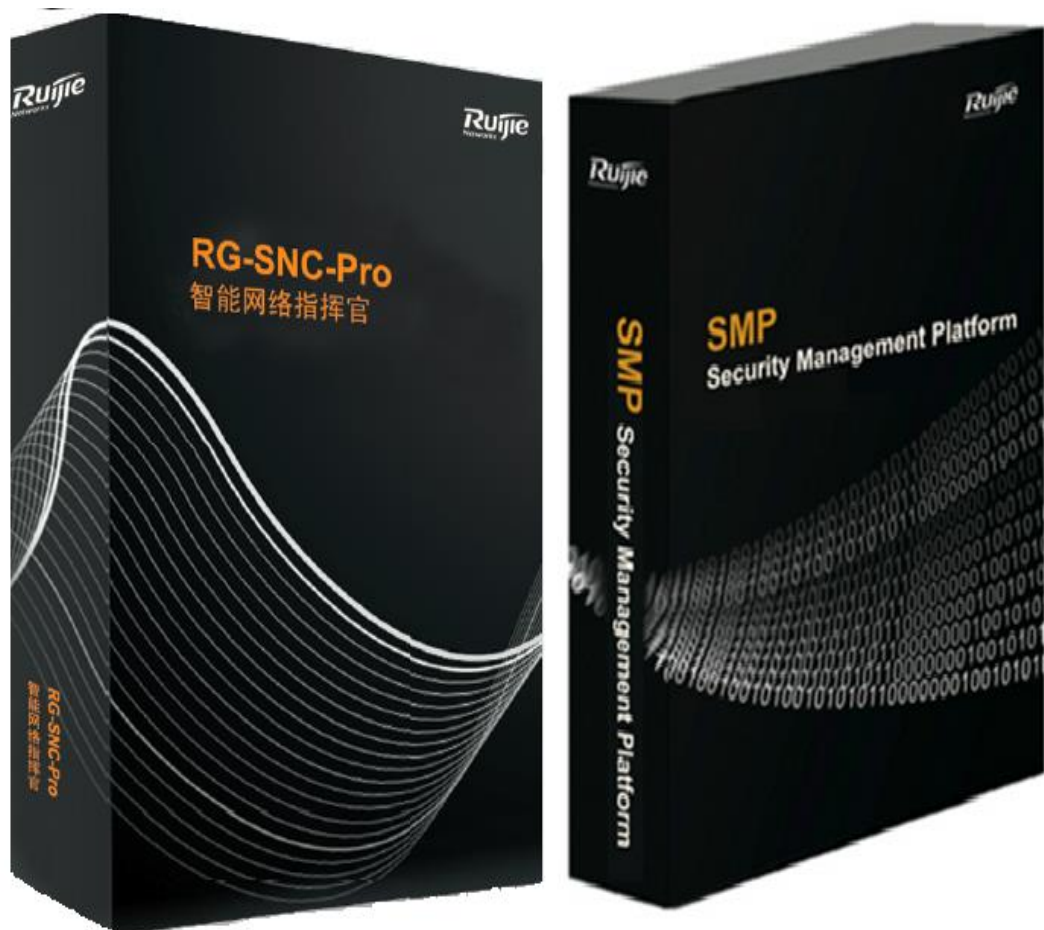


RG-Application Software FAQs V1.1



Copyright Statement

Ruijie Networks©2013

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

 ,  ,  ,  ,  ,
 ,  ,  ,  ,  ,
 ,  are registered trademarks of Ruijie Networks. Counterfeit is strictly prohibited.

Exemption Statement

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

1 Overview

This document provides a detailed description on the usage constraints of minimalist networks and the solutions to problems that frequently occur during network deployment, in order to guide the after-sales personnel to deploy and implement minimalist network solutions, thus improving deployment efficiency and quality.

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

- Ruijie Networks Websites : <http://www.ruijienetworks.com>
- Ruijie Service Portal : <http://case.ruijienetworks.com>

Welcome to report error and give advice in any Ruijie manual to Ruijie Service Portal

Related Documents

- RG-Application Software FAQs V1.1
-

Revision History

Date	Change contents	Reviser
2016.09.01	Initial Release	Amy & crystal
2017.02.01	Add new chapter of 4.1 SMP Q12-Q22, 4.2 SNC Q11, 4.3 SAM on Publication V1.1	TAC Oversea

2 Introduction to the Index

This document collects the frequently asked questions (FAQs) about minimalist networks and provides answers by category. Because the questions are not indexed, to search for a specific question, press the shortcut key **Ctrl+F** in the document and enter keywords of your question in the search box.

3 Contents

1	Overview	1-1
2	Introduction to the Index	2-2
3	Contents	3-3
4	FAQ	4-4
4.1	SMP	4-4
4.2	SNC	4-21
4.3	SAM	4-29

4 FAQ

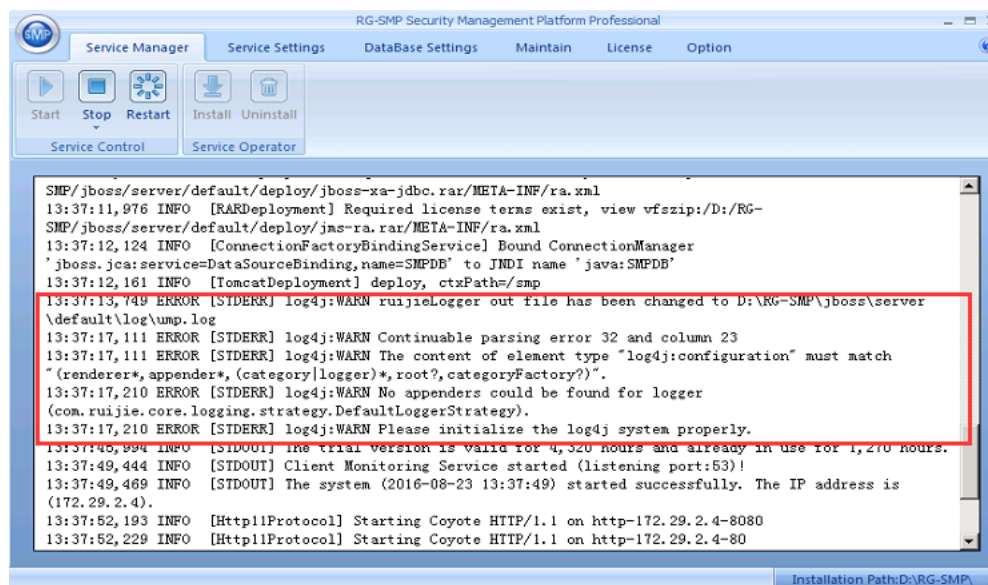
4.1 SMP

Q1: Database backup and restore

The database backed up on the Security Management Platform (SMP) can be restored to the SMP of the same version. For example, you can restore the database that is backed up on 2.63_EN_Build20151106 only to 2.63_EN_Build20151106.

Q2: Does it matter if a log4j error is displayed?

As shown in the following figure, the error marked in the red box does not affect the normal operation of the SMP. Such information is displayed during the startup of Tomcat.



Q3: Can the SMP be connected to a third-party NAS for web authentication?

The third-party NAS device should support the China Mobile Portal 2.0 protocol. For example on a H3C switch, if the following command can be run, it can be used to connect with an SMP.

```

portal url-param include user-mac param-name wlanusermac
portal url-param include nas-ip param-name wlanacip
portal url-param include user-url param-name url
  
```

```
[H3C]portal server smp ip 10.1.1.185 server-type ?
cmcc Server type is cmcc
imc Server type is imc
```

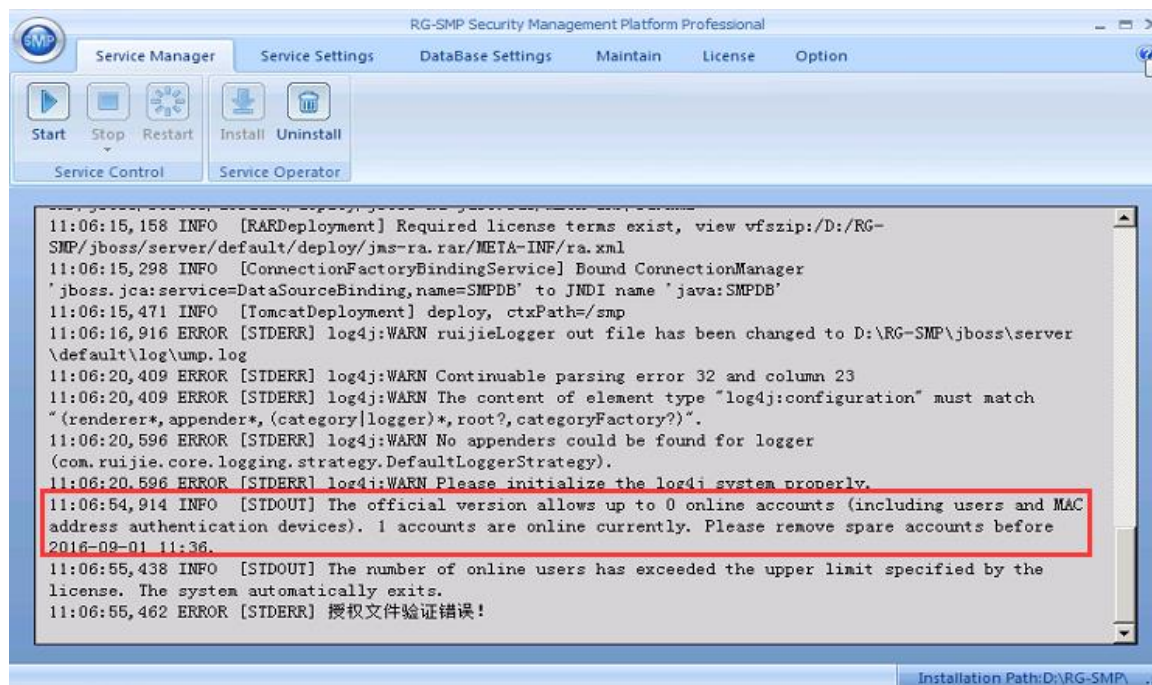
The supported H3C switches include H3C WX3024, H3C WX5004, and H3C WX5510.

