

# **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.



**Red-Giant**<sup>®</sup>, **Red-Giant ぞ**の。<sup>®</sup>, 锐捷<sup>®</sup> 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: <u>http://www.ruijienetworks.com/</u>
- Ruijie service portal: <u>http://case.ruijienetworks.com</u>



## Contents

Contents	
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	
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:

- <u>User Access Wired Access</u>
- <u>User Access Wireless Access</u>
- <u>User Access Correlation with External Identity Center</u>
- <u>User Access Web Authentication</u>
- <u>PEAP Authentication Configuration</u>

## 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 Temp	lates: All 💙			
Add Delete S	earch Device Import Device Sy	nchronize MAC		NAS Configurati	on Templates
Totally 3 Records   Each Pa	ige 20 Records   Page 1 / totally 1 P	ages   GO		DI.	
All  None	NAS IP	NAS MAC 🔻	NAS Configuration Templates	Operation	
	10.1.1.25	00d0f82233b3	<u>25</u>	Telnet   View   Modify	
	172.18.8.109	00d0ff123457	<u>109</u>	Telnet   View   Modify	
	172.18.8.85	001aa9c3f4c9	<u>85</u>	Telnet   View   Modify	
Totally 3 Records   Each Pa	age 20 Records   Page 1 / totally 1 P	ages   GO		D4	
<ol> <li>Tips:</li> <li>You can set a template for</li> <li>If you cannot telnet device</li> </ol>	r the devices sharing the same SNMP versi , please click <sup>®</sup> <u>here</u> to download the regis	on, authentication and Telnet parameters. ry repair tool. Please restart your browser	after repairing.		
AWarning: If the device information is n	ot registered in the system, the user auther	tication 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: Not Selected	Obtain Device Information   View Template   Add Template
NAS MAC:	(Format 00D0F8000001)
NAS Name: Template	Add WAS Configuration Template
NAS Location:	
NAS Information:	
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	

Basic Information					
* NAS IP:	10.1.1.25	(Format: 192	.168.20.1)		
* NAS Configuration Templates:	Ruijie Wireless Device 🗸	Obtain Devic	e Information	View Template   Add Template	
NAS MAC:	00d0f82233b3	(Format: 00E	0F8000001)	J	
NAS Name:	Ruijie		Click to obtain	in device information automatically.	
NAS Location:	32#AC		be consisten	it with the key or community name on	
NAS Information:	Ruijie 10G Wireless Switch By Ruijie Networks.	h(WS5708)	the device.		
🕡 Tips:					
You can set a template for the dev	ices sharing the same SNMF	version, auth	entication and	d Telnet parameters.	
				Add Reset Re	turn

To add a NAS configuration template, click Add Template.



Authentication & Authority > Device > NAS Configuration Templates > Add

Template Name:	RG-AC	* Type:	Ruijie Wired Device 🔽	
Identity Authentication Co	nfiguration			
Identity Authentication Key:				
D Tips:The system and devi hould be the same as that c	ces perform user authentica of the devices.	ation via the Radius Protocol. Identity auther	ntication key is used for the encryption of data	packets
Web Authentication Confi	guration			
Web authentication Key:				
Dips:After the Web authen	tication key is specified, the	system will support Web authentication.		
SNMP Configuration				
SNMP v2c Community:				
D Tips:The SNMP configural	iion should be the same as	that on the devices. Otherwise the system	cannot manage the devices.	
Security Management				
Device based NAC:	⊖Supported   Osup	pported		
1 Tips:				
You can set a template for t	he devices sharing the sam	ne SNMP version, authentication and Telnet	parameters.	

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



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.



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   G0				
AllNone	User Group Name 🔻	Operation			
	new2	View Modify			
	new1	View   Modify			
	Guest User Group View   Modify   Restore Default Settings				
	Default User Group	View Modify Restore Default Settings			
Totally 4 Records   Each Page 20 Records	Page 1 / totally 1 Pages   G0				

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

#### Authentication & Authority > User Group > Modify User Group

Access Central Rebavior Postrict Access Pulses		
Enable Wired Access	Enable Wireless Access	
Network Information Verification All	Network Information Verificati	on 🗌 All
HD Serial Number Verification	HD Serial Number Verificati	on
IP Type Authentication 💿 Static 🔘 Dynamic	IP Type Authentication 🔘 S	Static 🔘 Dynamic
	User IP Verification	
	User MAC Verification	
	User IMSI	
User IMSI		
NAS IP Verification	SSID Verification	^
NAS Port Verification		~
D Tips:		
1. Wireless SSID names are separated by commas (,), e.g., web-wired-SSID, web-wireles	s-SSID.	
<ol><li>The MAC address verification and the IMSI number/mobile phone number verification ca</li></ol>	nnot be enabled at the same time.	
3. When the network information auto-learning and the network information verification are	enabled, you can bind users to networks. Or the system wi	II bind users to networks through network information auto-learning in the
next authentication.		
<ol> <li>when the network information vehication is enabled, the client must upload network into failed.</li> </ol>	ormation and the uploaded network information must be co	nsistent with that in the user information. Otherwise, authentication may be
raireu. 5. Ruijie cliente, such as RC-SA For Windows, will unload all network information while off	ar clients do not unload bard disk serial number and IP ad	drace time
		areas gpc.
Other Settings		
✓ When network information verification is enabled, the server auto-learns the network bi	inding 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

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   60	
AllINone	User Group Name	Operation
	new2	View   Modify
	new1	View   Modify
	Guest User Group	View   Modify   Restore Default Settings
	Default User Group	View Modify Restore Default Settings
Totally 4 Records   Each Page 20 Records	Page 1 / totally 1 Pages   G0	

