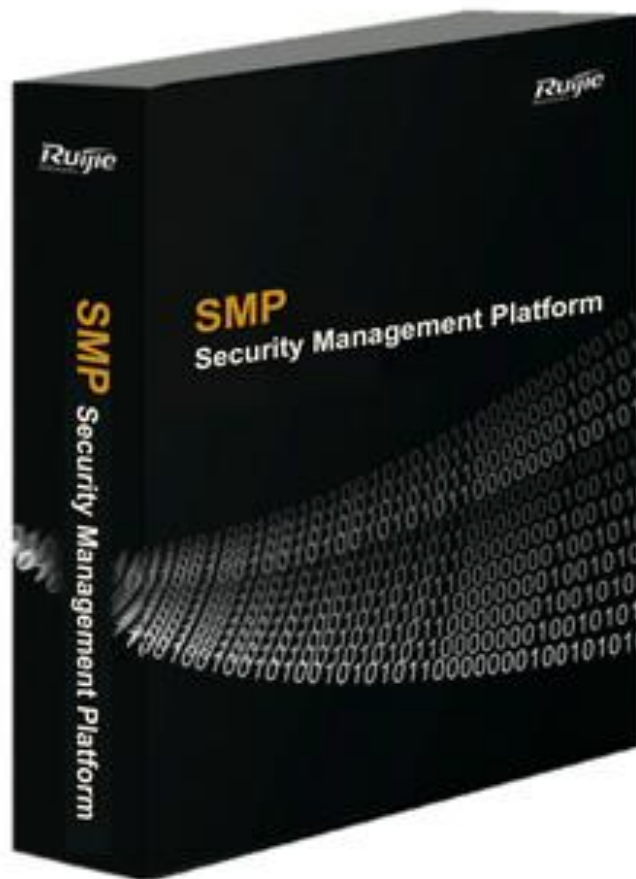




Ruijie Networks Co.,Ltd.



# SMP Implementation Cookbook V1.2

For SMP EN 2.63

## Preface

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.

*This cookbook is applicable for RG-SMP version 2.63\_EN\_Build20151106 and later version*

## 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-SMP Release Note
- RG-SMP Installation Guide
- RG-SMP Database Installation and Maintenance Guide

- RG-SMP Operation Guide

## Revision History

Date	Change contents	Reviser
2015.12	Initial publication V1.0	Scott
2016.07	Add SQL Server Installation V1.1	Oscar
2017.05	Adjust format	Oscar

## IP addresses and object names

In command configuration section, IP addresses and object names are shown for easy reading purpose. You should substitute your own IP addresses and object names when you configure your own product. Especially, it is not recommended to copy and paste the commands directly when you configure Ruijie wireless controller and switch for the first time. At least , you should identify which words stand for command , which stand for parameters or object names. You might input a question mark “?” to show available commands if required.

# Contents

Preface	2
Contents	5
1 Daily Maintenance	7
1.1 Login Web UI	
1.2 Check System Status	8
1.3 Installing the SQL Server	8
1.3.1 Installing SQL Server 2008 Enterprise Edition	9
1.3.2 Installing SQL Server 2012 Enterprise Edition	33
1.4 Backup Database	60
1.5 USB Dongle and License Management	61
2 Practical Scenarios	62
2.1 Wired Authentication	62
2.1.1 802.1x Authentication	63
2.1.2 Mac Authentication	67
2.1.3 Web Authentication	69
2.2 Wireless Authentication	72
2.2.1 Seamless 802.1x Authentication (BYOD)	73
2.2.2 Mac Authentication	77
2.2.3 Seamless Web Authentication (BYOD)	79
2.3 Authentication for Guest	84
2.3.1 QR Code Authentication (BYOD)	85
2.3.2 QR Code Card Authentication (BYOD)	91
2.3.3 Exemption Authentication (BYOD)	96
2.3.4 Staff Self-Service Guest Management	99
2.4 Integration with Windows Active Directory	100
3 Common Features	111
3.1 Access Control	111
3.2 Behavior Restrict	113
1.1.1 Multi-Access Limit	113
1.1.2 Offline Timer	114
1.1.3 Network Access Prohibited Period	116
3.3 Bulletin Information	117
3.4 Disclaimer Page	118
4 User Self-Service Management	120
5 Trouble Shooting	123
5.1 Authentication Failure Logs	123
5.2 Collect SMP Logs	123
6 Appendix	124

6.1	Ruijie Security Agent (SA)	124
-----	----------------------------	-----

# 1 Daily Maintenance

Before getting started, verify that you install Microsoft SQL Server and RG-SMP, then start SMP Service correctly.

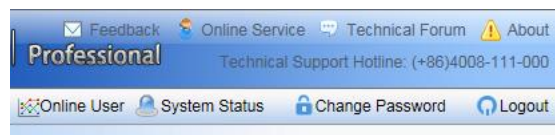
For Database and SMP installation, see *RG-SMP Installation Guide* and *RG-SMP Database Installation and Maintenance Guide*

## 1.1 Login Web UI

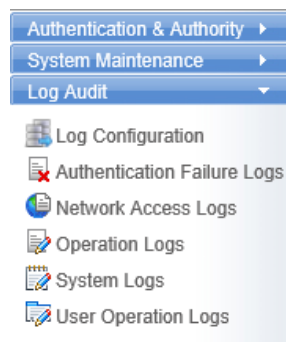
When you complete SMP installation and start SMP service successfully, visit SMP web UI at [http://Server\\_IP:8080/smp](http://Server_IP:8080/smp) or [https://Server\\_IP:8443/smp](https://Server_IP:8443/smp), the default Username is “*admin*” and password is “*11111111*”



**Note: Use IE 8.0 and above version in compatibility mode. Firefox and chrome may have compatible issues.**

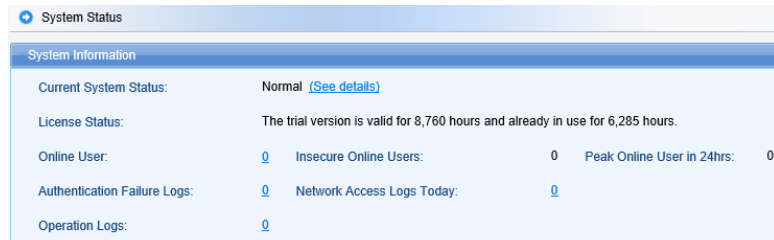


It is recommended to change password when login. Click “Change Password” in the top right on WEB UI.

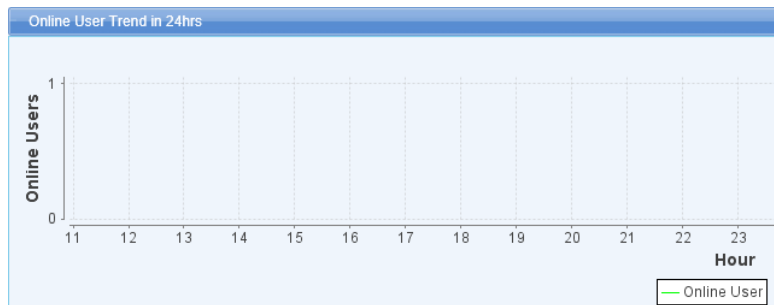


In this left side, it is the menu as shown, it includes three main components: *Authentication & Authority*, *System Maintenance* and *Log Audit*.

In the middle of the window, it is **System Status**



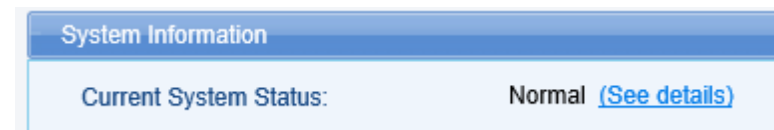
Under the system Information, it is the **Online User Trend in 24 hours**.



## 1.2 Check System Status

Click **System Status** in the up right corner, you can view **Current System Status**. Usually, it displays **Normal** as shown in below diagram which indicates SMP works properly.

If it displays **Abnormal** as shown in diagram, something must be wrong, click **See Details** to check.



## 1.3 Installing the SQL Server

The RG-SMP supports the **Microsoft SQL Server 2005** or **SQL Server 2008** as well as the **SQL Server 2012** as the background database. The installation steps for the latter two are described as below.



### 1.3.1 Installing SQL Server 2008 Enterprise Edition

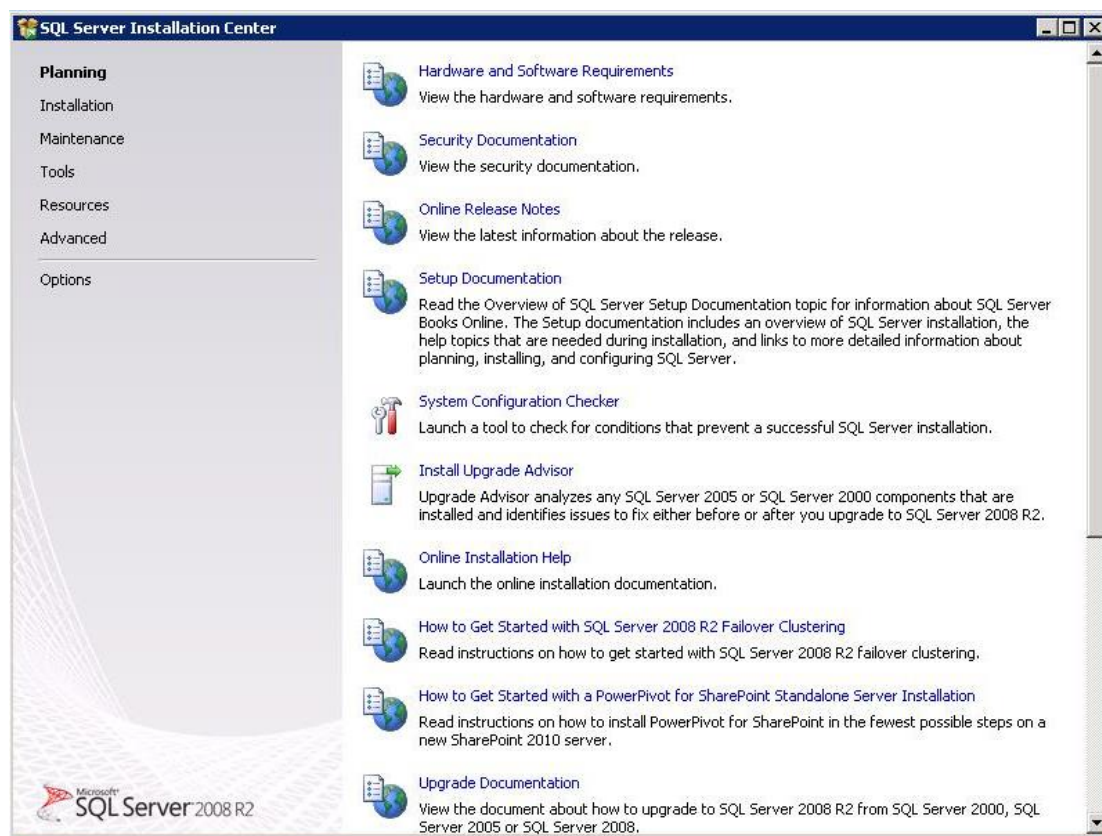
The operation of the RG-SMP system requires a background database. If you use the **Microsoft SQL Server 2008**, you must install the **Microsoft SQL Server 2008 Enterprise Edition**.

The **SQL Server 2008** is a large database server of Microsoft. This section describes the software and hardware configuration requirements for installing the **SQL Server 2008 Enterprise Edition**, detailed installation steps and notes.

- 1) Insert the CD of **SQL Server 2008 Enterprise Edition**, click **setup.exe**, and a message will be prompted asking whether to install the **NET framework**. Click **OK**.



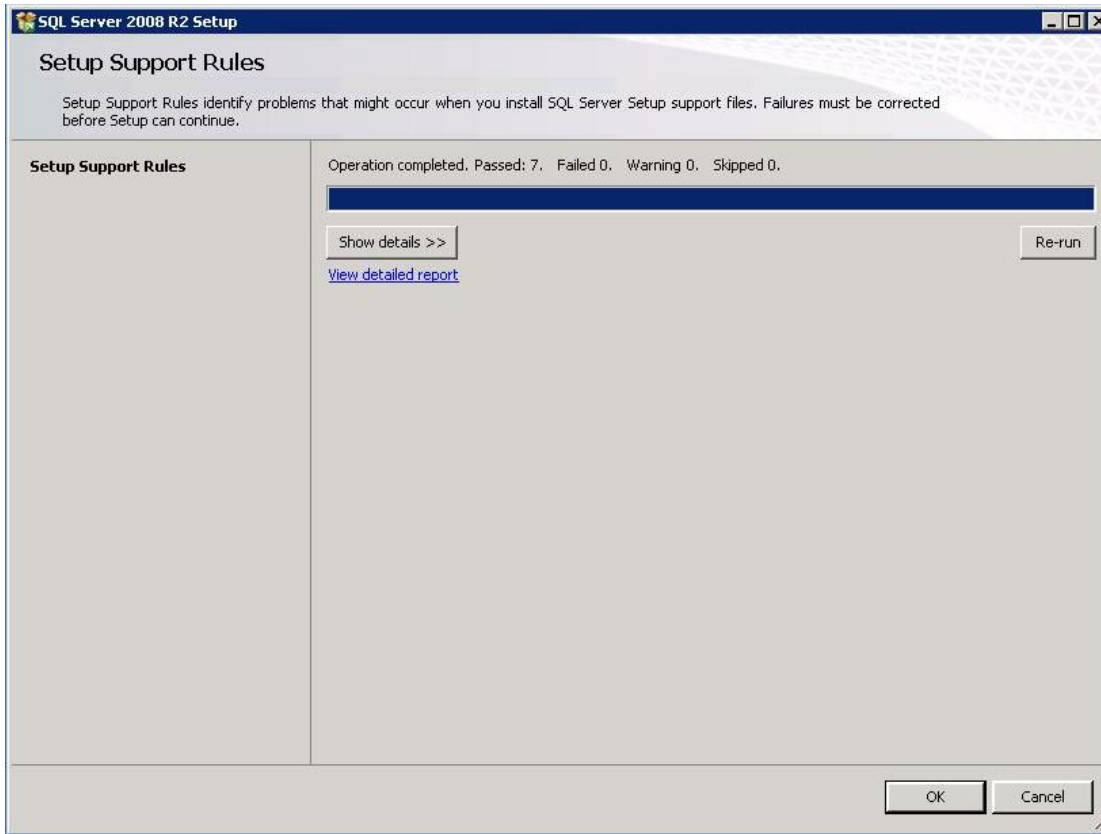
- 2) After automatic installation, the following interface is prompted.



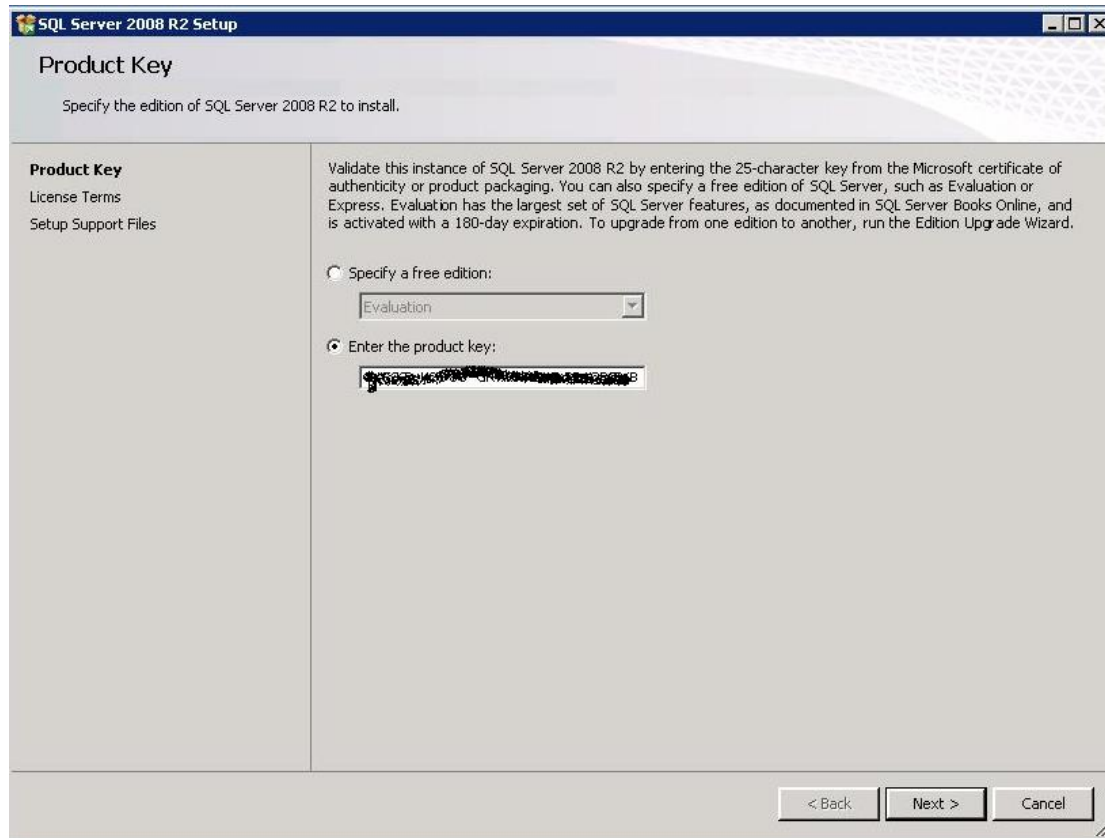
3) Click **Installation >New Installation or add features to an existing installation.**



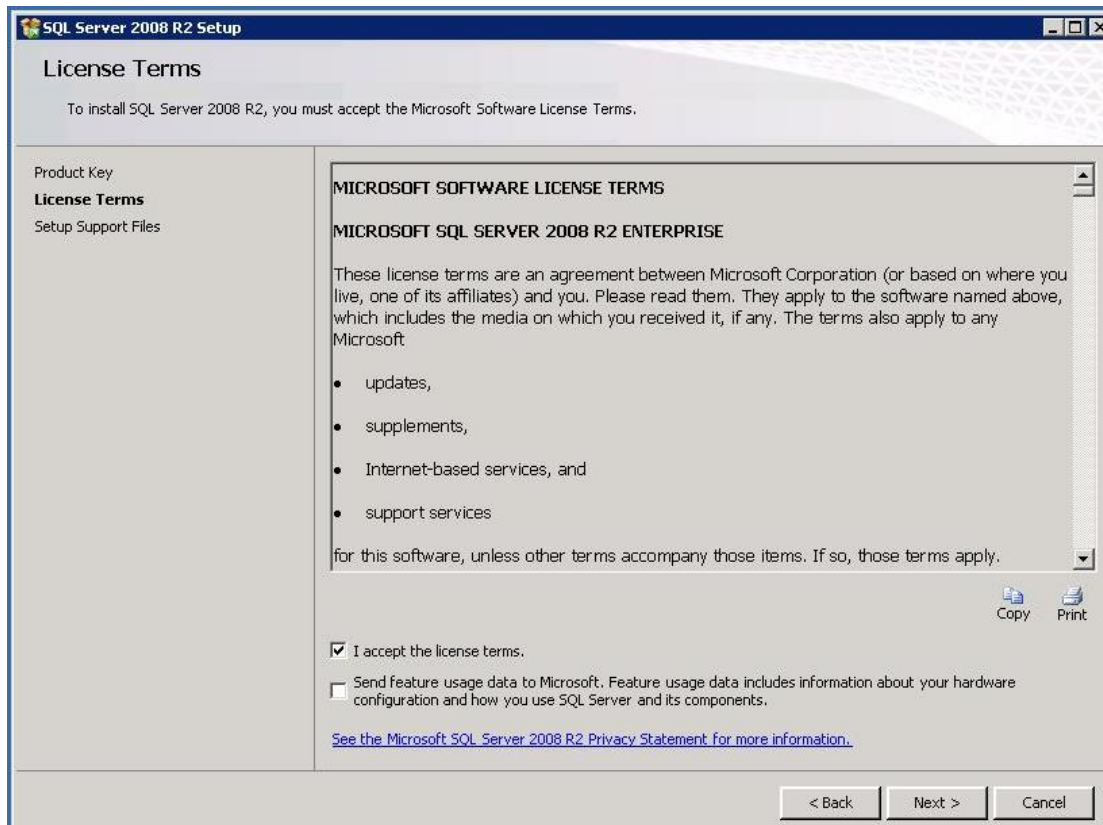
4) Click **OK.**



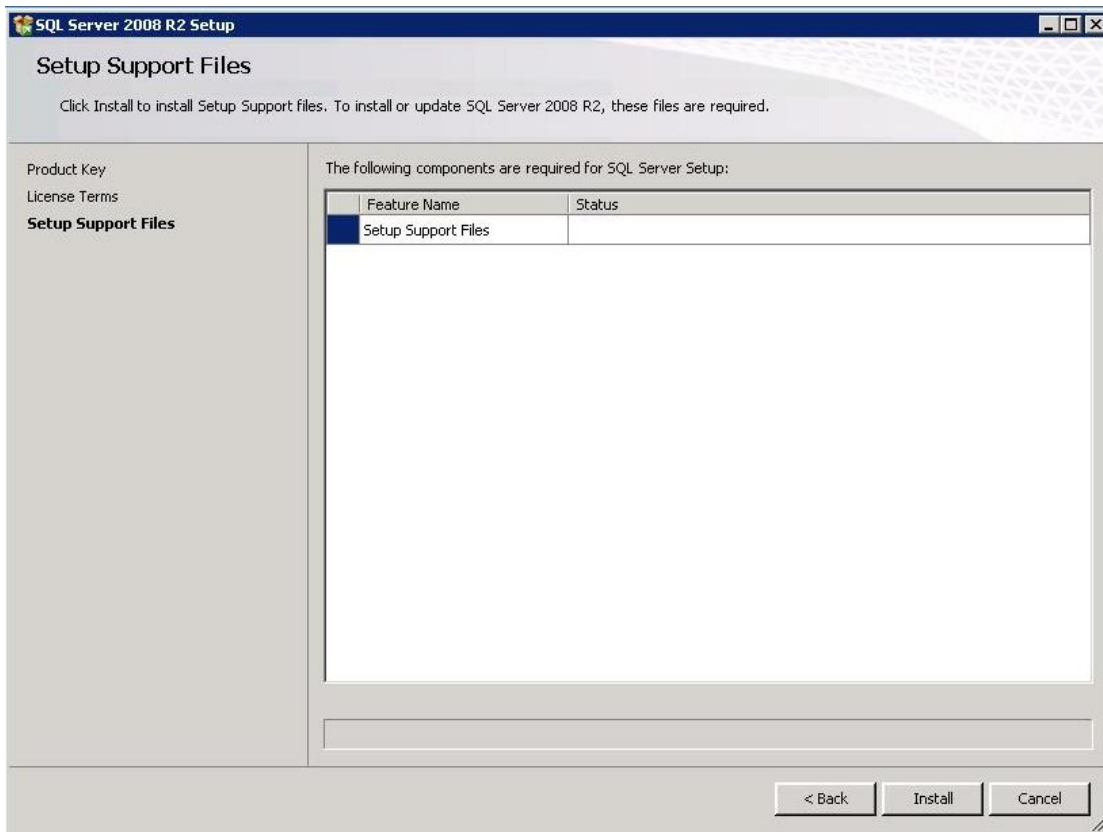
5) Click **Next**.



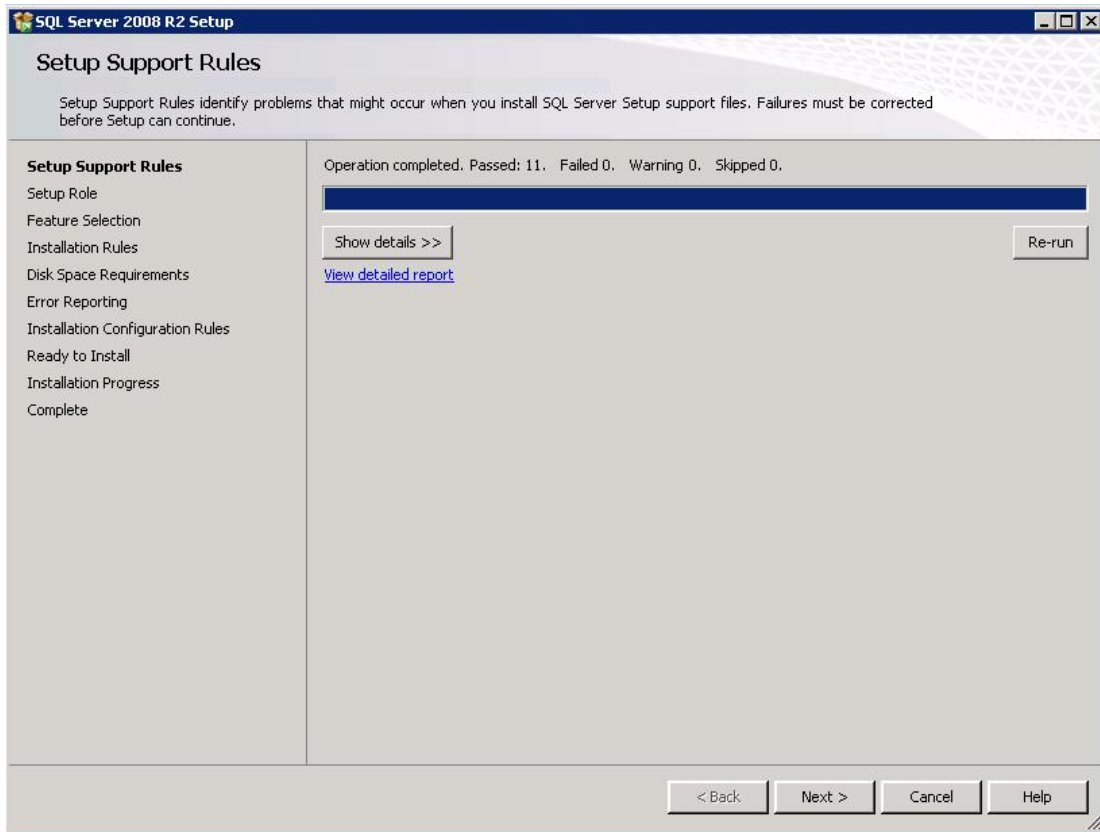
6) Tick **I accept the license terms**, and click **Next**.



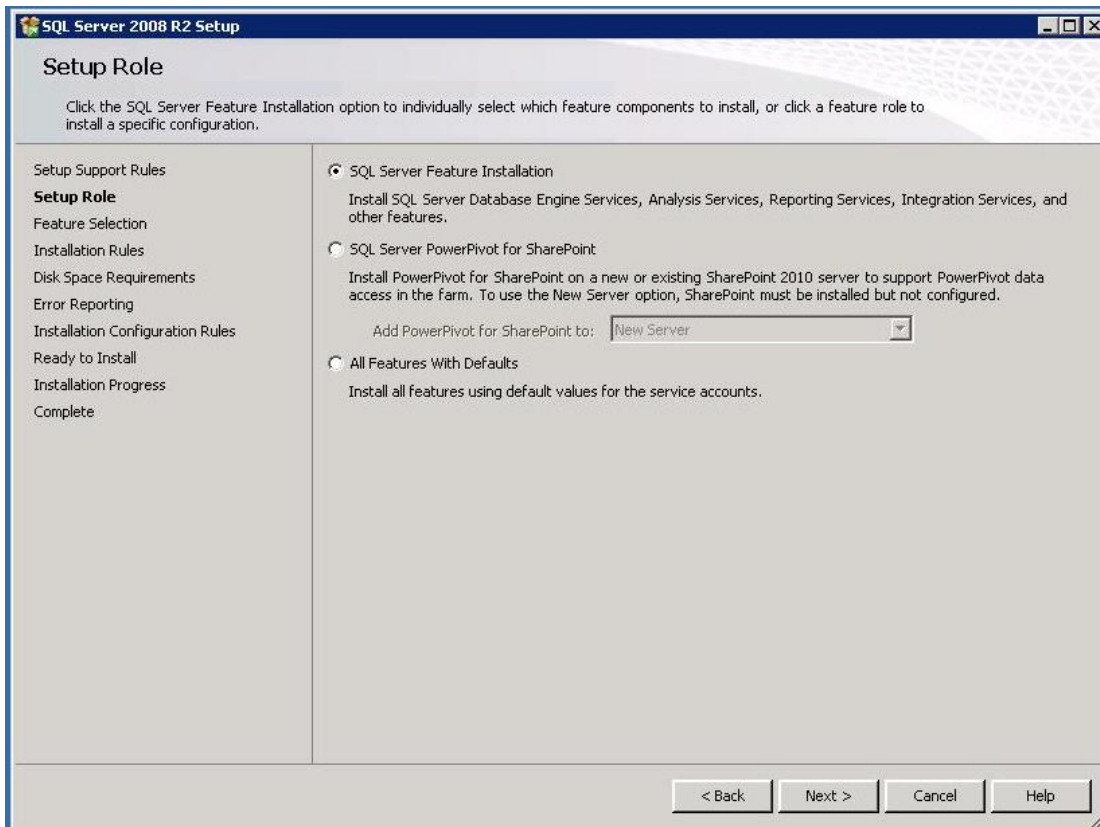
7) Click **Install**.



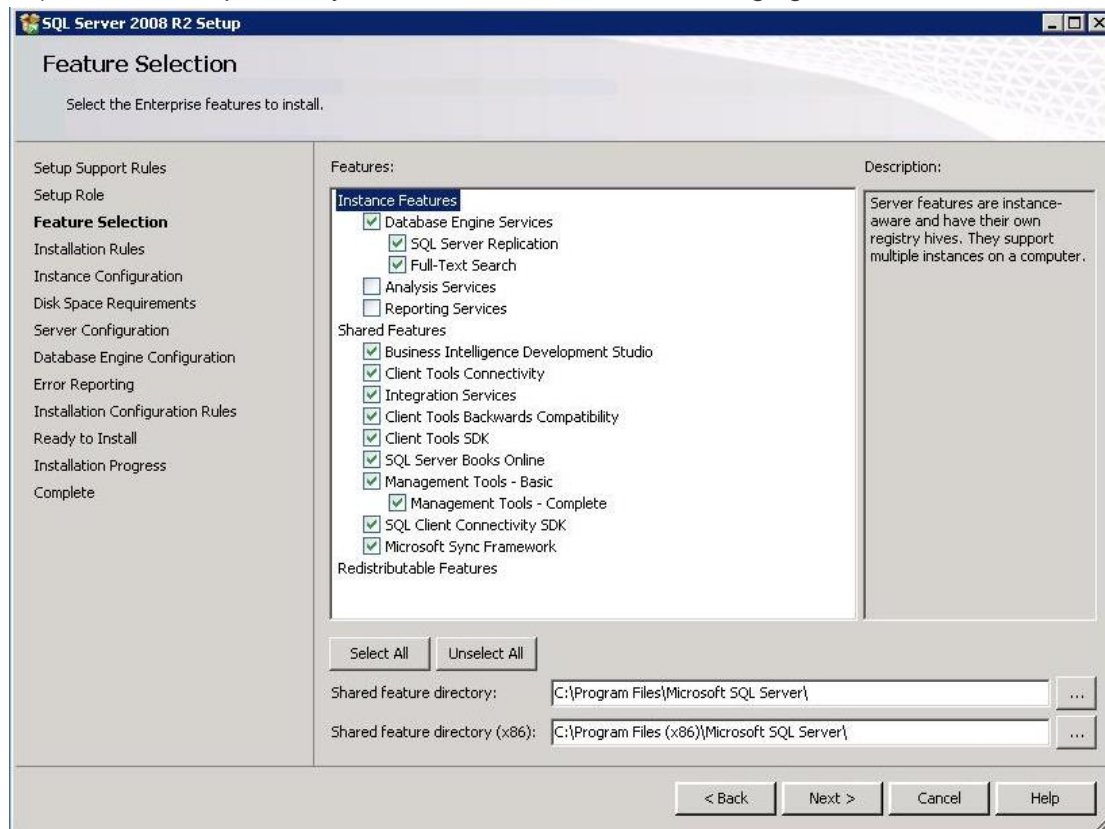
8) Click **Next**.



9) Click Next.

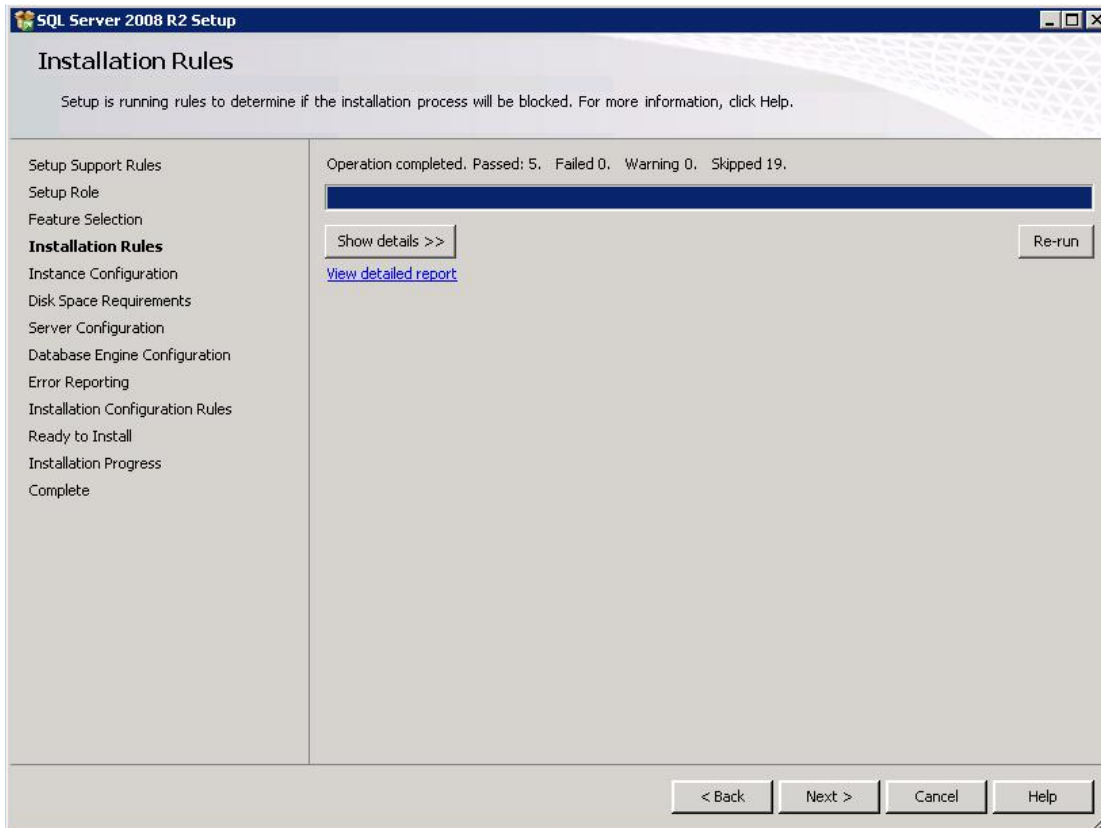


10) Tick the components you need as shown in the following figure, and then click **Next**.

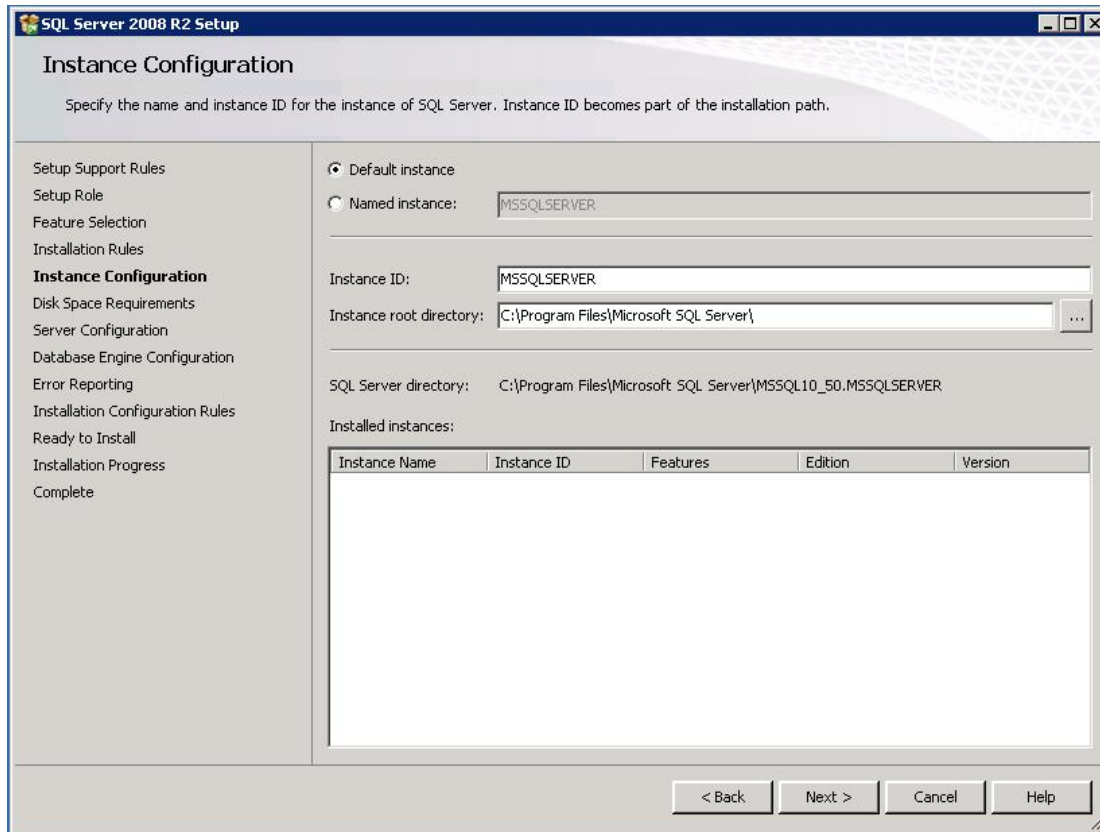


11) Click **Next**.

