

Configuration Guide

RG-SMP Professional_2.63_EN_Build20151106

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.

 ,  ,  ,  ,  ,  ,

 ,  ,  ,

 ,  ,  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.

Obtaining Technical Assistance

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

Contents

Contents	3
1 Configuration Guide	4
1.1 User Access – Wired Access.....	4
1.2 User Access – Wireless Access.....	7
1.3 User Access – Correlation with External Identity Center.....	8
1.4 User Access – Web Authentication.....	13
1.5 PEAP Authentication Configuration.....	28
2 FAQ	31

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:

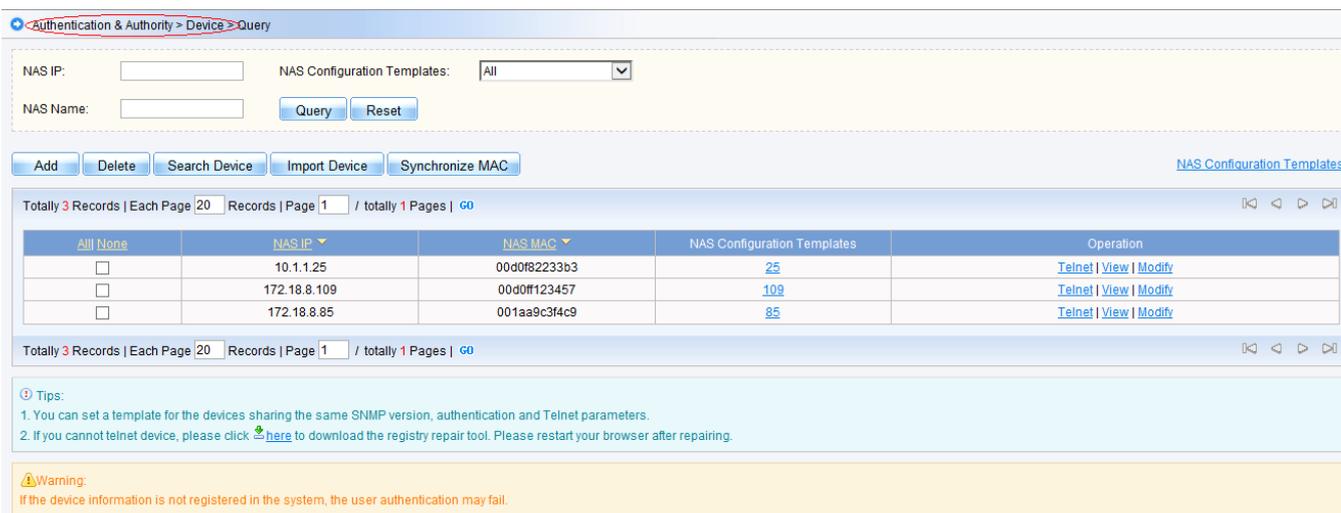
- [User Access – Wired Access](#)
- [User Access – Wireless Access](#)
- [User Access – Correlation with External Identity Center](#)
- [User Access – Web Authentication](#)
- [PEAP Authentication Configuration](#)

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.



Authentication & Authority > Device > Query

NAS IP: NAS Configuration Templates: All

NAS Name:

[NAS Configuration Templates](#)

Totally 3 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

All None	NAS IP	NAS MAC	NAS Configuration Templates	Operation
<input type="checkbox"/>	10.1.1.25	00d0f82233b3	25	Telnet View Modify
<input type="checkbox"/>	172.18.8.109	00d0ff123457	109	Telnet View Modify
<input type="checkbox"/>	172.18.8.85	001aa9c3f4c9	85	Telnet View Modify

Totally 3 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

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.

Authentication & Authority > Device > Add

Basic Information

* NAS IP: (Format: 192.168.20.1)

* NAS Configuration Templates: [Obtain Device Information](#) | [View Template](#) | [Add Template](#)

NAS MAC: (Format: 00D0F8000001)

NAS Name:

NAS Location:

NAS Information:

Select NAS Configuration Template *Add NAS Configuration Template*

Tips:
You can set a template for the devices sharing the same SNMP version, authentication and Telnet parameters.

[Add](#) [Reset](#) [Return](#)

Authentication & Authority > Device > Add

Basic Information

* NAS IP: (Format: 192.168.20.1)

* NAS Configuration Templates: [Obtain Device Information](#) | [View Template](#) | [Add Template](#)

NAS MAC: (Format: 00D0F8000001)

NAS Name:

NAS Location:

NAS Information:

Click to obtain device information automatically. The configured NAS configuration template must be consistent with the key or community name on the device.

Tips:
You can set a template for the devices sharing the same SNMP version, authentication and Telnet parameters.

[Add](#) [Reset](#) [Return](#)

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

Authentication & Authority > Device > NAS Configuration Templates > Add

Basic Information	
* Template Name:	RG-AC
* Type:	Ruijie Wired Device
Identity Authentication Configuration	
* Identity Authentication Key:	
Tips: The system and devices perform user authentication via the Radius Protocol. Identity authentication key is used for the encryption of data packets and should be the same as that of the devices.	
Web Authentication Configuration	
Web authentication Key:	
Tips: After the Web authentication key is specified, the system will support Web authentication.	
SNMP Configuration	
* SNMP v2c Community:	
Tips: The SNMP configuration should be the same as that on the devices. Otherwise the system cannot manage the devices.	
Security Management	
Device based NAC:	<input type="radio"/> Supported <input checked="" type="radio"/> Unsupported
Tips: You can set a template for the devices sharing the same SNMP version, authentication and Telnet parameters.	
<input type="button" value="Add"/> <input type="button" value="Reset"/> <input type="button" value="Close"/>	

- 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

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

Authentication & Authority > User Group > Query User Groups

User Group Name:

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

AllNone	User Group Name	Operation
<input type="checkbox"/>	new2	View Modify
<input type="checkbox"/>	new1	View Modify
<input type="checkbox"/>	Guest User Group	View Modify Restore Default Settings
<input type="checkbox"/>	Default User Group	View Modify Restore Default Settings

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

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

Authentication & Authority > User Group > Modify 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.
- When the network information verification is enabled, the client must upload network information and the uploaded network information must be consistent with that in the user information. Otherwise, authentication may be failed.
- Ruijie clients, such as RG-SA For Windows, will upload all network information while other clients do not upload hard disk serial number and IP address type.

Other Settings

Enable VPN Access

When network information verification is enabled, the server auto-learns the network binding information

The user can access the network only through Ruijie Security Agent.

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

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

Authentication & Authority > User Group > Query User Groups

User Group Name:

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

All/None	User Group Name	Operation
<input type="checkbox"/>	new2	View Modify
<input type="checkbox"/>	new1	View Modify
<input type="checkbox"/>	Guest User Group	View Modify Restore Default Settings
<input type="checkbox"/>	Default User Group	View Modify Restore Default Settings

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

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

Authentication & Authority > User Group > Modify 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.
- When the network information verification is enabled, the client must upload network information and the uploaded network information must be consistent with that in the user information. Otherwise, authentication may be failed.
- Ruijie clients, such as RG-SA For Windows, will upload all network information while other clients do not upload hard disk serial number and IP address type.

Other Settings

Enable VPN Access

When network information verification is enabled, the server auto-learns the network binding information

The user can access the network only through Ruijie Security Agent.

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

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

Authentication & Authority > External Identity Center

External Identity Center

Enable External Identity Center

Generic LDAP
 Windows AD Domain
 External Database
 Remote Radius Server
 Webservice

* LDAP Server IP:

* LDAP Server Port: (Default: 389)

* Root DN: [Auto-Obtain](#)

Root DN is the root node of an LDAP directory tree. For example, dc=my-domain and dc=com.

Support Anonymous

If the administrator password of the LDAP server is NULL, please select Anonymous Login.

* Administrator User Name:

For example, the administrator user name for OpenLDAP is the rootdn of the slapd.conf file. (For example, cn=Manager, dc=my-domain, and dc=com)

* Administrator Password:

For example, the administrator password for OpenLDAP is the rootpw of the slapd.conf file. (For example, secret)

* Identity Authentication Mode: Implement Identity Authentication by querying LDAP users Implement Identity Authentication by logging in to the LDAP server

* User ObjectClass:

* User Name Attribute Name:

The system queries users based on attributes of User ObjectClass and User Name Attribute Name.

* User Password Attribute Name:

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: [Select User Group](#)

If you don't configure the user group attribute name, all users newly learned will be added to this user group.