Q4: Can SMP support integrate with multiple third-party identity centers or AD domains?

For example, if both the Lightweight Directory Access Protocol (LDAP) protocol and active directory (AD) domain exist, the SMP support integrate with only one of them. However, the SMP support integrate with multiple AD domain servers.

Q5: When adding users to the SMP, the system indicates that the license is insufficient, and the SMP service manager indicates that at most 0 online user is allowed.

This message is displayed when the Micro Dongle is not correctly used. The Micro Dongle of the SMP and SNC is the same in look and may probably be misused. If the SNC Micro Dongle is used by fault, the SMP Micro Dongle can also be started, but the license displayed is incorrect.



Q6: What should I do if I forgot the password of the SMP admin?

In SMP2.63 and later versions, find the data table "T_ADMIN" in the database "SMPDB", and change the field of admin password to "316901EEFC21AE17FE07B76BF922CF5C", and the password is reset to "111111111". You can also run **Update T_ADMIN SET password='316901EEFC21AE17FE07B76BF922CF5C' where adminID='admin'** to reset the password.

Q7: How to calculate the number of SMP authenticated user?

SMP 2.63 authentication calculates the number of online users. It has nothing to do with the total number of created users, the number of allowed login times, and the type of the used client. For example, if you purchase 50 licenses, 50 concurrent online users are allowed.

Q8: How to synchronize the passwords if the SMP is integrated with AD domain Server?

On SMP 2.65 and earlier versions, the function "Learn new user's password during authentication" is enabled by default.

Each time when an AD domain user is authenticated, the user password is checked in the AD domain. The password will be saved locally if the password check is successful. When the communications between the SMP and the AD domain is faulty, the user password that is saved locally can be used for user authentication.

If the local password of the SMP is changed, the password in the AD domain is not affected. Upon user authentication, the password will be checked in the AD domain and saved to the SMP locally. If the password in the AD domain is changed, the new password is checked in the AD domain when it is used for authentication, and synchronized to the SMP. Given that Windows AD domain has a mechanism that can delay the expiration of the previous password, the previous password can still be used in a period of time after the AD domain password is changed.

Q9: How does an SMP perform authentication when SMP is integrated with multiple AD domains?

Use the format domain name\user name or user name@domain name to perform authentication in the designated domain.

Q10: What are the keep-alive configurations for SMP user in Web authentication?

Wired Web authentication user: It is recommended to enable the online status detection function for a wired Web authentication user (If the keep-alive page of successful authentication is turned off, the user is forced offline in three heartbeat periods).

Choose **Authentication & Authority > Portal Settings > Heartbeat Detection on Web-authenticated Users**

<input checked="" type="checkbox"/> Heartbeat Detection on Web-authenticated Users	
* Detection Interval:	<input type="text" value="5"/> minutes (Default: 5)

Wireless Web authentication user: Enable traffic keep-alive on the AC as recommended.

WS6108(config)#offline-detect interval 10 threshold 100

If the wireless data traffic is smaller than 100 bytes in 10 minutes, the wireless user is considered as offline.

Q11: Why Are 802.1x Authenticated Users Disconnected from the Network Immediately After They Go Online?

Fault symptom: A wireless 802.1x authentication device is associated with the Security Management Platform (SMP). After a user goes online on the SMP successfully, the user is disconnected from the network immediately. The prompts displayed on the AP show that the user goes offline actively because the four-way handshake fails.

Possible causes: Check authentication information on the SMP. No exception is found. Captured packets indicate that the authentication type configured on the AC is inconsistent with that on the SMP. The root cause is that wired 802.1x authentication is selected on the SMP.

Q12: The SMP Service of Version 2.63En Fails to Be Started Normally

Customer: UITM in Malaysia

Symptom: The logs as shown in the following figure show that the SMP service has been started.

```
14:55:30,437 INFO [STDOUT] Client Monitoring Service started (listening port:53)!
14:55:30,484 INFO [STDOUT] The system (2016-01-14 14:55:30) started successfully. The IP
address is (10.34.1.20).
14:55:32,590 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-10.34.1.20-8080
14:55:32,621 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-10.34.1.20-80
14:55:32,621 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-10.34.1.20-443
14:55:32,637 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-10.34.1.20-28080
14:55:32,652 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-10.34.1.20-9090
14:55:32,668 INFO [Http11Protocol] Starting Coyote HTTP/1.1 on http-10.34.1.20-8443
14:55:32,668 INFO [ServerImpl] JBoss (Microcontainer) [5.1.0.GA (build:
SVNTag=JBoss_5_1_0_GA date=200905221053)] Started in 1m:34s:614ms
```

Users fail to log in to the Web UI of the SMP and the user authentication fails.

Cause: About 2000 UITM users apply for authentication. The SMP service may fail to be started normally if there are a large number of authentication packets before start-up of the SMP service.

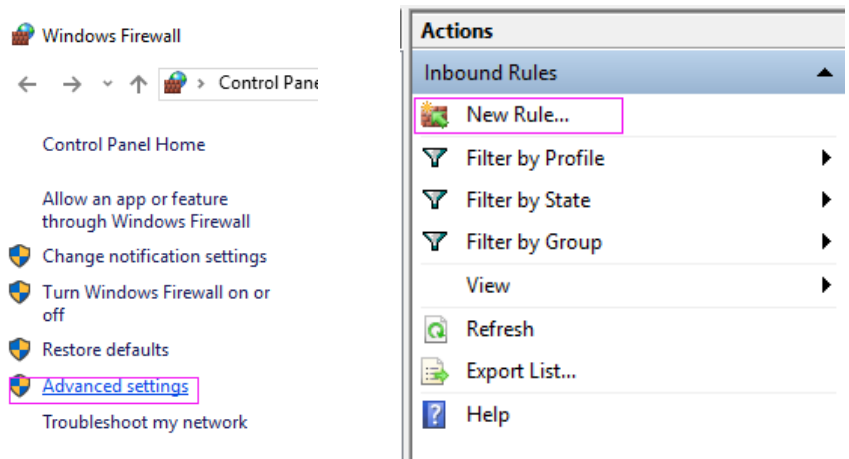
Perform the following operations to rectify the fault:

1. Access the installation directory of the SMP, collect the log folder and the **run.log** file, and submit them to the Technical Assistance Center (TAC).
2. Stop the SMP service.
3. Enable the firewall that comes with Windows, edit rules, and block TCP port 80 (user authentication port).
 - a) Enable the firewall.

Public network settings

- Turn on Windows Firewall
 - Block all incoming connections, including those in the list of allowed applications
 - Notify me when Windows Firewall blocks a new app
- Turn off Windows Firewall (not recommended)

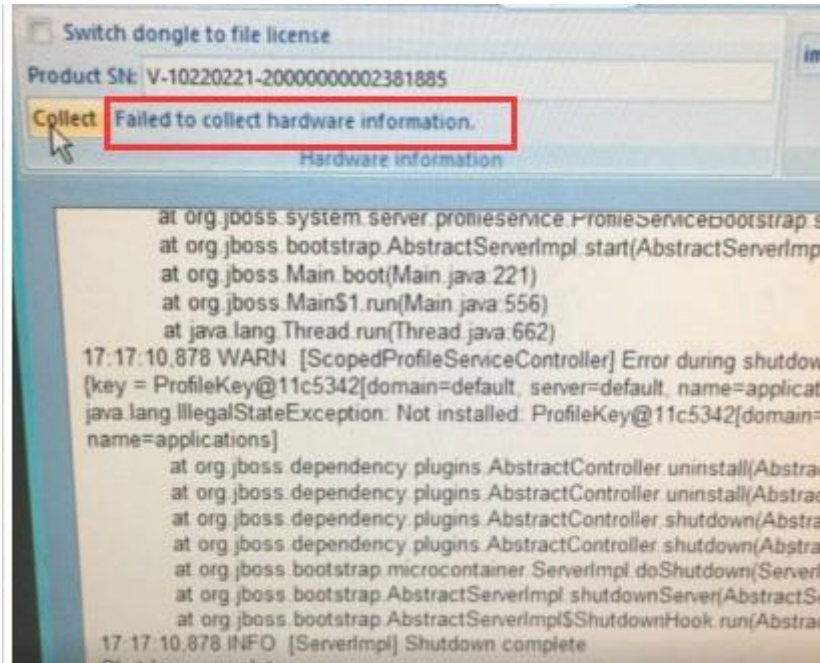
- b) Click Advanced Settings. In the Actions dialog box, select New Rule from the Inbound Rules from the drop-down list and edit a new rule for blocking TCP Port 80.



