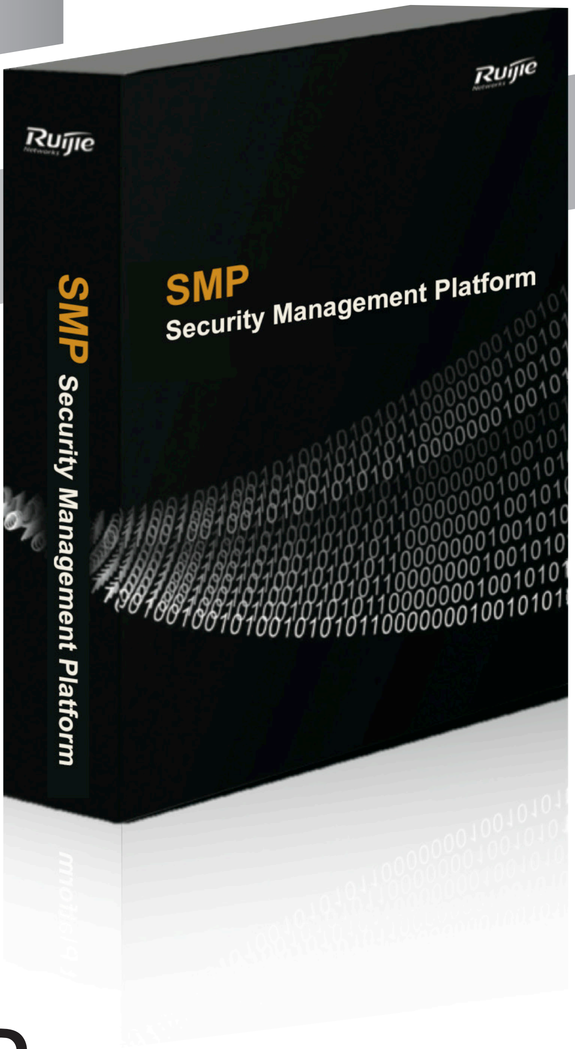


# RG-SMP

## Security Management Platform Datasheet

Ruijie Networks Co., Ltd.
For further information, please visit our website http://www.ruijienetworks.com

# Overview

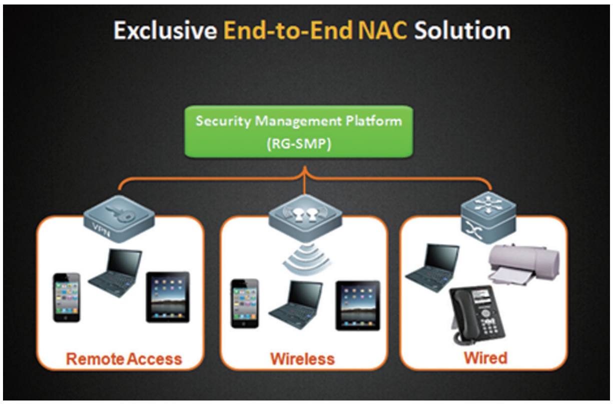
The Ruijie RG-SMP (Security Management Platform) is an enterprise-class security management application that provides insight into and control of Ruijie security and network devices. The Ruijie RG-SMP offers comprehensive security management across a wide range of Ruijie security appliances, including Ruijie intelligent switches and Wireless solutions. The Ruijie 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.

# Key Features

## Unified Wired and Wireless Network Access Control

The Ruijie RG-SMP offers a single, integrated security management platform for all wired, wireless and VPN (Virtual Private Network) devices. It supports not only dynamic authentication for different smart devices, but also integration with third-party RADIUS (Remote Authentication Dial-In User Service) and LDAP (Lightweight Directory Access Protocol) Directory services.