Existing users update the user group automatically

User Group Attribute Name:

If you configure User Group Attribute Name, the system will learn the user group from the LDAP server and add newly learned users to this group.

User Name Attribute Name: Address Attribute Name:

Telephone No. Attribute Name: Mobile No. Attribute Name:

Post Code Attribute Name: Email Address Attribute Name:

Test User Name:

Test Password: [Identity Authen](#)

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

[Modify](#) [Reset](#) [Refresh](#)

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.

Authentication & Authority > External Identity Center

External Identity Center

Enable External Identity Center

Generic LDAP
 Windows AD Domain
 External Database
 Remote Radius Server
 Webservice

No Windows AD Domain Server has been added to the system yet. Please click [Windows AD Domain Server](#) to view and configure the Windows AD Domain Server for login.

* Synchronization Interval for AD Domain User Info: days (from 1 to 28, default: 7)

Learn new users during authentication
 Learn the user group during new user authentication
 Existing users update the user group automatically

AD Domain User Attribute

- Beeper No.
- City/County
- Company
- Country
- Department
- Description

Attribute Mapping

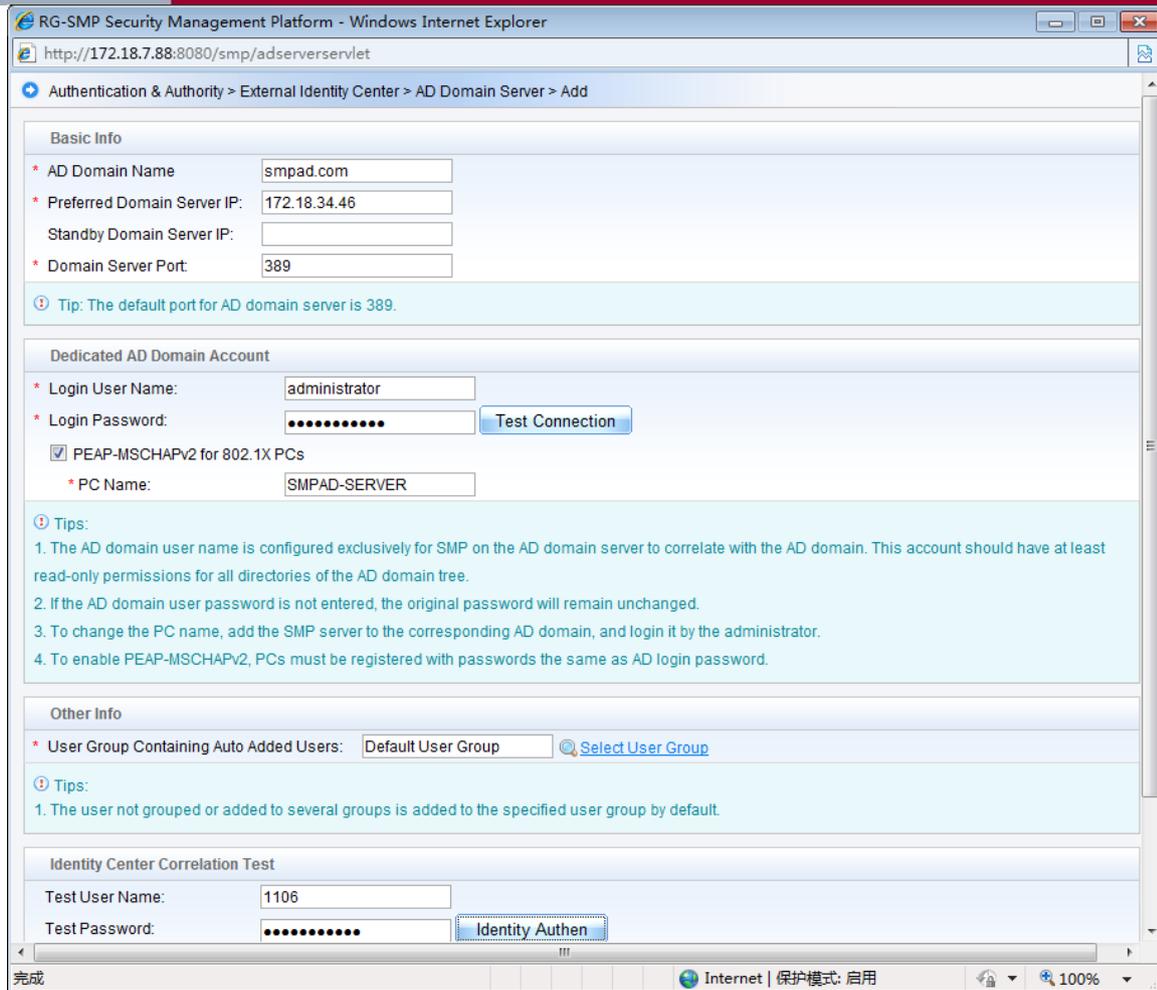
- Click the **Windows AD Domain Server** link to access the **AD Domain Server > Query** window. Click **Add** to add an AD domain server.

Authentication & Authority > External Identity Center > AD Domain Server > Query

AD Domain Name: Domain Server IP:

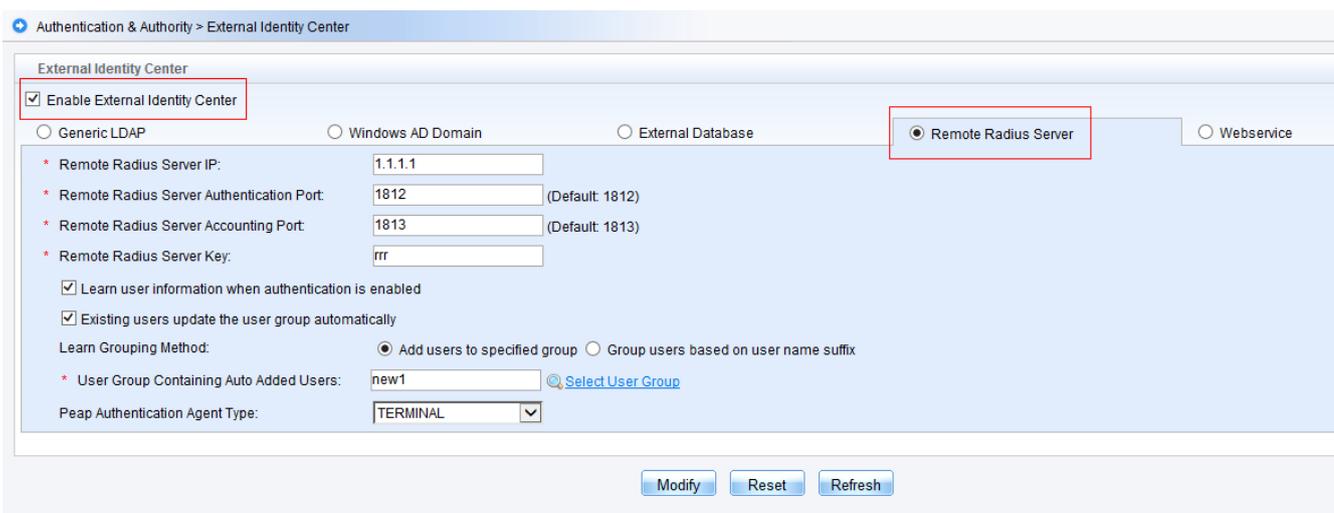
No matching AD domain server is found.

- 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.

External Identity Center

Enable External Identity Center

Generic LDAP
 Windows AD Domain
 External Database
 Remote Radius Server
 Webservice

* Database Type: SQL Server (Support SQL Server 2008 R2)
 * Database Server IP Address: 172.18.8.19
 * Database Server Port: 1433 (Default: 1433)
 * Administrator Account: sa
 * Administrator Password: ●●●●
 * Database Name: Test [Auto Obtain](#)
 * 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: [Select User Group](#)
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"/> to associate the tableUserInfo's <input type="text"/>	Add
Mobile No.	UserInfo	Mobile phone	Self Reference	Delete

Test User Name:
 Test Password: [Identity Authen](#)
You can verify whether a user passes database server authentication by entering a test user name and test password and clicking Identity Authentication.

[d_partyauthenservlet?kind=query#](#) [Modify](#) [Reset](#) [Refresh](#)

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.

