



**RG-SMP Professional\_2.63\_EN\_Build20151106**

**Operation Guide**

## Copyright statement

Ruijie Networks©2015

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

     ,  
     ,  
 , 锐捷® are registered trademarks of Ruijie Networks. Counterfeit is strictly prohibited.

## 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 will guide you through the operation of the system.

## Scope

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 Networks service portal: <http://case.ruijienetworks.com>

## Documentation Conventions

The symbols used in this document are described as below:



### Note

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

---



### Caution

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

---

## Product Overview

The RG-SMP (Security Management Platform) is an enterprise-class security management application that provides insight into and control of Ruijie security and network devices.

The RG-SMP offers comprehensive security management across a wide range of Ruijie security appliances, including Ruijie intelligent switches and Wireless solutions.

The RG-SMP is also compatible with other third-party networking devices with 802.1X protocol, enabling the AAA (authentication, authorization and accounting) network access control (NAC) policy according to user requirements.

The Ruijie RG-SMP allows users to manage office networks of all sizes for a broad spectrum of industries, with security compliance requirements of user identity, host health and security of network communication.

## Hardware Configuration

The RG-SMP system involves operation of the customers' business networks. Therefore, the hardware configuration of the servers installed with RG-SMP must meet the minimum requirements; otherwise, problems, such as slow authentication, high CPU usage, and slow access to the management page, will occur. It is advised to use the recommended configuration.

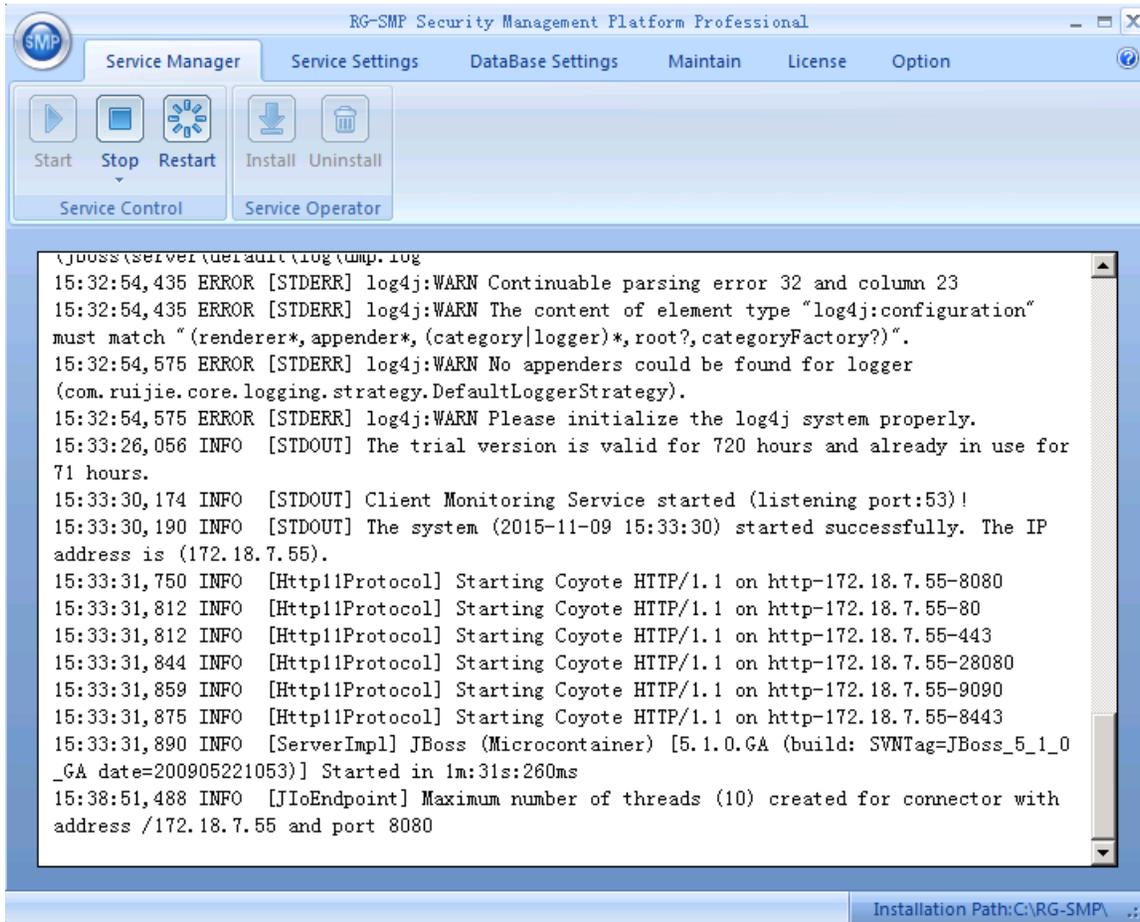
Item	Minimum Configuration	Recommended Configuration
Server	Dell PowerEdge R710 CPU: 2 x 4-core Intel Xeon E5606 2.13GHz RAM: 4 GB Disk: 130 MB IOPS, 100 GB space NIC: 3 x 1000 Mbps full-duplex NIC	Dell PowerEdge R710 CPU: 4 x 4-core Intel Xeon E5606 2.53GHz RAM: 16 GB Disk: 266 MB or above IOPS; 200 GB or above space (recommended: 500 GB) NIC: 3 x 1000 Mbps full-duplex NIC
HDD	The operating system (OS), SQL server, and RG-SMP system are installed in the same HDD with at least 100 GB space in total.	Disk C: It contains 80 GB or above space and is used to install the OS. Disk D: It contains 200 GB or above space and is used to install the RG-SMP system and the SQL server. Disk E: It contains 200 GB or above space and is used to back up the database files.
OS	The RG-SMP system can be installed in the following editions of Windows OS: Windows Server 2003 Standard Edition SP2 x86/x64 Windows Server 2003 Enterprise Edition SP2 x86/x64 Windows Server 2003 R2 Standard Edition SP2 x86/x64 Windows Server 2003 R2 Enterprise Edition SP2	Recommended: Windows Server 2003 Enterprise Edition SP2 x86/x64 Windows Server 2008 R2 Enterprise Edition SP1 x64

Item	Minimum Configuration	Recommended Configuration
	x86/x64 Windows Server 2008 Standard Edition SP2 x86/x64 Windows Server 2008 Enterprise Edition SP1 x86/x64 Windows Server 2008 R2 Enterprise Edition SP1 x64 Windows Server 2012 Standard Edition Windows Server 2012 Enterprise Edition	
Database	SQL Server 2005 Standard Edition SP2 x86/x64 SQL Server 2005 Enterprise Edition SP2 x86/x64 SQL Server 2008 Standard Edition SP1 x86/x64 SQL Server 2008 Enterprise Edition SP1 x86/x64 SQL Server 2008 R2 Enterprise Edition x64 SQL Server 2012 Standard Edition SP1 x86/x64 (Clustering is not supported at present.) SQL Server 2012 Enterprise Edition SP1 x86/x64 (Clustering is not supported at present.) SQL Server 2014 Standard Edition SP1 x86/x64 (Clustering is not supported at present.) SQL Server 2014 Enterprise Edition SP1 x86/x64 (Clustering is not supported at present.)	Recommended: SQL Server 2005 Enterprise Edition SP2 x86 SQL Server 2008 R2 Enterprise Edition SP1 x64

## Product Interfaces

### RG-SMP Service Manager

After RG-SMP is installed, install the RG-SMP services, and insert a dongle (or import a license file). After RG-SMP is successfully started, the following page is displayed:



## RG-SMP Management Platform

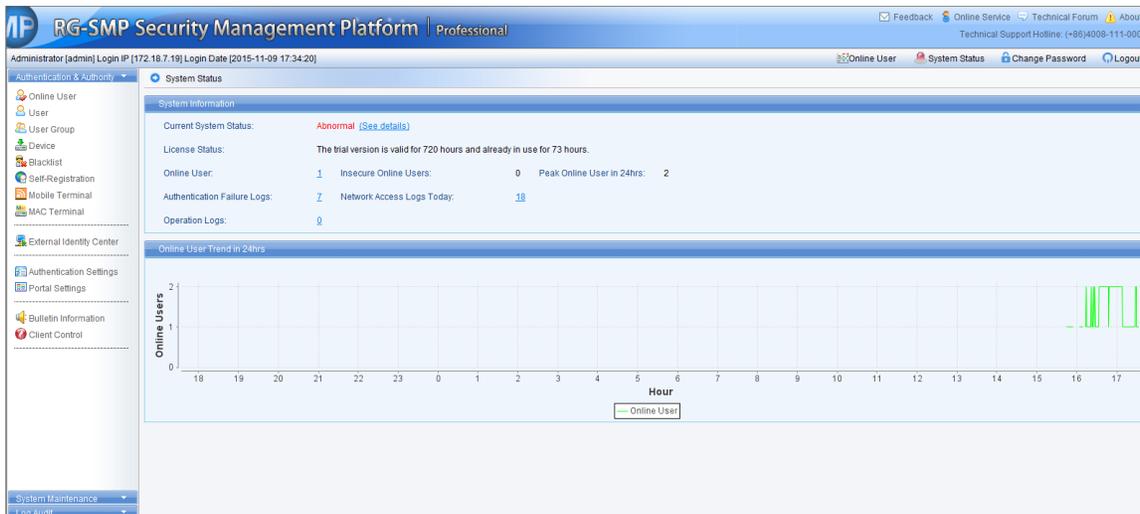
After RG-SMP is successfully started, you can log in to the RG-SMP management platform. In the browser, enter <http://smpip:8080/smp> (**smpip** is the IP address of the SQL server with RG-SMP installed, for example, <http://172.18.8.118:8080/smp>). If the **https** login mode is used, the login URL is <https://smpip:8443/smp>.

It is recommended to use the Internet Explorer 8.0 (or later versions) to log in to RG-SMP; and to enable the compatible mode of the explorer if existing.

The following figure shows the login page.



By default, the username is **admin**, and the password is **11111111**. The following figure shows the page after the login succeeds.



## Typical Scenarios

### User Access

#### Wired User Access

#### Function Description

N/A

#### Configuration Tips

- When adding a network access server (NAS), you must select the correct template in the **NAS Configuration Templates** option corresponding to the NAS type. Note that the SNMP community strings configured on the NAS and in the template must be the same; otherwise, the NAS information cannot be obtained.
- If the user already has a third-party ID, you can enable **Third Party Correlation Registration** on RG-SMP. Or, enable **SMS** or **Email** to verify authentication for RG-SMP local users.
- To enable 802.1X or Web authentication on the NAS, see its *Configuration Guide*.

#### Configuration Steps

### Adding a NAS

- 1) Choose **Authentication & Authority > Device** from the left menu.

The screenshot shows the 'Authentication & Authority > Device > Query' page in the RG-SMP Professional interface. The left sidebar has 'Device' highlighted. The main content area includes a search form with fields for 'NAS IP' and 'NAS Name', and a dropdown for 'NAS Configuration Templates' set to 'All'. Below the search form are buttons for 'Add', 'Delete', 'Search Device', 'Import Device', and 'Synchronize MAC'. A table displays one device record:

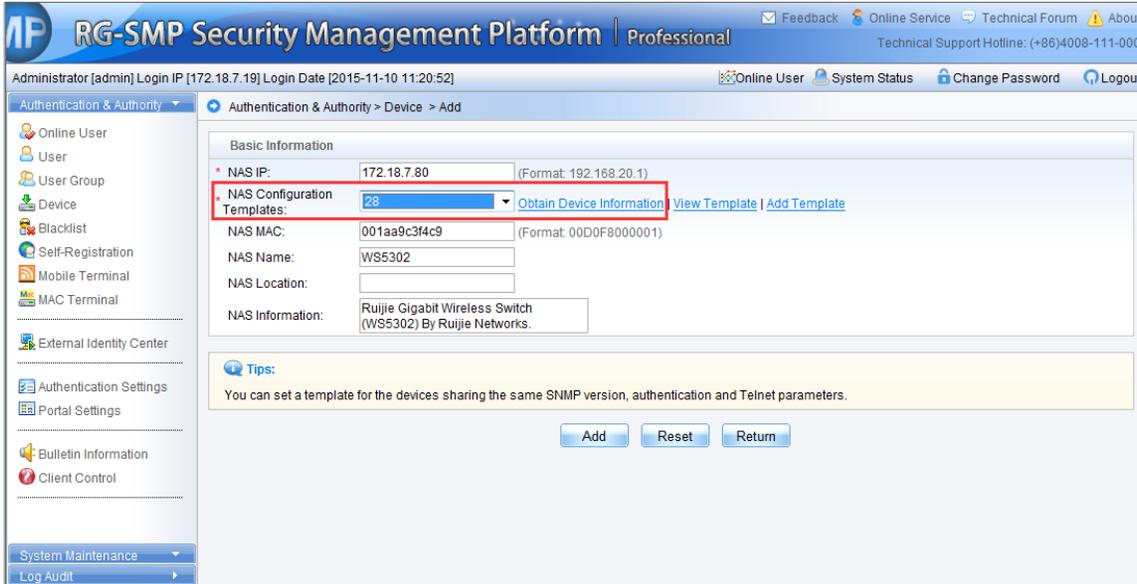
All None	NAS IP	NAS MAC	NAS Configuration Templates	Operation
<input type="checkbox"/>	10.1.1.28	00d0f82233bd	28	Telnet   View   Modify

Below the table, there are 'Tips' and a 'Warning' message:

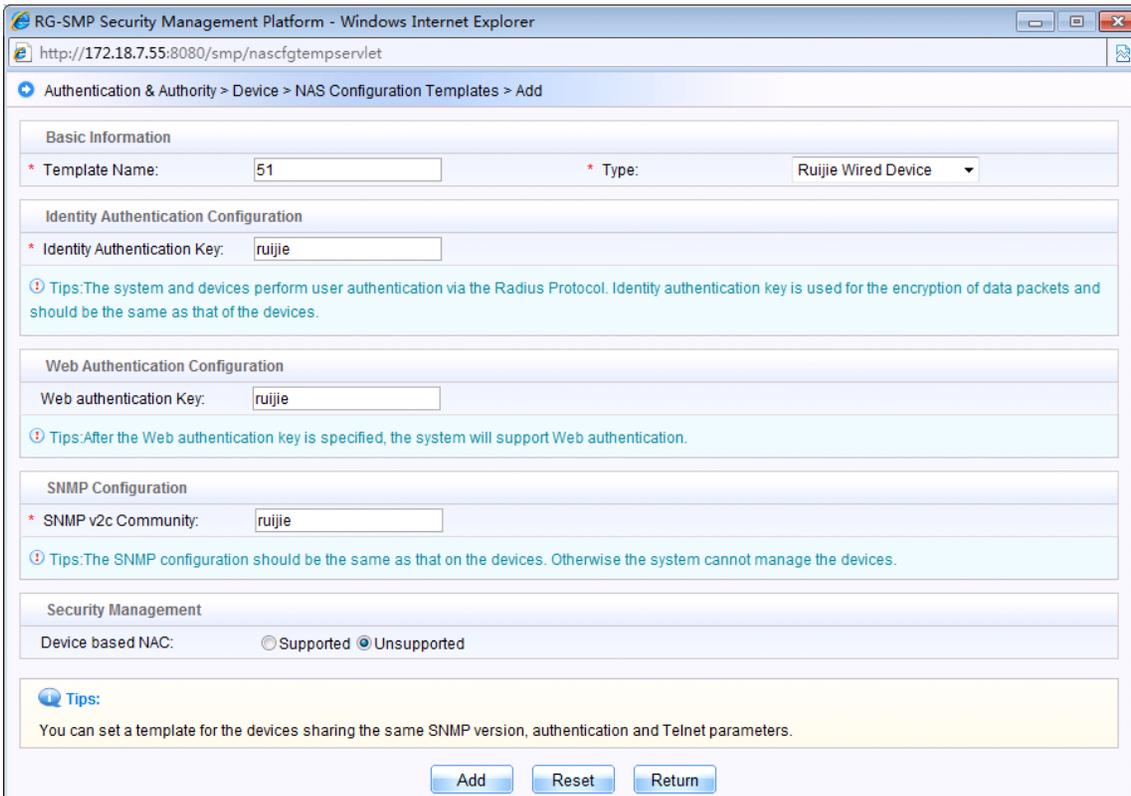
**Tips:**  
 1. You can set a template for the devices sharing the same SNMP version, authentication and Telnet parameters.  
 2. If you cannot telnet device, please click [here](#) to download the registry repair tool. Please restart your browser after repairing.

**Warning:**  
 If the device information is not registered in the system, the user authentication may fail.

2) Click **Add**. The **Add** window is displayed. Fill in the **NAS IP** and **NAS Configuration Templates** fields (you can select an existing NAS configuration template or add one). Click **Obtain Device Information**. RG-SMP will obtain device information automatically.



3) To add a NAS configuration template, click **Add Template**.



- 4) After device information is obtained successfully, click **Add**.



### Note

If device information fails to be obtained, check whether the device IP address and SNMPv2c Community are configured correctly. If yes, check whether the communication between RG-SMP and the device is normal. Some devices (for example, RG-ePortal) can be added even when their information cannot be obtained. If the NAS configuration template is inconsistent with the actual configuration of the device, choose **Authentication & Authority > Device** and click **NAS Configuration Templates** to add a NAS configuration template or modify the existing NAS configuration template.

## Adding a User Group

- 1) Choose **Authentication & Authority > User Group** from the left menu. Click **Add** or **Modify** to add or modify a user group in the corresponding configuration page.

Authentication & Authority > User Group > Query User Groups

User Group Name:

Totally 6 Records | Each Page 20 Records | Page 1 / totally 1 Pages |

AllNone	User Group Name	Operation
<input type="checkbox"/>	smpad.com/13btest	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	smpad.com/普通 用户 组	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	smpad.com/Users	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	ad	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Guest User Group	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Restore Default Settings</a>
<input type="checkbox"/>	Default User Group	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Restore Default Settings</a>

Totally 6 Records | Each Page 20 Records | Page 1 / totally 1 Pages |

2) Click **Add** or **Modify** to save the configuration.

Authentication & Authority > User Group > Add User Group

\* User Group Name:

Enable Wired Access

Network Information Verification  All

HD Serial Number Verification

IP Type Authentication:  Static  Dynamic

User IP Verification

User MAC Verification

User IMSI

NAS IP Verification

NAS Port Verification

Enable Wireless Access

Network Information Verification  All

HD Serial Number Verification

IP Type Authentication:  Static  Dynamic

User IP Verification

User MAC Verification

User IMSI

SSID Verification

**Tips:**

- Wireless SSID names are separated by commas (,), e.g., web-wired-SSID, web-wireless-SSID.
- The MAC address verification and the IMSI number/mobile phone number verification cannot be enabled at the same time.
- When the network information auto-learning and the network information verification are enabled, you can bind users to networks. Or the system will bind users to networks through network information auto-learning in the next authentication.



**Note** If a user of the added group is online, the modification will take effect in the next authentication.

## Adding or Importing a User

1) Choose **Authentication & Authority > User** to enter the user management page.

Authentication & Authority > User > Query Users

User Name:  Full Name:  User Group:  User Type: All User Status: All

Online or not: All In Blacklist or not: All  Accurate Search   [Advanced Search](#) [Query users offline for a long time](#)

[Import Users](#) [Import Network Binding Information](#) [Export All Results](#)

[Customize User Fields](#) [SIM Card Management](#) [Customize Query List](#) [User Information Self-Service Maintenance](#)

Totally 5 Records | Each Page 20 Records | Page 1 / totally 1 Pages | GO

All Name	User Name	Full Name	User Group	Type of Account	Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	Operation
<input type="checkbox"/>	1108	1108	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	1108@smpad.com	1108@smpad.com	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	smpad.com/1108	smpad.com/1108	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	smpad/1108	smpad/1108	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	test	111	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>

Totally 5 Records | Each Page 20 Records | Page 1 / totally 1 Pages | GO

2) Choose a user type as required among **Common User**, **Guest User**, and **Thirdparty User** (this option is offered only when **Third Party Correlation Registration** is enabled). Enter mandatory information, and click **Add** to complete it.

Authentication & Authority > User > Add User

Basic Information

\* User Type:  Common User  Guest User  Thirdparty User \* User Status:  Normal  Suspended

\* User Name:  \* Full Name:

Nick Name:

\* Password:  \* Confirm Password:

\* Type of Account Validity Period:  Never Expire  Delete Account when Expire  Suspend Account when Expire

\* User Group:  [Select User Group](#)

Customize User Fields [Add Custom User Fields](#)

No custom user field is found. Please click Add a Custom User Field to add it.

Detail Information

Gender:  Email Address:

ID Type:  ID Number:

Educational Background:  Telephone Number:

Mobile Number:  Address:

Postal Code:

Network Binding List [Add Network Binding List](#)

No network binding information of the user is found. Please click Add a Network Binding List to add it.

Tips:

- You can add or import the network binding information, which takes effect only when the user group enables network information verification.
- When network information verification is enabled for the user group, the system learns network information in the first user authentication and regards it as network binding information for

3) To add multiple users together, you can import a prepared file.

Authentication & Authority > User > Query Users

User Name:  Full Name:  User Group:  User Type: All User Status: All

Online or not: All In Blacklist or not: All  Accurate Search   [Advanced Search](#) [Query users offline for a long time](#)

[Customize User Fields](#) [SIM Card Management](#) [Customize Query List](#) [User Information Self-Service Maintenance](#)

Totally 6 Records | Each Page 20 Records | Page 1 / totally 1 Pages | GO

All None	User Name	Full Name	User Group	Type of Account	Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	Operation
<input type="checkbox"/>	1108	1108	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	1108@smpad.com	1108@smpad.com	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	smpad.com1108	smpad.com1108	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	smpad1108	smpad1108	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	test	111	ad	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	testuser	add	test	Never Expire			0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>

Totally 6 Records | Each Page 20 Records | Page 1 / totally 1 Pages | GO

Authentication & Authority > User > Import Users

Upload Files

Importing File (\*.xls\*.csv):  浏览...

Overwrite Existing Users

Delete users not contained in the imported file

**Tips:**

1. The number of users cannot exceed 10,000.
2. Only EXCEL or CSV files based on template format can be imported. Please click [here](#) to download an import template.
3. If the required information is not included in the Import Template, users can create a new file based on the template.



### Note

You can import a file of third-party users only when **Third Party Correlation Registration** is enabled.



### Note

If the user already have one of the following ID origins, you are advised to enable **External Identity Center**:

- a) Correlation with Generic Lightweight Directory Access Protocol (LDAP)
- b) Correlation with Windows AD Domain
- c) Correlation with External Database, such as SQL server, Oracle, MySQL, DB2, and PostgreSQL

- d) Remote Radius Server
- e) Webservice Server

## Configuring the NAS

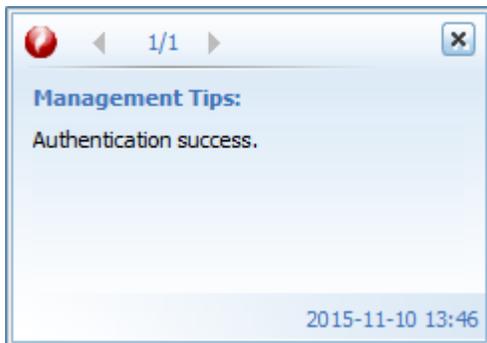
On the NAS, enable the 802.1X or Web authentication function as well as the port control function. For details, see its *Configuration Guide*.

## Authenticating a User

- 1) Connect the user terminal to a controlled port on the switch.
- 2) Use Ruijie Security Agent (RG-SA) for authentication.



If authentication is successful, the following page is displayed.

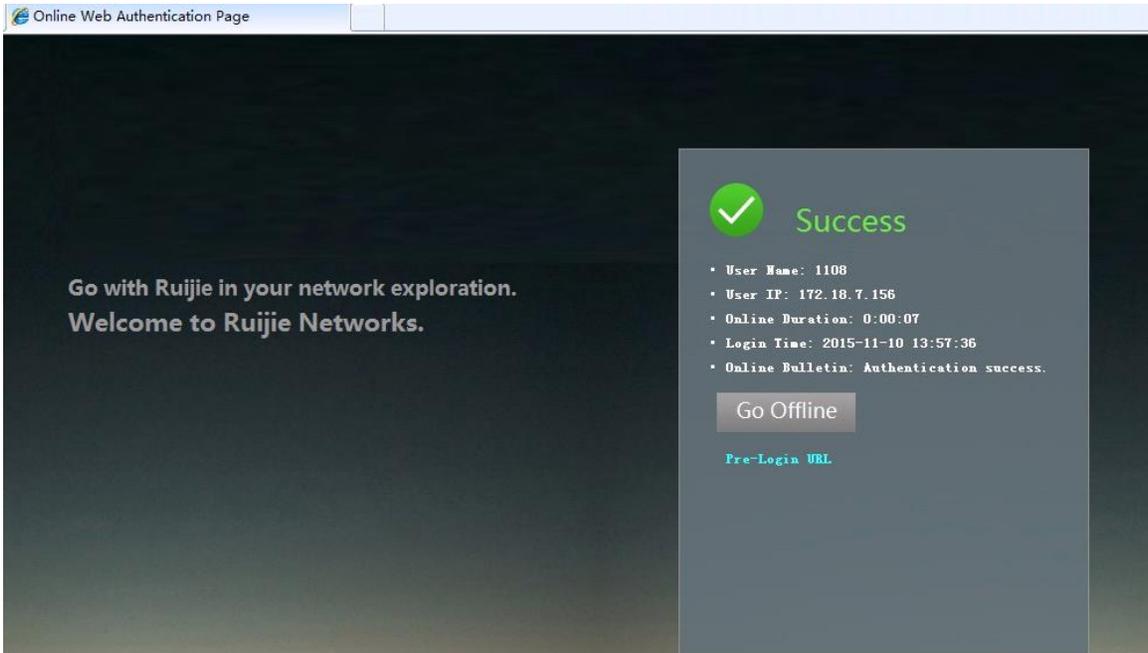




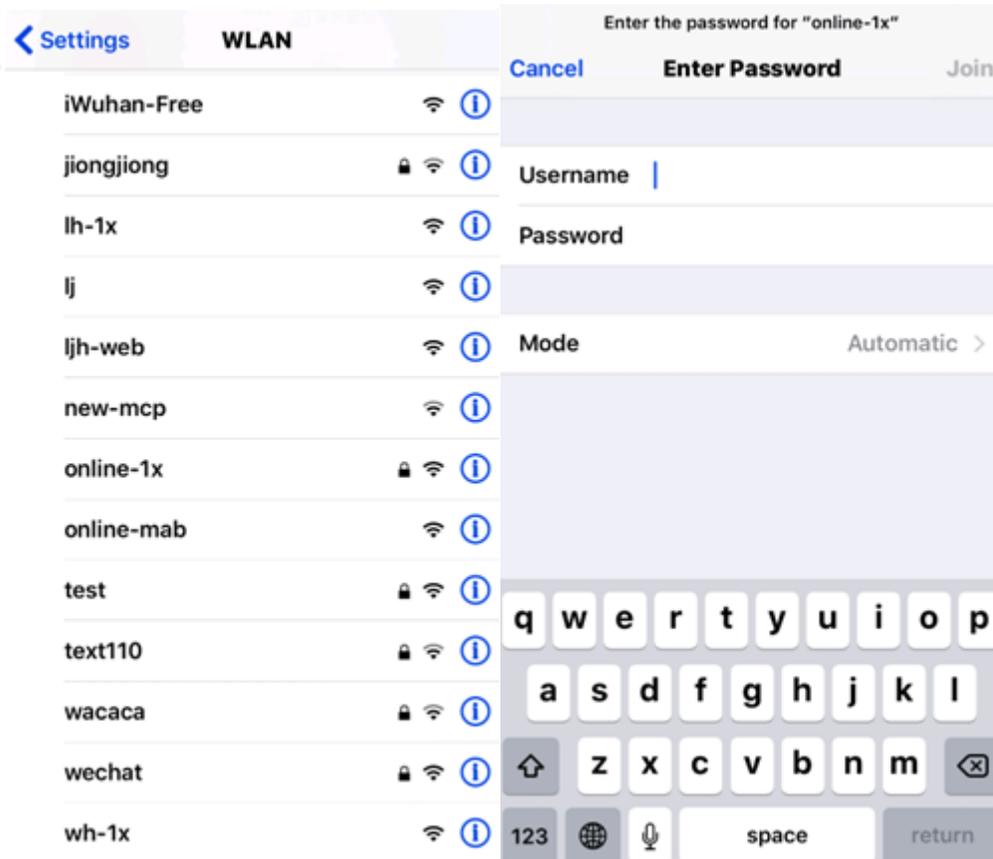
3) Use Web authentication to login.

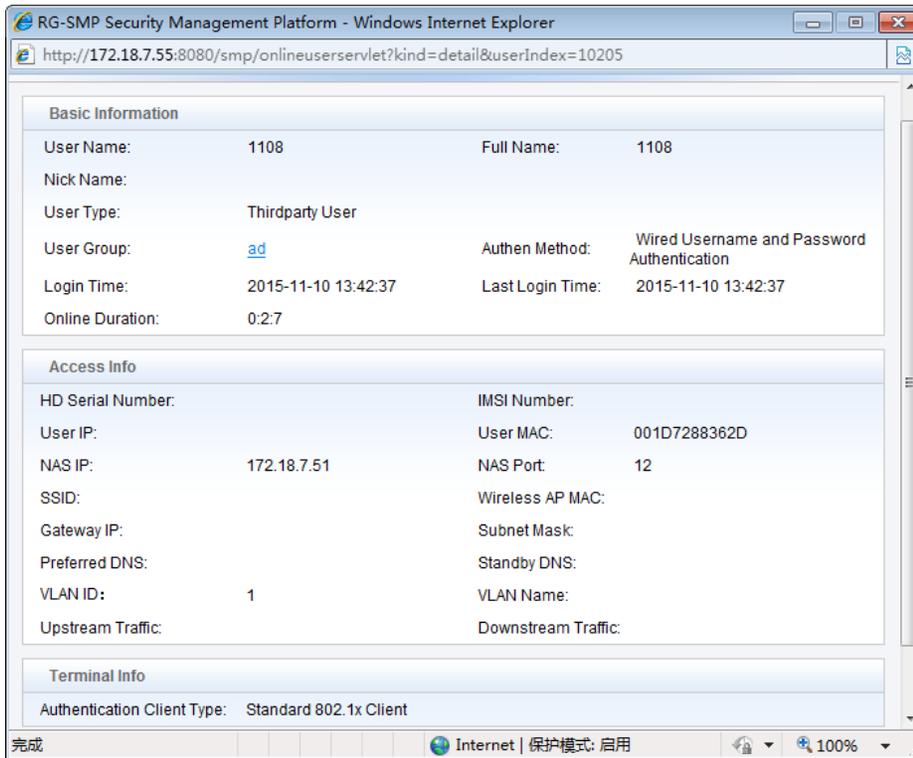


If authentication is successful, the following page is displayed.



4) Use the 802.1X client installed in the OS (e.g. iOS) for authentication. Choose **Settings** > **WLAN**. Enable WLAN, select the SSID to be connected, and enter the username and password.





## Wireless User Access

### Function Description

This section describes how to configure RG-SMP for wireless access authentication.

### Configuration Tips

See section [2.1.1.2 "Configuration Tips"](#).

### Configuration Steps

## Adding a NAS

See section [2.1.1.3.1 "Adding a NAS"](#).

## Adding a User Group

See section [2.1.1.3.2 "Adding a User Group"](#).

## Adding or Importing a User

See section [2.1.1.3.3](#) "错误!未指定书签。 [Adding or Importing a User](#)".

## Configuring the NAS

See section [2.1.1.3.4](#) "[Configuring the NAS](#)".

## Authenticating a User

See section [2.1.1.3.5](#) "[Authenticating a User](#)".

## Webauth User Access

### Function Description

Almost all terminals are installed with browsers, and the authentication client is not necessary. Therefore, Web authentication is the most simple and popular authentication mode. In addition, Web authentication enables you to customize the pages of advertisements, slogans, or redirection links, which meets the customers' requirements for advertising and notification.

### Configuration Tips

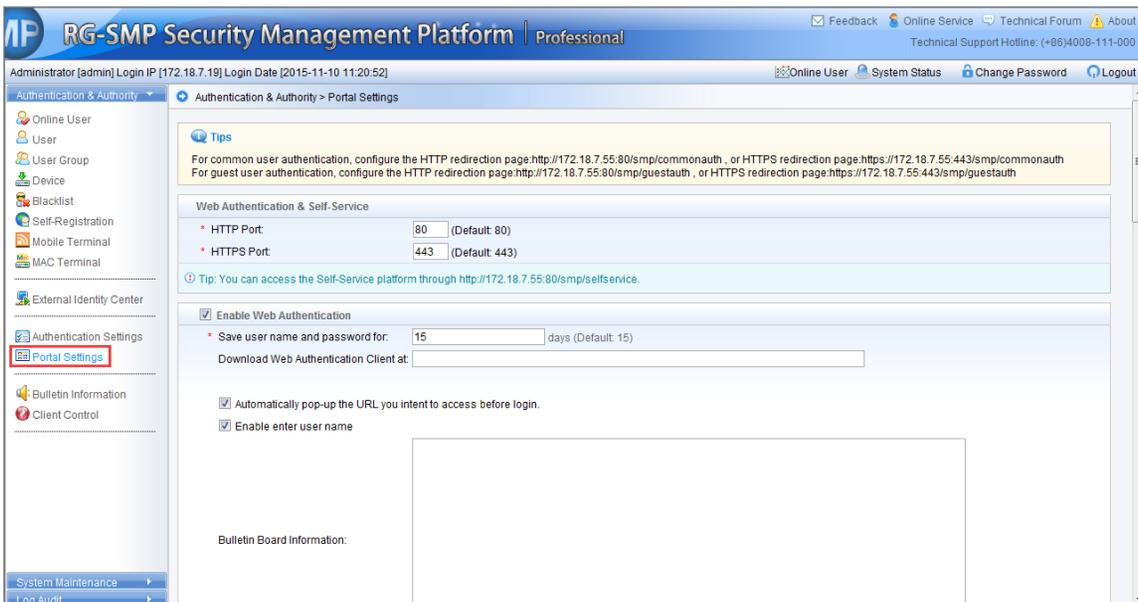
- Web authentication modes include Basic Web Authentication, Guest Password Authentication, Guest SMS Authentication, Guest QR Code Authentication, and Guest QR Card Authentication, and Authentication Exemption. You can enable an authentication mode based on the scenario.
  - i. Basic Web Authentication is aimed at internal employees.
  - ii. Guest Password Authentication is applicable to public areas, such as hotels.
  - iii. Guest SMS Authentication is aimed at guests who are waiting in public areas, such as banks, air ports, railway stations, and shopping malls. It is used for self-service registration to meet temperature network access requirements.
  - iv. Guest QC Code Authentication is applicable to visitors who need to access networks temporarily.
  - v. Guest QR Card Authentication is applicable to visitors who need to access networks temporarily.
  - vi. Authentication Exemption is applicable to public services, or offered by vendors for the brand promotion and market occupation.
- Web authentication is less secure than 802.1X. In this case, the random verification code is provided for users with higher demands on security. During Web authentication, in addition to the correct usernames and passwords, users need to enter the verification codes for secondary authentication to improve the security of network access.

- If the user already has a third-party ID, you can enable **Third Party Correlation Registration** on RG-SMP. Or, enable **SMS** or **Email** to verify authentication for RG-SMP local users.
- You must enable MAC authentication bypass (MAB) or Web authentication on the NAS. For details about the configurations, see the *Configuration Guide*. Currently, Web-MAB authentication is supported in wired access mode, and Web-MAB authentication is supported in wireless access mode.
- HTTPS access is supported. For details, see **Tips** in the **Authentication & Authority > Portal Settings** page.

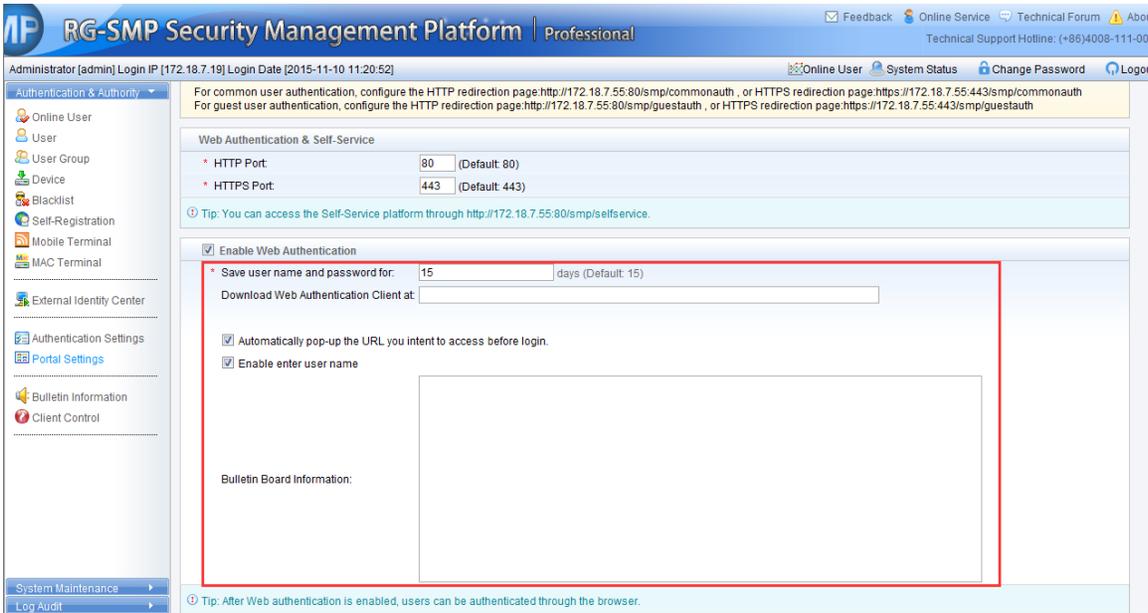
## Configuration Steps

### Basic Web Authentication

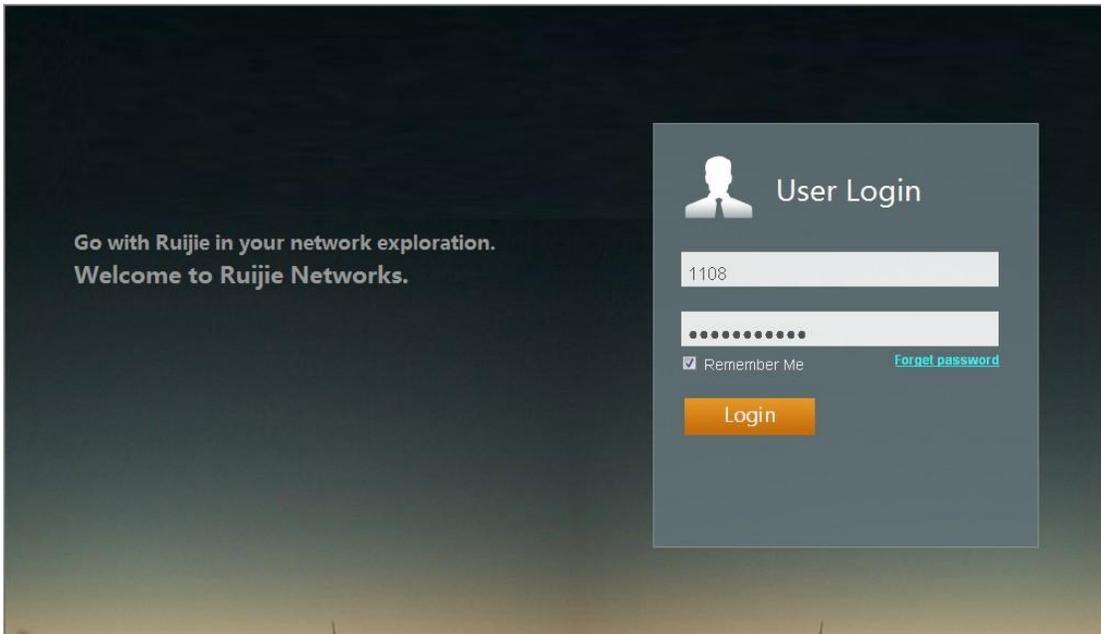
- 1) Choose **Authentication & Authority > Port Settings**, and check the **Enable Web Authentication** box to enter the Web authentication configuration page.



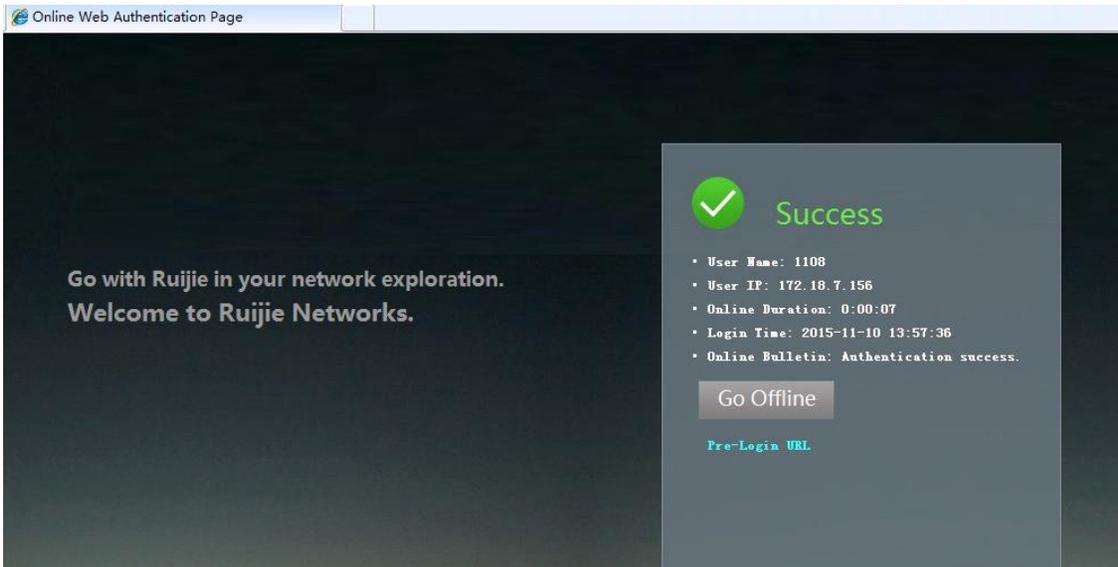
- 2) After the previous step, basic Web authentication is enabled. If it is disabled, users cannot get authenticated on Web. The administrator can customize the notification displayed on the Web authentication page in the **Bulletin Board Information** input box.



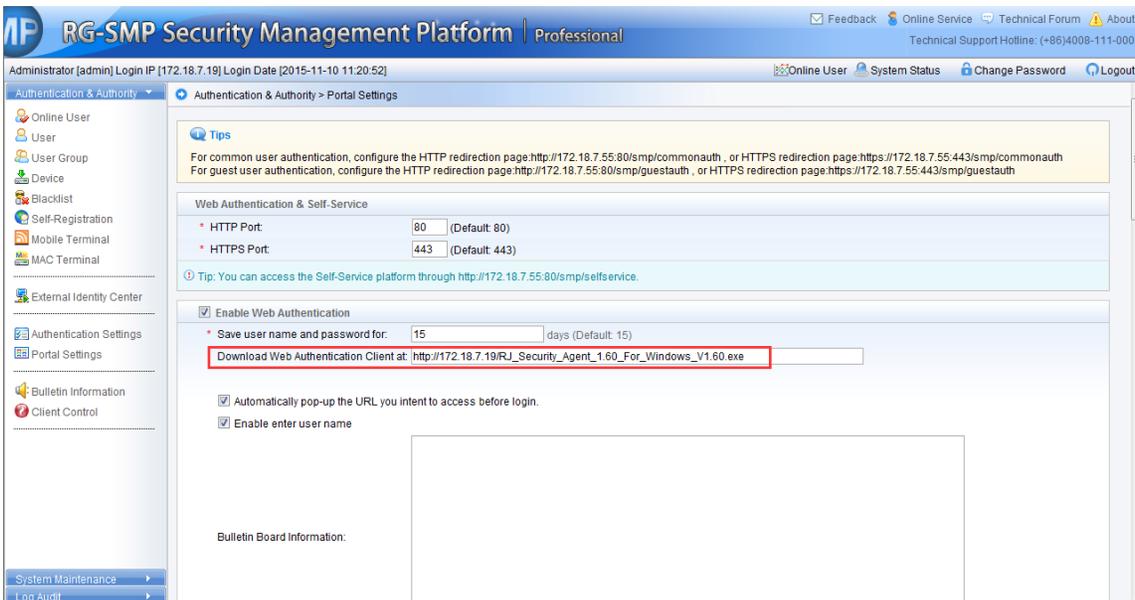
- 3) Configure the redirection URL for common users after authenticated on the NAS as advised in the tips of this page.
- 4) After the configuration is completed, the following URL page is displayed for users connected to controlled ports or associated with SSIDs enabled with Web authentication.