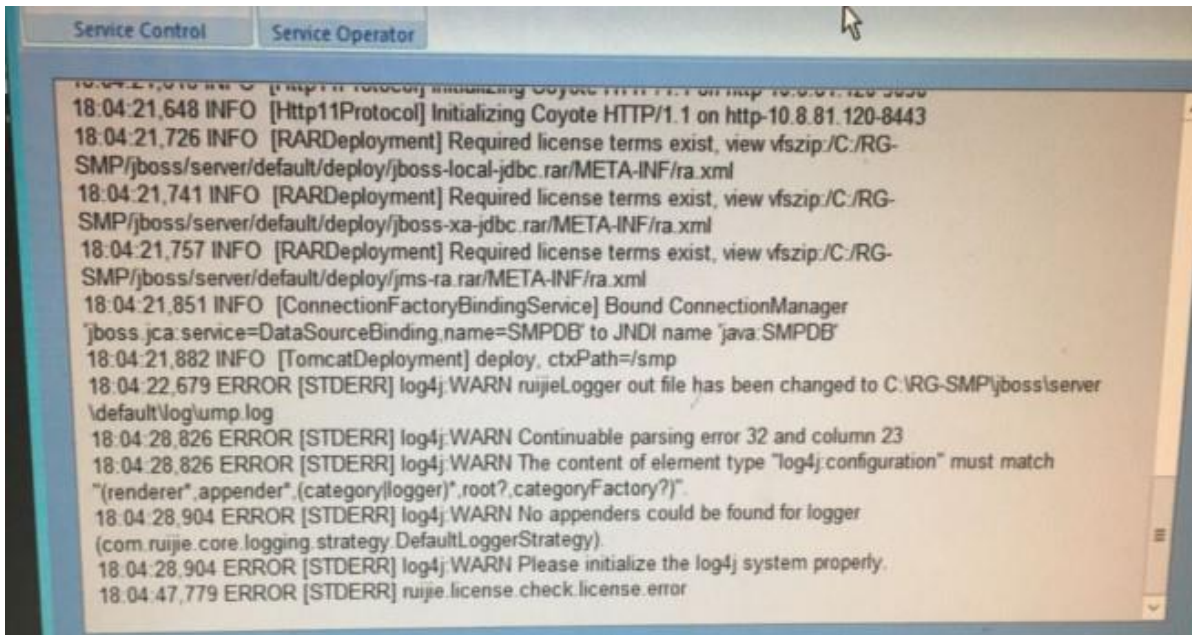
- 4. Start the SMP service.
- 5. Disable the firewall.

Q13: Hardware Information Fails to Be Collected After the SMP Service of Version 2.63 Is Deployed

Fault description: Hardware information fails to be collected after the SMP service is newly deployed, as shown in the following figure.



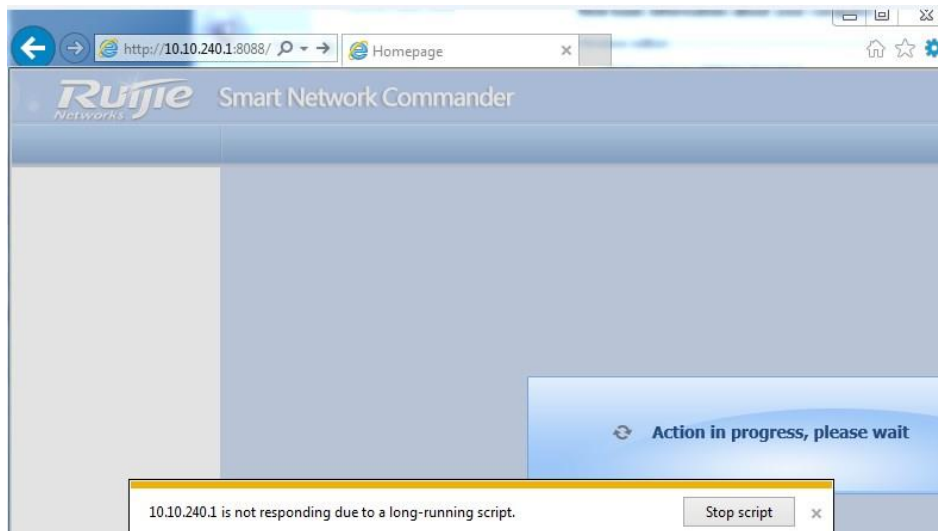
Solution: Install the patch (Release Notes for RG-SMP_2.63_EN_Build20151106 to rectify this fault. Ensure that all files are replaced. Otherwise, a license error will occur. In addition, install relevant patches.



Q14: What Will Happen After the Test Dongle of the SMP Is Inserted into the SNC?

The dongles of the Smart Network Commander (SNC) and SMP are completely the same in appearance and are both red.

If the test dongle of the SMP is inserted into the SNC mistakenly, the SNC service can be started normally. However, when the homepage of the SNC is opened, the homepage is stuck and a prompt, indicating that the SNC is not responding due to a long-running script, is displayed, as shown in the following figure.



Q15: What Do I Do When a Fault Occurs After the SMP and AD Domain Controller Are Associated?

Fault Symptom

The SMP and Active Directory (AD) domain controller are associated. The authentication will fail when a user logs in by using an AD account and the following prompt is displayed in the authentication logs of the SMP:

The password of the computer RG-SMP-SERVER is incorrect.

<input type="checkbox"/>	sheenaib	2015-09-09 12:05:21	10.10.100.253	A45E6007972E	Remote Windows AD domain authentication failed. Cause: The password of the computer RG-SMP-SERVER is incorrect. Reset the password as the administrator password, and perform the authenticationRemote system is busy, please try again later
--------------------------	----------	------------------------	---------------	--------------	--

Possible Causes

When the SMP and AD domain controller are associated, the PC account of the RG-SMP-SERVER needs to be added to the AD server. Otherwise, the SMP fails to associate with the AD domain controller normally.

Troubleshooting

Perform the following step to add the PC account of the RG-SMP-SERVER to the AD domain controller.

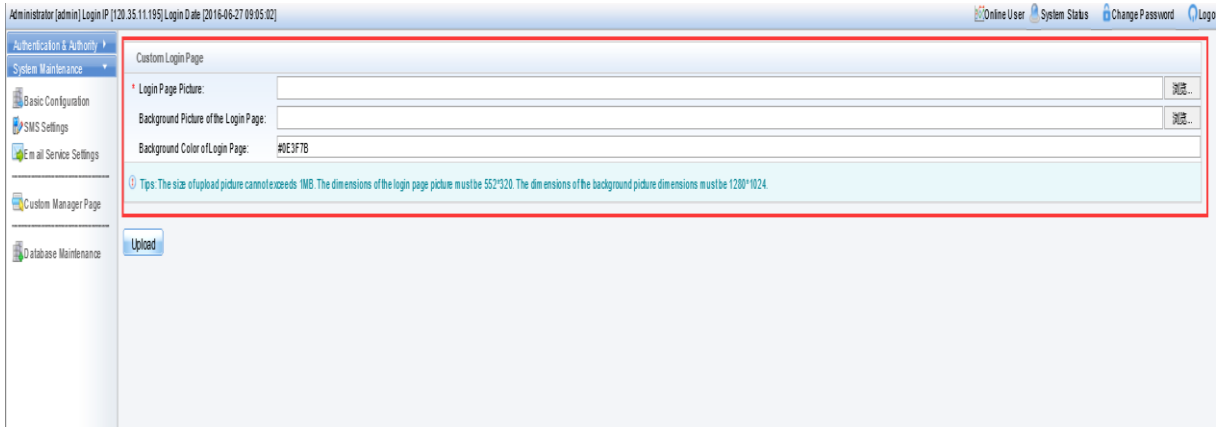
This step is a difficult step in deployment of the AD domain controller association because it involves the domain administrator or domain management account. There are three methods of registering a PC name and changing the password. Select a proper method based on the OS version of the deployed domain controller. Method 1 is applicable to Windows 2008 and later versions, method 2 is applicable to Windows 2003 and later versions, and Method 1 or method 2 is recommended.

No.	Deployment Mode	Domain Controller Type	Deployment Key Point	Recommendation Level
Method 1 3.2.3.1	A domain administrator creates a PC account and changes the PC password on the tool provided on the domain controller.	Windows 2008 and later versions (this method is applicable only to domain controllers of Windows 2008 and later versions. The ADSIEdit.msc tool is unavailable on Windows 2003, and the PC password cannot be changed even if the patch is installed).	<ol style="list-style-type: none"> 1. Apply to the domain administrator for a common domain user account for SMP and AD domain controller association, for example, smpadmin/ruijie_2014. 2. Apply to the domain administrator for a PC account, for example, RG-SMP-SERVER. 3. Instruct the domain administrator to change the registered PC password on the ADSIEdit.msc tool provided on the domain controller. Note that the changed password needs to be consistent with the password of the association account (smpadmin). 	Recommended
Method 2 3.2.3.2	The domain administrator creates a PC account on the domain controller and asks a common user to change the password.	Windows 2003 and later versions	<ol style="list-style-type: none"> 1. Apply to the domain administrator for a common domain user account for SMP and AD association, for example, smpadmin/ruijie_2014. 2. Apply to the domain administrator for a PC account. During registration, when selecting the option that the following users can add the PC to the domain, add the preceding common domain account smpadmin. 	Recommended

No.	Deployment Mode	Domain Controller Type	Deployment Key Point	Recommendation Level
			<p>3. On any PC added to the domain (or add SMP to the domain), use the approved common domain user account to log in to the device and run the .vbs script for changing the PC account password. The entered password needs to be consistent with the password of the associated account (smpadmin) during script running.</p>	
<p>Method 3 3.2.3.3</p>	<p>The domain administrator creates a PC account and runs a script to change the password on the domain controller.</p>	<p>Windows 2003 and later versions</p>	<ol style="list-style-type: none"> 1. Apply to the domain administrator for a common domain user account for SMP and AD association, for example, smpadmin/ruijie_2014. 2. Apply to the domain administrator for a PC account for registration on the account controller. 3. Instruct the domain administrator to run the .vbs script for changing the PC account password on the domain controller. The password entered during script running needs to be consistent with the password of the association account (smpadmin). 	<p>Not recommended</p>

Q16: How Do I Modify the Welcome Logo for Web Authentication?

Background: The SMP of the oversea edition allows users to customize the background picture, but not the welcome logo. If the welcome logo needs to be modified, the relevant file needs to be modified on the SMP server.



The following figure shows the operation steps.