External Identity Center

Enable External Identity Center

Generic LDAP
 Windows AD Domain
 External Database
 Remote Radius Server
 Webservice

* Remote Web Service Server IP:
 * Remote Web Service Server Port:
 * Remote Web Service Server Address: [Obtain](#)
 Remote Web Service Access URL:

You can click [Download WSDL File](#) to download the Web service information description file.

* Identity Authentication Mode:
 Log in to the remote Web server for Identity Authentication
 Query user Information on the Web service server for Identity Authentication

Learn new users during authentication

Learn the user group during new user authentication

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

If you don't configure mapping between the data element to be returned and user group information for the user information obtaining interface, all users newly learned will be added to the default user group.

Existing users update the user group automatically

Parameter Settings for Identity Authentication Interface

* Interface Name:

* Parameter indicates the user name in Data Type

* Parameter indicates the user password in Data Type [Add Parameter](#)

The return value in Type with content indicates that authentication succeeded.

Configure the User Information Obtaining Interface:
 Enable an Encryption and Decryption Plug-in:

Test User Name:
 Test Password: [Identity Authen](#)

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

Tip: If the Web service provided by the External Identity Center does not comply with WS-I specifications, or the security mechanism and other special configurations cause disconnection problems, please connect via the Web service adapter.

[Modify](#) [Reset](#) [Refresh](#)

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.

Authentication & Authority > User Group Query User Groups

User Group Name: [Query](#) [Reset](#)

[Add](#) [Delete](#)

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

AllNone	User Group Name	Operation
<input type="checkbox"/>	new2	View Modify
<input type="checkbox"/>	new1	View Modify
<input type="checkbox"/>	Guest User Group	View Modify Restore Default Settings
<input type="checkbox"/>	Default User Group	View Modify Restore Default Settings

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

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

User Group Name:

Multi-Access Limit

* An account can be used on a maximum of terminals at the same time (Default: 1)

An account can register mobile terminals (Default: 1)

A mobile terminal will be deregistered if it does not go online in consecutive days (Default: 90)

Tip: A registered mobile terminal can access a wireless SSID without providing the user name and password.

Time management of messages displayed on clients

A message displayed on a client automatically close in seconds (Time range: 5-300)

Tip: When auto-closing is disabled, the online bulletin and messages will not close automatically.

Ruijie Client Anti-Uninstall

Enable Ruijie Client Anti-Uninstall

Tip: When the Ruijie Client Anti-Uninstall is enabled, the Ruijie client user must enter a password before uninstalling the client.

User Password Management

Enable Initial Password Check (A user must change the initial password)

Enable Password Complexity Check

Enable Password Validity Period Check

Online users failing in Password Validity Check will be forced offline in minutes (Range: 3-60)

Enable Self-Service Password Change

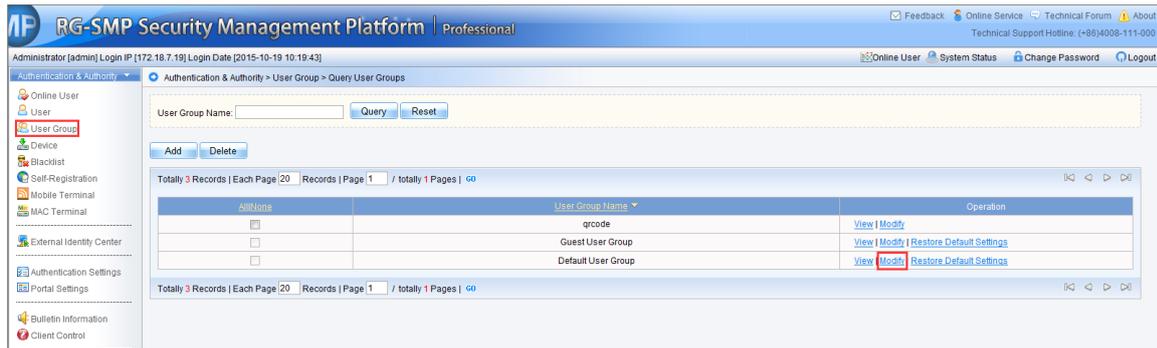
1.4.2 Configuring Offline Timer

Daily Timer

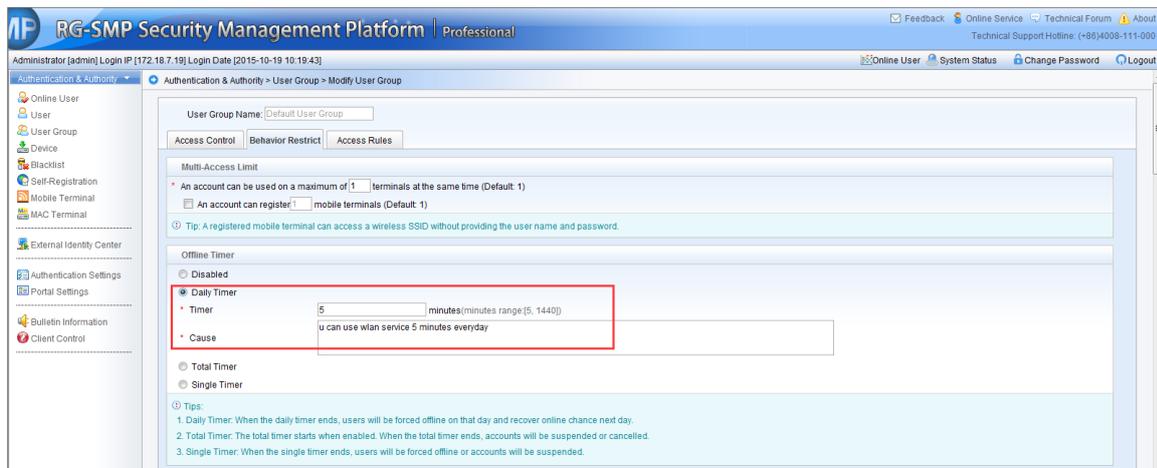
Daily Timer is used to set the maximum one-day online time X for users of a specified group on User Group setting page. (X is a positive integer in the unit of minutes, ranging from 5 to 1,440. The default value is 120 minutes.)

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.

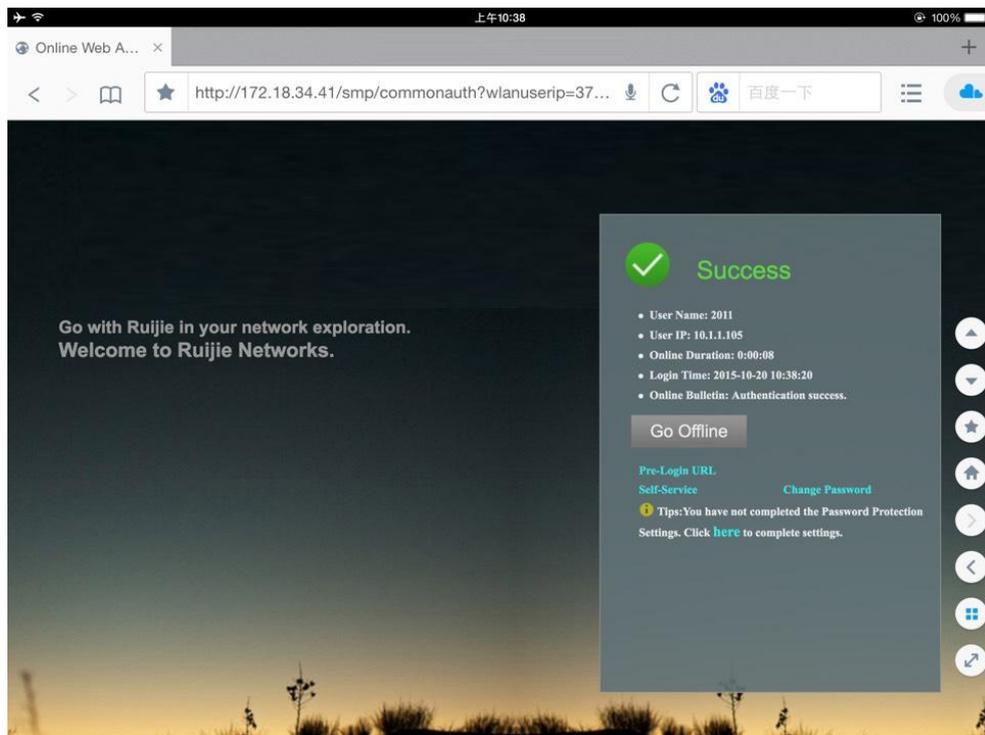
1. Choose **Authentication & Authority > User Group**, click **Modify** in the **Operation** column.