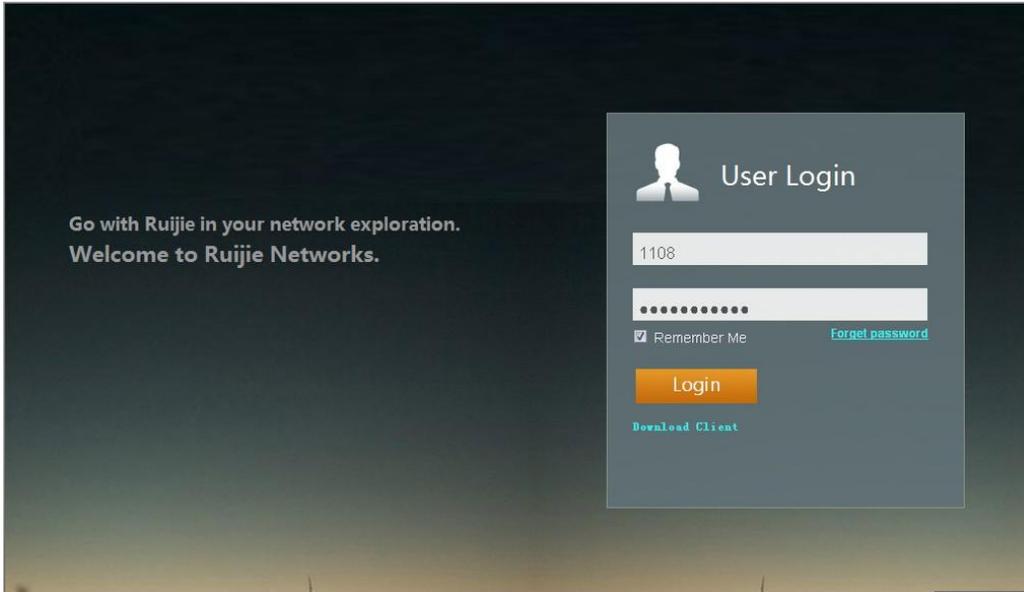
If authentication is successful, the following page is displayed.



5) If it is required that the RG-SA can be downloaded on the Web authentication page, configure the download address in the **Download Web Authentication Client** at input box. After configuration, users can download RG-SA by click **Download Client** hyperlink on the Web authentication page.



The following figure shows the **Download Client** hyperlink on the Web authentication page.

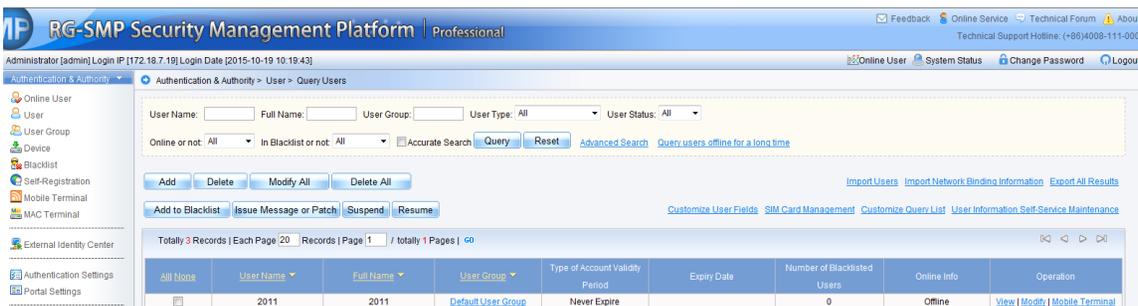


## Guest Password Authentication

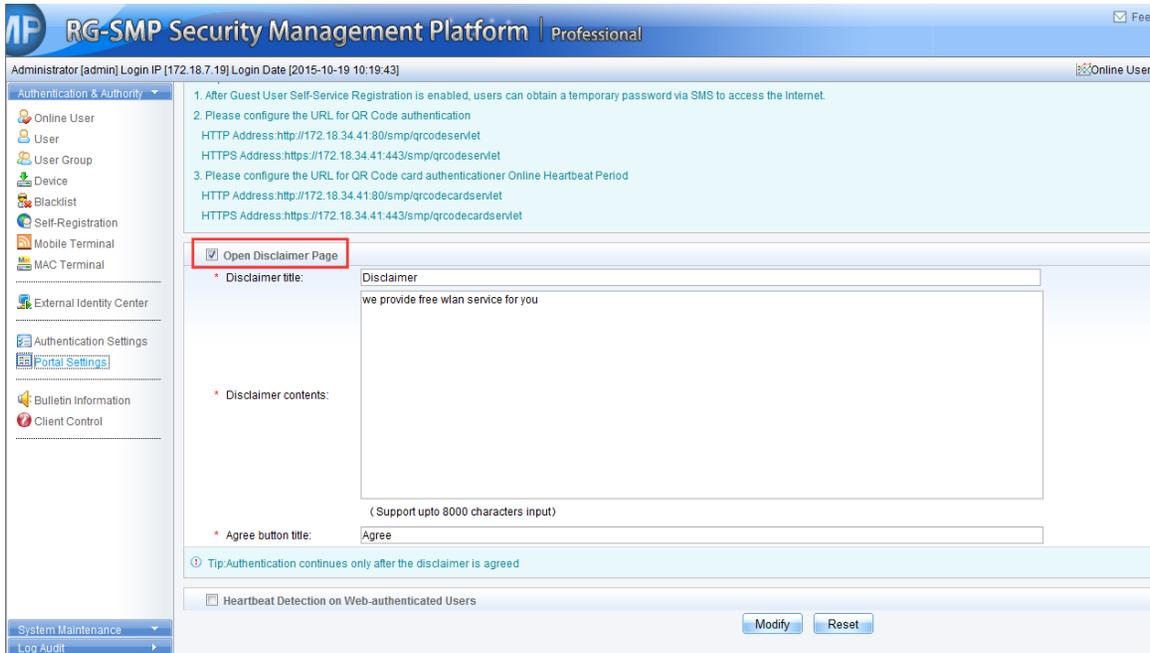
If the authentication disclaimer is configured, a guest must click **Agree** before authentication can continue.

Add the disclaimer to the basic Web authentication configuration. After the disclaimer is accepted by clicking **Agree**, guests only need to enter their passwords and click **Login** to access the network. (Note: A guest user is manually added by the system administrator, and the username and the password must be input correctly as configured.)

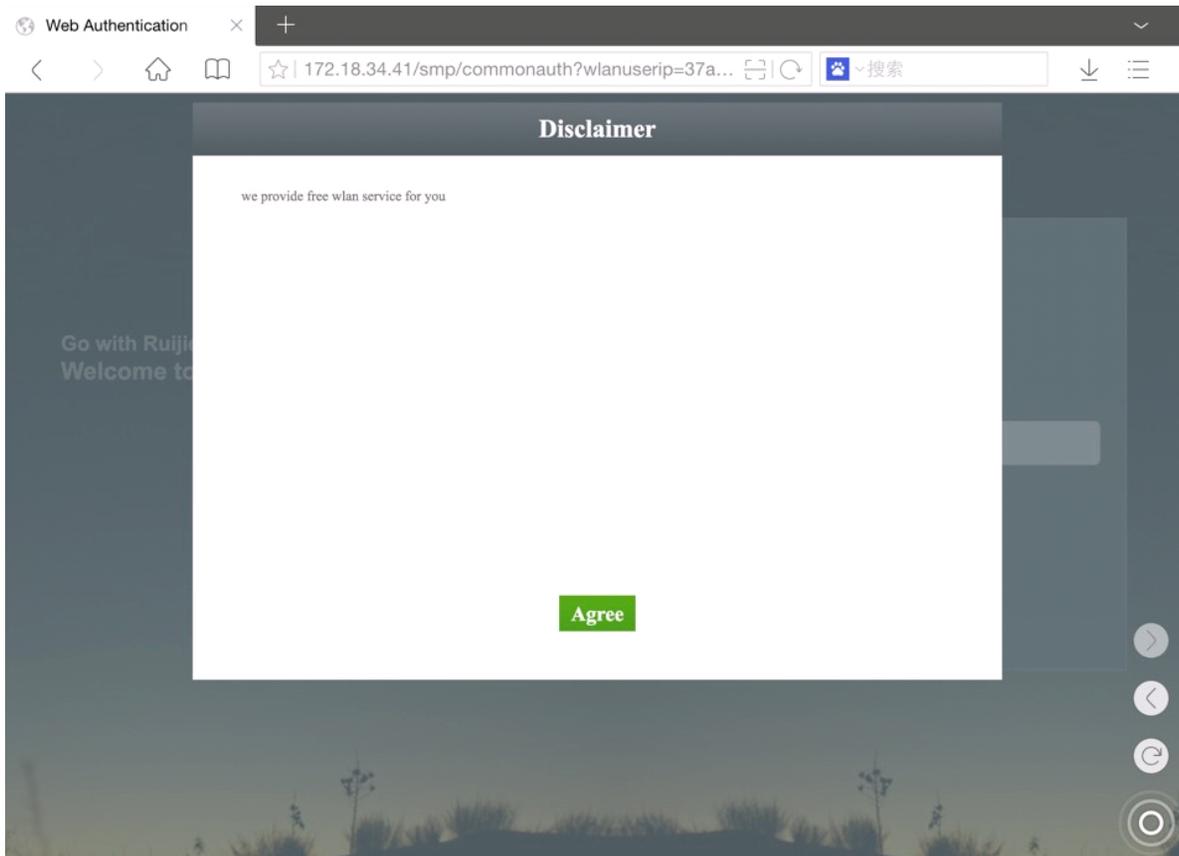
- 1) Choose **Authentication & Authority > User**, and click **Add** to add a guest whose username and password are 2011.

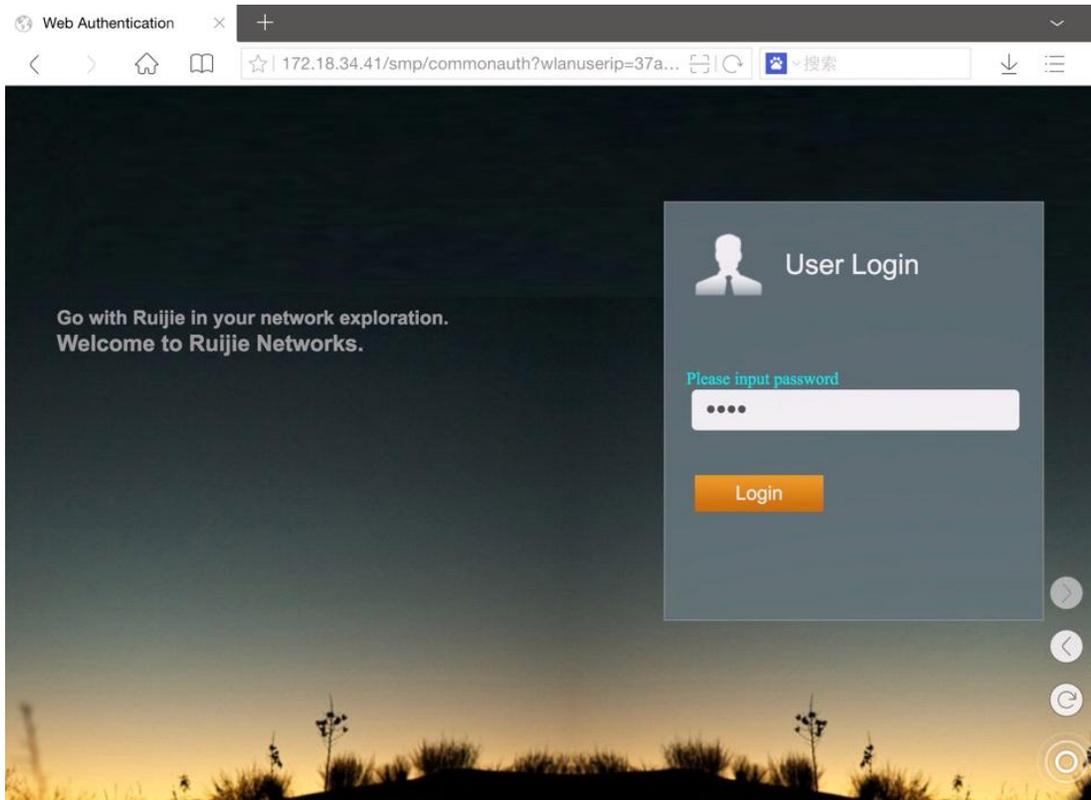


- 2) Choose **Authentication & Authority > Portal Settings**, check the **Open Disclaimer Page** box, configure the mandatory fields, and click **Modify** to save the modifications.

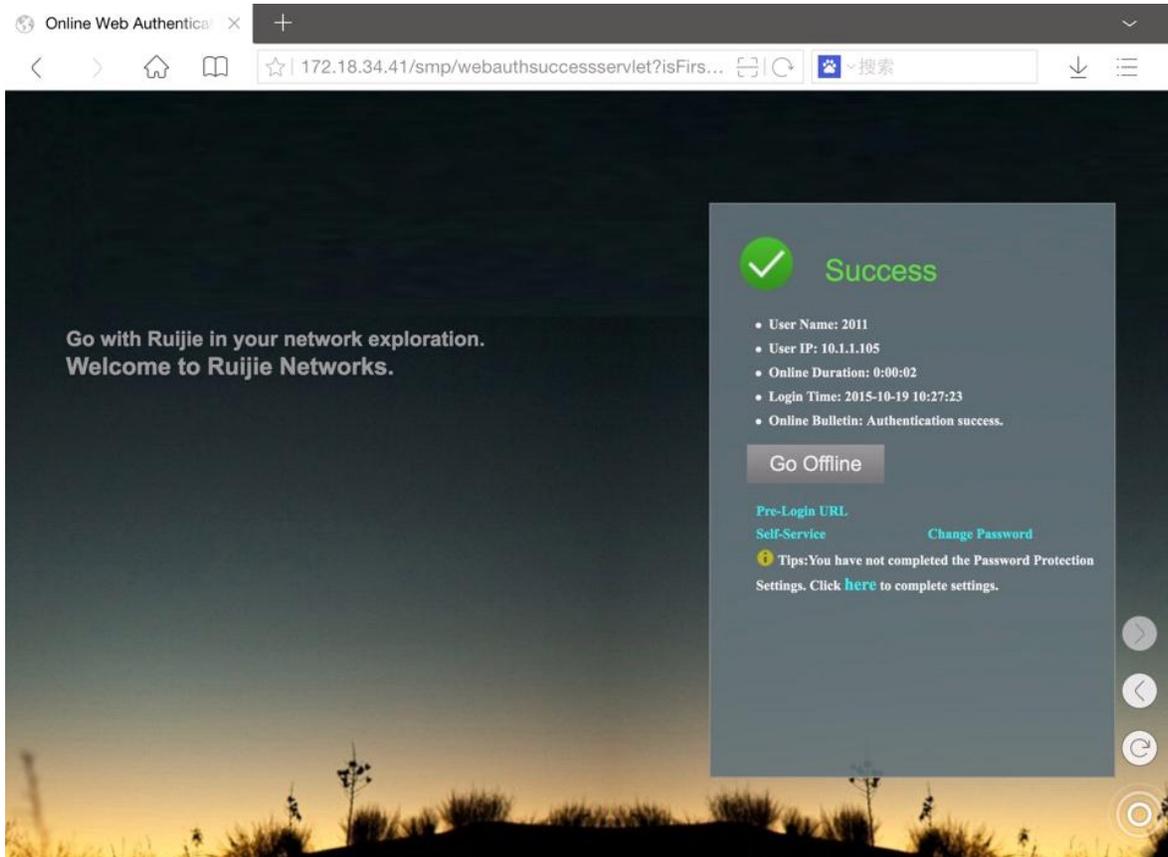


- 3) Configure the redirection URL for guests after authenticated on the NAS.
- 4) When a guest is used to access the network, a disclaimer page will be displayed. After the guest clicks Agree, the login page is displayed.





- 5) Enter the correct password, and the guest can successfully access the network.

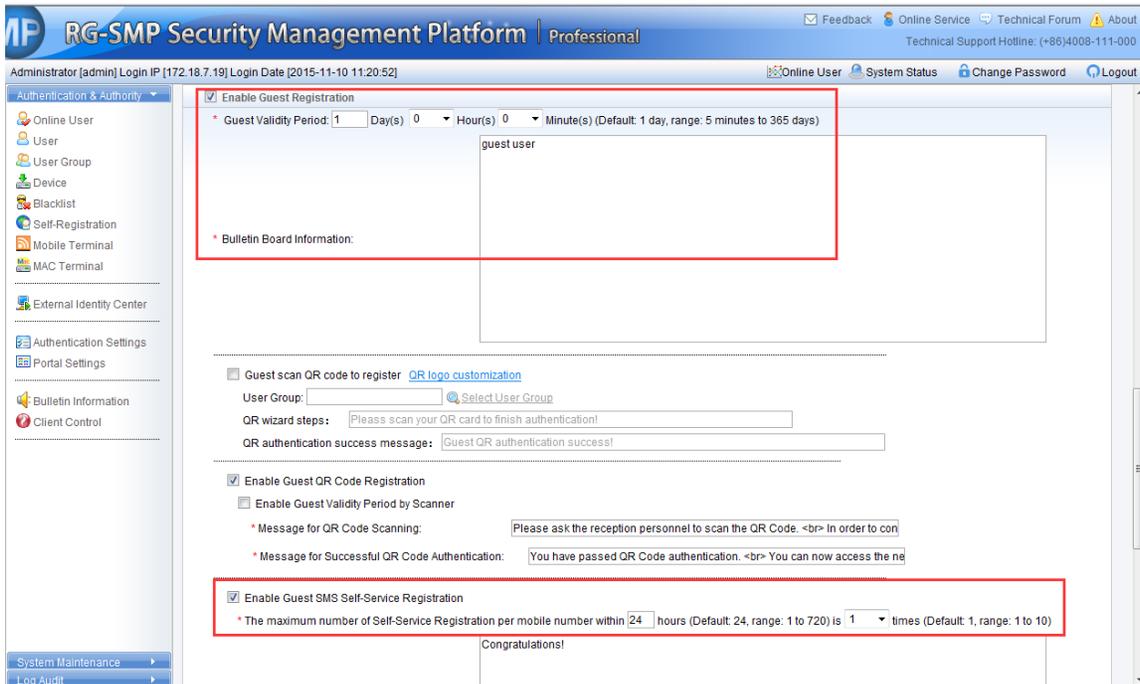


**Note** Here, the password and username of each user must be the same. These users are manually added by the system administrator. Before login, ensure that these users exist.

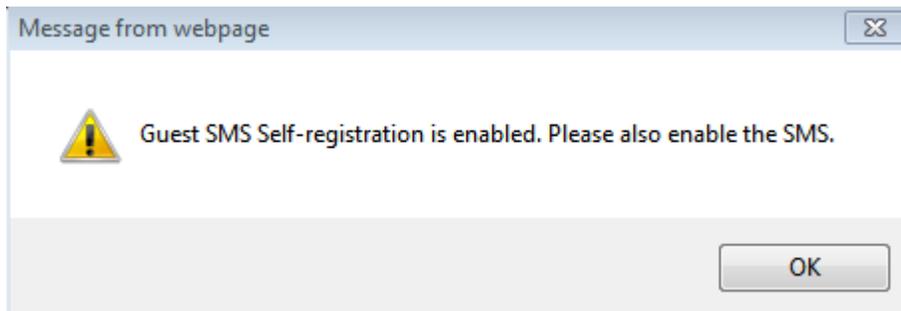
## Guest SMS Authentication

The administrator should complete configuration as follows:

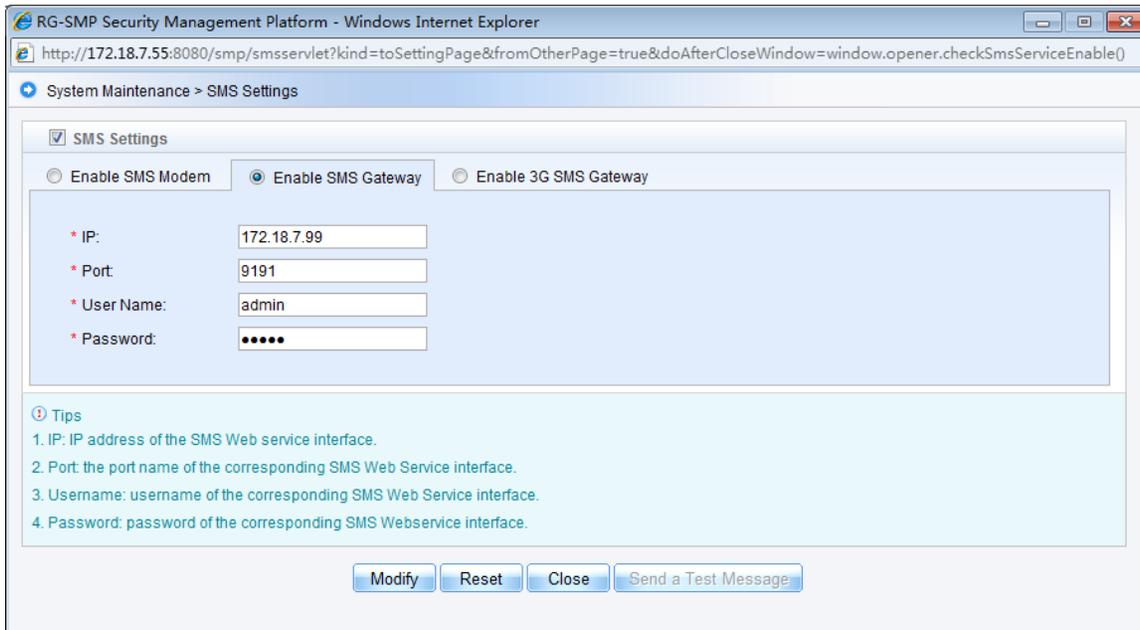
- 1) Choose **Authentication & Authority > Port Settings**, and check the **Enable Web Authentication** box to enter the Web authentication configuration page. After the **Enable Guest Registration** and **Enable Guest SMS Self-Service Registration** boxes are checked, the administrator can customize the options such as **Bulletin Board Information**, **Guest Validity Period**, and **The maximum number of Self-Service Registration per mobile number** on the guest registration page, and click **Modify** to save configuration.



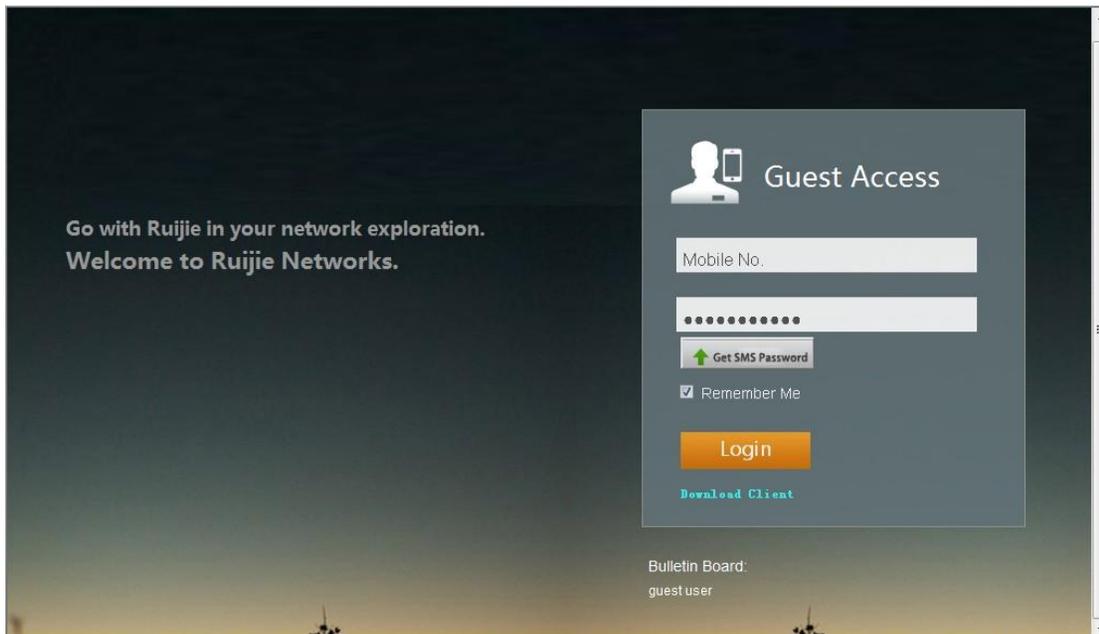
2) If the short message service (SMS) is not enabled, it is detected with the following prompt displayed. Click **OK**. The **SMS Settings** page will be displayed.



3) Check the **SMS Settings** box, and select the **Enable SMS Modem** or **Enable SMS Gateway** option for sending SMS based on the actual environment. If **Enable SMS Gateway** is selected, the customer must customize the SMS middleware based on the interface of the SMS gateway, which will not be detailed here. If **Enable SMS Modem** is selected, ensure that the SMS modem is connected to the RG-SMP server. If the SMS modem is a USB or USB-to-serial-port adapter, install the driver, which is available in the CD-ROM that is delivered with the SMS modem.



4) Configure the redirection URL of guest SMS authentication on the NAS. After the configuration is completed, the following page is displayed for users connected to the controlled ports or associated with SSIDs enabled with guest SMS authentication.



A user is authenticated by performing the following steps:

- Enter the mobile phone number, and click **Get SMS Password**.
- Enter the random SMS password received, and click **Login**. Authentication is successful.



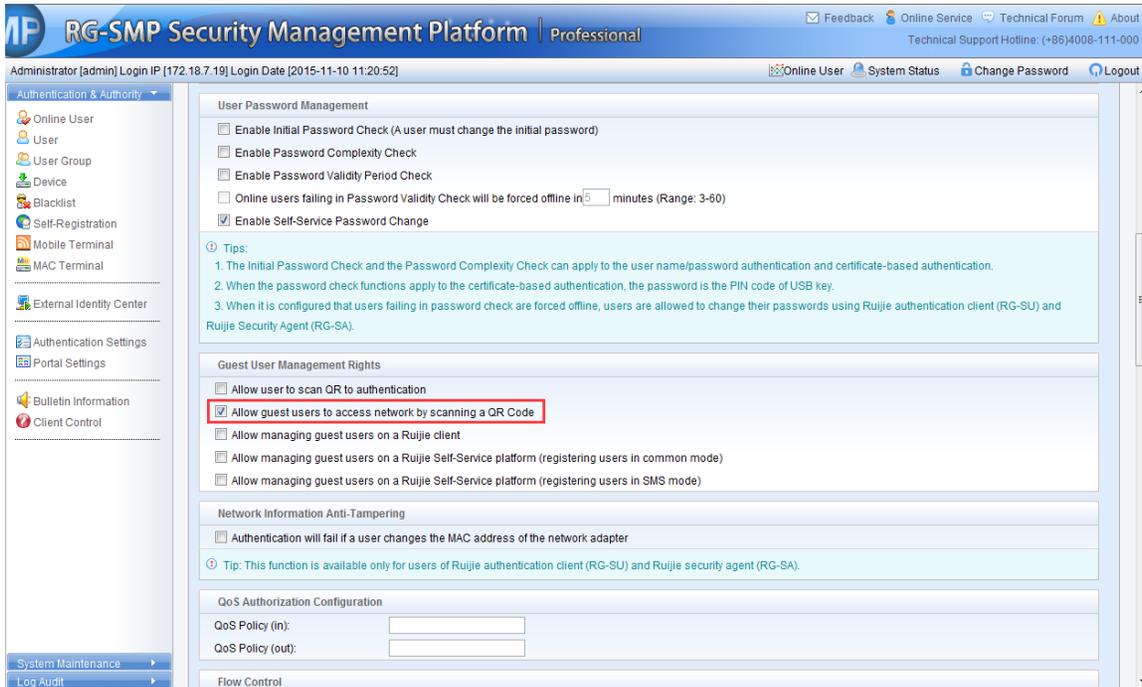
**Note** If no SMS password is received, check whether the SMS settings are correct or whether the SMS modem is correctly connected.

## Guest QR Code Authentication

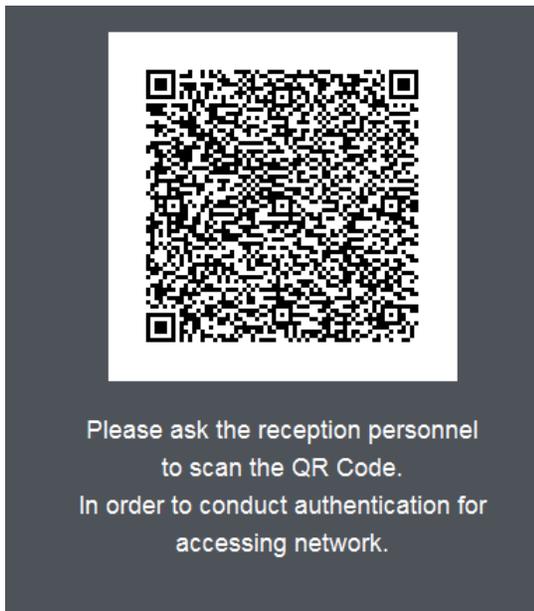
- 1) Choose **Authentication & Authority > Portal Settings**. Check the **Enable Guest Registration** and **Enable Guest QR Code Registration** boxes, and configure the **User Group**.

The screenshot displays the configuration interface for the RG-SMP Security Management Platform. The main configuration area is titled 'Web Authentication & Self-Service'. It includes fields for 'HTTP Port' (80) and 'HTTPS Port' (443). Below these are several checkboxes: 'Enable Web Authentication', 'Enable Authentication-Exemption Rule for Web Users', and 'Enable Guest Registration' (which is checked). The 'Enable Guest Registration' section contains a 'Guest Validity Period' set to 1 Day(s), 0 Hour(s), and 0 Minute(s), and a text area with the value 'guest user'. At the bottom, there is a section for 'Guest scan QR code to register' (checked), which includes a 'QR logo customization' link, a 'User Group' dropdown menu set to 'test', a 'QR wizard steps' field containing 'Please scan your QR card to finish authentication!', and a 'QR authentication success message' field containing 'Guest QR authentication success!'.

- 2) After the user group is configured, enable QR code authentication.



- 3) Configure the redirection URL of QR code authentication.
- 4) The following figures show the QR code for authentication:





## Guest QR Card Authentication

- 1) Choose **Authentication & Authority > Portal Settings**. Check the **Enable Guest Registration** and then the **Guest scan QR code to register** boxes.

Enable Guest Registration

\* Guest Validity Period: 1 Day(s) 0 Hour(s) 0 Minute(s) (Default: 1 day, range: 5 minutes to 365 days)

test qrcode

\* Bulletin Board Information:

---

Guest scan QR code to register [QR logo customization](#)

\* User Group:  [Select User Group](#)

\* QR wizard steps:

\* QR authentication success message:

- 2) Choose **Authentication & Authority > User Group**. Select the default user group, and click **Modify** in the **Operation** column. Click the **Behavior Restrict** tab in **Modify User Group** page, and check the **Allow user to scan QR to authentication** box under **Guest User Management Rights**.

Guest User Management Rights	
<input checked="" type="checkbox"/>	Allow user to scan QR to authentication
<input type="checkbox"/>	Allow guest users to access network by scanning a QR Code
<input type="checkbox"/>	Allow managing guest users on a Ruijie client
<input type="checkbox"/>	Allow managing guest users on a Ruijie Self-Service platform (registering users in common mode)
<input type="checkbox"/>	Allow managing guest users on a Ruijie Self-Service platform (registering users in SMS mode)

3) Enter the RG-SMP self-service platform as a user of the default group to check the QR card of the user.

4) On the **QR card** page, the user is able to print, save, or regenerate the QR card.

5) Configure the redirection URL of QR card authentication on the NAS.

6) After a user terminal is connected to the network, the following page is displayed when the user tries to browse a website.

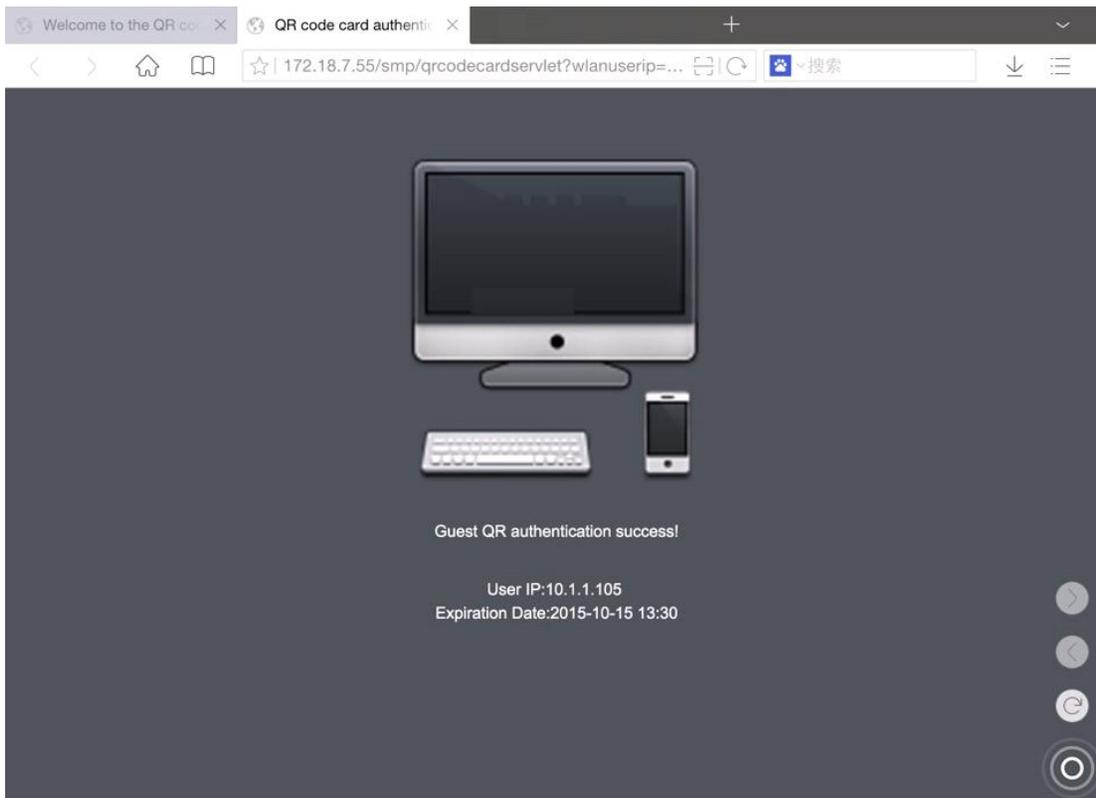


**Note** For iOS device, **Auto-Login** should be disabled before connecting to wireless network. Otherwise, iOS might disconnect the wireless network once guests switch to QR Code Scanner Tools.



7) Use the QR scan-supported tools (e.g. WeChat) to scan the QR codes generated on the self-service platform.

If authentication succeeds, the following page is displayed.



8) You can regenerate your QR card on the self-service platform by clicking **Regenerate QR**. In this case, the old QR card is revoked automatically.

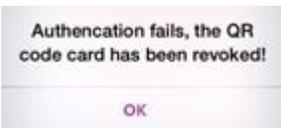
**QR card**

**QR brief introduction:**  
 QR is generation from your profile  
 Guest scan the QR to pass access authentication  
 guest who scan the QR will binding to your account

Buttons: Print QR code, QR saved as, **Regenerate QR**

Effective days (Default 7):   
 Effective scanning times (Default 30):

**Tips:**  
 Regenerate QR, the previous QR fails automatically



## Smart Authentication

Two smart authentication modes are available. One is 802.1X authentication. The other is Web-MAB (MAC Authentication Bypass) authentication which means Web authentication for the first time and later MAB authentication. The two modes are smart for a user who must enter the username and password for only the first authentication. In this document, smart authentication refers to the Web-MAB authentication mode.

When a user performs Web authentication for the first time, the MAC address of the user is automatically registered as a mobile terminal. Next time when the user tries to access, the user can be directly authenticated through MAB.

- 1) Choose **Authentication & Authority > User Group**, and click **Add** to add a user group. You can also click **Modify** to modify an existing user group, and enter the page for adding or modifying the user group.

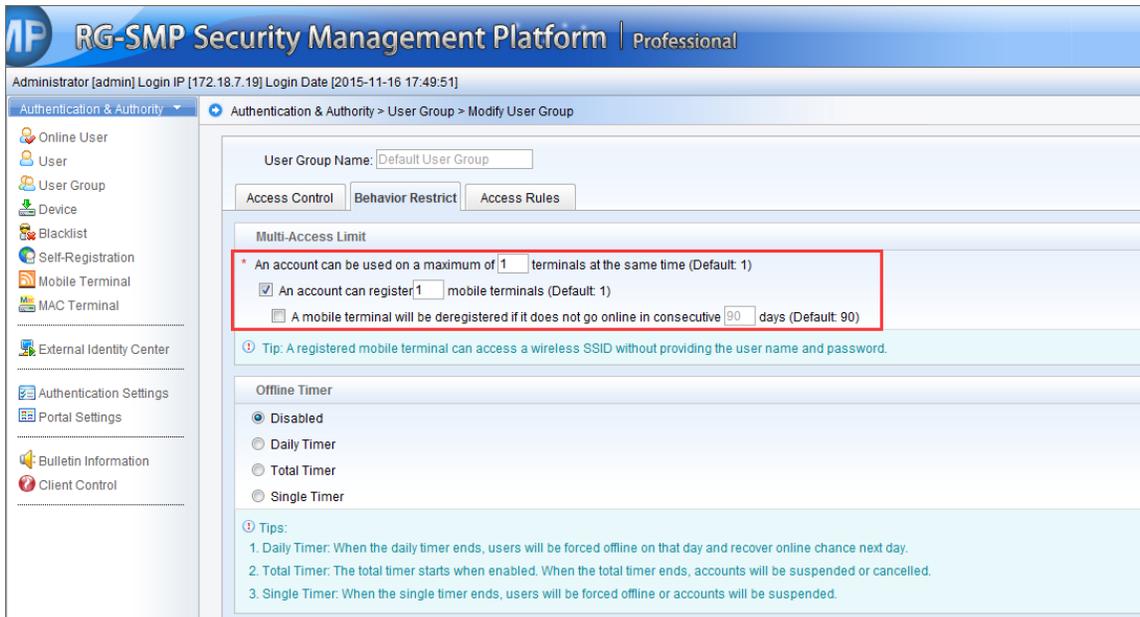
Authentication & Authority > User Group > Query User Groups

User Group Name:  Query Reset

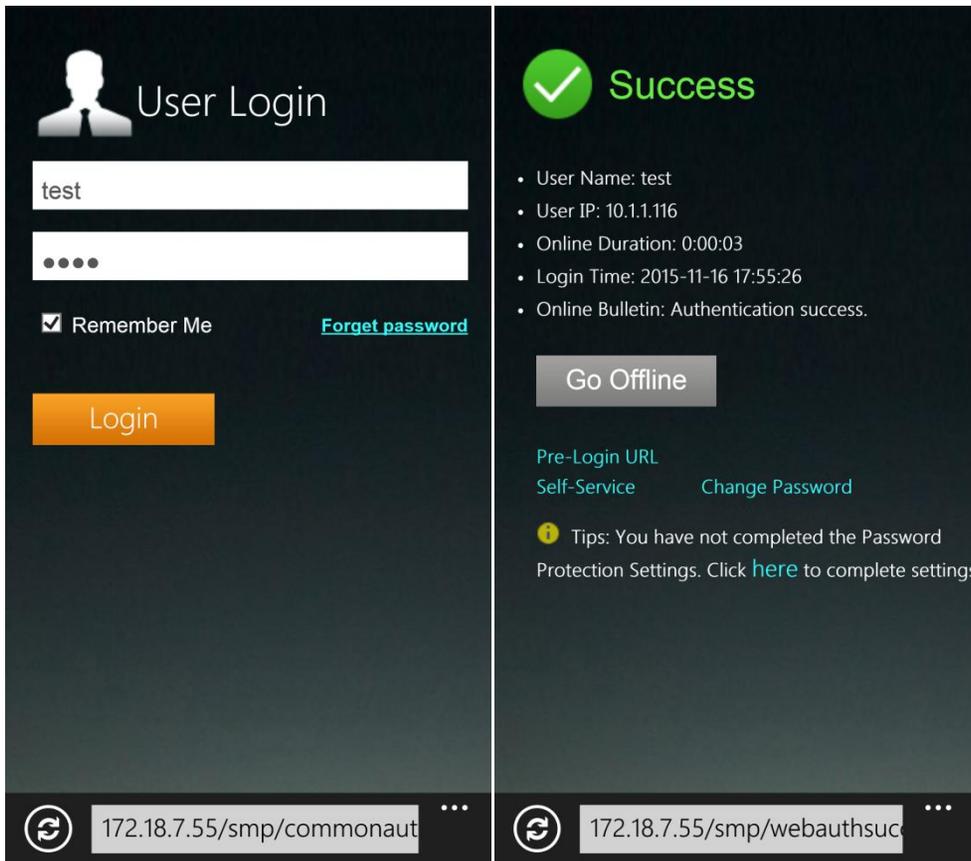
Buttons: Add Delete

All Users	User Group Name	Operation
<input type="checkbox"/>	Guest User Group	<a href="#">View</a> <a href="#">Modify</a> <a href="#">Restore Default Settings</a>
<input type="checkbox"/>	Default User Group	<a href="#">View</a> <a href="#">Modify</a> <a href="#">Restore Default Settings</a>

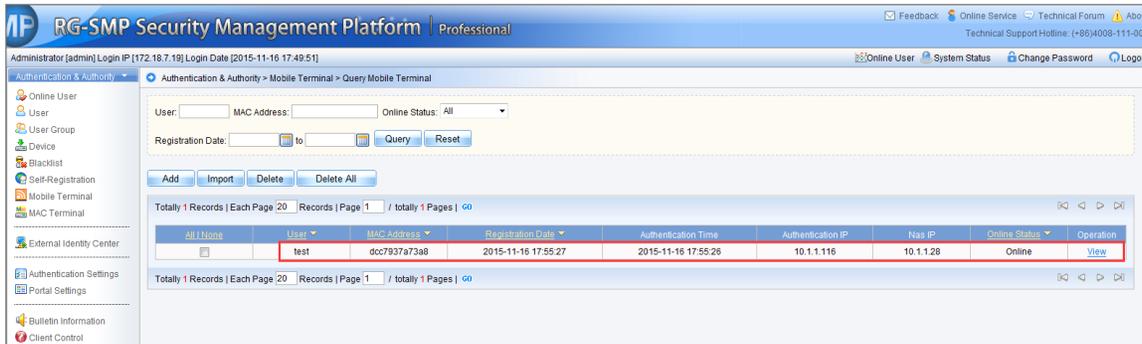
- 2) Select the **Behavior Restrict** tab, check the **An account can register X terminals at the same time** box and configure the times. Click **Modify** to save the settings.



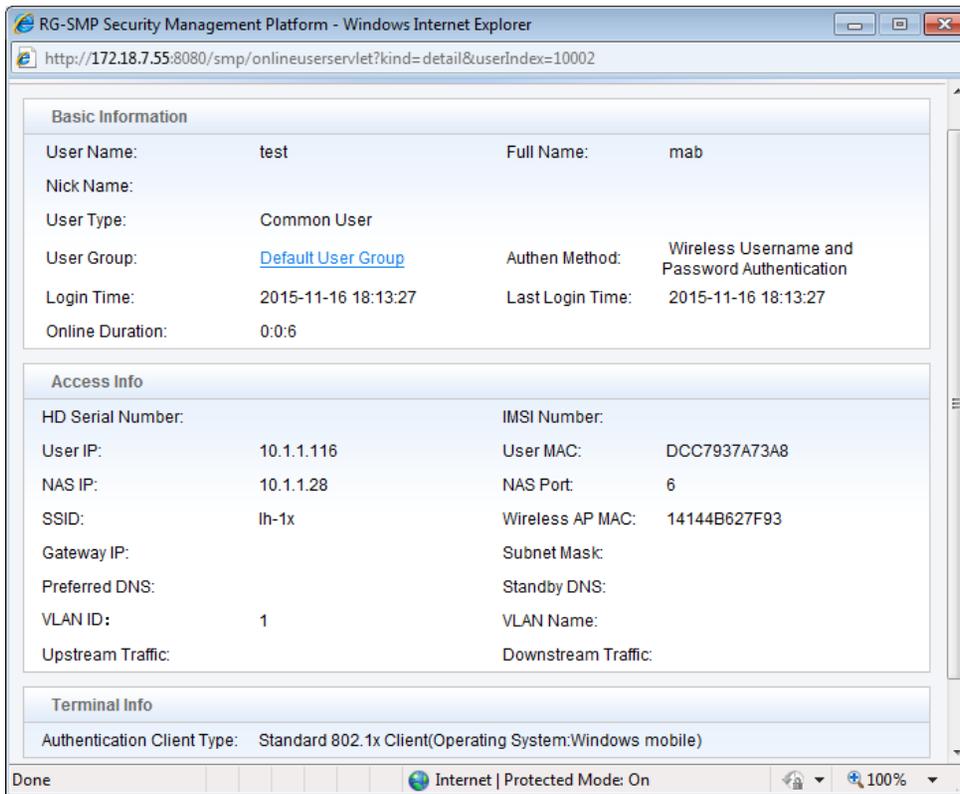
- 3) Configure Web authentication and MAB authentication on the NAS.
- 4) Use the common Web authentication, and enter the username and password to make authentication successful.



5) The user terminal is automatically registered on RG-SMP.



6) After the user goes offline, unplug and plug the network cable from the network port in wired access mode, or de-associate and re-associate the terminal from the SSID in wireless access mode. Then, the terminal will be automatically authenticated by MAB.



