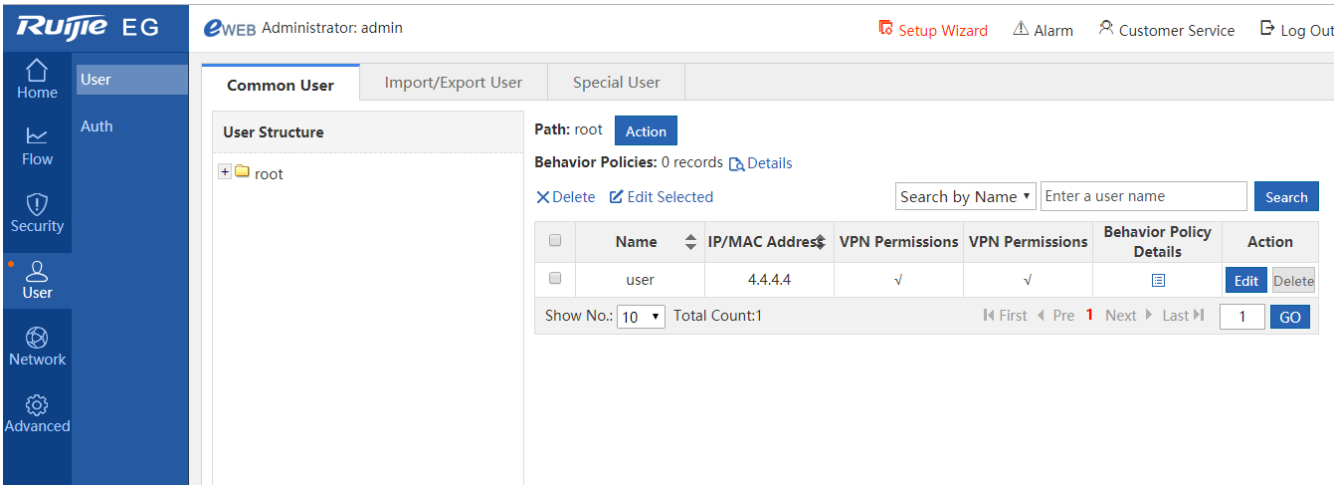

The page displays the number of online users, number of sessions, user traffic ranking, user group traffic ranking, VIP user traffic ranking, and user sessions ranking on the selected interface.

Click Details. The user traffic details window is displayed. For details, see the analysis of the user traffic details window in "Interface Traffic Analysis."

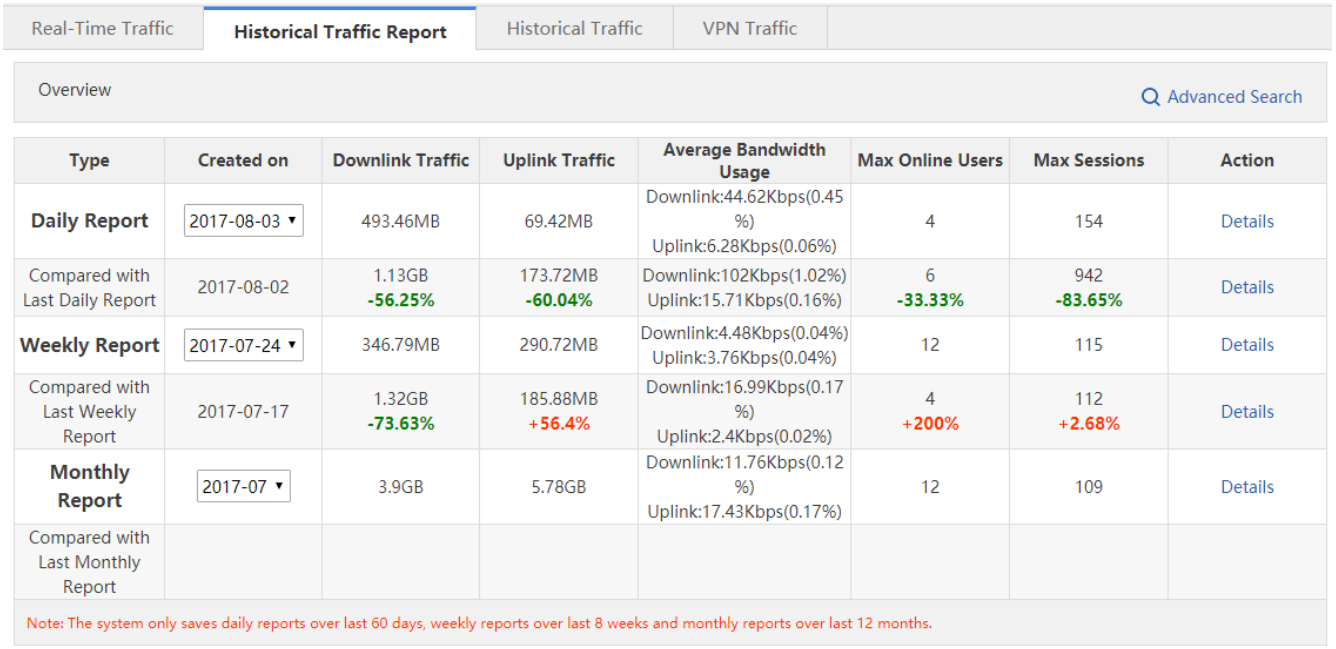
User group traffic: Users are divided into multiple groups (for example, by class, department, or floor). The EG device displays the traffic information and manages traffic by user group.




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



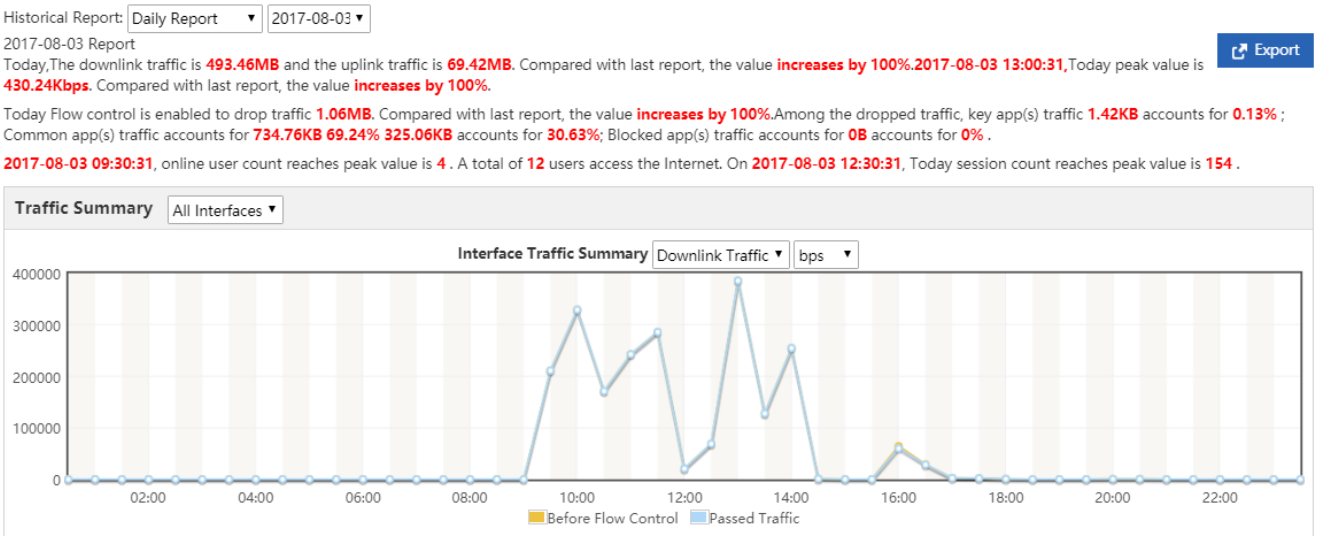

### 1.3.9.1.2 Historical Traffic Report



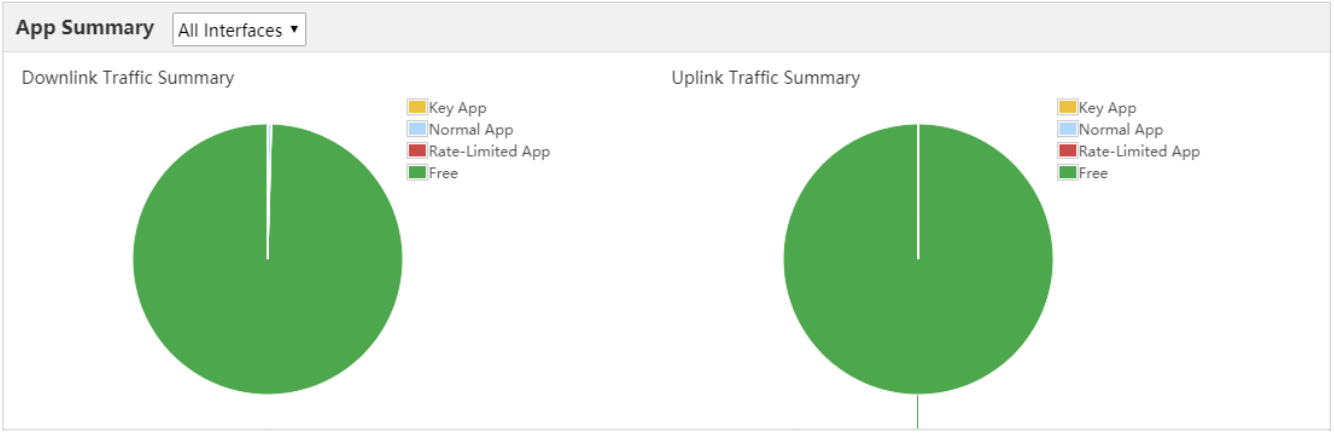

This page allows you to view daily reports in the last 60 days.

The daily reports show the total passed uplink/downlink traffic of all interfaces on one day, average bandwidth usage, maximum number of online users and maximum number of sessions within a specified time range. The daily report of the current period can be compared with that of the previous period.

Click Details to display specific traffic information, including the traffic trend of all interfaces, application traffic statistics, and user traffic statistics. You can also print and export reports.




| Type | Downlink | | | | Uplink | | | |
|---|---|---|---|---|---|---|---|---|
| | Passed Traffic | Dropped Traffic | Average Bandwidth (Usage%) | Max Bandwidth Per IP (Uplink/Downlink) (Usage%) | Passed Traffic | Dropped Traffic | Average Bandwidth (Usage%) | Max Bandwidth Per IP (Uplink/Downlink) (Usage%) |
| All Interfaces | 493.46MB | 1.06MB | 44.62Kbps(0.45%) | 376.49Kbps(3.76%) | 69.42MB | 0B | 6.28Kbps(0.06%) | 53.74Kbps(0.54%) |
| Gi0/6 | 493.46MB | 1.06MB | 44.62Kbps(0.45%) | 376.5Kbps(3.76%) | 69.42MB | 0B | 6.28Kbps(0.06%) | 53.74Kbps(0.54%) |



| Type | | Downlink | | | | Uplink | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Passed Traffic | Dropped Traffic | Average Bandwidth (Usage%) | Max Bandwidth Per IP (Uplink/Downlink) (Usage%) | Passed Traffic | Dropped Traffic | Average Bandwidth (Usage%) | Max Bandwidth Per IP (Uplink/Downlink) (Usage%) |
| Key App | All Interfaces | 2.76KB | 0B | 0bps(0.00%) | 0bps(0.00%) | 179.55KB | 0B | 17bps(0.00%) | 0bps(0.00%) |
| | Gi0/6 | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |
| | Gi0/7 | 2.76KB | 0B | 0bps(0.00%) | 11bps(0.00%) | 179.55KB | 0B | 17bps(0.00%) | 350bps(0.00%) |
| | Di1 | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |
| Rate-Limited App | All Interfaces | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |
| | Gi0/6 | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |
| | Gi0/7 | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |
| | Di1 | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |
| Normal App | All Interfaces | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |
| | Gi0/6 | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |
| | Gi0/7 | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |
| | Di1 | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) | 0B | 0B | 0bps(0.00%) | 0bps(0.00%) |

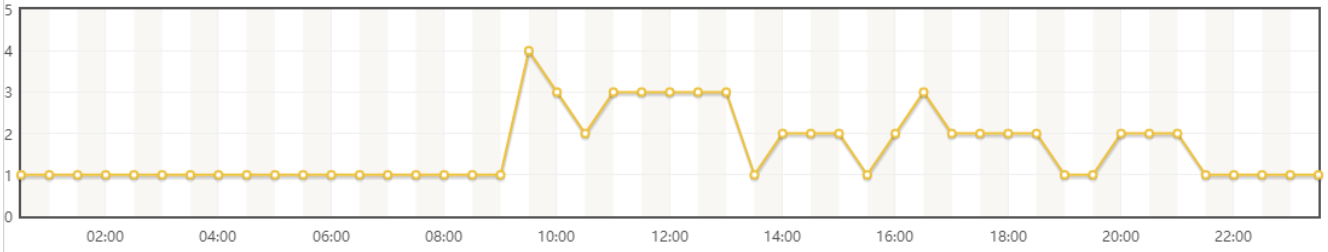
App | App Group

| No. | Name | Passed Traffic ■ Downlink ■ Uplink | Dropped Traffic |
|---|---|---|---|
| 1 | NetworkManagementProtocol/DNS | 2.75KB / 179.55KB | ↓0.00KB ↑0.00KB |

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

All Interfaces

Online Users | Sessions



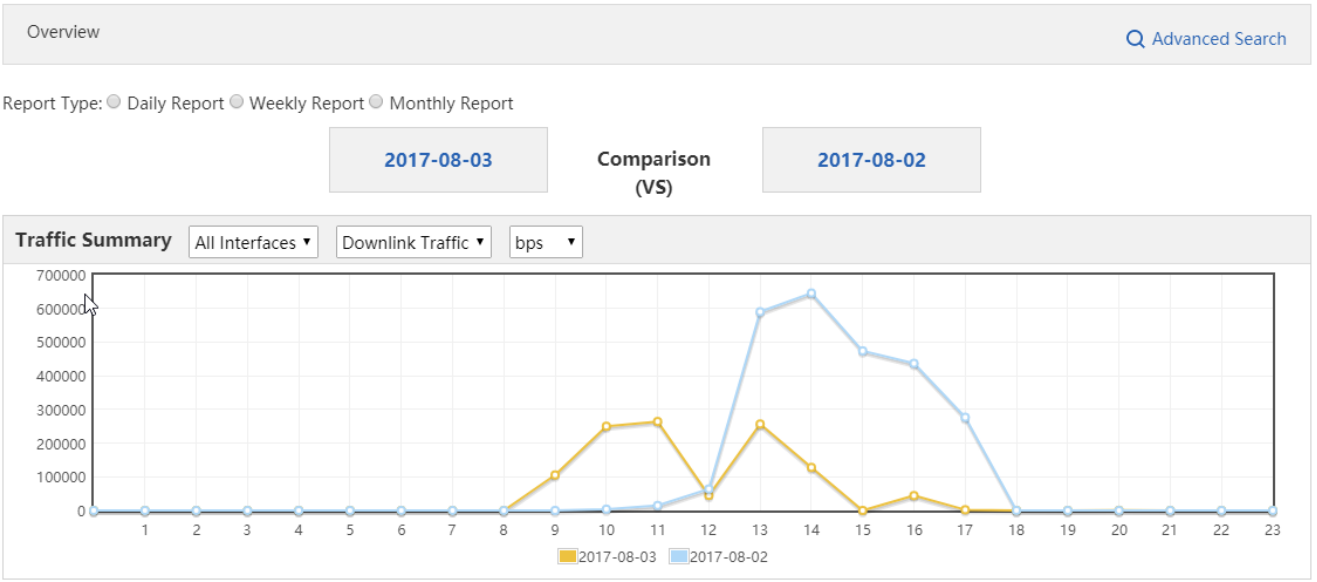

| Type | Peak | Average Per Minute |
|---|---|---|
| Online Users | 4 | 2 |
| Sessions | 154 | 14 |

User Traffic Ranking | User Group Traffic Ranking | VIP User Traffic Ranking

| No. | Name Local User | IP address | Passed Traffic ■ Downlink ■ Uplink | Dropped Traffic |
|---|---|---|---|---|
| 1 | /group10/ap1_user | 192.168.10.12 | 469.21MB / 66.53MB | ↓0.00KB ↑0.00KB |
| 2 | /group10/ap1_user | 192.168.10.2 | 20.56MB / 2.09MB | ↓1.06MB ↑0.00KB |
| 3 | /group10/ap1_user | 192.168.10.11 | 1.38MB / 315.53KB | ↓0.00KB ↑0.00KB |
| 4 | /group10/ap1_user/test1222 | 192.168.10.10 | 1.09MB / 227.57KB | ↓0.00KB ↑0.00KB |
| 5 | /192.168.1.8 | 192.168.1.8 | 614.46KB / 87.15KB | ↓0.00KB ↑0.00KB |

Click 

in the **Historical Traffic Report** page to display details about the comparison between the report of the current period and that of the previous period.

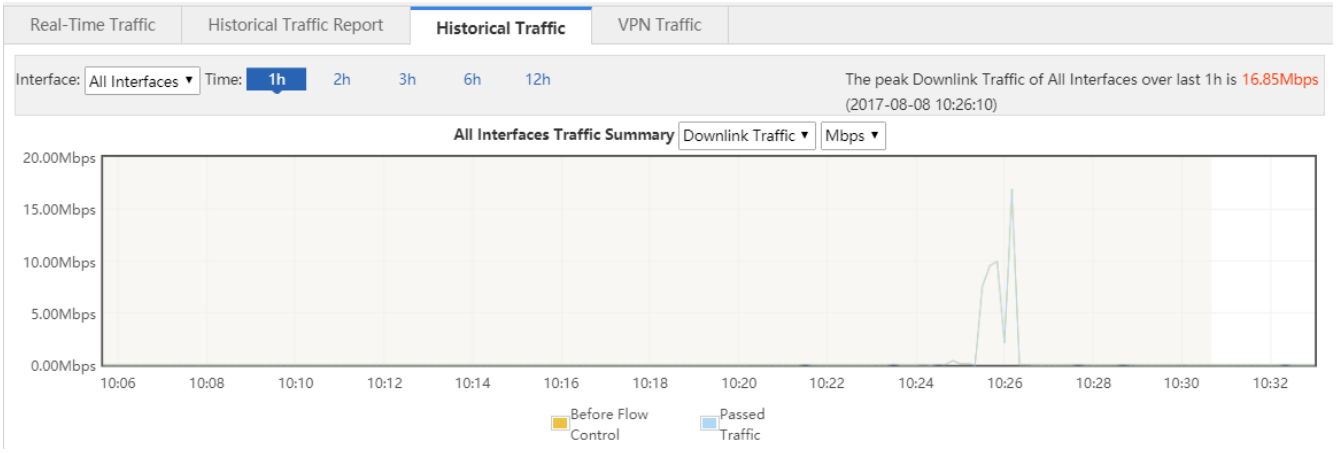



**Details**

| Type | 2017-08-03 | 2017-08-02 | Increase by |
|---|---|---|---|
| Total Traffic | 562.88MB | 1.3GB | -56.76% |
| Downlink Traffic | 493.46MB | 1.13GB | -56.25% |
| Uplink Traffic | 69.42MB | 173.72MB | -60.04% |
| Dropped Traffic | 1.06MB | 26.14MB | -95.94% |
| Average Bandwidth Usage | 0.25% | 0.59% | -0.33% |
| Average Rate | 50.9Kbps | 117.71Kbps | -56.76% |
| Max Rate | 430.24Kbps | 770.96Kbps | -44.19% |
| Average Online Users | 2 | 2 | 0% |
| Max Online Users | 4 | 6 | -33.33% |
| Average Sessions | 154 | 942 | -83.65% |
| Max Sessions | 154 | 942 | -83.65% |
| | Details | Details | |

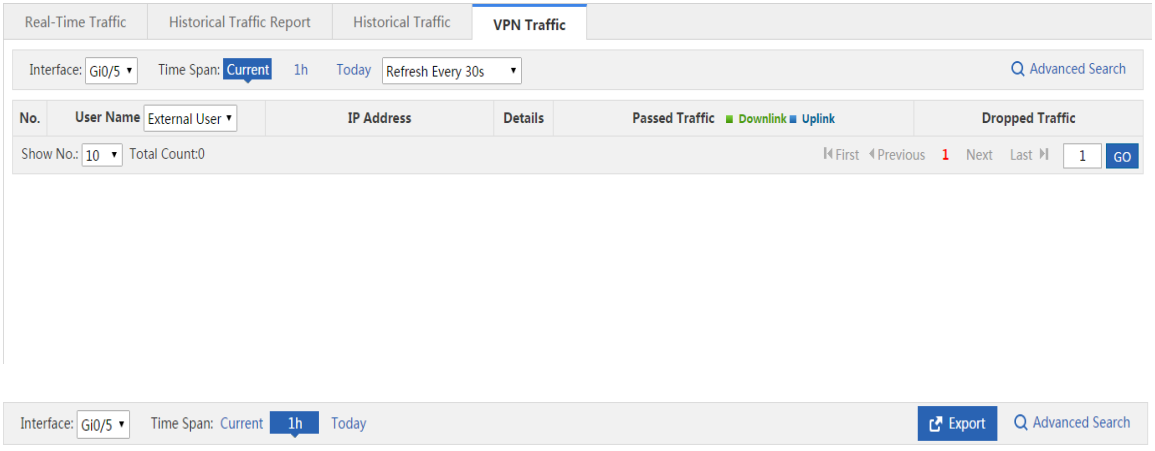
Back to Top | View Other Reports

### 1.3.9.1.3 Historical Traffic



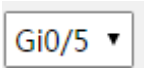

The interface traffic monitoring function displays the real-time interface traffic and specific real-time curve graph in the time unit. You can view the traffic curve monitored in real time of one day.

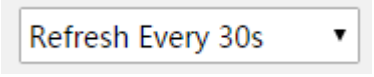
### 1.3.9.1.4 VPN Traffic





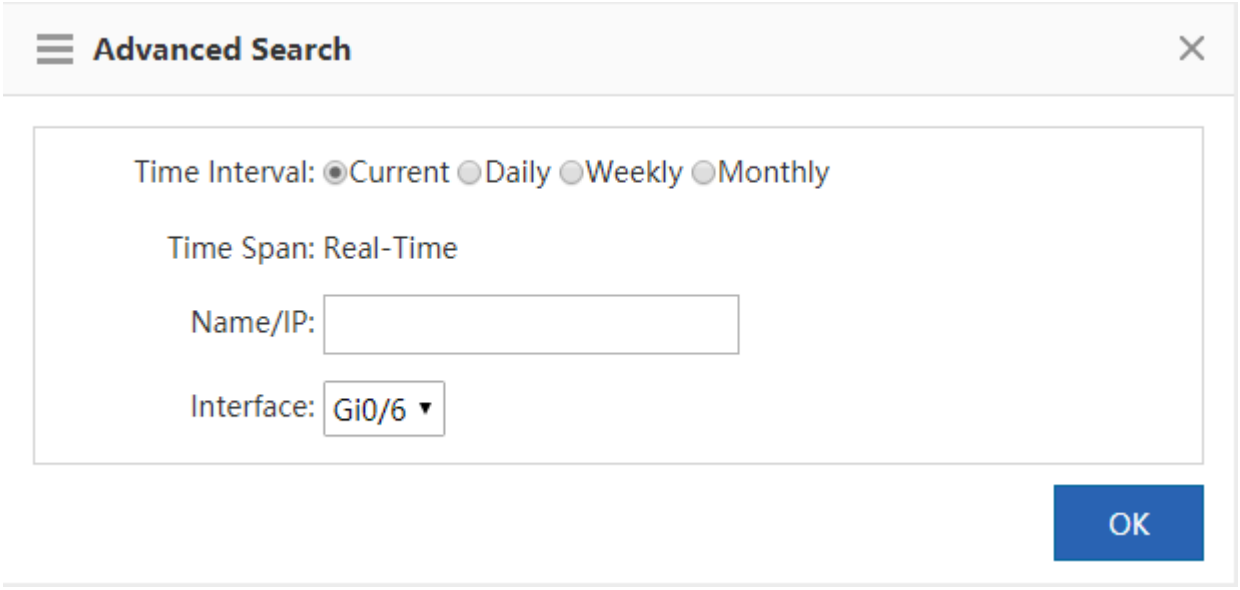


1. This page displays details about users who access the network via VPN dialup and information about the traffic of each VPN user.
2. Select a value from the 

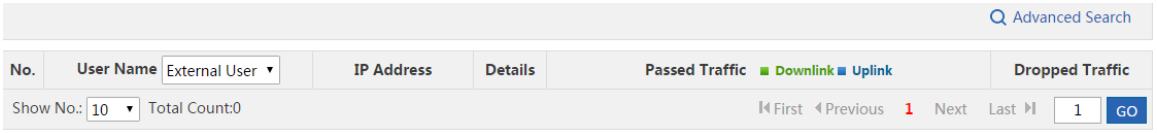
drop-down list to display the VPN traffic usage on an interface.
3. Select 10 seconds, 30 seconds, 1 minute from 

to update the current VPN traffic of the device or manually update the current VPN traffic of the device.
4. Click 

to query the traffic usage of a VPN user on an interface.

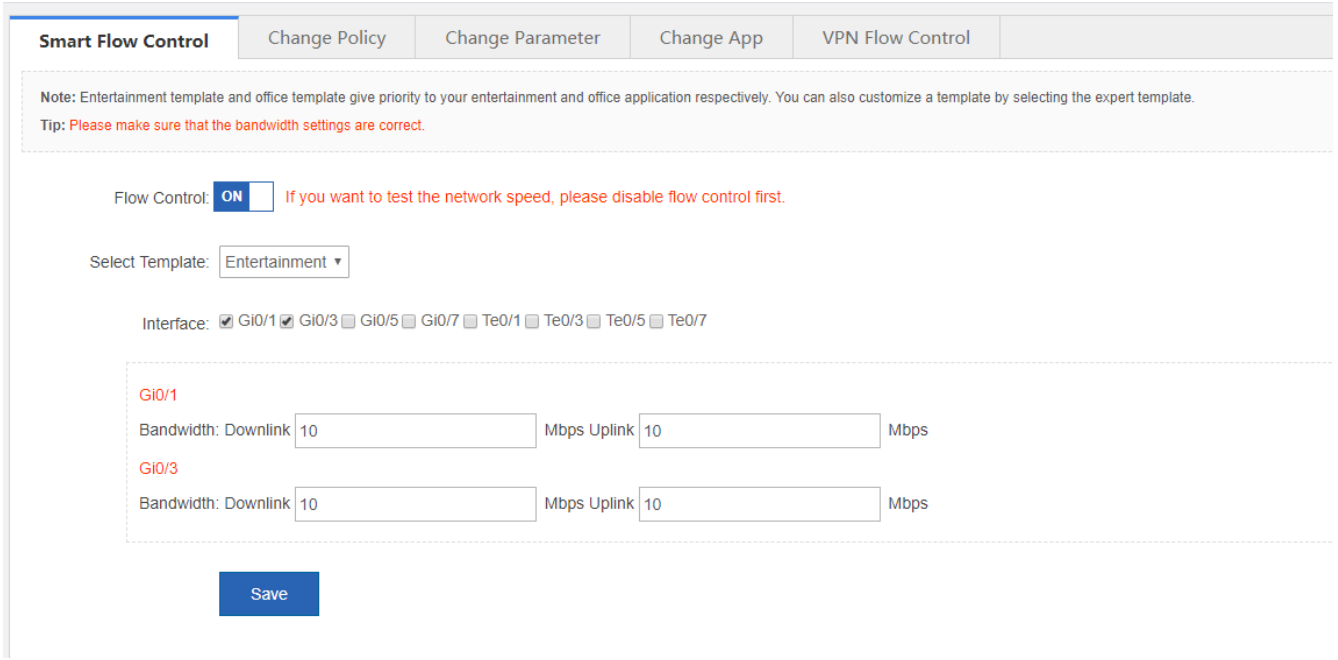



Enter a name or IP address, select a required interface, and click OK.



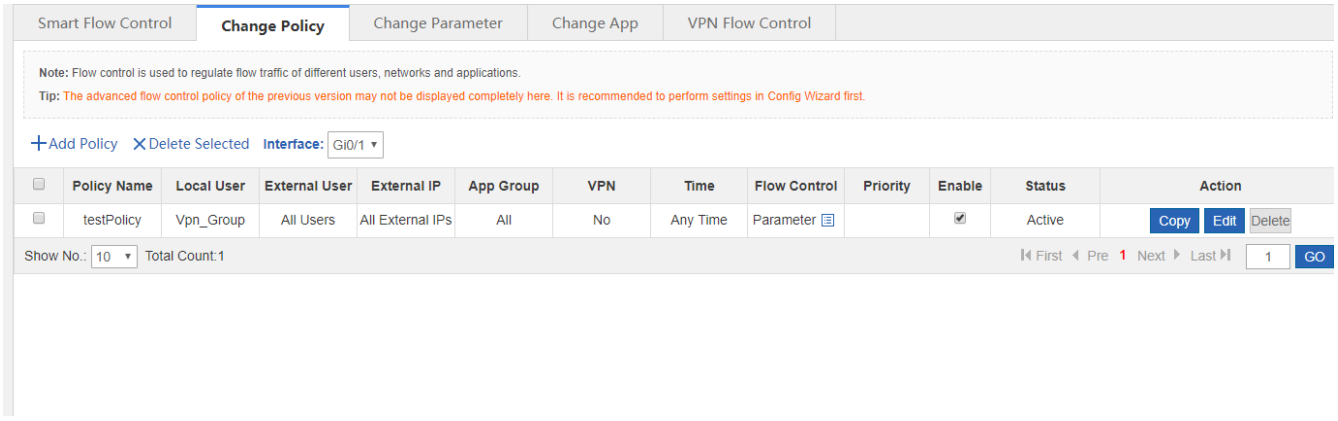

### 1.3.9.2 Flow Control Policy

#### 1.3.9.2.1 Smart Flow Control




Flow control templates are classified into Entertainment, Office and Expert templates. Entertainment template and office template give priority to your entertainment and office application respectively. You can also customize a template by selecting the Expert template.

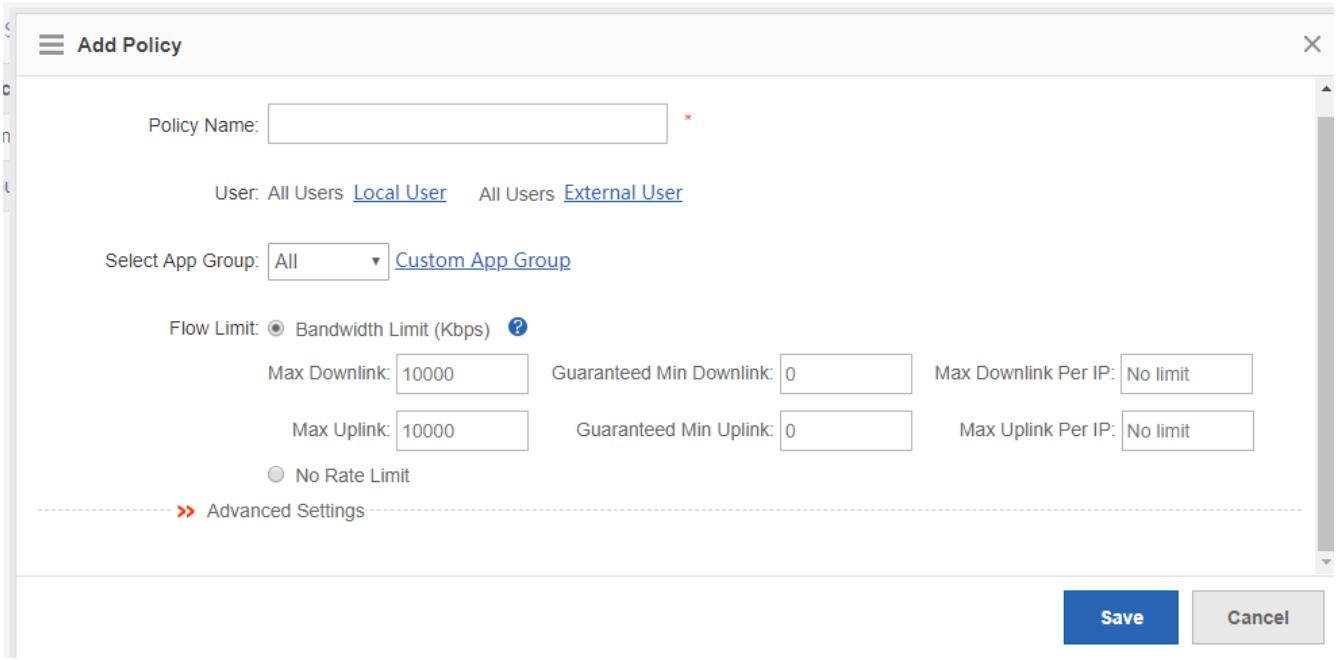
## 1.3.9.2.2 Change Policy

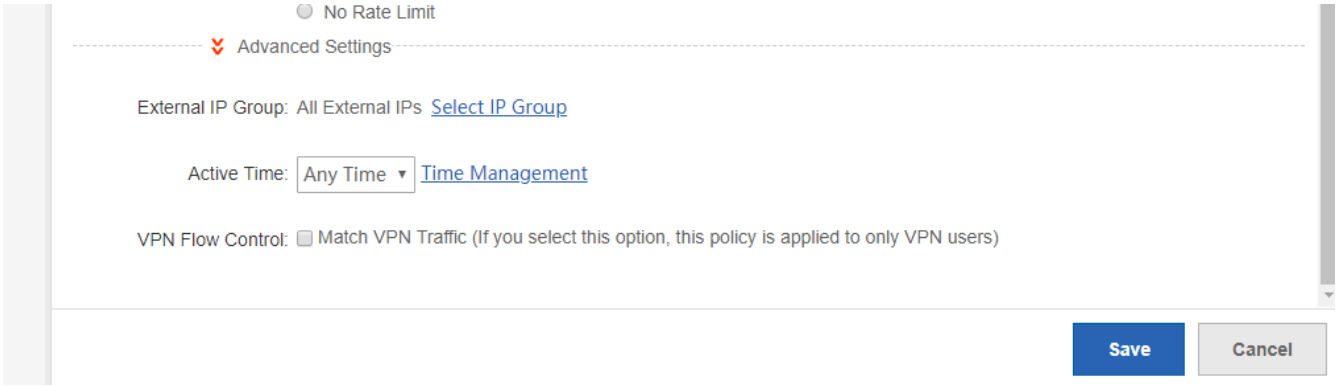



- Adding a policy

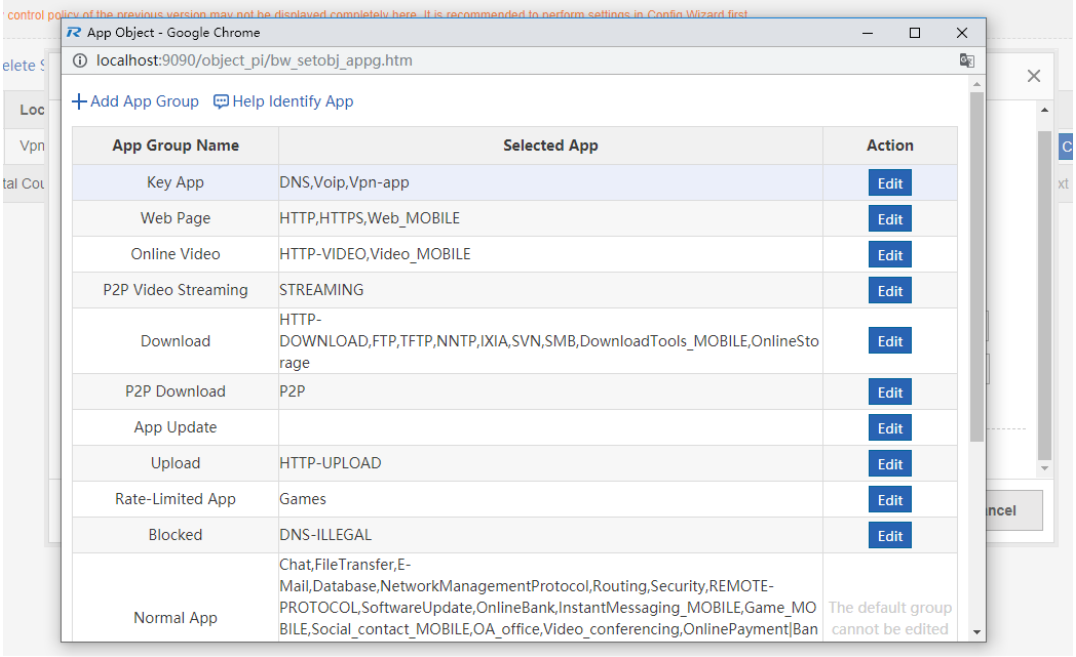
You can add a policy to manage internal network, users and applications according to network status and requirement.

Click Add Policy, and the **Add Policy** page will be displayed.




1. **Policy Name**: Enter a policy name in the **Policy Name** text box.
2. **Select App Group**: Select an application from the dropdown list. You can also customize an application by clicking Custom App Group.



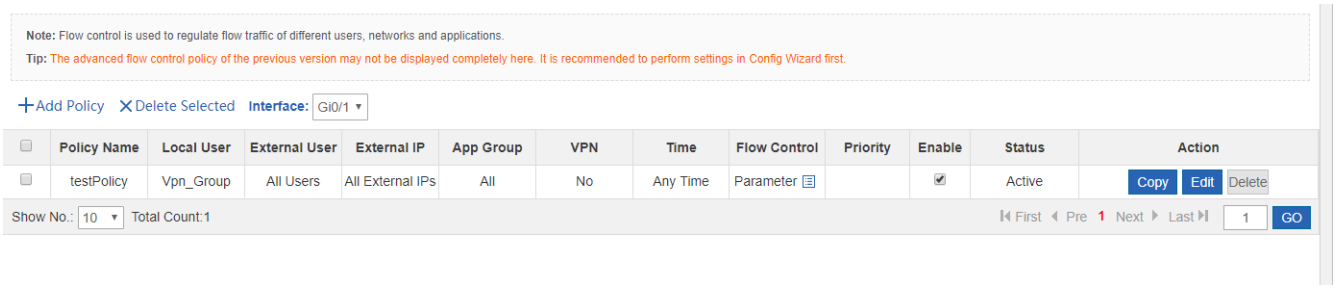

3. **Flow Limit**: Independent control, shared bandwidth, and no bandwidth limit.

4. **External IP Group**: Click Select IP Group to select an IP group.

5. **Active Time**: Select a time from the dropdown list. You can also customize the time by clicking Time Management.

- Viewing a policy

All flow control policies are contained in the list. You can delete or edit these policies.




1. Click in **App Group** to view details about this application group.

2. Enable or disable a policy by checking or unchecking the **Enable** box. If you disable a policy, its status will change to Inactive.

3. Status includes Active and Inactive. If the current time is not active time, the policy is inactive.

4. Click or to change the priority of policies. The first matched policy is ranked the top.

5. Click Edit to edit a policy.

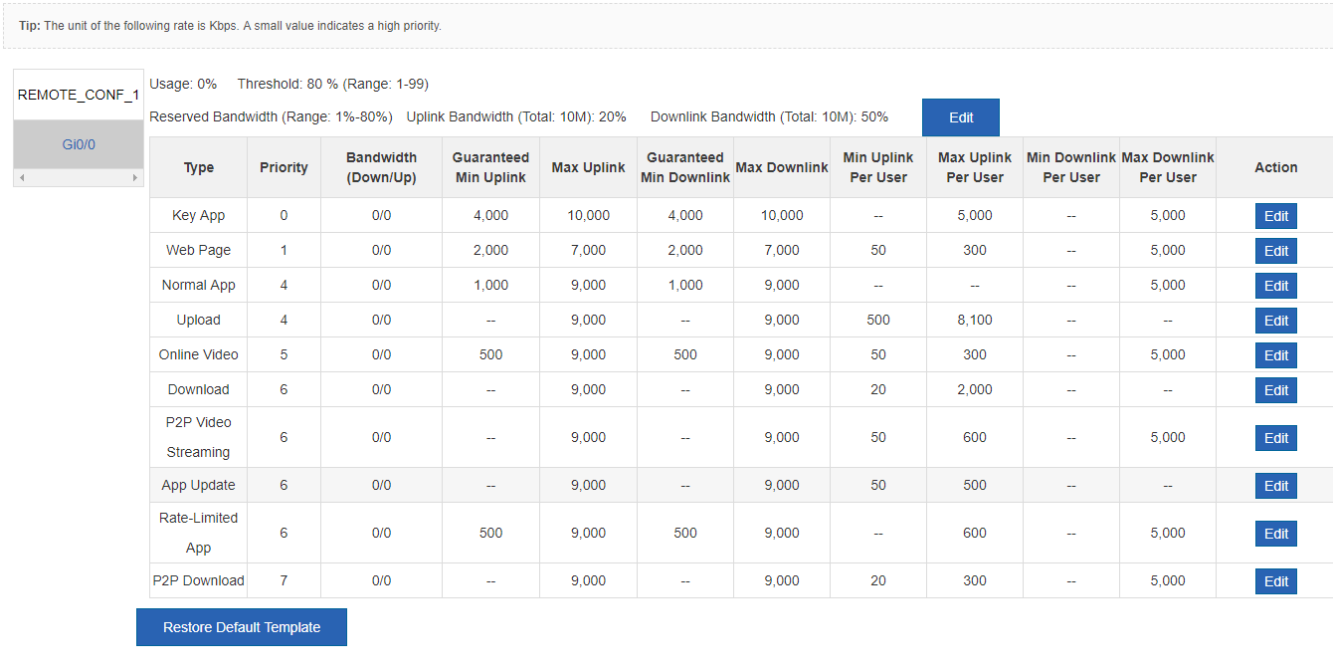
6. Click Delete to delete a policy.

- Copying a policy

Click Copy to copy a flow control policy of an interface to another interface.

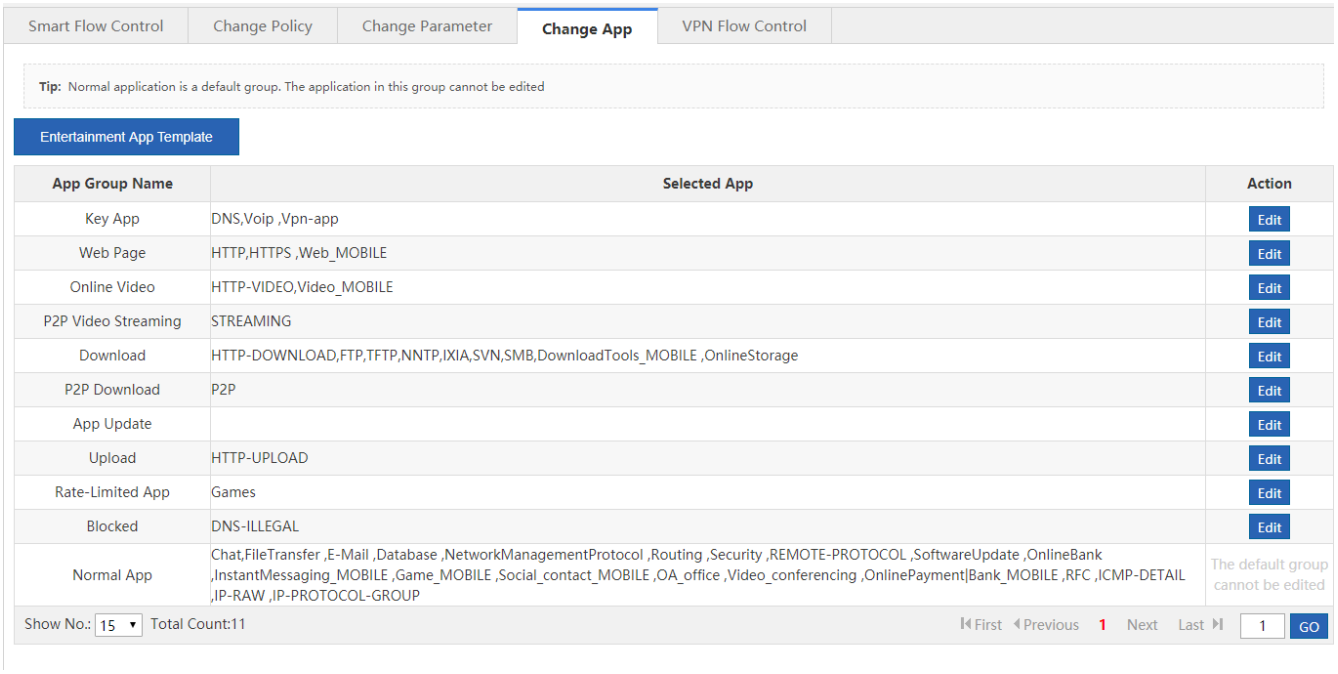

## 1.3.9.2.3 Change Parameter

You can edit settings according to real condition.

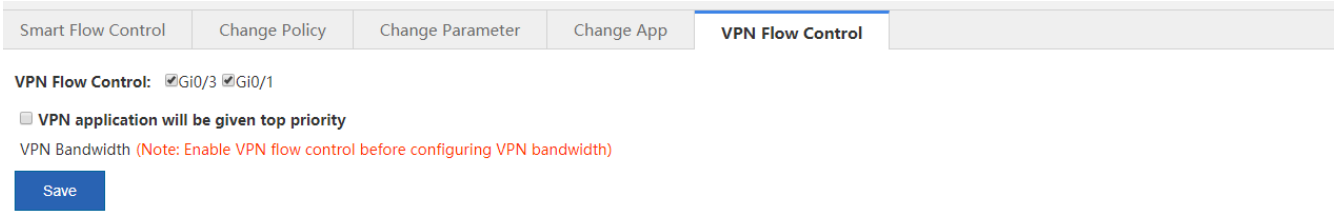



| Type | Priority | Bandwidth (Down/Up) | Guaranteed Min Uplink | Max Uplink | Guaranteed Min Downlink | Max Downlink | Min Uplink Per User | Max Uplink Per User | Min Downlink Per User | Max Downlink Per User | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Key App | 0 | 0/0 | 4,000 | 10,000 | 4,000 | 10,000 | -- | 5,000 | -- | 5,000 | Edit |
| Web Page | 1 | 0/0 | 2,000 | 7,000 | 2,000 | 7,000 | 50 | 300 | -- | 5,000 | Edit |
| Normal App | 4 | 0/0 | 1,000 | 9,000 | 1,000 | 9,000 | -- | -- | -- | 5,000 | Edit |
| Upload | 4 | 0/0 | -- | 9,000 | -- | 9,000 | 500 | 8,100 | -- | -- | Edit |
| Online Video | 5 | 0/0 | 500 | 9,000 | 500 | 9,000 | 50 | 300 | -- | 5,000 | Edit |
| Download | 6 | 0/0 | -- | 9,000 | -- | 9,000 | 20 | 2,000 | -- | -- | Edit |
| P2P Video Streaming | 6 | 0/0 | -- | 9,000 | -- | 9,000 | 50 | 600 | -- | 5,000 | Edit |
| App Update | 6 | 0/0 | -- | 9,000 | -- | 9,000 | 50 | 500 | -- | -- | Edit |
| Rate-Limited App | 6 | 0/0 | 500 | 9,000 | 500 | 9,000 | -- | 600 | -- | 5,000 | Edit |
| P2P Download | 7 | 0/0 | -- | 9,000 | -- | 9,000 | 20 | 300 | -- | 5,000 | Edit |

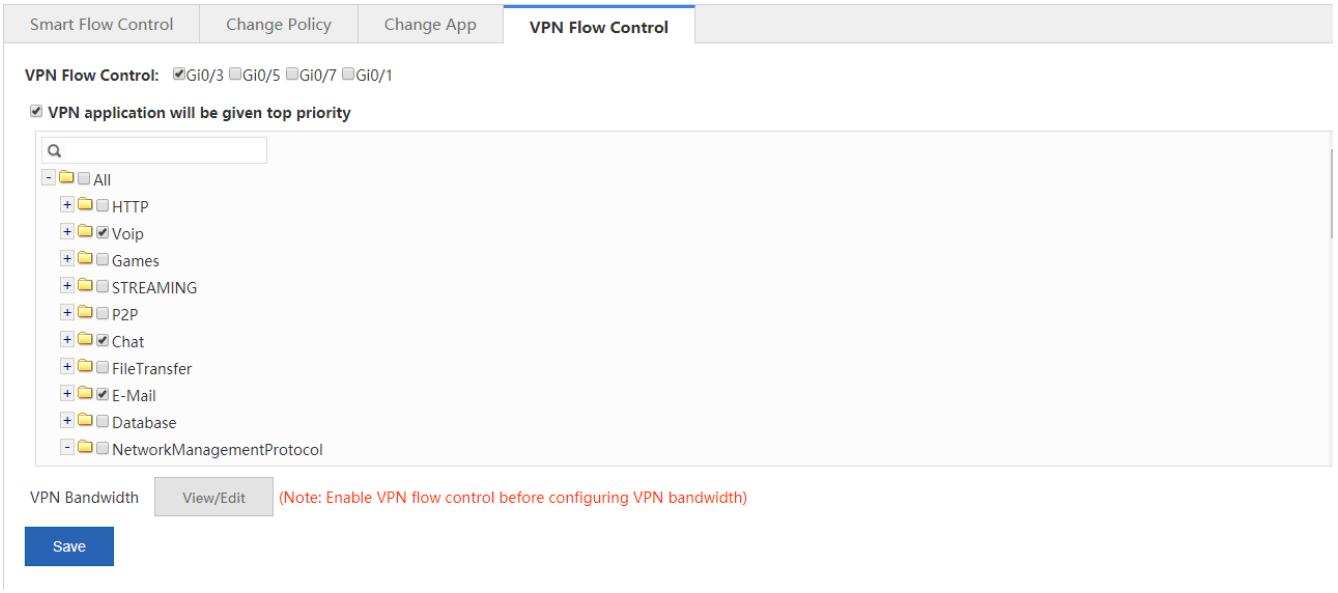
## 1.3.9.2.4 Change App




## 1.3.9.2.5 VPN Flow Control

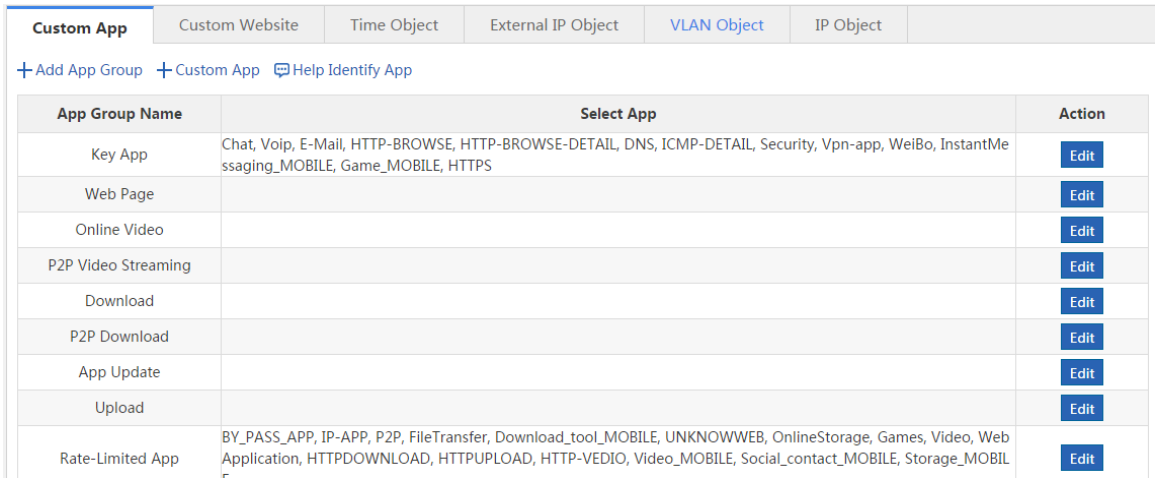



Click **View/Edit** to view details. You can also edit the settings here.

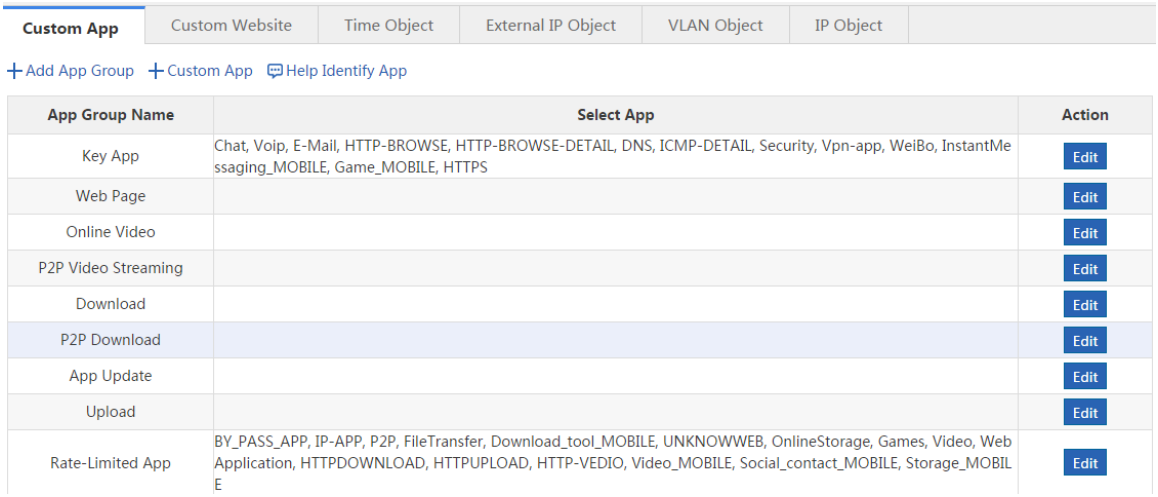



### 1.3.9.3 Object

The object configuration page is shown in the figure below.



### 1.3.9.3.1 Custom App

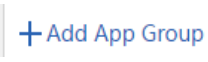



This page lists all application groups and applications contained in each application group in the system. Application groups of the key type, rate-limited type, block type, and normal type are application groups defined in the system and applications of other types are custom application groups.

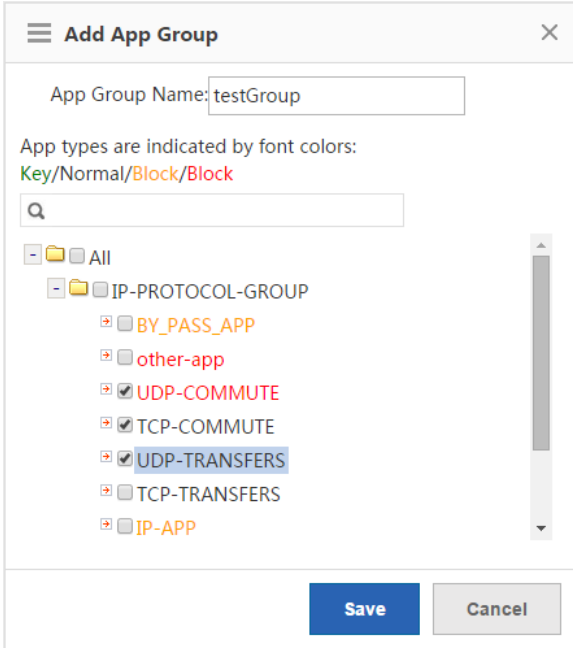
- **App Group**

Application groups help users to plan and manage the use of internal applications conveniently. It ensures smooth LAN access and prevents bandwidth waste.

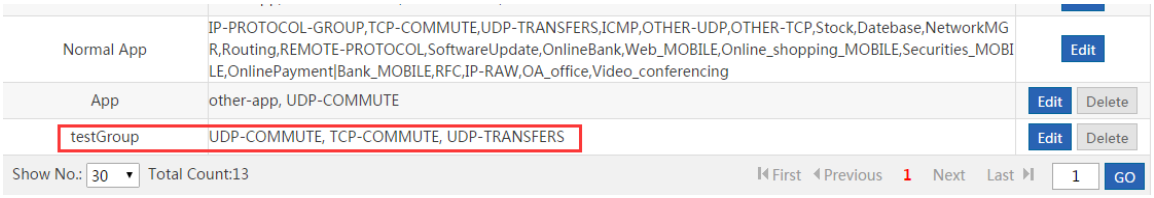
1. Adding a custom application group

Click  to custom an application group.



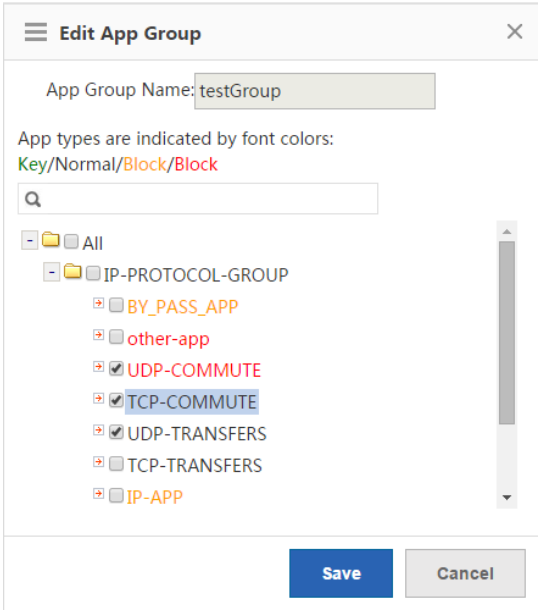


Enter a name in **App Group Name** and click **Save**. Then, the application group is displayed in the list.

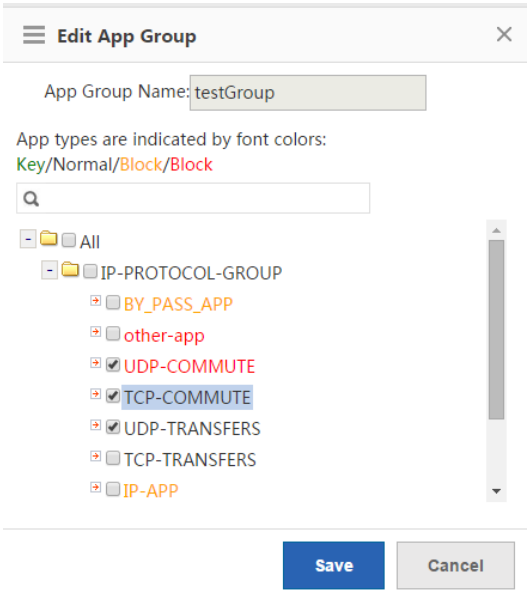



2. Editing an application group

Click Edit in a row of the list on the custom application group page to re-custom applications contained in an application group.




In the application group tree, add applications to or remove applications from the application group, and click Save.




Different colors of application names indicate different types of applications as follows:

Green: key applications

Orange: rate-limited applications

Red: blocked applications

Black: normal applications or deselected applications

Applications of the key type, rate-limited type, or blocked type can only be added to one application groups at the same time.

For example, if an application of the rate-limited type needs to be changed to the key type, delete the application from the rate-limited application group, and then add it to the key application group.

3. Deleting an application group

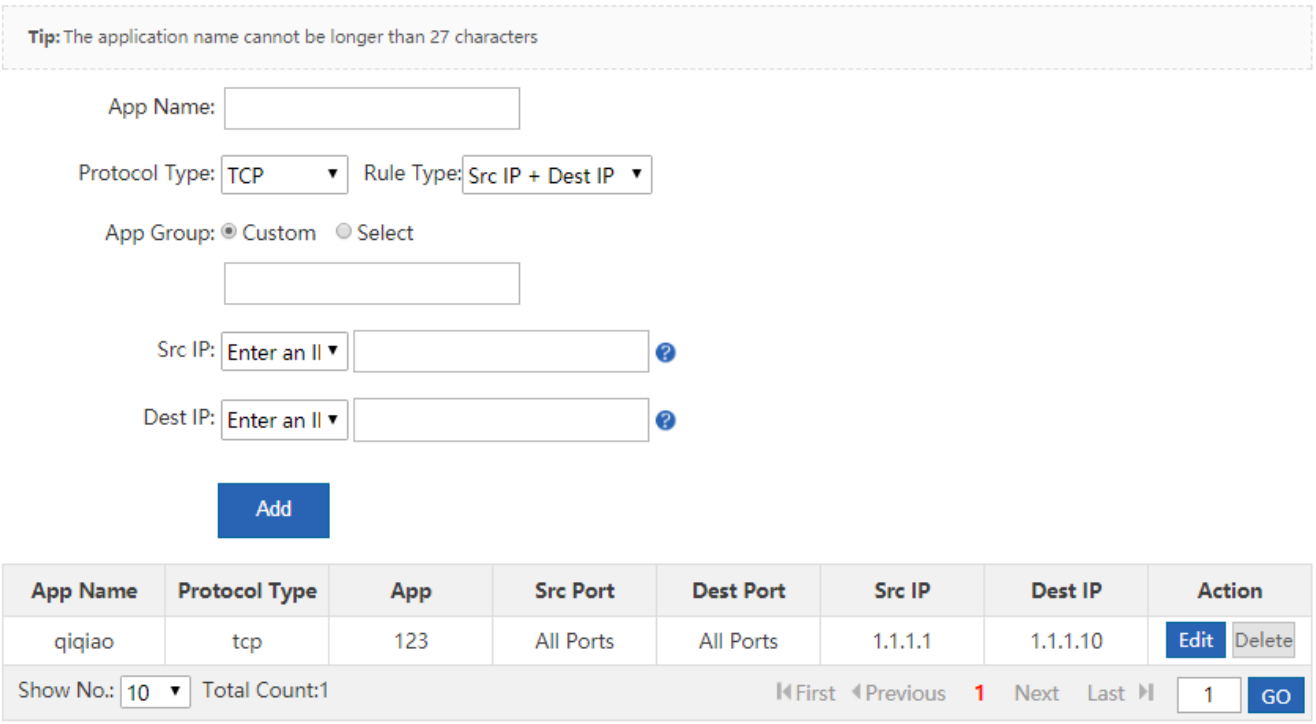
Click Delete in a row of the list on the custom application group page to delete a custom application group. The system application groups (that is, application groups of the key type, rate-limited type, blocked type, and normal type) cannot be deleted.

- **Custom App**

Apart from built-in network applications in the system, you can custom other network applications, for example, a port-based application or a target server-based application. Both built-in applications in the system and custom applications can be used for network application control, bandwidth management, and real-time network application monitoring in policies.

Note: Custom applications have the highest priority. That is, when a custom application collides with a built-in system application (for example, on the same port), the system prioritizes the custom network application.

On the **Custom App** page, click + Add Custom App. The custom application configuration page is displayed.

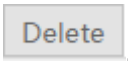



Create a custom application object: Enter a custom application name, set **Protocol Type**, **Rule Type**, and **App Group** (self-define an application type or use a built-in application type), enter the source or destination port and source or destination IP address based on the selected rule type, and click 

.

Edit a custom application: Select an application to be modified and click 

.

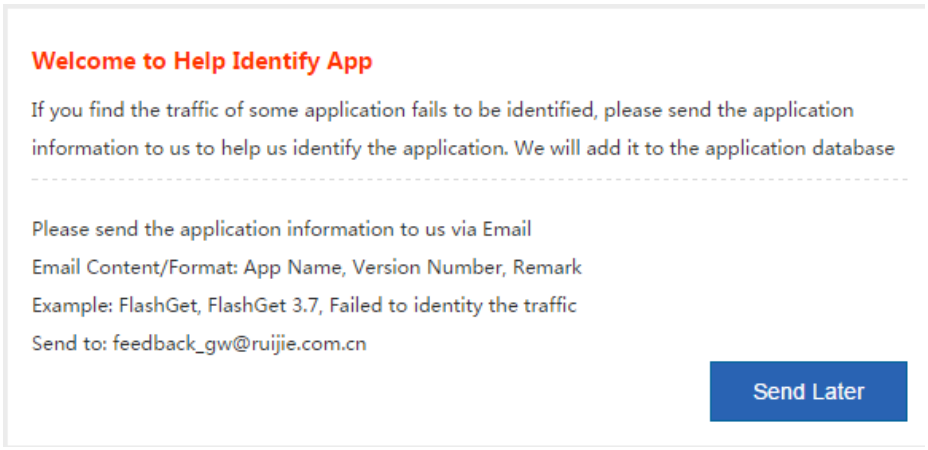
Delete a custom application: Select an application to be deleted and click 

.

- **Help Identify App**

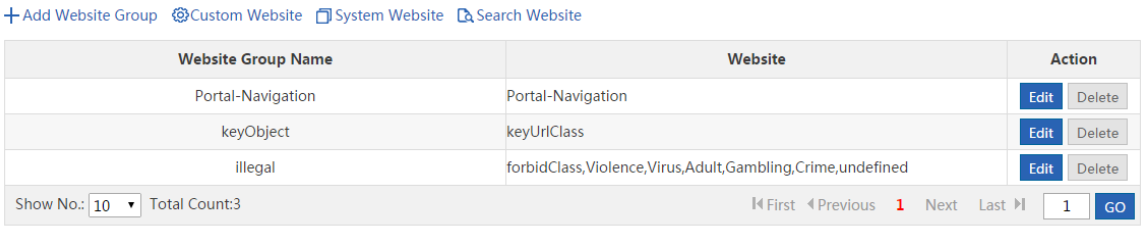
If the device cannot correctly identify the traffic of a network application,, click 

, and provide feedback as prompted. Ruijie Cloud Center will analyze the reported application and add it to the signature database to meet your requirements.




### 1.3.9.3.2 Custom Website

The **Custom Website** configuration page is shown in the figure below. This page displays all existing website groups and websites contained in each website group.



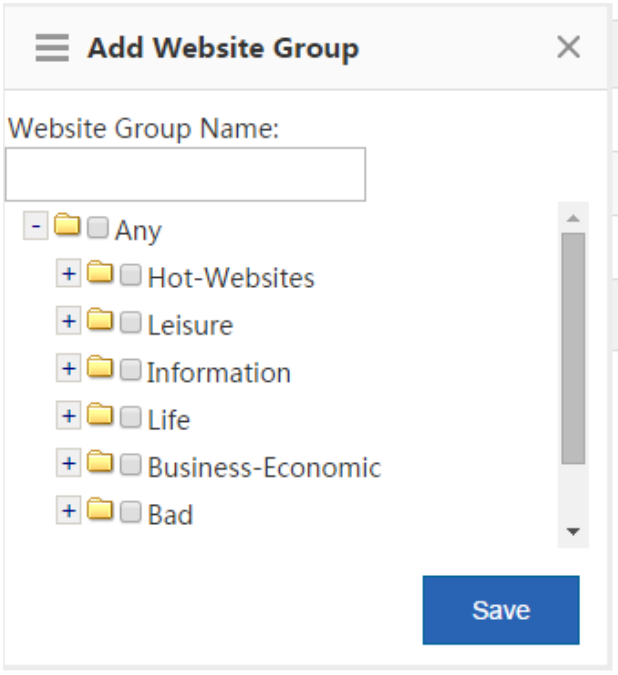

- **Website Group**

Website groups help users to plan and manage types of websites accessed by LAN users conveniently. It ensures smooth LAN access and prevents bandwidth waste.

1. Adding a website group

Click 

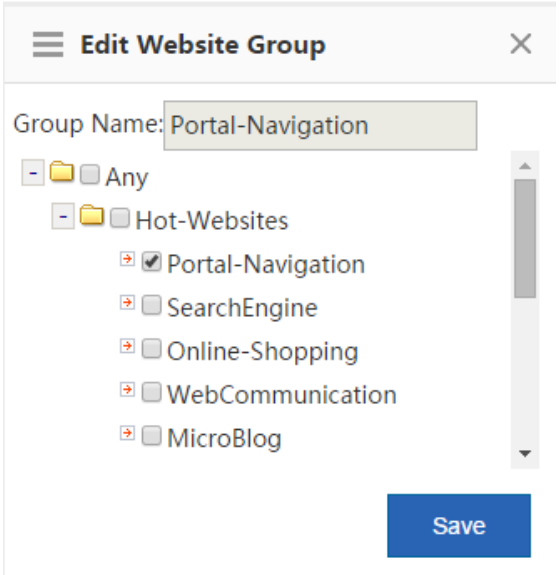
to custom a website group.




Enter the website group name, select the website types to be contained in the website group, and click Save.

2. Editing a website group

Click Edit in a row of the list on the custom website group page to edit the website types contained in a website group.




In the website group tree, add websites to or remove websites from the application group, and click Save.

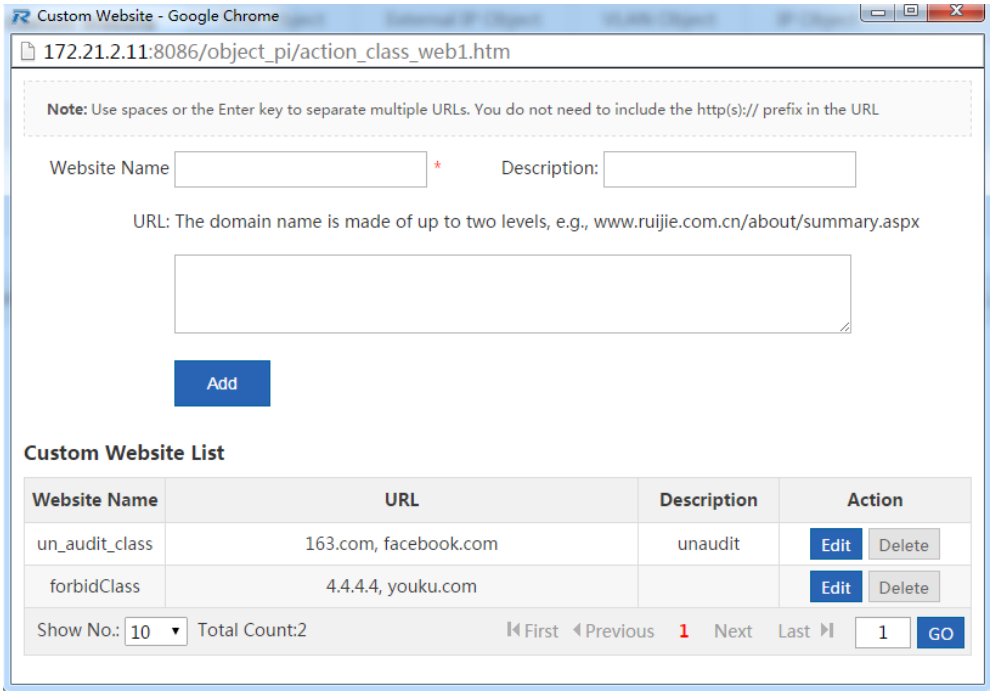
3. Deleting a website group

Click Delete in a row of the list on the custom website group page to delete the selected website group.

- **Custom Website**

Apart from built-in websites in the system, you can custom other websites, for example, classify several similar websites into one type. Both custom and built-in websites of the system can be applied to behavior policies.

On the **Custom Website** page, click Custom Website. The custom website configuration window is displayed.



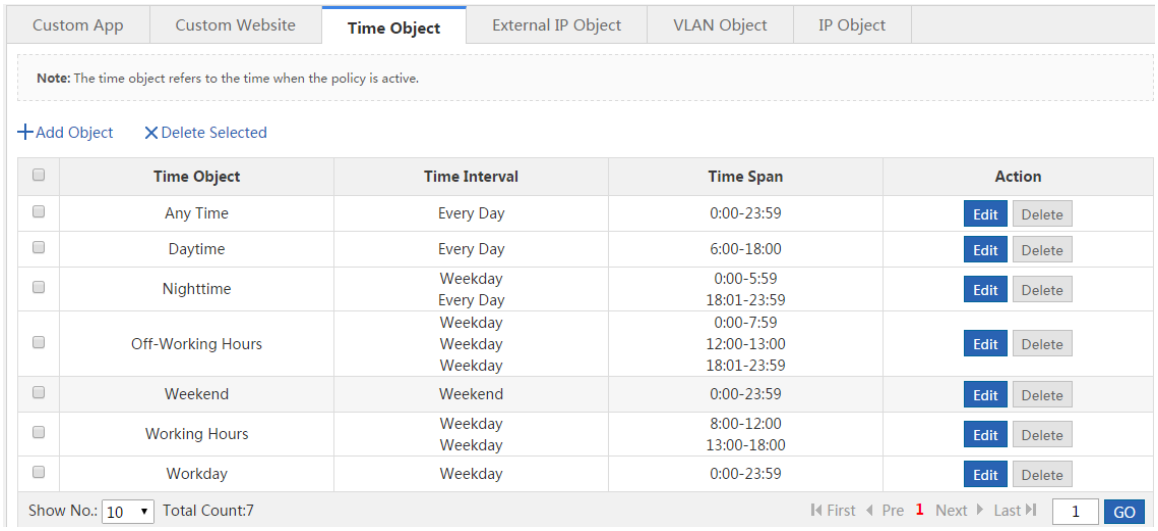

Create a custom website: Enter the website name, description, and website domain names contained in the website (separate multiple domain names by a comma (,)), and click Add. A maximum of 100 custom websites can be configured in the system.

Edit a custom website type: Select a website type to be modified and click Edit.

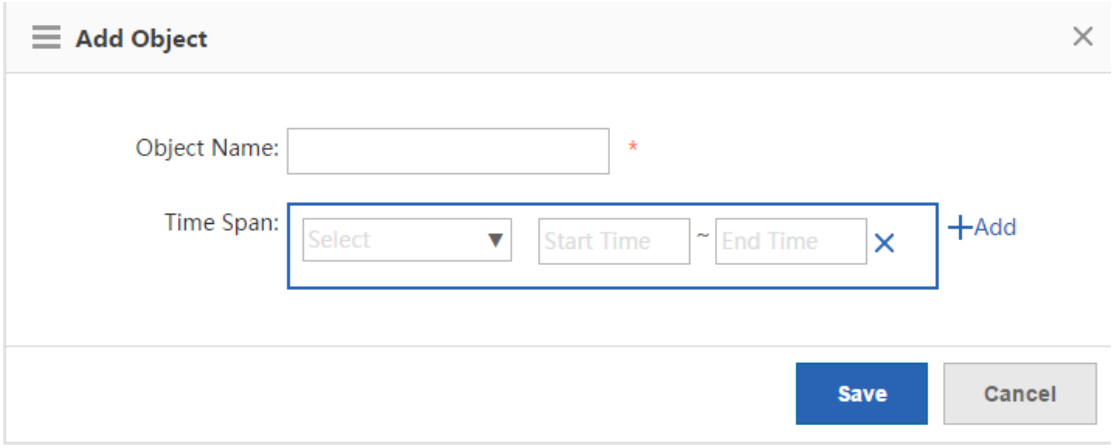
Delete a custom website type: Select a website to be deleted and click Delete.

### 1.3.9.3.3 Time Object

On the **Time Object** page, you can custom a time object for setting a policy.



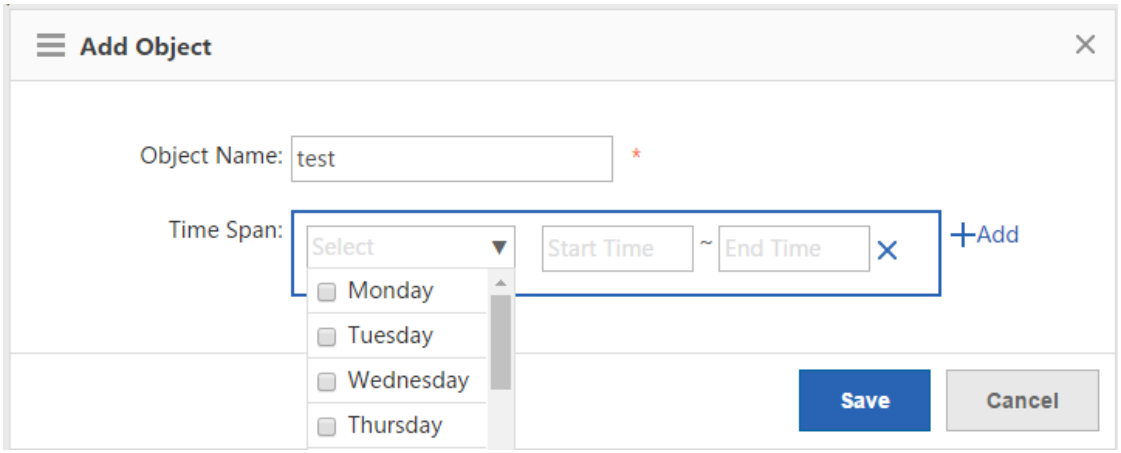

1. Add a time object: Click  . In the **Add Object** dialog box, enter the object name and set a time span. Multiple time spans can be set.



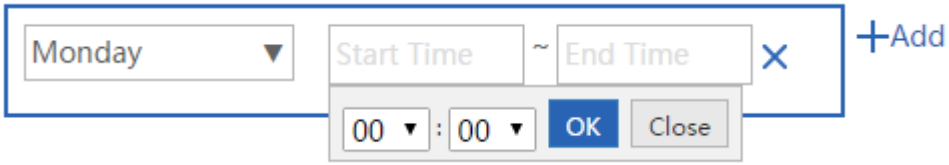

For example, to create a work time object:

(1) Object name: Enter a time object name in  .

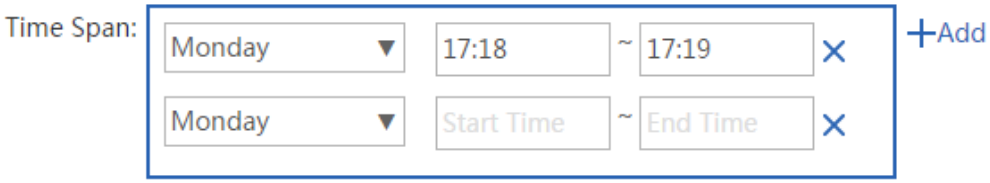
(2) Time span period: Select the period of a time span, that is, select from Monday to Sunday.



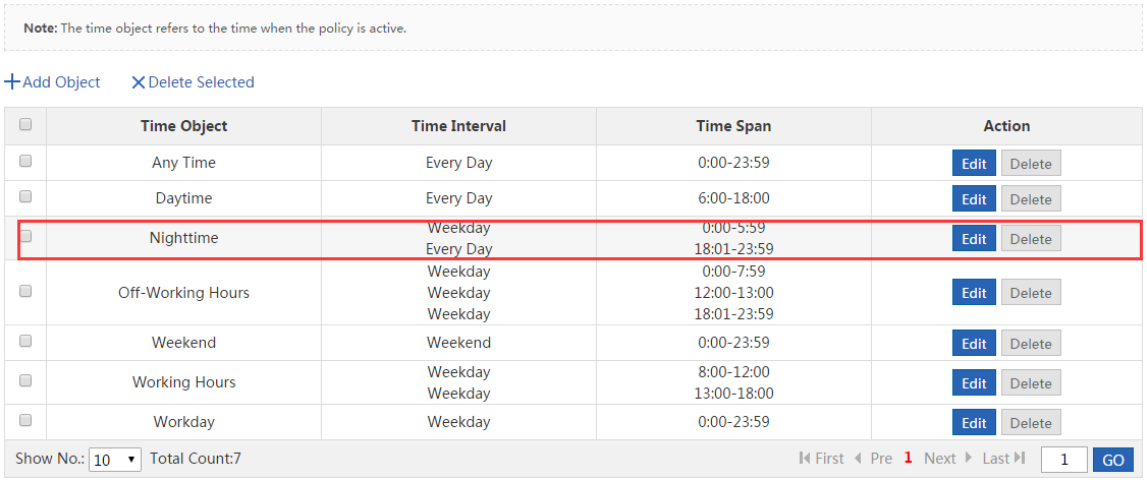

(3) Time span: Set the time span.




(4) Click **Add** to add another time span.



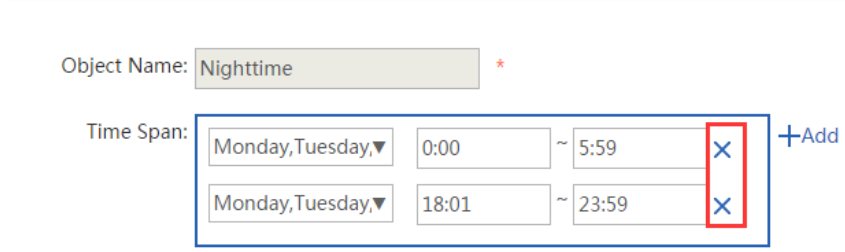

Click **Save**.



2. Edit a time object: Select a time object to be edited and click Edit. In the displayed dialog box, add, delete, or edit the time span.

3. Delete a time object: To delete a time object, select the time object in the list and click Delete.

4. Delete a time span: To delete a time span of a time object, select the time object and click **Edit**. In the displayed dialog box, select the time span to be deleted and click ×.

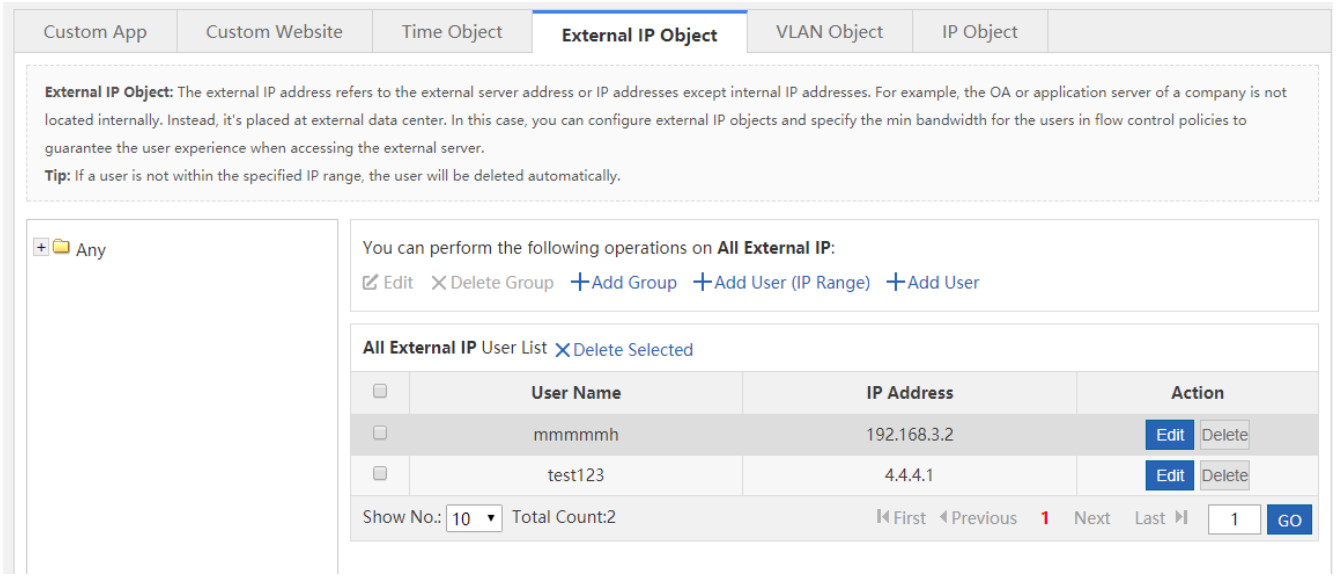



### 1.3.9.3.4 External IP Object

External IP objects are external server addresses or other IP addresses relative to internal IP addresses. For example, the OA server or service system server of a company is placed in the telecommunication equipment room or hosting center rather than in the company. To guarantee the rate for LAN users to access the server, you can configure the server address as an external IP object and configure the minimum bandwidth for the object in the flow control policy.