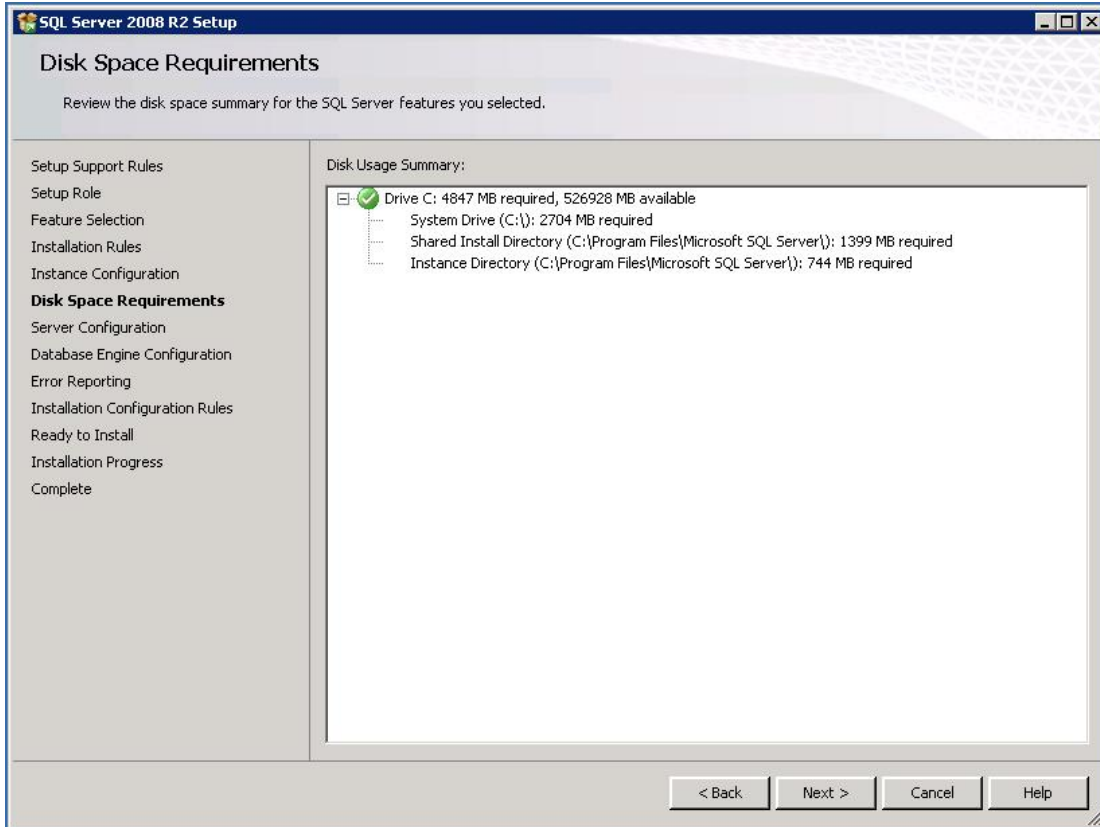




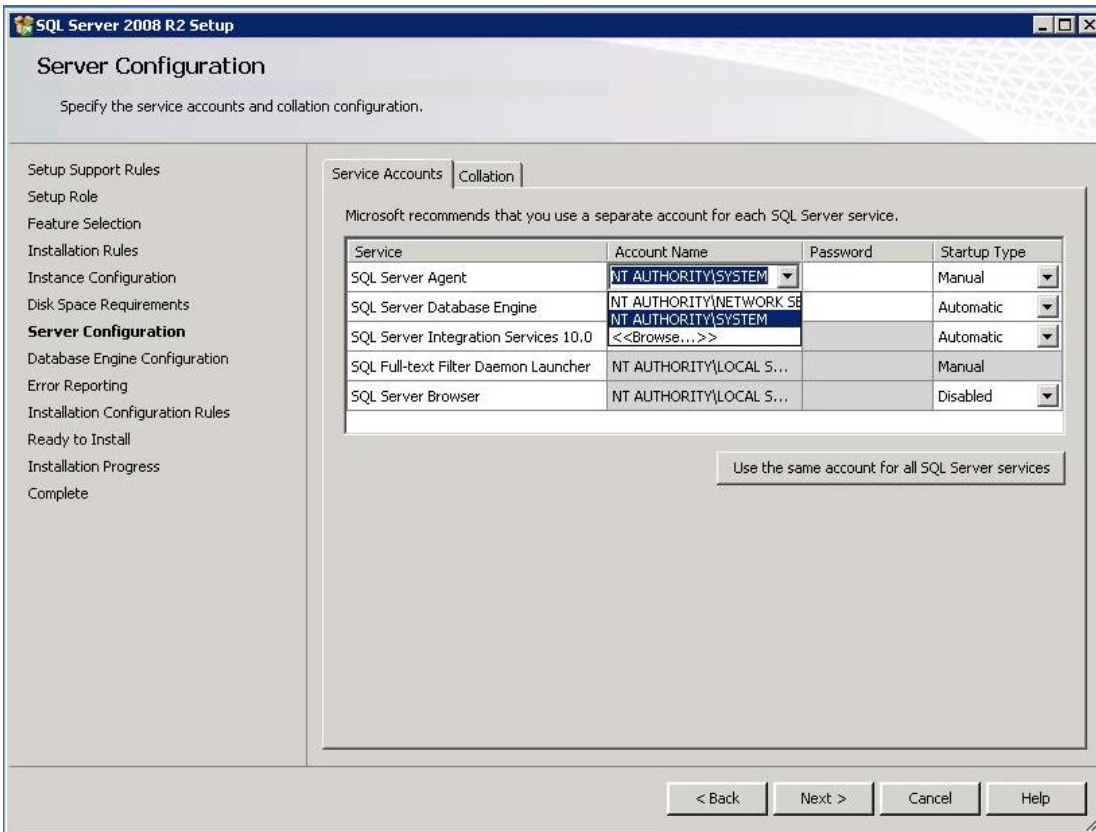
12) Choose **Default instance**, and then click **Next**.



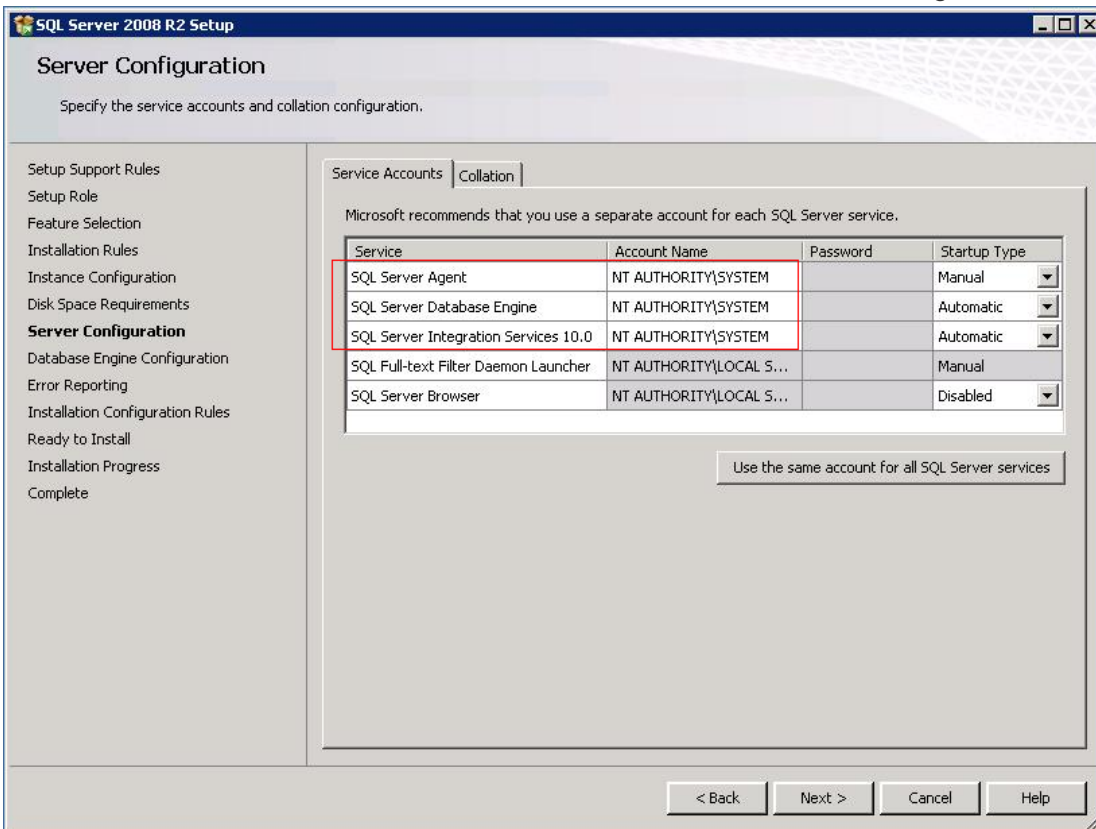
13) Click **Next**.

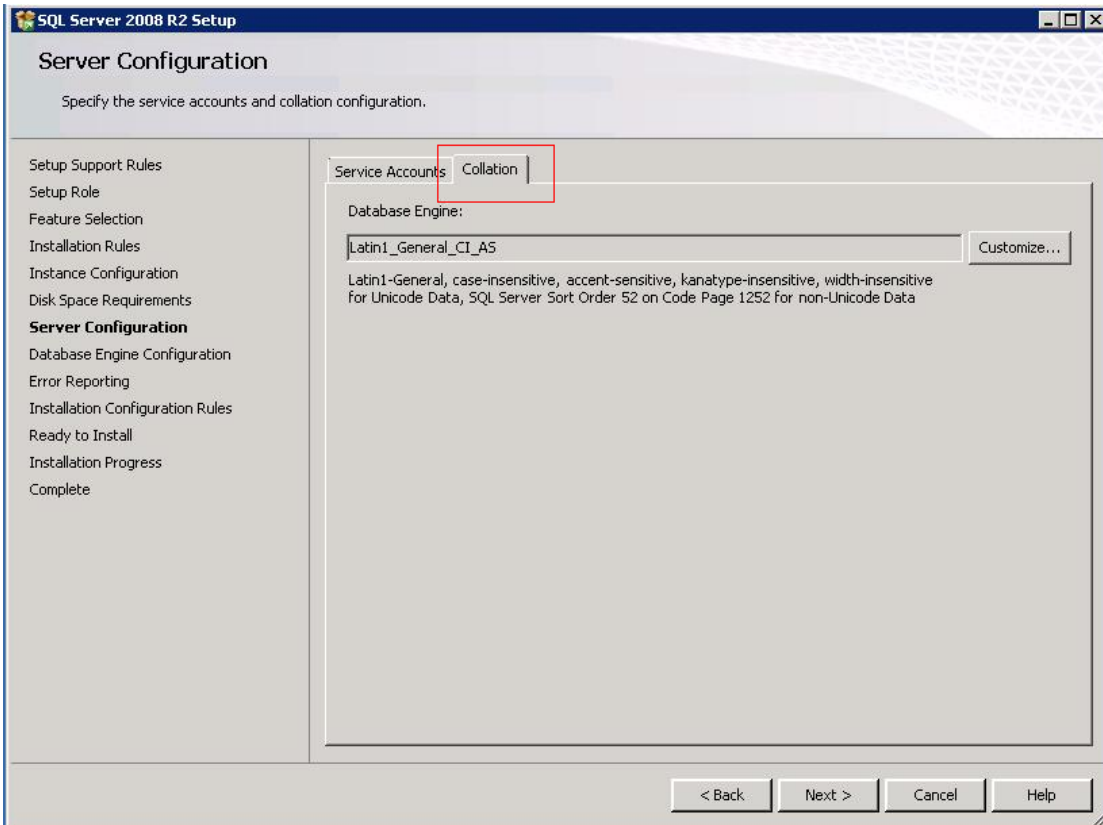


14) Choose **NT AUTHORITY\SYSTEM** from the **Account Name** drop-down list.

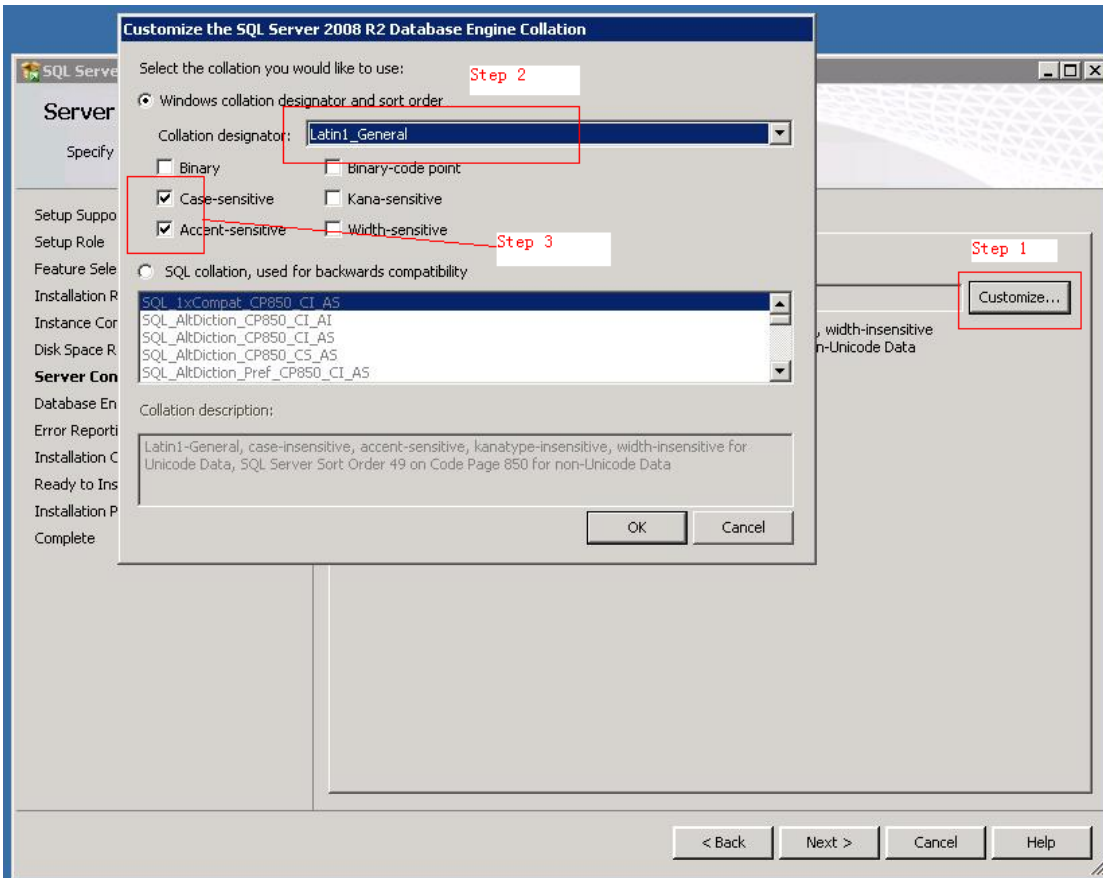


15) Choose **NT AUTHORITY/SYSTEM** for the three services as shown in the figure below.

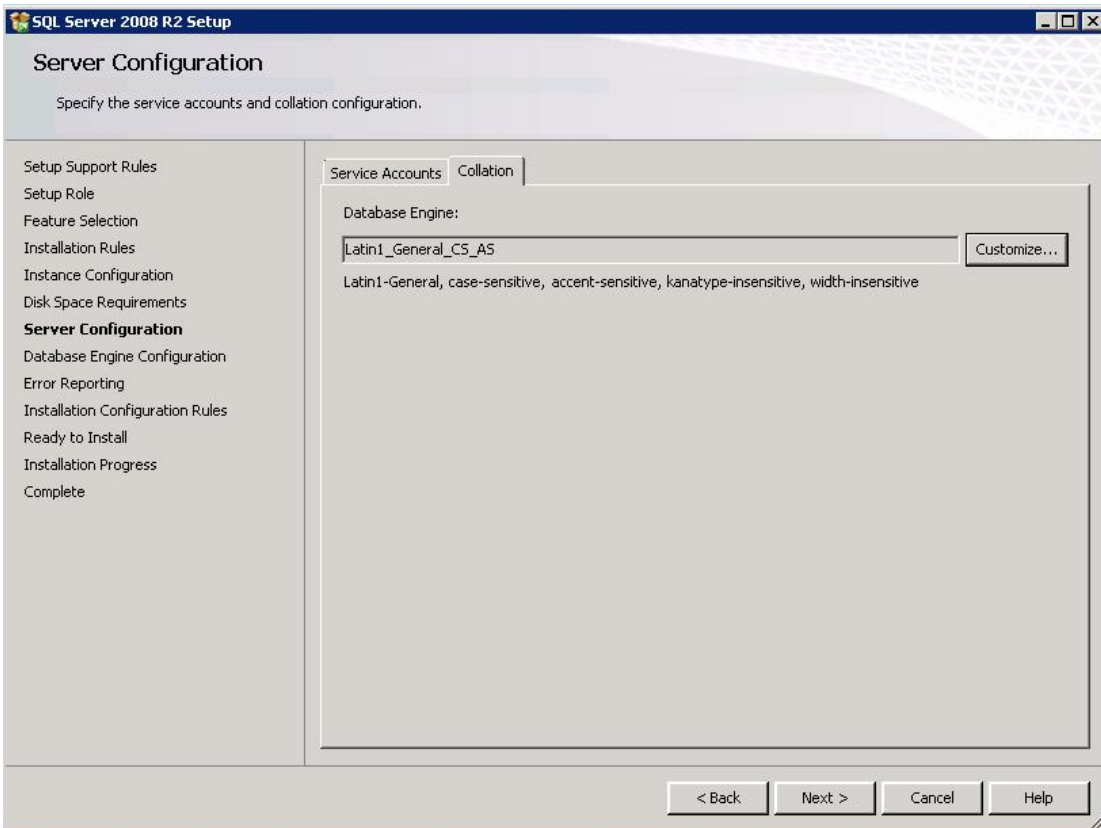


16) Choose the **Collation** tab.

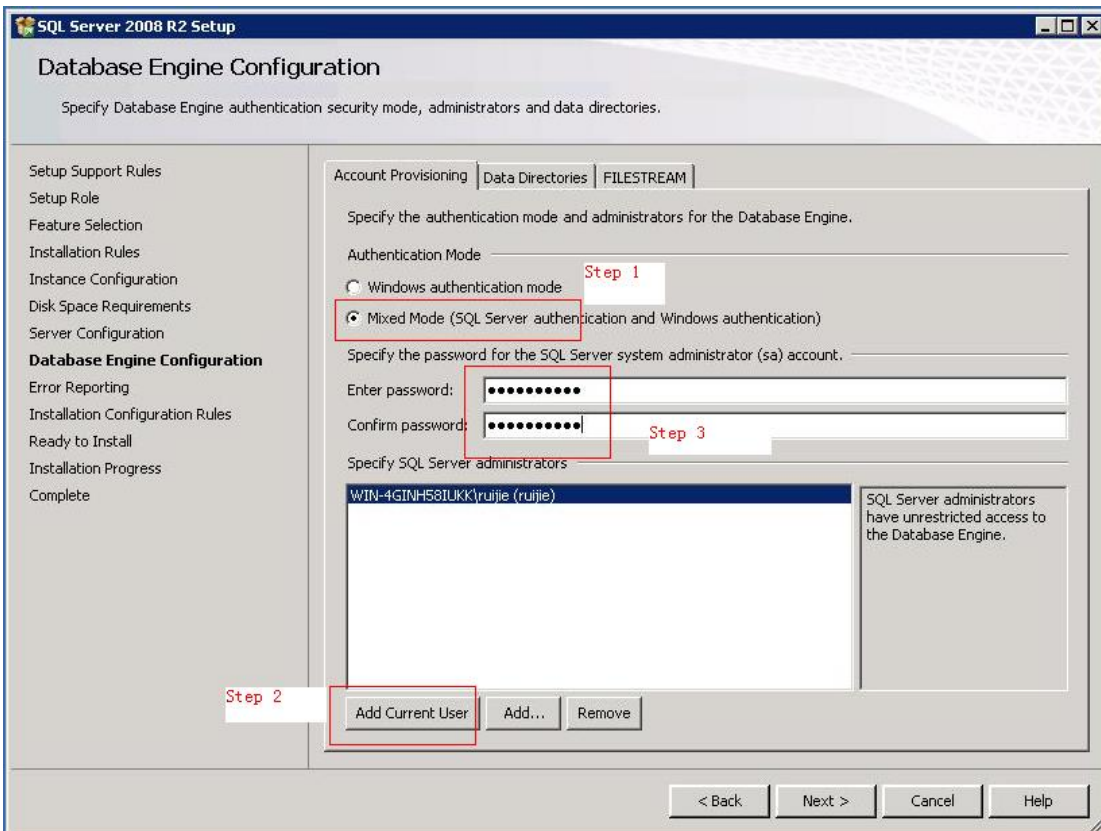
## 17) Configure collation. Make sure that the configuration is done exactly as shown in the following figure, or otherwise the SMP cannot run properly.



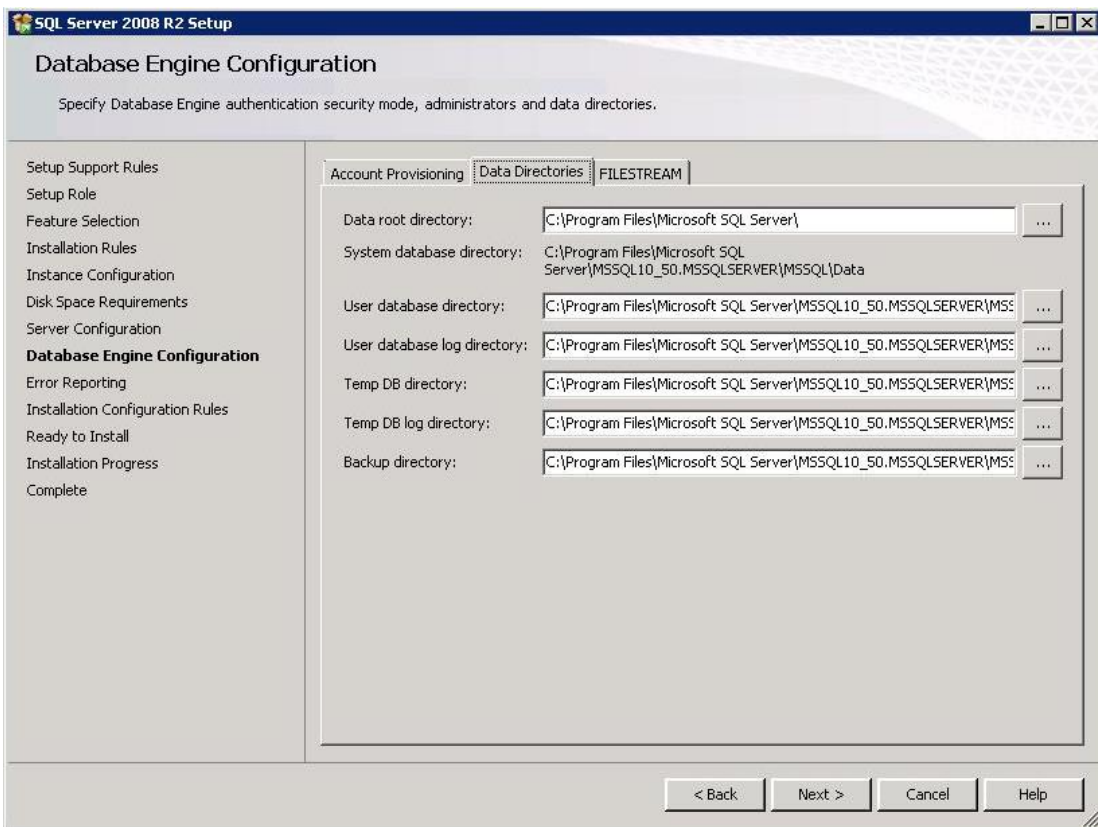
18) Click **Next**.



19) Configure a user account and a password.

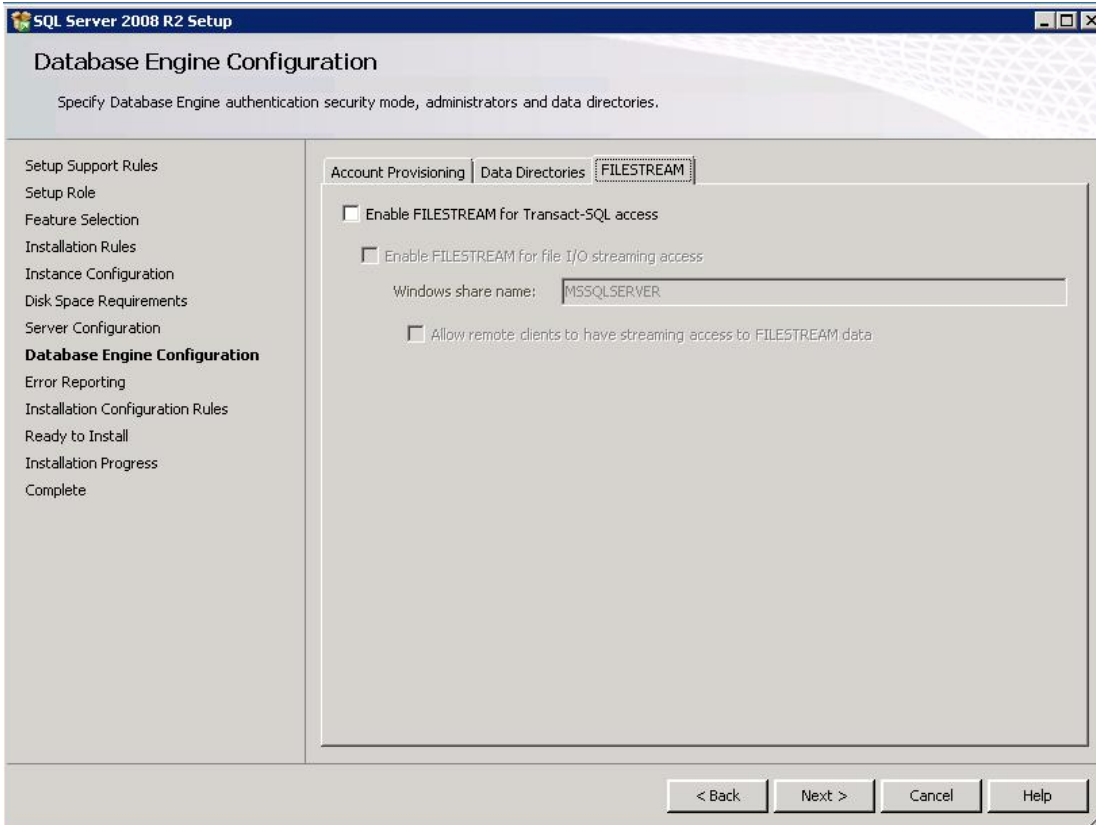


- 20) In the **Data Directories** tab, you can use the default configuration. If the default drive space is insufficient, choose another drive.

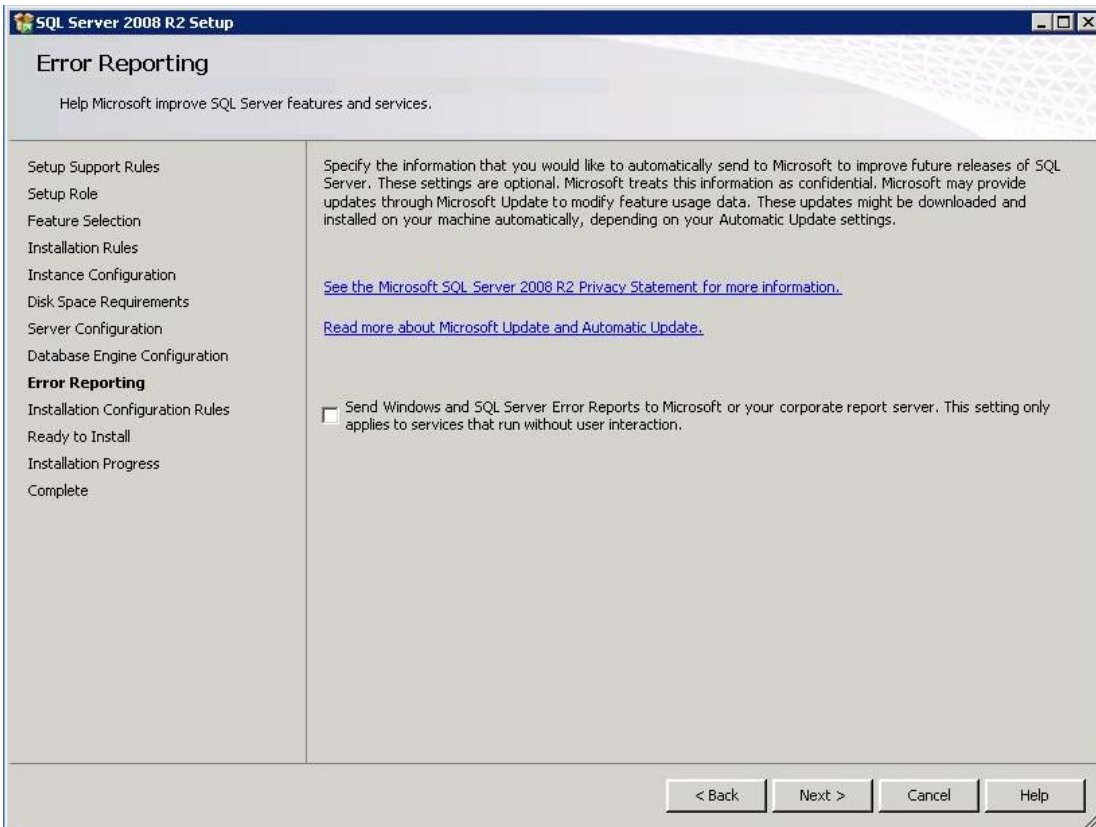


- 21) In the **FILESTREAM** tab, configure as shown in the following figure. Click **Next**.

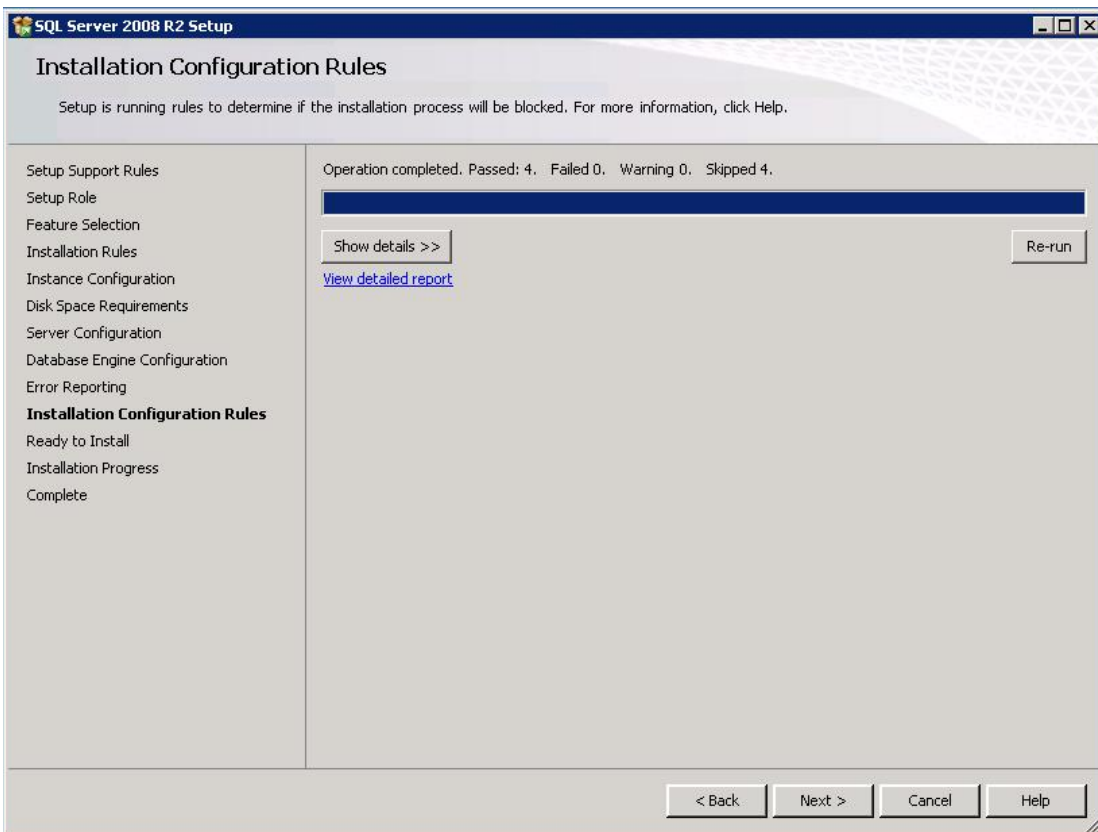




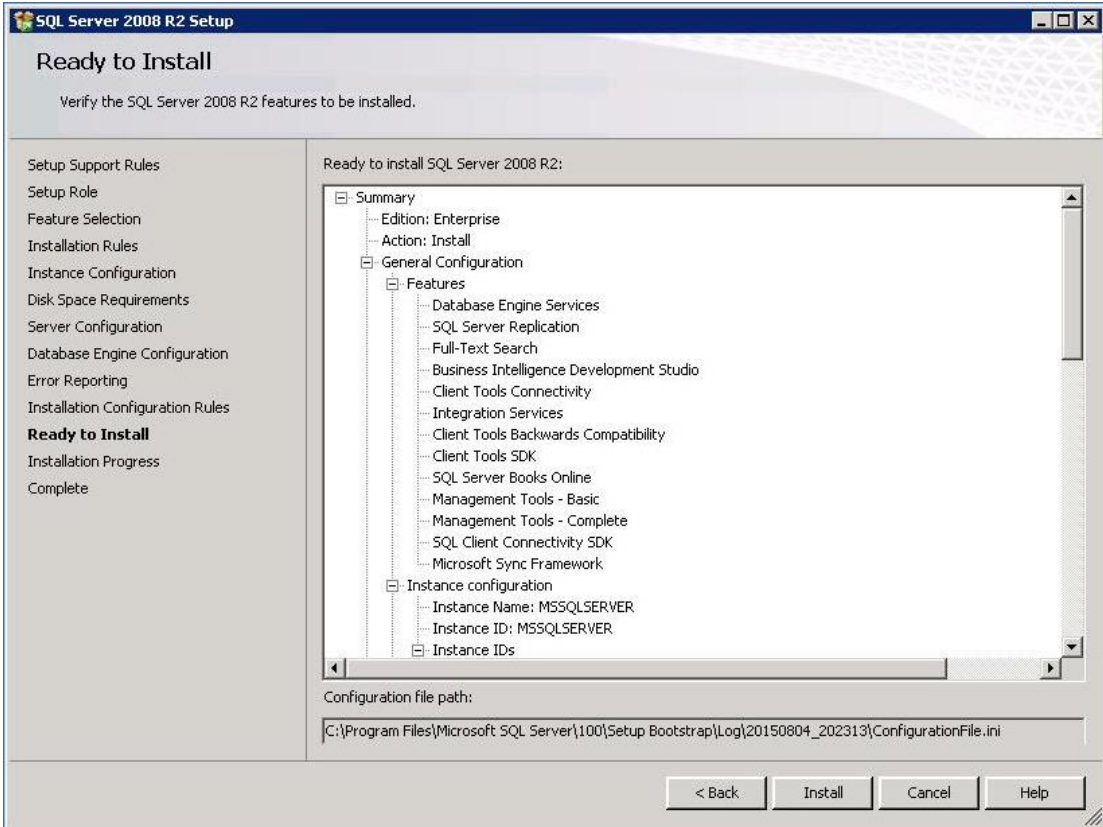
22) Click Next.



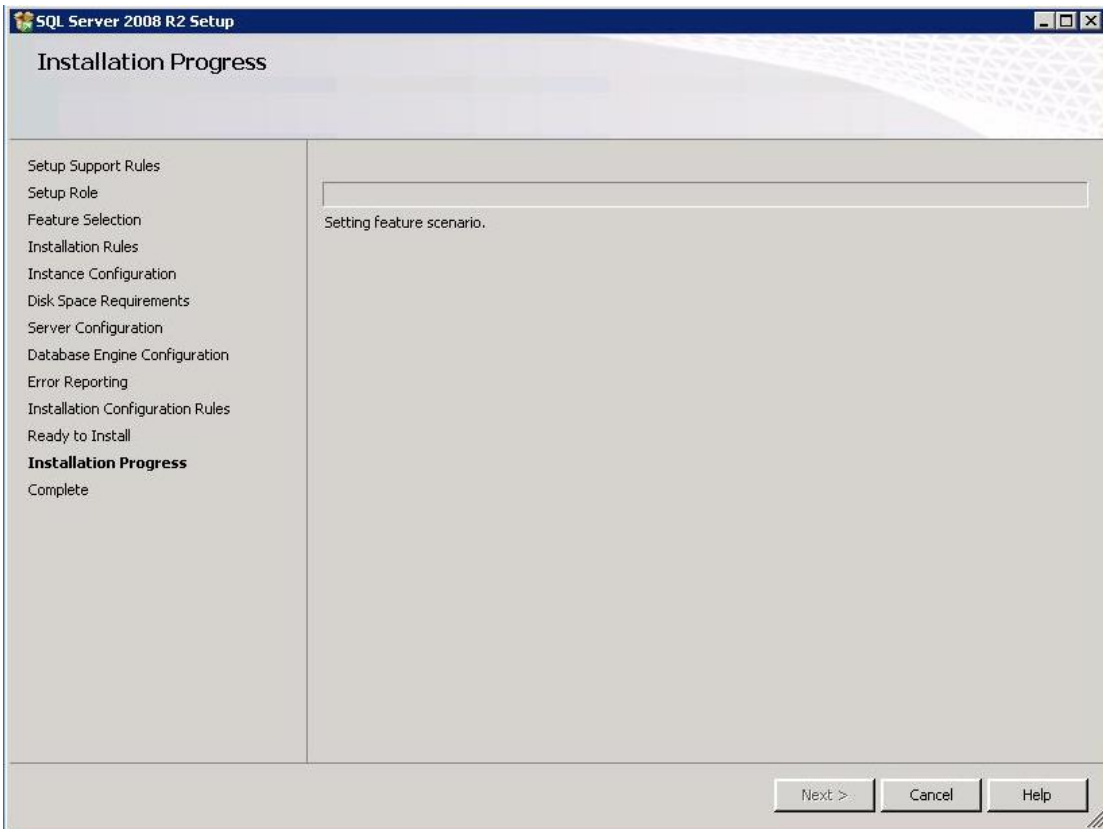
23) Click **Next**.



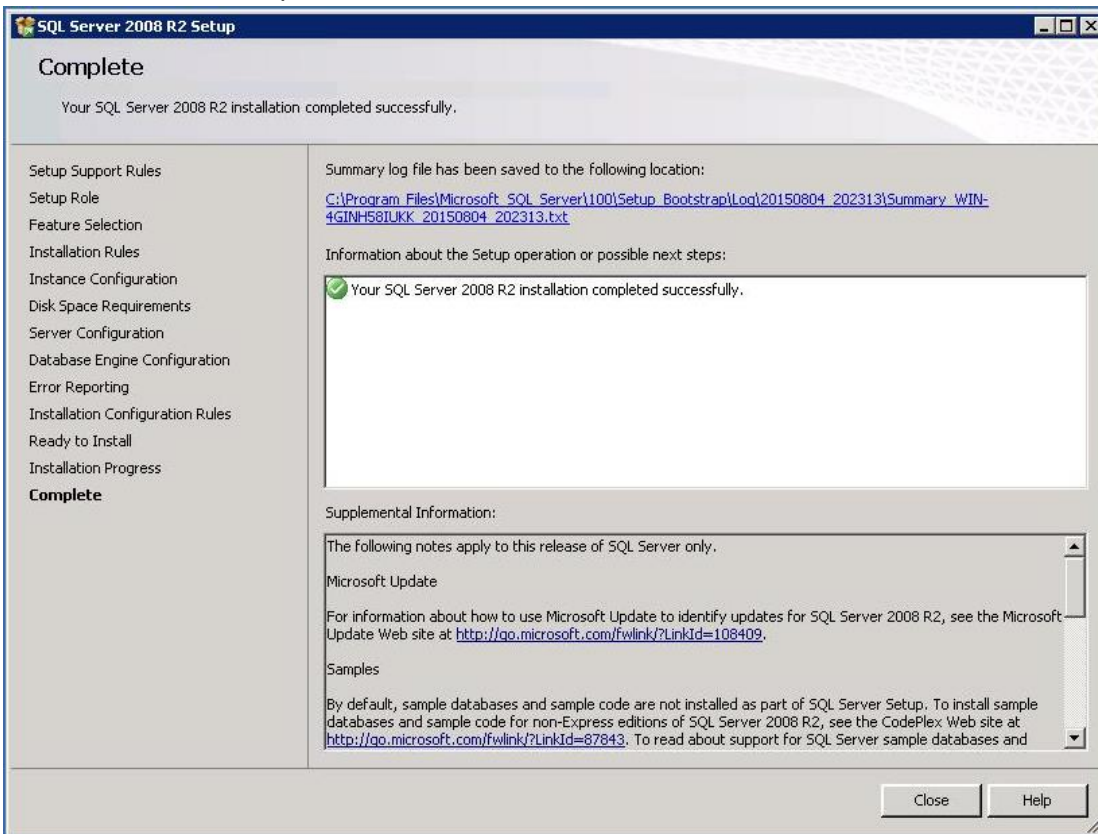
24) Click **Next**.



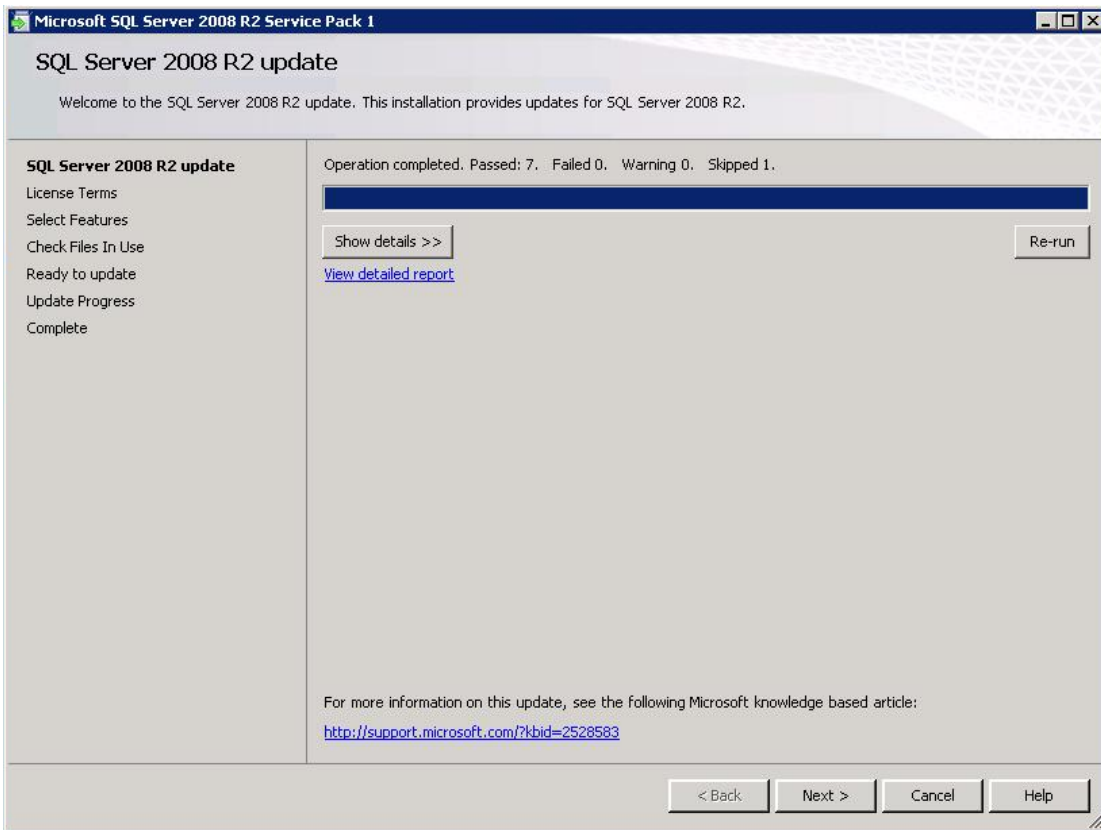
25) Click Next.



