

Security Gateway Web Configuration Guide

Models: SG-5110, SG-5105, SG-3110

Contents

1. Web Configuration.....	1
1.1 Overview.....	1
1.2 Applications.....	1
1.1.1 Managing Devices via Web Management System.....	1
1.3 Web Management System.....	2
1.1.2 Access to Web Management UI.....	2
1.1.3 Config Wizard.....	4
1.1.4 Main UI of Web Management System.....	7
1.1.5 Home.....	9
1.1.6 Service.....	13
1.1.7 Interface Status.....	14
1.1.8 Common.....	14
1.1.9 Flow Control.....	14
1.1.10 Behavior Management.....	49
1.1.11 Cache.....	75
1.1.12 Security.....	83
1.1.13 User.....	95
1.1.14 Network.....	120
1.1.15 Advanced.....	154

1. Web 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 SG (Security Gateway).

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

Currently, this document is applicable only to the gateway.

1.2 Applications

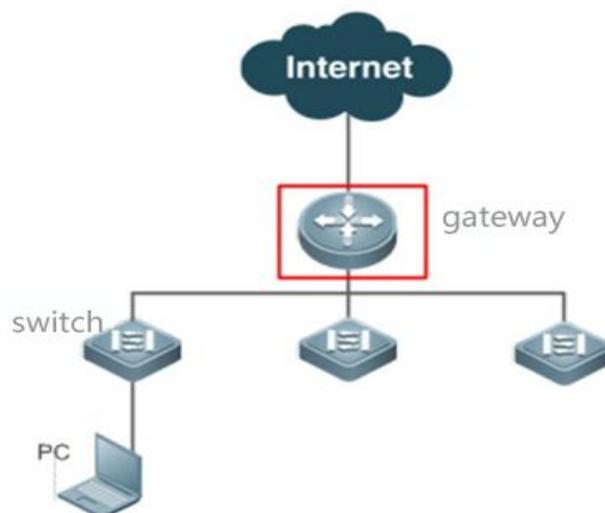
Application	Description
Web-based Management	After SG device is configured, you can access the Web management system from a browser.

1.1.1 Managing Devices via Web Management System

Scenario

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

Figure 1-1



NOTE:

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

Deployment

Configuration Environment Requirements

Client requirements:

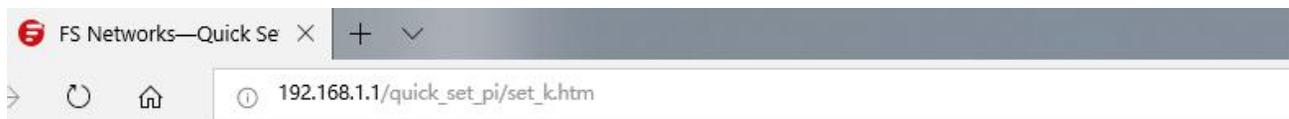
1. Network administrators can log in to the Web management UI from the browser of the Web management system client, to manage the gateway. Clients refer to PCs or other mobile terminals such as laptops.
2. Google Chrome, Firefox, IE8.0 and later versions, and some IE kernel-based browsers are supported. 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 SG egress gateway.

1.1.2 Access to Web Management UI

Step 1: Enter the IP address of the LAN interface, WAN interface, or management interface of the SG gateway 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 SG 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.

NOTE:

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.



Internet Explorer 10/11, Google Chrome, Firefox
Recommended

1. Enter the username and password and click  to access the main UI for device management.
2. If you enter the wrong username or password for five consecutive times, your account will be locked for one minute.



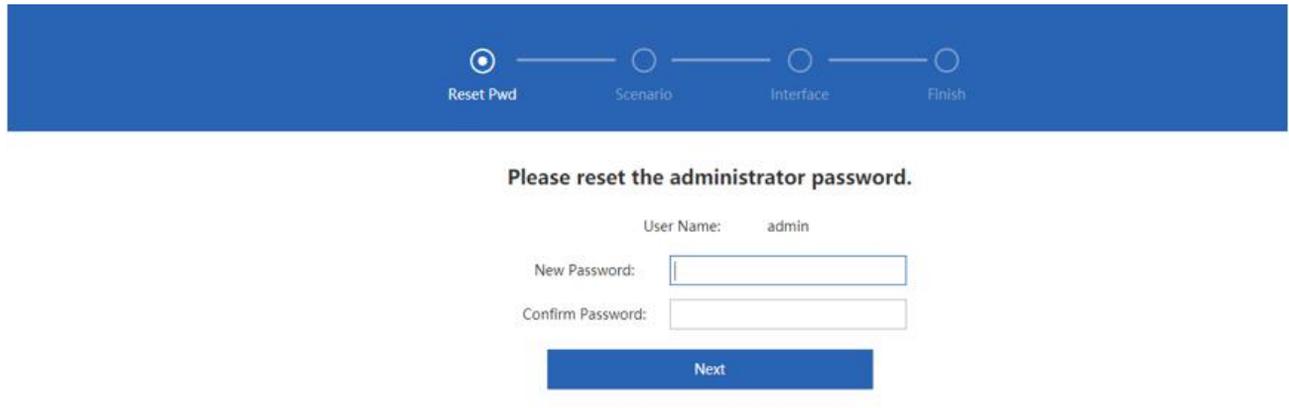
Internet Explorer 10/11, Google Chrome, Firefox
Recommended

NOTE:

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 SG 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.

1.1.3 Config Wizard

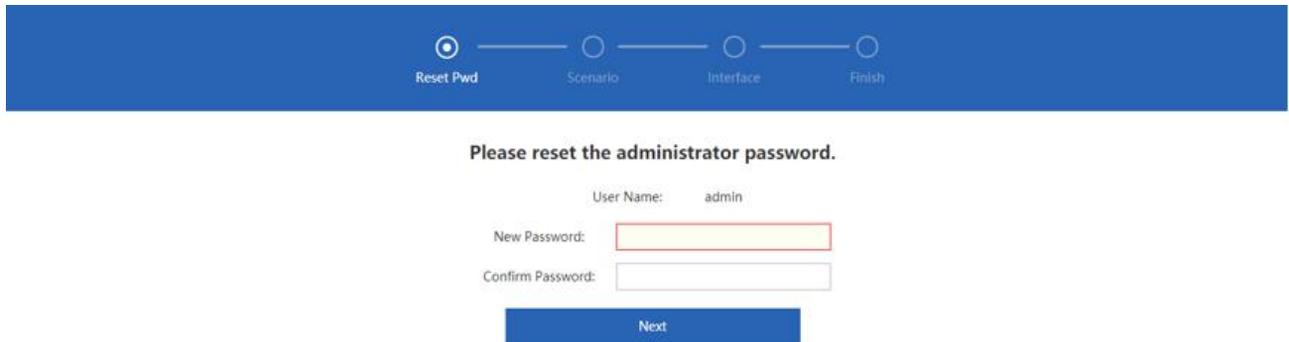
The SG device is not configured when you log in to the Web management UI for the first time. You will enter Config Wizard to reset the administrator password, select the scenario, enable smart flow control and configure WiFi.



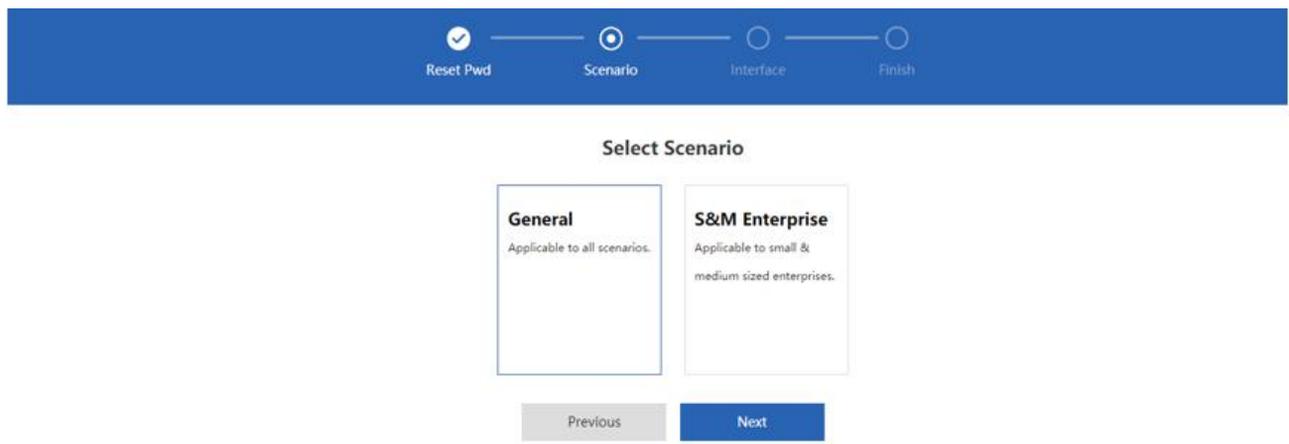
1.1.3.1 Quick Settings

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

NOTE:

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

(6) Save Configuration



Delivering...Please do not perform any operation.



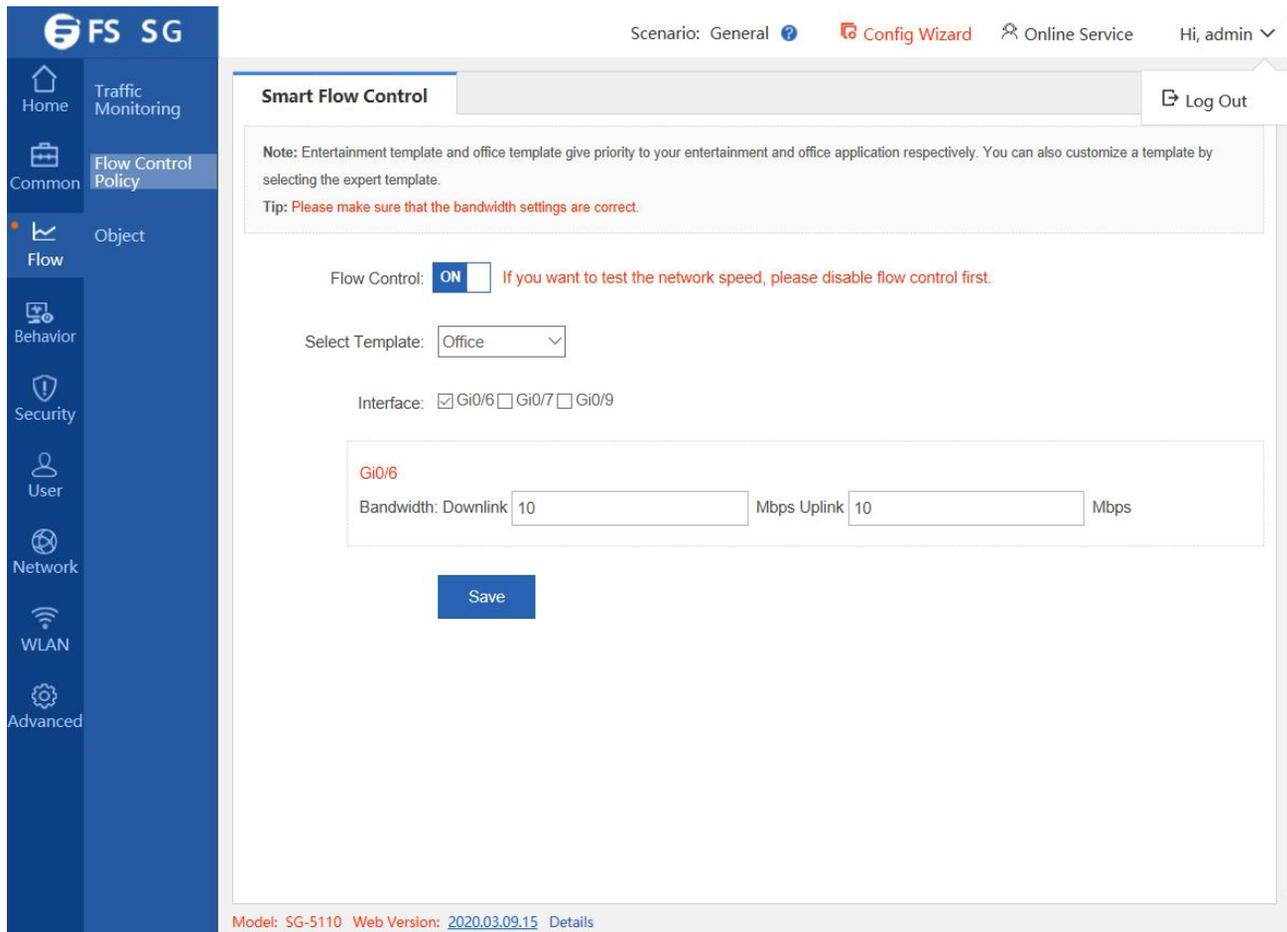
Operation succeeded.

Dashboard

Interface

1.1.4 Main UI of Web Management System

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



1.1.4.1 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 Wizard

Click  **Config Wizard**, 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.

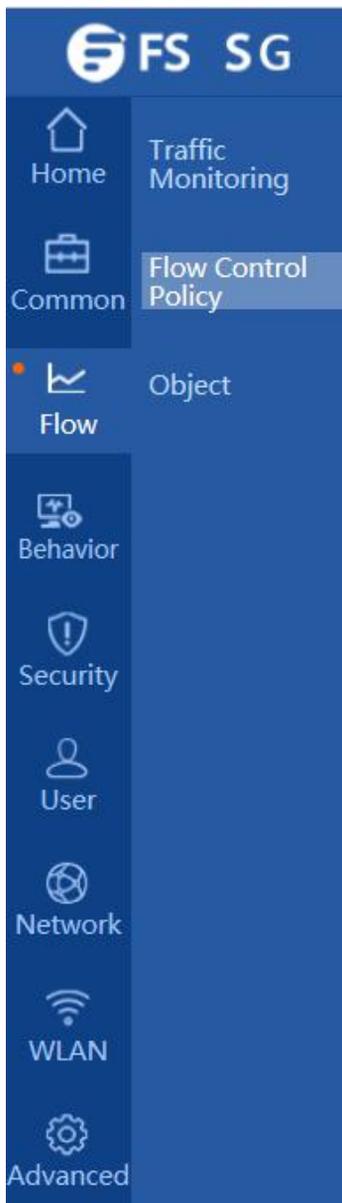
Log Out

After you complete device management, click  Log Out to exit the main UI of the Web management system of the SG device and return to the login page.

1.1.4.2 Left Area

This area lists all function menus of the SG 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.



1.1.4.3 Content Area

The Content allows you to complete function settings for the SG 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.

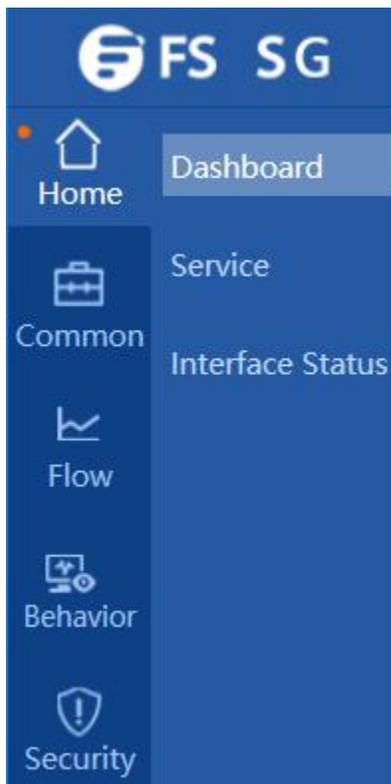
1.1.4.4 Foot Area

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.

1.1.5 Home

1.1.5.1 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.

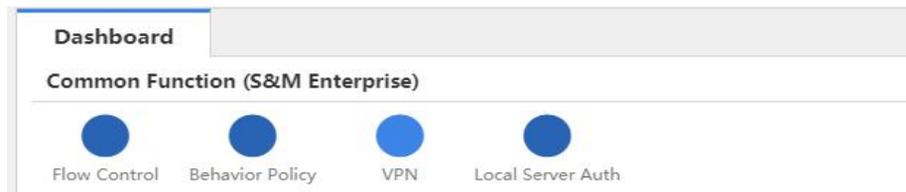


The Dashboard page displays common functions, interface information, the device CPU, memory usage, disk space, online users, system version, and system time. By analyzing the traffic trend, TOP10 applications in traffic, and TOP10 users in traffic on the current day, you can comprehensively learn about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

1.3.1.1.1 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.

1.3.1.1.2 Common Function



1.3.1.1.3 Interface Info

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

Interface Info



1.3.1.1.4 Device Info

Device Info

CPU Usage: **4.9%**

Memory Usage: **36.6%**

Online Users: **0**

Disk Space: **0.04%**

System Time: 2020-09-14 18:55:30

SG-5110 SG-5110 FSOS 11.9(1)B11S4

[Details](#)

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.

Device Info

CPU Usage: **4.8%** Memory Usage: **36.6%**

Online Users: **0** Disk Space: **0.04%**

System Time: 2020-09-14 18:58:04

SG-5110 SG-5110 FSOS 11.9(1)B11S4

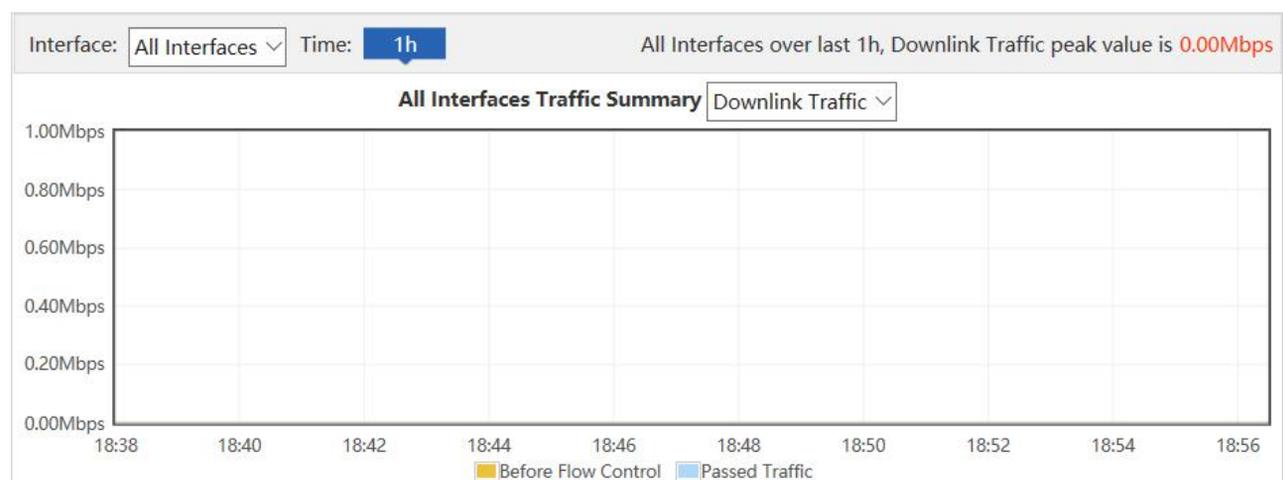
[Details](#)

Device Name: FS
 Booted on: 2020-09-14 18:37:35
 Uptime: 0:00:10:12
 Hardware Version: 1.00
 Firmware Version: SG-5110 FSOS 11.9(1)B11S4
 SN: H1P601B00001A
 MAC Address: 300D.9E81.2D53

1.3.1.1.5 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.

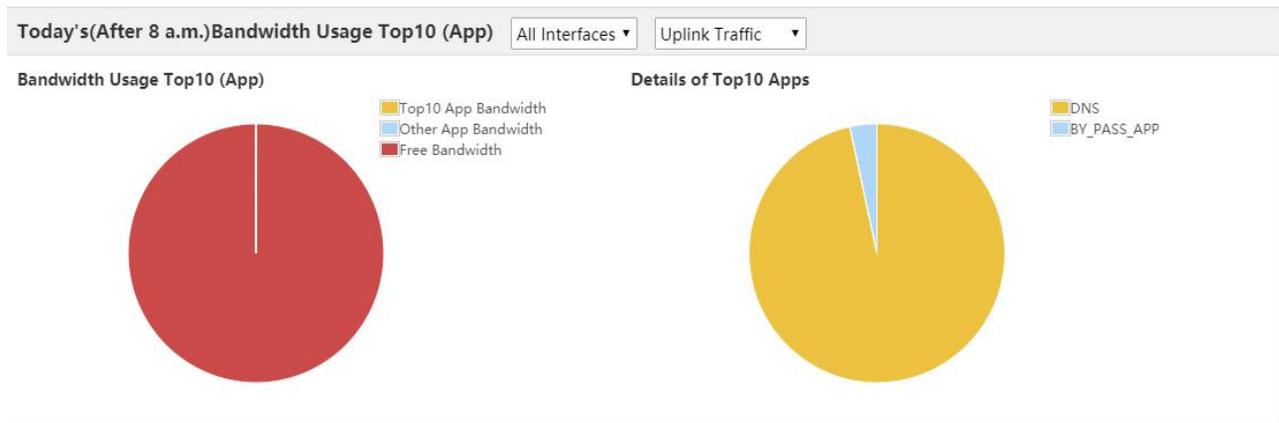
- **Interface**



- 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.

- Change the values in and to display the traffic trend of each interface on the current day.
- 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.
- Click Before Flow Control to hide the trend curve of the traffic prior to flow control and click Passed Traffic to hide the trend curve of passed traffic.

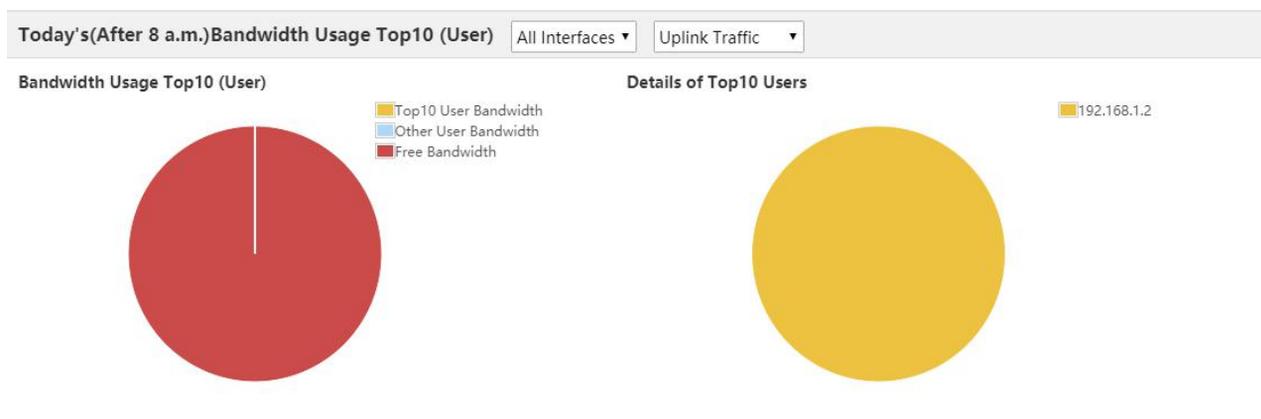
● **Today's (After 8 a.m.) Bandwidth Usage Top10 (App)**



- 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.
 - 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.
 - 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.
 - 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.
- 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.

- 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.

1.1.6 Service

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

Function Name	Status	Description	Action
Cache	Disabled	Provide resource cache, App cache, floating ADs and other functions. Note: The device will be restarted. Menu: [Cache > App Cache] [Cache > Resource Cache] [User > Floating AD]	<input type="button" value="Enable"/>
Central Management	Disabled	Support RAC-SNC central management. Menu: [Advanced > Central Management]	<input type="button" value="Enable"/>
Server Log	Disabled	Provide server log for SNC server and ELOG server. Menu: [Advanced > System Log > Server Log]	<input type="button" value="Enable"/>

1.1.7 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.

Interface	IP Address/Submask	Optical/Electrical Interface	Duplex	Speed	DNS	Status
Gi0/0	192.168.1.1/24	Electrical Interface	Auto-Negotiation	Auto-Negotiation		Connected
Gi0/1		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/2		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/3		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/4		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/5		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/6		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/7		Electrical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Gi0/9		Optical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected
Te0/0		Optical Interface	Auto-Negotiation	Auto-Negotiation		Not Connected

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

Show No.: 10 Total Count: 10

First Pre 1 Next Last 1 GO

1.1.8 Common

1.1.8.1 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

Common Functions

Common Functions

1 Change Password
Change Web & Telnet Password

2 Port Mapping
External Users Access Internal Server

3 Change Web Port
Change Device Management Port

4 Policy-Based Route
Specify a Line for an Internal Host

5 Interface Settings
Change Line or Add Line

6 Rate Limit on an IP
Set Rate Limit on an IP Address

7 User Blacklist
Deny Internal Users Access to Network

8 DHCP
Internal Users Obtains IP Addresses Automatically

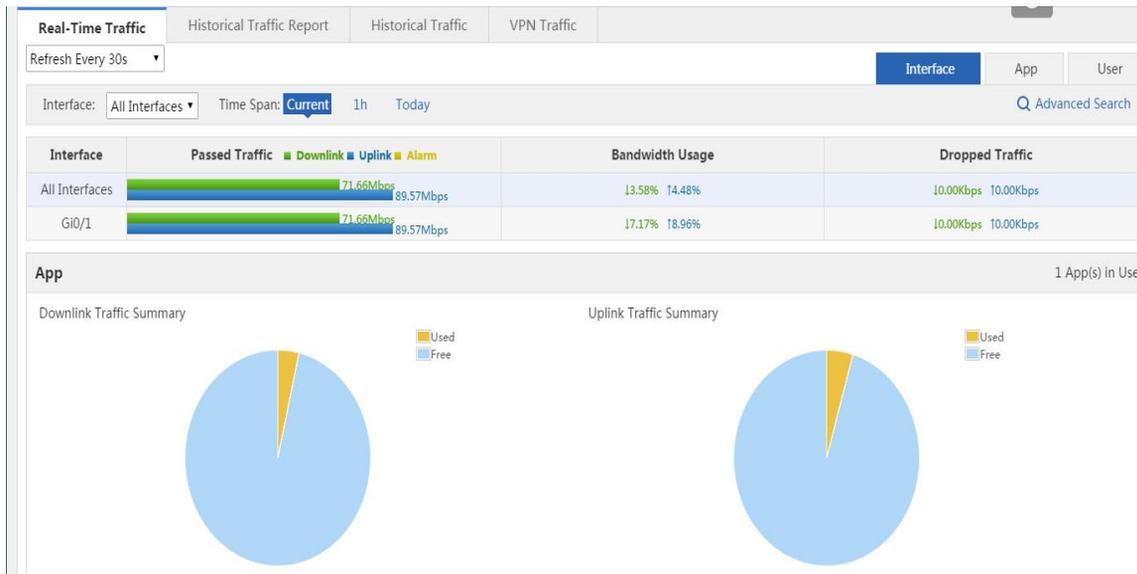
9 Common User
Custom User Object

1.1.9 Flow Control

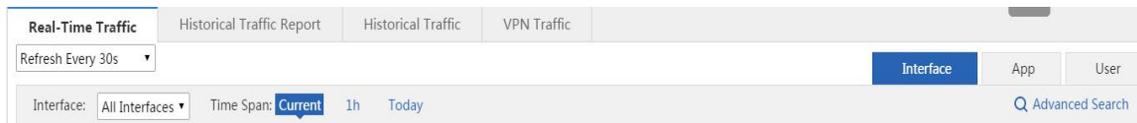
1.1.9.1 Traffic Monitoring

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

1.3.1.1.6 Real-time Traffic



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

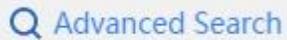


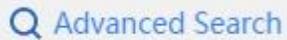
(1) Select **Refresh Every 30s** to automatically update the information about the current traffic of the device or manually update the information about the current traffic of the device.

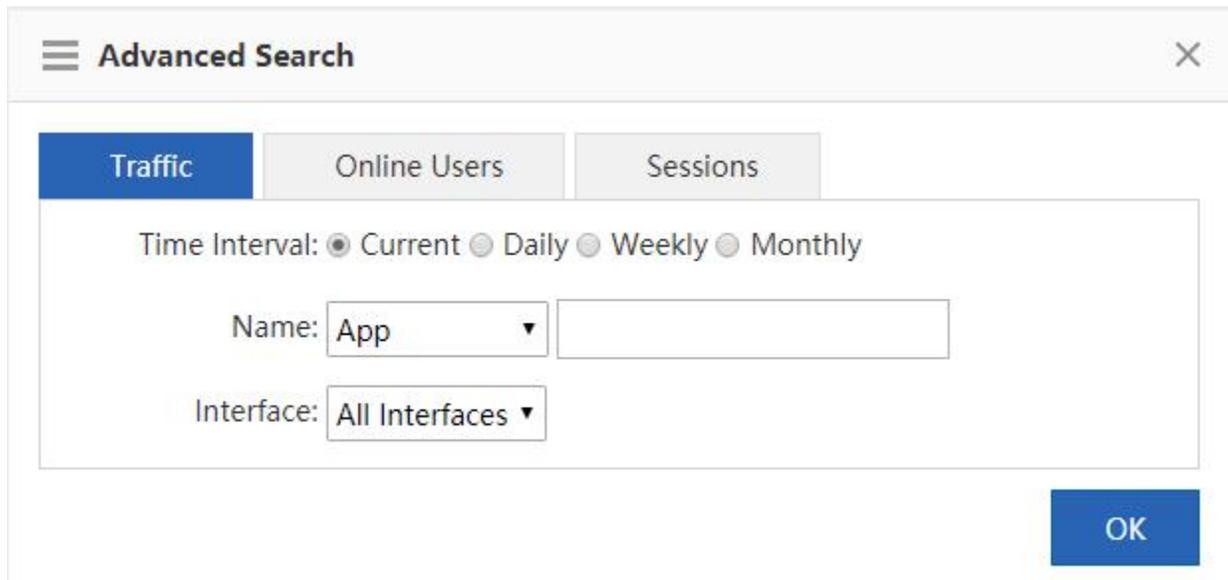
(2) Click **Interface** to display information about the device traffic by interface, application, or user.

(3) Select a line from **All Interfaces** to display traffic information of the line or select All Interfaces to display information about the total traffic of all lines.

(4) Click **Time Span: Current** to display information about the current traffic, or information about the overall traffic trend in the last one hour or on the current day. **Current** indicates that information about the current traffic is displayed.

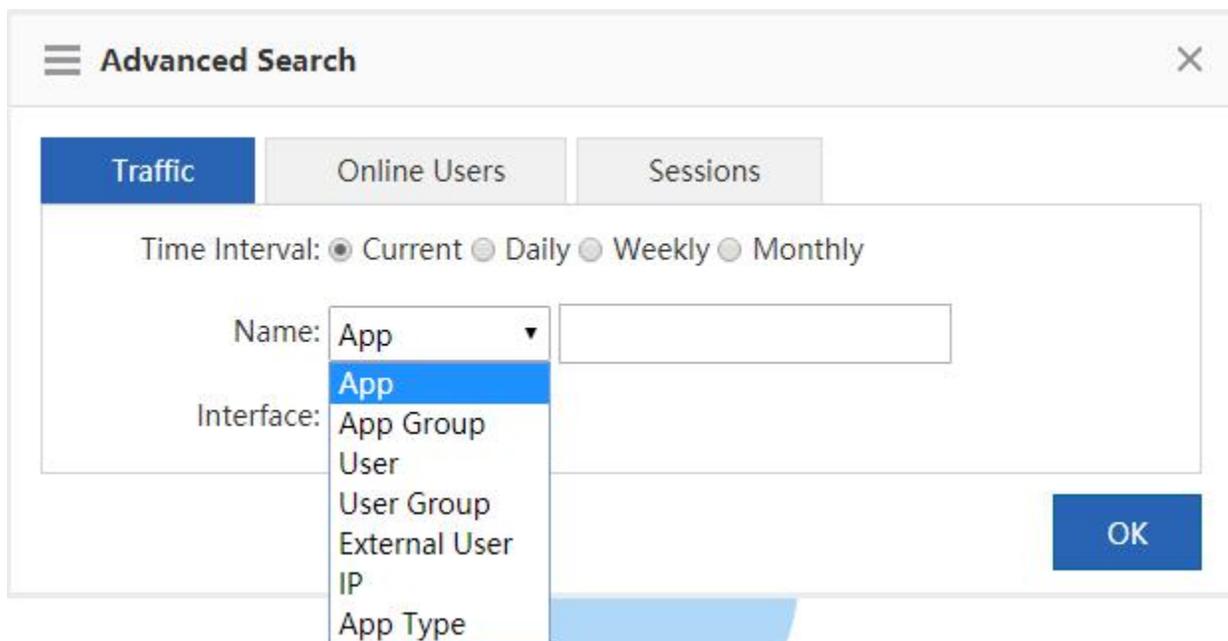


- (5) Click . A dialog box shown in the figure below is displayed. You can query details about the traffic, online users, and sessions.

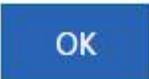


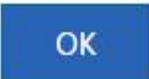
The dialog box titled "Advanced Search" has a close button (X) in the top right corner. It features three tabs: "Traffic" (selected), "Online Users", and "Sessions". Below the tabs, there is a "Time Interval" section with radio buttons for "Current" (selected), "Daily", "Weekly", and "Monthly". The "Name" field consists of a dropdown menu currently showing "App" and an adjacent text input box. The "Interface" field is a dropdown menu currently showing "All Interfaces". A blue "OK" button is located in the bottom right corner.

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.



This figure shows the "Advanced Search" dialog box with the "Name" dropdown menu open. The menu lists the following options: "App" (highlighted in blue), "App Group", "User", "User Group", "External User", "IP", and "App Type". The "Interface" dropdown menu remains set to "All Interfaces". The "OK" button is visible in the bottom right corner.



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

Real-Time Traffic | Historical Traffic Report | Historical Traffic | VPN Traffic

Search Result Q Advanced Search

Date: **Current**
 App: **All**
 Interface: **All Interfaces**

Average

No.	Name	Details	Passed Traffic	Downlink	Uplink	Dropped Traffic
Show No.: 10 Total Count: 0						

First Previous 1 Next Last GO

Traffic Details

No.	Name	IPAddress	Passed Traffic	Downlink	Uplink	Dropped Traffic
Show No.: 10 Total Count: 0						

First Previous 1 Next Last GO

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

Advanced Search X

Traffic | **Online Users** | Sessions

Time Interval: Current Daily Weekly Monthly

Interface: All Interfaces ▼

OK

OK

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

Real-Time Traffic | Historical Traffic Report | Historical Traffic | VPN Traffic

Search Result Q Advanced Search

Date: **Current**
 Interface: **All Interfaces**

User Count Summary

Average
2

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.