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

User Group Name: Default User Group		
Access Control Behavior Restrict Access Rules		
✓ Enable Wired Access	Enable Wireless Access	
Network Information Verification 🗌 All	Network Information Verification All	
HD Serial Number Verification	HD Serial Number Verification	
IP Type Authentication   Static  Dynamic	🗌 IP Type Authentication 💿 Static 🔘 Dynamic	
User IP Verification	User IP Verification	
	User MAC Verification	
	User IMSI	
User IMSI		
NAS IP Verification	SSID Verification	C
NAS Port Verification		
D Tips: 1 Wireless CCID names are constrained by common (1) a.e. web wired CCID, web wireless 1		
<ol> <li>Wretess SSID names are separated by commas (,), e.g., web-wrete-SSID, web-wretess-</li> <li>The MAC address verification and the IMSI number/mobile phone number verification cannot be addressed and the IMSI number/mobile phone number verification cannot be addressed and the IMSI number/mobile phone number verification.</li> </ol>	ot be enabled at the came time.	
3. When the network information auto-learning and the network information verification are en	abled, you can bind users to networks. Or the system will bind users to networks th	rough network information auto-learning in the
next authentication.		
4. When the network information verification is enabled, the client must upload network inform	nation and the uploaded network information must be consistent with that in the use	er information. Otherwise, authentication may be
ailed.		
5. 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		
I When network information verification is enabled, the server auto-learns the network bind	ling information	
The user can access the network only through Buijie 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**

- 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.



Authentication & Authority > External Identity Center

External identity Center				
Enable External Identity Center				
Generic LDAP	○ Windows AD Domain	<ul> <li>External Database</li> </ul>	O Remote Radius Server	O Webservice
* LDAP Server IP:				
* LDAP Server Port:	389	(Default: 389)		
* Root DN:		Auto-Obtain		
Root DN is the root node of an LDAP dire	ctory tree. For example, dc=my-doma	ain and dc=com.		
Support Anonymous				
If the administrator password of the LDA	e server is NULL, please select Anon	nymous Login.		
* Administrator User Name:				
For example, the administrator user nam	e for OpenLDAP is the rootdn of the s	slapd.conf file. (For example, cn=Manager, dc	=my-domain, and dc=com)	
<ul> <li>Administrator Password:</li> </ul>				
For example, the administrator password	I for OpenLDAP is the rootpw of the s	apd.conf file. (For example, secret)		
* Identity Authentication Mode:	<ul> <li>Implement Identity Author</li> </ul>	entication by querying LDAP users 🔘 Impler	nent Identity Authentication by logging in to the	LDAP server
* User ObjectClass:	person			
* User Name Attribute Name:	uid			
The system queries users based on a	ttributes of User ObjectClass and Us	ser Name Attribute Name.		
* User Password Attribute Name:	userPassword			
Enable an Encryption and Decryption Plu	g-in:			
Learn new users during authentication	n			
Learn the user group during new us	ser authentication			
* User Group Containing Auto Added Us	ers:	Select User Group		
If you don't configure the user group att	ribute 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 Nan	ne, the system will learn the user gro	up from the LDAP server and add newly learn	ed users to this group.	
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:		
Test User Name:				
Test Password:		Identity Authen		
You can verify whether a user passes LD	AP server authentication by entering	a test user name and test password and clic	king Identity Authentication.	

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.



Auther	ntication & Authority > External Identity	y Center				
Exterr	nal Identity Center					
🗹 Enat	ble External Identity Center					
O Ge	neric LDAP	Windows	AD Domain	O External Database	O Remote Radius Server	O Webservice
No W	/indow AD Domain Server has been :	added to the syste	m yet.Please click Wind	lows AD Domain Server" to view and con	figure the Windows AD Domain Server for login.	
* Syn	chronization Interval for AD Domain U	User Info: 7	days (fr	om 1 to 28, default: 7)		
~	Learn new users during authenticat	tion				
	Learn the user group during new u	user authenticatior	1			
~	Existing users update the user grou	up automatically				
	Beeper No.		Attribute Mapping			
	City/County Company					
	Country Department					
	Description					
		44				
	SMP User Attribute					
	Email Address					
	Mobile No.					
	Postal Code Telephone No.					
	·					
				Marilla Davada	2-6	
				wouldy Reset	tellesi	

3. 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 : Query Reset			
Add Delete Close				
	No matching AD domain server is found.			

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



RG-SMP Security Manageme	nt Platform - Windows Interne	et Explorer 📃 🗖 🗖
http://172.18.7.88:8080/smp/	/adserverservlet	
Authentication & Authority > Example 2	xternal Identity Center > AD Dom	nain Server > Add
Dagia Info		
Basic Into		
* AD Domain Name	smpad.com	
* Preferred Domain Server IP:	172.18.34.46	
Standby Domain Server IP:		
* Domain Server Port:	389	
(1) Tip: The default port for AD d	lomain server is 389.	
Dedicated AD Domain Accou	int	
* Login User Name:	administrator	]
* Login Password:	•••••	Test Connection
PEAP-MSCHAPv2 for 802.	1X PCs	
* PC Name:	SMPAD-SERVER	]
<ol> <li>The AD domain user name is read-only permissions for all dir 2. If the AD domain user passw</li> <li>To change the PC name, add</li> <li>To enable PEAP-MSCHAPv2,</li> </ol>	rectories of the AD domain tree. ord is not entered, the original pa i the SMP server to the correspor PCs must be registered with pa	asswords the same as AD login password.
Other Info		
* User Group Containing Auto A	Added Users: Default User Gr	roup Q Select User Group
<ol> <li>Tips:</li> <li>The user not grouped or added</li> </ol>	ed to several groups is added to	) the specified user group by default.
Identity Center Correlation T	est	
Test User Name:	1106	
Test Password:	•••••	Identity Authen
		• • • • • • • • • • • • • • • • • • •
, hk		😽 Internet   保护模式: 启用 🛛 🐴 🔻 💐 100% 🔻

