



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	1
Chapter 2 Configuration.....	1
2.1 Configuration in Windows Server.....	1
2.2 Configure IAM.....	11

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 2012 x64.

View basic information about your computer

Windows edition

Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Core(TM)2 Duo CPU T7700 @ 2.40GHz 2.10 GHz

Installed memory (RAM): 8.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: Limited Touch Support with 11 Touch Points

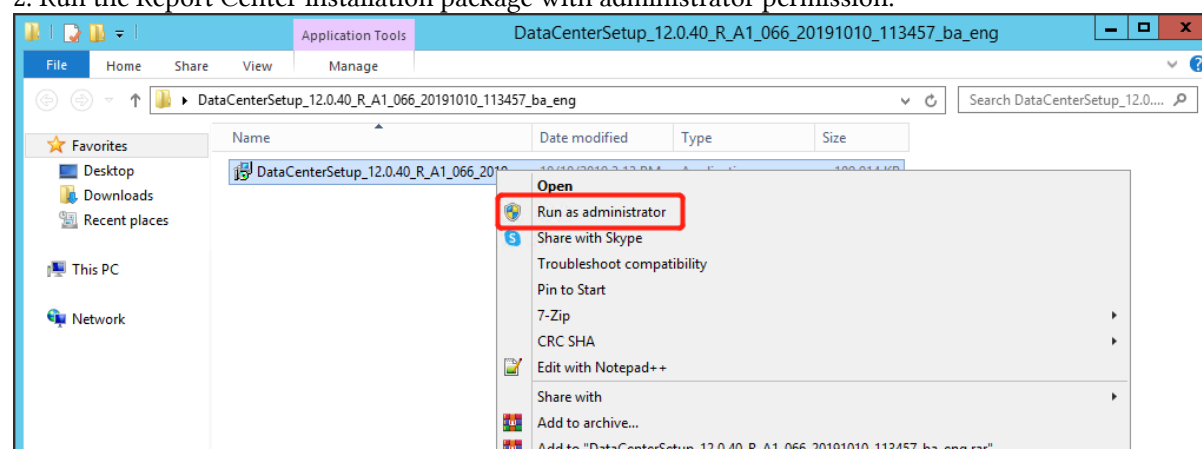
Computer name, domain, and workgroup settings

Computer name: WIN-6L9J2G79TUQ

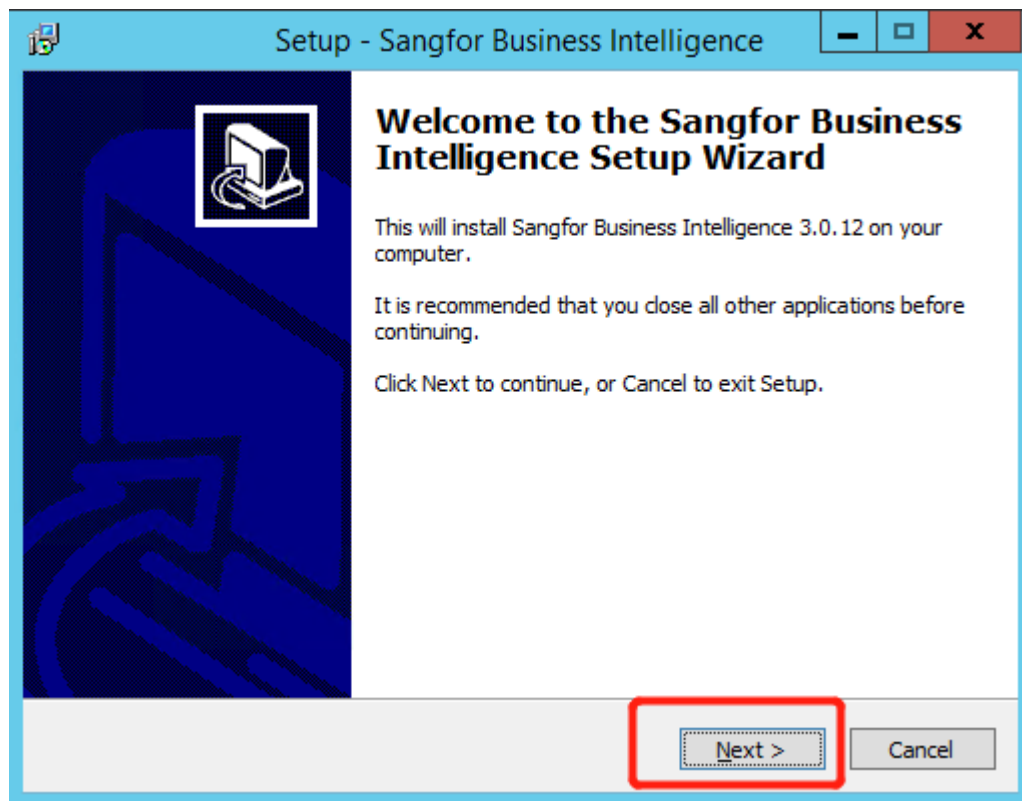
Full computer name: WIN-6L9J2G79TUQ.SCCORP.local

Computer description:

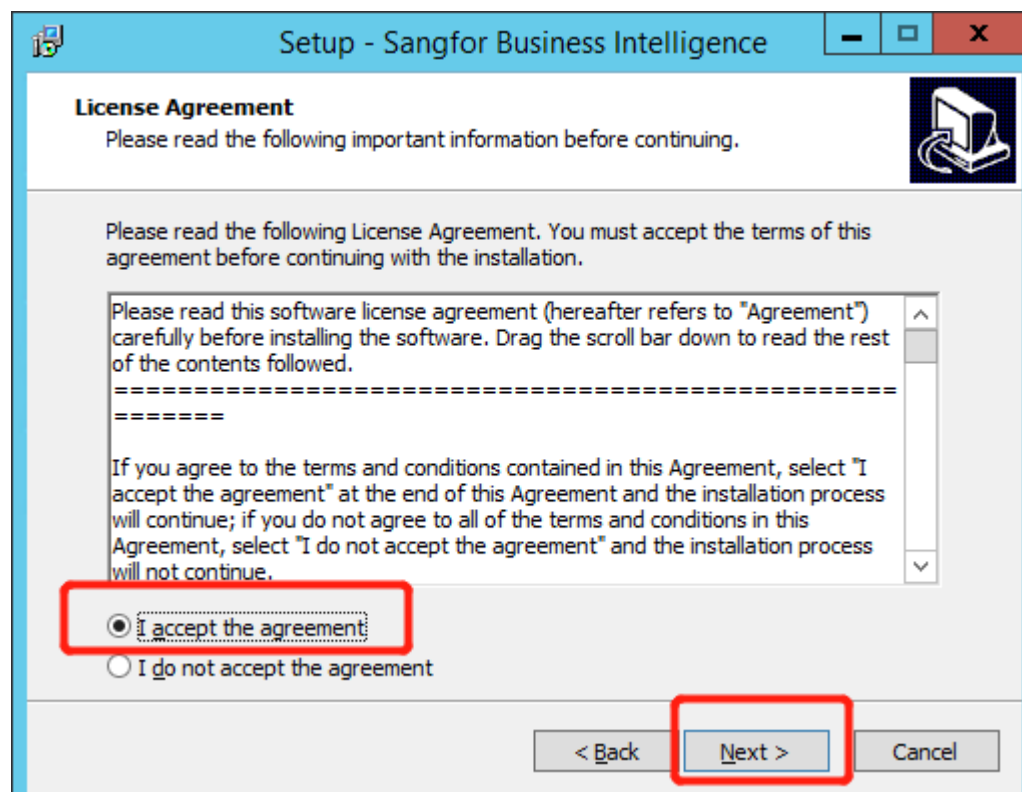
2. Run the Report Center installation package with administrator permission.