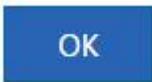
Advanced Search

Traffic Online Users **Sessions**

Time Interval: Current Daily Weekly Monthly

Time Span:

Interface:



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

Real-Time Traffic Historical Traffic Report Historical Traffic VPN Traffic

Search Result Q Advanced Search

Date: 2020.09.14

Interface: All Interfaces

Session Count Summary

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

Real-Time Traffic Historical Traffic Report Historical Traffic VPN Traffic

Refresh Every 30s

Interface App User

Interface: All Interfaces Time Span: **Current** 1h Today Q Advanced Search

Interface	Passed Traffic	Bandwidth Usage	Dropped Traffic
All Interfaces	<div style="display: flex; justify-content: space-between;"> Downlink 36.24Mbps Uplink 77.36Mbps </div>	↓1.81% ↑3.87%	↓0.00Kbps ↑0.00Kbps
Gi0/1	<div style="display: flex; justify-content: space-between;"> Downlink 36.24Mbps Uplink 77.36Mbps </div>	↓3.62% ↑7.74%	↓0.00Kbps ↑0.00Kbps

App 1 App(s) in Use

Downlink Traffic Summary

Uplink Traffic Summary

● 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).

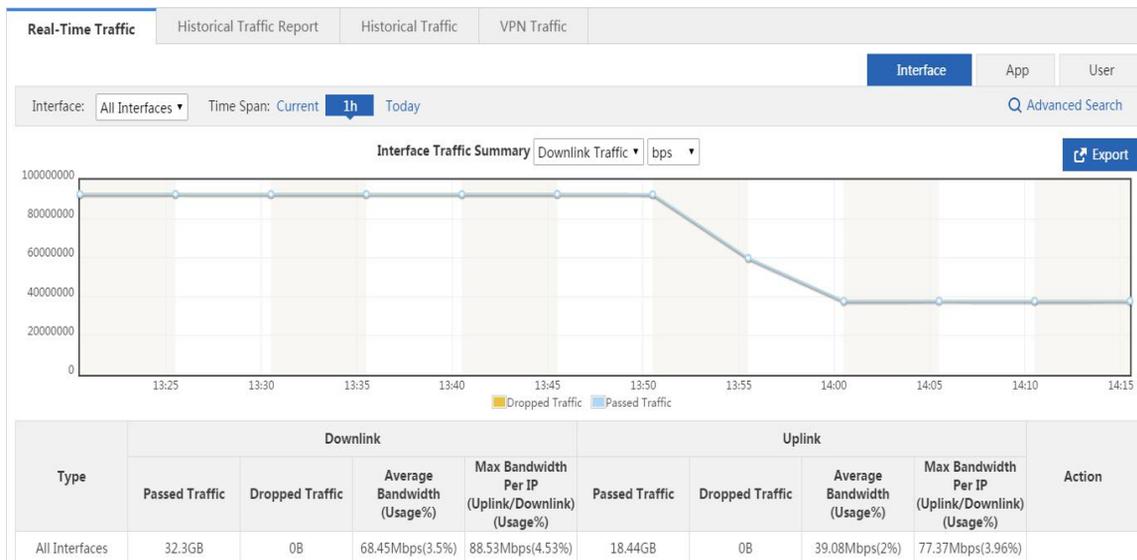
Q: How to clear a yellow alarm?

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.

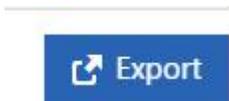
When a yellow alarm about the total traffic is generated and the bandwidth occupied by the rate-limited application group is high, limit the traffic of the rate-limited application group to prevent heavy traffic.

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



The curve in the figure above shows the traffic trend of the selected interface in the last one hour.



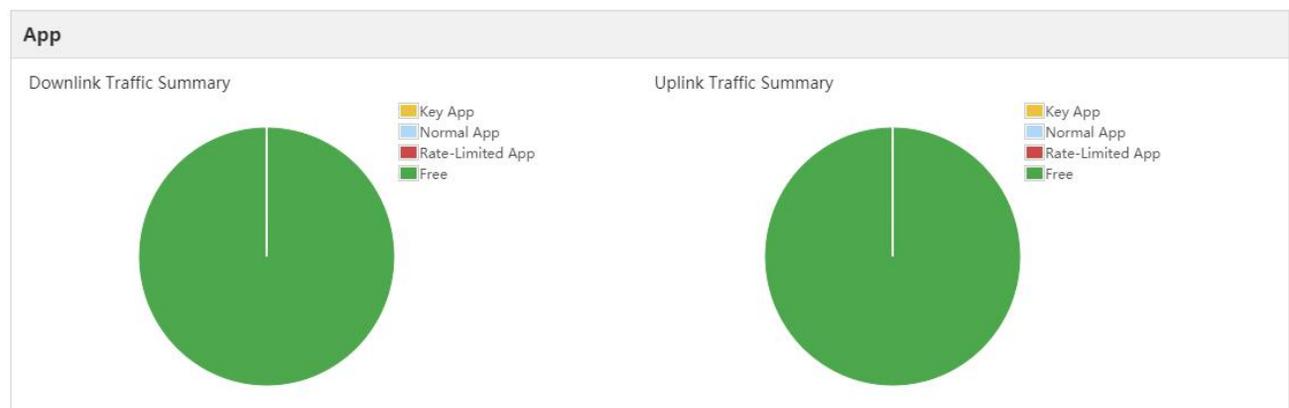
Click **Export** to export the traffic trend report to the local PC.

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

No.	Name	Details	Passed Traffic	Downlink	Uplink	Dropped Traffic
1	IP-PROTOCOL-GROUP	Details	36.24Mbps	77.38Mbps	10.00Kbps	10.00Kbps

Show No.: 10 Total Count:1

First Previous 1 Next Last 1 GO

Details

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

App Group Traffic Details - Google Chrome

172.21.6.94:9090/flow_pi/flow_appgroup_detail.htm

App Group:
IP-PROTOCOL-GROUP

Traffic(Kbps)

Interface	Downlink	Uplink	Dropped Traffic	Action
All Interfaces	37036.69	79103.33	10.00Kbps 10.00Kbps	Block

User **App**

No.	Name	Passed Traffic	Downlink	Uplink	Dropped Traffic
1	IP-PROTOCOL-GROUP/BY_PASS_APP	36.17Mbps	77.25Mbps	10.00Kbps	10.00Kbps

Show No.: 10 Total Count:1

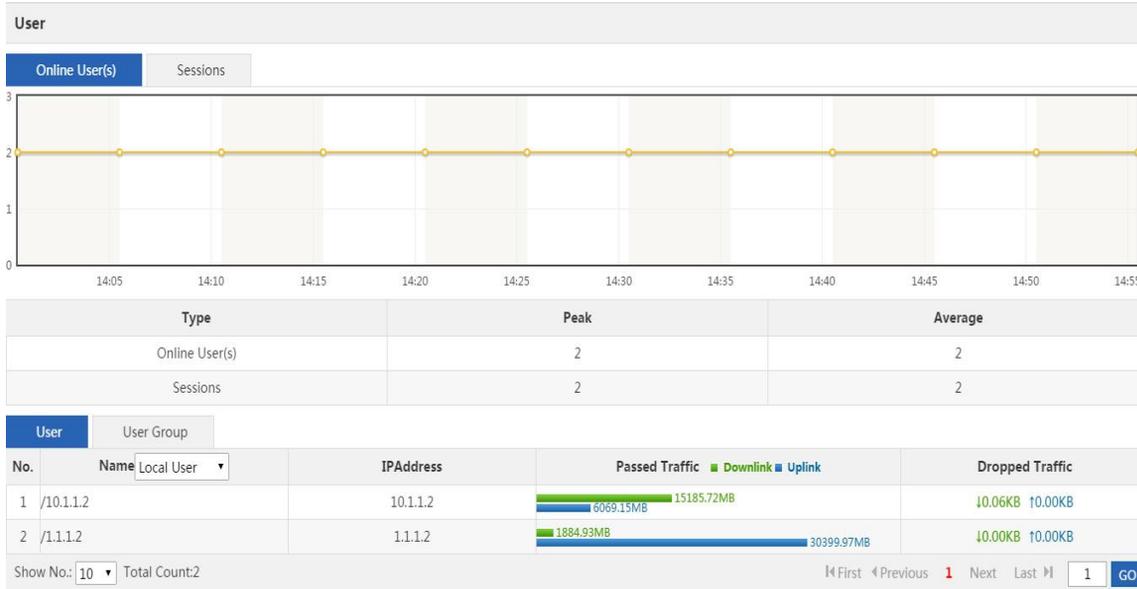
First Previous 1 Next Last 1 GO

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

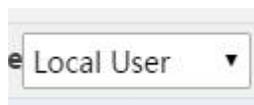
(3) User

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



The figure shows a detailed table titled 'User' with a '1 Online User(s)' indicator. It has two tabs: 'User' and 'User Group'. The table lists user traffic details:

No.	Name	Local User	IPAddress	Passed Traffic	Downlink	Uplink	Dropped Traffic
1	/10.1.1.2		10.1.1.2	6069.15MB	15185.72MB		↓0.06KB ↑0.00KB
2	/1.1.1.2		1.1.1.2	1884.93MB	30399.97MB		↓0.00KB ↑0.00KB



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.

The screenshot shows a web browser window titled 'User Traffic Details - Google Chrome' with the URL '172.21.6.94:9090/flow_pi/flow_user_detail.htm'. The page content includes:

- User Information:** Name: 10.1.1.2, Department: root.
- Traffic(Kbps):** A table with columns: Interface, Downlink, Uplink, Dropped Traffic, and Action. The row for 'All Interfaces' shows 32990.36 Kbps downlink, 13199.77 Kbps uplink, and 10.00Kbps dropped traffic. A 'Block' button is present in the Action column.
- App Flow Details:** A table with columns: No., Name, Passed Traffic (Downlink/Uplink), and Dropped Traffic. The first entry is 'IP-PROTOCOL-GROUP/BY_P ASS_APP' with 32.22Mbps downlink and 12.89Mbps uplink passed traffic, and 10.00Kbps dropped traffic. A 'Block' button is also present.
- Navigation:** 'Show No.: 10', 'Total Count:1', and pagination controls (First, Previous, 1, Next, Last) with a 'GO' button.



Click **Block** 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**

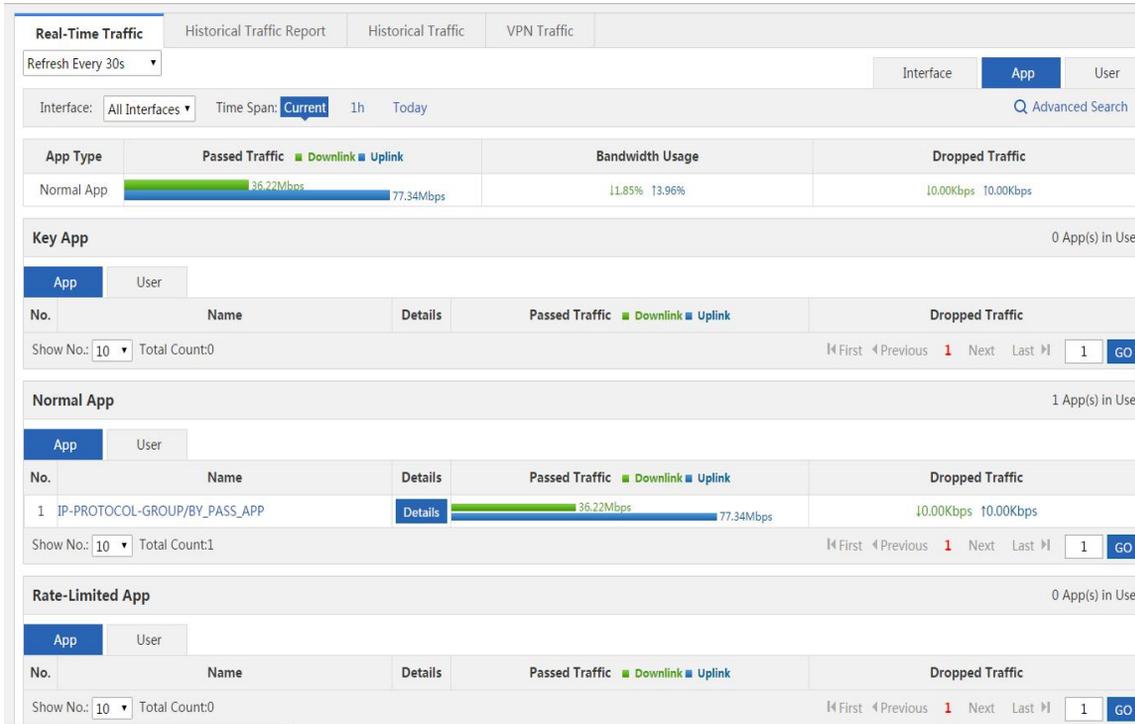
The application traffic analysis function collects statistics on the bandwidth usage of different applications. You can control and analyze



the traffic of an application to improve the traffic utilization rate. Click **App** on the **Real-Time Traffic** page. A page shown in the figures below is displayed.

The screenshot shows the top navigation and filter area of the Real-Time Traffic page. It includes:

- Refresh Every 30s dropdown.
- Navigation tabs: Interface, **App** (selected), and User.
- Interface: All Interfaces dropdown.
- Time Span: Current (selected), 1h, Today.
- Advanced Search icon and text.



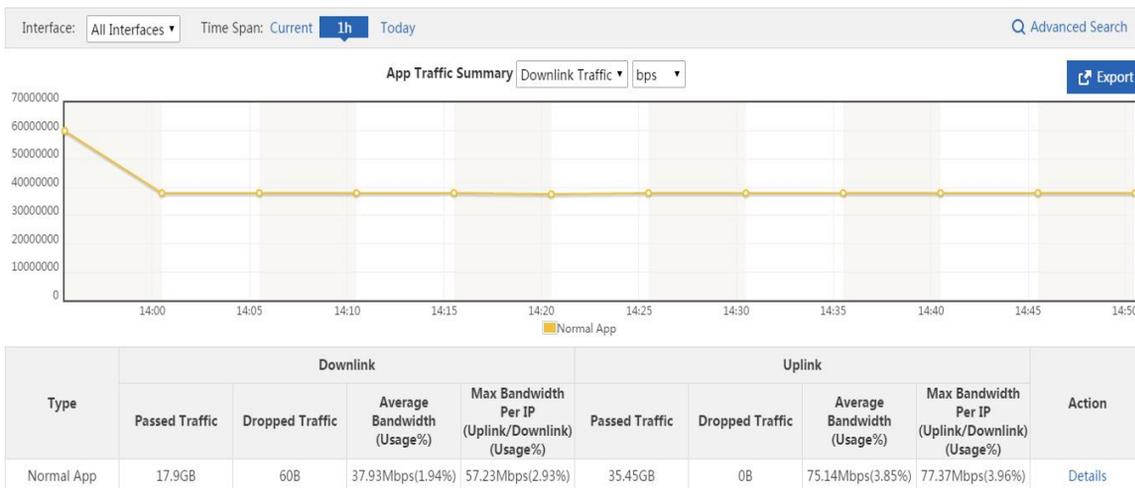
➤ **Overview:** The top area of the page displays information about the traffic of all interfaces, traffic of key applications, normal applications, and rate-limited applications.



(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



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 **Export** 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.

Key App					
App					
No.	Name	Passed Traffic	Downlink	Uplink	Dropped Traffic
Show No.: 10 Total Count:0					First Previous 1 Next Last 1 GO

Normal App					
App					
No.	Name	Passed Traffic	Downlink	Uplink	Dropped Traffic
1	IP-PROTOCOL-GROUP/BY_PASS_APP	<div style="width: 100%;"><div style="width: 100%;"></div></div> 17896.95MB		35454.55MB	↓0.06KB ↑0.00KB
Show No.: 10 Total Count:1					First Previous 1 Next Last 1 GO

Rate-Limited App					
App					
No.	Name	Passed Traffic	Downlink	Uplink	Dropped Traffic
Show No.: 10 Total Count:0					First Previous 1 Next Last 1 GO



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 key applications. Click **User** in **App**. Then, information about the traffic of users who are using the key applications on the interface is displayed.

App		User						
No.	Name	Local User	IPAddress	Details	Passed Traffic	Downlink	Uplink	Dropped Traffic
1	/192.168.1.46		192.168.1.46	Details	12.01Kbps			↓0.00Kbps ↑0.00Kbps
2	/192.168.1.2		192.168.1.2	Details	0.53Kbps			↓0.00Kbps ↑0.00Kbps
3	/192.168.1.41		192.168.1.41	Details	0.03Kbps			↓0.00Kbps ↑0.00Kbps
4	/10.168.195.208		10.168.195.208	Details	0.00Kbps			↓0.00Kbps ↑0.00Kbps
Show No.: 10 Total Count:4					First Previous 1 Next Last 1 GO			



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

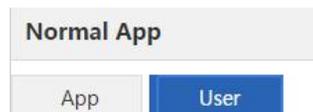
- 2. Normal Applications: The area displays the details about the running normal applications on the selected interface, traffic of each

application, details about users who are using the normal applications, and traffic of each user.

Normal App						1 App(s) in Use	
App		User					
No.	Name	Details	Passed Traffic		Dropped Traffic		
1	IP-PROTOCOL-GROUP/BY_PASS_APP	Details	36.22Mbps	77.32Mbps	10.00Kbps	10.00Kbps	

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

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

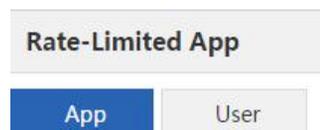
Normal App						1 App(s) in Use		
App		User						
No.	Name	Local User	IPAddress	Details	Passed Traffic		Dropped Traffic	
1	/10.1.1.2		10.1.1.2	Details	12.89Mbps	32.22Mbps	10.00Kbps	10.00Kbps
2	/1.1.1.2		1.1.1.2	Details	4.00Mbps	64.42Mbps	10.00Kbps	10.00Kbps

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

- 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.

Rate-Limited App						0 App(s) in Use	
App		User					
No.	Name	Details	Passed Traffic		Dropped Traffic		
Show No.: 10 Total Count:0 First Previous 1 Next Last H 1 GO							

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.

Rate-Limited App						0 App(s) in Use	
App		User					
No.	Name	Details	Passed Traffic		Dropped Traffic		

Details

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.

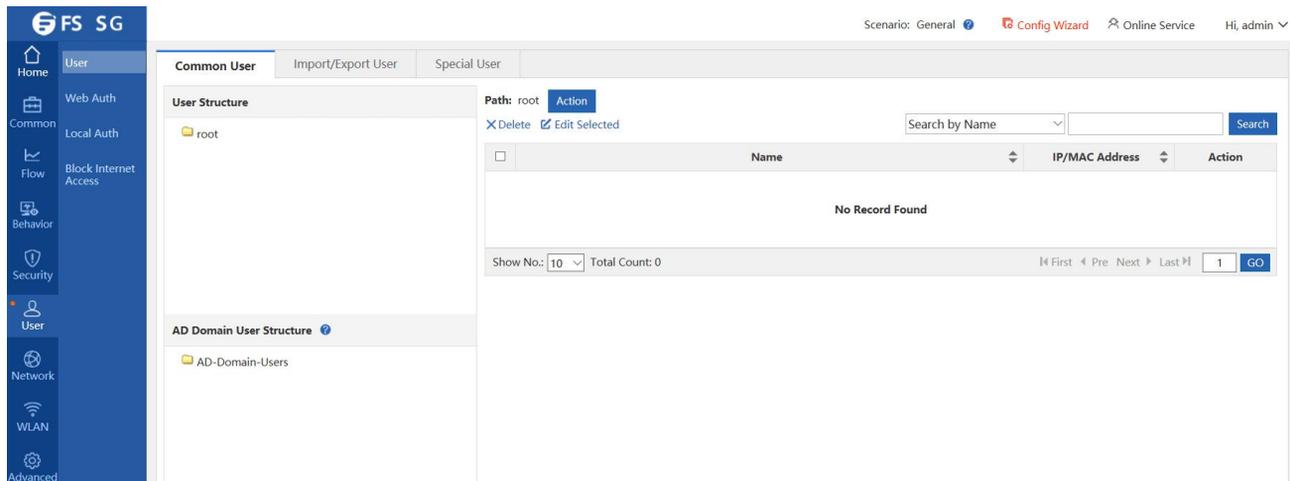
Details

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 SG device displays the traffic information and manages traffic by user group.



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



1.3.1.1.7 Historical Traffic Report

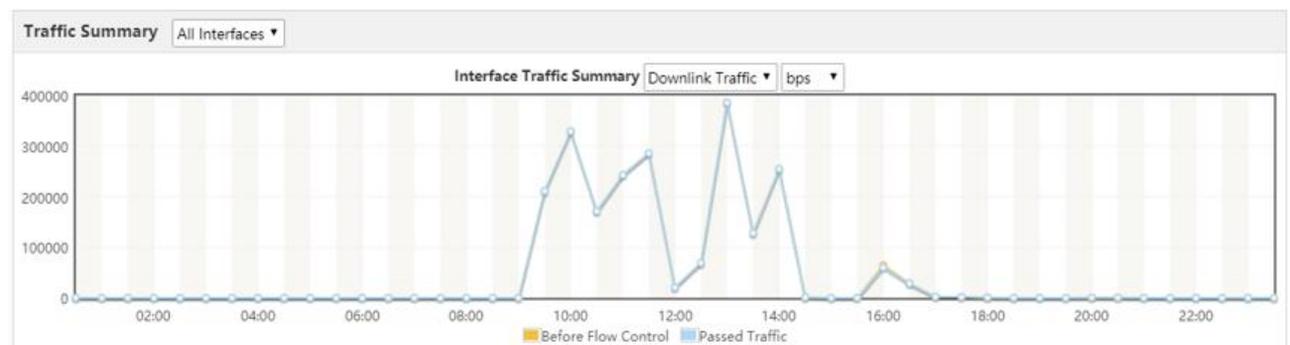
Type	Created on	Downlink Traffic	Uplink Traffic	Average Bandwidth Usage	Max Online Users	Max Sessions	Action
Daily Report							
Compared with Last Daily Report							
Weekly Report							
Compared with Last Weekly Report							
Monthly Report							
Compared with Last Monthly Report							

Note: The system only saves daily reports over last 60 days, weekly reports over last 8 weeks and monthly reports over last 12 months.

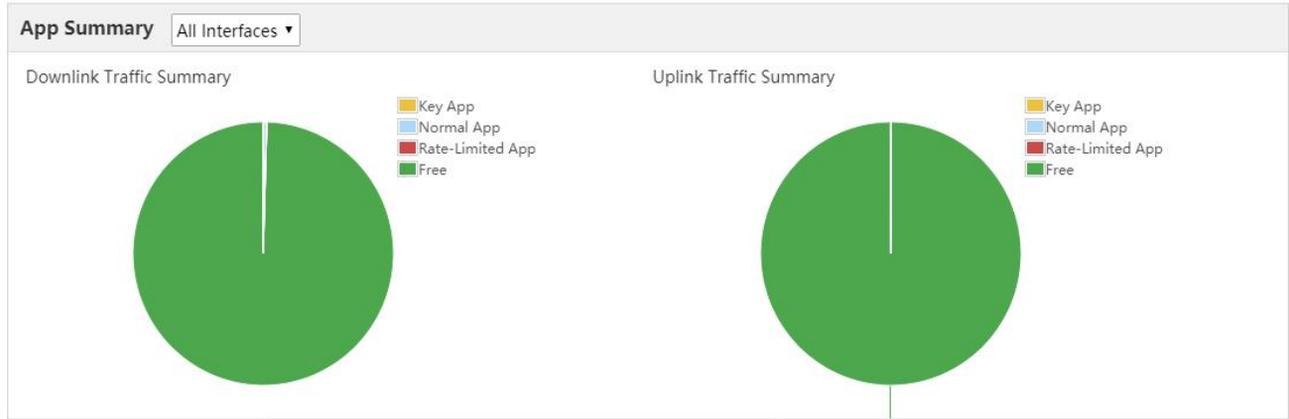
This page allows you to view daily reports in the last 60 days.

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	Dropped Traffic
1	NetworkManagementProtocol/DNS	↑2.75KB 179.55KB	↓0.00KB ↑0.00KB

Show No.: 10 ▾ Total Count:1 First Previous 1 Next Last 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	<div style="font-size: x-small; display: flex; justify-content: space-between;">66.53MB469.21MB</div>	↓0.00KB 10.00KB
2	/group10/ap1_user	192.168.10.2	<div style="font-size: x-small; display: flex; justify-content: space-between;">20.56MB12.09MB</div>	↓1.06MB 10.00KB
3	/group10/ap1_user	192.168.10.11	<div style="font-size: x-small; display: flex; justify-content: space-between;">1.38MB315.53KB</div>	↓0.00KB 10.00KB
4	/group10/ap1_user/test1222	192.168.10.10	<div style="font-size: x-small; display: flex; justify-content: space-between;">1.09MB227.57KB</div>	↓0.00KB 10.00KB
5	/192.168.1.8	192.168.1.8	<div style="font-size: x-small; display: flex; justify-content: space-between;">614.46KB87.15KB</div>	↓0.00KB 10.00KB

1.13GB
-56.25%

173.72MB
-60.04%

Downlink:102Kbps(1.02%)
Uplink:15.71Kbps(0.16%)

6
-33.33%

942
-83.65%

Details

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.

Overview
Advanced Search

Report Type: Daily Report Weekly Report Monthly Report

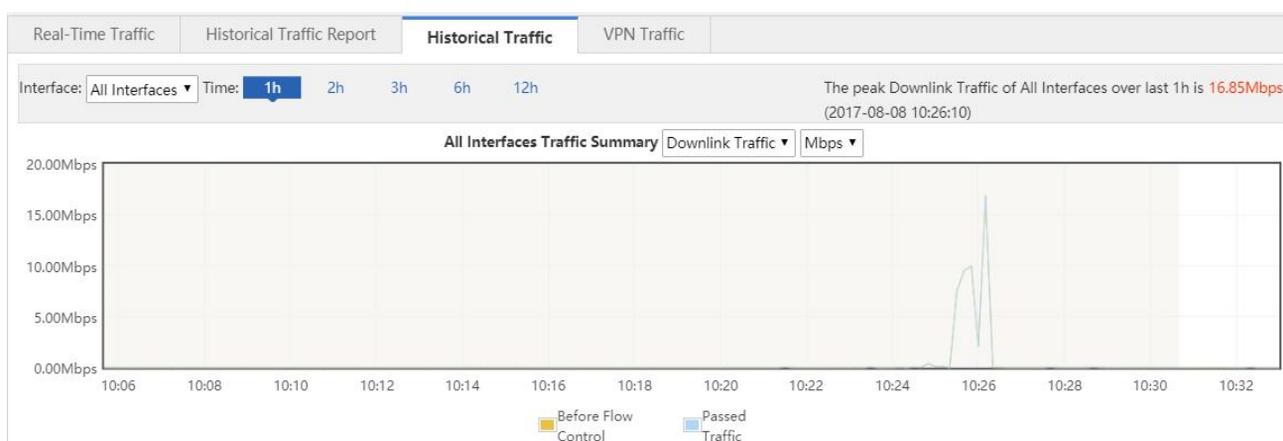
2017-08-03
Comparison (VS)
2017-08-02

Traffic Summary
All Interfaces ▾
Downlink Traffic ▾
bps ▾

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](#)

1.3.1.1.8 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.

1.3.1.1.9 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.

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

Advanced Search

Time Interval: Current Daily Weekly Monthly

Time Span: Real-Time

Name/IP:

Interface:

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

No.	User Name	IP Address	Details	Passed Traffic	Dropped Traffic
	External User			<input type="checkbox"/> Downlink <input type="checkbox"/> Uplink	

Show No.: Total Count:0

1.1.9.2 Flow Control Policy

1.3.1.1.10 Smart Flow Control

Smart Flow Control

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

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

Select Template:

Interface: Gi0/6 Gi0/7 Gi0/9

Gi0/6

Bandwidth: Downlink Mbps Uplink Mbps

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.

1.3.1.11 Change Policy

Smart Flow Control **Change Policy** Change Parameter Change App VPN Flow Control

Note: Flow control is used to regulate flow traffic of different users, networks and applications.
Tip: The advanced flow control policy of the previous version may not be displayed completely here. It is recommended to perform settings in Config Wizard first.

+Add Policy X Delete Selected Interface: GIO/1

<input type="checkbox"/>	Policy Name	Local User	External User	External IP	App Group	VPN	Time	Flow Control	Priority	Enable	Status	Action
<input type="checkbox"/>	testPolicy	Vpn_Group	All Users	All External IPs	All	No	Any Time	Parameter		<input checked="" type="checkbox"/>	Active	Copy Edit Delete

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

- **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.

Add Policy X

Policy Name:

User: All Users [Local User](#) All Users [External User](#)

Select App Group: [Custom App Group](#)

Flow Limit: Bandwidth Limit (Kbps) ?

Max Downlink: Guaranteed Min Downlink: Max Downlink Per IP:

Max Uplink: Guaranteed Min Uplink: Max Uplink Per IP:

No Rate Limit

[Advanced Settings](#)

Save

No Rate Limit

[Advanced Settings](#)

External IP Group: All External IPs [Select IP Group](#)

Active Time: [Time Management](#)

VPN Flow Control: Match VPN Traffic (If you select this option, this policy is applied to only VPN users)

Save

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](#)

+ Add App Group Help Identify App

App Group Name	Selected App	Action
Key App	DNS,Voip,Vpn-app	Edit
Web Page	HTTP,HTTPS,Web_MOBILE	Edit
Online Video	HTTP-VIDEO,Video_MOBILE	Edit
P2P Video Streaming	STREAMING	Edit
Download	HTTP-DOWNLOAD,FTP,TFTP,NNTP,IXIA,SVN,SMB,DownloadTools_MOBILE,OnlineStorage	Edit
P2P Download	P2P	Edit
App Update		Edit
Upload	HTTP-UPLOAD	Edit
Rate-Limited App	Games	Edit
Blocked	DNS-ILLEGAL	Edit
Normal App	Chat,FileTransfer,E-Mail,Database,NetworkManagementProtocol,Routing,Security,REMOTE-PROTOCOL,SoftwareUpdate,OnlineBank,InstantMessaging_MOBILE,Game_MOBILE,Social_contact_MOBILE,OA_office,Video_conferencing,OnlinePayment Ban	The default group cannot be edited

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

4. **External IP Group:** Click [Select IP Group](#) to select an IP group.

[Time Management](#)

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

● **Viewing a policy**

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

Note: Flow control is used to regulate flow traffic of different users, networks and applications.
 Tip: The advanced flow control policy of the previous version may not be displayed completely here. It is recommended to perform settings in Config Wizard first.

+ Add Policy X Delete Selected Interface: GI0/1

<input type="checkbox"/>	Policy Name	Local User	External User	External IP	App Group	VPN	Time	Flow Control	Priority	Enable	Status	Action
<input type="checkbox"/>	testPolicy	Vpn_Group	All Users	All External IPs	All	No	Any Time	Parameter		<input checked="" type="checkbox"/>	Active	Copy Edit Delete

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

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 to edit a policy.

6. Click to delete a policy.

● **Copying a policy**

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



1.3.1.1.12 Change Parameter

You can edit settings according to real condition.

Tip: The unit of the following rate is Kbps. A small value indicates a high priority.

REMOTE_CONF_1 Usage: 0% Threshold: 80 % (Range: 1-99)

Reserved Bandwidth (Range: 1%-80%) Uplink Bandwidth (Total: 10M): 20% Downlink Bandwidth (Total: 10M): 50%

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	
Web Page	1	0/0	2,000	7,000	2,000	7,000	50	300	--	5,000	
Normal App	4	0/0	1,000	9,000	1,000	9,000	--	--	--	5,000	
Upload	4	0/0	--	9,000	--	9,000	500	8,100	--	--	
Online Video	5	0/0	500	9,000	500	9,000	50	300	--	5,000	
Download	6	0/0	--	9,000	--	9,000	20	2,000	--	--	
P2P Video Streaming	6	0/0	--	9,000	--	9,000	50	600	--	5,000	
App Update	6	0/0	--	9,000	--	9,000	50	500	--	--	
Rate-Limited App	6	0/0	500	9,000	500	9,000	--	600	--	5,000	
P2P Download	7	0/0	--	9,000	--	9,000	20	300	--	5,000	

1.3.1.1.13 Change App

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

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

Entertainment App Template

App Group Name	Selected App	Action
Key App	DNS,Voip ,Vpn-app	Edit
Web Page	HTTP,HTTPS ,Web_MOBILE	Edit
Online Video	HTTP-VIDEO,Video_MOBILE	Edit
P2P Video Streaming	STREAMING	Edit
Download	HTTP-DOWNLOAD,FTP,TFTP,NNTP,IXIA,SVN,SMB,DownloadTools_MOBILE ,OnlineStorage	Edit
P2P Download	P2P	Edit
App Update		Edit
Upload	HTTP-UPLOAD	Edit
Rate-Limited App	Games	Edit
Blocked	DNS-ILLEGAL	Edit
Normal App	Chat,FileTransfer ,E-Mail ,Database ,NetworkManagementProtocol ,Routing ,Security ,REMOTE-PROTOCOL ,SoftwareUpdate ,OnlineBank ,InstantMessaging_MOBILE ,Game_MOBILE ,Social_contact_MOBILE ,OA_office ,Video_conferencing ,OnlinePayment Bank_MOBILE ,RFC ,ICMP-DETAIL ,IP-RAW ,IP-PROTOCOL-GROUP	The default group cannot be edited

Show No.: 15 Total Count:11 First Previous 1 Next Last GO

1.3.1.1.14 VPN Flow Control

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

VPN Flow Control: Gi0/3 Gi0/1

VPN application will be given top priority

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

[Save](#)

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

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

VPN Flow Control: Gi0/3 Gi0/5 Gi0/7 Gi0/1

VPN application will be given top priority

Q

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

VPN Bandwidth [View/Edit](#) (Note: Enable VPN flow control before configuring VPN bandwidth)

[Save](#)

1.1.9.3 Object

The object configuration page is shown in the figure below.

Custom App			Custom Website	Time Object	External IP Object	VLAN Object	IP Object
+ Add App Group + Custom App Help Identify 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_MOBIL	Edit					

1.3.1.15 Custom App

Custom App			Custom Website	Time Object	External IP Object	VLAN Object	IP Object
+ Add App Group + Custom App Help Identify 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_MOBIL	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.

