Configuration Guide

RG-SMP Professional_2.63_EN_Build20151106

Copyright Statement

Exemption Statement

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

Obtaining Technical Assistance

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

Contents

1 Configuration Guide

This chapter describes how to configure the typical functions of RG-SMP. After reading this chapter, you will have a preliminary understanding of the functions of RG-SMP and be able to complete basic security management configuration.

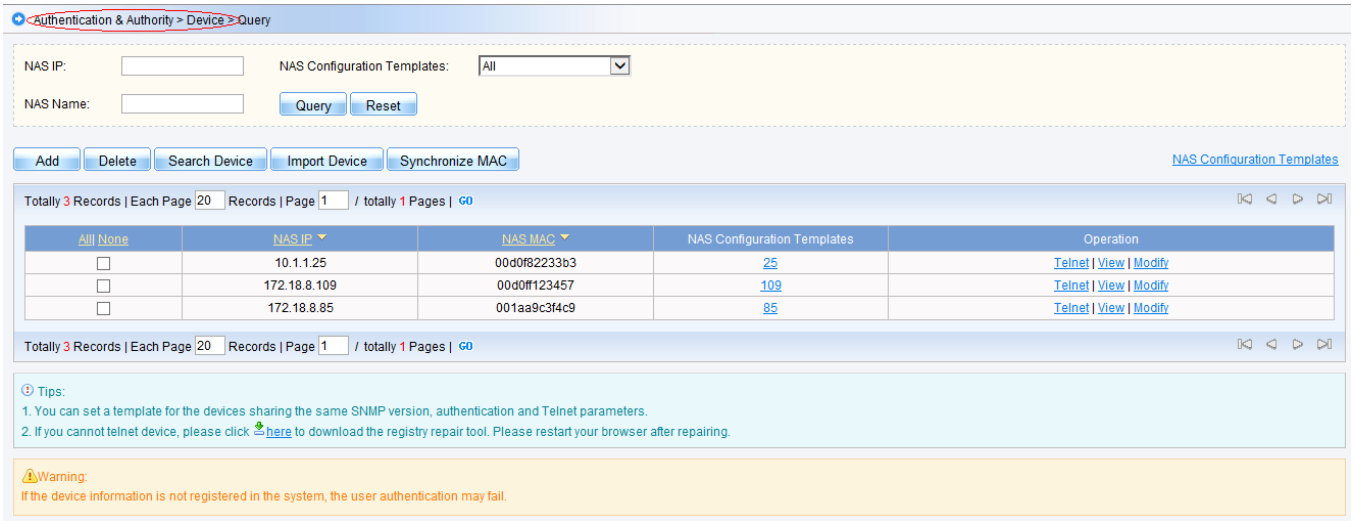
This chapter is organized as follows:

1.1 User Access – Wired Access

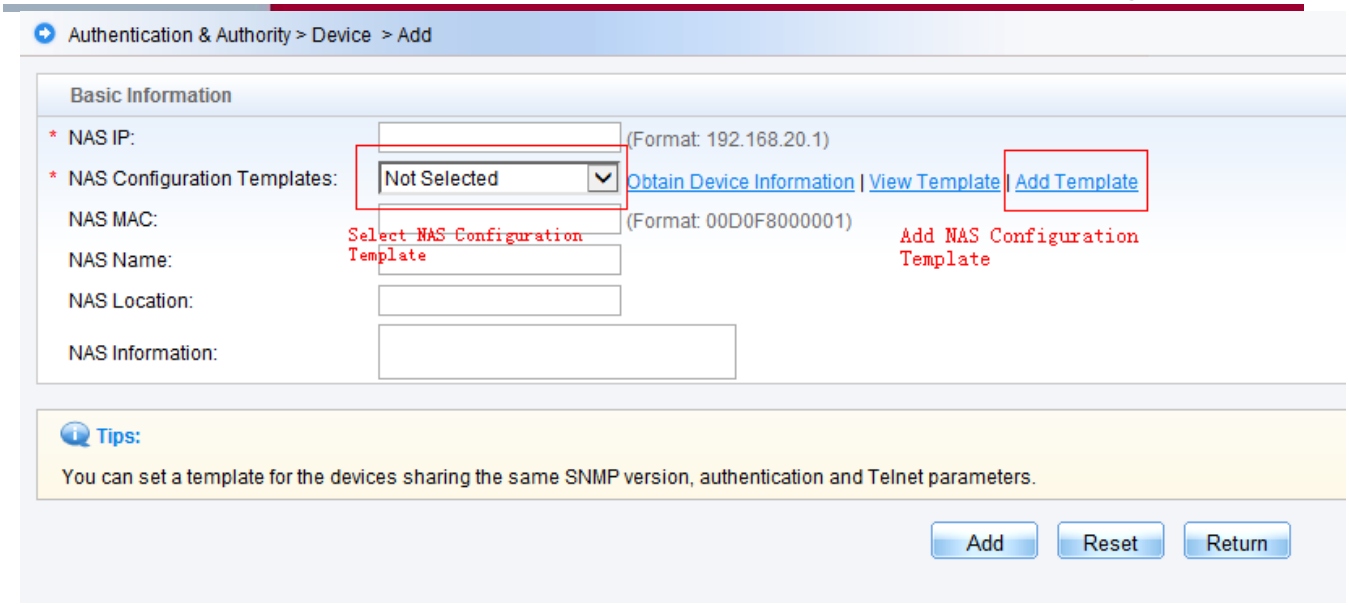
This section describes how to configure RG-SMP for authentication in wired access.

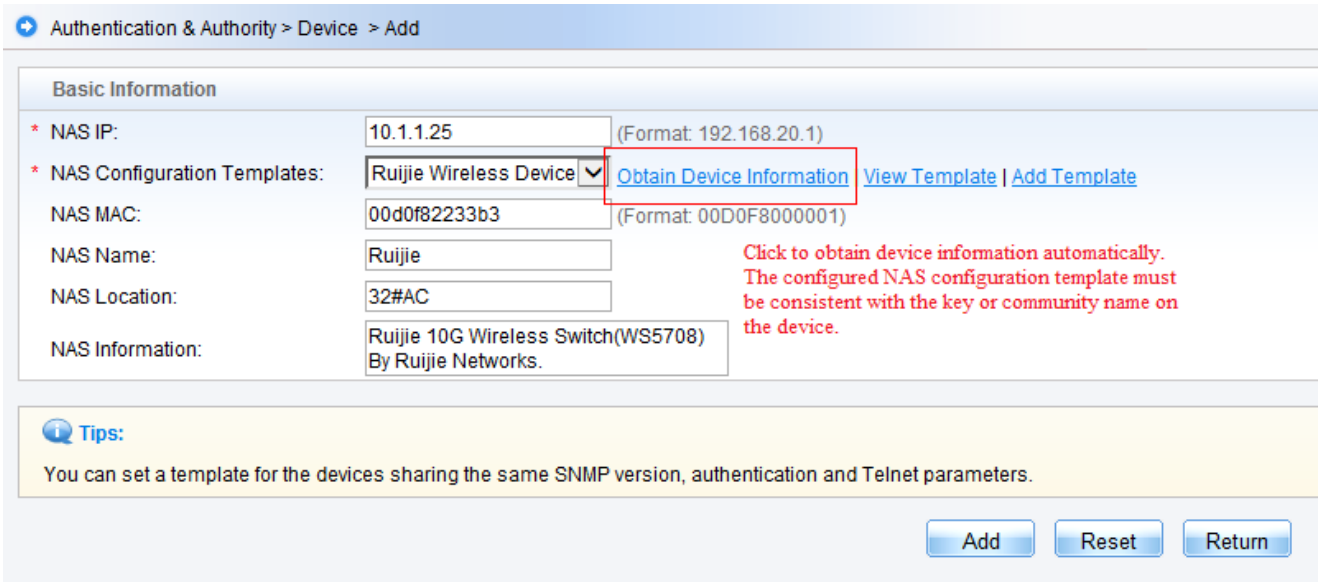
1.1.1 Adding Devices

1. Go to **Authentication & Authority** > **Device** from the left menu.

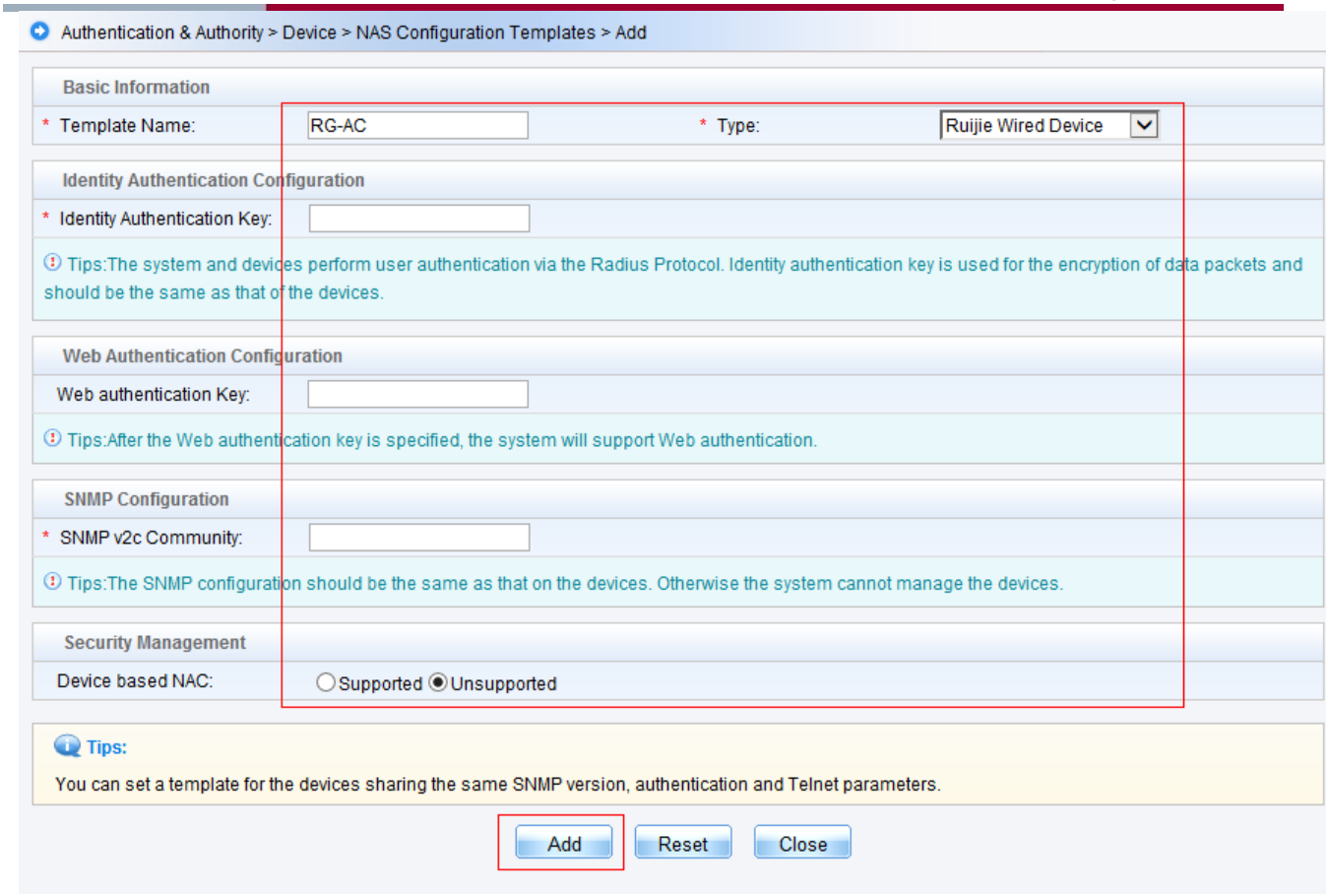


2. Click **Add**. The **Add** window is displayed. Fill in the **NAS IP** and **NAS Configuration Templates** fields (you can select an existing NAS configuration template or add one). Click **Obtain Device Information**. RG-SMP will obtain device information automatically.





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



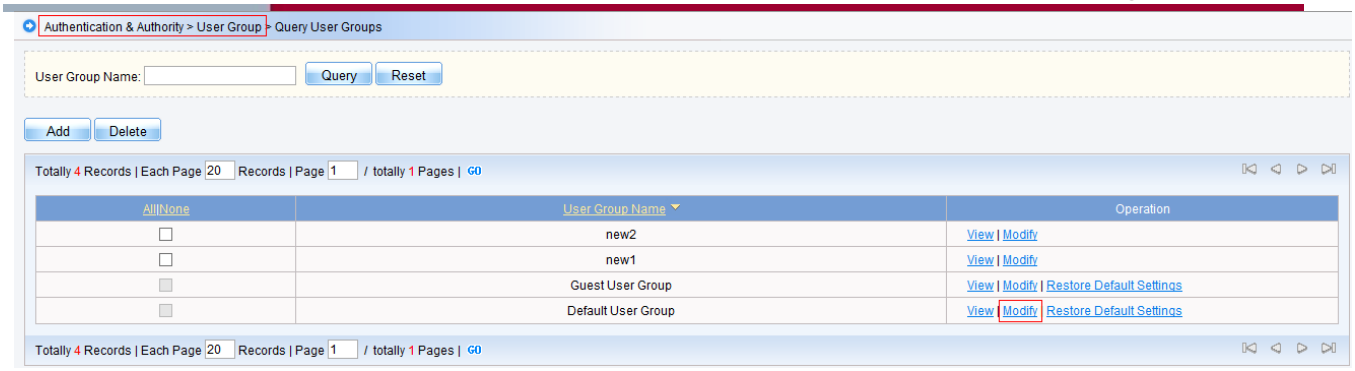
3. After device information is obtained successfully, click **Add**.

Note:

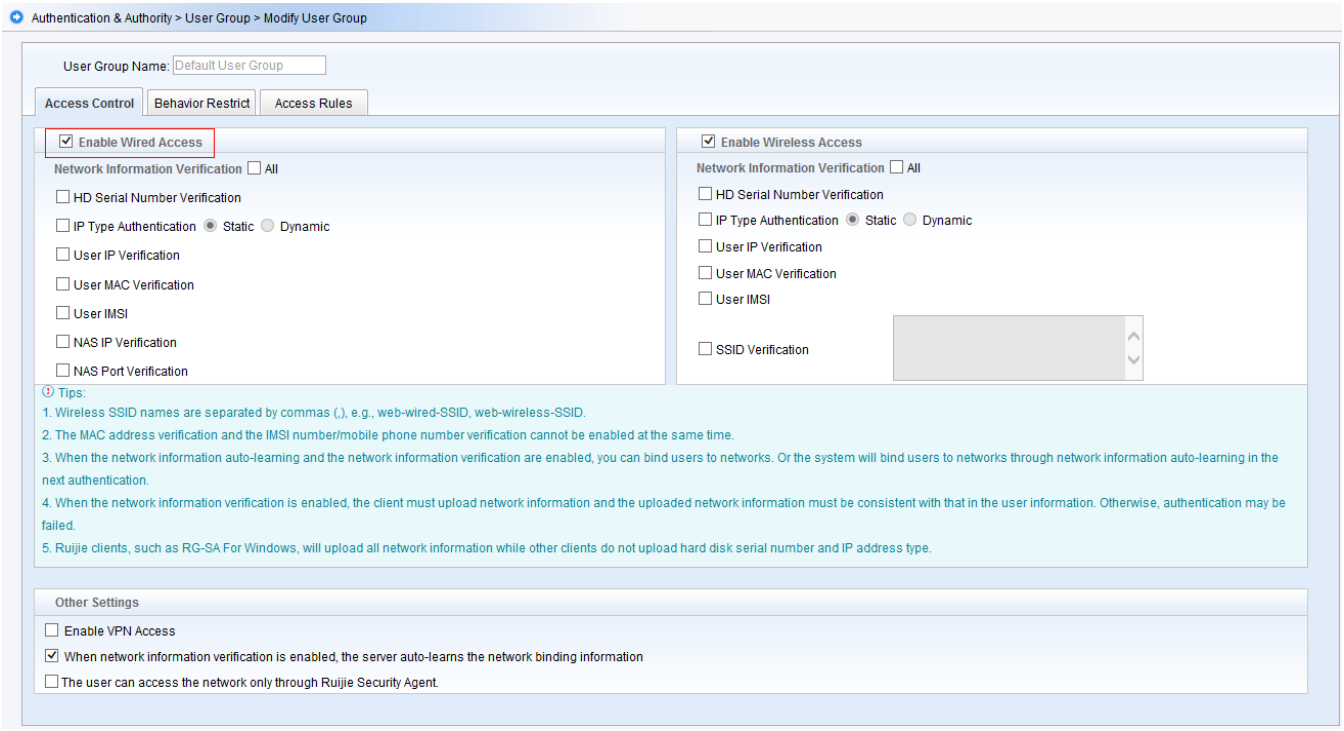
If device information fails to be obtained, check whether the device IP address and SNMPv2c Community are configured correctly. If yes, check whether the communication between RG-SMP and the device is normal. Some devices (for example, RG-ePortal) can be added even when their information cannot be obtained.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

1.1.2 Enabling Wired Access

1. Go to **Authentication & Authority** > **User Group** from the left menu. Click **Add** or **Modify** to access the configuration window of the corresponding user group.



