Operation Manual

RG-SAM+ ENTERPRISE_4.00_Build20150829

Copyright Statement

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Thank you for using our products. This manual matches RG-SAM+ ENTERPRISE_4.00_Build20150829.

Audience

This manual is intended for:

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

Obtaining Technical Assistance

- Ruijie Networks website: http://www.ruijienetworks.com/
- Ruijie service portal: http://case.ruijienetworks.com

Preface

Thank you for choosing the **RG-SAM+ Security Accounting Management System**. It is a great honor to provide you with Ruijie Networks products. We have sufficient user manuals that familiarize you with operations quickly. We also attach the e-document to the installation CD.

We have made great efforts to include comprehensive content in the manual and make it simple and easy to understand, helping you obtain all aspects including installation environment, basic operation, software usage and precautions. To help you use the RG-SAM+ system properly, please read carefully all the materials in the CD before you start to install and use it.

Ruijie Networks will update the RG-SAM+ software to improve performance and availability at any time. For this circumstance, Ruijie Networks will update related materials such as manuals and CDs in the first time. However, inconsistency in some details may still exist. We hope you to understand.

Ruijie Networks has made reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions. If necessary, Ruijie Networks will explain issues not covered by the document, and correct errors as soon as possible. The customer assumes full responsibility when misunderstanding it. Ruijie Networks welcomes customer comments and questions by dialing the hotline 4008111000. In no event will Ruijie Networks be liable to any damage caused by improper operation or for any performance problem caused by substandard hardware.

Chapter 1 System Features

Unified Authentication of Multiple Services

The RG-SAM+ security accounting management system ("RG-SAM+ system" for short) complies with the standard Remote Authentication Dial-In User Service (RADIUS) protocol and Ruijie extended RADIUS protocol. It can be configured to implement authentication in multiple forms, including the 802.1X and ePortal access in wired and wireless modes, as well as the virtual private network (VPN) access in wired mode. Multiple services can be set for users who use the Internet access service. In other words, users can gain access to the RG-SAM+ system by using different services, and the RG-SAM+ system conducts unified authentication and accounting.

Low Cost and High Performance

The RG-SAM+ system adopts the "PC server hardware + Windows software" platform, and SQL Server database, thereby providing a cost-effective and highly available solution for users.

The RG-SAM+ system uses the distributed modular architecture and TCP/IP-compliant communication mechanism, and supports smooth expansion, load balancing, disk array, and database backup. It caters to the demand for authentication, authorization, and accounting of large-, intermediate-, and small-sized networks.

Flexible and Open Billing Policies

The RG-SAM+ system uses an abstract billing model and customized billing policy to provide flexible and powerful billing policy configuration, thereby meeting different billing requirements of users. The billing policies of the RG-SAM+ system include the common billing policies and customized billing policies. With a common billing policy, users are charged regularly based on the Internet access duration and traffic (port traffic). The RG-SAM+ system, in combination with the gateway, is capable of conducting billing based on the domestic uplink traffic, domestic downlink traffic, international uplink traffic, and international downlink traffic that are classified by destination IP address. Customized billing policies provided by the RG-SAM+ system support segmented billing and area-based billing. Customized billing rules and customized billing policies are configured to provide flexible and diversified billing options for users.

Ease of Use

The RG-SAM+ system provides the Web-based management graphic user interface (GUI) and requires no software or plug-ins on the client, providing convenience for users. Users need to install only a browser on the client to perform data setting and information query, thereby reducing maintenance costs for customers. Users can manage the RG-SAM+ system at any time and any place.

The RG-SAM+ system also provides the self-service system for users, who can log in to a specified Web page and then apply for registration, query the review result and their user information, view online records and account records, and change passwords.

The RG-SAM+ system is designed with the advanced GUI for administrators to know the system and conduct system management conveniently. The GUI design simplifies user operations and uses clear tips, help, and templates to greatly enhance the product availability, thereby reducing training costs for RG-SAM+ system administrators and operators.

With the database maintenance function embedded in the RG-SAM+ system, users can complete database maintenance in one-click mode and easily configure remote backup over the File Transfer Protocol (FTP).

Flexible Security Control

The RG-SAM+ system encrypts interactive packets and passwords in the packets to prevent packet forgery and password theft. The RG-SAM+ system makes detailed records and prompts for unidentified authentication requests. Administrators can get details about online users by checking the time, user IP addresses, user MAC addresses, MAC addresses of access points (APs), and service set identifiers (SSIDs). When necessary, administrators can give warnings, impose punishment and perform control over users in violation of Internet rules by sending real-time short messages (SMs), adding a user to the blacklist, or forcing users to go offline.

The RG-SAM+ system also introduces system management privileges. System administrators can be granted privileges to effectively and accurately control the use of the system. The self-service system introduces self-service privileges. Users can be granted different self-service privileges to accurately control their access to the self-service system. IP addresses and other information of anonymous users are recorded for check.

The self-service system of the RG-SAM+ system is protected using the verification code to prevent security issues caused by openness of the self-service system.

High Stability, High Speed, and High Efficiency

The database connection pool technology helps the RG-SAM+ system implement high-speed buffering of data connections, increase the concurrent access traffic, and enhance the system capacity for bearing large-scale applications, ensuring stable and rapid performance of the system. Common parameters of the RG-SAM+ system are buffered in the memory, and the authentication and billing services are processed using the multi-thread technology, substantially improving the fast response to the authentication and billing services.

High Availability

An RG-AC cluster can be configured for the RG-SAM+ system to implement hot backup of services and data. When one server malfunctions, the other server takes over the services and data without manual intervention, ensuring that the system continuously provides services.

The automatic database maintenance function enables the RG-SAM+ system to automatically conduct regular maintenance on the database, thereby ensuring stable performance. Local backup and local + remote backup are available for disaster recovery of the database.

Chapter 2 Introduction to Ruijie Networks

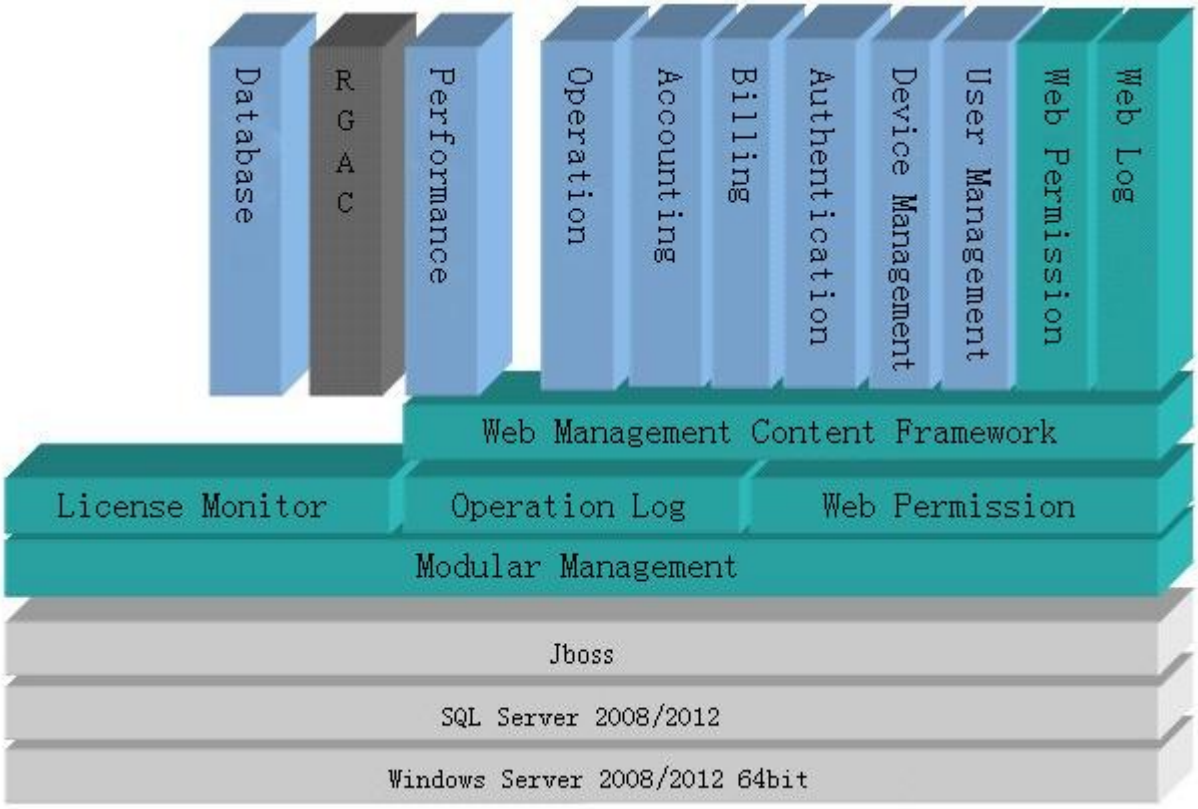
Ruijie Networks, founded in January 2000, follows the core business concept of grasping application trends keenly, meeting customer needs swiftly for 15 years, and has achieved extraordinary and leapfrog development in the fierce market environment. Nowadays, Ruijie Networks has become a professional network vendor with complete series of network product lines and application-based end-to-end network solutions, having thousands of high-quality employees and branches throughout 32 provinces, cities, and autonomous regions in China. For years, Ruijie Networks, by virtue of professional and convenient services and distinct network authentication training, provides strong support for customers to maximize their network investment value. Ruijie Networks solutions have been widely applied in information-based construction fields in China, such as education, finance, medicine, government, telecommunication, military, and enterprise.

Star-Net Ruijie Technology Park

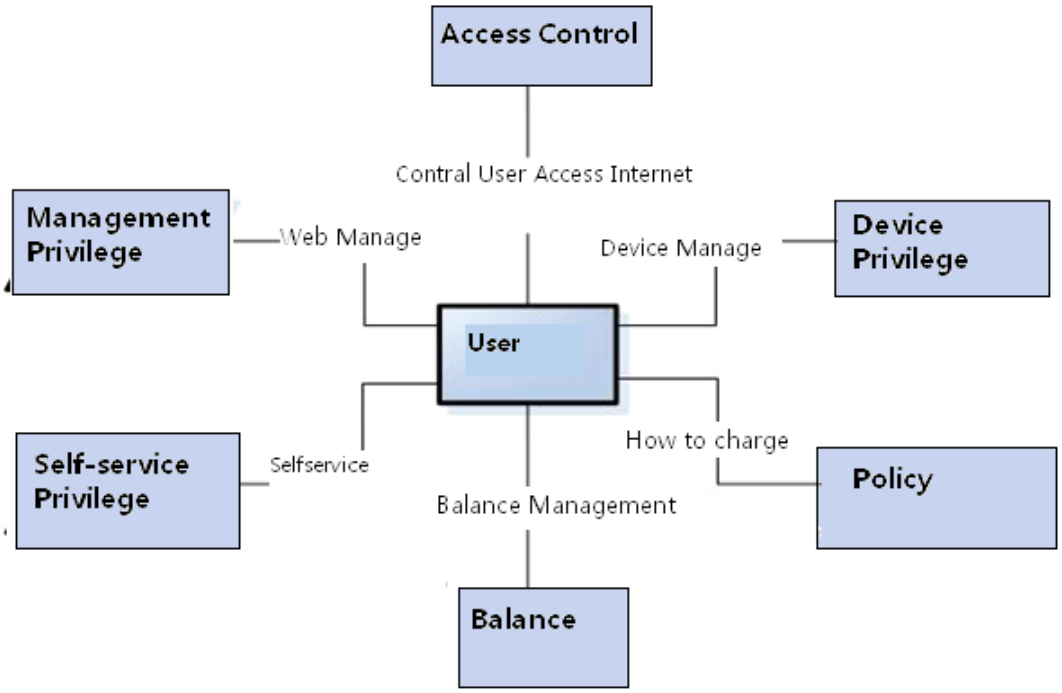
Chapter 3 Overview of the RG-SAM+ System

This chapter uses some pictures to show the architecture, user prototype, and typical deployment modes of the RG-SAM+ system as well as the RG-AC deployment so that you can deeply understand the deployment schemes of the RG-SAM+ system.

Architecture of the RG-SAM+ System



User Prototype of the RG-SAM+ System



Note:

"User" shown in the preceding figure is the user prototype of the RG-SAM+ system, and may refer to the following users in the RG-SAM+ system:

System administrator: associated with management privileges

Device administrator: associated with device privileges

Customized administrator: associated with all associable service entities

User: associated with accounts, billing policies, self-service privileges

Pre-cancelled user: associated with the same service entities as users but unable to use any associated service normally

Users are the basis of services. Users can independently exist without being associated with any services, but such existence is meaningless.

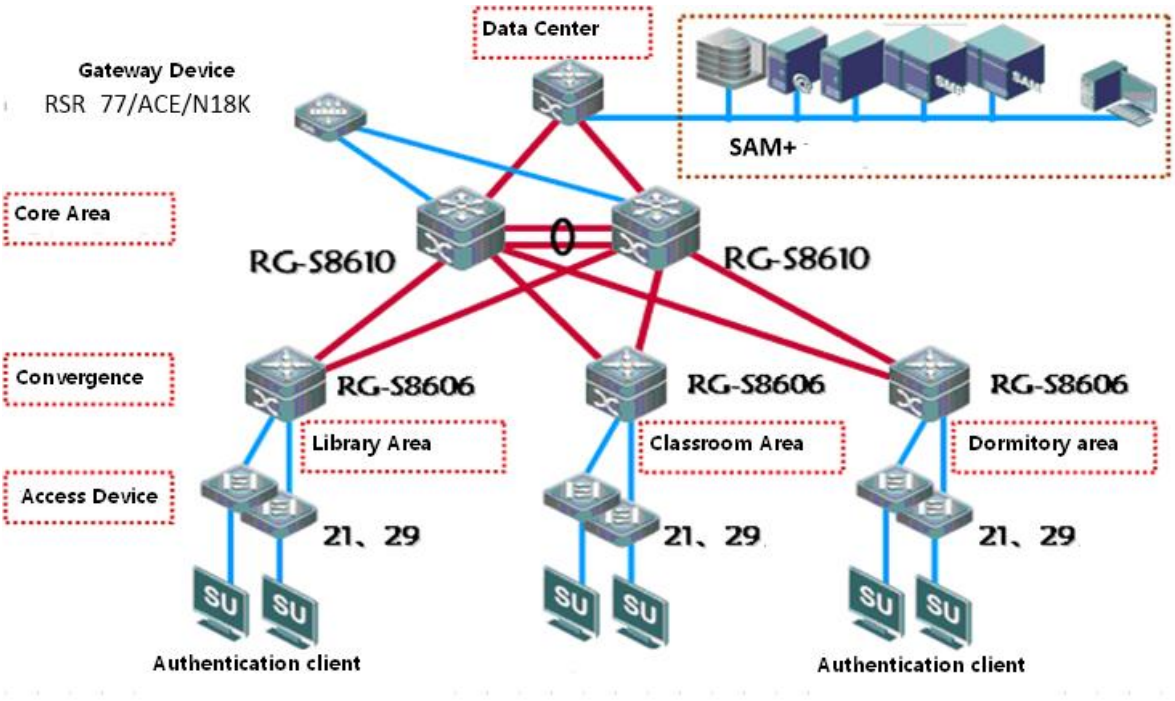
Users need to be associated with accounts (available balance for billing) and billing policies (how to conduct billing) so that billing can be conducted based on different situations.

For details about the association operations, see relevant sections.

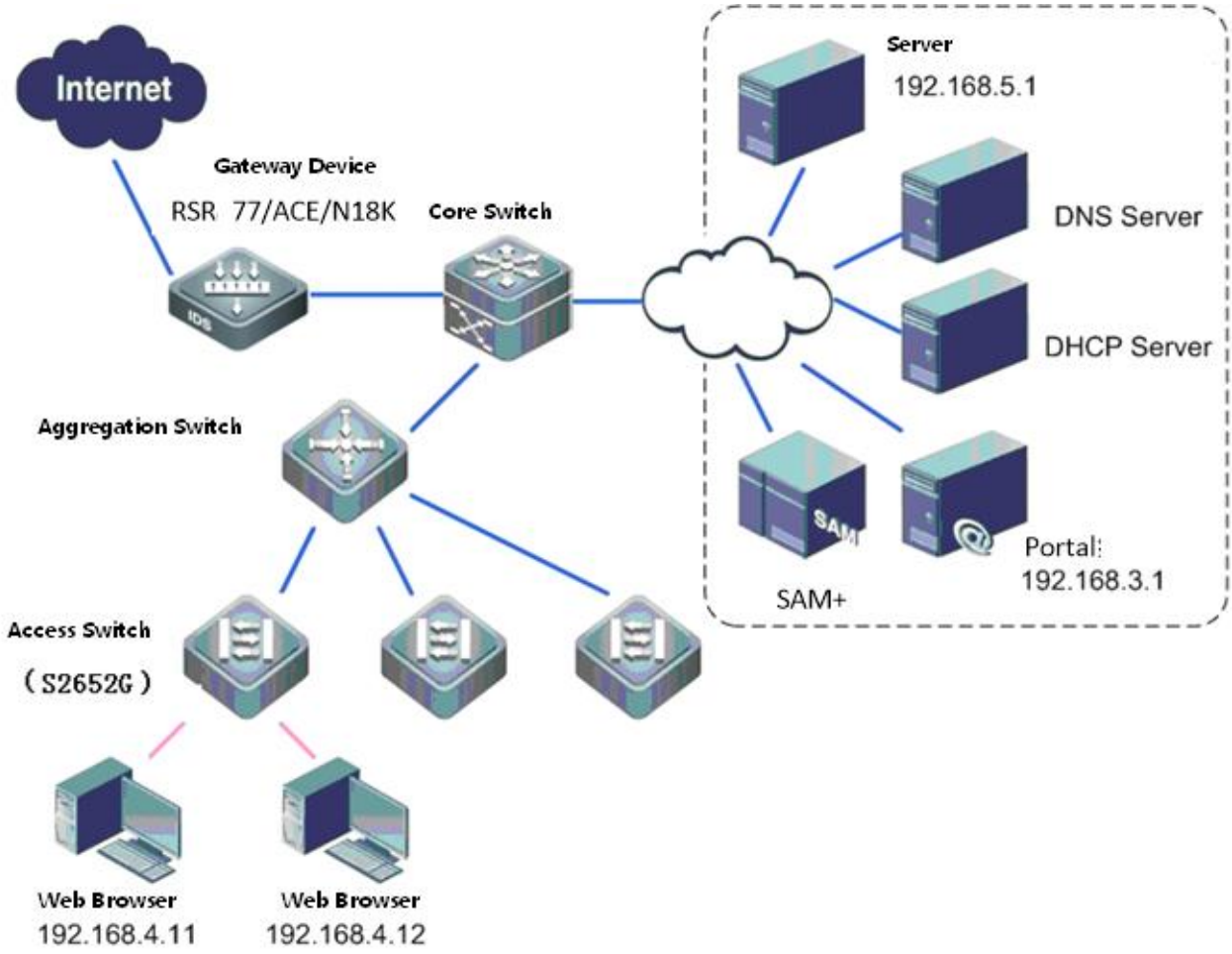
Typical Deployment Diagrams of the RG-SAM+ System

Currently, the RG-SAM+ system supports several typical deployment modes, including the standard 802.1X access mode, Portal access mode, VPN access mode, and wireless network access mode. The following figures show the typical deployment modes.

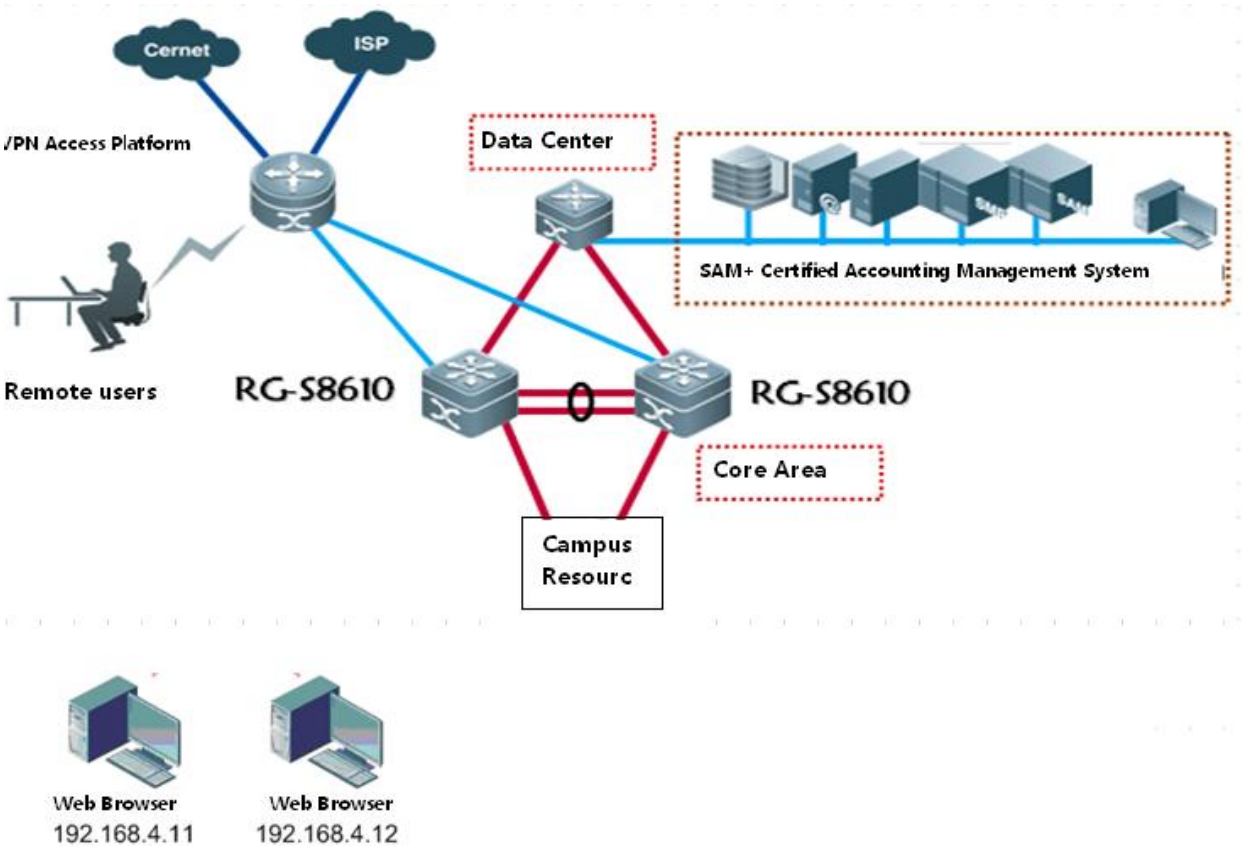
Deployment in Standard 802.1X Access Mode



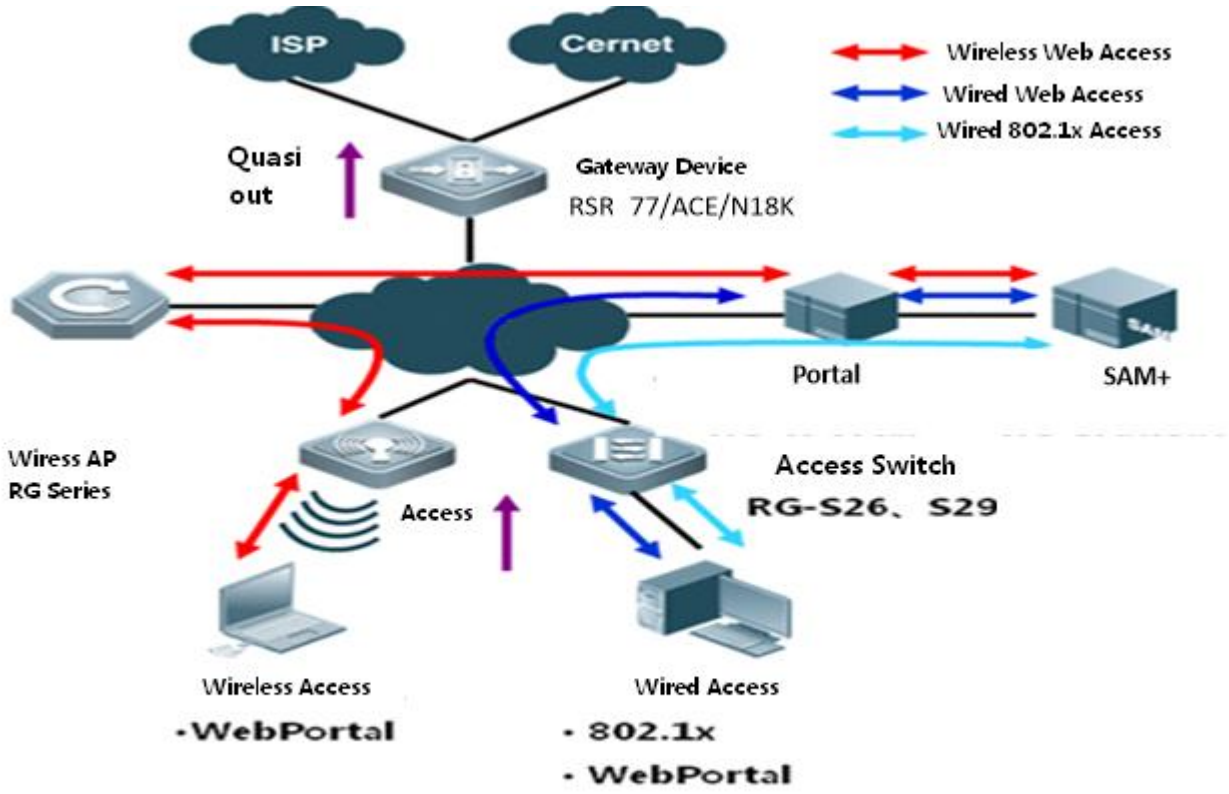
Deployment in Portal Access Mode



Deployment in VPN Access Mode

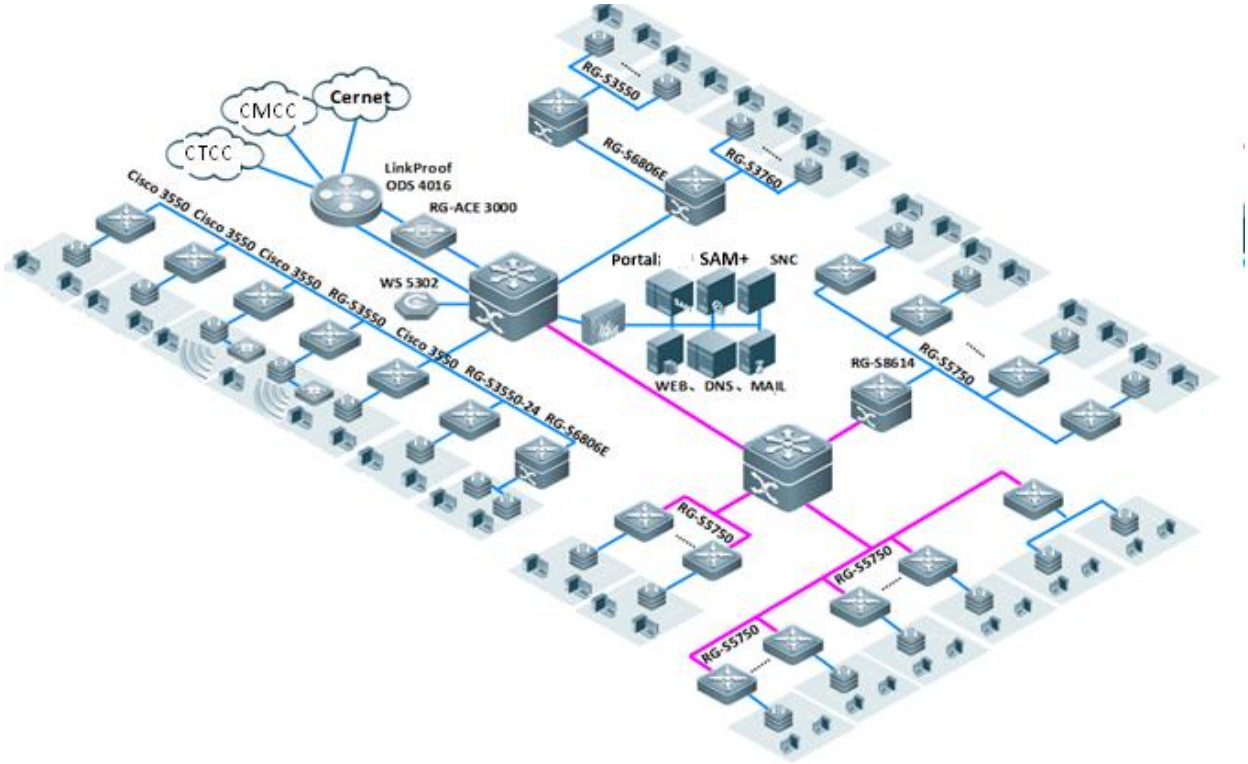


Deployment in Wireless Network Access Mode



Deployment in the Access Mode Using Five Integrations

Five integrations refer to the admission and exit integration, 802.1X authentication and Web authentication integration, wired device and wireless device integration, integration of the campus network and the network outside the campus, IPv4 address and IPv6 address integration.



RG-AC Deployment

Note

The RG-SAM+ system supports RG-ACs. The detailed deployment and operation instructions are attached to the delivered CD for your reference.

A cluster is a group of computers that provides users with a group of network resources as a whole. These computers composing a cluster are called cluster nodes. A high availability (HA) cluster is a server cluster technology with the aim of reducing service interruption. It minimizes the impact on services caused by software, hardware, or man-made faults by enabling service programs to continuously provide services.

An HA cluster is deployed to make the overall service of the cluster available as much as possible, thereby reducing losses caused by computer hardware and software exceptions. If a node of a cluster fails, the standby node takes over the services and data of the failed node in a short time. Therefore, a cluster never stops working for users. An HA cluster consisting of two nodes is called a two-node hot backup cluster, in which the two servers are backed up for each other. When one server malfunctions, the other server takes over the services automatically, ensuring that the system provides services continuously without manual intervention.

RG-AC 1.2 is a two-node hot backup cluster, which consists of two RG-SAM+ servers, with one server providing services (called the active server) and the other server working as backup (called the standby server). When the active

server malfunctions, services are transferred to the standby server and the standby server works in active mode to provide services. The faulty server is disconnected from the cluster. When the faulty server recovers and is added to the cluster again, it works in standby mode.

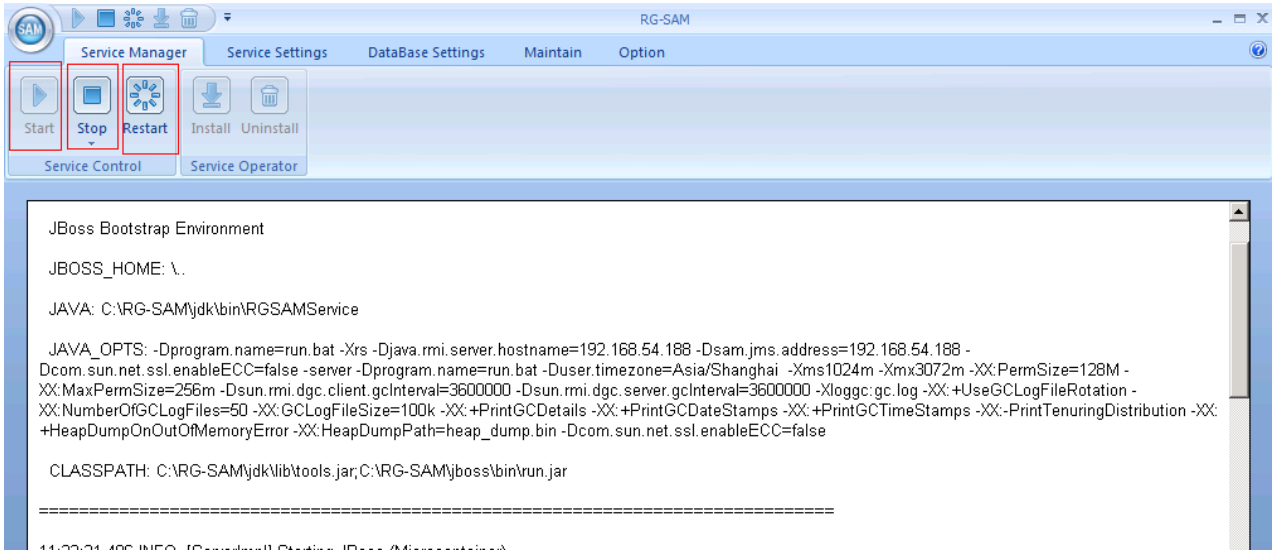
For the RG-AC deployment method, see the *RG-SAM+ Application Cluster RG-AC Configuration Guide* attached to the product CD.

Chapter 4 RG-SAM+ System Installation

The installation of the RG-SAM+ system requires the hardware device — one RG-SAM+ server at least. For details, see the *RG-SAM+ Security Accounting Management System Installation Manual* attached to the CD. You are recommended to optimize the security, maintenance, and performance of the server prior to installing the RG-SAM+ system, and have a deep understanding of the SQL Server 2008/SQL Server 2012 database, so as to ensure more stable and efficient operation of the RG-SAM+ system.

Chapter 5 RG-SAM+ System Startup

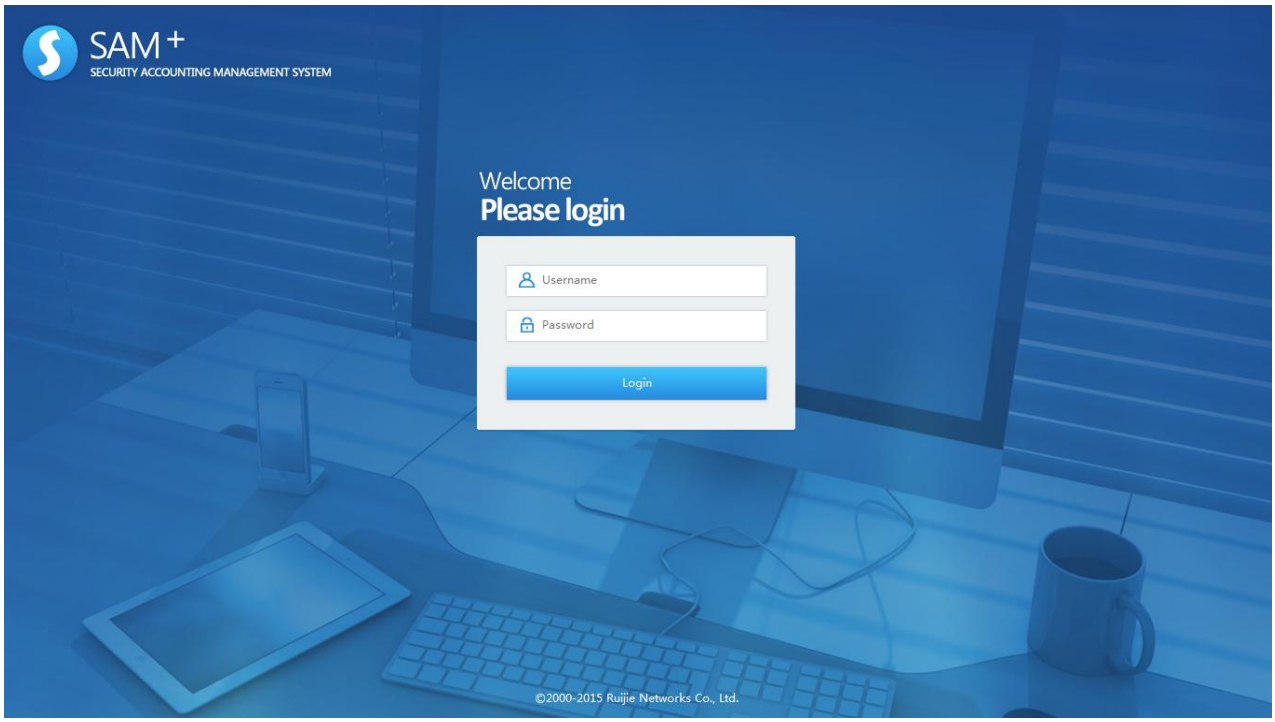
After installing the RG-SAM+ system, choose **Start**>**Program**>**Ruijie Networks**>**RG-SAM+ Security Accounting Management System** to start the service manager.



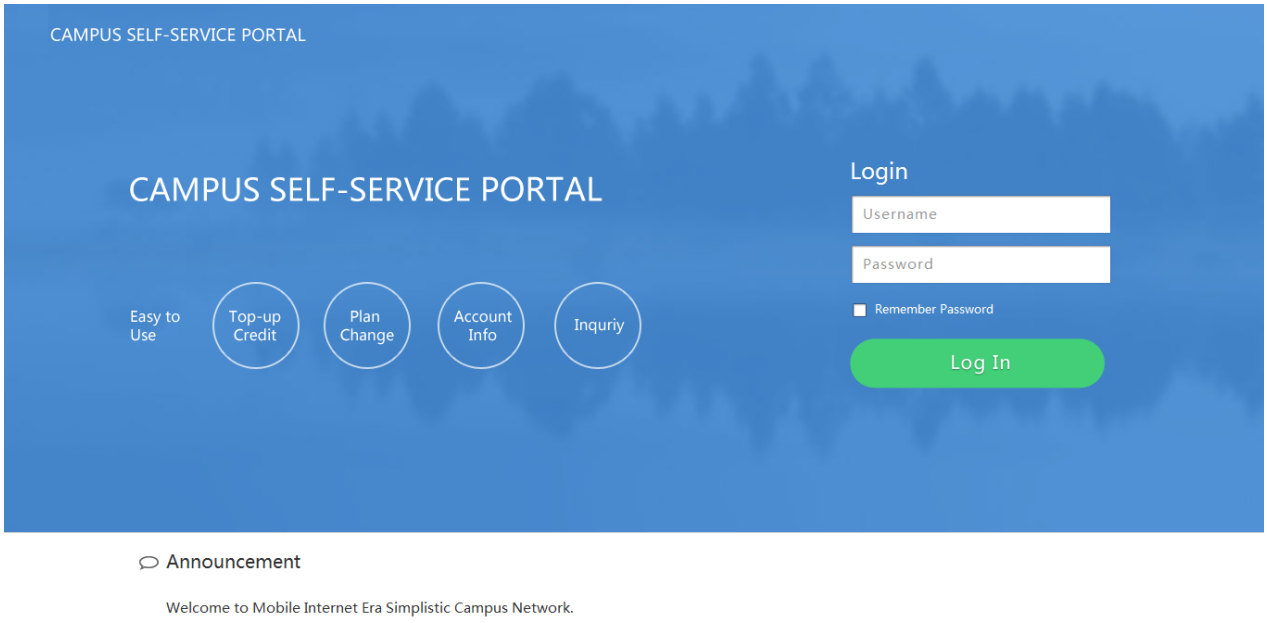
Click the start button or choose **Service Manager**>**Start** from the main menu.

After starting the RG-SAM+ system, open the Internet Explorer (IE) on Windows and enter **http://[***Web server address***]:8080/sam/** in the address bar to access the login page of the RG-SAM+ system, as shown in the following figure.

The address for accessing the RG-SAM+ system is **http://[***Web server address***]:8080/sam/**, for example, **http://192.168.1.1:8080/sam/**. You can use a safer transmission mode by entering **https://[***Web server address***]:8443/sam/**, for example, **https://192.168.1.1:8443/sam/**.



The address for accessing the RG-SAM+ self-service system is **http://[***Web server address***]:8080/selfservice/**, for example, **http://192.168.1.1:8080/selfservice/.** The login page of the self-service system is shown in the following figure.



It is recommended that you use IE and complete the following operations: In the IE, choose **Tools**>**Internet Options** from the main menu; in the **Internet Options** dialog box, click the **General** tab, and click **Settings** in **Temporary**

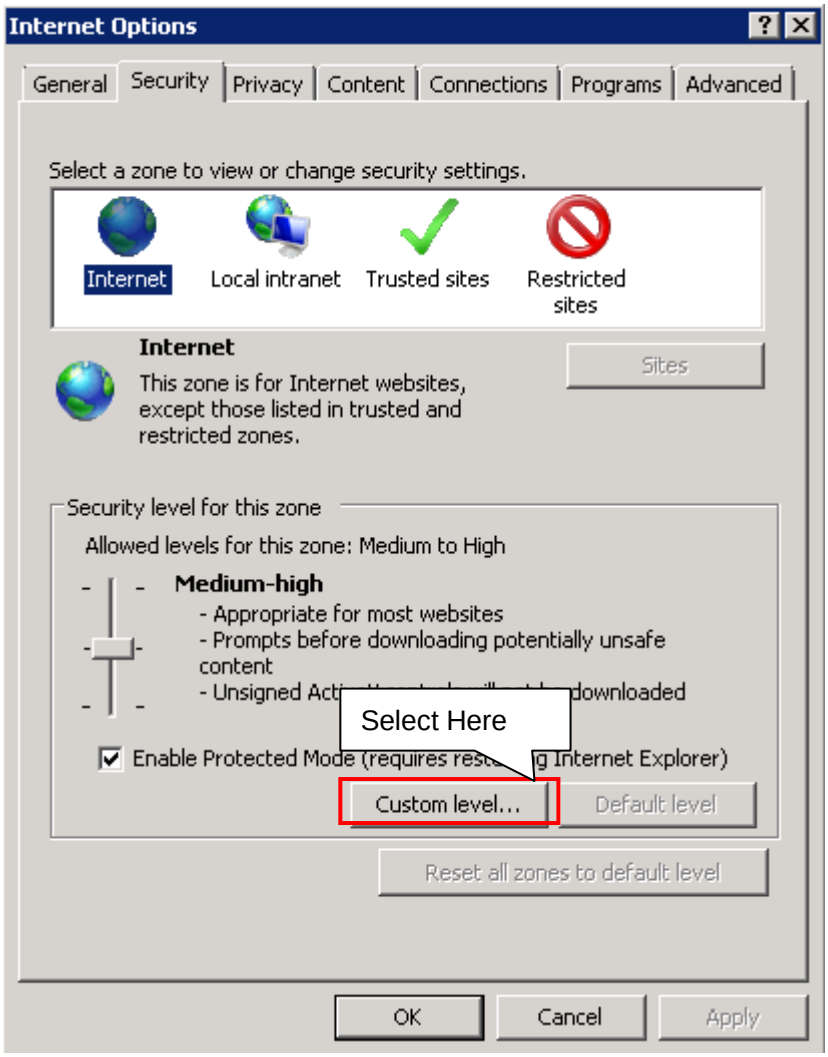
Internet files. In the **Settings** dialog box, click **Every visit to the page**. Click **OK**, and then click **OK** in the **Internet Options** dialog box.

In addition, choose **View**>**Font Size**>**Medium** from the main menu to set the best font for browsing the RG-SAM+ system.

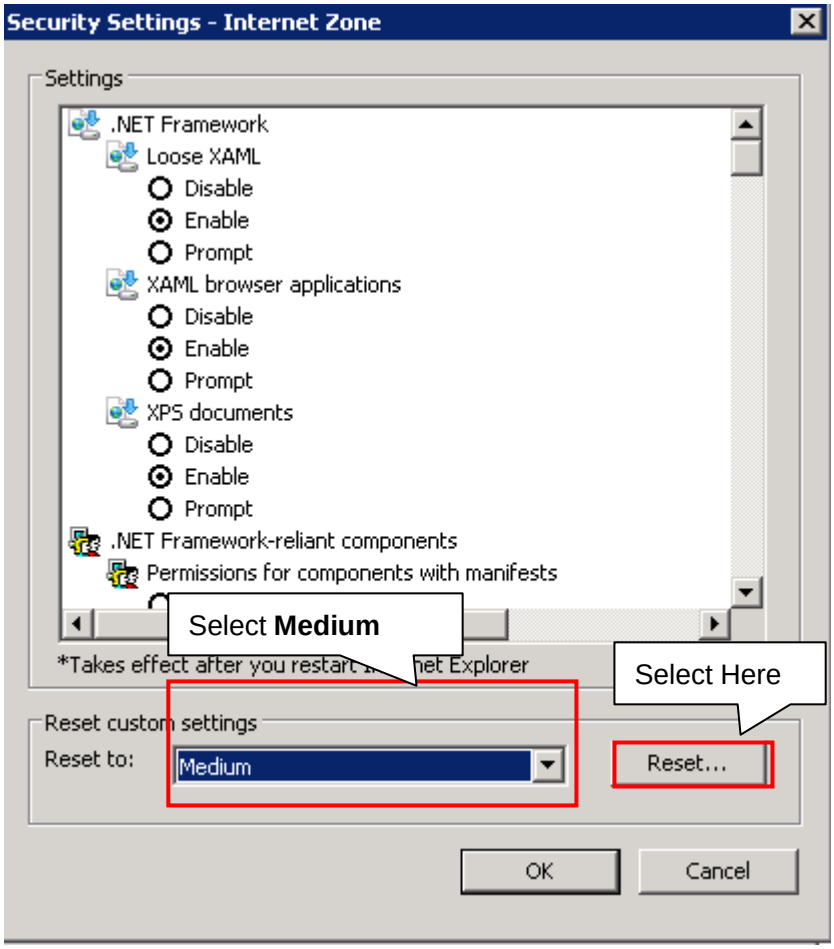
It is recommended that the resolution be set to 1440x900.

The RG-SAM+ system is designed with many script languages for page control. Therefore, complete the following settings to gain better experience:

Step 1: Choose **Tools**>**Internet Options** from the main menu. In the **Internet Options** dialog box, click the **Security** tab and then click **Custom level**.

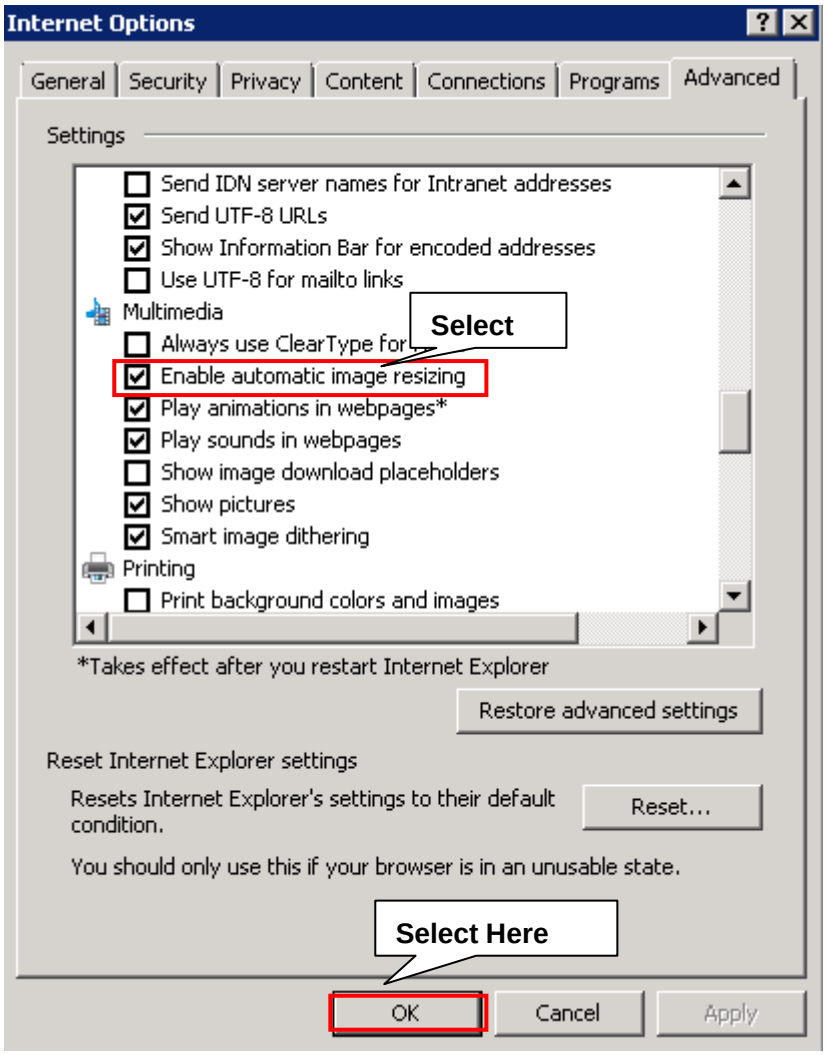


Step 2: In the **Security Settings – Internet Zone** dialog box, select **Medium** from the **Reset to** drop-down list and click **Reset**.



Step 3: Click **OK** and then click **OK** again till the **Internet Options** dialog box disappears.

Some functions of the RG-SAM+ system require long waiting time and animated images are displayed to indicate that an operation is in progress. Complete the following settings to ensure that animated images can be played normally. In the IE, choose **Tools**>**Internet Options** from the main menu. In the **Internet Options** dialog box, click the **Advanced** tab, select **Play animations in webpages***, and then click **OK**, as shown in the following figure.

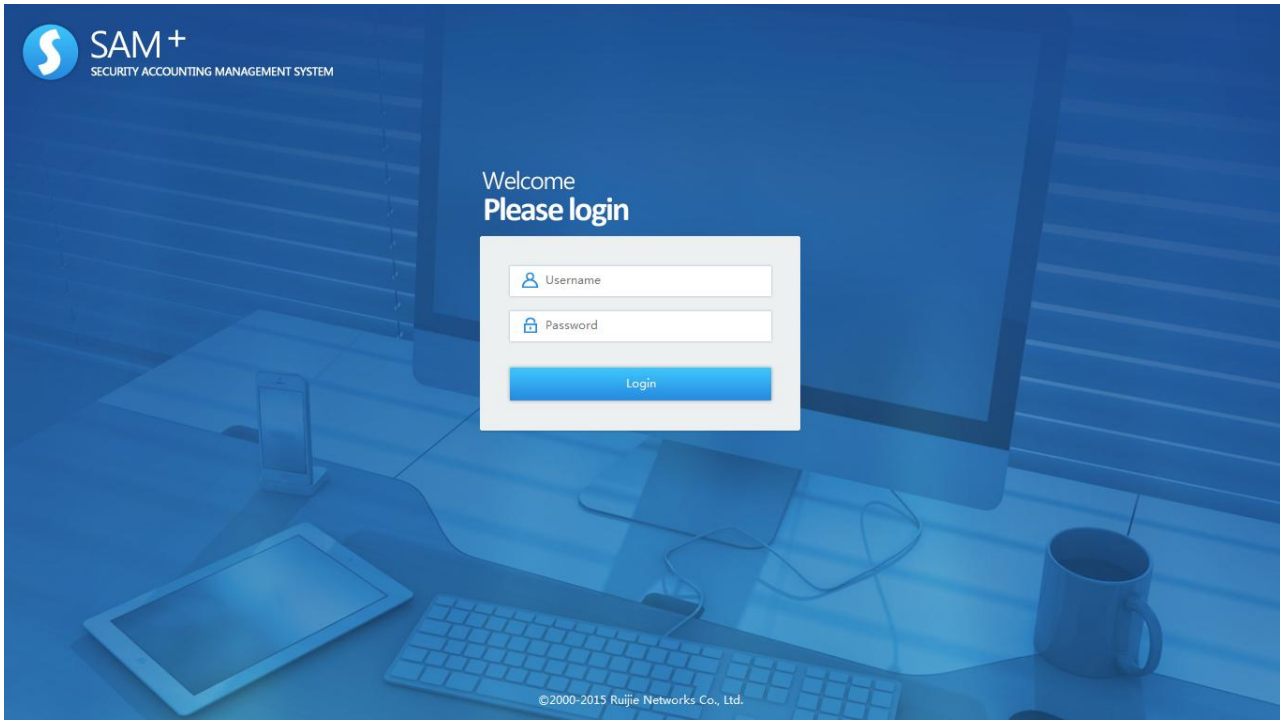

Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Send IDN server names for Intranet addresses
Send UTF-8 URLs
Show Information Bar for encoded addresses
Use UTF-8 for mailto links
Multimedia
Always use ClearType for
Enable automatic image resizing
Play animations in webpages*
Play sounds in webpages
Show image download placeholders
Show pictures
Smart image dithering
Printing
Print background colors and images
Select
*Takes effect after you restart Internet Explorer
Restore advanced settings
Reset Internet Explorer settings
Resets Internet Explorer's settings to their default condition.
Reset...
You should only use this if your browser is in an unusable state.
Select Here
OK
Cancel
Apply

Chapter 6 Introduction to the RG-SAM+ System

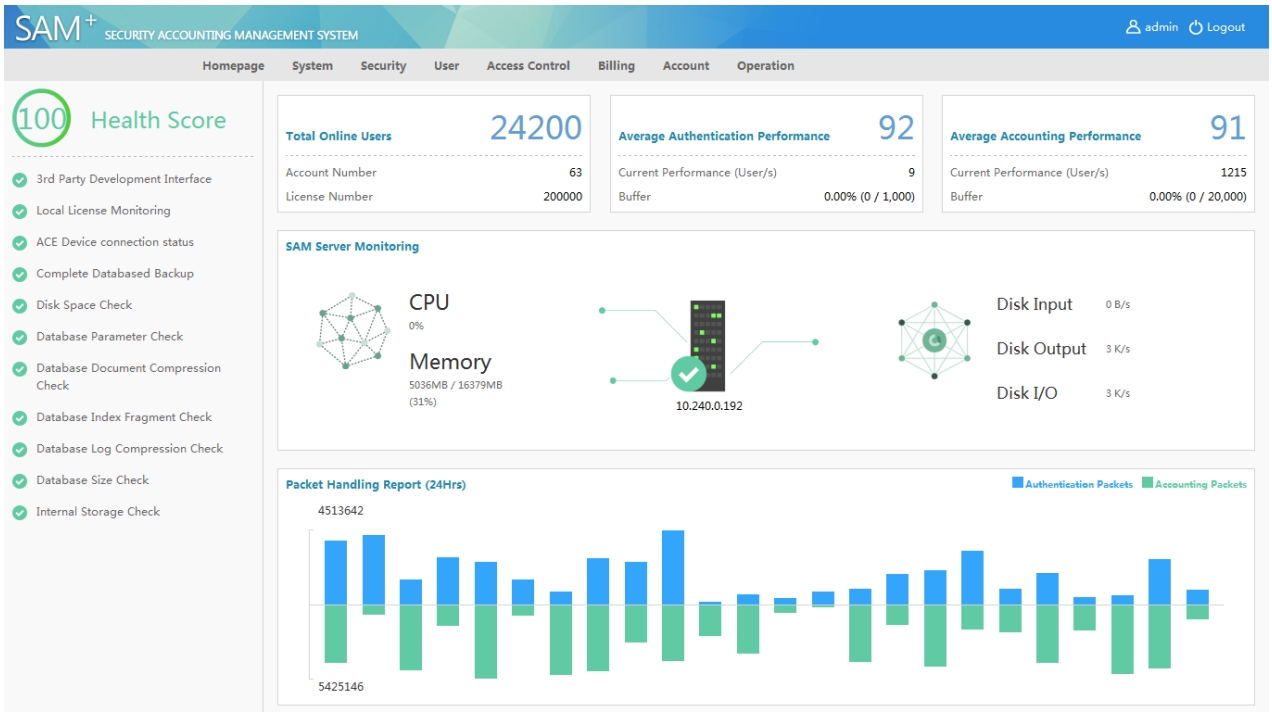
The RG-SAM+ system uses the soft and elegant phantom blue hue, which will not cause eyestrain after the long-time use of the RG-SAM+ system.

Login Page

The following figure shows the login page of the RG-SAM+ system.

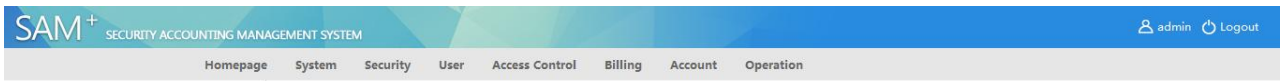


The default username and password of the super administrator are **admin** and **111** respectively. The homepage of the RG-SAM+ system is displayed after you enter the correct username and password and click **Login**.



As shown in the preceding figure, the homepage of the RG-SAM+ system includes three areas: top area, right area, and left area, which are separately described as follows.

Top Area



The top area includes the navigation menu, admin and logout icons, and logo of the RG-SAM+ system, as shown in the preceding figure.

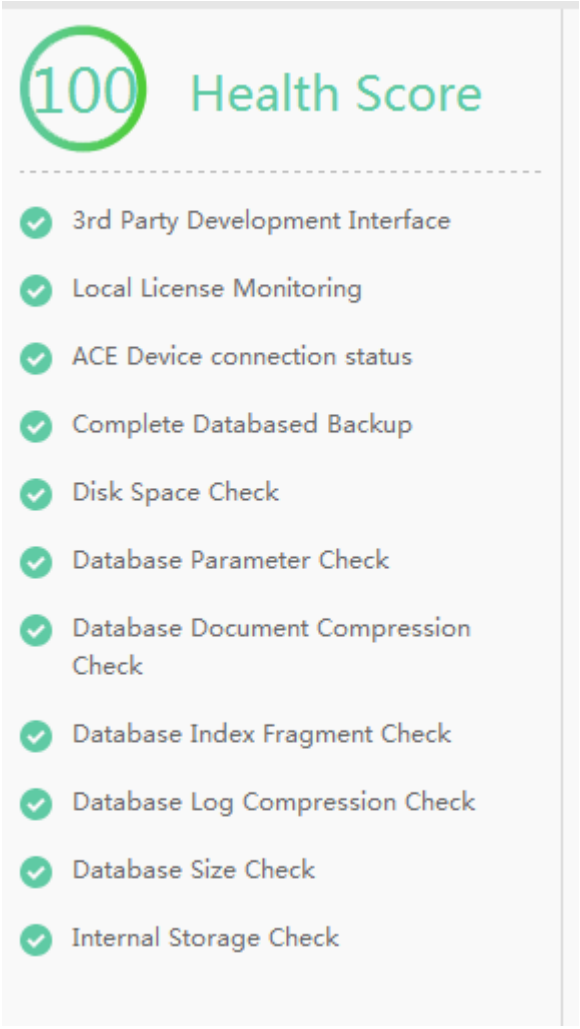
Homepage: You return to the home page after successful login if you click it.

Admin: If you click it, you access the administrator information and you can modify the personal information, especially change your password.

Logout: If you click it, you exit the RG-SAM+ system safely. This function is also provided in a drop-down menu to accommodate use habits of different users.

Left Area

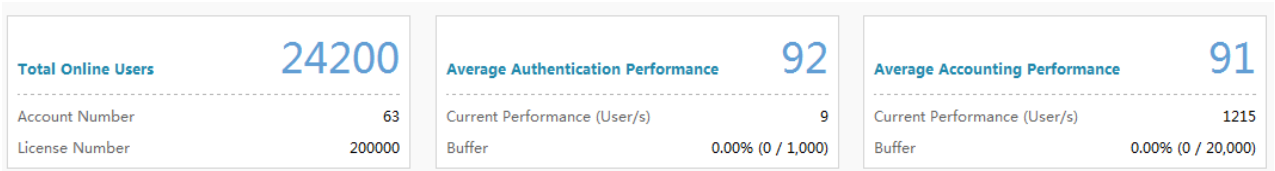
The following figure shows the left area of the RG-SAM+ system.



This area displays the health score of the RG-SAM+ system and displays the performance status in terms of complete database backup, database log backup, third-party development interface, and local license monitoring. Items in good operation status are marked in green and items in poor status are marked in red.

Right Area

The top part of this area displays the license authorization and performance data.



License Number: total number of users supported by the license bought by a customer, that is, maximum number of accounts that can be activated

Account Number: number of activated accounts in the system currently

Total Online Users: total number of online users

Average Authentication Performance: average authentication performance since the operation of the system

Current Performance: current authentication performance value

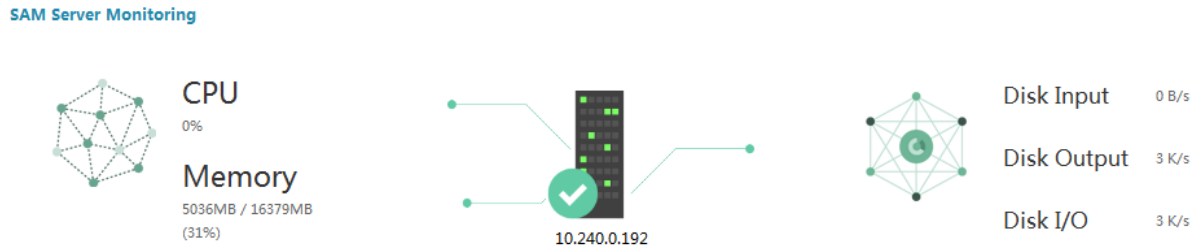
Buffer: authentication buffer status

Average Accounting Performance: average accounting performance since the operation of the system

Current Performance: current accounting performance value

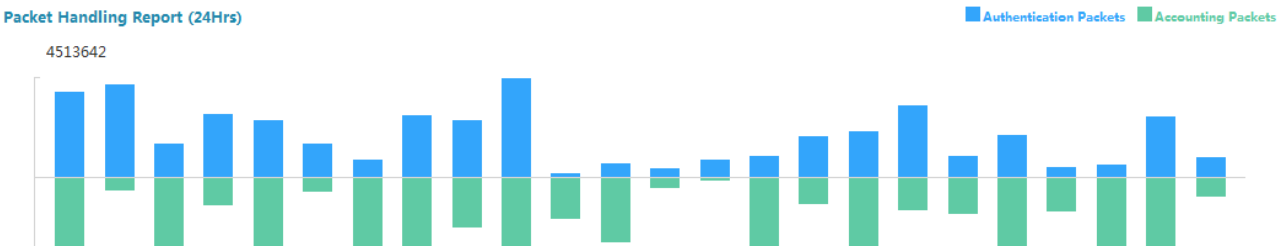
Buffer: accounting buffer status

The middle part of the right area displays the CPU, memory, and disk status of the RG-SAM+ server.



The RG-SAM+ server monitors and displays the CPU usage of the server, including the total memory, used memory, and utilization rate. It also displays the IP address, disk input, disk output, and disk input/output of the server with graphs.

The lower part of the right area displays the number of packets processed by the RG-SAM+ system per hour in last 24 hours.



The number of packets processed per hour in last 24 hours is displayed on a graph, on which you can view the packet processing status within 24 hours.

Global Configuration

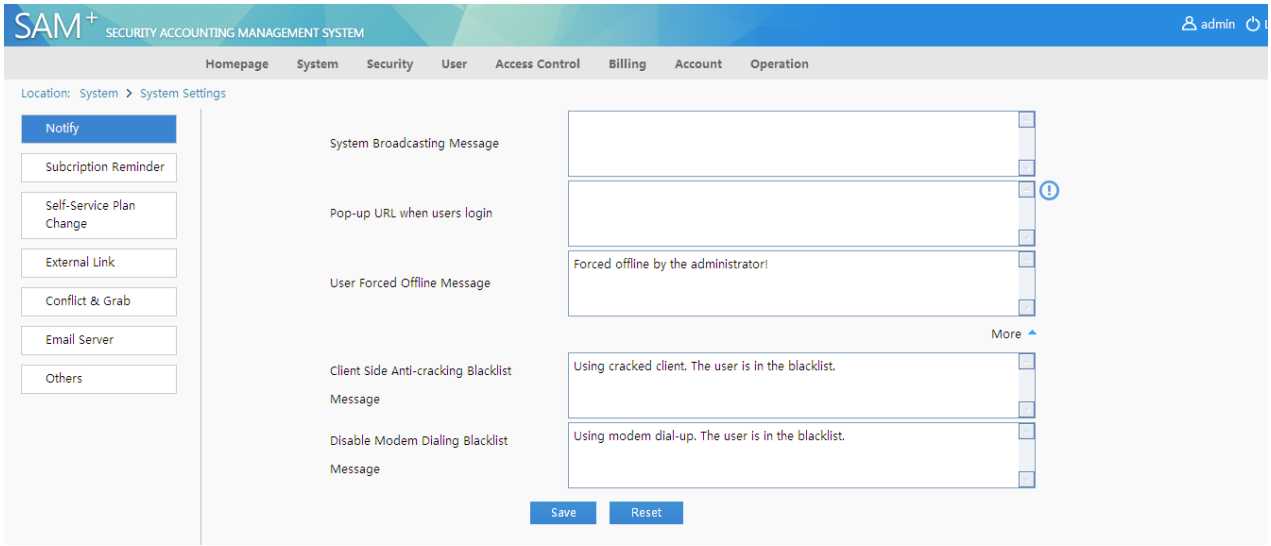
Before putting the RG-SAM+ system into formal operation, you must complete some global configuration for the RG-SAM+ system, including global parameter configuration, device adding, device group management, blacklist management, compatible component management, area settings, and management privileges. System management mainly refers to global parameter settings, and security management provides necessary control over privileges, which can be granted to administrators. Functions relevant to global configuration are mainly focused on system management and security management, which are described as follows:

System management is the settings of some parameters required for basic service operation. It consists of parameter settings and management of some global basic elements. System operation parameters are basis for the RG-SAM+ system, which uses some default parameter settings. The default parameter settings may not fully cater to your requirement. Therefore, before putting the RG-SAM+ system into formal operation, modify the parameters according to your need. Basic elements are some global system parameters, including IP addresses used throughout the network, devices and device groups to be managed. Such elements are mandatory for the formal operation of the RG-SAM+ system.

System Settings

Parameters in system settings include some parameters necessary for system operation. Default values are adopted for these parameters and you can change the values according to your requirements. For example, all online users can see system notifications and you can set the notification before formal operation of the RG-SAM+ system.

The **System Settings** menu provides various notifications, subscription reminder, conflict & grab, email server configuration. Each item is described in details as follows.



Notify: After configuring notifications, all online users can see the system broadcasting message when accessing the Internet by using Ruijie clients in dial-up mode. This message is called a broadcasting message or advertisement message, mainly used to make announcements to all Internet users.

Online Message:

Users can see the following types of messages after accessing the Internet by using Ruijie clients, and the messages can be set by administrators according to the situation. Note that only users who access the Internet by using Ruijie clients can view the messages.

System Broadcasting Message: You can edit a global broadcasting message, which can be seen by all users.

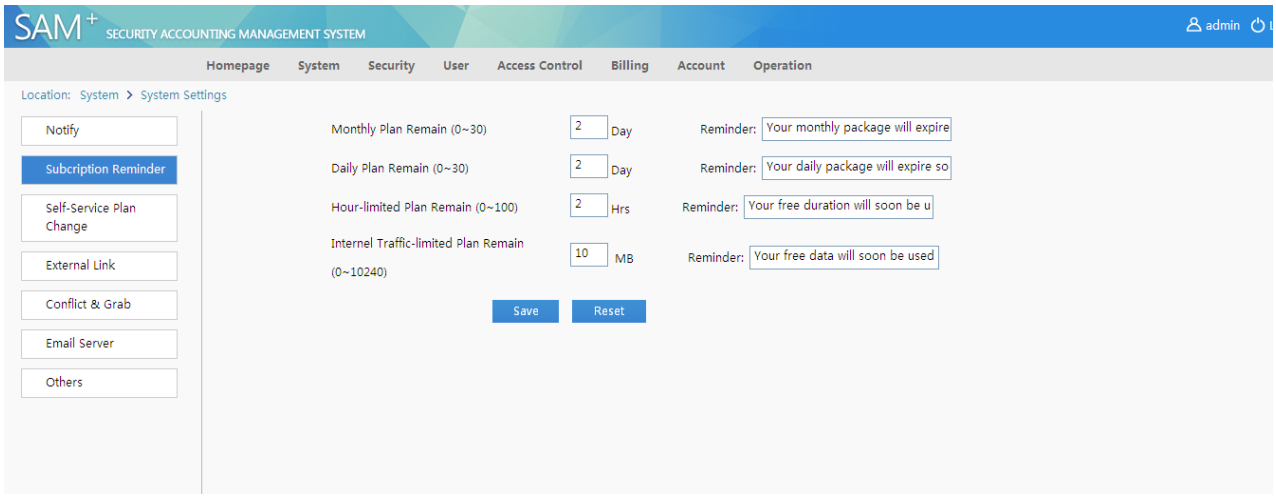
Pop-up URL when users login: After a user goes online, an IE page pops up on the client and jumps to this URL page.

User Forced Offline Message: This message is a unified prompt sent to a user who is forced to go offline by an administrator in the online user management before the user is offline. The default value is **Forced offline by the administrator!** Note that this message and the function of forcing users offline require that the community value of relevant devices in the RG-SAM+ system should be correct and the value should be granted the rw permission on the relevant devices. Otherwise, both the function of forcing users offline and user forced offline message are unavailable.

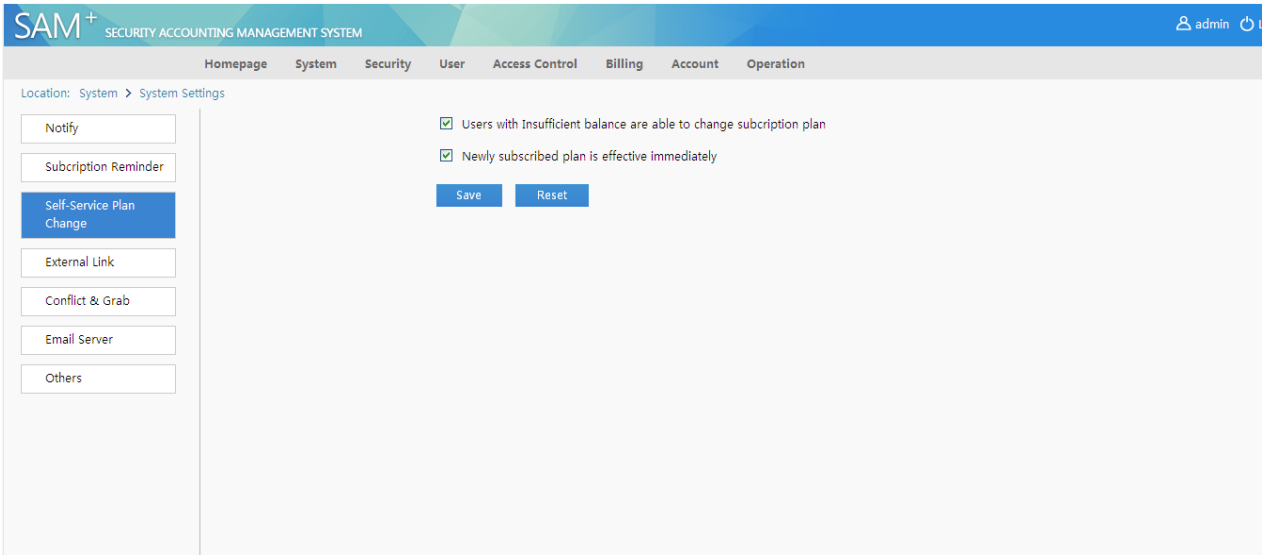
Disable Modem Dialing Blacklist Message: blacklist message displayed when a user is blacklisted because of modem dial-up.

Client Side Anti-cracking Blacklist Message: blacklist message displayed when a user is blacklisted because the user uses a cracked client.

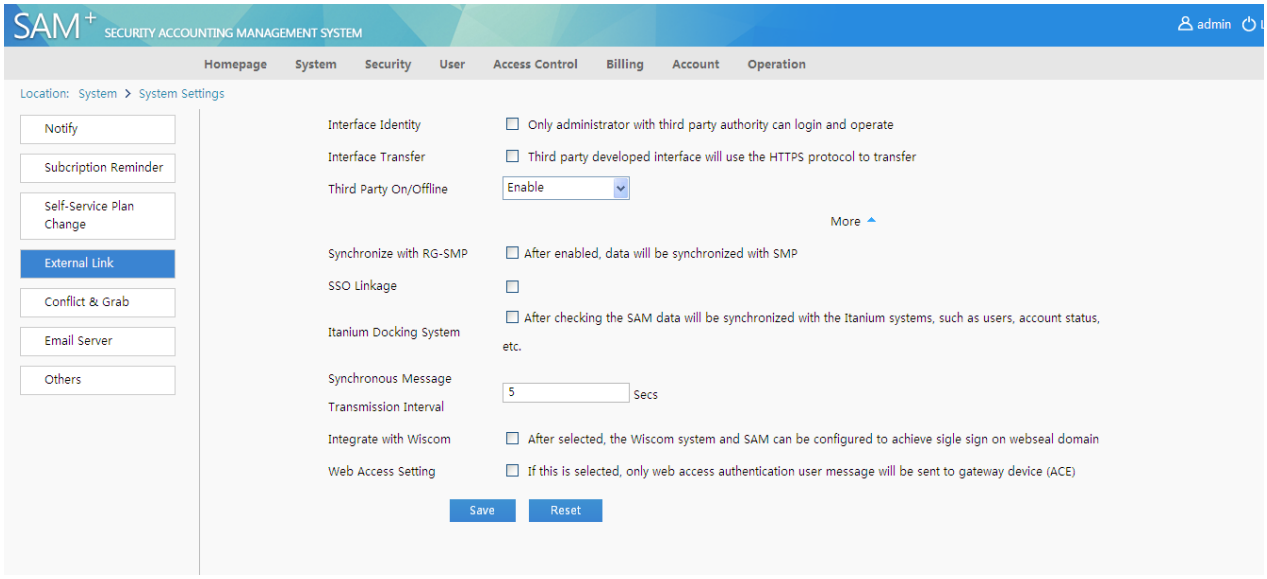
All messages are up to 250 bytes each and one Chinese character accounts for two bytes.



Subscription Reminder: Different messages are prompted for different users, for example, the number of remaining days is prompted for users who use a monthly plan.



Self-Service Plan Change: Administrators can set whether to allow plan change when a user's balance is insufficient and whether the new plan takes effect immediately.



External Link: Administrators can set whether to enable third party interface identity authentication, third party interface security transfer, and third party online/offline notification.

Third party here refers to a third-party system. Currently, the third party online/offline notification function of the RG-SAM+ system can be used to acquire information about online and offline users of the RG-SAM+ system. Currently,

this function is mainly used in combination with two schemes: gateway traffic billing scheme, and admission and exit gateway authentication scheme. In the application of the two schemes, the third party online/offline notification function must be enabled and the IP address of the RG-SAM+ system must be set on relevant systems so that the RG-SMP system, gateway billing device in the gateway traffic billing scheme and portal components in the admission and exit gateway authentication scheme connect to the RG-SAM+ system and receive third party online/offline message notifications. For configuration details, see the configuration description of the schemes. This function is disabled by default. If you want to apply the two schemes, enable this function and it takes effect immediately.

The other options are described as follows:

Synchronize with RG-SMP: After this function is enabled, and the synchronization port (9090) and server IP address of the RG-SMP system are set correctly, data can be synchronized between the RG-SAM+ system and the RG-SMP system, including adding, deleting, modifying network access servers (NASs) synchronously and deleting user information synchronously.

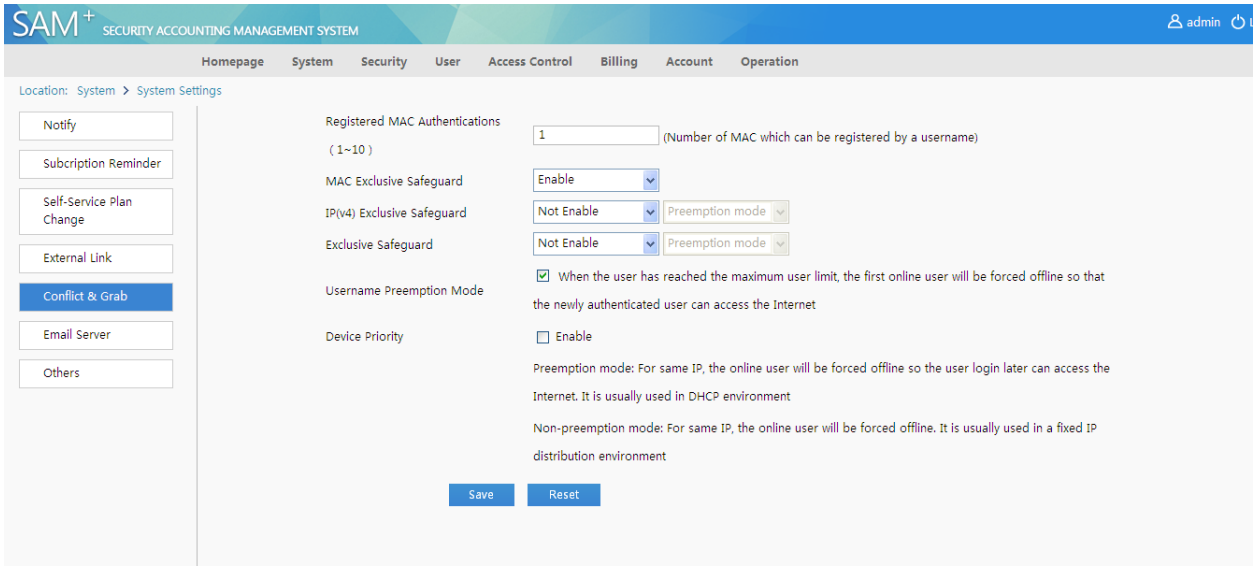
SSO Linkage: After this function is enabled, the correlation with the SSO correlation device is supported, single sign-on (SSO) is achieved, and the unified portal presentation is provided.

Itanlum Docking System: After this function is enabled, the RG-SAM+ system synchronizes relevant data with the Itanlum system.

The data to be synchronized includes user IDs, passwords, names, telephone numbers, addresses, and account status.

Integrate with Wiscom: After it is selected, the Wiscom system and RG-SAM+ system can be configured to achieve SSO webseal domain.

Web Access Setting: After it is selected, only Web access authentication user messages will be sent to the gateway.



Conflict & Grab:

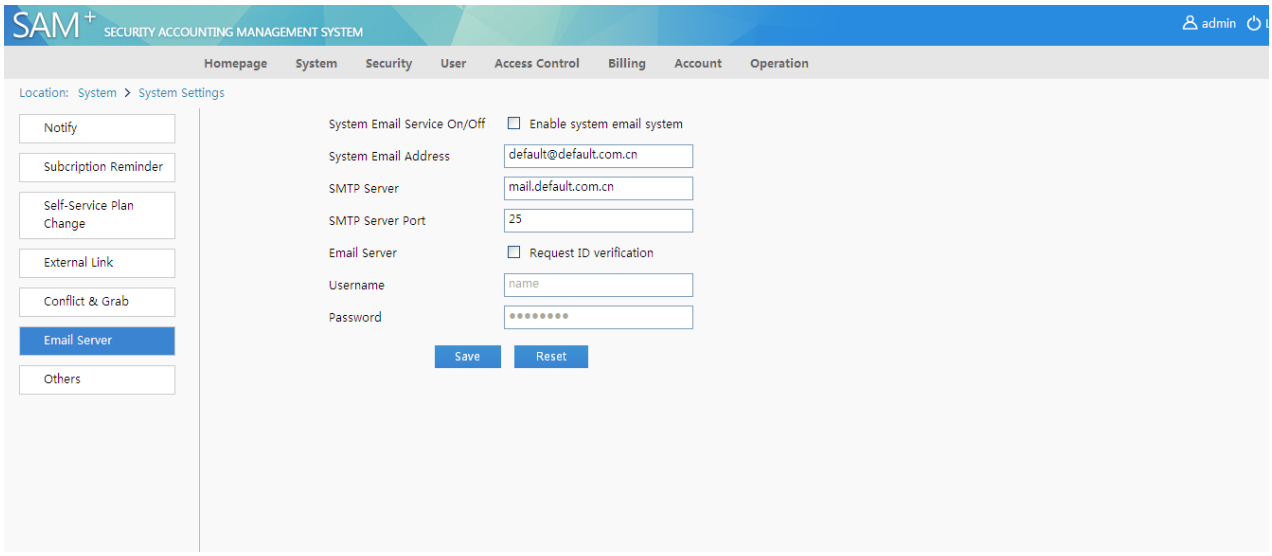
Registered MAC Authentications: specifies the number of MAC addresses that can be registered by a user.

MAC Exclusive Safeguard: This function is used to prevent users from faking MAC addresses to access the Internet so as to evade fees. It is enabled by default and it is recommended that the function be enabled. When a user attempts to go online through the MAC address of an online user from another computer, this function enables the RG-SAM+ system to reject the authentication.

IP(v4) Exclusive Safeguard: After this function is enabled, the RG-SAM+ system checks whether the IPv4 address of each user applying for authentication conflicts with the IPv4 addresses of currently online users.

Exclusive Safeguard: After this function is enabled, the RG-SAM+ system checks whether the IPv6 address of each user applying for authentication conflicts with the IPv6 addresses of currently online users.

Username Preemption Mode: When the number of currently online users reaches the upper limit, this function enables the RG-SAM+ system to force the user who goes online first to go offline so that the new authentication user can go online.



Email Server:

The email server settings include the setting of the system email address and the setting of the Simple Message Transfer Protocol (SMTP) server for sending emails. The two settings are linked, for example, when **STMP Server** is set to **mail.ruijie.com.cn**, **System Email Address** needs to be set to a value in the format of *xxxx*@**ruijie.com.cn**. If the SMTP server requires identity verification, select **Request ID verification** and enter the username and password for verification. Note: It is strongly recommended that you build an email server. Do not use free email servers because there are some limits, including transmission count within a short period and the email size.

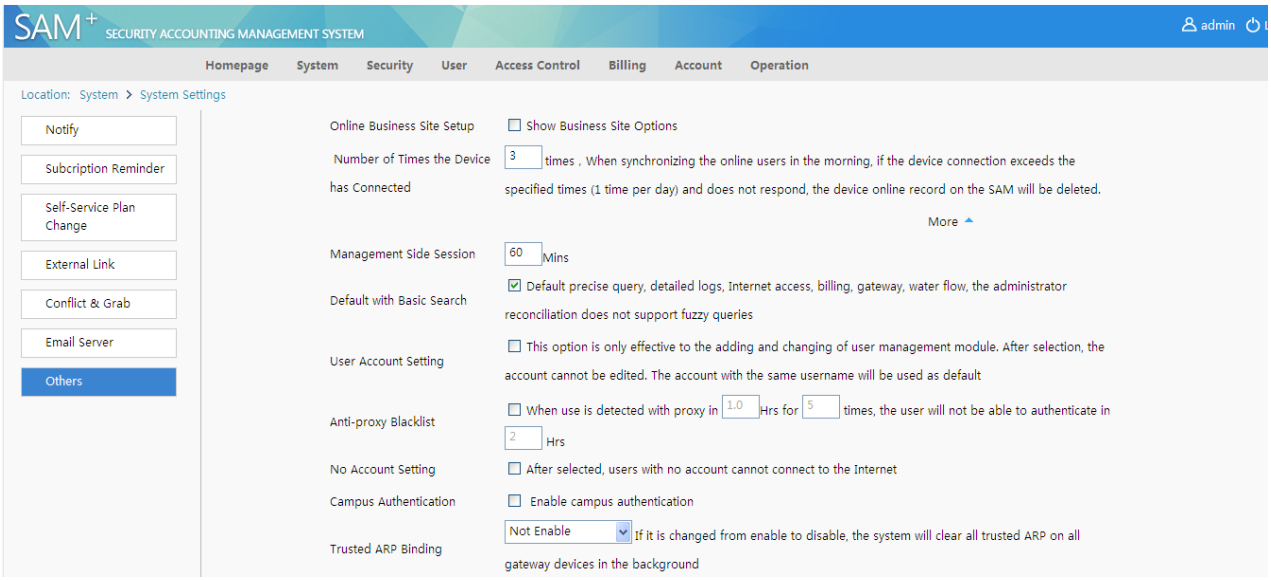
System email setting

The RG-SAM+ system has no independent email server, but some of its functions need to use the email sending function. Therefore, a third party email server needs to be configured. You may use the email sending function in the following services:

Retrieving passwords for self-service users: Users can retrieve their passwords with their usernames and corresponding email addresses (the email addresses must be matched with the email server) in the RG-SAM+ self-service system. The system email address is the address for sending the password retrieval emails. If the system email settings are incorrect or null, the password retrieval function of the self-service system is unavailable.

