



**SANGFOR**



# IAM

## Best Practices for Scenarios\_Activity Domain ADSSO

**Version 12.0.42**



## Change Log

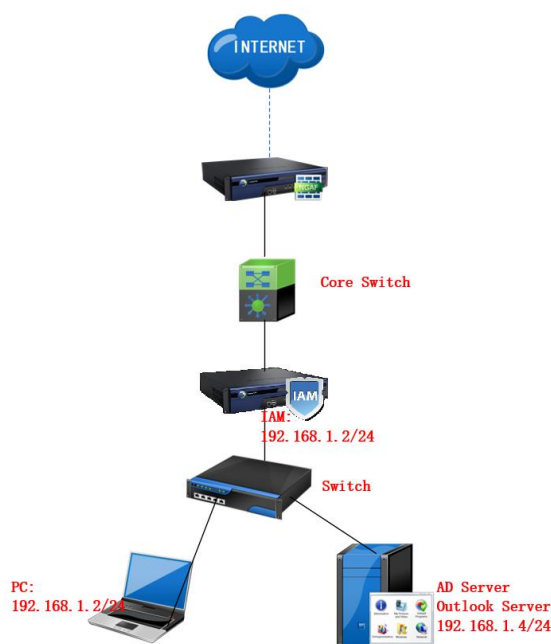
Date	Change Description
Aug 4, 2020	Version 12.0.42 document release.
May 17, 2021	Version 12.0.42 document update.

# CONTENT

Chapter 1 Scenario .....	1
1.1 Configure Steps.....	1
Chapter 2 How to Configure Activity Domain Server .....	2
2.1 Install MS AD function.....	2
2.2 Configure the domain controller server.....	9
2.3 Create usernames and passwords for other users in the domain.....	14
2.4 Join the PC to the domain.....	18
2.5 Enable the log audit function of AD Server .....	24
Chapter 3 How to Configure IAM.....	27
3.1 Add LDAP server .....	27
3.2 Configure SSO authentication options.....	28
3.3 Configure authentication policy on IAM.....	29
Chapter 4 Precautions .....	30

## Chapter 1 Scenario

A customer uses a Microsoft AD server to manage intranet users. All end users are Windows systems. The client's office applications are mainly applications from Microsoft companies such as Outlook; the customer wants to control intranet users and requires visualization of control, that is, a specific domain can be queried. The user's online behavior and traffic information also perform identity verification for intranet users. Integrating all customer needs, and at the same time, the customer uses the Microsoft AD domain to manage users. Among the several ways of combining Microsoft AD domain authentication, the script SSO has the highest success rate, but the customer does not allow to deliver scripts through the Microsoft AD domain, so we can choose ADSSO method.



AD Server:

IP: 192.168.1.4

Domain Name: sangfor.com

Account/Password: administrator/@sangfor123

Test PC:

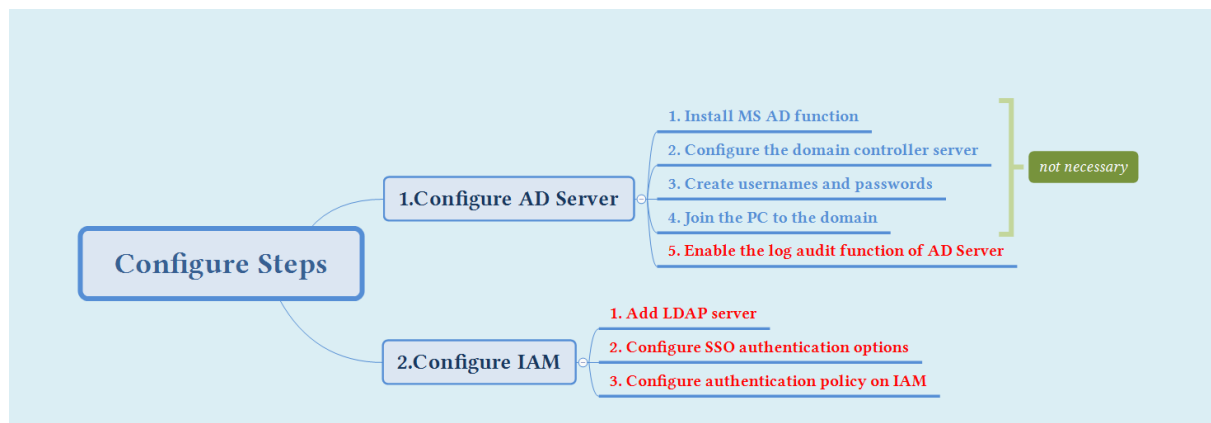
IP: 192.168.1.3

Account/Password: administrator/@sangfor123

Domain Account/Password: sangfortest/@sangfor123

### 1.1 Configure Steps

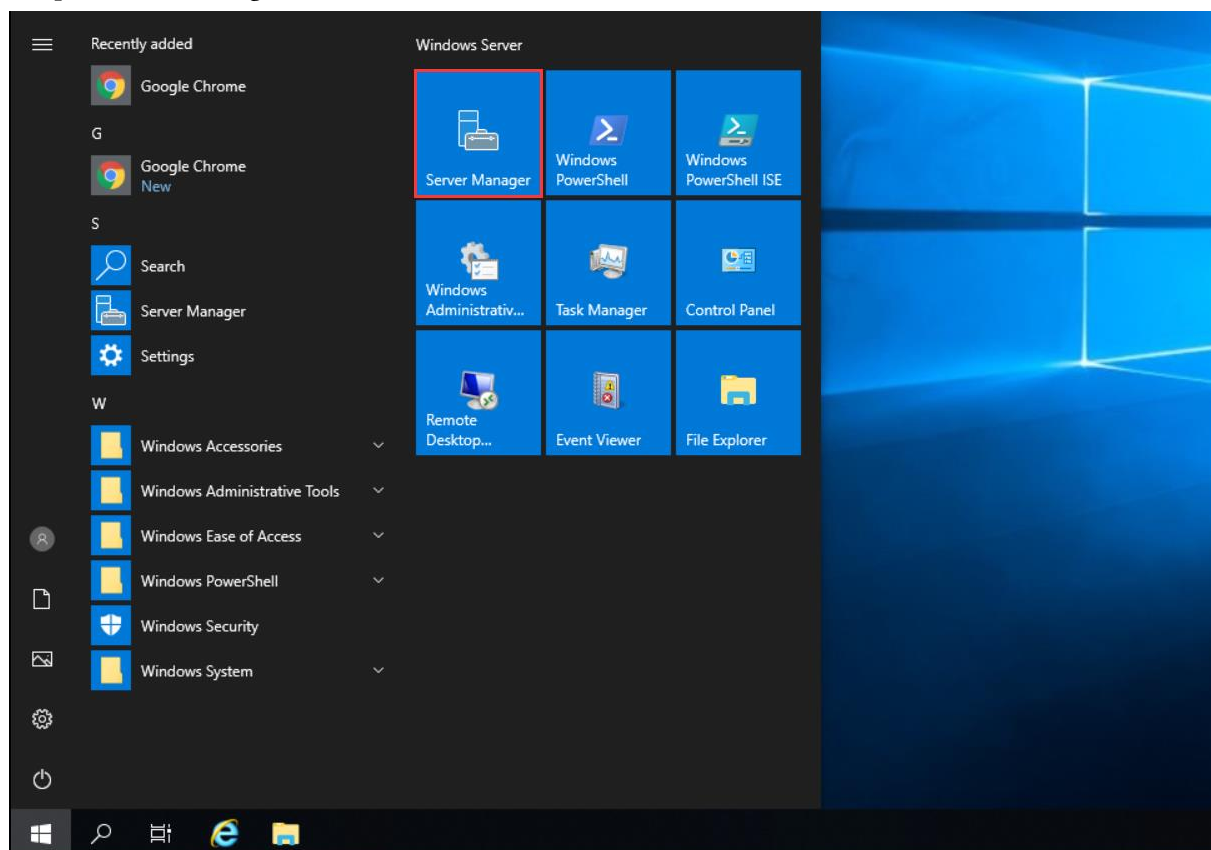
The configuration steps are as shown in the figure below. It should be noted that in order to make everyone familiar with the AD domain faster, we add the method of configuring the AD domain, which is the part marked "not necessary". If the customer has used the AD domain before and does not need to reconfigure the AD domain, then only need to configure other parts.



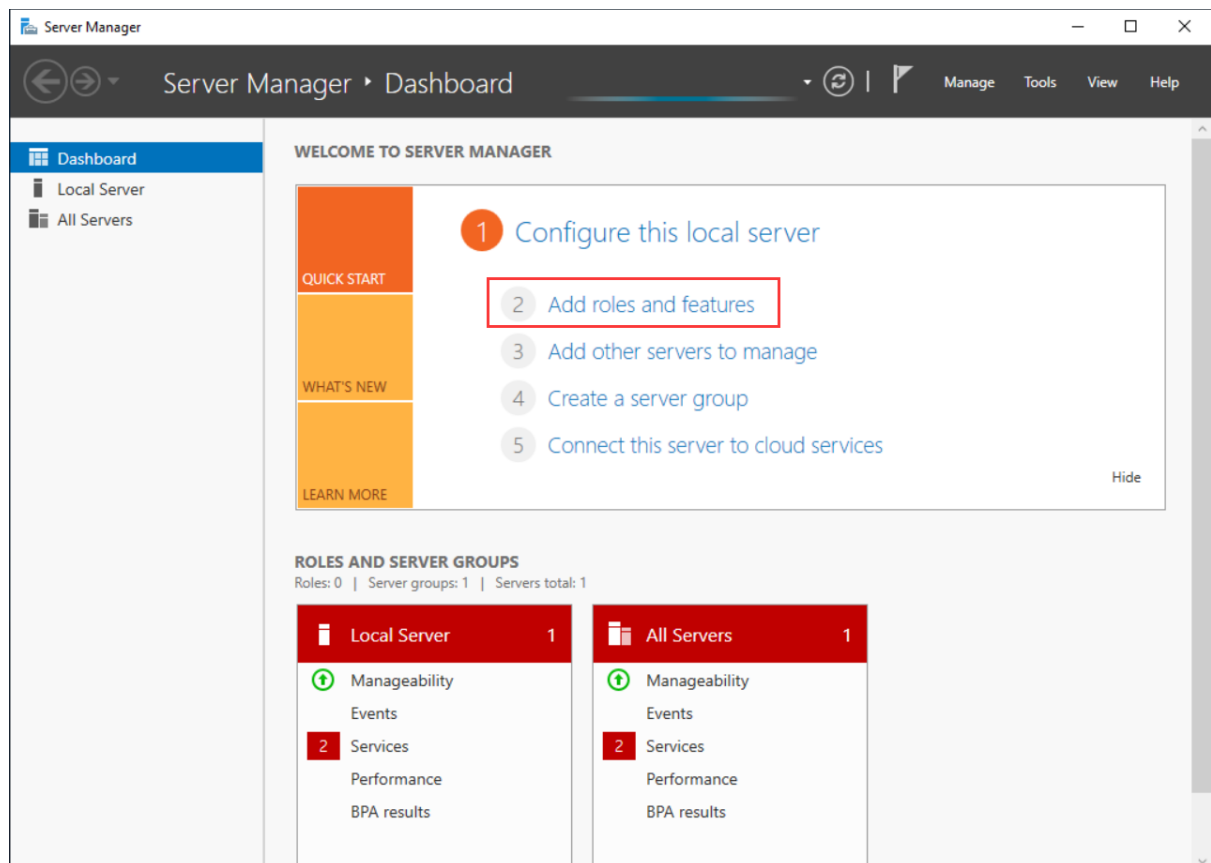
## Chapter 2 How to Configure Activity Domain Server

### 2.1 Install MS AD function

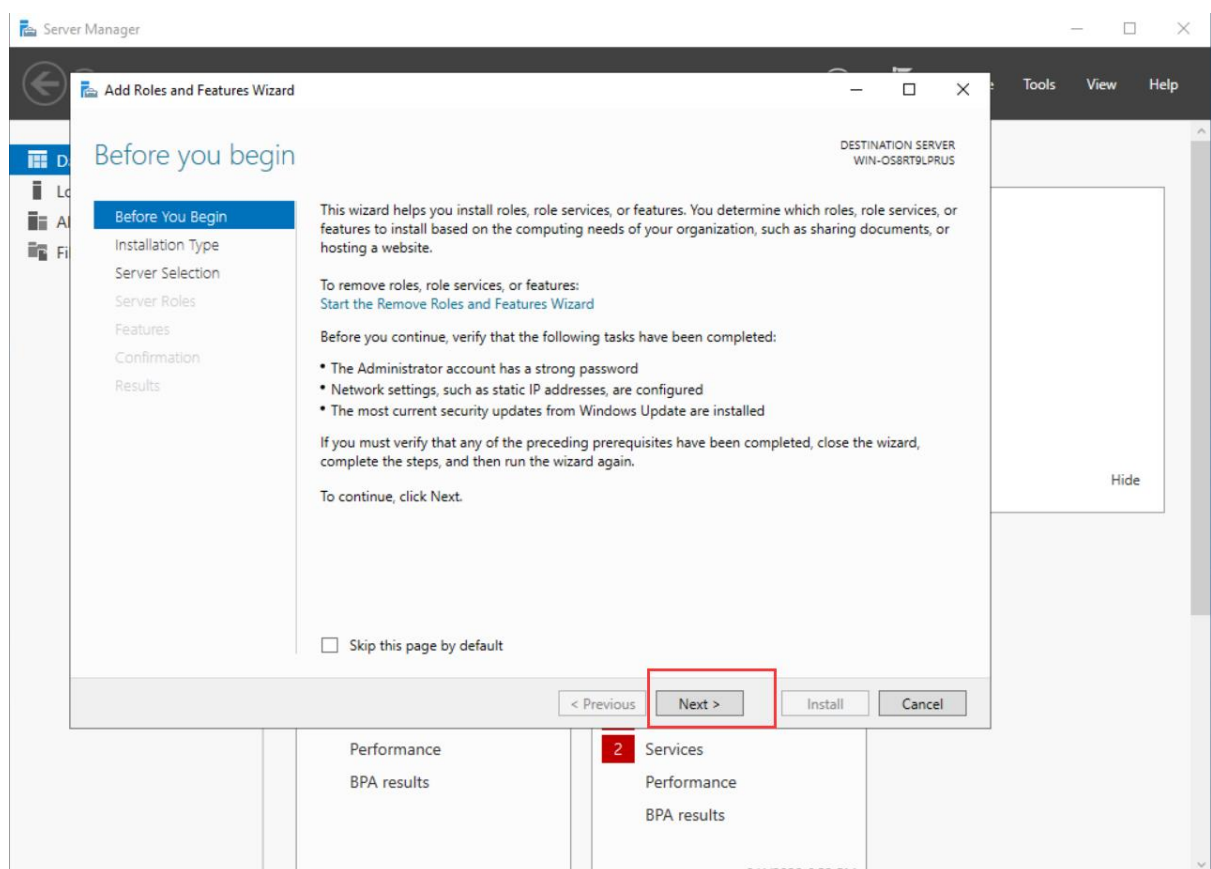
1. Open Server Manager in Windows Server 2019.



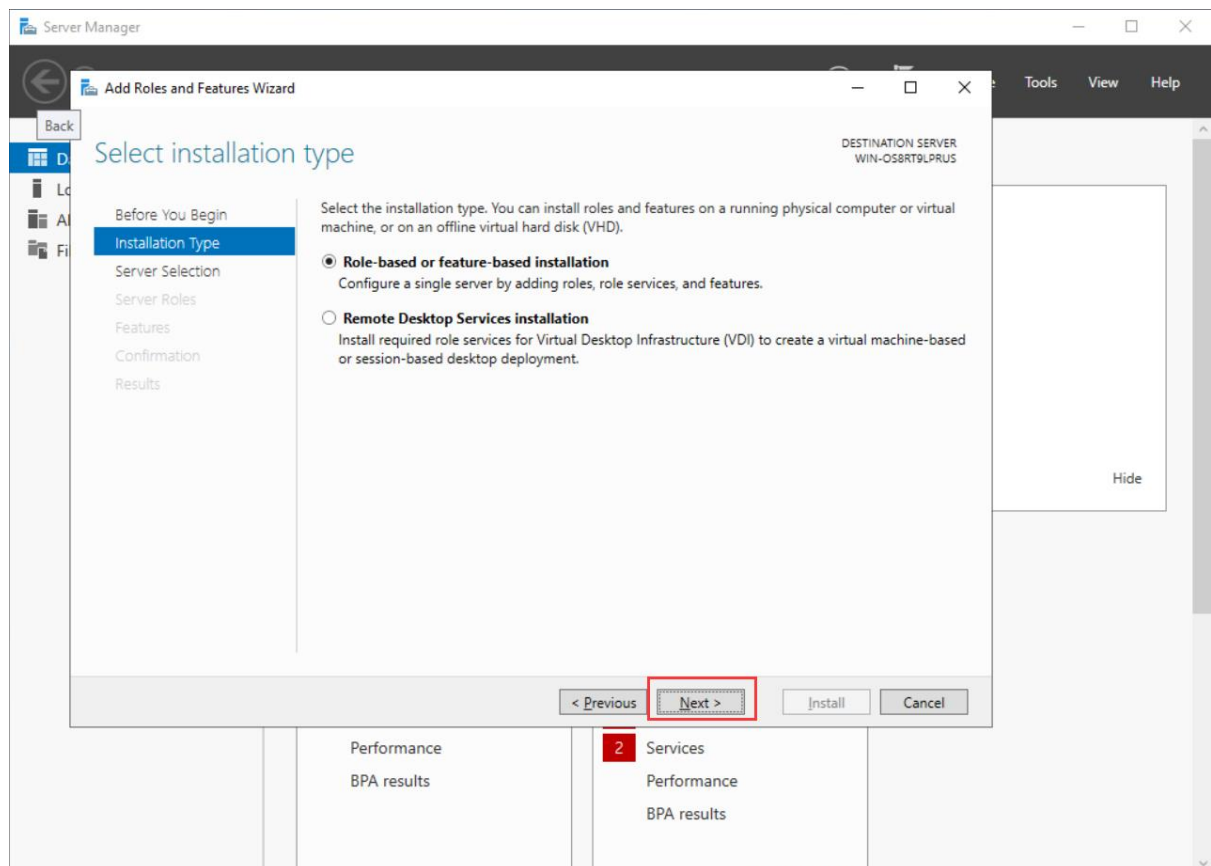
2. Click "Add roles and features".



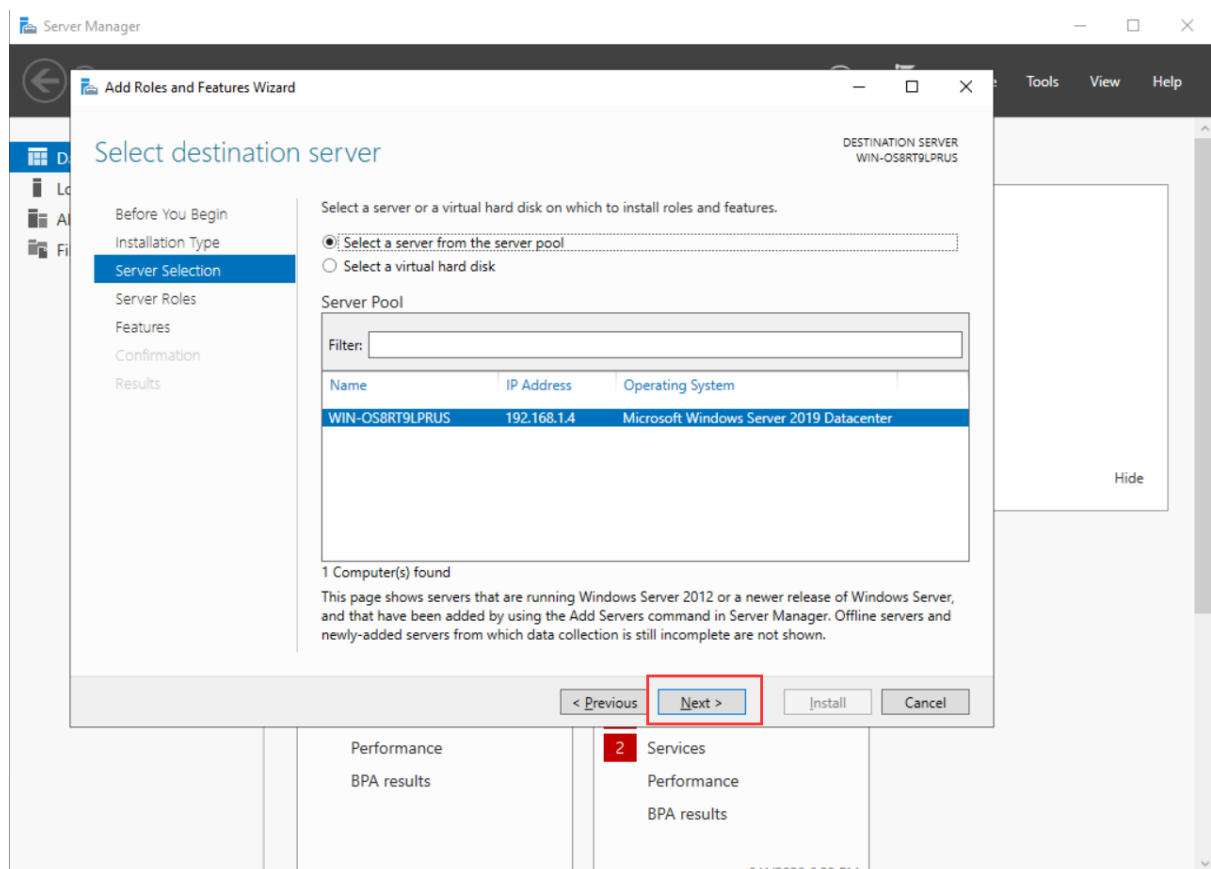
3. Click "Next".



4. Click "Next".

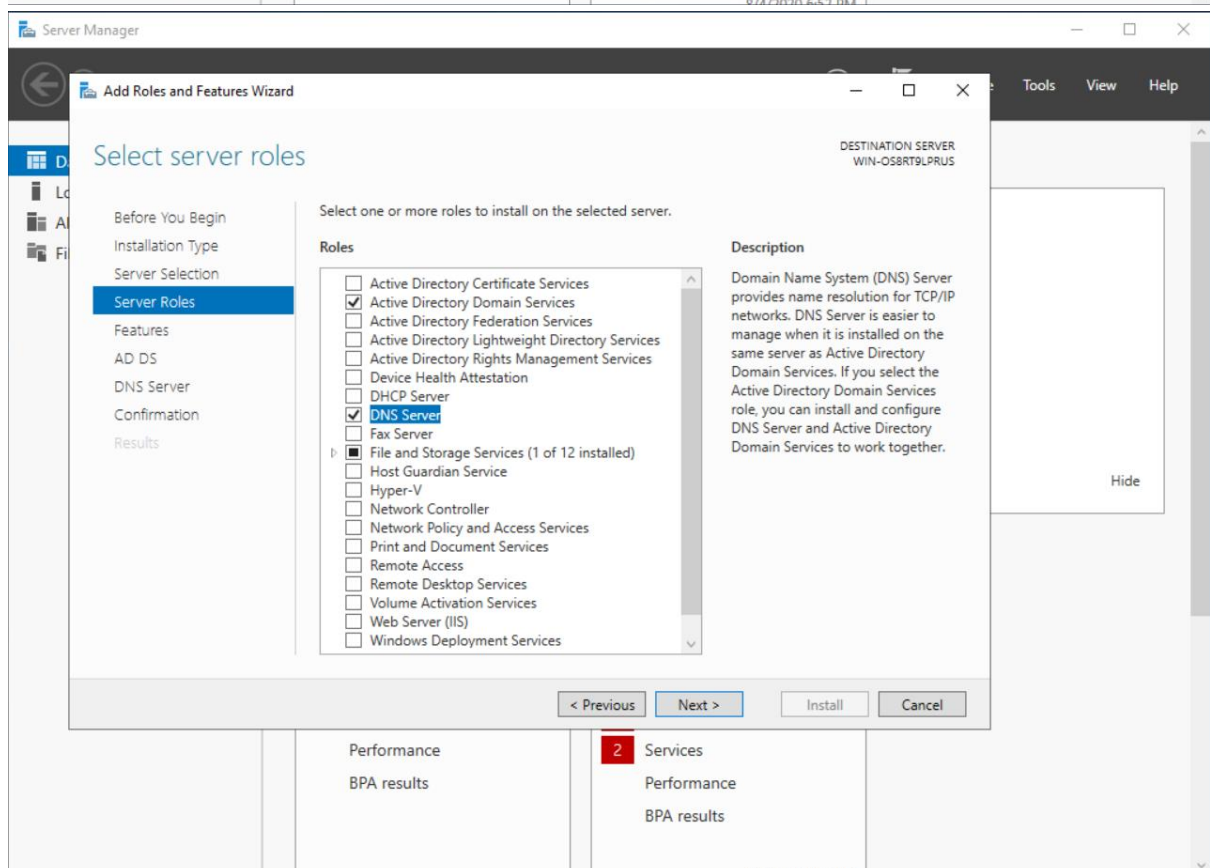
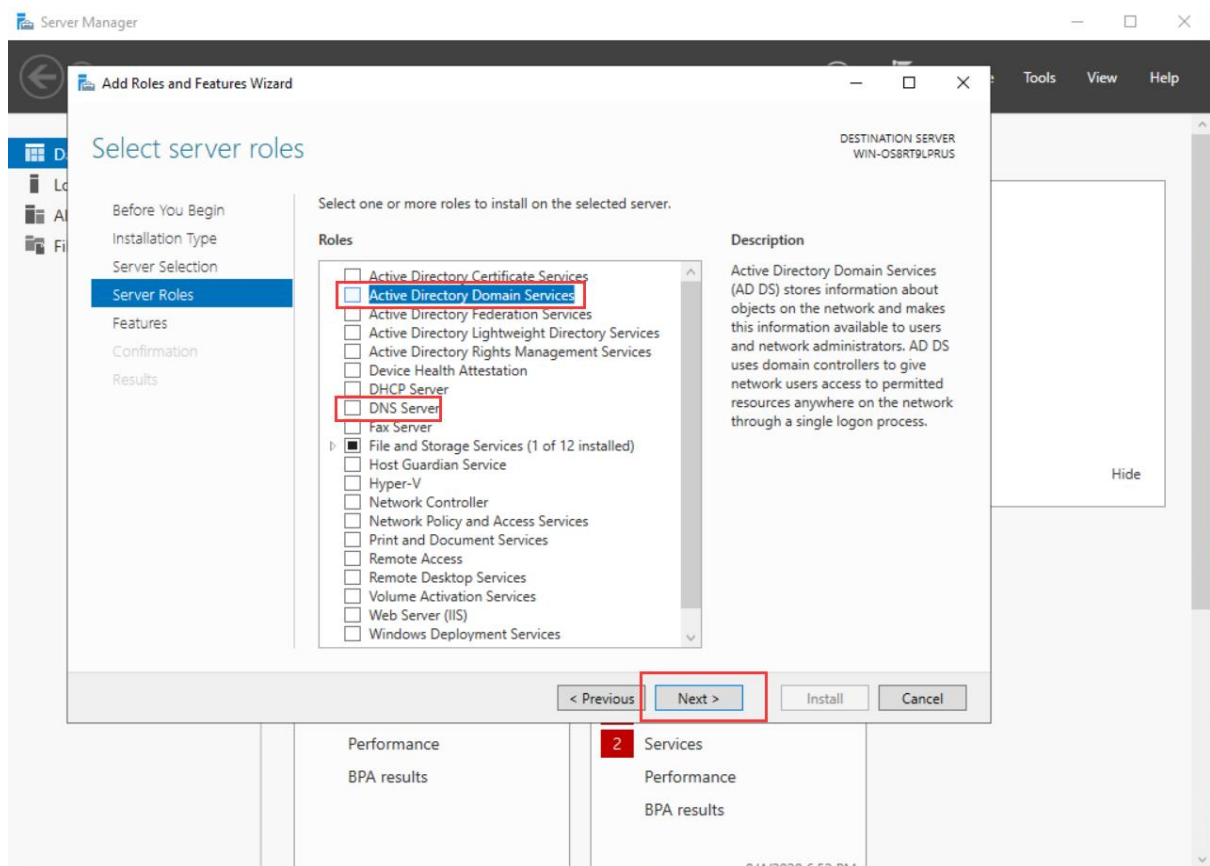


5. Click "Next".



6. Select the functions that need to be installed "Active Directory Domain Services" and "DNS Server", then click "Next".

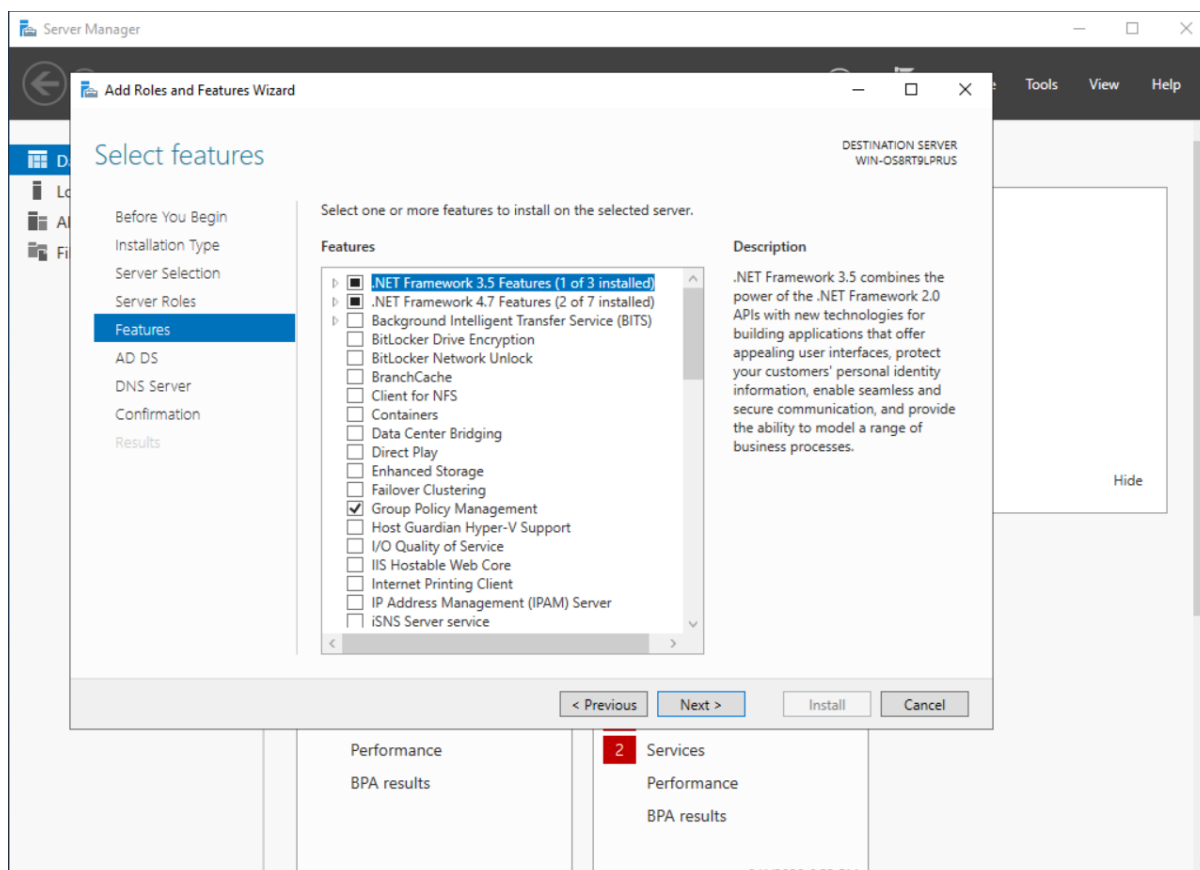
## Activity Domain ADSSO



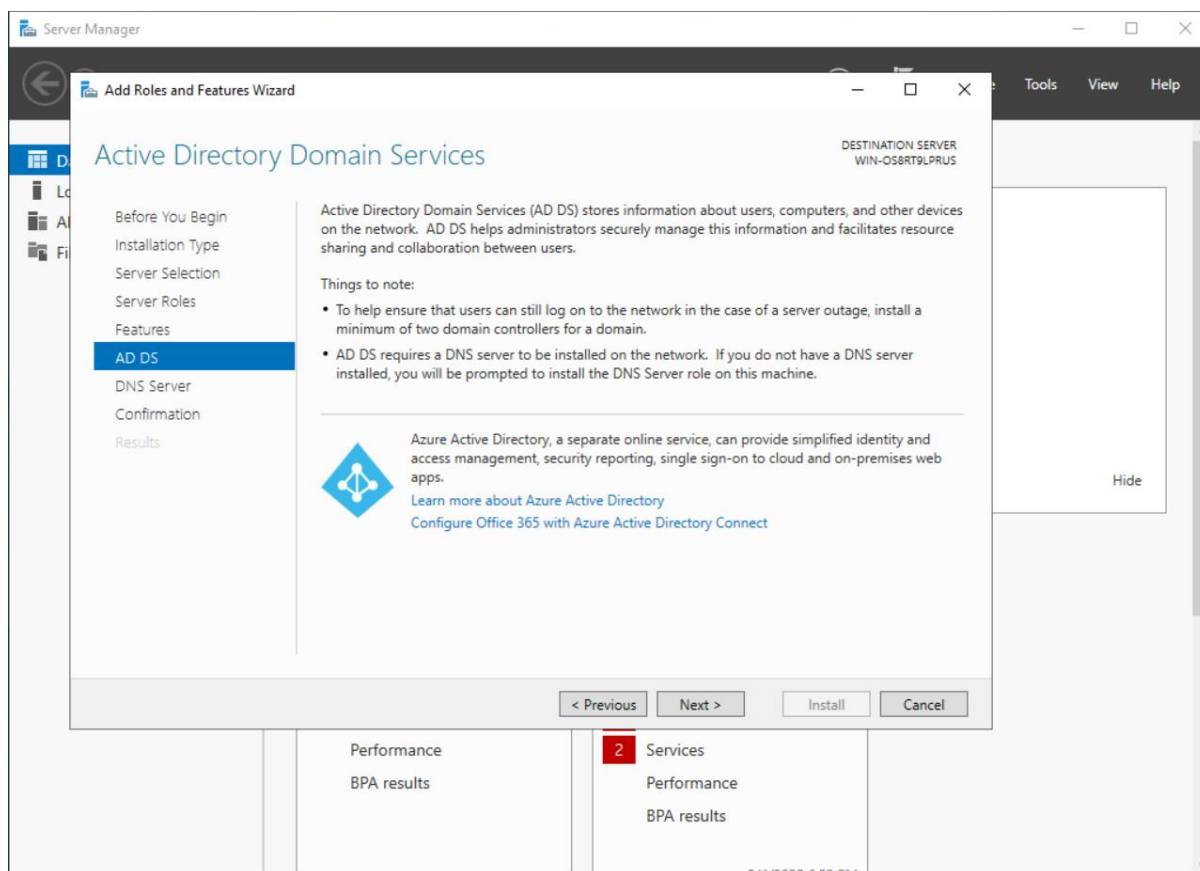
7. Click "Next".



## Activity Domain ADSSO

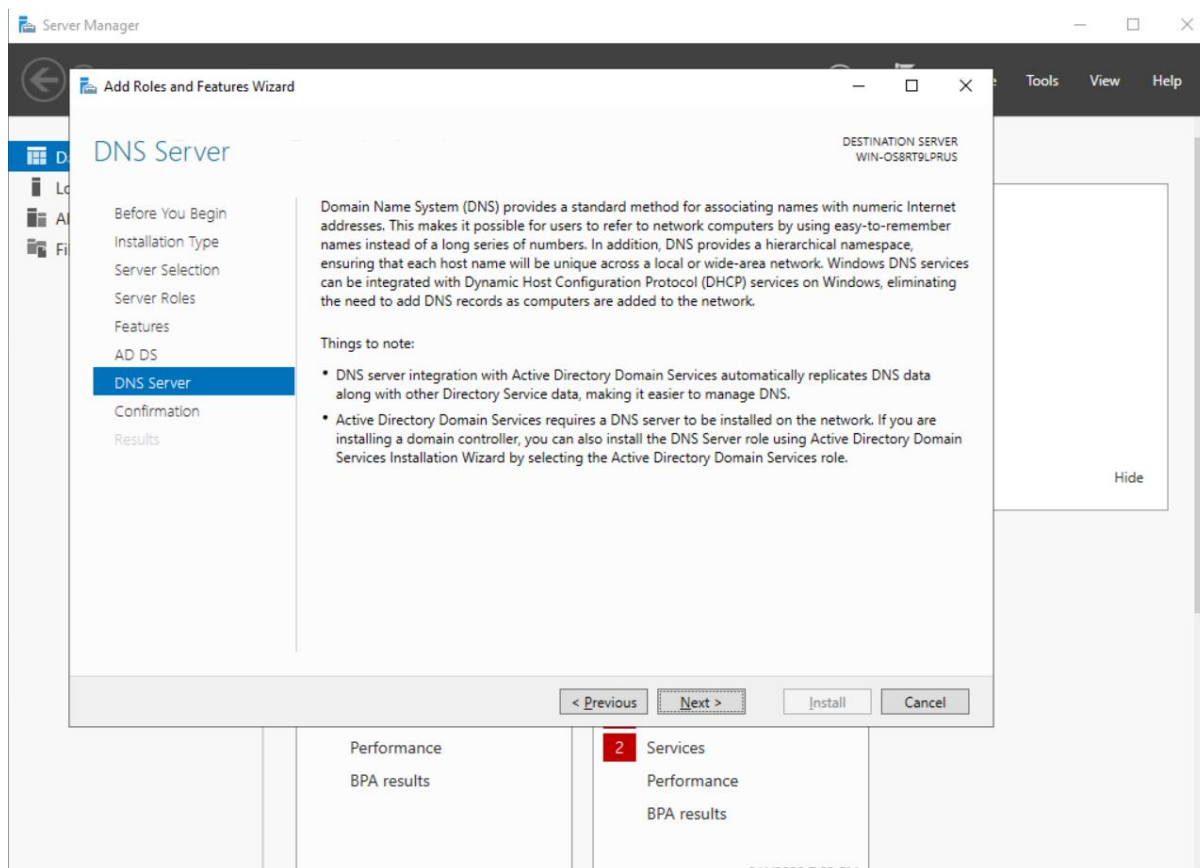


8. Click "Next".

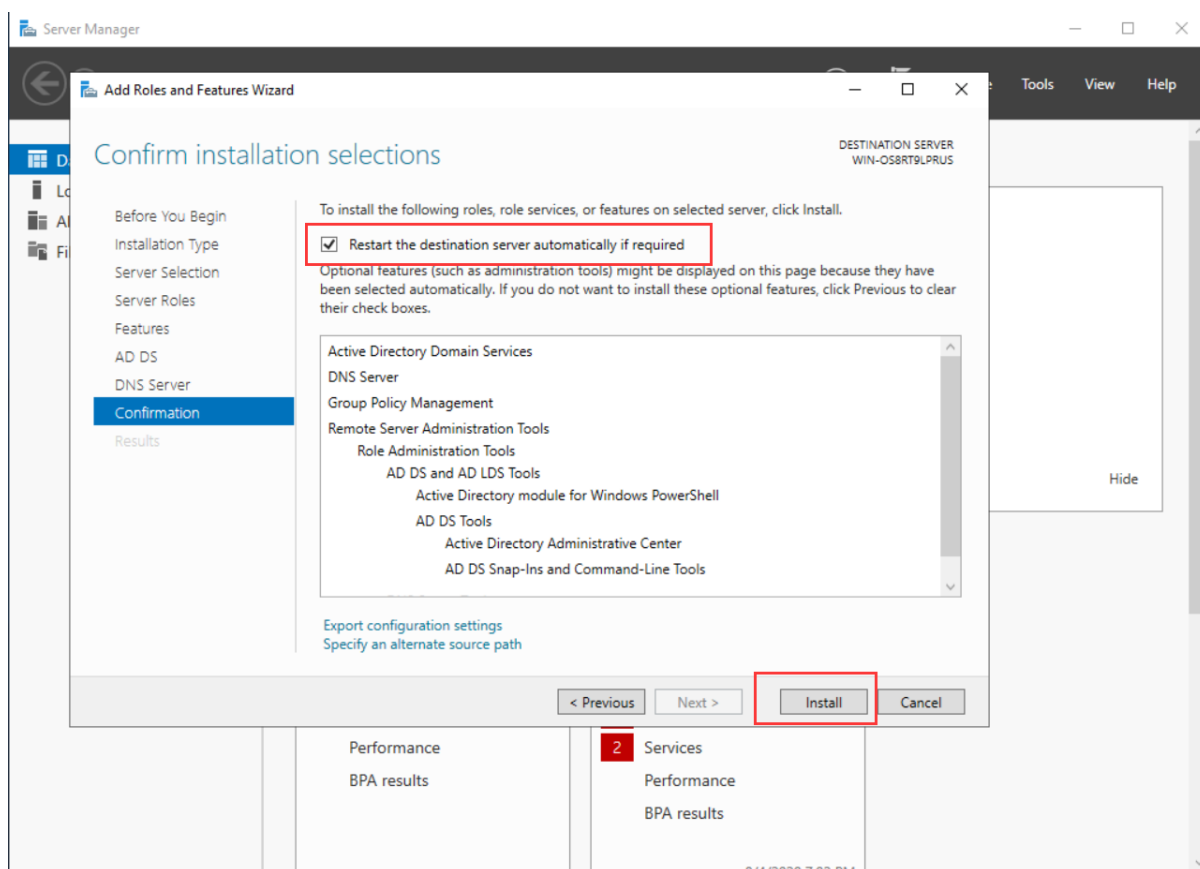


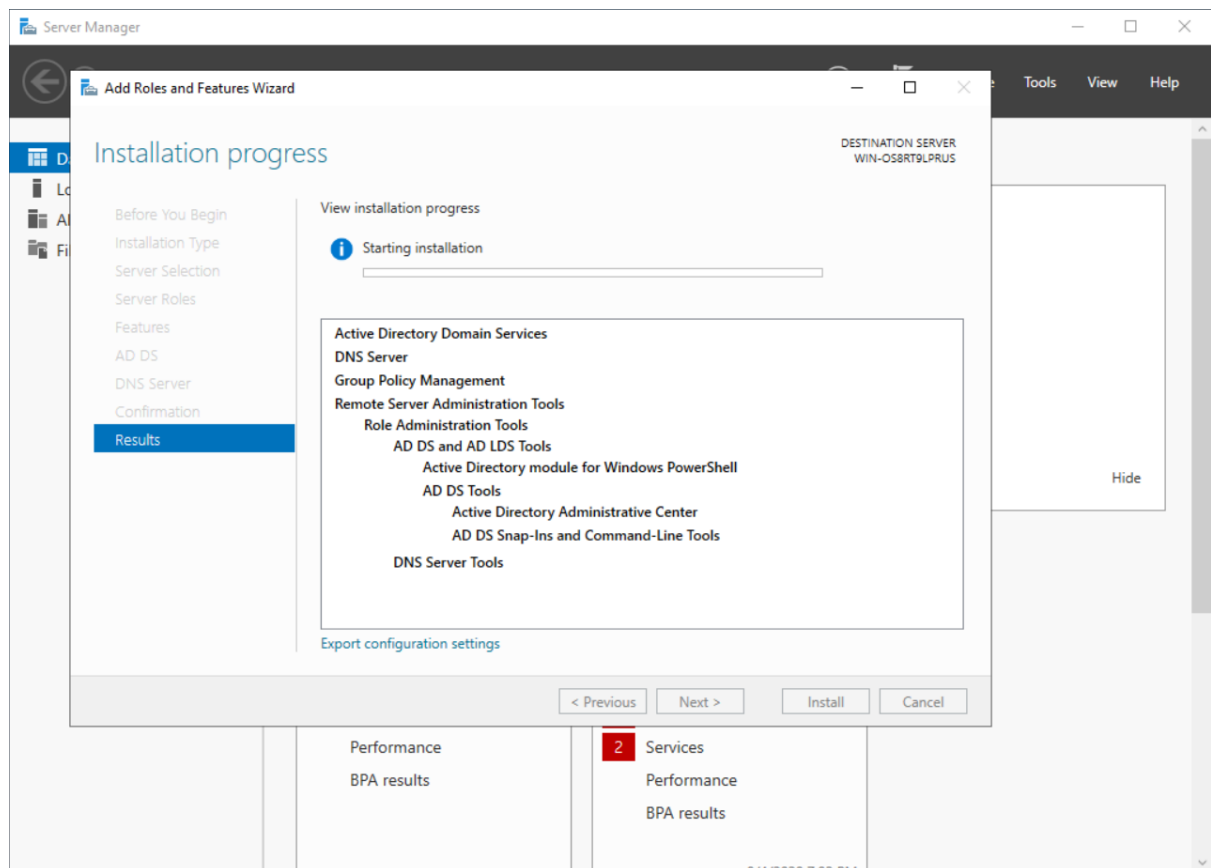
9. Click "Next".

## Activity Domain ADSSO

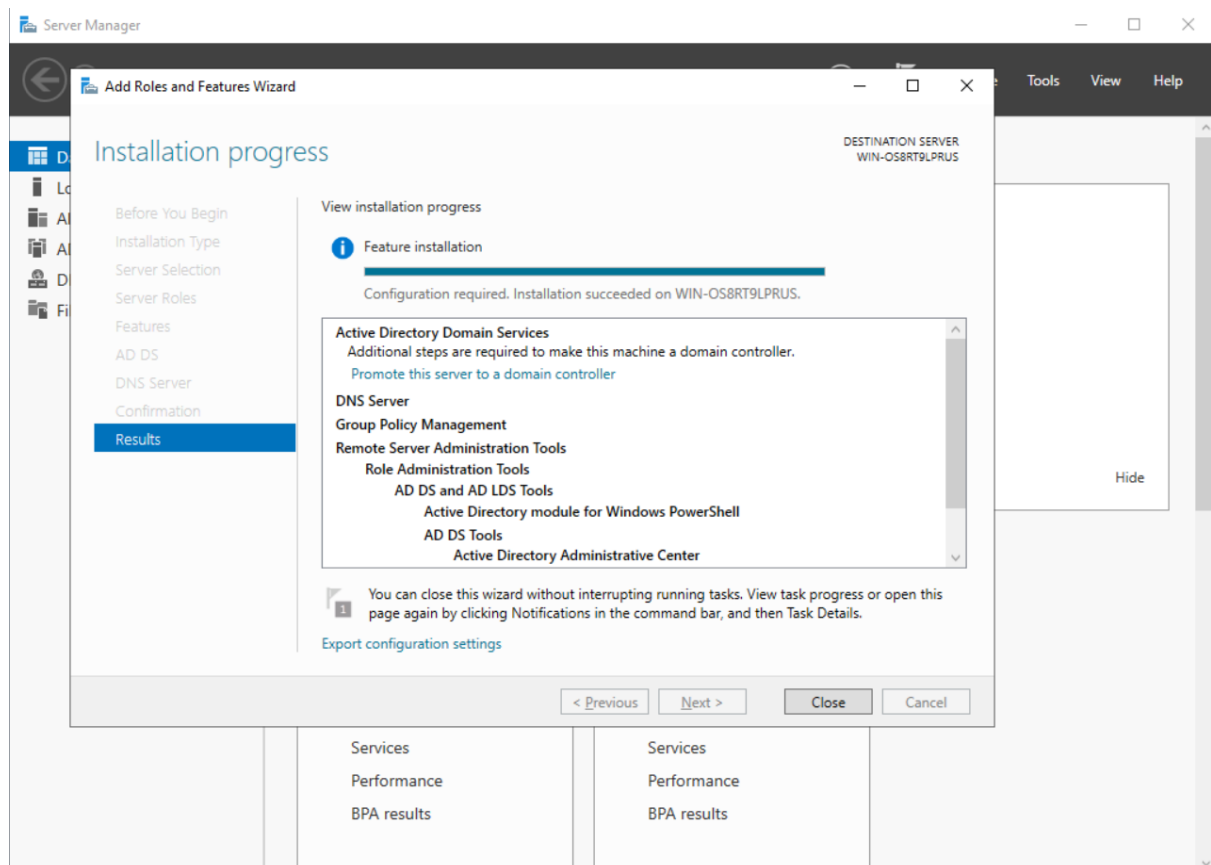


10. Click "Install".



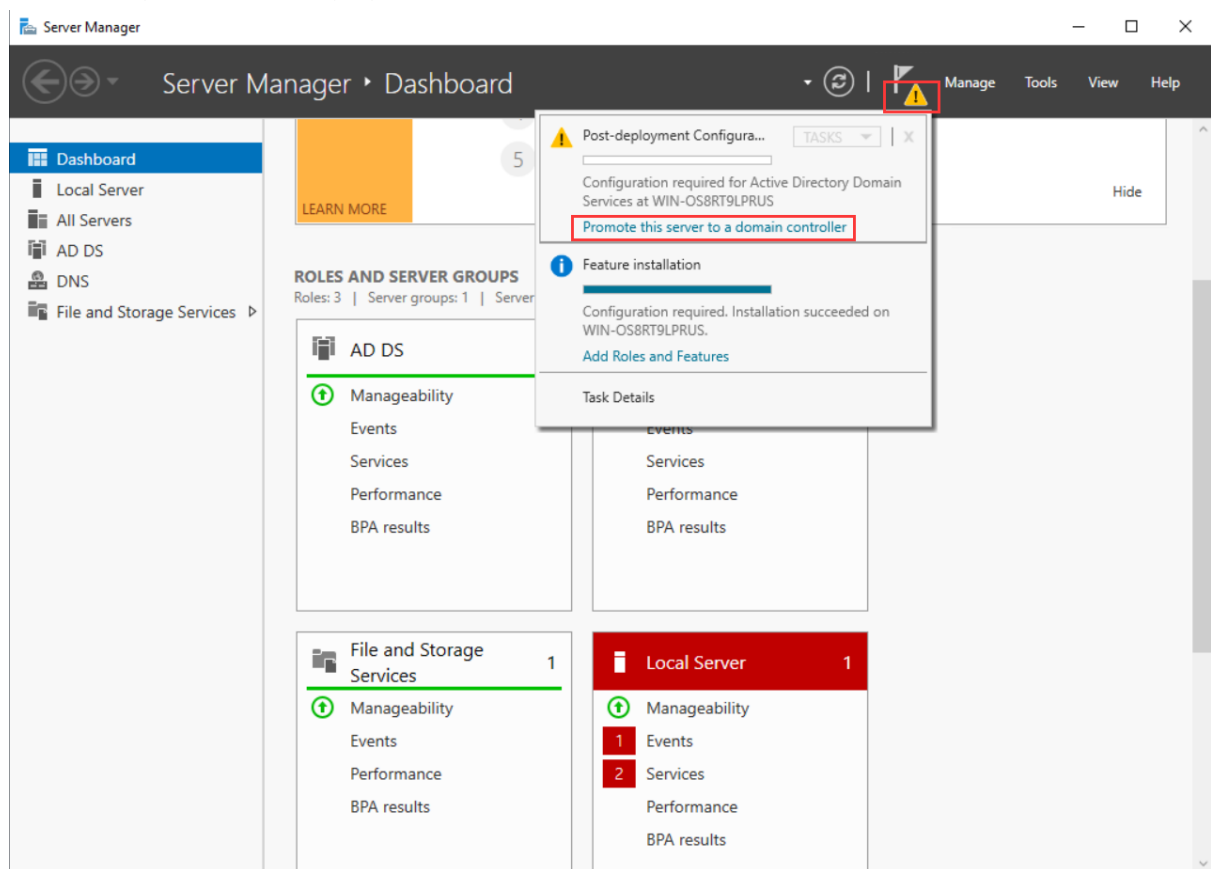


11. Click "Close" after installation.



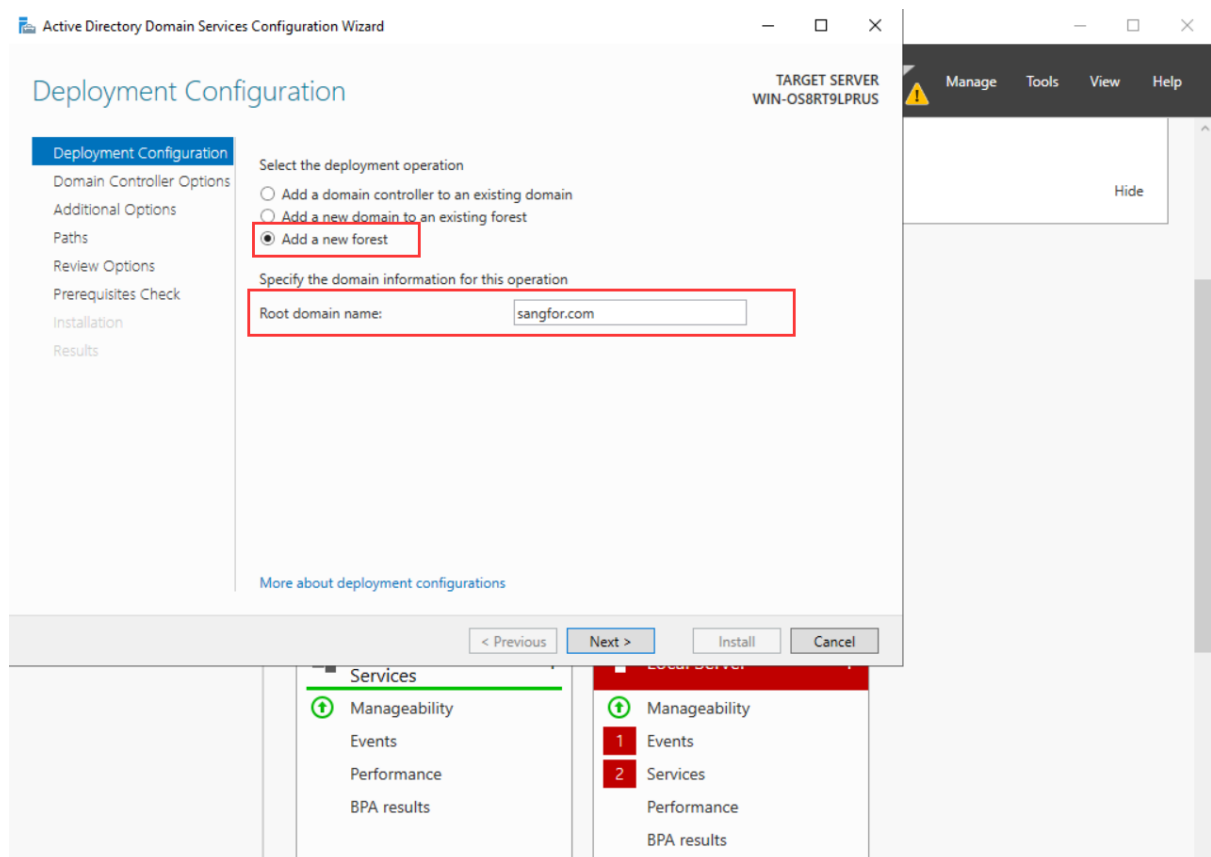
## 2.2 Configure the domain controller server

1. According to the following figure, select "Promote this server to a domain controller".

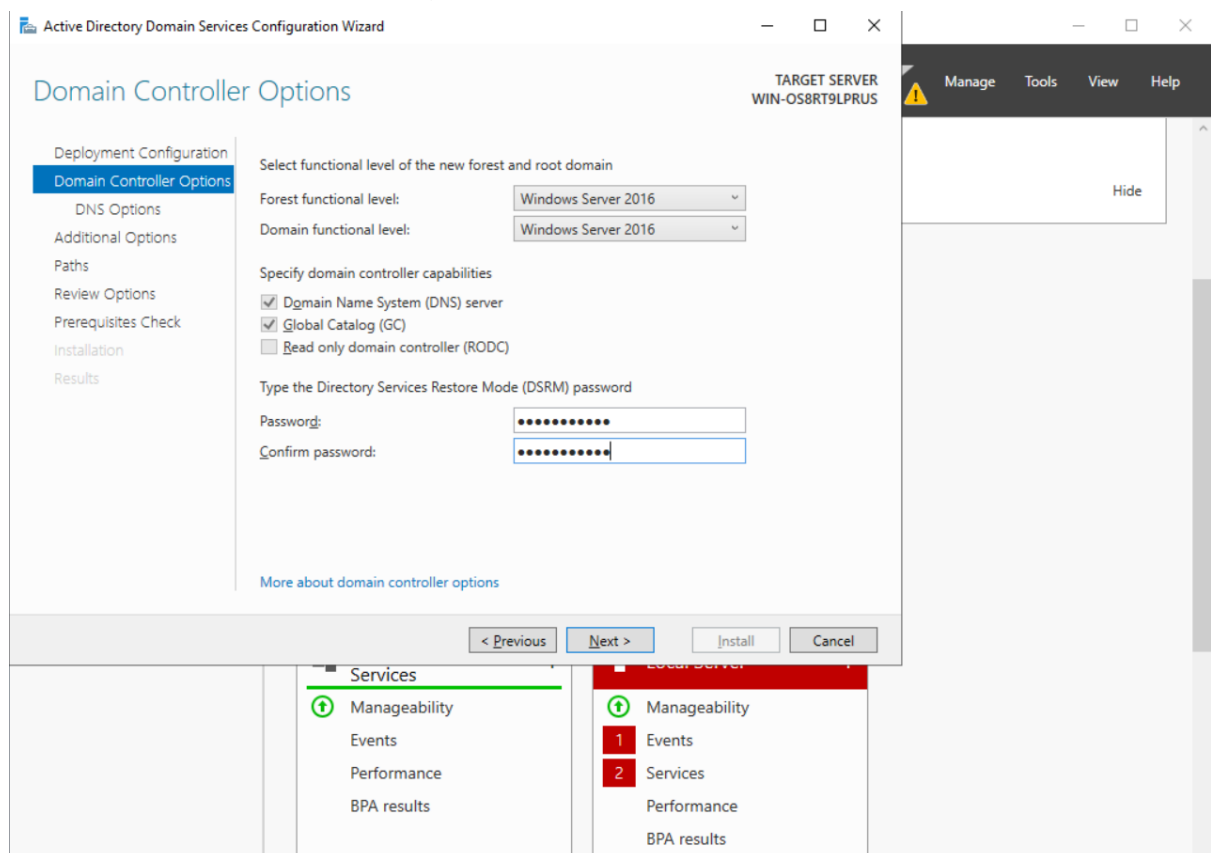


2. Configure the domain name for the AD domain, such as sangfor.com.

## Activity Domain ADSSO

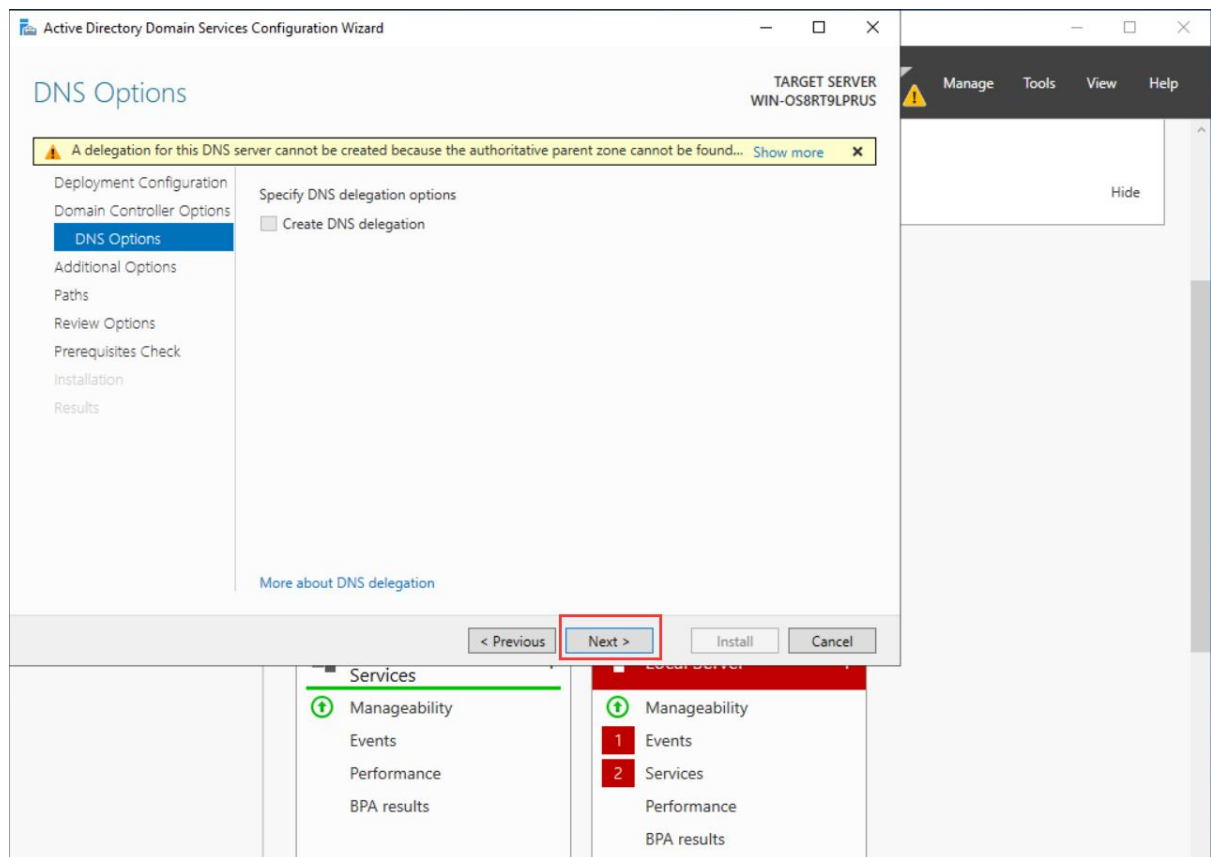


3. Set a password, for example @sangfortest.

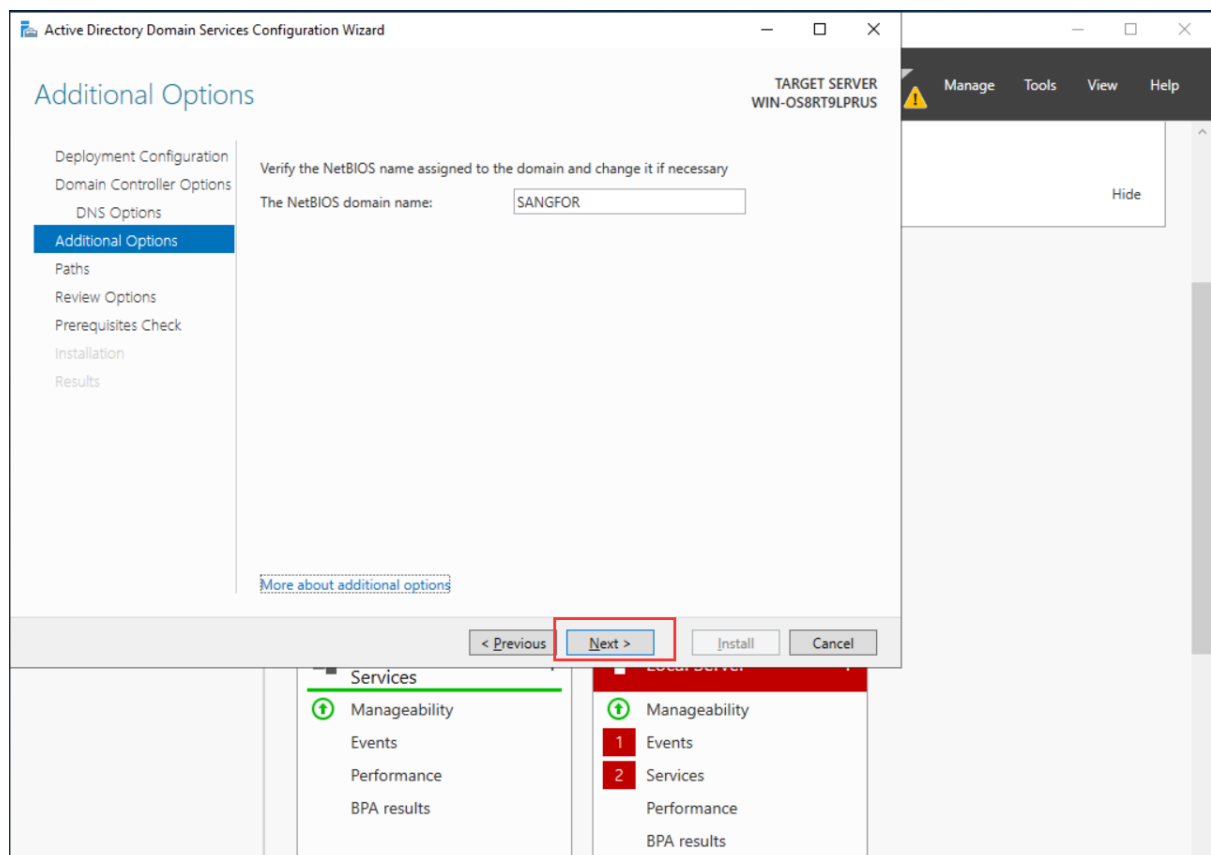


4. Click "Next".

## Activity Domain ADSSO

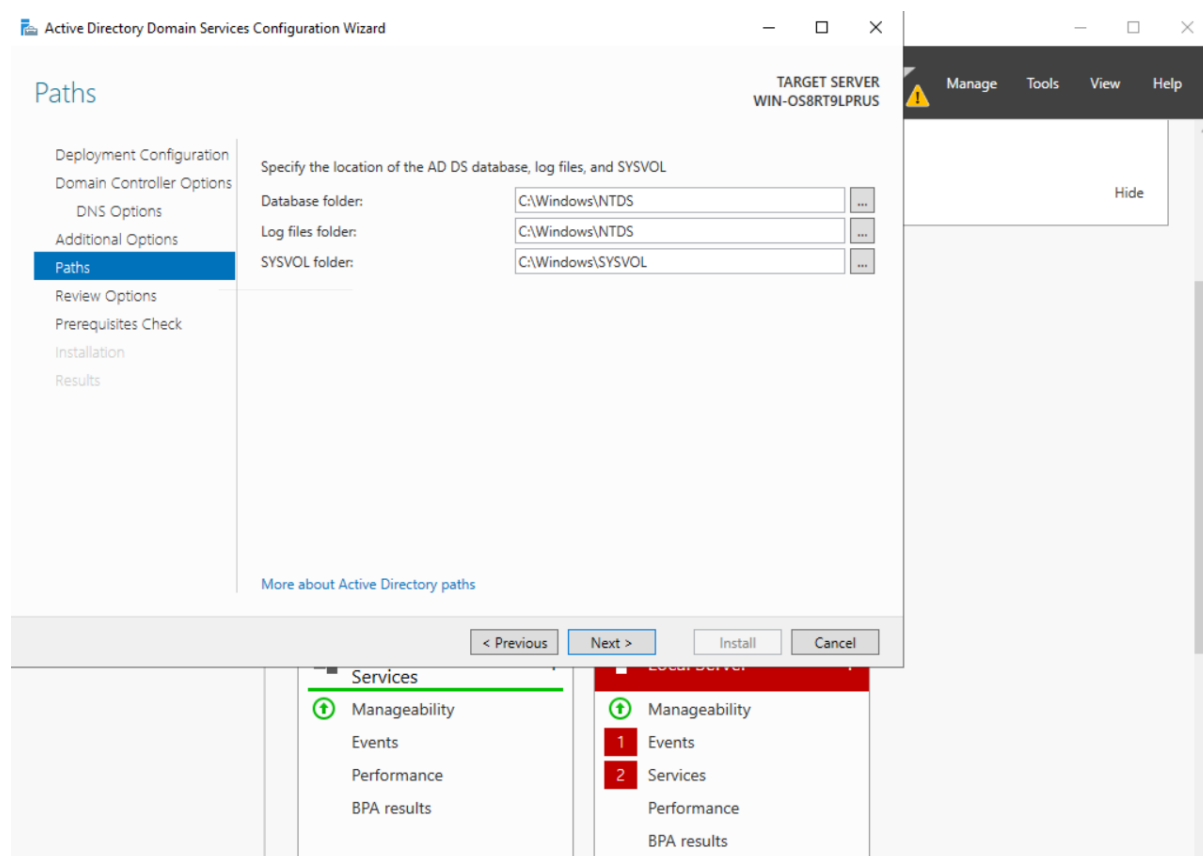


5. Set NETBIOS Domain Name, you can use the default SANGFOR.

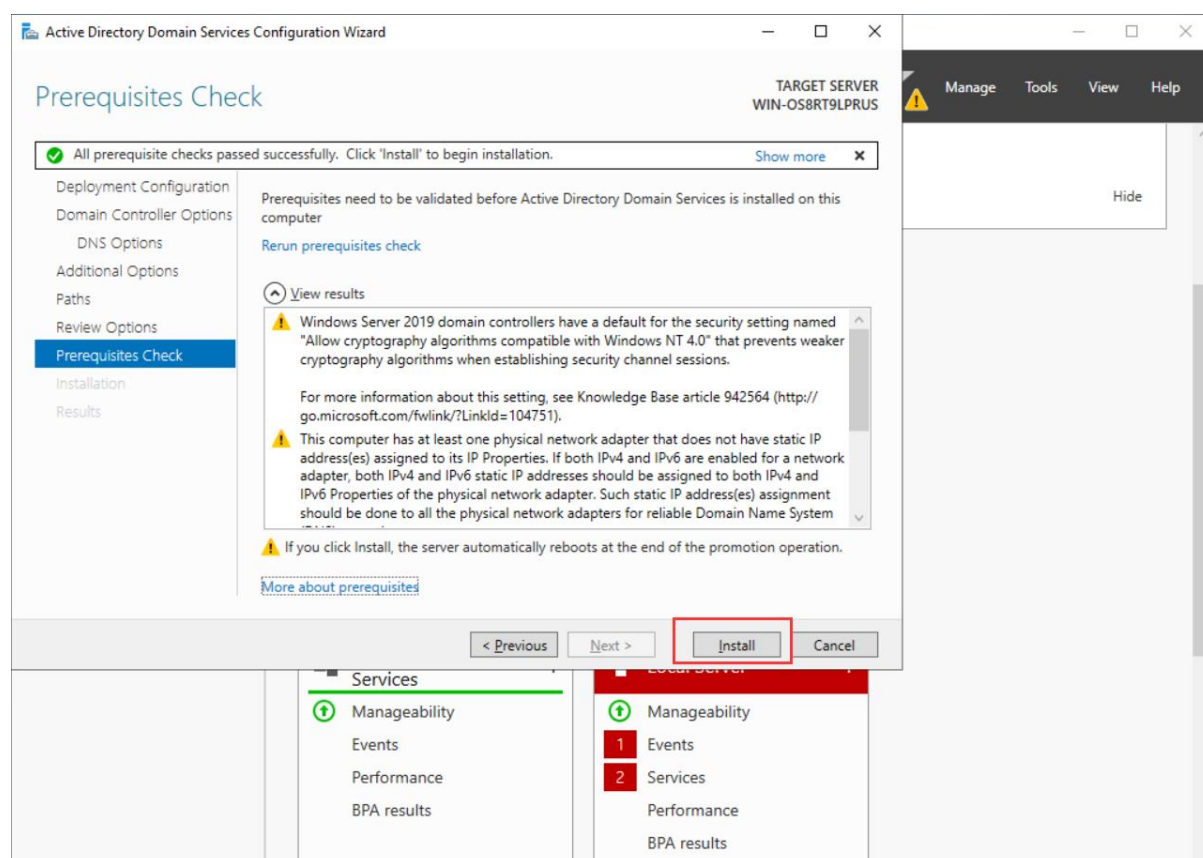


6. Click "Next".

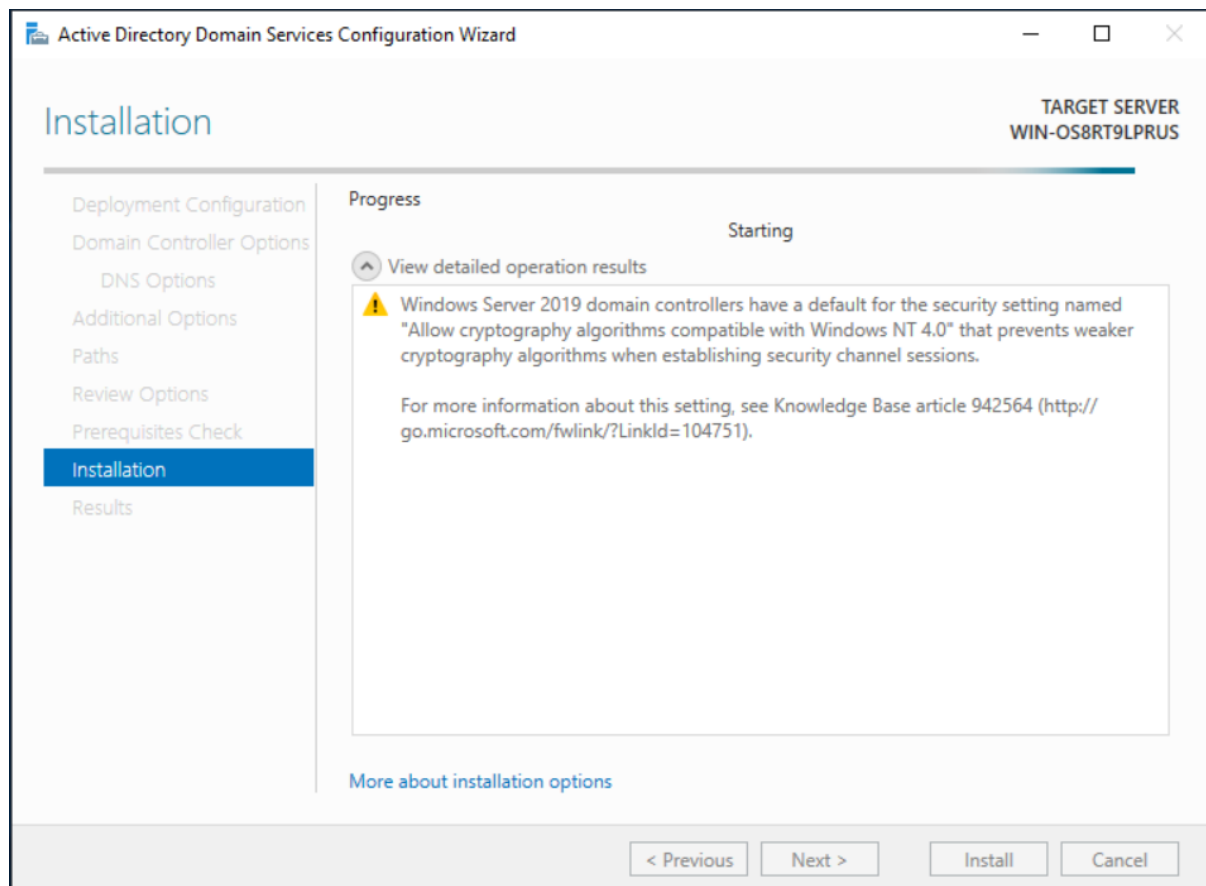
## Activity Domain ADSSO



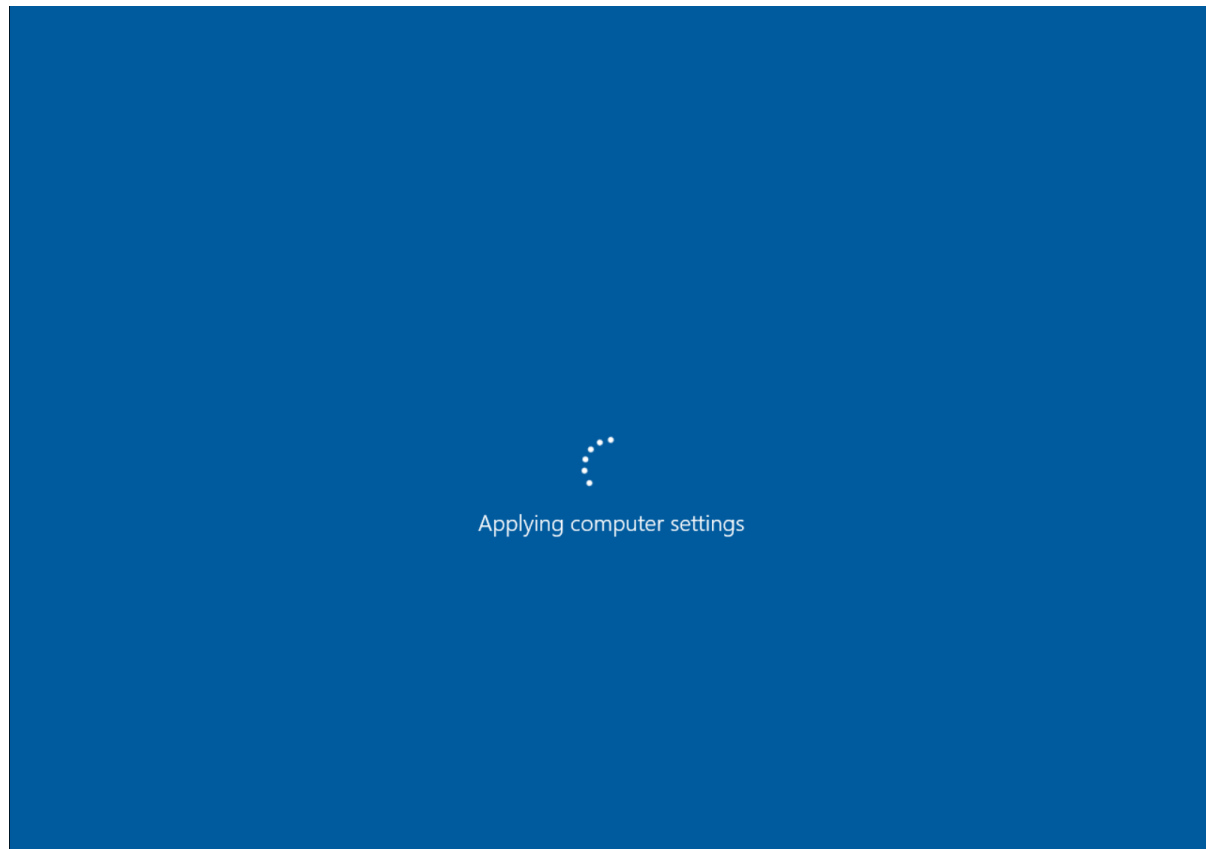
7. Select "Install".



8. Wait for the equipment to install and deploy related functions.



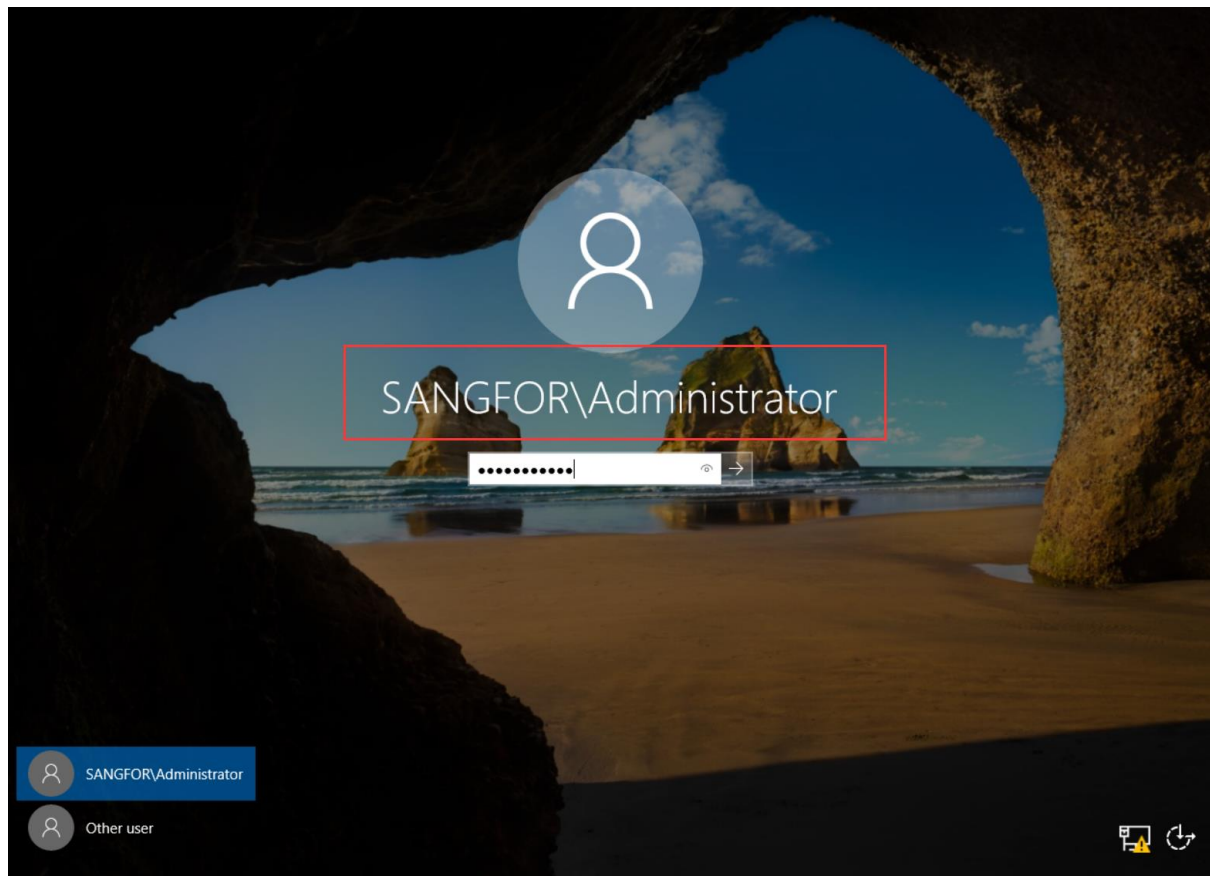
9. After the installation is complete, Windows Server will automatically restart.



10. After the Windows Server restarts, you can see on the login page that the default local administrator

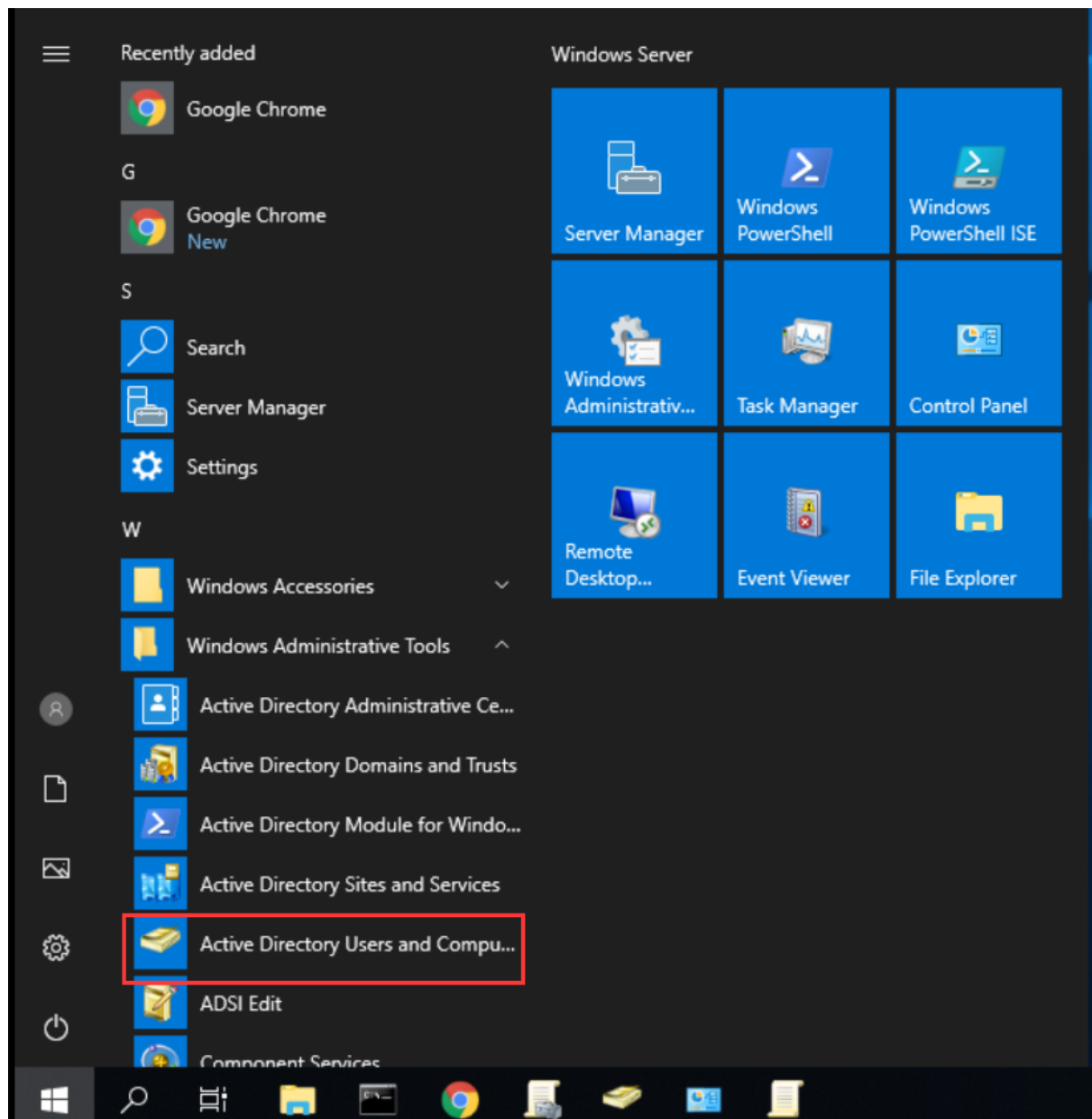


administrator who logs in to the operating system has become the administrator administrator in the domain, and the login password is the same as the password of the local administrator account.



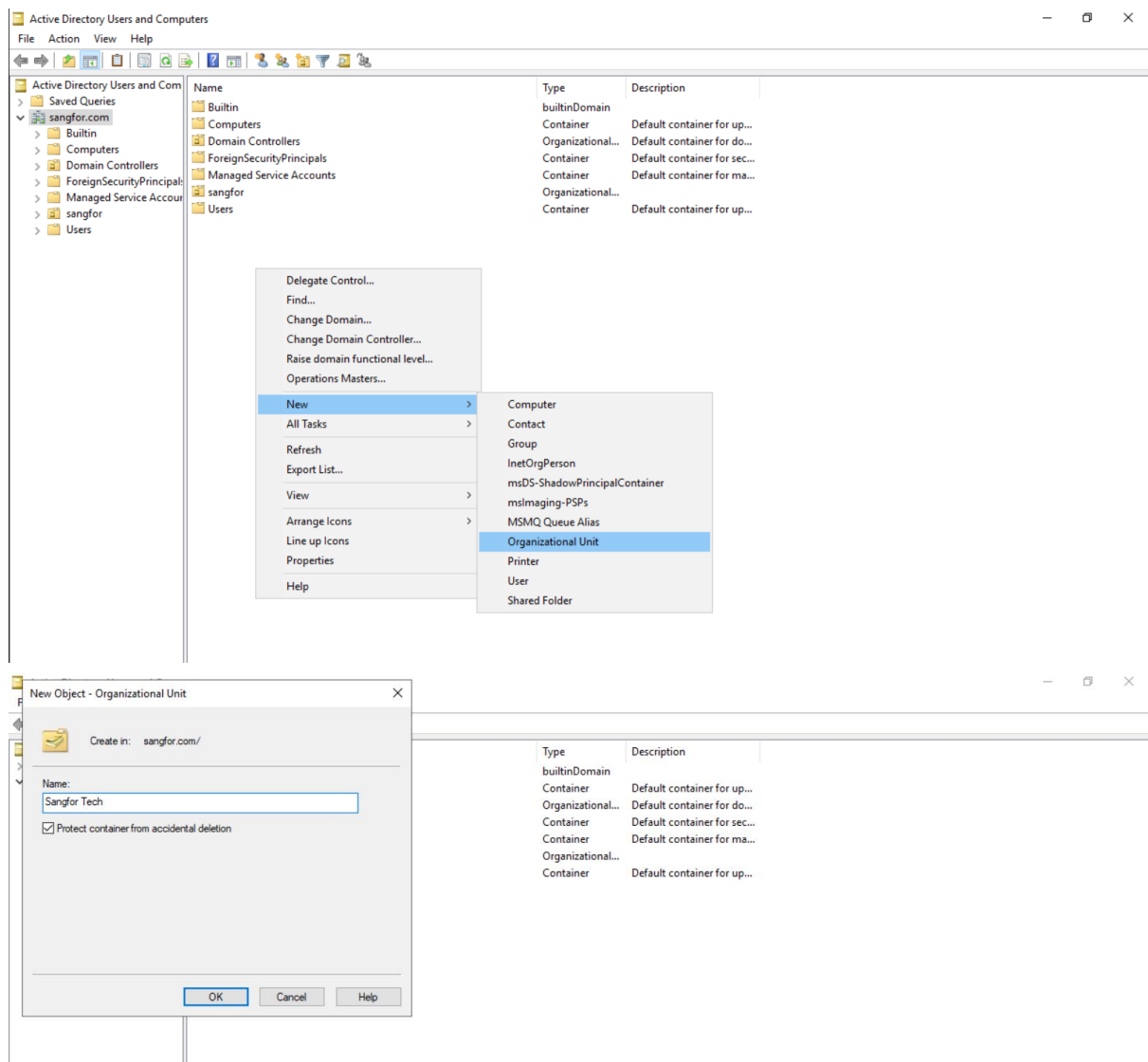
## 2.3 Create usernames and passwords for other users in the domain

1.Open "Active Directory Users and Computers".

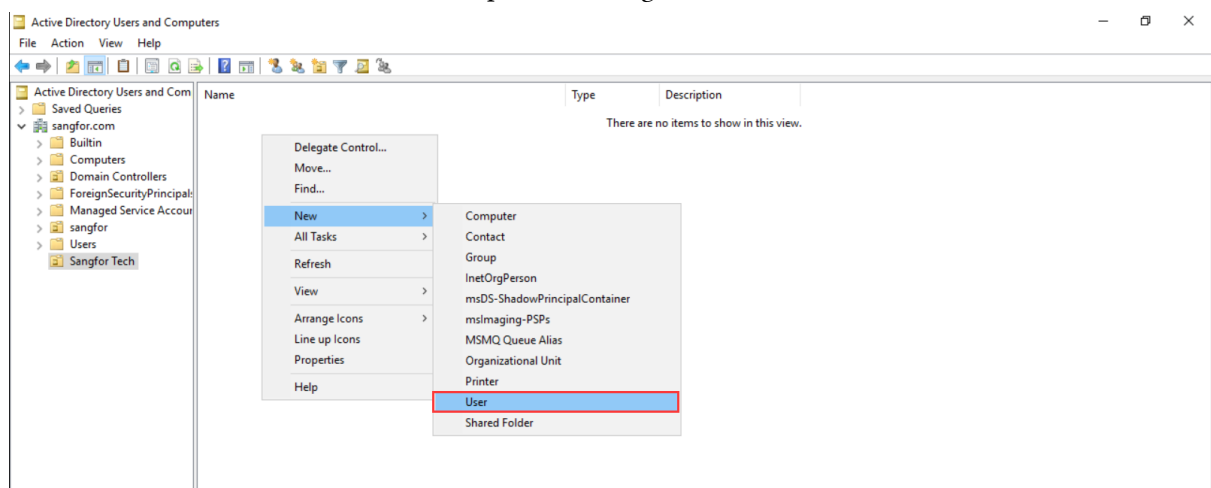


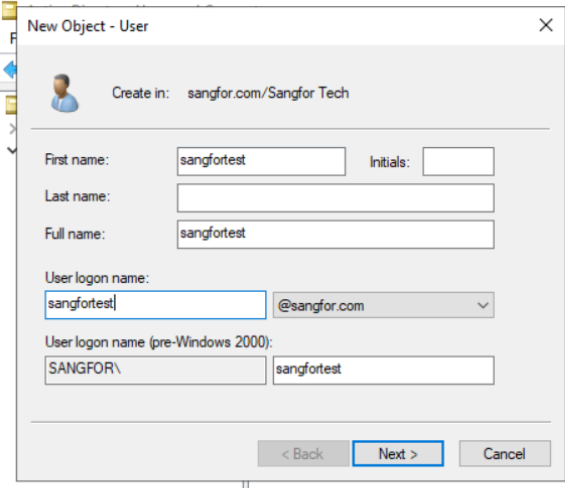
2. In order to facilitate the management of users according to the company's organizational structure, a logical container is created here to represent a department. For example, create a department called Sangfor Tech.

## Activity Domain ADSSO



3. Create a user in the container, for example called sangfortest.





New Object - User

Create in: sangfor.com/Sangfor Tech

First name: sangfortest Initials:

Last name:

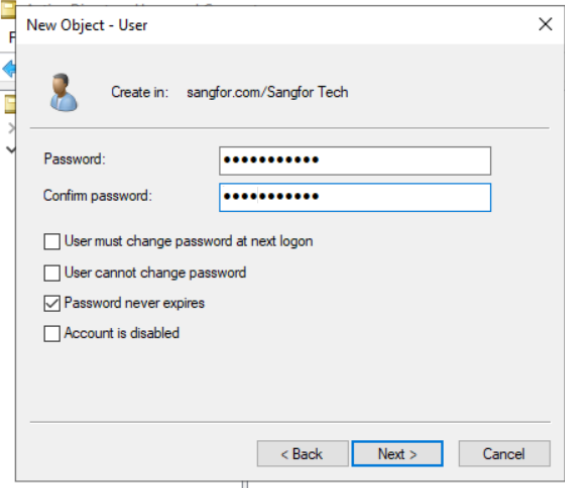
Full name: sangfortest

User login name: sangfortest @sangfor.com

User login name (pre-Windows 2000): SANGFOR\ sangfortest

< Back Next > Cancel

Set a login password for this user.



New Object - User

Create in: sangfor.com/Sangfor Tech

Password:

Confirm password:

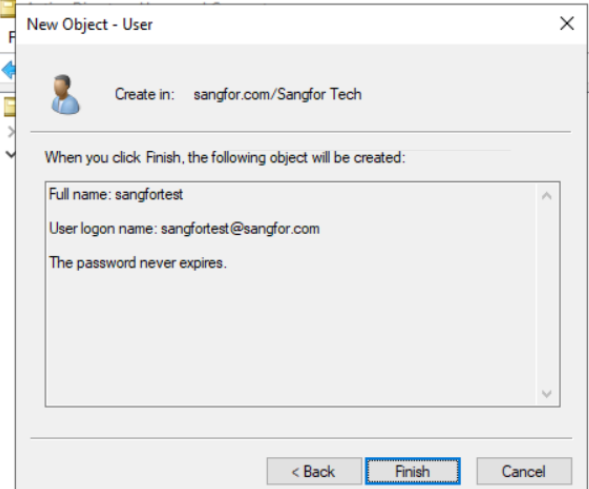
☐ User must change password at next login

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel



New Object - User

Create in: sangfor.com/Sangfor Tech

When you click Finish, the following object will be created:

Full name: sangfortest

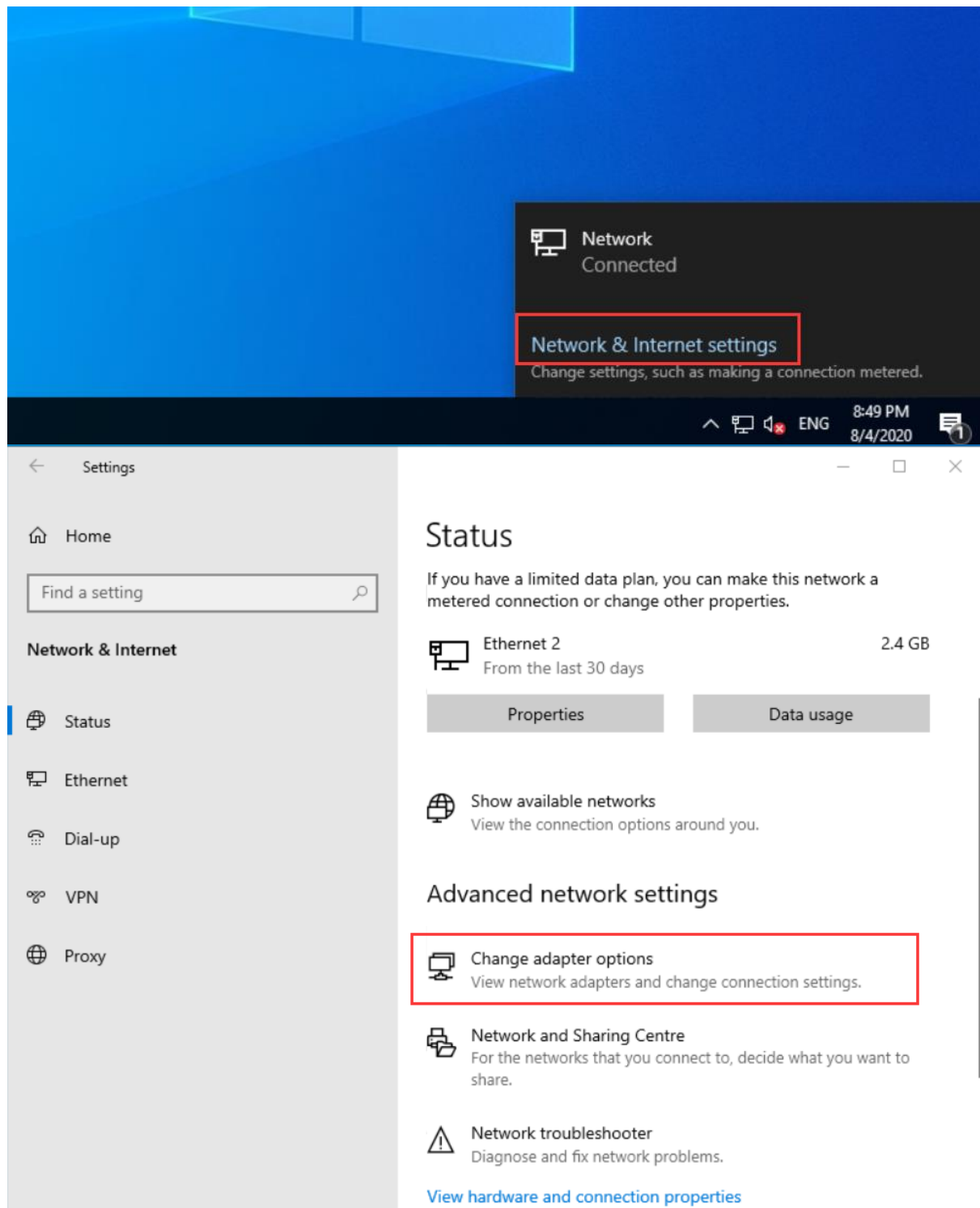
User login name: sangfortest@sangfor.com

The password never expires.

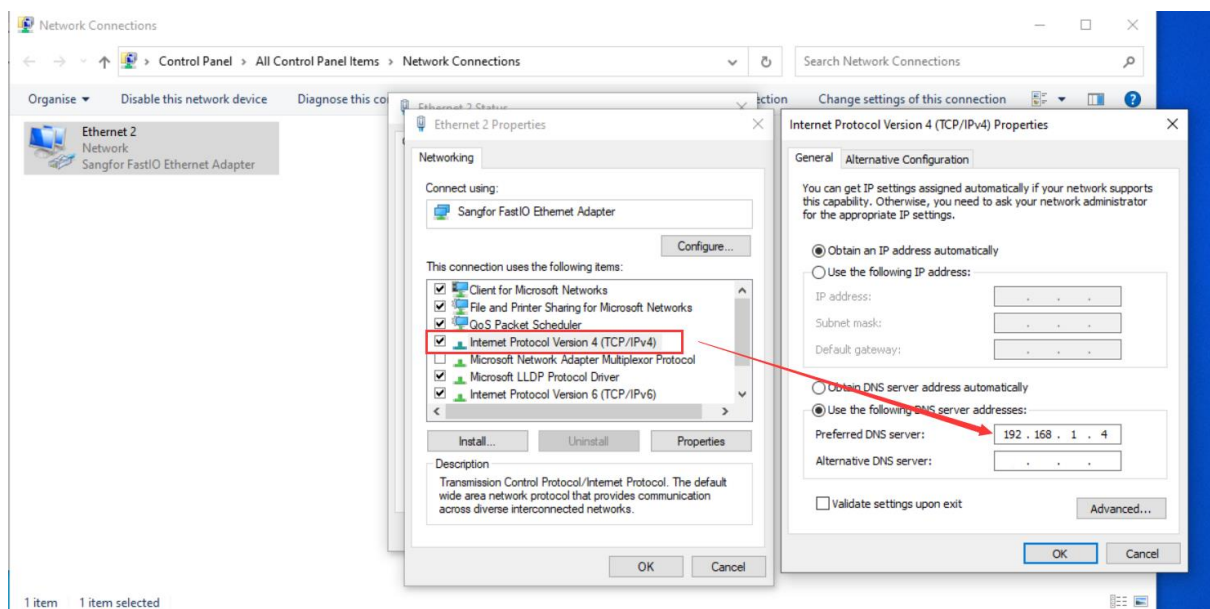
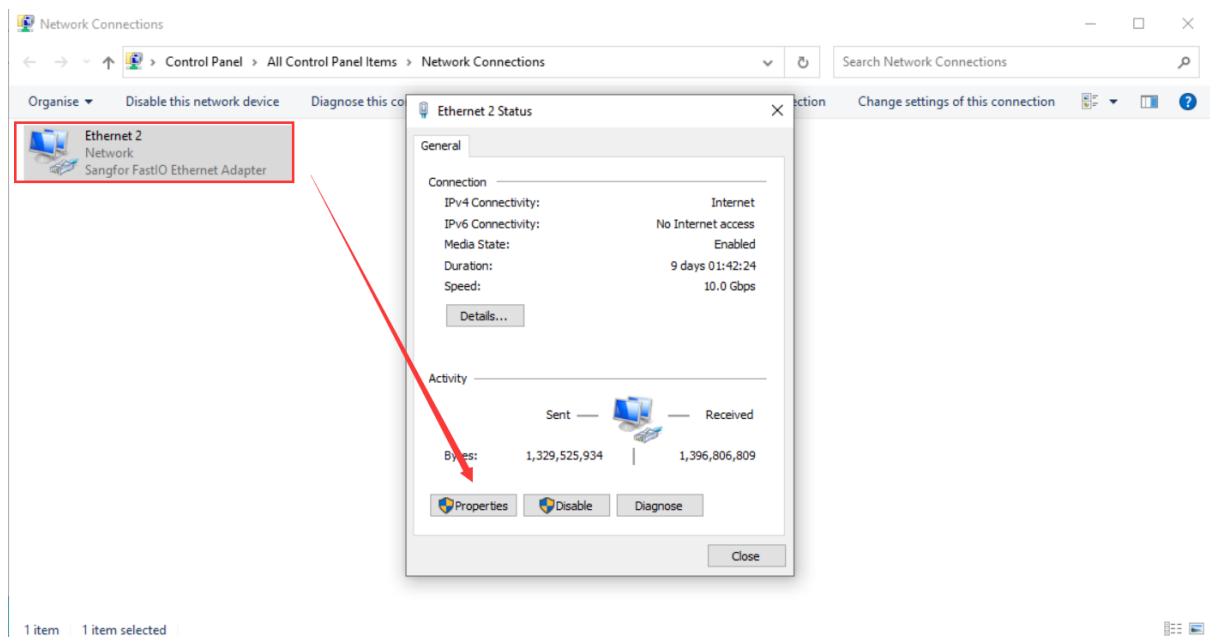
< Back Finish Cancel

## 2.4 Join the PC to the domain

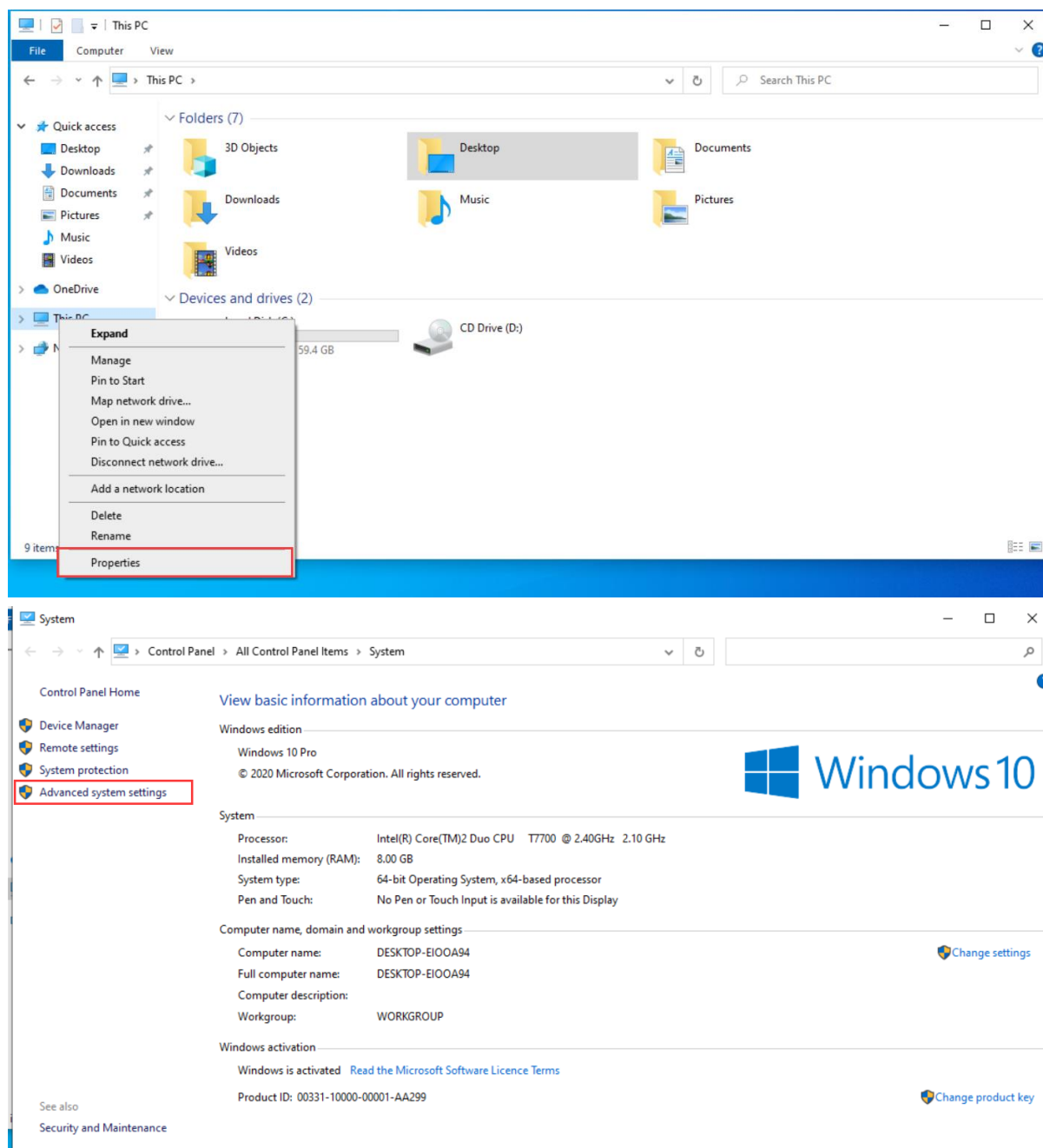
1. Configure the PC's network card, and configure DNS as the IP of the domain control server: 192.168.1.4.

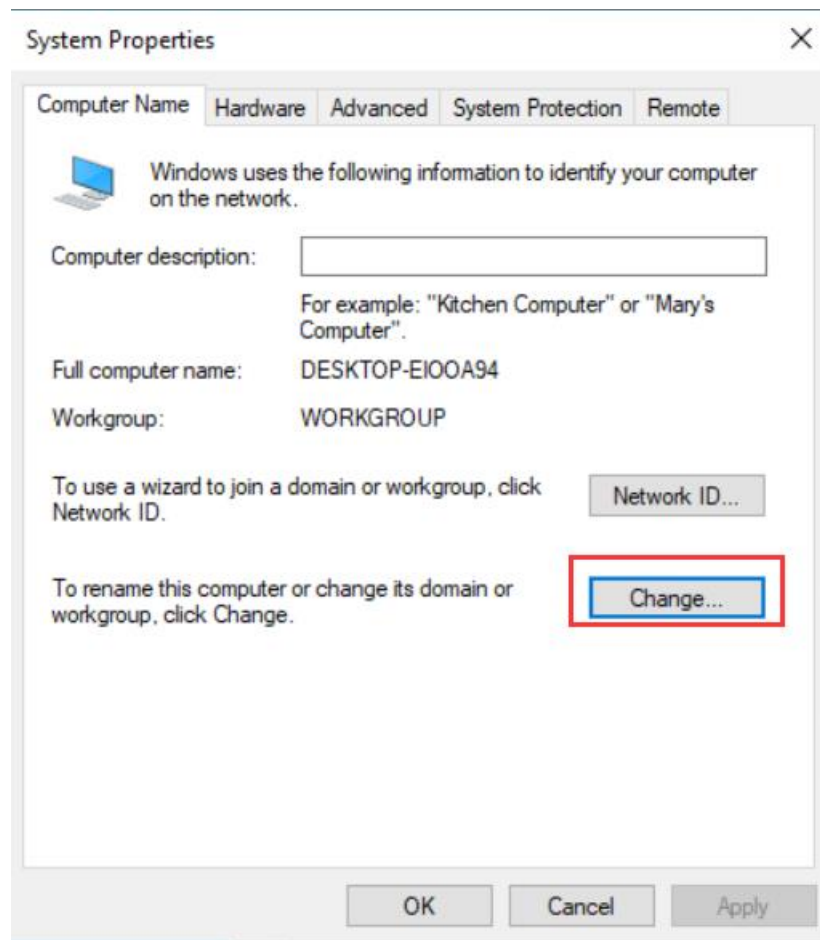


## Activity Domain ADSSO

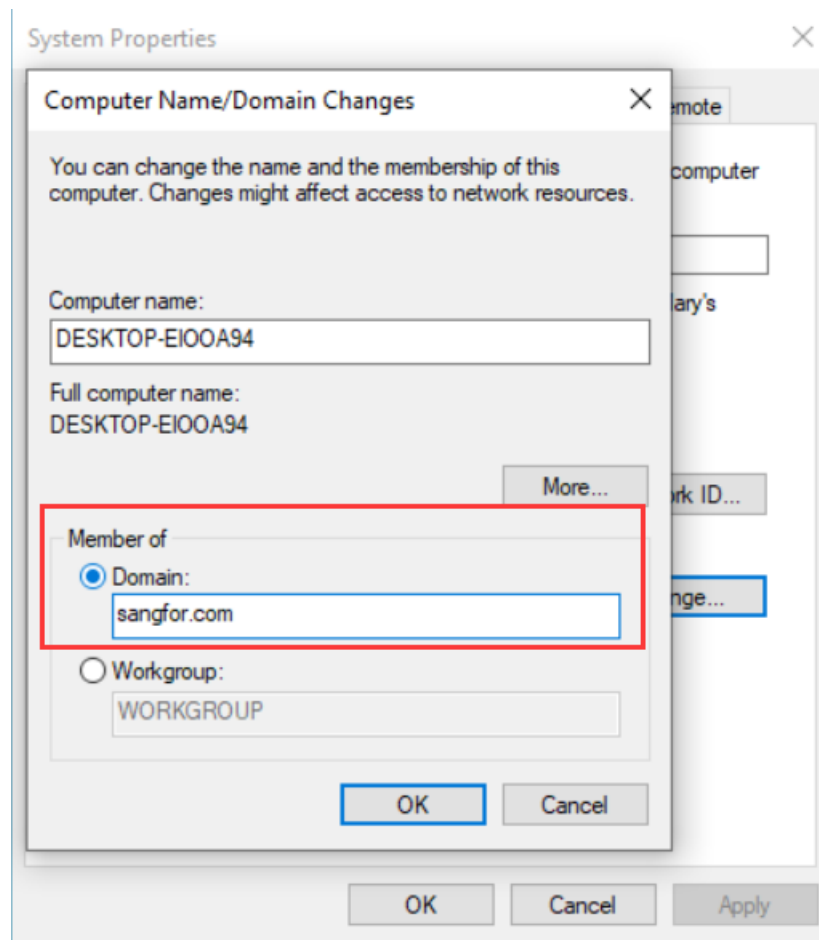


2. Join the PC to the domain.

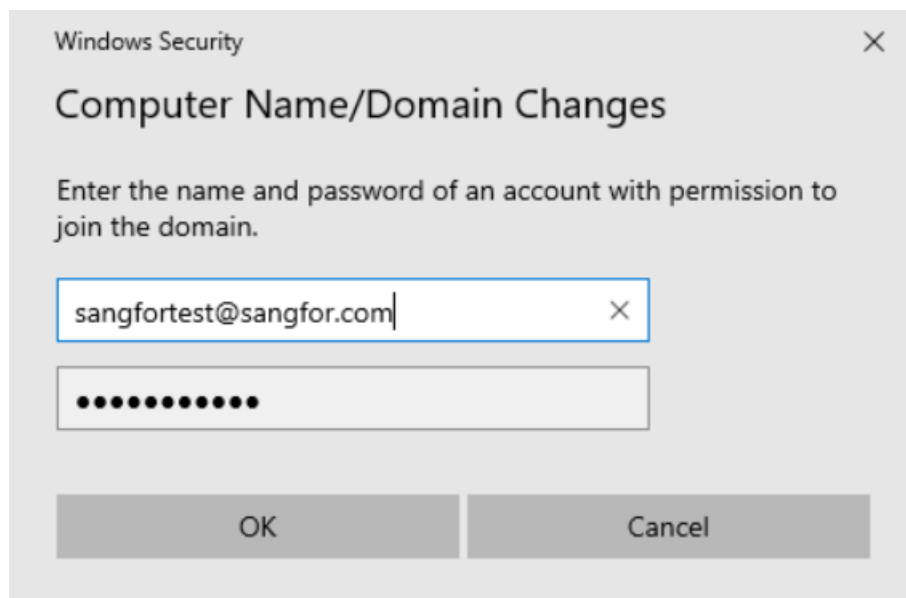




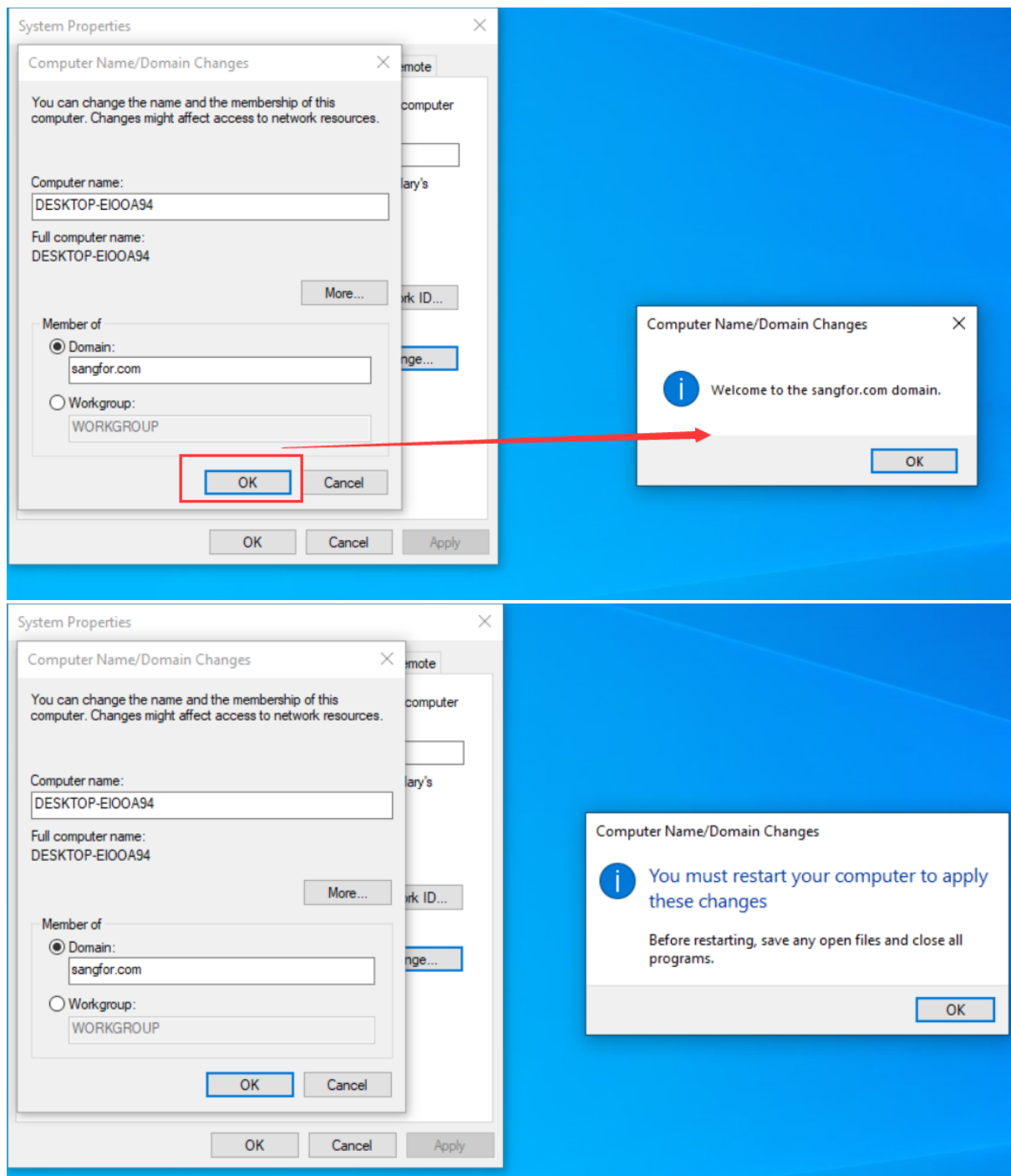


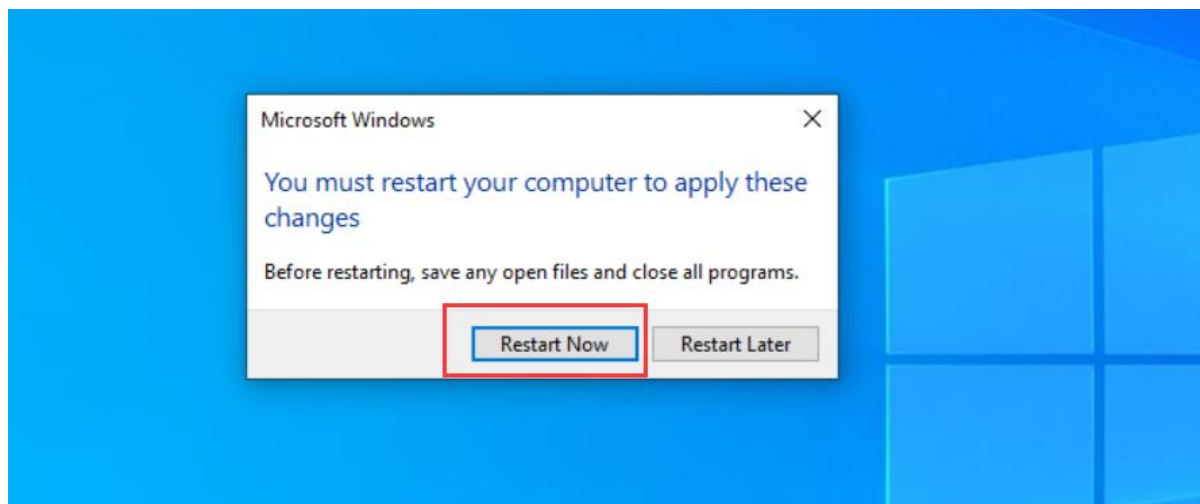


3. In the process of joining the domain, you need to verify your identity, just use the sangfortest user created on the AD domain control 192.168.1.4 for testing.

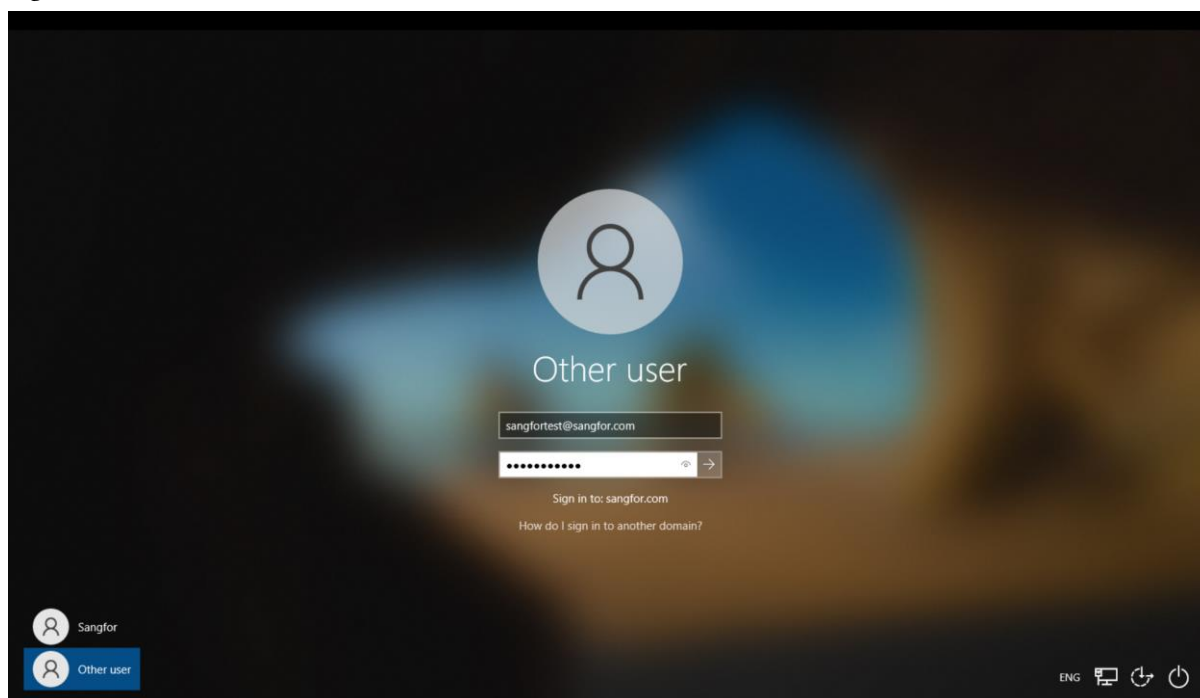


4. After successfully joining the domain, you need to restart the PC.



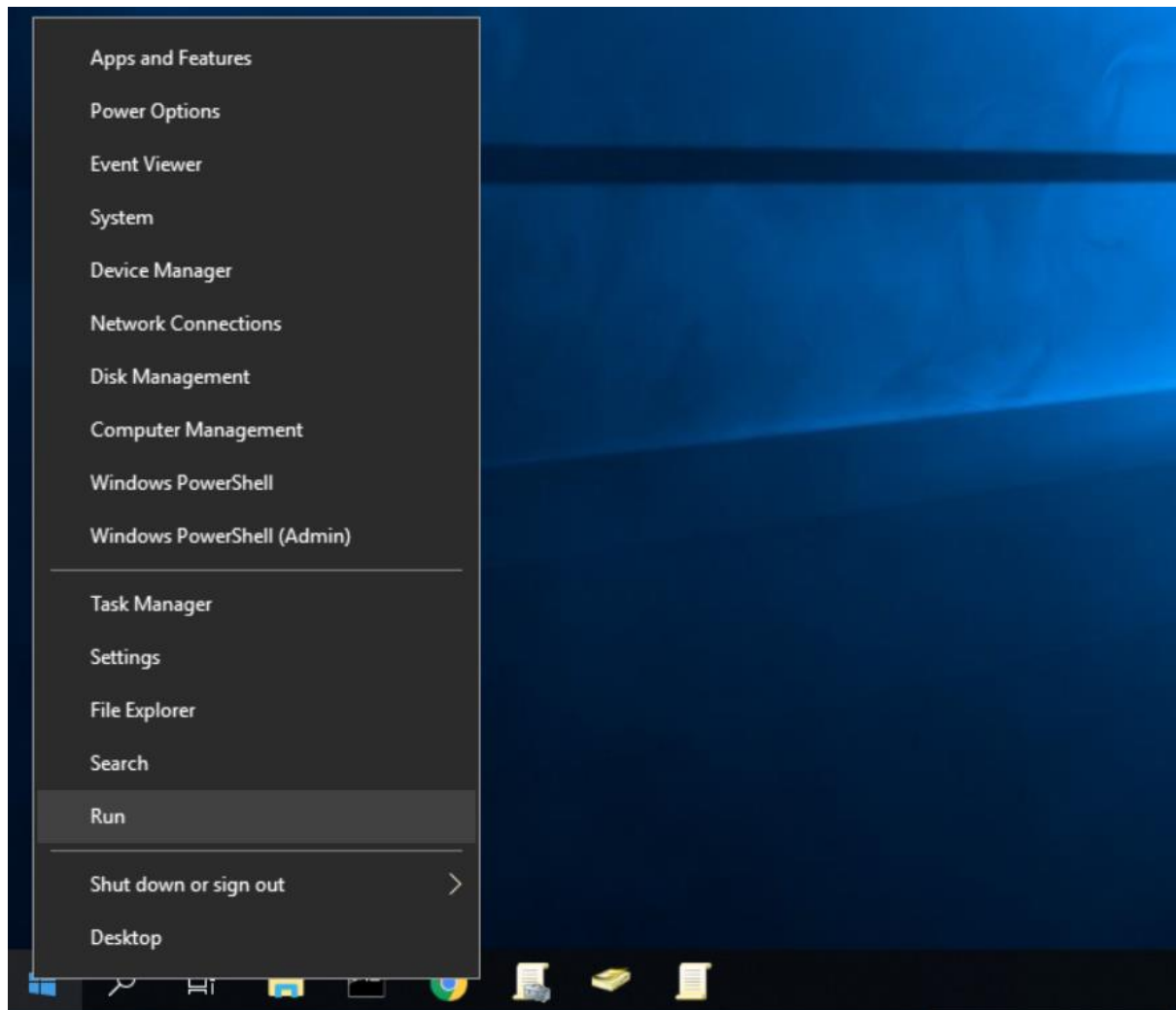


5. After restarting, you can see the login page of the PC, choose to use the domain account sangfortest to log in.

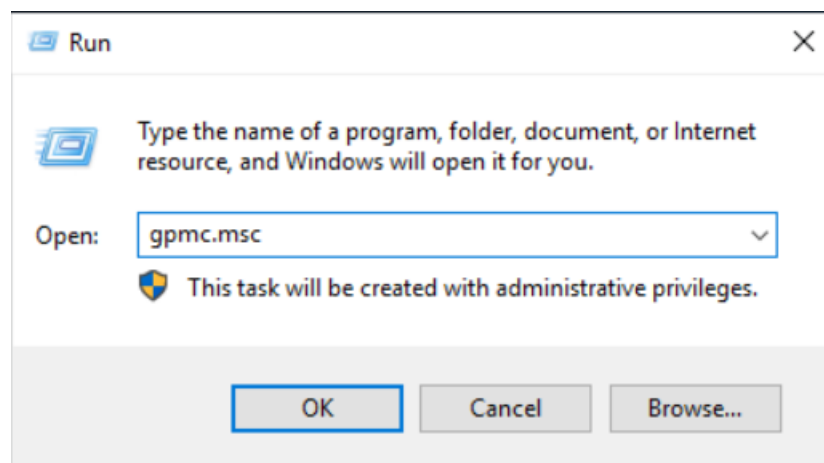


## 2.5 Enable the log audit function of AD Server

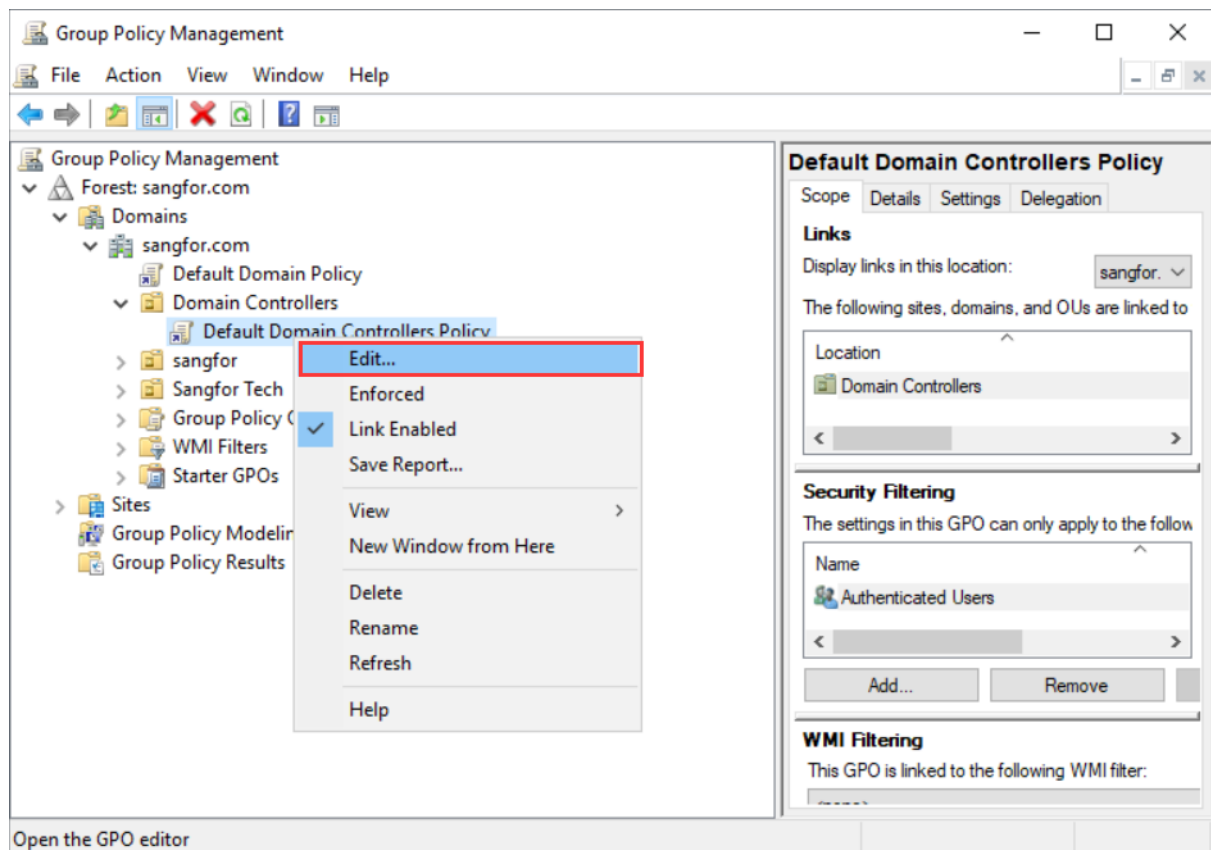
1. Open "Run".



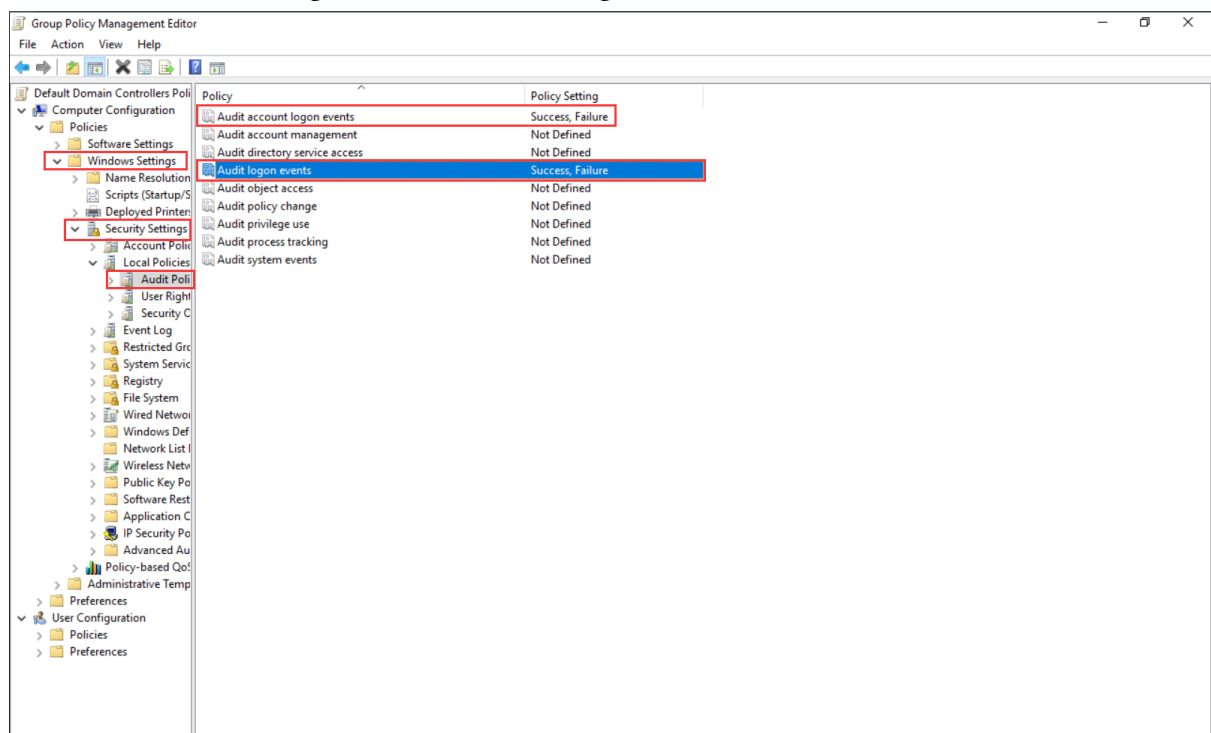
2. Enter "gpmc.msc".



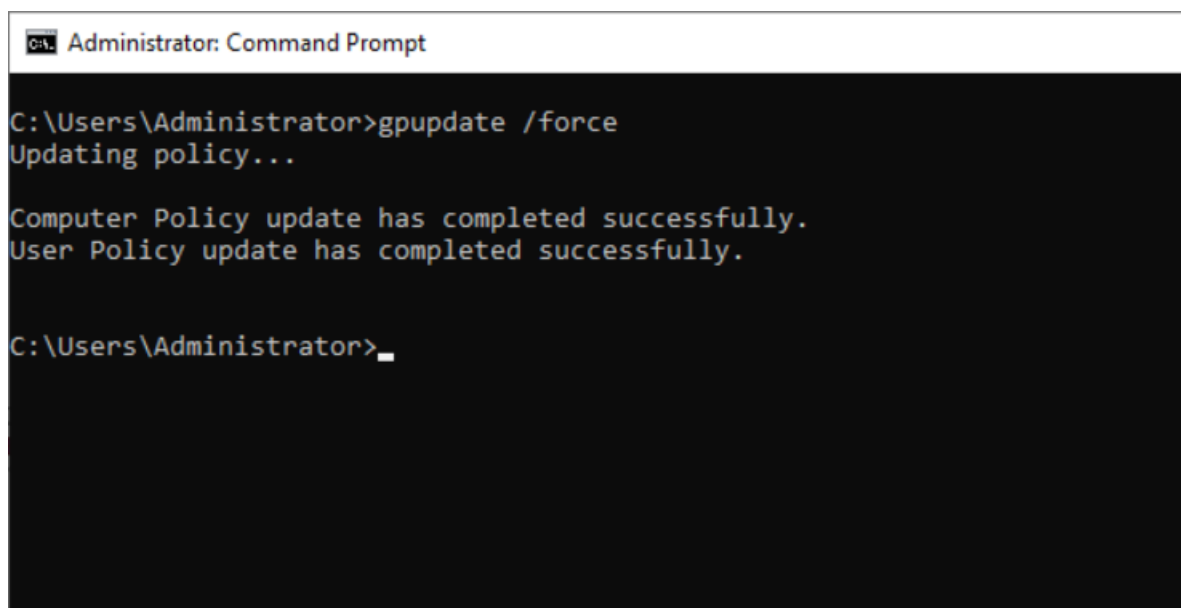
3. Right-click to edit "Default Domain Controllers Policy".