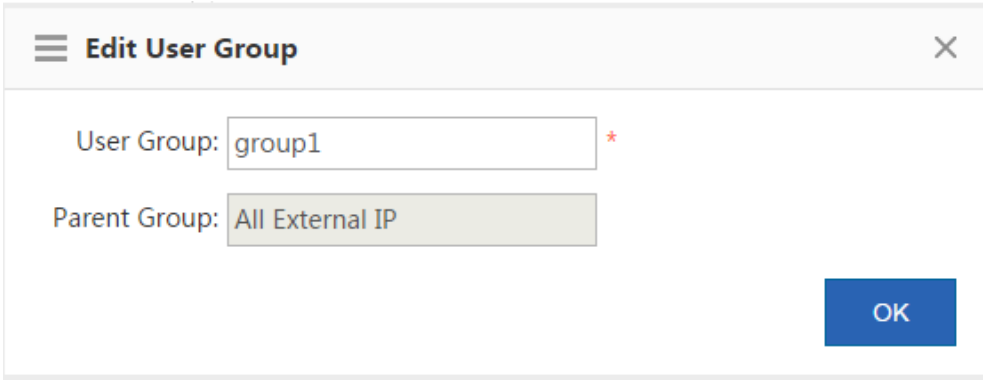
The system has a default object "/". When L2/3 class identification is enabled, if the destination IP address of a packet does not match any network object, it matches the default object "/" by default.

The external IP object configuration page is shown in the figure below.



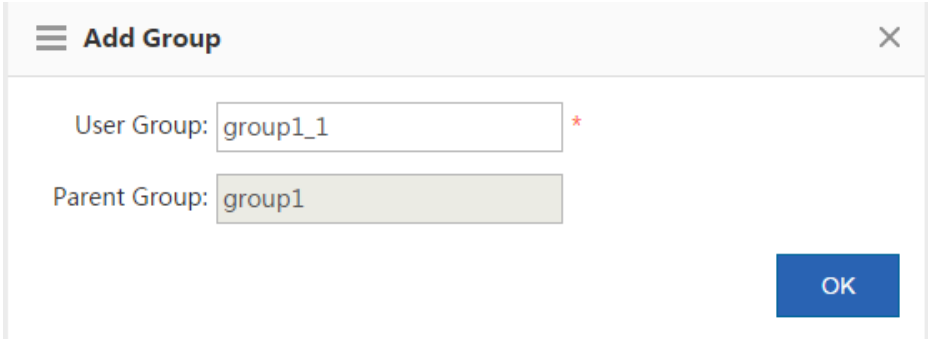
The tree-shaped hierarchy on the left side shows the organization structure of the current external IP objects. Select an external IP object. Information about the object is displayed on the right side, and you can edit or delete the object.

1. Click Edit Group to edit the selected external user group or external IP group, or modify the name of the external user group or external IP group.

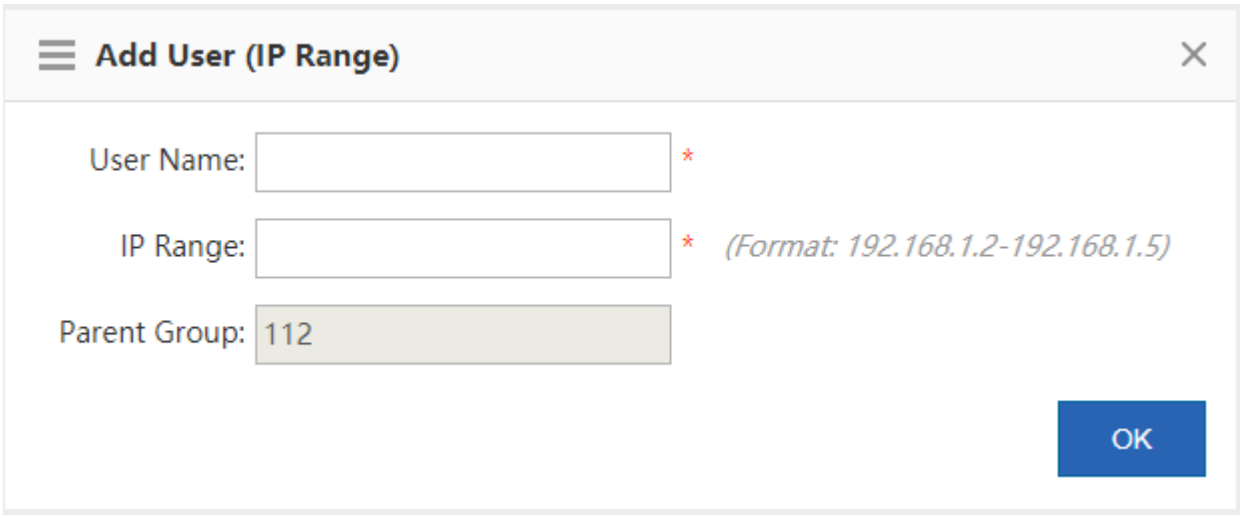



2. Click delete group to delete the selected external user group or external IP group from the organization structure of external IP objects.

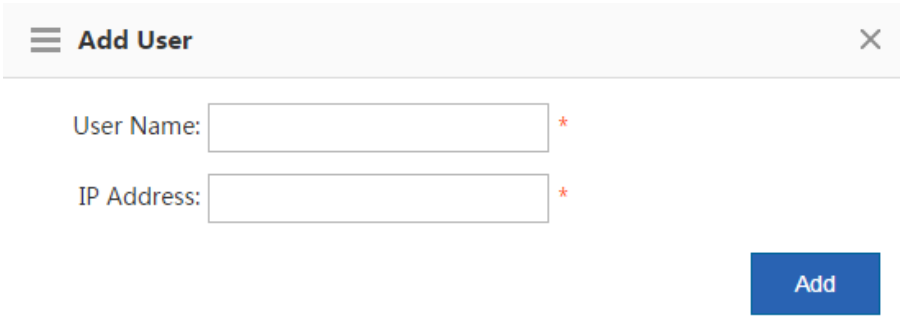
3. Click Add Group to create a sub group for the selected external user group.



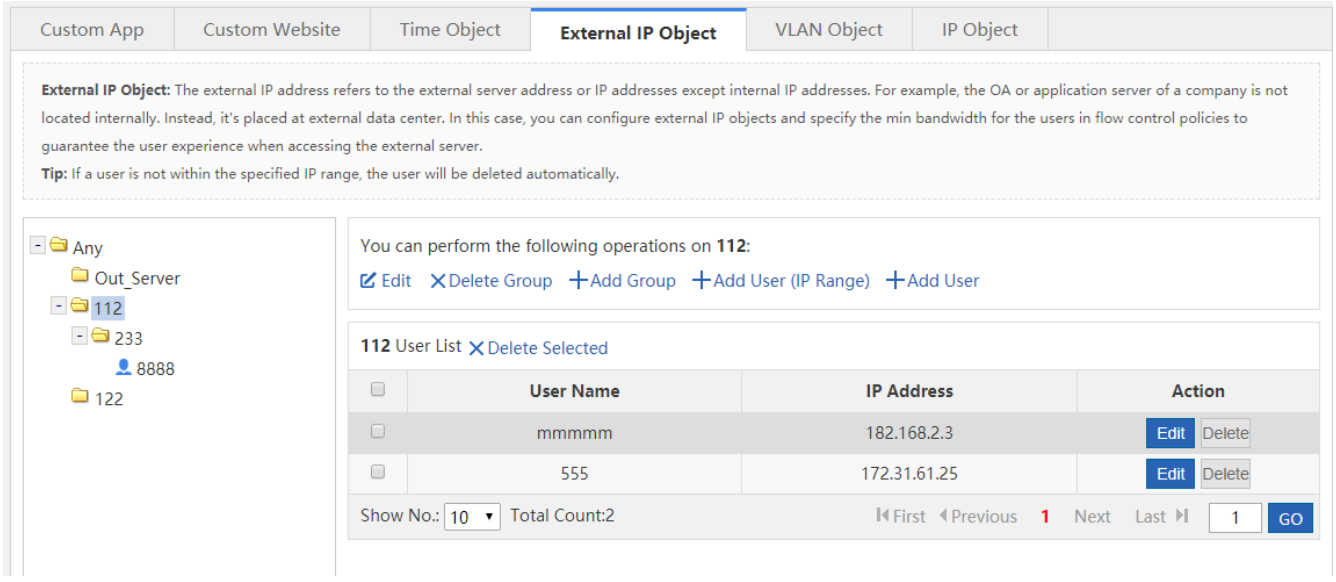

4. Click Add User (IP Range) to create an IP group under the selected external user group.




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

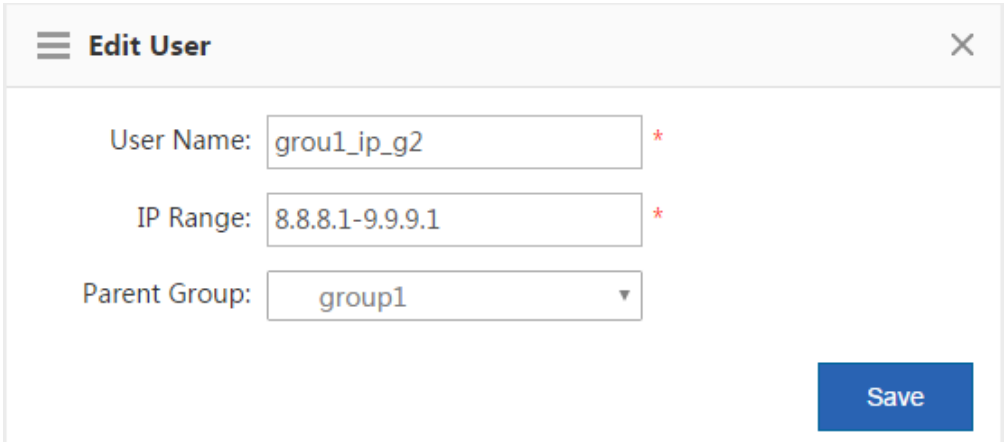



6. The user list of the external user group or external IP group is shown in the figure below.



The table shown in the figure above lists all users in the external user group or external IP group selected on the left pane. You can edit or delete a user.

Click Edit. The **Edit User** dialog box is displayed, and you can modify the username, IP address range, and parent group.



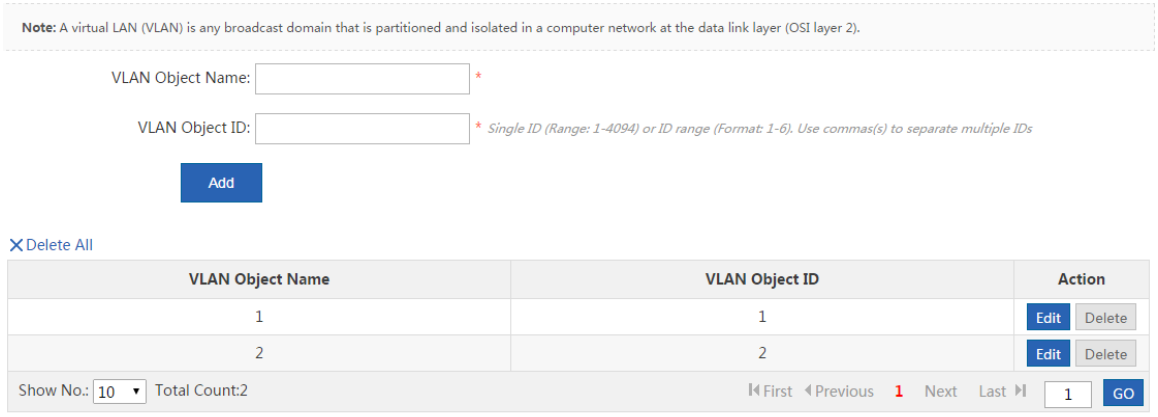

Click Delete to delete a user from the selected external user group or external IP group. You can select multiple users and click Delete.

### 1.3.9.3.5 VLAN Object

The VLAN IDs of VLAN objects cannot collide with each other. Multiple VLAN IDs are separated by a comma (,). If multiple consecutive VLAN IDs are configured for one VLAN object, use the hyphen (-) between the start VLAN ID and the end VLAN ID.

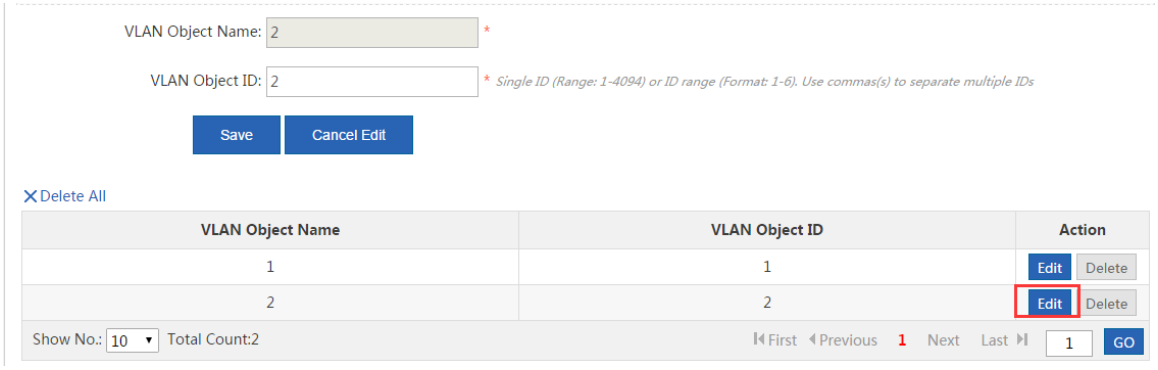
There is a default VLAN object named "any". When the L2/3 class identification is enabled, all data flows match the default VLAN object named "any" in gateway mode by default. In bridge mode, all data flows match the VLAN object corresponding to the native VLAN in the bridge by default. If the native VLAN of the bridge has no VLAN object, data flows match the default VLAN object "any".

The VLAN configuration page is shown in the figure below.




1. Create a VLAN object: Enter a VLAN object name and VLAN object ID and click Add.

2. Edit a VLAN object: Select the VLAN object to be edited and click Edit. For example, to edit a VLAN object "vlan1", click Edit, change the VLAN object name or VLAN object ID, and click Save.




3. Delete a VLAN object: Select the VLAN object to be deleted and click Delete. For example, to delete a VLAN object "vlan1", click Delete in the corresponding row. To delete all VLAN objects, click Delete All.

## 1.3.10 Behavior Management

### 1.3.10.1 Behavior Policy

The behavior policy module supports access audit, monitoring, and policy configuration of user behaviors. It provides required access audit information for users. It also allows administrators to manage user behaviors, leads users to correct network behaviors and time allocation, and prevents impact from improper information on users.

The policy matching for behavior management services has a certain priority sequence.

If the previous behavior management service does not block a packet, the packet is transferred to the next behavior management service for processing. If a behavior management service has blocked a packet, the packet will not be

transferred to the next behavior management service. The figure below shows the processing sequence of behavior management services.

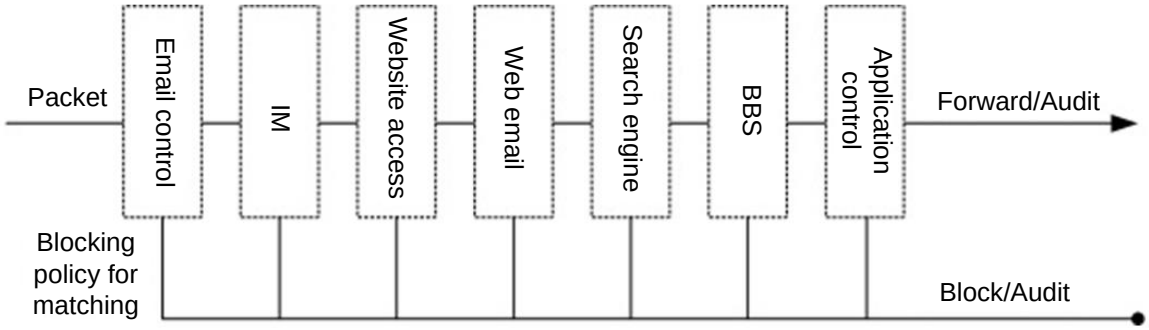



Figure: Processing Sequence of Behavior Management Services

Behavior policies are matched in the priority sequence of policy groups and rules.

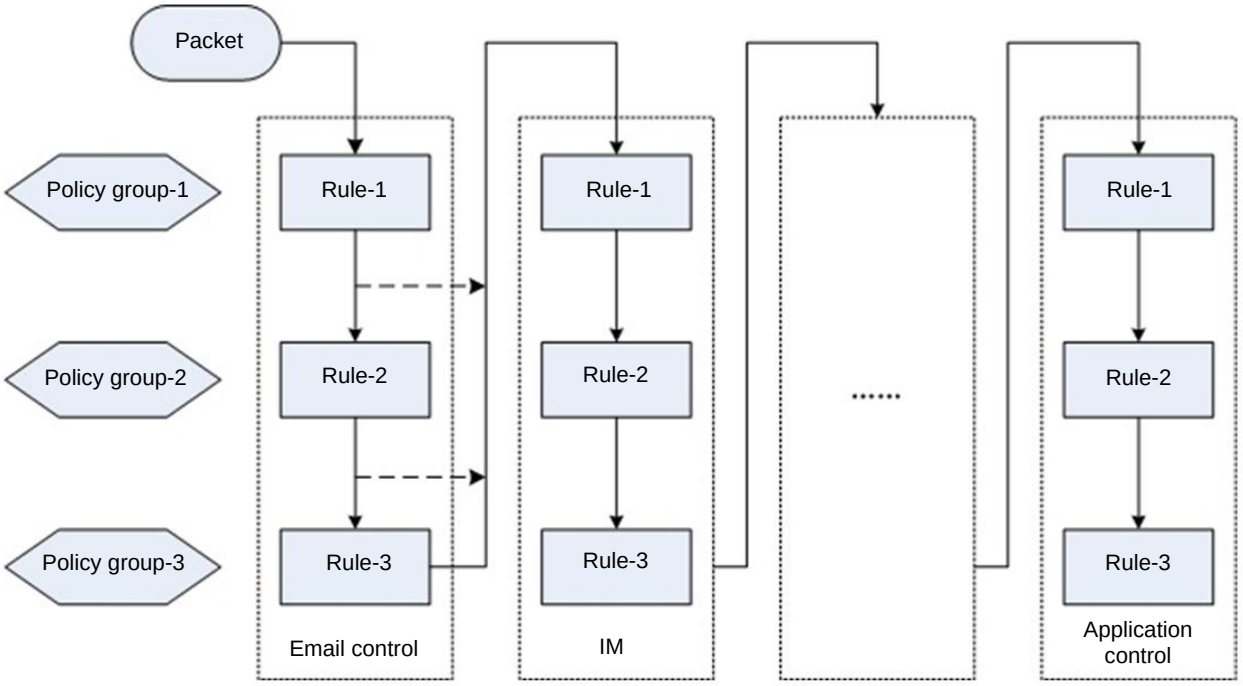
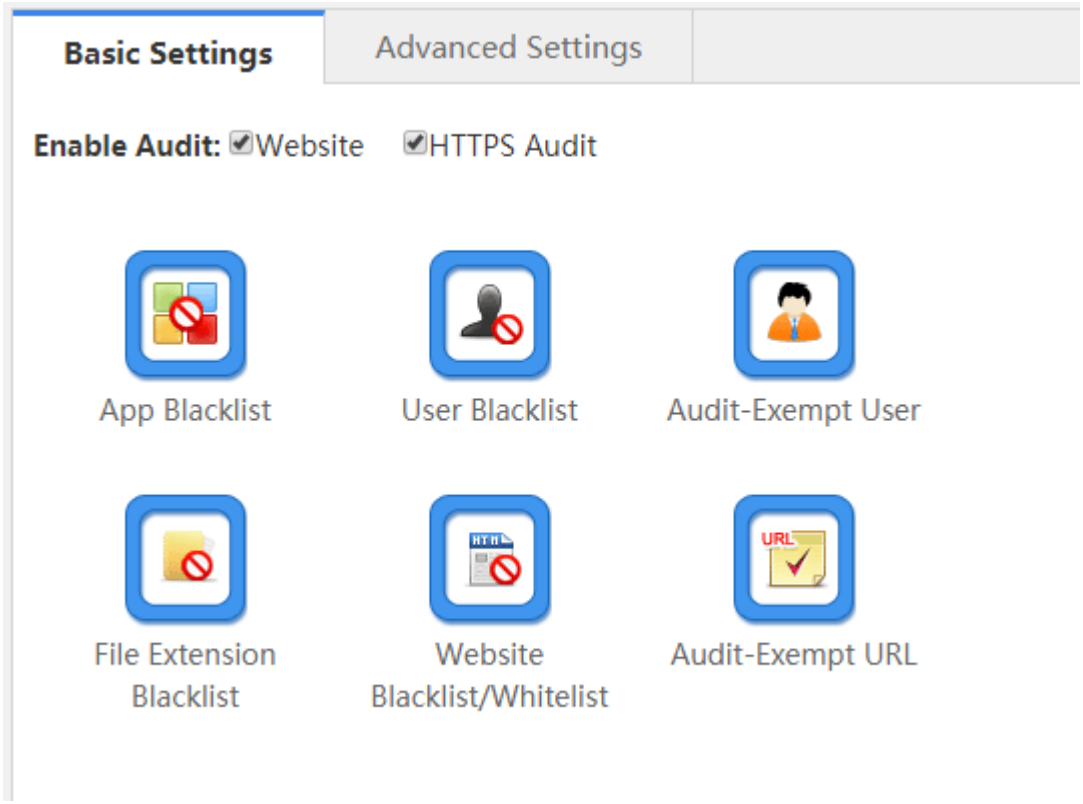



Figure: Matching Sequence Based on the Priorities of Policies and Rules

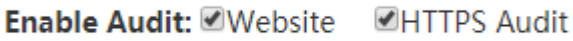
### 1.3.10.1.1 Basic Settings

This tab page allows you to enable or disable the default audit function for website access or Https audit. You can also perform special processing on some specific users, specific applications, specific websites, and specific file types, for example, conduct filtering or audit exemption.

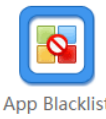



- **Enable Audit**

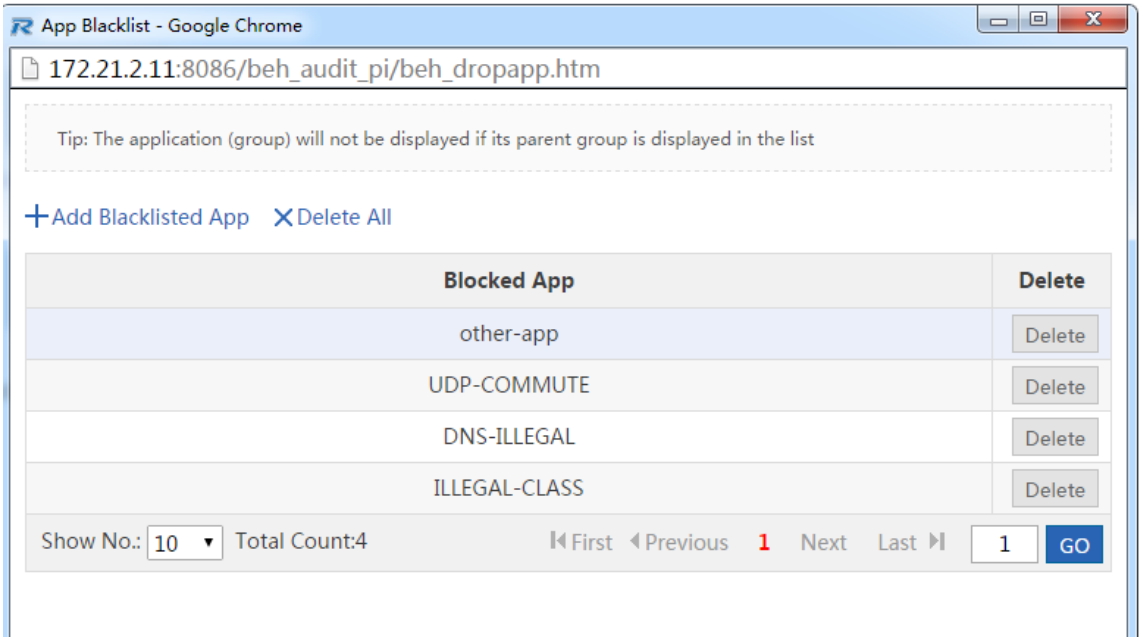
After the default audit function is enabled for an application, the device audits all Internet access records of the application. For example, if the default audit function is enabled for search engines, all search engine records of users will be audited. Otherwise, the device audits only Internet access records that match the behavior policy.



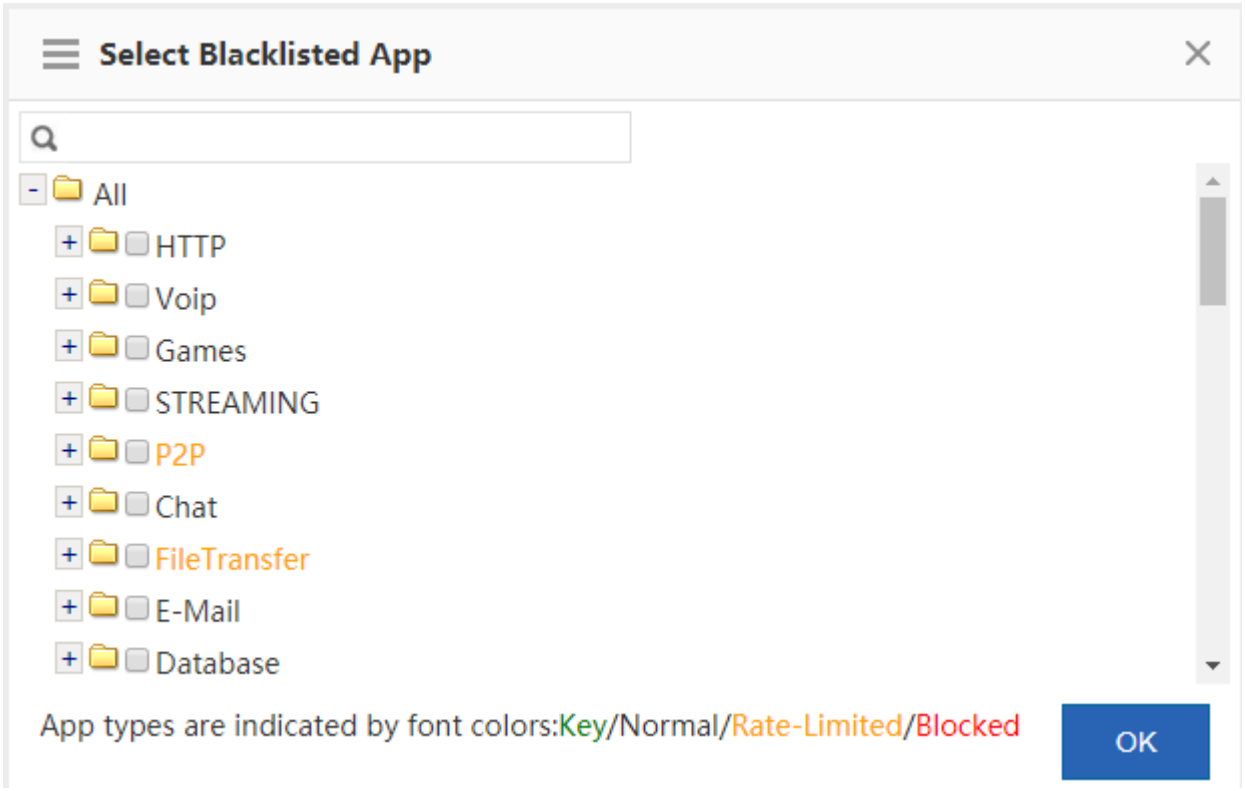

- **App Blacklist**



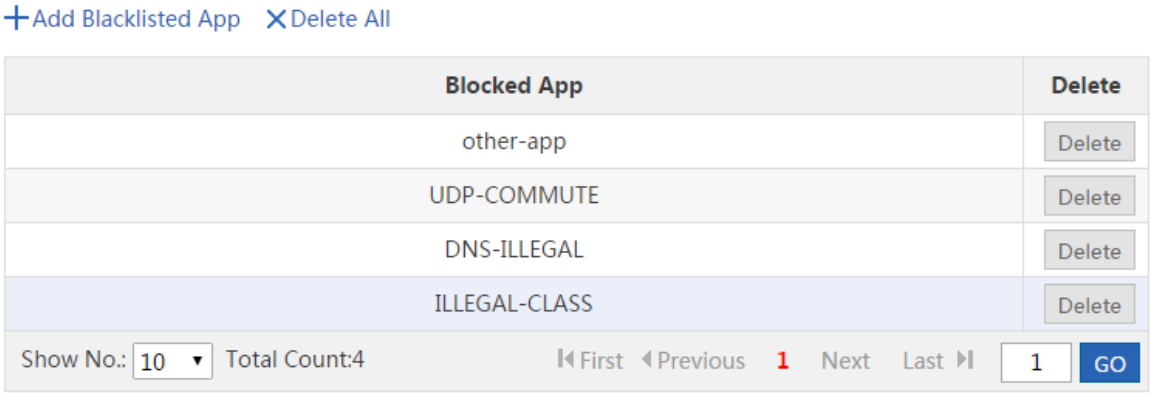

Click . A window shown in the figure below is displayed. You can view blacklisted applications, and can add applications to or delete applications from the blacklist.

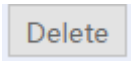



Click Add Blacklisted App. A window shown in the figure below is displayed.




Select an application to be blacklisted, for example, games, and click OK to blacklist the application.




Click 

to delete an application from the application blacklist.

Click 

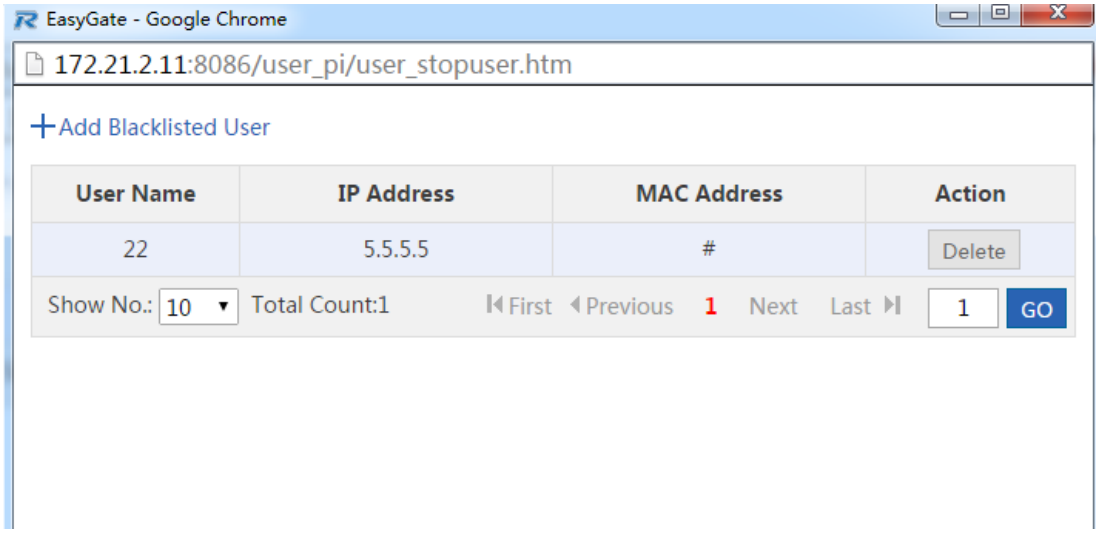
to delete all applications from the application blacklist.

After the application blacklist function is enabled, the device forbids any user from running applications in the blacklist.

- **User Blacklist**

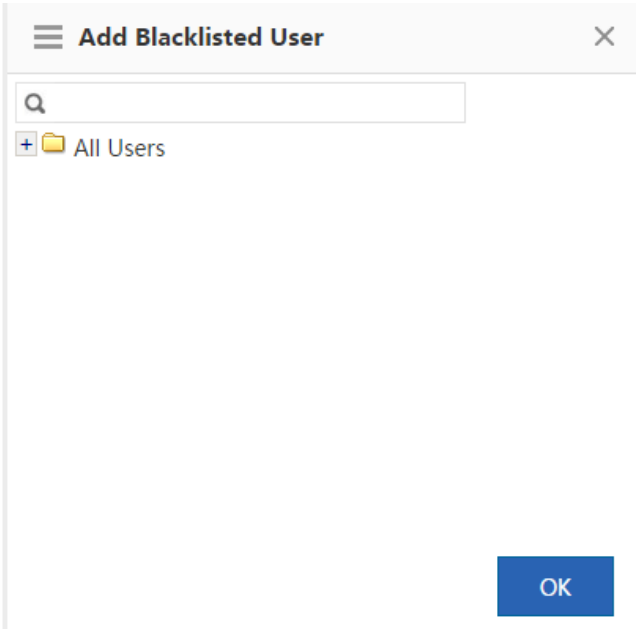
Click 

. A window shown in the figure below is displayed, and you can view blacklisted users, and can add users to or delete users from the blacklist.




Click 

. A window shown in the figure below is displayed.




Select a user to be blacklisted and click OK to add the user to the blacklist.

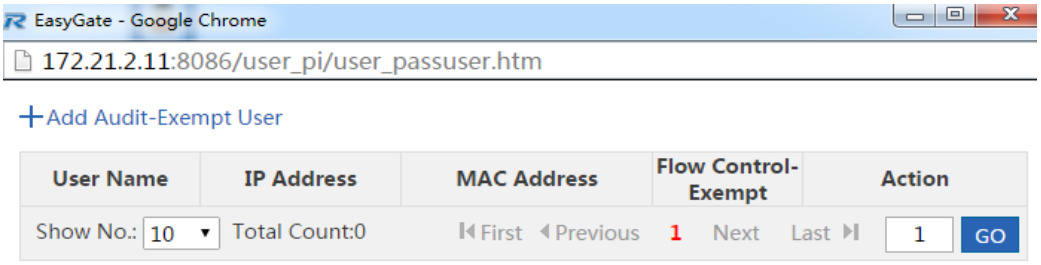
| User Name | IP Address | MAC Address | Action |
|---|---|---|---|
| 22 | 5.5.5.5 | # | Delete |

Click Delete to delete a user from the user blacklist.

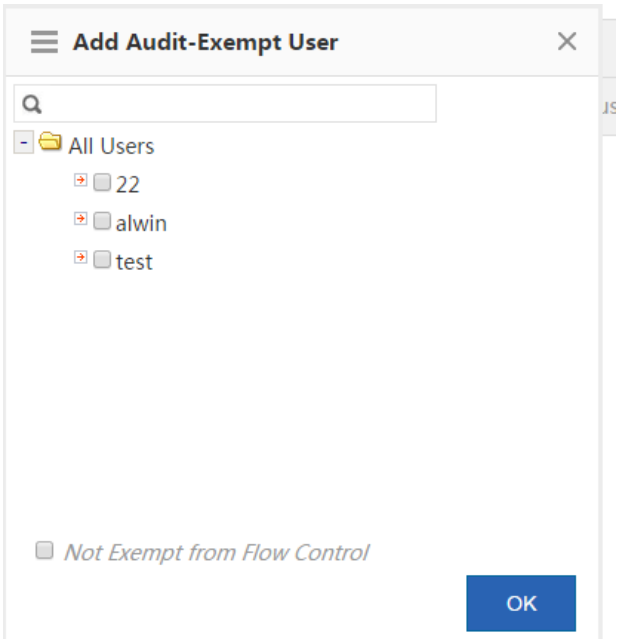
After the user blacklist function is enabled, the device will block the Internet access behaviors of blacklisted users.

- **Audit-Exempt User**

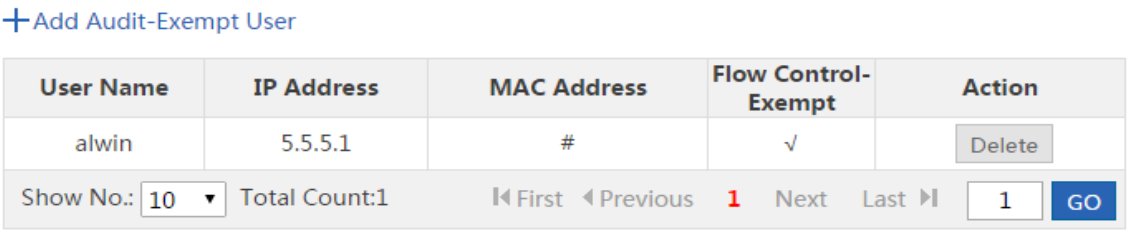
Click Audit-Exempt User . A window shown in the figure below is displayed. You can view the user devices exempt from audit, and can add or delete audit-exempt users.




Click Add Audit-Exempt User. A window shown in the figure below is displayed.




Select a user to be exempted from audit. Audit-exempt users are exempt from flow control by default. If flow control is required for an audit-exempt user, select Not Exempt from Flow Control and click OK.

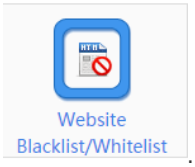



In the **Flow Control-Exempt** column, √ indicates that a user is exempt from flow control while × indicates that flow control is required for a user.

Click Delete to delete a user from the audit-exempt user list.

After the audit-exempt function is enabled, the device does not audit the Internet access records of audit-exempt users. If **Not Exempt from Flow Control** is selected, the rate limit rule in the flow control policy is also effective to audit-exempt users.

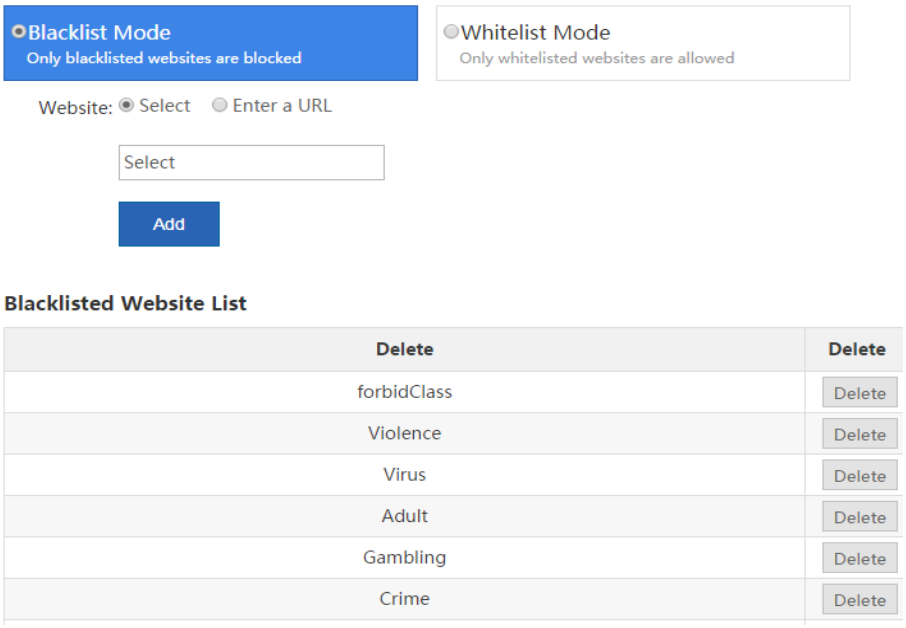
- **Website Blacklist/Whitelist**

Click 

. The website blacklist/whitelist configuration window is displayed. You can view the websites to be blacklisted, and can add websites to or delete websites from the blacklist.

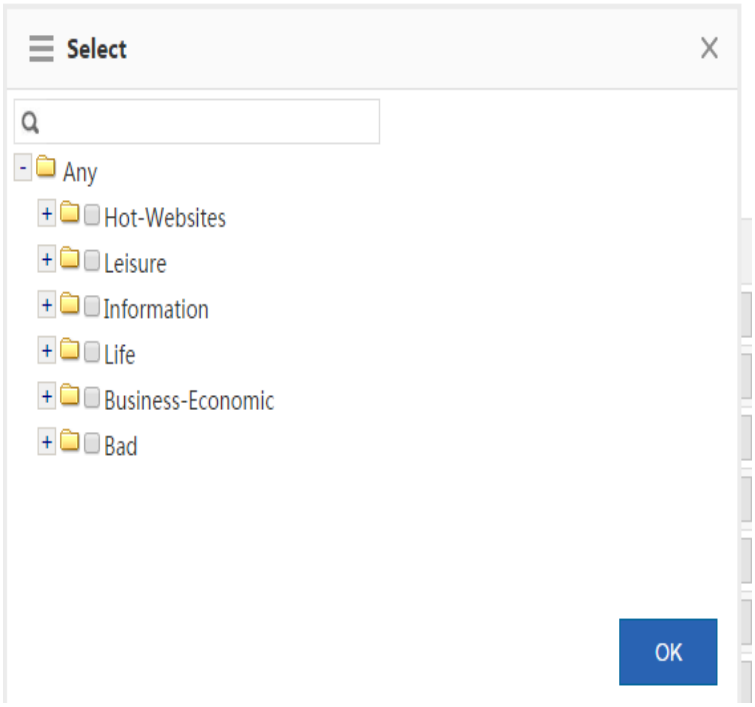
This function supports two modes: blacklist mode and whitelist mode.

1. **Blacklist Mode**: The device blocks only blacklisted websites and allows traffic of other websites to pass.




(1) Add a website to be blacklisted: You can select an existing URL category or directly enter a website URL.

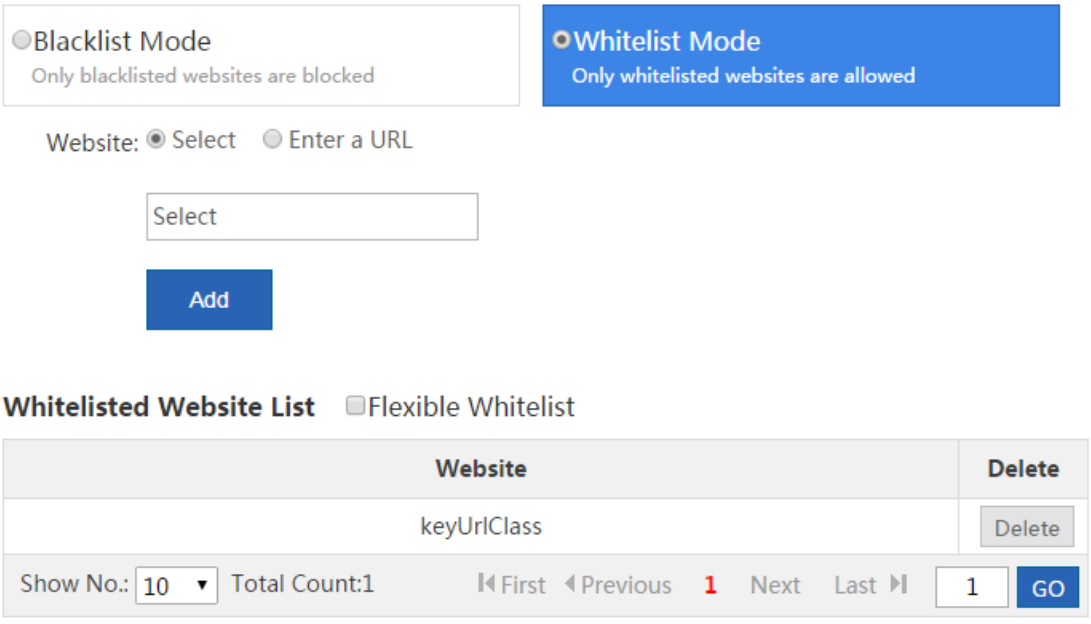
a. Select an existing URL category: Click Select and click the input box shown in the figure above. A window shown in the figure below is displayed. Select the URL category to be blacklisted and click OK.




b. Directly enter a website URL: As shown in figure below, click **Enter a URL**, enter a website URL to be blacklisted, and click Add.

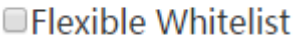

(2) Delete a blacklisted website: Select a website to be unblocked and click Delete.

2. **Whitelist Mode**: Users are allowed to access only whitelisted websites. The device blocks traffic of other websites.




(1) Add a whitelisted website: You can select an existing URL category or directly enter a website URL. The add operation is the same as that of adding a website to be blacklisted.

(2) Delete a whitelisted website: Select a website to be blocked and click Delete.

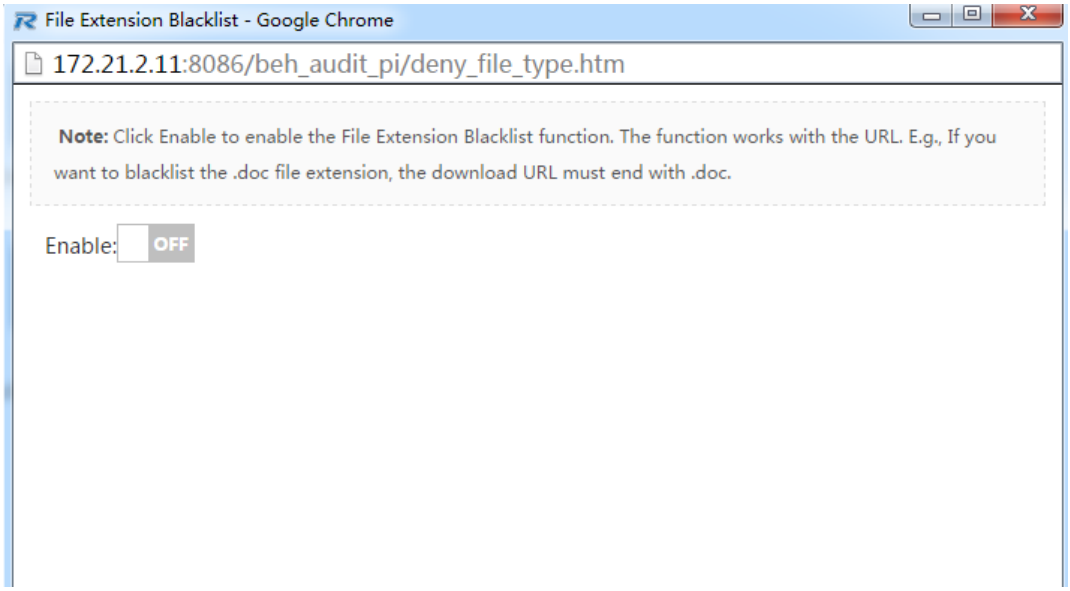
(3) Flexible whitelist: Select 

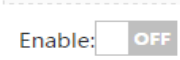
. URL requests initiated from a whitelisted website are allowed to pass. For example, if www.ruijie.com.cn is a whitelisted website, users are allowed to access all URLs on this Web page.

- **File Extension Blacklist**

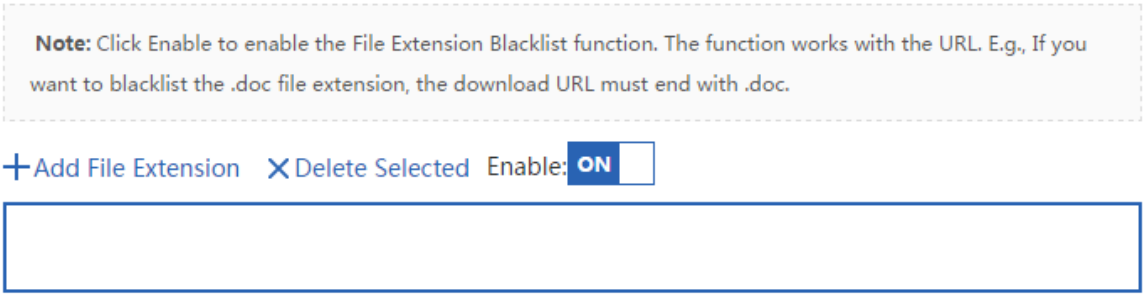
Click 

. A window shown in the figure below is displayed. You can view the type of file resources to be blacklisted, and can add a file type to or delete a file type from the blacklist.

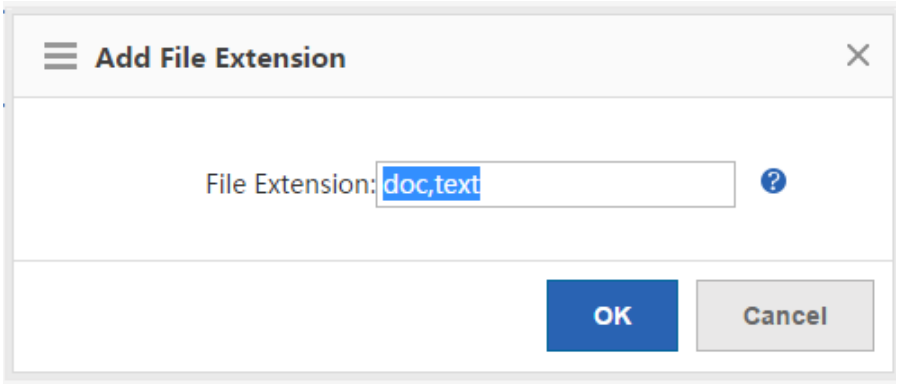



Click 

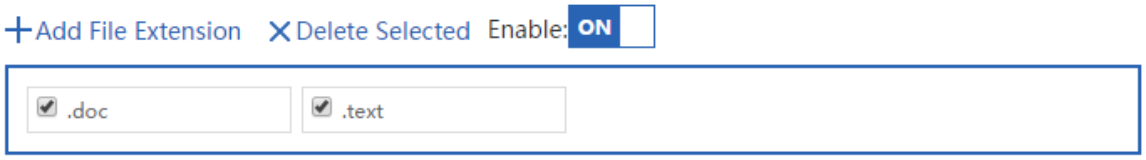
to enable the file extension blacklist function.



Click + Add File Extension to add the extensions of files to be blacklisted. Separate multiple extensions by a comma (,).



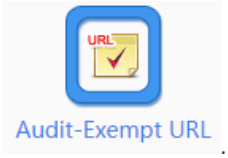

Enter the extensions of files to be blacklisted and click OK to add the extensions to the file extension blacklist.



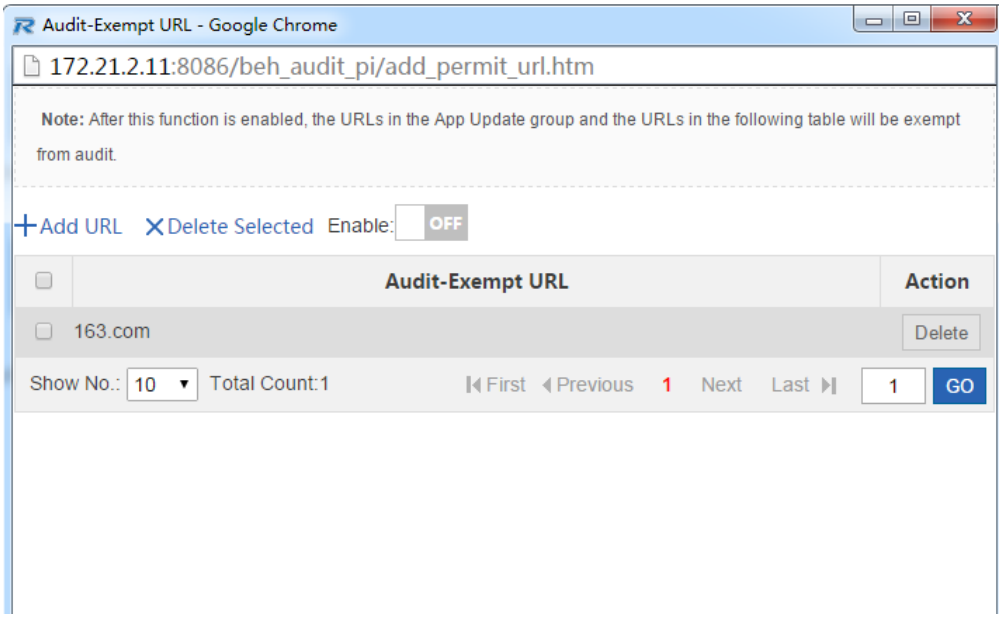

Click ✕ Delete Selected to delete a selected file type from the file extension blacklist.

After the file extension blacklist function is enabled, the device blocks the uploading and downloading of files of the specified type.

- **Audit-Exempt URL**

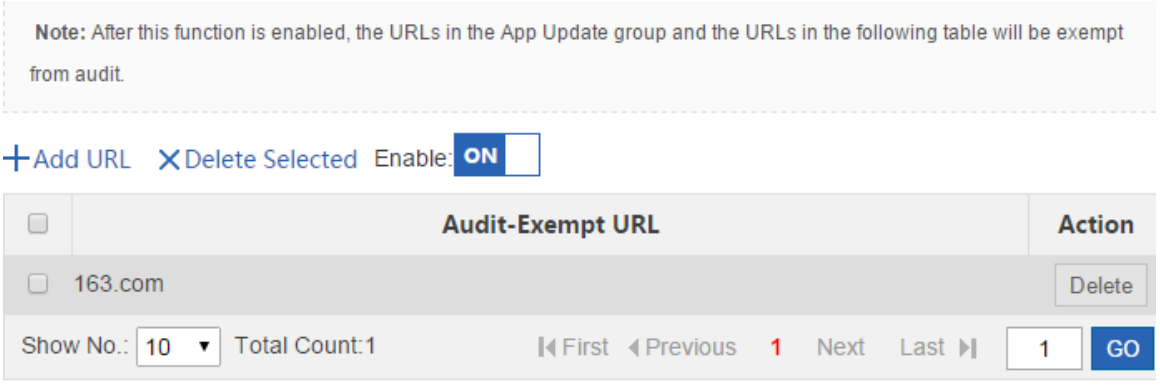
Click 

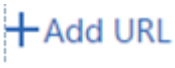
. A window shown in the figure below is displayed. You can view the websites exempt from audit, and can add or delete audit-exempt websites.



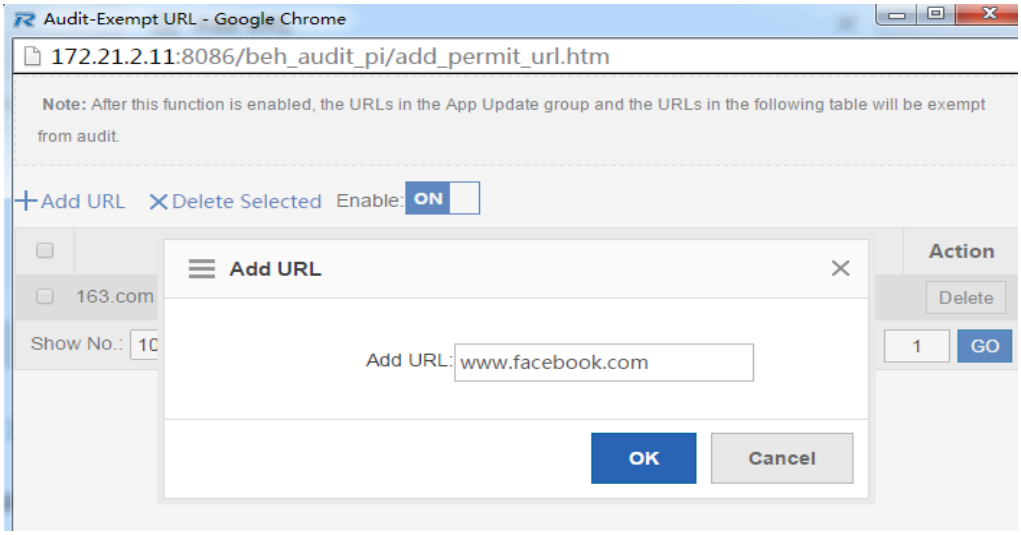

Click 

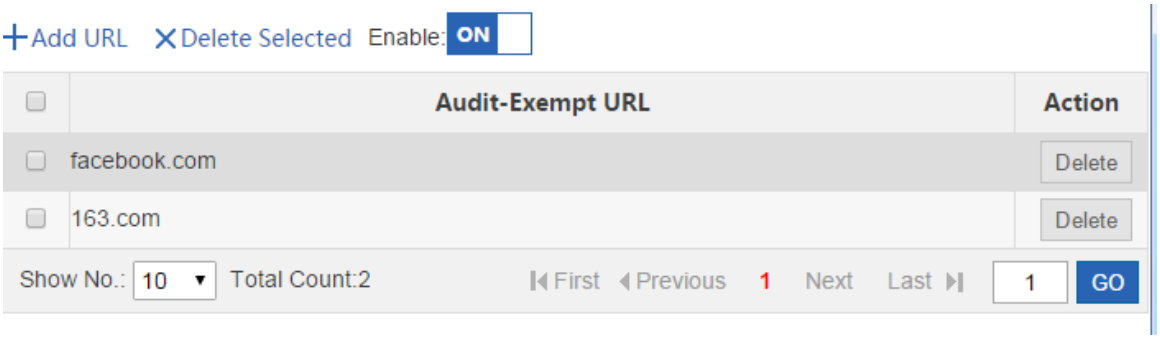
to enable the audit-exempt URL function.

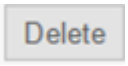



Click 

. In the window displayed, enter an audit-exempt URL and click **OK** to add the URL to audit-exempt URL list.




Click  to delete a URL from the audit-exempt URL list.



Click  to delete selected URLs from the audit-exempt URL list in batches.



After the audit-exempt URL function is enabled, the device neither audits the access behavior of users nor blocks users from accessing the website.

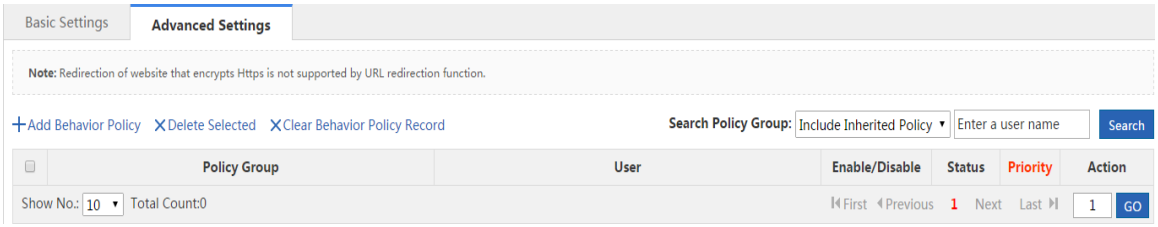
### 1.3.10.1.2 Advanced Settings

Information transfer via Internet has become a critical application of enterprises (institutions). Problems concerning confidentiality, health, political nature, and the like arise consequently.

The EG device of Ruijie Networks can effectively control the spread scope of key information and prevent possible legal risks.

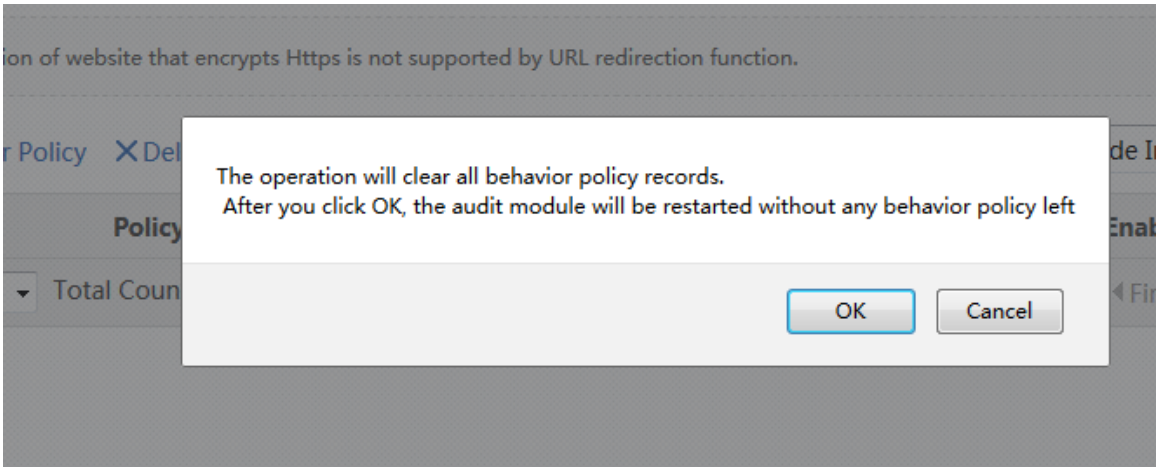
The EG device of Ruijie Networks is capable of monitoring information transfer channels such as email, Web mail, BBS, IM, Web search, FTP, Telnet, and Web page. It can comprehensively audit the email content, chat content, and posts.

The **Advanced Settings** configuration page is shown in the figure below.




This page allows you to manage and configure application control policies, website access policies, email audit policies, chat audit policies, forum posting policies, and search engine policies.

Click Clear Behavior Policy Record to clear all behavior audit records on the device, as shown in the figure below.

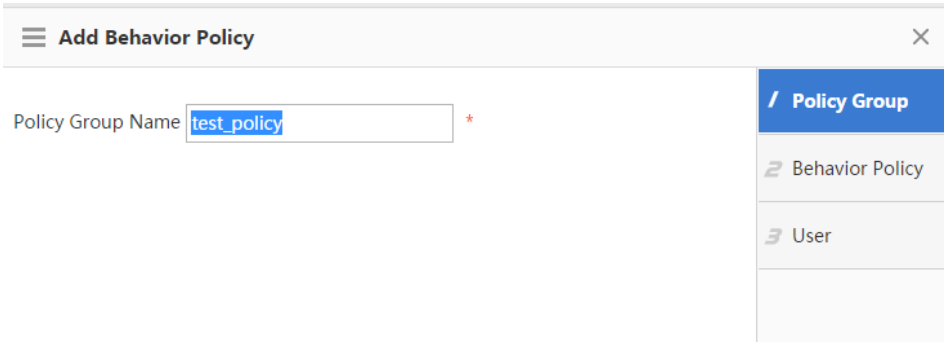



- **Creating and Editing a Policy**

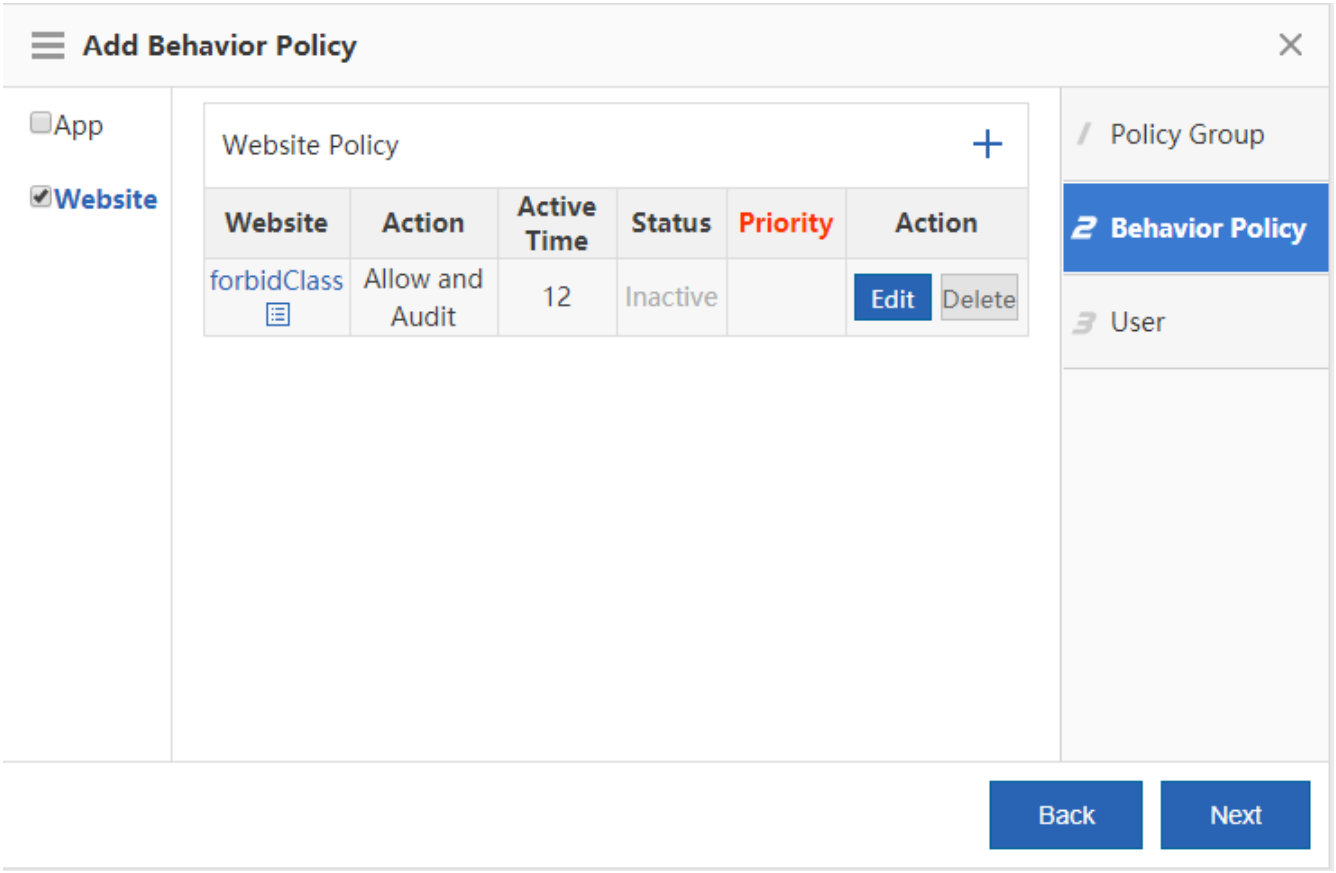
To create a behavior policy, do as follows:

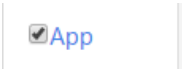
1. Click Add Behavior Policy. The **Add Behavior Policy** dialog box is displayed.

2. **Policy Group**: Enter the name that identifies the rule or purpose of a policy in the **Policy Group Name** text box.



3. **Behavior Policy**: Select a behavior rule to which the policy is to be applied, as shown in the figure below. You can select multiple behavior rules at a time.




Click a rule name on the left. All rules under the rule name are displayed. To edit a rule, select 

and then edit, delete, or add a rule. Click **Finish** to save the settings. For details about how to add rules of different types, see subsequent sections.

Action description:

**Allow and Audit**: The device does not block the Internet access behaviors of selected users but records their Internet access information.

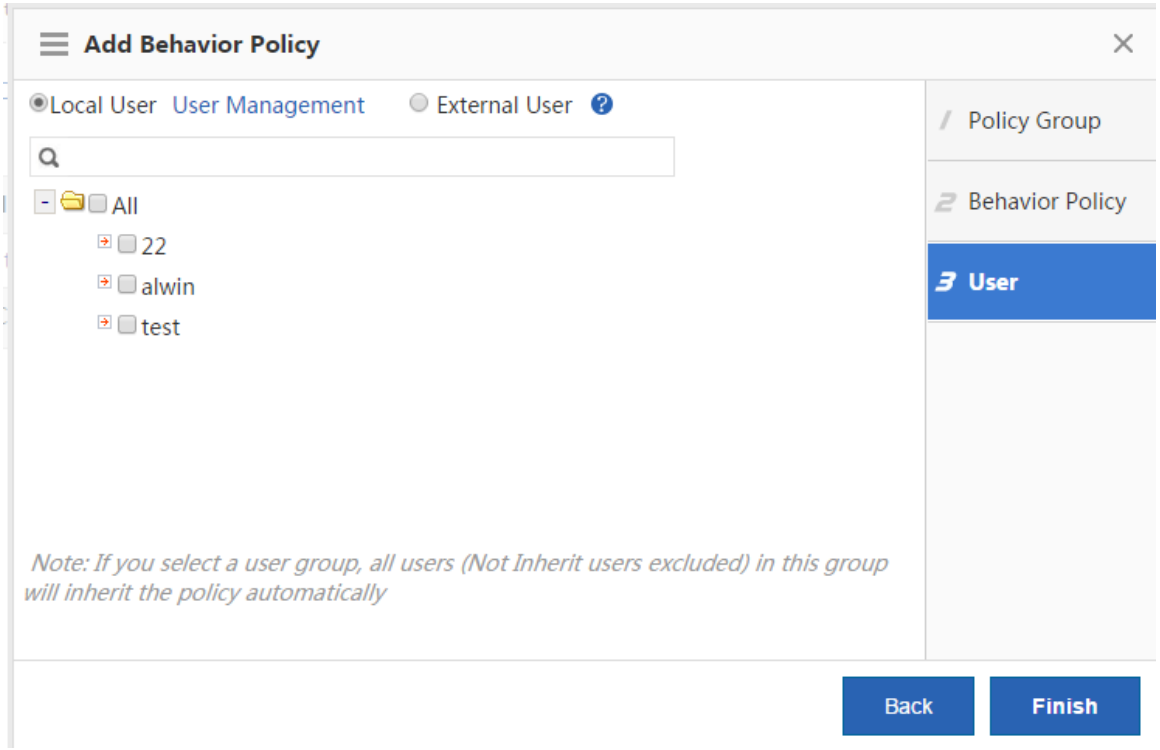
**Allow and Not Audit**: The device neither blocks the Internet access behaviors of selected users nor records their Internet access information.

**Block and Audit**: The device blocks the Internet access behaviors of selected users and records blocking information.

**Block and Not Audit**: The device blocks the Internet access behaviors of selected users but not records blocking information.

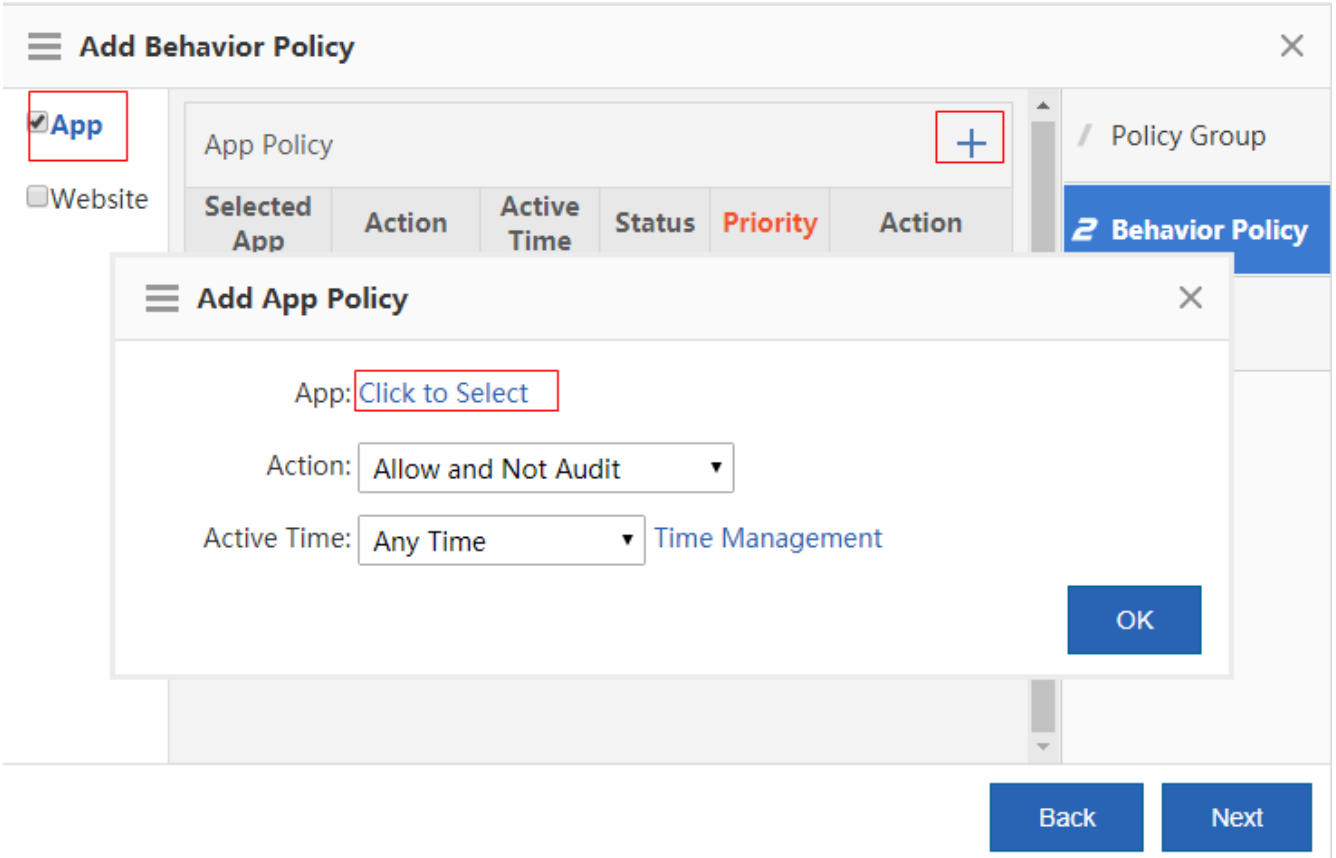
**Active Time**: Indicates the active time of a rule. A rule is effective only within the active time.

4. **User**: Select the users on which the policy takes effective. The users can be local users or external users. External users are users who pass third-party authentication, for example, VPN and Web-authenticated users.

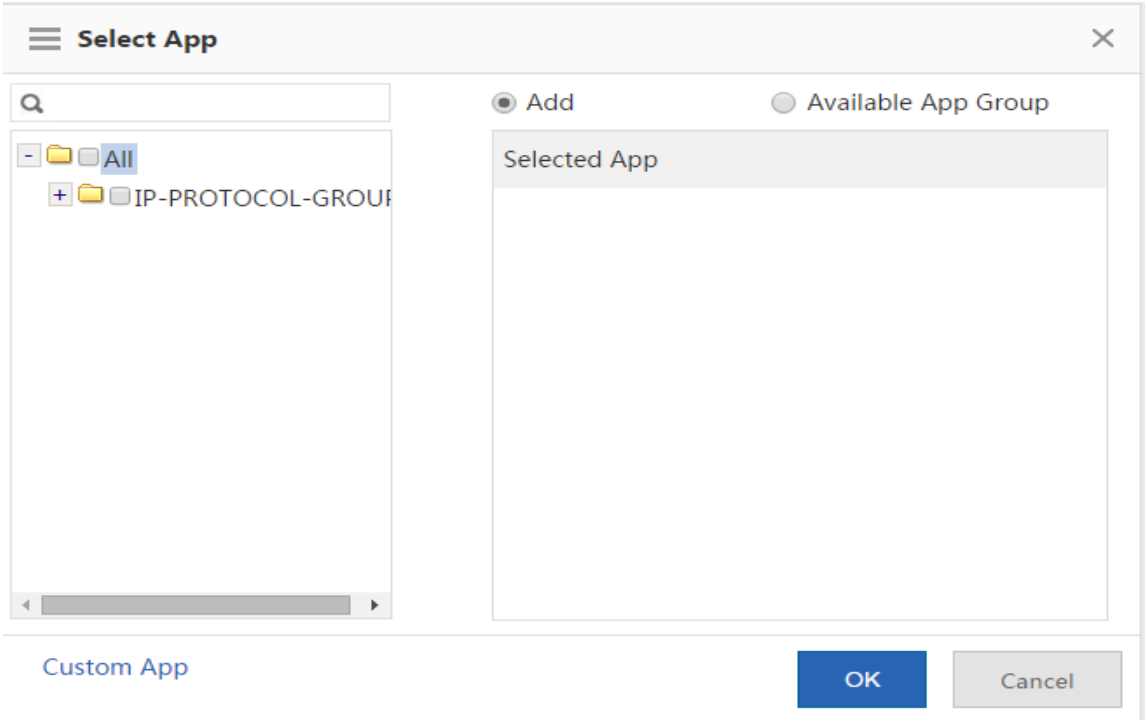



- **App Policy**

The **App Policy** page enables the device to monitor network behaviors of different applications, permit or block data flows of the applications, and audits control behaviors. To create an application policy, do as follows:



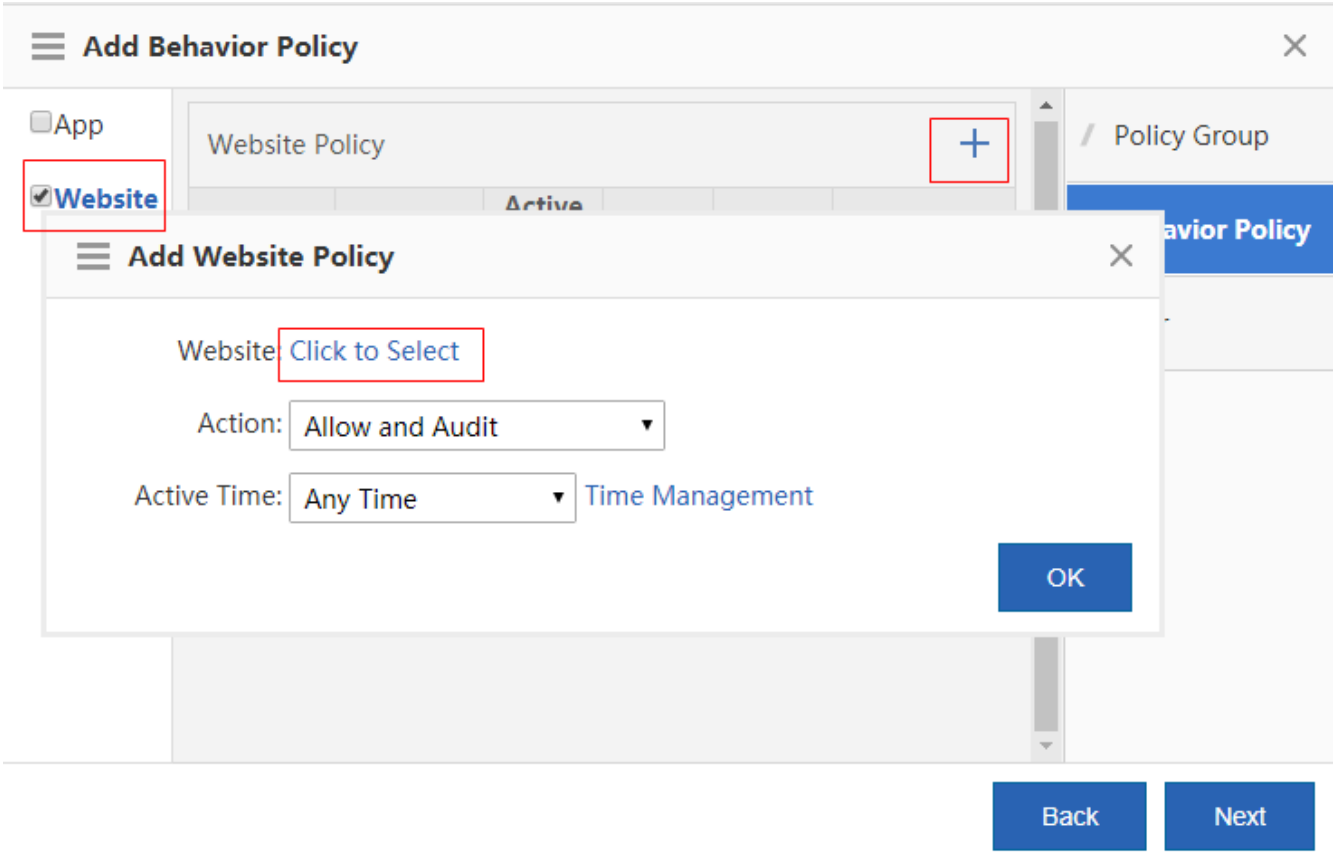

Select **App**. A page shown in the figure below is displayed.



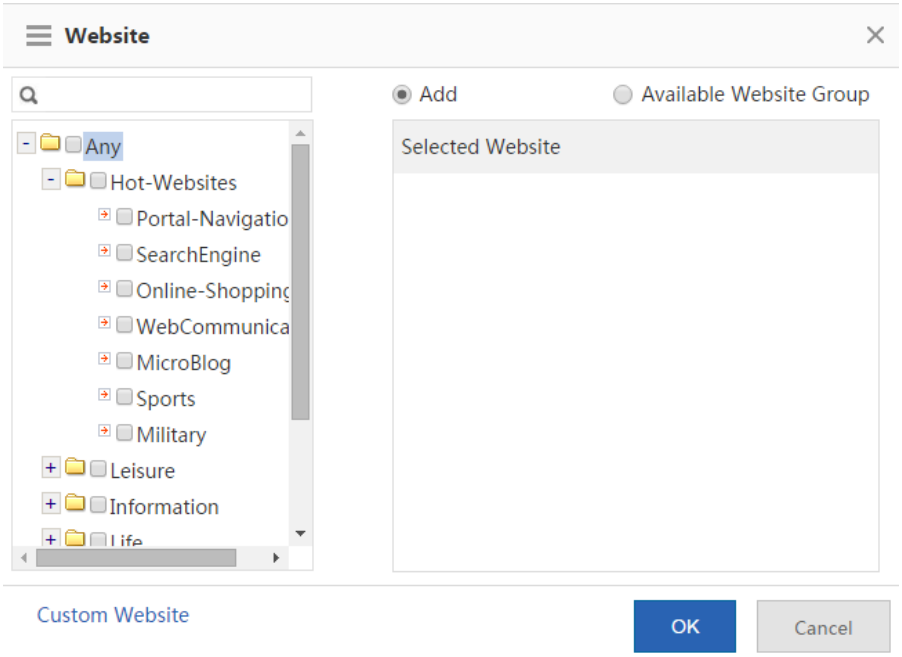
Click **Add** or **Available App Group**, as shown in the figure above. To create an application group, select the application to be controlled, enter the application group name, and click **OK**.

- **Website Policy**

A website policy is configured to monitor URL access, classify and audit URL access initiated by LAN users, and permit or block URL access as required. The configuration page is shown in the figure below.

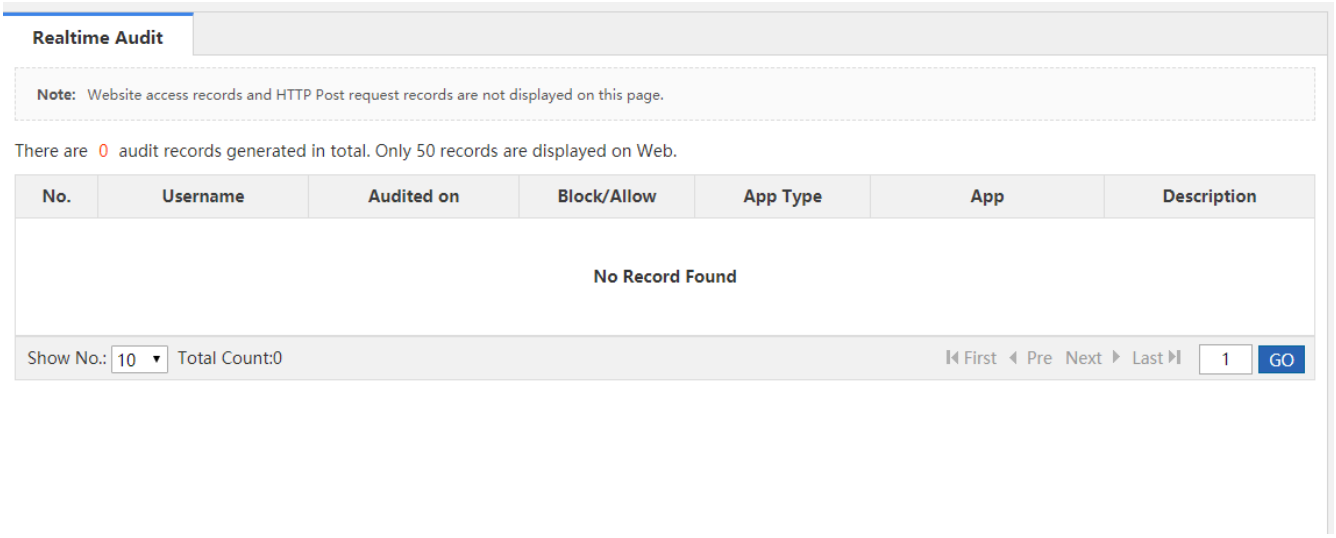



Click **Click to Select**. A window shown in the figure below is displayed.




The tree-shaped hierarchy on the left side shows the organization structure of configured URL categories in the current system. You can select a URL category for monitoring. If no URL category is selected, all categories will be monitored by default.