## **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.

Authentication & Authority > Extern	al Identity Center				
External Identity Center	1				
Inable External Identity Center					1
O Generic LDAP	O Wi	ndows AD Domain	O External Database	Remote Radius Server	O Webservice
* Remote Radius Server IP:		1.1.1.1	]		]
* Remote Radius Server Authen	ntication Port:	1812	(Default 1812)		
* Remote Radius Server Accour	nting Port:	1813	(Default 1813)		
* Remote Radius Server Key:		m	]		
Learn user information wh	en authentication is	enabled			
Existing users update the update	user group automati	ically			
Learn Grouping Method:		Add users to specified	group 🔘 Group users based on user name	suffix	
* User Group Containing Aut	o Added Users:	new1	Select User Group		
Peap Authentication Agent Typ	e:	TERMINAL	J		
			Modify	Refresh	

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



External Identity Ce

#### **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.

Enternaria dentity conter							
<ul> <li>Enable External Identity Center</li> </ul>	er			1			
O Generic LDAP	O Windows AD Domain		<ul> <li>External Database</li> </ul>		O Remote Radius Server	O Webservice	
* Database Type	SQL Server	🖌 (Supp	ort SQL Server 2008 R2)	]			
* Database Server IP Address	s: 172.18.8.19						
* Database Server Port:	1433	(Defau	ılt: 1433)				
* Administrator Account:	sa						
* Administrator Password:	••••						
* Database Name:	Test	Au	ito Obtain				
* Database Character Set:	◉ UTF-8 ◯ GBK						
* In Table User	rInfo 👻 Column UserID	<b>▼</b> i:	s user name, Column Passwo	ord 💌 is p	assword.		
Learn new users during	authentication						
<ul> <li>Learn the user group</li> </ul>	during new user authentication						
* User Group Containing /	Auto Added Users: new2	2	Select User Group				
If you don't configure ma	pping among the user group, table name	and column nar	ne, all users newly learned wi	II be added to this	user group.		
<ul> <li>Existing users update th</li> </ul>	ie user group automatically						
Enable an Encryption and D	Decryption Plug-in:						
If the user password of the	database server is encrypted, you can ena	able and configu	re an encryption and decryptic	n plug-in by clicki	ng 😩 Import Password Plug-in to in	mport a password plug-in	
You can configure mapping a	among the user group, table name and co	lumn name to e	nable the system to learn use	r information from	the database during user autheni	lication.	
					-		
User	Table Name		Column Name		Association		Operation
User Group 🗸	~		~		Use table's	×	Add
				to asso	ciate the tableUserInfo's	•	
Mobile No.	UserInfo		Moblie phone		Self Reference		Delete
Test User Name:	111						
Test Password	•••	Identity Au	then				
You can verify whether a use	er passes database server authentication	by entering a te	st user name and test passwo	ord and clicking Ide	entity Authentication.		
		-, ing a to					
					7		
partyauthenservlet?kind=que	ry#		Modify Res	et 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	O Windows AD Domain	◯ External Database	O Remote Radius Server	Webservice
* Remote Web Service Server IP:				
* Remote Web Service Server Port:				
* Remote Web Service Server Addr	ess:	Obtain		
Remote Web Service Access URL	L: http://:/			
You can click <sup>g</sup> <u>Download WSDL</u>	File to download the Web service informatio	n description file.		
* Identity Authentication Mode:	Log in to th	e remote Web server for Identity Authentication	□ ○ Query user Information on the Web service se	ver for Identity Authentication
Learn new users during authe	entication			
Learn the user group during	g new user authentication			
* User Group Containing Auto A	dded Users:	Q Select User Group		
If you don't configure mapping	between the data element to be returned and	d user group information for the user informat	on obtaining interface, all users newly learned will	be added to the default user group.
Existing users update the use	r group automatically			
	·			
Parameter Settings for Identit	y Authentication Interface			
* Interface Name:	¥			
* Parameter indicates the u	ser name in Data Type Charact 🗸			
* Parameter indicates the u	ser password in Data Type Charact 🗸 🗛	Id Parameter		
The return value in Type Chara	act 🗸 with content	indicates that authentication succeeded.		
Overfreen the Line of ferrentian O				
Conligure the Oser Information O	blanning interface.			
Enable an Encryption and Decrypt	tion Plug-in:			
Test User Name				
Test Password	Identity Aut	hen		
You can verify whether a user pas	ses remote web service server authenticatio	n by entering a test user name and test pass	word and clicking Identity Authentication.	
) Tip: If the Web service provided by t	he External Identity Center does not comply v	vith WS-I specifications, or the security mecha	nism and other special configurations cause disco	nnection problems, please connect via the V
ervice 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.

	ry User Groups									
User Group Name:	Query Reset									
Add Delete										
Totally 4 Records   Each Page 20 Records	Page 1 / totally 1 Pages   G0									
AllNone	User Group Name 🎽	Operation								
	new2	View   Modify								
	new2 new1	View   Modify View   Modify								
	new2 new1 Guest User Group	View   Modify View   Modify View   Modify   Restore Default Settings								
	new2 new1 Guest User Group Default User Group	View   Modify View   Modify View   Modify   Restore Default Settings View   Modify   Restore Default Settings								

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



User Group Name: Default User Group
Access Control Behavior Restrict Access Rules
Multi-Access Limit
* An account can be used on a maximum of 1 terminals at the same time (Default: 1)
An account can register 1 mobile terminals (Default: 1)
A mobile terminal will be deregistered if it does not go online in consecutive 90 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 0 seconds (Time range: 5-300)
Itip: When auto-closing is disabled, the online bulletin and messages will not close automatically.
Ruijie Client Anti-Uninstall
Enable Ruijie Client Anti-Uninstall
(1) 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.