The screenshot shows a web browser window titled "RG-SMP Security Management Platform - Windows Internet Explorer" with the URL "http://172.18.7.55:8080/smp/onlineuserservlet?kind=detail&userIndex=10002". The interface displays user information in three sections:

Basic Information			
User Name:	test	Full Name:	mab
Nick Name:			
User Type:	Common User		
User Group:	<a href="#">Default User Group</a>	Authen Method:	Wireless Username and Password Authentication
Login Time:	2015-11-16 18:13:27	Last Login Time:	2015-11-16 18:13:27
Online Duration:	0:0:6		

Access Info			
HD Serial Number:		IMSI Number:	
User IP:	10.1.1.116	User MAC:	DCC7937A73A8
NAS IP:	10.1.1.28	NAS Port:	6
SSID:	lh-1x	Wireless AP MAC:	14144B627F93
Gateway IP:		Subnet Mask:	
Preferred DNS:		Standby DNS:	
VLAN ID:	1	VLAN Name:	
Upstream Traffic:		Downstream Traffic:	

Terminal Info	
Authentication Client Type:	Standard 802.1x Client(Operating System:Windows mobile)

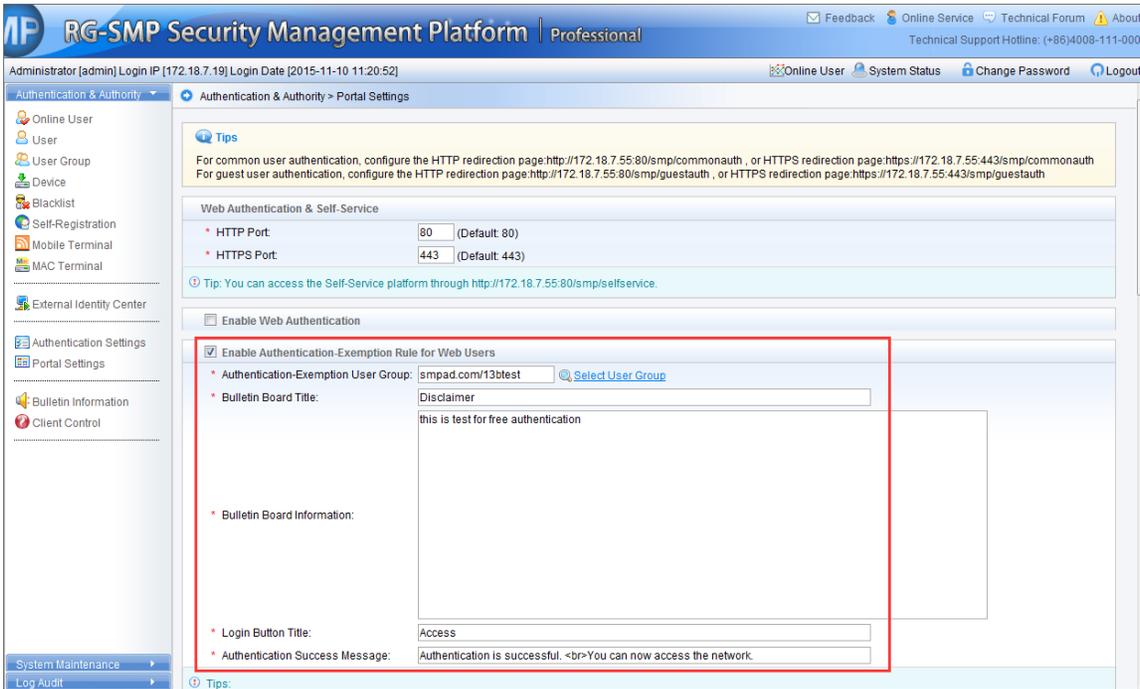


### Note

1. Both wired and wireless Web authentication supports the Web-MAB authentication mode.
2. When **Multi-Access Limit** is enabled, if the maximum number of registered mobile terminals using one username is reached, other user terminal entering this username cannot be authenticated.
3. If the **A mobile terminal will be deregistered if it does not go online in consecutive X days** box is checked and configured, a mobile terminal will be deregistered if it does not get re-authenticated in specified days.

## Authentication Exemption

- 1) Choose **Authentication & Authority > Port Settings**, and check the **Enable Web Authentication** box to enter the Web authentication configuration page. Check the **Enable Authentication-Exemption Rule for Web Users** box, and configure the **Authentication-Exemption User Group**, **Bulletin Board Information**, and so on.



- 2) Configure the redirection URL of authentication exemption.
- 3) After the user terminal is connected to the network, the following page is displayed when the user tries to browse a website.





## Network Information Verification

### Function Description

This section describes how to use the network information binding and verification functions of RG-SMP.

Currently, RG-SMP provides the function of verifying network information based on users. This verification mode is based on users, and can determine the network access requirements that every user must meet before accessing the network.

Modified settings will take effect upon next authentication of users.

### Configuration Tips

N/A

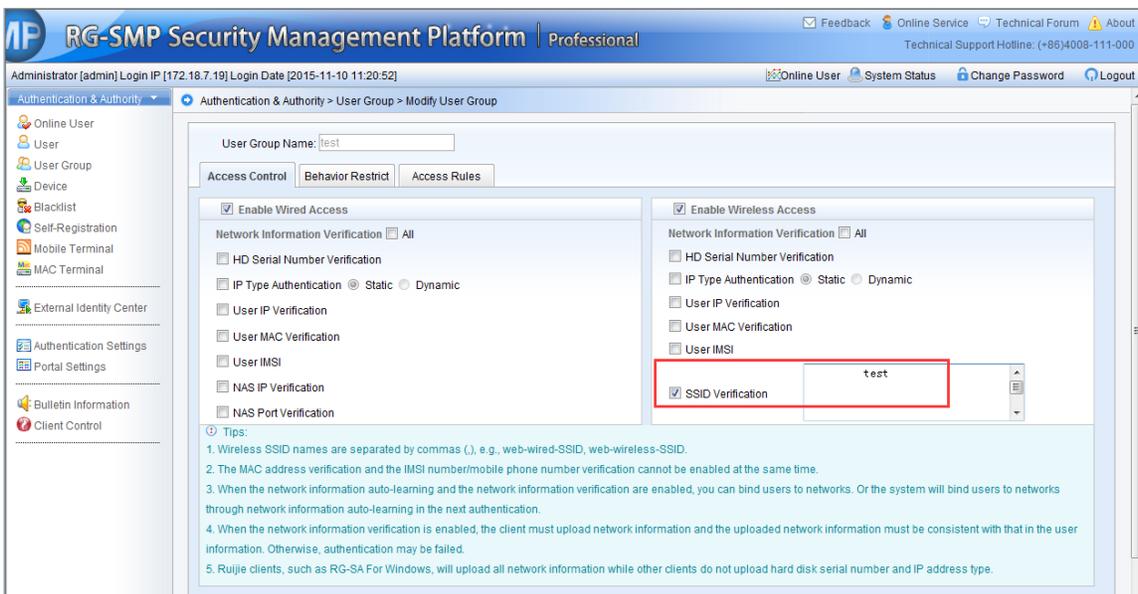
### Configuration Steps

## User Verification Rules

- 1) Choose **Authentication & Authority > User Group**, and click **Add** to add a user group. You can also click **Modify** to modify an existing user group.



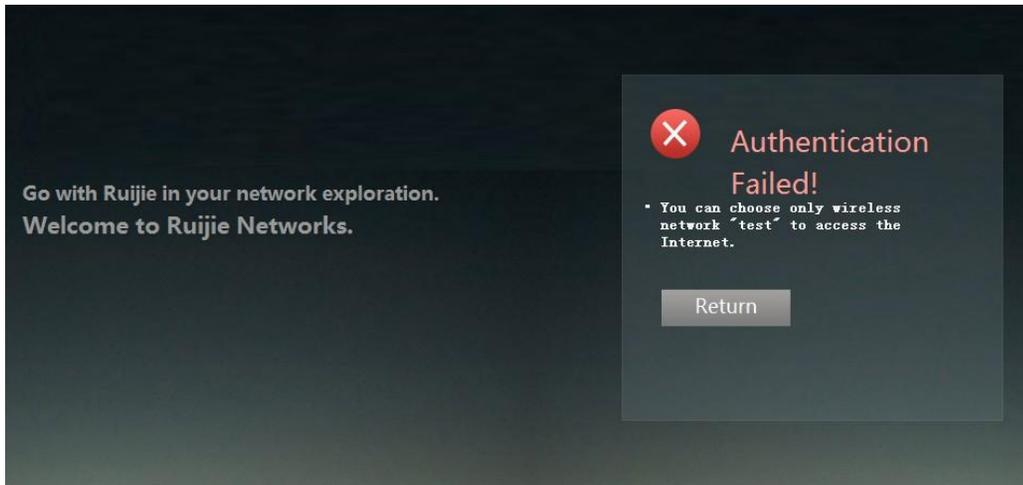
2) In the **Access Control** tab, configure different rules of network information verification for wired and wireless access.



3) Click **Modify**, and save the settings.

## User Verification

1) During user authentication, the user access information must be verified based on the preset network information verification rules before authentication can succeed.



**Note** In network information verification, **HD Serial Number Verification**, **IP Type Authentication**, and **User IMSI** verification cannot be implemented in Webauth user access mode.

## Offline Timer

### Function Description

This section describes how to use the offline timer of RG-SMP to control the online duration.

Currently, RG-SMP provides four modes of online duration control: **Disabled**, **Daily Timer**, **Total Timer**, and **Single Timer**.

### Configuration Tips

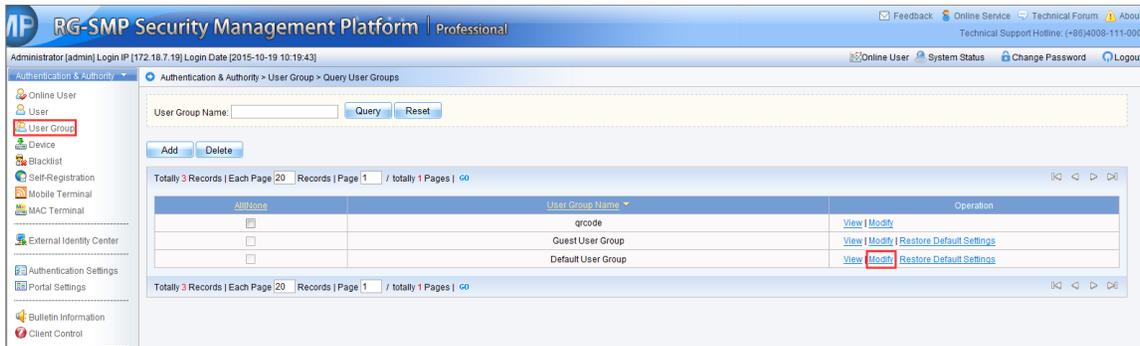
N/A

### Configuration Steps

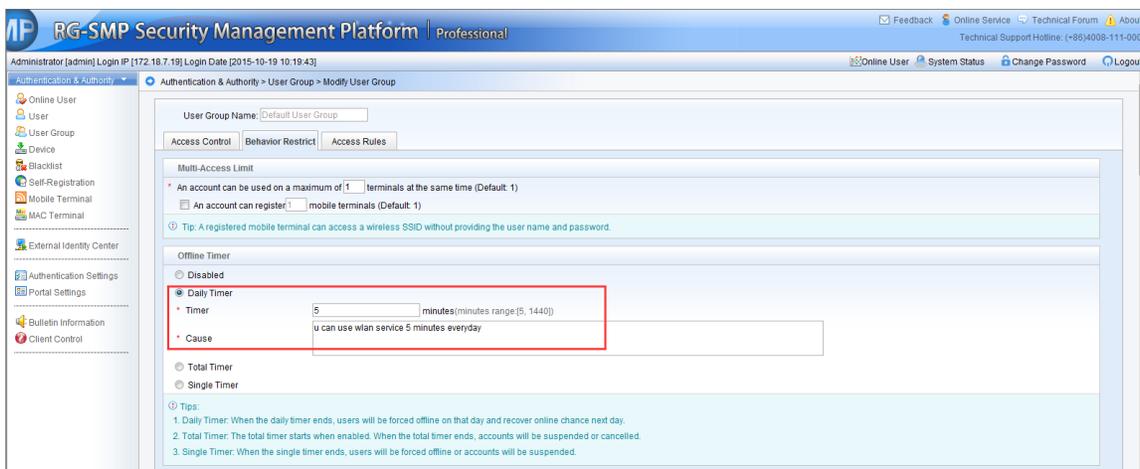
#### Daily Timer

Choose **Authentication & Authority > User Group**, and configure the daily timer which specifies the maximum online duration (**X** minutes) of a user per day for a specific user group. **X** is a positive integer. The default value is 120, and the value ranges from 5 to 1,440. The timer task is automatically started to test at the interval of one minute whether the daily online duration of any online user exceeds the limit. If yes, the system forces the user offline, and records the related information in the system log.

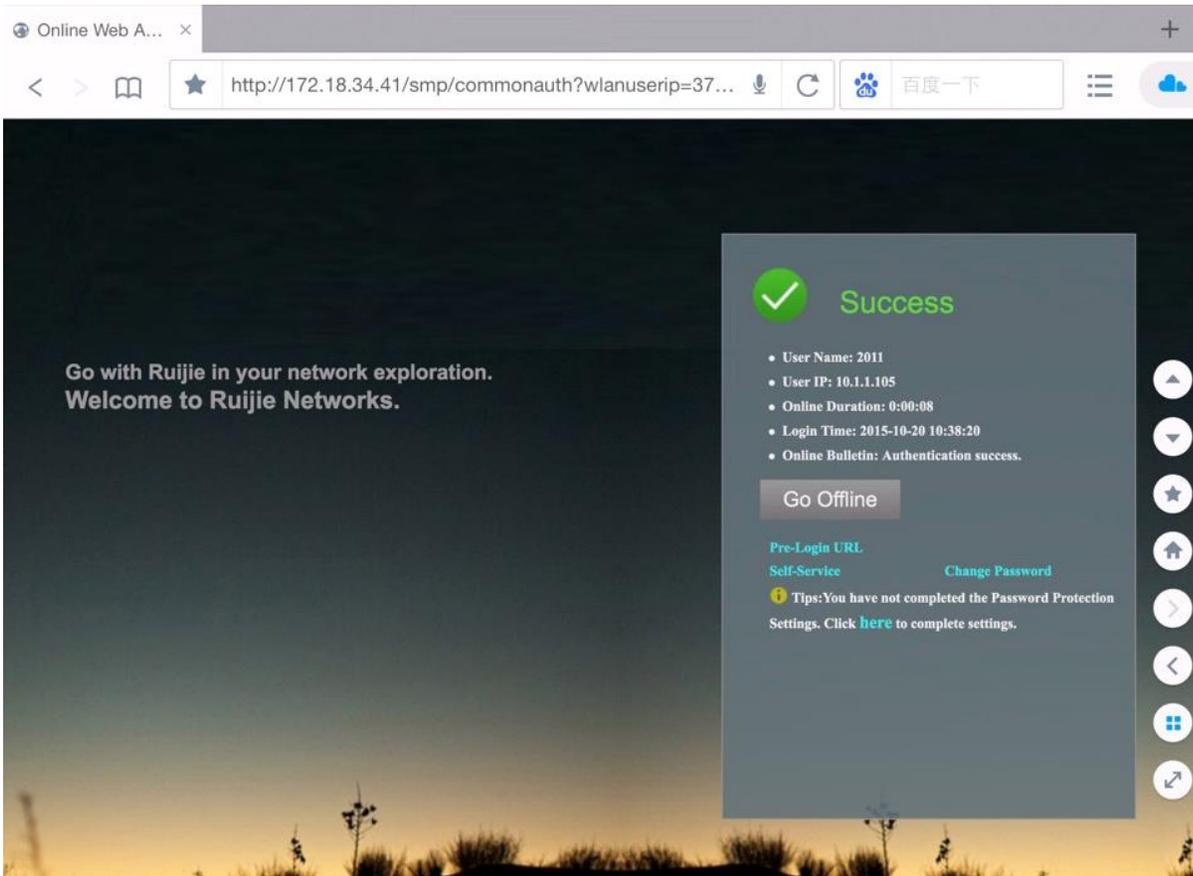
- 1) Choose **Authentication & Authority > User Group**, and click **Modify**.



2) Choose **Daily Timer**, set **Timer** to **5** minutes, and click **Modify** at the bottom of the page to save the changes.



3) Log in to RG-SMP as a user in the default user group. After the login succeeds, choose **Authentication & Authority > Online User** to check the online duration of the user.



4) If the online duration of the user exceeds five minutes, the user will be forced offline and suspended. Choose **Log Audit > System Logs** to display the system logs. If the following two logs are displayed, it indicates that settings of the daily timer have taken effect.

Log Audit > Network Access Logs > Query Logs

User Name:  User IP:  Offline Cause: All

Login Time: 2015-10-20 0:0:0 Logout Time: 2015-10-20 23:59:59 [Query](#) [Reset](#) [Advanced Search](#)

[Delete](#) [Export Query Results](#) [Delete All](#) [Network Traffic and Online Duration Report](#)

Totally 1 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

All None	User Name	User IP	Full Name	NAS IP	Login Time	Logout Time	Offline Cause	Operation
<input type="checkbox"/>	2011	10.1.1.105	2011	10.1.1.28	2015-10-20 10:38:20	2015-10-20 10:44:00	The offline timer ends!	<a href="#">View</a>

Totally 1 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

Log Audit > Operation Logs > Query Logs

Operator:  Log Content:  Record Time: 2015-10-20 - 2015-10-20 [Query](#) [Reset](#)

[Delete](#) [Delete All](#)

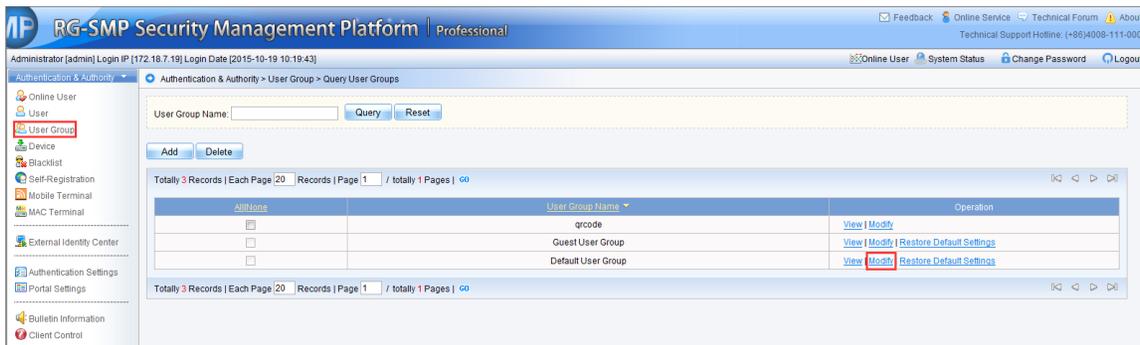
Totally 8 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

All None	Operator	Record Time	Log Content
<input type="checkbox"/>	system	2015-10-20 10:44:00	The daily offline timer of 5 minutes for User(2011, 10.1.1.105)ends with user suspension.

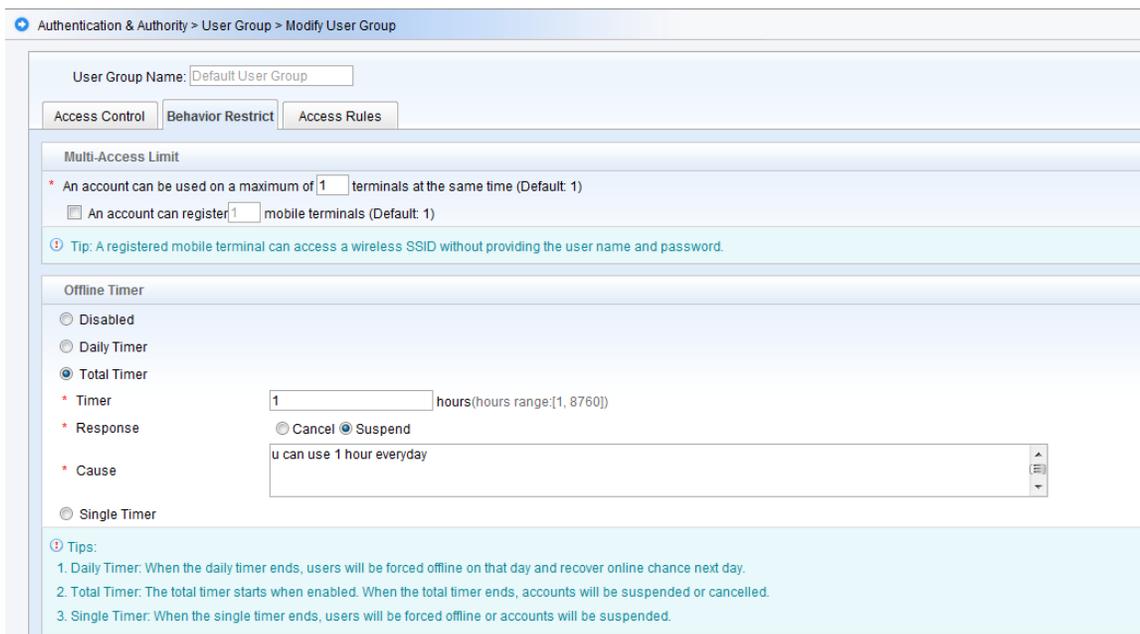
## Total Timer

Choose **Authentication & Authority > User Group**, and configure the total timer, which specifies the maximum accumulated online duration (**X** hours) of a user in a specified user group in total. **X** is a positive integer. The default value is 168, and the value ranges from 1 to 8,760. A scheduled task is automatically started to test at the interval of one minute whether the accumulated online duration of any online user exceeds the limit. If yes, the system forces the user offline, and records the related information in the system log.

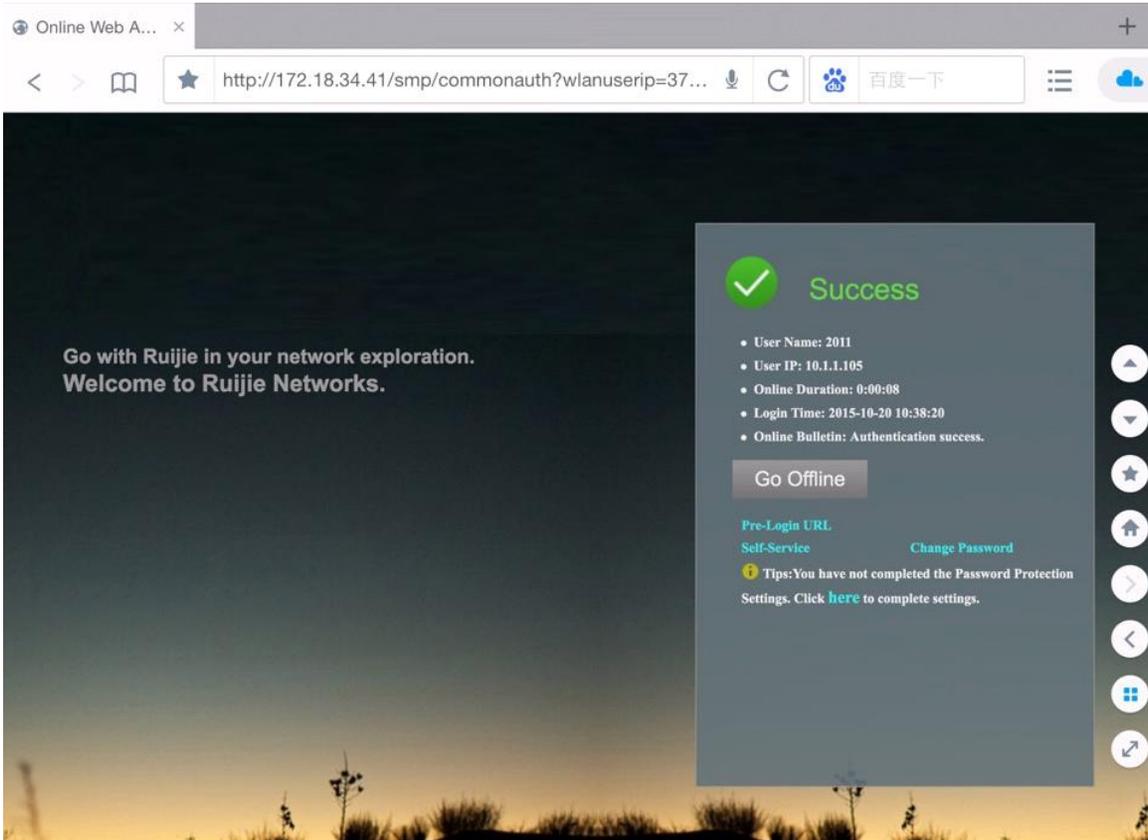
- 1) Choose **Authentication & Authority > User Group**, and click **Modify**.



- 2) Choose **Total Timer**, set **Timer** to 1 hour, and click **Modify** at the bottom of the page to save the changes.



- 3) Log in to RG-SMP as a user in the default user group. After the login succeeds, choose **Authentication & Authority > Online User** to check the online duration of the user.



4) If the accumulated online duration of the user exceeds one hour, the user will be forced offline and the user account is suspended. If the following two logs are displayed, it indicates that settings of the total timer have taken effect.

Log Audit > Network Access Logs > Query Logs

User Name:  User IP:  Offline Cause: All

Login Time: 2015-10-20 0:0:0 Logout Time: 2015-10-20 23:59:59 [Query](#) [Reset](#) [Advanced Search](#)

[Delete](#) [Export Query Results](#) [Delete All](#) [Network Traffic and Online Duration Report](#)

Totally 4 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

All None	User Name	User IP	Full Name	NAS IP	Login Time	Logout Time	Offline Cause	Operation
<input type="checkbox"/>	2011	10.1.1.118	2011	10.1.1.28	2015-10-20 11:16:36	2015-10-20 11:38:00	The offline timer ends!	<a href="#">View</a>

Log Audit > Operation Logs > Query Logs

Operator:  Log Content:  Record Time: 2015-10-20 - 2015-10-20 [Query](#) [Reset](#)

[Delete](#) [Delete All](#)

Totally 13 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

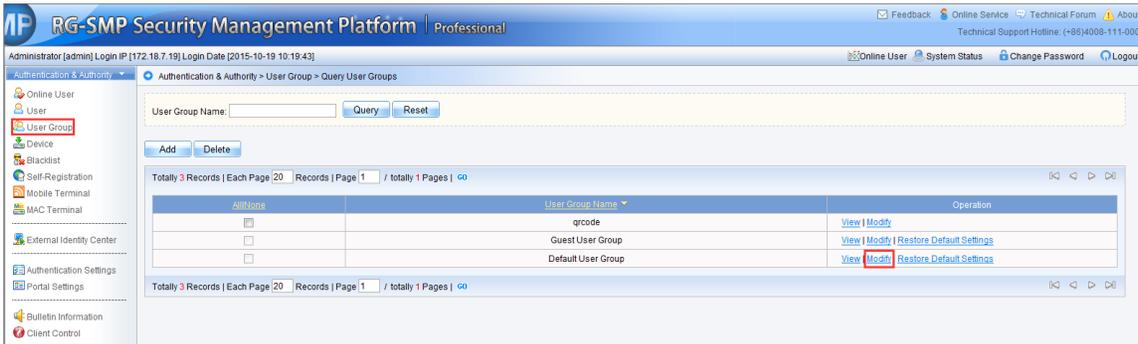
All None	Operator	Record Time	Log Content
<input type="checkbox"/>	system	2015-10-20 11:38:00	The total offline timer of 1 hour for User(2011, 10.1.1.118)ends with user suspension.
<input type="checkbox"/>	system	2015-10-20 11:38:00	The total offline timer of 1 hour for User(2011, 10.1.1.105)ends with user suspension.

## Single Timer

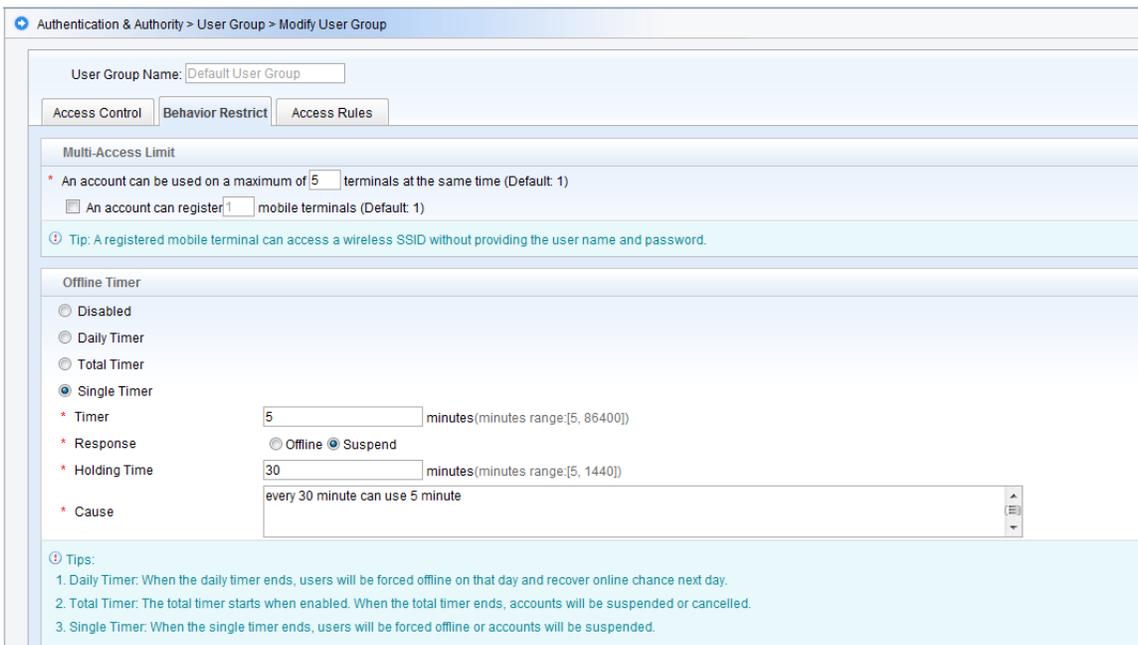
Choose **Authentication & Authority > User Group**, and configure the single timer, which specifies the maximum online duration (**X** minutes) of a user per authentication in a specified user group in one time. **X** is a positive integer. The default

value is 60, and the value ranges from 5 to 86,400. A scheduled task is automatically started to test at the interval of one minute whether the online duration of any online user exceeds the limit. If yes, the system forces the user offline, and records the related information in the system log.

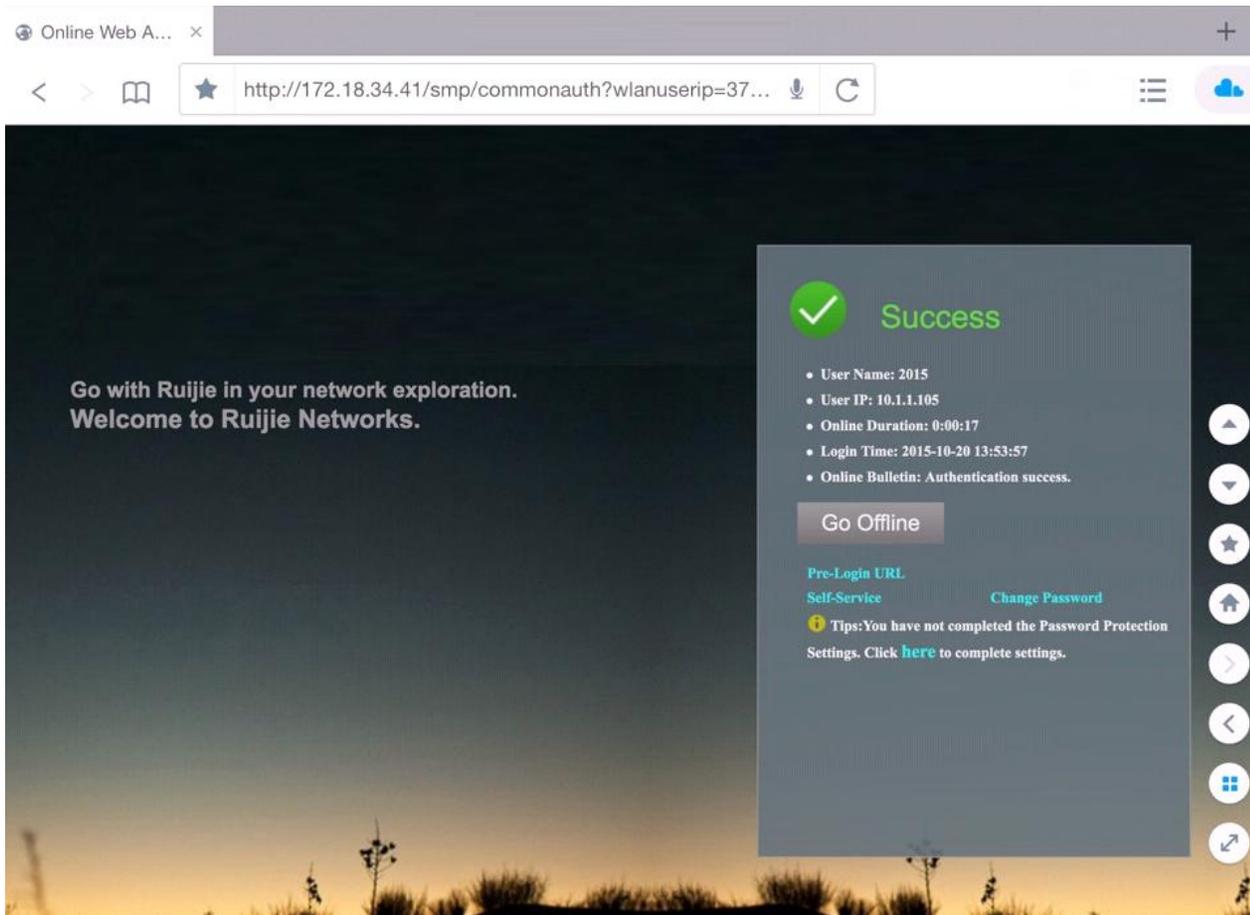
- 1) Choose **Authentication & Authority > User Group**, and click **Modify**.



- 2) Select **Single Timer**, set **Timer** to **5** minutes, and click **Modify** at the bottom of the page to save the changes.



- 3) Log in to RG-SMP as a user in the default user group. After the login succeeds, choose **Authentication & Authority > Online User** to check the online duration of the user.



4) If the one-time online duration of the user exceeds five minutes, the user will be forced offline. Choose **Log Audit > System Logs** to display the system logs. If the following two logs are displayed, it indicates that settings of the single timer have taken effect.

Log Audit > Network Access Logs > Query Logs

User Name:  User IP:  Offline Cause: All

Login Time: 2015-10-20 0:00:00 Logout Time: 2015-10-20 23:59:59 [Query](#) [Reset](#) [Advanced Search](#)

[Delete](#) [Export Query Results](#) [Delete All](#) [Network Traffic and Online Duration Report](#)

Totally 5 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

All None	User Name	User IP	Full Name	NAS IP	Login Time	Logout Time	Offline Cause	Operation
<input type="checkbox"/>	2015	10.1.1.105	2015	10.1.1.28	2015-10-20 13:53:57	2015-10-20 13:59:00	The offline timer ends!	<a href="#">View</a>

---

Log Audit > Operation Logs > Query Logs

Operator:  Log Content:  Record Time: 2015-10-20 - 2015-10-20 [Query](#) [Reset](#)

[Delete](#) [Delete All](#)

Totally 16 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

All None	Operator	Record Time	Log Content
<input type="checkbox"/>	system	2015-10-20 13:59:00	The single offline timer of 5 minutes for User(2015, 10.1.1.105)ends with user suspension of 30minutes.

## External Identity Center

### Authentication Using Generic LDAP Server

- 1) Choose **Authentication & Authority > External Identity Center**.
- 2) Check the **Enable External Identity Center** box, click the **Generic LDAP** tab, and configure correlation with LDAP.

The screenshot shows the 'External Identity Center' configuration page in the RG-SMP Professional interface. The 'Enable External Identity Center' checkbox is checked. The 'Generic LDAP' tab is selected. The configuration includes the following fields:

- LDAP Server IP: 172.18.34.50
- LDAP Server Port: 389 (Default: 389)
- Root DN: dc=maxccr,dc=com (with an 'Auto-Obtain' button)
- Support Anonymous:
- Administrator User Name: cn=Manager,dc=maxccr,dc=com
- Administrator Password: [Redacted]
- Identity Authentication Mode:  Implement Identity Authentication by querying LDAP users
- User ObjectClass: person
- User Name Attribute Name: cn
- User Password Attribute Name: cn

The screenshot shows the 'External Identity Center' configuration page in the RG-SMP Professional interface, focusing on the authentication settings. The configuration includes the following fields and options:

- User Password Attribute Name: cn
- Enable an Encryption and Decryption Plug-in:
- Learn new users during authentication:
- Learn the user group during new user authentication:
- User Group Containing Auto Added Users: new (with a 'Select User Group' button)
- Existing users update the user group automatically:
- User Group Attribute Name: [Empty field]
- User Name Attribute Name: cn
- Address Attribute Name: street
- Telephone No. Attribute Name: telephoneNumber
- Mobile No. Attribute Name: telephoneNumber
- Post Code Attribute Name: postalCode
- Email Address Attribute Name: [Empty field]
- Test User Name: test
- Test Password: [Redacted]

Buttons at the bottom: Modify, Reset, Refresh.

- 3) Click **Modify** to save the configuration.

### Correlation with Windows AD Domain

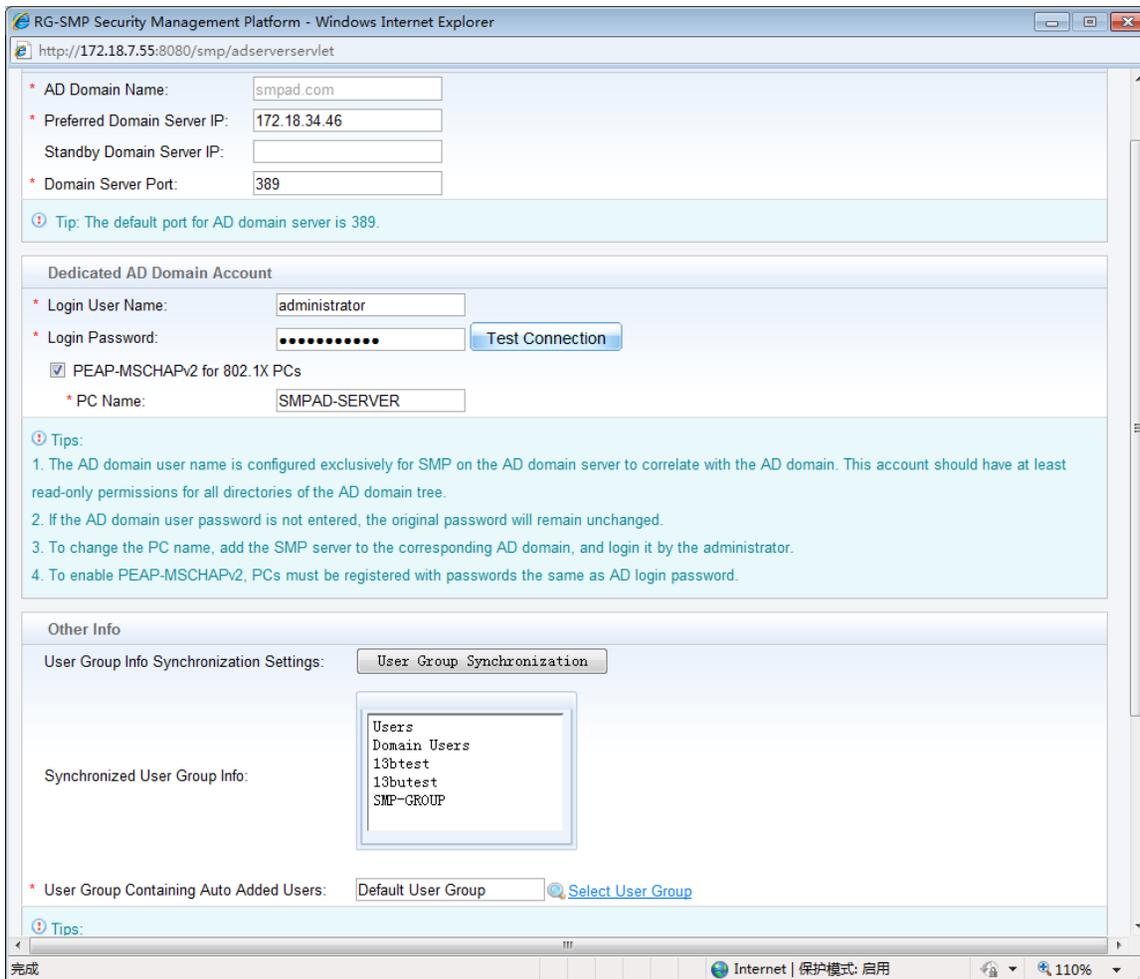
#### Configuration Tips

- Create a common user name by the administrator to correlate the RG-SMP server with the domain server.

- If it is required to support the Windows terminal authentication, apply for a PC username to the domain administrator and configure the password, which is the same as the password of the correlated account.
- Configure the IP address of the AD domain server as the DNS of the SMP server for domain name resolution.

## Configuration Steps

- 1) Choose **Authentication & Authority > External Identity Center > Windows AD Domain**, and click **Windows AD Domain Server** link. In the AD domain server setting page, set the **AD Domain Name**, **Domain Server Port** (default: 389), **Preferred Domain Server IP** and **Standby Domain Server IP** if needed. Currently, only one active and one standby domain servers are supported.



RG-SMP Security Management Platform - Windows Internet Explorer

http://172.18.7.55:8080/smp/adserverervlet

\* AD Domain Name:

\* Preferred Domain Server IP:

Standby Domain Server IP:

\* Domain Server Port:

Tip: The default port for AD domain server is 389.

Dedicated AD Domain Account

\* Login User Name:

\* Login Password:  [Test Connection](#)

PEAP-MSCHAPv2 for 802.1X PCs

\* PC Name:

Tips:

- The AD domain user name is configured exclusively for SMP on the AD domain server to correlate with the AD domain. This account should have at least read-only permissions for all directories of the AD domain tree.
- If the AD domain user password is not entered, the original password will remain unchanged.
- To change the PC name, add the SMP server to the corresponding AD domain, and login it by the administrator.
- To enable PEAP-MSCHAPv2, PCs must be registered with passwords the same as AD login password.

Other Info

User Group Info Synchronization Settings: [User Group Synchronization](#)

Synchronized User Group Info:

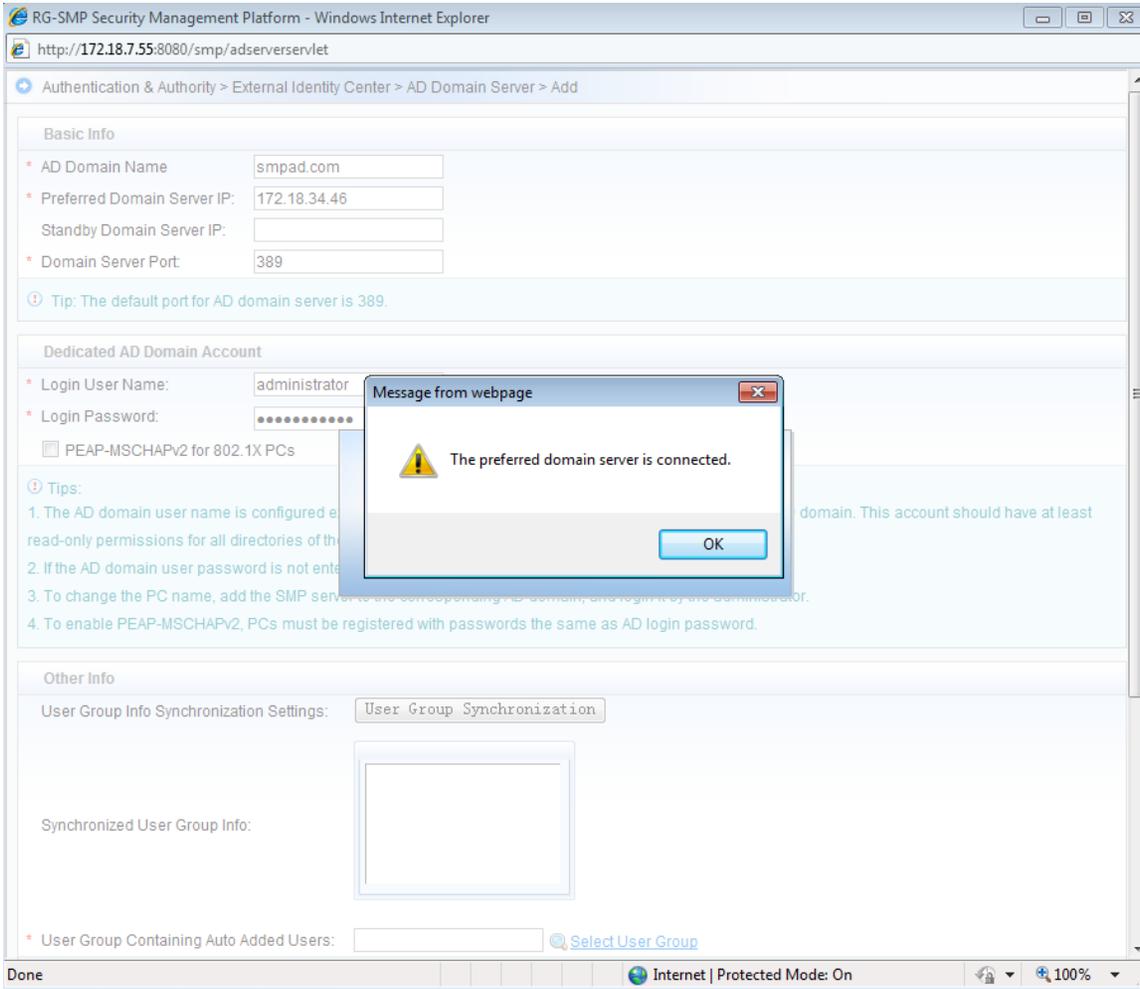
```

Users
Domain Users
13btest
13butest
SMP-GROUP
  
```

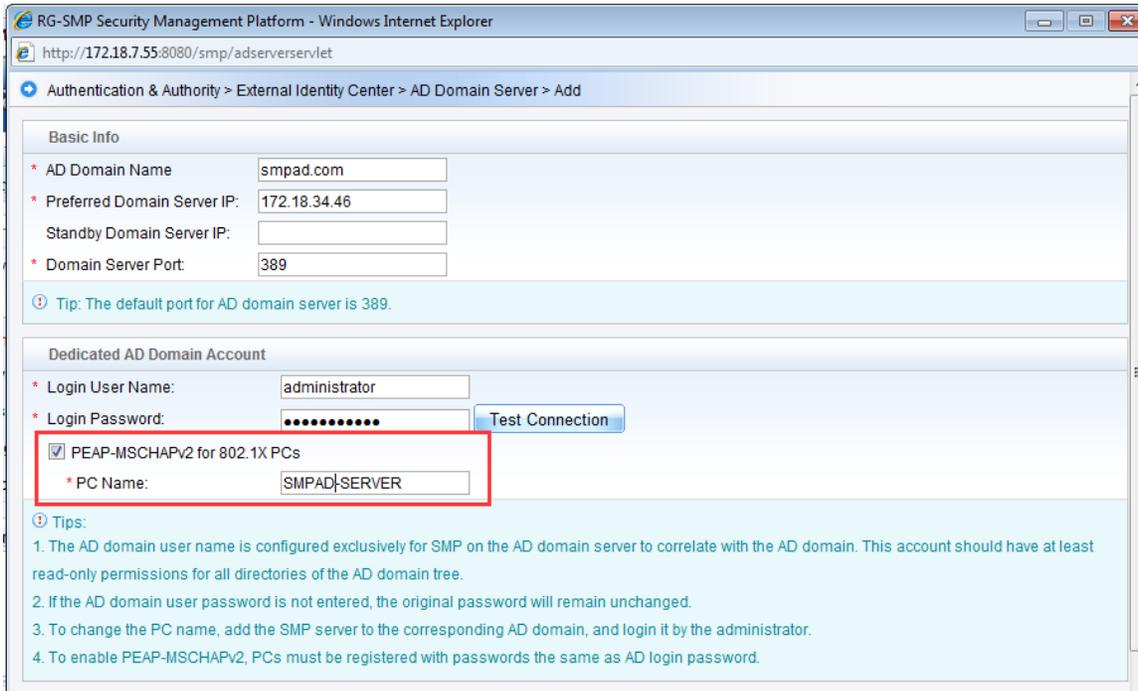
\* User Group Containing Auto Added Users:  [Select User Group](#)

Tip:

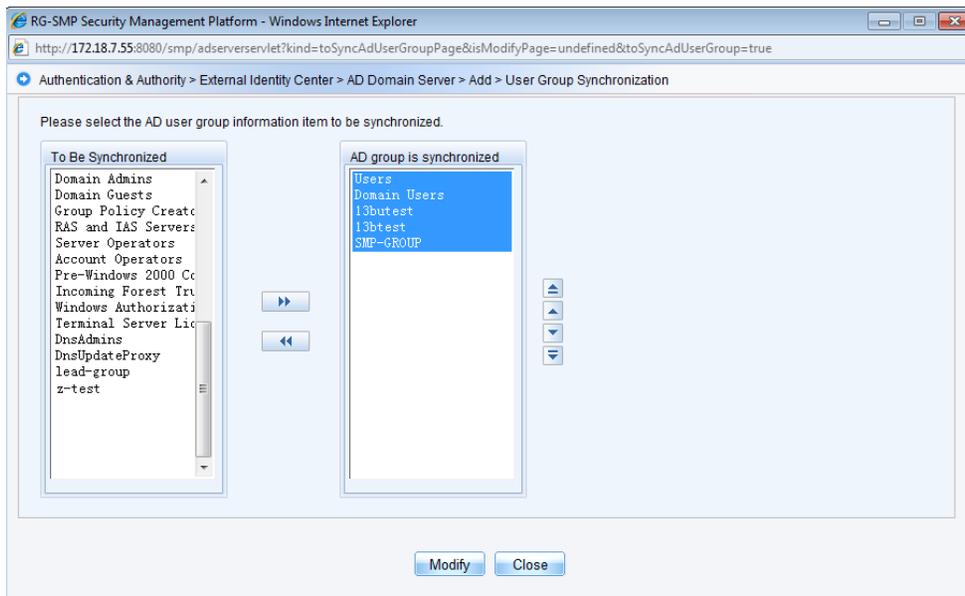
- 2) Enter the **Login User Name** and **Login User Password** under **Dedicated AD Domain Account** in the page. Click **Test Connection** to check whether the correlation user account is available.