1. 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.

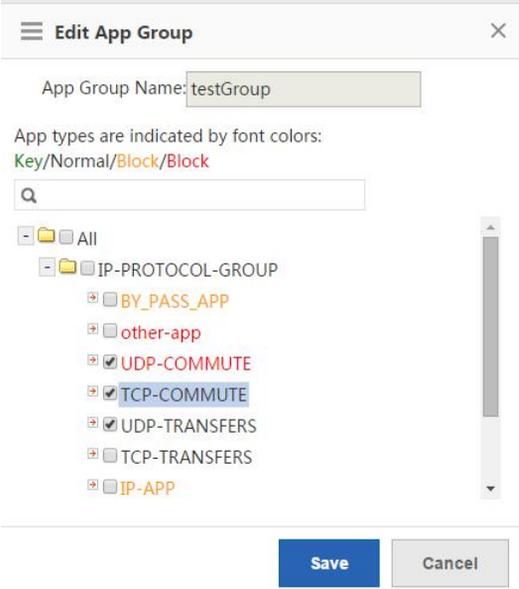
Normal App	IP-PROTOCOL-GROUP,TCP-COMMUTE,UDP-TRANSFERS,ICMP,OTHER-UDP,OTHER-TCP,Stock,Database,NetworkMGR,Routing,REMOTE-PROTOCOL,SoftwareUpdate,OnlineBank,Web_MOBILE,Online_shopping_MOBILE,Securities_MOBILE,OnlinePayment Bank_MOBILE,RFC,IP-RAW,OA_office,Video_conferencing	Edit
App	other-app, UDP-COMMUTE	Edit Delete
testGroup	UDP-COMMUTE, TCP-COMMUTE, UDP-TRANSFERS	Edit Delete

Show No.: 30 Total Count:13 First Previous 1 Next Last 1 GO

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

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  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 . The custom application configuration page is displayed.

Tip: The application name cannot be longer than 27 characters

App Name:

Protocol Type: Rule Type:

App Group: Custom Select

Src IP:

Dest IP:

App Name	Protocol Type	App	Src Port	Dest Port	Src IP	Dest IP	Action
qiqiao	tcp	123	All Ports	All Ports	1.1.1.1	1.1.1.10	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.: Total Count:1
 1

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 .

1.3.1.1.16 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.

[+ Add Website Group](#) [Custom Website](#) [System Website](#) [Search Website](#)

Website Group Name	Website	Action
Portal-Navigation	Portal-Navigation	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
keyObject	keyUrlClass	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
illegal	forbidClass,Violence,Virus,Adult,Gambling,Crime,undefined	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

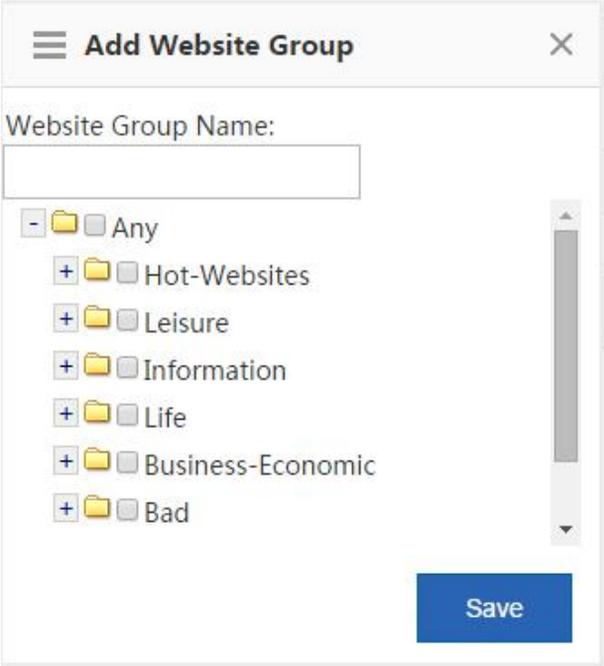
Show No.: Total Count:3
 1

- **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.

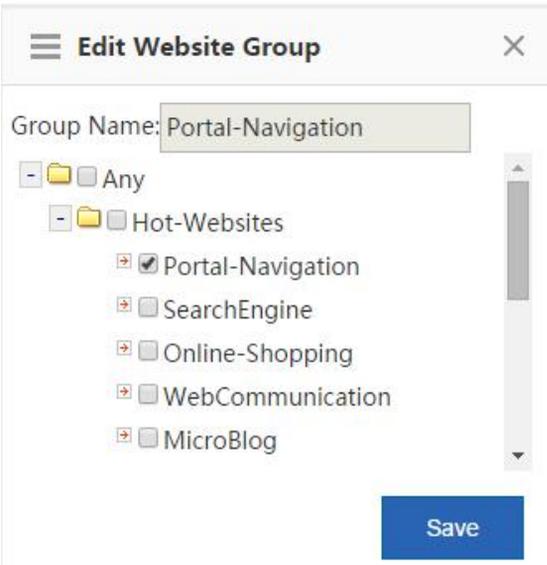


The dialog box titled "Add Website Group" has a close button (X) in the top right corner. It contains a text input field for "Website Group Name:". Below the input field is a tree view of website categories. The categories are: "Any" (with a minus sign), "Hot-Websites" (with a plus sign), "Leisure" (with a plus sign), "Information" (with a plus sign), "Life" (with a plus sign), "Business-Economic" (with a plus sign), and "Bad" (with a plus sign). A blue "Save" button is located at the bottom right of the dialog.

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

2. 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.



The dialog box titled "Edit Website Group" has a close button (X) in the top right corner. It contains a text input field for "Group Name:" with the value "Portal-Navigation". Below the input field is a tree view of website categories. The categories are: "Any" (with a minus sign), "Hot-Websites" (with a minus sign), "Portal-Navigation" (with a plus sign and a checked checkbox), "SearchEngine" (with a plus sign), "Online-Shopping" (with a plus sign), "WebCommunication" (with a plus sign), and "MicroBlog" (with a plus sign). A blue "Save" button is located at the bottom right of the dialog.

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

3. Deleting a website group

Click  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.

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

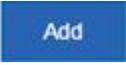
Website Name + Description:

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

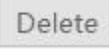


Custom Website List

Website Name	URL	Description	Action
un_audit_class	163.com, facebook.com	unaudit	 

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 . 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 .

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

1.3.1.17 Time Object

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

Custom App	Custom Website	Time Object	External IP Object	VLAN Object	IP Object
<p>Note: The time object refers to the time when the policy is active.</p>					
<p>+ Add Object X Delete Selected</p>					
<input type="checkbox"/>	Time Object	Time Interval	Time Span	Action	
<input type="checkbox"/>	Any Time	Every Day	0:00-23:59	Edit	Delete
<input type="checkbox"/>	Daytime	Every Day	6:00-18:00	Edit	Delete
<input type="checkbox"/>	Nighttime	Weekday	0:00-5:59	Edit	Delete
<input type="checkbox"/>	Off-Working Hours	Every Day	18:01-23:59	Edit	Delete
<input type="checkbox"/>		Weekday	0:00-7:59	Edit	Delete
<input type="checkbox"/>		Weekday	12:00-13:00	Edit	Delete
<input type="checkbox"/>	Weekend	Weekday	18:01-23:59	Edit	Delete
<input type="checkbox"/>		Weekend	0:00-23:59	Edit	Delete
<input type="checkbox"/>	Working Hours	Weekday	8:00-12:00	Edit	Delete
<input type="checkbox"/>		Weekday	13:00-18:00	Edit	Delete
<input type="checkbox"/>	Workday	Weekday	0:00-23:59	Edit	Delete

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

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

+ Add Object
X

Object Name: *

Time Span: Select ▼ Start Time ~ End Time X + Add

Save
Cancel

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**.

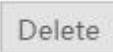
Note: The time object refers to the time when the policy is active.

+Add Object X Delete Selected

<input type="checkbox"/>	Time Object	Time Interval	Time Span	Action
<input type="checkbox"/>	Any Time	Every Day	0:00-23:59	Edit Delete
<input type="checkbox"/>	Daytime	Every Day	6:00-18:00	Edit Delete
<input type="checkbox"/>	Nighttime	Weekday Every Day	0:00-5:59 18:01-23:59	Edit Delete
<input type="checkbox"/>	Off-Working Hours	Weekday Weekday	0:00-7:59 12:00-13:00 18:01-23:59	Edit Delete
<input type="checkbox"/>	Weekend	Weekend	0:00-23:59	Edit Delete
<input type="checkbox"/>	Working Hours	Weekday Weekday	8:00-12:00 13:00-18:00	Edit Delete
<input type="checkbox"/>	Workday	Weekday	0:00-23:59	Edit Delete

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

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  .

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

Object Name: *

Time Span:

Monday, Tuesday, ▼	0:00	~	5:59		
Monday, Tuesday, ▼	18:01	~	23:59		

1.3.1.18 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.

≡ Edit User Group ✕

User Group: *

Parent 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.

≡ Add Group ✕

User Group: *

Parent Group:

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

≡ Add User (IP Range) ✕

User Name: *

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

Parent Group:



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

Add User
✕

User Name: *

IP Address: *

Add

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

Custom App
Custom Website
Time Object
External IP Object
VLAN Object
IP Object

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

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

- Any
 - Out_Server
 - 112
 - 233
 - 8888
 - 122

You can perform the following operations on **112**:

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

112 User List ✕ Delete Selected

	User Name	IP Address	Action
<input type="checkbox"/>	mmmmm	182.168.2.3	Edit Delete
<input type="checkbox"/>	555	172.31.61.25	Edit Delete

Show No.: Total Count:2

⏪ First
⏴ Previous
1
Next
⏵ Last
⏩
 GO

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

Edit User
✕

User Name: *

IP Range: *

Parent Group:

Save

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

www.fs.com

47

1.3.1.1.19 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.

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

VLAN Object Name: *

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

Add

[X Delete All](#)

VLAN Object Name	VLAN Object ID	Action
1	1	Edit Delete
2	2	Edit Delete

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

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**.

VLAN Object Name: *

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

Save **Cancel Edit**

[X Delete All](#)

VLAN Object Name	VLAN Object ID	Action
1	1	Edit Delete
2	2	Edit Delete

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

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 [X Delete All](#).

1.1.10 Behavior Management

1.1.10.1 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.

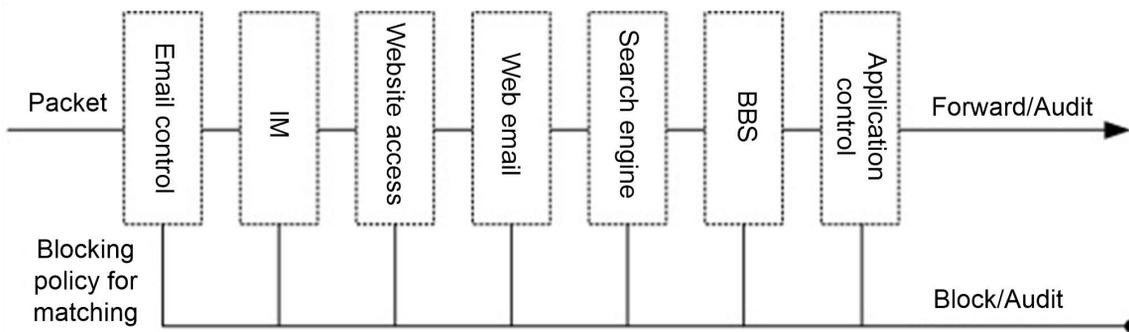


Figure: Processing Sequence of Behavior Management Services

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

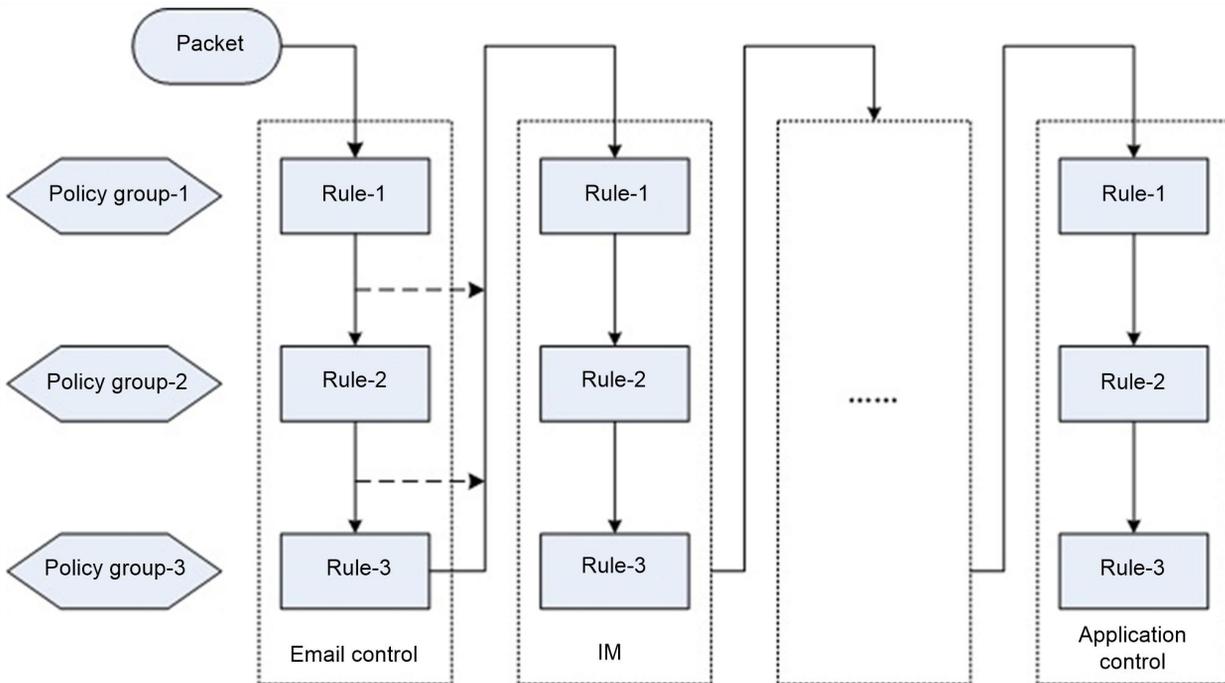
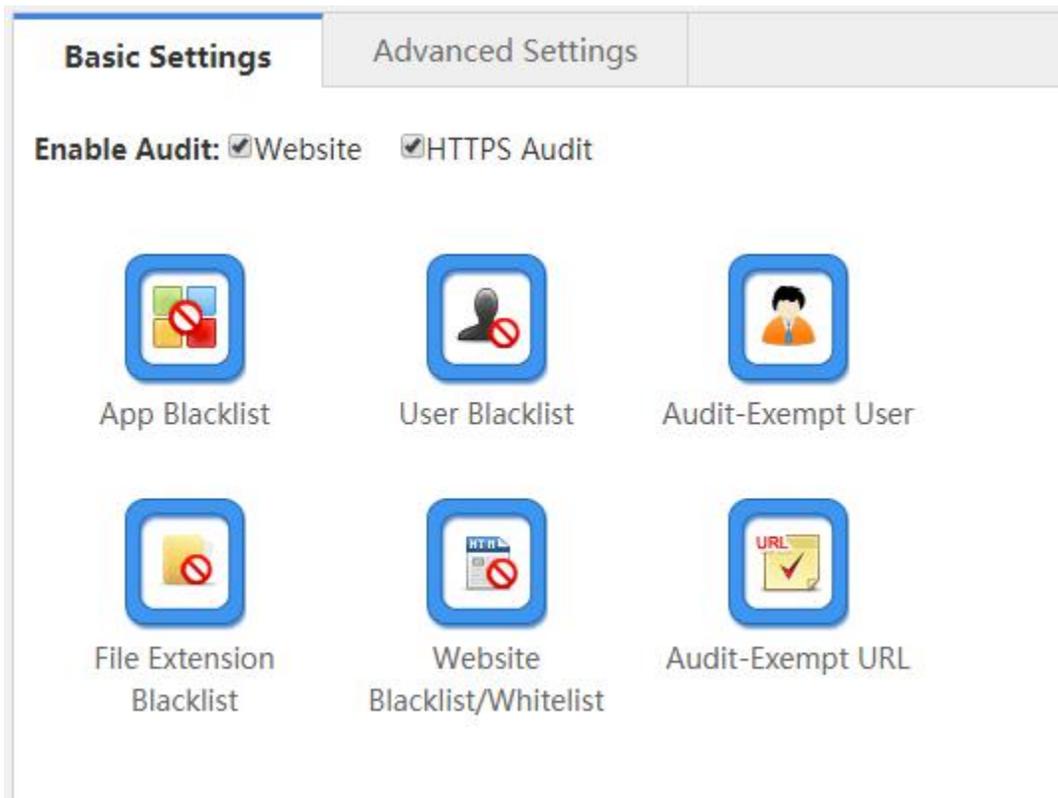


Figure: Matching Sequence Based on the Priorities of Policies and Rules

1.3.1.1.20 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.

Enable Audit: Website HTTPS Audit

- **App Blacklist**



Click [App Blacklist](#). 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.

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

[+ Add Blacklisted App](#) [X Delete All](#)

Blocked App	Delete
other-app	Delete
UDP-COMMUTE	Delete
DNS-ILLEGAL	Delete
ILLEGAL-CLASS	Delete

Show No.: Total Count:4
[First](#) [Previous](#) **1** [Next](#) [Last](#)
 [GO](#)

Click [+ Add Blacklisted App](#). A window shown in the figure below is displayed.

☰ **Select Blacklisted App**
✕

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

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

OK

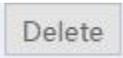


Select an application to be blacklisted, for example, games, and click **OK** to blacklist the application.

[+ Add Blacklisted App](#) [X Delete All](#)

Blocked App	Delete
other-app	<input type="button" value="Delete"/>
UDP-COMMUTE	<input type="button" value="Delete"/>
DNS-ILLEGAL	<input type="button" value="Delete"/>
ILLEGAL-CLASS	<input type="button" value="Delete"/>

Show No.: Total Count:4 **1**



Click **Delete** to delete an application from the application blacklist.



Click **X Delete All** 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 **User Blacklist** . 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.

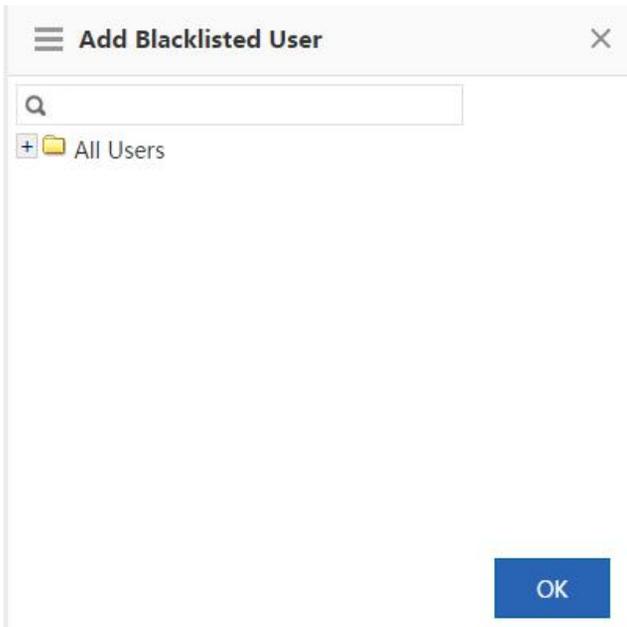
[+ Add Blacklisted User](#)

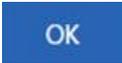
User Name	IP Address	MAC Address	Action
22	5.5.5.5	#	<input type="button" value="Delete"/>

Show No.: Total Count:1 **1**

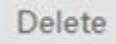
[+ Add Blacklisted User](#)

Click . A window shown in the figure below is displayed.



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

User Name	IP Address	MAC Address	Action
22	5.5.5.5	#	

Click  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**

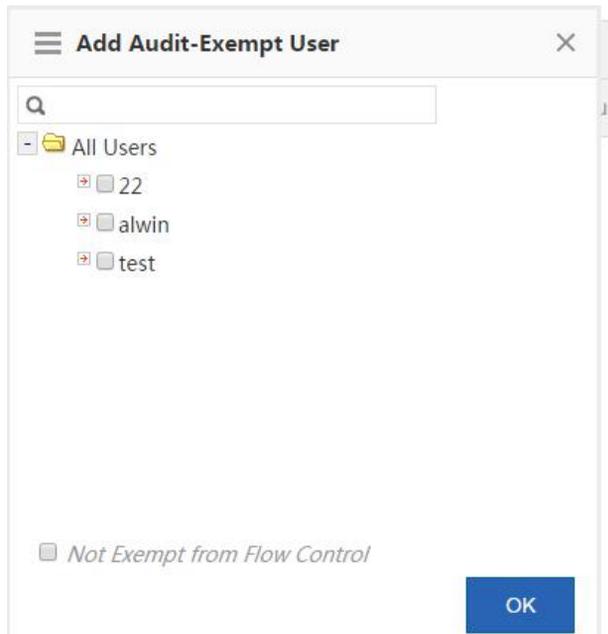


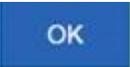
Click  . A window shown in the figure below is displayed. You can view the user devices exempt from audit, and can add or delete audit-exempt users.

[+ Add Audit-Exempt User](#)

User Name	IP Address	MAC Address	Flow Control-Exempt	Action
Show No.: <input type="text" value="10"/> Total Count:0				<input type="text" value="1"/>

Click [+ Add Audit-Exempt User](#). A window shown in the figure below is displayed.



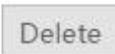
Select a user to be exempted from audit. Audit-exempt users are exempt from flow control by default. If flow control is required for an audit-exempt user, select *Not Exempt from Flow Control* and click .

[+ Add Audit-Exempt User](#)

User Name	IP Address	MAC Address	Flow Control-Exempt	Action
alwin	5.5.5.1	#	✓	<input type="button" value="Delete"/>

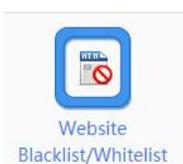
Show No.: Total Count:1

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  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 [Website Blacklist/Whitelist](#). 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.

Blacklist Mode
Only blacklisted websites are blocked

Whitelist Mode
Only whitelisted websites are allowed

Website: Select Enter a URL

Select

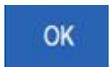
Add

Blacklisted Website List

Delete	Delete
forbidClass	<input type="button" value="Delete"/>
Violence	<input type="button" value="Delete"/>
Virus	<input type="button" value="Delete"/>
Adult	<input type="button" value="Delete"/>
Gambling	<input type="button" value="Delete"/>
Crime	<input type="button" value="Delete"/>

- (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



☰ **Select**
✕

- + + + + +
- + + + + +
- + + + + +
- + + + + +
- + + + + +
- + + + + +

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



Blacklist Mode
 Only blacklisted websites are blocked

Whitelist Mode
 Only whitelisted websites are allowed

Website: Select Enter a URL



Blacklisted Website List

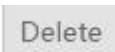
	Delete
4.4.4.4	Delete
youku.com	Delete

Show No.: 10 Total Count:2

 << First
 < Previous
 1
 Next
 Last >>

 1 **GO**

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



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

Blacklist Mode
 Only blacklisted websites are blocked

Whitelist Mode
 Only whitelisted websites are allowed

Website: Select Enter a URL



Whitelisted Website List Flexible Whitelist

Website	Delete
keyUrlClass	Delete

Show No.: 10 Total Count:1

 << First
 < Previous
 1
 Next
 Last >>

 1 **GO**

(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 .

Flexible Whitelist

(3) Flexible whitelist: Select . URL requests initiated from a whitelisted website are allowed to pass. For example, if www.FS.com.cn is a whitelisted website, users are allowed to access all URLs on this Web page.

● File Extension Blacklist



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.

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

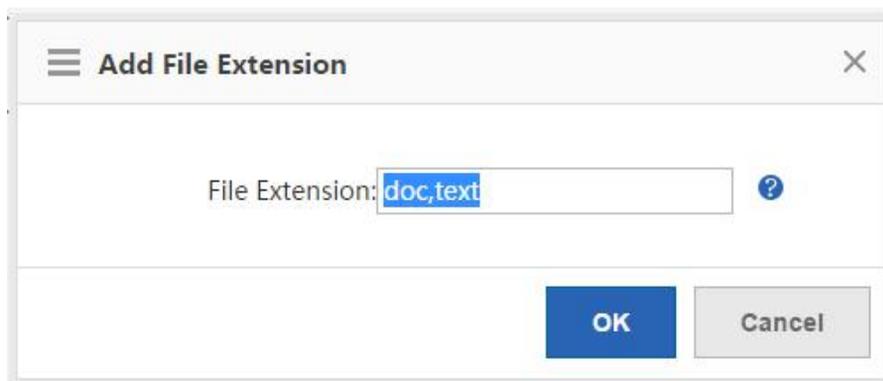
Enable: OFF

Click  to enable the file extension blacklist function.

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

+Add File Extension ×Delete Selected Enable: ON

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.

Enable: ON

<input checked="" type="checkbox"/> .doc	<input checked="" type="checkbox"/> .text
--	---

Click **X 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 **Audit-Exempt URL**. 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.

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

Enable: OFF

<input type="checkbox"/>	Audit-Exempt URL	Action
<input type="checkbox"/>	163.com	Delete

Show No.: 10 Total Count: 1

 << First
 < Previous
 1
 Next
 Last >>

Click Enable: ON to enable the audit-exempt URL function.

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

Enable: ON

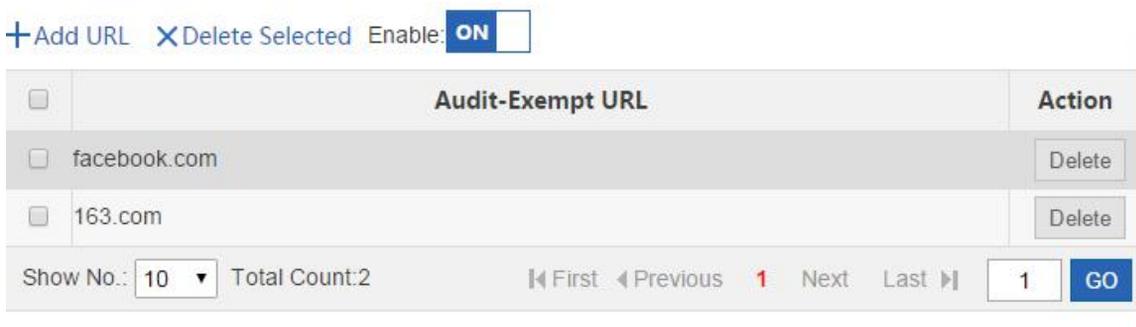
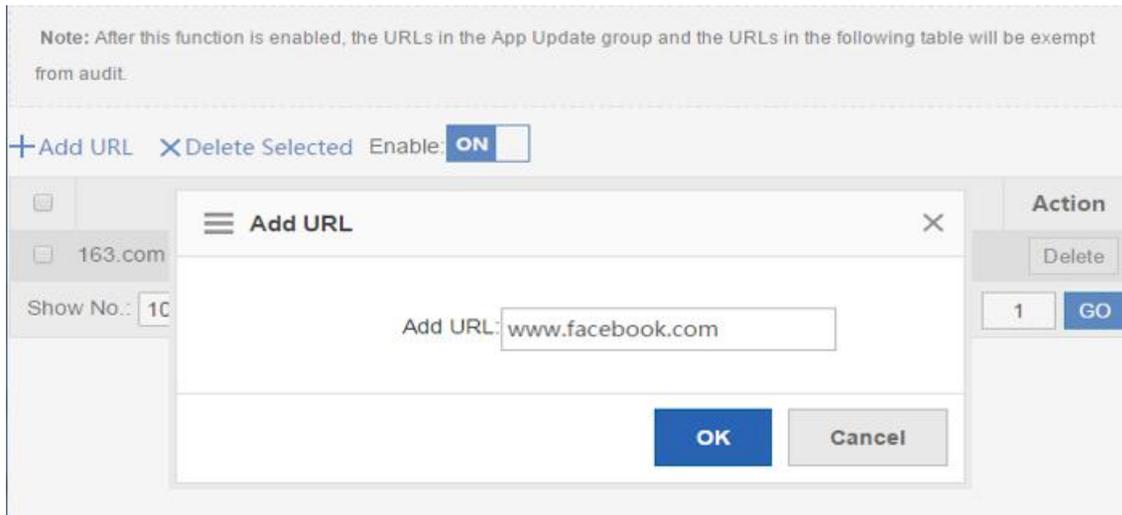
<input type="checkbox"/>	Audit-Exempt URL	Action
<input type="checkbox"/>	163.com	Delete

Show No.: 10 Total Count: 1

 << First
 < Previous
 1
 Next
 Last >>

+Add URL

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



Delete

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

XDelete Selected

Click **XDelete Selected** 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.

1.3.1.1.21 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 SG device of FS can effectively control the spread scope of key information and prevent possible legal risks.

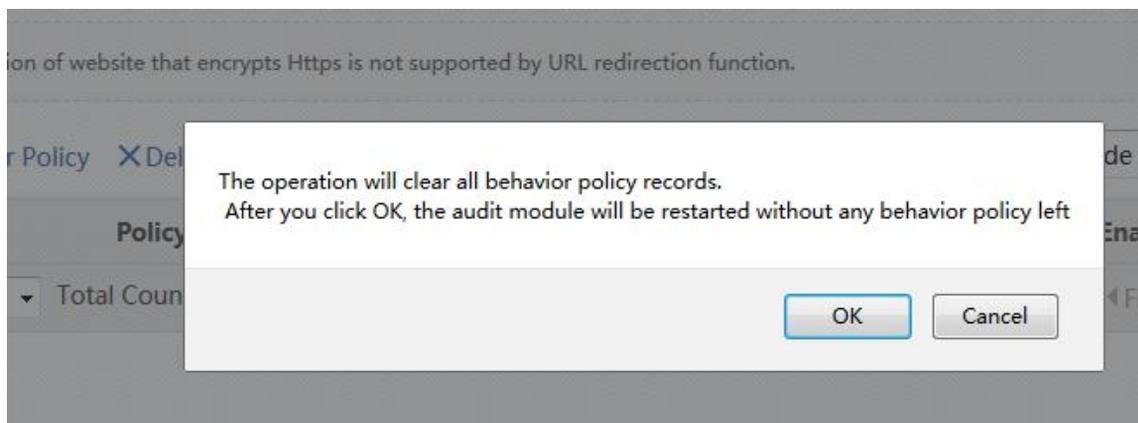
The SG device of FS is capable of monitoring information transfer channels such as email, Web mail, BBS, IM, Web search, FTP, Telnet, and Web page. It can comprehensively audit the email content, chat content, and posts.

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

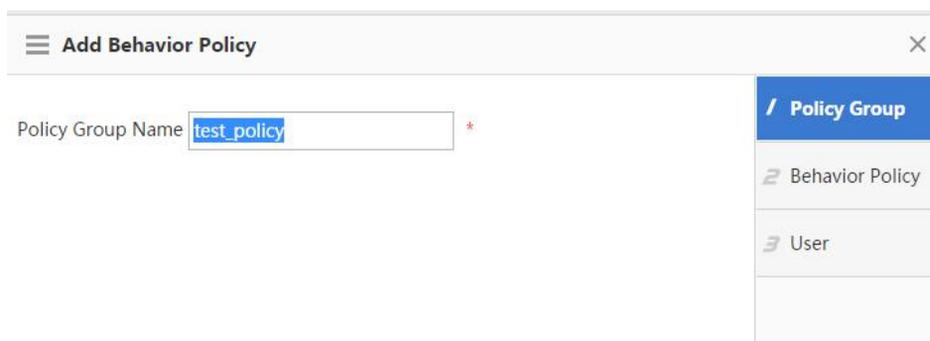


- **Creating and Editing a Policy**

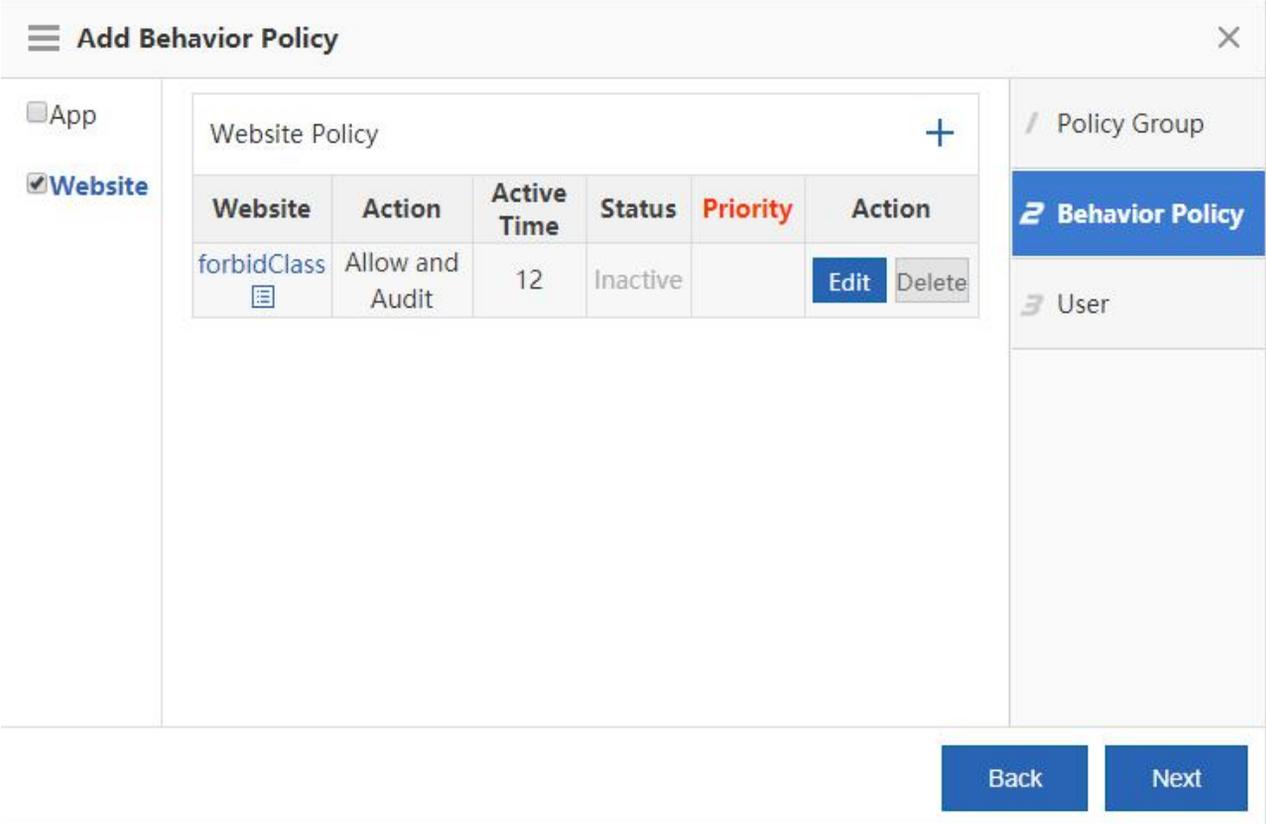
To create a behavior policy, do as follows:

+ Add Behavior Policy

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 App 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.