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



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



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

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

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!	View

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

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.

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

RG-SMP Security Management Platform Professional

Administrator [admin] Login IP [172.18.7.19] Login Date [2015-10-19 10:19:43]

Authentication & Authority > User Group > Query User Groups

User Group Name: Query Reset

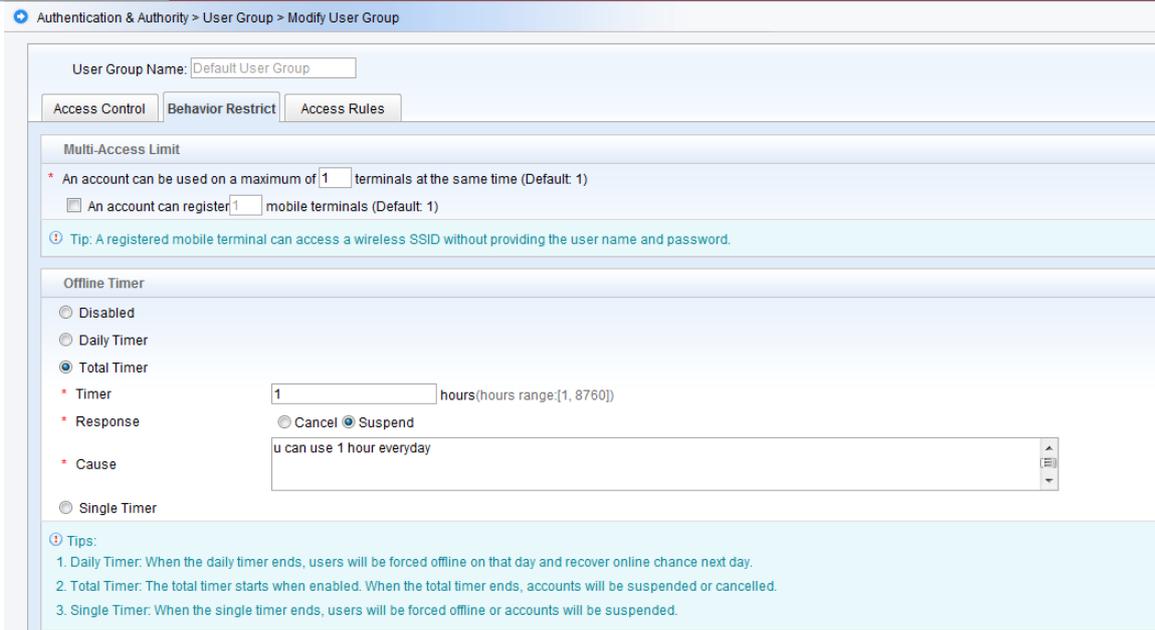
Add Delete

Totally 3 Records | Each Page 20 Records | Page 1 / totally 1 Pages | GO

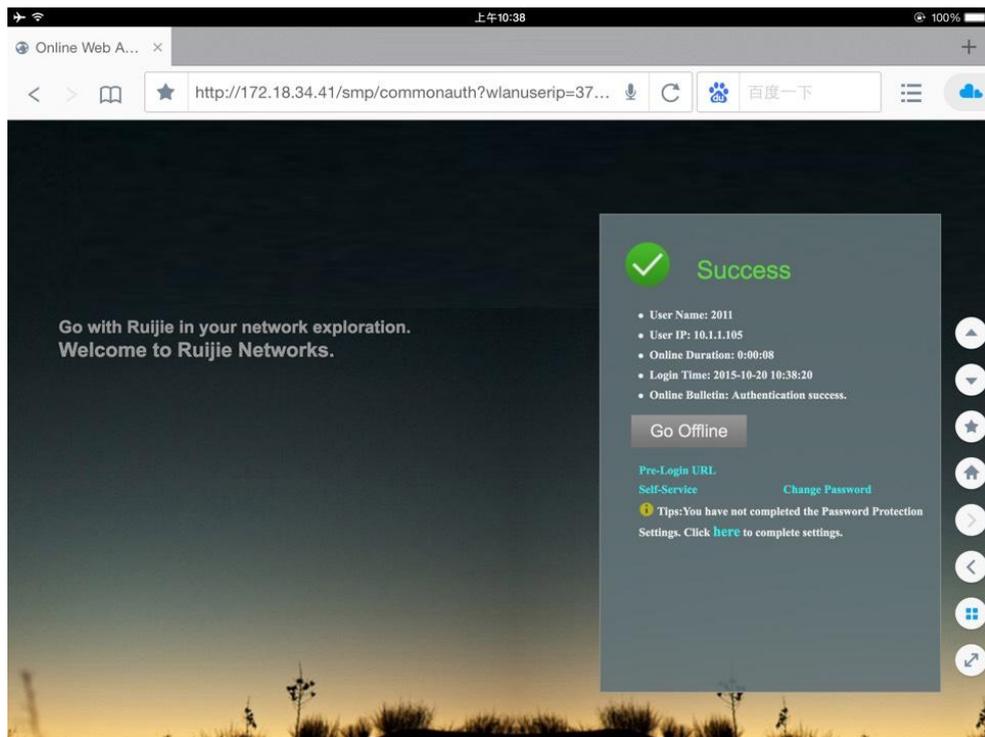
All None	User Group Name	Operation
<input type="checkbox"/>	grocode	View Modify
<input type="checkbox"/>	Guest User Group	View Modify Restore Default Settings
<input type="checkbox"/>	Default User Group	View Modify Restore Default Settings

Totally 3 Records | Each Page 20 Records | Page 1 / totally 1 Pages | GO

- 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.

Log Audit > Network Access Logs > Query Logs

User Name: User IP: Offline Cause: All

Login Time: 2015-10-20 0:00 Logout Time: 2015-10-20 23:59

[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!	View

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

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.

RG-SMP Security Management Platform Professional

Administrator [admin Login IP [172.18.7.19] Login Date [2015-10-19 10:19:43]

Authentication & Authority > User Group > Query User Groups

User Group Name: [Query](#) [Reset](#)

[Add](#) [Delete](#)

Totally 3 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [Go](#)

AllNone	User Group Name	Operation
<input type="checkbox"/>	qrcode	View Modify
<input type="checkbox"/>	Guest User Group	View Modify Restore Default Settings
<input type="checkbox"/>	Default User Group	View Modify Restore Default Settings

Totally 3 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [Go](#)

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

Authentication & Authority > User Group > Modify User Group

User Group Name:

Access Control | Behavior Restrict | Access Rules

Multi-Access Limit

- * An account can be used on a maximum of terminals at the same time (Default: 1)
- An account can register mobile terminals (Default: 1)

Tip: A registered mobile terminal can access a wireless SSID without providing the user name and password.

Offline Timer

Disabled
 Daily Timer
 Total Timer
 Single Timer

* Timer: minutes(minutes range:[5, 86400])

* Response: Offline Suspend

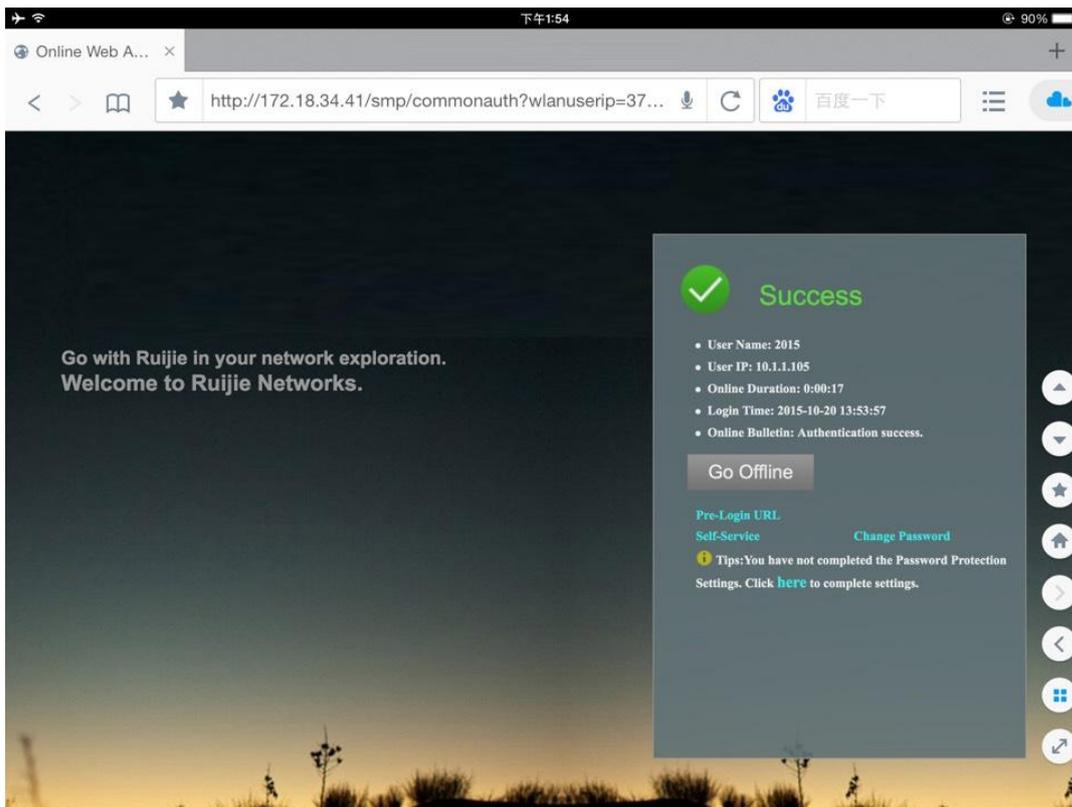
* Holding Time: minutes(minutes range:[5, 1440])