2. Check the **Enable Wired Access** check box and save the configuration.



1.2 User Access – Wireless Access

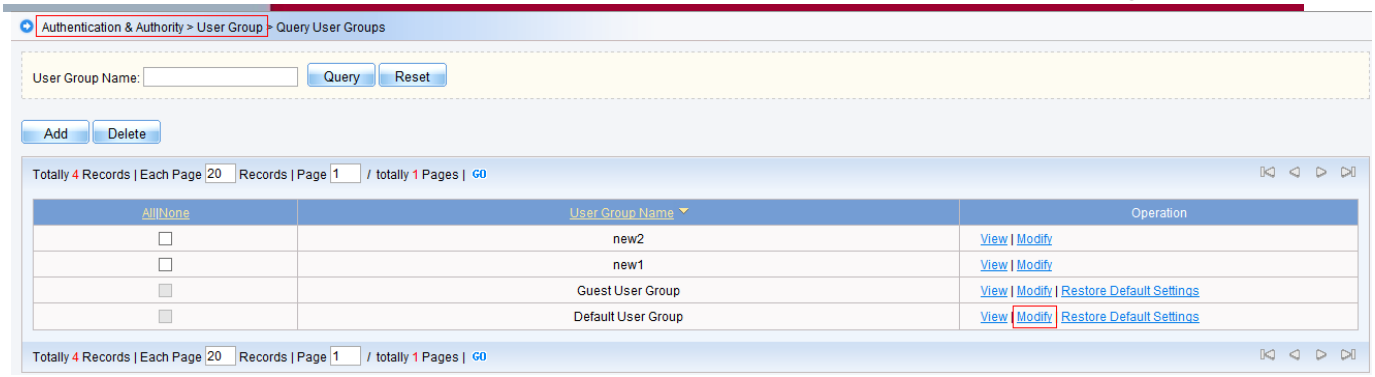
This section describes how to configure RG-SMP for authentication in wireless access.

1.2.1 Adding Devices

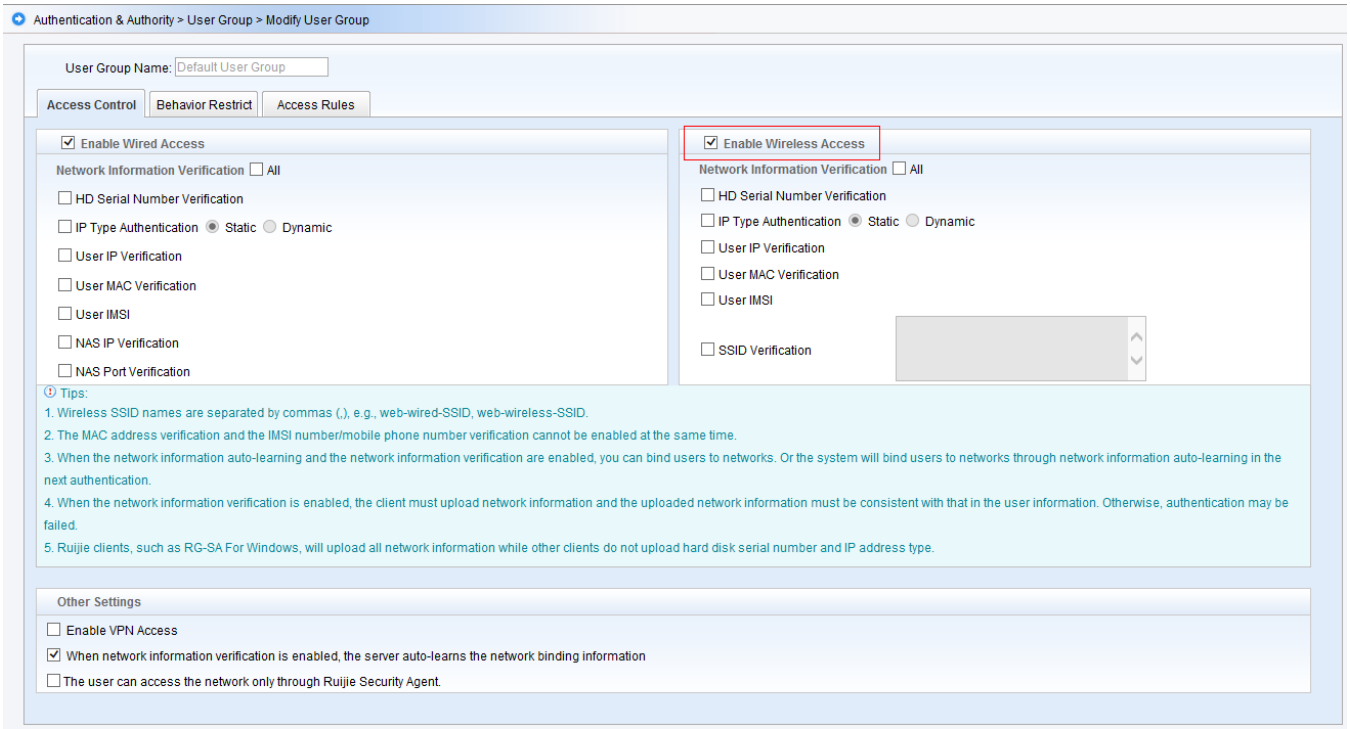
See section 1.1.1 "Adding Devices."

1.2.2 Enabling Wireless Access

1. Go to **Authentication & Authority** > **User Group** from the left menu. Click **Add** or **Modify** to access the configuration window of the corresponding user group.



2. Check the **Enable Wireless Access** check box and save the configuration.

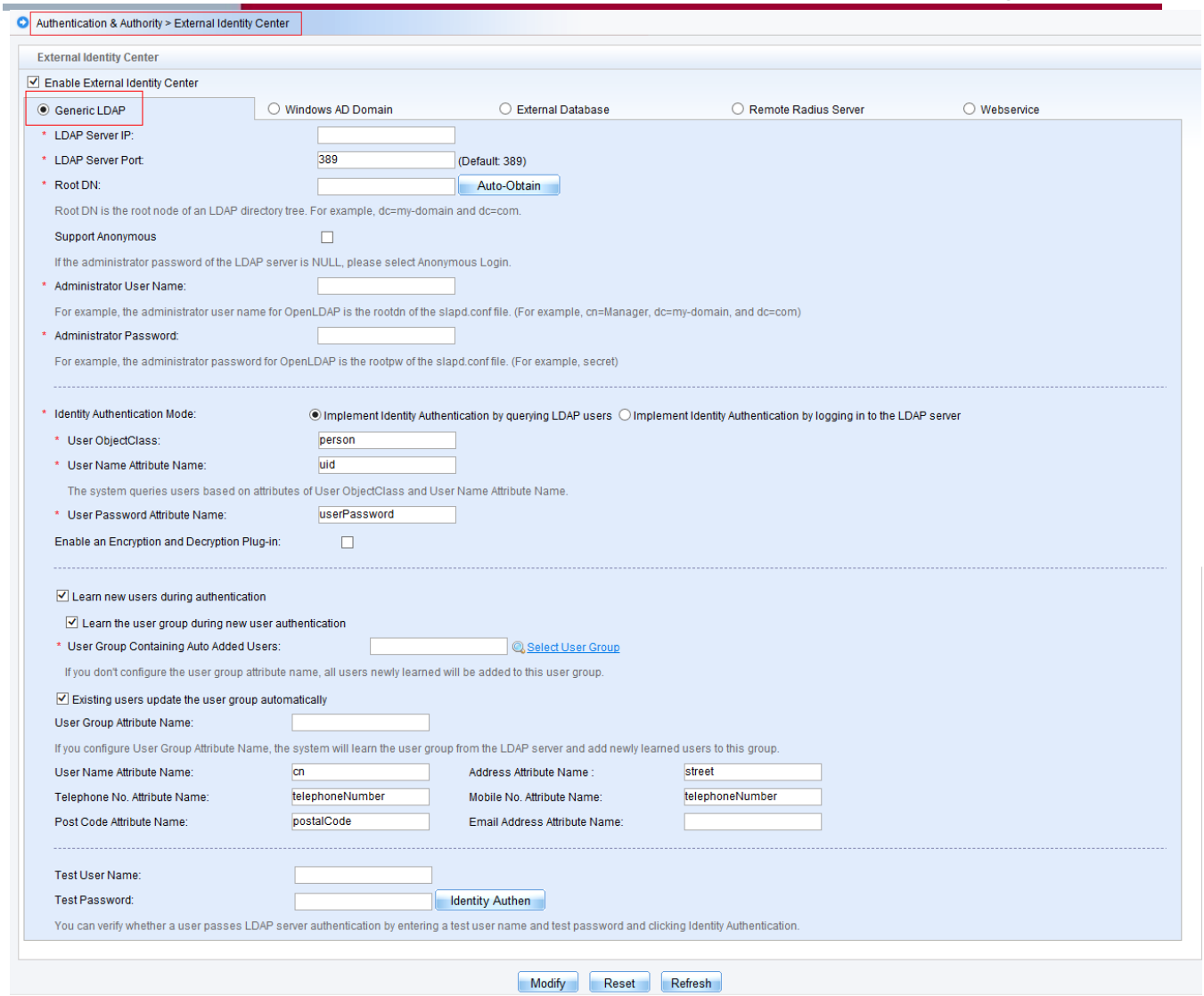


1.3 User Access – Correlation with External Identity Center

This section describes how to configure RG-SMP for correlation with the external identity center.

1.3.1 Authentication Using Generic LDAP Server

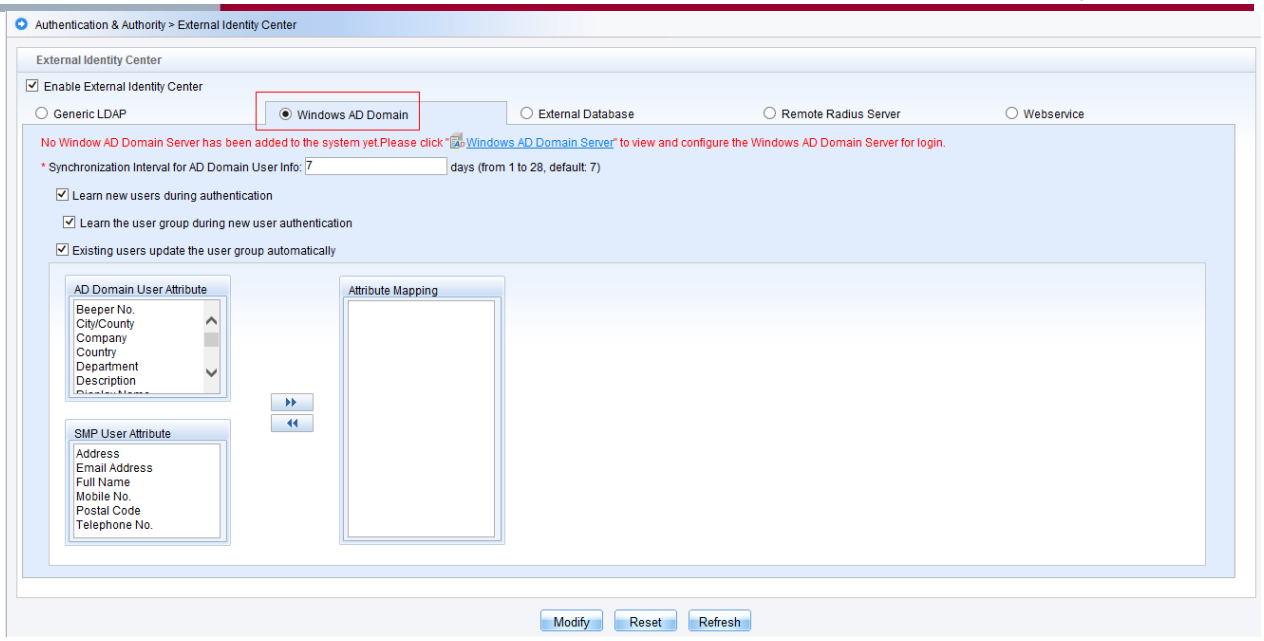
1. Go to **Authentication & Authority** > **External Identity Center**.
2. Check the **Enable External Identity Center** check box, click the **Generic LDAP** tab, and configure correlation with LDAP.



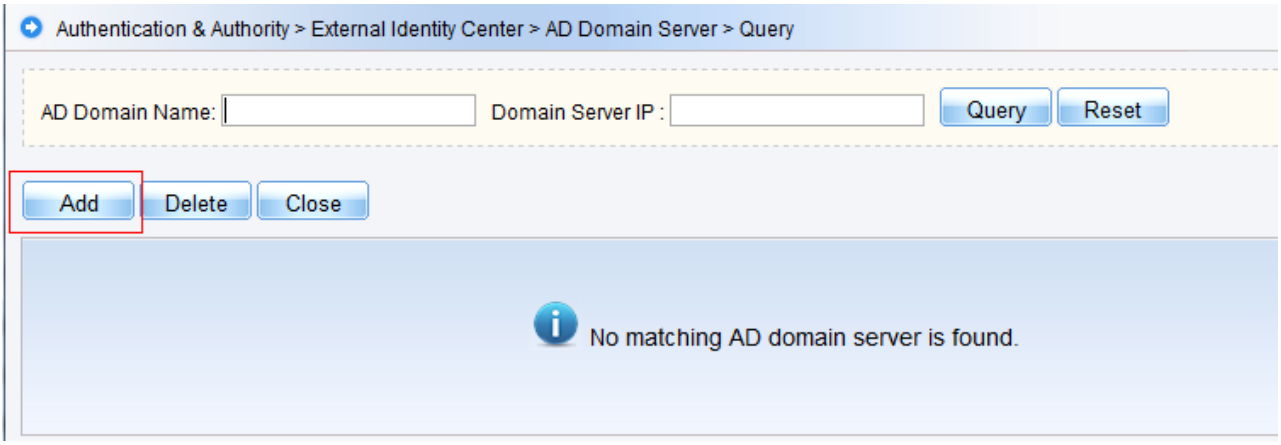
3. Click **Modify** to save the configuration.

1.3.2 Authentication Using Windows AD Domain

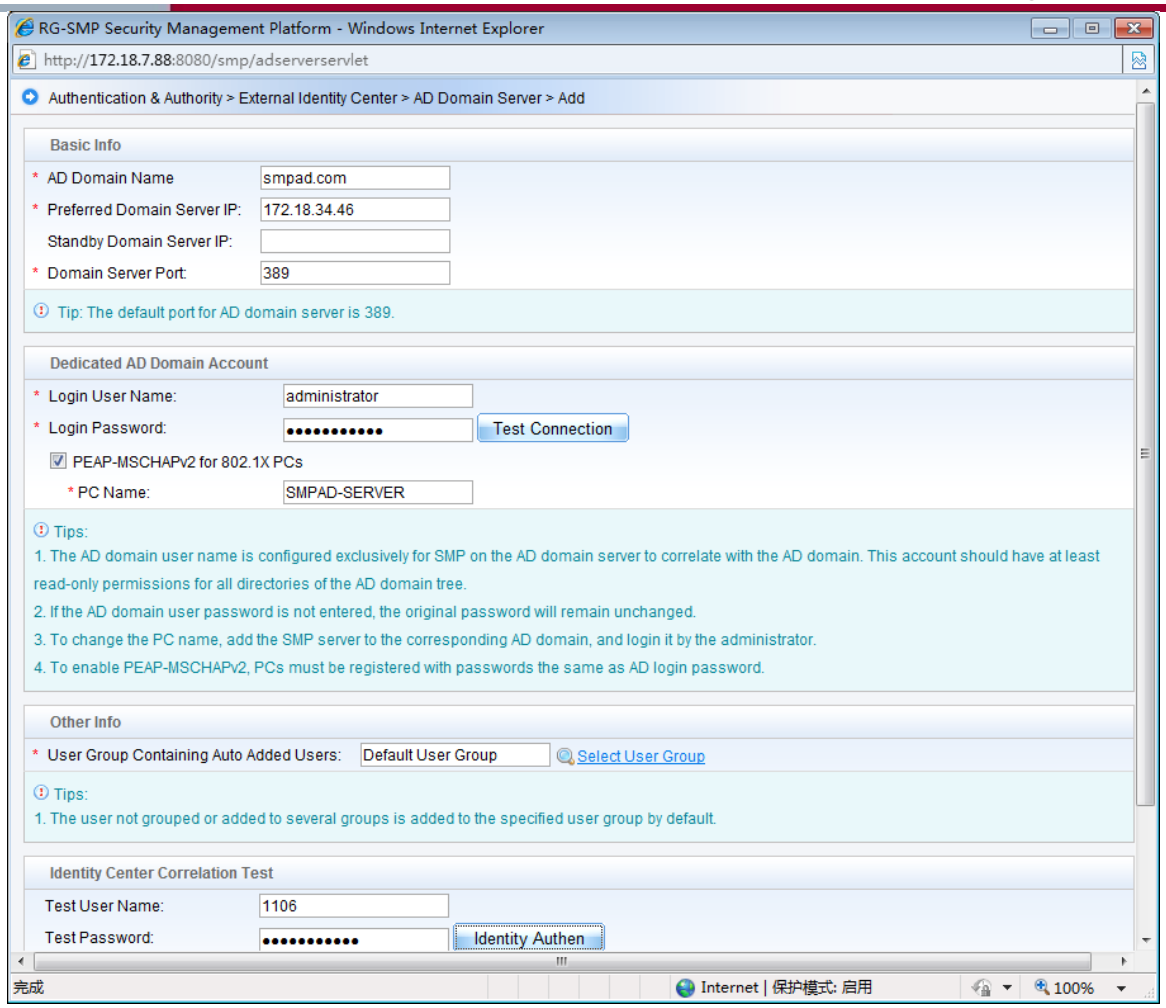
1. Go to **Authentication & Authority** > **External Identity Center**.
2. Check the **Enable External Identity Center** check box, click the **Windows AD Domain** tab, and configure correlation with Windows AD domain.