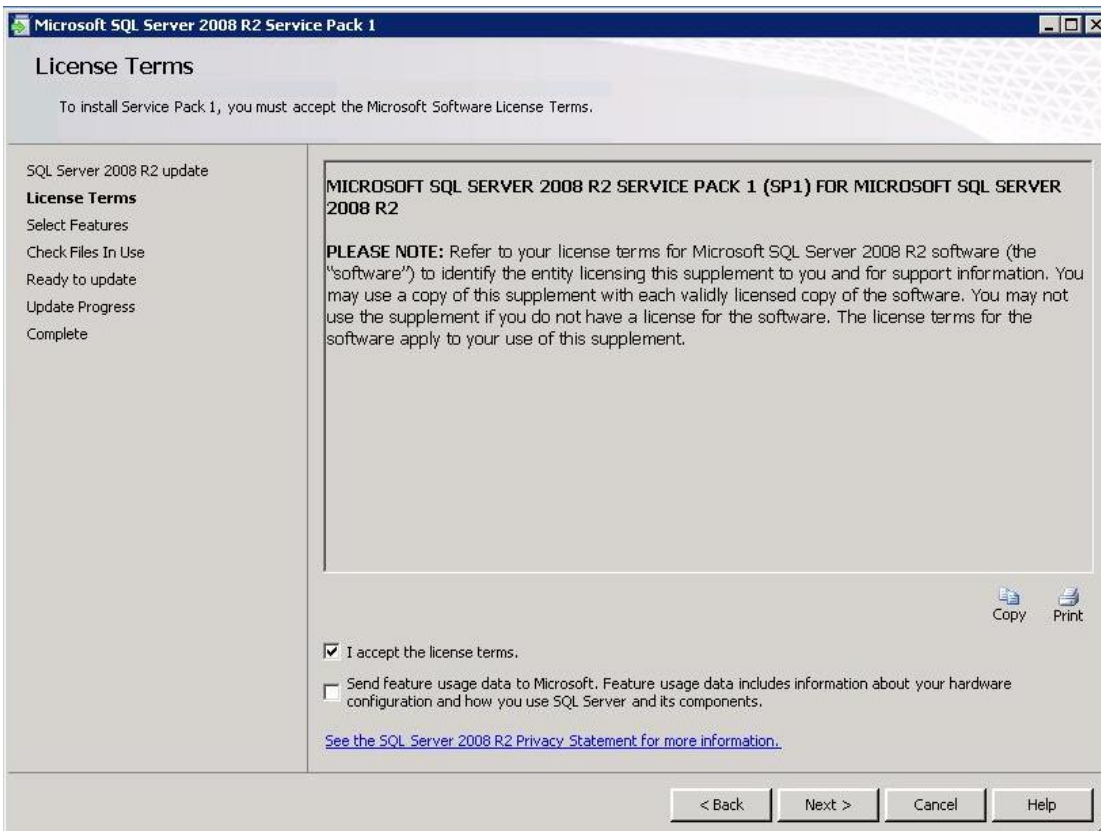
26) The installation is complete. Click **Close**.



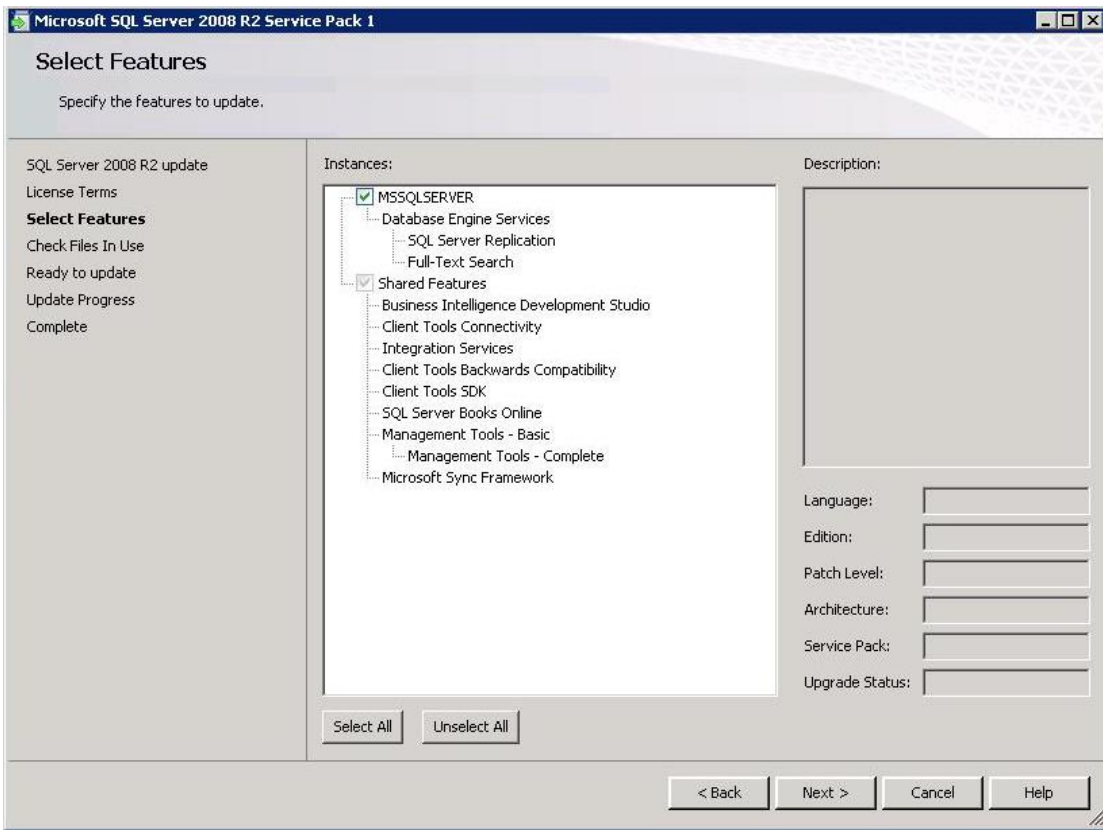
27) Double click the SP1 patch, and click **Next**.



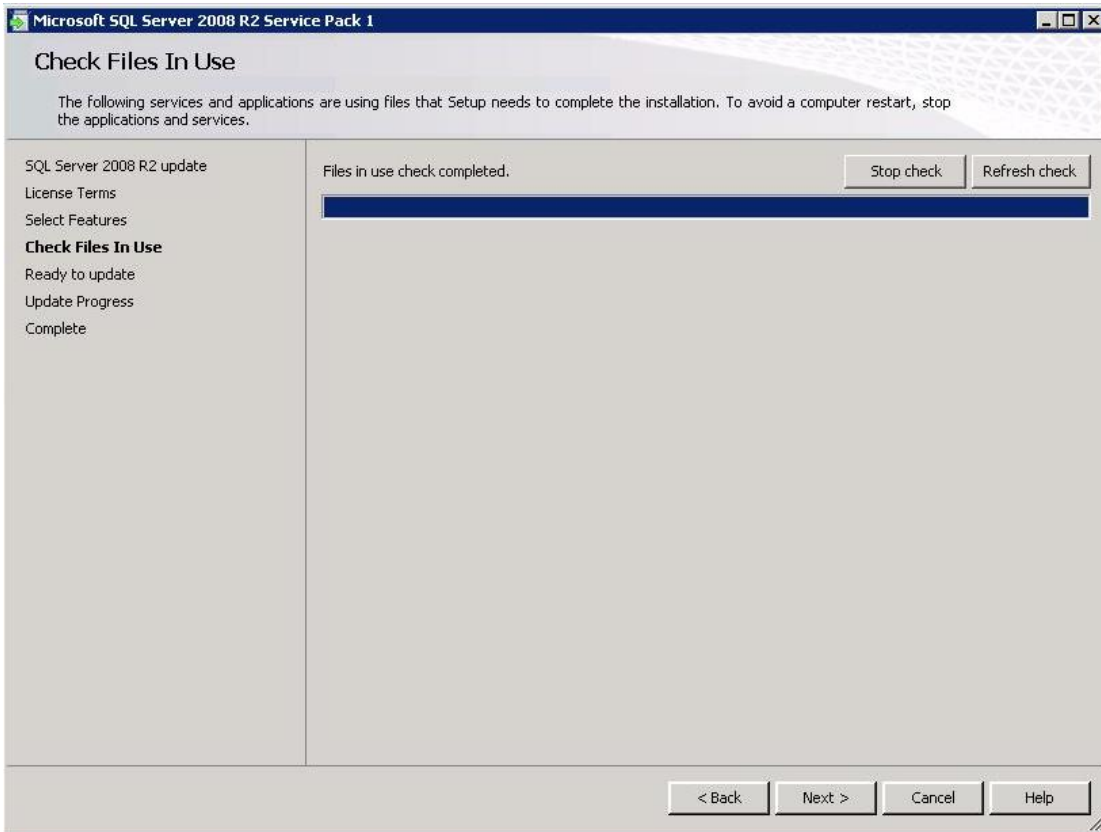
28) Tick **I accept the license terms**, and click **Next**.



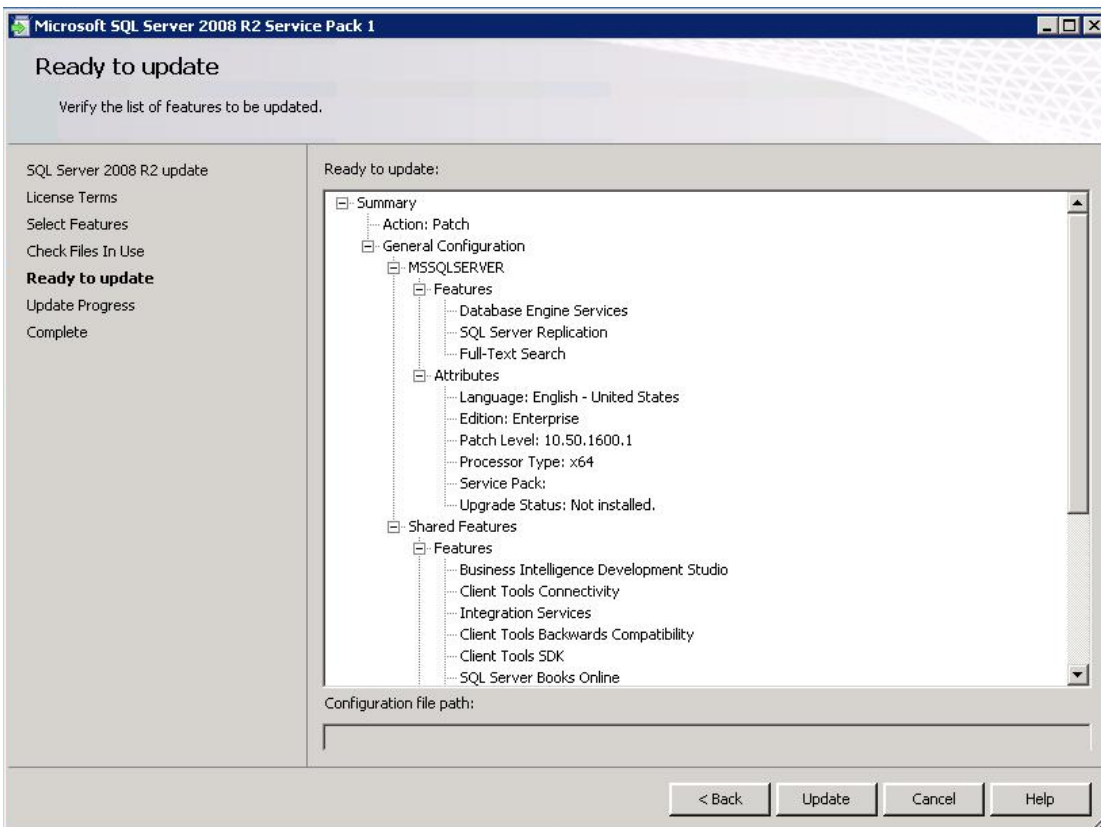
29) Click **Next**.



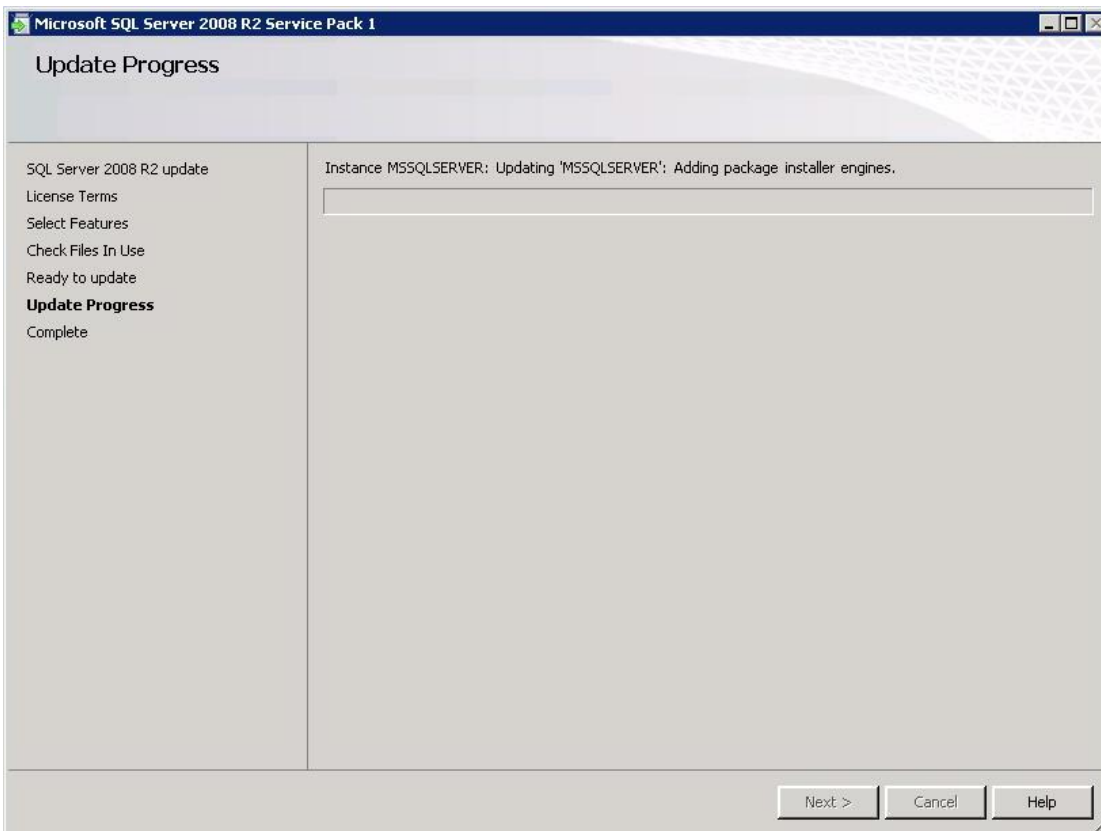
30) Click **Next**.



31) Click **Update**.

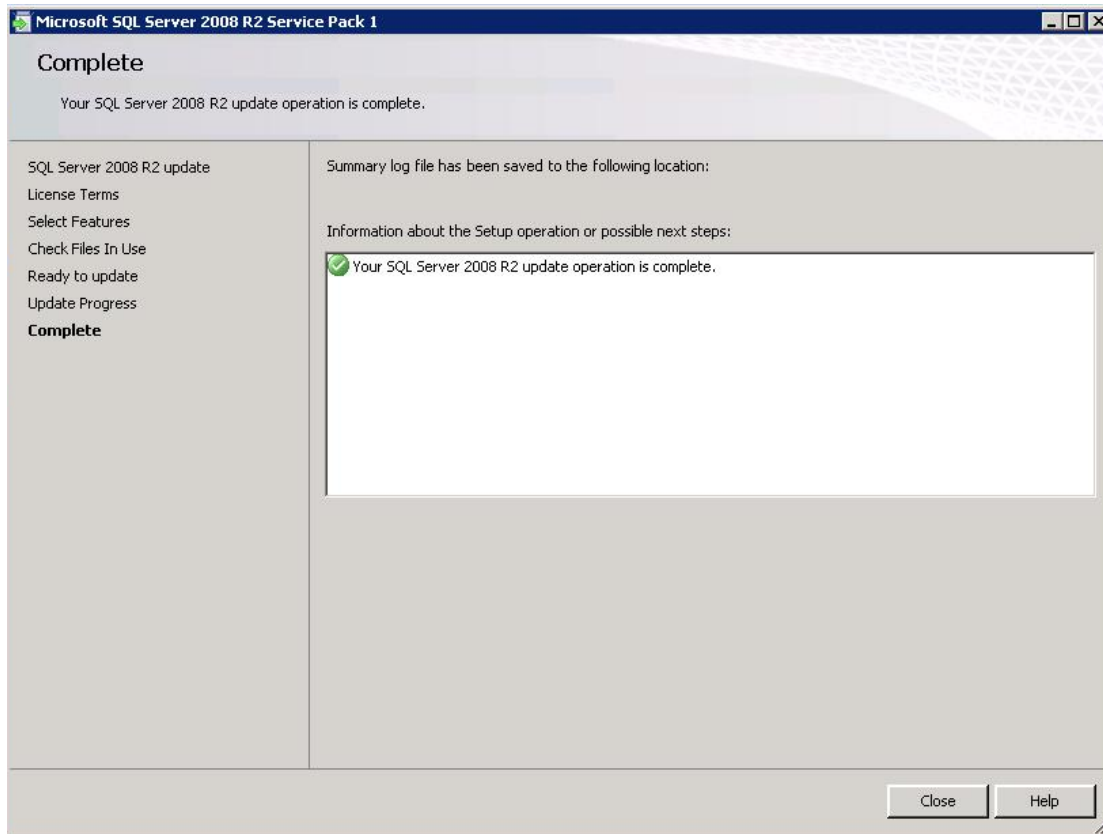


32) Click **Next**.



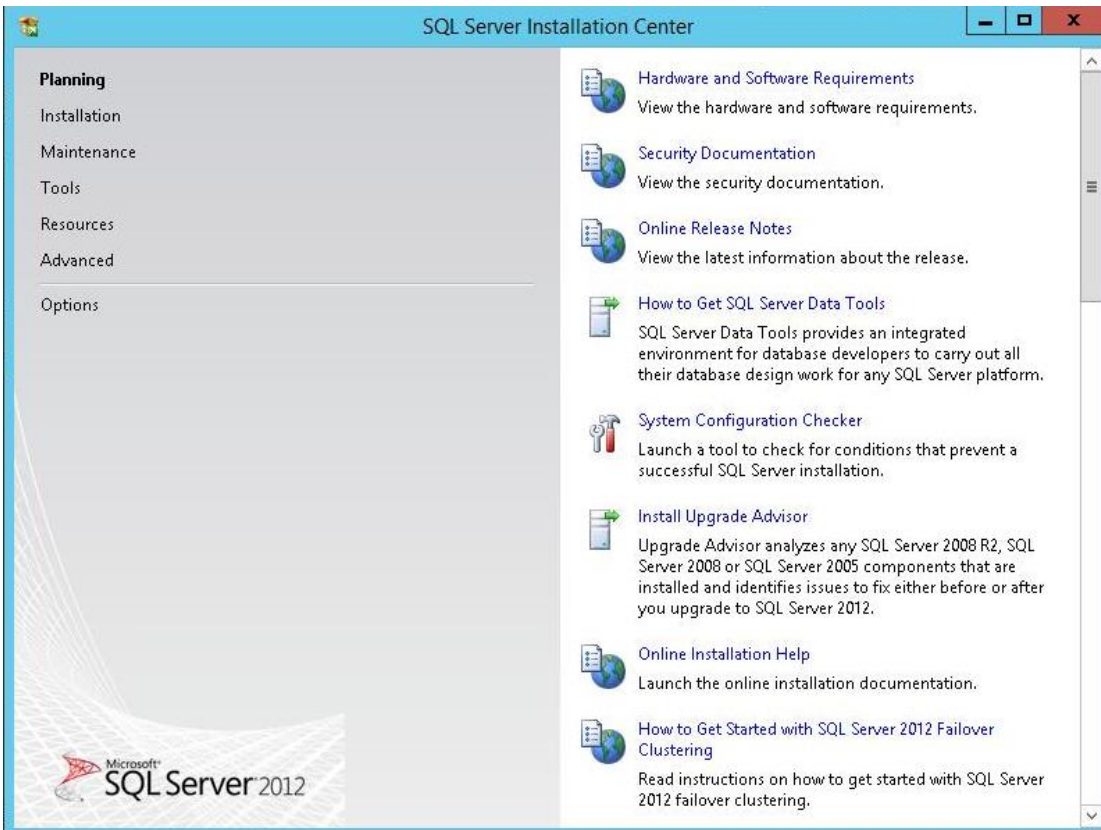


33) The installation is complete. Click **Close**.

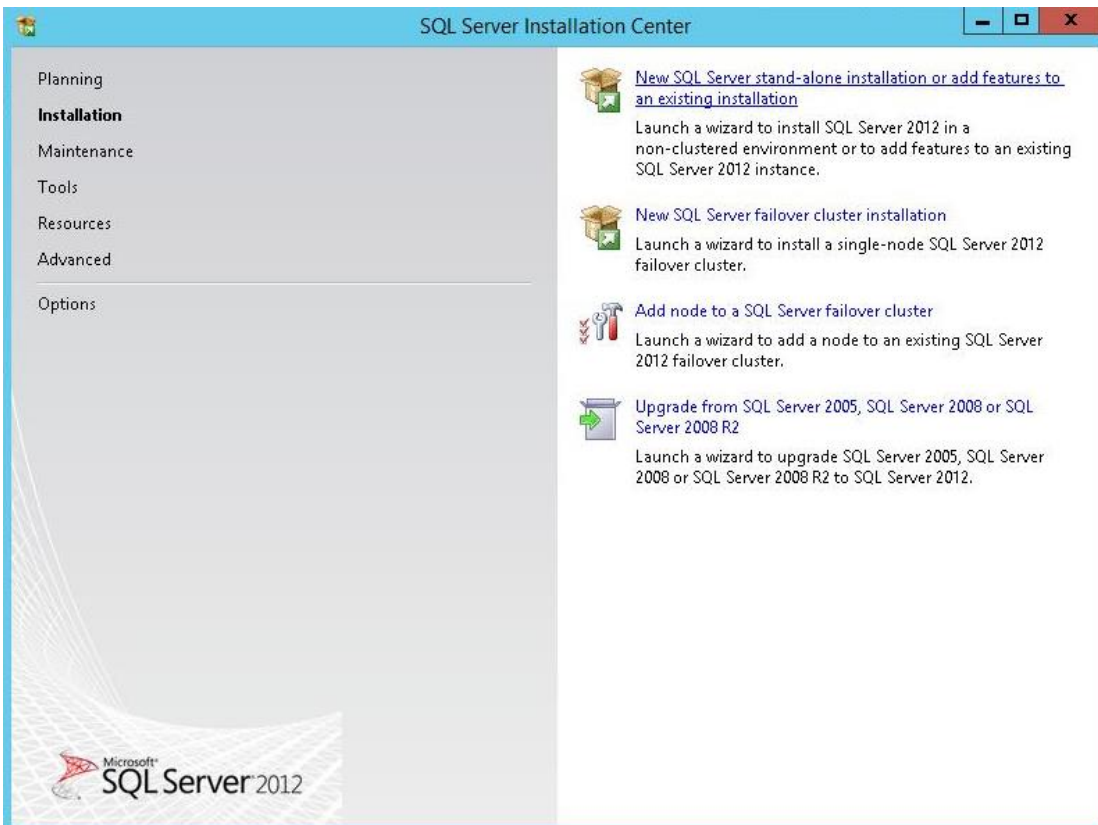


### 1.3.2 Installing SQL Server 2012 Enterprise Edition

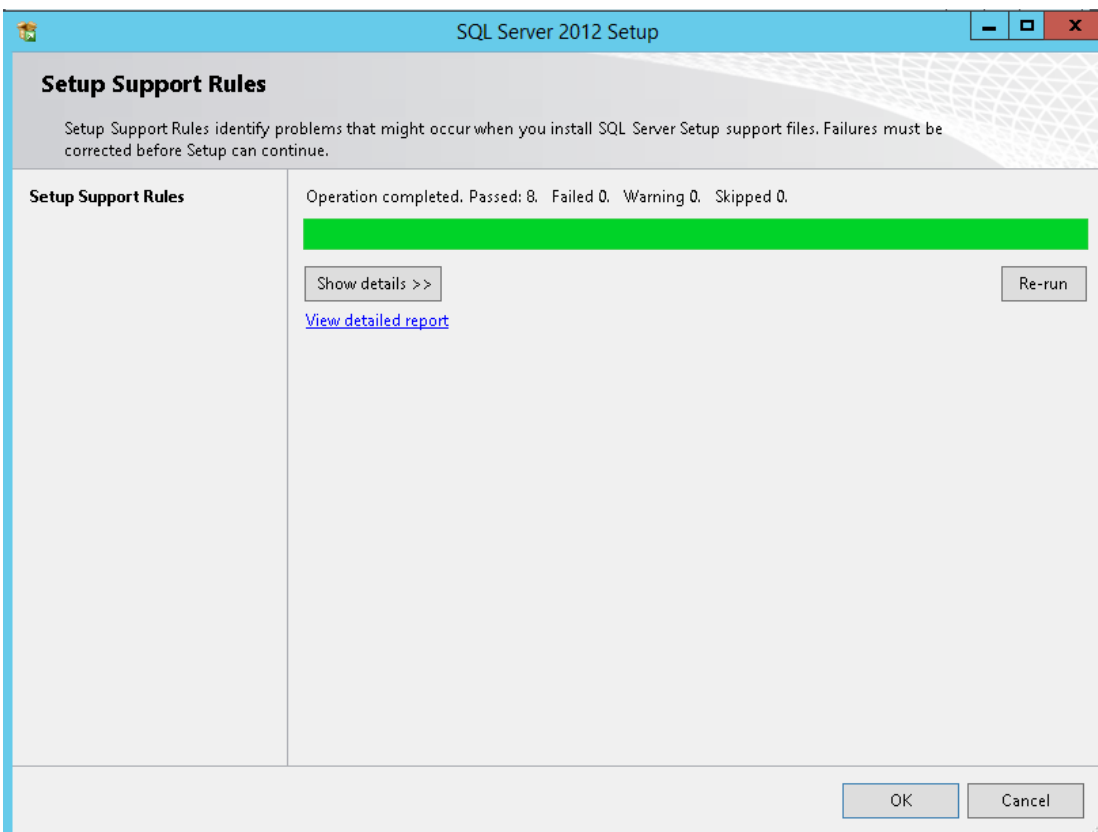
1) Double-click the **setup.exe** file, and the following interface is prompted.



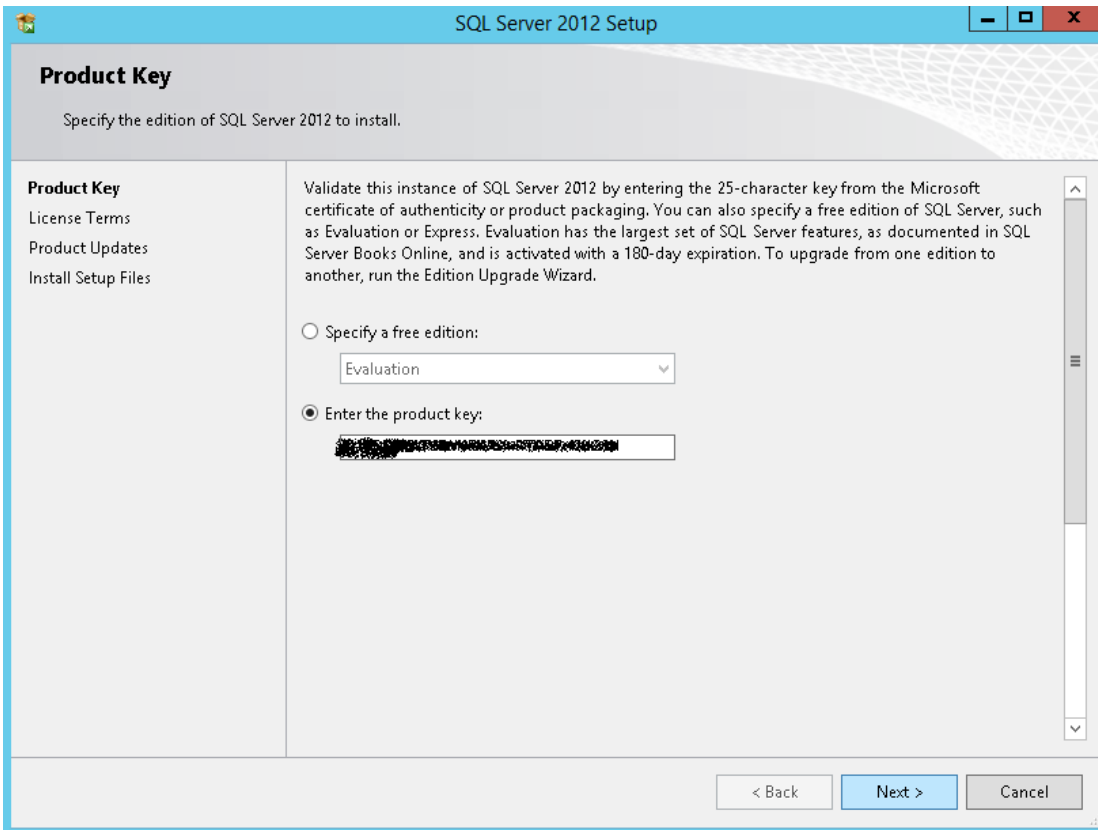
- 2) Click **Installation >New SQL Server stand-alone installation or add features to an existing installation.**



3) Click **OK**.

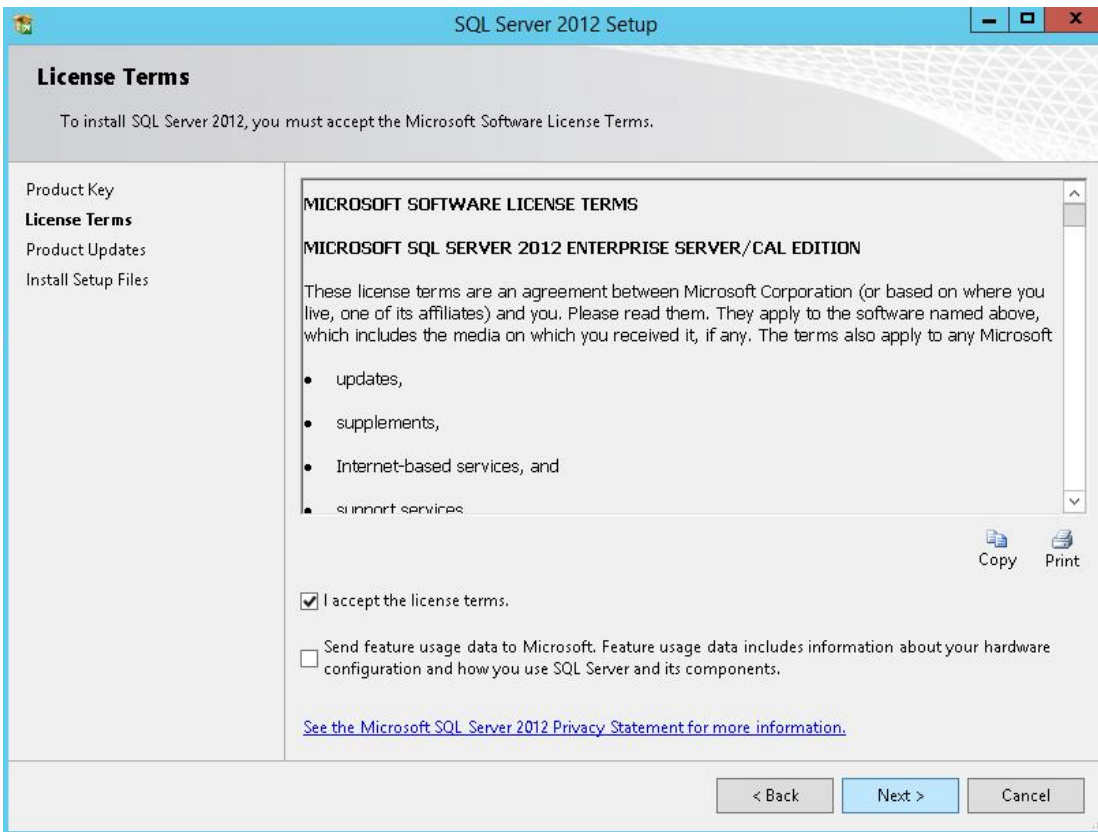


- 4) Click **Next**.

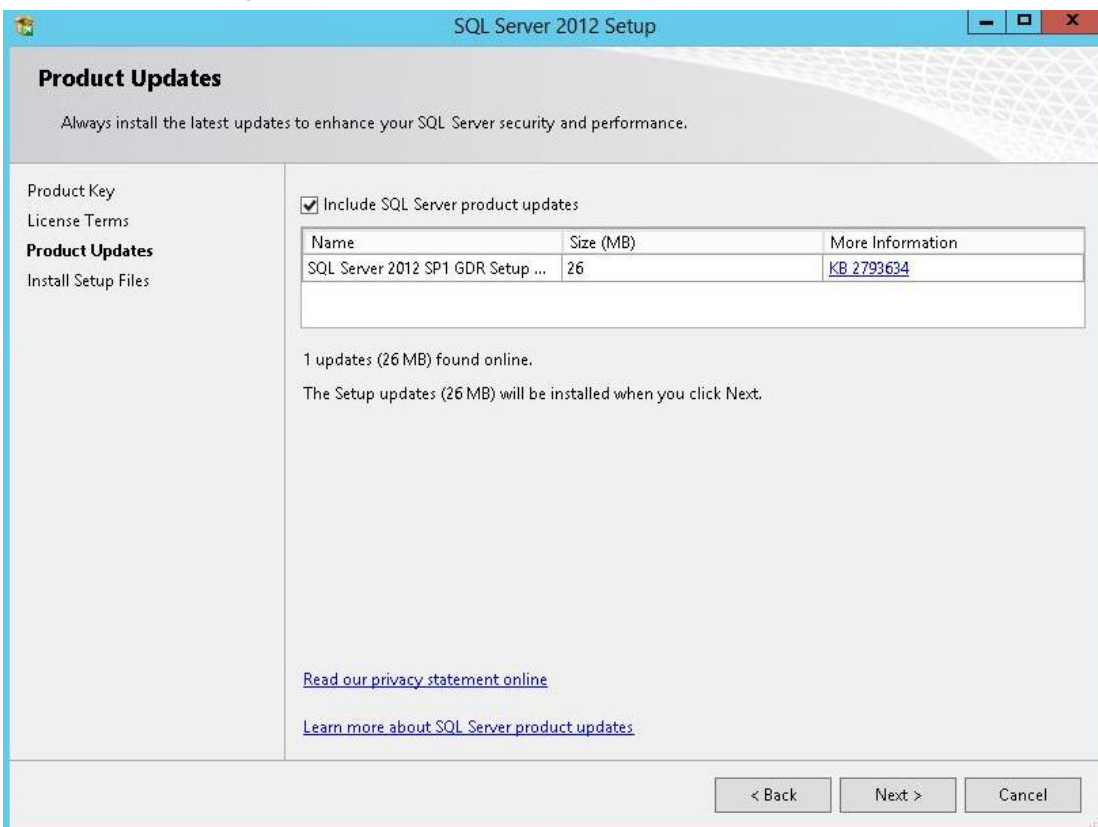


The screenshot shows the 'Product Key' step in the SQL Server 2012 Setup wizard. The window title is 'SQL Server 2012 Setup'. The main heading is 'Product Key' with the instruction 'Specify the edition of SQL Server 2012 to install.' On the left, there is a navigation pane with 'Product Key' selected, and other options: 'License Terms', 'Product Updates', and 'Install Setup Files'. The main area contains a text block explaining that the user must enter a 25-character product key from a Microsoft certificate or packaging, or choose a free edition like Evaluation or Express. Below this, there are two radio button options: 'Specify a free edition:' with a dropdown menu currently showing 'Evaluation', and 'Enter the product key:' which is selected. A text box for entering the product key is present but its content is obscured by a blacked-out area. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

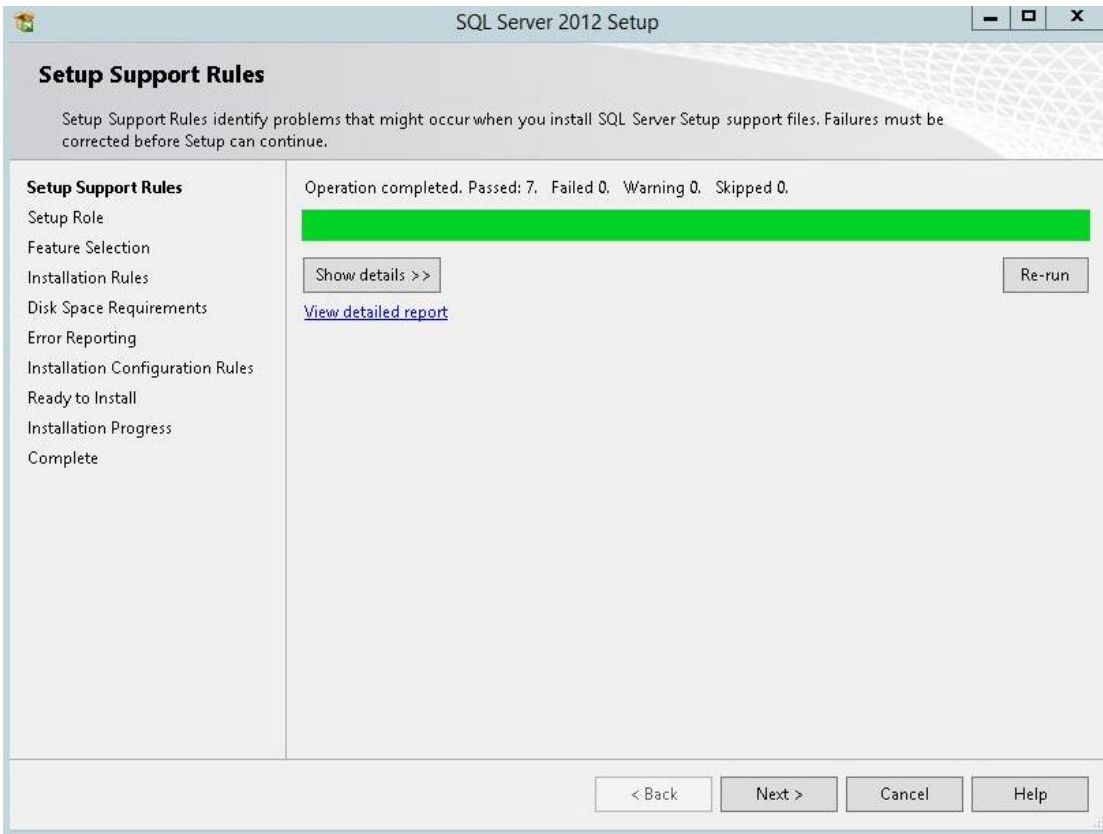
- 5) Tick **I accept the license terms**, and click **Next**.