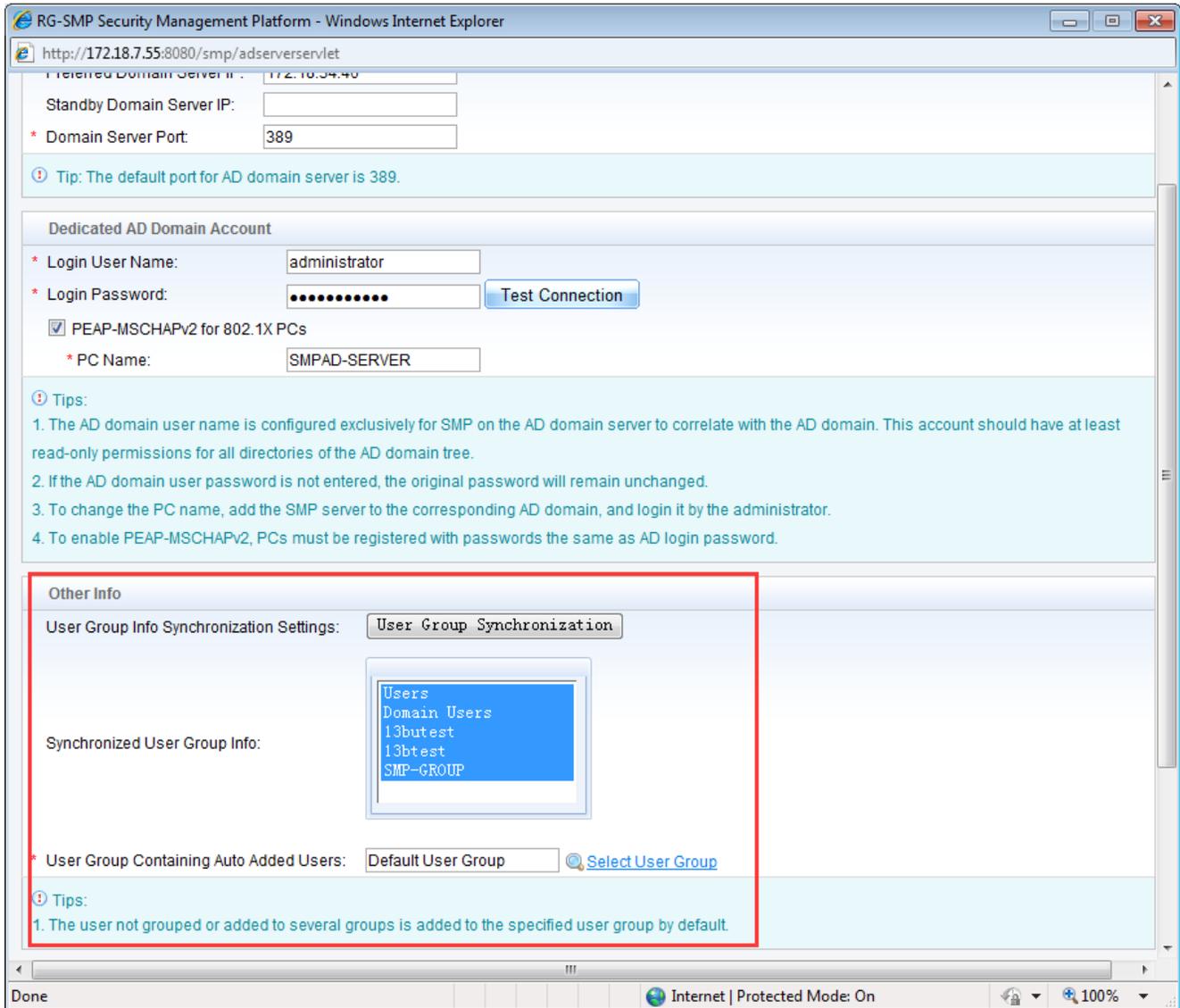


3) Check the **PEAP-MSCHAPv2 for 802.1X PCs** box if it is required to support Windows terminal authentication. Enter the applied PC name.

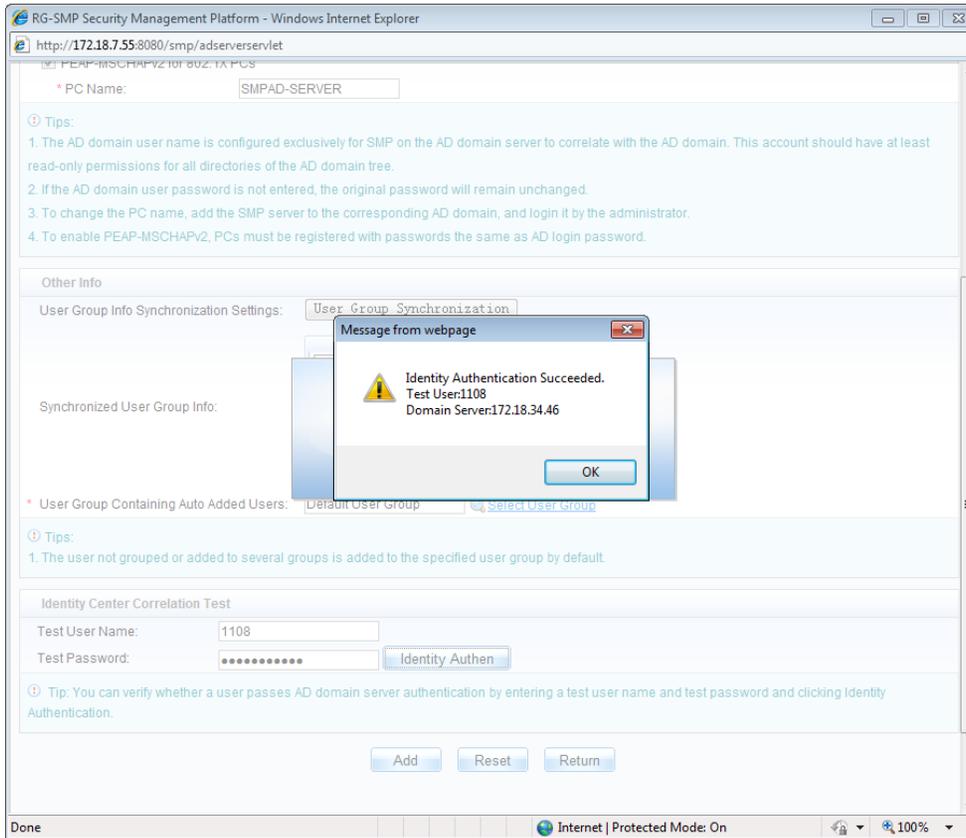


- 4) Configure the mapping relationship between AD domains and RG-SMP user groups, and set **User Group Containing Auto Added Users to Default User Group**.





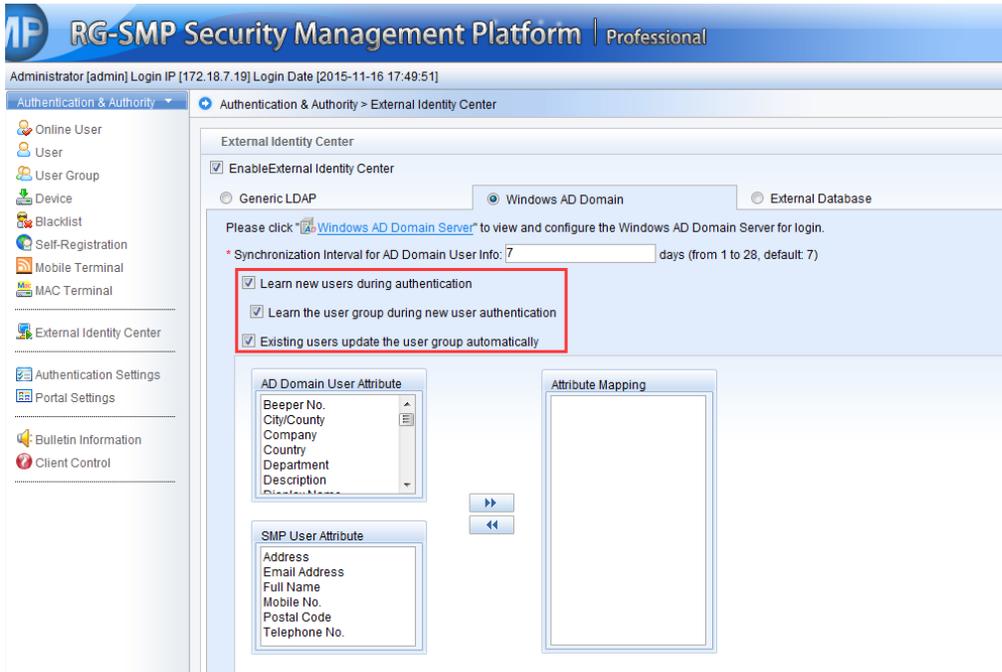
- 5) Enter the **Test User Name** and **Test Password**, click **Identify Authen** to conduct the identity center correlation test, and click **Add** to save the settings.



6) Configure whether to learn user information or user group information as follows:

- i. If the **Learn new users during authentication** box is checked, the AD user information is learned and updated to the local SMP when the AD domain user is being authenticated. If this box is not checked, the AD domain user information must be imported to the SMP in advance; otherwise, this AD domain user cannot be authenticated.
- ii. If the **Learn the new user group during new user authentication** box is checked, the user group information is learned and updated to RG-SMP when the AD domain user is being authenticated, and the learned information is synchronized based on the configuration in step 4. If this box is not checked, the default user group information is learned after all AD domain users are authenticated.
- iii. If the **Existing users update the user group automatically** box is checked, the user group information is updated to RG-SMP during each AD domain user authentication. If this box is not checked, the user group information learned during the first authentication is used.
- iv. You can configure the mapping relationship between AD domain user attributes and SMP user attributes. Then, the user attributes are automatically learned and updated to the user information created on the SMP during the AD domain user authentication.

The default settings are recommended.



## Correlation with External Database

- 1) Choose **Authentication & Authority > External Identity Center**.
- 2) Check the **Enable External Identity Center** check box and click the **External Database** tab.

External Identity Center

Enable External Identity Center

Generic LDAP
  Windows AD Domain
  External Database
  Remote Radius Server
  Webservice

\* Database Type:  (Support SQL Server 2008 R2)

\* Database Server IP Address:

\* Database Server Port:  (Default: 1433)

\* Administrator Account:

\* Administrator Password:

\* Database Name:

\* Database Character Set:  UTF-8  GBK

---

\* In Table:  Column:  is user name, Column:  is password.

Learn new users during authentication

Learn the user group during new user authentication

\* User Group Containing Auto Added Users:

If you don't configure mapping among the user group, table name and column name, all users newly learned will be added to this user group.

Existing users update the user group automatically

Enable an Encryption and Decryption Plug-in:

If the user password of the database server is encrypted, you can enable and configure an encryption and decryption plug-in by clicking [Import Password Plug-in](#) to import a password plug-in

---

You can configure mapping among the user group, table name and column name to enable the system to learn user information from the database during user authentication.

User	Table Name	Column Name	Association	Operation
<input type="text" value="User Group"/>	<input type="text"/>	<input type="text"/>	Use table's <input type="text"/>	<input type="button" value="Add"/>
			to associate the tableUserinfo's <input type="text"/>	
Mobile No.	Userinfo	Mobile phone	Self Reference	<input type="button" value="Delete"/>

---

Test User Name:

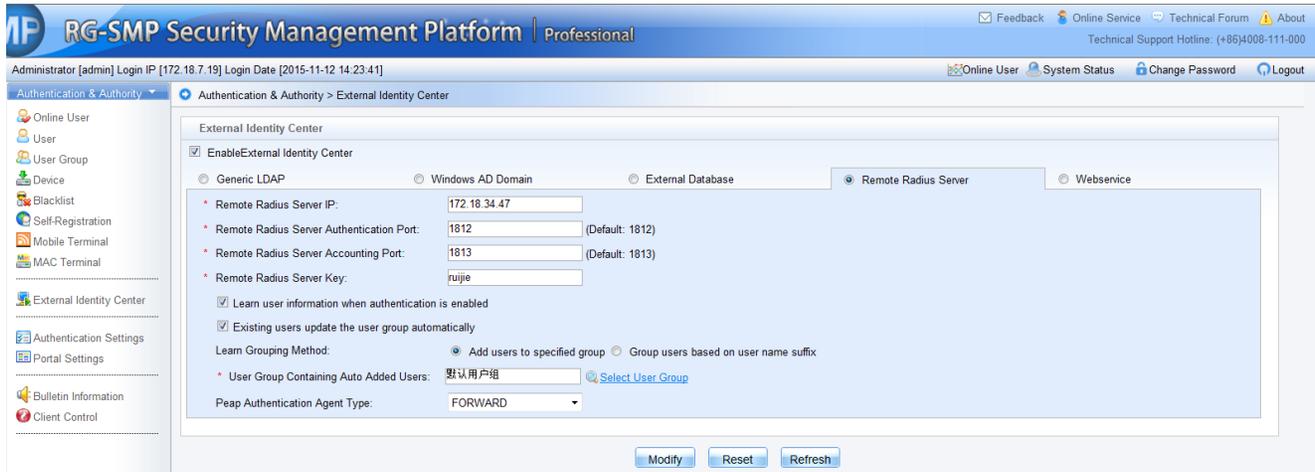
Test Password:

You can verify whether a user passes database server authentication by entering a test user name and test password and clicking Identity Authentication.

3) Configure correlation with the external database and click **Modify** to save the configuration.

## Authentication Using Remote RADIUS Server

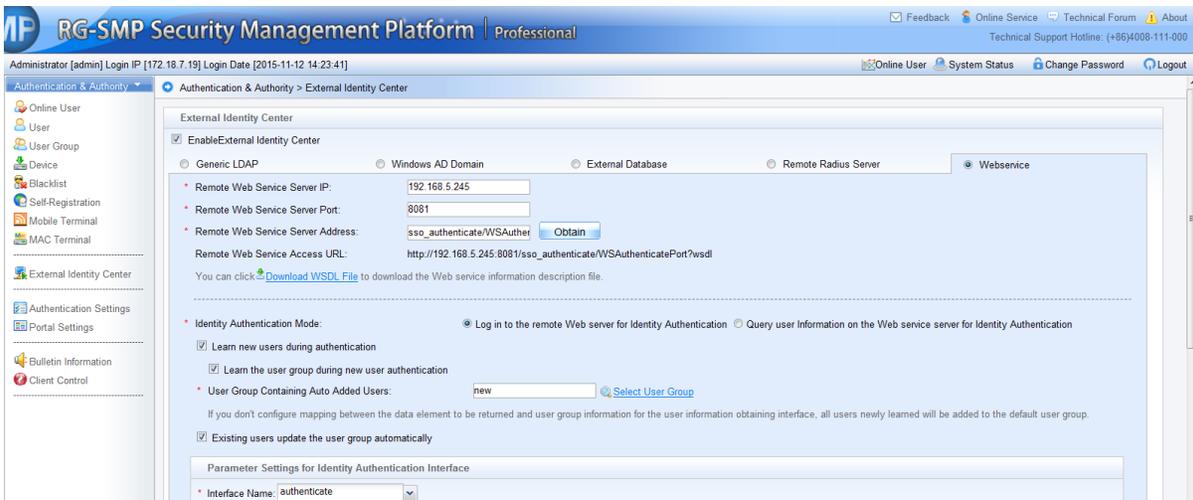
- 1) Choose **Authentication & Authority > External Identity Center**.
- 2) Check the **Enable External Identity Center** check box and click the **Remote Radius Server** tab.

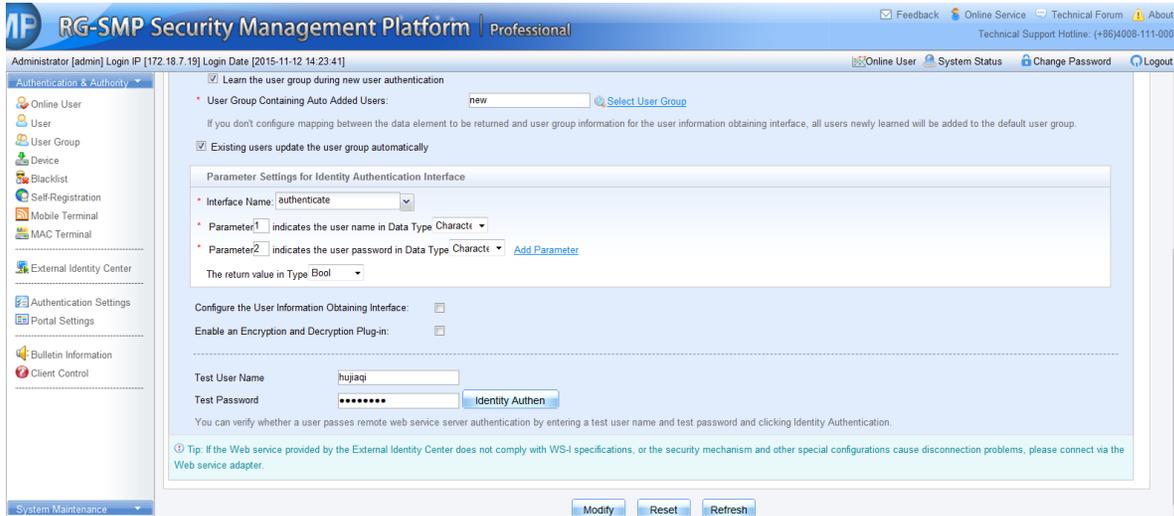


- 3) Configure correlation with remote RADIUS and click **Modify** to save the configuration.

## Correlation with Remote Web Service

- 1) Choose **Authentication & Authority > External Identity Center**.
- 2) Check the **Enable External Identity Center** check box and click the **Webservice** tab.





- 3) Configure correlation with the remote web service and click **Modify** to save the configuration.

## User Self-Registration

### User Self-Registration

#### Function Description

This section describes how to configure the user self-registration function. User self-registration methods include Email, SMS, Guest SMS Self-Registration, and ThirdParty Correlation Registration.

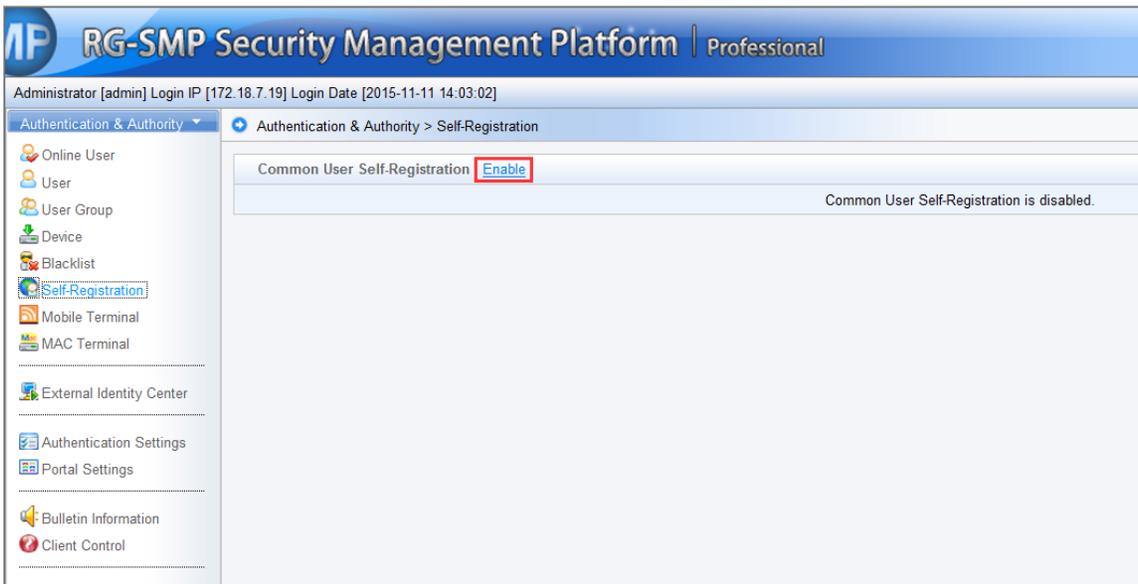
#### Configuration Tips

- To use the Email self-registration, enable the Email service first.
- To use the SMS self-registration, enable the SMS service first.

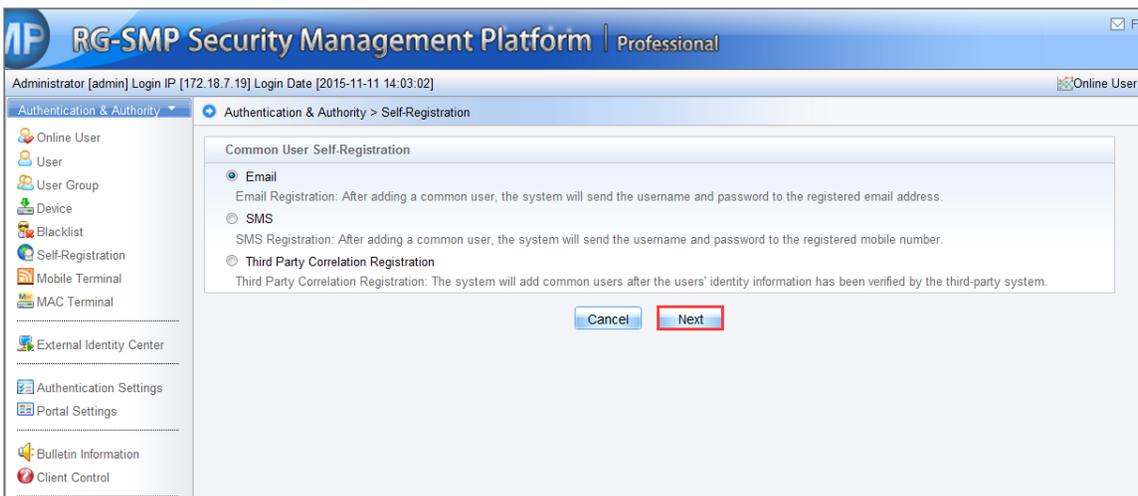
#### Configuration Steps

### Email Self-Registration

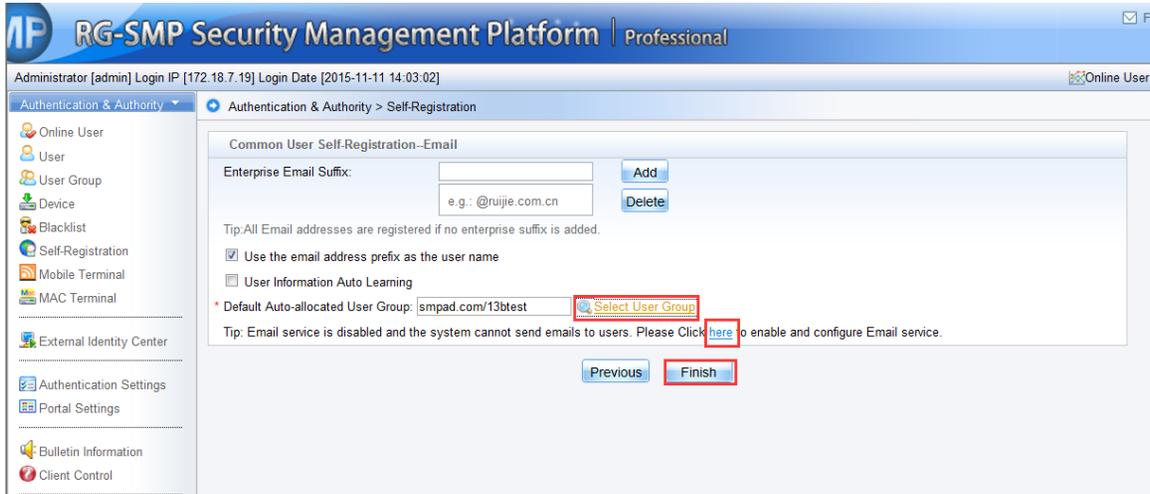
- 1) Choose **Authentication & Authority > Self-Registration**, and click **Enable** to enter the user self-registration configuration page.



2) Select **Email** as the self-registration mode, and click **Next**.

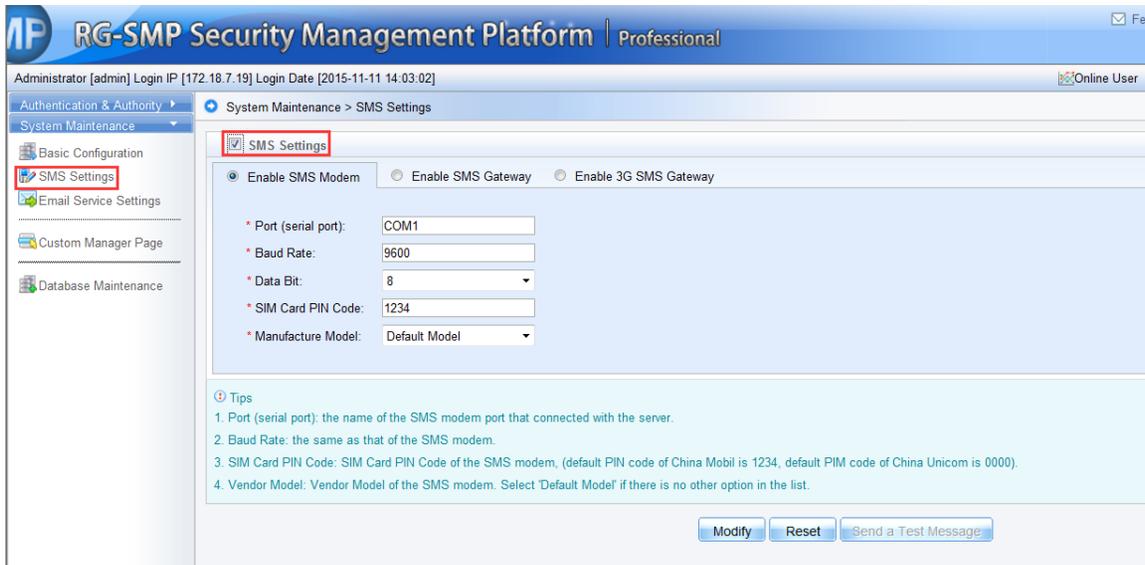


3) Select the default user group that is automatically allocated for self-registered users. After configuration is completed, click **Finish**. If the Email service is not enabled, click [here](#) to configure the Email service.

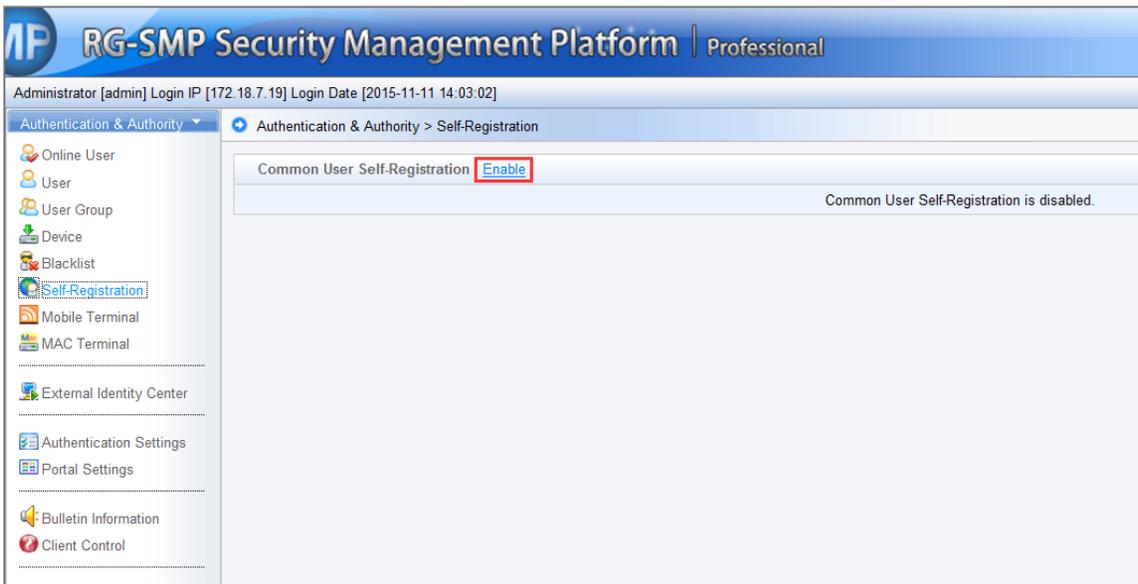


## SMS Self-Registration

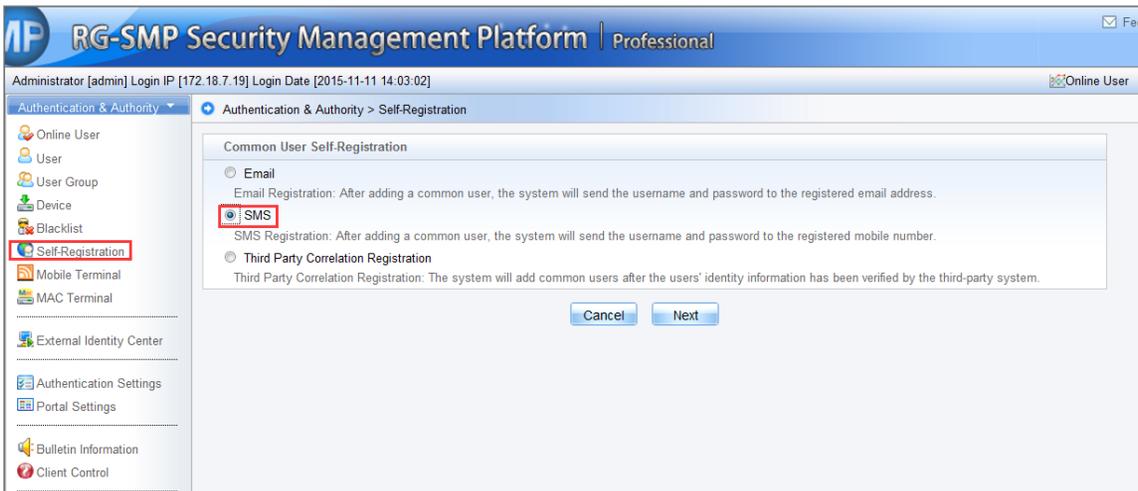
- 1) Choose **System Maintenance > SMS Settings**, check the **SMS Settings** box, configure parameters as shown in the following figure, and click **Modify** to save the settings. Before that, you can click **Send a Test Message** to verify the configuration.



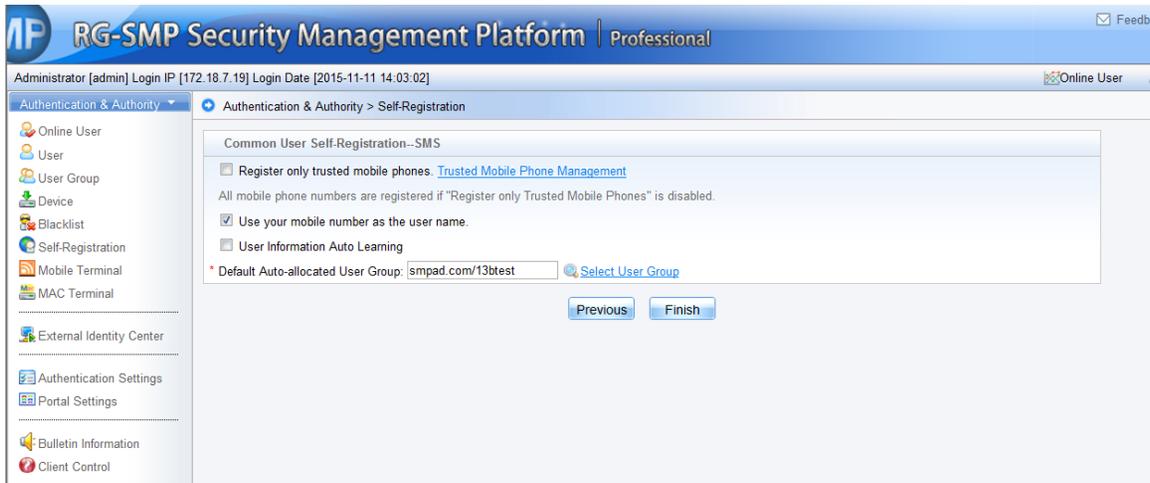
- 2) Choose **Authentication & Authority > Self-Registration**, click **Enable** to enable the SMS self-registration for common users and enter the configuration page.



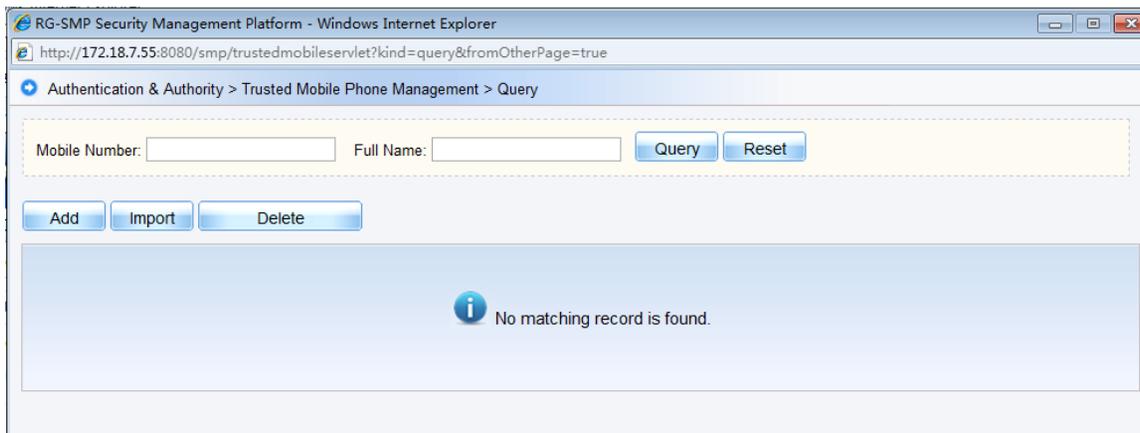
- 3) Select **SMS** as the self-registration mode, and click **Next**.



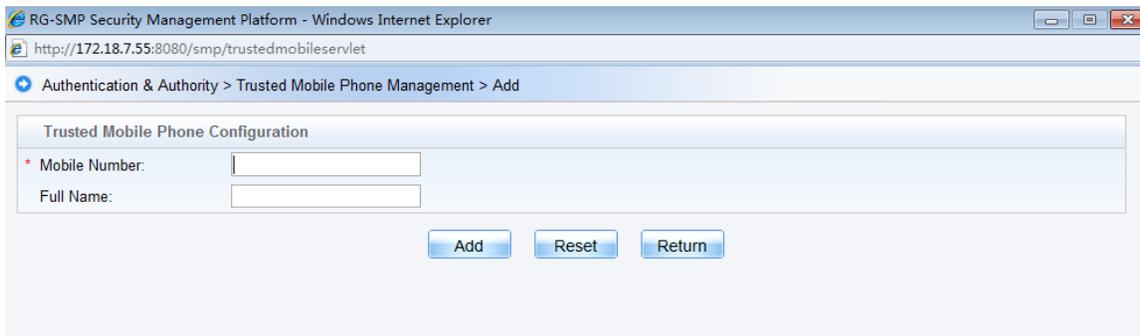
- 4) Click the **Select User Group** link in the **Default Auto-allocated User Group** field to choose a default group for SMS registered users, and click **Finish** to finish the settings.



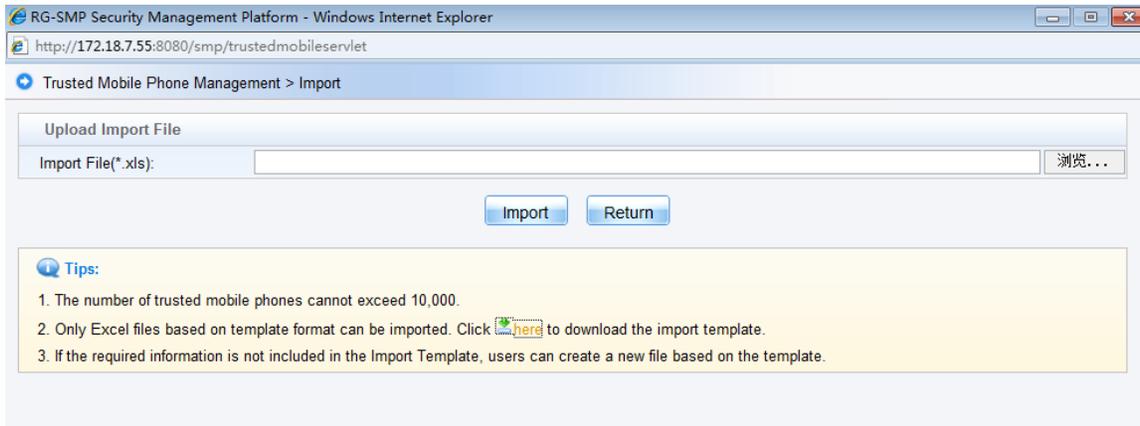
5) If only the specified mobile numbers can get registered, check the **Register only trusted phone phones** box. You can manage the trusted numbers by clicking **Trusted Mobile Phone Management**. This configuration help prevent unauthorized mobile phones from registration and access. Click **Finish** to finish the settings.



6) Click **Add** on **Trusted Mobile Phone Management** page to add a trusted mobile number.

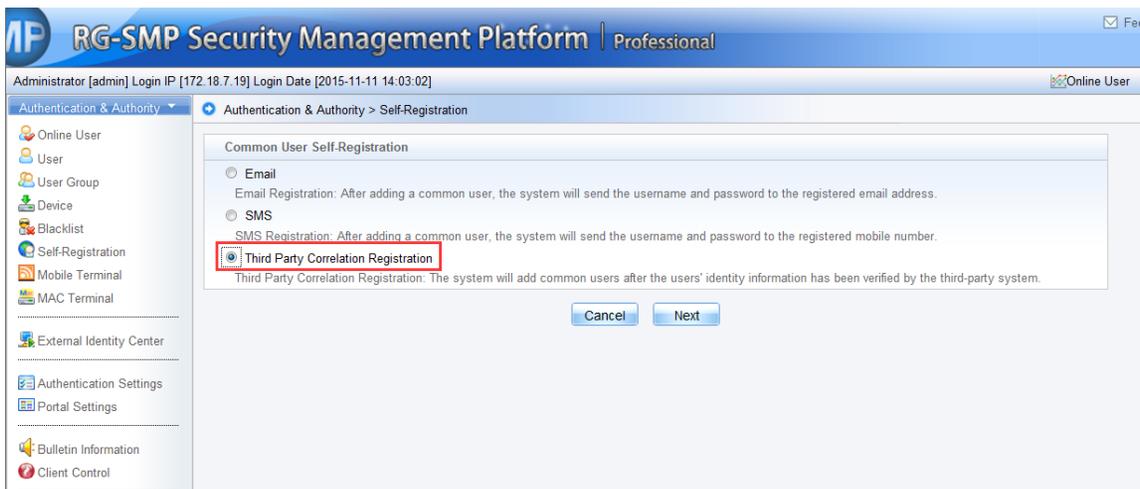


7) Click **Import** on **Trusted Mobile Phone Management** page to import multiple phone numbers as trusted at a time. You can click [here](#) in **Tips** on **Upload Import File** page to download the import template.



## Third Party Correlation Registration

- 1) Choose **Authentication & Authority > Self-Registration**, and click **Enable** to enter the user self-registration page. Select **Third Party Correlation Registration** as the self-registration mode, and click **Next**.



- 2) Fill in the third-party database information, and click **Next**.

Administrator [admin] Login IP [172.18.7.19] Login Date [2015-11-11 14:03:02]

Authentication & Authority > Self-Registration

Common User Self-Registration--Third Party Correlation Registration

SQL Server  
 MySQL  
 PostgreSQL  
 Oracle  
 DB2

\* Third Party Database Types:

\* Database Server IP Address:

\* Database Server Port:

\* Administrator Account:

\* Administrator Password:

\* Database Name:

\* User Information List Name:

3) Add the mapping between the user information and column name in the database, and click **Next**.

Administrator [admin] Login IP [172.18.7.19] Login Date [2015-11-11 14:03:02]

Authentication & Authority > Self-Registration

Common User Self-Registration--User Information Validation

Verification Criteria Configuration

User Information:

Column Name:

User Information	Column Name	Operation
User Name	USER_ID	<a href="#">Delete</a>

4) Configure the **User Information Learning**, and click **Finish** to complete the settings.



## Guest Registration

### Function Description

This section describes how a common guest gets registered.

### Configuration Tips

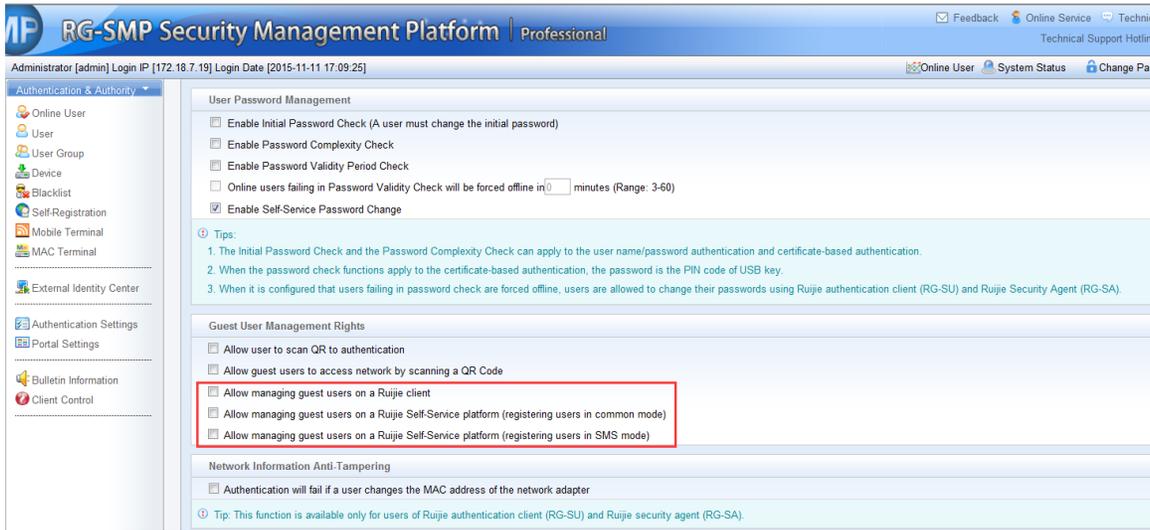
To register a guest using the SMS, enable the SMS service first.