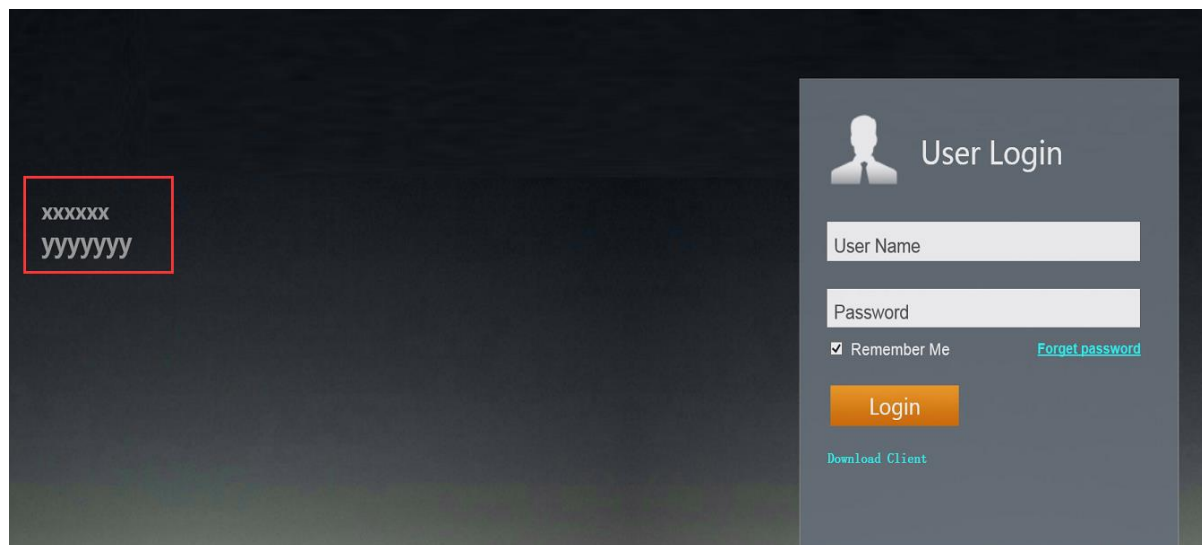
```

    <input id="disclaimerEnable" name="disclaimerEnable" type="hidden" value="<c:out value=
    <input id="disclaimerTitle" name="disclaimerTitle" type="hidden" value="<c:out value=
    <input id="disclaimerContent" name="disclaimerContent" type="hidden" value="<c:out val
    <input id="disclaimerLoginBtn" name="disclaimerLoginBtn" type="hidden" value="<c:out v

    <input id="loginActionName" name="loginActionName" type="hidden" value="./webauthservi

    <c:if test="${enableEsaAuthen}">
    <OBJECT ID="portalObject" CLASSID="CLSID:5744FEFB-DC23-4D1A-A5CE-C8191CC5DD43"
    </c:if>

    <div id="pageDiv" style="margin: auto; position: relative;">
    <div class="tip">
    <div class="tip1">xxxxxx</div>
    <div class="tip2">yyyyyy</div>
    </div>
    <div id="bulletin_div" class="bulletin" style="display:none;">
    <div class="bulletin_banner">
    <div id="closeImage" class="bulletin_op" onclick="opBulletin('
    </div>
    </div>
    <div class="bulletin_content_out">
    <div class="bulletin_content_inside">
    <c:out value='${normalNotificationBulletin}' escapexml:
    </div>
    </div>
    </div>
    <div id="formDiv" class="form div">
  
```



Q17: What Do I Do When the Prompt "smp_access_ip_used_by_online_user is used by the user" Is Displayed?

Fault symptom: The prompt "smp_access_ip_used_by_online_user is used by the user" is displayed in the authentication failure log on the Web page of the SMP. The address that reports the error is checked and it is found that the address is occupied by an online user (the online duration is long).

Troubleshooting

1. Check whether multiple DHCP servers assign the same IP address. (Ensure that the communication is normal, ping the online user to check whether the user is actually online.)
2. After checking that the user is actually online, check the configuration on the Network Access Switch (NAS) and SMP.

NAS configuration: Check the update period on the AC:

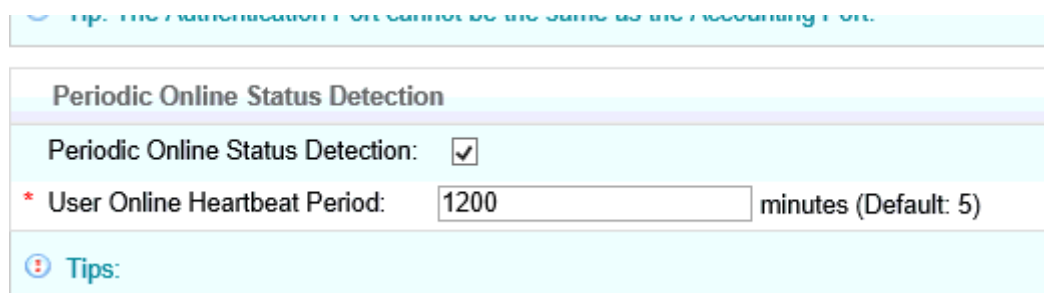
WS6008(config)#offline-detect interval 15 threshold 0 This command indicates that a user is forced to go offline when there is no traffic of the user within 15 minutes (8 hours by default).

WS6008(config)#aaa accounting update periodic 5 This command indicates that the accounting update period is 5 minutes by default.

Configuration on the Web page of the SMP: Check the user heartbeat detection interval.

If a non-SA client is used for authentication, the accounting update mechanism is adopted to keep online users alive. Enable the accounting update function on the device of the non-Ruijie security agent client and set the accounting update period to be consistent with the online heartbeat interval of the user.

If an SA client is used for 802.1x authentication, the heartbeat mechanism is adopted to keep online users alive. If the system fails to receive a heartbeat notification from an online user within three consecutive online heartbeat periods, the system considers that the user is offline and clears the user information.



The preceding figure shows an example of incorrect configuration. User Online Heartbeat Period is set to 1200 minutes, indicating that a user is forced to go offline after the system fails to receive a heartbeat notification from the user within three such periods (that is, 60 hours).

Q18: How Do I Rectify the Fault That a CA Certificate Error Is Prompted Before 802.1x Authentication Is Performed on a User?

Fault Symptom

A CA certificate error as shown in the following figure is displayed when 802.1x authentication is performed on a user.



Possible Causes

- Step 1. Disable 802.1x authentication. Check whether the connection is successful and whether an address can be obtained. Ensure that the network can be connected normally.
- Step 2. Use a mobile phone to perform 802.1x authentication.
- Step 3. Check the system status of the SMP and check whether prompts such as CA certificate expiration are displayed.
- Step 4. If no exception is found in Steps 1-2. Import the latest CA certificate for authentication.

Q19: What Do I Do When the PC Username on the Domain Controller for Authentication Is host/xxxx.xx?

Scenario Description:

A customer uses an AC to associate with the SMP and uses an AD domain controller as the authentication server. All PCs in the customer scenario are added to the domain controller, and PC usernames used for login are already added to the domain controller group and synchronized to the SMP server. (The domain controller group and members are already configured.)

Customer expectation: PC users log in from the Windows PC and click Wi-Fi to connect to the wireless network. The users do not need to enter the usernames or passwords, and the PCs automatically use the Windows credential for authentication.

Fault Description:

After most PCs served by the domain controller are connected to the wireless network associated with the domain controller, two errors as shown in the following figures occur. (When a PC attempts to connect to the wireless network multiple times, the user sometimes can use the username to log in successfully, for example, the username is KINGSLEY\shamundeswary.)

AllNone	User Name	Authentication Date	NAS IP	User IP	User MAC	Cause of Failure
<input type="checkbox"/>	host/shamundeswarykingsley.local	2016-09-18 14:48:44	10.10.100.253		34E6ADC37B7	The user name cannot exceed 32 bytes
<input type="checkbox"/>	host/shamundeswarykingsley.local	2016-09-18 14:46:16	10.10.100.253		34E6ADC37B7	The user name cannot exceed 32 bytes

AllNone	User Name	Authentication Date	NAS IP	User IP	User MAC	Cause of Failure
<input type="checkbox"/>	hostpriya.kingsley.local	2016-09-18 15:53:00	10.10.100.253		A402B9E0C47D	Remote Windows AD domain authentication failed. Cause: The user name does not exist.

Locating:

See the domain controller settings.

Solution:

In the domain controller settings, Windows users are configured to use their hostnames by default instead of their usernames to send authentication information.

In addition, run the `gpupdate /force` command on the CLI to update the group policy.

Q20: What Do I Do When the System Gives no Response After a User Enters the Username and Password and Clicks Log In on the Web Management Page?