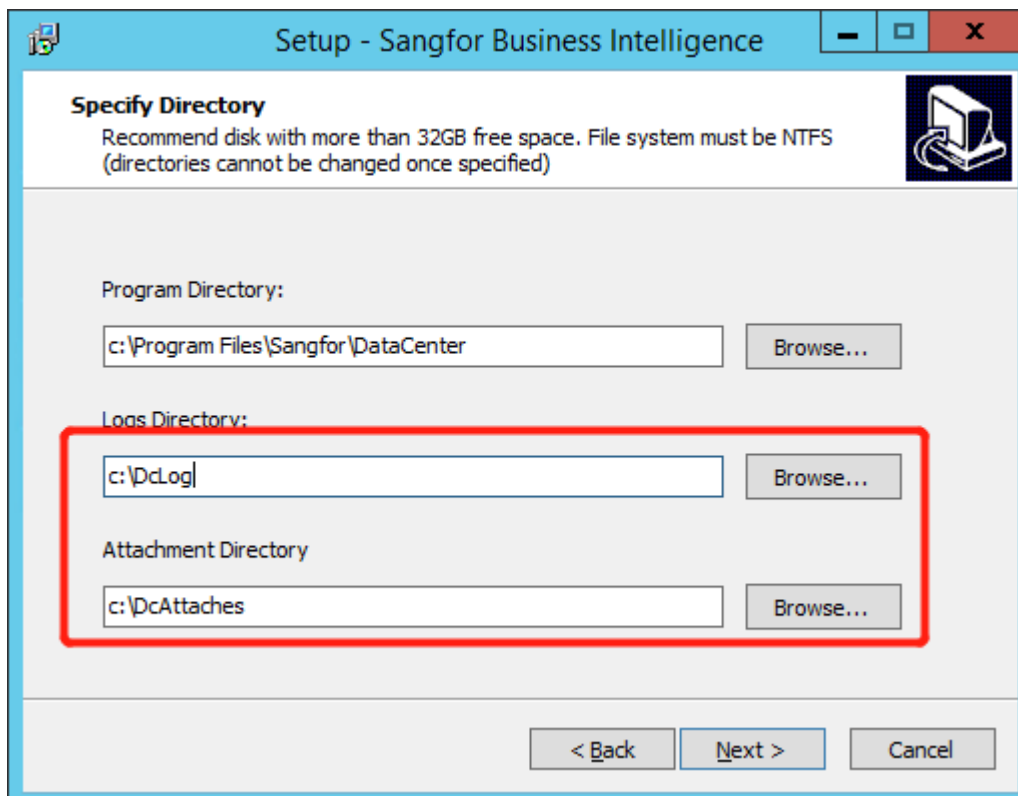
3. Click "Next"



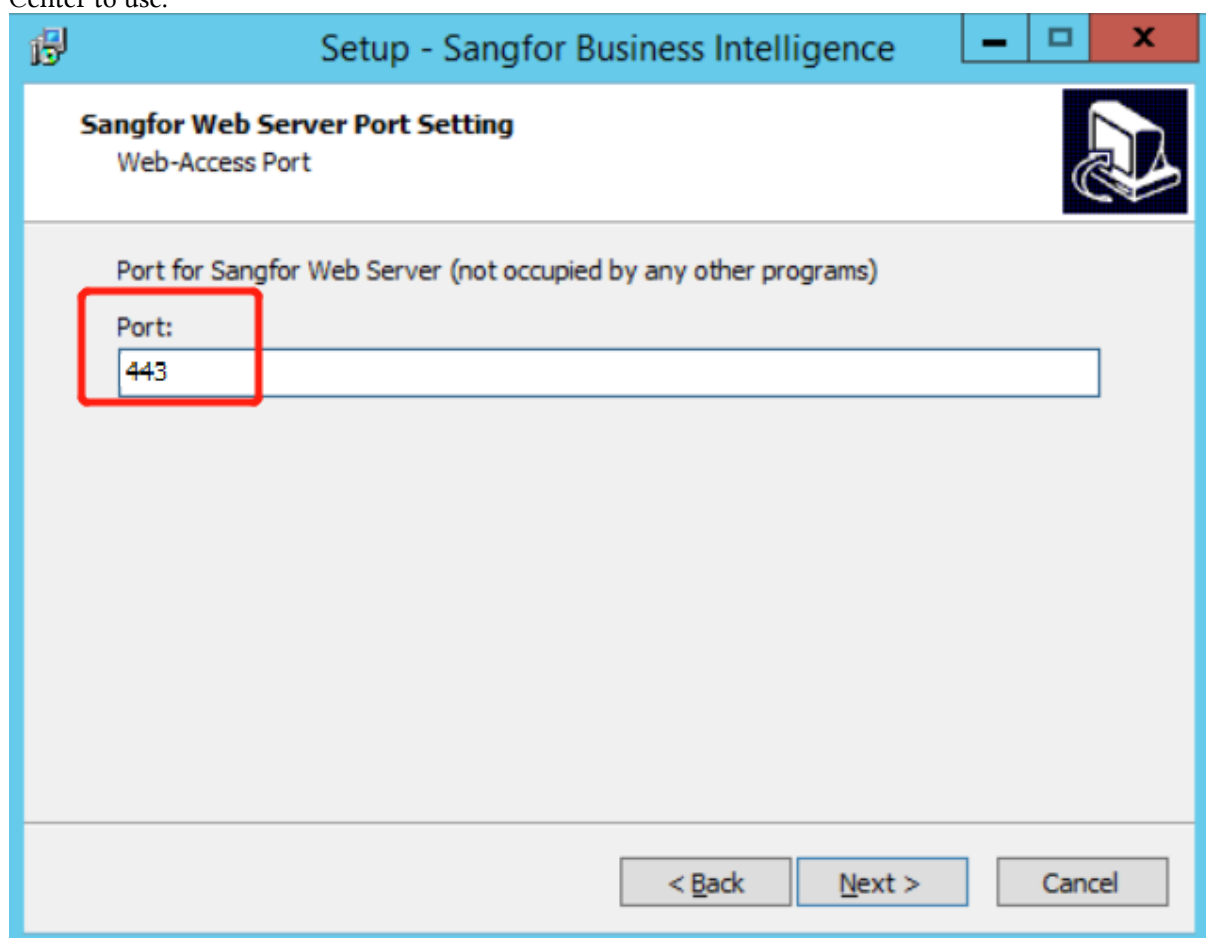
4. Click "Next"