* Cause:

Tips:

1. Daily Timer: When the daily timer ends, users will be forced offline on that day and recover online chance next day.
2. Total Timer: The total timer starts when enabled. When the total timer ends, accounts will be suspended or cancelled.
3. Single Timer: When the single timer ends, users will be forced offline or accounts will be suspended.

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.

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 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!	View

Log Audit > Operation Logs > Query Logs

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

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

Totally 15 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.

1.4.3 Configuring QR Code Authentication

Prerequisite:

Configure the redirection addresses of Web authentication:

HTTP address: <http://172.18.8.140:80/smp/qrcodecardervlet>

HTTPS address: <https://172.18.8.140:443/smp/qrcodecardervlet>

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

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 > Modify User Group**. Check **Allow user to scan QR to authentication** box in **Guest User Management Rights** to allow QR authentication for the default user group.

Guest User Management Rights

Allow user to scan QR to authentication

Allow guest users to access network by scanning a QR Code

Allow managing guest users on a Ruijie client

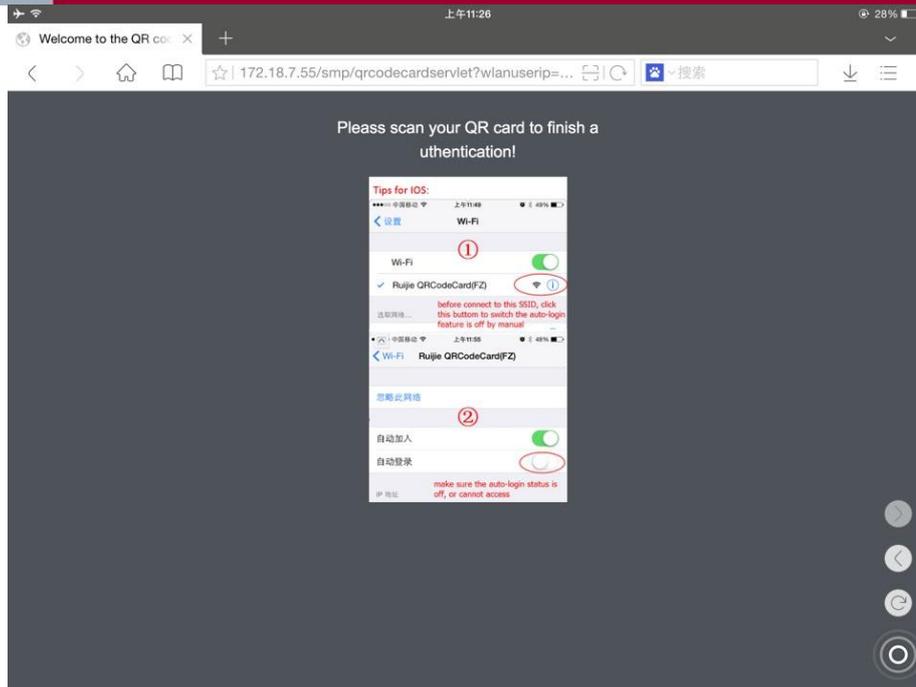
Allow managing guest users on a Ruijie Self-Service platform (registering users in common mode)

Allow managing guest users on a Ruijie Self-Service platform (registering users in SMS mode)

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

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

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

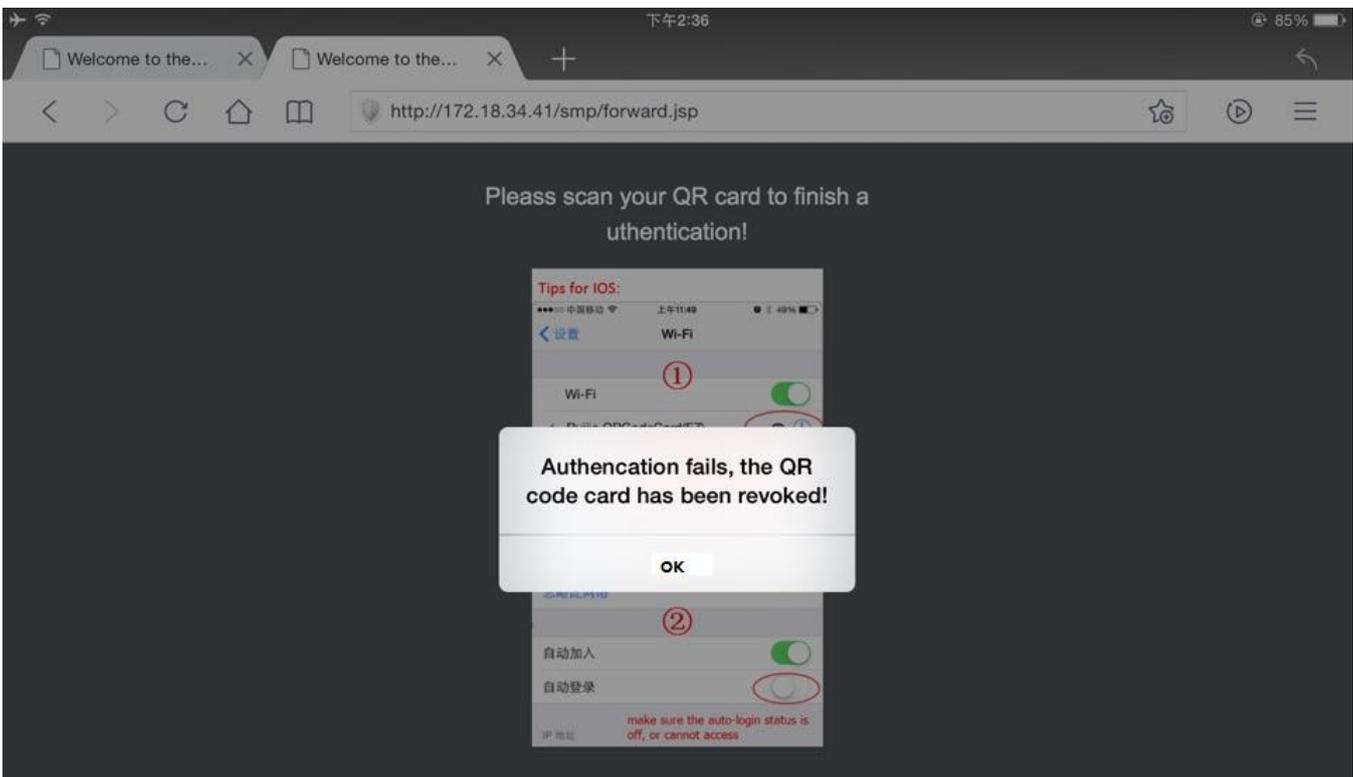
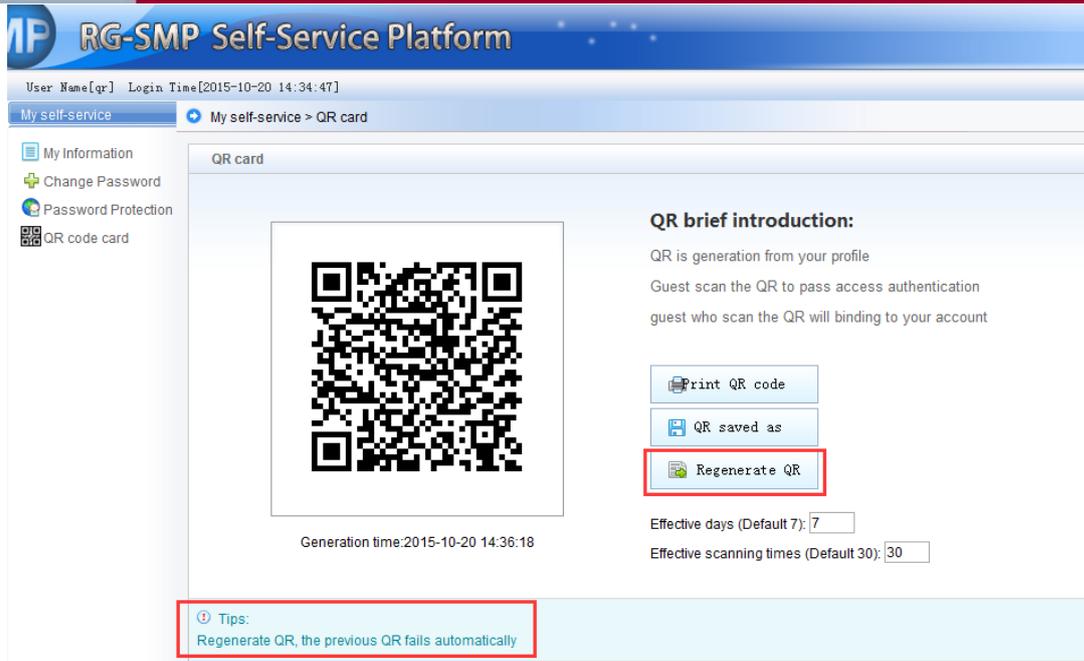


