IAM

Best Practices for Scenarios_Activity Domain IWA SSO

Version 12.0.42

Change Log

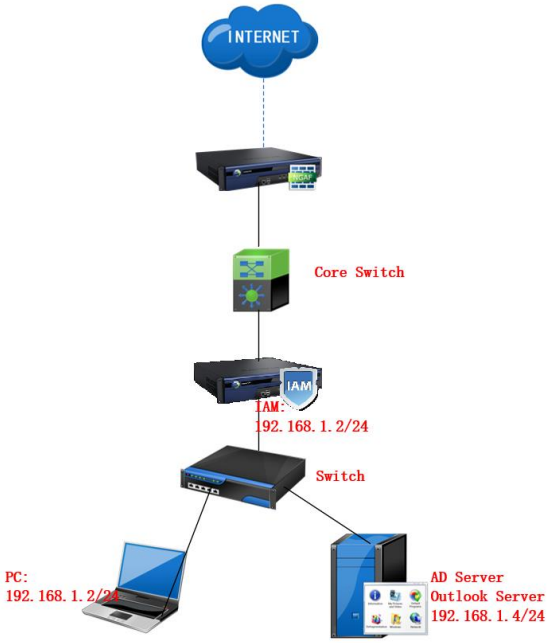
Date	Change Description
August 24, 2020	Version 12.0.42 document release.
May 17, 2021	Version 12.0.42 document update.

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 Enable SMBv1 of Windows Server 18
2.5 Join the PC to the domain 18
Chapter 3 How to Configure IAM 25
3.1 Add LDAP server 25
3.2 Configure Integrated Windows Authentication SSO 27
3.3 Configure authentication policy on IAM 28
Chapter 4 Precautions 29

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 Integrated Windows Authentication method.



AD Server:

IP: 192.168.1.4

Domain Name: sangfor.com

Account/Password: administrator/@sangfor123

Test PC:

IP: 192.168.1.3

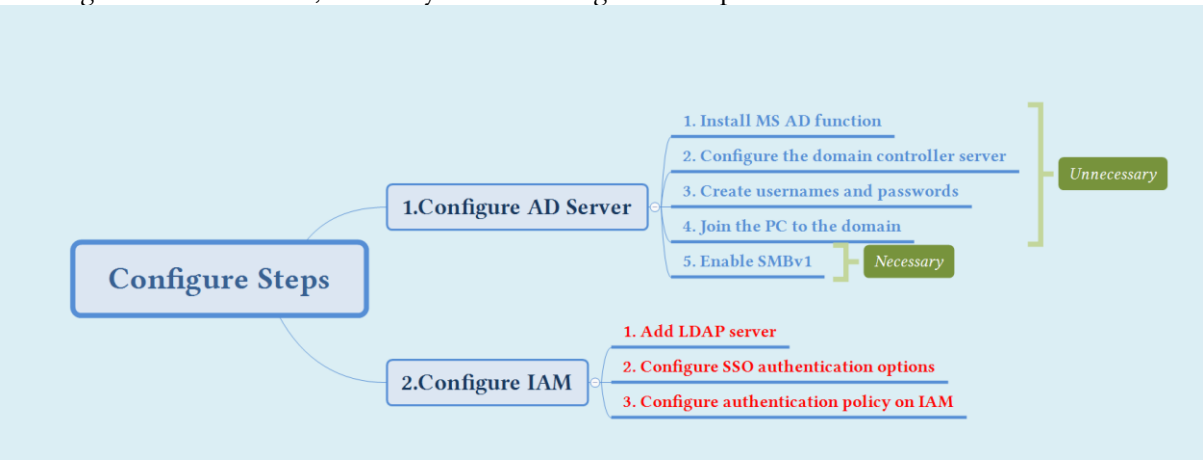
Account/Password: administrator/@sangfor123

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

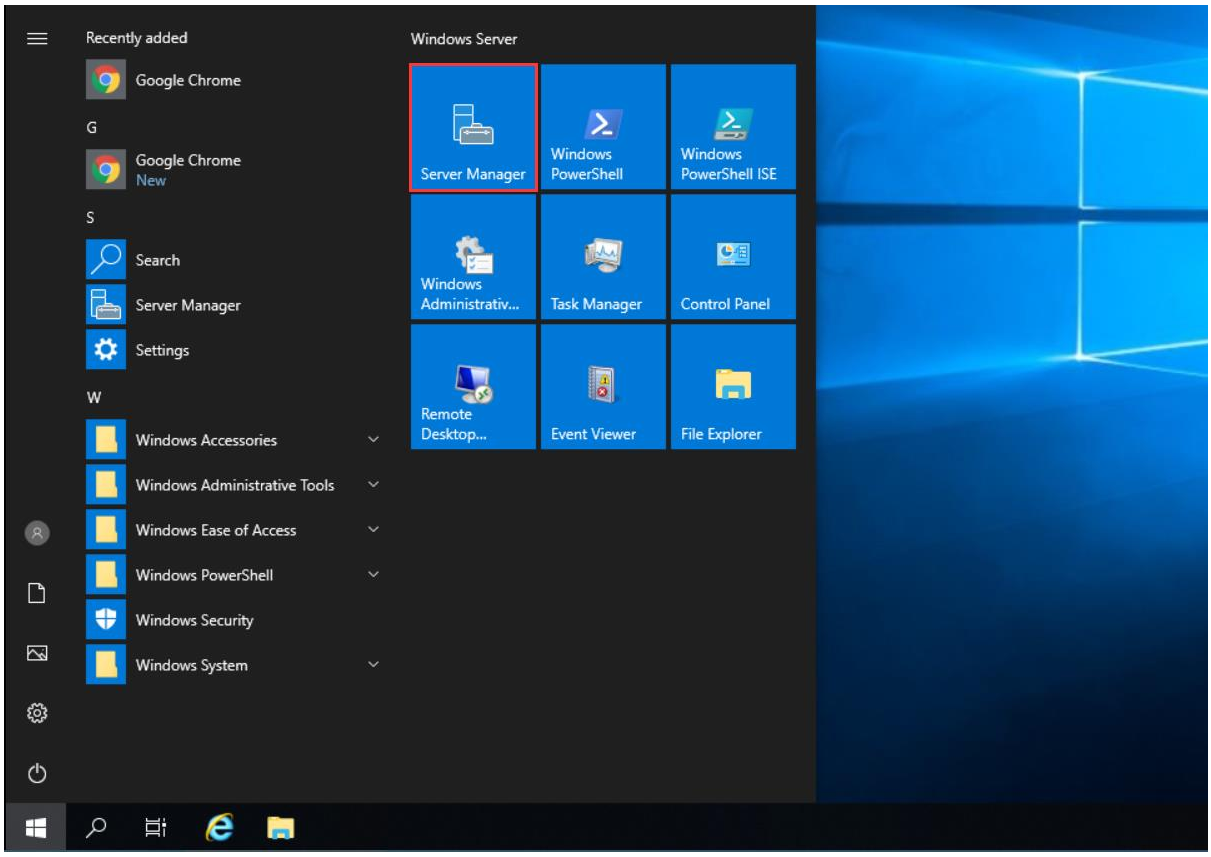
reconfigure the AD domain, then only need to configure other parts.



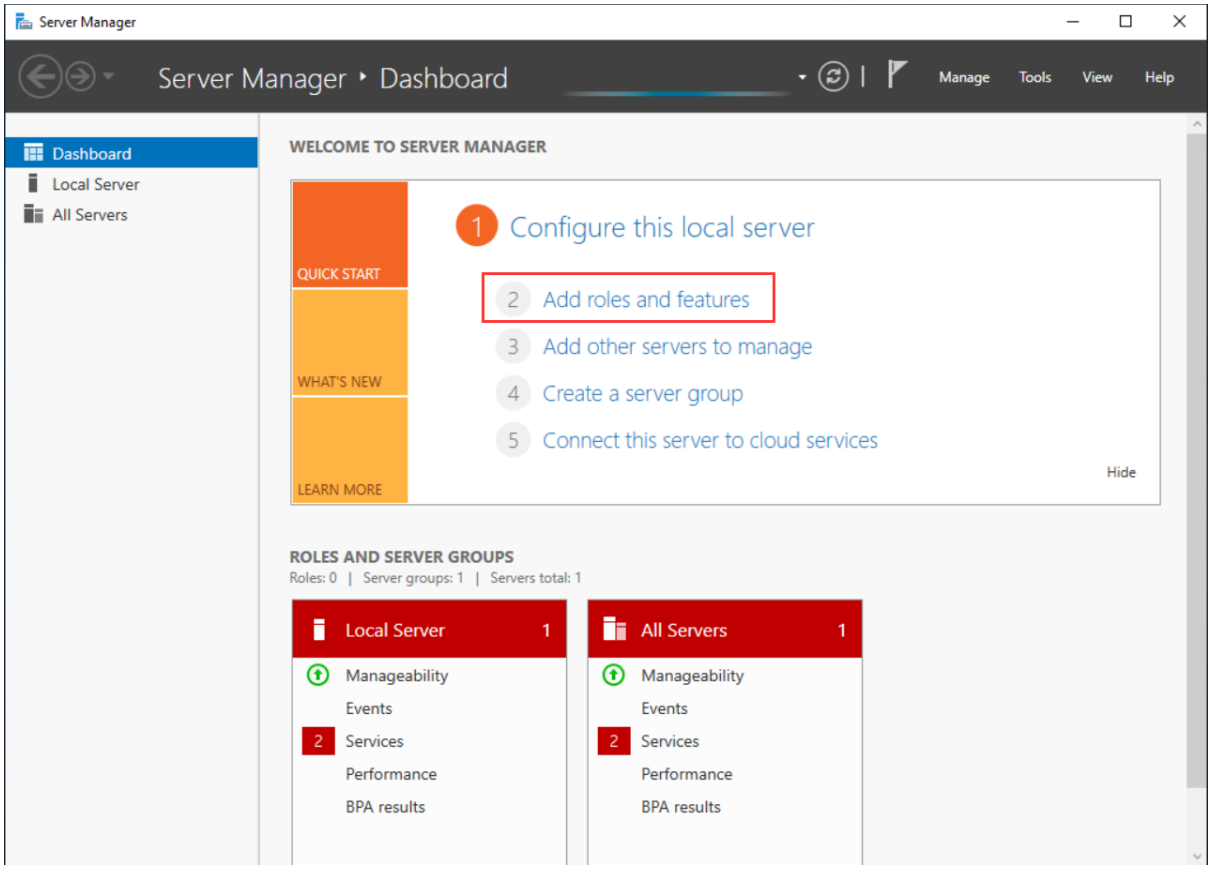
Chapter 2 How to Configure Activity Domain Server

