

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

**Operation Guide** 

#### **Copyright statement**

#### Ruijie Networks©2015

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



#### **Exemption statement**

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



#### Preface

Thank you for using our products. This manual will guide you through the operation of the system.

#### Scope

This manual is intended for:

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

#### **Obtaining Technical Assistance**

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

#### **Documentation Conventions**

The symbols used in this document are described as below:



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



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



# **Product Overview**

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

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

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

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

# Hardware Configuration

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

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



#### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

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

# **Product Interfaces**

### **RG-SMP Service Manager**

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



		RG-SMP Se	curity Management Pla	tform Professi	ional		- = X
SMP	Service Manager	Service Settings	DataBase Settings	Maintain	License	Option	۲
Start See	Stop Restart	Install Uninstall Service Operator					
(50) 15: 15: 15: (co 15: 15: 15: 15: 15: 15: 15: 15: 15: 15:	32:54,435 ERRO 32:54,435 ERRO 32:54,435 ERRO 32:54,575 ERRO 32:54,575 ERRO 33:26,056 INFO hours. 33:30,174 INFO 33:30,174 INFO 33:31,750 INFO 33:31,812 INFO 33:31,812 INFO 33:31,812 INFO 33:31,859 INFO 33:31,859 INFO 33:31,875 INFO 33:31,890 INFO 4 dat=20090522 38:51,488 INFO hress /172.18.7	adit(log(ump.log R [STDERR] log4j:) R [STDERR] log4j:) lerer*, appender*, () R [STDERR] log4j:) logging.strategy.] R [STDERR] log4j:) [STDOUT] The tr: [STDOUT] The tr: [STDOUT] The sy: 8.7.55). [Http11Protocol] [Http11Protocol] [Http11Protocol] [Http11Protocol] [Http11Protocol] [Http11Protocol] [Http11Protocol] [Http11Protocol] [ServerImp1] JB: 1053)] Started in [JIoEndpoint] M: 55 and port 8080	WARN Continuable pa WARN The content of category logger)*,; WARN No appenders of DefaultLoggerStrate WARN Please initial ial version is val: Monitoring Service stem (2015-11-09 18 Starting Coyote H Starting Coyote H	arsing error f element ty coot?, catego could be fou egy). lize the log id for 720 h e started (1 5:33:30) sta HTTP/1.1 on HTTP/1.1 on HTTP/1.1 on HTTP/1.1 on HTTP/1.1 on er) [5.1.0.GA hreads (10)	32 and c pe ~log4j rryFactory nd for lo (4j system ours and istening rted succ http-172. http-172. http-172. http-172. http-172. http-172. ttp-172. http-172. http-172.	olumn 23 :configuration" ?)". gger already in use fo port:53)! essfully. The IP 18.7.55-8080 18.7.55-80 18.7.55-443 18.7.55-9090 18.7.55-8043 SVNTag=JBoss_5_1_ or connector with	• • •
						Installation Path:C:\RG	-SMP\ .;;

#### **RG-SMP Management Platform**

After RG-SMP is successfully started, you can log in to the RG-SMP management platform. In the browser, enter <a href="http://smpip:8080/smp">http://smpip:8080/smp</a> (smpip is the IP address of the SQL server with RG-SMP installed, for example, <a href="http://htttp://http://http://http

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

The following figure shows the login page.



SIMP	RG-SMP Professional Security Management Platform	
ewp	security management Flatform	
	UserName:	
	Password:	
	Login	

By default, the username is **admin**, and the password is **111111111**. The following figure shows the page after the login succeeds.

IP RG-SMP	Security Managem	ent Platform   Pr	ofessional					🖂 Fee	dback 💈 Online Si Technic	ervice 🤤 Technical For al Support Hotline: (+86)	m 🚹 About
Administrator (admin) Login IP (1	72.18.7.19] Login Date [2015-11-09 17:34:	20]					20nlin	ie User	🐣 System Status	Change Password	O Logout
Authentication & Authority 👻	<ul> <li>System Status</li> </ul>										
Solution Online User	System Information										
Luser Group	Current System Status:	Abnormal (See details)									
A Device	License Status:	The trial version is valid for 720 ho	urs and already in u	se for 73 hours.							
Self-Registration	Online User:	1 Insecure Online Users:	0	Peak Online User	in 24hrs: 2						
Administrator (admin) Login IP (172:18.7.19] Login Date (2015-111-09 17:34.20)											
MAC Terminal	System Status       Change Passwort       O Logo         Online User       ● System Status       ● Change Passwort       ● Logo         Online User       ● System Status       ● Change Passwort       ● Logo         Online User       ● System Status       ● Change Passwort       ● Logo         Online User       ● System Status       ● Change Passwort       ● Logo         Online User       ● System Status       ● Change Passwort       ● Logo         © User Orage       ● System Status       ● Change Passwort       ● Logo         © User Orage       ● System Status       ● Change Passwort       ● Logo         © User Status:       The bial version is valid for 720 hours and already in use for 73 hours.       ●       ●         © Status:       The bial version is valid for 720 hours and already in use for 73 hours.       ●       ●       ●         © Status:       The bial version is valid for 720 hours and already in use for 73 hours.       ●       ●       ●         © Status:       I Insecure Online User:       I       Insecure Online User:       2       ●         © Oratis Status:       I Insecure Online User:       I       Insecure Online User:       1       Insecure Online User:       1         © Online User:       I       I Insecure Online										
💃 External Identity Center	Online User Trend in 24hrs										
Citent Control	2 5 5 1 0 1 10 19 20	21 22 23 0	i 2	3 4	5 6 Hour — Online User	ŻŚ	9 10	11	12 13	14 15 16	17



# **Typical Scenarios**

## **User Access**

Wired User Access

#### **Function Description**

N/A

#### **Configuration Tips**

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

#### **Configuration Steps**

# Adding a NAS

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

IP RG-SMP	Security M	anagement	Platform   Pr	✓ Fee ofessional	dback 💈 Online Se Technica	rvice 🤍 Technical Foru al Support Hotline: (+86)4	m 🚹 About .008-111-000
Administrator [admin] Login IP [1	172.18.7.19] Login Date	[2015-11-10 11:20:52]		🔀 Online User	System Status	Change Password	O Logout
Authentication & Authority 🔻	Authentication & A	uthority > Device > Query					A
Soline User	NAS IP:		NAS Configuration Templates	e: All	•		
Blacklint	NAS Name:		Query Reset				
Self-Registration	Add Delete	e Search Device	Import Device Synchr	onize MAC		NAS Configuration Ten	nplates
Mobile Terminal	Totally 1 Records	Each Page 20 Records	Page 1 / totally 1 Pages	;  G0		IQ Q (	> >0
💃 External Identity Center	<u>Alli None</u>	NAS IP	NAS MAC 🔻	NAS Configuration Templates		Operation	=
Authentication Settings		10.1.1.28	00d0f82233bd	<u>28</u>	Teine	et   <u>View</u>   <u>Modify</u>	
B Portal Settings	Totally 1 Records	Each Page 20 Records	Page 1 / totally 1 Pages	;  G0			> >0
Bulletin Information     Client Control	<ol> <li>Tips:</li> <li>You can set a tem</li> <li>If you cannot telne</li> </ol>	plate for the devices sharir at device, please click <mark></mark> <u>her</u>	ig the same SNMP version, a <u>e</u> to download the registry rep	uthentication and Telnet par- pair tool. Please restart your i	ameters. browser after repairin:	g.	
System Maintenance 🔻	Warning: If the device informa	tion is not registered in the	system, the user authenticat	on may fail.			

Innovation Beyond Networks



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.

IP RG-SMP S	Security Ma	nagement Pl	atform	Professio	Feedback 🗧	Online Servi Technical	rice 🙄 Technical Forun Support Hotline: (+86)40	n <u>A</u> About 108-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [20	15-11-10 11:20:52]			🖾 Online User 🚨 Syste	em Status	🔓 Change Password	O Logout
Authentication & Authority 🔻	Authentication & Auth	ority > Device > Add						
Second Contine User	Basic Information							
& User Group	* NAS IP:	172.18.7.80	(Format: 192.	168.20.1)				
Device	<ul> <li>NAS Configuration Templates:</li> </ul>	28	Obtain Device	Information View	v Template   Add Template			
🚰 Blacklist	NAS MAC:	001aa9c3f4c9	(Format: 00D0	F8000001)				
Self-Registration	NAS Name:	WS5302						
Mobile Terminal	NAS Location:							
MAC Terminal	NAS Information:	Ruijie Gigabit Wireless Sw (WS5302) By Ruijie Netwo	vitch rks.					
External Identity Center								
Authentication Settings	U Tips:							
Portal Settings	You can set a templat	te for the devices sharing the	same SNMP ve	rsion, authenticat	on and Telnet parameters.			
			Ac	ld Reset	Return			
Relief Information								
Client Control								
System Maintenance								
Log Audit								

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

🔏 RG-SMP Security Manageme	ent Platform - Windows Inte	rnet Explorer		
🕖 http:// <b>172.18.7.55</b> :8080/smp	o/nascfgtempservlet			
Authentication & Authority > E	Device > NAS Configuration Te	emplates > Add		
Basic Information				
* Template Name:	51	* Type:	Ruijie Wired Device 🔻	
Identity Authentication Cont	figuration			
* Identity Authentication Key:	ruijie			
① Tips:The system and device should be the same as that of	es perform user authenticatior the devices.	via the Radius Protocol. Identity authentica	tion key is used for the encryption of da	ata packets and
Web Authentication Configu	uration			
Web authentication Key:	ruijie			
① Tips:After the Web authentic	cation key is specified, the sys	tem will support Web authentication.		
SNMP Configuration				
* SNMP v2c Community:	ruijie	]		
I Tips: The SNMP configuration	on should be the same as that	on the devices. Otherwise the system can	not manage the devices.	
Security Management				
Device based NAC:	© Supported      O Supported	ted		
Tips: You can set a template for the	e devices sharing the same S	NMP version, authentication and Telnet par	ameters.	
		Add Reset Return		

Innovation Beyond Networks



#### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

IP RG-SMP	Security Ma	nagement	Platform   P	rofessional	eedback 💈 Online Se Technic	ervice 🙄 Technical Forur cal Support Hotline: (+86)4	m <u> A</u> bout 008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [20	15-11-10 11:20:52]		🖾 Online U	ser 🚨 System Status	Change Password	O Logout
Authentication & Authority 🔻	Authentication & Auth	ority > Device > Add					
Online User	Basic Information						
& User Group	* NAS IP:	172.18.7.51	(Format: 192.168.20.	1)			
Device	<ul> <li>NAS Configuration Templates:</li> </ul>	51	Obtain Device Inform	ation   View Template   Add	<u>i Template</u>		
Blacklist	NAS MAC:	14144b1b38cd	(Format: 00D0F8000	001)			
Self-Registration	NAS Name:	hujq51					
Mobile Terminal	NAS Location:						
MAC Terminal	NAS Information:	Ruijie Gigabit Security Access Switch (S26280	& Intelligence A G-I) By Ruijie +				
External Identity Center							
	🕡 Tips:						
Authentication Settings	You can set a templat	e for the devices sharing t	he same SNMP version, a	uthentication and Telnet p	arameters.		
Bulletin Information			Add	Reset Return	)		
🕜 Client Control							
System Maintenance 💌							

4) 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, choose **Authentication & Authority > Device** and click **NAS Configuration Templates** to add a NAS configuration template or modify the existing NAS configuration template.

# Adding a User Group

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



IP RG-SMP	Security Manage	ement Platform   Profession	Feedback 🖇 Online	Service 🖤 Technical Forum <u>À</u> About nical Support Hotline: (+86)4008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-10	11:20:52]	🖾 Online User 🚨 System Statu	s 🔓 Change Password 🕠 Logout
Authentication & Authority 🔻	Authentication & Authority > Us	er Group > Query User Groups		
😓 Online User				
🔒 User	User Group Name:	Query Reset		
🚨 User Group				
📥 Device	Add Delete			
Blacklist				
Self-Registration	Totally 6 Records   Each Page 2	0 Records   Page 1 / totally 1 Pages   G0		
Mobile Terminal	AU01-00-0	Lloor Crown Nome 💌		Orecelier
MAC Terminal	Allinone		1. Second	Operation
		smpad.com/13btest	<u>view</u> [	Modity
External Identity Center		smpad.com/普通 用户 组	View	Modify
2 Authentication Cattings		smpad.com/Users	View	Modify
PE Rotal Sattings		ad	View	Modify
		Guest User Group	View	Modify   Restore Default Settings
Sulletin Information		Default User Group	View	Modify   Restore Default Settings
Olient Control	Totally 6 Records   Each Page 2	0 Records   Page 1 / totally 1 Pages   60		
Svetom Maintonanco				
Log Audit				

2) Click Add or Modify to save the configuration.

IP RG-SMP S	ecurity Management Platform	☑ Feedback Sonline Service I Technical Forum About rofessional Technical Support Hotline: (+86)4008-111-000
Administrator [admin] Login IP [172	2.18.7.19] Login Date [2015-11-10 11:20:52]	🖄 Online User 🧟 System Status 🔒 Change Password 🛛 🗛 Logout
Authentication & Authority 🔻 🗌	Authentication & Authority > User Group > Add User Group	A
😓 Online User	• • • • • • • • • • • • • • • • • • •	
8 User	* User Group Name: test	
🚨 User Group	Access Central Babaier Bestirit Access Bules	
📥 Device	Access control Benavior Restrict Access Rules	
Blacklist	Enable Wired Access	C Enable Wireless Access
Self-Registration	Network Information Verification 🗐 All	Network Information Verification 🔲 All
Mobile Terminal	HD Serial Number Verification	HD Serial Number Verification
MAC Terminal	🔲 IP Type Authentication: 🔘 Static 🔘 Dynamic	IP Type Authentication:   Static  Dynamic
External Identity Center	User IP Verification	User IP Verification
	User MAC Verification	User MAC Verification
Authentication Settings	User IMSI	User IMSI
E Portal Settings	NAS IP Verification	
	NAS Port Verification	SSID Verification
Sulletin Information		v
Client Control	<ol> <li>Tips:</li> </ol>	
	1. Wireless SSID names are separated by commas (,), e.g., web-wired-	SSID, web-wireless-SSID.
	2. The MAC address verification and the IMSI number/mobile phone num	ber verification cannot be enabled at the same time.
System Maintenance 🔹	3. When the network information auto-learning and the network informati	on verification are enabled, you can bind users to networks. Or the system will
Log Audit 🕨 🕨	bind users to networks through network information auto-learning in the	next authentication.

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

# Adding or Importing a User

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



uthentication & Authority 👻		ate [2010-11-10 11.2)	0:52]				🖄 Online User	System Status	Change Password	O Logo
	<ul> <li>Authentication</li> </ul>	& Authority > User >	Query Users							
Online User	User Name:	Full Nan	ne: Use	r Group:	User Type: All	▼ Us	er Status: All 👻			
SUser Group Device	Online or not	All 🔻 In Blackl	ist or not: All	<ul> <li>Accurate Se</li> </ul>	archQuery	Reset Advanced	Search Query user:	s offline for a long	<u>time</u>	
Blacklist Self-Registration Mobile Terminal	Add C	Delete Modify	/ All Delete e or Patch Suspen	All d Resume	Customize User Field	is SIM Card Manage	Import Users Imp	ort Network Bindir ery List User Infor	ng Information Export All	<u>Results</u> Itenance
External Identity Center	Totally 5 Recor	rds   Each Page 20	Records   Page 1	/ totally 1 Pages	G0				14 A	
Authentication Settings	<u>All  None</u>	<u>User Name</u> 🔻	<u>Full Name</u> 🔻	User Group 🔻	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	Operation	
mental Settings		1108	1108	ad	Never Expire		0	Offline	View   Modify   Mobile T	Terminal
Bulletin Information		1108@smpad.com	1108@smpad.com	ad	Never Expire		0	Offline	View   Modify   Mobile T	Ferminal
Client Control		smpad.com\1108	smpad.com\1108	ad	Never Expire		0	Offline	View   Modify   Mobile T	Terminal
		smpad\1108	smpad\1108	ad	Never Expire		0	Offline	View   Modify   Mobile T	Terminal
		test	111	ad	Never Expire		0	Offline	View   Modify   Mobile T	Terminal

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

AP RG-SMP S	Security Mana	gement Pla	tform Professional		🖂 Feedback 💲 Online Se Technic	ervice 🖤 Technical Forun al Support Hotline: (+86)40	n 🔔 About 008-111-000
Administrator (admin) Login IP (17	2.18.7.19] Login Date [2015-11	-10 11:20:52]			🖾 Online User 🚨 System Status	🔓 Change Password	O Logout
Authentication & Authority 🔻	Authentication & Authority >	User > Add User					^
Se Online User	Basic Information						
User Out	* User Type:	Common User      Gue	est User O Thirdparty User	* User Status:	Normal      Suspended		
Contraction Contraction	* User Name:	testuser	7	* Full Name:	add		
Blacklist	Nick Name:						
Self-Registration	* Password:	•••	7	* Confirm Password:	•••		
Mobile Terminal	* Type of Account Validity	Never Expire      Delete	 e Account when Expire © Suspend				
📇 MAC Terminal	Period:	Account when Expire	7 -				
	* User Group:	test	Select User Group				
External Identity Center	Customize User Fields	Add Custom User Fields					=
Real Authentication Settings	No custom user field is fou	nd. Please click Add a Cus	tom User Field to add it.				
E Portal Settings	Detail Information						
Dullatin Information	Gender:	Not Selected	•	Email Address:			
Client Control	ID Type:	Not Selected	•	ID Number:			
	Educational Background:	Not Selected	•	Telephone Number:			
	Mobile Number:			Address:			
	Postal Code:						
	Network Binding List 🌳	Add Network Binding List					
	No network binding inform	ation of the user is found. P	lease click Add a Network Binding List	to add it.			
System Maintenance 💌	<ol> <li>Tips:</li> <li>You can add or import the</li> <li>When network information</li> </ol>	network binding information verification is enabled for th	n, which takes effect only when the use ne user group, the system learns netw	r group enables network in ork information in the first u	formation verification. ser authentication and regards it as n	etwork binding information	for

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



#### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

IP RG-SMP Security Management Platform Professional Echnical Support Hotline: (+85)4008-111-000									m 🚹 About 008-111-000	
Administrator [admin] Login IP [172.18.7.19] Login Date [2015-11-10 11:20:52] 😥 Online User 🔒 System Status 🔒 Change Password 🔍 Dogout										
Authentication & Authority 🔻	Authentication & Authonity 👻 💿 Authentication & Authonity> User> Query Users									
Contine User User User User Suser Group	Online User     User Name:     Full Name:     User Group:     User Type: All     User Status: All     Online or not     All     In Blacklistor not     All     Accurate Search     Query     Reset     Advanced     Reset     Advanced     Reset     Advanced     Reset     Advanced									
Backlist Backlist Self-Registration Mobile Terminal MAC Terminal	Covice     Covice								Results Itenance	
📕 External Identity Center	Totally 6 Reco	rds   Each Page 20	Records   Page 1	/ totally 1 Pages	G0					
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	
		1108	1108	ad	Never Expire		0	Offline	View   Modify   Mobile T	erminal
Bulletin Information		1108@smpad.com	1108@smpad.com	ad	Never Expire		0	Offline	View   Modify   Mobile T	erminal
Client Control		smpad.com\1108	smpad.com\1108	ad	Never Expire		0	Offline	View   Modify   Mobile T	erminal
		smpad\1108	smpad\1108	ad	Never Expire		0	Offline	View   Modify   Mobile T	erminal
		test	111	ad	Never Expire		0	Offline	View   Modify   Mobile T	erminal
		testuser	add	test	Never Expire		0	Offline	View   Modify   Mobile T	erminal
System Maintenance 🔹	Totally 6 Reco	rds   Each Page 20	Records   Page 1	/ totally 1 Pages	G0					

			0	0	-
ministrator (admin) Login IP (	172.18.7.19] Login Date [2015-11-10 11:20:52]	Online User	System Status	Change Password	C Logou
uthentication & Authority 🔻	Authentication & Authority > User > Import Users				
Online User	Upload Files				
User	Importing File (* xis/* csv):				刘贲
User Group	Overwrite Existing Lisers				
Device Disoklist	Delete users not contained in the imported file				
Self-Registration					
Mobile Terminal	Import Users Return				
🗄 MAC Terminal					
-	Q Tips:				
External Identity Center	1. The number of users cannot exceed 10,000.	-1-4-			
Authentication Settings	<ol> <li>Only EXCEL of CSV lifes based on template formatical be imported. Please click <u>shrele</u> to download an import emplate.</li> <li>If the required information is not included in the Import Template, users can create a new file based on the template.</li> </ol>	piate.			
Portal Settings					
Bulletin Information					
Client Control					
ystem Maintenance 🚬 💌					
System Maintenance					



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

Note

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

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



- d) Remote Radius Server
- e) WebService Server

# **Configuring the NAS**

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

# Authenticating a User

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

🕗 RG-SA	1.60 V1.60.20130403		х
RU	JIE		
		Self Service	
AuthMode	Wired MD5 Authentication	~	
User	smpad/1108	*	
Password	*****		
NIC	Intel(R) 82566MM Gigabit N	etwork C 💌	47
	🖌 Save Password 🗌 Automa	tic	
	Configure	Connect	

If authentication is successful, the following page is displayed.

Ø	×
Management Tips:	
Authentication success.	
	2015-11-10 13:46



🥝 RJ Security Agent 1	.60 V1.60.20130403		_ = ×
Bulletin Business D	Information Settings Suggestion Diagnostics		
		Online:	00:00:23
OS Version	Windows 7 Professional 32Bits(Version: 6.1.7600)	User:	smpad\1108
IP Mode	Static		
IP Address	172. 18. 7. 156		
Subnet Mask	255, 255, 255, 0		
Gateway	172. 18. 7. 1		
DNS Server	172. 18. 34. 46		
Alternative DNS Ser	rver		
NIC MAC	00-1D-72-88-36-2D		
OS MAC	00-1D-72-88-36-2D		
Harddisk SNO	K41MT7B25VM3		
IE Agent State	Disable		
			Reconnect
			Disconnect

3) Use Web authentication to login.

Go w Wel	ith Ruijie in your network ex come to Ruijie Networks	ploration.	User Lo 1108 Remember Me Login	ogin	

If authentication is successful, the following page is displayed.





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

Settings	WLAN				En	ter the	e pass	word f	for "or	nline-1	x"	
•				Cano	el	E	nter	Pass	swor	d		Join
iWuhan-Free		÷	()									
jiongjiong		ê ≑	()	Use	rname	e						
lh-1x		Ŷ	()	Pass	sword	I						
lj		Ŷ	()									
ljh-web		ŝ	()	Mod	le					Au	toma	tic >
new-mcp		Ŷ	()									
online-1x		₽ 奈	()									
online-mab		Ŷ	()									
test		₽ 🗢	()	<i>a</i> 1	w						ila	. n
text110		ê	()	Ч.					<u>'</u>			<u>с</u>
wacaca		ê	()	а	S	d	f	g	h	j	k	L
wechat		ج 🕯	1	ŵ	z	X	C	v	b	n	m	$\otimes$
wh-1x		ę	()	123	۲	₽		spa	ace		re	turn

Innovation Beyond Networks



Dusic information			
Jser Name:	1108	Full Name:	1108
Nick Name:			
Jser Type:	Thirdparty User		
Jser Group:	ad	Authen Method:	Wired Username and Password Authentication
_ogin Time:	2015-11-10 13:42:37	Last Login Time:	2015-11-10 13:42:37
Online Duration:	0:2:7		
Access Info			
ID Serial Number:		IMSI Number:	
Iser IP:		User MAC:	001D7288362D
IAS IP:	172.18.7.51	NAS Port:	12
SID:		Wireless AP MAC:	
Sateway IP:		Subnet Mask:	
referred DNS:		Standby DNS:	
LAN ID:	1	VLAN Name:	
Instream Traffic		Downstream Traffic	

#### Wireless User Access

#### **Function Description**

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

#### **Configuration Tips**

See section 2.1.1.2 "Configuration Tips".

#### **Configuration Steps**

# Adding a NAS

See section 2.1.1.3.1 "Adding a NAS".

# Adding a User Group

See section 2.1.1.3.2 "Adding a User Group"



## Adding or Importing a User

See section 2.1.1.3.3 "错误!未指定书签。Adding or Importing a User".

# **Configuring the NAS**

See section 2.1.1.3.4 "Configuring the NAS".

# Authenticating a User

See section 2.1.1.3.5 "Authenticating a User".

#### Webauth User Access

#### **Function Description**

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

#### **Configuration Tips**

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

#### Innovation Beyond Networks



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

#### **Configuration Steps**

# **Basic Web Authentication**

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

<b>IP RG-SMP</b>	Security Management	Platfo	rm	Professional			⊠ Fee	edback 울 Online Techr	Service 🙄 Technical Foru ical Support Hotline: (+86)4	m 🔒 About
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-10 11:20:52]						MOnline Use	r 🖲 System Status	Change Password	O Logout
Authentication & Authority 👻	Authentication & Authority > Portal Settings									*
Solution Continue User Continue User Continue User Group Continue User Group	Tips For common user authentication, configure the For guest user authentication, configure the H	e HTTP redire	tion page: n page:http	:http://172.18.7.55:80/s p://172.18.7.55:80/smp	mp/commonauth /guestauth , or Hi	h , or HTTP ITTPS redir	S redirection pa ection page:http	ige:https://172.18.7. ss://172.18.7.55:443	55:443/smp/commonauth /smp/guestauth	E
Blacklist	Web Authentication & Self-Service									
Self-Registration	* HTTP Port:	80 (Defa	lt 80)							
MAC Terminal	* HTTPS Port:	443 (Defa	lt 443)							
	() Tip: You can access the Self-Service platform	m through http:	/172.18.7.	55:80/smp/selfservice						
External Identity Center	Enable Web Authentication									
Authentication Settings	* Save user name and password for:	15		days (Default 15)						
Portal Settings	Download Web Authentication Client at:									
Bulletin Information     Client Control	<ul> <li>Automatically pop-up the URL you in</li> <li>Enable enter user name</li> </ul>	tent to access	oefore logi	in.						
System Maintenance	Bulletin Board Information:									*

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



#### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

<b>IP RG-SMP</b> S	ecurity Managemen	t Platform Professional	🗹 Feedback 💈 Online Ser Technica	vice 🙄 Technical Forum 🛕 Abou I Support Hotline: (+86)4008-111-00
Administrator [admin] Login IP [17	2.18.7.19] Login Date [2015-11-10 11:20:52]		🖾 Online User 🚨 System Status	Change Password OLogou
Authentication & Authority	For common user authentication, configure For guest user authentication, configure the	the HTTP redirection page:http://172.18.7.55:80/smp/commonauth , or HTTP HTTP redirection page:http://172.18.7.55:80/smp/guestauth , or HTTPS redir	S redirection page:https://172.18.7.55; ection page:https://172.18.7.55;443/sn	443/smp/commonauth np/guestauth
8 User	Web Authentication & Self-Service			
🚨 User Group	* HTTP Port	80 (Default 80)		
📥 Device	* HTTPS Port:	443 (Default: 443)		
Self-Registration	① Tip: You can access the Self-Service platf	rm through http://172.18.7.55:80/smp/selfservice.		
Mobile Terminal	Enable Web Authentication			
AC Terminal	* Save user name and password for:	15 days (Default: 15)		
External Identity Center	Download Web Authentication Client	at [		
Authentication Settings	Automatically pop-up the URL you	intent to access before login.		
E Portal Settings	Enable enter user name			
Client Control	Bulletin Board Information:			
System Maintenance	① Tip: After Web authentication is enabled, u	sers can be authenticated through the browser.		<u>-</u> _

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

Go with Ruijie in your network exploration. Welcome to Ruijie Networks.	User Login     108     Remember Me     Login

If authentication is successful, the following page is displayed.