3. Click the **Windows AD Domain Server** link to access the **AD Domain Server > Query** window. Click **Add** to add an AD domain server.

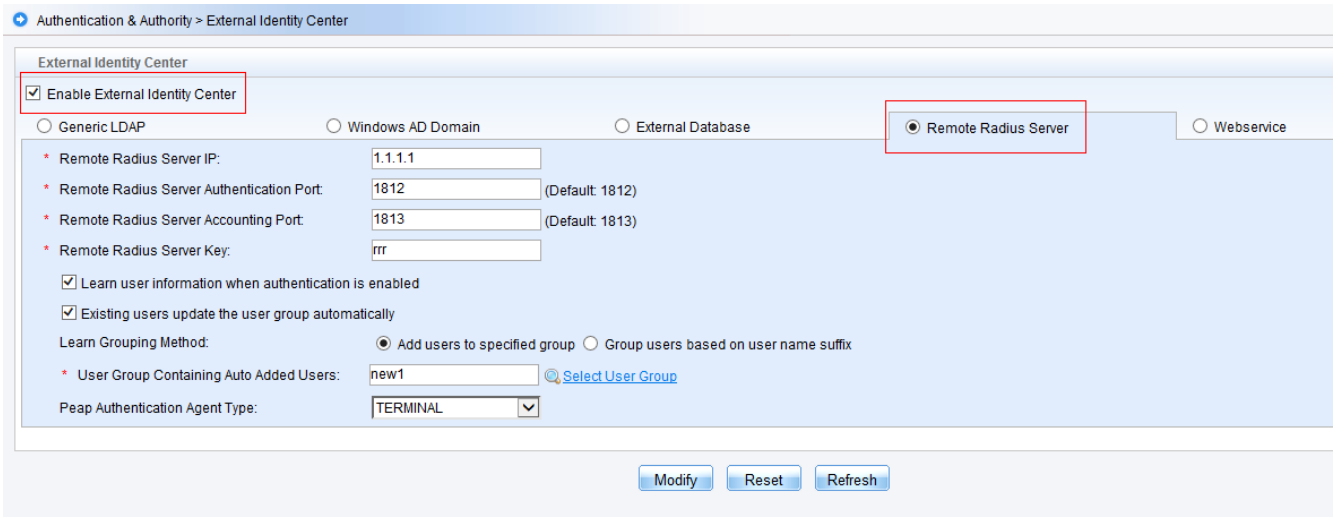


4. Configure the AD domain server and click **Add**.



1.3.3 Authentication Using Remote RADIUS Server

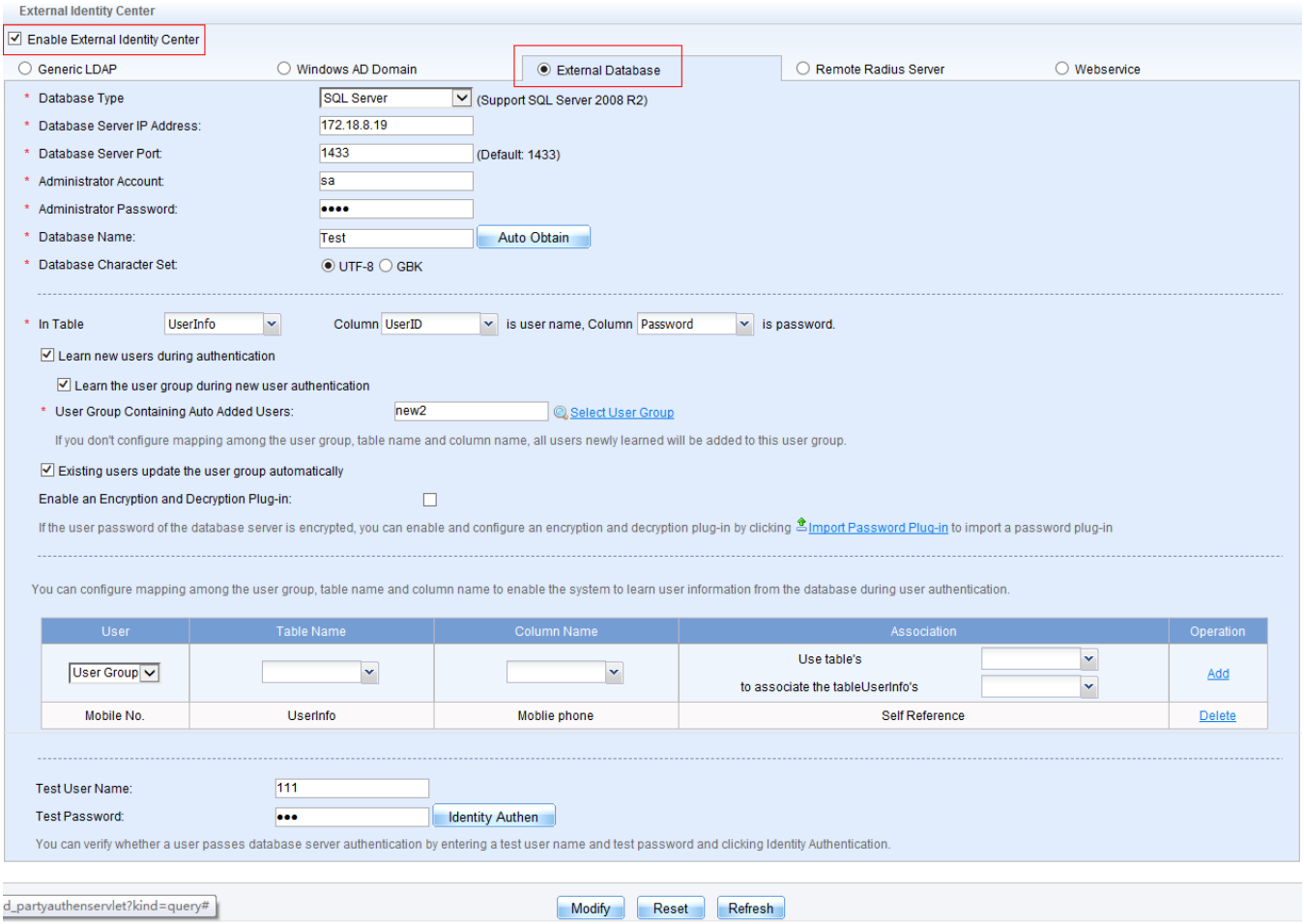
1. Go to **Authentication & Authority** > **External Identity Center**.
2. Check the **Enable External Identity Center** check box and click the **Remote Radius Server** tab.



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

1.3.4 Correlation with External Database

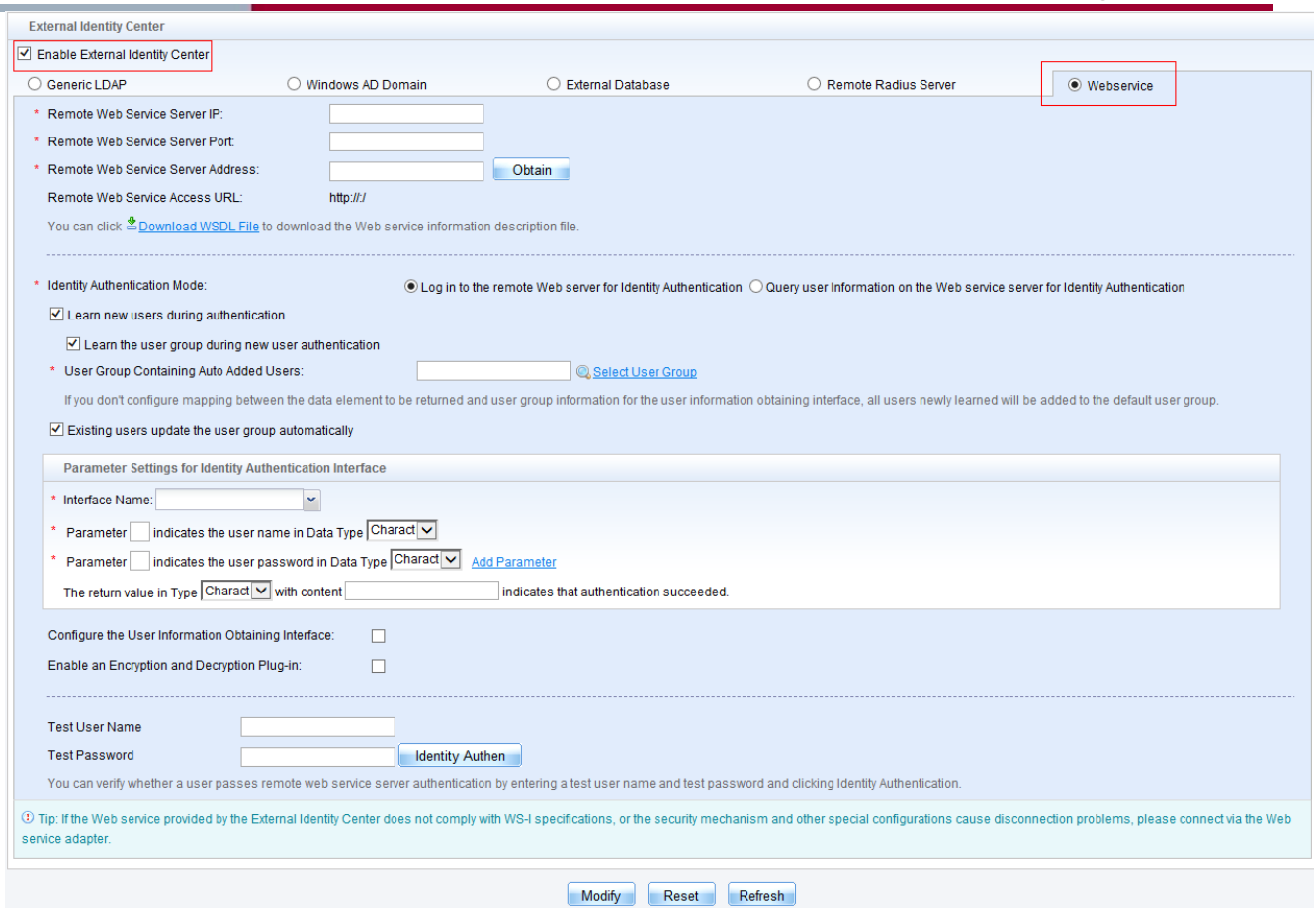
1. Go to **Authentication & Authority** > **External Identity Center**.
2. Check the **Enable External Identity Center** check box and click the **External Database** tab.



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

1.3.5 Correlation with Remote Web Service

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



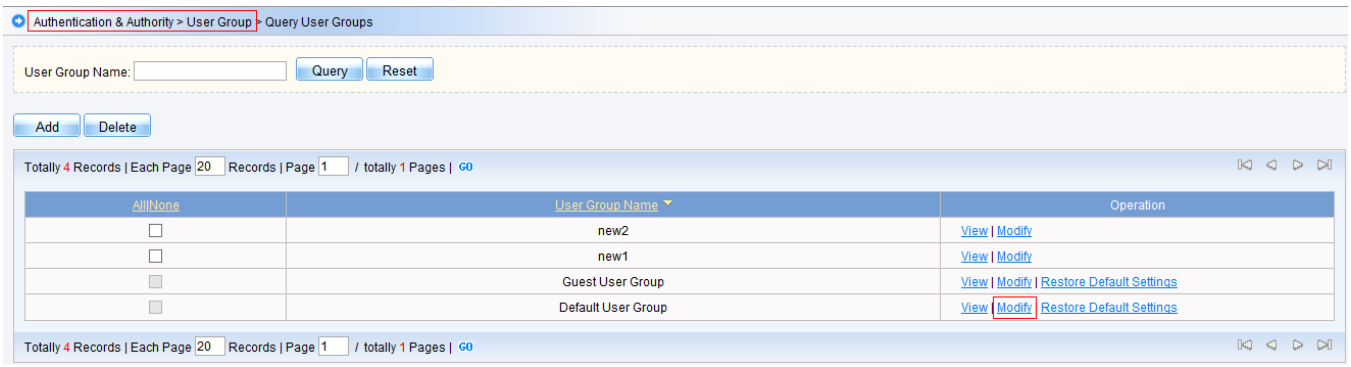
3. Configure correlation with the remote web service and click **Modify** to save the configuration.

1.4 User Access – Web Authentication

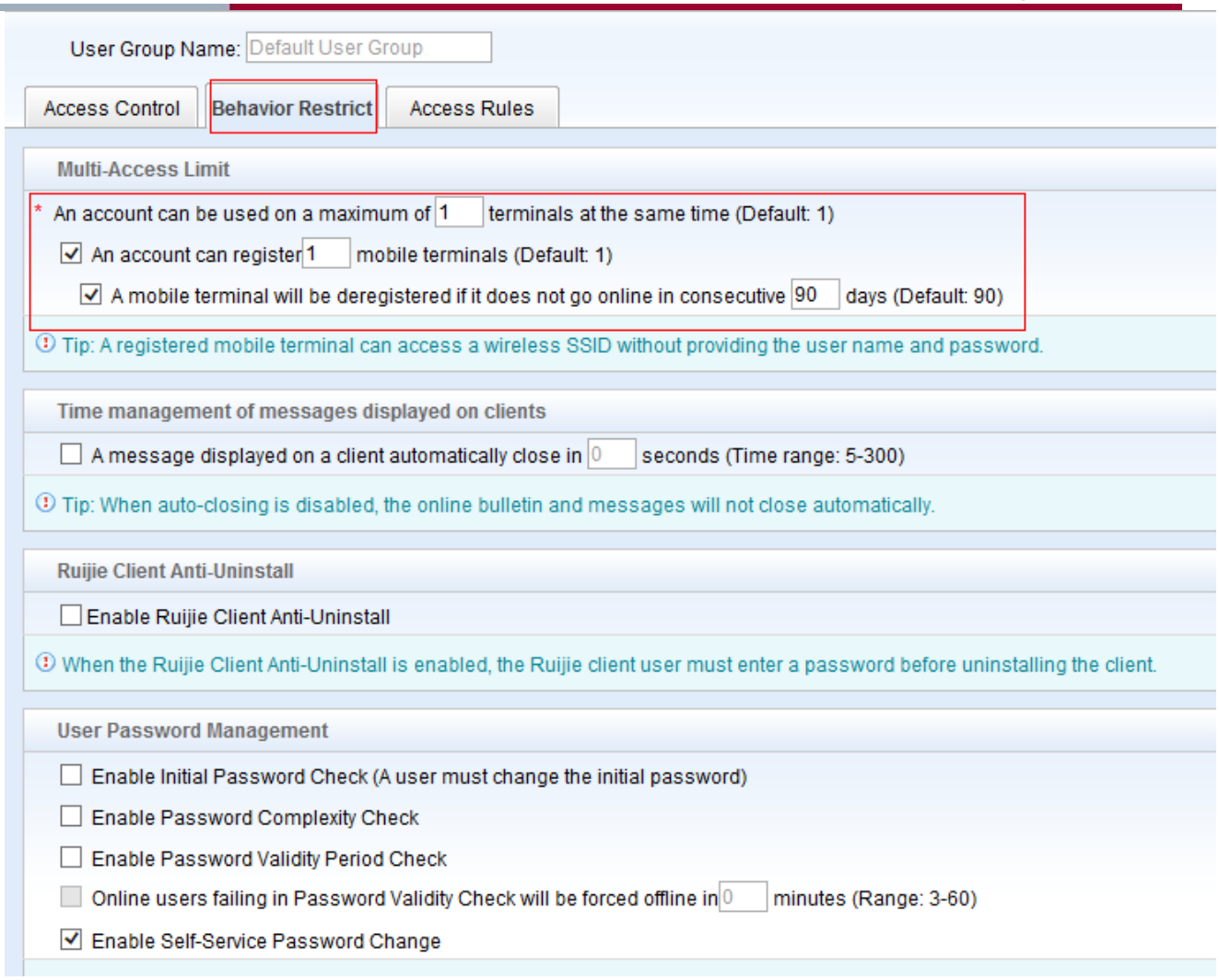
This section describes how to configure RG-SMP for authentication of mobile terminals.