2.1 Install MS AD function

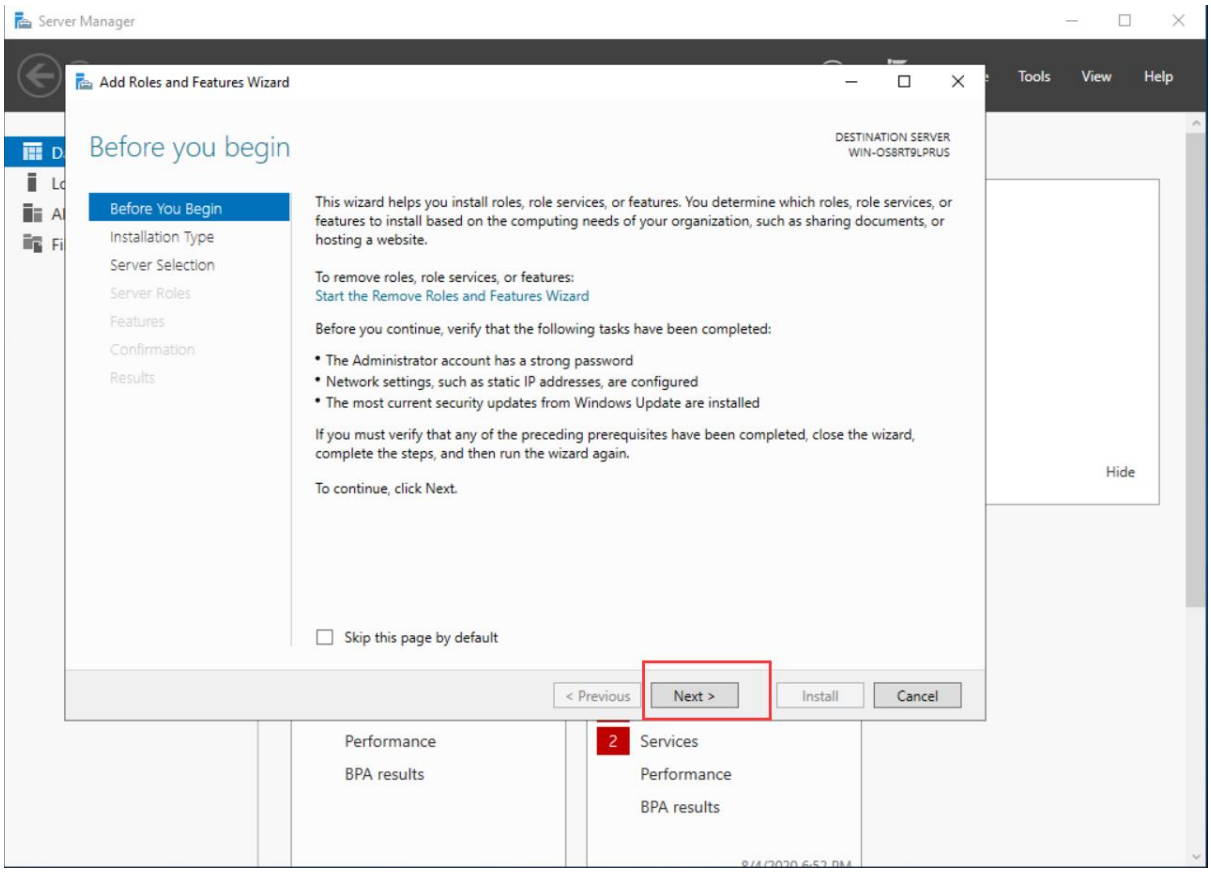
1. Open Server Manager in Windows Server 2019.



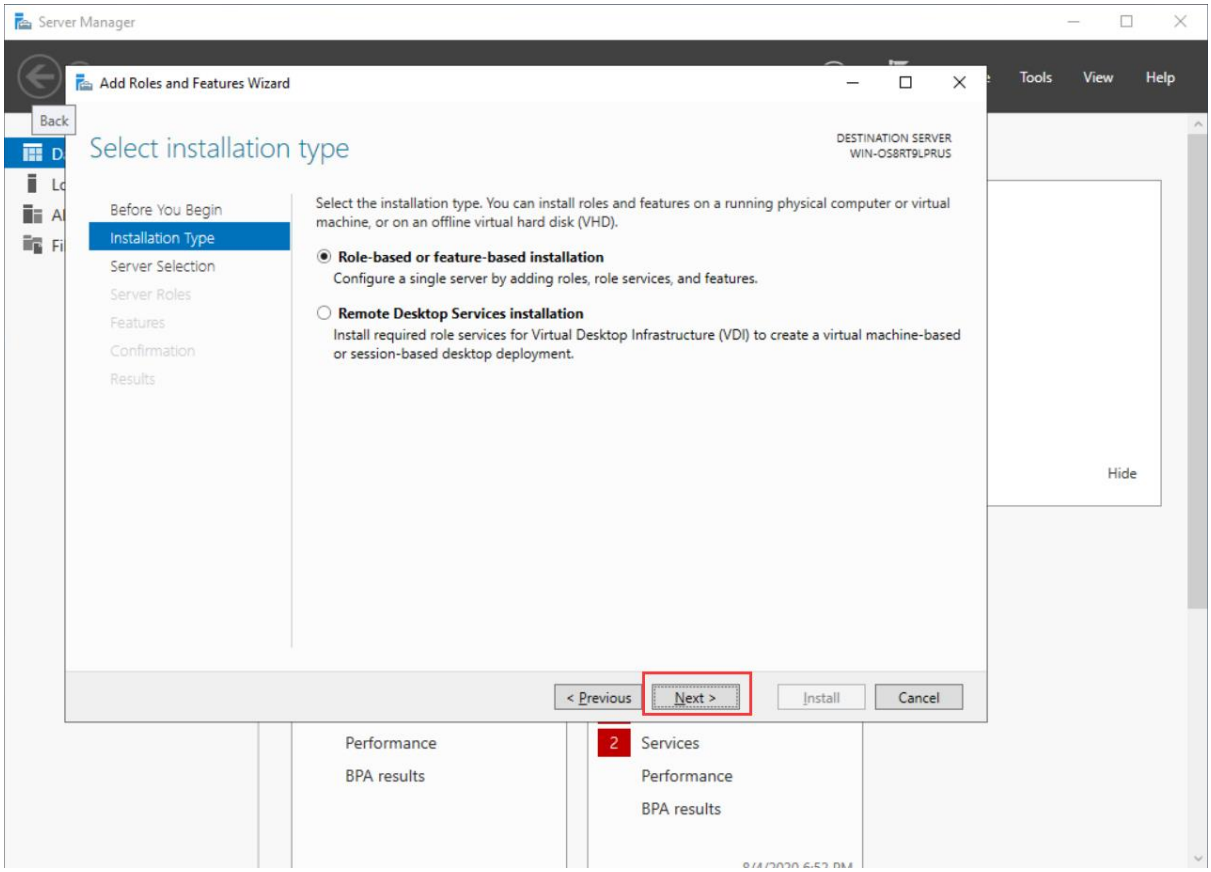
2.Click "Add roles and features".