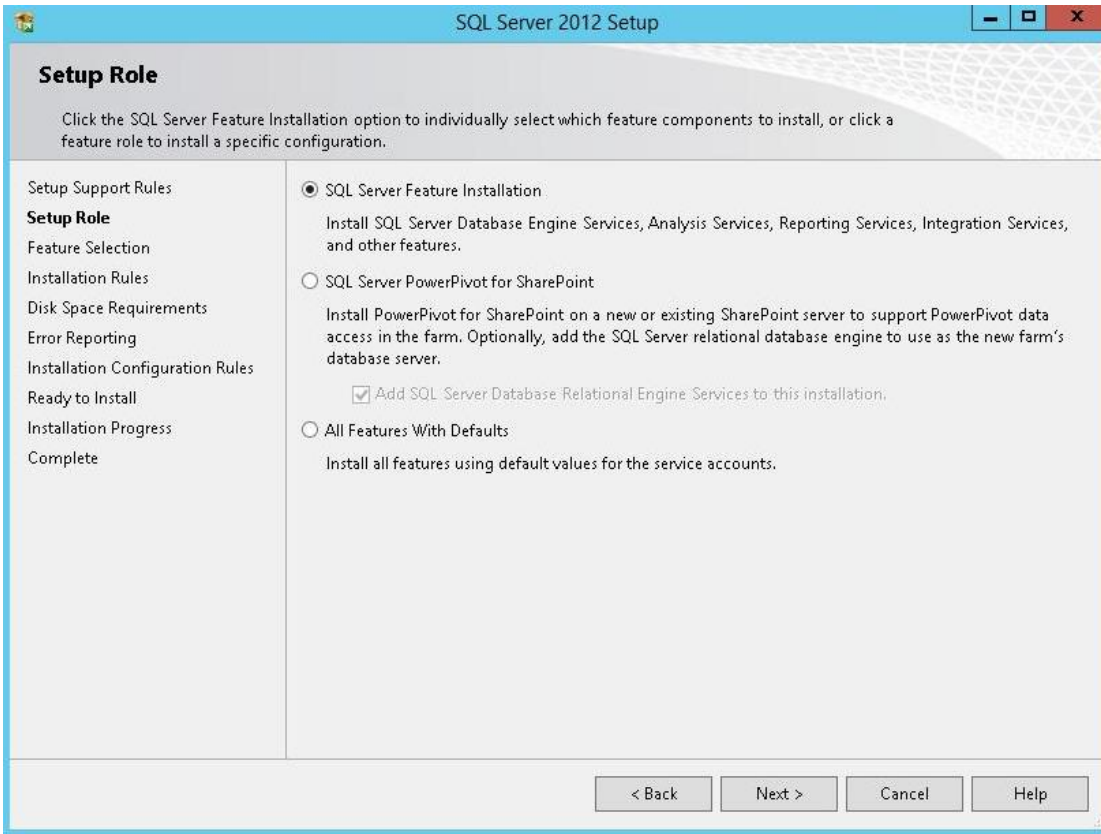
6) Keep the default setting, and click **Next**.



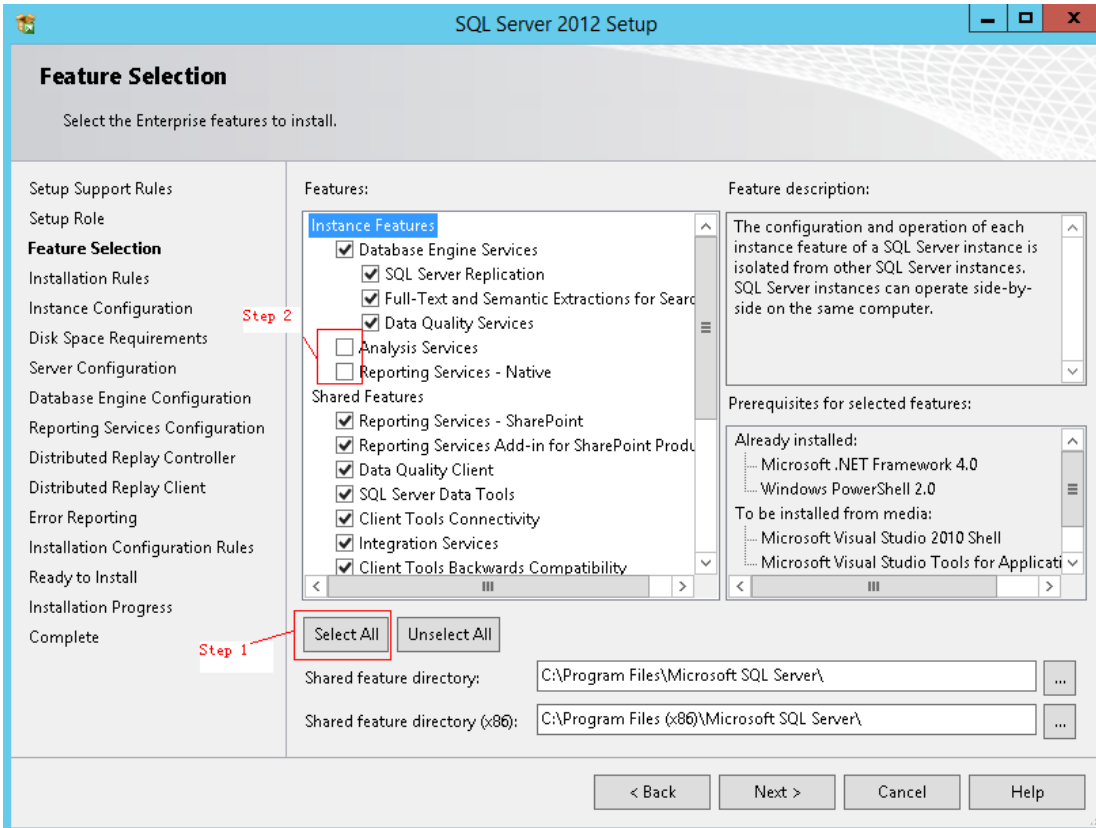
7) Click **Next**.



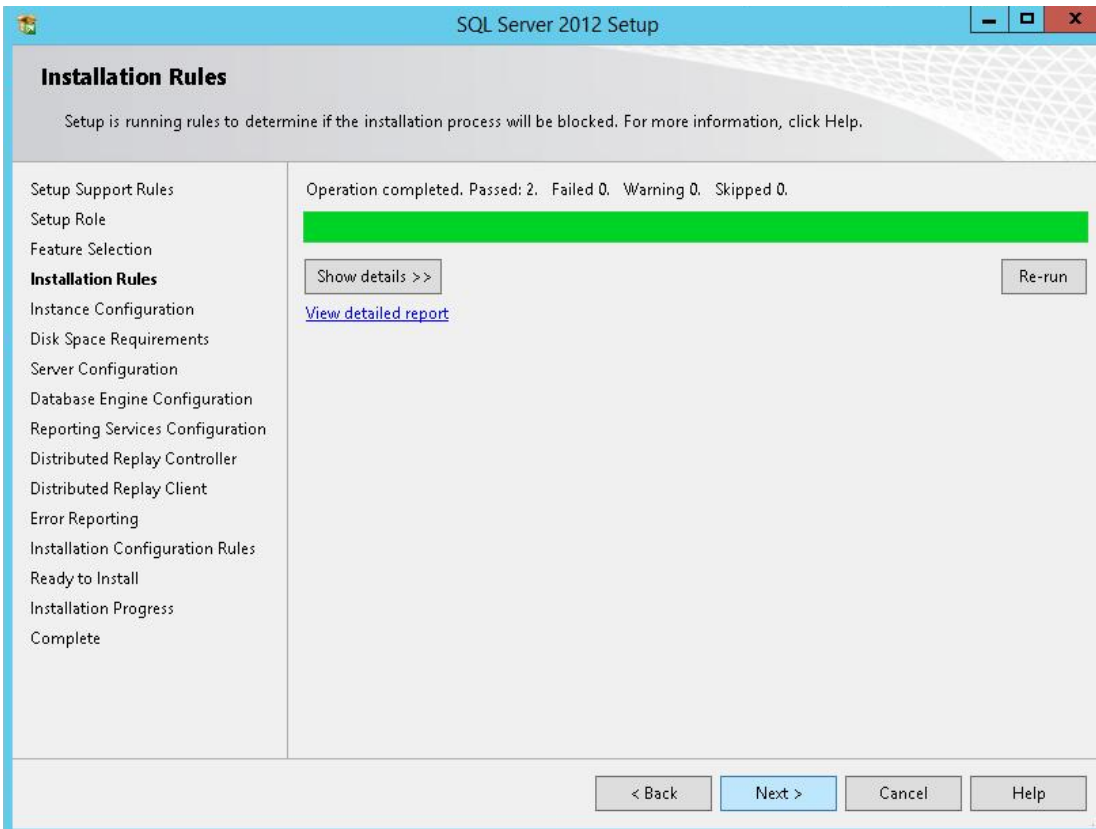
8) Click **Next**.



- 9) Tick the components you need as shown in the following figure, and then click **Next**.



10) Click **Next**.





- 11) Choose **Default instance**, and then click **Next**.

SQL Server 2012 Setup

### Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

Setup Support Rules  
Setup Role  
Feature Selection  
Installation Rules  
**Instance Configuration**  
Disk Space Requirements  
Server Configuration  
Database Engine Configuration  
Reporting Services Configuration  
Distributed Replay Controller  
Distributed Replay Client  
Error Reporting  
Installation Configuration Rules  
Ready to Install  
Installation Progress  
Complete

Default instance  
 Named instance: MSSQLSERVER

Instance ID: MSSQLSERVER

Instance root directory: C:\Program Files\Microsoft SQL Server\ ...

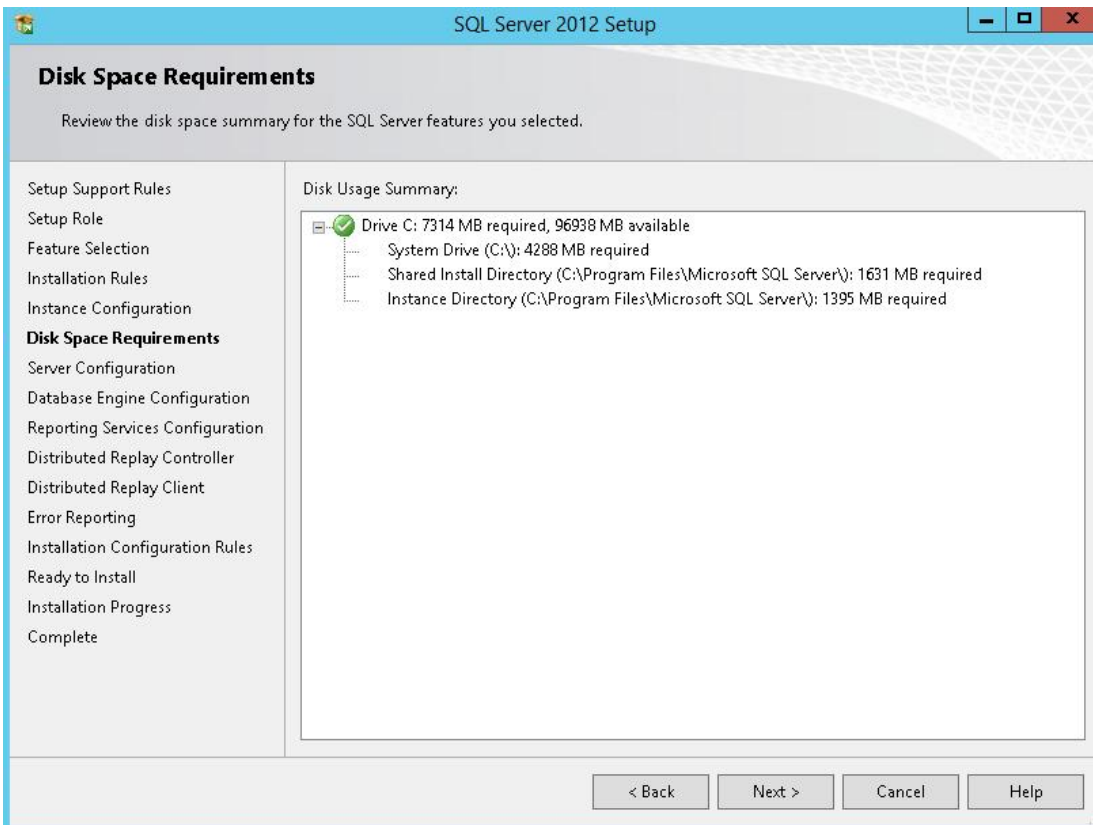
SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER

Installed instances:

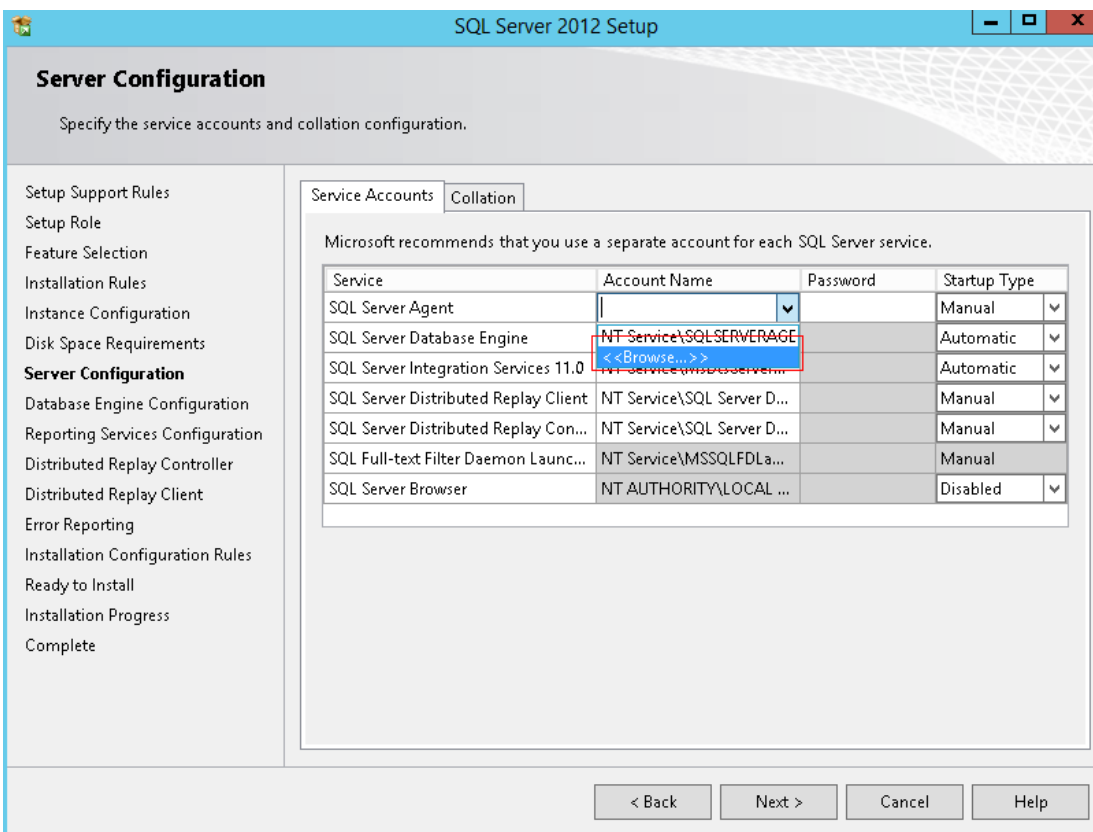
Instance Name	Instance ID	Features	Edition	Version
---------------	-------------	----------	---------	---------

< Back   Next >   Cancel   Help

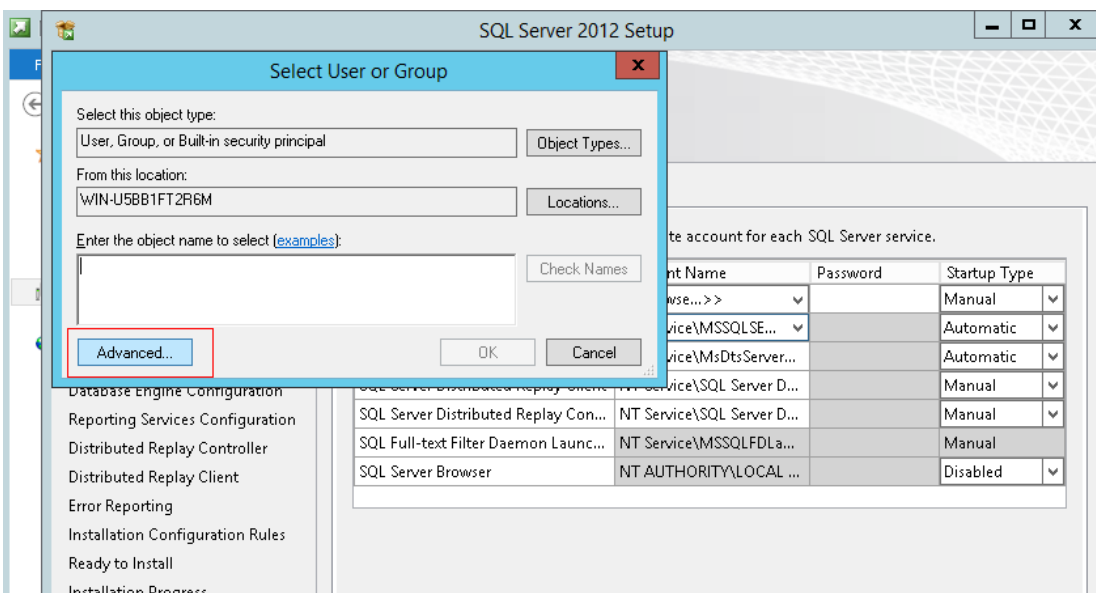
- 12) Click **Next**.



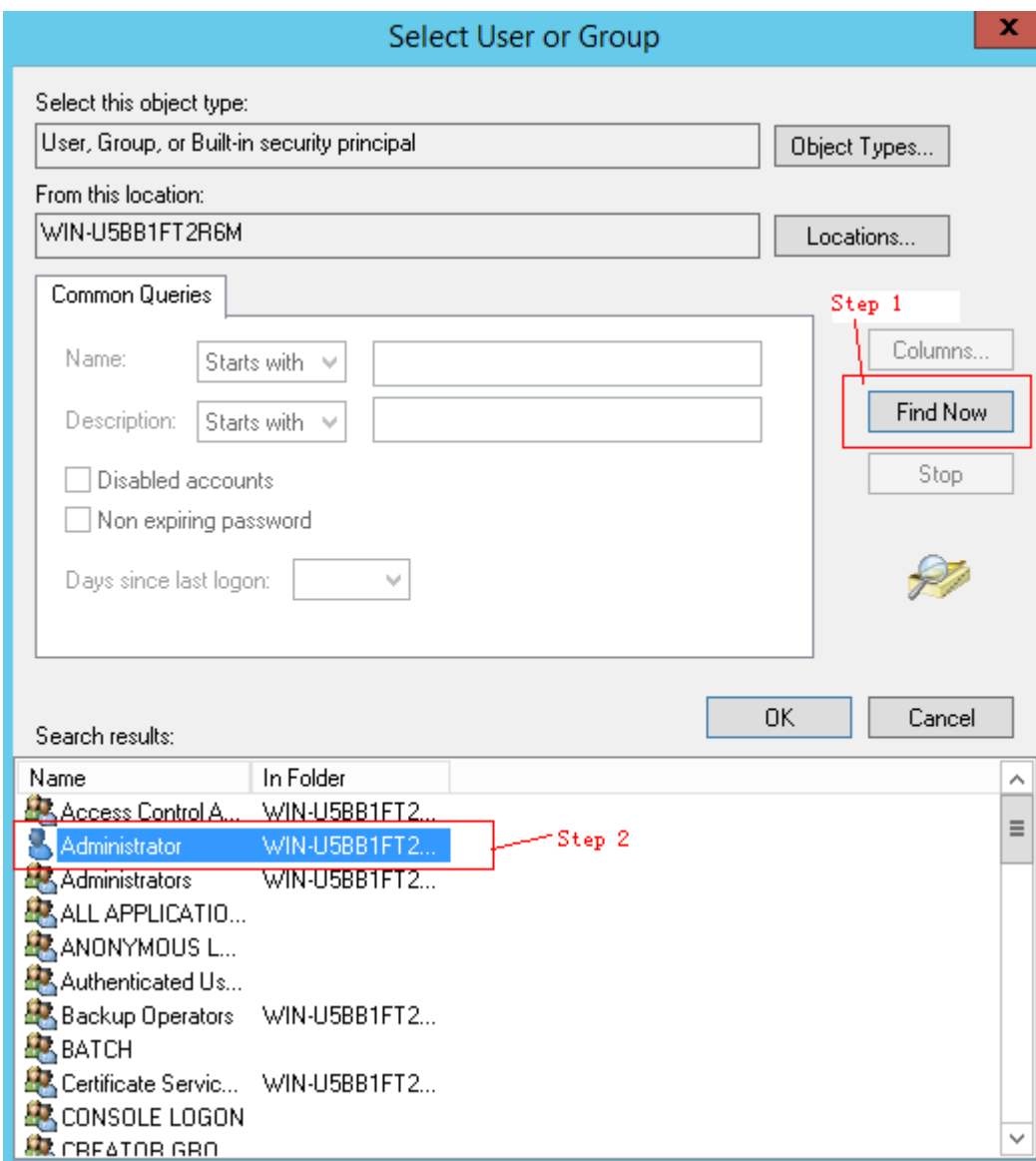
- 13) Choose **Browse** from the **Account Name** dropdown list.



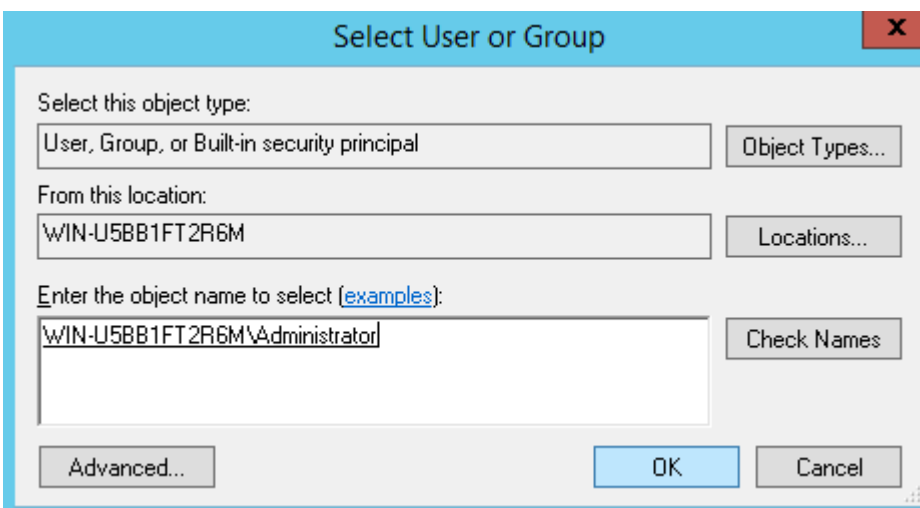
14) Click **Advanced**.



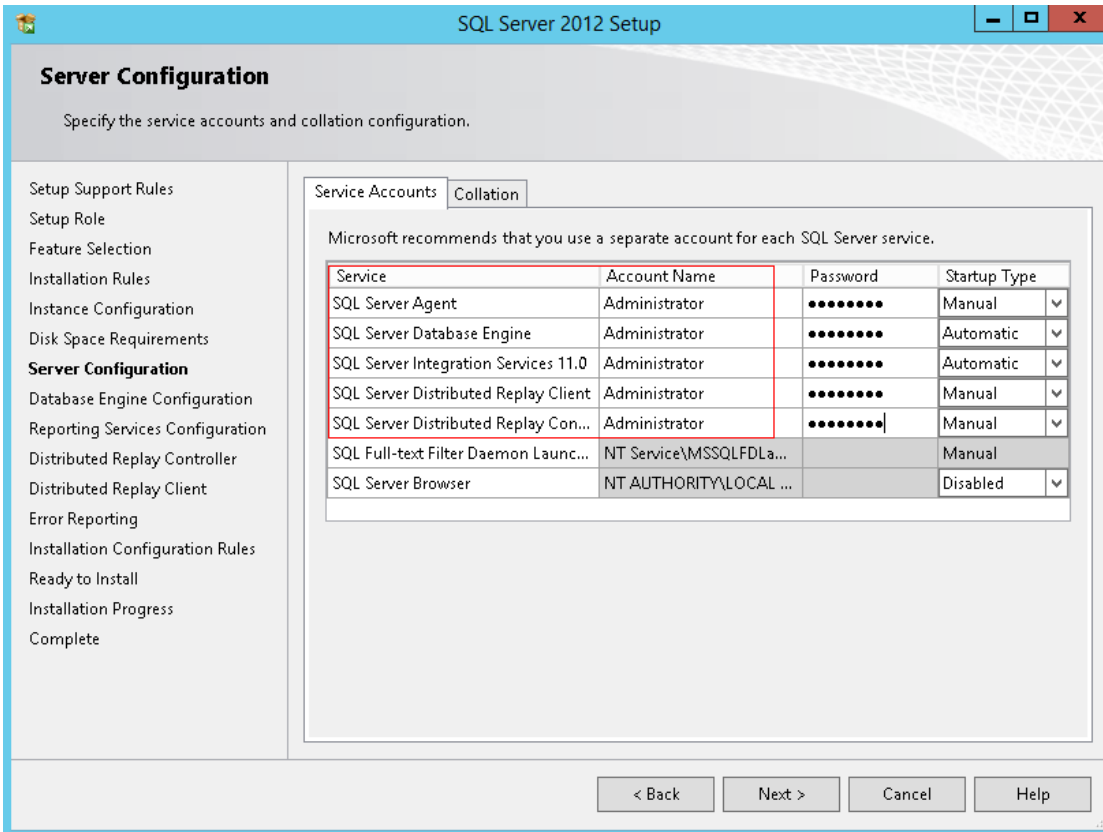
15) Click **Find Now**, and then choose the **Administrator** user.



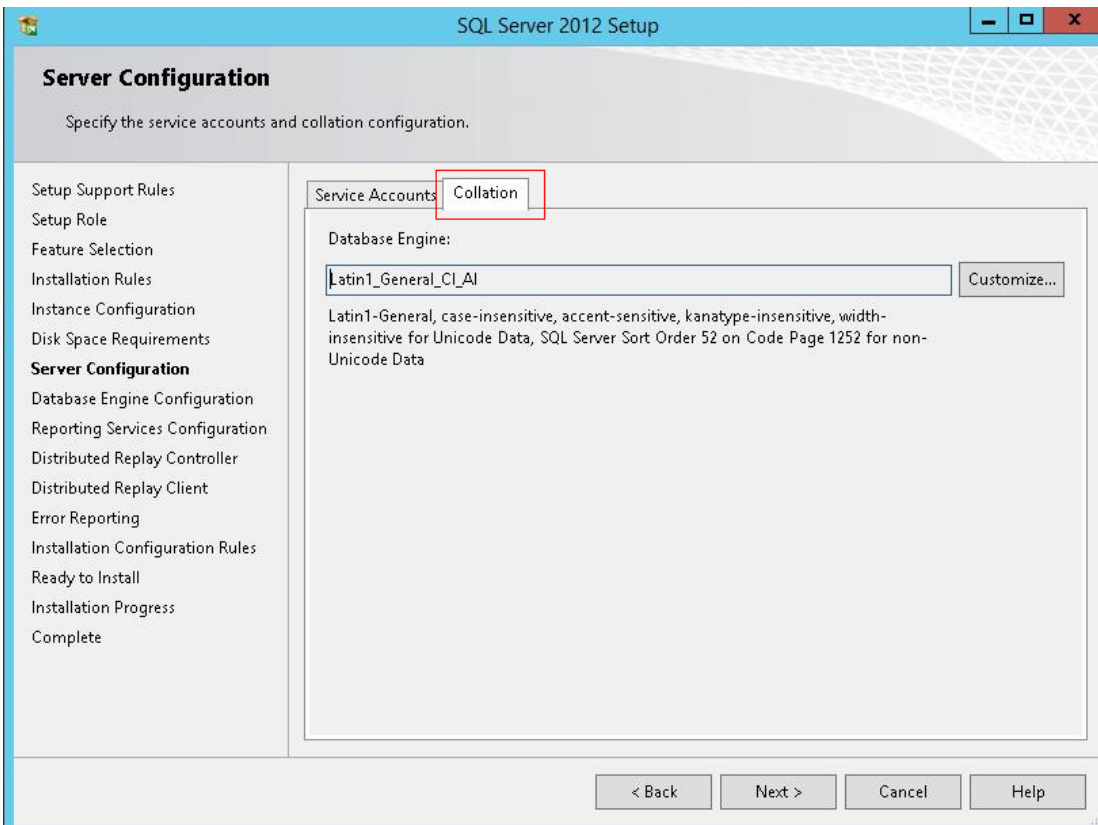
16) Click **OK**.



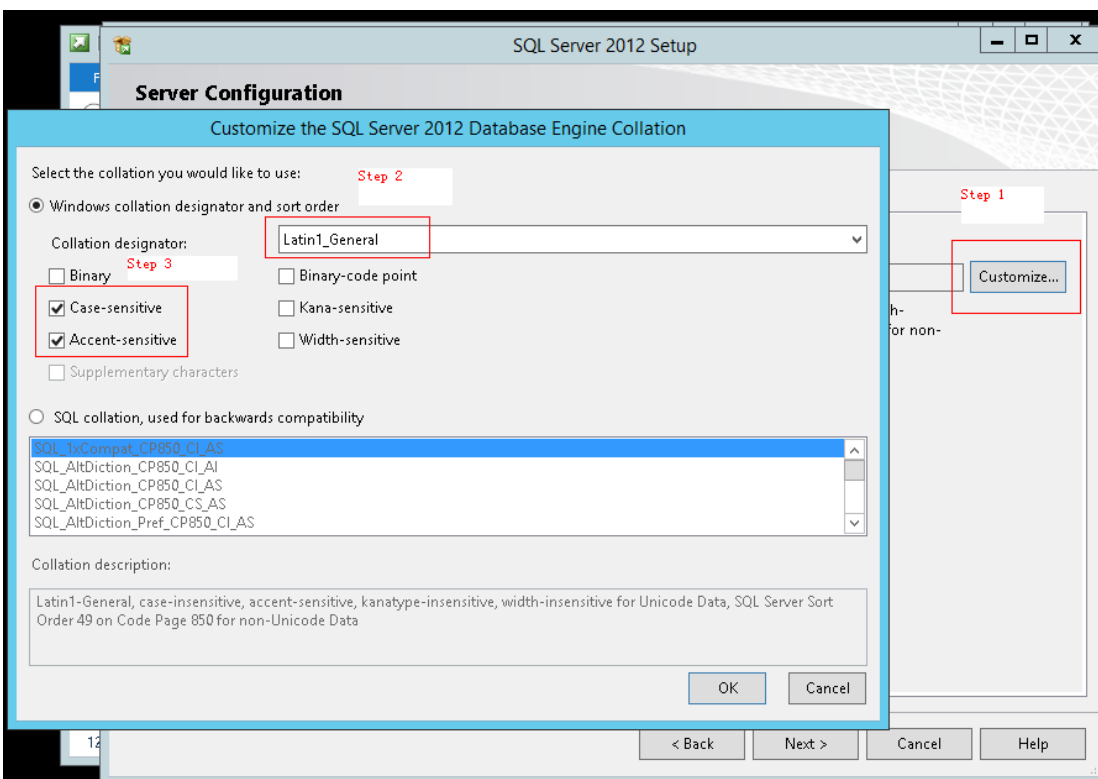
- 17) As shown in the following figure, choose **Administrator** for the five services, and input the system login password as the password.



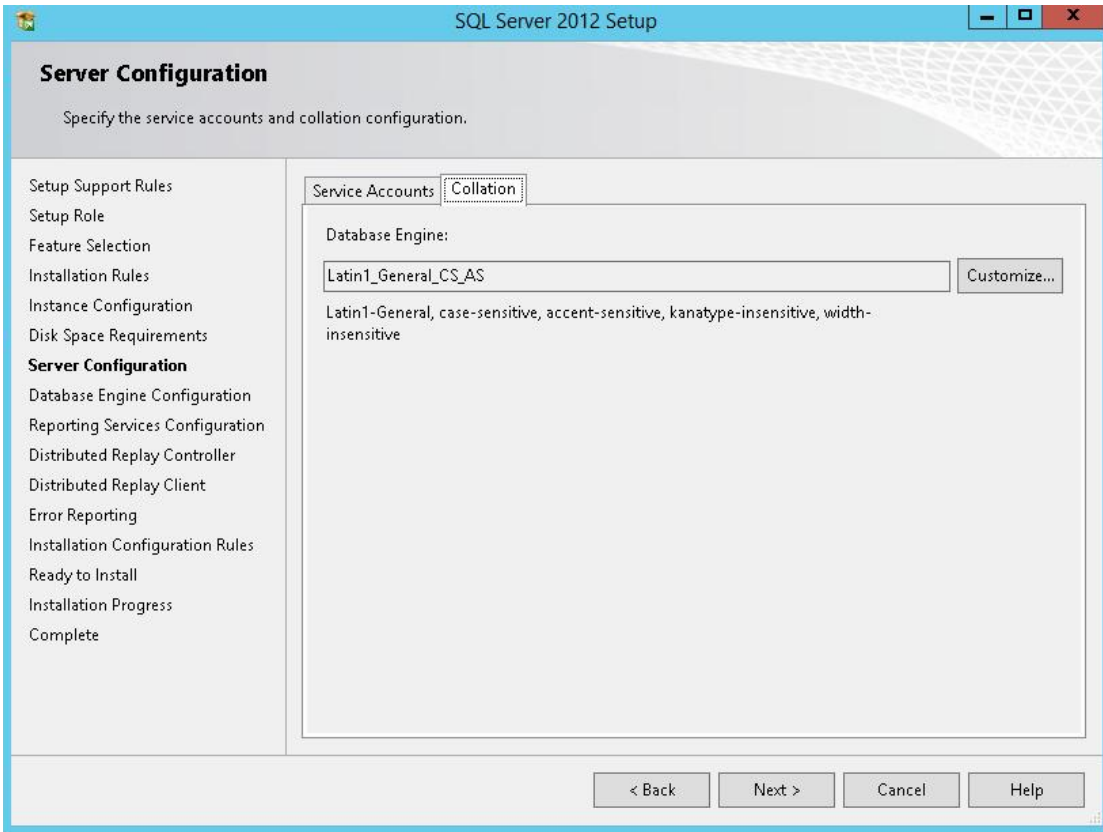
- 18) Choose the **Collation** tab.



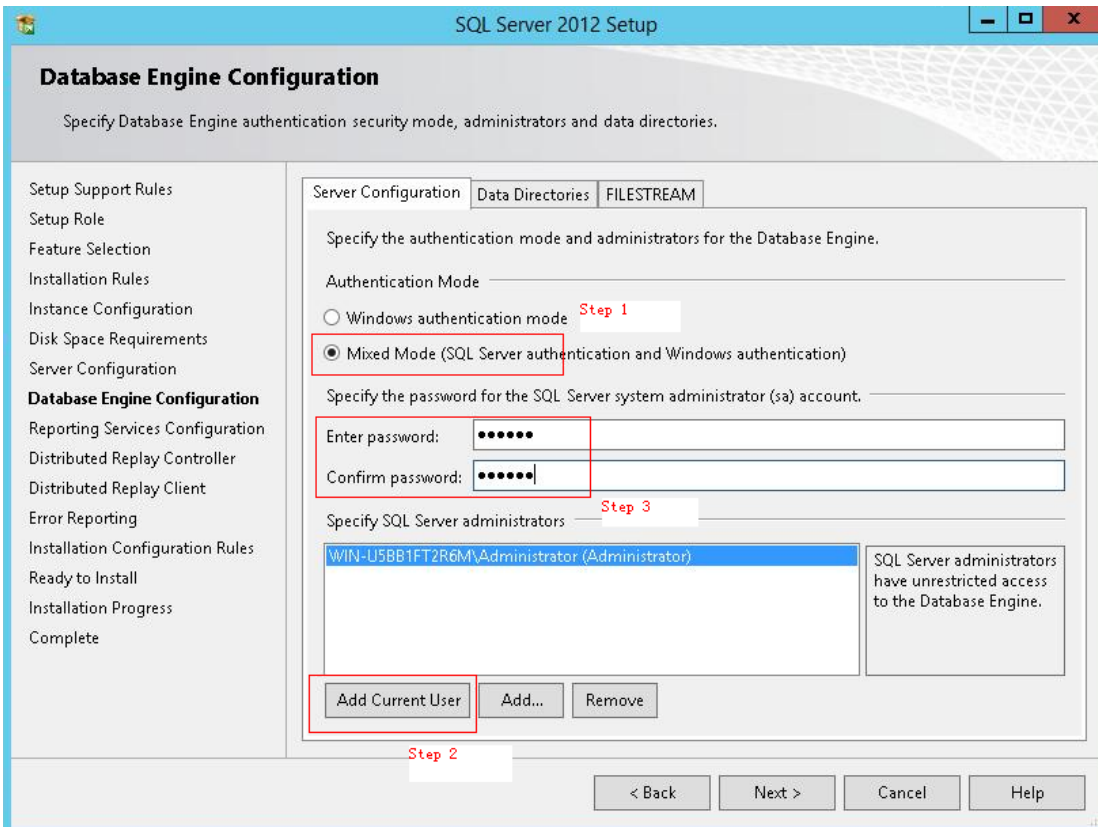
- 19) Configure collation. Make sure that the configuration is done exactly as shown in the following figure, or otherwise the SMP cannot run properly.



20) Click **Next**.

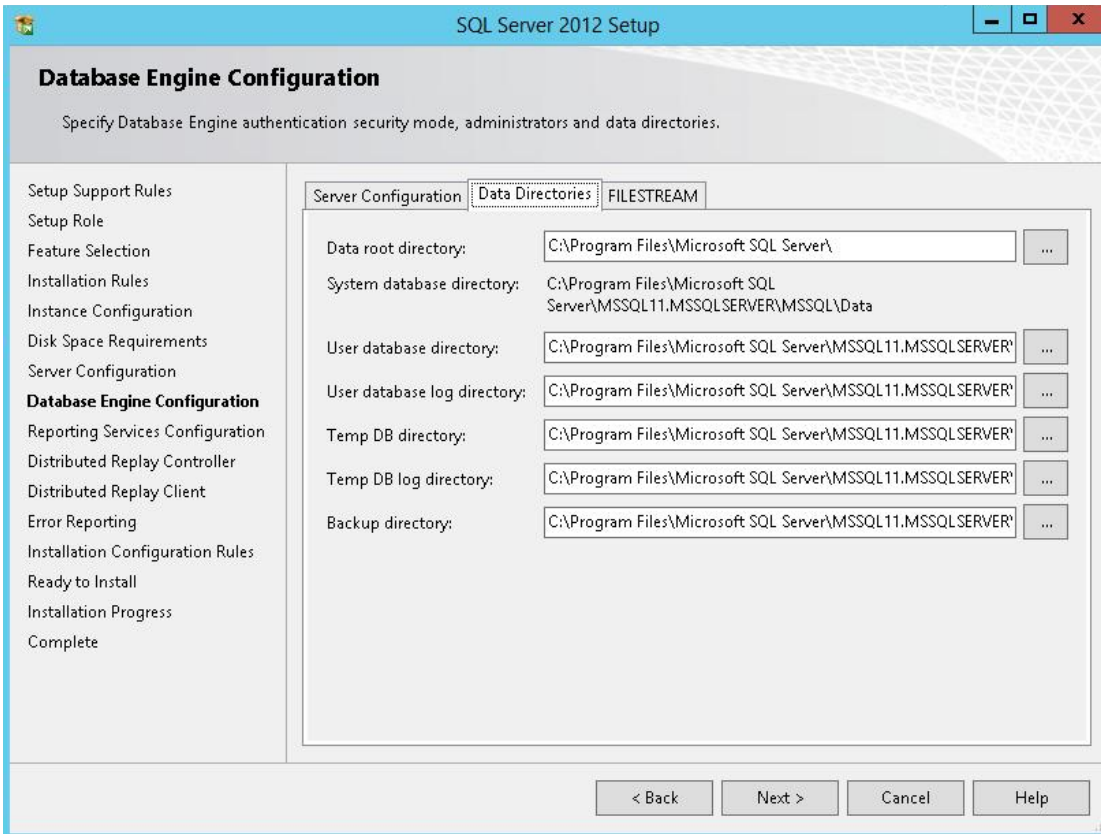


21) Configure a user account and a password.