1.4.1 Enabling Web Authentication of Mobile Terminals

1. Go to **Authentication & Authority** > **User Group** from the left menu. Click **Add** or **Modify** to access the configuration window of the corresponding user group.



2. Check the **An account can register** [ ] **mobile terminals** check box and save the configuration.



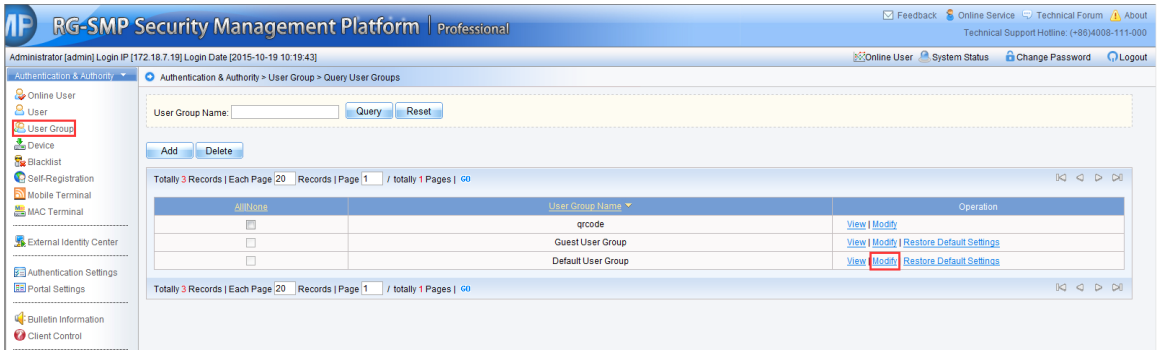
1.4.2 Configuring Offline Timer

Daily Timer

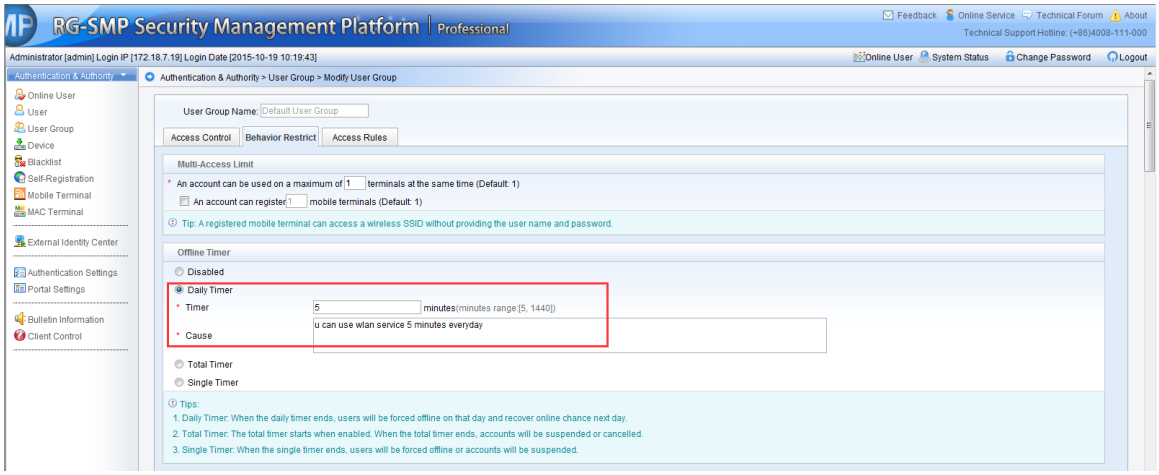
Daily Timer is used to set the maximum one-day online time X for users of a specified group on User Group setting page. (X is a positive integer in the unit of minutes, ranging from 5 to 1,440. The default value is 120 minutes.)

With Daily Timer enabled, the online time will be detected every 1 minute. If the maximum time X is exceeded, users will get offline, suspended and logged.

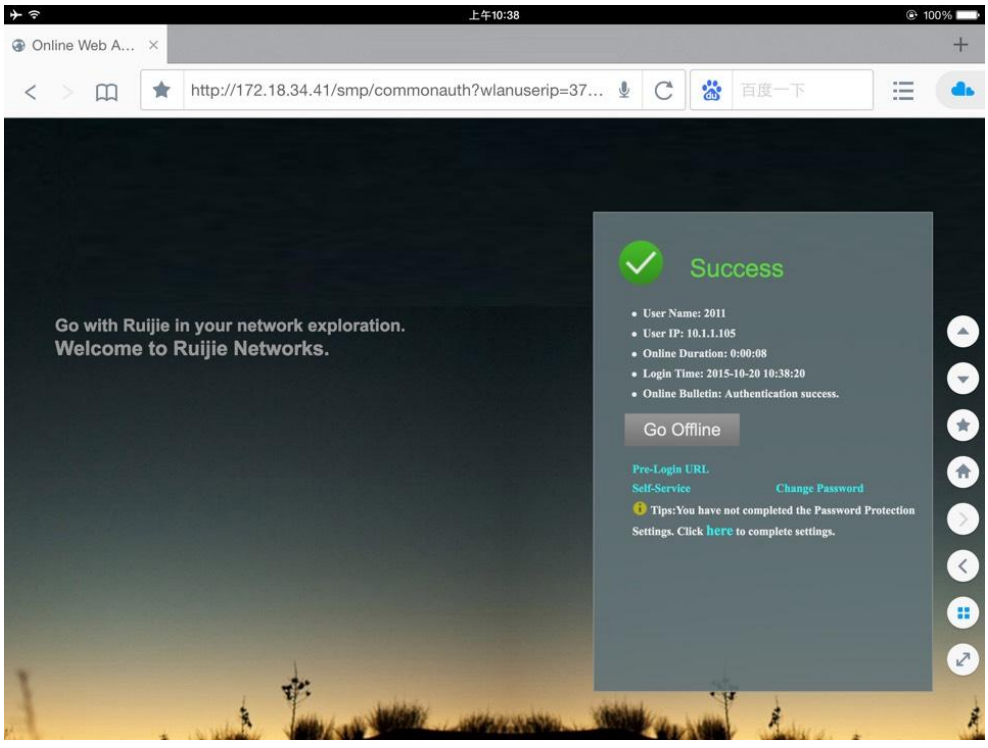
1. Choose **Authentication & Authority** > **User Group**, click **Modify** in the **Operation** column.



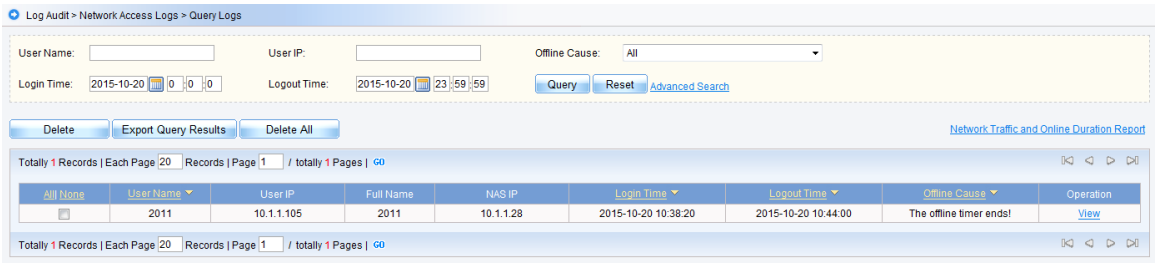
2. Choose **Offline Timer**, and click **Daily Timer** option, set **Timer** to 5 minutes, and click **Modify** to save the setting.

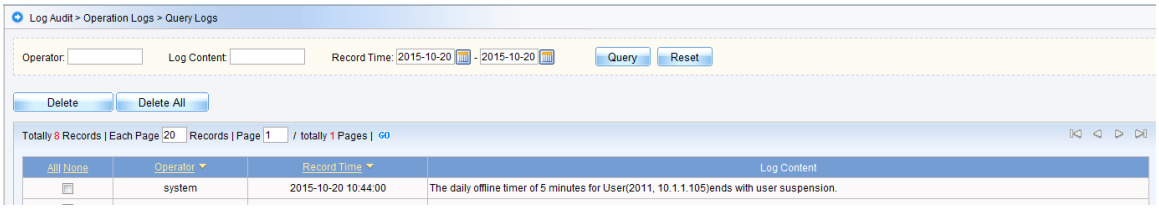


3. After users succeed in login, choose **Authentication & Authority** > **Online User** to view their online time.



4. If their online time exceeds 5 minutes, they will get offline and suspended; Choose **Log Audit** > **Network Access Logs** to verify the result.



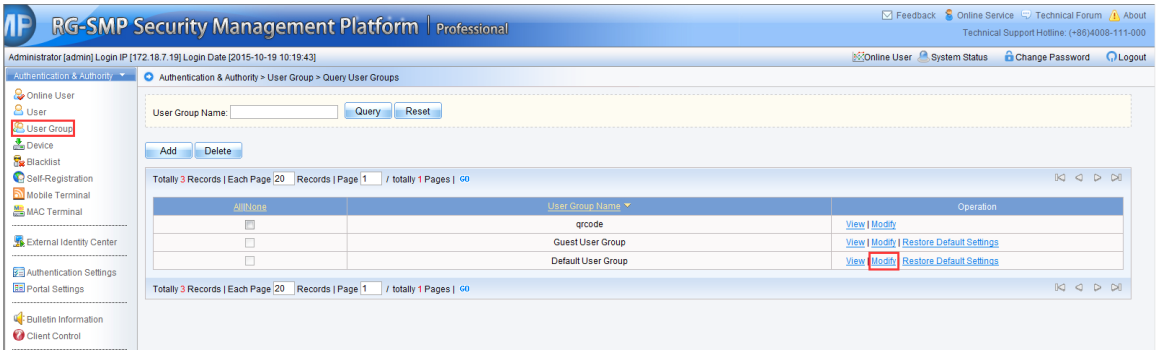


Total Timer

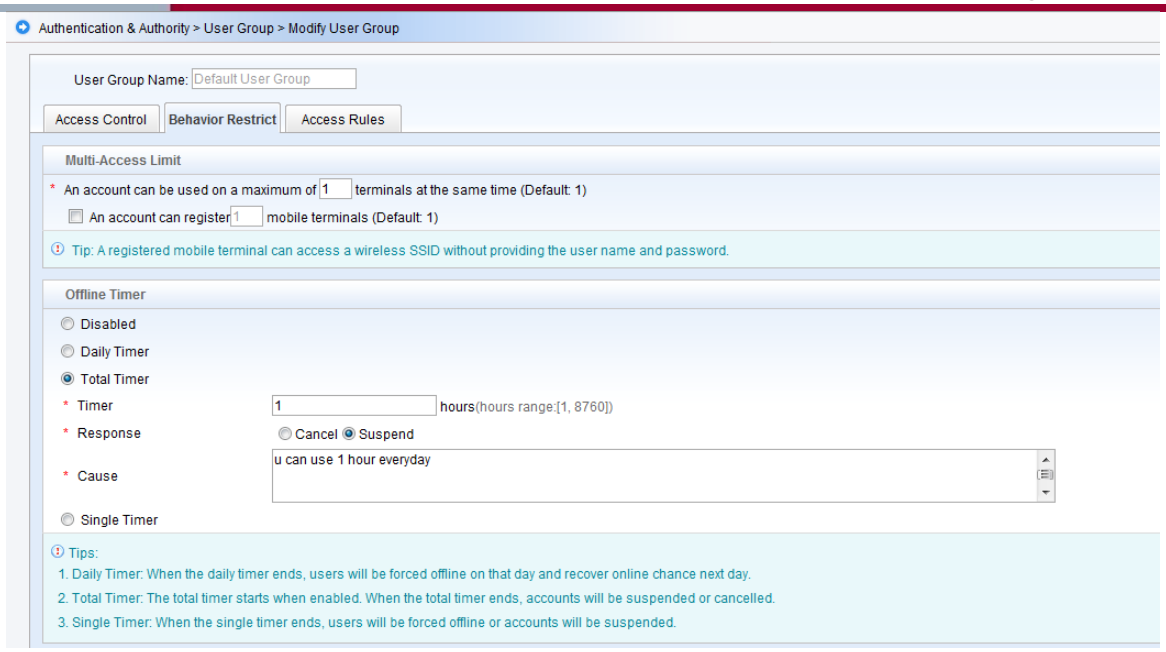
Total Timer is used to set the total online time X for users of a specified group on User Group setting page. (X is a positive integer in the unit of hours, ranging from 1 to 8,760. The default value is 168 hours.)

With Total Timer enabled, the online time will be detected every 1 minute. If the maximum time X is exceeded, users will get offline, suspended and logged.

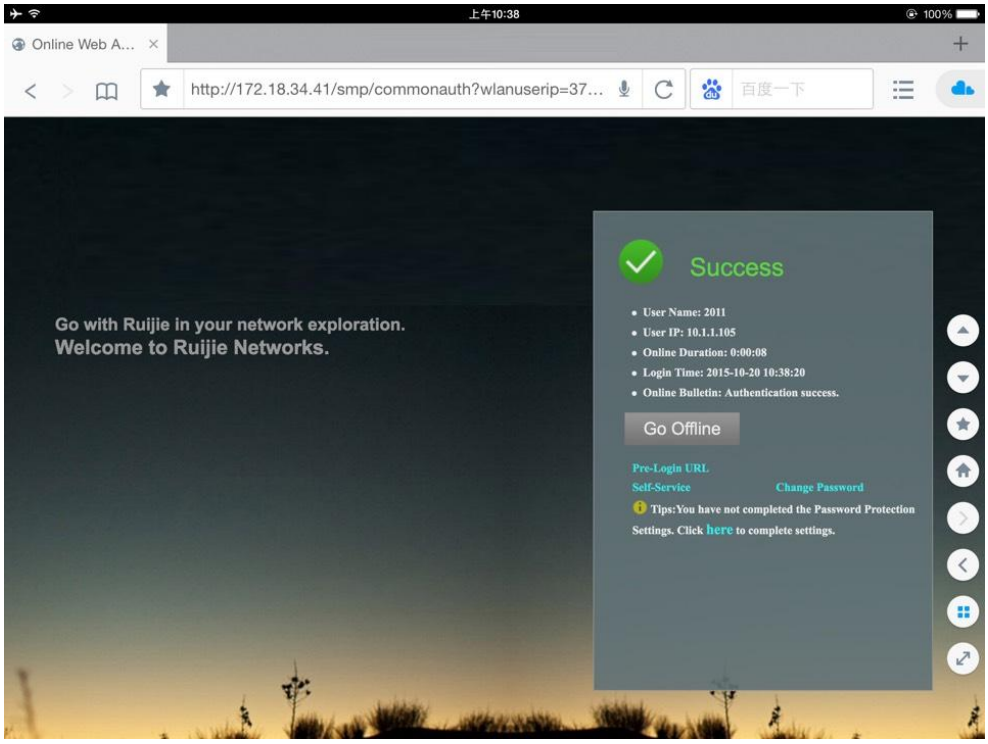
1. Choose **Authentication & Authority > User Group**, and click **Modify** in the **Operation** column.



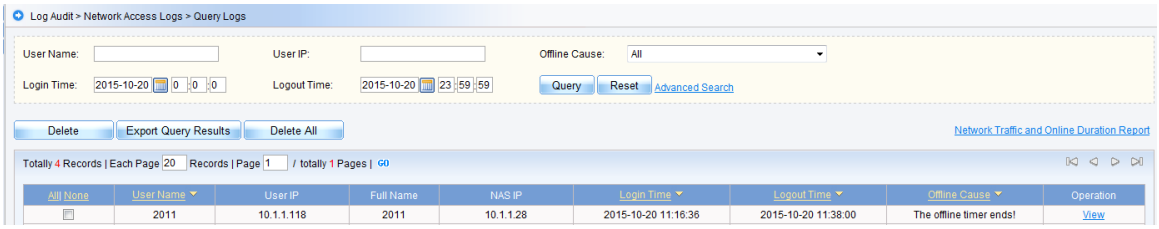
2. Choose **Authentication & Authority** > **User Group**, and click **Total Timer** option. Set **Timer** to 1 hour, and click **Modify** to save the setting.