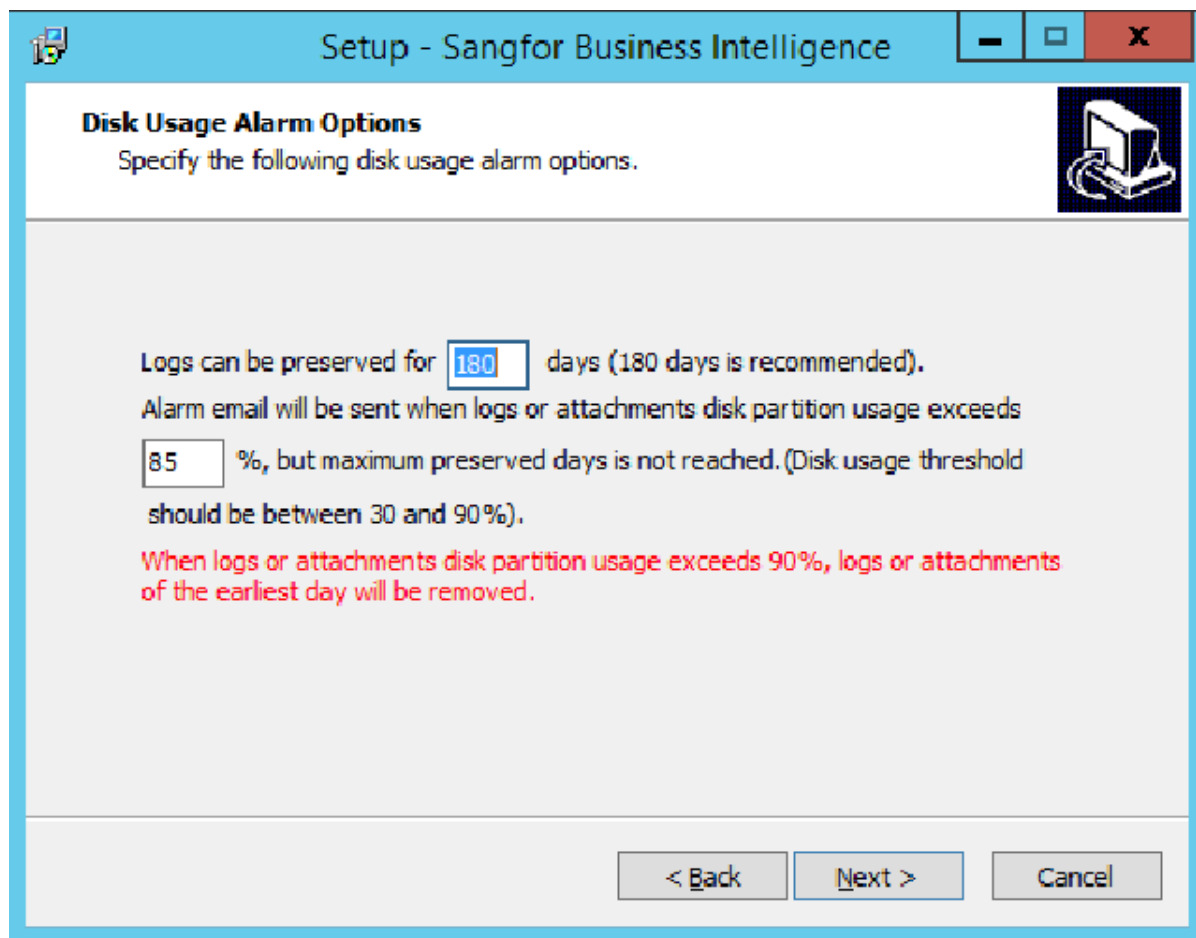
5. Select the disk partition for storing logs and attachments. Generally, it is not recommended to place it in the system partition, but it is recommended to place it in a partition with larger remaining storage space.



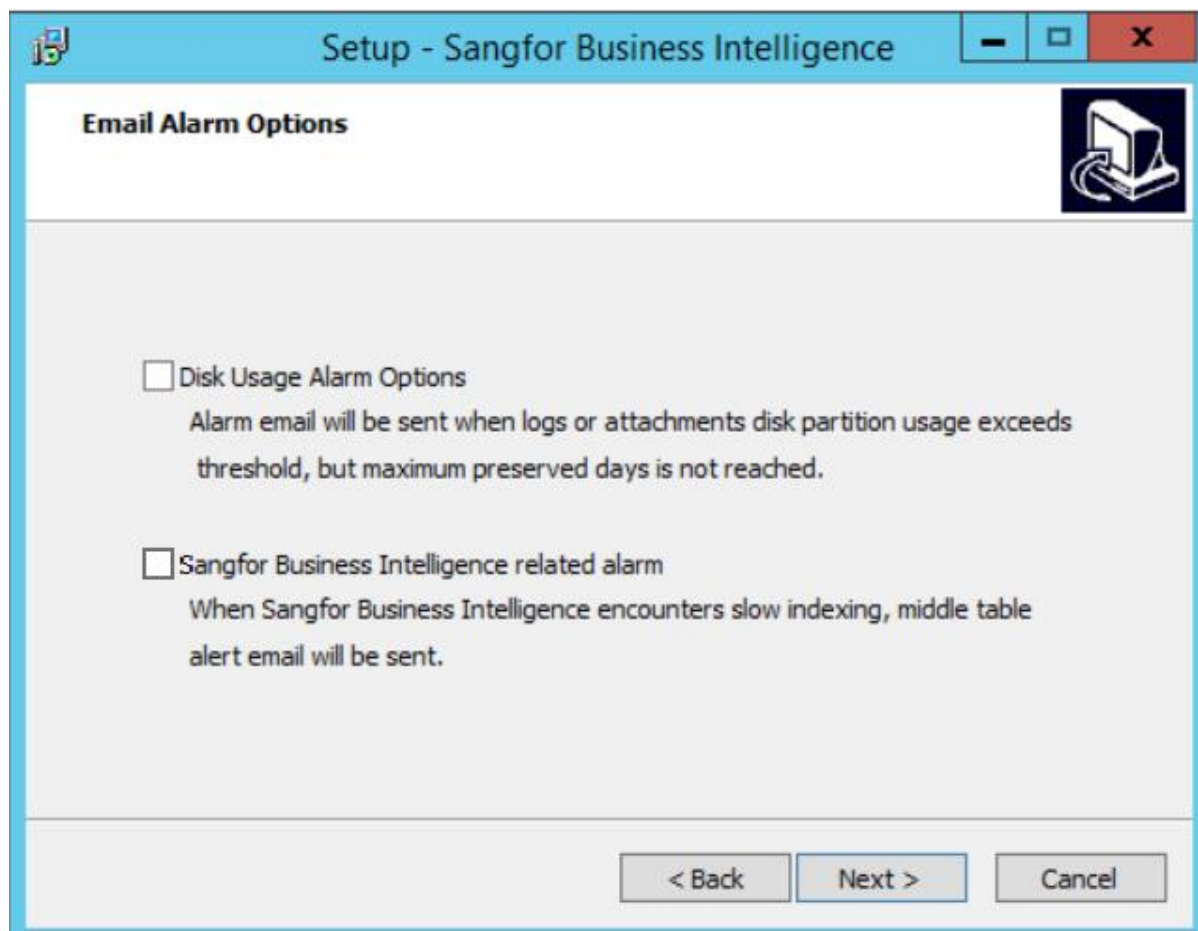
6. Assign a port to the Report Center to use it to access the Report Center Web page after installation. When services such as IIS are running in Windows Server, please select an unused port for Report Center to use.