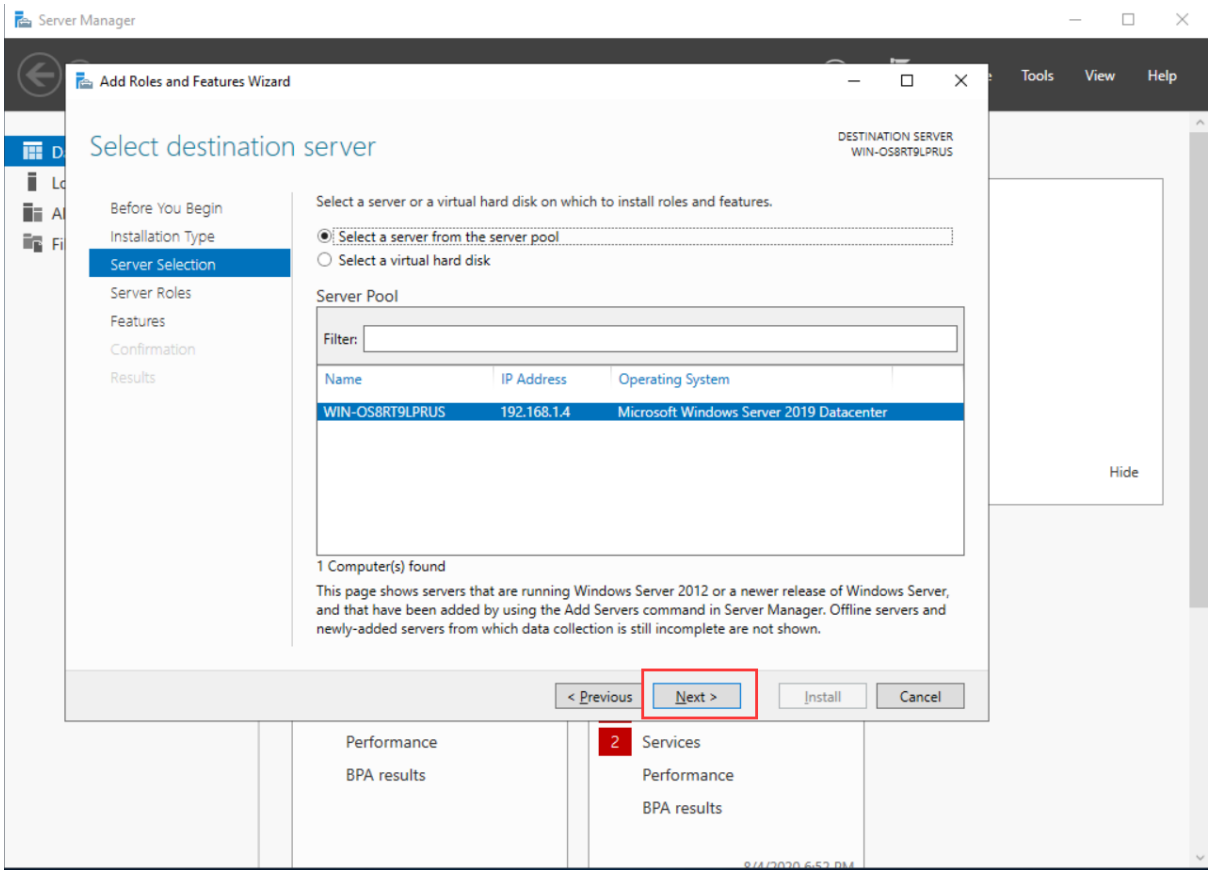
3.Click "Next".



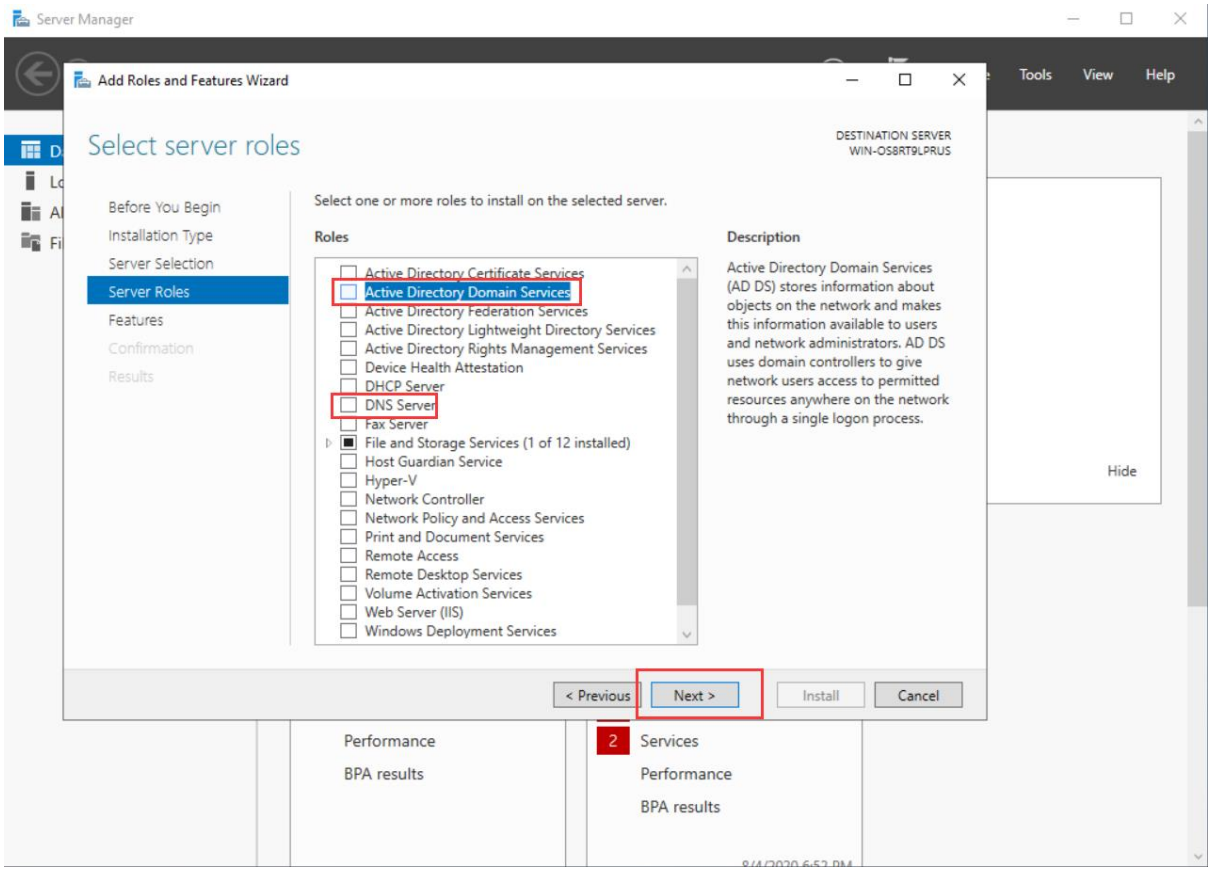
4. Click "Next".