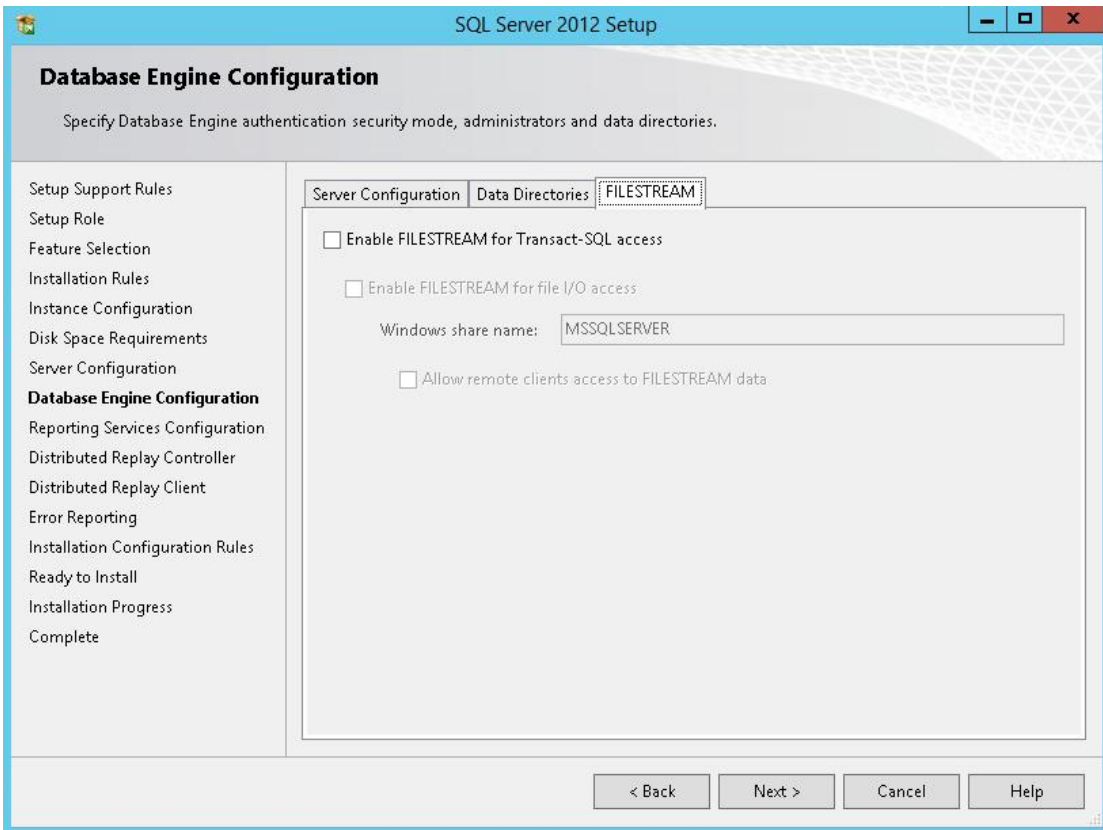


- 22) In the **Data Directories** tab, you may use the default configuration. If default drive space is insufficient, you may choose another drive.

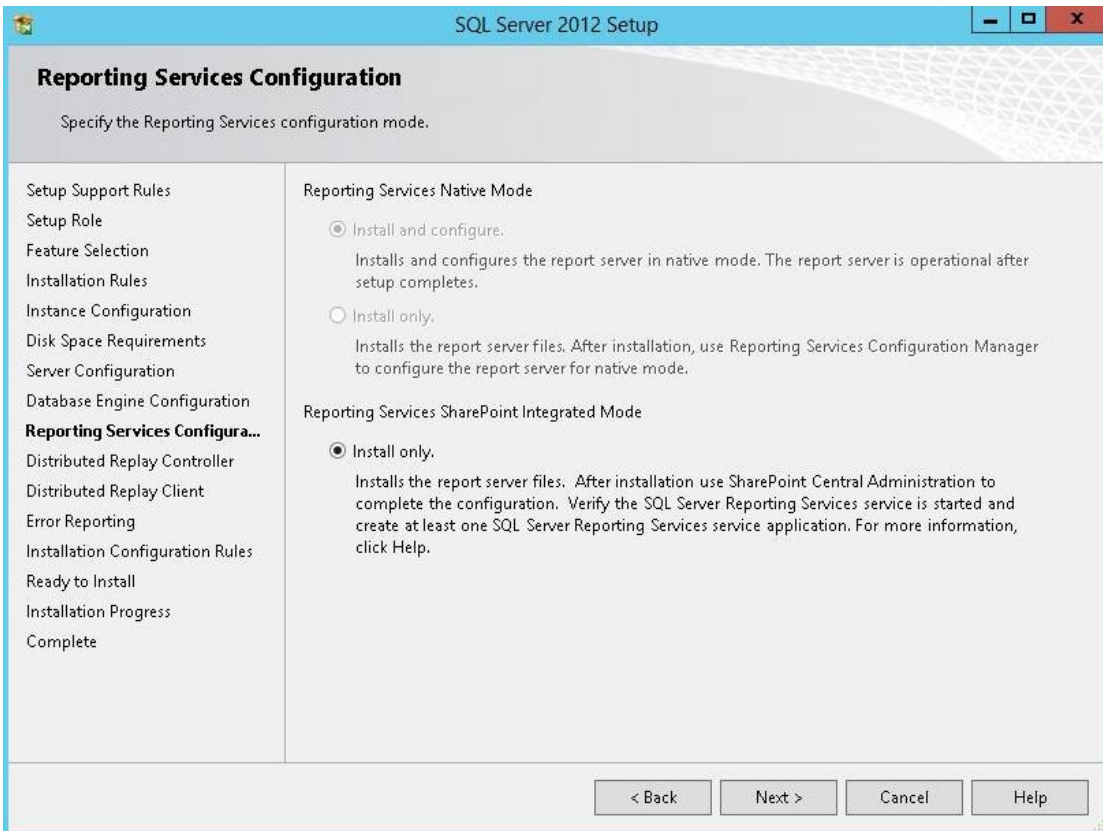




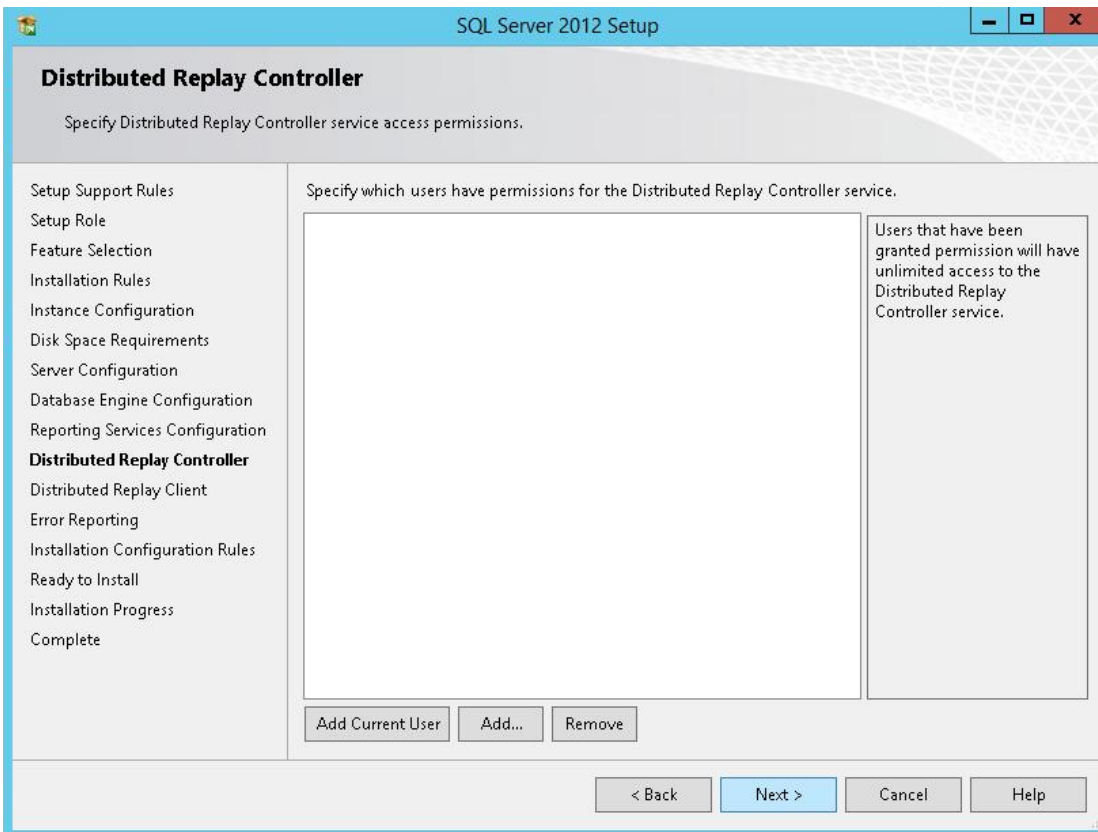
23) In the **FILESTREAM** tab, configure as shown in the following figure. Click **Next**.



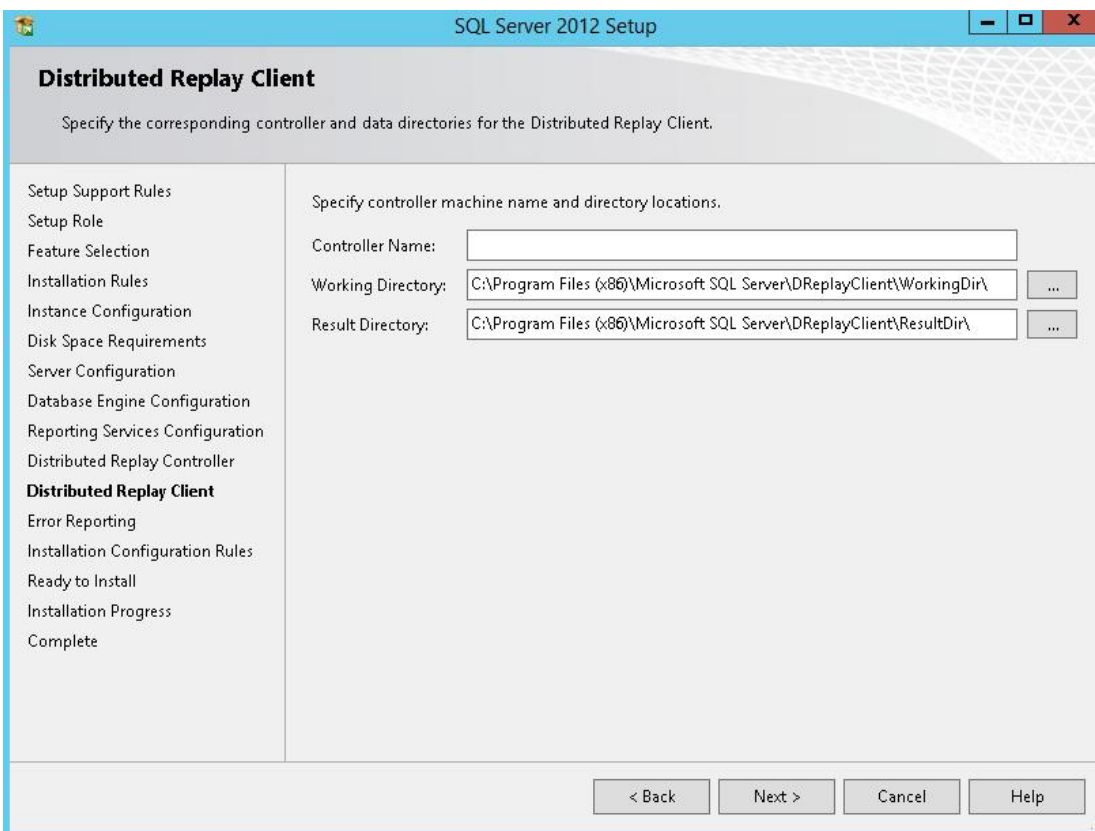
24) Click **Next**.



25) Click **Next**.



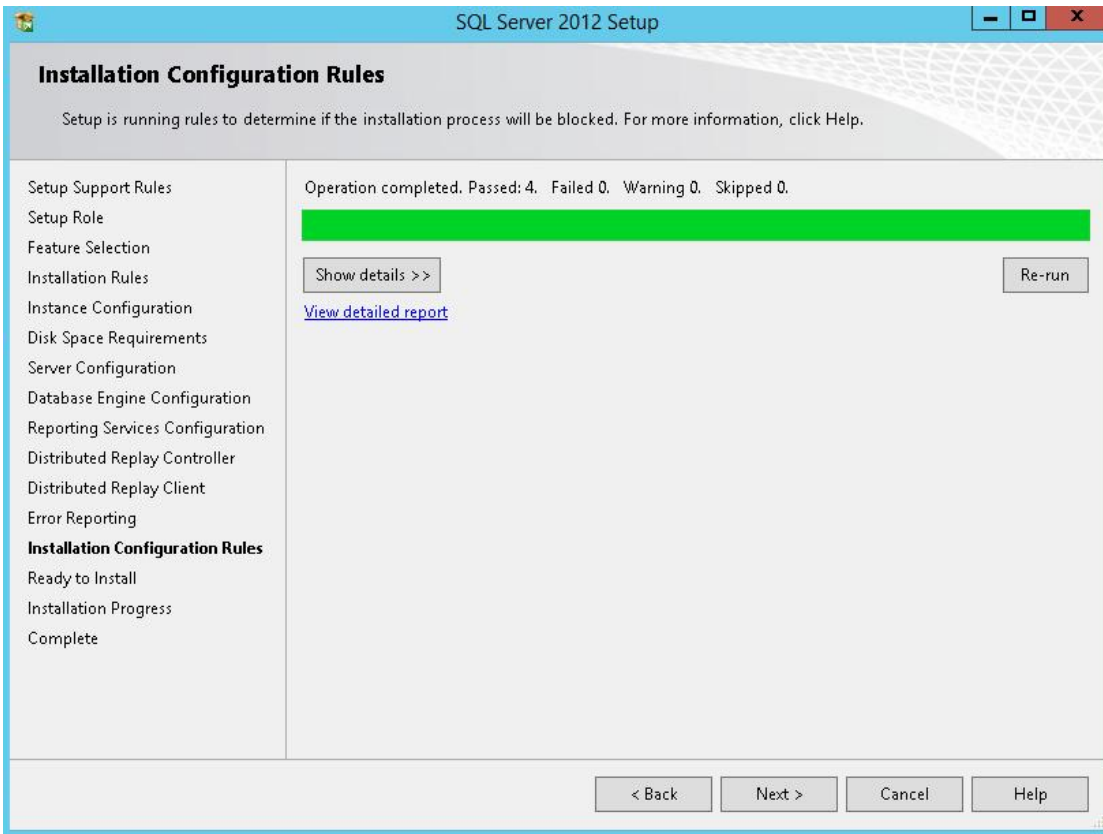
26) Click **Next**.



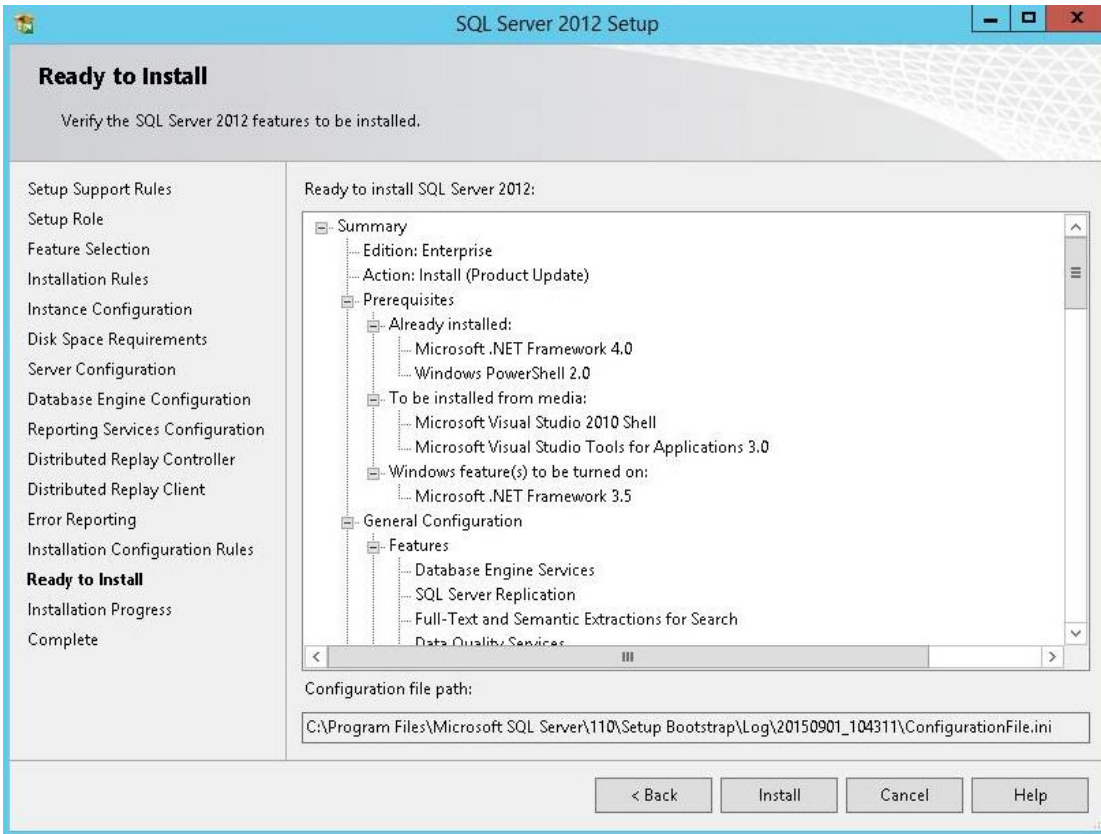
27) Click **Next**.



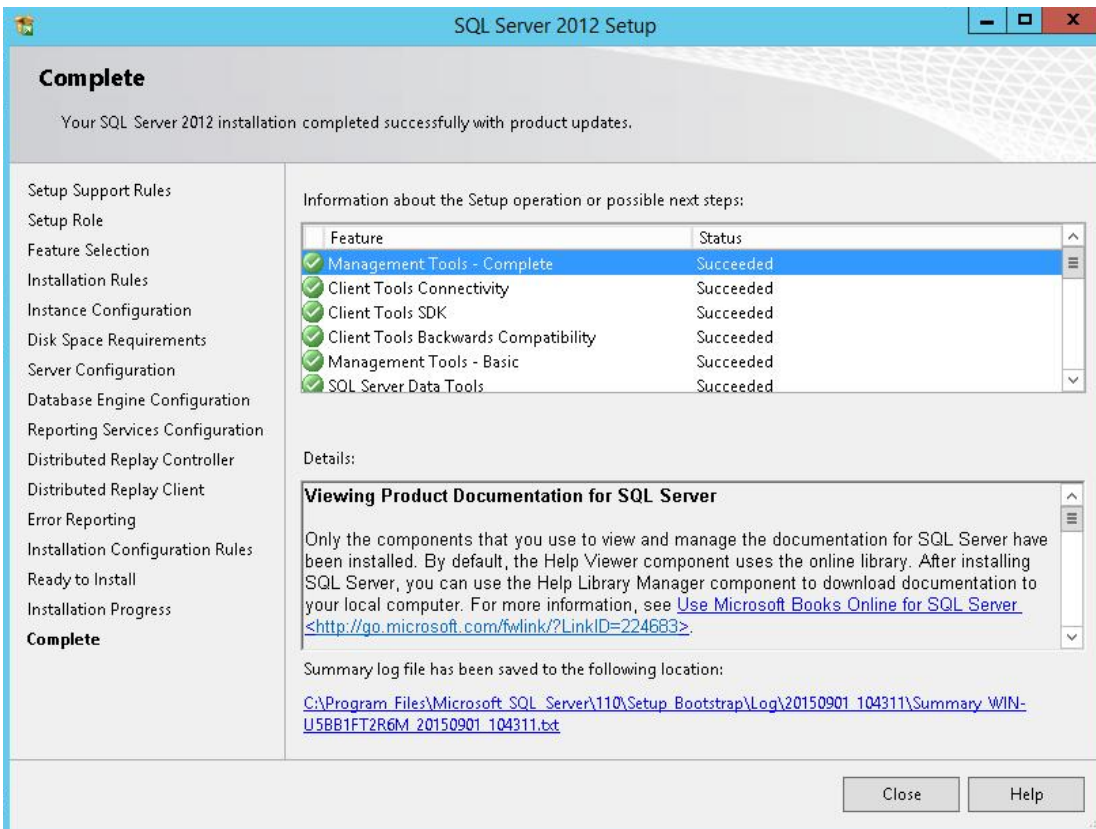
28) Click **Next**.



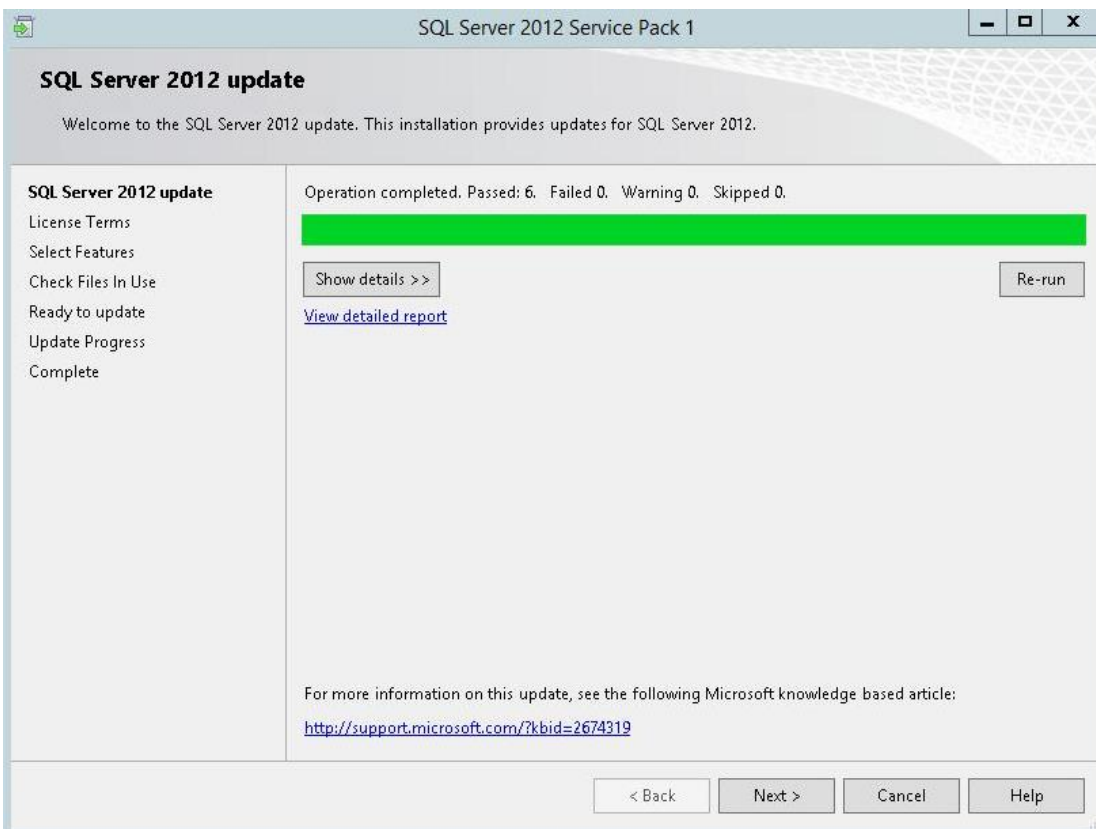
29) Click **Install**.



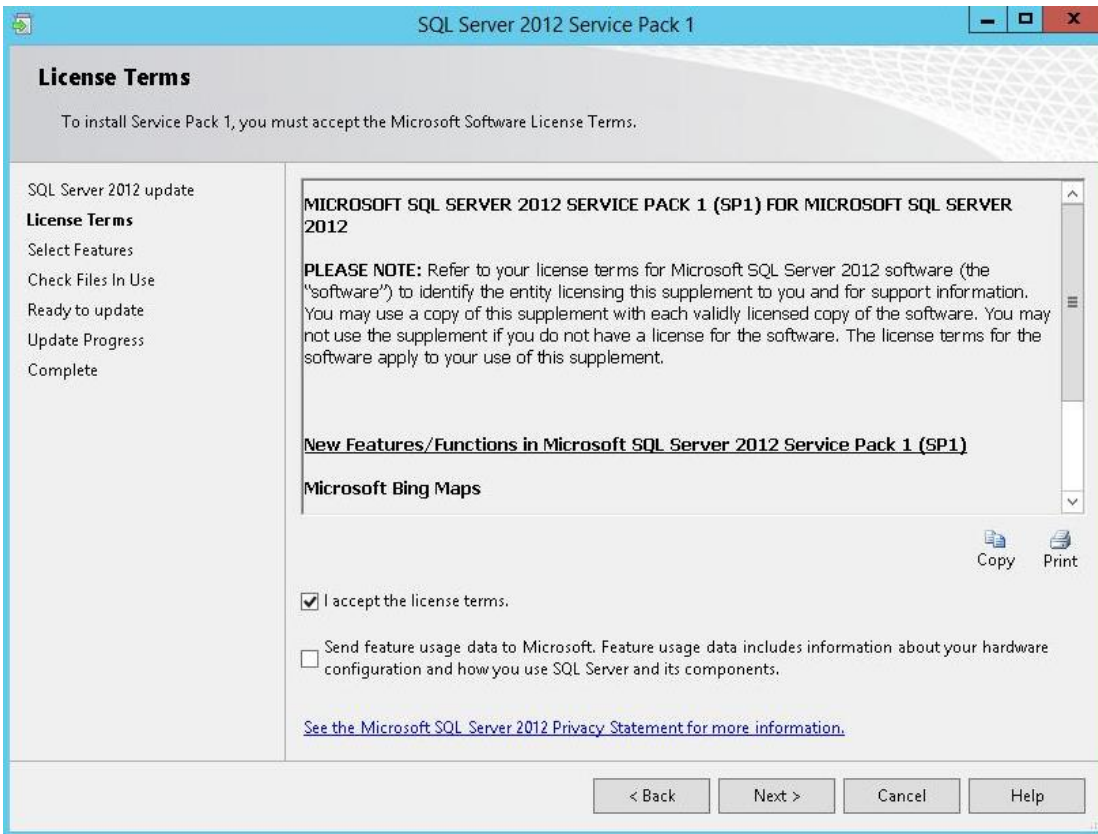
30) The installation is complete. Click **Close**.



31) Double click the SP1 patch, and click **Next**.

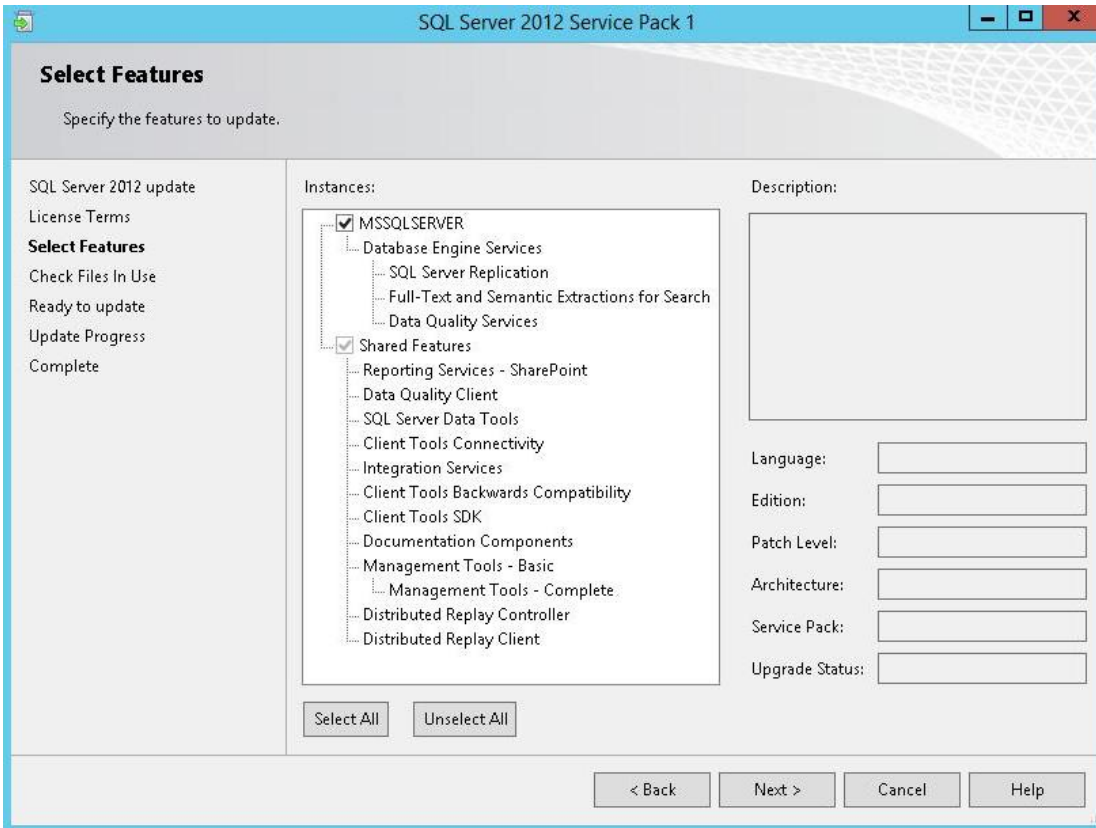


32) Tick **I accept the license terms**, and click **Next**.

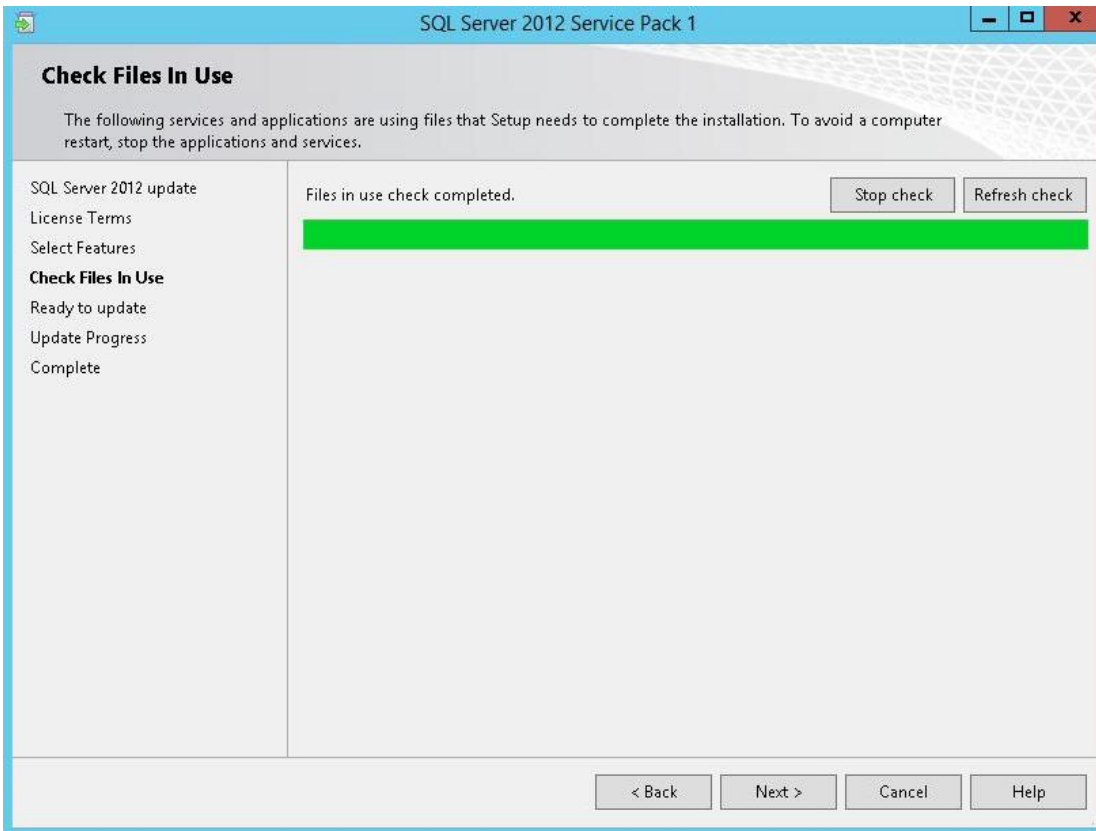


33) Click **Next**.

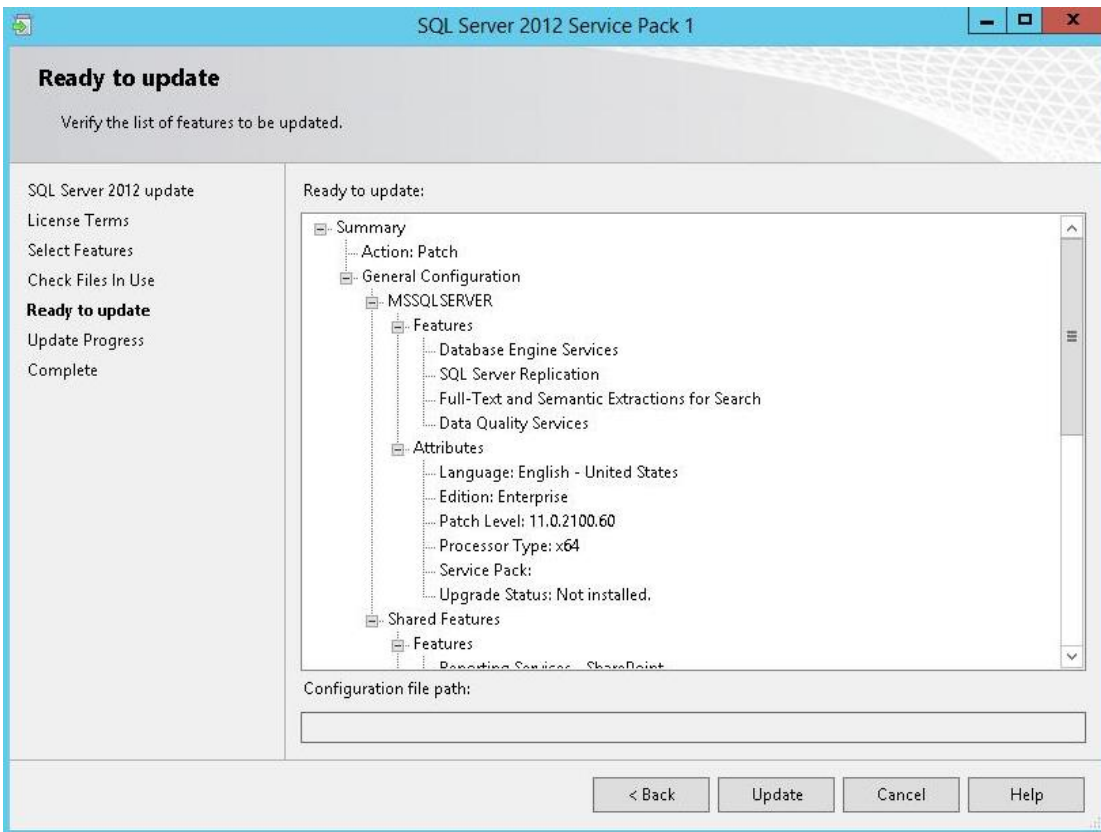




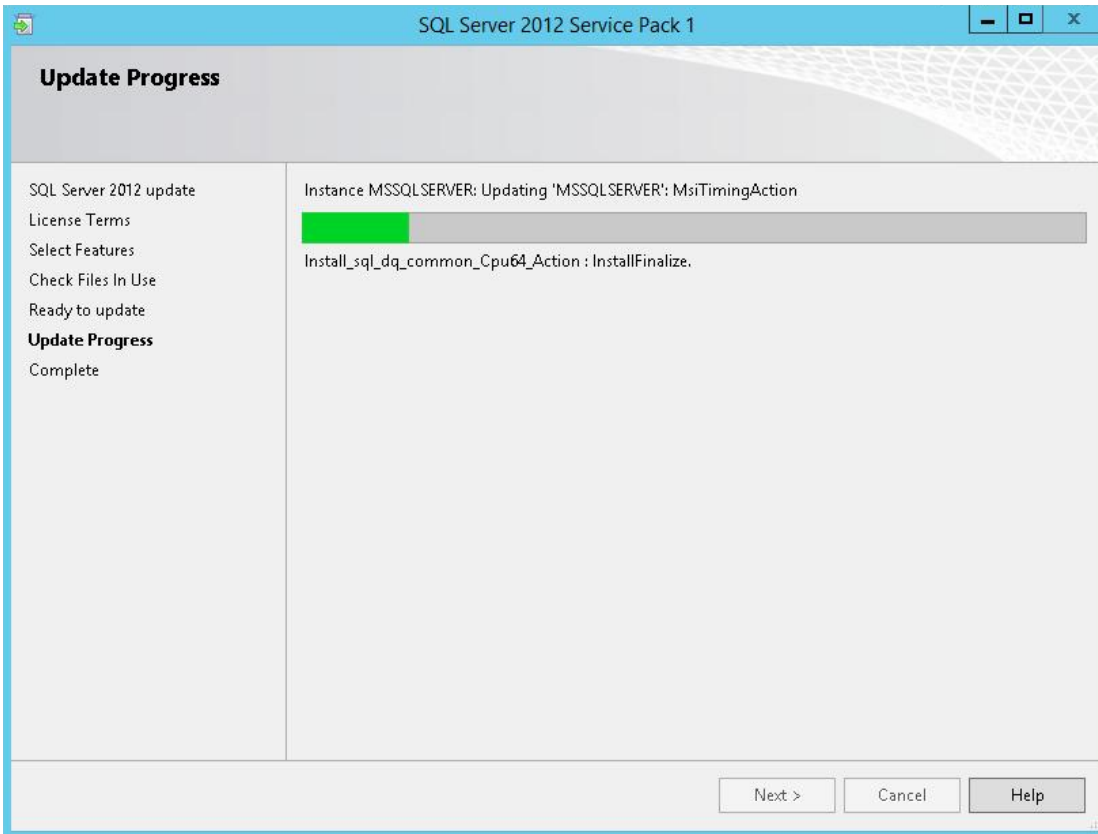
34) Click **Next**.



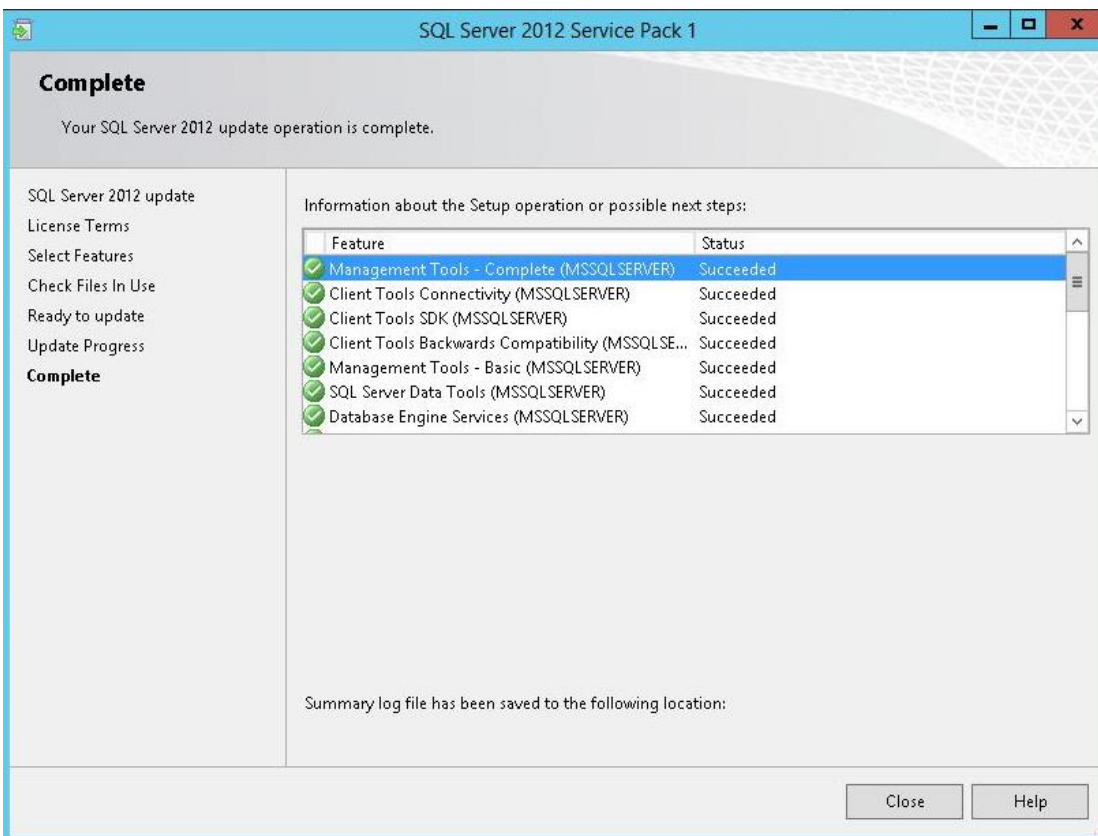
35) Click **Update**.



36) Click **Next**.