AP RG-SMP S	Security Management I	Platform Professional		🖂 Feedback 💈 Online Se Technica	rvice 🗢 Technical Forur al Support Hotline: (+86)40	n <u> About</u> 008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-10-19 10:19:43]			🖾 Online User 🚨 System Status	🔓 Change Password	
Authentication & Authority 👻	<ul> <li>Authentication &amp; Authority &gt; User Group &gt; Query</li> </ul>	User Groups				
Conline User	User Group Name:	Query Reset				
Device	Add Delete					
Self-Registration	Totally 3 Records   Each Page 20 Records   Page	age 1 / totally 1 Pages   G0				> 00
Mobile Terminal	AllINone		User Group Name 🔻	Operation		
			qrcode	View Modify		
💃 External Identity Center			Guest User Group	View   Modify   Restore Default Settings	1	
Authentication Settings			Default User Group	View Modify Restore Default Setting	1	
E Portal Settings	Totally 3 Records   Each Page 20 Records   Page 20	age 1 / totally 1 Pages   G0			19 9 0	> (>0
Client Control						

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

IP RG-SMP	Security Managem	ent Platform   Professional		🔽 Feedback 🍃 Online Se Technica	rvice 🗢 Technical Forun Il Support Hotline: (+86)40	n 🚹 About 008-111-000
Administrator [admin] Login IP [1	172.18.7.19] Login Date [2015-10-19 10:19:4	13]		🖾 Online User 🚨 System Status	🔓 Change Password	
Authentication & Authority	<ul> <li>Authentication &amp; Authority &gt; User Group</li> </ul>	ip > Modify User Group				^
Suser	User Group Name: Default Use	r Group				
🐣 User Group 🏂 Device	Access Control Behavior Restri	Access Rules				
Blacklist	Multi-Access Limit					
Mobile Terminal	* An account can be used on a may	imum of 1terminals at the same time (Default 1) mobile terminals (Default 1)				
	③ Tip: A registered mobile termina	I can access a wireless SSID without providing the user name and passwor	d.			
External Identity Center	Offline Timer					
Authentication Settings	Disabled					
Portal Settings	Daily Timer     Timer	5 minutes/minutes range/6_14400				
Glient Control	* Cause	u can use wlan service 5 minutes everyday				
	<ul> <li>Total Timer</li> <li>Single Timer</li> </ul>					
	<ul> <li>Tips:</li> <li>Daily Timer: When the daily time</li> </ul>	r ends, users will be forced offline on that day and recover online chance nex	t day.			
	2. Total Timer: The total timer start 3. Single Timer: When the single ti	s when enabled. When the total timer ends, accounts will be suspended or c mer ends, users will be forced offline or accounts will be suspended.	ancelled.			

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



Innovation Beyond Networks



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

0	Log Audit >	Network Acces	ss Logs > Query L	.ogs										
ι	Jser Name:			User IP:			Offline Cause	e: All		•				
L	.ogin Time:	2015-10-20	0 0 0	Logout Time:	2015-10-20	23:59:59	Query	Reset Advanced Se	arch					
	Delete	Exp	ort Query Results	Delete All							Network Traffic	and Online D	uration R	eport
Т	otally 1 Reco	ords   Each Pa	ge 20 Records	Page 1 / totally 1 Pa	ges   GO							N	0 0	
h	All Non	e Us	er Name 🔻	User IP	Full Name	NAS IP		Login Time 🔻	Logout Ti	me 🔻	Offline Cause 🔻	Ор	eration	
10			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!	2	/iew	
Т	otally 1 Reco	ords   Each Pa	ge 20 Records	Page 1 / totally 1 Pa	ges   GO							M	0 0	
0	L og Audit >	Operation Lo	ns > Query Lons											
	Log Addit	Operation Ed	go - Query Logo											
•	Operator:		Log Content	Re	cord Time: 2015-1	10-20 🛄 - 2015-10-20		Query Reset						
	Delete		lelete All											
	Totally 8 Rec	ords   Each Pa	age 20 Records	s   Page 1 / totally 1 Pa	iges   GO							K	< >	ÞI
	All Nor	<u>1e</u>	Operator 🔻	Record Ti	me 🔻				Log Conten	t				
			system	2015-10-20	10:44:00	The daily offline timer of	f 5 minutes fo	r User(2011, 10.1.1.105)	ends with user suspen	ision.				

#### **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.

Administrator (admin) Login IB (1	72 19 7 101 Logic Date (2015 10 10 10:10:42)		20 Online Liser C Pustern Status	Change Baseword	
Auministrator (aumini) Eugenne (	72.16.7.19 Login Date [2015-10-19 10.19.43]		Monnine Oser Saystern status	Change Password	(in Edgour
Autrentication & Autronty	<ul> <li>Authentication &amp; Authority &gt; User Group &gt; Query</li> </ul>	y User Groups			
Soline User User User Group	User Group Name:	Query Reset			
A Device	Add Delete				
Self-Registration	Totally 3 Records   Each Page 20 Records   P	age 1 / totally 1 Pages   60			
Mobile Terminal	AllINone	User Group Name 🔻	Operation		
		qrcode	View   Modify		
💃 External Identity Center		Guest User Group	View   Modify   Restore Default Settings	8	
		Default User Group	View Modify Restore Default Settings	5	
Portal Settings	Totally 3 Records   Each Page 20 Records   P	age 1 / totally 1 Pages   G0		N Q I	> >0
Client Control					