### Configuration Steps

- 1) Choose **Authentication & Authority > User Group**, select a user group and click **Modify** in the **Operation** column.



- 2) On the Modify/Add User Group page, click the Behavior Restrict tab, and select the Guest User Management Rights.



## User Information Self-Maintenance

### Function Description

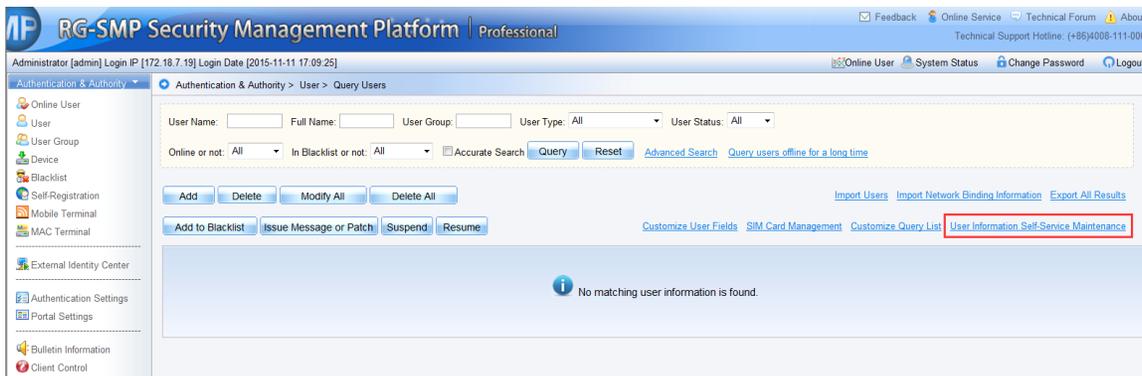
This section describes how to self-maintain the user information on the self-service platform.

### Configuration Tips

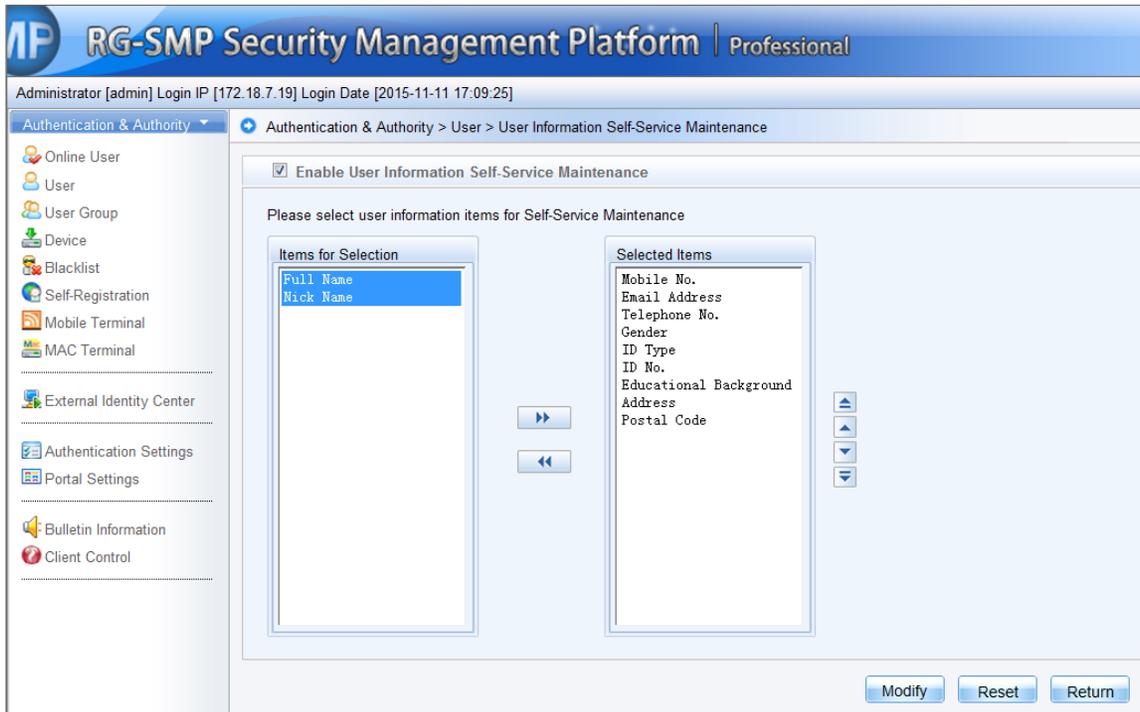
N/A

### Configuration Steps

- 1) Choose **Authentication & Authority > User**. On the user management page, click **User Information Self-Service Maintenance**.



- 2) On the user information self-service maintenance page, click the right-arrow button in the middle to move items from **Items for Selection** to **Selected Items**, and click **Modify** to save the settings.



- Log in to the self-service platform. On the **My Information** page, you can modify by yourself the user information items configured in step 2.

## Mobile Terminal Management

### Function Description

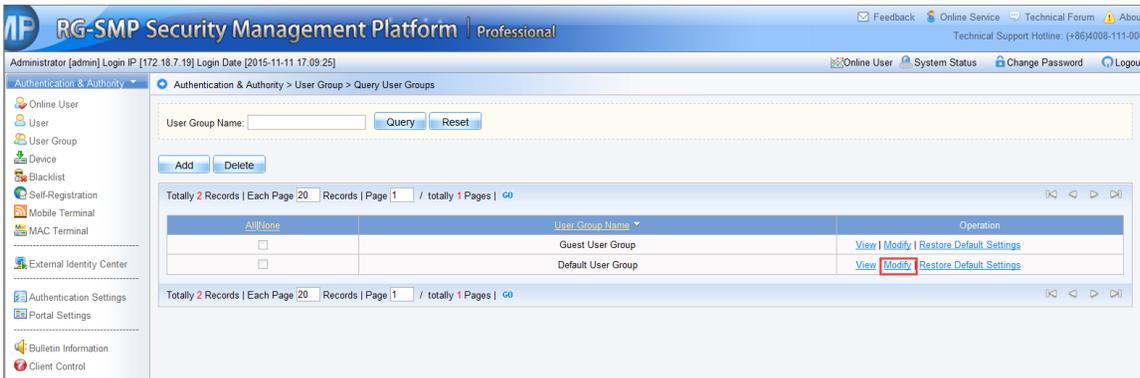
This section describes how to manage mobile terminals on the self-service platform.

### Configuration Tips

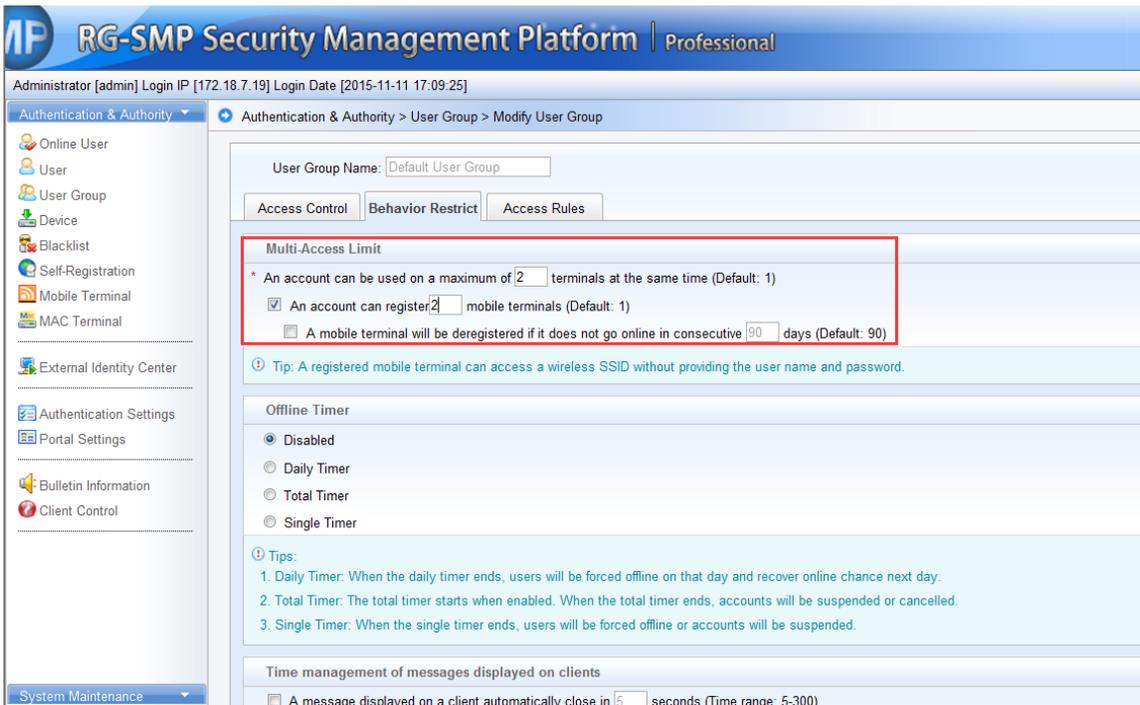
N/A

### Configuration Steps

- Choose **Authentication & Authority > User Group**, select a user group and click **Modify** in the Operation column.



2) On the **Modify/Add User Group** page, click the **Behavior Restrict** tab, and check the **An account can register X mobile terminals** box under **Multi-Access Limit**.



3) Log in to the self-service platform. On the **My Mobile Terminal** page, users can manage mobile terminals, for example, deleting mobile terminals, and viewing network access history and authentication failure logs.



## Common Functions

### Authentication & Authority

#### User and Security Management

#### Function Description

This section describes how to add users and manage security configurations on RG-SMP.

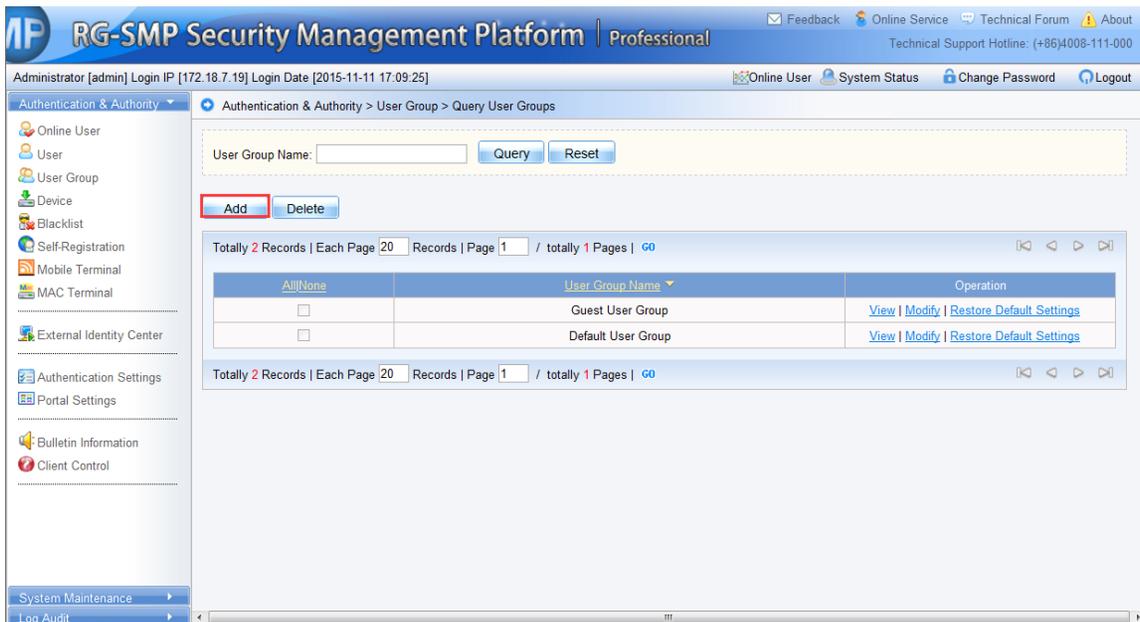
#### Configuration Tips

N/A

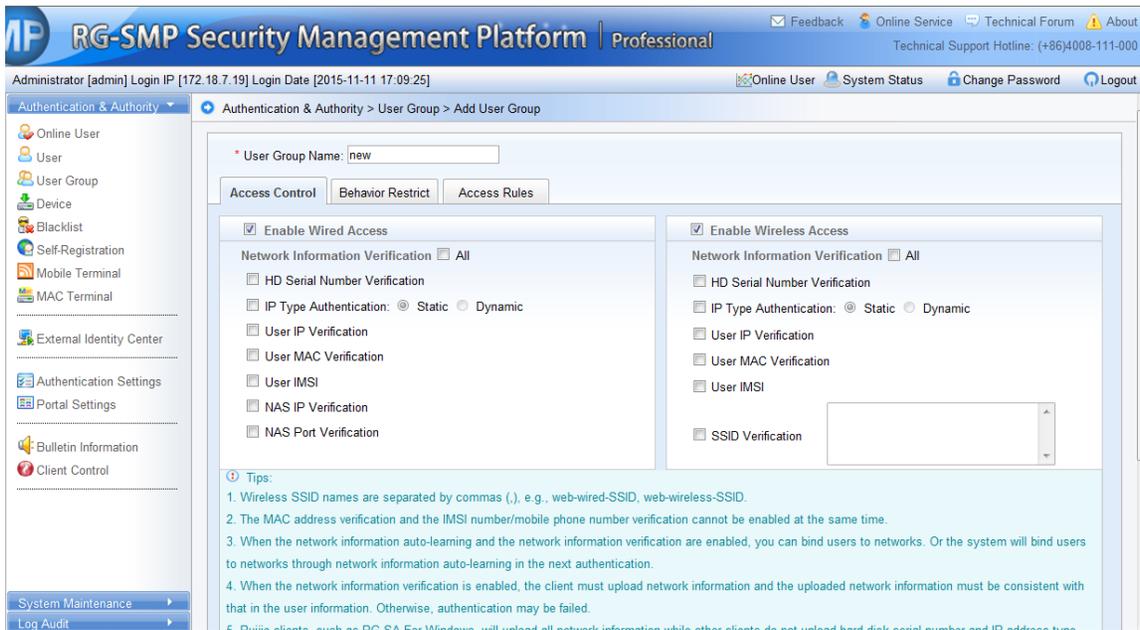
#### Configuration Steps

### Adding a User Group

- 1) Choose **Authentication & Authority > User Group** to enter the user group management page.

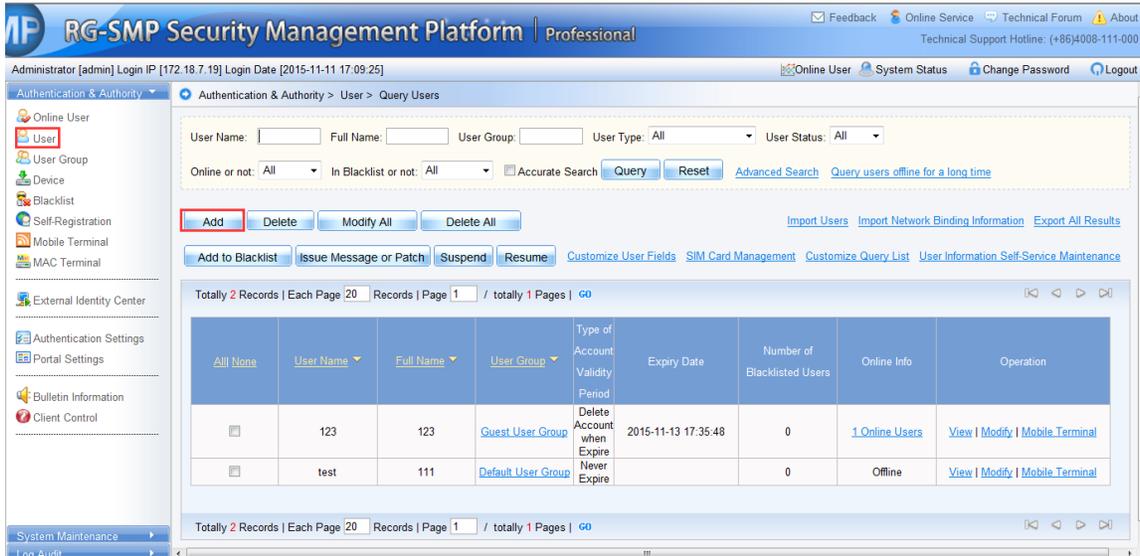


- 2) Click Add to enter the user group adding page. Add the User Group Name, configure the user group policies, and click Add.

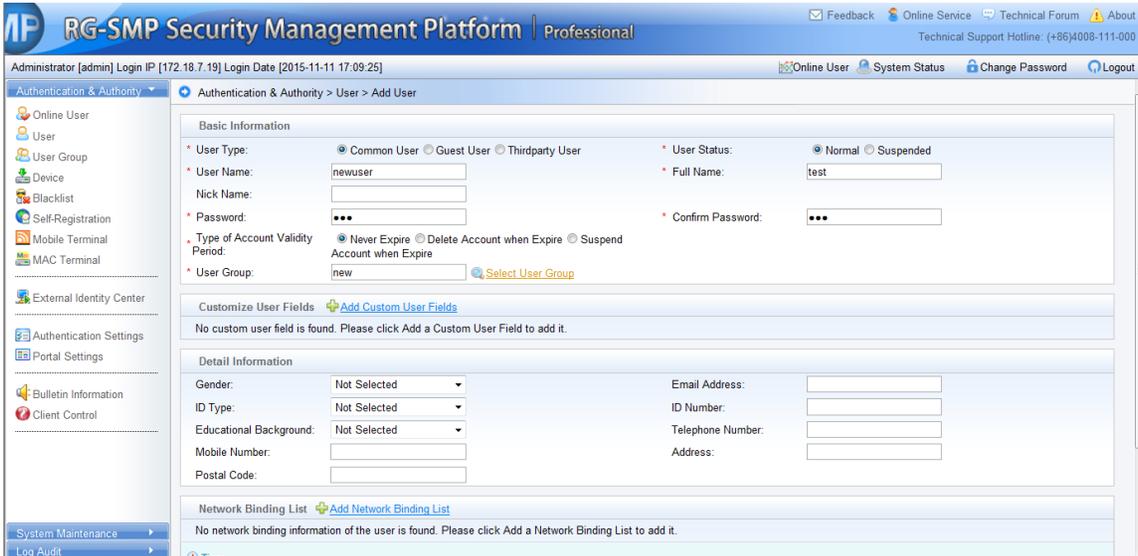


## Adding a User

- 1) Choose **Authentication & Authority > User** to enter the user management page.

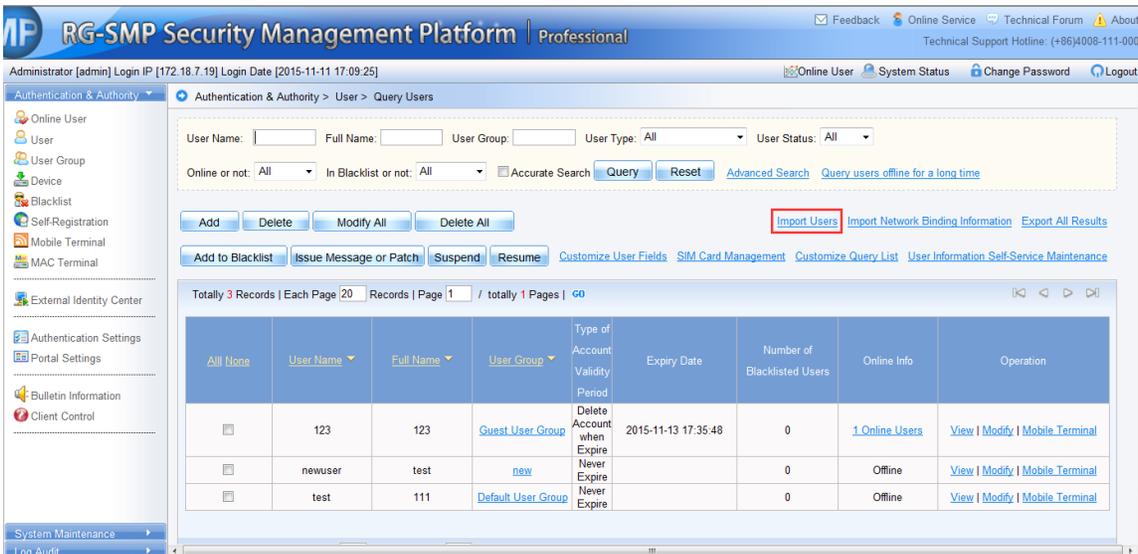


- 2) Click **Add** to enter the **Add User** page.

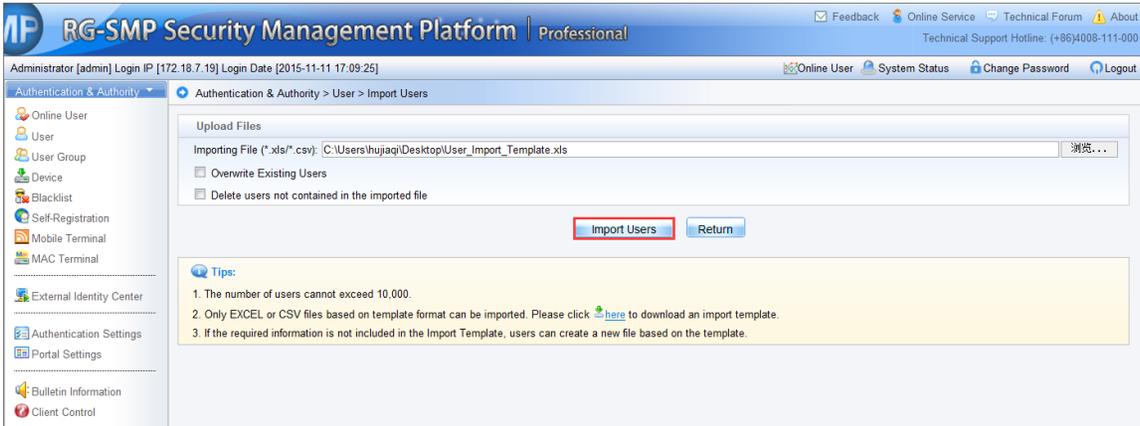


## Importing Users

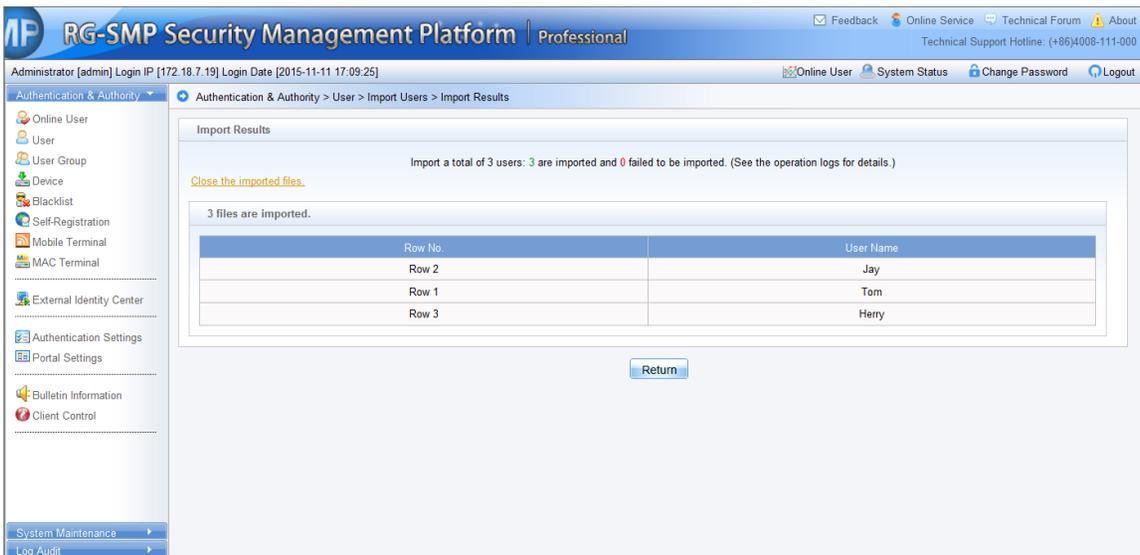
- 1) Choose **Authentication & Authority > User** to enter the user management page. Click **Import Users**.



- 2) On the user import page, download the template file, which is a \*.xls or \*.csv file. You can import user information that is bound with network information, and configure the import options, including **Overwrite Existing Users** and **Delete users not contained in the imported file**.



3) After users are imported, check the import results as follows:



## Modifying Users

1) Choose **Authentication & Authority > User** to enter the user management page. Select a user, and click **Modify All**.

The screenshot shows the 'Query Users' page in the RG-SMP Security Management Platform Professional. The breadcrumb navigation is 'Authentication & Authority > User > Query Users'. The page includes search filters for User Name, Full Name, User Group, User Type, and User Status. Below the filters are buttons for 'Add', 'Delete', 'Modify All' (highlighted with a red box), and 'Delete All'. There are also buttons for 'Add to Blacklist', 'Issue Message or Patch', 'Suspend', and 'Resume'. A table displays a list of users with columns for 'All None', 'User Name', 'Full Name', 'User Group', 'Type of Account Validity Period', 'Expiry Date', 'Number of Blacklisted Users', 'Online Info', and 'Operation'. The table contains four rows of user data.

All None	User Name	Full Name	User Group	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	Operation
<input type="checkbox"/>	123	123	Guest User Group	Delete Account when Expire	2015-11-13 17:35:48	0	1 Online Users	View   Modify   Mobile Terminal
<input type="checkbox"/>	Herry	Herry	Default User Group	Never Expire		0	Offline	View   Modify   Mobile Terminal
<input type="checkbox"/>	Jay	Jay	Default User Group	Never Expire		0	Offline	View   Modify   Mobile Terminal
<input type="checkbox"/>	newuser	test	new	Never Expire		0	Offline	View   Modify   Mobile Terminal

- 2) On the page for modifying users in batch, you can configure the **User Group Information** and **User Type Change**, and **Network Verification Information** clearing, as shown in the following figure:

The screenshot shows the 'Modify Users in Batches' page in the RG-SMP Security Management Platform Professional. The breadcrumb navigation is 'Authentication & Authority > User > Modify Users in Batches'. The page includes sections for 'User Group Information' (with a 'User Group' dropdown set to 'No Change'), 'User Type Change' (with radio buttons for 'Not Modify', 'Transfer from a common user to a thirdparty user', and 'Transfer from a thirdparty user to a common user'), and 'Network Verification Information' (with a 'Clear Network Verification Information' checkbox). There are 'Modify in Batch' and 'Return' buttons at the bottom. A 'Tips' section contains two numbered instructions.

**Tips:**

1. If the user group of a user is modified, the user group configuration will take effect on next authentication.
2. The user group of a guest user will not be modified.

## Customizing a Query List

- 1) Choose **Authentication & Authority > User Group**, and click **Customize Query List**.

Authentication & Authority > User > Query Users

User Name:  Full Name:  User Group:  User Type: All User Status: All

Online or not: All In Blacklist or not: All  Accurate Search   [Advanced Search](#) [Query users offline for a long time](#)

[Import Users](#) [Import Network Binding Information](#) [Export All Results](#)

[Customize User Fields](#) [SIM Card Management](#) [Customize Query List](#) [User Information Self-Service Maintenance](#)

Totally 6 Records | Each Page 20 Records | Page 1 / totally 1 Pages | GO

All None	User Name	Full Name	User Group	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	Operation
<input type="checkbox"/>	123	123	Guest User Group	Delete Account when Expire	2015-11-13 17:35:48	0	1 Online Users	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	Herry	Herry	Default User Group	Never Expire		0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	Jay	Jay	Default User Group	Never Expire		0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	newuser	test	new	Never Expire		0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>

2) Select a field (for example, **User Type**) to be displayed in the query list from **Items for Selection**, and click the right-arrow button in the middle to move the selected field to **Selected Items**, and click **Modify**. Click **Return** to return to the user information page. An extra field, **User Type**, is displayed in the queried user information.

Authentication & Authority > User > Custom Display List

Please select the item(s) to be included in the Query List.

**Items for Selection**

- Nick Name
- User Type**
- User Status
- Gender
- Email Address
- ID Type
- ID No.
- Educational Background
- Telephone No.
- Mobile No.
- Address
- Postal Code
- Attack Event Count
- Last Attack Event Time
- Last Login Time
- Account Administrator
- Account Registration Da

**Selected Items**

- User Name
- Full Name
- User Group
- Type of Account Validit
- Expiry Date
- Number of Blacklisted U
- Online Info

## Custom Display List

### Function Description

This section describes how to customize the display list of queried online users.

### Configuration Tips

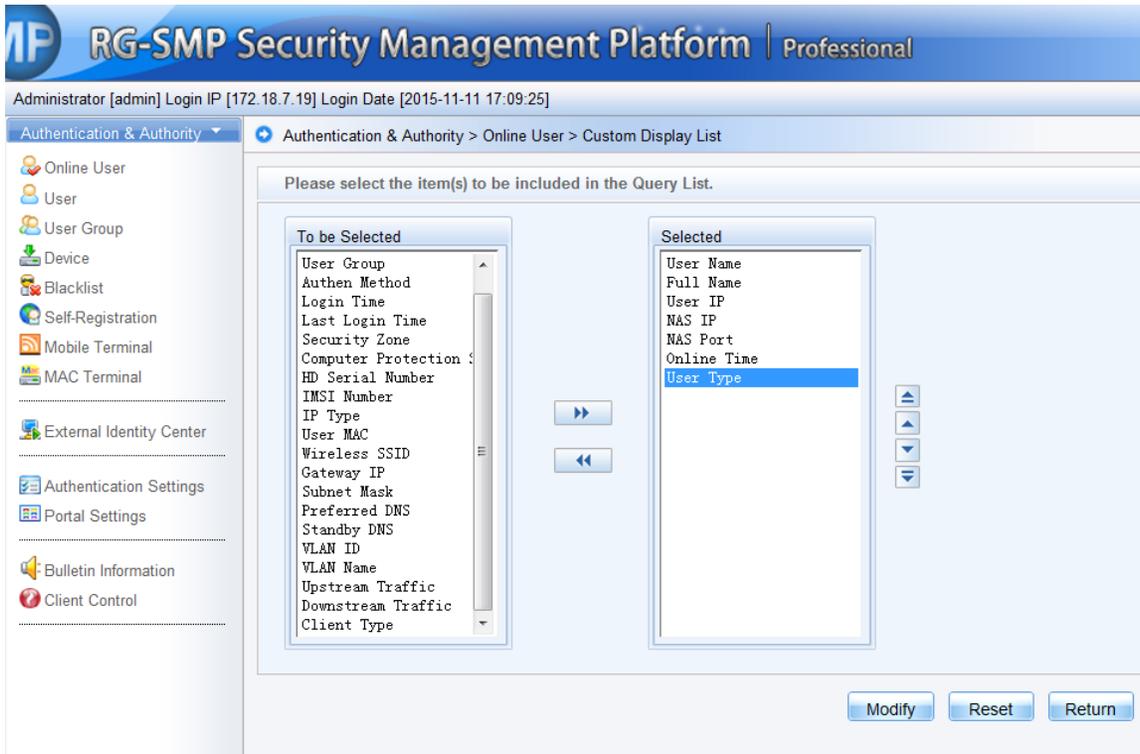
N/A

### Configuration Steps

- 1) Choose **Authentication & Authority > Online User**, and click **Customize Query List**.

The screenshot shows the RG-SMP Security Management Platform Professional interface. The breadcrumb navigation is 'Authentication & Authority > Online User > Query Online Users'. The page contains search filters for User Name, Full Name, User Group, User IP, and NAS IP, along with search buttons (Query, Reset, Advanced Search). Below the filters are action buttons: Clear Residual Users, Force Offline, Reauthenticate, Issue Message or Patch, Add to Blacklist, and a checkbox for 'Send online/offline notifications to a third-party system'. The 'Customize Query List' button is highlighted with a red box. A table below shows one record with columns: All, None, User Name, Full Name, User IP, NAS IP, NAS Port, Online Time, and Operation. The table contains one row with values: 123, 123, 10.1.1.105, 10.1.1.28, 1, 0:19:49, and a View link. A tips section at the bottom provides instructions on reauthentication and clearing residual users.

- 2) Select a field (for example, **User Type**) to be displayed in the query list from **To be Selected**, and click the right-arrow button in the middle to move the selected field to **Selected**, and click **Modify**. Click **Return** to return to the online user information page. An extra field, **User Type**, is displayed in the queried user information.



## Online Users Trend Chart

### Function Description

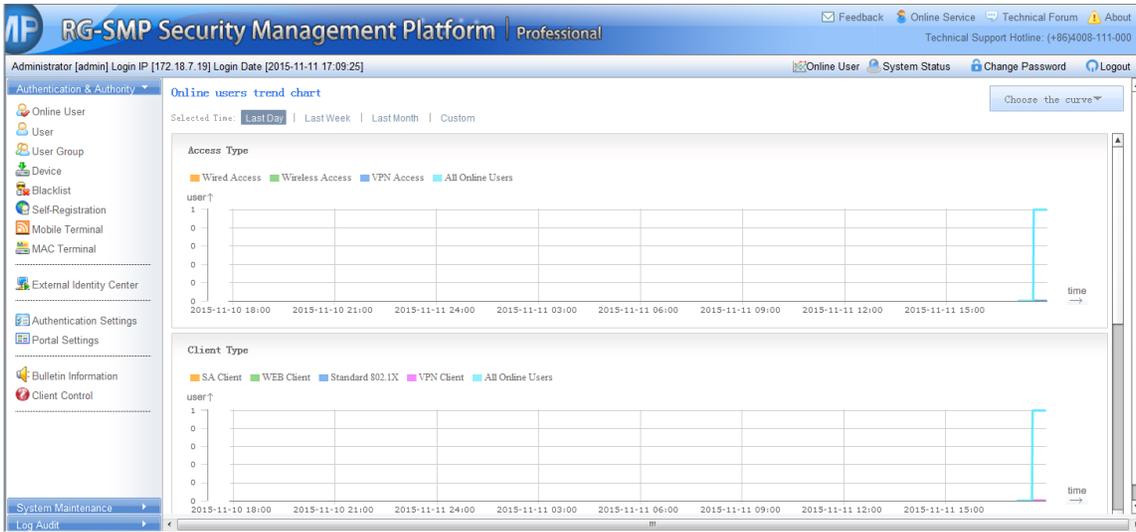
This section describes how to view the online user trend chart.

### Configuration Tips

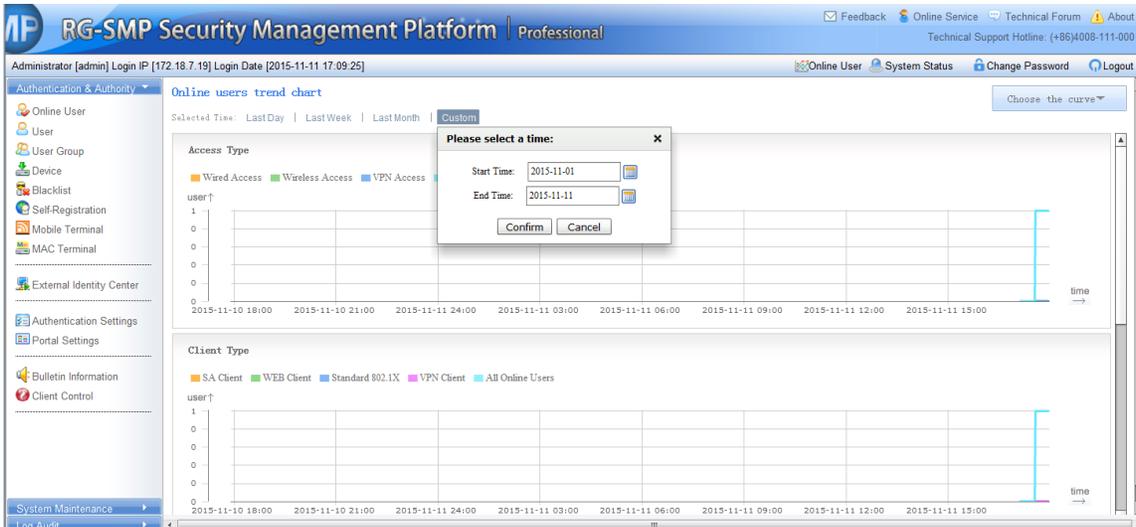
N/A

### Configuration Steps

- 1) Click **Online User** on the top navigation bar in homepage to enter the **Online User Trend Chart** page. Select **Last Day**, **Last Week**, **Last Month**, or **Custom** as required.



2) If you click **Custom**, a dialog box is displayed. Specify the start time and end time in the dialog box, and click **Confirm**.



## SIM Card Management

### Function Description

This section describes how to manage SIM cards.

### Configuration Tips

N/A

## Configuration Steps

### Adding the SIM Card Information

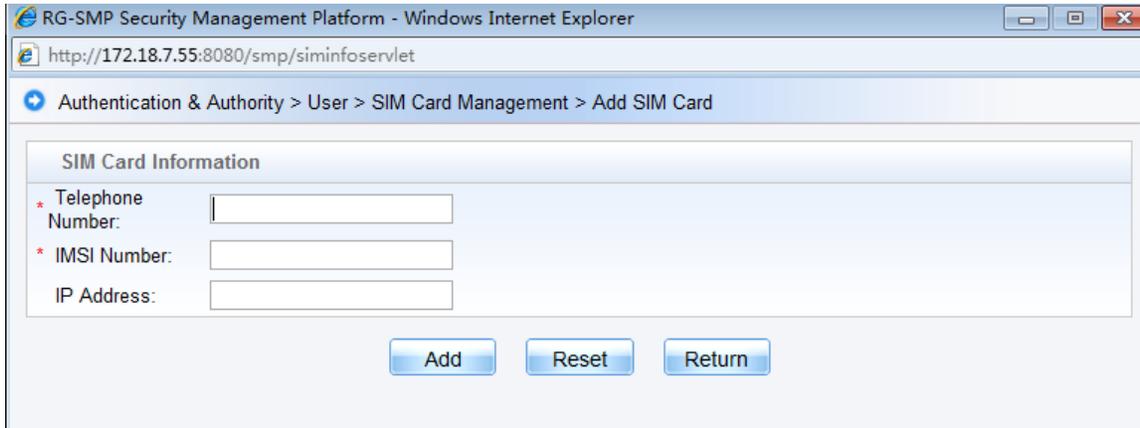
- 1) Choose **Authentication & Authority > User**, and click **SIM Card Management** to enter the SIM card management page.

The screenshot shows the 'Query Users' page in the RG-SMP Security Management Platform. The navigation bar includes 'Authentication & Authority > User > Query Users' and a highlighted 'SIM Card Management' link. Below the navigation bar, there are search filters for User Name, Full Name, User Group, User Type, and User Status. A table displays user information with columns for Account Validity Period, Expiry Date, Number of Blacklisted Users, Online Info, User Type, and Operation. The table contains 6 records.

	User Name	Full Name	User Group	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	User Type	Operation
<input type="checkbox"/>	123	123	Guest User Group	Delete Account when Expire	2015-11-13 17:35:48	0	1 Online Users	Guest User	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	Herry	Herry	Default User Group	Never Expire		0	Offline	Common User	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	Jay	Jay	Default User Group	Never Expire		0	Offline	Common User	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	newuser	test	new	Never Expire		0	Offline	Common User	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
<input type="checkbox"/>	test	111	Default User Group	Never Expire		0	Offline	Common User	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>

The screenshot shows the 'SIM Card Management' page in a Windows Internet Explorer browser. The page title is 'RG-SMP Security Management Platform - Windows Internet Explorer'. The address bar shows the URL 'http://172.18.7.55:8080/smp/siminfoservlet?kind=query'. The page content includes search fields for 'Telephone Number' and 'IMSI Number', and buttons for 'Query' and 'Reset'. Below the search fields are buttons for 'Add', 'Import', 'Delete', and 'Close'. A message box displays the text: 'No matching SIM card information is found.'

- 2) On the **SIM Card Management** page, click **Add** to add the SIM card information.



RG-SMP Security Management Platform - Windows Internet Explorer

http://172.18.7.55:8080/smp/siminfoservlet

Authentication & Authority > User > SIM Card Management > Add SIM Card

**SIM Card Information**

\* Telephone Number:

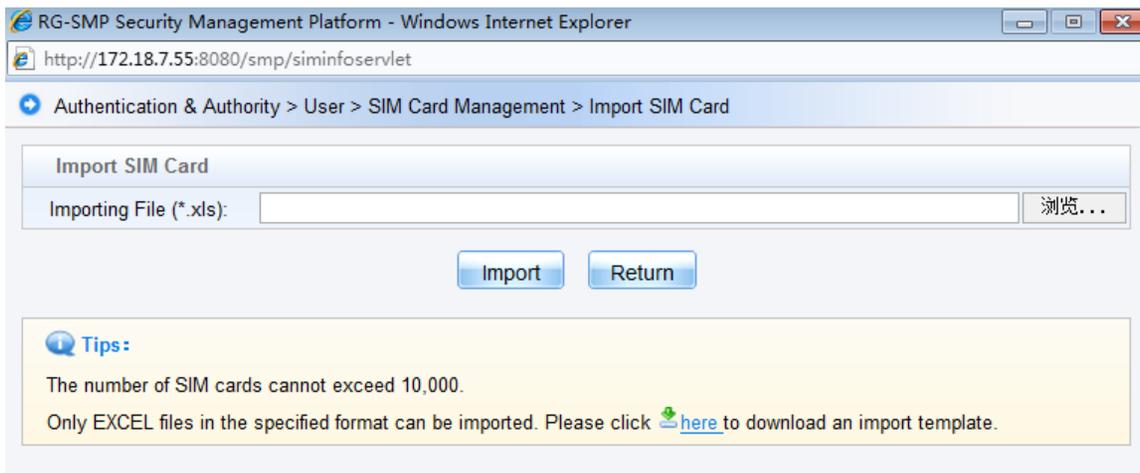
\* IMSI Number:

IP Address:

- 3) Click **Add** to complete addition.

## Importing the SIM Card Information

- 1) On the SIM card management page, click **Import** to import the SIM card information in batch.



RG-SMP Security Management Platform - Windows Internet Explorer

http://172.18.7.55:8080/smp/siminfoservlet

Authentication & Authority > User > SIM Card Management > Import SIM Card

**Import SIM Card**

Importing File (\*.xls):  浏览...

**Tips:**

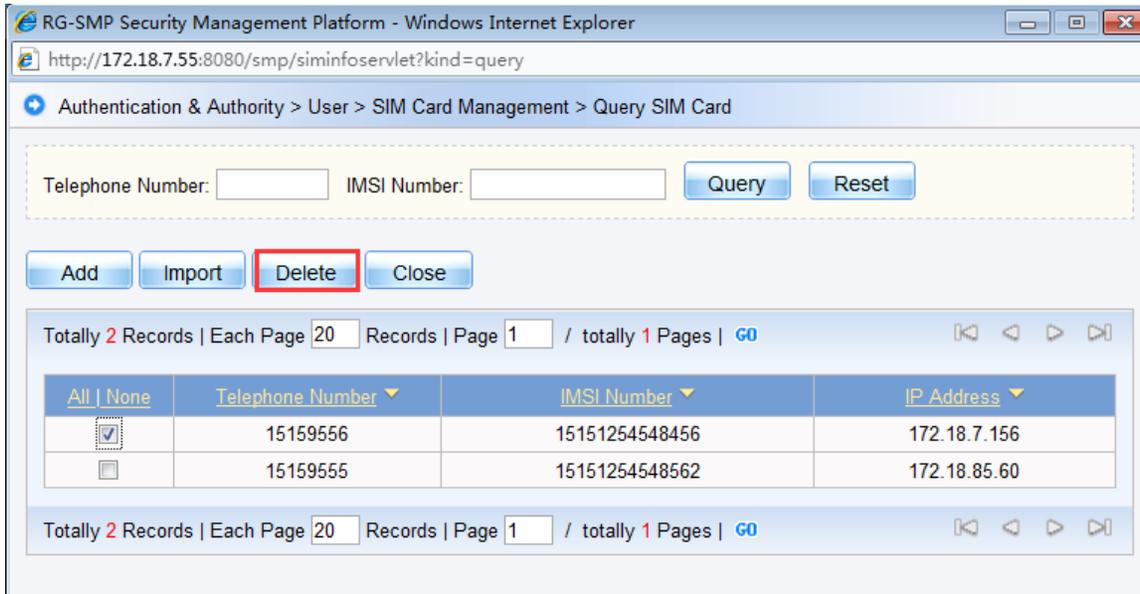
The number of SIM cards cannot exceed 10,000.

Only EXCEL files in the specified format can be imported. Please click [here](#) to download an import template.

- 2) Click **herein Tips** on the **Import SIM Card** page to download the import template. After the file filled with SIM card information is imported, click **Import** to complete addition in batch.