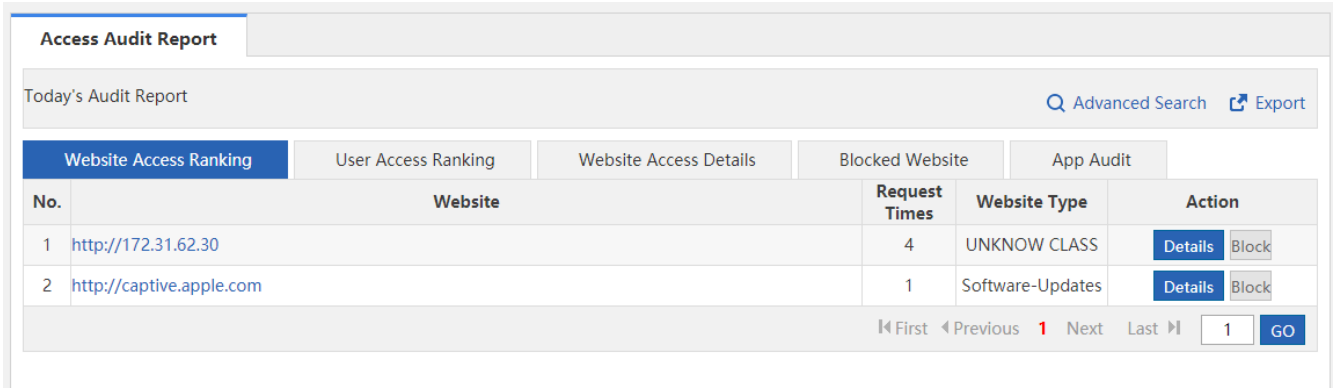
### 1.3.10.2 Realtime Audit




### 1.3.10.3 Access Audit Report

#### 1.3.10.3.1 Access Audit Report

The access audit report displays Web page-relevant access records, including the website access ranking, user access ranking, web access details, blocked website and application audit. The **Access Audit Report** page is shown in the figure below.

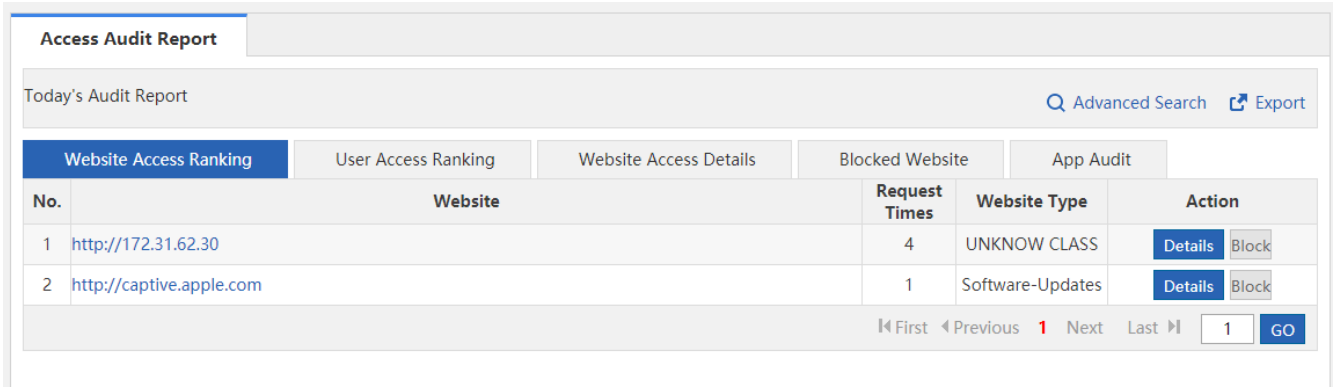



Click Advanced Search. The parameter selection page for advanced search is displayed. For details, see "Advanced Search" in this section.

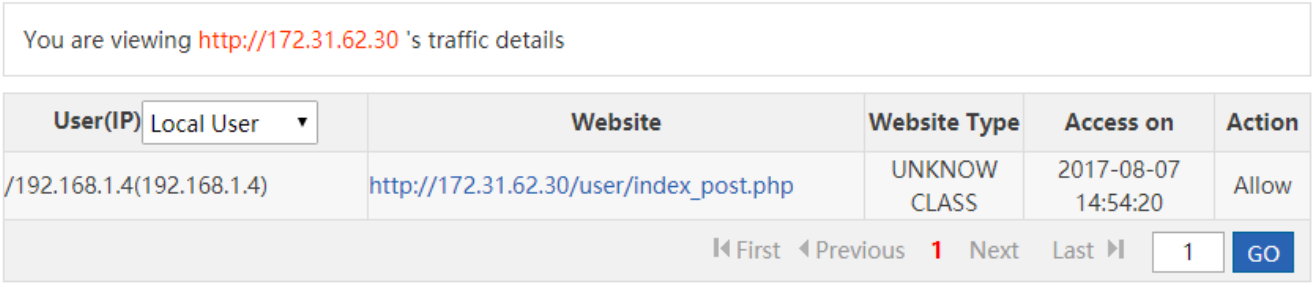
Click Export to export the search report results to the PC.

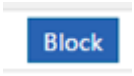
1. Website Access Ranking

This tab page displays the website access ranking, including the influence rank of a website, request times and website type, as shown in the figure below.




Click Details of a website to display traffic details about the website, for example, users who access the website and the access time.

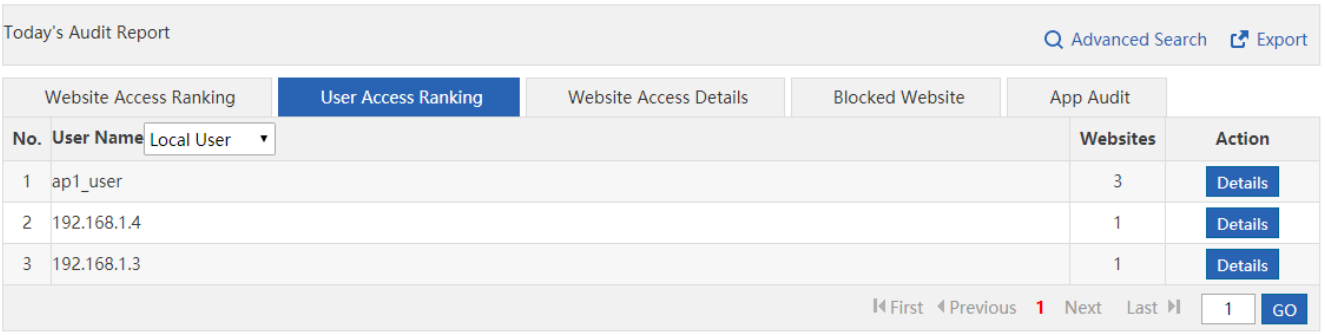


Click 

to block the selected website. Users cannot access a blocked website.

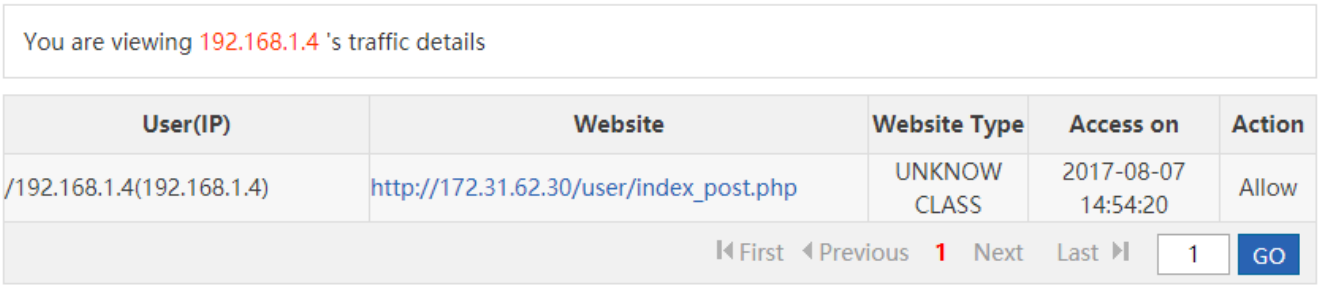
2. User Access Ranking

This tab page displays the ranking of the website number accessed by users. A user who accesses more websites is listed above a user who accesses less websites.

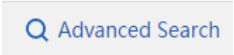



Click 

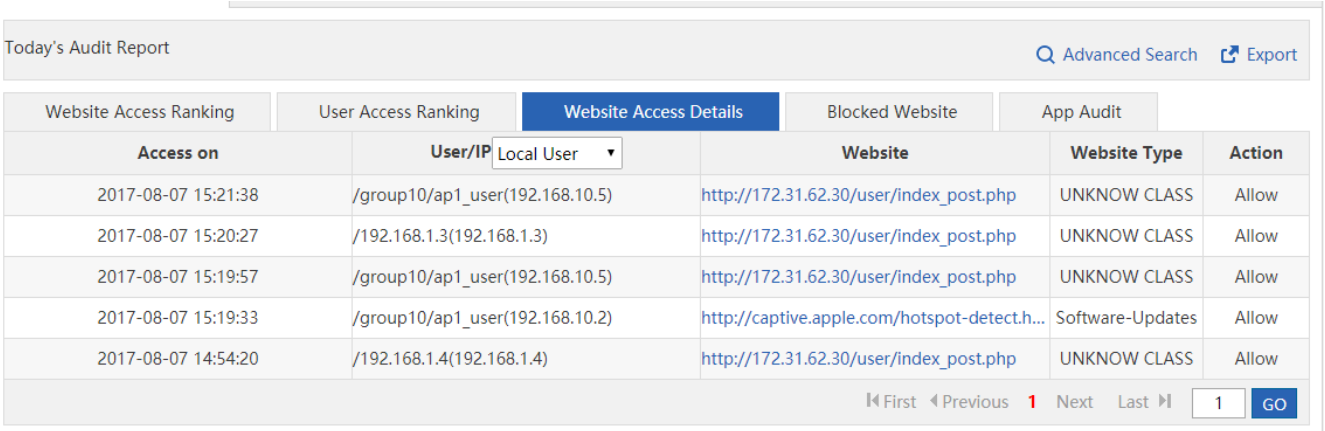
to display the websites accessed by a user, access time, and website type.




3. Website Access Details

This tab page displays details about all accessed websites. To view a specific website, click 

and enter the required URL.

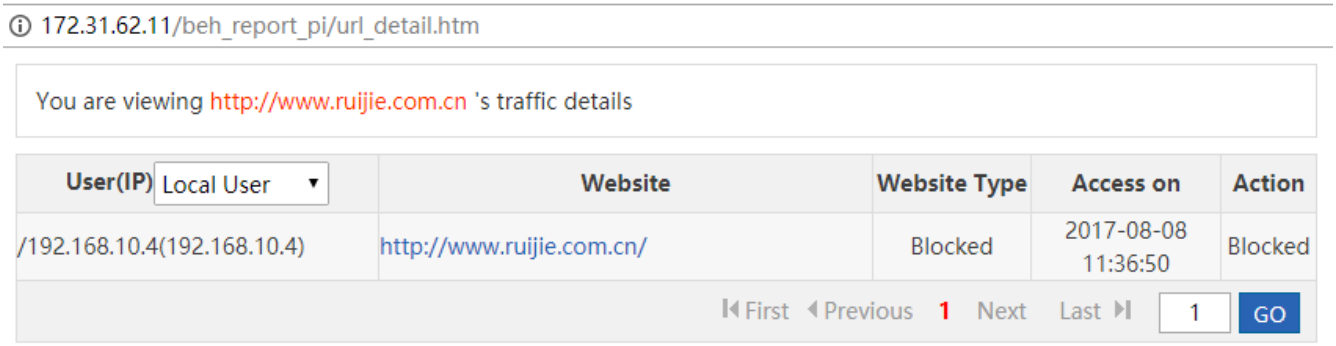


4. Blocked Website

This tab page displays information about all blocked websites in a list.

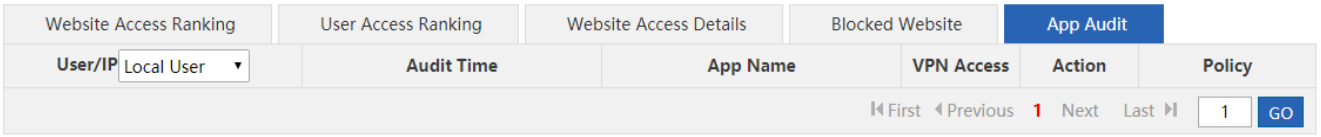

Click  to display traffic details about a selected website.





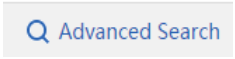

5. App Audit

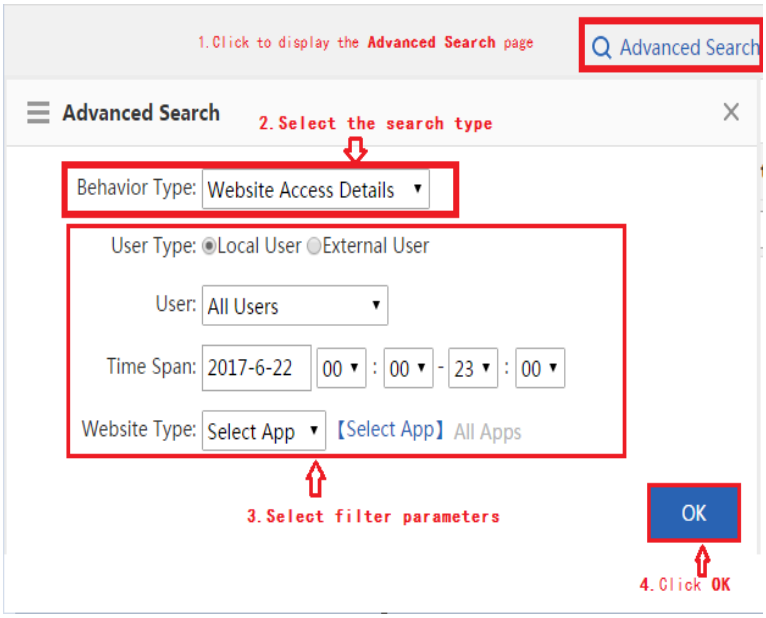
After application control rules are configured, the application audit function enables the device to audit, according to these rules, each application that generates Internet access behaviors, and to generate records in the device for checks. To use the application audit function, you must configure an application control policy in the behavior policy module. Only records that are audited according to the policy are displayed in the list, as shown in the figure below.

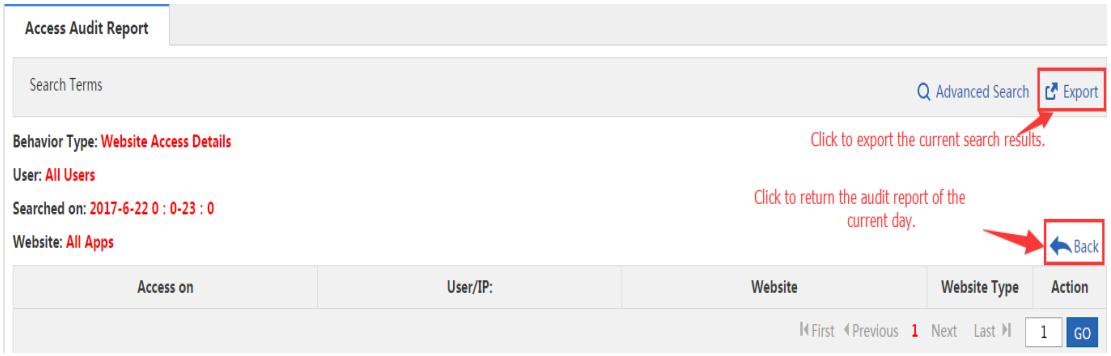



VPN access indicates whether a user accesses the Internet via VPN in the audited record.

6. Advanced Search

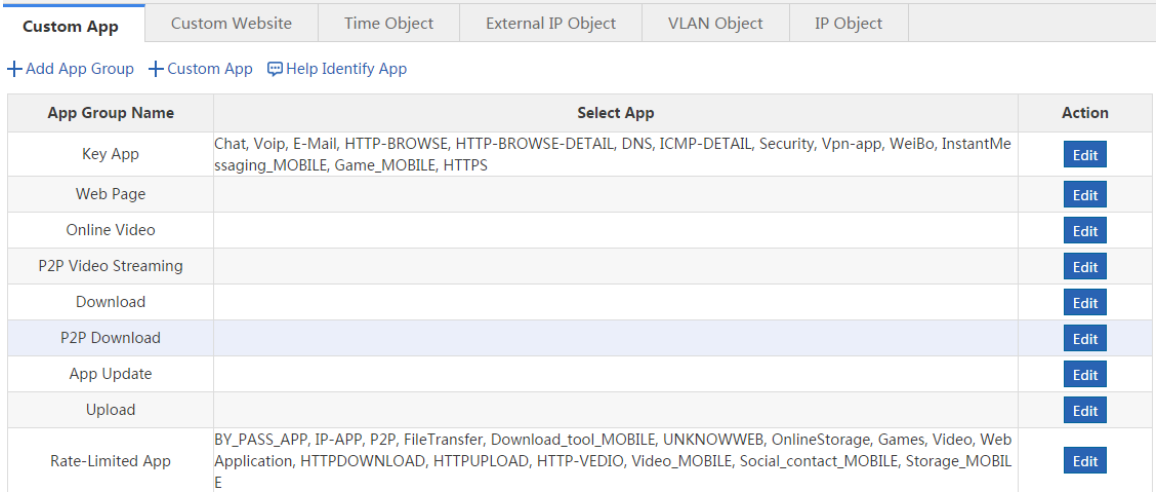
Click  to query records about website access within a specific time range. The advanced search page is shown in the figures below.




## 1.3.10.4 Object

### 1.3.10.4.1 Custom App




| App Group Name | Select App | Action |
|---|---|---|
| Key App | Chat, Voip, E-Mail, HTTP-BROWSE, HTTP-BROWSE-DETAIL, DNS, ICMP-DETAIL, Security, Vpn-app, WeiBo, InstantMessaging_MOBILE, Game_MOBILE, HTTPS | Edit |
| Web Page | | Edit |
| Online Video | | Edit |
| P2P Video Streaming | | Edit |
| Download | | Edit |
| P2P Download | | Edit |
| App Update | | Edit |
| Upload | | Edit |
| Rate-Limited App | BY_PASS_APP, IP-APP, P2P, FileTransfer, Download_tool_MOBILE, UNKNOWWEB, OnlineStorage, Games, Video, Web Application, HTTPDOWNLOAD, HTTPUPLOAD, HTTP-VEDIO, Video_MOBILE, Social_contact_MOBILE, Storage_MOBILE | Edit |

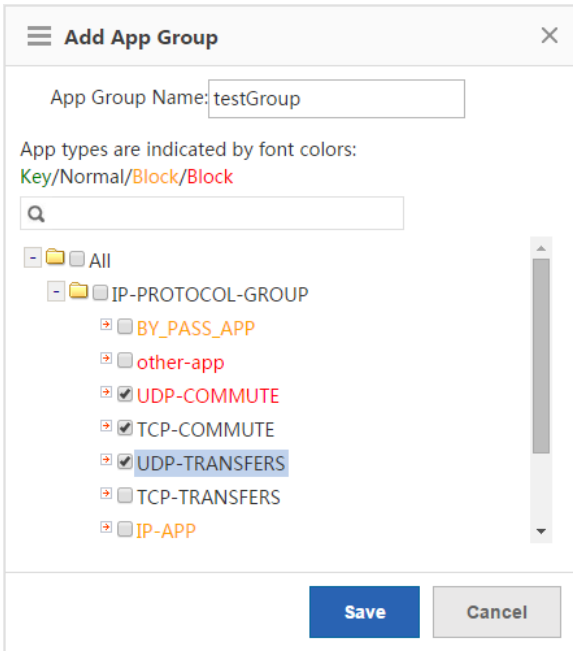
This page lists all application groups and applications contained in each application group in the system. Application groups of the key type, rate-limited type, block type, and normal type are application groups defined in the system and applications of other types are custom application groups.

- **App Group**

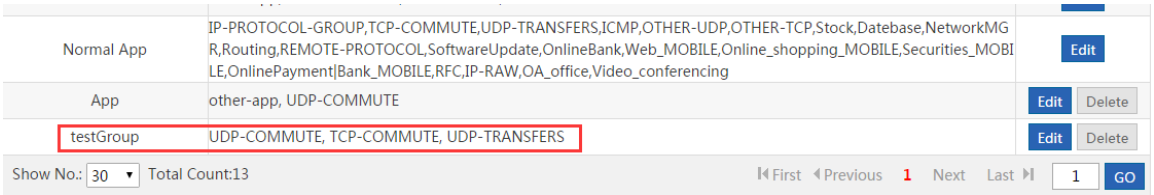
Application groups help users to plan and manage the use of internal applications conveniently. It ensures smooth LAN access and prevents bandwidth waste.

4. Adding a custom application group

Click + Add App Group to custom an application group.

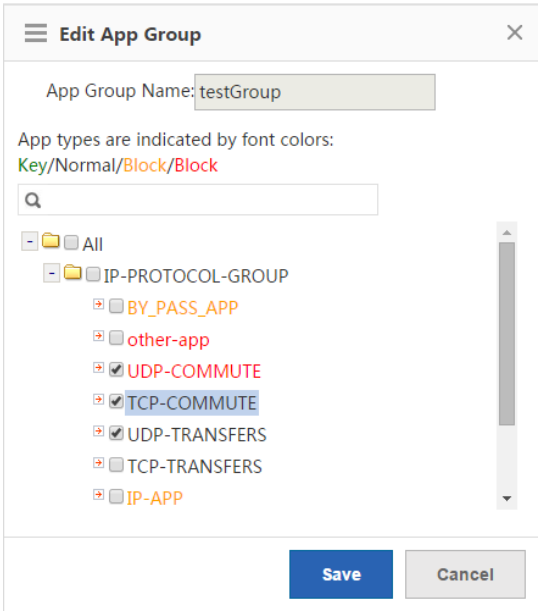



Enter a name in **App Group Name** and click **Save**. Then, the application group is displayed in the list.

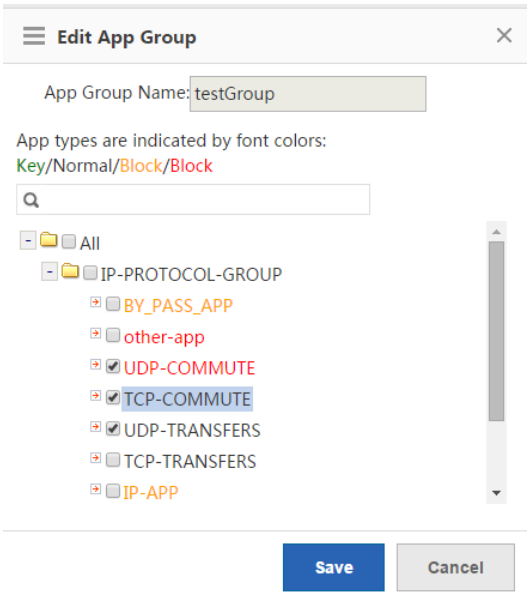



5. Editing an application group

Click Edit in a row of the list on the custom application group page to re-custom applications contained in an application group.




In the application group tree, add applications to or remove applications from the application group, and click Save.




Different colors of application names indicate different types of applications as follows:

Green: key applications

Orange: rate-limited applications

Red: blocked applications

Black: normal applications or deselected applications

Applications of the key type, rate-limited type, or blocked type can only be added to one application groups at the same time.

For example, if an application of the rate-limited type needs to be changed to the key type, delete the application from the rate-limited application group, and then add it to the key application group.

6. Deleting an application group

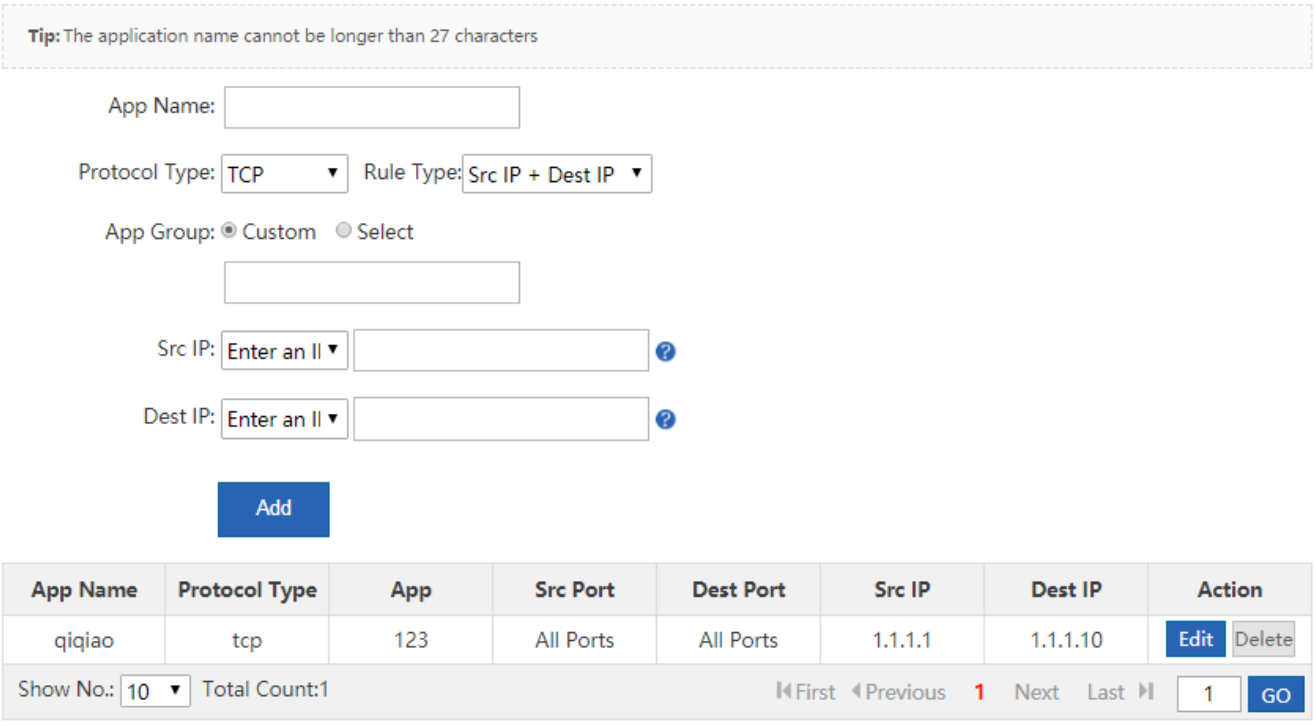
Click Delete in a row of the list on the custom application group page to delete a custom application group. The system application groups (that is, application groups of the key type, rate-limited type, blocked type, and normal type) cannot be deleted.

- **Custom App**

Apart from built-in network applications in the system, you can custom other network applications, for example, a port-based application or a target server-based application. Both built-in applications in the system and custom applications can be used for network application control, bandwidth management, and real-time network application monitoring in policies.

Note: Custom applications have the highest priority. That is, when a custom application collides with a built-in system application (for example, on the same port), the system prioritizes the custom network application.

On the **Custom App** page, click + Add Custom App. The custom application configuration page is displayed.



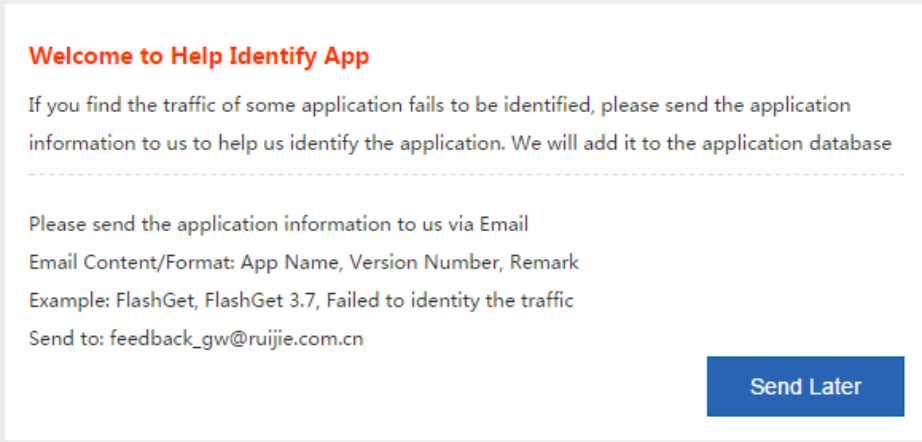

Create a custom application object: Enter a custom application name, set **Protocol Type**, **Rule Type**, and **App Group** (self-define an application type or use a built-in application type), enter the source or destination port and source or destination IP address based on the selected rule type, and click Add.

Edit a custom application: Select an application to be modified and click Edit.

Delete a custom application: Select an application to be deleted and click Delete.

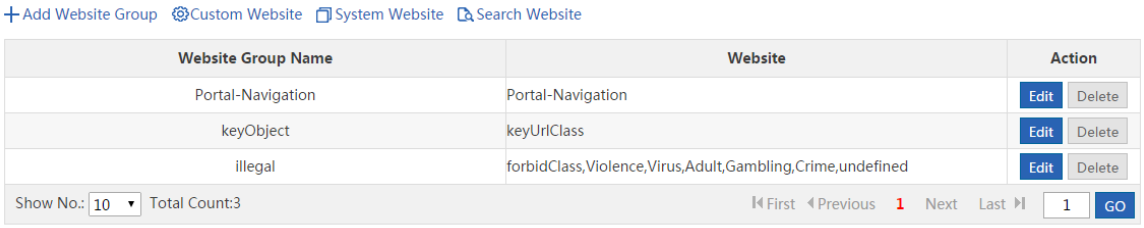
- **Help Identify App**

If the device cannot correctly identify the traffic of a network application,, click Help Identify App, and provide feedback as prompted. Ruijie Cloud Center will analyze the reported application and add it to the signature database to meet your requirements.




### 1.3.10.4.2 Custom Website

The **Custom Website** configuration page is shown in the figure below. This page displays all existing website groups and websites contained in each website group.



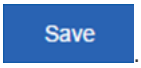

- **Website Group**

Website groups help users to plan and manage types of websites accessed by LAN users conveniently. It ensures smooth LAN access and prevents bandwidth waste.

4. Adding a website group

Click  to custom a website group.



Enter the website group name, select the website types to be contained in the website group, and click  .

5. Editing a website group

Click  in a row of the list on the custom website group page to edit the website types contained in a website group.



In the website group tree, add websites to or remove websites from the application group, and click  .

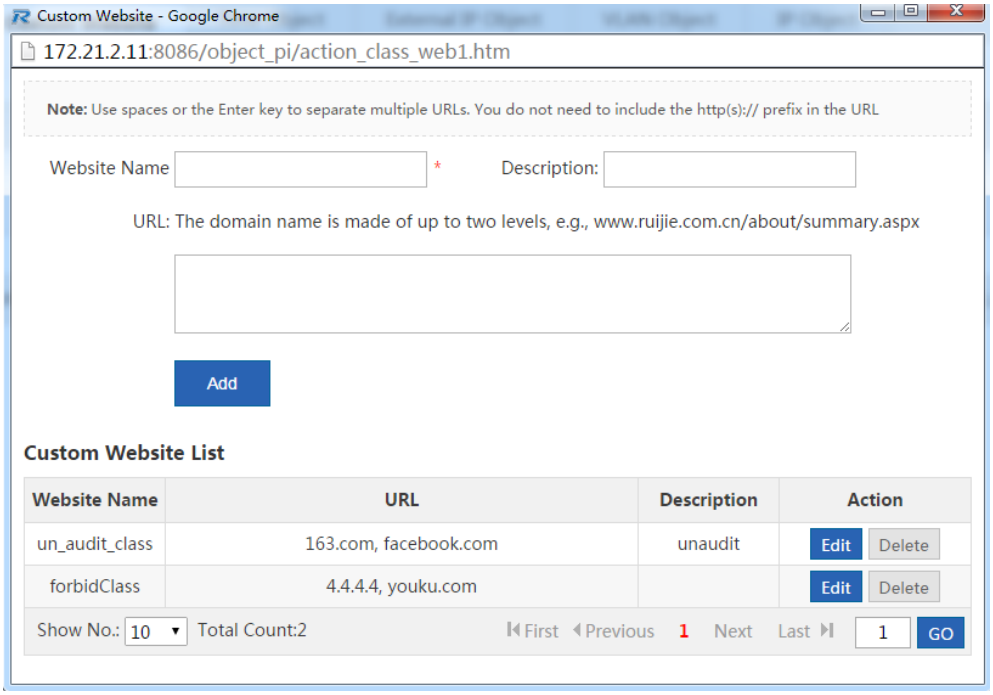
6. Deleting a website group

Click Delete in a row of the list on the custom website group page to delete the selected website group.

- **Custom Website**

Apart from built-in websites in the system, you can custom other websites, for example, classify several similar websites into one type. Both custom and built-in websites of the system can be applied to behavior policies.

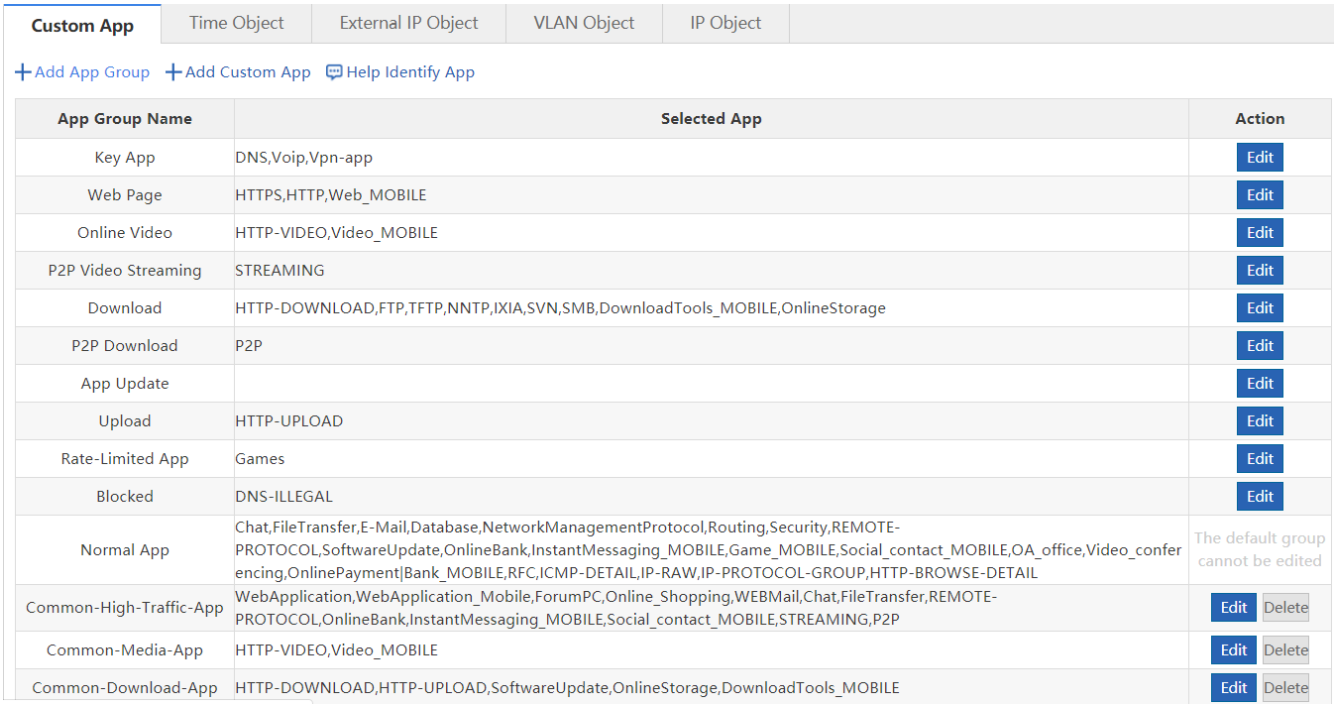
On the **Custom Website** page, click Custom Website. The custom website configuration window is displayed.




Create a custom website: Enter the website name, description, and website domain names contained in the website (separate multiple domain names by a comma (,)), and click Add. A maximum of 100 custom websites can be configured in the system.

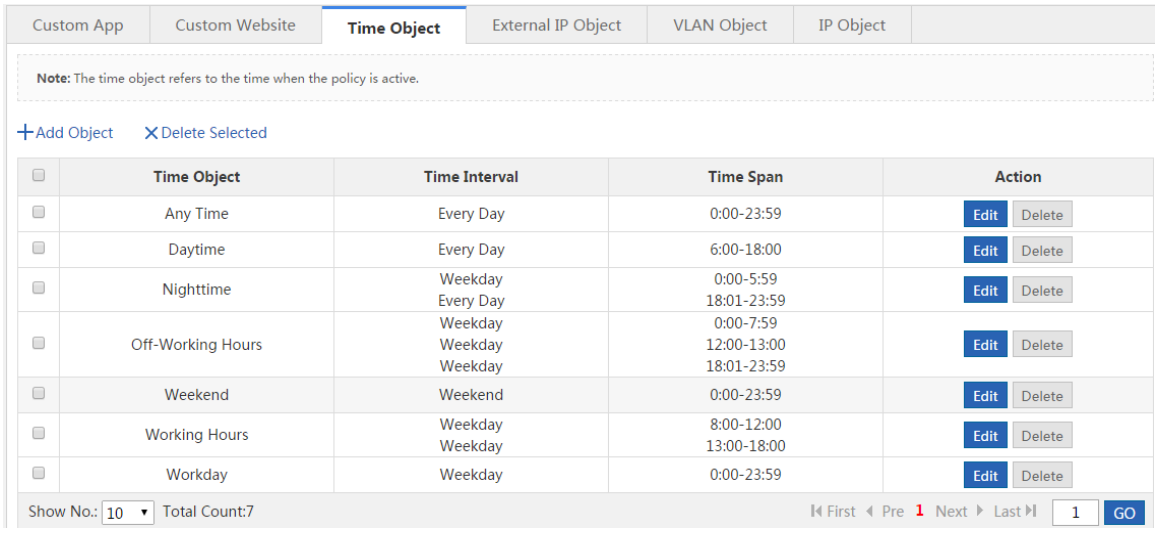
Edit a custom website type: Select a website type to be modified and click Edit.

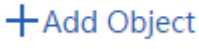
Delete a custom website type: Select a website to be deleted and click Delete.



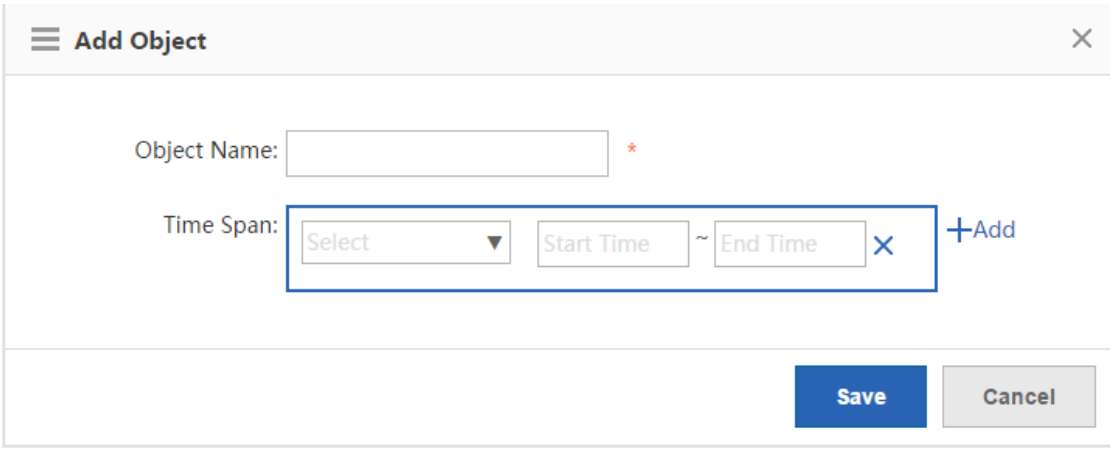

## 1.3.10.4.3 Time Object

On the **Time Object** page, you can custom a time object for setting a policy.




5. Add a time object: Click 

. In the **Add Object** dialog box, enter the object name and set a time span. Multiple time spans can be set.

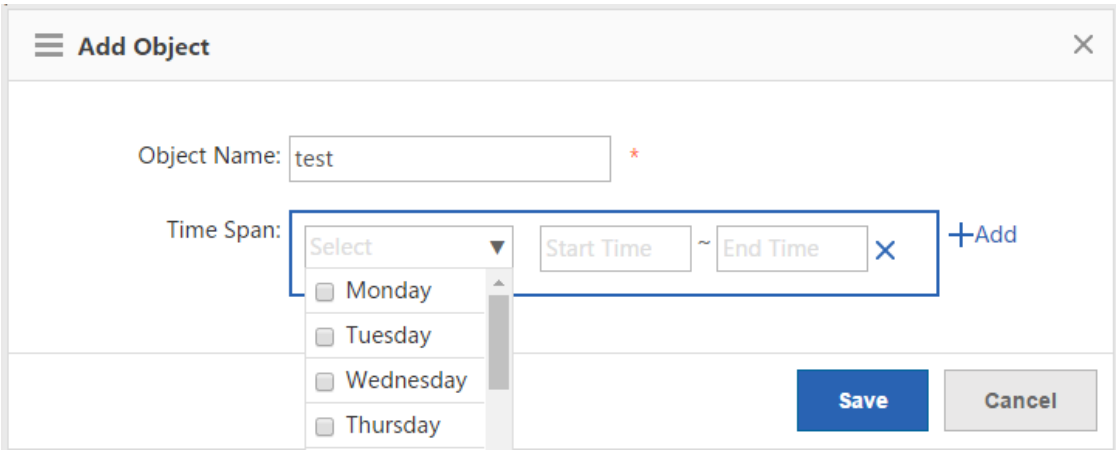



For example, to create a work time object:

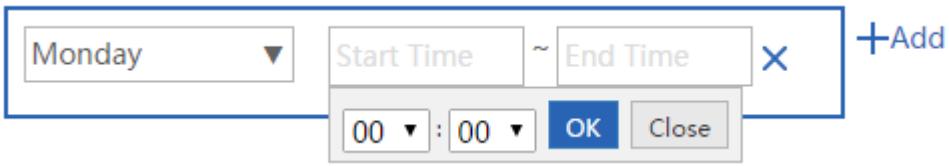
(5) Object name: Enter a time object name in 

.

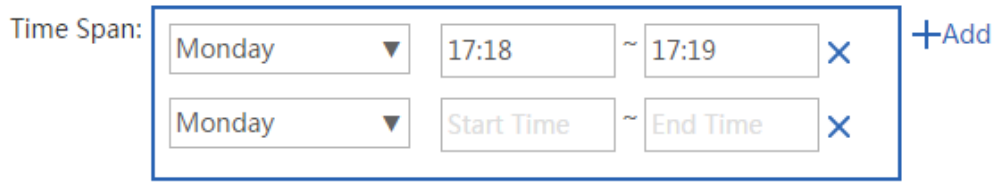
(6) Time span period: Select the period of a time span, that is, select from Monday to Sunday.



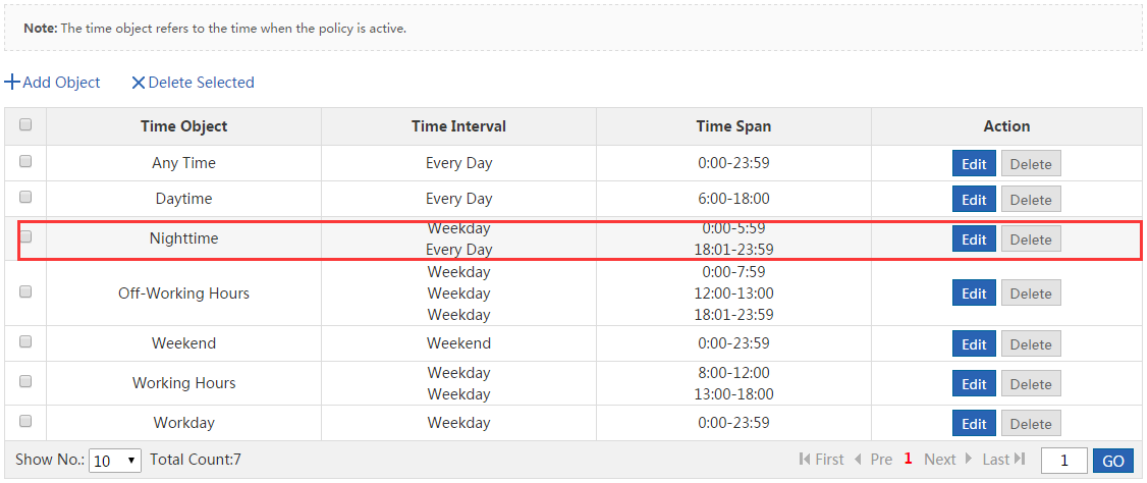

(7) Time span: Set the time span.




(8) Click **Add** to add another time span.



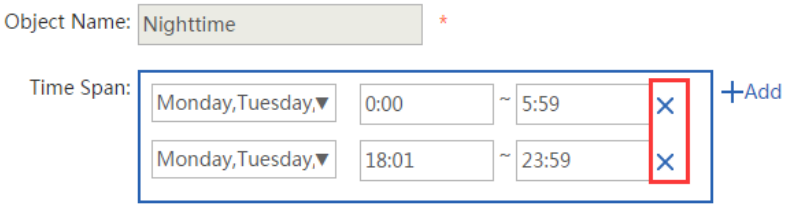

Click Save.




6. Edit a time object: Select a time object to be edited and click Edit. In the displayed dialog box, add, delete, or edit the time span.

7. Delete a time object: To delete a time object, select the time object in the list and click Delete.

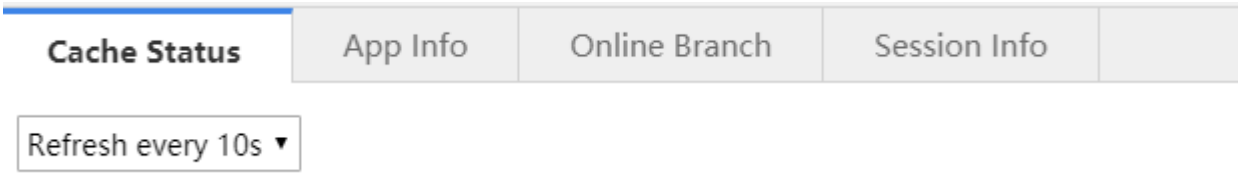
8. Delete a time span: To delete a time span of a time object, select the time object and click **Edit**. In the displayed dialog box, select the time span to be deleted and click ×.




## 1.3.11 Cache

### 1.3.11.1 Realtime Status

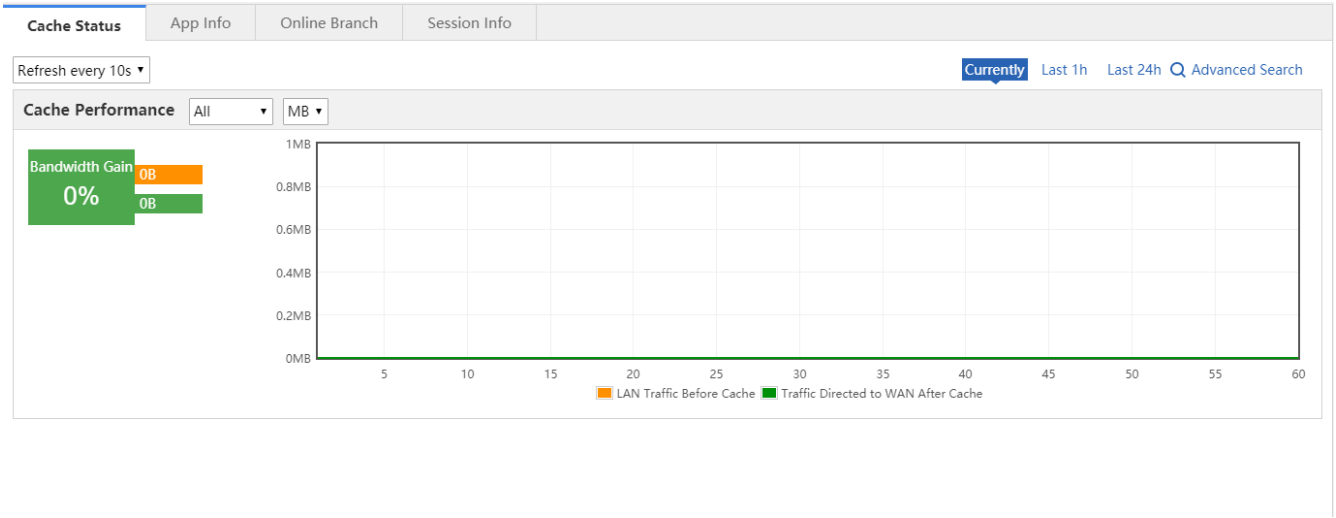
Realtime status refers to the realtime cache status, including the following information: :




If the device serves for a branch, the **Online Branch** feature will not be available.

### 1.3.11.1.1 Cache Status

The traffic tendency before cache and after cache is compared here.



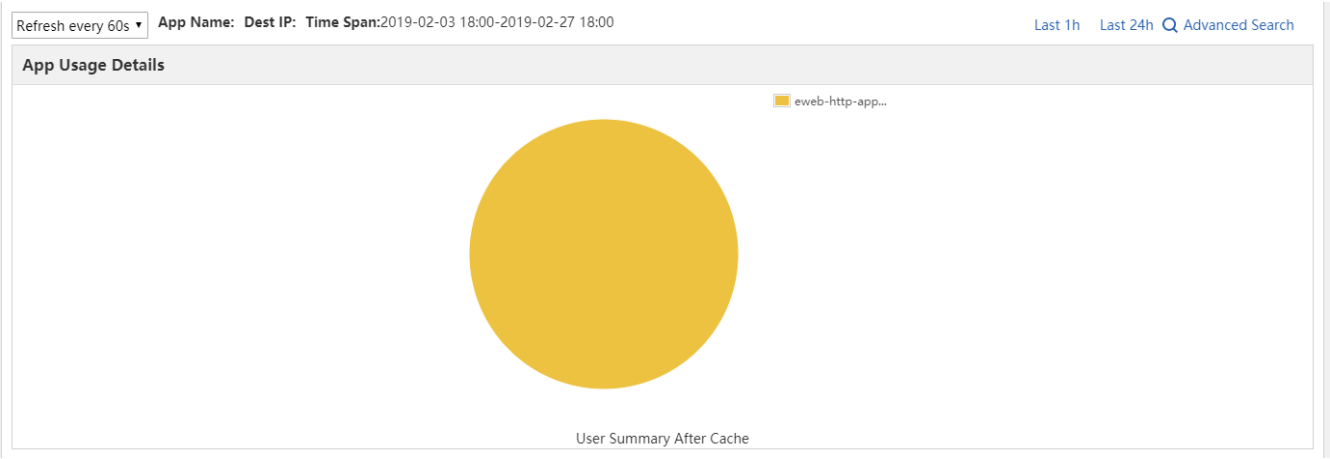

You can view traffic tendency based on time span, including **Currently**, **Last 1h**, and **Last 24h**. Traffic is further divided into **Uplink** or **Downlink**.

Bandwidth gain is the percentage that the saved traffic accounts for the total traffic.

### 1.3.11.1.2 App Info

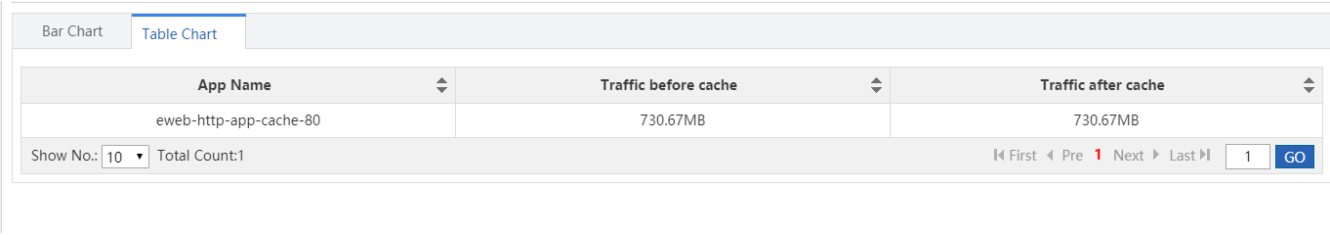
App information contains information about cached Apps.

The pie chart shows the top 10 Apps by cache traffic.




The bar chart shows the top 10 Apps (before and after cache) by cache traffic.

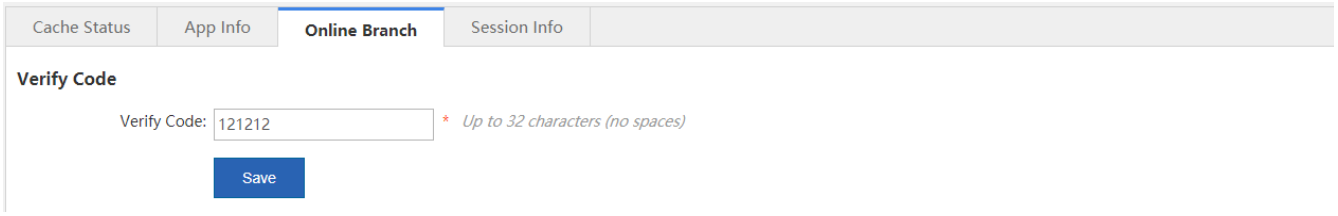

The table chart shows all Apps (before and after cache).



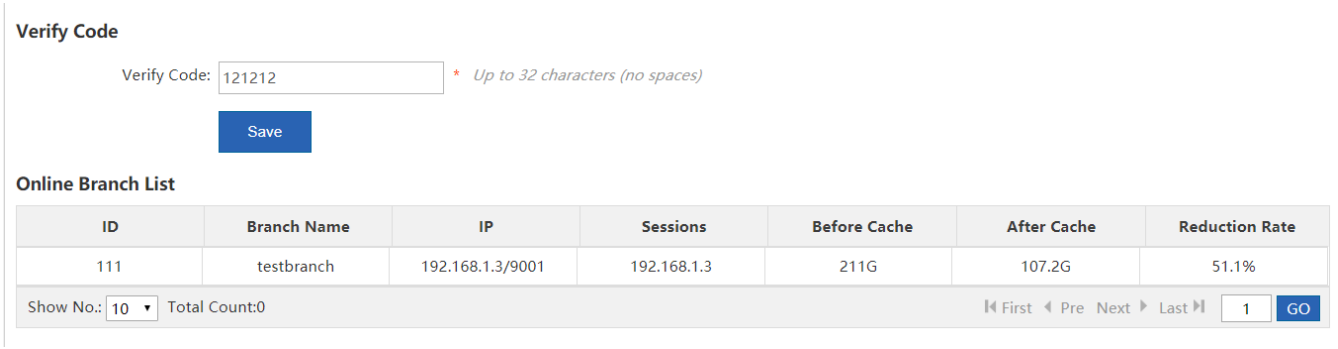

You can view traffic tendency based on time span, including **Last 1h**, and **Last 24h**. Traffic is further divided into **uplink** and **downlink** traffic.

### 1.3.11.1.3 Online Branch

The verify code is used for the branch to connect to headquarter. If you change the verify code, please notify the branch of the change.



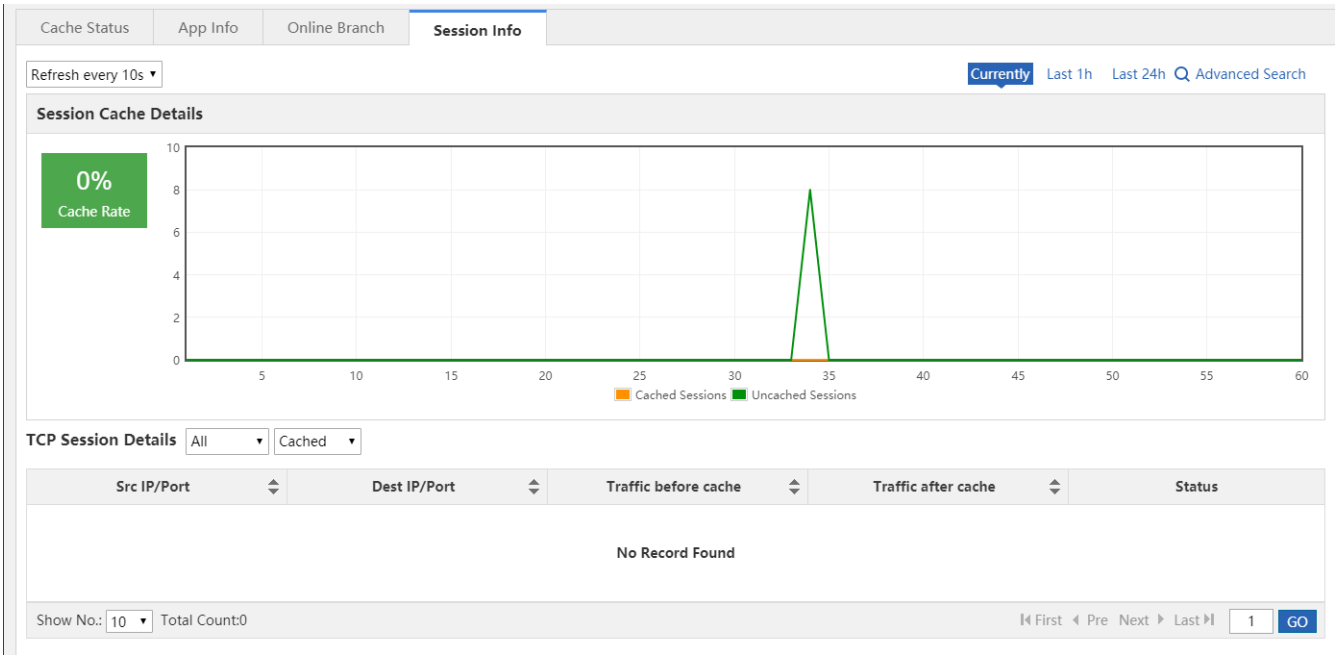

The online branch list contains branches already connected to the headquarter.




Reduction rate is the percentage that the saved traffic accounts for the total traffic.

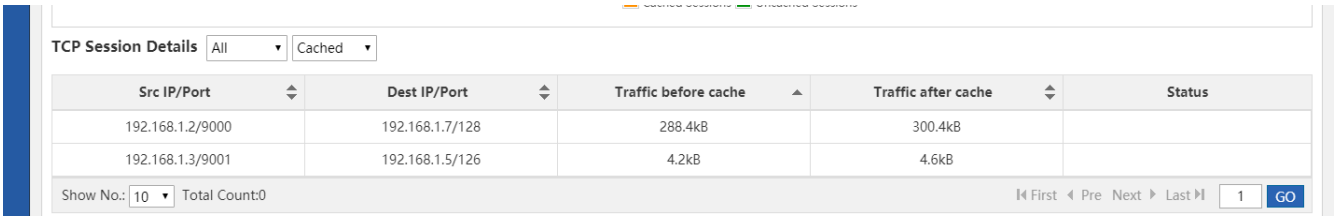
## 1.3.11.1.4 Session Info

Session information contains information about cached TCP sessions.




You can view traffic tendency based on time span, including **Currently**, **Last 1h**, and **Last 24h**. Uncached sessions over last 1 hour or 24 hours are not displayed.

TCP session details are shown as the following figure:




TCP sessions are classified into cached and uncached sessions.

**TCP Session Details** All Uncached

| Src IP/Port | Dest IP/Port | Uncached Traffic |
|---|---|---|
| 172.31.61.207/60768 | 192.168.1.4/6379 | 31B |
| 172.31.61.207/58919 | 192.168.1.4/6379 | 36B |
| 172.31.61.207/57704 | 192.168.1.4/6379 | 31B |
| 172.31.193.12/55451 | 192.168.2.2/445 | 0B |
| 172.31.61.207/60770 | 192.168.1.4/6379 | 31B |
| 172.31.61.207/58309 | 192.168.1.4/6379 | 50B |
| 172.31.61.207/56492 | 192.168.1.4/6379 | 19B |
| 172.31.61.207/61386 | 192.168.1.4/6379 | 31B |

TCP sessions are also divided into uplink and downlink sessions.

### 1.3.11.2 Resource Cache

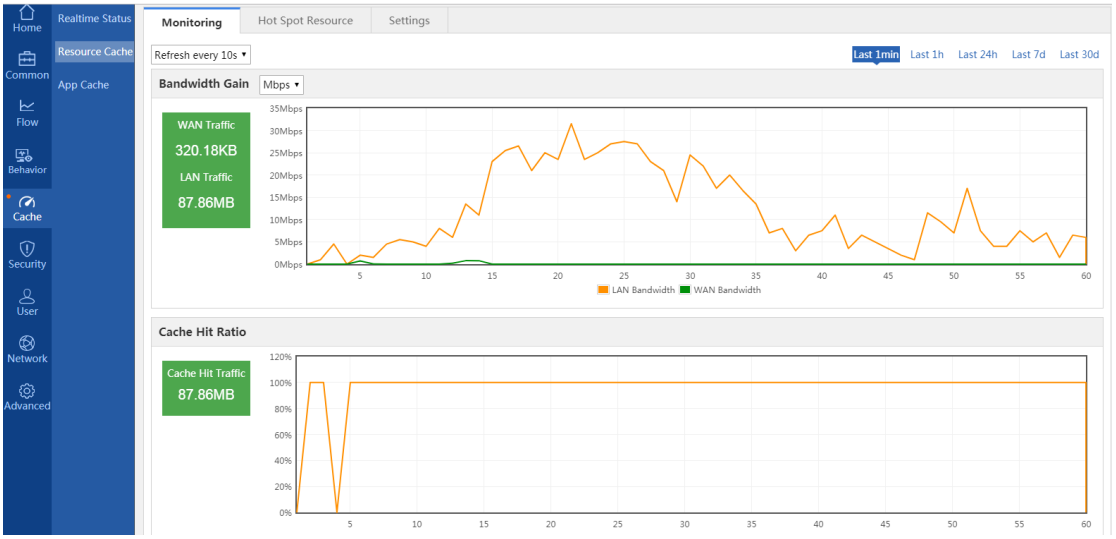
Resource refers to the files that can be downloaded or browsed online, including documents (e.g., PPT, WORD, EXECEL, TXT, RAR, and ZIP), images (e.g., JPG, PNG, and GIF) and videos (MP4, FLV, AVI, RMVB, and 3GP).

Resource cache refers to synchronizing resource from the specified server to a device. Afterwards, users can get the resource directly from the device without crossing WAN.

Resource cache can reduce bandwidth usage and save users from waiting for access.

#### 1.3.11.2.1 Monitoring

You can view bandwidth gain and cache hit ratio based on time span, including **Last 1min**, **Last 1h**, **Last 24h**, **Last 7d**, and **Last 30d**.



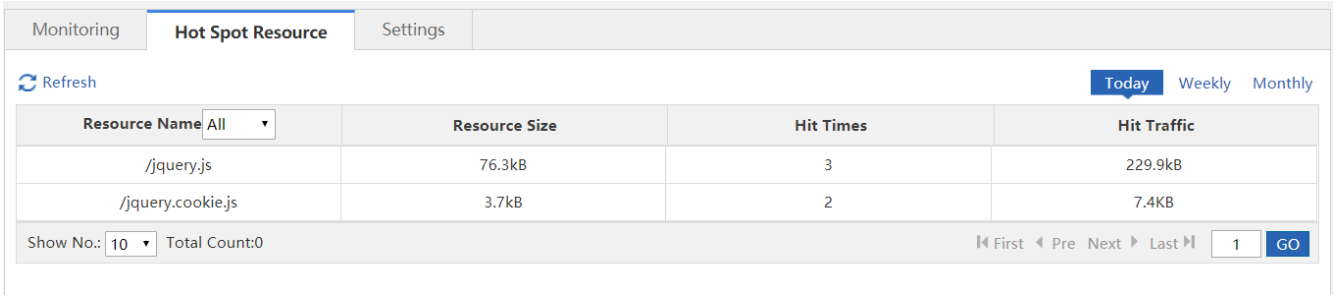

**LAN Traffic**: LAN traffic is the traffic consumed by the user when accessing resource from the device.

**WAN Traffic**: WAN traffic is the traffic consumed by the user when accessing resource from WAN.

**Hit Traffic**: Hit traffic is the cached resource traffic.

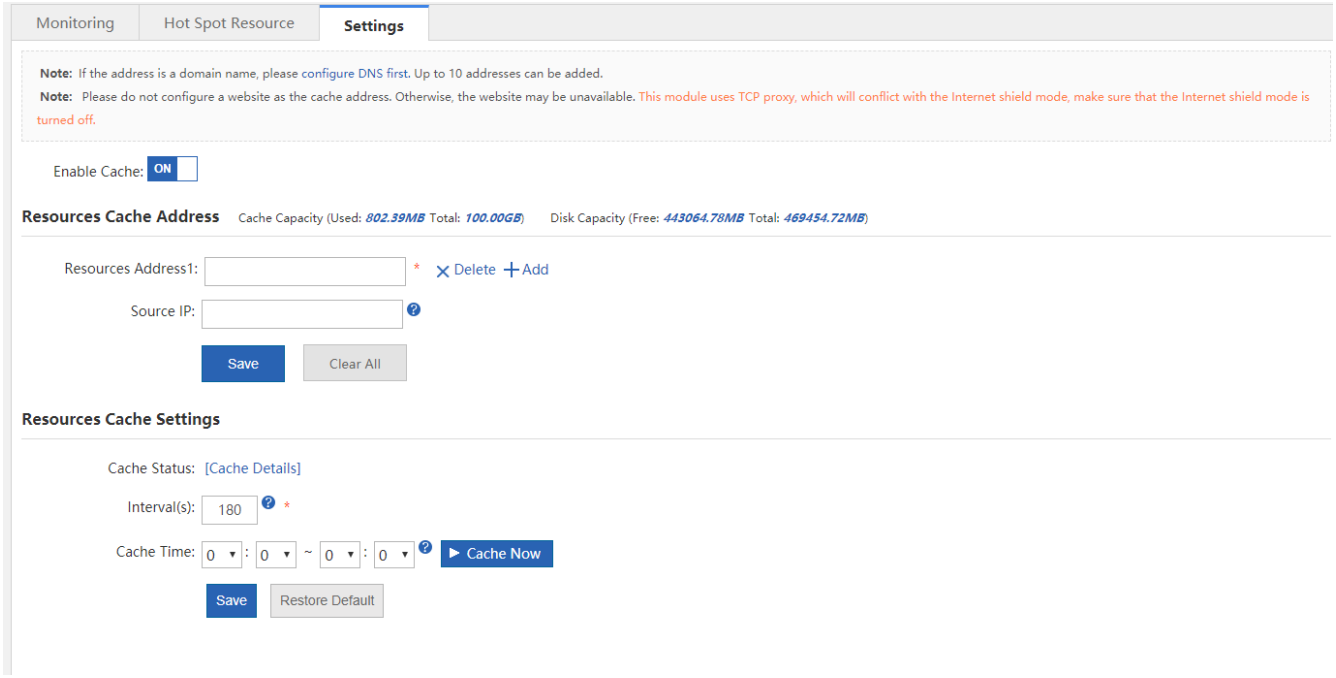
## 1.3.11.2.2 Hot Spot Resource

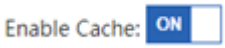
Hot spot resource contains resources cached frequently today, this week and this month.



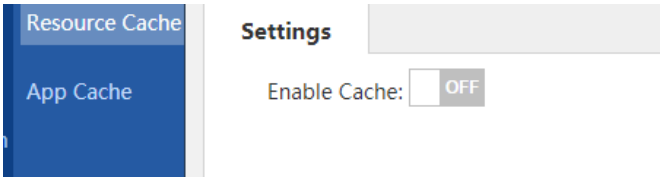

Click Refresh to refresh the hot spot resource list and wait for a few seconds. You can select a resource type from the **Resource Name** dropdown list.

### 1.3.11.2.3 Settings

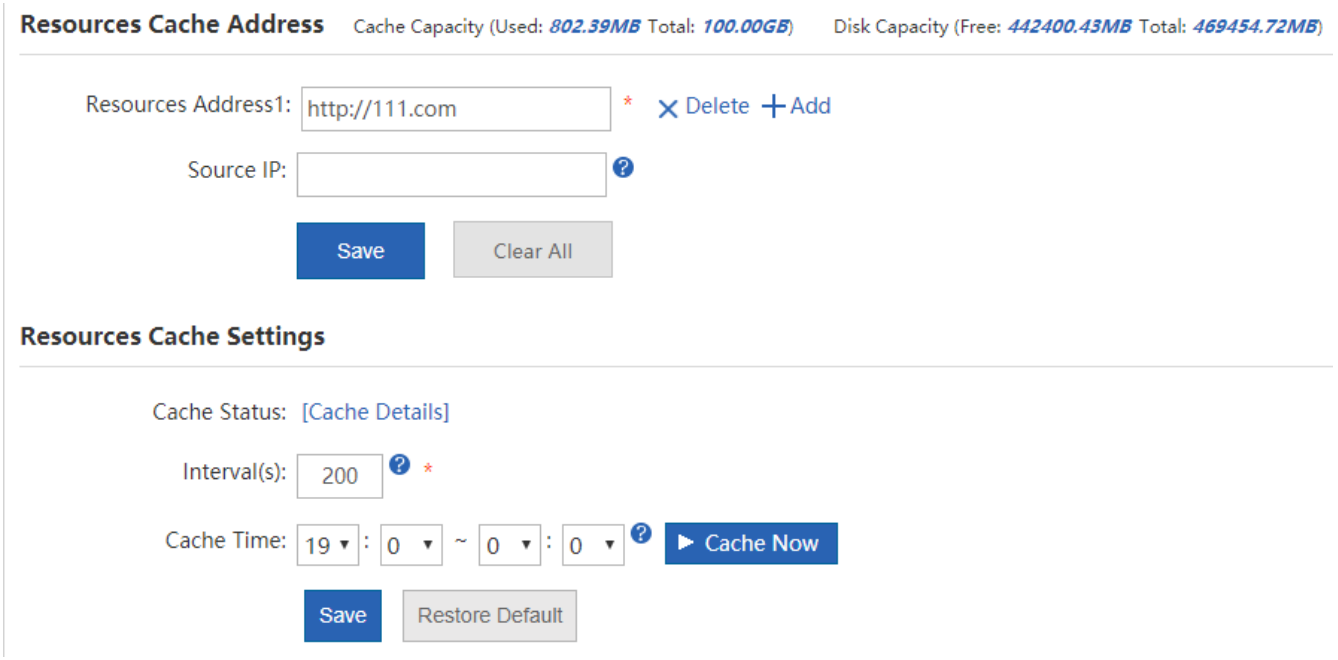



If you want to disable resource cache, please switch off 

. Cache will be disabled as shown in the following figure:




If you want to enable resource cache, please switch on 




**Resource Cache**: The device accesses resources on the specified server.

**Resource Cache Address**: The address must be a URL starting with http://. Up to 10 addresses can be configured. If you enable resource cache without configuring the address, no resource will be cached.

**Note**: If you configure a domain name as the resource cache address, a DNS server address is required.

**Cache Status**: The time when last cache takes place and the cached traffic volume.

**Cache Time**: You can specify a time span for the device to access the resource. It is recommended to avoid peak hours. If the end time is earlier than the start time, e.g., 23:00-3:00, it indicates that resource cache lasts from 23:00 today to 3:00 tomorrow.

**Cache Now**: You can start caching resource right now. Click the button during cache, resource cache will be stopped.

**Note**: If the start time is the same as the end time, resource will be cached all day long.

### 1.3.11.3 App Cache

The **App Cache** configuration page is shown in the figures below.

App Cache

**Note:** If address is a domain name, please configure DNS first. . The domain name cannot start with https. This module uses TCP proxy, which will conflict with the Internet shield mode, make sure that the Internet shield mode is turned off.

**Tip:** The Apple store server address is 'iosapps.itunes.apple.com', it is recommended to add this address.

APP Cache: ON Cache Details

APP Cache Capacity (Used: *1.91MB* Total: *100.00GB*) Disk Capacity (Free: *443064.73MB* Total: *469454.72MB*)

**Select App**

**Phone App:** iOS-based App Android-based App

**Office App:** Windows Patch 360 Safety Guard Patch Tencent Computer Manager

**Custom Type:** Use | to separate types. Example: ipa|apk

**Custom Feature:** Use | to separate features. Example: windowsupdate|360safe

**File Type:** ipa

**URL Feature:**

Save Clear All

## APP Server Address

All HTTP (Port 80)

**Address1:** * Delete

+Add

Save Clear All

## Cache Specified App App Name (Android-based and iOS-based Application)

**App Name1:** * Delete

+Add

Save Clear All

## Cache Specified App Time Window

**Address1:** * Delete

+Add

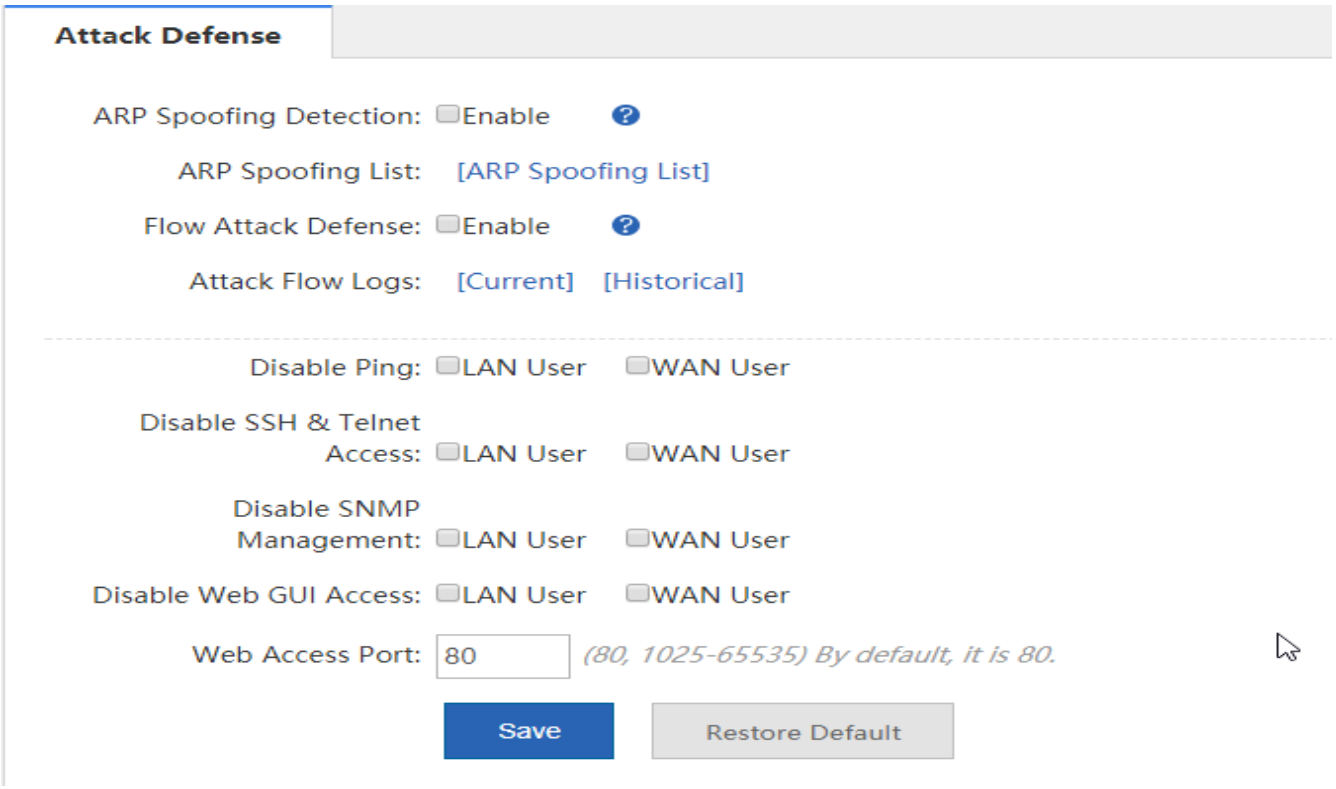
Save Clear All

## 1.3.12 Security

### 1.3.12.1 Attack Defense

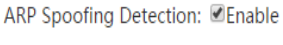
Attack defense can classify, filter, and limit the rate of data packets that need to be processed at the control layer, so as to control data packets and prevent attacks, thereby protecting key resources at the control layer.

The **Attack Defense** configuration page is shown in the figure below.

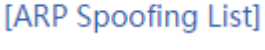



1. ARP attack defense

ARP attack is an attack technology against the Ethernet Address Resolution Protocol (ARP). With this attack, attackers can obtain encapsulated data packets on the LAN and even tamper the packets, and disconnect specific PCs or all PCs on the network.

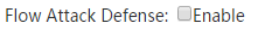
**ARP Spoofing Detection**: Select 

to limit the rate of ARP packets received locally. Up to 10 ARP packets are processed per second, and excessive ARP packets will be filtered out.

**ARP Spoofing List**: Click 

to list the hosts that are suspected to initiate ARP spoofing.

2. Flow attack defense

**Flow Attack Defense**: Select 

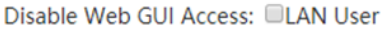
to enable flow attack defense. Flow attack packets that are beyond the threshold are dropped. An average of 200 packets are dropped per second and 300 packets are allowed to be dropped upon traffic burst.

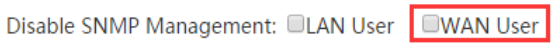
**Attack Flow Logs**: Click 

to display logs about current attacks or click 

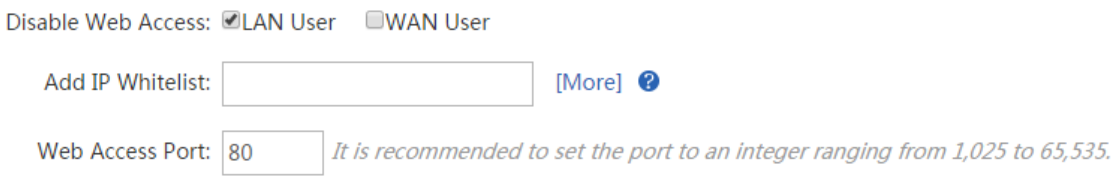
to display logs about historical attacks of the system.

3. Other attack defense

**Disable Web GUI Access**: Select **LAN User** in 

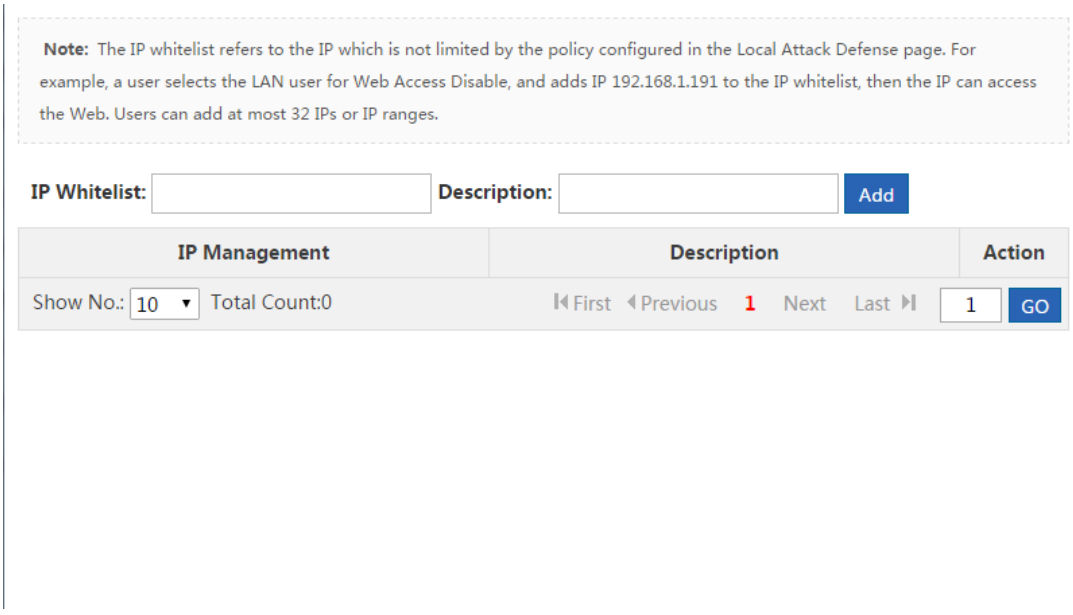
to forbid LAN users from logging in to the Web management system of the device. Select **WAN User** in 

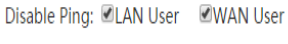
to forbid WAN users from logging in to the Web management system of the device.




**Add IP Whitelist**: Please enter the IP addresses of administrators, that is, IP addresses exempt from rate limit, so as to improve the device management efficiency for administrators. Click 

to display and manage IP addresses.

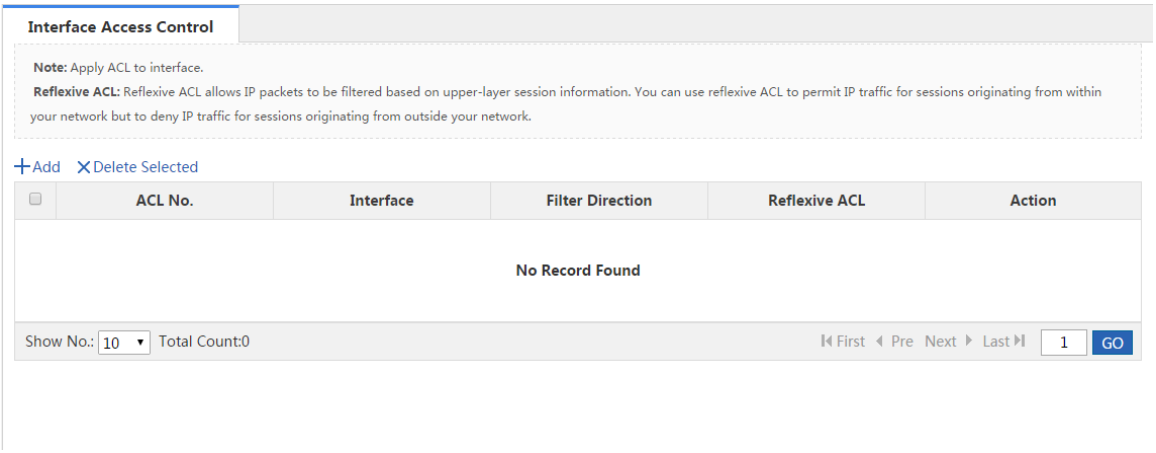



**Disable Ping**: Select 

to forbid LAN users or WAN users from pinging the device.

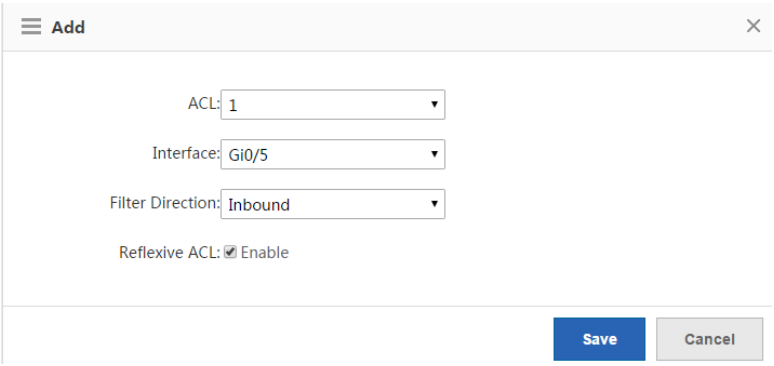
**Web Access Port**: The default port ID is 80. If you change the port ID, you need to add the port ID to the URL in the address bar when managing the device, that is, you need to enter **http://***ip addres:access port* in the address bar to access the device.