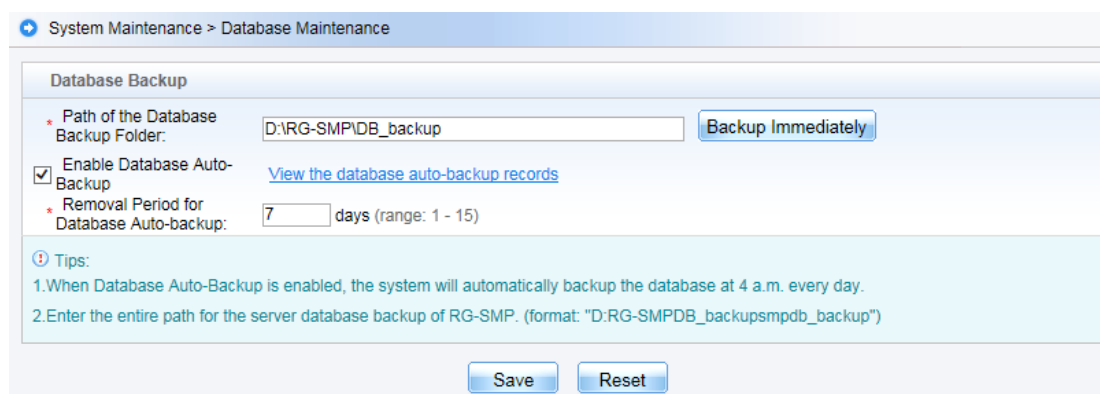
37) The installation is complete. Click **Close**.





## 1.4 Backup Database

In this section, you will learn how to backup database.

Go to **System Maintenance > Database Maintenance**, by default auto backup is enabled and the schedule is executed at 4:00 in the morning every day. You can set the removal period in which backup database will be removed automatically.



Click **Backup Immediately** to backup current database, then browse and save to local disk.

 **Tips:** Database backup succeeded. If your browser does not perform auto-download, click  [here](#) to download.

Close

## 1.5 USB Dongle and License Management

SMP license is a red USB dongle which looks like USB drive. Plug in USB dongle in SMP Server before starting SMP service. SMP detects USB dongle at first startup and every 30 minutes when started up. SMP service will stop if USB dongle is missing.

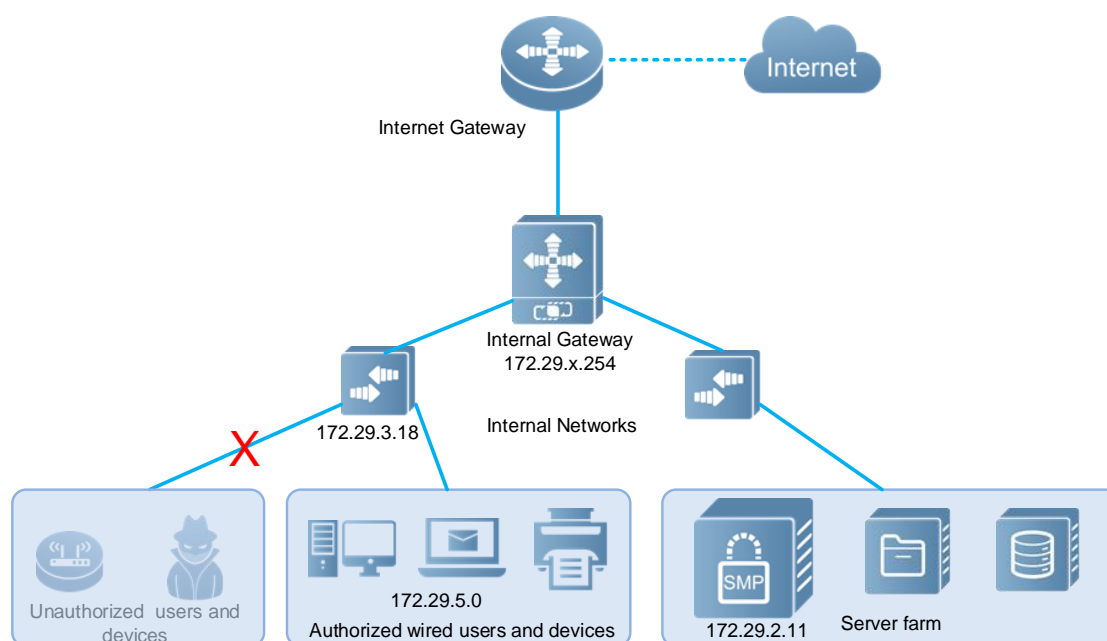
Click **System Status** in the top right on SMP WEB UI to display license status.

System Information					
Current System Status:	Normal <a href="#">(See details)</a>				
License Status:	The official version allows up to 150 online accounts (including users and MAC address authentication devices). 123 accounts are online currently.				
Online User:	<a href="#">123</a>	Insecure Online Users:	0	Peak Online User in 24hrs:	141
Authentication Failure Logs:	<a href="#">63</a>	Network Access Logs Today:	<a href="#">1228</a>		
Operation Logs:	<a href="#">113</a>				

## 2 Practical Scenarios

In this section, you will learn the most recommended SMP solutions for users in enterprise, education, and other industries either for wired and wireless network. The SMP solutions mainly includes 802.1x authentication, web authentication, MAC authentication, Guest Authentication and Windows AD integration which cover the most of practical scenarios.

### 2.1 Wired Authentication



As per diagram shown above, it is a typical enterprise network. Authorized wired users and devices, like personal computer, laptop, printer, IP phone, IP camera, are able to access Intranet and Internet. But unauthorized wired users & devices, like personal home device, guests are not able to access any resources or impact production network at all.

You will learn three authentication methods for wired access:

- 802.1x Authentication
- MAC Authentication
- Web Authentication

## 2.1.1 802.1x Authentication

802.1x Authentication allowed users to access network by verifying their username and password. For more information about IEEE standard 802.1x protocol, see *Ruijie Wireless configuration guide* or *Ruijie Switch configuration guide*.

There are three components in 802.1x Authentication.

- SMP server(Radius Server)
- Access switch(NAS ,Network Access Server)
- Computer with Ruijie SA Client(Security Agent)

In this example, we are using *Ruijie Gigabit Switch S2928G-E with software version 10.4(2b12)p6* as Access Switch , and *Ruijie Security Agent software version V1.60*.

**Note: Third party access switch which supports IEEE standard 802.1x protocol is applicable also.**

### Step 1, Configure SNMP on Access switch

Enable SNMP on access switch, set the read & write community string to “ruijie”.

```
snmp-server community ruijie rw
snmp-server host 172.29.2.11 traps Ruijie
snmp-server enable traps
```

### Step 2, Add Access switch to SMP

Edit SMP device template first, go to *Authentication & Authority > Device > NAS Configuration Templates*, modify *Ruijie Wired Device*, set the parameters as below,

All  None	Template Name	SNMP v2c community	Operation
<input type="checkbox"/>	VPN Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Standard Radius Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Ruijie Wireless Device	ruijie	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Ruijie Wired Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	RG-EG Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	RG-ACE Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Non-Ruijie Wired Device	public	<a href="#">View</a>   <a href="#">Modify</a>

Totally 7 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

Identity Authentication Key is used for Radius Server.

**Identity Authentication Configuration**

\* Identity Authentication Key:

*Tips:* The system and devices perform user authentication via the Radius Protocol. Identity authentication key is used for the encryption of data packets and should be the same as that of the devices.

Web Authentication Key is used for Web Portal.

**Web Authentication Configuration**

Web authentication Key:

*Tips:* After the Web authentication key is specified, the system will support Web authentication.

**Note: Web portal key is not occupied in 802.1x authentication, we just configure it for the following Web authentication in advance.**

SNMP community is used for SNMP management.

**SNMP Configuration**

\* SNMP v2c Community:

*Tips:* The SNMP configuration should be the same as that on the devices. Otherwise the system cannot manage the devices.

Click **Modify** when complete setting.

Go to **Authentication & Authority > Device > Add**, input **NAS IP address**, select **Device Template**, System will get relevant information via SNMP automatically. Click **Add** to finish.

\* NAS IP:  (Format: 192.168.20.1)

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

NAS MAC:  (Format: 00D0F8000001)

NAS Name:

NAS Location:

NAS Information:

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

### Step 3, Create account on SMP

Go to **Authentication & Authority > User > Add**, fill in required fields, here we create a user named "Henry" and put it into **Default User Group**. Common User indicates it is a SMP local user account.

**Basic Information**

\* User Type:  Common User  Guest User  Thirdparty User

\* User Name:

Nick Name:

\* Password:

\* Confirm Password:

\* User Status:  Normal  Suspended

\* Full Name:

\* Type of Account Validity Period:  Never Expire  Delete Account when Expire  Suspend Account when Expire

\* User Group:  [Select User Group](#)



#### Step 4, Configure Radius Server parameters on Access switch

```
aaa new-model
aaa accounting update
aaa accounting network For1x start-stop group radius
aaa authentication dot1x For1x group radius
radius-server host 172.29.2.11 key ruijie
dot1x accounting For1x
dot1x authentication For1x
```

#### Step 5, Enable 802.1x authentication on port

```
interface GigabitEthernet 0/21
dot1x port-control auto
```

#### Step 6, Install Ruijie SA (Security Agent) on End computer.

For more information about how to install SA, see [Appendix > SA](#).

#### Verification

Open SA, input username and password, click Connect.



Succeed in authentication.



Go to **SMP > Authentication & Authority > Online User**, you can view Henry is online now .

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

All   None	User Name	Full Name	User IP	NAS IP	NAS Port	Online Time	Operation
<input type="checkbox"/>	Henry	Henry Chan	172.29.5.1	172.29.3.18	21	0:7:49	<a href="#">View</a>   <a href="#">More...</a>

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

Go to **AccessSwitch**, execute command "**show dot1x summary**", the port-status is authenticated

```
AccessSwitch#show dot1x summary
ID      user      MAC          Interface VLAN Auth-State  Backend-State Port-Status User-Type Time
-----
41     henry    448a.5b3b.45db  Gi0/21   5   Authenticated  Idle          Authed      static  0days 0h 0m13s
AccessSwitch#
```

## 2.1.2 Mac Authentication

Actually, MAC authentication is a kind of 802.1x authentication, the difference is that in MAC authentication, both the username & password are device MAC address. Mac authentication is used for dumb devices which do not support 802.1x, like printer, IP camera, and IP phone and so on.

There are three components in MAC Authentication.

- SMP server(Radius Server)
- Access switch(NAS ,Network Access Server)
- Dumb devices

In this example, we are using *Ruijie Gigabit Switch S2928G-E with software version 10.4(2b12) p6* as Access Switch.

**Note: Third party access switch which supports IEEE standard 802.1x protocol is applicable also.**

Step 1, Go through [Step 1](#) ,2 , 4 in previous 802.1x Authentication Chapter, then enable MAC authentication on port

```
interface GigabitEthernet 0/21
dot1x port-control auto
dot1x mac-auth-bypass
```

### Step 2, Create MAC Account on SMP

Go to *Authentication & Authority > MAC Terminal >Add*, input MAC address, click Add.

MAC Terminal Information	
* Terminal MAC :	<input type="text" value="448a5b3b45"/> (Format:00D0F8000001)
Switch to the target VLAN after Authentication :	<input type="checkbox"/>
Terminal Description :	<input type="text" value="my printer"/>
<input type="button" value="Add"/> <input type="button" value="Reset"/> <input type="button" value="Return"/>	

## Verification

Connect your printer to network, it will pass the authentication in a few seconds.

Go to **SMP >Authentication & Authority > MAC Terminal**, the printer is in connected status.

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

All None	Terminal MAC	NAS IP	NAS Port	VLAN	Connection Status	Blacklisted or not	Terminal Description	Operation
<input type="checkbox"/>	448a5b3b45db	172.29.3.18	21		Connected	No	my printer	<a href="#">View</a>   <a href="#">Modify</a>

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

Go to Access Switch, execute command “show dot1x summary”, the username is MAC address.

```
AccessSwitch#show dot1x summary
ID      User      MAC      Interface  VLAN  Auth-State  Backend-State  Port-Status  User-Type  Time
-----
43      448a5b3... 448a.5b3b.45db  Gi0/21    5     Authenticated  Idle           Authed      static     0days 0h 2m 6s
AccessSwitch#
```

### 2.1.3 Web Authentication

Web authentication is applicable for scenarios in which users would not install additional client on their computer. When users try to access network, web authentication page pops up, users input their username & password to pass authentication.

There are three components in Web Authentication.

- SMP server(Radius and Portal Server)
- Access switch(NAS ,Network Access Server)
- Computer

In this example, we are using *Ruijie Gigabit Switch S2928G-E with software version 10.4(2b12) p6* as Access Switch.

**Note: Web Portal is Private protocol, so you should deploy Ruijie switch only, third party switch have compatibility issues.**

Step 1, Go through [Step 1](#) - 3 in previous 802.1x Authentication Section.

#### Step 2, Configure Radius Sever parameters on Access Switch

```
aaa new-model
aaa accounting update
aaa accounting network Forweb start-stop group radius
aaa authentication web-auth Forweb group radius
web-auth authentication v2 Forweb
web-auth accounting v2 Forweb
radius-server host 172.29.2.11 key ruijie
```

#### Step 3, Configure Web Portal parameters on Access Switch

```
portal-server eportalv2 ip 172.29.2.11 url http://172.29.2.11:80/smp/commonauth
web-auth portal eportalv2
web-auth portal key ruijie
```

```
http redirect direct-site 172.29.7.254 arp
web-auth offline-detect flow idle-timeout 10 threshold 100
```

**Note:** Go to *SMP > Authentication & Authority > Portal Settings > Tips*, you can find the detail URLs for different methods.

#### Step 4, Enable Web authentication on Port.

```
interface GigabitEthernet 0/21
web-auth port-control
arp-check
```

#### Step 5, Optional Settings

Bypass the public resources which allowed to be visited before Web authentication. For example, 192.168.5.1 is a Free Web Server

```
http redirect direct-site 192.168.5.1
```

Bypass the specific IP that is free of Web authentication. For example, 192.168.4.12 is IP address for Department Manager.

```
web-auth direct-host 192.168.4.12 arp
```

#### Verification

Visit any HTTP site, you will be redirect to Web authentication page, like below diagram.

**Restriction: Unable to redirect HTTPS web page.**

Input username & password , click Login. You will get Login success page .

Go to **SMP > Authentication & Authority > Online User**, you can view Henry is online now

All None	User Name ▾	Full Name ▾	User IP ▾	NAS IP ▾	NAS Port	Online Time ▾	Operation
<input type="checkbox"/>	<a href="#">Henry</a>	Henry Chan	172.29.5.1	172.29.3.18	21	0:3:41	<a href="#">View</a>

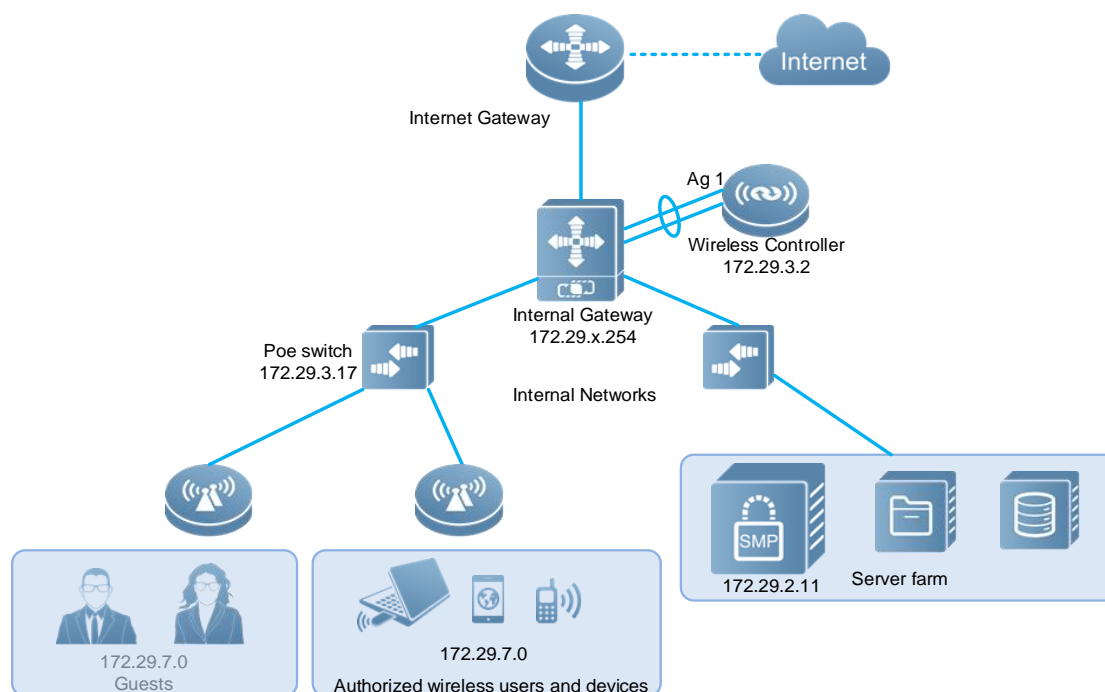
Go to Access Switch, execute command “**show web-auth user all**” to display online web user.

```
AccessSwitch#show web-auth user all
Statistics:
Type           Online Total
-----
v1 portal      0       0
v2 Portal      1       1
-----
Total          1       1

v1 Portal Authentication Users
Index Address      Online Time Limit Time used Status
-----
-----

v2 Portal Authentication Users
Index Address      Online Time Limit Time used Status
-----
-----
1      172.29.5.1      on    0d 00:00:00 0d 00:02:00 Authenticated
-----
AccessSwitch#
```

## 2.2 Wireless Authentication



As per diagram shown above (Ag 1 means Aggregate Port 1), it is a typical wireless network. Staff are able to access wireless network using their laptop, pad and mobile phone. SMP manages user accounts, authorities and other information.

In this section, you will learn three authentication methods for wireless access:

- Seamless 802.1x Authentication(BYOD)
- MAC Authentication
- Seamless Web Authentication(BYOD)

**Note: Usually, above three methods are applied for Staff. For guest users, see following section *Authentication for Guest*.**



## 2.2.1 Seamless 802.1x Authentication (BYOD)

Why we call it “Seamless” The perfect user experience it delivers. During seamless 802.1x authentication, you just need to input username & password at the first time connecting to wireless network, then never ever input again can you access network seamlessly in the future.

There are three components in this authentication.

- SMP server(Radius Server)
- Wireless Controller (NAS) and Access Points
- Wireless Users(Usually applied to Staff)

Below commands do not include basic wireless configurations, ensure your wireless network works properly before starting.

It is recommended to create a dedicate Wlan SSID for *Seamless 802.1x authentication*.

**Note: Ruijie BYOD is a Private solution, so you should deploy Ruijie wireless devices only, third party devices have compatibility issues.**

In this example, we are using *Ruijie Wireless Controller WS6108 and AP320-I with software version 11.1(5) B7*.

### Step 1, Configure SNMP on Wireless Controller

```
snmp-server community ruijie rw
snmp-server host 172.29.2.11 traps Ruijie
snmp-server enable traps
```

### Step 2, Add Wireless Controller to SMP


Edit SMP device template first, go to *Authentication & Authority > Device > NAS Configuration Templates*, modify *Ruijie Wireless Device*, set the parameters as below,

All   None	Template Name ▼	SNMP v2c community	Operation
<input type="checkbox"/>	VPN Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Standard Radius Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Ruijie Wireless Device	ruijie	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Ruijie Wired Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	RG-EG Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	RG-ACE Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Non-Ruijie Wired Device	public	<a href="#">View</a>   <a href="#">Modify</a>


Totally 7 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [Go](#)

⏪ ⏩ ⏴ ⏵

Identity Authentication Key is used for Radius Server.


Identity Authentication Configuration	
* Identity Authentication Key:	<input type="text" value="ruijie"/>
<p> Tips: The system and devices perform user authentication via the Radius Protocol. Identity authentication key is used for the encryption of data packets and should be the same as that of the devices.</p>	

Web Authentication Key is used for Web Portal

Web Authentication Configuration	
Web authentication Key:	<input type="text" value="ruijie"/>
<p> Tips: After the Web authentication key is specified, the system will support Web authentication.</p>	


**Note: Web portal key is not occupied in 802.1x authentication, we just configure it for the following Web authentication in advance.**

SNMP community is used for SNMP management.

SNMP Configuration	
* SNMP v2c Community:	<input type="text" value="ruijie"/>
<p> Tips: The SNMP configuration should be the same as that on the devices. Otherwise the system cannot manage the devices.</p>	

Click **Modify** when complete settings.

Go to **Authentication & Authority > Device > Add**, input **NAS IP address**, select **Device Template**, System will get relevant information via SNMP automatically. Click **Add** to finish.

Basic Information	
* NAS IP:	<input type="text" value="172.29.3.2"/> (Format: 192.168.20.1)
* NAS Configuration Templates:	<input type="text" value="Ruijie Wireless Device"/> <a href="#">Obtain Device Information</a>   <a href="#">View Template</a>   <a href="#">Add Template</a>
NAS MAC:	<input type="text"/> (Format: 00D0F8000001)
NAS Name:	<input type="text" value="WS6108"/>
NAS Location:	<input type="text"/>
NAS Information:	<input type="text" value="Ruijie Gigabit Wireless Switch(WS6108) By Ruijie Networks."/>
<p> <b>Tips:</b> You can set a template for the devices sharing the same SNMP version, authentication and Telnet parameters.</p>	
<input type="button" value="Add"/> <input type="button" value="Reset"/> <input type="button" value="Return"/>	

### Step 3, Create account on SMP

Go to **Authentication & Authority > User > Add**, fill in required fields, here we create a user named "Henry", and put it into **Default User Group**.

**Common User** indicates it is a SMP local user account.

Basic Information	
* User Type:	<input checked="" type="radio"/> Common User <input type="radio"/> Guest User <input type="radio"/> Thirdparty User
* User Name:	<input type="text" value="Henry"/>
Nick Name:	<input type="text"/>
* Password:	<input type="password" value="*****"/>
* Type of Account Validity Period:	<input checked="" type="radio"/> Never Expire <input type="radio"/> Delete Account when Expire <input type="radio"/> Suspend Account when Expire
* User Group:	<input type="text" value="Default User Group"/> <a href="#">Select User Group</a>
* User Status:	<input checked="" type="radio"/> Normal <input type="radio"/> Suspended
* Full Name:	<input type="text" value="Henry Chan"/>
* Confirm Password:	<input type="password" value="*****"/>

## Step 4, Configure Authentication method on SMP

Go to **SMP > Authentication & Authority > Authentication Settings > Authentication Parameters**, select **PEAP\_MSCHAP** in drop down list of **Preferred Wireless Authentication**.

Authentication Parameters	
* Authentication Port:	<input type="text" value="1812"/> (Default: 1812)
* Accounting Port:	<input type="text" value="1813"/> (Default: 1813)
Record Update Flow:	<input type="checkbox"/>
Enable Nick Name Authentication:	<input type="checkbox"/>
When account logins exceed the limit, deal as follows:	<input type="text" value="The new client will not be able to authenticate."/> <input type="button" value="v"/>
Preferred Wireless Authentication:	<input type="text" value="PEAP_MSCHAP"/> <input type="button" value="v"/>
Click <a href="#">here</a> to import the wireless authentication server certificate.	
Tip: The Authentication Port cannot be the same as the Accounting Port.	

## Step 5, Configure Radius Server and 802.1x parameters on Wireless Controller

```

aaa new-model
aaa authentication dot1x For1x group radius
aaa accounting network For1x start-stop group radius
radius-server host 172.29.2.11 key ruijie
dot1x valid-ip-acct enable
ip dhcp snooping

```

### Apply IP DHCP Snooping trust to uplink port

```

interface AggregatePort 1
ip dhcp snooping trust

```

## Step 6, Enable 802.1x authentication on WLAN ID.

```

wlansec 2
security rsn enable
security rsn ciphers aes enable
security rsn akm 802.1x enable
dot1x authentication For1x
dot1x accounting For1x

```

### Verification

Take Windows 7 as example, input username & password at the first time connecting to wireless network, click “connect” when security alert prompts, then you will be online.



Go to **SMP > Authentication & Authority > Online User**, you can view Henry is online now.

All   None	User Name	Full Name	User IP	NAS IP	NAS Port	Online Time	Operation
<input type="checkbox"/>	Henry	Henry Chan	172.29.7.2	172.29.3.2	2	0:5:2	<a href="#">View</a>

Go to wireless controller , execute command **show dot1x summary** , the port status is authenticated.

```
WS6108#show dot1x summary
ID      Username  MAC          Interface  VLAN  Auth-State  Backend-state  Port-Status  User-Type  Time
-----
1289    henry     ec26.cae1.1999 wlan 2    7    Authenticated  Idle         Authed     static    0days 0h 5m34s
WS6108#
```

Move away from this wireless coverage, disconnect the wireless network, and then go back again. The wireless network will be recovered seamlessly.

## 2.2.2 Mac Authentication

Actually, MAC authentication is a kind of 802.1x authentication, the difference is that in MAC authentication, both the username & password are device MAC. Mac authentication is used for wireless dumb devices that do not supports 802.1x like printer, IP camera, IP PDA and so on.

There are three components in this authentication.

- SMP server(Radius Server)
- Wireless Controller (NAS) and Access Points
- Wireless Dump Devices

Below commands do not include basic wireless configurations, ensure your wireless network works properly before starting.

It is recommended to create a dedicate Wlan SSID for *Mac Authentication*.

**Note: Ruijie BYOD is a Private solution, so you should deploy Ruijie wireless devices only, third party devices have compatibility issues.**

In this example, we are using *Ruijie Wireless Controller WS6108 and AP320-I with software version 11.1(5) B7*.

**Step 1, Go through [Steps 1](#) , 2 and 5 in previous Seamless 802.1x authentication (BYOD).**

```
dot1x valid-ip-acct enable
ip dhcp snooping
```

**Note: Above two commands is not required in MAC authentication**

**Step 2, Enable mac authentication on wireless controller**

```
wlansec 3
dot1x-mab
dot1x authentication For1x
dot1x accounting For1x
```

**Step 3, Create MAC account on SMP**

Go to *Authentication & Authority > MAC Terminal >Add*, input MAC address, click Add.

MAC Terminal Information	
* Terminal MAC :	<input type="text" value="28E14CB1719E"/> (Format:00D0F8000001)
Switch to the target VLAN after Authentication :	<input type="checkbox"/>
Terminal Description :	<input type="text" value="my wireless camera"/> x
<input type="button" value="Add"/> <input type="button" value="Reset"/> <input type="button" value="Return"/>	

## Verification

Connect your wireless dumb device to wireless network, no username & password is required .The device will be in connected status without authentication.

Go to **SMP >Authentication & Authority > MAC Terminal**, the wireless camera is in connected status.

All None	Terminal MAC	NAS IP	NAS Port	VLAN	Connection Status	Blacklisted or not	Terminal Description	Operation
<input type="checkbox"/>	28E14CB1719E	172.29.3.2	2		Connected	No	my wireless camera	<a href="#">View</a>   <a href="#">Modify</a>

Go to Access Switch , execute command **show dot1x summary**, the username is MAC address.

```
ws6108#show dot1x summary
ID      Username  MAC          Interface VLAN Auth-State  Backend-state Port-Status User-Type Time
-----
1304    28e14cb... 28e1.4cb1.719e wlan 2 7  Authenticated  Idle          Authed      static  0days 0h 4m17s
```

### 2.2.3 Seamless Web Authentication (BYOD)

The same to seamless 802.1x authentication(BYOD) , the main goal of this solution is to increase user experience while using wireless network .When connect to seamless web authentication network for the first time , you will be redirected to a web authentication page ,you need to input username & password to pass authentication .

For the second time, no web authentication is required any more, you will be in connected status directly. In addition, seamless web authentication combines both common web authentication and mac authentication.

There are three components in this authentication.

- SMP server(Radius and Portal Server)
- Wireless Controller (NAS) and Access Points
- Wireless Users(Usually applied to Staff)

Below commands do not include basic wireless configurations, ensure your wireless network works properly before starting.

It is recommended to create a dedicate Wlan SSID for *Seamless Web Authentication (BYOD)*.

**Note: Ruijie BYOD is a Private solution, so you should deploy Ruijie wireless devices only, third party devices have compatibility issues.**

In this example, we are using *Ruijie Wireless Controller WS6108 and AP320-I with software version 11.1(5) B7*.

**Step 1, Go through [Step 1](#) - 4 in previous Seamless 802.1x authentication (BYOD).**

**Step 2, Configure Radius Server parameters on wireless controller.**

```
aaa new-model
aaa accounting update
aaa accounting network Forweb start-stop group radius
aaa authentication web-auth Forweb group radius
aaa authentication dot1x For1x group radius
aaa accounting network For1x start-stop group radius
web-auth authentication v2 Forweb
web-auth accounting v2 Forweb
```

```
radius-server host 172.29.2.11 key ruijie
dot1x valid-ip-acct enable
ip dhcp snooping
```

### Apply IP DHCP Snooping trust to uplink port

```
interface AggregatePort 1
ip dhcp snooping trust
```

### Step 3, Configure Web Portal parameters on wireless controller

```
web-auth template web v2
 ip 172.29.2.11
 url http://172.29.2.11:80/smp/commonauth
web-auth portal eportalv2
web-auth portal key ruijie
http redirect direct-site 172.29.7.254 arp
web-auth offline-detect flow idle-timeout 10 threshold 100
```

**Note:** Go to *SMP > Authentication & Authority > Portal Settings > Tips*, you can find the detail URLs for different methods.

### Step 4, Apply Web authentication to specified WLAN ID

```
wlansec 4
web-auth portal web
web-auth accounting v2 Forweb
web-auth authentication v2 Forweb
webauth
dot1x-mab
dot1x authentication For1x
dot1x accounting For1x
```

**Note:** for wlansec 1, 1 indicates the wlan id, your wlan id may be not 1.

### Step 5, Optional Settings

Bypass the public resources which allowed to be visited before Web authentication. For example, 192.168.5.1 is a Free Web Server

```
http redirect direct-site 192.168.5.1
```

Bypass the specific IP that is free of Web authentication. For example, 192.168.4.12 is IP address for Department Manager.

```
web-auth direct-host 192.168.4.12 arp
```



## Step 6, Enable Web authentication on SMP

Go to *Authentication & Authority > Portal Settings*, Check *Enable Web Authentication* box. *Enable enter username (Optional)*, if you check this box, only password is required. You have to set username and password to the same in advance.

## Step 7, Enable MAC binding on SMP.

Go to *Authentication & Authority > User Group*, select *Default User Group* because we put Henry into this group, click *Modify*. Go to *Behavior Restrict > Multi-Access Limit*,

***An Account can be used on maximum of [] terminals at the same time***

Just as it suggests, this value allows the maximum number of your wireless device to login simultaneously.

***An account can register [] mobile terminals***

It enables the feature that SMP records and binds how many MAC addresses to user accounts when users logins web authentication with their separate wireless devices for the first time. Once there is a MAC-to-Account binding, the MAC address becomes credentials and username& password is not required any more during authentication.

**Note: The value should be less or equal to the number of “An account can be used on Maximum of [] terminal at the same time”**

For example, Henry have two wireless devices including his laptop and mobile phone. Network administrator configures parameters as shown above on SMP , so Henry is allowed to have both his wireless devices online in meantime , and SMP records and binds the two MAC addresses to Henry account ,which indicates both wireless devices have authority to do *seamless Web Authentication*.

Henry is not allowed to login on the third wireless device due to 2 maximum terminals limitation, and because SMP will not record the MAC address of the third wireless device because maximum 2 terminals is allowed to be recorded.

## Verification

Connect to wireless network, the web authentication page pops up automatically. If it does not, visit any http site to redirect to web authentication page. Input username and password, check *Remember Me* box, click *Login*.

**Note: Do not support HTTPS redirection.**

The screenshot shows a 'User Login' interface. The username field contains 'Henry' and the password field is masked with dots. The 'Remember Me' checkbox is checked. A 'Login' button is visible. Below the login form, a green checkmark and the word 'Success' indicate a successful login. A list of details follows: User Name: Henry, User IP: 172.29.7.4, Online Duration: 0:00:17, Login Time: 2015-11-25 14:22:38, and Online Bulletin: Authentication success. A 'Go Offline' button is present. At the bottom, there are links for 'Pre-Login URL', 'Self-Service', and 'Change Password', along with a tip: 'Tips: You have not completed the Password Protection Settings. Click here to complete settings.'

Go to **SMP > Authentication & Authority > Online User**, you can view Henry is online now.

All   None	User Name	Full Name	User IP	NAS IP	NAS Port	Online Time	Operation
<input type="checkbox"/>	Henry	Henry Chan	172.29.7.4	172.29.3.2	4	0:1:49	<a href="#">View</a>

Go to **SMP > Authentication & Authority > User**, select user *Henry*, click *Mobile Terminal* to display the MAC addresses SMP has recorded and bound to this account.

All   None	User	MAC Address	Registration Date	Authentication Time	Authentication IP	Online Status	Operation
<input type="checkbox"/>	Henry	ec26cae11999	2015-11-25 14:28:46	2015-11-25 14:28:46	172.29.7.4	Online	<a href="#">View</a>

You can also go to **SMP > Authentication & Authority > Mobile Terminal** to manage all MAC addresses SMP has recorded globally.

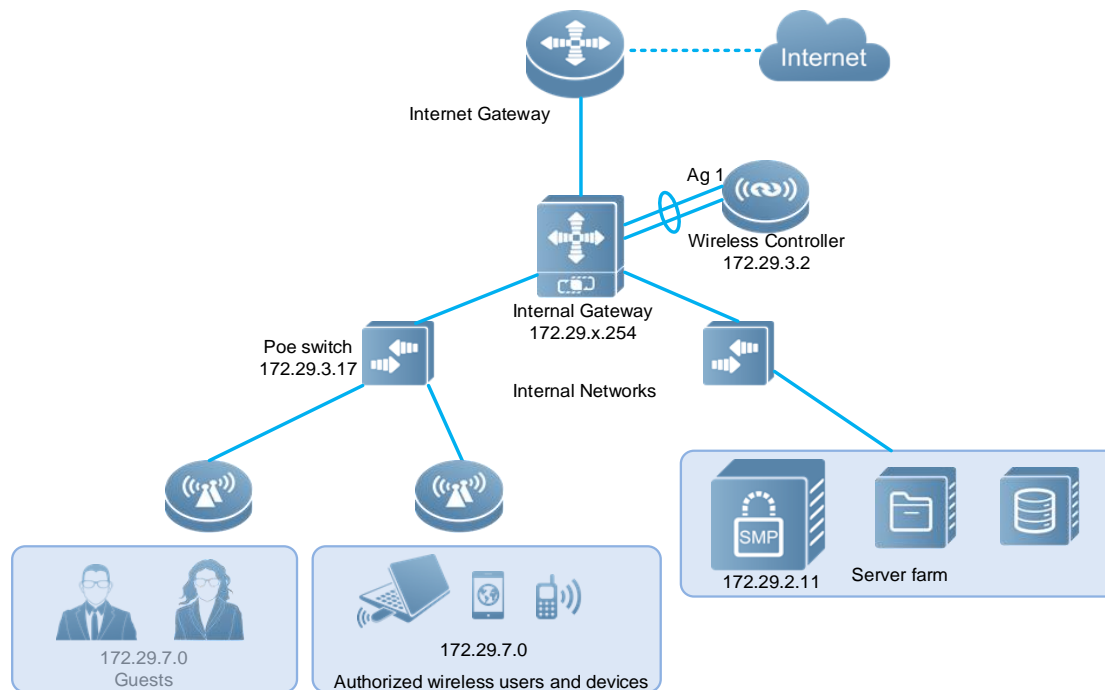
Totally 1 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [Go](#)

All   None	User	MAC Address	Registration Date	Authentication Time	Authentication IP	Nas IP	Online Status	Operation
<input type="checkbox"/>	Henry	ec28cae11999	2015-11-25 14:28:46	2015-11-25 14:28:46	172.29.7.4	172.29.3.2	Online	<a href="#">View</a>

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

Move away from this wireless coverage, disconnect the wireless network, then go back again. The wireless network will be recovered seamlessly.

## 2.3 Authentication for Guest



As per diagram shown above (Ag 1 means Aggregate Port 1), it is a typical wireless network. SMP provides three solutions for Guests authentications.

In this section, you will learn:

- QR Code Authentication(BYOD)
- QR Code Card Authentication(BYOD)
- Exemption Authentication(BYOD)

### 2.3.1 QR Code Authentication (BYOD)

QR Code is more and more popular and widely used in our daily life .This solution combines web authentication and QR Code and deliver a convenient way to guest for wireless access. Guest connects to wireless network, the same to common web authentication, guest will be redirected to a web page which prints one QR Code. Once Staff or receptionist scans the QR Code with their mobile phone, authentication succeeds.

There are four components in QR Code authentication,

- SMP(Portal and Radius Server)
- Wireless Controller(NAS) and Access Point
- Staff or Receptionist
- Guests

Below configuration do not include basic wireless settings, so ensure your wireless network works properly first before starting. Suggest to create a dedicate wlan ssid for *QRCode authentication (BYOD)*.

**Note: Ruijie BYOD is a Private solution, so you should deploy Ruijie wireless devices only, third party devices have compatibility issues.**

In this example, we are using *Ruijie Wireless Controller WS6108 and AP320-I with software version 11.1(5) B7*.

#### Step 1, Configure SNMP on wireless controller

```
snmp-server community ruijie rw
snmp-server host 172.29.2.11 traps Ruijie
snmp-server enable traps
```

#### Step 2, Add Wireless Controller to SMP

Edit SMP device template first, go to *Authentication & Authority > Device > NAS Configuration Templates*, modify *Ruijie Wireless Device*, set the parameters as below,

All None	Template Name	SNMP v2c community	Operation
<input type="checkbox"/>	VPN Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Standard Radius Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Ruijie Wireless Device	ruijie	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Ruijie Wired Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	RG-EG Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	RG-ACE Device	public	<a href="#">View</a>   <a href="#">Modify</a>
<input type="checkbox"/>	Non-Ruijie Wired Device	public	<a href="#">View</a>   <a href="#">Modify</a>

Totally 7 Records | Each Page 20 Records | Page 1 / totally 1 Pages | [GO](#)

Identity Authentication Key is used for Radius Server.

**Identity Authentication Configuration**

\* Identity Authentication Key:

*Tips: The system and devices perform user authentication via the Radius Protocol. Identity authentication key is used for the encryption of data packets and should be the same as that of the devices.*

Web Authentication Key is used for Web Portal

**Web Authentication Configuration**

Web authentication Key:

*Tips: After the Web authentication key is specified, the system will support Web authentication.*

SNMP community is used for SNMP management.

**SNMP Configuration**

\* SNMP v2c Community:

*Tips: The SNMP configuration should be the same as that on the devices. Otherwise the system cannot manage the devices.*

Click **“Modify”** when complete setting.

Go to **Authentication & Authority > Device > Add**, input **NAS IP address**, select **Device Template**, System will get relevant information via SNMP automatically. Click **Add** to finish.

**Basic Information**

\* NAS IP:  (Format: 192.168.20.1)

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

NAS MAC:  (Format: 00D0F8000001)

NAS Name:

NAS Location:

NAS Information:

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

### Step 3, create a new User Group for Staff, and give QR Code Scanning authority to this group.

Go to *Authentication & Authority > User Group>Add*, create a new user group names as *Staff*. Go to *Behavior Restrict> Guest User Management Rights*, Check box of *Allow guest to access network by scanning a QR Code*, then roll to bottom , click *Add*.

\* User Group Name:

Access Control Behavior Restrict Access Rules

**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)

### Step 4, create a new account, and put it into Group “Staff”.

Go to *Authentication & Authority > User > Add*, fill in required fields, here we create a user named “Scott”, and put it into user group *Staff*, click *Add*.

**Basic Information**

\* User Type:  Common User  Guest User

\* User Name:

Nick Name:

\* Password:

\* Type of Account Validity Period:  Never Expire  Delete Account when Expire  Suspend Account when Expire

\* User Group:  [Select User Group](#)

\* User Status:  Normal  Suspended

\* Full Name:

\* Confirm Password:

### Step 5, Enable QR Code Portal on SMP

Go to *SMP>Authentication & Authority >Portal Settings*, Check the box of *Enable Guest Registration*,

Enable Guest Registration

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

Check the box of *Enable Guest QR Code Registration*.

Enable Guest QR Code Registration

Enable Guest Validity Period by Scanner

\* Message for QR Code Scanning:

\* Message for Successful QR Code Authentication:

### Step 6, Configure Radius Server and 802.1x parameters on Wireless Controller

```
aaa new-model
aaa accounting update
```

```
aaa accounting network Forweb start-stop group radius
aaa authentication web-auth Forweb group radius
web-auth authentication v2 Forweb
web-auth accounting v2 Forweb
radius-server host 172.29.2.11 key ruijie
dot1x valid-ip-acct enable
ip dhcp snooping
```

### Apply IP DHCP Snooping trust to uplink port

```
interface AggregatePort 1
ip dhcp snooping trust
```

## Step 7, Configure Web Portal parameters on wireless controller

```
web-auth template qrcode v2
  ip 172.29.2.11
  url http://172.29.2.11:80/smp/qrcodeservlet
web-auth portal eportalv2
web-auth portal key ruijie
http redirect direct-site 172.29.7.254 arp
web-auth offline-detect flow idle-timeout 10 threshold 100
```

**Note:** Go to SMP > Authentication & Authority > Portal Settings > Tips, you can find the detail URLs for different methods.

## Step 8, Apply Web authentication to specified WLAN ID

```
wlansec 5
web-auth portal qrcode
web-auth accounting v2 Forweb
web-auth authentication v2 Forweb
webauth
```

## Step 9, Optional Settings

Bypass the public resources which allowed to be visited before Web authentication. For example, 192.168.5.1 is a Free Web Server

```
http redirect direct-site 192.168.5.1
```



### Verification

Receptionist Scott should be connected to wireless network via either *seamless 802.1x authentication* or *seamless web authentication* first. To verify online status, Go to **SMP>Authentication & Authority > Online User**, we can see Scott is online now.

All None	User Name	Full Name	User IP	NAS IP	NAS Port	Online Time	Operation
<input type="checkbox"/>	scott	chan	172.29.7.3	172.29.3.2	2	0:1:24	<a href="#">View</a>

At this moment, guest comes in and would like to use wireless network. Scott should guide guest to connect to special QR Code wireless network.

When guest connects to QR Code wireless network, he will be redirected to QR Code authentication page as shown in the diagram. If it does not, visit any http site to redirect to this authentication page.

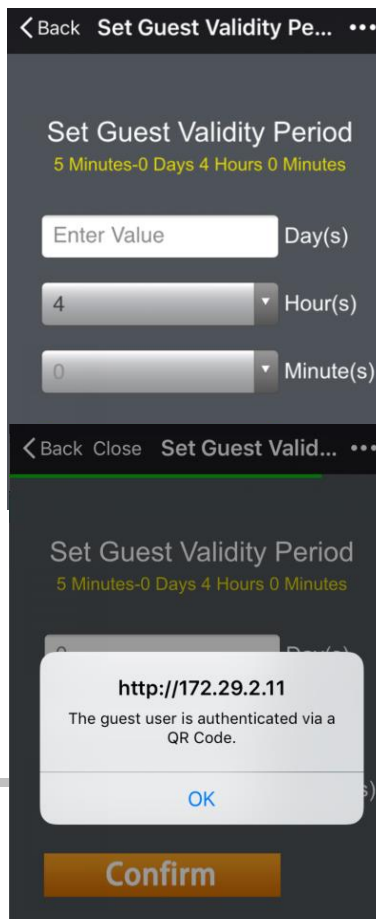
**Note: Do not support HTTPS redirection.**



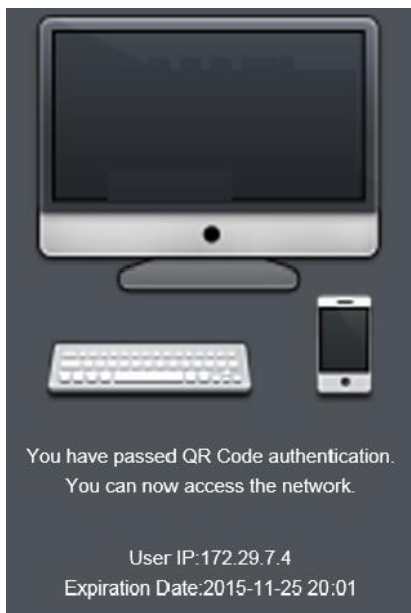
Then, Scott opens his QR Code Scanning App on his wireless device, and scans the QR Code. Next, set the guest validity period, click **Confirm**.

**Note: There are many kinds of QR Code scanner Apps on Android and IOS platform.**

System prompt on Scott's wireless device that authentication succeeds.



In meanwhile, system prompts on Guest's wireless device that authentication succeeds also.



Go to **SMP > Authentication & Authority > Online User**, we can see Guest, marked as Scott's guest, is online now.

All None	User Name	Full Name	User IP	NAS IP	NAS Port	Online Time	Operation
<input type="checkbox"/>	<a href="#">scott_Guest User_1</a>	scott_Guest User_1	172.29.7.4	172.29.3.2	3	0:1:30	<a href="#">View</a>
<input type="checkbox"/>	<a href="#">scott</a>	chan	172.29.7.3	172.29.3.2	2	0:9:54	<a href="#">View</a>

Go to wireless controller CLI, execute command "**show web-auth user all**", Scott's guest is online now .

```

WS6108#show web-auth user all
WS6108#show web-auth user all
Current user num: 2, Online 1
Address                online  Time Limit   Time used   Status      Name
-----
172.29.7.2             off    0d 00:00:00  0d 00:00:00  Initialized
172.29.7.4             on     0d 00:00:00  0d 00:02:19  Active      scott_Guest User_1
WS6108#
    
```

### 2.3.2 QR Code Card Authentication (BYOD)

Compare with QR Code Authentication, QR Code Card is more flexible, staff might print their QR Code on their name card, then guide guests to scan the QR Code to access the network.

There are four components in a complete QR Code Card authentication,

- SMP(Portal and Radius Server)
- Wireless Controller (NAS)and Access Point
- Print QR Code somewhere
- Guests

Below configuration do not include basic wireless settings, so ensure your wireless network works properly first before starting. Suggest to create a dedicate wlan ssid for *QR Code Card authentication (BYOD)*.

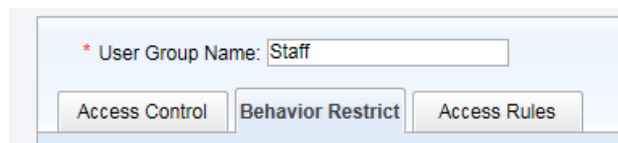
**Note: Ruijie BYOD is a Private solution, so you should deploy Ruijie wireless devices only, third party devices have compatibility issues.**

In this example, we are using *Ruijie Wireless Controller WS6108 and AP320-I with software version 11.1(5) B7*.

Step 1, Go through [Step 1](#) , 2 and 6 in previous chapter QR Code Authentication.

Step 2, create a new User Group for Staff, and give QR Code Card authority to this group.

Go to *Authentication & Authority > User Group>Add*, create a new user group named as *Staff* .Go to *Behavior Restrict> Guest User Management Rights*, Check box of *Allow user to scan QR to authentication*, then roll to bottom , click *Add*.



The screenshot shows a configuration window with a light blue background. At the top, there is a label '\* User Group Name:' followed by a text input field containing the word 'Staff'. Below this, there are three tabs: 'Access Control', 'Behavior Restrict', and 'Access Rules'. The 'Behavior Restrict' tab is currently selected and highlighted.

Guest User Management Rights
<input checked="" type="checkbox"/> Allow user to scan QR to authentication
<input type="checkbox"/> Allow guest users to access network by scanning a QR Code
<input type="checkbox"/> Allow managing guest users on a Ruijie client
<input type="checkbox"/> Allow managing guest users on a Ruijie Self-Service platform (registering users in common mode)
<input type="checkbox"/> Allow managing guest users on a Ruijie Self-Service platform (registering users in SMS mode)

**Note: Every user in this group has their own QR Code .Users can go to SMP Self-Service system at <http://smpIP:80/smp/selfservice> to manage their own QR Code.**

**Step 3, Create a new account , and put it into Group “Staff”.**

Go to *Authentication & Authority > User > Add*, fill in required fields, here we create a user named “Scott”, and put it into *Staff*, click *Add*.

Basic Information	
* User Type:	<input checked="" type="radio"/> Common User <input type="radio"/> Guest User
* User Name:	<input type="text" value="scott"/>
Nick Name:	<input type="text"/>
* Password:	<input type="password" value="*****"/>
* Type of Account Validity Period:	<input checked="" type="radio"/> Never Expire <input type="radio"/> Delete Account when Expire <input type="radio"/> Suspend Account when Expire
* User Group:	<input type="text" value="Staff"/> <a href="#">Select User Group</a>
* User Status:	<input checked="" type="radio"/> Normal <input type="radio"/> Suspended
* Full Name:	<input type="text" value="chan"/>
* Confirm Password:	<input type="password" value="*****"/>

**Step 4, Enable QR Code Card Portal on SMP**

Go to *SMP>Authentication & Authority >Portal Settings*, Check the box of *Enable Guest Registration*,

<input checked="" type="checkbox"/> <b>Enable Guest Registration</b>
* Guest Validity Period: <input type="text" value="0"/> Day(s) <input type="text" value="4"/> Hour(s) <input type="text" value="0"/> Minute(s) (Default: 1 day, range: 5 minutes to 365 days)

The *Validity Period* is the period that allows guest to access wireless network. Once time is up , guest will be forced offline.

Check the box of *Guest scan QR Code to register*.

<input checked="" type="checkbox"/> <b>Guest scan QR code to register</b> <a href="#">QR logo customization</a>
User Group: <input type="text" value="Default User Group"/> <a href="#">Select User Group</a>
* QR wizard steps : <input type="text" value="Pleass scan your QR card to finish authentication!"/>
* QR authentication success message : <input type="text" value="Guest QR authentication success!"/>

*User Group*: Guests will be put into *Default User Group* once authentication succeeds. You can create a special group for guests, then configure special authority accordingly.

**Step 5, Configure Web Portal parameters on wireless controller**

```
web-auth template qrccard v2
ip 172.29.2.11
```

```
url http://172.29.2.11:80/smp/qrcodecardervlet
web-auth portal eportalv2
web-auth portal key ruijie
http redirect direct-site 172.29.7.254 arp
web-auth offline-detect flow idle-timeout 10 threshold 100
```

**Note:** Go to *SMP > Authentication & Authority > Portal Settings > Tips*, you can find the detail URLs for different methods.

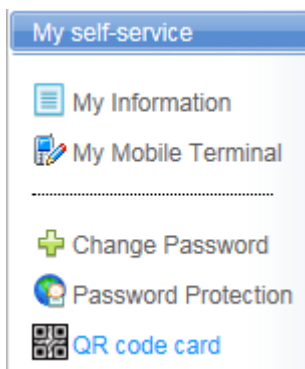
### Step 8, Apply Web authentication to specified WLAN ID

```
wlansec 6
web-auth portal qrcodecard
web-auth accounting v2 Forweb
web-auth authentication v2 Forweb
webauth
```

### Step 9, Generate QR Code Card.

Visit SMP self-service portal at <http://172.29.2.11:80/smp/selfservice>, login.

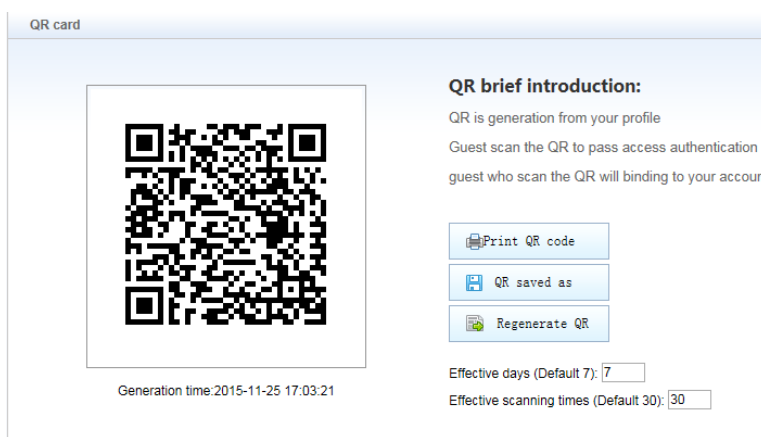
Go to *Myself-Service>QR Code card*,



As shown in the diagram, Scott has his own QR Code. He might print it on his name card or anywhere convenient for guests.

You might regenerate the QR Code immediately or auto regenerate in a period.

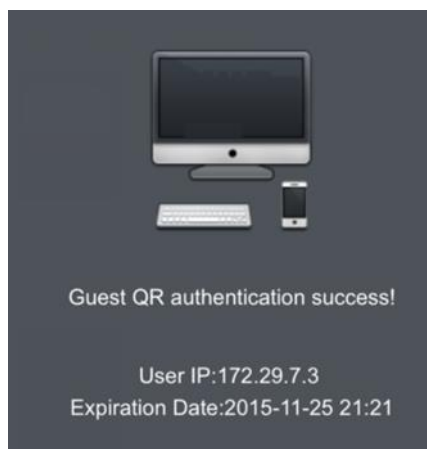
You might also limit the scanning times.



### Verification

Guest comes in and would like to use wireless network. Receptionist should guide guest to connect to special QR Code Card wireless network.

When guest connects to QR Code Card wireless network, receptionist should guide user to scan the prepared QR Code, then System prompts on Guest wireless device that authentication succeeds.



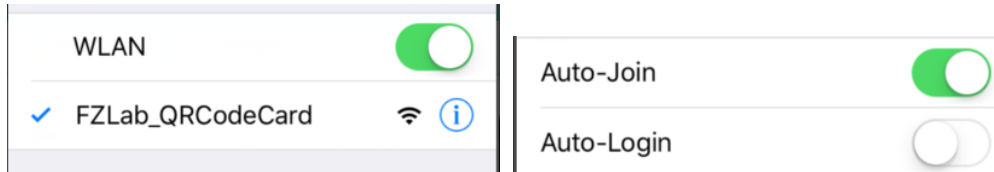
Go to **SMP > Authentication & Authority > Online User**, we can see guest is online now, and it marks as Scott's guest.

All	None	User Name	Full Name	User IP	NAS IP	NAS Port	Online Time	Operation
<input type="checkbox"/>		scott_28e14cb1719e	scott_28e14cb1719e	172.29.7.3	172.29.3.2	7	0:2:44	<a href="#">View</a>

Go to wireless controller CLI, execute command **"show web-auth user all"**, Scott's guest is online now.

```
ws6108#show web-auth user all
Current user num: 2, online 1
Address                online  Time Limit   Time used   Status      Name
-----
172.29.7.2             off    0d 00:00:00  0d 00:00:00  Initialized
172.29.7.3             on     0d 00:00:00  0d 00:04:53  Active      scott_28e14cb1719e
ws6108#
```

**Note: For ios device, additional setting is required. Guests should select detail setting, then disable *Auto-Login* first before connecting to wireless network. Otherwise, ios might disconnect the wireless network once guests switch to QR Code Scanner App.**



### 2.3.3 Exemption Authentication (BYOD)

Exemption Authentication is the most convenient and fastest solution for Guests , as long as guests agree the disclaimer ,they can access wireless network immediately.

There are four components,

- SMP(Portal and Radius Server)
- Wireless Controller (NAS)and Access Point
- Guests

Below configuration do not include basic wireless settings, so ensure your wireless network works properly first before starting. Suggest to create a dedicate wlan ssid for *Exemption Authentication (BYOD)*.

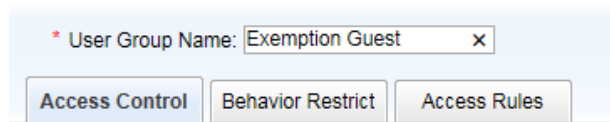
**Note: Ruijie BYOD is a Private solution, so you should deploy Ruijie wireless devices only, third party devices have compatibility issues.**

In this example, we are using *Ruijie Wireless Controller WS6108 and AP320-I with software version 11.1(5) B7*.

Step 1, Go through [Step 1](#) , 2 and 6 in previous chapter QR Code Authentication.

Step 2, create a new User Group for Exemption Authentication Guest

Go to *Authentication & Authority > User Group>Add*, create a new user group names as *Exemption Guest*. Click *Add*.



\* User Group Name:  x

Step 3, Enable Exemption Authentication Portal on SMP

Go to *SMP>Authentication & Authority >Portal Settings* , Check the box of *Enable Authentication-Exemption Rule For Web Users* , then select the user group *Exemption Guest*.



**Enable Authentication-Exemption Rule for Web Users**

\* Authentication-Exemption User Group:  [Select User Group](#)

Click *Modify*.

#### Step 4, Configure Web Portal parameters on wireless controller

```
web-auth template exemption v2
ip 172.29.2.11
url http://172.29.2.11:80/smp/freeauthenservlet
web-auth portal eportalv2
web-auth portal key ruijie
http redirect direct-site 172.29.7.254 arp
web-auth offline-detect flow idle-timeout 10 threshold 100
```

**Note:** Go to *SMP > Authentication & Authority > Portal Settings > Tips*, you can find the detail URLs for different methods.

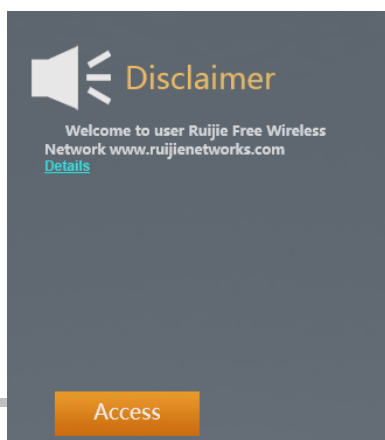
**URLs for different methods.**

#### Step 5, Apply Web authentication to specified WLAN ID

```
wlansec 7
web-auth portal exemption
web-auth accounting v2 Forweb
web-auth authentication v2 Forweb
webauth
```

#### Verification

Guest comes in and connects to wireless network, he will be redirected to a web page stating Disclaimer Rule. If it does not, visit any http site to redirect to authentication page.



**Note: Do not support HTTPS redirection.**

Click **Access** if guest agrees the rule, then authentication succeeds.

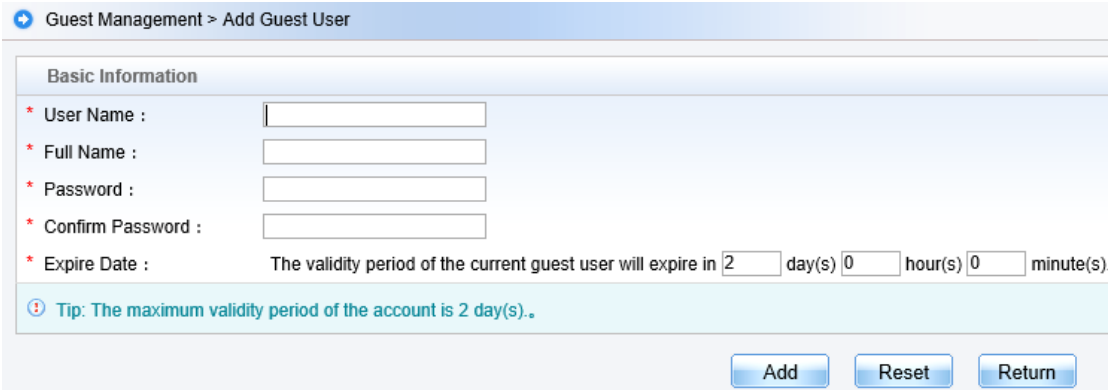


Go to **SMP>Authentication & Authority > Online User**, a new record of exemption user displays as shown below.

All None	User Name	Full Name	User IP	NAS IP	NAS Port	Online Time	Operation
<input type="checkbox"/>	<a href="#">Authentication-Exemption User_1</a>	Authentication-Exemption User_1	172.29.7.4	172.29.3.2	8	0:1:16	<a href="#">View</a>

### 2.3.4 Staff Self-Service Guest Management

In this example , network administrator can grant advanced authority to staff ,allowing them to manage their own Guest, so Guest can access network using *Wired and Wireless Authentication* mentioned in previous sections(MAC Authentication is not applicable).



The screenshot shows a web interface for adding a guest user. The breadcrumb navigation is "Guest Management > Add Guest User". The form is titled "Basic Information" and contains the following fields:

- \* User Name :
- \* Full Name :
- \* Password :
- \* Confirm Password :
- \* Expire Date : The validity period of the current guest user will expire in  day(s)  hour(s)  minute(s).

A tip message is displayed below the fields: **Tip: The maximum validity period of the account is 2 day(s).**

At the bottom right of the form, there are three buttons: "Add", "Reset", and "Return".

For detail configuration, see *User Self-Service Management* in following section.

## 2.4 Integration with Windows Active Directory

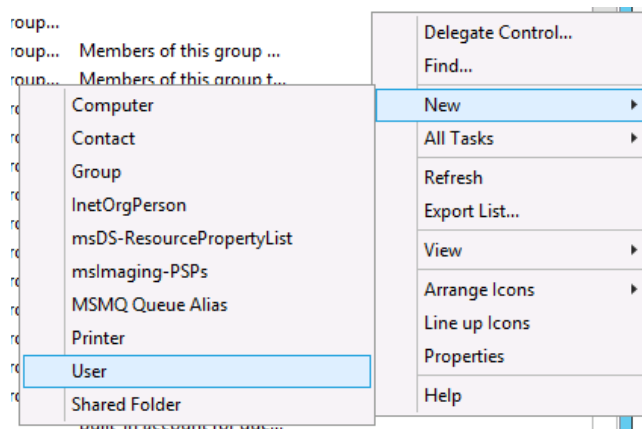
SMP supports integration with multiple external identity server, the most common one is Windows Active Directory. In this section, you will learn how to configure SMP and windows AD integration.

- Currently , SMP supports integration with Windows Server 2008/R2 and 2012
- Support the clients mentioned below,
  1. Web Authentication on Android, IOS, Windows Phone, Linux, MacOS , Windows.
  2. Wireless 802.1x authentication on Android、 ios、 Windows phone 、 linux、 MacOS ,Windows
  3. Wireless and wired 802.1x authentication on Windows with Ruijie Security Agent (SA)
- Support user login in below formats:
  1. Username
  2. Username@Domain Name
  3. Domain name\Username
  4. NetBios\Username

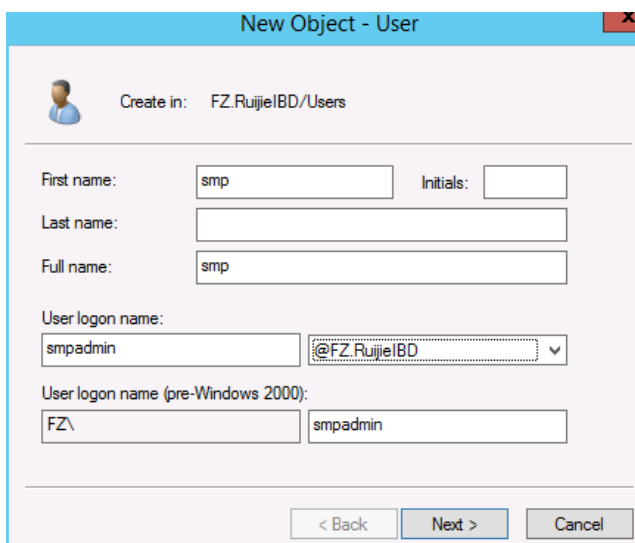
In this example, we are going to integrate SMP with Windows Server 2012 R2 Standard.

### Step 1, Create an AD user dedicate for integration.

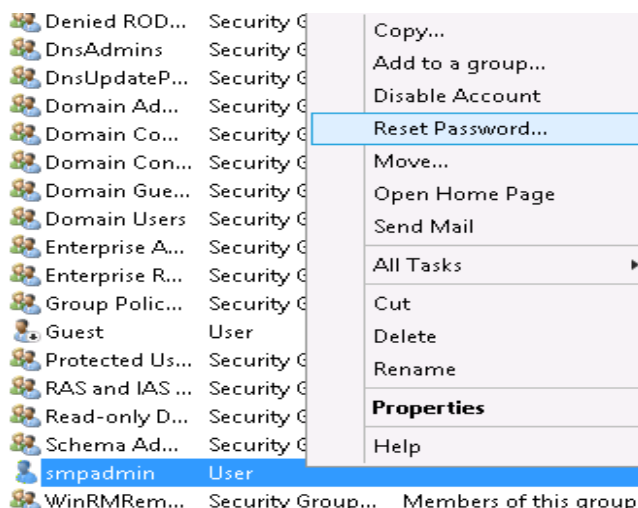
Go to *AD Controller > run > dsa.msc*, open *Active Directory Users and Computers*, create a new user and put it into *Domain Users* group.



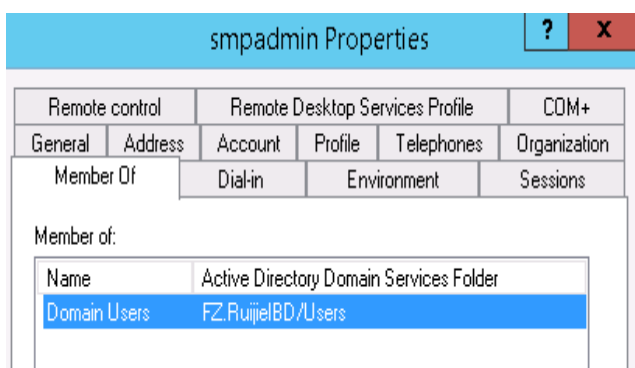
In this example, we create a new user, named *smpadmin*



Reset password to *Ruijie@SMP*



Then assign it to *Domain Users* group



**Step 2, Check the port status. Port 389 and 445 on AD controller should be open.**

You might verify port status using TELNET.

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>telnet 172.29.2.12 389_
```

The diagram indicates that the port 389 is open.

```
Telnet 172.29.2.12
_
```

**Step 3, Configure Domain DNS server on SMP server, so SMP is able to resolve Domain name.**

For example, 172.29.2.12 is AD controller IP address,

Launch a ping session on SMP Server to verify. For example, *FZ.RuijieIBD* is domain name.

```
Use the following DNS server addresses:
Preferred DNS server: 172 . 29 . 2 . 12
Alternate DNS server: . . .

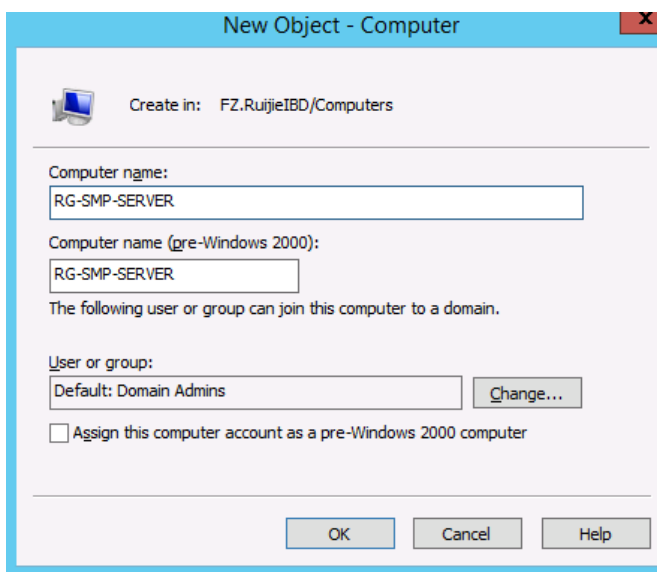
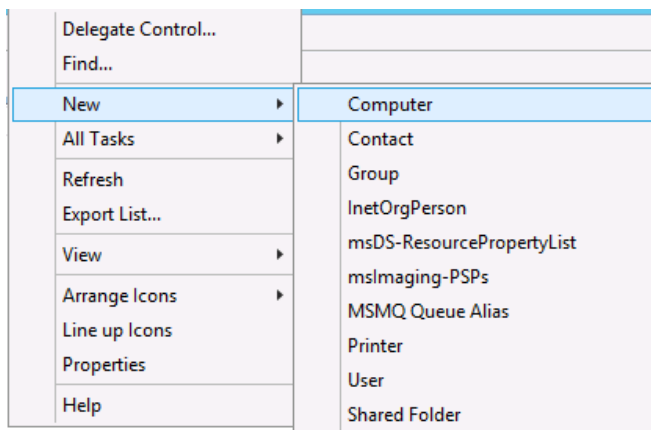
C:\Users\Administrator>ping fz.ruijieibd

Pinging fz.ruijieibd [172.29.2.12] with 32 bytes of data:
Reply from 172.29.2.12: bytes=32 time<1ms TTL=128
Reply from 172.29.2.12: bytes=32 time<1ms TTL=128
Reply from 172.29.2.12: bytes=32 time<1ms TTL=128
Reply from 172.29.2.12: bytes=32 time<1ms TTL=128

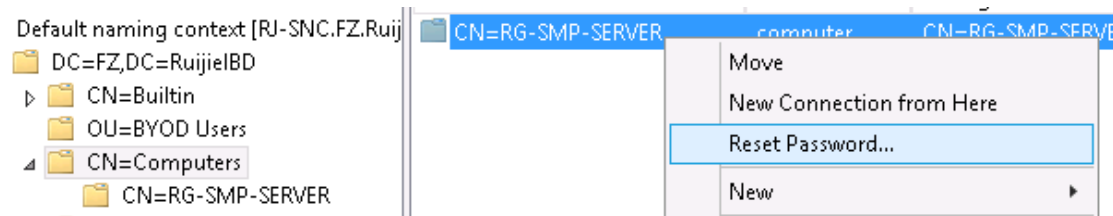
Ping statistics for 172.29.2.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**Step 4, Create a Computer account dedicate for integration.**

Go to *AD controller* > *run* > *dsa.msc*, create a computer named *RG-SMP-Server*.



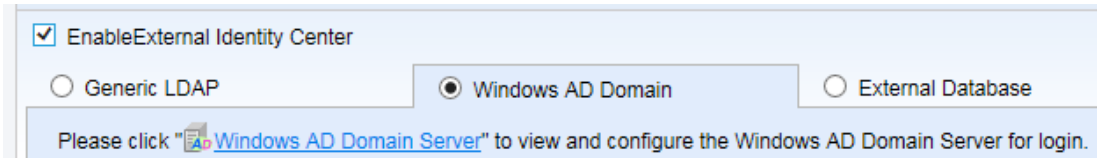
Then go to *run* > *adsiedit.msc*, reset password to *Ruijie@SMP*. The password must be the same to the user created in Step 1.



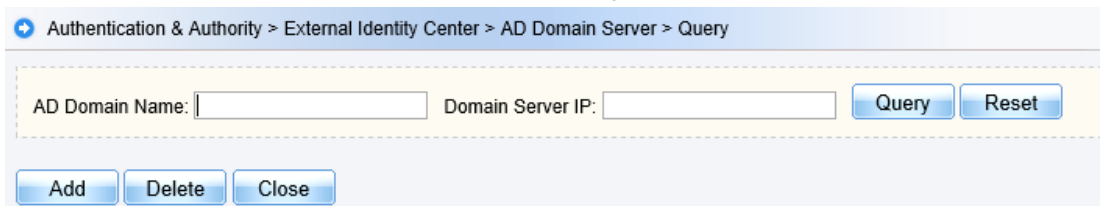
**Note:** *adsiedit.msc* is an administrative tool available for Windows server 2008 and later version.

## Step 5, Configure integration settings on SMP

Go to **SMP>Authentication & Authority > External Identity Center**, Check box of **Enable External Identity Center**. Switch to tab **Windows AD Domain**.



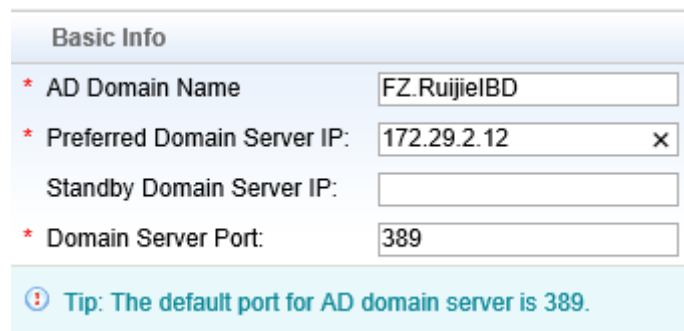
Click **Windows AD Domain Server**, a new configuration windows pops up, click **Add**.



In this example, we divide it to multiple parts to explain how to fill in required information.

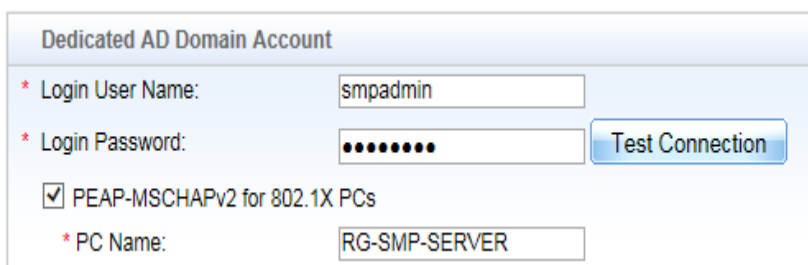
- Input AD Domain name,

Primary AD controller IP address, Standby AD controller IP address (not required), and Domain Server Port (Keep default).



- Input SMP **login User**

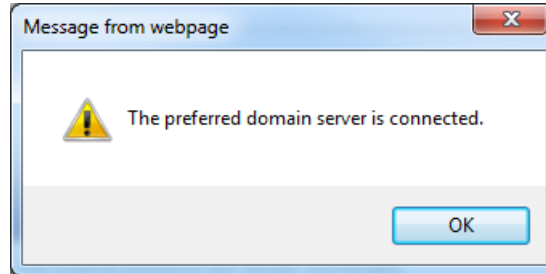
**Name**(the user created in Step 1) , **Login password** , check box of **PEAP-MSCHAPv2 for 802.1X PCs** for



**802.1x PCs** , and input **PC Name** (the computer created in Step 4).Then click **Test Connection** to verify.

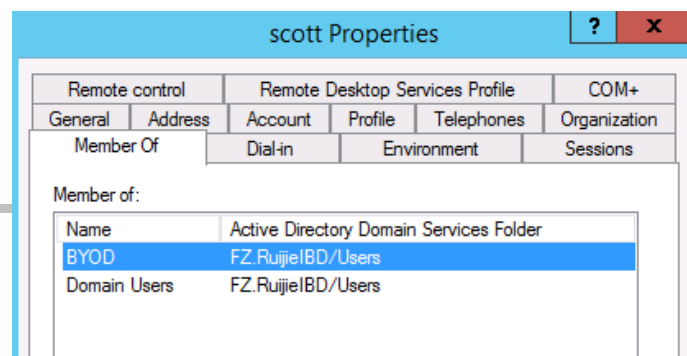
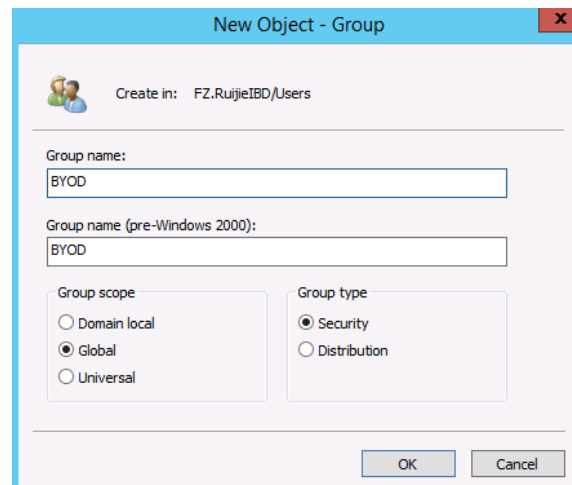
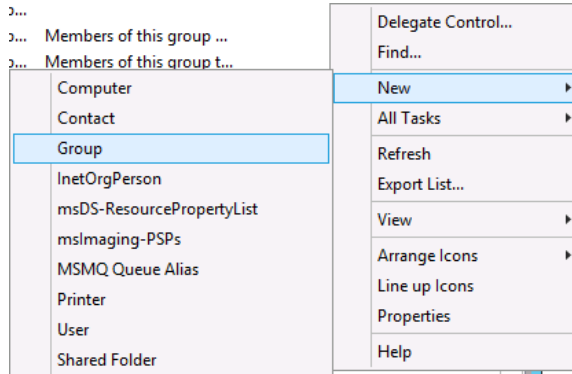


This message indicates that the connection between SMP and AD controller succeeds.



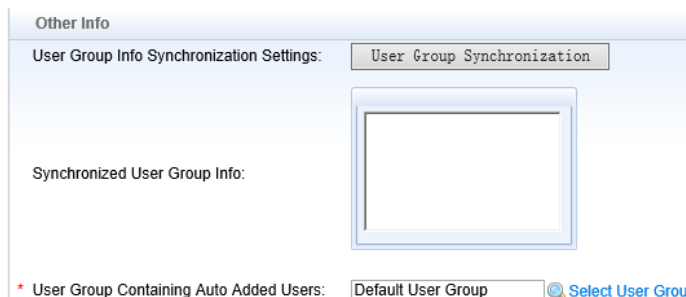
Next, we are going to synchronize Users and User Groups to SMP. SMP is capable of synchronizing Users in **User Group** from AD. Do not support synchronize users in **OU (Organization Unit)**.

In this example, we create a new User Group named **BYOD**.



Create a new user named **Scott**, assign this user to User Group **BYOD**.

Go to **Other Info**, In **User Group Containing Auto Added Users**, click **Select User Group**, and select **Default User Group**.

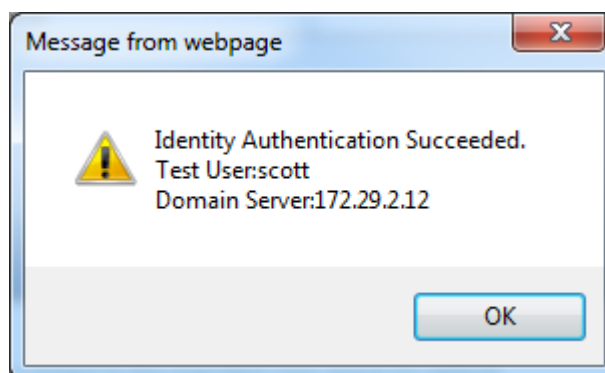


You might select other User Group in this option. This option takes effect only when **Learn the user group during new user authentication** is disabled, SMP will put all users into this special user group.

Next, go to **Identity Center Correlation Test**, input username **Scott** and password, the account we created previously, click **Identity Authen** to verify.



As shown in diagram, Identity verification succeeds. Click **Modify**,



- Go back to **Windows AD Domain settings**.

Please click "[Windows AD Domain Server](#)" to view and configure the Windows AD Domain Server for login.

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

Learn new users during authentication

Learn the user group during new user authentication

Existing users update the user group automatically

### *Synchronization Interval for AD Domain User Info [] days.*

By default, SMP will synchronize those learned user every 7 days. Actually, this setting is designed for inactive users. Active user will trigger synchronization every time they authenticates.

### *Learn new users during authentication*

When SMP and AD integration completes, SMP will not learn all users immediately, only when a new user launches an authentication request that triggers SMP to learn new users from AD.

If check this box, SMP will learn new user from AD and approve authentication even if this account does not exist in SMP before user authentication

If uncheck this box, SMP will not learn new from AD and will only approve authentication for accounts that already exist in SMP.

**Note: It is recommended to check this box.**

### *Learn the user group during new user authentication*

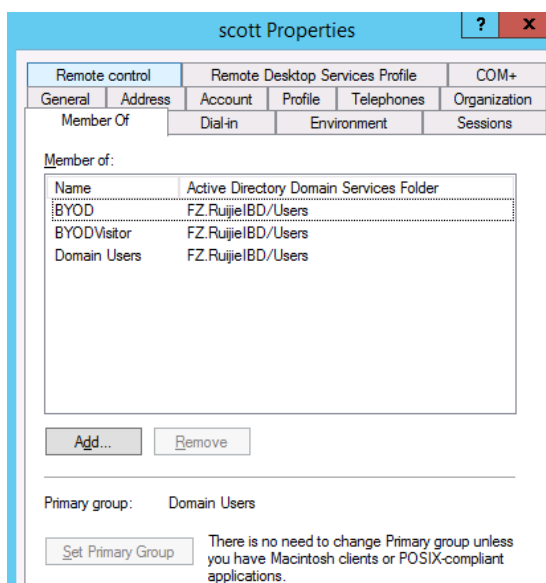
If check this box, SMP will auto learn user group from AD when there is a trigger, just the same to learn users mentioned above.

If uncheck this box, SMP won't learn user group, and will put learned users into a specified user group defined in *User Group Containing Auto Added Users*.

**Note: As shown in diagram , If you assign a user to multiple user groups , SMP only learns the top user group displayed in Member of .In this example , SMP learns user group BYOD.**

**In addition, SMP cannot learn Primary Group.**

**In this example, SMP cannot teach user group BYOD if you set**



it to *Primary Group*. **SMP will learn *BYOD* Visitor then.**

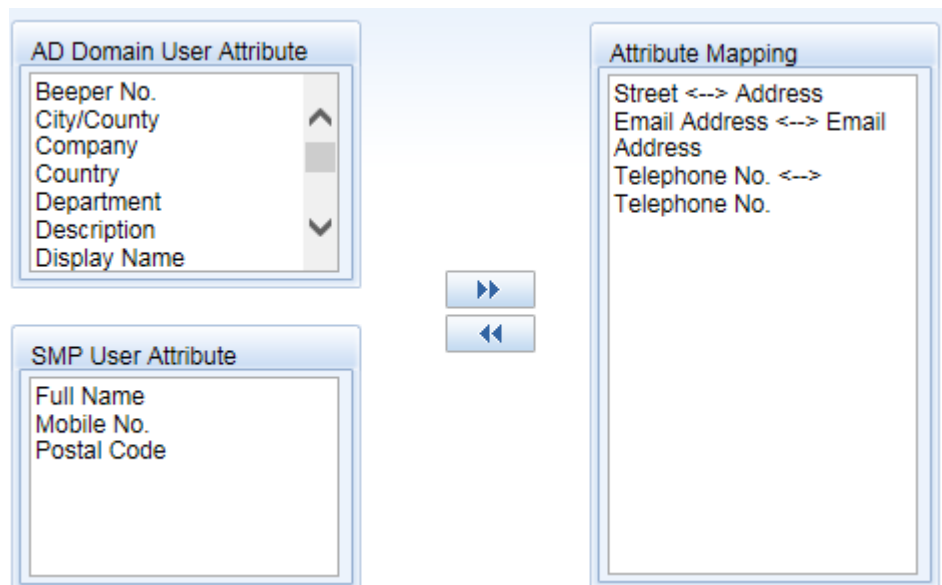
### *Existing users update the user group automatically*

If check this box, SMP will update local user and user group mapping information automatically every time users launch authentication requests.

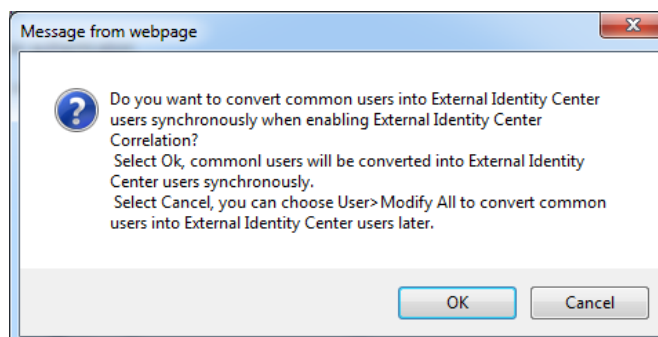
For example, at first **Scott** is assigned to user group **Guest**, SMP learns new user and put **Scott** into user group **Guest**. Some days, AD administrator reassign **Scott** to user group **BYOD**, SMP will update the mapping information and put **Scott** into user group **BYOD** Next time Scott authenticates.

**Note: It is recommended to check this box.**

- Map AD attributes to SMP local Attributes (Optional)



Click **Modify** when completes all above settings, below message pops up. This message indicates whether you would like to convert all current **Common User** to **Third Party User**.



There are three user types in SMP, you might go to *SMP > Authentication & Authority > User > Add > User Type* to view this option.

- **Common User:** SMP common Local user, you can manage the user on SMP.
- **Guest User:** SMP local user, you can assign *Guest user* to *Guest User Group* only. All guest user expire after a period.
- **Third party User:** The users learned from third party server, like windows AD, are classified as Third party user automatically. Third party user are able to be synchronized with third party server periodically. You can manage users on AD controller.

In this example, we click **Cancel** because SMP will learn new users from Windows AD.

## Verification

SMP and AD integration is just about the USER SOURCE, you should have knowledge of either *Wired Authentication*, *Wireless Authentication* or *Authentication for Guest*, the AUTHENTICATION SOLUTIONS before verification.

In this example, we are going to verify the integration function using *Wireless Authentication > Seamless 802.1x Authentication (BYOD)*

Firstly, connect to wireless network, input username **Scott** and password.  
We are using Windows 7.



Click **Connect**. Wait until authentication succeeds.



Go to **SMP > Authentication & Authority > Online User**, **Scott** is online now. Click **View**,

All/None	User Name	Full Name	User IP	NAS IP	NAS Port	Online Time	Operation
<input type="checkbox"/>	<a href="#">scott</a>	scott	172.29.7.3	172.29.3.2	2	0:0:53	<a href="#">View</a>

SMP has learned new user **Scott** and user group **BYOD** from AD **FZ.RuijieIBD**, and the user type is **Third party User**.

Basic Information			
User Name:	scott	Full Name:	scott
Nick Name:			
User Type:	Thirdparty User		
User Group:	<a href="#">FZ.RuijieIBD/BYOD</a>	Authen Method:	Wireless Username and Password Authentication
Login Time:	2015-11-30 15:07:56	Last Login Time:	2015-11-30 15:07:56
Online Duration:	0:1:23		

Go to **SMP > Authentication & Authority > User**, SMP has learned the new user.

<input type="checkbox"/>	scott	scott	<a href="#">FZ.RuijieIBD/BYOD</a>	Never Expire	0	<a href="#">1 Online Users</a>	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
--------------------------	-------	-------	-----------------------------------	--------------	---	--------------------------------	---

Go to **SMP > Authentication & Authority > User Group**, SMP has learned the new user group.

All/None	User Group Name	Operation
<input type="checkbox"/>	FZ.RuijieIBD/BYOD	<a href="#">View</a>   <a href="#">Modify</a>

**Note: If user *Scott* has been created on SMP in type *Common User* previously, SMP prefers local database and will not learn new user from AD.**

## 3 Common Features

### 3.1 Access Control

Sometimes, network administrator would like to control authorized user in a more strict way, for example, allow users in user group **OFFICEROOM** to access network via wired network with their own Laptop only. Allow users in user group **LOBBY** to access network via wireless network with their mobile phone only. To achieve this, SMP should be able to control the way (wired or wireless) user's login and bind IP and MAC address to user accounts.

In this example, We are going to configure Access Control.

Go to **SMP>Authentication & Authority >User Group**, select user group **OFFICEROOM**, click **Modify**,

**Note: You need to create User Group OFFICEROOM first**

AllNone	User Group Name	Operation
<input type="checkbox"/>	OFFICEROOM	<a href="#">View</a>   <a href="#">Modify</a>

Switch to Tab **Access Control**, as shown in below diagram, uncheck **Enable Wireless Access** to prohibited users from accessing network via wireless.

When both **User IP Verification** and **User MAC Verification** are checked, SMP will verify the IP and MAC address upon user logins.

User Group Name: OFFICEROOM

Access Control | Behavior Restrict | Access Rules

Enable Wired Access

Network Information Verification  All

HD Serial Number Verification

IP Type Authentication  Static  Dynamic

User IP Verification

User MAC Verification

User IMSI

NAS IP Verification

NAS Port Verification

Enable Wireless Access

Network Information Verification  All

HD Serial Number Verification

IP Type Authentication  Static  Dynamic

User IP Verification

User MAC Verification

User IMSI

SSID Verification

Check **When network information verification is enabled the server auto-learns the network binding information** to make SMP learn required information automatically upon first time login.

Other Settings	
<input type="checkbox"/>	Enable VPN Access
<input checked="" type="checkbox"/>	When network information verification is enabled, the server auto-learns the network binding information
<input type="checkbox"/>	The user can access the network only through Ruijie Security Agent.

**Note: To auto learn HD Serial Number Verification and IP Type Authentication, Ruijie SA is required.**

To add binding information manually, go to **Authentication & Authority >User**, select user and click **Modify**, go to **Add Network Binding list**, as shown in below diagram.

Access Mode	
<input checked="" type="checkbox"/>	Wired Access
<input checked="" type="checkbox"/>	Wireless Access

Network Binding Info	
HD Serial Number:	<input type="text"/>
User IP:	<input type="text"/> <a href="#">Query Idle IP Addresses</a>
User MAC:	<input type="text"/> (Format:00D0F8000001)
IMSI Number:	<input type="text"/> <a href="#">Select an Idle SIM Card</a>
NAS IP:	<input type="text"/>
NAS Port:	<input type="text"/>

To display the existing binding information, go to **Authentication & Authority >User**, select user and click **View**. Go to **Network Binding List**,

<input checked="" type="checkbox"/>	Jay	Jay Wong	<a href="#">OFFICEROOM</a>	Never Expire		0	Offline	<a href="#">View</a>   <a href="#">Modify</a>   <a href="#">Mobile Terminal</a>
-------------------------------------	-----	----------	----------------------------	--------------	--	---	---------	---

As shown in below diagram, there is one binding entry for User **Jay**.

Network Binding List						
Access Mode	HD Serial Number	User IP	User MAC	IMSI Number	NAS IP	NAS Port
Wired Access		172.29.5.50	448A5B3B45DB			

**Note: By default, an account can be used on maximum one terminal simultaneously, so in this case, SMP auto learns maximum one binding entry. In next section *Behavior Restrict*, we will learn the way to increase maximum terminal limit on a single account.**



## 3.2 Behavior Restrict

There are many features in *Behavior Restriction*, in this section, you will learn the most common ones. Go to *SMP>Authentication & Authority >User Group*, select user group *OFFICEROOM*, click *Modify*, Switch to Tab *Behavior Restrict*.

### 1.1.1 Multi-Access Limit

By default, one account can be used on maximum one terminal simultaneously. For example , Jay has a laptop and a mobile phone , now she logins with his account on her laptop , she will get failure error when she logins with the same account on her mobile phone.

**Note: To view login failure logs, go to** *Log Audit > Authentication Failure Logs*.

Multi-Access Limit
* An account can be used on a maximum of <input type="text" value="1"/> terminals at the same time (Default: 1)
<input type="checkbox"/> An account can register <input type="text" value="1"/> mobile terminals (Default: 1)
<b>Tip:</b> A registered mobile terminal can access a wireless SSID without providing the user name and password.

To increase the maximum terminal number, input a bigger value in the first table.

Regarding *An account can register [] mobile terminals* , we have mentioned this feature in section *Seamless Web Authentication (BYOD)* .By checking this box, SMP will learn Device MAC address and bind it to your account when you login via WEB AUTHENTICATION. The value indicates the numbers that SMP learns and binds.

**Note: The value should be less or equal to the value of** *an account can be used on Maximum of [] terminal at the same time*

In addition, there's an option allowing you to forcedly kick out the previous authenticated terminal, and let the new terminal be authenticated. Go to *SMP>Authentication & Authority >Authentication Settings > Authentication Parameters > When account logins exceed the limit*.

Authentication Parameters	
* Authentication Port: <input type="text" value="1812"/> (Default: 1812)	* Accounting Port: <input type="text" value="1813"/> (Default: 1813)
Record Update Flow: <input type="checkbox"/>	
Enable Nick Name Authentication: <input type="checkbox"/>	
When account logins exceed the limit, deal as follows: <input type="text" value="When the new client authenticates, the previous authenticated user will be forced to go offline. The new client will not be able to authenticate."/>	
Preferred Wireless Authentication: <input type="text" value="PEAP_MSCHAP"/>	
Click <a href="#">here</a> to import the wireless authentication server certificate.	
<b>Tip:</b> The Authentication Port cannot be the same as the Accounting Port.	

### 1.1.2 Offline Timer

Offline Timer allows network administrator to allocate specific timer to user group in which users have limited online duration for one time authentication. Usually, this feature is integrated with authentications for guests or paid users, like Exemption Authentication and QR Code Card Authentication.

There are three kinds of methods in Offline Timer.

#### Daily Timer

When the daily timer ends, users are forced offline and SMP will put user account in suspended status, so user cannot login any more until next day, the account will be recovered to normal status automatically.

You might also put user account back to Normal manually. Go to **Authentication & Authority > User > Select user and click Modify >Basic Information > User Status.**

**Note: When SMP forces user offline, go to *Log Audit > Authentication Failure Logs* and *Network Access Log* to view system logs and verify.**

<input type="checkbox"/>	Aaron	172.29.7.3	Aaron A	172.29.3.2	2015-12-01 17:17:11	2015-12-01 17:23:00	User online time over limit!	<a href="#">View</a>
<input type="checkbox"/>	<a href="#">Aaron</a>	2015-12-01 17:23:43	<a href="#">172.29.3.2</a>		28E14CB1719E	The user account is suspended	<a href="#">View</a>	

#### Total timer

When the total timer ends, user accounts will be suspended or cancelled.

Disabled  
 Daily Timer  
 Total Timer  
 \* Timer  hours(hours range:[1, 8760])  
 \* Response  Cancel  Suspend  
 Single Timer

If **Cancel** is selected, User will be forced offline and the account will be cancelled when the timer is up.

If Suspend is selected, User will be forced offline and the account will be put in suspend status when the timer is up .You might recover it to normal status manually if required.

**Note: When SMP forces user offline, go to** *Log Audit > Authentication Failure Logs* **and** *Network Access Log* **to view system logs and verify.**

### Single Timer

When the single timer ends, users will be forced offline or accounts will be suspended.

Disabled  
 Daily Timer  
 Total Timer  
 Single Timer  
 \* Timer  minutes(minutes range:[5, 86400])  
 \* Response  Offline  Suspend  
 \* Holding Time  minutes(minutes range:[5, 1440])  
 \* Cause

If Offline is selected, user will be forced offline .but user is able to authenticate with the same account again.

If suspend is selected, user will be forced offline, then SMP put this account in suspend status. After holding time, SMP will put account back to normal status automatically.

**Note: When SMP forces user offline, go to** *Log Audit > Authentication Failure Logs* **and** *Network Access Log* **to view system logs and verify.**

### 1.1.3 Network Access Prohibited Period

This feature allows network administrator to customize the time range in which users are prohibited to access network.

In below example, the rules allow user to access network in work hour during 8:00 am – 18:00 pm. The time and time zone must be correct on your SMP Server.

**Network Access Prohibited Period**

Every day :  :  --  :  (hh:mm)

Every week :  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday  
 :  --  :  (hh:mm)

Every year :  Month  Day  :  --  :  (hh:mm)

Designated Date :  ,  :  --  :  (hh:mm)

Period Type	Configuration	Operation
Every day	18:0 -- 23:59	<a href="#">Delete</a>
Every day	0:0 -- 8:0	<a href="#">Delete</a>

In the network access prohibited period, user authentication requests are denied and online users are forced offline and receive the following messages:

Off hour , cannot access to network

ⓘ Users authenticated through VPN, Web, and built-in client of an operating system will not receive the message of forced offline.

**Note:** Just as the tips suggests, the customized message will be pushed to only the users who installed Ruijie SA.

### 3.3 Bulletin Information

SMP allows to push bulletin information to users when they are authenticated.

**Note: This feature is applicable only for users who install Ruijie SA (Security Agent)**

Go to *Authentication & Authority > Bulletin Information*, edit the bulletin information.



The screenshot shows the 'Bulletin Information' configuration page. It features a text area for the bulletin message containing 'Welcome to Ruijie Networks.' Below this is a 'Bulletin Information URL' field with the value 'http://www.ruijienetworks.com' and a 'Verify' button. At the bottom, there is a checkbox for 'Enable Account Expiration Warning' which is checked.

**Bulletin Information URL:** The specific web page will auto pop up when users login.

In this example, we are using *Seamless 802.1x Authentication (BYOD)* to verify, the bulletin information pops up as expected.

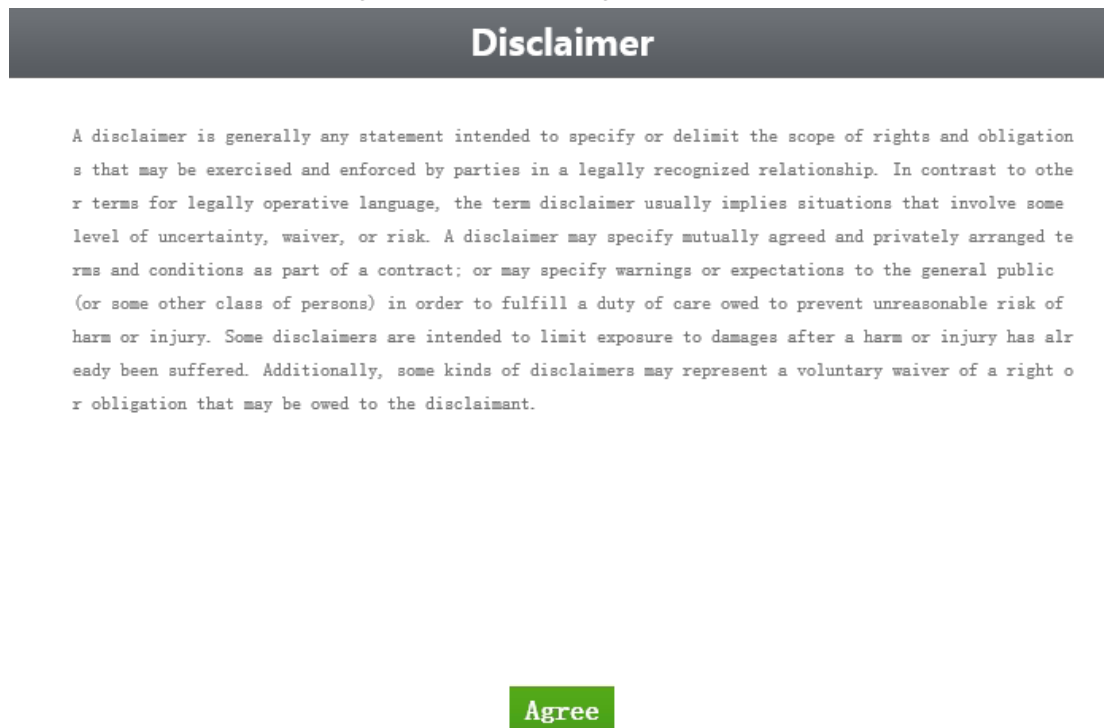


### 3.4 Disclaimer Page

Usually, network administrator would like to publish disclaimer for end users before authentication. To enable disclaimer page, go to **Authentication & Authority > Portal Settings > Open Disclaimer Page**, edit disclaimer contents. Move to the bottom, click **Modify** when finish.

<input checked="" type="checkbox"/> Open Disclaimer Page	
* Disclaimer title:	Disclaimer
* Disclaimer contents:	<p>A disclaimer is generally any statement intended to specify or delimit the scope of rights and obligations that may be exercised and enforced by parties in a legally recognized relationship. In contrast to other terms for legally operative language, the term disclaimer usually implies situations that involve some level of uncertainty, waiver, or risk.</p> <p>A disclaimer may specify mutually agreed and privately arranged terms and conditions as part of a contract; or may specify warnings or expectations to the general public (or some other class of persons) in order to fulfill a duty of care owed to prevent unreasonable risk of harm or injury. Some disclaimers are intended to limit exposure to damages after a harm or injury has already been suffered. Additionally, some kinds of disclaimers may represent a voluntary waiver of a right or obligation that may be owed to the disclaimant.</p> <p>( Support upto 8000 characters input )</p>
* Agree button title:	Agree

In this example, we are using **seamless web authentication (BYOD)** to verify .Connect to wireless SSID, redirect to authentication page, users need to Agree Disclaimer before input username and password.



**Note: This feature is applicable for *Seamless Web Authentication(BYOD)* only.**

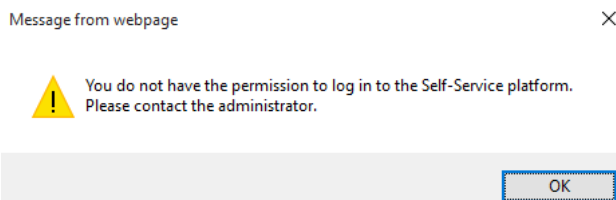
## 4 User Self-Service Management

SMP allows users to manage their own account using Self-Service Platform. In this example, you will learn most commonly used features.

Actually, in previous section QR Code Authentication (BYOD) and QR Code Card Authentication (BYOD), we mentioned a bit about self-service regarding QR Code management.

Visit SMP self-service page at <http://ServerIP/smp/selfservice>

By default, the self-service authority is disabled, system will prompts you message as shown below.



To enable self-service authority, go to **Authentication & Authority > User Group > select a user group, click Modify > switch to tab Behavior Restrict > Guest User Management Rights**, check any one box listed below. In this example, we check all boxes for convenient demonstration purpose.

Guest User Management Rights	
<input checked="" type="checkbox"/>	Allow user to scan QR to authentication
<input checked="" type="checkbox"/>	Allow guest users to access network by scanning a QR Code
<input checked="" type="checkbox"/>	Allow managing guest users on a Ruijie client
<input checked="" type="checkbox"/>	Allow managing guest users on a Ruijie Self-Service platform (registering users in common mode)
<input checked="" type="checkbox"/>	Allow managing guest users on a Ruijie Self-Service platform (registering users in SMS mode)



- **Allow user to scan QR to authentication:** Mentioned in *QR Code Card Authentication (BYOD)*

previously.

- **Allow guest users to access network by scanning a QR Code:** Mentioned in *QR Code Authentication (BYOD)* previously.

- **Allow managing guest users on a Ruijie client:** Users might manage guest user via Ruijie SA (Security Agent), as shown in below diagram.

The screenshot shows the 'Guest' management interface in the Ruijie Security Agent. At the top, there is a navigation bar with icons for Bulletin, Business Information, Settings, Guest, Suggestion, and Diagnostics. Below the navigation bar, the 'Guest' section is active, displaying a form to create a new guest user. The form includes the following fields:

- Guest Account:
- Guest Name:
- Password:
- Confirm Psw:
- Account Valid:  day  hour  minute

A hint message below the form states: "Hint: the max expiry date is 2 days". At the bottom of the form, there are two buttons: "Create" and "Reset".

**Note:** For more information about SA, see *Appendix > Ruijie Security Agent (SA)*.

- **Allow managing guest users on a Ruijie Self-Service platform (registering users in common mode):** Users might manage guest user via Service-Service Portal, as shown in below diagram.

The screenshot shows the 'Guest Management > Add Guest User' interface in the Ruijie Self-Service Portal. The page has a blue header with the breadcrumb 'Guest Management > Add Guest User'. Below the header, there is a section titled 'Basic Information' containing the following fields:

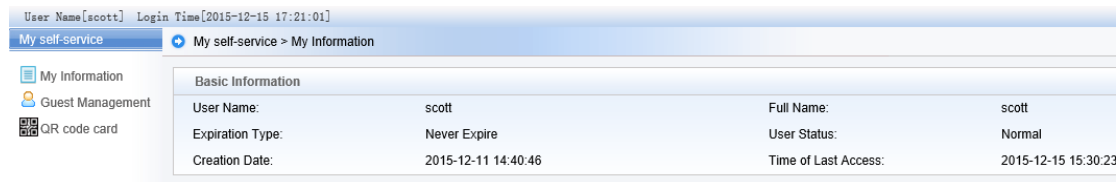
- \* User Name :
- \* Full Name :
- \* Password :
- \* Confirm Password :
- \* Expire Date : The validity period of the current guest user will expire in  day(s)  hour(s)  minute(s).

A tip message below the form states: "Tip: The maximum validity period of the account is 2 day(s).". At the bottom of the form, there are three buttons: "Add", "Reset", and "Return".

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

SMS authentication is not covered in this manual.

As shown in below diagram, it is the homepage of self-service portal. Actually, you can manage **Guest** and **QR Code Card** via this portal only.



The screenshot displays the user interface of the self-service portal. At the top, it shows the user's name as 'scott' and the login time as '2015-12-15 17:21:01'. Below this, there is a navigation menu with three options: 'My Information', 'Guest Management', and 'QR code card'. The 'My Information' option is selected, and the main content area displays a table of basic information for the user 'scott'.

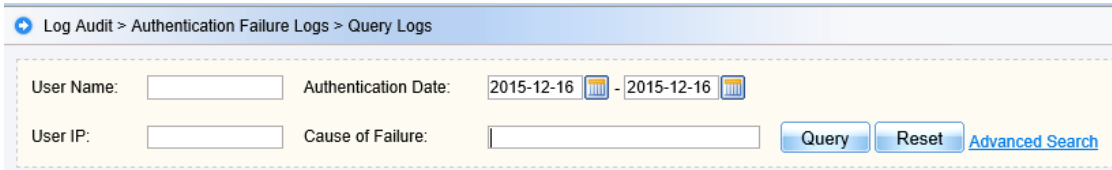
Basic Information			
User Name:	scott	Full Name:	scott
Expiration Type:	Never Expire	User Status:	Normal
Creation Date:	2015-12-11 14:40:46	Time of Last Access:	2015-12-15 15:30:23

## 5 Trouble Shooting

In this section, you will learn the most common way to trouble shooting on your SMP.

### 5.1 Authentication Failure Logs

Commonly, we might encounter authentication failure, it is recommended that go to **Log Audit > Authentication Failure Logs**, query historical authentication failure logs.



The screenshot shows a web interface for querying logs. The breadcrumb path is "Log Audit > Authentication Failure Logs > Query Logs". Below the breadcrumb is a search form with the following fields and controls:

- User Name:
- Authentication Date: 2015-12-16 [calendar icon] - 2015-12-16 [calendar icon]
- User IP:
- Cause of Failure:
- Buttons: Query, Reset, [Advanced Search](#)

If SMP prompts the cause of failure, like “The user account is suspended”, “User Name does not exist or password mistake”, follow the instruction to investigate in further.

**Note: If SMP prompts nothing , usually it is caused by network issue , double check the configuration on NAS device , also check the connectivity between NAS and SMP.**

### 5.2 Collect SMP Logs

Sometimes, you might encounter some unknown problems, suggest to read SMP installation guide and Implementation Guide carefully and double check the configurations.

if you still cannot solve it, you might go to SMP installation root path, for example D:\RG-SMP\log, copy the whole “log” folder, then submit a case on Ruijie Service Portal attached with the log file, remember to describe the issue as detail as you can to make your problem easy understanding, so that portal manager can solve this problem efficiently.

## 6 Appendix

### 6.1 Ruijie Security Agent (SA)

This example describes the usages of Ruijie Security Agent. You might find SA installation package in SMP matching materials. Currently, SA supports below operation systems:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8/8.1

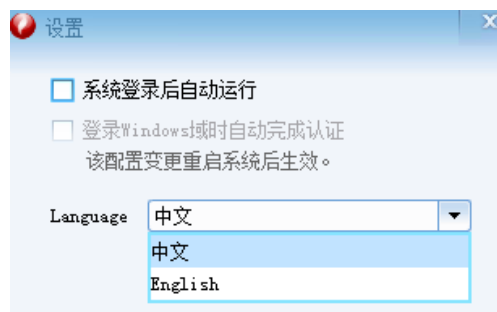
As shown in diagram, this is Ruijie SA icon. Double click the icon to open it.



Click the button in red line to open setting window.



Select Language English.

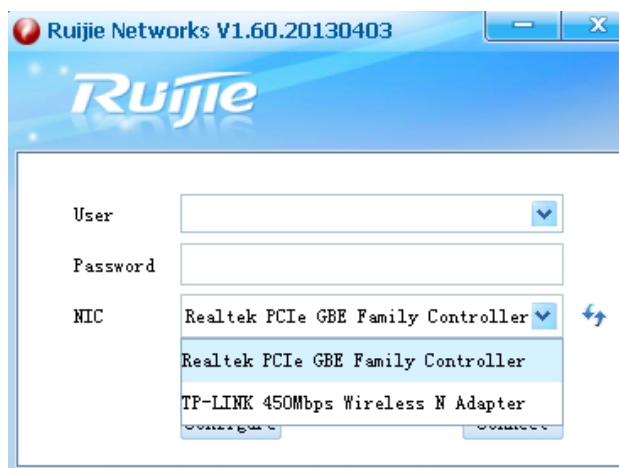


The user interface has been in English now.



SA can scan and recognize your Network Interface Card on your computer. Select correct NIC before authentication.

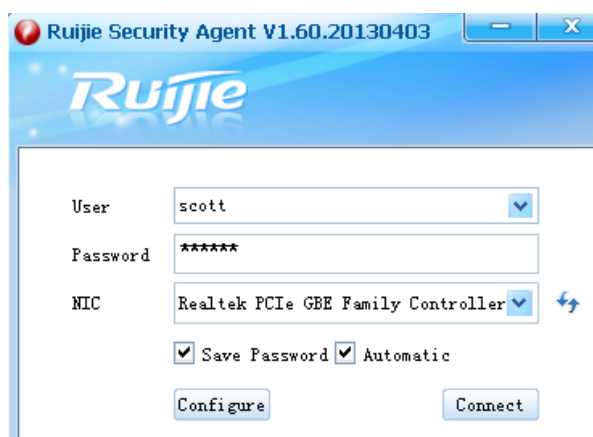
In this manual, SA is applied only for *Wired 802.1x Authentication*, so we select wired NIC here.



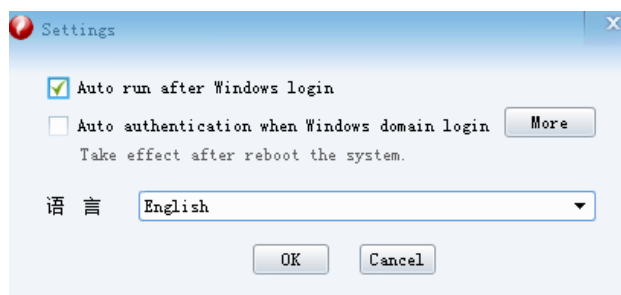
Go through Section mentioned in *Wired Authentication > 802.1x Authentication* first. Next, we are going to pass wired 802.1x authentication.

Input username and password.

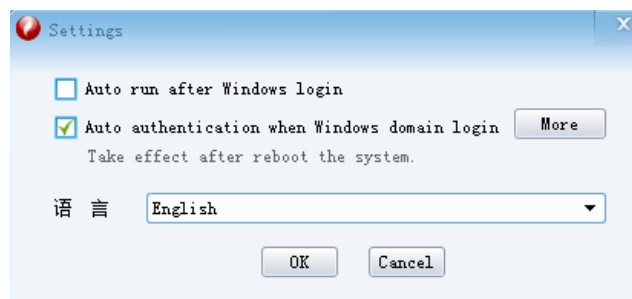
(Optional) Click *Save Password* and *Automatic*.



(Optional) Click **Configure**,  
You might allow SA to auto run after Windows Login.



(Optional) You might enable **Auto authentication when Windows domain login** if it is a Windows AD scenario.



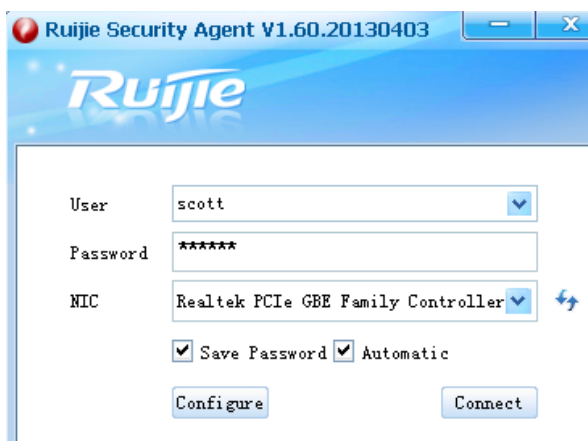
**Note:** You cannot enable both *Auto run after Windows login* and *Auto authentication when Windows domain login* simultaneously.

(Optional) Click **more**, you might enable *using domain login account as certified account*.



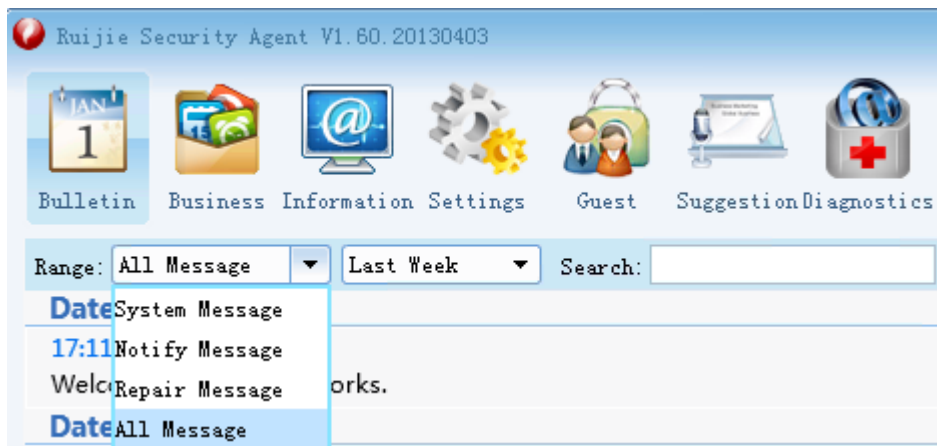
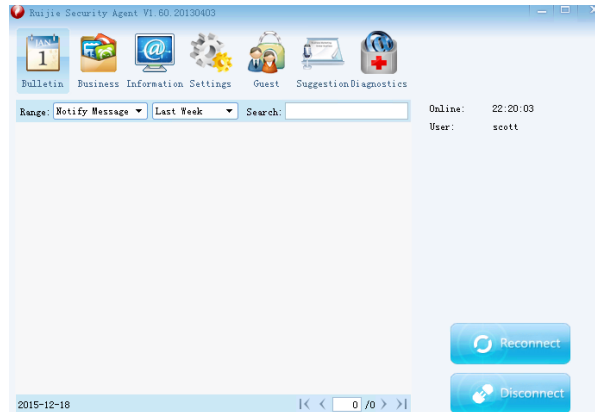
In this example, we are using SA to do Wired 802.1x Authentication.

Input username and password, click Connect to start authentication.



After authentication succeeds , you will see this windows.

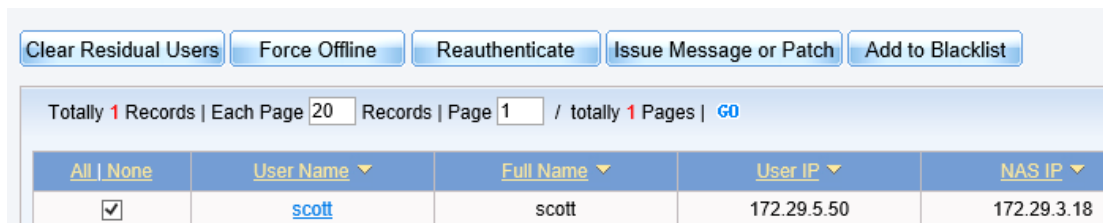
In the upper position , the menu contains **Bulletin**, **Business**, **Information**, **Settings**, **Guest**, and **Diagnostics**, you will learn part of the common components in next section.



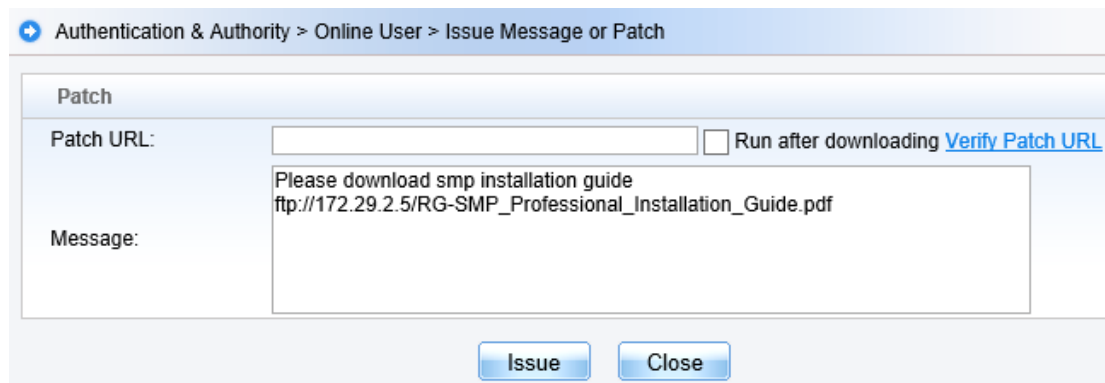
- Bulletin

**System Message:** Network administrator can propagate System Bulletin to all SA. Go to **Common Features > Bulletin Information** to configure this feature.

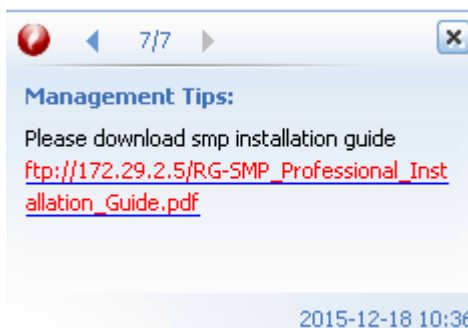
**Notify Message and Repair Message:** Network administrator can also push personal message to specific SA. Go to **SMP>Authentication & Authority > Online User > Select user > Issue Message or Patch**.



**Issue Message or Patch windows** pops up, input **Patch URL** (Optional) and **Message**, then click **Issue**.

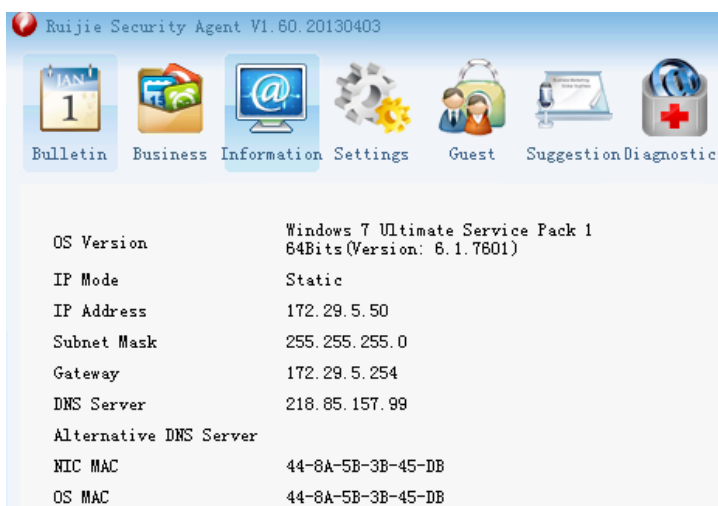


On SA side, a new message will pop up in the bottom right corner.



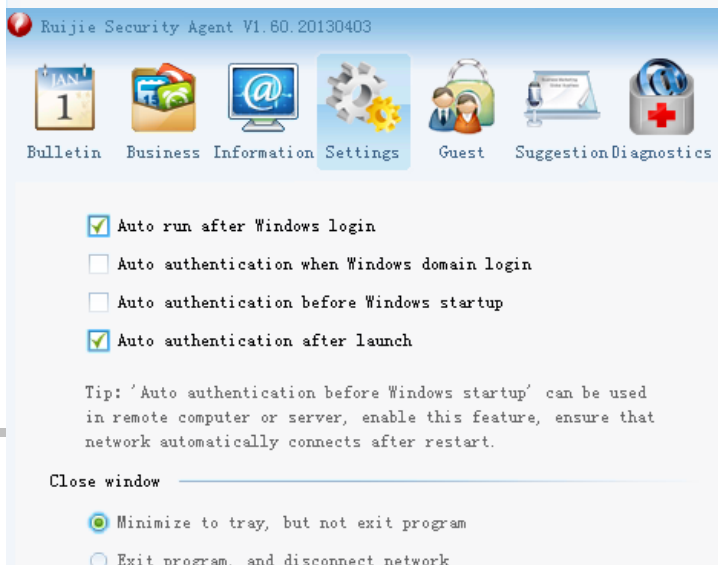
- Information

Click Information to obtain basic network information of your computer including the Operating System, IP address, Gateway, DNS Server and so on.



- Settings

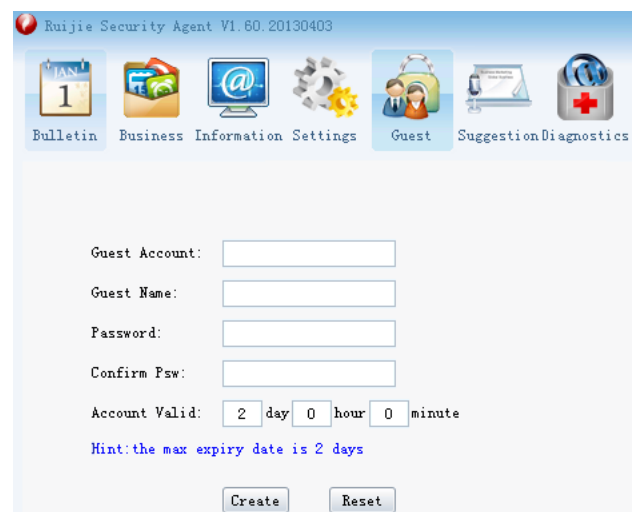
You might change the settings in this component.





- Guest

Go to *Common Features >User Self-Service Management > Allow managing guest users on a Ruijie client* to study this component.



Ruijie Security Agent V1.60.20130403

Navigation icons: Bulletin, Business Information, Settings, Guest, SuggestionDiagnostics

Form fields:

- Guest Account:
- Guest Name:
- Password:
- Confirm Psw:
- Account Valid:  day  hour  minute

Hint: the max expiry date is 2 days

Buttons: Create, Reset