Scan the QR code displayed in RG-SMP Self-Service Platform by using QR scanners (e.g. WeChat App).

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.

Authentication & Authority > User Group Query User Groups

User Group Name:

Totally 4 Records | Each Page 20 Records | Page 1 / totally 1 Pages | GO

AllNone	User Group Name	Operation
<input type="checkbox"/>	new2	View Modify
<input type="checkbox"/>	new1	View Modify
<input type="checkbox"/>	Guest User Group	View Modify Restore Default Settings
<input type="checkbox"/>	Default User Group	View Modify Restore Default Settings

Totally 4 Records | Each Page 20 Records | Page 1 / totally 1 Pages | GO

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

Authentication via Web SMS Verification Code

Enable Authentication via Web SMS Verification Code

* Expiry time of SMS Verification Code is: minutes (Default: 15 minutes, range: 5-30 minutes)

Enable Mobile Phone Number Authentication

Tips:

1. ESA. Please disable Authentication via SMS Verification Code when authentication-exemption is enabled.
2. SMS verification codes can be checked only by an embedded portal.
3. Expiry time of SMS verification codes: After obtaining an SMS verification code, the user must submit it within the expiry time of the verification code.
4. When "Enable Mobile Phone Number Authentication" is selected, the system will automatically display a text box for the user to enter a mobile phone number.

1.4.5 Configuring Web Authentication

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

RG-SMP Security Management Platform Professional

Administrator [admin] Login IP [172.18.7.19] Login Date [2015-11-12 14:23:41]

Enable Guest Registration

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

* Bulletin Board Information:

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

User Group: [Select User Group](#)

QR wizard steps:

QR authentication success message:

Enable Guest QR Code Registration

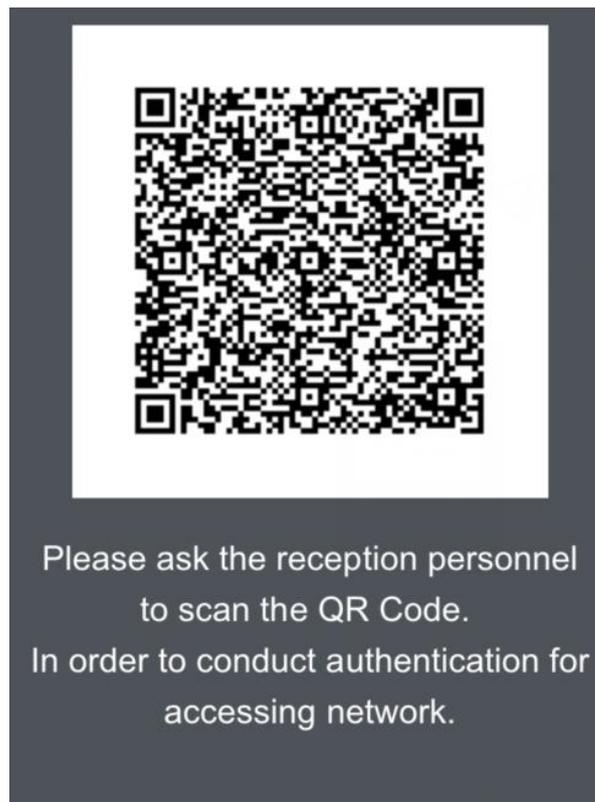
Enable Guest Validity Period by Scanner

Message for QR Code Scanning:

Message for Successful QR Code Authentication:

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:



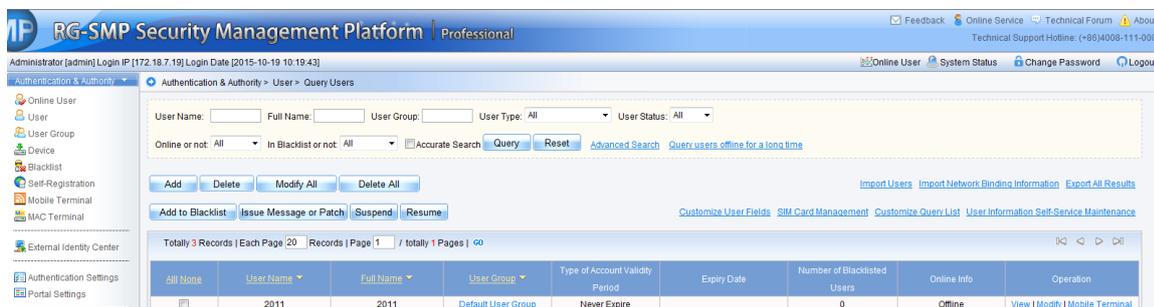
HTTPS access is supported. For details, see **Tips** in the **Authentication & Authority > Portal Settings** window.

1.4.6 Configuring Password Authentication

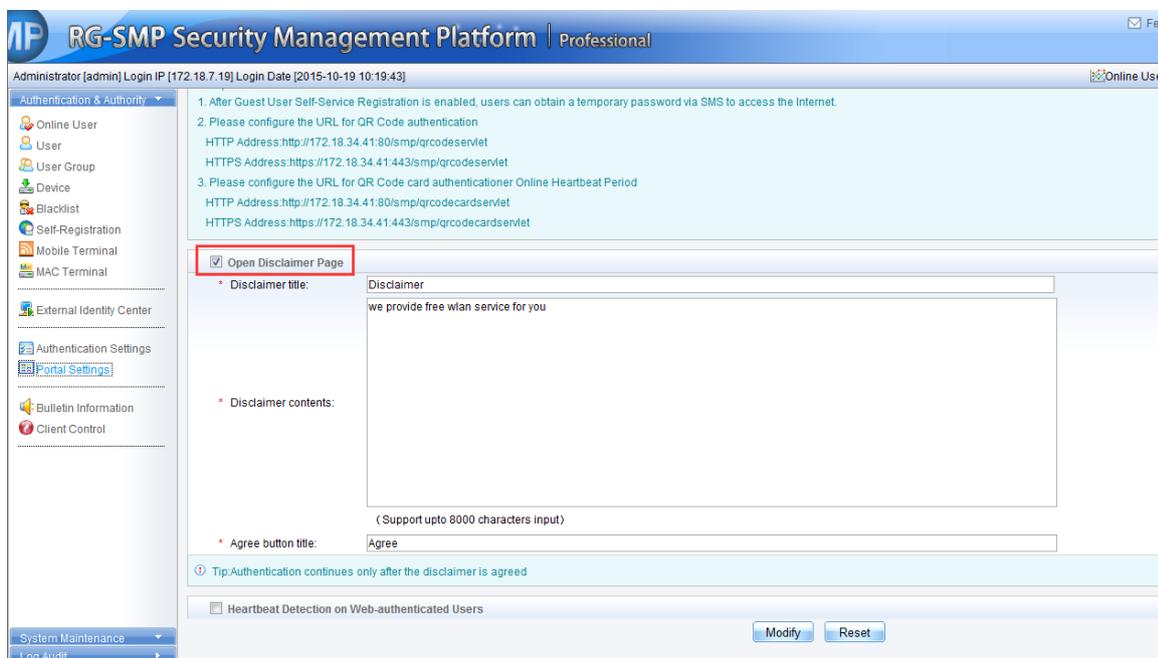
Disclaimer is added into the user authentication page. You can configure the disclaimer in **Portal Settings** menu.