Symptom:

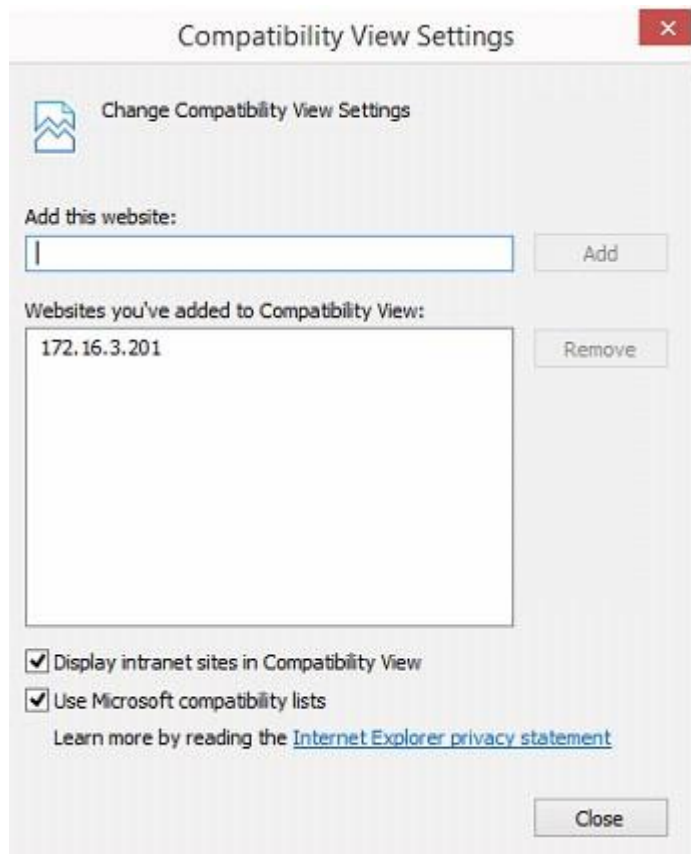
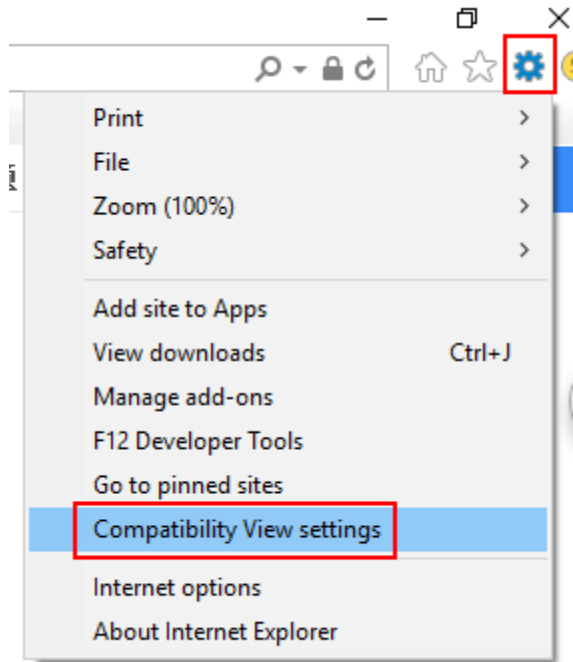
A user accesses the Web management page of the SMP, for example, the user enters <http://172.16.3.201:8080/smp> in the address box of browser. Then, the user enters the default username and password (admin and 11111111), and clicks Login. The system does not respond.



Root Cause:

The compatibility mode is disabled on the browser. Perform the following operations to enable the compatibility mode (note that some PCs support user login even if the compatibility mode is disabled).

1. The following uses Internet Explorer 10 as an example. Enable the compatibility mode and add the address of the SMP server to the compatibility mode range.



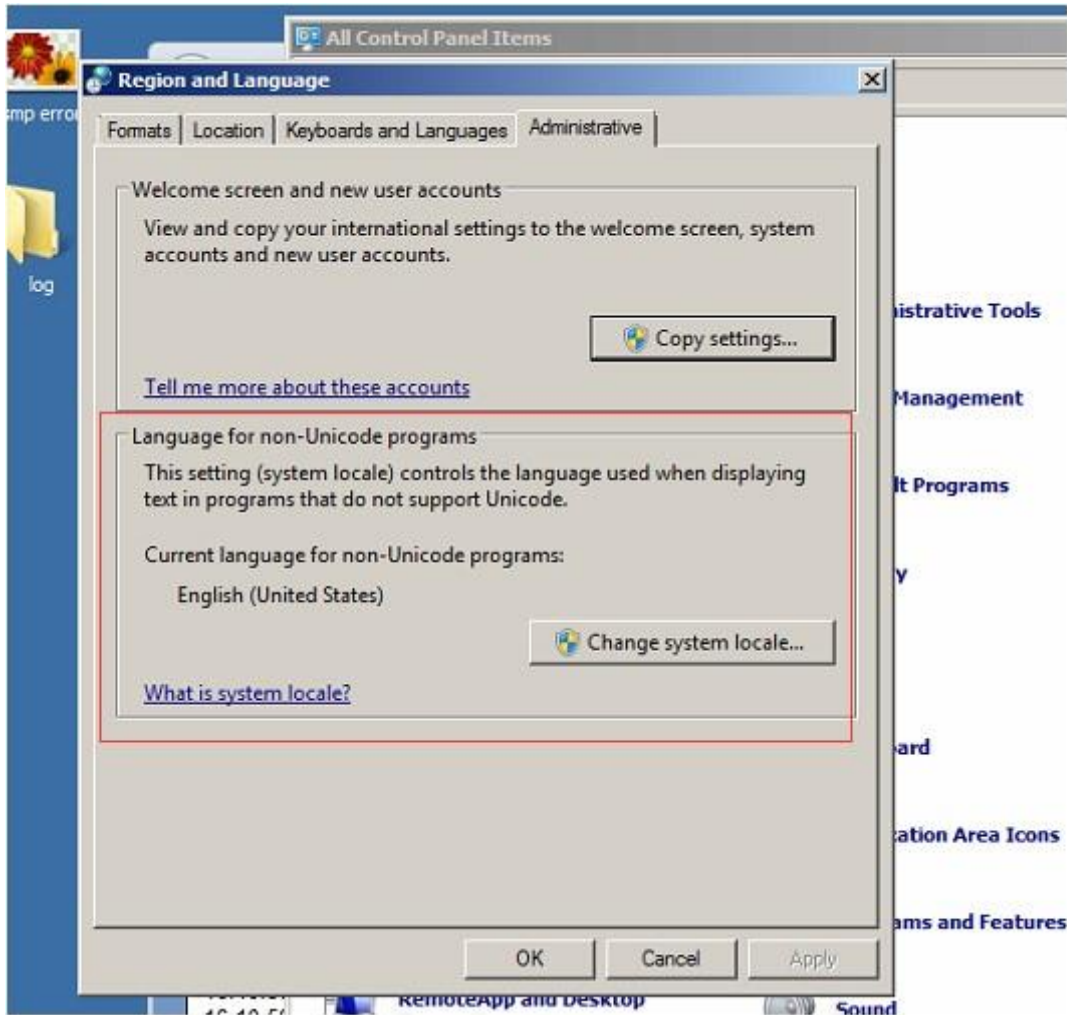
Note: If the fault persists, run the netstat -ano | findstr 8080 command on the SMP server to check whether Port 8080 is occupied.

```
C:\Users\harshit.singhal>netstat -ano | findstar 8080
'findstar' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\harshit.singhal>netstat -ano | findstr 8080
TCP        172.16.3.201:8080      0.0.0.0:0             LISTENING          1708
TCP        172.16.3.201:8080      192.168.113.164:49874 TIME_WAIT          0
TCP        172.16.3.201:8080      192.168.113.164:49875 TIME_WAIT          0
TCP        172.16.3.201:8080      192.168.113.164:49876 TIME_WAIT          0
TCP        172.16.3.201:8080      192.168.113.164:49877 TIME_WAIT          0
TCP        172.16.3.201:8080      192.168.113.164:49878 TIME_WAIT          0
TCP        172.16.3.201:8080      192.168.113.164:49879 TIME_WAIT          0
TCP        172.16.3.201:8080      192.168.113.164:49880 TIME_WAIT          0
TCP        172.16.3.201:28080    0.0.0.0:0             LISTENING          1708
```

Q21: How Do I Do When the SMP Server Needs to Be Modified to Support the Chinese Coding Mode?

Log in to Windows 2008, choose Control Panel > Clock, Language, and Region > Change Display Language and perform operations as shown in the following figure.



4.2 SNC

Q1: How to log in to the MySQL database?

On the SNC server, open the command prompt and enter the default installation directory C:\Program Files\MySQL\MySQL Server 5.1\bin (change the directory based on practical conditions), and run `mysql -uroot -padmin -P3307`. Log in to the MySQL using the user name root, password admin, and port No.3307, as shown in the figure below:

```

CA 命令提示符 - mysql -uroot -padmin -P3307
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd C:\Program Files\MySQL\MySQL Server 5
.5\bin

C:\Program Files\MySQL\MySQL Server 5.5\bin>mysql -uroot -padmin -P3307
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 307
Server version: 5.5.19 MySQL Community Server (GPL)

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> _
    
```

Q2: How can I restore the password for the SNC admin if I forgot it?

On the SNC server, open the command prompt locally, and enter the directory C:\Program Files\MySQL\MySQL Server 5.1\bin. Run `mysql -uroot -padmin -P3307` to log in to the MySQL, and run the following two commands:

```

Use emp;
update t_security_app_user set password = '21232f297a57a5a743894a0e4a801fc3' where id = 1;
    
```

If a message Query OK is displayed, the password has been restored to the default one, namely admin. If the information marked in red boxes in the following figure is displayed, the configuration is successful.

```

Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files\MySQL\MySQL Server 5.1\bin

C:\Program Files\MySQL\MySQL Server 5.1\bin>mysql -uroot -padmin -P 3307
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 52
Server version: 5.1.30-community MySQL Community Server (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> use emp;
Database changed
mysql> update t_security_app_user set password = '21232f297a57a5a743894a0e4a801f
c3' where id = 1;
Query OK, 0 rows affected (0.00 sec)
Rows matched: 1  Changed: 0  Warnings: 0

mysql> _
    
```

Q3: How to backup and restore the MySQL database of SNC?

The SNC database is saved in the database folder under the SNC installation directory, but not in the MySQL installation directory.

Disable the SNC Service first, backup the entire database folder under the SNC installation directory, and replace the original database folder for restoration.

Note: Ensure that the versions of the SNCs are the same. For example, the database saved on SNC_2.30(p2)_EN_Build2015121 can be restored only to RG-SNC_2.30(p2)_EN_Build20151211.

Q4: The SNC service is started normally and the login page is displayed normally, but the system freezes up when the user name and password are entered.

If the SMP micro dongle is used, the SNC service can also be started, but the license displayed is incorrect. The SNC Web management page can be displayed, but the system freezes up when the user name and password are entered.