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

SMTP Server

Please specify email recipient address (containing digits, letters, dot, underscore, hyphen and @ only)

Recipient: (addresses are separated by semicolon)

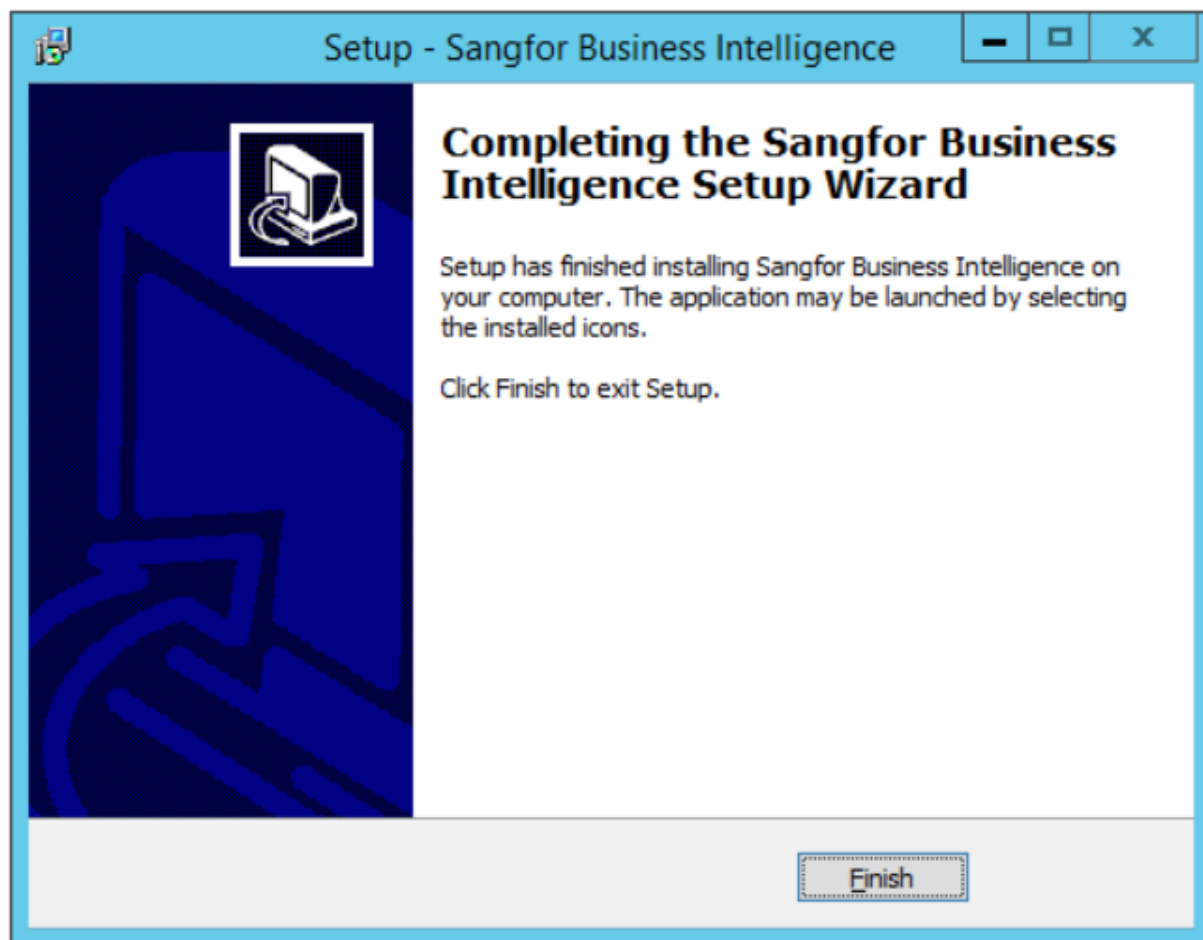
Sender Address:

Mail Server:

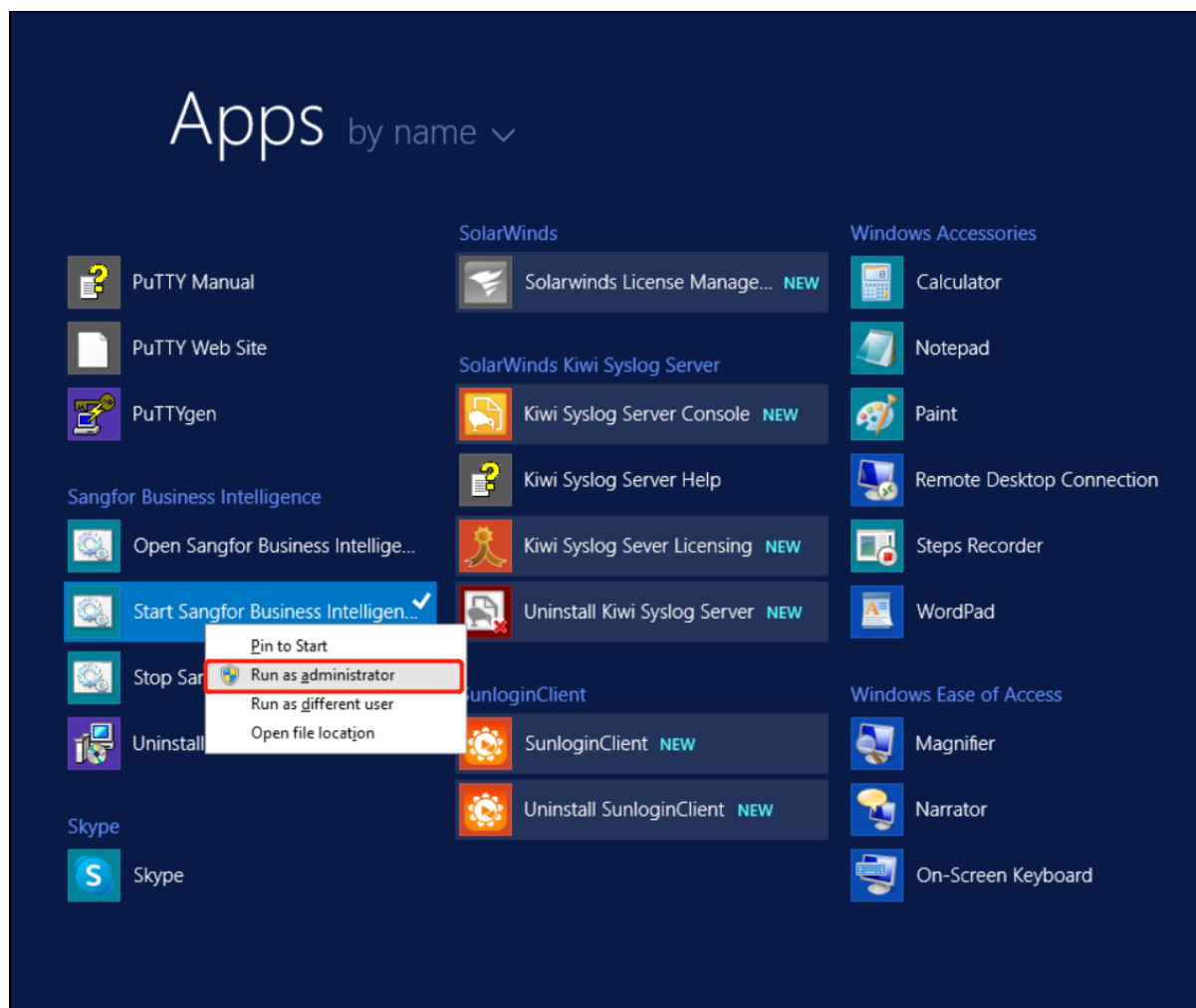
☐ Authentication required

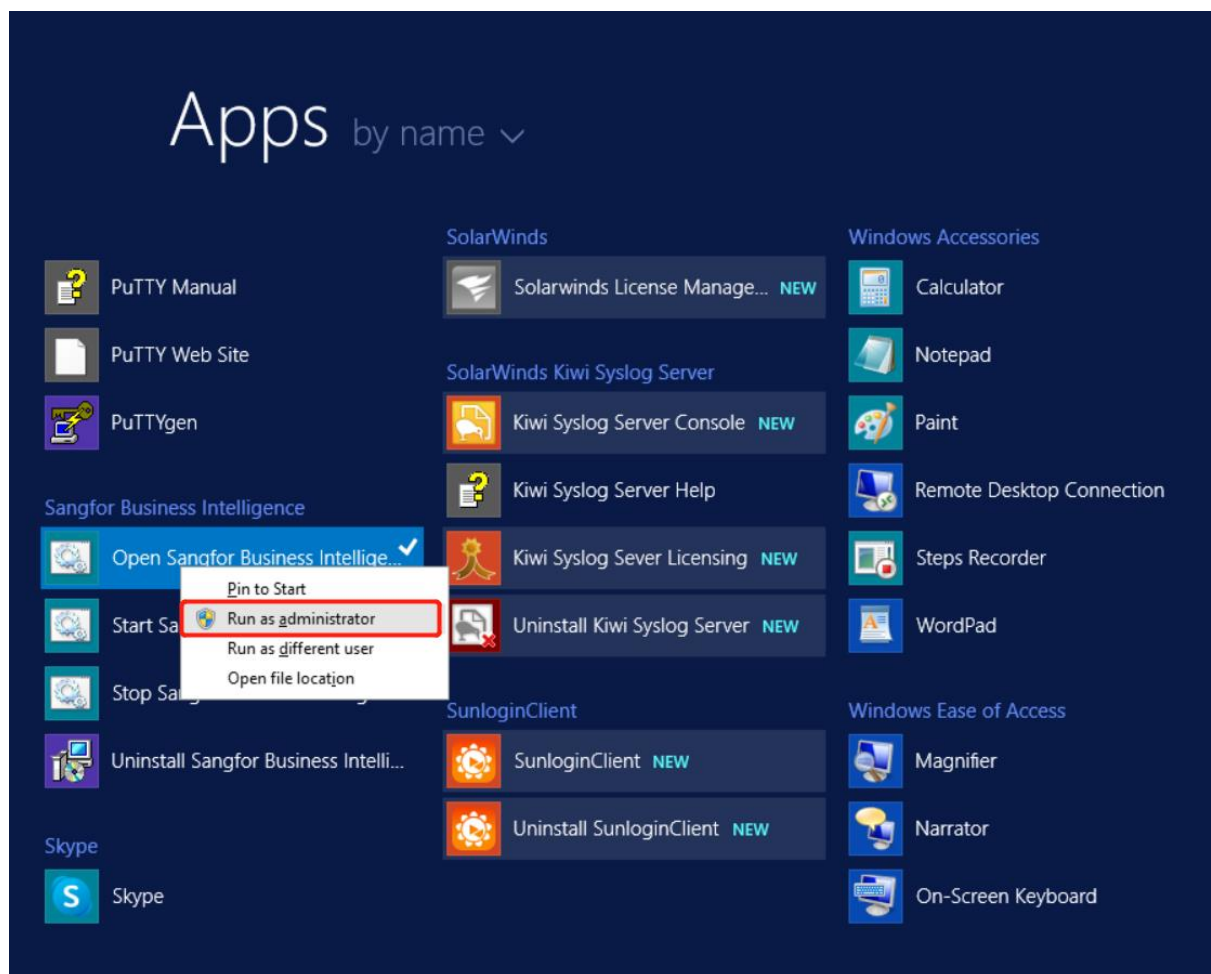
< Back **Next >** Cancel

9.Install Report Center.