Registration review: After users register with the self-service system, administrators can view the users and review their registrations. If the system email settings are correct, registered users will receive a notification email regarding their successful or failed review result. This email is sent from the system email address to the email address of registered users. If no system email is set, the system email is set incorrectly, or the user email address is not set, users will not receive notification emails.

If no email server is available, do not enable the email service so as to save processing resources.



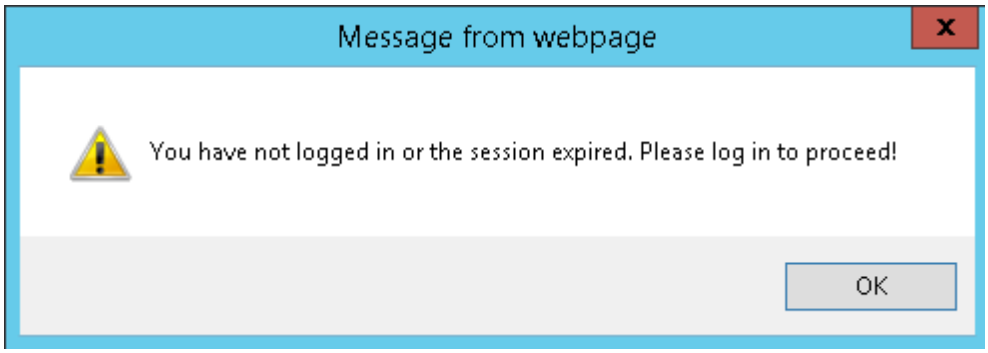
Others:

You can set whether to display cloud service platform settings and connection count.

The other options are described as follows:

Management Side Session: If an administrator does not perform any operation on the system within a period of time, the current session state is set to be expired for the sake of security. You can set the time here. The default value is 60

minutes. That is, if an administrator logs in and does not perform any operation within 60 minutes, a prompt as shown in the following figure is displayed.



Click **OK**. The system jumps to the login page, and the administrator needs to log in again before performing management operation.

Default with Basic Search: globally sets whether to perform the default fuzzy search when information records in the system are searched. It is deselected by default. When it is selected, all pages supporting the fuzzy search function use fuzzy search. When it is deselected, the precise search is used by default.

User Account Setting: sets whether to provide account setting on the user activation page. It is deselected by default. When it is selected, the account setting is not provided on the user activation page and an account with the name same as the username is directly linked with a user. When it is deselected, the account setting is provided and administrators can manually specify accounts linked with users.

Anti-proxy Blacklist: specifies that a user cannot pass authentication within a period of time if the user is detected to use proxy within a certain period for a specified number of times.

No Account Setting: After it is selected, users without accounts cannot access the Internet.

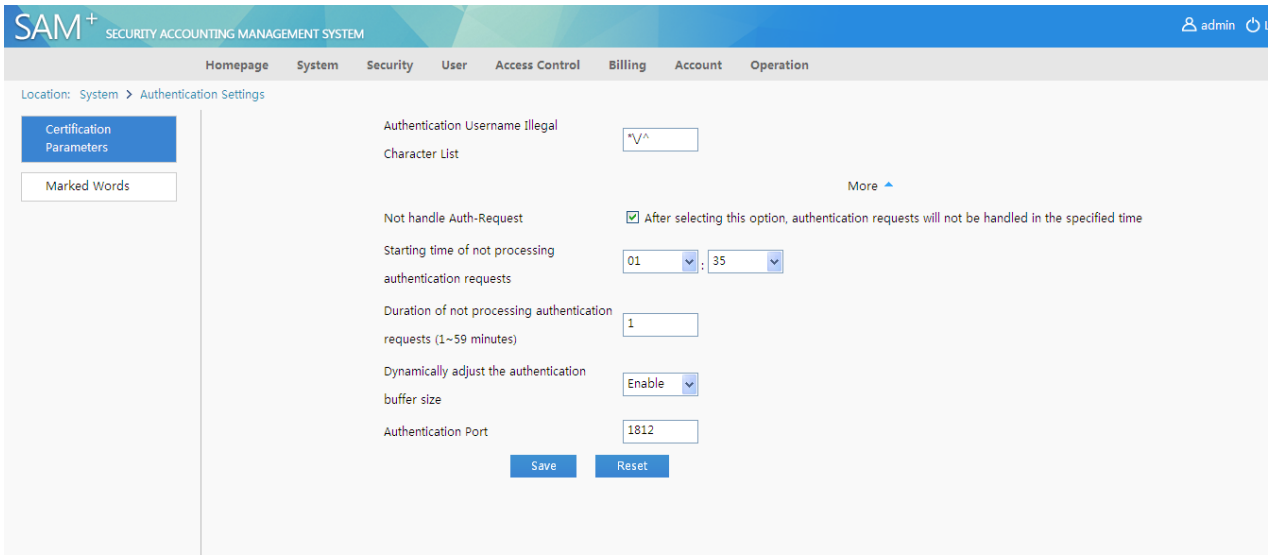
Trusted ARP Binding: This function is used to bind trusted Address Resolution Protocol (ARP) information to the gateway to prevent ARP spoofing. If it is set to **Enable**, when a user passes authentication, trusted ARP information is added to the gateway, and trusted ARP information is deleted from the gateway when the user goes offline. This function is disabled by default.

Authentication Settings

Authentication settings include parameter settings and failure reason settings.

Management of authentication parameters:

The change to the authentication port takes effect upon saving and the authentication service restarts immediately.



Duration of not processing authentication requests:

Duration of not processing authentication requests refers to the duration in which the RG-SAM+ system provides only the accounting function and disables the authentication function. As shown in the preceding figure, whether to enable the function of not processing authentication requests, the start time and duration of not processing authentication requests can be set. The start time ranges from 00:00 to 23:59 and the duration ranges from 1 minute to 59 minutes.

Authentication Username Illegal Character List

This function is used to set a collection of characters that cannot be contained in usernames for authentication. If a username contains one or more characters in this collection, the user cannot pass authentication.

Dynamically adjust the authentication buffer size:

This function is used to automatically reduce the buffer area when there are many timeout packets, and automatically expand the buffer area when there is no timeout packet. The maximum and minimum sizes of the buffer area are 100 and 1 respectively.

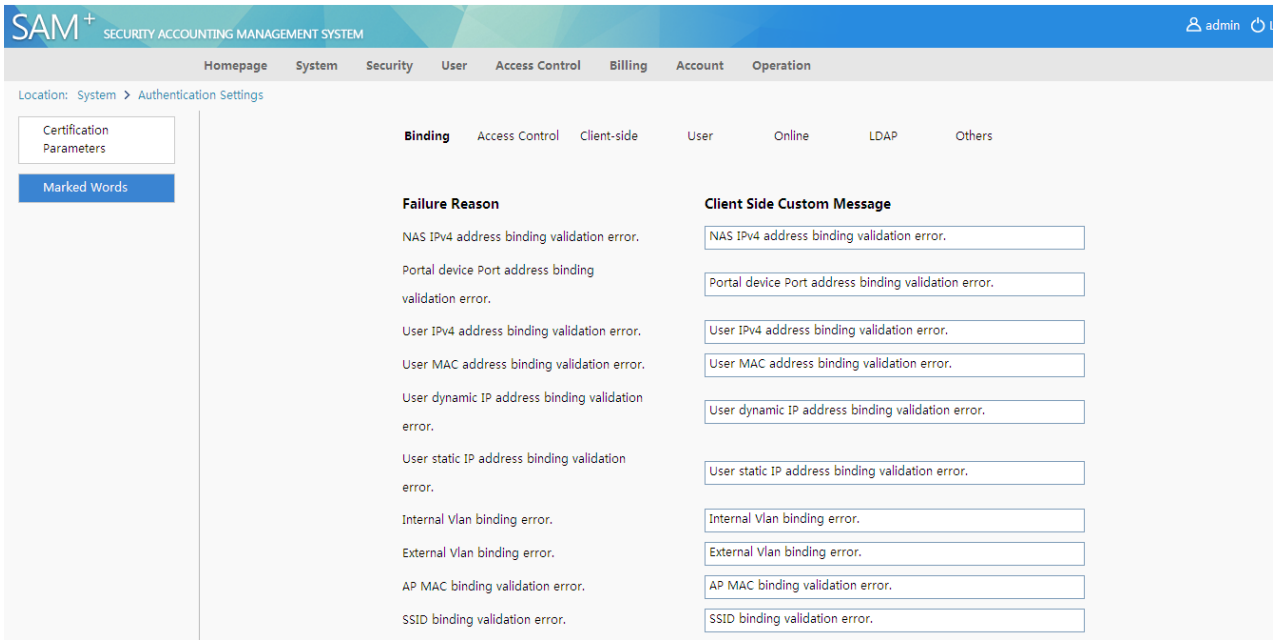
Notes:

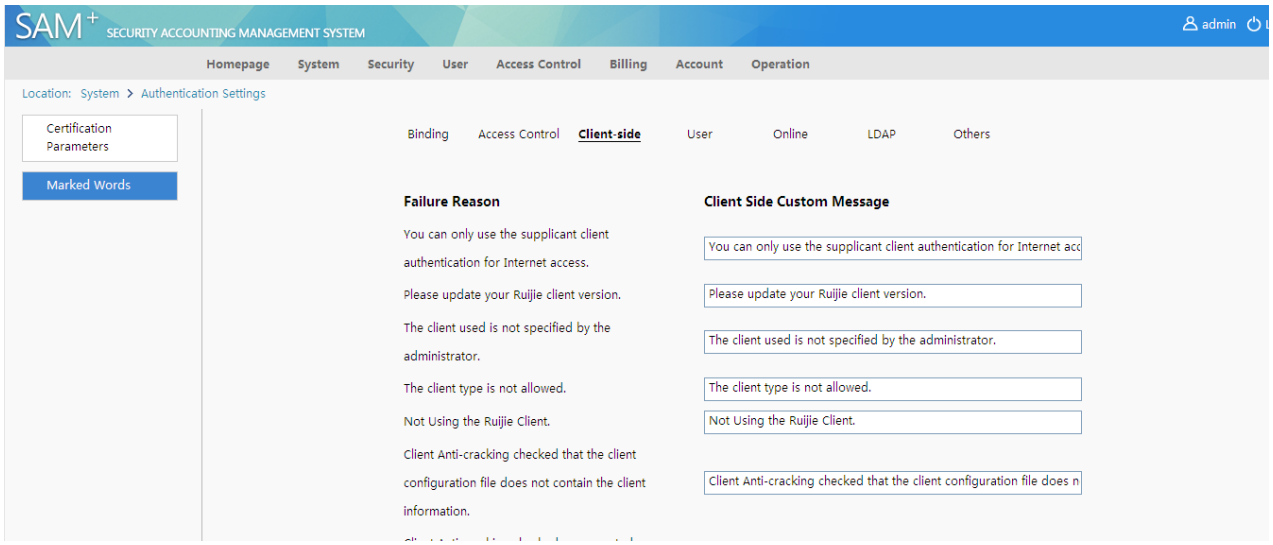
In the duration of not processing authentication requests, the RADIUS server does not respond to any authentication requests. Therefore, be careful when setting the duration of not processing authentication requests.

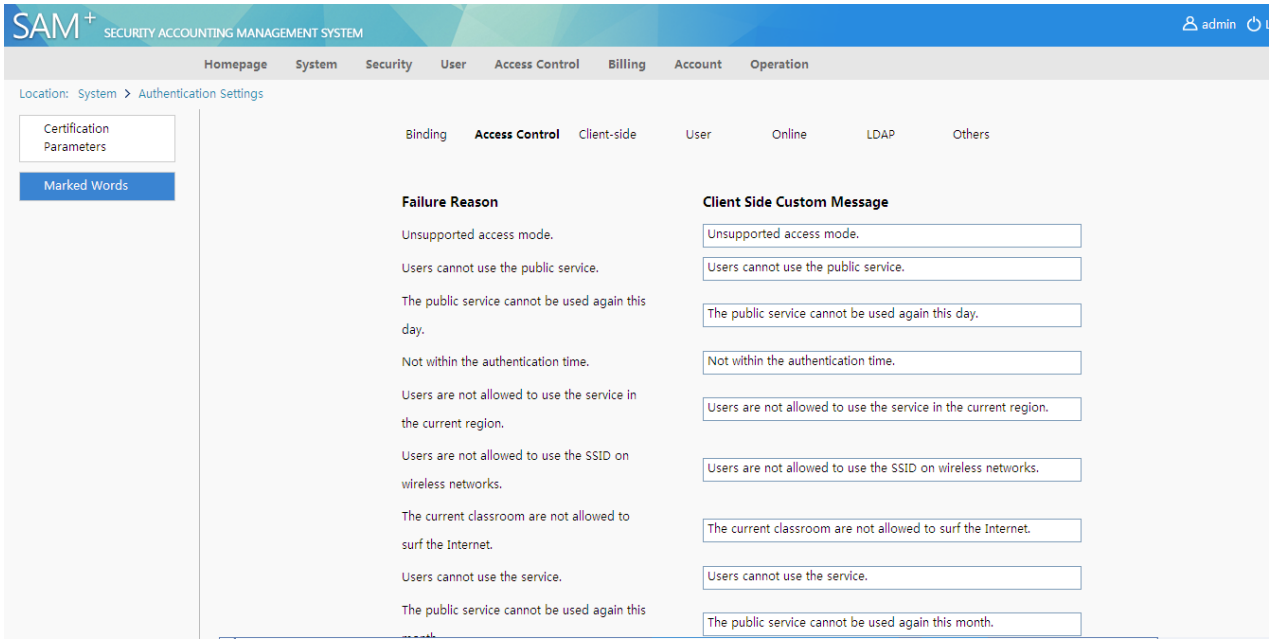
The function of not processing authentication requests relieves necessary overheads for the RADIUS server to a certain extent, and its effect is more obvious in peak hours for accounting packets.

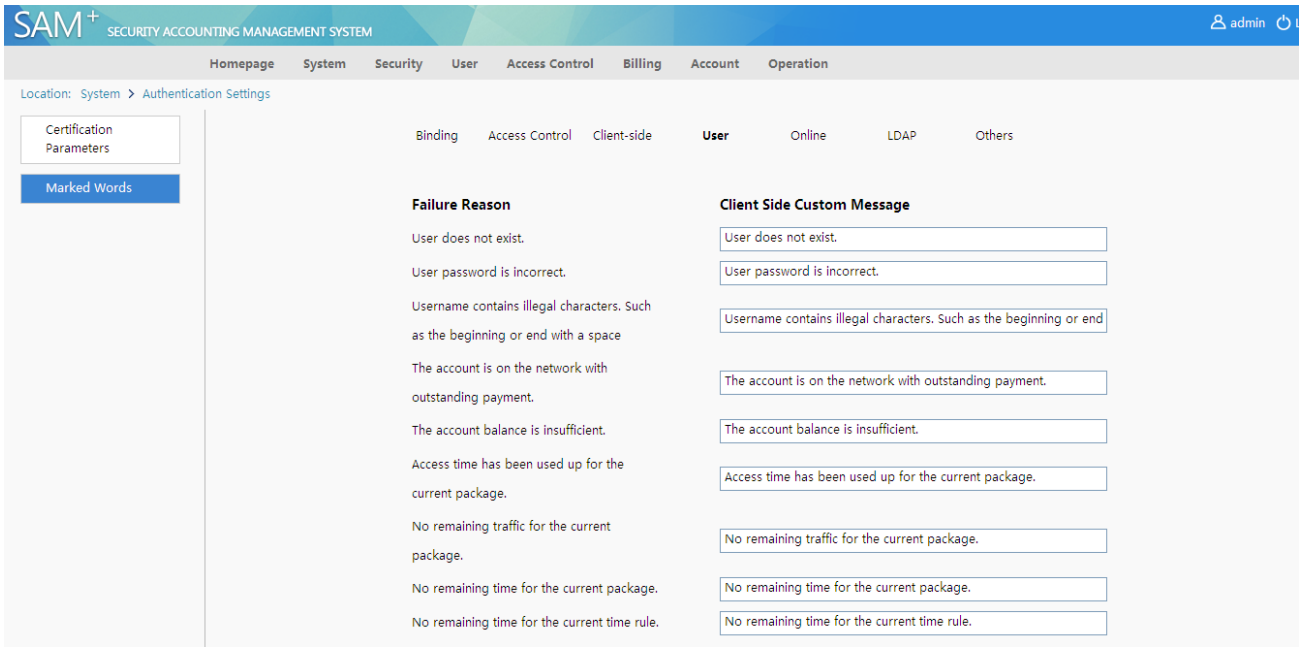
The permissible error is about 1 minute in the duration of not processing authentication requests.

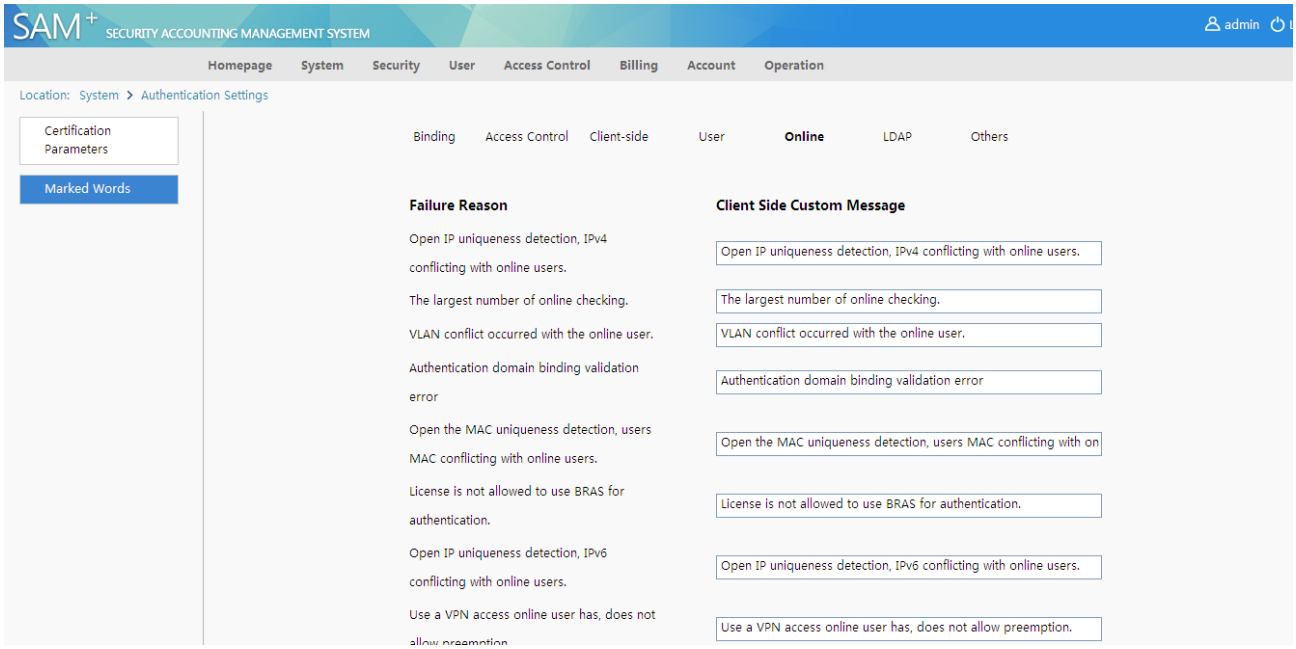
Settings of authentication failure reasons:

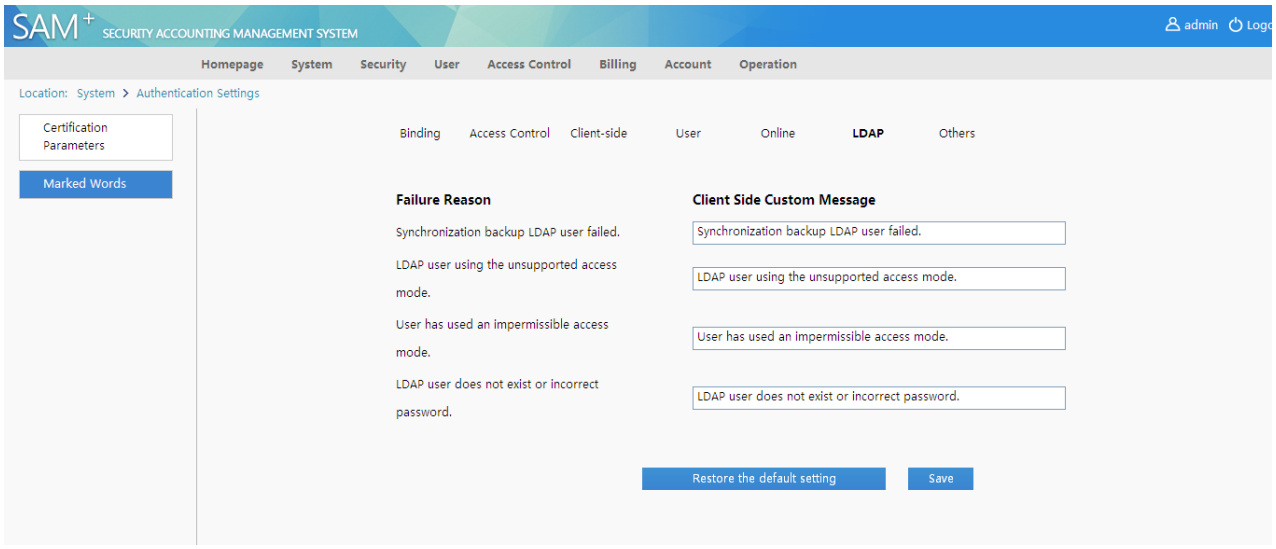

SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM
admin
Homepage System Security User Access Control Billing Account Operation
Location: System > Authentication Settings
Certification Parameters
Marked Words
Binding Access Control Client-side User Online LDAP Others
Failure Reason
Client Side Custom Message
NAS IPv4 address binding validation error.
Portal device Port address binding validation error.
User IPv4 address binding validation error.
User MAC address binding validation error.
User dynamic IP address binding validation error.
User static IP address binding validation error.
Internal Vlan binding error.
External Vlan binding error.
AP MAC binding validation error.
SSID binding validation error.

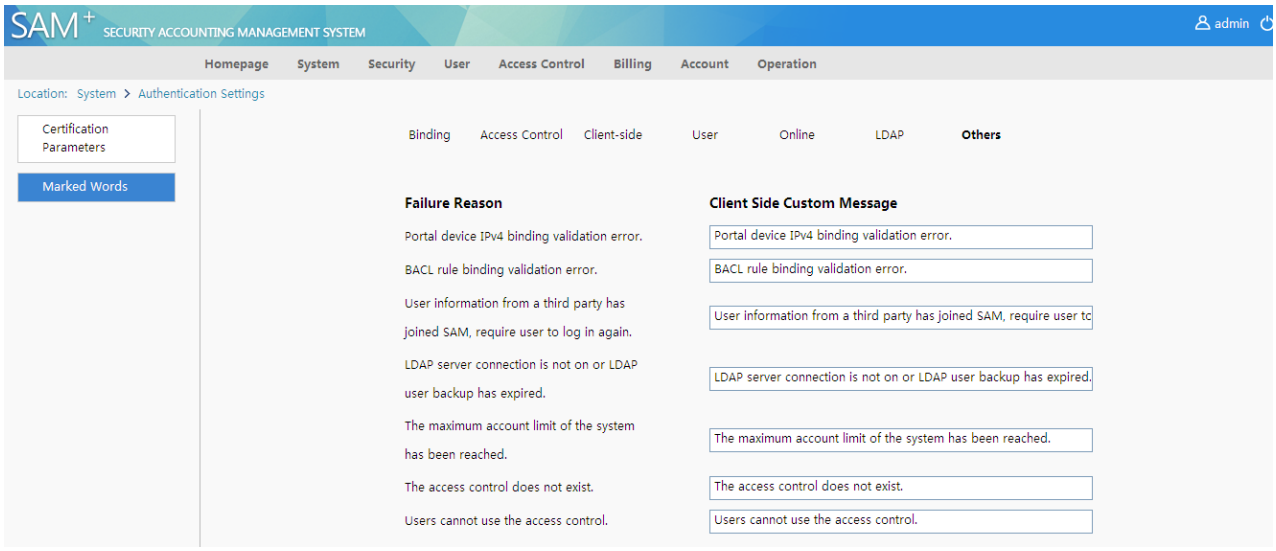

SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM
admin
Homepage System Security User Access Control Billing Account Operation
Location: System > Authentication Settings
Certification Parameters
Marked Words
Binding Access Control Client-side User Online LDAP Others
Failure Reason
Client Side Custom Message
You can only use the supplicant client authentication for Internet access.
Please update your Ruijie client version.
The client used is not specified by the administrator.
The client type is not allowed.
Not Using the Ruijie Client.
Client Anti-cracking checked that the client configuration file does not contain the client information.


SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM
admin
Homepage System Security User Access Control Billing Account Operation
Location: System > Authentication Settings
Certification Parameters
Marked Words
Binding Access Control Client-side User Online LDAP Others
Failure Reason
Client Side Custom Message
Unsupported access mode.
Unsupported access mode.
Users cannot use the public service.
Users cannot use the public service.
The public service cannot be used again this day.
The public service cannot be used again this day.
Not within the authentication time.
Not within the authentication time.
Users are not allowed to use the service in the current region.
Users are not allowed to use the service in the current region.
Users are not allowed to use the SSID on wireless networks.
Users are not allowed to use the SSID on wireless networks.
The current classroom are not allowed to surf the Internet.
The current classroom are not allowed to surf the Internet.
Users cannot use the service.
Users cannot use the service.
The public service cannot be used again this
The public service cannot be used again this month.


SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM
admin
Homepage System Security User Access Control Billing Account Operation
Location: System > Authentication Settings
Certification Parameters
Marked Words
Binding Access Control Client-side User Online LDAP Others
Failure Reason
Client Side Custom Message
User does not exist.
User does not exist.
User password is incorrect.
User password is incorrect.
Username contains illegal characters. Such as the beginning or end with a space
Username contains illegal characters. Such as the beginning or end
The account is on the network with outstanding payment.
The account is on the network with outstanding payment.
The account balance is insufficient.
The account balance is insufficient.
Access time has been used up for the current package.
Access time has been used up for the current package.
No remaining traffic for the current package.
No remaining traffic for the current package.
No remaining time for the current package.
No remaining time for the current package.
No remaining time for the current time rule.
No remaining time for the current time rule.


SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM
admin
Homepage System Security User Access Control Billing Account Operation
Location: System > Authentication Settings
Certification Parameters
Marked Words
Binding Access Control Client-side User Online LDAP Others
Failure Reason
Client Side Custom Message
Open IP uniqueness detection, IPv4 conflicting with online users.
Open IP uniqueness detection, IPv4 conflicting with online users.
The largest number of online checking.
The largest number of online checking.
VLAN conflict occurred with the online user.
VLAN conflict occurred with the online user.
Authentication domain binding validation error
Authentication domain binding validation error
Open the MAC uniqueness detection, users MAC conflicting with online users.
Open the MAC uniqueness detection, users MAC conflicting with on
License is not allowed to use BRAS for authentication.
License is not allowed to use BRAS for authentication.
Open IP uniqueness detection, IPv6 conflicting with online users.
Open IP uniqueness detection, IPv6 conflicting with online users.
Use a VPN access online user has, does not allow preemption.
Use a VPN access online user has, does not allow preemption.


SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM
admin
Homepage System Security User Access Control Billing Account Operation
Location: System > Authentication Settings
Certification Parameters
Marked Words
Binding Access Control Client-side User Online LDAP Others
Failure Reason
Client Side Custom Message
Synchronization backup LDAP user failed.
Synchronization backup LDAP user failed.
LDAP user using the unsupported access mode.
LDAP user using the unsupported access mode.
User has used an impermissible access mode.
User has used an impermissible access mode.
LDAP user does not exist or incorrect password.
LDAP user does not exist or incorrect password.
Restore the default setting
Save



Authentication failure prompt setting:

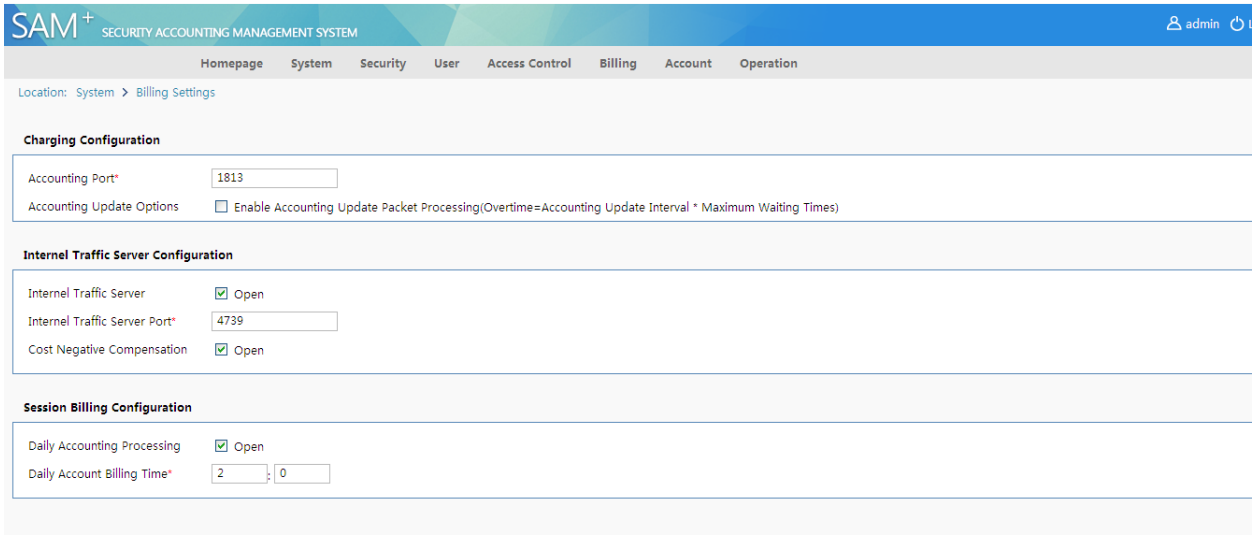
This function sets failure prompts.

Note:

You need to choose **System**>**Blacklist Management** from the main menu to set prompts for authentication failures of blacklisted users.

Billing Settings

The **Billing Settings** page is used to set parameters relevant to the billing service, mainly the accounting port. The default accounting port ID is 1813. An accounting port takes effect immediately after change and the billing service restarts immediately.



For description of the accounting update, see "Detailed Billing Description of the RG-SAM+ System."

Billing parameters relevant to the RG-SAM+ system and gateway traffic server concern the startup/shutdown of the gateway traffic server and port ID of the gateway traffic server. The gateway traffic server is shut down by default and the default port ID is 4739. The gateway traffic server needs to be started if the gateway traffic server scheme is used.

Billing parameters relevant to period-based fee deduction are **Daily Accounting Processing** and **Daily Account Billing Time**. **Daily Accounting Processing** is set to **Open** by default and the default value of **Daily Account Billing Time** is 02:00 a.m.

LDAP Configuration

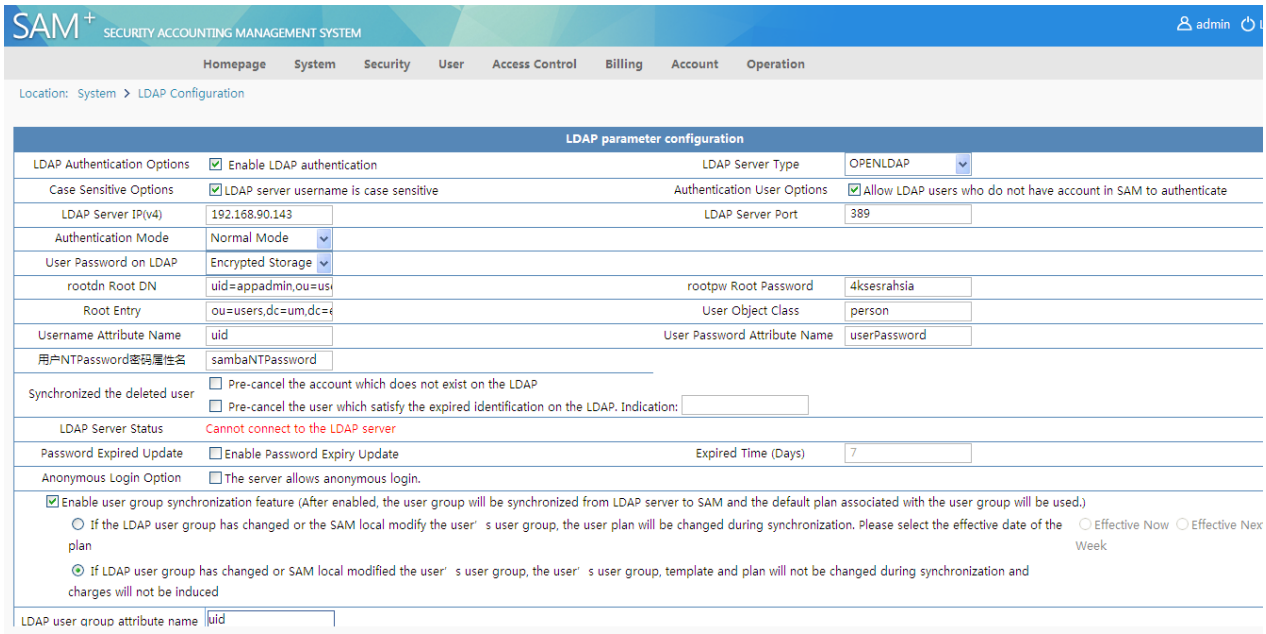
The RG-SAM+ system supports user authentication by means of OpenLDAP and Active Directory with two application modes, namely, normal mode and billing mode. Both OpenLDAP and Active Directory support the normal mode but only OpenLDAP supports the billing mode.

Normal mode

In normal mode, when a user attempts to pass the authentication of the RG-SAM+ system to access the Internet, the RG-SAM+ system checks whether the user password is correct. If the user password is incorrect, the user authentication is transferred to the Lightweight Directory Access Protocol (LDAP) server. If the user passes the authentication of the LDAP server, the user password is synchronized from the LDAP server to the RG-SAM+ system (the password synchronization must be enabled). In addition, if user information cannot be found on the RG-SAM+ system, the user authentication is also transferred to the LDAP server. If the user passes the authentication of the LDAP server, the user information is synchronized from the LDAP server to the RG-SAM+ system.

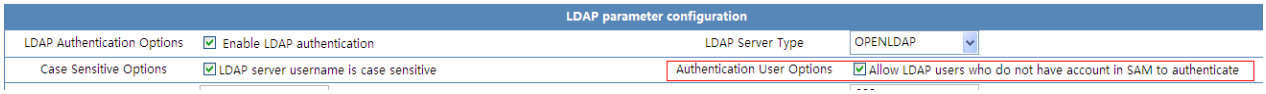
In normal mode, all billing is conducted on the RG-SAM+ system.

Enable user group synchronization feature in LDAP normal mode:



If you select **Enable user group synchronization feature** in normal mode, enter the user group attribute name that is set on the LDAP server, and enter the user group name on the LDAP server consistent with that on the RG-SAM+ system. Then, the entered user group information is synchronized from the LDAP server to the corresponding user group of the RG-SAM+ system. If a user group name on the LDAP server is blank in value mapping, it is synchronized to the **root** user group of the RG-SAM+ system by default.

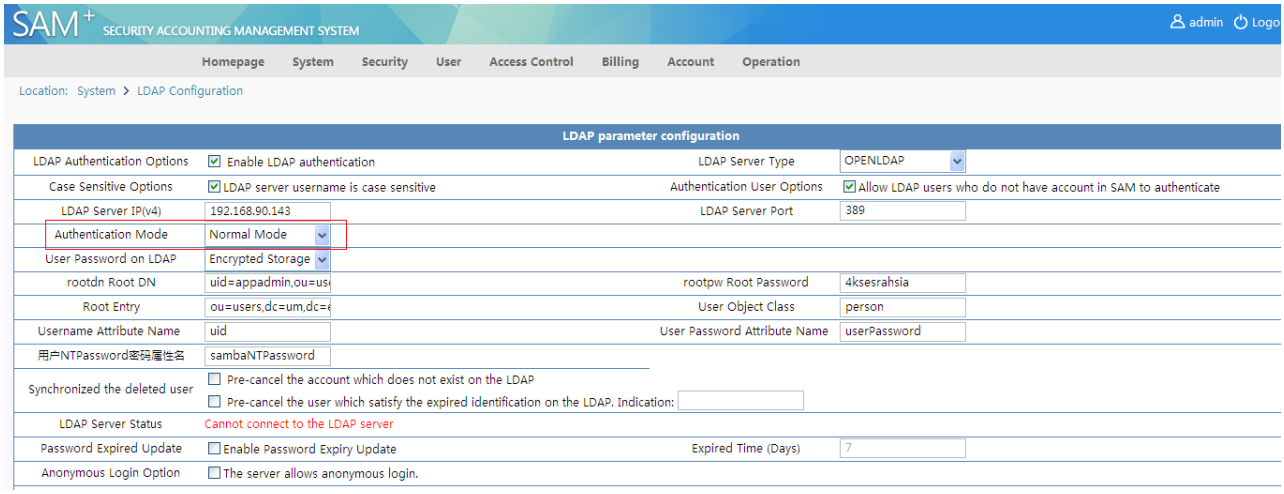
Authentication User Options: After you select this parameter, a user whose information does not exist on the RG-SAM+ system but exists on the LDAP server can pass the authentication.



Billing mode

In billing mode, when information about a user does not exist on the RG-SAM+ system, the user is authenticated by the LDAP server and the RG-SAM+ system does not conduct billing for this type of users. Another system that manages the LDAP server stores the available Internet access duration of the user on the LDAP server. The RG-SAM+ system reads the available Internet access duration from the LDAP server and makes judgments. If the available Internet access duration is greater than zero, the RG-SAM+ system pushes its available Internet access duration to the switch authentication device through SessionTimeOut of the RADIUS server. If the available Internet access duration is smaller than or equal to zero, the user authentication failed. Users whose information exist on the RG-SAM+ system is always authenticated by the RG-SAM+ system rather than by the LDAP server.

OpenLDAP authentication mode (normal mode)



When Authentication Mode is set to Normal Mode:

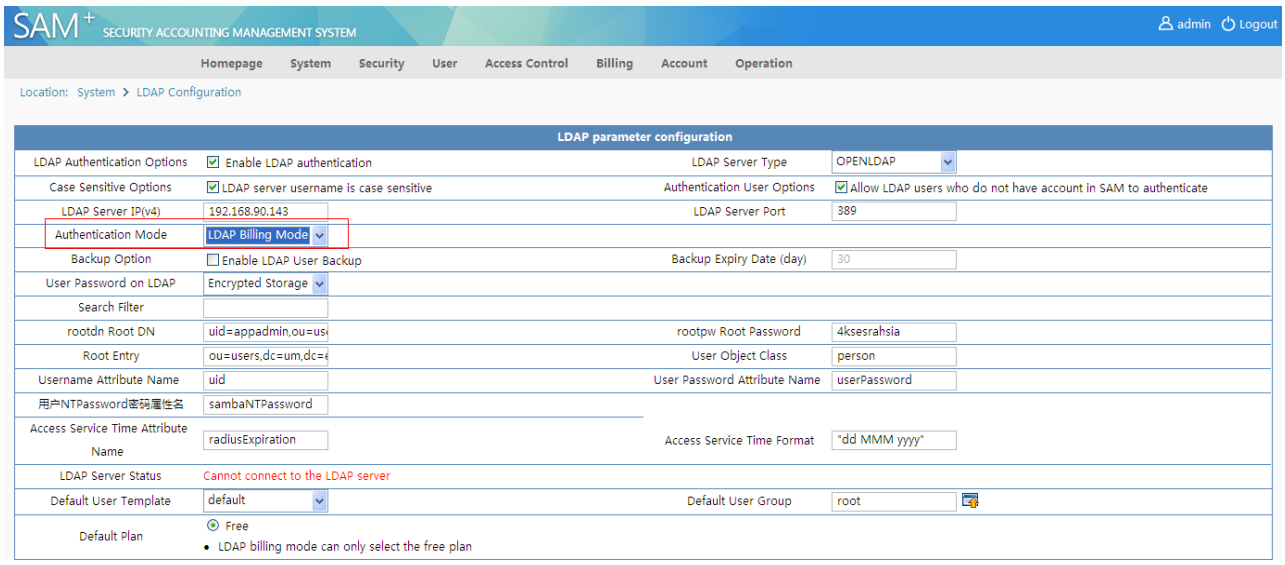
If information about a user does not exist in the RG-SAM+ system database, the RG-SAM+ system obtains the user password from the LDAP server based on the username and compares the user password with the entered password. If the entered password is correct, the RG-SAM+ system adds the user information to the database and the user becomes a user of the RG-SAM+ system. You can set **Default User Self-service Authority** to enable LDAP users added to the RG-SAM+ system to log in to the self-service system.

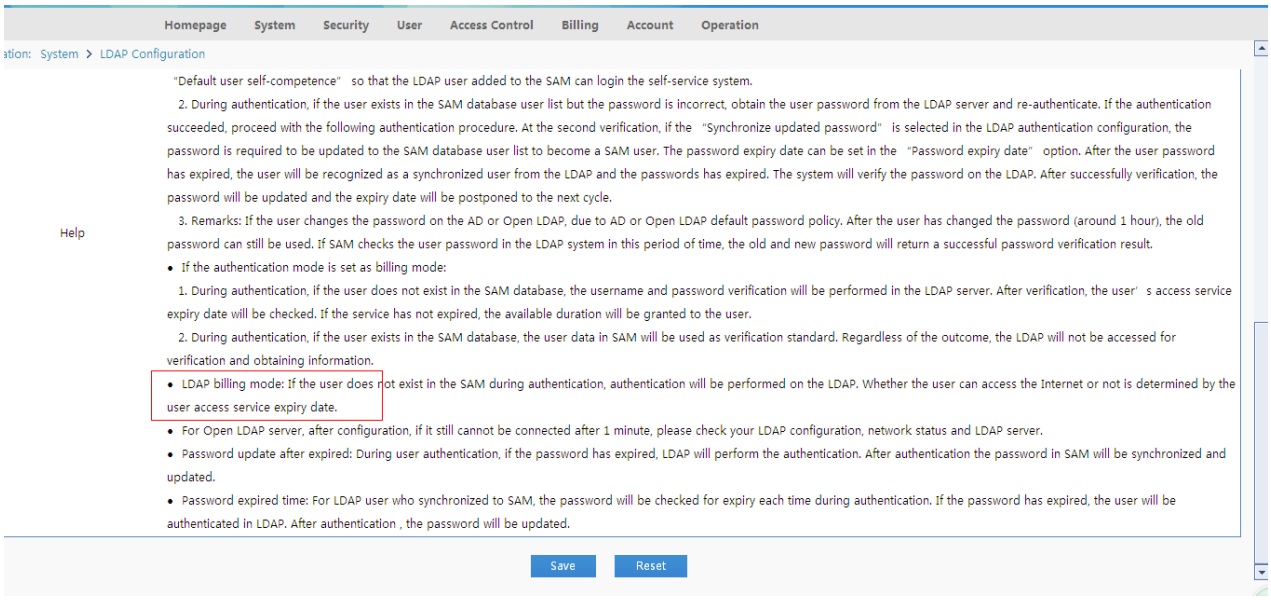
If information about a user exists in the RG-SAM+ system database but the password is incorrect, the RG-SAM+ system obtains the password from the LDAP server and performs verification again. If the user passes the verification, the RG-SAM+ system proceeds with subsequent authentication. If the option of synchronizing password update is selected in the LDAP authentication configuration, the password is updated to the RG-SAM+ system database and the user becomes a user of the RG-SAM+ system. You can set the password expiration time in **Expired Time (Days)**. When a user password expires, the RG-SAM+ system identifies that the user information is synchronized from the LDAP server, and the user password is beyond the expiration time, the RG-SAM+ system transfers the user information to the LDAP server for password authentication. After the user passes the authentication, the RG-SAM+ system updates the password and sets the expiration time one period later.

Note: If a user changes the password on Active Directory or OpenLDAP, the old and new passwords are both effective within a period of time (about one hour) after password change because of the default password policy. If the RG-SAM+ system finds the user password on the LDAP server, users can pass the authentication with either the new or the old password.

If usernames are case sensitive on the LDAP server, select **LDAP server username is case sensitive**. Otherwise, deselect it.

OpenLDAP authentication mode (billing mode)





Note: Ensure that the time of the LADP server is the same as that of the RG-SAM+ system. Otherwise, the user service may be expired improperly.

When Authentication Mode is set to LDAP Billing Mode:

If information about a user does not exist in the RG-SAM+ system database, the username and password are verified on the LDAP server. After the user passes the authentication, the RG-SAM+ system checks whether the access service duration (on the LDAP server) expires. If no, the RG-SAM+ system pushes the access service duration as the available Internet access duration of the user.

If information about a user exists in the RG-SAM+ system database, the RG-SAM+ system verifies the user according to its stored information, and it neither transfers authentication to the LDAP server nor obtains information from the LDAP server.

If the LDAP server cannot be connected or is abnormal in state and **Enable LDAP User Backup** is selected, the previous backup information (including the username, password, and access service duration) is used for authentication. Information backup is conducted only after successful authentication. After backup information expires, the backup information is updated after the first successful authentication after expiration. If the LDAP server is down and the backup information expires, the user cannot pass authentication.

In LDAP billing mode, administrators can set whether to back up user information on the LDAP server to the RG-SAM+ system database. Note that backup information obtained from the LDAP server is not stored in the user table but stored as special LDAP backup information, which is different from the operation in LDAP normal mode. You can choose **Operation**>**LDAP Backup** to view and modify the LDAP backup information.

LDAP parameters

LDAP Server IP(v4) — IP address of the LDAP server.

LDAP Server Port — port ID of the LDAP service. The default port ID is **389**.

LDAP Server Type — type of the LDAP server. The value is **OpenLDAP**.

rootdn — rootdn defined in the configuration file **slapd.conf** of OpenLDAP. It indicates anonymous login if it is not set.

rootpw — rootpw defined in the configuration file **slapd.conf** of OpenLDAP. The value needs to be entered in plain text and it indicates anonymous login if it is not set.

Root Entry — DN of the root node of the tree where a user is located. All users should be in this node, for example, **dc=universityname,dc=com**.

User Object Class — objectclass attribute of a user entry, for example, **inetorgPerson**.

Username Attribute Name — attribute indicating the login name in a user entry, for example, **uid**.

User Password Attribute Name — attribute indicating the password in a user entry, for example, **userPassword**.

User Password on LDAP — Select **Encrypted Storage** if user passwords are encrypted for storage, otherwise select **Unencrypted Storage**.

If **LDAP Server Type** is set to **OPENLDAP** and **User Password on LDAP** is set to **Encrypted Storage**, **User Password Attribute Name** does not need to be set.

Backup Option — In LDAP billing mode, administrators can set whether to back up user information on the LDAP server to the RG-SAM+ system database. Note that backup information obtained from the LDAP server is not stored in the user table but stored as special LDAP backup information, which is different from the operation in LDAP normal mode. You can choose **Operation**>**LDAP Backup** to view and modify the LDAP backup information.

Access Service Time Attribute Name — attribute indicating the access service duration in a user entry. The default value is **radiusExpiration**.

Access Service Time Format — time format of the access service duration attribute. Note that the time format is enclosed in double quotation marks.

Expired Time (Days) — effective storage duration of LDAP user passwords in the RG-SAM+ system database.

Anonymous Login Option — Select it if the LDAP server supports anonymous login. Otherwise, deselect it.

Default User Group — default user group to which LDAP users belong.

Default User Template — default user template of LDAP users.

Search Filter — If **Search Filter** is set, the RG-SAM+ system queries user information on the LDAP server based on the filter condition rather than the configured user object class. **%{User-Name}** indicates that it will be replaced with actual user IDs. For example,

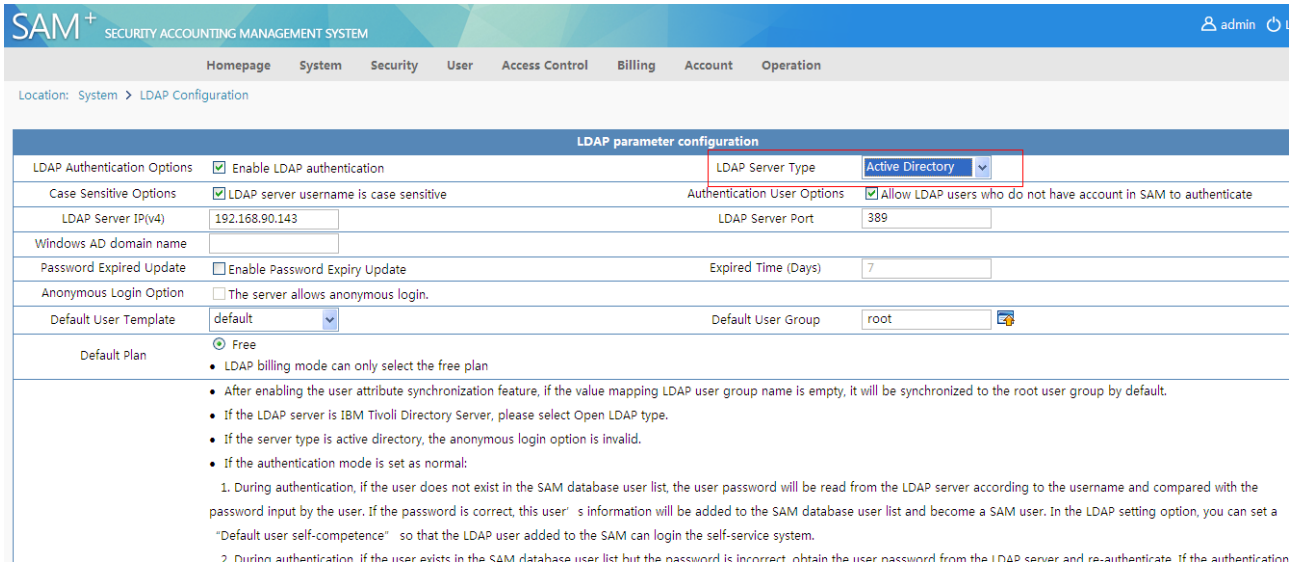
(&(objectclass=radiusprofile)(uid=%{User-Name})(|(eduPersonPrimaryAffiliation=faculty & staff)(eduPersonPrimaryAffiliation=student)))

%{User-Name} indicates the variable in place of usernames and the filter condition is not enclosed in double quotation marks.

Note: **Search Filter** and **User Object Class** are mutually exclusive. If **Search Filter** is set, the settings of **User Object Class** do not take effect.

Case Sensitive Options — If usernames are case sensitive on the LDAP server, select **LDAP server username is case sensitive**. Otherwise, deselect it.

Active Directory authentication configuration



Parameter description:

LDAP Server IP(v4) — IP address of the LDAP server.

LDAP Server Port — port ID of the LDAP service. The default port ID is **389**.

LDAP Server Type — type of the LDAP server. The value is **Active Directory**.

Windows AD domain name — domain name that must be contained in the login name for AD users (only the login name needs to be entered during login from SUs).

Default User Group — default user group to which LDAP users belong.

Default User Template — default user template of LDAP users.

Case Sensitive Options — If usernames are case sensitive on the LDAP server, select **LDAP server username is case sensitive**. Otherwise, deselect it.

Device Management

The RG-SAM+ server can be connected to many types of devices, including switches, routers, portal components, and wireless switches. The mode of connecting the devices to the RG-SAM+ server needs to be differentiated on the RG-SAM+ server. For the sake of server security, the RG-SAM+ system provides connection and processing services only for the devices registered with the RG-SAM+ system. The concept of device groups is introduced on the basis of devices for the ease of unified management.

Device-related functions are located in **Device Management** in **System**. The adding attributes show that the RG-SAM+ system supports the following device types currently:

- Ruijie switch
- Ruijie router
- Wireless switch
- Portal component
- Exit correlation device
- H3C compatible device
- Web gateway authentication device
- Trusted ARP binding gateway
- Other non-Ruijie authentication device

Ruijie switches refer to Ruijie switches of the S29*XX*, S26*XX*, S57*XX* and other models. When you set the device type to Ruijie switch, ensure that the switch is a Ruijie switch and the model is correct. Otherwise, some functions may be unavailable (for example, real-time SMS function, function of forcing users offline, and Web authentication).

Ruijie routers refer to Ruijie routers of R26*XX*, R36*XX*, R37*XX* and later models,. It is mainly applied in the VPN library scheme. For the scheme topology, see "Deployment in VPN Access Mode."

Wireless switches are designed for 802.1X-compliant wireless devices, which need to support any or multiple of RADIUS PAP, CHAP, EAP-MD5 authentication modes. Otherwise, the devices cannot pass the authentication through the RG-SAM+ system. Currently, wireless switches RG-WS5708, RG-WS5302, and other models are supported.

Portal components are a type of products released by Ruijie for implementing the portal mode of browser-based Internet authentication without clients, in combination with the S26*XX* series switches. Portal components are largely applied in the portal scheme. For the scheme topology, see "Deployment in Portal Access Mode."

Exit correlation devices refer to devices with NPE-relevant settings and determine the exit (such as education exit or telecommunication exit) for a user according to the exit correlation policy in the billing policy. Billing policies include monthly billing policies and daily billing policies.

H3C compatible devices refer to H3C switches.

The Web gateway authentication device refers to the RG-ACE, which is a gateway traffic control device of Ruijie used for controlling user traffic and conducting gateway authentication.

A trusted ARP binding gateway is a gateway supporting ARP binding. After authentication, a user's IP address, MAC address, and other information are bound to the gateway to prevent ARP spoofing.

Other non-Ruijie authentication devices refer to devices of other vendors, or devices with the types not listed above. Such devices may not support the particular functions of Ruijie devices, such as the function of forcing users offline, real-time SMS function, client version limit, and automatic client upgrade. If the RG-SAM+ system correlates with the RG-SMP system, set the device type to other non-Ruijie authentication device when adding devices.

When adding a device, you must select a device group attribute, which is only used by administrators to classify and manage devices conveniently. The RG-SAM+ system has a default device group. If you do not need to use this function, use the default device group for all devices.

Another purpose of a device group is to determine the scope of devices that can be managed by a device administrator, in combination with device management privileges. The details will be described in the device management privilege section.

Note

Areas settings:

If a device is an 802.1X-compliant access device (NAS) in the RG-SAM+ system, the area to which the device belongs can be selected. Area is an important concept for conducting area-based access control and area-based billing service in the RG-SAM+ system. In essence, an area to which a device belongs is the area to which a user authenticated on the device belongs. Such an area is called an area classified by device IP address.

In actual applications, for example, the device IP address sets of the library and dormitory are definite, you can add the library and dormitory area first, and then set devices (switches and routers) as the devices belonging to the areas.

Some advanced applications can be adopted after area setting, for example, you can confine some service to access areas and adopt area-based billing. For details, see relevant sections.

Note

Functions of key and community:

The key and community parameters need to be set for devices except the RG-NTD and RG-ACE. Key is used for verification during 802.1X authentication and community is a mandatory verification value for calling interface on switches.

A key is important for verification in RADIUS. If the key value of a device on the RG-SAM+ system is inconsistent with the key value of the device, the RADIOUS verification fails. That is, users cannot pass authentication through the device.

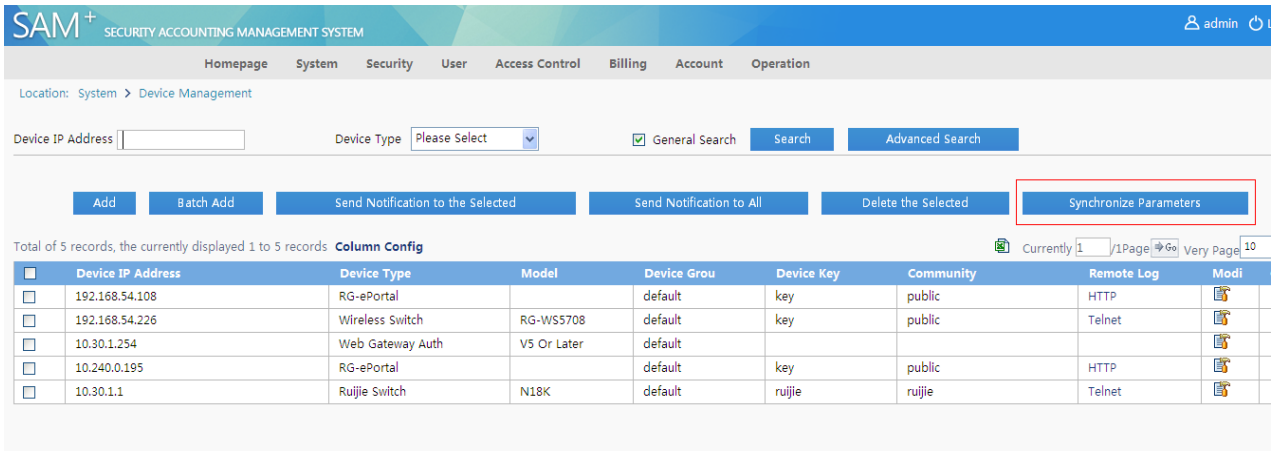
A community is a necessary key used by the RG-SAM+ system to interact with Ruijie devices. The community value should be set to the rw permission on Ruijie devices and involved functions include the function of forcing users offline, real-time SMS function, function of synchronizing online users on switches to the RG-SAM+ system, and parameter synchronization function. The preceding functions may be unavailable if a device is a non-Ruijie device, the community is set incorrectly, or the community value is not set to the rw permission. In addition, the availability of the preceding functions depends on the device type. For details, see relevant product specifications.

Note

Parameter synchronization function:

The parameter synchronization function is provided in **Device Management** so that administrators can modify device parameters on the Web management page conveniently.

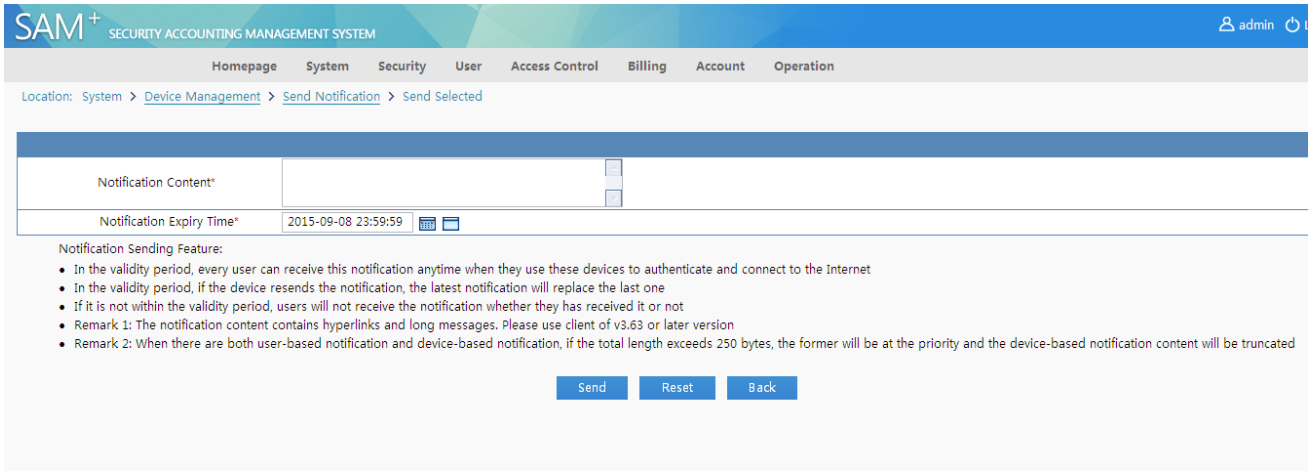
S26*XX* switches do not support key value acquisition but support the key setting. Therefore, on the management page of the RG-SAM+ system, key values on the devices are not displayed during parameter synchronization, but the key values can be correctly synchronized from the RG-SAM+ system to switches.



SM Sending Configuration

An SM can be configured for an authentication device of the RG-SAM+ system. When a user is authenticated and goes online through the device, the RG-SAM+ system sends the SM to the user. In this way, SMs are sent to desired users according to device-based scope.

The following figure shows the SM sending page.



On the preceding page, enter the content of the message to be sent in **Notification Content**. **Notification Expiry Time** indicates the expiration time of the message, and the message is sent prior to the expiration time. The two parameters are mandatory. Pay attention to the following items:

In the validity period, any user can receive this notification anytime when they are authenticated and access the Internet through these devices.

In the validity period, if a notification is resent to the device, the notification will replace the previous notification.

If the time is not within the validity period, users will not receive the notification no matter whether they have received it before.

Remark 1: If the notification content contains hyperlinks or a long message, use a client of V3.63 or a later version.

Remark 2: When there are both user-based notification and device-based notification, if the length exceeds 250 bytes, the former has a higher priority and the device-based notification displayed on the client will be truncated.

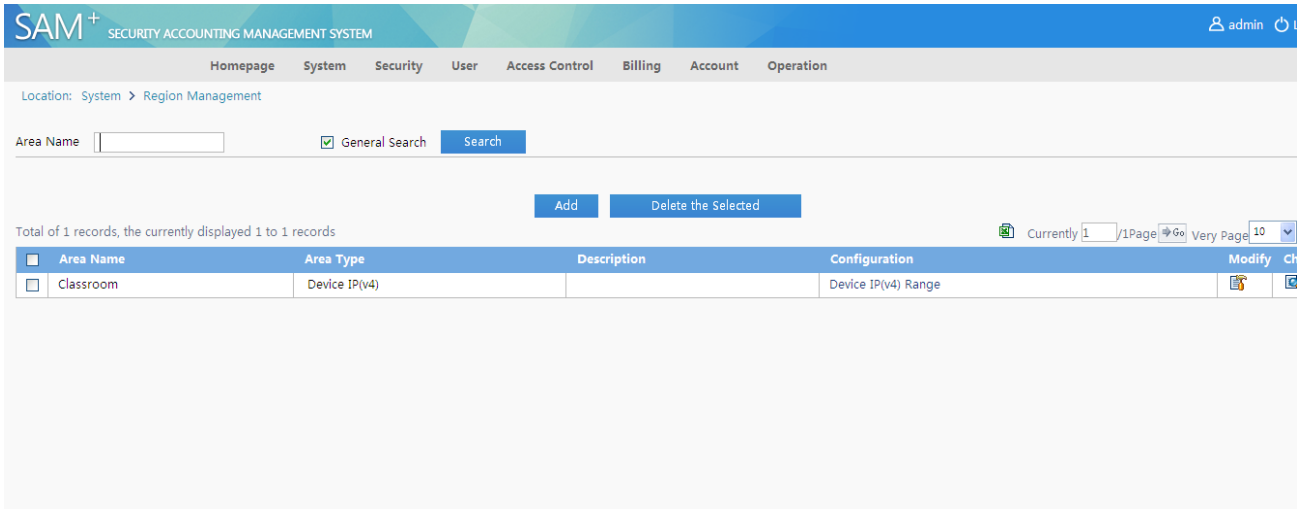
Precautions for Device Configuration

If there is a Web gateway authentication device, its time must be synchronous with the time of the RG-SAM+ system. Otherwise, a user may be forced to go offline before the available Internet access duration expires.

Region Management

One of the characteristics of the RG-SAM+ system is that abundant areas can be set and different correlation can be set by area, which facilitate network operation and management and implement more powerful functions.

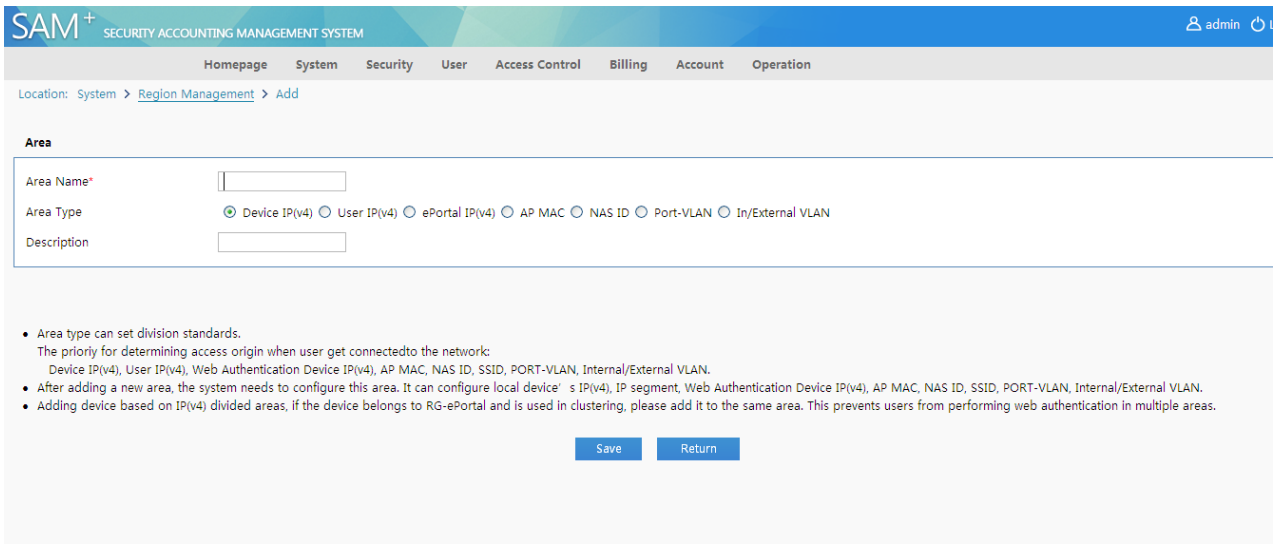
Choose **System**>**Region Management** from the main menu. The **Region Management** page is displayed, as shown in the following figure.



Areas can be classified by five types: by IP address range of access devices, by IP address range of users, by IP address range of Web authentication access devices, by AP range, and by NASID range. That is, areas are classified by the NAS IP address, IP address range, IP address of the Web authentication access device, AP MAC address, and NASID in the system.

Area Adding

Click **Add** to access the page of adding an area, as shown in the following figure.



In addition to **Area Name** and **Description**, you need to set **Area Type** when adding an area.

Area Type refers to the area classification criteria. It can be set to one of the following values on the RG-SAM+ system:

Device IP(v4): Areas are classified by the IP address range of devices.

User IP(v4): Areas are classified by the IP address segment range of users.

ePortal IP(v4): Areas are classified by the IP address range of Web access devices.

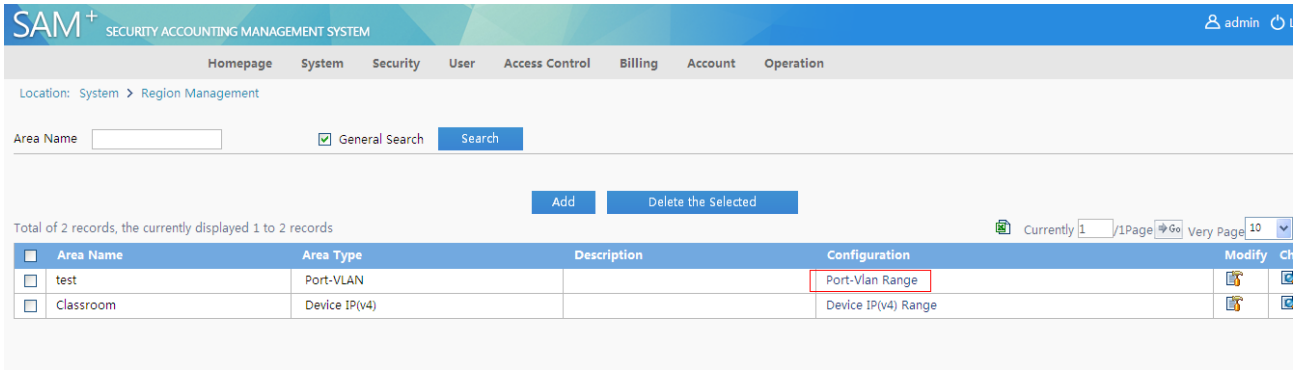
AP MAC: Areas are classified by the MAC address range of APs in the case of wireless access.

NAS ID: Areas are classified by the NAS ID range uploaded by wireless devices.

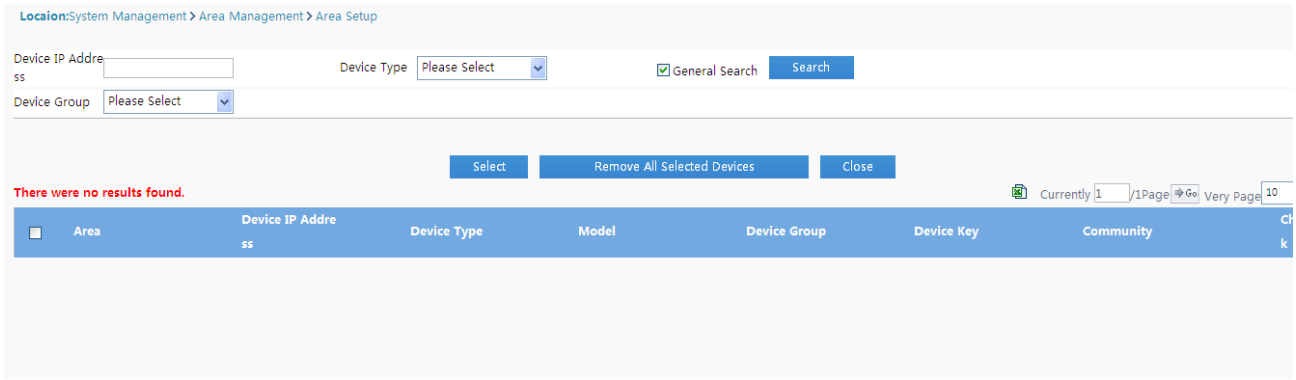
The priority for judging the area to which a user belongs is as follows: device IP address, user IP address, IP address of the Web authentication device, AP MAC address, and NAS ID. That is, information about the area to which an access user belongs is obtained in the preceding order.

Area Configuration

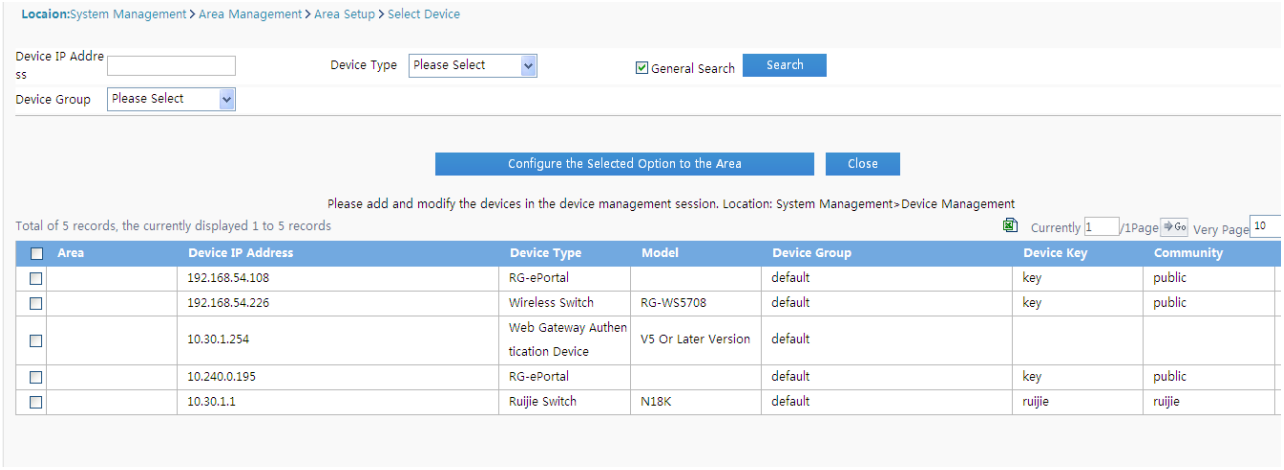
As described above, areas can be classified by device IP address, user IP address segment, IP address of the Web authentication device, and AP MAC address range. For such types of areas, relevant type elements need to be configured. The following describes how to configure the type element, beginning with areas classified by device IP address range.



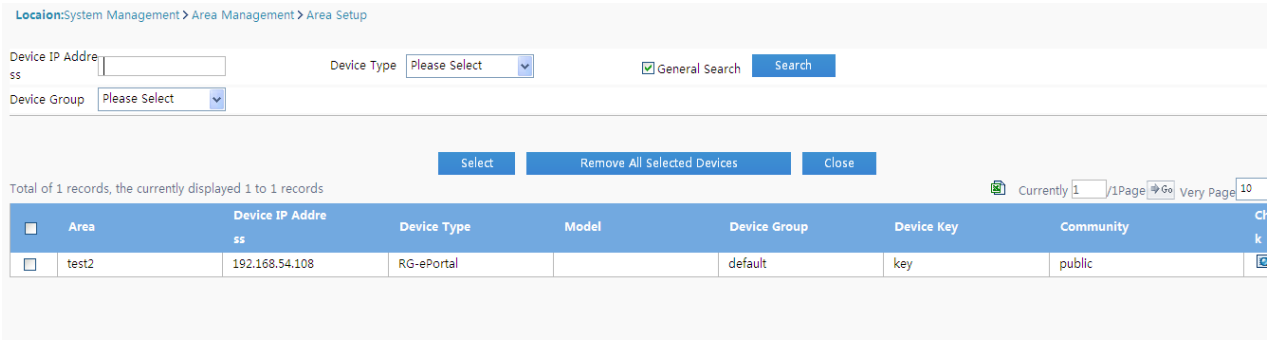
Click the configuration link of area **test** to access the configuration page. The device record of this area is blank at the first configuration, as shown in the following figure.



Click **Select**. A device list page is displayed, as shown in the following figure.



Select a device to be added to the area and click **Configure the Selected Option to the Area**. The selected device is added to area **test**, as shown in the following figure.



If, for example, a user applies for authentication from the device with IP address 192.168.54.108, the user belongs to area **test**.

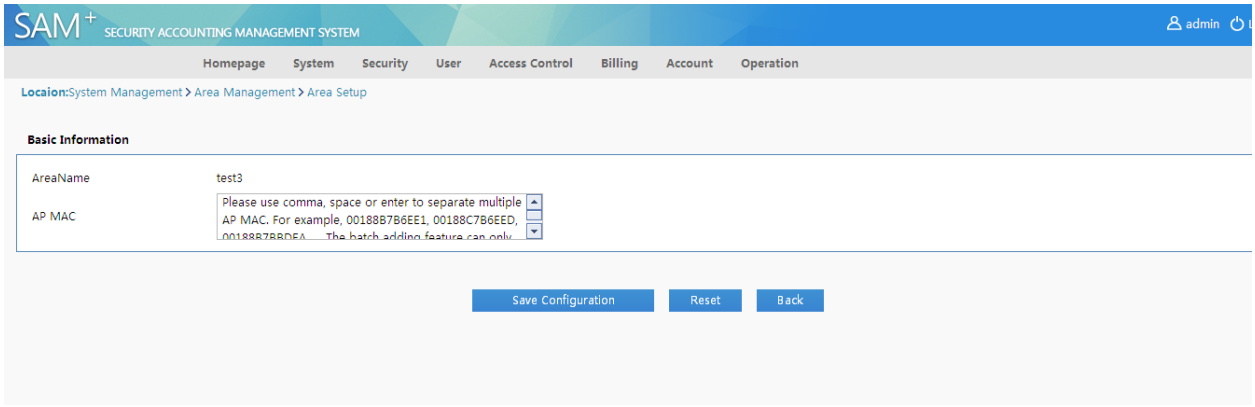
The configuration for areas classified by user IP address range is similar to that for areas classified by device IP address range. Refer to the preceding operations to complete the configuration.

The configuration for areas classified by IP address of the Web authentication access device is similar to that for areas classified by device IP address range. Refer to the preceding operations to complete the configuration.

The difference is that the device to be selected must meet the following requirement: The device type is switch, the device model is S26*XX*, and the Web authentication function is enabled on the device.

The following figure shows an area classified by AP MAC address.

Click the link of the area to access the configuration page of the area type. The device record of this area is blank at the first configuration, as shown in the following figure.

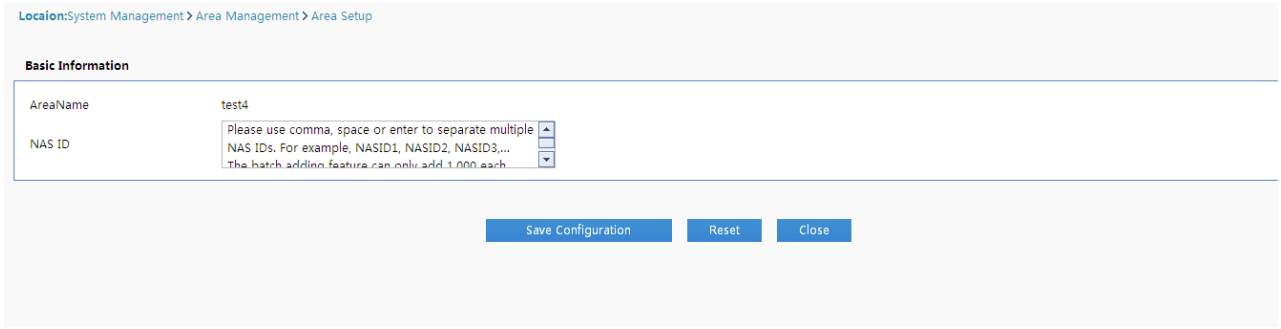


Follow the format example on the page. Click the input area, and the prompt disappears. Enter AP MAC addresses, which are separated by the **Enter** key. A maximum of 500 entries can be added. See the following figure.

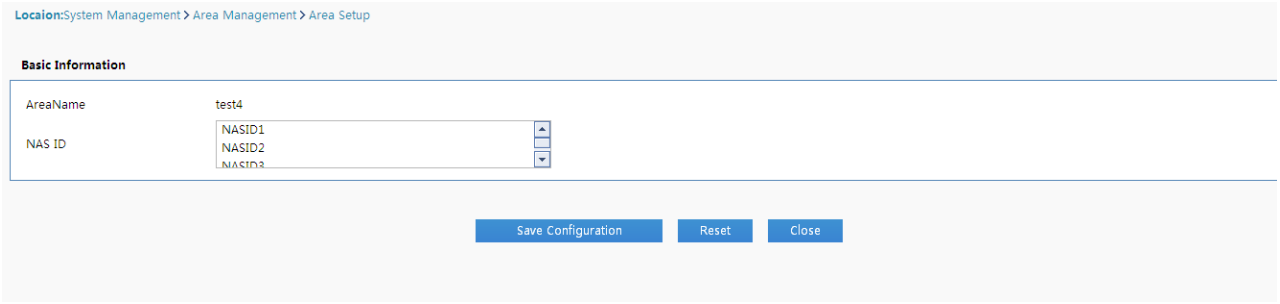
Click **Save Configuration** to finish configuring the AP MAC addresses for area **test3**.

The following figure shows an area classified by NAS ID range.

Click the link of the area to access the configuration page of the area type. The device record of this area is blank at the first configuration, as shown in the following figure.



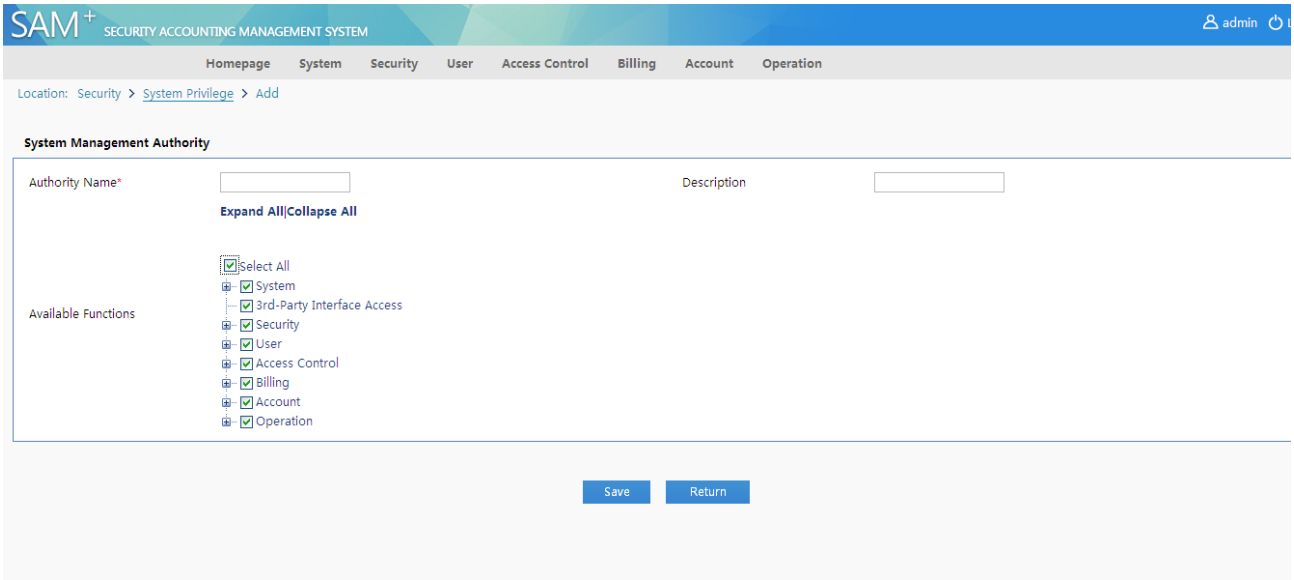
Follow the format example on the page. Click the input area, and the prompt disappears. Enter NAS IDs, which are separated by the **Enter** key. A maximum of 1000 entries can be added. See the following figure.



Click **Save Configuration** to finish configuring area **test4**.

System Management Privileges

System management privileges refer to management privileges that are set for functions of the RG-SAM+ Web management system. At first, there is only one administrator named **admin** on the RG-SAM+ system. Administrators of different properties must be set to facilitate service management. Functions that can be managed or used by administrators are set by their associated system management privileges. Currently, the system management privileges of the RG-SAM+ system can be accurate or controlled to every original function point, for example, the RG-SAM+ system can determine whether a user can add users or can only view users. The system management privilege page is designed with a tree structure for the ease of operations, as shown in the following figure.



As shown in the preceding figure, administrators can control every function point. Click the cross in front of each function module and then select detailed function points. The operations are simple and are not described here.