4. Enable "Audit account logon events" and "Audit logon events".



5. Enter "gpupdate /force" in CMD to force refresh of group policy.



```
Administrator: Command Prompt

C:\Users\Administrator>gpupdate /force
Updating policy...

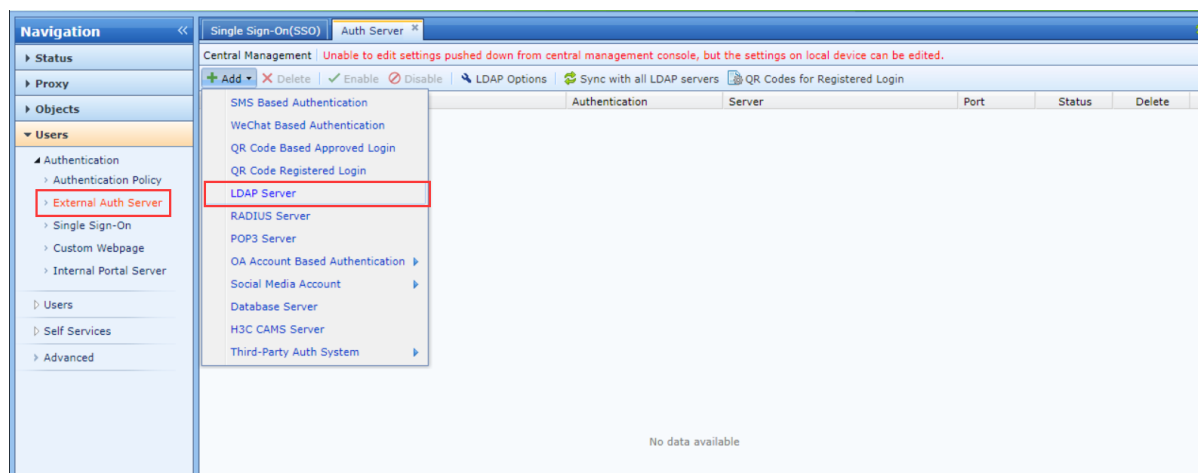
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

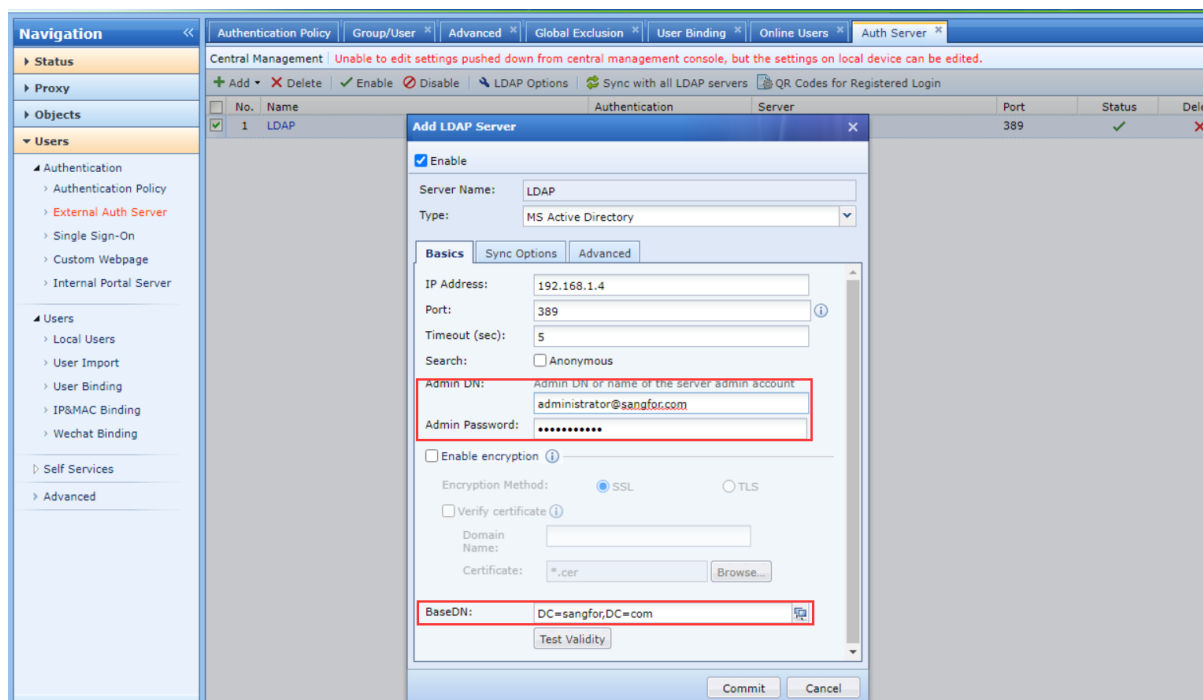
## Chapter 3 How to Configure IAM

### 3.1 Add LDAP server

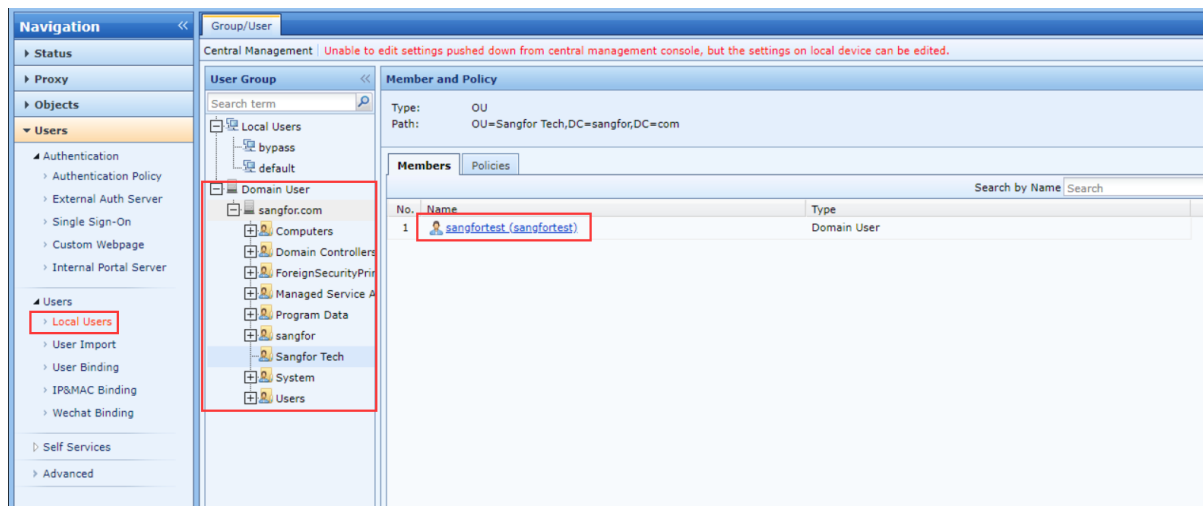
1. Add Microsoft AD server on IAM.



2. Pay attention to the user name to enter the complete domain name, you can use the created sangfortest@sangfor.com, but usually it is recommended to use the administrator account, to avoid the lack of permissions that cause IAM to be unable to interact with the Microsoft AD server. BaseDN can choose sangfor.

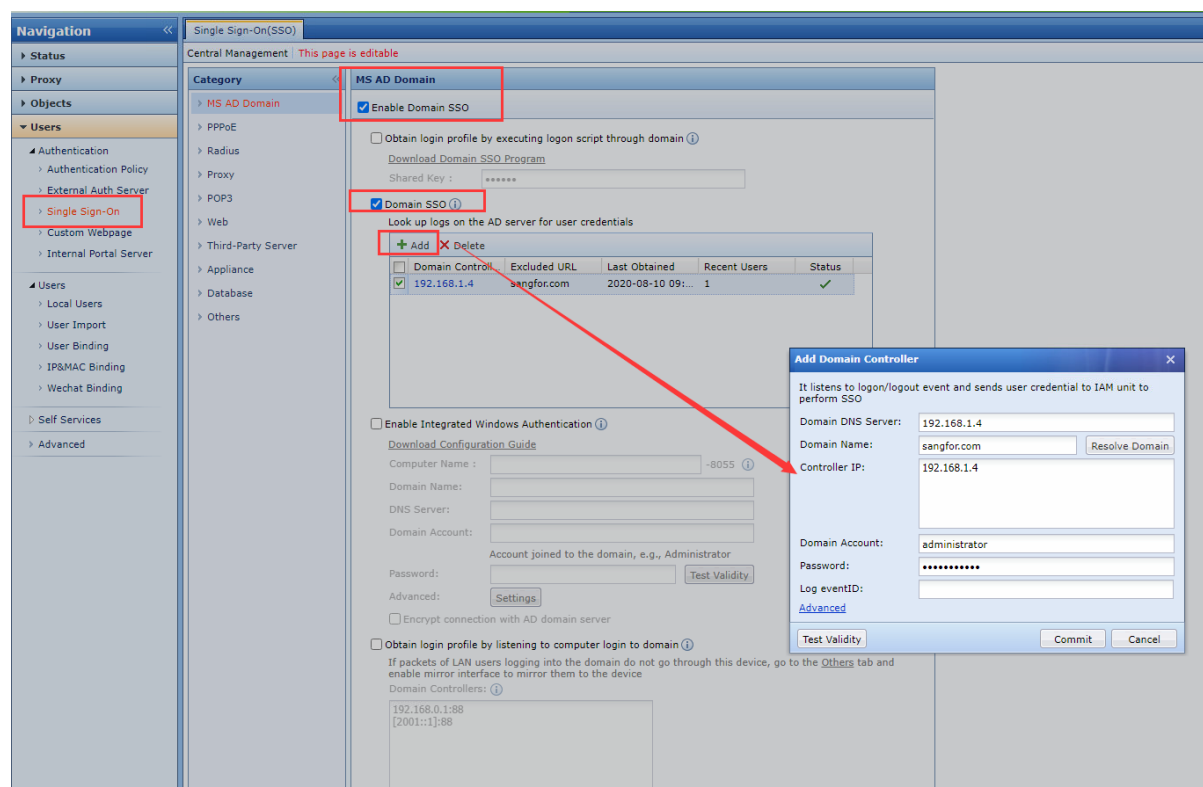


3. If IAM and AD can interact normally, then in the local user, you can see that IAM has obtained the domain user information of the AD server, including the sangfortest user we created before.



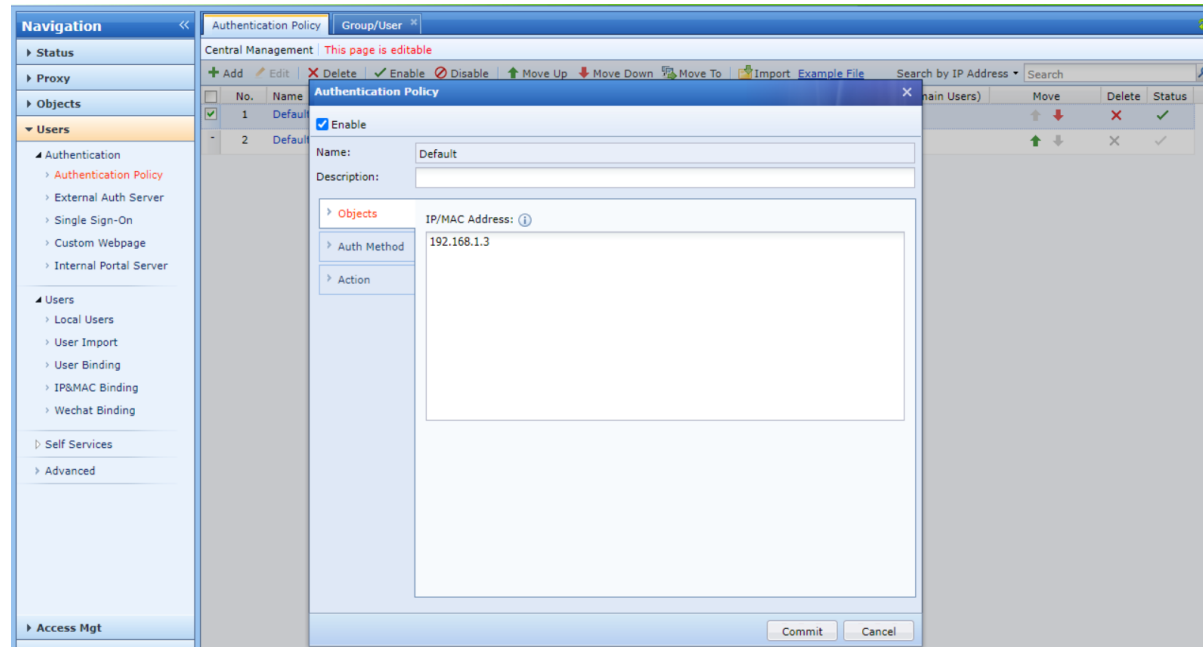
## 3.2 Configure SSO authentication options

1. Configure SSO authentication according to the preset Microsoft AD Server information.



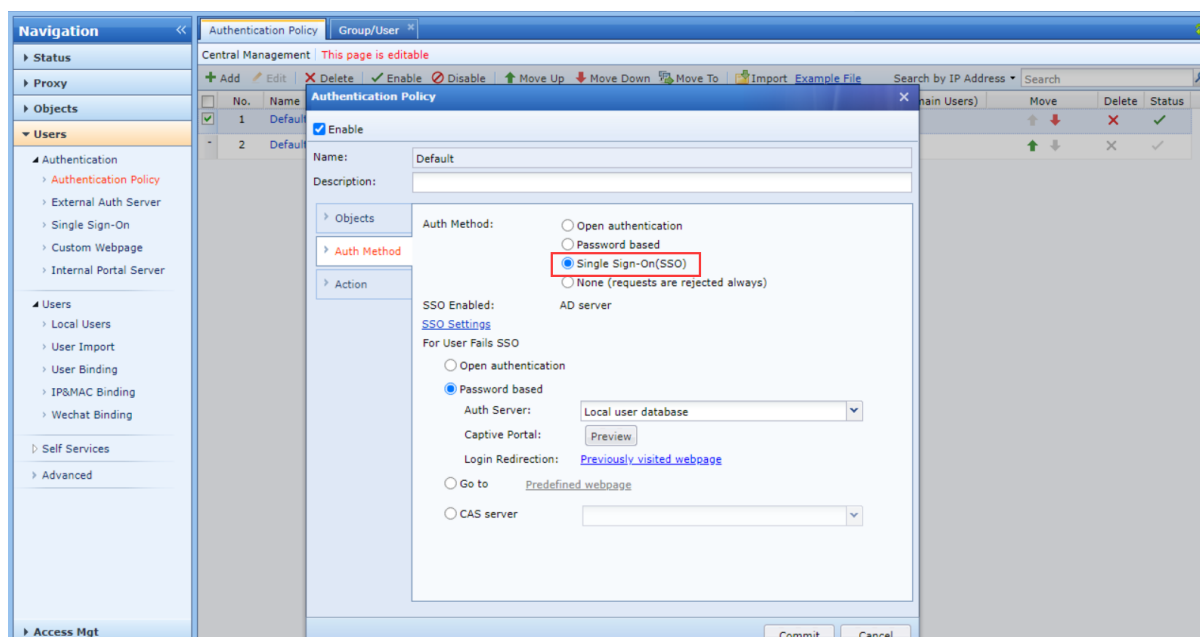
### 3.3 Configure authentication policy on IAM

1. Set the scope of the authentication strategy, that is, which IP should match the authentication policy.

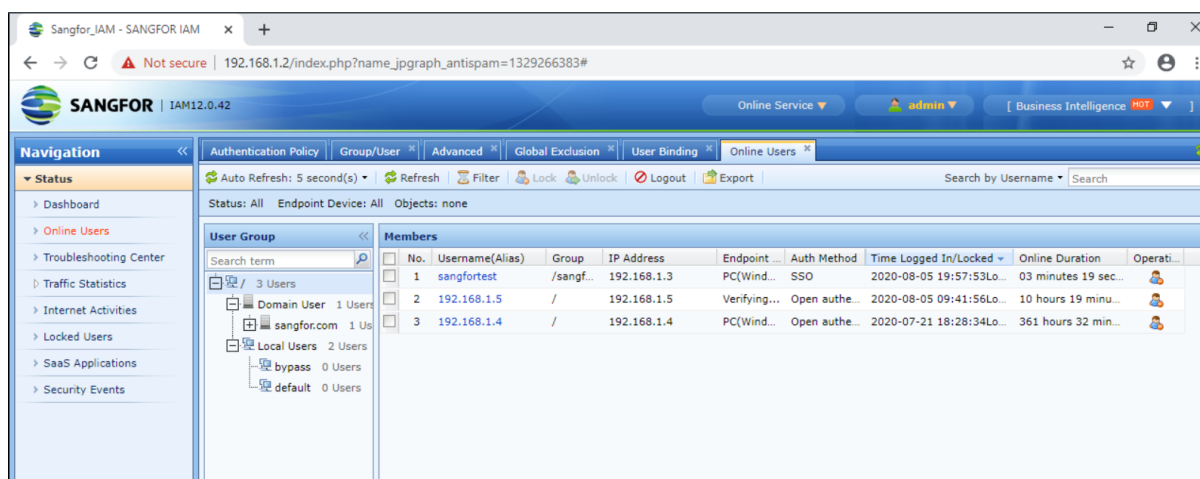


2. Select the authentication method as "SSO".



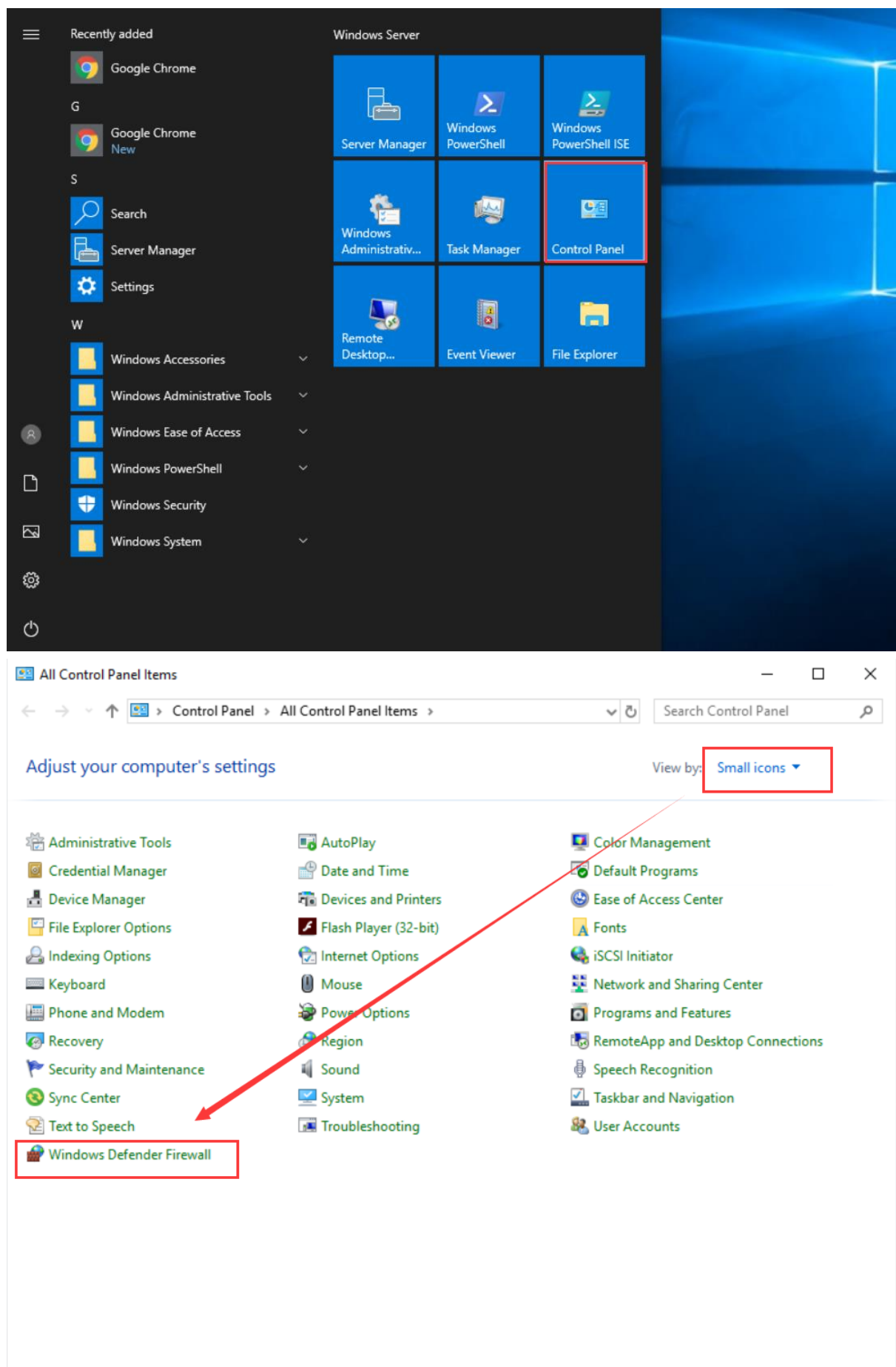


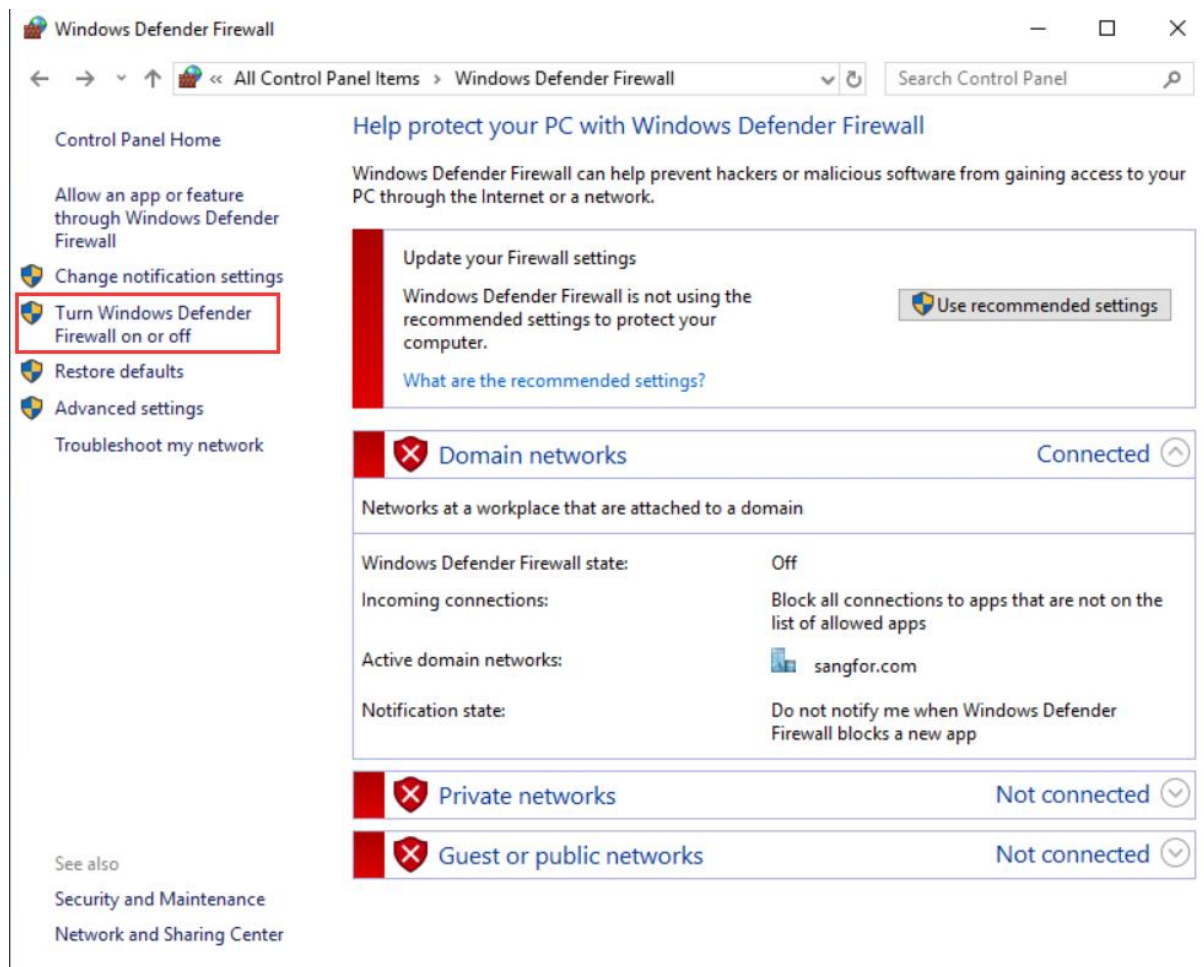
3. Restart the test PC 192.168.1.3 and log in to the PC with a domain account. You can see that PC 192.168.1.3 is online and the authentication method is SSO on the IAM.

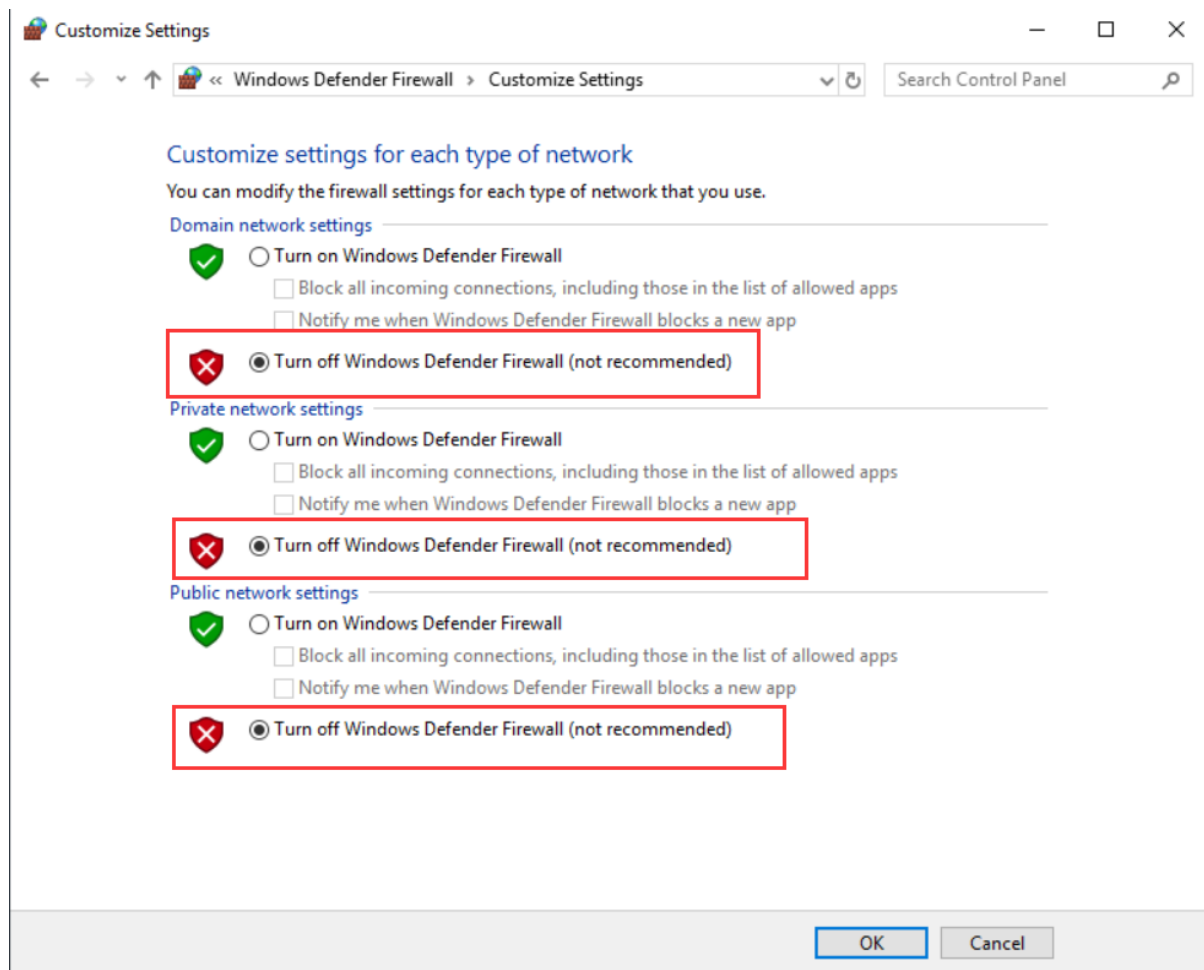


## Chapter 4 Precautions

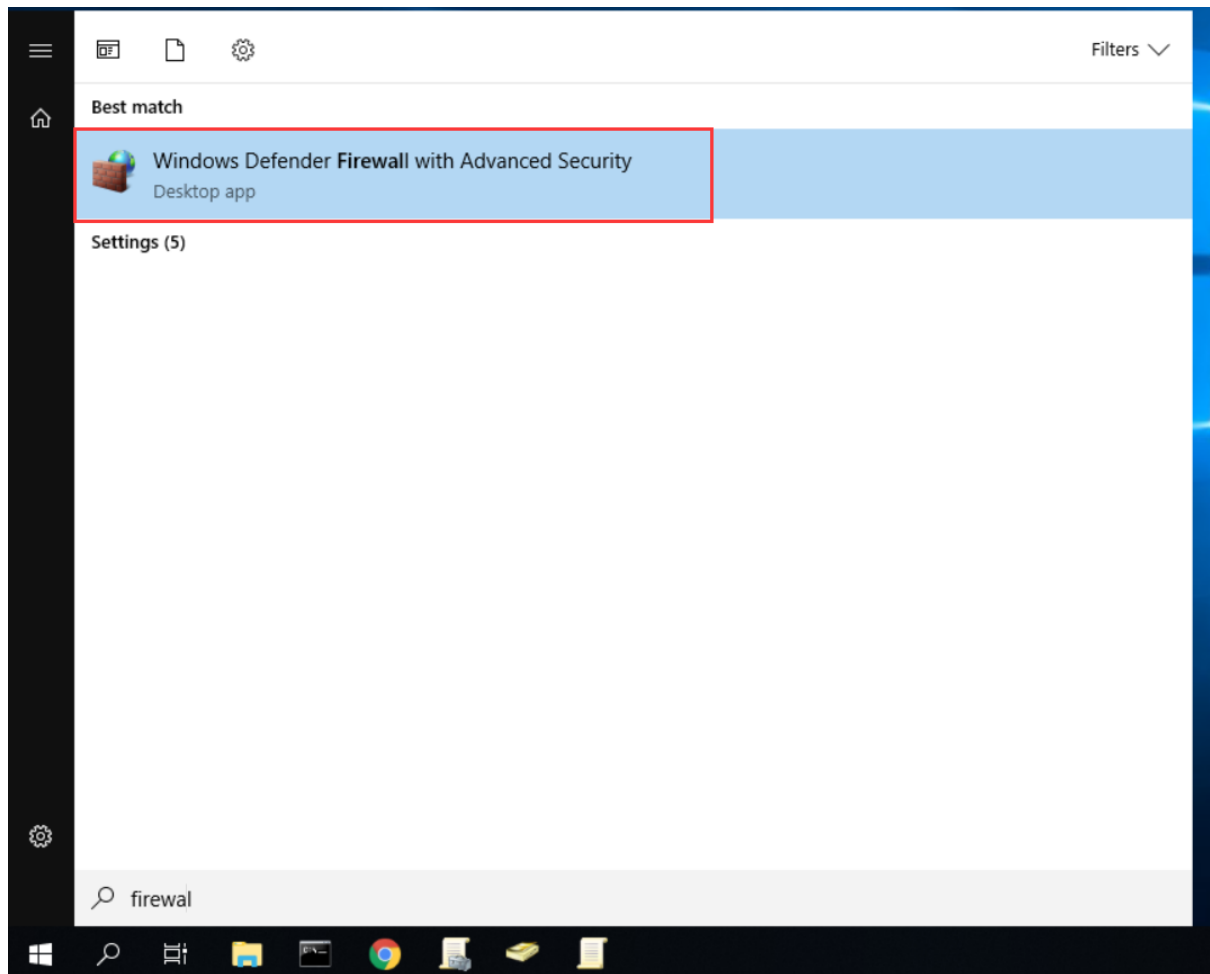
1. It is usually recommended to turn off the system firewall of Windows Server, because the security mechanism of Windows Server is very strict, which usually causes other devices to be unable to obtain relevant data from AD Server.

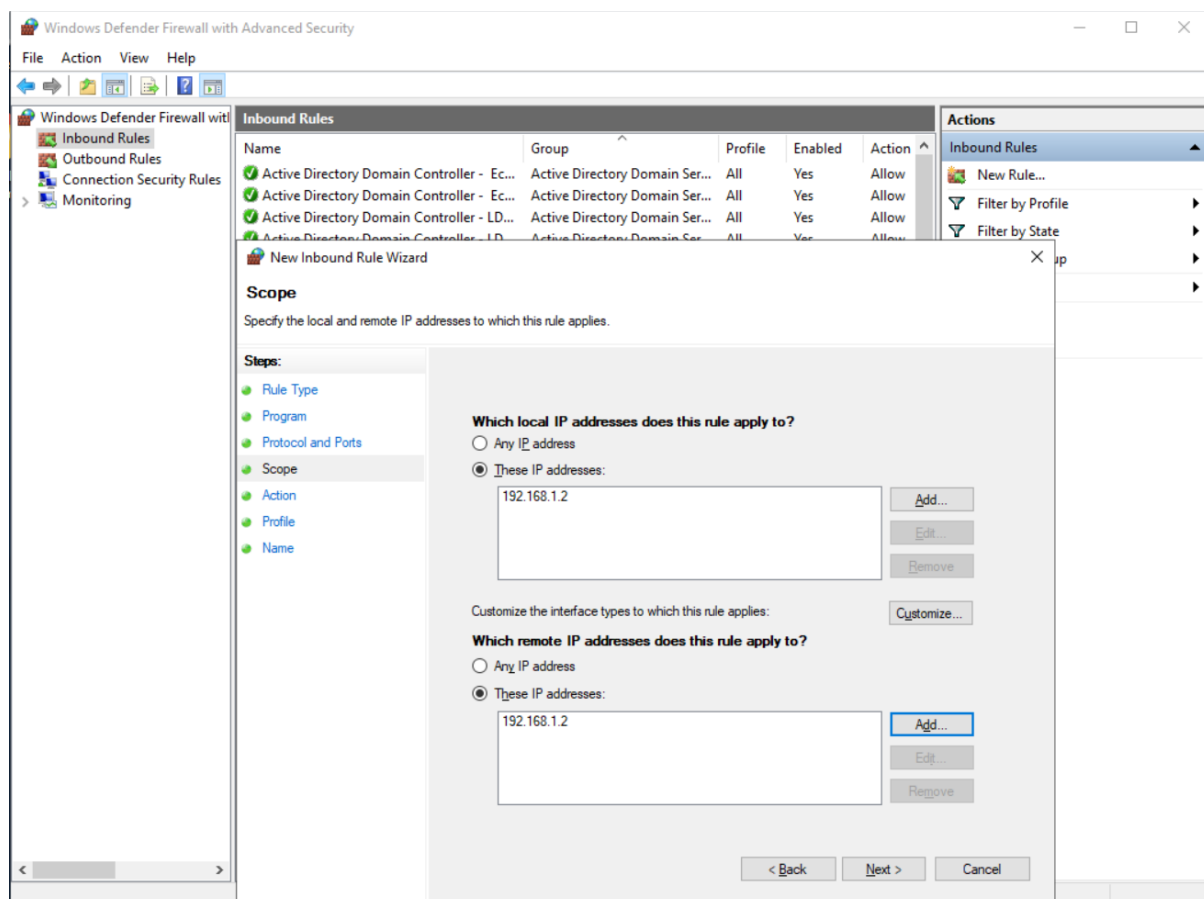






Or you can manually add firewall rules to allow related devices to access AD Server.







**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