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

IP RG-SMP S	Security Management	Platform Professional	Feedback 💈 Online Se Technica	rvice 🙄 Technical Forur al Support Hotline: (+86)40	n 🚹 About 108-111-000
Administrator (admin) Login IP [1]	2.18.7.19] Login Date [2015-11-10 11:20:52]		🖾 Online User 🚨 System Status	🔓 Change Password	<b>O</b> Logout
Authentication & Authority 👻	Authentication & Authority > Portal Settings				^
<ul> <li>Online User</li> <li>User</li> <li>User Group</li> <li>Device</li> </ul>	Tips For common user authentication, configure the For guest user authentication, configure the H	e HTTP redirection page http://172.18.7.55:80/smp/commonauth_or HTTP: ITTP redirection page.http://172.18.7.55:80/smp/guestauth_or HTTPS redir	S redirection page:https://172.18.7.55 ection page:https://172.18.7.55:443/sr	443/smp/commonauth np/guestauth	E
Blacklist	Web Authentication & Self-Service				
Self-Registration	* HTTP Port:	80 (Default: 80)			
MAC Terminal	* HTTPS Port:	443 (Default 443)			
	I Tip: You can access the Self-Service platform	n through http://172.18.7.55:80/smp/selfservice.			
External Identity Center	Enable Web Authentication				
Authentication Settings	* Save user name and password for:	15 days (Default: 15)			
E Portal Settings	Download Web Authentication Client at:	http://172.18.7.19/RJ_Security_Agent_1.60_For_Windows_V1.60.exe			
Client Control	<ul> <li>Automatically pop-up the URL you inlive</li> <li>Enable enter user name</li> </ul>	ent to access before login.		_	
System Maintenance  Cog Audit	Bulletin Board Information:				•

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





## **Guest Password Authentication**

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

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

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



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



#### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

IP RG-SMP S	Security Manage		M Fee		
Administrator [admin] Login IP [17	72.18.7.19] Login Date (2015-10-19	10:19:43]	Conline User		
Authentication & Authority 🔻	1. After Guest User Self-Service F	Registration is enabled, users can obtain a temporary password via SMS to access the Internet.			
🕹 Online User	2. Please configure the URL for (	QR Code authentication			
🚨 User	HTTP Address:http://172.18.34	.41:80/smp/grcodeservlet			
🚨 User Group	HTTPS Address:https://172.18.	34.41:443/smp/grcodeservlet			
📥 Device	3. Please configure the URL for (	QR Code card authenticationer Online Heartbeat Period			
Se Blacklist	HTTP Address:http://172.18.34	.41:80/smp/grcodecardservlet			
Self-Registration	HTTPS Address:https://172.18.	34.41:443/smp/grcodecardservlet			
Mobile Terminal					
📇 MAC Terminal	Open Disclaimer Page				
	<ul> <li>Disclaimer title:</li> </ul>	Disclaimer			
External Identity Center     Authentication Settings     Portal Settings     Control     Client Control	* Disclaimer contents:	(Support unto 8000 characters input)			
	* Agree button title:	Annee			
	Agree Sutter ute.	-300			
	Tip:Authentication continues only after the disclaimer is agreed				
	Heartbeat Detection on Web-authenticated Users				
System Maintenance 🔹		Modify Reset			

3) Configure the redirection URL for guests after authenticated on the NAS.

4) When a guest is used to access the network, a disclaimer page will be displayed. After the guest clicks Agree, the login page is displayed.



Innovation Beyond Networks





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



#### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide



# Note

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

# **Guest SMS Authentication**

The administrator should complete configuration as follows:

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



IP RG-SMP Se	ecurity Management Platform Professional	∑ Fee	dback 울 Online Se Technic	rvice 😳 Technical Forur al Support Hotline: (+86)40	n 🔔 About 108-111-000
Administrator [admin] Login IP [172.	18.7.19] Login Date [2015-11-10 11:20:52]	100 Online User	🖲 System Status	🔓 Change Password	C Logout
Authentication & Authority 💌	Enable Guest Registration				*
🕹 Online User	* Guest Validity Period: 1 Day(s) 0 ▼ Hour(s) 0 ▼ Minute(s) (Default: 1 day, range: 5 minutes	to 365 days)			
🚨 User	guest user				
😕 User Group					
📥 Device					
🚼 Blacklist					
Self-Registration					
Mobile Terminal	* Bulletin Board Information:				
📇 MAC Terminal					
External Identity Center					
Authentication Settings					
E Portal Settings					
	Guest scan QR code to register <u>QR logo customization</u>				
Generation Hereit Bulletin Information	User Group:				
🕜 Client Control	QR wizard steps: Pleass scan your QR card to finish authentication!				
	QR authentication success message: Guest QR authentication success!				
					=
	Enable Guest GR Code Registration				
	Enable Guest validity Period by Scanner				
	* Message for QR Code Scanning: Please ask the reception personnel to scan the C	ΩR Code. In α	order to con		
	* Message for Successful QR Code Authentication: You have passed QR Code authentication. 	er> You can now a	ccess the ne		
	Enable Guest SMS Self-Service Registration				
	* The maximum number of Self-Service Registration per mobile number within 24 hours (Default: 24, r	ange: 1 to 720) is	1 • times (Def:	ault: 1, range: 1 to 10)	
	Congratulations!				
System Maintenance					
Log Audit 🔸					-

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

Message f	from webpage	83
<u> </u>	Guest SMS Self-registration is enabled. Please also enable the SMS.	
	ОК	

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



& RG-SMP Security Manager	nent Platform - Windows Internet Explorer				
http://172.18.7.55:8080/sn	np/smsservlet?kind=toSettingPage&fromOtherPage=true&doAfterCloseWindow=window.opener.checkSmsServiceEnable()				
System Maintenance > SM	S Settings				
SMS Settings					
C Enable SMS Modem	Enable SMS Gateway     Enable 3G SMS Gateway				
* IP:	172.18.7.99				
* Port:	9191				
* User Name:	admin				
* Password:	•••••				
(1) Tips					
1. IP: IP address of the SMS	Web service interface.				
2. Port: the port name of the o	corresponding SMS Web Service interface.				
3. Username: username of th	ne corresponding SMS Web Service interface.				
4. Password: password of the corresponding SMS Webservice interface.					
	Modify Reset Close Send a Test Message				

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

Go with Ruijie in your network exploration. Welcome to Ruijie Networks.	▲   Cuest Access Mobile No. Mobile No. Cuest Ms Password Cuest Ms Password Remember Me Login Dovaloud Client
1	Bulletin Board: guest user

A user is authenticated by performing the following steps:

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





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

# **Guest QR Code Authentication**

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

	bout
	-000
Authinitisation (authin) cognin (F172):18.7.19) Cognin Date (2015-11-10 11:20:52) Authicitication & Authonitisation (configure the HTTP redirection page:http://172.18.7.55.80/smp/commonauth, or HTTPS redirection page:http://172.18.7.55.443/smp/commonauth For common user authentication, configure the HTTP redirection page:http://172.18.7.55.80/smp/commonauth, or HTTPS redirection page:http://172.18.7.55.443/smp/commonauth	fgout
B User         Web Authentication & Self-Service           B User Group         • HTTP Port         80         (Default 80)	
Blacklist	
Self-Registration       Image: Figure Self-Self-Registration         Mobile Terminal       Image: Figure Self-Self-Registration         MAC Terminal       Image: Figure Self-Self-Registration	Ш
Enable Automatication - xemption kulle for Vieo Users      Enable Guest Registration      Communication - xemption kulle for Vieo Users      Enable Guest Registration      Communication - xemption kulle for Vieo Users	
Image: Section 2     Image: Section 2	
Itelatin Information       Itelation       Itelation	
* Bulletin Board Information:	
Guest scan QR code to register <u>QR logo customization</u> User Group:       Test         Qselect User Group	
System Maintenance     OR wizard steps: Pleass scan your OR card to finish authentication!     OR authentication success message: Guest OR authentication success!	Ŧ

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



IP RG-SMP S	ecurity Management Platform Professional	Feedback 💈 Online S	ervice 🗢 Technical Foru cal Support Hotline: (+86)4	im <u> </u>
Administrator (admin) Login IP (17	2.18.7.19] Login Date [2015-11-10 11:20:52]	nline User 🐣 System Status	Change Password	O Logout
Authentication & Authonty    Authentication & Authonty     Contine User    User   User   Subset Group   Device  Subset Group  Subset Group  Mobile Terminal  MAC Terminal  External Identity Center	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 <sup>5</sup> minutes (Range: 3-80)           We Enable Self-Service Password Change           Tips:           1. The Initial Password Check and the Password Complexity Check can apply to the user name/password authenticat           2. When the password check functions apply to the certificate-based authentication, the password is the PIN code of U           3. When it is configured that users failing in password check are forced offline, users are allowed to change their pass	ion and certificate-based auth JSB key. swords using Ruijie authentic	entication. ation client (RG-SU) and	E
Authentication Settings     Bortal Settings     Gillent Information     Client Control	Guest User Management Rights  Guest User Management Rights  Allow user to scan QR to authentication  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)  Network Information Anti-Tampering			
System Maintenance	Authentication will fail if a user changes the MAC address of the network adapter     Tip: This function is available only for users of Ruijie authentication client (RG-SU) and Ruijie security agent (RG-SA     QoS Authorization Configuration     QoS Policy (in):     QoS Policy (out):     Flow Control	).		

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



Please ask the reception personnel to scan the QR Code. In order to conduct authentication for accessing network.





# **Guest QR Card Authentication**

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

☑ Enable Guest Registration	
* Guest Validity Period: 1 Day(s) 0 🔻 Hour(s) 0 🔻 Minute(s) (Default: 1 day, range: 5 minutes to 365 days)	
test grcode	
* Bulletin Board Information:	
Guest scan QR code to register <u>QR logo customization</u>	
* User Group: Default User Group 🔍 Select 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. Select the default user group, and click Modify in the Operation column. Click the Behavior Restrict tab in Modify User Group page, and check the Allow user to scan QR to authentication box under Guest User Management Rights.



Guest User Management Rights

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

		Ī	Ruíjie
SMP	RG-SMP Self-Ser	vice Platforn	n
elvip	2611-261	NICE LIGHOU	3
	UserName:	qr	
	Password:	•••	
	Validation Code:	7712 7712	
		Login	Forgot Password

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

IP RG-SM	P Self-Service Platform	
User Name[qr] Login Ti	me[2015-10-19 13:54:53]	
My self-service	My self-service > QR card	
My Information	QR card	
Password Protection		QR brief introduction:
R 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
	48366826	i∰rint QR code
		🔛 QR saved as
		Regenerate QR
		in information du
	Generation time:2015-10-19 13:54:55	Effective days (Default 7): 7
	550004201 Bille 2010 10 10 10.04.00	Effective scanning times (Default 30): 30
	① Tips: Regenerate QR, the previous QR fails automatically	

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



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



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

WLAN		Auto-Join	
<ul> <li>FZLab_ORCodeCard</li> </ul>	a 🕕		
122db_qrtoodcourd	• 🕑	Auto-Login	
		-	+

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

If authentication succeeds, the following page is displayed.

$\bigcirc$ Welcome to the QR co $~\times$	③ QR code card authentic × +	~
< > 公 四	☆   172.18.7.55/smp/qrcodecardservlet?wlanuserip= 🖯   ᢕ 🛛 🖄 × 搜索	$\downarrow$ $\equiv$
	Guest QR authentication success!	
	User IP:10.1.1.105 Expiration Date:2015-10-15 13:30	) () () ()

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





# **Smart Authentication**

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

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

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

ID BG-SMD	Security Management I	Datform Instantional	🖂 Feedback 💈 Online Se	rvice 🤝 Technical Forun	n 🚹 About	
	secondy management	Tadionni Protessional	Technica	al Support Hotline: (+86)40	J08-111-000	
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-16 17:49:51]		🖄 Online User 🚨 System Status	Change Password	O Logout	
Authentication & Authority 👻	Authentication & Authority > User Group > Query	User Groups				
Conline User	User Group Name:	Query Reset				
Levice	Add Delete					
Self-Registration	Totally 2 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60					
Mobile Terminal	AllNone	User Group Name 🔻	Operation			
		Guest User Group	View   Modify   Restore Default Settings	<u>8</u>		
💃 External Identity Center		Default User Group	View Modify Restore Default Settings	<u>8</u>		
Authentication Settings	Totally 2 Records   Each Page 20 Records   P	age 1 / totally 1 Pages   60		N 0 0	> (>0	
Sulletin Information						

Innovation Beyond Networks



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

<b>IP RG-SMP</b>	Security Management Platform   Professional
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-16 17:49:51]
Authentication & Authority 🔻	Authentication & Authority > User Group > Modify User Group
Online User     User     User     User Group     Device     Backlist     Self-Registration     Mobile Terminal     MAC Terminal     MAC Terminal      Mac Terminal	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.
Authentication Settings	Offline Timer   Disabled
Bulletin Information     Client Control	Daily Timer     Total Timer     Single Timer
	<ol> <li>Tips:</li> <li>Daily Timer: When the daily timer ends, users will be forced offline on that day and recover online chance next day.</li> <li>Total Timer: The total timer starts when enabled. When the total timer ends, accounts will be suspended or cancelled.</li> <li>Single Timer: When the single timer ends, users will be forced offline or accounts will be suspended.</li> </ol>

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



User Login	Success
test	User Name: test
••••	<ul> <li>Oser IP: 10.1.1.116</li> <li>Online Duration: 0:00:03</li> <li>Login Time: 2015-11-16 17:55:26</li> </ul>
Remember Me Forget password Login	Online Bulletin: Authentication success.     Go Offline     Pre-Login URL
	<ul> <li>Self-Service Change Password</li> <li>Tips: You have not completed the Password Protection Settings. Click here to complete settings</li> </ul>
(2) 172.18.7.55/smp/commonaut	(3) 172.18.7.55/smp/webauthsuce

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

<b>AP RG-SMP</b>	Security Man	agement	Platform   Pro	ofessional			Tecl	nical Support Hotline: (+8	3)4008-111-000
Administrator [admin] Login IP [1	172.18.7.19] Login Date (2015-	-11-16 17:49:51]				E.	Önline User 🚨 System Stat	is 🔒 Change Passwo	d OLogoul
Authentication & Authority 👻	Authentication & Authori	ty > Mobile Terminal >	Query Mobile Terminal						
Solution User	User: MAC	Address:	Online Status: All	-					
🛎 User Group	Registration Date:	🔲 to	Query Rese	et 💼					
Blacklist	Add Import	Delete Delete	All						
Mobile Terminal	Totally 1 Records   Each F	Page 20 Records   I	Page 1 / totally 1 Pages	60				10 0	D DI
	All I None	User 🔻	MAC Address 🔻	Registration Date 🔻	Authentication Time	Authentication IP	Nas IP	Online Status 👻 🛛 O	peration
External Identity Center		test	dcc7937a73a8	2015-11-16 17:55:27	2015-11-16 17:55:26	10.1.1.116	10.1.1.28	Online	View
Authentication Settings	Totally 1 Records   Each F	Page 20 Records   I	Page 1 / totally 1 Pages	60				Q QI	
Client Control									

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



Basic Information			
User Name:	test	Full Name:	mab
Nick Name:			
User Type:	Common User		
User Group:	Default User Group	Authen Method:	Wireless Username and Password Authentication
Login Time:	2015-11-16 18:13:27	Last Login Time:	2015-11-16 18:13:27
Online Duration:	0:0:6		
Access Info			
HD Serial Number:		IMSI Number:	
User IP:	10.1.1.116	User MAC:	DCC7937A73A8
NAS IP:	10.1.1.28	NAS Port:	6
SSID:	lh-1x	Wireless AP MAC:	14144B627F93
Gateway IP:		Subnet Mask:	
Preferred DNS:		Standby DNS:	
VLAN ID:	1	VLAN Name:	
Upstream Traffic:		Downstream Traffic	:
Terminal Info			
Authentication Client Type:	Standard 802.1x Client(Op	erating System:Windows r	nobile)



Note 1. Both wired and wireless Web authentication supports the Web-MAB authentication mode.

2. When **Multi-Access Limit** is enabled, if the maximum number of registered mobile terminals using one username is reached, other user terminal entering this username cannot be authenticated.

3. If the **A mobile terminal will be deregistered if it does not go online in consecutive X days** box is checked and configured, a mobile terminal will be deregistered if it does not get re-authenticated in specified days.

# **Authentication Exemption**

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


IP RG-SMP S	Security Managemen	t Platform Professional	🖂 Feedback 💈 Online S Technie	ervice 🔍 Technical Forur cal Support Hotline: (+86)40	m 🚹 About 008-111-000				
Administrator (admin) Login IP (17	72.18.7.19] Login Date [2015-11-10 11:20:52]		🖄 Online User 🚨 System Status	🔓 Change Password	🞧 Logout				
Authentication & Authority 🔻	<ul> <li>Authentication &amp; Authority &gt; Portal Settings</li> </ul>				^				
<ul> <li>➢ Online User</li> <li>➢ User</li> <li>➢ User Group</li> <li>▲ Device</li> </ul>	Tips     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/commonauth								
😽 Blacklist	Web Authentication & Self-Service				E				
Self-Registration	* HTTP Port	80 (Default: 80)							
Mobile Terminal	* HTTPS Port:	443 (Default 443)							
	Tip: You can access the Self-Service platform through http://172.18.7.55:80/smp/selfservice.								
External Identity Center	Enable Web Authentication								
Authentication Settings	Enable Authentication-Exemption Rule	e for Web Users							
Portal Settings	* Authentication-Exemption User Group:	smpad.com/13btest @ <u>Select User Group</u>							
Bulletin Information	* Bulletin Board Title:	Disclaimer							
Client Control	* Builetin Board Information:	this is test for free authentication							
	* Login Button Title:	Access							
System Maintenance	<ul> <li>Authentication Success Message:</li> </ul>	Authentication is successful. style="background-color: blue;">successful. br>You can now access the network.							
Log Audit	① Tips:				-				

2) Configure the redirection URL of authentication exemption.

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







### **Network Information Verification**

### **Function Description**

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

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

### **Configuration Tips**

N/A

### **Configuration Steps**

# **User Verification Rules**

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



Authentication & Authority > User Group > Query User Groups   User   User Group Name:   Query Reset     Add Delete     Totally 7 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60     MAC Terminal     Authentication Settings   Authentication Settings   Before aligned for	dministrator (admin) Login IP (	172.18.7.19] Login Date [2015-11-10 11:20	:52]	🖾 Online User 🚨 System Status	🔓 Change Password	O Logout
Online User   User Group Name:   Query Reset     Add Delete     Totally 7 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60     Totally 7 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60     MAC Terminal     Althouse     Authentication Settings     Portal Settings     Bibletin Information   Cuest Corup     Setternation     Bibletin Information   Cuest Corup     Setternation     Cuest Corup     View   Modify     Cuest Corup     View   Modify   Restore D	Authentication & Authority 👻	Authentication & Authority > User Gro	oup > Query User Groups			
Centrodus       Centrodus         Device       Elactist         Self-Registration       Modifie Terminal         MAC Terminal       Itelative Terminal         MAC Terminal       Itelative Terminal         MAC Terminal       Itelative Terminal         Authentication Settings       Itelative Terminal         MAC Terminal       Itelative Terminal         Machine       User Croup Name	Conline User	User Group Name:	Query Reset			
All Personal       Comparison       Description       Description         Mobile Terminal	Device Blacklist	Add Delete				
MAC Terminal     Attitions     User Group Name *     Operation       MAC Terminal     I     test     View Modify       External Identity Center     I     smpad.com/HB 用户 编     View Modify       Authentication Settings     I     smpad.com/Users     View Modify       Image: Portal Settings     Image: Portal Settings     Image: Portal Settings     View Modify       Image: Portal Settings     Image: Portal Settings     View Modify     View Modify       Image: Portal Settings     Image: Portal Settings     View Modify     View Modify       Image: Portal Settings     Image: Portal Settings     View Modify     View Modify       Image: Portal Settings     Image: Portal Settings     View Modify     View Modify       Image: Portal Settings     Image: Portal Settings     View Modify     View Modify       Image: Portal Settings     Image: Portal Settings     View Modify     View Modify       Image: Portal Settings     Image: Portal Settings     View Modify     View Modify       Image: Portal Settings     Image: Portal Settings     View Modify     View Modify	Self-Registration	Totally 7 Records   Each Page 20 F	Records   Page 1 / totally 1 Pages   G0			
Laternal identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Center identity Center         Image: Center identity Center         View I Modify           Image: Cent	DI Mobile Lerminal					
Leternal Identity Center         View   Modify           Image: Authentication Settings         Image: Smpad.com/13blest         View   Modify           Image: Authentication Settings         Image: Smpad.com/Users         View   Modify           Image: Portal Settings         Image: Smpad.com/User Group         View   Modify   Restore Default Settings           Image: Portal Settings         Image: Smpad.com/User Group         View   Modify   Restore Default Settings           Image: Portal Settings         Image: Smpad.com/User Group         View   Modify   Restore Default Settings	MAC Terminal	AllNone	User Group Name 💙		Operation	
Authentication Settings         Simpad.com/通用户组         View   Modify           IB Portal Settings         Image: Simpad.com/Users         View   Modify           IB Portal Settings         Image: Simpad.com/Users         View   Modify           Image: Simpad.com/Users         View   Modify         View   Modify	MAC Terminal	<u>All[None</u>	<u>User Group Name</u> ❤ test	<u>View Modify</u>	Operation	
Impendication Settings     View   Modify       Impendication Settings     Impendication	MAC Terminal	AllNone	<u>User Group Name</u> ❤ test smpad.com/13btest	<u>View</u> I Modify <u>View</u> I Modify	Operation	
Bit Portal Settings         ad         View   Modify <ul></ul>	MAC Terminal	AllNone	<u>User Group Name</u> ❤ test smpad.com/13btest smpad.com/普通 用户 组	View Modify View Modify View Modify	Operation	
Buildlin Information         Guest User Group         View   Modify   Restore Default Settings           Client Control         Default User Group         View   Modify   Restore Default Settings	MAC Terminal  External Identity Center  Authentication Settings	AllNone	User Group Name ➤ test smpad.com/13btest smpad.com/普通 用户 组 smpad.com/Users	View <mark>I Modify</mark> View I Modify View I Modify View I Modify	Operation	
Client Control Default User Group View   Modify   Restore Default Settings	MAC Terminal  Authentication Settings  Portal Settings		User Group Name マ test smpad.com/13btest smpad.com/普通 用户 组 smpad.com/Users ad	View Modify View Modify View Modify View Modify View Modify View Modify	Operation	
	MAC Terminal MAC Terminal Kenter I dentity Center Authentication Settings Portal Settings		User Group Name マ test smpad.com/13btest smpad.com/13btest smpad.com/Users ad d Guest User Group	View Modify View Modify View Modify View Modify View Modify View Modify Ex	Operation	

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

ID DC CMD	Sociurity Managament Diatform	🖂 Feedback 💈 Online Service 🦈 Technical Forum ႔ About
IF RG-SMP	Security Management Platform   Professional	Technical Support Hotline: (+86)4008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-10 11:20:52]	🖾 Online User 🥭 System Status 🔒 Change Password 🛛 🖓 Logout
Authentication & Authority 🔻	Authentication & Authority > User Group > Modify User Group	
<ul> <li>➢ Online User</li> <li>➢ User</li> <li>➢ User Group</li> <li>≟ Device</li> <li>☑ Blacklist</li> </ul>	User Group Name: test Access Control Behavior Restrict Access Rules C Enable Wired Access	Enable Wireless Access
Self-Registration	Network Information Verification 🗐 All	Network Information Verification 🔲 All
Mobile Terminal	HD Serial Number Verification	HD Serial Number Verification
	IP Type Authentication   Static  Dynamic	IP Type Authentication   Static  Dynamic
💃 External Identity Center	User IP Verification	User IP Verification
Authentication Settings	User MAC Verification	User MAC Verification
Portal Settings	User IMSI	test
	NAS IP Verification	SSID Verification
Client Control	NAS Port Verification	<b></b>
	<ul> <li>(b) Tips:</li> <li>1. Wireless SSID names are separated by commas (.), e.g., web-wireless SSID, web-wireless</li> <li>2. The MAC address verification and the IMSI number/mobile phone number verification or</li> <li>3. When the network information auto-learning and the network information verification are through network information auto-learning in the next authentication.</li> <li>4. When the network information verification is enabled, the client must upload network information verification are sensibled.</li> <li>5. Ruijle clients, such as RG-SA For Windows, will upload all network information while ot the sensitive of the sensition.</li> </ul>	ss-SSID. annot be enabled at the same time. enabled, you can bind users to networks. Or the system will bind users to networks formation and the uploaded network information must be consistent with that in the user ther clients do not upload hard disk serial number and IP address type.

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

# **User Verification**

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





# 

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

## **Offline Timer**

### **Function Description**

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

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

### **Configuration Tips**

N/A

### **Configuration Steps**

# **Daily Timer**

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

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



### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

IP RG-SMP	Security Management F	Platform Professional	🗹 Feedback 🏾 💈 Online Se Technica	rvice 🗢 Technical Foru al Support Hotline: (+86)4	m <u> A</u> bout 008-111-000				
Administrator (admin) Login IP (1	172.18.7.19] Login Date [2015-10-19 10:19:43]		🖾 Online User 🐣 System Status	🔓 Change Password	, Logout				
Authentication & Authority 🔻	Authentication & Authority > User Group > Query	User Groups							
Solution Contraction Contracti	User Group Name:	User Group Name Query Reset							
Device	Add Delete								
Self-Registration	Totally 3 Records   Each Page 20 Records   Pa	age 1 / totally 1 Pages   60		14 A					
Mobile Terminal	AllNone	User Group Name 🔻	Operation						
		grcode	View Modify						
💃 External Identity Center		Guest User Group	View   Modify   Restore Default Settings	1					
Authentication Settings		Default User Group	View Modify Restore Default Settings	1					
Portal Settings	Totally 3 Records   Each Page 20 Records   Pa	ige 1 / totally 1 Pages   60		R 0					
Generation Information									

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

IF RG-SMP Se	ecurity Manageme	nt Platform   Professional		Technic	al Support Hotline: (+86)40	008-111-000
Administrator [admin] Login IP [172.	18.7.19] Login Date [2015-10-19 10:19:43			🖾 Online User 🚨 System Status	🔓 Change Password	Q Logout
Authentication & Authority 🎽 🤇	Authentication & Authority > User Group	> Modify User Group				
Conline User Cuser User User Group Cuser Backlist Self-Registration Mobile Terminal MAC Terminal	User Group Name: Default User Access Control Behavior Restric Multi-Access Limit * An account can be used on a maxi An account can register	Croup  Access Rules  num of terminals at the same time (Default. 1)  oble terminals (Default. 1)  access advices SSIN without providing the sector name and reasonse				
Evternol Identity Center	TIP: A registered mobile terminal	an access a wireless SSID without providing the user name and password				
	Offline Timer					
Authentication Settings	Disabled					
E Portal Settings	Daily Timer					
Client Control	<ul> <li>Timer</li> <li>Cause</li> </ul>	5 minutes(minutes range:(5, 1440)) u can use wian service 5 minutes everyday				
	<ul> <li>Total Timer</li> <li>Single Timer</li> </ul>					
	<ol> <li>Tips;</li> <li>Daily Timer: When the daily timer</li> <li>Total Timer: The total timer starts</li> <li>Single Timer: When the single times</li> </ol>	ends, users will be forced offline on that day and recover online chance next when enabled. When the total timer ends, accounts will be suspended or ci er ends, users will be forced offline or accounts will be suspended.	day. incelled.			

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





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

Log Audit > N	Network Access Logs > Query Logs	i								
User Name:		User IP:	Offline	Cause: All	-					
Login Time:	2015-10-20 🗐 0 0 0	Logout Time: 2015-10-20	🔲 23 :59 :59 Que	ry Reset Advanced Search	<u>h</u>					
Delete	Export Query Results	Delete All				Network Traffic and	d Online Duration Report			
Totally 1 Reco	rds   Each Page 20 Records   Pa	age 1 / totally 1 Pages   G0								
All None	y <u>User Name</u> ▼	User IP Full Name	NAS IP	Login Time 🔻	Logout Time 🔻	Offline Cause 🔻	Operation			
	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 Reco	rds   Each Page 20 Records   Pa	age 1 / totally 1 Pages   G0								
Log Audit >	Operation Logs > Query Logs									
Operator:	Operator Log Content Record Time: 2015-10-20 - 2015-10-20 Reset									
Delete	Delete All									
Totally 8 Reco	ords   Each Page 20 Records   P	Page 1 / totally 1 Pages   G0								
All Non	e <u>Operator</u> 🔻	Record Time 💙			Log Content					
	system	2015-10-20 10:44:00	The daily offline timer of 5 min	Ites for User(2011, 10.1.1.105) end	Is with user suspension.					



# **Total Timer**

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

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

IP RG-SMP S	RG-SMP Security Management Platform Professional Centre Control Contro									
Administrator (admin) Login IP (1	72.18.7.19] Login Date [2015-10-19 10:19:43]		🖾 Online User 🚨 System Status	🔓 Change Password	<b>O</b> Logout					
Authentication & Authority 🔻	Authentication & Authority > User Group > Query	User Groups								
Solution Contraction Contracti	User Group Name:	User Group Name Query Rest								
🚵 Device	Add Delete									
Self-Registration	Totally 3 Records   Each Page 20 Records   Pa	ge 1 / totally 1 Pages   G0			> >0					
Mobile Terminal	All[None	User Group Name 🔻	Operation							
		grcode	View   Modify							
💃 External Identity Center		Guest User Group	View   Modify   Restore Default Settings	<u>s</u>						
		Default User Group	View Modify Restore Default Settings	<u>s</u>						
Portal Settings	Totally 3 Records   Each Page 20 Records   Pa	ge 1 / totally 1 Pages   60			> >					
Client Control										

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

Authentication & Authority > User Group > Modify User Group						
User Group Name: Default	User Group estrict 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)					
Itip: A registered mobile term	ninal can access a wireless SSID without providing the user name and password.					
Offline Timer						
Disabled						
Daily Timer						
<ul> <li>Total Timer</li> </ul>						
* Timer	1 hours (hours range:[1, 8760])					
* Response	Cancel  Suspend					
* Cause	u can use 1 hour everyday (田)					
Single Timer						
<ol> <li>Tips:</li> <li>Daily Timer: When the daily 1</li> <li>Total Timer: The total timer 3</li> <li>Single Timer: When the single</li> </ol>	timer ends, users will be forced offline on that day and recover online chance next day. starts when enabled. When the total timer ends, accounts will be suspended or cancelled. gle timer ends, users will be forced offline or accounts will be suspended.					