By default, the RG-SAM+ system provides several system management privilege templates, with the names and functions described as follows:

Cashier: has the fee operation privileges.

Network administrator: has all privileges except security, billing, and accounting.

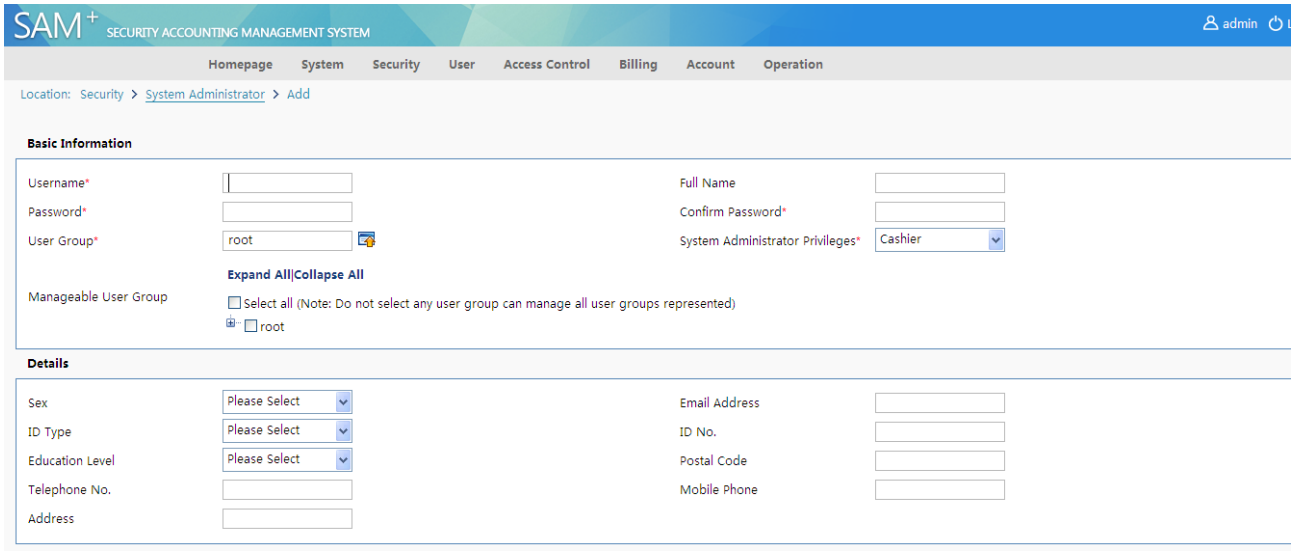
System administrator: has all privileges except security management.

User administrator: has the privilege of conducting basic management on users and user accounts.

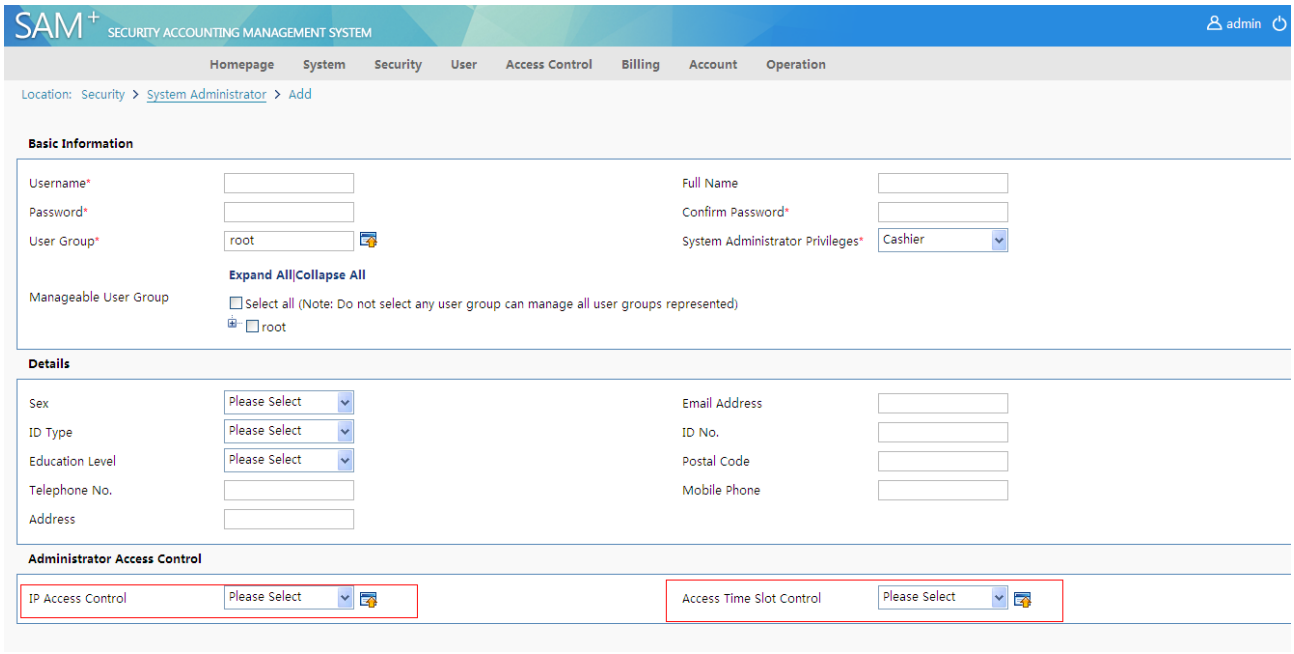
Accounting administrator: has the accounting management privileges.

The preceding names and associated privileges are only templates provided by the system. You can modify the names and privileges, add templates, or delete templates and create new ones, which will not hurt the system.

System management privileges can be added when a system administrator or customized administrator is added or modified, as shown in the following figure. System management privileges are indispensable for system administrators.



The access of system administrators can be limited by IP address and time range.



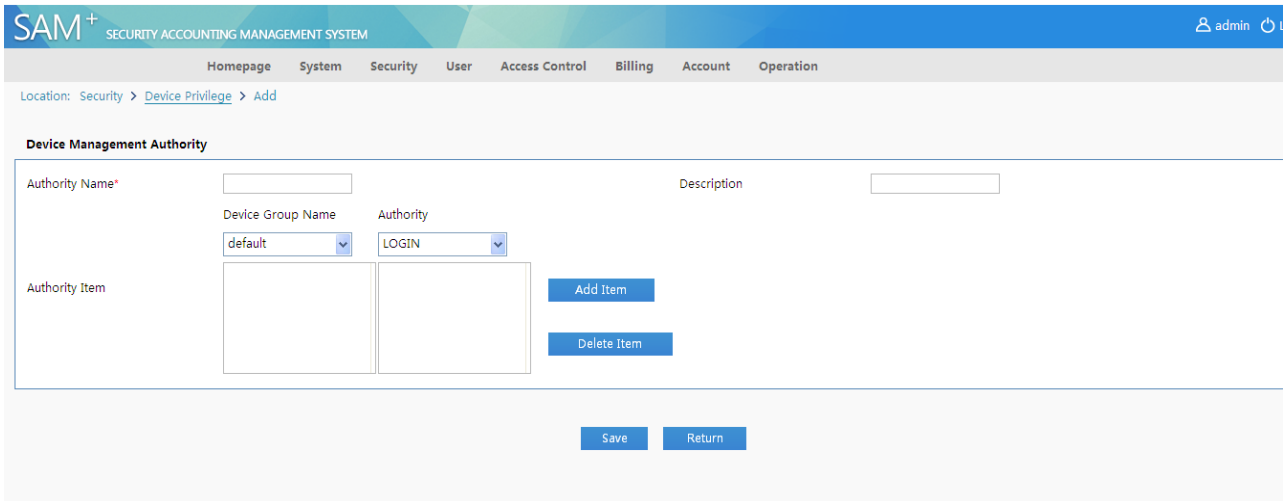
Device Management Privileges

Device management privileges are used to control device management in the following aspects:

Devices that can be managed by an administrator

Privilege settings for login device on the switch

Devices that can be managed are classified by device group. The privilege setting on the switch is to grant privileges to each manageable device on the basis of device groups. The two points compose the virtual concept set of device management privileges, which is also called a policy set.



The preceding figure shows the page of privilege configuration. Two key attributes are **Device Group Name** and **Authority**. By configuring the mapping between device group names and authorities on the page, you can add the device set that can be managed by an administrator and set different privileges for the administrator. Currently, the privileges include the following types: LOGIN, NAS_PROMPT, ADMINISTRATIVE, and authorities 1-15. For the meanings of LOGIN, NAS_PROMPT, and ADMINISTRATIVE, refer to the RADIUS protocol. In general, ADMINISTRATIVE or authority 15 (highest authority) are selected, depending on the switch privilege configuration. You can complete the configuration by referring to the configuration guide.

Note: Authority 1 of the lowest level is adopted if no authority is selected.

Administrators need to enable the function with switches [the following takes the S21*XX* series switch as an example. Refer to corresponding description for other types of switches].

```
221#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
221(config)#line vty
221(config-line)#login authentication radius
221(config-line)#end
221#write memory
Building configuration...
[OK]
221#_
```

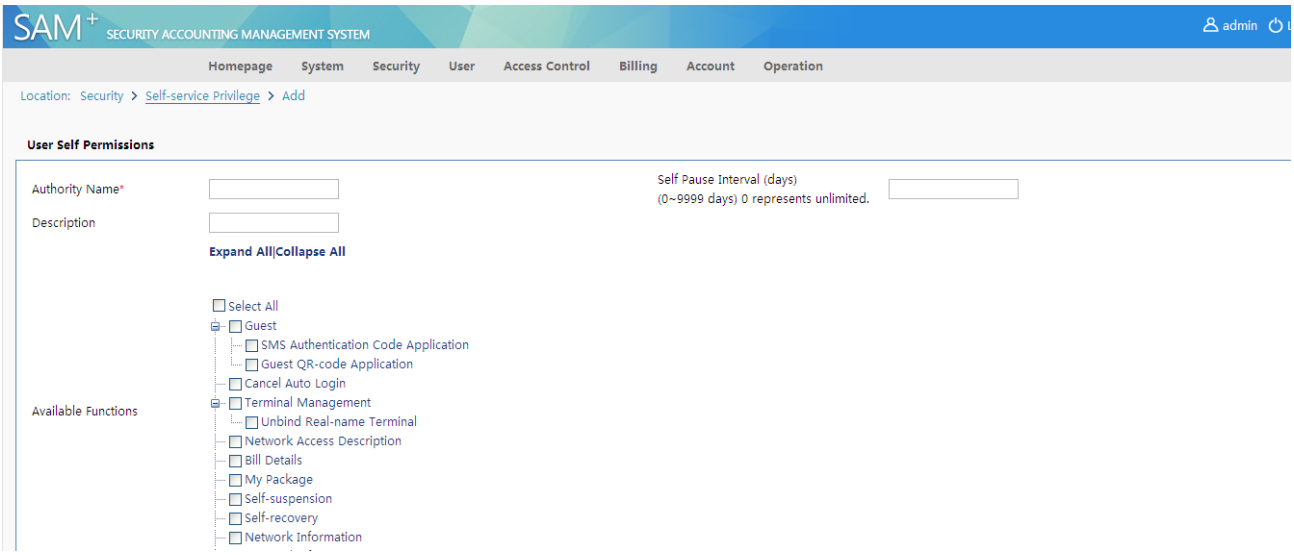
To cancel the login mode, do as follows.

```
221#con
Enter configuration commands, one per line.  End with CNTL/Z.
221(config)#line vty
221(config-line)#no login authentication
221(config-line)#end
221#write memory
Building configuration...
[OK]
```

Note: You can run the **show privilege** command in privilege mode to view administrator privileges.

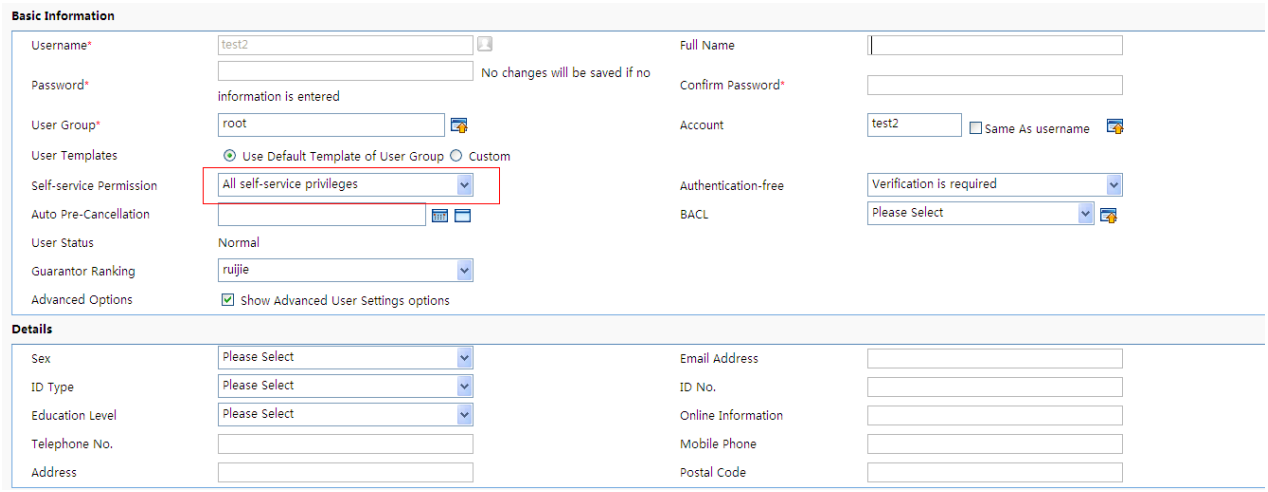
Self-Service Privileges

Self-service privileges are function privileges available to users who log in to the self-service system.



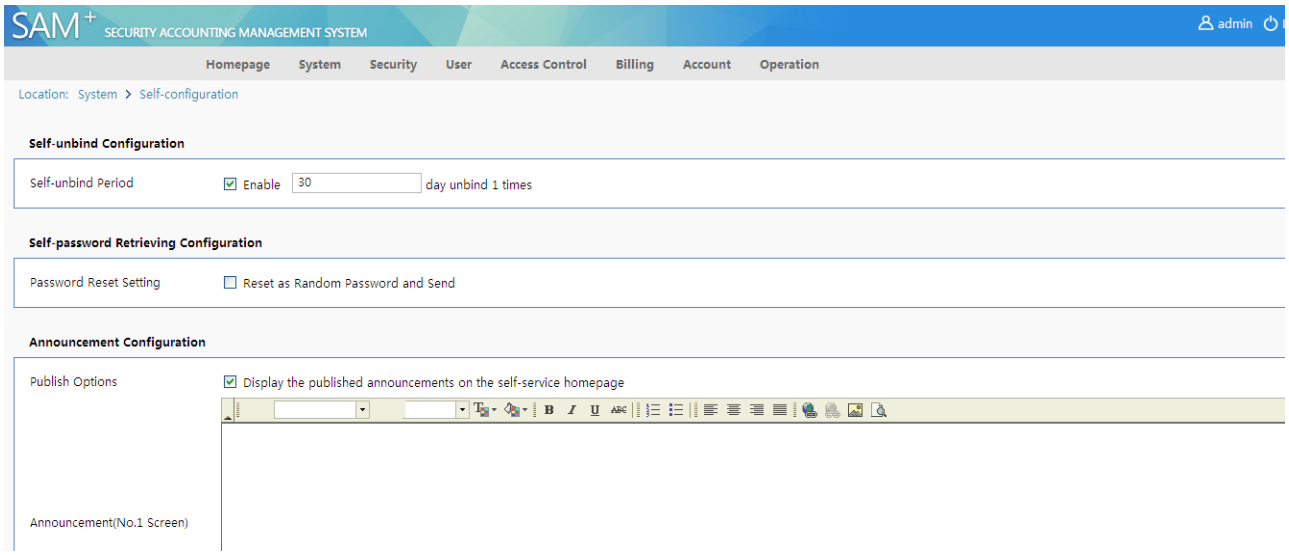
User self-service privileges are applicable to users who log in to the self-service system with real names. Currently, the self-service privileges can be used to control a single independent user, that is, different users can perform different operations (use different functions) on the self-service system according to the self-service privileges granted to them. Particularly, you can set the self-service pause interval to prevent users from using the self-service pause function infinitely, causing management inconvenience.

The RG-SAM+ system provides a default template named **All self-service privileges**, which is a reserved privilege and cannot be deleted or renamed. You can configure user self-service privileges in the adding or modification operation. The default privilege is **All self-service privileges**. See the following figure.



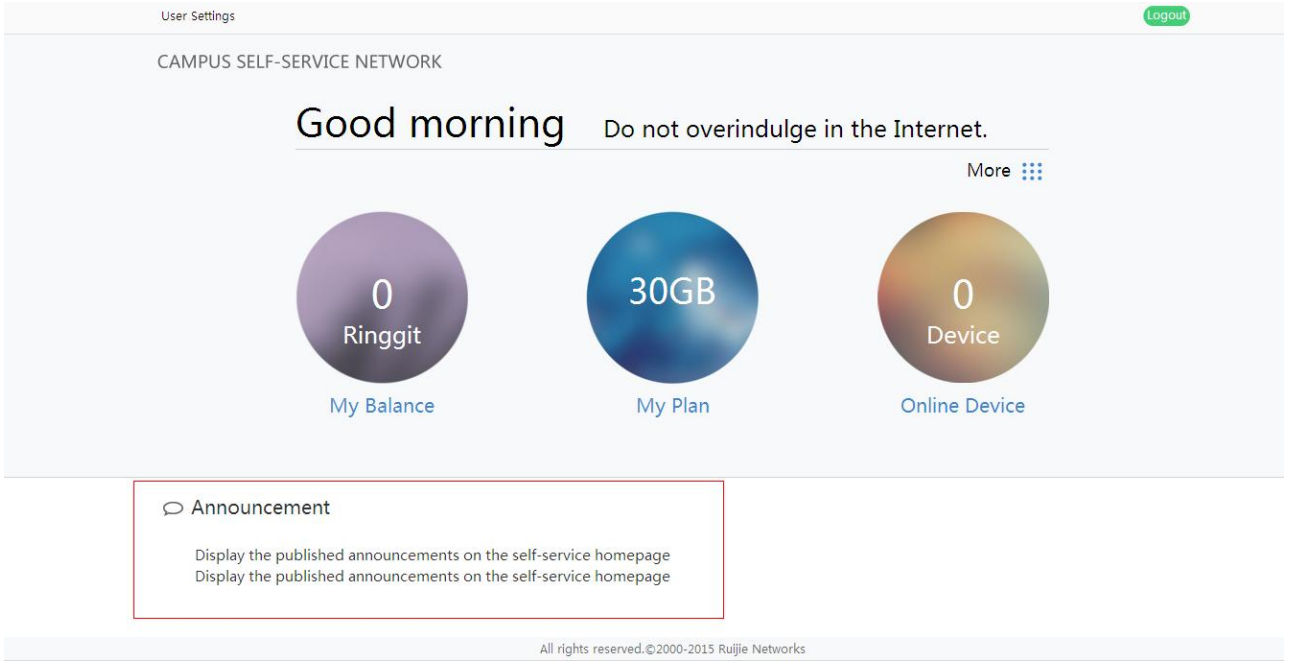
Publishing of Self-Service Page Information

Choose **System**>**Self-configuration** from the main menu, and configure information to be displayed on the login page of the self-service system of the RG-SAM+ system, as shown in the following figure. The information is used to publish notifications and messages.

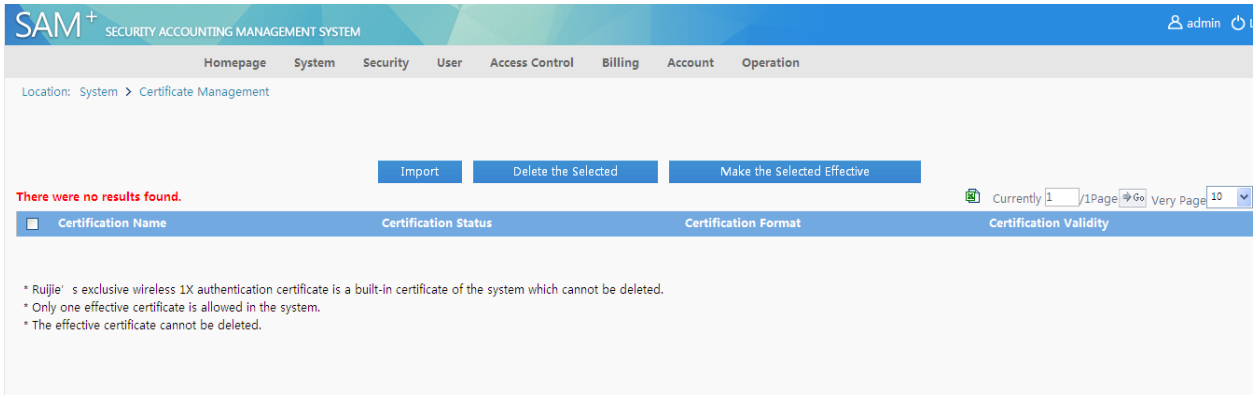


Select **Display the published announcements on the self-service homepage** to enable this function. Enter the information to be published in **Announcement**. You can set the font, font size, and color for information to be published, and add pictures and hyperlinks to customize picture- and text-contained information to be published on the self-service system.

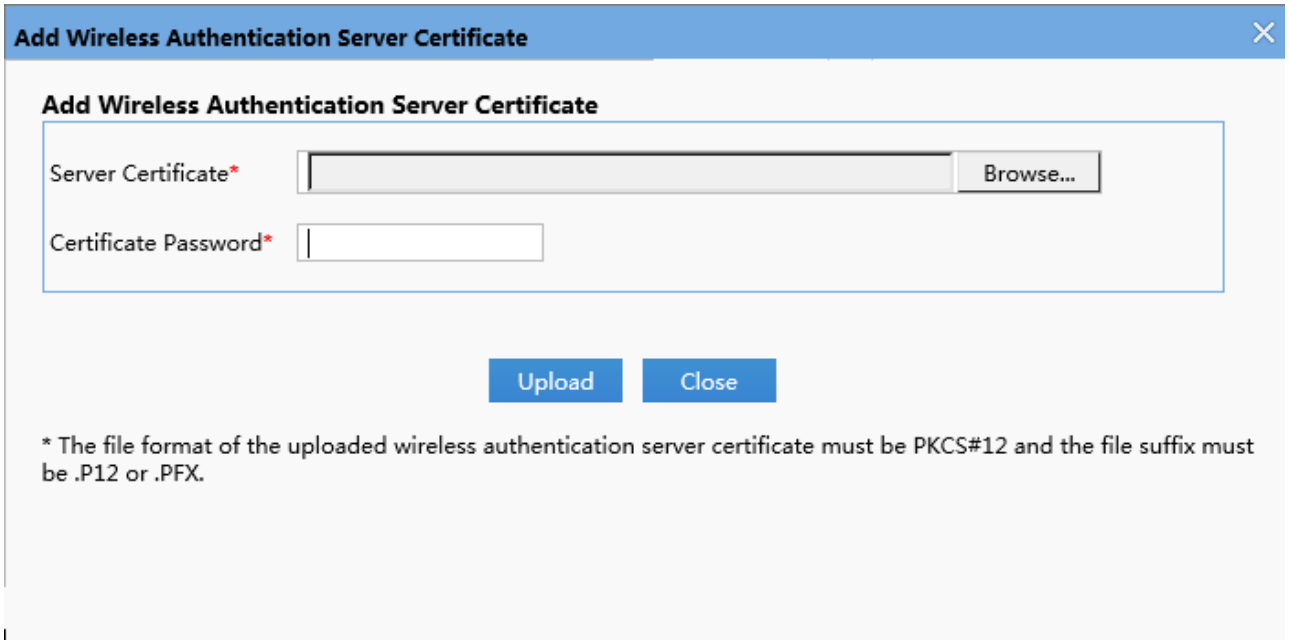
After information is configured on the management page, the display at the self-service system is shown in the following figure.



Certificate Management



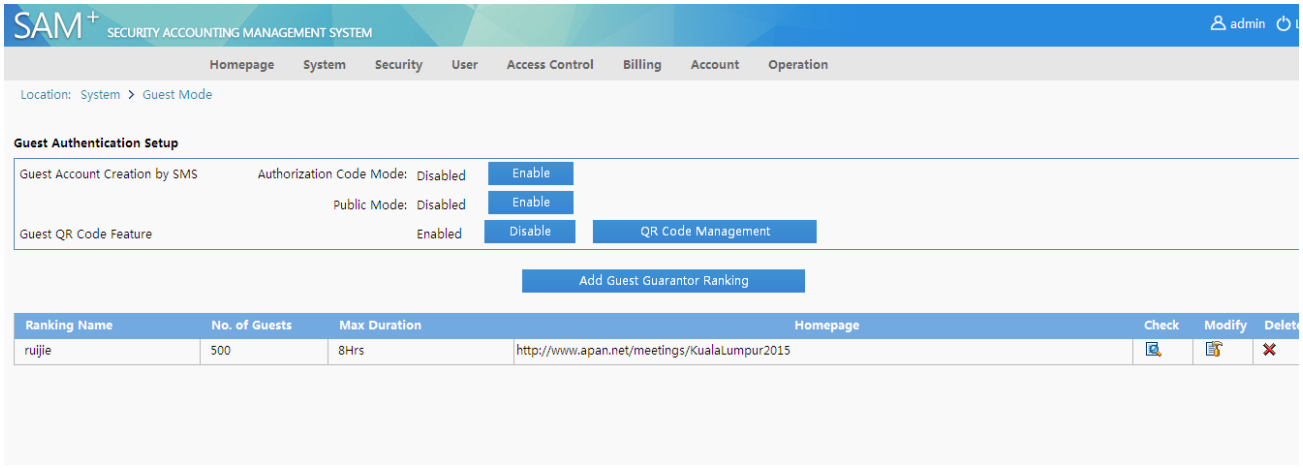
Only certificates suffixed with .p12 or pfx can be imported.



Guest Mode

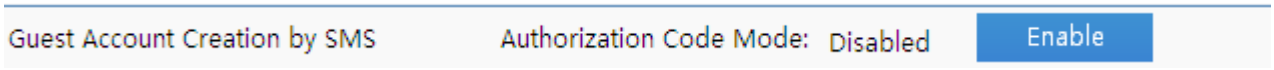
The guest mode management is used to configure the Internet access process for guests. Specifically, it provides the functions of enabling or disabling the SMS authorization code function on the self-service page, enabling or disabling the authorization QR code on the self-service page, activating the pubic QR code, and managing the guarantor ranking.

Choose **System**>**Guest Mode** from the main menu. A page as shown in the following figure is displayed.



1) Enable or disable the SMS authorization code function.

a. Enable the SMS authorization code function.



Disabled indicates that the SMS authorization code function is unavailable on the self-service page.

The SMS authorization code function is available on the self-service page after **Enable** is clicked.

b. Disable the SMS authorization code function.

Enabled indicates that the SMS authorization code function is available at the self-service end.

The SMS authorization code function is unavailable at the self-service end after **Disable** is clicked.

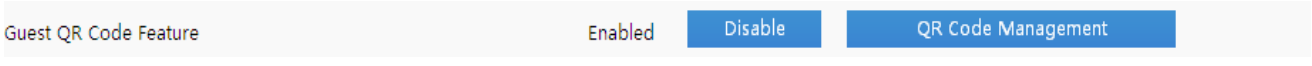
2) Enable or disable Guest QR Code Feature.

a. Enable Guest QR Code Feature.

Disabled indicates that the authorization QR code function is unavailable at the self-service end and the public QR code function is unavailable at the service end.

The authorization QR code function is available at the self-service end and the public QR code function is unavailable at the service end after Enable is clicked.

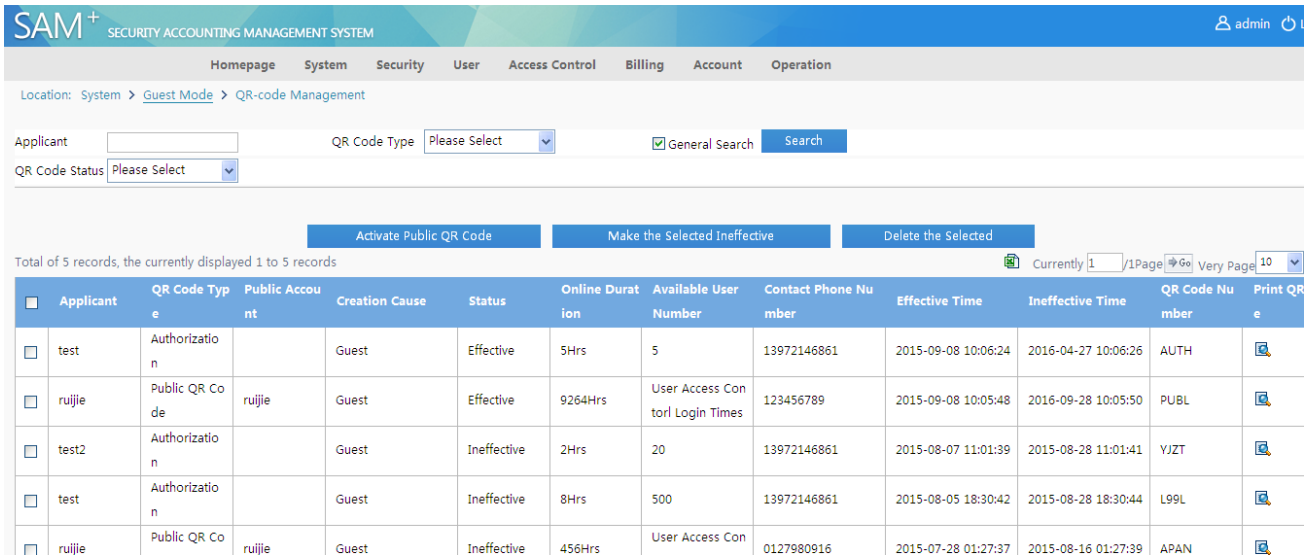
b. Disable Guest QR Code Feature and activate Public QR Code.



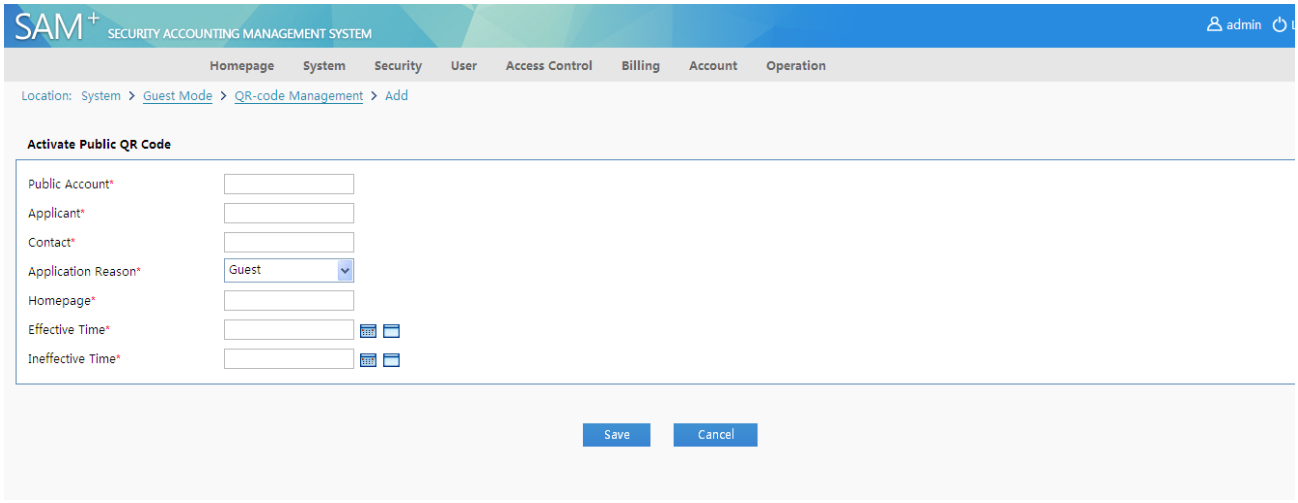
Enabled indicates that the authorization QR code function is available on the self-service page and the public QR code can be activated on the service page.

The authorization QR code function is unavailable on the self-service page and the public QR code cannot be activated on the service page after Disable is clicked.

After QR Code Management is clicked, the RG-SAM+ system lists activated public QR codes, as shown in the following figure.



By clicking Activate Public QR Code, an administrator can access the page to enter information for activating a public QR code.

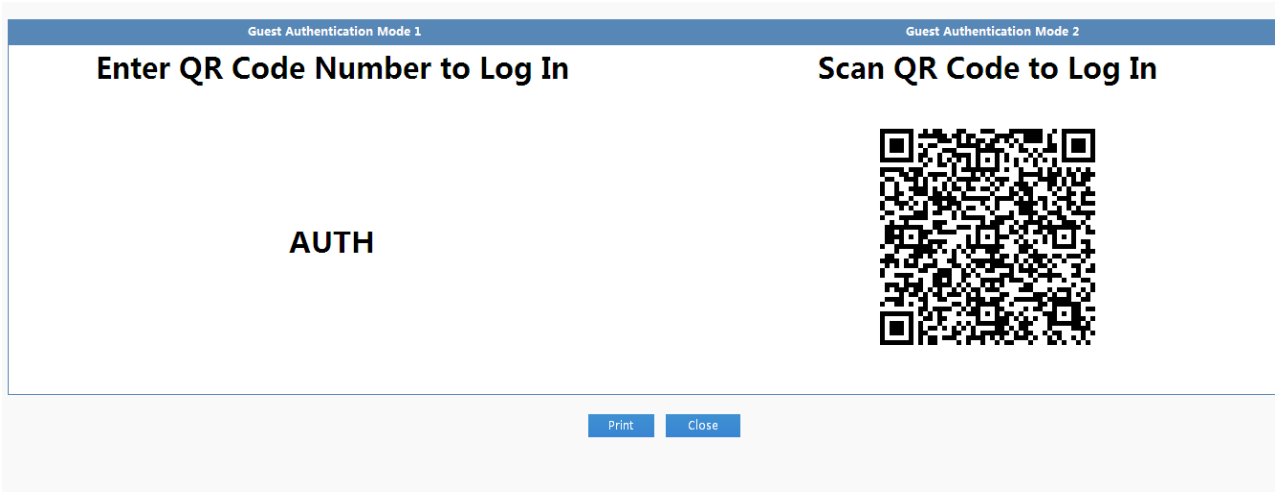


After entering information, the administrators should click Save to activate the public QR code.

Notes: Public Account: Enter an account with the guarantor privilege. Applicant: Enter an account with the guarantor privilege. Homepage: homepage displayed after a guest logs in to the system with QR code.

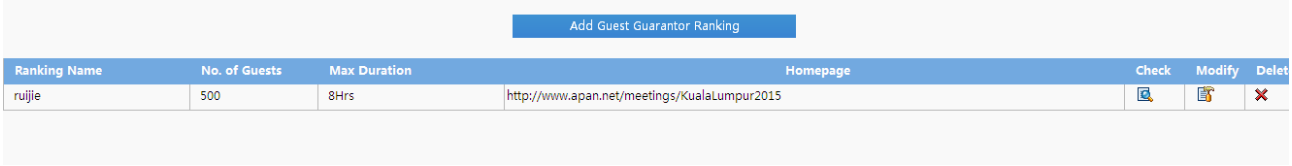
You can change the status of a public QR code by clicking the Activate Public QR Code or Make the Selected Ineffective button. A public QR code can be in the Not Effective, Effective, or Ineffective state, and the state is irreversible.

You can print QR code information in this line by clicking Printing QR Code.

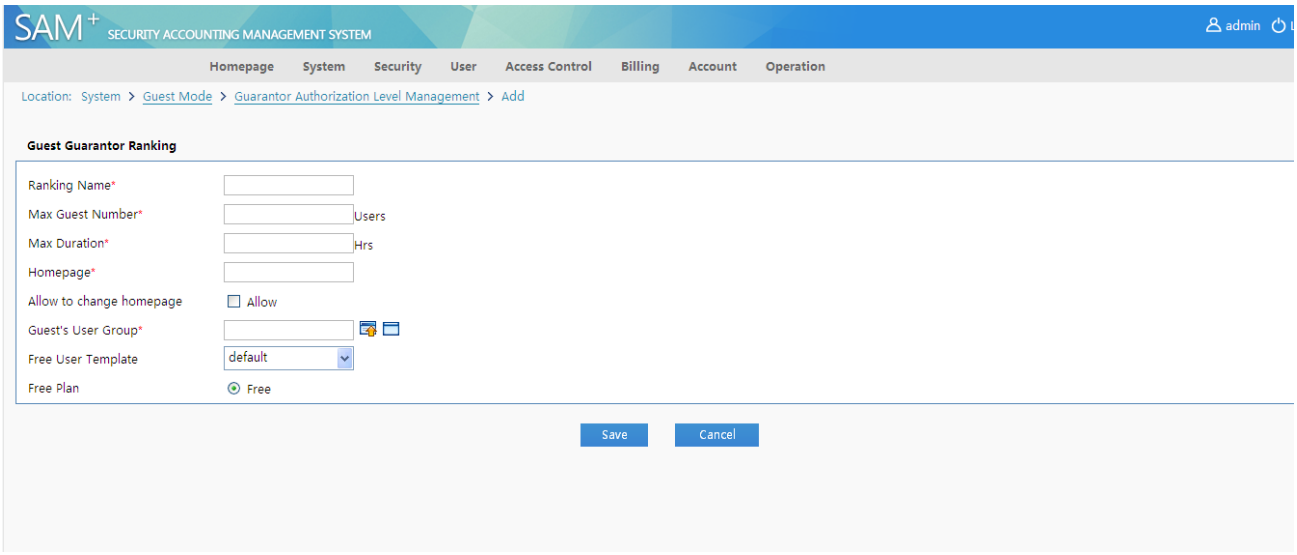


3) Guarantor ranking management

Guarantor ranking management allows administrators to add, view, change, and delete a guarantor ranking.



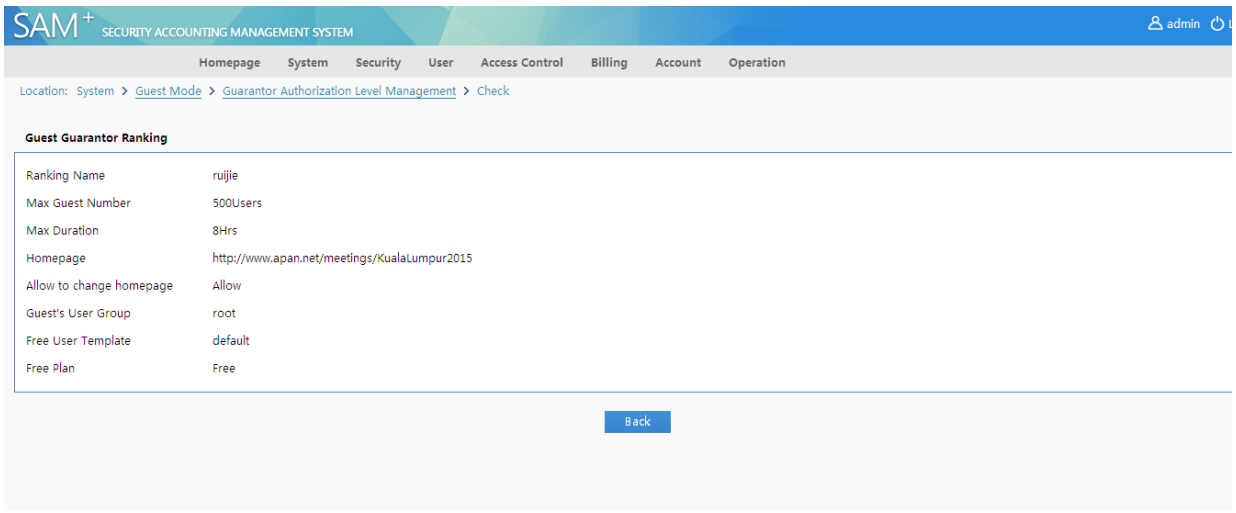
Add Guest Guarantor Ranking: Set **Ranking Name**, **Max Guest Number**, **Max Duration**, **Homepage**, **Allow to change homepage**, **Free User Template**, and other parameters to add a ranking, as shown in the following figure.



Configuration description:

1) **Max Guest Number** defines the upper limit on the number of guests when the guarantor of a ranking activates the SMS authorization code or authorization QR code on the self-service page.
2) **Max Duration** defines the upper limit on the Internet access duration of guests when the guarantor of a ranking activates the SMS authorization code or authorization QR code on the self-service page.
3) **Homepage** defines the page displayed on the browser after a guest passes authentication.
4) **Allow to change homepage** determines whether a guarantor is allowed to define the page displayed upon successful guest authentication when the guarantor activates an authorization QR code on the self-service page.
5) For **Free User Template**, you can choose **User Management**>**User Template Management**>**User Templates** to configure a free user template. Currently, temporary guest accounts support only free packages in the system.

Viewing guest guarantor rankings: You can view details about the guarantor ranking. The following figure shows information about a guarantor of ranking 11.



Changing a guest guarantor ranking: You can modify information about the guarantor ranking. For details, see the section of adding a guest guarantor ranking.

Deleting a guest guarantor ranking: You can delete configuration about a guarantor ranking.

Access Control

Access Control is a centralized control platform provided by the RG-SAM+ system to allow customers and end users to use all the services and functions. In an 802.1X-compliant system, a dial-up client must pass the authentication of the access device and verification of the authentication server before accessing the Internet. The network access privilege is granted by the authentication server. This process of authentication and authorization is embodied in RG-SAM+ access control.

Limiting Duplicate Logins

Duplicate Login refers that a user is allowed to have multiple online records at the same time.

This function is becoming more and more prevalent in the Internet. Similar to the family-based telecommunication billing mode, multiple clients in one family are allowed to access the Internet simultaneously. Different from that, Ruijie Networks' duplicate login function poses stricter authentication requirements, that is, multi-login clients must use the same correct username and password for successful authentication.

For multi-login clients by using the same username, all of them share the access permission, billing policy, and account balance as one. That is, all the clients are subject to the same configuration of authentication and billing, and have the same access permissions. In conclusion, multi-login clients have the following characteristics:

The access permissions are the same.

On the **User Management** page, the access permission of a user can be configured by choosing a user template set with access permissions. To apply different access controls to multi-login clients, enter "*username@access control name*" on each client on the login page. Those clients enjoy the equal rights of using different access controls.

The adopted billing policy is the same.

On the **User Management** page, the billing mode of a user can be configured by choosing a user template set with billing policies. Those clients enjoy the same associated billing policy.

Duplicated logins are all billed.

For the real-time billing policies (such as Duration Billing Policy), billing is conducted on each accessed client and fees are deducted from the account balance.

For the periodic billing policies (such as Monthly Billing Policy), billing starts automatically when a new billing cycle starts. The rule is user-based. Therefore, duplicate logins will be ignored and the user is billed with cyclic charge.

If not associated with any billing policy, the user will not be billed.

For details about the billing policies and billing rules, see the section "Billing Management."

Duplicate logins are all recorded.

For multi-login clients, the RG-SAM+ system records their online details like network access and account status (in the case of billing).

Duplicate logins are all controlled.

The information of multi-login clients is listed in the online user table, including IP addresses, MAC addresses, access control policies, and so on. The usernames they use are the same. You can monitor them, send SMSs to them, or force them offline. For details, see "Online User Management."

Note

Difference from Proxy Login

The greatest difference is that the billing, access control verification, and access permissions are independently controlled for each multi-login user. Nevertheless, users who connect to a proxy to access the Internet are charged with only one bill, and are out of control of the RG-SAM+ system, causing capital and security risks. Therefore, the proxy mode must be eradicated. In addition to providing duplicate logins, the RG-SAM+ system prevents Internet access in proxy mode. For details, see "Proxy Agent Prohibition."

Note

Configuration Description

Duplicate logins are supported on each access control for the maximum number configured. If the limit on duplicate logins is not configured in a plan, it will be determined by the allowed duplicate logins set in access control. If configured, the duplicate logins cannot exceed both settings in access control and the user template.

In wireless Web portal access mode, it is recommended to set the number of duplicated logins to 1 unless it is necessary to configure it (for example, multiple users need to use the same account in the test or conference environment).

If billing is required for dial-up VPN users, set the number of duplicate logins to 1.

Difference of Duplicate Login Limit Set in Plans and in Access Control

Duplicate Login Limit in Access Control (A) is used to limit the duplicate logins for one service of a plan.

Duplicate Login Limit in Plans (B) on **User Template** is used to limit the duplicate logins for a plan.

1) If B is not enabled, A will take effect.
2) If B is enabled and configured: When B < A, B will limit the duplicate login. When B > A, A will limit the duplicate login.

Gateway Configuration

If **It does not allow traffic through the gateway server** is selected in **Gateway Access Restriction**, the traffic of users who access the Internet by using this access control cannot go through the gateway. The prerequisite for the configuration to take effect is that the gateway should be deployed in transparent mode.

If an application control engine (ACE) is deployed and the admission and exit authentication scheme is adopted, **Gateway Strategy** must be set to the same as that for the ACE. For example, if the gateway strategy for an ACE is **deny** which stops user traffic to go through the gateway, the access control with the same gateway strategy will conduct

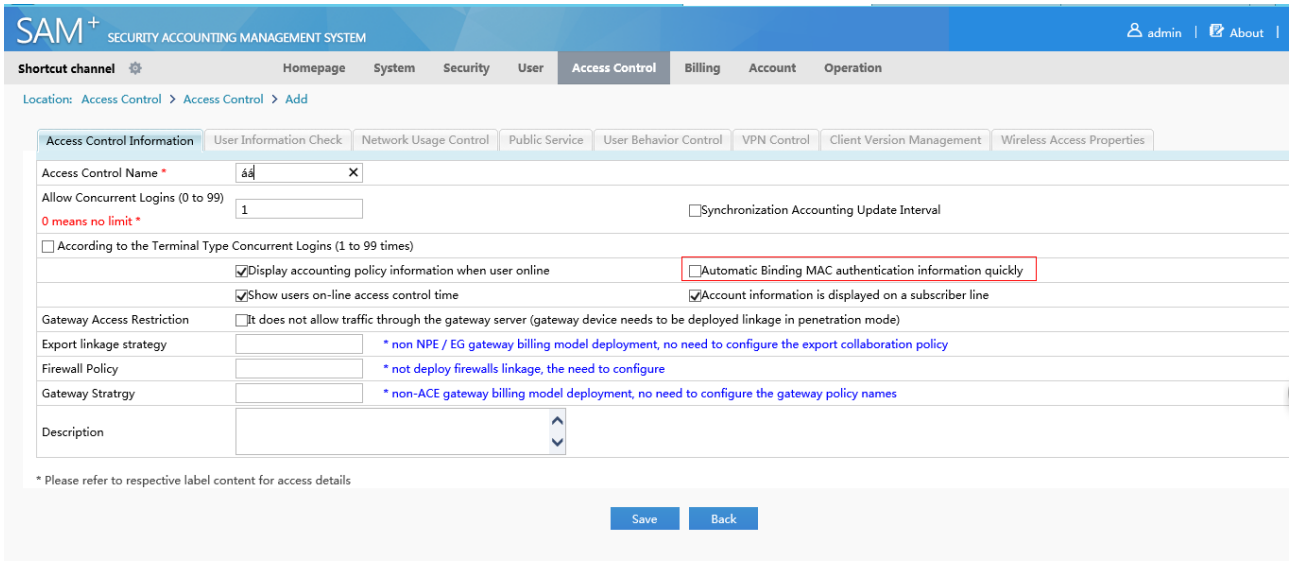
the same behavior. If **Gateway Strategy** is set, do not forget to enable **It does not allow traffic through the gateway server**.

The RG-SAM+ system implements an interconnection to ACE 5.0 to support the maximum available traffic control and threshold notification.

Quick MAC Authentication

Quick MAC Authentication allows users to access the Internet without username and password verification. MAC addresses can be bound in automatic mode and manual mode.

To start the automatic mode, choose **Access Control**>**Access Control**>**Modify** on the RG-SAM+ management platform, and select **Automatic Binding MAC authentication information quickly**, as shown in the following figure. If **Automatic Binding MAC authentication information quickly** is deselected, the manual mode is started.



Access Time Range Limit

Access Time Range refers to the time period in which users can access the Internet in dial-up mode.

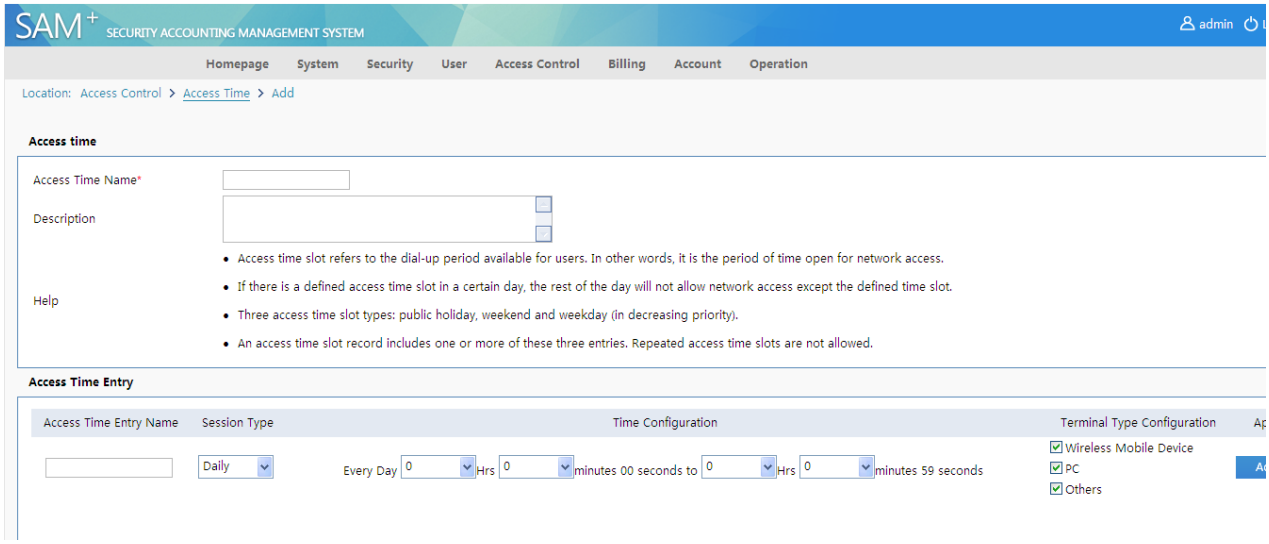
If an access time range is defined for a certain day, access is not allowed out of the access time range.

Notes: 1. If the login time of a user is not within the access time range, the user is not allowed to access the Internet in dial-up mode.

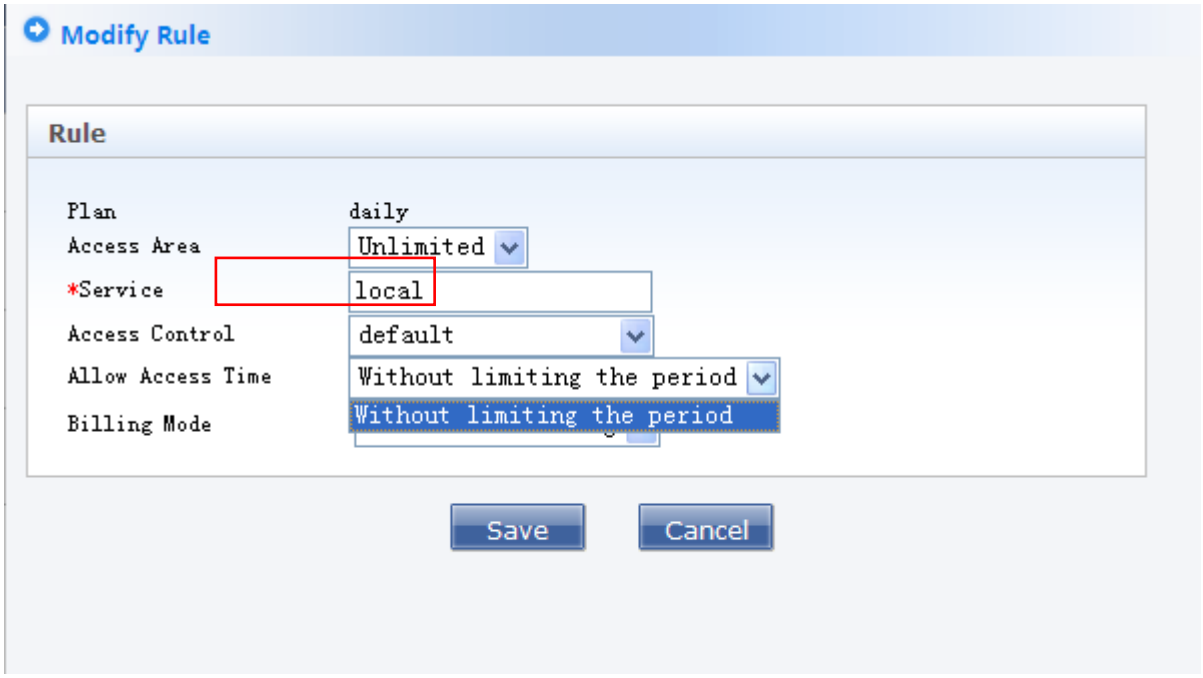
2. If no access time range is set for a user, the user is allowed to access the Internet in dial-up at any time.

Access Time Range is classified into Daily, Weekend, and Holiday with ascending priorities.

One access time range may contain one or more entries of these types. However, the range entries of the same type cannot have overlapped periods.



If an access time range is specified in a plan rule, any user in this plan must obey the time settings. After dial-up, the login time of one of the users will be checked whether within the access time range. If not, a message is prompted on the client.



User Information Check

User access information should be checked to admit only the users authenticated by the allowed channels. The user information check function helps make the following judgments:

User IP(v4): When a client works in an IPv4 environment, a user can go online only through the IPv4 address to which it is bound.

User IP(v6): When a client works in an IPv6 environment, a user can go online only through the IPv6 address to which it is bound.

Access IP Type: Dynamic/Static.

User MAC: When the MAC address of a user is bound, the user can go online only through the MAC address.

NAS IP(v4): When an NAS uses an IPv4 address, a user can go online only after accessing the NAS IPv4 address to which it is bound.

NAS IP(v6): When an NAS uses an IPv6 address, a user can go online only after accessing the NAS IPv6 address to which it is bound.

NAS Port: A user can go online only after accessing the NAS port to which it is bound.

AP MAC: A user can go online only through an AP using the AP MAC address (applicable only to the wireless mode) to which it is bound.

SSID: If the SSID of a user is bound, the user can go online only through the network service using the SSID (applicable only to the wireless mode) to which it is bound.

Web Authentication Device IP(v4): A user can go online only through the IP address of the Web authentication access device (applicable only to the ePortal scheme) to which it is bound.

Web Authentication Device Port: A user can go online only through the port of the Web authentication access device (applicable only to the ePortal scheme) to which it is bound.

The following lists elements that can be bound in different access modes:

Wired 802.1X access: **User IP(v4)**, **User IP(v6)**, **User MAC**, **NAS IP(v4)**, **NAS IP(v6)**, **NAS Port**, and **Access IP Type**

ePortal access: **User IP(v4)**, **User MAC**, **Web Authentication Device IP(v4)**, and **Web Authentication Device Port**

Wireless 802.1X access: **User IP(v4)**, **User MAC**, **NAS IP(v4)**, **AP MAC**, **SSID**, and **Access IP Type**

Wireless Web portal access: **User MAC**, **NAS IP(v4)**, **AP MAC**, and **SSID**

VPN dial-up access: **User IP(v4)** and **NAS IP(v4)**

Web pure Internet access: **User IP(v4)**

Smart device 802.1X access: **User MAC**, **NAS IP(v4)**, **AP MAC**, and **SSID**

Wired standard portal access: **User IP(v4)**, **User MAC**, **NAS IP(v4)**, and **NAS Port**

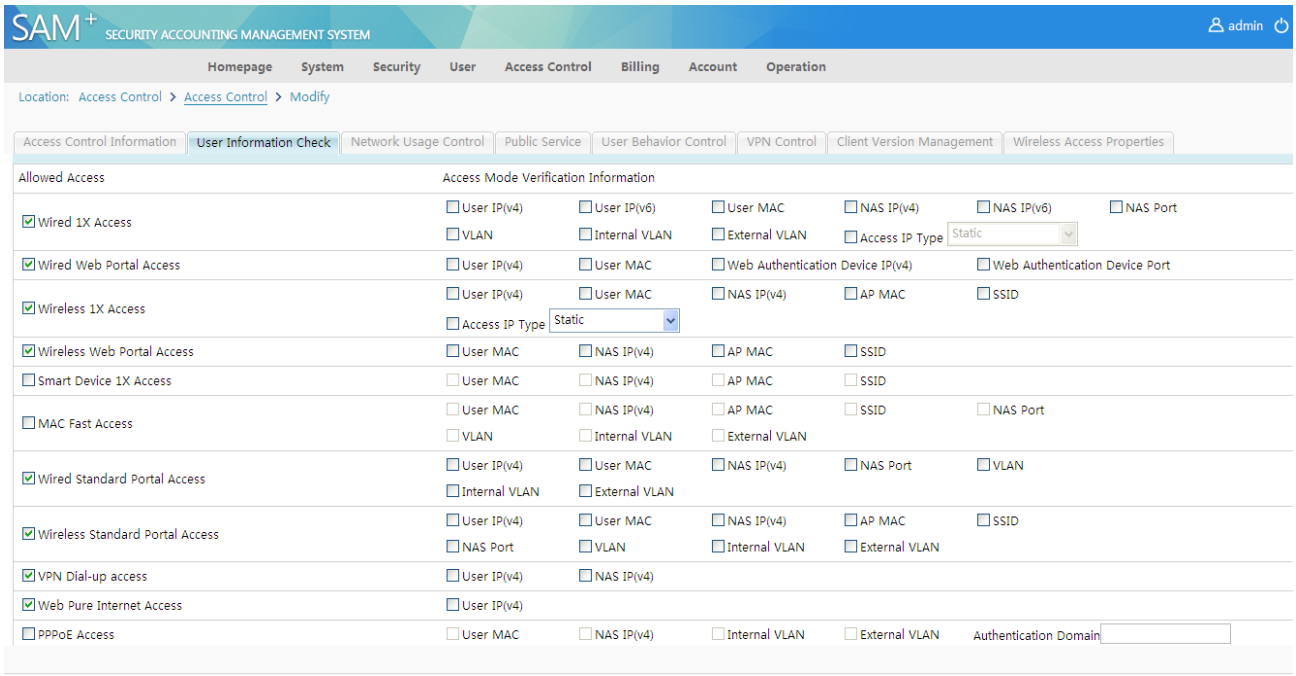
Wireless standard portal access: **User IP(v4)**, **User MAC**, **NAS IP(v4)**, **AP MAC**, and **SSID**

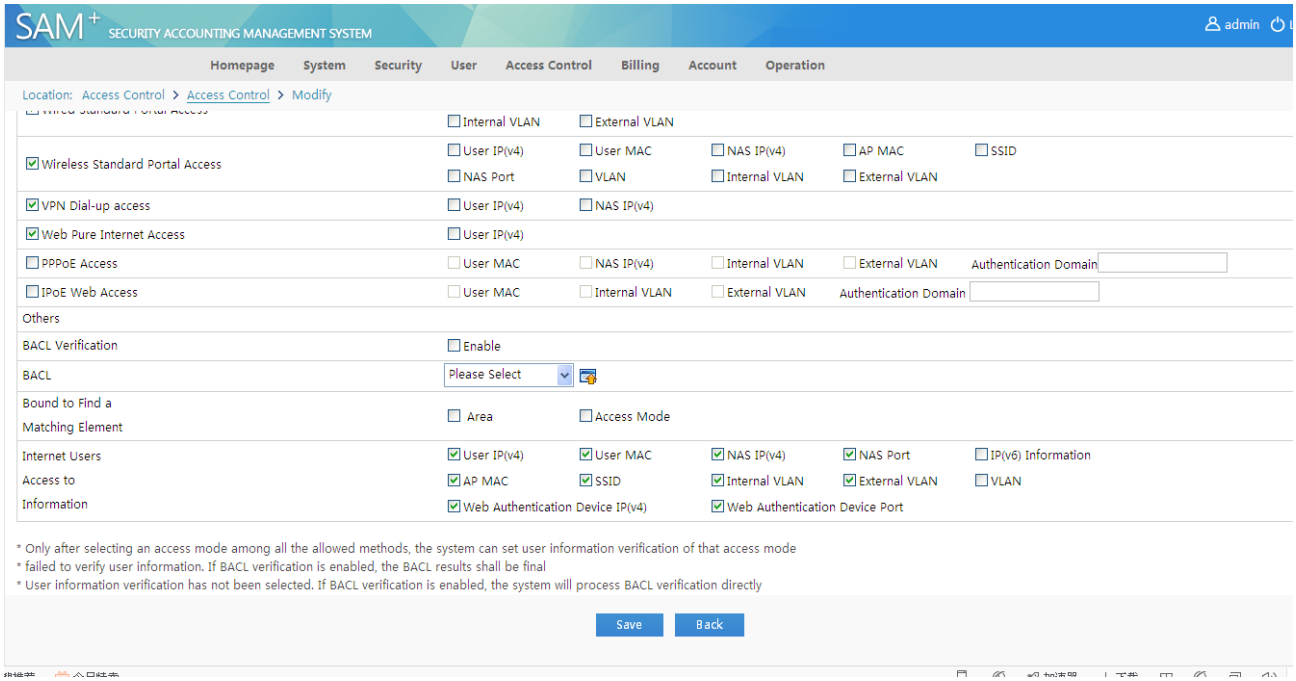
MAC fast access: **User MAC**, **NAS IP(v4)**, **AP MAC**, and **SSID**

PPPoE access: **User MAC**, **NAS IP(v4)**, **Internal VLAN**, **External VLAN**, and **Authentication Domain**

IPoE Web access: **User MAC** and **Authentication Domain**

The following figures show the configuration pages.





If an item is deselected, it will not be verified. For example, if **Access IP Type** is deselected, users' access IP address types are not checked. That is, users can apply for authentication in dial-up mode by using any type of IP addresses. For example, they can connect to an external network over the Dynamic Host Configuration Protocol (DHCP) or use static IP addresses

Note

Disabling User Information Check

When all the options of the user information check are deselected, the function is disabled.

Note

Unbinding User Information

User information is changeable because of potential network topology changes. The most common causes include the user relocation, switch changes, or network adapter replacement in actual applications. As a result, the changes of user information should be synchronized to the system. Administrators can modify user information in the database or choose **User**>**User Management**>**User Search**>**Batch Modification** to unbind user information in batches, in combination with the function described in "Acquisition of Information About Internet Access Users" to start automatic binding of the latest user access information.

User Information Acquisition

User Information Acquisition can automatically acquire information about users who pass the authentication, to facilitate user information management for administrators. Administrators do not need to enter user IP addresses, MAC addresses, and other tedious information when adding users. Information that can be automatically acquired includes the following:

User IP(v4): IPv4 address of the network adapter for user authentication in dial-up mode. A user's IPv4 address can be a static IP address or a dynamic IP address, depending on the dial-up mode.

User MAC: MAC address of the network adapter for user authentication in dial-up mode.

NAS IP(v4): NAS IPv4 address

NAS Port: NAS port ID (PID)

Web Authentication Device IP(v4): IP address of the Web authentication access device in the ePortal scheme.

Web Authentication Device Port: port ID of the Web authentication access device in the ePortal scheme.

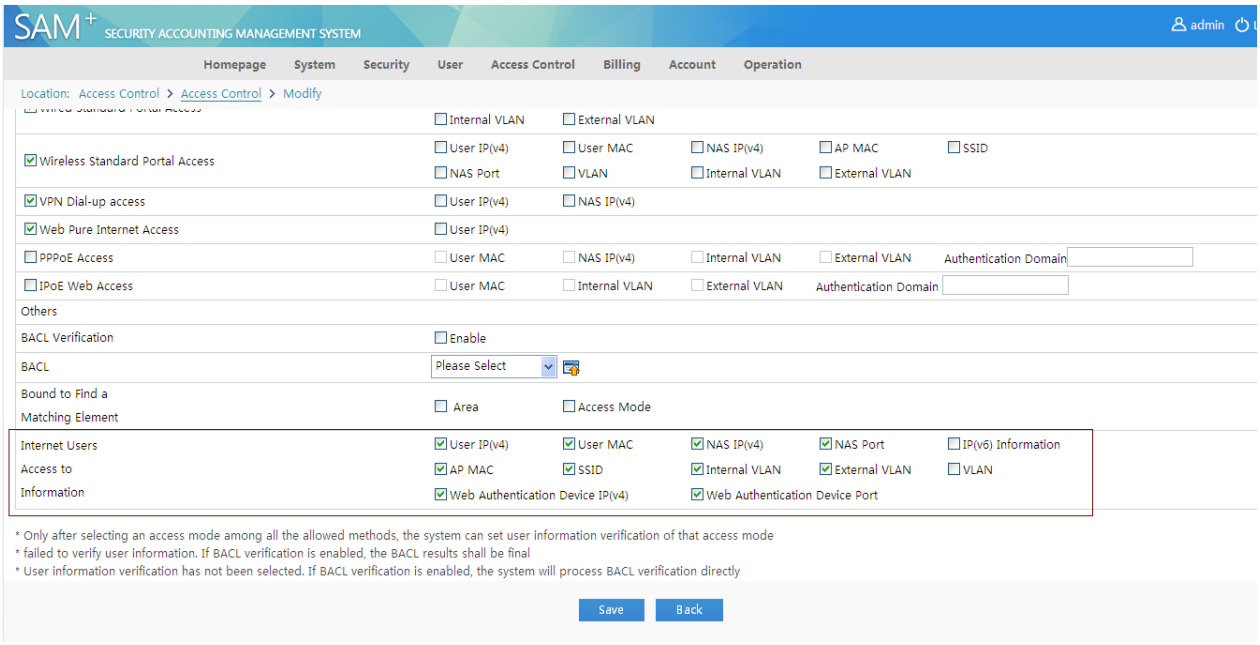
IP(v6) Information: includes the IPv6 addresses of users, NASs, and gateways, and temporary IPv6 addresses of users.

AP MAC: MAC address of the connected AP

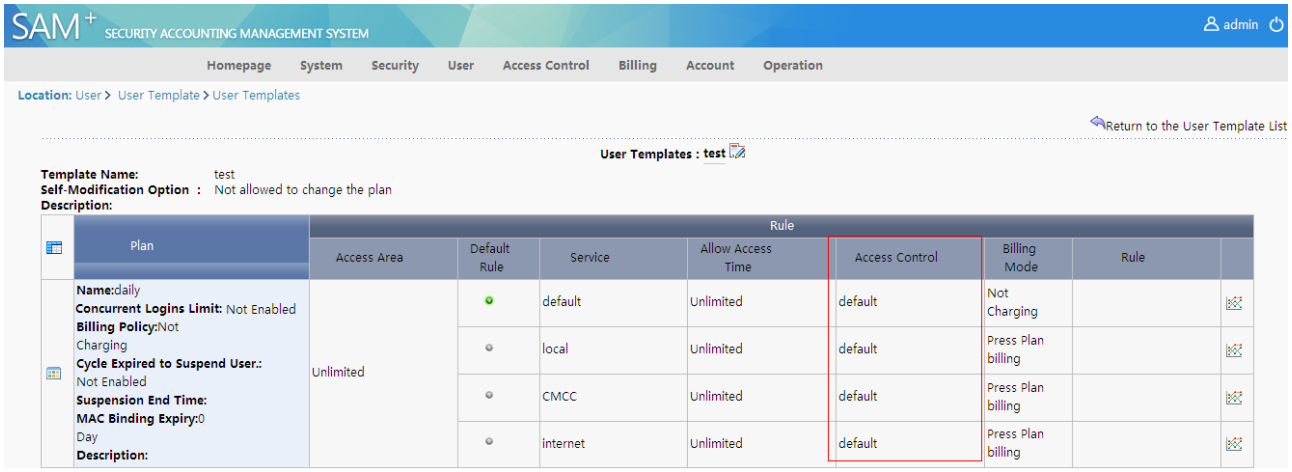
SSID: connected Wi-Fi SSID

Operation steps:

Select or add one access control named **default**. Choose **Access Control**>**Access Control**>**Add/Modify**, click the **User Information Check** tab, and then select items to be automatically collected in **Internet Users Access to Information**.



Choose **User**>**User Templates**, and apply the access control **default** in the plan of the user.



If the user uses the **default** access control for the first authentication, the RG-SAM+ system automatically records the user information at the first time.

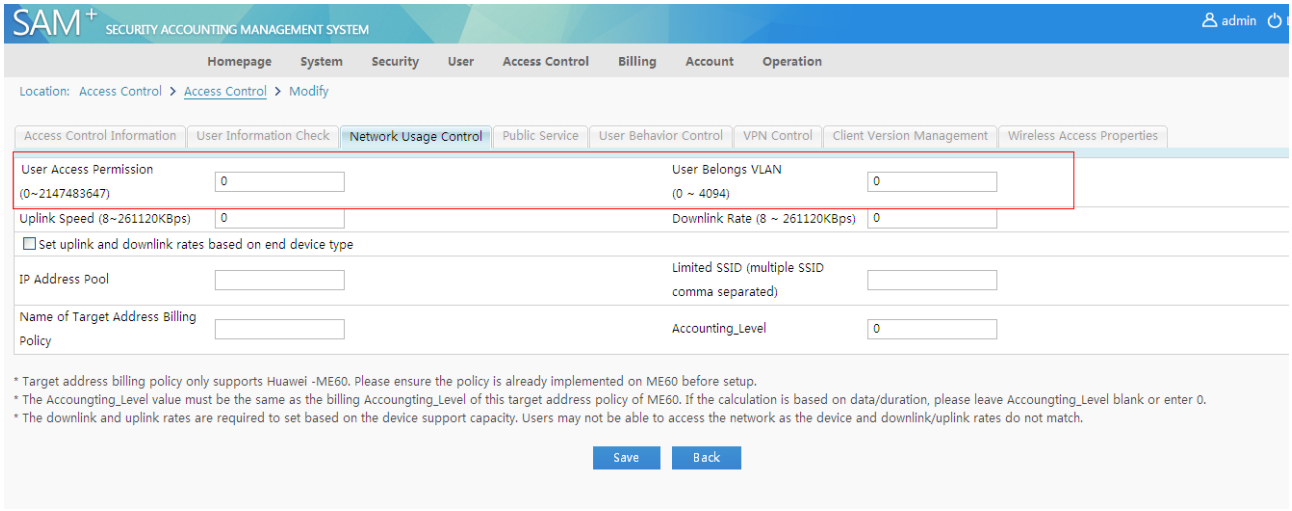
Note

Deleting User Information Binding

Deleting user information binding is equal to unbinding user information. After deletion, the RG-SAM+ system automatically acquires user information at the next authentication.

Uplink and Downlink Rate Limit

After a user passes authentication, the RG-SAM+ server, according to the access control configuration of the user, notifies the switch to control the uplink and downlink rates of the user. The range of uplink and downlink rates is from 0 kbit/s to 1024 kbit/s, and the value **0** indicates no limit.



Public Service

Public service is defined for one unique type of access control. It allows users who have the access control privilege to go online through it regardless of whether they are in special state or become unqualified due to out of duration and traffic.

The public service provided by the RG-SAM+ system aims at allowing the fresh account holders or users in arrears to apply for authentication in dial-up mode, and use the recharging, to-be-deducted amount prepayment, and transfer functions to recharge amount to accounts so that they can continue to access the Internet.

Pay attention to the following points:

Maximum Frequency of Use (Every Day or Every Month)

The times that the public service can be used every day should be restricted. Users enjoying the public service use computers at different levels, and the number of daily or monthly use times are affected by many conditions. Despite of that, the RG-SAM+ system will restrict the number to 1 to 9. The use of the public service will be recorded by the system.

When the use times exceed the allowed daily/monthly number, the user is not allowed to use the public service in that day/month.

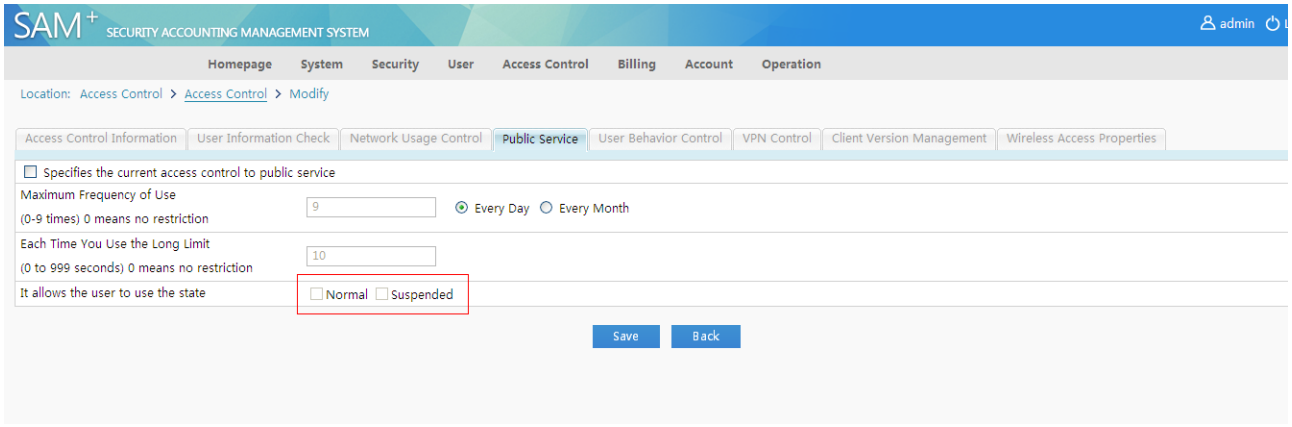
Each Time You Use the Long Limit

The public service must be used by restrictions. The allowed duration for each use ranges from 1 second to 999 seconds.

The available duration of the public service must be smaller than the re-authentication interval of the switch.

No billing is conducted on the public service and no account flows are generated.

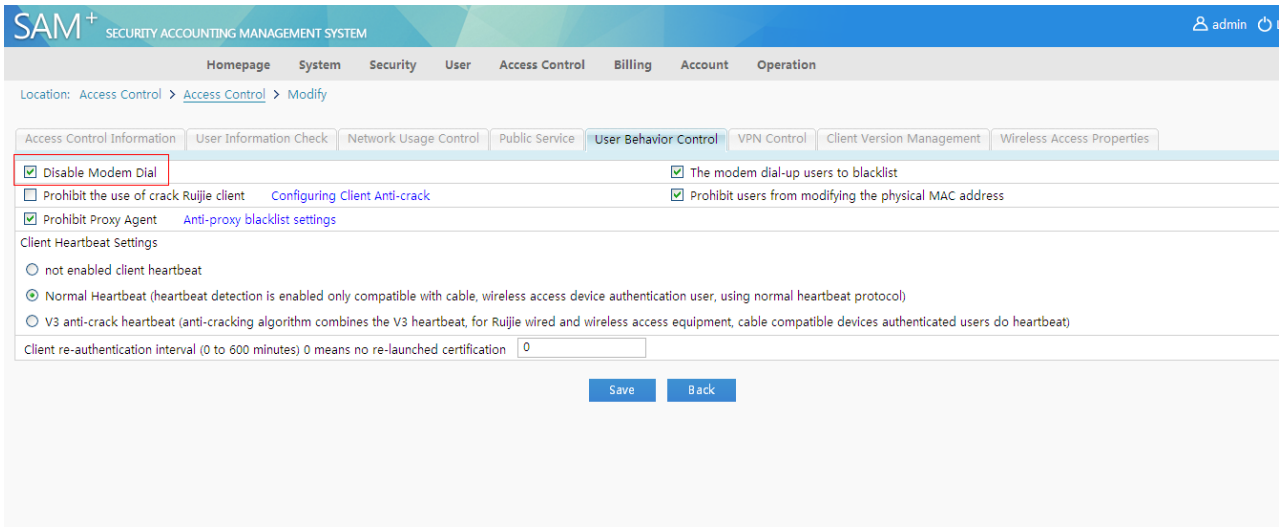
For DHCP authentication and switch re-authentication, the number of use times should be your expected value plus one.



Modem Dial-up Disabling

Modem Dial-up refers to the operation process that a user accesses a LAN by using Ruijie dial-up App **Su** and then visits another LAN through the first LAN in other ways. Such dial-up is often forbidden in applications with high security requirements, such as banking and financial systems, thereby preventing data disclosure.

The RG-SAM+ system supports the modem dial-up disabling function. Choose **Access Control** >**Access Control** >**Modify**. After **Disable Modem Dial** is selected, the configuration is delivered to a client. Ruijie dial-up App **Su** on the client starts to monitor whether a user performs modem dial-up. If yes, **Su** will immediately force the user offline, and notify the RG-SAM+ server for recording.



Note

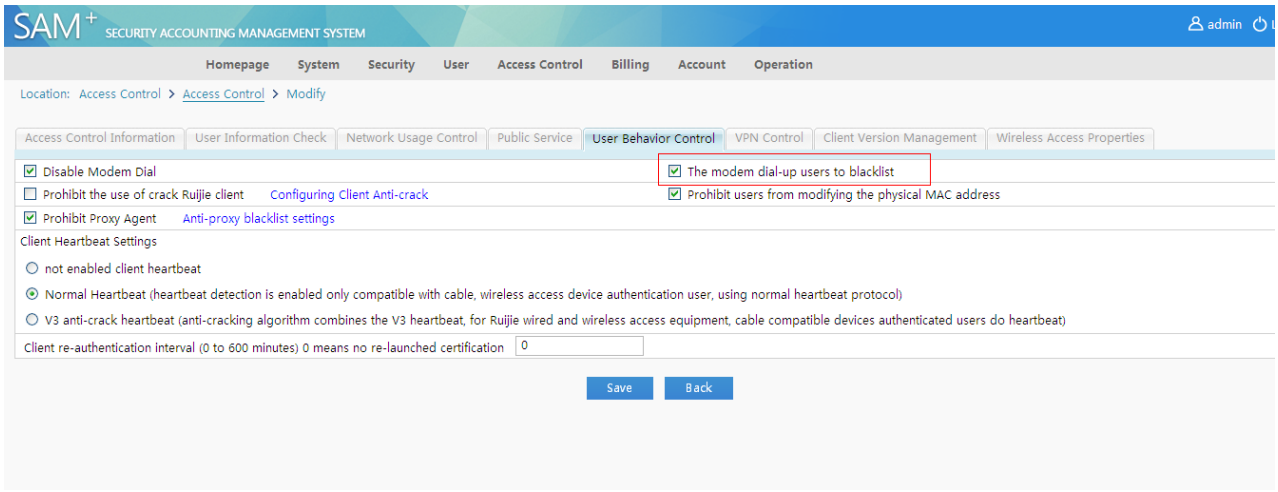
Disabling and Blacklisting Modem Dial-up Users

In general, the modem dial-up disabling function is used in combination with the function of blacklisting modem dial-up users, to guarantee the security of the network system and system data to the maximum extent. For details, see "Blacklisting Modem Dial-up Users."

Blacklisting Modem Dial-up Users

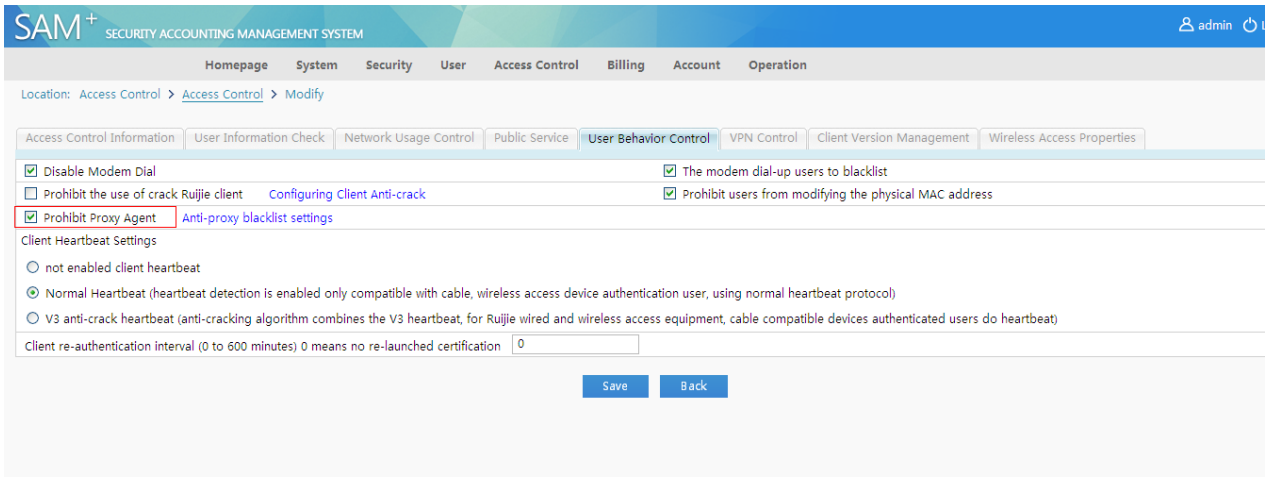
Under the premise of disabling the modem dial-up, you can decide whether to blacklist modem dial-up users. The blacklisting function forces users to go offline when they use modem dial-up for the first time, and rejects their re-authentication, thereby ensuring network system security to the maximum extent.

Blacklisted users are kept in the blacklist of modem dial-up permanently. If they want to access the Internet again, they need to apply to the network management center. They can access the Internet only after administrators manually delete their blacklist records.



Proxy Agent Prohibition

In proxy mode, the local host functions as a proxy agent or server. When the proxy host can use network resources, other hosts can also use the network resources through the proxy.



Proxy agents will cause great harm to networks, including:

Firstly, for clients that access the Internet through a proxy server, their IP addresses displayed externally are the IP address of the proxy server. As long as the proxy server can access the Internet, the clients can use network resources free of charge without authentication and billing by the RG-SAM+ server, causing huge fee losses.