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



Authentication & Authority > User Group > Modify User Group

User Group Name: De Access Control Behavi	fault User Group or Restrict Access Ru	es	
Multi-Access Limit			
* An account can be used	on a maximum of 1 te ster1 mobile terminals	minals at the same time (Default. 1) (Default. 1)	
Tip: A registered mobile	e terminal can access a wi	reless SSID without providing the user name and password.	
Offline Timer			
Disabled			
Daily Timer			
Total Timer			
* Timer	1	hours(hours range:[1, 8760])	
* Response	🔘 Cancel 🖲 S	uspend	
* Cause	u can use 1 hou	r everyday	(E)
Single Timer			
<ol> <li>Tips:</li> <li>Daily Timer: When the idea of the second second</li></ol>	daily timer ends, users will mer starts when enabled. ' s single timer ends, users '	be forced offline on that day and recover online chance next day. Vhen the total timer ends, accounts will be suspended or cancelled. vill be forced offline or accounts will be suspended.	

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



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



O Log Audit > N	letwork Access Logs > Query I	Logs									
User Name: Login Time:	User Name:         User IP:         Offline Cause:         All           Login Time:         2015-10-20         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         <										
Delete	Delete Export Query Results Delete All Network Traffic and Online Duration Report										
Totally 4 Recor	ds   Each Page 20 Records	s   Page 1 / totally 1 Pag	ges  <del>G</del> O								
All None	User Name 🔻	User IP	Full Name	NAS IP	Login Time 🔻	Logout Time 🔻	Offline Cause 💙	Operation			
	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 > C	Iperation Logs ≻ Query Logs										
Operator:	Log Content:	Reco	rd Time: 2015-10-	20 🔚 - 2015-10-20 🔚	Query Reset						
Delete	Delete All										
Totally 13 Rec	Totally 13 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60										
All None	<u>Operator</u> 🕶	Record Tim	<u>ie</u> 🗸			Log Content					
	system	2015-10-20 11	1:38:00 Th	ie total offline timer of 1 hour fo	r User(2011, 10.1.1.118) ends with	user suspension.					
	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.

IP RG-SMP S	Security Management F	Platform   Professional	🖂 Feedback 💈 Online Se Technic	rvice 🗢 Technical Foru al Support Hotline: (+86)4	m 🚹 About				
Administrator [admin] Login IP [1]	72.18.7.19] Login Date [2015-10-19 10:19:43]		🖾 Online User 🐣 System Status	Change Password	O Logout				
Authentication & Authority 👻	Authentication & Authority > User Group > Query	User Groups							
Solution Contraction Contracti	User Group Name:	Query Reset							
Levice	Add Delete								
Self-Registration	Totally 3 Records   Each Page 20 Records   Pa	ige 1 / totally 1 Pages   60							
Mobile Terminal	AllNone	User Group Name	Operation						
		qrcode	View   Modify						
💃 External Identity Center		Guest User Group	View   Modify   Restore Default Setting	<u>s</u>					
		Default User Group	View Modify Restore Default Setting	<u>s</u>					
Portal Settings	Totally 3 Records   Each Page 20 Records   Pa	age 1 / totally 1 Pages   60			> >0				
Client Control									

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 > Liser Group > Modify Liser Group					
- Address of a Address of a	or or oup - mouny ober or oup				
User Group Name: Defa	ult User Group				
Access Control Behavior	Restrict Access Rules				
Multi-Access Limit					
* An account can be used o	n a maximum of 5 terminals	at the same time (Default: 1)			
An account can regist	er 1 mobile terminals (Defaul	t 1)			
I Tip: A registered mobile t	erminal can access a wireless S	SID without providing the user name and password.			
Offline Timer					
Disabled					
Daily Timer					
Total Timer					
Single Timer					
* Timer	5	minutes(minutes range:[5, 86400])			
* Response	Offline  Suspend				
* Holding Time	30	minutes(minutes range:[5, 1440])			
* Cause	every 30 minute can use	9 5 minute			
() Tips:					
1. Daily Timer: When the da	ily timer ends, users will be force	ed offline on that day and recover online chance next day.			
2. Total Timer: The total tim	er starts when enabled. When the	e total timer ends, accounts will be suspended or cancelled.			
3. Single Timer: When the s	single timer ends, users will be fo	preed offline or accounts will be suspended.			

3. 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 > Netw	ork Access Logs > Query Log	IS						
User Name:		User IP:		Offline	Cause: All	-		
Login Time: 20	15-10-20 🛄 0 :0 :0	Logout Time:	2015-10-20 🛅	23 :59 :59 Que	Reset Advanced Search	<u>h</u>		
Delete	Export Query Results	Delete All					Network Traffic and	Online Duration Report
Totally 5 Records	Each Page 20 Records   I	Page 1 / totally 1 Page	es   GO					N O P N
All None	User Name 🔻	User IP	Full Name	NAS IP	Login Time 🔻	Logout Time 🔻	Offline Cause 🔻	Operation
	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 > Oper	ation Logs > Query Logs							
Operator:	Log Content:	Reco	ord Time: 2015-10	-20 🛄 - 2015-10-20 🛄	Query Reset			
Delete All								
Totally 16 Records	Each Page 20 Records	Page 1 / totally 1 Pa	iges   <del>G</del> O					
All None	Operator 🔻	Record Time	•			Log Content		
	system	2015-10-20 13	:59:00 Th	e single offline timer of 5 mir	utes for User(2015, 10.1.1.105)en	ids with user suspension of 30mir	iutes.	