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





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

Log Audit > Netw	ork Access Logs > Query Lo	ogs						
User Name:		User IP:		Offline	Cause: All	<b>~</b>		
Login Time: 20	15-10-20 🔲 0 0 0	Logout Time:	2015-10-20 🛅	23 59 59 Que	Reset Advanced Searc	<u>ch</u>		
Delete	Export Query Results	Delete All					Network Traffic and	d Online Duration Re
Fotally 4 Records	Each Page 20 Records	Page 1 / totally 1 Pag	es GO					
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 > Opera	ation Logs > Query Logs							
Operator:	Log Content:	Recor	d Time: 2015-10-	-20 🗐 - 2015-10-20 🗐	Query Reset			
Delete	Delete All							
Fotally 13 Records	Each Page 20 Records	Page 1 / totally 1 Pag	ies   GO					
All None	Operator 🔻	Record Time	×			Log Content		
	system	2015-10-20 11	38:00 TI	he total offline timer of 1 hour fo	r User(2011, 10.1.1.118) ends with	user suspension.		
		0045 40 00 44						

# **Single Timer**

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



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

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

IP RG-SMP S	RG-SMP Security Management Platform   Professional Technical Support Holine (+894008-111-00)									
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 👻	Authentication & Authority > User Group > Query	User Groups								
Solution Continue User User Solution Content C	User Group Name:	Query Reset								
🚵 Device	Add Delete									
Self-Registration	Totally 3 Records   Each Page 20 Records   Page 20	age 1 / totally 1 Pages   60			P (20					
Mobile Terminal	AllINone	User Group Name 🄝	Operation							
		grcode	View Modify							
💃 External Identity Center		Guest User Group	View Modify Restore Default Setting	1						
		Default User Group	View Modify Restore Default Settings	1						
Portal Settings	Totally 3 Records   Each Page 20 Records   Page	age 1 / totally 1 Pages   60		14 4 6	> 04					
Glient Control										

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

Authentication & Authority > Us	er Group > Modify User Group	
-		
User Group Name: Defa	ault User Group	
Access Control Behavio	r Restrict Access Rules	
Multi-Access Limit		
* An account can be used o	n a maximum of 5 terminals a	at the same time (Default: 1)
🔲 An account can regist	er 1 mobile terminals (Default	t 1)
I Tip: A registered mobile	terminal can access a wireless S	SID without providing the user name and password.
Offline Timer		
O Disabled		
Daily Timer		
Total Timer		
Single Timer		
* Timer	5	minutes (minutes range: [5, 86400])
* Response	Offline I Suspend	
* Holding Time	30	minutes (minutes range: [5, 1440])
* Cause	every 30 minute can use	2 5 minute A 田田 名字
() Tips:		
1. Daily Timer: When the da	aily timer ends, users will be force	d 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	single timer ends, users will be fo	rced offline or accounts will be suspended.

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



#### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide



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

Log Audit > Network A	Access Logs > Query Logs								
User Name:	User Name: User IP: Offine Cause: All								
Login Time: 2015-1	10-20 🔲 0 ‡0 ‡0	Logout Time: 2	015-10-20 🔲 2	23 : 59 : 59 Quer	Reset Advanced Search	1			
Delete	Export Query Results	Delete All					Network Traffic and	Online Duration Report	
Totally 5 Records   Each	ch Page 20 Records   P	age 1 / totally 1 Pages	60						
All None	User Name 🔻	User IP	Full Name	NAS IP	Login Time 🔻	Logout Time 🔻	<u>Offline Cause</u> ▼	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 > Operation	n Logs > Query Logs								
Operator:	Operator Log Content Record Time: 2015-10-20 2015-10-20 2015-10-20 2015-10-20 2015-10-20 2015-10-20 2015-10-20								
Delete Delete All									
Totally 16 Records   Ea	ach Page 20 Records	Page 1 / totally 1 Page	es G0						
All None	<u>Operator</u> 💙	Record Time	~			Log Content			
	system	2015-10-20 13:59	9:00 Th	e single offline timer of 5 min	Ites for User(2015, 10.1.1.105)en	ds with user suspension of 30min	utes.		

Innovation Beyond Networks



# **External Identity Center**

### Authentication Using Generic LDAP Server

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

AP RG-SMP S	ecurity Managemer	nt Platform   Profe	ssional	⊠ Feed	lback 💲 Online Servi Technica	ice 🗢 Technical Forun al Support Hotline: (+86)4	1 🔔 About 008-111-000
Administrator [admin] Login IP [172	2.18.7.19] Login Date [2015-11-12 14:23:41]			🔀 Online User	🚨 System Status	Change Password	
Authentication & Authority 👻	<ul> <li>Authentication &amp; Authority &gt; External Ident</li> </ul>	tity Center					*
😂 Online User	External Identity Center						
a User	EnableExternal Identity Center						
Loser Group	Generic LDAP	Windows AD Domain	External Database	Remote Radius Server	Webservice	9	
Blacklist	LDAP Server IP:	172.18.34.50					
Self-Registration	IDAP Server Port:	389	(Default: 389)				=
Mobile Terminal	* Root DN:	dc=maxcrc.dc=com	Auto-Obtain				
📇 MAC Terminal	Root DN is the root node of an LDAP d	irectory tree. For example, dc=my-dom	ain and dc=com.				
External Identity Center	Support Anonymous						
	If the administrator password of the LD/	AP server is NULL, please select Anony	/mous Login.				
Authentication Settings	* Administrator User Name:	cn=Manager,dc=maxcrc,de	 P				
E Portal Settings	For example, the administrator user na	me for OpenLDAP is the rootdn of the s		, dc=my-domain, and dc=com)			
Bulletin Information	* Administrator Password:	•••••					
Olient Control	For example, the administrator passwo	rd for OpenLDAP is the rootpw of the sl	apd.conf file. (For example, secret)				
	* Identity Authentication Mode:	Implement Identity Auther	ntication by querying LDAP users 🔘 Imp	lement Identity Authentication by logging in to the	LDAP server		
	* User ObjectClass:	person					
	* User Name Attribute Name:	cn					
	The system queries users based on	attributes of User ObjectClass and Use	r Name Attribute Name.				
System Maintenance 🔹	* User Password Attribute Name:	cn					-

IP RG-SMP Se	IP Security Management Platform Professional					☑ Feedback 💈 Online Service 📼 Technical Forum 🔔 Technical Support Hotline: (+86)4008-11		
Administrator [admin] Login IP [172.1	8.7.19] Login Date [2015-11-12 14:23:41]				⊠Online User 🚨 System Status	🔓 Change Password		
Authentication & Authority 👻	The system queries users based on attr	ibutes of User ObjectClass and I	Jser Name Attribute Name.					
Se Online User	* User Password Attribute Name:	cn						
Sulser	Enable an Encryption and Decryption Plug	-in:						
Buser Group								
A Device								
Se Blacklist	Learn new users during authentication							
Self-Registration	Learn the user group during new use	r authentication						
Mobile Terminal	<ul> <li>User Group Containing Auto Added Use</li> </ul>	rs: new	Select User Group					
📇 MAC Terminal	If you don't configure the user group attri	bute name, all users newly learn	ed will be added to this user group.					
External Identity Center	Existing users update the user group a	utomatically						
	User Group Attribute Name:							
Authentication Settings	If you configure User Group Attribute Name	e, the system will learn the user	group from the LDAP server and add newly lea	rned users to this group.				
EB Portal Settings	User Name Attribute Name:	cn	Address Attribute Name:	street				
-4	Telenhone No. Attribute Name:	telenhoneNumber	Mobile No. Attribute Name:	telephoneNumber				
Bulletin Information				compromotion damped				
Client Control	Post Code Attribute Name:	postalCode	Email Address Attribute Name:					
	Test User Name:	test					-	
	Test Deserved		Laterative Audiona					
	rest massword.	••••	Identity Autrien					
	You can verify whether a user passes LDA	P server authentication by enteri	ng a test user name and test password and cl	icking Identity Authentication.				
System Maintenance 🔹			Modify Reset	Refresh			-	

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

### **Correlation with Windows AD Domain**

### **Configuration Tips**

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



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

### **Configuration Steps**

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

×				
http:// <b>172.18.7.55</b> :8080/smp/a	dserverservlet			
* 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	domain server is	389.		
Dedicated AD Domain Acc	ount			
* Login User Name:	administra	ator		
* Login Password:	•••••	••••	Test Connection	
PEAP-MSCHAPv2 for 80	2.1X PCs			
* PC Name:	SMPAD-S	ERVER		
1. The AD domain user name is read-only permissions for all dir 2. If the AD domain user passw 3. To change the PC name, add	s configured exc rectories of the A rord is not entered the SMP source	lusively for SMP or AD domain tree. ed, the original pas	he AD domain server to correlate with the AD domain. This account should har word will remain unchanged.	ve at least
The AD domain user name is read-only permissions for all dir If the AD domain user passw To change the PC name, add To enable PEAP-MSCHAPv2 Other Info	s configured exc rectories of the A rord is not entered d the SMP serve 2, PCs must be	lusively for SMP or AD domain tree. ed, the original pas er to the correspond registered with pas	the AD domain server to correlate with the AD domain. This account should har word will remain unchanged. ng AD domain, and login it by the administrator. words the same as AD login password.	ve at least
The AD domain user name is read-only permissions for all dir If the AD domain user passw To change the PC name, add To enable PEAP-MSCHAPv2 Other Info User Group Info Synchronizat	s configured exc rectories of the A rord is not enterd d the SMP serve 2, PCs must be	lusively for SMP or AD domain tree. ed, the original pas er to the correspond registered with pas	he AD domain server to correlate with the AD domain. This account should have word will remain unchanged. Ing AD domain, and login it by the administrator. words the same as AD login password.	ve at least
The AD domain user name is read-only permissions for all dir     If the AD domain user passw     To change the PC name, add     To enable PEAP-MSCHAPv2     Other Info     User Group Info Synchronizat     Synchronized User Group Info	s configured exc rectories of the A rord is not enterr d the SMP serve 2, PCs must be ion Settings:	lusively for SMP or AD domain tree. ad, the original pass or to the correspond registered with pass User Group : Users Domain Users 13btest 13butest SMP-GROUP	he AD domain server to correlate with the AD domain. This account should har word will remain unchanged. ng AD domain, and login it by the administrator. words the same as AD login password.	ve at least
The AD domain user name is read-only permissions for all dir     If the AD domain user passw     To change the PC name, add     To enable PEAP-MSCHAPV2     Other Info     User Group Info Synchronizat     Synchronized User Group Info	s configured exc rectories of the A rord is not enterr d the SMP serve 2, PCs must be tion Settings:	lusively for SMP or AD domain tree. ed, the original pass ar to the correspond registered with pass User Group : Users Domain Users 13btest 13butest SMP-GROUP Default User Grou	he AD domain server to correlate with the AD domain. This account should har word will remain unchanged. ng AD domain, and login it by the administrator. words the same as AD login password. mohronization a Select User Group	ve at least
The AD domain user name is read-only permissions for all dir     If the AD domain user passw     To change the PC name, add     To enable PEAP-MSCHAPV2     Other Info     User Group Info Synchronizat     Synchronized User Group Info     User Group Containing Auto 2     Tips:	s configured exc rectories of the A rord is not enterd d the SMP serve 2, PCs must be tion Settings: tion Settings:	lusively for SMP or AD domain tree. ed, the original pass er to the correspond registered with pass User Group : Users Domain Users 13btest 13btest 13btest SMP-GROUP	the AD domain server to correlate with the AD domain. This account should have word will remain unchanged. Ing AD domain, and login it by the administrator. Ing AD domain, and login password. Inchronization Inchroniz	ve at least

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



👙 RG-SMP Security Management I	Platform - Window	Internet Explorer		
http://172.18.7.55:8080/smp/ad	lserverservlet			
Authentication & Authority > Example 2	xternal Identity Cer	ter > AD Domain Server > Add		
Pasic Info				
t AD Demois Nerre	a second second			
* 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 3	9.		
Dedicated AD Domain Accou	Int			
* Login User Name:	administrator			
* Login Password:	•••••			
PEAP-MSCHAPv2 for 802	1X PCs			
(1) Tino:		Ihe preferred domain server is connected.		
1. The AD domain user name is	s configured e	domain. This account should har	ve at lea	ast
read-only permissions for all di	rectories of the	ОК		
2. If the AD domain user passw	ord is not ente			
3. To change the PC name, add	i the SMP server .	ano con opponanty i 2 aomain, ana logini k of aro aominica al 01.		
4. To enable PEAP-MSCHAPv2,	PCs must be regi	tered with passwords the same as AD login password.		
Other Infe				
User Group Info Synchronizati	ion Settings:	ser Group Synchronization		
User Group into Gynchronizau	ion oettings.			
Synchronized User Group Info	D:			
* Llaar Oraun Containir - Auto J	ddad Llaara;			
Oser Group Containing Auto A	Added Osers.	w select User Group	0.1	

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



🔗 RG-SMP Security Management	Platform - Windows Internet Exp	lorer	- • •
http://172.18.7.55:8080/smp/ac	dserverservlet		
Authentication & Authority > E	xternal Identity Center > AD Doi	nain Server > Add	
Basic Info			
* AD Domain Name	smpad.com		
* Preferred Domain Server IP:	172.18.34.46		
Standby Domain Server IP:			
* Domain Server Port:	389		
Tip: The default port for AD of Dedicated AD Domain Account to a single provide the second seco	tomain server is 389.		
* Login User Name:	administrator		
PEAP-MSCHAPv2 for 802 * PC Name:	1X PCs SMPAD-SERVER		
<ol> <li>Tips:</li> <li>The AD domain user name is read-only permissions for all di</li> <li>If the AD domain user passw</li> <li>To change the PC name, add</li> <li>To enable PEAP-MSCHAPv2,</li> </ol>	s configured exclusively for SMF rectories of the AD domain tree rord is not entered, the original d the SMP server to the corresp .PCs must be registered with p	on the AD domain server to correlate with the AD domain. This account should h password will remain unchanged. onding AD domain, and login it by the administrator. vasswords the same as AD login password.	iave at least

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

SG-SMP Security Management Platform - Windows Internet	t Explorer				
http://172.18.7.55:8080/smp/adserverservlet?kind=toSyncAdUserGroupPage&isModifyPage=undefined&toSyncAdUserGroup=true					
Authentication & Authority > External Identity Center > AD	Domain Server > Add > User Group Synchronization				
Autorimication & Automy & External identity Center & AD       Please select the AD user group information item to be s       Domain Admins       Domain Admins       Domain Guests       Group Policy Create       RAS and IAS Servers       Server Operators       Account Operators       Pre-Windows 2000 Cc       Incoming Forest Ir.       Windows Authorizati       Terninal Server Lic       DnsUpdateProxy       lead-group       z-test	synchronized.				
	Modify Close				



<i> </i> RG-SMP Security Managemen	t Platform - Wind	lows Internet Explor	er						×
http://172.18.7.55:8080/smp/a	adserverservlet								٦
Freieneu Domain Geiverni.	172.10.34.40								
Standby Domain Server IP:									
* Domain Server Port:	389								
Itip: The default port for AD	domain server i	s 389.							
Dedicated AD Domain Acco	ount								1
* Login User Name:	administr	ator							
* Login Password:	•••••		Test Connec	tion					
PEAP-MSCHAPv2 for 80	2.1X PCs								
* PC Name:	SMPAD-S	ERVER							
2. If the AD domain user pass 3. To change the PC name, ac 4. To enable PEAP-MSCHAPV Other Info	word is not enter Id the SMP serve 2, PCs must be r	ed, the original pas In to the correspond registered with pase	sword will rem ing AD domair swords the sar	nain unchang n, and login it me as AD log	ged. : by the adr gin passwo	ninistrator. ord.			III
User Group Info Synchroniza	ation Settings:	User Group Sy	nchronizati	on					
Synchronized User Group In	ıfo:	Users Domain Users 13butest 13btest SMP-GROUP							
<ul> <li>* User Group Containing Auto</li> <li>① Tips:</li> <li>1. The user not grouped or ad</li> </ul>	) Added Users: Ided to several g	Default User Grou	ip 🔍 S	elect User G	iroup Jefault.				
								•	Ŧ
Done				😜 In	ternet   Pro	tected Mode: On	🕼 👻 🔍 100	% +	

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



RG-SMP Security Managen	ent Platform - Windows Internet Explorer	
http:// <b>172.18.7.55</b> :8080/sm	o/adserverservlet	
PEAP-MSCHAPV2101	302.1X PUS	
* PC Name:	SMPAD-SERVER	
D Tips:		
I. The AD domain user na	e is configured exclusively for SMP on the AD domain server to correlate with the AD don	nain. This account should have at least
ead-only permissions for	Il directories of the AD domain tree.	
2. If the AD domain user pa	ssword is not entered, the original password will remain unchanged.	
3. To change the PC name	add the SMP server to the corresponding AD domain, and login it by the administrator.	
4. To enable PEAP-MSCH/	Pv2, PCs must be registered with passwords the same as AD login password.	
Other Info		
Lloor Croup Info Supphro	ization Cottingo: Heer Group Synchronization	
Oser Group Into Synchro	Message from webpage	
	A Identity Authentication Succeeded	
	Test User:1108	
Synchronized User Grou	Info: Domain Server:172.18.34.46	
	ОК	
User Group Containing A	Ito Added Users: Default User Group Select User Group	
Tips:		
1. The user not grouped or	added to several groups is added to the specified user group by default.	
Identity Center Correlat	n Test	
Test User Name:	1108	
Test Password:	Identity Authen	
D. Tim Version and the both		
<ul> <li>Trp. You can verify whet Authentication</li> </ul>	er a user passes ALD domain server authentication by entering a test user name and tes	password and clicking identity
	Add Depart Deturn	
	Add Reset Return	
	Teters at Destanted Made	On

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

The default settings are recommended.



IP RG-SMP	Security Management Platform   Professional
Administrator [admin] Login IP [1	172.18.7.19] Login Date [2015-11-16 17:49:51]
Authentication & Authority 👻	Authentication & Authority > External Identity Center
<ul> <li>Online User</li> <li>User</li> <li>User Group</li> </ul>	External Identity Center
Device	Generic LDAP     Windows AD Domain     External Database
<ul> <li>Blacklist</li> <li>Self-Registration</li> <li>Mobile Terminal</li> <li>MAC Terminal</li> <li>MAC Terminal</li> <li>External Identity Center</li> <li>Authentication Settings</li> <li>Portal Settings</li> <li>Portal Settings</li> <li>Client Control</li> </ul>	Please click " Windows AD Domain Server," to view and configure the Windows AD Domain Server for login.  * Synchronization Interval for AD Domain User Info; 7  U Learn new users during authentication U Learn the user group during new user authentication Existing users update the user group automatically  AD Domain User Attribute Beeper No. Chyl/County County Contry County Count

### **Correlation with External Database**

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



External Identity Center					
Enable External Identity Center			1		
O Generic LDAP	O Windows AD Domain	<ul> <li>External Database</li> </ul>	O Remote Radius Server	O Webservice	
* Database Type	SQL Server	(Support SQL Server 2008 R2)	1		
* 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				
<ul> <li>In Table</li> <li>UserInfo</li> <li>✓ Learn new users during auther</li> </ul>	Column UserID	v is user name, Column Passw	ord 💉 is password.		
<ul> <li>Learn the user group during</li> </ul>	new user authentication				
* User Group Containing Auto Ad	Ided Users: new2	Select User Group			
If you don't configure mapping a	among the user group, table name ar	nd column name, all users newly learned w	ill be added to this user group.		
<ul> <li>Existing users update the user</li> </ul>	group automatically				
Enable an Encryption and Decrypt	ion Plug-in:	]			
If the user password of the databa	se server is encrypted, you can enab	le and configure an encryption and decrypti	on plug-in by clicking 😩 Import Password Plug-in to	mport a password plug-in	
You can configure mapping among	the user group, table name and colu	mn name to enable the system to learn use	er information from the database during user authen	tication.	
User	Table Name	Column Name	Association	O	peration
User Group 🗸	<b>v</b>	<b>v</b>	Use table's	×	Add
			to associate the tableUserInfo's	×	
Mobile No.	UserInfo	Moblie phone	Self Reference		Delete
Test User Name:	111				
Test Password:	•••	Identity Authen			
You can verify whether a user pass	es database server authentication by	y entering a test user name and test passw	ord and clicking Identity Authentication.		
		Modify	et Refresh		
		inouily ites			

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

### Authentication Using Remote RADIUS Server

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



IP RG-SMP	RG-SMP Security Management Platform Professional				🖸 Feedback 💈 Online Senice 🗢 Technical Forum 🔔 Abou Technical Support Hotline: (+86)4008-111-007			
Administrator [admin] Login IP [1]	2.18.7.19] Login Date [2015-11-12 14:23:41]			🖾 Online User 🕭	System Status	🔓 Change Password	C Logout	
Authentication & Authority 👻	<ul> <li>Authentication &amp; Authority &gt; External Identity Ce</li> </ul>	nter						
Solution Contraction Contraction	External Identity Center							
Le Device	Generic LDAP	Windows AD Domain	External Database	Remote Radius Server	Ø Webservice	e		
	<ul> <li>Remote Radius Server IP:</li> <li>Remote Radius Server Authentication Port:</li> <li>Remote Radius Server Accounting Port:</li> <li>Remote Radius Server Key:</li> <li>Learn user information when authenticatio</li> <li>Existing users update the user group auto Learn Grouping Method:</li> <li>User Group Containing Auto Added Users: Peap Authentication Agent Type:</li> </ul>	172 18 34 47 1812 1813 ruijie n is enabled imatically ④ Add users to specified 默认用卢绾 FORWARD	(Default: 1812) (Default: 1813) group <sup>●</sup> Group users based on user name suffix <sup>●</sup> <u>Select User Group</u>					
			Modify Reset Refresh					

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

### **Correlation with Remote Web Service**

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

AP RG-SMP S	Security Management Platform   Professional	M Feedback	Sonline Serv	ice 🔍 Technical Forum al Support Hotline: (+86)4	About 008-111-000
Administrator [admin] Login IP [17	2.18.7.19] Login Date [2015-11-12 14:23:41]	🔀 Online User	System Status	🔓 Change Password	
Authentication & Authority 👻	Authentication & Authority > External Identity Center				•
♣ Online User ▲ User	External Identity Center				
🖉 User Group 🏂 Device	EnableExternal Identity Center     Generic LDAP     Windows AD Domain     External Database     Remote Radi	ius Server	Webservic	e	
Backlist         Self-Registration         Mobile Terminal         MAC Terminal         External Identity Center	* Remote Web Service Server IP:     [192.168.5.245]       * Remote Web Service Server Port:     8061       * Remote Web Service Server Address:     sso_authenticate/WSAuther       Obtain     Remote Web Service Access URL:       http://192.168.5.245.0001/sso_authenticate/WSAutherticate				E
Authentication Settings	* Identity Authentication Mode:  © Log in to the remote Web server for Identity Authentication  © Query user Informatio	n on the Web service servi	er for Identity Aut	hentication	
Image: Selletin Information         Image: Client Control         Image: Client Control	Iteam the user group during new user authentication         * User Group Containing Auto Added Users:         prew       @ 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 un         If you don't configure mapping between the data element to be returned and user group information for the user information obtaining interface, all un         If you don't configure mapping between the data element to be returned and user group information for the user information obtaining interface, all un	sers newly learned will be	added to the defa	iult user group.	
	Parameter Settings for Identity Authentication Interface  Interface Name: authenticate				



IP RG-SMP Se	ecurity Management Platform Professional	🖂 Feedback 💲 Online Ser Technic	vice 🙄 Technical Forun al Support Hotline: (+86)4	n 🔔 Abo 4008-111-0	ut O
Administrator [admin] Login IP [172.1	8.7.19] Login Date [2015-11-12 14:23:41]	🗺 Online User 🔎 System Status	🔓 Change Password	<b>O</b> Logo	Jt
Administrator [admin] Logn IP [172 -Authentication & Authority * © Online User User Group © Diser Group © Dise Group © Billschist © Self Registration © Mobile Terminal © Mobile Terminal	Learn the user group during new user authentication     User Group Containing Auto Added Users: new <u>Q Select User Group</u> If you don't configure mapping between the data element to be returned and user group information for the user information obtaining interface, a     Existing users update the user group automatically     Parameter Settings for Identify Authentication Interface     Interface Name; authenticate     Parameter	all users newly learned will be added to the def	fault user group.		ŕ
Authentication Settings     Borlal Settings     Bulletin Information     Client Control	Test User Name Test Vasor an Variante Distaining Interface: Test User Name Test Vasor Name You can verify whether a user passes remote web service server authentication by entering a test user name and test password and clicking Ident 'Top. If the Web service provided by the External Identity Center does not comply with WS-I specifications, or the security mechanism and other spe Web service adapter.	ity Authentication.	ms, please connect via th	ie	E
System Maintenance 🔹	Modify Reset Refresh				

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

# **User Self-Registration**

### **User Self-Registration**

#### **Function Description**

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

### **Configuration Tips**

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

### **Configuration Steps**

# **Email Self-Registration**

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



AP RG-SMP S	Security Management Platform   Professional
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-11 14:03:02]
Authentication & Authority 🔻	Authentication & Authority > Self-Registration
Soline User	Common User Self-Registration Enable
😕 User Group	Common User Self-Registration is disabled.
📥 Device	
🚰 Blacklist	
Self-Registration	
Mobile Terminal	
MAC Terminal	
🕵 External Identity Center	
Authentication Settings	
EE Portal Settings	
Rulletin Information	
Client Control	

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

ID DC CMD	Sequrity Management Blatform	🖂 Fee
ng-smp	Security Management Platform   Professional	
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-11 14:03:02]	Online User
Authentication & Authority 🔻	Authentication & Authority > Self-Registration	
Online User User User Group Device Device Blacklist Self-Registration Mobile Terminal External Identity Center Authentication Settings Portal Settings Dotal Settings Device	Common User Self-Registration   Email Email Registration: After adding a common user, the system will send the username and password to the registered email address.  SMS SMS Registration: After adding a common user, the system will send the username and password to the registered mobile number.  Third Party Correlation Registration Third Party Correlation Registration: The system will add common users after the users' identity information has been verified by the third-party system Cancel Next	
Client Control		

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



#### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

IP RG-SMP	Security Management Platform   Professional	Fe
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-11 14:03:02]	Monline User
Authentication & Authority 🔻	Authentication & Authority > Self-Registration	
Second Se	Common User Self-RegistrationEmail	
😕 User Group	Enterprise Email Suffix: Add	
Blacklist	Tip:All Email addresses are registered if no enterprise suffix is added.	
Self-Registration	☑ Use the email address prefix as the user name	
MAC Terminal	User Information Auto Learning     Default Auto-allocated User Group: smpad.com/13btest	
💃 External Identity Center	Tip: Email service is disabled and the system cannot send emails to users. Please Click here on able and configure Email service.	
Authentication Settings	Previous	
E Portal Settings		
Sulletin Information		
Client Control		

# **SMS Self-Registration**

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

IP RG-SMP	Security Mana	gement Platform   Professional	M Fee
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-1	1 14:03:02]	ine User
Authentication & Authority	System Maintenance > SM	S Settings	
System Maintenance	SMS Settings		
SMS Settings	Enable SMS Modem	Enable SMS Gateway     Enable 3G SMS Gateway	
Custom Manager Page	* Port (serial port): * Baud Rate: * Data Bit: * SIM Card PIN Code: * Manufacture Model:	COM1 9600 8 • 1234 Default Model •	
	<ul> <li>① Tips</li> <li>1. Port (serial port): the name</li> <li>2. Baud Rate: the same as th</li> <li>3. SIM Card PIN Code: SIM C</li> <li>4. Vendor Model: Vendor Model</li> </ul>	of the SMS modem port that connected with the server. at of the SMS modem. ard PIN Code of the SMS modem, (default PIN code of China Mobil is 1234, default PIM code of China Unicom is 0000). lel of the SMS modem. Select 'Default Model' if there is no other option in the list. Modify Reset Send a Test Message	

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



AP RG-SMP S	Security Management Platform   Professional
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-11 14:03:02]
Authentication & Authority 🔻	• Authentication & Authority > Self-Registration
♣ Online User ▲ User	Common User Self-Registration Enable
🐣 User Group	Common User Self-Registration is disabled.
📥 Device	
🚼 Blacklist	
Self-Registration	
Mobile Terminal	
📇 MAC Terminal	
Authentication Settings	
E Portal Settings	
Bulletin Information	
Client Control	

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

IP RG-SMP	Security Management Platform Professional	M Feed
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-11 14:03:02]	Online User
Authentication & Authority 👻	Authentication & Authority > Self-Registration	
Online User User User Group User Group Elacklist Self-Registration Mobile Terminal MAC Terminal External Identity Center Authentication Settings Portal Settings User Settings Elevent Information Client Control	Common User Self-Registration  Email Email Registration: After adding a common user, the system will send the username and password to the registered email address.  SMS SMS SMS SMS Third Party Correlation Registration Third Party Correlation Registration: The system will add common users after the users' identity information has been verified by the third-party system.  Cancel Next	

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



IP RG-SMP	Security Management Platform Professional	M Feedba
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-11 14:03:02]	Online User
Authentication & Authority 👻	Authentication & Authority > Self-Registration	
Secondaria Contraction Contractico Contrac	Common User Self-RegistrationSMS	
& User Group	Register only trusted mobile phones. Trusted Mobile Phone Management	
Levice	All mobile phone numbers are registered if "Register only Trusted Mobile Phones" is disabled.	
🚼 Blacklist	Use your mobile number as the user name.	
Self-Registration	User Information Auto Learning	
Mobile Terminal	* Default Auto-allocated User Group: smpad.com/13btest	
MAC Terminal	Previous Finish	
💃 External Identity Center		
Authentication Settings		
Portal Settings		
Bulletin Information		
Client Control		

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

🔗 RG-SMP Security Management Platform - Windows Internet Explorer	
10 http://172.18.7.55:8080/smp/trustedmobileservlet?kind=query&fromOtherPage=true	
Authentication & Authority > Trusted Mobile Phone Management > Query	
Mobile Number: Full Name: Query Reset	
Add Import Delete	
No matching record is found.	