## Deleting the SIM Information

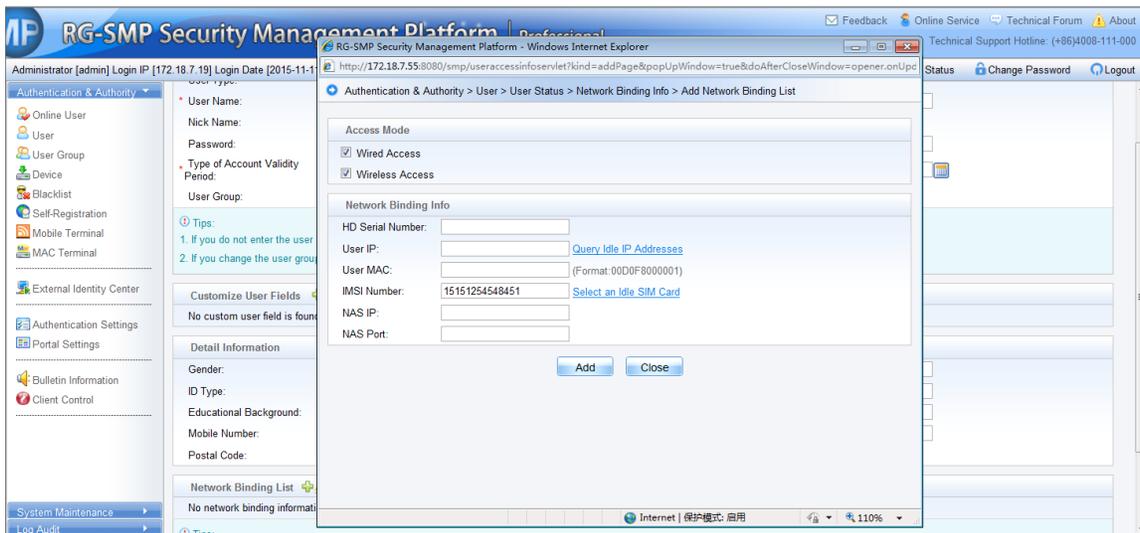
- 1) On the SIM card management page, select the SIM cards to be deleted, and click **Delete**.



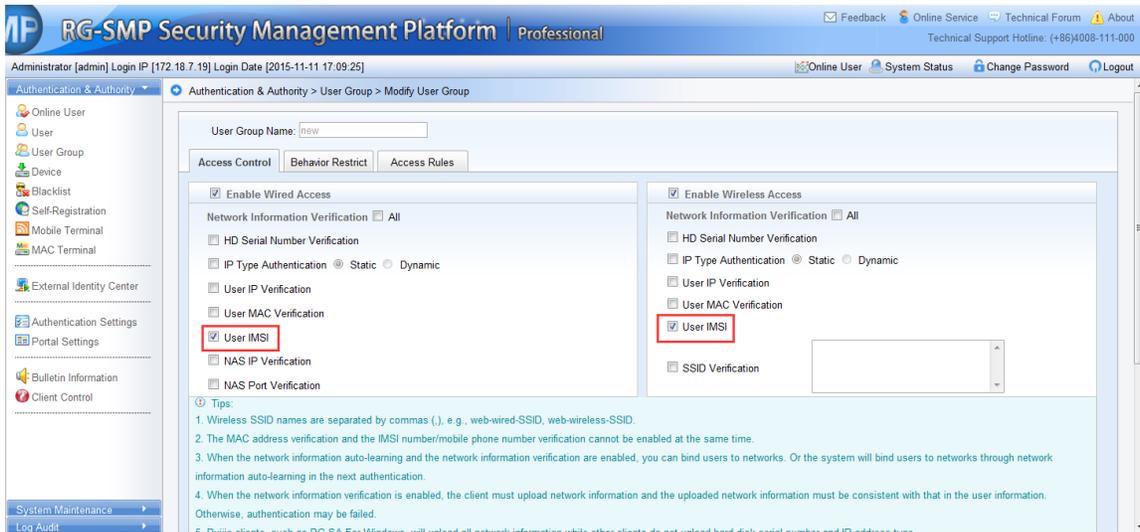
- Click **OK** to delete the selected SIM cards.

## Binding the SIM Card Information

- When a user is added, the SIM card information bound to the user is added simultaneously.



- Choose **Authentication & Authority > User Group > Modify User Group**, and check the **User IMSI** boxes under the wired and wireless access modes. After this configuration is completed, the SIM card information bound to the user will be verified during user authentication.



## VPN Access

### Function Description

This section describes how to configured related parameters on RG-SMP to support users' access to the network through the virtual private network (VPN).

### Configuration Tips

N/A

### Configuration Steps

#### Adding a NAS

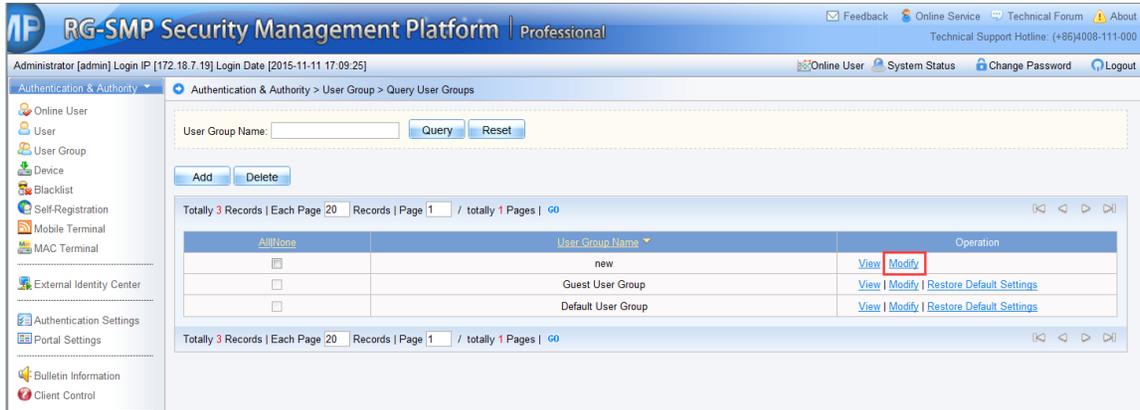
See section [2.1.1.3.1 "Adding a NAS"](#).

#### Adding a User

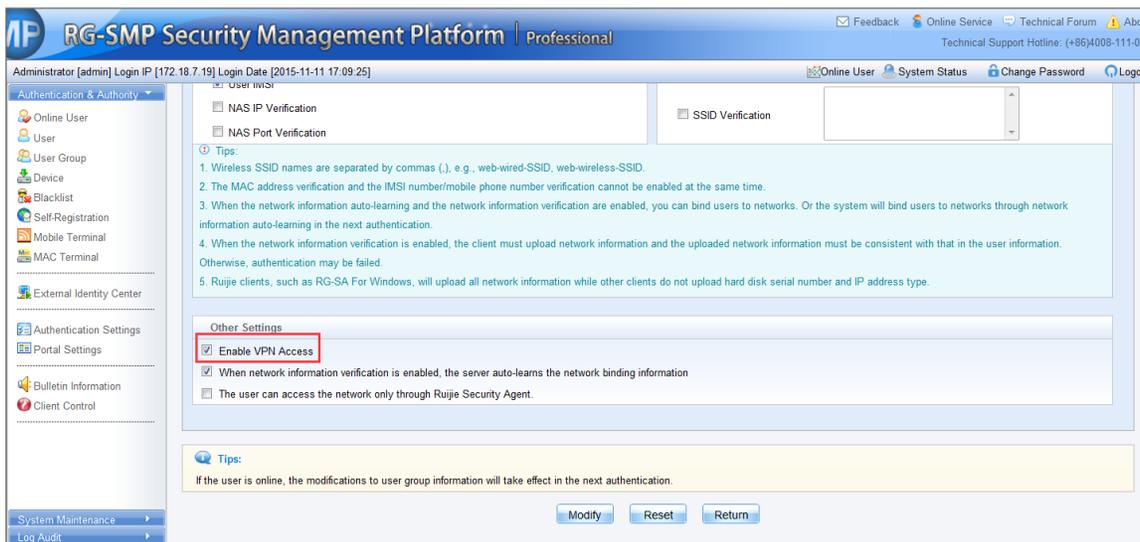
See section [2.1.1.3.2 "Adding a User"](#).

### Enabling VPN Access

- 1) Choose **Authentication & Authority > User Group**, choose a user group and click **Add** or **Modify**. The related user group configuration page is displayed.



2) Check the **Enable VPN Access** box, and click **Add/Modify** to save the configuration.



## Network Access Prohibited Period

### Function Description

This section describes how to configure the authentication prohibited period on RG-SMP.

Authentication cannot be performed during the network access prohibited period. If an offline user attempts authentication, it fails during the prohibited period. If an online user stays online until the period is coming, the user will be forced offline. Within the configured authentication prohibited period, user authentication is prohibited.

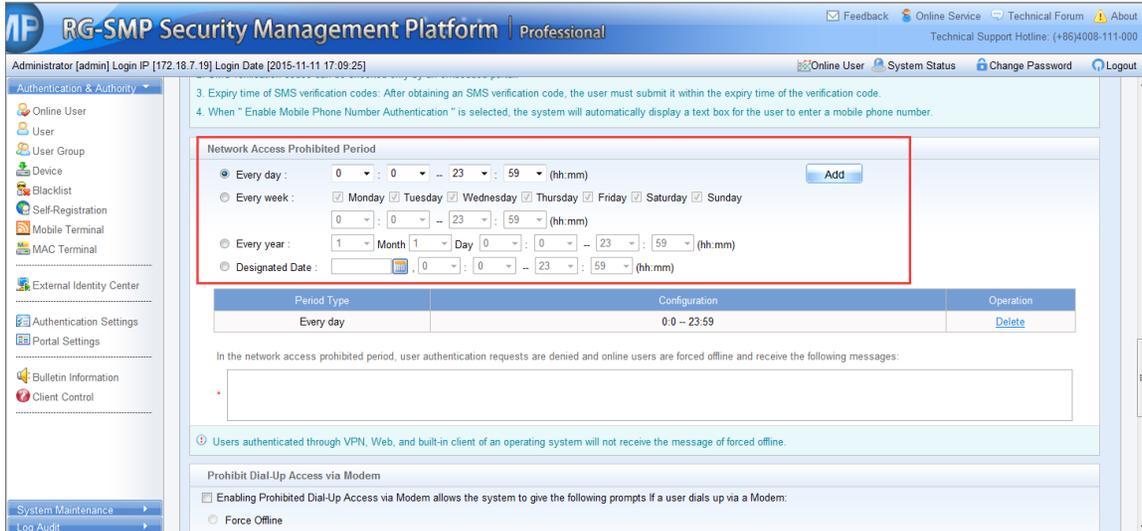
For authentication failures in the authentication prohibited period, the failure cause can be customized.

### Configuration Tips

N/A

## Configuration Steps

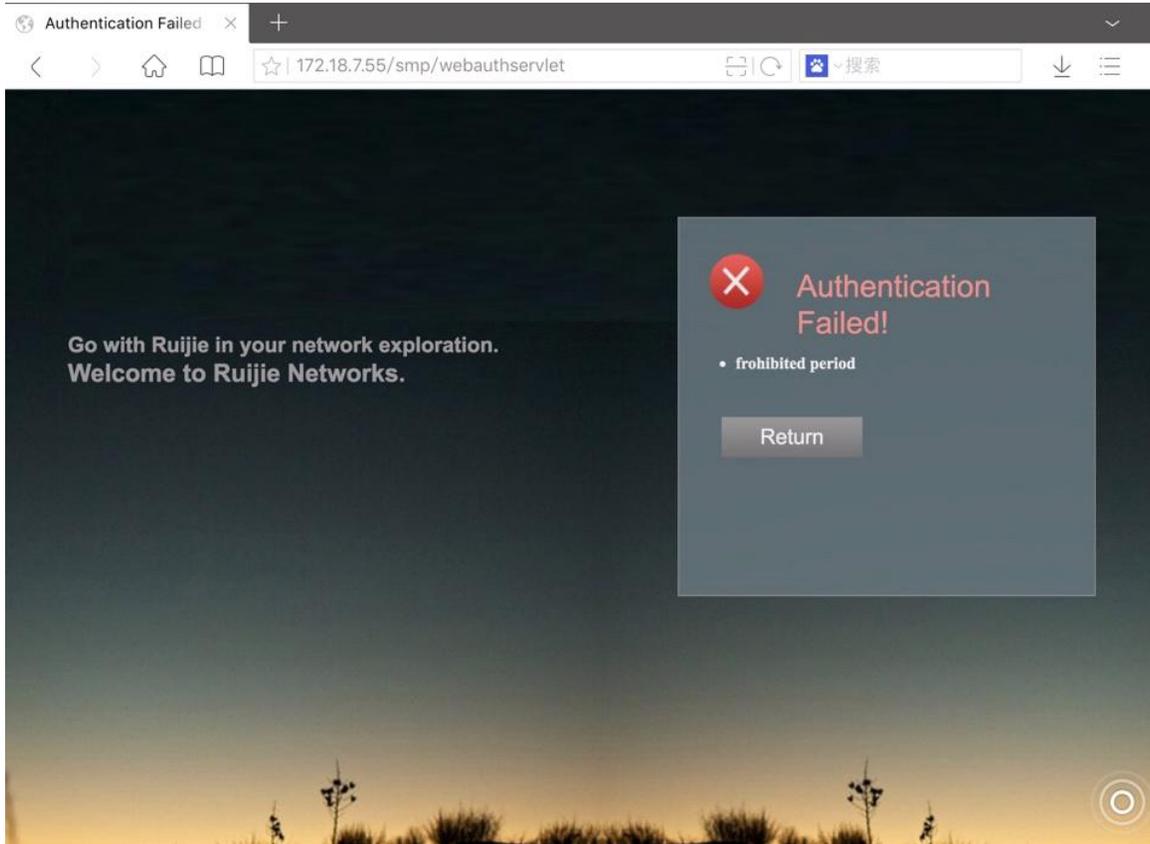
- 1) Choose **Authentication & Authority > User Group**, click **Add** or **Modify** to enter the user group management page to configure the prohibited period.



- 2) Click **Add** or **Modify** to save the settings.

## Terminal Authentication

- 1) Authentication will fail in the specified authentication prohibited period.



## Mobile Terminal Management

### Function Description

This section describes how to manage mobile terminals on RG-SMP.

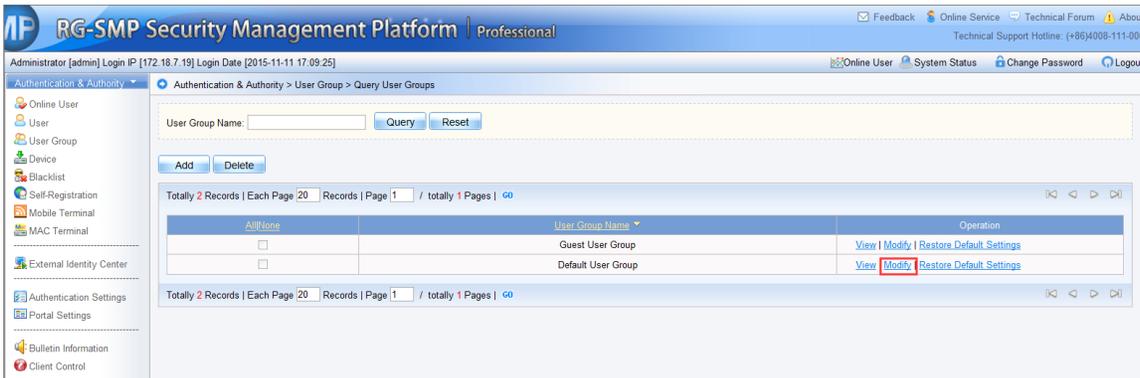
### Configuration Tips

N/A

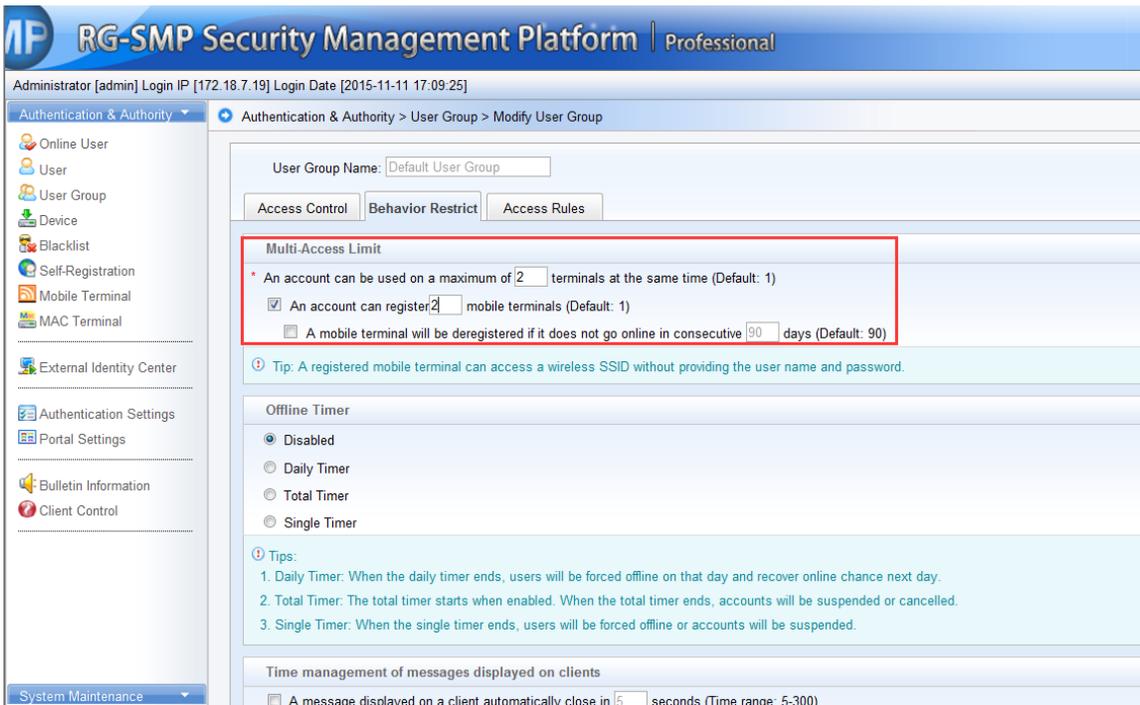
### Configuration Steps

## Adding Mobile Terminals

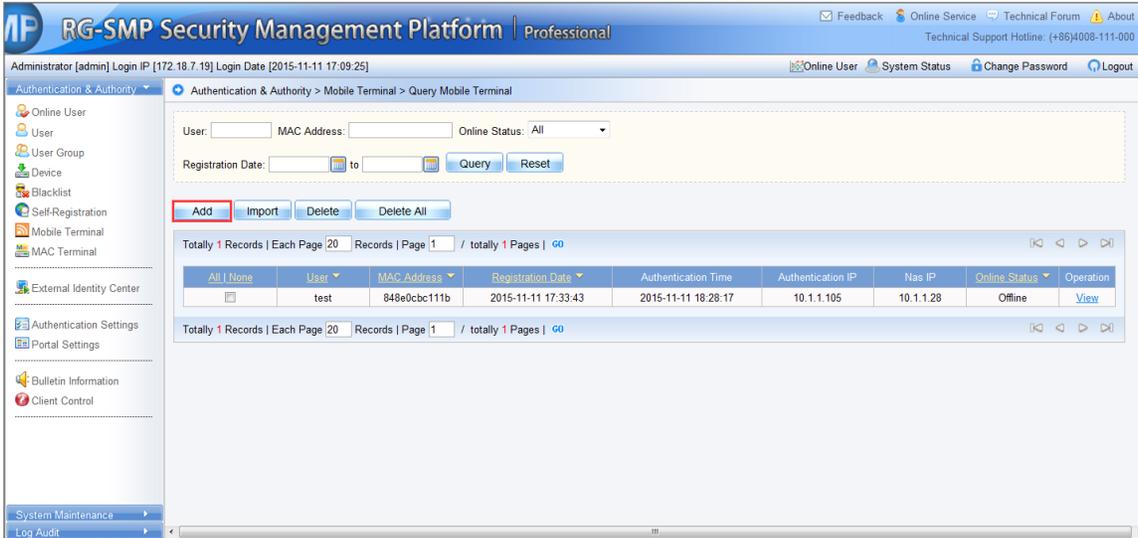
- 1) Choose **Authentication & Authority > User Group**, and click **Modify**.



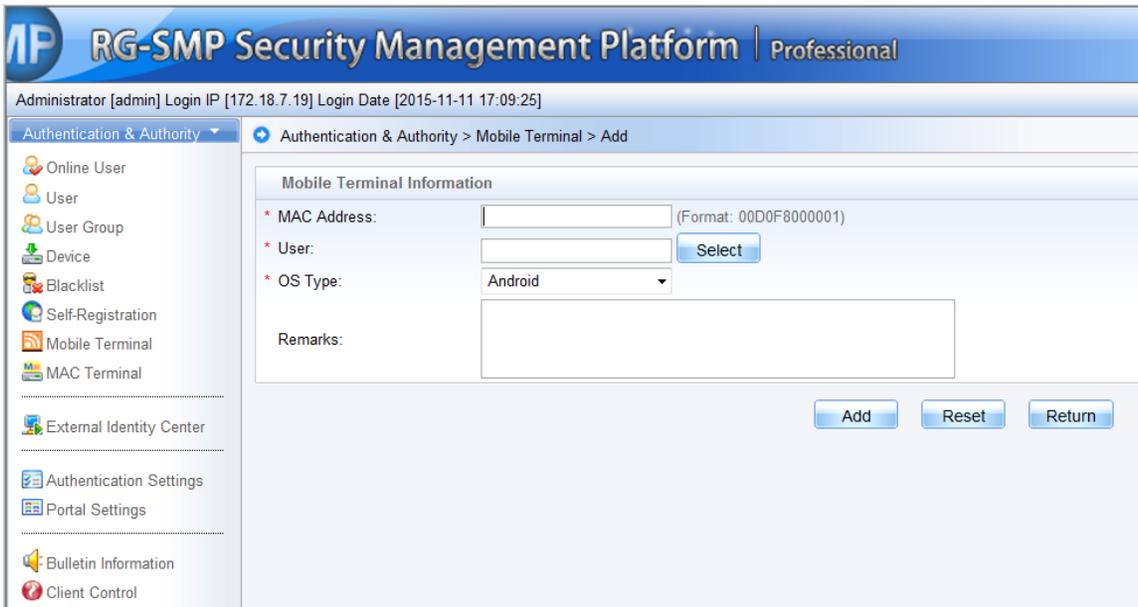
2) Select the **Behavior Restrict** tab, and check the **An account can register X mobile terminals** box to limit the maximum registered number of mobile terminals for one user account.



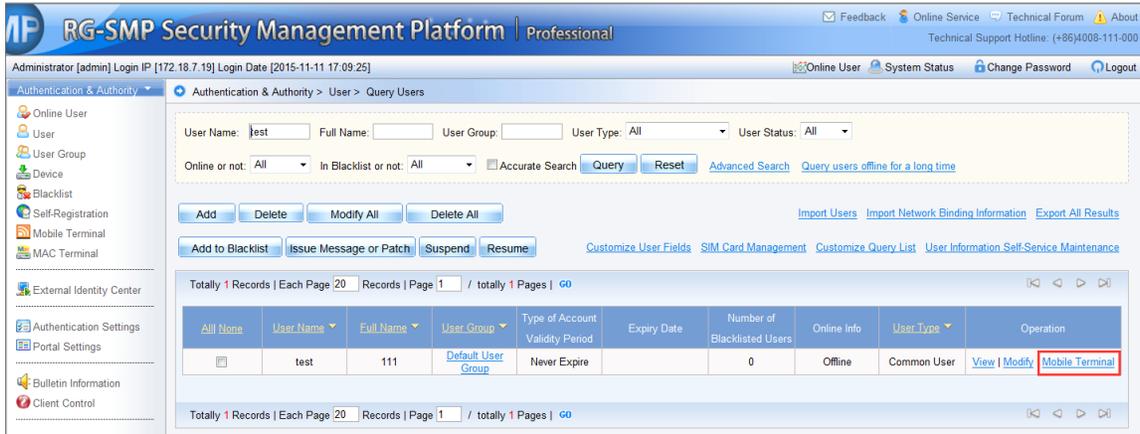
3) Choose **Authentication & Authority > Mobile Terminal** to go to the mobile terminal management page. Click **Add**.



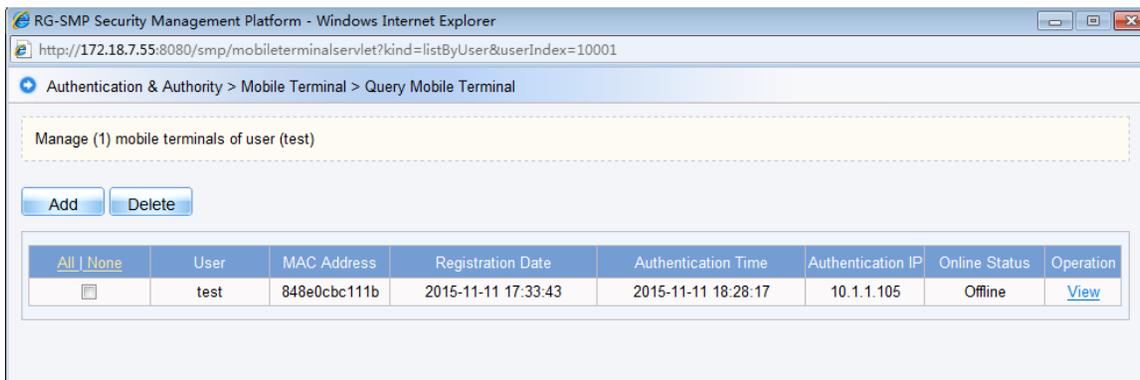
4) Enter the terminal information, and click **Add** to add the mobile terminal.



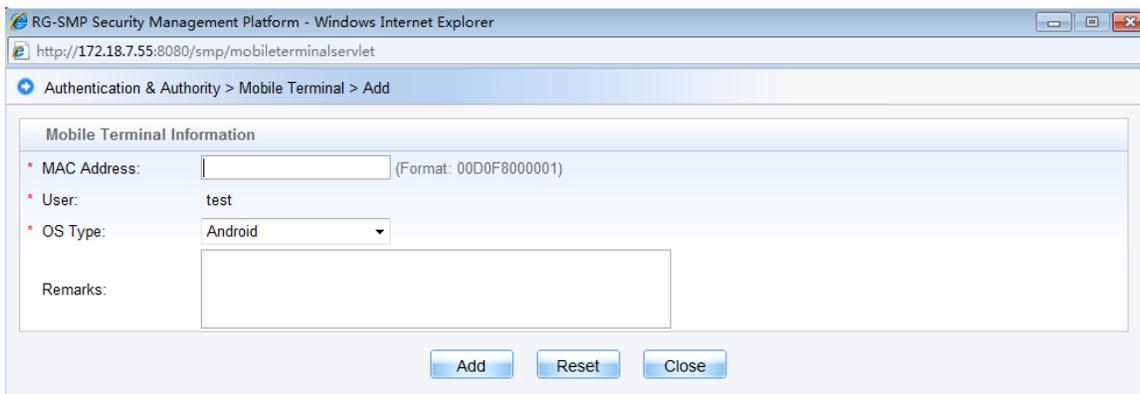
5) Alternatively, choose **Authentication & Authority > User** to enter the user management page. Select a user, and click **Mobile Terminal** to enter the mobile terminal management page of the user.



6) Click **Add**.

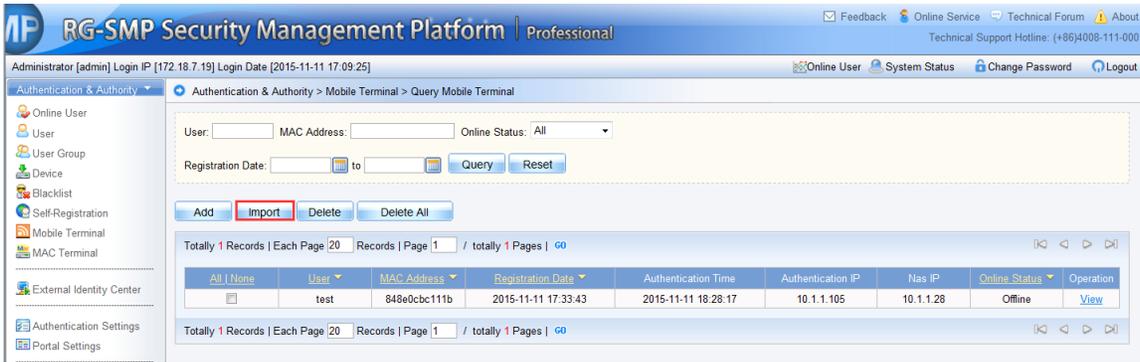


7) Enter the terminal information, and click **Add** to complete the addition.

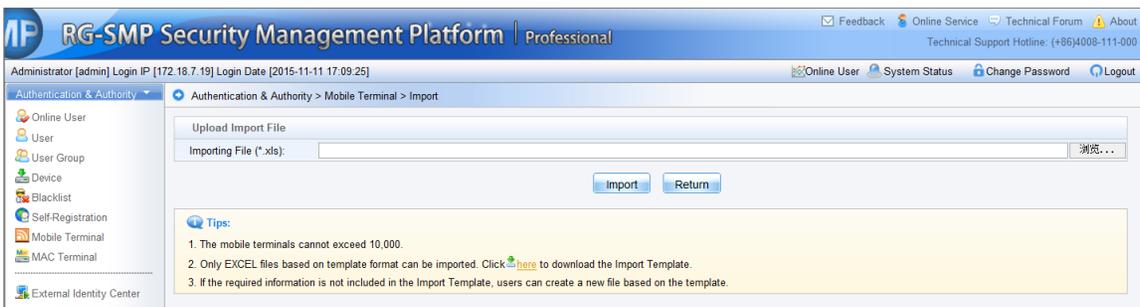


## Importing Mobile Terminals

- 1) Choose **Authentication & Authority > Mobile Terminal** to enter the mobile terminal management page. Select mobile terminals to be imported, and click **Import** to enter the mobile terminal import page.

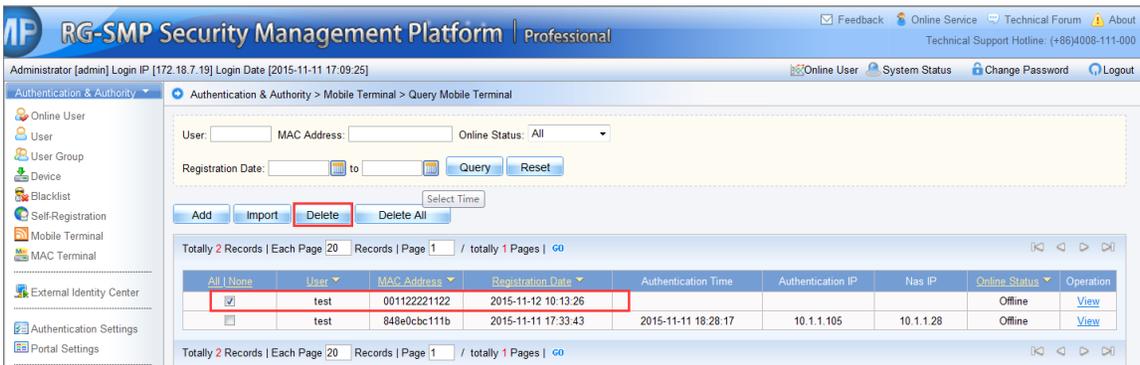


- 2) Select an **xls**. file to be imported. You can click [here](#) to download the import template, and then click **Import** to import mobile terminals.

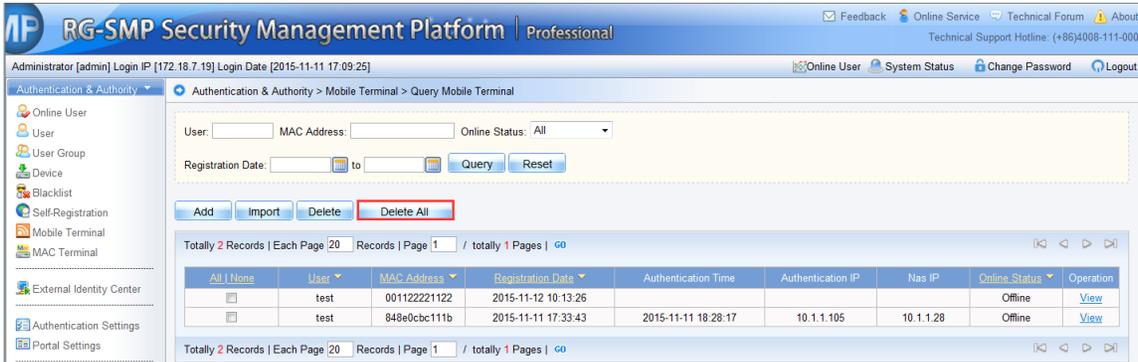


## Deleting Mobile Terminals

- 1) Choose **Authentication & Authority > Mobile Terminal** to enter the mobile terminal management page. Select a mobile terminal, and click **Delete** to delete the selected mobile terminal.



- 2) Choose **Authentication & Authority > Mobile Terminal** to go to the mobile terminal management page. Select multiple mobile terminals, and click **Delete All** to delete all the selected mobile terminals.



## MAC Terminal

### Function Description

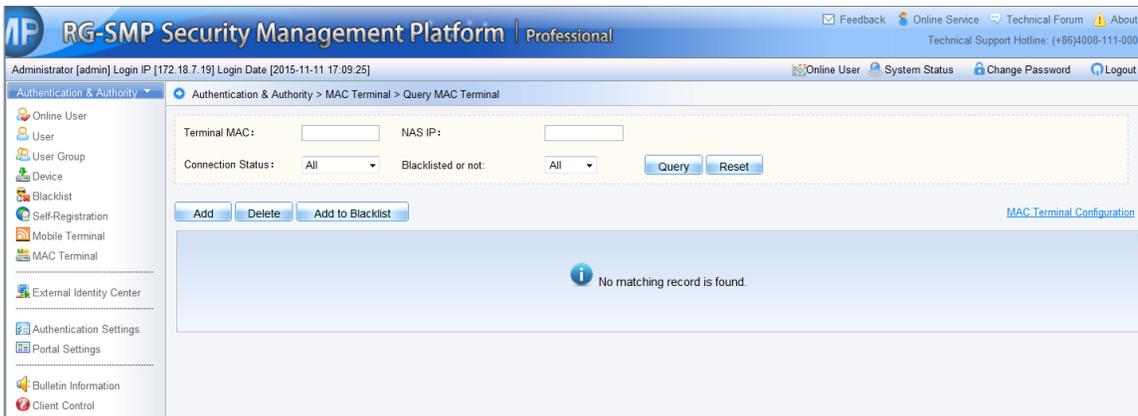
This section describes how to add some devices (such as printers and punch card machines) on the RG-SMP. These devices do not support installation of the RG-SA, but must be connected to the network through 802.1X authentication.

### Configuration Tips

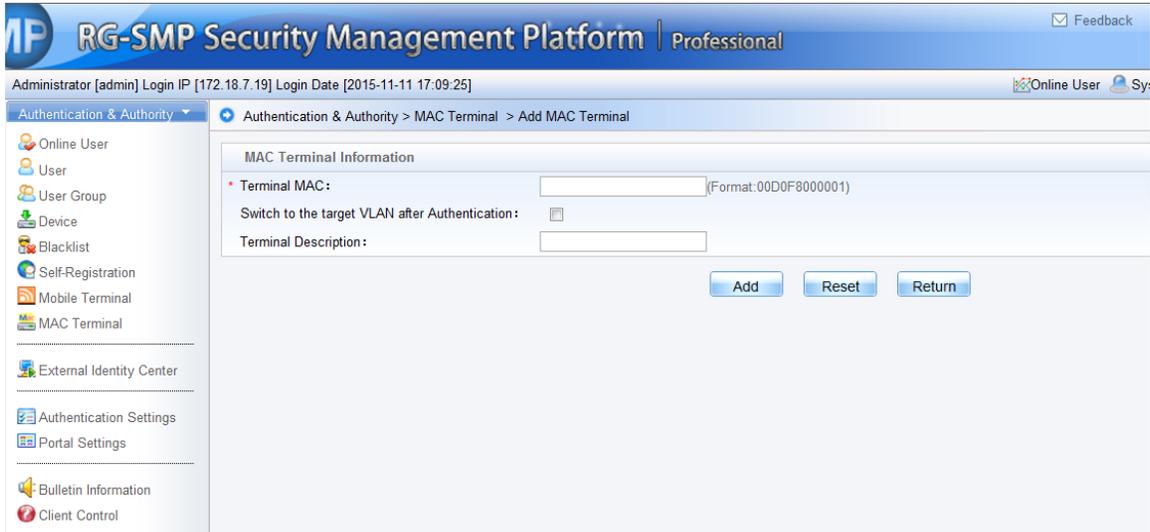
N/A

### Configuration Steps

- 1) Choose **Authentication & Authority > MAC Terminal** to enter the MAC address authentication management page.



- 2) Click **Add** to enter the page for adding a MAC address authentication device. Enter the information related to the MAC address authentication device.



- 3) Click **Add** to complete the addition.

## Authentication Settings

### Function Description

This section describes how to configure Authentication Parameters and enable Periodic Online Status Detection, PEAP Authentication of Windows Client, and Account Expiration Warning on RG-SMP.

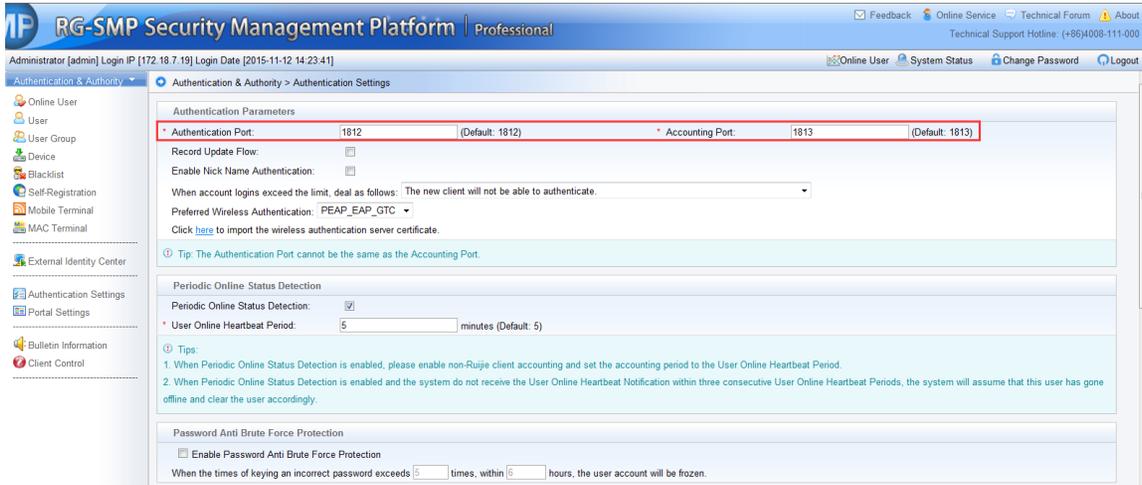
### Configuration Tips

N/A

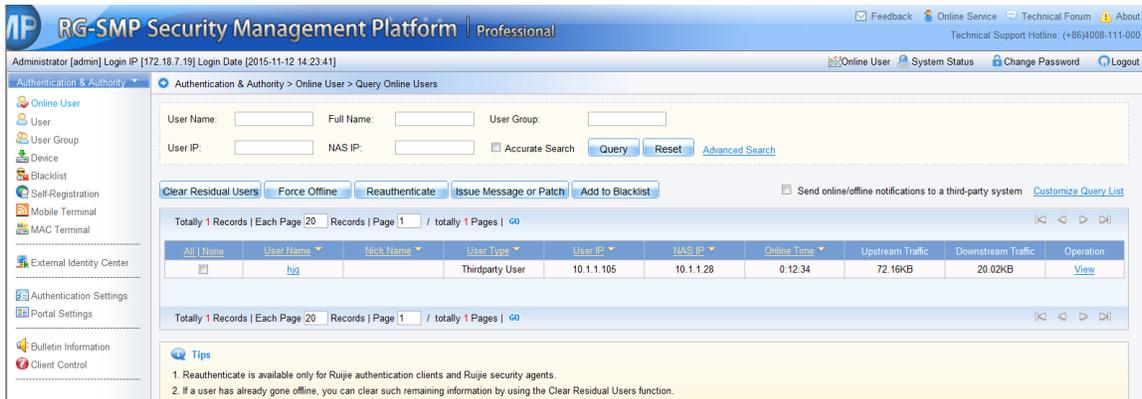
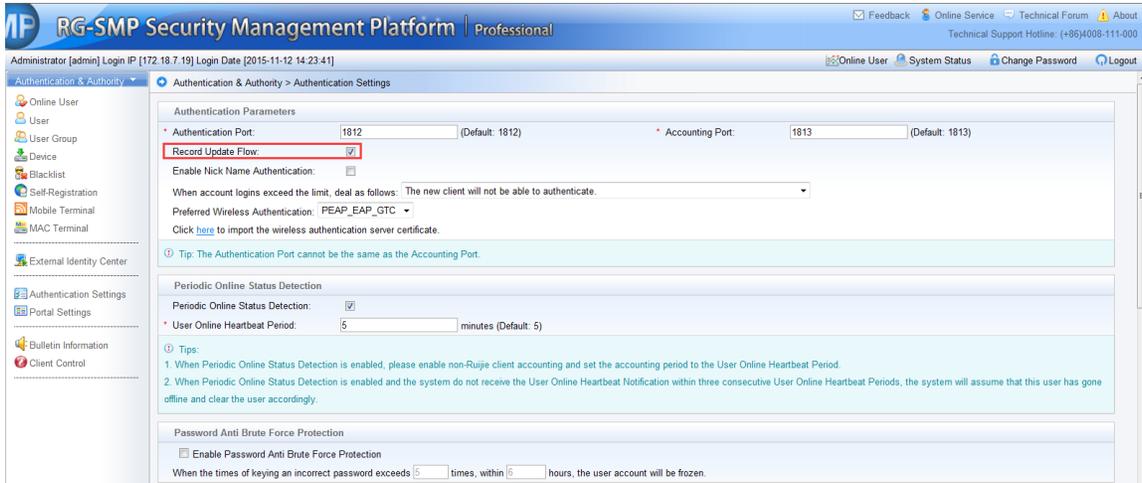
### Configuration Steps

## Configuring Authentication Parameters

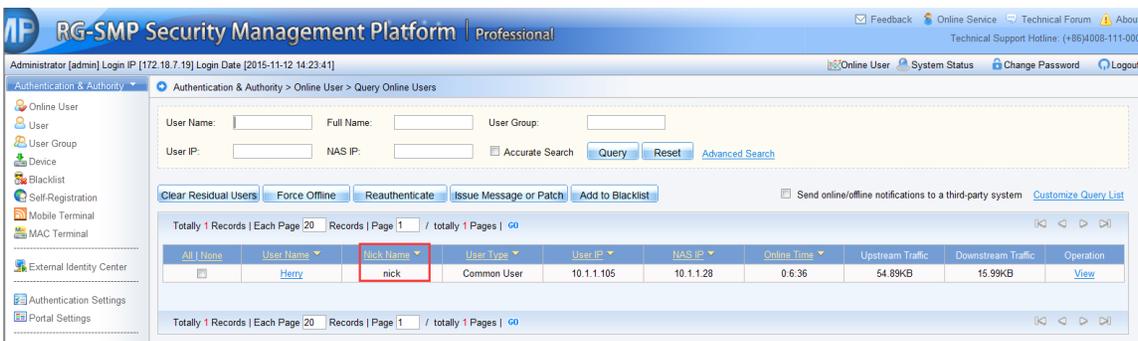
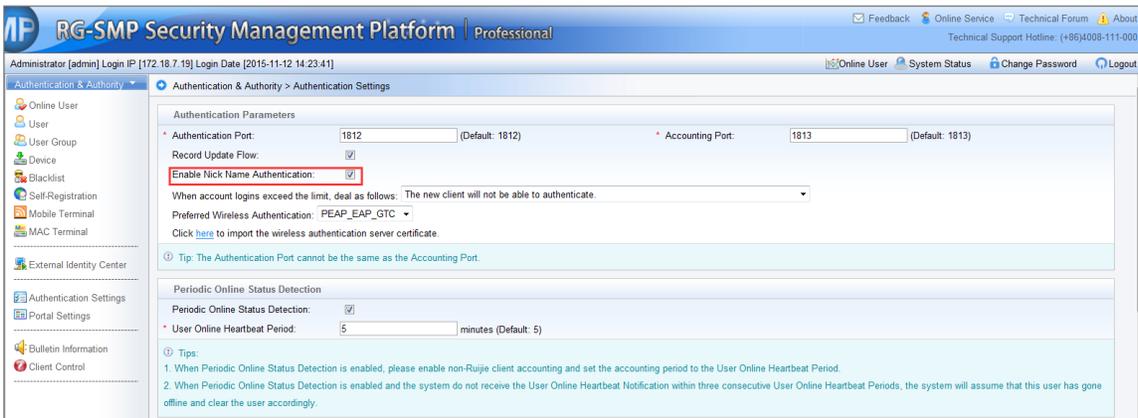
- 1) Choose **Authentication Settings** on the left navigation bar to enter the authentication parameter configuration page. Configure **Authentication Port** and **Accounting Port**. The default ports are recommended.



2) Check the **Record Update Flow** box to enable traffic recording. After this option is selected, the uplink and downlink traffic will be displayed on the online user management page.

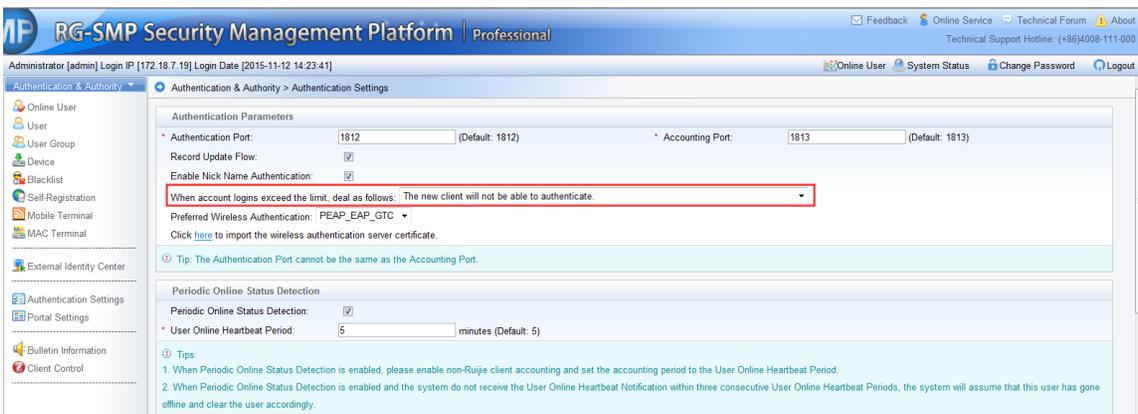


3) Check the **Enable Nick Name Authentication** box so that users can use the nick names and passwords for authentication. If authentication is successful, the user information will be displayed on the online user management page.