## 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.

V 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 groode	
* Bulletin Board Information:	
Guest scan QR code to register <u>QR logo customization</u>	
* User Group: Default User Group	
* QR wizard steps: Pleass scan your QR card to finish authentication!	
* QR authentication success message: Guest QR authentication success!	

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)

Innovation Beyond Networks



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

			R	ujie
	G-SMP	vice Pla	tform	
SWP 5	en-ser	vice ria	lionni	
U	serName:	qr	]	
Pa	assword:	•••	]	
Va	alidation Code:	7712 7	712	
		Login		Forgot Password

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

IP RG-SM	P Self-Service Platform	A STATE OF A
User Name[qr] Login Ti	ime[2015-10-19 13:54:53]	
My self-service	My self-service > QR card	
My Information Change Password	QR card	
Password Protection		QR brief introduction:
醫習 QR code card		QR is generation from your profile
		Guest scan the QR to pass access authentication
		guest who scan the QR will binding to your account
		@Print QR code
		E QR saved as
		📷 Regenerate QR
	Generation time:2015-10-19 13:54:55	Effective days (Default 7): 7 Effective scanning times (Default 30): 30
	① Tips: Regenerate QR, the previous QR fails automatically	

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.



Authentication & Authority > User Group > Query User Groups

er Group Name:	ary Reset		
Add Delete			
tally 4 Records   Each Page 20 Records   Page 1	/ totally 1 Pages L G0		
tany 4 records   Edon't age 20 records   1 age 1			
	User Group Name 🔻	Operation	
	User Group Name V new2	Operation View   Modify	
	User Group Name  rew2 new1	Operation <u>View   Modify</u> <u>View   Modify</u>	
	User Group Name new2 Guest User Group	Operation View   Modify View   Modify View   Modify   Restore Default Settings	

#### 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.

IP RG-SMP Se	P Security Management Platform Professional			🖸 Feedback 💈 Online Service 🗢 Technical Forum 🕧 Abo Technical Support Hotline: (+86)4008-111-0					
dministrator (admin) Login IP (172.1	8.7.19] Login Date [2015-11-12 14:23:41]	00	nline User 🔎 S	ystem Status	Change Password	() Logo			
uthentication & Authority 👻	Enable Guest Registration								
Online User User User Group Device	* Guest Validity Period: 1 Day(s) 0	<ul> <li>Minute(s) (Default: 1 day, range: 5 minutes to 365 days)</li> </ul>							
Blacklist Self-Registration Mobile Terminal MAC Terminal External Identity Center	* Bulletin Board Information:								
Authentication Settings Portal Settings	Guest scan QR code to register <u>QR logo customization</u>								
Bulletin Information Client Control	QR wizard steps: Pleass scan your QR card to finis QR authentication success message: Guest QR authe	L stoup h authentication! ntication success!							
	Enable Guest QR Code Registration								
	Enable Guest Validity Period by Scanner								
	Message for QR Code Scanning:	Please ask the reception personnel to scan the QR Code. h order to conduct authentica	tion for a						
ystem Maintenance 🔹	Message for Successful QR Code Authentication:	You have passed QR Code authentication. Vou can now access the network.							

- 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.



AP RG-SMP S	ecurity Management Platform Professional						
Administrator (admin) Login IP (17	2.18.7.19] Login Date [2015-11-10 11:20:52] 💥 Online User 🖉 System Status 🔒 Change Password 🕠 Logout						
Authentication & Authority	For common user authentication, configure the HTTP redirection page http://172.18.7.55.80/smp/commonauth , or HTTPS redirection page.https://172.18.7.55.443/smp/commonauth For guest user authentication, configure the HTTP redirection page.http://172.18.7.55.80/smp/guestauth , or HTTPS redirection page.https://172.18.7.55.443/smp/guestauth						
User	Web Authentication & Self-Service						
	HTTP Port         80         (Default 80)           HTTPS Port         443         (Default 443)						
Self-Registration	① Tip: You can access the Self-Service platform through http://172.18.7.55:80/smp/selfservice.						
Mobile Terminal	Enable Web Authentication						
External Identity Center	Enable Authentication-Exemption Rule for Web Users						
Authentication Settings	Guest Validity Period: 1 Day(s) 0      Hour(s) 0      Minute(s) (Default: 1 day, range: 5 minutes to 365 days)						
EE Portal Settings	guest user						
Client Control							
	* Bulletin Board Information:						
	User Group: [est Question: Carbon Coupting and						
System Maintenance	OR wizard steps: Please scan your QR card to finish 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.

P RG-SMP Security Management Platform Professional Education (Security Management Platform Review) 2 Technical Support Holline (+98,008-111-00)									About 08-111-000	
dministrator (admini) Login IP (172.18.7.19) Login Date (2015-10-19 10.19.43) 😥 Online User 🐣 System Status 🔒 Change Password 🖓 L								O Logout		
Authentication & Authority 👻	<ul> <li>Authentication</li> </ul>	& Authority > User > Query	Users							
Colline User User User Goup Self-Registration Mobile Terminal MAC Terminal	Contract Contend Contract Contract Contract Contract Contract Contract Contract									esults hance
😹 External Identity Center	Totally 3 Rect	ords   Each Page 20 Reco	rds   Page 1 / totally 1 F	Pages   GO					RODI	
Authentication Settings	All None	User Name 🔻	<u>Full Name</u> 🔻	User Group 🔻	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	Operation	
		2011	2011	Default User Group	Never Expire		0	Offline	View   Modify   Mobile Terr	ninal