Exclusive End-to-End NAC Solution
Security Management Platform
(RG-SMP)
VPN
Remote Access
Wireless
Wired

Exclusive End-to-End NAC Solution

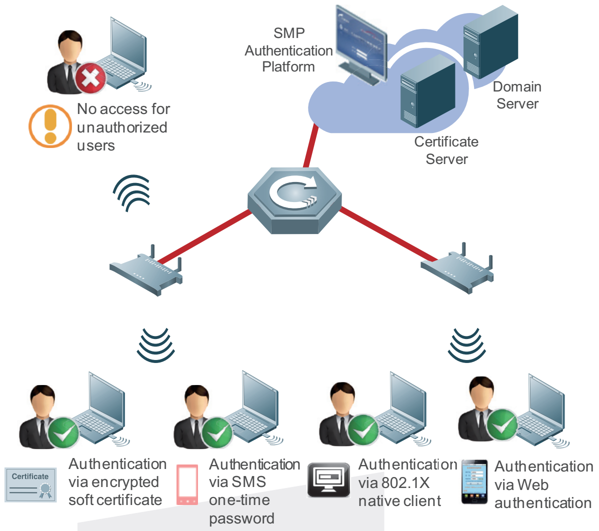
## BYOD Solution Support

The Ruijie RG-SMP supports dynamic Wireless Guest Account control policy based on user identity and mobile platform in use. It also supports self-service guest account creation with SMS authentication on all latest smart device platforms such as smartphone, tablet, etc.

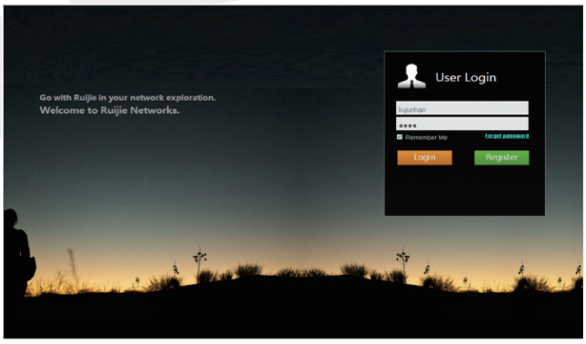
RG-SMP for Unified Management of BYOD

## Comprehensive Identity Authentication

The Ruijie RG-SMP supports web-based authentication and wireless identity authentication based on 802.1X protocol. Through flexible binding of user credentials, IP address, MAC address, switch IP address, switch port and serial number of hard disk, the user identity can be verified. It provides network access authority control, user online/offline records and regular user account clearance. User blacklist can also be managed using the Ruijie RG-SMP. RG-SMP delivers an extensive library of authentication modes including web portal authentication, two-factor authentication for staff, QR code authentication and SMS authentication. The following diagram illustrates the interface display and principles of the four authentication methods.


No access for unauthorized users
SMP Authentication Platform
Domain Server
Certificate Server
Certificate
Authentication via encrypted soft certificate
Authentication via SMS one-time password
Authentication via 802.1X native client
Authentication via Web authentication

RG-SMP with Comprehensive Authentication Modes



Go with Ruijie in your network exploration.
Welcome to Ruijie Networks.

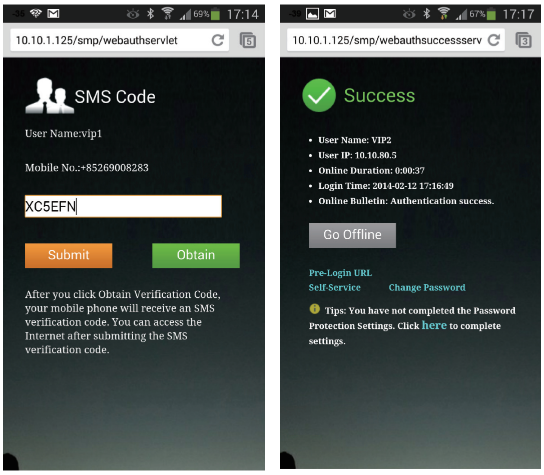
User Login

liujunhan

●●●●

☑ Remember Me

Customized Web Portal Authentication



10.10.1.125/smp/webauthservlet

SMS Code

User Name:vip1

Mobile No.:+85269008283

XC5EFN

Submit | Obtain

After you click Obtain Verification Code, your mobile phone will receive an SMS verification code. You can access the Internet after submitting the SMS verification code.

10.10.1.125/smp/webauthsuccessserv

Success

- User Name: VIP2
- User IP: 10.10.80.5
- Online Duration: 0:00:37
- Login Time: 2014-02-12 17:16:49
- Online Bulletin: Authentication success.