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)

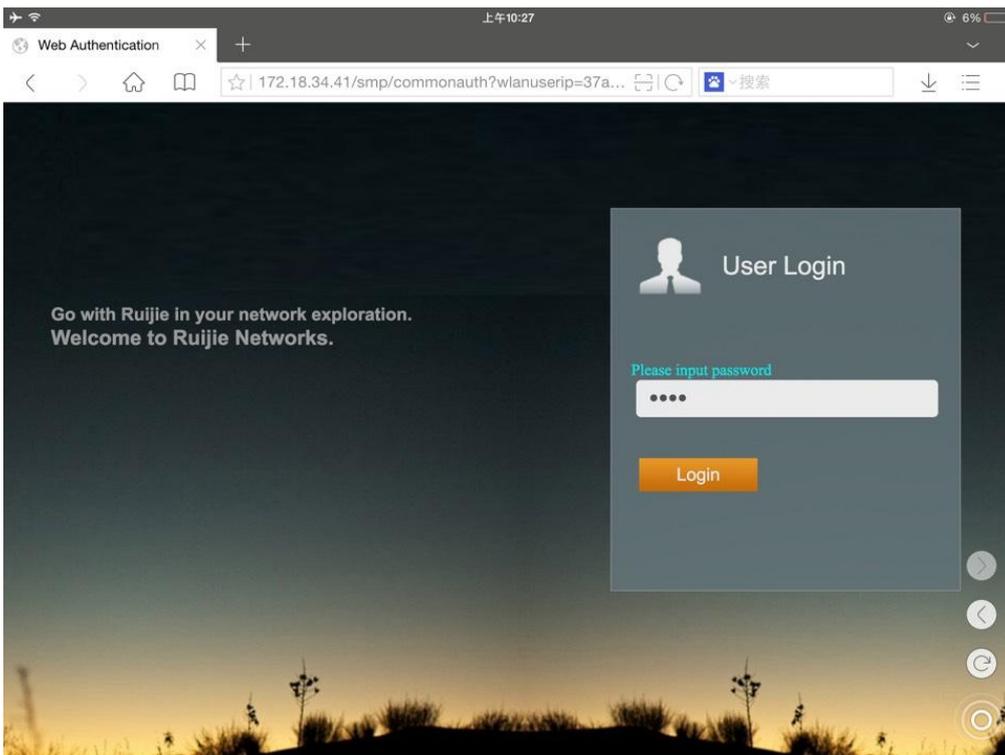
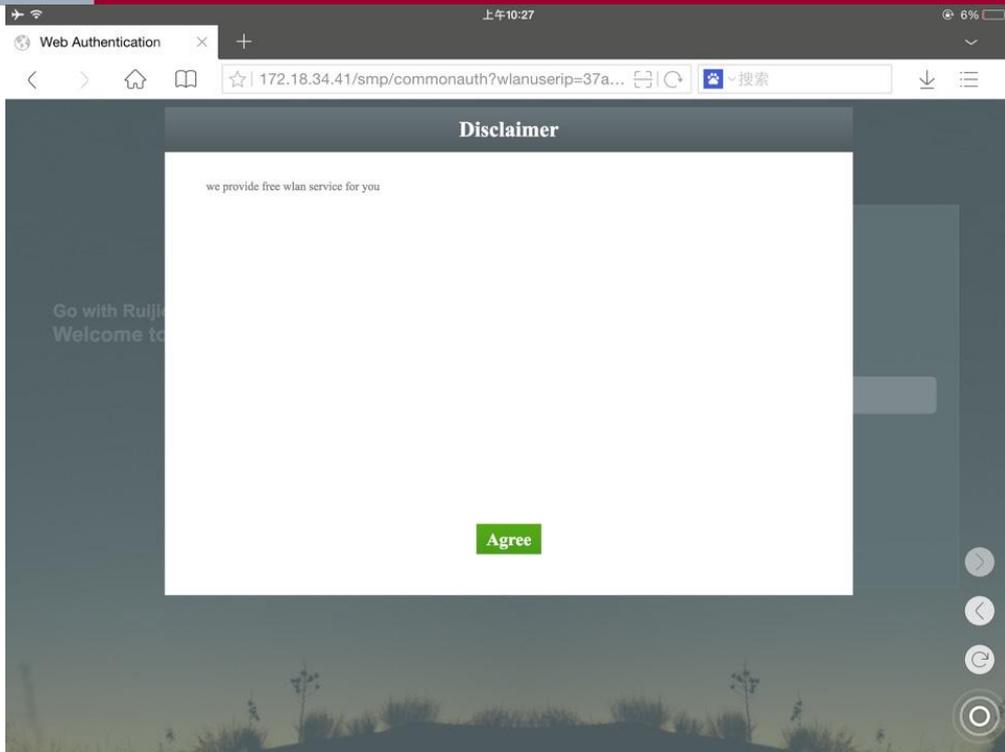
1. Choose **Authentication & Authority > User**. Click **Add** to add User 2011 with 2011 as its password.



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

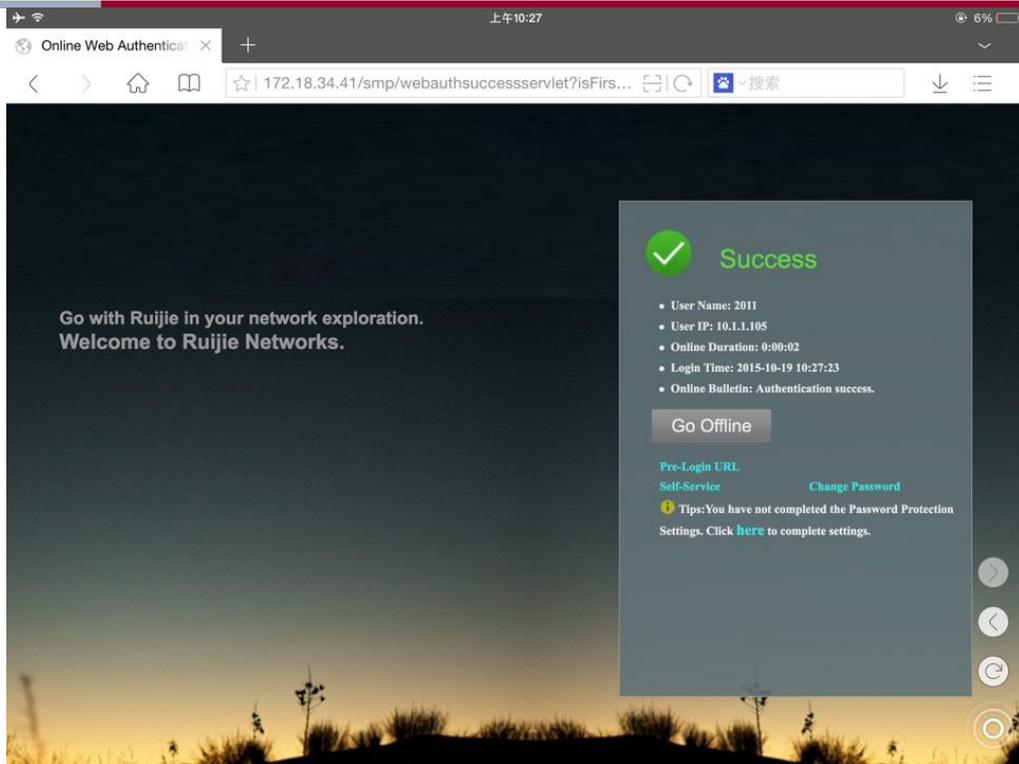


3. After Wi-Fi is connected, the disclaimer page is displayed. After the disclaimer is agreed, the login page will be displayed.