Q5: The SNC server cannot be started and is stuck on the Web Service Starting screen.

Step 1: Check whether the firewall is disabled.

Step 2: Check whether multiple network interface cards are used and disable the unwanted ones.

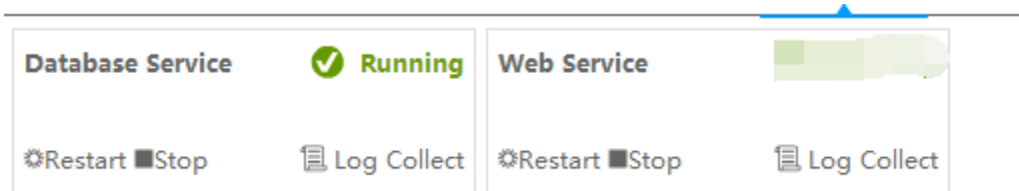
Step 3: Check whether MySQL services in the system is enabled; if not, enable the services manually.

Step 4: Check whether the MySQL Port 3307 of the database is occupied.

Step 5: Check whether ports snmp(udp161), ftp(udp69), syslog(udp514), and tcp8088 are occupied.

Step 6: Check whether the configurations of the hardware meets requirements, for example, whether the memory is too small.

Step 7: Choose Web Service > Log Collect to collect the logs and report it to Ruijie post-sales department.



Q6: The Device type is displayed as Unknown and no panel figure is displayed.

The fault may be caused by the following issues:

Step 1. The Simple Network Management Protocol (SNMP) and Telnet templates are configured incorrectly.

Check whether the SNMP and Telnet templates are correct.

Step 2. The SNC is unreachable for the device.

Check whether the SNC server and the device can be pinged.

Step 3. The device model is not supported by SNC and a customization is required.

- a) Choose Device > Select a device > Basic Info, and obtain the SysOID.

Basic Info	CPU	Memory	Temperature	Alarm
VSU-S57			IP	172.29.2.254
Switch			Model	s5750-24gt/8sfp-e
Ruijie Networks			SysOID	1.3.6.1.4.1.4881.1.1.10.1.111
255.255.255.0			MAC Address	14:14:4b:7d:00:7b
			Device Location	
14 days, 18:28:30.37			Last Synchronization Time	2016-01-01 16:35:49 Sync

- b) Provide the device model and panel figure.
- c) Report the information to Ruijie, and we will customize the panel based on practical conditions.

Q7: Does the SNC support the device of 3rd Party manufacturers?

The SNC manages a device using the SNMP and Telnet. The devices from other manufacturers should support the SNMP and Telnet. The SNC supports the standard request for comments (RFC) management information database (MIB). However, the SNMP may vary with different manufacturers, and the MIB may not fully conform to standards (some manufacturers may realize the functions supported by a standard MIB in a private MIB). Therefore, the functions vary with different devices.

Q8: What is the update interval for the different modules on SNC?

Step 1: For the devices that are added to the monitored device list and are displayed in Top N utilization on the SNC Home Page, the update interval is 5 minutes and such interval cannot be changed.

Step 2: For the devices that are added to the real-time monitored device list, the update intervals of the monitoring indicators can be changed, and it impacts the intervals of the single device view and all view. It does not impact the Top N utilization on the SNC Home Page.

Step 3: For Topology, The update interval 1 min and cannot be changed. If an alarm, for example, a link down alarm, is generated in the update interval, the SNC will not upgrade the status of the topology link immediately unless you click the synchronization button manually. The SNC will perform the updated status after 1 min interval.

Q9: There is no responding when telnet device via SNC.

Step 1: This fault is caused when the safety strategy of the Internet Explorer (IE) forbids the direct calling of Telnet in the IE. In this case, you can change the registration table by copying the following content to the notebook, save it as a .rag file, and double click it to run the file.