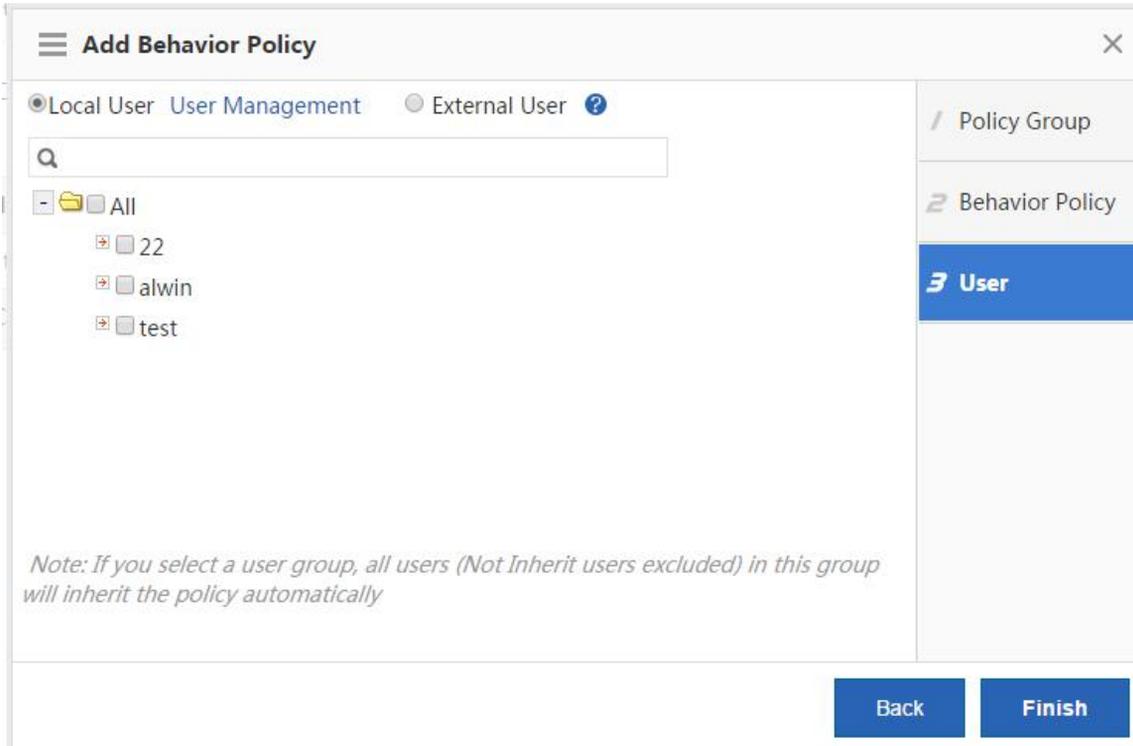
Allow and Not Audit: The device neither blocks the Internet access behaviors of selected users nor records their Internet access information.

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.

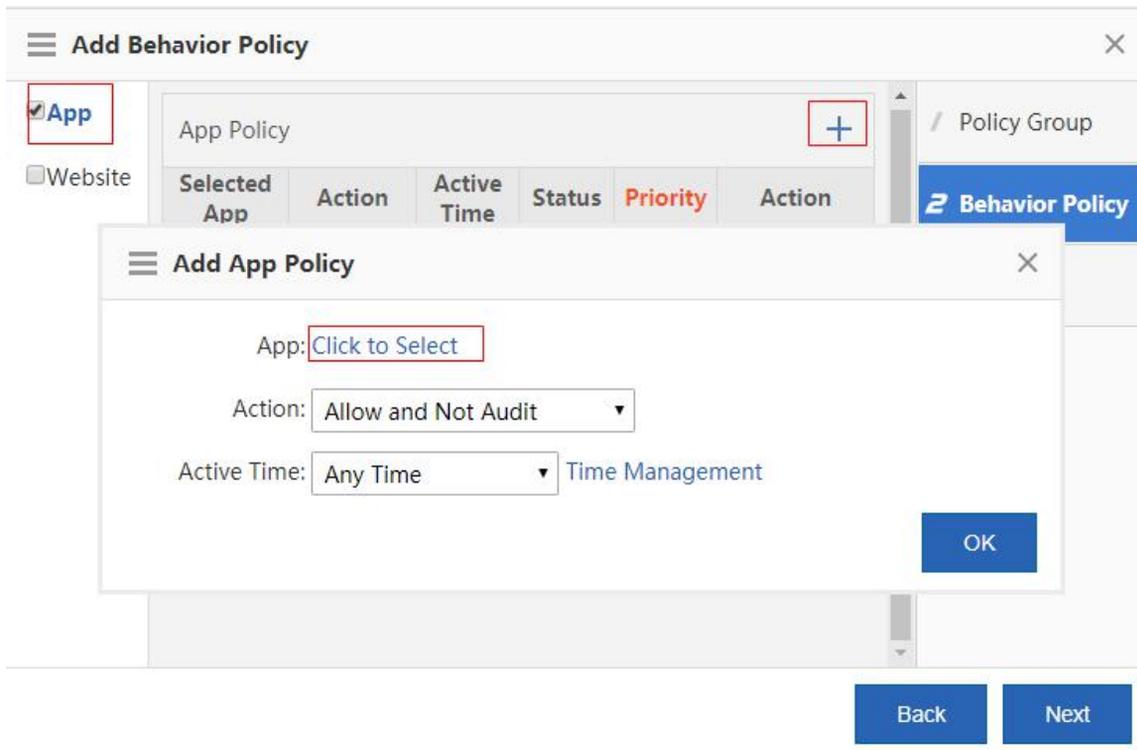
Active Time: Indicates the active time of a rule. A rule is effective only within the active time.

- 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.

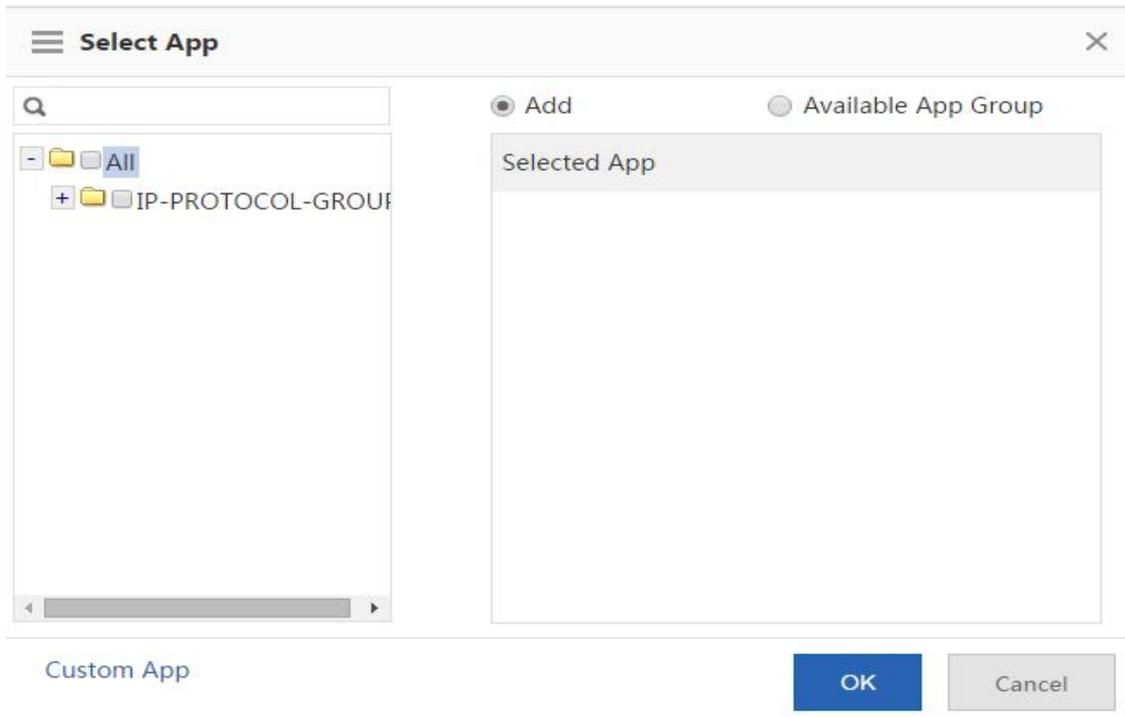


- **App Policy**

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:



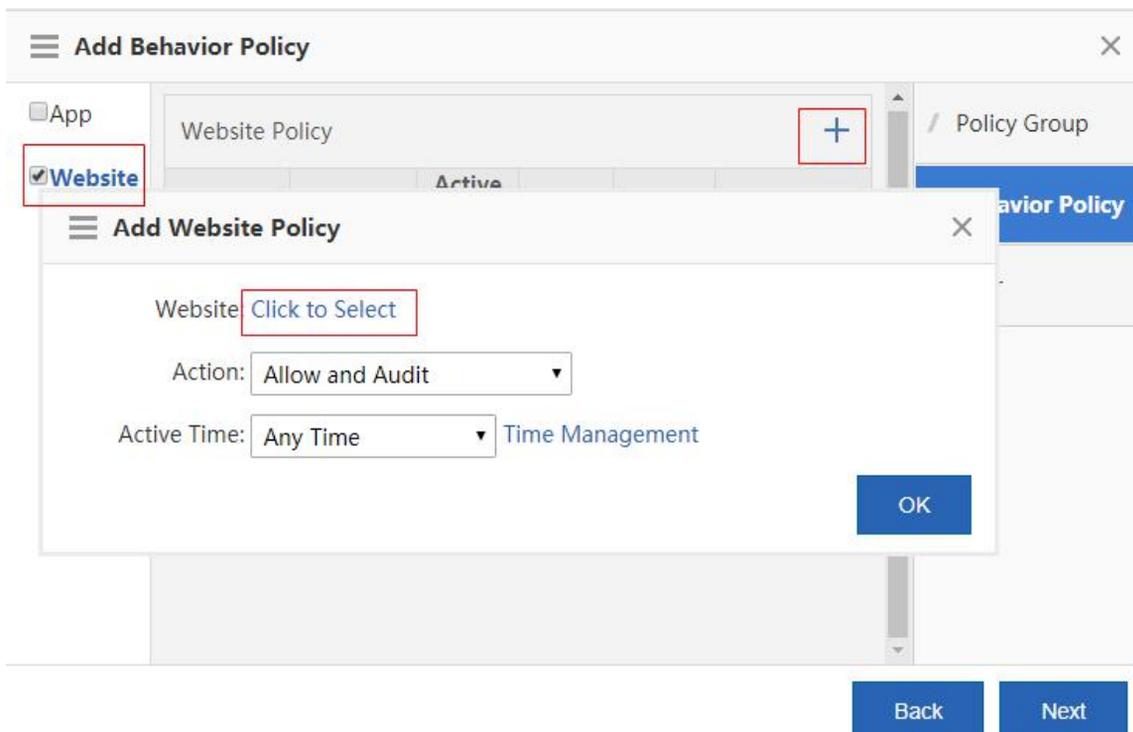
Select **App**. A page shown in the figure below is displayed.



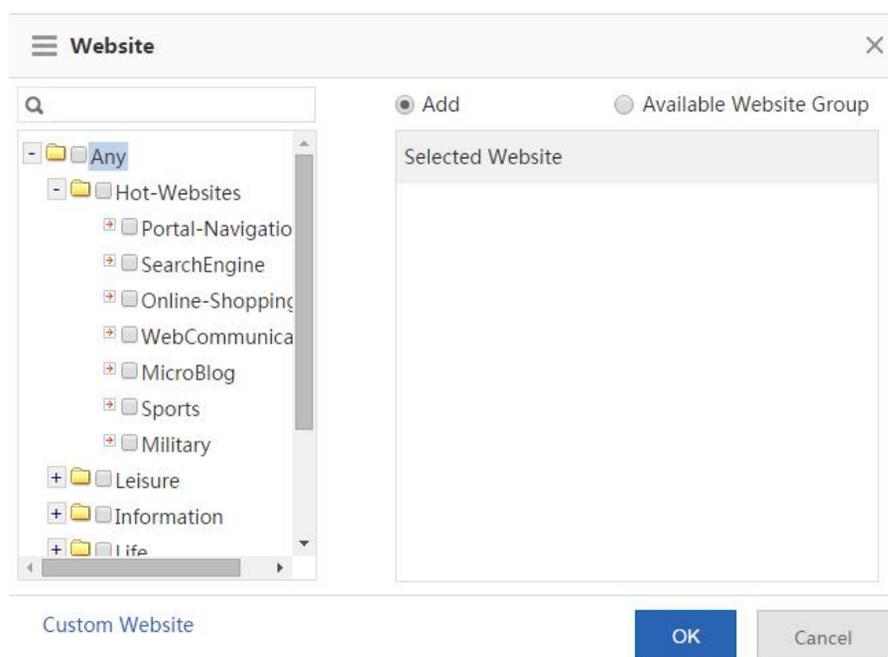
Click **Add** or **Available App Group**, as shown in the figure above. To create an application group, select the application to be controlled, enter the application group name, and click **OK**.

- **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.

1.1.10.2 Realtime Audit

Realtime Audit

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

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

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

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

1.1.10.3 Access Audit Report

1.3.1.1.22 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.

No.	Website	Request Times	Website Type	Action
1	http://172.31.62.30	4	UNKNOW CLASS	Details Block
2	http://captive.apple.com	1	Software-Updates	Details Block

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.

You are viewing <http://172.31.62.30> 's traffic details

User(IP)	Website	Website Type	Access on	Action
/192.168.1.4(192.168.1.4)	http://172.31.62.30/user/index_post.php	UNKNOW CLASS	2017-08-07 14:54:20	Allow



Click **Block** 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.

Today's Audit Report Advanced Search Export

Website Access Ranking		User Access Ranking	Website Access Details	Blocked Website	App Audit
No.	User Name	Local User	Websites	Action	
1	ap1_user		3	Details	
2	192.168.1.4		1	Details	
3	192.168.1.3		1	Details	

First Previous 1 Next Last 1 GO



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

You are viewing 192.168.1.4 's traffic details

User(IP)	Website	Website Type	Access on	Action
/192.168.1.4(192.168.1.4)	http://172.31.62.30/user/index_post.php	UNKNOW CLASS	2017-08-07 14:54:20	Allow

First Previous 1 Next Last 1 GO

3. Website Access Details

This tab page displays details about all accessed websites. To view a specific website, click [Advanced Search](#) and enter the required URL.

Access Audit Report

Today's Audit Report Advanced Search Export

Website Access Ranking		User Access Ranking	Website Access Details	Blocked Website	App Audit
Access on	User/IP	Local User	Website	Website Type	Action

First Previous 1 Next Last 1 GO

4. Blocked Website

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

Access Audit Report

Today's Audit Report Advanced Search Export

Website Access Ranking		User Access Ranking	Website Access Details	Blocked Website	App Audit
No.	Website	Request Times	Website Type	Action	

First Previous 1 Next Last 1 GO

Details

Click **Details** 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.

Website Access Ranking		User Access Ranking		Website Access Details		Blocked Website		App Audit				
User/IP	Local User	Audit Time		App Name		VPN Access	Action	Policy				
						First	Previous	1	Next	Last	1	GO

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

6. Advanced Search

Advanced Search

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

Advanced Search

Advanced Search

Behavior Type: Website Access Details

User Type: Local User External User

User: All Users

Time Span: 2020-9-14 00 00 - 23 00

Website Type: Select App [\[Select App\]](#) All Apps

OK

Access Audit Report				
Search Terms				Advanced Search Export
Behavior Type: Website Access Details User: All Users Searched on: 2020-9-14 00:00-23:00 Website: All Apps				
Back				
Access on	User/IP	Website	Website Type	Action
First Previous 1 Next Last GO				

1.1.10.4 Object

1.3.1.1.23 Custom App

Custom App	Custom Website	Time Object	External IP Object	VLAN Object	IP Object
+ Add App Group + Custom App Help Identify 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_too_MOBILE, UNKNOWWEB, OnlineStorage, Games, Video, Web Application, HTTPDOWNLOAD, HTTPUPLOAD, HTTP-VEDIO, Video_MOBILE, Social_contact_MOBILE, Storage_MOBIL E				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.

1. Adding a custom application group

Click [+ Add App Group](#) to custom an application group.

☰ **Add App Group**
✕

App Group Name:

App types are indicated by font colors:
Key/Normal/Block/Block

- [-] All
- [-] IP-PROTOCOL-GROUP
 - BY_PASS_APP
 - other-app
 - UDP-COMMUTE
 - TCP-COMMUTE
 - UDP-TRANSFERS
 - TCP-TRANSFERS
 - IP-APP

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

Normal App	IP-PROTOCOL-GROUP,TCP-COMMUTE,UDP-TRANSFERS,ICMP,OTHER-UDP,OTHER-TCP,Stock,Datebase,NetworkMGR,Routing,REMOTE-PROTOCOL,SoftwareUpdate,OnlineBank,Web_MOBILE,Online_shopping_MOBILE,Securities_MOBILE,OnlinePayment Bank_MOBILE,RFC,IP-RAW,OA_office,Video_conferencing	Edit
App	other-app, UDP-COMMUTE	Edit Delete
testGroup	UDP-COMMUTE, TCP-COMMUTE, UDP-TRANSFERS	Edit Delete

Show No.: 30 Total Count:13 First Previous 1 Next Last 1 GO

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.

Edit App Group
✕

App Group Name:

App types are indicated by font colors:
Key/Normal/Block/Block

- [-] All
- [-] IP-PROTOCOL-GROUP
 - BY_PASS_APP
 - other-app
 - UDP-COMMUTE
 - TCP-COMMUTE
 - UDP-TRANSFERS
 - TCP-TRANSFERS
 - IP-APP

[Save](#)
[Cancel](#)



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

Edit App Group
✕

App Group Name:

App types are indicated by font colors:
Key/Normal/Block/Block

- [-] All
- [-] IP-PROTOCOL-GROUP
 - BY_PASS_APP
 - other-app
 - UDP-COMMUTE
 - TCP-COMMUTE
 - UDP-TRANSFERS
 - TCP-TRANSFERS
 - IP-APP

[Save](#)
[Cancel](#)

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  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 . The custom application configuration page is displayed.

Tip: The application name cannot be longer than 27 characters

App Name:

Protocol Type: Rule Type:

App Group: Custom Select

Src IP: 

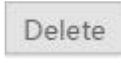
Dest IP: 

App Name	Protocol Type	App	Src Port	Dest Port	Src IP	Dest IP	Action
qiqiao	tcp	123	All Ports	All Ports	1.1.1.1	1.1.1.10	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.: Total Count:1
 1

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 

1.3.1.1.24 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.

[+ Add Website Group](#)
[Custom Website](#)
[System Website](#)
[Search Website](#)

Website Group Name	Website	Action
Portal-Navigation	Portal-Navigation	Edit Delete
keyObject	keyUrlClass	Edit Delete
illegal	forbidClass,Violence,Virus,Adult,Gambling,Crime,undefined	Edit Delete

Show No.: Total Count:3

[First](#)
[Previous](#)
[Next](#)
[Last](#)
 [GO](#)

- **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.

Add Website Group

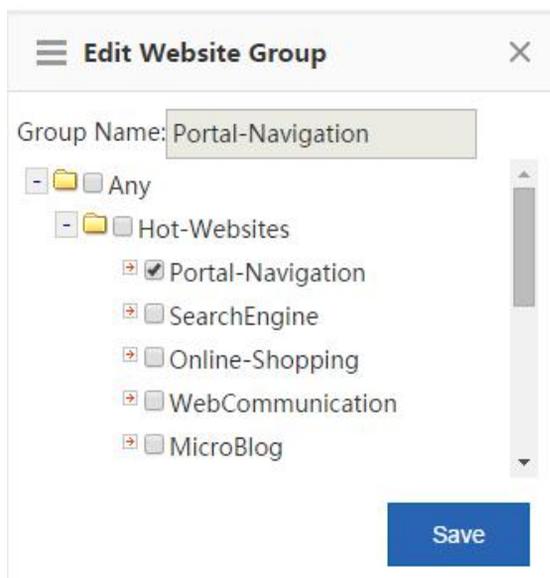
Website Group Name:

- Any
- Hot-Websites
- Leisure
- Information
- Life
- Business-Economic
- Bad

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

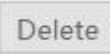
2. Editing a website group

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 .

3. Deleting a website group

Click  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.

Custom Website

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

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

Website Name * Description:

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



Custom Website List

Website Name	URL	Description	Action	
un_audit_class	163.com, facebook.com	unaudit		
forbidClass	4.4.4.4, youku.com			

Show No.: Total Count:2     

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 . 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 .

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

Custom App	Time Object	External IP Object	VLAN Object	IP Object
+ Add App Group + Add Custom App Help Identify App				
App Group Name	Selected App			Action
Key App	DNS,Voip,Vpn-app			Edit
Web Page	HTTPS,HTTP,Web_MOBILE			Edit
Online Video	HTTP-VIDEO,Video_MOBILE			Edit
P2P Video Streaming	STREAMING			Edit
Download	HTTP-DOWNLOAD,FTP,TFTP,NNTP,IXIA,SVN,SMB,DownloadTools_MOBILE,OnlineStorage			Edit
P2P Download	P2P			Edit
App Update				Edit
Upload	HTTP-UPLOAD			Edit
Rate-Limited App	Games			Edit
Blocked	DNS-ILLEGAL			Edit
Normal App	Chat,FileTransfer,E-Mail,Database,NetworkManagementProtocol,Routing,Security,REMOTE-PROTOCOL,SoftwareUpdate,OnlineBank,InstantMessaging_MOBILE,Game_MOBILE,Social_contact_MOBILE,OA_office,Video Conferencing,OnlinePayment Bank_MOBILE,RFC,ICMP-DETAIL,IP-RAW,IP-PROTOCOL-GROUP,HTTP-BROWSE-DETAIL			The default group cannot be edited
Common-High-Traffic-App	WebApplication,WebApplication_Mobile,ForumPC,Online_Shopping,WEBMail,Chat,FileTransfer,REMOTE-PROTOCOL,OnlineBank,InstantMessaging_MOBILE,Social_contact_MOBILE,STREAMING,P2P			Edit Delete
Common-Media-App	HTTP-VIDEO,Video_MOBILE			Edit Delete
Common-Download-App	HTTP-DOWNLOAD,HTTP-UPLOAD,SoftwareUpdate,OnlineStorage,DownloadTools_MOBILE			Edit Delete

1.3.1.1.25 Time Object

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

Custom App	Custom Website	Time Object	External IP Object	VLAN Object	IP Object
<p>Note: The time object refers to the time when the policy is active.</p>					
+ Add Object X Delete Selected					
<input type="checkbox"/>	Time Object	Time Interval	Time Span	Action	
<input type="checkbox"/>	Any Time	Every Day	0:00-23:59	Edit	Delete
<input type="checkbox"/>	Daytime	Every Day	6:00-18:00	Edit	Delete
<input type="checkbox"/>	Nighttime	Weekday Every Day	0:00-5:59 18:01-23:59	Edit	Delete
<input type="checkbox"/>	Off-Working Hours	Weekday Weekday Weekday	0:00-7:59 12:00-13:00 18:01-23:59	Edit	Delete
<input type="checkbox"/>	Weekend	Weekend	0:00-23:59	Edit	Delete
<input type="checkbox"/>	Working Hours	Weekday Weekday	8:00-12:00 13:00-18:00	Edit	Delete
<input type="checkbox"/>	Workday	Weekday	0:00-23:59	Edit	Delete
Show No.: <input type="text" value="10"/>		Total Count:7		First Pre Next Last <input type="text" value="1"/> GO	

1. Add a time object: Click **+Add Object**. 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:

Object Name:

- (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**.

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

+Add Object X Delete Selected

<input type="checkbox"/>	Time Object	Time Interval	Time Span	Action
<input type="checkbox"/>	Any Time	Every Day	0:00-23:59	Edit Delete
<input type="checkbox"/>	Daytime	Every Day	6:00-18:00	Edit Delete
<input type="checkbox"/>	Nighttime	Weekday Every Day	0:00-5:59 18:01-23:59	Edit Delete
<input type="checkbox"/>	Off-Working Hours	Weekday Weekday Weekday	0:00-7:59 12:00-13:00 18:01-23:59	Edit Delete
<input type="checkbox"/>	Weekend	Weekend	0:00-23:59	Edit Delete
<input type="checkbox"/>	Working Hours	Weekday Weekday	8:00-12:00 13:00-18:00	Edit Delete
<input type="checkbox"/>	Workday	Weekday	0:00-23:59	Edit Delete

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

- 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.
- Delete a time object: To delete a time object, select the time object in the list and click [Delete](#) .
- 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 [X](#) .

Object Name: *

Time Span:

<input type="text" value="Monday,Tuesday,▼"/>	<input type="text" value="0:00"/>	~	<input type="text" value="5:59"/>	X	+Add
<input type="text" value="Monday,Tuesday,▼"/>	<input type="text" value="18:01"/>	~	<input type="text" value="23:59"/>	X	

1.1.11 Cache

1.1.11.1 Realtime Status

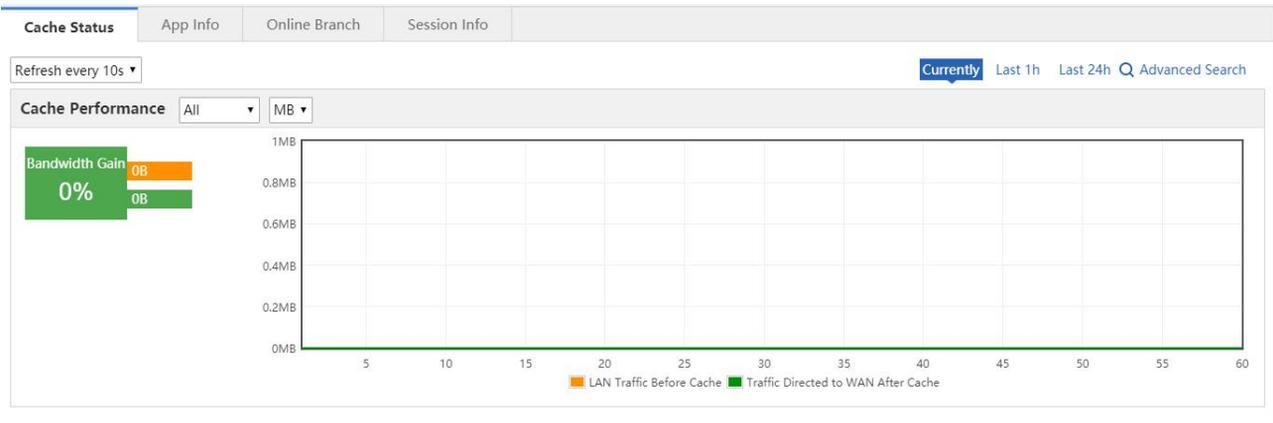
Realtime status refers to the realtime cache status, including the following information: :

Cache Status	App Info	Online Branch	Session Info
---------------------	----------	---------------	--------------

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

1.3.1.126 Cache Status

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



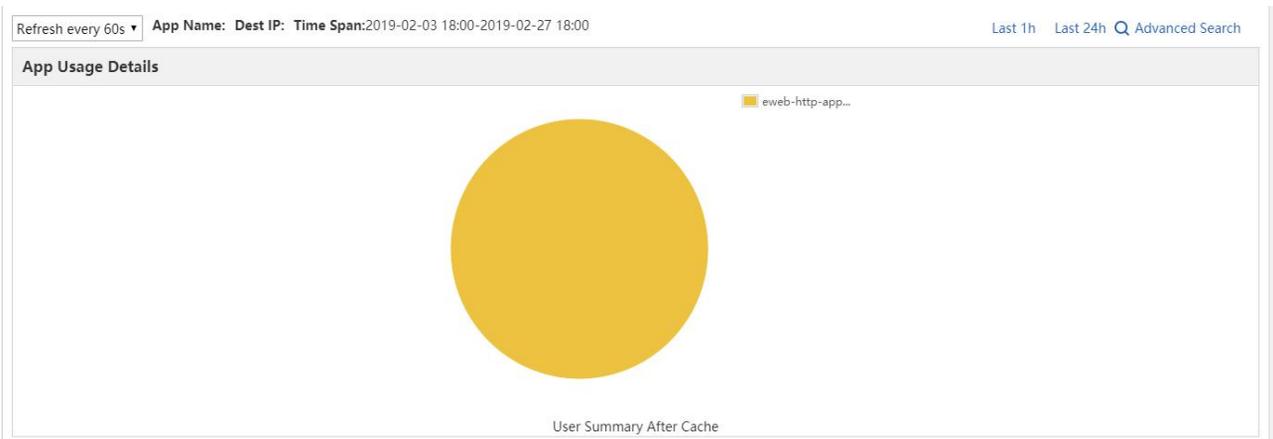
You can view traffic tendency based on time span, including **Currently**, **Last 1h**, and **Last 24h**. Traffic is further divided into **Uplink** or **Downlink**.

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

1.3.1.127 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).

App Name	Traffic before cache	Traffic after cache
eweb-http-app-cache-80	730.67MB	730.67MB

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

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

1.3.1.1.28 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.

Cache Status	App Info	Online Branch	Session Info
Verify Code			
Verify Code: <input type="text" value="121212"/> * Up to 32 characters (no spaces)			
<input type="button" value="Save"/>			

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

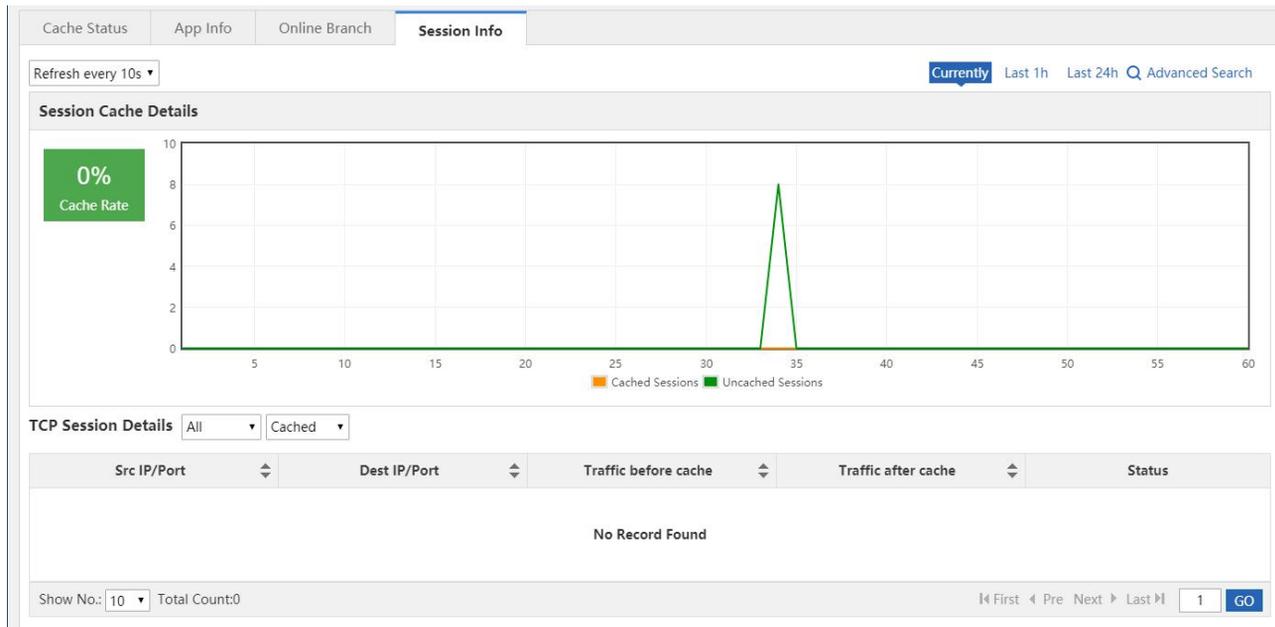
ID	Branch Name	IP	Sessions	Before Cache	After Cache	Reduction Rate
111	testbranch	192.168.1.3/9001	192.168.1.3	211G	107.2G	51.1%

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

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

1.3.1.1.29 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:

The screenshot shows the 'TCP Session Details' section with filters for 'All' and 'Cached'. The table below has the following data:

Src IP/Port	Dest IP/Port	Traffic before cache	Traffic after cache	Status
192.168.1.2/9000	192.168.1.7/128	288.4kB	300.4kB	
192.168.1.3/9001	192.168.1.5/126	4.2kB	4.6kB	

At the bottom, there is a 'Show No.: 10' dropdown, 'Total Count:0', and pagination controls including 'First', 'Pre', 'Next', 'Last', and a 'GO' button.

TCP sessions are classified into cached and uncached sessions.

The screenshot shows the 'TCP Session Details' section with filters for 'All' and 'Uncached'. The table below has the following data:

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.