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

IP RG-SMP S	Security Manage	ement Platform Professional	M Fee
Administrator (admin) Login IP (17	72.18.7.19] Login Date (2015-10-19 1	0:19:43]	🖾 Online User
Authentication & Authority 🔻	1. After Guest User Self-Service F	tegistration is enabled, users can obtain a temporary password via SMS to access the Internet.	
😂 Online User	2. Please configure the URL for G	IR Code authentication	
2 User	HTTP Address:http://172.18.34.	41:80/smp/grcodeservlet	
🐣 User Group	HTTPS Address:https://172.18.3	34.41:443/smp/grcodeservlet	
📥 Device	3. Please configure the URL for G	R Code card authenticationer Online Heartbeat Period	
器 Blacklist	HTTP Address:http://172.18.34.	41:80/smp/grcodecardservlet	
Self-Registration	HTTPS Address:https://172.18.3	34.41:443/smp/grcodecardservlet	
Mobile Terminal			
📇 MAC Terminal	Open Disclaimer Page		
	* Disclaimer title:	Disclaimer	
💃 External Identity Center		we provide free wlan service for you	
Authentication Settings			
En Portal Settings			
Dullatia lafamatian	* Disclaimer contents;		
Olicet Oceteci			
Chent Control			
		(Support upto 8000 characters input)	
	<ul> <li>Agree button title:</li> </ul>	Agree	
	① Tip:Authentication continues o	nly after the disclaimer is agreed	
	Heartbeat Detection on We	eb-authenticated Users	
System Maintenance		Modify Reset	
Log Audit			

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

 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.



D	Authentication & Authority > Authentication Settings	
---	------------------------------------------------------	--

Authentication Parameters					
* Authentication Port:	1812	(Default: 1812)	* Accounting Port:	1813	(Default: 1813)
Record Update Flow:					
Enable Nick Name Authentication:					
When account logins exceed the limit,	deal as follows: The new	client will not be able to authenticate.		$\sim$	
Preferred Wireless Authentication: PE	AP_EAP_GTC 🗸				
Click here to import the wireless auth	entication server certificate				
① Tip: The Authentication Port cannot b	e the same as the Accoun	ing Port.			
Periodic Online Status Detection					
Periodic Online Status Detection:	✓				
* User Online Heartbeat Period:	5	minutes (Default: 5)			
<ol> <li>Tips:</li> <li>When Periodic Online Status Detection</li> <li>When Periodic Online Status Detection</li> <li>When Periodic Online Status Detection</li> <li>and clear the user accordingly.</li> </ol>	n is enabled, please enab n is enabled and the syste	le non-Ruijie client accounting and set th m do not receive the User Online Heartb	e accounting period to the User Online Hea eat Notification within three consecutive Us	rtbeat Period. er Online Heartbeat Per	iods, the system will assume that this user has gone offline
Password Anti Brute Force Protectio	n				
Enable Password Anti Brute Force	Protection				
When the times of keying an incorrect	password exceeds 5	times, within 6 hours, the user	account will be frozen.		
✓ Enable PEAP Authentication for	Nindows Client				
* Auto-connect to SSID:					
WIFI Security Type:	WPA2 V				
WIFI Encryption Type:	AES V				
Second Stage of PEAP Authentication	PEAP_MSCHAP V				
Click here to download WIFI Helper.					
① Tip: Administrators can download and a state of the	d distribute the WIFI helpe	r to Windows users.			
Account Expiration Warning					
Account Expiration Warning:	<b>v</b>				
SMS Account Expiration Warning:					
Email Account Expiration Warning:					
* Sending Account Expiration Warning	days before. (Def	ault: 7; Range: 1 to 30)			
Every day, at 9 🗸 o'clock to 22	o'clock to send Email/	SMS account expiration warning			
Every 24 hours to send Email/S	MS account expiration war	ning (Default: 24, Range: 1 to 360)			
<ol> <li>Tips: Enabling SMS/Email Account E Warning will be re-sent.</li> </ol>	xpiration Warning allows th	ne system to hourly check the online statu	is within the configured period and sends t	ne warning messages i	if necessary. In every warning period, the Account Expiration

#### Modify Reset

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

Authentication & Authonity *	Authentication & Authority > Authenticati	on Settings				
Solution Continue User	Authentication Parameters					
User	* Authentication Port:	1812	(Default: 1812)	* Accounting Port:	1813	(Default: 1813)
Device	Record Update Flow:					
Blacklist	Enable Nick Name Authentication:					
Self-Registration	When account logins exceed the limit, o	teal as follows: When	the new client authenticates, the previou	s authenticated user will be forced to go offli	ne. 🖌	
Mobile Terminal	Preferred Wireless Authentication: PEA	P_MSCHAP				
📇 MAC Terminal	Click here to import the wireless auther	ntication server certifica	ite.			
🕵 External Identity Center	① Tip: The Authentication Port cannot be	the same as the Acco	unting Port.			
	Periodic Online Status Detection					
Authentication Settings	Periodic Online Status Detection:					
	User Online Heartbeat Period:	5	minutes (Default: 5)			
📢 Bulletin Information	① Tips:					
Olient Control	1. When Periodic Online Status Detection	is enabled, please en	able non-Ruijie client accounting and se	t the accounting period to the User Online He	eartbeat Period.	
	2. When Periodic Online Status Detection	is enabled and the sys	stem do not receive the User Online Hea	rtbeat Notification within three consecutive U	ser Online Heartbeat Pe	riods, the system will assume that this user has gone offline
	and clear the user accordingly.					

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.