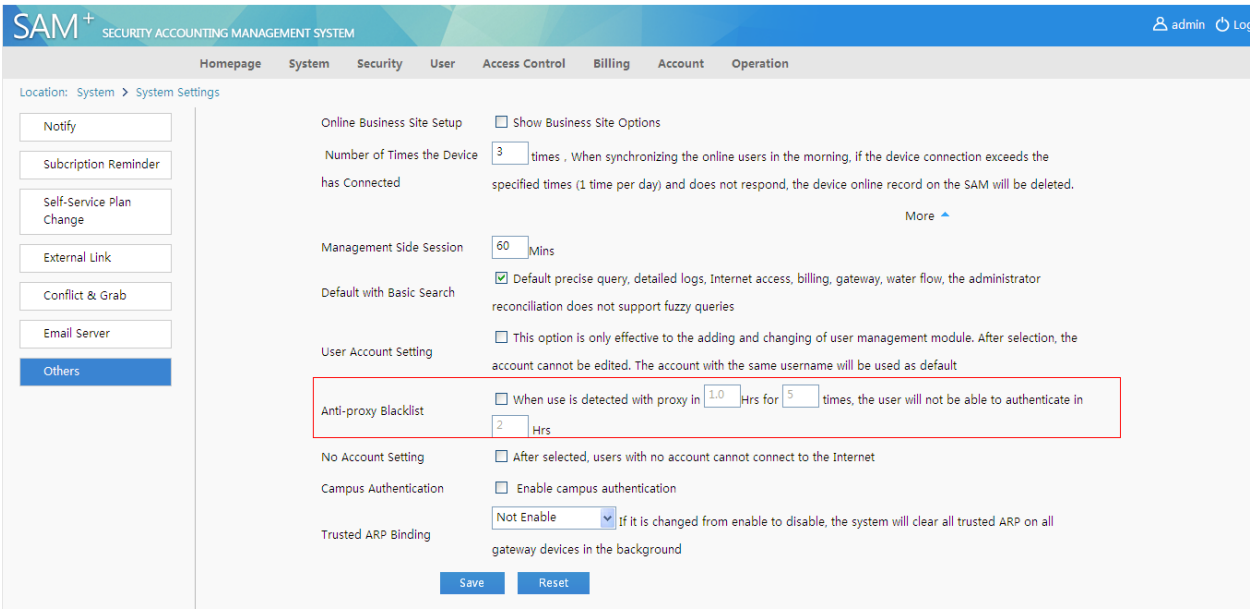
Secondly, clients that access the Internet through a proxy server can hide their IP addresses. Users may use such clients to access server resources restricted to some IP addresses and even attack the network, causing network management difficulties. Therefore, proxy agents need to be strictly prevented in actual applications.

To shield such a proxy loophole, the RG-SAM+ system provides the function of **Prohibit Proxy Agents** by virtue of access control. The RG-SAM+ system supports the proxy agent prohibition function. It sends a signal of enabling the proxy agent prohibition function to a client. The **Su** makes judgment on whether a user establishes a proxy server. After

detecting a proxy agent of a user, the **Su** immediately forces the user to go offline, sends a message to the RG-SAM+ server, and records the user offline cause in the RG-SAM+ system.

Working mechanism of a proxy server: A proxy server is similar to an agent in our lives. Assume that your computer is host A, you desire to get data from host B, and host C is a proxy server. Host A establishes a connection to host C. After receiving the data request from host A, host C establishes a connection to host B, downloads data requested by host A from host B, and sends the data to host A, completing the proxy task.

Choose **System**>**System Settings**>**Others**, and click **More** to display more options. The **Anti-proxy Blacklist** item is displayed, as shown in the following figure.



Select **Anti-proxy Blacklist** and configure it. If it is detected that the number of proxy times of a user exceeds the configured value within a certain period of time, the user will be blacklisted and cannot apply for authentication within a period of time.

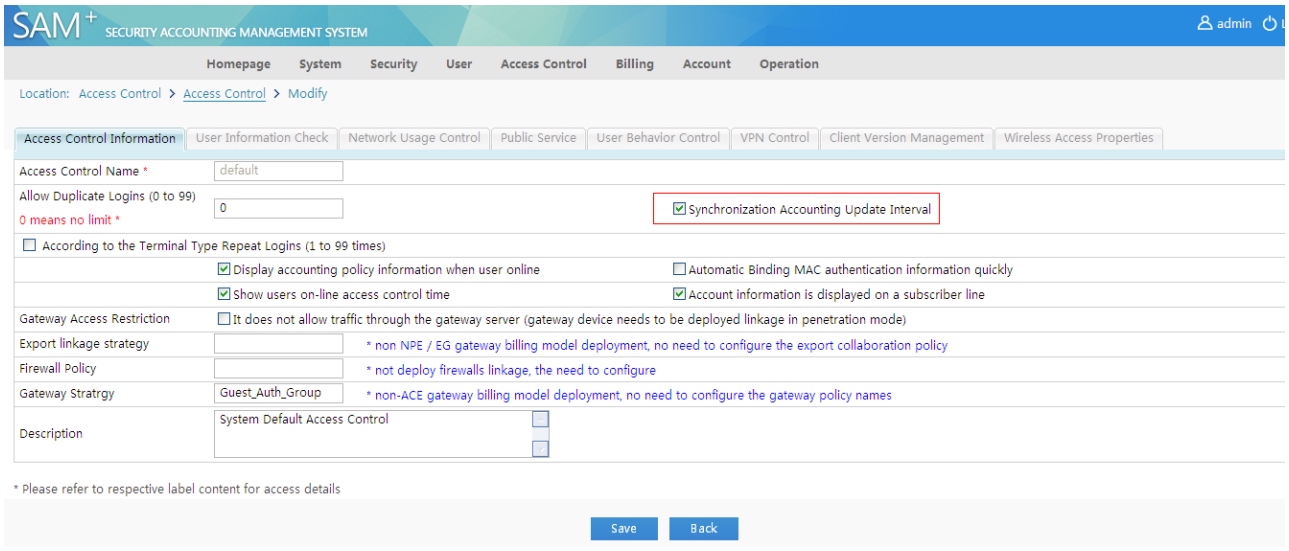
Accounting Update Interval

The duration billing policy provides the accounting update function, the enabling of which, however, is restricted by the service configuration:

If the accounting update function is enabled in the billing configuration, but the function of **Synchronizing Accounting Update Interval** is disabled in the access control, the accounting update function is unavailable.

If the accounting update function is disabled in the billing configuration, the accounting update function is unavailable even if the function of **Synchronizing Accounting Update Interval** is enabled in the access control.

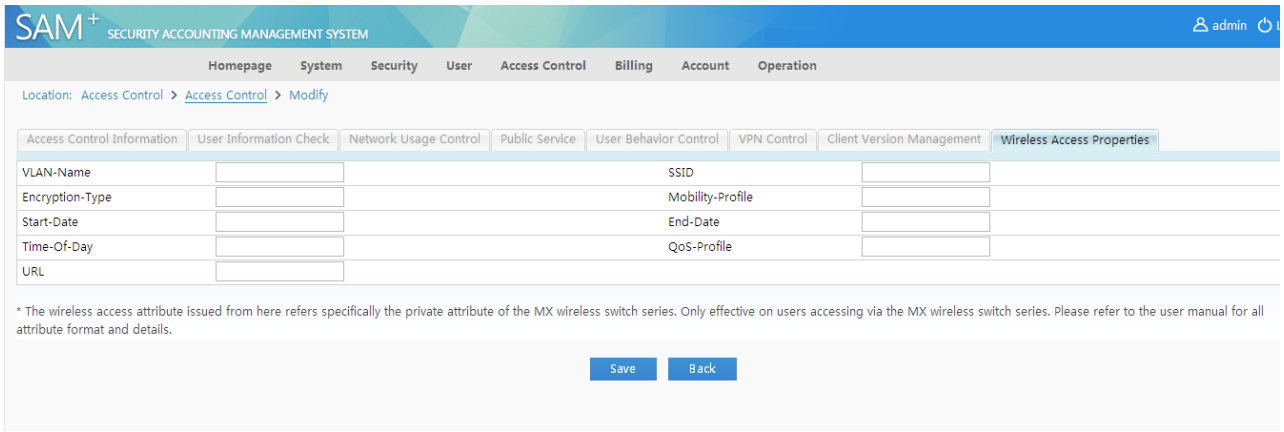
The function of synchronizing the accounting update interval needs to be enabled in the access control of a user and the accounting update function needs to be enabled in the billing configuration so that the accounting update is available. For details about accounting update function of billing, see the billing section.



In the wireless environment, a wireless switch determines whether to send accounting update packets after this function is enabled/disabled. The accounting update function does not need to be configured on wireless switches.

Wireless Private Attributes

In wireless access mode, after a user passes authentication, the RG-SAM+ system will issue wireless private attributes to the MX series switches, so as to manage the wireless Internet access behaviors of users. The following figure shows the optional wireless private attributes.



The format and meaning of attributes and their parameters are described as follows:

VLAN-Name: is composed of English letters or digits with no more than 16 characters, excluding spaces. This attribute specifies an available VLAN name for a user.

SSID: is composed of English letters or digits with no more than 32 characters, excluding spaces. This attribute specifies the SSID of a wireless network that can be used by a user.

Encryption-Type: The value is an integer ranging from 0 to 127 and their meanings are as follows:

1— AES_CCM encryption

2— Reserve

4 — TKIP

8 — WEP-104

16 — WEP-40

32 — No encryption

64 — Static Wired Equivalent Privacy (WEP)

You can specify multiple encryption types. For example, you can use both WEP-104 and WEP-40, and set **Encryption-Type** to **24**.

Mobility-Profile: The value is composed of English letters or digits with no more than 32 characters, excluding spaces. This attribute specifies the access control policy for a user (the access control policy is configured on MX series wireless switches and defines the AP that can be directly or indirectly connected an MX wireless switch for a user).

Start-Date: The value is in the format of *YY/MM/DD-HH:MM* and this attribute specifies the start time of using a wireless network for a user.

End-Date: The value is in the format of *YY/MM/DD-HH:MM* and this attribute specifies the end time of using a wireless network for a user.

Time-Of-Day: The value is a string of no more than 253 characters and the meanings of options are as follows:

never: A user cannot use the network at any time.

any: A user can use the network at any time.

al: A user can use the network at any time (same as **any**).

You can also specify a range in the format of "time-of-day weekly mark time[,|]weekly mark time[,|]…".

mo — Monday

tu — Tuesday

we — Wednesday

th — Thursday

fr — Friday

sa — Saturday

su — Sunday

wk — Monday to Friday

The time format is *hhmm-hhmm*, in 24-hour system.

For example, **time-of-day tu1000-1600,th1000-1600** indicates that a user can use the network from 10:00 to 16:00 on Tuesday and from 10:00 to 16:00 on Thursday.

QoS-Profile: The QoS profile attribute, in combination with the authentication function, dynamically provides the preconfigured QoS function for a user or a group of users who pass authentication.

URL: The value is string of no more than 247 characters in the URL format beginning with **http://**. This attribute, in wireless Web portal mode, specifies the URL of the redirected page for authenticated users.


Note

Configuration:

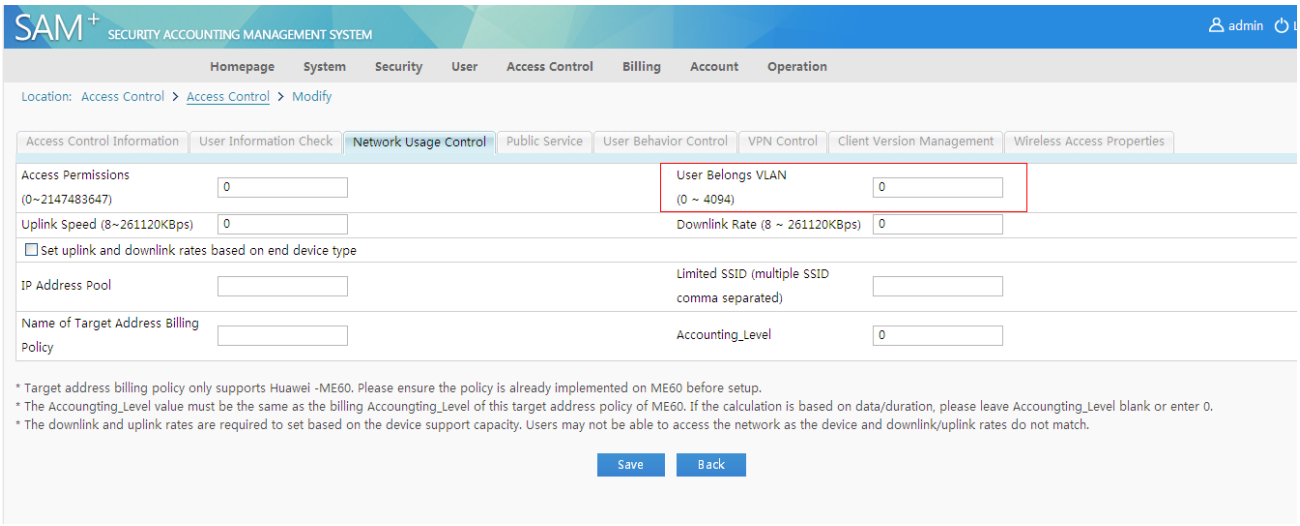
1. Improper configuration of private attributes for wireless switches may cause repeated user authentications (for example, if a non-existent VLAN name or an SSID different from the SSID used by a user is issued, the user will continuously apply for authentication due to failure to access the Internet). Therefore, administrators should comprehend them beforehand.
2. The SSID private attribute is equivalent to the preceding SSID binding function. It is recommended that the SSID private attribute not be configured and the binding function of the RG-SAM+ system be used.
3. When **Start-Date** and **End-Date** are set simultaneously, ensure that **Start-Date** < current time < **End-Date**. Otherwise, users cannot use the network.

VLAN

A VLAN is an end-to-end logical network that is built using network management software on the basis of the switching LAN, and can traverse different network segments and different networks. VLAN is proposed for resolving Ethernet broadcasting and security problems. It uses VLAN IDs to classify users into smaller work groups to restrict their Layer 2 interworking. Each work group is a VLAN. The advantage of VLAN is to restrict the broadcasting scope, build virtual work groups, and dynamically manage networks.

User VLANs can be configured in two locations at the RG-SAM+ system. On the **Access Control** edit page, you can specify a unified VLAN ID to all users who use the same access control; or you can also specify a VLAN ID for a user during modification. When an exclusive and unified access control VLAN IDs are both specified for a user, the VLAN ID issued to the user is the former one configured in the user template. That is, the user VLAN is prior to the access control VLAN.

The VLAN configuration in the **Access Control** module is shown in the following figure.



VLAN ID Description

A VLAN ID ranges from 0 to 4096. The value 0 indicates that no VLAN is set. If the ID of a user VLAN or access control VLAN is 0, observe the following principles:

When the access control VLAN ID is set to 0 but the user VLAN ID is set to a non-zero value, the user VLAN ID is issued.

When the access control VLAN ID is set to a non-zero value but the user VLAN ID is set to 0, the access control VLAN ID is issued.

When the access control VLAN ID and user VLAN ID are both set to non-zero values, the user VLAN ID is issued according to the principle of user VLAN ID in preference to the access control VLAN ID.

When the access control VLAN ID and user VLAN ID are both set to 0, the VLAN ID of the source port is issued to this port, that is, the VLAN ID of the source port keeps unchanged.

VLAN Conflict

VLANs conflict because a port is occupied by a user of a VLAN domain. Another user also wants to access the Internet through this port and uses a different VLAN ID, resulting in conflicts. To check VLAN conflicts, query the online user table. If a port of a switch has a VLAN ID of an online user in addition to a VLAN ID to be issued, it is considered that a VLAN conflict exists and another user is not allowed to go online.

VLAN Jumping

A VLAN ID is granted to each switch port, indicating a VLAN domain. When the issued VLAN ID is inconsistent with the VLAN ID of the source port, the issued VLAN ID is granted to the port, resulting in VLAN ID change of the port, which is called VLAN jumping.

Maximum Available Duration

When a user dials up, the RG-SAM+ server notifies the switch of the maximum Internet access duration. After the access duration is used up, the switch immediately gets the user offline. The maximum available duration of a user is restricted by three elements:

Each Time You Use the Long Limit

When a user passes authentication by using the public service, the issued maximum available duration is the limit on the duration of each use of the public service.

Duration Reversely Calculated by Billing

The billing module calculates the available Internet access duration for a user based on the account balance of the user.

Maximum Access Time Range

The time difference between the Internet access time of a user and the allowed access time range also determines the maximum available duration of the user.

The preceding elements jointly determine the maximum available duration of a user. When a user passes authentication in dial-up mode by using the public service, the allowed duration of each use of the public service is the maximum available duration of a user. In other cases, the maximum available duration is the duration reversely calculated by the billing module or maximum available duration in the access time range, whichever is smaller.

Authentication-free

The authentication-free function disables check on some items of the access control. Note that not all access control items are authentication-free. For example, when the authentication-free function is effective, the system also needs to check whether a user has the privilege, check the times of public service use and duration. The following lists items in the authentication-free scope:

- User Information Check
- Client Type Check
- Client Version Check
- Non-Ruijie Client Check

VPN

Overview

VPN is an extension to a private network and contains Internet-similar shared or public network links. It allows two PCs to transfer data in the shared or public links by simulating point-to-point private links.

Users who work at home or in travel can establish a remote connection to the enterprise server through VPN, which is supported by the basic structure of the public network (for example, Internet). For users, VPN is a point-to-point connection between a PC (a VPN client) and a community server (a VPN server). VPN is independent of the specific basic structure of a shared or public network, because it seems that data is sent over a dedicated private link logically.

Enterprises can also use VPN to establish route connections for offices in different locations, or connect to other enterprises over a public network (for example, Internet) while ensuring secure communication.

With remote access and route connection, an organization can use VPN connections to substitute long-haul dial-up or leased line for local dial-up or leased line provided by the Internet service provider (ISP).

VPN Solution Requirements

In recent years, libraries in universities and colleges purchase a large number of online databases for readers, including engineering indexes, science abstracts, chemical abstracts, and many Chinese and English full-text electronic journals. Students and teachers living outside the campus cannot access these databases.

The reason is as follows: The purchased databases are not stored on the library server but the providers' servers. After libraries pay fees, database service providers check whether a user is an authorized user based on the IP address of the user. IP addresses of the campus network are within the authorized range and all Internet access computers on the campus network can access the databases. IP addresses for used by teachers and students living outside the campus for Internet access are out of the IP address range of the campus network. Database service providers consider that they are public users and reject their access.

To resolve this problem, Ruijie proposed the AAA&VPN solution.

For the solution topology, see "Deployment in VPN Access Mode."

Before accessing database resources, users living outside the campus connect to the VPN server in dial-up mode. The VPN server allocates campus IP addresses to the users, who can use library resources as they are on the campus network.

Basic Support of the RG-SAM+ System

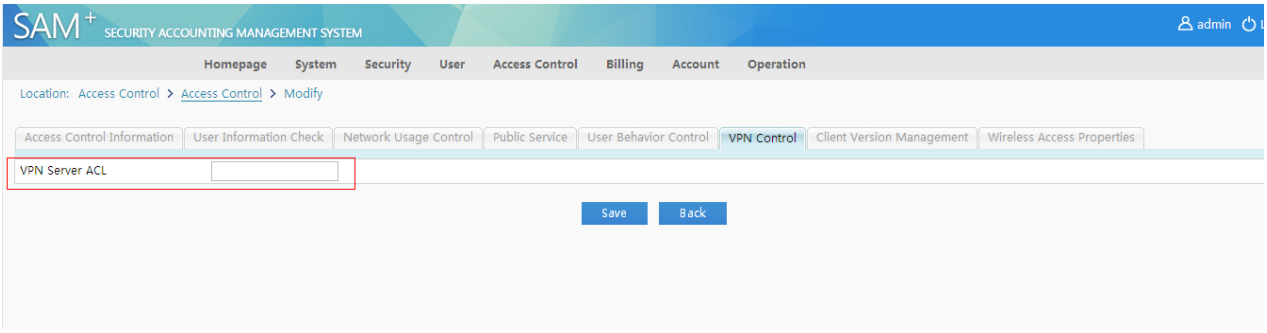
Security assurance needs to be provided for the access to an intranet through the insecure Internet. The RG-SAM+ system provides a range of security verification functions for the VPN dial-up mode, to ensure that authentication connections are secure when a user access an intranet from an insecure external network.

Firstly, the RG-SAM+ system provides the function of verifying the user identity validity. VPN dial-up users need to be users registered with the RG-SAM+ system and can provide correct usernames and passwords to prove their identities.

Secondly, users applying for authentication must meet a range of security verification requirements defined in the access control.

Thirdly, according to the VPN principle, a VPN dial-up user needs an Intranet IP address so as to have the privilege to access the Intranet. On the user information edit page, you can allocate an IP address to the user. When the IP address is issued to the user during VPN dial-up process, the user is within the intranet control range.

Lastly, the RG-SAM+ system supports the access control list (ACL) of the VPN server. Administrators can configure the ACL of the VPN server for VPN dial-up users in the ACL so that the VPN server conducts access control when receiving an authentication request.



Extended Support of the RG-SAM+ System

You need to pay attention to the following items in terms of the VPN function:

TunnelClient: public network address of a user who initiates a VPN connection

TunnelServer: public network address of the VPN server

The two items respectively record the IP address of a client on the public network in the case of a VPN connection and the IP address of the server exposed to the public network. They are recorded in the Internet access details of the RG-SAM+ system for future query.

Note

Difference between VPN users and normal users

VPN is not a user type but a network access mode used by users. There are no VPN users. For example, if a user accesses the Internet through a VPN server, the access mode of the user is VPN access mode. The access control adopted by the user is differentiated by the access control name in the client of the user, which is the same as normal users.

How to handle the situation in which users have no IP addresses to be issued to them?

If an IP address to be issued is not set for a user in the VPN solution, the user can still pass authentication but the RG-SAM+ system cannot notify the user of the intranet IP address to be used. The VPN router provides a range of IP addresses to be issued. When the RG-SAM+ system has no IP address to be issued for a user, the VPN router selects an IP address from the preset IP address range for the user

according to an algorithm. The RG-SAM+ system, however, cannot judge whether the IP address is an intranet IP address and what are the Internet access privileges of the IP address.

Telnet

Overview

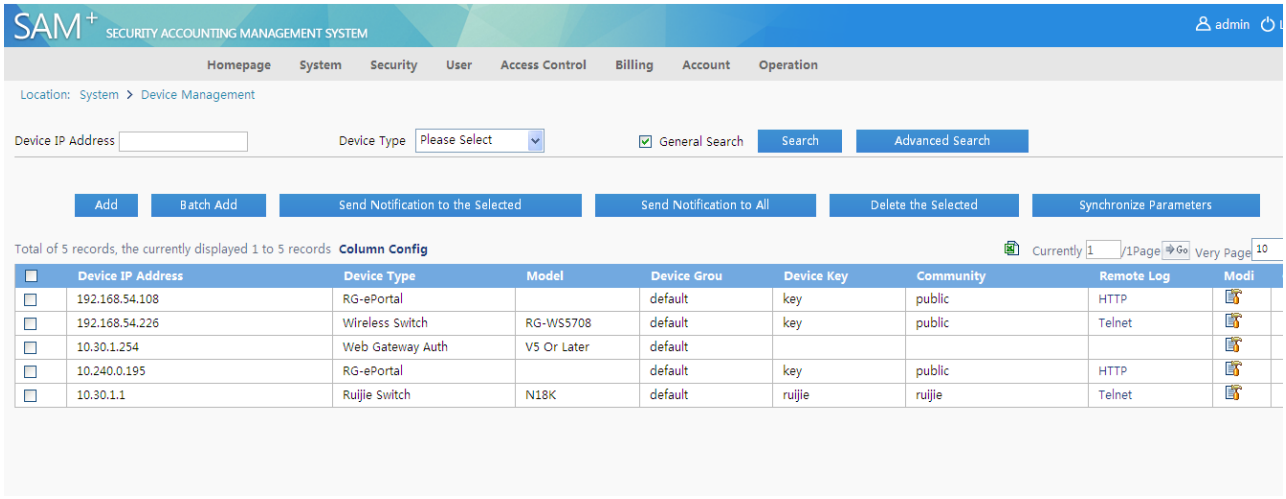
A terminal connecting to the host can log in to the local system easily. This capability can be extended to another terminal. Distributed applications such as databases, files, or printers are resources that can be shared as original. Telnet is a realization of such capacity which makes the mode of accessing shared resources possible. Telnet is a protocol that is applied mostly widely in the TCP/IP protocol family. It provides a universal tool for accessing Internet and network resources. It allows users to communicate with remote servers, and supports different physical terminals through negotiation, providing great flexibility.

Basic Support of the RG-SAM+ System

The RG-SAM+ system supports Telnet and allows device administrators to manage parameter settings in Telnet mode. After the administrator telnets to a device, the administrator should enter the username and password. Then, the authentication request is sent to the RG-SAM+ server, which verifies the user identity and issues permissions.

The RG-SAM+ system must collaborate with Telnet-capable devices.

Firstly, the devices has been added in **Device Management**.



Secondly, you should enable login authentication and set the authentication mode on the devices. For details, see the device description.

Thirdly, you need to set device management privileges and link them to a device administrator. When the device administrator telnets to a device, device management privileges are assigned to the administrator accordingly.

For details about device administrators and device management privileges, see relevant sections.

Error Prompts

Note: The prompts may vary with versions.

No.	Server Logs	Client Prompts
0	NAS IPv4 address binding validation error.	NAS IPv4 address binding validation error.
1	Portal device Port address binding validation error.	Portal device Port address binding validation error.
2	User IPv4 address binding validation error.	User IPv4 address binding validation error.
3	User MAC address binding validation error.	User MAC address binding validation error.
4	User dynamic IP address binding validation error.	User dynamic IP address binding validation error.
5	User static IP address binding validation error.	User static IP address binding validation error.
6	Portal device IPv4 binding validation error.	Portal device IPv4 binding validation error.
7	BACL rule binding validation error.	BACL rule binding validation error.
8	Open IP uniqueness detection, IPv4 conflicting with online users.	Open IP uniqueness detection, IPv4 conflicting with online users.
9	Your account has reached the maximum concurrent online user limit.	Your account has reached the maximum concurrent online user limit.
10	User does not exist.	User does not exist.
11	User password is incorrect.	User password is incorrect.
13	User information from a third party has joined SAM, require user to log in again.	User information from a third party has joined SAM, require user to log in again.
14	LDAP server connection is not on or LDAP user backup has expired.	LDAP server connection is not on or LDAP user backup has expired.
15	Synchronization backup LDAP user failed.	Synchronization backup LDAP user failed.
16	Unsupported access mode.	Unsupported access mode.
17	Username contains illegal characters. Such as the beginning or end with a space	Username contains illegal characters. Such as the beginning or end with a space
18	LDAP user using the unsupported access mode.	LDAP user using the unsupported access mode.
19	The maximum account limit of the system has been reached.	The maximum account limit of the system has been reached.
20	The access control does not exist.	The access control does not exist.
21	Users cannot use the access control.	Users cannot use the access control.
22	Users cannot use the public service.	Users cannot use the public service.
23	The public service cannot be used again this day.	The public service cannot be used again this day.

No.	Server Logs	Client Prompts
24	Access device are not associated with access area.	Access device are not associated with access area.
25	The area does not allow to use the access control.	The area does not allow to use the access control.
27	The service has expired.	The service has expired.
28	User has used an impermissible access mode.	User has used an impermissible access mode.
29	You can only use the supplicant client authentication for Internet access.	You can only use the supplicant client authentication for Internet access.
30	Please update your Ruijie client version.	Please update your Ruijie client version.
31	The client used is not specified by the administrator.	The client used is not specified by the administrator.
32	The client type is not allowed.	The client type is not allowed.
33	Not Using the Ruijie Client.	Not Using the Ruijie Client.
34	Client Anti-cracking checked that the client configuration file does not contain the client information.	Client Anti-cracking checked that the client configuration file does not contain the client information.
35	Client Anti-cracking checked unsupported Anti-cracking algorithm.	Client Anti-cracking checked unsupported Anti-cracking algorithm.
40	The account is on the network with outstanding payment.	The account is on the network with outstanding payment.
41	The account balance is insufficient.	The account balance is insufficient.
42	Access time has been used up for the current package.	Access time has been used up for the current package.
43	No remaining traffic for the current package.	No remaining traffic for the current package.
44	No remaining time for the current package.	No remaining time for the current package.
45	No remaining time for the current time rule.	No remaining time for the current time rule.
46	No remaining traffic for the current authentication device rule.	No remaining traffic for the current authentication device rule.
47	No remaining traffic for the current international uplink traffic rule.	No remaining traffic for the current international uplink traffic rule.
48	No remaining traffic for the current international downlink traffic rule.	No remaining traffic for the current international downlink traffic rule.
49	No remaining traffic for the current domestic uplink traffic rule.	No remaining traffic for the current domestic uplink traffic rule.
50	No remaining traffic for the current domestic downlink traffic rule.	No remaining traffic for the current domestic downlink traffic rule.
51	No remaining traffic for the current gateway	No remaining traffic for the current gateway traffic rule.

No.	Server Logs	Client Prompts
	traffic rule.	
60	Local users please do not select roaming.	Local users please do not select roaming.
61	The local server does not support roaming authentication of the device.	The local server does not support roaming authentication of the device.
62	The user has not enabled roaming authentication.	The user has not enabled roaming authentication.
70	Illegal access request, wrong EAP-Message code.	Illegal access request, wrong EAP-Message code.
71	Illegal access request, may be due to the key and system settings do not match.	Illegal access request, may be due to the key and system settings do not match.
72	Response timeout.	Response timeout.
80	Not within the authentication time.	Not within the authentication time.
81	VLAN conflict occurred with the online user.	VLAN conflict occurred with the online user.
82	The device administrator does not have the permissions to login this device.	The device administrator does not have the permissions to login this device.
83	Your package changes are being processed.	Your package changes are being processed.
84	Internal Vlan binding error.	Internal Vlan binding error.
85	External Vlan binding error.	External Vlan binding error.
86	Authentication domain binding validation error	Authentication domain binding validation error
90	Users are not allowed to use the service in the current region.	Users are not allowed to use the service in the current region.
91	Users are not allowed to use the access control in the current region.	Users are not allowed to use the access control in the current region.
92	User is not allowed in the current region.	User is not allowed in the current region.
100	AP MAC binding validation error.	AP MAC binding validation error.
101	SSID binding validation error.	SSID binding validation error.
102	Open the MAC uniqueness detection, users MAC conflicting with online users.	Open the MAC uniqueness detection, users MAC conflicting with online users.
103	User physical MAC address has been modified.	User physical MAC address has been modified.
104	The number of compatible device is more than limit.	The number of compatible device is more than limit.
106	Portal device Port binding validation error.	Portal device Port binding validation error.
107	License is not allowed to use BRAS for authentication.	License is not allowed to use BRAS for authentication.
108	Open IP uniqueness detection, IPv6 conflicting with online users.	Open IP uniqueness detection, IPv6 conflicting with online users.
110	User has been suspended.	User has been suspended.

No.	Server Logs	Client Prompts
112	Illegal username or other abnormalities.	Illegal username or other abnormalities.
113	LDAP user does not exist or incorrect password.	LDAP user does not exist or incorrect password.
115	Users are not allowed to use the SSID on wireless networks.	Users are not allowed to use the SSID on wireless networks.
36	Users cannot use the service.	Users cannot use the service.
180	The public service cannot be used again this month.	The public service cannot be used again this month.
200	NAS IPv6 address binding validation error.	NAS IPv6 address binding validation error.
202	User IPv6 address binding validation error.	User IPv6 address binding validation error.
191	User cannot use the target service.	User cannot use the target service.
192	Cannot use the target service.	Cannot use the target service.
999	System configuration error, it may be the losing of author.ini file.	System configuration error, it may be the losing of author.ini file.
1000	Issue a Challenge Packet.	Issue a Challenge Packet.
1001	Forward Packet.	Forward Packet.
93	This service is unavailable in your current location.	This service is unavailable in your current location.
94	Switching failed due to failure in network gateway deployment.	Switching failed due to failure in network gateway deployment.
95	Failed to open the gateway.	Failed to open the gateway.
96	Your account has reached the maximum concurrent online user limit.	Your account has reached the maximum concurrent online user limit.
97	User does not have device management authority.	User does not have device management authority.
193	Online users have left in the table.	Online users have left in the table.
194	Cannot provide switching service for offline users.	Cannot provide switching service for offline users.
195	Online users have left in the table.	Online users have left in the table.
98	Cannot switch from the external network service to the external network service.	Cannot switch from the external network service to the external network service.
99	IP is inconsistent before and after switching.	IP is inconsistent before and after switching.
121	Username conflict occurred during authentication.	Username conflict occurred during authentication.
122	IPv4 conflict occurred during authentication.	IPv4 conflict occurred during authentication.
123	User MAC conflict occurred during authentication.	User MAC conflict occurred during authentication.

No.	Server Logs	Client Prompts
87	The period has expired and the package has changed. Please log out and refresh.	The period has expired and the package has changed. Please log out and refresh.
130	User is online in the other region.	User is online in the other region.

Billing Management

Overview

The billing module, one of the core RG-SAM+ services, is targeted at implementing billing on all services provided by the RG-SAM+ system.

The billing module collects original online data generated after use, processes the data, performs billing according to the associated billing policies, deducts fees from accounts, and generates account flows for other processing and querying.

The RG-SAM+ system can conduct billing on users for their Internet access based on the Internet access duration and 802.1X traffic (port traffic) by using Ruijie Networks billing-supported switches. In addition, by utilizing Ruijie Networks RG-NTD or RG-ACE, the RG-SAM+ system can conduct billing based on the access destination traffic for different IP addresses. The RG-SAM+ system also supports periodical fee deduction for users' Internet access behaviors.

Another function of the billing module is to manage accounts, including basic management, payment, refund, and transfer operations.

Preparations

Billing Accounts

After a user accesses the Internet, fees are deducted from the account balance of the user. Accounts are one of the most important entities for billing in the RG-SAM+ system. They store information about fees arising from in users' Internet access behaviors. This section describes management of user accounts, which involves two functions:

Account Management: basic service management of accounts, including **Search**, **Add**, **Modify**, and **Delete the Selected**.

Fees Management: account fee management, including **Payment**, **Refund**, and **Transfer**.

Accounts are independent of users for more flexible association. One user must associate with only one account and vice versa.

Fee information is recorded based on accounts. When a user accesses the Internet, the RG-SAM+ system deducts billing fee from the associated account.

Overdraft Options are offered for account settings. If **The account can be overdrawn** is selected, an **Overdraft Fee** or the line of credit must be set. When the balance is insufficient, the credit line will be reduced. When the credit line is used up, the account is thought as in arrears.

An account can be in the **Normal**, **Overdraft**, or **Arrearage** state. If overdraft is not allowed for an account, the account is in the arrearage state after the balance is used up. If overdraft is allowed for an account, the credit line is reduced after the balance is used up, and the account becomes in the overdraft state; after the credit line is used up, the account becomes in the arrearage state.

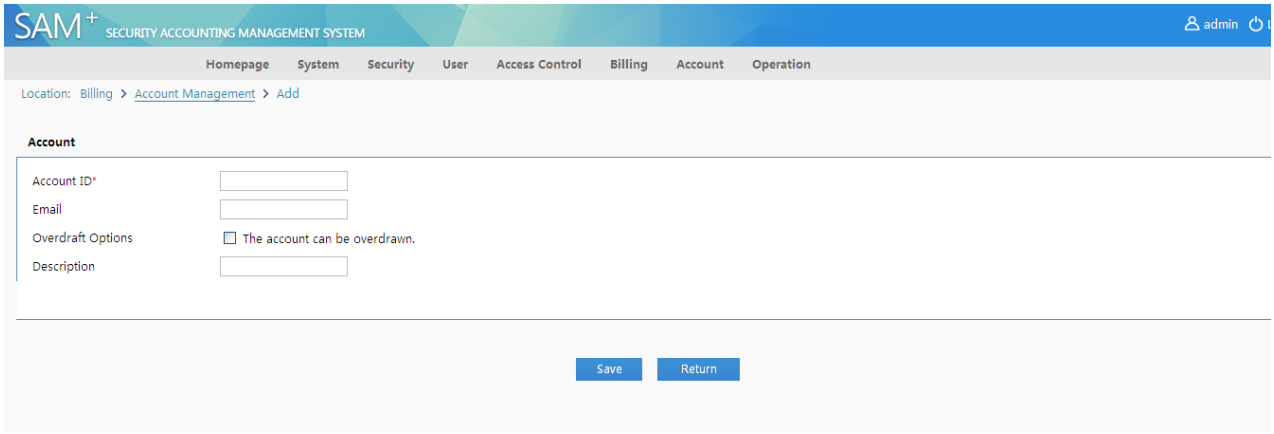
Note

Impact of account arrearage on users:

A user in the arrearage state cannot access the Internet unless the account is allowed in overdraft and the credit line is used up.

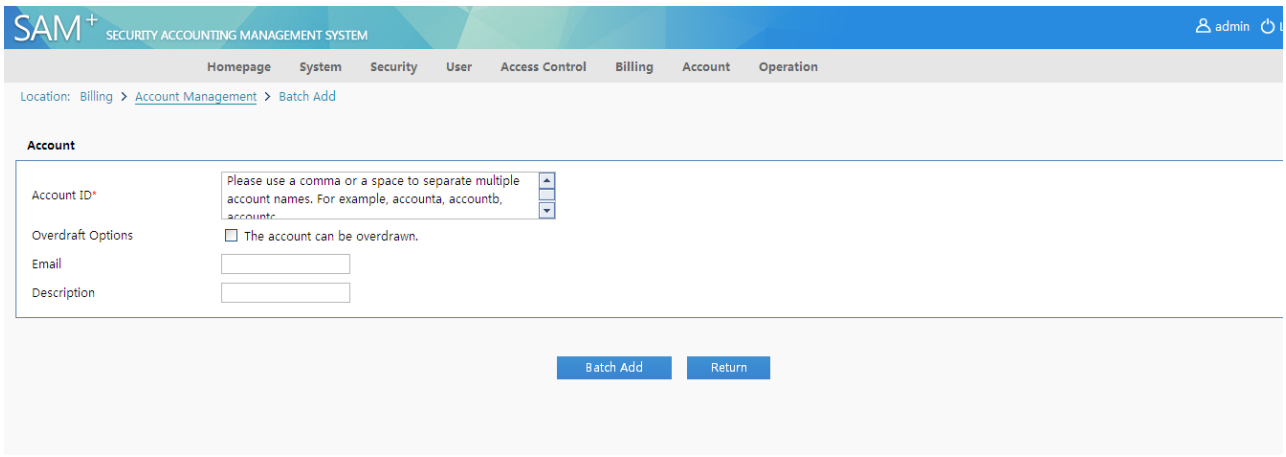
Adding Accounts

There are three methods of adding accounts: **Add** (one account), **Batch Add** (multiple accounts), and **Create Account** (same as the username). Method 1: Choose **Billing**>**Account Management** from the main menu to directly add an account. Click **Add**. The account adding page is displayed, as shown in the following figure.

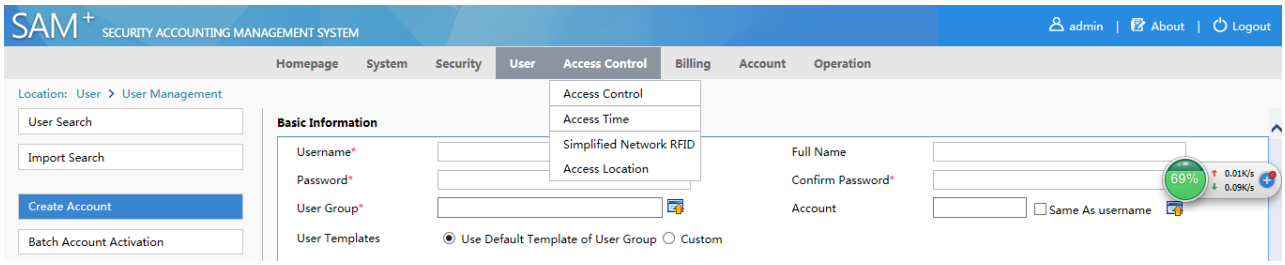


Account ID is mandatory. Click **Save** to save the account.

Method 2: In addition to the account adding function, **Account Management** in **Billing** provides the batch adding function. Click **Batch Add**. The batch adding page is displayed, as shown in the following figure.



Method 3: Choose **User**>**User Management**>**Create Account**, and select **Same As username** in the **Account** box to create an account with the name same as the username, as shown in the following figure.



By default, overdraft is not allowed for accounts.

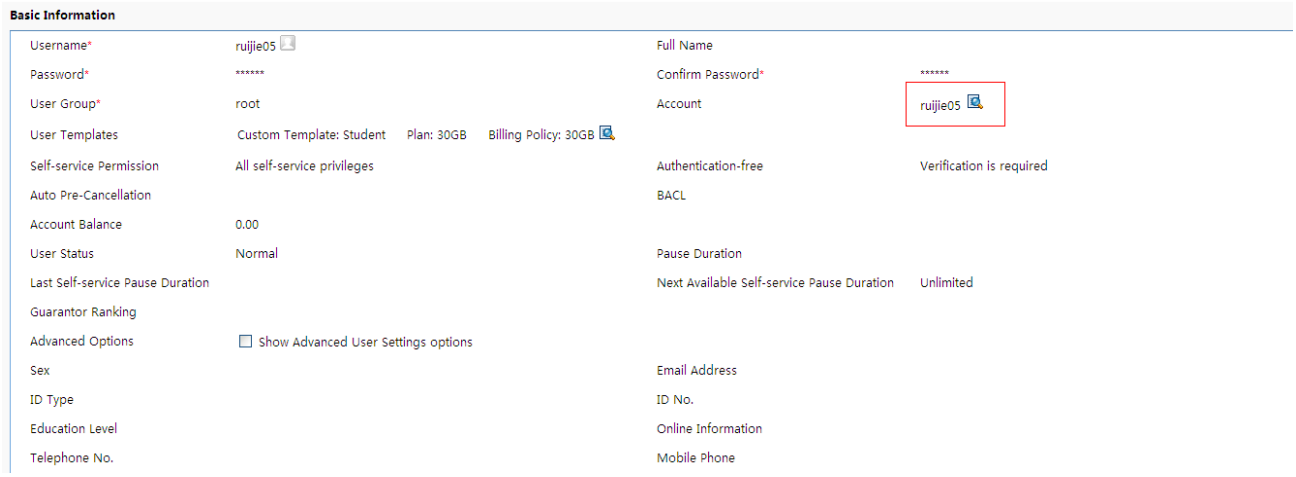
Account Payment

After an account is added following the first way, the message "Successfully added Account" is prompted. Click **OK** to display the account information page. On the page, click **Payment** to pay money.

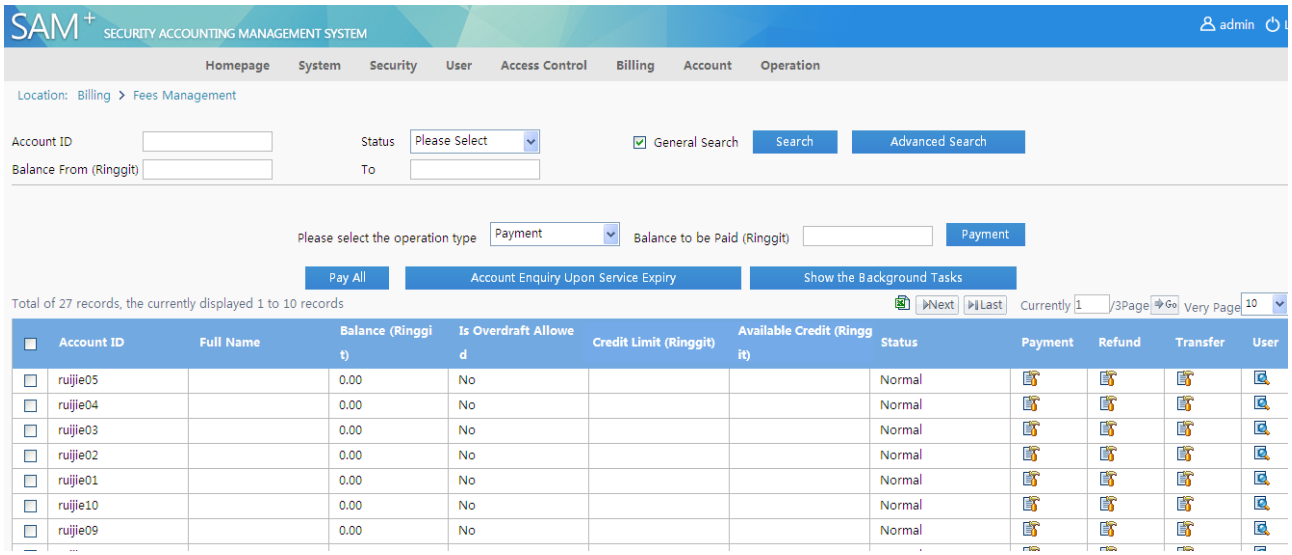
Choose **Billing**>**Account Management**, click **Check** in the account table to view the account information.

Choose **User**>**User Management**, search for a user and double-click the username to display the basic information.

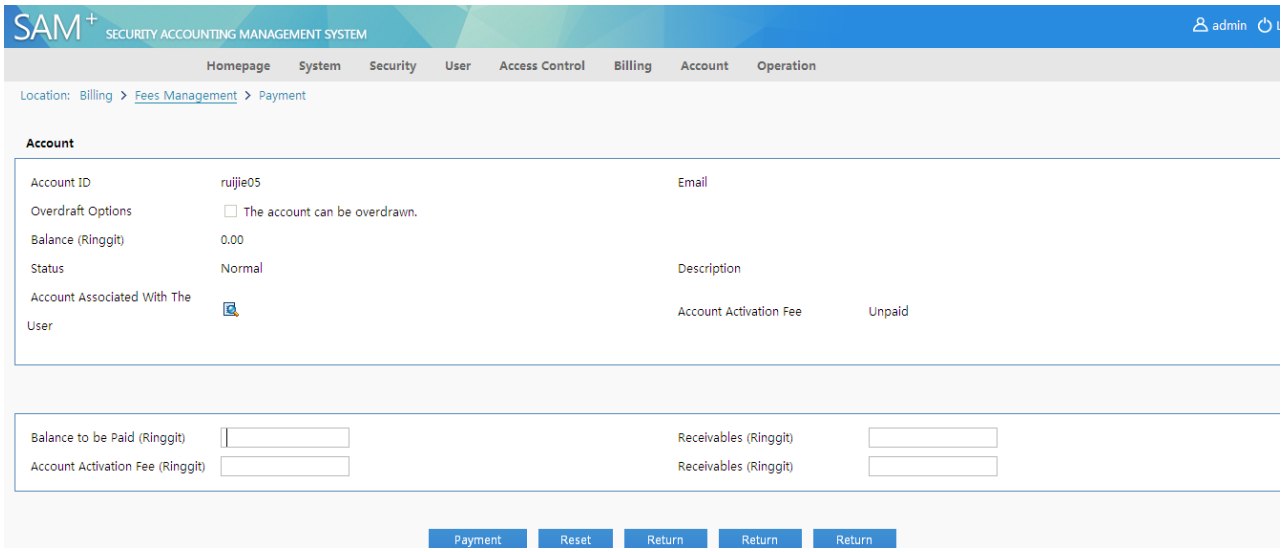
You can click  in the **Account** box, as shown in the following figure. Click the payment button on the page to pay for accounts as mentioned above.



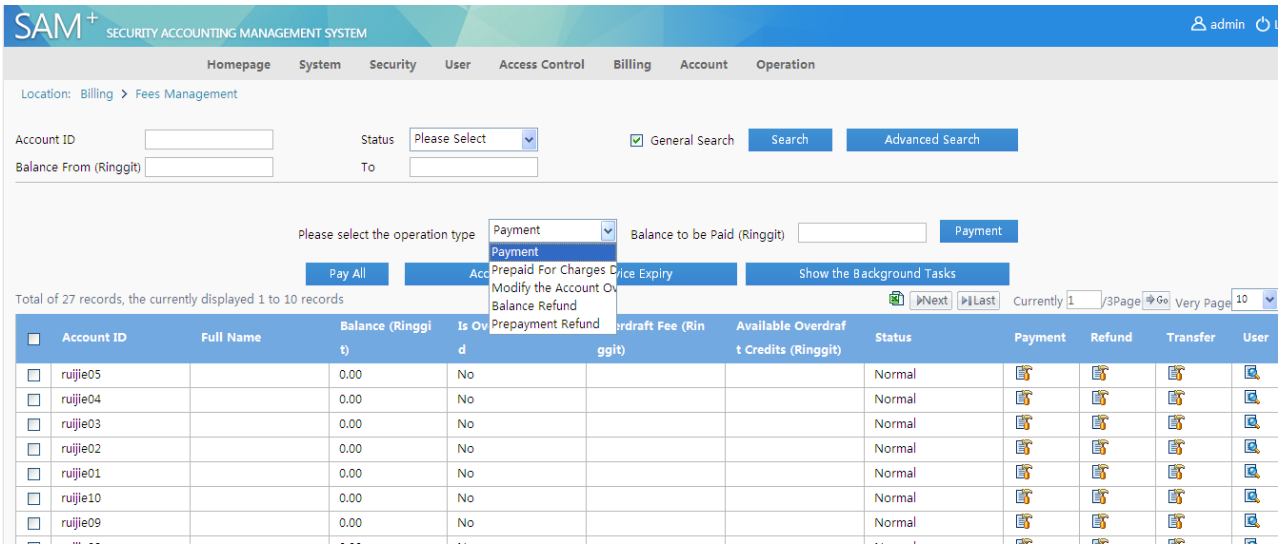
Choose **Billing**>**Fees Management**, click **Search** or **Advanced Search** to search for required accounts for payment, as shown in the following figure.



Choose an account, and click  in the **Payment** column. The payment page is displayed, as shown in the following figure.



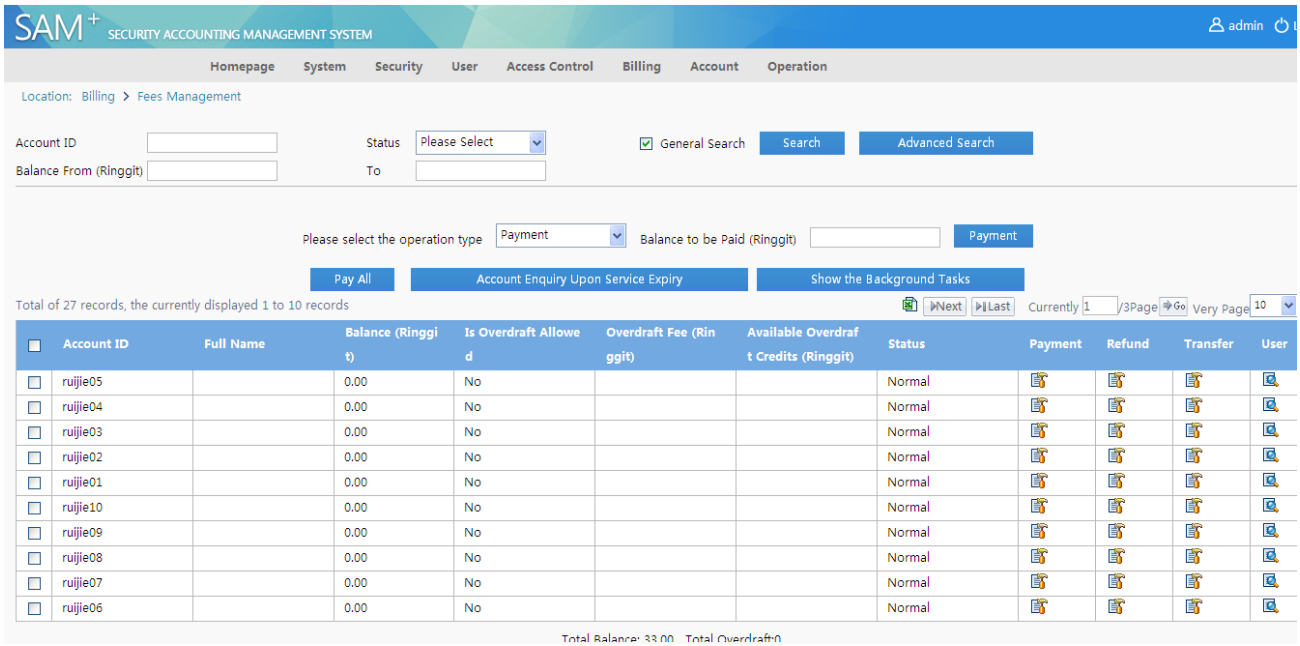
The RG-SAM+ system provides the functions of multiple and all payment. Choose **Billing>Fees Management**. Select accounts in the account table. Choose the operation type, enter the amount to be paid in **Balance to be Paid**, and click **Payment** to pay for selected accounts, as shown in the following figure. If you click **Pay All**, payment is conducted for all accounts that are searched out (all records in the list). It may take a long time to pay for all the accounts, and the specific operation process is displayed at the background. You can click **Show the Background Tasks** for details.



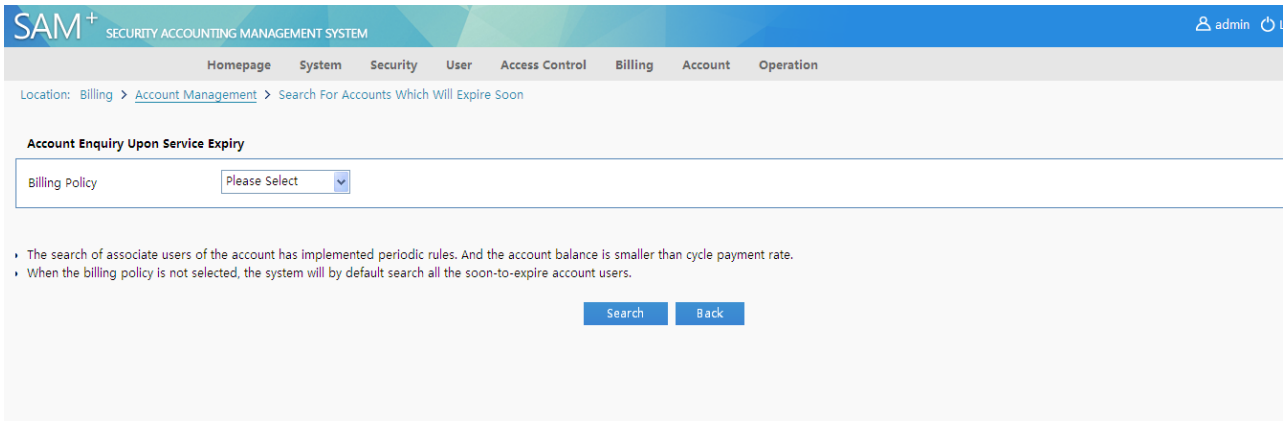
Account credit line modification and balance refund can be also performed on accounts. The operation method is similar to that of batch payment. The batch modification of credit lines is applicable only to accounts that can be overdrawn.

Other Operations

On the **Billing**>**Account Management** list page, you can view, modify, delete, and print account information. You can click an operation button behind an account in the list to perform the required operation, as shown in the following figure.



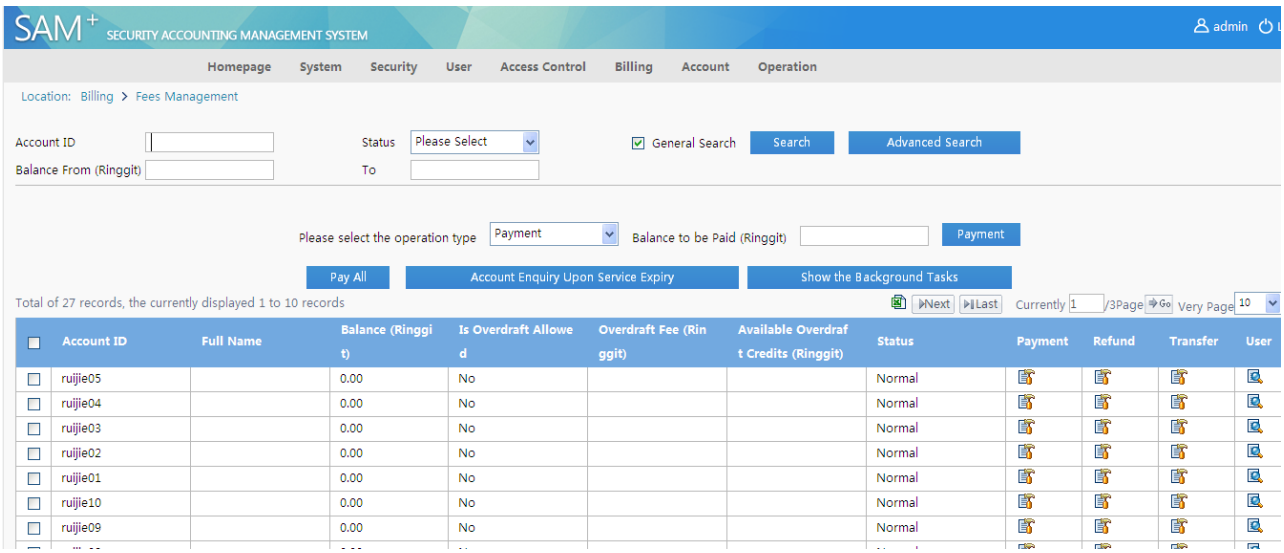
Click **Account Enquiry Upon Service Expiry** to view information about the time of arrearage or overdraft.



When using **Advanced Search**, you can search for accounts based on whether accounts are associated with users. A user associated with an account may be cancelled but the account is kept for reconciliation. For such a case, you can use the search function to search for accounts that are not used.

On the **Billing**>**Fees Management** page, you can perform refund and transfer operations on accounts by clicking  behind an account in the list, as shown in the following figure.

The RG-SAM+ system supports the refund of online users. When a user is online, the refund operation will force the user to go offline and blacklist the user for 2 minutes, ensuring that the user will not go online again during refund.



Fee Deduction

An account is a place for depositing money. The billing policy defines how to deduct fees from accounts. In the RG-SAM+ system, a user is associated with a user template, in which various billing plans are configured and different plans can use different billing policies. Therefore, users are associated with billing policies.

The description above shows that the RG-SAM+ system supports three types of billing. The following describes preparations for the three types of billing.

Preparations for Authentication Device Traffic Billing

A switch supporting RADIUS accounting is required, such as Ruijie Networks RG-2126G switches, RG-ePortal, and R36*XX* series VPN routers.

Configuration on a Switch

The following uses the RG-2126G switch as an example to describe the billing configuration. For details, see the configuration descriptions of Ruijie Networks switch products. The billing configuration is simple. You need to only register the RADIUS Server (that is, accounting server) after 802.1Xis enabled.

To register the accounting server, telnet to the RG-2126G switch and run the following commands to complete the configuration:

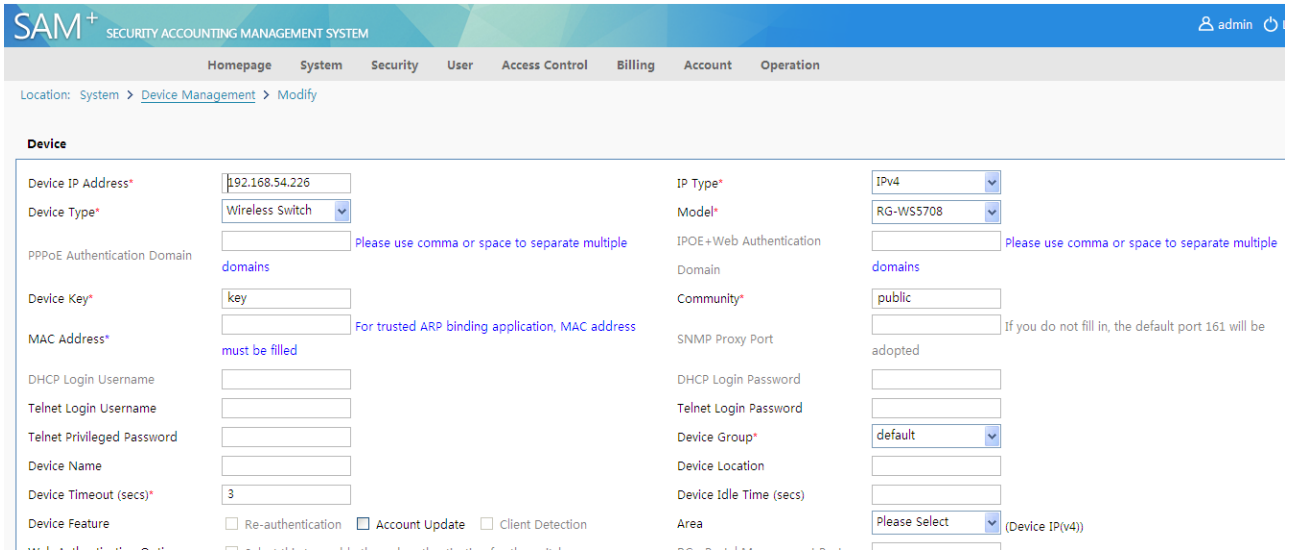
configure terminal	Enter the global configuration mode.

aaa accounting server (ip)	Set the IP address of the RADIUS server.
aaa accounting acc-port (port)	Set the port ID of the RADIUS server.
aaa accounting	Enable the 802.1X accounting function.
end	Exit the global configuration mode.
write memory	Save the configuration.
show accounting	Display the accounting function configuration.

Configuration in the RG-SAM+ System

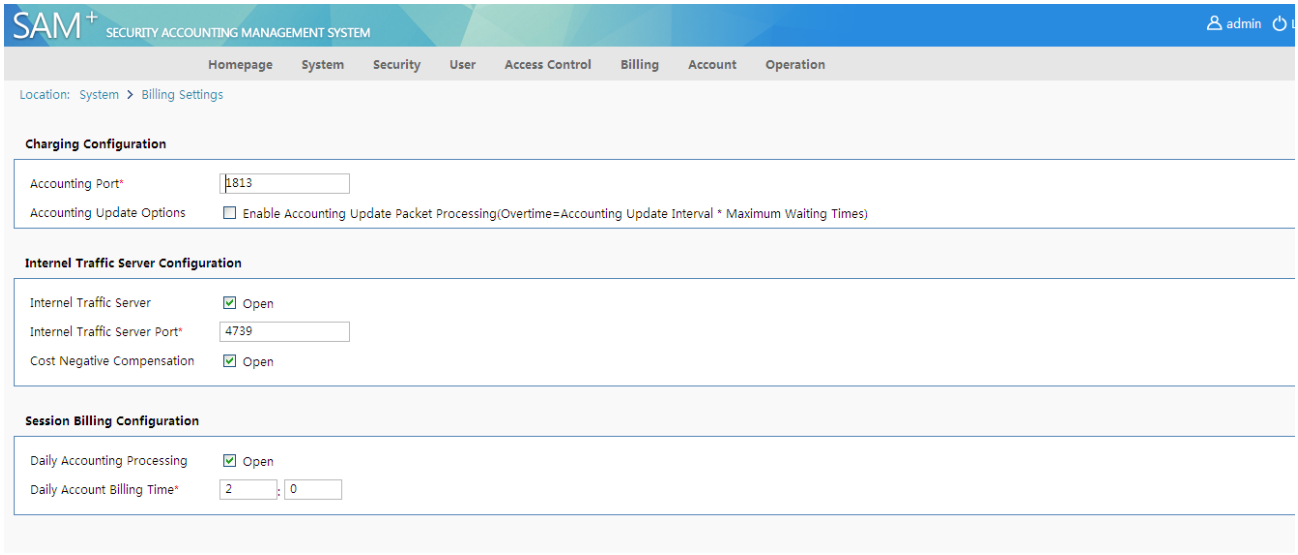
Add a device.

The RG-SAM+ system serves as a RADIUS server and therefore, it must know information about the NAS switch, including **Device IP Address**, **Device Key** and **Community** for the communication between the switch and the RADIUS server, and other optional information. The key and community on the RADIUS server must be consistent with those on the RADIUS client (NAS). Otherwise, authentication will fail. You can choose **System**>**Device Management** from the main menu of the RG-SAM+ system to add a device. The device adding page is shown in the following figure.



Set billing parameters.

After adding the device, set billing parameters in the RG-SAM+ system mainly the accounting port. The default **Accounting Port** is 1813. You can choose **System**>**Billing Settings** from the main menu of the RG-SAM+ system to set billing parameters. The billing parameter setting page is shown in the following figure.



Preparations for Internet Traffic Billing

Internet Traffic Billing is supported on Ruijie Networks RG-RSR77 or RG-ACE, and RG-N18K.

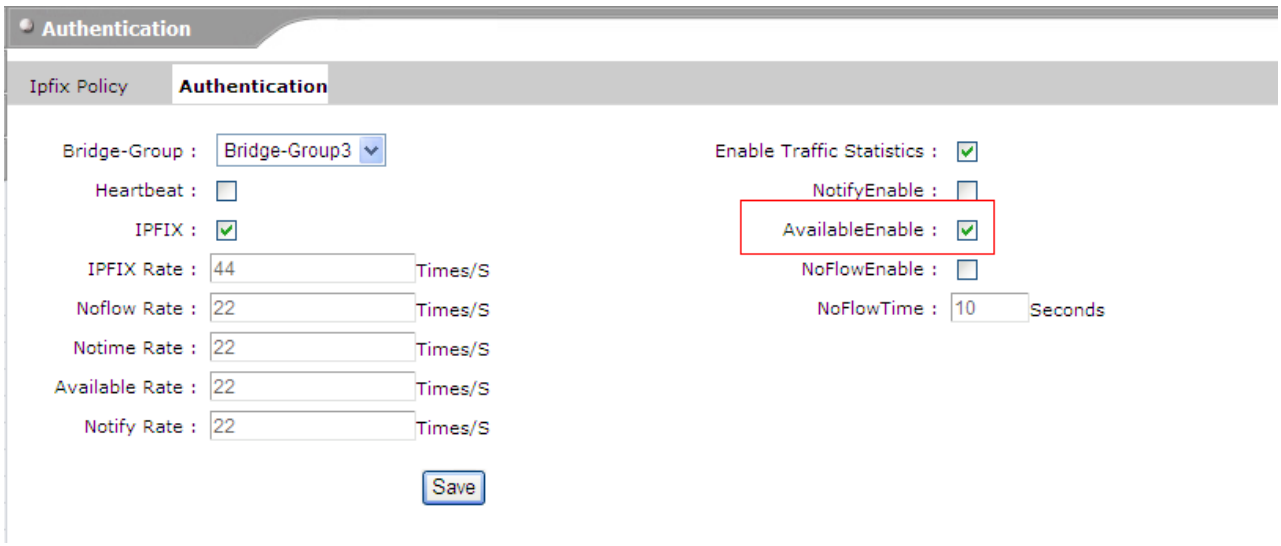
For the configuration of the RG-ACE, see relevant configuration description.

Note

Note

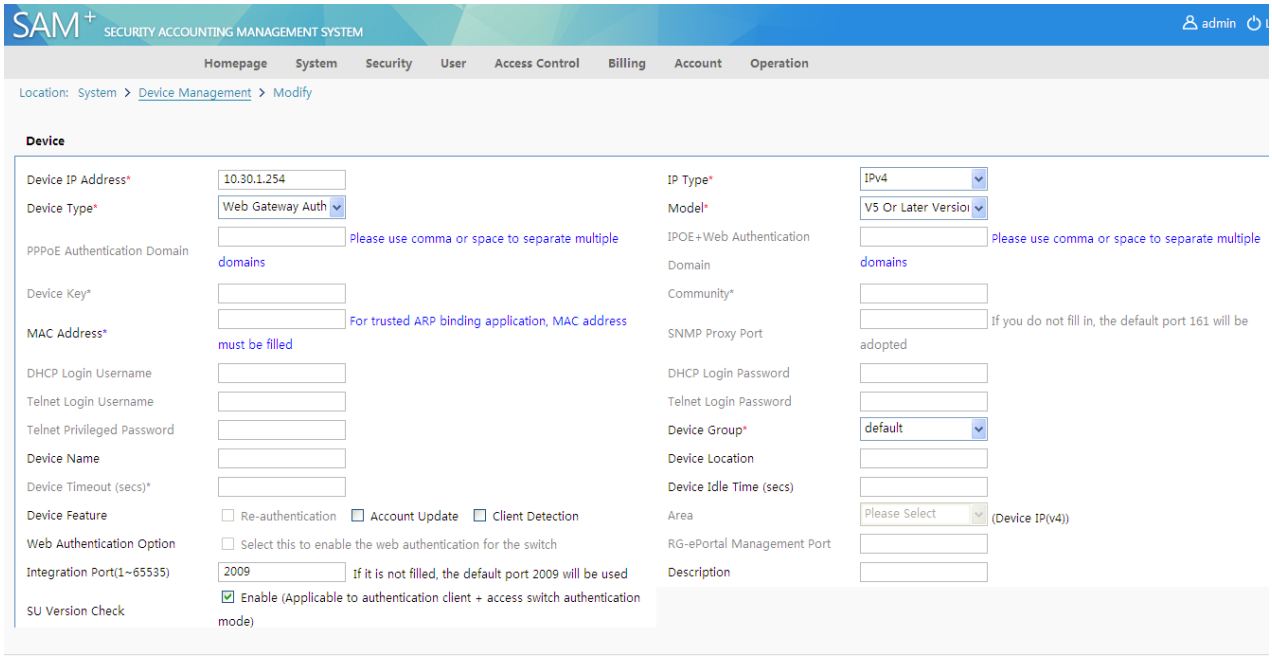
Configuration in the ACE V5

When an Internet traffic billing policy is adopted and the RG-SAM+ system needs to associate with the ACE V5, **AvailableEnable** should be enabled in the ACE, as shown in the following figure. If **AvailableEnable** is disabled, no fee will be deducted for users' Internet access behaviors.

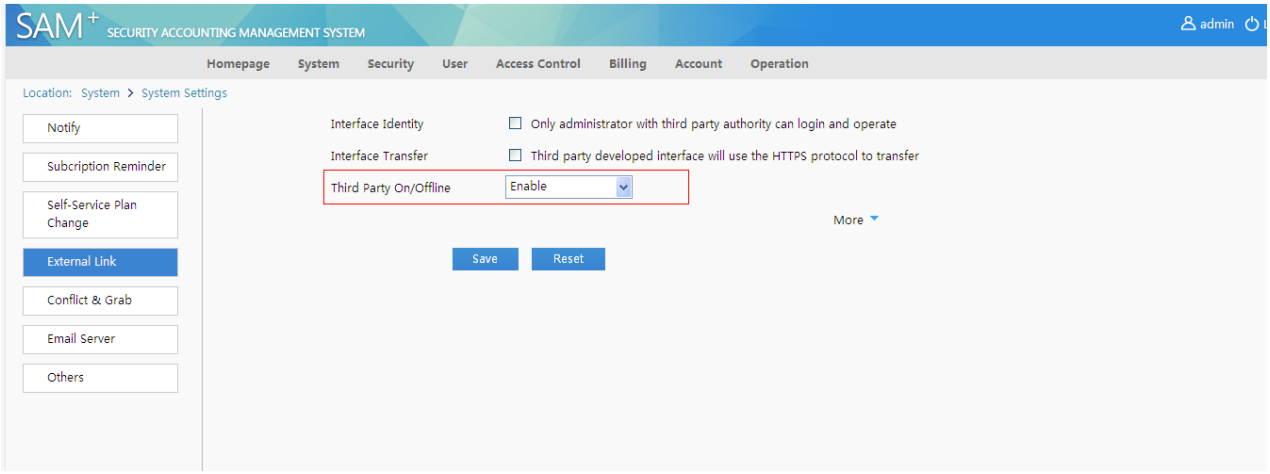


Configuration in the RG-SAM+ System

Add a device: The RG-ACE device must be added to the RG-SAM+ system for management. You can choose System>Device Management from the main menu of the RG-SAM+ system and select RG-ACE from Device Type drop-down list to add a device. The device adding page is shown in the following figure.

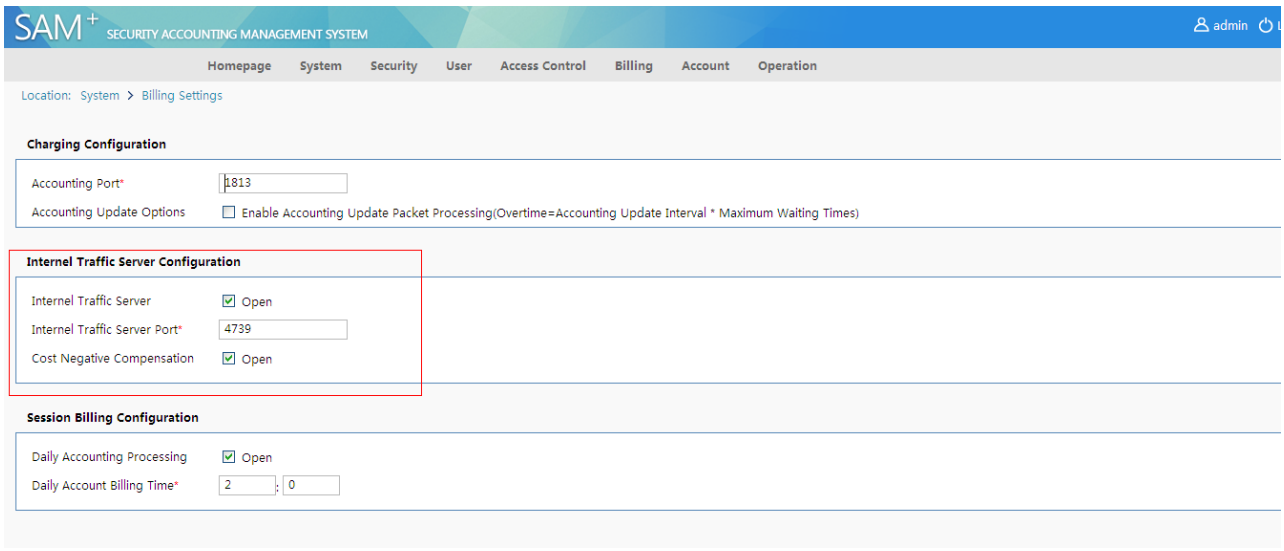


Enable third party online/offline notification: Third Party On/Offline needs to be set to Enable on the RG-SAM+ system so that the RG-SAM+ system interacts with the RG-ACE. You can choose System>System Settings from the main menu, click External Link, and set Third Party On/Offline to Enable, as shown in the following figure.



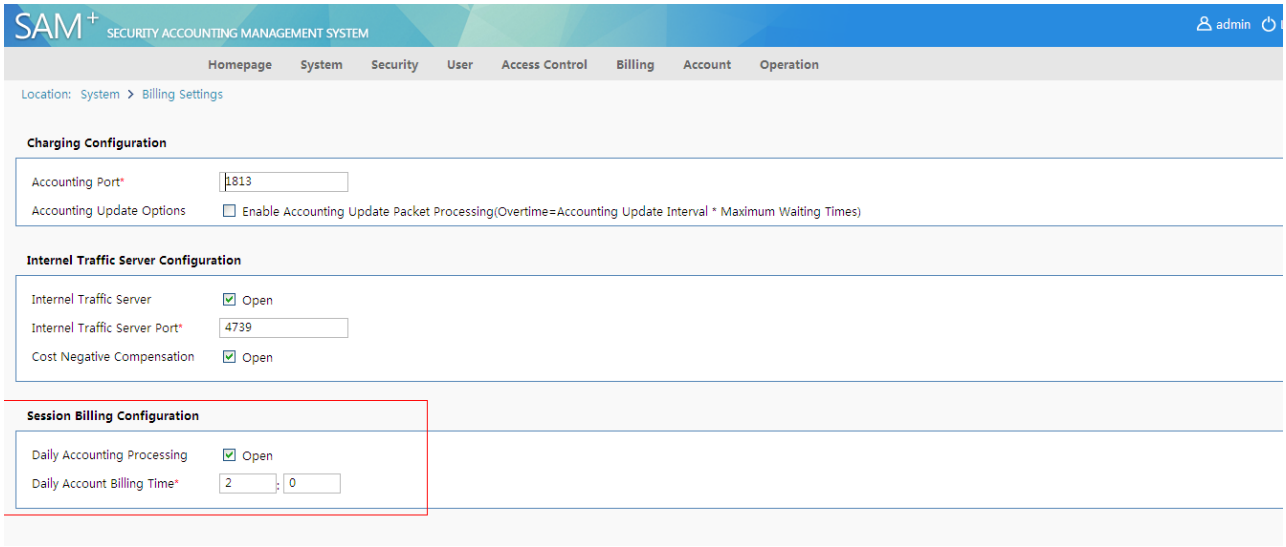
Set billing parameters: Billing parameters relevant to the RG-ACE in the RG-SAM+ system are mainly the startup/shutdown and port configuration of the gateway traffic server. By default, the gateway traffic server is shut down and the default port ID is 4739. To use the Internet traffic billing policy, start the Internet Traffic Server. You can choose

System>Billing Settings from the main menu to set billing parameters. The billing parameter setting page is shown in the following figure.



Preparations for Duration Billing

Duration billing parameters in the RG-SAM+ system includes whether to enable duration billing and the accounting time. The duration billing is enabled by default and the default billing time is 02:00 a.m. You can choose **System**>**Billing Settings** from the main menu and complete configuration in **Session Billing Configuration**. The configuration page is shown in the following figure.



The billing configuration of the RG-SAM+ system takes effect in real time. Real-time synchronization is supported in the NLB environment, but it is not recommended that the configuration be changed frequently.

Configuring Billing Policies

Billing Policies

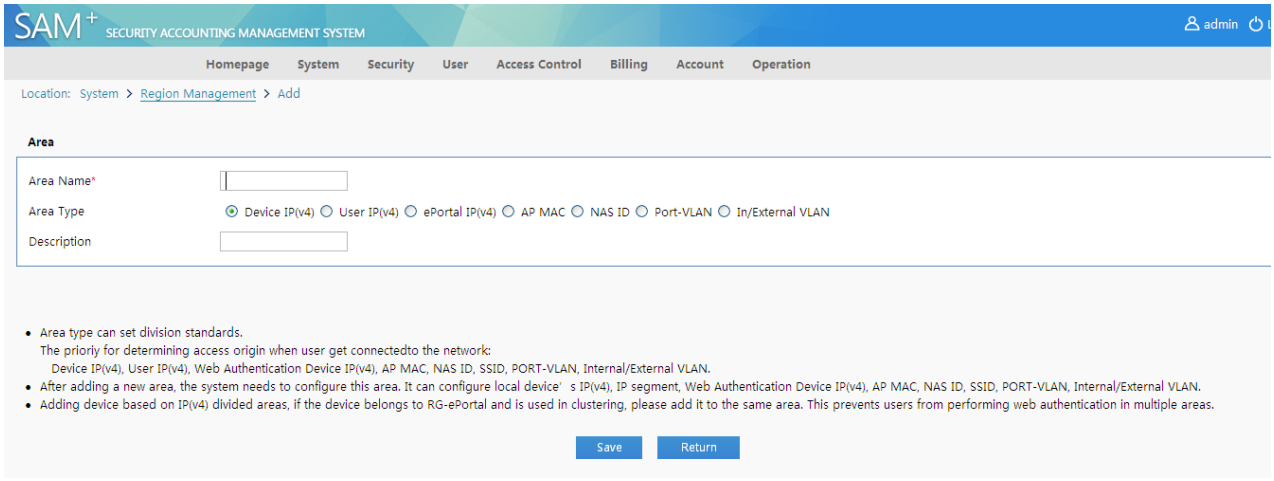
The RG-SAM+ system provides open and flexible billing policies. Besides **Daily Billing Policy** and **Monthly Billing Policy**, **Duration Billing Policy** is supported including yearly, quarterly, and other custom period billing. In authentication traffic billing and Internet traffic billing rules, not only the common rates but also segment rates for accumulations in a period can be set. In addition, the three billing policies can be flexibly combined.

Area-based Billing

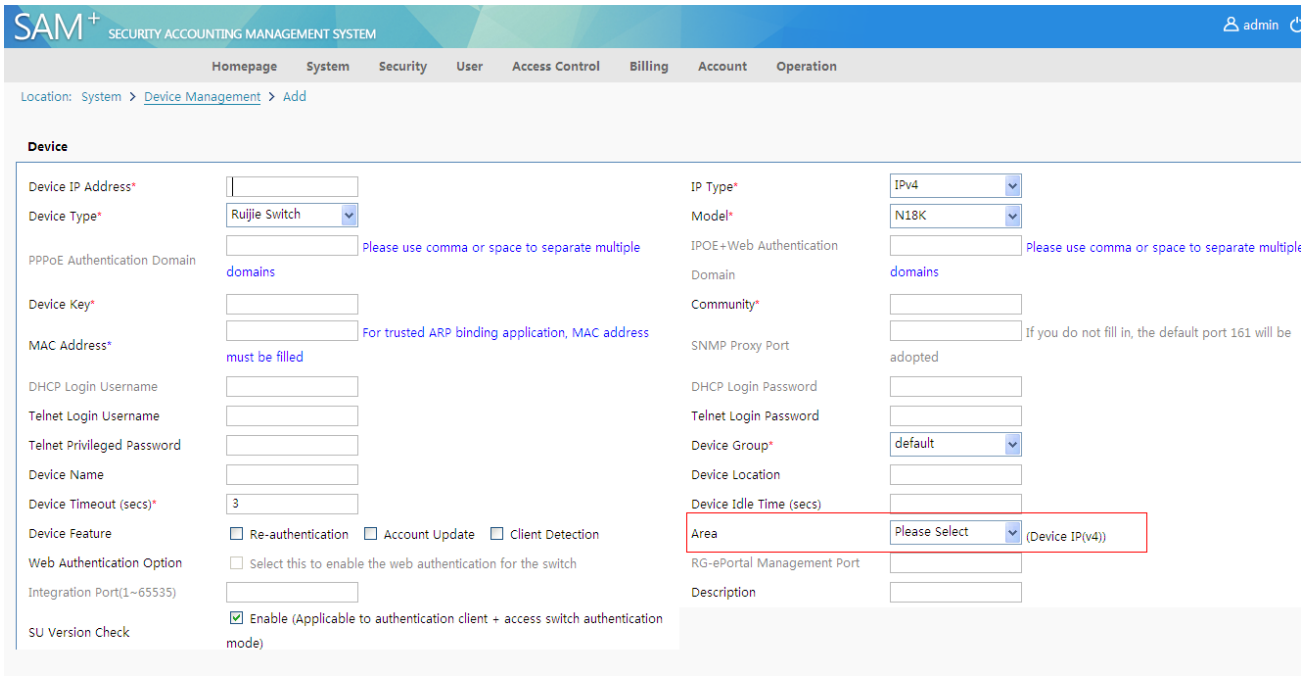
Definition:

The network center requires different billing rules in different areas, as follows: The Internet access service is free of charge in computer rooms and libraries and is charged for 1.00 Ringgit per hour in dormitories. The configuration steps are as follows:

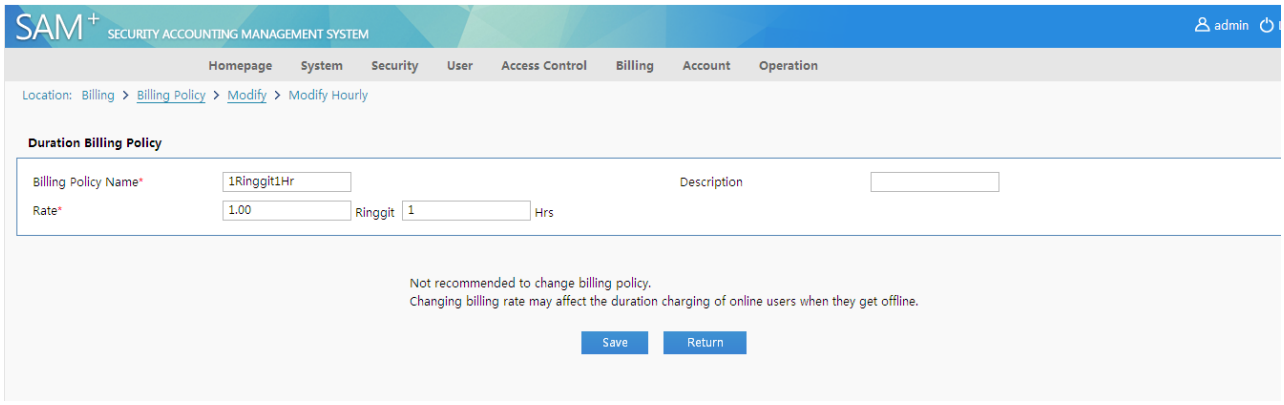
Choose **System**>**Region Management** from the main menu. On the **Region Management** page, click **Add**. On the page that is displayed, enter the **Area Name** to add an area, as shown in the following figure.