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.

Authentication & Authority > Authentication Settings

Authentication Parameters

* Authentication Port: (Default: 1812) * Accounting Port: (Default: 1813)

Record Update Flow:

Enable Nick Name Authentication:

When account logins exceed the limit, deal as follows:

Preferred Wireless Authentication:

Click [here](#) to import the wireless authentication server certificate.

Tip: The Authentication Port cannot be the same as the Accounting Port.

Periodic Online Status Detection

Periodic Online Status Detection:

* User Online Heartbeat Period: minutes (Default: 5)

Tips:

- When Periodic Online Status Detection is enabled, please enable non-Ruijie client accounting and set the accounting period to the User Online Heartbeat Period.
- When Periodic Online Status Detection is enabled and the system do not receive the User Online Heartbeat Notification within three consecutive User Online Heartbeat Periods, the system will assume that this user has gone offline and clear the user accordingly.

Password Anti Brute Force Protection

Enable Password Anti Brute Force Protection

When the times of keying an incorrect password exceeds times, within hours, the user account will be frozen.

Enable PEAP Authentication for Windows Client

* Auto-connect to SSID:

WIFI Security Type:

WIFI Encryption Type:

Second Stage of PEAP Authentication:

Click [here](#) to download WIFI Helper.

Tip: Administrators can download and distribute the WIFI helper to Windows users.

Account Expiration Warning

Account Expiration Warning:

SMS Account Expiration Warning:

Email Account Expiration Warning:

* Sending Account Expiration Warning days before. (Default: 7; Range: 1 to 30)

Every day, at o'clock to o'clock to send Email/SMS account expiration warning

Every hours to send Email/SMS account expiration warning (Default: 24; Range: 1 to 360)

Tips: Enabling SMS/Email Account Expiration Warning allows the system to hourly check the online status within the configured period and sends the warning messages if necessary. In every warning period, the Account Expiration Warning will be re-sent.

2. Change Preferred Wireless Authentication to PEAP-MSCHAP.

Authentication & Authority > Authentication Settings

Authentication Parameters

* Authentication Port: (Default: 1812) * Accounting Port: (Default: 1813)

Record Update Flow:

Enable Nick Name Authentication:

When account logins exceed the limit, deal as follows:

Preferred Wireless Authentication:

Click [here](#) to import the wireless authentication server certificate.

Tip: The Authentication Port cannot be the same as the Accounting Port.

Periodic Online Status Detection

Periodic Online Status Detection:

User Online Heartbeat Period: minutes (Default: 5)

Tips:

- When Periodic Online Status Detection is enabled, please enable non-Ruijie client accounting and set the accounting period to the User Online Heartbeat Period.
- When Periodic Online Status Detection is enabled and the system do not receive the User Online Heartbeat Notification within three consecutive User Online Heartbeat Periods, the system will assume that this user has gone offline and clear the user accordingly.

- 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

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

Authentication & Authority > Mobile Terminal > Query Mobile Terminal

User: MAC Address: Online Status: All

Registration Date: to

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

All None	User	MAC Address	Registration Date	Authentication Time	Authentication IP	Nas IP	Online Status	Operation
<input type="checkbox"/>	111	1234567141b6	2013-12-19 11:30:48	2013-12-20 15:14:13	172.18.8.197	172.18.8.85	Offline	View

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

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.

Authentication & Authority > 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"/>	111	111	new2	Never Expire		0	Offline	View Modify Mobile Terminal
<input type="checkbox"/>	1111	1111	Default User Group	Never Expire		0	Offline	View Modify Mobile Terminal
<input type="checkbox"/>	222	222	new2	Never Expire		0	Offline	View Modify Mobile Terminal
<input type="checkbox"/>	666	666	new2	Never Expire		0	Offline	View Modify Mobile Terminal
<input type="checkbox"/>	777	7777777	new2	Never Expire		0	Offline	View Modify Mobile Terminal
<input type="checkbox"/>	hkp	huangkaipen	new2	Never Expire		0	Offline	View Modify Mobile Terminal

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

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.

Authentication & Authority > Mobile Terminal > Query Mobile Terminal

User: MAC Address: Online Status: All

Registration Date: to

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

All None	User	MAC Address	Registration Date	Authentication Time	Authentication IP	Nas IP	Online Status	Operation
<input type="checkbox"/>	111	1234567141b6	2013-12-19 11:30:48	2013-12-20 15:14:13	172.18.8.197	172.18.8.85	Offline	View

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

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

Authentication & Authority > Mobile Terminal > Import

Upload Import File

Importing File (*.xls):

Tips:

- The mobile terminals cannot exceed 10,000.
- Only EXCEL files based on template format can be imported. Click [here](#) to download the Import Template.
- If the required information is not included in the Import Template, users can create a new file based on the template.

1.5.4 Deleting Mobile Terminals

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

Authentication & Authority > Mobile Terminal > Query Mobile Terminal

User: MAC Address: Online Status: All

Registration Date: to

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

All None	User	MAC Address	Registration Date	Authentication Time	Authentication IP	Nas IP	Online Status	Operation
<input checked="" type="checkbox"/>	111	1234567141b6	2013-12-19 11:30:48	2013-12-20 15:14:13	172.18.8.197	172.18.8.85	Offline	View

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

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

Authentication & Authority > Mobile Terminal > Query Mobile Terminal

User: MAC Address: Online Status: All

Registration Date: to

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

All None	User	MAC Address	Registration Date	Authentication Time	Authentication IP	Nas IP	Online Status	Operation
<input type="checkbox"/>	111	1234567141b6	2013-12-19 11:30:48	2013-12-20 15:14:13	172.18.8.197	172.18.8.85	Offline	View

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

2 FAQ

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

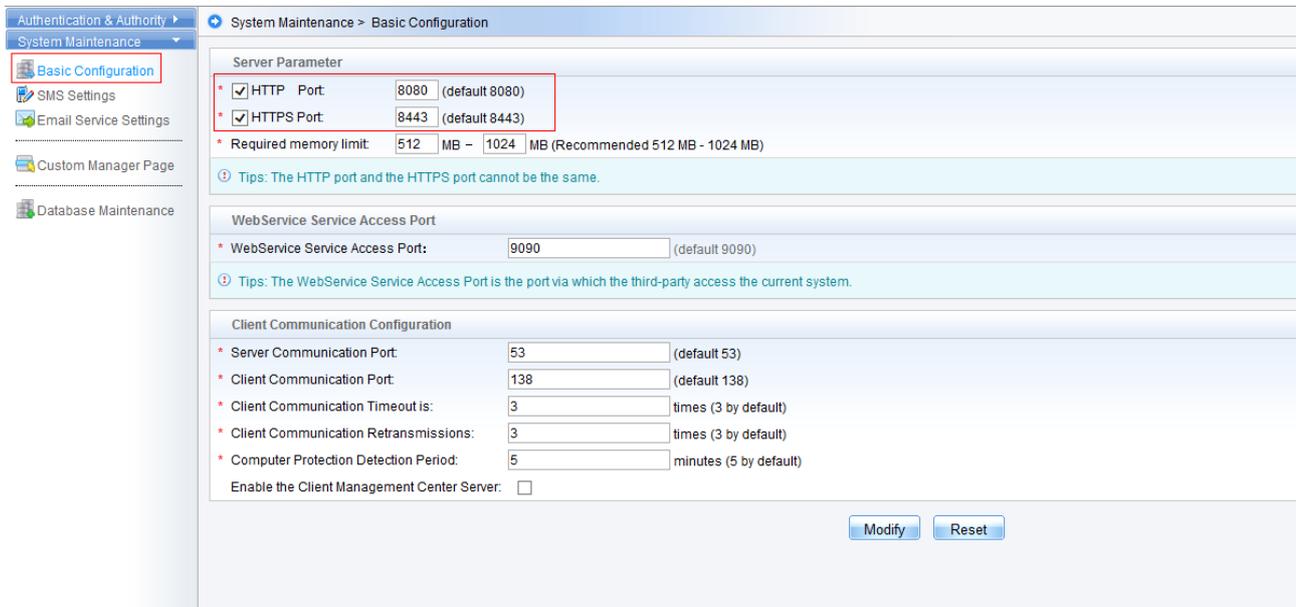
Type `http://local IP address:8080/smp/index.jsp` in the address bar of your browser. Enter the user name (**admin**) and password (**11111111**) of the system administrator in the login window.

- 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.

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