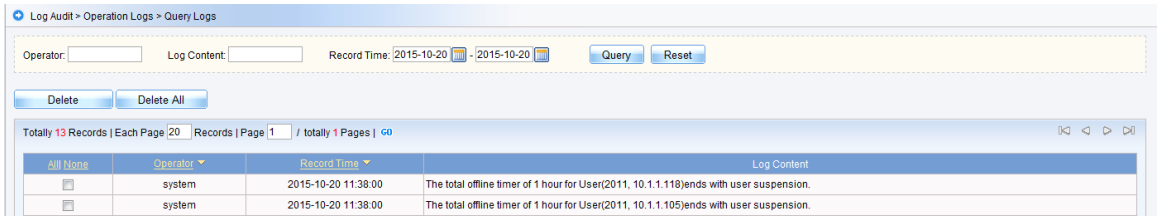


3. After users succeed in login, choose **Authentication & Authority > Online User** to view their online time.



4. If their online time exceeds 1 hour, they will get offline and suspended; Choose **Log Audit > Network Access Logs** to verify the result.



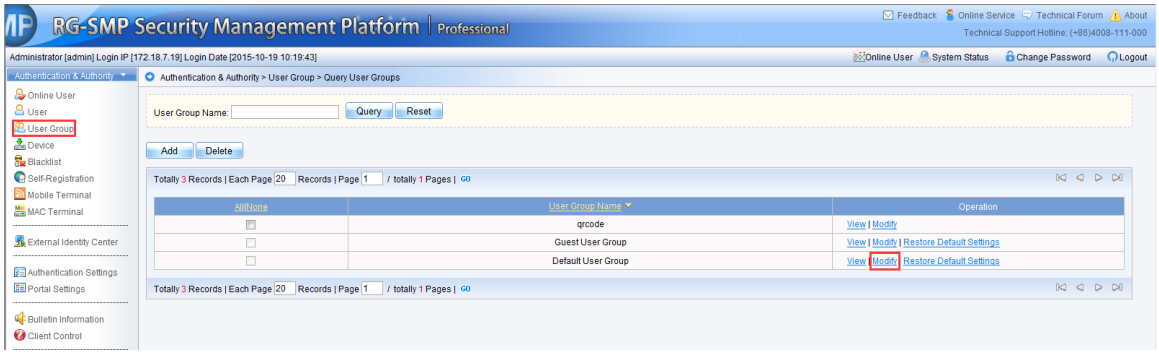


Single Timer

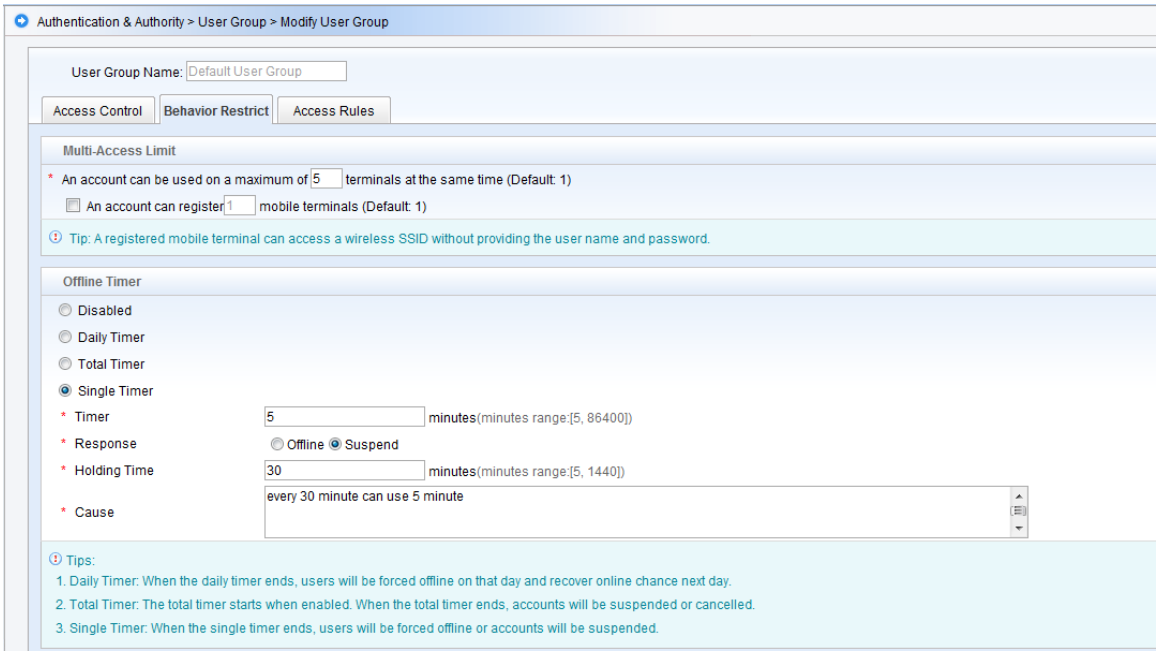
Single Timer is used to set the maximum single online time X for users of a specified group on User Group setting page. (X is a positive integer in the unit of minutes, ranging from 5 to 86,400. The default value is 60 minutes.)

With Single Timer enabled, the online time will be detected every 1 minute. If the maximum time X is exceeded, users will get offline, suspended and logged.

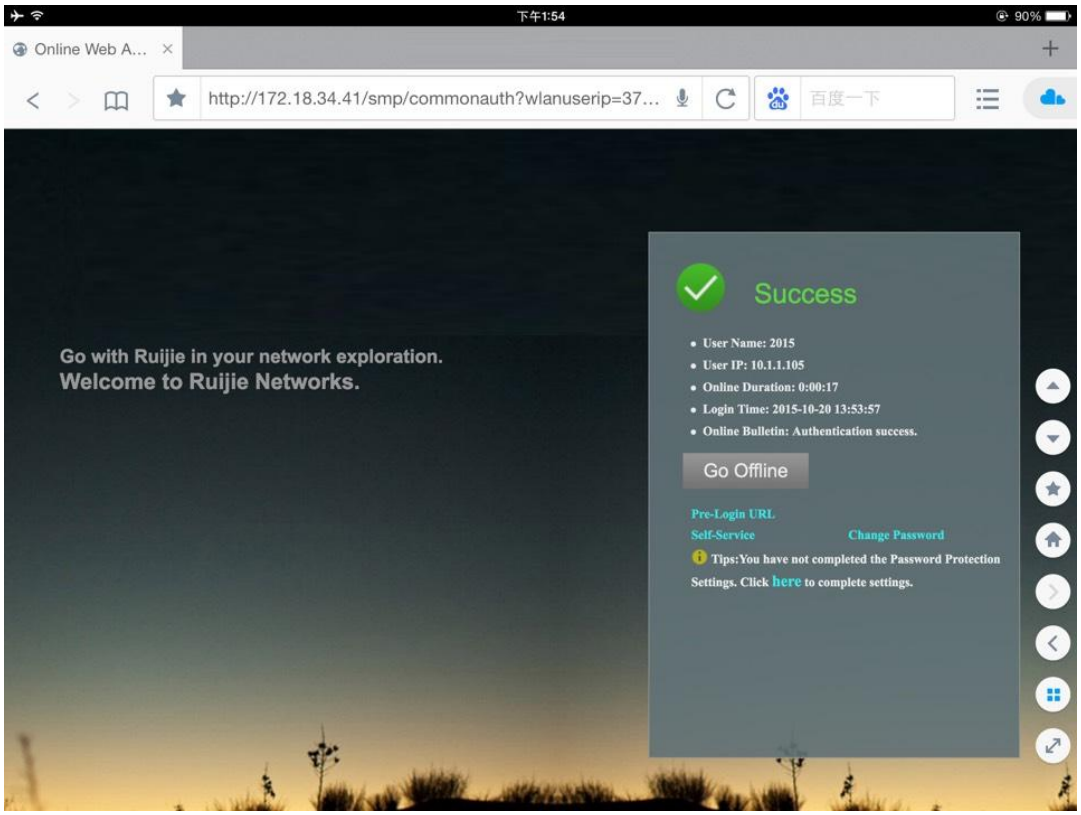
1. Choose **Authentication & Authority > User Group**, and click **Modify** in the **Operation** column.



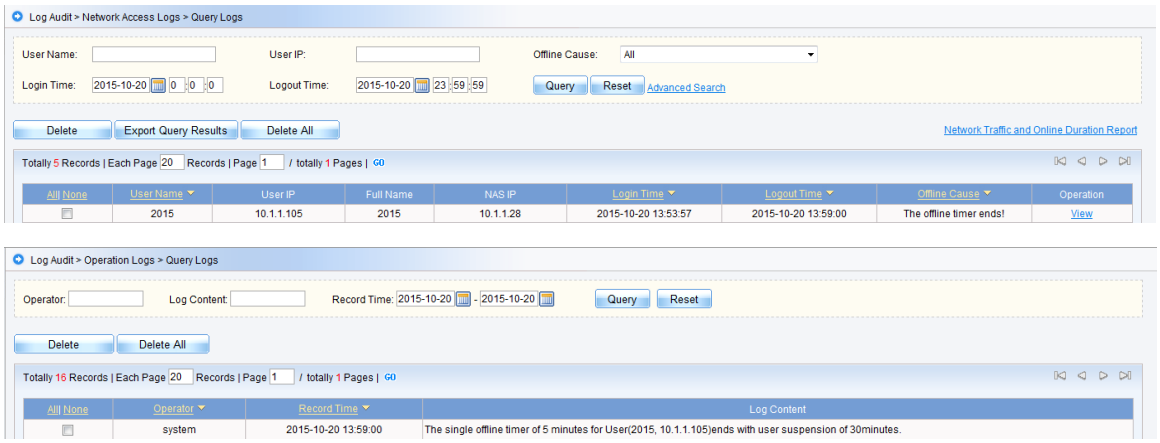
2. Choose **Authentication & Authority > User Group**, and click **Single Timer option**. Set **Timer** to 5 minutes, and click **Modify** to save the setting.



3. After users succeed in login, choose **Authentication & Authority > Online User** to view their online time.



4. If their online time exceeds 5 minutes, they will get offline and suspended; Choose **Log Audit > Network Access Logs** to verify the result.



1.4.3 Configuring QR Code Authentication

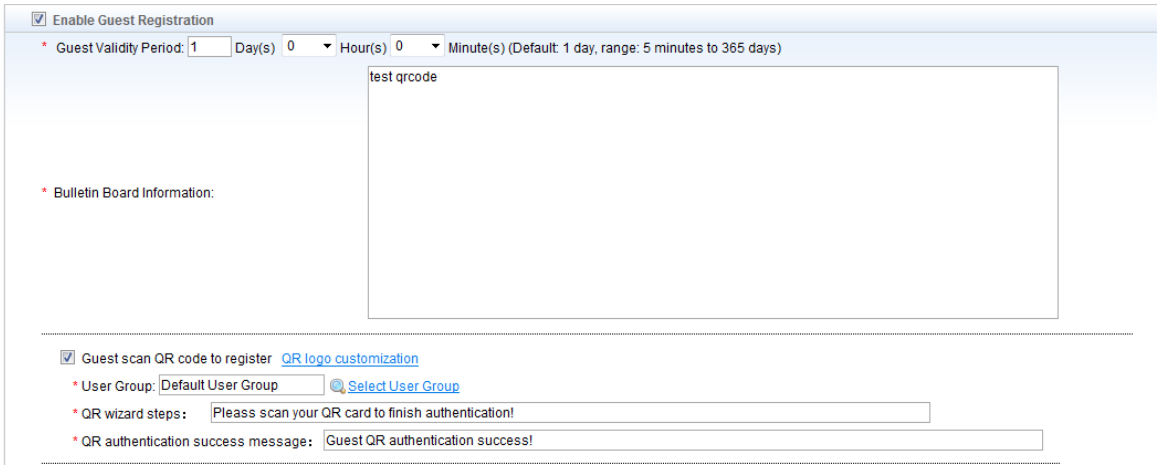
Prerequisite:

Configure the redirection addresses of Web authentication:

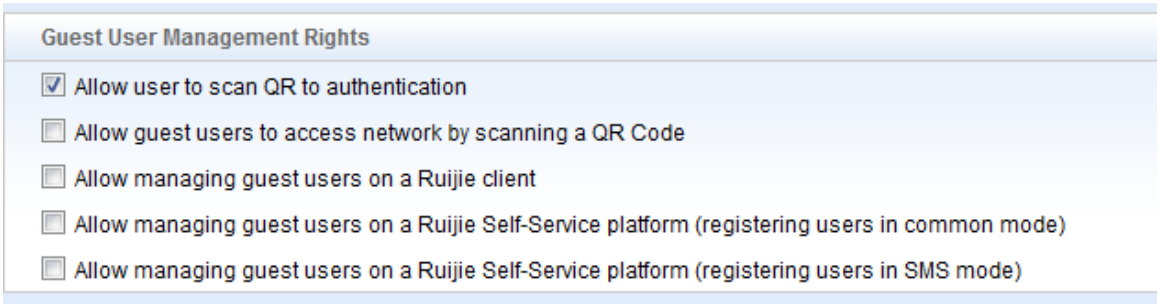
HTTP address: http://172.18.8.140:80/smp/qrcodecardservlet

HTTPS address: https://172.18.8.140:443/smp/qrcodecardservlet

1. Choose **Authentication & Authority** > **Portal Settings**, and check **Enable Guest Registration** box to enable QR code authentication.



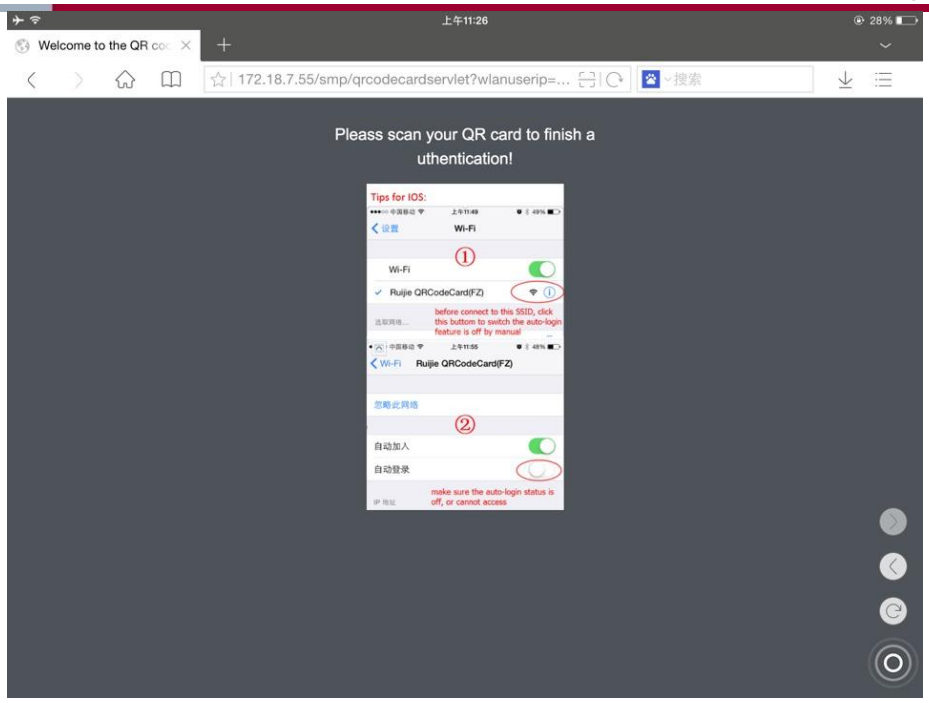
2. Choose **Authentication & Authority** > **User Grou**p > **Modify User Grou**p. Check **Allow user to scan QR to authentication** box in **Guest User Management Rights** to allow QR authentication for the default user group.