1.1.11.2 Resource Cache

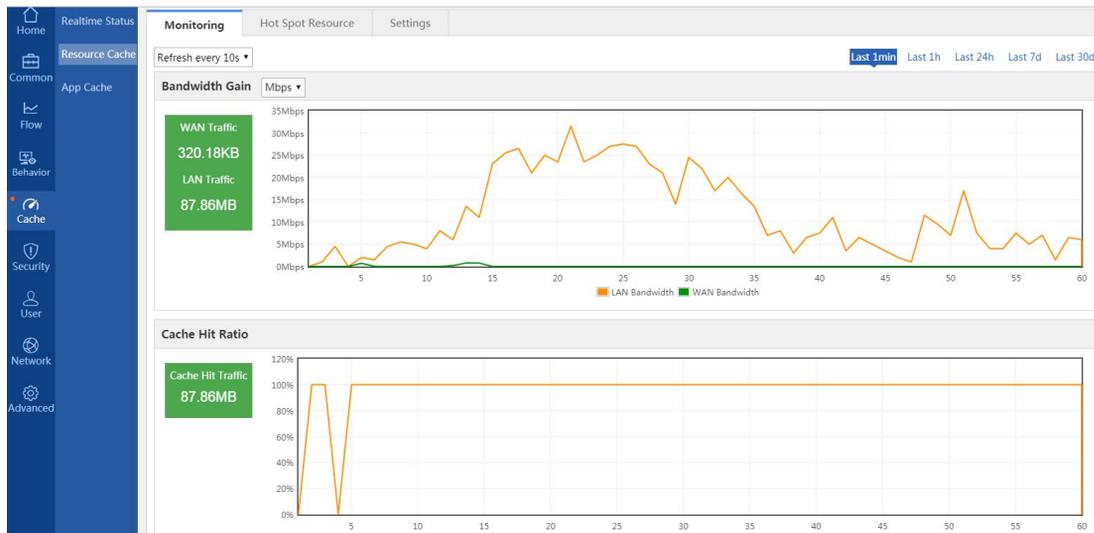
Resource refers to the files that can be downloaded or browsed online, including documents (e.g., PPT, WORD, EXCECEL, TXT, RAR, and ZIP), images (e.g., JPG, PNG, and GIF) and videos (MP4, FLV, AVI, RMVB, and 3GP).

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.

1.3.1.1.30 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.

1.3.1.1.31 Hot Spot Resource

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

Resource Name	Resource Size	Hit Times	Hit Traffic
/jquery.js	76.3kB	3	229.9kB
/jquery.cookie.js	3.7kB	2	7.4KB

Refresh Today Weekly Monthly

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

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.

1.3.1.132 Settings

Monitoring
Hot Spot Resource
Settings

Note: If the address is a domain name, please configure DNS first. Up to 10 addresses can be added.
Note: Please do not configure a website as the cache address. Otherwise, the website may be unavailable. This module uses TCP proxy, which will conflict with the Internet shield mode, make sure that the Internet shield mode is turned off.

Enable Cache: ON

Resources Cache Address Cache Capacity (Used: 802.39MB Total: 100.00GB) Disk Capacity (Free: 443064.78MB Total: 469454.72MB)

Resources Address1: * ✕ Delete + Add

Source IP: ?

Resources Cache Settings

Cache Status: [\[Cache Details\]](#)

Interval(s): ? *

Cache Time: : ~ : ?

If you want to disable resource cache, please switch off . Cache will be disabled as shown in the following figure:

Resource Cache
Settings

Enable Cache: OFF

If you want to enable resource cache, please switch on

Resources Cache Address

Cache Capacity (Used: **802.39MB** Total: **100.00GB**)Disk Capacity (Free: **442400.43MB** Total: **469454.72MB**)Resources Address1: * [X Delete](#) [+ Add](#)Source IP: ?[Save](#)[Clear All](#)

Resources Cache Settings

Cache Status: [\[Cache Details\]](#)Interval(s): ? *Cache Time: : ~ : ? [▶ Cache Now](#)[Save](#)[Restore Default](#)

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.

1.1.11.3 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:

APP Server Address

All HTTP (Port 80)

Address1: * +Add

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

App Name1: * +Add

Cache Specified App ? Time Window

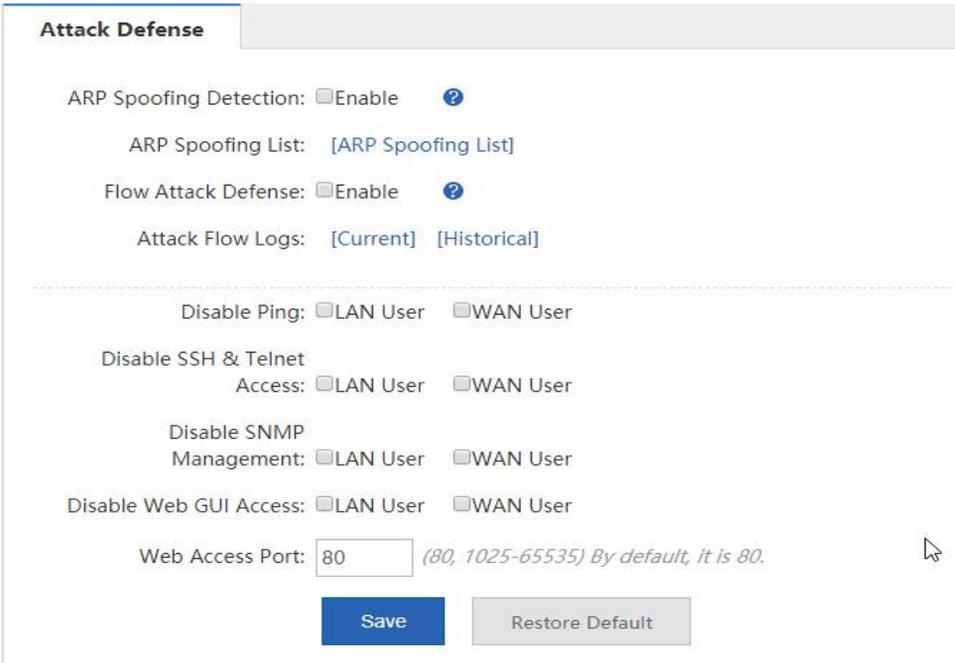
Address1: * +Add

1.1.12 Security

1.1.12.1 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 **Enable** 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 [\[ARP Spoofing List\]](#) to list the hosts that are suspected to initiate ARP spoofing.

2. Flow attack defense

Flow Attack Defense: Select **Enable** 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 [\[Current\]](#) to display logs about current attacks or click [\[Historical\]](#) to display logs about historical attacks of the system.

3. Other attack defense

Disable Web GUI Access: Select **LAN User** in **LAN User** to forbid LAN users from logging in to the Web

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

Disable Web Access: LAN User WAN User

Add IP Whitelist: [\[More\]](#) [?](#)

Web Access Port: *It is recommended to set the port to an integer ranging from 1,025 to 65,535.*

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 [\[More\]](#) to display and manage IP addresses.

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

IP Whitelist: **Description:**

IP Management	Description	Action
Show No.: <input type="text" value="10"/> Total Count:0	First Previous 1 Next Last	<input type="text" value="1"/> <input type="button" value="GO"/>

Disable Ping: Select **Disable Ping:** LAN User WAN User 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 address:access port` in the address bar to access the device.

1.1.12.2 Interface Access Control

Interface Access Control

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

[+Add](#) [X Delete Selected](#)

☐	ACL No.	Interface	Filter Direction	Reflexive ACL	Action
No Record Found					

Show No.: Total Count:0
[First](#)
[Pre](#)
[Next](#)
[Last](#)

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 to generate an ACL, which serves as a firewall.

Reflexive ACL: Enable

The firewall supports status-tracking-based ACLs. Select [Reflexive ACL: Enable](#) to configure reflective ACLs.

☰ Add
✕

ACL:

Interface:

Filter Direction:

Reflexive ACL: Enable

Save
Cancel

1.1.12.3 ARP Entry

ARP Entry

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

Total ARP Entries: 5 Search by IP/MAC: Search

	IP Address	MAC Type	Type
<input type="checkbox"/>	172.168.1.1	00d0.f86b.dcbe	Static Binding
<input type="checkbox"/>	192.168.10.3	f0c8.50fa.e10c	Static Binding
<input type="checkbox"/>	192.168.10.4	683e.34d7.13e1	Static Binding
<input type="checkbox"/>	192.168.20.2	683e.34d7.13e1	Static Binding
<input type="checkbox"/>	192.168.20.11	e8b4.c8e9.ece1	Static Binding

Show No.: Total Count: 5

⏪ First
⏩ Pre
Next
⏪ Last
1
GO

ARP Settings

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

Disable ARP Learning: Gi0/0 Gi0/2 Gi0/4 Gi0/5

Enable Gratuitous ARP: Gi0/0 Gi0/2 Gi0/4 Gi0/5

Save

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.

The Bind function will change all the dynamic ARP entries to static ARP entries. Are you sure you want to continue?

Prevent this page from creating additional dialogs.

OK
Cancel

2. ARP entries

	IP Address	MAC Type	Type
<input type="checkbox"/>	1.1.1.2	0000.0101.0102	Dynamic Binding

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.

ARP Settings

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

Disable ARP Learning: Gi0/0 Gi0/2 Gi0/4 Gi0/5
 Enable Gratuitous ARP: Gi0/0 Gi0/2 Gi0/4 Gi0/5

[Save](#)

1.1.12.4 ACL

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

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

ACL: 2 [Add ACL](#) [Delete ACL](#) [+Add ACE](#) [X Delete Selected](#)

Show No.: 10 Total Count: 1 [First](#) [Pre](#) 1 [Next](#) [Last](#) [GO](#)

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](#).

Add ACL ✕

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

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

[OK](#) [Cancel](#)

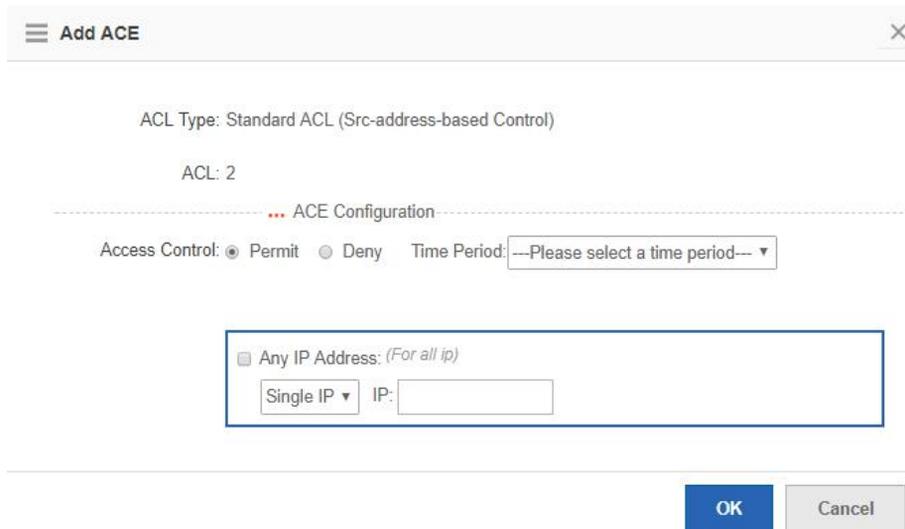
2. Adding an ACE

Select an ACL from the **ACL: 2** 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.



Add ACE [X]

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

ACL: 2

... ACE Configuration ...

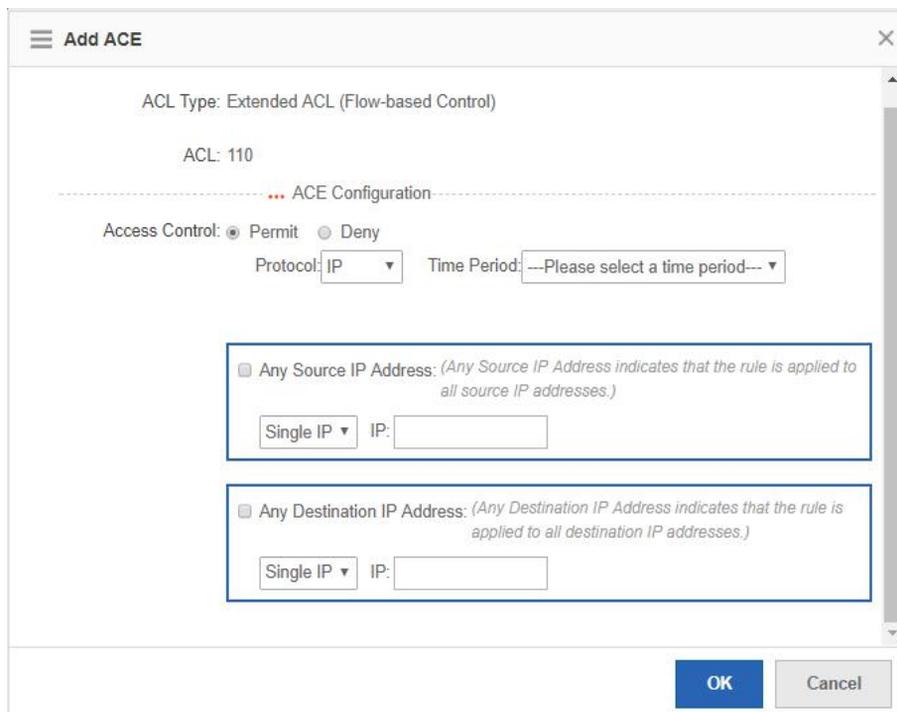
Access Control: Permit Deny Time Period: ---Please select a time period---

Any IP Address: (For all ip)

Single IP

OK **Cancel**

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  to generate an extended ACE.



Add ACE [X]

ACL Type: Extended ACL (Flow-based Control)

ACL: 110

... ACE Configuration ...

Access Control: Permit Deny

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

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

Single IP

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

Single IP

OK **Cancel**

Single IP
 IP&Mask
 IP&Wildcard

Select the address type from IP&Mask IP&Wildcard 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.

NOTE:

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

ACL

ACL: test_extend

<input type="checkbox"/>	NO.	Src IP /Wildcard	Src Port	Access Control	Protocol	Dest IP/Wildcard	Dest port	Time Period	Status	Action
<input checked="" type="checkbox"/>	1	4.4.4.1/0.0.0.0		Permit	ip	5.5.5.6/0.0.0.0		All Time	Effective	Edit Move

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

Click to adjust the sequence of ACEs.

Click to edit the selected ACE.

Click to delete the selected ACE.

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

1.1.12.5 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

Global Sessions

Attack Defense

Note: Prevent forwarding error.

Uplink Attack Defense: [\[Global Config\]](#) [\[Single IP Config\]](#) ?

New Session Limit: [\[Global Config\]](#) [\[Single IP Config\]](#) [\[Sessions Attacks List\]](#) ?

Session Limit

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

[+ Add Sessions Policy](#) [View Sessions Per IP](#)

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

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

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**

Uplink Attack Defense: [Global Config] [\[Singal IP Config\]](#)

Click **[Global Config]** in . In the window displayed, configure the default maximum number of per-IP-based uplink packets per second.

Global Uplink Attack Defense

Uplink Packets Per IP: *pps (0 ~ 100000)*

3,000-5,000 recommended.

Save

Uplink Attack Defense: [\[Global Config\]](#) [\[Singal IP Config\]](#) . In the window displayed, configure the maximum number of uplink packets for a specific IP address.

It indicates the maximum uplink IP packets. The priority is higher than the default policy.
If an IP is wrongly analyzed as a virtual IP, this function can help users to move it to the real IP list.

IP-Based Uplink Attack Defense

IP :

Uplink Packets: (0 - 100,000)

IP	Uplink Packets (pps)	Action
Show No.: <input type="text" value="10"/> Total Count:0 ⏪ First ⏪ Previous 1 Next ⏩ Last ⏩ <input type="text" value="1"/> <input type="button" value="GO"/> 		

- New Session Limit

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

New Session Limit: [\[Global Config\]](#) [\[Single IP Config\]](#) [\[Sessions Attacks List\]](#)

Global Max New Sessions

Max New Sessions Per Second During First 3 Minutes After Startup: (0 - 100,000) Recommendation: 2,000 - 5,000

Max New Sessions Per Second During Device Operation: (0 - 100,000) Recommendation: 1,000 - 3,000

Max New Sessions Per Real Host Per Second: (0 - 100,000) Recommendation: 10-100

It indicates the maximum sessions added by a real host per second. The priority is higher than the default policy.
 If an IP is wrongly analyzed as a virtual IP, this function can help users to move it to the real IP list.

IP-Based Max New Sessions

IP:

Max New Sessions Per Second: (0 - 100,000)

Save

IP	Max New Sessions Per Second	Action
3.1.1.2	1000	Edit Delete

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

Host Type	Host IP	Time	Sessions Stopped
Show No.: 10 Total Count:0 First Previous 1 Next Last 1 GO			

2. Sessions Limit

Session Limit

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

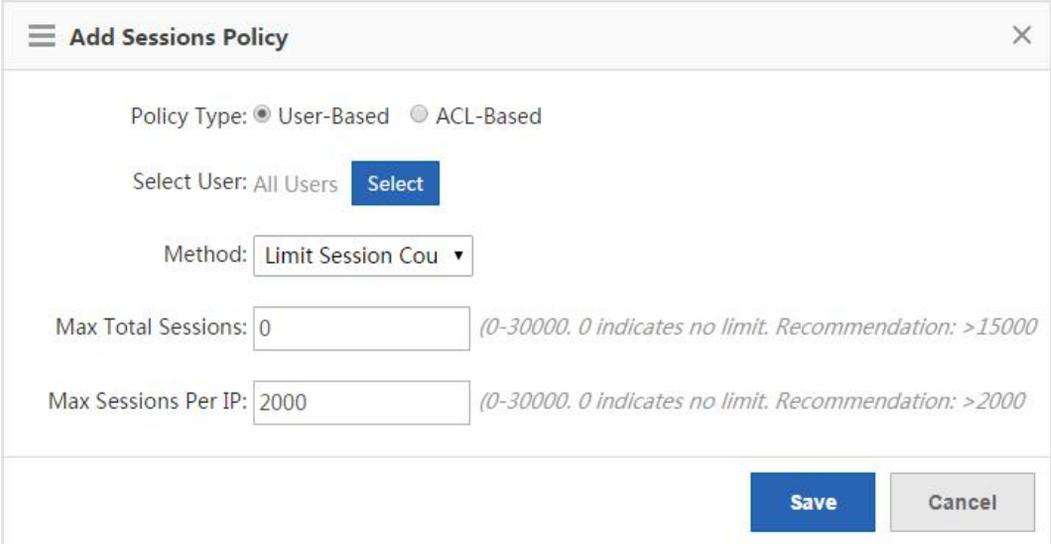
[+ Add Sessions Policy](#) [View Sessions Per IP](#)

Policy Type	User/ACL	Method	Max Total Sessions	Max Sessions Per IP	Status	Priority	Action
Show No.: 10 Total Count:0 First Previous 1 Next Last 1 GO							

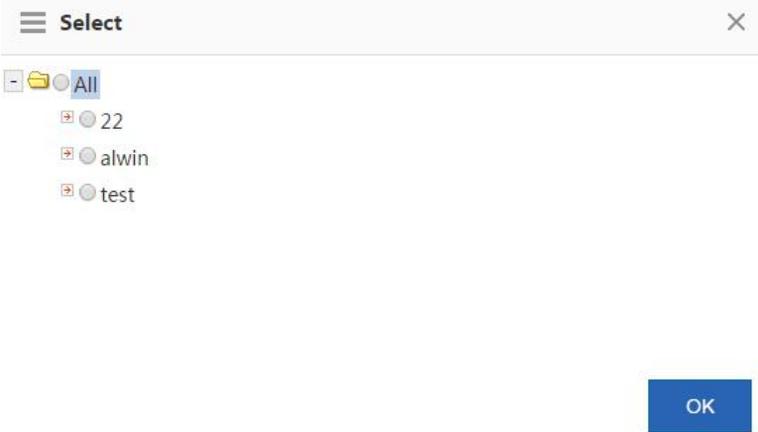
+ Add Sessions Policy

Click **+ Add Sessions Policy** 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 . In the **Select** dialog box, select users whose session quantity needs to be limited, and click .



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

Method: Select the required control mode from the  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

☰ **Add Sessions Policy**
✕

Policy Type: User-Based ACL-Based

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

Method:

Max Total Sessions: *(0-200000. 0 indicates no limit. Recommendation: >100000)*

Save
Cancel

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 [Add an ACL] 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

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

[+ Add Sessions Policy](#)
[View Sessions Per IP](#)

Policy Type	User/ACL	Method	Max Total Sessions	Max Sessions Per IP	Status	Priority	Action
ACL-Based	1	Limit Session Count	No limit	\	Active		Edit Delete
User-Based	All Users	Limit Session Count	No limit	1000	Active		Edit Delete

Show No.: Total Count:2

1 [GO](#)

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.

View Sessions Per IP		
ip	User	Sessions
192.168.1.2	/192.168.1.2	30

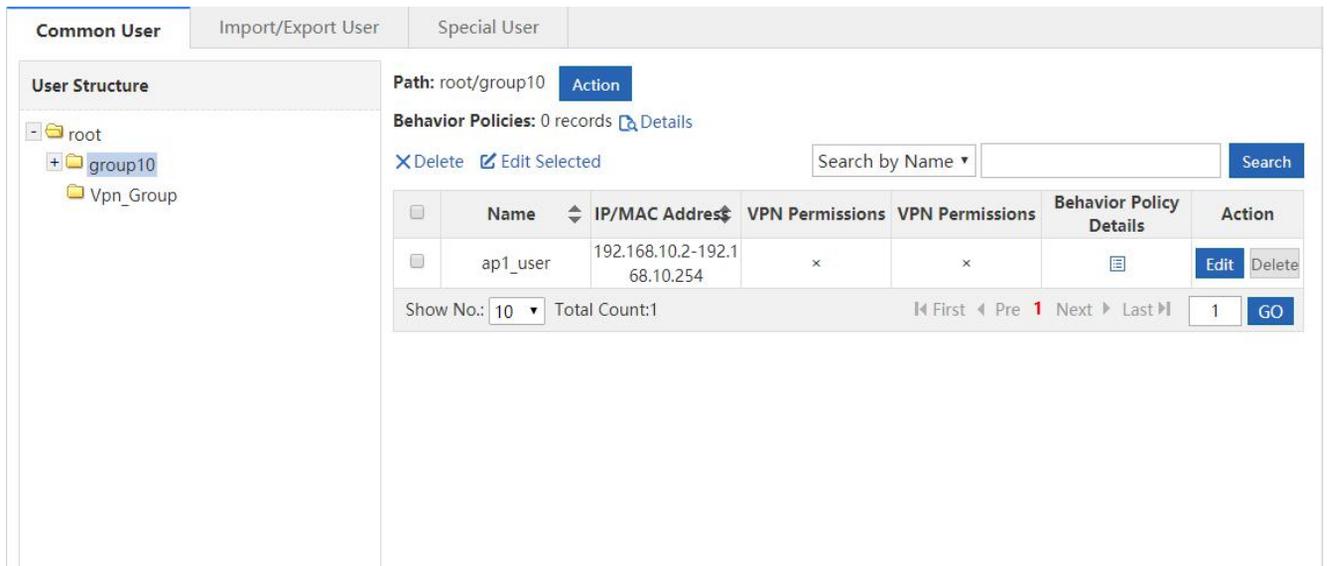
Show No.: Total Count:1 << First < Previous **1** Next Last >>

1.1.13 User

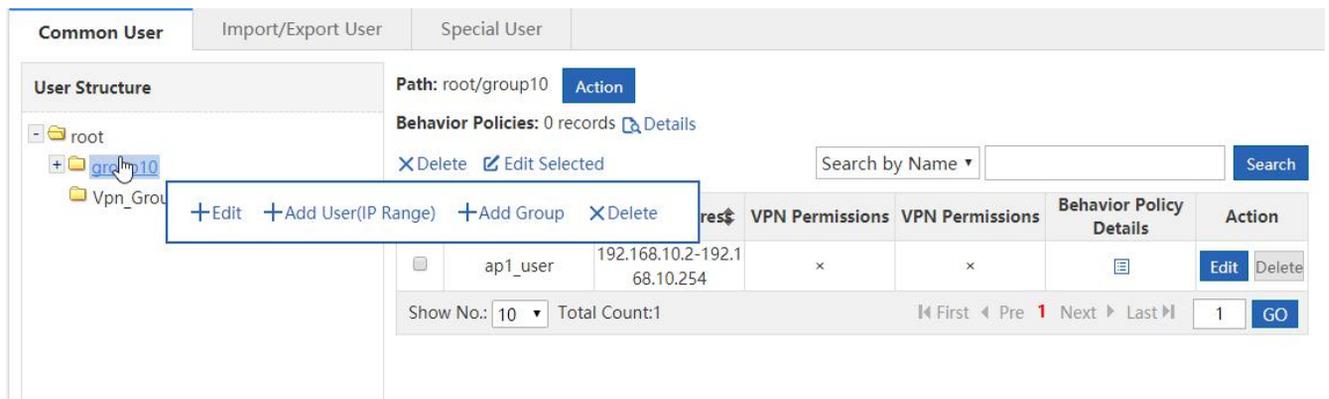
1.1.13.1 User Organization

1.3.1.1.33 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.

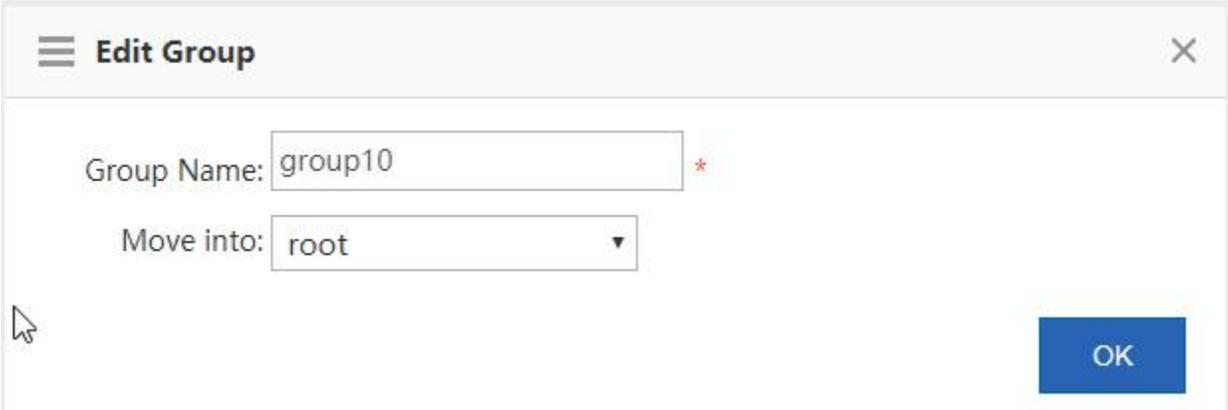


The tree-shaped hierarchy on the left side shows the organization structure of all users in the system. Select a user group. Information about the user group is displayed on the right side. You can edit and delete the information. To modify a user (group), click the user group on the left side. Then,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



+Edit

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.

+Add Group

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

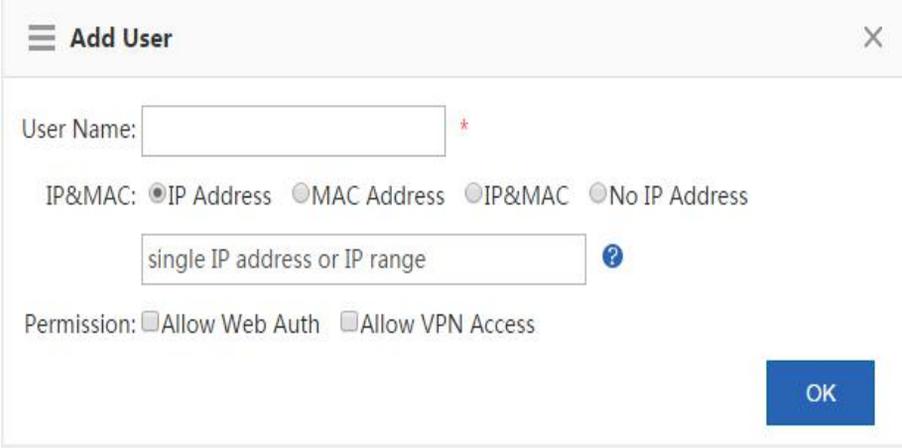


A user group name supports at most 31 characters.

XDelete

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

3. Click  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  to add a group, delete a group, and add a user.



5. User list of a user group

Path: root/testGroup [Action](#)

Behavior Policies: 0 records [Details](#)

[Delete](#) [Edit Selected](#) Search by Name [Search](#)

<input type="checkbox"/>	Name	IP/MAC Address	Behavior Policy Details	Action
<input type="checkbox"/>	testUser	9.9.9.2	Details	Edit Delete
<input type="checkbox"/>	chu	9.9.9.1	Details	Edit Delete

Show No.: 10 Total Count:2 [First](#) [Pre](#) 1 [Next](#) [Last](#) 1 [GO](#)

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

[View testUser's Policy](#) [×](#)

[+Associate More](#) [XDisassociate](#) Not Inherit (Not use policy of its parent group) [+Behavior Policy](#)

<input type="checkbox"/>	Policy Group	Type	Status	Action
No Record Found				

Show No.: 10 Total Count:0 [First](#) [Pre](#) [Next](#) [Last](#) 1 [GO](#)

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.

[Edit Selected User](#) [×](#)

Permission: Allow Internal Web Auth Allow VPN Access

Change Password: Allow Internal Web Auth User Password Change

Deny Login: Deny Internal Web Auth

[OK](#)

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

Edit User
✕

User Name: *

IP&MAC: IP Address MAC Address IP&MAC No IP Address

?

Permission: Allow Internal Web Auth Allow VPN Access

Move into :

OK

9. Enter a username or IP address in **Search by Name** **Search** to search for the required user. The search result is displayed in the table below.

✕ Delete Edit Selected

Search by Name **Search**

	Name	IP/MAC Address	Behavior Policy Details	Action
<input type="checkbox"/>	testUser	9.9.9.2		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.: Total Count:1

1

1.3.1.1.34 Import/Export User

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

Common User **Import/Export User** Special User

Note: Importing users from a CSV file helps user management
Tip: Please name the file as **user-info.csv** and fill in the file according to the following instructions

File Name: No file selected. Edit Conflicted User

Example

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

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

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

Click No file chosen , locate the **user-info.csv** file, and click .

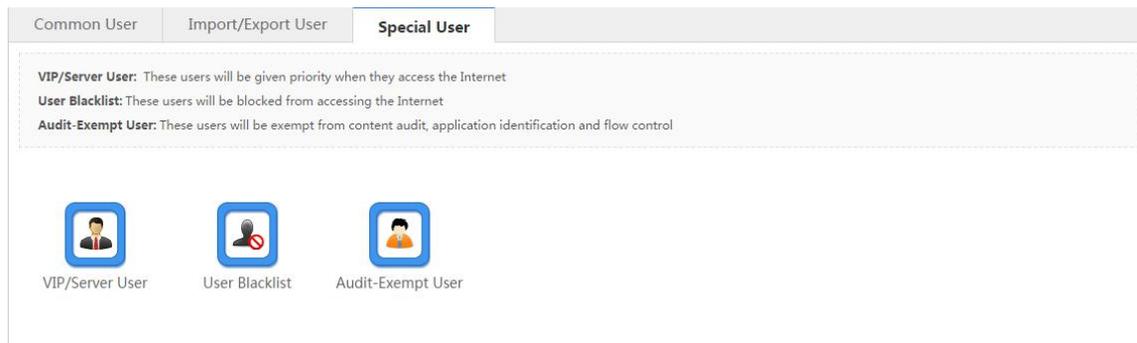
Note: Importing users from a CSV file helps user management
Tip: Please name the file as **user-info.csv** and fill in the file according to the following instructions

File Name: user-info.csv Edit Conflicted User

Export User: Click to download the **user-info.csv** file.

1.3.1.1.35 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



VIP/Server User

. 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

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



Audit-Exempt User

. 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."

1.1.13.2 Authentication/Advertisement Push

Authentication/advertisement push includes Web authentication and application authentication.

1.3.1.1.36 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.

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

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

Tip 2 : If you want to enable Telnet for Web Auth, VPN, SSLVPN and Branch, please choose System Settings > Change Password to reset the Telnet password.

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

Tip 4 : Before you enable the rate limit on SAM, please disable the flow control function on Flow>Flow Control Policy>Setting

Internal Portal Auth
 Push AD
 External Portal Auth
 Disable Web Auth

Save

● **Internal Portal Auth**

Options: iPortal Auth Push AD ePortal Auth Disable Web Auth

WiFiDog Auth: Local user preferentially [RADIUS Server](#) [SNMP Settings](#) [Online User](#)

Auth User: Common User [User Management](#)

Server Port: 8081 (1025 - 65535)

Share Account:

Advertising Mode: No AD

AD URL: Format: https://www.fs.com (Please configure DNS)

Seamless Auth: Enable ?

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

>> Advanced Settings

Save

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.

Search User: by User Na

User Name	IP	Action
Show No.: <input type="text" value="10"/> Total Count:0 <input type="button" value="First"/> <input type="button" value="Previous"/> 1 <input type="button" value="Next"/> <input type="button" value="Last"/> <input type="text" value="1"/> <input type="button" value="GO"/> 		

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.

Advanced Settings

Custom Logo: Enable *(On indicates custom logo and Off indicates default logo)*

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

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

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

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

Idle Timeout: Enable
 In *(300-3600) seconds interval, idle STAs will be kicked off.*

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

Auth-Exempt IP: Enable *You can configure either IP range or single IP address. Up to 50 auth-exempt IP addresses are supported*

IP Address: Submask: × +Add

● External Portal Auth

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

Internal Portal Auth
 Push AD
 External Portal Auth
 Disable Web Auth

Auth Solution:

Primary Server IP: *

Redirected URL: *

Specified User Subnet: [Add Backup Server](#) ?

Auth Server: [RADIUS Server](#) Please configure the auth server again when the device has a new gateway or works in the bridge mode.

NAS ID: *

NAS IP:

Encryption Method:

Encryption Password:

User Escape: Enable ?

Server Check: Enable ?

SNMP Server: [SNMP Settings](#) SNMP destination IP address is mandatory

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.

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

Backup Server ID:
 Backup Server IP: *

Redirected URL: *
 Access Network: ?

Backup Server ID	Backup Server IP	Redirected URL	User	Action
3	192.168.0.1		Null	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Show No.: Total Count:1

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

Note: Switching between gateway and bridge modes can take effect only after you configure the authentication server again. If Radius authentication is enabled for the Web authentication module and VPN/SSLVPN module, this authentication server list is shared.

Tip: If the authentication port ID is set to 0, the server does not provide authentication service. If the accounting port ID is set to 0, the service does not provide accounting service.

Tip: When the active server is unreachable, authentication requests will be sent to the first reachable standby server. Please register an account on the server with default password ruijie. If you want to enable Seamless Auth and User Escape, the account is mandatory. If there are multiple authentication servers, the password, timeout, and retransmission times are shared. If Ruijie SMP serves as a portal server, it is recommended to set the timeout to 2 seconds and retransmission times to 3. If it is a Ruijie Eportal server, set the timeout to 2 seconds and retransmission times to 1.

Password: * (The password is shared by Auth servers)

Timeout(s): (1-1,000) Retransmission Times: (0-100)

Server IP: * Auth Port: (0-65535) Accounting Port: (0-65535) Username: +Add

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.