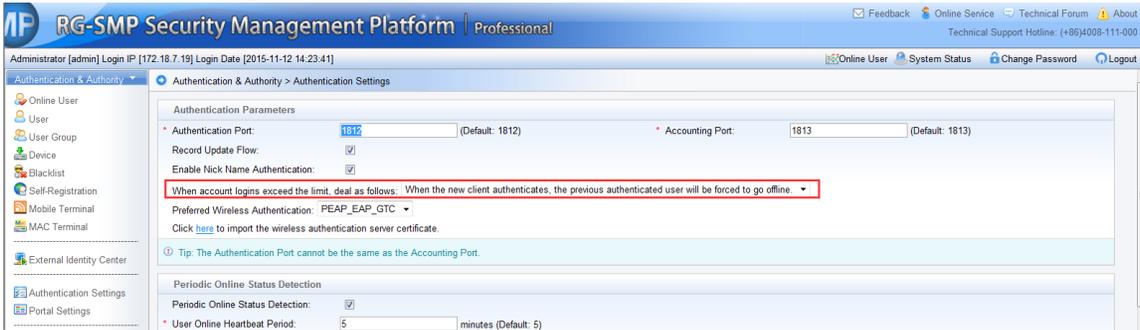
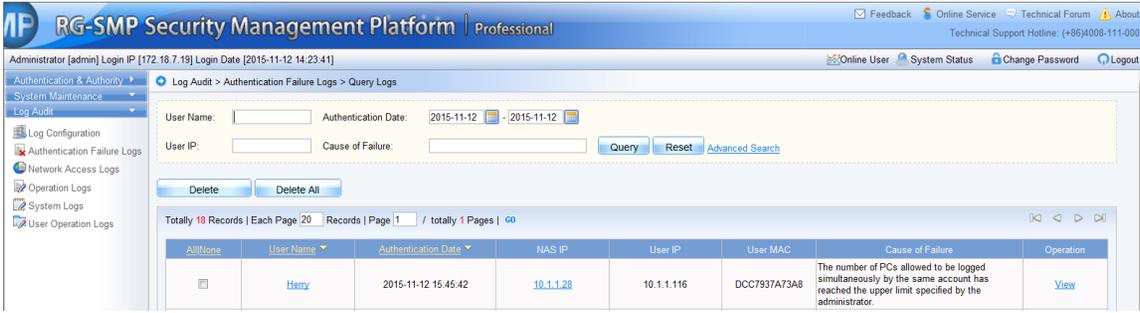


4) Configure the processing mode when the login times of the same account exceeds the limit. Options of processing modes include:

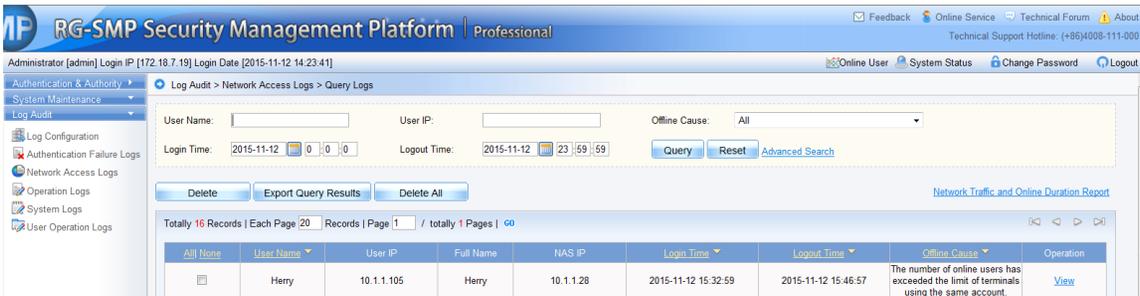
- The new client cannot be authenticated.
- When the new client authenticates, the previous authenticated user will be forced offline.



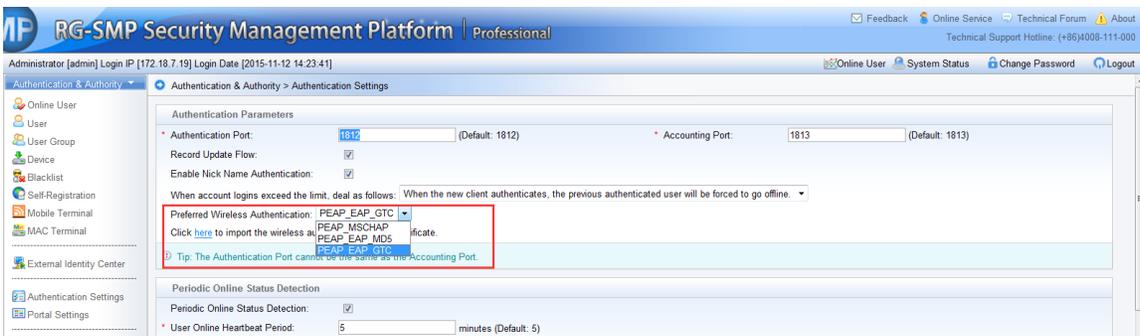
- If the first processing mode is selected, the authentication failure information of the new client will be displayed in the authentication failure log.



- If the second processing mode is selected, the information indicating that the user is successfully authenticated but is forced offline will be displayed in the network access history.

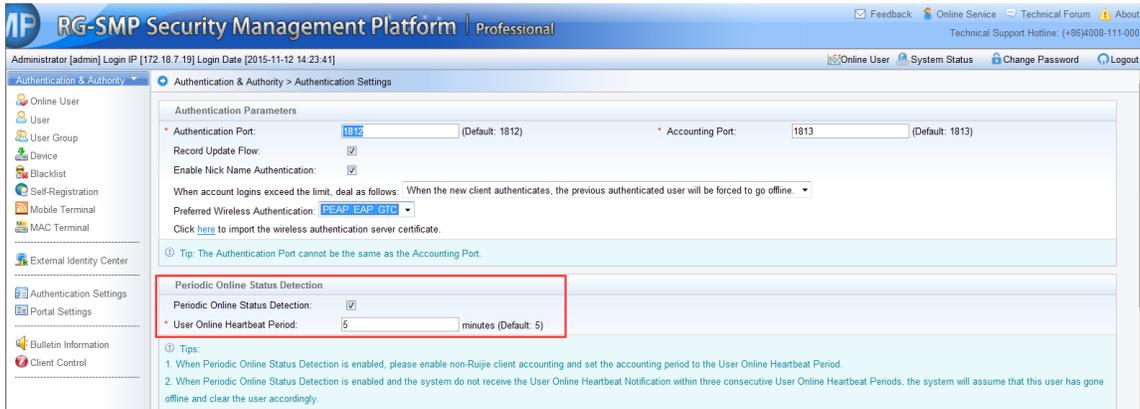


- 5) Configure the **Preferred Wireless Authentication** mode. Options include **PEAP\_MSCHAP**, **PEAP\_EAP\_MD5**, and **PEAP\_EAP\_GTC**.



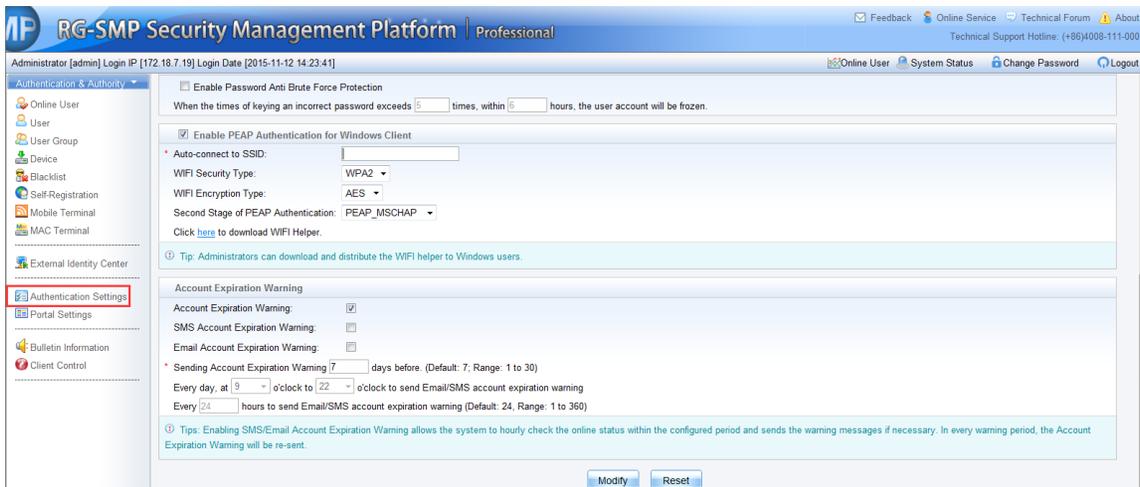
## Enabling Periodic Online Status Detection

- 1) Choose **Authentication & Authority > Authentication Settings** from the left navigation bar to enter the authentication parameter configuration page. Check the **Periodic Online Status Detection** box, and configure the **User Online Heartbeat Period**.

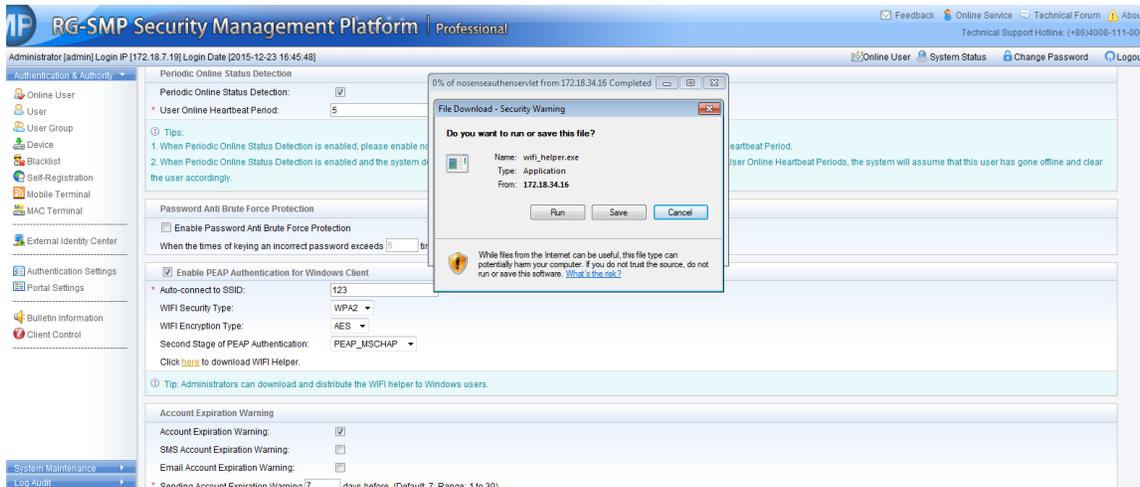


## Enabling PEAP Authentication for Windows Client

- 1) Choose **Authentication & Authority > Authentication Settings** from the left navigation bar to enter the authentication parameter configuration page. Check the **Enable PEAP Authentication for Windows Client** box, configure the authentication parameters, and save the settings.

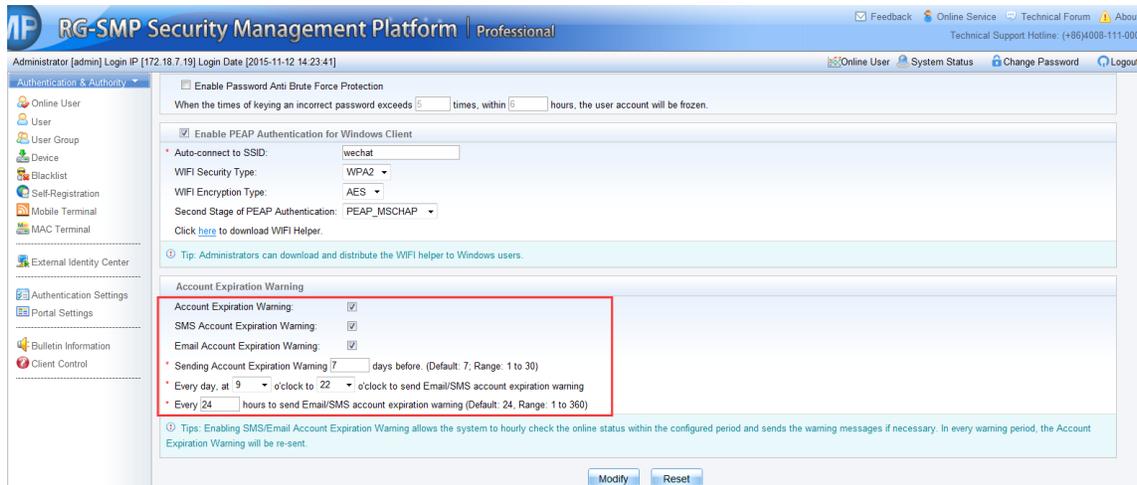


- 2) The administrator can download and transfer the Wi-Fi helper to Windows users.



## Enabling Account Expiration Warning

- 1) Account Expiration Warning: Choose **Authentication & Authority > Authentication Settings** from the left navigation bar to enter the authentication parameter configuration page. Choose the **Account Expiration Warning** box to enable this function.



- 2) SMS Account Expiration Warning: Choose **Authentication & Authority > Authentication Settings** from the left navigation bar to enter the authentication parameter configuration page. Check the **SMS Account Expiration Warning** box to enable this function. After the day, time, and interval, the warning is sent.
- 3) Email Account Expiration Warning: Choose **Authentication & Authority > Authentication Settings** from the left navigation bar to enter the authentication parameter configuration page. Check the **Email Account Expiration Warning** box to enable this function. Then, configure the day, time, and interval for sending the warning.

## Portal Settings

### Function Description

This section describes how to configure the **Web Authentication & Self-Service**, **Enable Web Authentication**, **Enable Authentication-Exemption Rule for Web Users**, **Enable Guest Registration**, **Open Disclaimer Page**, and **Heartbeat Detection on Web-authenticated Users** on the RG-SMP.

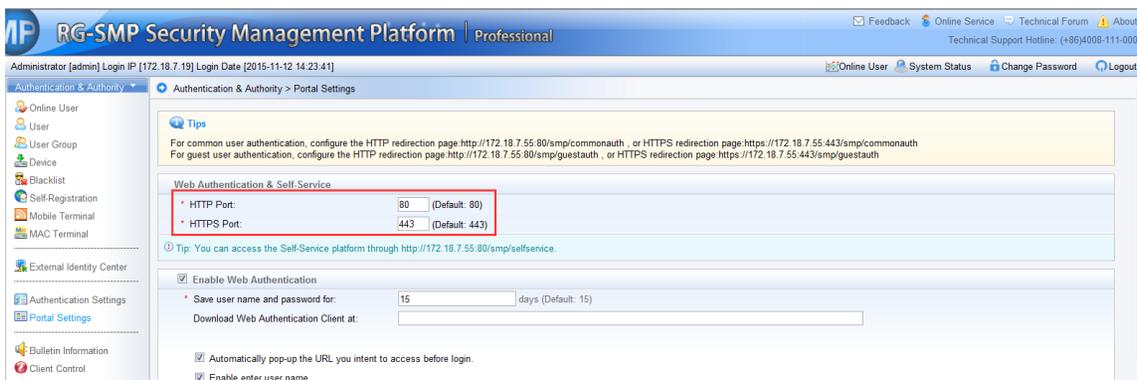
### Configuration Tips

N/A

### Configuration Steps

## Configuring Web Authentication & Self-Service

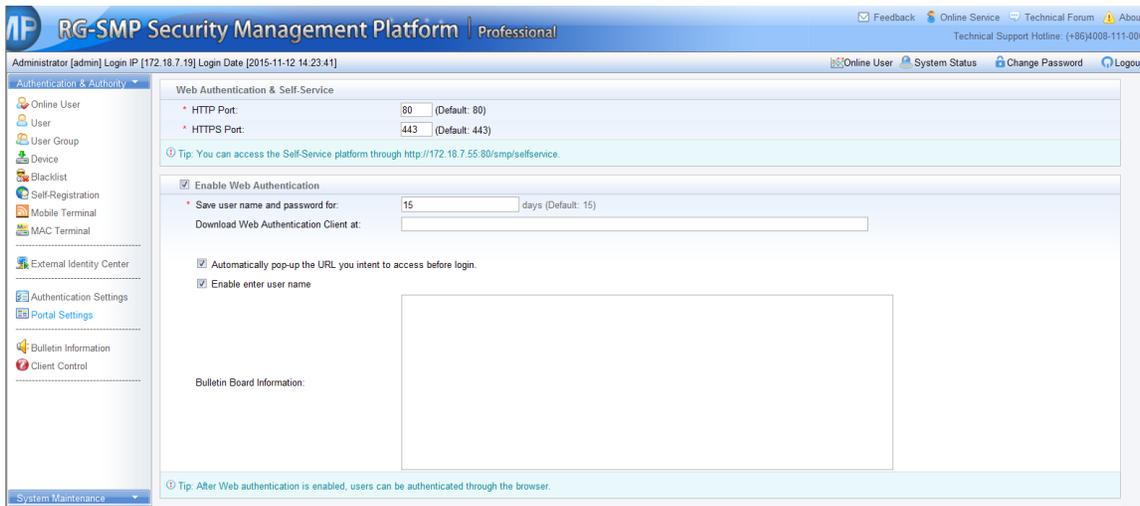
- 1) Choose **Authentication & Authority > Port Settings**, and check the **Enable Web Authentication** box to enter the Web authentication configuration page.



- 2) Configure the **HTTP Port** and **HTTPS Port**. The default values are recommended.

## Enabling Web Authentication

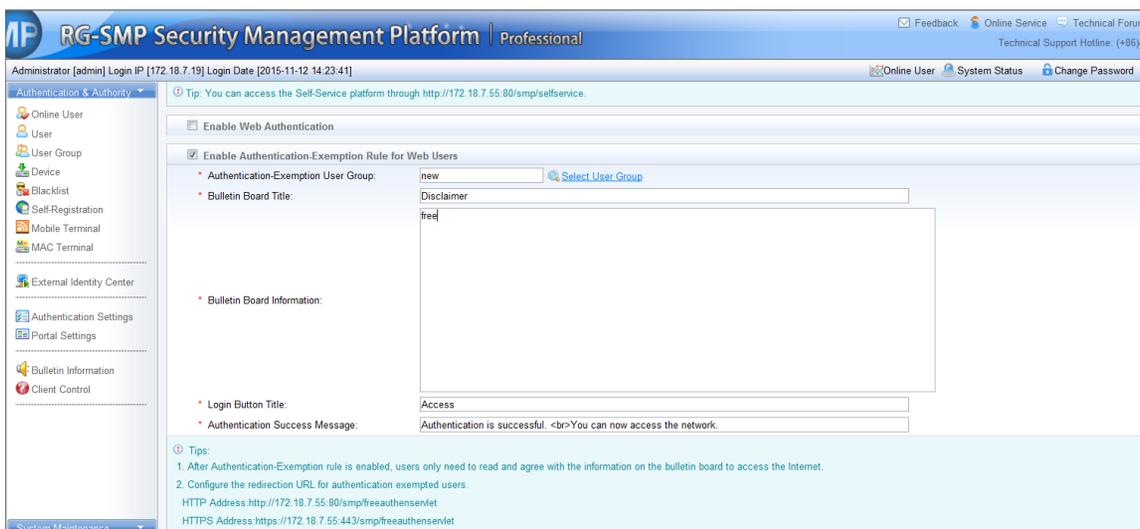
- 1) Choose **Authentication & Authority > Port Settings**, and check the **Enable Web Authentication** box to enter the Web authentication configuration page.



2) Configure the **Save user name and password for: X days**. Network access users can use the browser for authentication.

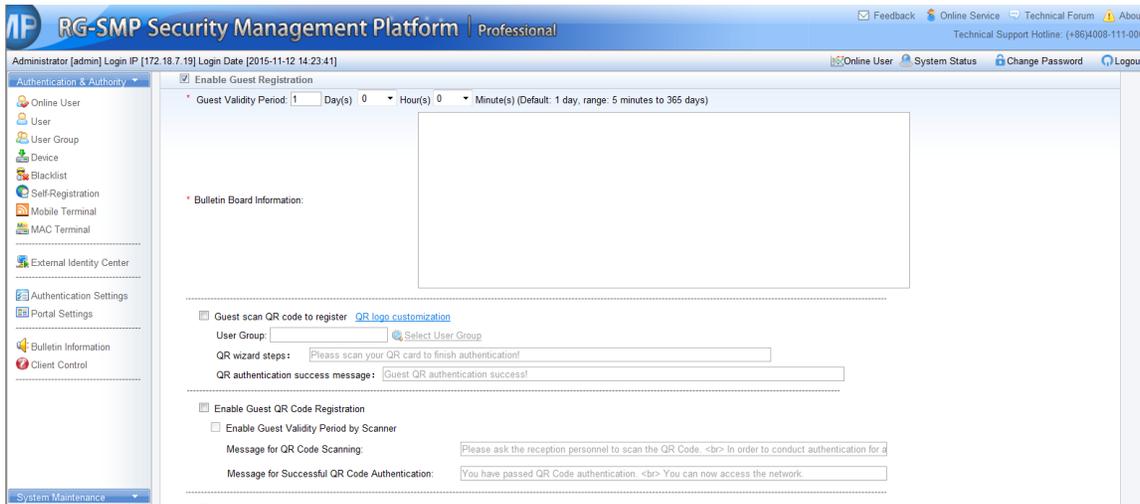
## Enabling Authentication-Exemption Rule for Web Users

Choose **Authentication & Authority > Port Settings**, check the **Enable Authentication-Exemption Rule for Web Users** box, and configure the **Authentication-Exemption User Group** to which authentication-exempted users belong, **Bulletin Board Information**, and so on.

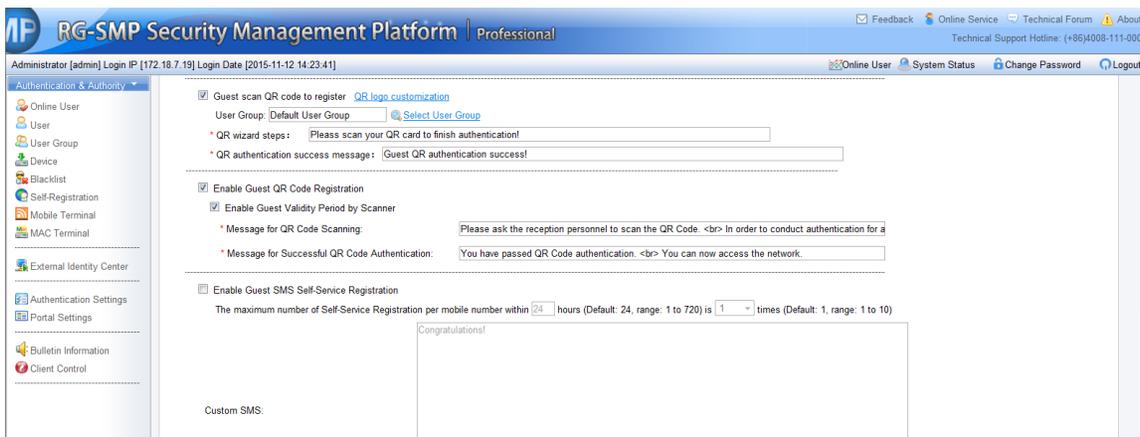


## Enabling Guest Registration

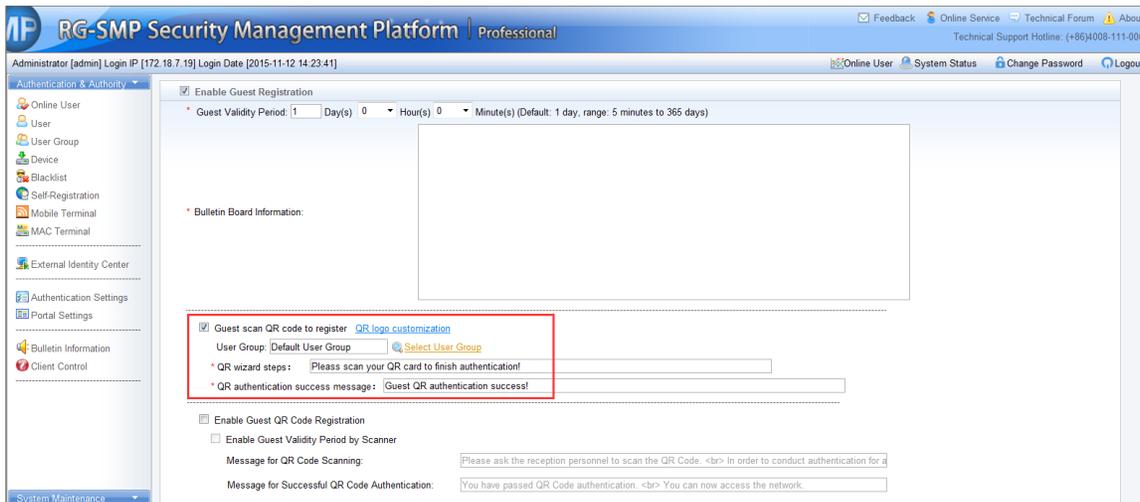
1) Choose **Authentication & Authority > Port Settings**, check the **Enable Guest Registration** box, and configure the **Guest Validity Period** and **Bulletin Board Information**.



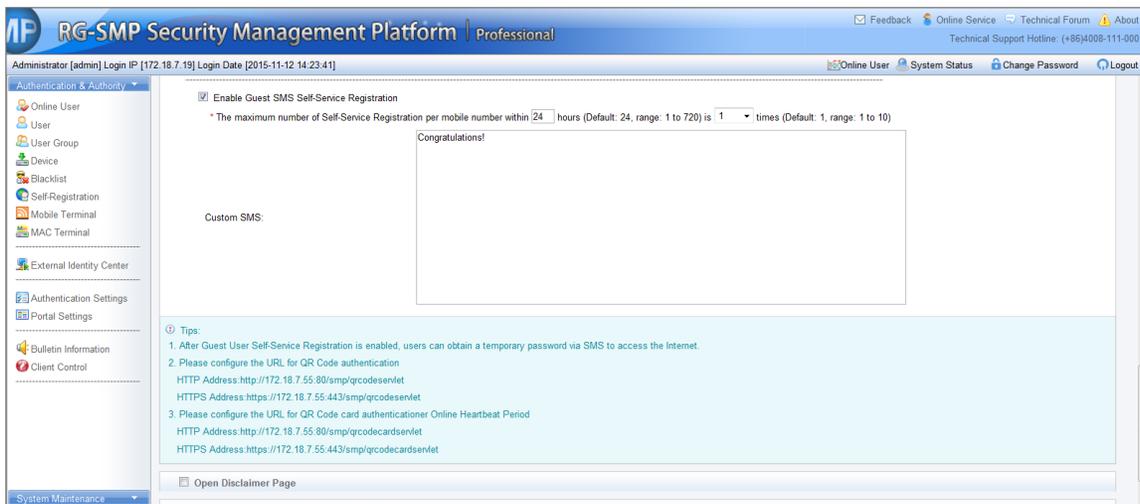
2) Check the **Enable Guest QR Code Registration** box so that a common user can open an account for a guest by scanning the QR code of the guest.



3) Check the **Guest scan QR Code to register** box so that a guest user can register by scanning the QR code of a common user.

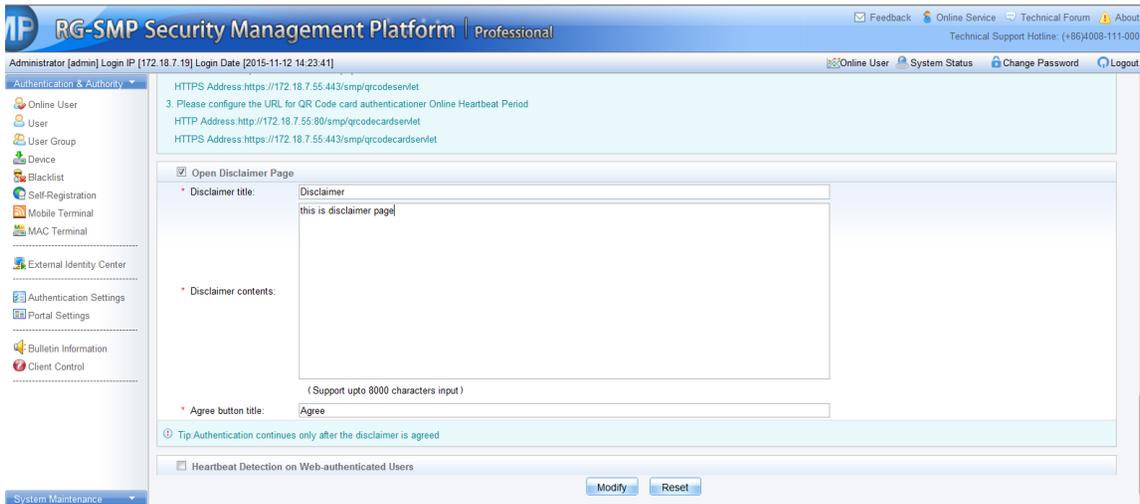


4) Check the **Enable Guest SMS Self-Service Registration** box so that a guest can register by using SMS.



## Opening Disclaimer Page

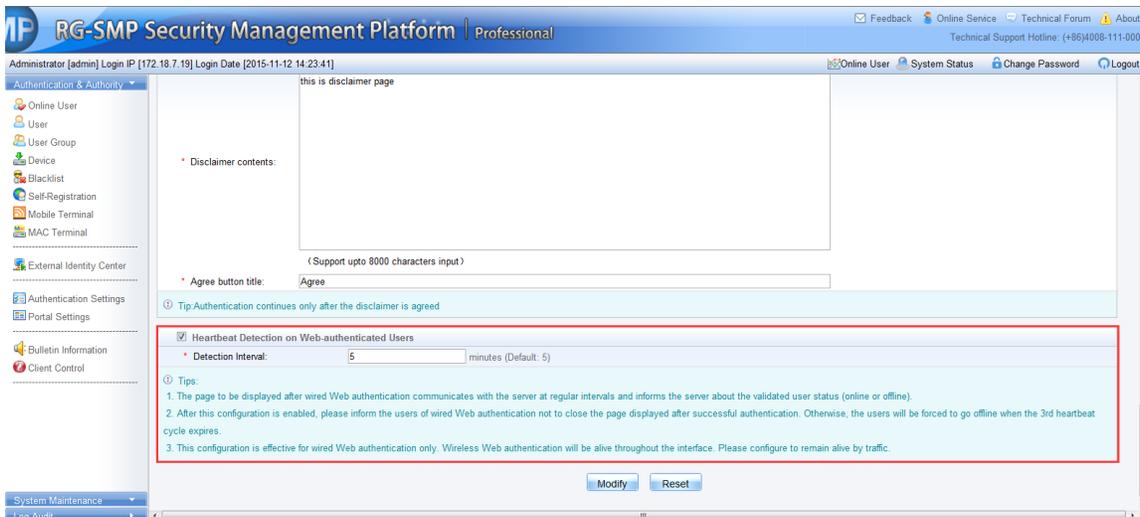
1) Choose **Authentication & Authority > Port Settings** to enter the Web authentication configuration page.



- 2) Check the **Open Disclaimer Page** box, configure the **Disclaimer Contents**, and click **Modify** to save the settings.

## Configuring Heartbeat Detection on Web-authenticated Users

- 1) Choose **Authentication & Authority > Port Settings** to enter the Web authentication configuration page.



- 2) Check the **Heartbeat Detection on Web-authenticated Users** box, and configure the **Detection Interval**.

## Bulletin Information

### Function Description

This section describes how to use the bulletin information function of RG-SMP.

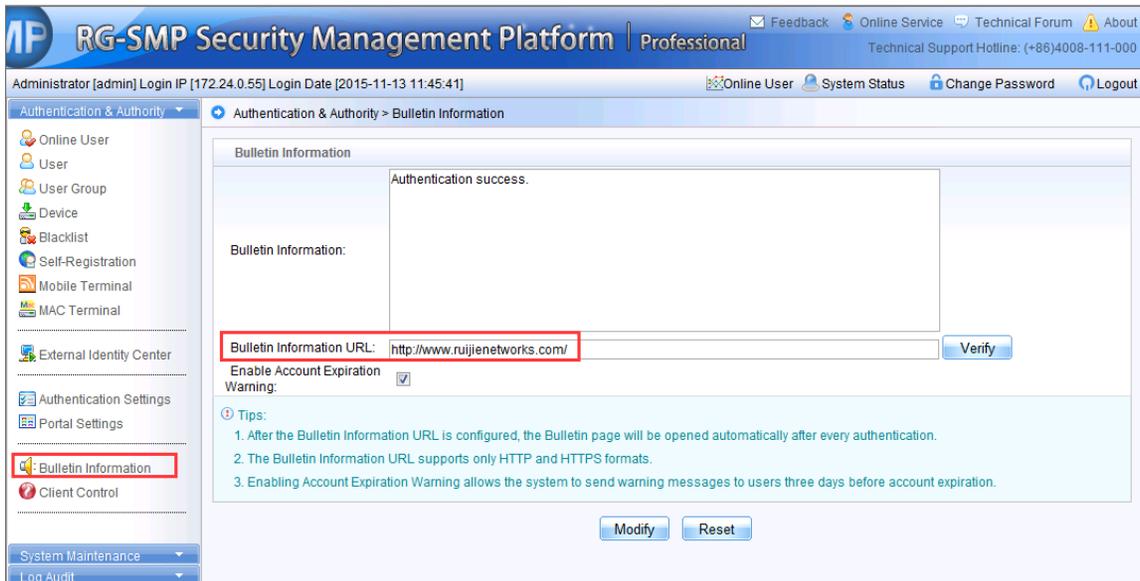
With this function configured, a user can see an online information notification after being authenticated, or a specified URL to release other notifications or advertisements after each authentication.

## Configuration Tips

N/A

## Configuration Steps

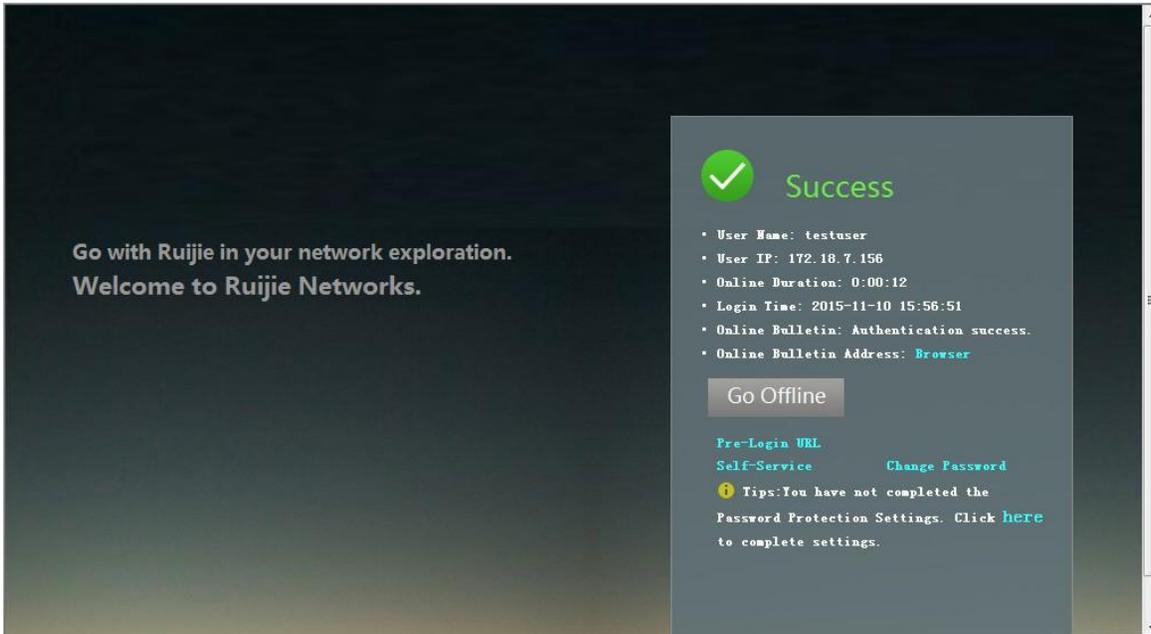
- 1) Choose **Authentication & Authority > Bulletin Information** to enter the **Bulletin Information** page, and configure the **Bulletin Information URL**.



- 2) Click **Modify** to save the settings.

## Terminal Authentication

- 1) The following page is displayed if Web authentication of a user is successful.



2) The configured online bulletin link is displayed on the authentication success page. Click this **Browser** hyperlink in **Online Bulletin Address** field to open the website such as <http://www.ruijienetworks.com/>.



#### Note

If the mode of overwriting online bulletin page is enabled, the online bulletin page cannot be displayed. Therefore, a user cannot proactively go offline. In this case, the user can go offline by accessing the self-service platform at <http://smpip/smp/selfservice>.



Note



Note

Or, during the wired Web authentication, do not close the authentication success page. If this page is closed, RG-SMP will force the user offline three heartbeat periods later.



Note



Note

Or, configure a traffic-based keepalive threshold. After a user is authenticated in wireless mode and goes online, if the traffic generated in a period of time is smaller than the threshold, the user will be forced to go offline.

## Client Anti-Crack

### Function Description

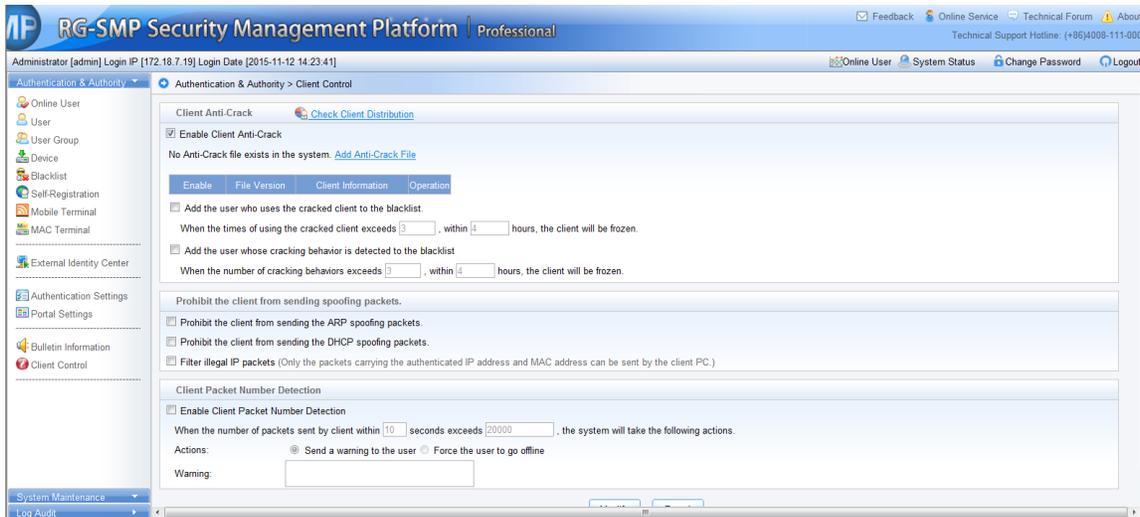
This section describes how to configure the client anti-crack function.

## Configuration Tips

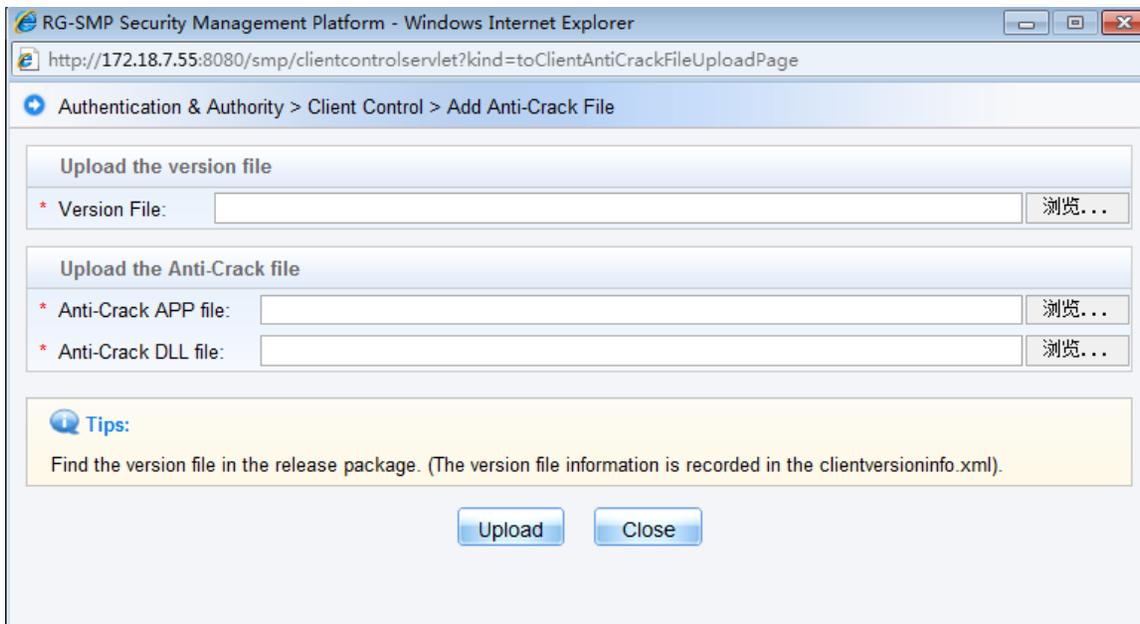
N/A

## Configuration Steps

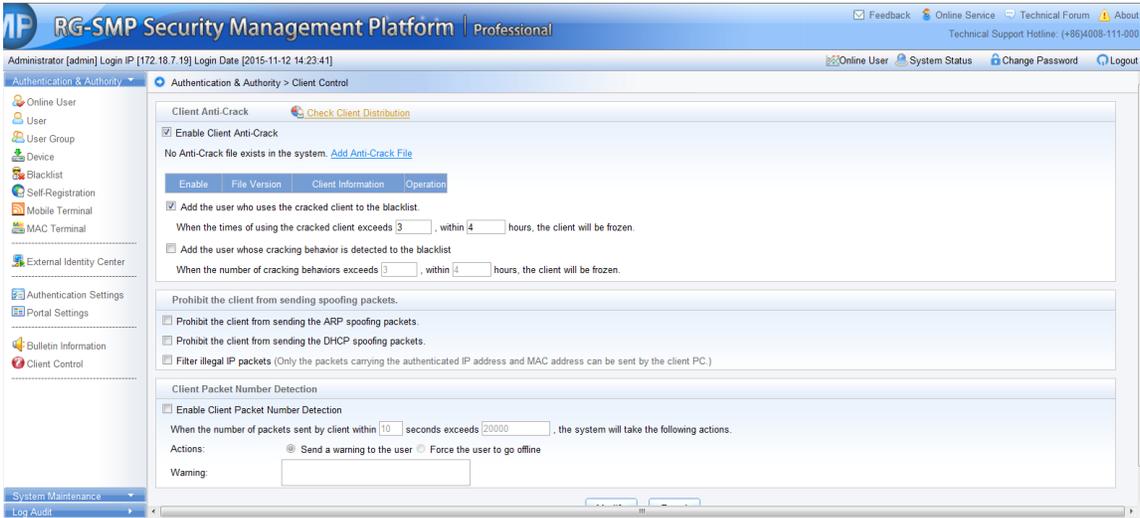
- 1) Choose **Authentication & Authority > Client Control** to enter the **Client Control** page. Check the **Enable Client Anti-Crack** box to enable this function.



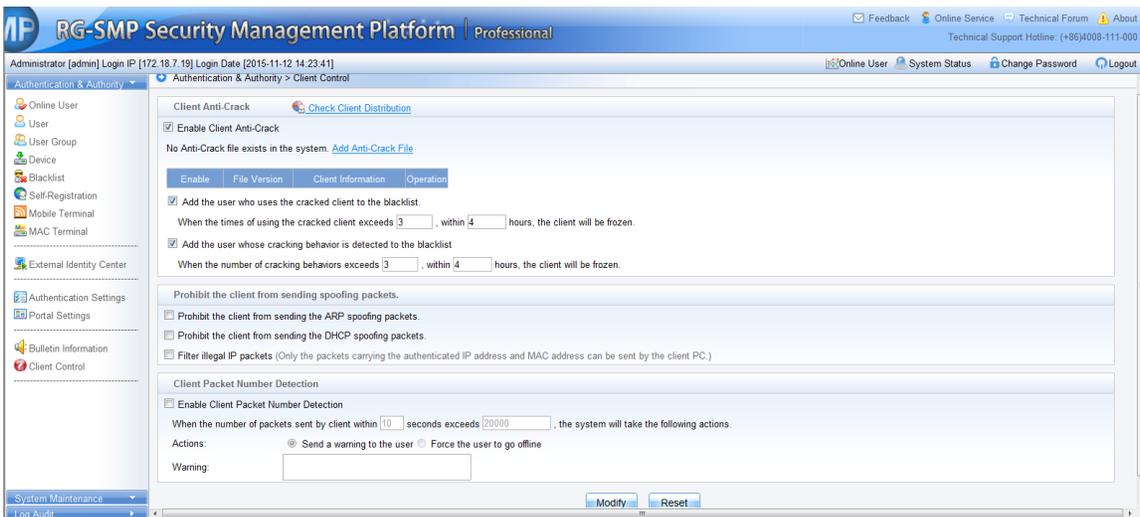
- 2) Click **Add Anti-Crack File** to import **Version File**, an **Anti-Crack APP File**, and **Anti-Crack DLL File** for client control.