Authentication & Authernalise	ority > Mobile Terminal	> Query Mobile Terminal						
User: MA	C Address:	Online Status						
Registration Date:	to	Query	Reset					
Add Import	Delete Delet	te All						
Totally 1 Records   Eac	h Page 20 Records	Page 1 / totally 1 Page	ages   GO				K	
All I None	<u>User</u> 🔻	MAC Address 🔻	Registration Date	Authentication Time	Authentication IP	Nas IP	Online Status 🔻	Operation
	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   Eac	h Page 20 Records	Page 1 / totally 1 Page	ages   GO				K	

- 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 8	& Authority > User > Que	ry Users							
Conline User User User User Device Concentration	User Name:	Full Name:	User Group:	User Type:	All Use Reset Advanced	r Status: All	for a long time			
Self-Registration Self-Registration Mobile Terminal	Registration     Add     Delete     Modify All     Delete All     Import Users     Import Users     Import Network Einding Information     Export All Results       e Terminal     Add to Blacklist     Issue Message or Patch     Suspend     Resume     Customize User Fields     SIM Card Management     Customize Query List     User Information Self-Service Maintenance									
💃 External Identity Center	Totally 6 Recor	rds   Each Page 20 Re	cords   Page 1 / totall	y 1 Pages   GO						
Authentication Settings	Alli None	<u>User Name</u> 🔻	<u>Full Name</u> 🔻	User Group 🔻	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	Operation	
		111	111	new2	Never Expire		0	Offline	View   Modify   Mobile Terminal	
Eulletin Information		1111	1111	Default User Group	Never Expire		0	Offline	View   Modify Mobile Terminal	
Oclient Control		222	222	new2	Never Expire		0	Offline	View   Modify Mobile Terminal	
		666	666	new2	Never Expire		0	Offline	View   Modify   Mobile Terminal	
		777	7777777	new2	Never Expire		0	Offline	View   Modify   Mobile Terminal	
		hkp	huangkaipen	new2	Never Expire		0	Offline	View   Modify Mobile Terminal	
	Totally 6 Recor	ds   Each Page 20 Re	cords   Page 1 / totall	y 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 & Aut	ority > Mobile Terminal	> Query Mobile Terminal						
User: MA Registration Date:	C Address:	Online Status	Reset					
Add	Delete Delet	te All						
Totally 1 Records   Eac	h Page 20 Records	Page 1 / totally 1 Page	ages   GO					
All   None	<u>User</u> ▼	MAC Address 🔽	Registration Date	Authentication Time	Authentication IP	Nas IP	<u>Online Status</u> ▼	Operation
	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   Eac	h Page 20 Records	Page 1 / totally 1 Pa	ages   GO					

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



•	Authentication & Authority > Mobile Terminal > Import
	Upload Import File
	Importing File (*.xls):
	Import
	Q Tips:
	1. The mobile terminals cannot exceed 10,000.
	2. Only EXCEL files based on template format can be imported. Click 🖄 here to download the Import Template.
	3. 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

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

Authentication & Authority	ority > Mobile Terminal	> Query Mobile Terminal						
User: MAC	C Address:	Online Status:	All V Reset					
Add Import	Delete Dele	te All	nesi GD				D	
		,	<b></b> 1 00					
<u>All   None</u>								Operation
$\checkmark$	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 Pag	ges GO				IQ	

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

Authentication & Authority 🍷	Authentication & Authority	y > Mobile Terminal >	Query Mobile Terminal						
Authentication & Authonty >   Mack Address:   Online User   Subser Group   Balacidist   Certification   Mobile Terminal   Mack Address:   Online Status:   Add   Import   Delete    Delete   Delete									
Self-Registration Mobile Terminal MAC Terminal	Add Import I Totally 1 Records   Each Pa	Delete Delete	e All	ages  GO					
External Identity Center	All I None	<u>User</u> ▼ 111	MAC Address  1234567141b6	Registration Date  2013-12-19 11:30:48	Authentication Time 2013-12-20 15:14:13	Authentication IP 172.18.8.197	Nas IP 172.18.8.85	<u>Online Status</u> ▼ Offline	Operation <u>View</u>
Authentication Settings	Totally 1 Records   Each Pa	age 20 Records	Page 1 / totally 1 Pa	ages   GO				M	A D DI
Bulletin Information     Client Control									

## 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.

Authentication & Authority 🕨	<ul> <li>System Maintenance &gt; Basic Configuration</li> </ul>								
System Maintenance	Server Parameter								
SMS Settings	* HTTP Port. 8080 (default 8	080)							
Email Service Settings	* VHTTPS Port: 8443 (default 8-	443)							
	* Required memory limit: 512 MB - 10	24 MB (Recommended 5	12 MB - 1024 MB)						
Custom Manager Page	③ Tips: The HTTP port and the HTTPS port can	not be the same.							
Database Maintenance WebService Service Access Port									
	* WebService Service Access Port:	9090	(default 9090)						
	① Tips: The WebService Service Access Port is	the port via which the third-	party access the current system.						
	Client Communication Configuration								
	* Server Communication Port:	53	(default 53)						
	* Client Communication Port:	138	(default 138)						
	* Client Communication Timeout is:	3	times (3 by default)						
	* Client Communication Retransmissions:	3	times (3 by default)						
	* Computer Protection Detection Period:	5	minutes (5 by default)						
	Enable the Client Management Center Server								
			Modify Reset						

# 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.

`	~	!	@	#	\$	%	^	&	*
(	)	(	)	[	]	{	}	_	١
_	-	=	+	,		&	,	+	,
;	:	"	"	د	,	<	>	%	
د	,	"	"		‰	`	o	]	^
«	>	ľ	]	!		#	\$		*
;	<	=	>	_		/	:	?	@
{		}	~	[	$\backslash$				