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

<i> </i> RG-SMP Security Managemer	nt Platform - Windows Internet Explorer	- • 💌
http://172.18.7.55:8080/smp/	trustedmobileservlet	
Authentication & Authority >	> Trusted Mobile Phone Management > Add	
Trusted Mobile Phone Co	nfiguration	
* Mobile Number:		
Full Name:		
	Add Reset Return	

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



RG-SMP Security Management Platform - Windows Internet Explorer     http://172.18.7.55:8080/smp/trustedmobileservlet	
Trusted Mobile Phone Management > Import	
Upload Import File	
Import File(*.xls):	浏览
	rt Return
<ol> <li>The number of trusted mobile phones cannot exceed 10,000.</li> </ol>	
2. Only Excel files based on template format can be imported. Click 🌋	e to download the import template.
3. If the required information is not included in the Import Template, users	an create a new file based on the template.

# **Third Party Correlation Registration**

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

<b>IP RG-SMP</b>	Security Management Platform Professional	. Feed
Administrator [admin] Login IP [*	72.18.7.19] Login Date [2015-11-11 14:03:02]	Monline User
Authentication & Authority 🔻	Authentication & Authority > Self-Registration	
Online User User User Group Device Blacklist Self-Registration Mobile Terminal Mobile Terminal External Identity Center Authentication Settings Portal Settings Selletin Information Client Control	Common User Self-Registration   Email Email Registration: After adding a common user, the system will send the username and password to the registered email address.  SMS SMS SMS Registration: After adding a common user, the system will send the username and password to the registered mobile number.  Third Party Correlation Registration Third Party Correlation Registration: The system will add common users after the users' identity information has been verified by the third-party system.  Cancel Next	

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



IP RG-SMP	Security Manager	nent Platfor	m Professional
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-11 14:03	:02]	
Authentication & Authority 🔻	Authentication & Authority > Self-R	egistration	
Soline User	Common User Self-Registration-	-Third Party Correlation Re	egistration
Cost Group	* Third Party Database Types:	<ul> <li>SQL Server</li> <li>MySQL</li> <li>PostgreSQL</li> <li>Oracle</li> <li>DB2</li> </ul>	
Mobile Terminal	* Database Server IP Address:	172.18.34.16	
📇 MAC Terminal	* Database Server Port:	1433	
External Identity Center	* Administrator Account: * Administrator Password:	smp ●●●●●●	
E Authentication Settings	* Database Name:	SMPDB_266	Auto Obtain
EE Portal Settings	* User Information List Name:	T_USER	▼
Sulletin Information			Previous Next

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

AP RG-SMP	Security Man	agement F	latform	) Profes	sional
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-1	1-11 14:03:02]			
Authentication & Authority 🔻	Authentication & Authorit	ty > Self-Registration			
Second Contract Contr	Common User Self-Reg	gistrationUser Informa	tion Validation		
Buser Group	User Information:	Full Name	•	Add	
Self-Registration Mobile Terminal MAC Terminal	User Information User Name	Column Name USER_ID	Opera Dele	tion te	
External Identity Center				Previous	Next
Authentication Settings					

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



IP RG-SMP S	Security Management Platform   Professional
Administrator [admin] Login IP [17	/2.18.7.19] Login Date [2015-11-11 14:03:02]
Authentication & Authority 🔻	Authentication & Authority > Self-Registration
Second Se	Common User Self-Registration-User Information Learning
& User Group	* Default Auto-allocated User Group: smpad.com/Domain U
La Device	User Information Learning
🚼 Blacklist	User Information: User Group -
Self-Registration	Column Name: USER_GROUP_NAM ~ Add
Mobile Terminal	User Information Column Name Operation
	User Group USER_GROUP_NAME Delete
External Identity Center  Authentication Settings  Control Settings  Control Settings  Control	Previous Finish

### **Guest Registration**

### **Function Description**

This section describes how a common guest gets registered.

### **Configuration Tips**

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

### **Configuration Steps**

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

IP RG-SMP S	Security Management I	Platform Professional	Feedback 💈 Online Servic Technical	ce 🗢 Technical Forur I Support Hotline: (+86)	n <u>(1)</u> About \$008-111-000
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-11 17:09:25]	i∰Online	e User 🚨 System Status	Change Password	C Logout
Authentication & Authority 👻	Authentication & Authority > User Group > Quer	y User Groups			
Conline User	User Group Name:	Query Reset			
Levice	Add Delete				
Self-Registration	Totally 2 Records   Each Page 20 Records   Pa	ge 1 / totally 1 Pages   G0		P A	
Mobile Terminal	All None	User Group Name 🔻	Operatio	on	
		Guest User Group	aw   Modify   Restore Default S	ettings	
Sector External Identity Center		Default User Group	w Modify Restore Default S	ettings	
Authentication Settings	Totally 2 Records   Each Page 20 Records   Pa	ge 1 / totally 1 Pages   60		Q	
Bulletin Information     Client Control					

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



IP RG-SMP Se	ecurity Management Platform Professional	Feedback Solution Of the Service Technic Technical Support Hotlin					
Administrator [admin] Login IP [172.	18.7.19] Login Date [2015-11-11 17:09:25]	🐼 Online User 🐣 System Status 🔒 Change Par					
Authentication & Authonty  Conline User User User Group Becce Bellacklist Mobile Terminal MAC Terminal Excent Machine Content	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)         We nable Self-Service Password Change         Tips:         1. The Initial Password Check and the Password Complexity Check can apply to the user name/password authentication and certificate-based authentication.         2. When the password check functions apply to the certificate-based authentication, the password is the PIN code of USB key:         3. When it is configured that users failing in password certificate-date of diffice, users are allowed to change their passwords using Ruijie authentication client (RG-SU) and Ruijie Security Agent (RG-SA).						
Authentication Settings     Bortal Settings     Authentication     Client Control	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 Ruije Client         Allow managing guest users on a Ruije Self-Senice platform (registering users in common mode)         Allow managing guest users on a Ruije Self-Senice platform (registering users in SMS mode)         Network Information Anti-Tampering         Authentication will fail if a user changes the MAC address of the network adapter         Ø Tip. This function is available only for users of Ruije authentication client (RG-SU) and Ruije security agent (RG-SA).						

### **User Information Self-Maintenance**

### **Function Description**

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

#### **Configuration Tips**

N/A

### **Configuration Steps**

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

AP RG-SMP S	Security Management Platform   Professional	🖂 Feedback 💈 Online Se Techr	ervice 🔍 Technical Forur ical Support Hotline: (+86)	008-111-000
Administrator [admin] Login IP [17	2.18.7.19] Login Date [2015-11-11 17:09:25]	🔀 Online User 🚨 System Status	🔓 Change Password	
Authentication & Authority 👻	Authentication & Authority > User > Query Users			
Online User User User Subser Group Content Device SubsetRegistration	User Name: Full Name: User Group: User Type: All User Status: A Online or not: All I In Blacklist or not: All III Accurate Search Query Reset Advanced Search Q Add Delete Modify All Delete All	ul  uery users offline for a long time Import Users Import Network Bim	ing Information Export All	Results
Mobile Terminal	Add to Blacklist Issue Message or Patch Suspend Resume Customize User Fields	s SIM Card Management Customize Query List User In	formation Self-Service Mair	tenance
External Identity Center      Authentication Settings      Dortal Settings      Settings      Settings	No matching user information is for	sund.		
Client Control				

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



Administrator (admin) Login IP (1)	Security Management Platform Professional
Administrator [admin] Login IP [17 Authentication & Authority  Conline User Conlin	72.18.7.19] Login Date [2016-11-11 17:09:25]  Authentication & Authority > User > User Information Self-Service Maintenance  Enable User Information items for Self-Service Maintenance  Items for Selection  Full Name Nick Name   Please select user information items for Self-Service Maintenance  Full Name  Please select user information items for Self-Service Maintenance  Full Name  Please select user information items for Self-Service Maintenance  Please select user information items for Self-Service Maintenance  Please select user information items for Self-Service Maintenance  Full Name  Please select user information items for Self-Service Maintenance  Please select user information items for Self-Service Maintenance  Full Name  Postal Code
	Modify Reset Return

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

### **Mobile Terminal Management**

#### **Function Description**

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

#### **Configuration Tips**

N/A

#### **Configuration Steps**

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



IP RG-SMP	RG-SMP Security Management Platform Professional			vice 😌 Technical Forur al Support Hotline: (+86)	n 🔔 About 4008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-11 17:09:25]	E Contraction of the second	Online User 🚨 System Status	Change Password	C Logout
Authentication & Authority 👻	Authentication & Authority > User Group > C	uery User Groups			
Solution Open	User Group Name:	Query Reset			
Device	Add Delete				
Self-Registration	Totally 2 Records   Each Page 20 Records	Page 1 / totally 1 Pages   G0		10 Q	
Mobile Terminal	AllNone	User Group Name 🔻	Opera	tion	
		Guest User Group	View   Modify   Restore Default	Settings	
Sternal Identity Center		Default User Group	View Modify Restore Default	Settings	
Authentication Settings	Totally 2 Records   Each Page 20 Records	Page 1 / totally 1 Pages   60		D (1)	
Client Control					

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

<b>AP RG-SMP :</b>	
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-11 17:09:25]
Authentication & Authority 👻	Authentication & Authority > User Group > Modify User Group
<ul> <li>Online User</li> <li>User</li> <li>User Group</li> <li>Device</li> </ul>	User Group Name: Default User Group Access Control Behavior Restrict Access Rules
Blacklist	Multi-Access Limit
Self-Registration Mobile Terminal MAC Terminal KAC Terminal KExternal Identity Center	An account can be used on a maximum of 2 terminals at the same time (Default: 1)     An account can register(2 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.
Authentication Settings	Offline Timer
E Portal Settings	Disabled
Bulletin Information     Client Control	Daily Timer     Total Timer     Single Timer
	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.         The supervised account of the supervised accounts will be suspended.         The supervised accounts will be suspended.
System Maintenance 🔹	Time management of messages displayed on clients         A message displayed on a client automatically close in 5         seconds (Time range: 5-300)

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

IP RG-SMI	P Self-Service	Platform	1.111					About
User Name[test] Logir	Time[2015-11-11 17:34:12]							QLogout
My self-service	My self-service> My Mobile	Terminal						
My Information								
Guest Management	MAC		NAS IP	SSID	Register Status	Online Status	Operation	
W My Mobile Terminal	848e0cbc111b	10.1.1.105	10.1.1.28	10-hujq	Registered	Online	Delete   Authentication Failure Logs   Online History	
Change Password	<ol> <li>Tip: You can register your mobile t password.</li> </ol>	erminal. A maximum of 2 m	obile terminal(s) can be regi	stered. After being registere	d, the mobile terminal can be	e connected to the correspon	nding SSID without asking you to enter the user name and	



# **Common Functions**

# **Authentication & Authority**

### **User and Security Management**

#### **Function Description**

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

#### **Configuration Tips**

N/A

### **Configuration Steps**

# Adding a User Group

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

ID DC CHD		mont Distance la serie	M Feedb	ack 🛛 울 Online Ser	vice 🙄 Technical Forun	n 🔔 About
IP RG-SMP	Security Manage	ement Platform   Professional		Technic	al Support Hotline: (+86)	008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-11 17:	09:25]	Online User	less System Status	🔒 Change Password	C Logout
Authentication & Authority 👻	Authentication & Authority > Use	er Group > Query User Groups				
😂 Online User						
🚨 User	User Group Name:	Query Reset				
🚨 User Group						
📥 Device	Add Delete					
💱 Blacklist	Add Delete					
Self-Registration	Totally 2 Records   Each Page 20	Records   Page 1 / totally 1 Pages   G0			IQ Q	
Mobile Terminal						
📇 MAC Terminal	AllNone	User Group Name			Operation	
_		Guest User Group		View   Modi	ify   Restore Default Settin	<u>igs</u>
External Identity Center		Default User Group		View   Modi	ify   Restore Default Settin	igs
Authentication Settings	Totally 2 Records   Each Page 20	Records   Page 1 / totally 1 Pages   60				
Portal Settings						
Sulletin Information						
Olient Control						
System Maintenance						
Log Audit						'

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



### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

IP RG-SMP :	Security Management Platform	✓ Feedbessional	oack 💈 Online Ser Technic	vice 🙄 Technical Forum al Support Hotline: (+86)4	About 008-111-000
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-11 17:09:25]	ine User	🚨 System Status	🔓 Change Password	C Logout
Authentication & Authority 👻	Authentication & Authority > User Group > Add User Group				^
<ul> <li>♀ Online User</li> <li>♀ User</li> <li>֎ User Group</li> <li>▲ Device</li> </ul>	* User Group Name: new Access Control Behavior Restrict Access Rules				
😼 Blacklist	Enable Wired Access	Enable Wireless Ac	cess		
Self-Registration	Network Information Verification 🗐 All	Network Information V	erification 🔲 All		
Mobile Terminal	HD Serial Number Verification	HD Serial Number Ve	erification		E
a MAC Terminal	IP Type Authentication:   Static  Dynamic	IP Type Authentication	on: 🖲 Static 🔍 D	ynamic	
External Identity Center	User IP Verification	User IP Verification			
	User MAC Verification	User MAC Verification	n		
Authentication Settings	User IMSI	User IMSI			
Bulletin Information	<ul> <li>NAS IP Verification</li> <li>NAS Port Verification</li> </ul>	SSID Verification		•	
Client Control	① Tips:				
	<ol> <li>Wireless SSID names are separated by commas (,), e.g., web-wired-SSID,</li> <li>The MAC address unification and the MAS number (mahile phase number).</li> </ol>	web-wireless-SSID.	anna tina		
	2. The WAC address verification and the INISI number/mobile phone number ve     3. When the network information auto-learning and the network information veri	finication cannot be enabled at the	e same time. Lusers to networks (	Or the system will bind use	ars.
	to networks through network information auto-learning in the next authentication	n.	access to networks. (	and ayoton win only use	
	4. When the network information verification is enabled, the client must upload	network information and the uploa	aded network informa	tion must be consistent w	th
System Maintenance	that in the user information. Otherwise, authentication may be failed.				
Log Audit	5 Duijio cliente, such as DG SA For Mindows, will uplead all notwork informat	ion while other cliente de not unle	ad hard dick corial n	umber and ID address type	

# Adding a User

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

IP RG-SMP	Security N	<b>Aanagem</b>	ient Plat	form   Pro	fessior	nal	P F	eedback 💈 Online Tec	Service 🖃 Technical Forun hnical Support Hotline: (+86)4	n About
Administrator [admin] Login IP [1]	72.18.7.19] Login Date	[2015-11-11 17:09:2	5]				Conline U	ser 🚨 System Stat	us 🔓 Change Password	O Logout
Authentication & Authority 🔻	Authentication 8	Authority > User >	Query Users							
♀ Online User	User Name: Online or not: All	Full Nam	e: Us	ser Group:	User	Type: All Query Reset	User Status:      Advanced Search G	UI -	a long time	
Self-Registration Self-Registration Mobile Terminal MAC Terminal	Add De Add to Blacklis	elete Modify	All Dele e or Patch Suspe	ete All	Customize	User Fields SIM Card I	Import Use Management <u>Custor</u>	rs Import Network E nize Query List Use	Binding Information Export Al	I Results
5 External Identity Center	Totally 2 Records	s   Each Page 20	Records   Page 1	/ totally 1 Pages	GO					
Authentication Settings	<u>Ali  None</u>	<u>User Name</u> ▼	<u>Full Name</u> 🔻	<u>User Group</u> ▼	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	Operation	
Client Control		123	123	Guest User Group	Delete Account when Expire	2015-11-13 17:35:48	0	<u>1 Online Users</u>	View   Modify   Mobile Term	ninal
		test	111	Default User Group	Never Expire		0	Offline	View   Modify   Mobile Term	ninal
System Maintenance	Totally 2 Record	s   Each Page 20	Records   Page 1	/ totally 1 Pages	GO				B< <	

2) Click Add to enter the Add User page.



#### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

IP RG-SMP S	Security Mana	gement Pla	tform Professional		⊠ Feedback 🛛 💈 Online Ser Technic	vice 🙄 Technical Forun al Support Hotline: (+86)4	008-111-000
Administrator (admin) Login IP (17	2.18.7.19] Login Date (2015-11-	11 17:09:25]			🖾 Online User 🚨 System Status	🔓 Change Password	O Logout
Authentication & Authority 👻	Authentication & Authority	> User > Add User					^
Solution	Basic Information						
Buser Group	* User Type:	Common User OGues	t User 🔘 Thirdparty User	* User Status:	Normal O Suspended		
A Device	* User Name:	newuser		* Full Name:	test		
Blacklist	Nick Name:						
Self-Registration	* Password:	•••		* Confirm Password:	•••		
Mobile Terminal	Type of Account Validity Period:	Never Expire O Delete Account when Expire	Account when Expire  Suspend				
	* User Group:	new	Select User Group				E
External Identity Center	Customize User Fields	Add Custom User Fields					
Authentication Settings	No custom user field is fou	nd. Please click Add a Custo	im User Field to add it.				
E Portal Settings	Detail Information						
C. Dullatia lafamatian	Gender:	Not Selected		Email Address:			
Client Control	ID Type:	Not Selected		ID Number:			
	Educational Background:	Not Selected		Telephone Number:			
	Mobile Number:			Address:			
	Postal Code:						
	Network Binding List 崤	Add Network Binding List					
System Maintenance	No network binding informa	tion of the user is found. Plea	ase click Add a Network Binding List	o add it.			
Log Audit 🔸	0 T						

# **Importing Users**

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

IP RG-SMP Security Management Platform Professional Professional Technical Support Hotime: (+86)4008-111-000											
Administrator (admin) Login IP (172.18.7.19) Login Date (2015-11-11 17.09.25) 😥 Online User 🐣 System Status 🔒 Change Password 🔍 Dogout											
Authentication & Authority 👻	O Authentication & Authority > User > Query Users										
Solution Contractions of the second s	User Name: Full Name: User Group: User Type: All User Status: All   Online or not: All  In Blacklist or not: All  In Black										
See Blacklist           Self-Registration           Mobile Terminal           MAC Terminal	stration minal Mad to Blacklist issue Message or Patch Suspend Resume Customize User Fields SIM Card Management Customize Query List User Information Self-Senice Maintenance										
External Identity Center	Totally 3 Records	Each Page 20	Records   Page  1	/ totally 1 Pages	GU					E 1	
Authentication Settings     B Portal Settings	All None										
Oclient Control		123	123	Guest User Group	Delete Account when Expire	2015-11-13 17:35:48	0	<u>1 Online Users</u>	View   Modify   Mobile Termi	nal	
		newuser	test	new	Never Expire		0	Offline	View   Modify   Mobile Termi	nal	
		test	111	Default User Group	Never Expire		0	Offline	View   Modify   Mobile Termi	nal	
System Maintenance											

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



IP RG-SMP		M Feed	Iback 💈 Online Ser Technic	vice 🔍 Technical Forur al Support Hotline: (+86)	n 🔔 About 1008-111-000
Administrator [admin] Login IP [1]	2.18.7.19] Login Date [2015-11-11 17:09:25]	Online User	🚨 System Status	🔒 Change Password	O Logout
Authentication & Authority 👻	Authentication & Authority > User > Import Users				
<ul> <li>♀ Online User</li> <li>♀ User</li> <li>♀ User Group</li> <li>▲ Device</li> <li>♀ Blacklist</li> </ul>	Upload Files Importing File (*.xts/*.csv): C:\Users\hujiaq\Desktop\User_Import_Template.xts C:\Users\hujiaq\Desktop\User_Import_Template.xts Delete users not contained in the imported file			) ( )	1览
Self-Registration Mobile Terminal MAC Terminal	Import Users Return				
External Identity Center	<ol> <li>The number of users cannot exceed 10,000.</li> <li>Only EXCEL or CSV files based on template format can be imported. Please click <sup>2</sup>/<sub>here</sub> to download an import template.</li> <li>If the required information is not included in the Import Template, users can create a new file based on the template.</li> </ol>	e.			
Portal Settings					

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

IP RG-SMP Security Management Platform Professional Continue Control C										
Administrator (admin) Login IP [17	72.18.7.19] Login Date [2015-11-11 17:09:25]	🐼 Online User 🦲 System Status 🛛 🔓 Change Password 🛛 🕠 Logout								
Authentication & Authority 👻	<ul> <li>Authentication &amp; Authority &gt; User &gt; Import Users &gt; Import Results</li> </ul>									
➢ Online User Ser	Import Results									
Subser Group	Import a total of 3 users: 3 are imported and 0 failed Close the imported files.	I to be imported. (See the operation logs for details.)								
Self-Registration	3 files are imported.									
Mobile Terminal	Row No.	User Name								
a MAC Terminal	Row 2	Jay								
External Identity Center	Row 1	Tom								
	Row 3	Herry								
Authentication Settings										
Portal Settings	R	eturn								
- Bulletin Information										
Sustam Maintananca										
Log Audit										

# **Modifying Users**

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



IP RG-SMP S	Security N	lanagem	ent Platf	orm   Prof	ession	al	F	eedback 울 Online Tec	Service 🖃 Technical Forum	About 08-111-000	
Administrator (admin) Login IP (17	'2.18.7.19] Login Date	[2015-11-11 17:09:2	5]				Monline U	ser 🚨 System Stat	us 🔒 Change Password		
Authentication & Authority 👻	Authentication 8	Authority > User >	Query Users								
Sonline User User User Group	User Name: Full Name: User Group: User Type: All Vuser Status: All										
Blacklist         Solf-Registration         Mobile Terminal         MAC Terminal         Statement         Statement	Add De Add to Blacklist Totally 6 Records	elete Modify Issue Message	All Delete or Patch Susper Records   Page 1	e All	istomize ( GO	Jser Fields SIM Card M	Import Users anagement Customiz	Import Network Bin	ing Information Export All Res Iformation Self-Service Maintena	<u>ance</u>	
Authentication Settings	Alli None	<u>User Name</u> 👻	<u>Full Name</u> 🔻	<u>User Group</u> ▼	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	Operation		
Olient Control		123	123	Guest User Group	Delete Account when Expire	2015-11-13 17:35:48	0	<u>1 Online Users</u>	View   Modify   Mobile Termin	<u>ial</u>	
		Herry	Herry	Default User Group	Never Expire		0	Offline	View   Modify   Mobile Termin	ial	
		Jay	Jay	Default User Group	Never		0	Offline	View   Modify   Mobile Termin	ıal	
System Maintenance		newuser	test	new	Never Expire		0	Offline	View   Modify   Mobile Termin		

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

IP RG-SMP	Security Ma	⊠ Feedback 💈 Online Ser Technic	vice 🙄 Technical Forun cal Support Hotline: (+86)4	n 🚹 About 1008-111-000			
Administrator [admin] Login IP [1	72.18.7.19] Login Date [201	5-11-11 17:09:25]			🖾 Online User 🚨 System Status	Change Password	O Logout
Authentication & Authority 🔻	<ul> <li>Authentication &amp; Auth</li> </ul>	nority > User > Modify Users in	Batches				
➢ Online User ➢ User	User Group Informa	tion					
& User Group Device	User Group: User Type Change	No Change	•				
Blacklist	User Type:	<ul> <li>Not Modify</li> <li>Transfer from a co</li> <li>Transfer from a thi</li> </ul>	mmon user to a thirdparty user rdparty user to a common user				
MAC Terminal	Network Verificatio	n Information					
External Identity Center	Clear Network Verifica	tion Information: 🔟					
Authentication Settings			Mo	dify in Batch Return			
Portal Settings	Tips:						
Bulletin Information	1. If the user group of	a user is modified, the user gro	up configuration will take effect on	next authentication.			
Client Control	2. The user group of a	guest user will not be modified					

# **Customizing a Query List**

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



IP RG-SMP Security Management Platform   Professional Events Content of the Service Content Platform   Professional Technical Support Hotime: (+86)4008-11										About 008-111-000	
Administrator (admin) Login IP (172.18.7.19) Login Date (2015-11-11 17.09.25) 😥 Online User 🙆 System Status 🔒 Change Password 🖓 L											
Authentication & Authority 🔻	Authentication 8	Authority > User >	Query Users							-	
Se Online User User User Group Bovice	User Name: Full Name: User Group: User Type: All User Status: All  Online or not: All  In Blacklist or not: All  Accurate Search Query Reset Advanced Search Query users offline for a long time										
Blacklist Self-Registration Mobile Terminal	Add De Add to Blacklist	lete Modify	All Delete	e All	istomize l	Jser Fields SIM Card M:	Import Users	Import Network Bin	ding Information Export All Re	esults nance	
🕵 External Identity Center	Totally 6 Records	s   Each Page 20	Records   Page 1	/ totally 1 Pages	<b>GO</b>						
Authentication Settings	All None										
Olient Control		123	123	Guest User Group	Delete Account when Expire	2015-11-13 17:35:48	0	<u>1 Online Users</u>	View   Modify   Mobile Termi	inal	
		Herry	Herry	Default User Group	Never		0	Offline	View   Modify   Mobile Termi	inal	
		Jay	Jay	Default User Group	Never		0	Offline	View   Modify   Mobile Termi	inal	
System Maintenance		newuser	test	new	Never Expire		0	Offline	View   Modify   Mobile Termi	inal	

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

IP RG-SMP S	Security Manage	ment Pla	tform   Professio	onal								
Administrator [admin] Login IP [172.18.7.19] Login Date [2015-11-11 17:09:25]												
Authentication & Authority 👻	Authentication & Authority > User	> Custom Display L	ist									
Solution User												
Super 2	Please select the item(s) to be	included in the Qu	ery List.									
😕 User Group	Items for Selection		Selected Items									
a Device	Nick Name		User Name									
🔯 Blacklist	User Type User Status		Full Name User Group									
Self-Registration	Gender Email Address		Type of Account Validit Expiry Date									
Mobile Terminal	ID Type		Number of Blacklisted U									
	Educational Background		Uniine info									
<u> External Identity</u> Center	Telephone No. Mobile No.											
Authentication Settings	Postal Code			▼								
Portal Settings	Last Attack Event Count											
	Last Login Time Account Administrator											
Rulletin Information	Account Registration Da											
🕜 Client Control												
			Modif	y Reset Return								
System Maintenance 🔹 🕨												
Log Audit												


# **Custom Display List**

### **Function Description**

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

### **Configuration Tips**

N/A

## **Configuration Steps**

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

IP RG-SMP :	Security Managemen	t Platform	Professional		Feedback	Sonline Service 📼 Tech Technical Support Ho	nical Forum (1) About
Administrator [admin] Login IP [17	2.18.7.19] Login Date [2015-11-11 17:09:25]				🖾 Online User 🚨 Sys	stem Status 🛛 🔓 Change I	Password OLogout
Authentication & Authority 👻	Authentication & Authority > Online User > 0	Query Online Users					
<ul> <li>Online User</li> <li>User</li> <li>User Group</li> <li>Device</li> </ul>	User Name: Full Na User IP: NAS IF	me:	User Group:	Query Reset A	lvanced Search		
Self-Registration Self-Registration Mobile Terminal	Clear Residual Users Force Offline Totally 1 Records   Each Page 20 Record	Reauthenticate Issue	e Message or Patch Add	to Blacklist 🔲 Se	nd online/offline notifications	to a third-party system	Sustomize Query List
	All   None User Name 🔻				NAS Port		Operation
External Identity Center	<u>123</u>	123	10.1.1.105	10.1.1.28	1	0:19:49	View
Authentication Settings	Totally 1 Records   Each Page 20 Record	is   Page 1 / totally 1 Page	ages   GO				K A P K
Client Control	Tips     Reauthenticate is available only for Ruijle a     If a user has already gone offline, you can	authentication clients and Rui clear such remaining informa	jie security agents. tion by using the Clear Reside	ual Users function.			