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL]
```

"iexplore.exe"=dword:00000000.

If the fault persists, proceed to Step 2.

Step 2: Install SecureCRT on the PC, and choose Options > Global Options > Web browser to set SecureCRT as the default Telnet program, and try to telnet again.

Q10: Can the SNC monitor and manage the server or PC client?

The SNC can discover and display a terminal device in a topology, but can only display the basic information.

You need to enable the SNMP service on the server or PC, and configure the corresponding community string.

Service Faults

The Device Is Unreachable over SNMP and the Device Information Cannot Be Obtained

1. The SNC and device cannot ping each other.

Countermeasure: The network malfunctions. Ask the customer to help rectify the fault.

2. SNMP Port 161 is blocked by the firewall. Use the MIB tool to check whether the port is actually blocked by the firewall.

Countermeasure: The fault is caused by environment settings. Ask the customer to help rectify the fault.

3. No SNMP community string is configured for the device.

Countermeasure: Run the following command on the device (the command uses the community string public as an example): snmp-server community public rw

4. The SNMP community string configured on the device is inconsistent with the SNMP template on the SNC.

Countermeasure: Set the SNMP community string on the device so that it is consistent with the SNMP template on the SNC.

When SNMP Connection Is Reachable, the Device Model Cannot Be Identified and Unknown Is Displayed

1. The device model is not embedded. Choose Device > Device Model to check whether the model can be found.

Countermeasure: Choose Device > Device Model and add this model. You can check the sysoid on the device details page.

2. When the device is added, an incomplete MIB is obtained.

Countermeasure: Access the device details page and click Synchronize.

3. The device MIB is not implemented correctly. Access the device details page and check whether sysoid is set to a value..

Countermeasure: Reach out to us on Skype (Skype account :service_rj@ruijienetworks.com) at any time for assistance.

The CLI Shows That the Device CPU Usage, Memory Usage, and Temperature Are Low but a Threshold Exceeding Alarm Is Generated on the SNC

For all faults that information on the SNC is inconsistent with that on the CLI, rectify the faults as follows and use the MIB tool to obtain the oid value:

1. The value returned by the MIB tool is always high. Use the MIB tool to obtain the oid values of the CPU, memory, and temperature for verification.

CPU OID: .1.3.6.1.4.1.4881.1.1.10.2.36.1.1

Memory OID: .1.3.6.1.4.1.4881.1.1.10.2.35.1.1.1

Temperature OID in sequence: 1.3.6.1.4.1.4881.1.1.10.2.1.1.16.0 /1.3.6.1.4.1.4881.1.1.10.2.1.1.44.1.5/
1.3.6.1.4.1.4881.1.1.10.2.1.1.23.1.3

Countermeasure: Reach out to us on Skype (Skype account :service_rj@ruijienetworks.com) at any time for assistance.

2. The CPU usage, memory usage, and temperature soar instantaneously but the values returned by the MIB tool are within the normal range. Start packet capture on the SNC server to capture SNMP packets. Determine the observation period based on the fault occurrence frequency and analyze the SNMP packets that are captured in the observation period to check whether the CPU usage, memory usage, and temperature soar instantaneously.

Countermeasure: None. It reflects the real status of the device. If the alarm can be ignored, you can cancel performance monitoring of the device.

The Device Is Reachable but an Unavailability Alarm Is Reported on the SNC

1. It is true indeed that the device is unreachable at some time. Capture ICMP packets on the SNC server for verification and determine the observation period based on the alarm occurrence frequency.

Countermeasure: Ask the customer to locate and rectify the network fault. If the alarm can be ignored, you can enable the device not to generate the unavailability alarm in the alarm event.

Failure to Backup Configuration

1. The telnet template is configured incorrectly.

Countermeasure: Change the telnet template parameters to be consistent with actual parameters.

2. The network does not work properly. Run the following command on the device for verification: copy flash:config.text tftp://SNC-IP/a.text.

Countermeasure: Ask the customer to rectify the network fault.

3. The device model is unknown.

Countermeasure: Connect the device to the SNC over SNMP successfully. If the device cannot be identified yet, manually add the device model.

4. The device name contains special characters such as #.

Countermeasure: Remove special characters such as #.


The Topology Is Incomplete

1. Key devices (core device or convergence device) are not included for management.

Countermeasure: Configure an SNMP community string for the key devices, and enable device auto-discovery so that the key devices could be managed.

2. The **Complete L2 switch info.** Option is not selected.

Countermeasure: Telnet to many devices to ensure that the devices (all managed devices) are reachable, enable topology discovery, and select the **Complete L2 switch info.** Option.

Complete L2 switch info. 

No Syslog Are Generated

1. There is no relevant log server configuration on the device.

Countermeasure: Make relevant configuration.

2. Capture syslog packets on the SNC to check whether syslog packets are filtered out by the firewall.

Countermeasure: Modify the firewall policy.

System Faults

A Prompt, Indicating That Hardware Information Verification Fails, Is Displayed When a License File Is Imported, or a Prompt, Indicating That the Hardware Code Is Inconsistent with the Current Device, Is Displayed When the Web Service Fails to Be Started

1. The device whose hardware information is collected, is not the machine, into which the license file is imported.

Countermeasure: Use the current server to re-collect hardware information and go through the file license application process.

2. The license file of another server is imported.

Countermeasure: Import the license file of the current server.

3. The version of the device whose hardware information is collected, is incompatible with the version of the device, into which the license file is imported. For example, the version of the device whose hardware information is collected is vmotion whereas the version of the device, into which the license file is imported, is a universal version.

Countermeasure: If the version of the device whose hardware information is collected is not an expected version, install the expected version and re-collect hardware information. Therefore, go through the SNC server change process. If the version of the device whose hardware information is collected is an expected version, uninstall the current version, install the correct version, and import the license file.

4. The hardware information is changed during hardware information collection and license file importing.

Countermeasure: For a common version, this fault occurs when the main board, hard disk, or NIC is changed. In this case, reapply a license in the scene of host change and re-collect hardware information.

For the vmotion version, this fault occurs when the OS is re-installed (regardless of whether the OS of the physical machine or virtual machine is installed). In this case, reapply a license in the scene of host change and re-collect hardware information.

The Web Service Fails to Be Started

1. The memory is insufficient.

Countermeasure: Increase the memory to ensure that the minimum memory is 4 GB.

2. In case port conflict occurs, enable all ports, including the Web service port 8088 /TFTP port 69 /trap port 162 /syslog port 514/tomcat port 8080. Move the cursor over the Web service. A conflict prompt should be displayed. If no prompt is displayed, use the port viewer tool to locate and rectify the fault. For example, if Port 8080 conflicts, there is a high possibility that two java.exe files are found in the process.