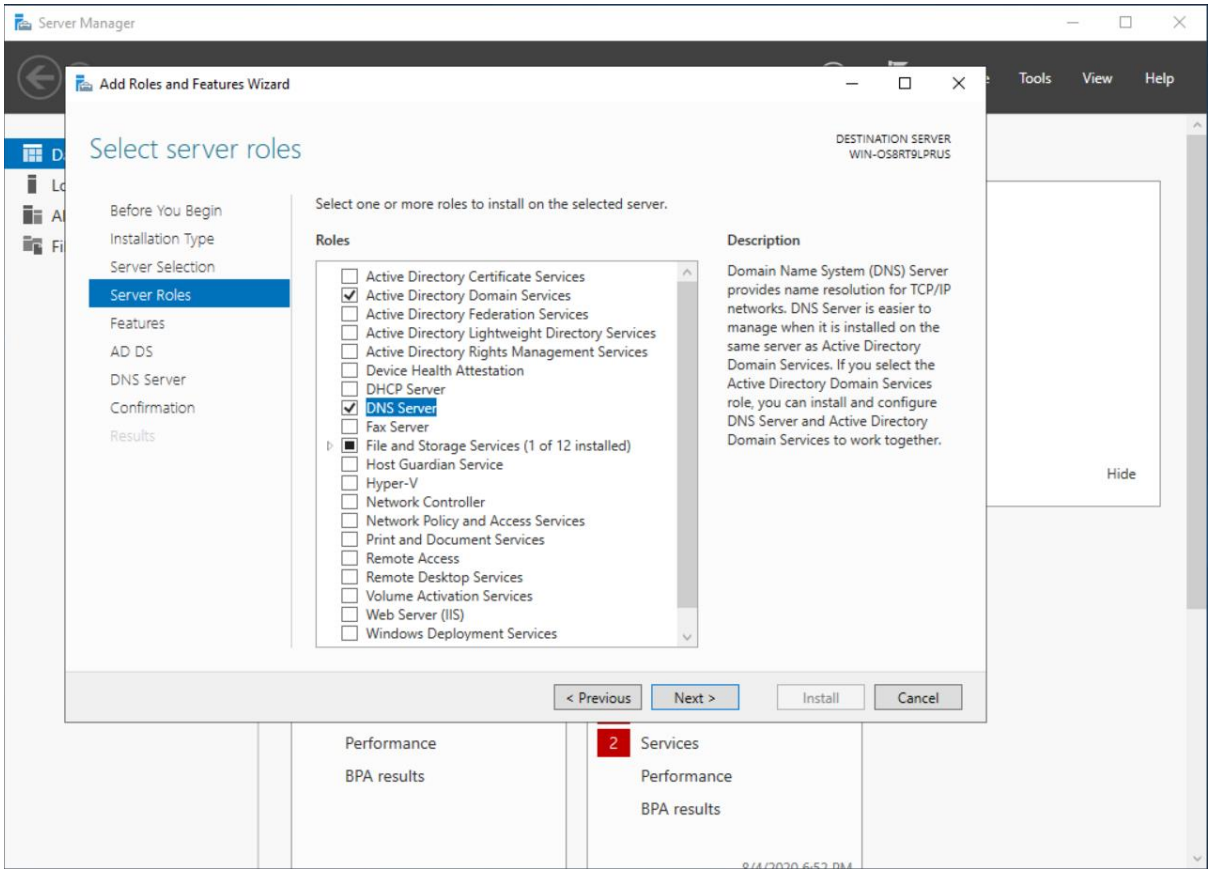


5. Click "Next".

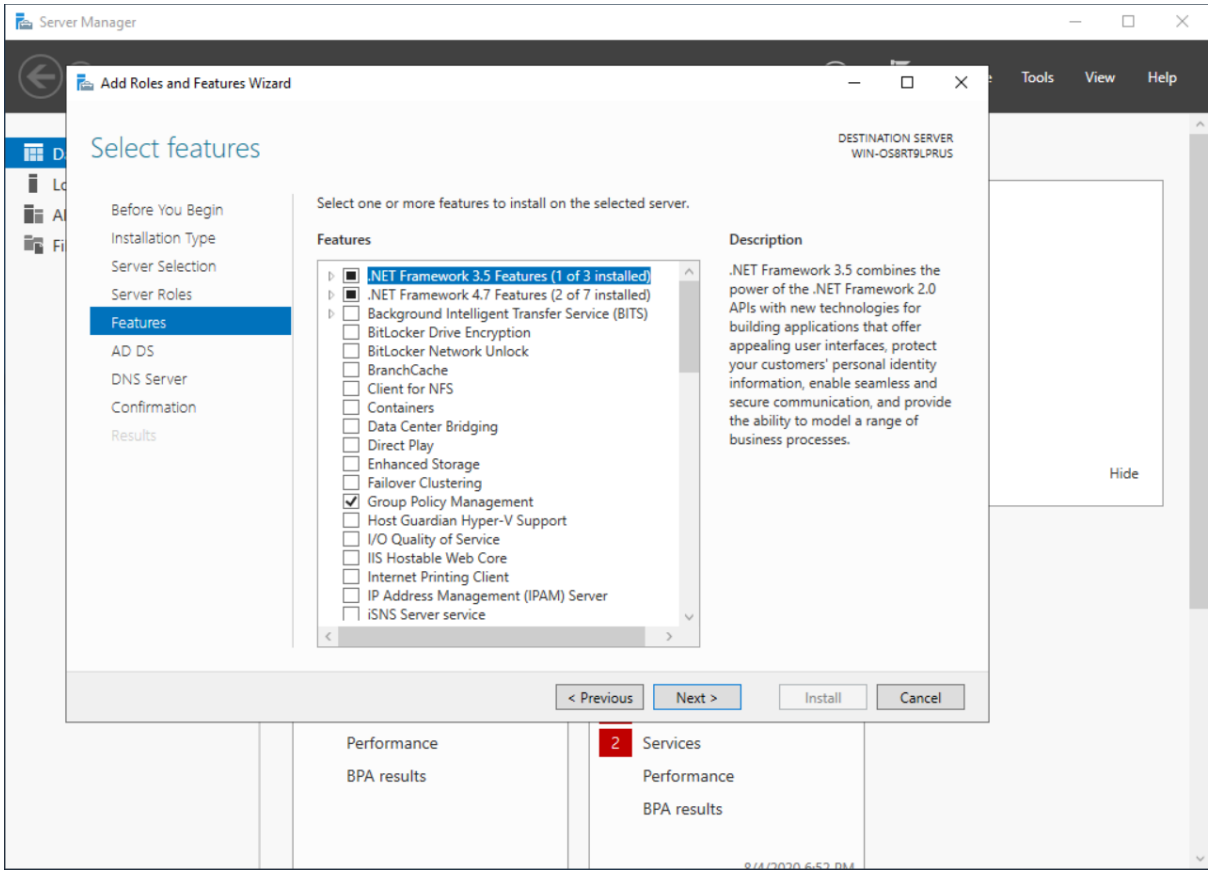


6. Select the functions that need to be installed "Active Directory Domain Services" and "DNS Server", then click "Next".

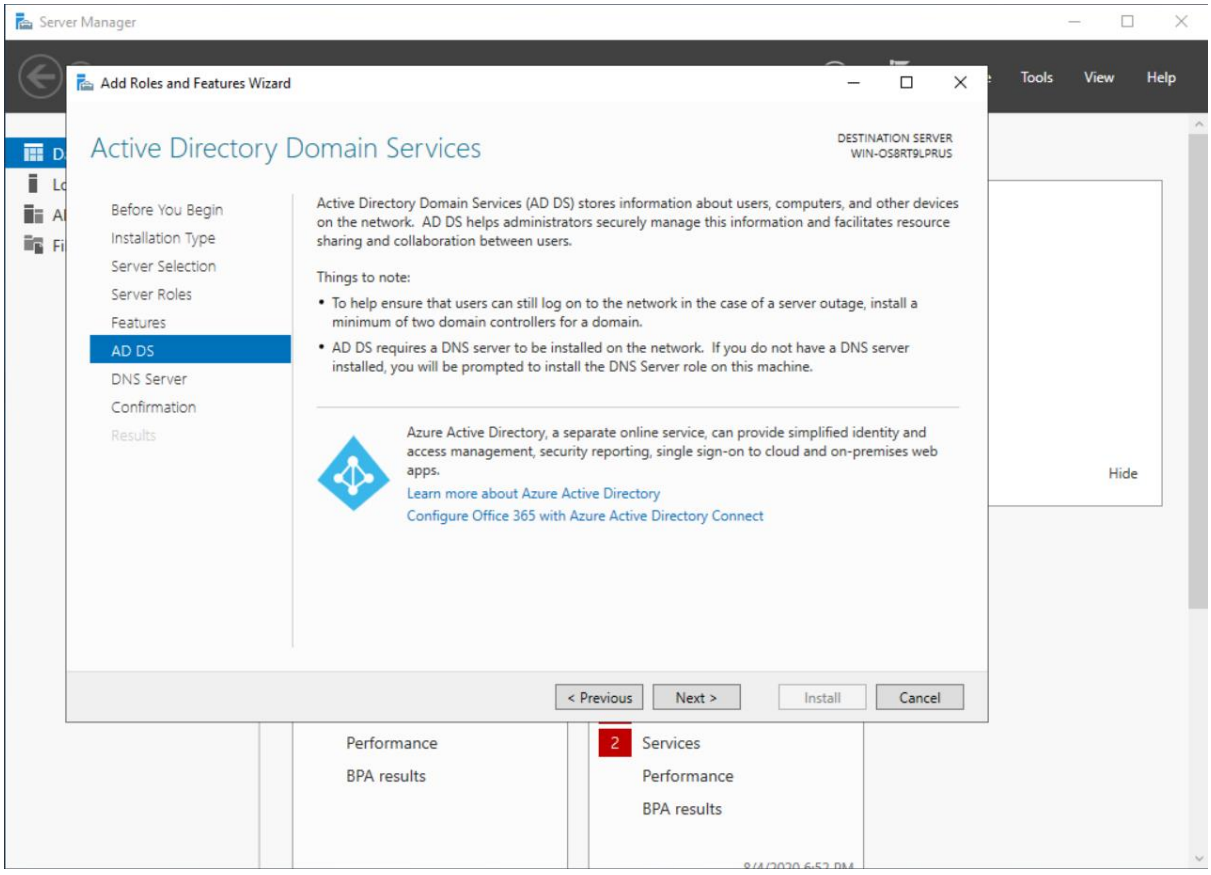

Server Manager
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-OS8RT9LPRUS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Performance
BPA results
2
Services
Performance
BPA results


Server Manager
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-OS8RT9LPRUS
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Performance
BPA results
2
Services
Performance
BPA results