3. Log in to RG-SMP Self-Service Platform by users in the default group to view their QR codes.

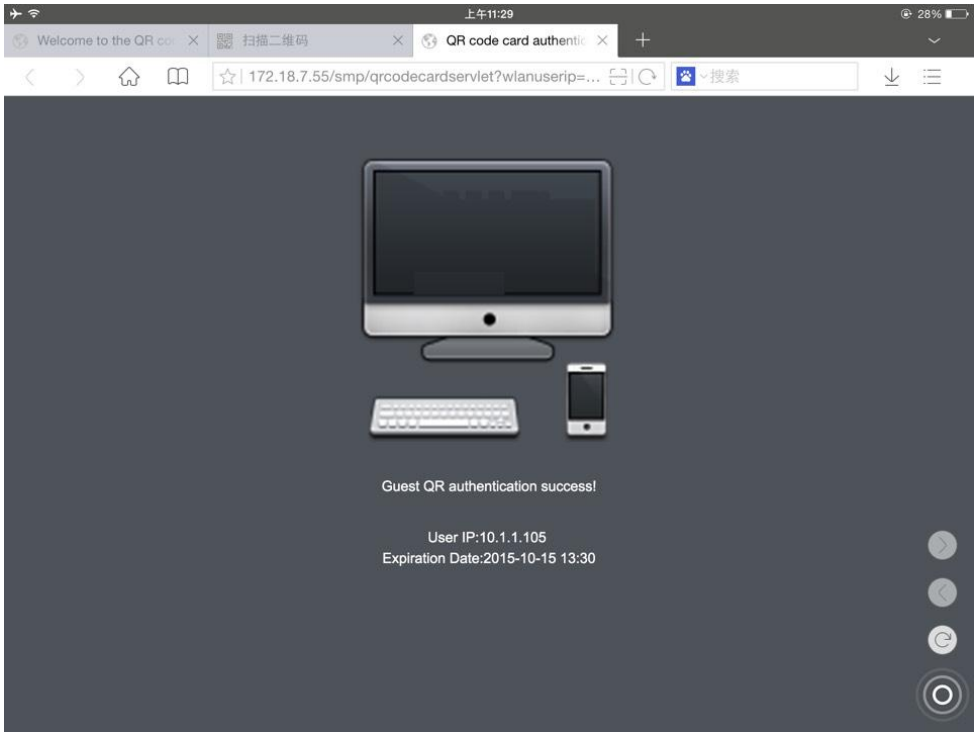
4. Click **Print QR code**, **QR saved as**, or **Regenerate QR** to print, save or regenerate QR code.

5. After Wi-Fi is connected, the following page is displayed in the browser.

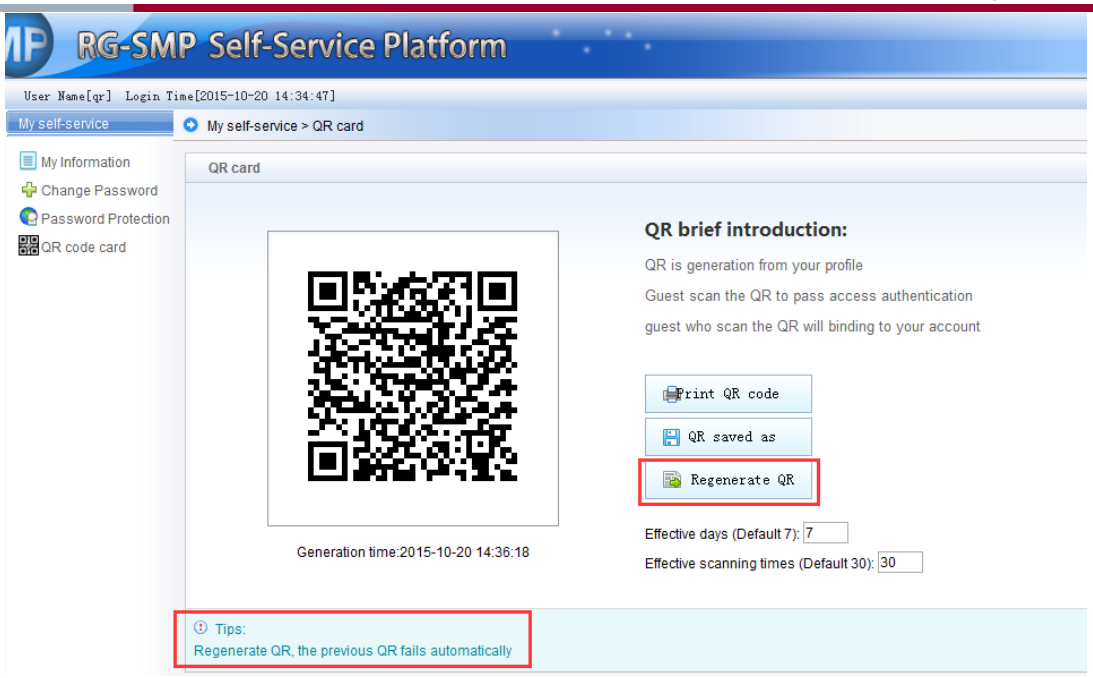


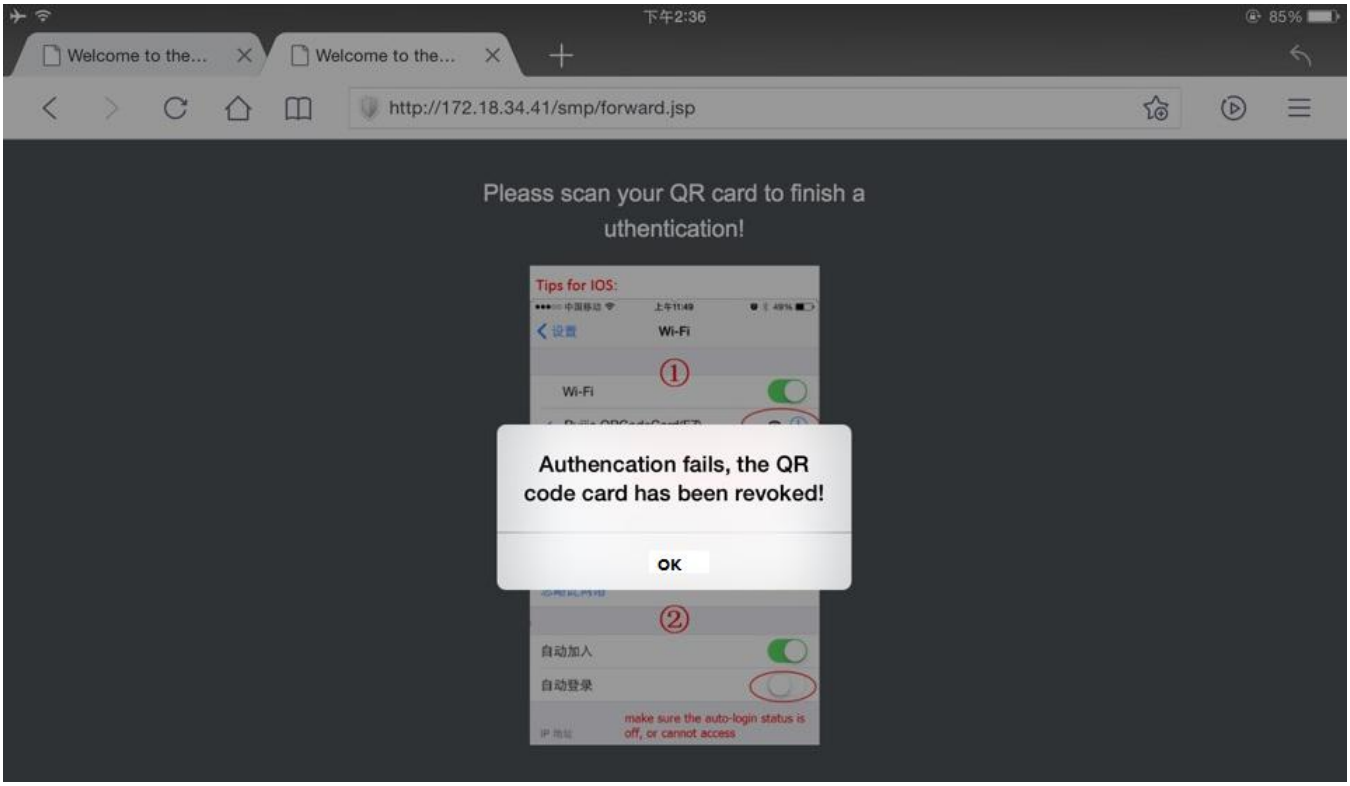
Scan the QR code displayed in RG-SMP Self-Service Platform by using QR scanners (e.g. WeChat App).

1. If the following page is displayed, QR authentication succeeds and access is available.



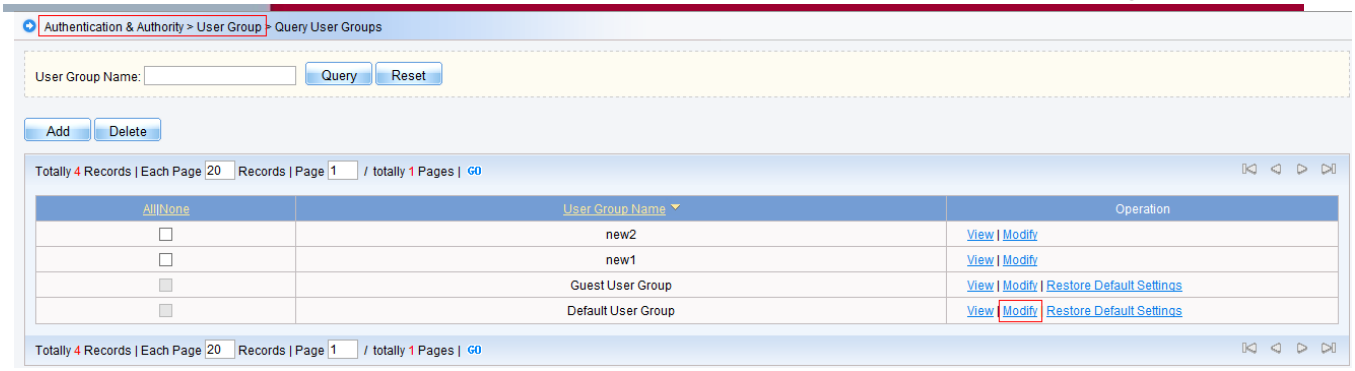
2. The **Regenerate QR** function in RG-SMP Self-Service Platform will deactivate previous QR codes.



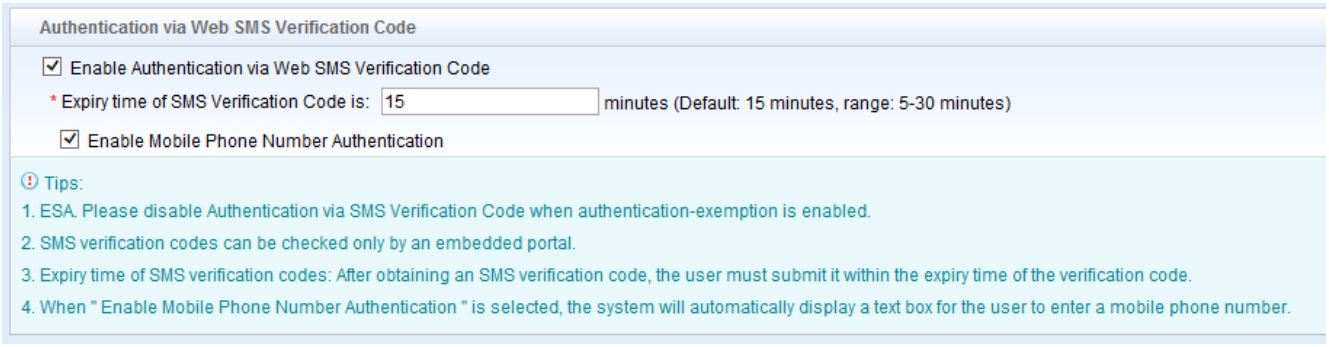


1.4.4 Random Verification Code of Web Authentication

1. Go to **Authentication & Authority** > **User Group** from the left menu. Click **Add** or **Modify** to access the configuration window of the corresponding user group.

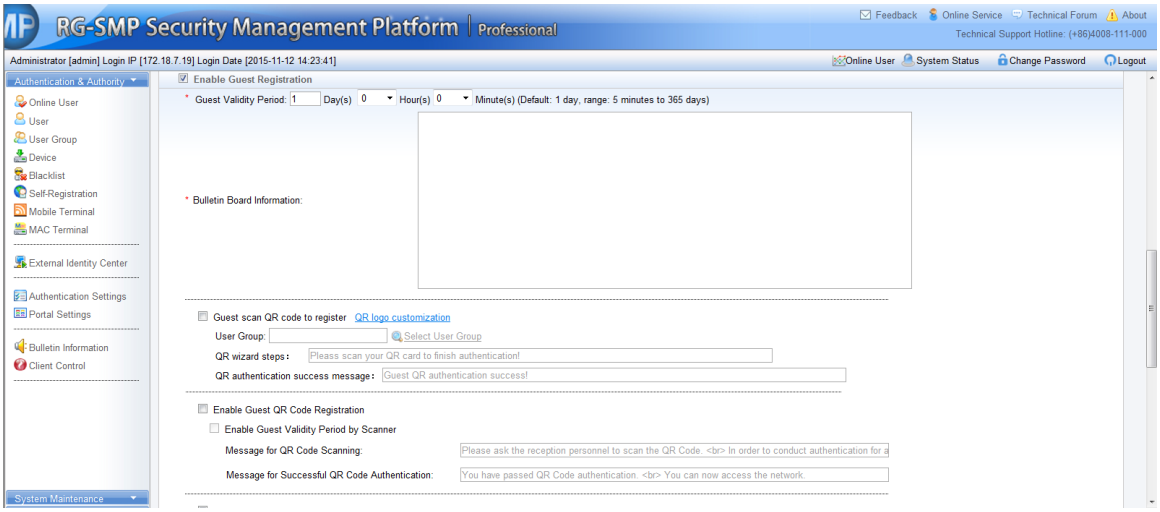


2. Check the **Enable Authentication via Web SMS Verification Code** check box and save the configuration.

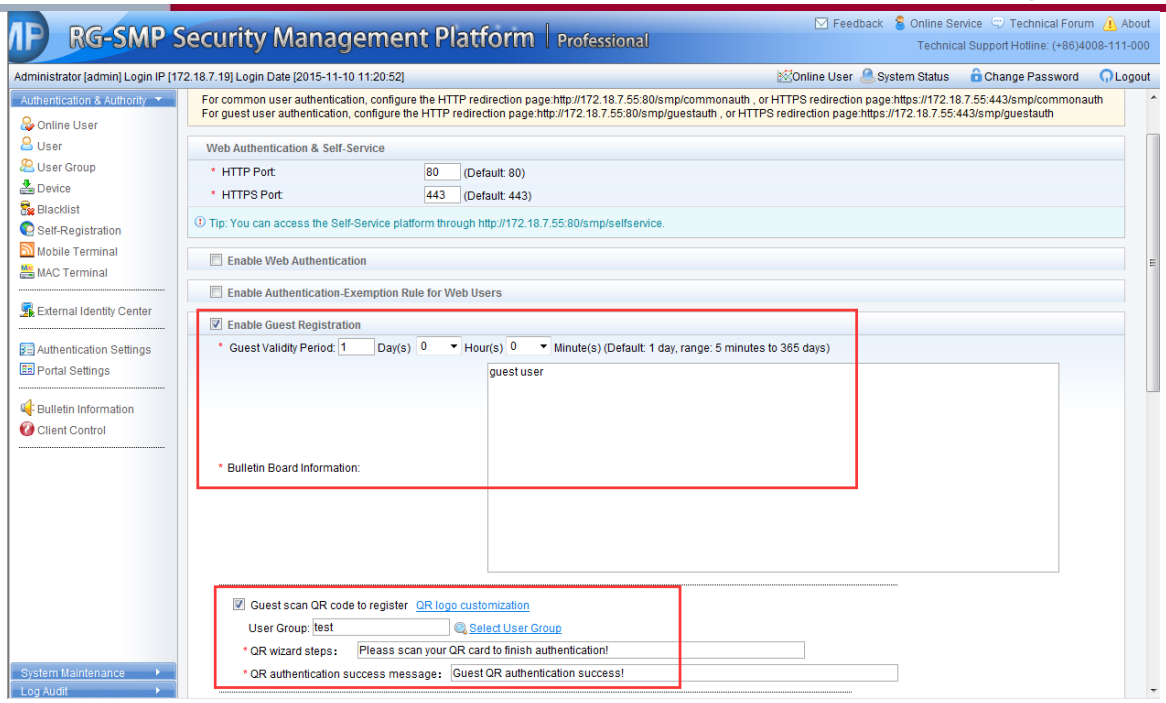


1.4.5 Configuring Web Authentication

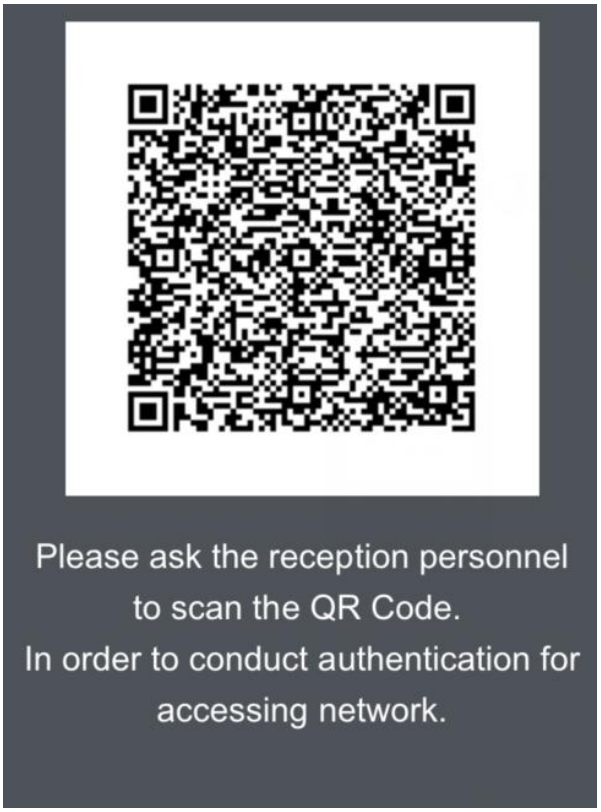
1. Go to **Authentication & Authority** > **Portal Settings**.