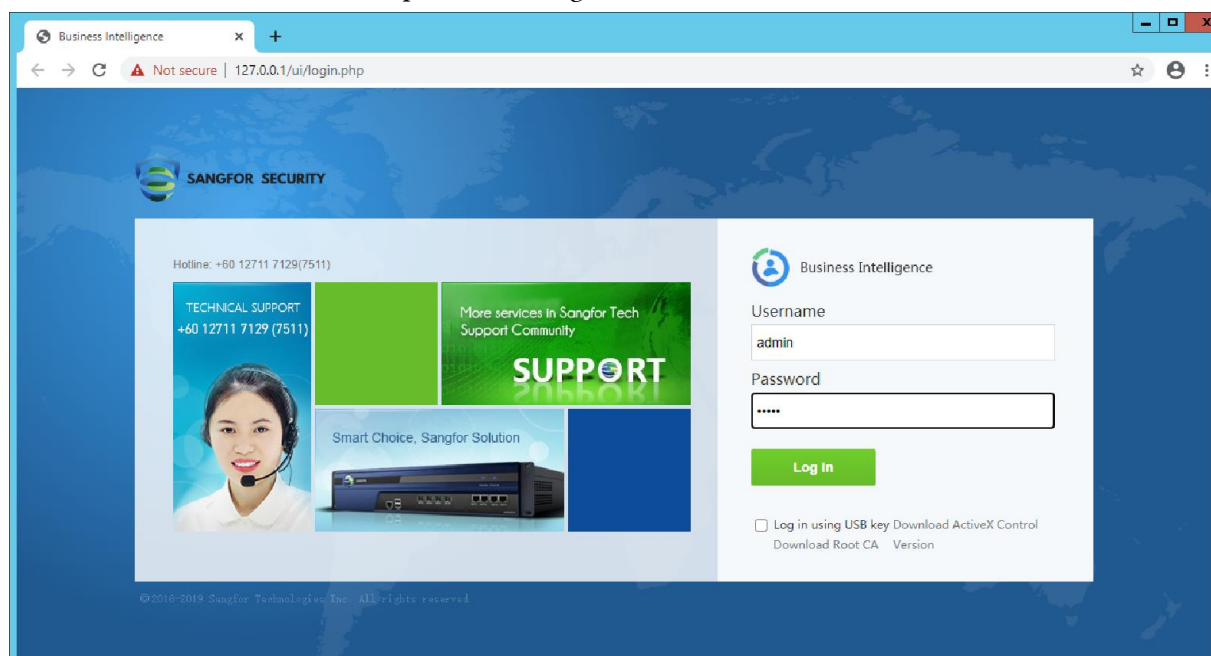


10. Login in Report Center Web Console.



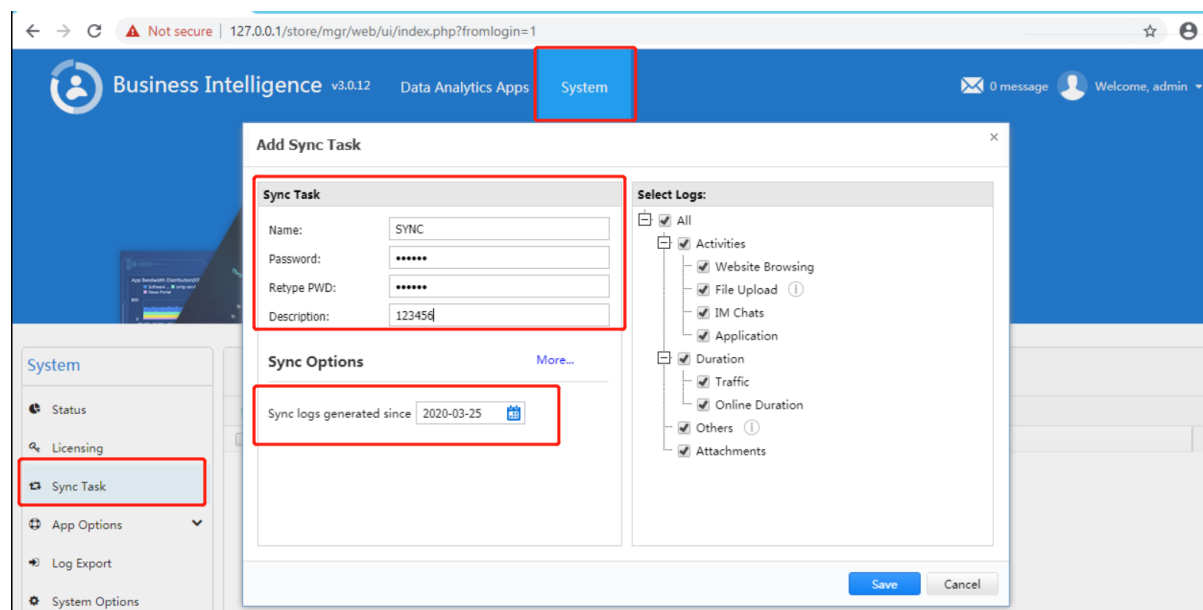


11. Use admin/admin account and password to login.

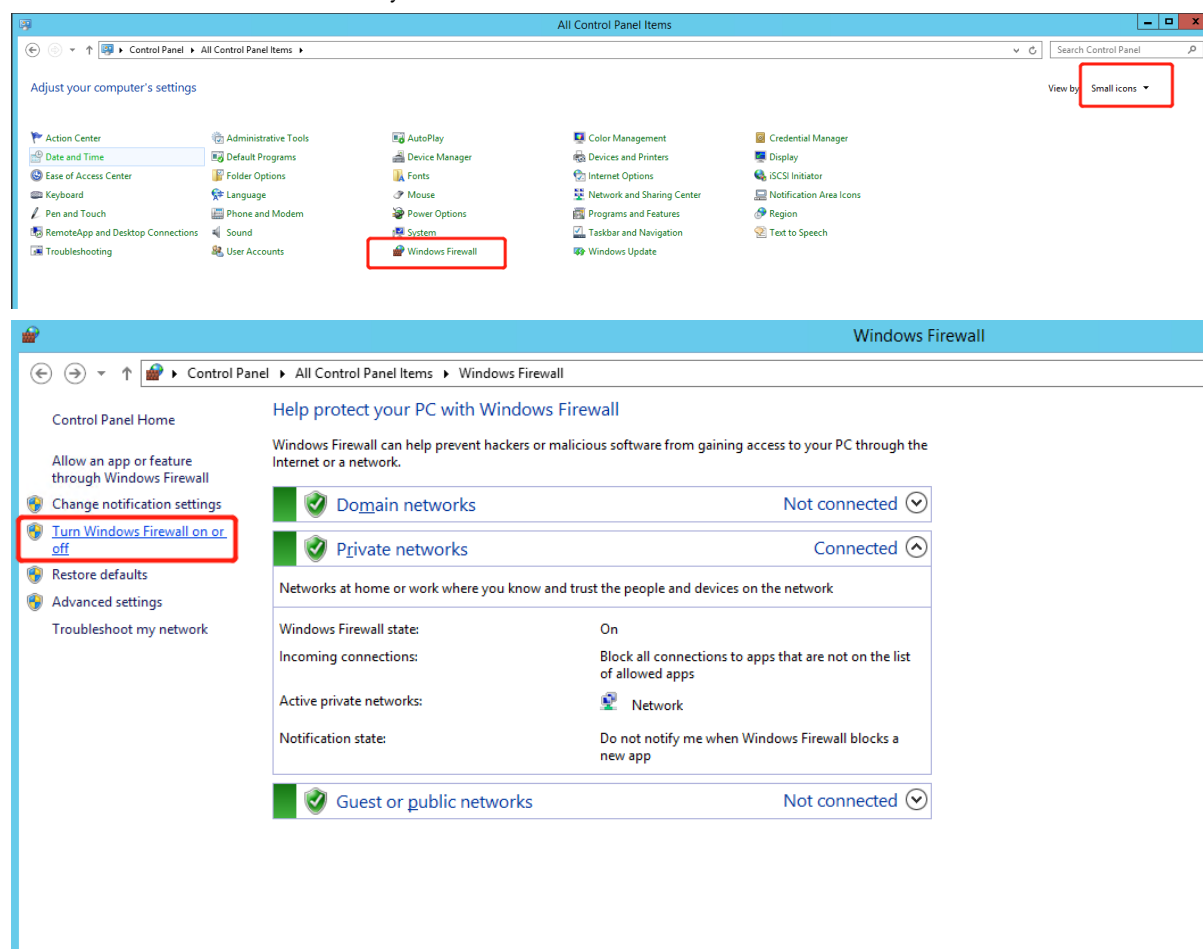


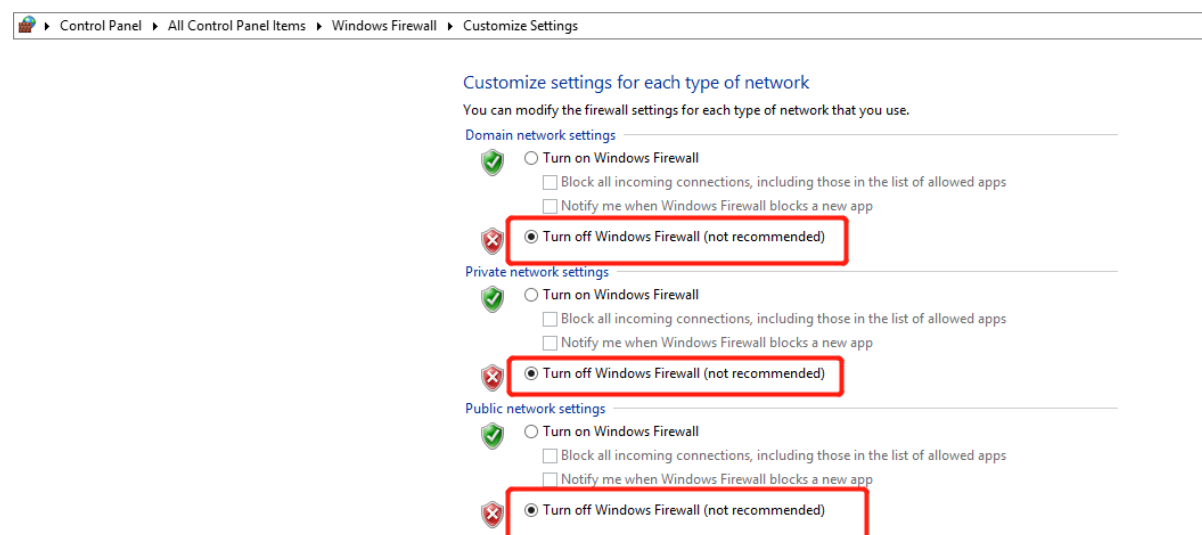
12. Configure a synchronization policy after logging in, and use this synchronization policy to synchronize logs later on IAM.