Advanced Settings

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

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

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

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

Idle Timeout: Enable

In (300-3600) seconds interval, idle STAs will be kicked off.

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

● Push AD

Options: Portal Auth Push AD Portal Auth Disable Web Auth

AD URL: (Please configure DNS)

Session Timeout: Enable

Advanced Settings

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

Idle Timeout: Enable

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

Save

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

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

● Advanced Settings for User Authentication

Custom Logo: Enable (On indicates custom logo and Off indicates default logo)

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

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

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

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

Idle Timeout: Enable

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

Auth-Exempt IP: Enable You can configure either IP range or single IP address. Up to 50 auth-exempt IP addresses are supported

IP Address: Submask:

Save

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.

1.3.1.1.37 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.

Web Auth
Web Auth-Exempt

Auth-Exempt Network: All users including unauthenticated users can access the auth-exempt network. Up to 500 IP addresses and 500 IP ranges are supported.

Auth-Exempt User: The user can access the Internet without authentication and no ADs will be displayed. Up to 500 IP addresses and 500 IP ranges are supported.

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

Auth-Exempt Network

+ Add X Delete Selected Search Network: by IP Address/I Search

	IP Address	Submask	Description	Action
<input type="checkbox"/>	4.4.4.4	255.255.255.255		Edit Delete
<input type="checkbox"/>	43.3.3.3	255.255.255.255		Edit Delete

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

Auth-Exempt User

+ Add X Delete Selected Search User: by IP Address/I Search

	IP Address	Submask	Description	Action
<input type="checkbox"/>				

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

Auth-Exempt URL

[+Add](#) [X>Delete Selected](#) System Favorite URL: Sina iPhone WeChat
 URL: [Search](#)

<input type="checkbox"/>	URL	Action
<input type="checkbox"/>	*.qpic.cn,*.weixin.qq.com,weixin.qq.com	Delete
<input type="checkbox"/>	*.weibo.com,*.sina.com	Delete
<input type="checkbox"/>	*.iphone.com	Delete
<input type="checkbox"/>	*.facebook.com	Delete
<input type="checkbox"/>	ww.12.com	Delete

Show No.: Total Count:5

[First](#) [Pre](#) **1** [Next](#) [Last](#) [GO](#)

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 Network

[+Add](#) [X>Delete Selected](#)
Search Network: [Search](#)

<input type="checkbox"/>	IP Address	Submask	Description	Action
<input type="checkbox"/>	4.4.4.4	255.255.255.255		Edit Delete
<input type="checkbox"/>	43.3.3.3	255.255.255.255		Edit Delete

Show No.: Total Count:2

[First](#) [Previous](#) **1** [Next](#) [Last](#) [GO](#)

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 User

[+Add](#) [X>Delete Selected](#)
Search User: [Search](#)

<input type="checkbox"/>	IP Address	Submask	Description	Action
--------------------------	------------	---------	-------------	--------

Show No.: Total Count:0

[First](#) [Previous](#) **1** [Next](#) [Last](#) [GO](#)

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

Auth-Exempt URL

+ Add X Delete Selected System Favorite URL: Sina iPhone WeChat URL:

<input type="checkbox"/>	URL	Action
<input type="checkbox"/>	*.qqpic.cn,*.weixin.qq.com,weixin.qq.com	<input type="button" value="Delete"/>
<input type="checkbox"/>	*.weibo.com,*.sina.com	<input type="button" value="Delete"/>
<input type="checkbox"/>	*.iphone.com	<input type="button" value="Delete"/>
<input type="checkbox"/>	*.facebook.com	<input type="button" value="Delete"/>
<input type="checkbox"/>	ww.12.com	<input type="button" value="Delete"/>

Show No.: 10 Total Count:5 First Pre 1 Next Last 1 GO

1.1.13.3 Local Auth

1.3.1.1.38 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.

Auth Policy

Local Server Auth OFF

2. Changing policy priority

Click or to swap the match order of policies.

Auth Policy | Auth Server | **Advanced Settings** | Whitelist Settings | Single Sign-On | User Permission | Online Info

Note: 1. Bridge mode is not supported.
2. Any two among Web authentication, marketing authentication and local server authentication cannot be enabled at the same time.
3. You can configure username and password on the User page.
4. You can view AD domain user information on the User page.
5. Users who fail single sign-on will be matched with the other policies.
6. Please disable flow control if you want to configure rate limit on cloud accounts for Auth Integration with Cloud. Otherwise, rate limiting may not function accurately.

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

<input type="checkbox"/>	Policy Name	IP Range	Auth Server	Policy Type	Policy Status	Status	Match Order	Action
<input type="checkbox"/>	3	192.168.65.2-192.168.65.254	Account Auth	Voucher	<input checked="" type="checkbox"/> Enable	Active		<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	voucher_performance	192.168.2.2-192.168.63.254	Account Auth	Voucher	<input checked="" type="checkbox"/> Enable	Active		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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

3. Adding/Editing an authentication policy

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

Note: 1. Bridge mode is not supported.
 2. Any two among Web authentication, marketing authentication and local server authentication cannot be enabled at the same time.
 3. You can configure username and password on the User page.
 4. You can view AD domain user information on the User page.
 5. Users who fail single sign-on will be matched with the other policies.
 6. Please disable flow control if you want to configure rate limit on cloud accounts for Auth Integration with Cloud. Otherwise, rate limiting may not function accurately.

+ Add Policy X Delete Selected Disable Local Server Auth: Auth Integration with Cloud:

Policy Name	IP Range	Status	Match Order	Action
12	All IP Addresses	Active	↓	Edit Delete
111	All IP Addresses	Active	↑ ↓	Edit Delete
3	All IP Addresses	Active	↑	Edit Delete

Show No.: 10 Total Count: 3

4. Deleting an authentication policy

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

172.31.193.50 says
 Are you sure you want to delete policy?

OK Cancel

Scenario: General Config Wizard Online Service Hi, admin

User Permission Online Info

Note: 1. Bridge mode is not supported.
 2. Any two among Web authentication, marketing authentication and local server authentication cannot be enabled at the same time.
 3. You can configure username and password on the User page.
 4. You can view AD domain user information on the User page.
 5. Users who fail single sign-on will be matched with the other policies.
 6. Please disable flow control if you want to configure rate limit on cloud accounts for Auth Integration with Cloud. Otherwise, rate limiting may not function accurately.

+ Add Policy X Delete Selected Disable Local Server Auth: Auth Integration with Cloud:

Policy Name	IP Range	Auth Server	Policy Type	Policy Status	Status	Match Order	Action
<input checked="" type="checkbox"/>	12	All IP Addresses	Account Auth	Account	<input checked="" type="checkbox"/> Enable	Active	↓ Edit Delete
<input checked="" type="checkbox"/>	111	All IP Addresses	Null	Single Sign-On	<input checked="" type="checkbox"/> Enable	Active	↑ ↓ Edit Delete
<input checked="" type="checkbox"/>	3	All IP Addresses	Account Auth	Voucher	<input checked="" type="checkbox"/> Enable	Active	↑ Edit Delete

Show No.: 10 Total Count: 3

First Pre 1 Next Last 1 GO

1.3.1.1.39 Auth Server

1. Deleting an authentication server

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

The screenshot shows the 'Auth Server' configuration page with a confirmation dialog box. The dialog box contains the text: '172.31.193.50 says Are you sure you want to delete authentication(s) server?'. There are 'OK' and 'Cancel' buttons. The background shows a table of authentication servers with columns for Name, Auth Type, Auth Server, and Action. The table contains four rows: '22' (SMS Auth), 'testserver' (WeChat Auth), 'wechatServer' (WeChat Auth), and 'ladaServer' (LDAP Server). A 'Delete Selected' button is highlighted in the top left of the table area.

2. Adding/Editing SMS authentication

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

The screenshot shows the 'Auth Server' configuration page with the 'Add Auth Server' menu expanded. The menu options are: '+SMS Auth', '+WeChat Auth', '+QR Code Auth', '+QR Code Self-Service Auth', and '+LDAP Server'. The 'SMS Auth' option is highlighted. The background shows the same table of authentication servers as in the previous screenshot.

The screenshot shows the 'SMS Auth' configuration dialog box. It contains the following fields:

- Name: smsServer *
- SMS Gateway: Ali Cloud Communication ?
- SMS Appkey: 123123 *
- SMS Secretkey: 123 *
- SMS Signature: 1321 *
- SMS Template: 123123 *
- Pre-enter Mobile Number: Enable ?

 There is an 'OK' button at the bottom right. The background shows the 'Auth Server' configuration page with the 'Add Auth Server' menu expanded.

3. Adding/Editing WeChat authentication

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

Auth Policy | **Auth Server** | Advanced Settings | Whitelist Settings | Single Sign-On | User Permission | Online Info

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

+Add Auth Server X Delete Selected

Name	Auth Type	Auth Server	Action
testserver	WeChat Auth	-	Edit Delete
wechatServer	WeChat Auth	-	Edit Delete
ladaServer	LDAP Server	6.6.6.1	Edit Delete
smsServer	SMS Auth	-	Edit Delete

Show No.: 10 Total Count:4 First Pre 1 Next Last 1 GO

- +SMS Auth
- +WeChat Auth**
- +QR Code Auth
- +QR Code Self-Service Auth
- +LDAP Server

Auth Policy | **Auth Server** | Advanced Settings | Whitelist Settings | Single Sign-On | User Permission | Online Info

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

+Add Auth Server X Delete Selected

Name	Auth Type	Auth Server	Action
<input type="checkbox"/> testserver			
<input type="checkbox"/> wechatServer			
<input type="checkbox"/> ladaServer			
<input type="checkbox"/> smsServer			

Show No.: 10 Total Count:4 First Pre 1 Next Last 1 GO

WeChat Auth

Name:

SSID:

shopId:

appId:

secretKey:

Obtain Mobile Number: Enable [Settings](#)

[OK](#)

Auth Server	Action
-	Edit Delete
-	Edit Delete
6.6.6.1	Edit Delete
-	Edit Delete

First Pre 1 Next Last 1 GO

4. Adding/Editing LDAP server authentication

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

Auth Policy | **Auth Server** | Advanced Settings | Whitelist Settings | Single Sign-On | User Permission | Online Info

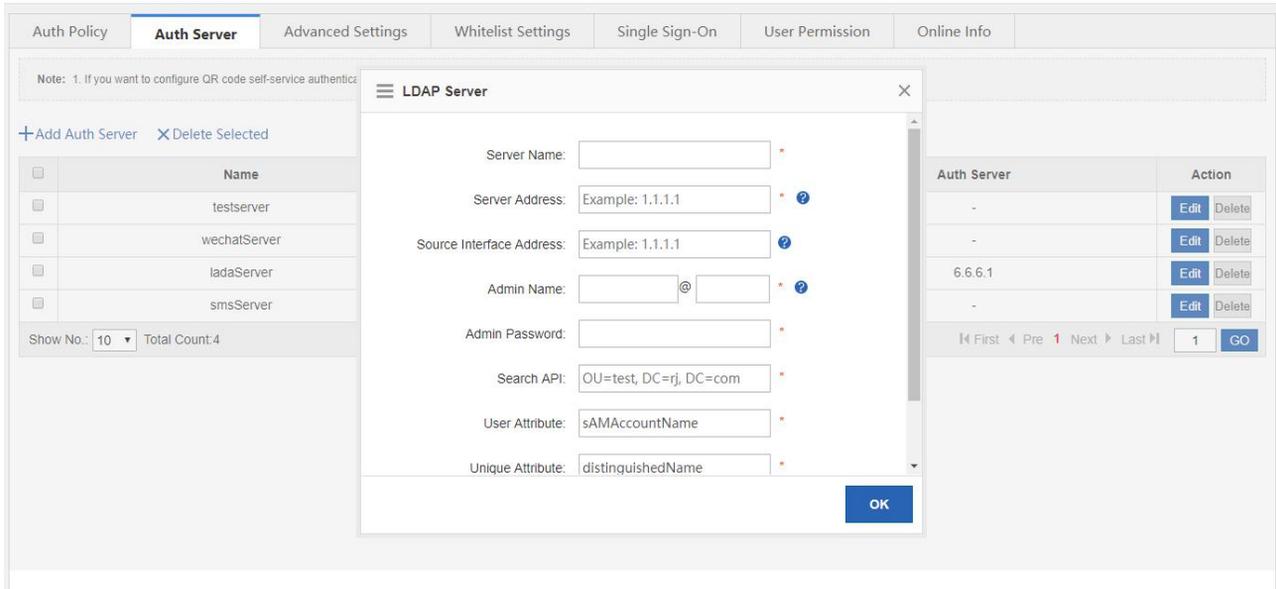
Note: 1. If you want to configure QR code self-service authentication, please enable WeChat Whitelist in Local Server Auth > Advanced Settings.

+Add Auth Server X Delete Selected

Name	Auth Type	Auth Server	Action
testserver	WeChat Auth	-	Edit Delete
wechatServer	WeChat Auth	-	Edit Delete
ladaServer	LDAP Server	6.6.6.1	Edit Delete
smsServer	SMS Auth	-	Edit Delete

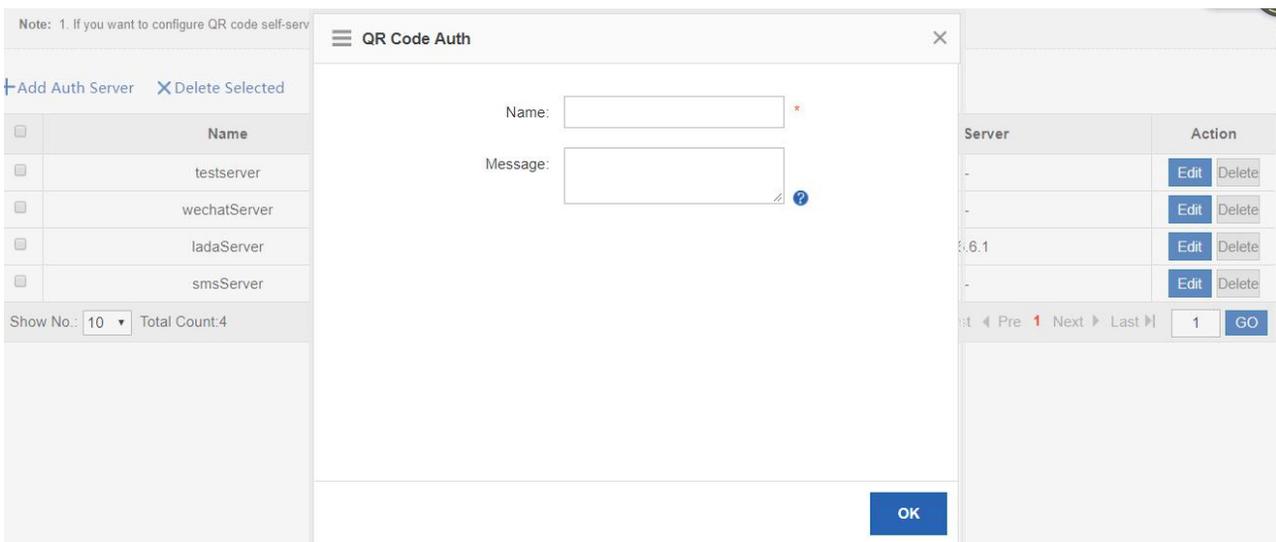
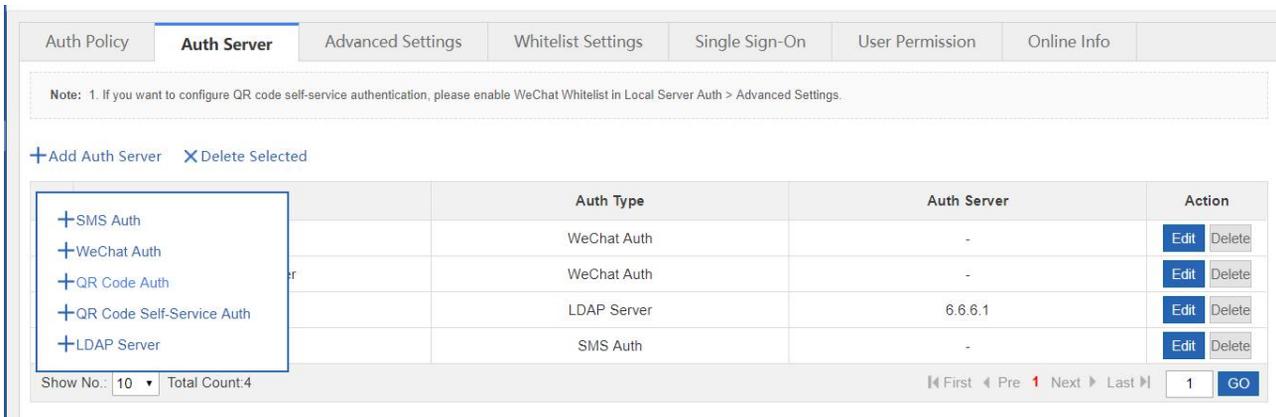
Show No.: 10 Total Count:4 First Pre 1 Next Last 1 GO

- +SMS Auth
- +WeChat Auth
- +QR Code Auth
- +QR Code Self-Service Auth
- +LDAP Server**



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.

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

+ Add Auth Server X Delete Selected

	Auth Type	Auth Server	Action
+SMS Auth	WeChat Auth	-	Edit Delete
+WeChat Auth	WeChat Auth	-	Edit Delete
+QR Code Auth	LDAP Server	6.6.6.1	Edit Delete
+QR Code Self-Service Auth	SMS Auth	-	Edit Delete
+LDAP Server			

Show No.: 10 Total Count:4 First Pre 1 Next Last 1 GO

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

+ Add Auth Server X Delete Selected

Name	Server	Action
<input type="checkbox"/> testserver	-	Edit Delete
<input type="checkbox"/> wechatServer	-	Edit Delete
<input type="checkbox"/> ladaServer	6.6.6.1	Edit Delete
<input type="checkbox"/> smsServer	-	Edit Delete

Show No.: 10 Total Count:4 First Pre 1 Next Last 1 GO

QR Code Self-Service Auth

Name: *

QR Code IP: * ?

Dynamic Code: ?

Message: ?

[Generate QR Code](#)

[OK](#)

1.3.1.1.40 Advanced Settings

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

Auth Policy	Auth Server	Advanced Settings	Whitelist Settings	Single Sign-On	User Permission	Online Info
<p>Network Type: <input checked="" type="radio"/> L2 Network <input type="radio"/> L3 Network</p> <p>Auth Page IP: <input type="text" value="Example: 192.168.1.1"/> ?</p> <p>Unauthorized Uptime: <input type="text" value="0"/> min ?</p> <p>Authorized Uptime: <input type="text" value="0"/> min ?</p> <p>Auto Remember MAC: <input type="checkbox"/> Enable ?</p> <p>Seamless Auth: <input type="text" value="Close"/> ?</p> <p>Ageout Time: <input type="text" value="60"/> Days ?</p> <p>Fetch MAC Through DHCP Snooping: <input type="checkbox"/> Enable ?</p> <p>Force Inactive Users Offline: <input checked="" type="checkbox"/> Enable ?</p> <p>Over: <input type="text" value="60"/> (1-65535) minutes, the clients with a rate lower than <input type="text" value="0"/> (0-10)KB/s will be forced offline.</p> <p>HTTPS Redirection: <input type="checkbox"/> Enable ?</p> <p>WeChat Whitelist: <input type="text" value="Enable"/> (If you enable QR code self-service authentication, please select Enable.)</p> <p>Authorization Control: <input type="checkbox"/> Enable ?</p> <p>Terminal Control: <input type="checkbox"/> Enable ?</p> <p>File Name: <input type="text" value="Choose File No file chosen"/> ? <input type="button" value="Replace Logo"/> <input type="button" value="Restore Logo"/></p> <p><input type="button" value="Save"/></p>						

1.3.1.1.41 Whitelist Settings

Auth Policy	Auth Server	Advanced Settings	Whitelist Settings	Single Sign-On	User Permission	Online Info												
<p>Whitelisted User: This user is allowed to access Internet without authentication. No AD will be pushed to this user. Up to 50 IP addresses are supported. Example: 192.168.1.2 and 192.168.2.2-192.168.2.10.</p> <p>Whitelisted External IP: All users are allowed to access this external IP address. Up to 50 IP addresses are supported. Example: 192.168.1.2 and 192.168.2.2-192.168.2.10.</p> <p>Whitelisted URL: All users are allowed to access this URL. Up to 100 URLs are supported. You can configure the key word of the URL. Example: If google.com is configured, users can access www.google.com and translate.google.com.</p> <p>Whitelisted MAC: This MAC address is allowed to access Internet without authentication. No AD will be pushed to this MAC address. Up to 100 MAC addresses are supported. Example: 0011.0022.0033.</p> <p>Blacklisted MAC: This MAC address is not allowed to access Internet. Up to 100 MAC addresses are supported. Example: 0011.0022.0033.</p> <p>Temporary Blacklist: You can configure valid time for whitelisted users, whitelisted external IP addresses, whitelisted MAC addresses and blacklisted MAC addresses. After the time expires, the settings will be removed automatically.</p> <p>Tip: Local authentication and Web authentication cannot both be enabled.</p>																		
<p>Whitelisted User</p> <p>+Add Whitelisted User X Delete Selected</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>IP Address</th> <th>Valid Time(min)</th> <th>Active Time(min)</th> <th>Description</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="6">Show No.: <input type="text" value="10"/> Total Count:0 First Previous 1 Next Last 1 GO</td> </tr> </tbody> </table>							<input type="checkbox"/>	IP Address	Valid Time(min)	Active Time(min)	Description	Action	Show No.: <input type="text" value="10"/> Total Count:0 First Previous 1 Next Last 1 GO					
<input type="checkbox"/>	IP Address	Valid Time(min)	Active Time(min)	Description	Action													
Show No.: <input type="text" value="10"/> Total Count:0 First Previous 1 Next Last 1 GO																		
<p>Whitelisted IP</p> <p>+Add Whitelisted External IP X Delete Selected</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>IP Address</th> <th>Valid Time(min)</th> <th>Active Time(min)</th> <th>Description</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="6">Show No.: <input type="text" value="10"/> Total Count:0 First Previous 1 Next Last 1 GO</td> </tr> </tbody> </table>							<input type="checkbox"/>	IP Address	Valid Time(min)	Active Time(min)	Description	Action	Show No.: <input type="text" value="10"/> Total Count:0 First Previous 1 Next Last 1 GO					
<input type="checkbox"/>	IP Address	Valid Time(min)	Active Time(min)	Description	Action													
Show No.: <input type="text" value="10"/> Total Count:0 First Previous 1 Next Last 1 GO																		
<p>Whitelisted URL</p> <p>+Add Whitelisted URL X Delete Selected</p>																		

1.3.1.1.42 Single Sign-On

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

1.3.1.1.43 User Permission

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

Registered User	Privileged Group	Search by Username	Search	
<input type="checkbox"/>	User Name	User Type	MAC Address (Terminal Type)	Action
<input type="checkbox"/>	7epzyk	Local User	8c85.90b2.0d21	Edit Delete
<input type="checkbox"/>	mv4yuc	Local User	b0e2.35ca.c64b	Edit Delete
<input type="checkbox"/>	6rvwq5	Local User	3063.6ba0.2b56	Edit Delete
<input type="checkbox"/>	w2qyv2	Local User	80ad.16ea.1dc3	Edit Delete

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

Registered User	Privileged Group	Search by Username	Search
<input type="checkbox"/>	User Name	User Type	Action
<input type="checkbox"/>	tuphfn	Local User	Delete

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

1.3.1.1.44 Online Info

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

1.1.13.4 SAM Auth

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

1.3.1.1.45 IPFIX Accounting

IPFIX Accounting

IPFIX: Internet Protocol Flow Information Export (IPFIX) is an accounting technology. IPFIX monitors traffic flows through a switch or router, counts the number of bytes and packets, and sends the data to an accounting server.
Tip: Accounting requires SAM correlation SAM

IPFIX Settings

IPFIX: Enable (Please set SAM to Auth & Accounting Mode)

Null Traffic Detection: Enable (Please disable Kick Inactive Users Off on the Web Auth > Advanced Settings page)

Rate Limit: * 1-65535

[Save](#)

IPFIX

[+ Add Policy](#) [X Delete Selected](#)

<input type="checkbox"/>	Policy ID	Src IP Group	Dst IP Group	Traffic Type	Policy Status	Status	Priority	Action
<input type="checkbox"/>	22	0	0	Campus	<input checked="" type="checkbox"/> Enable	Active		Edit Delete

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

1. Enabling IPFIX

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

2. Adding an IPFIX policy

Click [+ Add Policy](#) to add a policy. Enter a policy ID, a source IP group and a destination group, select the traffic type and click [Save](#)

IPFIX Settings

IPFIX: Enable (Please set SAM to Auth & Accounting Mode)

Null Traffic Detection: Enable (Please disable Kick Inactive Users Off on the Web Auth > Advanced Settings page)

Rate Limit: *

[Save](#)

IPFIX

[+ Add Policy](#) [X Delete Selected](#)

<input type="checkbox"/>	Policy ID	Src IP Group	Dst IP Group	Traffic Type	Policy Status	Status	Priority	Action
<input type="checkbox"/>	22	0	0	Campus	<input checked="" type="checkbox"/> Enable	Active		Edit Delete

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

IPFIX

Policy ID: * Range: 1-100

Src IP Group: * Range: 0-1,000 IP Object Group

Dst IP Group: * Range: 0-1,000

Traffic Type:

[Save](#)

3. Deleting an IPFIX policy

Click [Delete](#) to delete an IPFIX policy or click [X Delete Selected](#) to delete selected IPFIX policies.

1.3.1.1.46 Correlation

Click [SAM](#) to enable or disable SAM correlation. Enter the address of the SAM server into the Server IP Address text box.

IPFIX: Internet Protocol Flow Information Export (IPFIX) is an accounting technology. IPFIX monitors traffic flows through a switch or router, counts the number of bytes and packets, and sends the data to an accounting server.
Tip: Accounting requires SAM correlation SAM

Change Password Restart System Time Enhancement SNMP **Correlation**

The SAM association mode is determined by the device type when the SAM server adds a gateway device. By default, two EG modes are supported.

Gateway Auth & Accounting Mode: Authentication, accounting, user routes, real-name flow control are supported. When the SAM server adds a gateway device, select Web Gateway Auth Device. The default port ID is 2009. To enable IPFIX traffic-based charging, select this mode.

Gateway Auth Mode: Only authentication, user routes, and real-name flow control are supported. Accounting is not supported. When the SAM server adds a gateway device, select Egress Associated Device. The default port ID is 2012.

Server Association

Association Type: Disable Association
Disable Association
Enable SAM Association

1.1.13.5 Block Internet Access

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

Block Internet Access

Note: All users will be blocked from accessing the Internet except whitelisted users
Tip: Please make sure to disable Floating AD, App Cache and Resource Acceleration before enabling Block Internet Access.

Enable

+ Add Whitelisted User X Delete Selected

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

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

Block Internet Access

Note: All users will be blocked from accessing the Internet except whitelisted users
Tip: Please make sure to disable Floating AD, App Cache and Resource Acceleration before enabling Block Internet Access.

Enable

Add Whitelisted User

Q

- All Users
- Vpn_Group
 - test

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

OK

	IP Address	MAC Address	Delete
First Previous 1 Next Last	1	GO	

Select the whitelisted user and click **OK** :

Block Internet Access

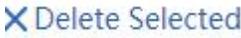
Note: All users will be blocked from accessing the Internet except whitelisted users
Tip: Please make sure to disable Floating AD, App Cache and Resource Acceleration before enabling Block Internet Access.

Enable

+ Add Whitelisted User X Delete Selected

	User Name	IP Address	MAC Address	Delete
<input type="checkbox"/>	test	#	#	Delete

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

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

1.1.13.6 Floating AD

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

Floating AD

Tip: Please make sure to disable Block Internet Access before enabling Floating AD.
 The floating AD conflicts with policy-based route.

Floating AD: Enable (Please restart the device after the settings are complete)

AD URL:
The URL cannot be longer than 255 characters

Block AD Based on IP: +Add

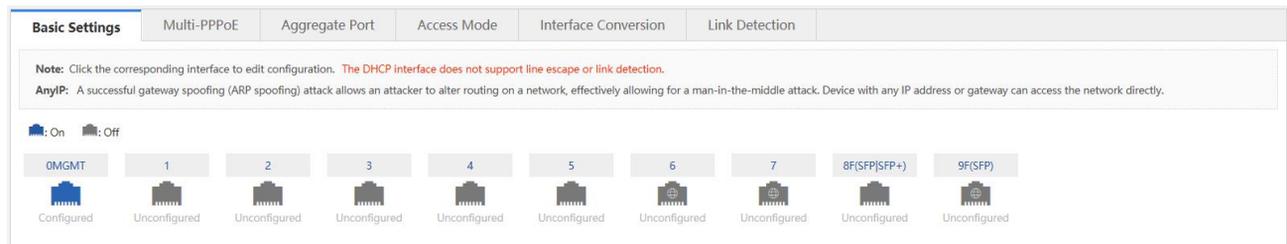
Block AD Based on Domain Name: +Add

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.

1.1.14 Network

1.1.14.1 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.



1.3.1.1.47 Basic Interface Settings

- Port Configuration



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



2 (Gi0/2) Setting
[Interface Conversion](#)
[Sub Interface](#)
[DHCP Settings](#)

IP Address: *

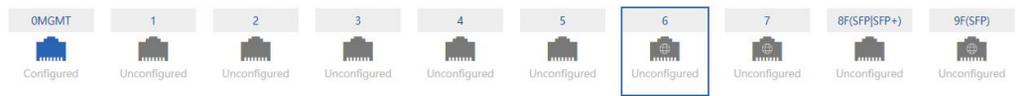
Submask: *

Advanced Settings

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

Submask: Enter the mask address of the network segment.

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.



6 (Gi0/6) Setting Static IP Interface Conversion Sub Interface

IP Address: *

Submask: *

Gateway: *

Advanced Settings

Save Clear

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

- **Static IP**

The figure above shows the static IP address configuration page. When **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.

6 (Gi0/6) Setting PPPoE(ADSL) Interface Conversion Sub Interface

Username: *

Password: *

IP Address: Auto-obtain

Advanced Settings

Save Clear

- **DHCP**

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

6 (Gi0/6) Setting DHCP Interface Conversion Sub Interface

IP Address: Auto-obtain

Advanced Settings

Save Clear

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.

1.3.1.148 Multi-link Aggregation

Basic Settings	Multi-PPPoE	Aggregate Port	Access Mode	Interface Conversion	Link Detection
Load Balance: <input type="text" value="Src IP + Dest IP"/> +Add					
Aggregate Port	Member Port	Action			
No Record Found					
Show No.: <input type="text" value="10"/> Total Count: 0					<input type="button" value="First"/> <input type="button" value="Pre"/> <input type="button" value="Next"/> <input type="button" value="Last"/> <input type="text" value="1"/> <input type="button" value="GO"/>

Click [+Add](#). In the window displayed, select an aggregate port and member ports, and click .

+ Add Aggregate Port
×

Aggregate Port:

Type: LAN Port WAN Port

Member Port: Gi0/0 Gi0/1 Gi0/2 Gi0/3 Gi0/4 Gi0/5 Te0/0 ?

1.3.1.149 Access Mode

Bridge Mode : The device works as a bridge which can create a single aggregate network from multiple communication networks or network segments.

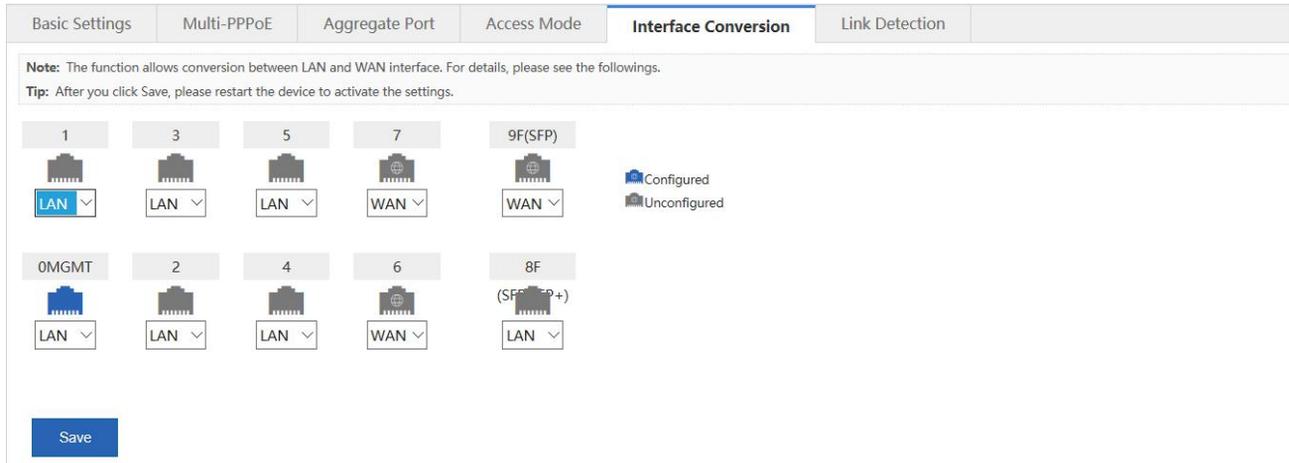
Gateway Mode : The device works as a router which can forward packets.

Access Mode: Bridge Mode Gateway Mode

Select the required access mode, and click . The device switches to the selected mode successfully after restart.

1.3.1.150 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.