2. Enable SMS first if you want to enable **Guest SMS-Self-Service Registration**.
3. Check the **Enable Guest Registration** and **Enable Guest QR Code Registration** check boxes, and configure the URL for QR code authentication.



QR code for authentication:



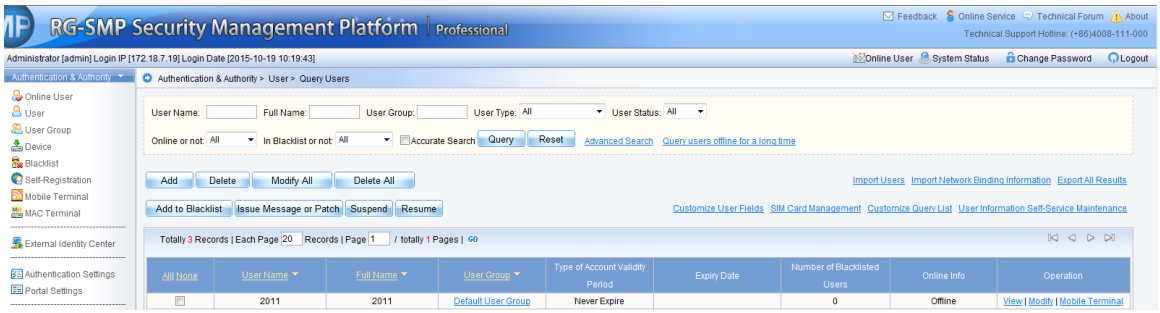
HTTPS access is supported. For details, see **Tips** in the **Authentication & Authority** > **Portal Settings** window.

1.4.6 Configuring Password Authentication

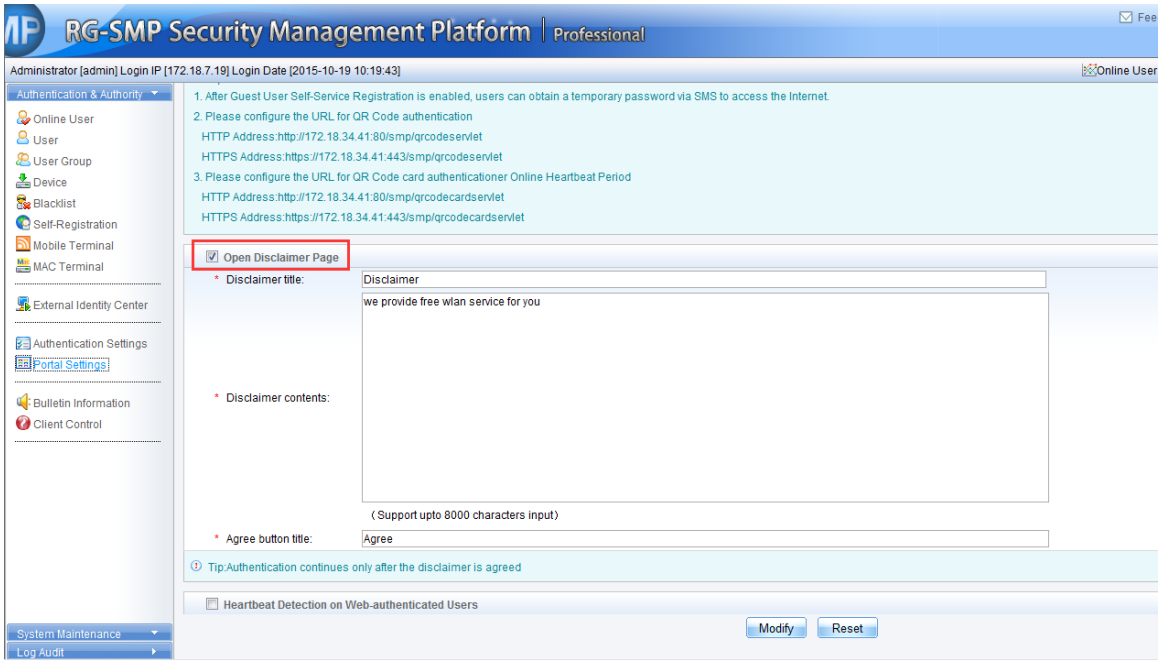
Disclaimer is added into the user authentication page. You can configure the disclaimer in **Portal Settings** menu.

Authentication can continue only after the disclaimer is accepted. Then, enter the password and click **OK** to get access. (Note: Users are added by the administrator. Username and password must match)

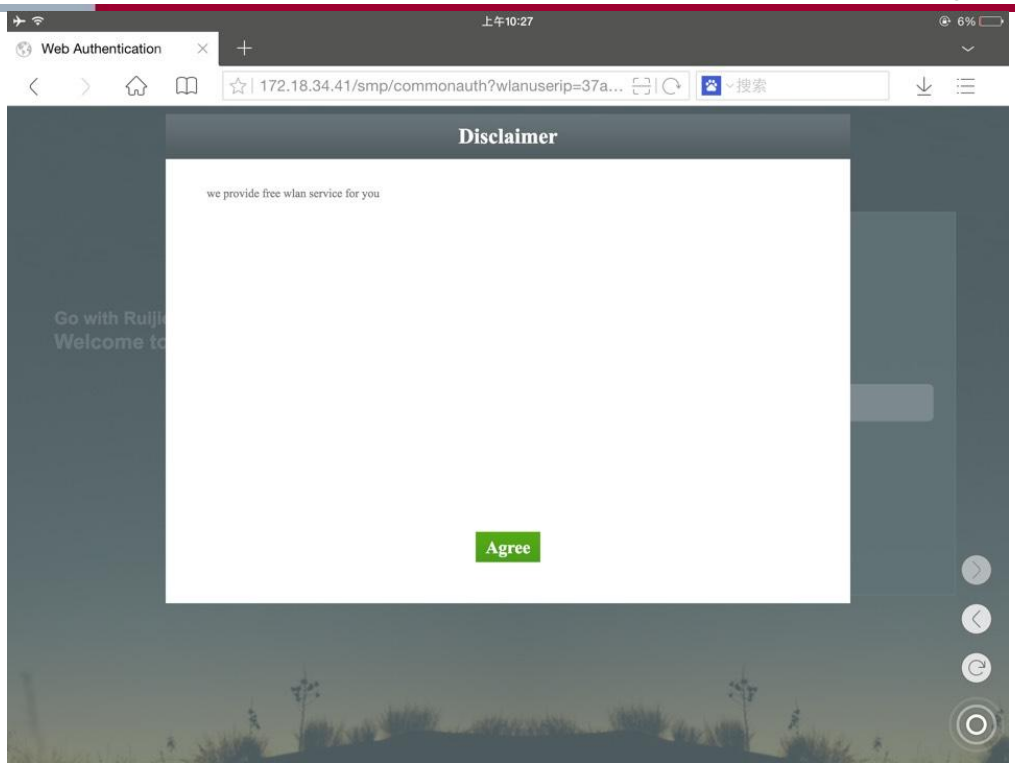
1. Choose **Authentication & Authority** > **User**. Click **Add** to add User 2011 with 2011 as its password.

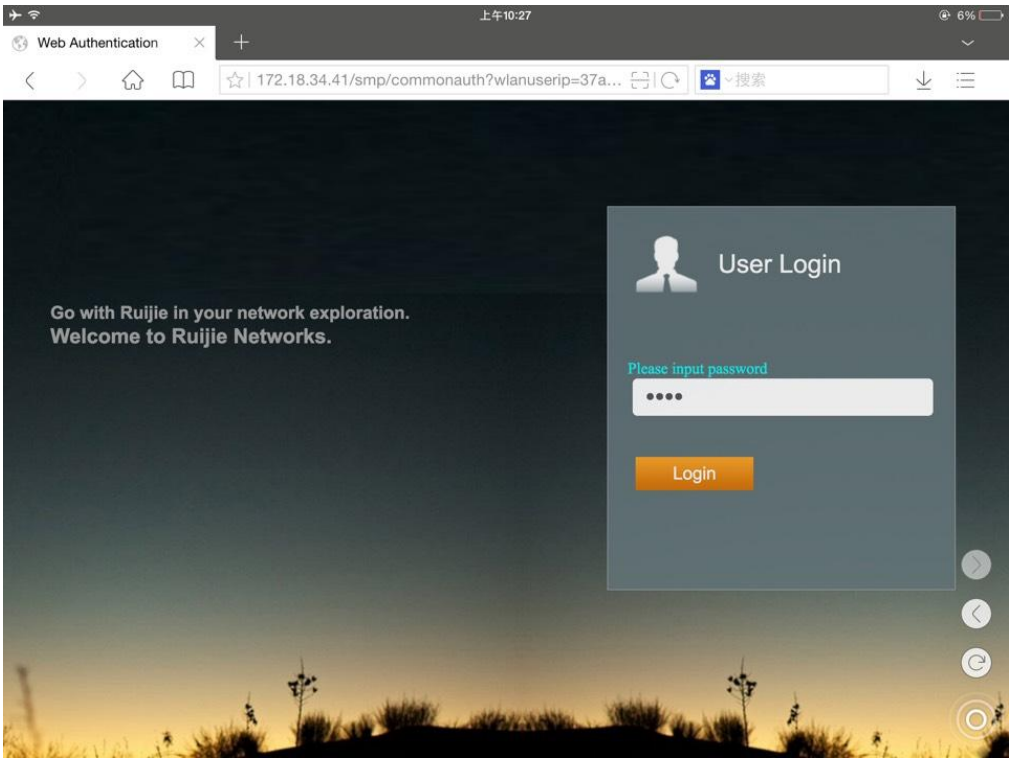


2. Choose **Portal Settings**, check **Open Disclaimer Page** box to enable and configure the disclaimer. Click **Modify** to save the configuration.



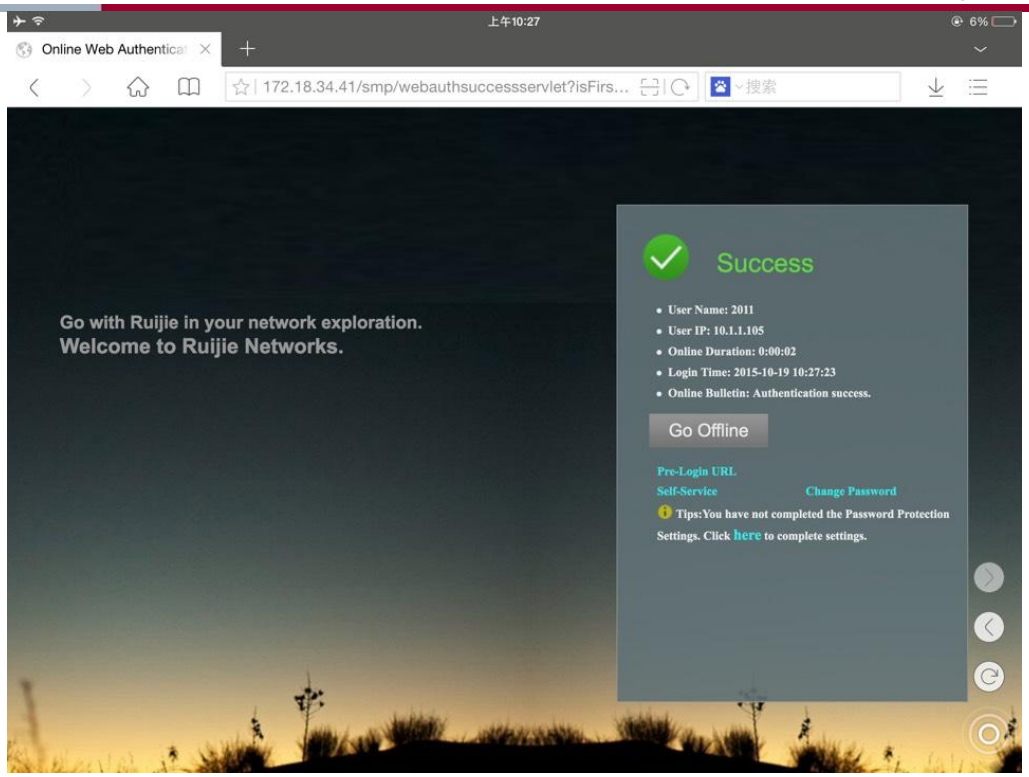
3. After Wi-Fi is connected, the disclaimer page is displayed. After the disclaimer is agreed, the login page will be displayed.





4. Enter the correct password to get access.

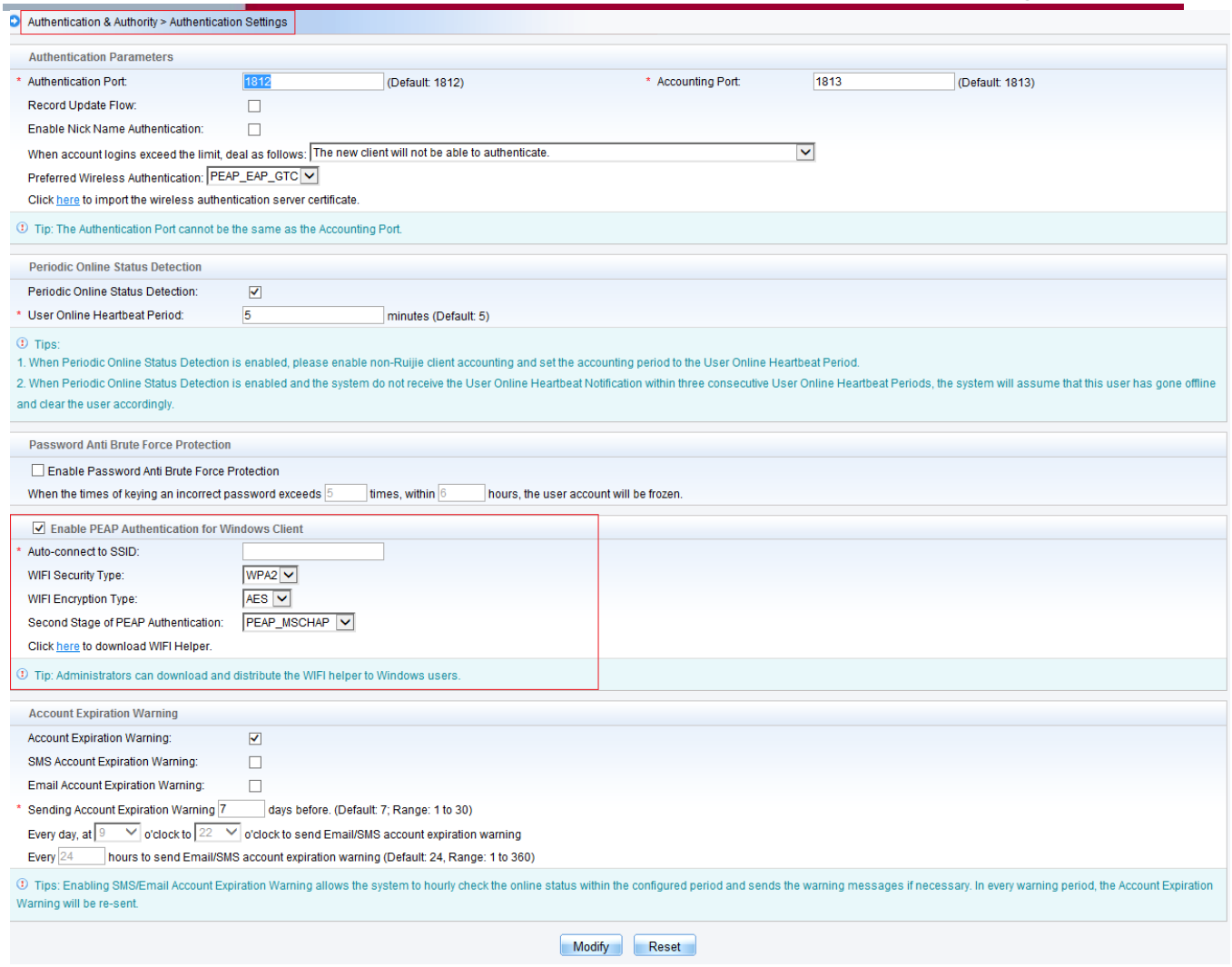
Note: The username and password must match. For users are added by the administrator, make sure that the users have been created.