Sync Log to Report Center



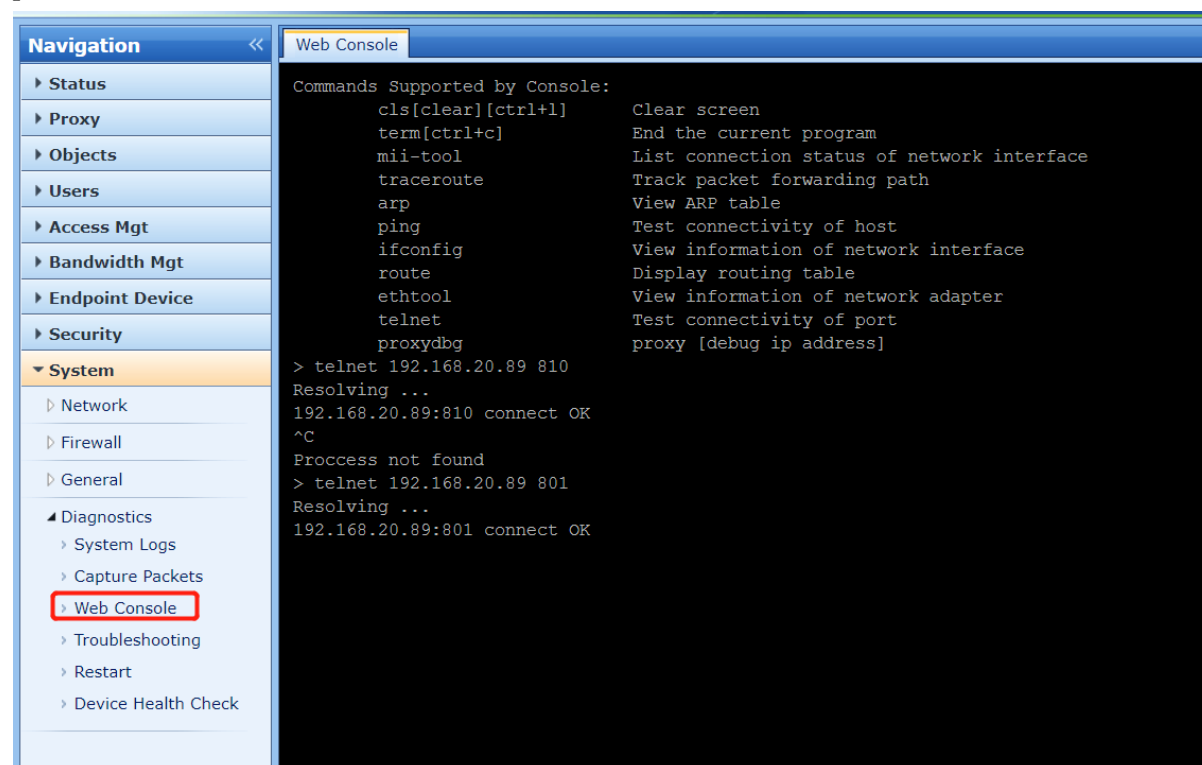
13. Turn off the windows firewall, or release the data on the relevant ports separately. When the windows firewall is turned on, the data on ports 801 and 810 used by IAM and Report Center communication will be blocked by default.