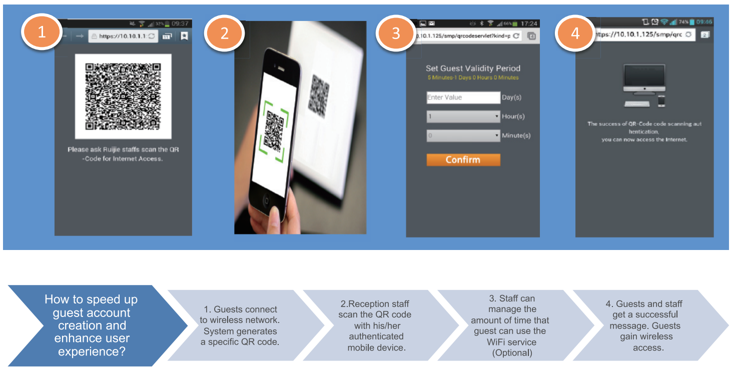
Go Offline

Pre-Login URL

Self-Service Change Password

Tips: You have not completed the Password Protection Settings. Click here to complete settings.

Two-factor Authentication for Staff (Password + SMS)



1. https://10.10.1.1

Please ask Ruijie staffs scan the QR -Code for Internet Access.

3. 0.10.1.125/smp/qrcodeservlet?kind=p

Set Guest Validity Period

5 Minutes-1 Days 0 Hours 0 Minutes

Enter Value Day(s)

1 Hour(s)

0 Minute(s)

Confirm

4. ttps://10.10.1.125/smp/qrc

The success of QR-Code code scanning aut hentication,
you can now access the Internet.

How to speed up guest account creation and enhance user experience?

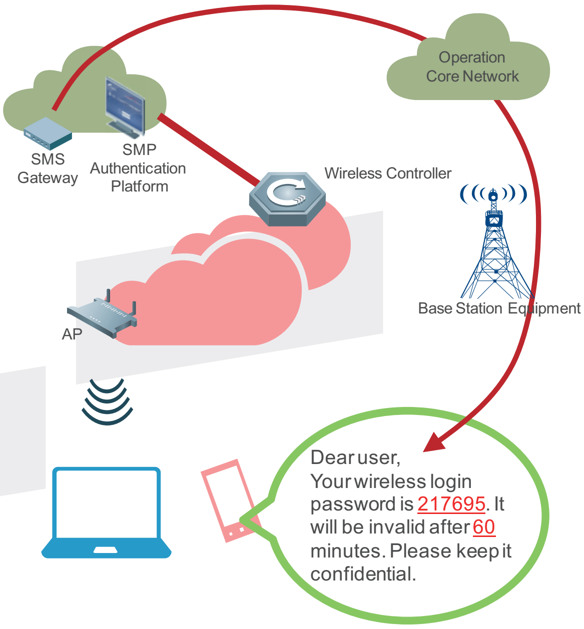
1. Guests connect to wireless network. System generates a specific QR code.

2.Reception staff scan the QR code with his/her authenticated mobile device.

3. Staff can manage the amount of time that guest can use the WiFi service (Optional)

4. Guests and staff get a successful message. Guests gain wireless access.

QR Code Authentication

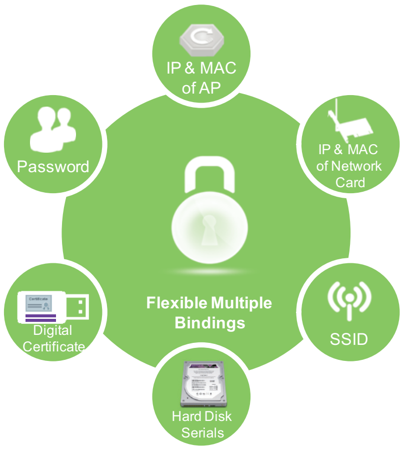


Dear user,
Your wireless login password is 217695. It will be invalid after 60 minutes. Please keep it confidential.