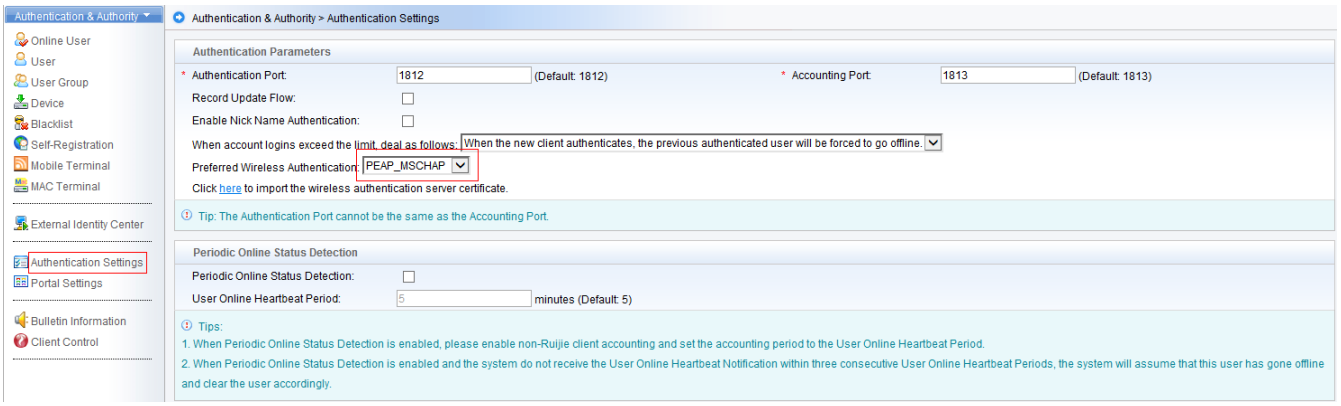
1.5 PEAP Authentication Configuration

1.5.1 Steps

1. Go to **Authentication & Authority** > **Authentication Settings**. Configure the SSID, security type, encryption type, and authentication protocol of PEAP authentication based on the actual network conditions. The value of **Auto-connect to SSID** must be consistent with the SSID configured for RG-SMP and the SSID is for 802.1X authentication.



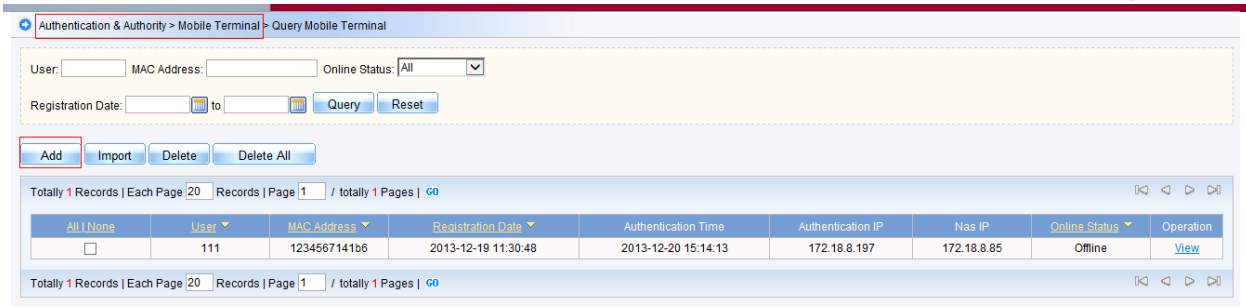
2. Change **Preferred Wireless Authentication** to **PEAP-MSCHAP**.



3. Click **Modify** when the configuration is completed. This enables PEAP authentication for users who have downloaded Wi-Fi Helper on the redirected web authentication page.

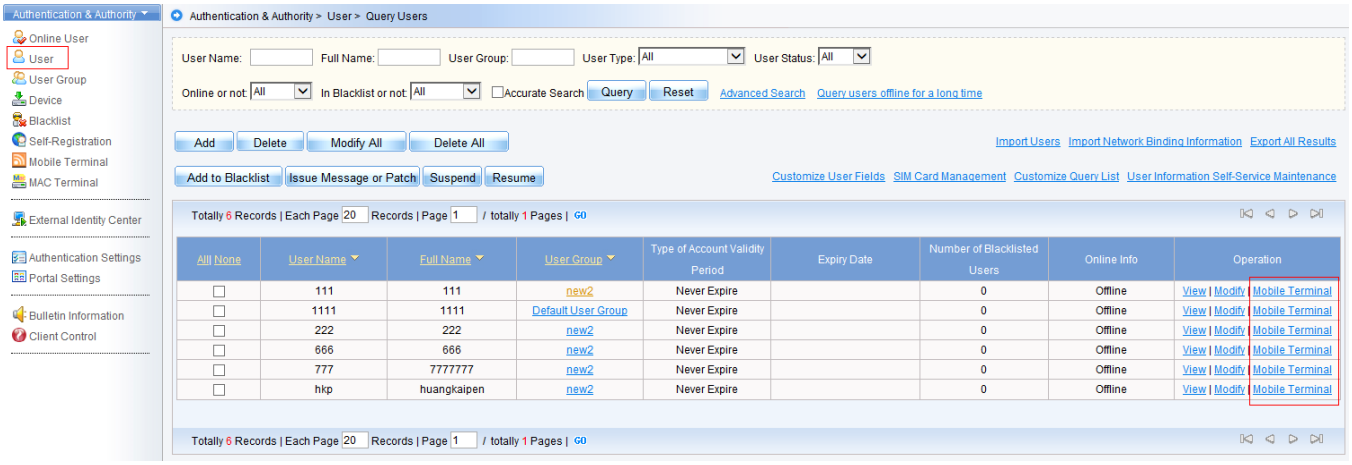
1.5.2 Adding Mobile Terminals

1. Go to **Authentication & Authority > Mobile Terminal**.



2. Click **Add** to add mobile terminals.

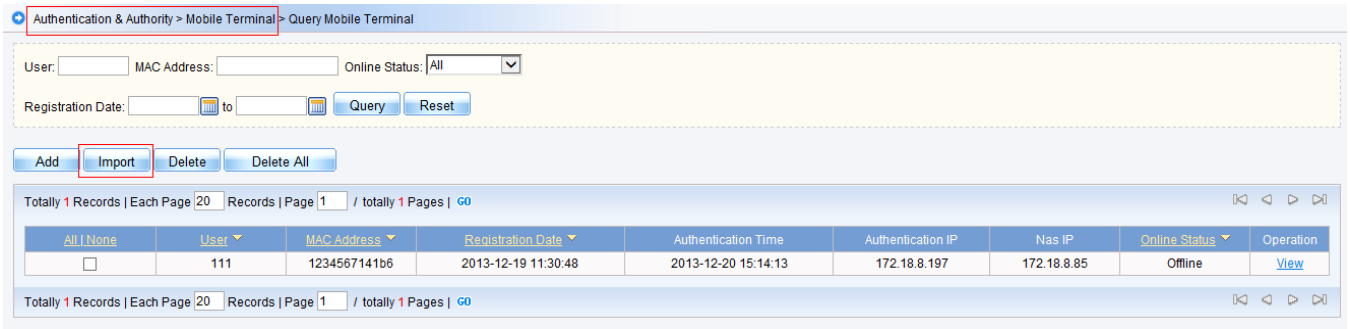
3. Go to **Authentication & Authority** > **User** and click **Mobile Terminal** to access the **Mobile Terminal** window of the corresponding user.



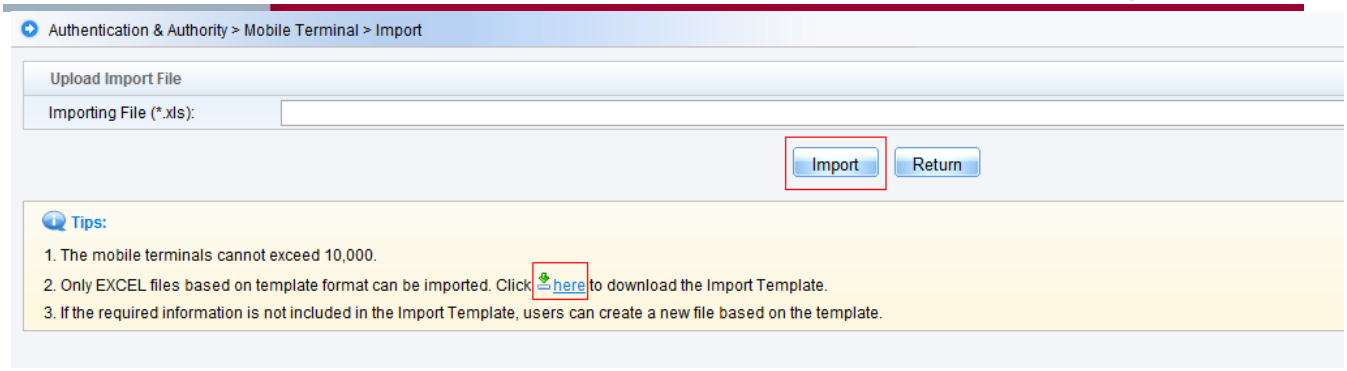
4. Click **Add** to add mobile terminals.

1.5.3 Importing Mobile Terminals

1. Go to **Authentication & Authority** > **Mobile Terminal** and click **Import**. The **Import** window is displayed.

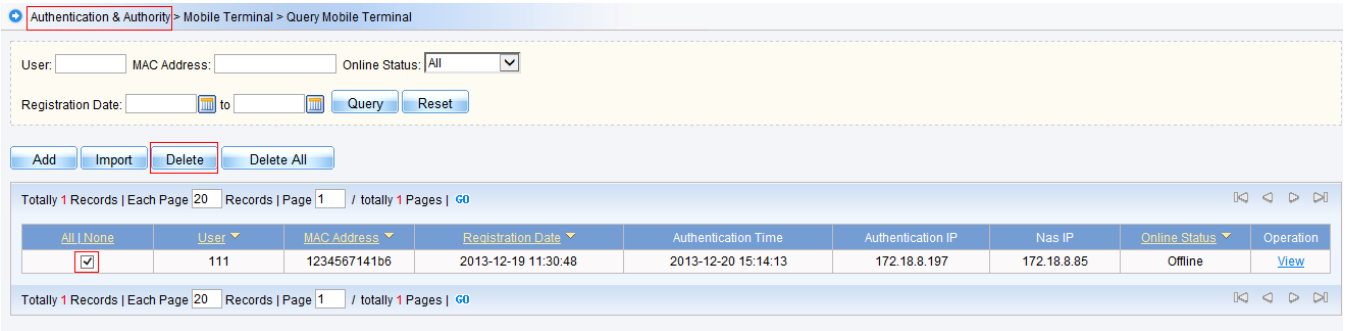


2. Select the Excel file to be imported and click **Import**.

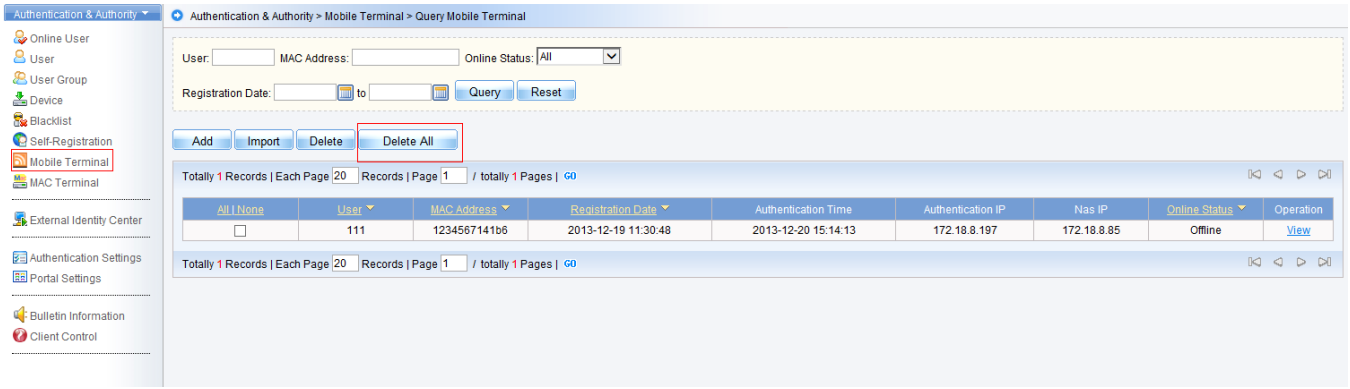


1.5.4 Deleting Mobile Terminals

1. Go to **Authentication & Authority** > **Mobile Terminal**, select a mobile terminal, and click **Delete**. The selected mobile terminal is deleted.



2. Go to **Authentication & Authority** > **Mobile Terminal** and click **Delete All**. The listed mobile terminals are deleted.



2 FAQ

1. How can I log in to RG-SMP for the first time?

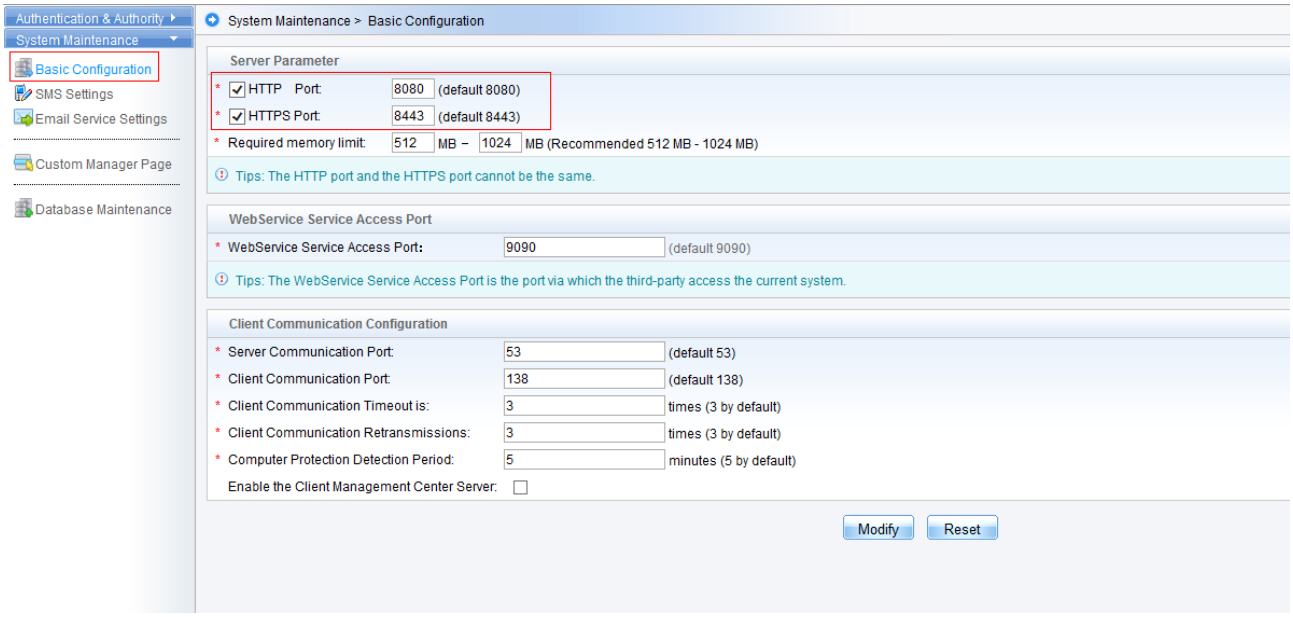
Type **http://***local IP address***:8080/smp/index.jsp** in the address bar of your browser. Enter the user name (**admin**) and password (**111111111**) of the system administrator in the login window.

2. 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 user name and password for login) in the **Service Manager** of RG-SMP.

3. How can I change the HTTP or HTTPS port for login to RG-SMP?

Go to **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.



4. Why does the system always prompt that session timed out and return to the login window 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 type the URL of RG-SMP in the address bar.

5. Why does the system prompt existence of unsupported characters?

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

`	~	!	@	#	$	%	^	&	*
(	)	（	）	[	]	{	}	—	'
_	-	=	+	,	.	&	′	+	,
;	:	“	”	‘	’	<	>	%	
‘	’	“	”	…	‰	、	。	]	^
《	》	【	】	!	"	#	$		*
;	<	=	>	—	.	/	:	?	@
{	|	}	～	[	\				