### 1.3.12.2 Interface Access Control

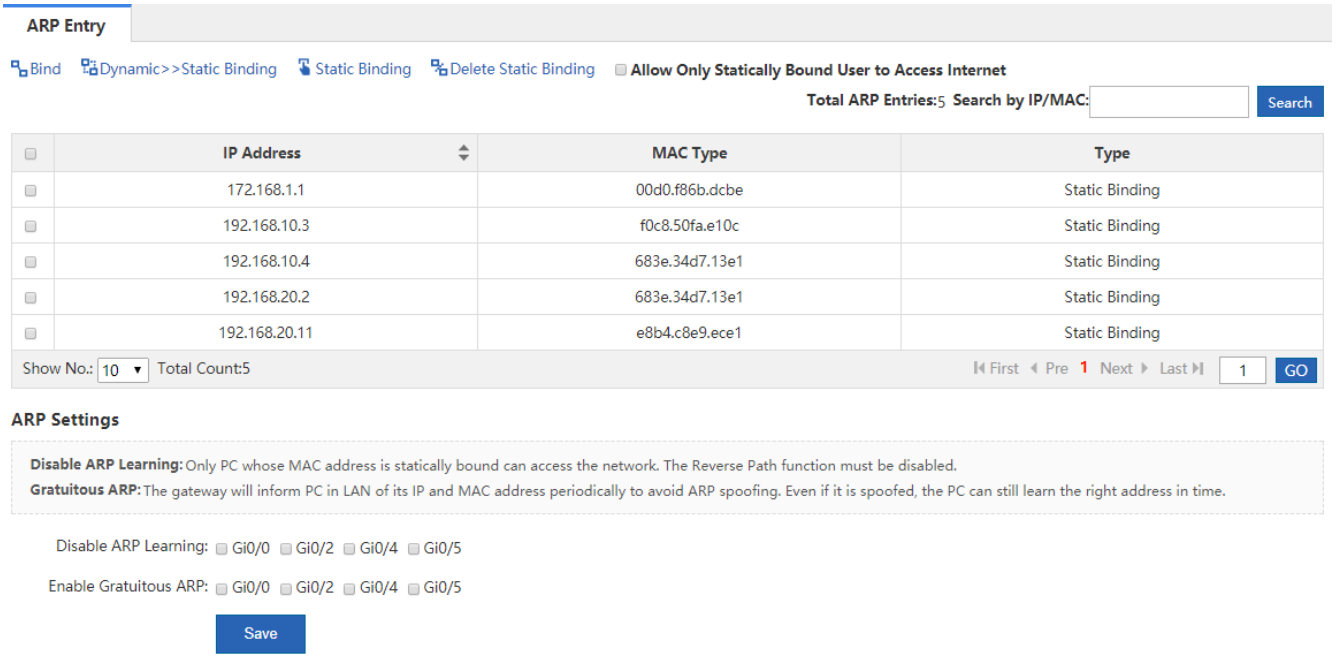



Click +Add . In the **Add** dialog box, select an ACL and match it to an interface, set the packet filter direction (**Inbound** or **Outbound**), and click Save to generate an ACL, which serves as a firewall.

The firewall supports status-tracking-based ACLs. Select Reflexive ACL: Enable to configure reflective ACLs.



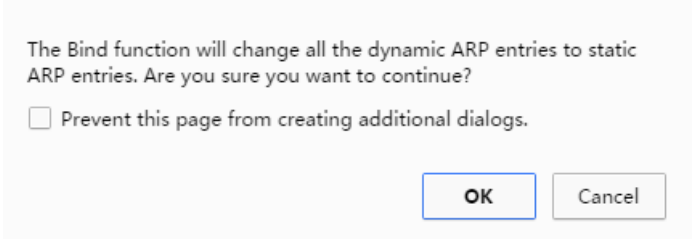
## 1.3.12.3 ARP Entry



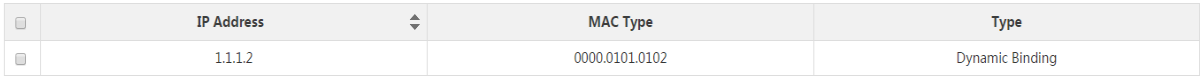

1. One-click binding

The device supports the one-click binding function, which allows users to rapidly bind dynamic ARP entries. Click Bind .

A dialog box shown in the figure below is displayed.




2. ARP entries




The table shown in the figure above lists IP/MAC entries bound statically or dynamically.

3. Static binding deletion

On the **ARP Entry** page, select IP/MAC entries, for which static binding needs to be deleted, and click Delete Static Binding .

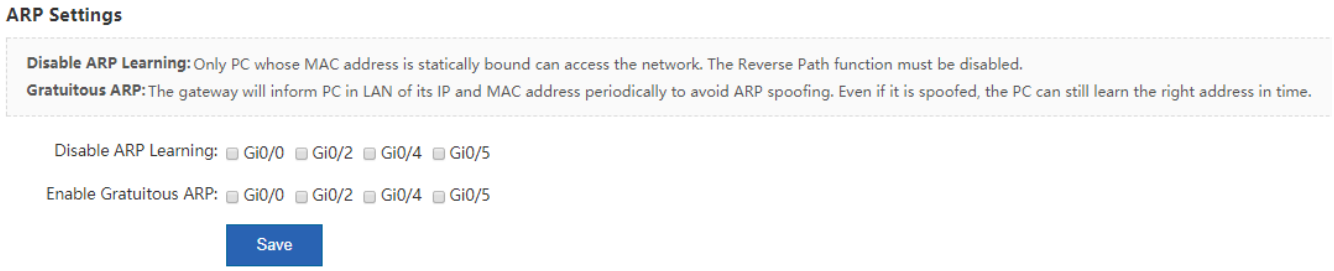
4. Change of dynamic binding to static binding

On the **ARP Entry** page, select IP/MAC entries, for which static binding needs to be changed to dynamic binding, and click Dynamic>>Static Binding .

5. ARP settings

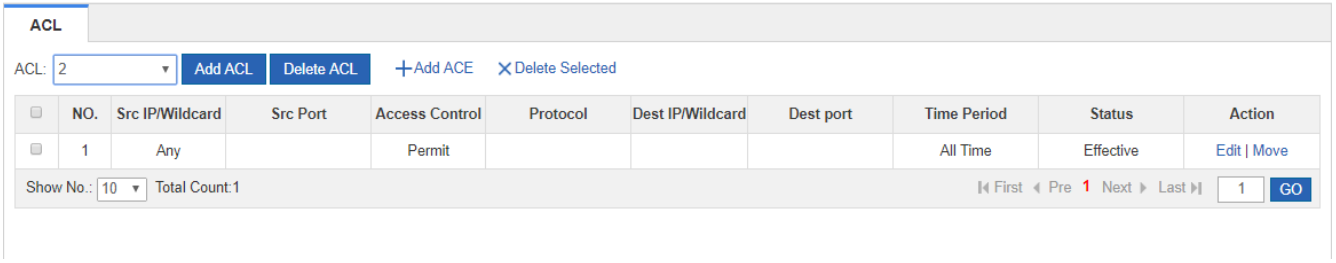
**Disable ARP Learning**: Select an interface, on which ARP learning needs to be disabled. If it is disabled, only PCs bound with MAC addresses statically can access the Internet.

**Enable Gratuitous ARP**: When a network interface of the device functions as the gateway of the connected downlink devices, if a downlink device pretends to be a gateway and the gratuitous ARP function is enabled on the interface, the interface can be configured to send gratuitous ARP requests periodically to advertise its identity of being the authentic gateway.




## 1.3.12.4 ACL

The ACL function allows you to configure ACL objects to enhance network security, as shown in the figure below.




1. Adding an ACL

Click Add ACL. The **Add ACL** dialog box is displayed. Set **ACL Type** to **Standard ACL (Src-address-based Control)** or **Extended ACL (Flow-based Control)**, enter the ACL name, and click OK.


**2.** Adding an ACE

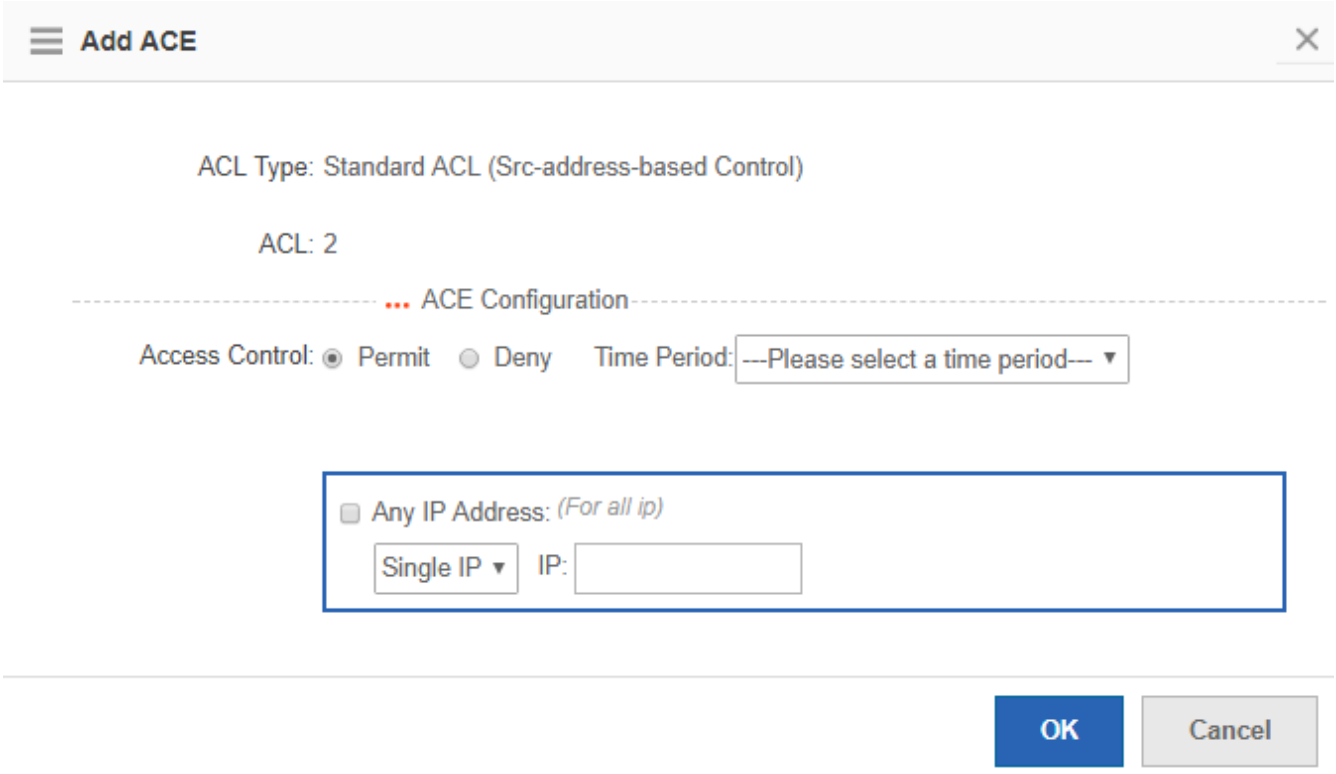
Select an ACL from the 

drop-down list, for which an Access Control Entry (ACE) needs to be added. Click 

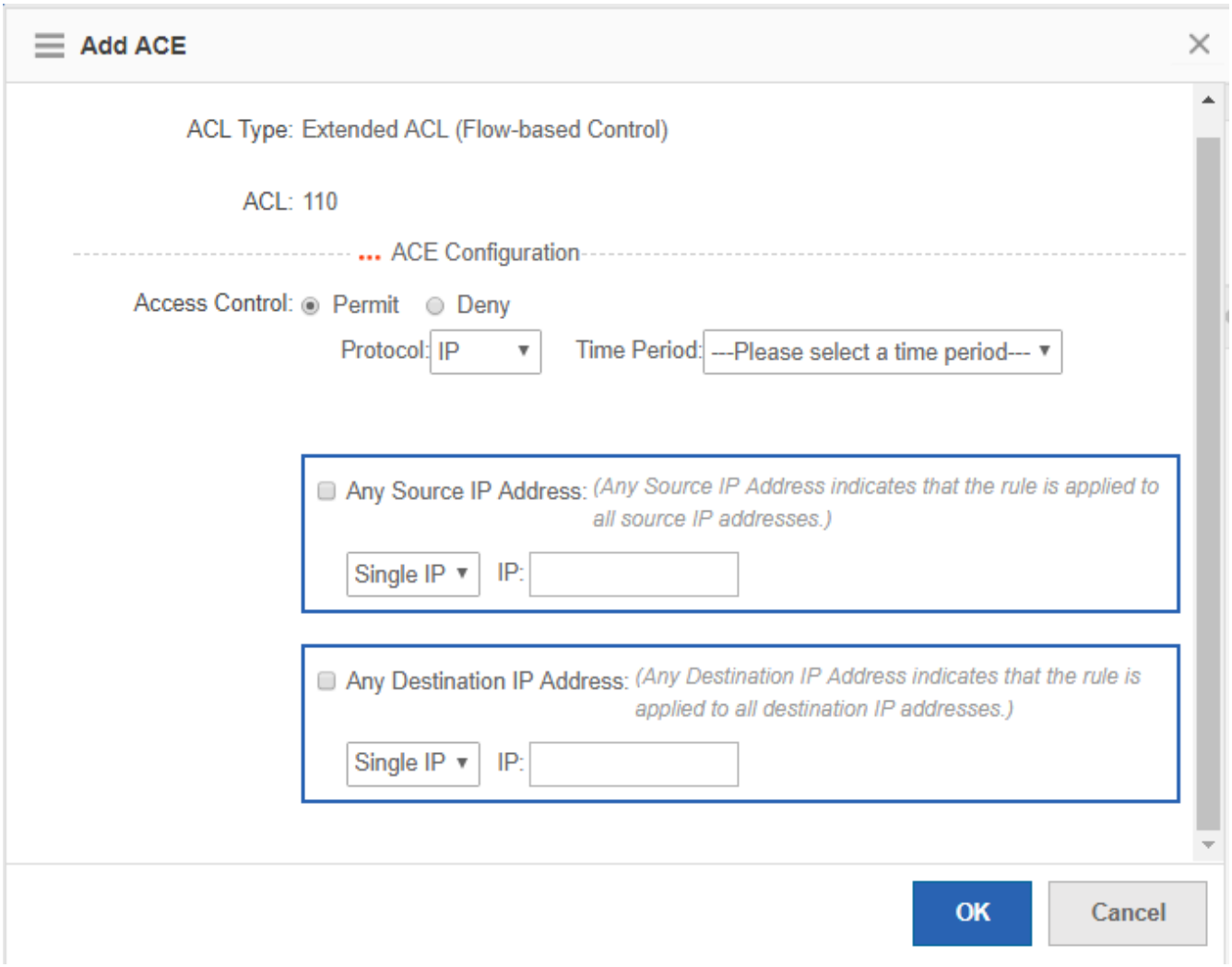
. In the **Add ACE** dialog box, set the ACE.

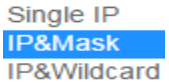
**Standard ACL (Src-address-based Control)**: Select the access control action and effective time, enter the IP address, and click 

to generate a standard ACE.



**Extended ACL (Flow-based Control)**: Select the access control action, protocol type and effective time, configure the source IP address, destination IP address, source port and destination port, and click OK to generate an extended ACE.




Select the address type from 

for the source IP address and destination IP address.

**Single IP Address**: Enter a single source or destination IP address.

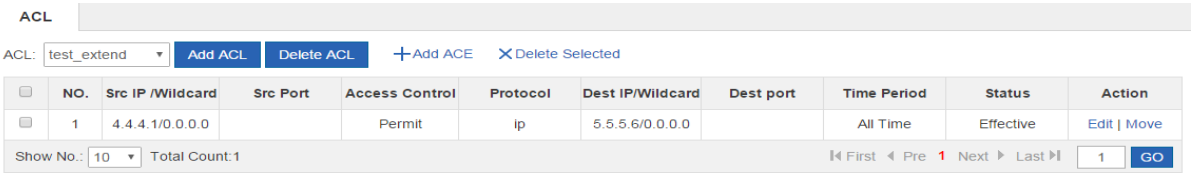
**Mask Configuration**: Enter an IP address range in the form of a mask for the source or destination address.

**Wildcard**: Enter an IP address range in the form of a wildcard for the source or destination address.

1. The source or destination IP address and source or destination port ID can be set to any value.

2. The wildcard mask specifies the bits to be ignored in an IP address when the IP address is compared with other IP addresses. In a wildcard mask, **1** indicates that the corresponding bit in an IP address is ignored and **0** indicates that the bit must be retained. If a wildcard mask is ignored, 0.0.0.0 is considered as the default mask word.

3. **ACL**




Click Move to adjust the sequence of ACEs.

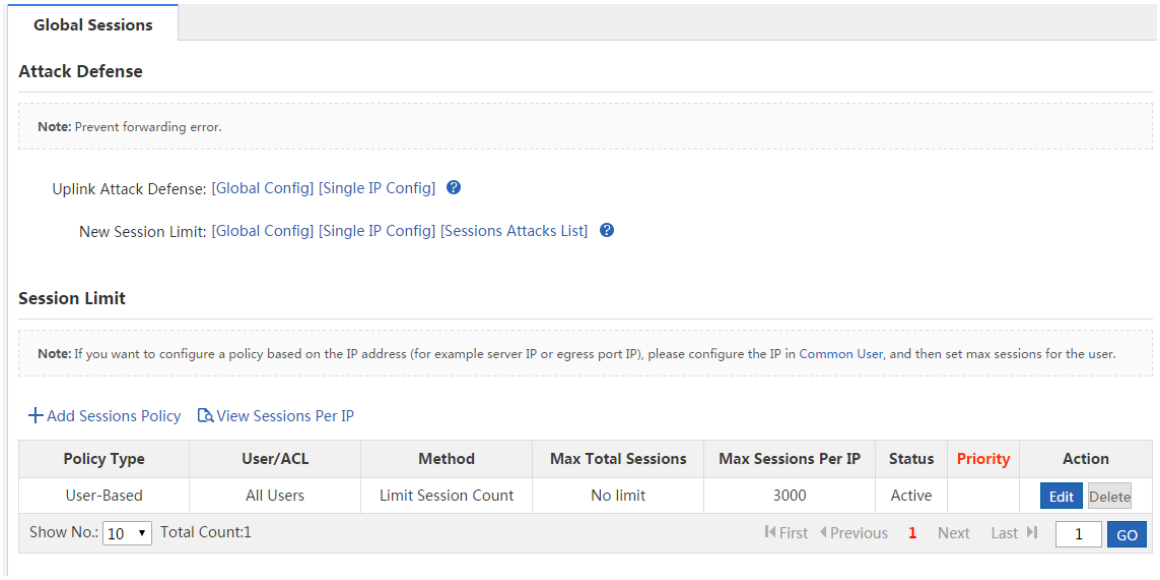
Click Edit to edit the selected ACE.

Click Delete Selected to delete the selected ACE.

The unauthenticated users will be redirected to this URL when access the Internet.

## 1.3.12.5 Max Sessions

The Max session function restricts the total number of sessions that are allowed to pass through the device. The **Global Sessions** configuration page is shown in the figure below




1. **Attack Defense**

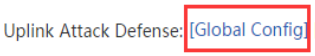
The attack defense function is configured to prevent device forwarding exceptions from abnormal attack behaviors of LAN users and uplink attacks on the LAN, and limit the number of new sessions.

**Note:** Prevent forwarding error.

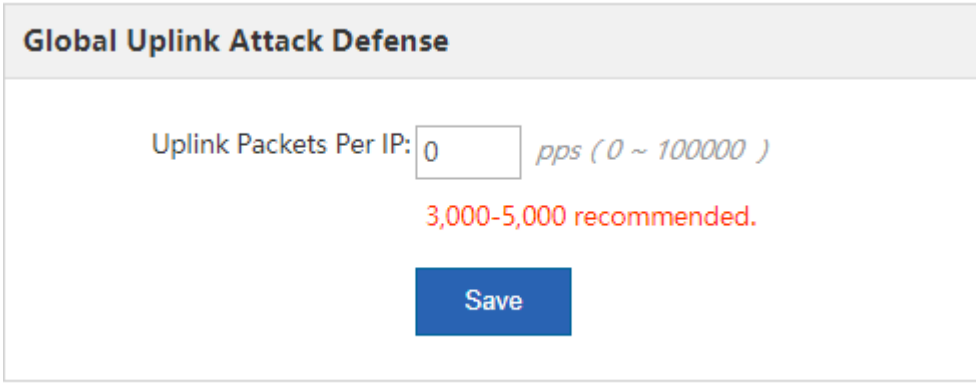
Uplink Attack Defense: [Global Config] [Singal IP Config]

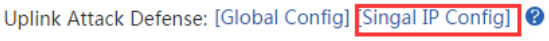
Max New Sessions: [Global Config] [Singal IP Config] [Sessions Attacks List]

- Uplink Attack Defense

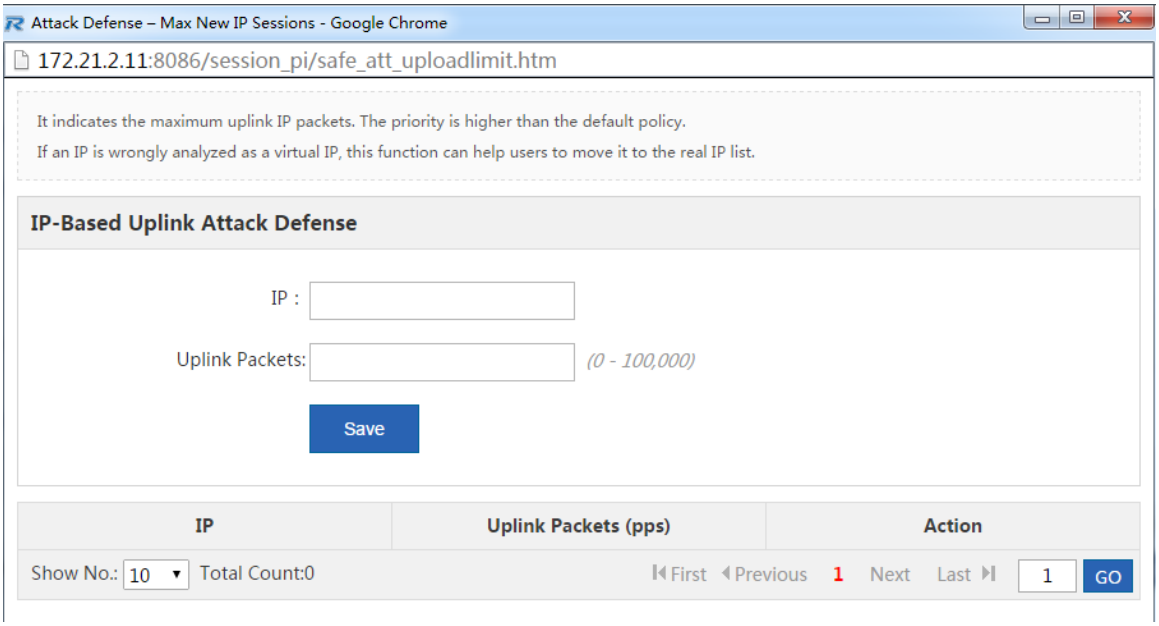
Click **[Global Config]** in 

. In the window displayed, configure the default maximum number of per-IP-based uplink packets per second.



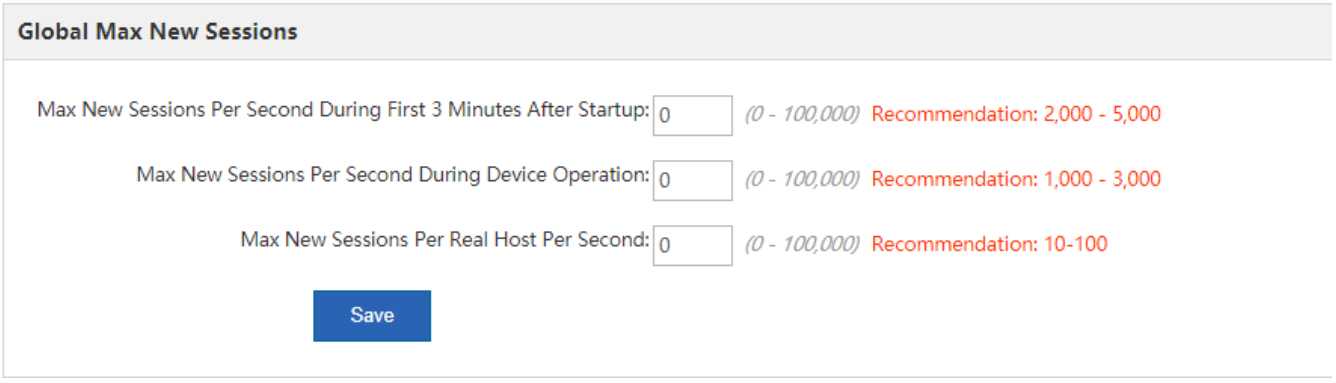

Click **[Single IP Config]** in 

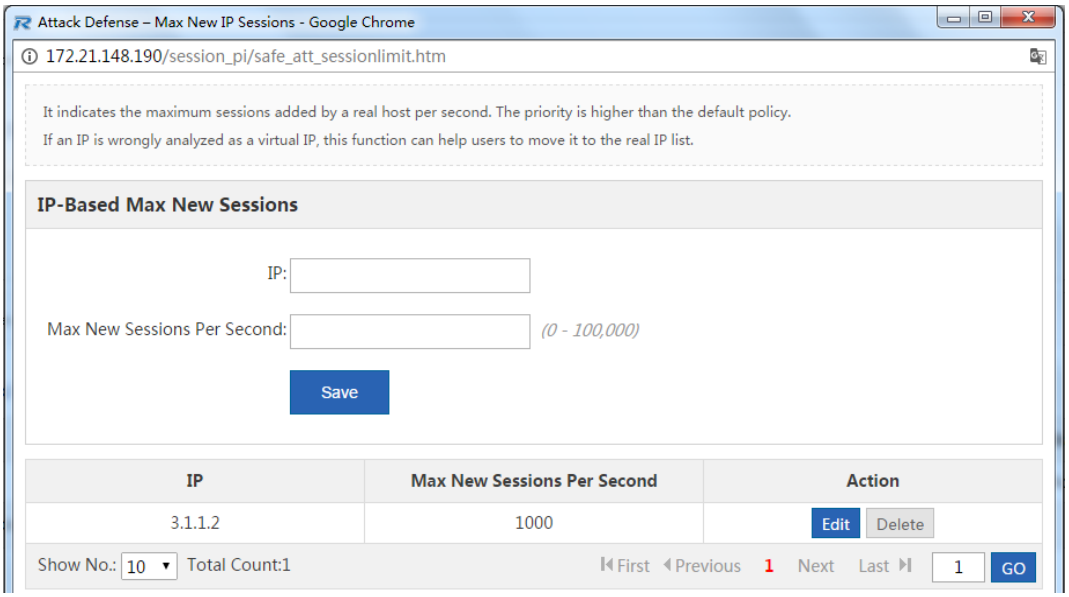
. In the window displayed, configure the maximum number of uplink packets for a specific IP address.

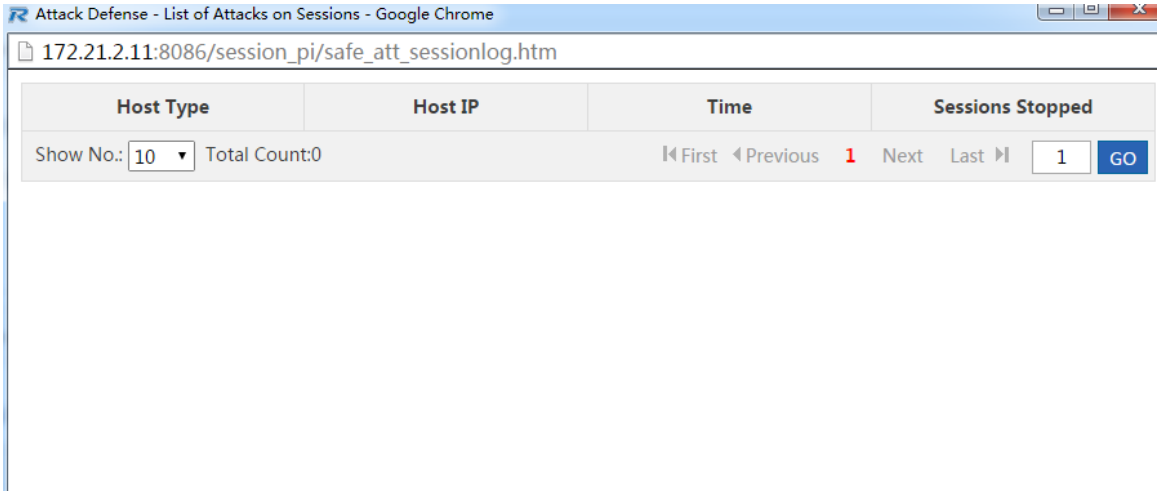



- New Session Limit

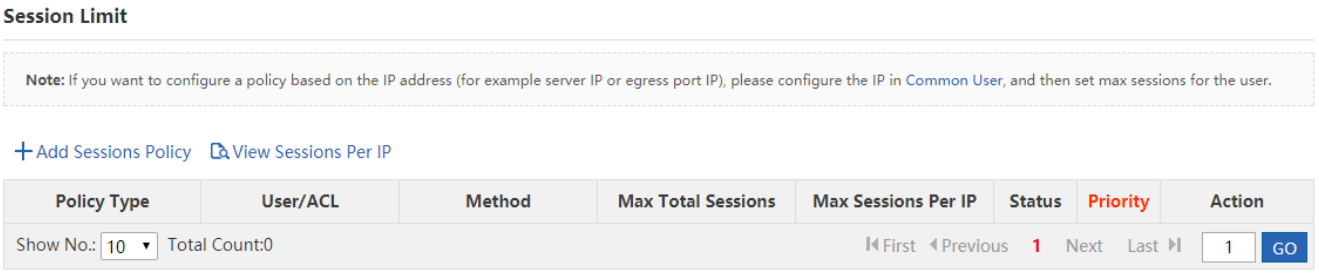
The New Sessions Limit function includes Global Config, Single IP Config, and Sessions Attacks List.



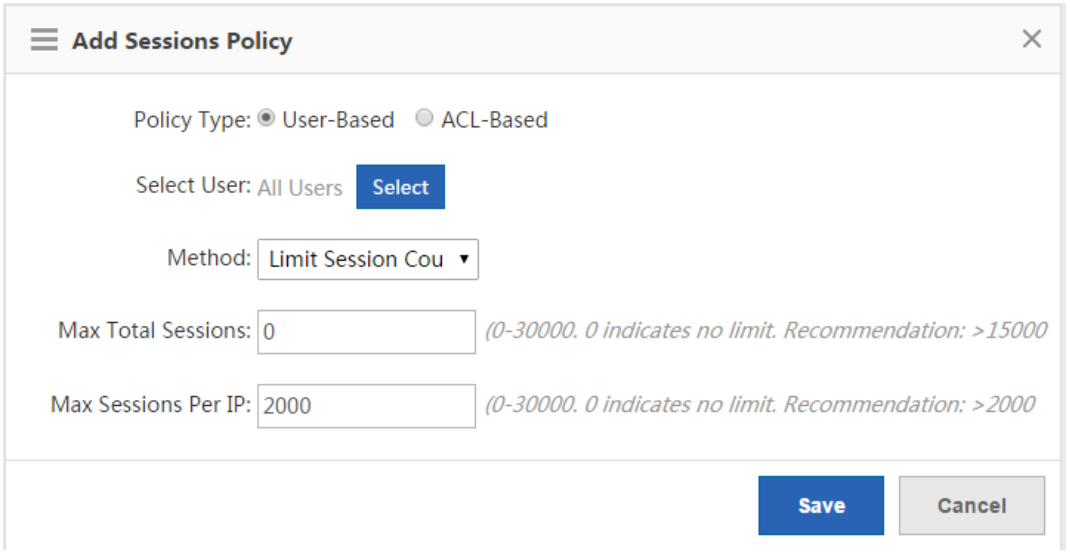




2. **Sessions Limit**

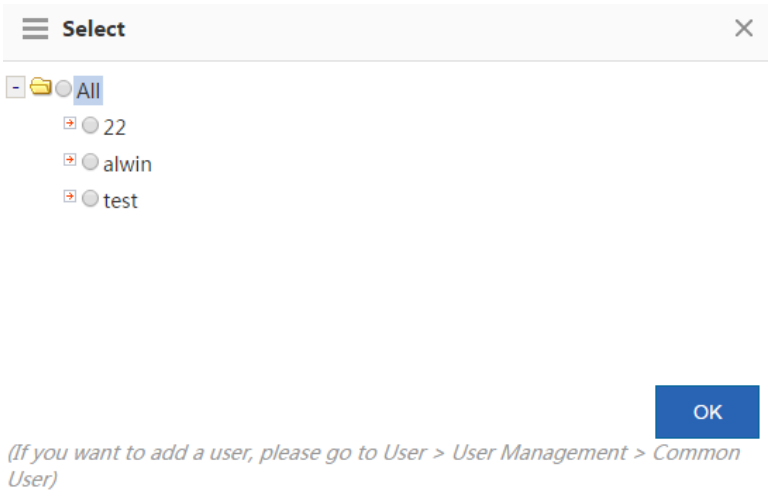



Click  to create a session quantity limit policy. There are two types of session quantity limit policies: user-based and ACL-based.

(1) User-based session quantity limit policy

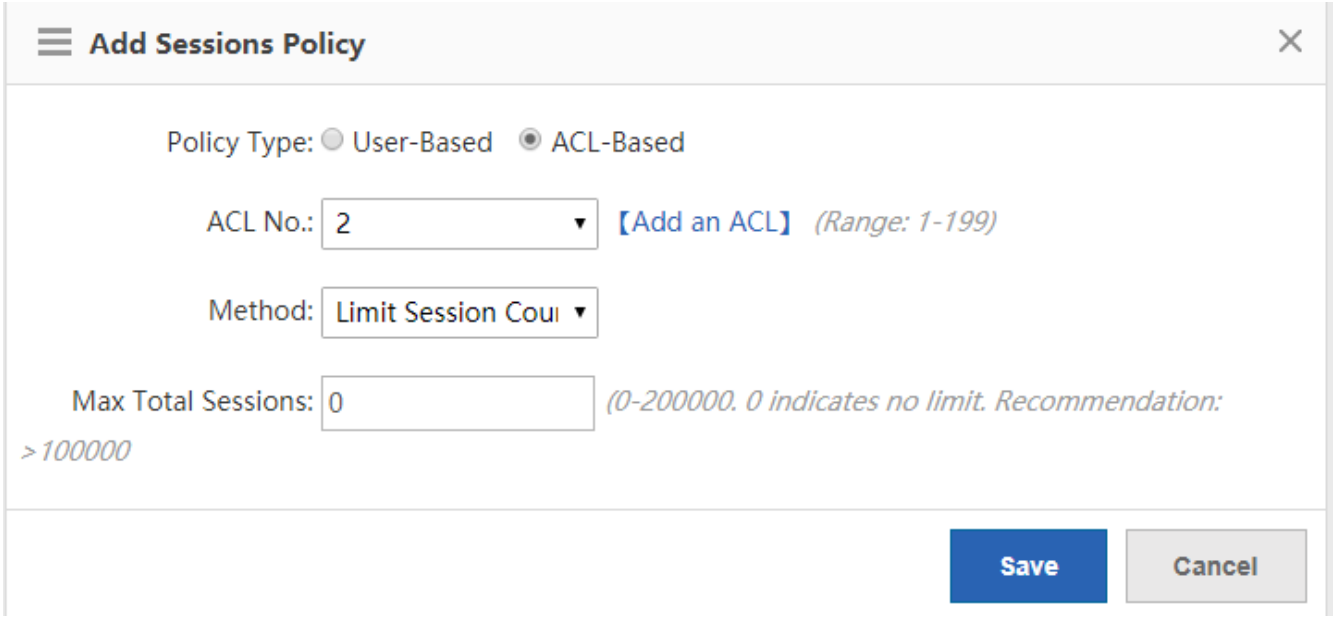


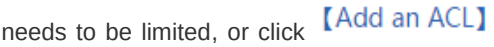

**Select User**: Click Select. In the **Select** dialog box, select users whose session quantity needs to be limited, and click Save.

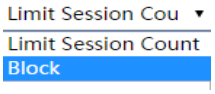



**Method**: Select the required control mode from the Limit Session Count / Block drop-down list. If you select **block** from the drop-down list, selected users are not allowed to access the WAN. If you select **Limit Session Count** from the drop-down list, you need to set the maximum number of sessions and the maximum number of per-IP-based sessions. The session quantity ranges from 1 to 200,000 (the session quantity range varies with the product model).

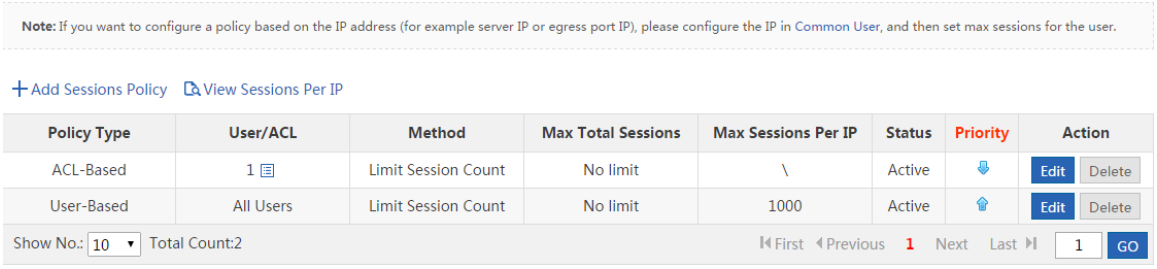
(2) ACL-based session quantity limit policy




**ACL No.**: The  drop-down list next to **ACL No.** lists the configured ACL IDs in the system. You can select the ID of the ACL, in which the session quantity needs to be limited, or click  to create an ACL. For details about how to create an ACL, see the configuration in **Security** > **ACL**.

**Method**: Select the required control mode from the  drop-down list. If you select **block** from the drop-down list, users who match the selected ACL are not allowed to access the WAN. If you select **Limit Session Count** from the drop-down list, you need to set the maximum number of sessions. The session quantity ranges from 1 to 200,000 (the session quantity range varies with the product model).

**3.** List of session quantity limit policies




The table shown in the figure above lists all session quantity limit policies configured in the system.

**Policy Type**: Indicates that a policy is ACL-based or user-based.

**Status**: Indicates whether the policy is effective currently.

A session quantity limit policy configured later has a higher priority than that configured earlier. Click  or  in the **Priority** column to adjust the priority of an existing policy.

Click Edit to modify an existing policy or click Delete to delete a policy.

**4.** View Sessions Per IP

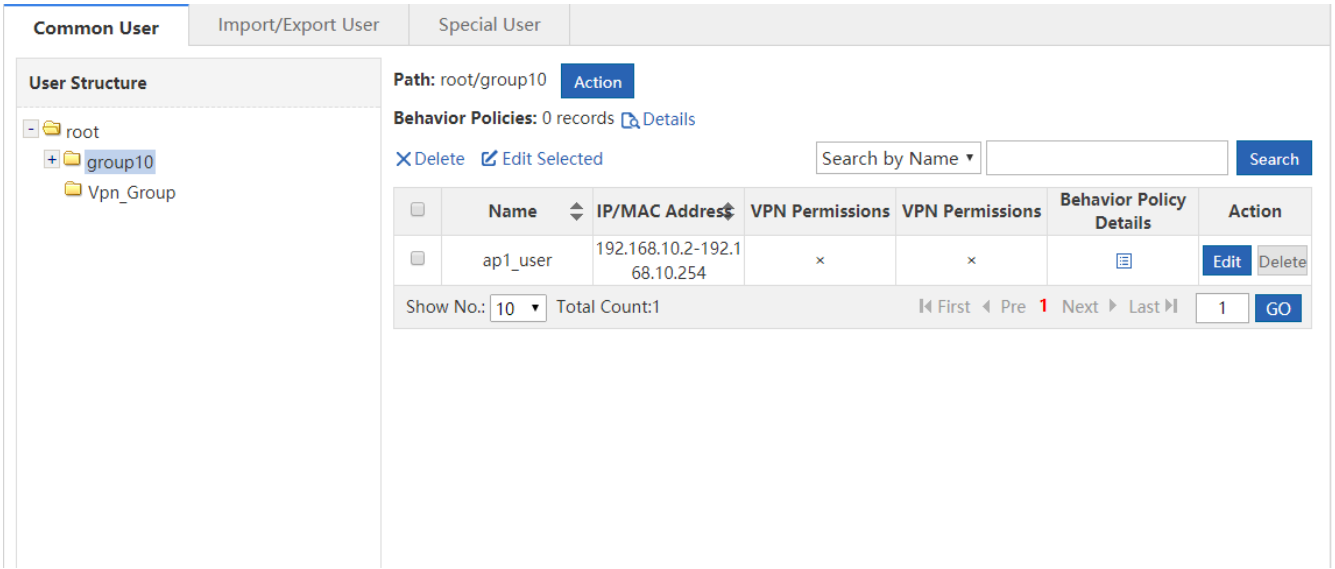
Click View Sessions Per IP to display the flow session quantity of an IP address that requires the per-IP-based flow session quantity limit.


## 1.3.13 User

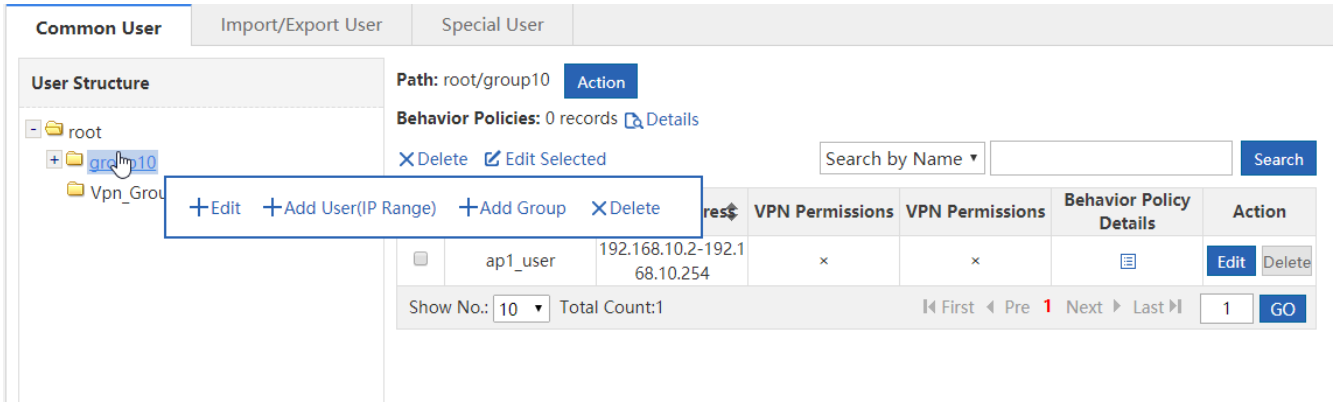
### 1.3.13.1 User Organization

#### 1.3.13.1.1 User Management

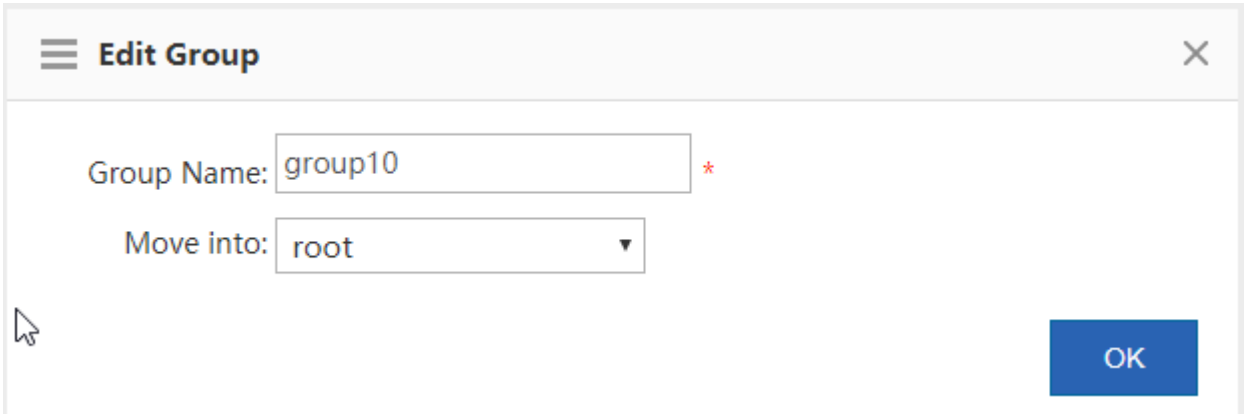
Users on the device may be LAN users, Web authenticated users, or VPN users. A user can log in to the VPN and perform Web authentication. For example, create a user named "John" under the Finance Department, enable the VPN and Web authentication functions for the user, and bind the username with the IP address of the user's PC. Then, the device can perform normal audit and flow control not only when the user accesses the Internet in the company but also when the user logs in via Web or VPN. The VPN here refers to a Point-to-Point Tunneling Protocol (PPTP) VPN, Layer 2 Tunneling Protocol (L2TP) VPN, or Virtual Private Network over Secure Sockets Layer (SSL VPN).



The tree-shaped hierarchy on the left side shows the organization structure of all users in the system. Select a user group. Information about the user group is displayed on the right side. You can edit and delete the information. To modify a user (group), click the user group on the left side. Then, information about the user group is displayed, as shown in the figure below.

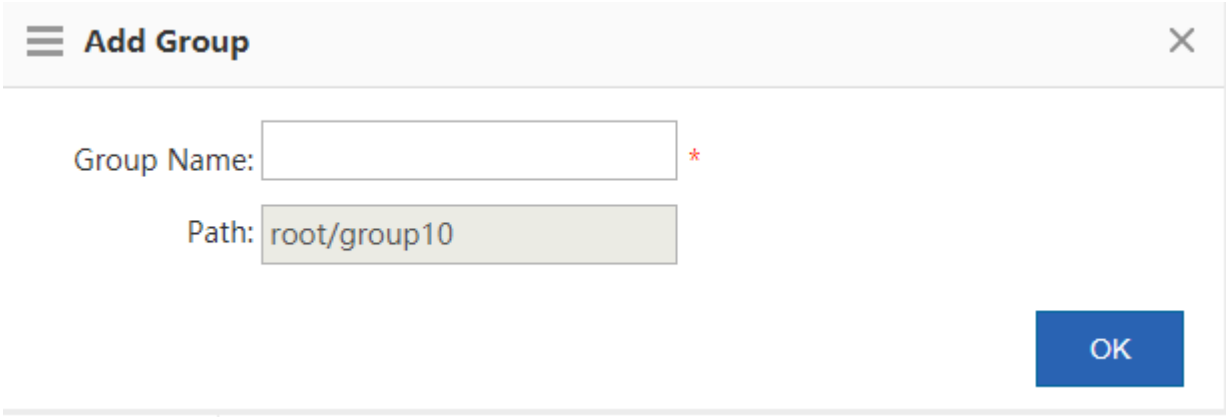



1. Click Edit to edit the selected user group, as shown in the figure below.




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

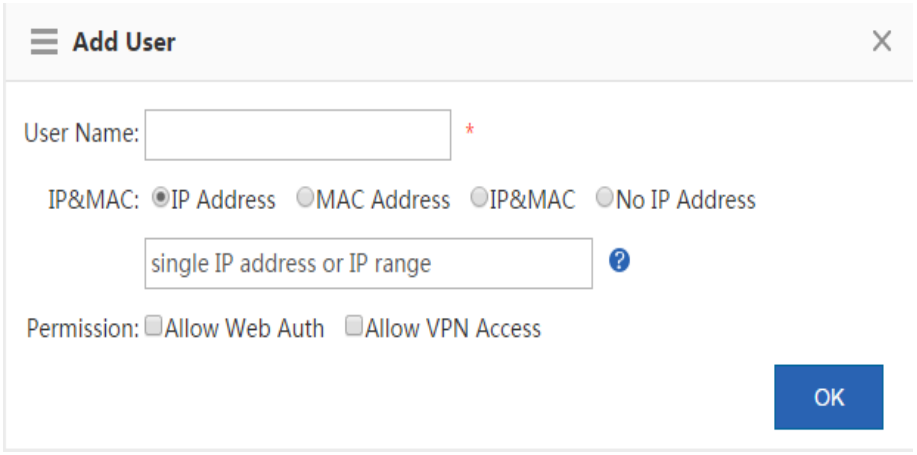
Click Add Group to create a sub user group for the selected user group, as shown in the figure below.




A user group name supports at most 31 characters.

2. Click Delete to delete the selected user group from the user organization structure. All users in the user group will be deleted.

3. Click Add User(IP Range) to create a user under the selected user group.




**User Name**: Indicates the name of a user, which is also the username for VPN login or Web authentication.

**Permission**: Indicates whether the username and password are allowed to be used for Web authentication or VPN login. If yes, the password cannot be null. Otherwise, login will fail.

**Password**: Indicates the password for Web authentication or VPN login.

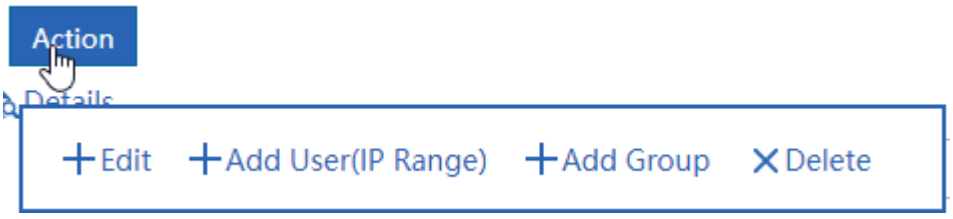
**Change Password**: It is displayed only when **Allow Web Auth** is selected. It indicates whether to allow a user to change the password after the user passes Web authentication.

**Deny Login**: It is displayed only when **Allow Web Auth** is selected. If it is selected, a user cannot access the WAN but can access only LAN resources after passing Web authentication.

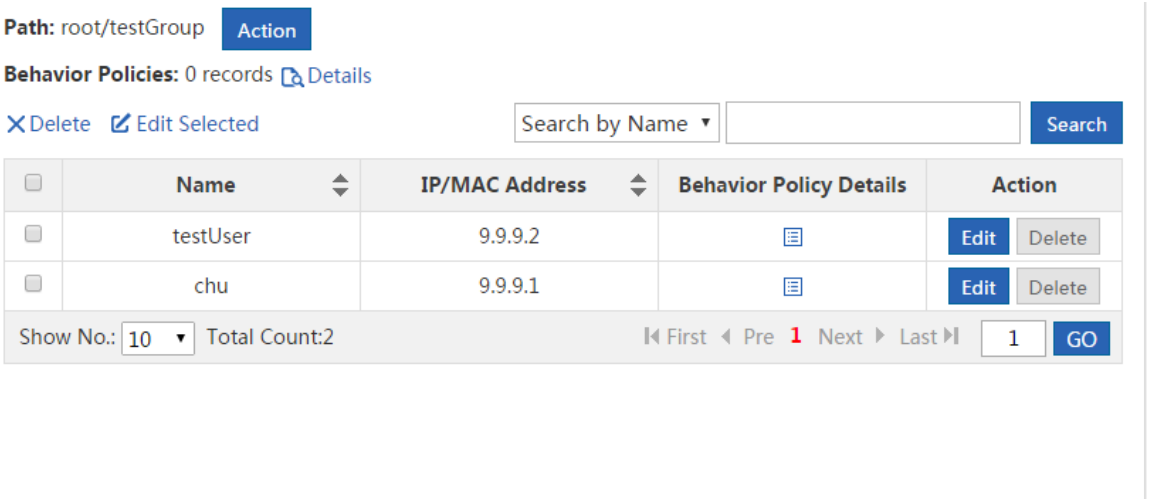
**IP&MAC**: Indicates the IP address or MAC address of the user. You can configure an IP range or configure both an IP address and a MAC address. An IP range needs to be configured in the "start IP address-end IP address" format.

**Bind**: It can be configured only when **Allow Web Auth** is selected. Unidirectional binding and bidirectional binding are supported. Bidirectional binding refers that a user can only use a specified address for real-name authentication and the specified address is used only by the user. Unidirectional binding refers that a user can only use a specified address for real-name authentication but other users can also use this address.

4. You can also click Action to add a group, delete a group, and add a user.

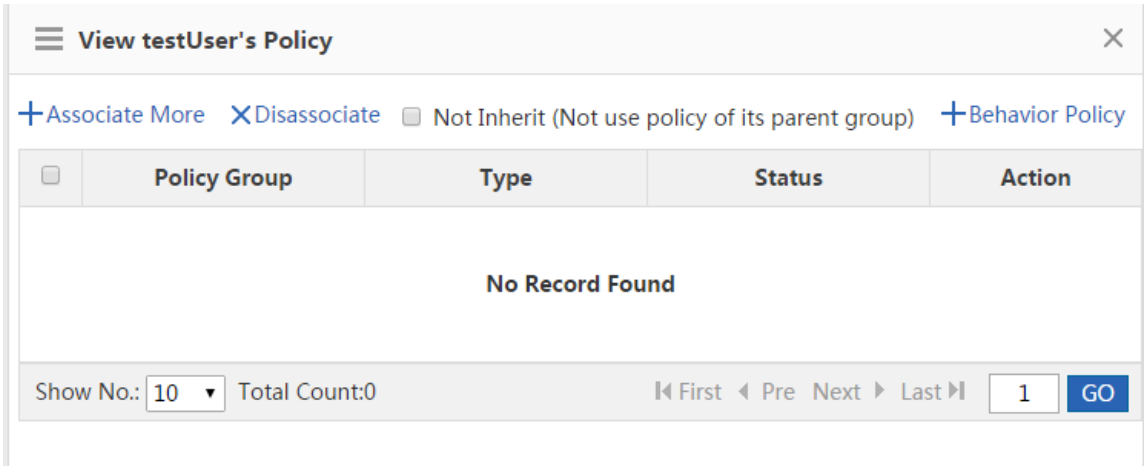



5. User list of a user group



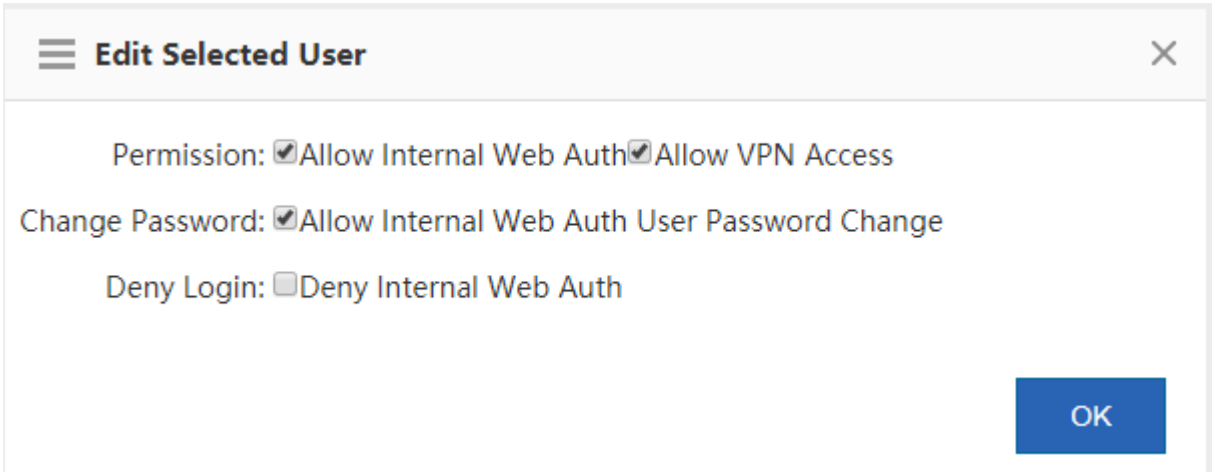

The table shown in the figure above lists all users contained in the user group selected on the left side. You can edit or delete a user.

6. Click . Details about behavior policies associated with the user (group) are displayed, as shown in the figure below.

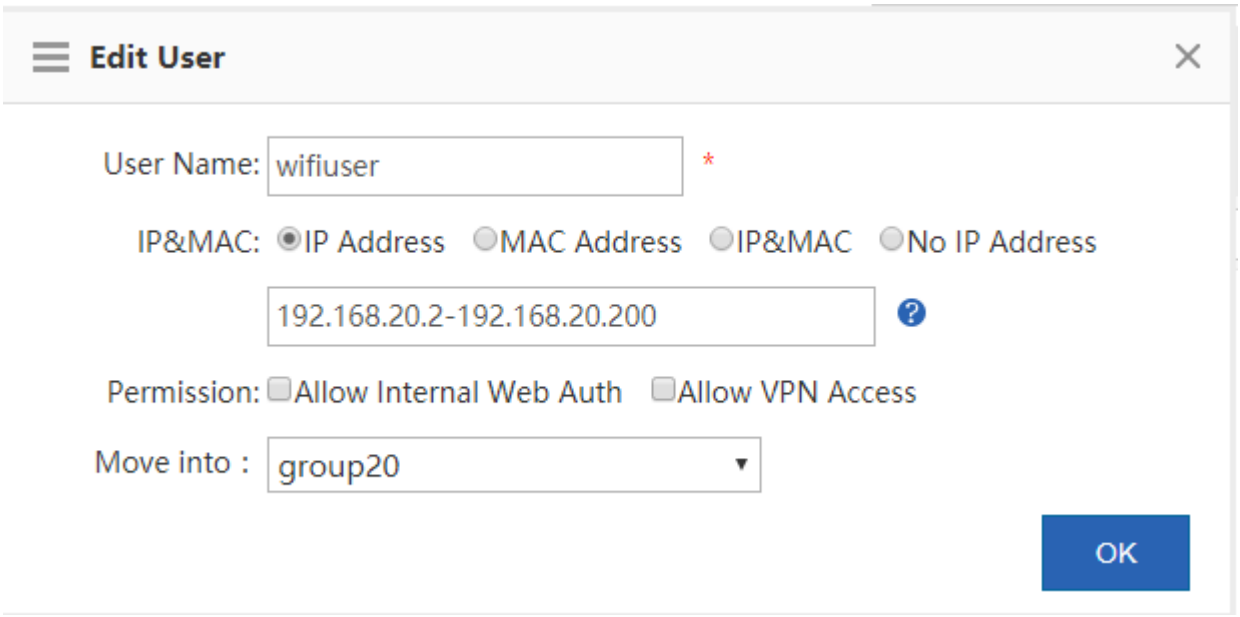



Click Associate More . The system redirects to the **Advanced** page in **Flow** > **Behavior Policy**.

7. Select required users and click Delete Edit Selected to delete or edit the users in batches, as shown in the figure below.

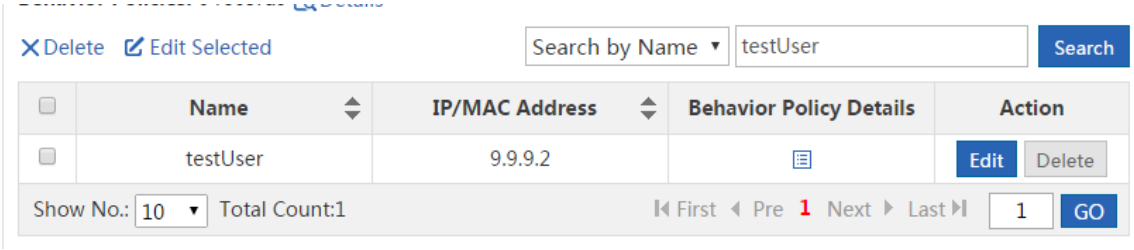



8. Click Edit to edit user parameters. For description of each parameter, see the user creation section above.



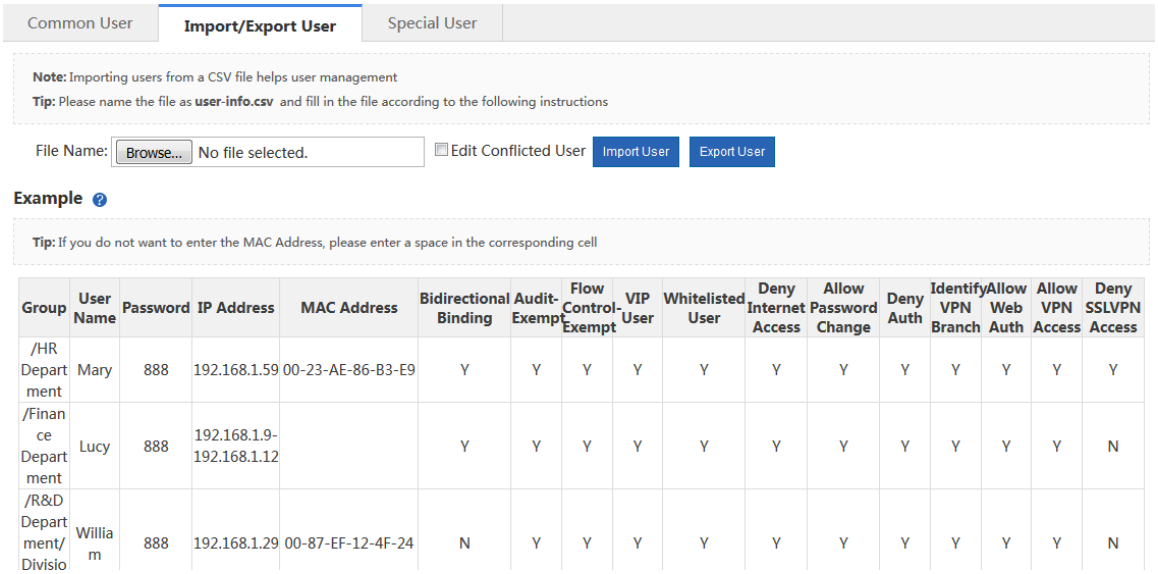

9. Enter a username or IP address in 

to search for the required user. The search result is displayed in the table below.




### 1.3.13.1.2 Import/Export User

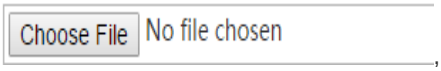
You can import and export user information. The **Import/Export User** configuration page is shown in the figure below.

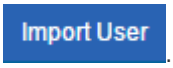



| Group | User Name | Password | IP Address | MAC Address | Bidirectional Binding | Audit-Exempt | Flow Control-Exempt | VIP User | Whitelisted User | Deny Internet Access | Allow Password Change | Deny Auth | Identify VPN Branch | Allow Web Auth | Allow VPN Access | Deny SSLVPN Access |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| /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/Divisio | William | 888 | 192.168.1.29 | 00-87-EF-12-4F-24 | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N |

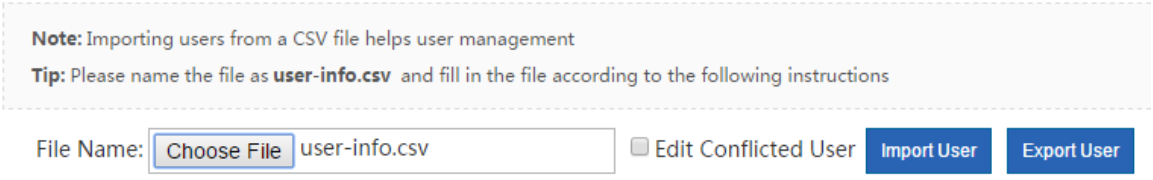
**Import User**: Administrators can import user information by a file. Locally create a table named **user-info.csv** and enter user information in the following format in the table.

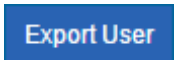
| Group | User Name | Password | IPAddress | MACAddress | Bidirectional Binding | Audit-Exempt | Flow Control-Exempt | VIP User | Whitelisted User | Deny Internet Access | Allow Password Change | Deny Auth | Identify VPN Branch | Allow Web Auth | Allow VPN Access | Deny SSLVPN Access |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| /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 |

Click : 

, locate the **user-info.csv** file, and click 

.

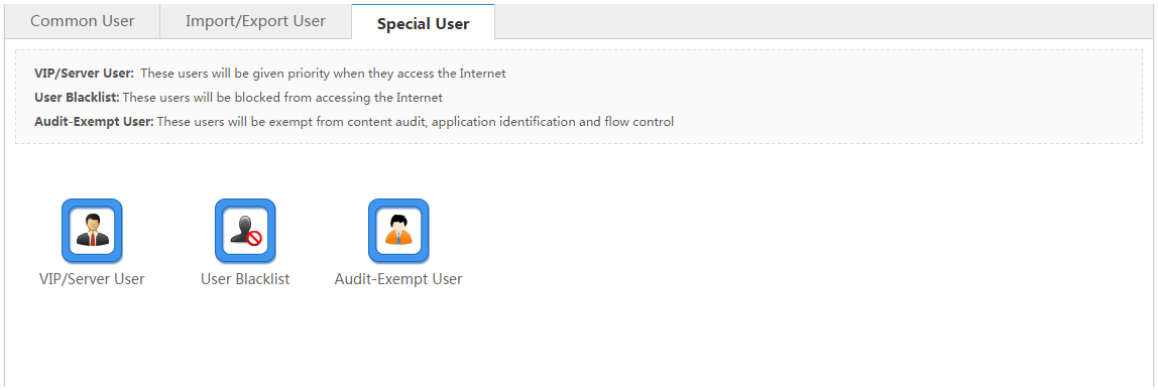



**Export User**: Click 

to download the **user-info.csv** file.

#### 1.3.13.1.3 Special User

Special users include VIP/server users, blacklisted users, and audit-exempt users. The **Special User** configuration page is shown in the figure below.




**VIP/Server User**: Refers to key users or LAN server users with a higher priority in the guaranteed Internet access speed.

Click 

. The VIP/server user configuration window is displayed, and you can add or delete a VIP/server user. For detailed operations, see "VIP User" in 1.3.5.2.1 "Smart Flow Control."

**User Blacklist**: If want to deny all Internet access behaviors of a user, you can add the user to the blacklist. Click 

. The user blacklist configuration window is displayed, and you can add or delete a blacklisted user. For detailed operations, see "User Blacklist" in 1.3.5.4.1 "Basic Settings."

**Audit-Exempt User**: Refers to users who are exempt from content audit, traffic audit, and flow control. For example, the Internet access behaviors of a boss generally do not need to be audited, and therefore, the boss can be set as an audit-exempt user. Click 

. The audit-exempt user configuration window is displayed, and you can add or delete an audit-exempt user. For detailed operations, see "Audit-exempt User" in 1.3.5.4.1 "Basic Settings."

### 1.3.13.2 Authentication/Advertisement Push

Authentication/advertisement push includes Web authentication and application authentication.

#### 1.3.13.2.1 Web Authentication

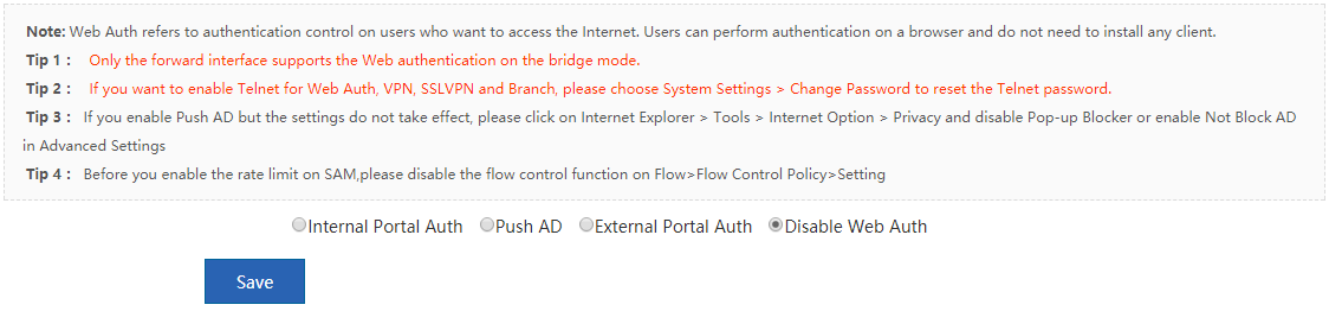
Web authentication refers to user authentication.

User authentication is an authentication method for controlling user access permissions over network resources. The authentication process can be implemented using a common browser. When a WAN user needs to access the Internet, the

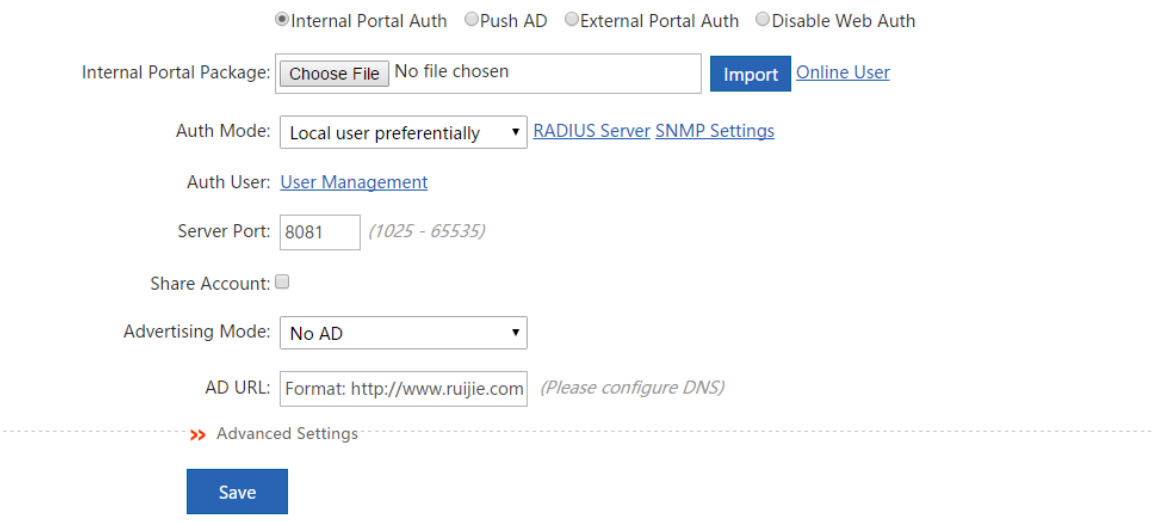
authentication device forces the user to log in to a specific site and the user can access services at the site free of charge. When a user needs to use other information on the Internet, authentication must be performed on the Web authentication server. The user can use Internet resources only after passing the authentication. If a user attempts to access other WANs over the Hypertext Transfer Protocol (HTTP), the user is forced to access the Web authentication portal. Web authentication provides users with convenient management functions, and allows users to launch advertisements, social services, and personalized services on the Web portal.

The device supports internal authentication and external authentication. If internal authentication is selected, no external server is required and the device can provide the service function. If external authentication is selected, the ePortal server and the Remote Authentication Dial In User Service (RADIUS) server need to be set up.

Click ◉Disable Web Auth to disable user authentication.

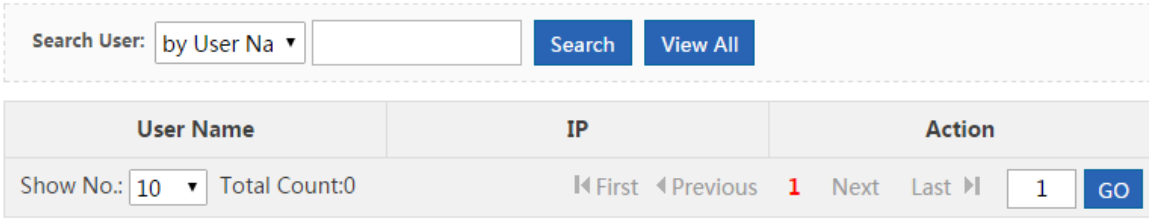



- **Internal Portal Auth**

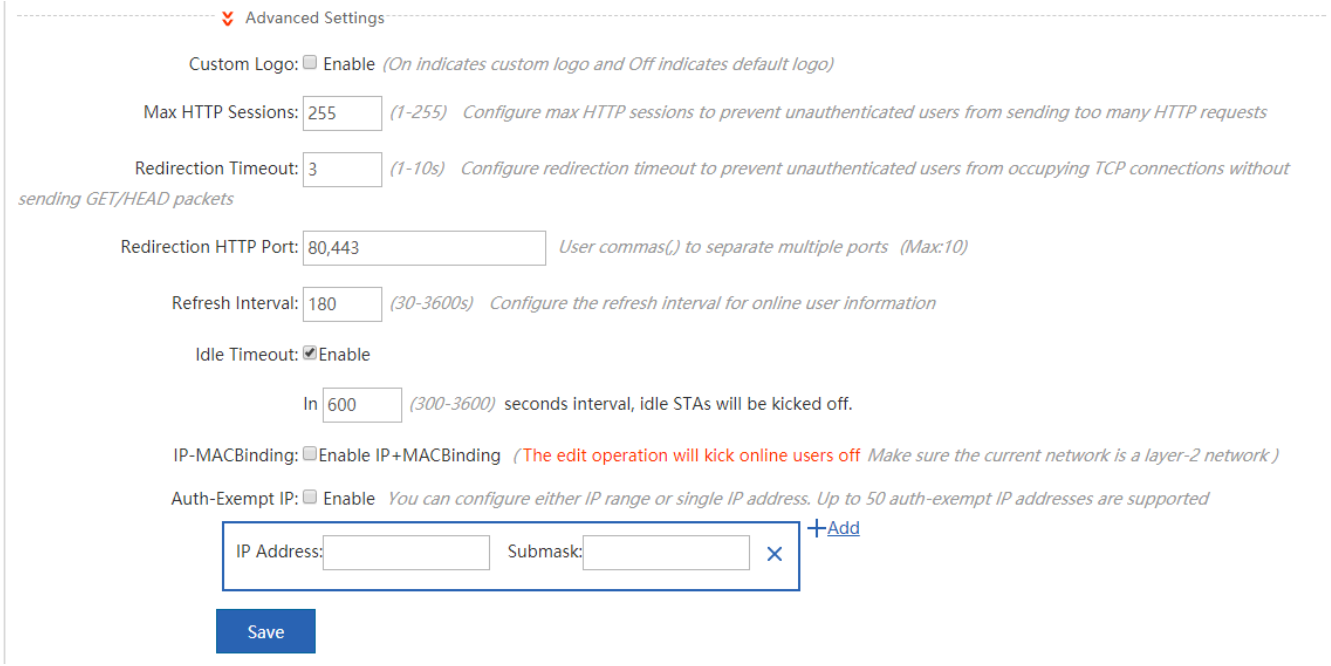



1. **Internal Portal Package:** You can import authenticated user information in the specified format.

Click Online User . A window shown in the figure below is displayed, and you can view online authenticated users. You can select a user and force the user to go offline, or query online users.

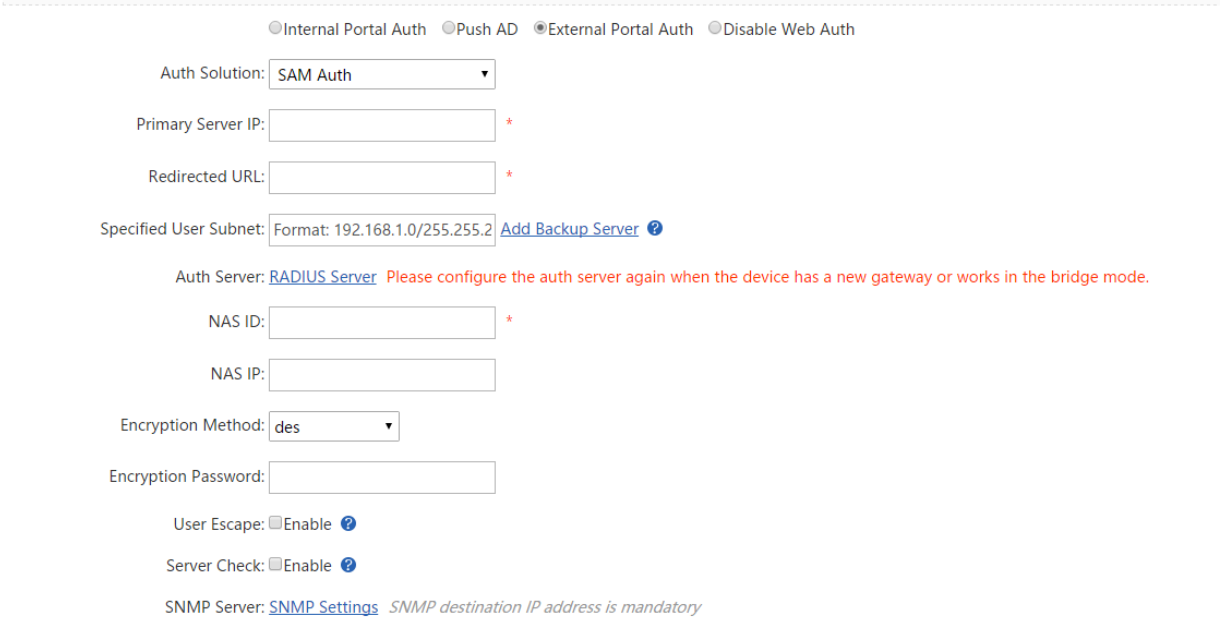



2. **Auth Mode**: When **Internal Portal Auth** is enabled, local user information, user information obtained from the RADIUS server, or both can be used for user validity authentication. **Server user preferentially** is recommended but the RADIUS server needs to be set up first.
3. **Auth User**: Authentication user.
4. **Server Port**: Indicates the port of the internal portal server. The value ranges from **1025** to **65535** and the default value is **8081**. You can change the server port.
5. **Share Account**: Generally, an account can only be used by one IP address at a time. You can select Share Account: to share one account with multiple IP addresses. The account that logs in later is effective after **Share Account** is disabled.
6. **Advertising Mode**: Indicates the display mode of advertisements. You can select advertisement after authentication or select no advertisement.
7. **AD URL**: Indicates the URL of the advertisement page.
8. **Advanced Settings**: Click >> Advanced Settings. You can configure more information, as shown in the figure below.

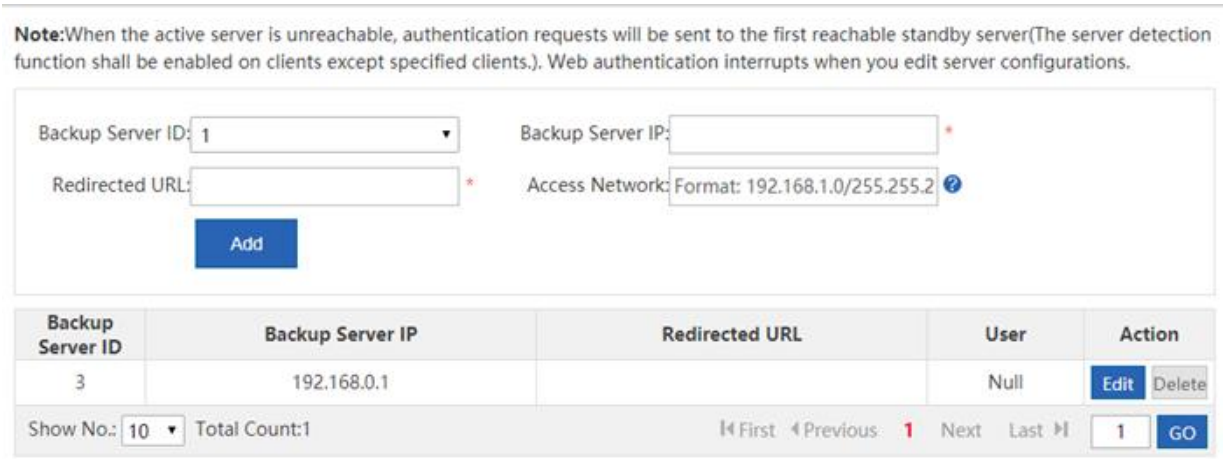


- **External Portal Auth**

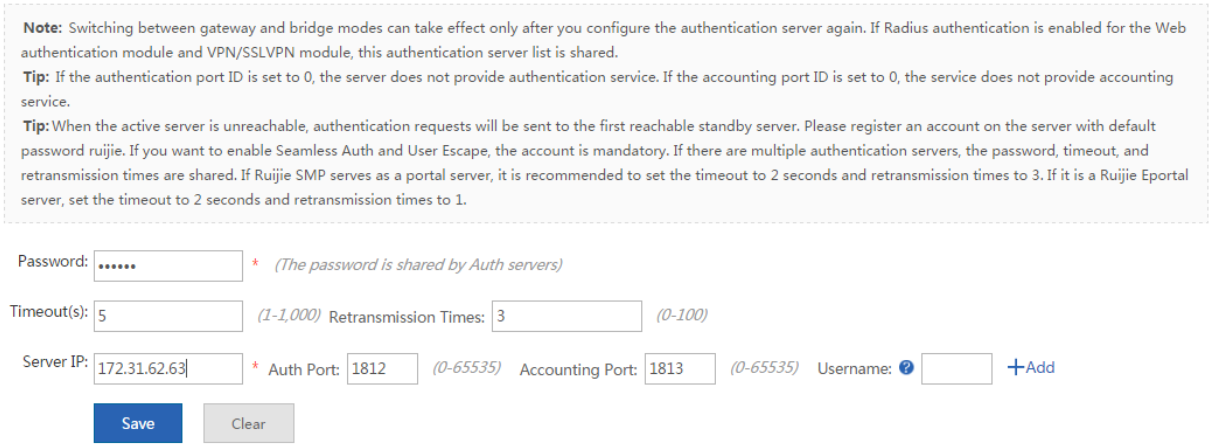
External authentication includes SMP authentication and SAM authentication. The figures below show the configuration pages of the two types of authentication.



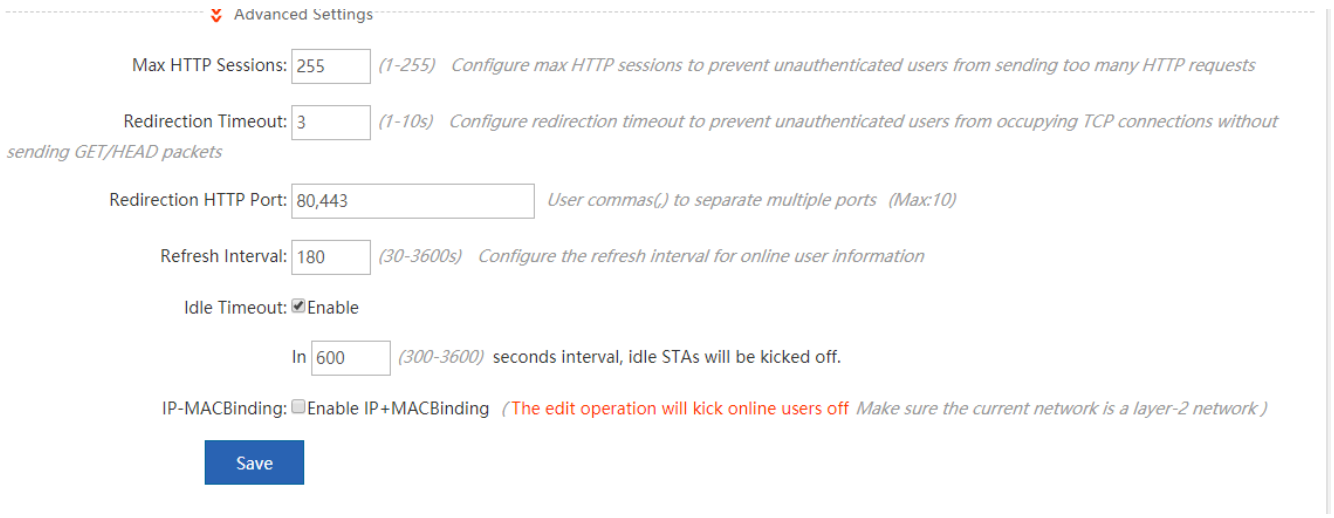

1. **Auth Solution:** Indicates the authentication solution including SAM and SMP authentications.
2. **Primary Server IP**: Enter the IP address of the ePortal server. In general, the authentication page is provided by the ePortal server.
3. **Redirected URL**: Enter the URL of the authentication page. When an unauthenticated user accesses network resources, the system automatically redirects it to the authentication page. The page will not be displayed after a user passes authentication.
4. **Specified User Subnet**: Indicates users in a network segment permitted by the ePortal server for authentication. Users who are not in the network segment do not need to pass authentication.
5. **Backup Server**: When the communication function of the primary server fails, it automatically switches to the backup server. The Web authentication service is interrupted when the server configuration is edited. A maximum of four backup portal servers can be added on the Web management system, as shown in the figure below.