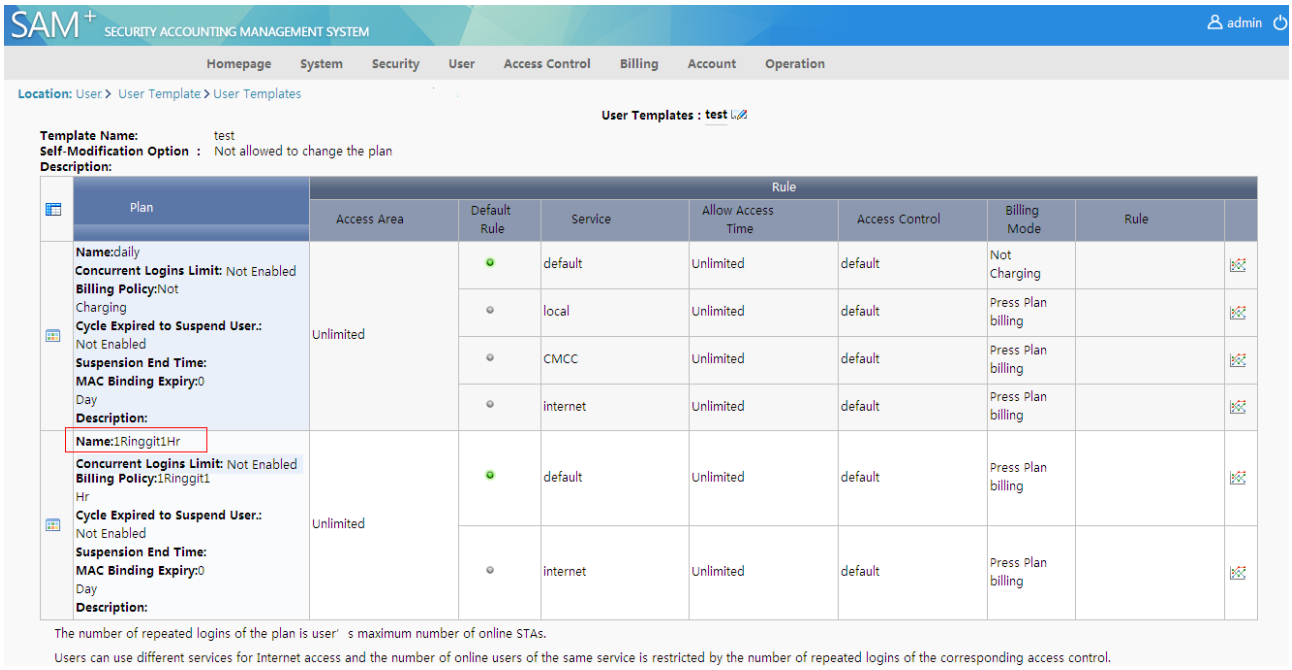
Choose **System**>**Device Management** from the main menu. On the page that is displayed, click **Add** to add a device and set the area attribute for the device, as shown in the following figure.



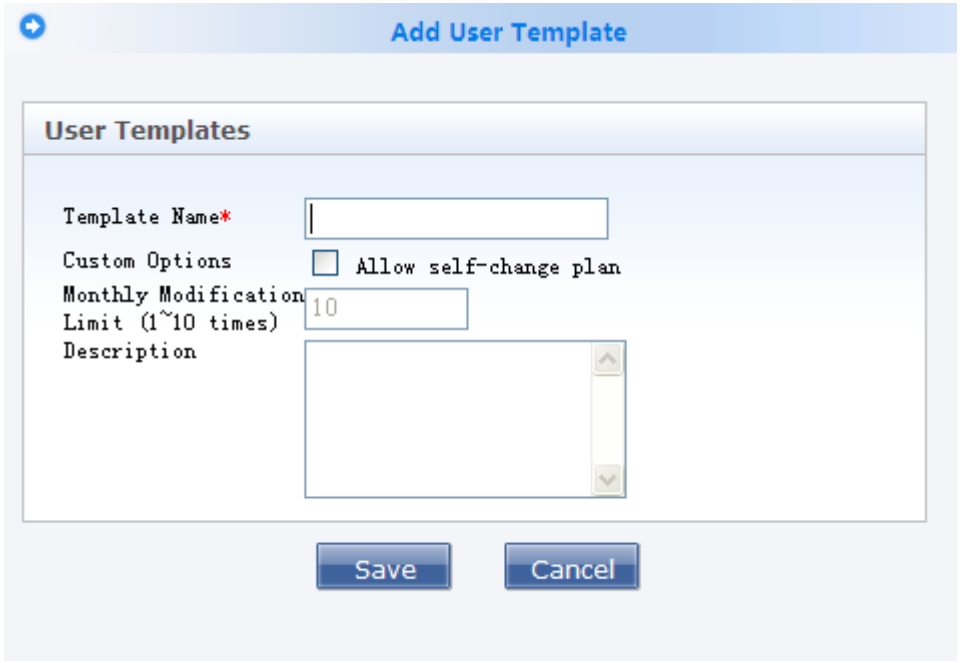
Set **Rate** to **1.00 Ringgit per 1 hour** in **Duration Billing Policy** in **Billing**, as shown in the following figure.



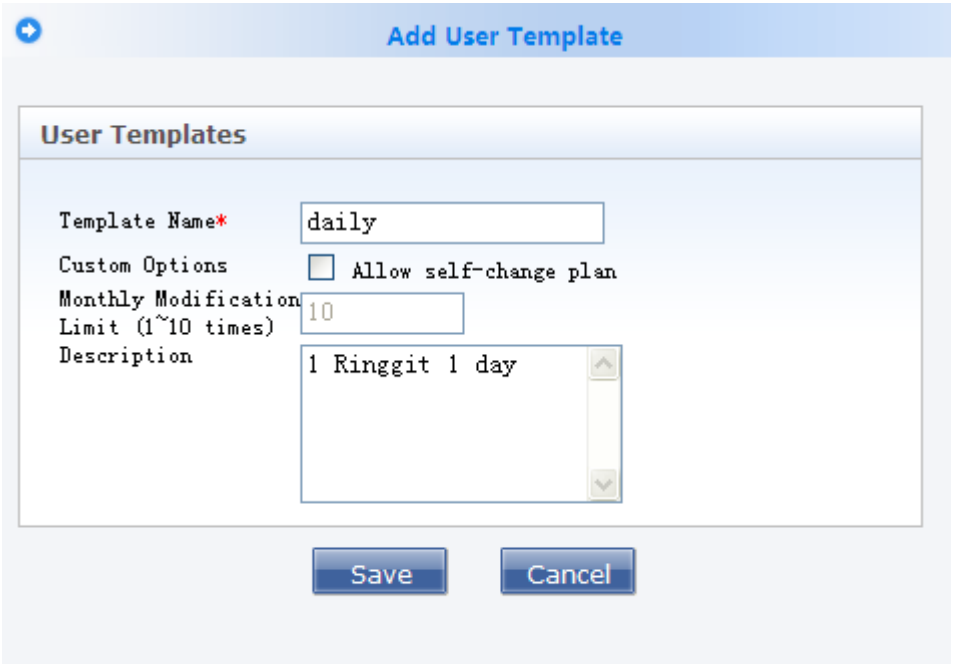
Add a user template named **test**.



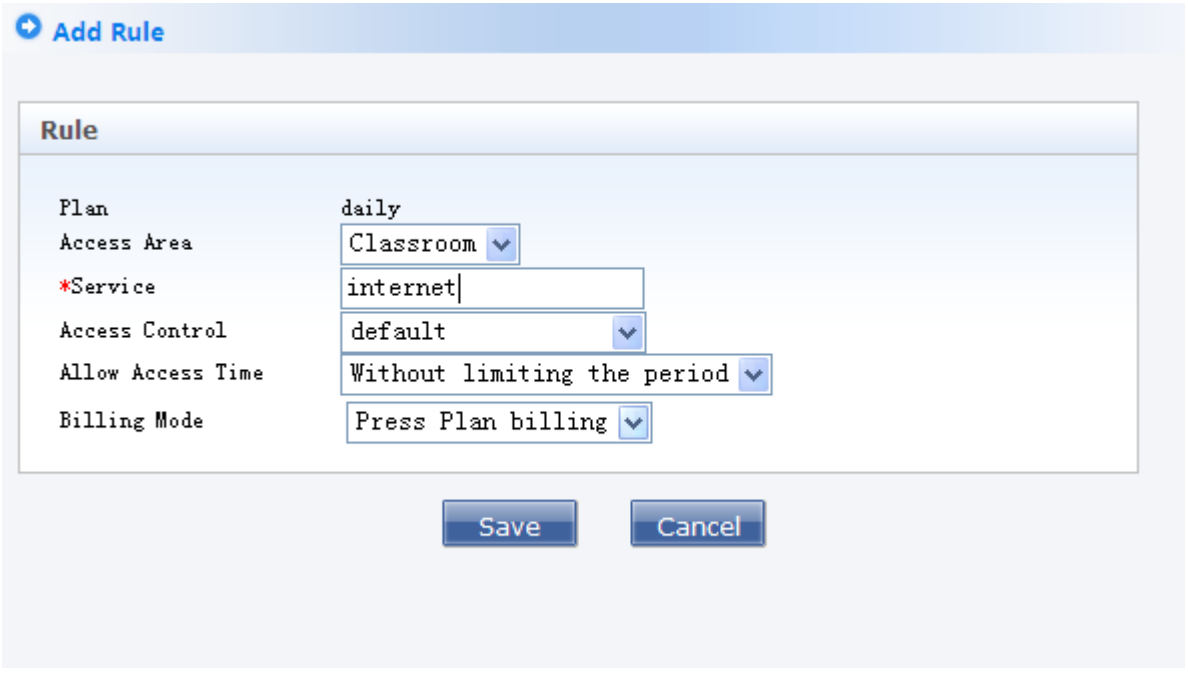
The following describes the procedure for adding a user template. Choose **User Management**>**User Template Management**>**User Templates** from the main menu. Click **Add**. The **Add User Template** page is displayed, as shown in the following figure.



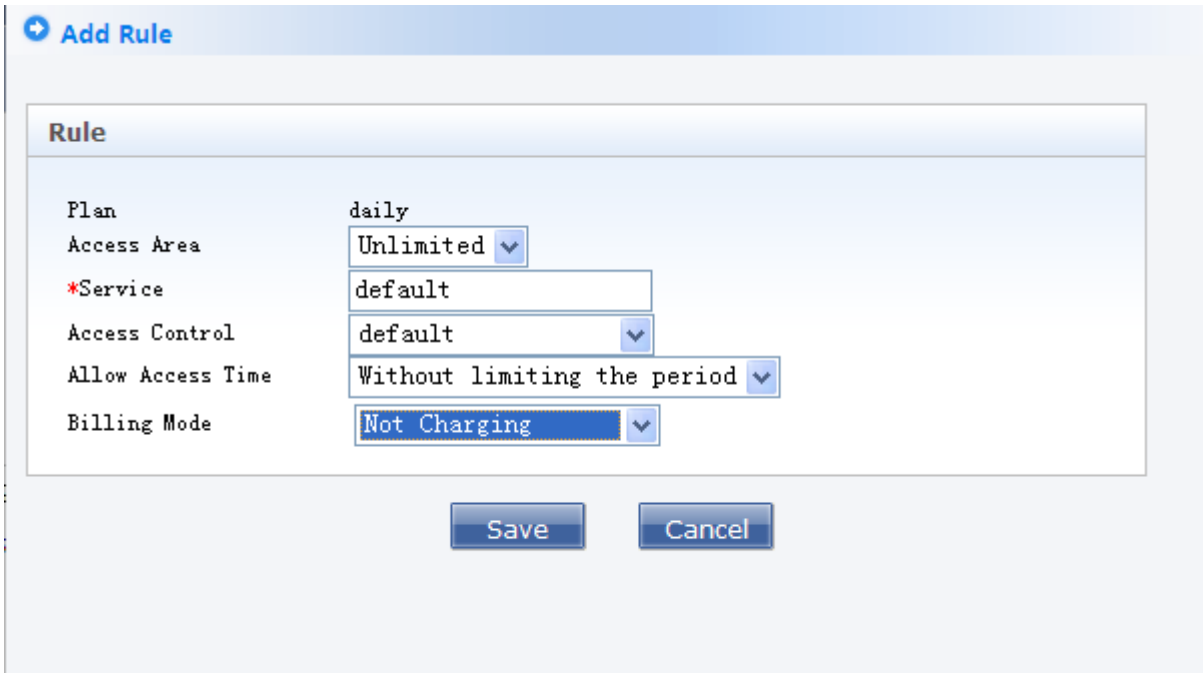
Add a plan named **daily** for the template, as shown in the following figure.



Add two billing rules to the plan, one rule is for classrooms and the other is for other areas. The following figure shows the **Add Rule** dialog box.



Plan-based billing is adopted for classrooms.



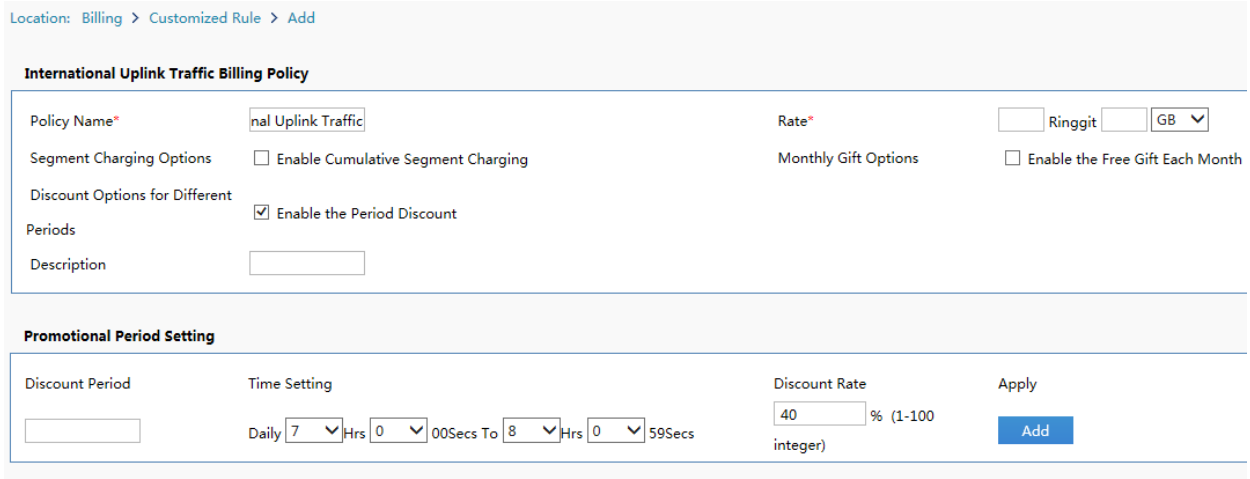
No billing is conducted for other areas.

Associate a new user with the template named **test**. Then, one Ringgit per day is deducted when the user accesses the Internet service in classrooms, and no fee is deducted when the user accesses the Internet service in other areas.

Period Discount of Traffic

In **Customized Rule**, select **Enable the Period Count** to enable discount for international uplink/downlink traffic and domestic uplink/downlink traffic. When the period discount is enabled, the RG-SAM+ user traffic provided by the ACE will be billed at the configured discount (for example, if the value is set to 40%, only 40% of the fee is deducted).

The following figure shows the page of enabling the period discount in the billing policy of international uplink traffic.



Segment Charging

Definition:

Segment Charging is based on **Duration Billing**. Therefore, a segment billing policy requires one or more duration billing policies to periodically clear users' accumulated traffic.

A period-associated accumulation is the duration accumulation, wireless traffic accumulation, and NTD traffic accumulation of a user in each period. The accumulation is set for the segment billing rule of monthly restricted NTD traffic. If the accumulation of a user reaches the limit, the user cannot access the Internet. The accumulation is cleared and is reset to 0 at the beginning of the next period.

If duration billing is not required, set the rate in the period rule to 0 and set the period length to a large value.

The network center requests the following billing mode: A monthly plan is adopted for users and segment billing is conducted on the gateway traffic of users to prevent the occupation of a large number of network bandwidths because of enormous use of P2P tools such as BT. The billing requirements are as follows: A monthly fee of 10 Ringgit is deducted for each user, the gateway traffic within 0-1 Gbit/s is free of charge, and 2 Ringgit is deducted per Gbit/s traffic if the gateway traffic is larger than 1 Gbit/s. The configuration steps in the RG-SAM+ system are as follows:

Choose **Billing**>**Customized Rule** from the main menu and add segment rules for total Internet traffic on the page that is displayed.

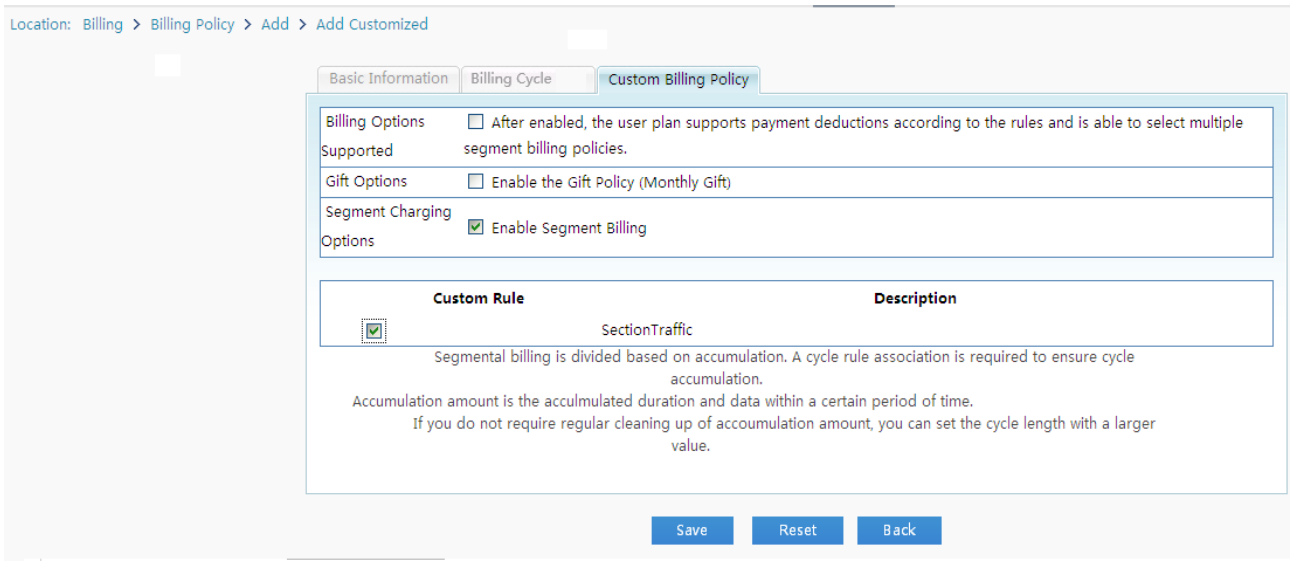
Pay attention to the following point: If the rate is set from 0 to *x* (multiple intervals are allowed) but no rate is set from *x* to infinitely large, the traffic consumed by a user using this billing policy cannot exceed *x*. If yes, the user cannot access the Internet any more. A 50 days-contained billing policy can be configured as follows: set the period to 50 days, period fee rate to 20 Ringgit, rate for the interval from 0-100 hours to 0, and rate for the interval from 100-200 hours to 1 Ringgit. Do not set the rate for the interval from 200 hours to infinitely great. Users using the billing policy cannot access the Internet after consuming 200 hours within 50 days (including free 100 hours and paid 100 hours).

Restrictions:

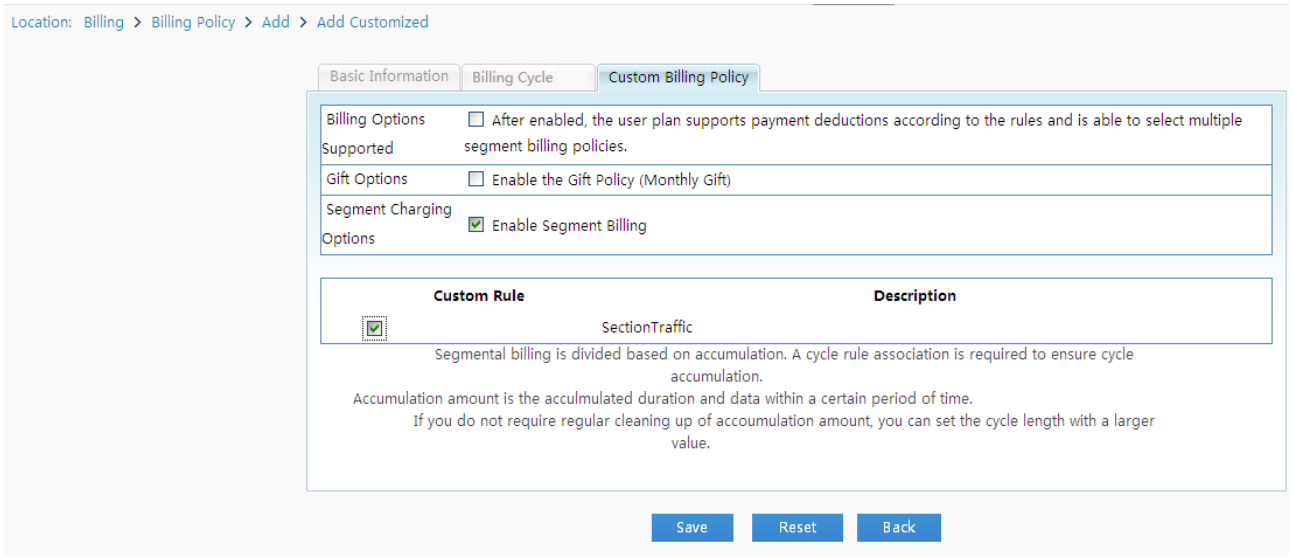
1) Only the total Internet traffic is supported.
2) The **Partition Activation Fees** can be charged for each segment and can be deducted when a user goes online.
3) The RG-SAM+ system sends only the available traffic in an interval to the ACE during authentication.
4) A user is forced to go offline after the traffic in a segment is used up.

Defining policies:

Choose **Billing**>**Billing Policy** from the main menu. On the page that is displayed, click **Add** and then click **Add Customized**. Click the **Billing Cycle** tab and set the period rate to 10 Ringgit/month, as shown in the following figure.



Choose **Billing**>**Billing Policy** from the main menu. On the page that is displayed, click **Add** and then click **Add Customized**. Click the **Custom Billing Policy** tab, select **Enable Segment Billing**, and select the segment rule set in the previous step, as show in the following figure.



Billing Policy Combination

In addition to preceding billing policies, multiple rules can be flexibly combined. Nevertheless, the following limitations exist:

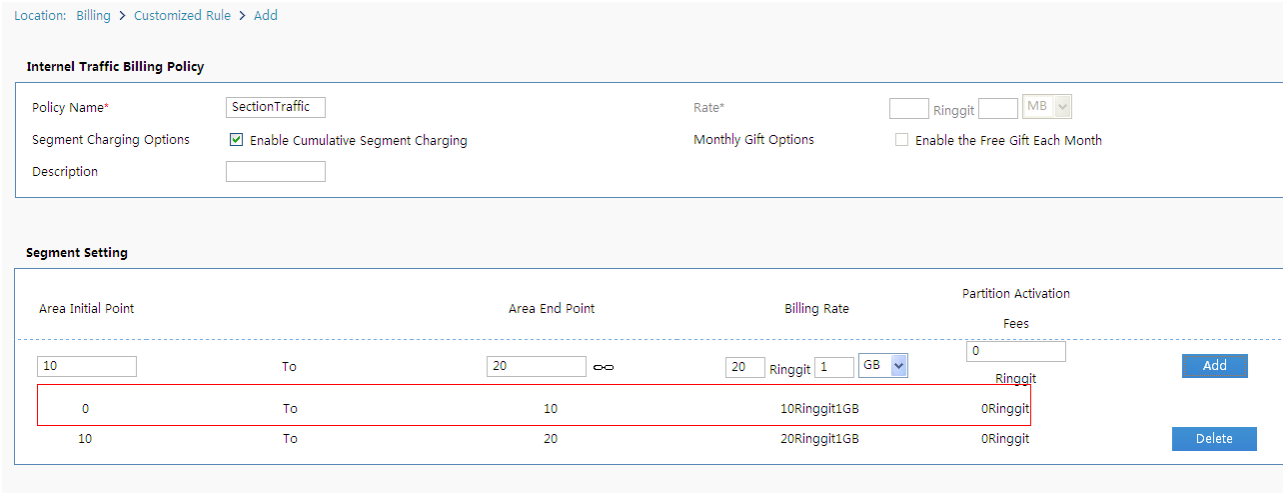
A segment charging rule must be associated with a duration rule.

Only one segment rule can be set if segment billing is adopted.

A segment rule cannot cover the total gateway traffic and traffic of each subcategory at the same time.

For example, the network center requests the following billing policy: A monthly fee of 10 Ringgit is deducted for each user, a total of 1 Gbit/s gateway traffic is free of charge, and 1 Ringgit per hour is deducted if the total gateway traffic exceeds 1 Gbit/s. The configuration procedure in the RG-SAM+ system is as follows:

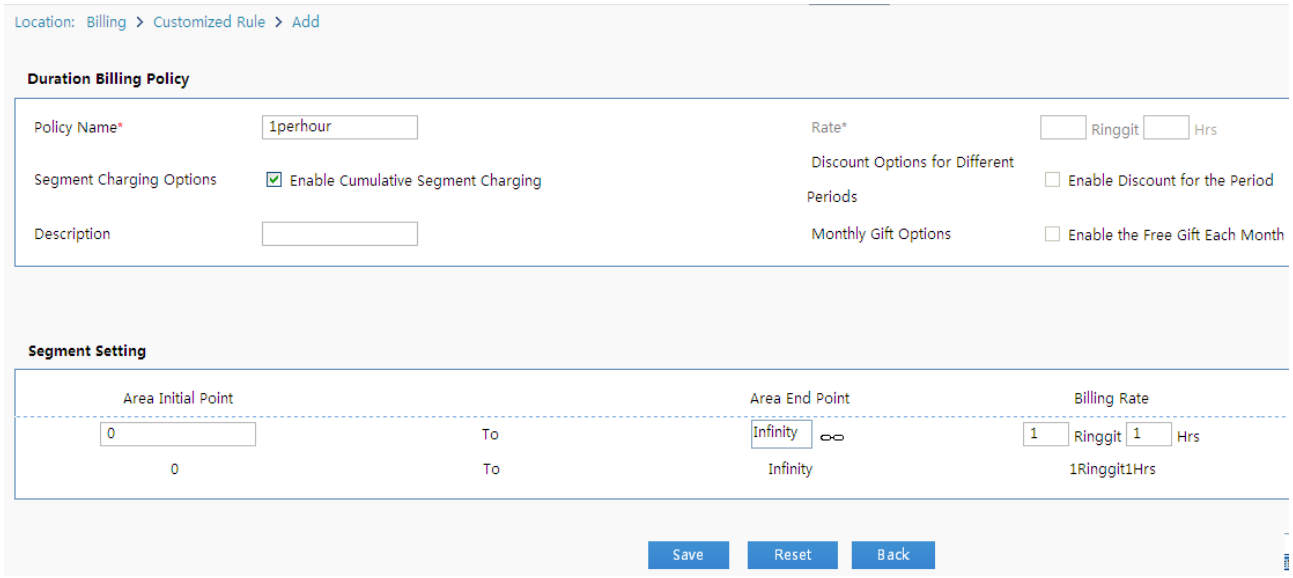
Choose **Billing**>**Customized Rule** from the main menu. On the page that is displayed, click **Add** and add segment rule for total gateway traffic, as shown in the following figure.



Note

Only one segment is set, as shown in the preceding figure, the traffic from 0-1 Gbit/s is free of charge, indicating that a user is allowed to use a maximum of 1 Gbit/s traffic.

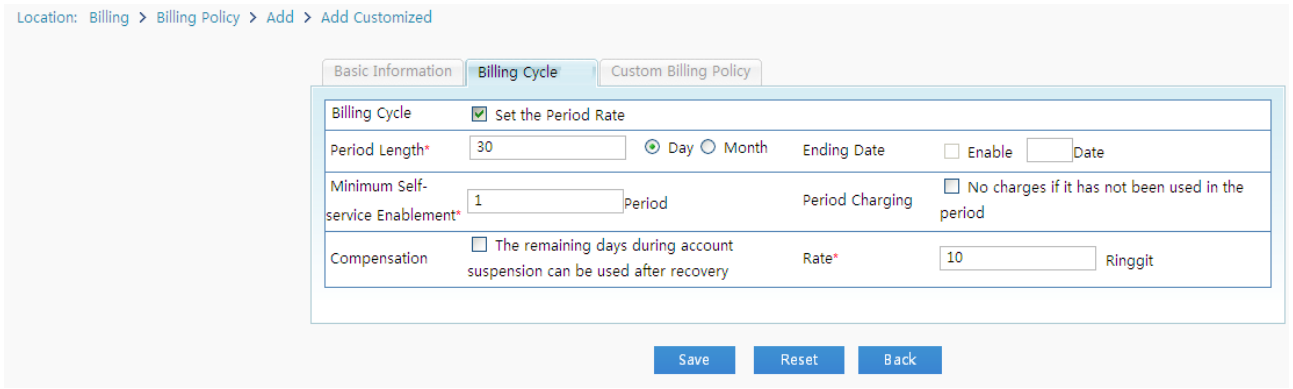
Choose **Billing**>**Customized Rule** from the main menu. On the page that is displayed, click **Add** and add a duration-based segment rule, as shown in the following figure.



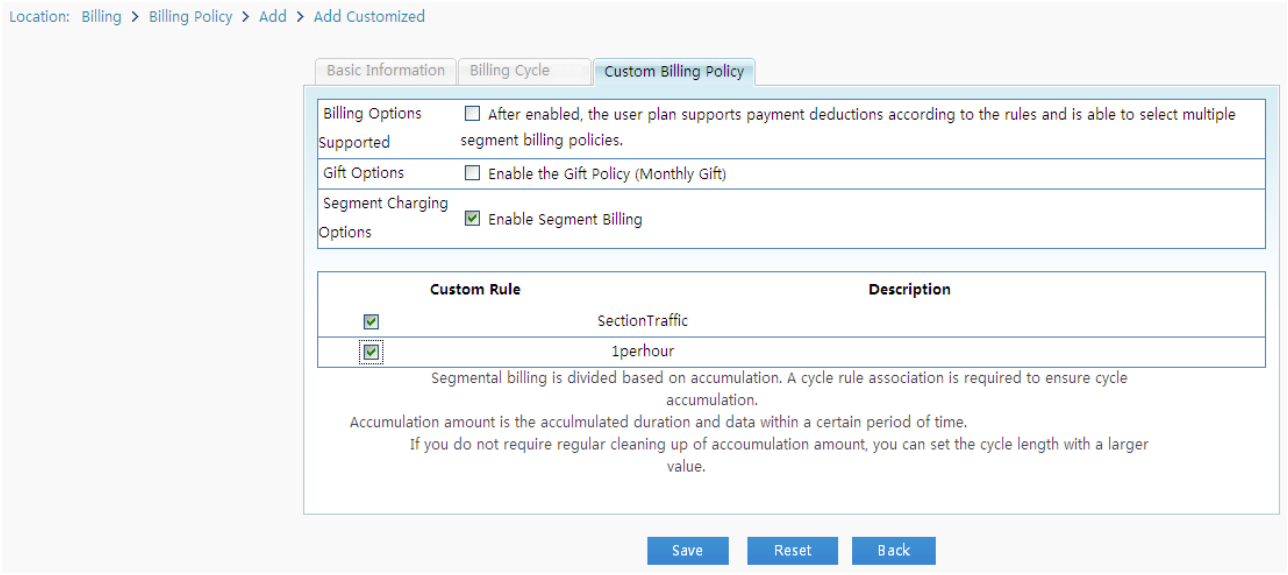
Note

The interval from 0 to infinitely great is a special segment, indicating that no segment is adopted and the rate is 1 Ringgit/hour.

Choose **Billing**>**Billing Policy** from the main menu. On the page that is displayed, click **Add** and then click **Add Customized**. Click the **Billing Cycle** tab and set the period rate to 10 Ringgit/month, as shown in the following figure.



Choose **Billing**>**Billing Policy** from the main menu. On the page that is displayed, click **Add** and then click **Add Customized**. Click the **Custom Billing Policy** tab, select **Enable Segment Billing**, and select the segment rule, as show in the following figure.



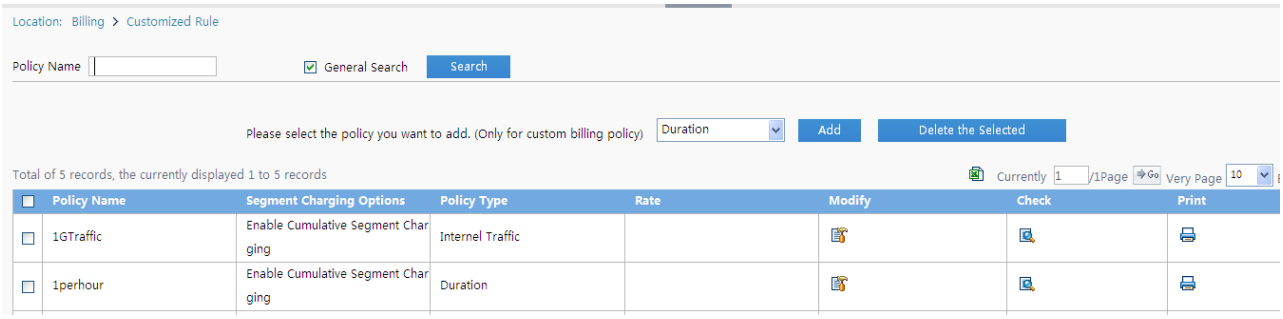
When a user uses multiple Internet billing policies (for example, combination of domestic uplink traffic and domestic downlink traffic) simultaneously, the RG-SAM+ system allots the fees to different types of traffic on average intelligently.

Different Billing Rules for Different Services

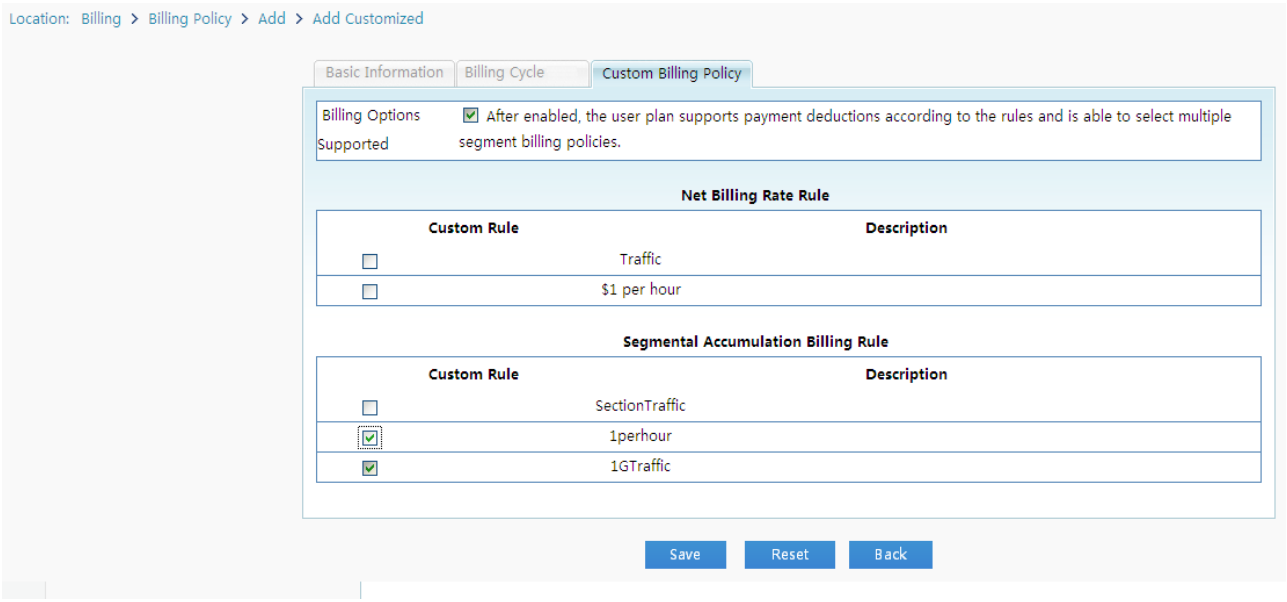
The billing policy of different billing rules for different services is added to adapt to more flexible plan use. In this billing policy, the billing is conducted on the same type of traffic at different rates in one plan (for example, in a plan, service A is charged 1 Ringgit/hour and service B is charged 2 Ringgit/hour).

The configuration steps of this billing policy are as follows:

1) On the **Customized Rule** page, add required billing rules.



2) On the **Custom Billing Policy** tab, complete the settings, as shown in the following figure.

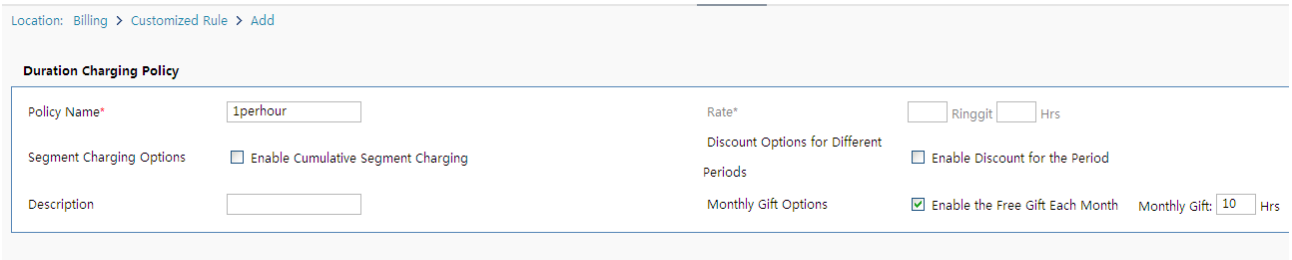


If you select **Billing Options Supported**, the current billing policy uses different billing rules for different services. Existing billing rules of the RG-SAM+ system are displayed in the lower part of the page and can be selected.

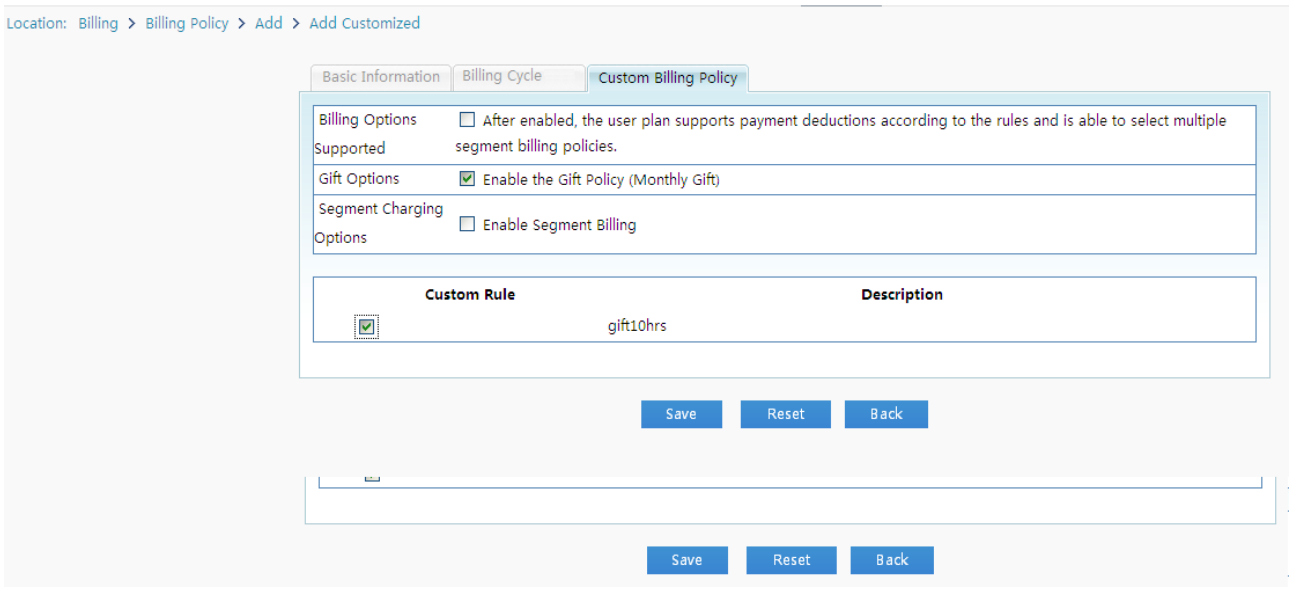
Note: For the configuration of the plan using different billing policies for different services, see "User Template."

Gift Billing

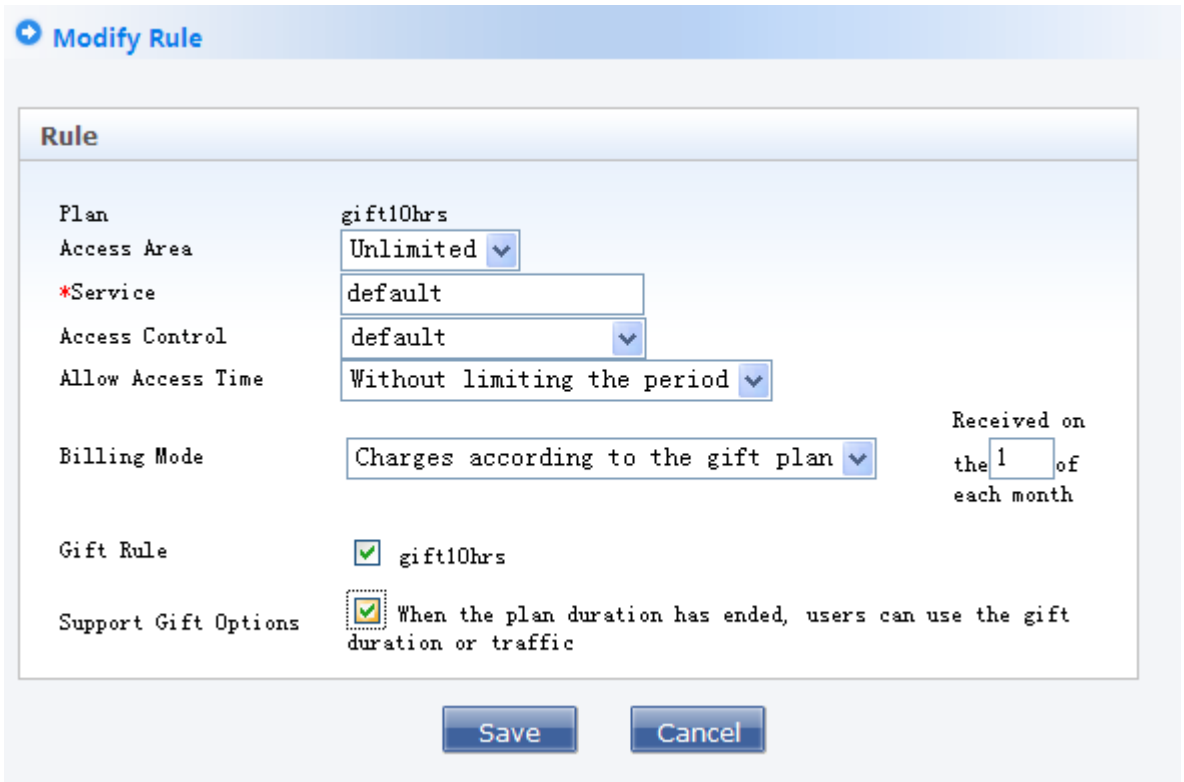
When adding a duration or traffic-based policy on the **Customized Rule** page, select **Enable the Free Gift Each Month** and set the gifted duration or traffic.



When adding a customized billing policy, select **Enable the Gift Policy (Monthly Gift)** and select the configured gift rule.



Add a plan associated with the billing policy in the user template and modify the policy.



Select **Charges according to the gift plan** from the **Billing Mode** drop-down list and set the gift date and gift rule. If **Support Gift Options** is not selected, a user cannot use the gifted duration when the account balance of the user is insufficient to activate the current period. After **Support Gift Options** is selected, a user can still use the gifted duration even if the account balance of the user is insufficient to activate the current period.

Changing Billing Policies

It is recommended not to change the billing policy, but to create one to replace it. The rate modification may have an impact on the duration- or gateway traffic-based billing of online users when they go offline. After the rate in a duration billing rule is modified, the modified billing policy can be synchronized to other hosts in the network load balancing (NLB) environment.

A modified billing policy can take effect immediately or in next period.

Till now, you must have a full understanding of the rich and flexible billing function of the RG-SAM+ system.

The billing output is account flows, which are the input of the accounting module. The billing module calculates the fee of a user, deducts the fee from the user's account balance, and generates an account flow. Multiple account flows can be generated for multiple billing rules, for example, account flows are generated for duration-based billing and gateway traffic-based billing.

You can view accounting summaries and statements to query account flows. For details, see the subsequent accounting module description.

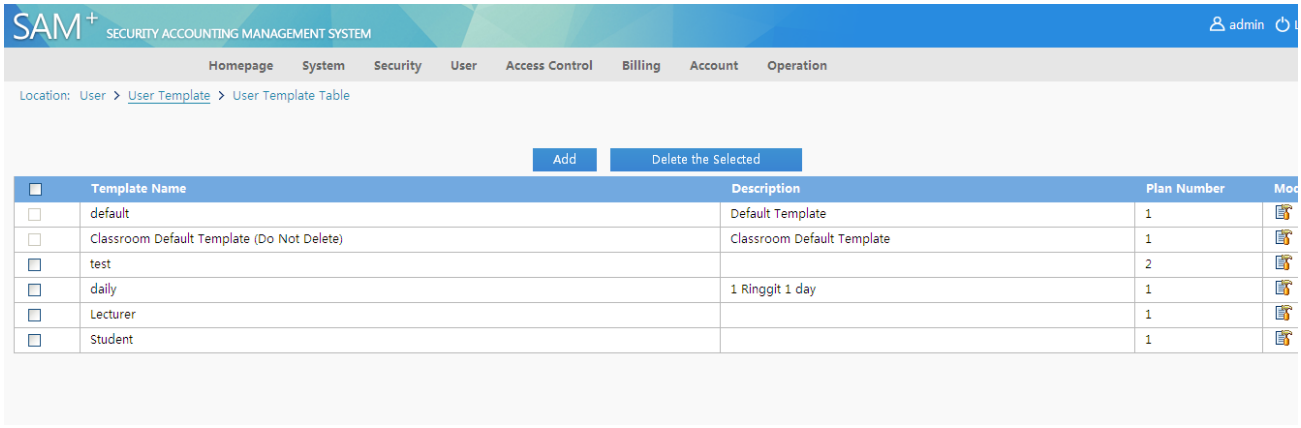
User

Overview

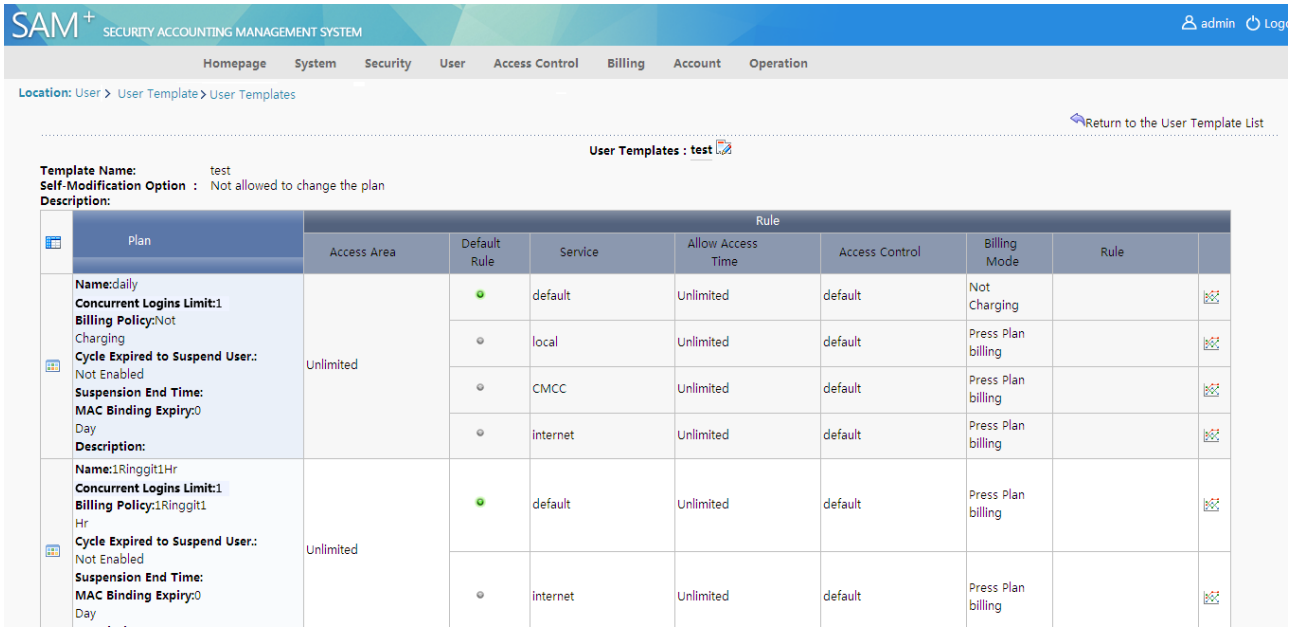
Users of the RG-SAM+ system include users accessing the Internet through the RG-SAM+ system and users managing the RG-SAM+ system. User is a basic concept in the system and is closely related to other modules. For details about services associated with users, see "User Prototype of the RG-SAM+ System."All services of the RG-SAM+ system are provided to users. The services are meaningless if there are no users in the RG-SAM+ system. In the RG-SAM+ system, users include normal users, system administrators, device administrators, and customized administrators.

User Template

User templates can combine billing policies, areas, and access rules. You can quickly set billing policies and services for users by using a user template, and complete unified settings on all users in a user group by using the default template of the user group. For relevant operations, see user management and user group management.



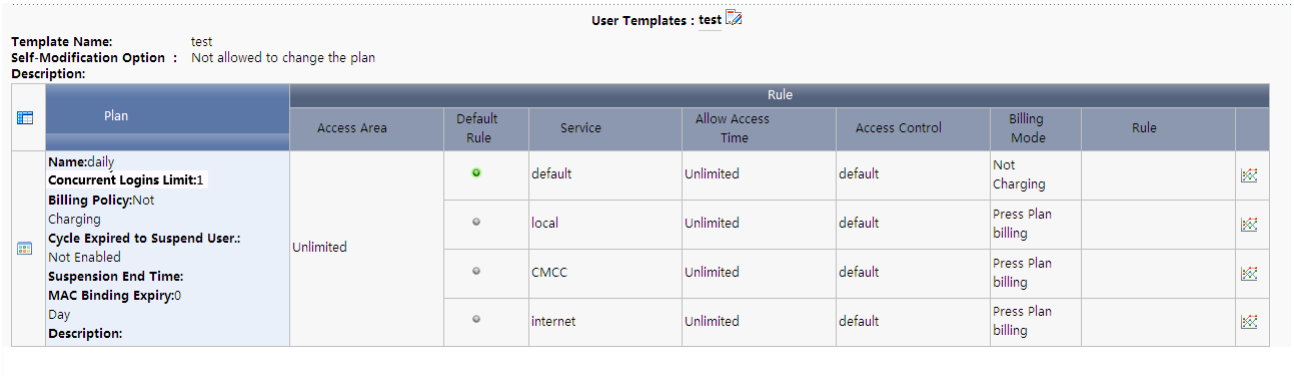
On **User Template**, you can add, delete and modify user templates. The following illustrates how to add a user template, including adding/modifying/deleting a plan, and adding/deleting/modifying a rule.



Multiple plans can be added to one user template, one plan can contain multiple rules, and a rule can be associated with services, access control, and access time slots. The operation of adding a user template is described as follows:

Choose **User**>**User Template** from the main menu. In the user template list, click **Add**. The **Add User Template** page is displayed.

After adding a template, you can add a plan to the template. The operation of adding a plan is described as follows:

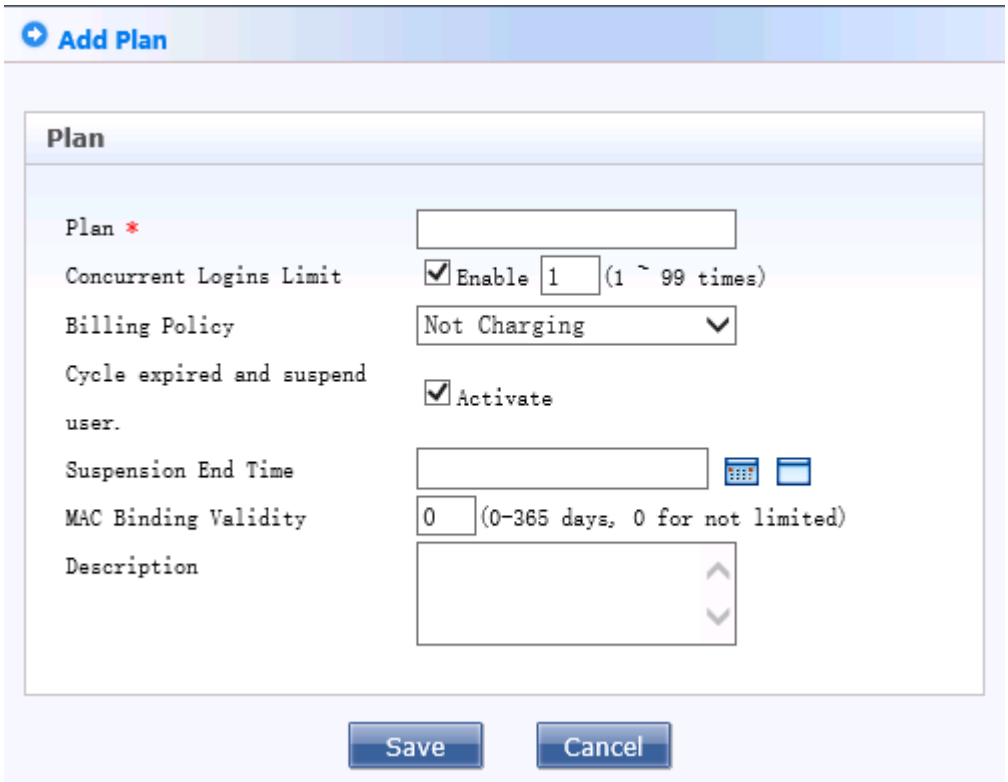


User Templates : test

Template Name: test
Self-Modification Option : Not allowed to change the plan
Description:

Plan	Rule							
	Access Area	Default Rule	Service	Allow Access Time	Access Control	Billing Mode	Rule	
Name:daily Concurrent Logins Limit:1 Billing Policy:Not Charging Cycle Expired to Suspend User.: Not Enabled Suspension End Time: MAC Binding Expiry:0 Day Description:	Unlimited	●	default	Unlimited	default	Not Charging		
		○	local	Unlimited	default	Press Plan billing		
		○	CMCC	Unlimited	default	Press Plan billing		
		○	internet	Unlimited	default	Press Plan billing		

Click **Add Plan**. On the **Add Plan** page, fill in the plan parameters and select a billing policy. After a plan is added successfully, a default access rule is created. The **Add Plan** page is as shown in the following figure.



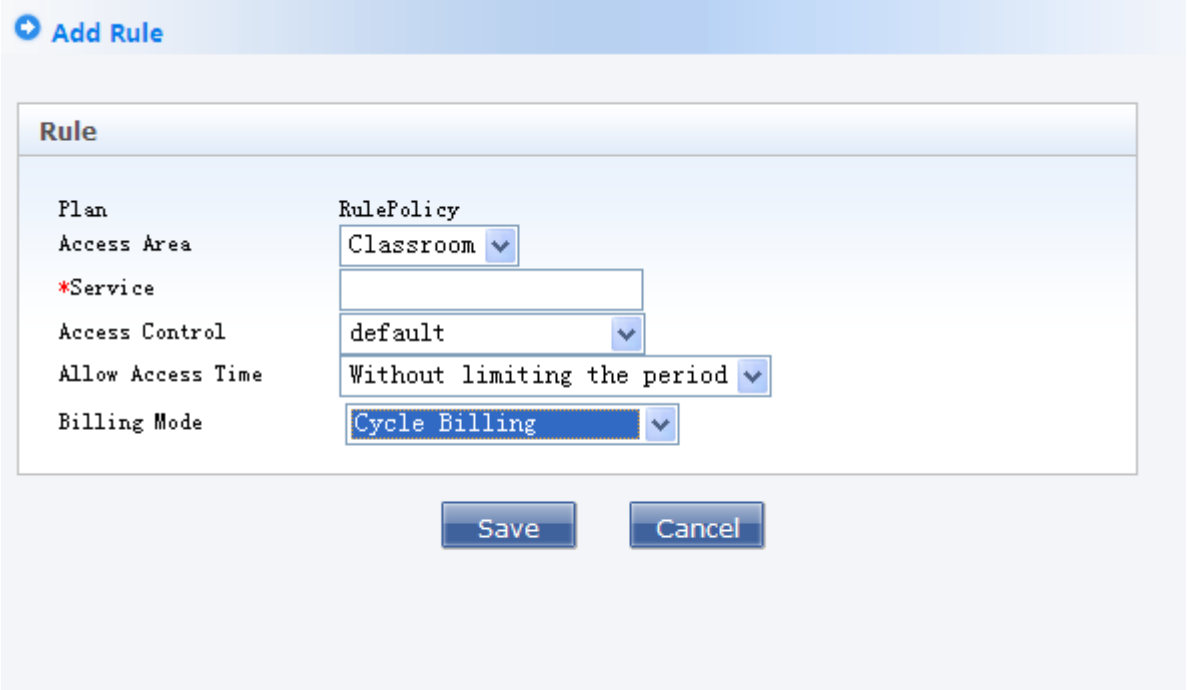
Plan: A plan is associated with a billing policy. After adding a user, you need to select a user template and a plan. Then, the user is associated with the billing policy of the plan.

Cycle expired and suspend user indicates that all users associated with of the plan are in the suspended state after the cycle expires, and the users are not allowed to activate the next cycle even if they have sufficient balance. The **suspension end time** must be set if **Cycle expired and suspend user** is set to **Activate**.

For example, a billing policy associated with a plan is cycle billing, **Cycle expired and suspend user** is set to **Activate**, and the suspension end time is set to September 1, 2013. If the billing time of the next cycle of users associated with the plan is July 2, 2013, the users are suspended (users cannot activate the next cycle, that is, users cannot pass

authentication) on July 2, 2013. The user status is resumed till the suspension end time of September 1, 2013. And the users can successfully activate the next cycle if their balance are sufficient.

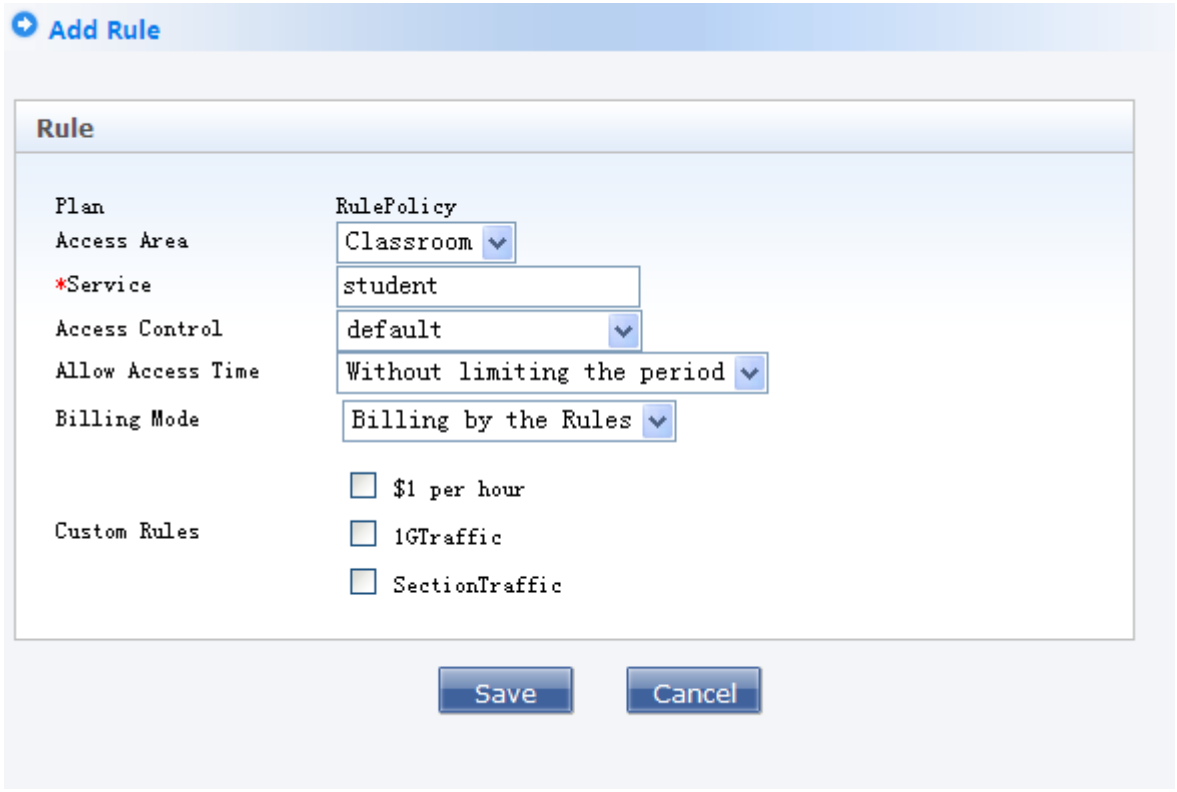
The following describes how to add a rule to a plan. The following figure shows the **Add Rule** page.



Rule: A rule includes access areas, services, access control, access time and billing mode.

Note: A service refers to the service selected during authentication on the SU client.

Plans of different billing types for different services: This type of plan needs to be associated with billing policies of using different billing rules for different services.



Restrictions:

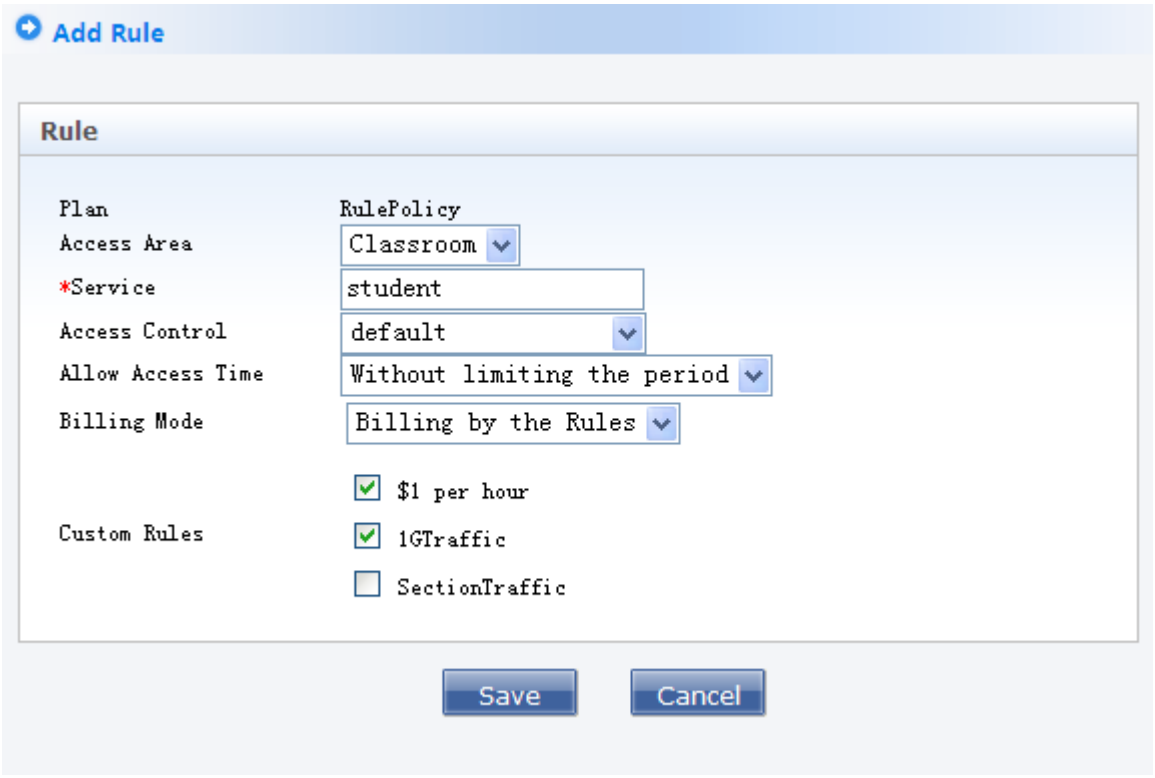
1) Only one billing rule of the same type can be selected.
2) Total gateway traffic and classified traffic cannot be selected simultaneously.
3) The same billing rule can be associated with different services.
4) One plan can contain only one cycle billing rule.

Specific configuration:

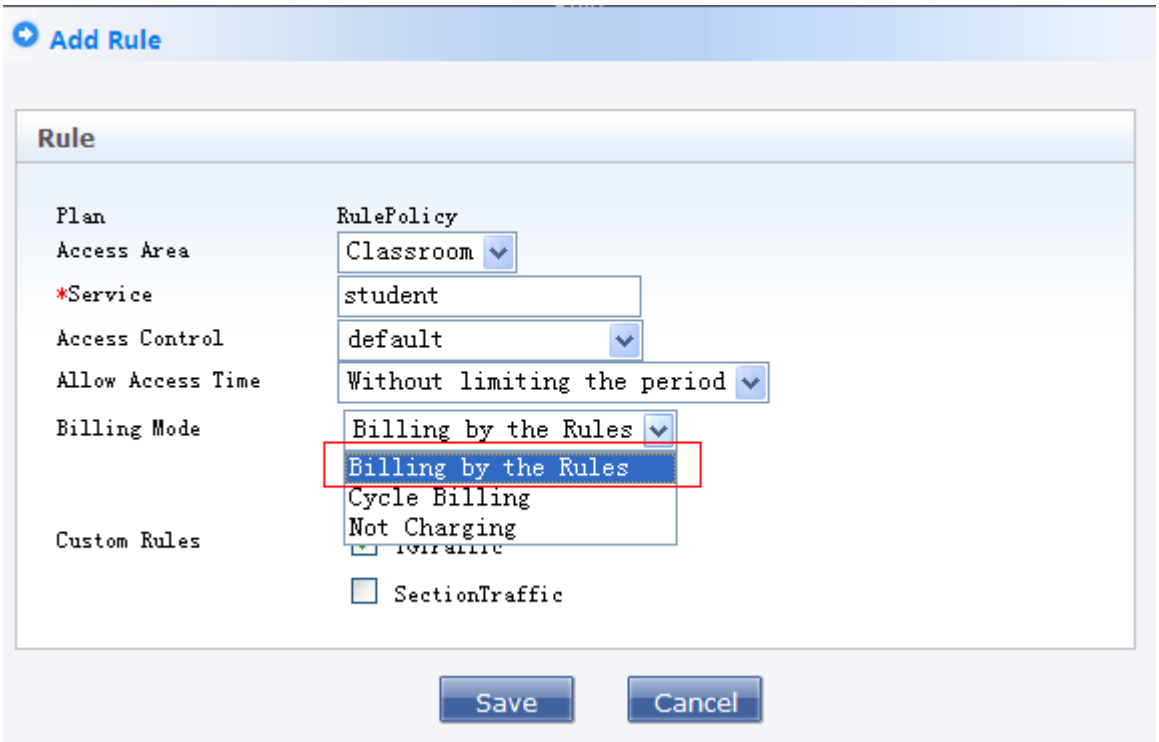
1) Configure one required billing policy of using different billing rules for different services in the current plan.

Note: For the configuration method, see "Different Billing Rules for Different Services."

2) The following figures show the plan configuration.



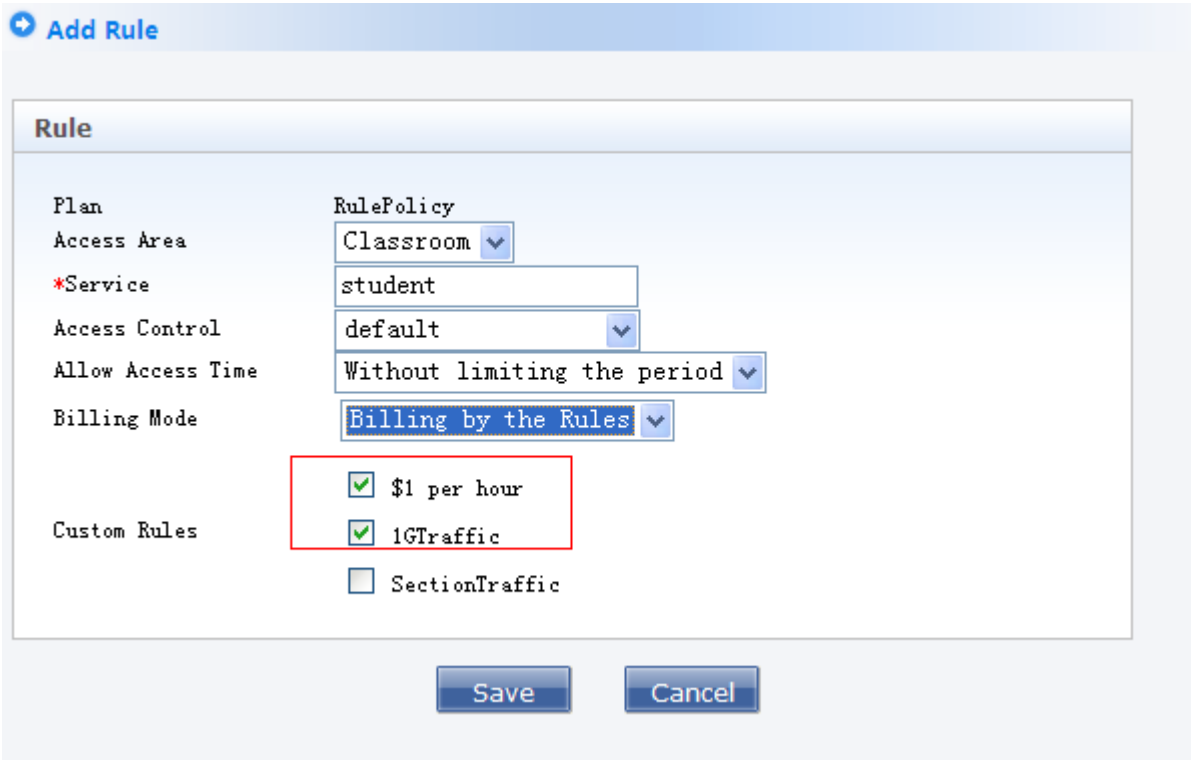
3) Billing Mode



For plans using different billing rules for different services, there are three types of billing modes: **Billing by the Rules**, **Cycle Billing**, and **Not Charging**.

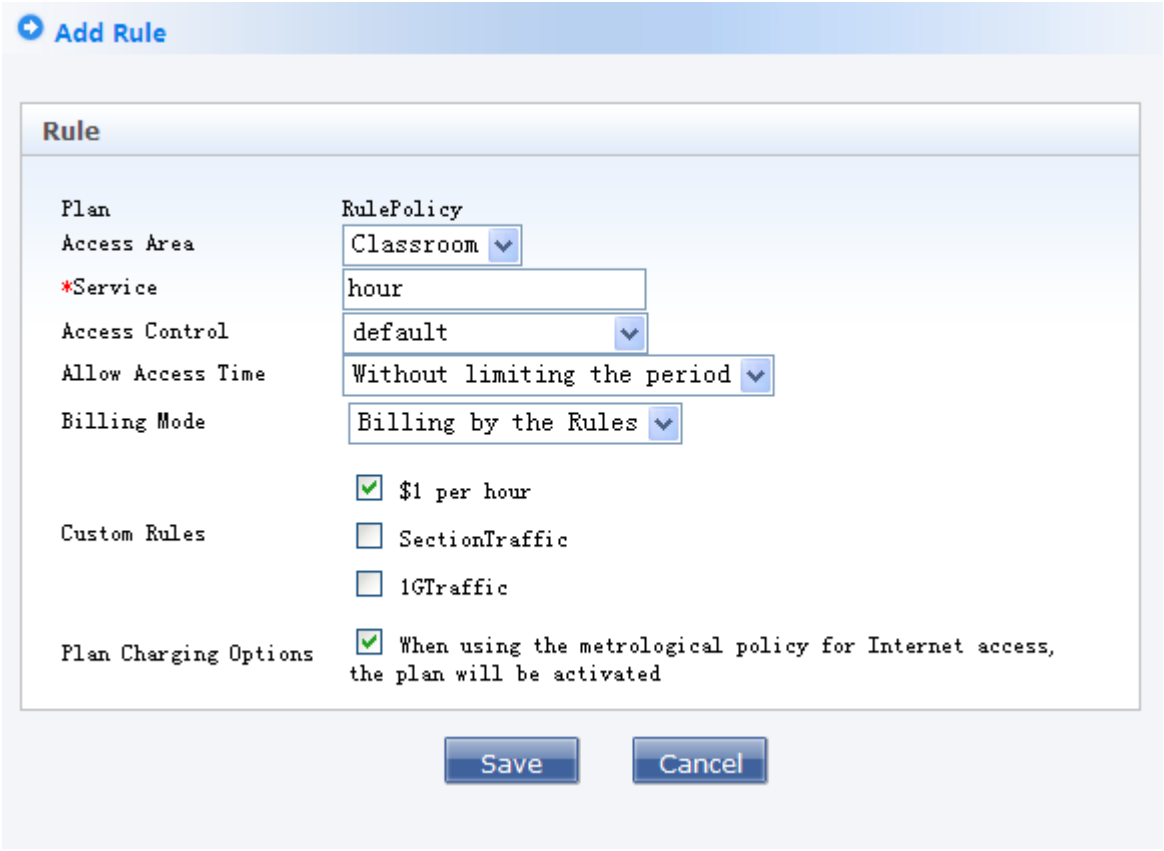
(Note: **Cycle Billing** is displayed only when a cycle rule is contained in a billing policy associated with the current plan. When a user using such a billing mode goes online, only the cycle fee of the current cycle is collected and no other fees are collected.)

4) Custom Rules



Billing rules contained in a billing policy associated with a plan are all displayed here. Multiple different types of billing rules can be selected for one service.

5) Plan Charging Options



Plan Charging Options controls whether fee deduction is triggered for the current service when a plan with **Billing Mode** set to **Not Charging** is not adopted. It is selected by default.

The display of this option needs to meet the following conditions:

1) A billing policy associated with a plan is that no fee is deducted if no service is used.
2) Rules selected in customized rules are pure rate billing rules.

When **Plan Charging Options** is not selected and a user accesses the Internet by using the service in the plan, only billing is conducted but a new cycle is not started.

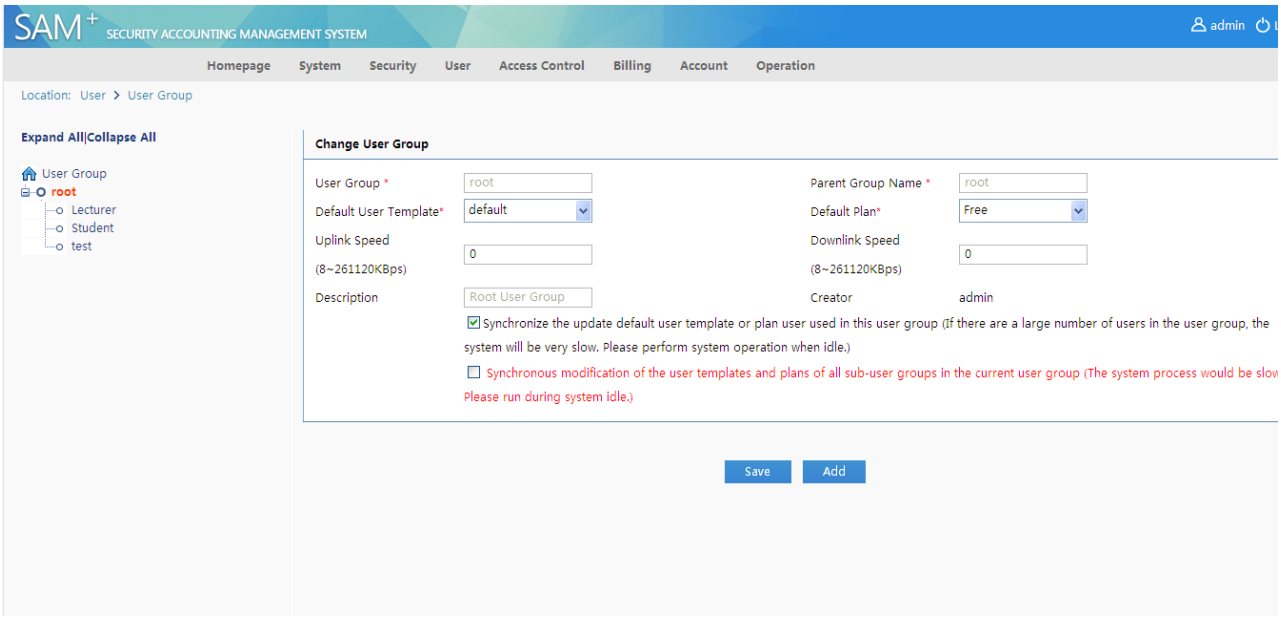
User Group

A user group is a virtual collection of users, with the aim of better managing and classifying users. A default template can be set for a user group so as to rapidly configure billing policies and services for users in the user group.

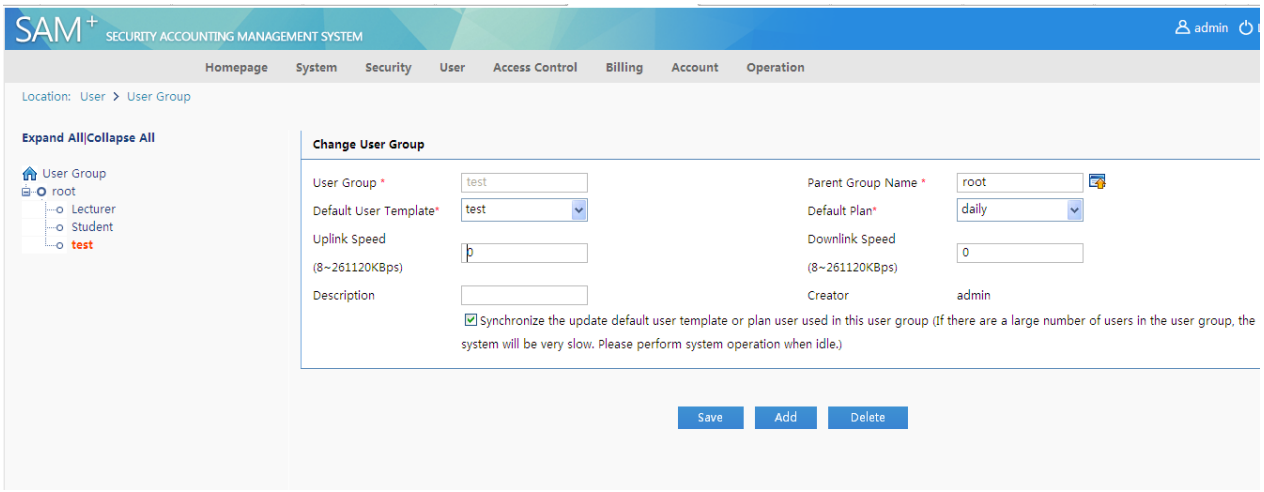
There is a default root user group named **ROOT**. Each user group has a parent user group except **ROOT**. The parent user group of **ROOT** is **ROOT** itself. Each user group has only one position in the entire user group system.

Each user belongs only to one user group but one user group can contain multiple users.

User group operations are simple. The following figure shows user group operations.



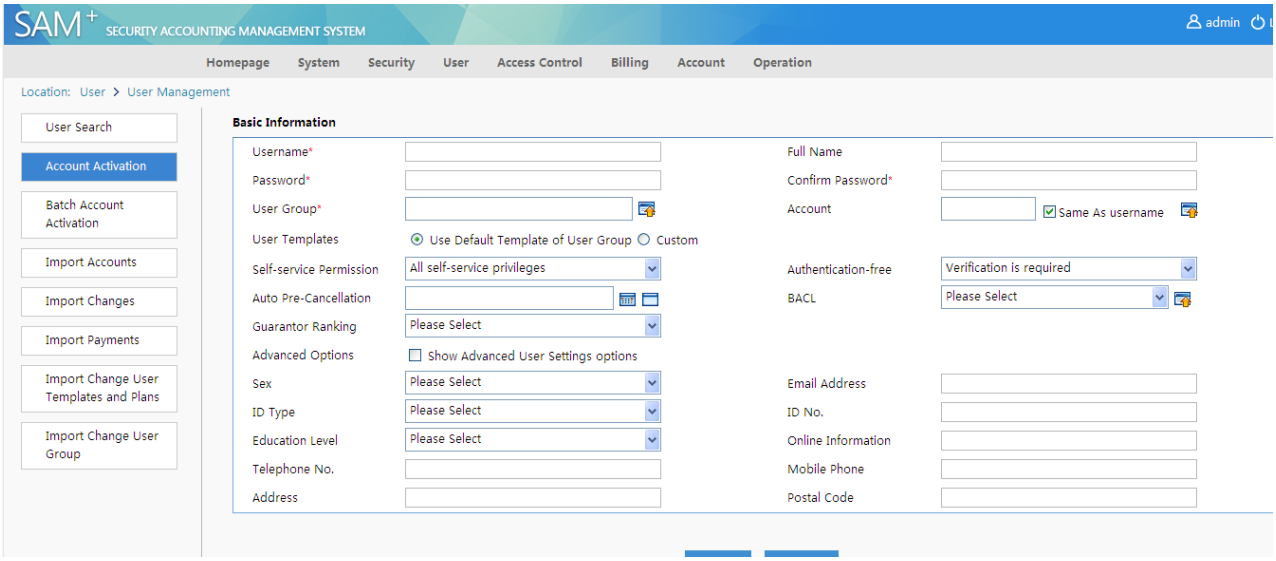
View user group details and modify a user group.