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



IP RG-SMP :	Security Management Platform Professional
Administrator [admin] Login IP [1]	72.18.7.19] Login Date [2015-11-11 17:09:25]
Authentication & Authority 👻	Authentication & Authority > Online User > Custom Display List
➢ Online User ➢ User	Please select the item(s) to be included in the Query List.
😕 User Group	To be Selected Selected
Device D	User Group Authen Method Login Time Security Zone Computer Protection : HD Serial Number IPT Type User MAC Wireless SSID Gateway IP Subnet Mask
Portal Settings     Settings     Settings     Client Control	Preferred DNS Standby DNS VLAN ID VLAN Name Upstream Traffic Client Type Modify Reset Return

# **Online Users Trend Chart**

## **Function Description**

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

## **Configuration Tips**

N/A

### **Configuration Steps**

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



IP RG-SMP	Security Management Platform Professional	☑ Feedback 💈 Online Sen Technic	rice 🙄 Technical Forum al Support Hotline: (+86)4	About 11-000
Administrator [admin] Login IP [1]	2.18.7.19] Login Date [2015-11-11 17:09:25]	🖾 Online User 🚨 System Status	G Change Password	O Logout
Authentication & Authority 🔻	Online users trend chart		Choose the cu	TYSY A
♣ Online User ▲ User	Selected Time: Last Day   Last Week   Last Month   Custom			
😕 User Group	Access Type			A
Blacklist	Wired Access Wireless Access VPN Access All Online Users			
Mobile Terminal				
Authentication Settings	0 2015-11-10 18:00 2015-11-10 21:00 2015-11-11 24:00 2015-11-11 03:00 2015-11-11 06:00 2015-11-11 09:00	2015-11-11 12:00 2015-11-11	15:00	÷
Client Control	SARAL Type     ■ SAB Client ■ Standard 802.1X ■ VPN Client ■ All Online Users user↑			
				ne
System Maintenance	2015-11-10 18:00 2015-11-10 21:00 2015-11-11 24:00 2015-11-11 03:00 2015-11-11 06:00 2015-11-11 09:00	2015-11-11 12:00 2015-11-11	15:00	

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

Administrator (admin) Login IP (172.18.7.19) Login Date (2015-11.11 17:09.25)       Image Passwood () Log         Authentication & Authonity ()       Online User ()       Status ()       Online User ()       Status ()       Online User ()       Choose the curve         Online User ()       User ()       User ()       Status ()       Online User ()       Choose the curve         Online User ()       User ()       Status ()       Online User ()       Choose the curve         Online User ()       User ()       Status ()       Online User ()       Choose the curve         Online User ()       User ()       Status ()       Online User ()       Status ()       Choose the curve         Status ()       Status ()       User ()       Status () <t< th=""><th>ID RG-SMD</th><th>Security Management Pla</th><th>tform Professional</th><th>🖂 Fe</th><th>edback 💈 Online Servi</th><th>ice 🖤 Technical Forun</th><th>n 🔔 About</th></t<>	ID RG-SMD	Security Management Pla	tform Professional	🖂 Fe	edback 💈 Online Servi	ice 🖤 Technical Forun	n 🔔 About
Administrator [admin] Login P [172:18.7.19] Login Date [2015-11:11 17:09:26]       Contine User @ System Status @ Change Password @ Log         Administrator [admin] Login P [172:18.7.19] Login Date [2015-11:11 17:09:26]       Contine User @ System Status @ Change Password @ Log         @ Online User       Contine Users trend chart       Choose the curve         @ Online User       Salestiel Ties: LastDay   LastWeek   LastWoek   LastWoek   LastWoek   LastWoek   LastWoek   LastWoek   LastWoek   LastWoek   LastWoek   LastWeek   LastWee	I MO-SINIT .	becanty Management ria	COTTI Protessional		Technica	al Support Hotline: (+86)4	1008-111-000
Authentication & Authority **       Online users trend chert       Choose the curve*         Online users       Satertet Tise: LastOpy   LastWeek   LastMont   Custom         Busic Group       Satertet Tise: LastOpy   LastWeek   LastMont   Custom         Conserved       Satertet Tise: LastOpy   LastWeek   LastMont   Custom         Mobile Terminal       MAC Terminal         MAC Terminal       Confirm         Cancer Type       Confirm         Confirm       Cancel         Oline users       User f         Confirm       Cancel         Out and thenticy Center       Confirm         Cancer Type       Satert Time: Distributi I         Satert Time:       Distributi I         Confirm       Cancel         Objection       Confirm         Confirm       Cancel         Objection       Confirm         Satert Time:       Distributi Information         Confirm       Cancel         Satert Type       Satert Type         Satert Type       Satert Type         Satert Type       Satert WEE Chert Standard Woll X         Contert Confirm       Cancel         Online Users       Usert	Administrator [admin] Login IP [17	/2.18.7.19] Login Date [2015-11-11 17:09:25]		Monline Us	er 🚨 System Status	🔓 Change Password	C Logout
Colline User   Subser   Subser Group   Device   Subschild   Self-Registration   Mobile Terminal   MAC Terminal   Statetter Time:   Authentication Settings   Burdenti Authon Cancer   Self-Registration   Self-Registration   Subschild   General Mathematication Settings   Burdenti Authon Mathemation   Schlenti User   Schlenti User	Authentication & Authority 👻	Online users trend chart				Change the m	17.Ve T
User         © User Group         © Dexice         © Dexice         © More Access Type         © Ward Access Wireless Access VPN Access         © More Registration         © Mole Terminal         © Atchentication Settings         © Detrice         © Detrice         © Authentication Settings         © Client Type         © Client Type         © Client Type         © Client Type	Secondaria Contine User	Selected Time: LastDay   LastWeek   LastMonth	Custom				
West Group       Access Type         Device       Ward Access Type         West Group       Ward Access Windess Access         Start Time:       2015-11-11         Mobile Terminal       Image: Cleart Type         Mc Terminal       Image: Cleart Type         Start Time:       2015-11-11         Mobile Terminal       Image: Cleart Type         Start Time:       2015-11-10 2010         Start Time:       2015-11-11 24:00         2015-11-10 18:00       2015-11-11 24:00         2015-11-10 18:00       2015-11-11 24:00         2015-11-10 18:00       2015-11-11 24:00         2015-11-10 18:00       2015-11-11 24:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00         2015-11-10 18:00       2015-11-11 18:00	Ser Contraction of the series		Please select a time:	:			
Bulckist     Balckist     Belleckist     Belle	😕 User Group	Access Type					
Set Edechait       user f       Ede Time:       2015-11-11         Mobile Terminal       1       Confirm       Cancel         MAC Terminal       0       0       0       0         Set Registration       0       0       0       0       0         Set Registration       0       0       0       0       0       0         Set Registration       0       0       0       0       0       0       0         Set Registration       0 <td>Device</td> <td>📕 Wired Access 📕 Wireless Access 📕 VPN Access</td> <td>Start Time: 2015-11-01</td> <td></td> <td></td> <td></td> <td></td>	Device	📕 Wired Access 📕 Wireless Access 📕 VPN Access	Start Time: 2015-11-01				
Weble Terminal       0	Blacklist	user↑	End Time: 2015-11-11				
Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit lemmal         Implicit lemmal       Implicit lemmal       Implicit lemmal       Implicit	Self-Registration	1	Confirm				
Subscription formation     Set Subscription     Subscrite     Subscription     Subscription     Subscrite     Subscripti		0	Commin Cancer				
Restand Identity Center          •	E MAC Terminal	0 -					
Authentication Settings         0215-11-10 81:00 2015-11-10 21:00 2015-11-11 24:00 2015-11-11 06:00 2015-11-11 09:00 2015-11-11 12:00 2015-11-11 12:00           B Portal Settings         Client Type           Billelin Information         SA Client WEB Client Standard 502.1X VPN Client All Online Users	Kenternal Identity Center	0					
Authentication Settings     Client Type     SA Client WEB Client Standard 802.1X VPN Client All Online Users     Web Client Control		0	-11.24-00 2015-11-11.02-00 2015-11-11.0	6-00 2015-11-11 00-00 2015-11-11	12.00 2015-11-11	5-00	me →
Bulletin Information     SA Gient WEB Gient Standard 802.1X     VTPN Client All Online Users	Authentication Settings	2013-11-10 18/00 2013-11-10 21/00 2013-11-	-11 24100 2015-11-11 03100 2015-11-11 0	8100 2013-11-11 09100 2013-11-11	. 12100 2013-11-111	.5100	
Cristin Type     Cristin Type     Sulletin Information     SA Cleret     WEB Client     Standard 802.1X     VPN Client     All Online Users     Userf	EE Portal Settings	Client Time					
Glient Control       User^		Citent Type					
(d) Client Control user↑	We Bulletin Information	SA Client WEB Client Standard 802.1X	N Client 🔲 All Online Users				
	<b>W</b> Client Control	user↑					
		0					
		0 -					
		0 -					
0		0 -					ime
System Maintenance	System Maintenance	0 2015-11-10 18:00 2015-11-10 21:00 2015-11	-11 24:00 2015-11-11 03:00 2015-11-11 0	6:00 2015-11-11 09:00 2015-11-11	1 12:00 2015-11-11 1	5:00	→ _

## **SIM Card Management**

## **Function Description**

This section describes how to manage SIM cards.

# **Configuration Tips**

N/A



# **Configuration Steps**

# Adding the SIM Card Information

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

IF RG-SMP Security Management Platform Professional Security Management Platform Professional Technical Support Hotline: (+864008-111-000											
Administrator [admin] Login IP [17	2.18.7.19] Login Date	2015-11-11 17:09:	25]					Monline Us	er 🚨 System Stat	us 🔒 Change Password	C Logout
Authentication & Authority 👻	Authentication 8	Authority > User >	Query Users								
😂 Online User											
🚨 User	User Name:	Full Nar	ne:	User Group:		Jser Type: All	<ul> <li>User Sta</li> </ul>	itus: All 🔻			
Ser Group	Online or not: All	<ul> <li>In Black</li> </ul>	list or not: All	- Accura	ite Search	Query Reset	Advanced Sear	ch Query users o	ffline for a long time		
Blacklist											
Self-Registration	Add De	elete Modif	íy All De	elete All				Import Users	Import Network Bin	ding Information Export All Re	esults
MAC Terminal	Add to Blacklis	t Issue Messag	e or Patch Sus	spend Resume		Customize User Field	Is SIM Card Manag	ement Customize	Query List User I	formation Self-Service Mainter	<u>iance</u>
💃 External Identity Center	Totally 6 Record	s   Each Page 20	Records   Page 1	/ totally 1 Pa	ges   GO					A D	
Authentication Settings	<u>Alli None</u>	<u>User Name</u> 🔻	<u>Full Name</u> 🔻	User Group 🔻	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	<u>User Type</u> 🔻	Operation	
Client Control		123	123	Guest User Group	Delete Account when Expire	2015-11-13 17:35:48	0	<u>1 Online Users</u>	Guest User	View   Modify   Mobile Term	inal
		Herry	Herry	Default User Group	Never		0	Offline	Common User	View   Modify   Mobile Term	inal
		Jay	Jay	Default User Grou	Never		0	Offline	Common User	View   Modify   Mobile Term	inal
	8	newuser	test	new	Never		0	Offline	Common User	View   Modify   Mobile Term	inal
System Maintenance	8	test	111	Default User Grou	Never		0	Offline	Common User	View I Modify I Mobile Term	inal
RG-SMP Securi	Image: RG-SMP Security Management Platform - Windows Internet Explorer         Image: http://172.18.7.55:8080/smp/siminfoservlet?kind=query							x			
Authentication & Authority > User > SIM Card Management > Query SIM Card											
Telephone Number: Query Reset											
Add Import Delete Close											
No matching SIM card information is found.											

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



	Aanagement Platform - Windows Internet Explorer	×
🖉 http://172.18.7.55	8080/smp/siminfoservlet	
Authentication 8	Authority > User > SIM Card Management > Add SIM Card	
SIM Card Inform	nation	
* Telephone Number:		
* IMSI Number:		
IP Address:		
	Add Reset Return	

3) Click Add to complete addition.

# Importing the SIM Card Information

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

🥖 RG-SMP Security Management Platform - Windows Internet Explorer	- • 💌
http://172.18.7.55:8080/smp/siminfoservlet	
Authentication & Authority > User > SIM Card Management > Import SIM Card	
Import SIM Card	
Importing File (*.xls):	浏览
Import	
🙀 Tips:	
The number of SIM cards cannot exceed 10,000.	
Only EXCEL files in the specified format can be imported. Please click 🖄 here to download an import template.	

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

# **Deleting the SIM Information**

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



🟉 RG-SMP Securi	ty Management Platform - Wind	dows Internet Explorer		- (	• <b>×</b>			
🕖 http://172.18.7	http://172.18.7.55:8080/smp/siminfoservlet?kind=query							
Authenticatio	n & Authority > User > SIM Car	d Management > Query SIM Card						
Telephone Nun	nber: IMSI Numb	er: Query	Reset					
Add	mport Delete Close	•			<b>*</b> 2			
Totally 2 Recor	rds   Each Page 20 Records	Page 1 / totally 1 Pages   G0	US, S		N			
<u>All   None</u>	Telephone Number 🔻	IMSI Number 💙	IP Address <b>\</b>	-				
	15159556	15151254548456	172.18.7.156	5				
	15159555	15151254548562	172.18.85.60	)				
Totally 2 Recor	rds   Each Page 20 Records	Page 1 / totally 1 Pages   G0	K <					

2) Click **OK** to delete the selected SIM cards.

# **Binding the SIM Card Information**

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

IP RG-SMP Security Man	Redback      Redback	nline Service 🤤 Technical Forum 👍 About Technical Support Hotline: (+86)4008-111-000
Administrator [admin] Login IP [172.18.7.19] Login Date [2015-1	11 🔊 http://172.18.7.55:8080/smp/useraccessinfoservlet?kind=addPage&popUpWindow=true&doAfterCloseWindow=opener.onUpc	Status 🔓 Change Password 🕠 Logout
Authentication & Authonity	Authentication & Authority > User > User Status > Network Binding Info > Add Network Binding List     Access Mode     Virred Access     Wireless Access	
Image: Self-Registration         Image: Self-Registration           Image: Self-Registration         Image: Self-Registration	Network Binding Info           HD Serial Number:           user IP:           Query Idle IP Addresses           User MAC:	
External Identity Center     Customize User Fields     No custom user field is fo     El Portal Settings     Detail Information	M/SI Number: 15151254548451 Select an Idle SIM Card     NAS IP:     NAS Port:	
Gender:     ID Type:     Educational Background     Mobile Number:     Centrol	Add Close	
Postal Code: Network Binding List No network binding inform	♀. ati	

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



IP RG-SMP	Security Management Platform   Professional	🖸 Feedback 💲 Online Service 🗢 Technical Forum 🕧 About Technical Support Hotline: (+86)4008-111-000							
Administrator [admin] Login IP [1]	72.18.7.19] Login Date [2015-11-11 17:09:25]	🐼 Online User 🧶 System Status 🛛 🔒 Change Password 🛛 🕠 Logout							
Authentication & Authority 🔻	Authentication & Authority > User Group > Modify User Group								
<ul> <li>♣ Online User</li> <li>▲ User</li> <li>▲ User Group</li> <li>▲ Device</li> </ul>	User Group Name: new Access Control Behavior Restrict Access Rules								
🚼 Blacklist	Enable Wired Access	Enable Wireless Access							
Self-Registration	Network Information Verification 🗐 All	Network Information Verification 🔲 All							
Mobile Terminal	HD Serial Number Verification	HD Serial Number Verification							
C User Group Device Device E Blacklist Self-Registration Mobile Terminal E McC Terminal E McC Terminal E Leternal Identity Center D Authentication Settings D Portal Settings D Detal Settings D	IP Type Authentication  Static Dynamic	IP Type Authentication   Static  Dynamic							
External Identity Center	Ilser IP Verification	User IP Verification							
		User MAC Verification							
Authentication Settings	Viser MAC venication	V User IMSI							
Bulletin Information	NAS Det Verification	SSID Venfication							
Client Control	① Tios:								
	1. Wireless SSID names are separated by commas (), e.g., web-wireless-SSID.								
	2. The MAC address verification and the IMSI number/mobile phone number verification cannot be	2. The MAC address verification and the IMSI number/mobile phone number verification cannot be enabled at the same time.							
	3. When the network information auto-learning and the network information verification are enabled	I, you can bind users to networks. Or the system will bind users to networks through network							
	information auto-learning in the next authentication.								
Sustem Maintananaa	4. When the network information verification is enabled, the client must upload network information	n and the uploaded network information must be consistent with that in the user information.							
Log Audit	Otherwise, authentication may be failed.	ate de net unlead hard diek eend number and ID address ture							

## **VPN Access**

### **Function Description**

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

#### **Configuration Tips**

N/A

**Configuration Steps** 

# Adding a NAS

See section 2.1.1.3.1 "Adding a NAS".

# Adding a User

See section 2.1.1.3.2 "Adding a User".

# **Enabling VPN Access**

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



PRG-SMP Security Management Platform Professional Professional Technical Support Hotime: (+85)4088-111-00						
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-11 17:09:25]		🖾 Online User 🚨 System Status	🔒 Change Password		
Authentication & Authority 👻	<ul> <li>Authentication &amp; Authority &gt; User Group</li> </ul>	> Query User Groups				
Second Continue User	User Group Name:	Query Reset				
Device	Add Delete					
Self-Registration	Totally 3 Records   Each Page 20 Rec	ords   Page 1 / totally 1 Pages   G0		IQ Q		
Mobile Terminal						
📇 MAC Terminal	AllNone	<u>User Group Name</u> 💙	O	peration		
		new	View Modify			
5 External Identity Center		Guest User Group	View   Modify   Restore	Default Settings		
		Default User Group	View   Modify   Restore	Default Settings		
Authentication Settings						
E Portal Settings	Totally 3 Records   Each Page 20 Rec	ords   Page 1 / totally 1 Pages   G0		IQ Q		
Client Control						

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

IP RG-SMP S	ecurity Management Platform Professional		Feedback 💈 Online Se	vice 🔍 Technical Forun	1 🔔 About
Administrator (admin) Legin IP (172	18.7.1911 Jorin Data (2016 11.11.17:09:26)		Conline Lleer 🧖 Svetem Status	Change Receiverd	
Authentication & Authonty * © Online User User User Group © Blacklat © Self-Registration Mobile Terminal MAC Terminal	In Strain Cognitibility (Strain 11 11 10 2 25)     Strain 11 11 11 10 2 25)     Strain 11 11 11 10 2 25)     Strain 11 11 11 11 11 11 11 11 11 11 11 11 11	Soft the system will bind users to networks through network mation must be consistent with that in the user information.			
External Identity Center     Authentication Settings     Dertal Settings     Bulletin Information     Client Control	Other Settings           Image: Setting Seting Setting Setting Setting Setting Setting Settin	rmation	maa ana i dudisaa yyo.		
System Maintenance	Tipe: If the user is online, the modifications to user group information will take effect in the next authenticat     Modify     Rev	tion. eset Return			

# **Network Access Prohibited Period**

#### **Function Description**

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

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

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

### **Configuration Tips**

N/A



### **Configuration Steps**

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



2) Click Add or Modify to save the settings.

#### **Terminal Authentication**

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





# **Mobile Terminal Management**

#### **Function Description**

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

#### **Configuration Tips**

N/A

**Configuration Steps** 

# **Adding Mobile Terminals**

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



IP RG-SMP S	Security Managemen	t Platform Professional	⊠ Feedback 💈 Online Sen Technic	vice 🗢 Technical Forur al Support Hotline: (+86)	n 🚹 About 4008-111-000
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-11 17:09:25]		⊠Online User 🚨 System Status	Change Password	C Logout
Authentication & Authority 👻	Authentication & Authority > User Group > C	uery User Groups			
Se Online User	User Group Name:	Query Reset			
📥 Device	Add Delete				
Self-Registration	Totally 2 Records   Each Page 20 Records	Page 1 / totally 1 Pages   G0		R A	
Mobile Terminal	AllINone	User Group Name 🔻	Operat	tion	
		Guest User Group	View   Modify   Restore Default	Settings	
Sector External Identity Center		Default User Group	View Modify Restore Default	Settings	
Authentication Settings	Totally 2 Records   Each Page 20 Records	Page 1 / totally 1 Pages   60		P PJ	
Client Control					

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

<b>IP RG-SMP :</b>						
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-11 17:09:25]					
Authentication & Authority 👻	Authentication & Authority > User Group > Modify User Group					
<ul> <li>Online User</li> <li>User</li> <li>User Group</li> <li>Device</li> </ul>	User Group Name: Default User Group           Access Control         Behavior Restrict         Access Rules					
🚰 Blacklist	Multi-Access Limit					
Self-Registration Mobile Terminal MAC Terminal	An account can be used on a maximum of 2 terminals at the same time (Default: 1)     ☑ An account can register2 mobile terminals (Default: 1)     ☑ A mobile terminal will be deravistered if it does not no online in consecutive 90 days (Default: 90)					
External Identity Center	Tip: A registered mobile terminal can access a wireless SSID without providing the user name and password.					
E Portal Settings	Disabled					
Client Control	<ul> <li>Daily Timer</li> <li>Total Timer</li> <li>Single Timer</li> </ul>					
	<ol> <li>Tips:</li> <li>Daily Timer: When the daily timer ends, users will be forced offline on that day and recover online chance next day.</li> <li>Total Timer: The total timer starts when enabled. When the total timer ends, accounts will be suspended or cancelled.</li> <li>Single Timer: When the single timer ends, users will be forced offline or accounts will be suspended.</li> </ol>					
	Time management of messages displayed on clients					
System Maintenance 🔻	A message displayed on a client automatically close in 5 seconds (Time range: 5-300)					

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



<b>IP RG-SMP</b>	Security Management Platform Professional	☑ Feedback Soline Service □ Technical Forum A About Technical Support Hotline: (+86)4008-111-000
Administrator [admin] Login IP [1]	2.18.7.19] Login Date [2015-11-11 17:09:25]	🖾 Online User 🦲 System Status 🔒 Change Password 🛛 🕠 Logout
Authentication & Authority 👻	Authentication & Authority > Mobile Terminal > Query Mobile Terminal	
Contine User User User User User Group Device ReadBacklist	User: MAC Address: Online Status: All	
Self-Registration	Add Import Delete Delete All	
Mobile Terminal	Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60	
Eutomal Identity Center	All   None User  MAC Address  Kegistration Date  Authentication	on Time Authentication IP Nas IP <u>Online Status</u> Operation
	test 848e0cbc111b 2015-11-11 17:33:43 2015-11-11 1	18:28:17 10.1.1.105 10.1.1.28 Offline View
Authentication Settings	Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60	
Bulletin Information		
Client Control		
System Maintenance		
Log Audit	( )	•

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

IP RG-SMP	Security Ma	nagement l	Platform Professional	
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015	5-11-11 17:09:25]		
Authentication & Authority 🔻	Authentication & Auth	ority > Mobile Terminal > A	Add	
Solution Online User	Mobile Terminal Info	ormation		
& User Group	* MAC Address:		(Format: 00D0F8000001)	
Levice	* User:		Select	
😪 Blacklist	* OS Type:	Android	•	
Self-Registration Content of the	Remarks:			
External Identity Center			Add Reset Return	
Authentication Settings				
Portal Settings				
4 Bulletin Information				
Client Control				

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



IP RG-SMP	Security I	Manage	ment Pl	atform	Profession	al		⊠ Feedba	ck 💲 Online Ser Technic	vice 🙄 Technical Forur al Support Hotline: (+86)	n <u> A</u> bou 1008-111-00
Administrator [admin] Login IP [1	72.18.7.19] Login Dat	e (2015-11-11 17:0	9:25]					🐼 Online User 🧯	System Status	🔓 Change Password	<b>O</b> Logou
Authentication & Authority 👻	<ul> <li>Authentication</li> </ul>	& Authority > Use	r > Query Users								
Solutione User User User Group	User Name: tes Online or not: A	st Full N	ame:	User Group:	User T	ype: All	User Status     Advanced Search	All  Query users offi	ne for a long time		
Self-Registration Mobile Terminal	Add D Add to Blacklis	elete Mo	dify All	Delete All	me <u>Cu</u> s	stomize User Fields	SIM Card Managem	Import Users In ent Customize Q	port Network Bindi uery List User Info	ng Information Export Al	<u>I Results</u> ntenance
External Identity Center	Totally 1 Record	ds   Each Page 20	Records   Page	e 1 / totally 1	Pages   GO						> >
Authentication Settings	All None	<u>User Name</u> 🔻	<u>Full Name</u> 💙	User Group 🔻	Type of Account Validity Period	Expiry Date	Number of Blacklisted Users	Online Info	User Type 🔻	Operation	
		test	111	Default User Group	Never Expire		0	Offline	Common User	View Modify Mobile	<u>Ferminal</u>
Client Control	Totally 1 Record	ds   Each Page 20	Records   Page	e 1 / totally 1	Pages   GO						> >

#### 6) Click Add.

C http://172.18.7.5	http://172.18.7.55:8080/smp/mobileterminalservlet?kind=listByUser&userIndex=10001										
Authentication & Authority > Mobile Terminal > Query Mobile Terminal											
Manage (1) mob	ile terminals of us	ser (test)									
All None		MAC Address	Registration Date		Authentication IP	Online Status	Operation				
	test	848e0cbc111b	2015-11-11 17:33:43	2015-11-11 18:28:17	10.1.1.105	Offline	View				

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

🔏 RG-SMP Security Manag	ement Platform - Windows Internet Explorer	- • •						
e http://172.18.7.55:8080/	'smp/mobileterminalservlet							
Authentication & Authority > Mobile Terminal > Add								
Mobile Terminal Info	rmation							
* MAC Address:	(Format: 00D0F8000001)							
* User:	test							
* OS Type:	Android 🔹							
Remarks:								
	Add Reset Close							

# **Importing Mobile Terminals**

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



IP RG-SMP	ecurity Management Platform	essional	Feedbac	k 💈 Online Serv Technic	rice 🔍 Technical For al Support Hotline: (+8)	um 🔔 Abou 6)4008-111-00
Administrator [admin] Login IP [1	.18.7.19] Login Date [2015-11-11 17:09:25]		🔀 Online User 🦉	System Status	Change Password	C Cogou
Authentication & Authority 👻	Authentication & Authority > Mobile Terminal > Query Mobile Terminal					
<ul> <li>➢ Online User</li> <li>➢ User</li> <li>➢ User Group</li> <li>丞 Device</li> <li>※ Blacklist</li> <li>Q: Self-Registration</li> </ul>	User: MAC Address: Online Status: All Registration Date: to Query Reset Add Import Delete Delete All					
Mobile Terminal	Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages	G0			N Q	
	All   None User  MAC Address  Registration	Date  Authentication Time	Authentication IP	Nas IP	Online Status 🔻	Operation
The External Identity Center	test 848e0cbc111b 2015-11-11 1	2015-11-11 18:28:17	10.1.1.105	10.1.1.28	Offline	View
Authentication Settings	Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages	G0			10 Q	

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

IP RG-SMP S	Security Management Platform Professional	Feedback Soline Ser Technic	rice 🙄 Technical Forum 🕧 About al Support Hotline: (+86)4008-111-000
Administrator [admin] Login IP [17	2.18.7.19] Login Date [2015-11-11 17:09:25]	🖾 Online User 🚨 System Status	Change Password OLogout
Authentication & Authority 💌	Authentication & Authority > Mobile Terminal > Import		
<ul> <li>♀ Online User</li> <li>♀ User</li> <li>♀ User Group</li> <li>▲ Device</li> <li>♀ Blacklist</li> </ul>	Upload Import File Importing File (*.xls): Return		浏览
Self-Registration Mobile Terminal MAC Terminal Sector Terminal Sector Terminal Sector Terminal Sector Terminal	Trps:     The mobile terminals cannot exceed 10,000.     Only EXCEL files based on template format can be imported. Click there to download the Import Template.     S. If the required information is not included in the Import Template, users can create a new file based on the template.		