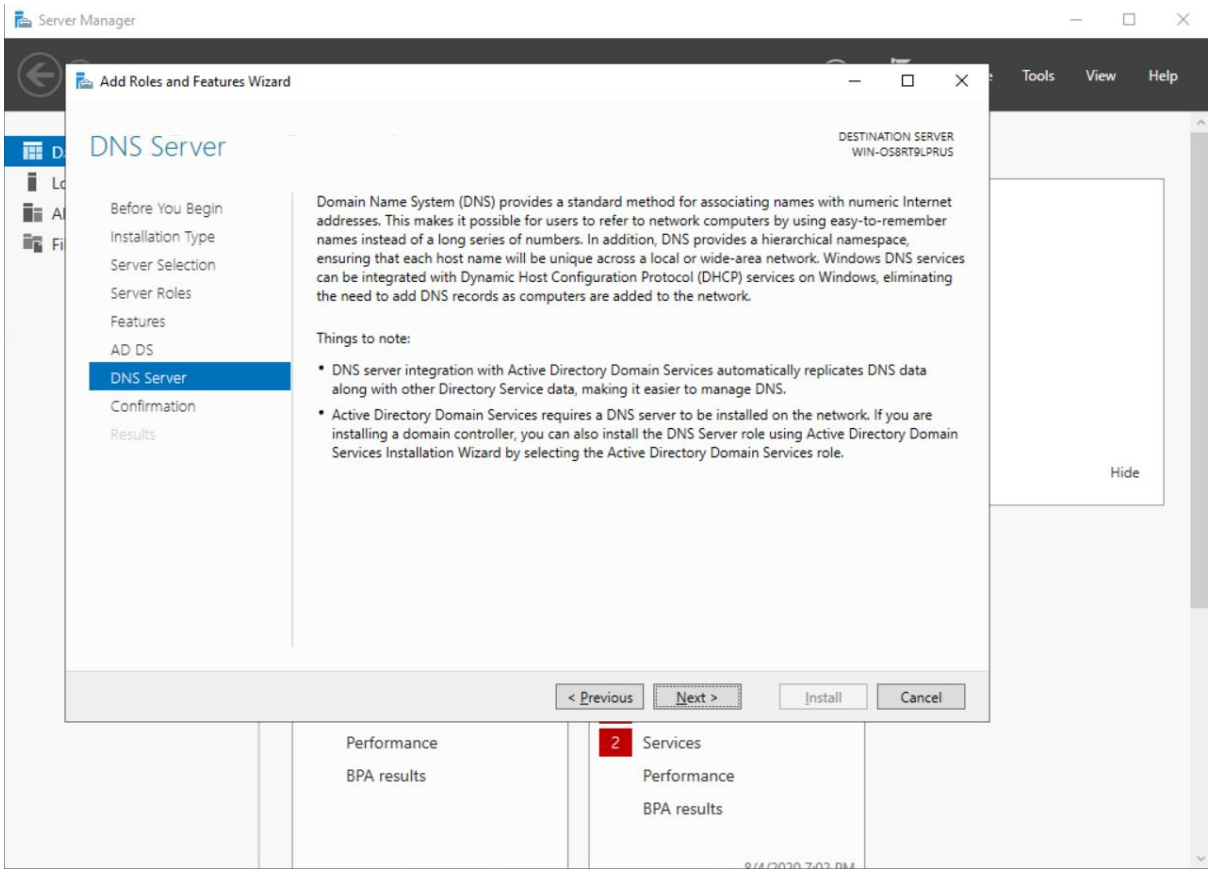
7. Click "Next".



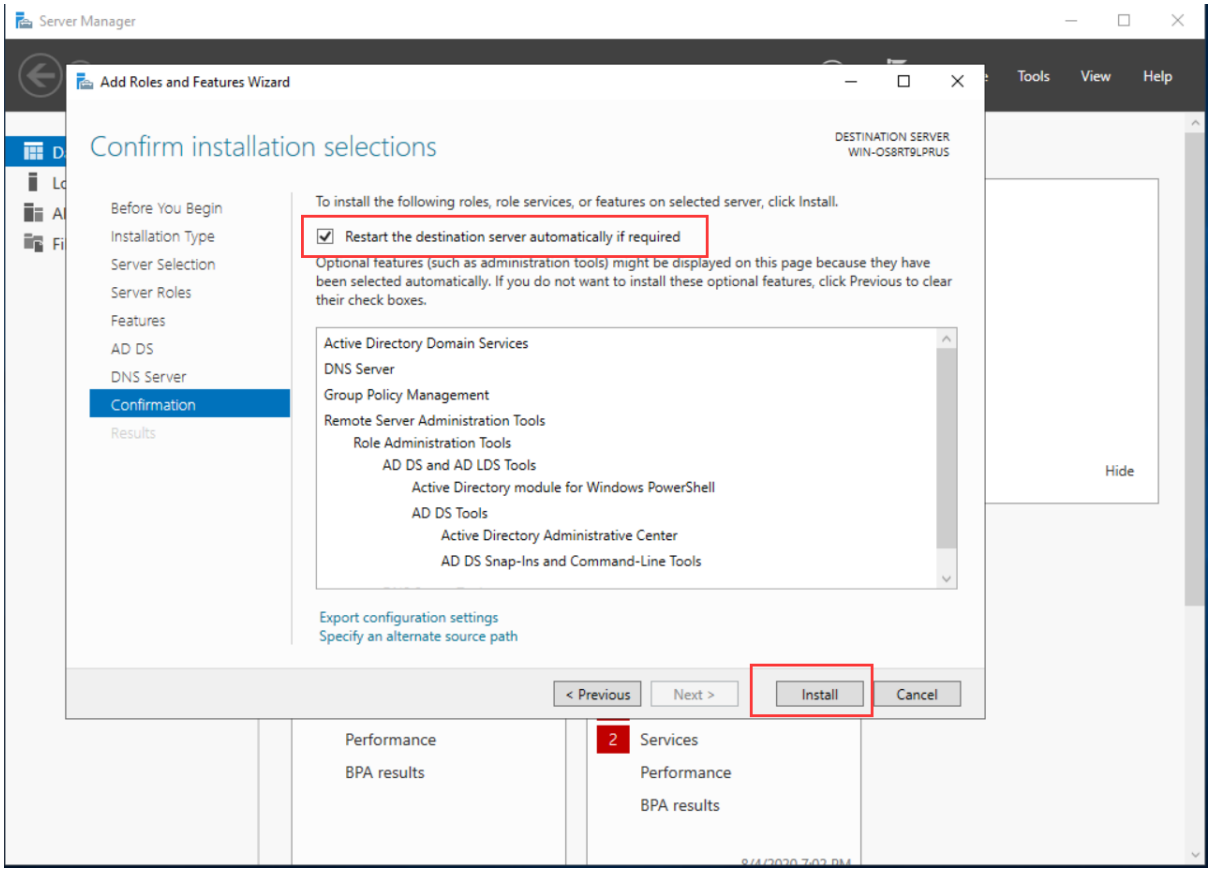
8. Click "Next".