- 3) Check the **Add the user who uses the cracked client to the blacklist** box, to configure the maximum number of times a cracked client can be used within a specified period before the client is frozen.



4) Check the **Add the user whose cracking behavior is detected to the blacklist** box to configure the maximum number of cracking behaviors anti detected within a specified period before a client is frozen.



## System Maintenance

## SMS Settings

## Function Description

This section describes how to configure the SMS service.

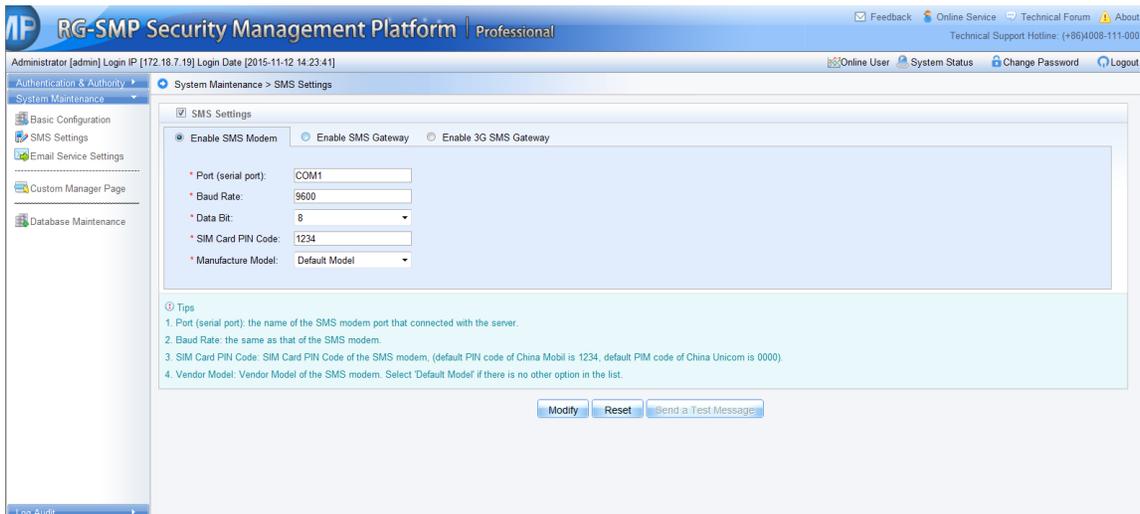
## Configuration Tips

N/A

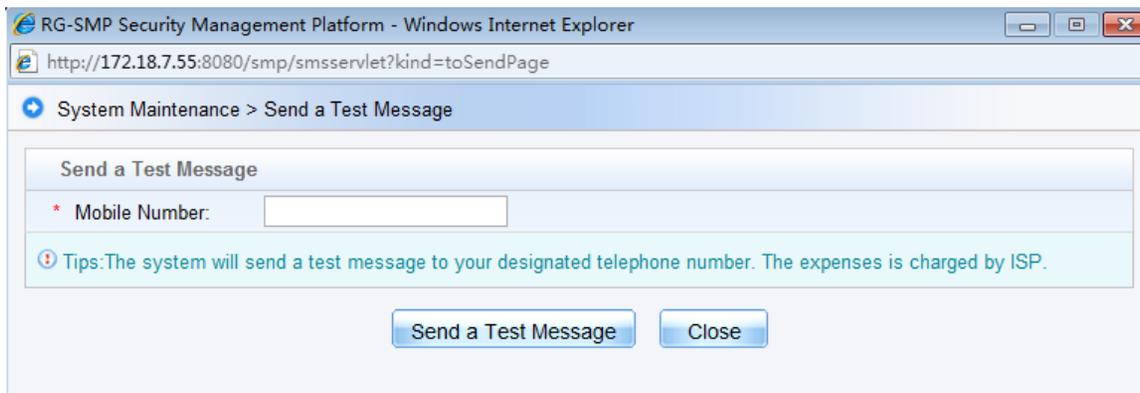
## Configuration Steps

### Configuring the SMS Modem

- 1) Choose **System Maintenance > SMS Settings** to enter the SMS configuration page. Select **Enable SMS Modem**.

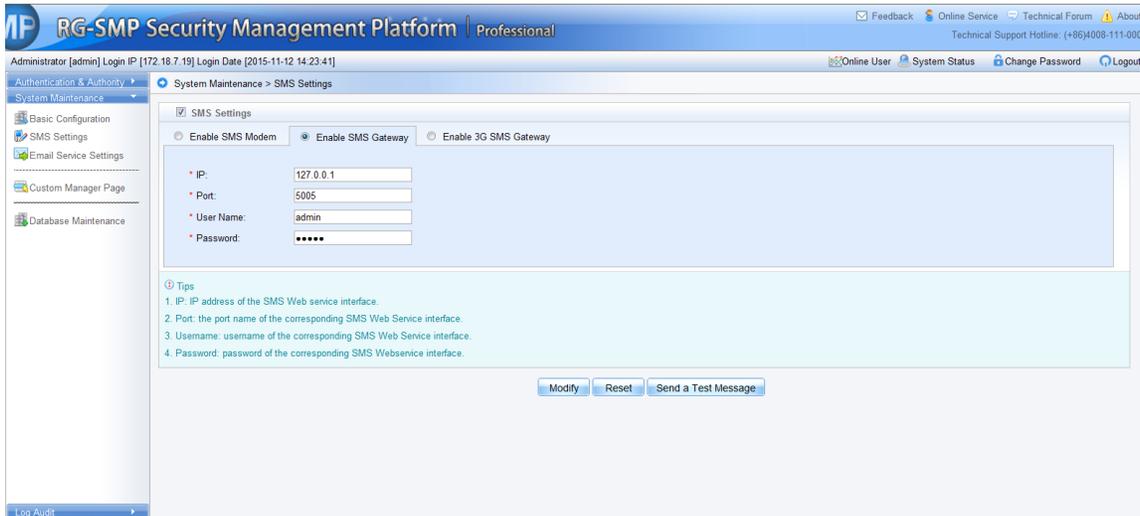


- 2) Configure parameters related to the SMS modem, and click **Modify** to save the settings. Click **Send a Test Message** to test the configuration.

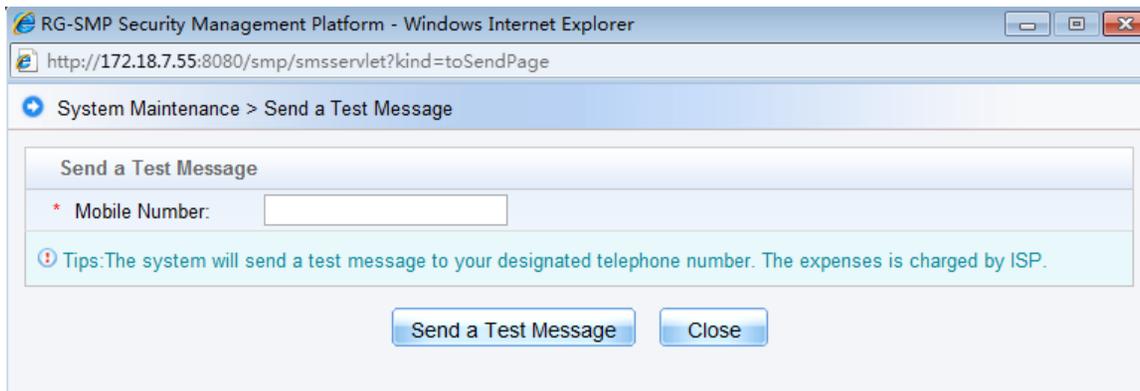


### Configuring the SMS Gateway

- 1) Choose **System Maintenance > SMS Settings** to enter the SMS configuration page. Select **Enable SMS Gateway**.



2) Configure parameters related to the SMS gateway, and click **Modify** to save the settings. Click **Send a Test Message** to test the configuration.



## Email Service Settings

### Function Description

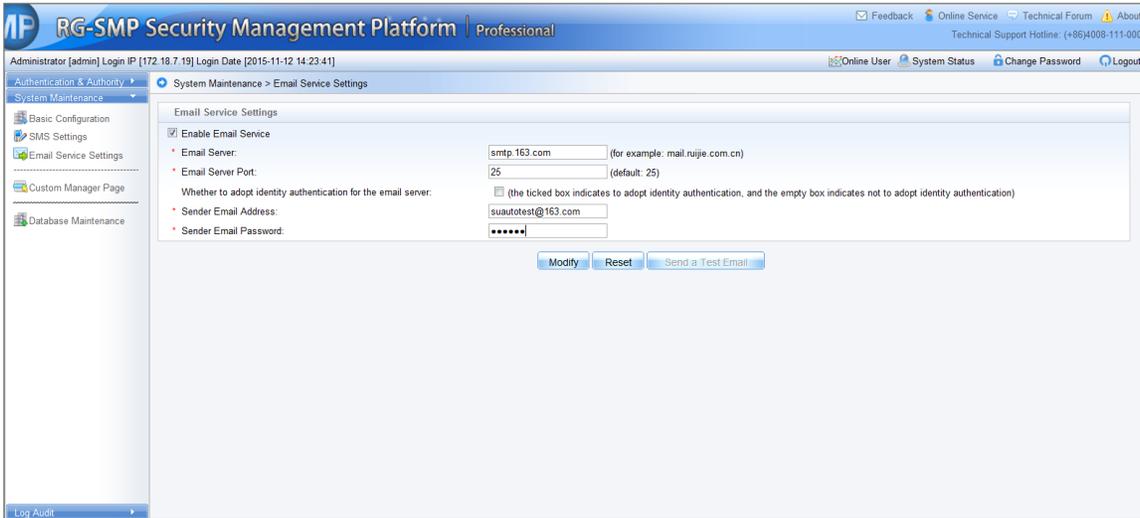
This section describes how to configure the Email service.

### Configuration Tips

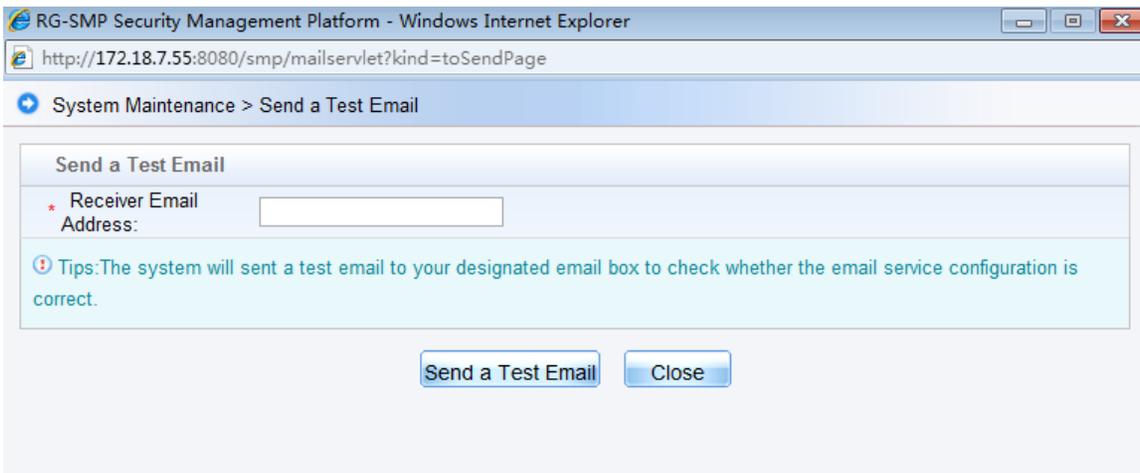
N/A

### Configuration Steps

1) Choose **System Maintenance > Email Service Settings** to enter the Email service configuration page. Check the **Enable Email Service** box.



2) Configure parameters related to the Email service, and click **Modify** to save the settings. Click **Send a Test Email** to test the configuration.



## Custom Manager Page

### Function Description

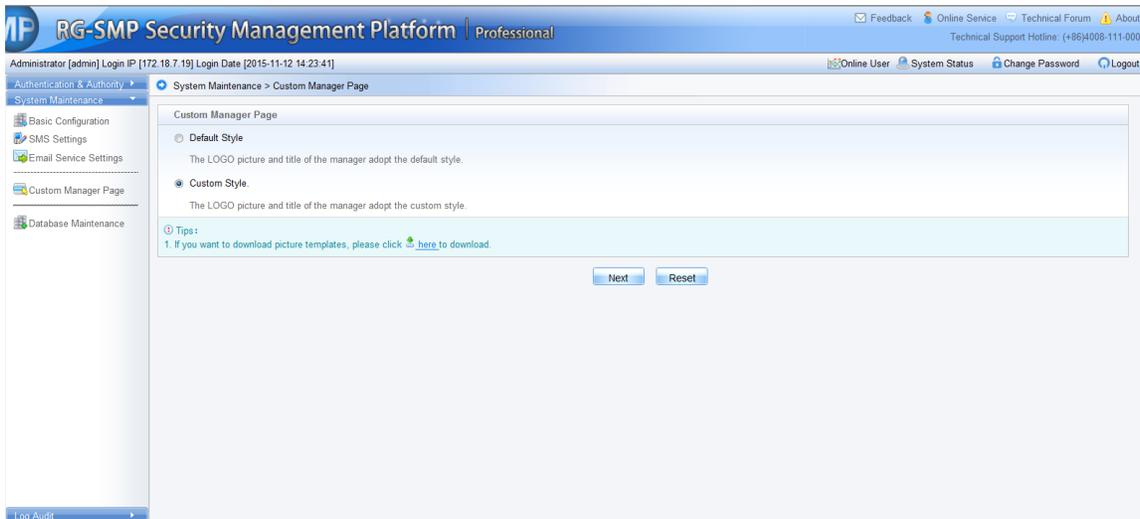
This section describes how to customize the background picture of the RG-SMP management platform. When customizing the background pictures for the first time, you need to customize that of the login page, title page, and wizard page in sequence. The later change requires no order.

### Configuration Tips

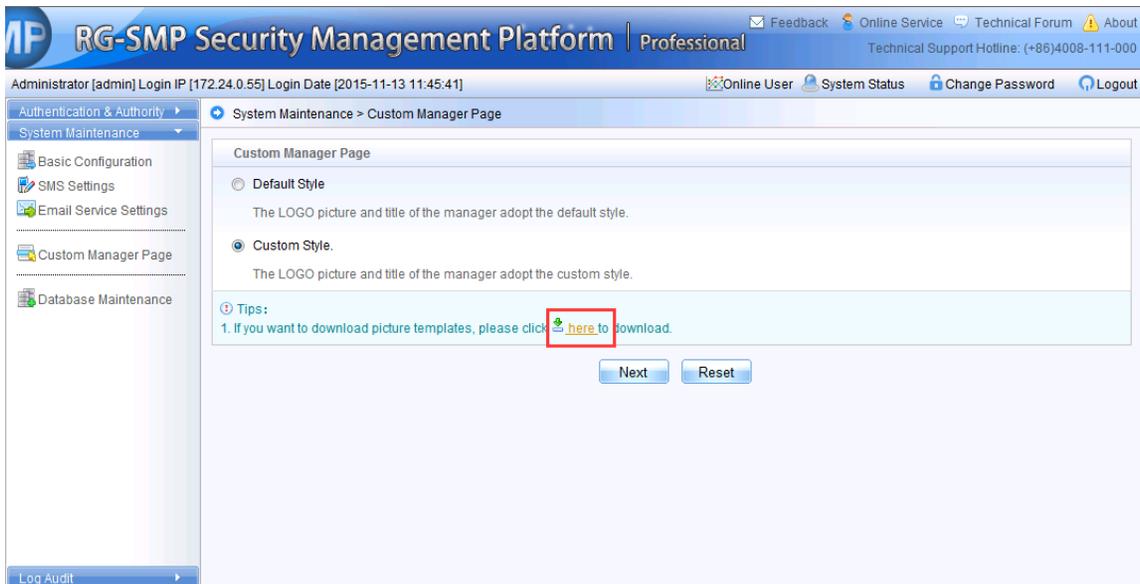
N/A

## Configuration Steps

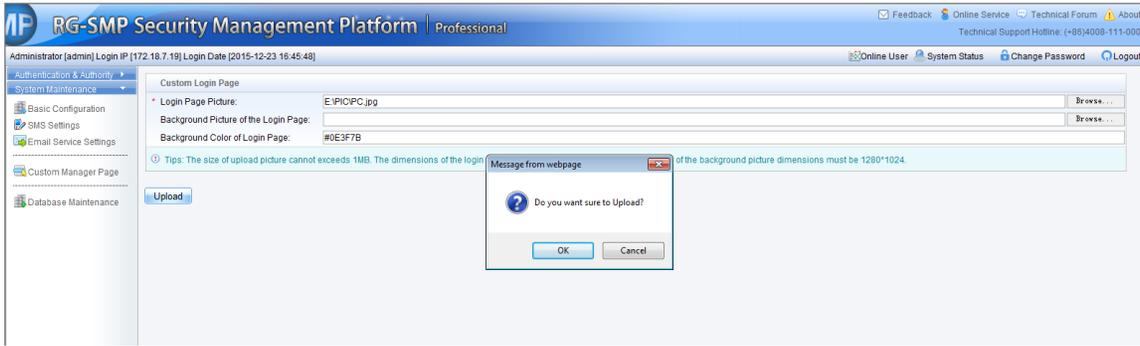
- 1) Choose **System Maintenance > Custom Manager Page** to enter the picture customization page.



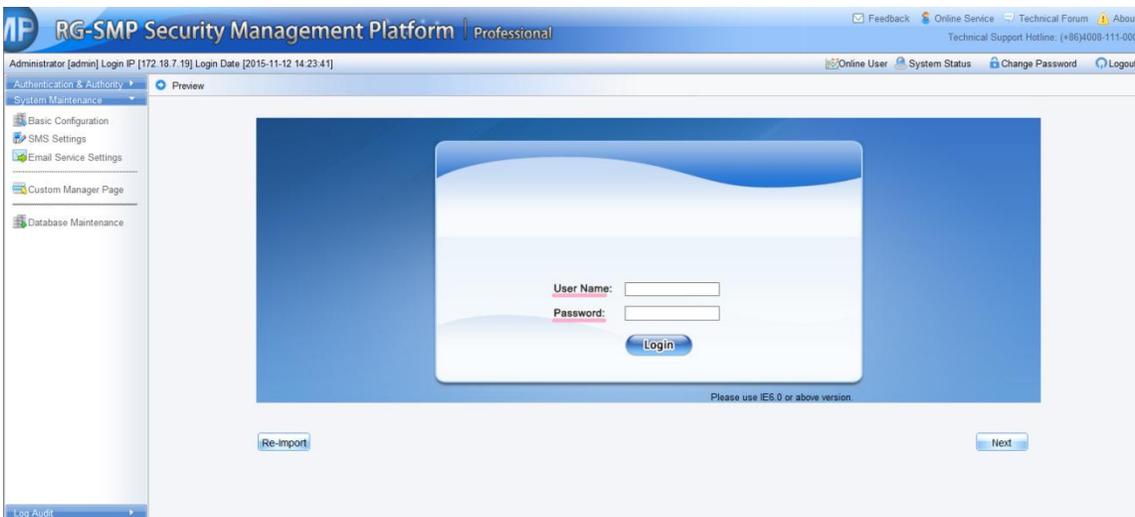
- 2) Select **Custom Style**, and click **Next** to start customization. You can click **here** in **Tips** to download the picture template.



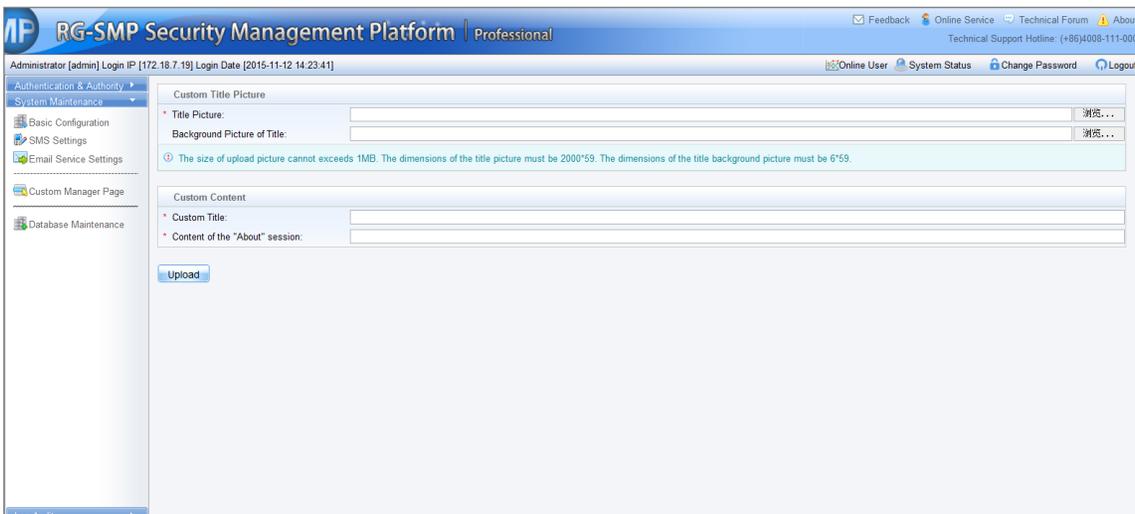
- 3) Select the **Login Page Picture**, **Background Picture of the Login Page**, and **Background Color of Login Page**, and click **Upload** to upload these pictures. Then, go to the preview page.



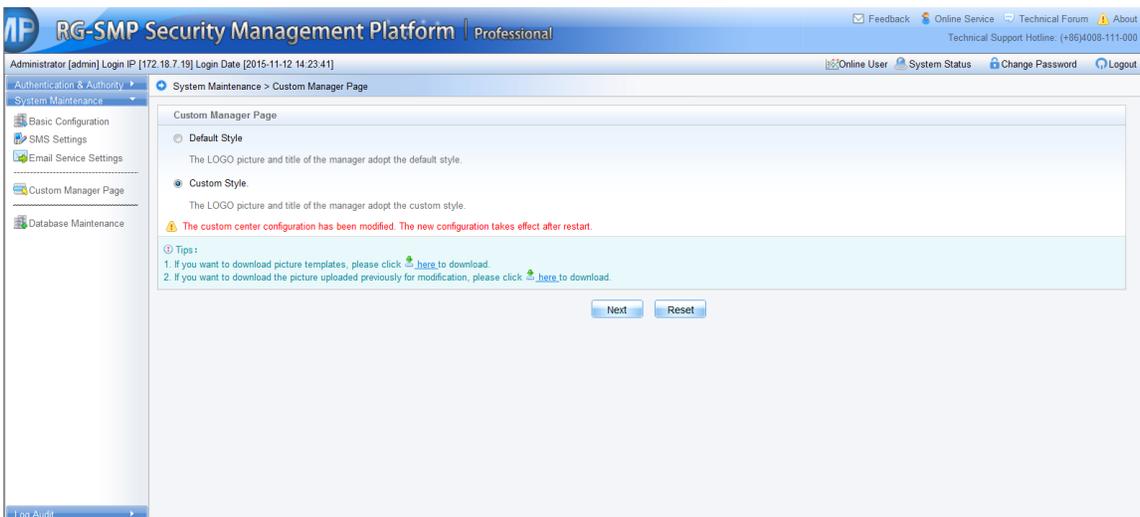
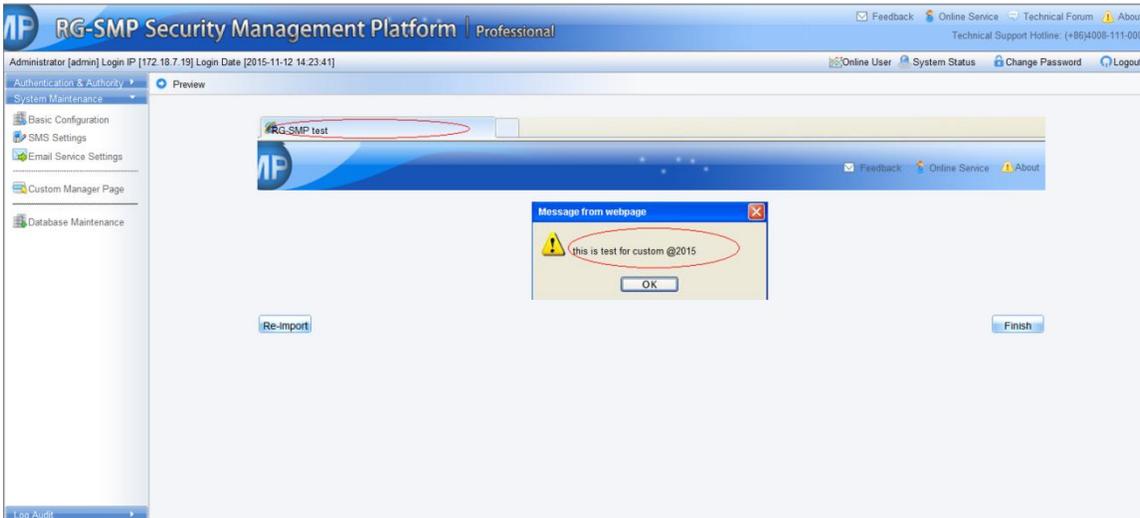
4) Click **Re-import** to import another pictures for the login page. Click **Next** to customize the title pictures.



5) Select the title picture and text description, and click **Upload**. Then, go to the preview page.



6) Click **Re-import** to import the title picture and text description again. Click **Finish** to complete the settings.



7) Restart RG-SMP to enable changes.

## Database Maintenance

### Function Description

This section describes how to back up the database.

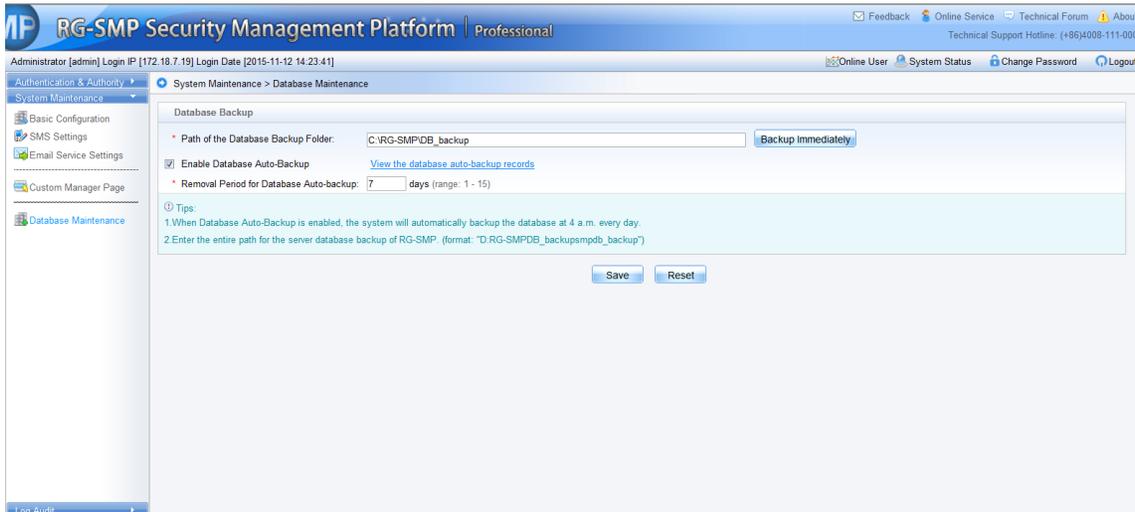
### Configuration Tips

N/A

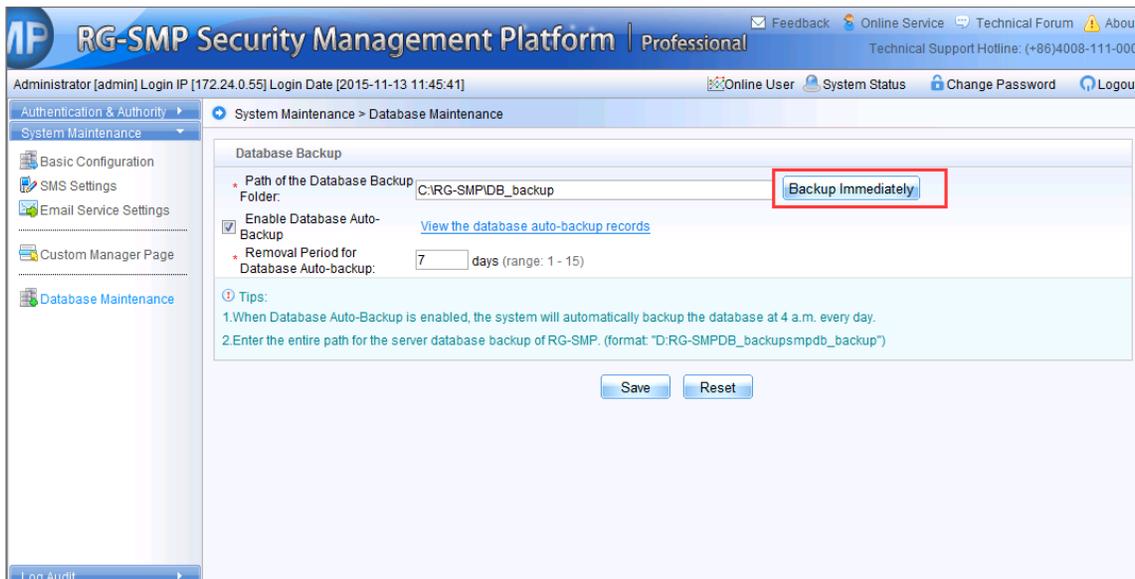
## Configuration Steps

### Manual Backup

- 1) Choose **System Maintenance > Database Maintenance** to enter the **Database Maintenance** page.



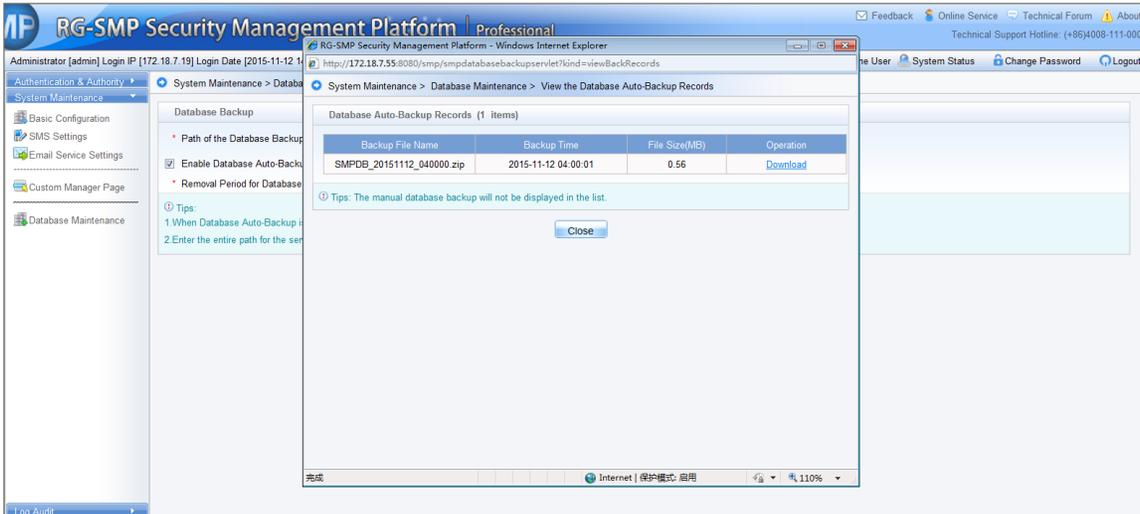
- 2) On the **Database Maintenance** page, click **Backup Immediately** to back up the current database immediately.



- 3) After backing up is complete, you can save the backup file.

### Automatic Backup

- 1) Choose **System Maintenance > Database Maintenance** to enter the **Database Maintenance** page.

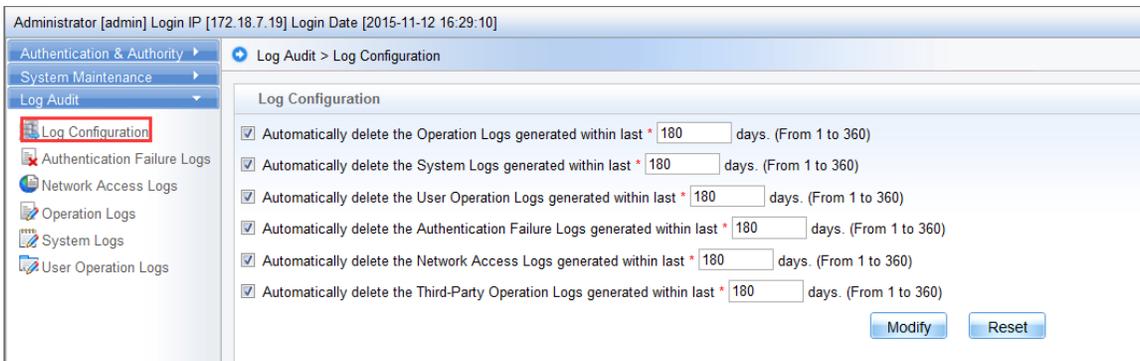


2) On the **Database Maintenance** page, check the **Enable Database Auto-Backup** box, configure the backup path, and click **Save** to save the settings.

## Log Audit

### Log Configuration

1) Choose **Log Audit > Log Configuration**, and configure the automatic deletion time for each type of logs.



### Authentication Failure Logs

1) Choose **Log Audit > Authentication Failure Logs** to view authentication failure logs of users.

Administrator [admin] Login IP [172.18.7.19] Login Date [2015-11-12 16:29:10]

Log Audit > Authentication Failure Logs > Query Logs

User Name:  Authentication Date: 2015-11-12 - 2015-11-12

User IP:  Cause of Failure:  [Query](#) [Reset](#) [Advanced Search](#)

[Delete](#) [Delete All](#)

Totally 18 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [Go](#)

All Name	User Name	Authentication Date	NAS IP	User IP	User MAC	Cause of Failure	Operation
<input type="checkbox"/>	Henry	2015-11-12 15:45:42	10.1.1.28	10.1.1.116	DCC7937A73A8	The number of PCs allowed to be logged simultaneously by the same account has reached the upper limit specified by the administrator.	<a href="#">View</a>
<input type="checkbox"/>	dcc7937a73a8	2015-11-12 15:40:43	10.1.1.28		DCC7937A73A8	The mobile terminal has not been registered or MAC Terminal does not exist.	<a href="#">View</a>
<input type="checkbox"/>	Henry	2015-11-12 15:31:18	10.1.1.28	10.1.1.105	848E0CBC111B	The user is not found.	<a href="#">View</a>
<input type="checkbox"/>	hujq	2015-11-12 14:43:17	10.1.1.28	10.1.1.105	848e0cbc111b	The authenticator returns an authentication failure message (for unknown reason)	<a href="#">View</a>
<input type="checkbox"/>	hujq	2015-11-12 14:43:17	10.1.1.28	10.1.1.105	848E0CBC111B	No response from the Radius server 172.18.34.57	<a href="#">View</a>
<input type="checkbox"/>	hujq	2015-11-12 14:43:13	10.1.1.28	10.1.1.105	848E0CBC111B	No response from the Radius server 172.18.34.57	<a href="#">View</a>
<input type="checkbox"/>	98fae35ae0c	2015-11-12 14:39:39	10.1.1.28		98FAE35AE0C	The mobile terminal has not been registered or MAC Terminal does not exist.	<a href="#">View</a>
<input type="checkbox"/>	848e0cbc111b	2015-11-12 14:26:36	10.1.1.28		848E0CBC111B	The mobile terminal has not been registered or MAC Terminal does not exist.	<a href="#">View</a>
<input type="checkbox"/>	848e0cbc111b	2015-11-12 14:26:36	10.1.1.28		848E0CBC111B	The mobile terminal has not been registered or MAC Terminal does not exist.	<a href="#">View</a>

## Network Access Logs

- 1) Choose **Log Audit > Network Access Logs** to view network access logs of users.

Administrator [admin] Login IP [172.18.7.19] Login Date [2015-11-12 16:29:10]

Log Audit > Network Access Logs > Query Logs

User Name:  User IP:  Offline Cause: All

Login Time: 2015-11-12 0:0:0 Logout Time: 2015-11-12 23:59:59 [Query](#) [Reset](#) [Advanced Search](#)

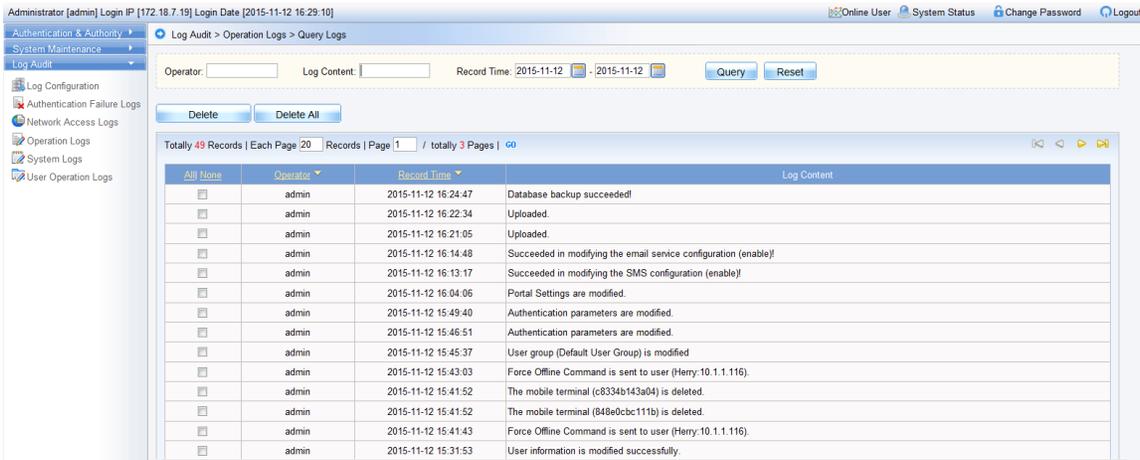
[Delete](#) [Export Query Results](#) [Delete All](#) [Network Traffic and Online Duration Report](#)

Totally 17 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [Go](#)

All Name	User Name	User IP	Full Name	NAS IP	Login Time	Logout Time	Offline Cause	Operation
<input type="checkbox"/>	Henry	10.1.1.116	Henry	10.1.1.28	2015-11-12 15:46:57	2015-11-12 15:57:27	The device detects that the user goes offline.	<a href="#">View</a>
<input type="checkbox"/>	Henry	10.1.1.105	Henry	10.1.1.28	2015-11-12 15:32:59	2015-11-12 15:46:57	The number of online users has exceeded the limit of terminals using the same account.	<a href="#">View</a>
<input type="checkbox"/>	Henry	10.1.1.116	Henry	10.1.1.28	2015-11-12 15:43:22	2015-11-12 15:44:19	User goes offline.	<a href="#">View</a>
<input type="checkbox"/>	Henry	10.1.1.116	Henry	10.1.1.28	2015-11-12 15:42:04	2015-11-12 15:43:03	Be forced offline.	<a href="#">View</a>
<input type="checkbox"/>	Henry	10.1.1.116	Henry	10.1.1.28	2015-11-12 15:41:11	2015-11-12 15:41:43	Be forced offline.	<a href="#">View</a>
<input type="checkbox"/>	hujq	10.1.1.105	hujq	10.1.1.28	2015-11-12 15:16:45	2015-11-12 15:31:04	User goes offline.	<a href="#">View</a>
<input type="checkbox"/>	hujq	10.1.1.105	hujq	10.1.1.28	2015-11-12 15:12:49	2015-11-12 15:16:11	User goes offline.	<a href="#">View</a>
<input type="checkbox"/>	test	10.1.1.105	test	10.1.1.28	2015-11-12 14:50:37	2015-11-12 15:12:35	User goes offline.	<a href="#">View</a>
<input type="checkbox"/>	hujq	10.1.1.105	hujq	10.1.1.28	2015-11-12 14:43:53	2015-11-12 14:50:21	User goes offline.	<a href="#">View</a>
<input type="checkbox"/>	hujiaqi	10.1.1.105	hujiaqi	10.1.1.28	2015-11-12 14:27:01	2015-11-12 14:42:45	User goes offline.	<a href="#">View</a>
<input type="checkbox"/>	newuser	10.1.1.105	test	10.1.1.28	2015-11-12 14:25:21	2015-11-12 14:25:36	Be forced offline.	<a href="#">View</a>
<input type="checkbox"/>	newuser	10.1.1.105	test	10.1.1.28	2015-11-12 14:24:12	2015-11-12 14:25:20	Be forced offline.	<a href="#">View</a>
<input type="checkbox"/>	123 (Deleted)	10.1.1.118	123	10.1.1.28	2015-11-12 13:54:47	2015-11-12 13:55:20	Be forced offline.	<a href="#">View</a>

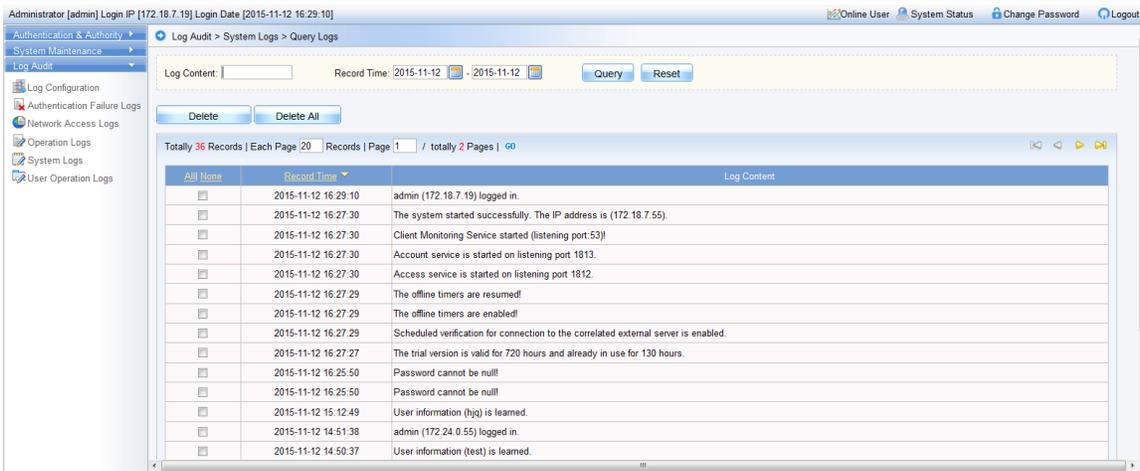
## Administrator Operation Logs

- 1) Choose **Log Audit > Operation Logs** to display the operation logs of the administrator.



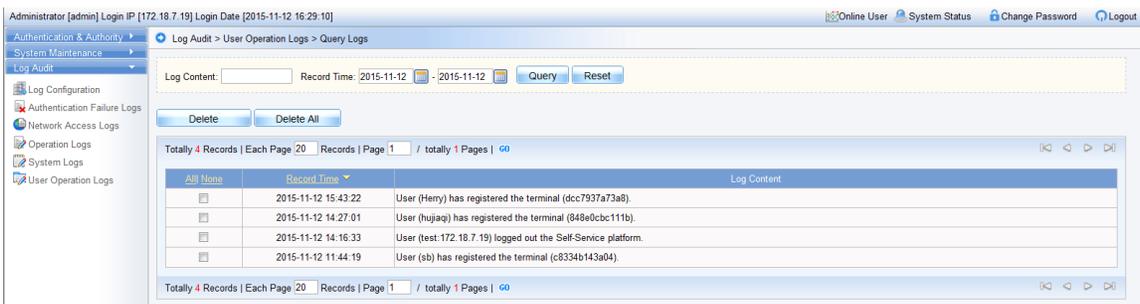
## System Logs

- 1) Choose **Log Audit > System Logs** to view the system logs.



## User Operation Logs

- 1) Choose **Log Audit > User Operation Logs** to view the operation logs of users.



## FAQ

- How to log in to RG-SMP for the first time?

Enter **http://local IP address:8080/smp/index.jsp** in the address bar of your browser. Enter the username (**admin**) and password (**11111111**) of the system administrator in the login page.

- Why does the system prompt database exception in an RG-SMP startup failure?

The database is configured incorrectly. Check whether the actual configurations of the database are consistent with the database configurations (including the server IP address, server port, database name, and username and password for login) in RG-SMP Service Manager.

- How to change the RG-SMP HTTP or HTTPS port for login?

Choose **System Maintenance > Basic Configuration**. Change the **HTTP Port** or **HTTPS Port** number. You can also enable or disable login to RG-SMP in HTTP or HTTPS mode.

The screenshot shows the 'Basic Configuration' page in the RG-SMP interface. The 'Server Parameter' section has 'HTTP Port' set to 8080 and 'HTTPS Port' set to 8443. The 'WebService Service Access Port' is set to 9090. The 'Client Communication Configuration' section includes: Server Communication Port (53), Client Communication Port (138), Client Communication Timeout (3 times), Client Communication Retransmissions (3 times), and Computer Protection Detection Period (5 minutes). There are 'Modify' and 'Reset' buttons at the bottom right.

- Why does the system prompt that session timed out and return to the login page when I click the View button?

Currently, RG-SMP allows logging in only through the Internet Explorer rather than through **My Computer** or **Resource Manager**. When the problem occurs, restart the Internet Explorer and enter the URL of RG-SMP in the address bar.

- Why does the system prompt existence of unsupported characters?

Currently, RG-SMP supports Chinese characters, letters, numbers, and common punctuation marks listed below.

`	~	!	@	#	\$	%	^	&	*
(	)	(	)	[	]	{	}	_	'
_	-	=	+	,	.	&	'	+	,
;	:	“	”	‘	’	<	>	%	

'	,	“	”	...	%o	`	o	]	^
《	》	【	】	!	"	#	\$		*
;	<	=	>	—	.	/	:	?	@
{		}	~	[	\				