If a selected user group contains a sub-user group and **Synchronous modification of the user templates and plans of all sub-user groups in the current user group** is selected, the same modification is made to user templates and plans of the current user group and all sub-user groups in the current user group.

Normal Users

Normal users are users who can actually enjoy all functions and services provided by the RG-SAM+ system. There is no normal user in the system initially. User **Admin** adds administrators, who add users. Normal users are controlled by licenses. You can choose **User**>**User Management** from the main menu to perform relevant operations. The following figure shows the user adding page.



User Information

Username and **Password** are mandatory attributes of a user. A username uniquely identifies a user in the system and a password is a passport for a user to access the Internet. Administrators can set user attributes on the **User Management** page as required. User attributes include basic information, details, network information, function information, and available services.

Basic Information

In addition to the username and password, basic information includes accounts, self-service privileges, authentication-free setting, billing policy, and advanced options. The attributes are very important and are described as follows:

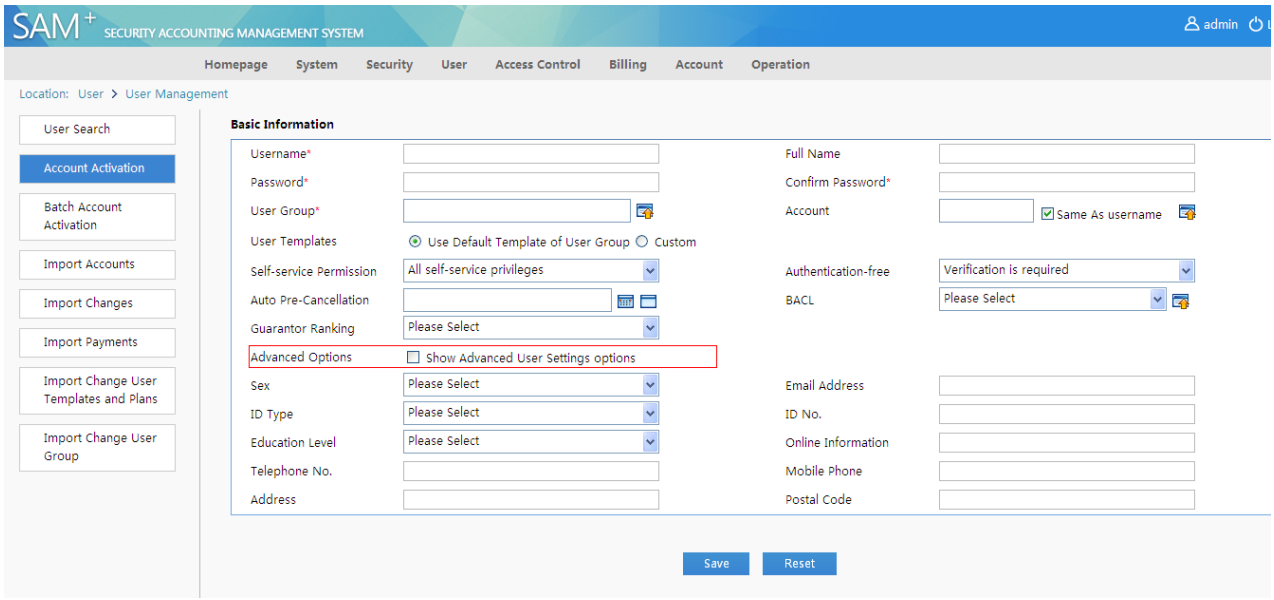
Account: functions as a user's electronic wallet for storing money. An account is used for deduction of Internet access fees and impact caused by recharging, payment, and refund operations is also embodied in accounts. If the account of a user is in arrears, the user cannot pass authentication or go online. A user can be associated with only one account and one account can be associated with only one user in the system.

Self-service Permission: specifies operations that can be performed by users on the self-service page. Different privileges can be set for different users. For example, if the self-service privilege associated with user A supports only self-service registration, use A can only view and perform the self-service registration operation when the user logs in to the self-service system. If the self-service privilege associated with user B supports self-service recharging in addition to self-service registration, use B can view and perform the self-service recharging operation in addition to self-service registration when the user logs in to the self-service system.

Authentication-free: determines whether to verify the access control content of a user (including the binding of the user IP address, MAC address, NAS IP address, and NAS port, BACL, and client version, for details, see the access control module section). You can select **Verification is required** or **Verification-free**.

Billing Policy: measures the value of the Internet access service. If billing is required for a user, a billing policy needs to be associated and one billing policy can contain multiple relationships of service — billing rule sets. A service — billing rule set defines how to charge a service. Therefore, a billing policy can be described as a set of billing modes for services contained in the billing policy.

Advanced Options: Advanced options can be disabled. After disabling, only basic information is displayed.



Detailed Information

In details, administrators can set the sex, ID type, ID No., education level, and online information based on user conditions. If **Online Information** is set, online information is displayed as a pop-up menu after a user passes client authentication and goes online.

In binding information, the following information can be set: user IPv4 address, user IPv6 address, user MAC address, NAS IPv4 address, NAS IPv6 address, NAS port ID, IPv4 address of the Web authentication access device, port ID of the Web authentication access device, SSID, and AP MAC address. The information will be written into the database. After a user attempts to pass authentication and go online, the RG-SAM+ system checks whether the field information sent from the client is the same as the information in the database if user information check is required in the access control. If yes, the user passes the authentication and goes online. After BACL check is enabled in the access control of a user, the system performs BACL check if the user information verification fails. If the user passes the BACL check, the user passes authentication and goes online, which is the meaning of the BACL attribute. Other attributes are not meaningful in function. After they are set, they can be displayed on the self-service page and users can configure their network environment according to the settings.

In network information, the following information can be set: gateway IPv4 address, subnet mask, preferred DNS, standby DNS, user IPv6 address (local link), gateway IPv6 address, and number of IPv6 addresses.

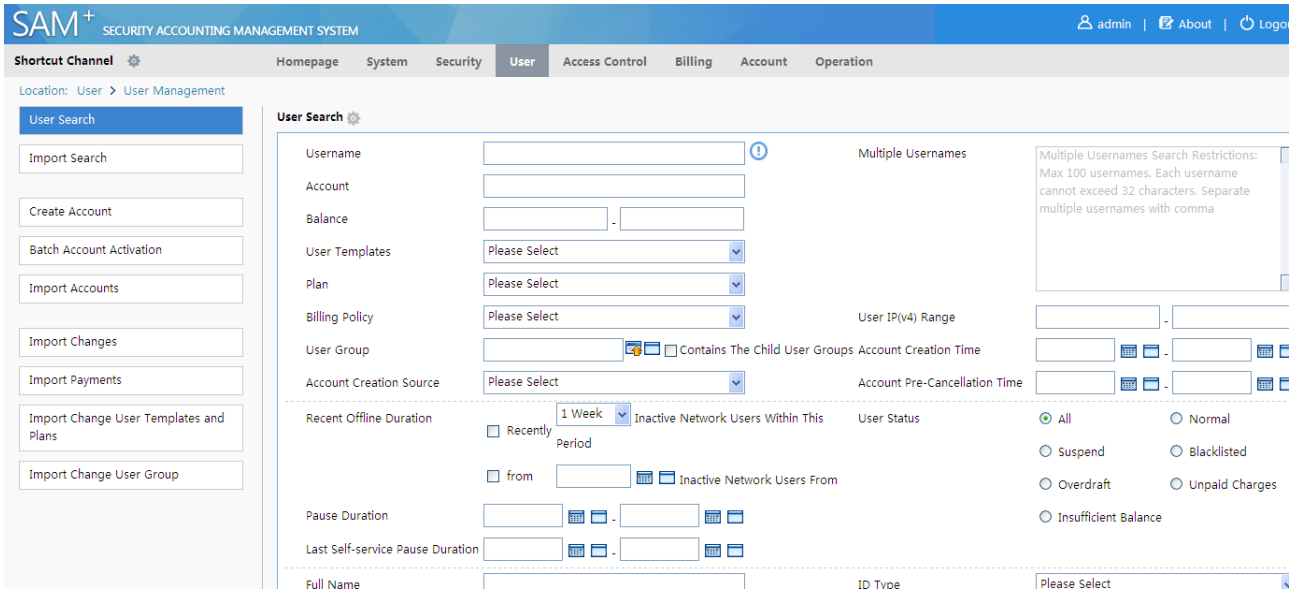
Function information includes the IPv4 address to be issued and account activation fee. An IPv4 address to be issued refers to an IP address issued by a VPN server to a user in a VPN solution. Account activation fee refers to the handling charge paid for account activation. **Overdraft Options**: If an account associated with a user is an overdraft account, this option sets whether the user can access the Internet when the credit line of the account is used up. This option is meaningless for users associated with non-overdraft accounts. When a user is associated with a cycle billing policy, the start time of the current period, next accounting time, and expiration time of the normal Internet access are also displayed.

Additional information: Some user information can be customized as required. The system supports 20 pieces of customized information. For details, see "Field Customization Management."

User Management

Normal users support the same basic functions as other service entities: adding a user, modifying a user, deleting a user, querying users, and printing user information. In addition, the following functions are supported.

User Search

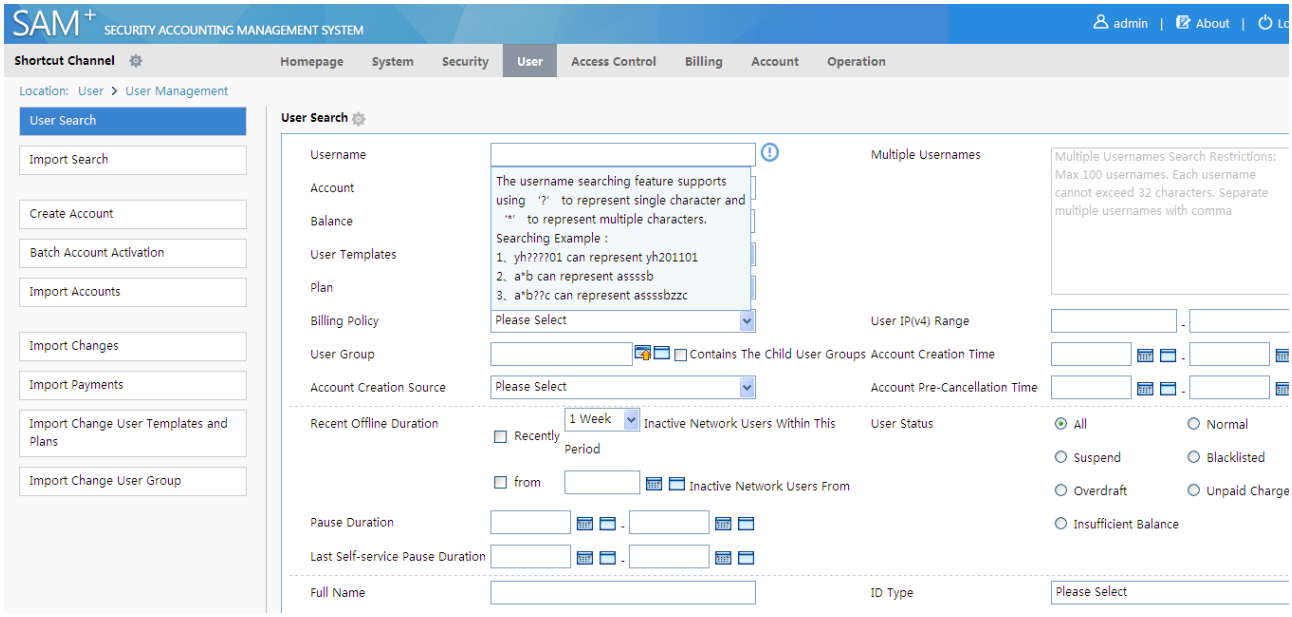


The user scope to be searched depends on users and operation purposes. Therefore, simple search conditions cannot meet various requirements. A very large area is required for displaying all search conditions. Therefore, the function of customizing search combinations is provided here.

Search by matching mode

The matching mode can be set to matching the start, matching the end, and matching any location, catering to different user naming scenarios. For example, in the naming mode of student ID + dormitory ID, when users need to be searched by student ID, you can select the mode of matching the start and conduct fuzzy search by student ID; when

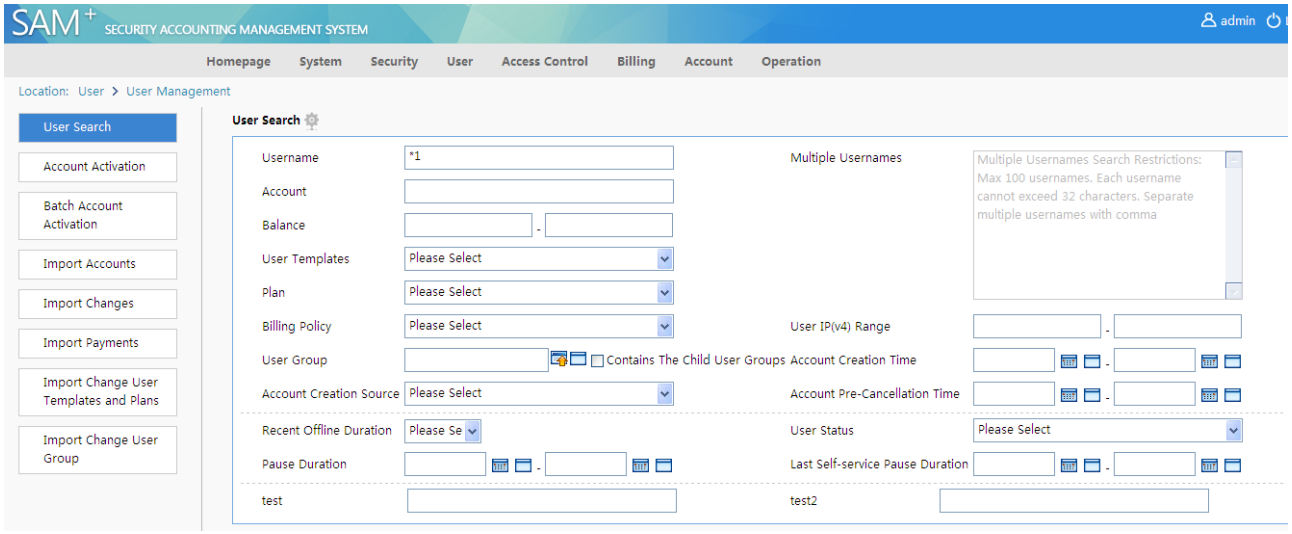
users need to be searched by dormitory ID, you can select the mode of matching the end and conduct fuzzy search by dormitory ID.



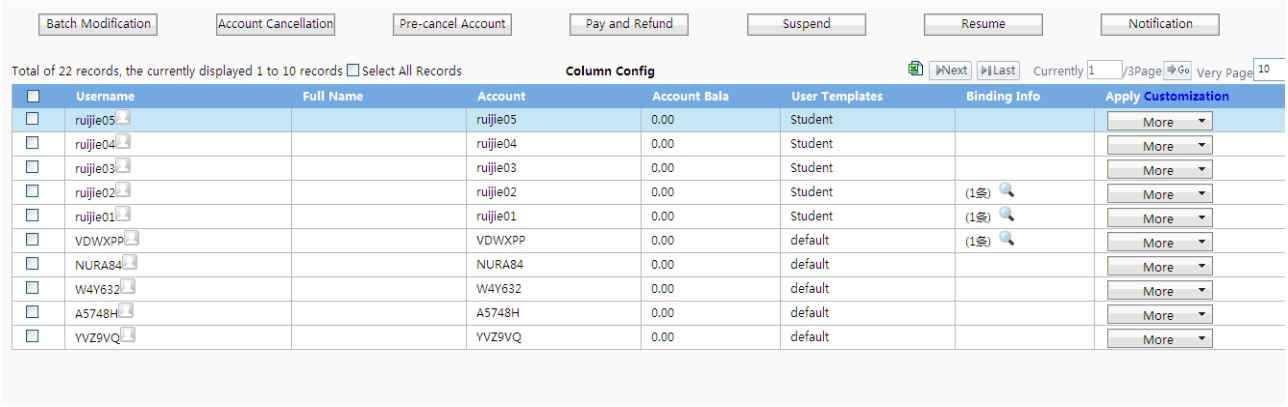
Search by wildcard

The **Username** field allows using the character "?" to replace a single character and using the character "*" to replace multiple characters (the search by matching mode is not applicable when a wildcard is used).

Enter a wildcard in **Username** for user search, as shown in the following figure.



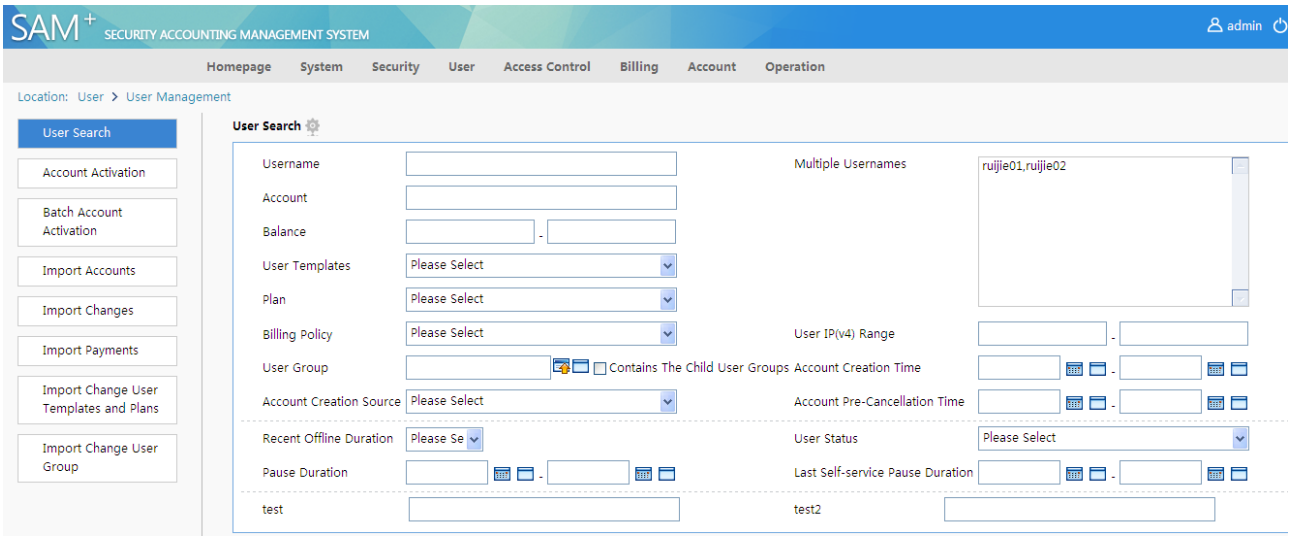
Click **Search**. The user information that is searched out is displayed, as shown in the following figure.



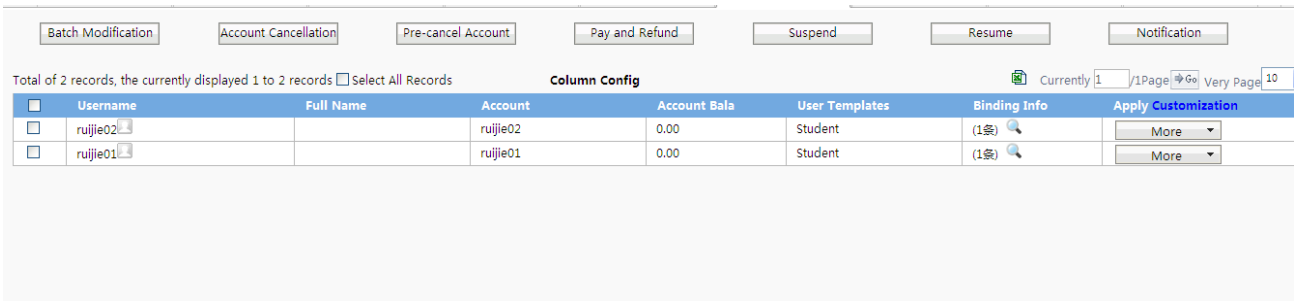
Multiple username search

Note: Only one of the username search, multiple username search, and import search is available. For example, if import search is used, username search and multiple username search are unavailable.

To clearly search for multiple certain users, administrators can use the multiple username search function (multiple username search does not support wildcard and fuzzy search), as shown in the following figure.

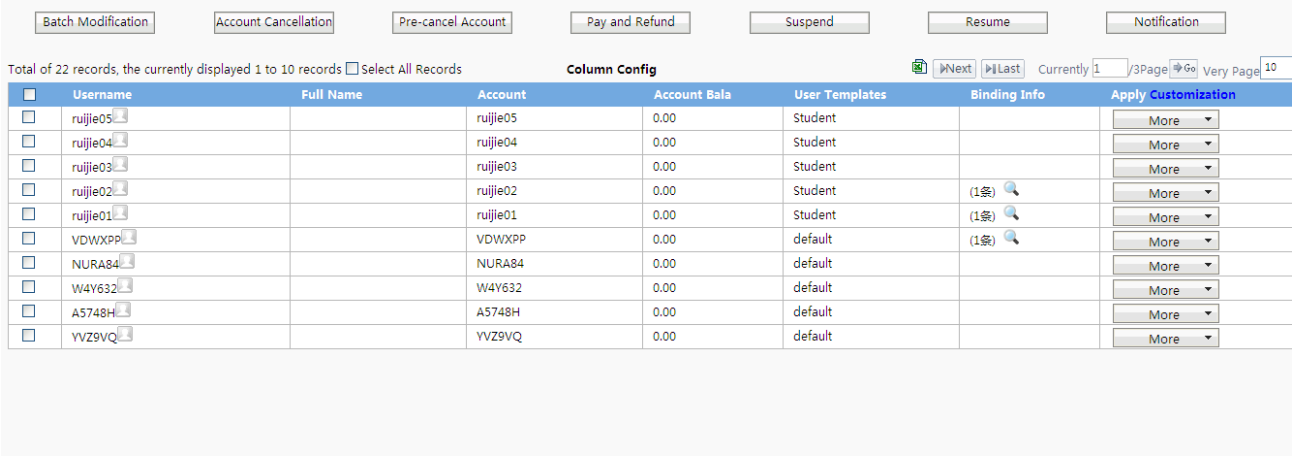


Enter names of users to be searched and click **Search**, as shown in the following figure.



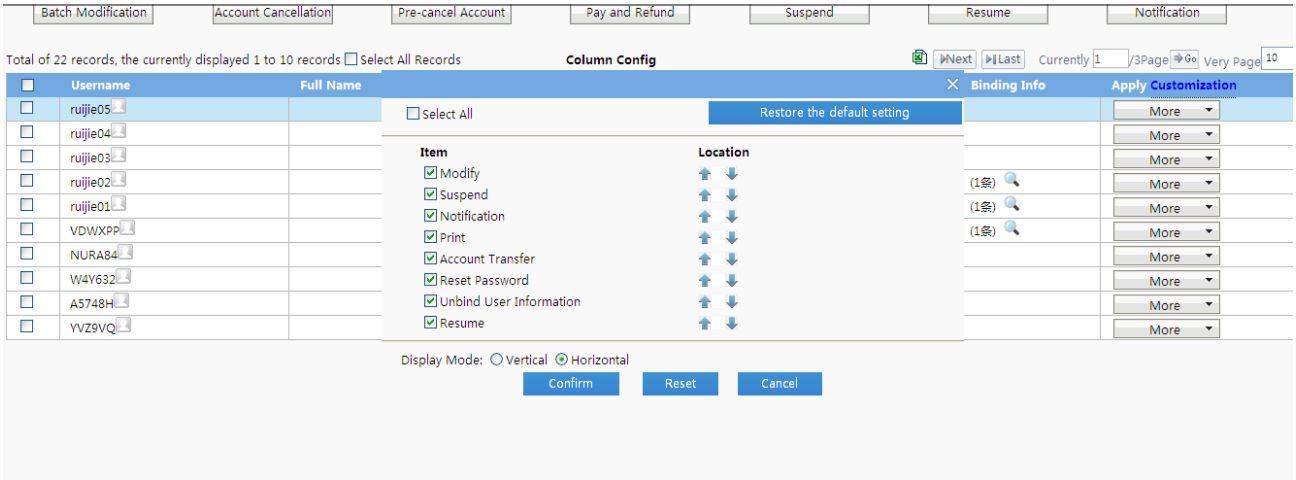
User list

After **Search** is clicked, a page listing the search results is displayed, as shown in the following figure.

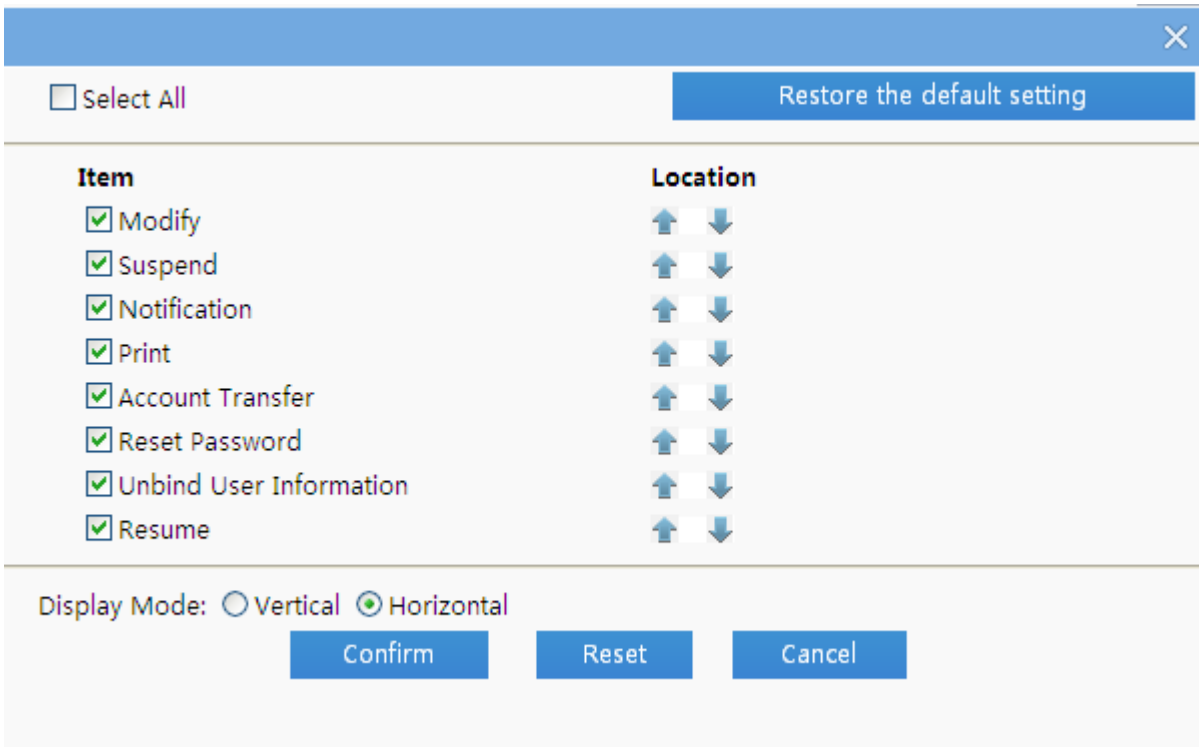


More operations

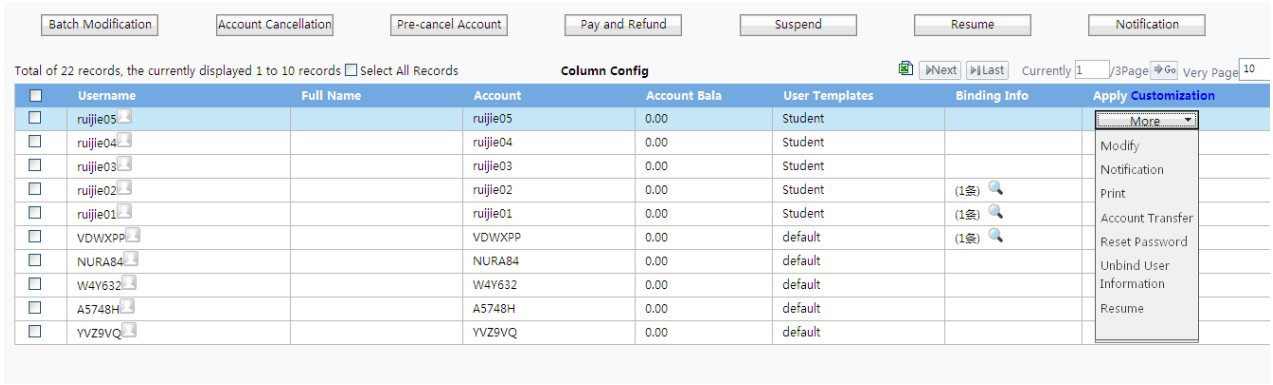
A large number of function buttons are introduced to the list to facilitate post-search service operations and cater to operation habits of different administrators. Function buttons can be customized for more operations, as shown in the following figure.



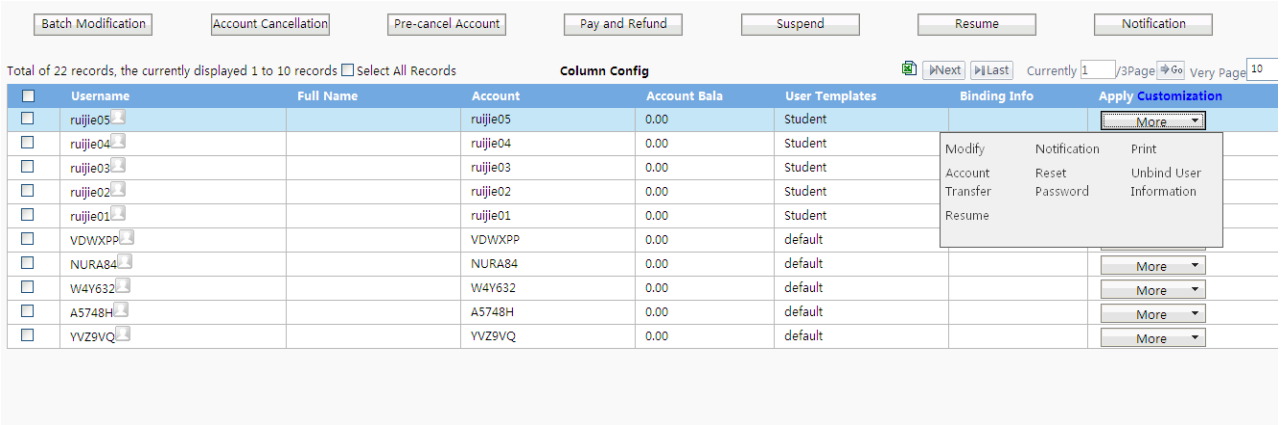
More operation function customization



Vertical display of the drop-down list displayed when you click **More**:

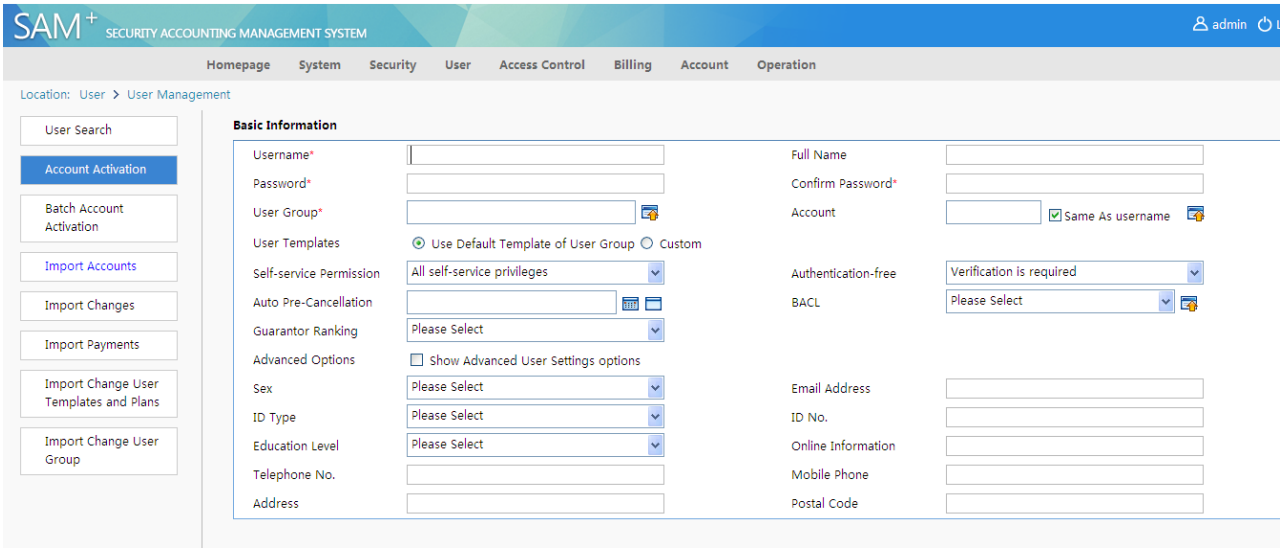


Horizontal display of the drop-down list displayed when you click **More**:



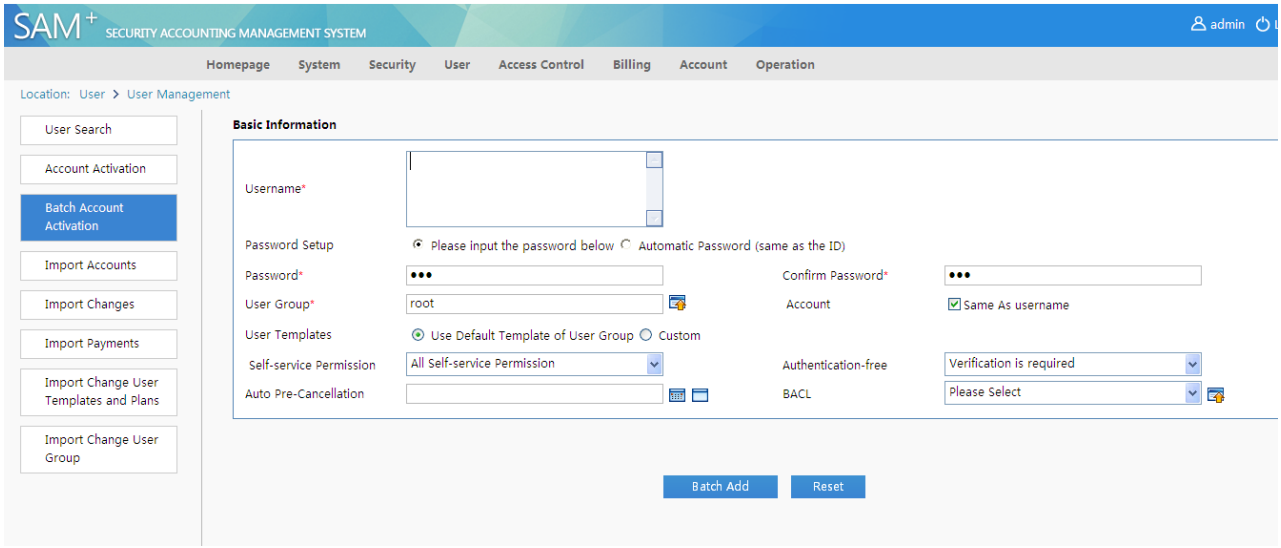
Account Activation

Account activation page:



Batch Account Activation

Batch account activation page:



Restrictions on batch account activation:

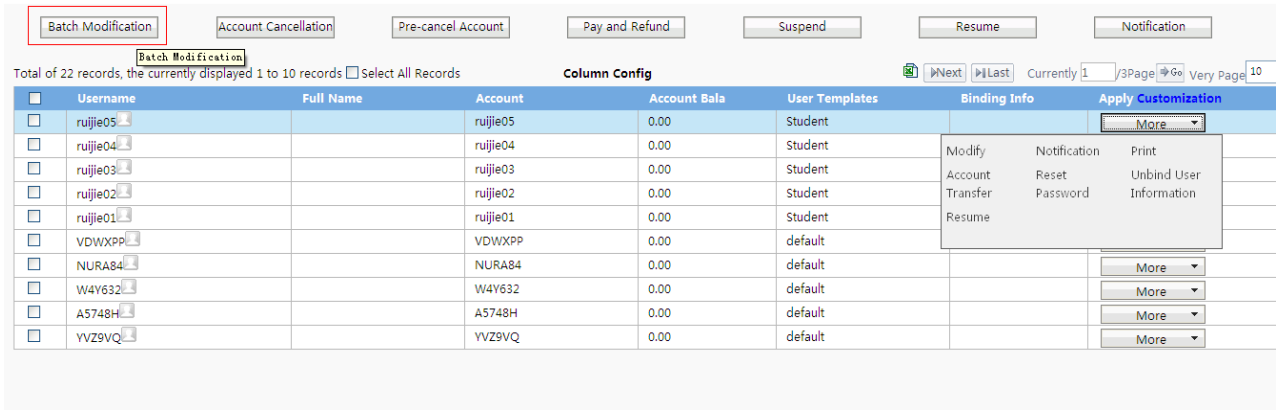
This function supports a maximum of 500 users.

Usernames are separated by a comma (,) or space ( ).

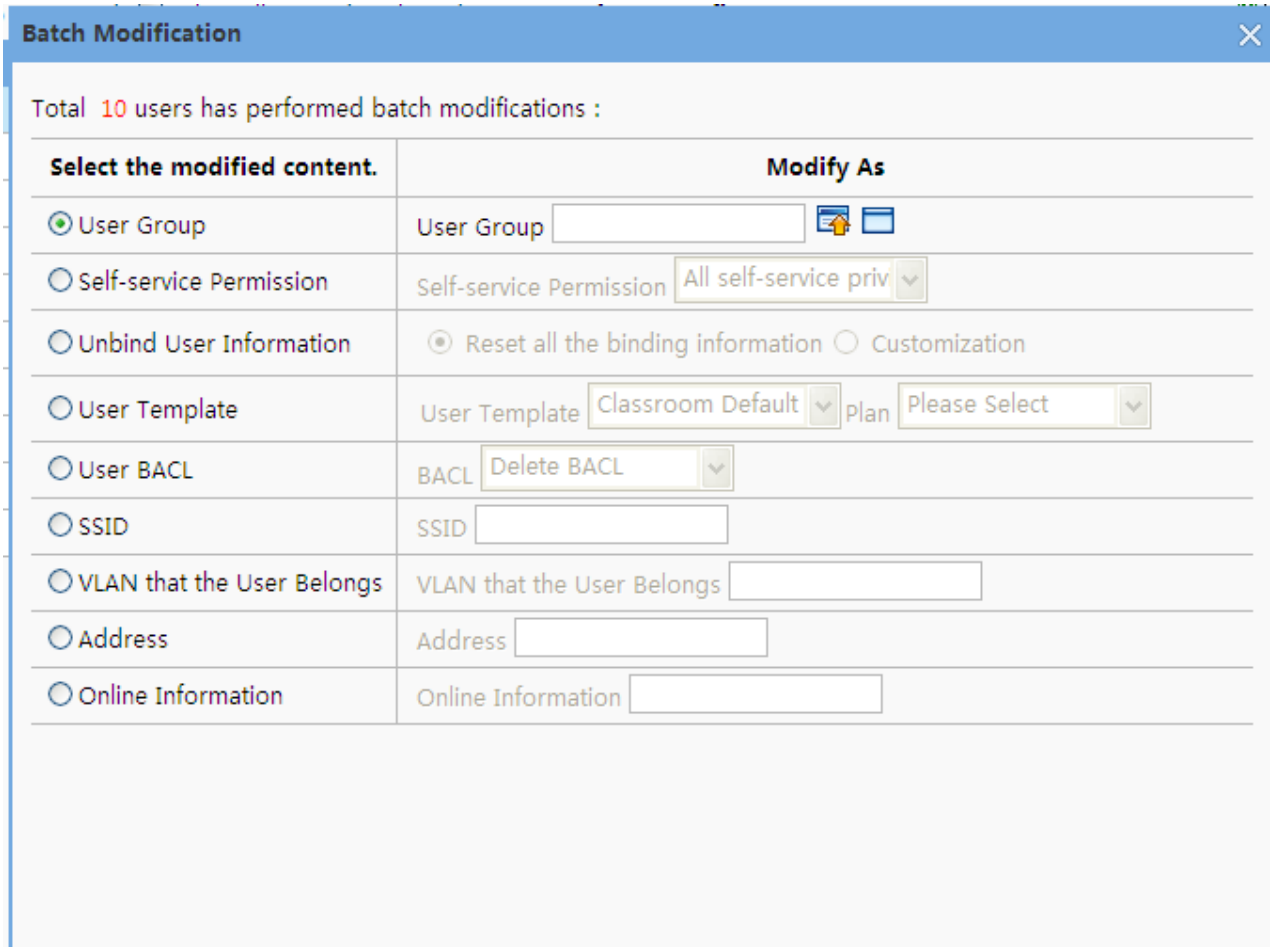
Batch Modification

Choose **User**>**User Management** from the main menu and click **Batch Modification** on the page that is displayed. You can select a certain number of users and modify their user group, self-service privileges, bound user information, user template, user BACL, SSID, user VLAN, address, and online information at a time.

Entry of the batch modification page:



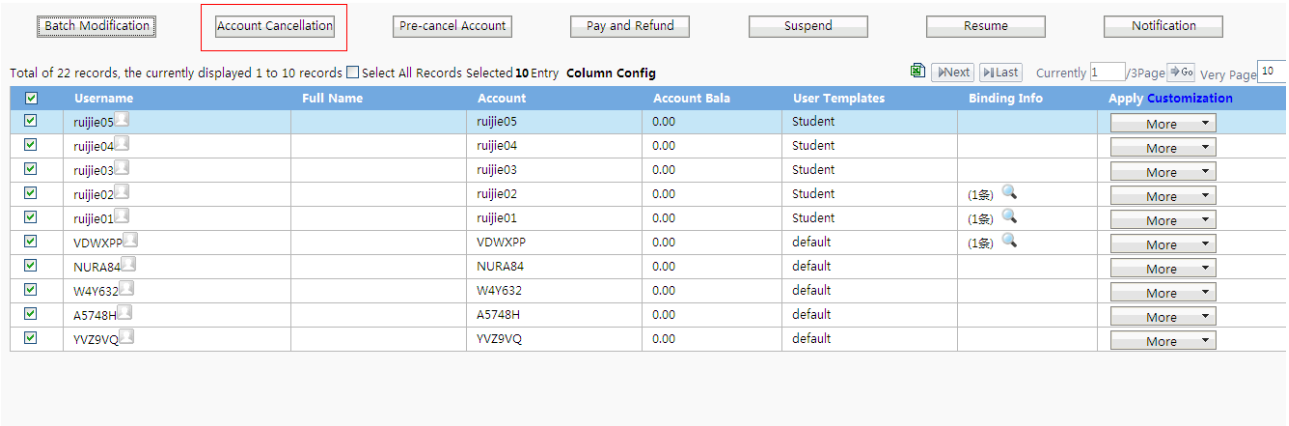
Batch modification page:



When unbinding user information in batches, you can define the bound information to be unbound, such as the user IP address, user MAC address, NAS IP address, NAS port ID, IP address of the Web authentication access device, port ID of the Web authentication access device, SSID, and AP MAC address (if user information is bound, the unbinding operation can be performed; if no user information is bound, no change is required).

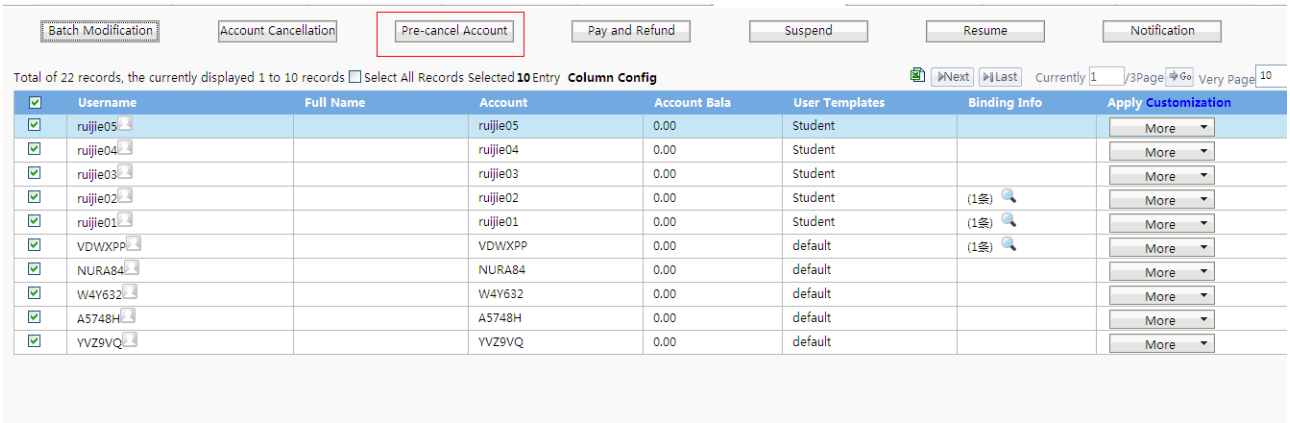
Account Cancellation

Entry of the account cancellation page:



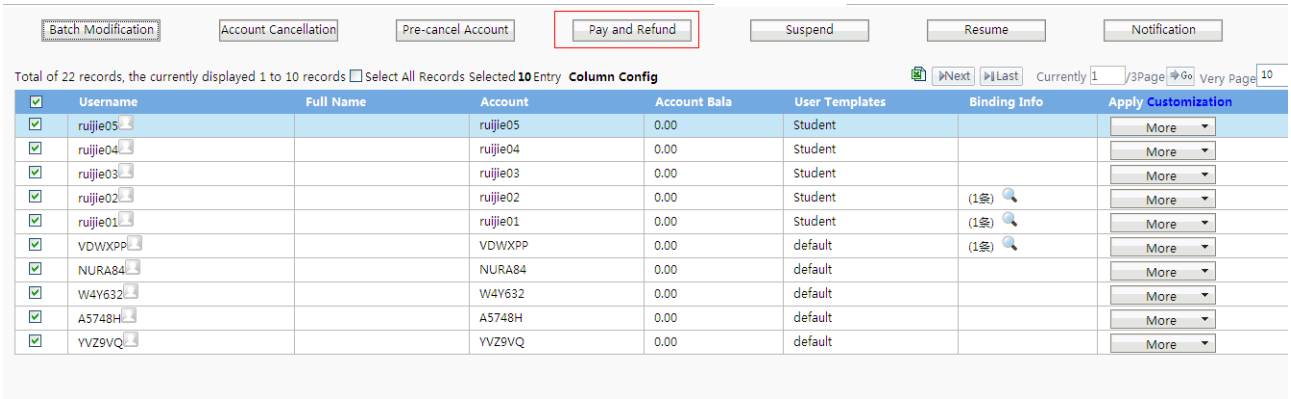
Account Pre-cancellation

Entry of the account pre-cancellation page:

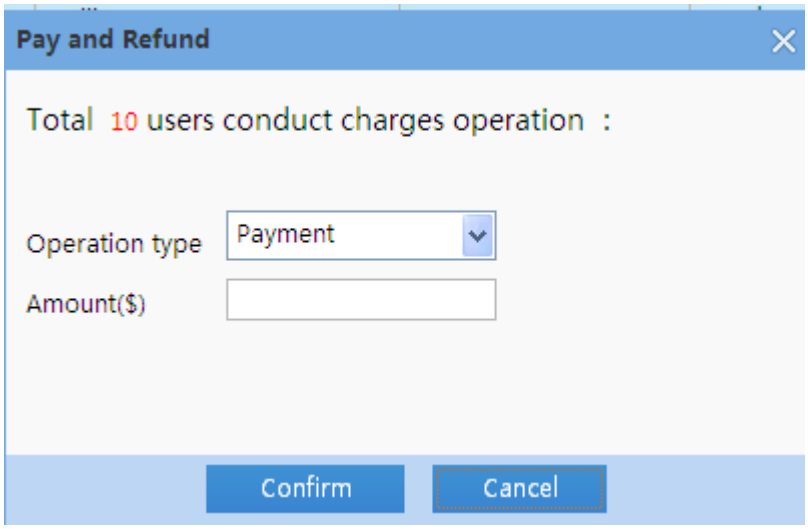


Payment and Refund

Entry of the payment and refund page:



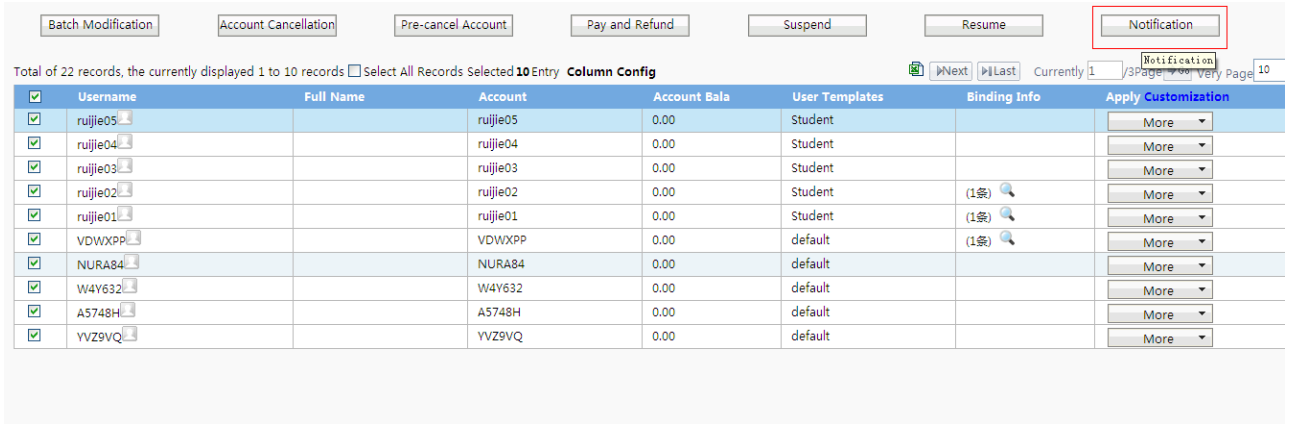
Payment and refund page:



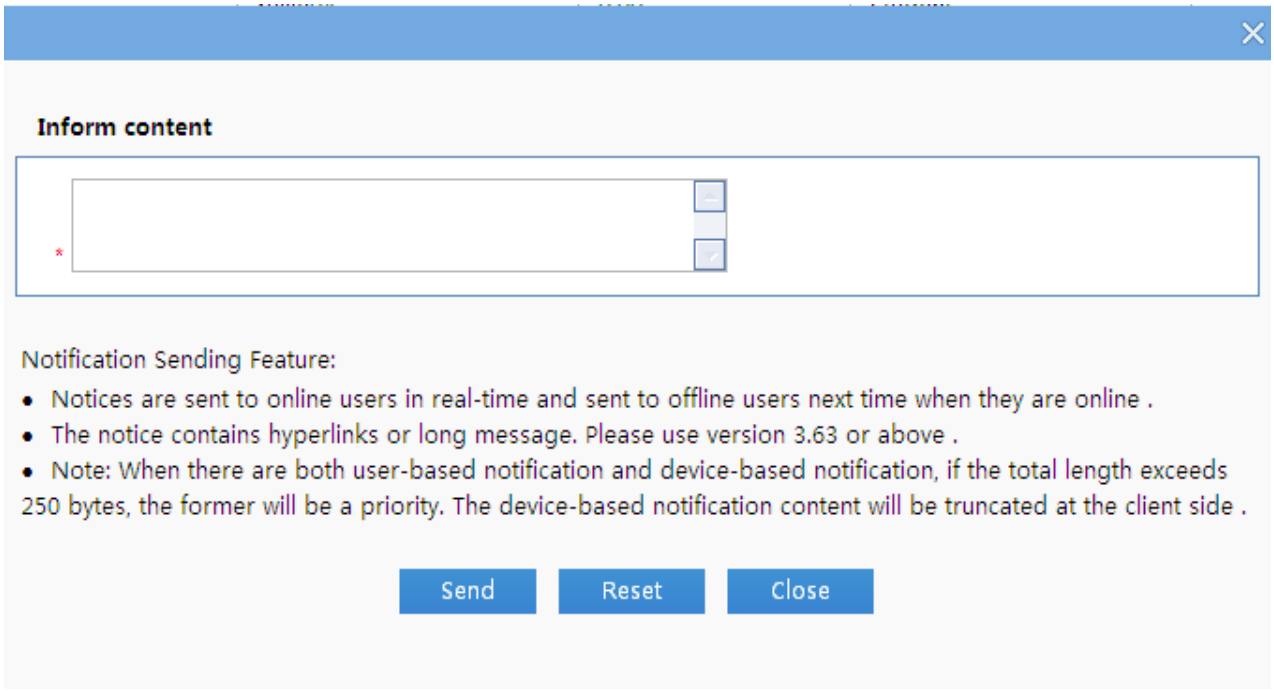
Notification

You can send a notification to users on the user management page. After a notification is sent, currently online users will receive the notification immediately and offline users will receive the notification when they go online next time. You can select users who meet search conditions and send a notification to them, or send a notification to all users at a time.

Entry of the notification page:



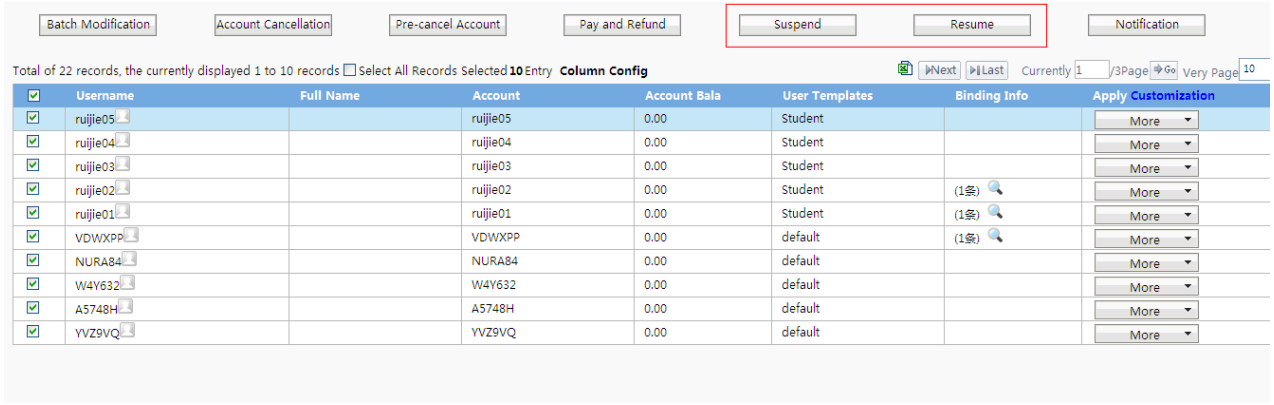
Notification page:



Suspension and Resumption

The suspension and resumption functions are available to normal users.

Entry of the suspension and resumption pages:



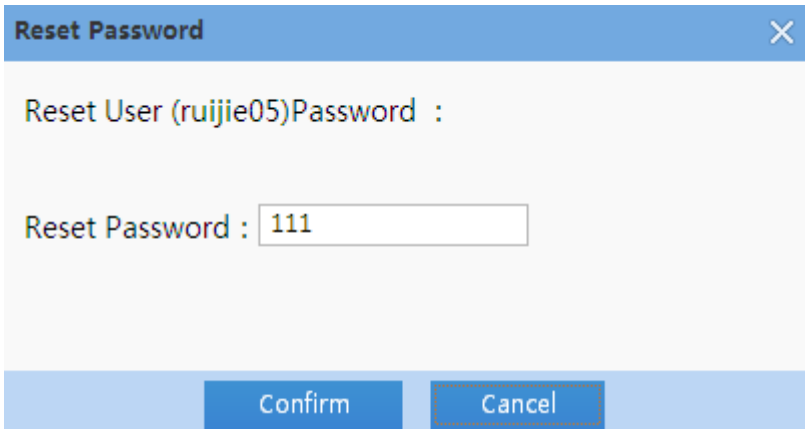
Users can be changed from the normal state to the suspended state. When a user is suspended, the user cannot access the Internet, but can log in to the self-service system, and the Internet access billing, cycle billing, and gateway traffic-based billing are all suspended. On the contrary, users can be changed from the suspended state to the normal state. For resumed users who use the cycle billing policy, you can conduct cycle billing for them for consumption. The user status column displays the current status of a user, which can be normal or suspended. You can also query the user status on the user management page.

If you suspend an online user, the user is forced to go offline and then suspended. Users can perform the self-service suspension and resumption operations on the self-service system.

Password Reset

You can reset a user password. The default reset password is 111, which can be changed.

Click **More** to access the **Reset Password** dialog box.

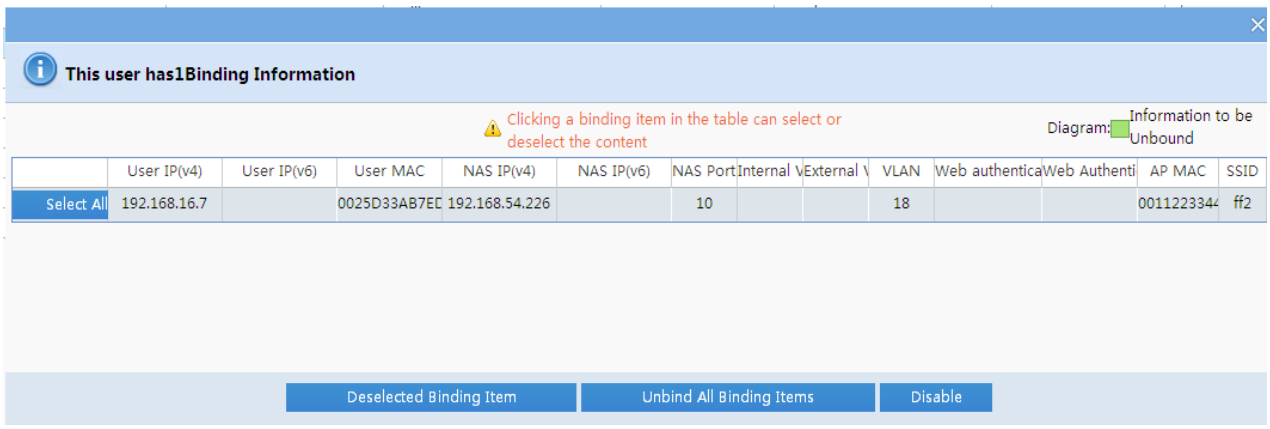


Unbinding

You can unbind one bound item or all bound items for a specified user.

Click **More** to access the unbinding page.

The following figure shows the unbinding page.



Import

The RG-SAM+ system provides a range of import operations to facilitate service operations to be performed on user information files for administrators.

Import restrictions:

Quantity restriction:

A maximum of 10,000 records are supported by import operations except import search.

As high as 500 users can be searched each time during import search.

A maximum of 50 columns are supported.

The following file types are supported:

Pure text format (*.txt)

EXCEL file (*.xls/*.xlsx)

The size of a file cannot be larger than 10 MB.

When pure text files are imported, separators can only be tab, space, comma, and semicolon.

The column header can contain only English letters, digits, and "_", "(", and ")".

Basic import process (successful process):

Select a file.

Verify the file format.

Select fields to be mapped.

Verify the file content.

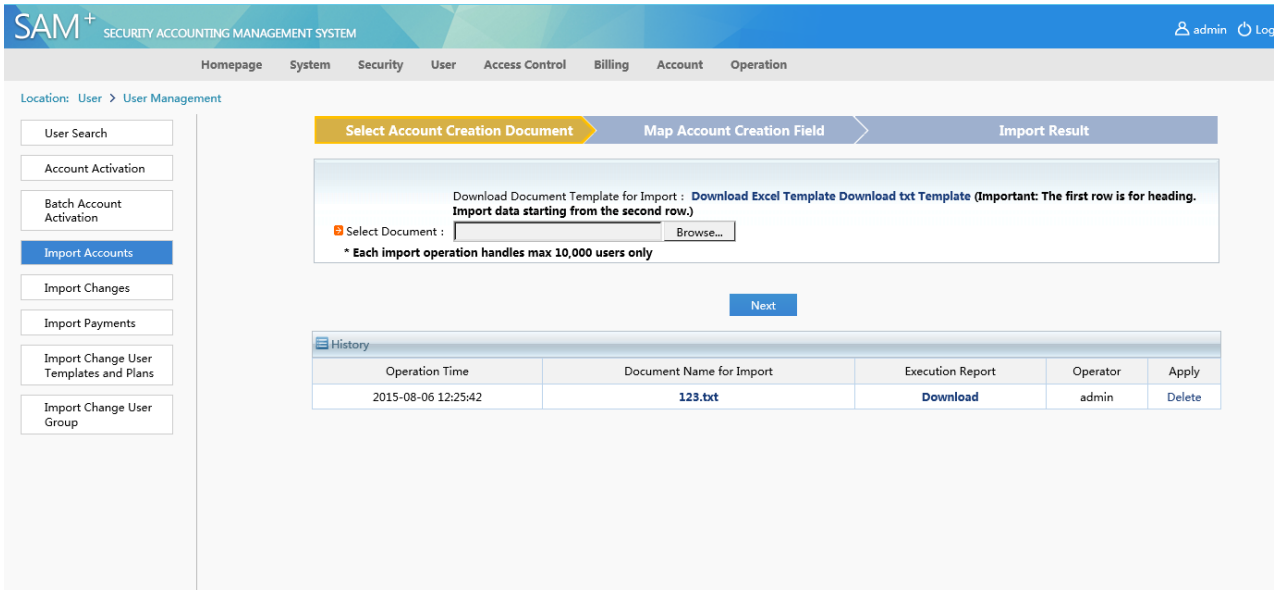
Import file content.

Make import records.

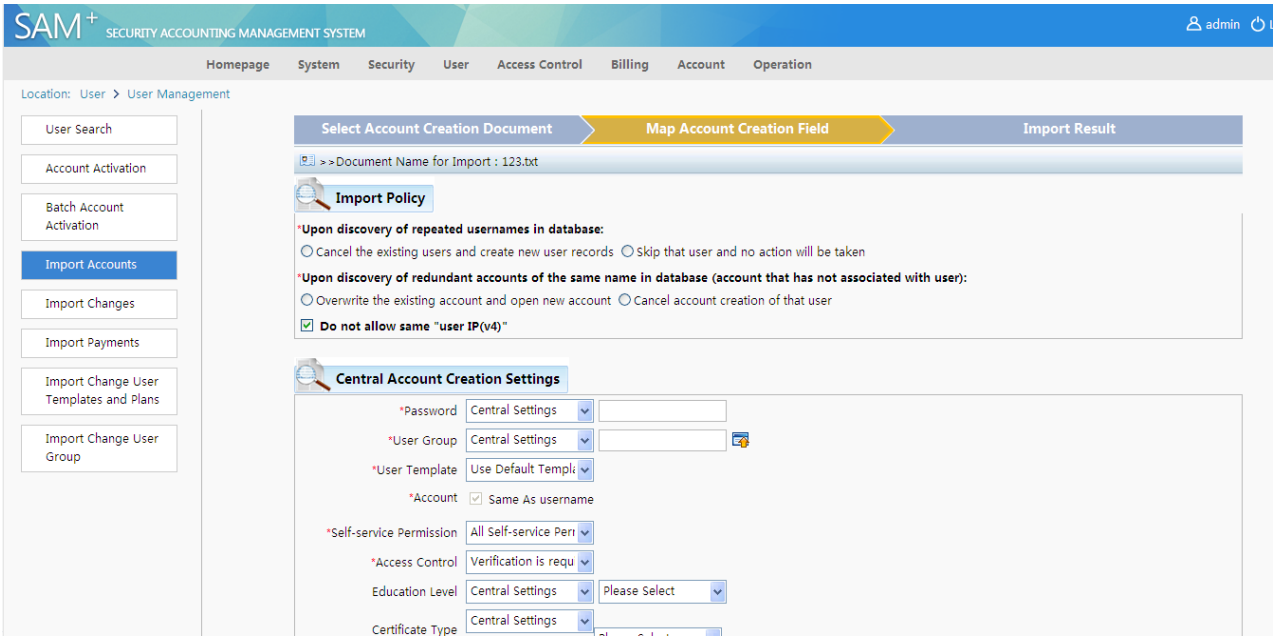
View import results.

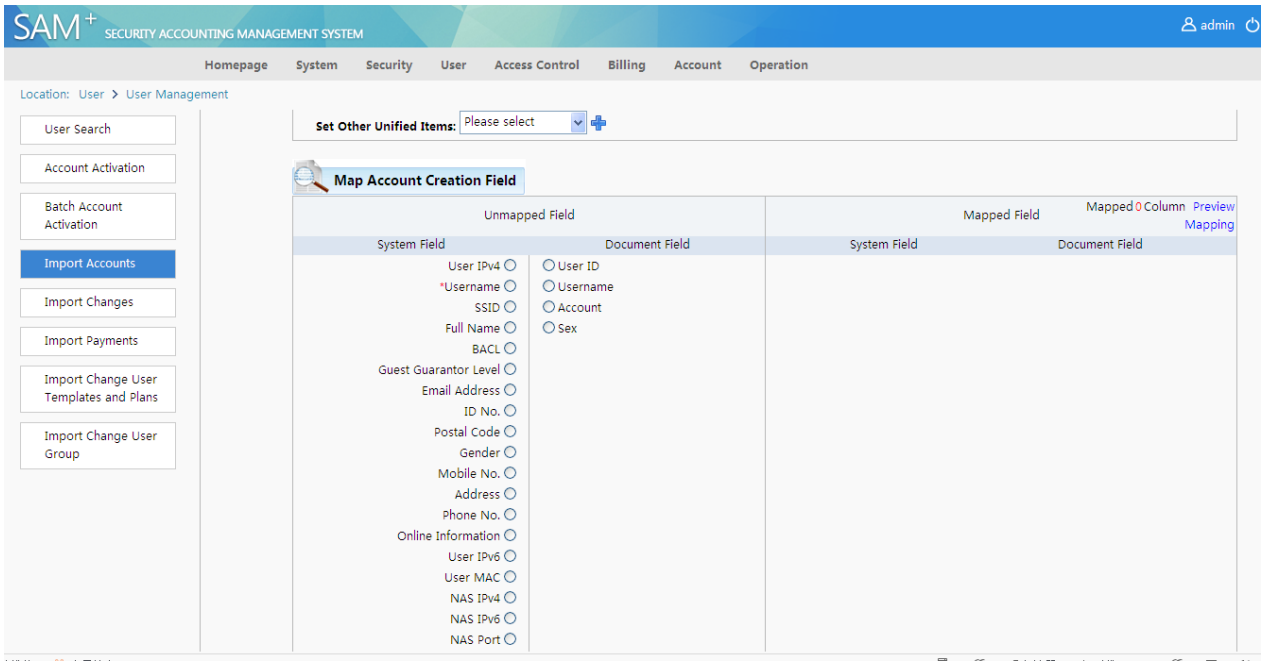
Import Accounts

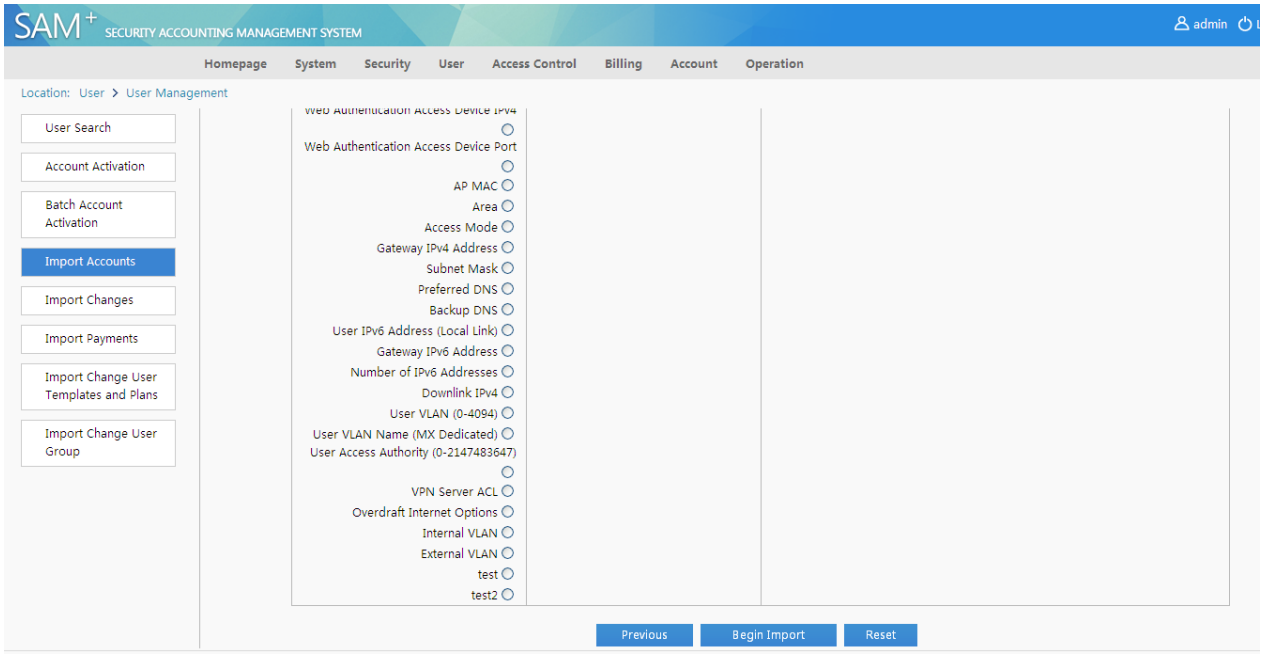
Entry of the account import operation:



Field mapping page:


SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM
admin
Homepage System Security User Access Control Billing Account Operation
Location: User > User Management
User Search
Account Activation
Batch Account Activation
Import Accounts
Import Changes
Import Payments
Import Change User Templates and Plans
Import Change User Group
Select Account Creation Document
Map Account Creation Field
Import Result
>>Document Name for Import : 123.txt
Import Policy
*Upon discovery of repeated usernames in database:
Cancel the existing users and create new user records
Skip that user and no action will be taken
*Upon discovery of redundant accounts of the same name in database (account that has not associated with user):
Overwrite the existing account and open new account
Cancel account creation of that user
Do not allow same "user IP(v4)"
Central Account Creation Settings
*Password
Central Settings
*User Group
Central Settings
*User Template
Use Default Templa
*Account
Same As username
*Self-service Permission
All Self-service Perr
*Access Control
Verification is requ
Education Level
Central Settings
Please Select
Certificate Type
Central Settings

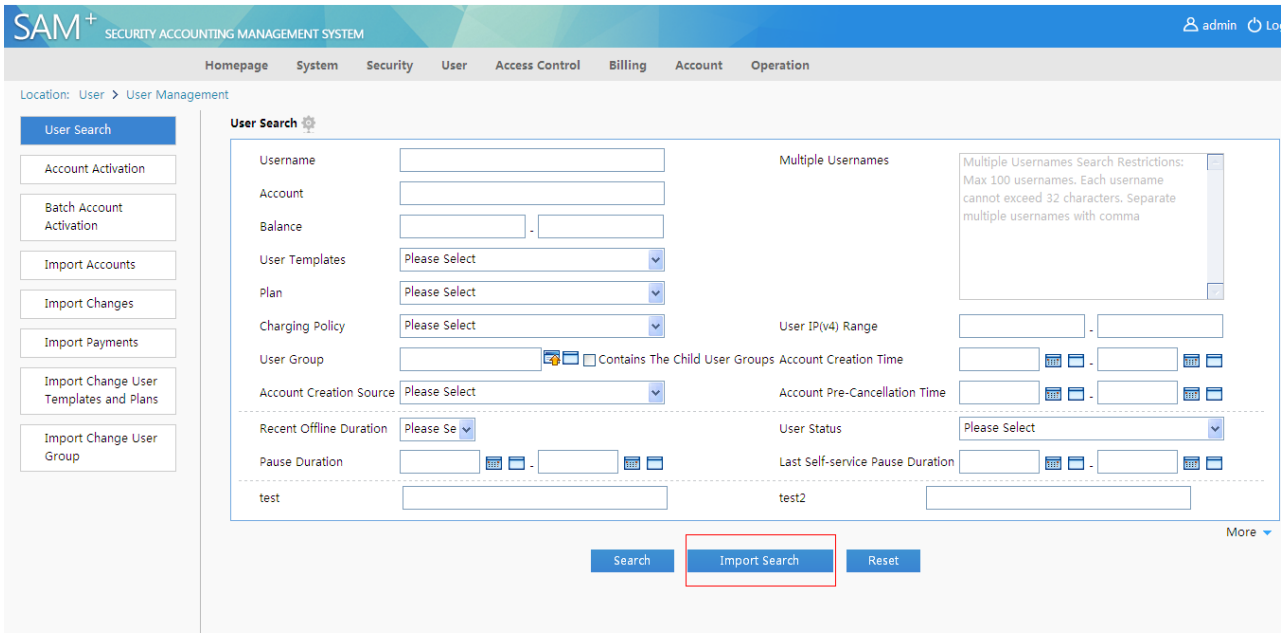

SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM
admin
Homepage System Security User Access Control Billing Account Operation
Location: User > User Management
User Search
Account Activation
Batch Account Activation
Import Accounts
Import Changes
Import Payments
Import Change User Templates and Plans
Import Change User Group
Set Other Unified Items:
Please select
Map Account Creation Field
Unmapped Field
Mapped Field
Mapped 0 Column
Preview Mapping
System Field
Document Field
System Field
Document Field
User IPv4
*Username
SSID
Full Name
BACL
Guest Guarantor Level
Email Address
ID No.
Postal Code
Gender
Mobile No.
Address
Phone No.
Online Information
User IPv6
User MAC
NAS IPv4
NAS IPv6
NAS Port
User ID
Username
Account
Sex



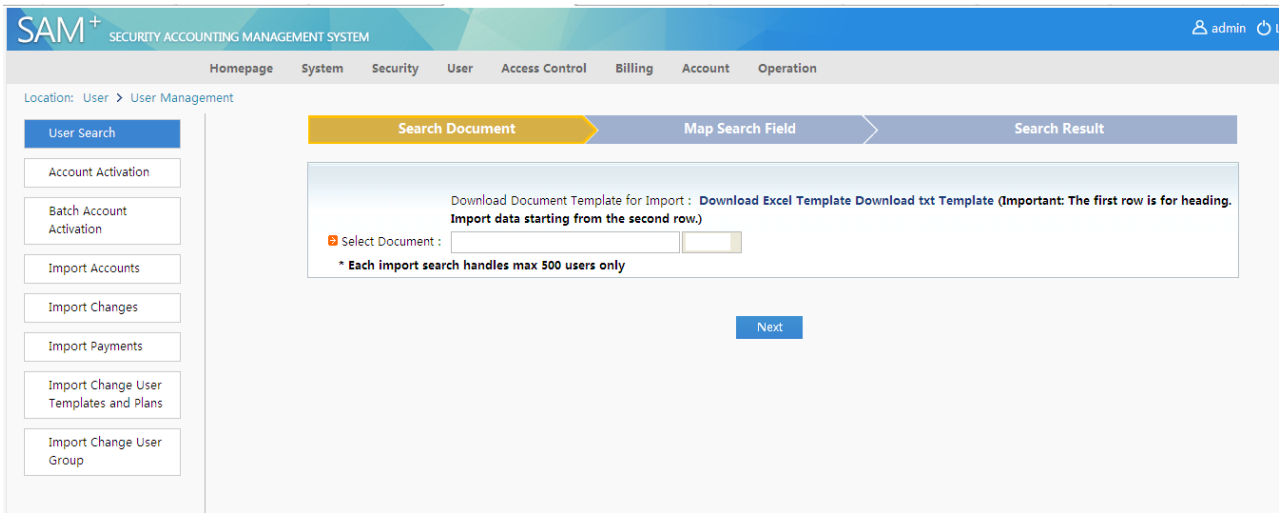
Import Search

The search import supports the search for usernames or certificate numbers.

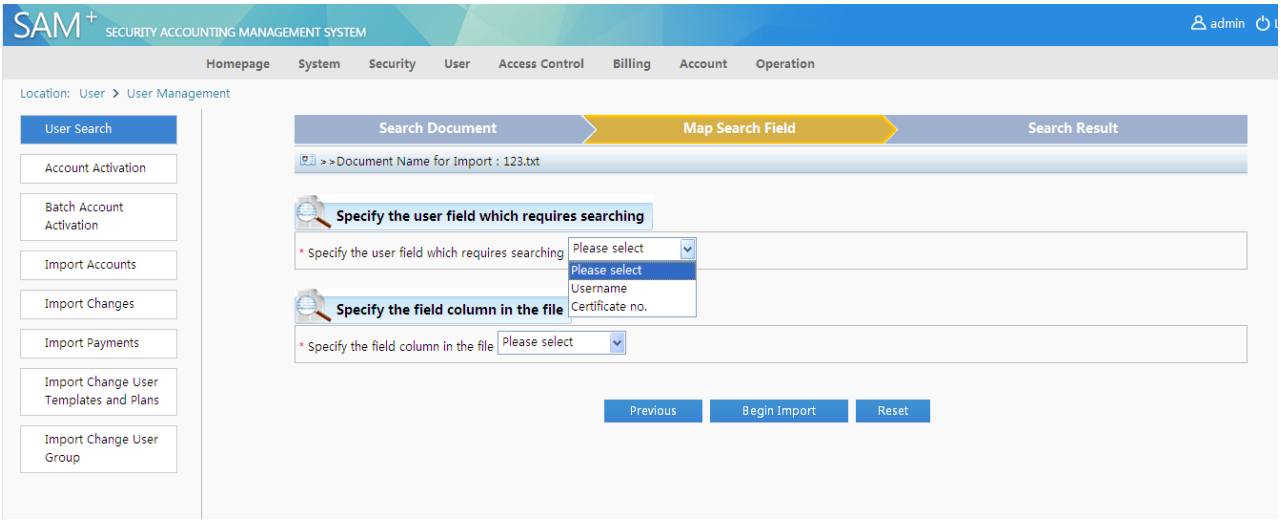
Entry of the search import page:



File selection page:



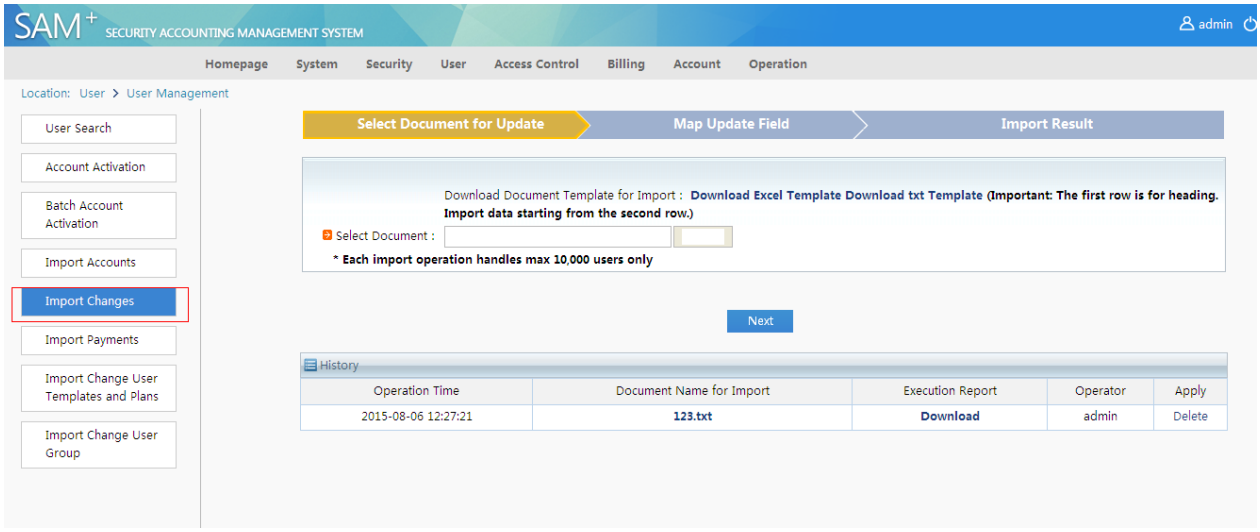
Field mapping page:



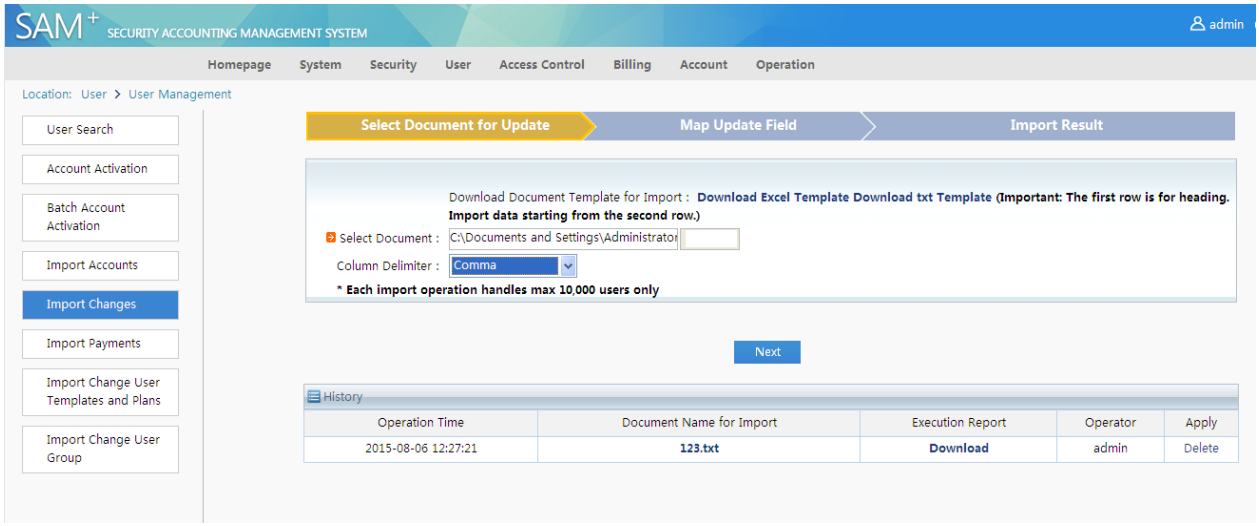
Note: After cancelling search import conditions, you need to click **Search** to search out required users.