# **Deleting Mobile Terminals**

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

IP RG-SMP	Security M	anagem	ent Platfo	orm Profession	al	⊠ Feedba	k 🔓 Online Serv Technic	ice 🙄 Technical Foru al Support Hotline: (+86)	m 🔔 About 4008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2	015-11-11 17:09:2	5]			🖾 Online User 🦉	System Status	🔓 Change Password	O Logout
Authentication & Authority 🔻	Authentication & A	uthority > Mobile T	erminal > Query Mobil	e Terminal					
<ul> <li>➢ Online User</li> <li>➢ User</li> <li>➢ User Group</li> <li>ঐ Device</li> <li>➢ Blacklist</li> <li>☑ Self-Registration</li> <li>➢ Mobile Terminal</li> </ul>	User: Registration Date: AddImport	MAC Address:	Select Ti Delete All	nline Status: All Query Reset	2				
MAC Terminal	Totally 2 Records   E	ach Page 20 R	lecords   Page 1 /	totally 1 Pages   G0				D4 4	
	All   None	<u>User</u> 🔻	MAC Address 🔻	Registration Date 🕶	Authentication Time	Authentication IP	Nas IP	<u>Online Status</u> ▼ 0	peration
External Identity Center		test	001122221122	2015-11-12 10:13:26				Offline	View
Authentication Settings		test	848e0cbc111b	2015-11-11 17:33:43	2015-11-11 18:28:17	10.1.1.105	10.1.1.28	Offline	View
E Portal Settings	Totally 2 Records   E	ach Page 20 R	lecords   Page 1 /	totally 1 Pages   G0				R 0	

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



IP RG-SMP	Security M	anagem	ent Platfo	orm Professiona	Û	🖂 Feedba	ck 💈 Online Sen Technic	vice 🙂 Technical For al Support Hotline: (+8	um 🔔 Abo 6)4008-111-00
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2	015-11-11 17:09:2	5]			⊠Online User 🦨	System Status	Change Password	i 📿 Logou
Authentication & Authority 👻	Authentication & A	uthority > Mobile 1	ferminal > Query Mobile	e Terminal					
Contine User User User User Subser Group Continue Self-Registration Mobile Terminal	User: Registration Date: AddImport	MAC Address:	O Delete All	nline Status: All				D DI	
MAC Terminal	Totally 2 Necolda   E	aciiri age 20	acorda (1 age /	totally 11 ages 1 to					
External Identity Center	All None	User V	MAC Address	Registration Date  2015-11-12 10:13:26	Authentication Time	Authentication IP	Nas IP	Online Status V	Uperation View
Authentication Settings		test	848e0cbc111b	2015-11-11 17:33:43	2015-11-11 18:28:17	10.1.1.105	10.1.1.28	Offline	View
E Portal Settings	Totally 2 Records   E	ach Page 20 F	ecords   Page 1 /	totally 1 Pages   G0				IQ Q	

# **MAC Terminal**

### **Function Description**

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

### **Configuration Tips**

N/A

### **Configuration Steps**

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

IP RG-SMP	Security Management Platform Professional	Feedback 💈 Online Sen Technic	vice 🙄 Technical Forum 👍 About al Support Hotline: (+86)4008-111-000
Administrator [admin] Login IP [17	2.18.7.19] Login Date [2015-11-11 17.09:25]	🖾 Online User 🚨 System Status	Change Password 🛛 Change Dassword
Authentication & Authority 👻	Authentication & Authority > MAC Terminal > Query MAC Terminal		
Conline User	Terminal MAC: NAS IP:		
Levice	Connection Status: All   Blacklisted or not: All   Query Reset		
Blacklist	Add Delete Add to Blacklist		MAC Terminal Configuration
Mobile Terminal	No matching record is found.		
Authentication Settings			
Client Control			

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



IP RG-SMP	Security Management F	Platform Professional	⊠ Feed	back
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-11 17:09:25]		i Conline User	🔔 Sy:
Authentication & Authority 🔻	Authentication & Authority > MAC Terminal > Action Authority >	dd MAC Terminal		
<ul> <li>Online User</li> <li>User</li> <li>User Group</li> <li>Device</li> <li>Blacklist</li> <li>Self-Registration</li> <li>Mobile Terminal</li> <li>MAC Terminal</li> <li>External Identity Center</li> <li>Authentication Settings</li> <li>Portal Settings</li> </ul>	MAC Terminal Information  • Terminal MAC: Switch to the target VLAN after Authentication: Terminal Description:	(Format: 00D0F8000001)		
Sulletin Information				

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

# **Authentication Settings**

### **Function Description**

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

### **Configuration Tips**

N/A

### **Configuration Steps**

# **Configuring Authentication Parameters**

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



IP RG-SMP S	Security Managem	ent Platfor	m Profession	nal			Feedback 💈 Online Serv Technic	ice 🙄 Technical Forum al Support Hotline: (+86)4	About 008-111-000
Administrator (admin) Login IP (17	2.18.7.19] Login Date [2015-11-12 14:23:41	]					nline User 🚨 System Status	🔓 Change Password	
Authentication & Authority *	Authentication & Authority > Authentic	ation Settings							
Soline User	Authentication Parameters								
A User Group	* Authentication Port:	1812	(Default: 1812)		* Accounting Port:	1813	(Default: 1813)		
📥 Device	Record Update Flow:								
🚰 Blacklist	Enable Nick Name Authentication:	PT							
Self-Registration	When account logins exceed the limit	deal as follows: The new	v client will not be able to	o authenticate.		•			
Mobile Terminal	Preferred Wireless Authentication: Pl	EAP_EAP_GTC -							
📇 MAC Terminal	Click here to import the wireless authority	ntication server certificate							
🕵 External Identity Center	Tip: The Authentication Port cannot	be the same as the Accou	inting Port.						
Authentiantian Cattings	Periodic Online Status Detection								
Partal Settings	Periodic Online Status Detection:	<b>V</b>							
	* User Online Heartbeat Period:	5	minutes (Default: 5	i)					
Bulletin Information     Client Control	<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>Offline and clear the user accordingly.</li> </ol>	in is enabled, please enab in is enabled and the syst	ole non-Ruijie client accor tem do not receive the Us	unting and set the accoun ser Online Heartbeat Notifi	ting period to the User Online cation within three consecution	Heartbeat Period. Ve User Online Hear	tbeat Periods, the system will as	sume that this user has g	jone
	Password Anti Brute Force Protect	ion							
	Enable Password Anti Brute Ford	e Protection							
	When the times of keying an incorrect	password exceeds 5	times, within 6	hours, the user accoun	t will be frozen.				

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

	RG-SMP	Security Management Platform   Professional	Feedback 🗧 C	Dnline Service 🗢 Technical Foru Technical Support Hotline: (+86	im 🔔 A )4008-111
Carlos A Automatication Parameters  Conserved  Conserved Con	strator [admin] Login IP [1	172.18.7.19] Login Date [2015-11-12 14:23:41]	Monline User 🚨 System	n Status 🔒 Change Password	ĢL
in class is	ntication & Authority 🔻	Authentication & Authority > Authentication Settings			
Image: State Stat	line User	Authantication Daramatare			
Percent part of congeneration of the series as the Accounting Part (b)	er	* Automatication in a damatica Det	4042 (D-6-	H: 4042)	
is in the second logic second is list, data is allow: The verified will not be able to authenticate:       Image: Second logic second is list, data is allow: The verified will not be able to authenticate:         is its minute       Image: Second logic se	er Group	Autoentication Port. (Default: ToT2) Accounting Port.	1615 (Detaul	it. 1013)	
State       Evaluation         Beginstration       Perford         Verse accord loging in second being in the data status       In the data in the d	ice	Record Update Flow:			
Rightanding       When account logins exceed the lum, deal as falous: The three cleff will not be able to authenticute.       •         Prefered Winess Authenticution: FPC-R2-PG-CFC       •         Dick logins to most the same as the Accounting Pixt.       •         Prefered Winess Status Direction:       •         ************************************	klist	Enable Nick Name Authentication:			
Be Terminal Be Te	-Registration	When account logins exceed the limit, deal as follows: The new client will not be able to authenticate.	•		
C initial C ini	ile Terminal	Preferred Wireless Authentication: PEAP_EAP_GTC +			
and Merthy Certer   Image: Status Detection	C Terminal	Click here to import the wireless authentication server certificate.			
Periodic Colline Status Detection Perio	mal Identity Center	① Tip: The Authentication Port cannot be the same as the Accounting Port.			
National Status Periodic Online Status Detection:   I User Online Status Detection:   I Orga   I User Online Status Detection:   I Orga   I Orga <td>antication Sattinge</td> <td>Periodic Online Status Detection</td> <td></td> <td></td> <td></td>	antication Sattinge	Periodic Online Status Detection			
User Online Heatbeat Period: <ul> <li></li></ul>	al Settings	Periodic Online Status Detection:			
the hefemation it Control it Con	ar ootaniyo	* User Online Heartbeat Period: 5 minutes (Default: 5)			
	tin Information	() Tine:			
2. When Periodic Online Status Detection is enabled and the system do not receive the User Online Heatbeat Netification within three consecutive User Online Heatbeat Periods, the system will assume that this user has gone differe and clear the user accordingly. Password Anti Brute Force Protection  Carbon Brock Protection  The the times of keying an incorrect password exceeds is times, within is hours, the user account will be force. Centrol Anti Brute Force Protection  Carbon Brock Control Force Protection  The the times of keying an incorrect password exceeds is times, within is hours, the user account will be force. Centrol Anti Brute Force Protection  Centrol Antion Brute Protection Receives and the system Status Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication & Authority > Online User > Outer Control Force Protection  Centrol Adventication  Centro	t Control	1. When Periodic Online Status Detection is enabled, please enable non-Ruijie client accounting and set the accounting period to the User Or	nline Heartbeat Period.		
offine 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.         CPC-SEME Security Management Platform       Professional         Tardy Latencial Souther		2. When Periodic Online Status Detection is enabled and the system do not receive the User Online Heartbeat Notification within three conser	cutive User Online Heartbeat Periods, the syst	tem will assume that this user has	gone
Password Anti Brute Force Protection Charles Dassword Anti Brute Processora Charles Dassword Anti Brute Dassword Anti Charles Dassword Anti Brute Dassword Anti Brute Dassword Anti Charles Dassword Anti Brute Dassword Anti Brute Dassword Anti Charles Dassword Anti Brute Dassword Anti Brute Dassword Anti Charles Dassword Anti Brute Dassword Anti Brute Dassword Anti Charles Dassword Anti Brute Processora Charles Dassword Anti Brute Dassword Anti Brute Dassword Anti Brute Dassword Anti Brute Dassword Anti Charles Dassword Anti Brute Processora Charles Dassword Anti Brute Dassword Dassword Anti Brute Dassword Anti B		offline and clear the user accordingly.			
Pessword Anti Brute Force Protection  Password Anti Brute Force Protection  Password Anti Brute Force Protection  When the times of Keying an incorrect password exceeds is times, within in hours, the user account will be frozen.  Proceeding and the force of the for					
Enable Password Arti Brute Force Protection When the times of Keying an incorrect password exceeds intens, within incorrect password exceeds intens within incorrect password exceeds intens within incorrect password exceeds in the pass intens in the pass intens in the pass intens inten		Password Anti Brute Force Protection			
When the times of keying an incorrect password exceeds in times, within in hours, the user account will be forcen.         Image: Second Seco		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.			
atal genuing Ugin ( Tri ( Tri ( US))     atal genuing Ugin ( Tri ( US)) <th>RG-SMP</th> <th>Security Management Platform Professional</th> <th>☑ Feedback S in the second second</th> <th>Online Service 🙄 Technical Fon Technical Support Hotline: (+86</th> <th>um 🔔 5)4008-11</th>	RG-SMP	Security Management Platform Professional	☑ Feedback S in the second	Online Service 🙄 Technical Fon Technical Support Hotline: (+86	um 🔔 5)4008-11
Clear Residual Users Force Offine     Registration     Dia remnal     Clear Residual Users   Force Offine     Registration     Dia remnal     Clear Residual Users   Force Offine     Registration     Dia remnal     Clear Residual Users   Force Offine     Result     Lister Pare     User Rame:     Full Records   Each Page 20     Records   Page 1 / totally 1 Pages        User Rame:        Clear Residual Users              Clear Residual Users  Clear Residual Users   <	trator (admin) Login IP (	172.10.7.19 Login Date [2015-11-12 14:23:41]	Syster	n Status 🔲 Change Password	- 50
ne User Name: Full Name: User Group: r Group ice Schist Registration ble Terminal C T	tication & Authority	Authentication & Authority > Online User > Query Online Users			
Coop       User Name:       Coler Name: <t< td=""><td>ne User</td><td>Liner Manner</td><td></td><td></td><td></td></t<>	ne User	Liner Manner			
Cloudy       User IP:       NAS IP:          Accurate Search         Query Reset         Advanced Search         Cuery         Reset         Advanced	r	oser droup.			
Celar Residual Users       Force Offline       Reauthenticate       Issue Message or Patch       Add to Blacklist       Send online/offline notifications to a third-party system       Customize Outer VL         Registration       Re Fernial       Totally 1 Records   Each Page 20, Records   Page 1, / totally 1 Pages   60       Id < Dot	r Group	User IP: NAS IP: Accurate Search Query Reset Advanced S	Search		
Clear Residual Users       Force Offline       Reauthenticate       Issue Message or Patch       Add to Blacklist       Send online/offline notifications to a third-party system       Cutary Lig       Output       Uit       Output	-kliet				
Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   c0     Id < Dot	Registration	Clear Residual Users Force Offline Reauthenticate Issue Message or Patch Add to Blacklist	Send online/offline notifications to	a third-party system Customize	Query L
Terminal Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   0   Totally 1 Records   Each Page 20 Recor	ile Terminal				
All Hone     User Name ▼     Nock Name ▼     User Type ▼     User U *     NAS.IP ▼     Online Time ▼     Upstream Traffic     Downstream Traffic     Operation       and identity Center     big     Thirdparty User     10.1.1.05     10.1.1.28     0.12.34     72.16KB     20.02KB     View       enriciation Settings al Settings     Totally 1 Records   Each Page 20     Records   Page 1 / / totally 1 Pages   co     Image: Setting 2     Image: Settin	CTerminal	Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   G0		0	
enal Identity Center enal Identity Center big Thirdparty User 10.1.1.105 10.1.1.28 0.12.34		All I None User Name Y Nick Name Y User Type Y User IP Y NAS IP Y	Online Time 🔽 🛛 Unstream Traffic	Downstream Traffic	pration.
Importivity Settings     Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60     IVEN     IVEN       elin Information nt Control     III. Readthenticate is available only for Ruije authentication clients and Ruije security agents.     IVEN     IVEN     IVEN	ernal Identity Center	Interview         Oser rype         Oser rype         Oser rype           Image: Third and the second	0-12-34 72 46VP	20.02KB	nation
al Settings al Settings totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60 IV C Dil etin Information t Control II . Reauthenticate is available only for Ruije authentication clients and Ruije security agents.		E 101 1100 1011120	0.12.04 F2.10KD	20.0210	
all Settings       Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60       Id < Dil	hentication Settings				
etin Information et Control  1. Resultenticate is available only for Ruije authentication clients and Ruije security agents.	tal Settings	Totally 1 Records   Each Page 20 Records   Page 1 / totally 1 Pages   60			
ent manufacture nt Control 1. Reauthenticate is available only for Ruijie authentication clients and Ruijie security agents.	atin Information				
In Common 1. Reauthenticate is available only for Ruijie authentication clients and Ruijie security agents.					
	eun mormación	C Tips			

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



ing-simp.	security Mailage	ment Plat	TOTTTT Protessional			Technic	al Support Hotline: (+86):	4008-111-000
Administrator (admin) Login IP [1	72.18.7.19] Login Date [2015-11-12 14:	23:41]			2 Onlin	e User 🐣 System Status	🔓 Change Password	O Logout
Authentication & Authority 👗	Authentication & Authority > Aut	nentication Settings						
Second Se	Authentication Parameters							
B User Group	* Authentication Port:	1812	(Default: 1812)	* Accounting Port:	1813	(Default: 1813)		
La Device	Record Update Flow:	V						
🚼 Blacklist	Enable Nick Name Authenticatio	n: 🔍						
😨 Self-Registration	When account logins exceed the	limit, deal as follows:	The new client will not be able to authenticate.		•			
Mobile Terminal	Preferred Wireless Authentication	PEAP_EAP_GTC	•					
📇 MAC Terminal	Click here to import the wireless	authentication server ce	ertificate.					
Sternal Identity Center	Tip: The Authentication Port ca	mot be the same as the	e Accounting Port.					
Antherstine Cettines	Periodic Online Status Detect	on						
Dortal Settinge	Periodic Online Status Detection	<b>V</b>						
	* User Online Heartbeat Period:	5	minutes (Default: 5)					
Bulletin Information	(1) Tips:							
Olient Control	1. When Periodic Online Status De	tection is enabled, plea	se enable non-Ruijie client accounting and set th	e accounting period to the User Onlin	e Heartbeat Period.			
	2 Million Derindia Online Status De	ention in anablad and t	the sustain do not receive the Lleer Online Hearth	ant Matification within three concernt	us Lloss Online Hearthe	Deriodo, the sustem will av	eumo that this usor has	2000

ninistrator (admin) Login IP (1	9] Login Date [2015-11-12 14:23:41] 😥 🔂 Change Password 🖓
thentication & Authority 👻	thentication & Authority > Online User > Query Online Users
Online User	Name: Full Name: User Group:
b User Group g Device g Blacklist g Self-Registration	IP: NAS IP: Accurate Search Query Reset Advanced Search Residual Users Force Offine Reauthenticate Issue Message or Patch Add to Blacklist Search
user Group g Device Blacklist Self-Registration Mobile Terminal MAC Terminal	IP:       NAS IP: <ul> <li>Accurate Search</li> <li>Query</li> <li>Residual Users</li> <li>Force Offline</li> <li>Reauthenticate</li> <li>Issue Message or Patch</li> <li>Add to Blacklist</li> <li>Send online/offline notifications to a third-party system</li> <li>Query</li> <li>Add to Blacklist</li> <li>Send online/offline notifications to a third-party system</li> <li>Query</li> <li>Ially 1 Records   Each Page 20</li> <li>Records   Each Page 20</li> <li>Record</li></ul>
User Group gDevice eBlacklist StelfRegistration Mobile Terminal MAC Terminal	IP:       NAS IP: <ul> <li>Accurate Search</li> <li>Query</li> <li>Residual Users</li> <li>Force Offline</li> <li>Reauthenticate</li> <li>Issue Message or Patch</li> <li>Add to Blacklist</li> <li>Send online/offline notifications to a third-party system</li> <li>Customize Query</li> <li>Ially 1 Records   Each Page 20</li> <li>Recidual Users</li> <li>Veck Hams V</li> <li>User Type V</li> <li>User IV: Veck Hams V</li> <li>Veck Hams V</li> <li>User Type V</li> <li>User IV: Veck Hams Veck Hams V</li></ul>

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

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

IP RG-SMP	Security Managen	nent Platf	Orm Professional			Feedback 💈 Online Serv Technic	ice 🗢 Technical Forun al Support Hotline: (+86)4	About 008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-12 14:23:4	11]				🐼 Online User 🚨 System Status	🔓 Change Password	O Logout
Authentication & Authority *	Authentication & Authority > Authen	tication Settings						<u>^</u>
Solution Online User	Authentication Parameters							
B User Group	* Authentication Port:	1812	(Default: 1812)	* Accounting Port:	1813	(Default: 1813)		
La Device	Record Update Flow:	<b>V</b>						
🚼 Blacklist	Enable Nick Name Authentication:	7						
Self-Registration	When account logins exceed the lim	it, deal as follows: Th	e new client will not be able to authenticate	6	•			E
Mobile Terminal	Preferred Wireless Authentication:	PEAP_EAP_GTC -						
📇 MAC Terminal	Click here to import the wireless aut	nentication server certi	ficate.					
External Identity Center	Tip: The Authentication Port cannot	t be the same as the A	Accounting Port.					
Authentication Sattings	Periodic Online Status Detection							
Portal Settings	Periodic Online Status Detection:	V						
	* User Online Heartbeat Period:	5	minutes (Default: 5)					
Bulletin Information     O     Client Control	Tips:     When Periodic Online Status Detect     When Periodic Online Status Detect     when Periodic Online Status Detect     offline and clear the user accordingly.	tion is enabled, please tion is enabled and the	enable non-Ruijie client accounting and se system do not receive the User Online He	t the accounting period to the User Online I artbeat Notification within three consecutive	Heartbeat Pe User Online	riod. Heartbeat Periods, the system will as	sume that this user has g	one

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



IP RG-SMP	Security N	☑ Feedback 💈 Online Service 🤤 Technical Forum 🔔 Abo Technical Support Hotline: (+86)4008-111-0							
Administrator [admin] Login IP [1	72.18.7.19] Login Date	[2015-11-12 14:23:41]					🖾 Online User 🚨 System Status	Change Password	C Logou
Authentication & Authority   System Maintenance	Log Audit > Auth	entication Failure Logs > 0	Query Logs						
Log Audit	User Name:	Authen	tication Date: 2015-11-12	- 2015-11-12 🛅					
Log Configuration	User IP:	Cause	of Failure:		Query Reset A	dvanced Search			
Network Access Logs	Delete	Delete All							
🛱 System Logs	Totally 18 Records	I Each Page 20 Recor	ds   Page 1 / totally 1 Pages	60				K 0 D	D)
	All[None	User Name 🔻	Authentication Date	NAS IP	User IP	User MAC	Cause of Failure	Operation	
		<u>Herry</u>	2015-11-12 15:45:42	<u>10.1.1.28</u>	10.1.1.116	DCC7937A73A8	The number of PCs allowed to be logged simultaneously by the same account has reached the upper limit specified by the administrator.	s <u>View</u>	

Administrator (admin) Login IP (17	2.18.7.19] Login Date [2015-11-12 14:23:41]	🐼 Online User 🚨 System Status	Change Password	C Logou
Authentication & Authority 👻	Authentication & Authority > Authentication Settings			
Conline User User User Group Device Backlist CSelf-Registration	Authentication Parameters         * Authentication Port:       1512         * Authentication Port:       1812         Record Update Flow:       Image: Constraint of the second transformer of the	(Default: 1813)		
Mobile Terminal	Preferred Wireless Authentication: PEAP_GIC  Click here to import the wireless authentication server certificate			
External Identity Center	<ul> <li>Tip: The Authentication Port cannot be the same as the Accounting Port.</li> </ul>			
Authentication Settings	Periodic Online Status Detection Periodic Online Status Detection: V User Online Hantsher Period for the status Detection for the status Periodic Status Detection (Status Detection)			

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

IP RG-SMP	Security N	<b>Aanagem</b>	ent Platfor	m   Profe	ssional		M Fee	edback 💈 Online Service 😅 Technical Supp	Technical Forum ( ort Hotline: (+86)4008	About
Administrator [admin] Login IP [1	72.18.7.19] Login Date	[2015-11-12 14:23:4	1]				Monline Use	er 🦲 System Status 🛛 🔒 Ch	ange Password 🛛 🤇	Logout
Authentication & Authority 🕨	Log Audit > Net	work Access Logs >	Query Logs							*
System Maintenance 🔹										
Log Audit 👻	User Name:		User IP:			Offline Cause: All		-		
Log Configuration	Login Time: 2	016 11 12 🥅 0	0 0 Locout T	imo: 2016.1	1 12 3 23 69 69	Quant				
Authentication Failure Logs	Login rime. 2	013-11-12	c jo cogouri	2013-1	25,05,05	Query Reset	Advanced Search			
Wetwork Access Logs										
Operation Logs	Delete	Export Query	Results Delete A	All				Network Traffic and	Online Duration Repo	भू
System Logs	Totally 16 Record	s I Each Page 20	Records   Page 1 / to	otally 1 Pages I G	0					0
up Oser Operation Logs										
	All None	<u>User Name</u> 🔻	User IP	Full Name	NAS IP	Login Time 🌱	Logout Time 🚩	Offline Cause 🔻	Operation	=
		Herry	10.1.1.105	Herry	10.1.1.28	2015-11-12 15:32:59	2015-11-12 15:46:57	The number of online users have exceeded the limit of termina using the same account.	ls <u>View</u>	

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

IP RG-SMP S	ecurity Management Platform   Professional	⊠ Feedback 💈 Online Serv Technic	ice 🗢 Technical Forum al Support Hotline: (+86)4	About 008-111-000
Administrator [admin] Login IP [172	. 18.7.19] Login Date [2015-11-12 14:23:41]	🖾 Online User 🚨 System Status	🔓 Change Password	C Logout
Authentication & Authority 👻	Authentication & Authority > Authentication Settings			^
Second Contine User	Authentication Parameters			
🔏 User Group	* 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, deal as follows: When the new client authenticates, the previous authenticated user will be forced to go offline.			E
Mobile Terminal	Preferred Wireless Authentication: PEAP_EAP_GTC 👻			
📇 MAC Terminal	Click here to import the wireless au PEAP FAP MD5 ificate.			
External Identity Center	Tip: The Authentication Port cannet the time same as the Accounting Port.			
Authoritication Sottings	Periodic Online Status Detection			
Portal Settings	Periodic Online Status Detection:			
	User Online Heartbeat Period: 5     minutes (Default: 5)			

Innovation Beyond Networks



# **Enabling Periodic Online Status Detection**

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

AP RG-SMP	Security Management Platform   Professional	🖂 Feedback 💲 Online Service 🤤 Technical Forum 🧃 Technical Support Hotline: (+86)4008-	About -111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date (2015-11-12 14:23:41)	⊠Online User 🦲 System Status 🔒 Change Password 🕠	Logout
Authentication & Authority 👻	Authentication & Authority > Authentication Settings		-
Se Online User User Belleer Group	Authentication Parameters           * Authentication Port:         1812         (Default: 1812)         * Accounting Port:         1813	3 (Default: 1813)	
Device	Record Update Flow.		
Self-Registration Content of the	When account logins exceed the limit, deal as follows: When the new client authenticates, the previous authenticated user will be forced to go offline.  Preferred Wireless Authentication:  PERPERPENDING OF CONTRACT,		н
External Identity Center	Other milling         or import use interest administration reverse counciliate.           O         Tip: The Authentication Port cannot be the same as the Accounting Port.		
Authentication Settings	Periodic Online Status Detection Periodic Online Status Detection ' User Online Heartbeat Period: 5 minutes (Default: 5)		
Bulletin Information     Client Control	Tips:     Tips:     Tips:     Vhen Pariodic Online Status Detection is enabled, please enable non-Ruije client accounting and set the accounting period to the User Online Heartbeat     Vhen Pariodic Online Status Detection is enabled and the system do not receive the User Online Heartbeat Notification within three consecutive User Onlin     offline and clear the user accordingly.	Period. Ine Heartbeat Periods, the system will assume that this user has gone	

# **Enabling PEAP Authentication for Windows Client**

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

IP RG-SMP S	Security Manageme	nt Platform Professional	☑ Feedback S Online Service □ Technical Forum A Abo Technical Support Hotline: (+86)4008-111-00			
Administrator [admin] Login IP [17]	2.18.7.19] Login Date [2015-11-12 14:23:41]		⊠ Online User 🚨 System Status	🔓 Change Password	C Logout	
Admentationa (selaming cogning) cogning (selamin	Chailer Password Anti Brack Password Anti Brack Force     When the times of kaying an incorrect p     Translee PEAP Authentication for     Auto-connect to SSID:     WiFI Encryption Type:     Second Stage of PEAP Authentication:     Click hars to download WFI Helper:     Translematic to a control ownload and or     Account Expiration Warning:	Protection ssword exceeds interes, within in hours, the user account will be finzen. Windows Client PEAP MSCHAP  PEAP_MSCHAP  istribute the WFI helper to Windows users.				
Bulletin Information     Otient Control	SMS Account Expiration Warning: Email Account Expiration Warning: * Sending Account Expiration Warning 7 Every giad of the sense of the sense of the sense Every 24 hours to send Email/SM (1) Tips: Enabling SMS/Email Account Ex- Expiration Warning will be re-sent.	days before. (Default: 7; Range: 1 to 30)     octock to send Email/SMS account expiration warning     account expiration warning (Default: 24, Range: 1 to 360)     xiration Warning allows the system to hourly check the online status within the configured period and sends the v     Modify Reset	varning messages if necessary. In every v	varning period, the Accourt	ŧ	