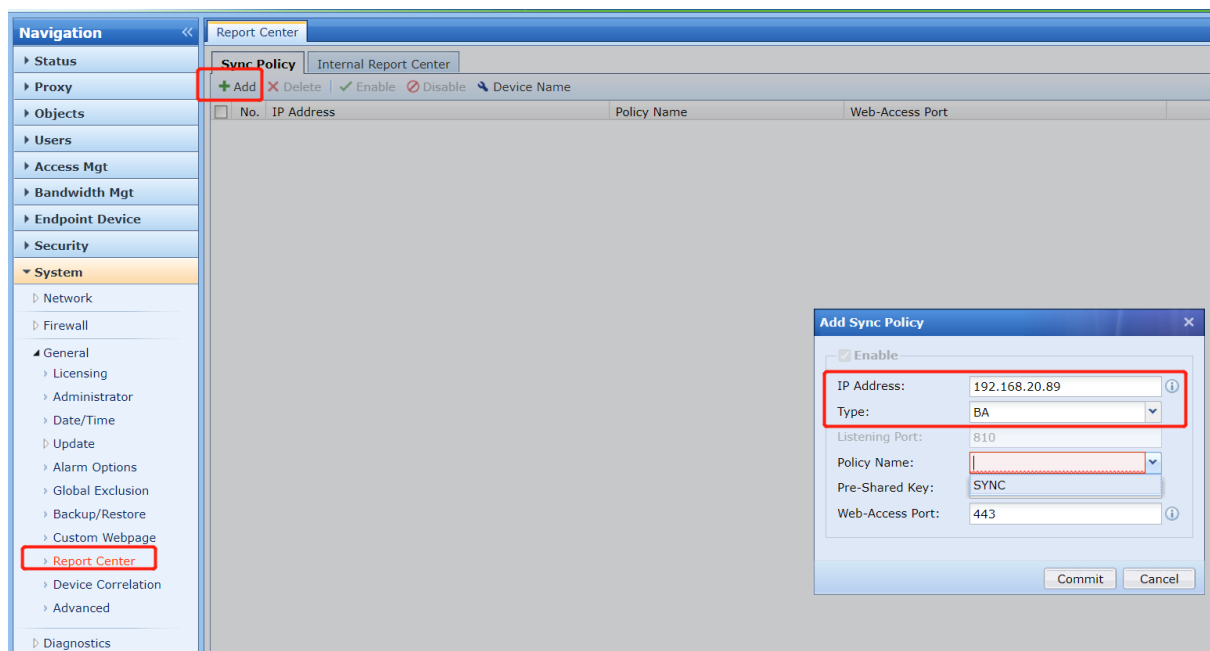
2.2 Configure IAM

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

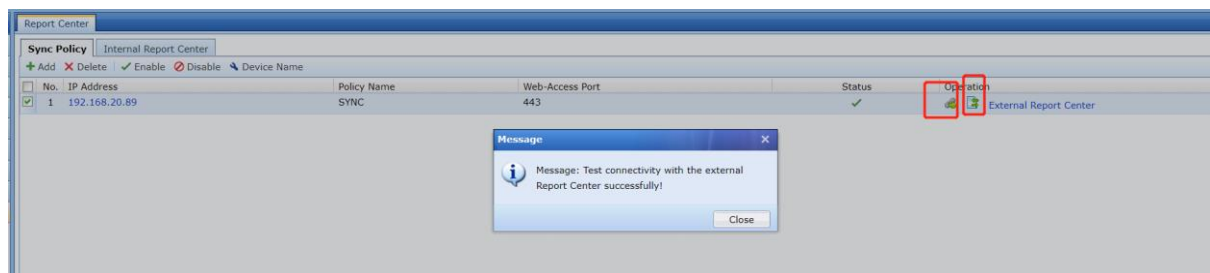


2. Enter the IP of the Windows Server, then select the synchronization policy, and select the corresponding synchronization strategy name and fill in the secret key.

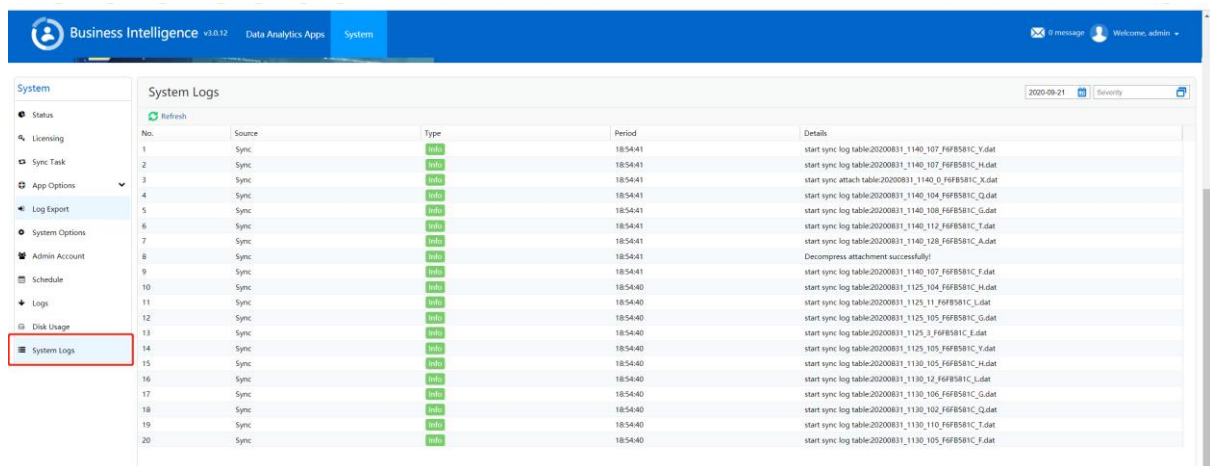
Sync Log to Report Center



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

Business Intelligence v1.0.12
Data Analytics Apps
System

0 message
Welcome, admin

Sangfor Business Intelligence
Be Aware of Online Behaviors
Dig for Data of More Values

System

- Status
- Licensing
- Sync Task
- App Options
- Log Export
- System Options
- Admin Account
- Schedule
- Logs
- Disk Usage
- System Logs

Status

Used: 19.65GB (3.93%)
Available: 480.00GB (96.07%)

Refresh

No.	Device Name	Last Sync	Sync Index To	Sync Intermediate Table To	Sync Data To	Server IP
1	IAM2088	2020-09-21 19:36	2020-08-16 02:08:00	2020-08-14 22:25	2020-09-21 17:20	192.168.20.88

Columns

- No.
- Device Name
- Last Sync
- Sync Index To
- Sync Intermediate Table To
- Sync Data To
- Server IP
- Gateway ID

Report Center
Dashboard
All Activities

Dashboard
Logs
Traffic Statistics
Internet Activities
Endpoints
Search
Reports

Time Taken: 6.91s
Period: 2016-08-30 00:00:00 to 2020-09-21 23:59:59 All Day
Action: Log,Reject,Alert

2016-08-30 00:00:00
All
Go
Options
Export

All Activities
Logs > All Activities

No.	Username	Group	Endpoint Device	App Category	Application	Action	Time	Details
1	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:17:09	
2	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:17:09	
3	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:57	
4	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:57	
5	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:45	
6	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:45	
7	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:33	
8	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:33	
9	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:18	
10	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:18	
11	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:06	
12	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:16:06	
13	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:15:54	
14	192.168.20.89	/	Unknown	Mail	Exchange MAPI	Log	2020-08-16 00:15:54	

W.: www.sangfor.com | W.: community.sangfor.com | E.: tech.support@sangfor.com

1



SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc