SANGFOR

IAM

Best Practices for Scenarios_Sync Log to Report Center

Version 12.0.42

Change Log

Date	Change Description
Sept 18, 2020	Version 12.0.42 document release.
May 17, 2021	Version 12.0.42 document update.

CONTENT

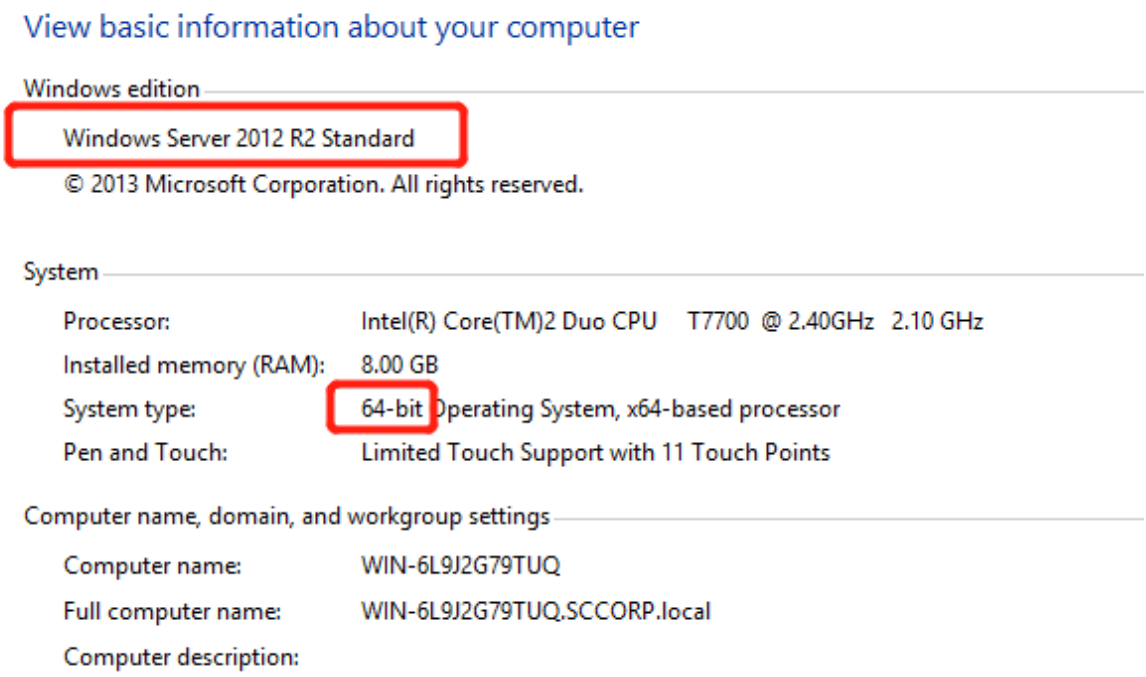
Chapter 1 Scenario

For some medium and large enterprises, IAM has limited built-in disk space and hopes to use an external log center to store more logs, so as to facilitate the storage of audit logs and the traceability of information in the future.

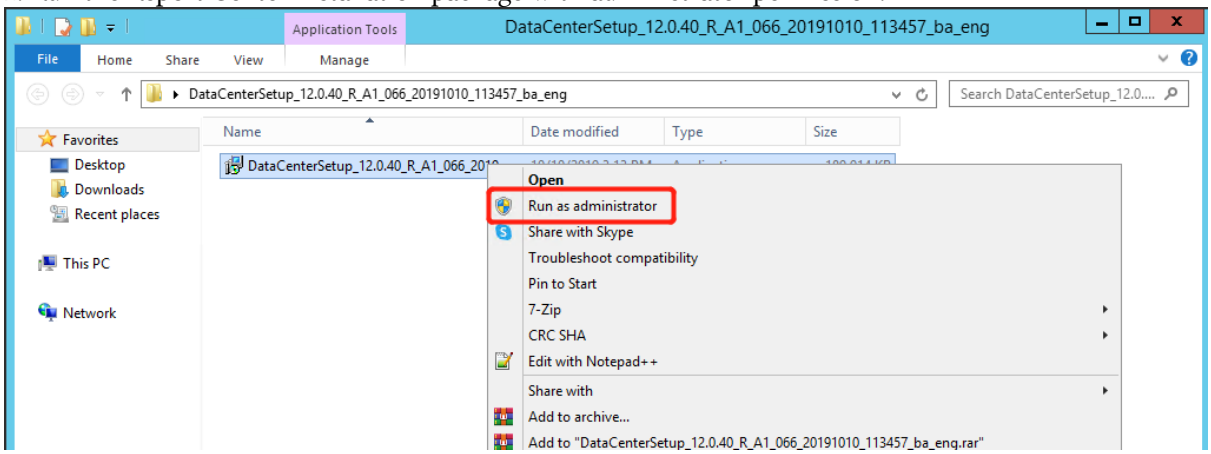
Chapter 2 Configuration

2.1 Configuration in Windows Server

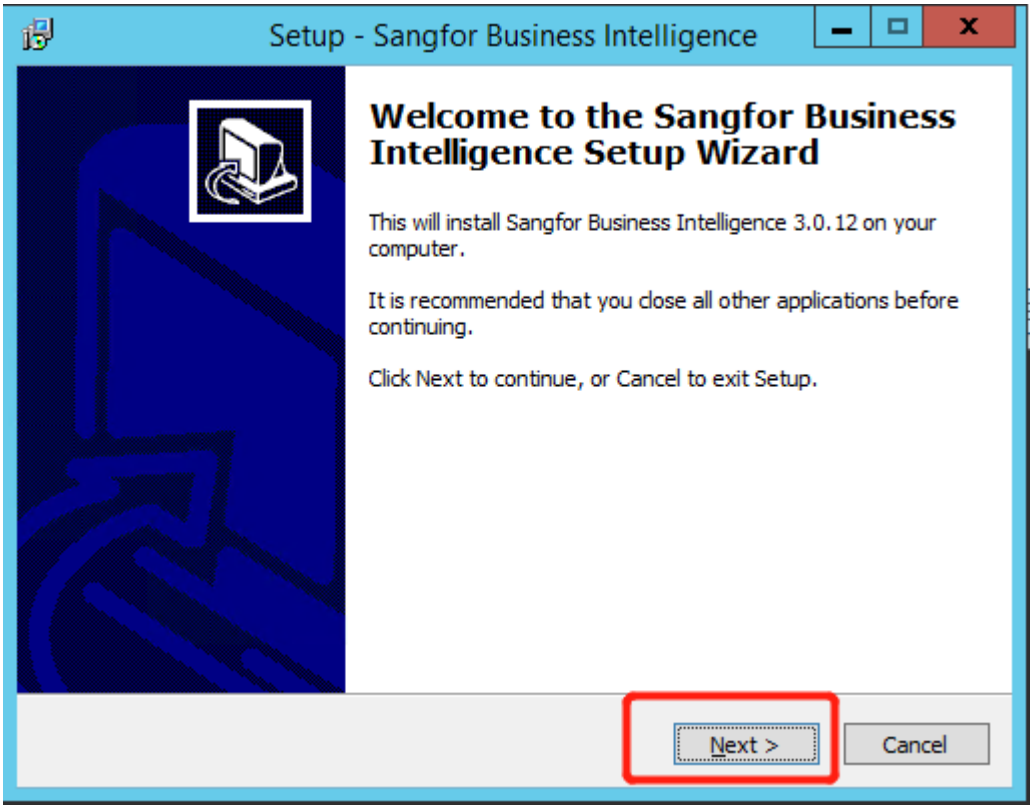
1. Prepare a Windows Server, which requires a version newer than Windows Server 2018 x64.



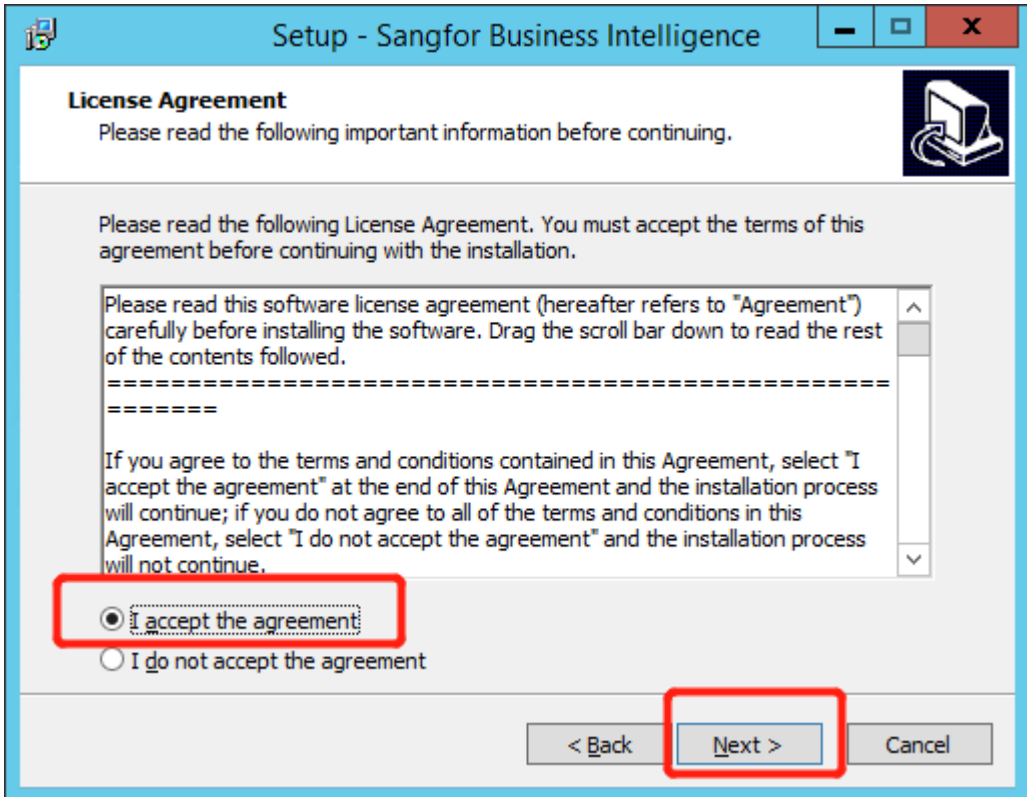
2. Run the Report Center installation package with administrator permission.



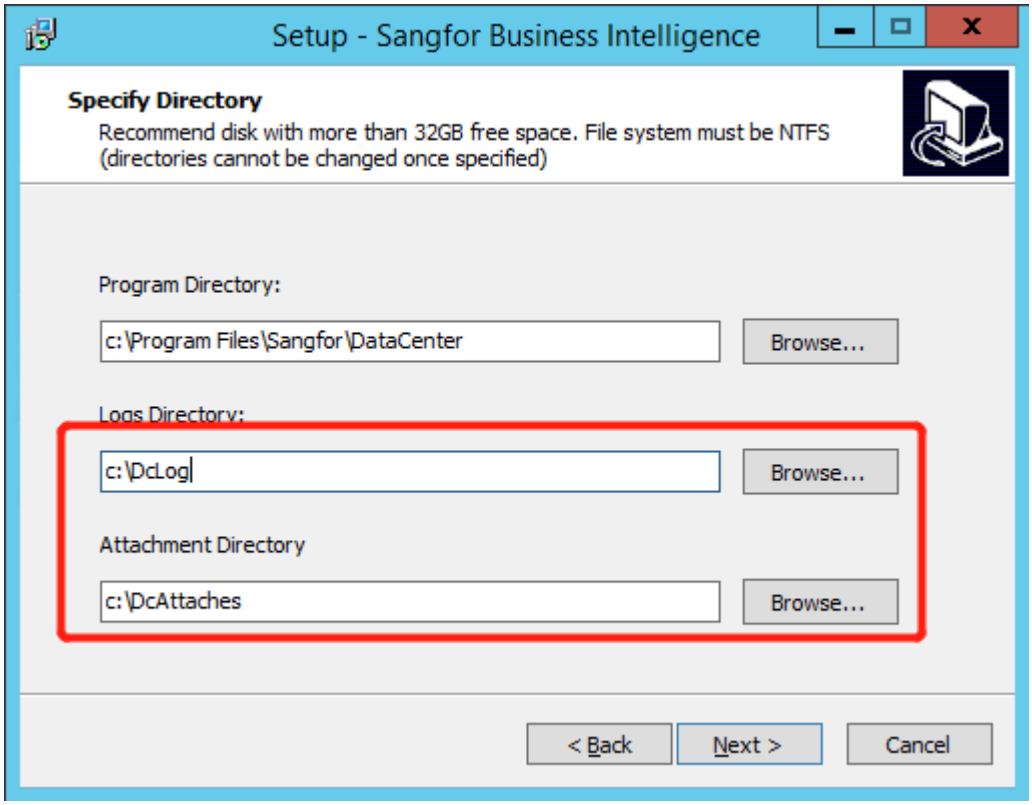
3. Click "Next"



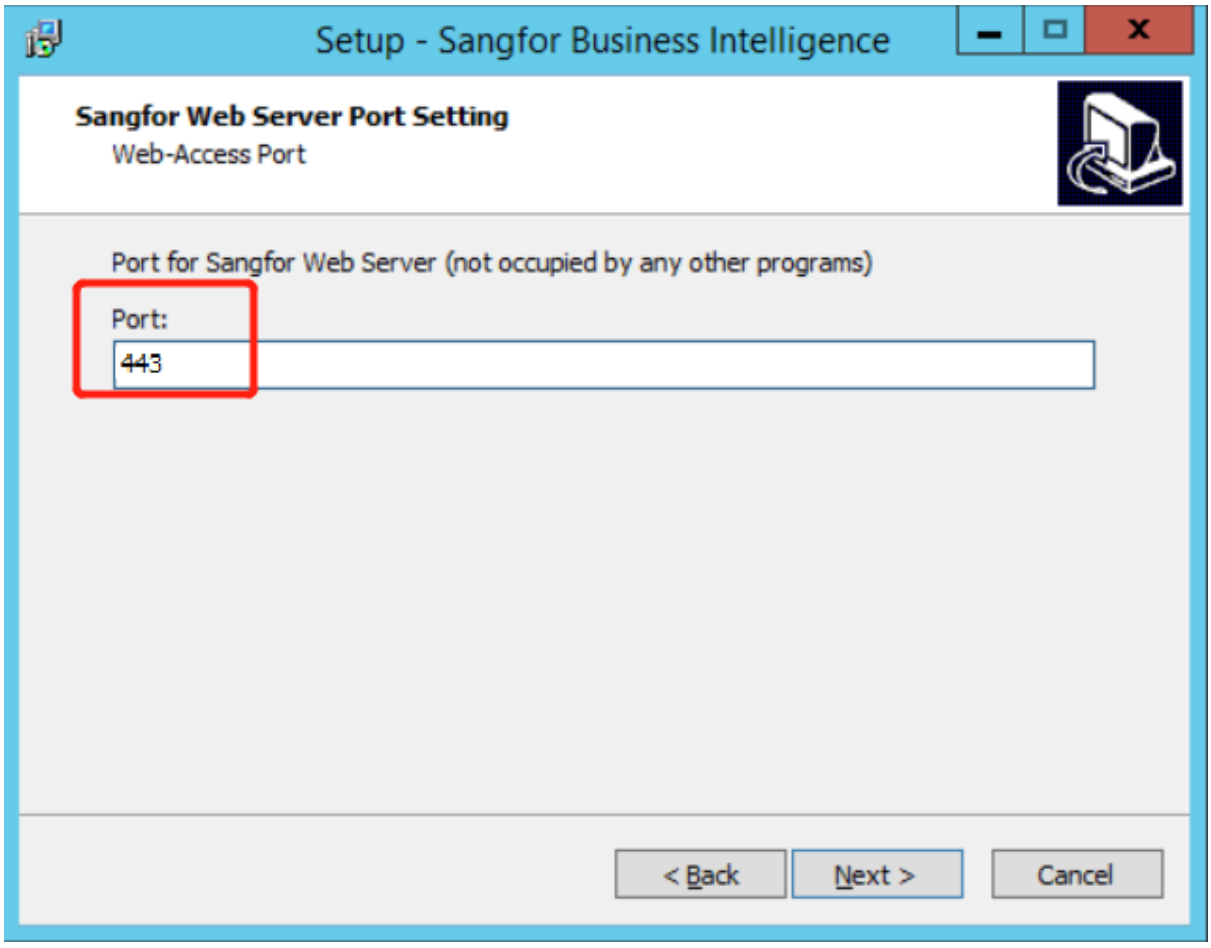
4. Click "Next"



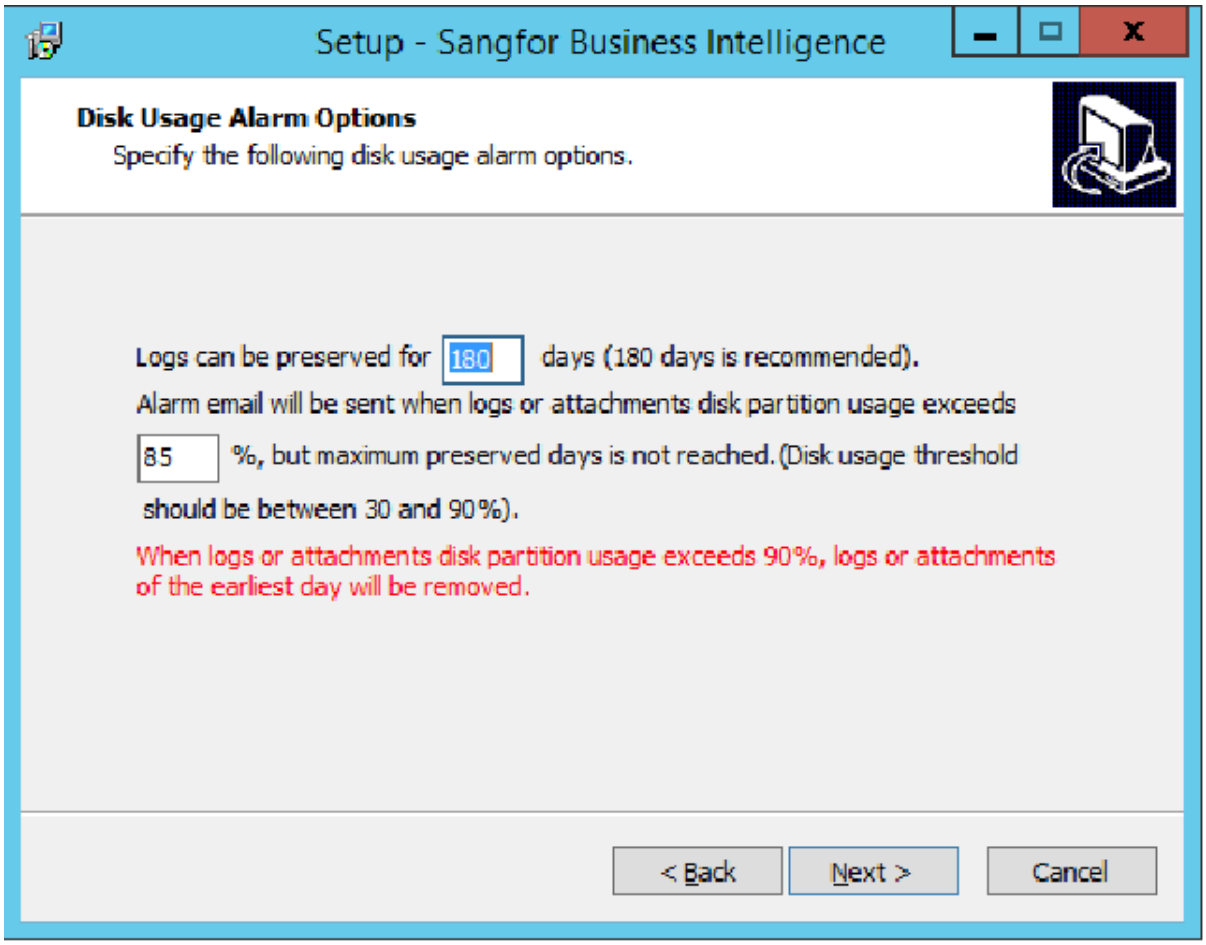
5. Select the disk partition for storing logs and attachments. Generally, it is not recommended to place it in the system partition, but it is recommended to place it in a partition with larger remaining storage space.



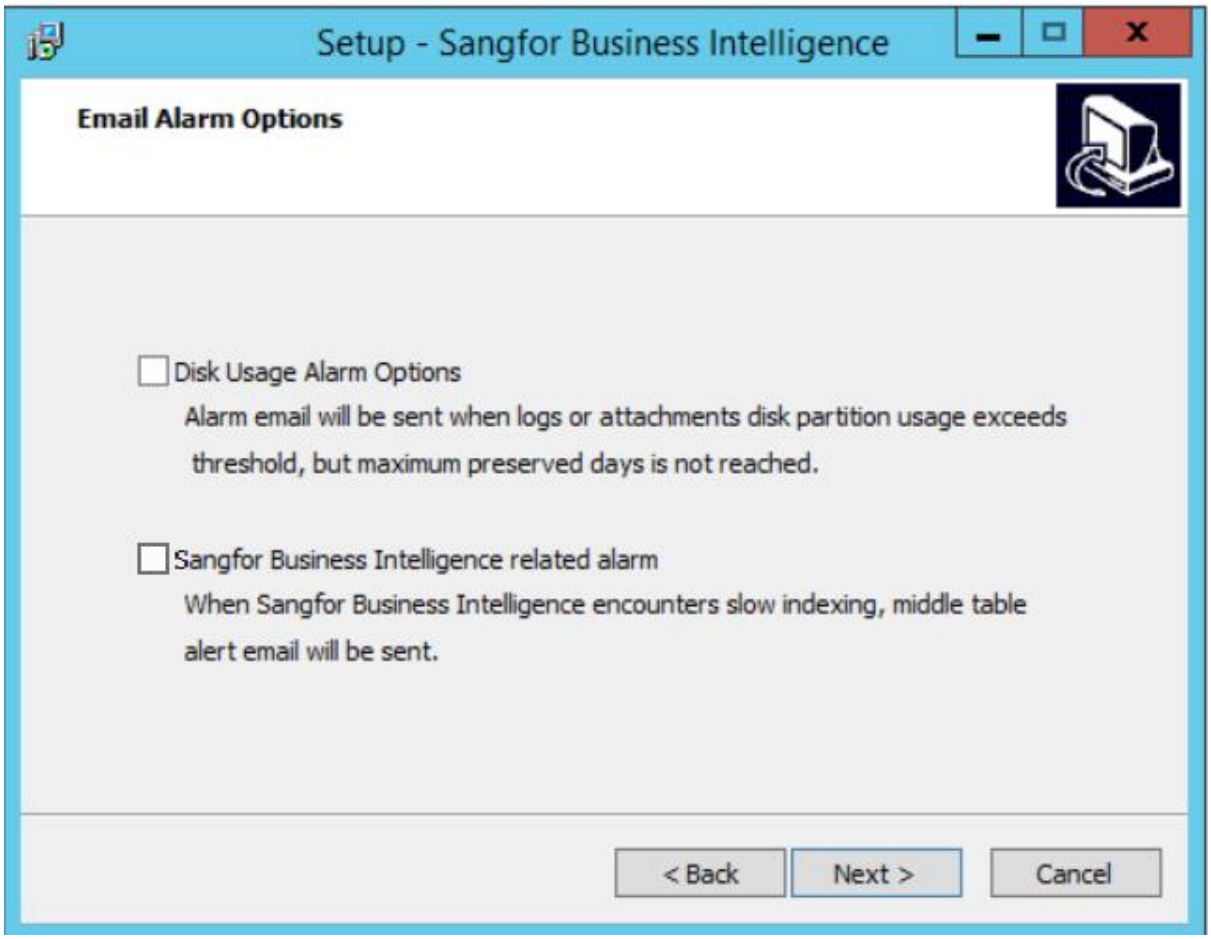
6. Assign a port to the Report Center to use it to access the Report Center Web page after installation. When services such as IIS are running in Windows Server, please select an unused port for Report Center to use.