Import Changes

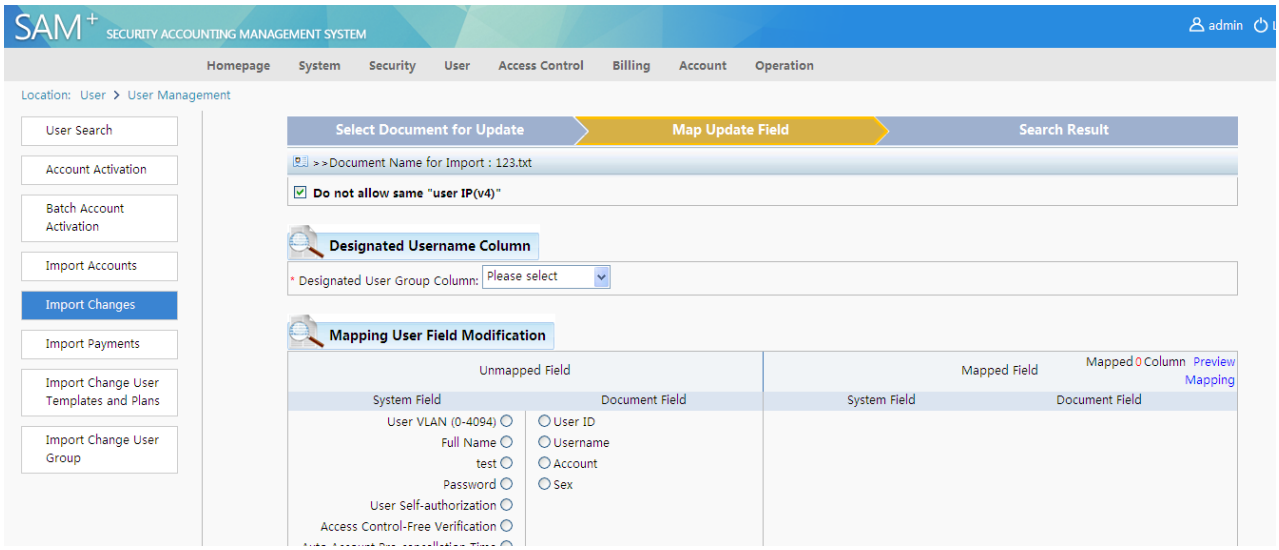
Entry of the change import page:

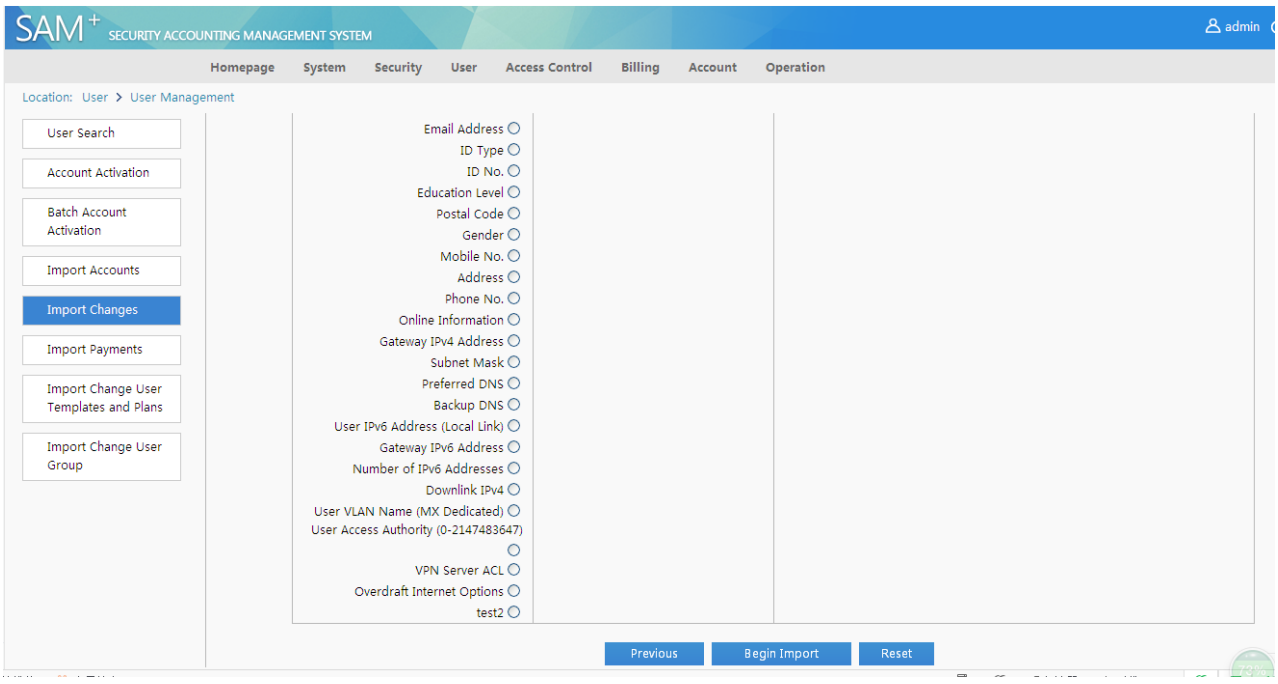


File selection page:



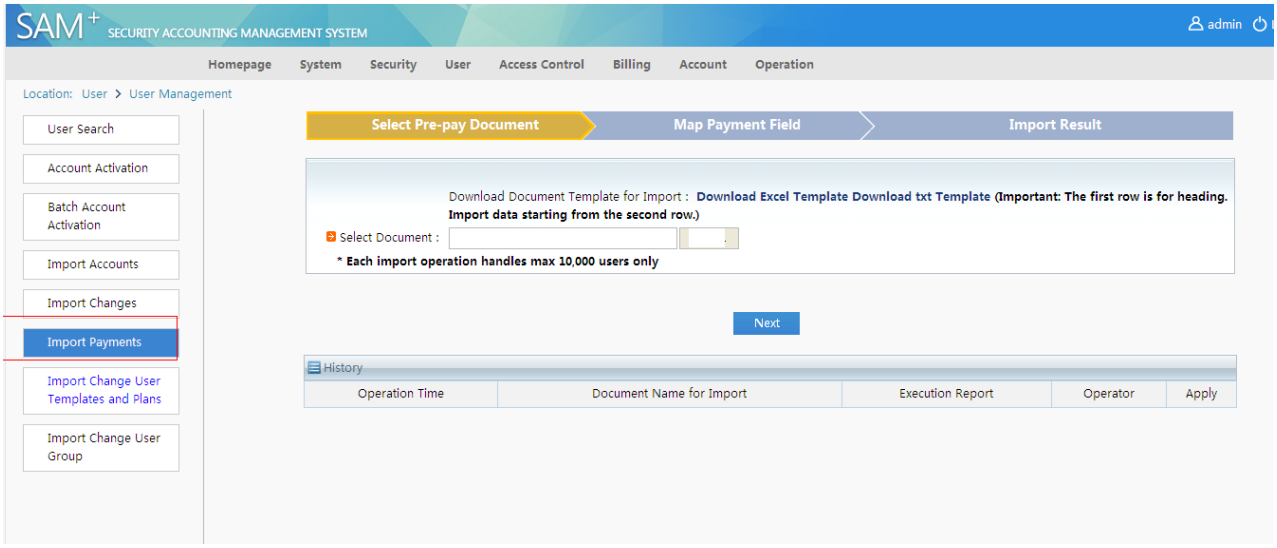
Field mapping page:



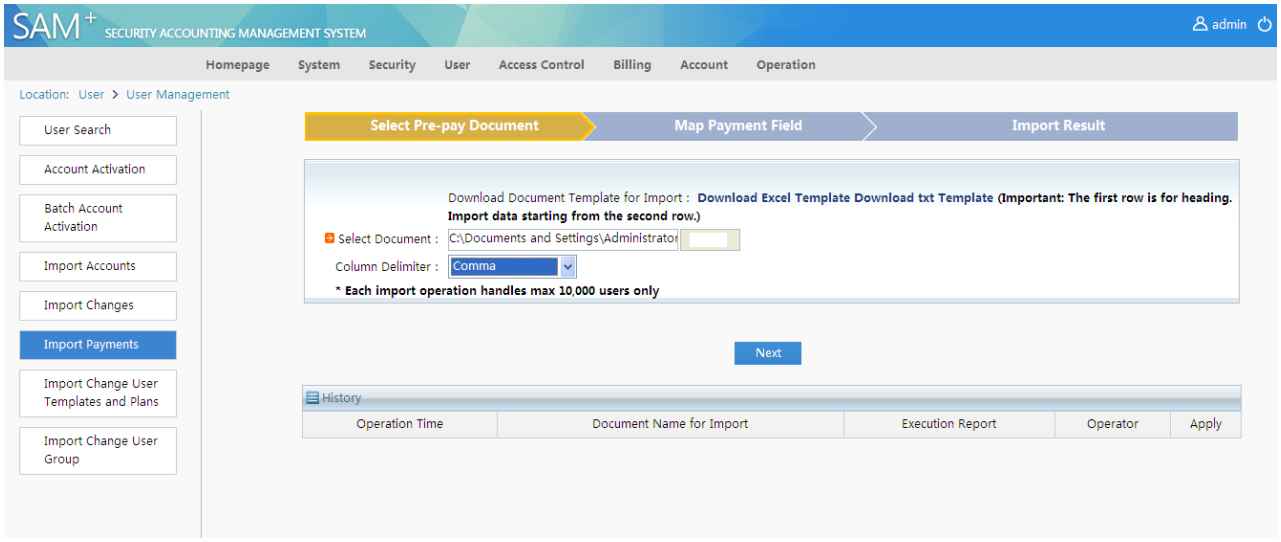


Import Payments

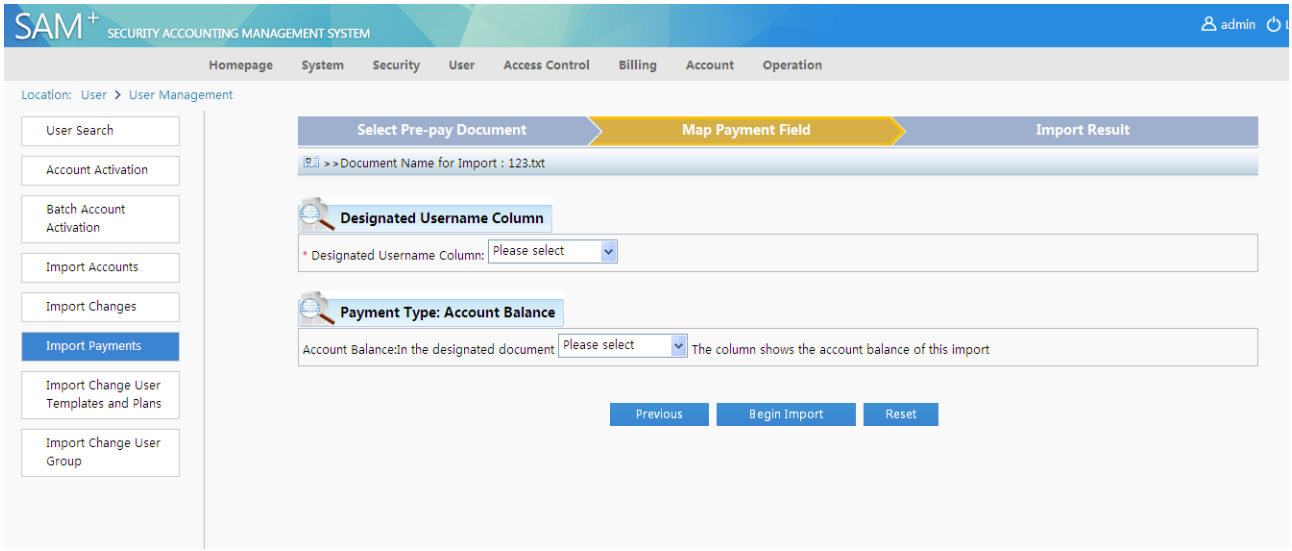
Entry of the payment import page:



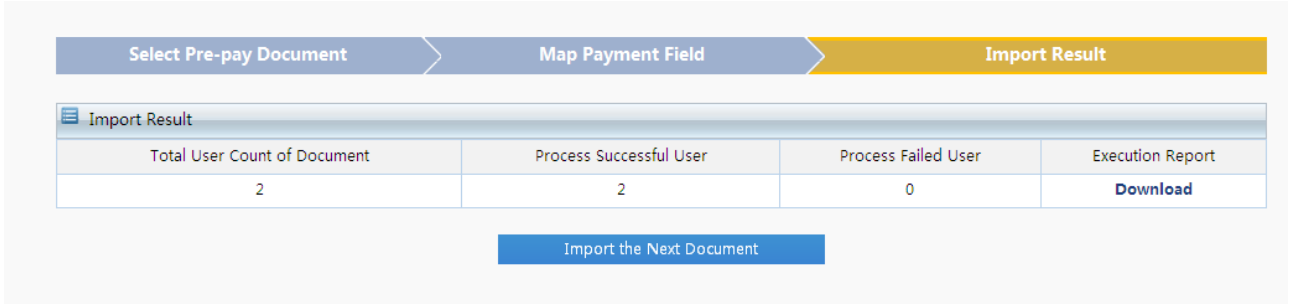
File selection page:



Field mapping page:

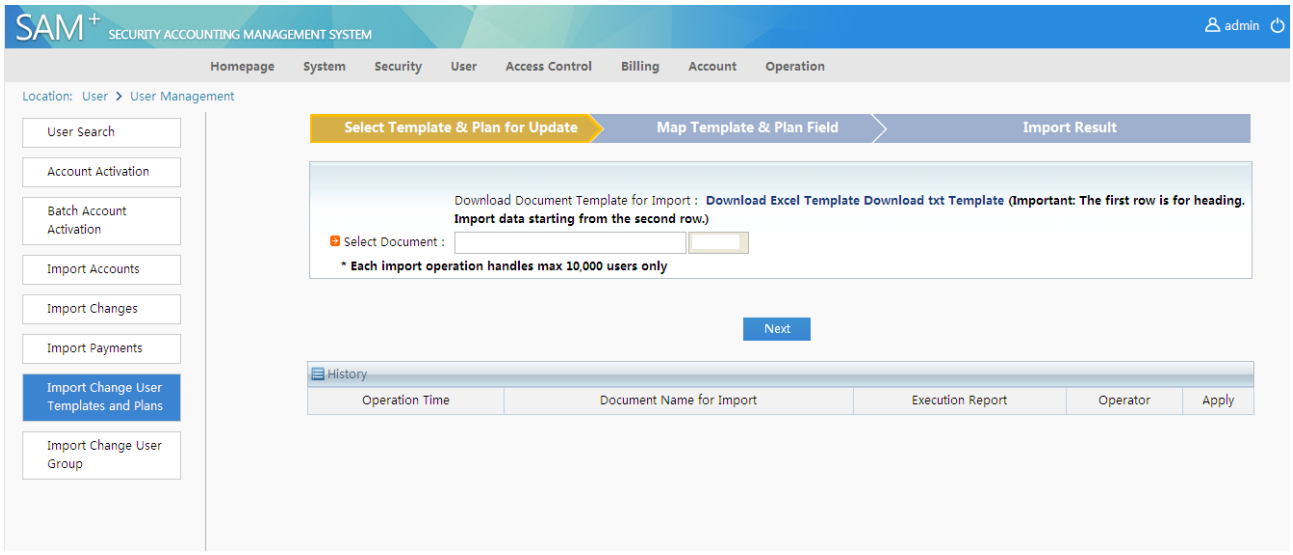


Import result page:

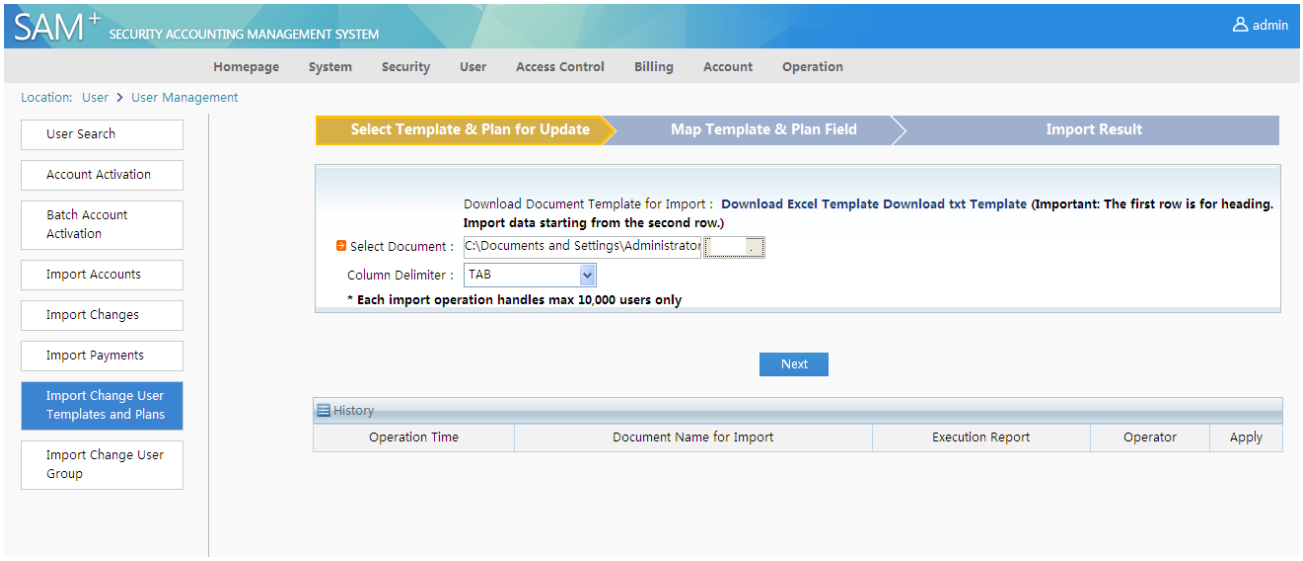


Import Change User Templates and Plans

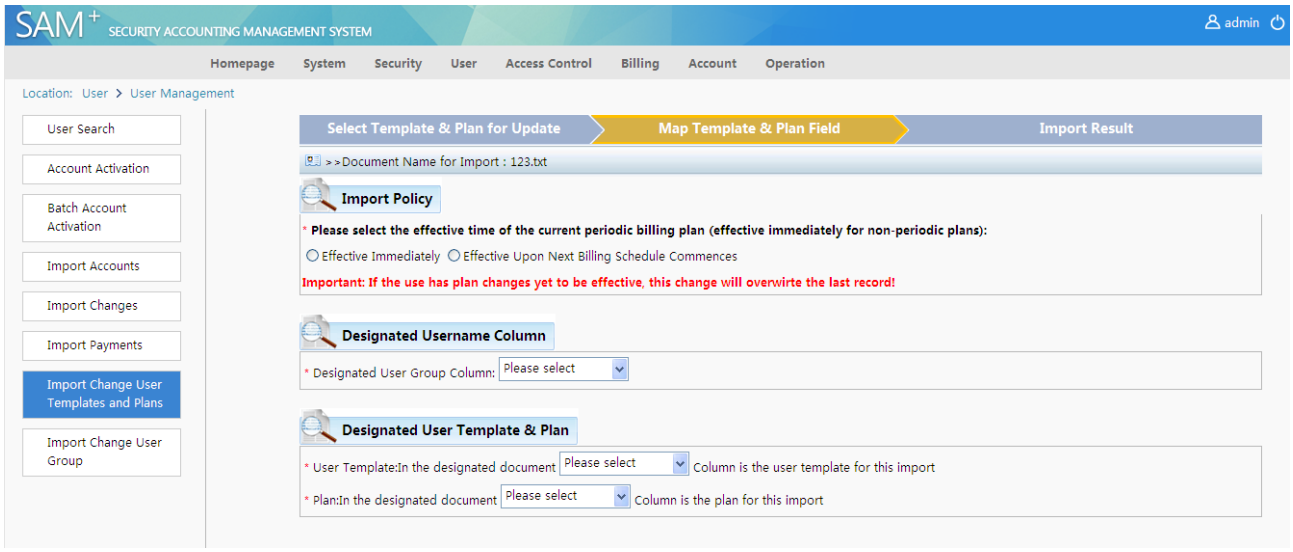
Entry of the **Import Change User Templates and Plans** page:



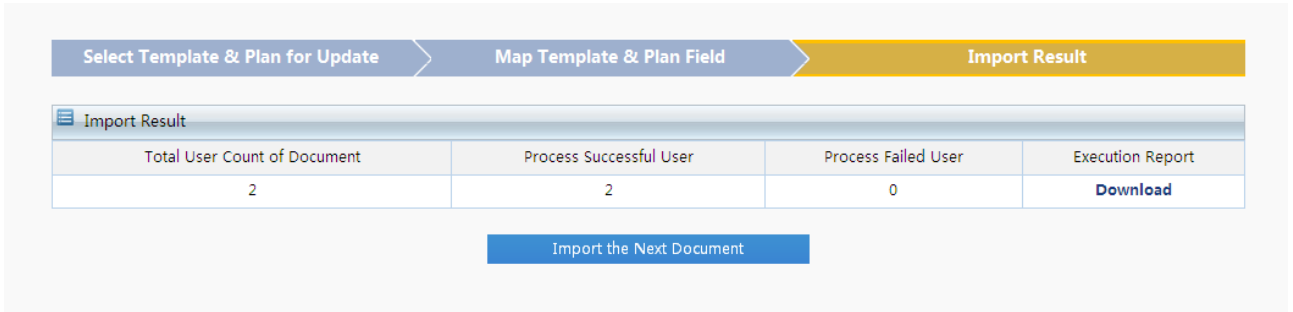
File selection page:



Field mapping page:

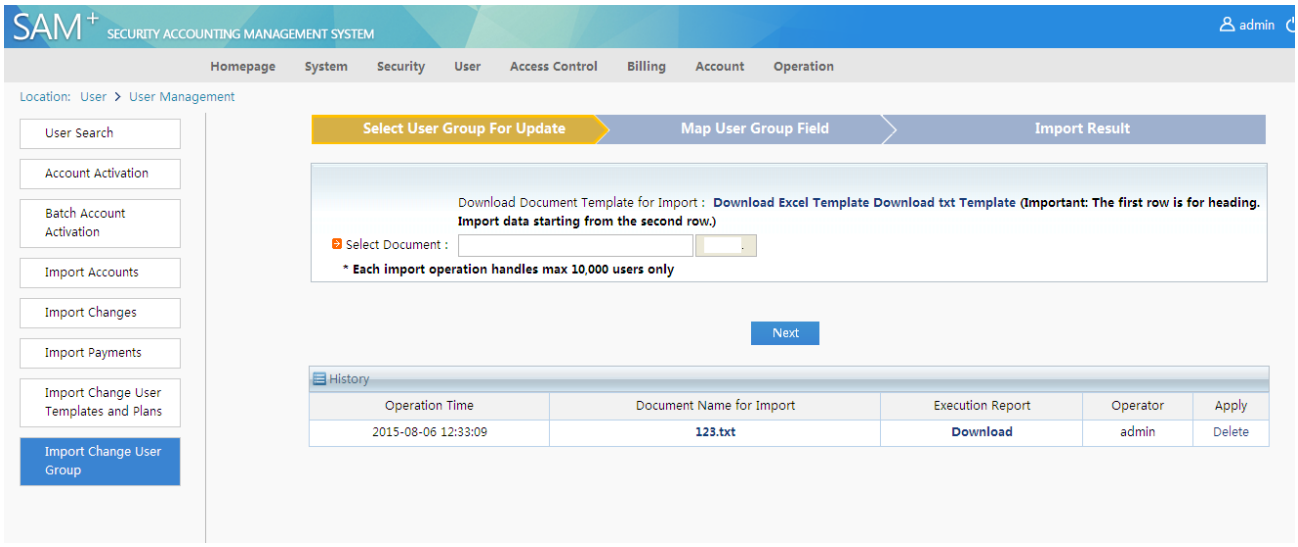


Import result page:

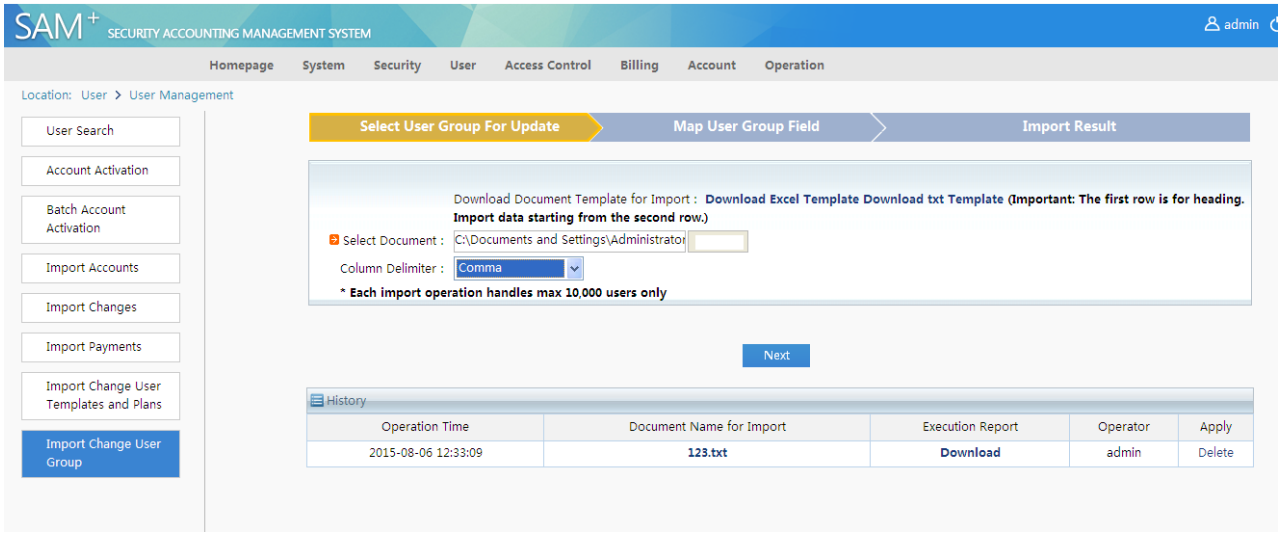


Import Change User Group

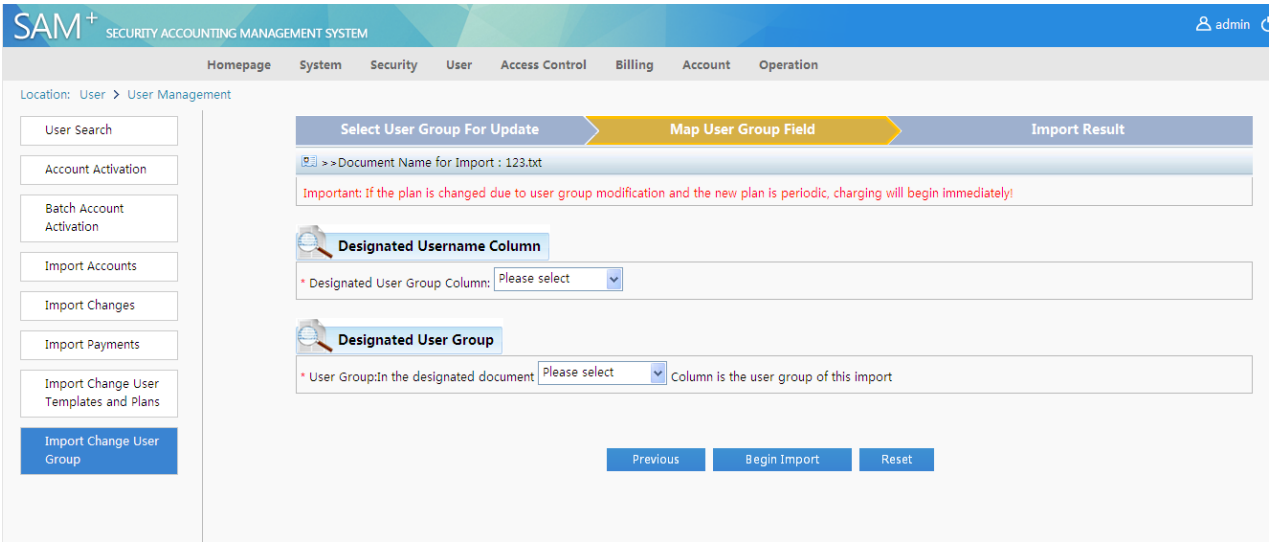
Entry of the **Import Change User Group** page:



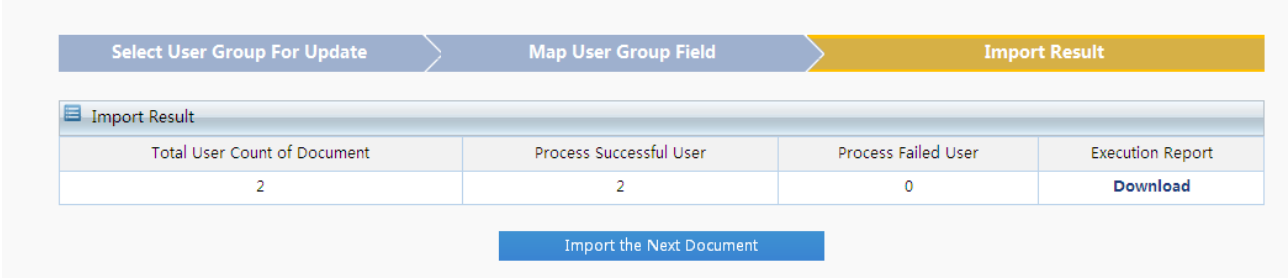
File selection page:



Field mapping page:



Import result page:



Note: When viewing user details, administrators can find that some users have IPv6 address information, such as the user IPv6 address and number of IPv6 addresses. Such information does not exist when a user is added. It is sourced from users who pass authentication and go online from machines using IPv6 addresses. The clients transmit the IPv6 address information to the RG-SAM+ system, which is recorded in user management and online user table.

Note

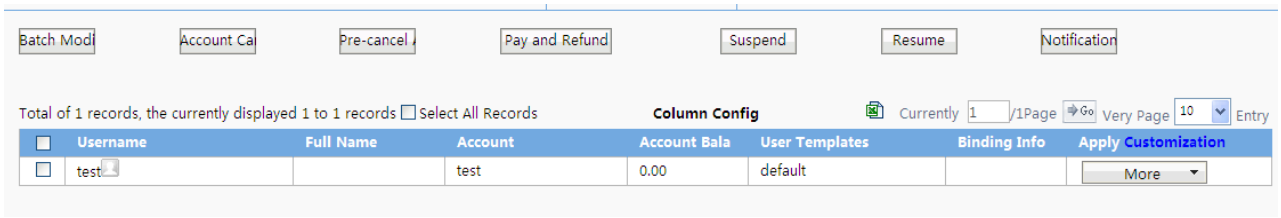
When a user is deleted, Internet access details and account flows of the user are not synchronously deleted, which need to be manually deleted.

Pre-cancelled Users

Pre-cancelled users cannot be created but are only converted from normal users and they cannot use any services of the system. Normal users in different user states can be converted into pre-cancelled users. In other words, conversion from normal users into pre-cancelled users is equivalent to the operation of transferring files in a hard disk to the recycle bin, where files can be cleared or restored. Likewise, pre-cancelled users can be completely deleted or converted into normal users.

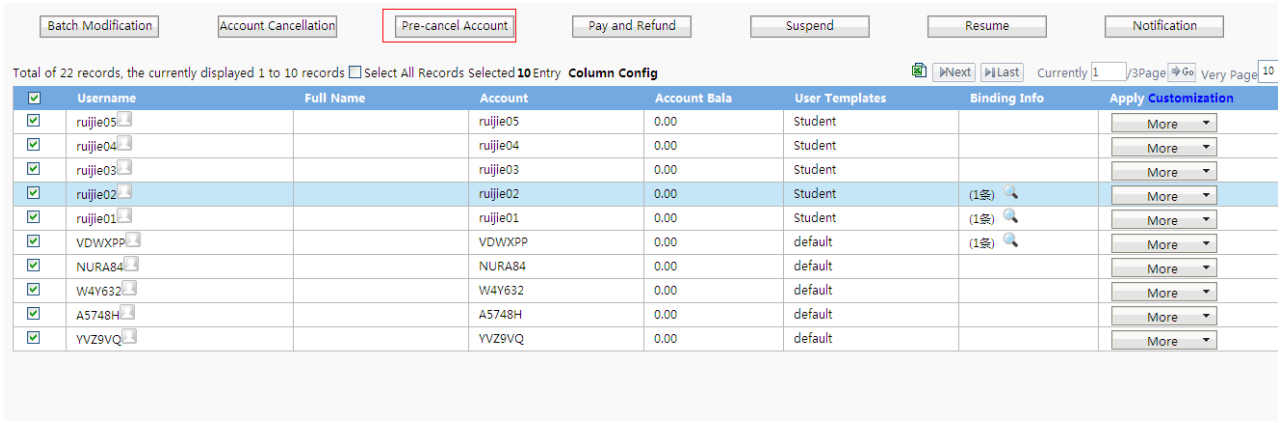
The basic deleting, modifying, query, and printing functions are available for pre-cancelled users.

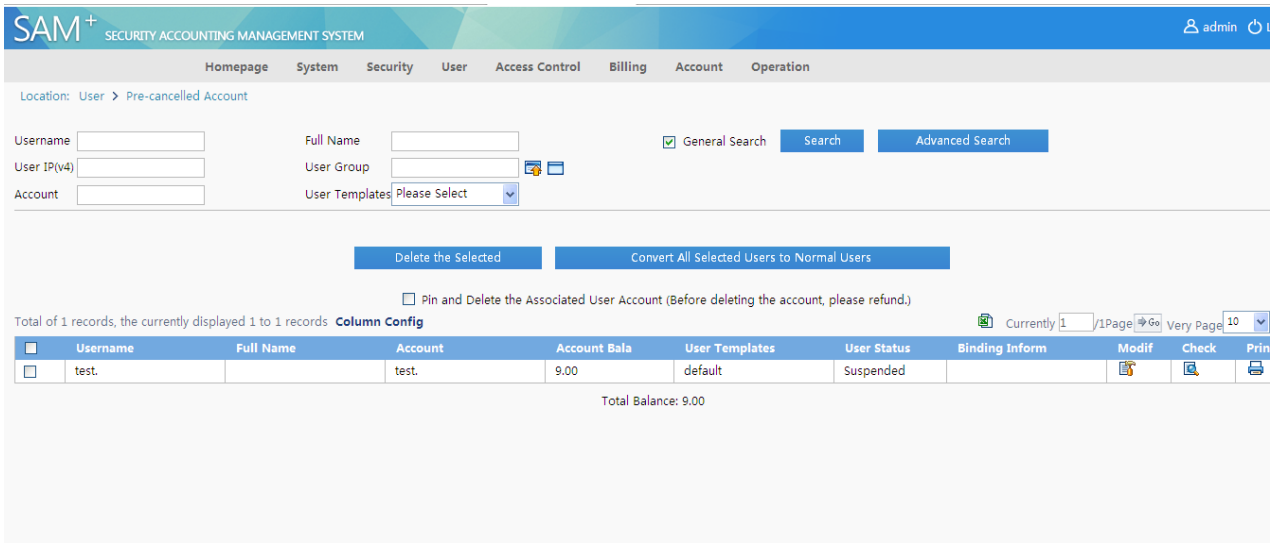
Click **Pre-cancel Account** to convert normal users into pre-cancelled users, as shown in the following figure.



If you select user **test** and click **Pre-cancel Account**, the user does not exist in normal user management and is transferred to the pre-cancelled user list.

On the **Pre-cancelled Account** page, you can click **Convert All Selected to Normal Users** to convert selected pre-cancelled users into normal users. Then, the users can pass authentication, access the Internet, and use system services. See the following figures.

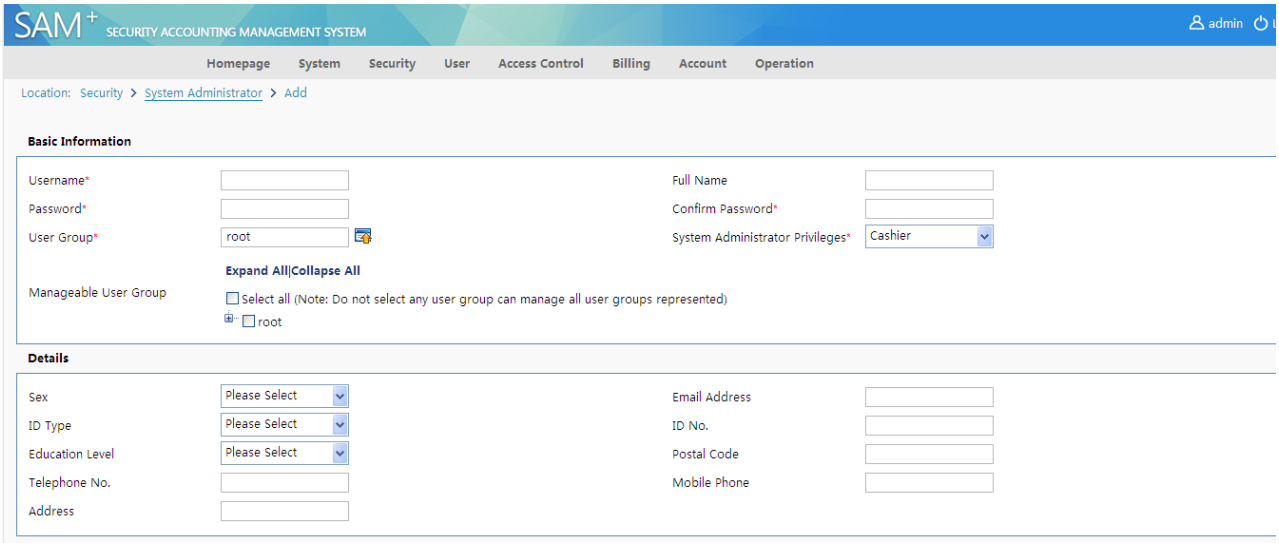




In the preceding figure, if you select user **test** and convert it into a normal user, the user can pass authentication, go online, and access the Internet again.

System Administrators

System administrators are a type of users who can log in to the management page of the RG-SAM+ system in Web mode and perform management operations. Choose **Security**>**System Administrator** to complete relevant system administrator operations. Operations that system administrators can perform on the management page of the RG-SAM+ system depends on their associated system management privileges. The default system management privileges of the system are cashier, network administrator, system administrator, financial administrator, and user administrator. (For details about system management privileges, see relevant sections in the system management privilege description.)



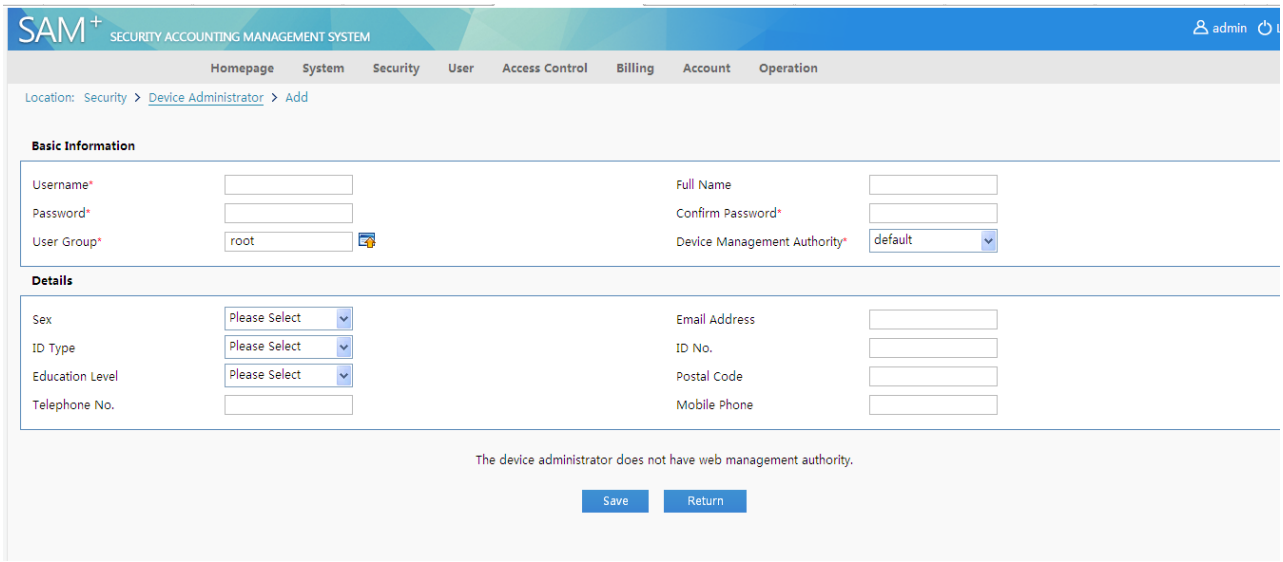
The preceding figure shows that in comparison with normal users, system administrators have one hallmark attribute in **Basic Information**: **System Administrator Privileges**, but do not have the account, billing policy, self-service privilege, service, and other attributes. System administrators manage the management page of the RG-SAM+ system. Different system administrators can be granted different functions, that is, system management privileges.

On the left of **System Administrator Privileges**, you can specify the user group to which an administrator belongs and user groups that can be managed by the administrator.

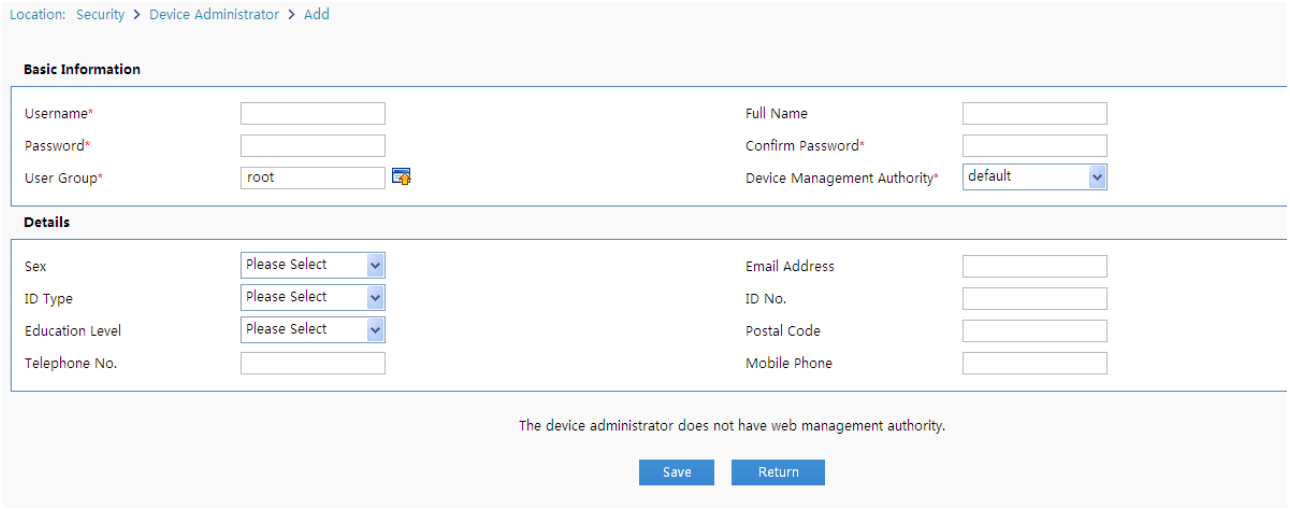
System administrators can set the IP address access control and access time range control.

A default system administrator named **admin** is created during system installation, who has all system management privileges. **admin** cannot be deleted or managed on the system administrator management page. You can log in to the system as user **admin** and click **admin** in the upper right corner to set administrator information and access control.

Device Administrators



Device administrators can log in to some network devices such as switches and routers in telnet mode and manage users. You need to choose **Security**>**Device Administrator** to complete settings and device administrators need to pass the RADIUS authentication to log in to the devices to be managed. Similar to system administrators, device administrators have device management privileges, which are used to set device groups that can be managed by each device administrator and management commands that can be used by each device administrator. For details about device management privileges, see the device management privilege section.



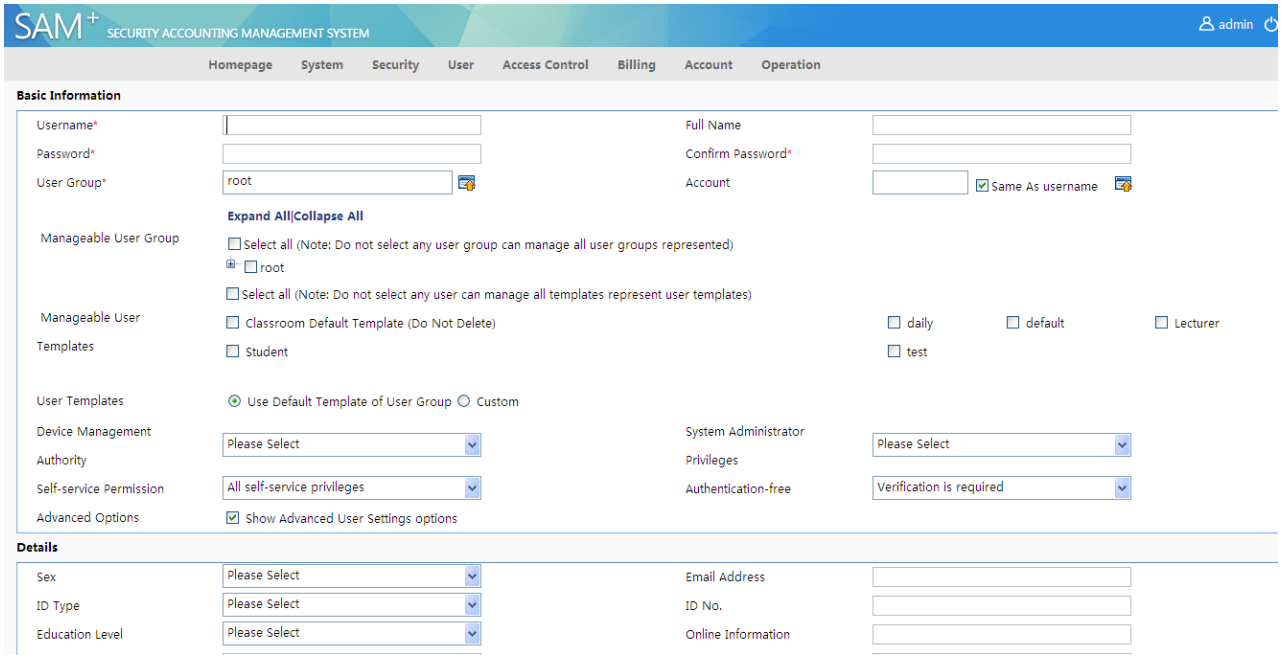
The preceding figure shows that in comparison with normal users, device administrators have **Device Management Authority** but do not have the account, billing policy, self-service privilege, service, and other attributes. Device administrators log in to network devices and perform management operations. They can be granted different functions, that is, device management privileges.

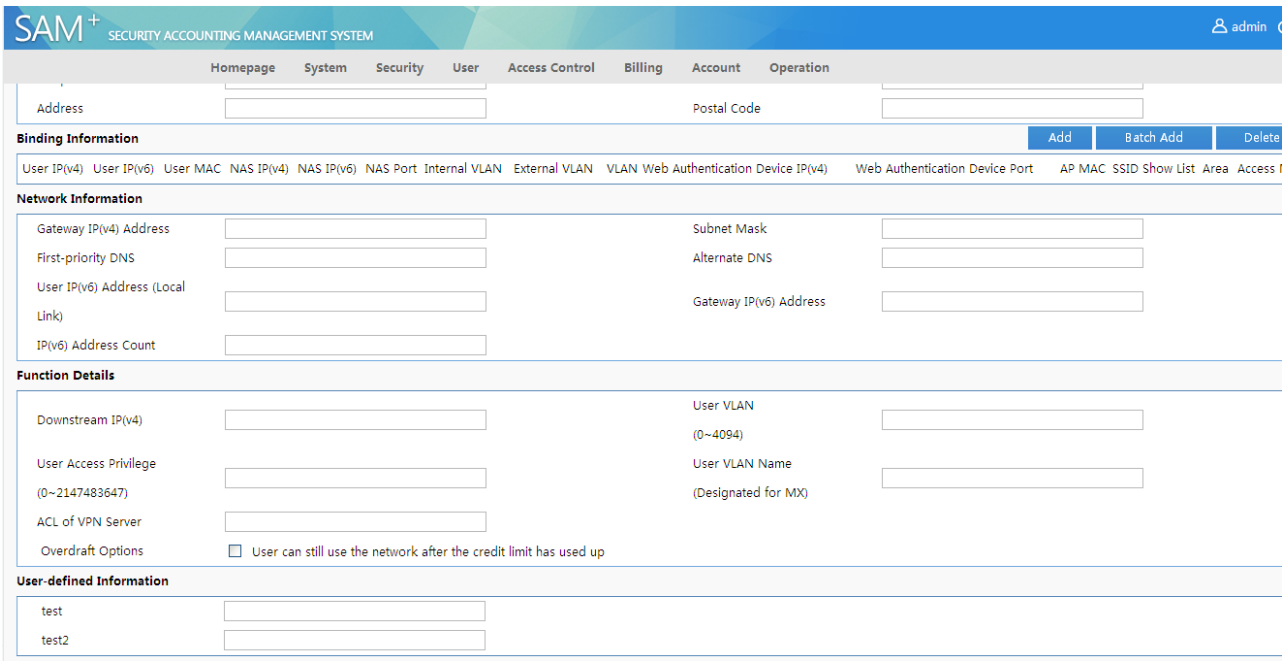
The basic adding, deleting, modifying, query, and printing functions are available for device administrators.

Customized Administrators

Customized administrators are a type of users defined in the RG-SAM+ system 3.X. Customized administrators can access the Internet in dial-up mode as normal users, manage the RG-SAM+ system as system administrators, manage devices as device administrators, and log in to the self-service end to perform self-service operations. In addition, customized administrators can be associated with user self-service privileges, system management privileges, and device management privileges, and have all attributes of normal users. Customized administrators are controlled by licenses. You can choose **Security**>**Custom Administrator** from the main menu to complete customized administrator settings.

The following figures show the page of adding a customized administrator.





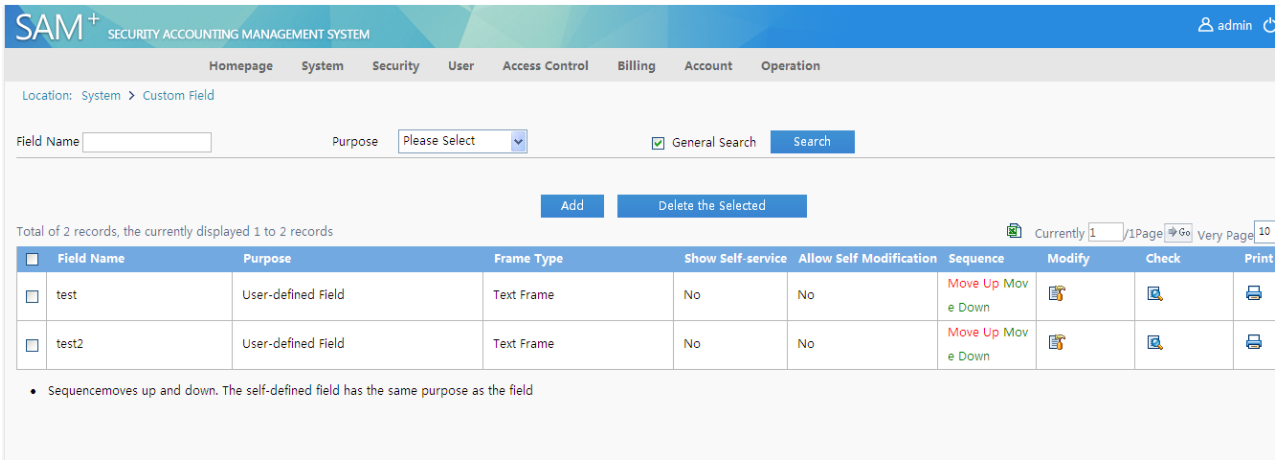
The device management privileges allow customized administrators to log in to devices and manage devices; the system management privileges allow customized administrators to access the management page of the RG-SAM+ system in Web mode and perform relevant operations within their privileges; the self-service privileges allow customized administrators to access the self-service page of the RG-SAM+ system in Web mode and perform relevant self-service operations within their privileges. Customized administrators have the account, billing policy, service, and other attributes of normal users, and can pass authentication, go online, and use services of the RG-SAM+ system as normal users. Nevertheless, attributes are optional for them except usernames and passwords. A customized administrator has no management privilege if no attribute is set. For example, if no system management privilege is set for a customized administrator, the customized administrator does not have the privilege to access the management page of the RG-SAM+ system in Web mode.

The basic adding, deleting, modifying, query, and printing functions are available for customized administrators.

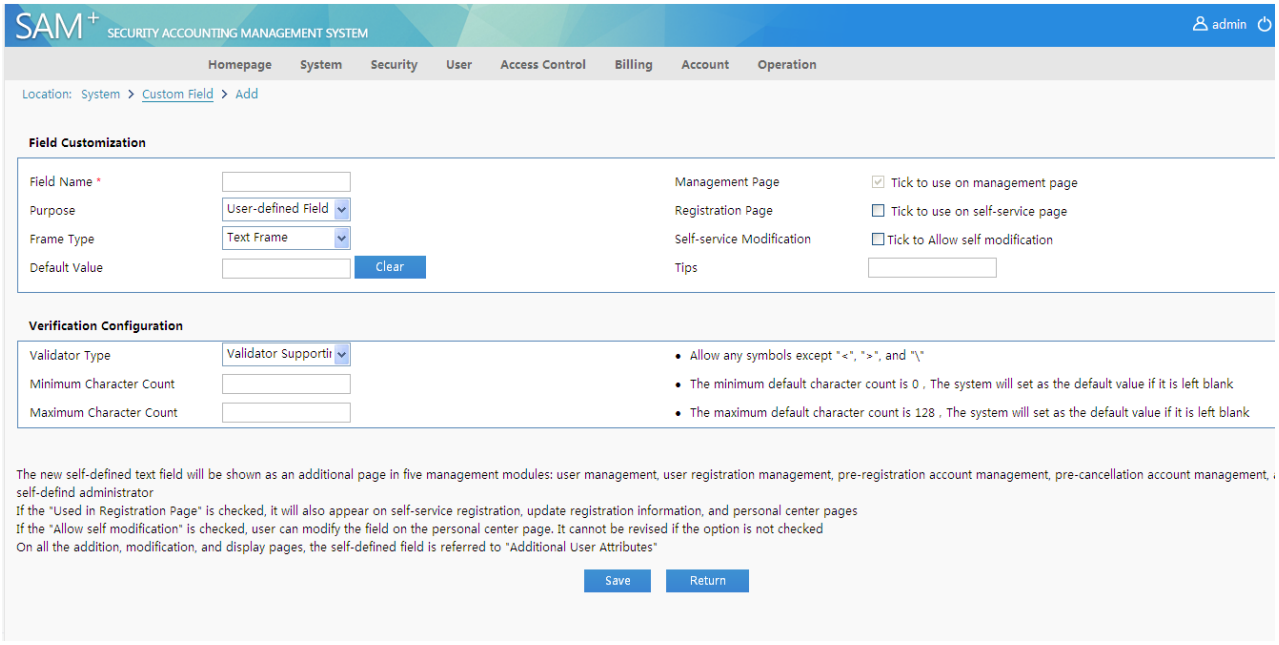
The pre-cancellation operation cannot be performed on customized administrators.

Custom Field

The RG-SAM+ system supports a maximum of 20 customized fields. The following figure shows the **Custom Field** page.



The following figure shows the operation page.

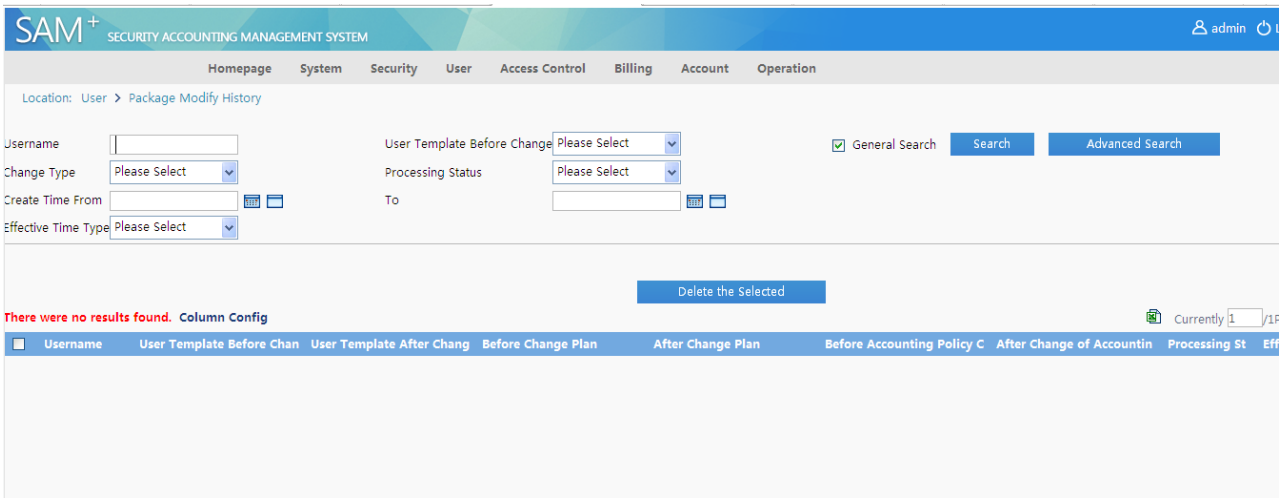


The operation is simple. You can follow prompts on the page to complete the field customization operation.

Package Modify History

Package Modify History refers to records about the change of billing plans made in self-service mode on the self-service page and the batch modification of user plans performed on the management page.

Billing plan change records can be queried, viewed, printed, and deleted on the management page. The following figure shows the **Package Modify History** page.



Guarantor and Guest

The guarantor and guest management enables administrators to manage guarantors (such as the guarantor ranking, activated SMS authorization code, and activated authorization QR code) and view and cancel temporary accounts of guests. You can choose **User**>**Guarantor and Guest** from the main menu to set the function. The function includes guarantor management and guest management.

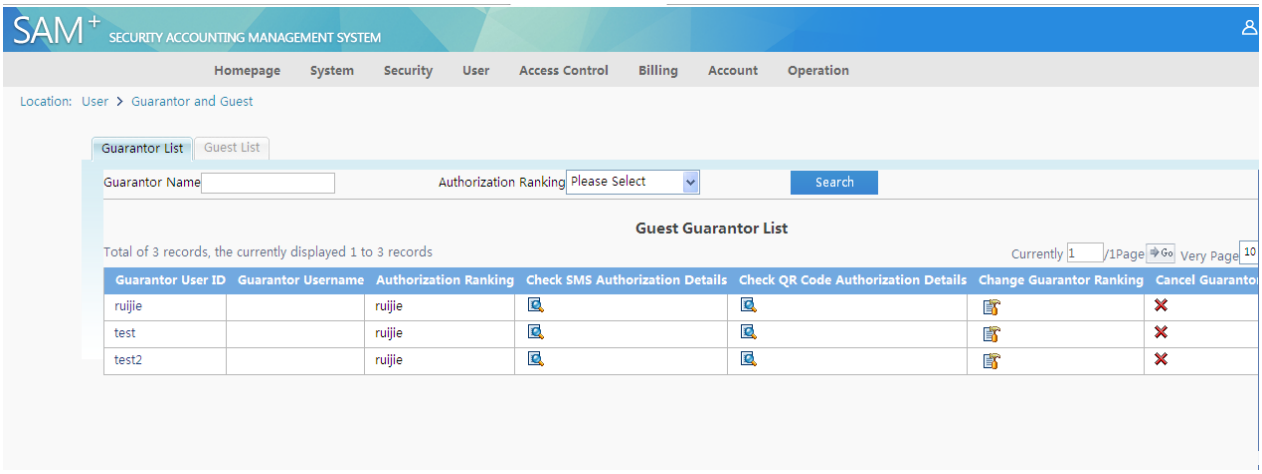
Guarantor Management

In guarantor management, you can manage the activated effective (or not effective) SMS authorization code or authorization QR code of a guarantor, cancel the account of a guest under the guarantor, view guarantor information, change the guarantor ranking, and cancel the guarantor's qualification.

The specific functions are as follows:

1) Search for guarantors.

For example, search for all guarantors with the username containing the letter z and the guarantor ranking of l1.



Administrators need to enter only search conditions, for example, keywords contained in usernames of guarantors (case-sensitive for letters) or guarantors' authorization ranking, and then click **Search**. Then, guarantors meeting the conditions are listed.

2) View information about the activated SMS authorization code of a guarantor.

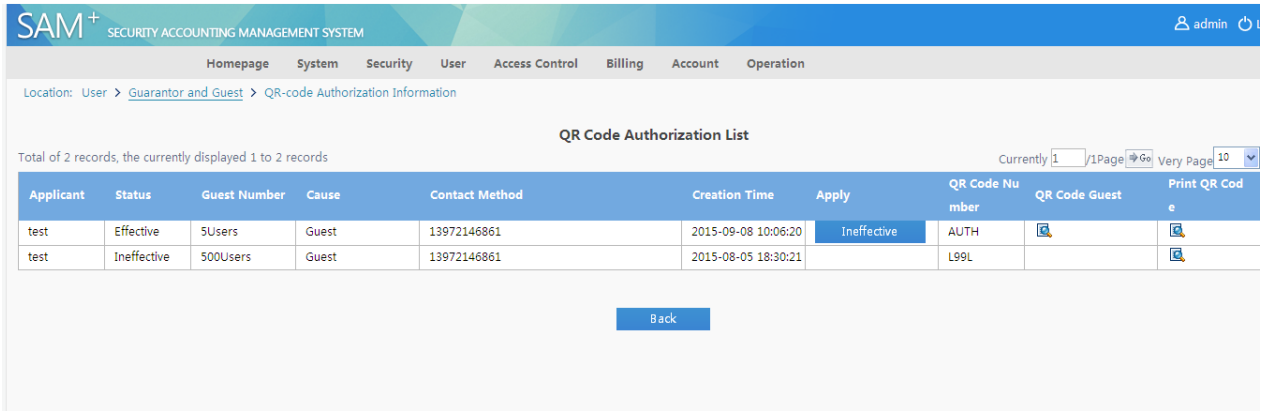
Administrators click  in **Check SMS Authorization Details** of a guarantor to view records about all activated SMS authorization codes of the guarantor, including the SMS authorization code, activation time, effective time, ineffective time, status, guest quantity, cause, and contact information.

The operation function in the SMS authorization code list allows administrators to change the status of the current SMS authorization code. For example, change a not effective SMS authorization code to an effective one or change an effective SMS authorization code to an ineffective one.

The function of viewing the guest list allows administrators to view information about the activated temporary account of an SMS authorization code. Administrators can cancel the account of a guest in the list.

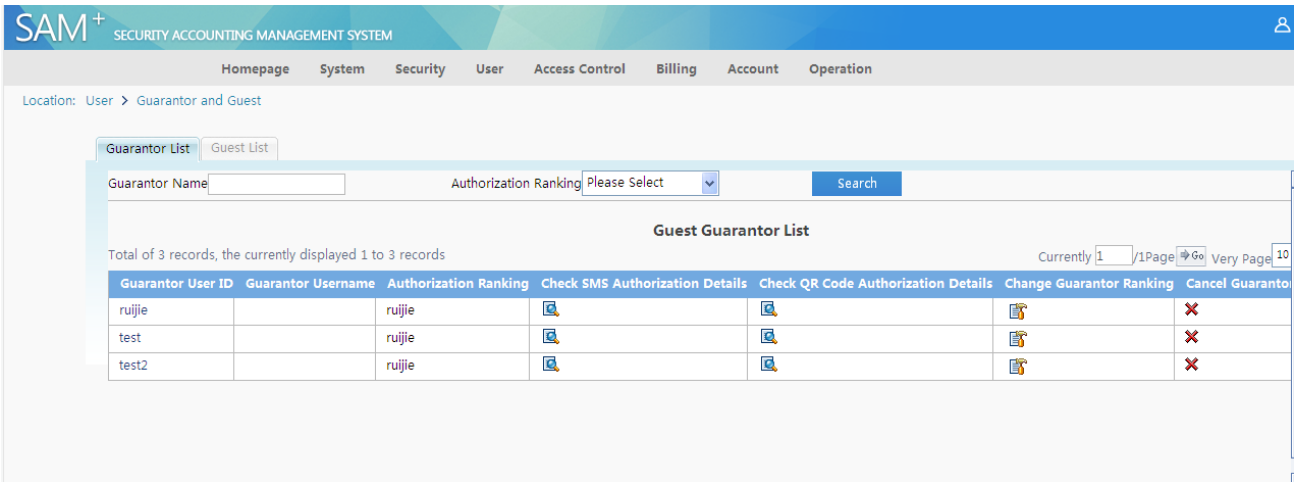
3) View the activated authorization QR code of a guarantor.

Administrators click  in **Check QR Code Authorization Details** of a guarantor to view records about activated authorization QR codes of the guarantor, including the activation time, effective time, ineffective time, status, guest quantity, cause, and contact information. See the following figure.



The operation function provided in the authorization QR code list allows administrators to change the status of a QR code. For example, you can change a not effective QR code to an effective one or change an effective QR code to an ineffective one.

The QR code guest function allows administrators to view all guests activated through the authorization QR code. Administrators can cancel the account of a guest in the list. See the following figure.



The **Print QR Code** function allows administrators to directly print a QR code for scanning.

4) View guarantor information.

Administrators can view guarantor details, including basic information, details, binding information, and network information. For details, see the user information section.

5) Change the guarantor ranking of a guarantor.

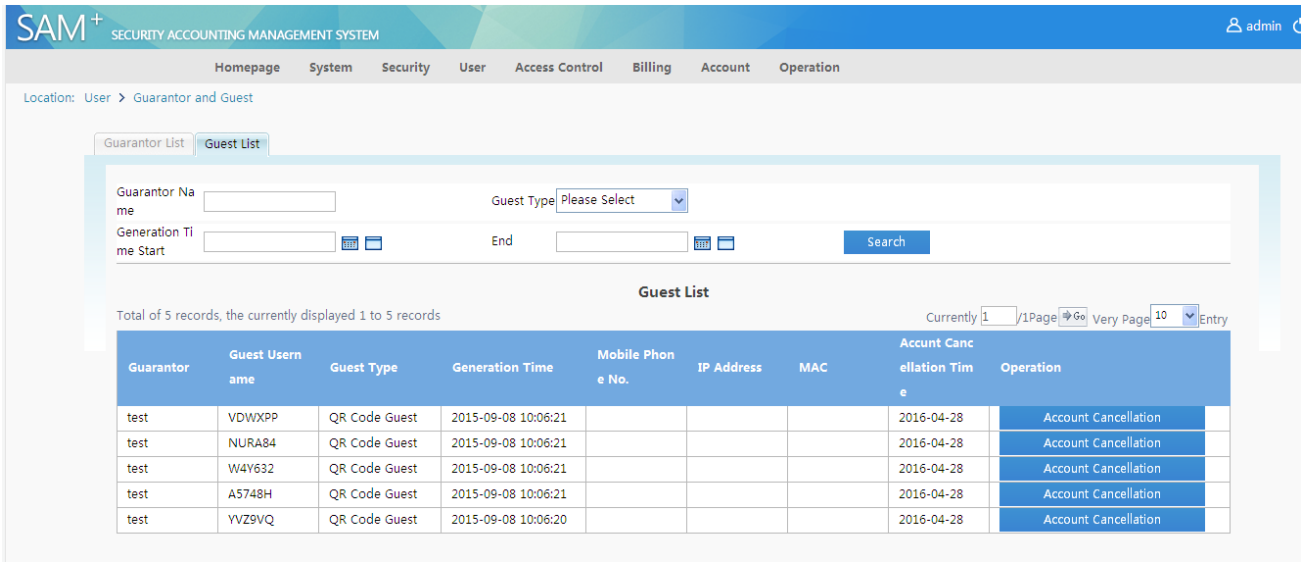
Administrators can change the ranking of a guarantor. Note: The ranking change of a guarantor will cause the cancellation of all temporary accounts that are in use under the guarantor. For the configuration of the guarantor ranking, see the guest authentication mode management section.

6) Delete the guarantor ranking

Administrators can delete the ranking of a guarantor. Note: The ranking deletion of a guarantor will cause the cancellation of all temporary accounts that are in use under the guarantor.

Guest Management

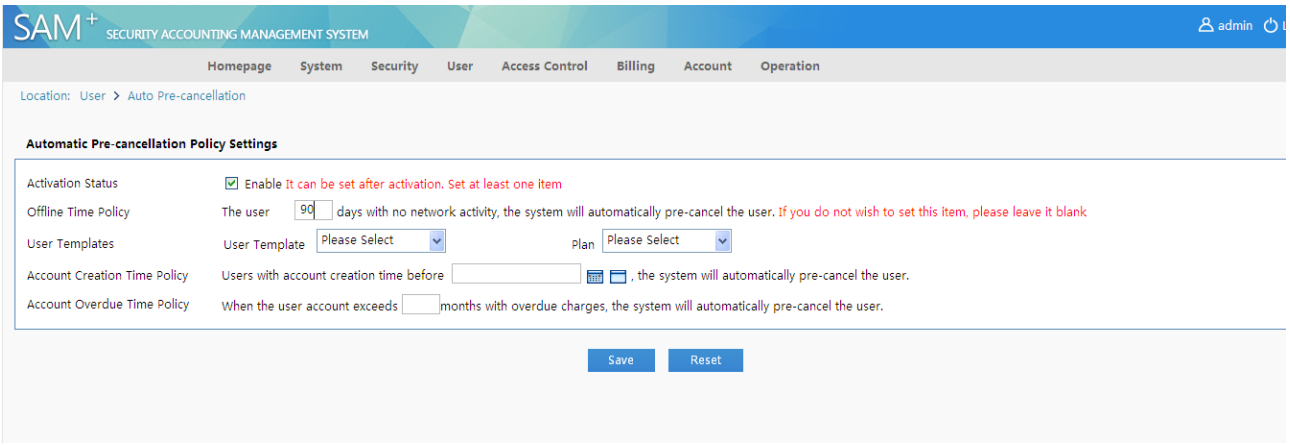
In guest management, you can view the list of temporary accounts of a guest. Administrators can directly cancel the temporary accounts of a guest. Choose **User**>**Guarantor and Guest** from the main menu and click the **Guest List** tab to view the list of all temporary guests.



1) Query temporary guests. Administrators can set the guarantor username keyword, guest type, time range of the activation of the SMS authorization code or authorization QR code to search for guest accounts to be handled.
2) Cancel temporary accounts. Note: Temporary accounts cannot be restored after cancellation. Therefore, exercise caution when cancelling temporary accounts.

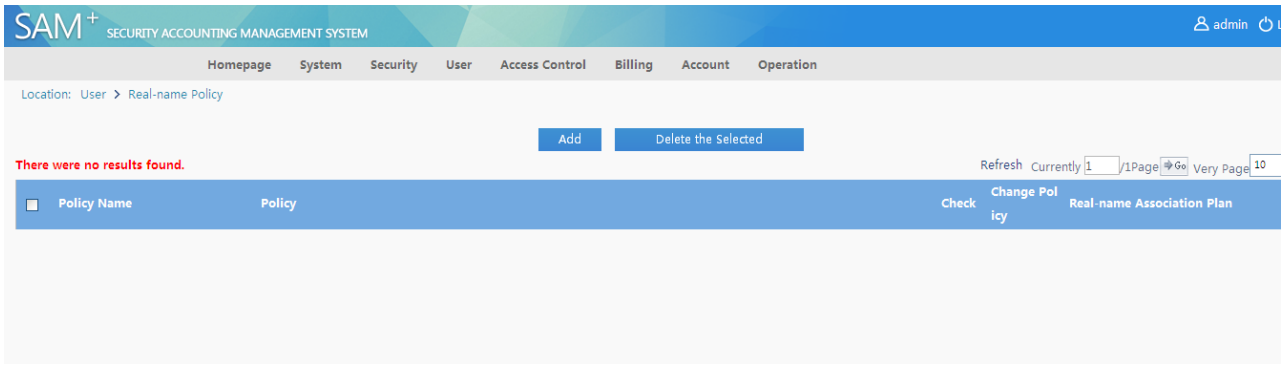
Automatic Pre-Cancellation Policy Settings

By setting the automatic pre-cancellation policy, you can perform pre-cancellation on users who do not apply for authentication within a period of time or on users who are activated prior to a time point.

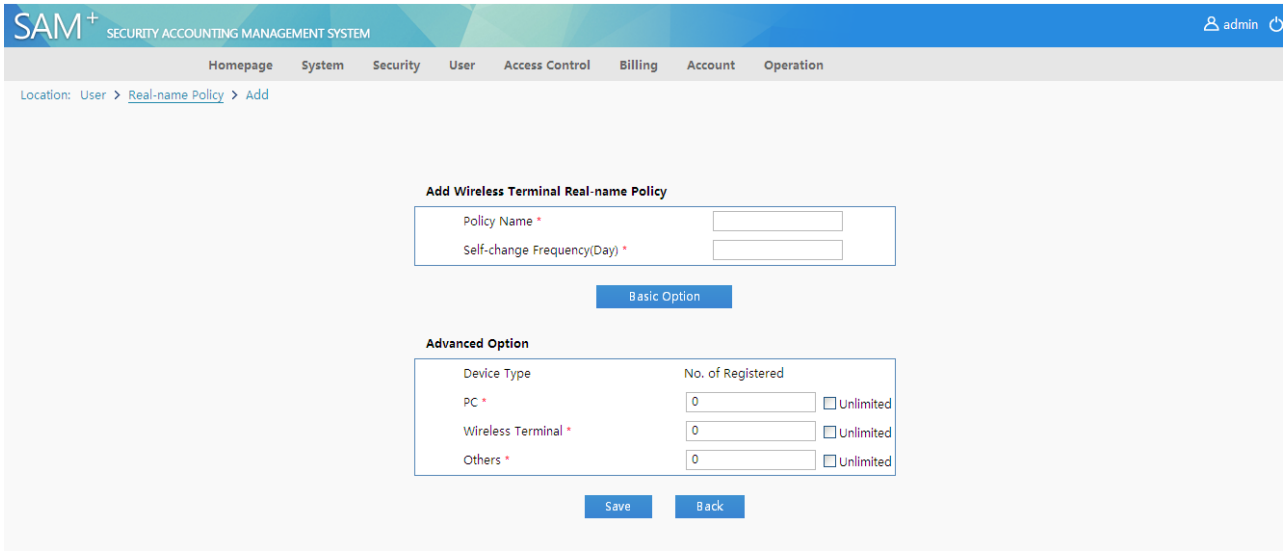


Offline Time Policy, **User Templates**, and **Account Creation Time Policy** can be flexibly combined. If a specific user template is selected for pre-cancellation, it is recommended that this template be combined with either or both of the offline time policy or account creation time policy.

Real-name Policy Management for Wireless Terminals

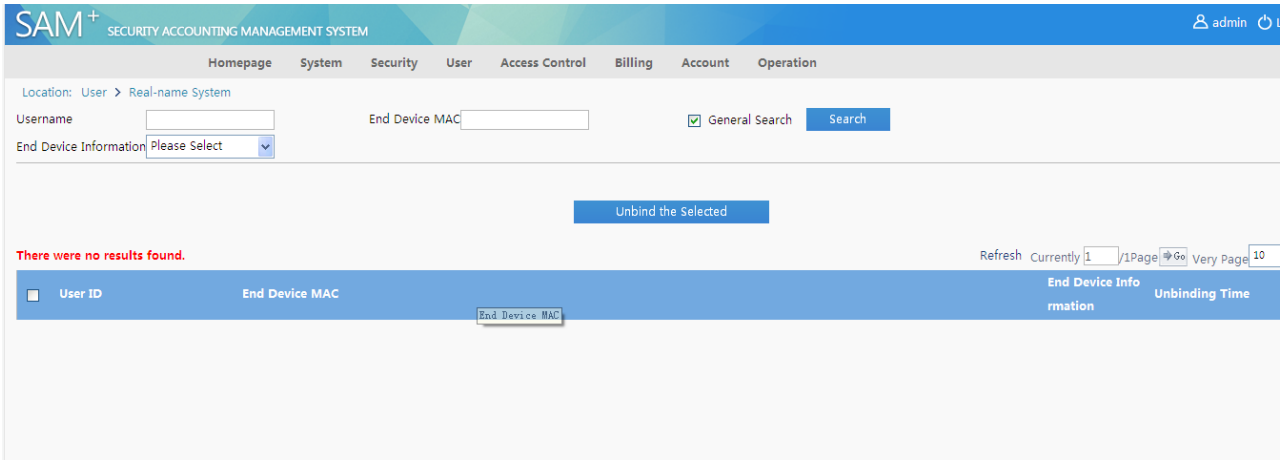


A real-name policy can be added or deleted.



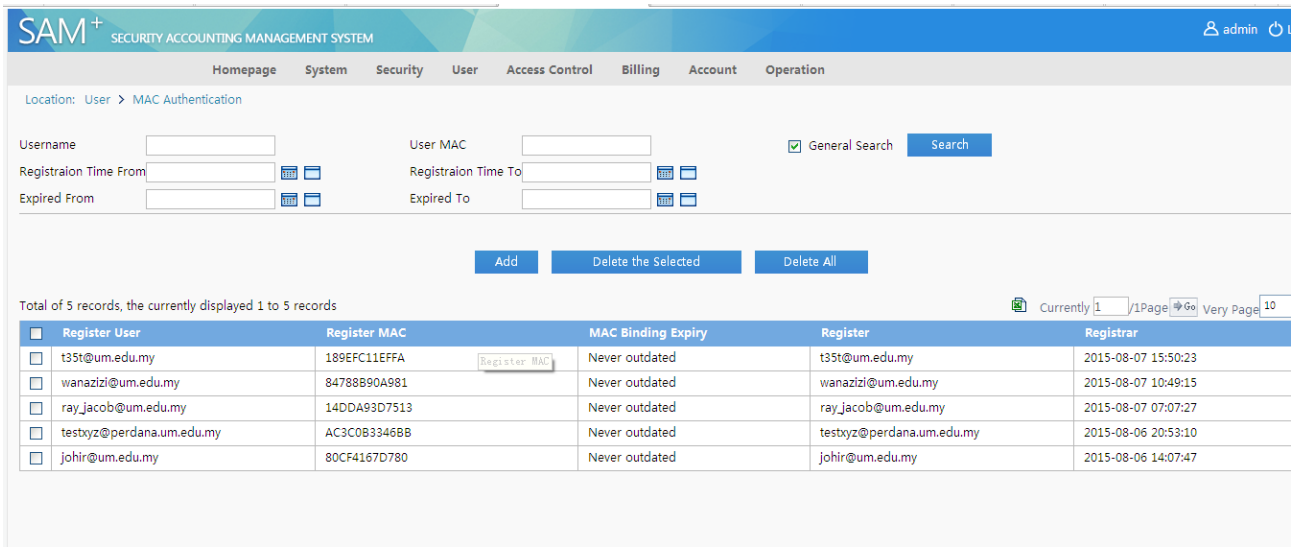
Real-name System Management for Wireless Terminals

Choose **User**>**Real-name System** to view the list of bound devices. You can also unbind bound devices.

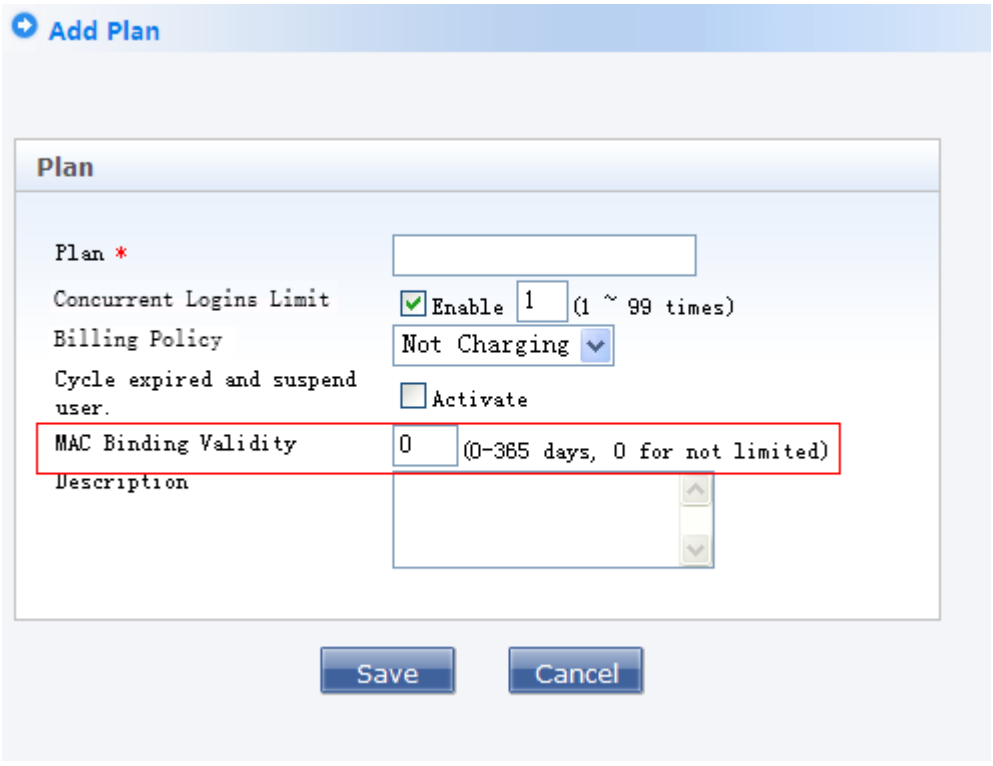


Quick MAC Authentication Management

Choose **User**>**MAC Authentication** from the main menu. The records about MAC address authentication are displayed. The records can be deleted.



You can set **MAC Binding Validity** (0-365 days) when adding a plan, as shown in the following figure. Bound MAC addresses are automatically unbound after the MAC address binding validity period expires.

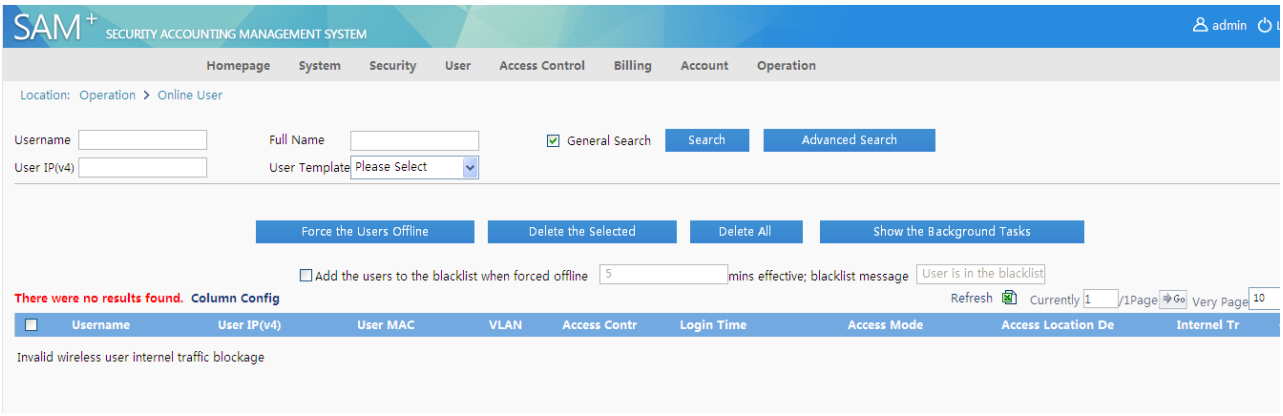


Online Users

A user can access the Internet in dial-up mode from Ruijie SU client after you add the user, set the Internet access service for the user, and complete billing association and account payment. The RG-SAM+ system records users' Internet access information and administrators can understand the Internet use conditions of users according to the information.