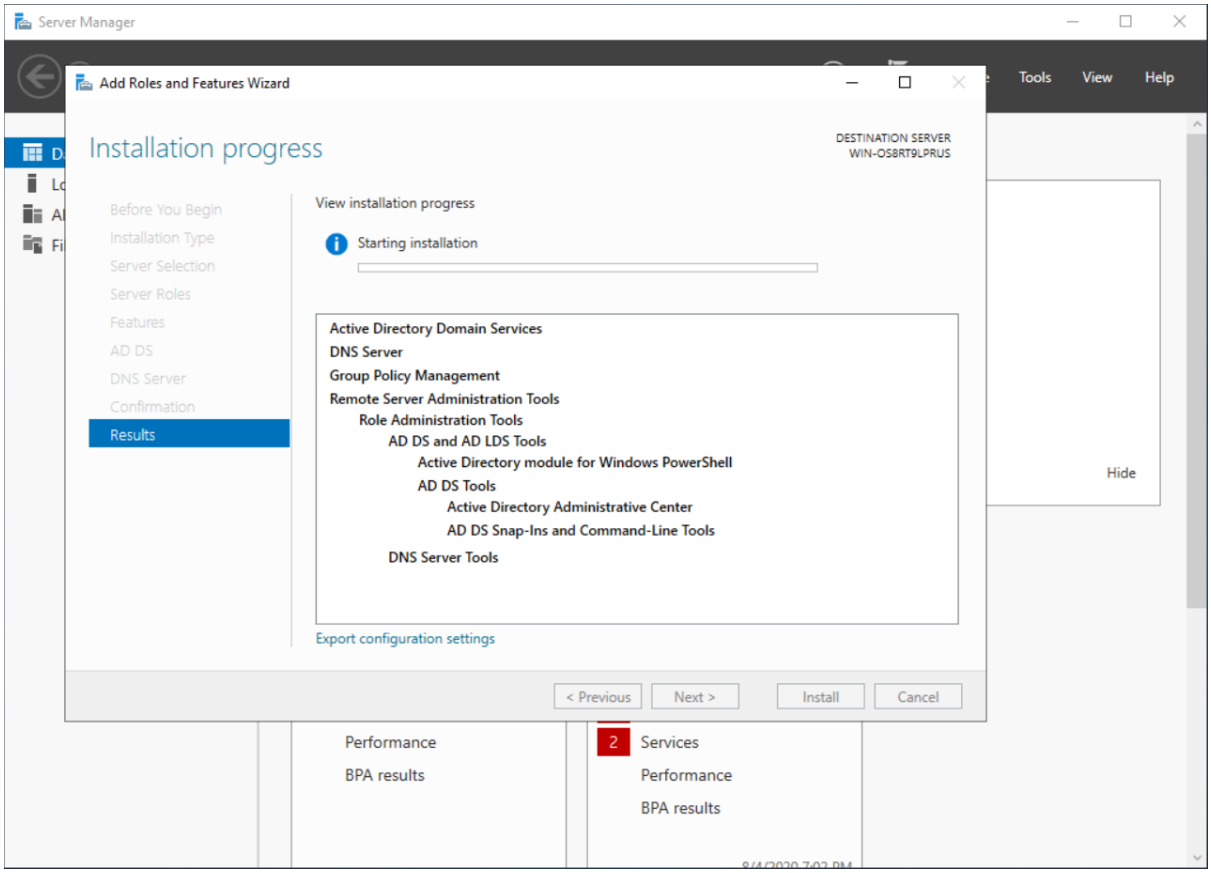


9. Click "Next".

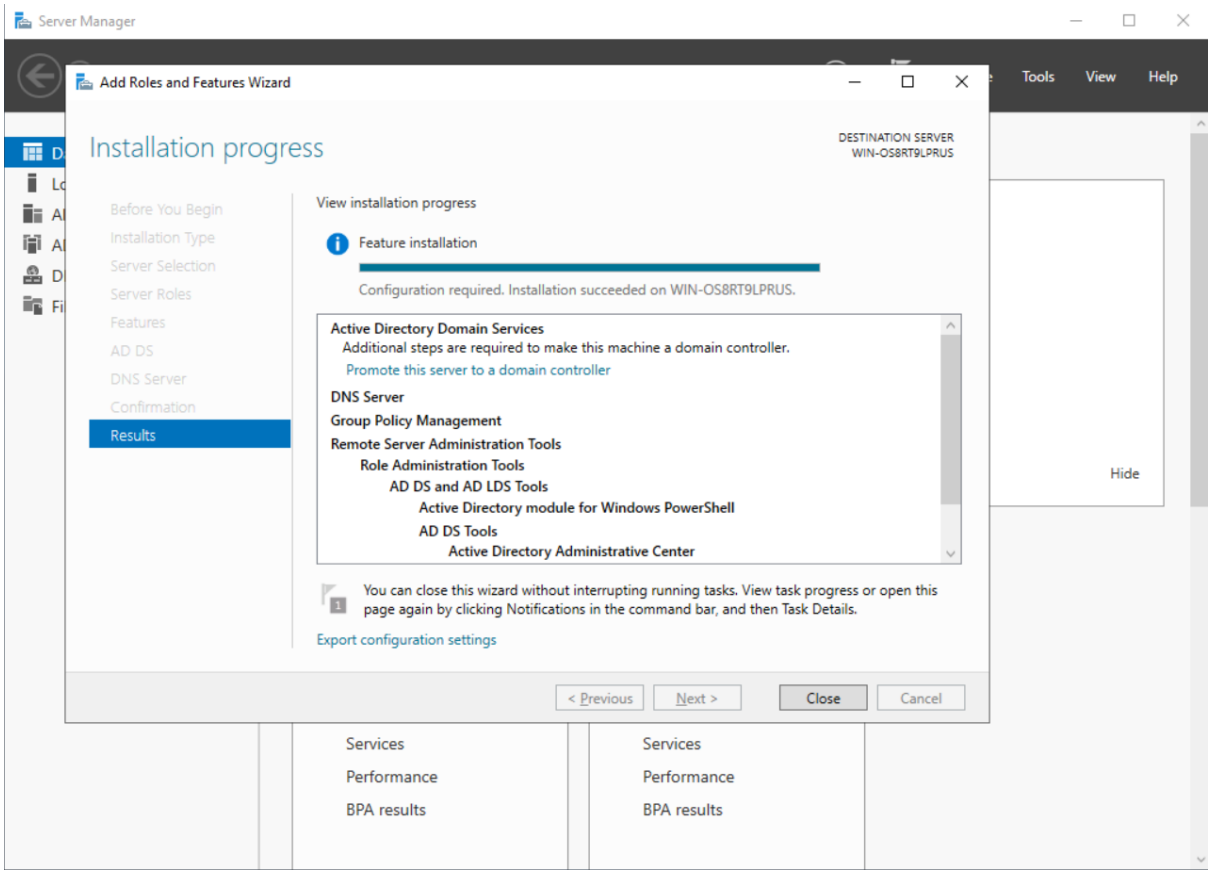


10. Click "Install".



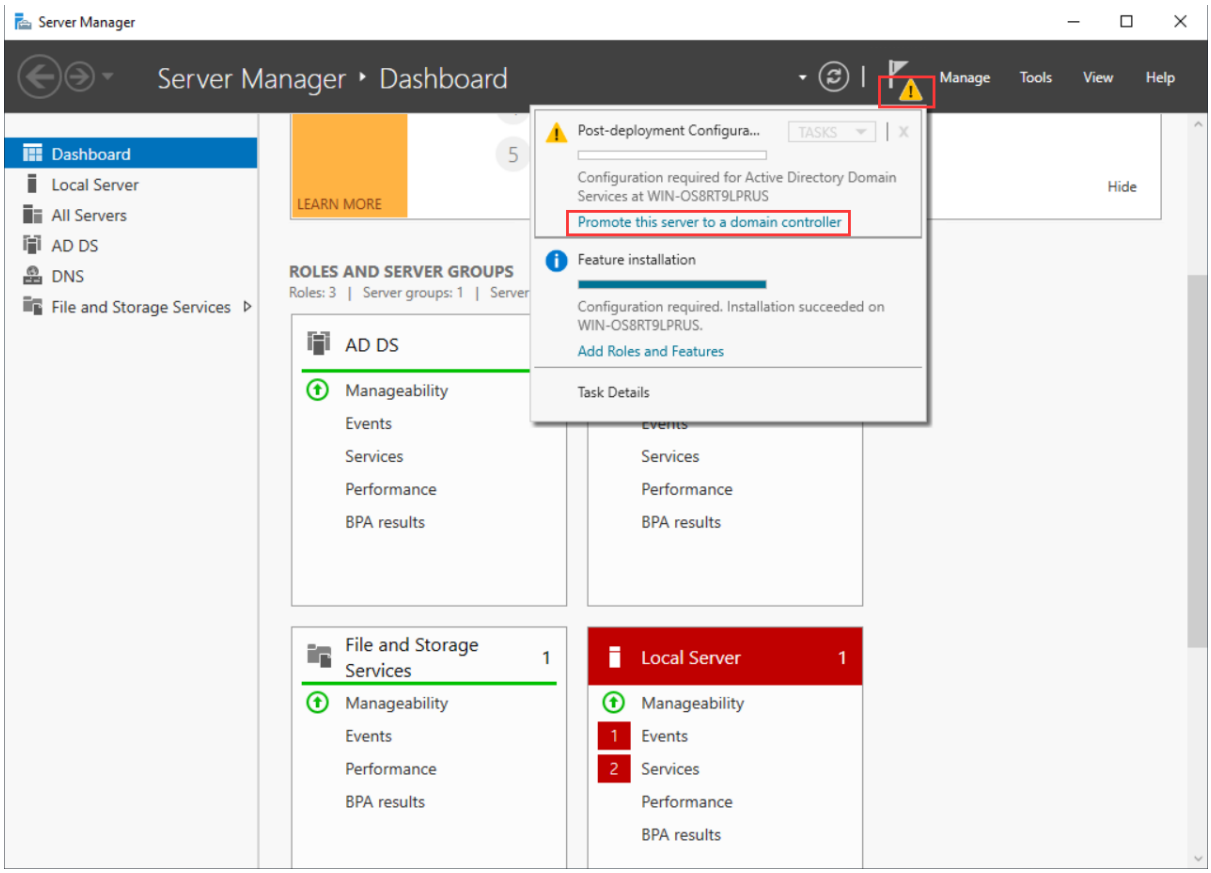


11. Click "Close" after installation.

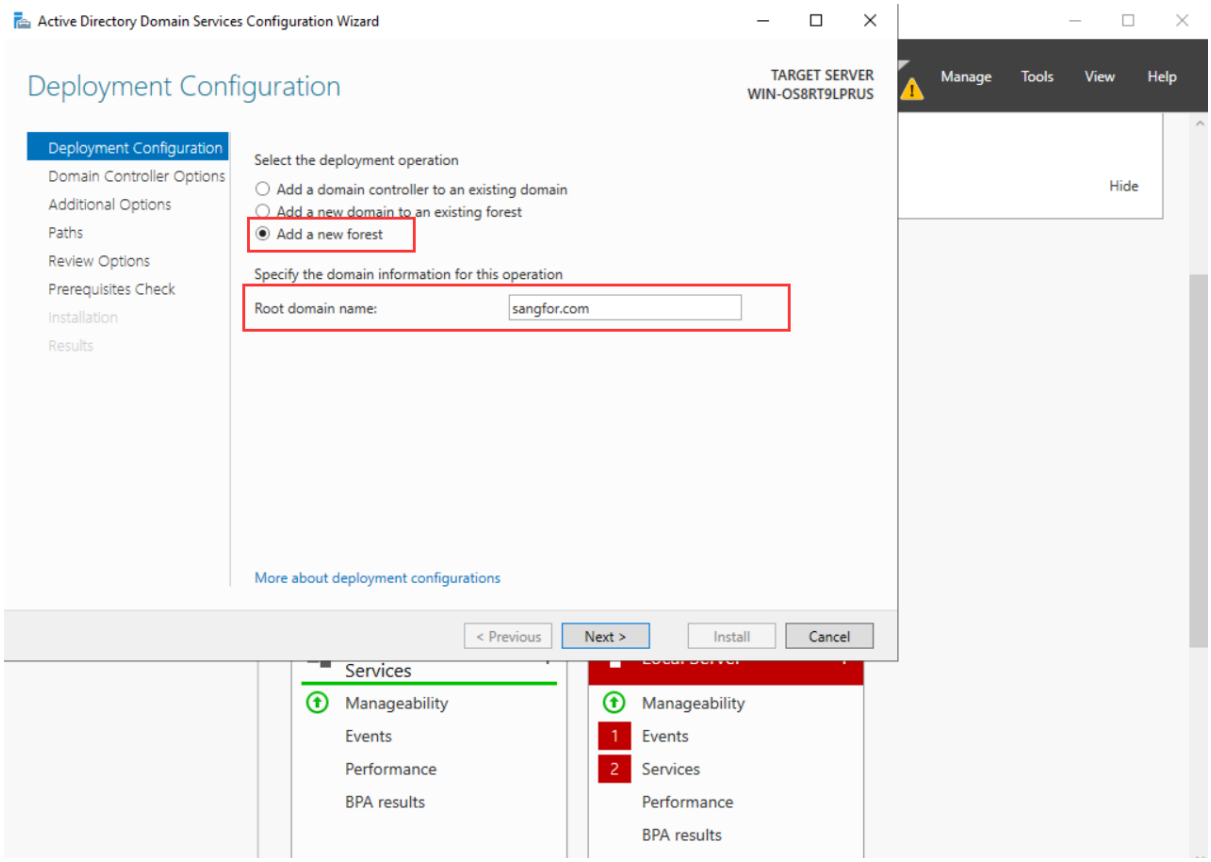


2.2 Configure the domain controller server

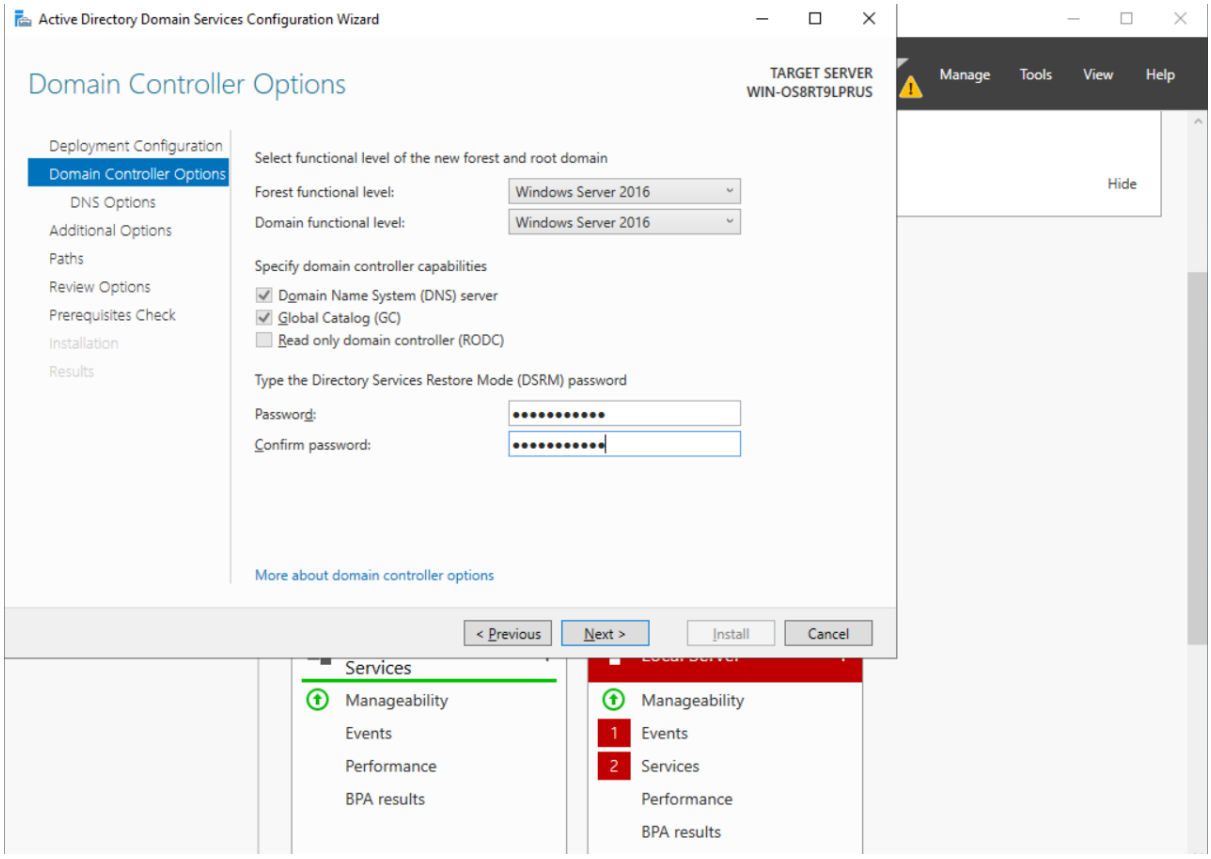
1. According to the following figure, select "Promote this server to a domain controller".



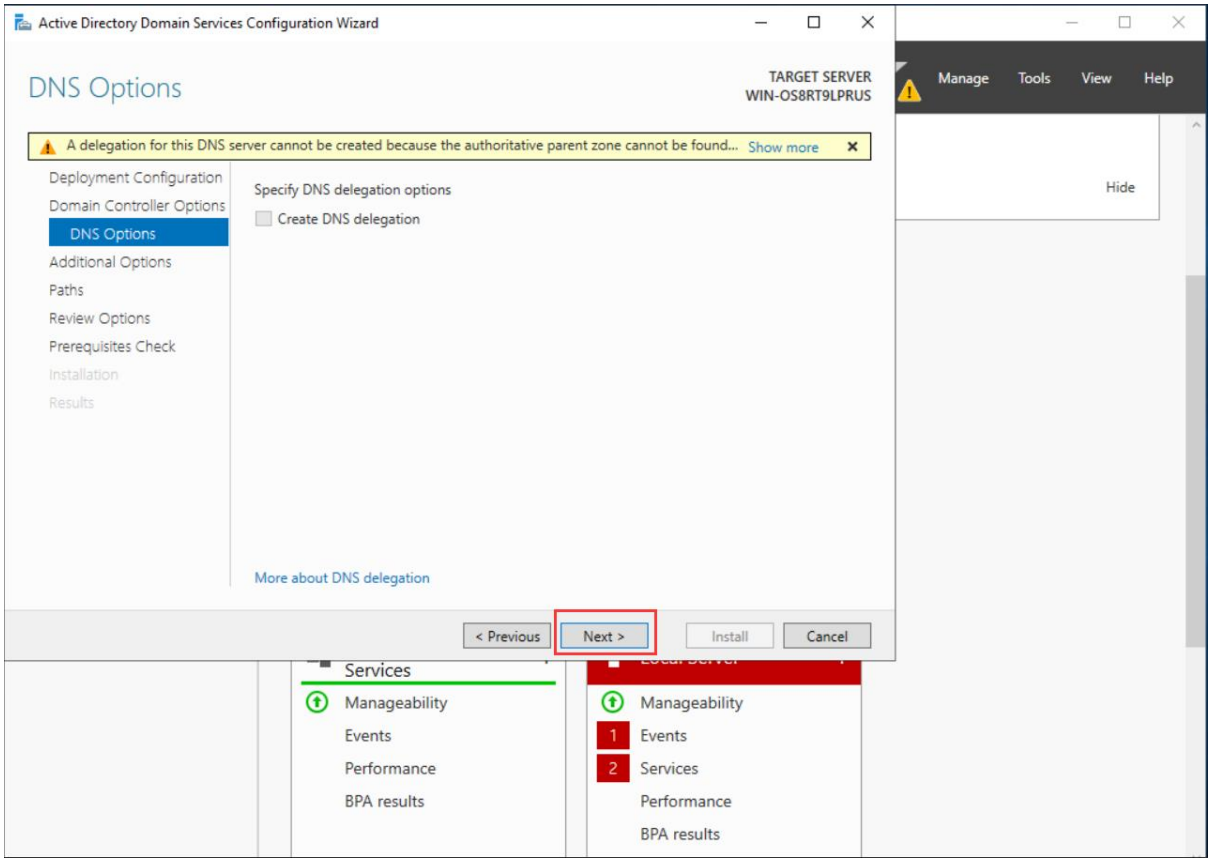
2. Configure the domain name for the AD domain, such as sangfor.com.