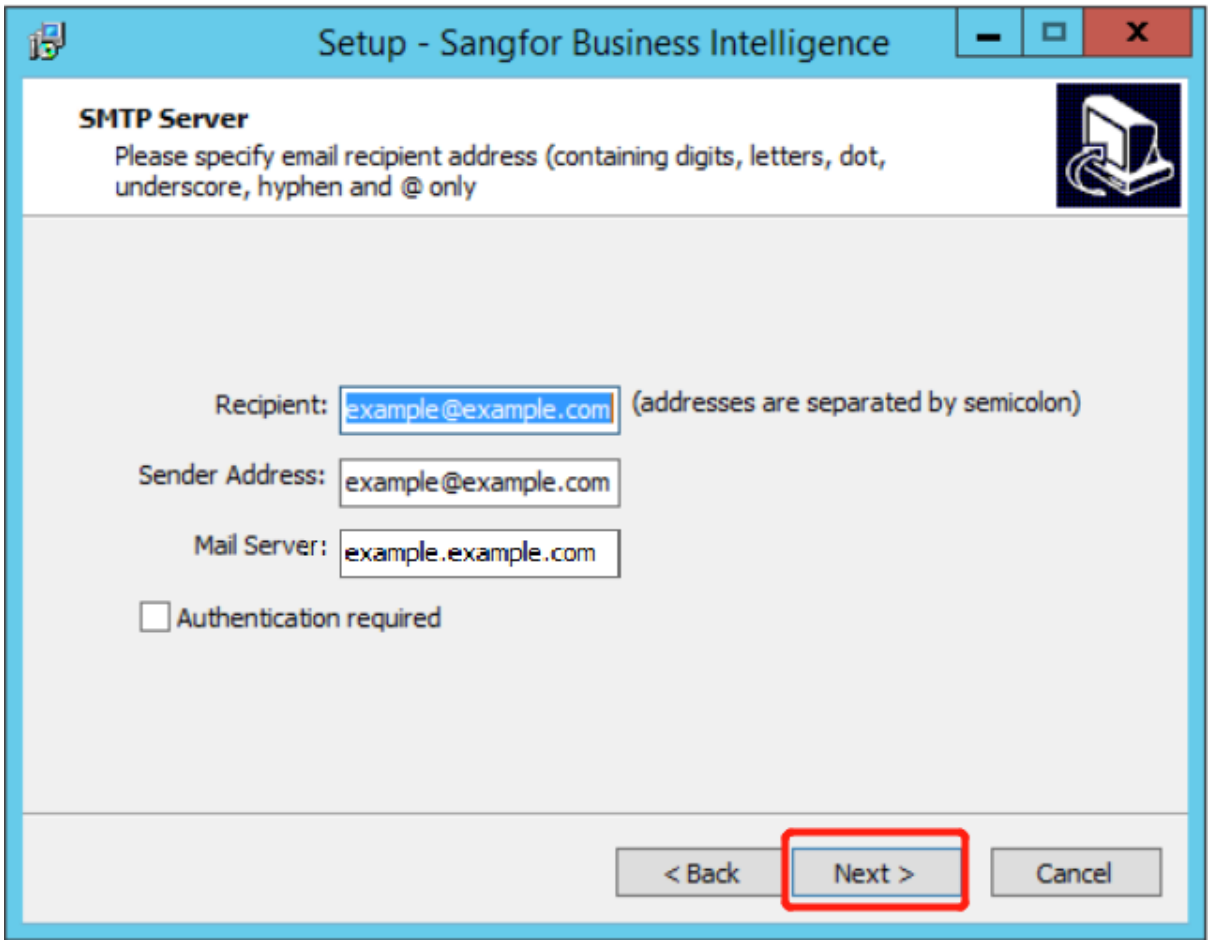


7. Click "Next"

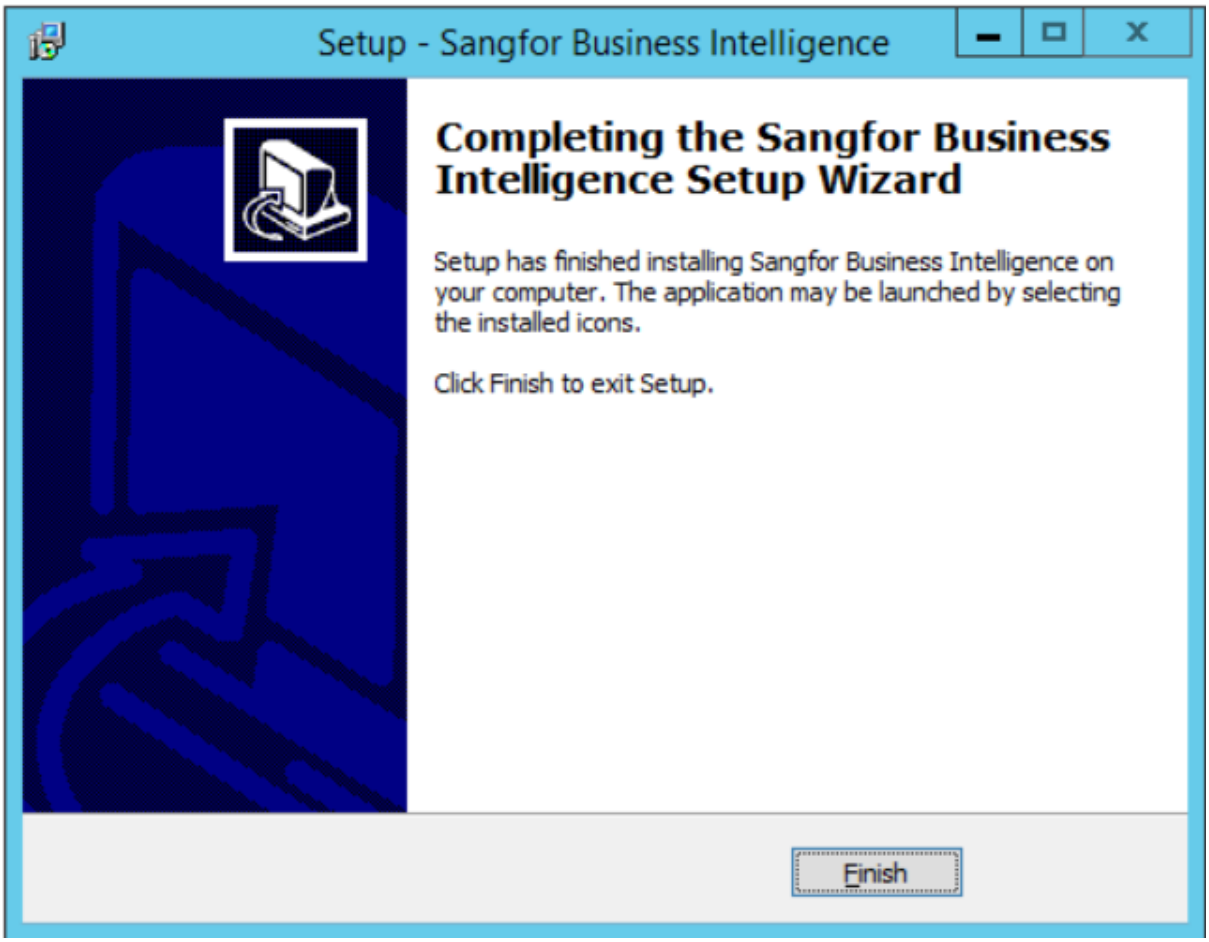


8. There is no need to configure the disk alarm for the time being, and it can be configured on the web page after the installation is complete.

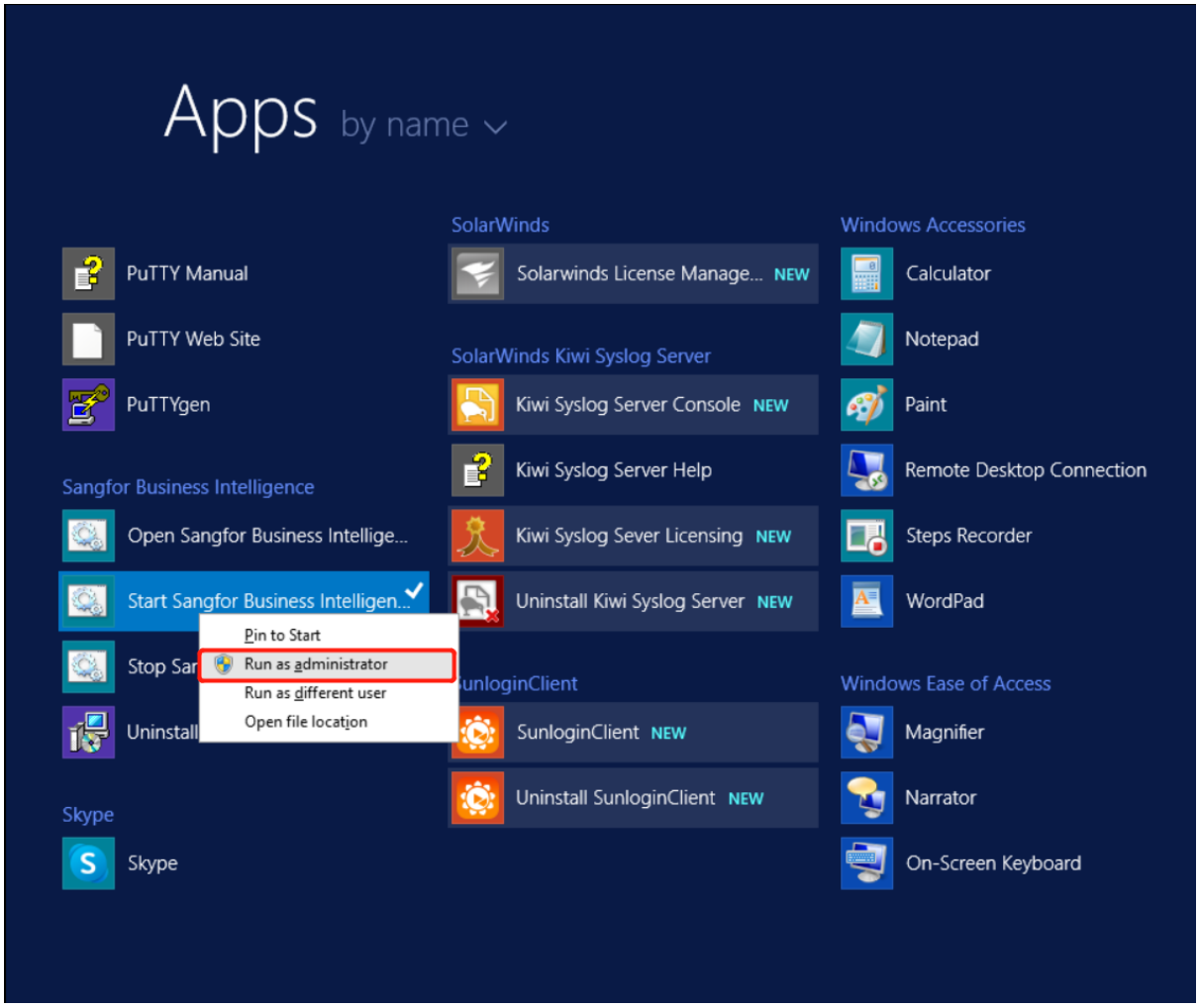

Setup - Sangfor Business Intelligence
Email Alarm Options
Disk Usage Alarm Options
Alarm email will be sent when logs or attachments disk partition usage exceeds threshold, but maximum preserved days is not reached.
Sangfor Business Intelligence related alarm
When Sangfor Business Intelligence encounters slow indexing, middle table alert email will be sent.
< Back
Next >
Cancel