Online User Management

After a user goes online, the online user management of the RG-SAM+ system allows you to view online users, as shown in the following figure.



The preceding figure shows online users and their Internet access information, for example, IPv4 and IPv6 addresses used for Internet access. In addition, you can perform some operations on online users, for example, force users offline, send SMs, block the gateway traffic, and view the gateway traffic.

The gateway traffic query function requires the support of the gateway RG-NTD or RG-ACE, and only the RG-NTD supports the gateway traffic blocking function. Without the gateway support, the two functions are actually unavailable. In the gateway traffic billing scheme, you can view gateway traffic information of online users in real time to understand their gateway traffic consumption, and the gateway traffic blocking function allows you to manually control in real time whether users can access a network outside the gateway. If the gateway traffic blocking function is enabled for a user using the gateway traffic-based billing scheme, the user cannot access network resources outside the RG-NTD.

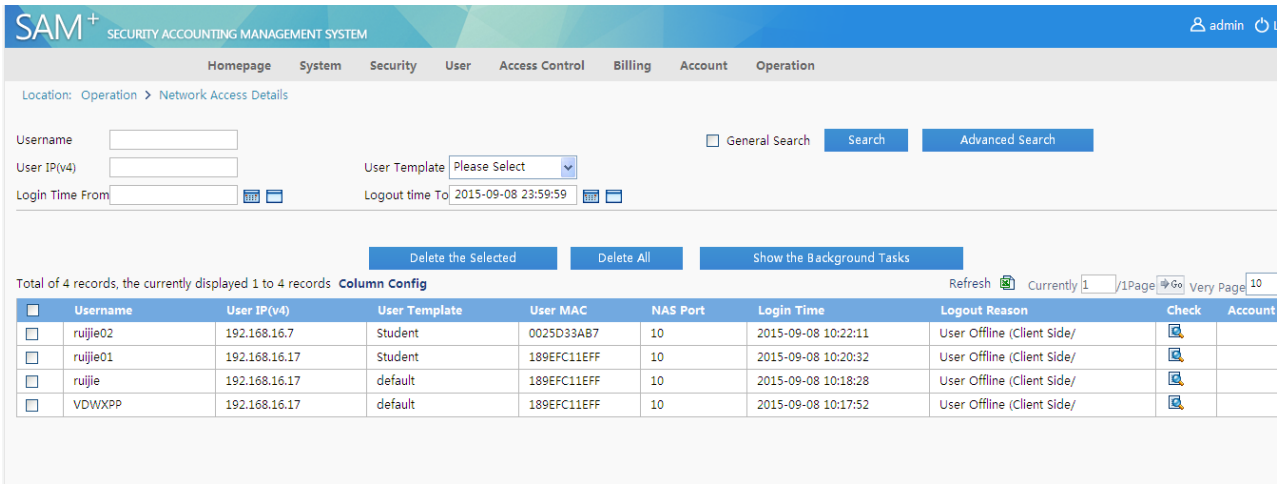
The functions of forcing users offline and sending SMs are described in the device section. They need the support of Ruijie switches. You can view descriptions of a relevant product to understand the function support conditions. In general, it is recommended that the function of forcing users offline be used in combination with the blacklist function because a client automatically goes online in dial-up mode again after being forced offline. Therefore, if your purpose is to make a user not go online any longer or for a period time, you need to blacklist the user and force the user offline.

The function of sending SMs is a pragmatic function provided for administrators to send notifications in real time. Online users can receive SMs sent from administrators through clients in real time. Note that correct community values need to be set for devices and the community must be granted the rw permission. The function of sending SMs needs the support of Ruijie switches and the clients must be Ruijie SUs.

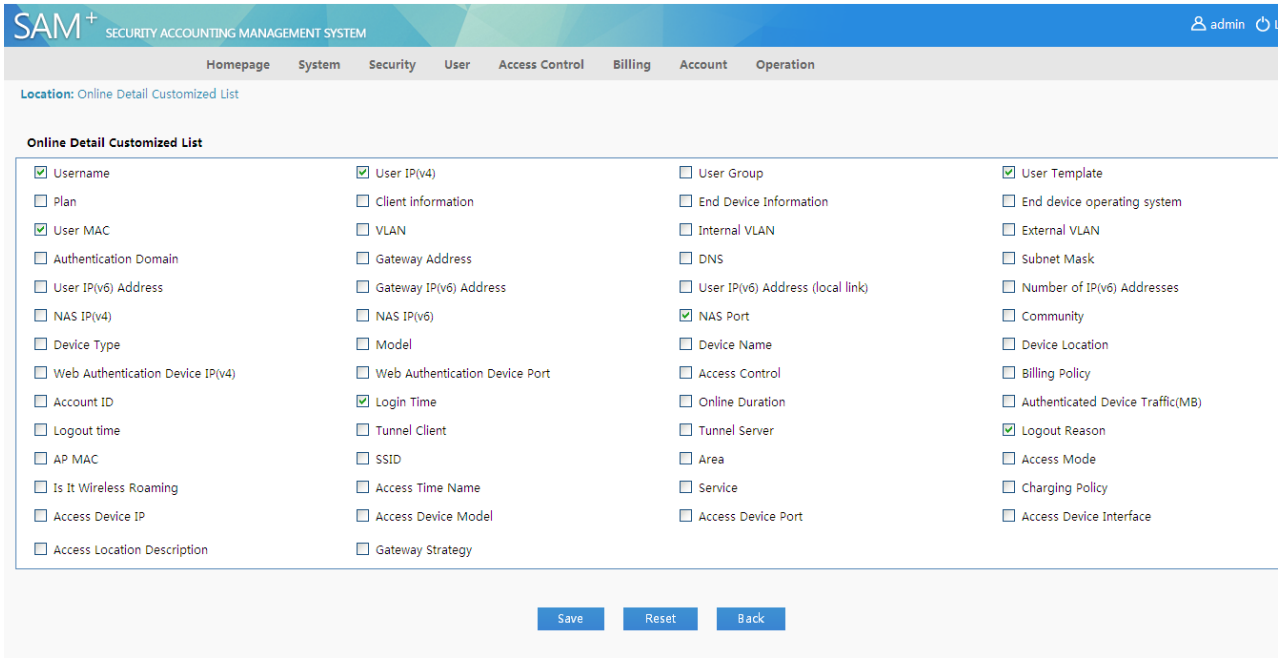
In addition to preceding functions, the search, batch deletion, advanced search, and details view are available for online users. The operation procedures of these functions are similar to those of other functions and are not described here. The batch deletion function is used to manually delete records of online users when online user information in the RG-SAM+ system is inconsistent with online user information in the switch. For example, many online users are falsely online because of a power failure of the switch or other causes. Before the power recovery of the switch, the batch deletion function can be used to delete online user information so that correct online user information is displayed in the online user table after the power recovery of the switch.

Internet Access Details

Internet access details are generated after online users go offline. Administrators can view Internet access details to clearly know the Internet access time of a user, IP address and MAC address used for Internet access. Administrators can also analyze Internet access behaviors of Internet access users based on the Internet access details, for example, the offline cause recorded in the Internet access details is a good entry point for analysis. By analyzing offline causes, administrators know the current network situation and Internet access behaviors and habits of Internet access users. Then, network administrators can restructure or optimize the network accordingly.

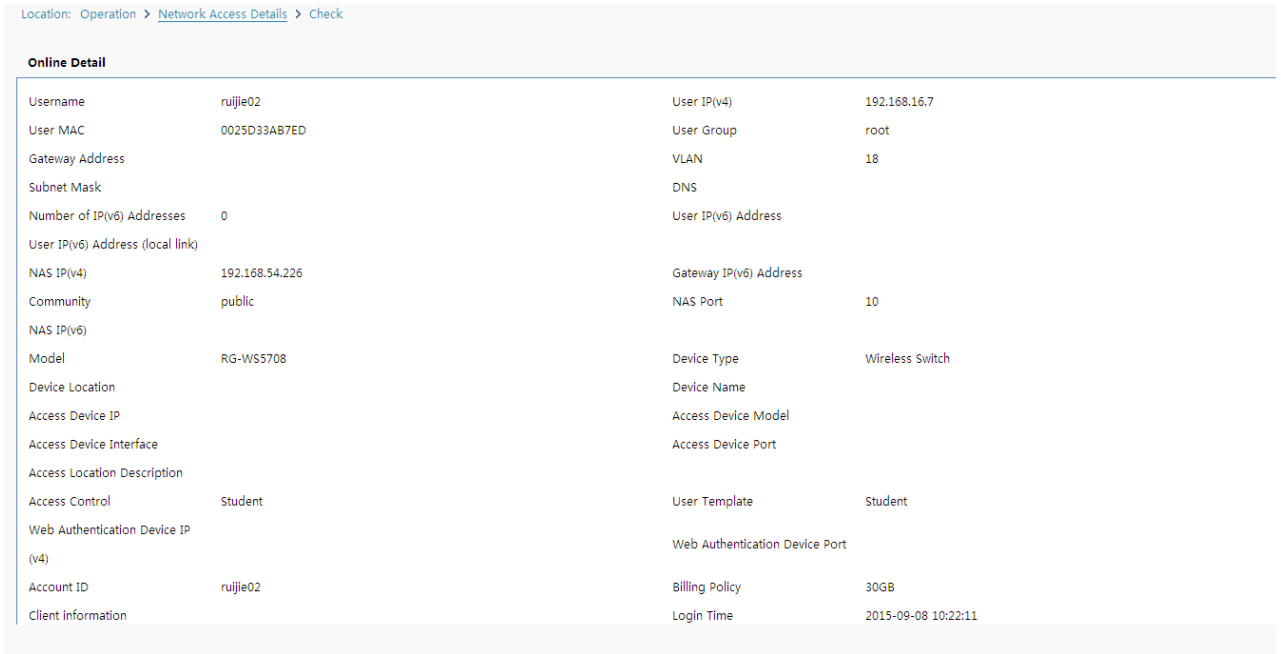


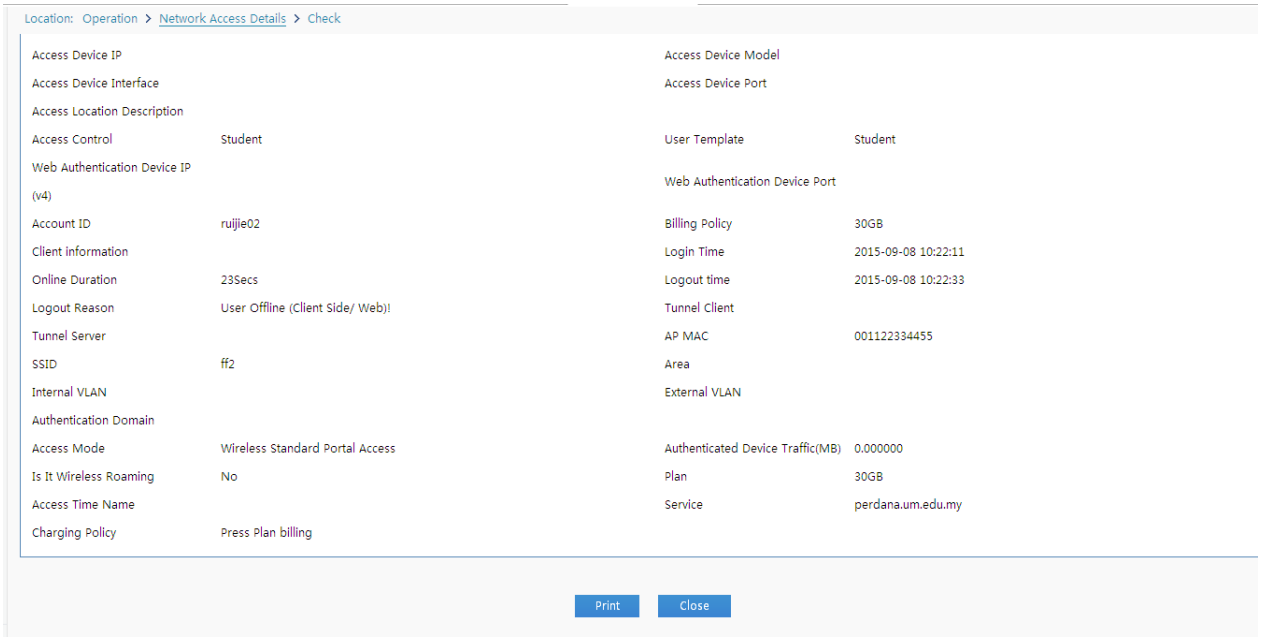
The preceding figure shows the Internet access details list, which displays the items that concern customers most. You can click **Online Detail Customized List** to customize items to be displayed in the Internet access details list as required. The following figure shows the page of customizable items. After an item is selected, information about the item is displayed in the Internet access details list.



Note that Internet access details are history records of online users, including services used by the users, and their IP addresses. Some information displayed may be different from current user information because of user information changes, which is reasonable.

Click  in the **Check** column for one Internet access details record or double-click a specific Internet access details record. A page as shown in the following figures is displayed.





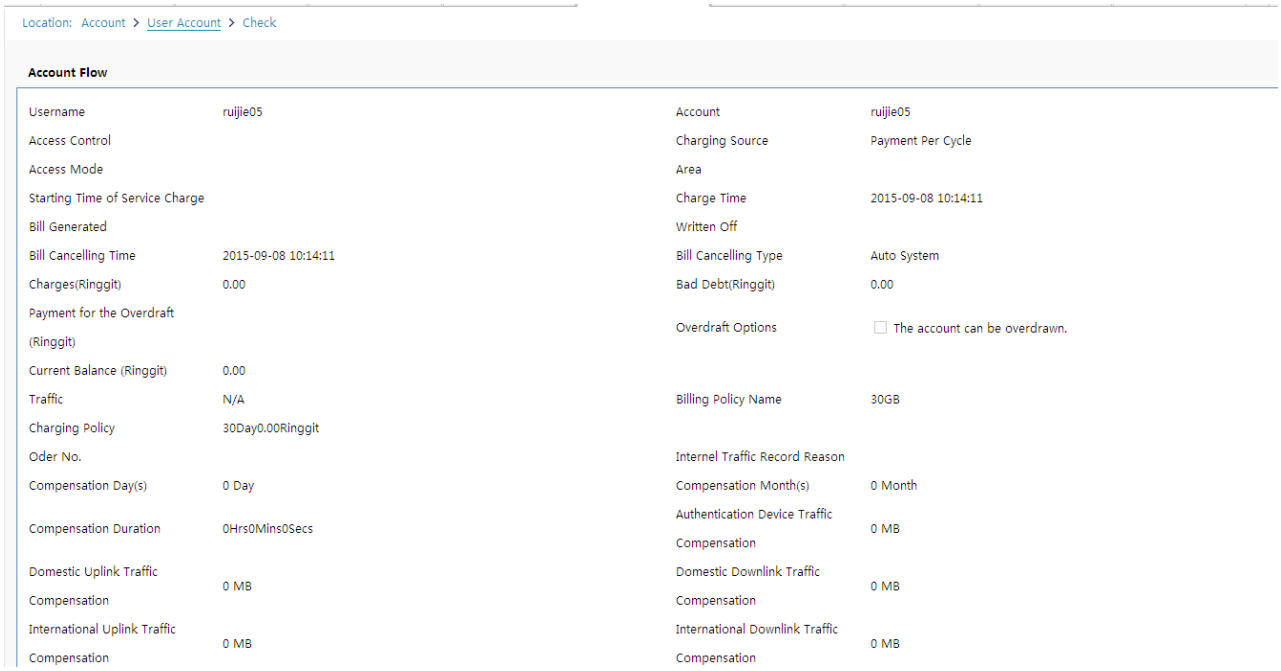
User IP address information is the network information used for the Internet access and is not described here. The following describes the IPv6 address information and **Tunnel Client** and **Tunnel Server** in the VPN scheme:

IPv6 address information: includes the user IPv6 address, IPv6 address quantity, and gateway IPv6 address, which are not recorded in the Internet access details if no IPv6 address is configured for the client.

VPN scheme information: includes **Tunnel Client** and **Tunnel Server**. **Tunnel Client** refers to the external network IP address of a client that accesses the Intranet through the VPN server in the VPN scheme, and **Tunnel Server** refers to the external IP address of the VPN server in the VPN scheme. For more details, see the relevant RFC document. The two items are blank for users who access the Intranet not through the VPN server.

Note that a large number of Internet access details are generated every day and the amount is astounding after a long time. Therefore, the RG-SAM+ system provides the function of automatically and periodically deleting Internet access details. The relevant configuration is described in the system maintenance section. Automatic clearing is indispensable and is a guarantee for continuous and stable running of the RG-SAM+ system.

An account flow is generated for an Internet access detail record requiring accounting. You can click the button in the **Account Flow** column to view the account flow of an Internet access detail record. A page similar to the following is displayed. No account flow will be generated for Internet access details that do not require accounting and no buttons will be displayed in the **Account Flow** column.



Location: Account > User Account > Check

Account Flow

Username	ruijie05	Account	ruijie05
Access Control		Charging Source	Payment Per Cycle
Access Mode		Area	
Starting Time of Service Charge		Charge Time	2015-09-08 10:14:11
Bill Generated		Written Off	
Bill Cancelling Time	2015-09-08 10:14:11	Bill Cancelling Type	Auto System
Charges(Ringgit)	0.00	Bad Debt(Ringgit)	0.00
Payment for the Overdraft (Ringgit)		Overdraft Options	The account can be overdrawn.
Current Balance (Ringgit)	0.00		
Traffic	N/A	Billing Policy Name	30GB
Charging Policy	30Day0.00Ringgit		
Oder No.		Internel Traffic Record Reason	
Compensation Day(s)	0 Day	Compensation Month(s)	0 Month
Compensation Duration	0Hrs0Mins0Secs	Authentication Device Traffic Compensation	0 MB
Domestic Uplink Traffic Compensation	0 MB	Domestic Downlink Traffic Compensation	0 MB
International Uplink Traffic Compensation	0 MB	International Downlink Traffic Compensation	0 MB

Note

IP address display in wireless access mode in Internet access details

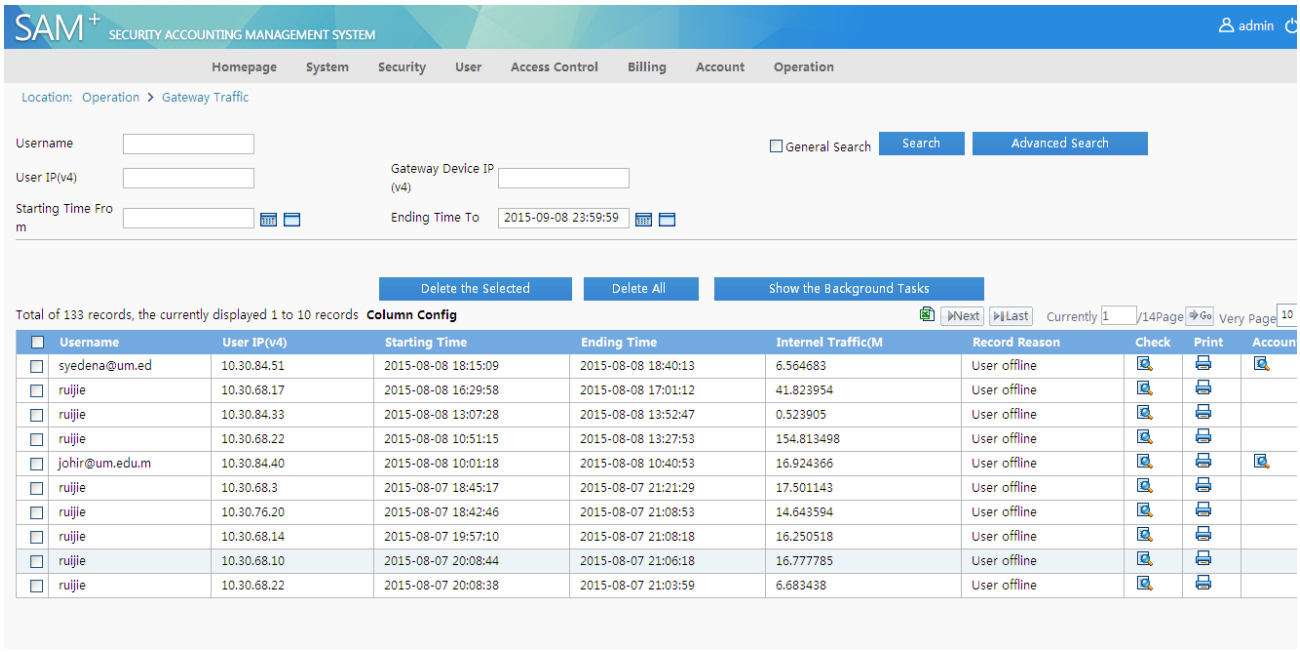
In the Internet access details, if a record is about the wireless access mode, the user IP address may not be displayed and the possible causes are as follows:

The wireless client of a user uses a static IP address (that is, the IP address is not automatically obtained through DHCP).

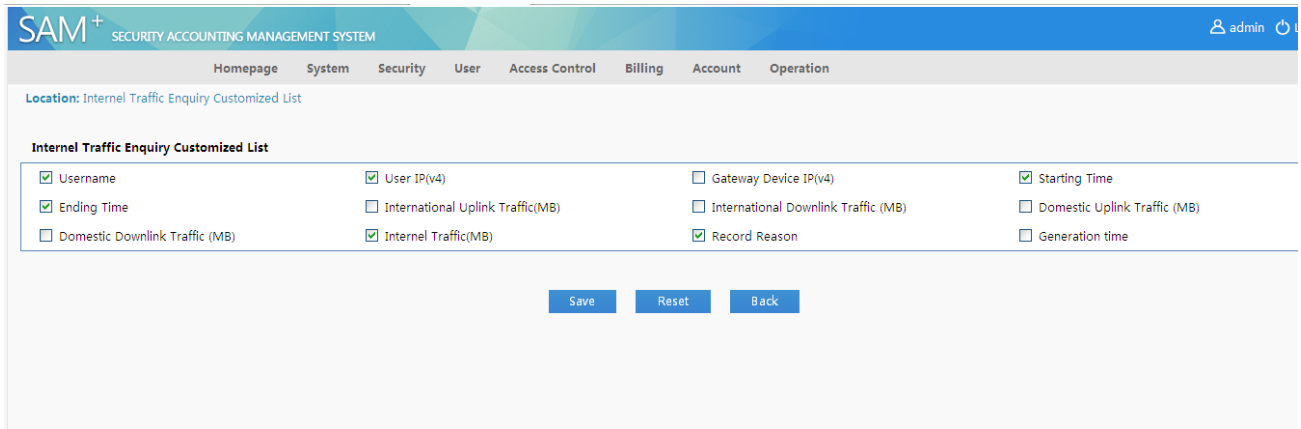
The record is a roaming record.

Gateway Traffic

In addition to Internet access details, relevant gateway traffic information is generated if the NTD gateway traffic is used after a user goes offline. See the following figure.

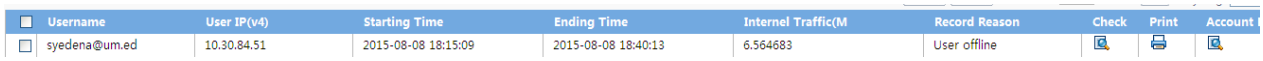


Gateway traffic information includes the username, user IP(v4) address, start time, end time, total gateway traffic, and reason record. You can click **Internal Traffic Enquiry Customized List** to customize items to be displayed in the gateway traffic information list, as shown in the following figure.

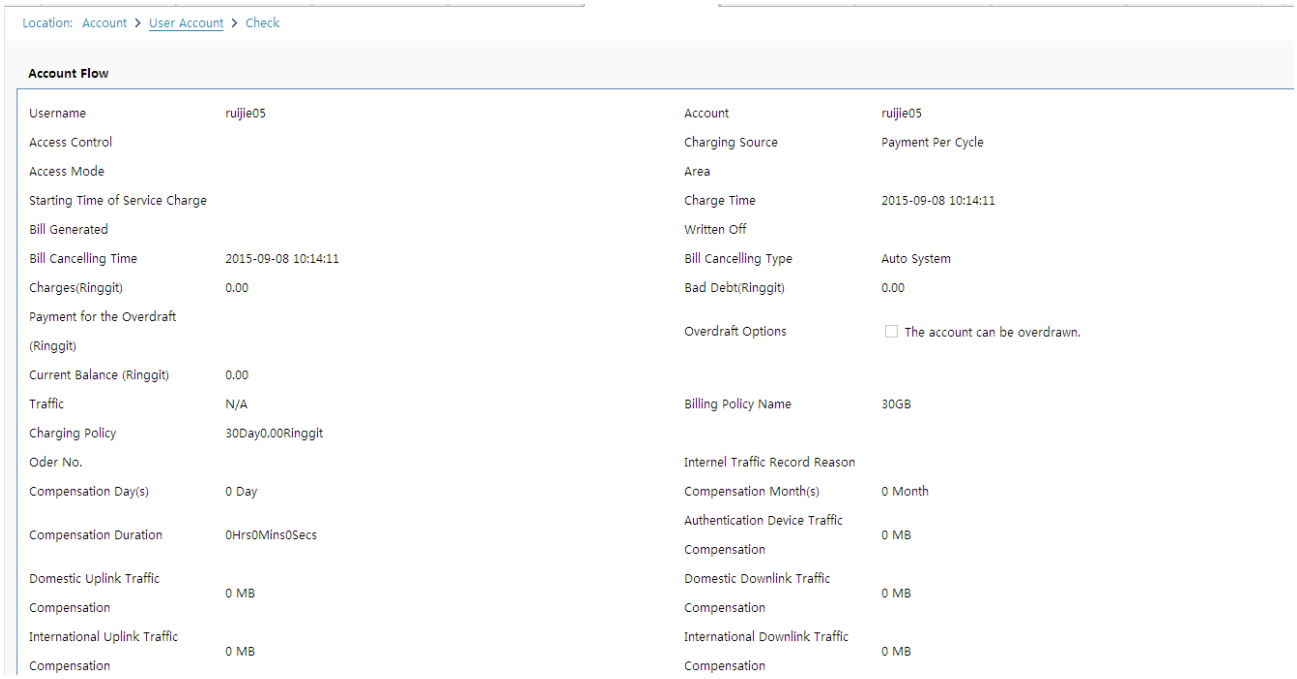


Gateway traffic information also covers the international uplink traffic, international downlink traffic, domestic uplink traffic, domestic downlink traffic. Customize items to be displayed in the gateway traffic information list according to actual conditions.

When billing is conducted on one gateway record, one link is provided in the **Account Flow** column at the end of a record for you to view associated account flow information. The following figure shows the link in the **Account Flow** column of the last record in the list in the preceding figure.



Click the link in the **Account Flow** column. The account flow view page is displayed, as shown in the following figure.

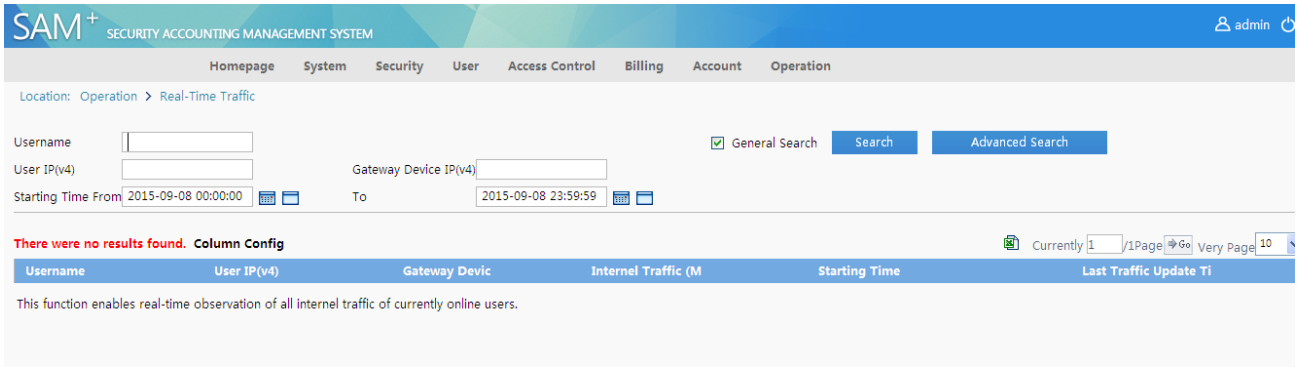


On this page, various types of traffic involved during the Internet access of a user are listed after the total gateway traffic. "N/A" is displayed behind other traffic information, indicating that no fees are incurred for the traffic.

From the angle of management application, when a user using the NTD gateway traffic goes offline, if you need to purely know the consumption of various types of traffic, you can use the gateway traffic query function. If you need to know the fees arising from the previous Internet access, you can use the account flow query function.

Real-Time Traffic

The function of querying real-time traffic of a gateway needs to be used in combination with the RG-NTD or RG-ACE so that it is meaningful in the gateway traffic billing scheme.



Pay attention to the following points when using the function of querying real-time traffic of a gateway:

The real-time performance of the gateway traffic information depends on the frequency of sending traffic information by the RG-NTD or RG-ACE. If the frequency of the RG-NTD or RG-ACE to send traffic information is slow, the real-time performance is poor. The frequency cannot be set to a very high value. Otherwise, the performance of the RG-SAM+ server and resource consumption of other functions may be affected. For specific configuration, see the RG-NTD or RG-ACE relevant document description.

The display of traffic information does not mean that billing is conducted on the traffic because billing is conducted only when a user goes offline normally in the gateway traffic billing scheme. If a user does not go offline, billing is not actually conducted. Therefore, traffic information here is a real-time view tool in the gateway traffic billing scheme and cannot be used as a billing basis.

System Maintenance

After the RG-SAM+ system is put into formal operation, administrators need to monitor and maintain the operation condition of the RG-SAM+ system, periodically conduct log clearing and maintenance on the database of the RG-SAM+ system, and restrict illegitimate users on the network in real time and stop them from accessing the Internet. Network administrators also need to handle network faults in a timely manner that may arise. For these, the RG-SAM+ system provides some monitoring and maintenance tools, including the blacklist, log, online repair reporting, online repair reporting FAQ management, and database maintenance.

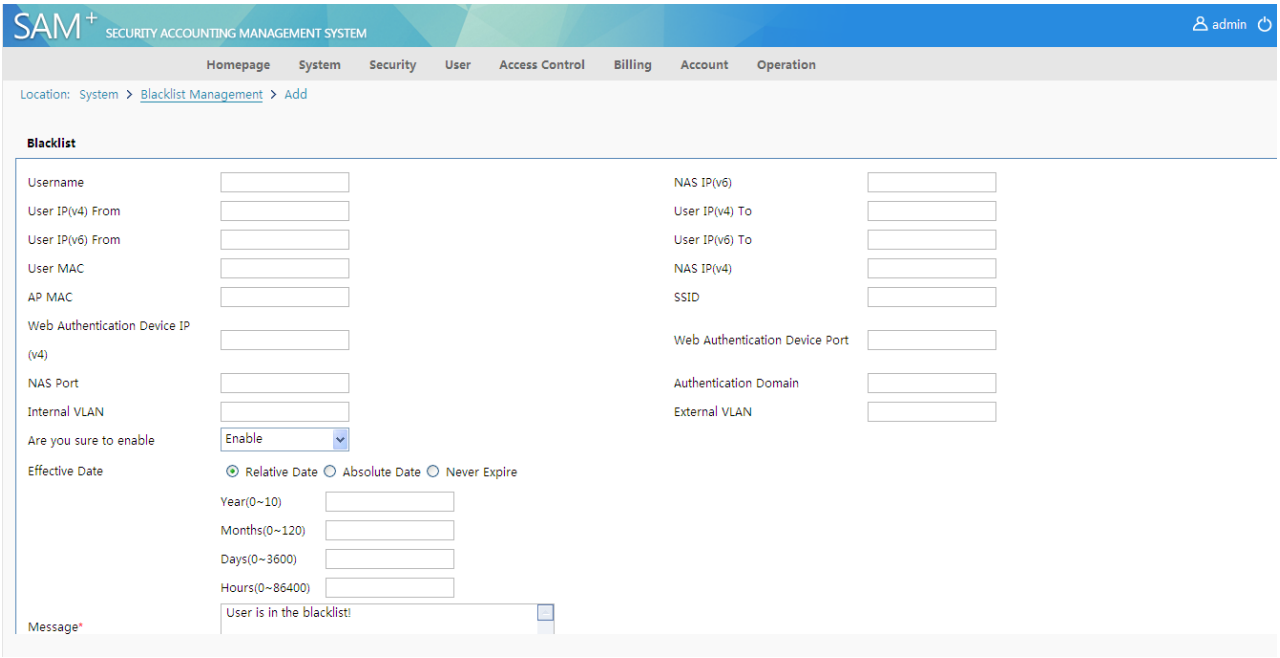
Blacklist

The blacklist function is applicable to online users rather than administrators who logs in to the system in Web mode or self-service users. The blacklist has the following functions in terms of applications:

Special network elements such as special IP address segment or special MAC addresses can be blacklisted before the RG-SAM+ system is put into operation. In this way, this information will not be used falsely or used by online users, thereby preventing unexpected impact.

For malicious attack behaviors, the usernames, IP addresses, or MAC addresses of these attack sources can be blacklisted as a means of punishment. Note that this function can be used together with the function of forcing users offline, that is, you can blacklist a user and then force the user offline.

The following figure shows the elements that can be added to the blacklist.



The differences between enable/disable and effective are as follows:

If the blacklist function is disabled, it does not mean the function is effective or ineffective. In general, it can be understood that no blacklist is set if the blacklist function is disabled.

If the blacklist function is enabled, whether the blacklist plays its role depends on whether it expires. If the blacklist function does not expire, it is effective. If the blacklist function expires, it is ineffective.

You can set whether to enable/disable the blacklist function when adding an item to the blacklist, or enable/disable an item or a blacklisted item after adding. Whether the blacklist function expires is automatically judged by the RG-SAM+ system. After the validity period expires, the blacklist function automatically becomes ineffective. If you need to make the blacklist function play its role, change the effective date of the blacklist.

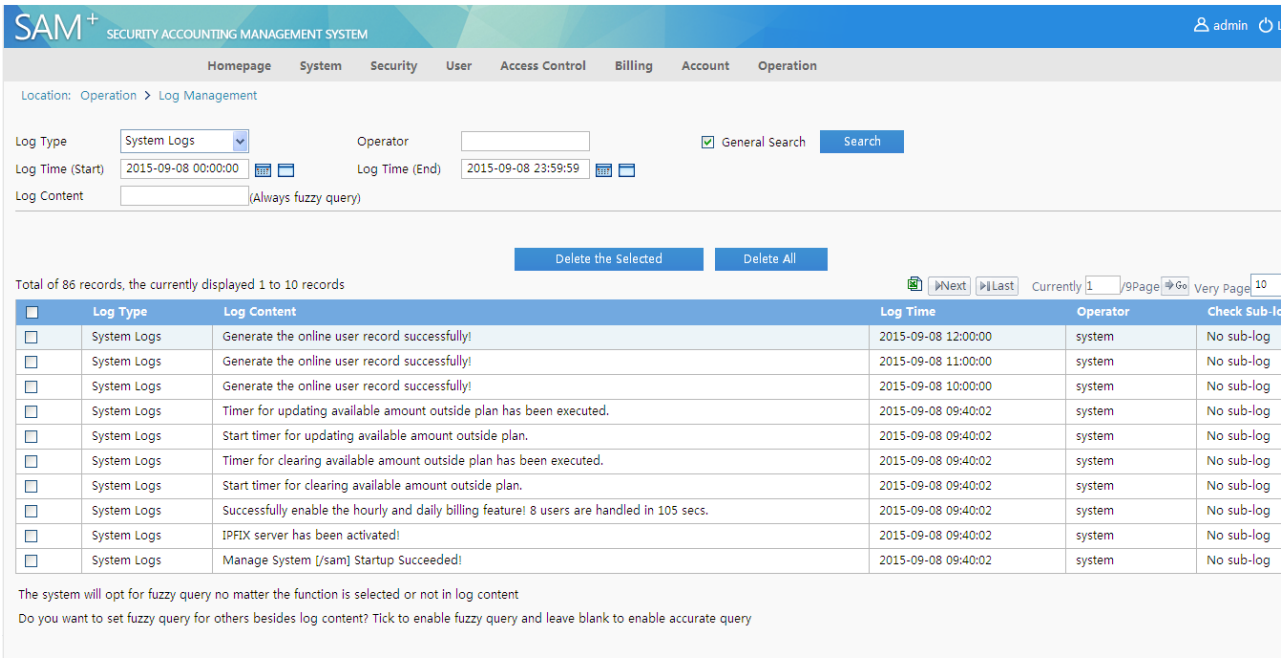
Log

The RG-SAM+ system provides detailed and abundant logs so that administrators can understand the operating condition of the system, network authentication condition, usage condition of the self-service system, as well as management condition of the management system from the logs. Logs of the RG-SAM+ system are classified into five types:

- System logs
- Authentication logs
- Administrator logs
- Self-service operation logs
- Operation & maintenance (O&M) logs
- Third-party development interface logs

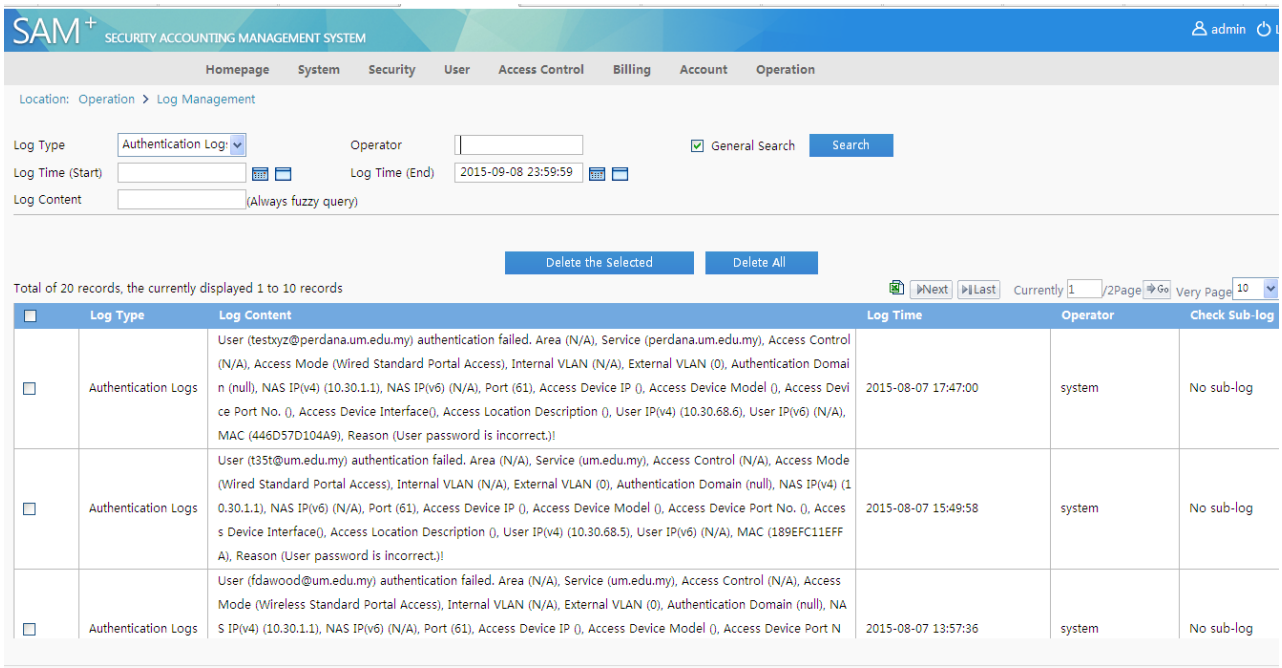
System Logs

System logs are operating records of the RG-SAM+ system, which cover the system startup, shutdown, periodical operations performed during system operating such as daily accounts, periodical generation of bills, and system-level function operations. System exceptions are also reflected in the system logs. The following figure shows typical system logs.



Authentication Logs

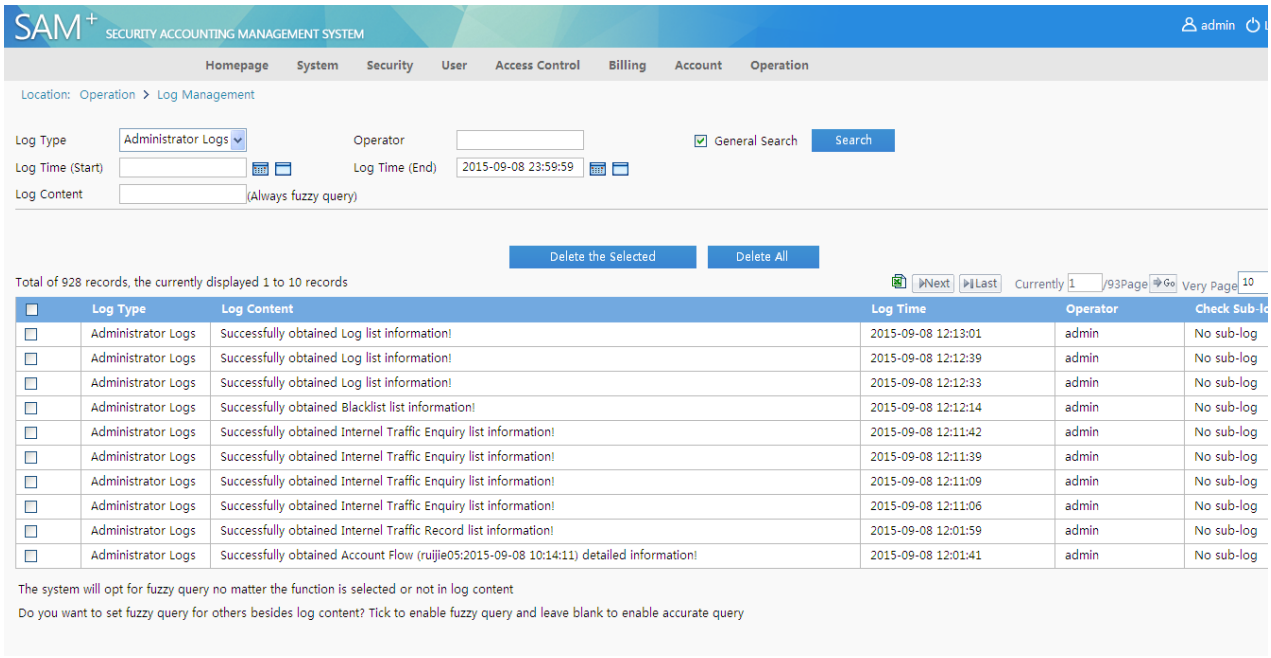
Authentication logs are records about authentication failures of users who attempt to access the Internet. In consideration of performance impact and actual applications, the RG-SAM+ system does not record users who pass the authentication successfully in authentication logs, because such users can be queried in online user records and Internet access details. Authentication logs record the username of a user who fail to pass authentication, user IP address, MAC address, NAS address, port ID, Internet access time, and cause of authentication failure, which is the most important. The following figure shows the typical authentication logs.



The preceding figure shows that the authentication failure is caused by the IP address binding error of the user. After querying the user information, it is found that the bound IP address of the user is 192.168.0.2, but the actual IP address of the user is 192.168.1.2, and the authentication fails because the IP address binding is enabled for the required service.

Administrator Logs

Administrator logs are records about management operations of administrators, including the basic adding, deleting, modifying, and query. Advanced function operations are also logged. For operations such as the deletion of account flows, logs and sub-logs are recorded in administrator logs for counterfoils, to prevent false deletion. The following figure shows typical administrator logs.

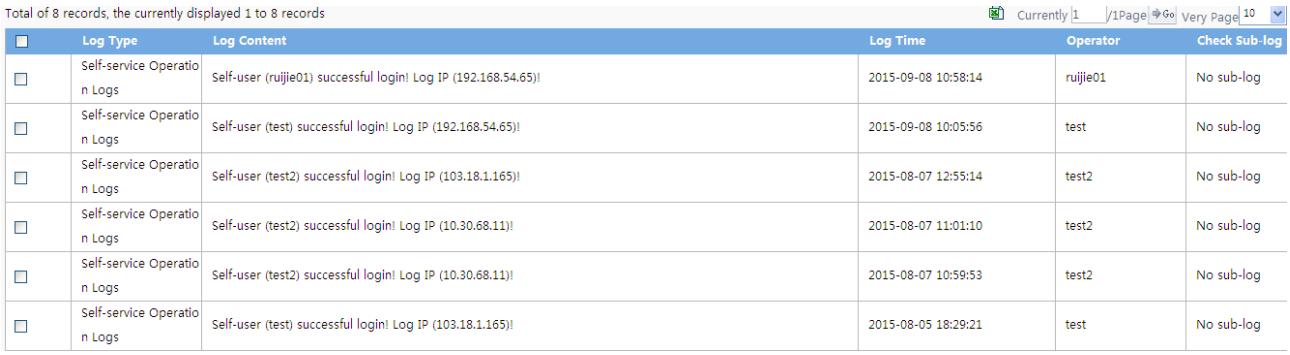


The preceding figure shows all the operations performed by administrator **admin** and a sub-log is recorded for the operation of deleting an account flow. Click the sub-log. A page similar to the following is displayed.

The sub-log clearly records specific information about the deleted account flow.

Self-Service Operation Logs

Self-service operation logs record operations performed on the self-service system by users who log in to the self-service system anonymously or with real names. In comparison with other logs, self-service operation logs record the IP addresses of users who log in to the self-service system anonymously because of openness of the self-service system. The following figure shows typical self-service operation logs.



User IP addresses for login, login time, and operations are recorded in detail regardless of whether users log in to the self-service system anonymously or with real names, which provides a good reference for network administrators to understand the usage condition of the self-service system.

O&M Logs

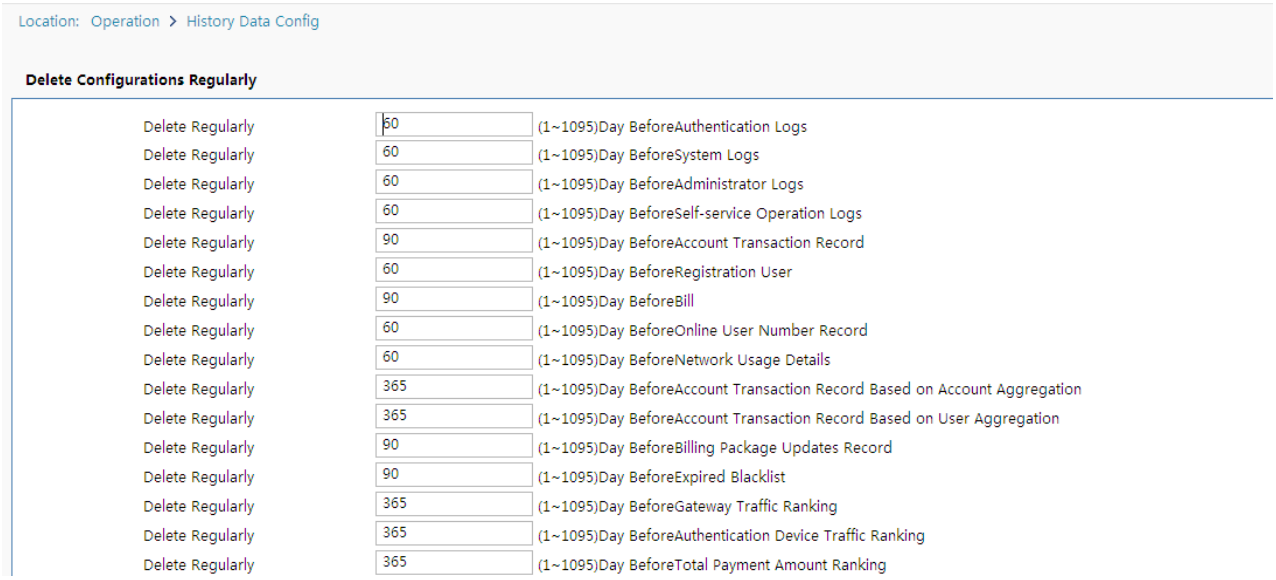
O&M logs are generated during automatic maintenance of the system. All normal maintenance information and exceptions identified during maintenance are recorded in O&M logs.

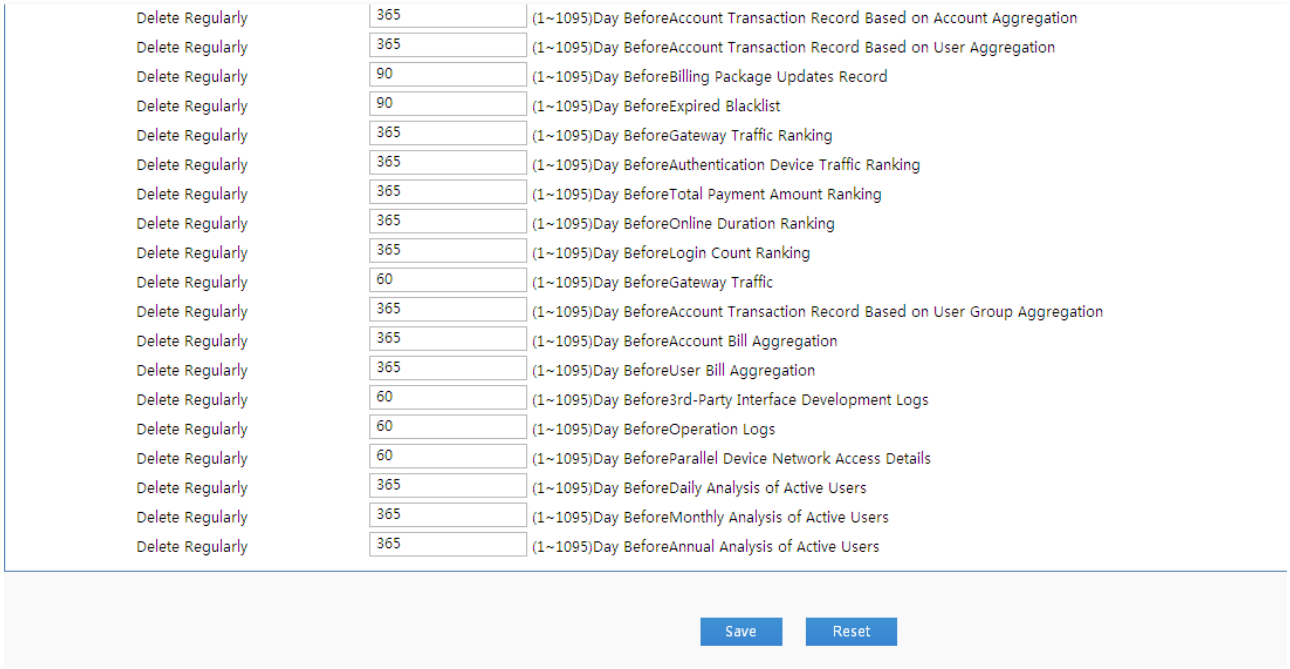
Third-Party Development Interface Logs

Third-party development interface logs record operations performed by a third party on the RG-SAM+ system.

Automatic Deletion of History Data

Some system data may become useless with the elapse of time. You can set the storage duration of such data on the automatic maintenance configuration page. The system automatically deletes data beyond the storage duration to free up storage resources and prevent system performance deterioration caused by more and more redundant data in the database.



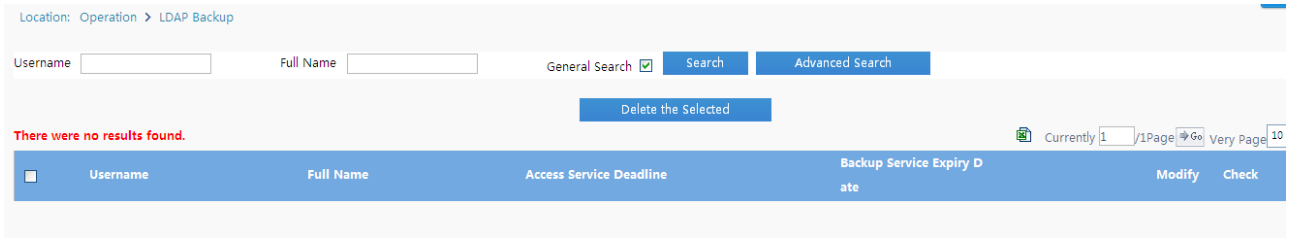


Fee-relevant information such as the account flow is involved in accounts and the deletion of such information is disabled by default.

LDAP Backup

If you configure the LDAP billing mode in "LDAP Configuration" and enable the LDAP user backup, the RG-SAM+ system writes the user information from the LDAP server into the database during user authentication so that users can still pass authentication and access the Internet even if the LDAP server is unavailable.

The LDAP backup information management function implements the management of user information backed up from the LDAP server.



Operation Report

Choose **Operation**>**Operation Report** from the main menu.

System operation reports are used to check whether the system is in the normal operation state currently.

Each time the system completes automatic maintenance, the system displays the result in the system operation report.

If a hidden risk is identified in the system, you can view the details. If an administrator considers that it is not a risk, the administrator can manually clear the hidden risk.

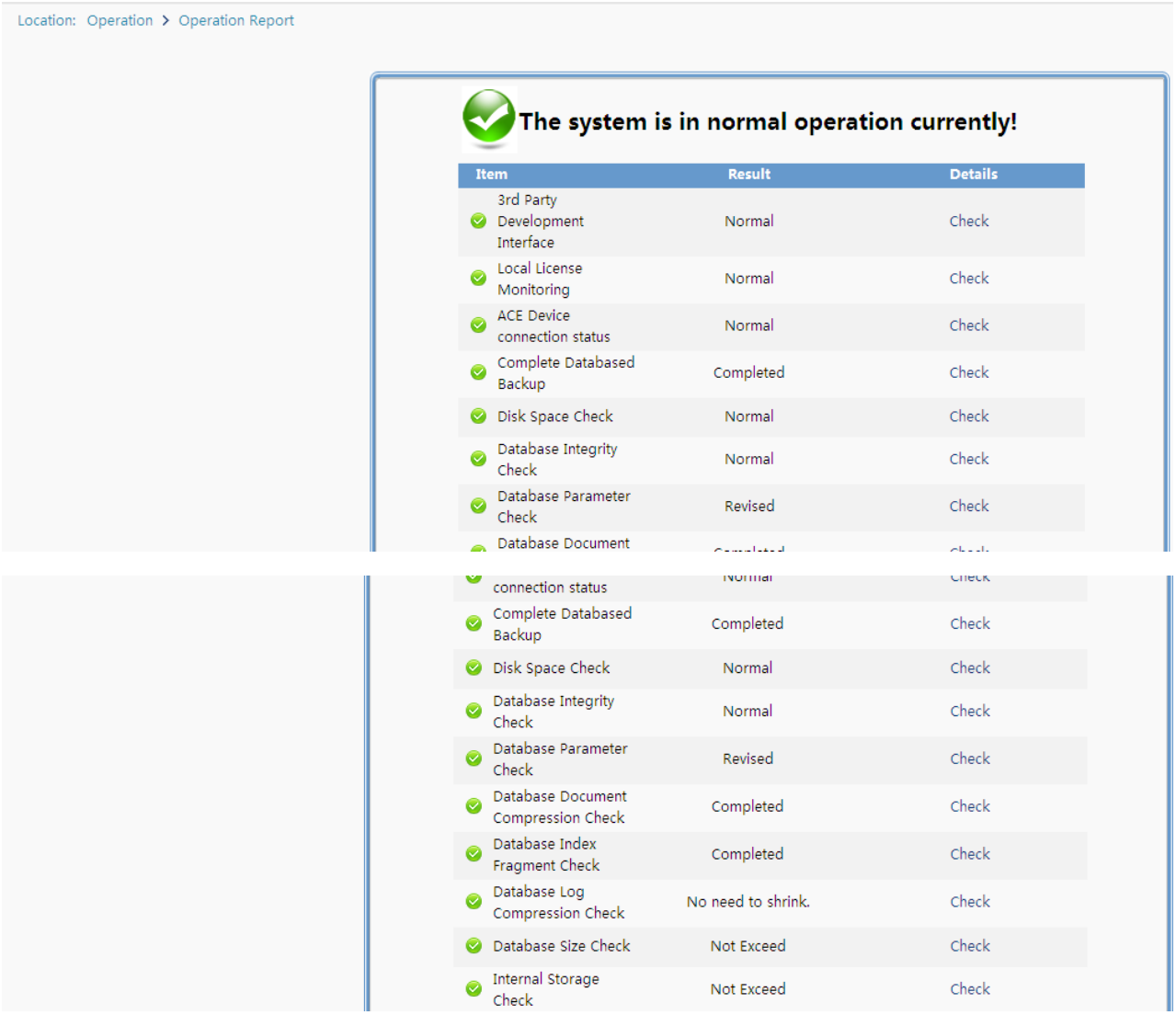
Manual clearing of alarms:

If the result of an automatic system maintenance item is **Alert** in the system operation report, a **Clear** button is displayed behind the details button. After you click the **Clear** button, the status of the maintenance item is changed to **Normal** and no hidden risk prompt is displayed on the home page and system report.

Automatic clearing of alarms:

If this item is normal during automatic system detection next time, the alarm is automatically cleared and the status is changed to normal. No hidden risk prompt is displayed on the home page and system report.

The following figure shows the system operation report page.



For details, see the *RG-SAM+ System Maintenance and Security Instructions.doc*.

System Maintenance

Administrators can set whether to enable the automatic system maintenance function.

Administrators can manually back up the database in system maintenance regardless of whether the automatic system maintenance function is enabled.

Administrators can set the backup policy after enabling automatic system maintenance. There are four backup policy schemes: complete backup, complete backup + transaction log backup, complete backup + remote backup, complete backup + transaction log backup + remote backup.

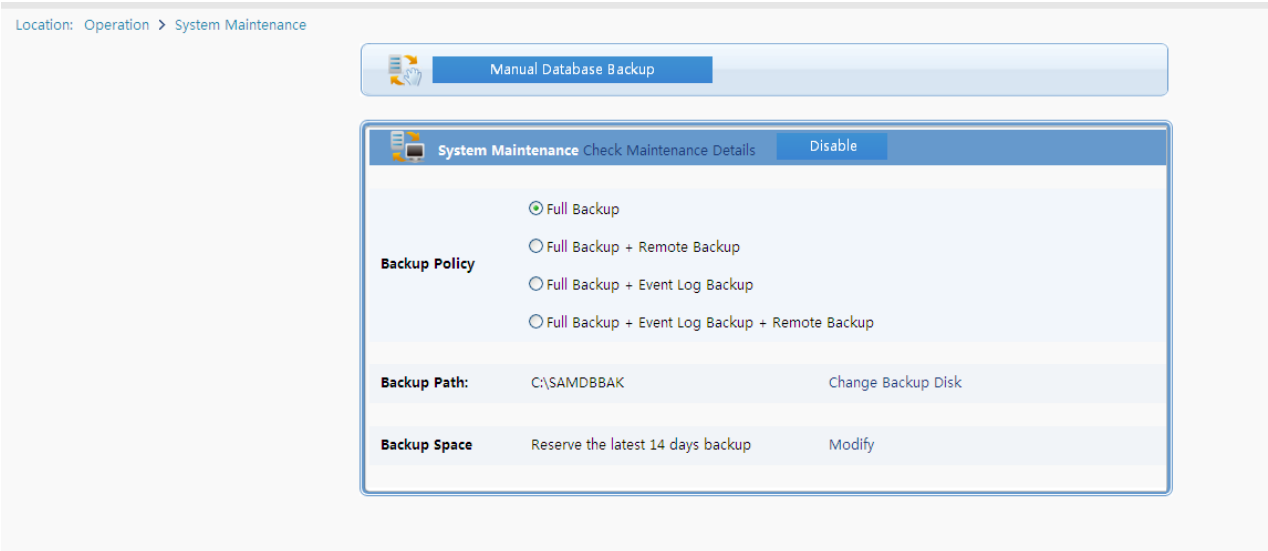
Administrators can change the backup disk. The backup disk is set during installation and can be changed here.

Administrators can change the backup space management policy. There are three backup space management schemes: retaining backup in recent *N* (3-60) days; retaining the backup as much as possible based on the space of the backup disk; not making new backup when the disk space is insufficient (it is estimated that the available disk space is sufficient for backing up files of one day).

Administrators can change the interval (*M* minutes, with the value ranging from 5-60 minutes) of backing up transaction logs and modify parameters relevant to remote backup (FTP).

For details, see the *RG-SAM+ System Maintenance and Security Instructions.doc*.

The following figure shows the system maintenance page.



Account Processing

Account Overview

When using the RG-SAM+ system to provide the operation services, you need to frequently understand the system operation condition, for example, the system revenue, expenditure, user payment, Internet access consumption, function consumption, and operation conditions of different services, you may need to collect statistics on operational data and make statements at the end of a month or year. Therefore, account management is very important. The account management of the RG-SAM+ system provides a simple, convenient, and pragmatic management mode for you. The following describes how to use account management of the RG-SAM+ system to help you manage the accounts of the system operation service.

Several Account Concepts

Account flow

Period-based fee deduction, duration-based fee deduction, and traffic-based fee deduction arising from Internet access, and fee deduction caused by functions used by users (such as account payment, transfer, and refund) (in other words, operations relevant to the account amount of users) need to be recorded. The time, amount, traffic, and other information of each fee deduction are recorded in account flows.

Bill

A bill is a consolidation of various account flows of a user or an account, that is, the consolidation of the revenue, expenditure, Internet access duration, Internet access traffic, account balance, and to-be-deducted amount of a user or an account within a period of time.

Arrearage bill

An arrearage bill is a bill that is not in the written-off state when beyond the writing-off expiration time.

Account consolidation

Account consolidation is the process of consolidating a range of various types of account flows into one or more bills according to certain statistics rules.

Non-written-off state

When the balance of an account is insufficient to pay the fee incurred by the Internet access or function operation, the generated account flow is in the non-written-off state. When one account flow is in the non-written-off state, the bill generated due to account consolidation is also in the non-written-off state.

Written-off state

When the balance of an account is sufficient to pay the fee incurred by the Internet access or function operation, the generated account flow is in the written-off state. After all account flows are in the written-off state, the bill generated due to account consolidation is in the written-off state.

Writing off

Writing off is a process of changing a bill or account flow that is in the non-written-off state to the writing-off state by means of payment, transfer, or recharging.

Bad debt

When an arrearage bill is not paid within a very long period of time, the RG-SAM+ system needs to make bad debt processing for this arrearage bill. The bills and account flows after bad debt processing are marked as "written-off state" and the writing-off type is defined as "bad debt".

Account registration

Account registration is to register the amount paid from a third-party system (such as user card agent or recharge card agent) to the RG-SAM+ system or from the RG-SAM+ system to a third-party system in the RG-SAM+ system. One account flow is generated each time account registration occurs. The writing-off type of the account flow is "*XX* account registration receipt" or "*XX* account registration payment". The account flow is in the written-off state and the bill generated due to account consolidation is also in the written-off state.

Account Status Change

If the account balance is insufficient to pay the fee during the generation of an account flow, the account flow is in the non-written-off state.

If the account balance is sufficient to pay the fee during the generation of an account flow, the account flow is in the written-off state.

When multiple account flows are consolidated into a bill, the bill is in the non-written-off state if one account flow is in the non-written-off state.

When money is added to an account by means of payment, recharging, or transfer, the account flows and bills that are in the non-written-off state are written off first.

The condition of writing-off of an account flow is as follows: When the balance of an account is not smaller than 0 after money adding and the account is in the normal state, the account flows that are in the non-written-off state are written off, the status of account flows are updated to written-off, and the writing-off type (such as payment or transfer) is recorded.

The condition of writing-off of a bill is as follows: After money is added to an account, the writing-off state of a bill is updated to written-off and the writing-off type (payment and transfer) is recorded only when the account balance of account flows associated with a bill is not smaller than 0 and the account is in the normal state, that is, the account flows associated with the bill are all in the written-off state.

Note

Description of the writing-off type:

The writing-off types of account flows and bills include payment, transfer receipt, balance recharging, self-service balance recharging, self-service activation, bad debt, and system automation. When an account flow generated about the system itself is set to the written-off state by the system unconditionally, the writing-off type of the recorded account flow is system automation. For example, when payment is performed on an account, account flows and bills associated with the account that are not in the written-off state are written off and a payment account flow is generated, which is in the written-off state, and the writing-off type is recorded as system automation.

Changes in the account consolidation status of account flows reflect the conversion relationship between account consolidation states of account flows. There are three account consolidation states:

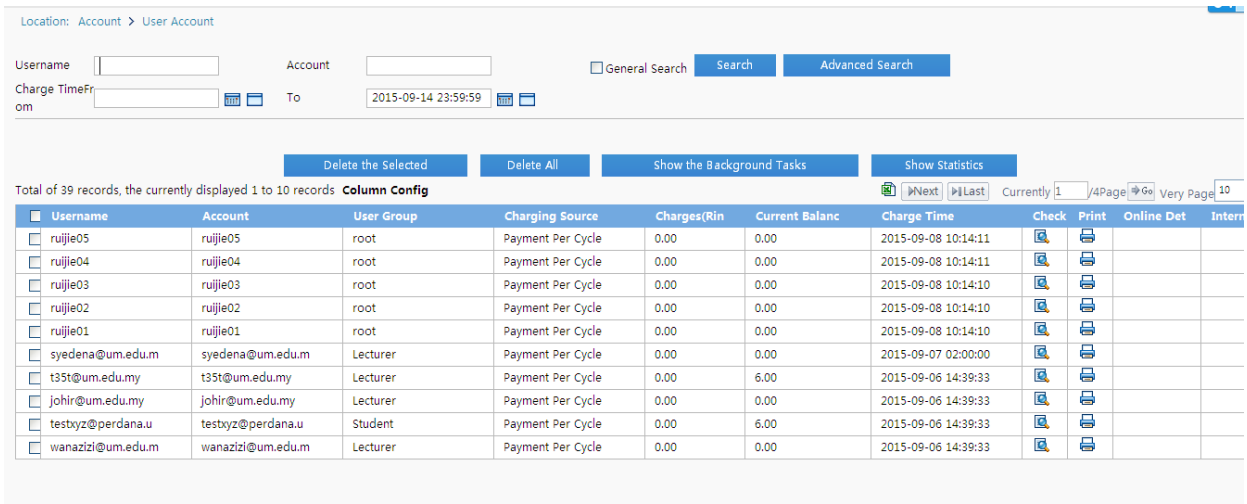
Manual account consolidation (account flows are selected manually, account consolidation options are set manually, and bills are consolidated manually)

Monthly automatic account consolidation (account consolidation options are set at a time, and the system automatically conducts account consolidation every month, without manual intervention)

After an account associated with a user is changed, if the account is in arrears and there are outstanding non-written-off account flows, the account flows of the account still exist. The outstanding account flows can be cleared by means of payment or bad debt processing.

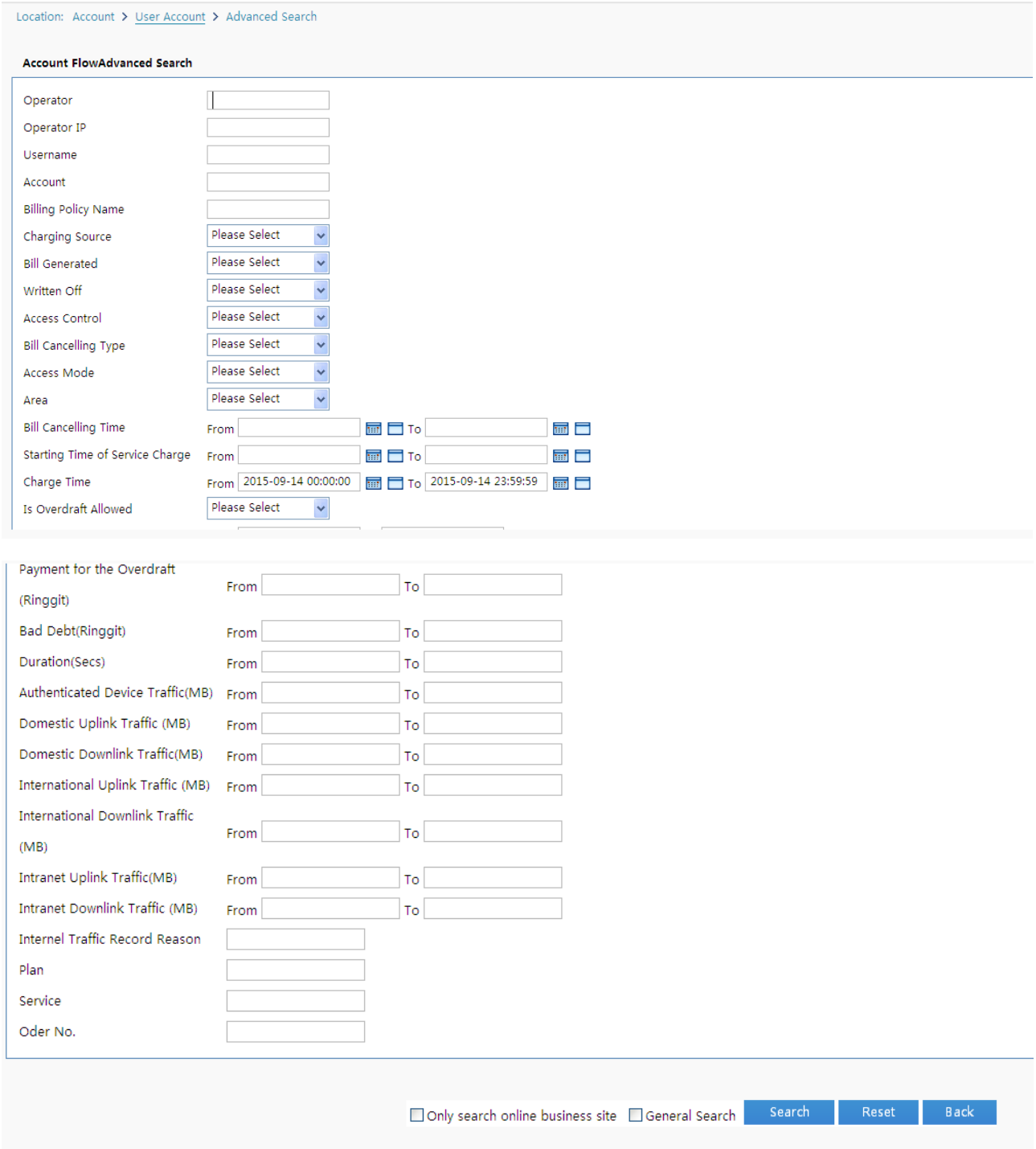
Account Flow

The account flow management provides the functions of querying, deleting, and printing various types of account flows. Choose **Account**>**User Account** from the main menu. On the account flow list page, you can specify combined search conditions and perform relevant operations, as shown in the following figure.



Account Flow List Page

On this page, you can set simple search combinations using the account name, username, and generation time (exact search and fuzzy search are supported), delete account flows that are searched out, view statistics, and view and print each record. Statistics display system payments and receipts in records that are searched out by billing source (this function is also available at the self-service client) so that you clearly understand the account conditions of the system.



Account Flow Advanced Search Page

Note

Billing source description

A billing source refers that how an account flow is generated. It includes duration-based fee deduction, port traffic-based fee deduction, fee deduction based on total gateway traffic, fee deduction based on domestic uplink traffic, fee deduction based on domestic downlink traffic, fee deduction based on international uplink traffic, fee deduction based on international downlink traffic, period-based fee deduction, account activation fee, payment, to-be-deducted amount prepayment, refund, transfer receipt, transfer payment, balance recharging, to-be-deducted amount recharging, self-service balance recharging, self-service to-be-deducted recharging, manual account registration receipt, manual account registration payment, recharging card account registration receipt, recharging card account registration payment, self-service activation, to-be-deducted amount appropriation, and preference.

Description of segment account flows

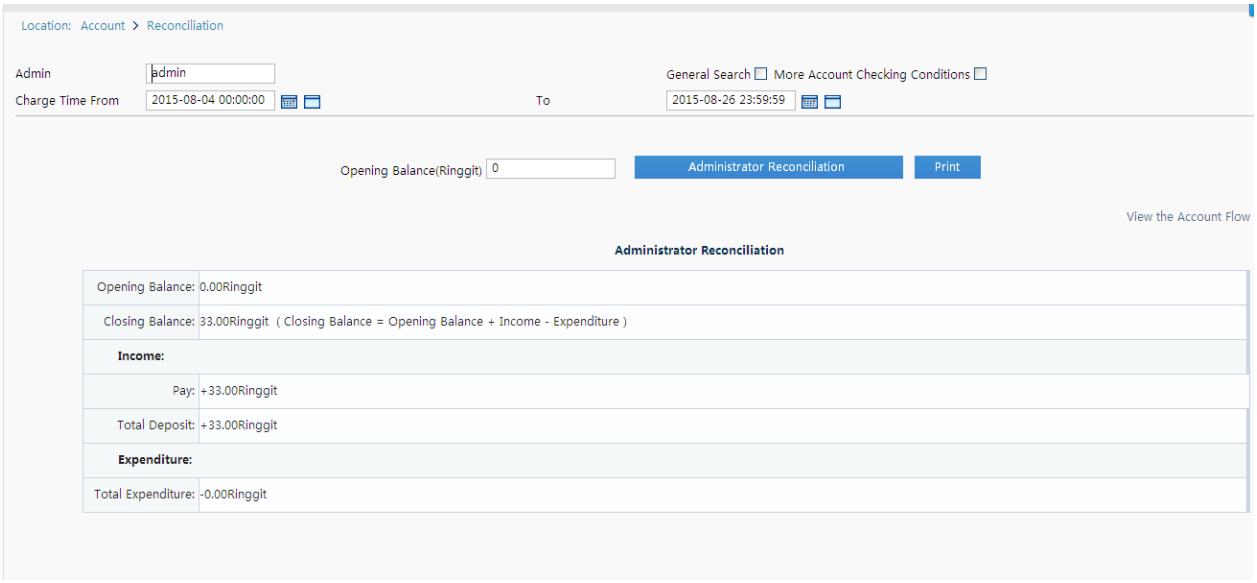
Segment traffic billing rule: When an Internet access operation traverses multiple segments, multiple account flows will be generated. For example:

The segment billing rule is that the charge is 1 Ringgit/1 Gbit/s when the traffic is within 1-2 Gbit/s, and 0.5 Ringgit/1 Gbit/s when the traffic is within 2-3 Gbit/s. 2.5 Gbit/s traffic is consumed in this Internet access operation.

Two account flows will be generated, one for 2 Gbit/s traffic and the other for 0.5 Gbit/s traffic.

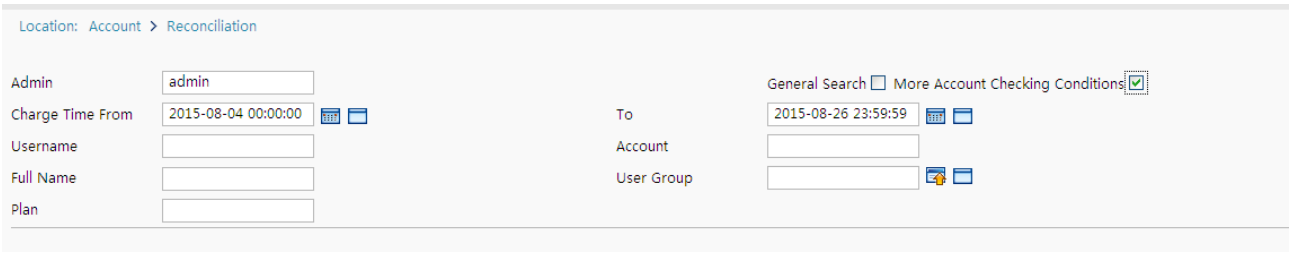
Administrator Reconciliation

The administrator reconciliation provides the reconciliation and printing functions for administrators to check the cashiering services. The following figure shows the administration reconciliation page.

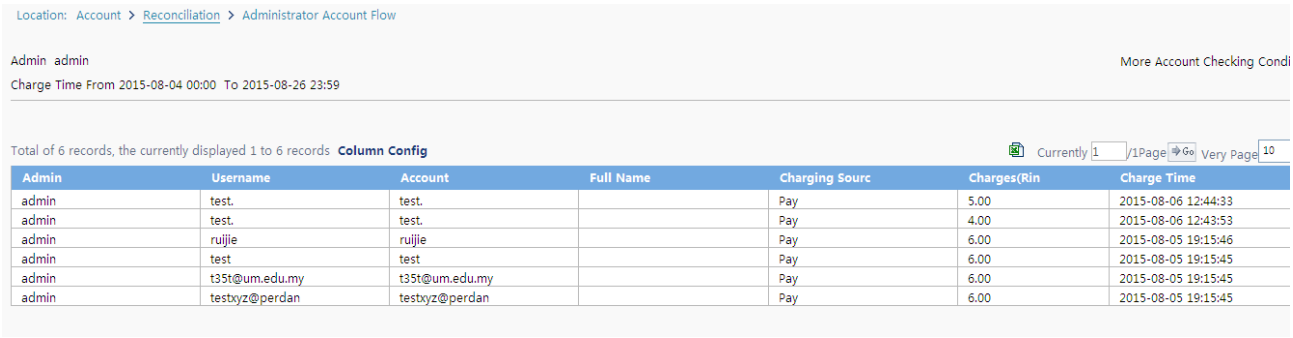


The preceding figure shows that administration reconciliation can be used to check the account amount handled by an administrator within a period of time, with the payment and receipt details in a list. You can also specify a time range to collect statistics on account payment and receipt details of the entire system within the time range.

You can also specify more reconciliation search conditions to make specific statistics.



Click the link of viewing account flows to view detailed account flows.



Visualized O&M

Star Map

The RG-SAM+ system enables start map to vividly display online users in an image. You can locate users by using the name, IP address, or MAC address on this map. This map also displays some O&M notifications, which can be viewed by administrators. The following figure shows the star map.

Chapter 7 Self-Service Portal

The RG-SAM+ system allows users to query business details and plan information in the Campus Self-Service Portal.

Chapter 8 FAQs

1. **The option of MX series switches does not exist in Device Type. How can the RG-SAM+ system support authentication of MX series switches?**

Set the Device Type to Wireless Switch for MX series switches and the Model to Other Model.

2. **How to know the RG-SAM+ version?**

Click **About** in the upper right corner on the page of the system. Then, the version information of the RG-SAM+ system is displayed.

3. **How to do if the entire content cannot be printed on one page?**

On the page to be printed, choose **File**>**Page Setup** from the main menu. On the **Page Setup** page, set **Left**, **Right**, **Top**, and **Bottom** to **0** in **Margins** area so that the scope for printing can be large, and click **OK** to save the page settings. Re-print the content to view whether the page content can be completely printed out.

If the printed content is still incomplete, the designed Web page may be very wide. In this case, access the **Page Setup** page again, and set **Orientation** to **Landscape**. If the printed content is still incomplete, copy all content on the Web page to a WORD document and print the WORD document.

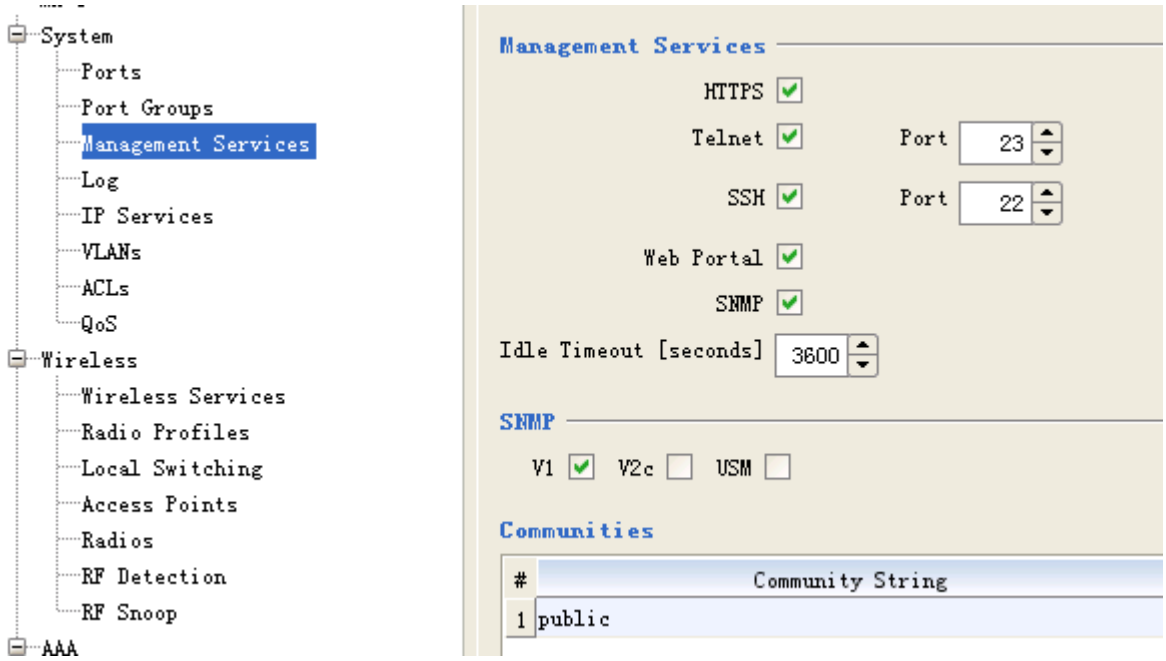
If images or background color on the Web page cannot be printed out, in the IE, choose **Tools**>**Internet Options** from the main menu. In the **Internet Options** dialog box, click the **Advanced** tab, select **Print Background Colors and Images**, and click **OK** to print out the images or background colors on the Web page.

In addition, if a Web page is composed of several frame pages, content in each frame page cannot be completely printed out if you choose **File**>**Print** from the main menu. In this case, you must print the content in each frame page to ensure that complete content is printed out. When printing a frame page, right-click the target frame page and choose **Print** from the shortcut menu. In the **Print** dialog box, select **Only print the selected frame** and click **Print**.

4. **For users who access the network through MX series wireless switches, when they do not go offline actively, online user records are deleted from the RG-SAM+ system 1-2 minutes later but the users are actually online?**

Verify that the community of the device added to the RG-SAM+ system is consistent with that of ringmaster.

Verify that the SNMP configuration on the ringmaster is correct. See the following figure.



5. For users authenticated through H3C switches, the NAS port ID is a very large integer.

The NAS port ID in the RADIUS packets from the H3C switch is a very large integer.

6. The Internet access details of users connected through H3C switches display offline causes that are difficult to understand, such as code9 and code8.

Offline causes are read from accounting packets of switches when users go offline. The conditions when the H3C switch upload code8 and code9 are not understood and such causes are displayed as their original information.