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



IP RG-SMP	Security Managemer	nt Platform	Professional	🖸 Feedback 🍃 Online Service 🤝 Technical Forum 🕧 Abou Technical Support Hotline: (+86)4008-111-000
Administrator (admin) Login IP (1	172.18.7.19] Login Date [2015-12-23 16:45:48]			🖄 Online User 🚨 System Status 🔓 Change Password 🛛 🕠 Logou
Authentication & Authority 👻	Periodic Online Status Detection			
Se Online User	Periodic Online Status Detection:	<b>V</b>	0% of nosenseauthenserviet from 1/2.18.34.16 Completed E 2	3
Subser	* User Online Heartbeat Period:	5	File Download - Security Warning	
😕 User Group	(1) Tine:		Do your much to not account this file?	
📥 Device	1. When Periodic Online Status Detection is	enabled, please enable no	to you want to run or save this file?	eartbeat Period.
🕵 Blacklist	2. When Periodic Online Status Detection is	enabled and the system d	Name: wifi_helper.exe	Jser Online Heartbeat Periods, the system will assume that this user has gone offline and clear
Self-Registration	the user accordingly.		Type: Application	
Mobile Terminal			From: 172.18.34.16	
📇 MAC Terminal	Password Anti Brute Force Protection		Run Save Cancel	
📕 External Identity Center	Enable Password Anti Brute Force Pro When the times of keying an incorrect pas	otection ssword exceeds 5 tir	While files from the internet can be useful this file tune can	
Authentication Settings	Enable DEAD Authontication for Win	down Cliont	I when the norm the incenter can be determined in the type can be determined in the incenter of the source, do not the source, do not the source, do not the source of	
Portal Settings	Auto connect to SSID:	402	<ul> <li>Tun or save this solitivare. <u>What is the tipk?</u></li> </ul>	
	WELCOUNTRY TYPE:	WR42 -		
Rulletin Information	wirr Security Type.	WPA2 +		
🕜 Client Control	WIFI Encryption Type:	AES 👻		
	Second Stage of PEAP Authentication:	PEAP_MSCHAP -		
	Click here to download WIFI Helper.			
	① Tip: Administrators can download and d	istribute the WIFI helper to \	Windows users.	
	Account Expiration Warning			
	Account Expiration Warning:	V		
	SMS Account Expiration Warning:			
System Maintenance	Email Account Expiration Warning:			
Log Audit 🔸	* Sending Account Expiration Warning 7	days before (Default	7: Range: 1 to 30)	

# **Enabling Account Expiration Warning**

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

IP RG-SMP S	Security Management Platform Professional Continue Security Platform Professional Continue Security Management Platform Professional Continue Security Platform Platform Professional Continue Security Platform Platform Platform Professional Continue Security Platform	About 111-000				
Administrator [admin] Login IP [17	12.18.7.19] Login Date [2015-11-12 14.23.41] 😥 Online User 🦲 System Status 🔒 Change Password 🕠	Logout				
Authentication & Authority	Enable Password Anti Brute Force Protection     When the times of Keying an incorrect password exceeds      times, within      hours, the user account will be frozen.	*				
Sulser Group	C Enable PEAP Authentication for Windows Client					
A Device	* Auto-connect to SSID: wechat					
Se Blacklist	WIFI Security Type: WPA2 -					
Self-Registration	WIFI Encryption Type: AES -					
Mobile Terminal	Second Stage of PEAP Authentication: PEAP_MSCHAP					
📇 MAC Terminal	Click here to download WIFI Helper.					
External Identity Center	① Tip: Administrators can download and distribute the WFI helper to Windows users.					
Authentication Settings	Account Expiration Warning					
Portal Settings	Account Expiration Warning.					
Bulletin Information						
Client Control	Linner Zocken Capital Contraining. E					
	Serioung Account Expansion Hvaning (F) durys before (Denauti, F, Range, H) 3 V/	=				
	every day, at 3 ° o circick to 22 ° o circick to serial cmail/ows account expiration warning ° Every [24 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.					
	Modify Reset					

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

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



# **Portal Settings**

### **Function Description**

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

### **Configuration Tips**

N/A

## **Configuration Steps**

# **Configuring Web Authentication & Self-Service**

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

IP RG-SMP	Security Management Platform Professional	☑ Feedback 💈 Online Ser Technic	vice 🔍 Technical Forun cal Support Hotline: (+86)4	About 008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-12 14:23:41]	🖾 Online User 🚨 System Status	🔓 Change Password	O Logout
Authentication & Authority 🔻	Authentication & Authority > Portal Settings			^
Contine User User User User Set Group Set Device Set D	Tips     For common user authentication, configure the HTTP redirection page http://172.18.7.55.80/smp/commonauth.or HTTPS redirection page https://172.18.7.55.80/smp/guestauth.or HTTPS redirection page https://172	.7.55:443/smp/commonauth 443/smp/guestauth		
Mobile Terminal	HTTP Port: 80     Default: 80)     HTTPS Port: 443     Default: 443     Default: 443     Offsult: 443     Offsult: 443			E
External Identity Center	Enable Web Authentication     Save user name and password for:     Device 4 Authentication Client at:			
Sulletin Information	☑ Automatically pop-up the URL you intent to access before login. ☑ Enable enter user name			

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

# **Enabling Web Authentication**

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



IP RG-SMP S	ecurity Management P	latform Professional	⊠ Feedback 💲 Online Ser Technic	vice 🙄 Technical Forun al Support Hotline: (+86)4	About 1008-111-000
Administrator [admin] Login IP [172	2.18.7.19] Login Date [2015-11-12 14:23:41]		⊠ Online User 🚨 System Status	Change Password	
Authentication & Authority 🔻	Web Authentication & Self-Service				^
Soline User	* HTTP Port:	80 (Default: 80)			
Super Contraction of the second secon	* HTTPS Port:	443 (Default: 443)			
Le Device	Itp: You can access the Self-Service platform through	ugh http://172.18.7.55:80/smp/selfservice.			
Blacklist	Enable Web Authentication				
Self-Registration	* Save user name and password for:	15 days (Default: 15)			
AC Terminal	Download Web Authentication Client at:				
External Identity Center     Authentication Settings     Dortal Settings     Bulletin Information     Client Control	Automatically pop-up the URL you intent Enable enter user name Bulletin Board Information:	o access before login.			E
System Maintenance 🔹	① Tip: After Web authentication is enabled, users ca	in be authenticated through the browser.			

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

# **Enabling Authentication-Exemption Rule for Web Users**

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

IP RG-SMP S	Security Management P	latform   Profe	ssional	🖂 Feed	lback 💲 Online Sen Technic	ice 🙄 Technical Forum al Support Hotline: (+86)400
Administrator [admin] Login IP [17]	2.18.7.19] Login Date [2015-11-12 14:23:41]			Monline User	System Status	Change Password
Authentication & Authority 🔻	I Tip: You can access the Self-Service platform through	ough http://172.18.7.55:80/smp/	selfservice.			
Second Se	Enable Web Authentication					
ዶ User Group	Enable Authentication-Exemption Rule for	r Web Users				
Levice	* Authentication-Exemption User Group:	new	Q Select User Group			
Blacklist	Bulletin Board Title:	Disclaimer				
Self-Registration     Mobile Terminal     MAC Terminal     External Identity Center     Authentication Settings     Bolletin Information	* Bulletin Board Information:	free				
	<ul> <li>Login Button Title:</li> </ul>	Access				
	<ul> <li>Authentication Success Message:</li> </ul>	Authentication is successf	ul. You can now access the network.			
Sustan Majatanaco 🔹	Tips:     After Authentication-Exemption rule is enabled, ut     Configure the redirection URL for authentication e     HTTP Address.http://172.18.7.55.80/smp/freeauthe     HTTPS Address.https://172.18.7.55.43/smp/freeauthe     HTTPS Address.https://172.18.7.55.43/smp/freeauthe	sers only need to read and agre xempted users. enservlet uthenservlet	e with the information on the bulletin board to access the Internet.			

# **Enabling Guest Registration**

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



IP RG-SMP S	Security Management Platform	N Professional ∑ Feedback	8 Online Servic Technical	ce 🖃 Technical Forun I Support Hotline: (+86)4	n 🔔 About 1008-111-000
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-12 14:23:41]	🐼 Online User	System Status	Change Password	C Logout
Authentication & Authority *	Enable Guest Registration				
Se Online User	* Guest Validity Period: 1 Day(s) 0 - Hour(s) 0	<ul> <li>Minute(s) (Default: 1 day, range: 5 minutes to 365 days)</li> </ul>			
8 User					
8 User Group					
La Device					
Sa Blacklist					
Self-Registration	Difference in the second second second				
Mobile Terminal	* Bulletin Board Information:				
and the main and t					
🚮 External Identity Center					
Authentication Settings					
E Portal Settings	Guest scan QR code to register <u>QR logo customization</u>	2			
Pullatin Information	User Group: QSelect Use	er Group			
Client Centrel	QR wizard steps: Pleass scan your QR card to finis	sh authentication!			
	QR authentication success message: Guest QR auth	entication 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. In order to conduct authentication for a			
	Message for Successful QR Code Authentication:	You have passed QR Code authentication. <td></td> <td></td> <td></td>			
System Maintenance					

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

IP RG-SMP Security Management Platform   Professional	☑ Feedback 💈 Online S Tech	ervice 😌 Technical Forun iical Support Hotline: (+86)4	n 🚹 About
Administrator [admin] Login IP [172.18.7.19] Login Date [2015-11-12 14:23:41]	🖾 Online User 🚨 System Status	🔓 Change Password	O Logout
Authentication & Authonsy            Portine User             Portine User	authentication for a utility of the second s		

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



IF RG-SMP Security Management Platform Professional			🖂 Feedback 💲 Online Service 🤝 Technical Forum 🔒 About Technical Support Hotline: (+86)4008-111-000			
Administrator [admin] Login IP [172	2.18.7.19] Login Date [2015-11-12 14:23:41]		🖾 Online User 🚨 System Status	Change Password		
Authentication & Authority	Enable Guest Registration					
Solution User	* Guest Validity Period: 1 Day(s) 0 • Hour(s) 0	<ul> <li>Minute(s) (Default: 1 day, range: 5 minutes to 365 days)</li> </ul>				
User Group     User Group     Device     Device     Self-Registration     Mobile Terminal     MAC Terminal     External Identity Center     Device     Authentication Settings	* Bulletin Board Information:					
Portal Settings	Guest scan QR code to register QR logo customization					
Rulletin Information	User Group: Default User Group	r <u>Group</u>				
Client Control	* QR wizard steps: Pleass scan your QR card to finit * QR authentication success message: Guest QR authentication	authentication!				
	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. br> In order to conduct auther	ntication for a			
Sustam Maintananaa	Message for Successful QR Code Authentication:	You have passed QR Code authentication. You can now access the network.				

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

IP RG-SMP	Security Management Plat	form Professional	🖂 Feedback 💈 Online Se Techn	rvice 🖃 Technical Forur ical Support Hotline: (+86)	n 🔔 About 4008-111-000
Administrator [admin] Login IP [1]	72.18.7.19] Login Date [2015-11-12 14:23:41]		🖾 Online User 🚨 System Status	Change Password	
Authentication & Authonsy *	Enable Guest SMS Self-Service Registration * The maximum number of Self-Service Registration Custom SMS:	on per mobile number within 24 hours (Default: 24, range: 1 to 720) is 1 v times (Defau Congratulations!	it: 1, range: 1 to 10)		
Euroria conungs     Euroria conungs     Client Control	Tips:     The Class User Self-Service Registration is enabled, us     Please configure the URI, for QR Code authentication     HTTP Address.http://172.18.7.55.80/smp/qrccdeservlet     HTTPS Address.http://172.18.7.55.80/smp/qrccdesarvlet     HTTPS Address.http://172.18.7.55.80/smp/qrccdecardservl     ITTPS Address.http://172.18.7.55.80/smp/qrccdecardservl	ers can obtain a temporary password via SMS to access the Internet. et ner Online Heartbeat Period let servlet			

# **Opening Disclaimer Page**

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



IP RG-SMP S	Security Mana	🖂 Feedback 🛛 💲 Online Ser Technic	☑ Feedback 💈 Online Service 🖘 Technical Forum 👍 Abou Technical Support Hotline: (+86)4008-111-00		
Administrator (admin) Login IP [17:	2.18.7.19] Login Date [2015-11-1	2 14:23:41]	🖾 Online User 🐣 System Status	🔓 Change Password	C Logout
Authentication & Authority *	HTTPS Address:https://172 3. Please configure the URL f HTTP Address:http://172.10 HTTPS Address:https://172	18.7.55.443/smp/grcodesen/et or QR Code card authenticationer Online Heartbeat Period 7.55.80/smp/grcode-ardsen/et 18.7.55.431/smp/grcode-ardsen/et			-
🕹 Oser Group 🍰 Device	Open Disclaimer Pag				
Self-Registration Suble Terminal Mobile Terminal Mobile Terminal Sublemation Sublemation Sublemation Sublemation Sublemation Client Control	Disclaimer title:     Disclaimer contents:	Osclaimer this is disclaimer page (Support upto 8000 characters input)			
	* Agree button title:	Agree			
System Maintenance	Tip:Authentication continue     Heartbeat Detection of	es only after the disclaimer is agreed In Web-authenticated Users Modify Reset			

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

# **Configuring Heartbeat Detection on Web-authenticated Users**

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

IP RG-SMP S	Security Manag		☑ Feedback Source Control Forum A About Technical Support Hotline: (+86)4008-111-000
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-12	14:23:41]	🖾 Online User 🦲 System Status 🔒 Change Password 🛛 🕠 Logout
Authentication & Authority  Coline User User User Gue Duser Group Eve Blacklist Mobile Terminal Mobile Terminal	* Disclaimer contents:	this is disclaimer page	
External Identity Center Authentication Settings	* Agree button title:      Tip:Authentication continues	(Support upto 8000 characters input) Agree only after the disclaimer is agreed	
Eulletin Information	<ul> <li>Heartbeat Detection or</li> <li>Detection Interval:</li> <li>Tips:</li> <li>The page to be displayed aft</li> <li>After this configuration is enicycle expires.</li> <li>This configuration is effective</li> </ul>	Web-authenticated Users	alidated user status (online or offine). entication. Otherwise, the users will be forced to go offine when the 3rd heartbeat onfigure to remain alive by traffic.
System Maintenance 🔹		Modify Reset	

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

## **Bulletin Information**

#### **Function Description**

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

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



# **Configuration Tips**

N/A

# **Configuration Steps**

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

IP RG-SMP	Security Mana	igement Platfo	rm Professional	edback 💈 Online Se Technic	rvice 🖤 Technical Forur al Support Hotline: (+86)40	m <u> A</u> bout 008-111-000
Administrator [admin] Login IP [1	72.24.0.55] Login Date [2015-1	1-13 11:45:41]	🖾 Online Use	er 🚨 System Status	🔒 Change Password	O Logout
Authentication & Authority 🔻	<ul> <li>Authentication &amp; Authority</li> </ul>	> Bulletin Information				
Solution Continue User	Bulletin Information					
& User Group		Authentication success.				
Blacklist						
Self-Registration	Bulletin Information:					
Mobile Terminal						
💃 External Identity Center	Bulletin Information URL:	http://www.ruijienetworks.com/			Verify	
Authentication Settings	Warning:	V				
Portal Settings	<ol> <li>Tips:</li> <li>After the Bulletin Inform</li> </ol>	ation URL is configured, the Bulleti	in page will be opened automatically	after every authenticat	ion.	
Bulletin Information     Client Control	2. The Bulletin Information 3. Enabling Account Expire	n URL supports only HTTP and HT ation Warning allows the system to	TPS formats. ) send warning messages to users (	three days before acco	unt expiration.	
			Modify Reset			
System Maintenance 🔹						

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

### **Terminal Authentication**

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





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



Note

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



User Name[testuser] Log	in Time[2015-11-10 15:59	9:21]			<b>O</b> Logo
My self-service	My self-service > My Inf	ormation			
My Information	Basic Information				
🐈 Change Password	User Name:	testuser	Full Name:	add	
Password Protection	Expiration Type:	Never Expire	User Status:	Normal	
	Creation Date:	2015-11-10 11:43:15	Time of Last Access:	2015-11-10 15:56:40	



Note

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

Administrator [admin] Login IP	[172.18.7.19] Login Date [2015-11-10 11:20:52]	M.On	line User 🕌 System Status	Change Password
Authentication & Authority	Custom SMS:			
Solution User				
Cuser Generation				
Device				
Blacklist				
Self-Registration				
Mobile Terminal	① Tips:			
MAC Terminal	1. After Guest User Self-Service Registration is enabl	ed, users can obtain a temporary pass	word via SMS to access the In	itemet.
	2. Please configure the URL for QR Code authenticat	on		
External Identity Center	HTTPS Address:http://172.18.7.55:80/smp/grcodeset	viet		
	3 Please configure the URL for OR Code card auther	nticationer Online Heartbeat Period		
Authentication Settings	HTTP Address:http://172.18.7.55:80/smp/grcodecar	dservlet		
a Fontar Seturigs	HTTPS Address:https://172.18.7.55:443/smp/qrcod	ecardservlet		
Illetin Information				
Client Control	Open Disclaimer Page		_	
	Heartbeat Detection on Web-authenticated Us	ers		
	* Detection Interval: 5	minutes (Default 5)		
	Tips:			
	1. The page to be displayed after wired Web authention	ation communicates with the server at	regular intervals and informs	the server about the valid
	user status (online or offline).			
	2. After this configuration is enabled, please inform the	e users of wired Web authentication no	ot to close the page displayed	after successful authentic
	Otherwise, the users will be forced to go offline when 2. This configuration is offective for wired Web author	ine 3rd neartbeat cycle expires. tication only Wireless Web authenticat	ion will be alive throughout th	o interfaco. Pleaco config
	remain alive by traffic.	acaton only. Thereas treb addrenaea	and will be alloc alloughout an	e interface. I reade conligu
System Maintenance 🔹 🕨		Modify Reset		
Log Audit				

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

# **Client Anti-Crack**

Note

## **Function Description**

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



### **Configuration Tips**

N/A

## **Configuration Steps**

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

IP RG-SMP	Security Management Platform Professional	🖂 Feedback 🧧 Online Ser Technic	vice 🖃 Technical Forun al Support Hotline: (+86):	h About
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-12 14:23:41]	🖾 Online User 🚨 System Status	Change Password	☐ Logout
Authentication & Authority 👻	Authentication & Authority > Client Control			
Se Online User User Suser Group	Client Anti-Crack Client Distribution			
Device Backlist Self-Registration	No Arti-Crack file exists in the system. <u>Add Anti-Crack File</u> Enable File Version Client Information Operation			
Mobile Terminal	Add the user who uses the cracked client to the blacklist. When the times of using the cracked client exceeds 3 , within hours, the client will be frozen.			
External Identity Center	Add the user whose cracking behavior is detected to the blacklist When the number of cracking behaviors exceeds 3, within hours, the client will be frozen.			
Portal Settings	Prohibit the client from sending spooling packets.  Prohibit the client from sending the ARP spooling packets.			
Sulletin Information	Prohibit the client from sending the DHCP spoofing packets.  Filter illegal IP packets (Only the packets carrying the authenticated IP address and MAC address can be sent by the client PC.)			
	Client Packet Number Detection  Client Packet Number Detection When the number of packets sert by client within 10 seconds exceeds 20000, the system will take the following actions.			
	Actions:       Send a warning to the user      Force the user to go offline     Warning:			
System Maintenance				

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

CRG-SMP Security Management Platform - Windows Internet Explorer					
http://172.18.7.55:8080/smp/clientcontrolservlet?kind=toClientAntiCrackFileUploadPage					
Authentication & Authority > Client Control > Add Anti-Crack File					
Upload the version file					
* Version File:	浏览				
Upload the Anti-Crack file					
* Anti-Crack APP file:	浏览				
* Anti-Crack DLL file:	浏览				
* Anti-Crack DLL file: ② Tips: Find the version file in the release package. (The version file information is recorded in the clientversioninfo.xml). Upload Close					

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



IP RG-SMP Security Management Platform   Professional Control (1894)				
Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-12 14:23:41]	🖾 Online User 🚨 System Status	Generation Change Password	C Logout
Authentication & Authority 👻	Authentication & Authority > Client Control			^
Se Online User User User Group	Client Anti-Crack Client Distribution			
📥 Device 🕵 Blacklist 😢 Self-Registration	No Anti-Grack file exists in the system. <u>Add Anti-Crack File</u> Enable File Version Client Information Operation			
Mobile Terminal	Add the user who uses the cracked client to the blacklist.           When the times of using the cracked client exceeds 3         within 4         hours, the client will be fozen.			
Sternal Identity Center	Add the user whose cracking behavior is detected to the blacklist When the number of cracking behaviors exceeds 3, within 4, hours, the client will be frozen.			E
Authentication Settings	Prohibit the client from sending spoofing packets.			
Sulletin Information	Irrolmat the client from serioning the Aver spooting packets.     Prohibit the client from senting the DHCP spoofing packets.     Filter Blegal IP packets (Only the packets carrying the authenticated IP address and MAC address can be sent by the client PC.)			
	Client Packet Number Detection			
	Enable Client Packet Mumber Detection When the number of packets sent by client within 10 seconds exceeds 20000, the system will take the following actions. Actions:     Send a warning to the user      Force the user to go offline Warning:			
System Maintenance  Log Audit	· · · · · · · · · · · · · · · · · · ·			

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

P RG-SMP	P Security Management Platform Professional Confine Service Configuration Half			n 🔔 Abou 4008-111-00
fministrator [admin] Login IP [1	72.18.7.19[Login Date [2015-11-12 14.23.41]	i⊠Online User≜System Status	Change Password	C Logou
Authentication & Authonity Online User User User Group	Client Anti-Crack Client Distribution Client Anti-Crack No Anti-Crack Rie exists in the system. Add Anti-Crack File			
Blacklist Self-Registration Mobile Terminal MAC Terminal	Enable         File Version         Client information         Operation           Image: Add the user who uses the cracked client to the blacklist.         When the times of using the cracked client exceeds 3 , within 4 , hours, the client will be frozen.           Image: Add the user whose cracking behavior is detected to the blacklist.         When the times of using the cracking behavior is detected to the blacklist.			
Authentication Settings	Prohibit the client from sending beckets.     Prohibit the client from sending the ARP spoofing packets.     Prohibit the client from sending the DHCP spoofing packets.     Prohibit the client from sending the DHCP spoofing packets.			
Client Control	Filter liegal (P packets (Only the packets carrying the authenticated IP address and MAC address can be sent by the client PC.)     Cillent Packet Number Detection     Enable Client Packet Number Detection     When the number of packets sent by client within [10] seconds exceeds [20000], the system will take the following actions.			
	Actions:  Send a warning to the user  Force the user to go offline Warning:			
/stem Maintenance	Modify			

# **System Maintenance**

# **SMS Settings**

# **Function Description**

This section describes how to configure the SMS service.

# **Configuration Tips**

N/A



### **Configuration Steps**

# **Configuring the SMS Modem**

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

IP RG-SMP S	ecurity Management Platform Professional	☑ Feedback 💈 Online Service 🤤 Technical Forum и About Technical Support Hotline: (+86)4008-111-000		
Administrator [admin] Login IP [172	2.18.7.19] Login Date [2015-11-12 14:23:41]	⊠Online User 🚨 System Status	Change Password	C Logout
Authentication & Authority	System Maintenance > SMS Settings			
System Maintenance	I SMS Settings			
Bettings	Enable SMS Modem     Enable SMS Gateway     Enable 3G SMS Gateway			
Email Service Settings				
Custom Manager Page	* Port (serial port): COM1 * Baud Rate: 9600			
Database Maintenance	* Data Bit: 8 🗸			
	* SIM Card PIN Code: 1234			
	* Manufacture Model: Default Model -			
	0 Tips 1. 1. Port (serial port), the name of the SMS modern port that connected with the server. 1. Dot (serial port), the name of the SMS modern port that connected with the server.			
	2. Baud Rate: the same as that of the SMS modem.			
	3. SIM Card PIN Code: SIM Card PIN Code of the SMS modem, (default PIN code of China Mobil is 1234, default PIM code of China Unicom is 0000).			
	<ol><li>Vendor Model: Vendor Model of the SMS modem. Select 'Default Model' if there is no other option in the list.</li></ol>			
	Modify Reset Send a Test Message			
Log Audit				

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

🔗 RG-SMP Security Management Platform - Windows Internet Explorer 📃 📼 🔤
http://172.18.7.55:8080/smp/smsservlet?kind=toSendPage
System Maintenance > Send a Test Message
Send a Test Message
* Mobile Number:
③ Tips:The system will send a test message to your designated telephone number. The expenses is charged by ISP.
Send a Test Message Close

# **Configuring the SMS Gateway**

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



IP RG-SMP S	Security Mana	gement Platf	Orm Professional	🖂 Feedback 💲 Online Ser Technic	rice 🙄 Technical Forun al Support Hotline: (+86)4	n 🚹 About 008-111-000
Administrator [admin] Login IP [17	2.18.7.19] Login Date [2015-11-1	2 14:23:41]		🖾 Online User 🔎 System Status	Change Password	
Authentication & Authority	System Maintenance > SM	IS Settings				
System Maintenance	SMS Settings					
Basic Configuration	Enable SMS Modem	Enable SMS Gateway	Enable 3G SMS Gateway			
Email Service Settings		,	,			
	* IP:	127.0.0.1				
Custom Manager Page	* Port:	5005				
🚮 Database Maintenance	* User Name:	admin				
	* Password:	•••••				
	Tips     ID: ID: address of the SMS I	Web envire interfere				
	2. Port: the port name of the c	corresponding SMS Web Servic	interface.			
	3. Username: username of the	e corresponding SMS Web Ser	ce interface.			
	4. Password: password of the	corresponding SMS Webservio	interface.			
			Modify Reset Send a T	est Message		
Les Auto						

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

EG-SMP Security Management Platform - Windows Internet Explorer		x
http://172.18.7.55:8080/smp/smsservlet?kind=toSendPage		
System Maintenance > Send a Test Message		
Send a Test Message		
* Mobile Number:		
Ips:The system will send a test message to your designated telephone number. The expenses is charged by	y ISP.	
Send a Test Message Close		

# **Email Service Settings**

#### **Function Description**

This section describes how to configure the Email service.