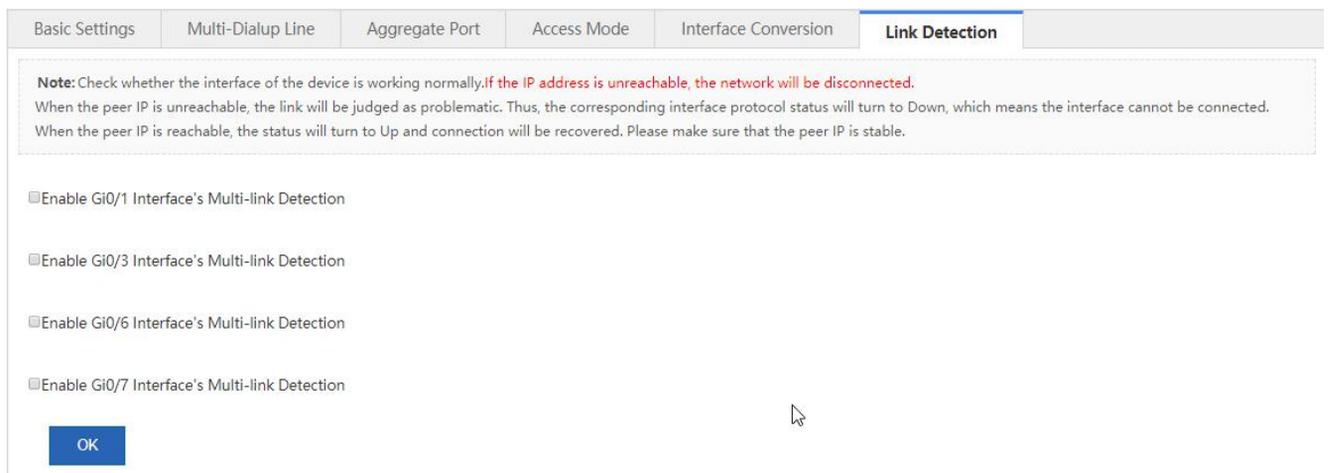
Click a drop-down list to convert an LAN port into a WAN port or vice versa and click . The interface mode takes effect after the device is restarted.

1.3.1.1.51 Multi-PPPoE



1.3.1.1.52 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:

Enable Gi0/6 Interface's Multi-link Detection

Select the interface to be detected. For example, select Gi0/6. The link detection configuration items of Interface Gi0/6 will be displayed.

IP Address: * Next Hop IP: * Detection Interval: ms

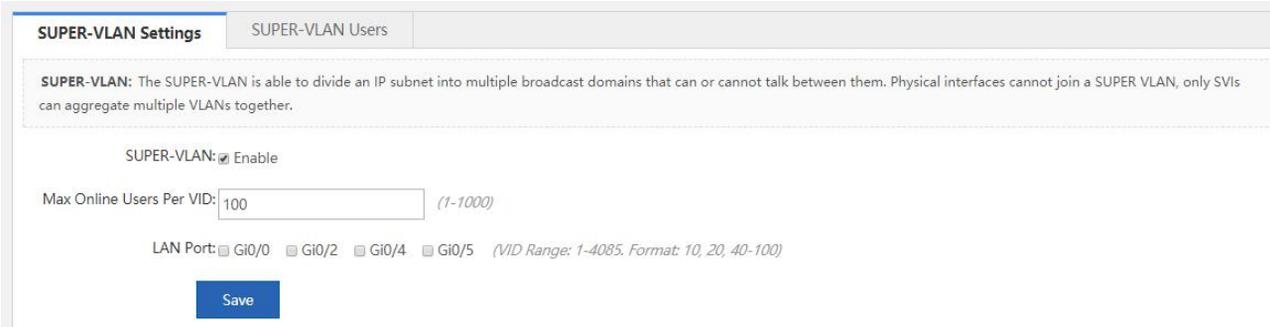
- To detect whether the interface is reachable, enter an address that can be pinged successfully in **IP Address**.
- Enter the next-hop IP address. If the device is a LAN device, enter the gateway address. If it is not configured, the next-hop address is the ping IP address by default.
- Set **Detection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

1.1.14.2 SUPER-VLAN

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

1.3.1.1.53 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 to save the configuration.

1.3.1.1.54 Online SUPER-VLAN Information

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

SUPER-VLAN Settings

SUPER-VLAN Users

Note: The maximum online user count per VID is 100. For other VLANs, if there is no online users, nothing will be listed.

Tip: If duplicate IP exists, an IP conflict may occur.

No data.

1.1.14.3 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.

1.3.1.1.55 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.

Priority: The policy-based route, application-based route, and IP-based route all serve packet forwarding. When they exist at the same time, the priority is listed as follows: policy-based route > application-based route > static route > default route.

Note: Policy-based route is a flexible packet forwarding policy. A next hop address is required in Ethernet environment, and an interface is required in PPPoE environment.

Interface:

Policy Priority: * (0~65535)

ACL ID: [\[Add ACL\]](#)

Outbound Interface/Next Hop: [PPPoE Environment] *An interface is required in PPOE environment.*

Policy-Based Route List Interface: [X Delete All](#)

Policy Priority	ACL ID	Interface	Next Hop Address	Action
No Record Found				

Show No.: Total Count: 0

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 [Add](#).

ACL list: You can click [\[Add ACL\]](#) 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

Policy-Based Route List Interface: [X Delete All](#)

Policy Priority	ACL ID	Interface	Next Hop Address	Action
No Record Found				

Show No.: Total Count:0 First Pre Next Last 1 [GO](#)

Edit a policy: In the policy-based route list, click [Edit](#) to modify a policy.

Delete a policy: In the policy-based route list, click [Delete](#) to delete a policy. You can click [X Delete All](#) in the upper right corner to delete all routing policies in the policy group.

1.3.1.1.56 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.

Policy-Based Route **IP-Based Route** Load Balance

Priority: The policy-based route, application-based route, and IP-based route all serve packet forwarding. When they exist at the same time, the priority is listed as follows: policy-based route > application-based route > static route > default route.
IP-Based Route: It can transmit packet according to the specified path and includes static route, address database and default root. Among them, the default route has the lowest priority.

[+Add Static Route](#) [+Add Default Route](#) Filter Criteria:

Dest Network	Submask	Next Hop Address	Outbound Interface	Route	Action
0.0.0.0	0.0.0.0	172.31.62.1		Primary Route	Edit Delete

Show No.: Total Count:1 First Pre **1** Next Last 1 [GO](#)

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.

☰ **Add Default Route**
✕

Outbound Interface:

Next Hop IP: * (Gateway Address)

Route: * (The primary route will be given top priority. Backup route-N: A smaller N indicates a higher priority.)

OK
Cancel

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

[+Add Static Route](#) [+Add Default Route](#)
Filter Criteria: All

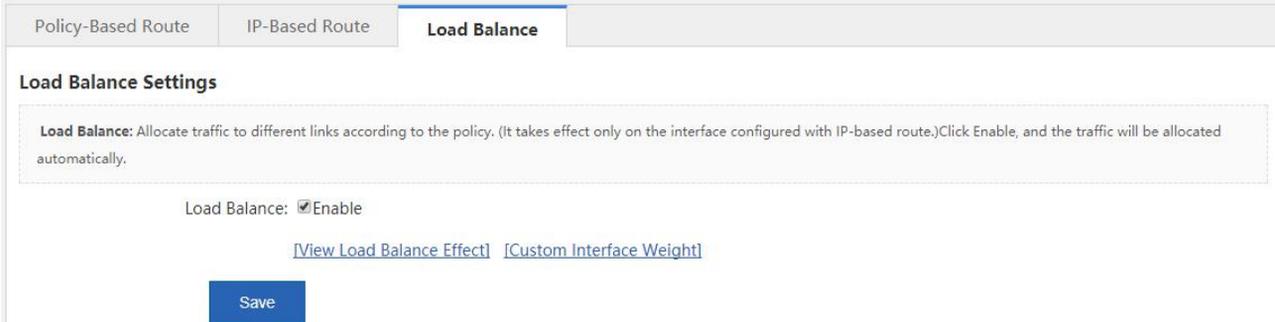
Dest Network	Submask	Next Hop Address	Outbound Interface	Route	Action
0.0.0.0	0.0.0.0	200.23.0.1	GigabitEthernet 0/6	Primary Route	Edit Delete
0.0.0.0	0.0.0.0	200.100.0.1	TenGigabitEthernet 0/7	Primary Route	Edit Delete
0.0.0.0	0.0.0.0	200.24.0.1	TenGigabitEthernet 0/6	Primary Route	Edit Delete
0.0.0.0	0.0.0.0	6.6.6.1		Primary Route	Edit Delete
0.0.0.0	0.0.0.0	200.16.0.1	FortyGigabitEthernet 0/1	10	Delete
172.21.0.0	255.255.0.0	172.18.31.193		Primary Route	Edit Delete

Show No.: 10 Total Count:6
⏪ First ◀ Pre 1 Next ▶ Last ⏩ 1 [GO](#)

Click **Delete** to delete a default route.

1.3.1.157 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.

1.1.14.4 DNS

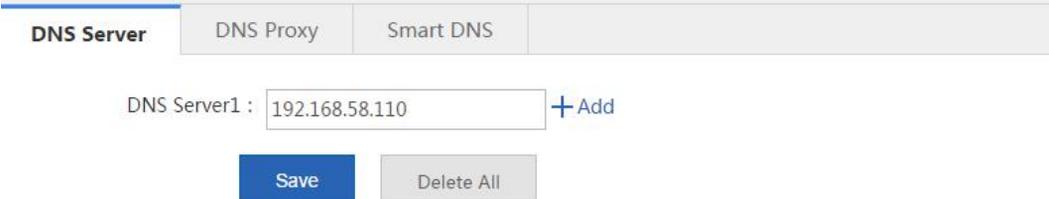
The Domain Name Server (DNS) configuration includes the DNS server configuration, DNS proxy configuration, and smart DNS configuration.

1.3.1.158 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](#).



1.3.1.159 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.

Basic Settings: The DNS agent function must be enabled if you want to make the function like DNS proxy, DNS blacklist and DNS whitelist take effect.
DNS Whitelist: You can configure IP address and DNS server which will not be affected by the DNS proxy function.
IP Range Format: 192.168.1.1-192.168.1.150

Basic Settings | DNS Blacklist | DNS Whitelist

Note: When the DNS proxy is enabled, the LAN client can configure the DNS freely without affecting the Internet connection. Please configure the ISP for the specific line on Interface page after enabling the DNS proxy function.

Enable DNS Proxy on LAN Port: Gi0/0 Gi0/2 Gi0/4 Gi0/5
 Enable DNS on WAN Port: Gi0/1 Gi0/3 Gi0/6 Gi0/7

Save

DNS Proxy Statistics

DNS Requests Intercepted: 0
 DNS Replies Intercepted: 0
 DNS Blacklist Hit: 0 DNS Whitelist Hit: 0
 User Route Hit: 0 Load Balance Hit: 0

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.

Basic Settings | **DNS Blacklist** | DNS Whitelist

Rogue IP/IP Range: * **Add**

IP/IP Range	Action
5.5.5.5	Delete

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

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).

Basic Settings		DNS Blacklist		DNS Whitelist	
Type:	IP/IP Range	*	IP/IP Range:		* Add
Type			DNS Whitelist		Action
Show No.:	10	Total Count:	0		First Previous 1 Next Last GO

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.

1.1.14.5 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.

1.3.1.1.60 Config Wizard

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



What is VPN?

Technology for establishing LANs on the Internet
Virtual Private Network (VPN) refers to the technology for establishing dedicated networks on the Internet. A virtual dedicated data transmission channel can be established between two nodes on the Internet over a VPN. The two nodes mutually transfer data through this channel without external interference or eavesdropping.

Small LANs form large LANs
Branches access the VPN of the headquarters to share the information platforms, resources, and data of the company.

Mobile users access company network
Employees who go home or have business trips can access the VPN of the company for work through computers.

[Configure](#)

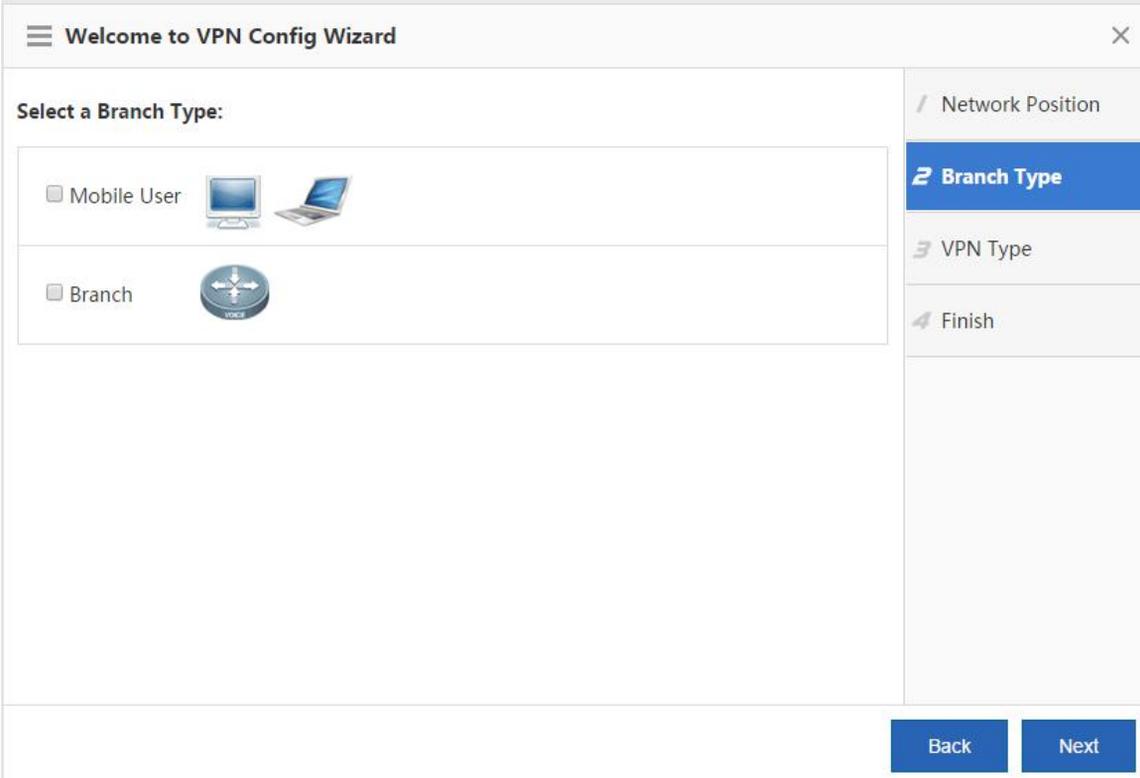
Click **Configure** to configure a VPN. A page shown in the figure below is displayed.



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  to display the **Branch Type** page shown in the figure below.



Welcome to VPN Config Wizard

Select a Branch Type:

Mobile User 

Branch 

Network Position

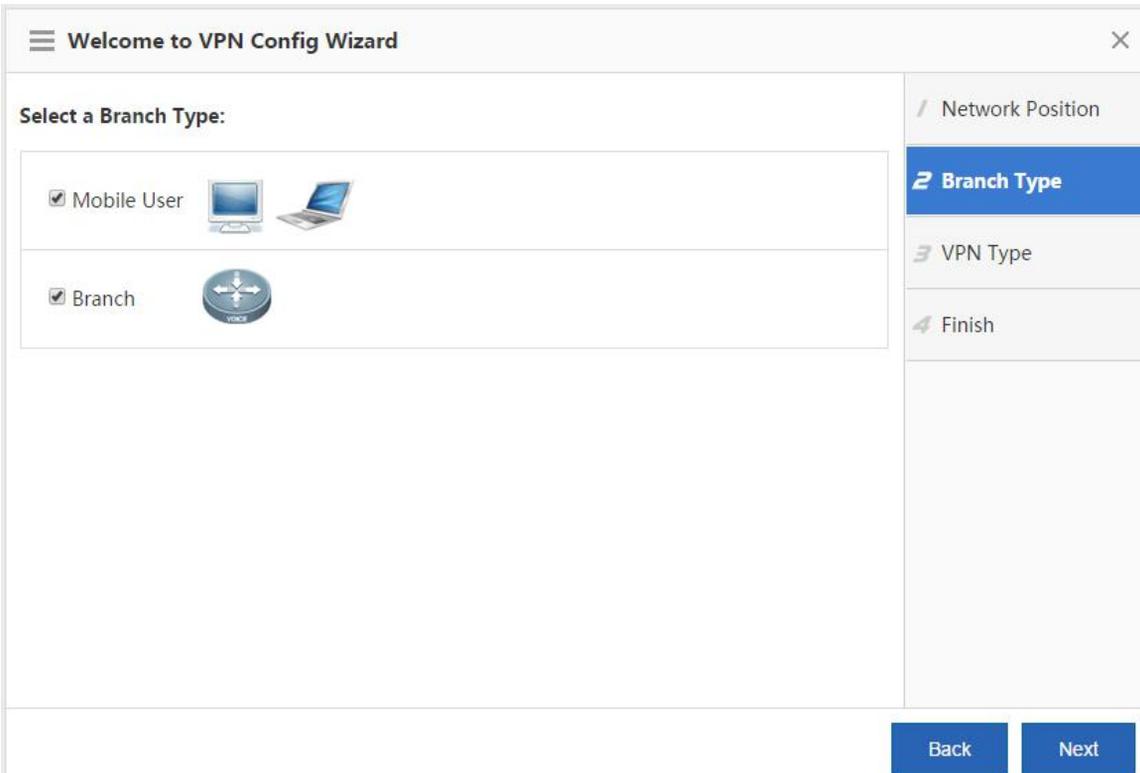
2 Branch Type

3 VPN Type

4 Finish

Back Next

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.



Welcome to VPN Config Wizard

Select a Branch Type:

Mobile User 

Branch 

Network Position

2 Branch Type

3 VPN Type

4 Finish

Back Next

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.

☰ Welcome to VPN Config Wizard
✕

Enter Basic Information

Client IP Range: ~ *

Please make sure that the IP addresses are not in use in the LAN.

HQ Domain Name:

Primary DNS Server:

Secondary DNS Server:

If a mobile user wants to access the LAN through the domain name, a DNS server address should be configured which is usually the same with the address of the LAN DNS server.

>> Advance Settings <<

1 Network Position

2 Branch Type

3 VPN Type

4 Configure Basic Info

5 Manage Account

6 Configure L2TP IPsec

7 Finish

Back
Next

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.

through the domain name, a DNS server address should be configured which is usually the same with the address of the LAN DNS server.

>> Advance Settings <<

Local Tunnel IP: *

Local Tunnel Mask: *

PPTP Keepalive Interval: second(s)

L2TP Keepalive Interval: second(s).

L2TP Verification Code: Enable

Allow HQ to Access

Branch: Enable 

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

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

1. Before enable the function, please first plan the network segment, plan the tunnel IPs allocated to all branches, and enable the "Allow HQ to Access Branch" function on the corresponding device.

2. It is recommended to configure the "Branch Tunnel IP" from the end IP of the "Client IP Range", for example, if the "Client IP Range" is from 192.168.3.2 to 192.168.3.254, then please set the "Branch Tunnel IP" to an IP address greater than 192.168.3.254.

Note: If multiple networks exist in a branch, please follow the following format.

Branch Tunnel IP	The branch network		
<input type="text" value="192.168.3.254"/>	<input type="text" value="172.18.102.0"/>	<input type="text" value="255.255.255.0"/>	+
<input type="text" value="192.168.3.254"/>	<input type="text" value="172.18.103.0"/>	<input type="text" value="255.255.255.0"/>	×

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

Add Branch User Name: Password: **Add**

☰ Welcome to VPN Config Wizard
✕

Save Account on

Local Device
 Other System ?

Add Branch User Name: Password: **Add**

Type:	User Name	Action
+	testuser	编辑 删除

Show No.: 10 Total Count:1
 ⏪ First ⏴ Previous 1 Next Last ⏩ 1 **GO**

Back
Next

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

☰ Welcome to VPN Config Wizard
✕

Save Account on

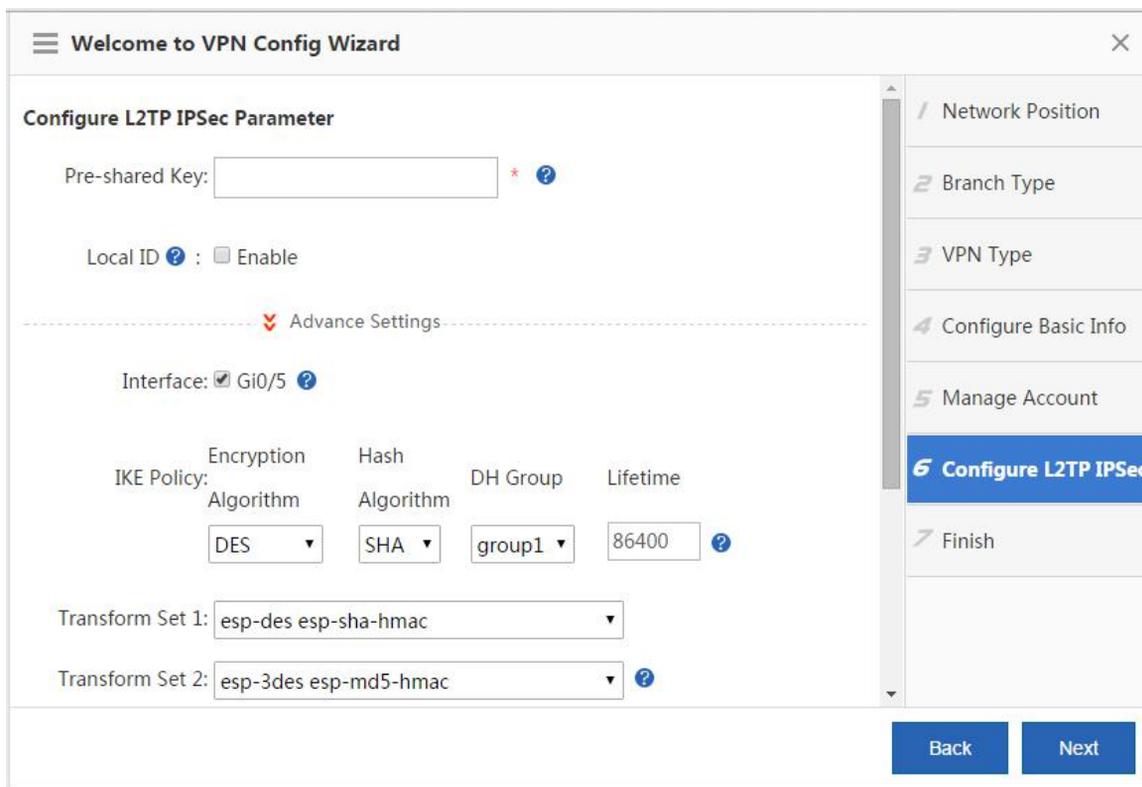
Local Device
 Other System ?

Add Branch User Name: Password: **Add**

Type:	User Name	Action
+	testuser	编辑 删除

Back
Next

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.



Welcome to VPN Config Wizard

Configure L2TP IPsec Parameter

Pre-shared Key: * ?

Local ID ? : Enable

----- Advance Settings -----

Interface: Gi0/5 ?

IKE Policy:	Encryption	Hash	DH Group	Lifetime
	Algorithm	Algorithm		
	DES	SHA	group1	86400 ?

Transform Set 1:

Transform Set 2: ?

Back Next

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.

☰ Welcome to VPN Config Wizard
✕

Configure L2TP IPSec Parameter

Pre-shared Key: * ?

Local ID ? : Enable *

⌵ Advance Settings

Interface: Gi0/5 ?

IKE Policy:	Encryption Algorithm	Hash Algorithm	DH Group	Lifetime
	<input type="text" value="DES"/>	<input type="text" value="SHA"/>	<input type="text" value="group1"/>	<input type="text" value="86400"/>

Transform Set 1:

Transform Set 2:

- 1 Network Position
- 2 Branch Type
- 3 VPN Type
- 4 Configure Basic Info
- 5 Manage Account
- 6 Configure L2TP IPSec
- 7 Finish

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.

☰ Welcome to VPN Config Wizard
✕

Configure IPSec Parameter

Pre-shared Key: * ?

Local ID ? : Enable

Network Config Wizard

Local Network	The branch network	Outbound Interface	
192.168.1.0	IP	Please select an interface	+
255.255.255.0	mask		✕
192.168.10.0	IP	Please select an interface	+
255.255.255.0	mask		✕

⌵ Advance Settings

Encryption Hash

- 1 Network Position
- 2 Branch Type
- 3 VPN Type
- 4 Configure IPSec
- 5 Finish

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

☰ Welcome to VPN Config Wizard
✕

The VPN is created.

Then:

View branch configuration. [View](#)

- 1 Network Position
- 2 Branch Type
- 3 VPN Type
- 4 Configure Basic Info
- 5 Manage Account
- 6 Configure L2TP IPsec
- 7 Finish

Back
Finish

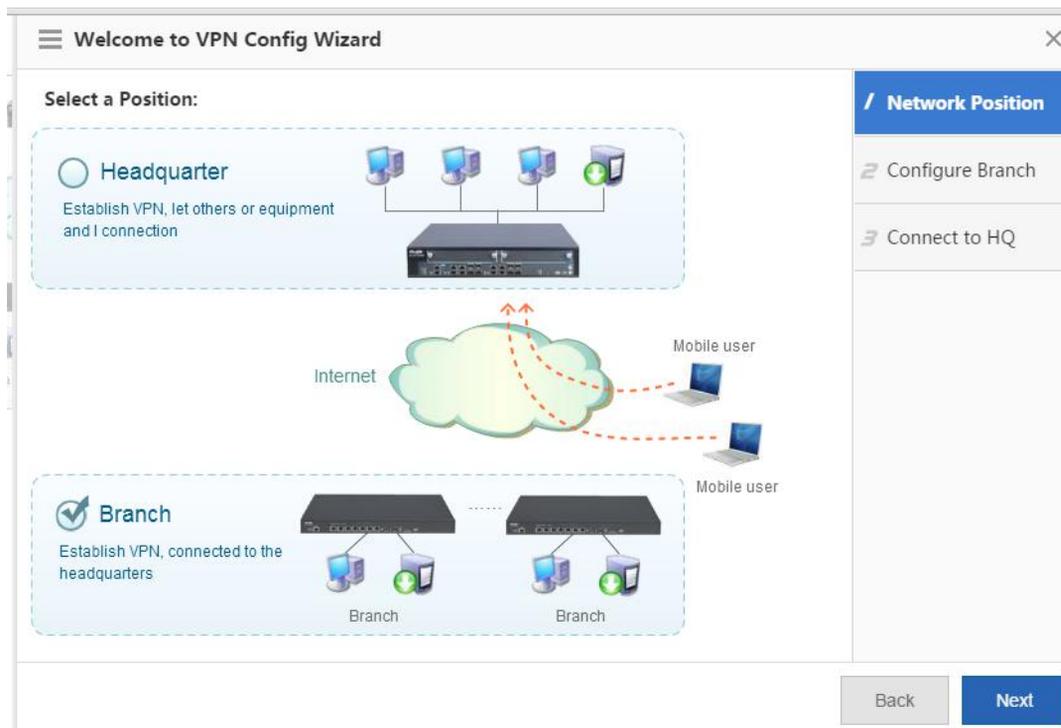
Click [View](#) to display all configurations, as shown in the figure below. Click **Finish** in the lower right corner to complete the VPN configuration for the headquarters device.

Mobile User				
Public IP:	172.21.2.114			
Configuration Step:	+ Windows XP Configuration Reference + Windows 7 Configuration Reference			
Branch L2TP IPsec VPN				
Public IP:	172.21.2.114			
Pre-shared Key:	123456			
HQ Network:	Network:192.168.1.0 Submask:255.255.255.0			
Transform Set 1:	esp-des esp-sha-hmac			
: Transform Set 2:	esp-3des esp-md5-hmac			
IKE Policy:	No.	Encryption Algorithm	Hash Algorithm	DH Group
	1	3DES	SHA	group1
	2	DES	SHA	group1
	3	3DES	SHA	group2
	4	DES	MD5	group1
5	DES	SHA	group1	
L2TP Verification Code:	Disable			
Allow HQ to Access	Disable			

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

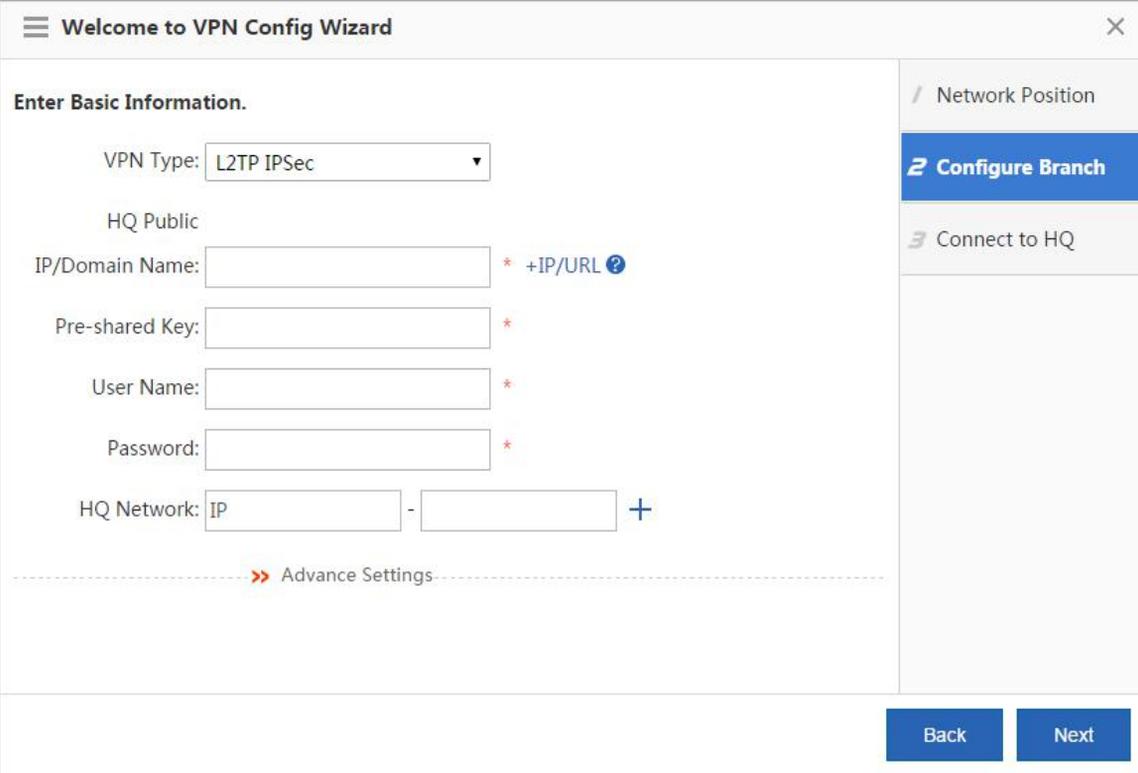
server of the headquarters device.

- **VPN Configuration for the Branch Device**



Next

Click **Branch** and click **Next** 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

Allow HQ to Access

Branch: Enable

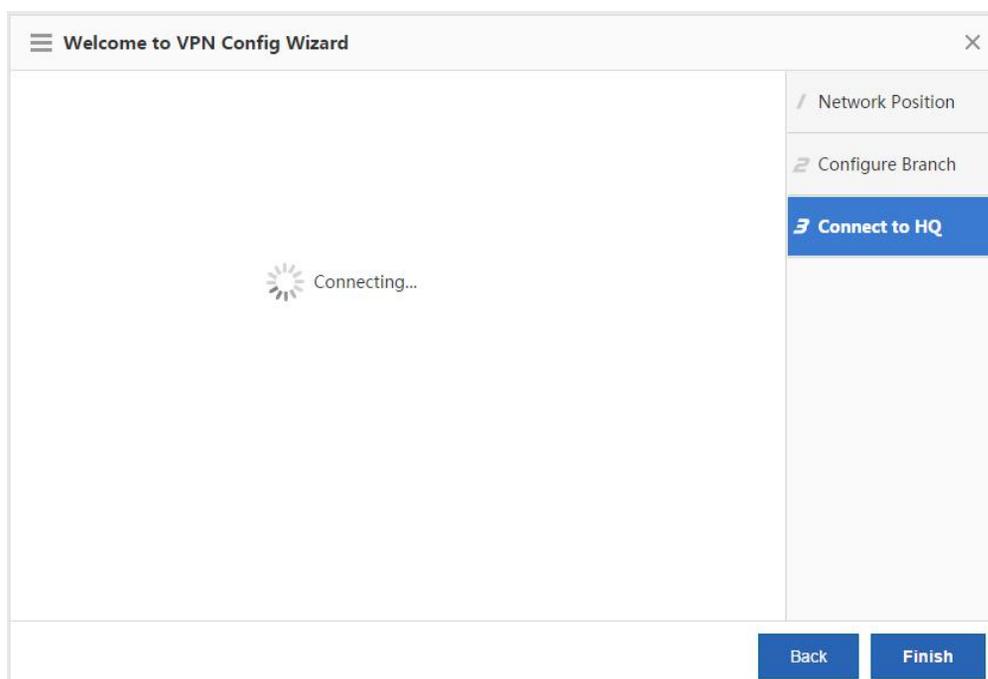
is selected, when a branch device accesses the WAN, the traffic goes through the VPN and

Allow HQ to Access

Branch: Enable

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.

1.3.1.1.61 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. 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.

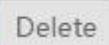
When the current device serves as a VPN branch device, it connects to the headquarters device above. Click to set the current device as a VPN branch device and connect it to other devices. You can click this icon multiple times to connect the current device to multiple VPN headquarters devices. The current device can be connected to a maximum of nine VPN headquarters devices.

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.

If the current device serves only as a VPN branch device, you can click to configure this device as the VPN headquarters device.

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    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.

Local VPN

View headquarter configuration | **View branch configuration**

Basic Parameters Edit Clear

VPN Type: PPTP L2TP IPsec L2TP IPsec

Client IP Range: 192.168.7.1 to 192.168.7.254 *

HQ Domain Name:

Primary DNS Server: 192.168.58.110 Secondary DNS Server: 192.168.58.111

Local Tunnel IP: 192.168.7.1 * Local Tunnel Mask: 255.255.255.0 *

Other System: Enable

L2TP Keepalive Interval: 600 second(s)

Cancel

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.

Local VPN

View headquarter configuration | View branch configuration

HQ 1 | HQ 2

VPN Parameters Edit Clear

VPN Type: L2TP IPsec

Enable ?

