SANGFOR

IAM

Best Practices for Scenarios_Activity Domain Script SSO

Version 12.0.42

Change Log

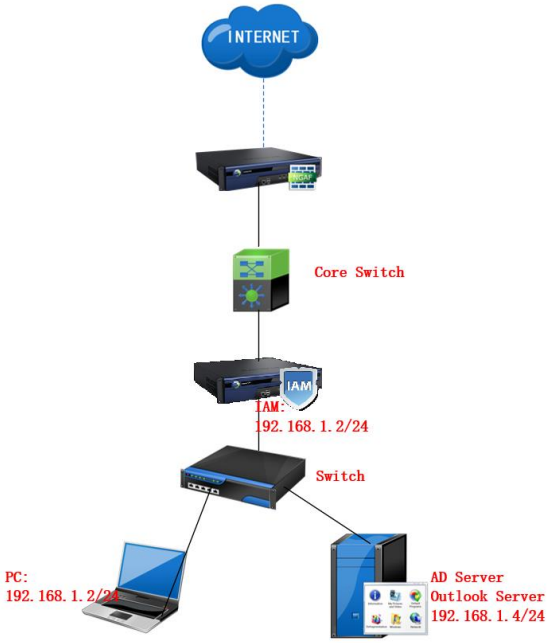
Date	Change Description
Aug 4, 2020	Version 12.0.42 document release.
May 17, 2021	Version 12.0.42 document update.

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
Chapter 3 How to Configure IAM 24
3.1 Add LDAP server 24
3.2 Configure script SSO on IAM and AD Server 26
3.3 Configure the login and logout script on the AD 27
3.4 Configure authentication policy on IAM 34
Chapter 4 Precautions 35

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. The customer is allowed to deliver scripts through the Microsoft AD domain and requires a higher SSO Success rate, so choose to use scripted SSO.



AD Server:

IP: 192.168.1.4

Domain Name: sangfor.com

Account/Password: administrator/@sangfor123

Test PC:

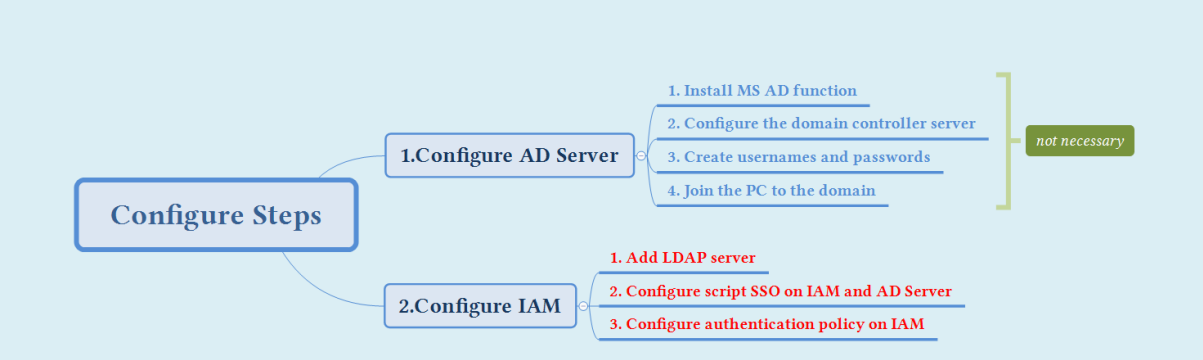
IP: 192.168.1.3

Account/Password: administrator/@sangfor123

Domain Account/Password: sangfortest/@sangfor123

1.1 Configure Steps

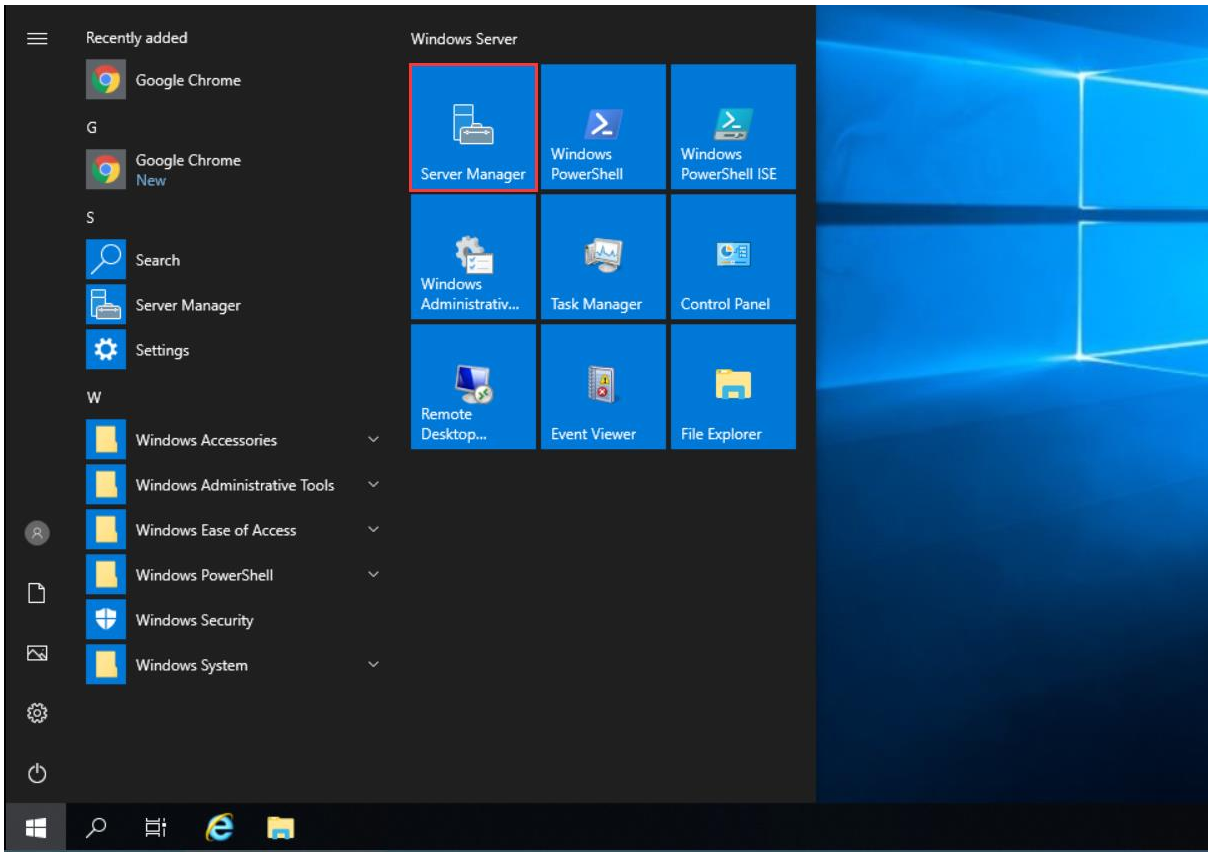
The configuration steps are as shown in the figure below. It should be noted that in order to make everyone familiar with the AD domain faster, we add the method of configuring the AD domain, which is the part marked "not necessary". If the customer has used the AD domain before and does not need to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



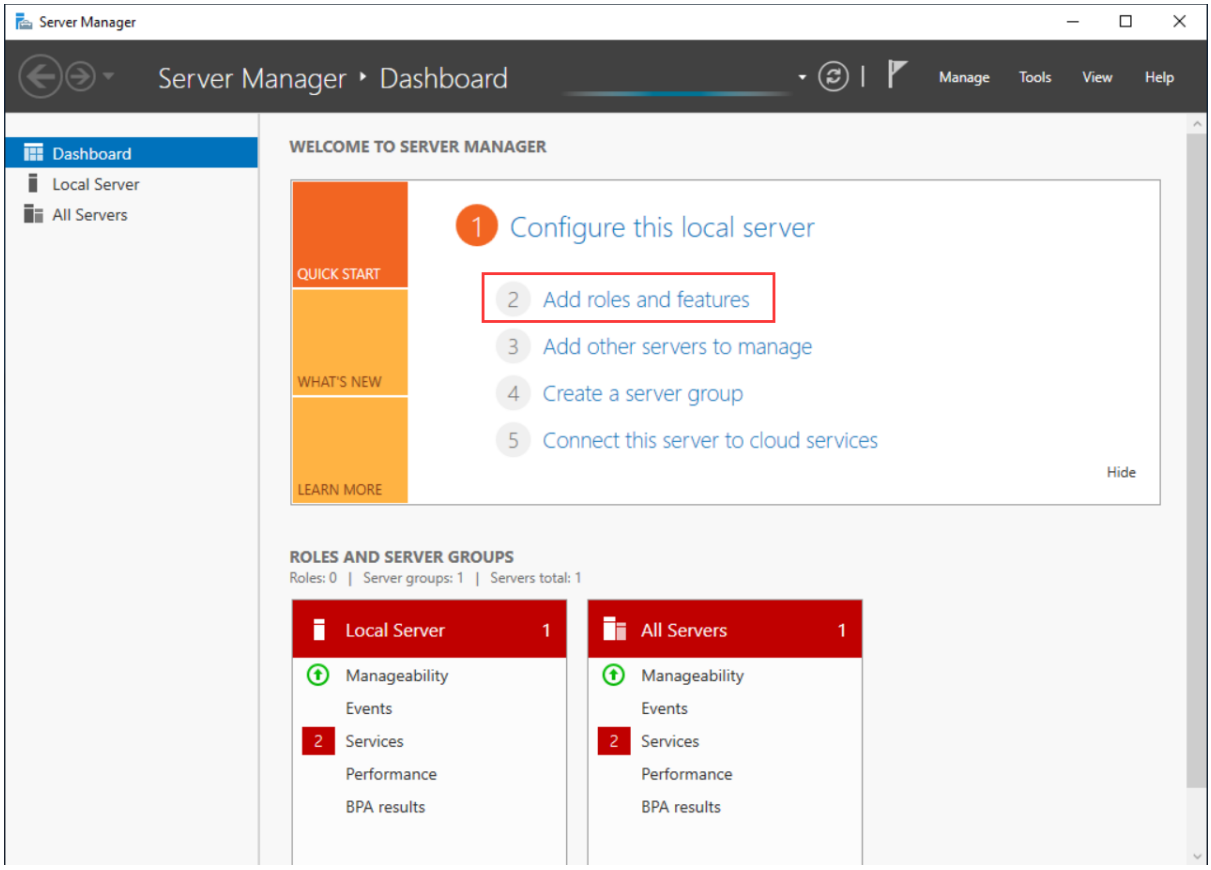
Chapter 2 How to Configure Activity Domain Server

2.1 Install MS AD function

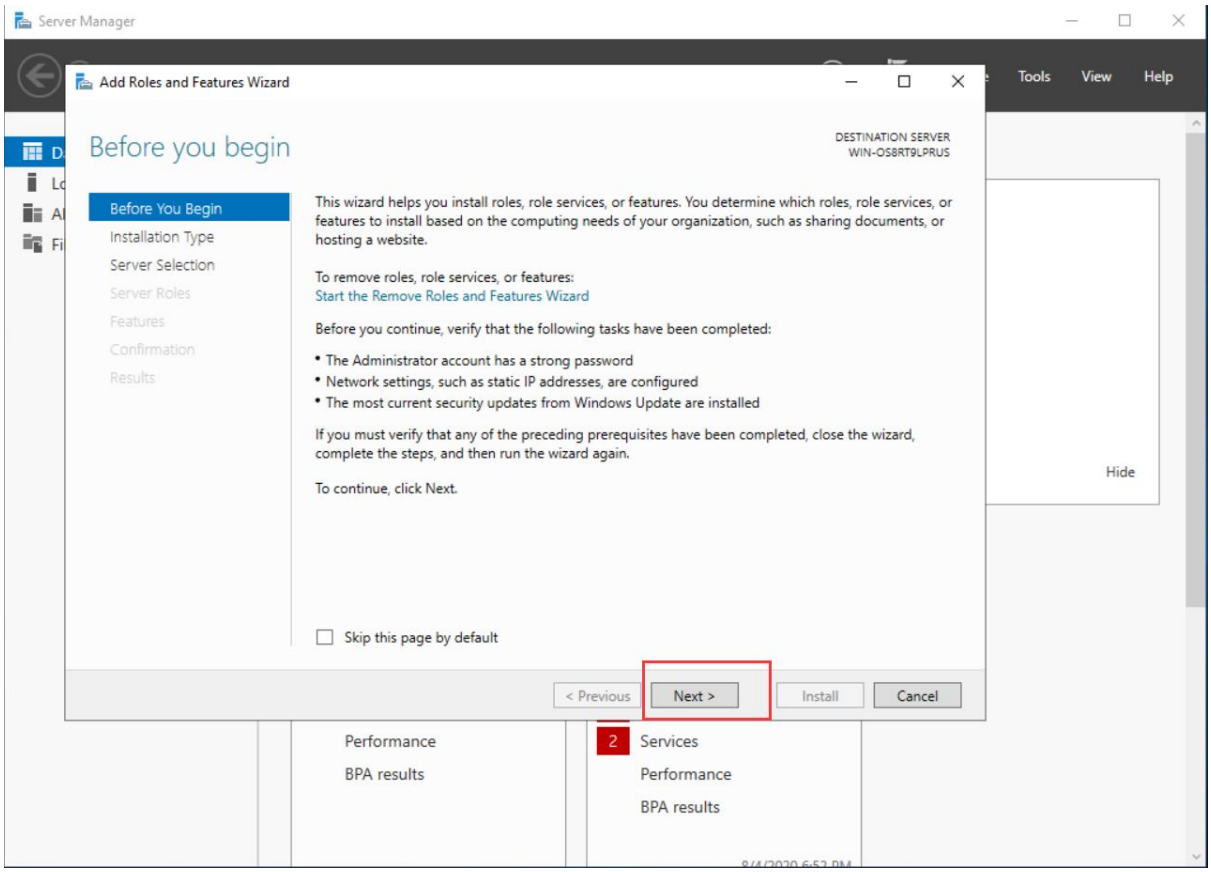
1. Open Server Manager in Windows Server 2019.



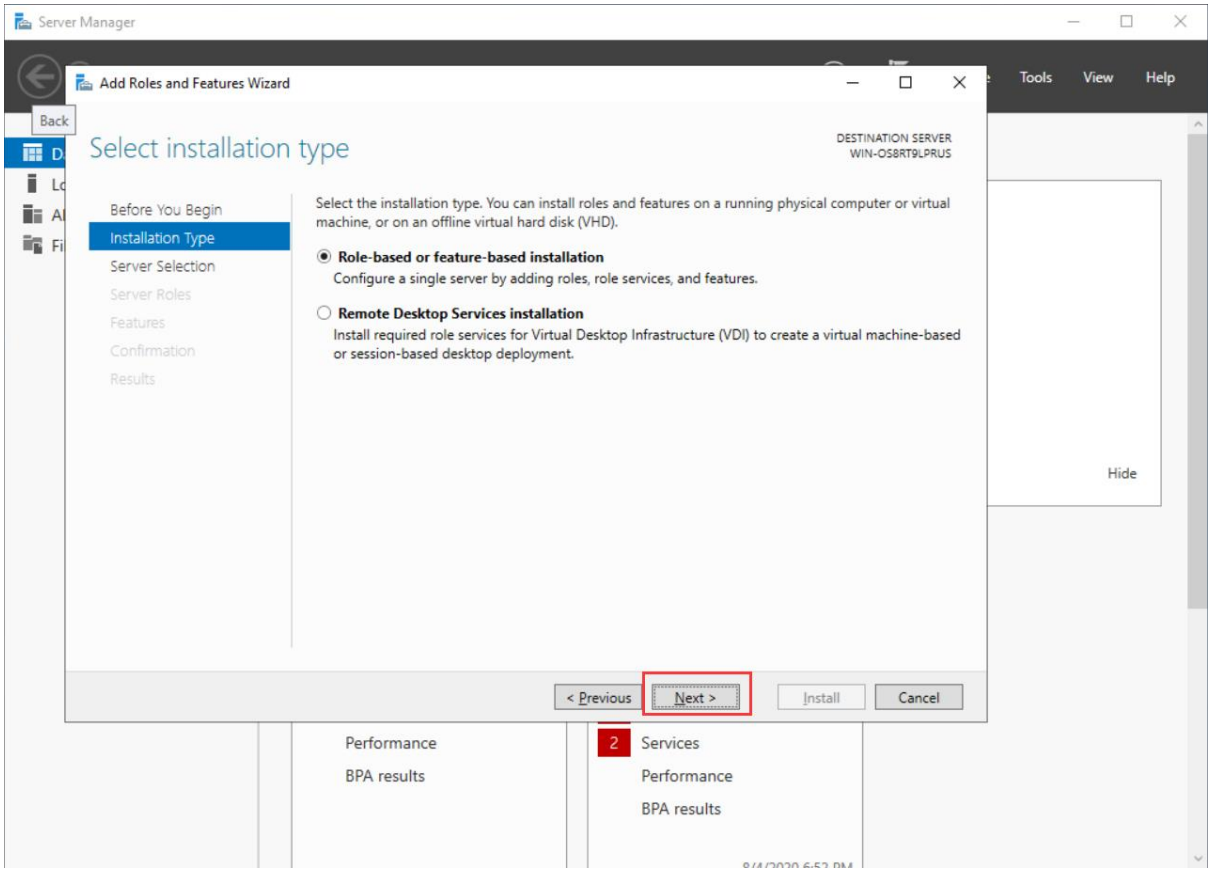
2.Click "Add roles and features".



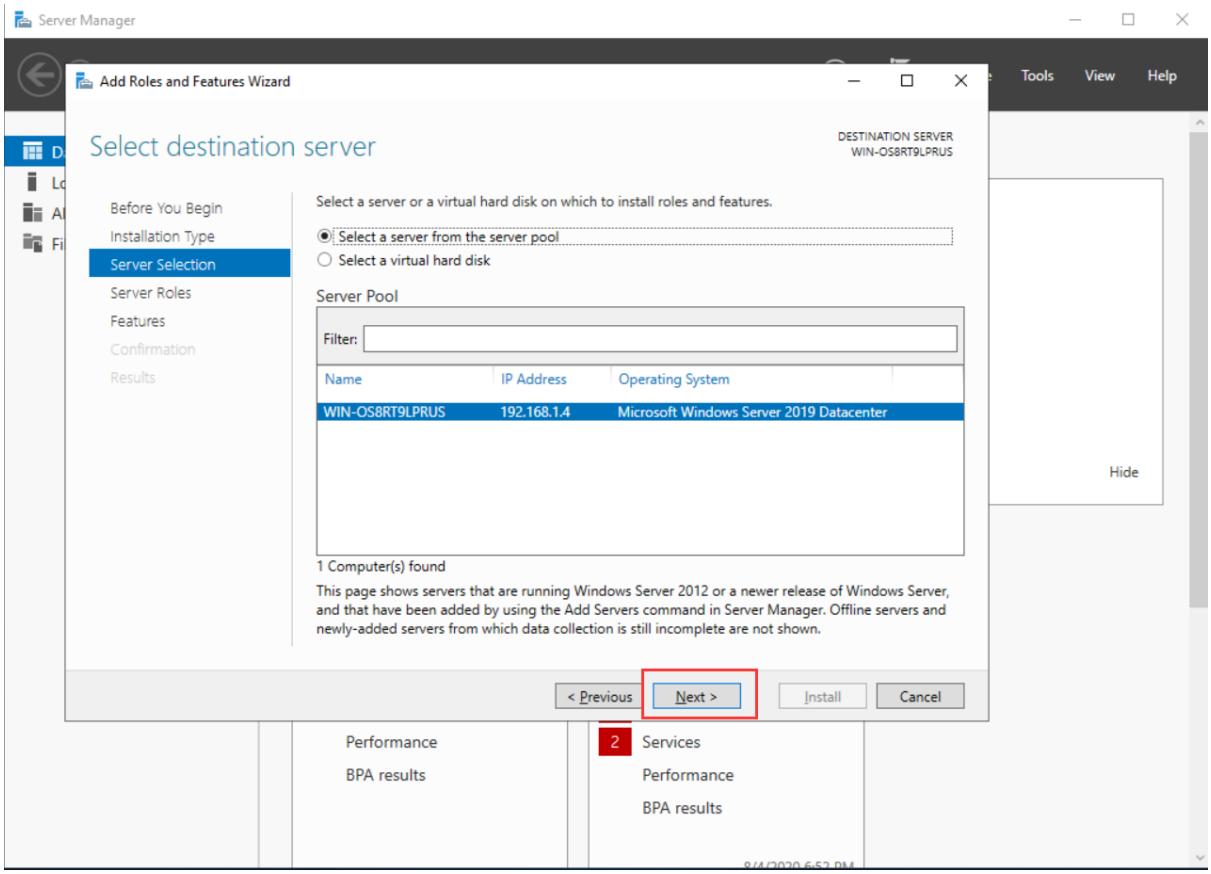
3.Click "Next".



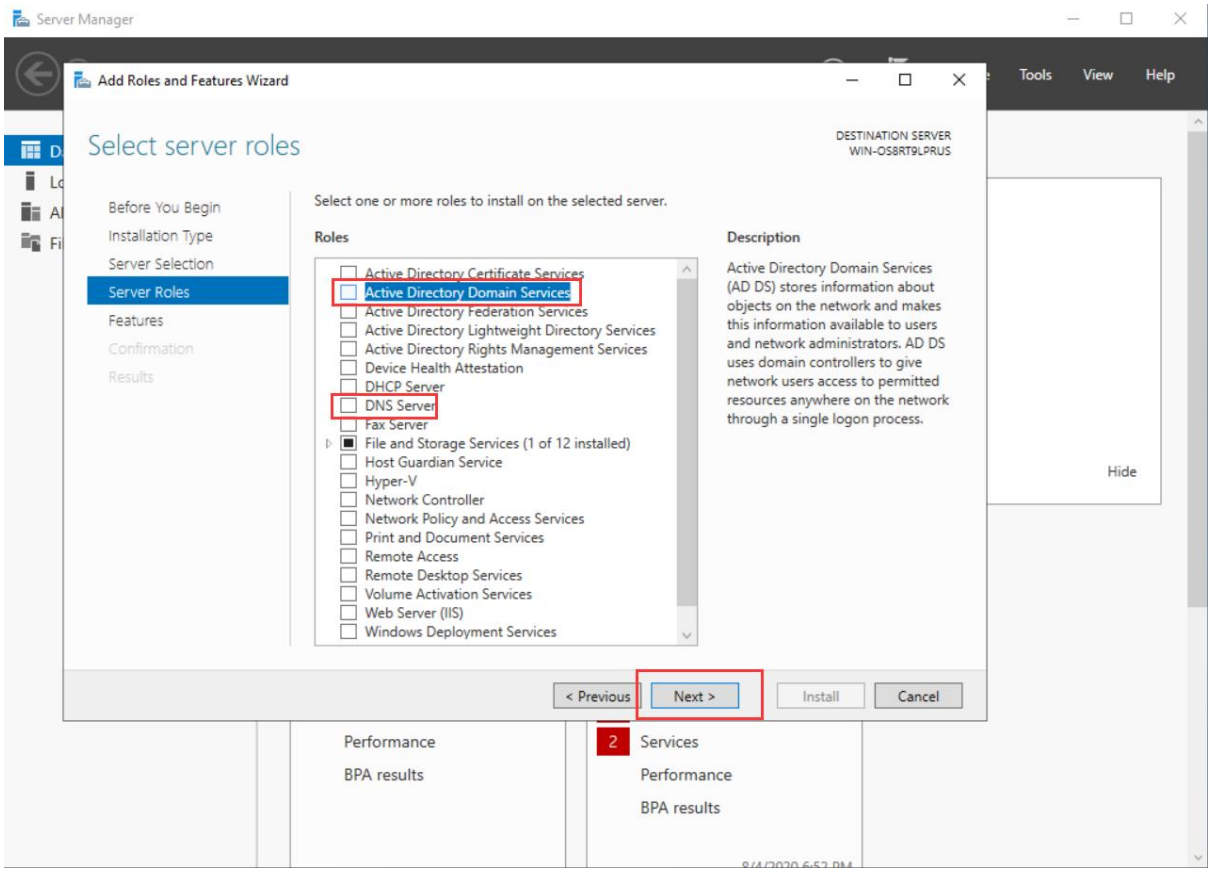
4. Click "Next".

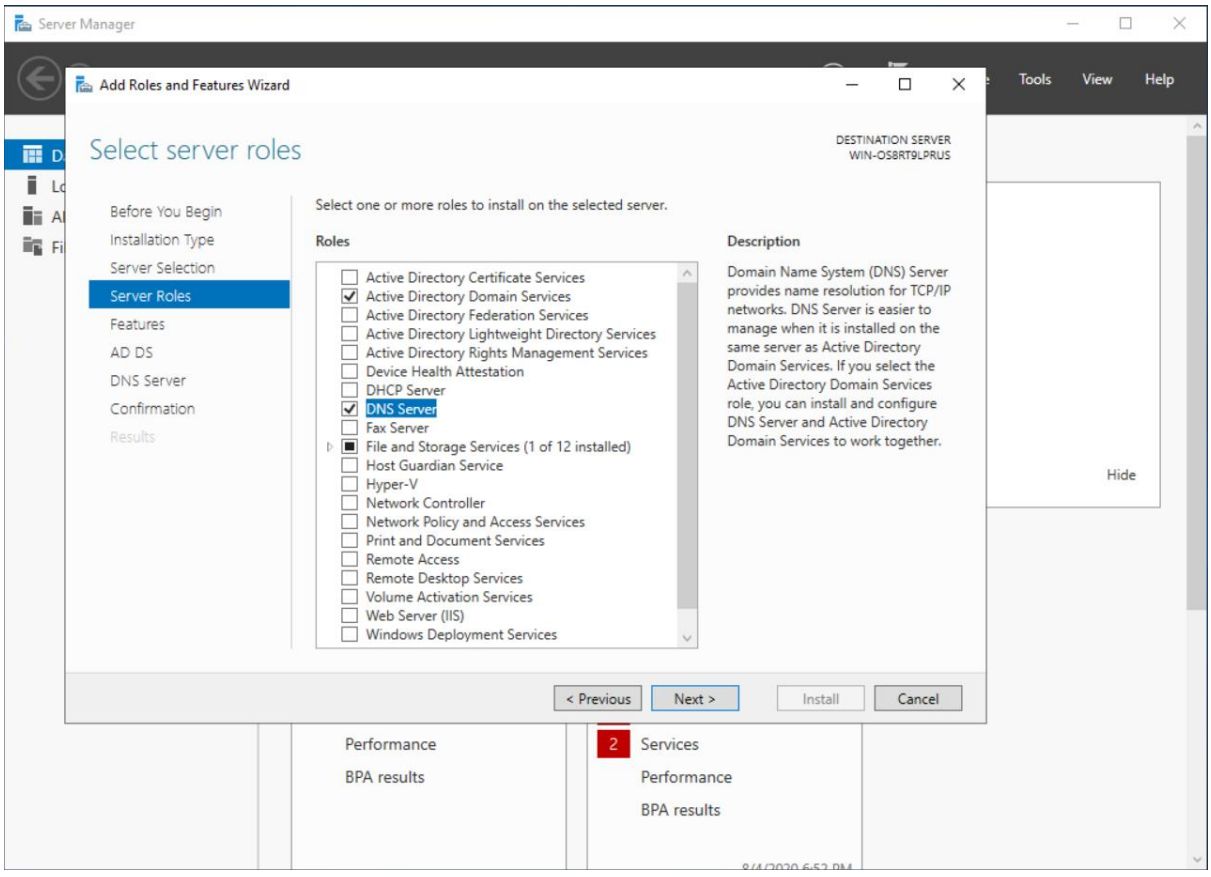

Server Manager
Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WIN-OS8RT9LPRUS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Performance
BPA results
2
Services
Performance
BPA results

5. Click "Next".

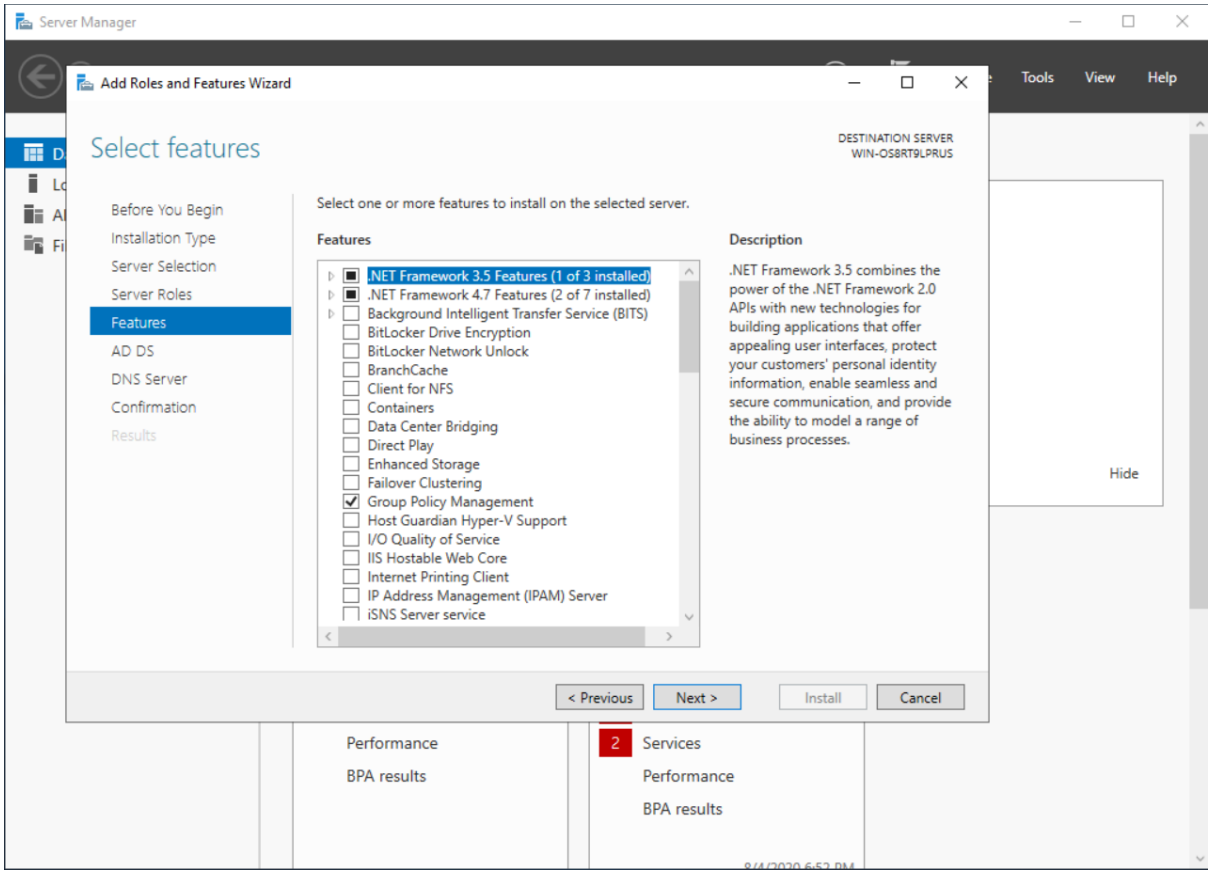

Server Manager
Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-OS8RT9LPRUS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WIN-OS8RT9LPRUS
192.168.1.4
Microsoft Windows Server 2019 Datacenter
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Performance
BPA results
2
Services
Performance
BPA results

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

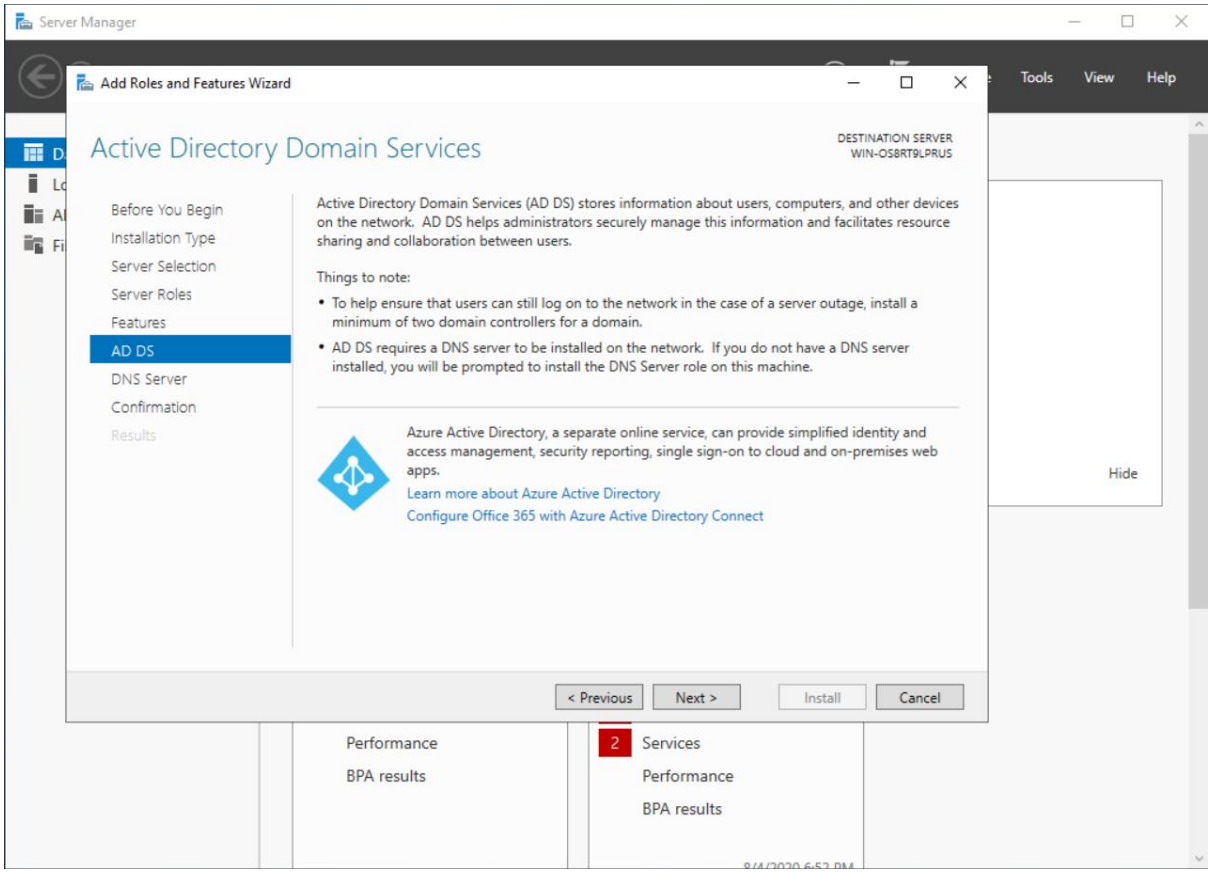




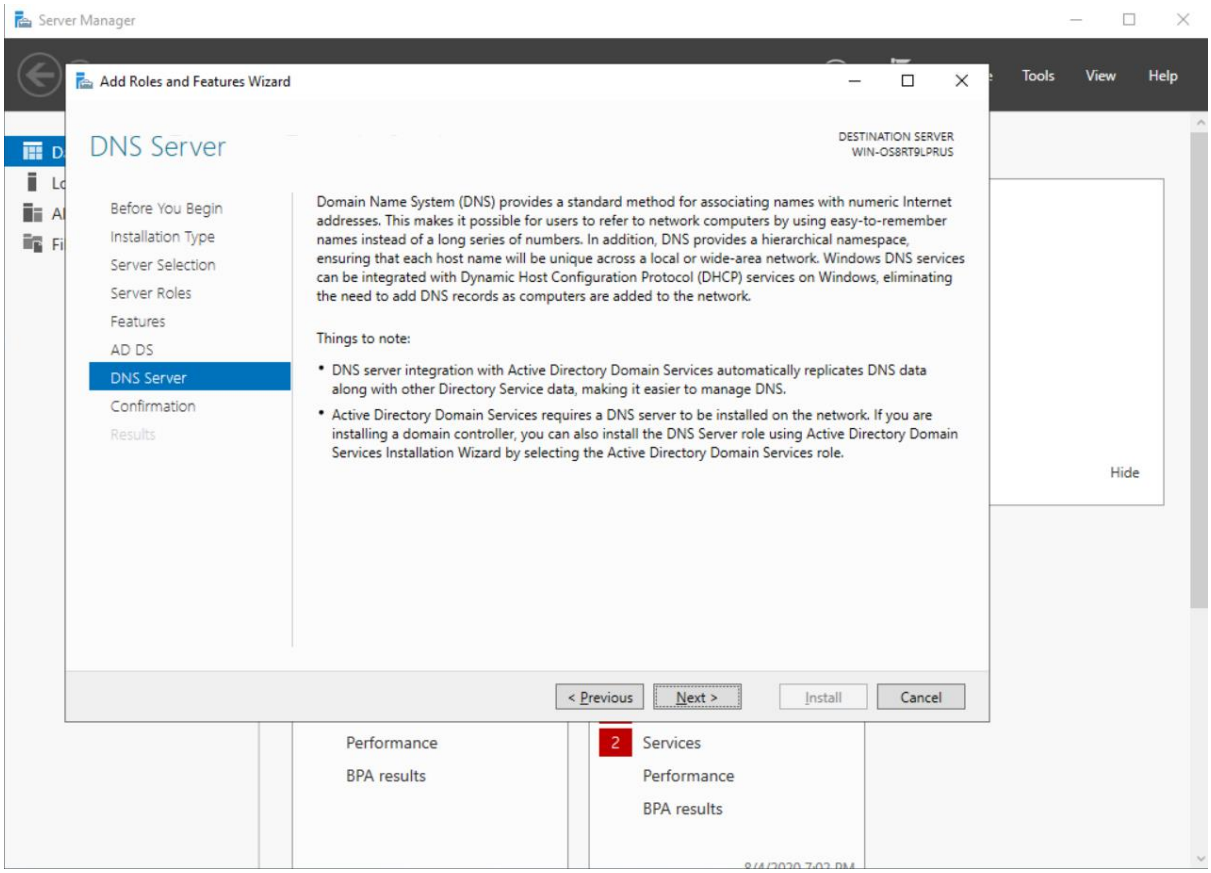
7. Click "Next".



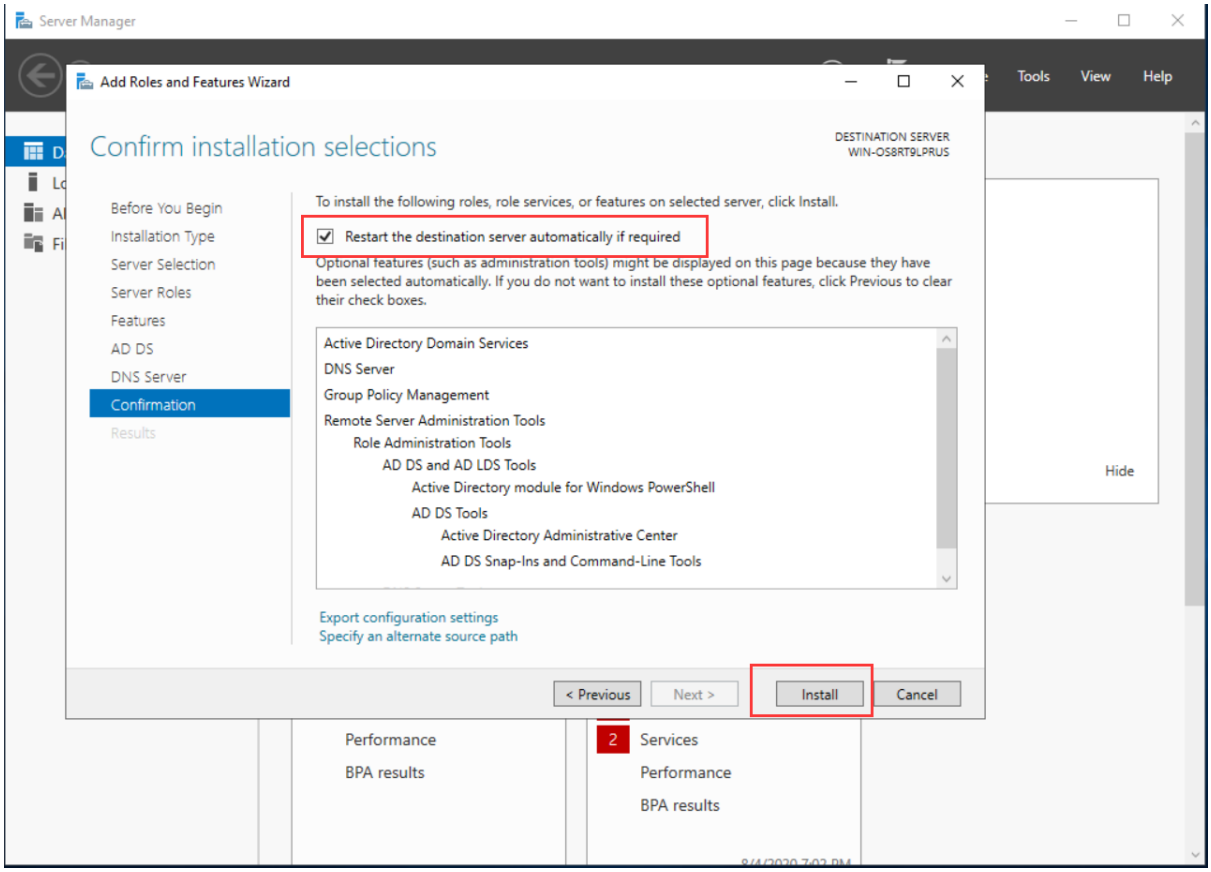
8. Click "Next".

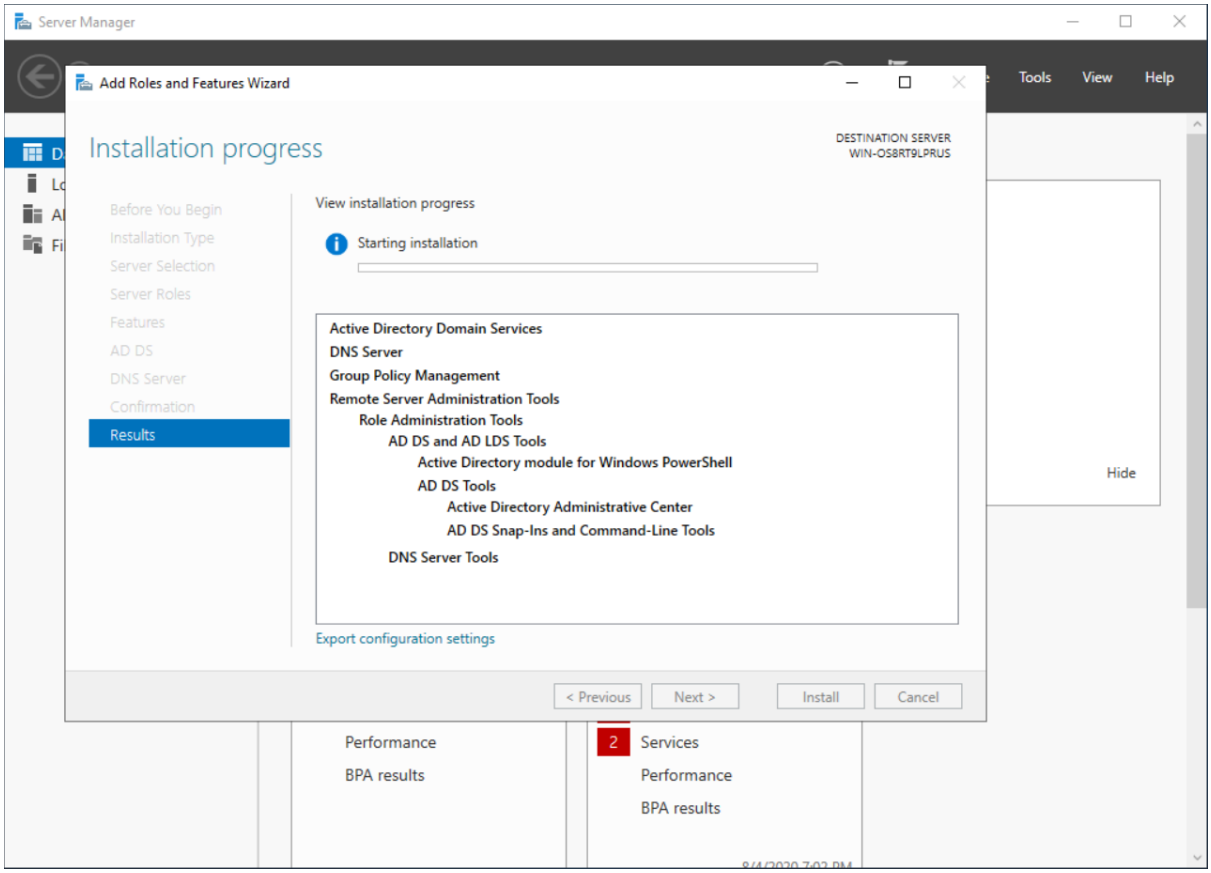


9. Click "Next".

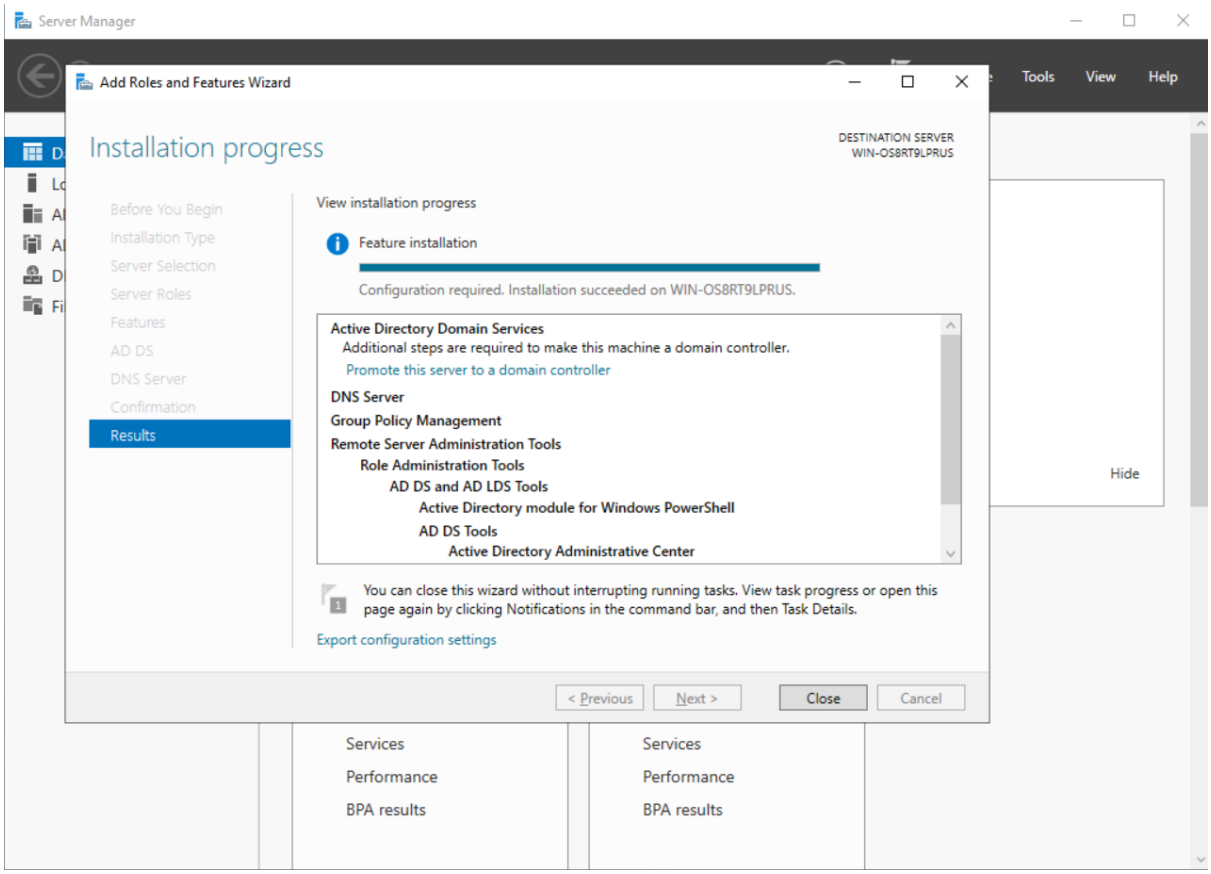


10. Click "Install".



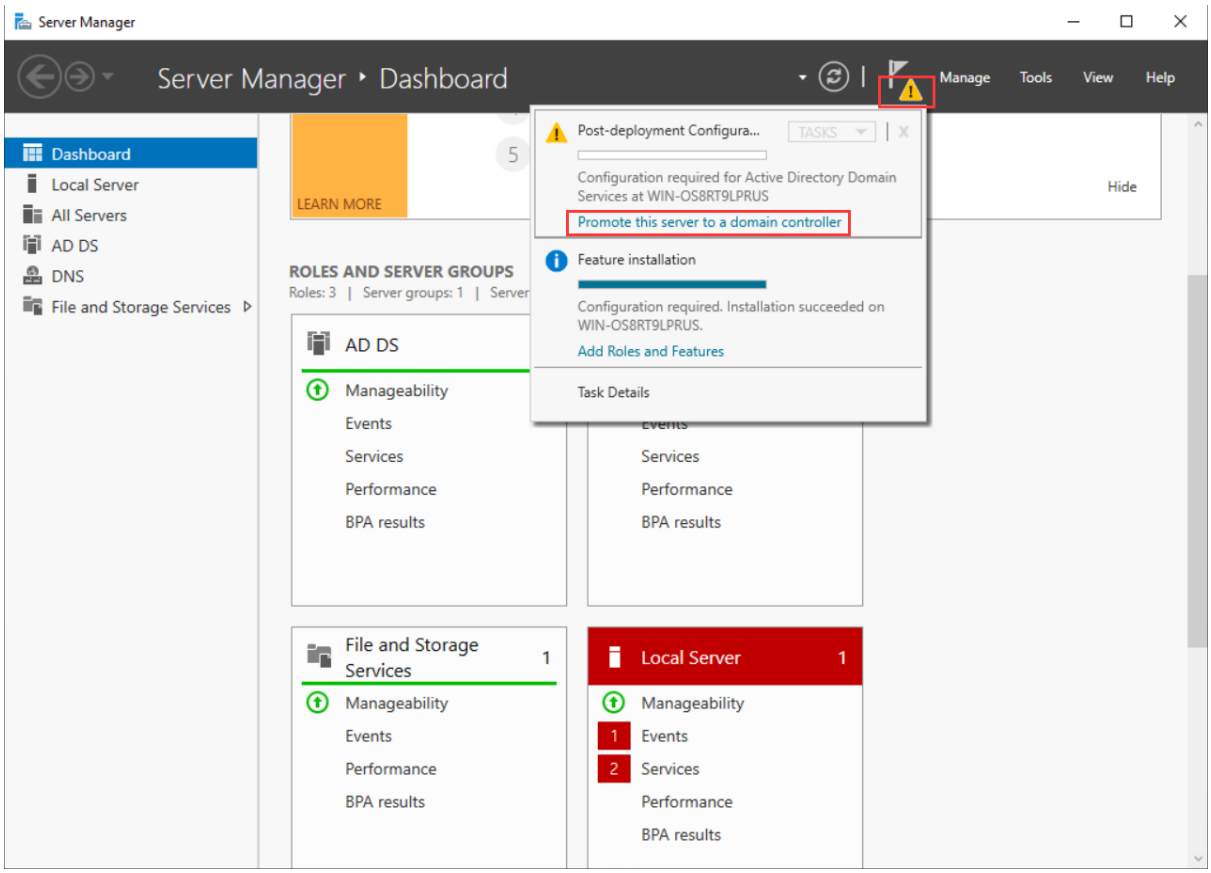


11. Click "Close" after installation.

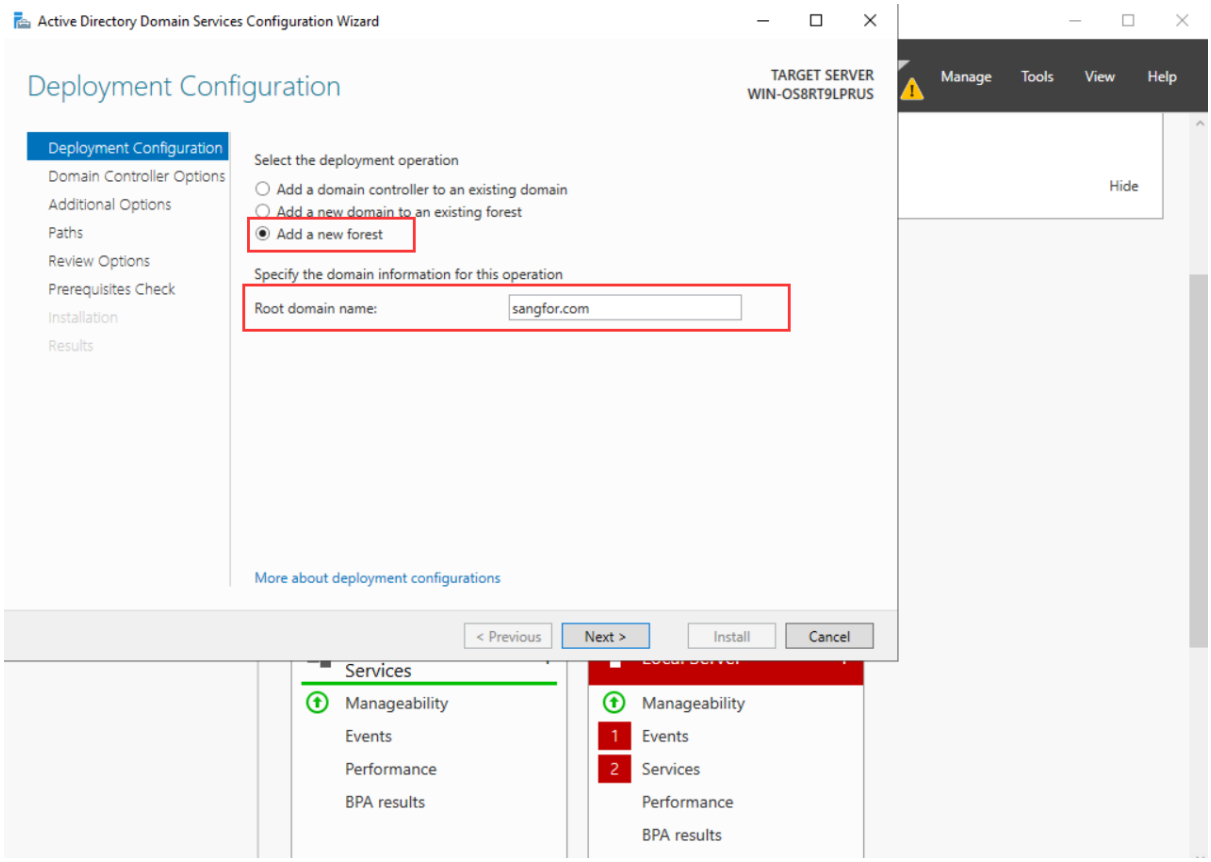


2.2 Configure the domain controller server

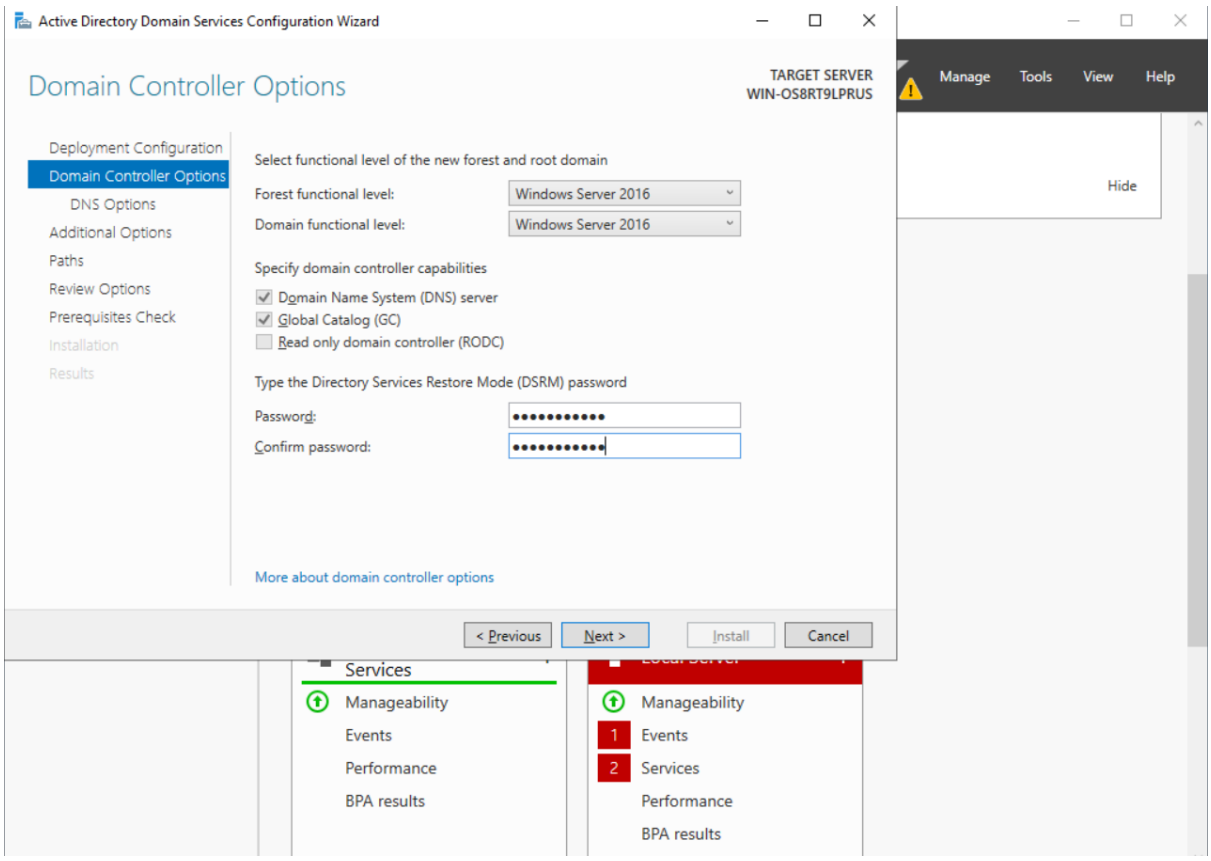
1. According to the following figure, select "Promote this server to a domain controller".



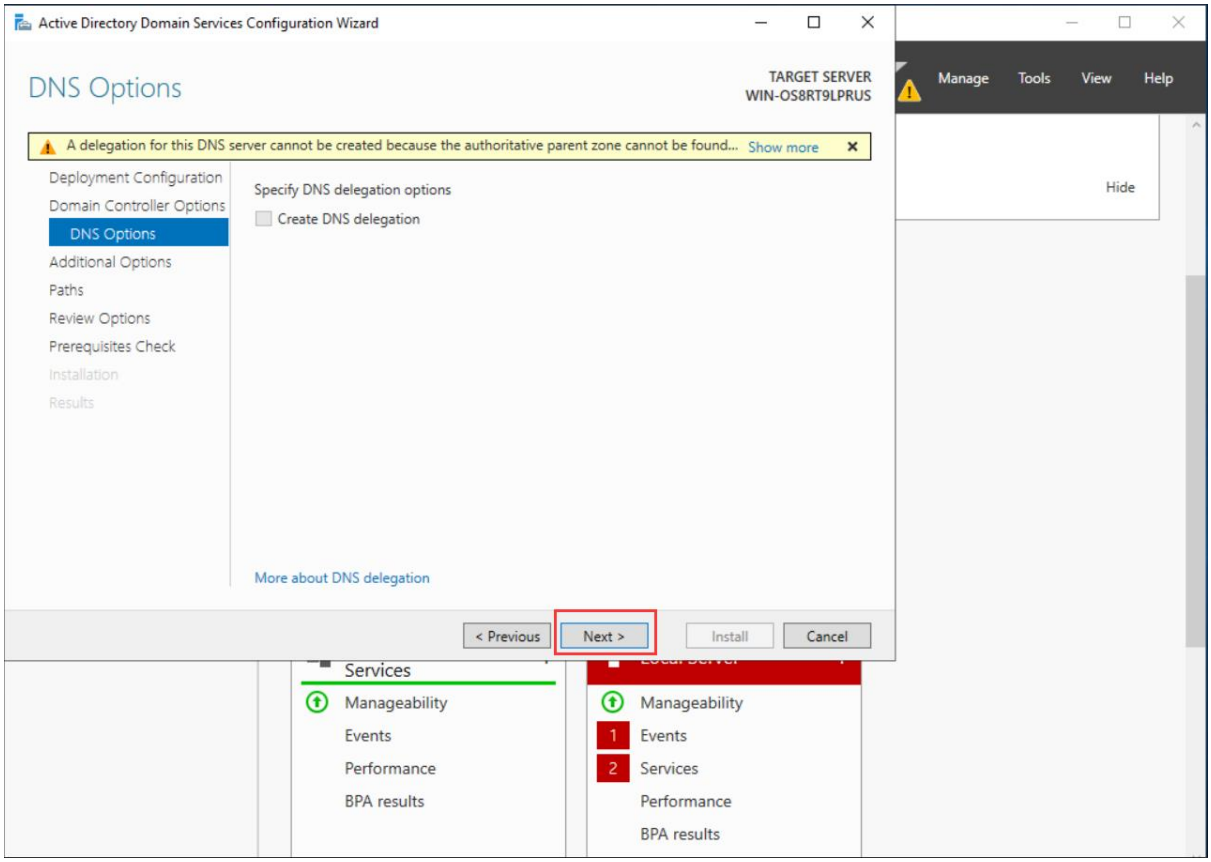
2. Configure the domain name for the AD domain, such as sangfor.com.



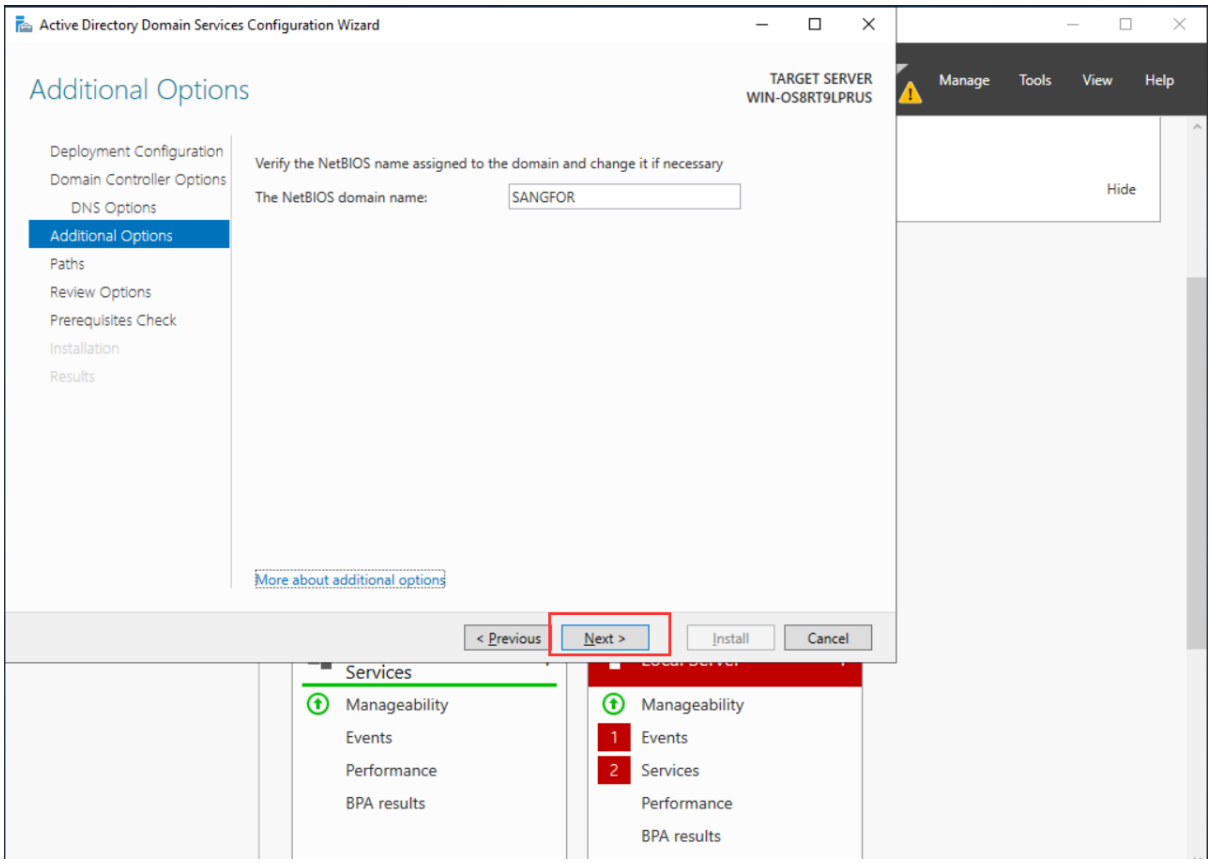
3. Set a password, for example @sangfortest.



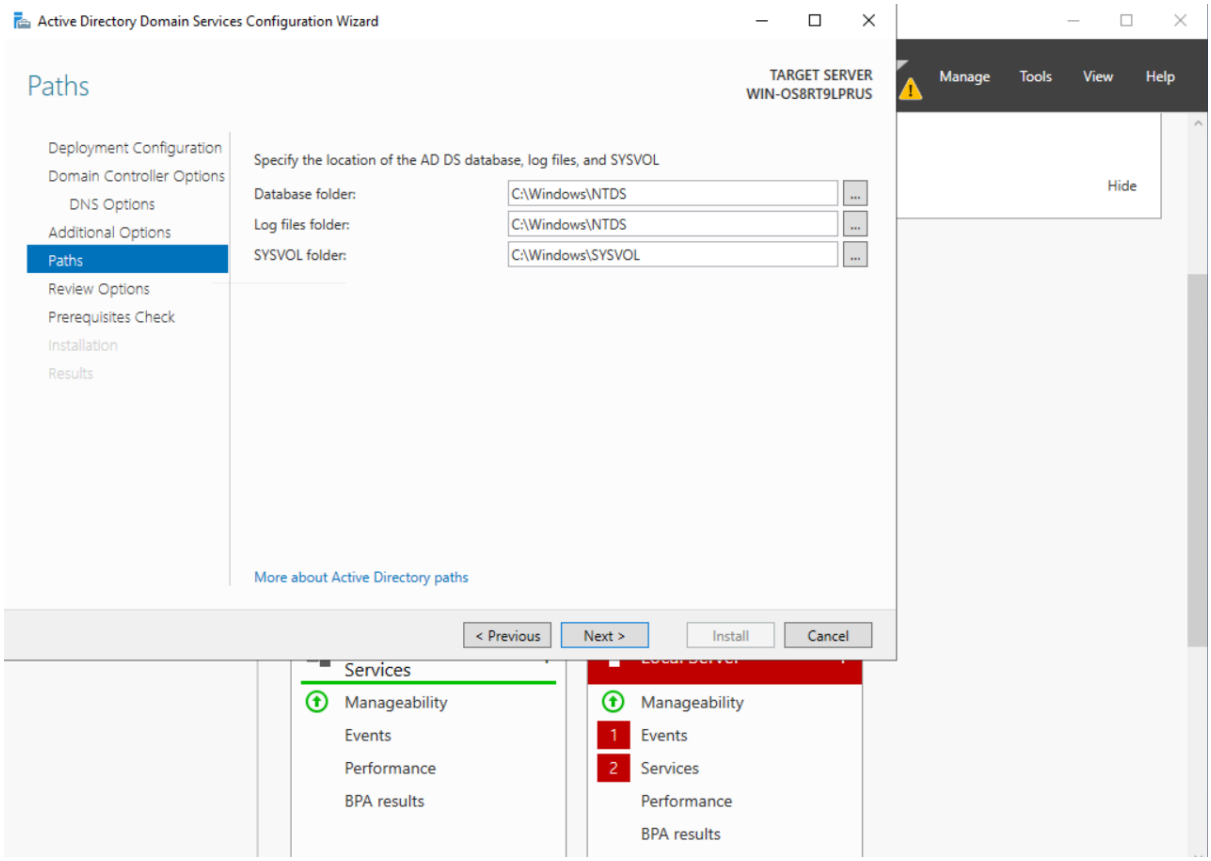
4.Click "Next".



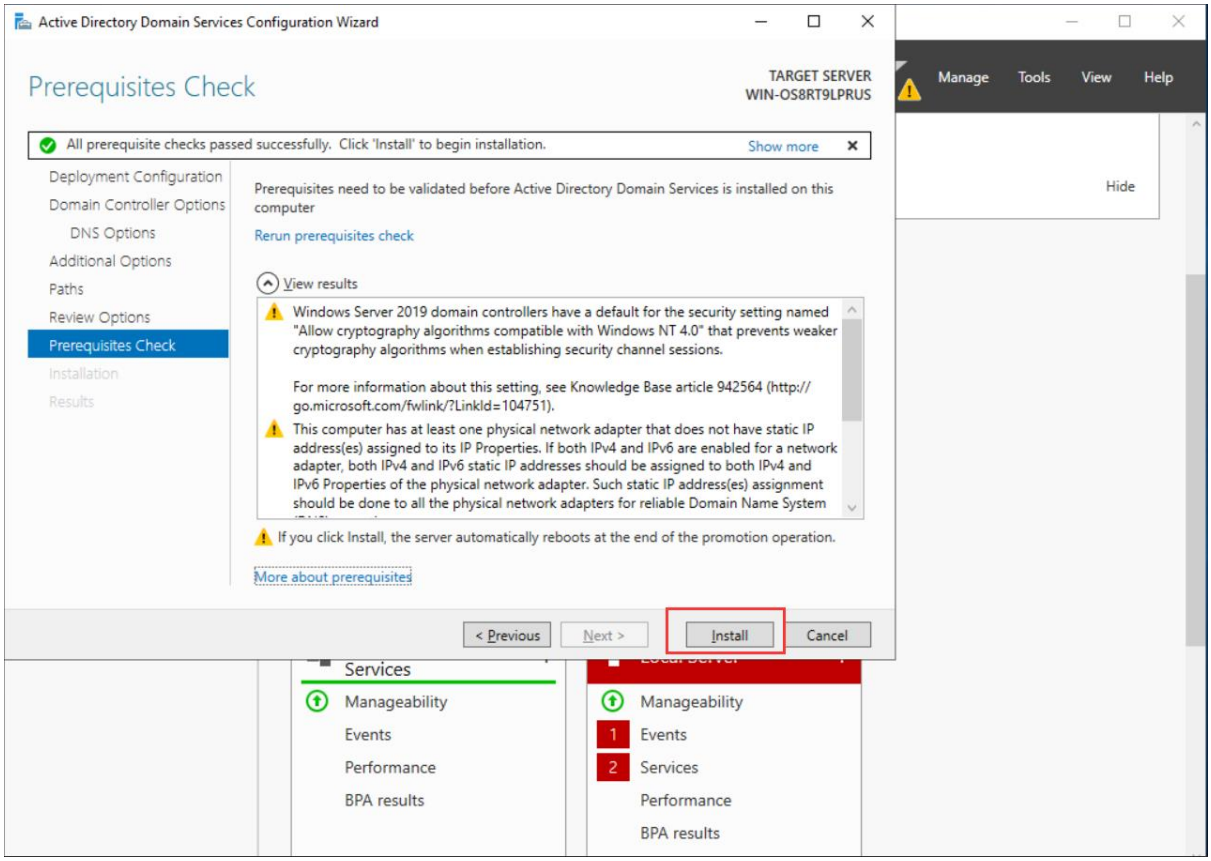
5. Set NETBIOS Domain Name, you can use the default SANGFOR.



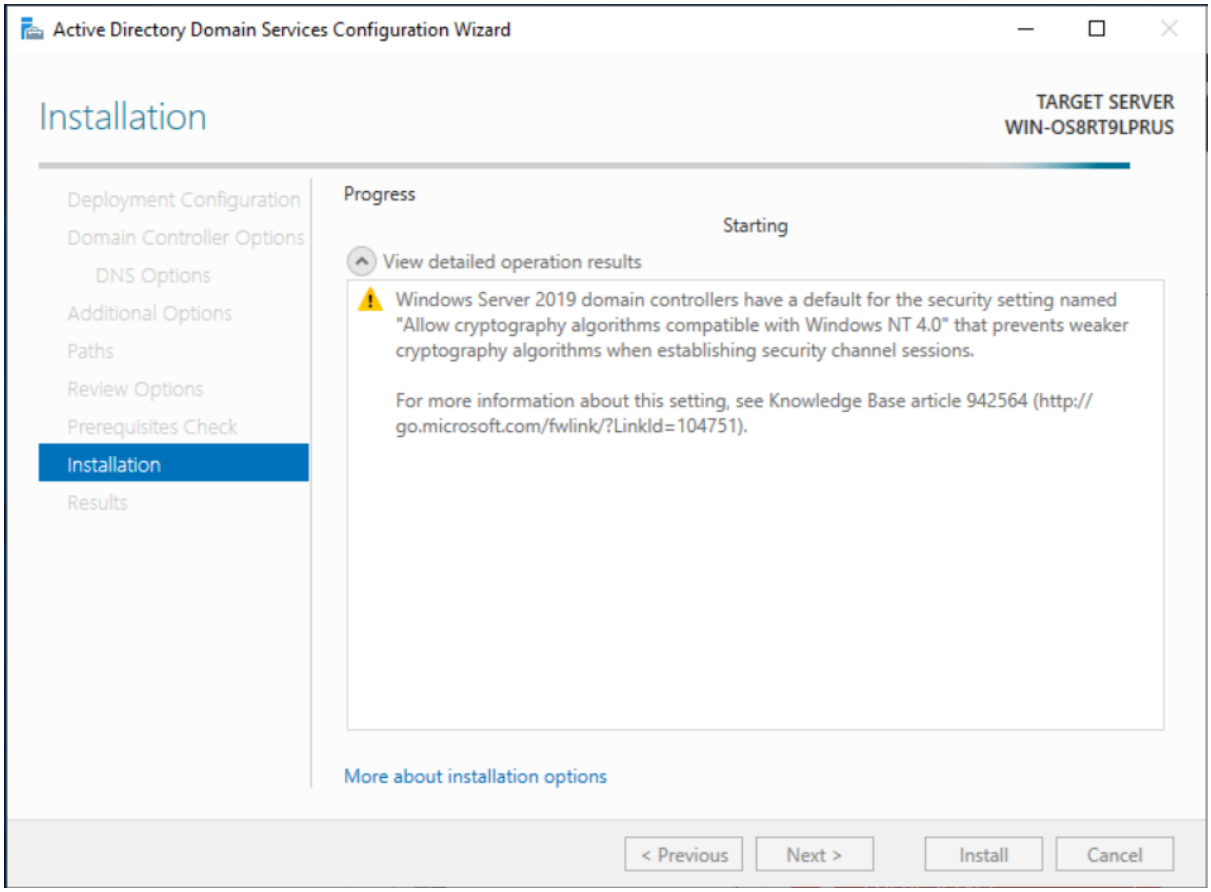
6.Click "Next".



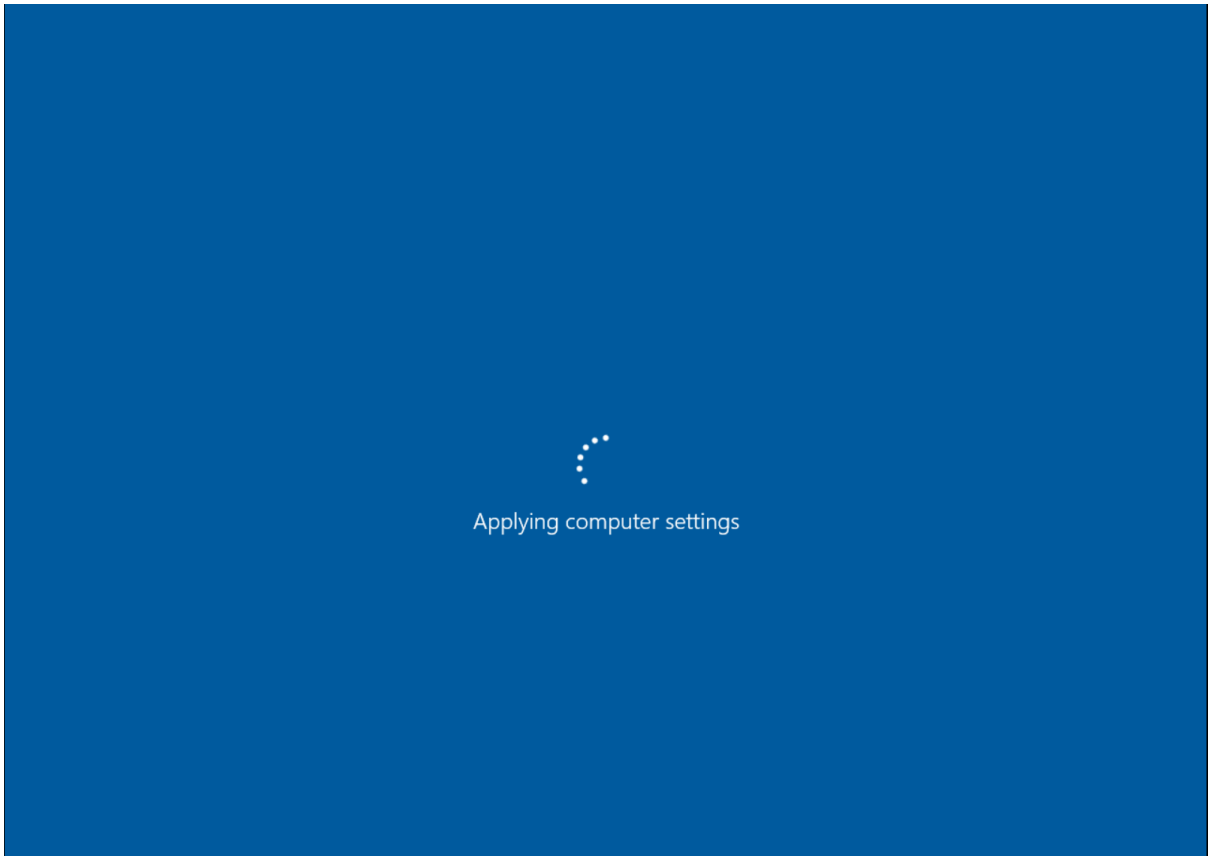
7.Select "Install".



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

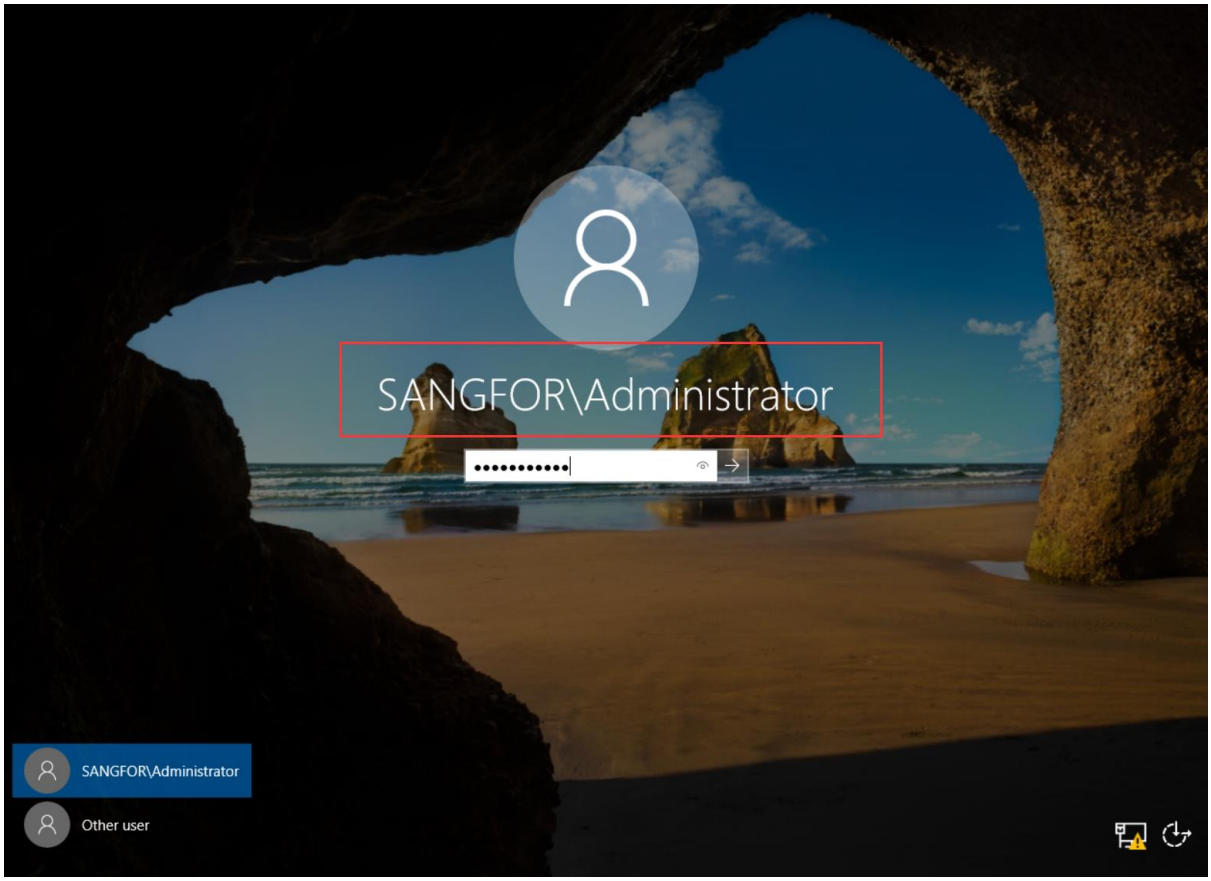


9. After the installation is complete, Windows Server will automatically restart.



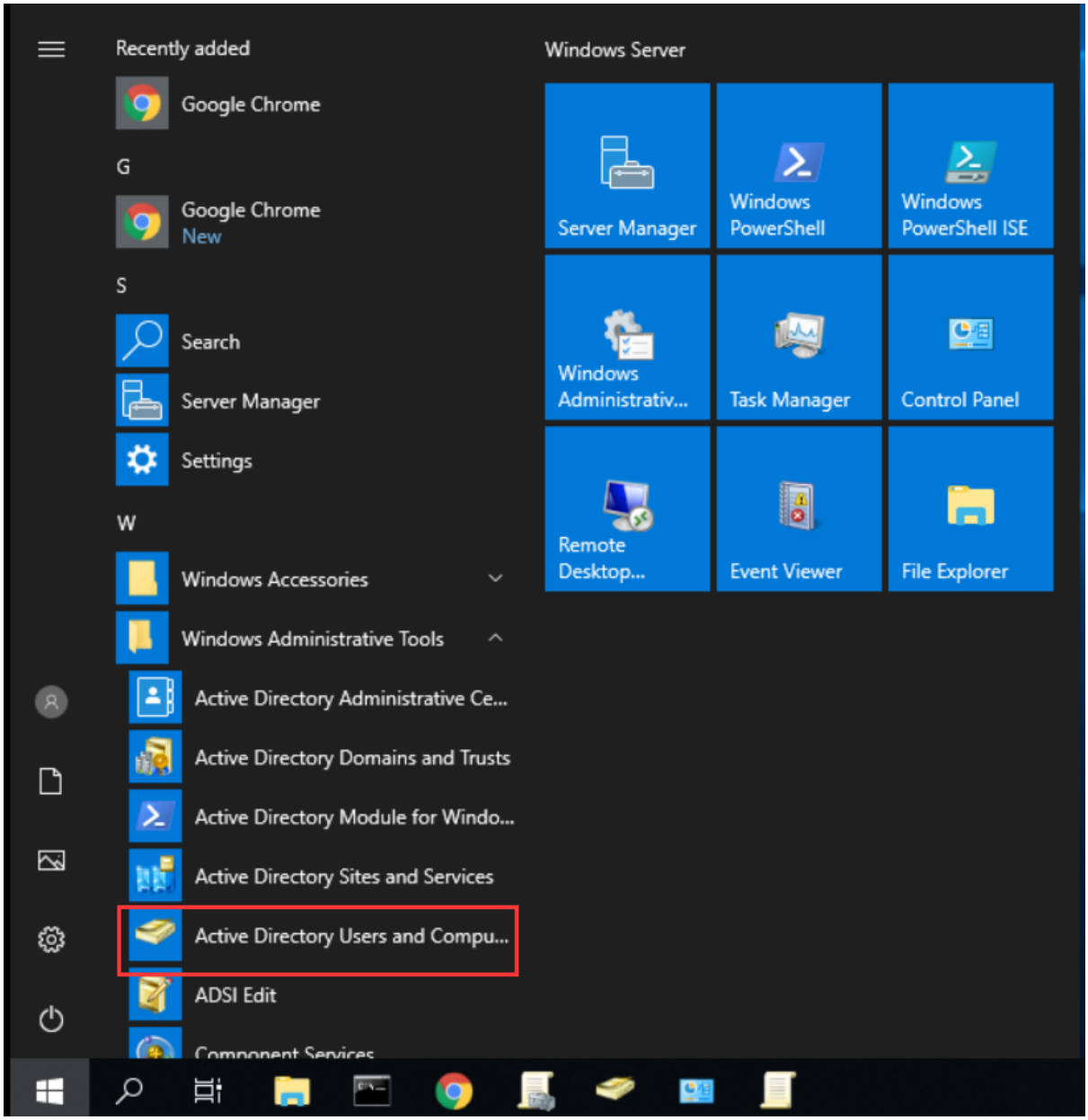
10. After the Windows Server restarts, you can see on the login page that the default local administrator

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.

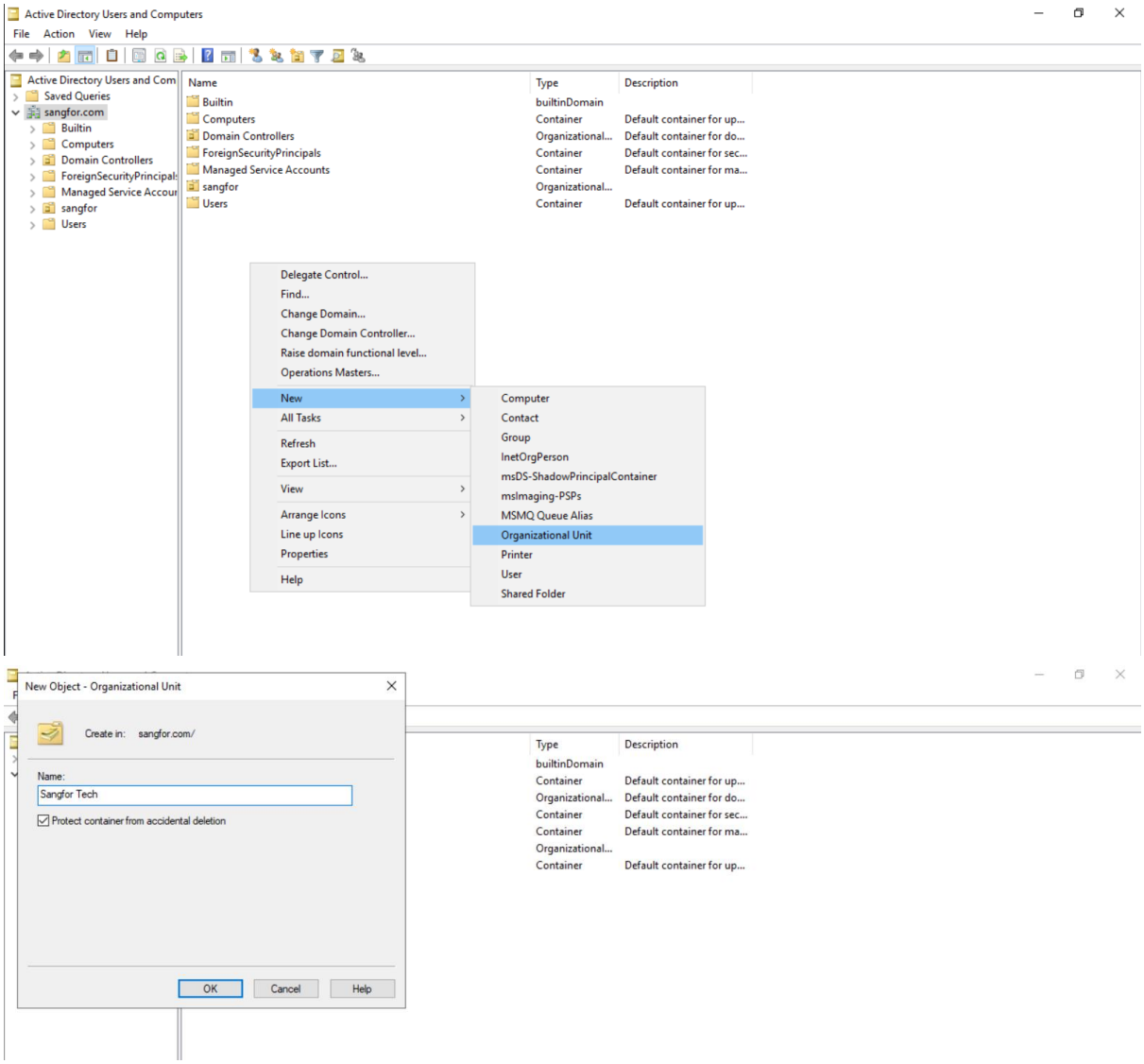


2.3 Create usernames and passwords for other users in the domain

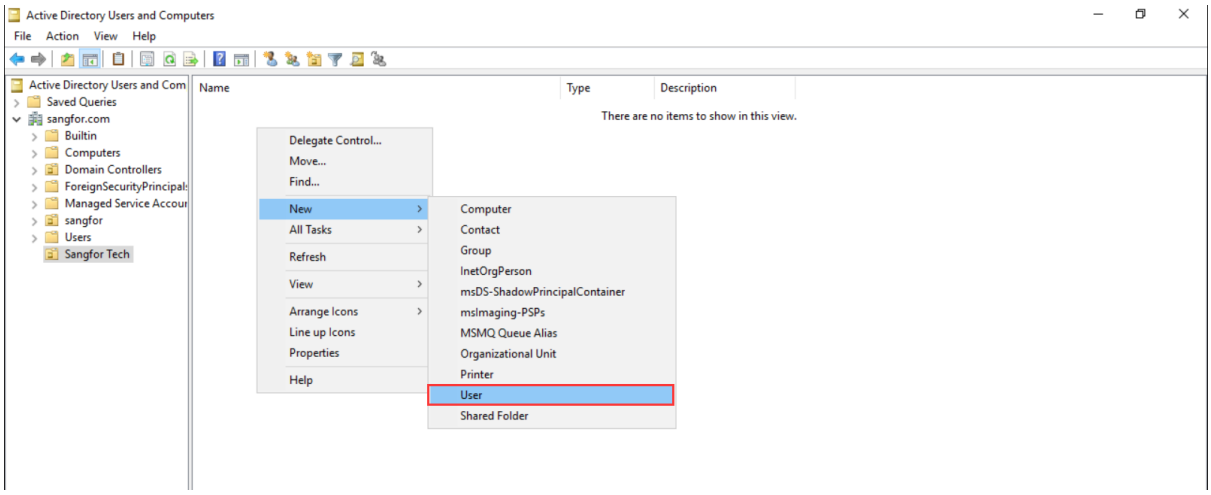
1.Open "Active Directory Users and Computers".

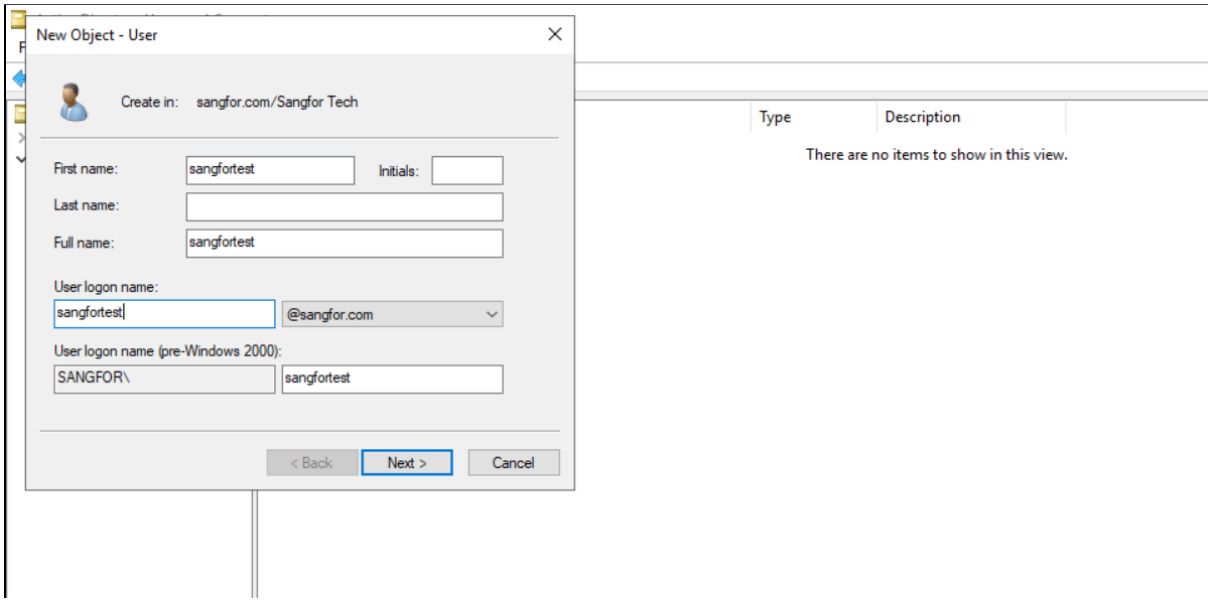


2. In order to facilitate the management of users according to the company's organizational structure, a logical container is created here to represent a department. For example, create a department called Sangfor Tech.

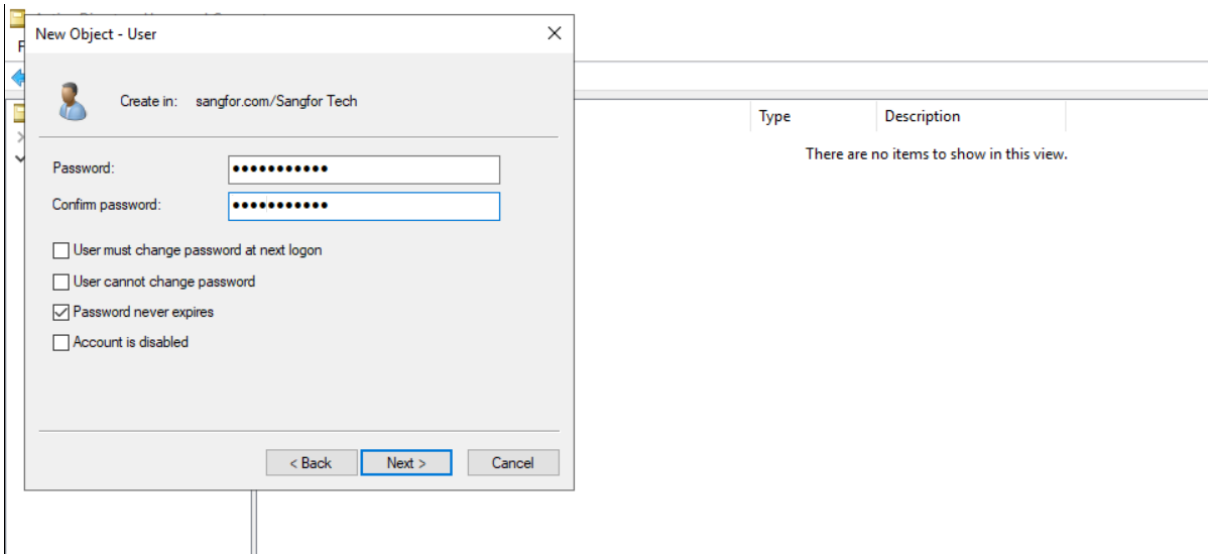


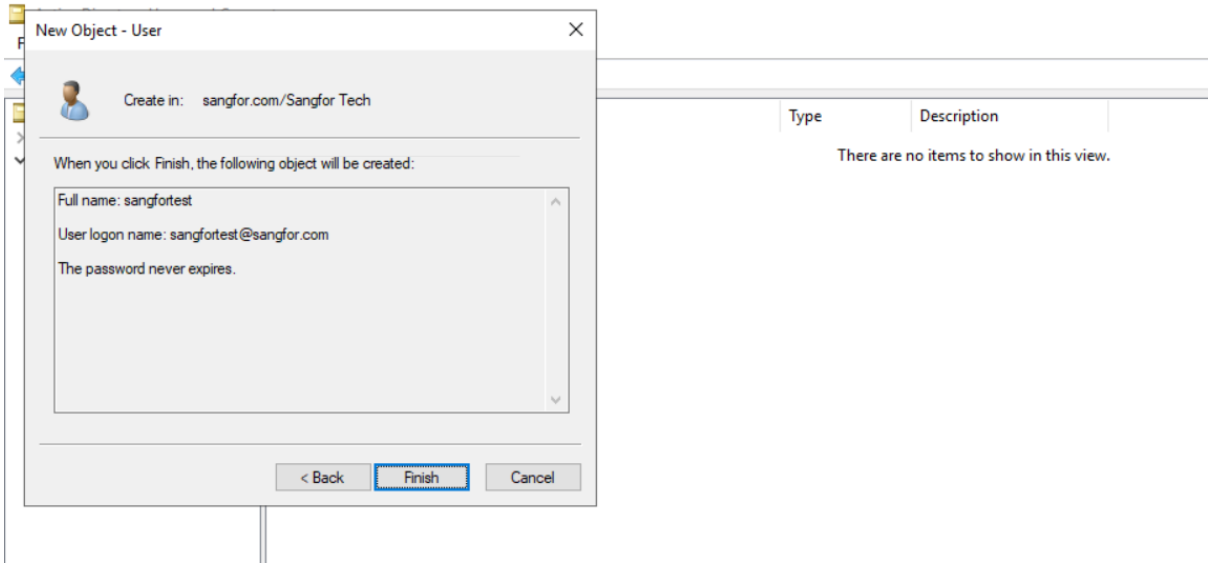
3. Create a user in the container, for example called sangfortest.





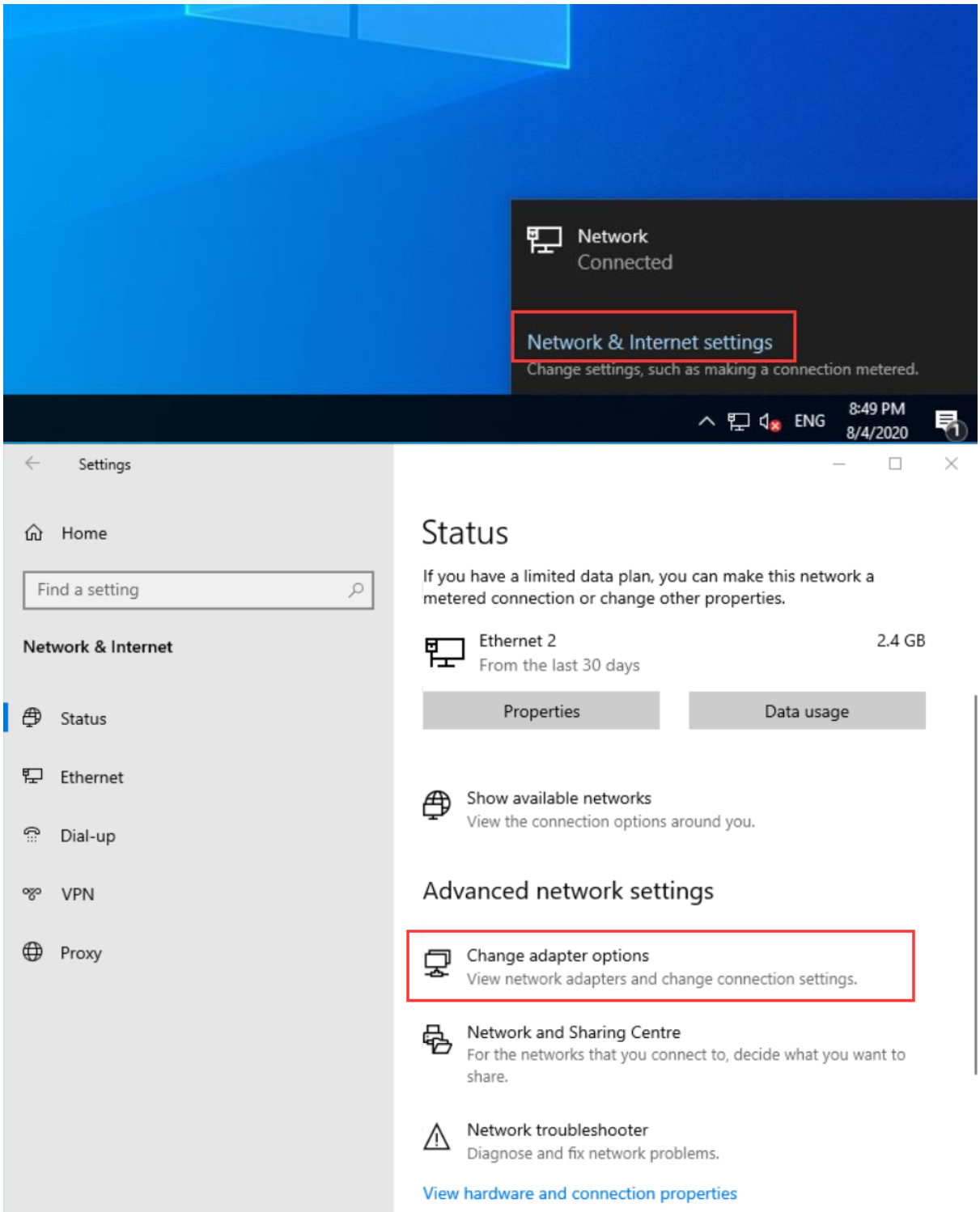
Set a login password for this user.

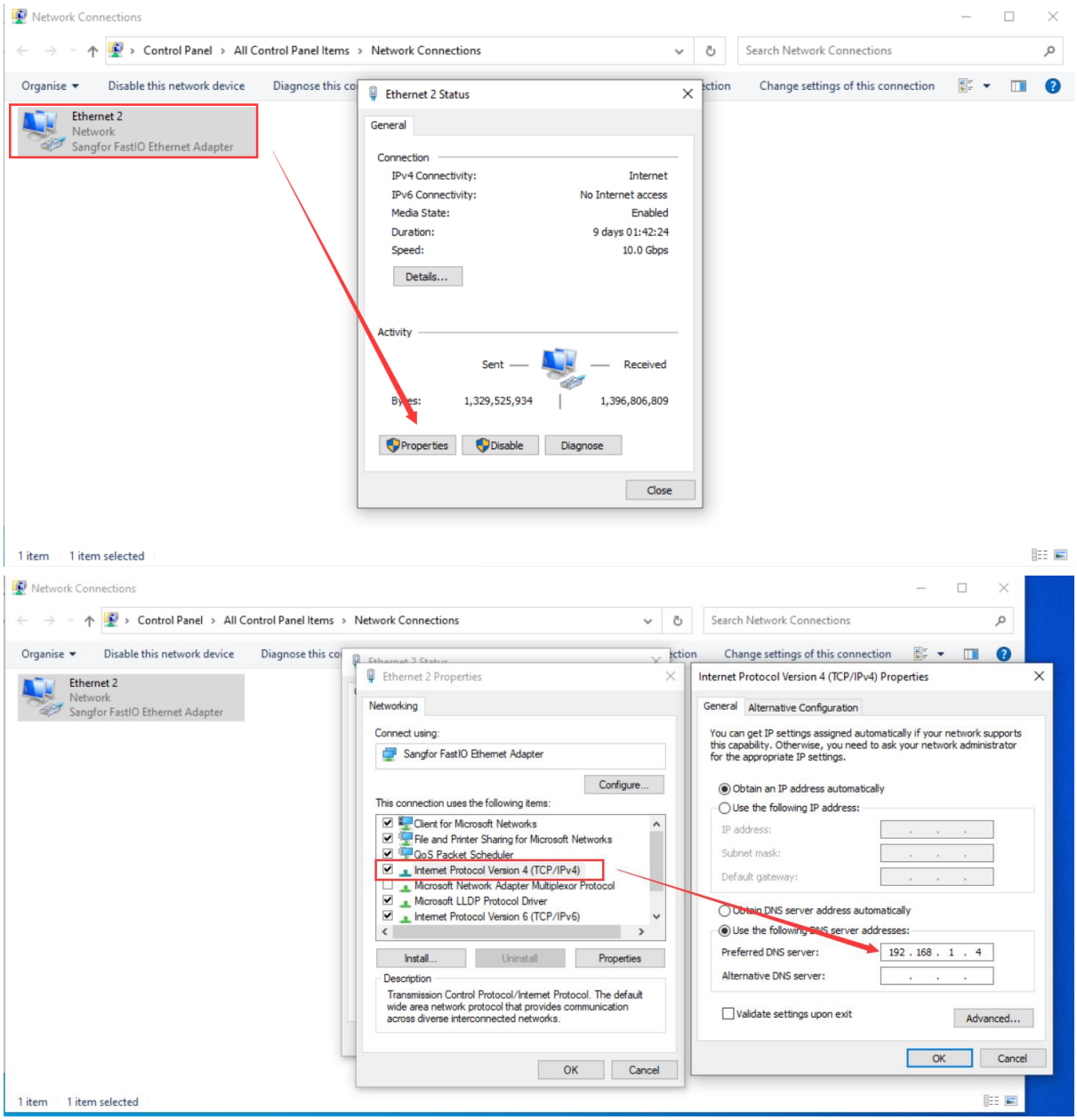




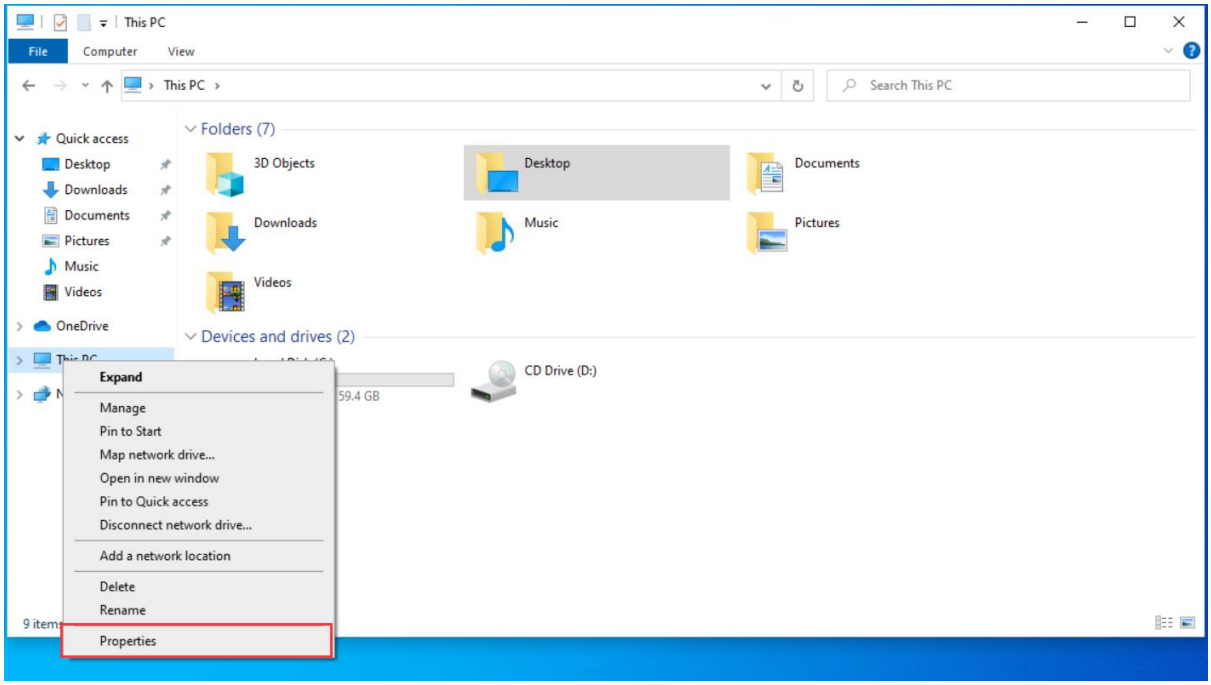
2.4 Join the PC to the domain

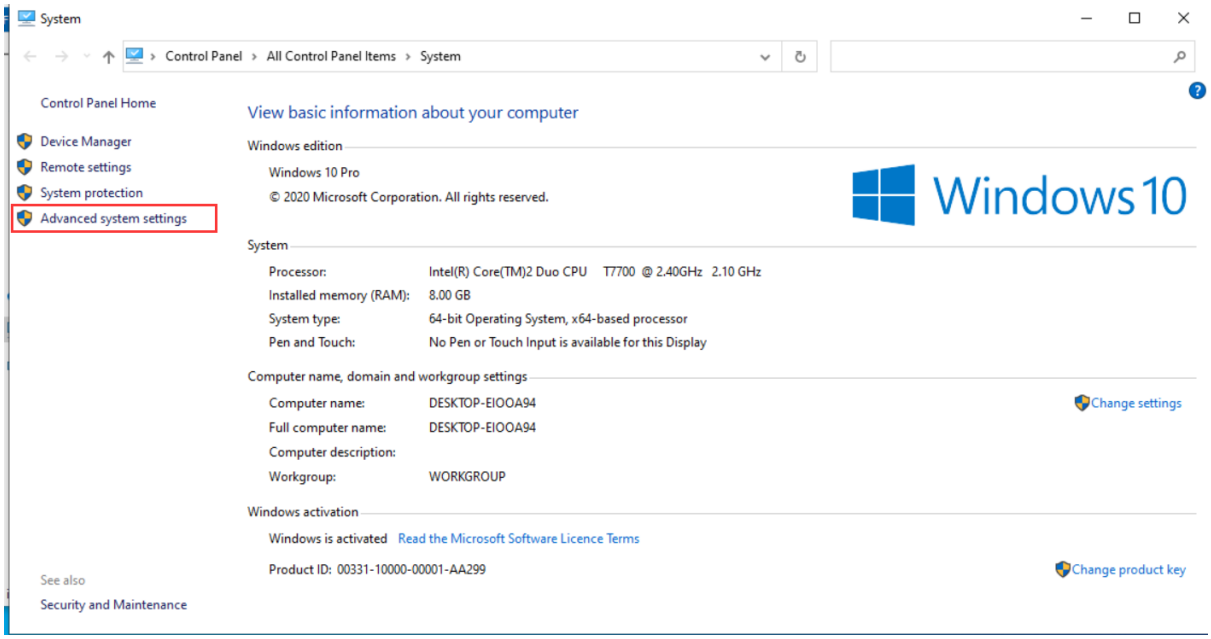
1. Configure the PC's network card, and configure DNS as the IP of the domain control server: 192.168.1.4.

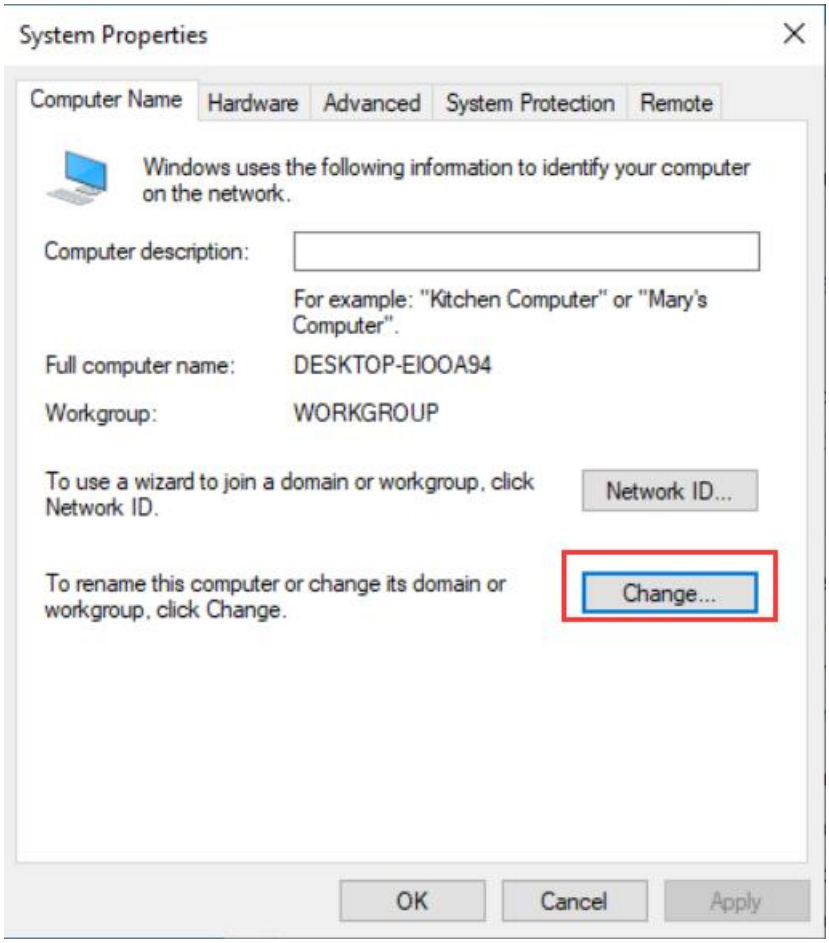


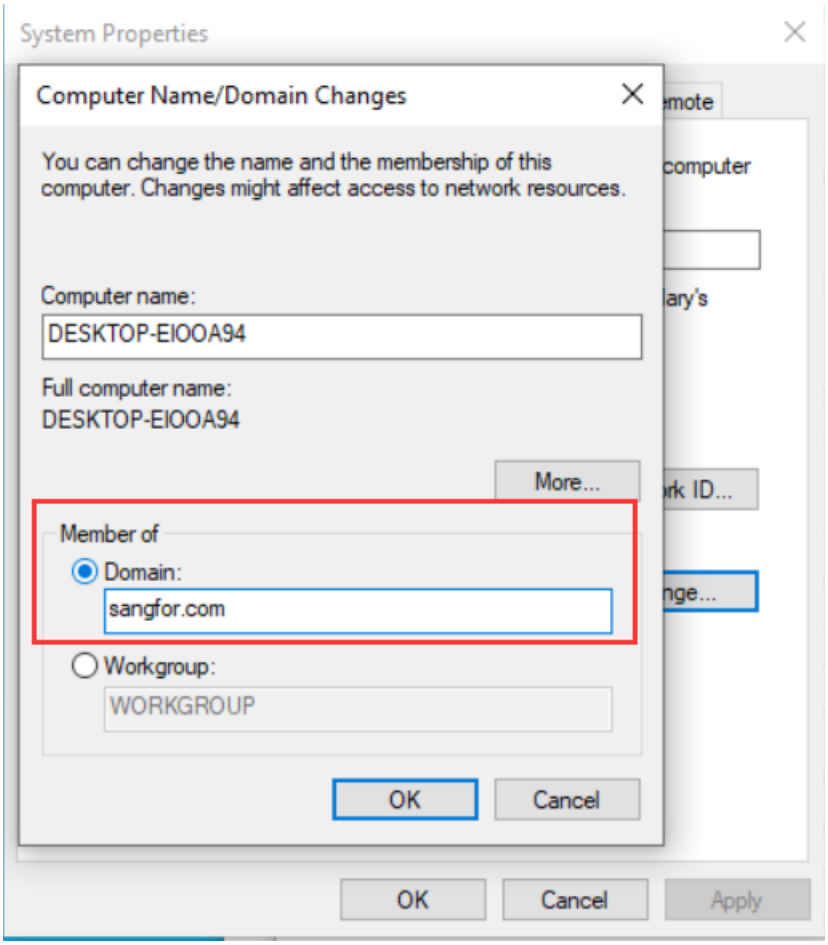


2. Join the PC to the domain.

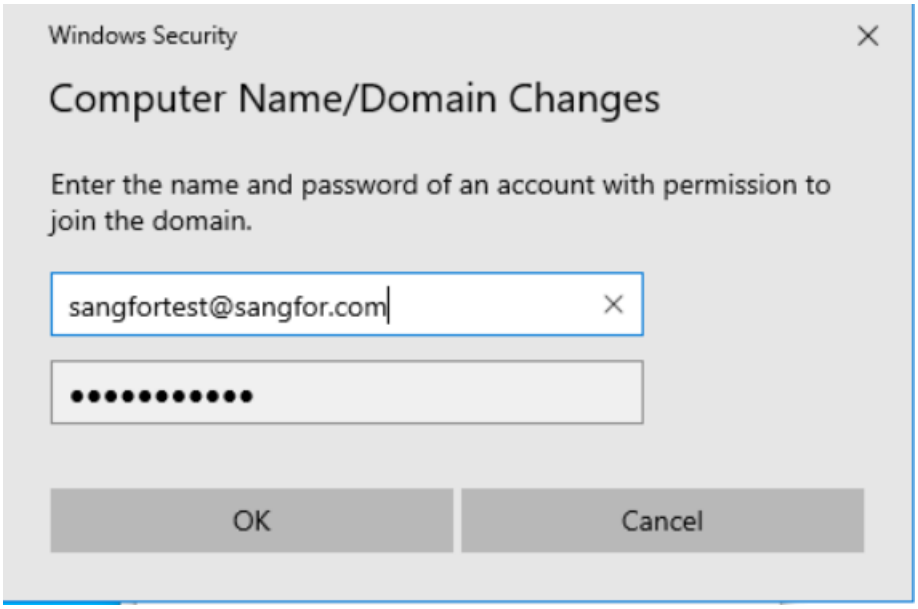

This PC
File
Computer
View
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (2)
CD Drive (D:)
59.4 GB
Expand
Manage
Pin to Start
Map network drive...
Open in new window
Pin to Quick access
Disconnect network drive...
Add a network location
Delete
Rename
Properties


System
Control Panel
All Control Panel Items
System
Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
View basic information about your computer
Windows edition
Windows 10 Pro
© 2020 Microsoft Corporation. All rights reserved.
Windows 10
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: No Pen or Touch Input is available for this Display
Computer name, domain and workgroup settings
Computer name: DESKTOP-EIOOA94
Full computer name: DESKTOP-EIOOA94
Computer description:
Workgroup: WORKGROUP
Change settings
Windows activation
Windows is activated Read the Microsoft Software Licence Terms
Product ID: 00331-10000-00001-AA299
Change product key
See also
Security and Maintenance

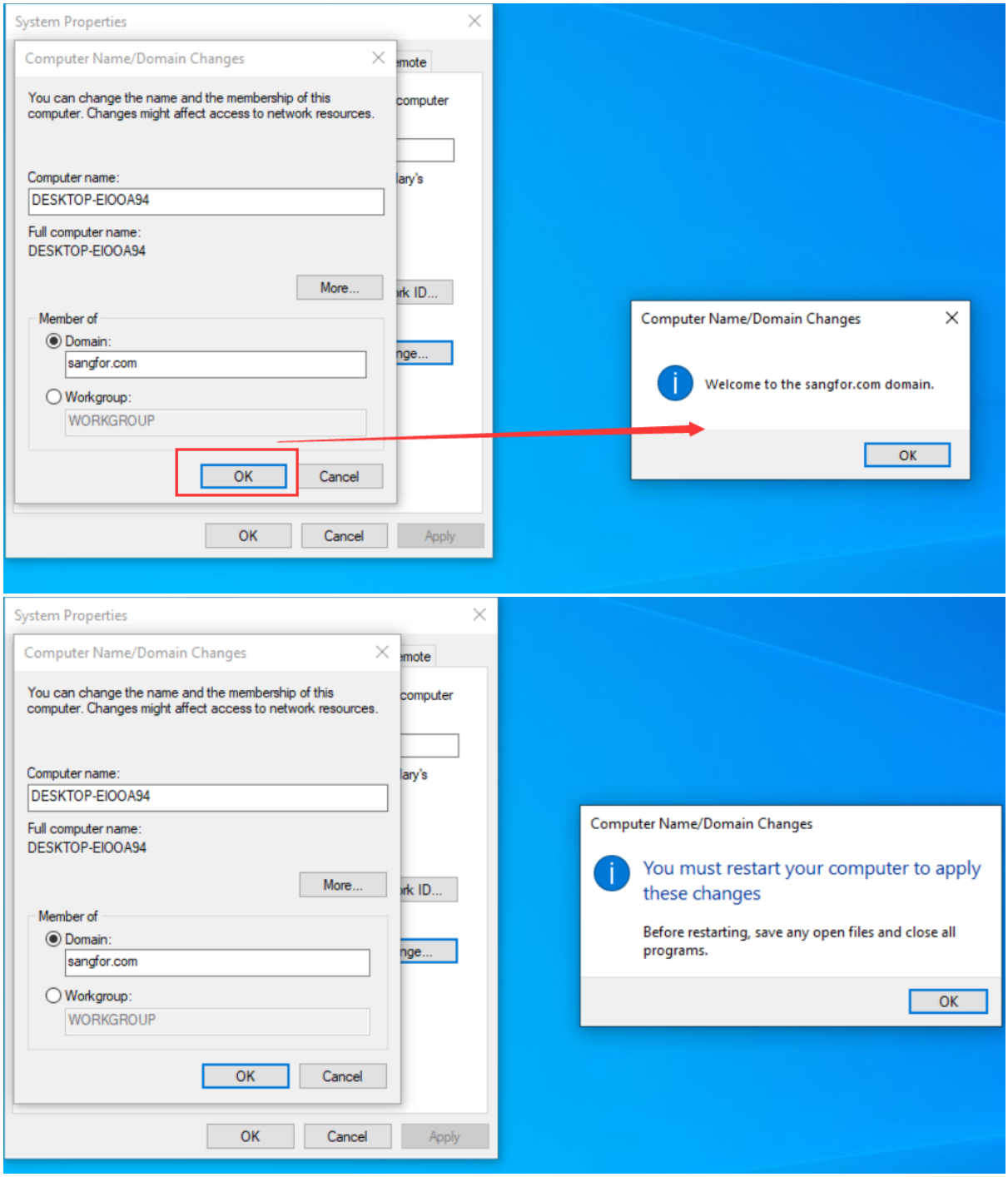

System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "Kitchen Computer" or "Mary's Computer".
Full computer name:
DESKTOP-EIOOA94
Workgroup:
WORKGROUP
To use a wizard to join a domain or workgroup, click Network ID.
Network ID...
To rename this computer or change its domain or workgroup, click Change.
Change...
OK
Cancel
Apply

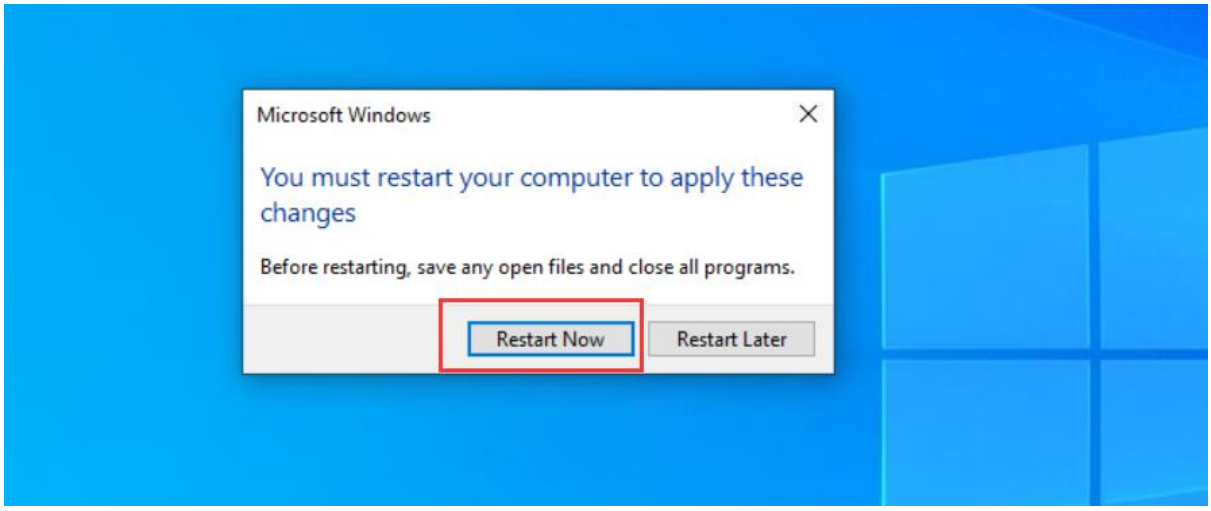


3. In the process of joining the domain, you need to verify your identity, just use the sangfortest user created on the AD domain control 192.168.1.4 for testing.

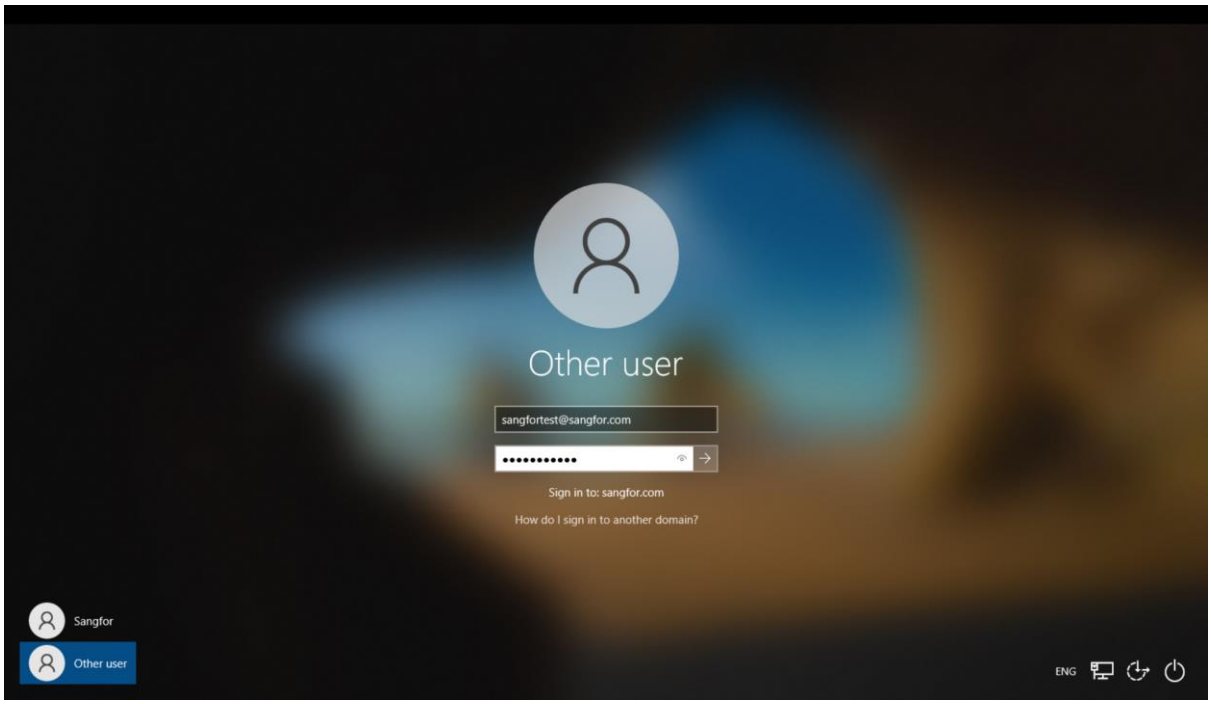


4. After successfully joining the domain, you need to restart the PC.


System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
DESKTOP-EIOOA94
Full computer name:
DESKTOP-EIOOA94
More...
Member of
Domain:
sangfor.com
Workgroup:
WORKGROUP
OK
Cancel
OK
Cancel
Apply
Computer Name/Domain Changes
Welcome to the sangfor.com domain.
OK
System Properties
Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
DESKTOP-EIOOA94
Full computer name:
DESKTOP-EIOOA94
More...
Member of
Domain:
sangfor.com
Workgroup:
WORKGROUP
OK
Cancel
OK
Cancel
Apply
Computer Name/Domain Changes
You must restart your computer to apply these changes
Before restarting, save any open files and close all programs.
OK



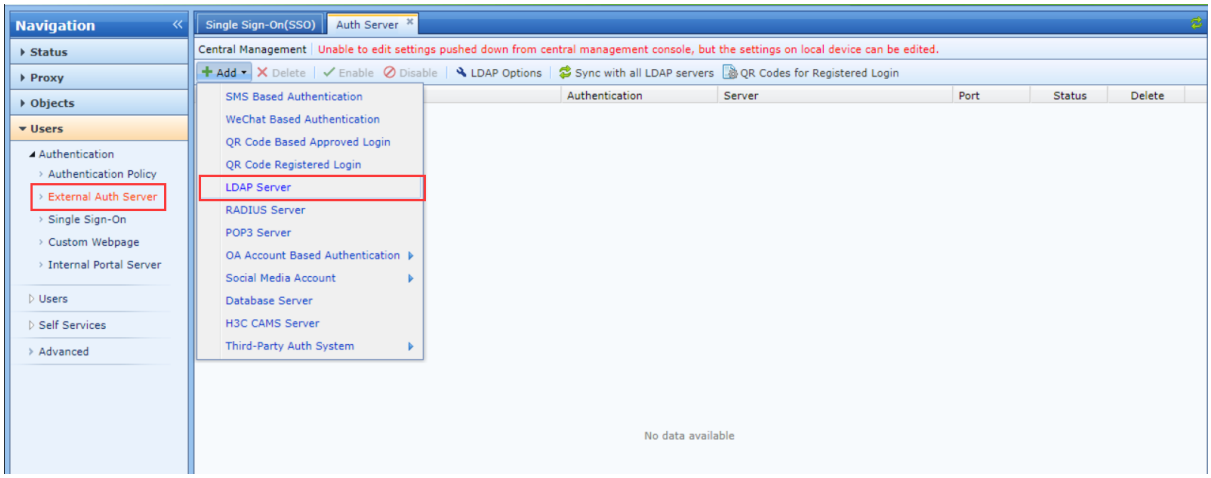
5. After restarting, you can see the login page of the PC, choose to use the domain account sangfortest to log in.



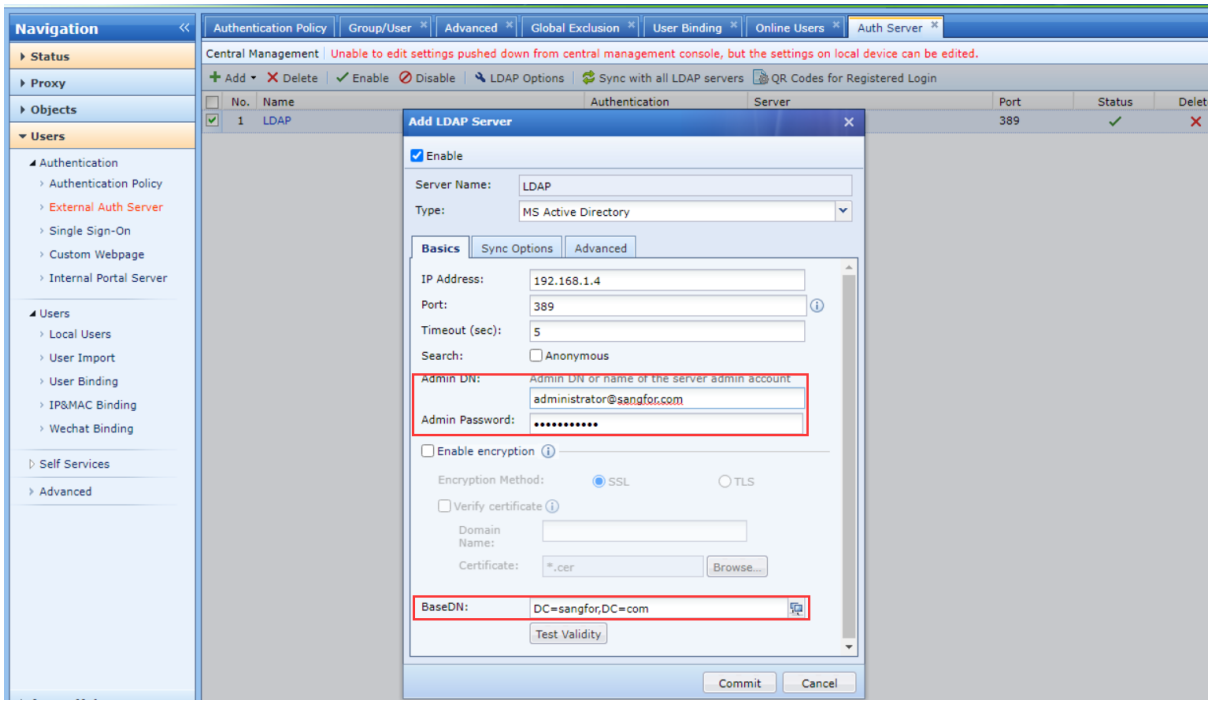
Chapter 3 How to Configure IAM

3.1 Add LDAP server

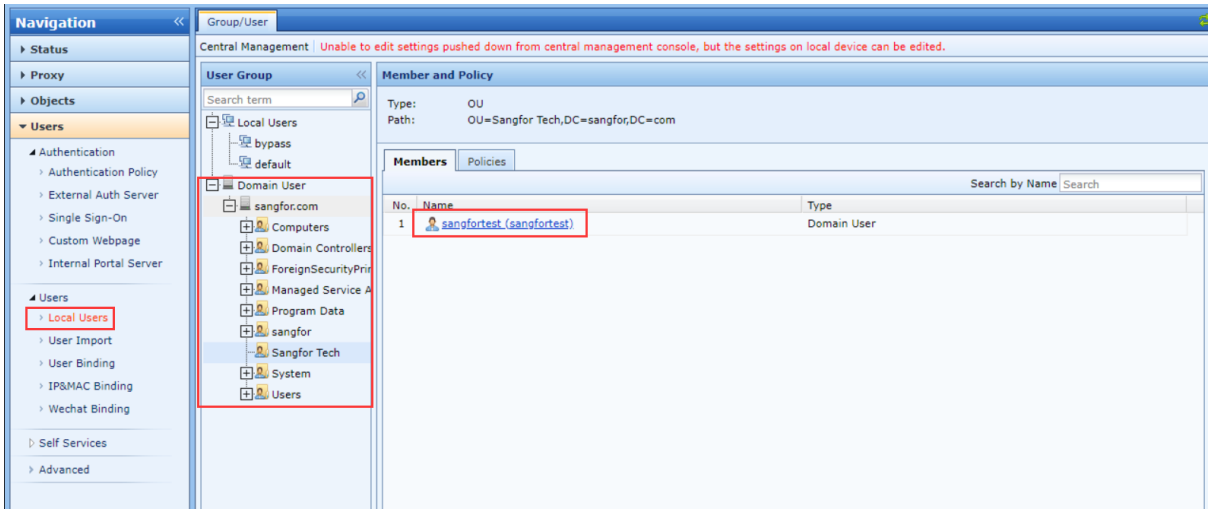
1. Add Microsoft AD server on IAM.



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.

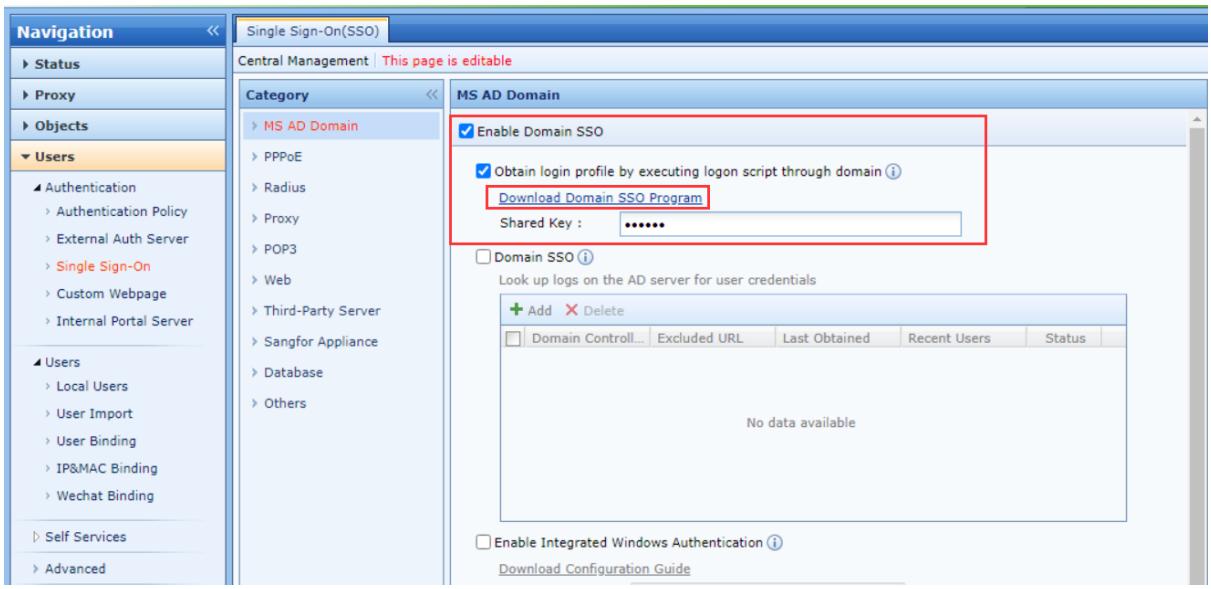


3. If IAM and AD can interact normally, then in the local user, you can see that IAM has obtained the domain user information of the AD server, including the sangfortest user we created before.

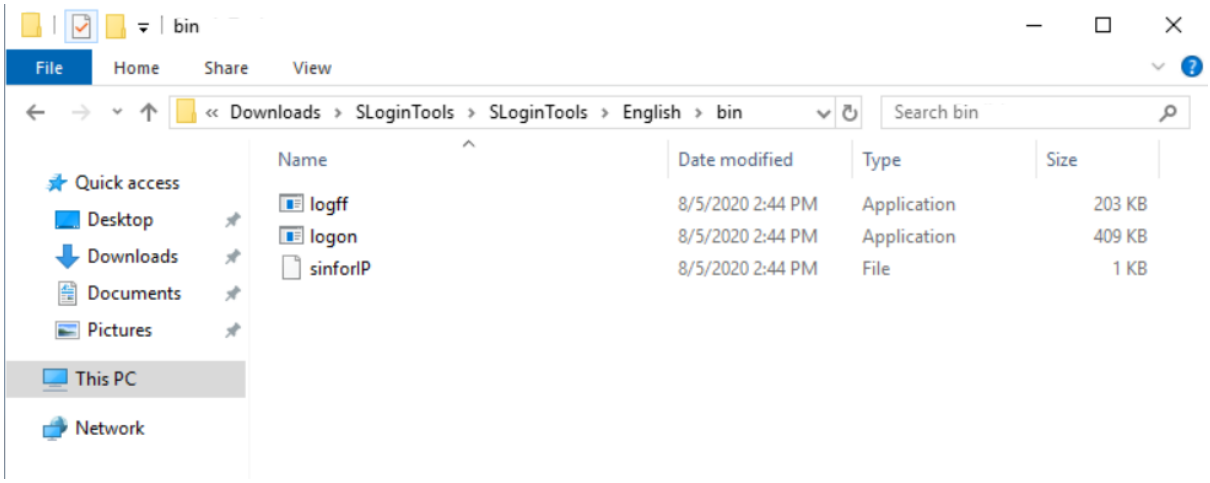


3.2 Configure script SSO on IAM and AD Server

1. Turn on "Domain SSO" and turn on script SSO. Here you need to configure a shared secret key for authentication, for example, it is set to 123456.

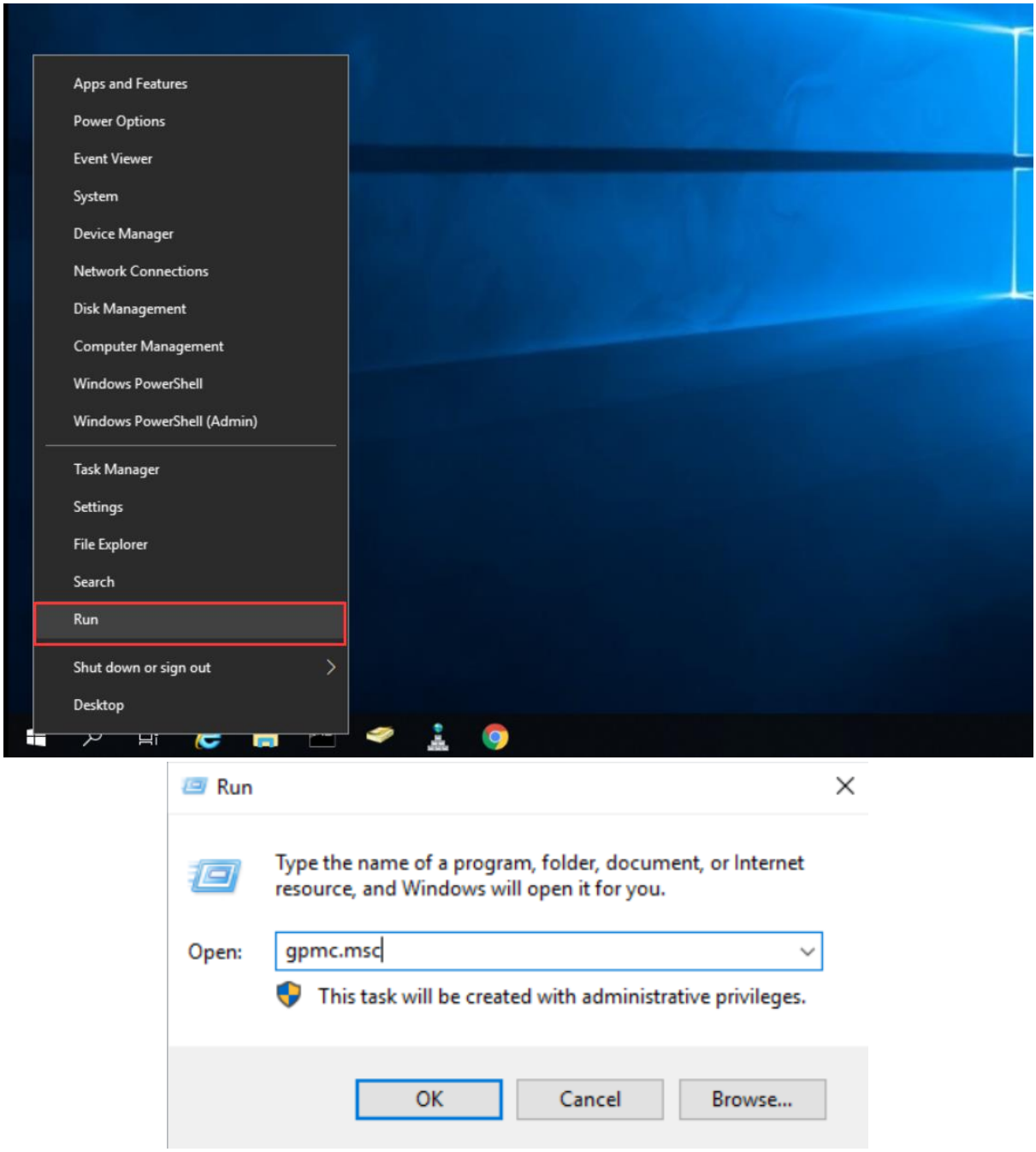


2. Download the program from the page, including the login script and logout script.

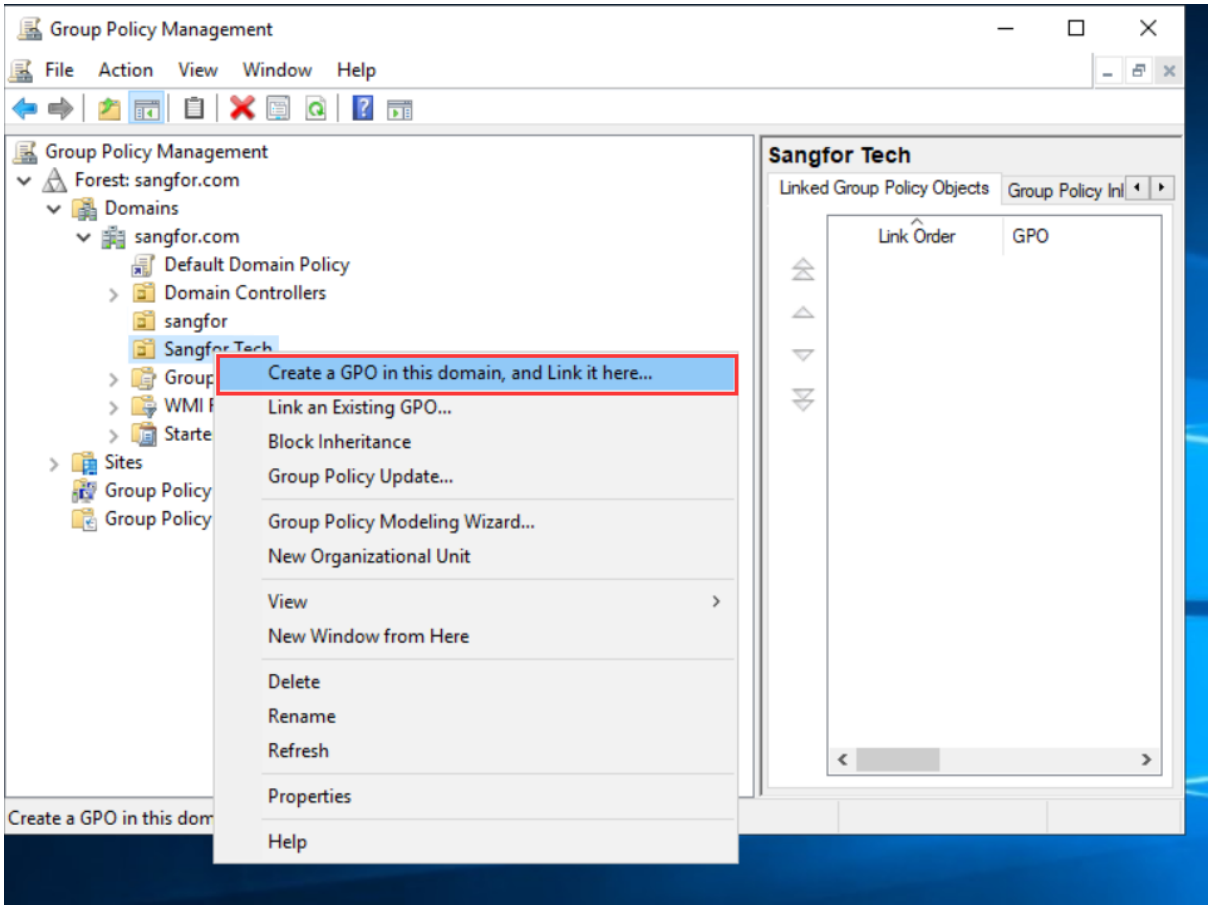


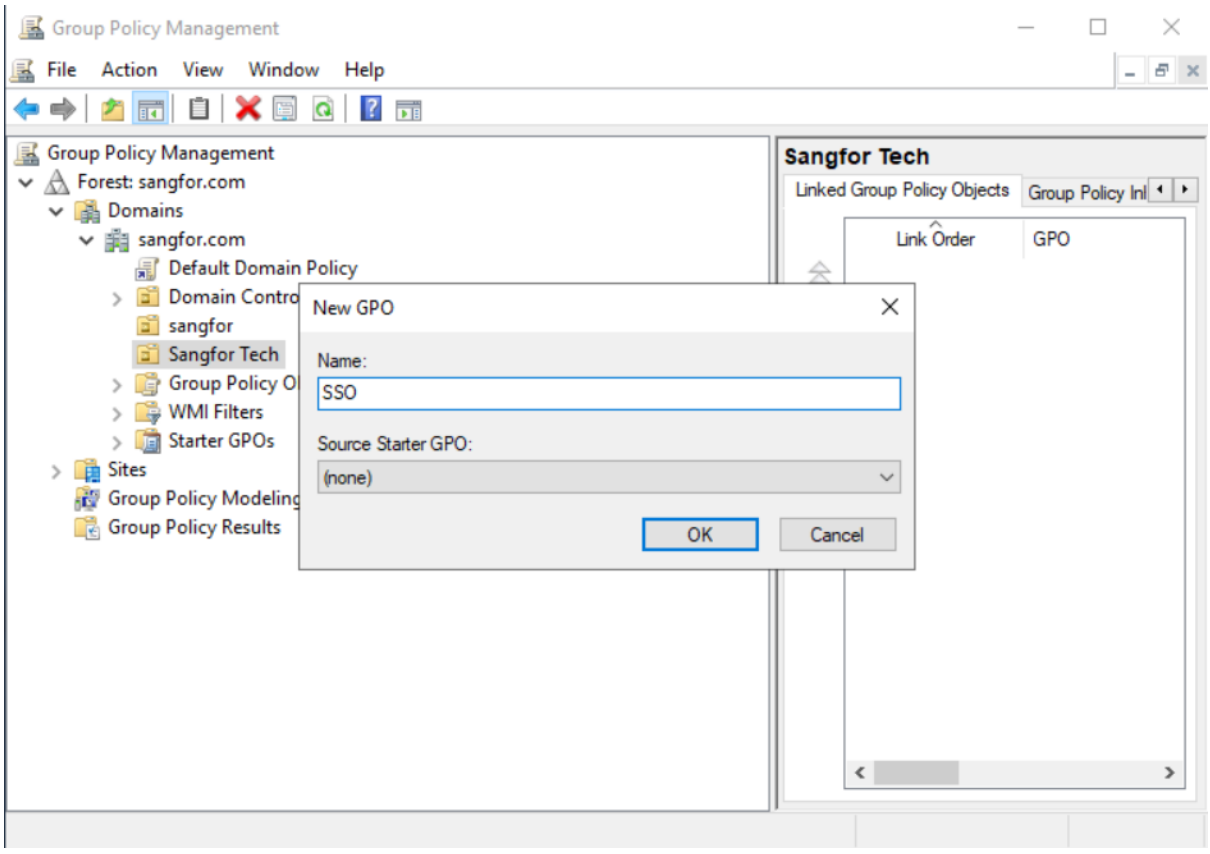
3.3 Configure the login and logout script on the AD server

1. Open "Group Policy Management" in "Run".

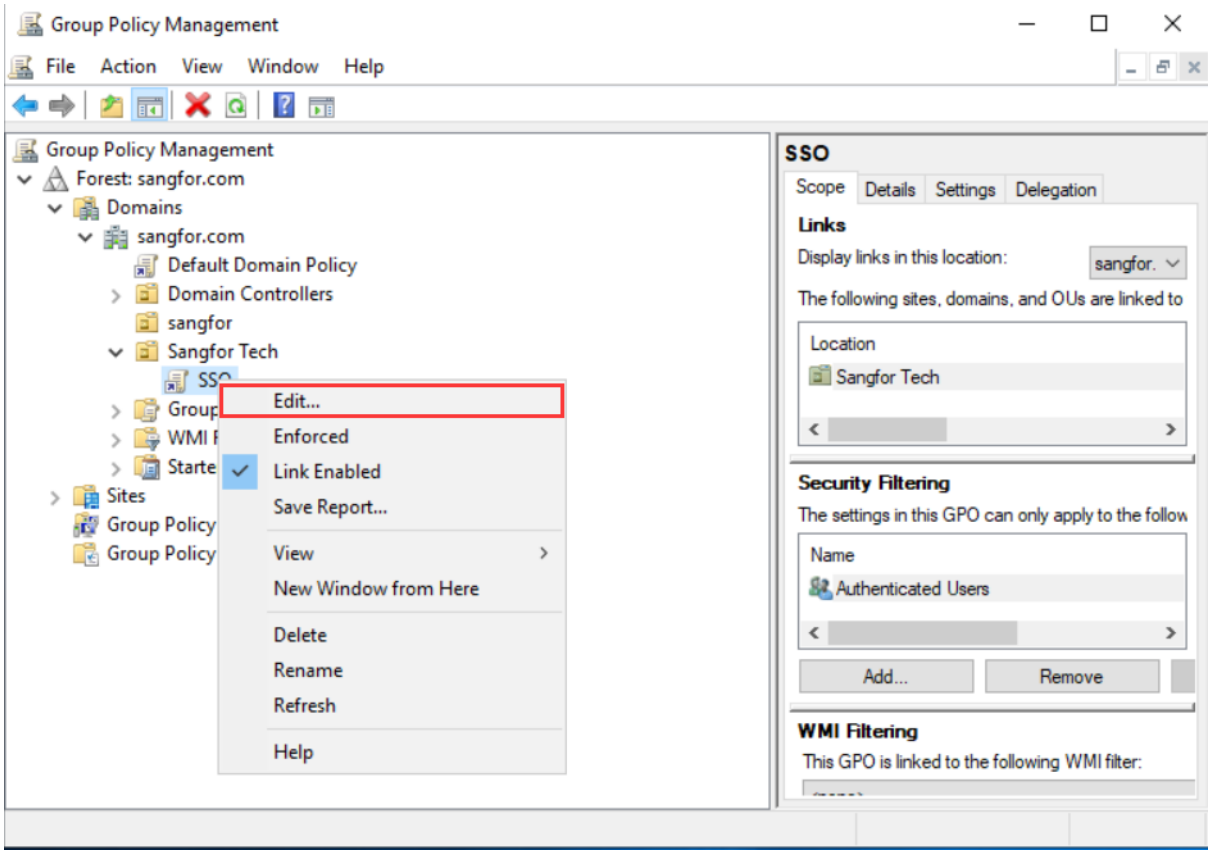


2. Create a GPO for the newly created Sangfor Tech container, and create a name for the GPO.

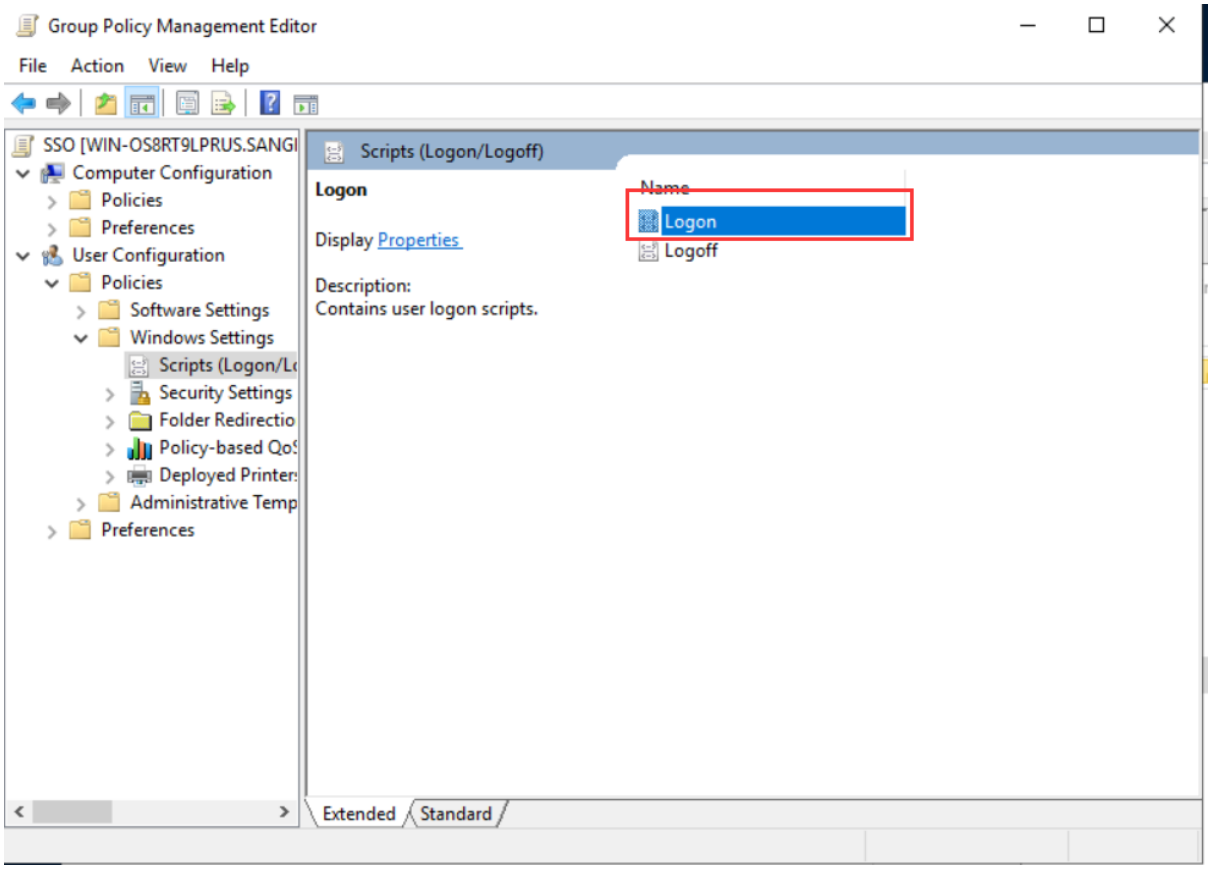




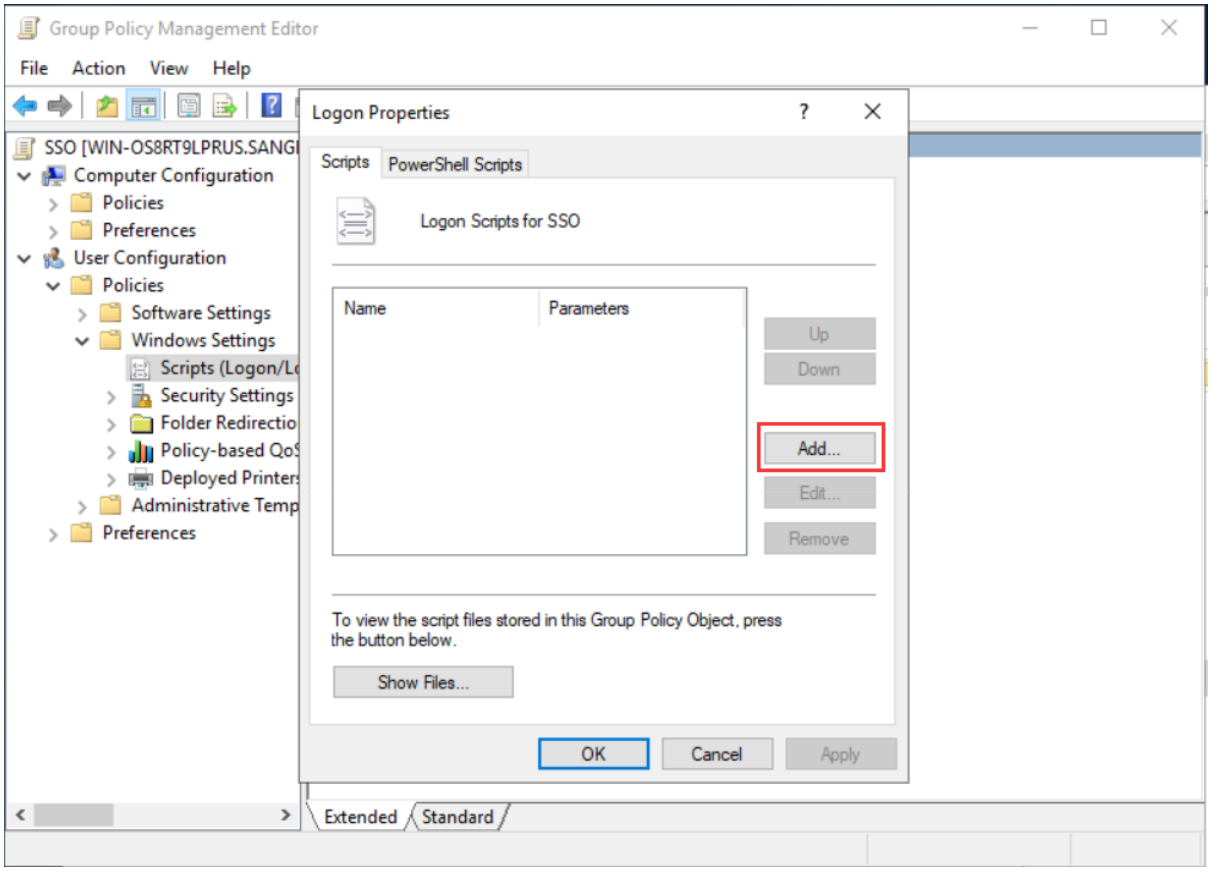
3. Use the right mouse button to select Edit GPO.

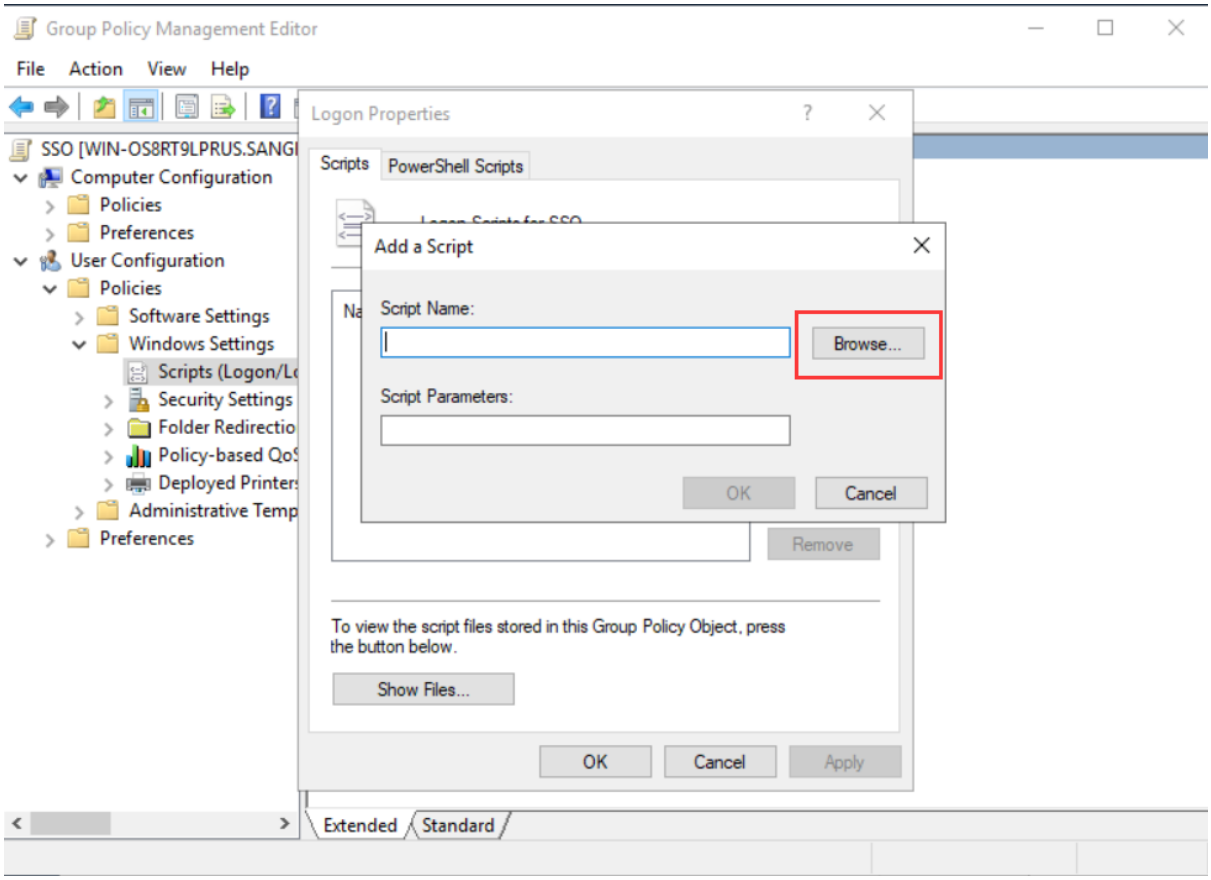


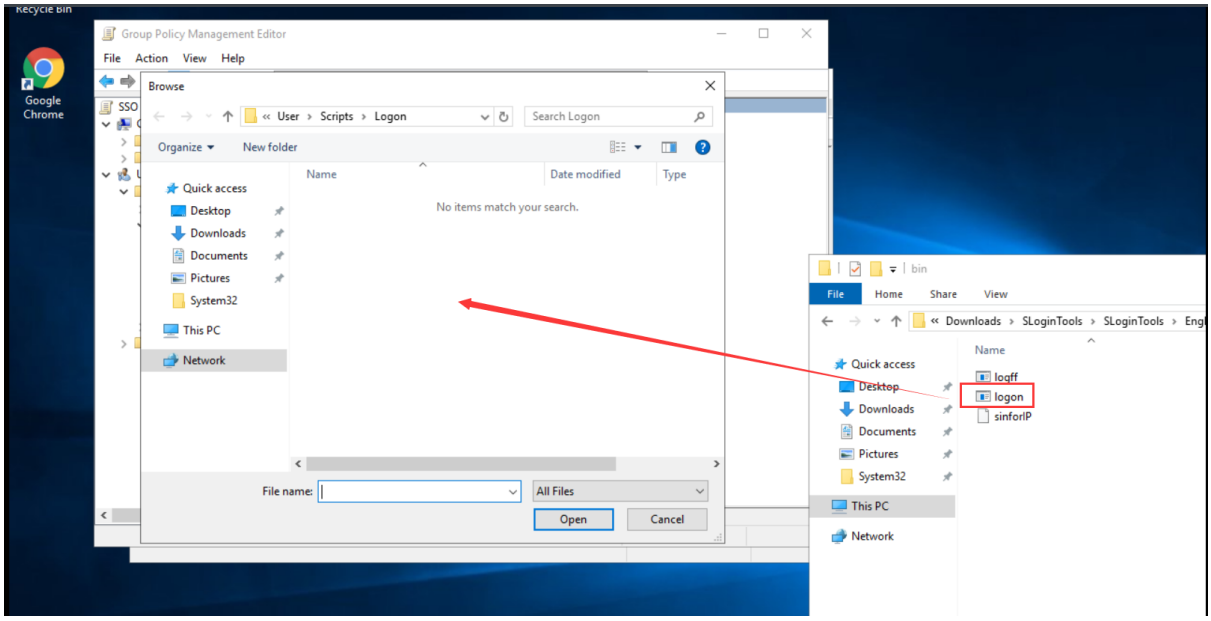
4. Find the script login configuration in "User Configuration".



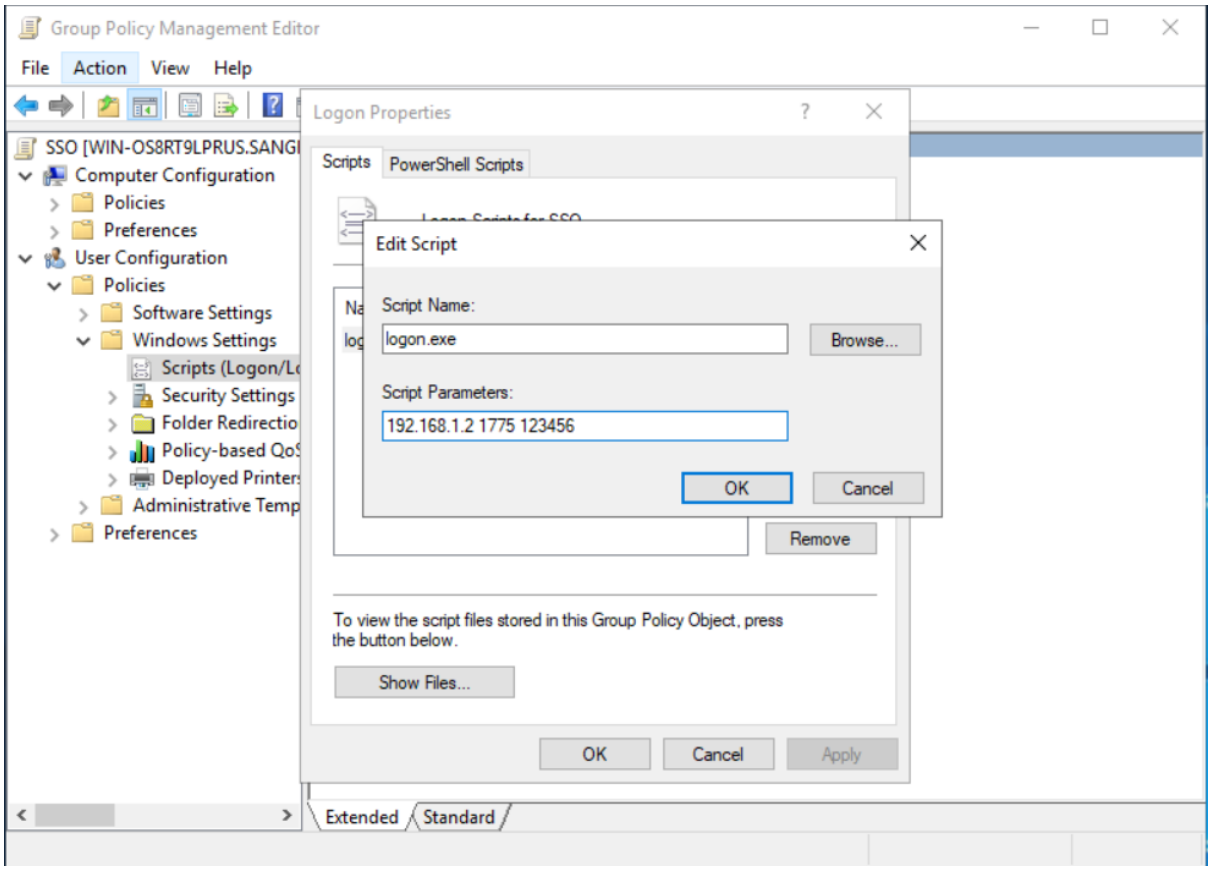
5. Select the Logon script, click "Add", and then select "Broswe" to copy the login script we downloaded from the IAM page to the specified path.


Group Policy Management Editor
File Action View Help
SSO [WIN-OS8RT9LPRUS.SANGI
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Scripts (Logon/L
Security Settings
Folder Redirectio
Policy-based QoS
Deployed Printers
Administrative Temp
Preferences
Logon Properties
Scripts
PowerShell Scripts
Logon Scripts for SSO
Name
Parameters
Up
Down
Add...
Edit...
Remove
To view the script files stored in this Group Policy Object, press the button below.
Show Files...
OK
Cancel
Apply
Extended
Standard

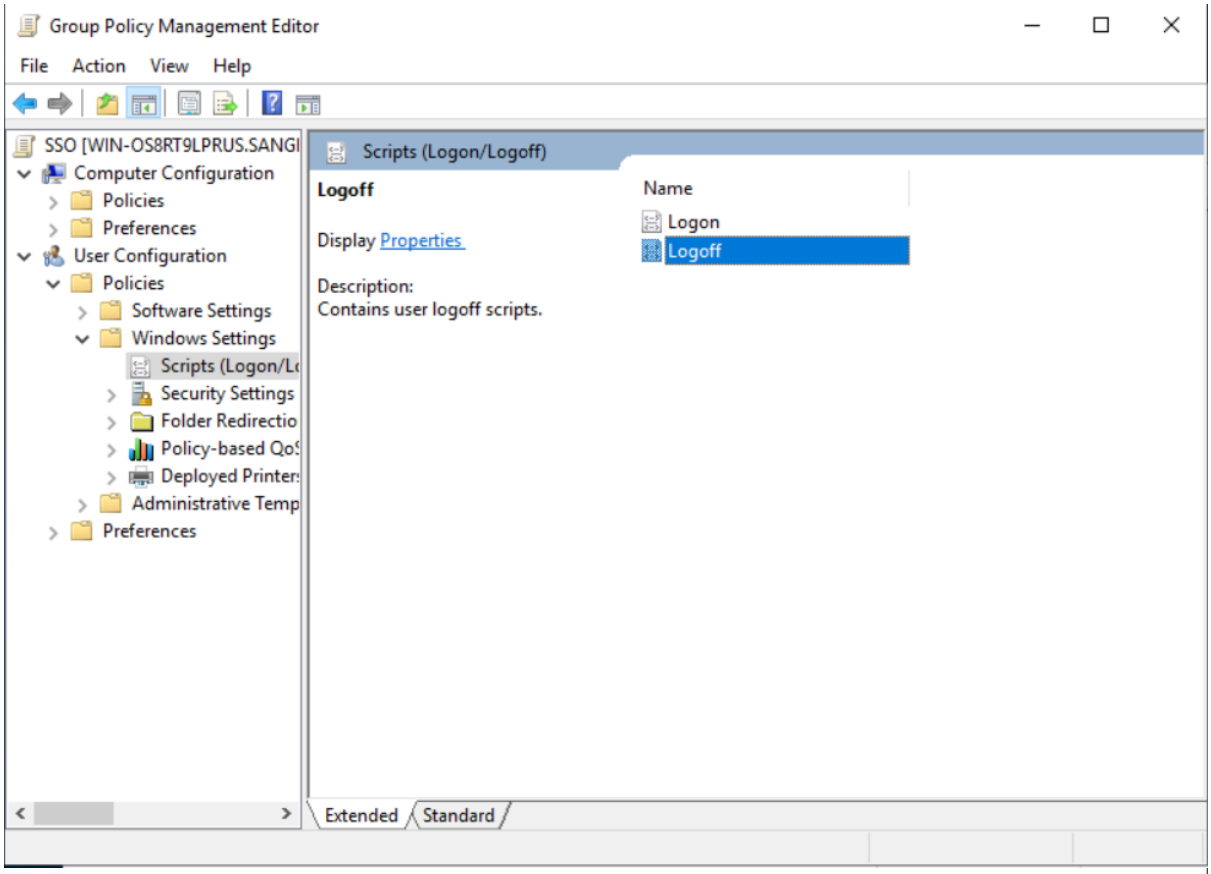

Group Policy Management Editor
File Action View Help
SSO [WIN-OS8RT9LPRUS.SANGI
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Scripts (Logon/L
Security Settings
Folder Redirectio
Policy-based QoS
Deployed Printers
Administrative Temp
Preferences
Logon Properties
Scripts
PowerShell Scripts
Add a Script
Script Name:
Browse...
Script Parameters:
OK
Cancel
Remove
To view the script files stored in this Group Policy Object, press the button below.
Show Files...
OK
Cancel
Apply
Extended
Standard

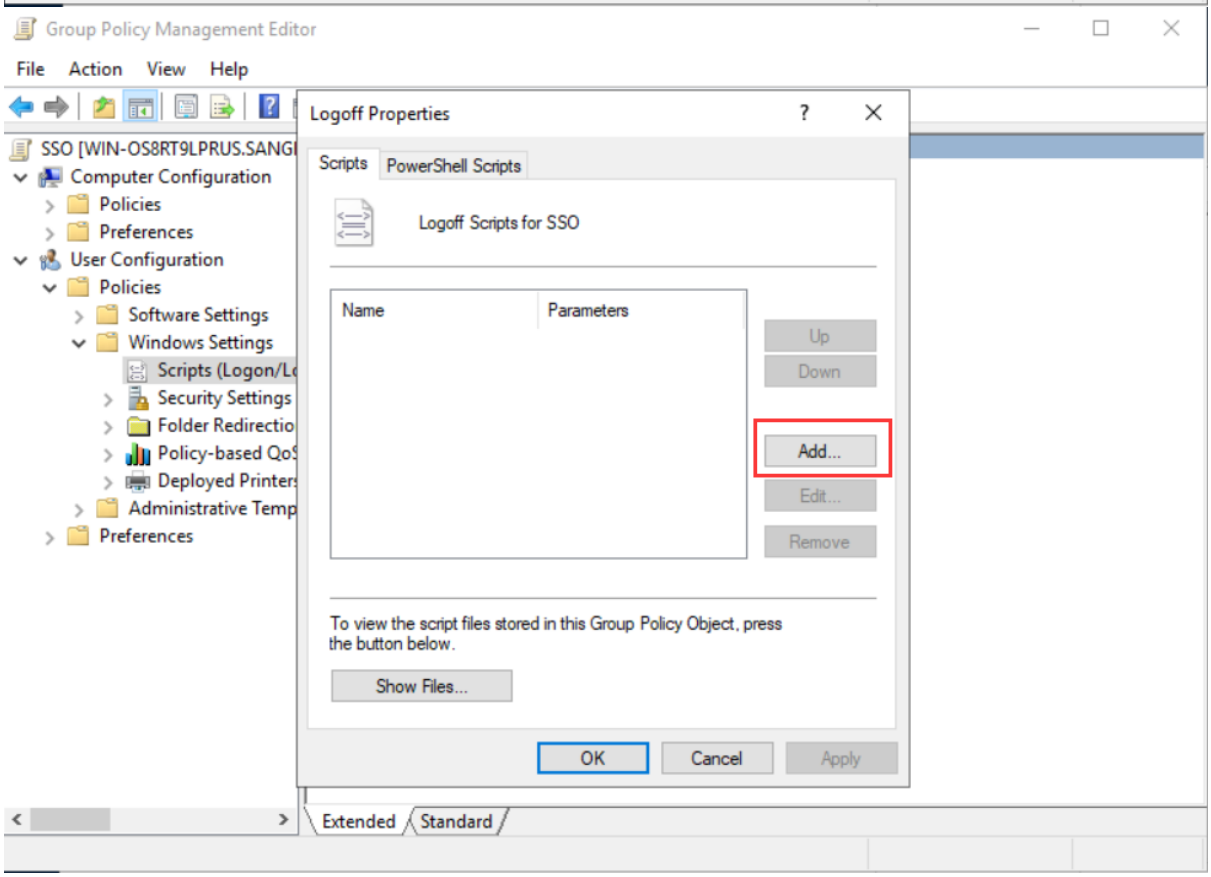


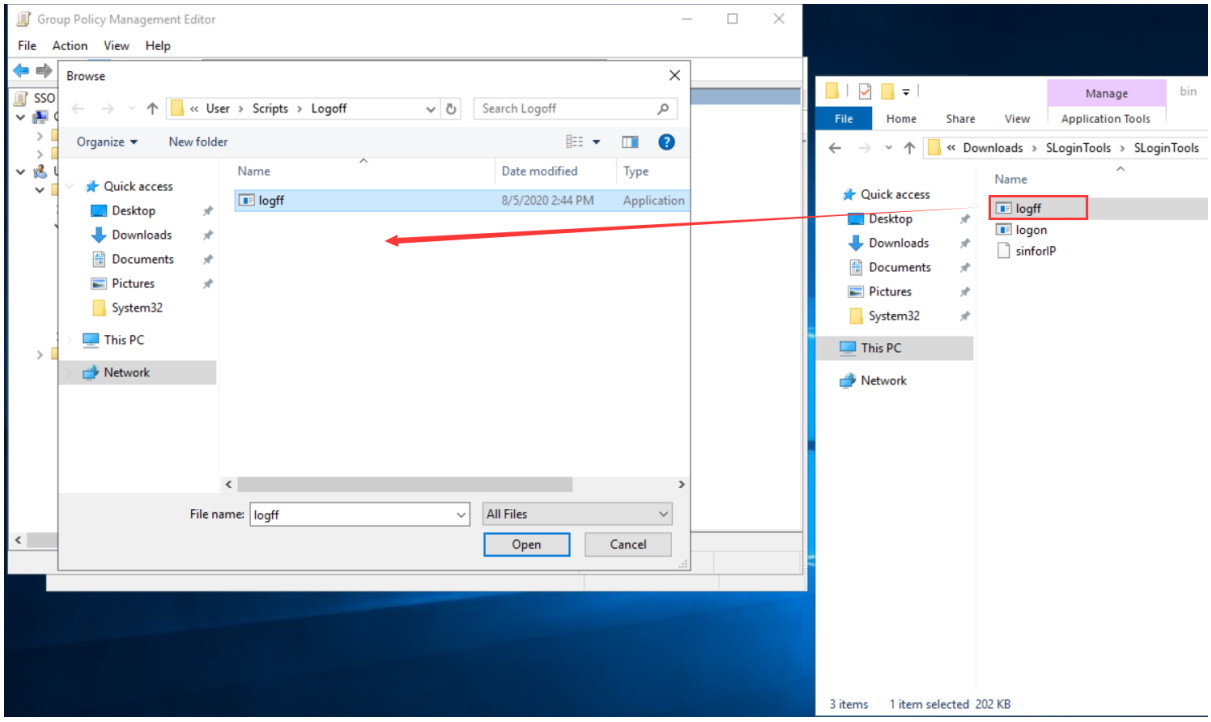
5. Set the parameters of the script single sign-on, first write the IAM address 192.168.1.2 and then fill in the port 1775, IAM uses the UDP1775 port to accept the authentication information actively transmitted by the PC, and fill in the shared secret key 123456 that we configured on the IAM page.

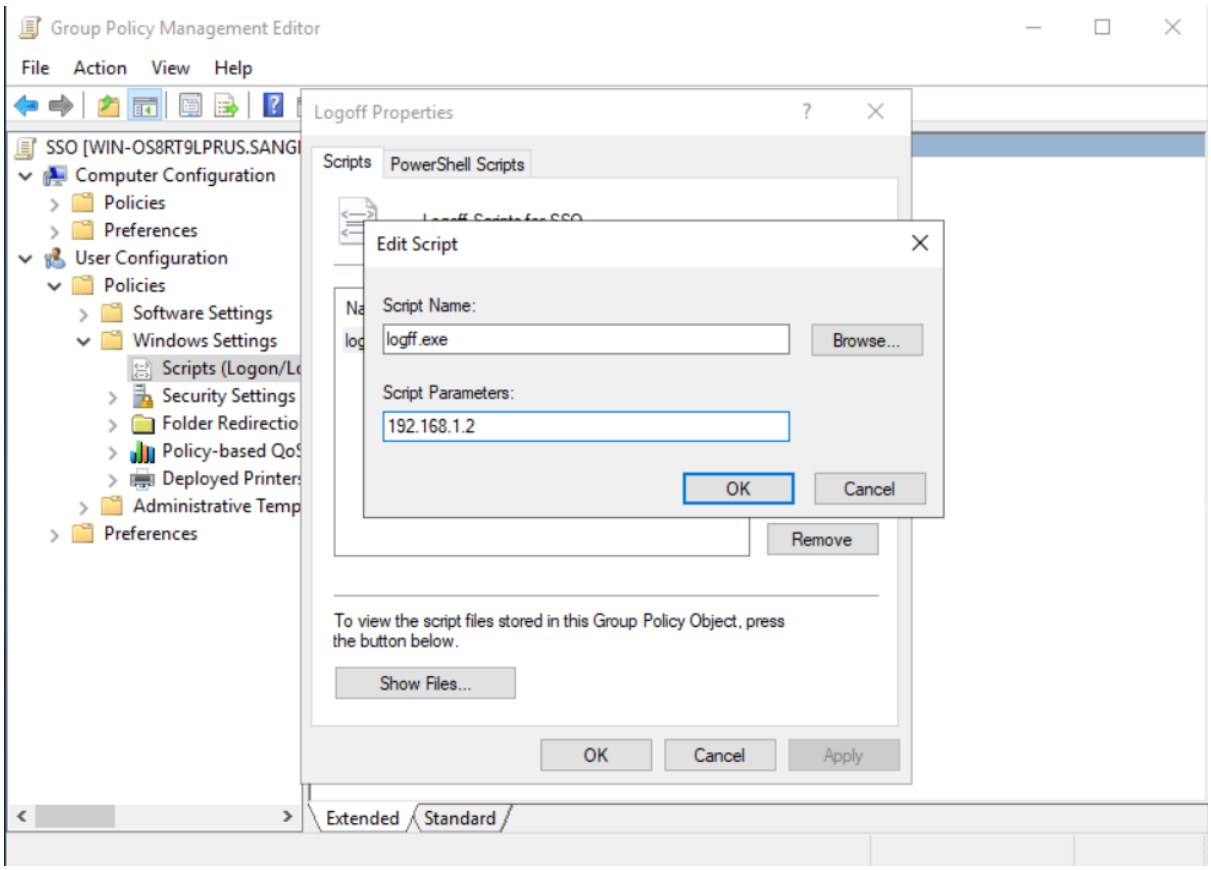


6. For the Logoff script, also copy the Logoff program we downloaded from the IAM page to the specified path, and fill in the script parameter as IAM's IP192.168.1.2.


Group Policy Management Editor
File Action View Help
SSO [WIN-OS8RT9LPRUS.SANGI
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Scripts (Logon/Lo
Security Settings
Folder Redirectio
Policy-based QoS
Deployed Printers
Administrative Temp
Preferences
Scripts (Logon/Logoff)
Logoff
Display Properties
Description:
Contains user logoff scripts.
Name
Logon
Logoff
Extended
Standard


Group Policy Management Editor
File Action View Help
Logoff Properties
Scripts
PowerShell Scripts
Logoff Scripts for SSO
Name
Parameters
Up
Down
Add...
Edit...
Remove
To view the script files stored in this Group Policy Object, press the button below.
Show Files...
OK
Cancel
Apply
Extended
Standard

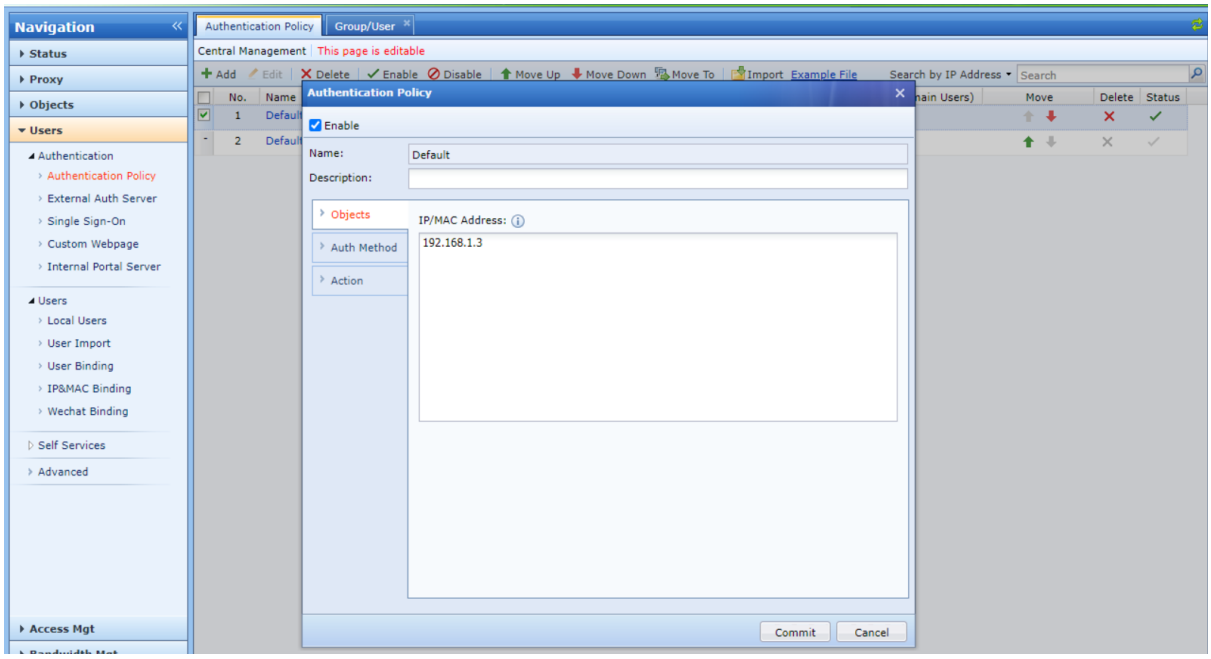




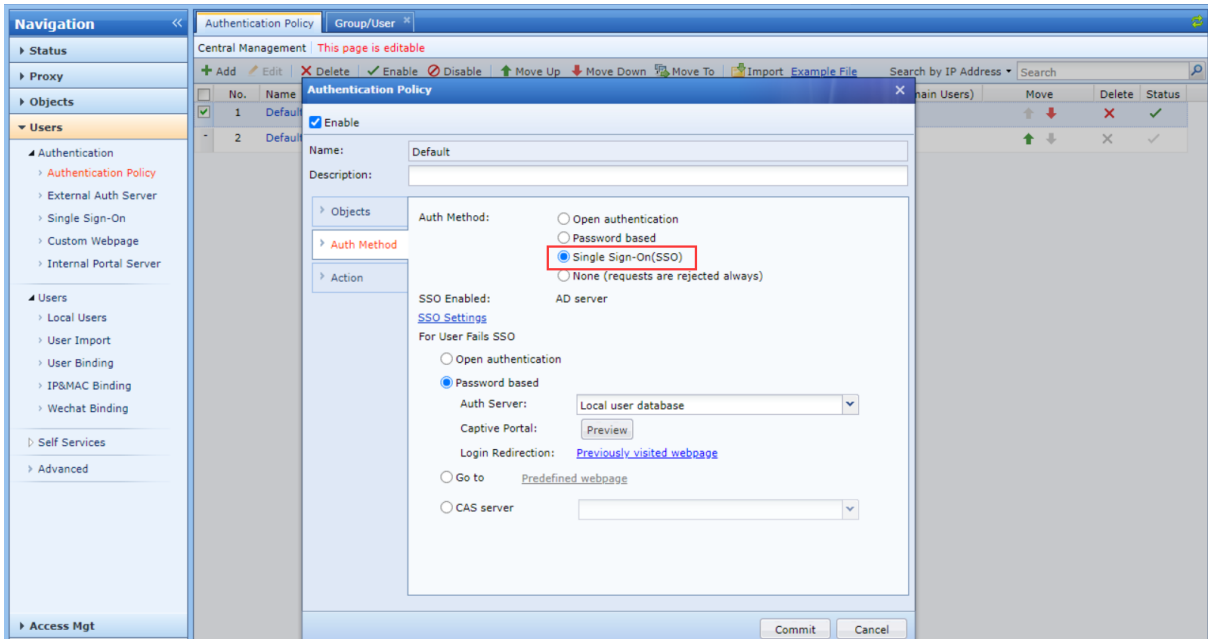
7. After modifying the AD domain server, use the gpupdate/force command to forcibly refresh all group policies.

3.4 Configure authentication policy on IAM

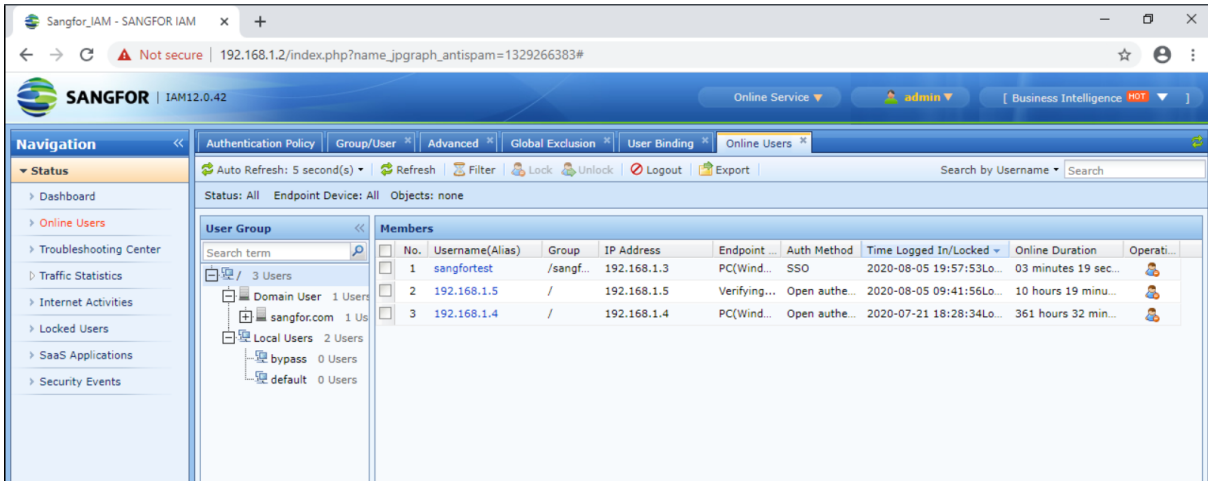
1. Set the scope of the authentication strategy, that is, which IP should match the authentication policy.



2. Select the authentication method as "SSO".

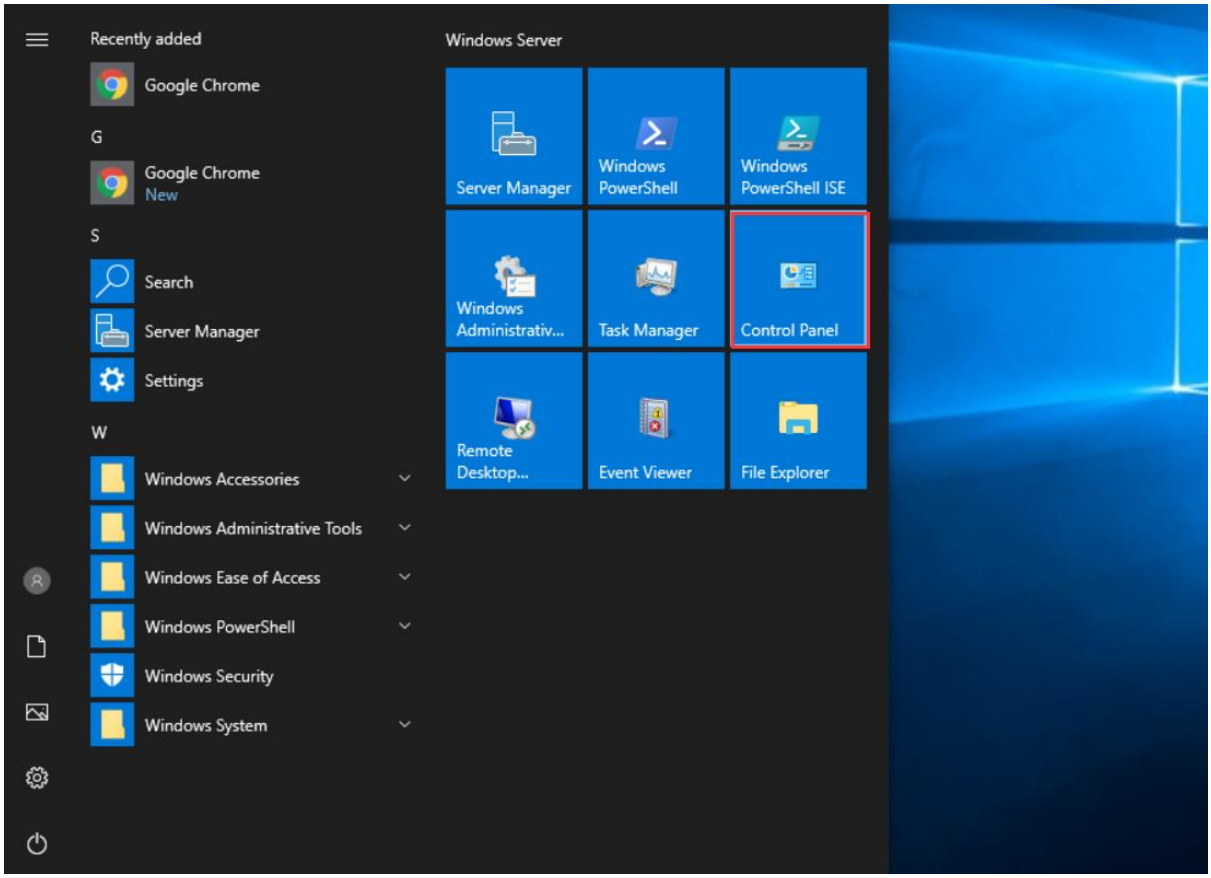


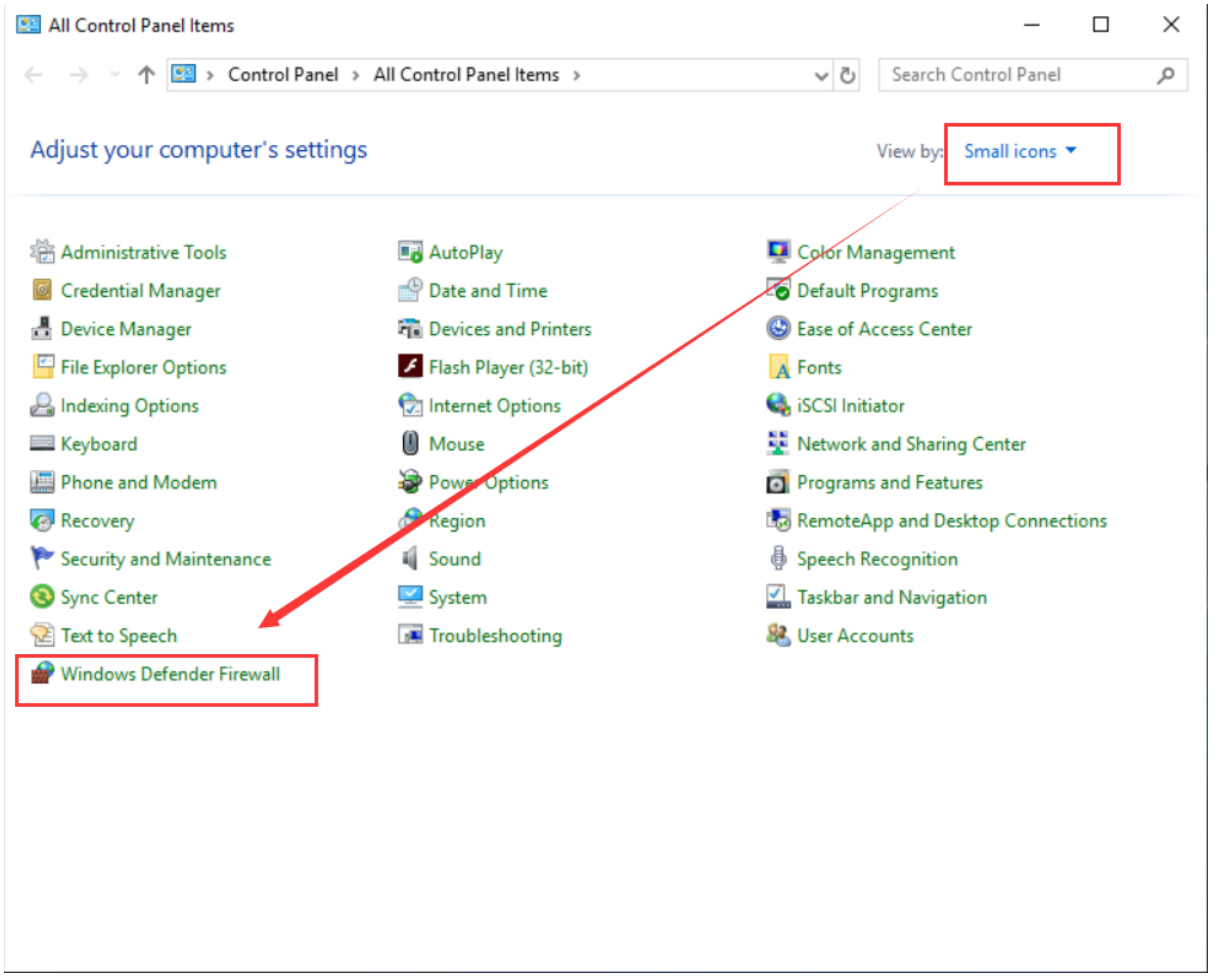
3. Restart the test PC192.168.1.3 and log in to the PC with a domain account. You can see that PC192.168.1.3 is online and the authentication method is SSO on the IAM.

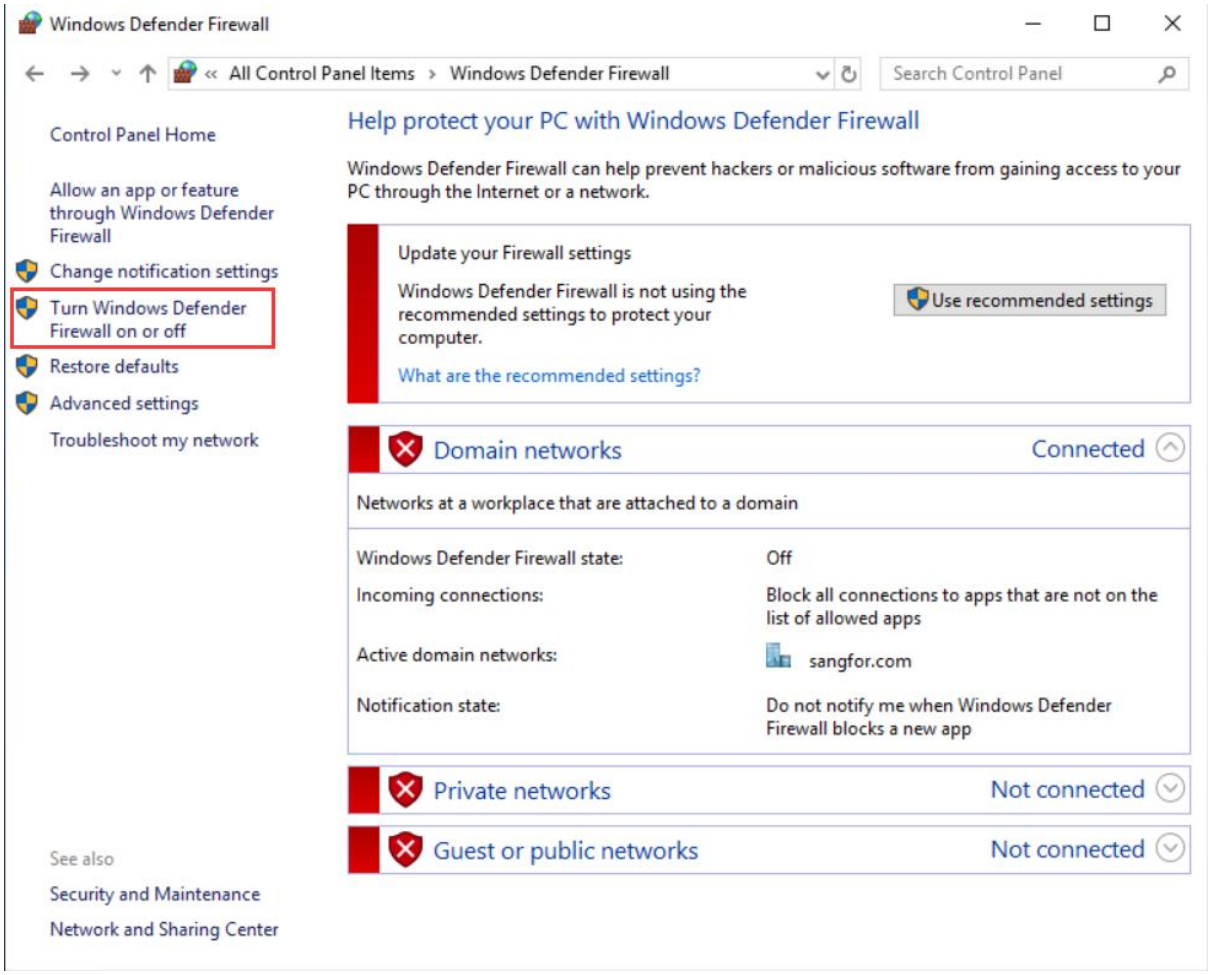


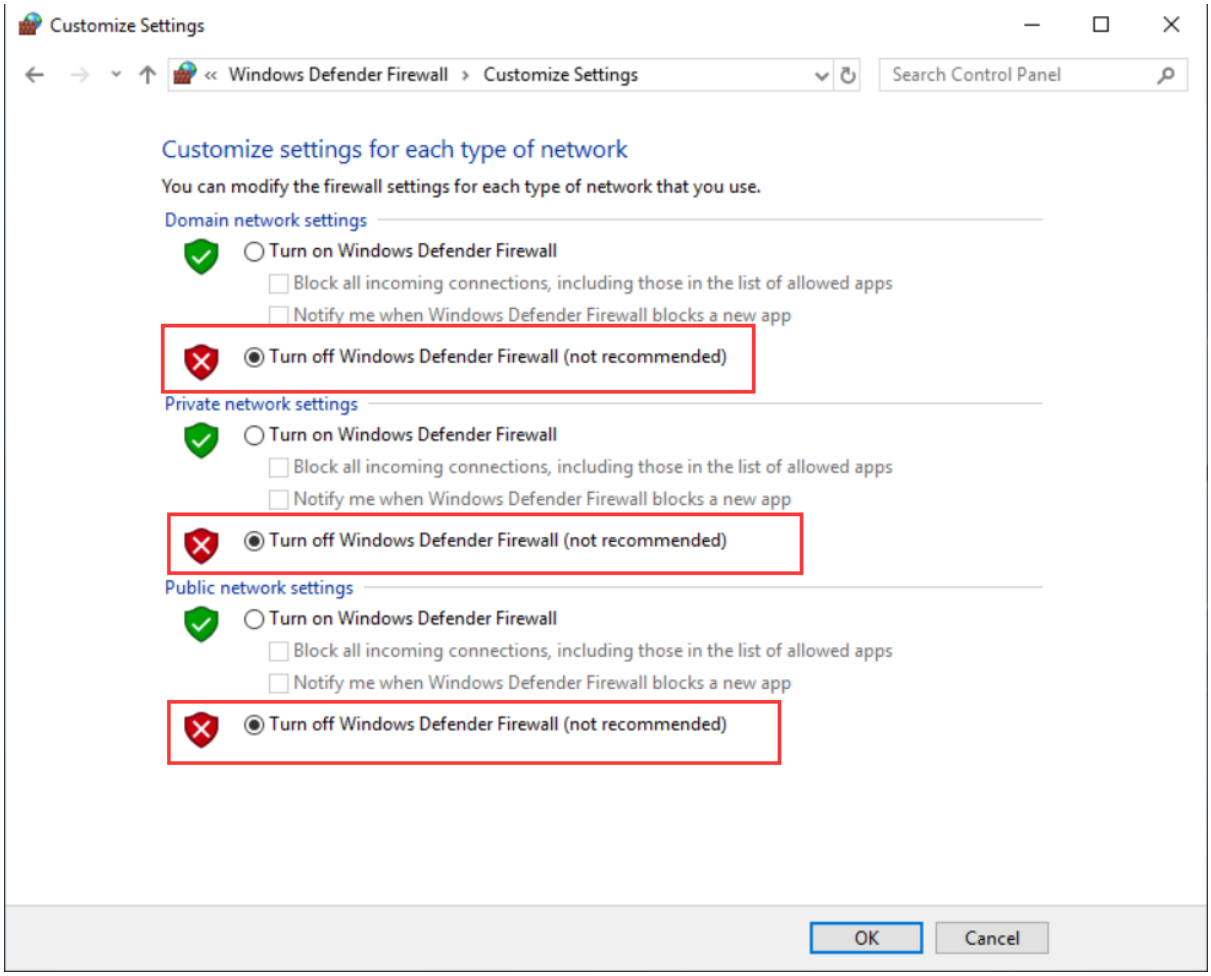
Chapter 4 Precautions

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.

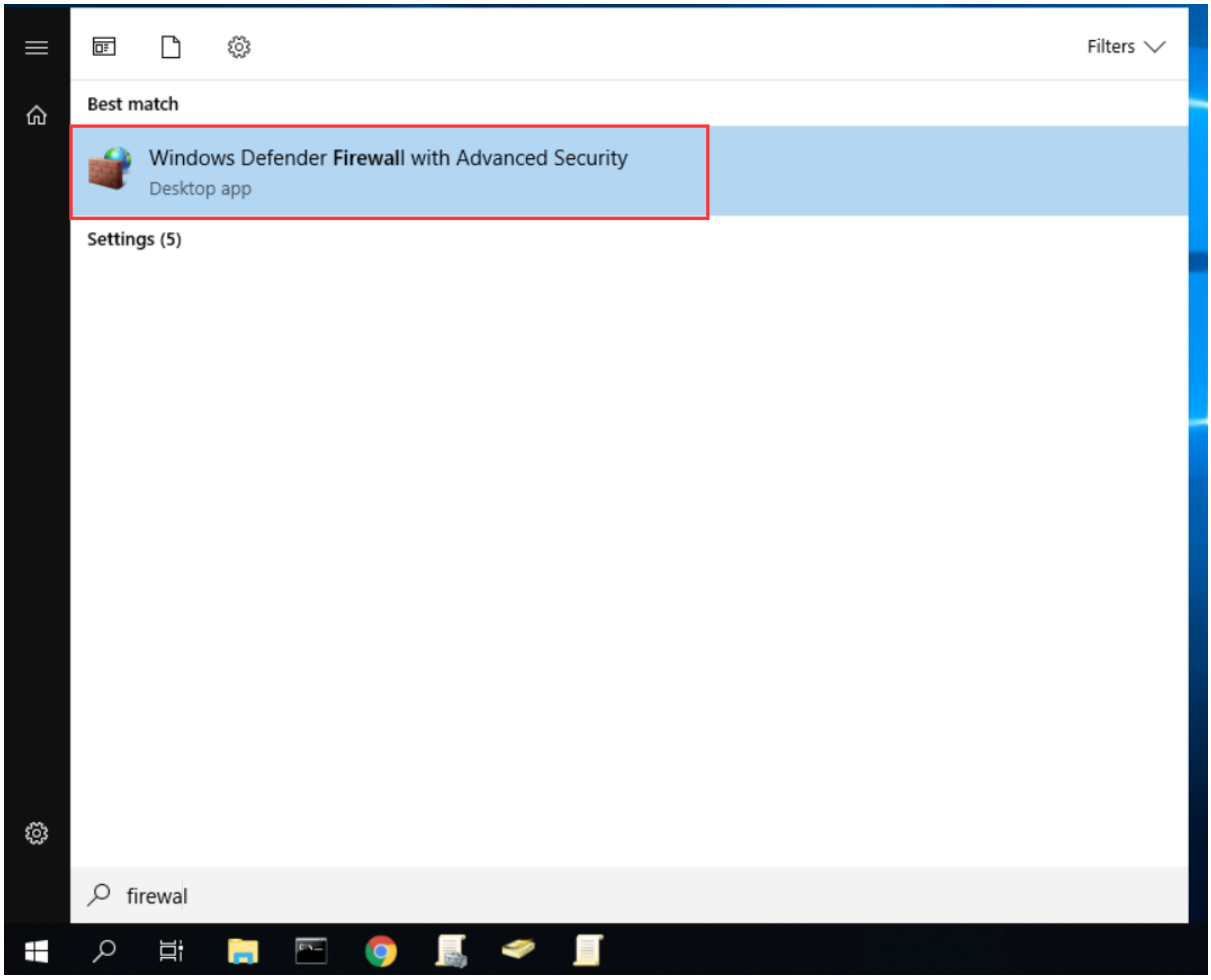


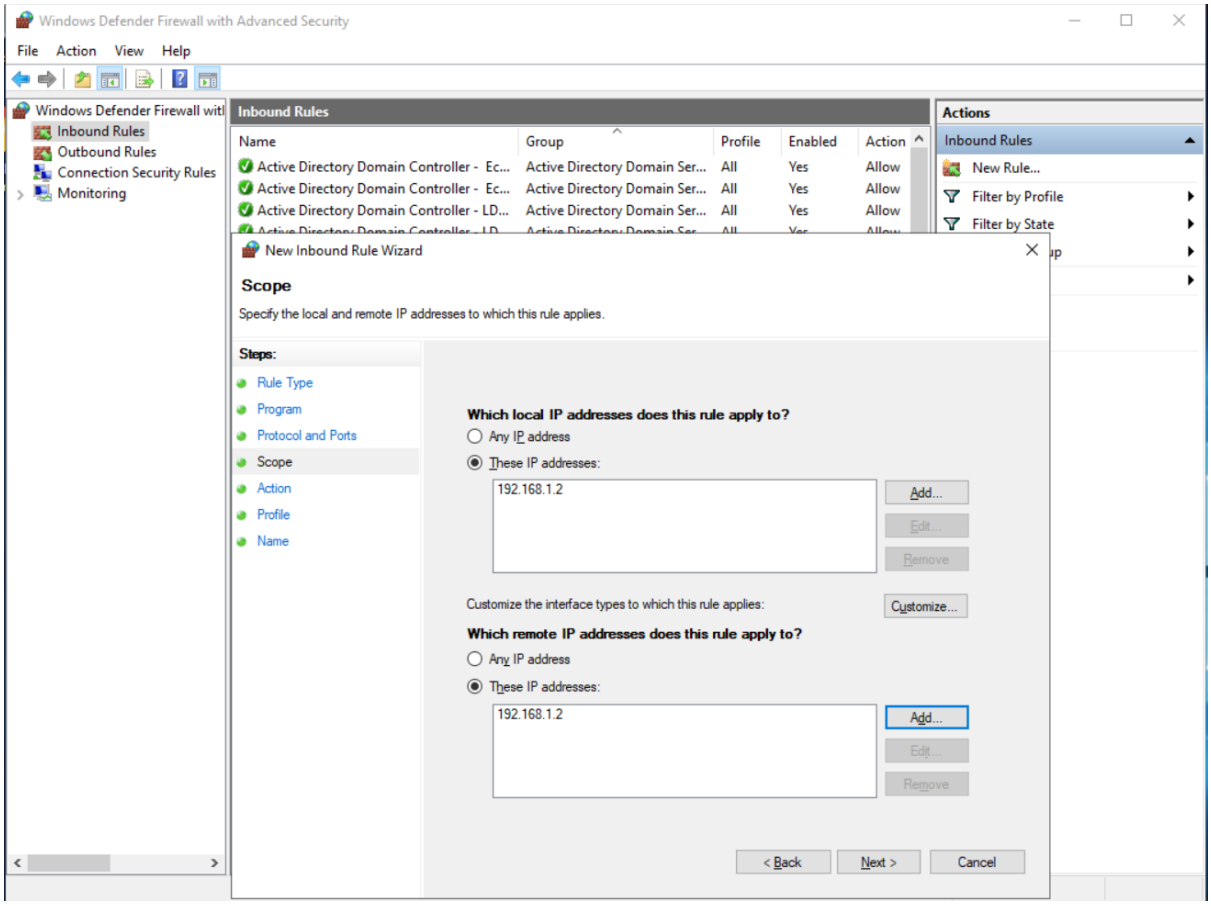

All Control Panel Items
Control Panel › All Control Panel Items ›
Search Control Panel
Adjust your computer's settings
View by: Small icons
Administrative Tools
Credential Manager
Device Manager
File Explorer Options
Indexing Options
Keyboard
Phone and Modem
Recovery
Security and Maintenance
Sync Center
Text to Speech
Windows Defender Firewall
AutoPlay
Date and Time
Devices and Printers
Flash Player (32-bit)
Internet Options
Mouse
Power Options
Region
Sound
System
Troubleshooting
Color Management
Default Programs
Ease of Access Center
Fonts
iSCSI Initiator
Network and Sharing Center
Programs and Features
RemoteApp and Desktop Connections
Speech Recognition
Taskbar and Navigation
User Accounts


Windows Defender Firewall
« All Control Panel Items › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Update your Firewall settings
Windows Defender Firewall is not using the recommended settings to protect your computer.
What are the recommended settings?
Use recommended settings
Domain networks
Connected
Networks at a workplace that are attached to a domain
Windows Defender Firewall state:
Off
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active domain networks:
sangfor.com
Notification state:
Do not notify me when Windows Defender Firewall blocks a new app
Private networks
Not connected
Guest or public networks
Not connected
See also
Security and Maintenance
Network and Sharing Center



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


Filters
Best match
Windows Defender Firewall with Advanced Security
Desktop app
Settings (5)
firewal


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Active Directory Domain Controller - Ec...
Active Directory Domain Ser...
All
Yes
Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
New Inbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
192.168.1.2
Add...
Edit...
Remove
Customize the interface types to which this rule applies:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
192.168.1.2
Add...
Edit...
Remove
< Back
Next >
Cancel