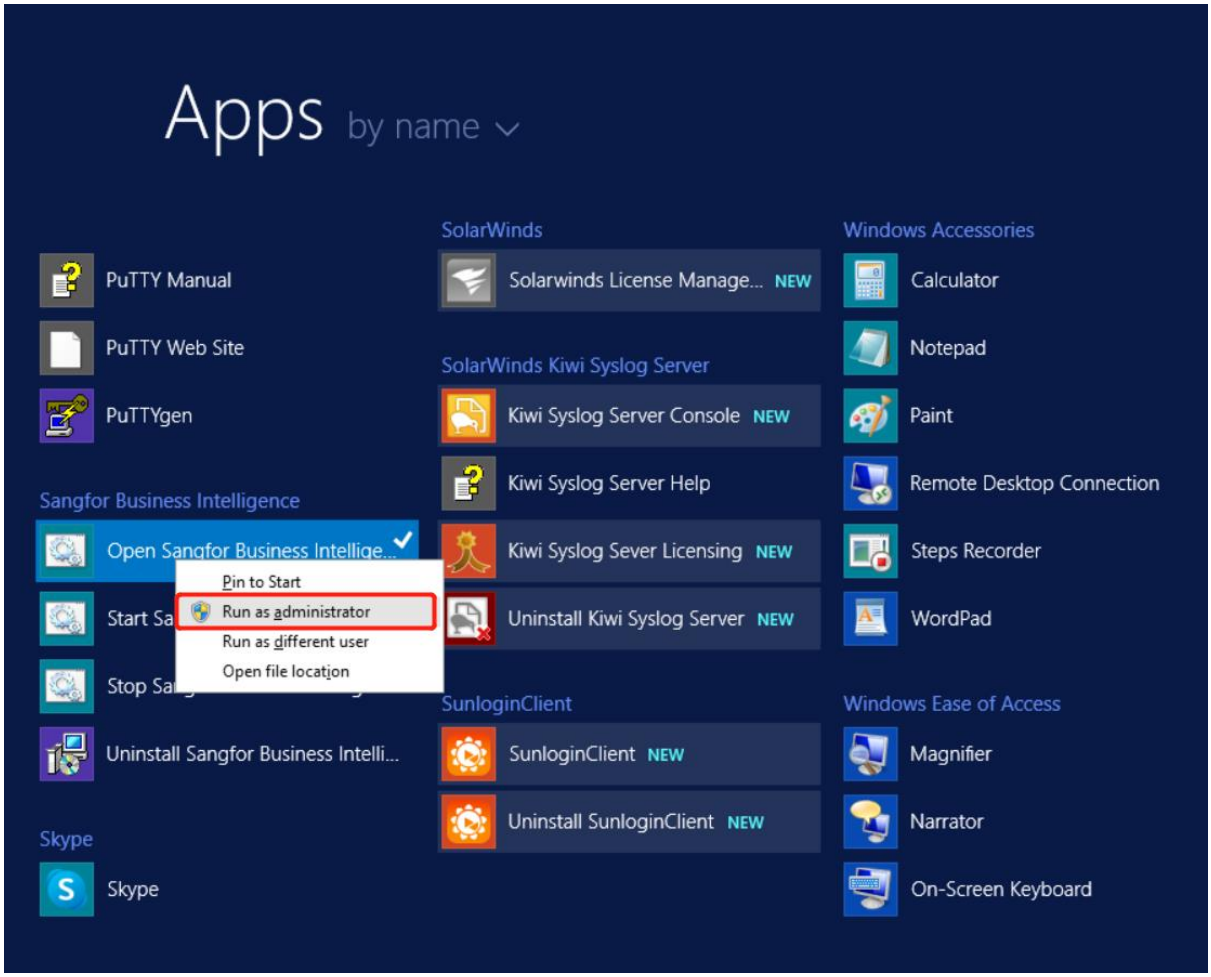


9.Install Report Center.

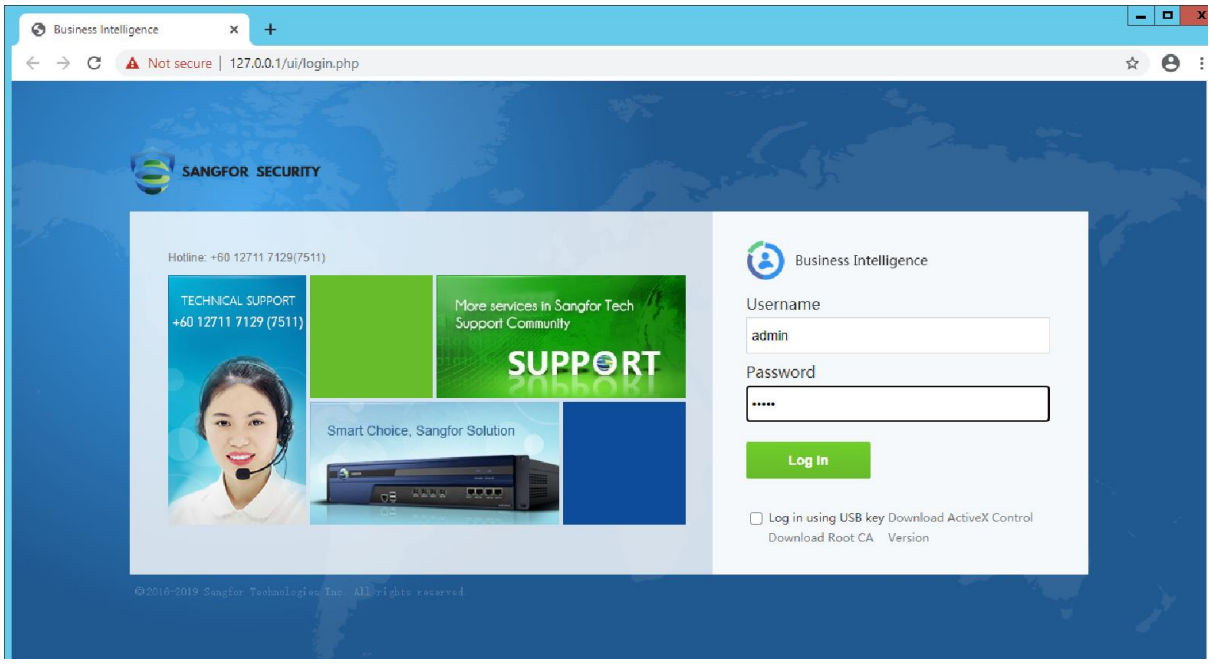


10. Login in Report Center Web Console.

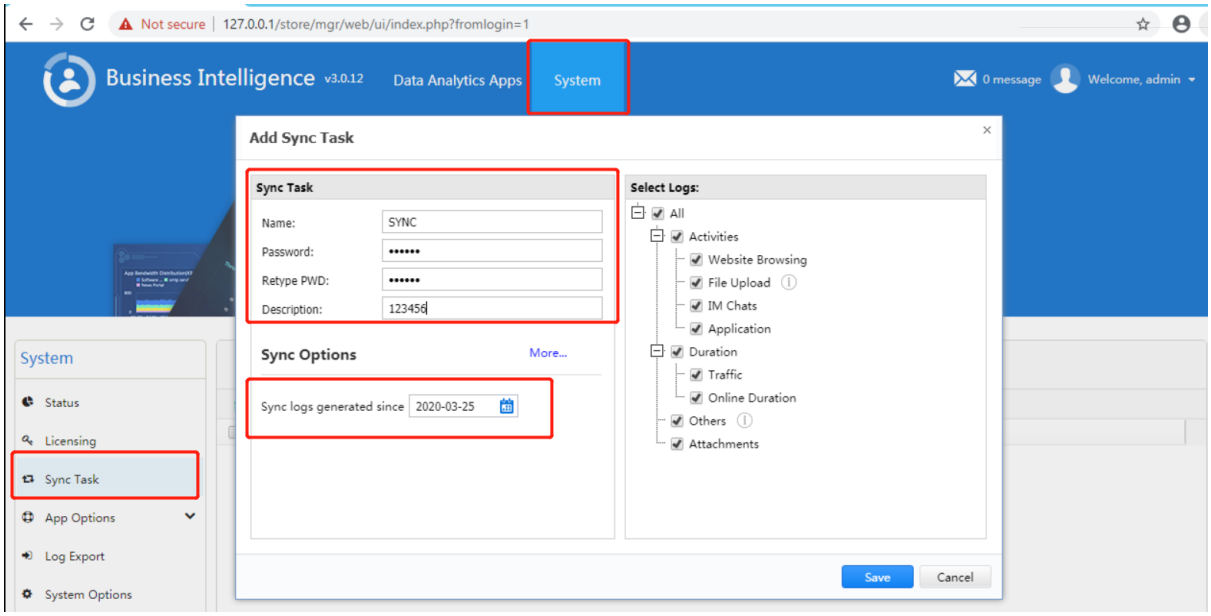

Apps by name
PuTTY Manual
PuTTY Web Site
PuTTYgen
Sangfor Business Intelligence
Open Sangfor Business Intellige...
Start Sangfor Business Intelligen...
Stop San
Uninstall
Skype
Skype
SolarWinds
Solarwinds License Manage... NEW
SolarWinds Kiwi Syslog Server
Kiwi Syslog Server Console NEW
Kiwi Syslog Server Help
Kiwi Syslog Sever Licensing NEW
Uninstall Kiwi Syslog Server NEW
unloginClient
SunloginClient NEW
Uninstall SunloginClient NEW
Windows Accessories
Calculator
Notepad
Paint
Remote Desktop Connection
Steps Recorder
WordPad
Windows Ease of Access
Magnifier
Narrator
On-Screen Keyboard
Pin to Start
Run as administrator
Run as different user
Open file location



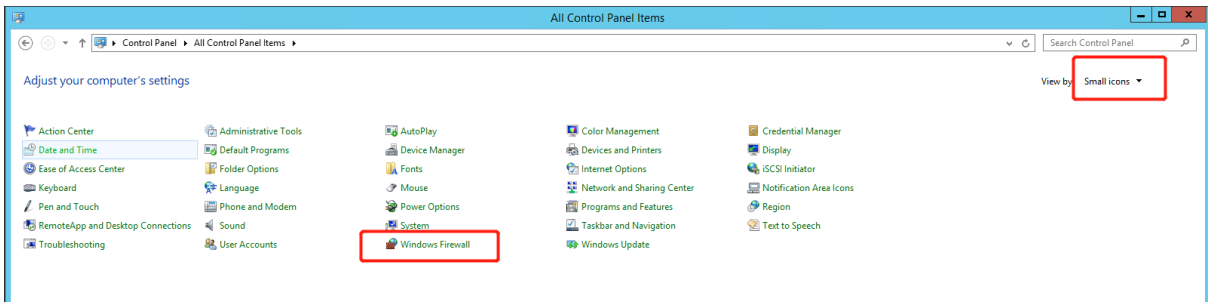
11. Use admin/admin account and password to login.

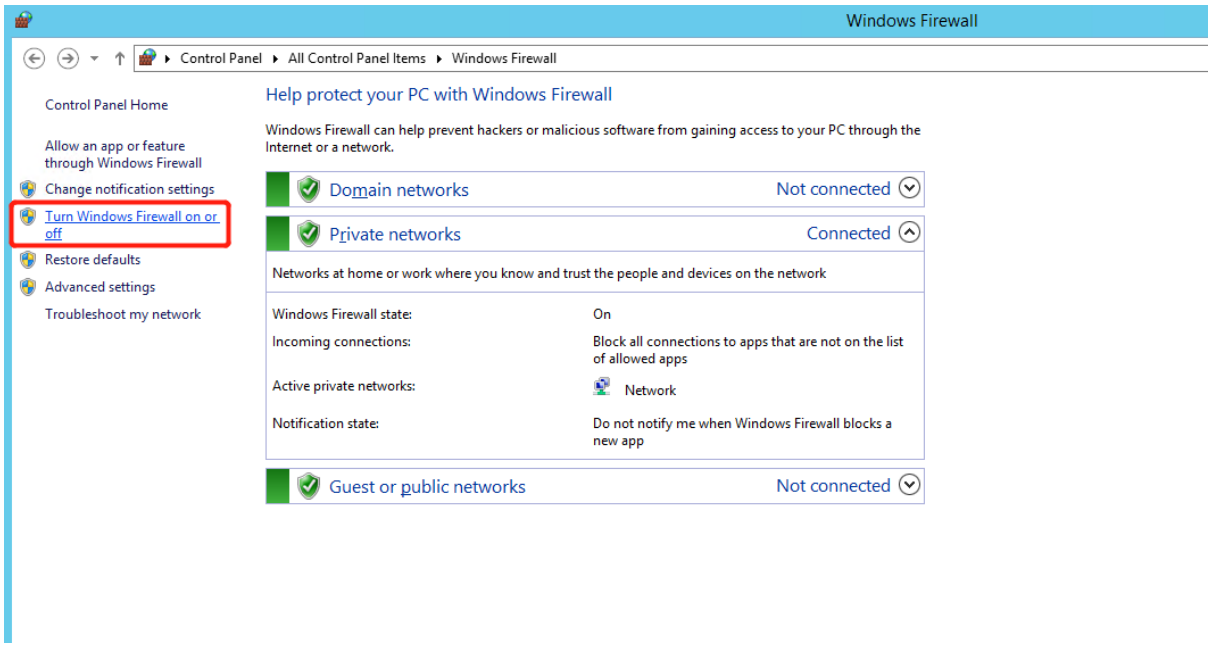


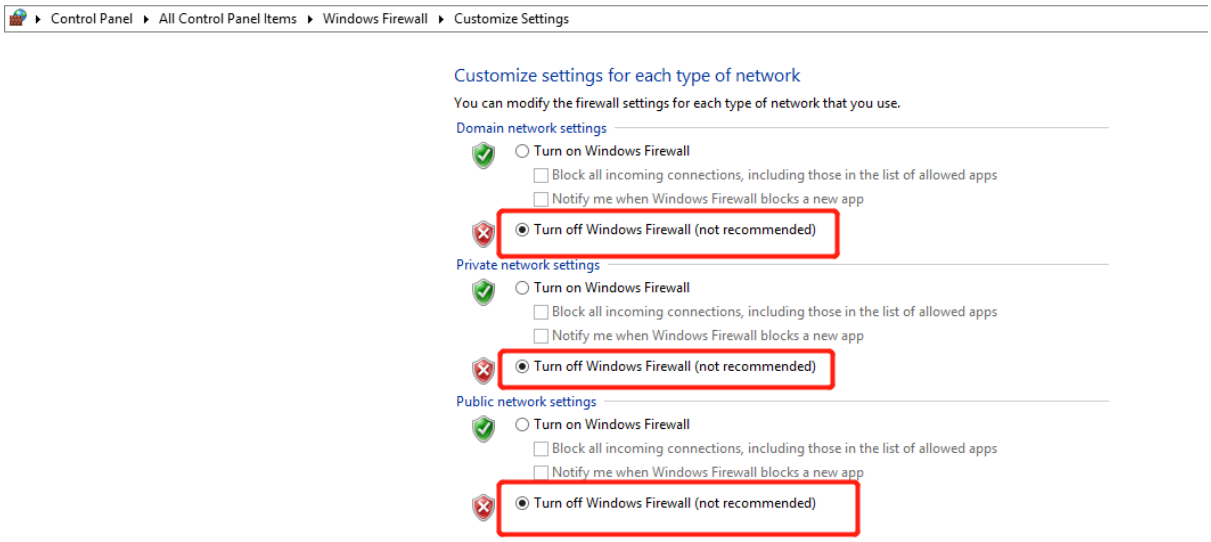
12. Configure a synchronization policy after logging in, and use this synchronization policy to synchronize logs later on IAM.



13. Turn off the windows firewall, or release the data on the relevant ports separately. When the windows firewall is turned on, the data on ports 801 and 810 used by IAM and Report Center communication will be blocked by default.

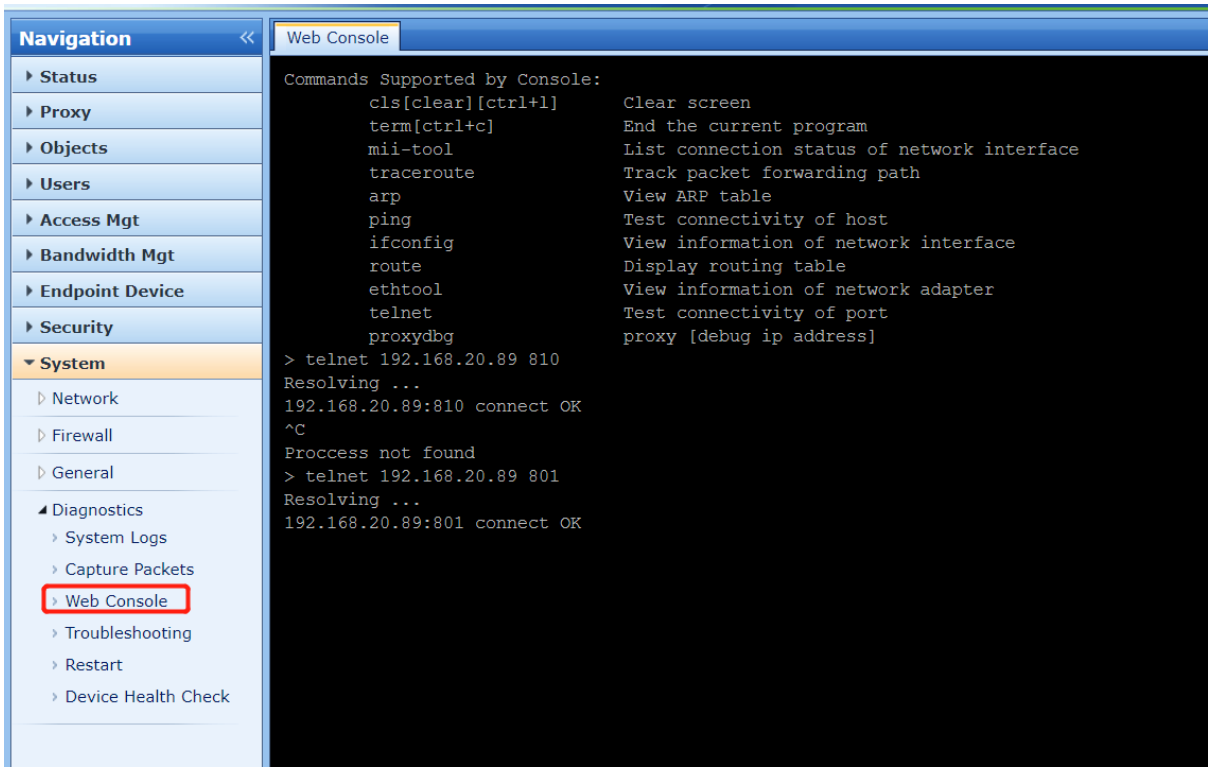




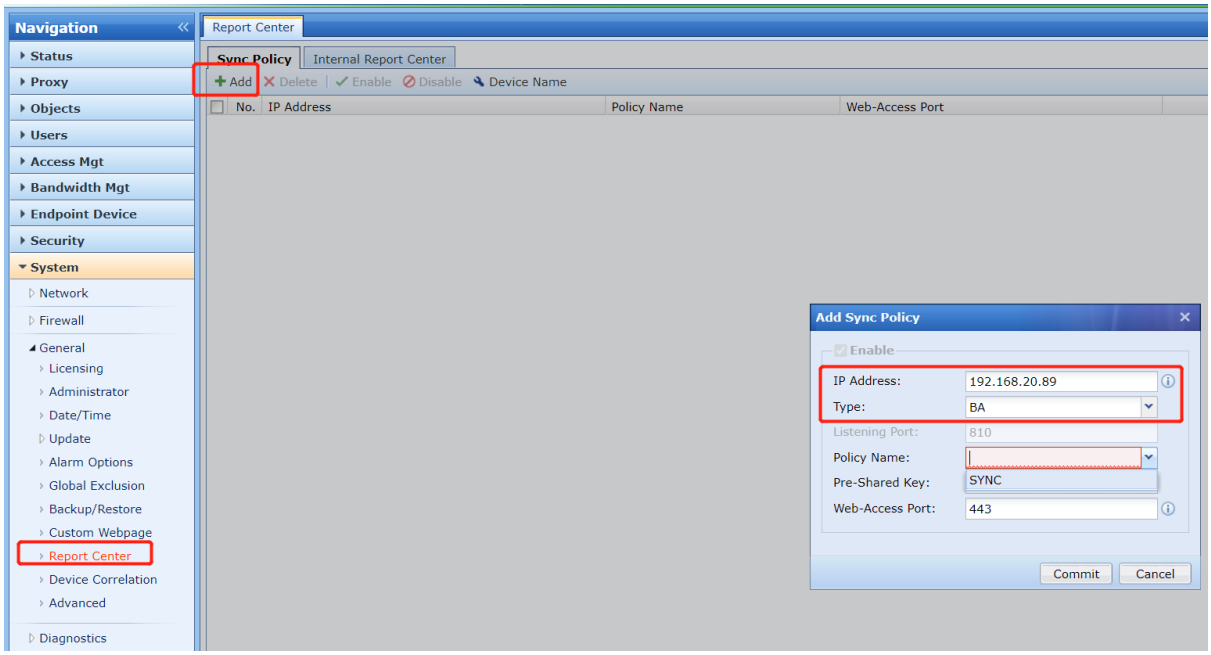


2.2 Configure IAM

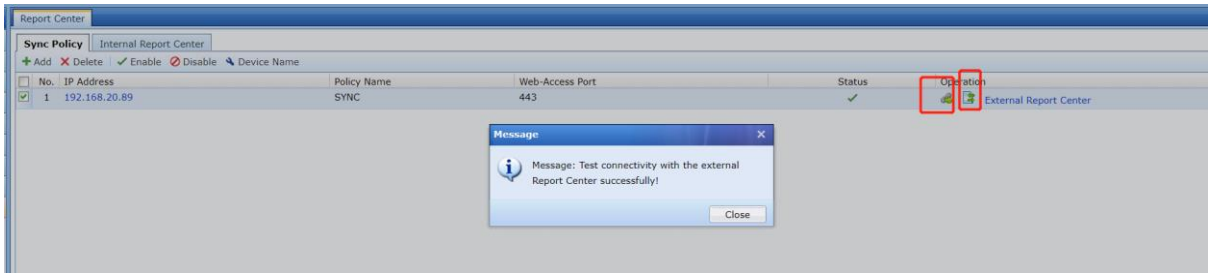
1. Test connectivity in IAM, IAM and Windows Server must be able to access each other's 801 and 810 ports.



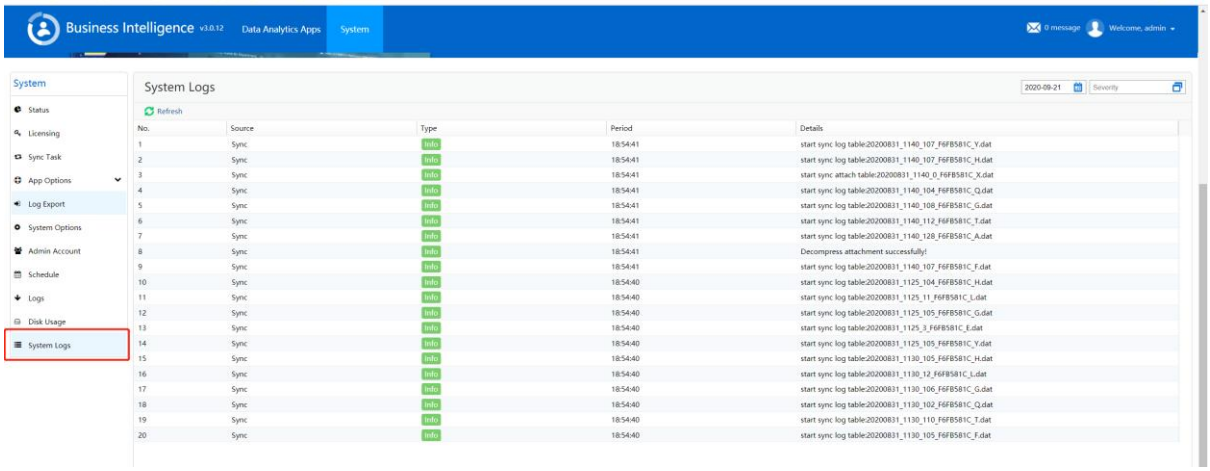
2. Enter the IP of the Windows Server, then select the synchronization policy, and select the corresponding synchronization strategy name and fill in the secret key.



3. Test connectivity and choose to synchronize logs.



4. If the logs can be synchronized normally, you can see the following logs in the system log of the report center.



5. Query the progress of the log center index and mediate table, and the log at this time can be queried when the index and mediate table are generated.

Sync Log to Report Center