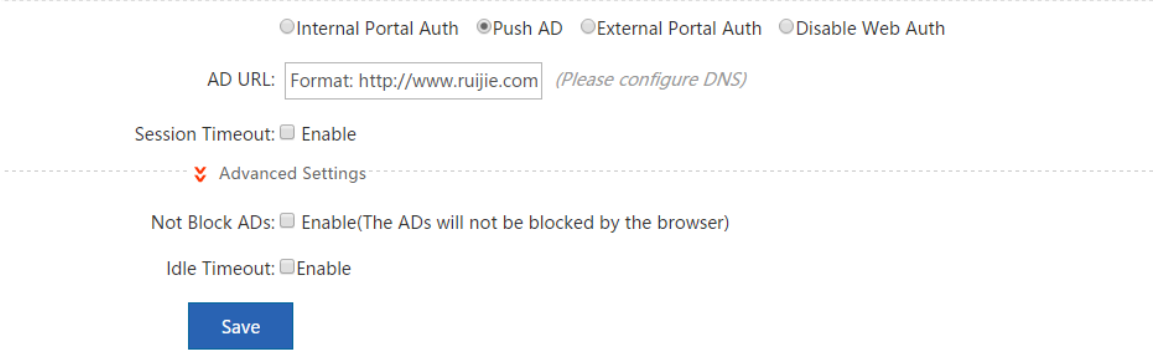

6. **Auth Server:** Indicates the Radius Server, as shown in the figure below.



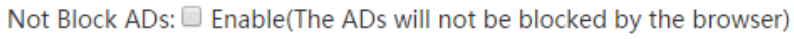

7. **NAS ID:** ID of the Network Access Server.
8. **NAS IP:** IP of the Network Access Server.
9. **Encryption Method:** Portal Authentication parameters encryption method. Supports **des**, **des_ecb**, **des_ecb3** and **md5** encryption.
10. **User Escape**: If the server is unavailable, users can automatically go online when no authentication page is displayed. It must be used in conjunction with the server detection function.
11. **Server Check:** if the portal escape mode is enabled, and more than one server is configured, server check is needed. If it is enabled, device will check the server whether available periodically.
12. **SNMP Server:** SNMP Server configuration.
13. Advanced Settings: Click » Advanced Settings . More information is displayed, as shown in the figure below. For details, see the section of advanced settings for user authentication.



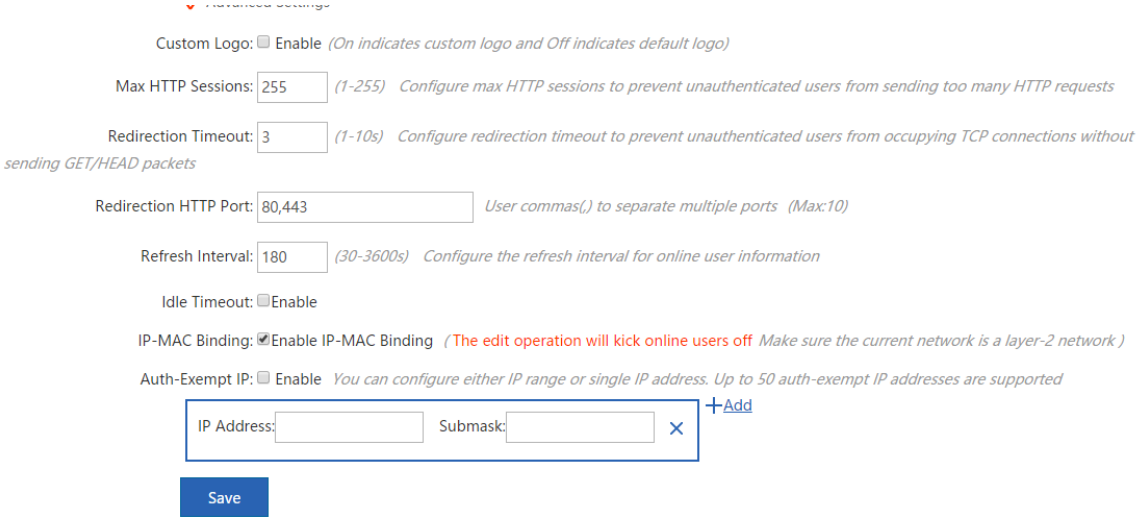

- **Push AD**




After the advertisement push service is saved, the advertisement URL page is displayed when a target user accesses the Internet for the first time.




- **Advanced Settings for User Authentication**




1. **Max HTTP Sessions**: Indicates the maximum number of HTTP sessions of each unauthenticated user. When an unauthenticated user accesses network resources, the user PC sends an HTTP session connection request. The device intercepts the HTTP packet, redirects the page and requests the user to complete Web authentication. To prevent the same unauthenticated user from initiating excessive HTTP connection requests and save device resources, you need to limit the maximum number of HTTP sessions for unauthenticated users. It is not recommended to set the maximum number of HTTP sessions to 1 for unauthenticated users. By default, the maximum number of HTTP sessions of unauthenticated users is 255.

2. **Redirection Timeout**: Indicates the timeout time for maintaining a redirection connection. When an unauthenticated user accesses network resources via HTTP, the user's TCP connection request will be intercepted and a TCP connection will be established between the user and the authentication device. After the TCP connection is established, the authentication device needs to wait for the user to send the HTTP GET/HEAD packet, and then replies to the redirection packet and disconnect the connection. The parameter aims at preventing users from not sending GET/HEAD packets and occupying TCP connections for a long time. By default, the timeout time for maintaining a redirection connection is 3 seconds.

3. **Redirection HTTP Port**: A maximum of 10 different destination port IDs can be configured. When a user accesses network resources (for example, the user accesses the Internet from the browser), the user PC sends an HTTP packet. The authentication device intercepts the HTTP packet from the user to determine whether the user is accessing network resources. If yes, the authentication device prevents the user from accessing network resources and displays the authentication page to the user. By default, the authentication device intercepts HTTP packets with the port ID of 80.

4. **Refresh Interval**: Indicates the update interval of online user information. The authentication device maintains online user information periodically, including online duration, to monitor the network resource usage of the online users. For example, if the online duration of a user is greater than or equal to the time limit, the user is stopped from using the network. By default, the authentication device updates online user information every 60 seconds.

5. **Kick Inactive Users Off**: Indicates the go-offline detection mode of users. There are two modes of detecting whether a user is offline: 1. A user can click **Offline** on the authentication page. 2. In user traffic-based detection mode, it is considered that a user is offline if the traffic of the user does not increase within 15 minutes. The two modes are enabled by default. False detection risks may occur.

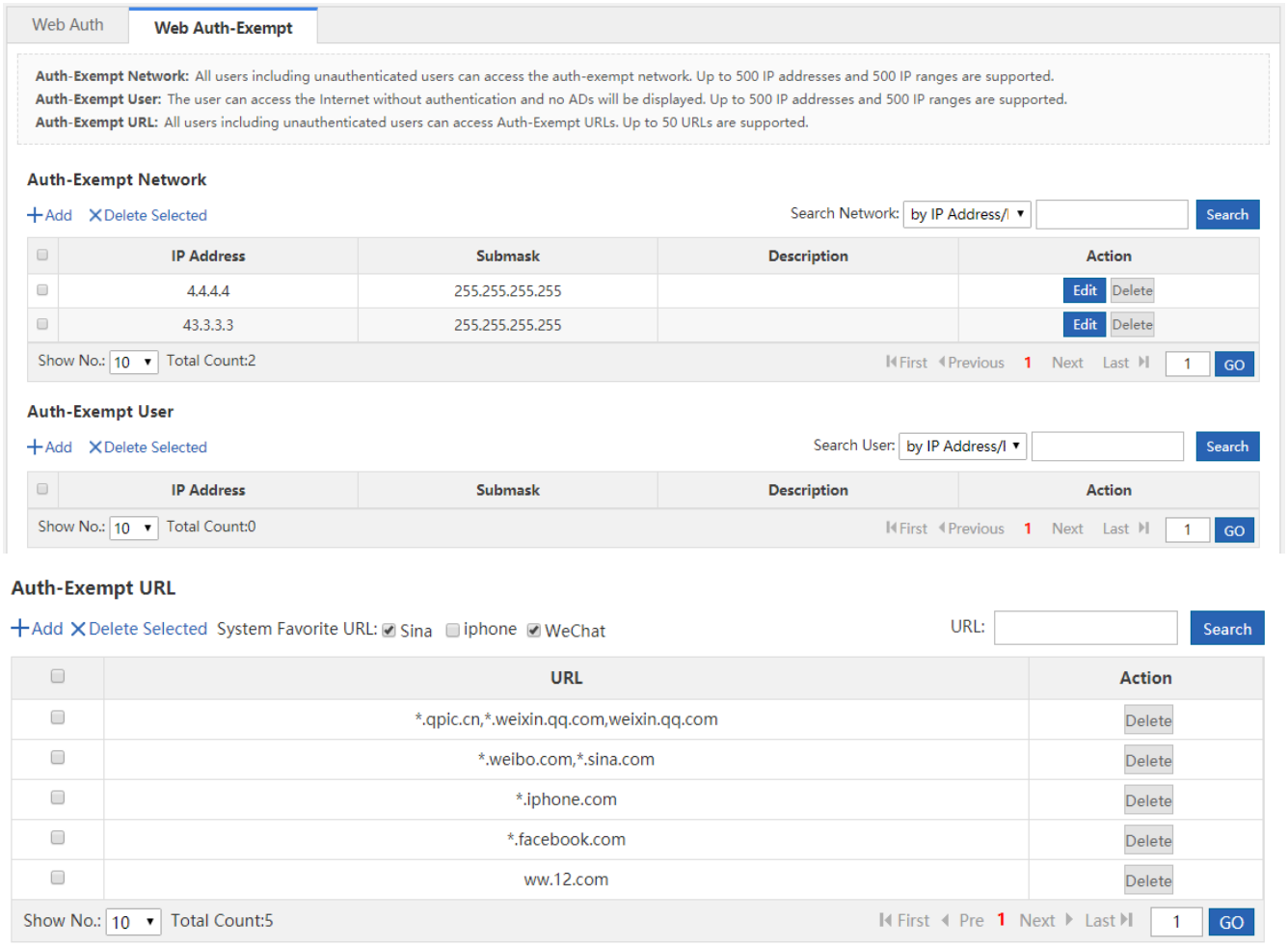
6. **IP-MAC Binding**: Indicates the user IP-MAC binding mode. You can select IP-based binding or MAC plus IP-based binding. In a Layer-2 network, you can select the username plus MAC/IP binding. In a Layer-3 network, you can only select the username plus IP binding. Otherwise, the network is disconnected after binding.

### 1.3.13.2.2 Web Authentication Exemption

**Auth-Exempt Network**: Enter the IP address of the network resource server. All users including unauthenticated users can access this IP address. A maximum of 500 entries are supported.

**Auth-Exempt User**: An authentication-exempt user can directly access the Internet without authentication and no advertisement will be pushed to the user. A maximum of 500 entries can be configured.

**Auth-Exempt URL**: All users including unauthenticated users can access Auth-Exempt URLs. Up to 50 URLs are supported.

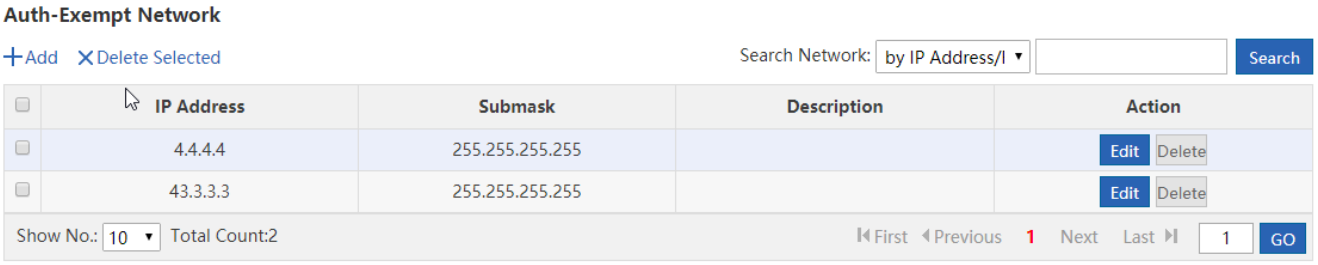






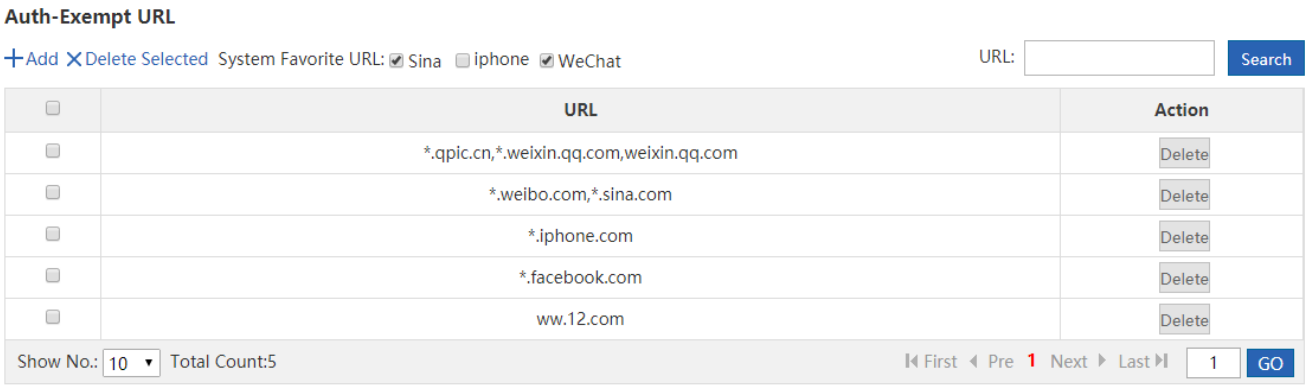
**Auth-Exempt Network**: A maximum of 500 authentication-exempt network resources are supported. You can use this option to configure authentication-exempt network resources which unauthenticated users can also access. After it is configured, if a website is an authentication-exempt network resource, all users (including unauthenticated users) can access this website. By default, no authentication-exempt network resources are configured and unauthenticated users cannot access network

resources. (Note: You can configure a single IP address or an IP range (in the format of IP address + mask, for example, 192.168.1.0 255.255.255.0). The IP range is also an authentication-exempt resource.)




**Auth-Exempt User**: A maximum of 500 authentication-exempt users can be configured. If a user is within the range of authentication-exempt user IP addresses, the user can access all accessible network resources without passing Web authentication. By default, no authentication-exempt user is configured and all users can access network resources only after passing Web authentication. (Note: You can configure a single IP address or an IP range (in the format of IP address + mask, for example, 192.168.1.0 255.255.255.0). The IP range is also an authentication-exempt resource.)


**Auth-Exempt URL**: A maximum of 50 authentication-exempt URL can be configured. All the users including unauthenticated users can access Auth-Exempt URLs.

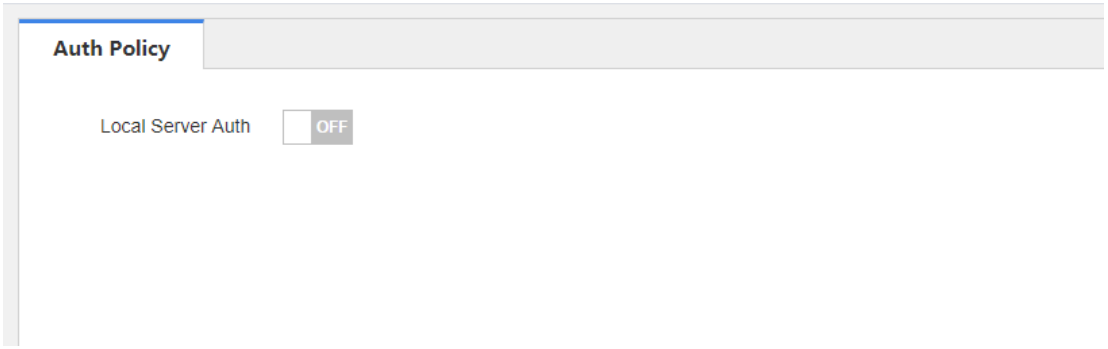



## 1.3.13.3 Local Auth

## 1.3.13.3.1 Auth Policy

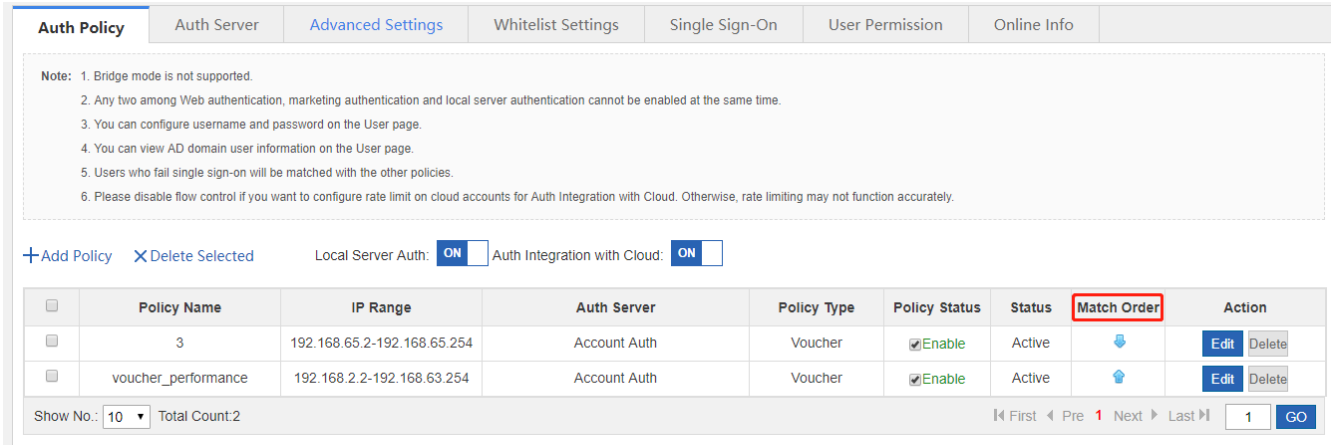
1. Enabling local server authentication

Choose **User** > **Local Auth** > **Auth Policy** and check local server authentication status. If local server authentication is disabled, only the **Auth Policy** sub-menu is available.



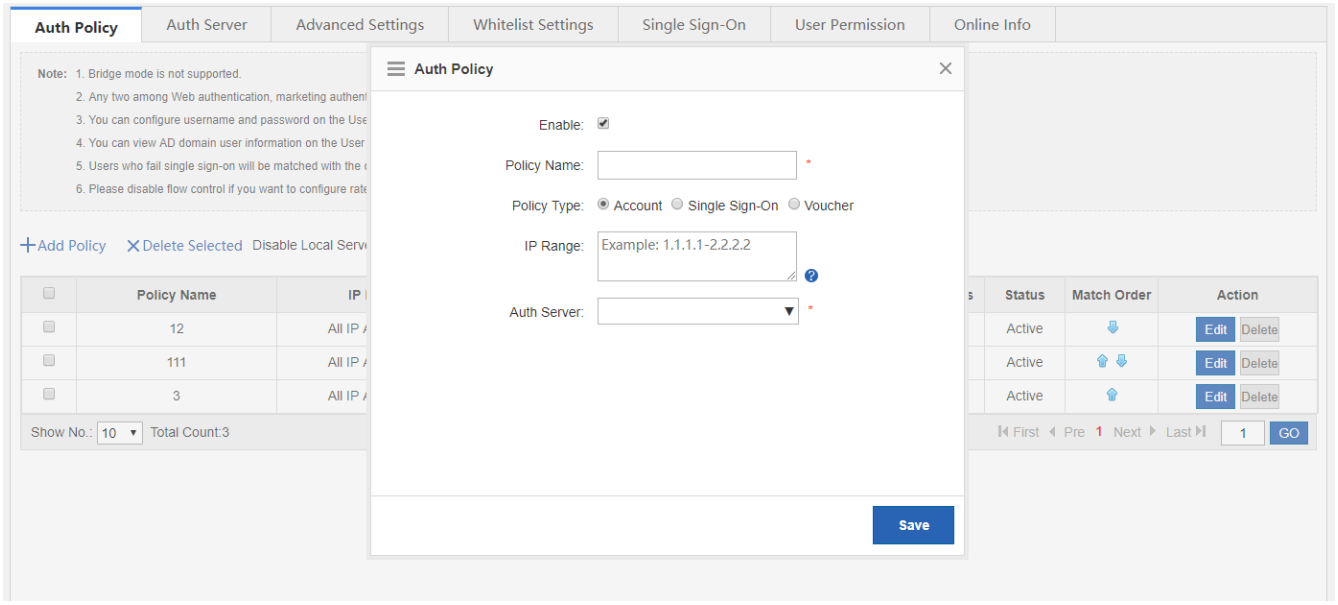

2. Changing policy priority

Click or to swap the match order of policies.



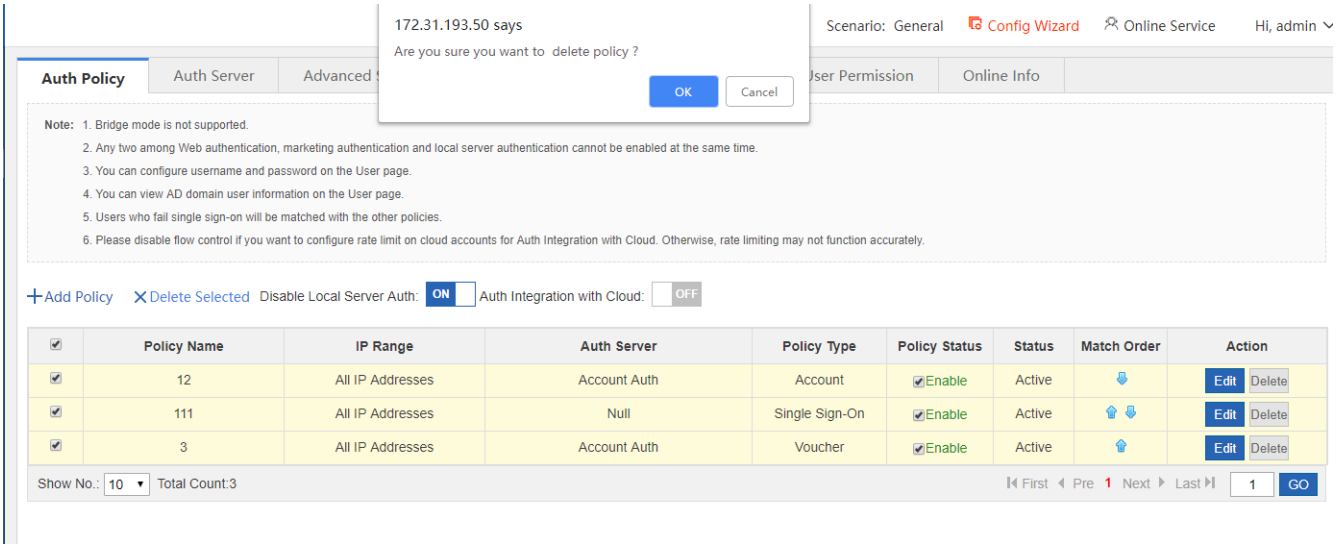

3. Adding/Editing an authentication policy

You can add or edit a policy only after checking the **Enable** box.



4. Deleting an authentication policy

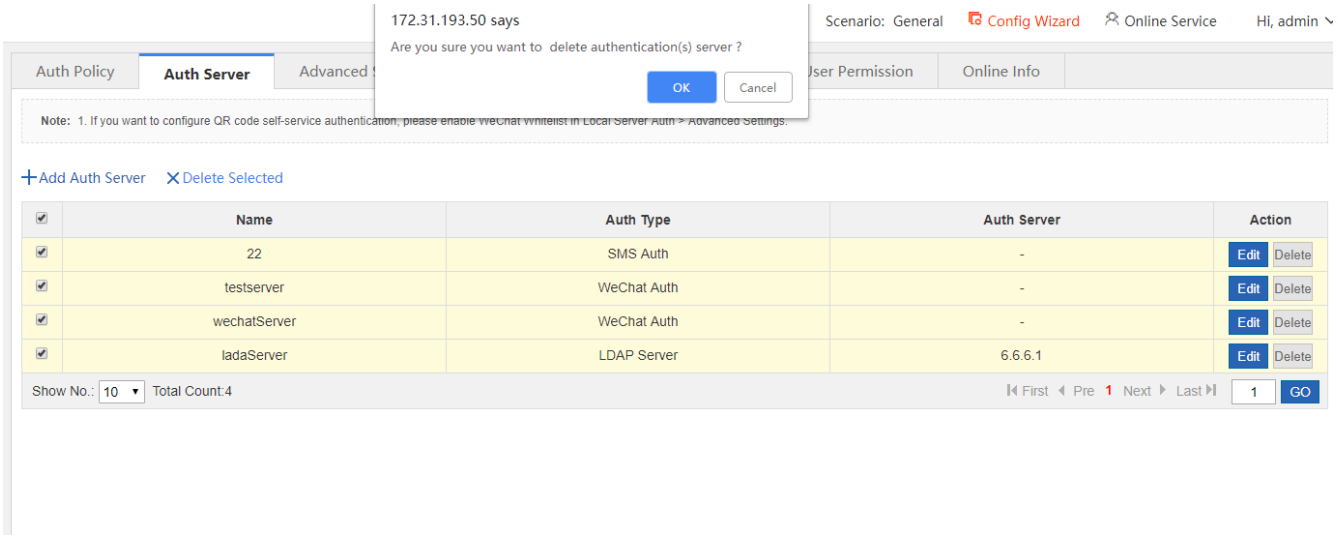
Click Delete to delete a policy or click Delete Selected to delete selected policies.




## 1.3.13.3.2 Auth Server

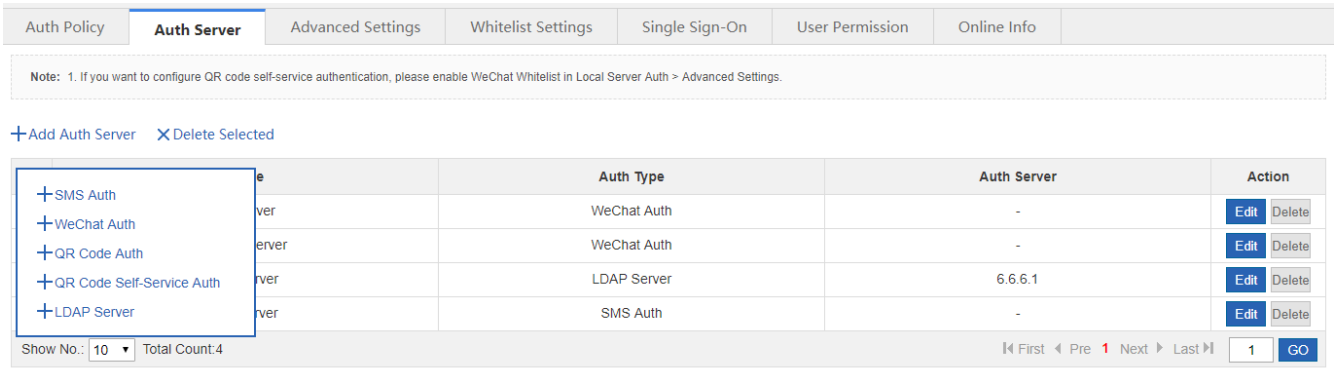
1. Deleting an authentication server

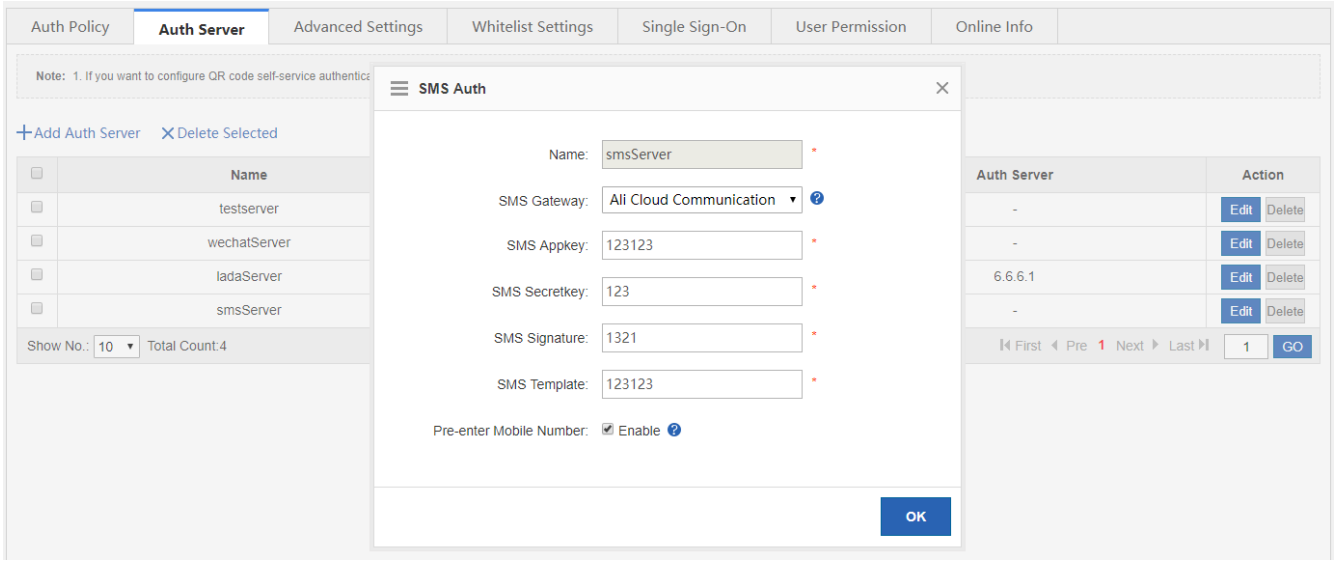
Click Delete to delete a server or click Delete Selected to delete selected servers.




2. Adding/Editing SMS authentication

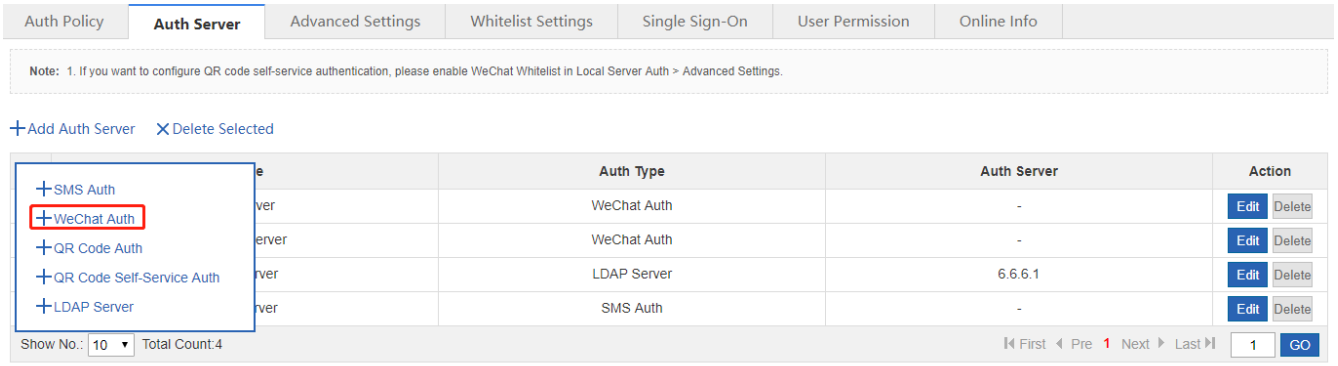
Click Add Auth Server to expand the authentication menu. You can select SMS authentication here.

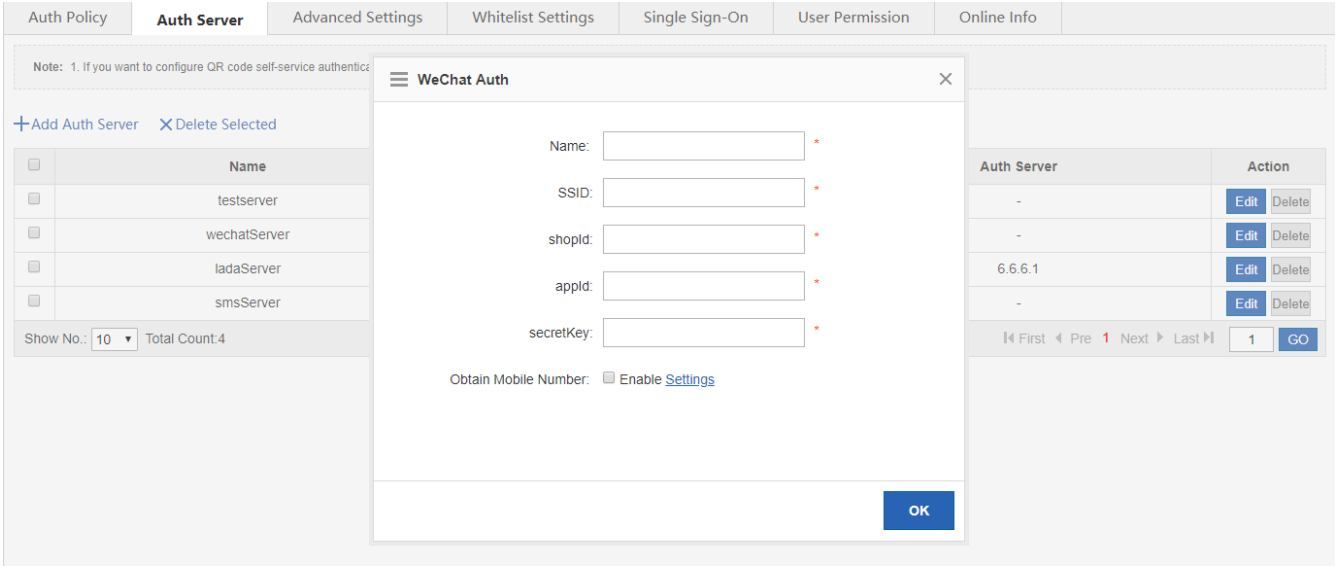



3. Adding/Editing WeChat authentication

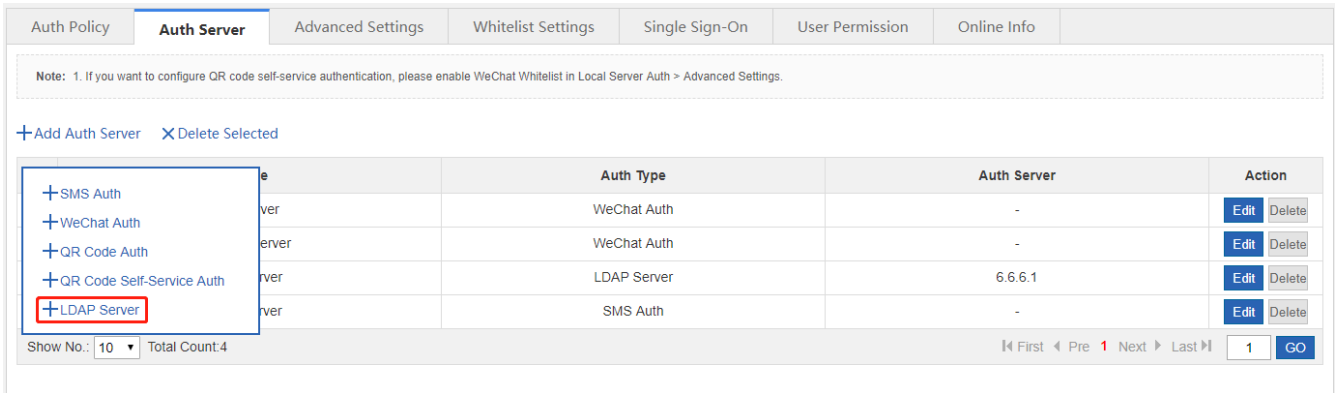
Click + Add Auth Server to expand the authentication menu. You can select WeChat authentication here.

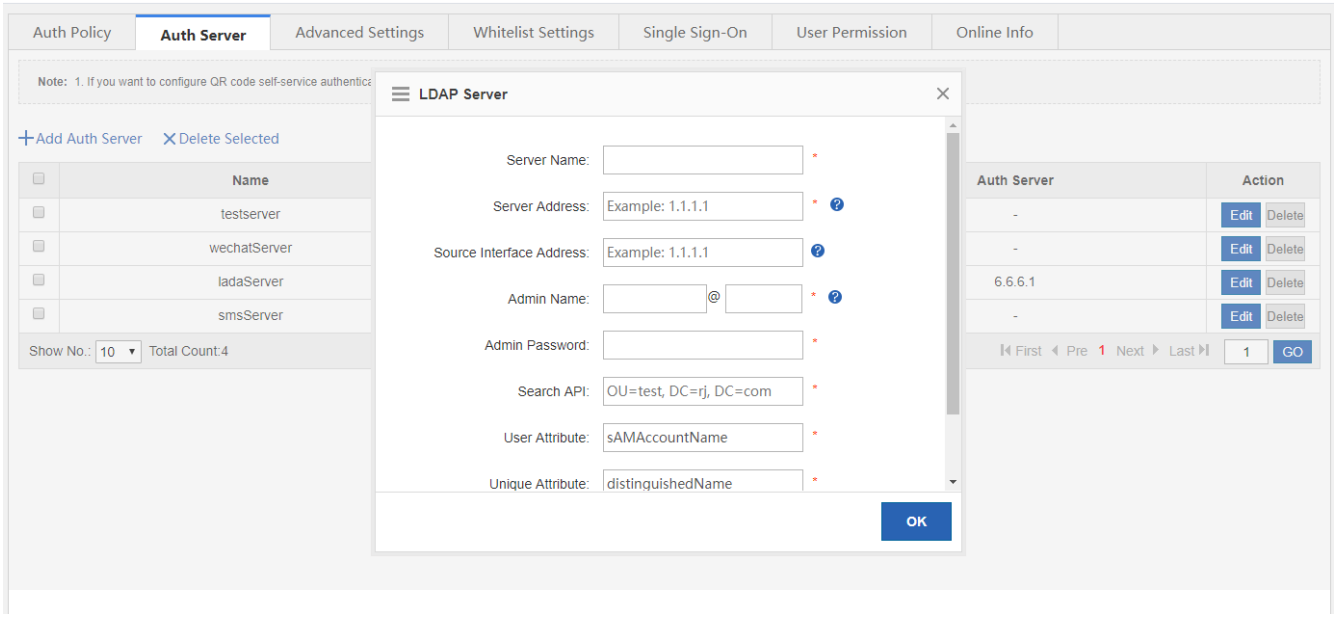



4. Adding/Editing LDAP server authentication

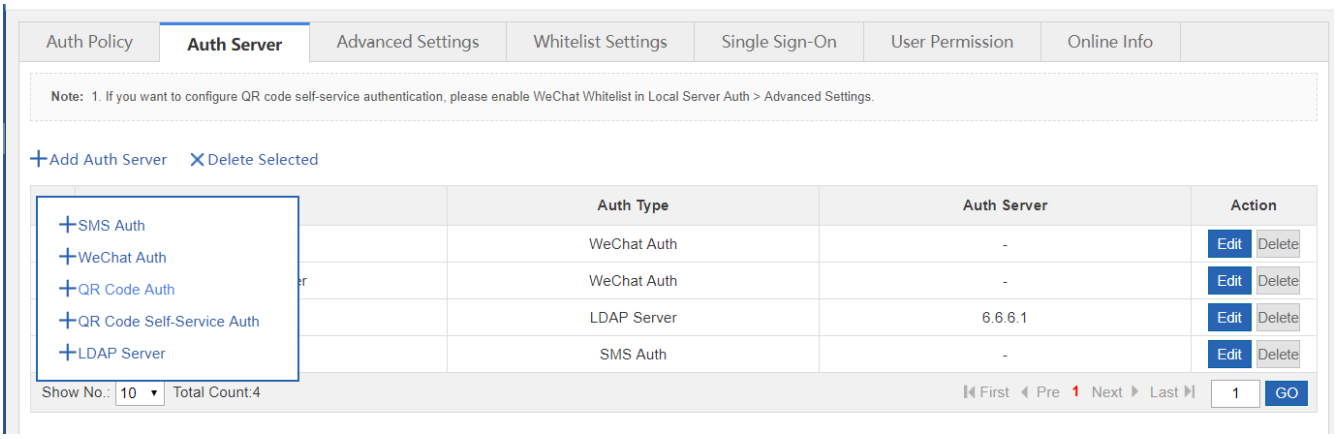
Click Add Auth Server to expand the authentication menu. You can select LDAP server here.

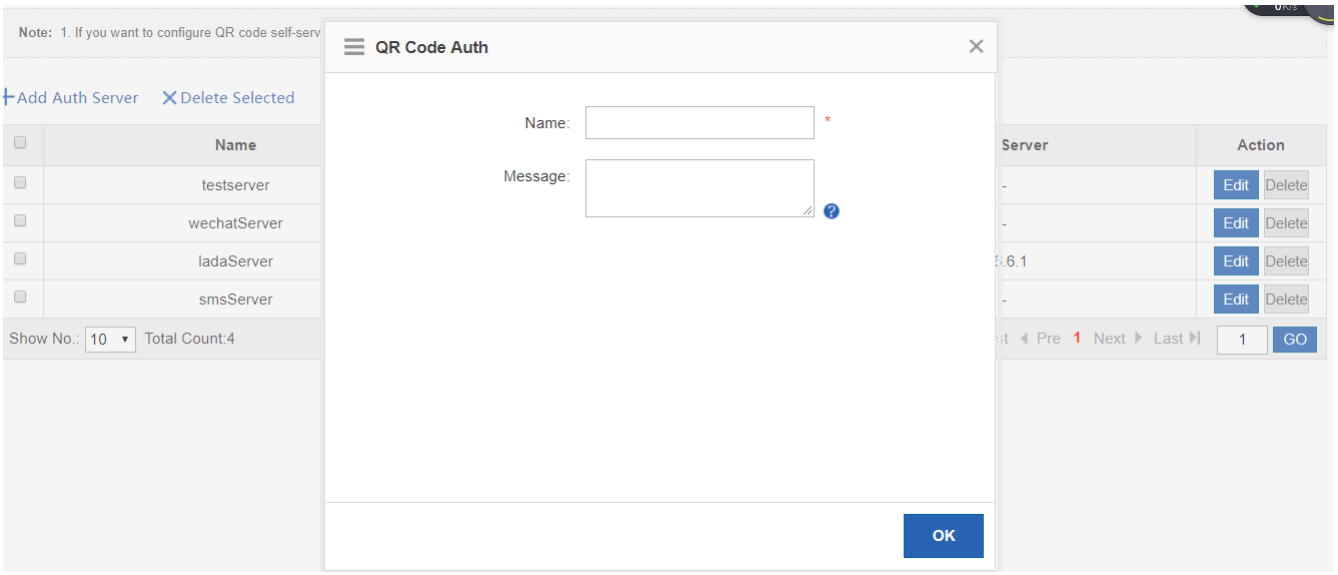





5. Adding/Editing QR code authentication

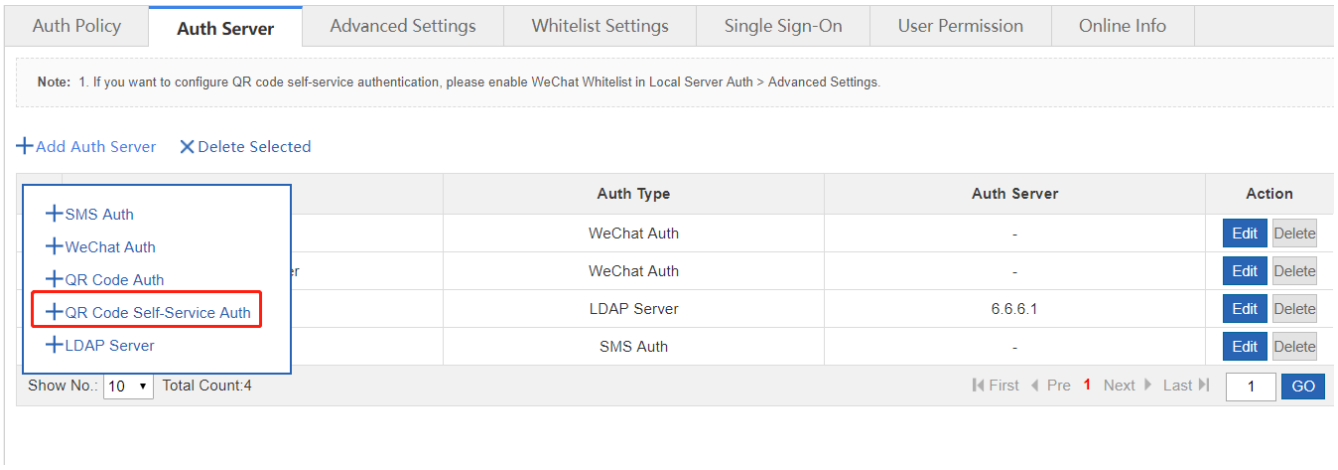
Click Add Auth Server to expand the authentication menu. You can select QR code authentication here.

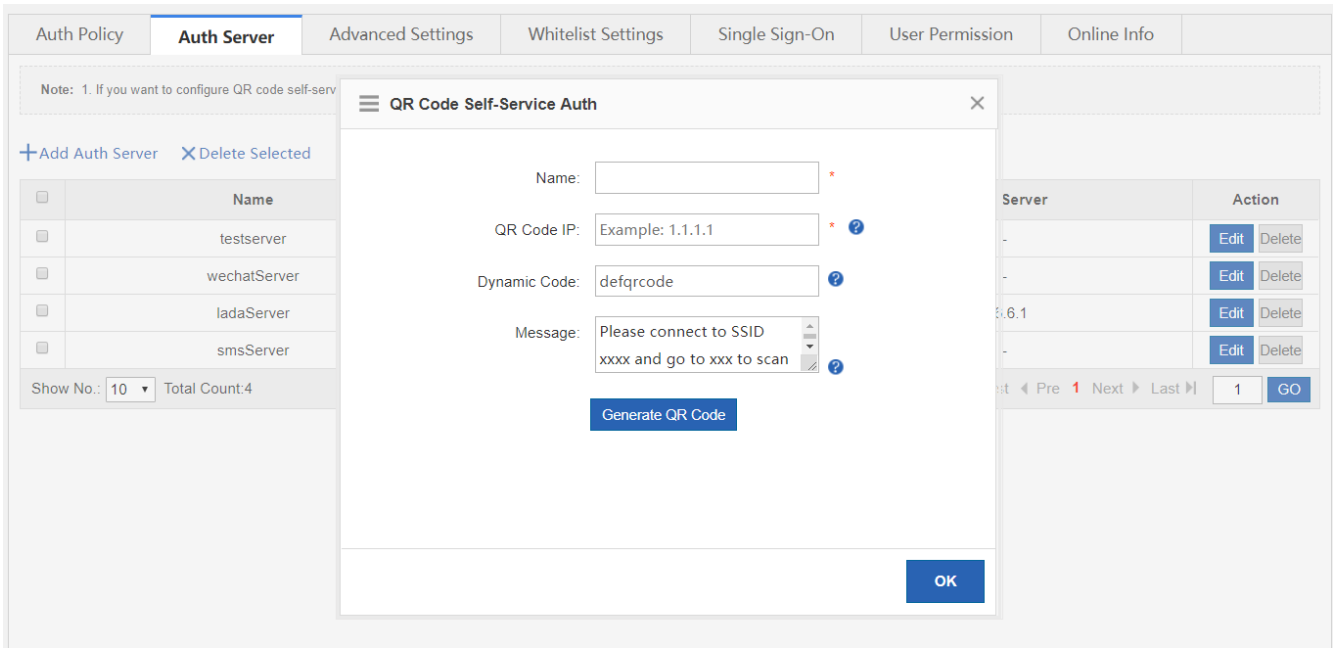





6. Adding/Editing QR code authentication

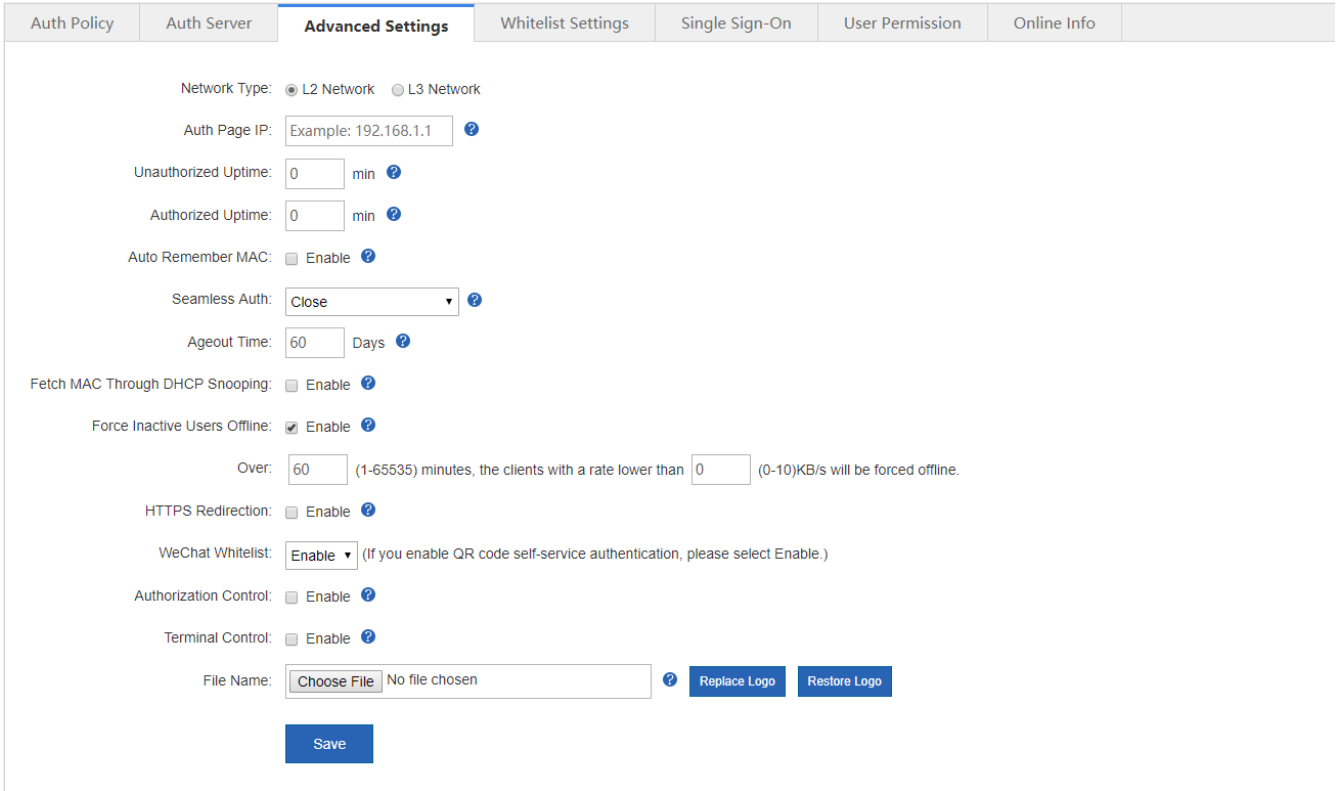
Click +Add Auth Server to expand the authentication menu. You can select QR code self-service authentication here.



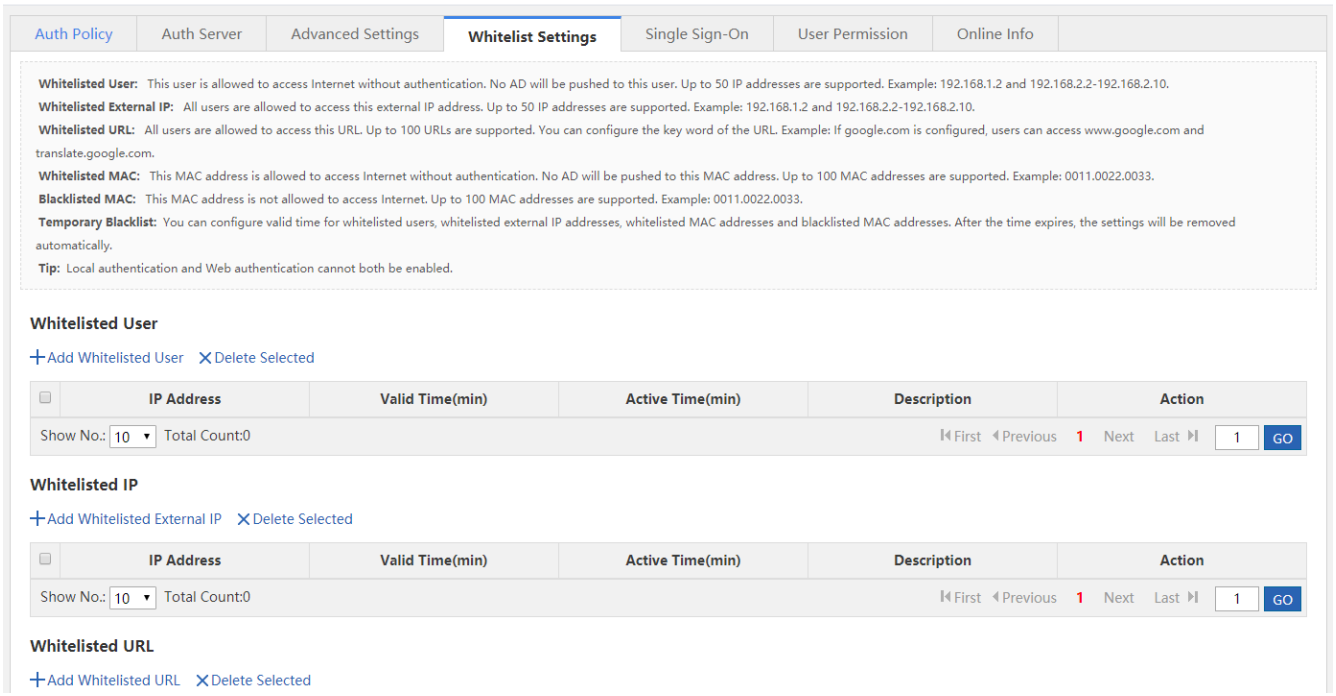



## 1.3.13.3.3 Advanced Settings

Choose **User** > **Local Server Auth** > **Advanced Settings** to enter the configuration page.

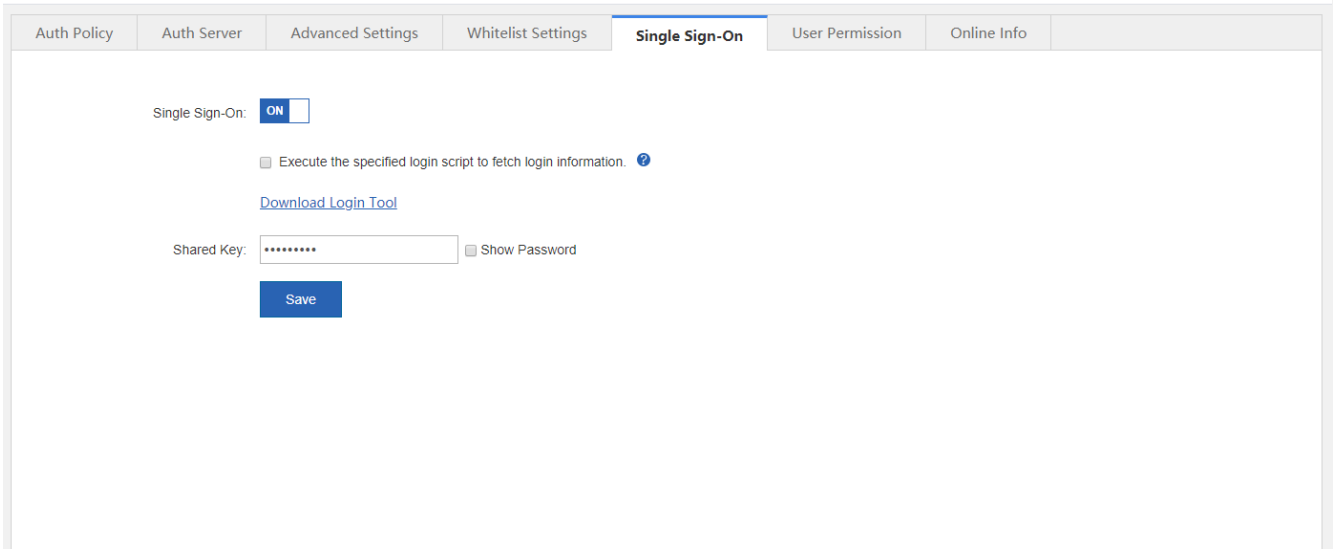


## 1.3.13.3.4 Whitelist Settings



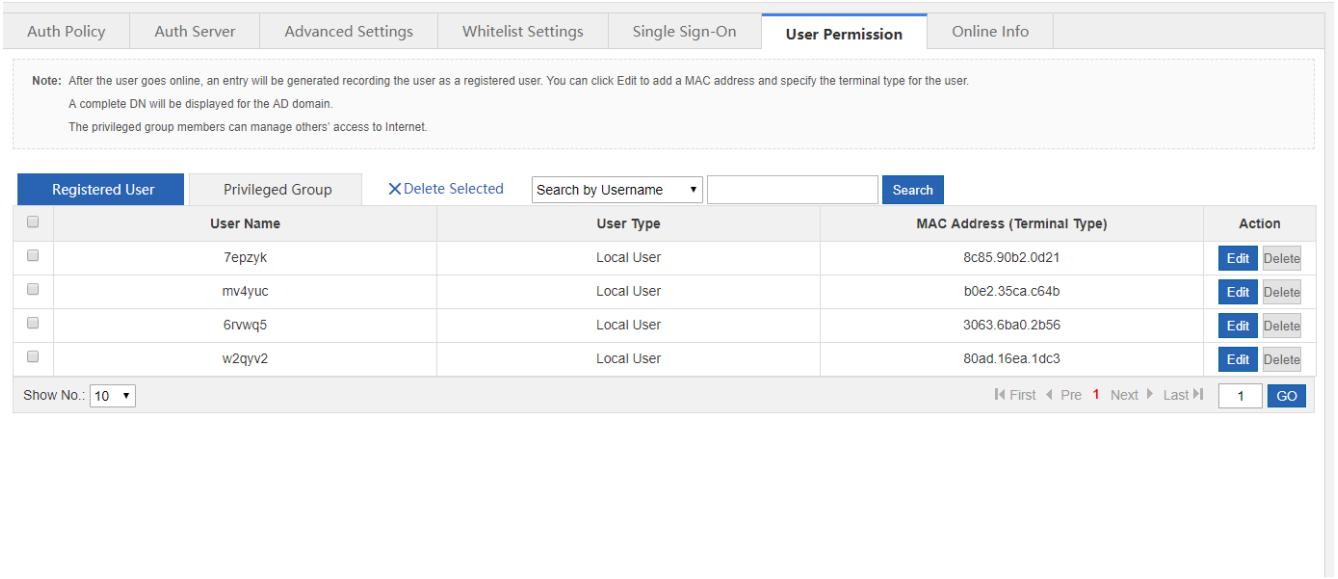

## 1.3.13.3.5 Single Sign-On

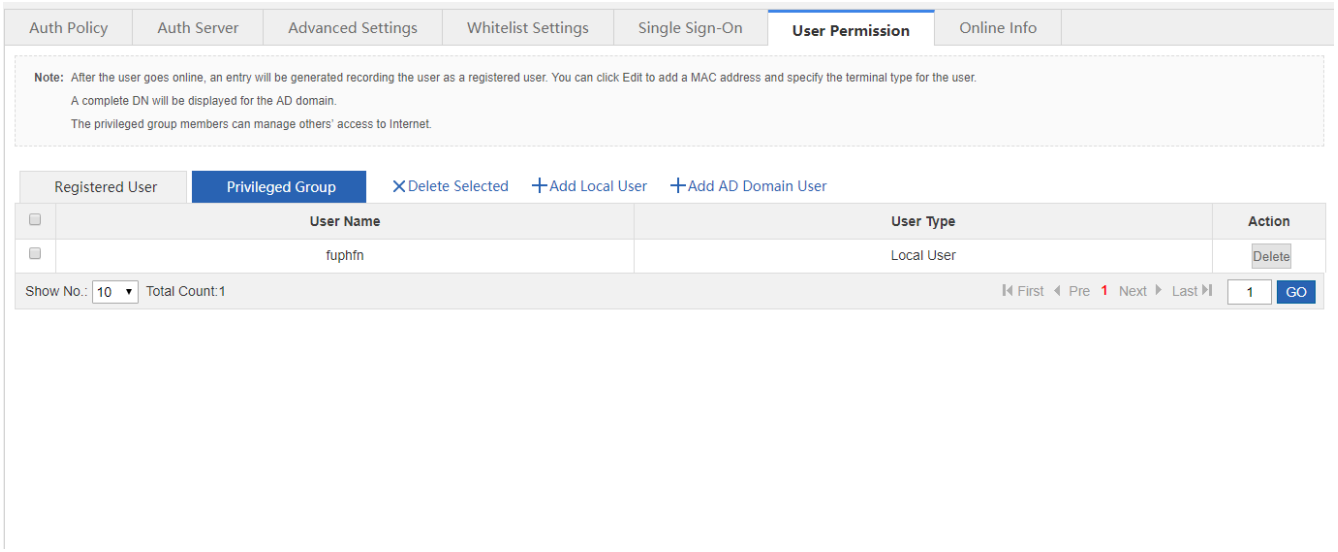
Choose **User** > **Local Auth** > **Single Sign-on**, and single sign-on settings will be displayed.



### 1.3.13.3.6 User Permission

Choose **User** > **Local Auth** > **User Permission**, and registered user and privileged group settings will be displayed.



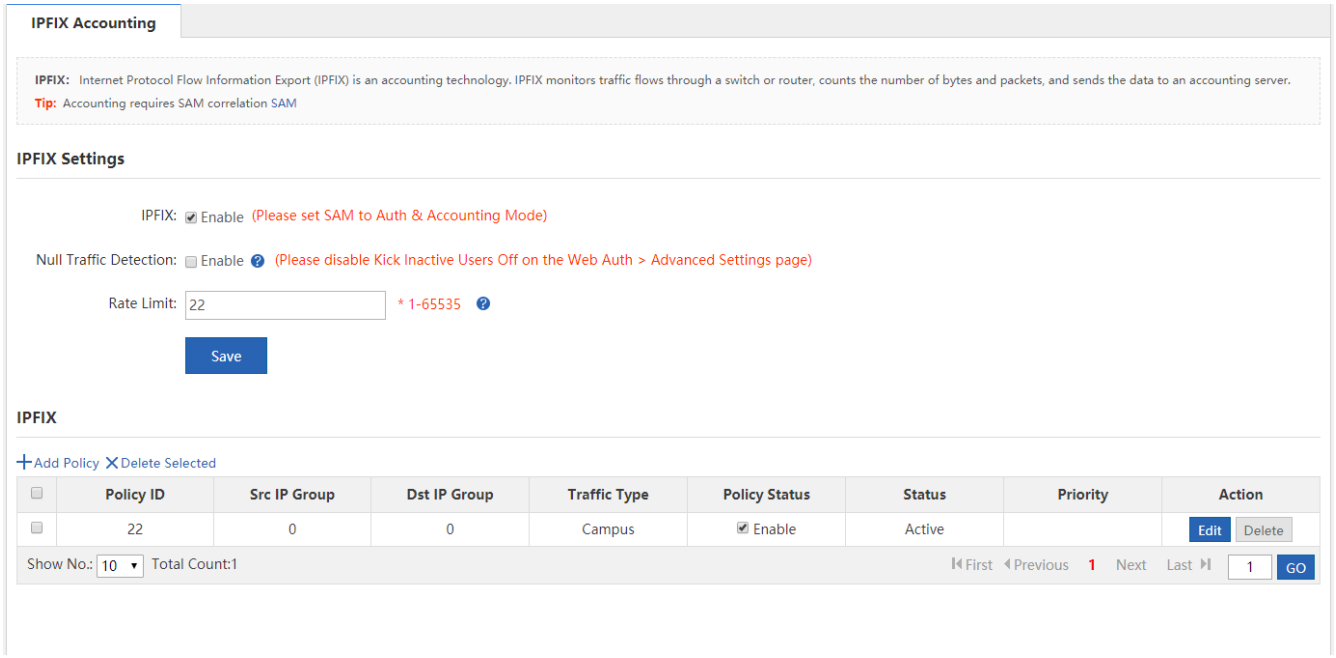

### 1.3.13.3.7 Online Info

Choose **User** > **Local Auth** > **Online Info**, and the user information will be displayed. You can click Force Offline to kick off users.

### 1.3.13.4 SAM Auth

Link-sam sends notification of SAM/SMP servers to IPFIX and provides interfaces to IPFIX for this purpose.

### 1.3.13.4.1 IPFIX Accounting




1. Enabling IPFIX

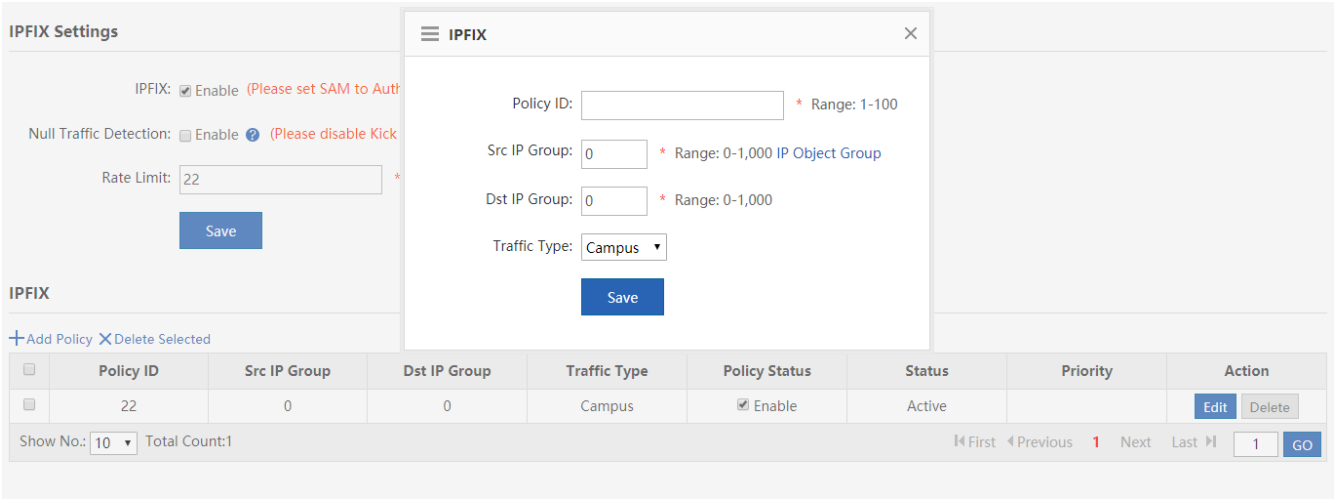
   Check the **IPFIX** box to enable this feature.

2. Adding an IPFIX policy

Click 

to add a policy. Enter a policy ID, a source IP group and a destination group, select the traffic type and click 

.

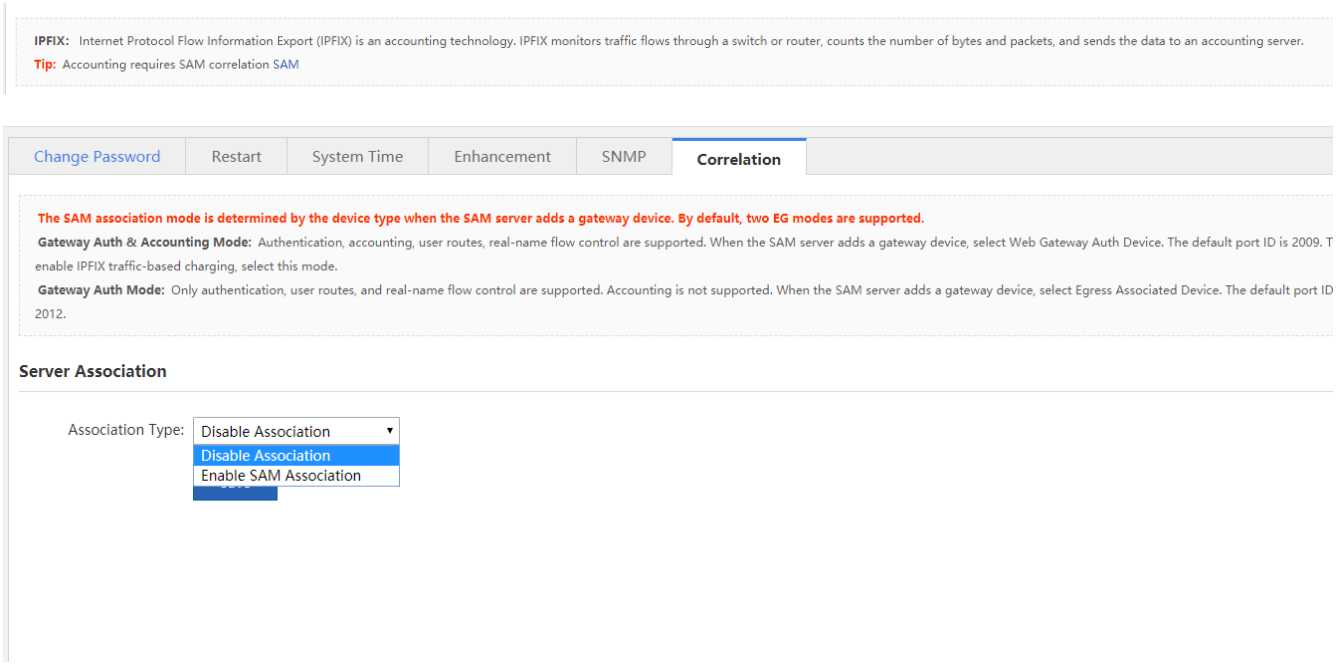



3. Deleting an IPFIX policy

Click Delete to delete an IPFIX policy or click Delete Selected to delete selected IPFIX policies.

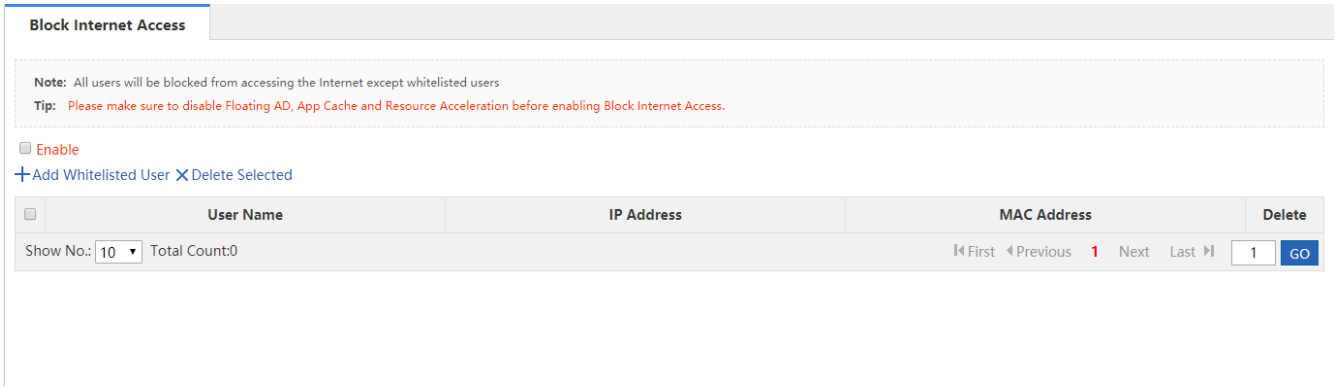
## 1.3.13.4.2 Correlation

Click SAM to enable or disable SAM correlation. Enter the address of the SAM server into the **Server IP Address** text box.

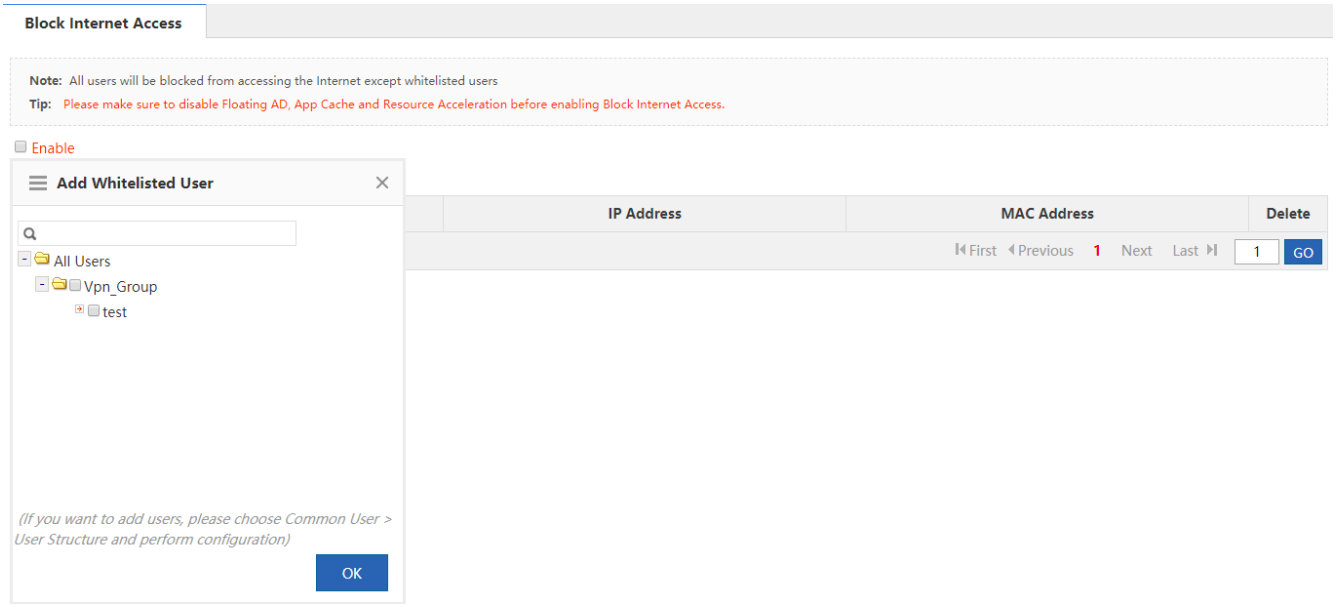



## 1.3.13.5 Block Internet Access

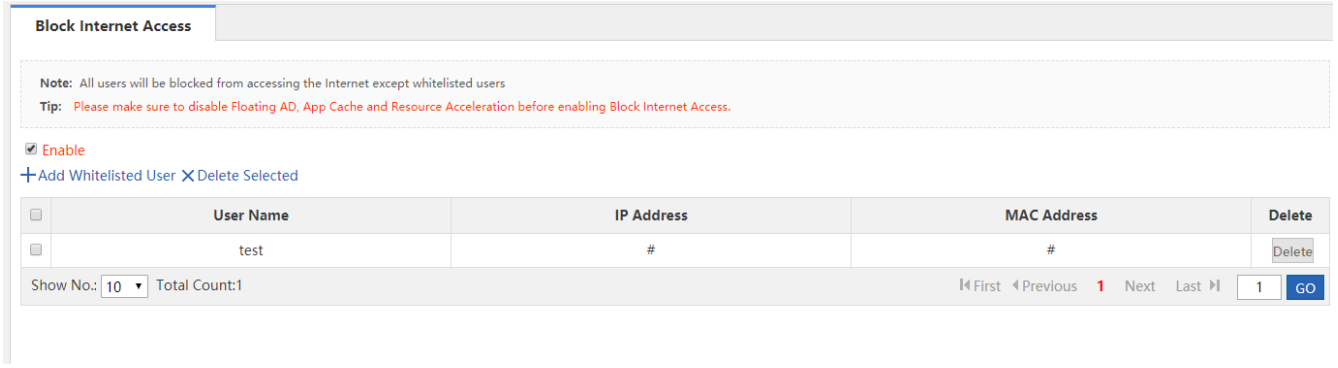
If you enable **Block Internet Access**, all internal users cannot access the Internet unless configured as whitelisted users.




Click Add Whitelisted User to add at least one whitelisted user before enabling this function.



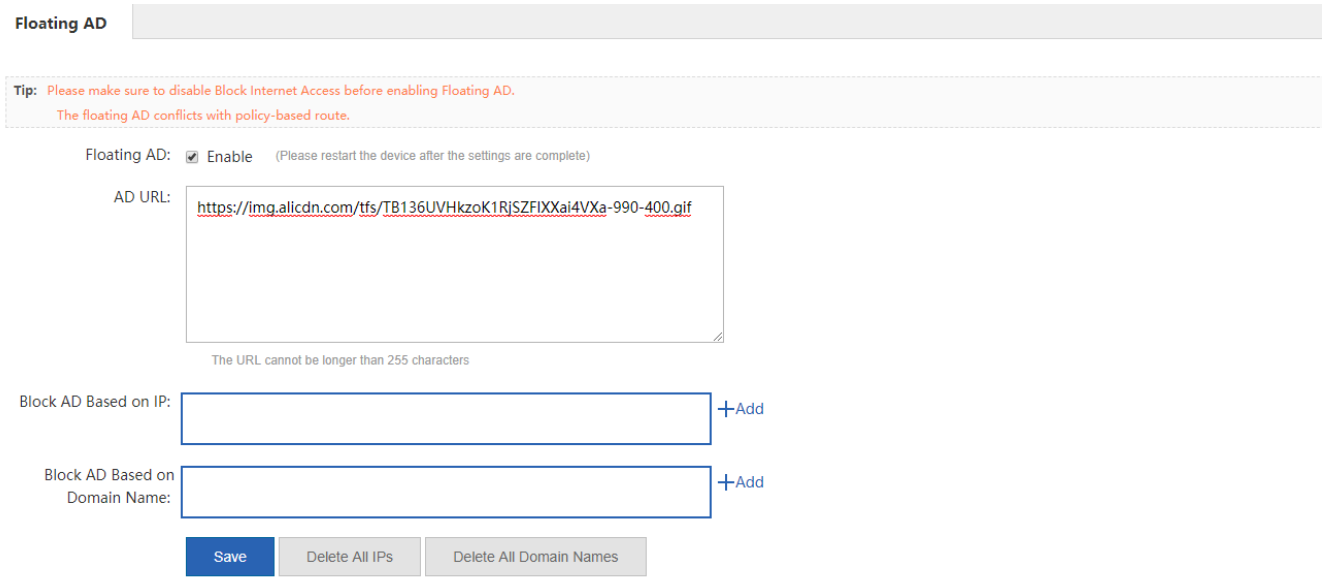

Select the whitelisted user and click OK :




Click Delete to delete a whitelisted user or click Delete Selected to delete selected whitelisted users.

### 1.3.13.6 Floating AD

If you enable this function for the first time, please restart the device to activate settings.

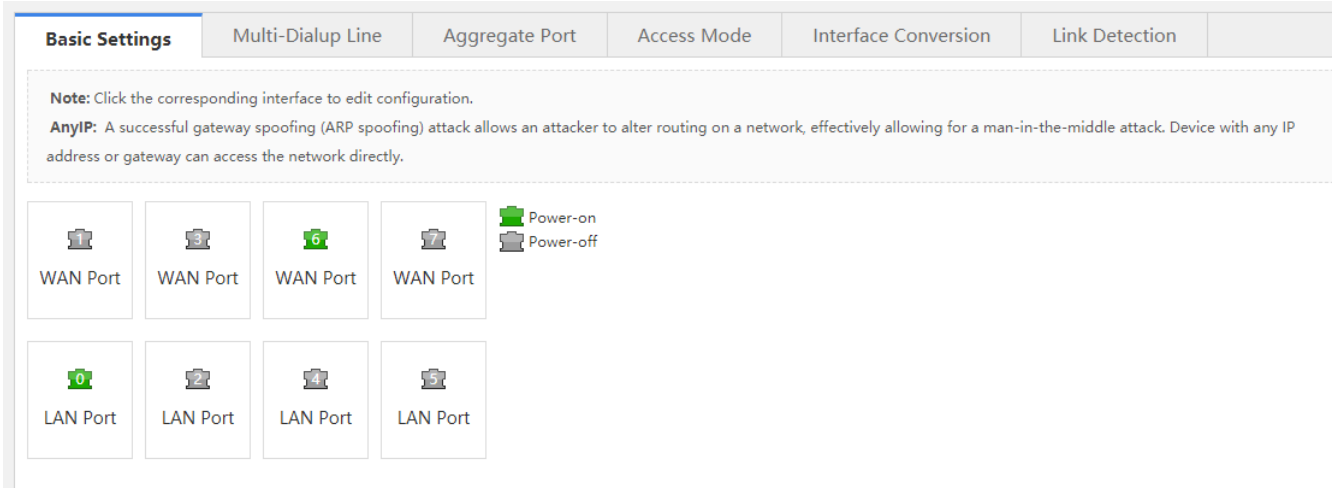


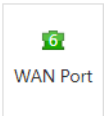

You can block AD based on the IP address or the domain name. After you enable floating AD, the AD will pop up when you browse the webpage.

## 1.3.14 Network

### 1.3.14.1 Interface

Interface configuration is the key configuration for implementing Internet access for LAN users. It determines whether LAN users can access the Internet successfully. The interface configuration page is shown in the figure below.





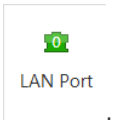
highlighted in green indicates that the interface is powered on (with the network cable connected) and 

in gray indicates that the interface is powered off (without network cable connected).

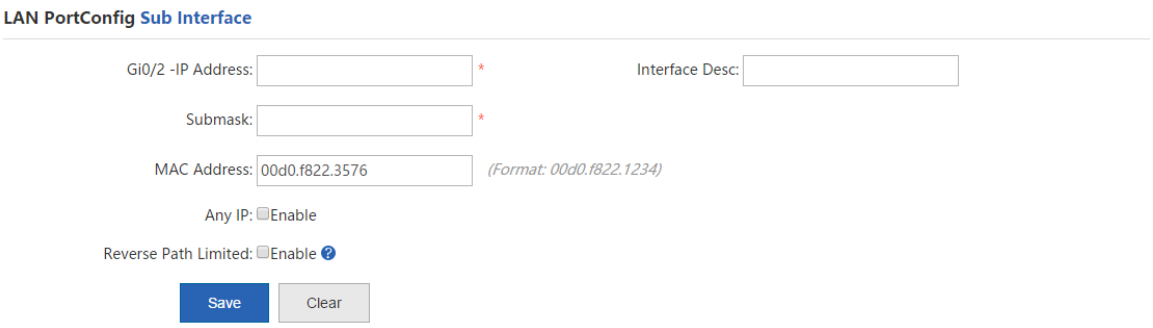
Interfaces are configured differently in gateway mode and bridge mode, which are described in the following sections.

### 1.3.14.1.1 Basic Interface Settings

- **LAN Port Configuration**

Click a required LAN port to configure it, for example, click 

.


**Ag1-IP Address**: Enter the IP address of the LAN port.

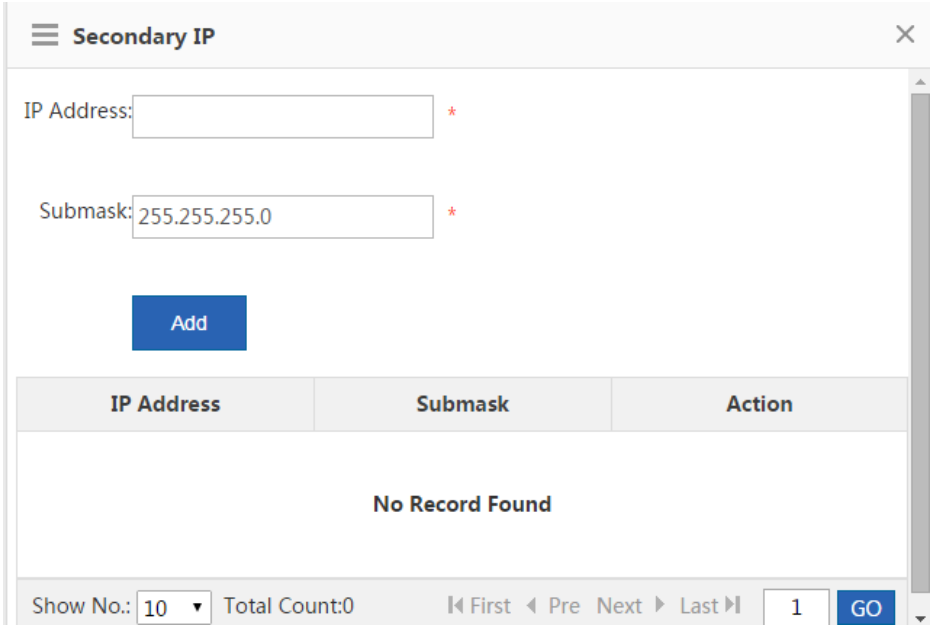
**Submask**: Enter the mask address of the network segment.

**MAC Address**: Indicates the physical address of the interface. It is used to prevent internal physical address conflicts and generally does not need to be configured.

**Any IP**: After the any IP function is enabled, LAN PCs can access the Internet without IP addresses or with random IP addresses. That is, this function prevents the failure of some PCs in accessing the Internet even if they are assigned incorrect IP addresses.

**Reverse Path Limited**: After this function is enabled, packets received from the CERNET interface are sent out still through the CERNET interface. And the device does not search the routing table when replying with response packets. The purpose is to prevent the occurrence of the following case: When the device responds to a DNS request from a user of, for example, China Telecom, through the CERNET interface, the device searches the routing table and finds that the response packet needs to be sent out through the interface of China Telecom; and the ISP will take measures to block packets from the CERNET interface, which will result in packet loss and a packet parsing failure.

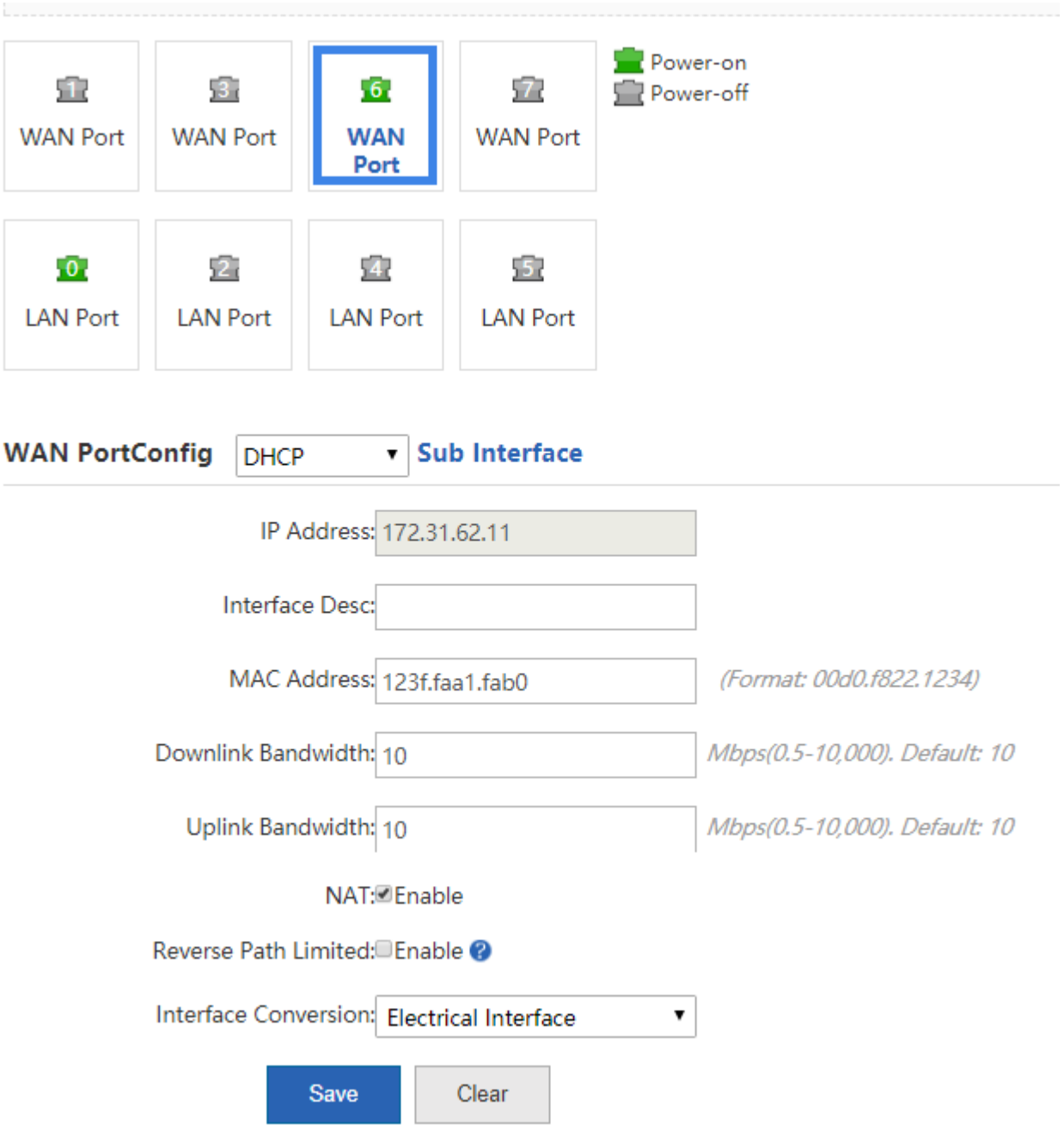
**Secondary IP**: An Ethernet interface supports multiple IP addresses. Secondary IP addresses are IP addresses other than the IP address configured for the first time. Click Secondary IP to manage secondary IP addresses of the selected interface.




**Sub Interface**: Sub interfaces are multiple logical interfaces derived from one physical interface, that is, multiple logical interfaces are associated with one physical interface. The logical interfaces belonging to the same physical interface share the physical configuration parameters of the physical interface but have independent link-layer and network-layer configuration parameters.

- **WAN Port**

Select the required WAN port. The configuration page shown in the figure below is displayed.



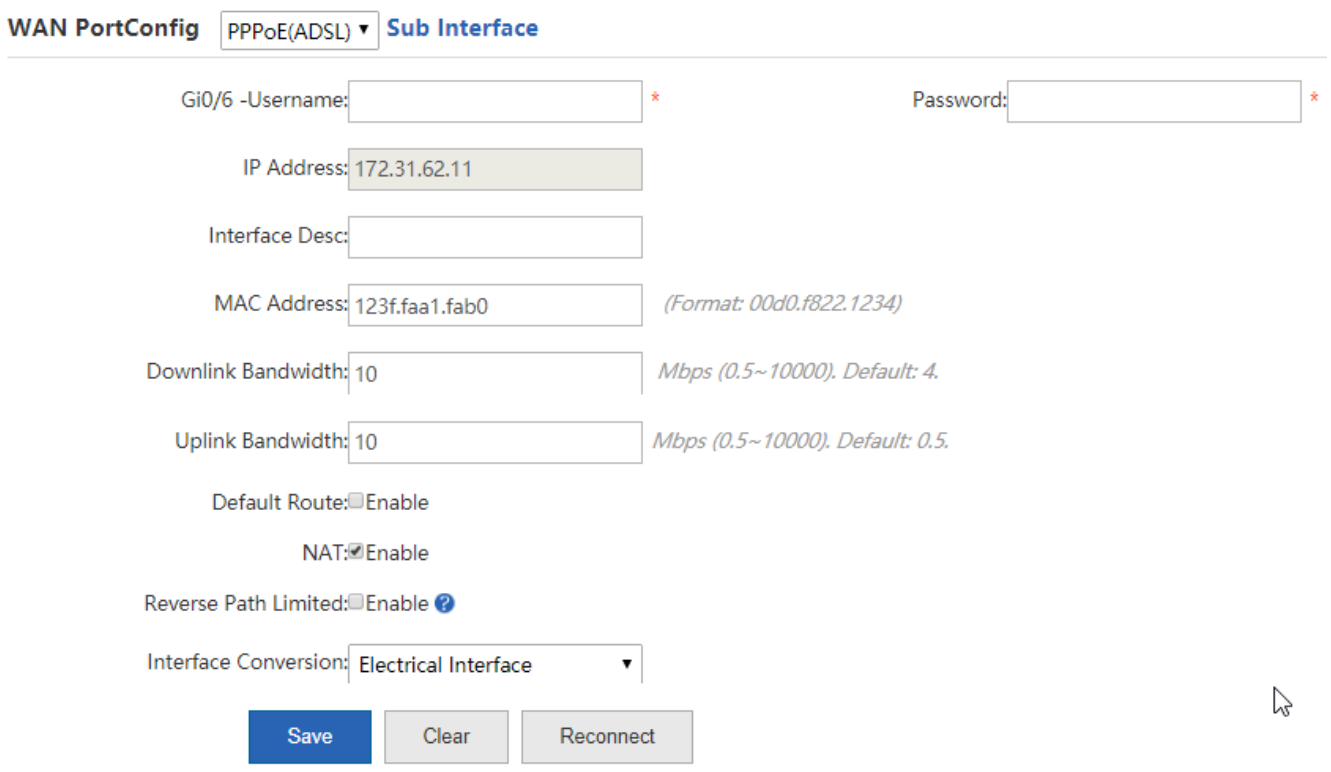

1. **WAN PortConfig**: WAN port configuration includes **Static IP**, **DHCP**, and **PPPoE(ADSL)**.

- Static IP

The figure above shows the static IP address configuration page. When **WAN PortConfig** is set to **Static IP**, configure the IP address, subnet mask, and next-hop address (which can be understood as a gateway) assigned by the ISP.

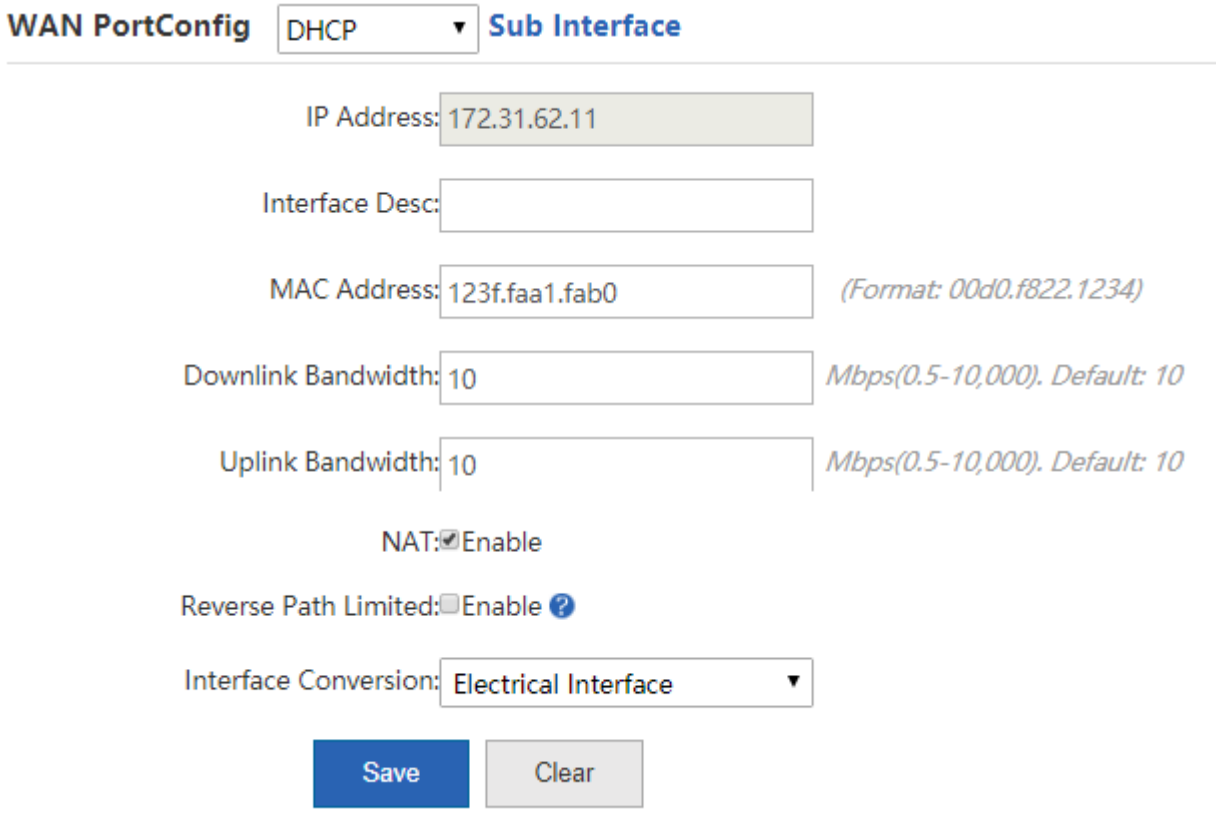
- PPPoE(ADSL)

Select **PPPoE(ADSL)**, and enter the dialup account and password obtained from the ISP, as shown in the figure below.




- DHCP

If you select **DHCP**, the system dynamically obtains IP addresses.

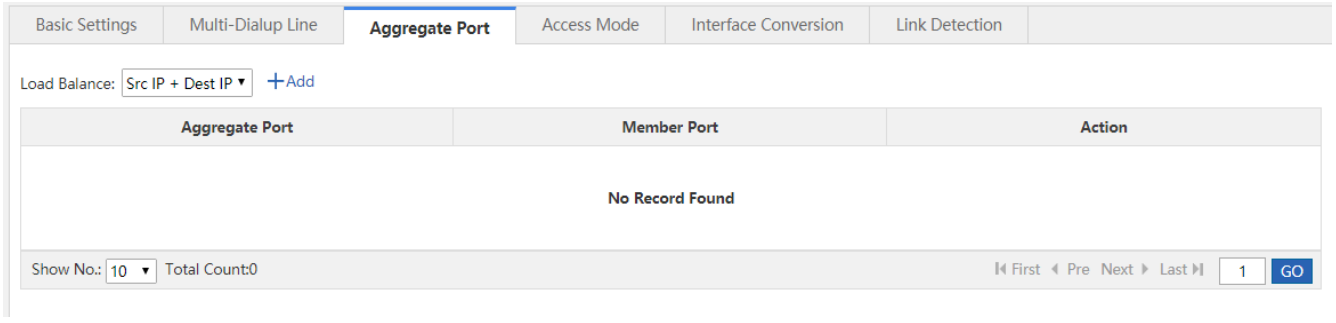



2. Other WAN port configuration items:

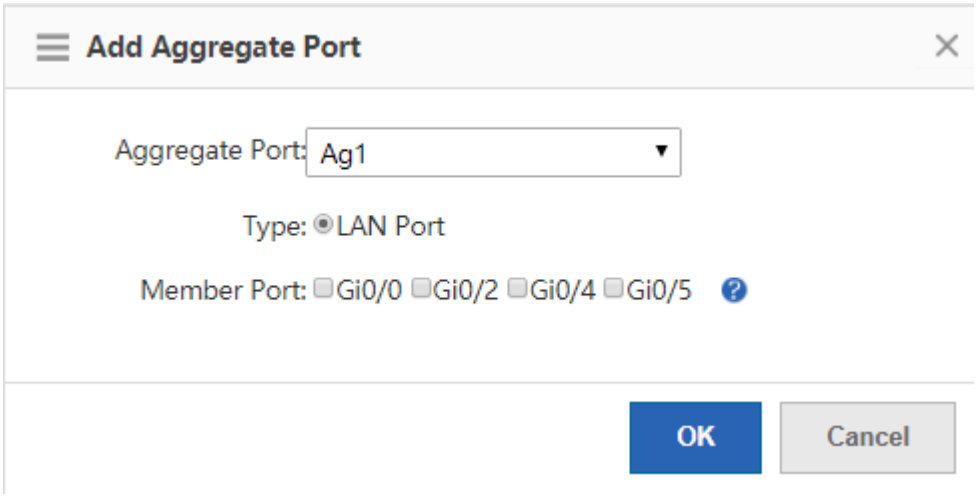
1) **Interface Conversion**: Indicates that this interface can be used as an SFP interface or electrical interface. Generally, not all WAN ports support this function.

2) **Uplink Bandwidth** and **Downlink Bandwidth**: Indicate the maximum bandwidths supported by the interface. Enter the actual bandwidth obtained from your ISP. The value ranges from 0.5 Mbps to 1000 Mbps. The default value is 10 Mbps.

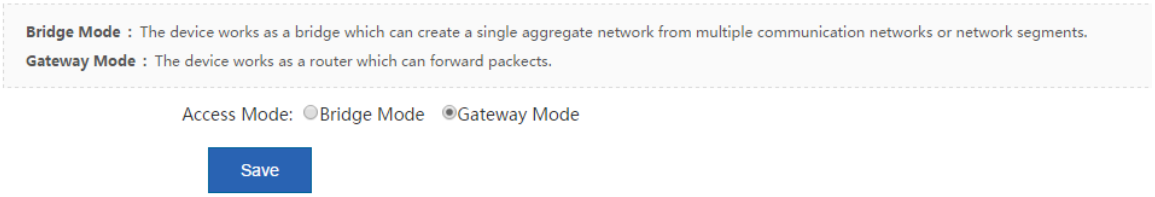
### 1.3.14.1.2 Multi-link Aggregation




Click +Add. In the window displayed, select an aggregate port and member ports, and click OK.




### 1.3.14.1.3 Access Mode

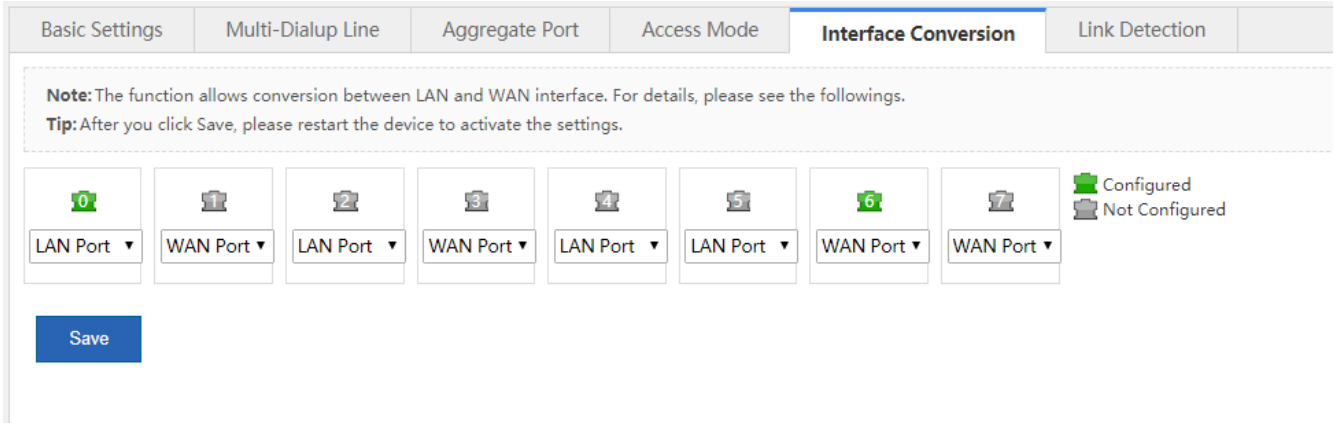



Select the required access mode, and click 

. The device switches to the selected mode successfully after restart.

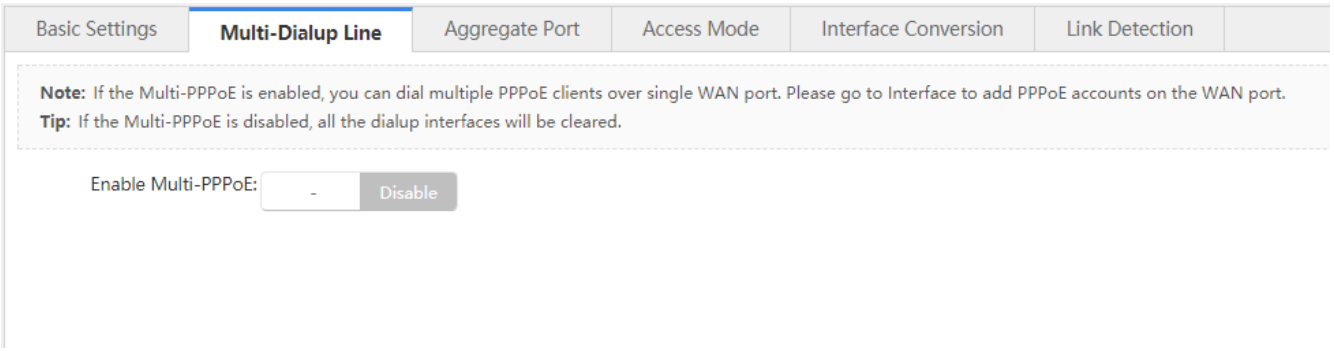
### 1.3.14.1.4 Interface Conversion

Each interface supports conversion between the LAN port mode and the WAN port mode. The interface conversion configuration page is shown in the figure below.



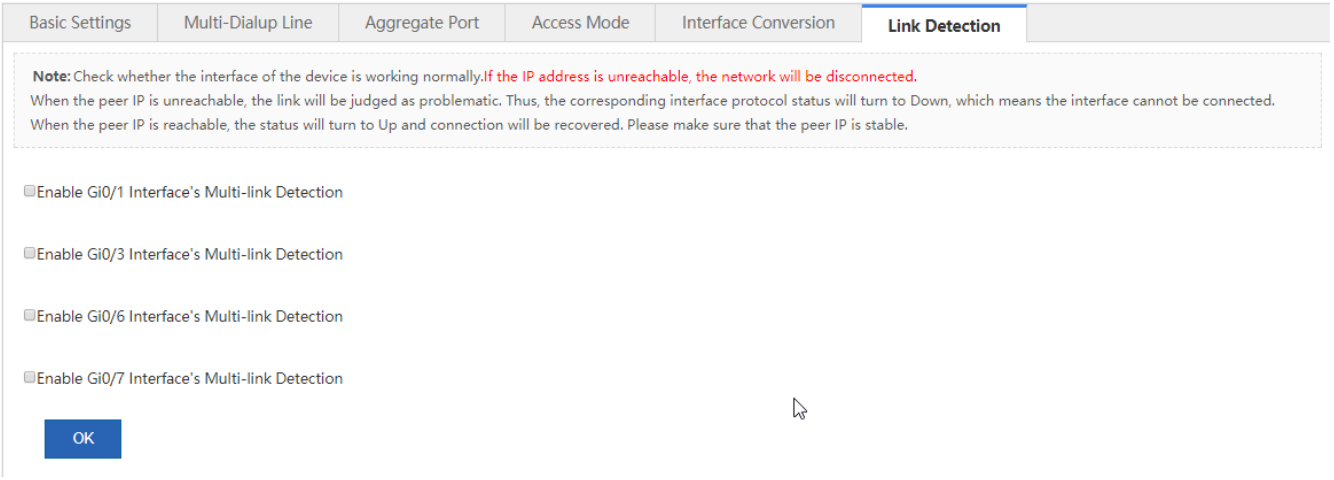
Click a drop-down list to convert an LAN port into a WAN port or vice versa and click Save. The interface mode takes effect after the device is restarted.

### 1.3.14.1.5 Multi-PPPoE

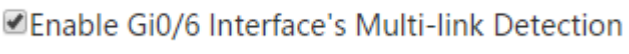



### 1.3.14.1.6 Link Detection

Link detection is used to detect whether a WAN interface of the device functions properly. The configuration page is shown in the figure below.




Configuration steps:

Select the interface to be detected. For example, select 

. The link detection configuration items of Interface Gi0/6 will be displayed.


1. To detect whether the interface is reachable, enter an address that can be pinged successfully in **IP Address**.
2. Enter the next-hop IP address. If the device is a LAN device, enter the gateway address. If it is not configured, the next-hop address is the ping IP address by default.

3. Set **Detection Internal**. The default value is 1s.

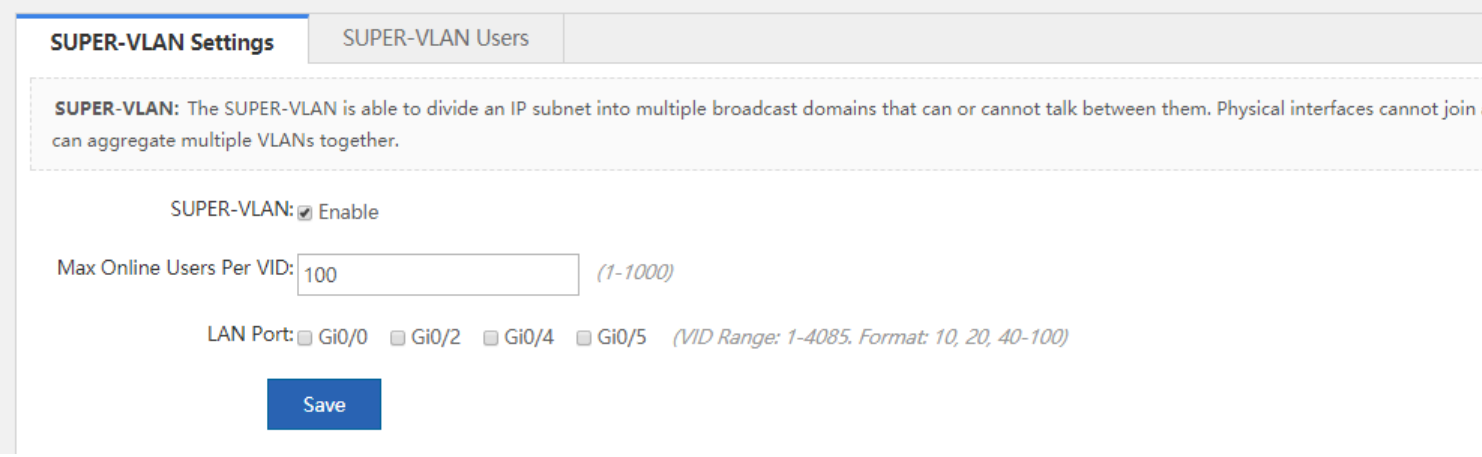
4. Click OK. If the IP address can be pinged successfully, a prompt is displayed, indicating that the network is good. Otherwise, another prompt is displayed, indicating that the network is disconnected.

### 1.3.14.2 SUPER-VLAN

With Super VLAN, the traffic of each VLAN can be transmitted and received by a designated LAN interface, without configuring sub interfaces.

#### 1.3.14.2.1 SUPER-VLAN Configuration

This page allows you to enable and configure the SUPER-VLAN function. The configuration page is shown in the figure below.




**SUPER-VLAN**: Click Enable to enable the SUPER-VLAN function.

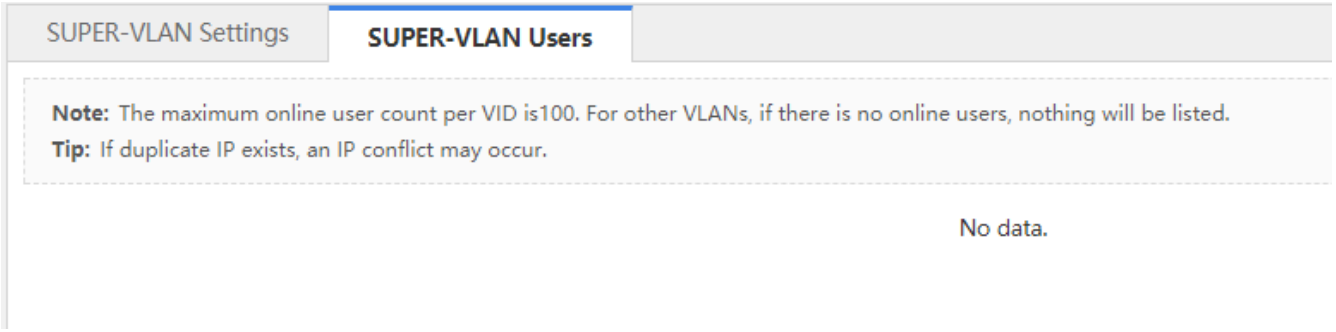
**Max Online Users per VID**: Indicates the maximum number VLANs that can be created. The value ranges from **1** to **1,000**.

**LAN Port**: Select required LAN ports. Then, relevant configuration items are displayed below **LAN Port**. The VID ranges from **1** to **4085**. VID ranges of two interfaces cannot be overlapped. For example, if the VID of a port ranges from 1–1000, the VID range of another port cannot be 500–600 and must be beyond 1–1000.

Click Save to save the configuration.

#### 1.3.14.2.2 Online SUPER-VLAN Information

This page displays information about online super VLANs, as shown in the figure below.




### 1.3.14.3 Route/Load

Route: The policy-based route, application-based route, and common IP route can serve as rules for packet forwarding. When a policy-based route is configured, the priorities are as follows: Policy-based route > Application-based route > Static route (address library) > Default route.

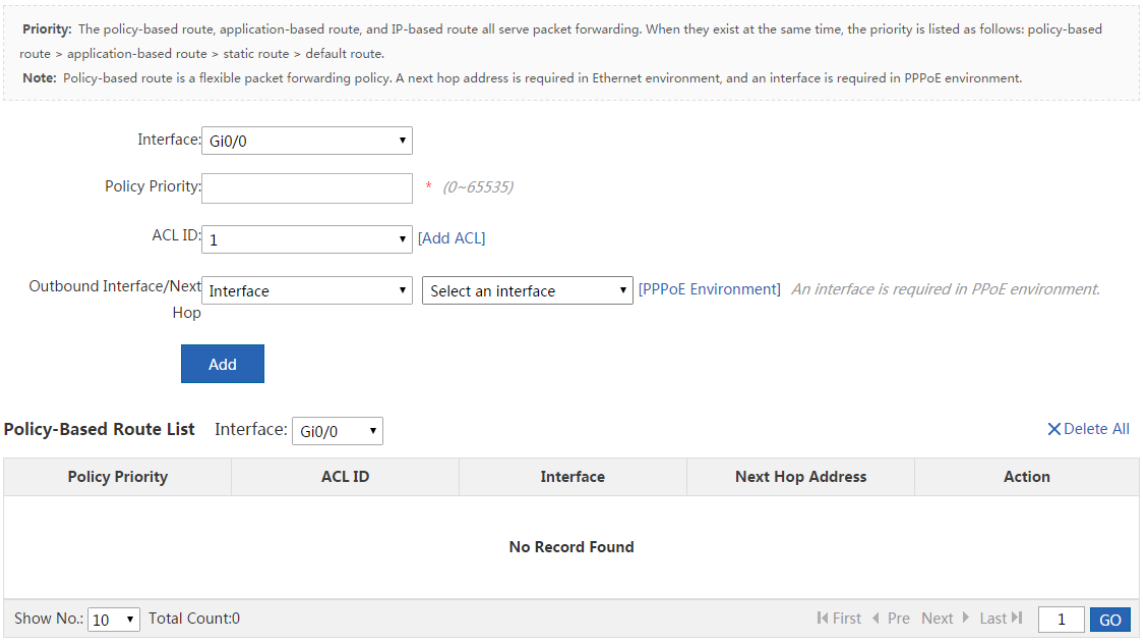
Load: A network egress is usually connected to two or more ISP links, for example, clients of education users can be connected to the CERNET line and China Telecom/China Netcom line. Multiple ISP links share traffic or serve as backups according to certain policies, that is, implement load balancing among the links.

#### 1.3.14.3.1 Policy-based Routing

The Policy-based Routing (PBR) provides a data packet routing and forwarding mechanism that is more flexible than target network-based routing. The PBR allows the device to determine, according to the route map, how to process data packets. The route map shows the next-hop forwarding device of a data packet.

A route map dedicated for PBR must be specified and must be created before PBR is applied. A route map consists of multiple policies. After PBR is applied to an interface, the device checks all packets received by the interface. Data packets that do not conform to any policy in the route map are processed in the common routing and forwarding mode. Data packets that conform to a policy in the route map are processed according to the actions defined in the policy.

The PBR configuration page is shown in the figure below.




1. PBR settings: Select the required interface, set the policy priority, select the ACL (to be applied to a specific policy), enter the next-hop address, and click  .

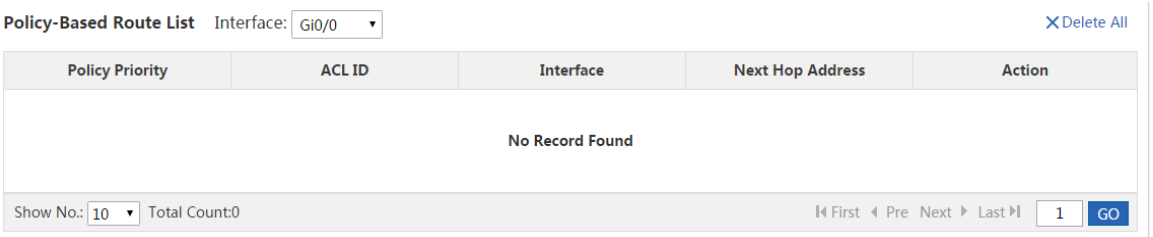


ACL list: You can click  to add an ACL list. For detailed operations, see "ACL."



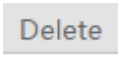
Next hop: refers to the next closest router a packet can go through. The next hop is among the series of routers that are connected together in a network and is the next possible destination for a data packet. More specifically, next hop is an IP address entry in a router's routing table, which specifies the next closest optimal router in its routing path. Every single router maintains its routing table with a next hop address, which is calculated based on the routing protocol used and its associated metric.

**2. Policy-Based Route List**




Edit a policy: In the policy-based route list, click  to modify a policy.



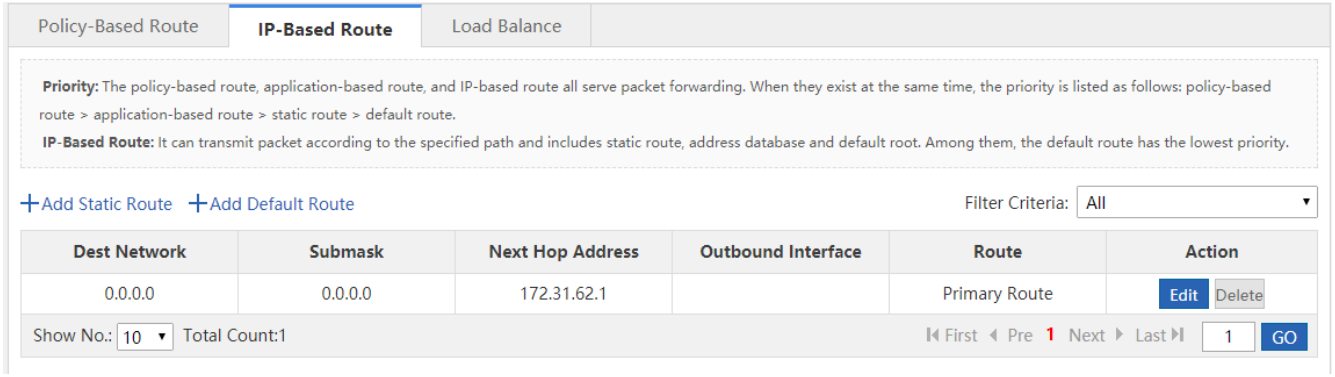
Delete a policy: In the policy-based route list, click  to delete a policy. You can click  in the upper right corner to delete all routing policies in the policy group.

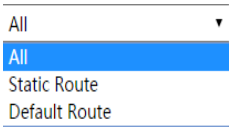
### 1.3.14.3.2 IP-Based Route

Common IP routing enables the transmission of packets destined for a specified target network along the predefined path.

Common IP routes include static routes and default routes. The default routes have the lowest priority.

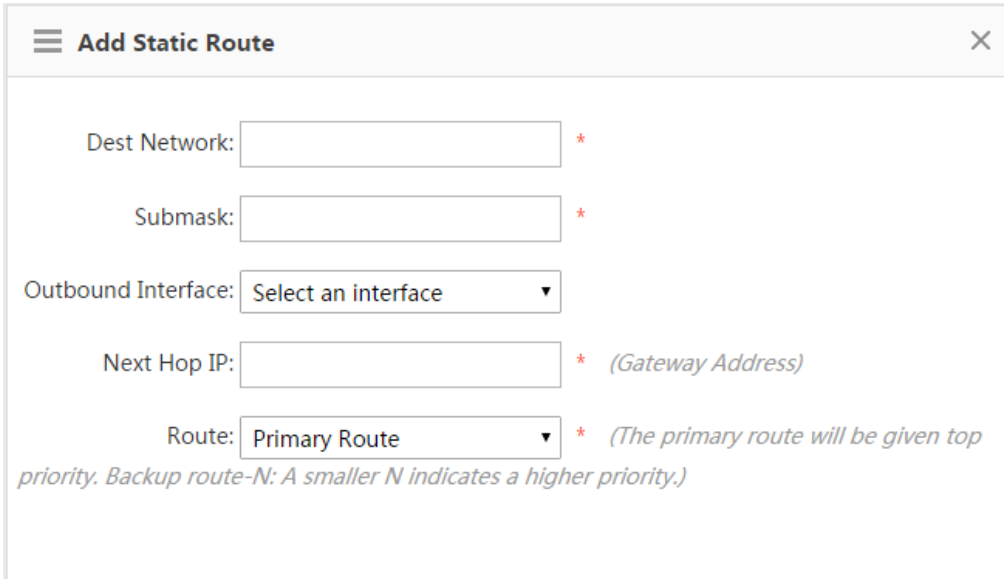
The common routing configuration page is shown in the figure below.




The table as shown in the figure above lists static routes and default routes configured in the system. You can select a value from the **Filter Criteria** 

drop-down list to display only static routes or default routes.

1. **Static route**: Click +Add Static Route. The **Add Static Route** dialog box is displayed, as shown in the figure below.




**Dest Network**: Indicates the destination network segment of a route.

**Submask**: Indicates the mask of the destination network segment.

**Outbound Interface**: Indicates the outbound interface of a route.

**Next Hop IP**: Indicates the inbound interface address of the next-hop route (gateway).

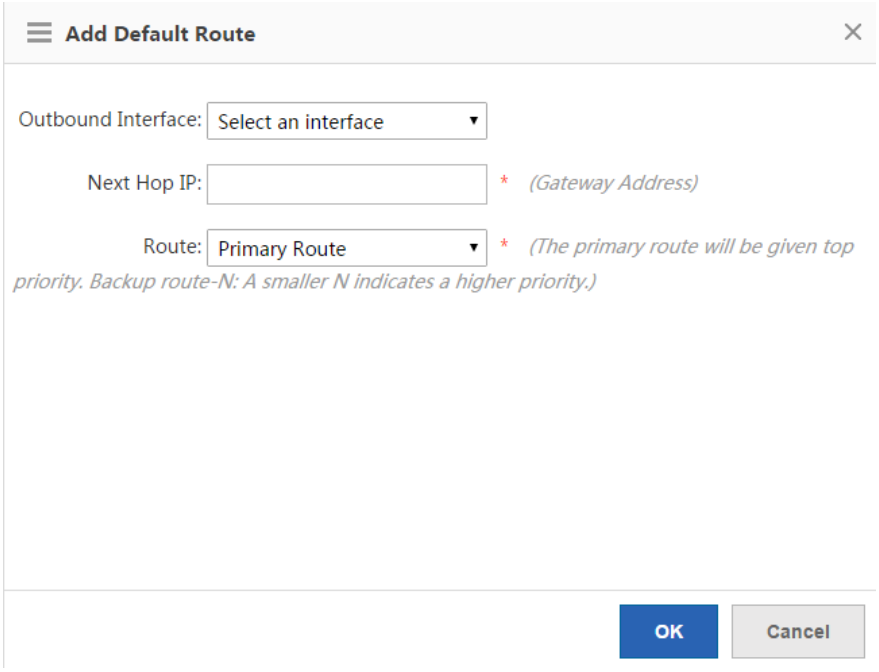
**Route**: Specifies the route priority. The primary route has the highest priority. For the backup route-N, a smaller value of N indicates a higher route priority.

Click OK to create a static route.

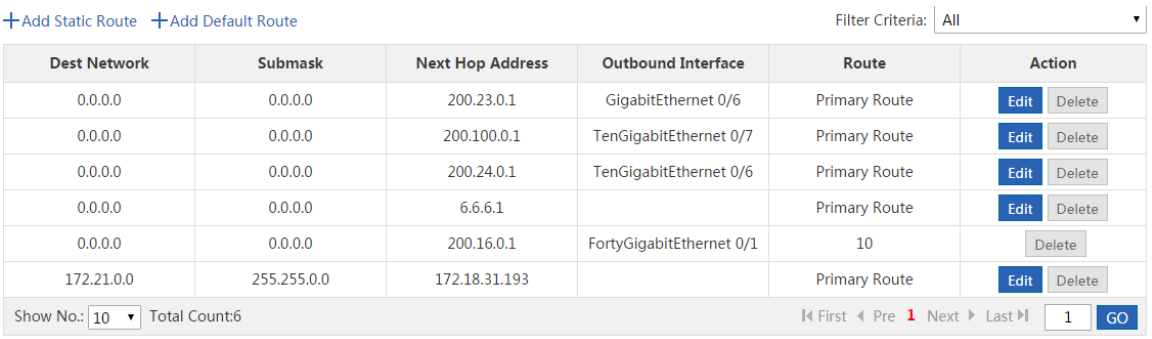
| Dest Network | Submask | Next Hop Address | Outbound Interface | Route | Action |
|---|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 172.21.148.1 | | Primary Route | Edit Delete |
| 2.1.1.0 | 255.255.255.0 | 12.1.1.2 | | Primary Route | Edit Delete |
| 11.1.1.0 | 255.255.255.0 | 12.1.1.2 | | Primary Route | Edit Delete |

Click Delete to delete a static route.

2. **Default route**: Click +Add Default Route. The **Add Default Route** dialog box is displayed, as shown in the figure below.



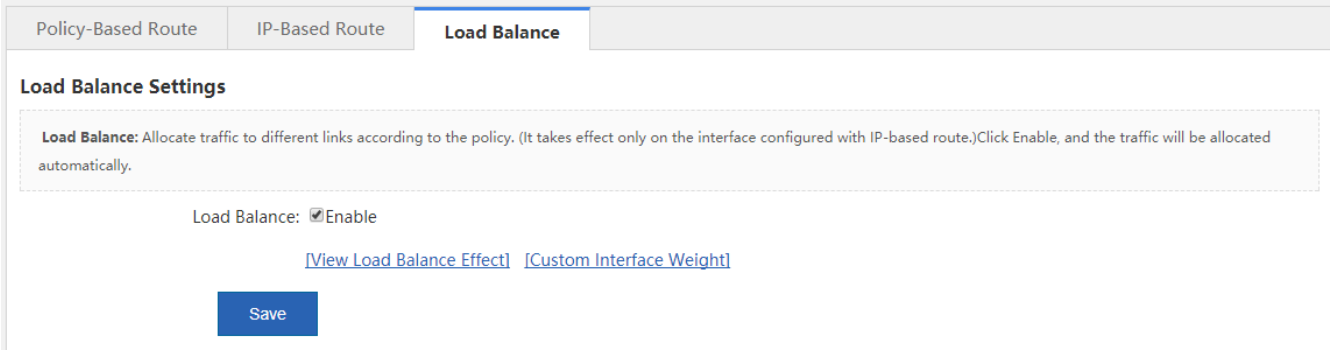

Select the outbound interface of a route, enter the next-hop IP address, set **Route**, and then click OK to create a default route.




Click Delete to delete a default route.

### 1.3.14.3.3 Load Balancing

Load balancing of multiple links can distribute traffic among multiple links according to certain policies, so that improve the utilization rate of link resources.




Click [View Load Balance Effect] to display the load balancing effect.

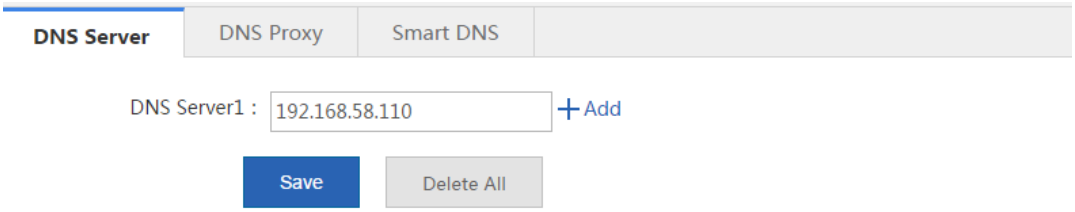
### 1.3.14.4 DNS

The Domain Name Server (DNS) configuration includes the DNS server configuration, DNS proxy configuration, and smart DNS configuration.

### 1.3.14.4.1 DNS Server

A DNS name server is a server that stores the DNS records for a domain.

On the **DNS Server** page, configure the DNS server address for the device. Up to two DNS server addresses can be configured. Click +Add to configure the second DNS server address and then click Save.



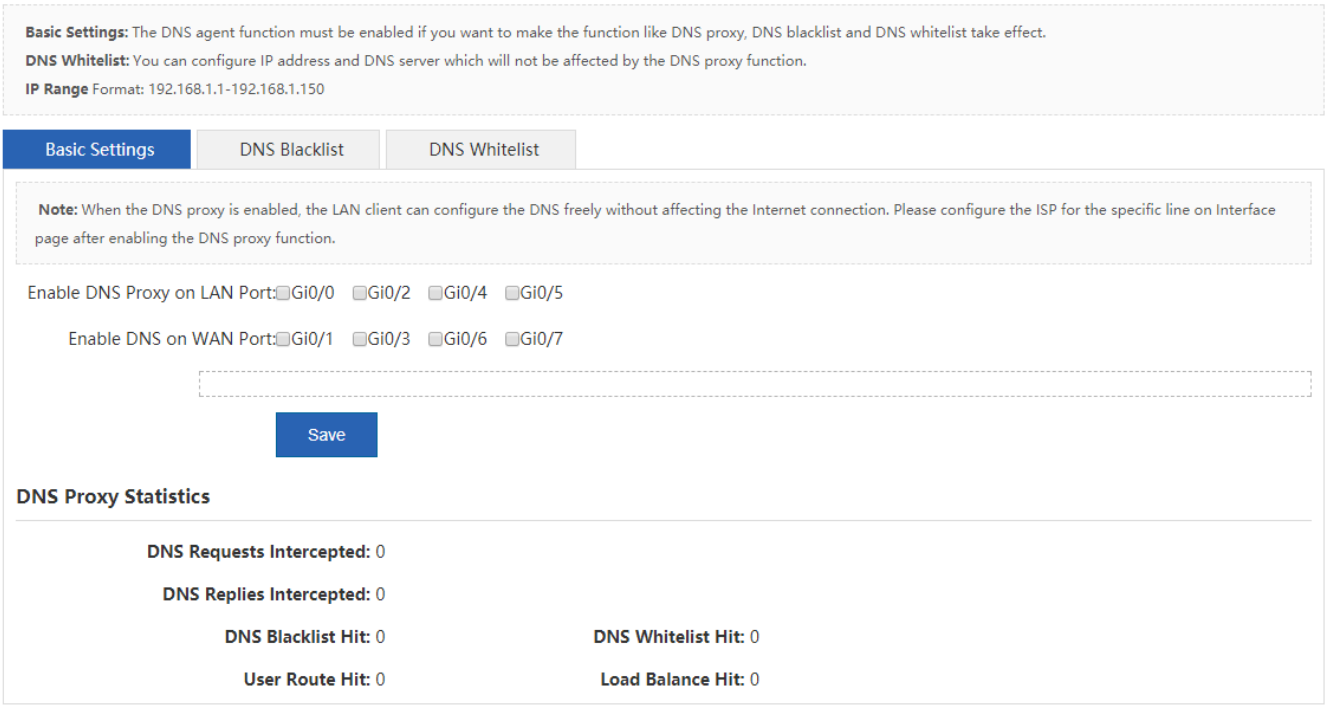

### 1.3.14.4.2 DNS Proxy

The DNS proxy is generally deployed on the frontend router and located between a DNS server and user PCs. It processes DNS domain name resolution requests of users on behalf of the DNS server. The configuration of the DNS proxy includes basic settings, DNS blacklist, and DNS whitelist.

- Basic Settings

Basic settings are the premise for the DNS proxy function to take effect. The basic settings of the DNS proxy need to be configured first in order to implement the DNS blacklist and DNS whitelist functions.

The DNS server address needs to be configured on WAN interfaces.

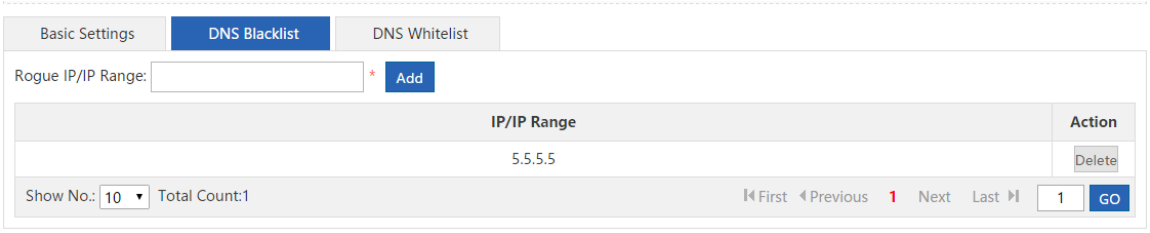



As shown in the figure above, select WAN interfaces on which the DNS proxy is to be configured, configure DNS server addresses (1 or 2 DNS server addresses can be configured for each interface and at least one needs to be configured), and

then click Save to complete the configuration. Note that you can select either of the following two solutions based on the ISP line for load balancing: by line bandwidth or by line load.

- DNS Blacklist

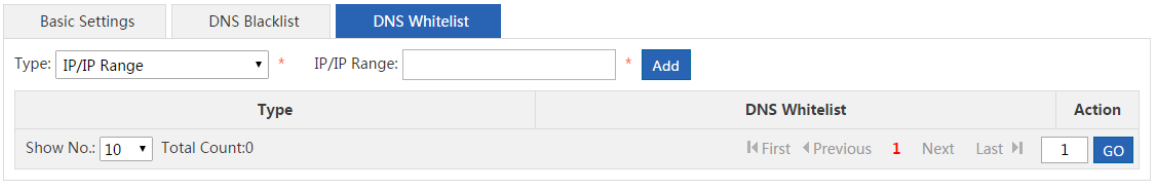
The **DNS Blacklist** page allows you to add rogue IP addresses to the blacklist. When the DNS proxy intercepts a DNS response packet and finds that the IP address corresponding to the domain name contained in the response is included in the blacklist, the DNS proxy discards the packet, so as to prevent users from being hijacked to rogue websites by this IP address.




As shown in the figure above, enter a rogue IP address or IP range and click Add to add it to the DNS blacklist. You can click Delete on the right of an IP record to delete an IP address or IP range from the DNS blacklist.

- DNS Whitelist

The **DNS Whitelist** page allows you to configure some special resources that do not need to be controlled by the DNS proxy (including IP addresses and DNS server addresses).



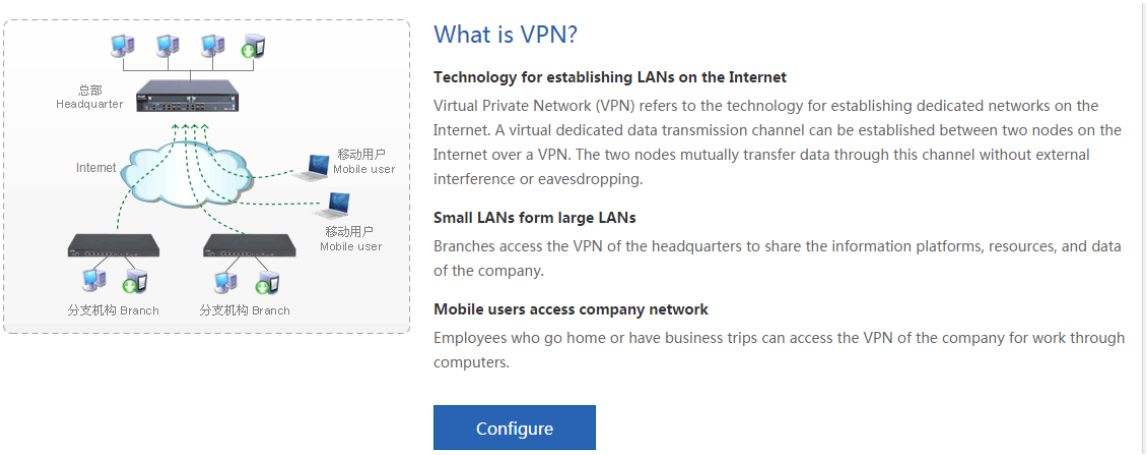

As shown in the figure above, you can select **IP/IP Range** or **DNS Server**, enter the IP address, and click Add to complete the configuration. You can click Delete on the right of a record to delete the record from the DNS whitelist.

### 1.3.14.5 VPN

Virtual Private Networks (VPNs) are not authentic physical links but virtual lines. 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.

#### 1.3.14.5.1 Config Wizard

The configuration page shown in the figure below is displayed when you configure the VPN function for the first time.

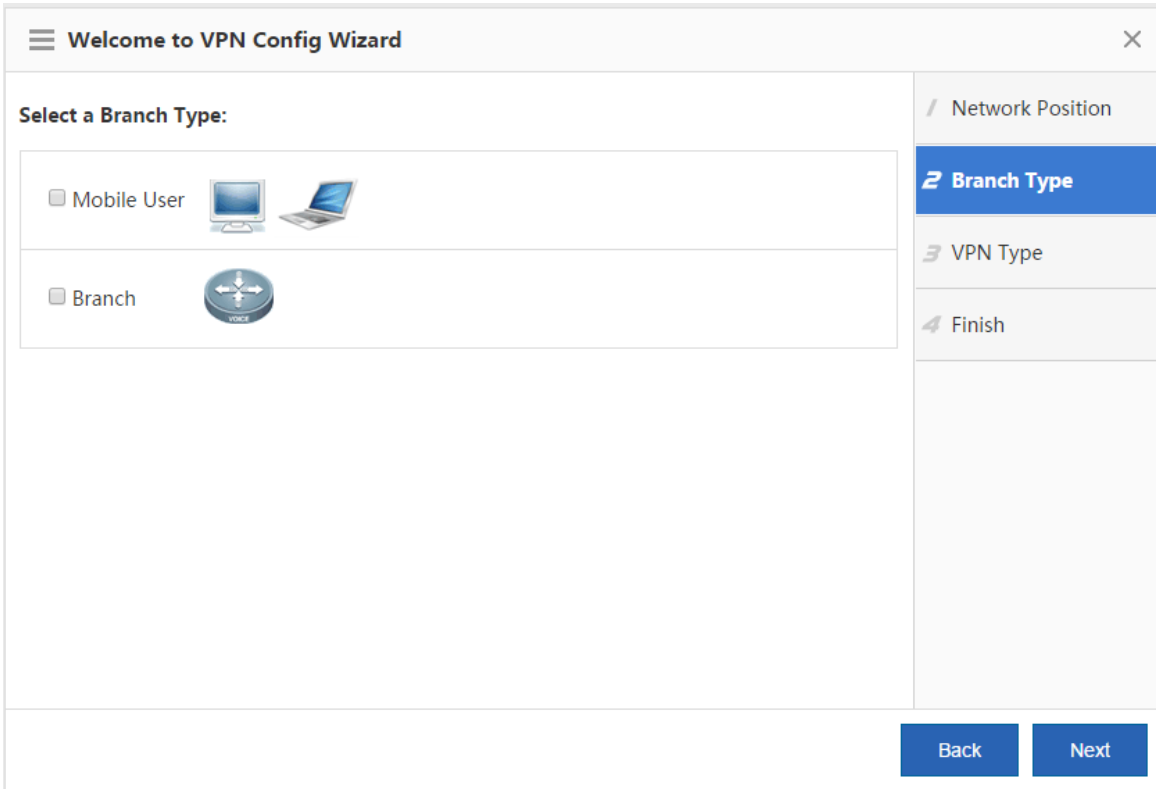



Click **Configure** to configure a VPN. A page shown in the figure below is displayed.

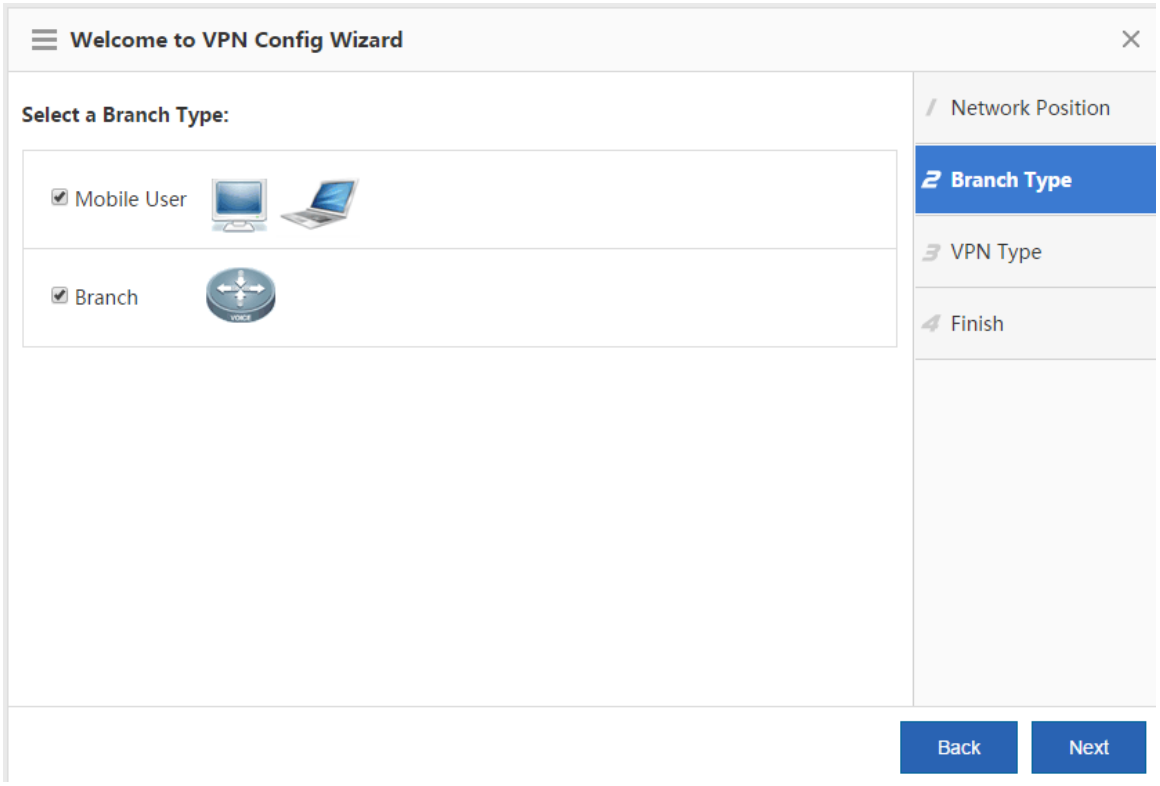
Select **Headquarter** or **Branch** based on actual conditions. The following describes the VPN configuration for both the headquarters device and branch device.

- **VPN Configuration for the headquarters device**

On the **Network Position** page, click **Headquarter**, and click Next to display the **Branch Type** page shown in the figure below.

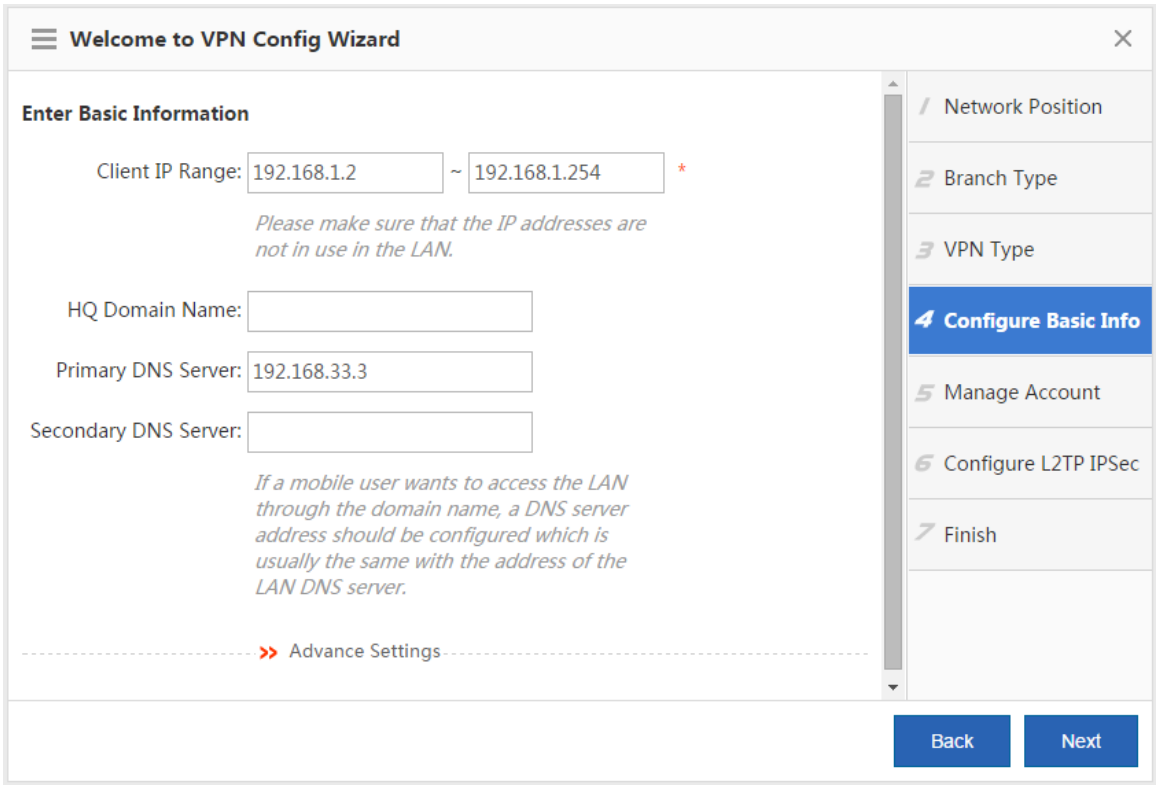



Generally, **Mobile User** is selected. If branches of a company need to be connected to the headquarters VPN, select **Branch** at the same time. Click **Next** to display the **VPN Type** page.




Select a protocol as required. Relevant configuration steps will be displayed. For example, if **PPTP** or **L2TP** is selected, the **Configure Basic Info** and **Manage Account** steps are added. Click **Next** to display the **Configure Basic Info** page, as shown in the figure below.

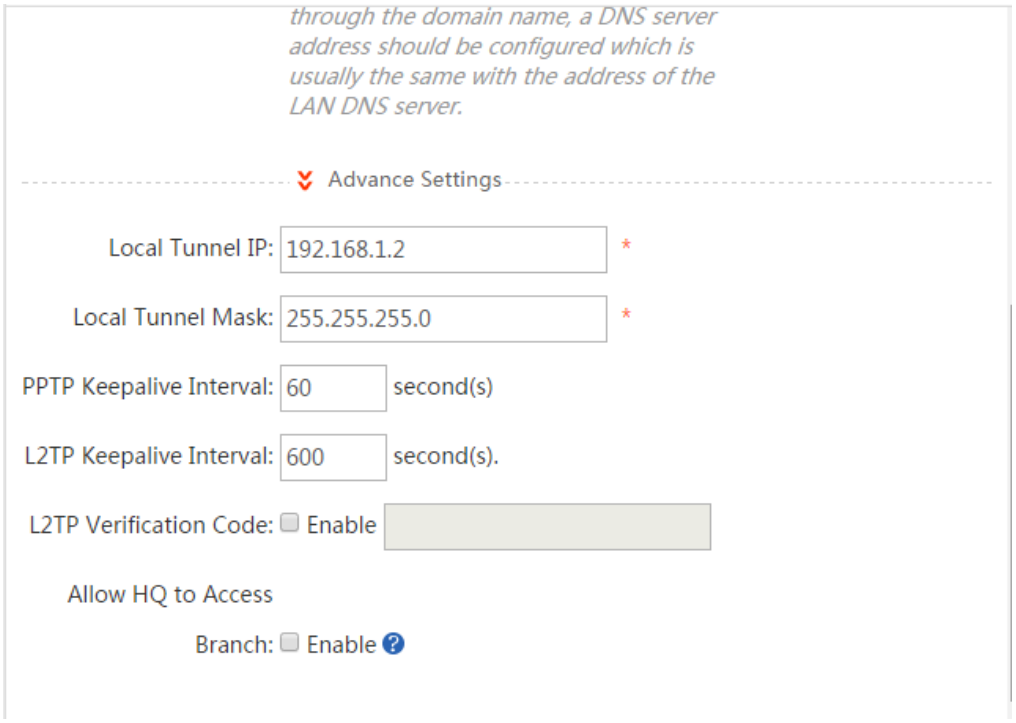
On the **Configure Basic Info** page, you can configure relevant PPTP and L2TP VPN parameters for the headquarters device.




**Client IP range**: Indicates the tunnel IP addresses allocated to VPN clients. The number of IP addresses must be equal to the number of VPN clients to be connected.

**DNS server**: If a VPN client needs to access the system in the LAN by using a domain name, the DNS server address needs to be configured. The address is generally consistent with the IP address of the DNS server used in the LAN.

Click » next to **Advance Settings**. More configuration parameters are displayed.




**Local Tunnel IP**: Indicates the tunnel IP address used by the local device when a remote client establishes a VPN tunnel with the local device over PPTP or L2TP. By default, the first IP address in the client address range is adopted.

**PPTP Keepalive Interval**: If this parameter is set, the device actively detects the tunnel status when no valid packet is received from the peer of the tunnel within the interval. The default value (60 seconds) is recommended.

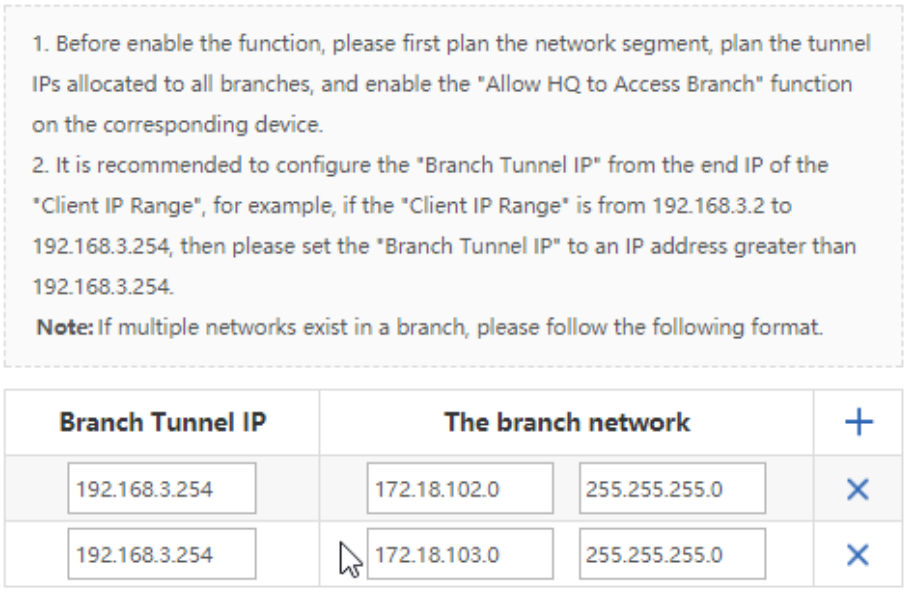
**L2TP Keepalive Interval**: Indicates the retransmission parameter for tunnel control messages. The system automatically clears a tunnel if no session is detected within the specified interval. The default value (600 seconds) is recommended.

**L2TP Verification Code**: By default, no tunnel verification is required for establishing an L2TP tunnel. If an L2TP tunnel needs to be verified, the same verification code must be configured on both sides of the L2TP tunnel.

**Allow HQ to Access Branch**: If the headquarters device needs to access the branch LANs, please configure the tunnel IP addresses for branches to access the headquarters device as well as the LAN network segment of each branch in advance.

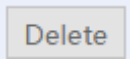
Select **Enable** in 

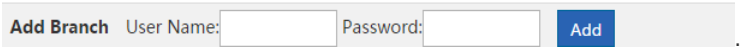
and fill in the table displayed. If you move the cursor over  , the configuration guide is displayed.



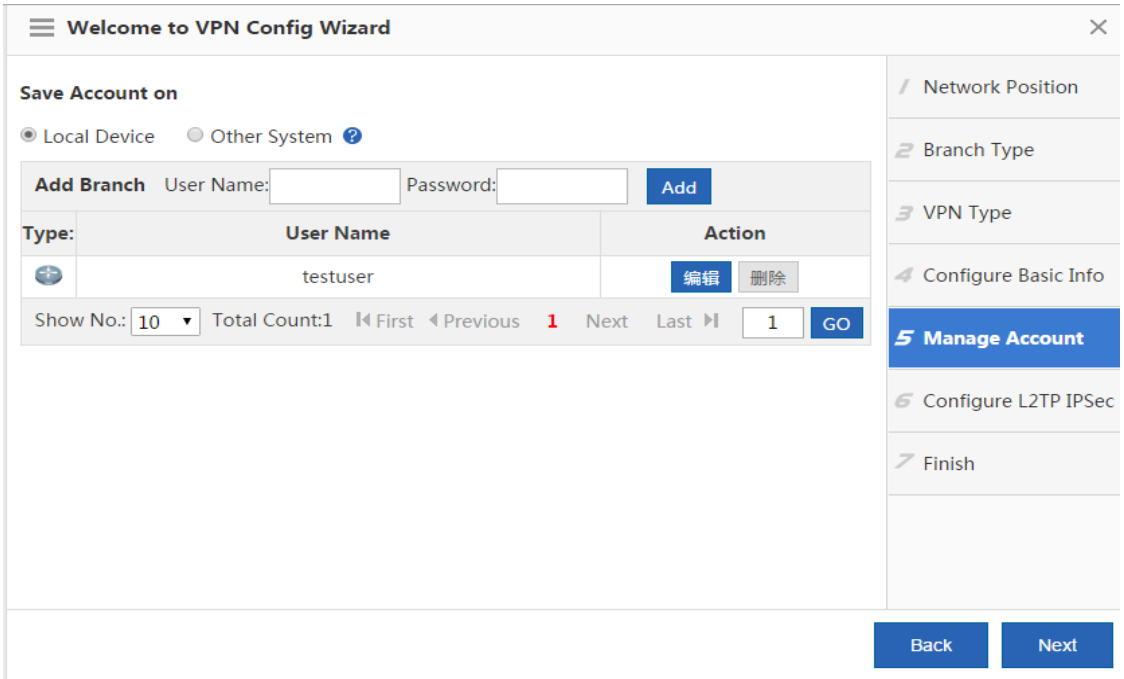

After completing basic information, click **Next**.

The figure below shows the **Manage Account** page. You can configure user information to verify the identities of clients that attempt to access the local device remotely via PPTP or L2TP. You can set **Save Account on** to **Local Device** or **Other System**. The figure below shows **Save Account on** to **Local Device**. The table in the lower part lists usernames and passwords configured on the device. You can click 

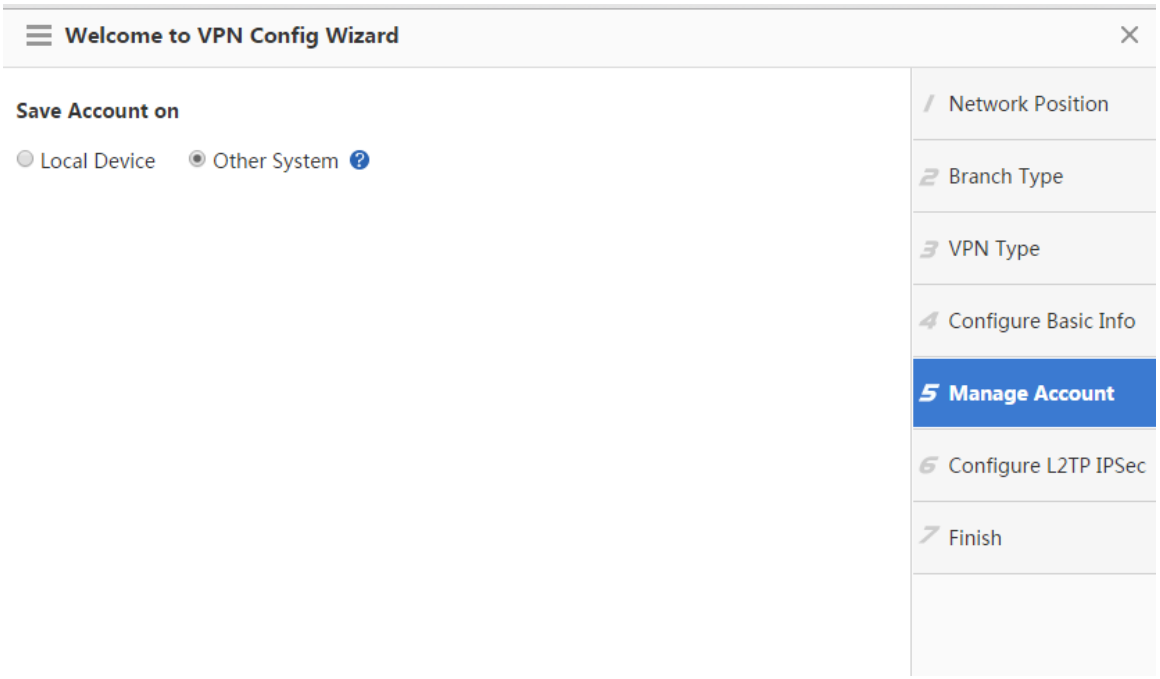
or 

to modify or delete existing usernames and passwords, or add a username and password in 

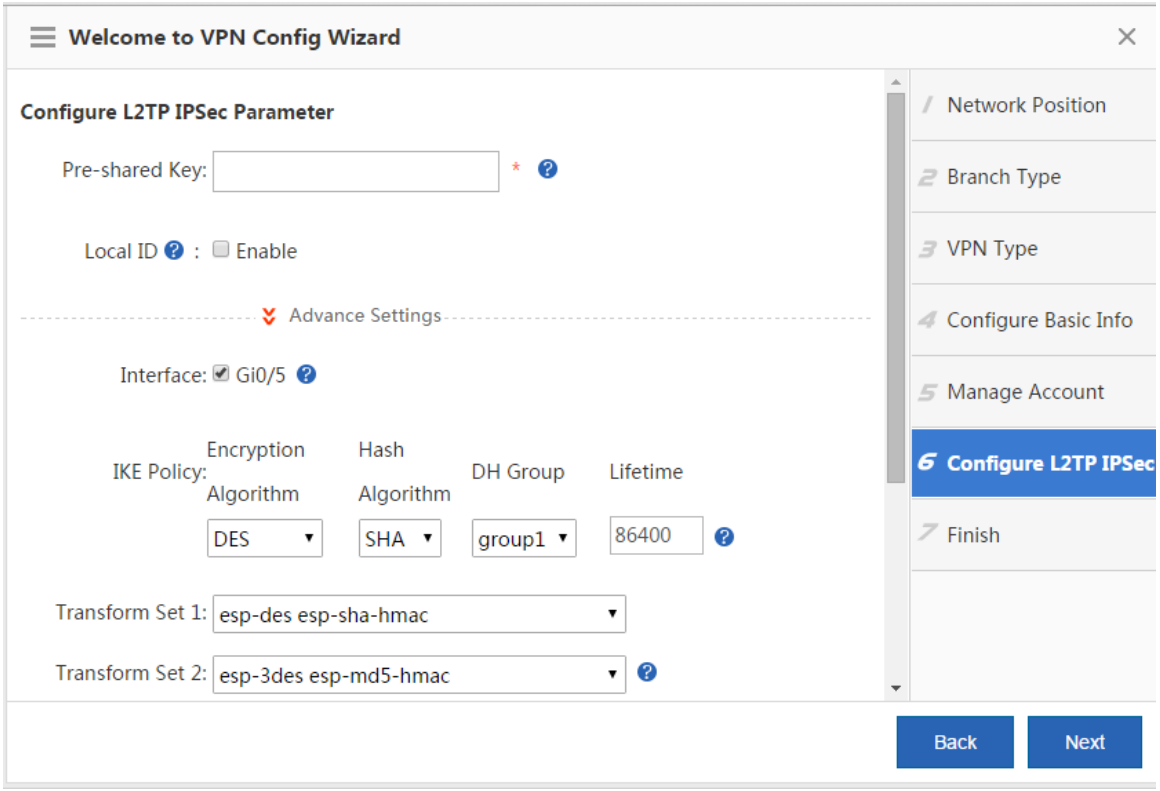
.



If you click **Other System**, as shown in the figure below, a third-party server is used to manage user information.




L2TP over IPSec is a combination of L2TP and IPSec. If you select L2TP over IPSec for the VPN headquarters device, you need to configure IPSec parameters on the configuration page shown in the figure below, in addition to L2TP parameters on the **Configure Basic Info** and **Manage Account** pages.



**Pre-shared Key**: Mobile users and branches can successfully dial in to the headquarters device only after they enter correct keys.

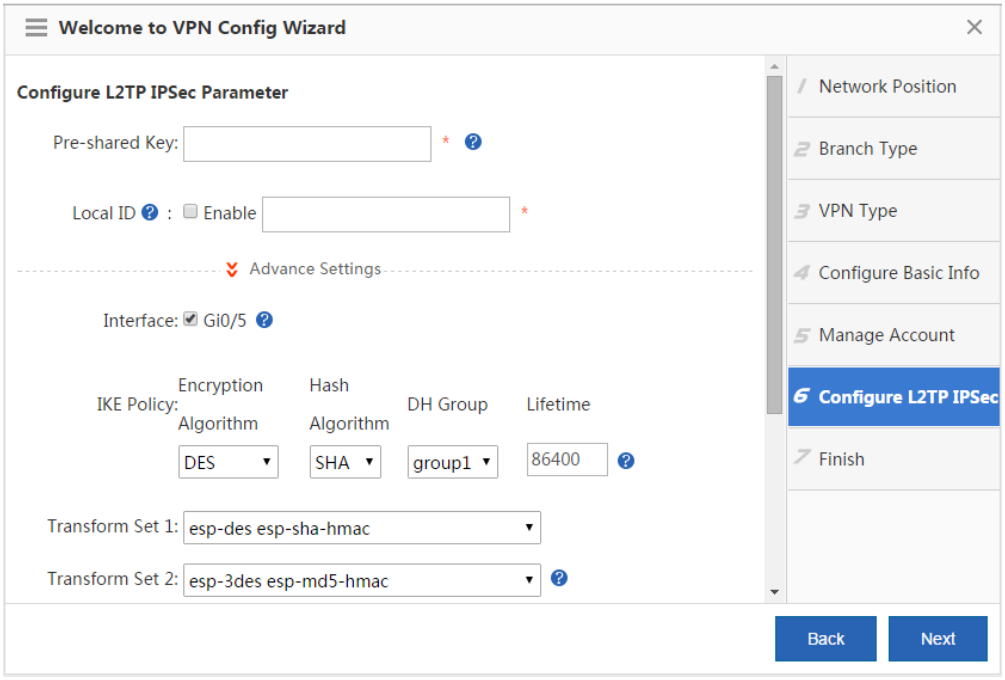
**Interface**: An encryption mapping collection needs to be configured for each interface that the IPSec communication passes through. (The encryption mapping collection links transform sets with data flows, and describes the peer address and necessary communication parameters. It comprehensively describes content required for IPSec communication with the remote peer. An IPSec security association can be established only by using encryption mapping entries.) WAN interfaces configured for the local device are listed herein and are selected by default.

**IKE Policy**: Select the parameter encryption algorithm, hash algorithm, and Diffie-Hellman group identifier used by the IKE protocol. Both parties participating in IKE negotiation have at least one consistent IKE policy, which is indispensable for successful IKE negotiation.

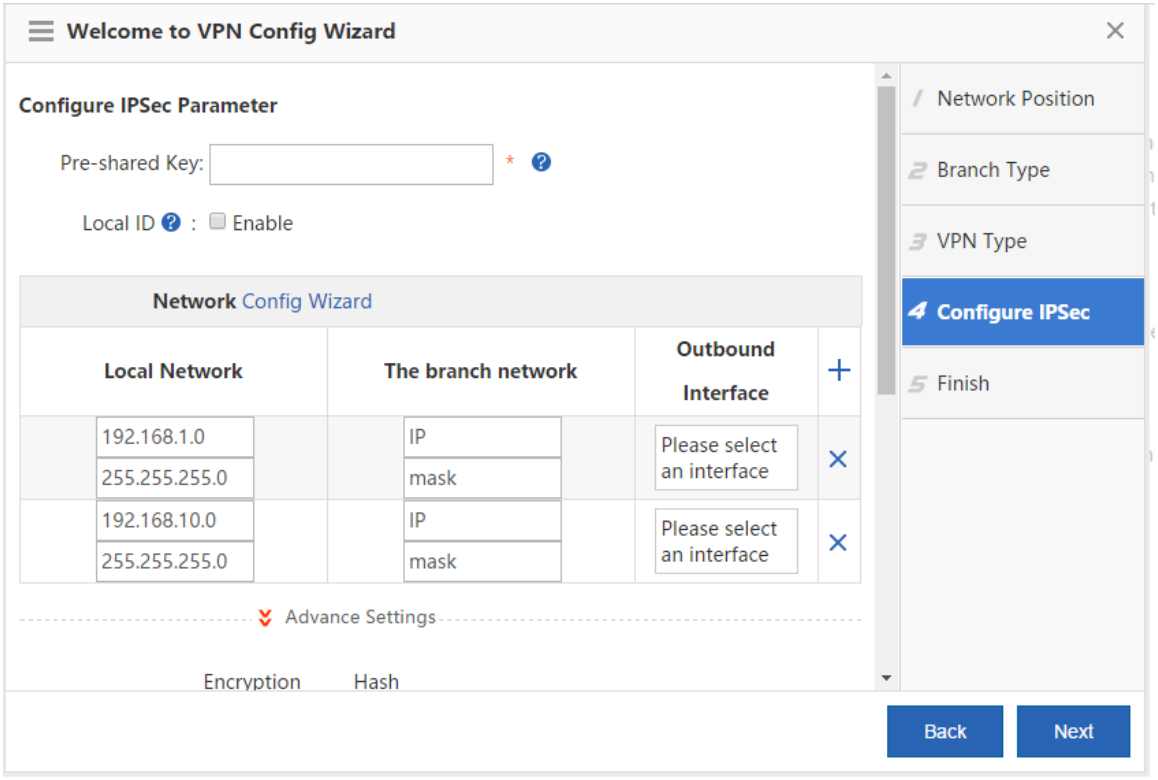
**Transform Set**: A transform set is a collection of specific security protocols and algorithms. During IPSec negotiation, peers consistently use a specific transform set to protect specific data flows.

**Lifetime**: When the existence duration of an IPSec tunnel reaches the lifecycle, both parties automatically re-negotiate to establish another tunnel, so as to effectively prevent tunnel cracking. The default value (1 hour) is recommended.

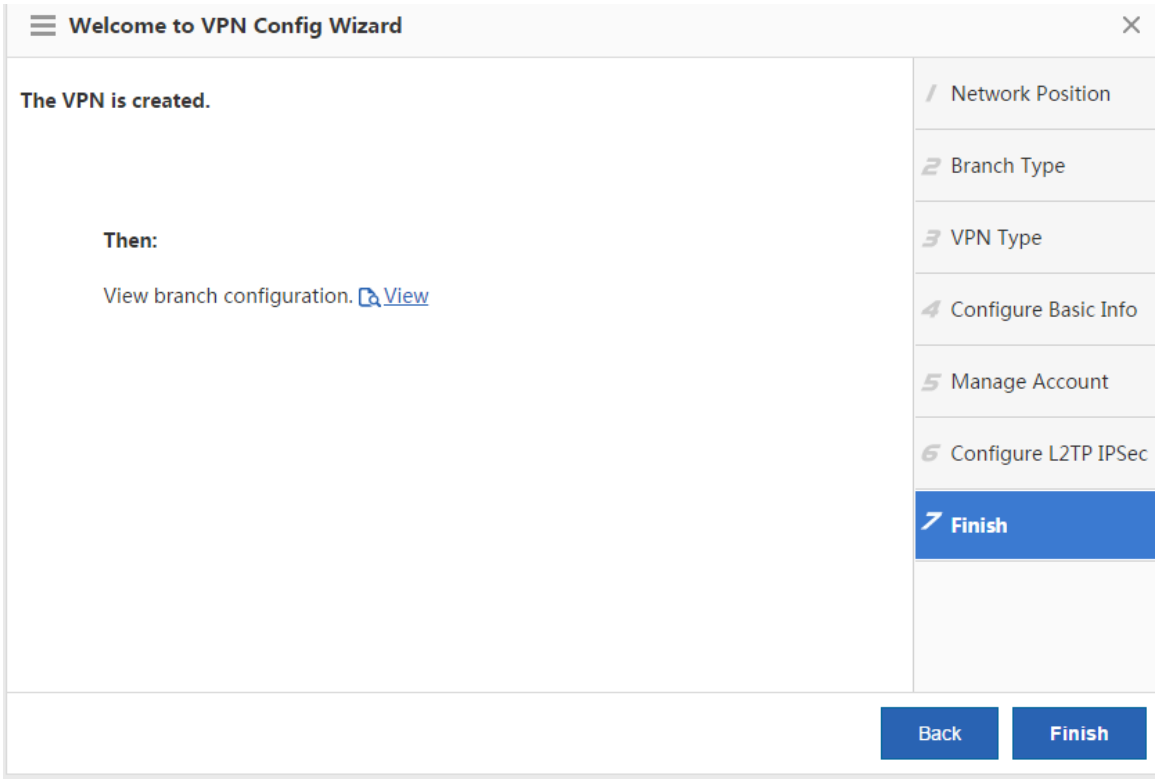
The figure below shows the configuration page of IPSEC VPN parameters for the headquarters device.



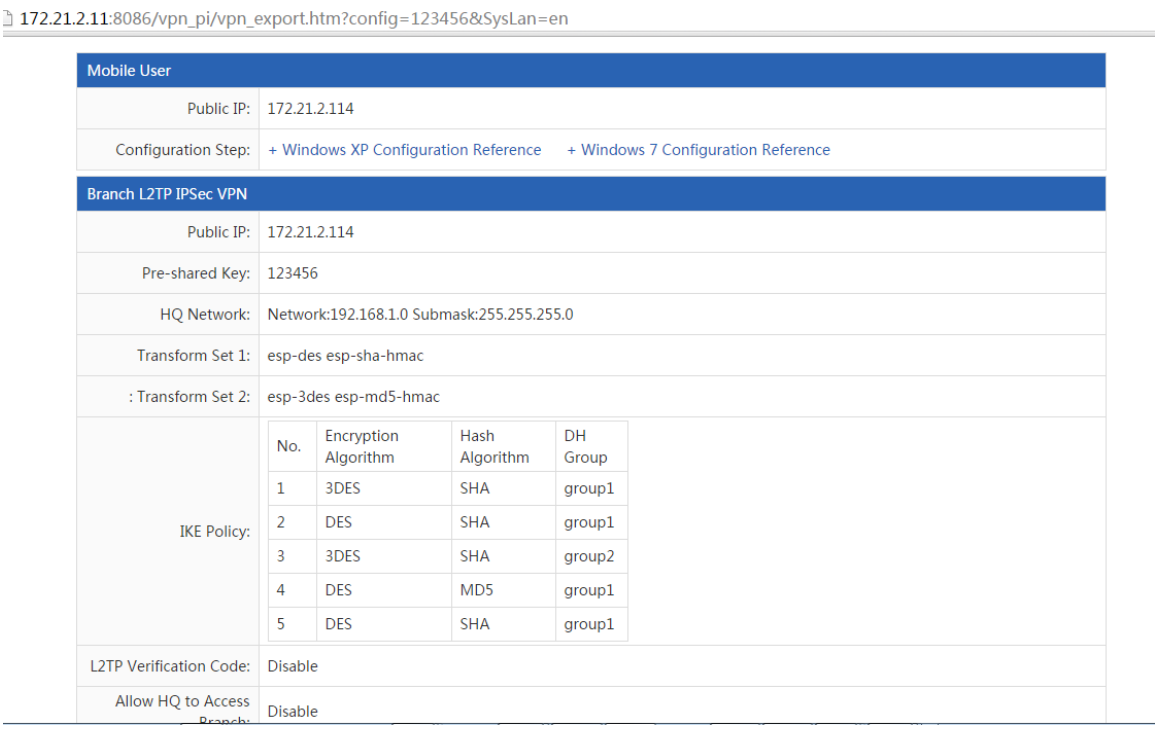

The basic parameters are almost the same as those on the L2TP over IPSec configuration page described above except that **Network Config Wizard** is added. You can configure the network segments that can be mutually accessed between the headquarters device and the branch device via encrypted IPSec tunnels.




After the VPN parameters are set, click **Next**. The **Finish** page is displayed, as shown in the figure below.

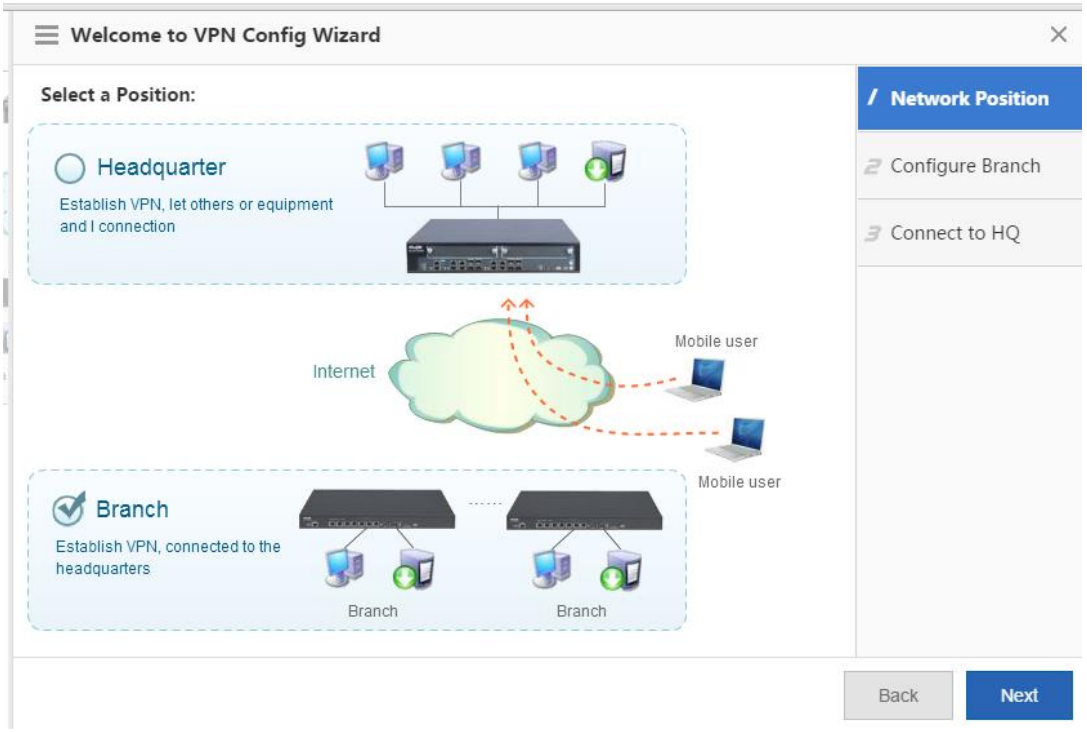


Click View to display all configurations, as shown in the figure below. Click **Finish** in the lower right corner to complete the VPN configuration for the headquarters device.



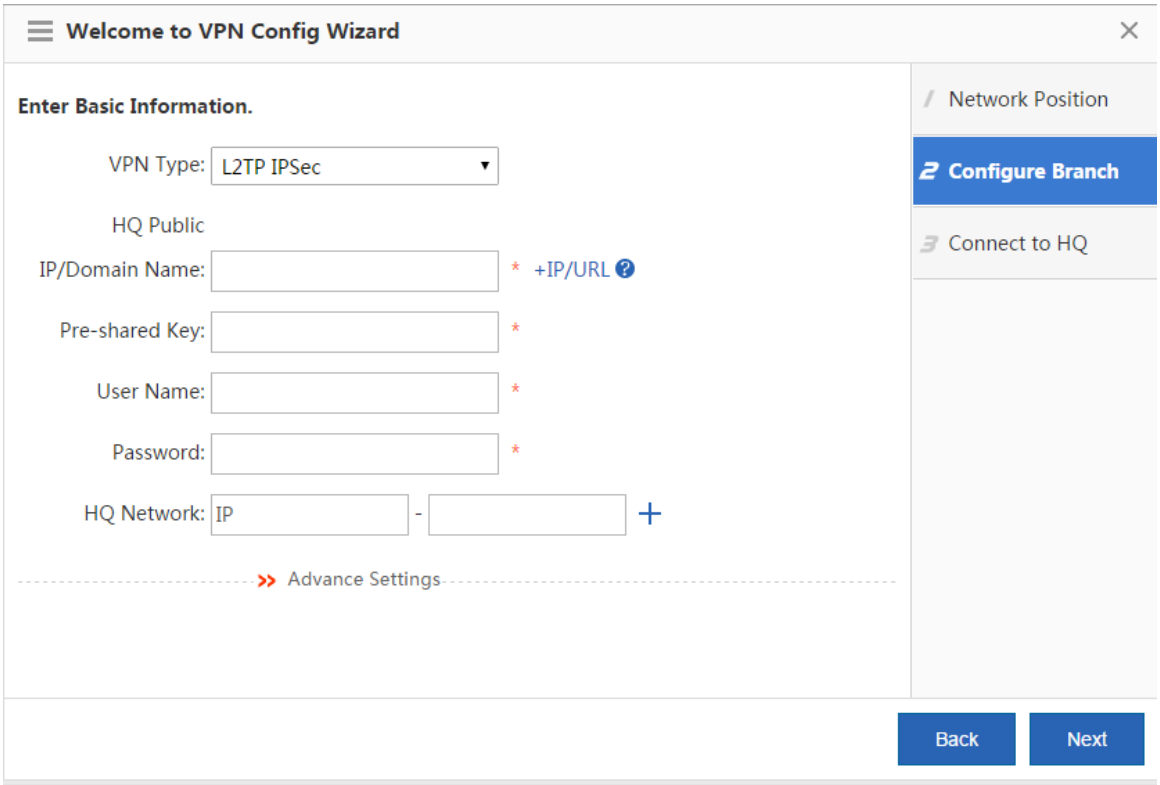

You can also click the configuration reference buttons to display reference guidance on how PCs of mobile users connect to the VPN server of the headquarters device.

- **VPN Configuration for the Branch Device**




Click **Branch** and click  to display the **Configure Branch** page, as shown in the figure below.






**VPN Type**: Select **L2TP IPSec**, **L2TP**, or **IPSec** based on actual conditions.

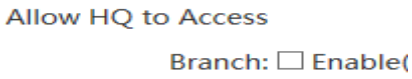
**HQ Public IP/Domain Name**: Enter the public IP address of the VPN server in the headquarters.

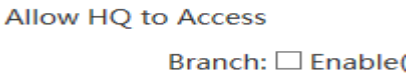
**Pre-shared Key**: The value needs to be consistent with the pre-shared key of the VPN server in the headquarters. You can request the pre-shared key from the VPN server administrator in the headquarters.

**User Name** and **Password**: Enter the username and password for logging in to the VPN.

**HQ Network**: Configure the LAN network segment for the headquarters device to be accessed.

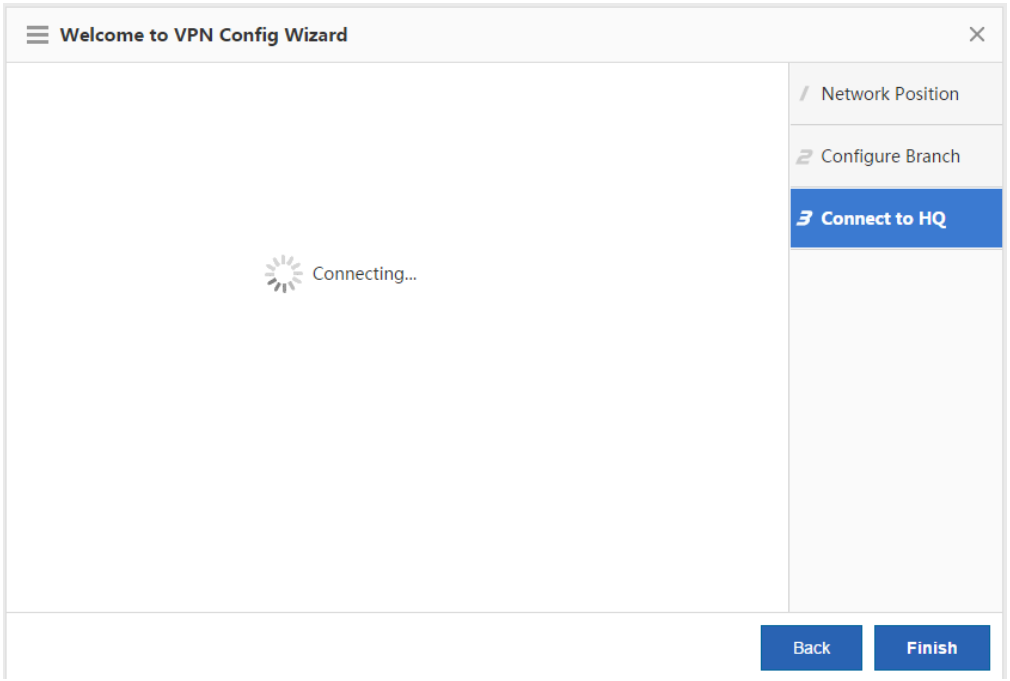
**Local ID**: It needs to be configured when **IPSec** or **L2TP IPSec** is selected. After the local ID display is enabled, the headquarters device can obtain the branch name.

**Advanced Settings**: The advanced settings include the IKE policy, transform set, and whether to allow the headquarters device to access branch LANs. They need to be consistent with VPN settings on the headquarters device. It should be especially noted that, if 

is selected, when a branch device accesses the WAN, the traffic goes through the VPN and then is transmitted to the headquarters device to access the WAN; if 

is deselected, only the traffic destined for the LAN network segment of the headquarters device is transmitted through the VPN and other traffic is directly transmitted to the WAN through the network egress of the branch device.

Click **Next** to display the **Connect to HQ** configuration page, as shown in the figure below.

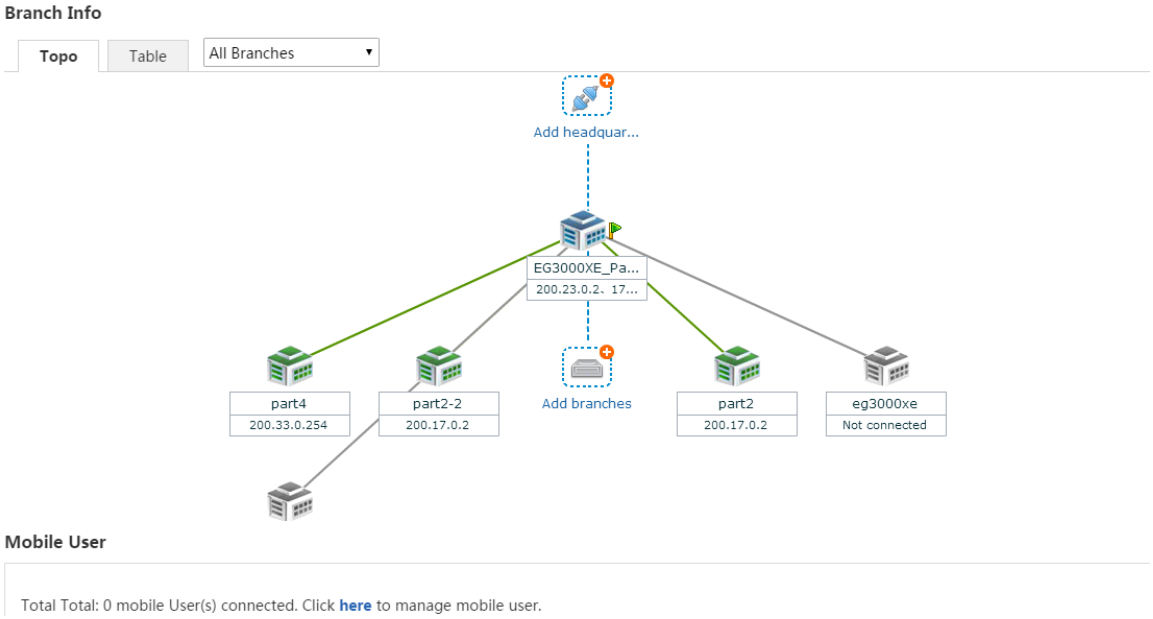



The message "Connecting..." is displayed, indicating that the branch device is connecting to the VPN network of the headquarters device. A connection success or failure prompt is displayed after a period of time. After a connection success prompt is displayed, click **Finish** in the lower right corner to complete the VPN configuration of the branch device.

## 1.3.14.5.2 VPN

- **Topo Page**

After the VPN configuration is completed, the configuration page shown in the figure below is displayed.




You can view the position of the current device in the VPN environment from the topology. The device marked with "EG3000XE xxx" is the device you are configuring, just as 

shown in the figure above. You can click this icon to view or modify the VPN configuration of the current device. The lines and devices in gray in the topology indicate connection failures while lines and devices in green and devices in blue indicate connection success.

When the current device serves as a VPN branch device, it connects to the headquarters device above. Click 

to set the current device as a VPN branch device and connect it to other devices. You can click this icon multiple times to connect the current device to multiple VPN headquarters devices. The current device can be connected to a maximum of nine VPN headquarters devices. For detailed configuration steps, see 1.3.8.5.1 "Config Wizard."

When the current device serves as a VPN headquarters device, it connects to the device below. If the current device serves as the L2TP or L2TP IPSec VPN headquarters device, 

is displayed. Click this icon to add an account.

If the current device serves only as a VPN branch device, as shown in the figure below, you can click 

to configure this device as the VPN headquarters device. For configuration steps, see 1.3.8.5.1 "Config Wizard."

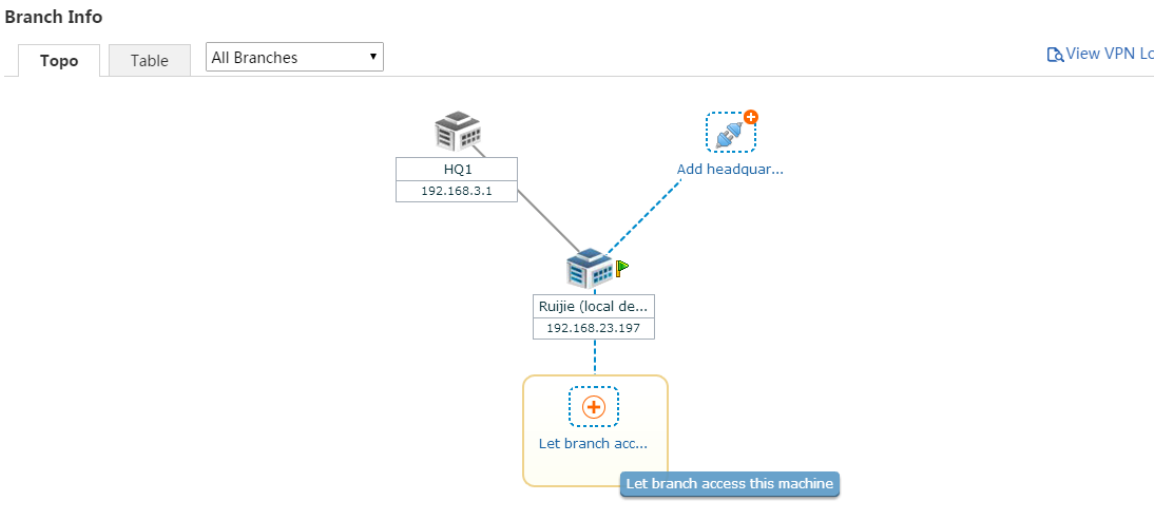
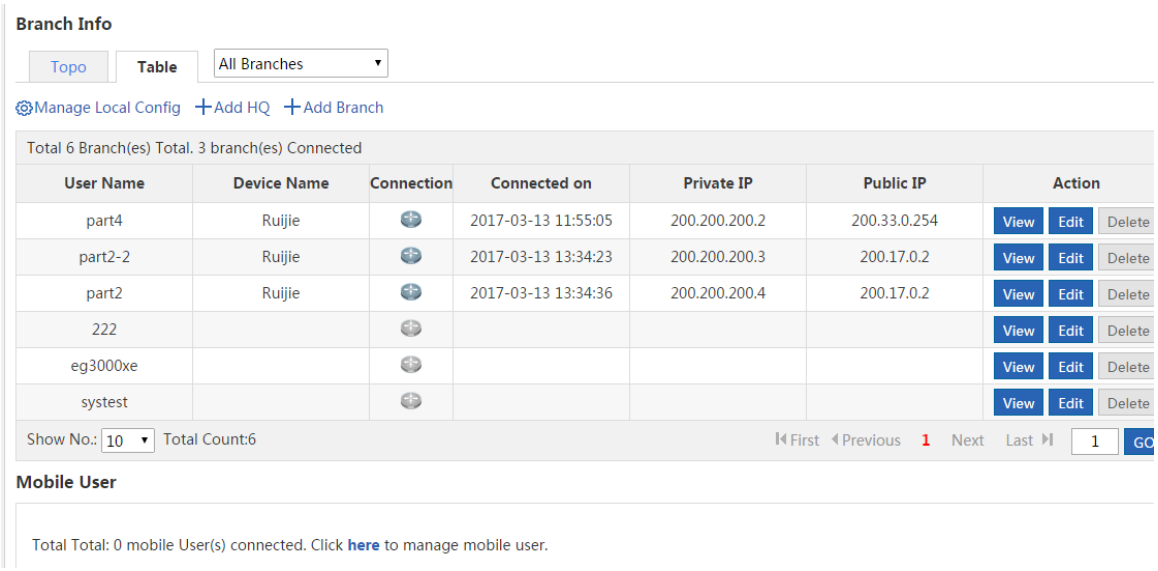



Table Page

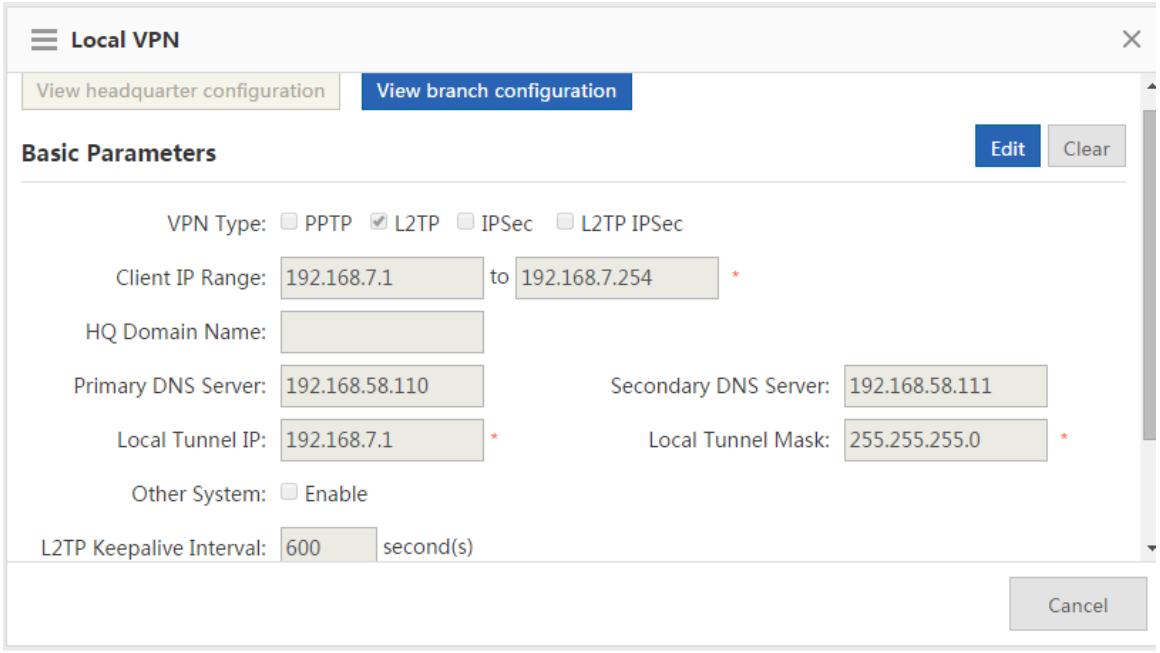



As shown in the figure above, the first one provides information about the connected headquarters device with the current device serving as a VPN branch device; the second one provides information about the connected branch device with the current device serving as a VPN headquarters device.

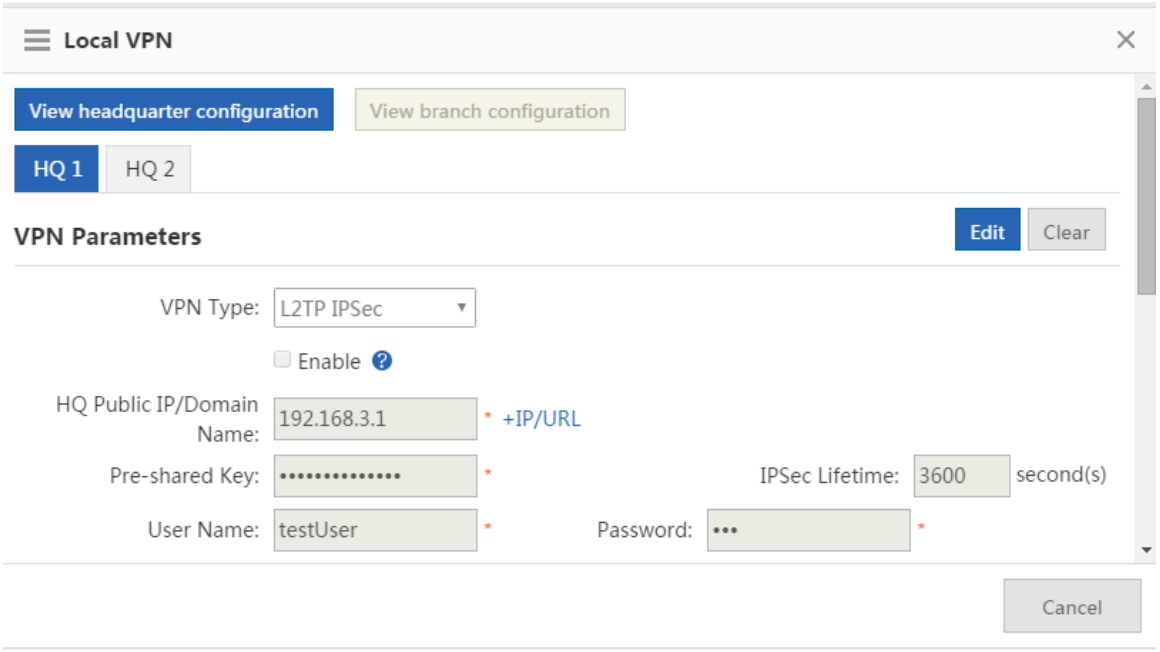
Click Manage Local Config to view or modify the VPN configuration of the current device. Click Add HQ to configure the current device as a VPN branch device and connect it to multiple headquarters devices. Click Add Branch to add user information. Click View Edit Delete in the **Action** column of the table to view, edit, or delete selected users.

- **Viewing headquarter configuration/branch configuration**

You can click the icon of the current device on the **Topo** page or click **Manage Local Config** on the **Table** page to display the VPN configuration of the current device, as shown in the figure below.

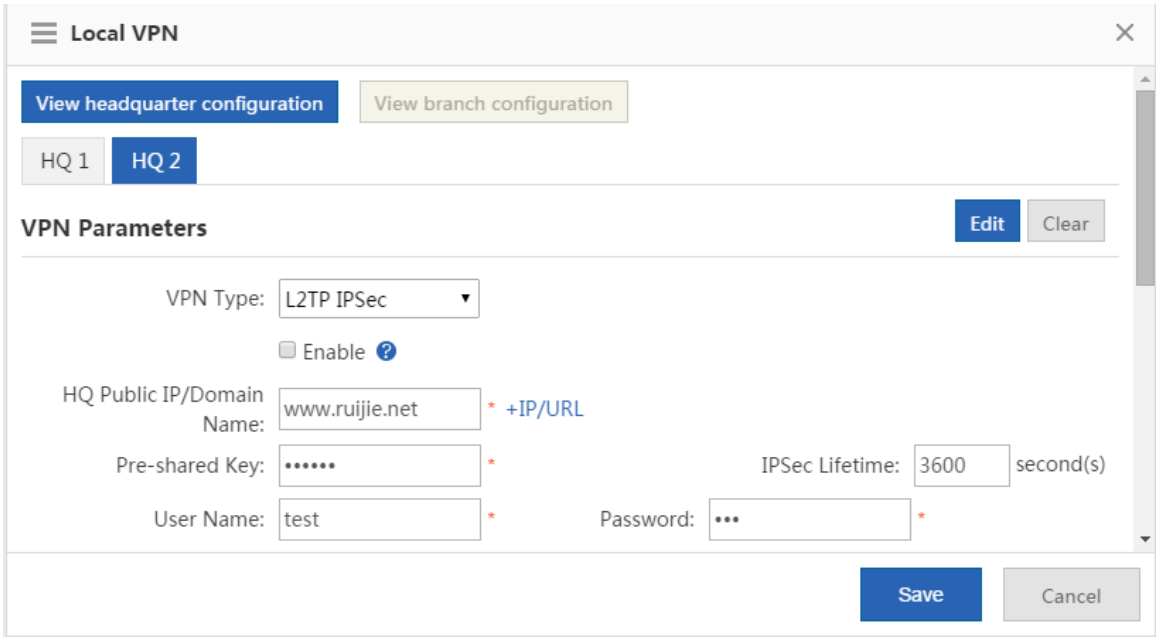



When View headquarter configuration is gray, the configuration of the current device that serves as a VPN headquarters device is displayed. Click View branch configuration to switch to the configuration page of the current device that serves as a VPN branch device, as shown in the figure below.



If the current device serves as a VPN branch device and connects to multiple headquarters devices, multiple options are displayed. For example, HQ 1 HQ 2 indicates that the VPN configuration of the current device connected to Headquarters 1 is displayed. Click HQ 2. The VPN configuration of the current device connected to Headquarters 2 is displayed.

Click Edit to edit the configuration of the selected VPN, as shown in the figure below.

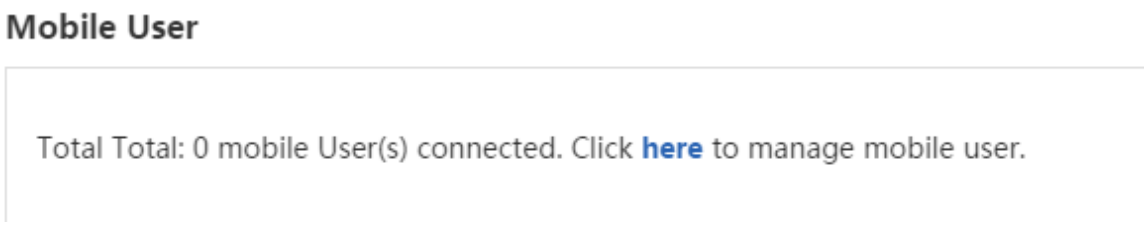



After the editing is completed, click Save.

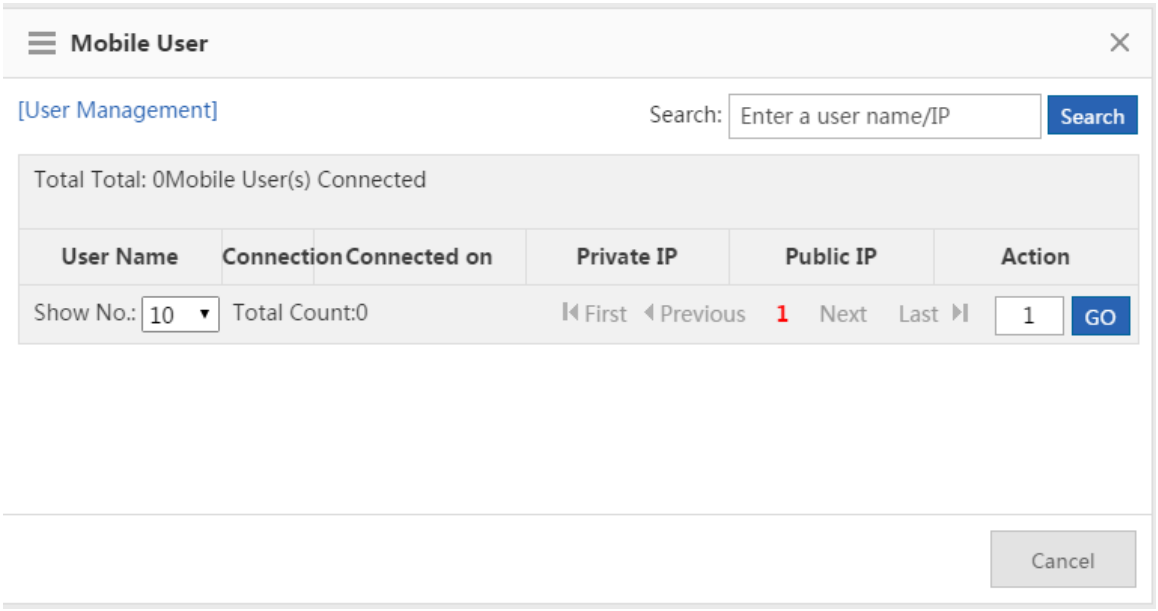
Click Clear to clear the configuration of the selected VPN. If the current device connects to the device of Headquarters 2, it will be disconnected from the device of Headquarters 2 after you click **Clear**.

- **Mobile User**

When the current device is configured as a VPN headquarters device, the configuration of mobile users is displayed on the VPN monitoring page, as shown in the figure below.



Click here. The mobile user management page shown in the figure below is displayed. You can view, modify, or delete a mobile user or click [User Management] to manage mobile users on this page.

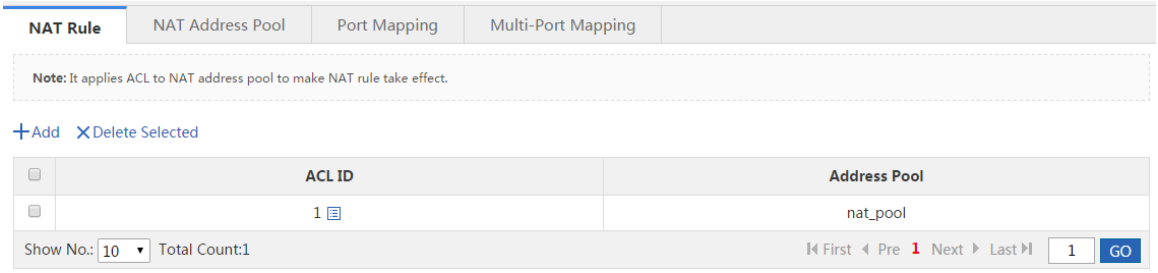



### 1.3.14.6 NAT/Port Mapping

The Network Address Translation (NAT) is a technology of translating internal private network addresses (IP addresses) into valid public IP addresses. NAT allows presenting an institution with one public IP address on the Internet.

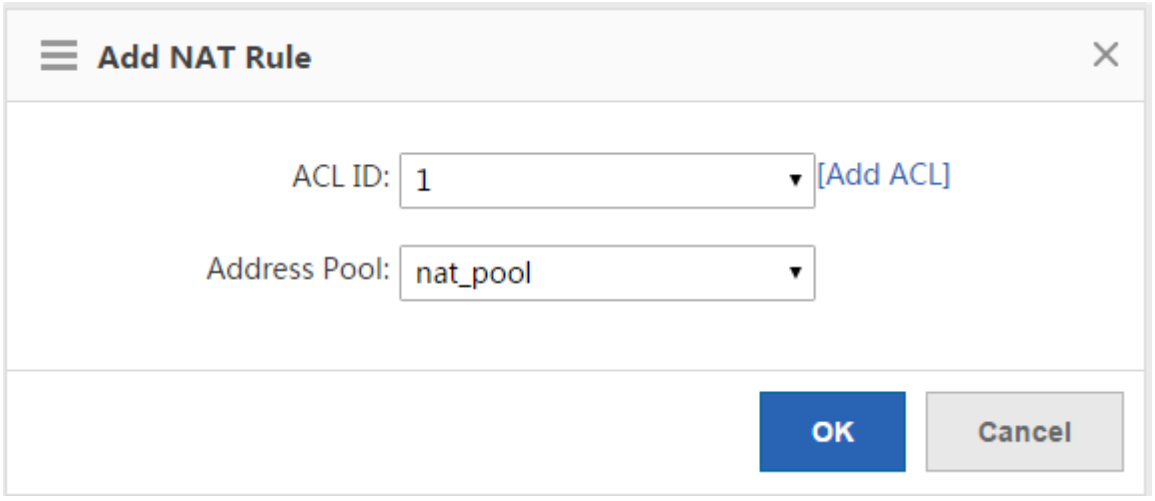
#### 1.3.14.6.1 NAT Rule

The NAT rule function is to apply an ACL to an NAT address pool. Only addresses that match this ACL will be translated.




**ACL ID**: Select the ID or name of the ACL to be applied to the NAT rule.

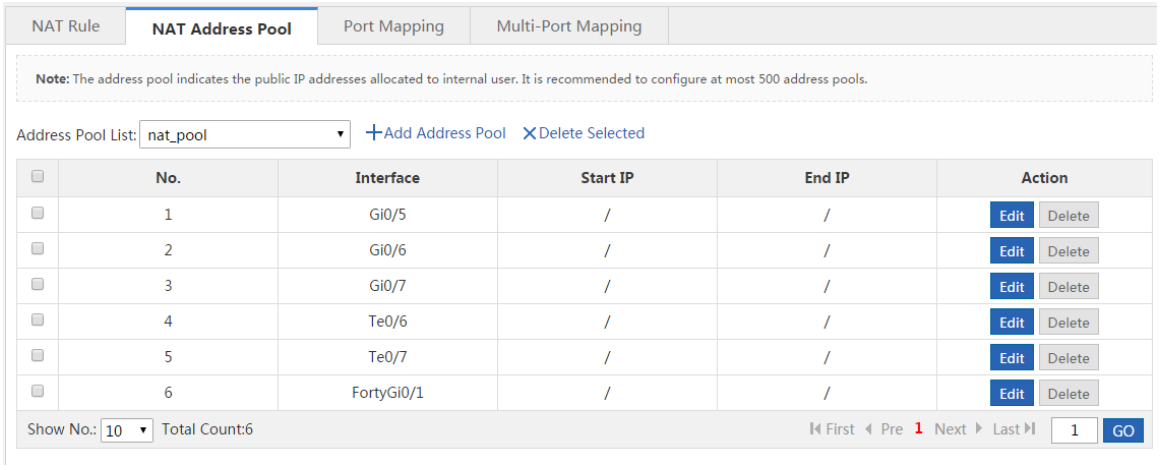
**Address Pool**: Select the address pool, to which the ACL is to be applied.




Click **OK** to add an NAT rule.

### 1.3.14.6.2 NAT Address Pool

Dynamic NAT enables device to automatically translate the unregistered IP addresses from an address pool to registered IP addresses. It is recommended to configure at most 500 address pools.




Click **Add Address Pool**. In the **Add Address Pool** dialog box, set parameters, as shown in the figure below.


**Address Pool Name**: Indicates the name of an address pool. If you need to add an address to an existing address pool, click


and select the existing address pool from the drop-down list.

**WAN Port**: Select the WAN ports to be added. Information shown in the figure below is displayed after a WAN port is selected.


Enter the start IP address and end IP address. If only one IP address is available, keep the end IP address be consistent with the start IP address. You can configure multiple IP ranges for one address pool and the IP ranges cannot be overlapped.

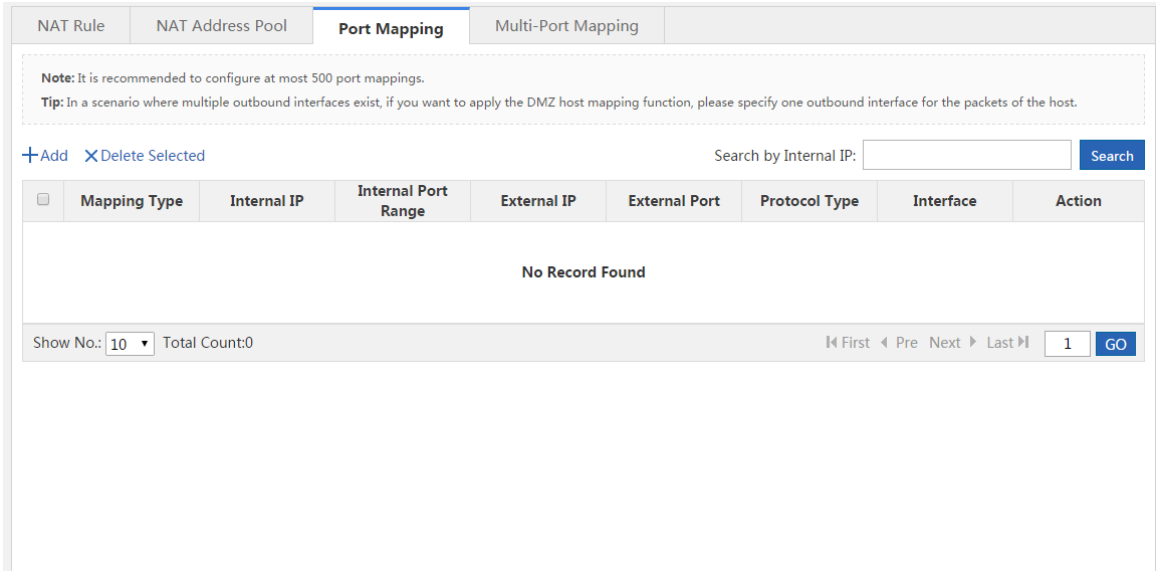
After the configuration, click 

.

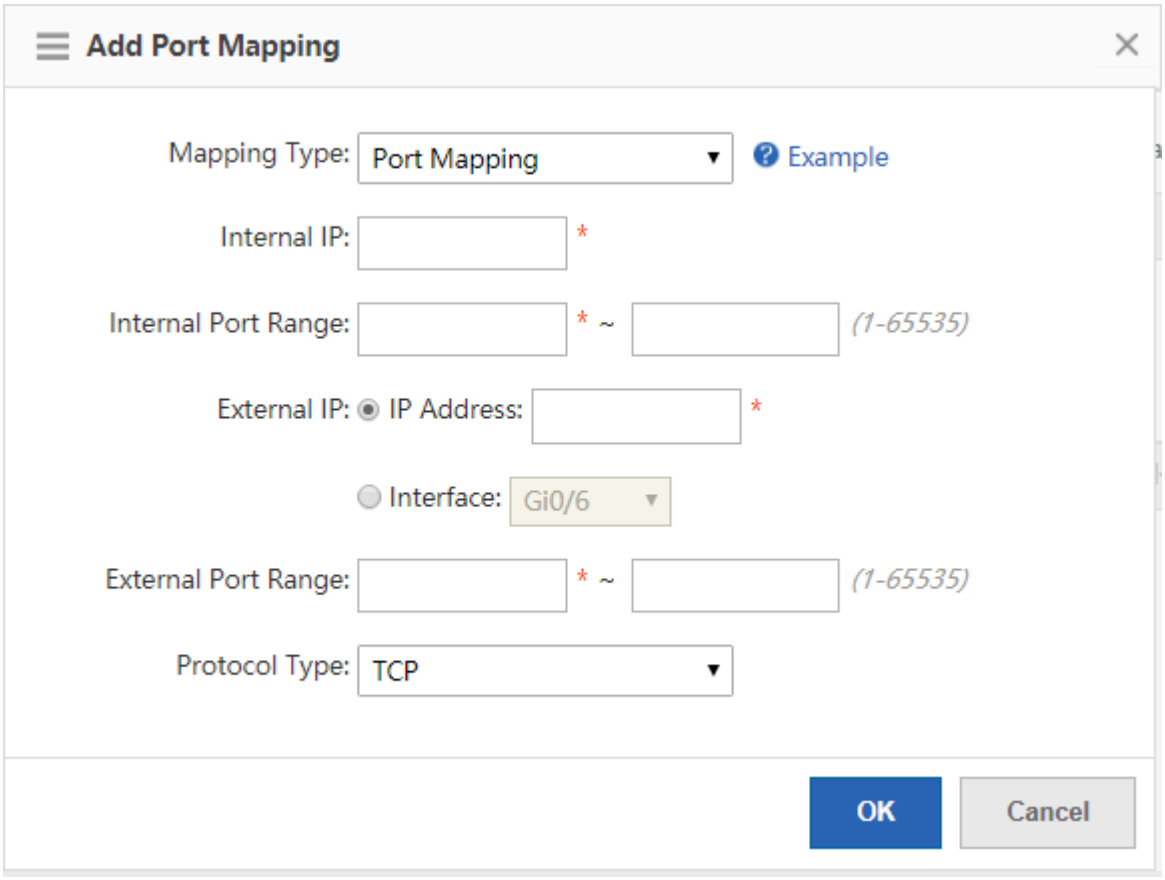
### 1.3.14.6.3 Port Mapping

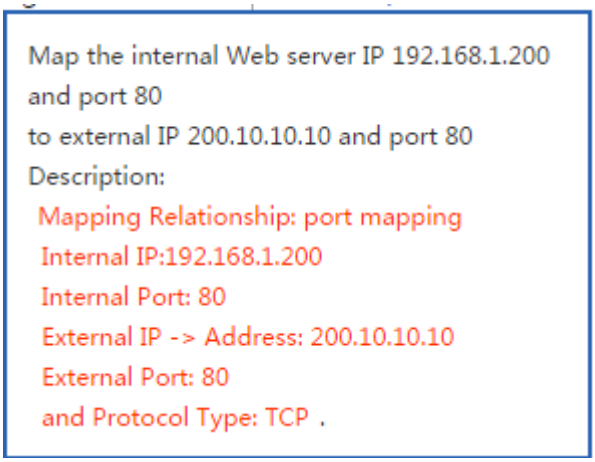
Port mapping includes port mapping and device mapping (DMZ host).

Port mapping is shown in the figure below.




Click **Add**. In the **Add Port Mapping** dialog box shown in the figure below, configure port mapping.






**Internal IP Range**: Indicates the LAN IP address to be mapped to the WAN, and is usually the IP address of your server.

**Internal Port Range**: Indicates the port to be mapped to the WAN.

**External IP**: Indicates the IP address of the WAN. If you click **Interface**, all the IP addresses configured for the WAN interface will be mapped.

**External Port Range**: Indicates a port on the WAN. The value ranges from **1** to **65,535**.

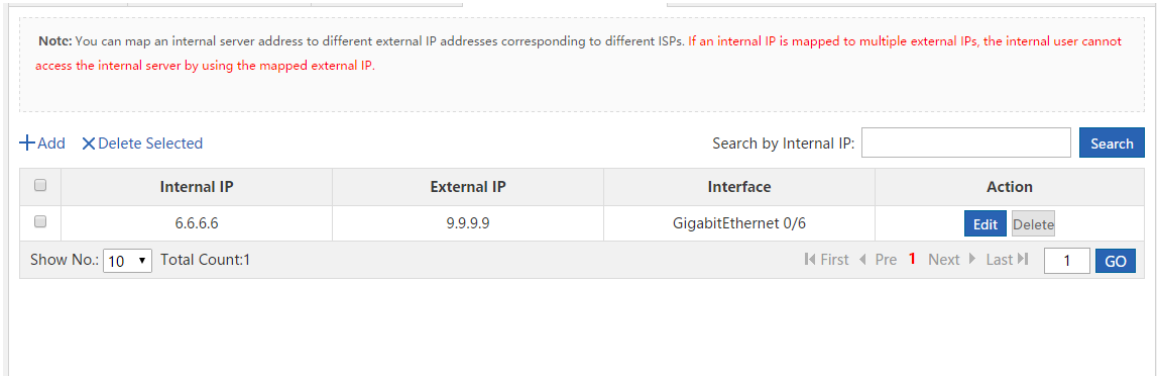
**Protocol Type**: Select **TCP** or **UDP** as required.

After the setting, click OK.

### 1.3.14.6.4 Multi-Port Mapping

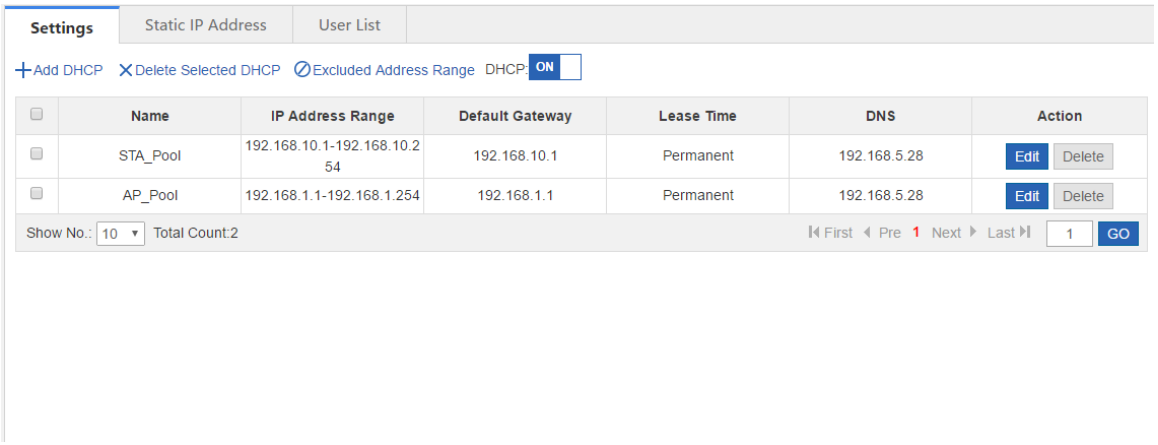
Multi-port mapping is configured to access a single LAN server via multiple ISP addresses.

For example, the LAN server with the IP address 1.1.1.1 needs to be accessed via 2.2.2.2 on the outbound interface Gi0/5 of the China Telecom network, via 3.3.3.3 on the outbound interface Gi0/6 of the China Unicom network, and via 4.4.4.4 on the outbound interface Gi0/7 of the China Mobile network.

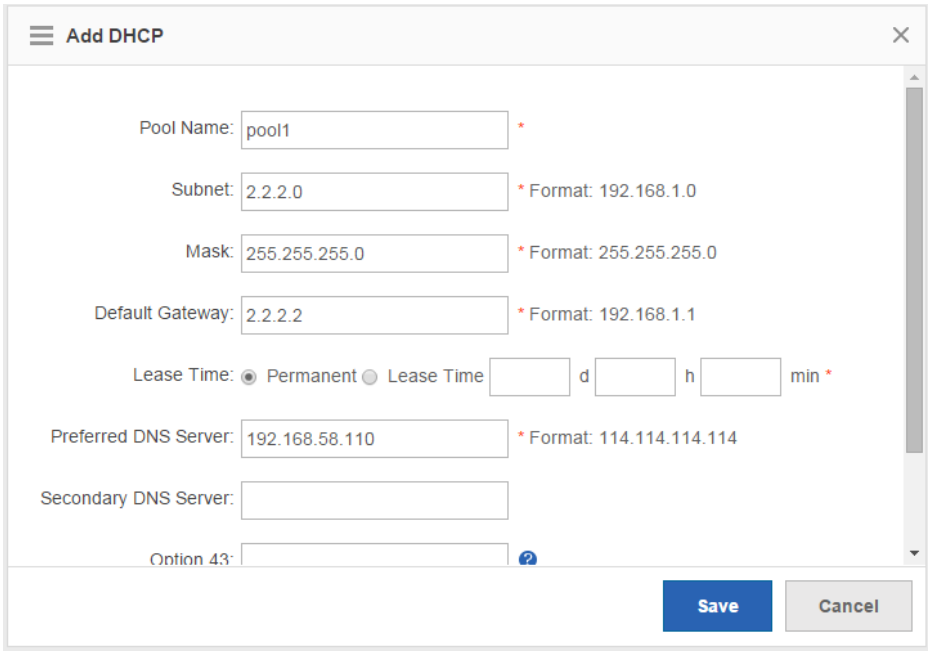


## 1.3.14.7 DHCP

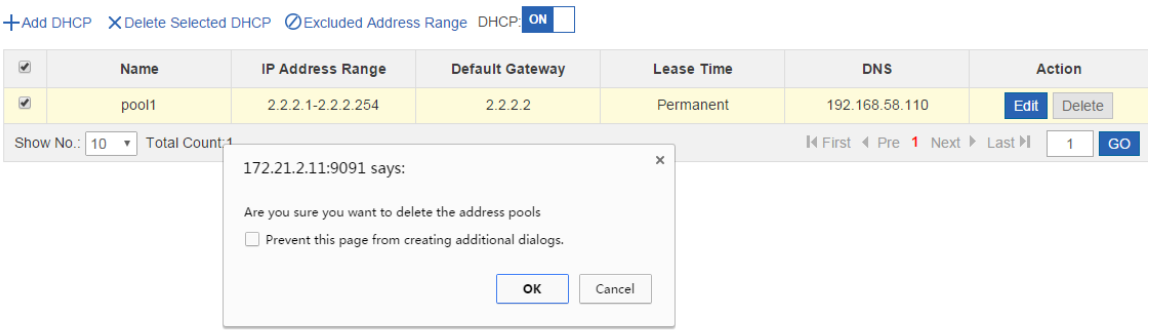
### 1.3.14.7.1 Server Settings



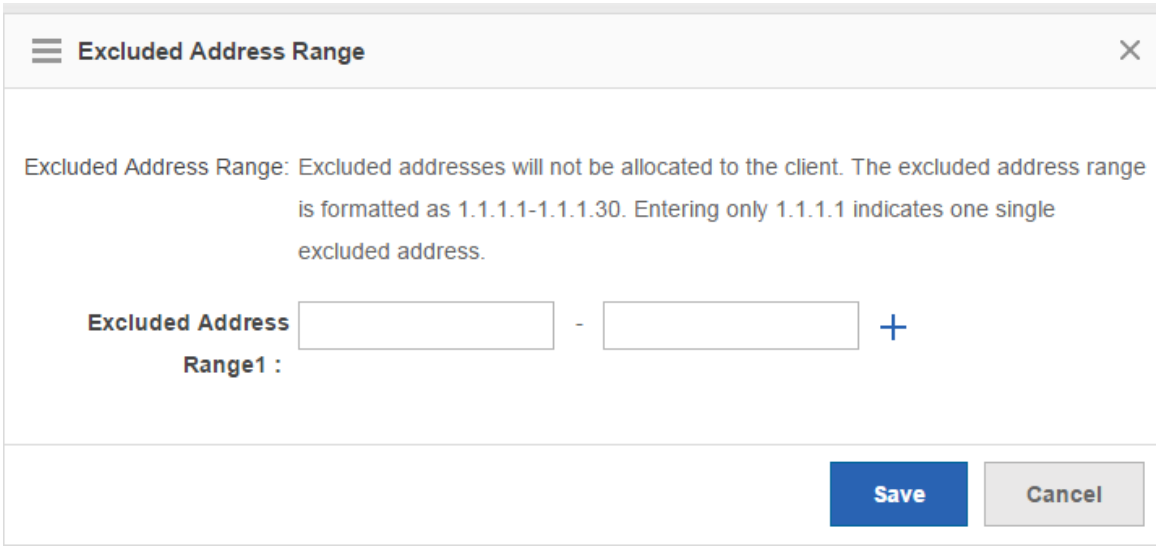

- Add DHCP




- Delete Selected DHCP



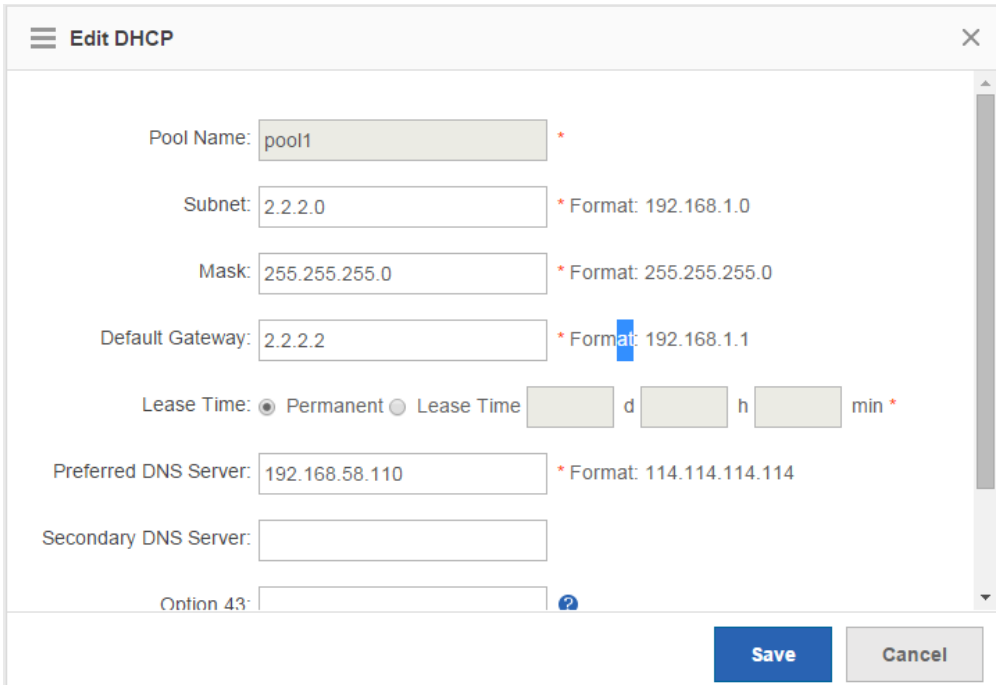

- Excluded Address Range




**Excluded Address Range**: You can configure multiple excluded IP ranges. IP addresses in these ranges are not allocated to users.

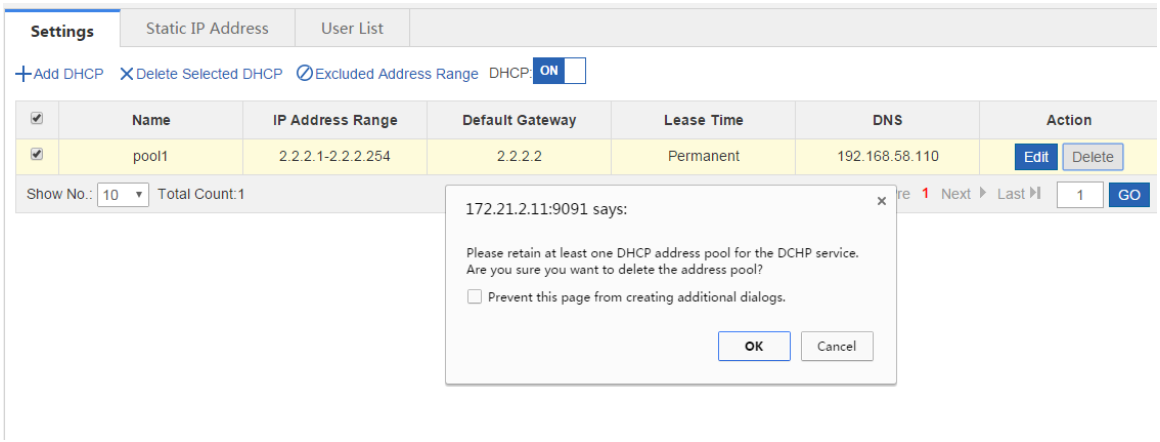
- DHCP


- Edit DHCP



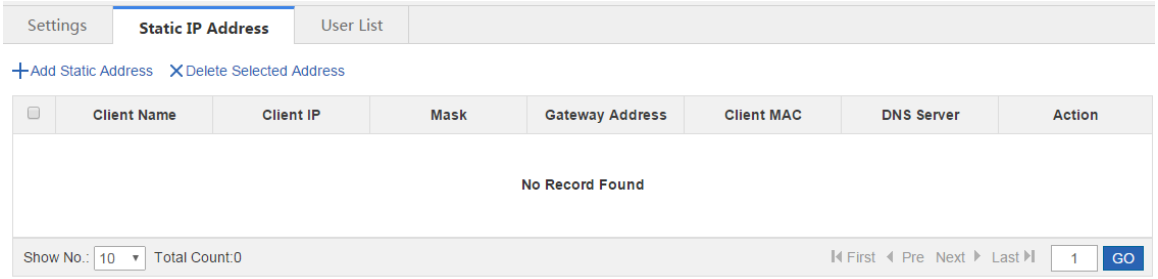

In the DHCP list, click **Edit**. In the dialog box displayed, edit the DHCP address pool.

- Deleting a DHCP address pool

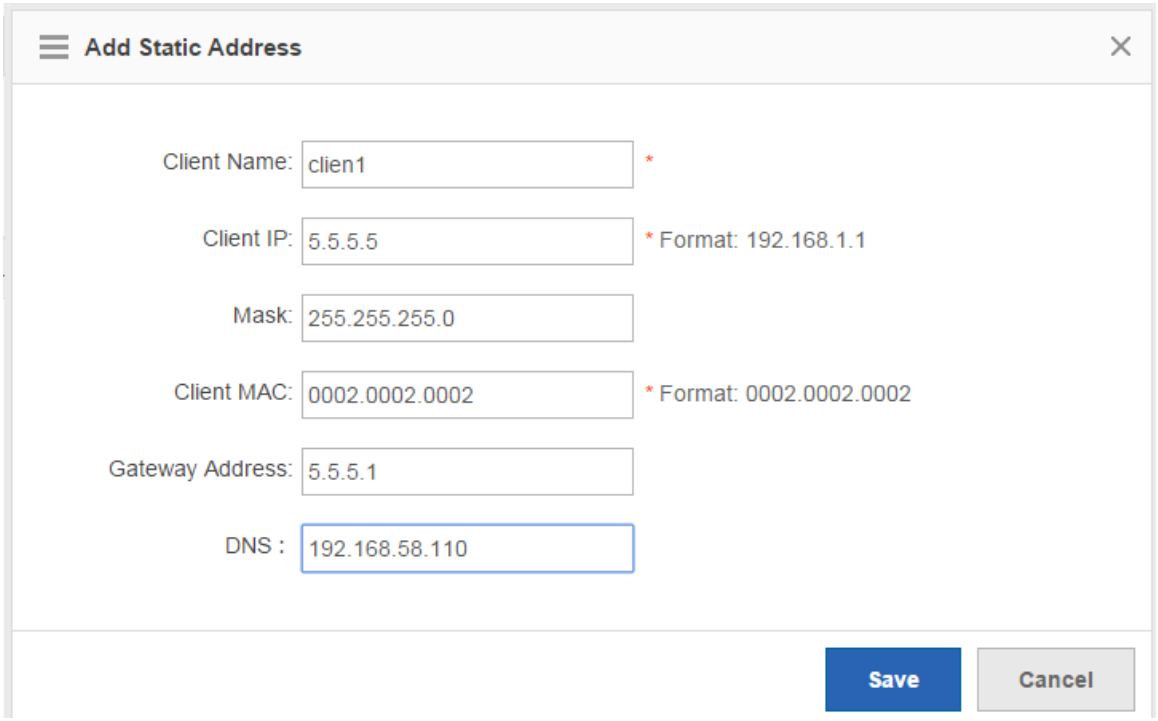



In the DHCP list, click **Delete**. In the confirmation dialog box displayed, click **OK** to delete the DHCP address pool.

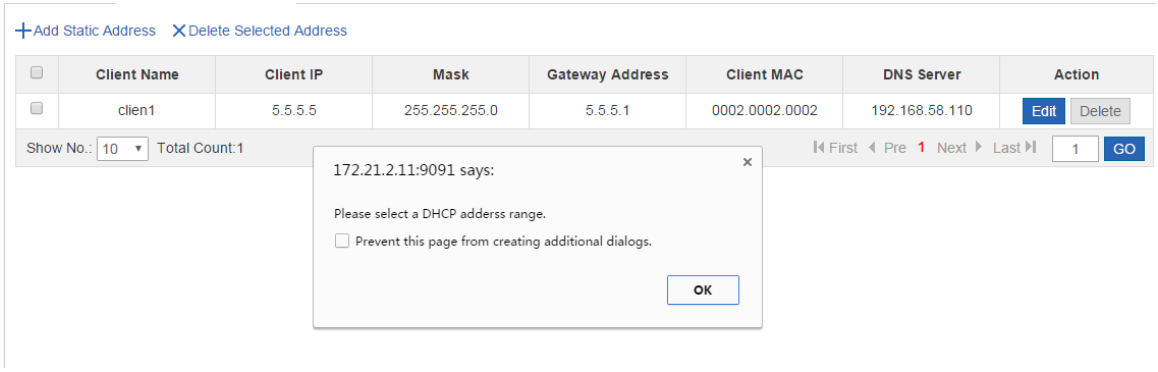
### 1.3.14.7.2 Static IP Address



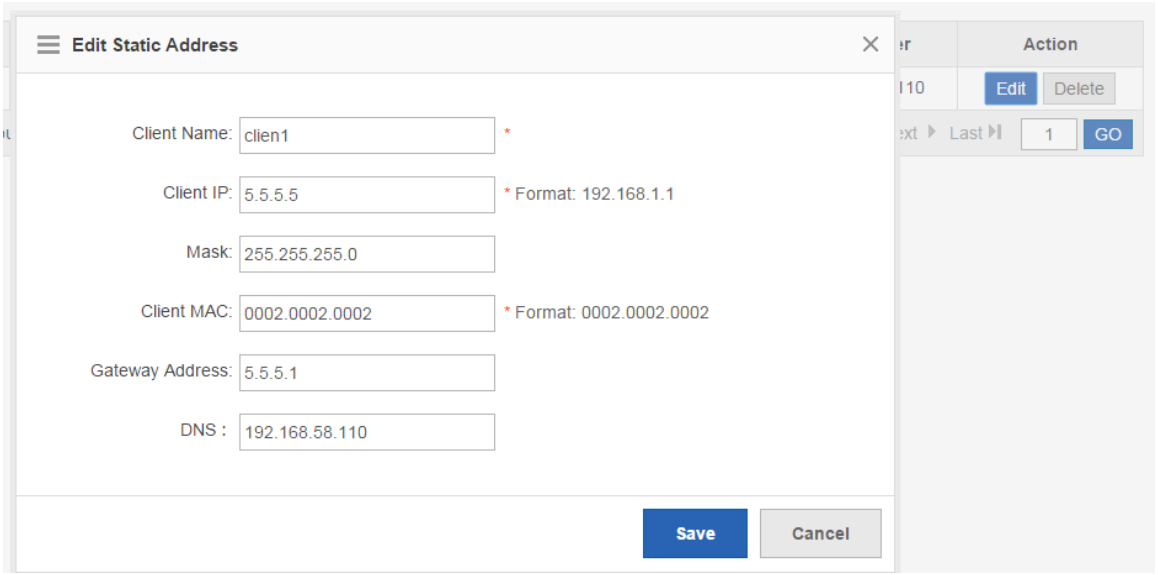

- Add Static Address




- Delete Selected Address

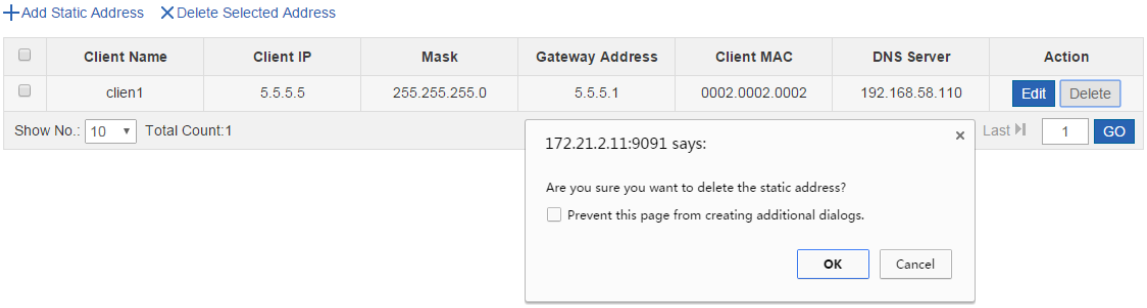


- Edit Static Address



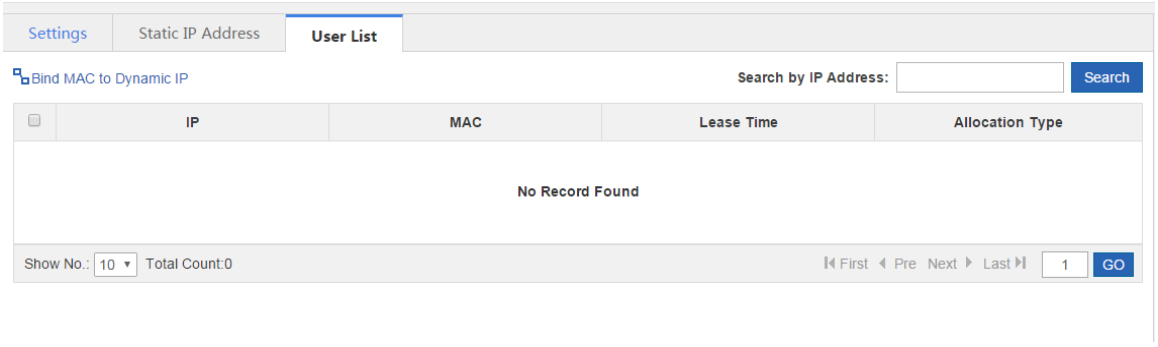

In the static address list, click **Edit**. In the dialog box displayed, edit the static address.

- Deleting a static address




In the static address list, click **Delete**. In the confirmation dialog box displayed, click **OK** to delete the static address.

### 1.3.14.7.3 User List




- Bind MAC to Dynamic IP

In the user list, select the record to be bound and click **Bind MAC to Dynamic IP** to complete binding.

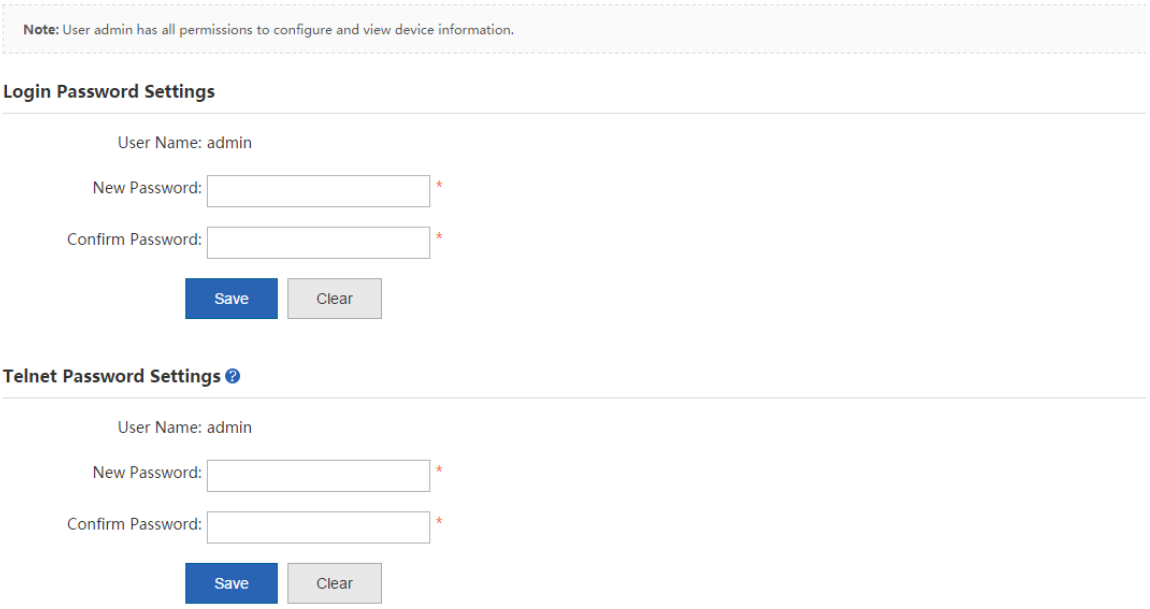
- Search by IP Address

Enter the IP address to be searched and click **Search**.


## 1.3.15 Advanced

### 1.3.15.1 System

#### 1.3.15.1.1 Change Password

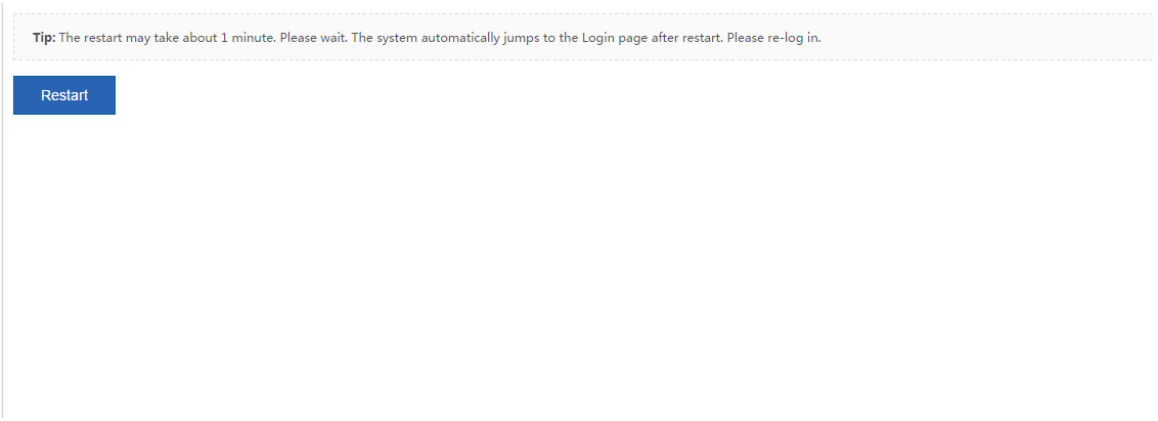



**Web password**: To configure the device on the Web page, you must use this password for login. Only administrators can configure information on this page. That is, this page is visible only to user **admin**. Password of user **admin** can be changed here.

**Telnet password**: To configure the device in Telnet mode, you must use the telnet password for login.

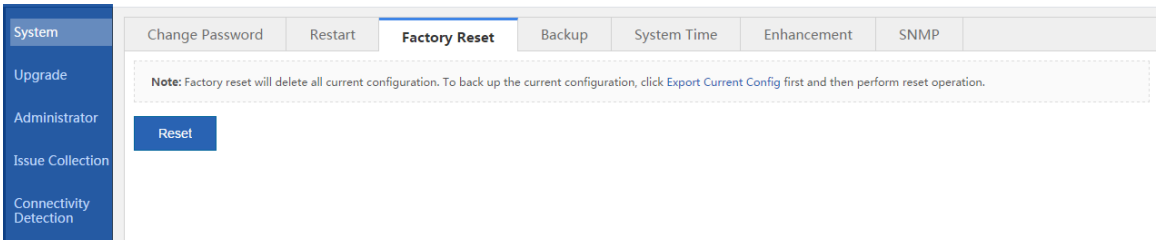
Keep the new password properly and use the new password for next login.

### 1.3.15.1.2 Restart



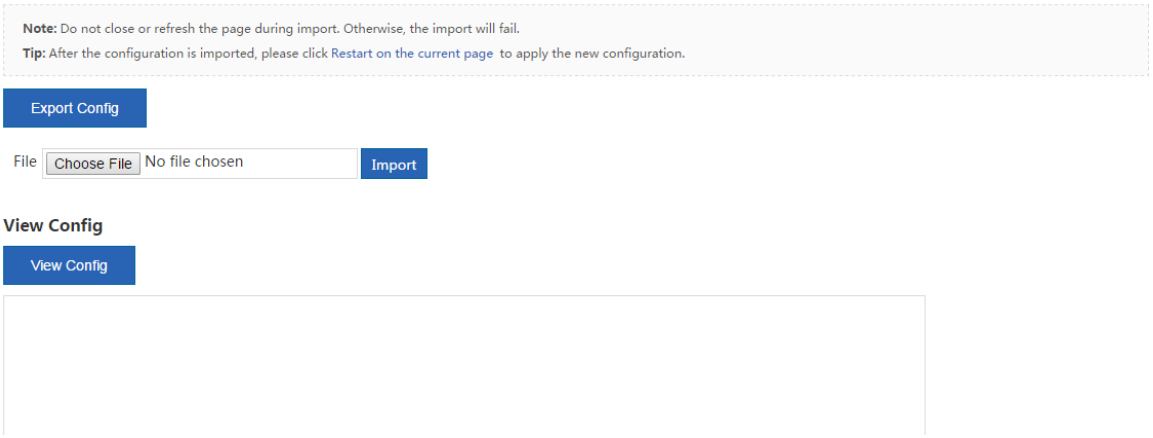

Click **Restart** to restart the device. The device restart takes about 1 minute. Do not perform any operations during this period. The system automatically refreshes the current page after the device is restarted successfully.

### 1.3.15.1.3 Factory Reset




Factory Reset will delete all current configurations on the device and the device will be restored to the default configuration state. If you want to keep the existing configuration, it is recommended to click **Export Current Config** to export the current configuration.

### 1.3.15.1.4 Backup




Configuration export: Export current configuration of the device to the local PC for backup.

Click **Export Config**. The file saving dialog box is displayed, and you can select a file storage position.

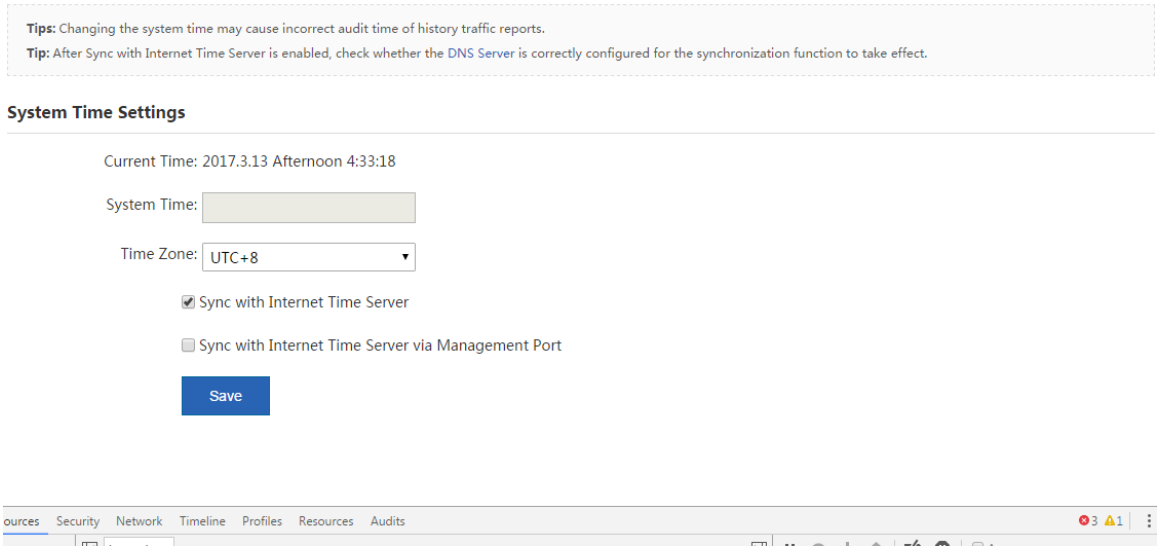
Configuration backup: Upload the configuration backup file from the local PC to the device for restoration.

Click **Choose File** and select a backup file on the local PC (the file name must be **config.text**). Then, click **Import** to import the backup file.

To make the imported configuration take effect, restart the device. If the imported configuration contains errors, click **Cancel** before the imported configuration takes effect.

Configuration display: Click **View Config** to display all configuration commands on the current device.

### 1.3.15.1.5 System Time



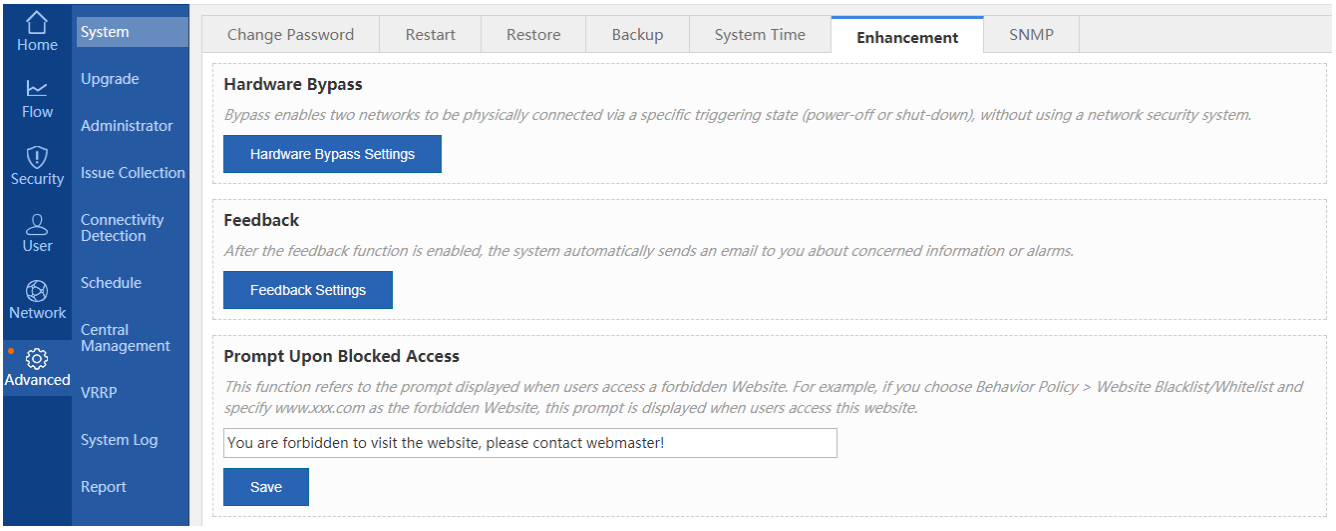


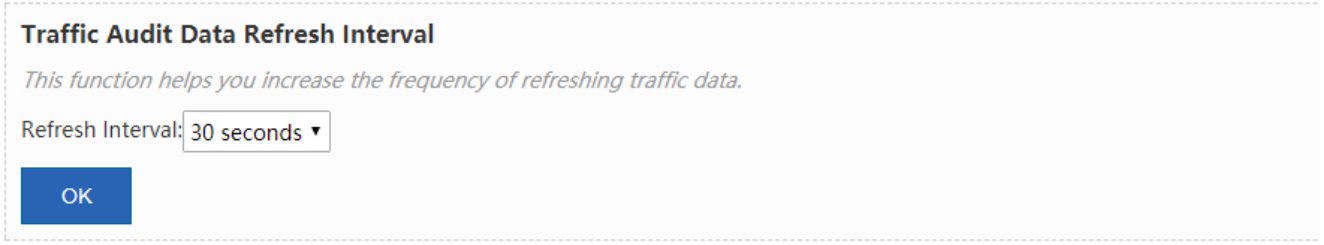


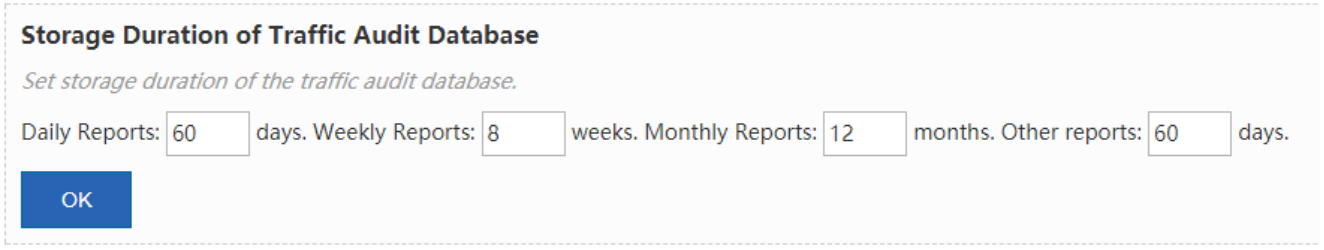
The system time function allows you to set the current time for the device.

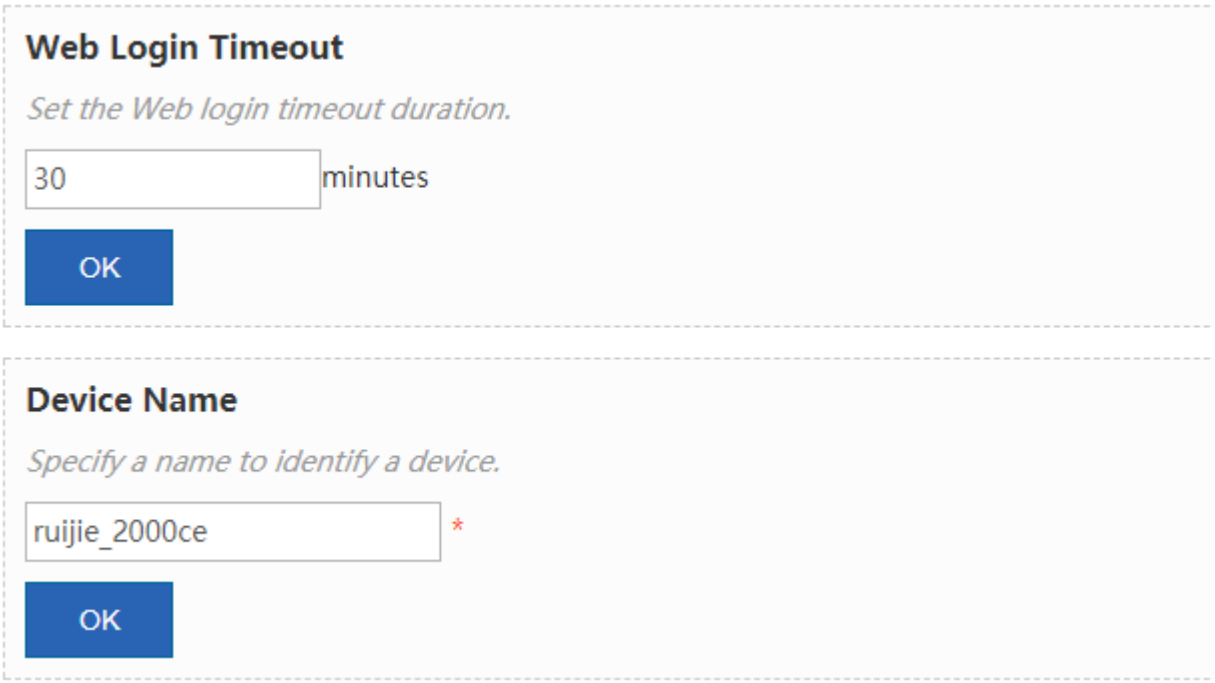
You can select **Sync with Internet Time Server**. Then, the device time will be always consistent with the Internet time. The function can only take effect after a correct DNS server is configured. If no DNS server is configured, choose **Network** > **DNS** to configure the DNS server.

### 1.3.15.1.6 Enhancement



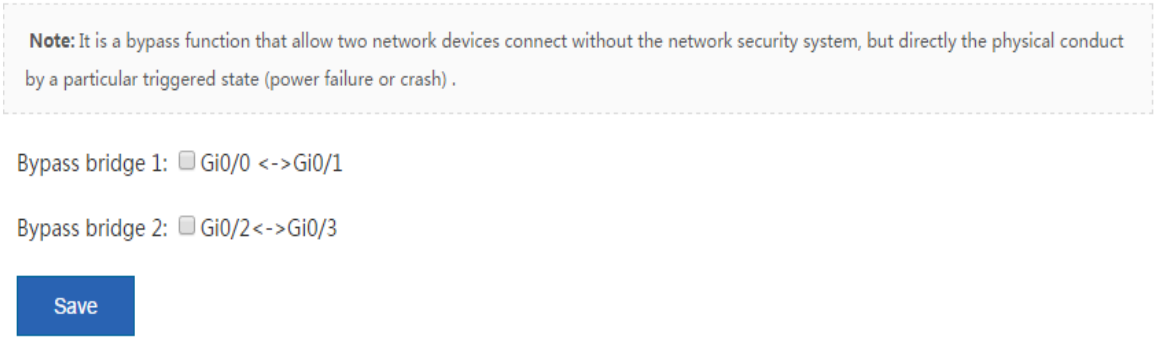



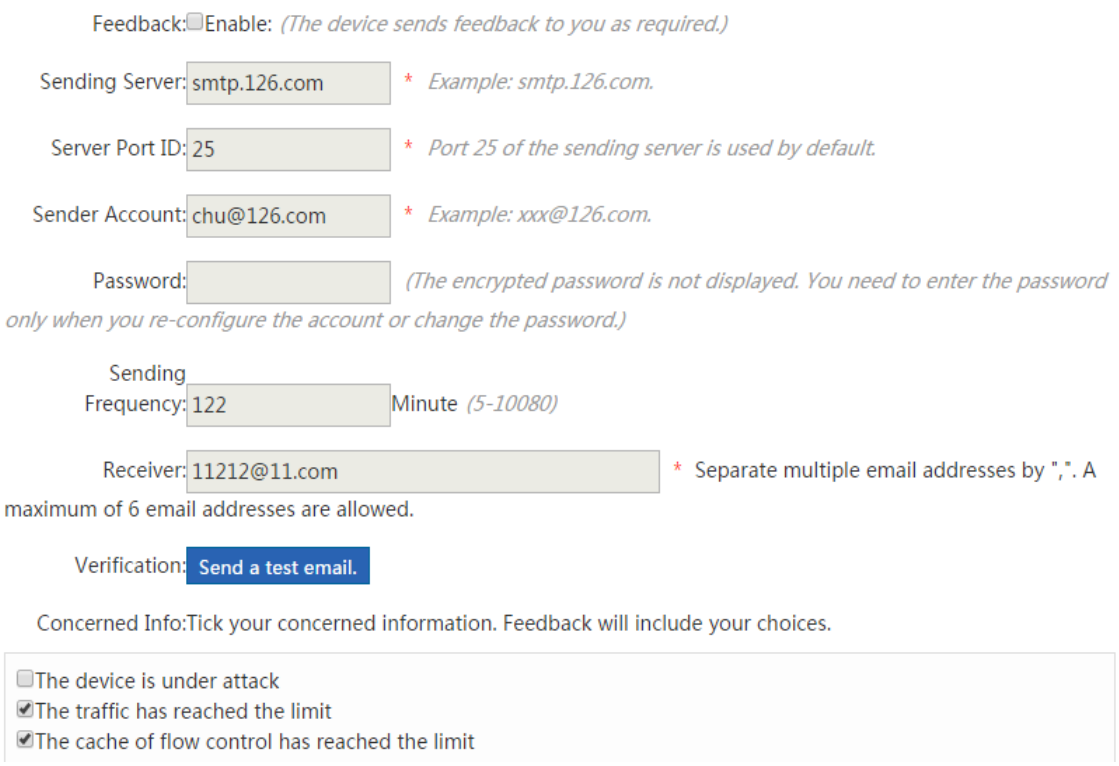

This page allows you to configure some enhancement functions for the device.

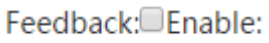
The hardware bypass function enables two networks to be physically connected upon a specific triggering state (power-off or shut-down), without using a network security system. Click Hardware Bypass Settings. A window shown in the figure below is displayed.




Select a bypass line and click **Save**.

The feedback function enables the device to send some alarms to you via emails and remind you to handle these alarms, so as to ensure normal and stable running of the device. Click Feedback Settings. A window shown in the figure below is displayed.




**Feedback**: Select  before configuring this function.


**Sending Server**: Enter the server of your primary address for sending emails. Assume that you have an email address *serv@ facebook.com* and you want to use the email address as the primary address for sending emails. Enter any of the following three servers: (POP3 server: pop.163.com |SMTP server: smtp.163.com |IMAP server: imap.163.com).

**Server Port ID**: Enter the port of the sending server. Use the default value unless otherwise specified.

**Sender Account**: Enter the primary address for sending emails, for example, serv@163.com.

**Password**: Enter the password of the primary address for sending emails, that is, the password of the sender account.

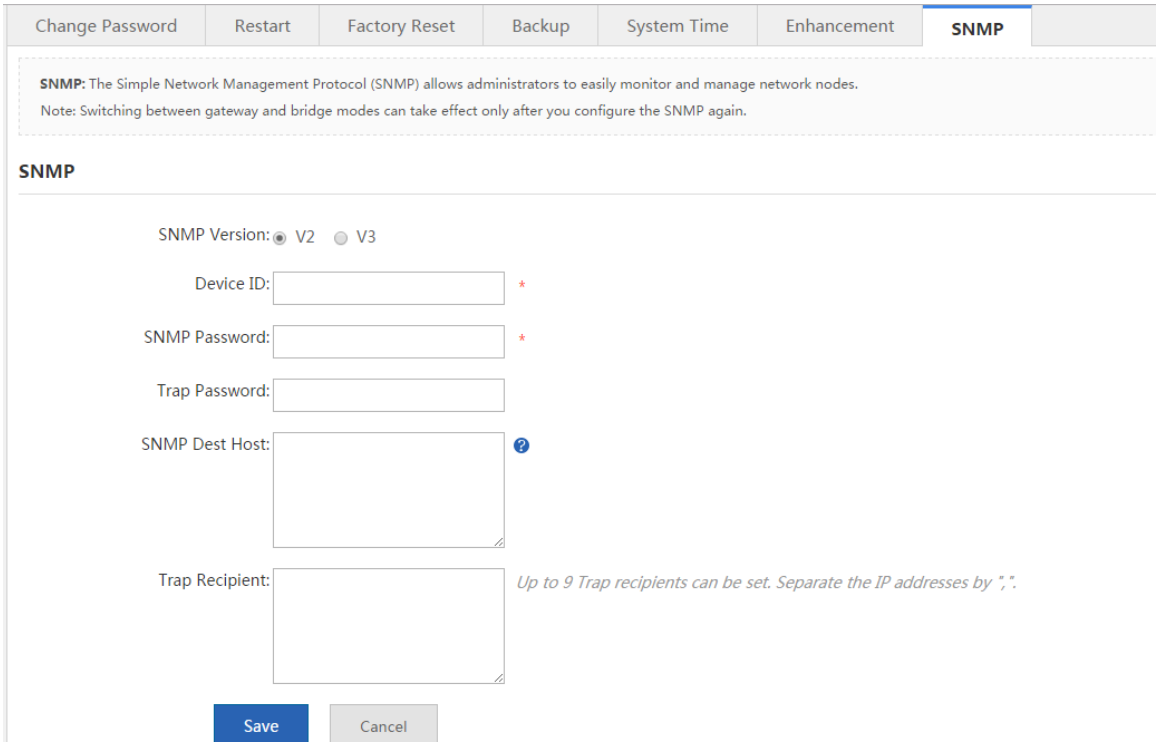
**Sending Frequency**: Set the frequency for sending alarms to your specified email address. By default, only one notification is sent every 60 minutes. For example, if a memory insufficiency alarm is generated, the device sends an alarm email to you once every hour.

**Receiver**: Enter your email address which can be used to receive alarms.

**Concerned Info**: All alarm types supported by the system are listed here. You can select one as required. After selection, if an alarm of the selected one is generated, the device sends the alarm to your email address.


**Industry**, **Organization**, **and Tel. No.**: You are recommended to enter actual information so that better services can be provided for you.

### 1.3.15.1.7 SNMP

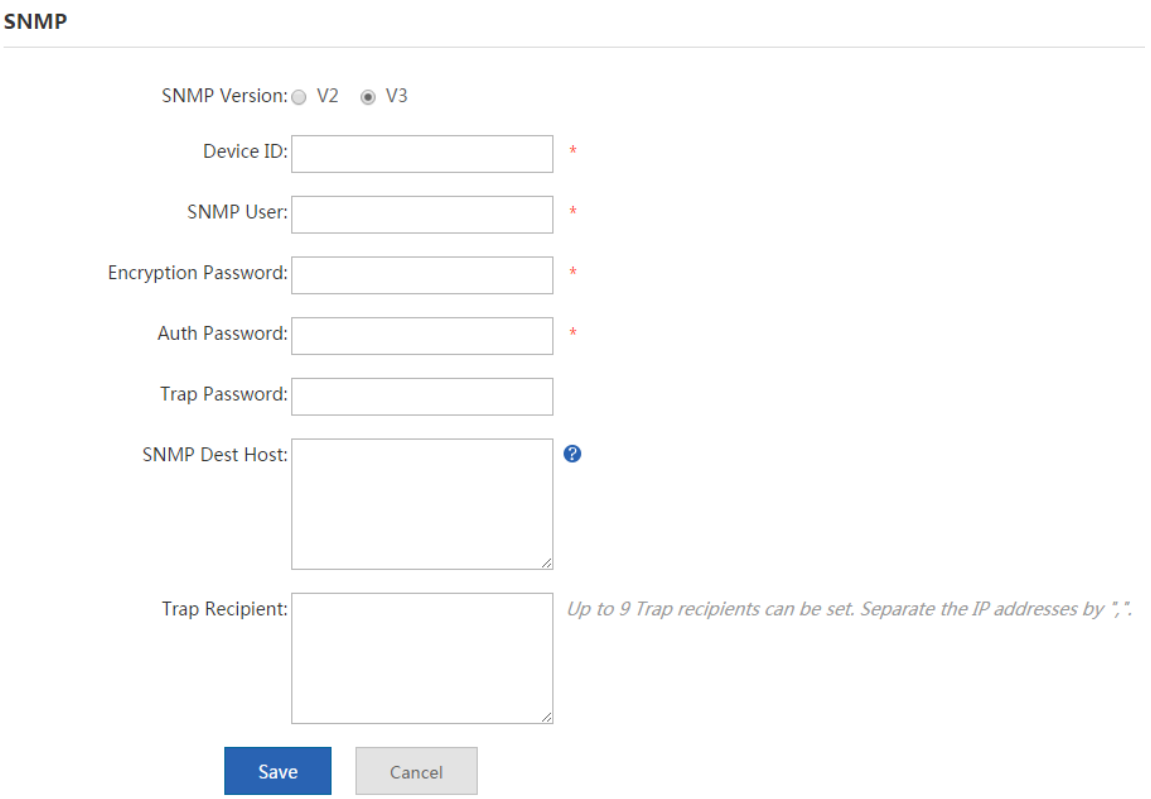



**SNMP**

The Simple Network Management Protocol (SNMP) allows administrators to easily monitor and manage network nodes.

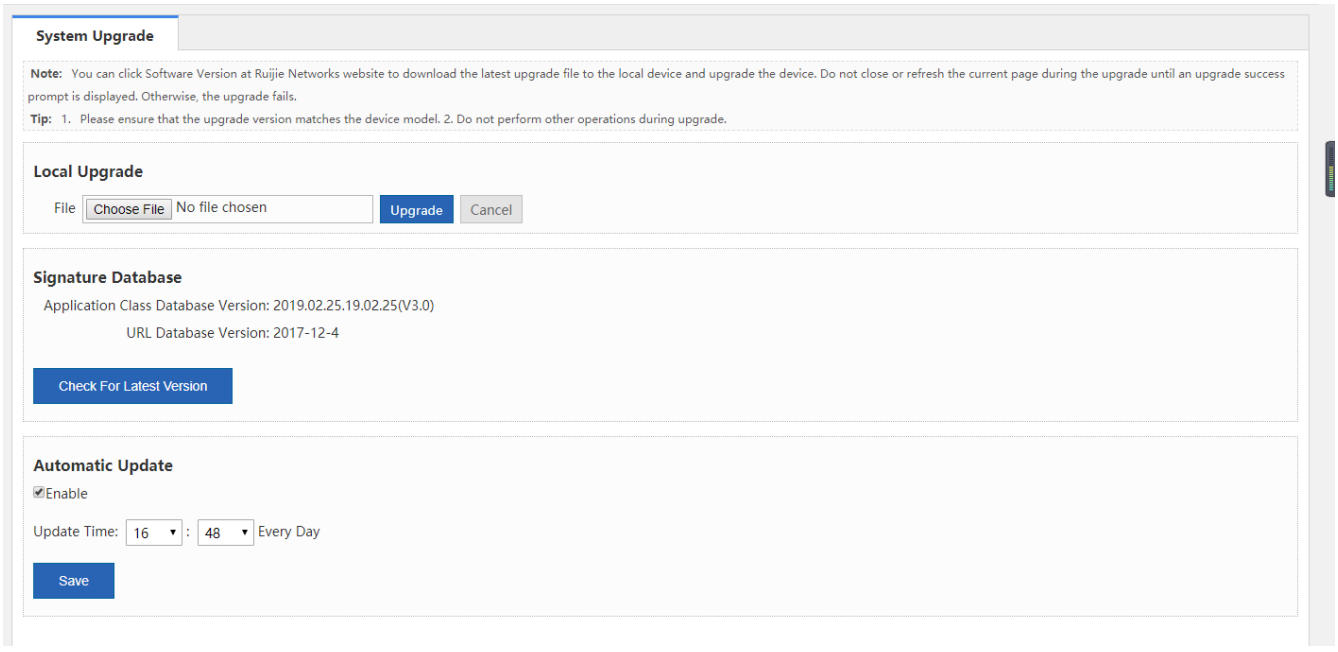
1. **SNMP Version**: The device supports SNMPv2 and SNMPv3. The figure above shows the configuration of SNMPv2.
2. **Device ID**: Indicates the ID of SNMP server.
3. **SNMP Password**: Indicates the password for the management host to connect to the current device.
4. **Trap Password**: Indicates the password for connecting to the management host. When an alarm is generated, the device actively sends the alarm to the management host.
5. **Trap Recipient**: Indicates the list of management hosts that will receive device alarms. A maximum of ten hosts can be configured.

The figure below shows the configuration of SNMPv3.




Security settings are enhanced in SNMPv3. The encryption password and authentication password of SNMP users need to be configured.

### 1.3.15.2 Upgrade

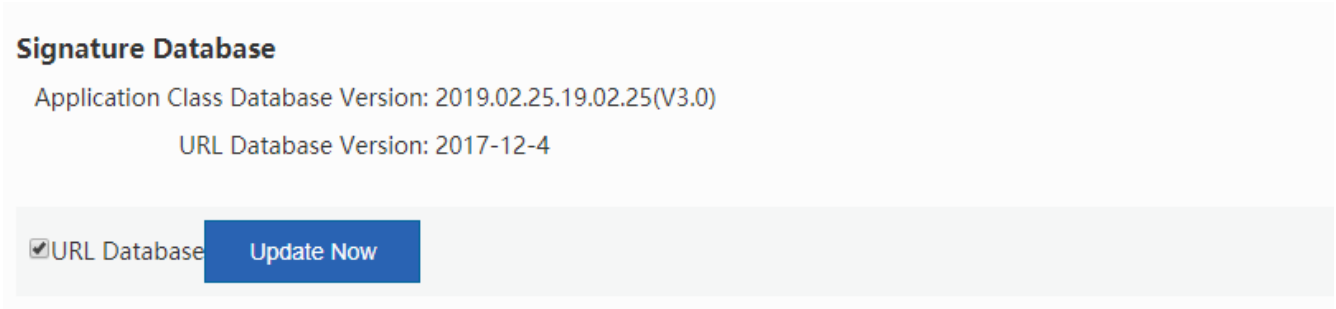


You can click the software version at Ruijie Networks official website to download the latest upgrade file to the local device and upgrade the device on this page. Do not close or refresh the page during the upgrade until an upgrade success prompt is displayed. Otherwise, the upgrade will fail. The upgrade takes about 50 seconds.

If the software main program needs to be upgraded, the file must be named **rgos.bin**. In addition, ensure that the model of the upgrade version is the same as the model of the device.

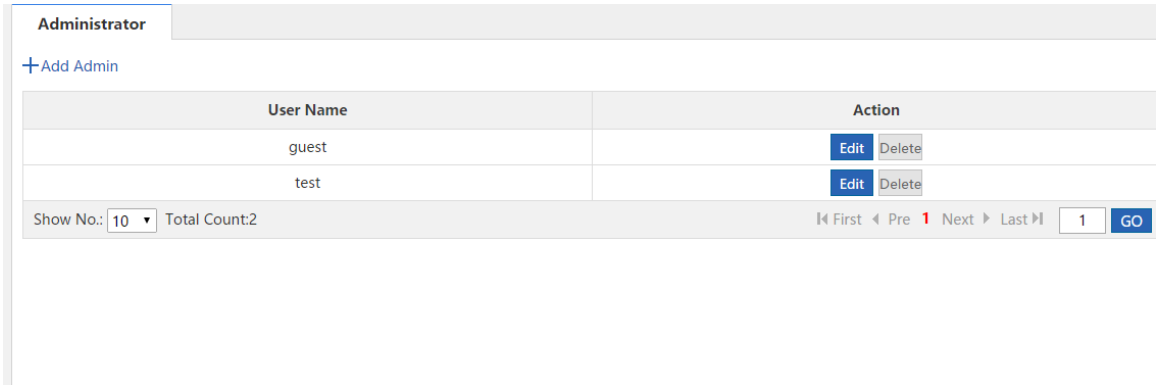
**Local Upgrade**: Click **Choose File** and select the upgrade package from your local PC. Click **Upgrade**. A progress bar is displayed, indicating that the upgrade is underway. Wait patiently and do not perform any operations. An upgrade success prompt will be displayed about 50 seconds later. Click **OK**.

**Signatrue Database**: It is used to check for the latest signature/URL library. If a later version is available, please click Update Now to update the signature/URL library.



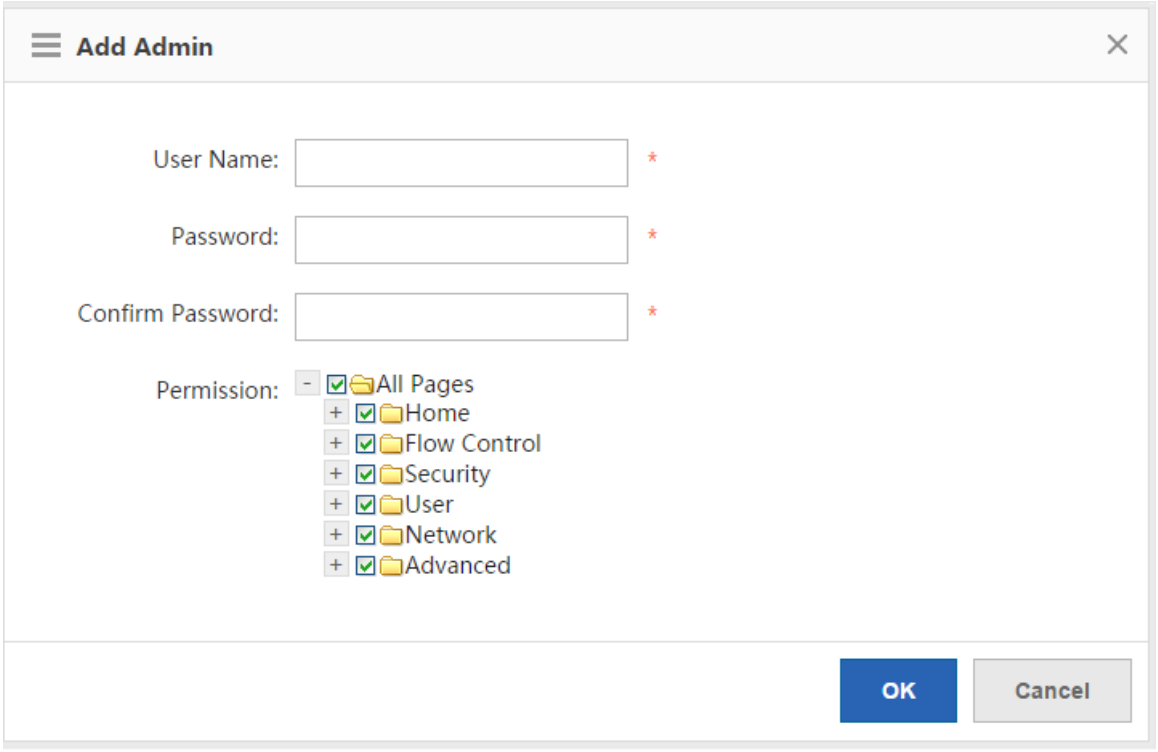

**Automatic Update**: You can specify a time for automatic update.

### 1.3.15.3 Administrator




Device administrators added on the **Administrator** page can log in to the Web management system to conduct routine maintenance or management on the device, but cannot run commands via Telnet. User **manager** and user **guest** cannot be deleted. To ensure security, only user **admin** can view and edit information on this page.

Click **Add Admin** to add an administrator. Ensure that **User Name**, **Password**, and **Confirm Password** cannot be null.



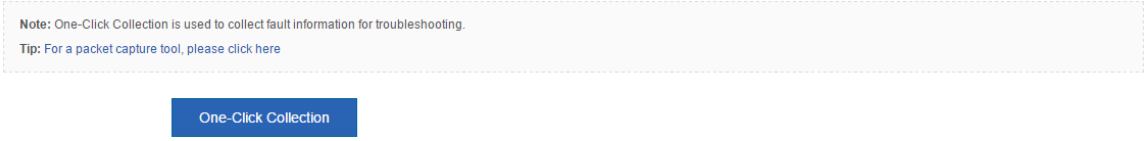

**User Name**: Enter an administrator name. English names are recommended and Chinese names should be avoided, for example, zhangs.

**Password**: The password is used by the administrator for login to the Web management system.

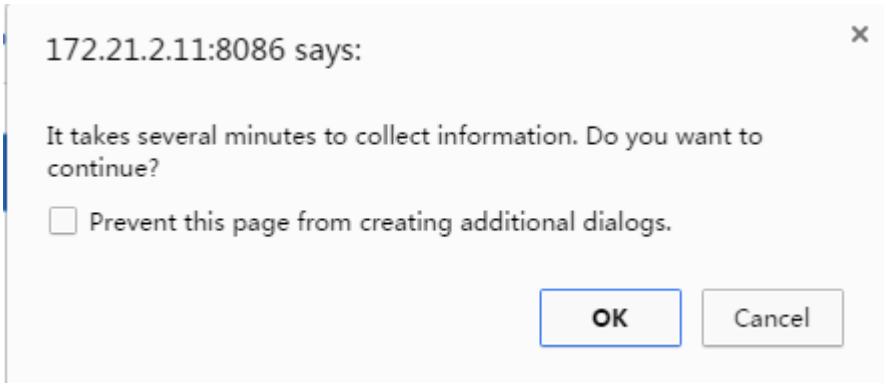
**Permission**: You can grant management function permissions to the administrator.

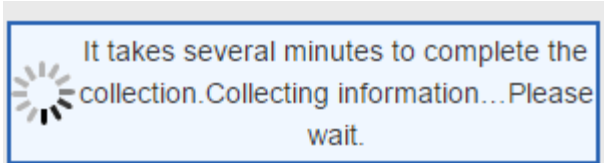
### 1.3.15.4 Issue Collection

The one-click collection function collects device fault information for troubleshooting.



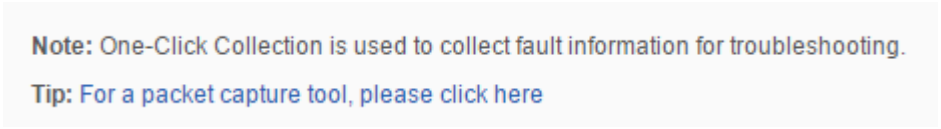

Click **OK**, and wait for the device to collect information.

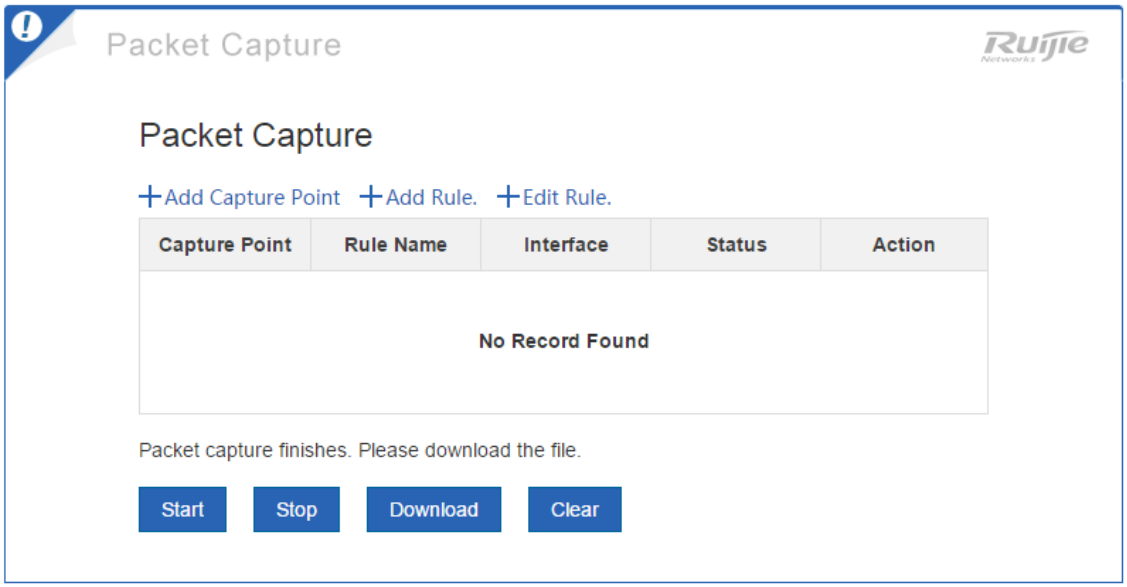



After the collection, click  to generate a package, for example, **tech_vsd0_20150727172504.tar.gz**. This package facilities fault analysis by engineers.


Packet capture tool: For details about the packet capture function of the device, click the URL. The packet capture page is shown in the figure below.

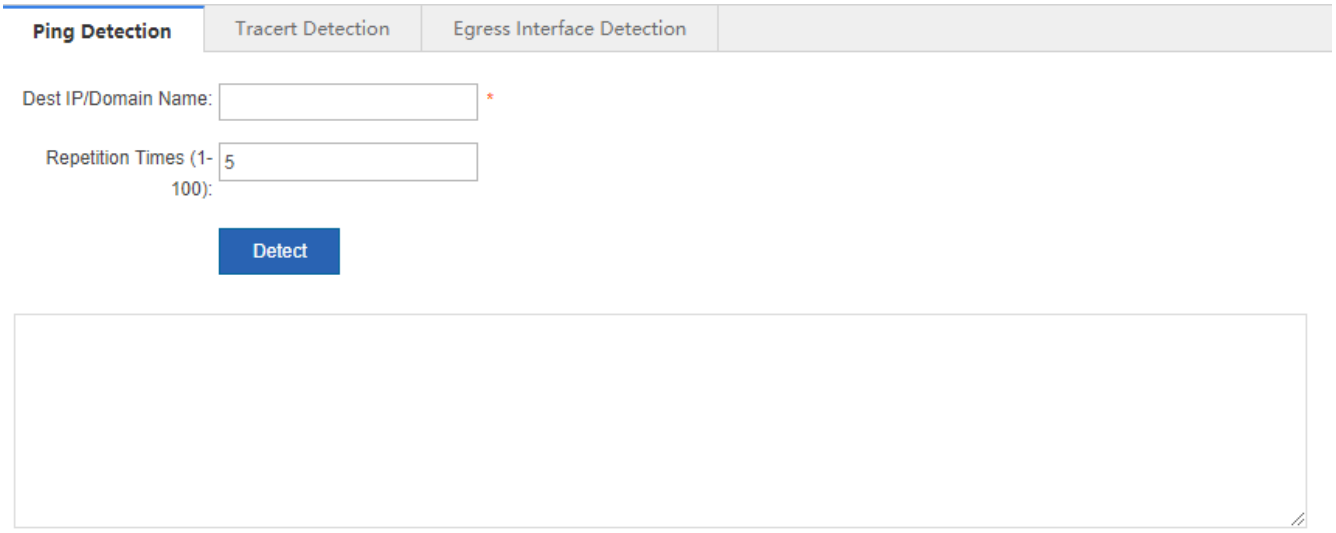



Note: This function is provided for engineers to locate faults. Do not use it at discretion. Otherwise, the network will be affected.

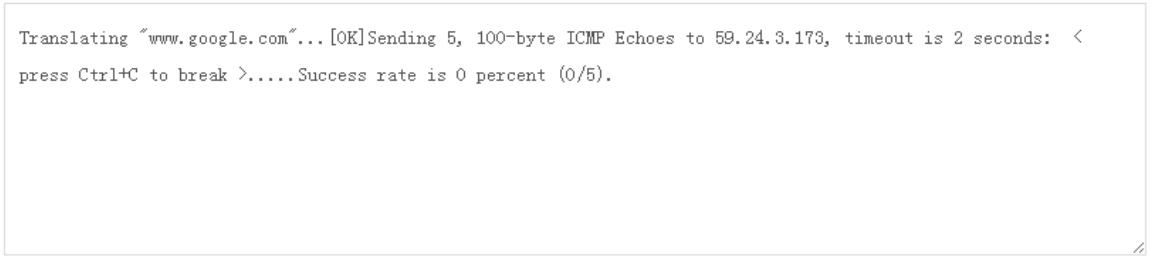
### 1.3.15.5 Connectivity Detection

Connectivity detection includes ping detection and tracert detection.

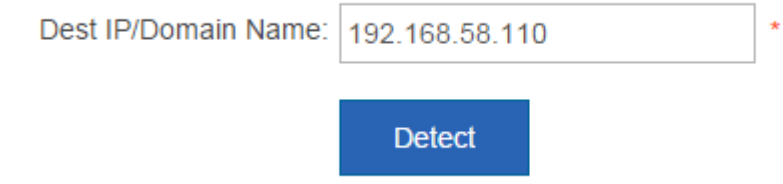



The ping detection page is shown in the figure below.


Enter the destination IP address or domain name and click **Detect**. The detection result shown in the figure below is displayed.




The tracert detection page is shown in the figure below.

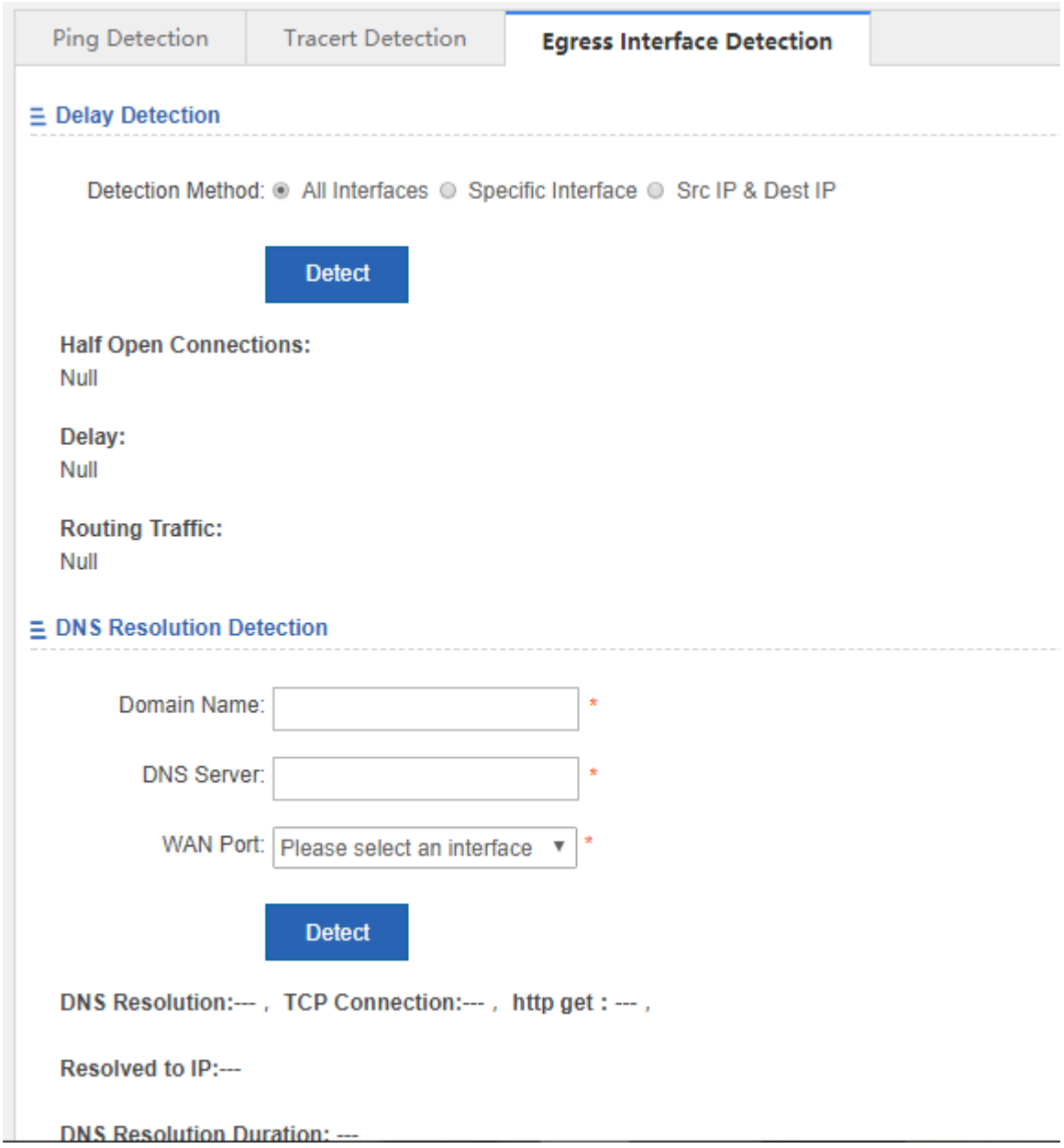


Enter the destination IP address or domain name and click **Detect**. The detection result shown in the figure below is displayed.

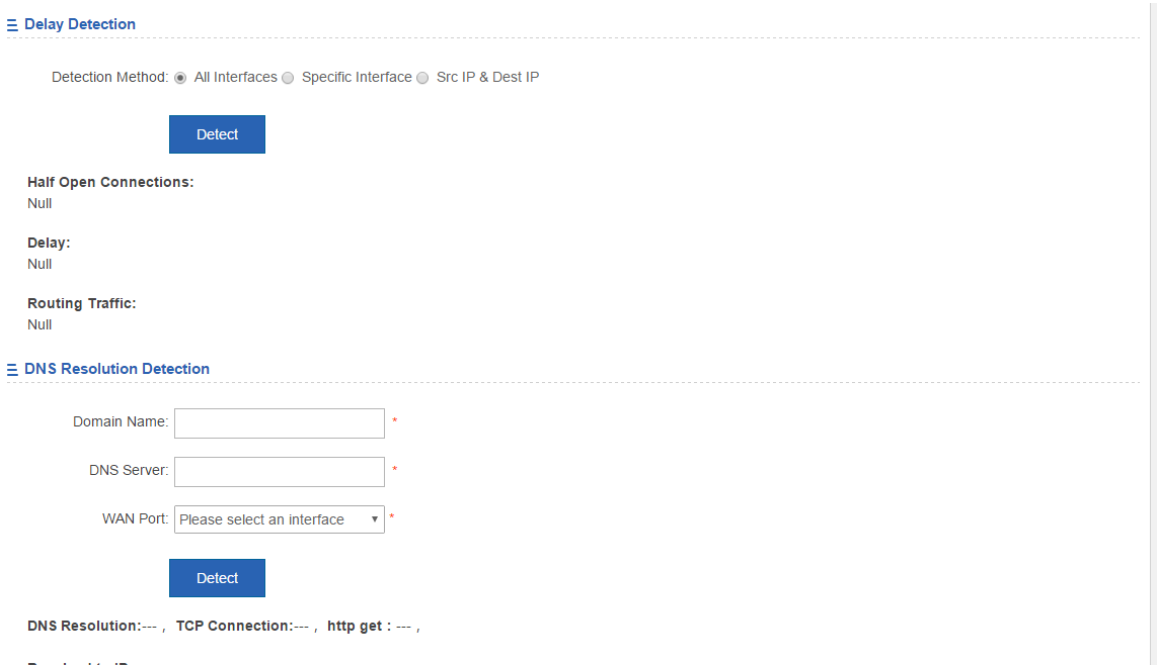
```
  < press Ctrl+C to break >Tracing the route to 192.168.58.110 1         172.21.2.1      3 msec    1 msec    1
msec 2      172.21.255.13     <1 msec   <1 msec   <1 msec 3      172.21.255.70      1 msec   <1 msec   <1 msec
4      173.18.124.10      1 msec    1 msec    1 msec 5      172.21.255.70      1 msec    2 msec    1 msec 6
172.21.255.73      1 msec    1 msec    1 msec 7       172.21.255.1      1 msec    1 msec    1 msec 8
192.168.59.178      1 msec    1 msec    1 msec 9     192.168.59.177      2 msec    1 msec    2 msec 10
192.168.59.26      2 msec    1 msec    4 msec 11       172.22.0.18      3 msec    2 msec    2 msec 12
192.168.58.110      1 msec    1 msec    2 msec
```

Egress interface detection includes delay detection and DNS resolution detection.

The delay detection page is shown in the figure below.



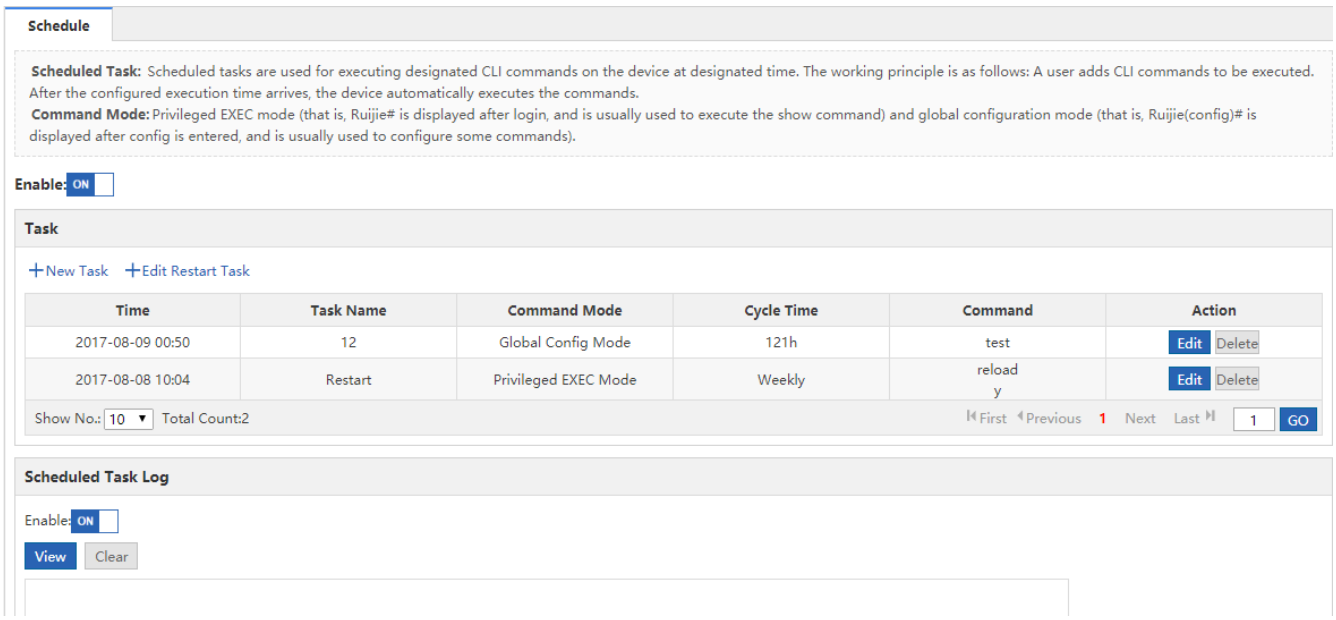

The DNS resolution detection is shown in the figure below.




## 1.3.15.6 Scheduled Task

**Scheduled Task**: Scheduled tasks are used for executing specified CLI commands on the device at a specified time. The working principle is as follows: A user adds CLI commands to be executed. After the configured execution time arrives, the device automatically executes the commands.

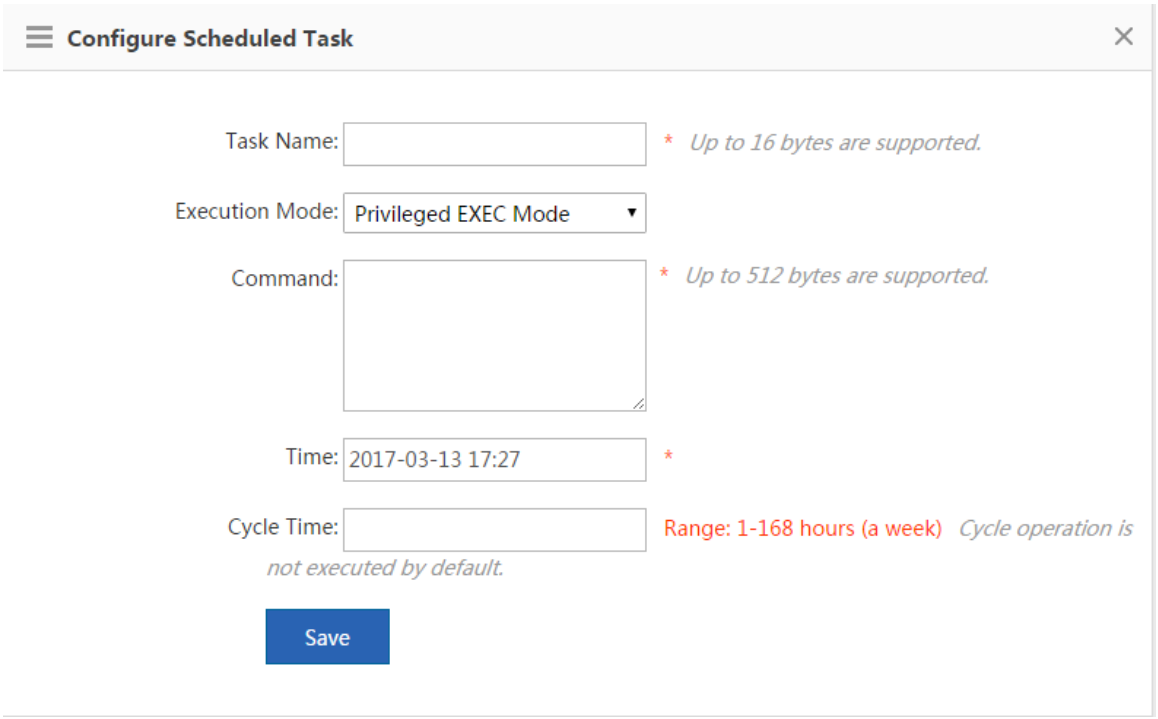
**Command Mode**: The command mode includes the privileged EXEC mode and global configuration mode. In privileged EXEC mode, the execution permission is the privileged EXEC mode permission (that is, **Ruijie#** is displayed after login, and the **show** command is usually executed in this mode). In global configuration mode, the execution permission is the configuration mode permission (that is, **Ruijie(config)#** is displayed after **config** is entered, and some commands are usually configured in this mode).



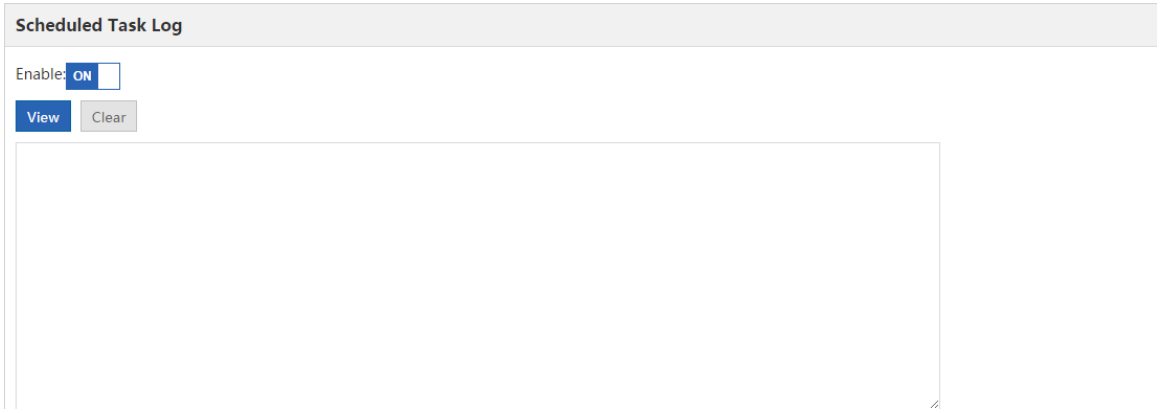
Click 

to enable the scheduled task function and then configure a scheduled task. Click **New Task**.

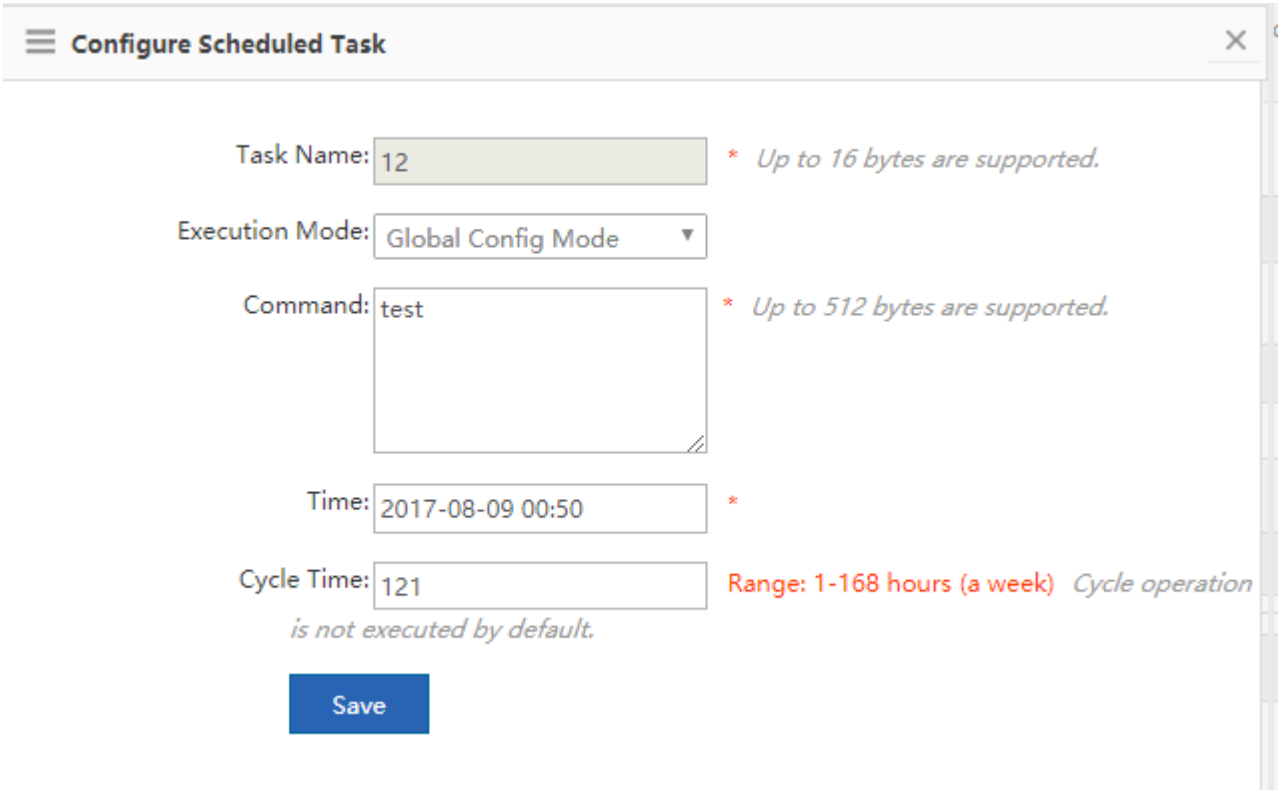
The **Configure Scheduled Task** dialog box is displayed, as shown in the figure below.

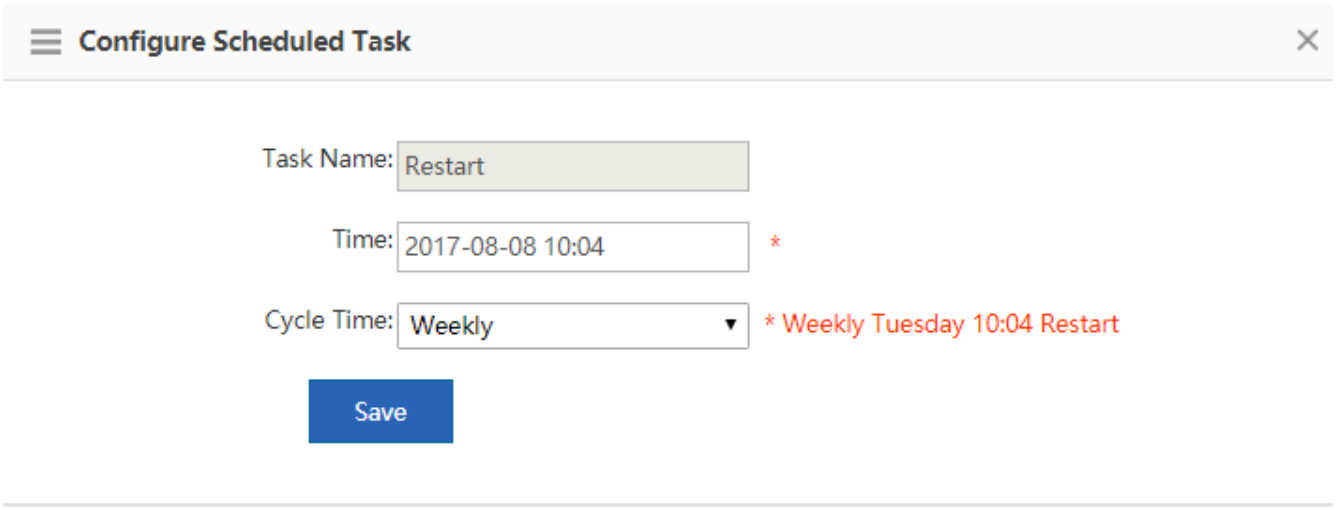



After a scheduled task is executed, you can view scheduled task logs after enabling the scheduled task log function, as shown in the figure below.

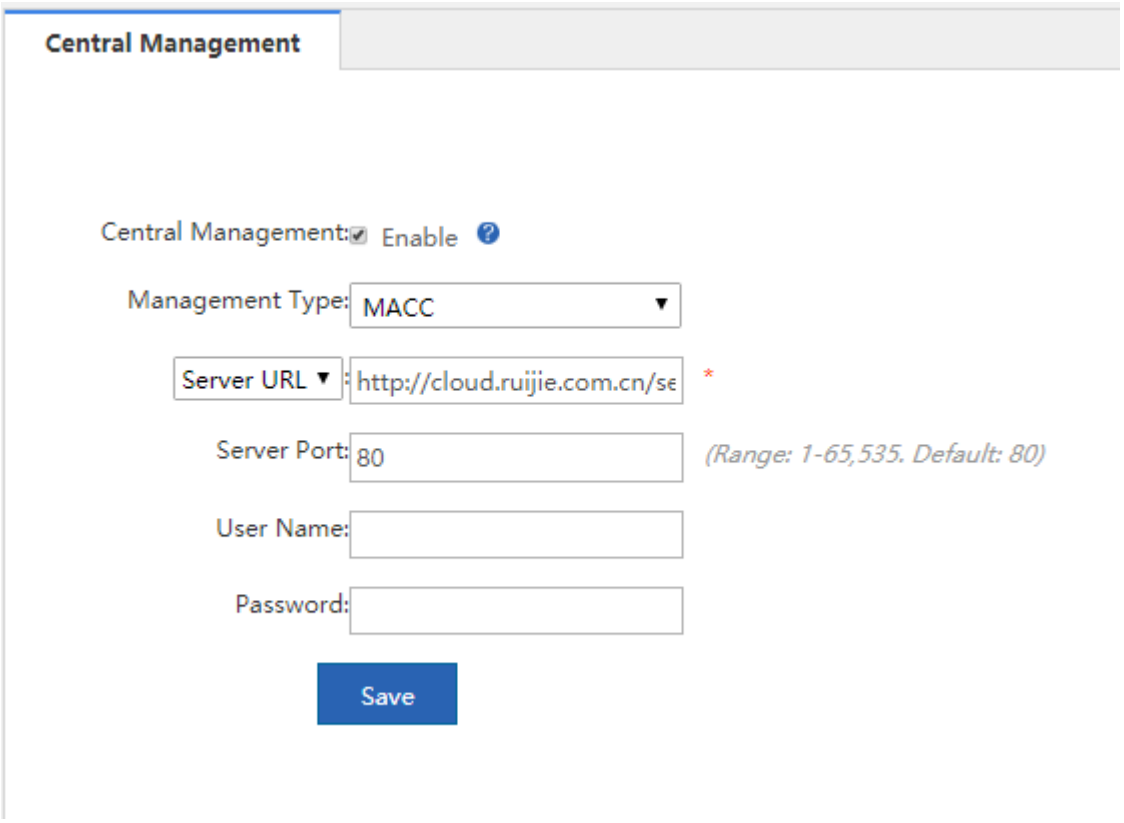



Set the time for periodical execution of scheduled tasks in **Cycle Time**, as shown in the figure below.


Configure Scheduled Task
Task Name: 12
* Up to 16 bytes are supported.
Execution Mode: Global Config Mode
Command: test
* Up to 512 bytes are supported.
Time: 2017-08-09 00:50
*
Cycle Time: 121
Range: 1-168 hours (a week) Cycle operation is not executed by default.
Save

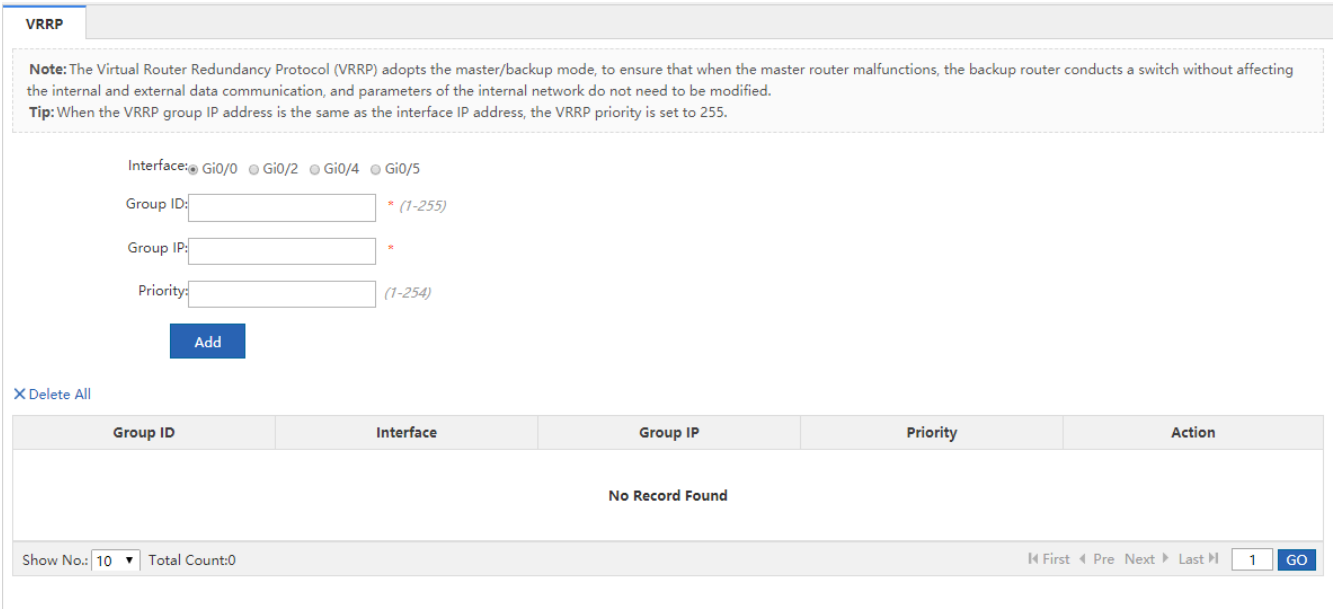

Configure Scheduled Task
Task Name: Restart
Time: 2017-08-08 10:04
*
Cycle Time: Weekly
* Weekly Tuesday 10:04 Restart
Save

### 1.3.15.7 Central Management




Central management includes MCP management and RAC-SNC management.

### 1.3.15.8 VRRP



The Virtual Router Redundancy Protocol (VRRP) is designed in master/backup mode. When the master router malfunctions, the backup router takes over the data and services of the master router without affecting the internal and external data communication, and LAN parameters do not need to be modified.

**Interface**: All LAN interfaces of the device are listed. Select an interface to be configured.

**Group ID**: Enter the ID that identifies a VRRP policy.

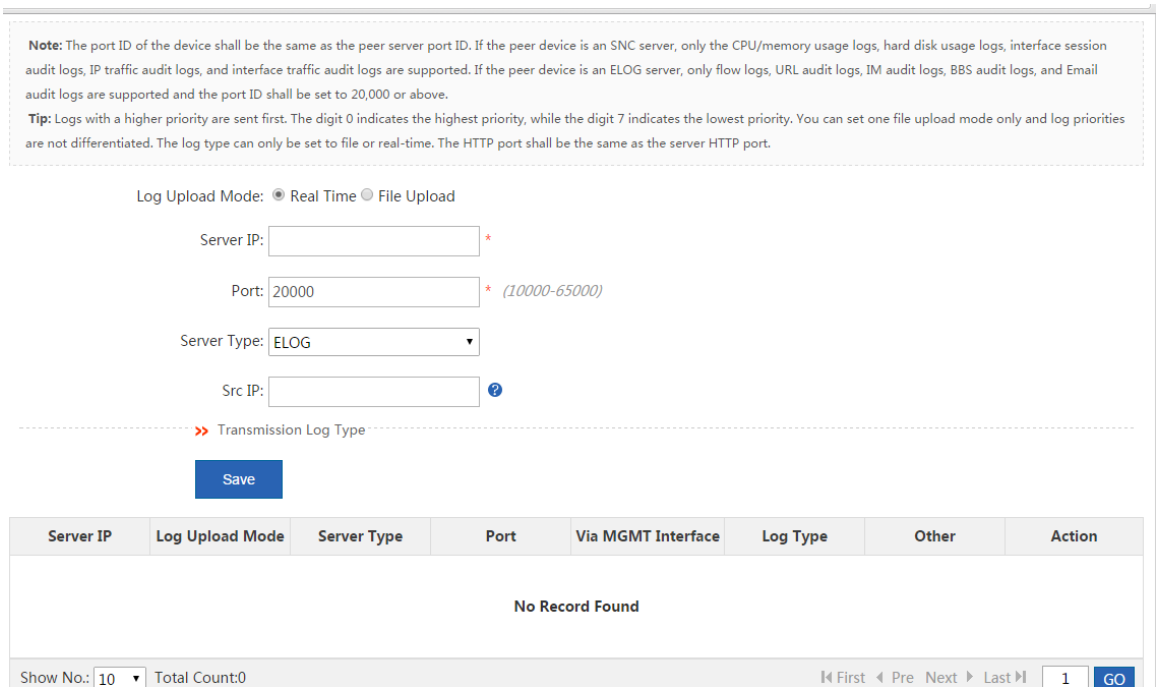
**Group IP**: Enter the IP address of the VRRP group. Note that if the IP address entered is the same as the IP address of the selected interface, the device automatically sets the VRRP priority to 255 and the priority cannot be changed.

**Priority**: Indicates the VRRP policy matching sequence of the same interface.

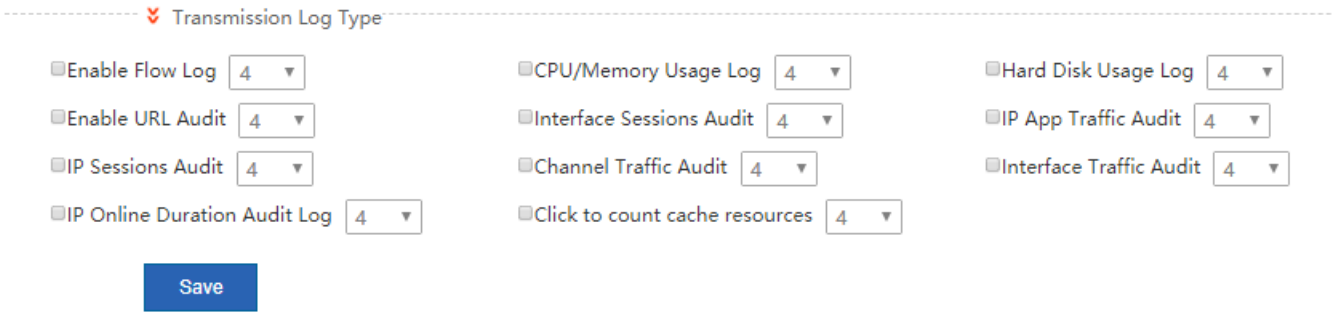
## 1.3.15.9 System Log

### 1.3.15.9.1 Server Log

The server log function enables the device to send audited logs to the specified log server. The log types supported by the EG device are shown in the figure below. Configure required types of logs to be sent to the specified server.

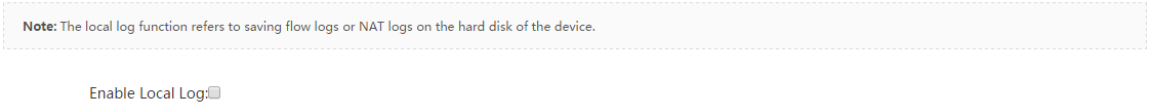



1. **Server IP:** Enter the IP address of the server for receiving logs.
2. **Port**: Different port ranges have different meanings. A port ID smaller than 20000 indicates the E-LOG server while a port ID of 20000 or larger values indicates the SNC server. The E-LOG server supports only URL and flow logs while the SNC server supports all logs.
3. **Transmission Log Type:**



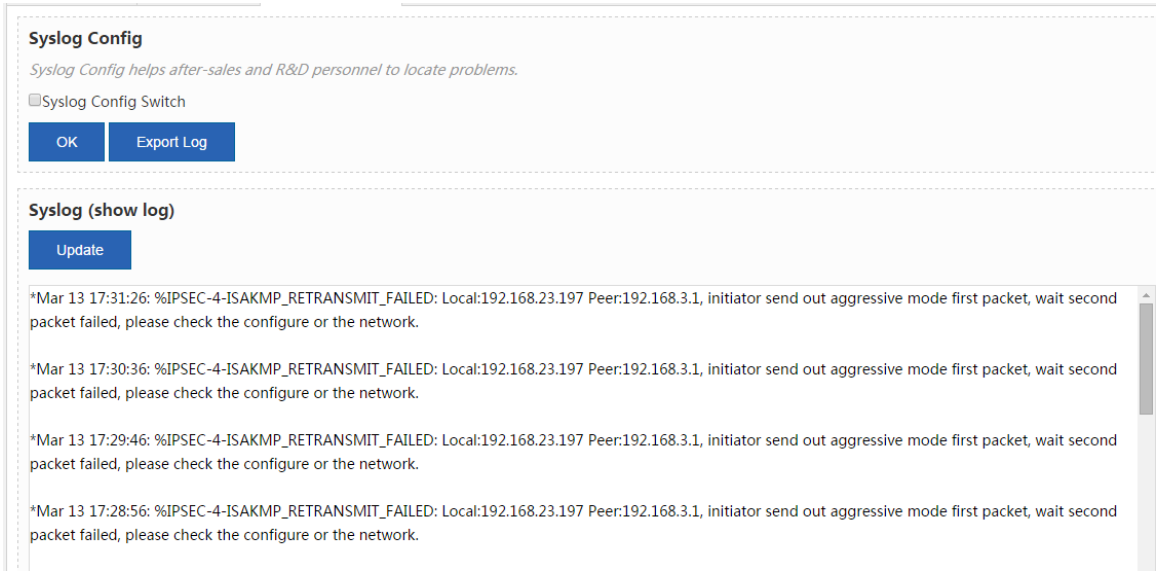

### 1.3.15.9.2 Local Log

The local log function enables the device to save flow logs or NAT logs to the hard disk of the device. Select Enable Local Log: to enable the local log function. A page shown in the figure below is displayed.

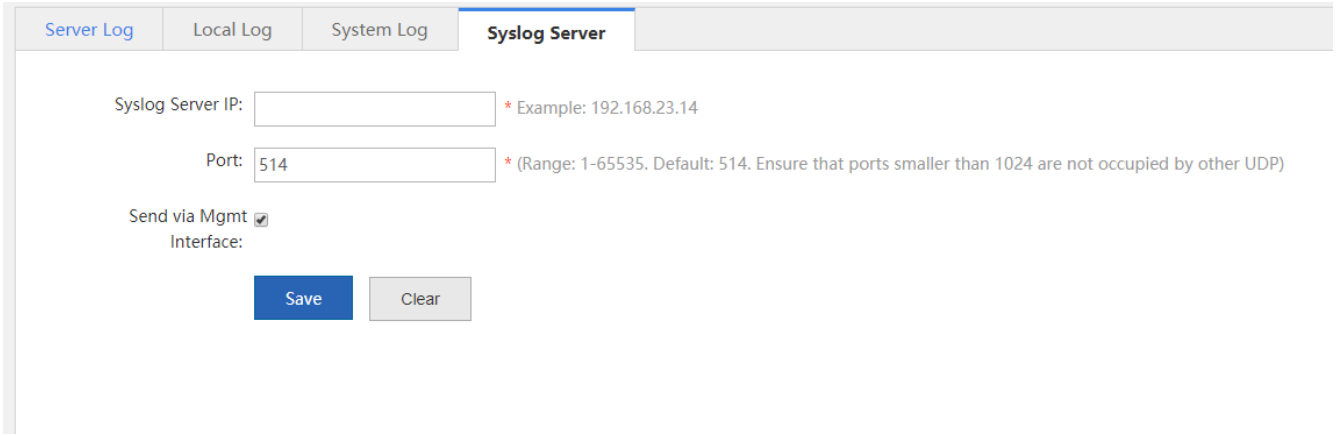



### 1.3.15.9.3 System logs

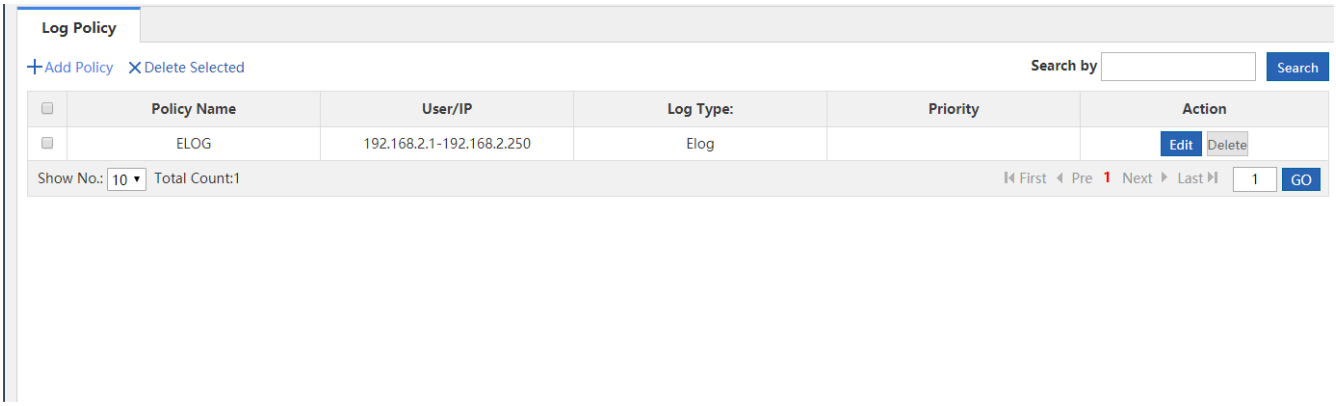
**View system logs**: Click **Update**. The current logs in the system are updated, as shown in the figure below.



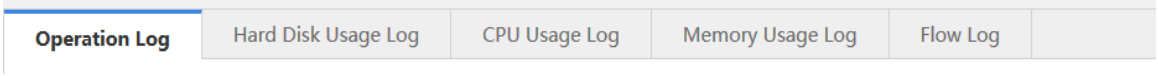

Syslog Server



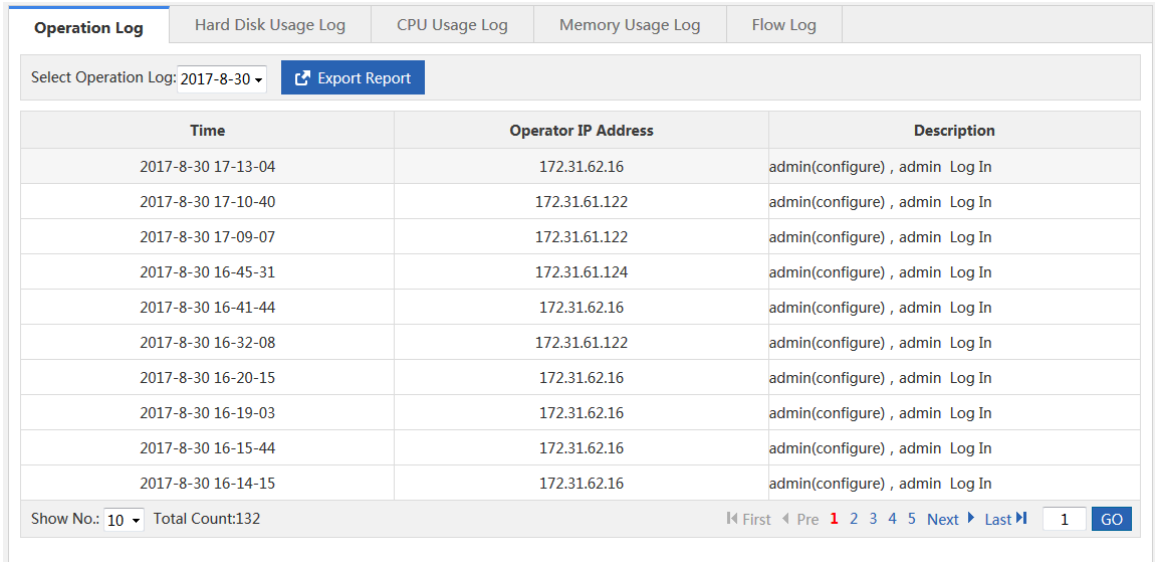

### 1.3.15.10 Log Policy




### 1.3.15.11 Report

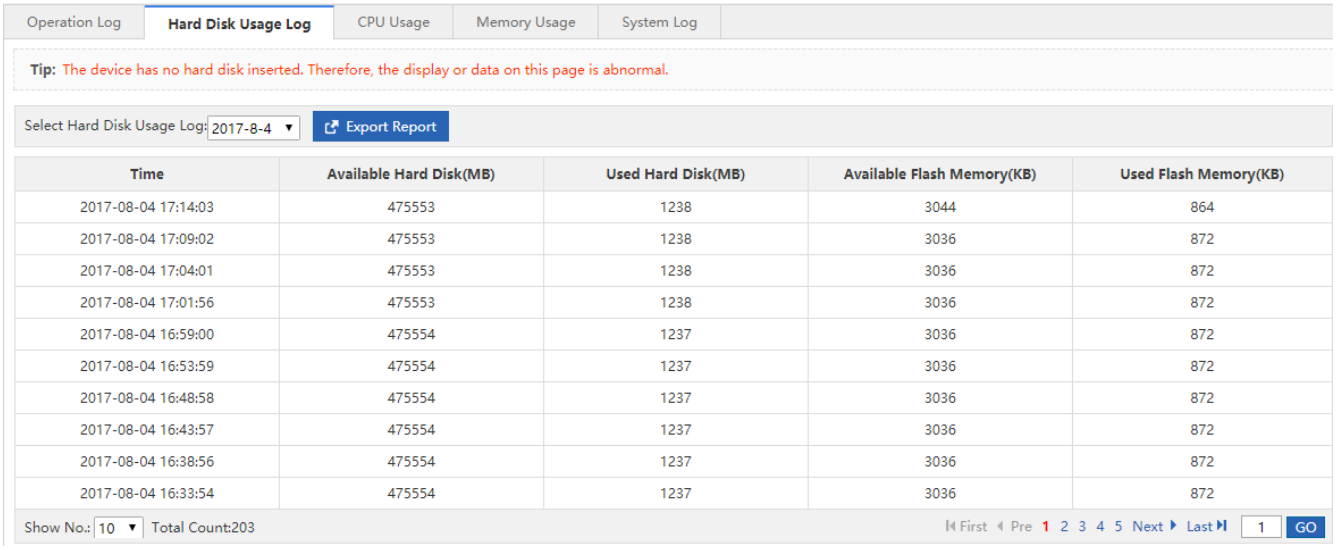


### 1.3.15.11.1 Operation Log



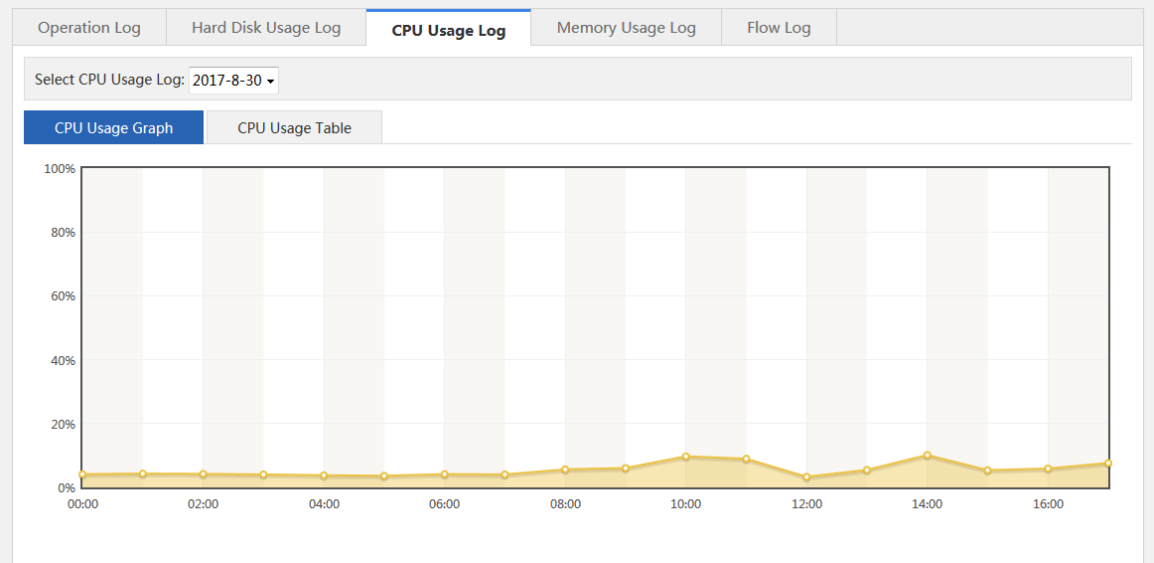

This function displays device operations.

### 1.3.15.11.2 Hard Disk Usage Log



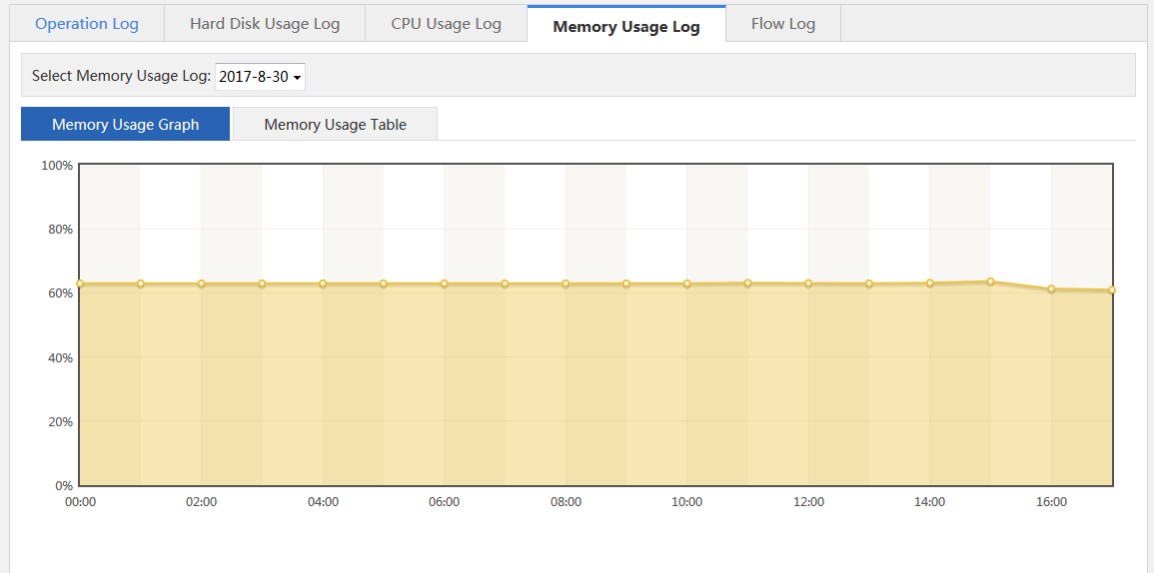

This function displays the usage of the device hardware.

### 1.3.15.11.3 CPU Usage Log



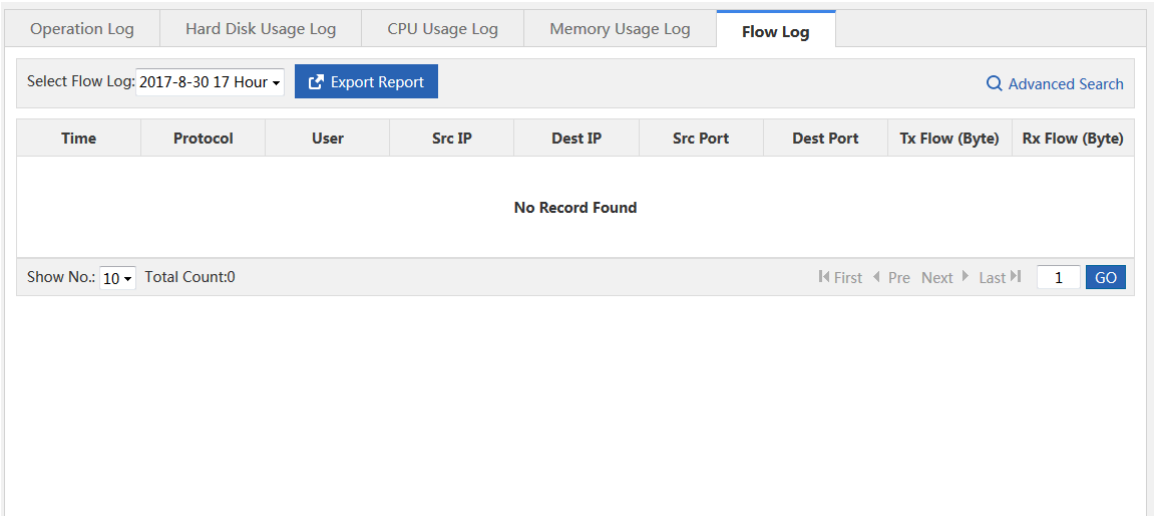

This function displays the CPU usage in different time ranges on a day.

### 1.3.15.11.4 Memory Usage Log




This function displays the memory usage in different time ranges on a day.

### 1.3.15.11.5 Flow Log




This function displays the flow usage on a day.

**Advanced Search**: You can select required flow records.