SMS Authentication

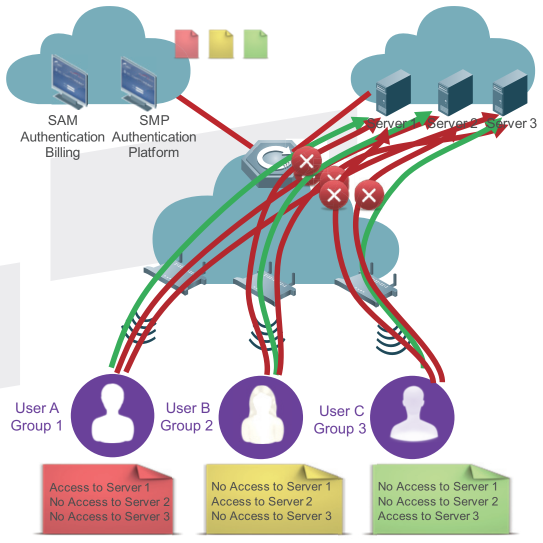
## Host Endpoint Protection Support

By obtaining updates from Microsoft WSUS (Windows Server Update Services), the Ruijie RG-SMP enables administrators to deploy the latest operating system updates to computers running Windows. Anti-virus software is also supported to protect the system against malicious attacks. Blacklist and whitelist can be managed on the endpoint device software to block undesirable or risky users. In addition, the Ruijie RG-SMP prevents unauthorized access and MAC Address Spoofing, ensuring network and service availability and business continuity. The Ruijie RG-SMP software offers multiple bindings of user instances to ensure high-level security of password, end device and network access. The features enable fast location of users and end devices for immediate troubleshooting.



User Info Multiple Binding

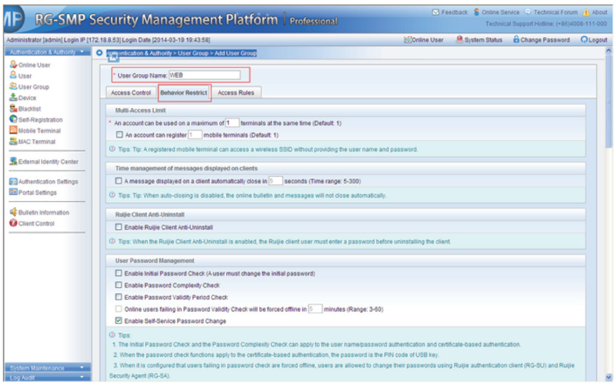
The RG-SMP offers comprehensive security with flexible management. The solution enables dynamic access control rules with flexible Role/User/IP-based VLAN quarantine. The solution ensures that user is only allowed to access to the preset network via flexible access rights restriction based on different user groups, login domains, end device types, etc.



User Info Multiple Binding

## Simple Web Operation

Ruijie RG-SMP supports a user-friendly Web GUI interface to perform all the related SMP security configurations and user access status management.



Administrator [admin] Login IP [172.18.8.53] Login Date [2014-03-19 19:43:58]

Authentication & Authority > User Group > Add User Group

* User Group Name: WEB

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)

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

Time management of messages displayed on clients

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

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

Ruijie Client Anti-Uninstall

□ Enable Ruijie Client Anti-Uninstall

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

User Password Management

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

□ Enable Password Complexity Check

□ Enable Password Validity Period Check

□ Online users failing in Password Validity Check will be forced offline in 5 minutes (Range: 3-60)

☑ Enable 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 check are forced offline, users are allowed to change their passwords using Ruijie authentication client (RG-SU) and Ruijie Security Agent (RG-SA).

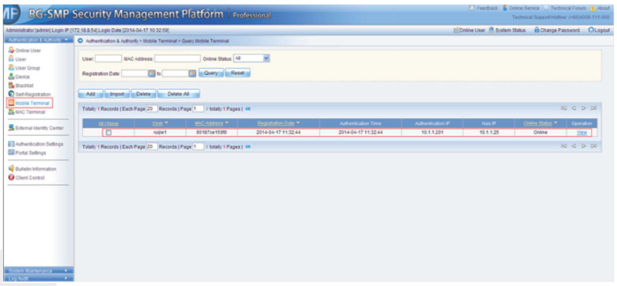
Web GUI Interface Display

## Detailed Security Track Record

RG-SMP presents a board array of reports and analysis to facilitate security management. The solution offers detailed online user information including Username, IP, MAC, VLAN ID, NAS IP, Login Time, Authentication Method, Wireless SSID, Upstream/Downstream Traffic (Ruijie RG-ACE Internet Application Security Gateway integration required), Client Type, etc.

Ruijie RG-SMP offers various kinds of logs for easy management:

- Authentication Failure Logs
- Network Access Logs
- Operation Logs
- System Logs
- User Operation Logs
- 360-Day Record



Administrator [admin] Login IP [172.18.8.54] Login Date [2014-04-17 10:32:59]

Authentication & Authority > Mobile Terminal > Query Mobile Terminal

User: MAC Address: Online Status: All

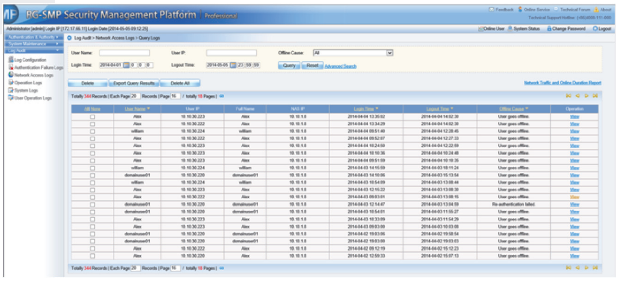
Registration Date: to

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

| All \| None | User | MAC Address | Registration Date | Authentication Time | Authentication IP | Nas IP | Online Status | Operation |
|---|---|---|---|---|---|---|---|---|
| □ | ruijie1 | 90187ce156f9 | 2014-04-17 11:32:44 | 2014-04-17 11:32:44 | 10.1.1.201 | 10.1.1.25 | Online | View |

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

Mobile Device Management



Administrator [admin] Login IP [172.17.66.11] Login Date [2014-05-05 09:12:25]

Log Audit > Network Access Logs > Query Logs

User Name: User IP: Offline Cause: All

Login Time: 2014-04-01 0 0 0 Logout Time: 2014-05-05 23 59 59

Totally 344 Records | Each Page 20 Records | Page 16 / totally 18 Pages |

| All \| None | User Name | User IP | Full Name | NAS IP | Login Time | Logout Time | Offline Cause | Operation |
|---|---|---|---|---|---|---|---|---|
| □ | Alex | 10.10.30.223 | Alex | 10.10.1.8 | 2014-04-04 13:35:02 | 2014-04-04 14:02:30 | User goes offline. | View |
| □ | Alex | 10.10.30.222 | Alex | 10.10.1.8 | 2014-04-04 13:34:29 | 2014-04-04 14:02:30 | User goes offline. | View |
| □ | william | 10.10.30.224 | william | 10.10.1.8 | 2014-04-04 09:51:40 | 2014-04-04 12:28:45 | User goes offline. | View |
| □ | Alex | 10.10.30.222 | Alex | 10.10.1.8 | 2014-04-04 09:52:07 | 2014-04-04 12:27:33 | User goes offline. | View |
| □ | Alex | 10.10.30.223 | Alex | 10.10.1.8 | 2014-04-04 10:24:50 | 2014-04-04 12:22:59 | User goes offline. | View |
| □ | Alex | 10.10.30.223 | Alex | 10.10.1.8 | 2014-04-04 10:10:36 | 2014-04-04 10:24:48 | User goes offline. | View |
| □ | Alex | 10.10.30.223 | Alex | 10.10.1.8 | 2014-04-04 09:51:59 | 2014-04-04 10:10:35 | User goes offline. | View |
| □ | william | 10.10.30.224 | william | 10.10.1.8 | 2014-04-03 14:15:59 | 2014-04-03 18:11:24 | User goes offline. | View |
| □ | domainuser01 | 10.10.30.220 | domainuser01 | 10.10.1.8 | 2014-04-03 14:10:06 | 2014-04-03 15:13:54 | User goes offline. | View |
| □ | william | 10.10.30.224 | william | 10.10.1.8 | 2014-04-03 10:54:09 | 2014-04-03 13:08:44 | User goes offline. | View |
| □ | Alex | 10.10.30.223 | Alex | 10.10.1.8 | 2014-04-03 12:15:22 | 2014-04-03 13:08:30 | User goes offline. | View |
| □ | Alex | 10.10.30.222 | Alex | 10.10.1.8 | 2014-04-03 09:03:01 | 2014-04-03 13:08:15 | User goes offline. | View |
| □ | domainuser01 | 10.10.30.220 | domainuser01 | 10.10.1.8 | 2014-04-03 12:14:47 | 2014-04-03 13:04:59 | Re-authentication failed. | View |
| □ | domainuser01 | 10.10.30.220 | domainuser01 | 10.10.1.8 | 2014-04-03 10:54:01 | 2014-04-03 11:55:27 | User goes offline. | View |
| □ | Alex | 10.10.30.223 | Alex | 10.10.1.8 | 2014-04-03 10:33:09 | 2014-04-03 11:54:29 | User goes offline. | View |
| □ | Alex | 10.10.30.223 | Alex | 10.10.1.8 | 2014-04-03 09:03:00 | 2014-04-03 10:03:08 | User goes offline. | View |
| □ | domainuser01 | 10.10.30.220 | domainuser01 | 10.10.1.8 | 2014-04-02 19:03:06 | 2014-04-02 19:58:54 | User goes offline. | View |
| □ | domainuser01 | 10.10.30.220 | domainuser01 | 10.10.1.8 | 2014-04-02 19:03:00 | 2014-04-02 19:03:03 | User goes offline. | View |
| □ | Alex | 10.10.30.222 | Alex | 10.10.1.8 | 2014-04-02 09:12:19 | 2014-04-02 15:12:23 | User goes offline. | View |
| □ | Alex | 10.10.30.220 | Alex | 10.10.1.8 | 2014-04-02 12:59:33 | 2014-04-02 15:07:13 | User goes offline. | View |

Totally 344 Records | Each Page 20 Records | Page 16 / totally 18 Pages |

Log Generation and Management

# Technical Specifications

| Product Specifications | Technical Specifications |
|---|---|
| Network Access Control | Support wired, wireless and VPN network access control (NAC) |
| | Support IEEE 802.1x access authentication, without the need for any client agent installation |
| | Support MAC address authentication, without the need for any client agent installation |
| | Support Web Portal authentication for staff<br>Support two-factor authentication using user credentials as well as one-time password via SMS to verify user's pre-registered mobile phone number |
| | Support Web Portal authentication for visitors<br>Support Web Self-Service Platform for visitors to establish temporary/one-time user accounts (via SMS) |
| | Support QR-Code authentication for visitors<br>Visitors require QR-Code authorization by any authenticated user before network access |
| | Support different QoS bandwidth policies application to different users based on their role within the organization and the device type currently in use |
| | Support per user, per device, and per application/TCP-port prioritization (require integration with Ruijie RG-ACE Internet Application Security Gateway) |
| | Support web-based management interface |
| | Support report and analysis generation to show details and correlation of user, authentication and device information for troubleshooting and locating problems |
| | Support AAA framework providing complete separation of Authentication and Authorization sources |
| | Support authorization for LDAP, AD, Kerberos, Token Server, SQL compliant database |
| | Support integrated, network based, device profiler utilizing collection via SNMP, DHCP, HTTP, AD and ActiveSync |
| | Support complex PKI deployment and AAA server certificate signed by external CA whilst validating internal PKI signed client certificates |
| | Support NAC health check allowing both agent and agentless methods and the solution acts as a permanent or dissolvable health agent for Windows, Linux, and Macintosh platforms |
| Third-party Certification System Integration | Support 3rd party RADIUS authentication integration |
| | Support user data collection of 3rd party certification information from Java / web service based interface |
| | Support Microsoft Windows Active Directory (AD) domain integration, including seamless Single-Sign-On integration for a complete 802.1X authentication and Windows AD authentication |

| Product Specifications | Technical Specifications |
|---|---|
| Third-party Certification System Integration | Support the integration with LDAP server to obtain user identity information to achieve unified authentication |
| Learning and Support for Multi-element Binding | Support terminal hard drive serial number, SSID, user name, password, terminal IP, terminal MAC, network access control device (NAS) IP, NAS port active learning as well as multi-element flexible combination of binding elements (May require agent installation) |
| User Management | Support account creation, cancellation and user group management<br>Support customized user information fields, such as department, age, etc.<br>Support Self-Service Platform (Web) for visitors to establish temporary/one-time user accounts<br>Support dynamic user blacklist which prohibits user to login in specified period of time<br>Support for setting account usage period and auto account cancellation when expired, with user notification in advance |
| | Support users login broadcast messages pop up, or web page pop up<br>Support Disclaimer Acceptance message pop up and visitors need to click "Accept" before accessing the network<br>Support authentication suspension period, during that period the user disabled cannot authenticate or access the Internet |
| | Support online user management, including message broadcast, online users status review, forced offline as well as online user re-authentication, information gathering and remote assistance |
| | Support maximum user password attempts before user account is locked |
| | Support direct access to the user's physical NIC MAC address, to prevent tampering of the MAC address |
| | Support limited number of devices, quota or bandwidth per user |
| | Support caching of MAC address for post guest authentication and guests do not need to re-authenticate during the valid access period |
| | Support bulk import of guest accounts and enable notification of credentials via email |
| | Support sponsored approval workflow for guest self-registration which the new SSID registration requires approval from internal staff |
| | Support display of post login session statistics page for users to review and monitor usage or quota assigned |
| | Support network-based devices ACL, VLAN, and host ACL network access control |
| User Authentication | Support seamless 802.1x authentication, without the need for any client agent installation and multi-vendor network access |
| | Support Web Portal authentication for staff<br>Optionally support two-factor authentication using user credentials as well as one-time password via SMS to verify user's pre-registered mobile phone number |
| | Support Web Portal authentication for visitors<br>Support Web Self-Service Platform for visitors to establish temporary/one-time user accounts (via SMS or e-mail) |

| Product Specifications | Technical Specifications |
|---|---|
| User Authentication | Support QR-Code authentication for visitors<br>Visitors require QR-Code authorization by any authenticated user before network access |
| | Support MAC Address Bypass (MAB) authentication for devices which cannot support IEEE 802.1x protocol |
| | Support auto-login for self-registration workflow |
| End Point Compatibility | Support the latest Windows, Mac desktops and support for Apple, Android mobile device platform |
| | Support device-based portal page and automatic screen fit feature for various screen resolution mobile device platform |
| Host Security Management<br>(Agent installation required) | Support 3rd party antivirus software integration, allowing software installation detection, operation, and updates patches can be pushed remotely |
| | Support integration with Windows Security Center |
| | Support the installation program to detect and repair software that must be installed to force the download and installation, prohibit the installation software prompts to uninstall; support processes running, registry keys, Windows service entry inspection and repair; support external connection port for management, prohibiting the use of USB, CD-ROM loaded with connectors; support Windows patch updates the mandatory or non-mandatory; support switch-based ACL, the switch VLAN, ACL implementation of quarantine host |
| Asset Management<br>(Agent installation required) | Support the collection of the user's software and hardware information, hardware information when the user changes, CPU, memory, motherboards, hard drives and other information for logging |
| Network Security Management | Support ARP spoofing prevention features that enable trusted gateway ARP entries to prevent ARP spoofing gateway device, the client also supports static binding ARP information |
| | Support role-based user security management |
| | Support dynamic, stateful access rights into the network once authenticated based on source, destination, and/or ports |
| | Support defining rules for access rights based on any combination of time, location, user identity, device identity, and extended attributes from the authentication database |
| | Support defining policies for users who can access the network, with which mobile device and which parts of the network they can access |
| | Support users to allow traffic, deny traffic, reject traffic, route traffic, and blacklist (remove from the network) |
| | Support blacklisting of wireless devices once firewall / ACL access rule violations are detected or revocated<br>(Ruijie RG-SMP Client installation is required) |

| Product Specifications | Technical Specifications |
|---|---|
| Network Security Management | Support the automatic recognition of operating system and product type of the end devices |
| | Support display of users' internet usage (integration with RG-ACE Internet Application Security Gateway required) |
| | Support integration with RG-IDS devices that can collect IDS devices reported security incidents and the source of the attack for direct processing; critical server's IP address configuration for more sensitive event handling and protection |
| User-based Internet Application Control | Support integration with RG-ACE Internet Application Security Gateway; the gateway supports real-time analysis on the L7 Internet Application that the authenticated users are using; the gateway supports user-based application control which the user can be selected from the Authentication System |
| System Reliability | Support Microsoft Windows and SQL Server cluster hot standby |
| | Support over 50,000 users by license extension |
| | Support backup cluster node with uninterrupted authentication traffic when node failure occurs |
| | Support high availability redundancy design for resiliency |

## System Hardware & Software Requirements:

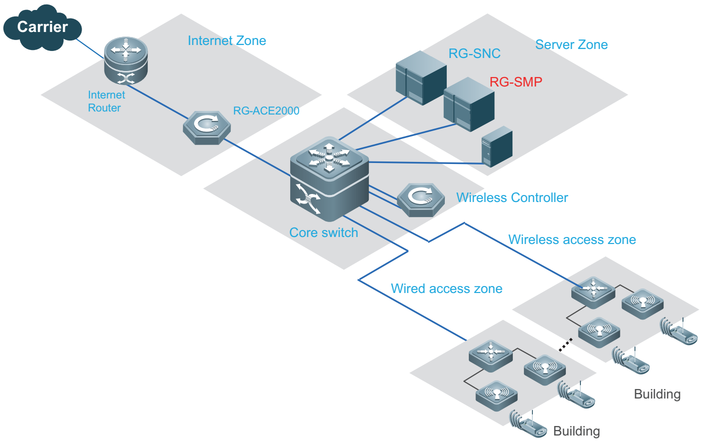
- Minimum Specification:

| Hardware Platform Requirement | |
|---|---|
| Processor | Intel Xeon 2.8GHz Quad Core x 2 or above |
| Memory | 4G or above |
| Storage | 160G or above |
| Network Card | 3 x Gigabit Ports |
| Operating System and Database | |
| Operation System | Windows Server 2003 Enterprise Edition SP2 or above |
| Database | SQL Server 2005 Enterprise Edition SP2 or above |

- Recommended Specification for Large Deployment (Over 15,000 users):

| Hardware Platform Requirement | |
|---|---|
| Processor | Intel Xeon 2.8GHz Quad Core x 2 or above |
| Memory | 16G or above |
| Storage | 500G or above |
| Network Card | 3 x Gigabit Ports |
| Operating System and Database | |
| Operation System | Windows Server 2008 Enterprise Edition SP1 or above (x64) |
| Database | SQL Server 2008 Enterprise Edition SP1 or above (x64) |

# Typical Applications



Enterprise Network Access Control for Wired & Wireless Users

Ruijie RG-SMP is proven to achieve unified network access management and security accounting & authentication management:

1. Unified User Management System: A single portal capable of identifying different users. All wired, wireless and VPN users are centrally managed using the RG-SMP platform. RG-SMP further maps with the Microsoft Windows Active Directory and achieves true unification. Windows AD is the master controller of all user account management. All changes are simultaneously updated to the web account. Each user is only required to have one set of username and password.

2. Self-service Guest Management: QR Code Authentication is deployed to cater for the increasing Wi-Fi demand from visiting guests. Guests can scan a QR code posted in the public area and are automatically granted login ID and password for Wi-Fi access. IT administrators can easily adjust the validation period of the QR code and password. This measure effectively lessens the burden on guest network management.

3. Advanced Guest Management: RG-SMP offers the QR code authentication measure. Authorized staff who has logged in the company network can grant guest access rights. This binds the guest's network activity logs to the staff's account together, offering an easy record for management. Guest first connects to the wireless network and a QR code page will be shown. The guest can ask any authorized staff to scan the QR code and access rights are granted right away.

4. User Authorization: User-specific restrictions are available. Management staff has free network access. Guests can only access to the Internet.

# Ordering Information

| Model | Description |
|---|---|
| RG-SMP-Pro-EN | RG-SMP 2.X professional edition, supports RADIUS identity authentication, including BYOD and NAC features.<br>Software requirement for SMP:<br>• Windows Server 2003 or above<br>• SQL Server 2000 or above |
| RG-SMP-Pro-EN-license-50 | Concurrent User License for RG-SMP 2.X professional edition, includes permission for 50 concurrent users. |

Ruijie Networks

Innovation Beyond Networks

## Ruijie Networks Co., Ltd.

### Headquarter in Beijing

Address: Floor 11, East Wing, ZhongYiPengAo Plaza, No.29
Fuxing Road, Haiddian District, Beijing 100036,China
Email: info@ruijie.com.cn
Tel: (8610) 5171-5961
Fax: (8610) 5171-5997

### Regional Office in Hong Kong

Address: Unit 09,20/F, Millennium City 2, 378 Kwun Tong
Road, Kowloon,Hong Kong
Email: sales-hk@ruijienetworks.com
Tel: (852) 3620-3460
Fax: (852) 3620-3470

### Supply Chain in Fuzhou

Address: JuYuan Star-net Ruijie Technology Park, No. 618
JinShan road, Fuzhou City, 350002, China
Tel: (86591) 83057888
(86591) 83057000

### Regional Office in Malaysia

Address: Office Suite 19-12-3A, Level 12, UOA Center, No.19
Jalan Pinang, 50450 Kuala Lumpur
Email: sales-my@ruijienetworks.com
Tel: (603) 21811071

For further information, please visit our website http://www.ruijienetworks.com

This material was made in Jan, 2013. The pictures and technical data inside are only for reference. All rights reserved.