## **Configuration Tips**

N/A

## **Configuration Steps**

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



IP RG-SMP S	Security Management Platform	Professional	☑ Feedback 💈 Online Ser Technic	vice 🗢 Technical Forun al Support Hotline: (+86)4	1 About
Administrator [admin] Login IP [17	2.18.7.19] Login Date [2015-11-12 14:23:41]		🐼 Online User 🕭 System Status	Change Password	
Authentication & Authority 🕨	System Maintenance > Email Service Settings				
System Maintenance	Email Service Settings				
BASS Settings	C Enable Email Service				
Email Service Settings	* Email Server:	smtp.163.com (for example: mail.ruijie.com.cn)			
	* Email Server Port:	25 (default: 25)			
式 Custom Manager Page	Whether to adopt identity authentication for the email server:	(the ticked box indicates to adopt identity authentication, and the empty	ty box indicates not to adopt identity authent	ication)	
Batabasa Maintanansa	* Sender Email Address:	suautotest@163.com			
Database Maintenance	* Sender Email Password:	•••••			
		Modify Reset Send a Test Email			
Log Audit 🔹 🕨					

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

🟉 RG-SMP Security Management Platform - Windows Internet Explorer	
http://172.18.7.55:8080/smp/mailservlet?kind=toSendPage	
<ul> <li>System Maintenance &gt; Send a Test Email</li> </ul>	
Send a Test Email	
* Receiver Email Address:	
Tips:The system will sent a test email to your designated email box to check whether the email service co correct.	nfiguration is
Send a Test Email Close	
Correct.	niigurauon 15

### **Custom Manager Page**

#### **Function Description**

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

## **Configuration Tips**

N/A



## **Configuration Steps**

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

IP RG-SMP	Security Management Platform Professional	☑ Feedback S Online Service □ Technical Forum A About Technical Support Hotline: (+86)4008-111-000			
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-12.14:23:41]	⊠ Online User 🚨 System Status	🔒 Change Password	C Logout	
Authentication & Authority +	System Maintenance > Custom Manager Page				
System Maintenance	Custom Manager Page				
SMS Settings	⑦ Default Style				
Email Service Settings	The LOGO picture and title of the manager adopt the default style.				
Custom Manager Dave	Custom Style.				
	The LOGO picture and title of the manager adopt the custom style.				
🕵 Database Maintenance	(i) Tips: 1. If you want to download picture templates, please click $\overset{\bullet}{\simeq}$ here to download.				
Log Audit	Next				

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

IP RG-SMP	Security Management Platform Professional Technical Support Hotline: (+86)4008-111-00	ut O				
Administrator [admin] Login IP [1	72.24.0.55] Login Date [2015-11-13 11:45:41] 🔯 Online User 🧶 System Status 🔓 Change Password 🕠 Logo	Jt				
Authentication & Authority 🔸	System Maintenance > Custom Manager Page					
System Maintenance	Custom Manager Page					
📝 SMS Settings	◎ Default Style					
Exemail Service Settings The LOGO picture and title of the manager adopt the default style.						
🗟 Custom Manager Page	Custom Style. The LOGO picture and title of the manager adopt the custom style.					
式 Database Maintenance	① Tips : 1. If you want to download picture templates, please click 💁 <u>here t</u> o <mark>Jownload.</mark>					
	Next Reset					
Log Audit						

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



IP RG-SMP Security Management Platform Professional Cetaback Source Cetaback Cetabac								
Administrator (admin) Login IP (17	72.18.7.19] Login Date [2015-12-23 16:45:48]				🖾 Online User 🐣 System Status	Change Passy	word OL	ogout
Authentication & Authority > System Maintenance >	Custom Login Page							
Basic Configuration	* Login Page Picture:	E:\PIC\PC.jpg					Browse	
🛃 SMS Settings	Background Picture of the Login Page:	#05057D					prowse	
Custom Manager Page	Background Color of Login Page. I Tips. The size of upload picture cannot Upload	process 78	Message from webpage	of the background picture dimensions must	be 1280*1024.			
			OK Cancel					

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

IP RG-SMP Security Mana	☑ Feedback 💈 Online Service 🤤 Technical Forum 🔔 About Technical Support Hotline: (+86)4008-111-000			
Administrator [admin] Login IP [172.18.7.19] Login Date [2015-11-1	2 14:23:41]	😥 Online User 🐣 System Status 🔒 Change Password 🛛 🕠 Logout		
Authentication & Authority				
Basic Configuration     Settings     Email Service Settings				
Custom Manager Page				
Database Maintenance				
	User Name: Password:			
	Pler	ase use IE6.0 or above version.		
Re-In	port	Next		
Log Audit				

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

IF RG-SMP Security Management Platform Professional				🖂 Feedback 💈 Online Sen Technic	Feedback Soline Service Technical Forum A About Technical Support Hotline: (+86)4008-111-000			
Administrator (admin) Login IP [17	2.18.7.19] Login Date [2015-11-12 14:23:41]			🖾 Online User 🐣 System Status	G Change Password	O Logout		
Authentication & Authonty  System Maintenance  Basic Configuration  SMS Settings  Famil Service Settings	Custom Title Picture  * Title Picture: Background Picture of Title:  ① The size of upload picture cannot exceent	s 1MB. The dimensions of the title picture must be	1000°59. The dimensions of the title background pic	ture must be 6°59.		浏览 浏览		
Custom Manager Page	Custom Content <sup>6</sup> Custom Title: <sup>6</sup> Content of the "About" session: Upload							
Log Audit								

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


### RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

IP RG-SMP	Security Management Platform   Profess	onal	C Feedback 💲 Online Serv Technic	rice 🗢 Technical Foru al Support Hotline: (+86)	m 🦲 About 4008-111-000
Administrator [admin] Login IP [1	72.18.7.19] Login Date [2015-11-12 14:23:41]		Online User 🧢 System Status	Change Password	CLogout
Authentication & Authority	O Preview			-	
System Maintenance					
SMS Settings	RG-SMP test				
Email Service Settings					
Curtom Manager Page			Feedback 😗 Online Service	e (1)About	
		Message from webpage			
B Database Maintenance					
		this is test for custom @2015			
		OK			
	Re-Import			Finish	
Lon Audit					
Log Audit					
Log Addit					
	Security Management Diatform		🕑 Feedback 💈 Online Servi	ce 😇 Technical Forum	About
NP RG-SMP	Security Management Platform	onal	🗹 Feedback 💈 Online Servi Technica	ce 🗢 Technical Forum I Support Hotline: (+86)4	About 008-111-000
Administrator (admin) Login IP [1	Security Management Platform Professi	onal	∑ Feedback 💲 Online Servi Technica ISOnline User 🙆 System Status	ce 😇 Technical Forum I Support Hotline: (+86)4 🔒 Change Password	About 008-111-000
Administrator [admin] Login IP [1 Authentication & Authonty + System Maintenance	Security Management Platform Professi 72 187 19] Login Date (2015-11-12 14 23 41) • System Maintenance > Custom Manager Page	anal	Feedback Sonline Servi Technica 愛Online User 会System Status	ce 🗢 Technical Forum I Support Hotline: (+86)4	About 008-111-000
Administrator [admin] Login IP [1 Authentication & Authonty + System Manenance	Security Management Platform Professi 172 18.7.19] Logn Date [2015-11-12 14-23.41] • System Maintenance > Custom Manager Page Custom Manager Page	onal	∑ Feedback 🔹 Online Seni Technica ⊠Online User 🐣 System Status	ce 🗢 Technical Forum I Support Hotline: (+86)4 Change Password	About 008-111-000
Administrator (admin) Login P (1 Authentication & Authenty + System Mantenance Basic Configuration SMS Settings	Security Management Platform Professi 72 18.7.19] Logn Date [2015-11-12 14-23.41] System Maintenance > Custom Manager Page Custom Manager Page Default Style	onal	⊡ Feedback 🔹 Online Servi Technica i⊠Online User 🐣 System Status	Ce 🗢 Technical Forum I Support Hotline: (+86)4	About 008-111-000 Cogout
Administrator (admin) Login IP (1 Authentication & Authenty > System Mantenance Static Configuration >> SMS Settings Email Senice Settings	Security Management Platform Professi 72 187.19 Logn Date [2015-11-12 14-23.41] System Maintenance - Custom Manager Page Custom Manager Page Default Style The LOGO picture and title of the manager adopt the default style.	onal	⊡ Feedback 💲 Online Servi Technica iti©Online User 🐣 System Status	ce     ⊃ Technical Forum I Support Hotime: (+86)4	About 008-111-000
Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 Authentication & Authonty + System Mandenance Sessic Configuration Sessic Settings Email Senice Settings Custom Manager Page	Security Management Platform Professi 72 18 7.19] Logn Date [2015-11-12 14 23 41] System Maintenance > Custom Manager Page Custom Manager Page Default Style The LOGO picture and bile of the manager adopt the default style. Custom Style.	onal	⊡ Feedback 💲 Online Servi Technica ionline User 🐣 System Status	ce 🗢 Technical Forur I Support Hotline: (+86)4 A Change Password	About 008-111-000 OB-000
Administrator (admin) Login IP (1 Authentication & Authonty - System Mandenance Statings SMS Settings Email Service Settings Custom Managor Page	Security Management Platform Professi 72.18.7.19] Login Date (2015-11-12 14 23 41] System Mainteance > Custom Manager Page Custom Manager Page Default Style The LOGO picture and title of the manager adopt the default style. Custom Style. The LOGO picture and title of the manager adopt the custom style.	onal	C Feedback Seni Technica ⊯≦'Online User @ System Status	ce  ☐ Technical Forum I Support Hotline: (+85)4	1 (1) About 008-111-000 (1) Logout
Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 Admentication & Authordy > system Mandenance Statis Settings Statis Settings Email Service Settings Custom Manager Page Custom Manager Page	Security Management Platform Professi 172 18.7.19 Logn Date (2015-11-12 14-23.41) System Maintenance > Custom Manager Page Custom Manager Page Custom Style The LOGO picture and title of the manager adopt the default style. Custom Style The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style.	onal	⊡ Feedback 💲 Online Servi Technica ISÖOnline User 🐣 System Status	Ce  ☐ Technical Forum I Support Hotime: (+85)4	1 (About 008-111-000 (Cogout
Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 System Mantenance System Mantenance System Settings Email Service Settings Custom Manager Page Database Maintenance	Security Management Platform Professi T2 18 7.19 Logn Date (2015-11-12 14-23-41) System Maintenance > Custom Manager Page Custom Manager Page Custom Style The LOGO picture and title of the manager adopt the default style. Custom Style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The submit of the custom custom customer adopt the custom style. The custom customer configuration has been modified. The new configuration takes effect the submit of th	onal	I Feedback Sonline Servi Technica I System Status	Ce ♥ Technical Forum I Support Hotime (+85)4	About     O08-111-000     O     Cogout
Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 System Mantenance System Mantenance System Settings Custom Manager Page Custom Manager Page	Security Management Platform Professi 72.18.7.19 Logn Date (2015-11-12 14-23-41) System Maintenance > Custom Manager Page Custom Manager Page Default Style The LOGO picture and title of the manager adopt the default style. Custom Style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and the picture uplated previously for modification, please click	onal ect after restart.	○ Feedback Sontine Servi Technica Sontine User System Status	ce <sup>©</sup> Technical Forum (Support Hotime (+86)4 A Change Password	About           008-111-000           OLegout
Administrator (admin) Login IP (1 Authentication & Authony > System Mantenance	Security Management Platform Professi 72.18.7.19 Login Date (2015-11-12 14-23.41) System Maintenance > Custom Manager Page Custom Manager Page Default Style The LOGO picture and title of the manager adopt the default atyle. Custom Style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The custom center configuration has been modified. The new configuration takes et the logo picture and title of the manager adopt the custom style. The custom center configuration has been modified. The new configuration takes et the logo picture and title of the manager adopt the custom style. The custom center configuration has been modified. The new configuration takes et the logo picture and the picture upleaded previously for modification, please click	onal tect after restart.	○ Feedback Sonline Servi Technica Sonline User System Status	ce <sup>©</sup> Technical Forum I Support Hotime (+86)4  Change Password	1 € About 008-111-000 ∩ Legout
Administrator (admin) Logia P (1 Authentication & Authenty + System Mantenance Basic Configuration SMS Settings Custom Manager Page Custom Manager Page Database Maintenance	Security Management Platform Professi 27.18.7.19 Login Date (2015-11-12 14-23.41) System Maintenance > Custom Manager Page Custom Manager Page Default Style The LOGO picture and title of the manager adopt the default style. Custom Style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The Custom center configuration has been modified. The new configuration takes et Tips: 1. If you want to download picture templates, please click <u>here</u> to download. 2. If you want to download the picture uploaded previously for modification, please click	ect after restart.	☐ Feedback Sonline Servi Technica System Status	ce <sup>□</sup> Technical Forum I Support Hotline (+85)4 Change Password	1 € About 008-111-000
Administrator (admin) Loga IP (1 Authentication & Authenty - System Mantenance Basic Configuration SMS Settings Castor Manager Page Custorn Manager Page Database Maintenance	Security Management Platform Profession 72 187.19 Logn Date (2015-11-12 14-23.41) System Maintenance - Coastom Manager Page Custom Manager Page Default Style The LOGO picture and title of the manager adopt the default style. Custom Style. The LOGO picture and title of the manager adopt the default style. Custom Style. The Custom Center configuration has been modified. The new configuration takes of Tipes: 1. Byou want to download picture templates, please click <u>here</u> to download. 2. Tyou want to download the picture uplaaded previously for modification, please click	enal ict after restart.  ict after restart.  Reset Reset	Seedback Sonine Servi Technica Monine User System Status	ce 🗢 Technical Forum I Support Hotime: (+86)4	About 008-111-000
Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 Authentication & Authenty * System Mantenance Selic Configuration % SMS Settings Email Senice Settings Custom Manager Page Custom Manager Page	Security Management Platform Professi 72 18.7.19 Logn Date [2015-11-12 14 23 41] System Manistenance > Custom Manager Page Custom Manager Page Default Style The LOGO picture and title of the manager adopt the default style. Custom Style. The LOGO picture and title of the manager adopt the custom style. Custom Style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The LOGO picture and the of the manager adopt the custom style. The Custom style adopt the c	enal  Let aller restart.  Let aller restart.  Reset	Seedback Sonline Seni Technica ∭Online User System Status	ce  Technical Forum I Support Hotime: (+85)4 Change Password	About 008-111-000
Custom Manager Page	Security Management Platform Professi 72 18 7.19 Logn Date (2015-11-12 14 23 41) System Maintenance > Custom Manager Page Custom Manager Page Default Style The LOGO picture and bile of the manager adopt the default style. Custom Style. The LOGO picture and bile of the manager adopt the custom style. Custom Style. The Custom Center configuration has been modified. The new configuration takes of O Tips: 1. Hypov want to download picture templates, please click <u>here</u> to download. 2. Hypov want to download the picture uploaded previously for modification, please click	bet after restart.	I Feedback Sontine Servi Technica ISOnline User A System Status	ce ⊃ Technical Forum I Support Hotime: (+85)4	About 008-111-000
Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 Authentication & Authonty System Mandenance Sessic Configuration Sessic Sestings Ermal Sence Settings Custom Manager Page Database Maintenance	Security Management Platform Professi 72.18.7.19 Login Date (2015-11-12 14 23 41) System Maintenance > Custom Manager Page Custom Manager Page Custom Maintenance > Custom Manager adopt the default style. The LOGO picture and title of the manager adopt the default style. Custom Style: The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The Custom Center configuration has been modified. The new configuration takes et 0 Tigs: 1 Syou want to download picture templates, please click here, to download. 2 Styou want to download the picture uploaded previously for modification, please click	bet after restart.	☐ Feedback Sontine Servi Technica ISOnline User A System Status	ce ⊃ Technical Forum I Support Hotime (+85)4	About 008-111-000
Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 Authentication & Authonty System Mandenance System Mandenance Settings Email Senice Settings Email Senice Settings Custom Manager Page	Security Management Platform Professi 72 18.7.19 Login Date (2015-11-12 14-23.41) System Maintenance > Custom Manager Page Custom Manager Page Custom Style The LOGO picture and title of the manager adopt the default style. Custom Style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The custom center configuration has been modified. The new configuration takes ef O Tops: 1. If you want to download picture implates, phase click <u>here</u> to download. 2. If you want to download the picture uploaded previously for modification, please click	ect after restart.  there to download.  Next Reset	☐ Feedback Sontine Servi Technica Monitore User  System Status	ce ♥ Technical Forum I Support Hotime (+85)4	a (), About 008-111-000 () Legout
Administrator (admin) Login IP (1 Administrator (admin) Login IP (1 Authentication & Authonty System Mandenance System Mandenance Email Senice Settings Email Senice Settings Custom Manager Page	Security Management Platform Professi 12 18 7.19 Logn Date (2015-11-12 14-23.41) System Maintennee > Custom Manager Page Custom Manager Page Custom Manager Page Custom Style The LOGO picture and title of the manager adopt the default style. Custom Style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The LOGO picture and title of the manager adopt the custom style. The custom center configuration has been modified. The new configuration takes of G Tipp: 1.1 you want to download picture templates, plass cick Anager to download. 2.1 you want to download the picture uplaaded previously for modification, please cick	onal wet after restart.    terms to download.   Next Reset	☐ Feedback Sontine Servi Technica Monime User  System Status	ce ♥ Technical Forum I Support Hotime (+85)4	a <u>)</u> About 008-111-000 Cugout

7) Restart RG-SMP to enable changes.

#### **Database Maintenance**

## **Function Description**

This section describes how to back up the database.

### **Configuration Tips**

N/A



#### **Configuration Steps**

# **Manual Backup**

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

IP RG-SMP S	Security Management Platform Professional	🖂 Feedback 💈 Online Serv Technica	ce 🗢 Technical Forum Il Support Hotline: (+86)4	008-111-000
Administrator [admin] Login IP [17	2.18.7.19] Login Date [2015-11-12 14:23:41]	🔯 Online User 🐣 System Status	Change Password	
Authentication & Authority 🕨	System Maintenance > Database Maintenance			
System Maintenance	Database Backup			
SMS Settings	* Path of the Database Backup Folder: C:\RG-SMPIDB_backup	Backup Immediately		
Custom Manager Page	Enable Database Auto-Backup     View the database auto-backup records     Removal Period for Database Auto-backup: 7 days (range: 1 - 15)			
Database Maintenance	© Tips: 1.When Database Auto-Backup is enabled, the system will automatically backup the database at 4 a.m. every day. 2 Enter the entire path for the server database backup of RG-SMP. (format: "D.RG-SMPDB_backupsmpdb_backupsmpdb_backup")			
	Save			
Log Audit				

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

IP RG-SMP Sec	Curity Management Platform Professional Technical Support Hotline: (+86)4008-111-000
Administrator [admin] Login IP [172.24.	0.55] Login Date (2015-11-13 11:45:41) 🖄 Online User 🕭 System Status 🔓 Change Password 📿 Logout
Authentication & Authority 🕨 💿 s	System Maintenance > Database Maintenance
System Maintenance	Database Backup         Path of the Database Backup         Folder:         Enable Database Auto-         Backup         View the database auto-backup records         Backup         Removal Period for         7       days (range: 1 - 15)         Tips:         When Database Auto-Backup is enabled, the system will automatically backup the database at 4 a.m. every day.         Enter the entire path for the server database backup of RG-SMP. (format "D-RG-SMPDB_backupsmpdb_backup")
Log Audit 🕨	

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

# **Automatic Backup**

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



Iministrator (admin) Login IP [1	172 18 7 191 Login Date (2015-11-12 1	RG-SMP Security Management Platfor	m - Windows Internet Explorer	0		he Liser A System Status	Change Password	
Authentication & Authority	<ul> <li>System Maintenance &gt; Databa</li> </ul>	http://172.18.7.55:8080/smp/smpdata System Maintenance > Database M	Ibasebackupservlet/kind=viewBack	Auto-Backup Records		System Status	Change r assword	(1) Logot
System Maintenance 💦 👻		• ojotoni mamonanoo · batababon						
Basic Configuration	Database Backup	Database Auto-Backup Records (	1 items)					
SMS Settings	* Path of the Database Backup	Backup File Name	Backup Time	File Size(MB)	Operation			
Email Service Settings	Enable Database Auto-Backu	SMPDB_20151112_040000.zip	2015-11-12 04:00:01	0.56	Download			
Custom Manager Page	* Removal Period for Database							
Database Maintenance	Tips: 1.When Database Auto-Backup i 2.Enter the entire path for the ser	Ups: Ine manual database backup	Will not be displayed in the list.					

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

# Log Audit

### Log Configuration

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

Administrator [admin] Login IP [17	72.18.7.19] Login Date [2015-11-12 16:29:10]
Authentication & Authority	Log Audit > Log Configuration
Log Audit	Log Configuration
Log Configuration Authentication Failure Logs Network Access Logs Operation Logs System Logs Jew User Operation Logs	<ul> <li>Automatically delete the Operation Logs generated within last * 180 days. (From 1 to 360)</li> <li>Automatically delete the System Logs generated within last * 180 days. (From 1 to 360)</li> <li>Automatically delete the User Operation Logs generated within last * 180 days. (From 1 to 360)</li> <li>Automatically delete the Authentication Failure Logs generated within last * 180 days. (From 1 to 360)</li> <li>Automatically delete the Network Access Logs generated within last * 180 days. (From 1 to 360)</li> <li>Automatically delete the Third-Party Operation Logs generated within last * 180 days. (From 1 to 360)</li> <li>Automatically delete the Third-Party Operation Logs generated within last * 180 days. (From 1 to 360)</li> </ul>

#### **Authentication Failure Logs**

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



Alexandre O. Alexandre N								
m Maintenance	Log Audit > Autr	hentication Hailure Logs > 0	Juery Logs					
Jdit 👻	Liser Name:	Author	tigation Data: 2016 11 12	2016 11 12 🚍				
Configuration	Oser Marile.	Addien	2010-11-12	2010-11-12				
hentication Failure Logs	User IP:	Cause	of Failure:		Query Reset	dvanced Search		
work Access Logs								
eration Logs	Delete	Delete All						
tem Logs								
r Operation Logs	Totally 18 Records	Each Page 20 Record	ds   Page 1 / totally 1 Pages	G0				
	AllNone	User Name 🔻	Authentication Date	NAS IP	User IP	User MAC	Cause of Failure	Operation
		Herry	2015-11-12 15:45:42	<u>10.1.1.28</u>	10.1.1.116	DCC7937A73A8	The number of PCs allowed to be logged simultaneously by the same account has reached the upper limit specified by the	View
							administrator.	
		dcc7937a73a8	2015-11-12 15:40:43	<u>10.1.1.28</u>		DCC7937A73A8	The mobile terminal has not been registered or MAC Terminal does not exist.	View
		Herry	2015-11-12 15:31:18	<u>10.1.1.28</u>	10.1.1.105	848E0CBC111B	The user is not found.	View
		hujq	2015-11-12 14:43:17	<u>10.1.1.28</u>	10.1.1.105	848e0cbc111b	The authenticator returns an authentication failure message (for unknown reason)	View
		hujq	2015-11-12 14:43:17	<u>10.1.1.28</u>	10.1.1.105	848E0CBC111B	No response from the Radius server 172.18.34.57.	View
		hujq	2015-11-12 14:43:13	<u>10.1.1.28</u>	10.1.1.105	848E0CBC111B	No response from the Radius server 172.18.34.57.	View
		98fae35aea0c	2015-11-12 14:39:39	10.1.1.28		98FAE35AEA0C	The mobile terminal has not been registered or MAC Terminal does not exist.	View
		848e0cbc111b	2015-11-12 14:26:36	10.1.1.28		848E0CBC111B	The mobile terminal has not been registered or MAC Terminal does not exist.	View

#### **Network Access Logs**

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

Administrator (admin) Login IP (1	72.18.7.19] Login Date	[2015-11-12 16:29:1	[0				🐼 Online Us	er 🦲 System Status 🛛 🔒 Chan	ge Password 🛛 🕠 l
Authentication & Authority 🕨	Log Audit > Net	work Access Logs >	Query Logs						
System Maintenance	User Name: Login Time: 2	015-11-12 🛄 0 :	User IP: 0 :0 Logout Tin	ne: 2015-1	1-12 🛄 23 :59 :59	Offine Cause: All Query Reset	Advanced Search	•	
Operation Logs	Delete	Export Query	Results Delete All					Network Traffic and Or	line Duration Report
System Logs	Totally 17 Records	s   Each Page 20	Records   Page 1 / tota	ally 1 Pages   GC					
	All None	User Name 🔻	User IP	Full Name	NAS IP	Login Time 🔻	Logout Time 🔻	Offline Cause 🔻	Operation
		Herry	10.1.1.116	Herry	10.1.1.28	2015-11-12 15:46:57	2015-11-12 15:57:27	The device detects that the user goes offline	View
		Herry	10.1.1.105	Herry	10.1.1.28	2015-11-12 15:32:59	2015-11-12 15:46:57	The number of online users has exceeded the limit of terminals using the same account.	View
		Herry	10.1.1.116	Herry	10.1.1.28	2015-11-12 15:43:22	2015-11-12 15:44:19	User goes offline.	View
		Herry	10.1.1.116	Herry	10.1.1.28	2015-11-12 15:42:04	2015-11-12 15:43:03	Be forced offline.	View
		Herry	10.1.1.116	Herry	10.1.1.28	2015-11-12 15:41:11	2015-11-12 15:41:43	Be forced offline.	View
		hjq	10.1.1.105	hjq	10.1.1.28	2015-11-12 15:16:45	2015-11-12 15:31:04	User goes offline.	View
		hjq	10.1.1.105	hjq	10.1.1.28	2015-11-12 15:12:49	2015-11-12 15:16:11	User goes offline.	View
		test	10.1.1.105	test	10.1.1.28	2015-11-12 14:50:37	2015-11-12 15:12:35	User goes offline.	View
		hujq	10.1.1.105	hujq	10.1.1.28	2015-11-12 14:43:53	2015-11-12 14:50:21	User goes offline.	View
		hujiaqi	10.1.1.105	hujiaqi	10.1.1.28	2015-11-12 14:27:01	2015-11-12 14:42:45	User goes offline.	View
		newuser	10.1.1.105	test	10.1.1.28	2015-11-12 14:25:21	2015-11-12 14:25:36	Be forced offline.	View
		newuser	10.1.1.105	test	10.1.1.28	2015-11-12 14:24:12	2015-11-12 14:25:20	Be forced offline.	View
		123 (Deleted)	10.1.1.118	123	10.1.1.28	2015-11-12 13:54:47	2015-11-12 13:55:20	Be forced offline.	View

### Administrator Operation Logs

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



Administrator [admin] Login IP [1]	72.18.7.19] Login Date	[2015-11-12 16:29:10]		🔀 Online User 🚨 System Status	Change Password	C Logout
Authentication & Authority	Log Audit > Oper	ration Logs > Query Logs				
Log Audit	Operator:	Log Content:	Record Tin	ne: 2015-11-12 🚍 - 2015-11-12 🚍 Query Reset		
Authentication Failure Logs	Delete	Delete All				
System Logs	Totally 49 Records	Each Page 20 Record	Is   Page 1 / totally 3 Pages	<b>GO</b>		
User Operation Logs	All  None	Operator 💙	Record Time 💙	Log Content		
		admin	2015-11-12 16:24:47	Database backup succeeded!		
		admin	2015-11-12 16:22:34	Uploaded.		
	8	admin	2015-11-12 16:21:05	Uploaded.		
		admin	2015-11-12 16:14:48	Succeeded in modifying the email service configuration (enable)!		
		admin	2015-11-12 16:13:17	Succeeded in modifying the SMS configuration (enable)!		
		admin	2015-11-12 16:04:06	Portal Settings are modified.		
		admin	2015-11-12 15:49:40	Authentication parameters are modified.		
		admin	2015-11-12 15:46:51	Authentication parameters are modified.		
		admin	2015-11-12 15:45:37	User group (Default User Group) is modified		
		admin	2015-11-12 15:43:03	Force Offline Command is sent to user (Herry:10.1.1.116).		
		admin	2015-11-12 15:41:52	The mobile terminal (c8334b143a04) is deleted.		
		admin	2015-11-12 15:41:52	The mobile terminal (848e0cbc111b) is deleted.		
	8	admin	2015-11-12 15:41:43	Force Offline Command is sent to user (Herry:10.1.1.116).		
		admin	2015-11-12 15:31:53	User information is modified successfully.		

## System Logs

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

Administrator [admin] Login IP [1]	72.18.7.19] Login Date [2	015-11-12 16:29:10]		🖾 Online User 🚨 System Status	🔓 Change Password	O Logout
Authentication & Authority 🕨	Log Audit > System	n Logs > Query Logs				
System Maintenance	Log Content:	Record Tim	2: 2015-11-12 Cuery Reset			
Network Access Logs	Delete	Delete All				
Operation Logs	Totally 36 Records   I	Each Page 20 Records   Pag	e 1 / totaliy 2 Pages   60			
With the second	<u>All  None</u>	Record Time 🌱	Log Content			
	<u> </u>	2015-11-12 16:29:10	admin (172.18.7.19) logged in.			
		2015-11-12 16:27:30	The system started successfully. The IP address is (172.18.7.55).			
		2015-11-12 16:27:30	Client Monitoring Service started (listening port:53)!			
		2015-11-12 16:27:30	Account service is started on listening port 1813.			
		2015-11-12 16:27:30	Access service is started on listening port 1812.			
		2015-11-12 16:27:29	The offline timers are resumed!			
		2015-11-12 16:27:29	The offline timers are enabled!			
		2015-11-12 16:27:29	Scheduled verification for connection to the correlated external server is enabled.			
		2015-11-12 16:27:27	The trial version is valid for 720 hours and already in use for 130 hours.			
		2015-11-12 16:25:50	Password cannot be null!			
		2015-11-12 16:25:50	Password cannot be null!			
		2015-11-12 15:12:49	User information (hjq) is learned.			
		2015-11-12 14:51:38	admin (172.24.0.55) logged in.			
		2015-11-12 14:50:37	User information (test) is learned.			

### **User Operation Logs**

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

Administrator [admin] Login IP [17	72.18.7.19] Login Date [	2015-11-12 16:29:10]	1994 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 - 1995 -	Online User 👌	System Status	Change Password	
Authentication & Authority	Log Audit > User	Operation Logs > Query Logs					
System Maintenance  Log Audit  Log Configuration	Log Content:	Record Time: 2015-1	1-12 📄 - 2015-11-12 📋 Query Reset				
Authentication Failure Logs	Delete	Delete All					
Operation Logs	Totally 4 Records   I	Each Page 20 Records   Page	/ totally 1 Pages   G0			M 4	
📝 System Logs							_
User Operation Logs	All None						
		2015-11-12 15:43:22	User (Herry) has registered the terminal (dcc7937a73a8).				
		2015-11-12 14:27:01	User (hujiaqi) has registered the terminal (848e0cbc111b).				
		2015-11-12 14:16:33	User (test:172.18.7.19) logged out the Self-Service platform.				
		2015-11-12 11:44:19	User (sb) has registered the terminal (c8334b143a04).				
	Totally 4 Records   I	Each Page 20 Records   Page	1 / totally 1 Pages   60			10 Q	





# FAQ

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

Enter http://local IP address:8080/smp/index.jsp in the address bar of your browser. Enter the username (admin) and password (111111111) of the system administrator in the login page.

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

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

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

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

Authentication & Authority 🕨	System Maintenance > Basic Configuration
System Maintenance 🔹 🔹	
Basic Configuration	Server Parameter
By SMS Settings	* VHTTP Port: 8080 (default 8080)
🖾 Email Service Settings	* VHTTPS Port. 8443 (default 8443)
	* Required memory limit: 512 MB - 1024 MB (Recommended 512 MB - 1024 MB)
Custom Manager Page	① Tips: The HTTP port and the HTTPS port cannot be the same.
式 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

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

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

Why does the system prompt existence of unsupported characters?

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

、	~	!	@	#	\$	%	٨	&	*
(	)	(	)	[	]	{	}		١
_	-	=	+	,		&	,	+	,
. ,	:	u	"	6	,	<	>	%	



## RG-SMP Professional\_2.63 \_EN\_Build20151106 Operation Guide

6	,	"	33		‰	`	0	]	^
	»	ľ	]	!	"	#	\$		*
;	<	=	>	_	•	/	:	?	@
{		}	~	[	$\backslash$				