Countermeasure: Uninstall the software that causes the conflict, change the port ID for the software, and disable relevant services.

3. This fault occurs in an upgrade scenario. The database of an earlier version is used for replacement or restoration after an upgrade.

Countermeasure: Data of the earlier version is inherited after the upgrade and no manual intervention is required. Use the database that is not manually intervened after the upgrade.

4. A version is newly installed and the database of an earlier version is used for replacement or restoration.

Countermeasure: Use the database of the version that is newly installed, to complete configuration and deployment.

5. The imported file license is lost, for example, there is wlan-license-100 but the WLAN license component is lost.

Countermeasure: The required licenses are not completely purchased or the license may be lost. Retrieve the complete license file and then import it.

The Web Service Automatically Stops for No Reason during System Running

1. Virtual machine migration occurs but a common version is installed, and the file license fails.

Countermeasure: Install the vmotion version, go through the host change process, and re-apply for the license file.

2. The test license expires.

Countermeasure: Contact local after-sales engineers to renew the license or purchase the formal license.

The MySQL Service Fails to Be Started and Error 1067 Is Reported When the Service Is Manually Started

1. The database is damaged because of an abrupt power failure of the server or other causes.

Countermeasure: Perform the following steps to restore device information. Other data needs to be re-configured. Before performing these operations, negotiate with the customer first.

- A. Stop the MySQL-SNC service. Access the SNC installation directory and open the \mysql\my.ini file, add innodb_force_recovery=6 (if the database cannot be opened, set it to 1-5 in sequence for testing) to the end of the file. Then, start the MySQL-SNC service.
- B. Install navicat and run the following command to configure a database connection: localhost 3307 root admin.
- C. Right-click the et_telnet_tmpl and et_snmp_tmpl tables and choose Dump SQL File from the shortcut menu to back up the et_telnet_tmpl and et_snmp_tmpl tables.
- D. Open the et_device table, open the asset import template, and enter IP addresses in the Device IP column in the template, and enter the SNMP template name and Telnet template name (can be found in et_telnet_tmpl and et_snmp_tmpl) corresponding to snmptmpl_id and telnettmpl_id in the snmp\telnet template in the asset template.
- E. Uninstall and then re-install the SNC. Start navicat, restore the et_telnet_tmpl and et_snmp_tmpl tables, and then import the edited asset template.

A Lot of Accessed Web Pages Are Abnormal, the Web Service Is Abnormal, or the Web Service Is Always Starting

- 1. The disk where the SNC installation directory is located is fully occupied.
Countermeasure: Expand the disk, clear unnecessary files, or re-install the SNC to a disk with sufficient space.
- 2. The MySQL service is abnormal. Access the OS management tool and check whether a large number of errors are generated for the MySQL service in the event manager.
Countermeasure: Refer to the case that error 1067 is reported when the MySQL service is started.

When a License File Generated by the Dongle Is Imported After a Host Change, a Prompt Is Displayed, Indicating That No Dongle Is Inserted and the License File Cannot Be Imported

- 1. The license process is not performed in this scenario.
Countermeasure: Copy the license file to the SNC installation directory \snc\WEB-INF\classes\ and then start the Web service.

4.3 SAM

Q1: What Are Precautions When 802.1x Authentication Is Conducted Using the SAM+ System and Wireless Device?

When the authentication client that comes with Windows is used for 802.1x authentication, Access Control must be set to Smart Device Access in the SAM+ system. Otherwise, authentication fails.

Q2: What Are the Steps of Setting the Authorization QR Code?

Step 1: Create a Guest Guarantor

Choose System > Guest Mode from the main menu to access the Guest Authentication Setup page. Click Add Guest Guarantor Ranking to create a Guarantor.

Guest Authentication Setup

Guest Account Creation by SMS: Enabled Disabled

Authorization Code Mode:

Public Mode:

Guest QR Code Feature: Enabled

Add Guest Guarantor Ranking

Ranking Name	No. of Guests	Max Duration	Homepage	Check	Modify	Delete
test1	12	2Hrs	172.29.2.2:8080/sam			
QR1	1	1Hrs	WWW.BAIDU.COM			
QR2	1	1000Hrs	www.baidu.com			
QR3	1	1Hrs	www.baidu.com			
QR4	1	1000Hrs	www.baidu.com			

Guest Guarantor Ranking

Ranking Name*

Max Guest Number* Users

Max Duration* Hrs

Homepage*

Allow to change homepage Allow

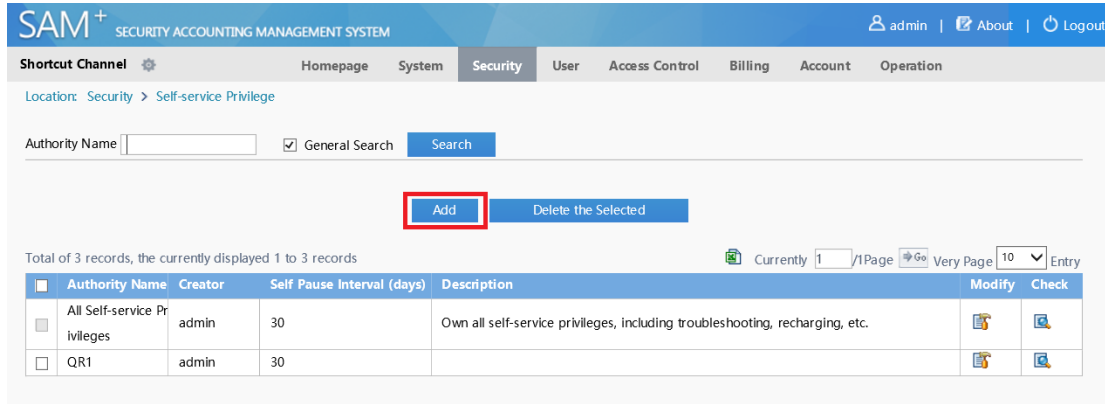
Guest's User Group*

Free User Template

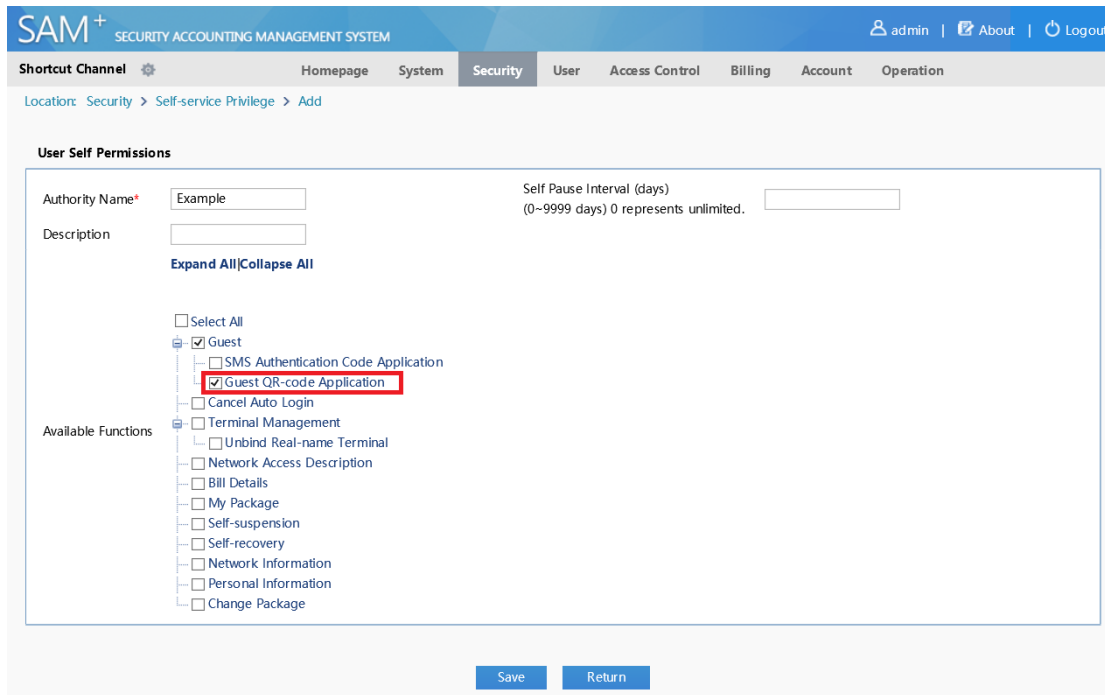
Free Plan Free

Step 2: Set the self-service privilege

Choose Security > Self-service Privilege from the main menu to access the Self-service Privilege page. Click Add to add a user self-service permission.



Select Guest QR-code Application in Available Functions.



Step 3: Create a user

Choose User > User Management from the main menu to access the User Management page. Click Create Account to add a user.

SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM admin | About | Logout

Shortcut Channel **User Search** | Homepage | System | Security | **User** | Access Control | Billing | Account | Operation

Location: User > User Management

User Search

Import Search

Create Account

Batch Account Activation

Import Accounts

Import Changes

Import Payments

Import Change User Templates and Plans

Import Change User Group

User Search

Username Multiple Usernames

Account

Balance -

User Templates Please Select

Plan Please Select

Billing Policy Please Select User IP(v4) Range

User Group Contains The Child User Groups Account Creation Time

Account Creation Source Please Select Account Pre-Cancellation Time

Recent Offline Duration 1 Week Inactive Network Users Within This Period

Recently

from Inactive Network Users From

Pause Duration -

Last Self-service Pause Duration -

Search Reset

In Basic Information, select the created self-service permission and guarantor ranking.

SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM admin | About | Logout

Shortcut Channel | Homepage | System | Security | **User** | Access Control | Billing | Account | Operation

Location: User > User Management

User Search

Import Search

Create Account

Batch Account Activation

Import Accounts

Import Changes

Import Payments

Import Change User Templates and Plans

Import Change User Group

Basic Information

Username* Example Full Name

Password* Confirm

User Group* Account Same As username

User Templates Use Default Template of User Group Customize

Self-service Permission Example Authentication-free Verification is required

Auto Pre-Cancellation BAACL Please Select

Guarantor Ranking Example

Advanced Options Show Advanced User Settings options

Sex Please Select Email Address

ID Type Please Select ID No.

Education Level Please Select Online Information

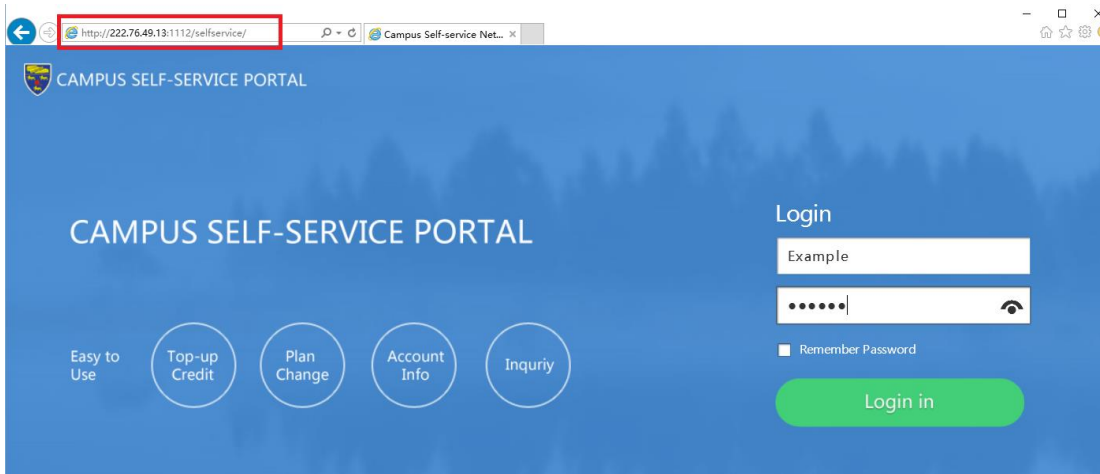
Telephone No. Mobile Phone

Address Postal Code

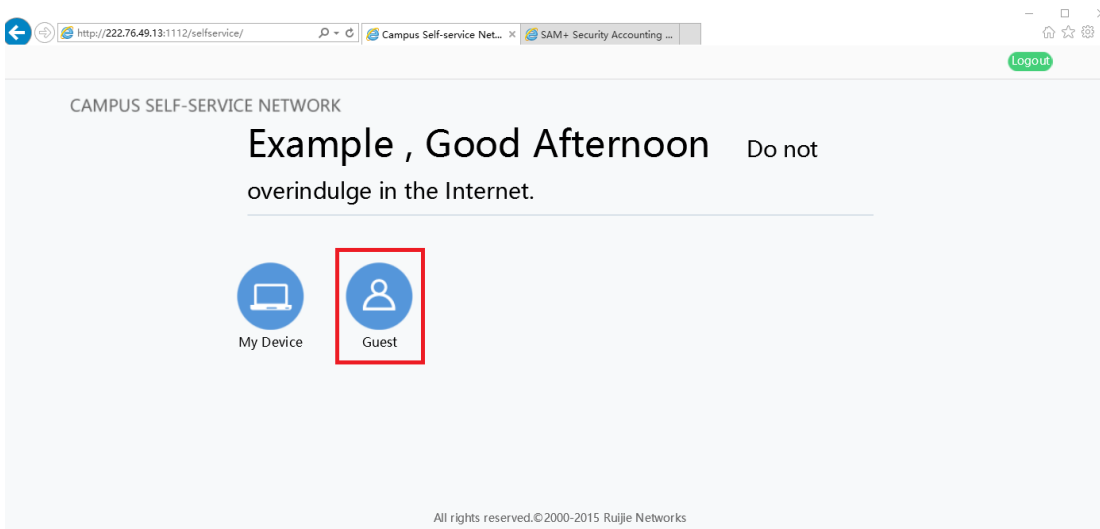
Save Reset

Step 4: Generate an authorization QR code

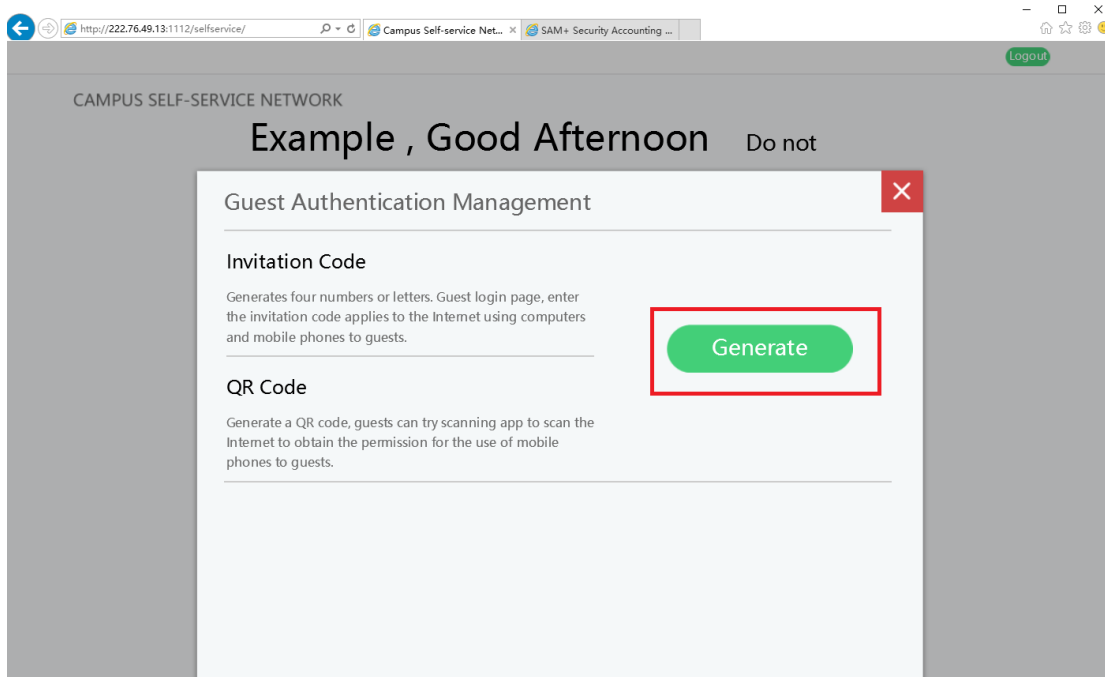
Enter the self-service platform address <http://xxx.xx.xx.xx:xxxx/selfservice/> in the address box of the browser, and then enter the created username and password for login.



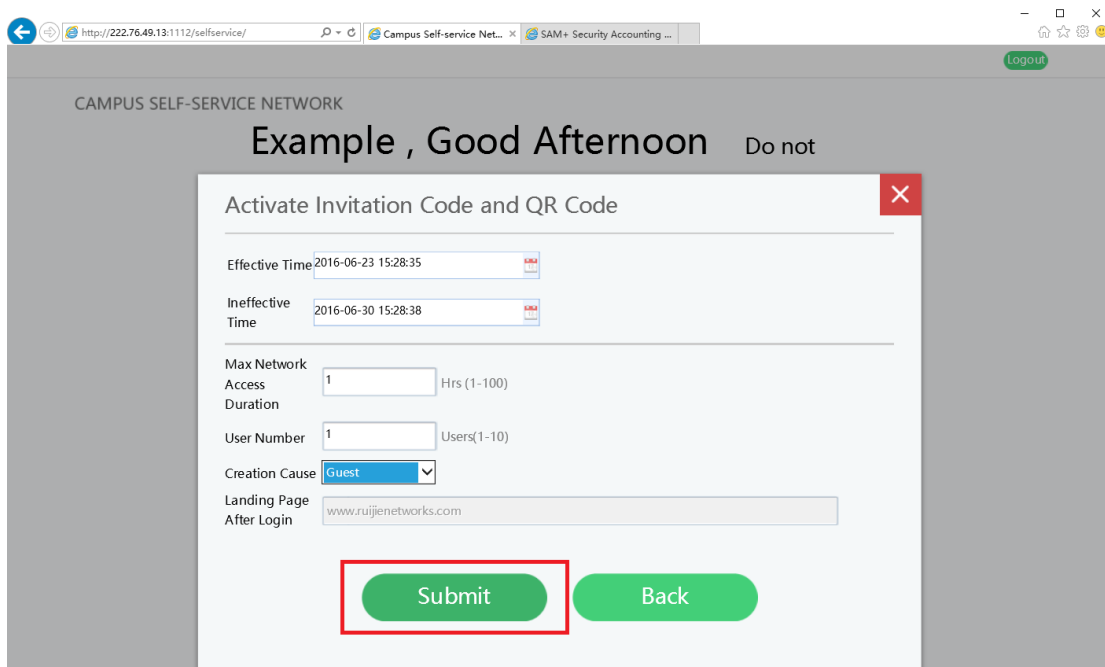
Click Guest on the user home page.



Click Generate in the displayed Guest Authentication Management dialog box.



Set authorization QR code parameters and then click Submit.



The QR code is generated successfully, as shown in the following figure.