HQ Public IP/Domain Name: 192.168.3.1 * +IP/URL

Pre-shared Key: *

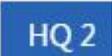
IPsec Lifetime: 3600 second(s)

User Name: testUser * Password: ... *

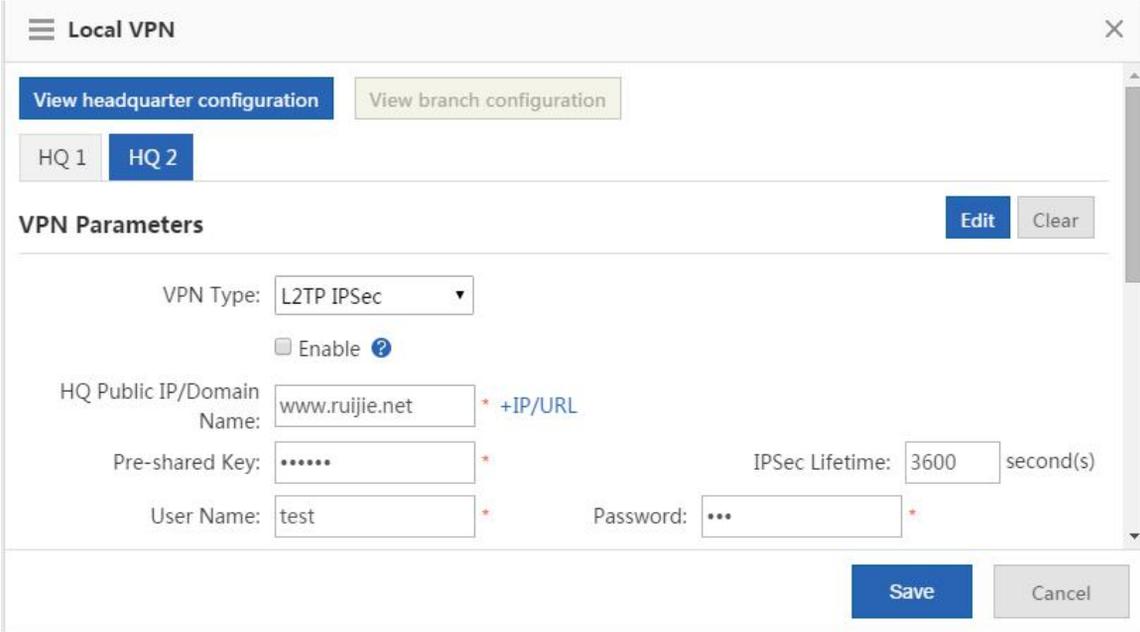
Cancel

If the current device serves as a VPN branch device and connects to multiple headquarters devices, multiple options are displayed. For

example,   indicates that the VPN configuration of the current device connected to Headquarters 1 is displayed.

Click . The VPN configuration of the current device connected to Headquarters 2 is displayed.

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



After the editing is completed, click .

Click  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.

Mobile User

Total Total: 0 mobile User(s) connected. Click [here](#) to manage mobile user.

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.

☰ Mobile User
✕

[User Management]

Search: Search

Total Total: 0 Mobile User(s) Connected

User Name	Connection	Connected on	Private IP	Public IP	Action
Show No.: <input type="text" value="10"/> Total Count: 0 ⏪ First ⏩ Previous 1 Next Last ⏪ 					

GO

Cancel

1.1.14.6 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.

1.3.1.1.62 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.

NAT Rule

NAT Address Pool

Port Mapping

Multi-Port Mapping

Note: It applies ACL to NAT address pool to make NAT rule take effect.

+ Add ✕ Delete Selected

	ACL ID	Address Pool
<input type="checkbox"/>	1 📄	nat_pool

Show No.: Total Count: 1

 ⏪ First ⏩ Pre 1 Next ⏪ Last ⏪

GO

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.

☰ Add NAT Rule
✕

ACL ID: [Add ACL]

Address Pool:

OK
Cancel

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

1.3.1.1.63 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

1.3.1.1.64 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.

Map the internal Web server IP 192.168.1.200 and port 80 to external IP 200.10.10.10 and port 80

Description:

Mapping Relationship: port mapping

Internal IP:192.168.1.200

Internal Port: 80

External IP -> Address: 200.10.10.10

External Port: 80

and Protocol Type: TCP .

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.

1.3.1.1.65 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.

Note: You can map an internal server address to different external IP addresses corresponding to different ISPs. If an internal IP is mapped to multiple external IPs, the internal user cannot access the internal server by using the mapped external IP.

+ Add X Delete Selected Search by Internal IP: Search

	Internal IP	External IP	Interface	Action
<input type="checkbox"/>	6.6.6.6	9.9.9.9	GigabitEthernet 0/6	Edit Delete

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

1.1.14.7 DHCP

1.3.1.166 Server Settings

Settings Static IP Address User List

+ Add DHCP X Delete Selected DHCP O Excluded Address Range DHCP: ON

<input type="checkbox"/>	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
<input type="checkbox"/>	STA_Pool	192.168.10.1-192.168.10.254	192.168.10.1	Permanent	192.168.5.28	Edit Delete
<input type="checkbox"/>	AP_Pool	192.168.1.1-192.168.1.254	192.168.1.1	Permanent	192.168.5.28	Edit Delete

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

● Add DHCP

Add DHCP ✕

Pool Name: *

Subnet: * Format: 192.168.1.0

Mask: * Format: 255.255.255.0

Default Gateway: * Format: 192.168.1.1

Lease Time: Permanent Lease Time d h min *

Preferred DNS Server: * Format: 114.114.114.114

Secondary DNS Server:

Option 43: ?

[Save](#) [Cancel](#)

● Delete Selected DHCP

+ Add DHCP X Delete Selected DHCP O Excluded Address Range DHCP: ON

<input checked="" type="checkbox"/>	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
<input checked="" type="checkbox"/>	pool1	2.2.2.1-2.2.2.254	2.2.2.2	Permanent	192.168.58.110	Edit Delete

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

172.21.2.11:9091 says:

Are you sure you want to delete the address pools

Prevent this page from creating additional dialogs.

[OK](#) [Cancel](#)

- **Excluded Address Range**

☰ Excluded Address Range
✕

Excluded Address Range: Excluded addresses will not be allocated to the client. The excluded address range is formatted as 1.1.1.1-1.1.1.30. Entering only 1.1.1.1 indicates one single excluded address.

Excluded Address - **+**

Range1 :

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

- **DHCP**

+ Add DHCP
 ✕ Delete Selected DHCP
 ⊗ Excluded Address Range
 DHCP: ON

- **Edit DHCP**

☰ Edit DHCP
✕

Pool Name: *

Subnet: * Format: 192.168.1.0

Mask: * Format: 255.255.255.0

Default Gateway: * Format: 192.168.1.1

Lease Time: Permanent Lease Time d h min *

Preferred DNS Server: * Format: 114.114.114.114

Secondary DNS Server:

Option 43: ?

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

● **Deleting a DHCP address pool**

Settings Static IP Address User List

+ Add DHCP X Delete Selected DHCP O Excluded Address Range DHCP: ON

<input checked="" type="checkbox"/>	Name	IP Address Range	Default Gateway	Lease Time	DNS	Action
<input checked="" type="checkbox"/>	pool1	2.2.2.1-2.2.2.254	2.2.2.2	Permanent	192.168.58.110	Edit Delete

Show No.: 10 Total Count: 1

172.21.2.11:9091 says:

Please retain at least one DHCP address pool for the DHCP service. Are you sure you want to delete the address pool?

Prevent this page from creating additional dialogs.

[OK](#) [Cancel](#)

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

1.3.1.1.67 Static IP Address

Settings **Static IP Address** User List

+ Add Static Address X Delete Selected Address

<input type="checkbox"/>	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
No Record Found							

Show No.: 10 Total Count: 0

First Pre Next Last 1 GO

● **Add Static Address**

Add Static Address X

Client Name: *

Client IP: * Format: 192.168.1.1

Mask:

Client MAC: * Format: 0002.0002.0002

Gateway Address:

DNS:

[Save](#) [Cancel](#)

● **Delete Selected Address**

+ Add Static Address X Delete Selected Address

<input type="checkbox"/>	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
<input type="checkbox"/>	clien1	5.5.5.5	255.255.255.0	5.5.5.1	0002.0002.0002	192.168.58.110	Edit Delete

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

172.21.2.11:9091 says:

Please select a DHCP address range.

Prevent this page from creating additional dialogs.

[OK](#)

● **Edit Static Address**

Edit Static Address X

Client Name: *

Client IP: * Format: 192.168.1.1

Mask:

Client MAC: * Format: 0002.0002.0002

Gateway Address:

DNS:

[Save](#) [Cancel](#)

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

● **Deleting a static address**

+ Add Static Address X Delete Selected Address

<input type="checkbox"/>	Client Name	Client IP	Mask	Gateway Address	Client MAC	DNS Server	Action
<input type="checkbox"/>	clien1	5.5.5.5	255.255.255.0	5.5.5.1	0002.0002.0002	192.168.58.110	Edit Delete

Show No.: 10 Total Count: 1 Last 1 GO

172.21.2.11:9091 says:

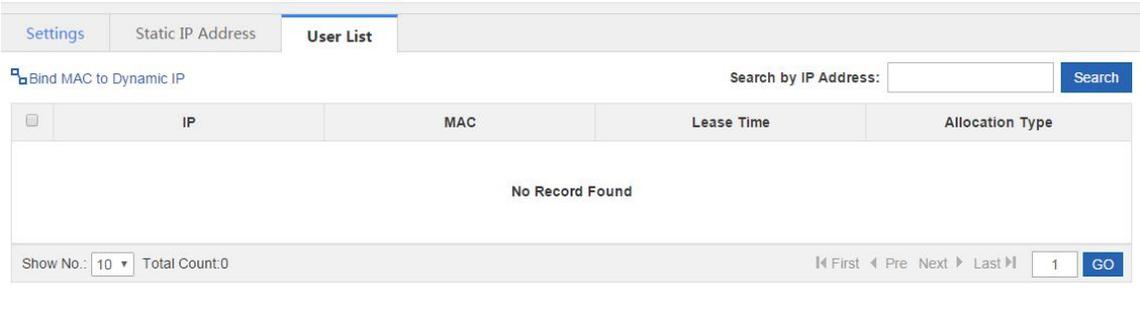
Are you sure you want to delete the static address?

Prevent this page from creating additional dialogs.

[OK](#) [Cancel](#)

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

1.3.1.1.68 User List



IP	MAC	Lease Time	Allocation Type
No Record Found			

- **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**.



1.1.15 **Advanced**

1.1.15.1 **System**

1.3.1.1.69 **Change Password**

Note: User admin has all permissions to configure and view device information.

Login Password Settings

User Name: admin

New Password: *

Confirm Password: *

Telnet Password Settings

User Name: admin

New Password: *

Confirm 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.

1.3.1.1.70 **Restart**

Tip: The restart may take about 1 minute. Please wait. The system automatically jumps to the Login page after restart. Please re-log in.

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.

1.3.1.1.71 **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.

1.3.1.1.72 Backup

Note: Do not close or refresh the page during import. Otherwise, the import will fail.

Tip: After the configuration is imported, please click **Restart** on the current page to apply the new configuration.

Export Config

File No file chosen

View Config

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.

1.3.1.1.73 System Time

Change Password	Restart	Factory Reset	Backup	System Time	Enhancement	SNMP/SAM
-----------------	---------	---------------	--------	--------------------	-------------	----------

Tips: Changing the system time may cause incorrect audit time of history traffic reports.

Tip: After Sync with Internet Time Server is enabled, check whether the **DNS Server** is correctly configured for the synchronization function to take effect.

System Time Settings

Current Time: 2020.9.14 Afternoon 8:32:52

Reset Time:

Time Zone:

Sync with Internet Time Server

Sync with Internet Time Server via Management Port

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.

1.3.1.1.74 Enhancement

System	Change Password	Restart	Restore	Backup	System Time	Enhancement	SNMP
--------	-----------------	---------	---------	--------	-------------	-------------	------

Hardware Bypass
Bypass enables two networks to be physically connected via a specific triggering state (power-off or shut-down), without using a network security system.

[Hardware Bypass Settings](#)

Feedback
After the feedback function is enabled, the system automatically sends an email to you about concerned information or alarms.

[Feedback Settings](#)

Prompt Upon Blocked Access
This function refers to the prompt displayed when users access a forbidden Website. For example, If you choose Behavior Policy > Website Blacklist/Whitelist and specify www.xxx.com as the forbidden Website, this prompt is displayed when users access this website.

You are forbidden to visit the website, please contact webmaster!

[Save](#)

Traffic Audit Data Refresh Interval
This function helps you increase the frequency of refreshing traffic data.

Refresh Interval: seconds ▾

[OK](#)

Storage Duration of Traffic Audit Database
Set storage duration of the traffic audit database.

Daily Reports: days. Weekly Reports: weeks. Monthly Reports: months. Other reports: days.

[OK](#)

Storage Duration of Content Audit Database
Set storage duration of the content audit database.

Content Audit Data: days.

[OK](#)

Web Login Timeout
Set the Web login timeout duration.

minutes

[OK](#)

Device Name
Specify a name to identify a device.

*

[OK](#)

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.

Note: It is a bypass function that allow two network devices connect without the network security system, but directly the physical conduct by a particular triggered state (power failure or crash) .

Bypass bridge 1: Gi0/0 <->Gi0/1

Bypass bridge 2: Gi0/2 <->Gi0/3

Save

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: Enable: *(The device sends feedback to you as required.)*

Sending Server: * Example: smtp.126.com.

Server Port ID: * Port 25 of the sending server is used by default.

Sender Account: * Example: xxx@126.com.

Password: *(The encrypted password is not displayed. You need to enter the password only when you re-configure the account or change the password.)*

Sending Frequency: Minute *(5-10080)*

Receiver: * Separate multiple email addresses by ",". A maximum of 6 email addresses are allowed.

Verification: [Send a test email.](#)

Concerned Info: Tick your concerned information. Feedback will include your choices.

- The device is under attack
- The traffic has reached the limit
- The cache of flow control has reached the limit

Feedback: Select [Feedback: Enable:](#) 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: Tel. No.:

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

1.3.1.1.75 SNMP

Change Password
Restart
Factory Reset
Backup
System Time
Enhancement
SNMP

SNMP: The Simple Network Management Protocol (SNMP) allows administrators to easily monitor and manage network nodes.
 Note: Switching between gateway and bridge modes can take effect only after you configure the SNMP again.

SNMP

SNMP Version: V2 V3

Device ID: *

SNMP Password: *

Trap Password:

SNMP Dest Host: ?

Trap Recipient: Up to 9 Trap recipients can be set. Separate the IP addresses by ",".

Save
Cancel

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.

SNMP

SNMP Version: V2 V3

Device ID: *

SNMP User: *

Encryption Password: *

Auth Password: *

Trap Password:

SNMP Dest Host: ?

Trap Recipient: *Up to 9 Trap recipients can be set. Separate the IP addresses by ",".*

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

1.1.15.2 Upgrade

System Upgrade

Note: You can click Software Version at Ruijie Networks website to download the latest upgrade file to the local device and upgrade the device. Do not close or refresh the current page during the upgrade until an upgrade success prompt is displayed. Otherwise, the upgrade fails.

Tip: 1. Please ensure that the upgrade version matches the device model. 2. Do not perform other operations during upgrade.

Local Upgrade

File: No file chosen

Signature Database

Application Class Database Version: 2019.02.25.19.02.25(V3.0)
URL Database Version: 2017-12-4

Automatic Update

Enable

Update Time: : Every Day

You can click the software version at FS 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.

NOTE:

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**.

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



Signature Database

Application Class Database Version: 2019.10.12.19.10.12(V3.0)

URL Database Version: 2018-5-7



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

1.1.15.3 Administrator

Administrator

[+ Add Admin](#)

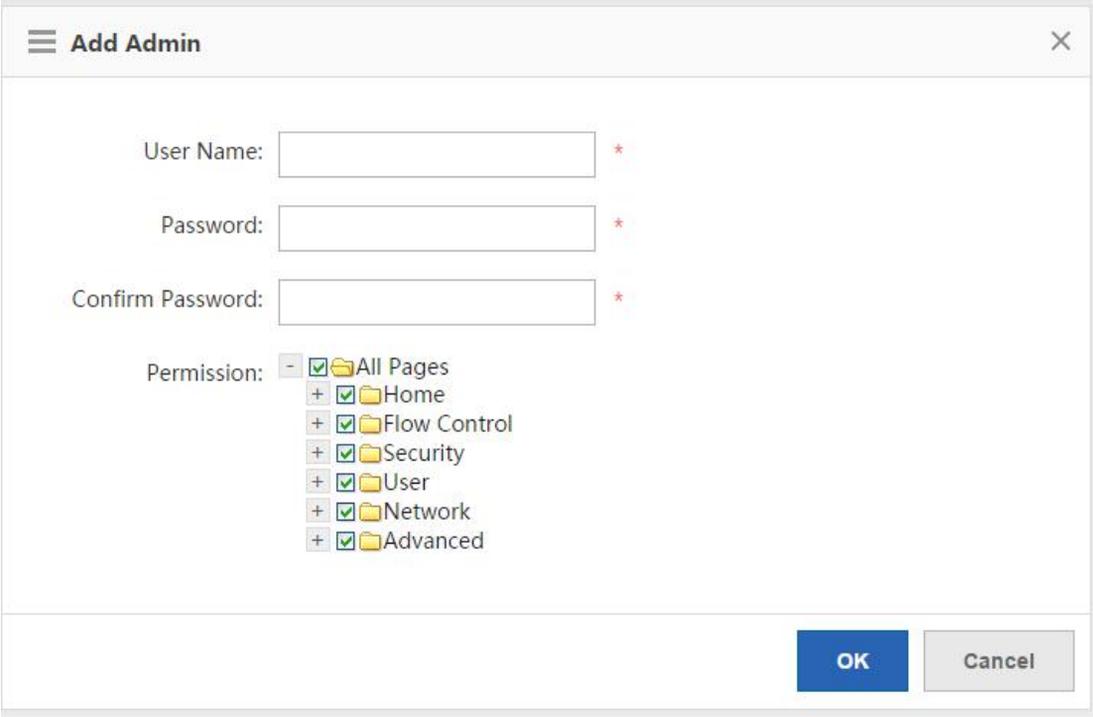
User Name	Action
guest	Edit Delete
test	Edit Delete

Show No.: Total Count:2

[First](#) [Pre](#) [Next](#) [Last](#)
 [GO](#)

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.



The **Add Admin** dialog box contains the following fields and options:

- User Name:** A text input field with a red asterisk indicating it is required.
- Password:** A text input field with a red asterisk indicating it is required.
- Confirm Password:** A text input field with a red asterisk indicating it is required.
- Permission:** A list of permissions with checkboxes:
 - All Pages
 - Home
 - Flow Control
 - Security
 - User
 - Network
 - Advanced

At the bottom right, there are **OK** and **Cancel** buttons.

User Name: Enter an administrator name.

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.

1.1.15.4 Issue Collection

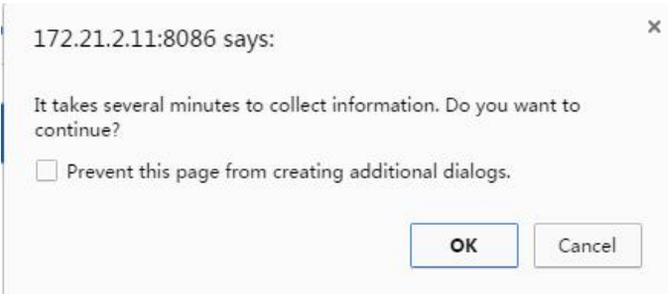
The one-click collection function collects device fault information for troubleshooting.

Note: One-Click Collection is used to collect fault information for troubleshooting.

Tip: For a packet capture tool, please click [here](#)

One-Click Collection

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

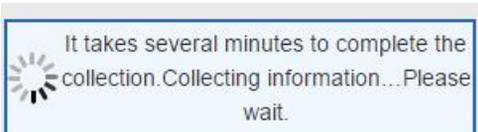


The dialog box from 172.21.2.11:8086 says:

It takes several minutes to collect information. Do you want to continue?

Prevent this page from creating additional dialogs.

Buttons: **OK**, **Cancel**



It takes several minutes to complete the collection. Collecting information... Please wait.

Download

After the collection, click **Download** to generate a package, for example, **tech_vsd0_20150727172504.tar.gz**. This package facilitates 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: One-Click Collection is used to collect fault information for troubleshooting.

Tip: For a packet capture tool, please click [here](#)

Packet Capture

[+Add Capture Point](#) [+Add Rule](#) [+Edit Rule](#).

Capture Point	Rule Name	Interface	Status	Action
No Record Found				

Packet capture finishes. Please download the file.

Start
Stop
Download
Clear

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

1.1.15.5 Connectivity Detection

Connectivity detection includes ping detection and tracer detection.

Ping Detection

Tracert Detection

Egress Interface Detection

Dest IP/Domain Name: *

Repetition Times (1-100):

Detect

The ping detection page is shown in the figure below.

Dest IP/Domain Name: *

Repetition Times (1-100):

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 >Translating "www.google.com"... [OK]Sending 5, 100-byte ICMP Echoes to 59.24.3.173, timeout is 2 seconds: <
press Ctrl+C to break >....Success rate is 0 percent (0/5).
```

The tracert detection page is shown in the figure below.

Dest IP/Domain Name: *

Detect

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.

Ping Detection	Tracert Detection	Egress Interface Detection	
----------------	-------------------	-----------------------------------	--

Delay Detection

Detection Method: All Interfaces Specific Interface Src IP & Dest IP

Detect

Half Open Connections:
Null

Delay:
Null

Routing Traffic:
Null

DNS Resolution Detection

Domain Name: *

DNS Server: *

WAN Port: *

Detect

DNS Resolution:--- , TCP Connection:--- , http get : --- ,

Resolved to IP:---

The DNS resolution detection is shown in the figure below.

Delay Detection

Detection Method: All Interfaces Specific Interface Src IP & Dest IP

[Detect](#)

Half Open Connections:
Null

Delay:
Null

Routing Traffic:
Null

DNS Resolution Detection

Domain Name: *

DNS Server: *

WAN Port: *

[Detect](#)

DNS Resolution:--- , TCP Connection:--- , http get : --- ,

1.1.15.6 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, **FS#** 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, **FS(config)#** is displayed after **config** is entered, and some commands are usually configured in this mode).

Schedule

Scheduled Task: Scheduled tasks are used for executing designated CLI commands on the device at designated 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: Privileged EXEC mode (that is, FS# is displayed after login, and is usually used to execute the show command) and global configuration mode (that is, FS(config)# is displayed after config is entered, and is usually used to configure some commands).

Enable:

Task

[+ New Task](#) [+ Add Restart Task](#)

Time	Task Name	Command Mode	Cycle Time	Command	Action
Show No.: <input type="text" value="10"/> Total Count: 0					First Previous 1 Next Last 1 GO

Scheduled Task Log

Enable:

[View](#) [Clear](#)



Click **Enable: ON** 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.

Configure Scheduled Task ✕

Task Name: * *Up to 16 bytes are supported.*

Execution Mode: ▾

Command: * *Up to 512 bytes are supported.*

Time: *

Cycle Time: h min **Range: 1-168 hours (a week)** *Cycle operation is not executed by default.*

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.

Scheduled Task Log

Enable: ON

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

☰ **Configure Scheduled Task**
✕

Task Name: * *Up to 16 bytes are supported.*

Execution Mode: ▾

Command: * *Up to 512 bytes are supported.*

Time: *

Cycle Time: h min Range: 1-168 hours (a week) *Cycle operation is not executed by default.*

☰ **Configure Scheduled Task**
✕

Task Name:

Time: *

Cycle Time: ▾ * Weekly Monday undefined Restart

1.1.15.7 Central Management

Central management includes MCP management and RAC-SNC management.

1.1.15.8 VRRP

VRRP

Note: The Virtual Router Redundancy Protocol (VRRP) adopts the master/backup mode, to ensure that when the master router malfunctions, the backup router conducts a switch without affecting the internal and external data communication, and parameters of the internal network do not need to be modified.

Tip: When the VRRP group IP address is the same as the interface IP address, the VRRP priority is set to 255.

Interface: Gi0/0 Gi0/2 Gi0/4 Gi0/5

Group ID: * (1-255)

Group IP: *

Priority: (1-254)

[Add](#)

[X Delete All](#)

Group ID	Interface	Group IP	Priority	Action
No Record Found				

Show No.: Total Count:0 First Pre Next Last [GO](#)

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.

1.1.15.9 System Log

1.3.1.1.76 Server Log

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

Note: The port ID of the device shall be the same as the peer server port ID. If the peer device is an SNC server, only the CPU/memory usage logs, hard disk usage logs, interface session audit logs, IP traffic audit logs, and interface traffic audit logs are supported. If the peer device is an ELOG server, only flow logs, URL audit logs, IM audit logs, BBS audit logs, and Email audit logs are supported and the port ID shall be set to 20,000 or above.

Tip: Logs with a higher priority are sent first. The digit 0 indicates the highest priority, while the digit 7 indicates the lowest priority. You can set one file upload mode only and log priorities are not differentiated. The log type can only be set to file or real-time. The HTTP port shall be the same as the server HTTP port.

Log Upload Mode: Real Time File Upload

Server IP: *

Port: * (10000-65000)

Server Type: ▼

Src IP: ?

» Transmission Log Type

Server IP	Log Upload Mode	Server Type	Port	Via MGMT Interface	Log Type	Other	Action
No Record Found							

Show No.: Total Count:0 First ◀ Pre Next ▶ Last ▶ 1

- Server IP:** Enter the IP address of the server for receiving logs.
- 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.
- Transmission Log Type:**

Transmission Log Type

<input type="checkbox"/> Enable Flow Log <input type="text" value="4"/> ▼	<input type="checkbox"/> CPU/Memory Usage Log <input type="text" value="4"/> ▼	<input type="checkbox"/> Hard Disk Usage Log <input type="text" value="4"/> ▼
<input type="checkbox"/> Enable URL Audit <input type="text" value="4"/> ▼	<input type="checkbox"/> Interface Sessions Audit <input type="text" value="4"/> ▼	<input type="checkbox"/> IP App Traffic Audit <input type="text" value="4"/> ▼
<input type="checkbox"/> IP Sessions Audit <input type="text" value="4"/> ▼	<input type="checkbox"/> Channel Traffic Audit <input type="text" value="4"/> ▼	<input type="checkbox"/> Interface Traffic Audit <input type="text" value="4"/> ▼
<input type="checkbox"/> IP Online Duration Audit Log <input type="text" value="4"/> ▼	<input type="checkbox"/> Click to count cache resources <input type="text" value="4"/> ▼	

1.3.1.1.77 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.

Note: The local log function refers to saving flow logs or NAT logs on the hard disk of the device.

Enable Local Log:

1.3.1.1.78 System logs

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

Syslog Config
Syslog Config helps after-sales and R&D personnel to locate problems.

Syslog Config Switch

OK Export Log

Syslog (show log)

Update

```
*Mar 13 17:31:26: %IPSEC-4-ISAKMP_RETRANSMIT_FAILED: Local:192.168.23.197 Peer:192.168.3.1, initiator send out aggressive mode first packet, wait second packet failed, please check the configure or the network.
*Mar 13 17:30:36: %IPSEC-4-ISAKMP_RETRANSMIT_FAILED: Local:192.168.23.197 Peer:192.168.3.1, initiator send out aggressive mode first packet, wait second packet failed, please check the configure or the network.
*Mar 13 17:29:46: %IPSEC-4-ISAKMP_RETRANSMIT_FAILED: Local:192.168.23.197 Peer:192.168.3.1, initiator send out aggressive mode first packet, wait second packet failed, please check the configure or the network.
*Mar 13 17:28:56: %IPSEC-4-ISAKMP_RETRANSMIT_FAILED: Local:192.168.23.197 Peer:192.168.3.1, initiator send out aggressive mode first packet, wait second packet failed, please check the configure or the network.
```

Syslog Server

Server Log
Local Log
System Log
Syslog Server

Syslog Server IP: * Example: 192.168.23.14

Port: * (Range: 1-65535. Default: 514. Ensure that ports smaller than 1024 are not occupied by other UDP)

Send via Mgmt

Interface:

Save Clear

1.1.15.10 Log Policy

Log Policy
+ Add Policy X Delete Selected
Search by Search

	Policy Name	User/IP	Log Type:	Priority	Action
<input type="checkbox"/>	ELOG	192.168.2.1-192.168.2.250	Elog		Edit Delete

Show No.: Total Count:1

⏪ First
⏩ Pre 1
Next
⏪ Last
 GO

1.1.15.11 Report

Operation Log

Hard Disk Usage Log

CPU Usage Log

Memory Usage Log

Flow Log

1.3.1.1.79 Operation Log

Operation Log

Hard Disk Usage Log

CPU Usage Log

Memory Usage Log

Flow Log

Select Operation Log:
Export Report

Time	Operator IP Address	Description
2020-9-14 20:38-04	192.168.1.2	admin(configure), On the scheduled task page, enable/disable a scheduled task log
2020-9-14 20:38-03	192.168.1.2	admin(configure), On the scheduled task page, enable/disable a scheduled task log
2020-9-14 20:38-02	192.168.1.2	admin(configure), On the scheduled task page, enable/disable a scheduled task log
2020-9-14 20:37-38	192.168.1.2	admin(configure), On the scheduled task page, enable/disable a scheduled task
2020-9-14 20:36-30	192.168.1.2	admin(configure), On the scheduled task page, enable/disable a scheduled task
2020-9-14 20:36-23	192.168.1.2	admin(configure), On the scheduled task page, enable/disable a scheduled task
2020-9-14 18-43-43	192.168.1.2	admin(configure), admin Log In
2020-9-14 18-36-28	192.168.1.2	admin(configure), admin Log In
2020-9-14 18-22-06	192.168.1.2	admin(configure), On the Config Wizard page, save settings.
2020-9-14 18-21-10	192.168.1.2	admin(configure), admin Log In

This function displays device operations.

1.3.1.1.80 Hard Disk Usage Log

Operation Log

Hard Disk Usage Log

CPU Usage Log

Memory Usage Log

Flow Log

Tip: An abnormal display or data may be generated on this page if no hard disk is inserted.

Select Hard Disk Usage Log:
Export Report

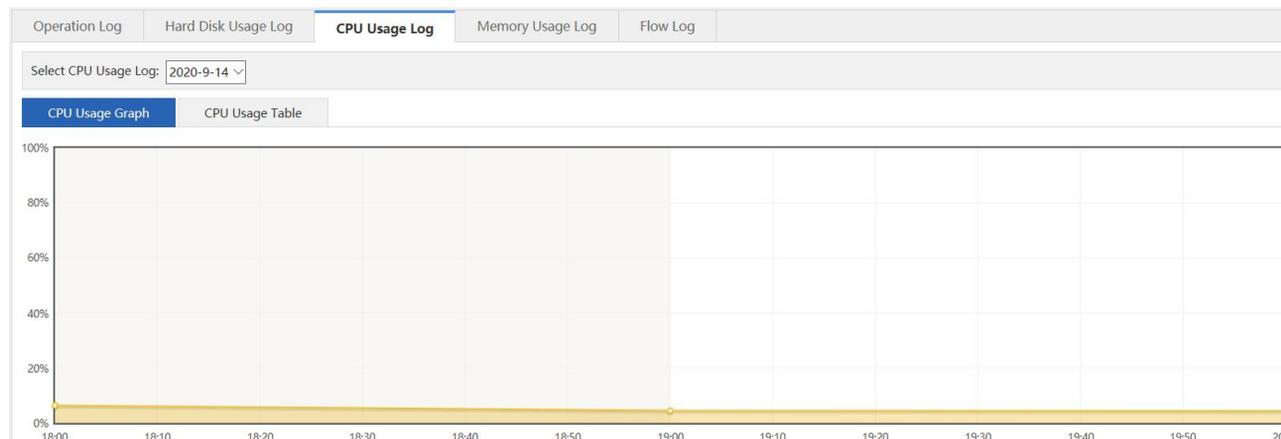
Time	Available Hard Disk(MB)	Used Hard Disk(MB)	Available Flash Memory(KB)	Used Flash Memory(KB)
2020-09-14 20:38:53	890666	48107	941924	57364
2020-09-14 19:38:52	890667	48106	941980	57308
2020-09-14 18:38:52	890668	48105	942036	57252
2020-09-14 18:29:55	890669	48104	942064	57224
2020-09-14 18:10:09	890669	48104	942112	57176

Show No.: Total Count: 5

⏪ First
⏩ Pre 1
Next
⏪ Last
 GO

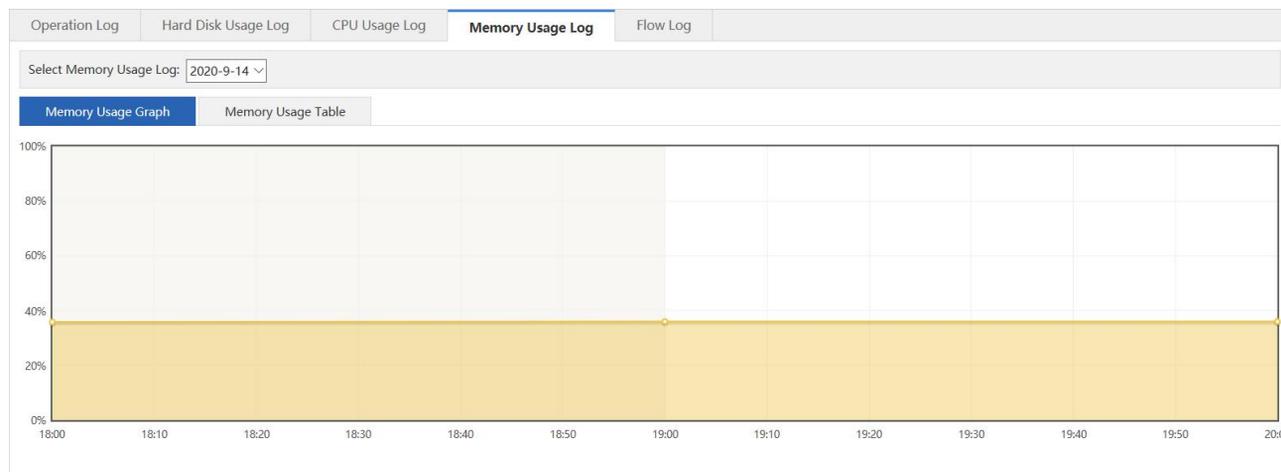
This function displays the usage of the device hardware.

1.3.1.181 CPU Usage Log



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

1.3.1.182 Memory Usage Log



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

1.3.1.1.83 Flow Log

Operation Log	Hard Disk Usage Log	CPU Usage Log	Memory Usage Log	Flow Log	
---------------	---------------------	---------------	------------------	-----------------	--

Flow Log: [Export Report](#) Q Advanced Search

Time	Protocol	User	Src IP	Dest IP	Src Port	Dest Port	Tx Flow (Byte)	Rx Flow (Byte)
No Record Found								

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

This function displays the flow usage on a day.

Advanced Search: You can select required flow records.

Advanced Search ✕

Select
 Protocol:

Start Time:

Select User: Select User Enter Source IP

[\[Select User\]](#)

Dest IP:

Src Port: (0-65535)

Dest Port: (0-65535)



 <https://www.fs.com>



The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.