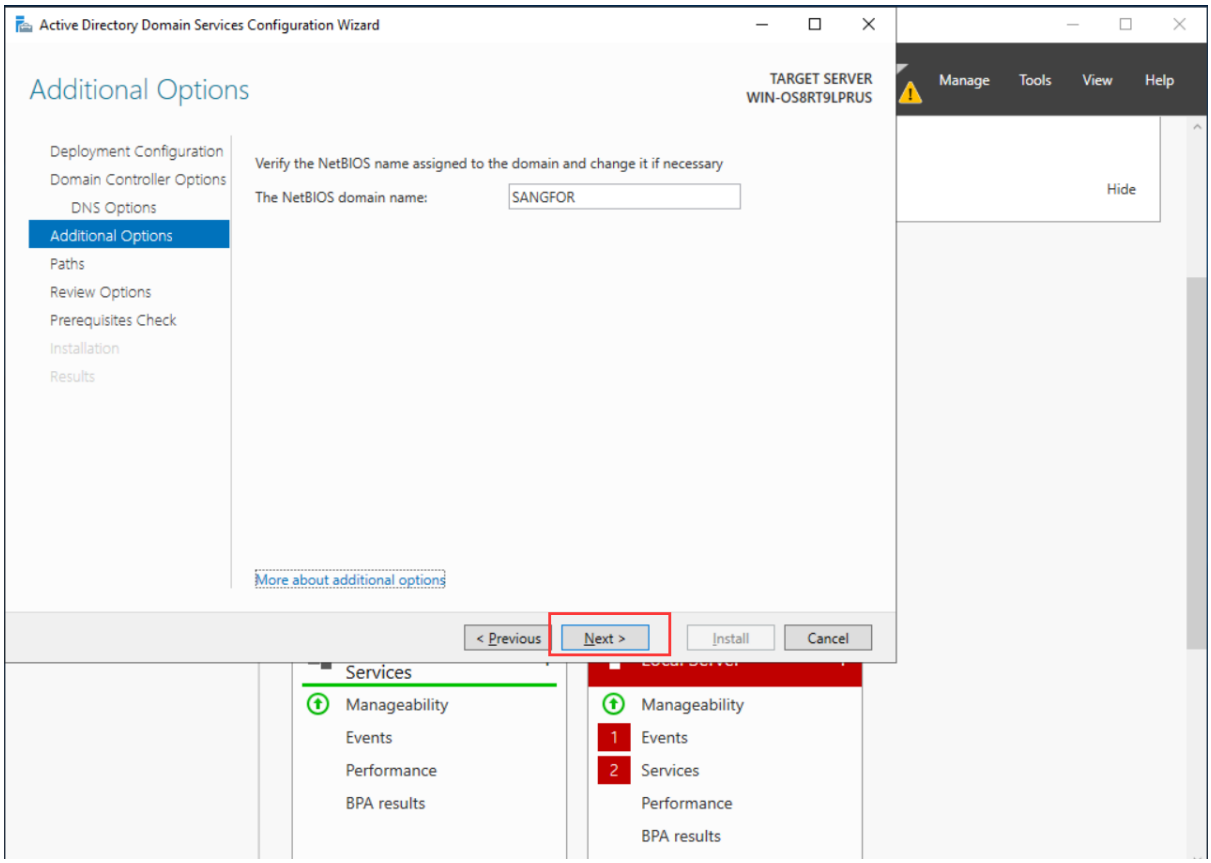
3. Set a password, for example @sangfortest.



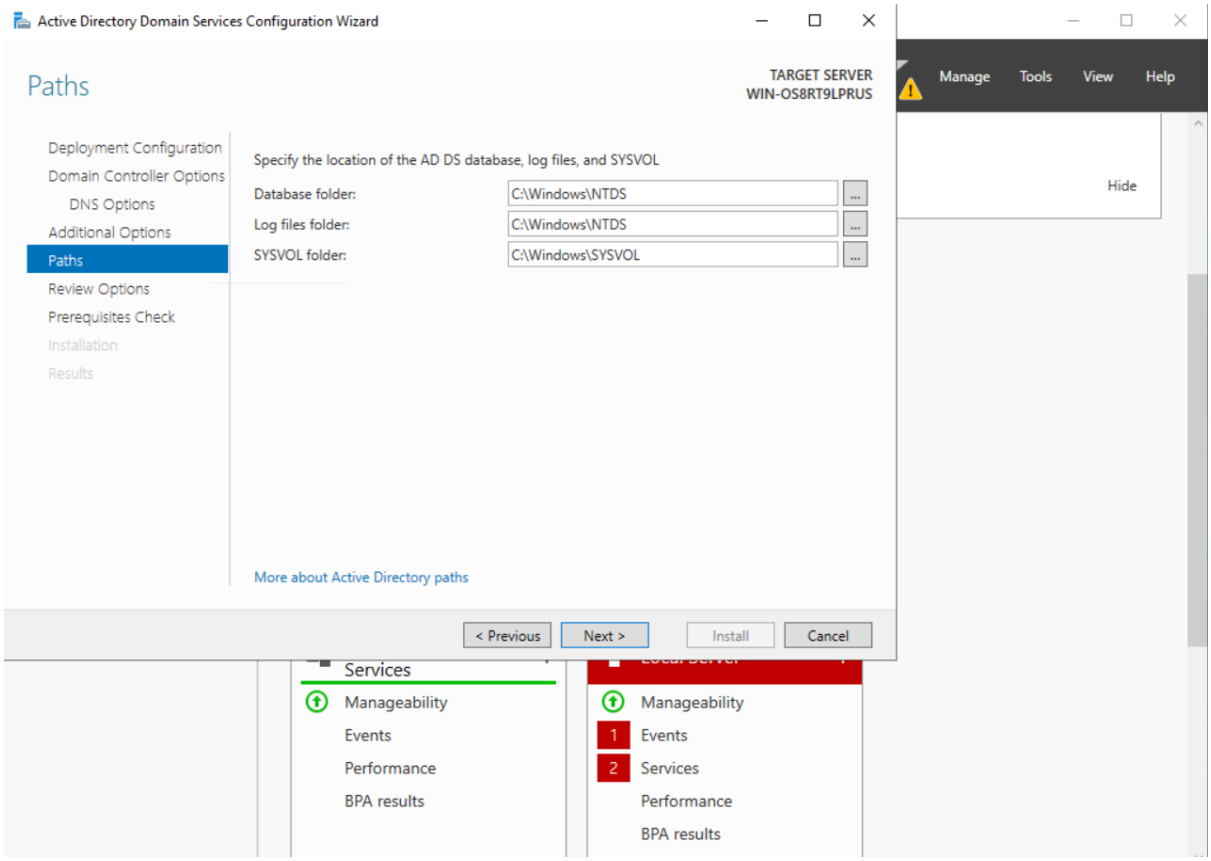
4. Click "Next".



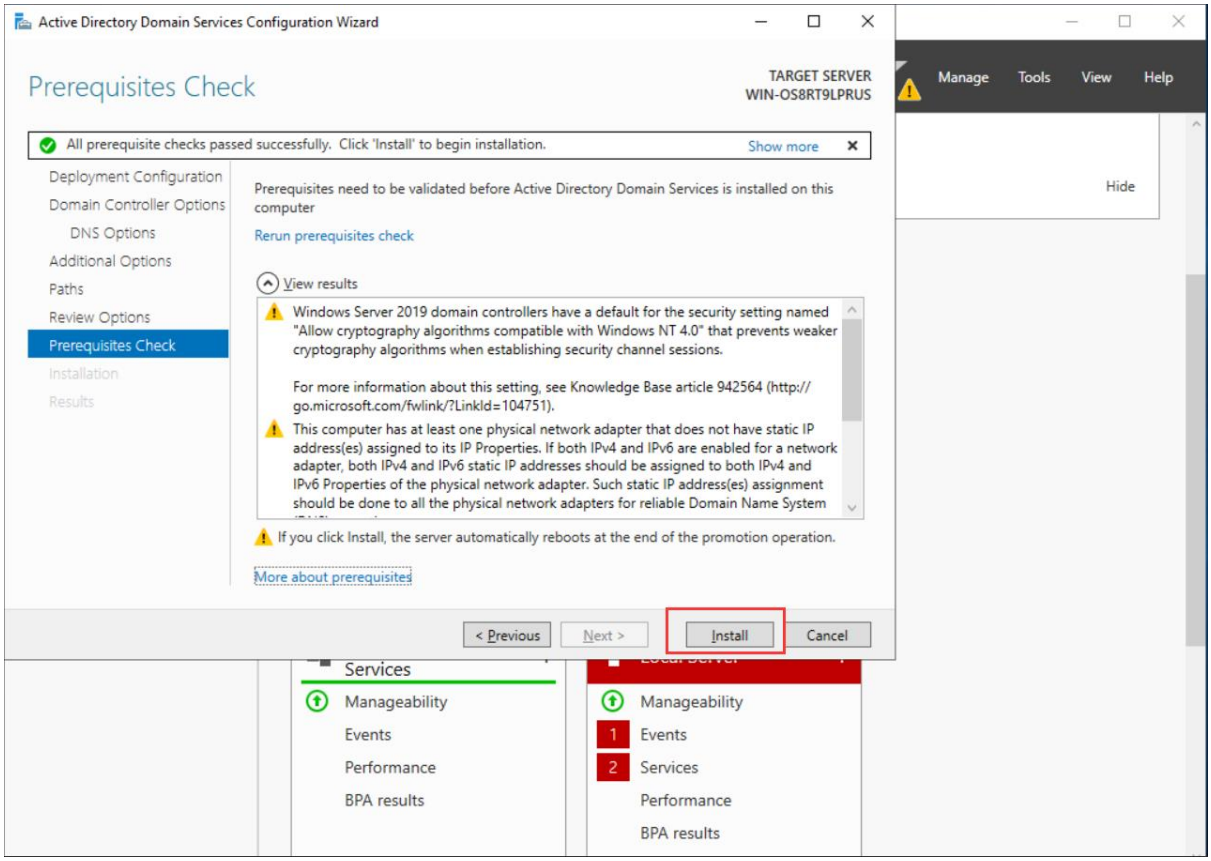
5. Set NETBIOS Domain Name, you can use the default SANGFOR.



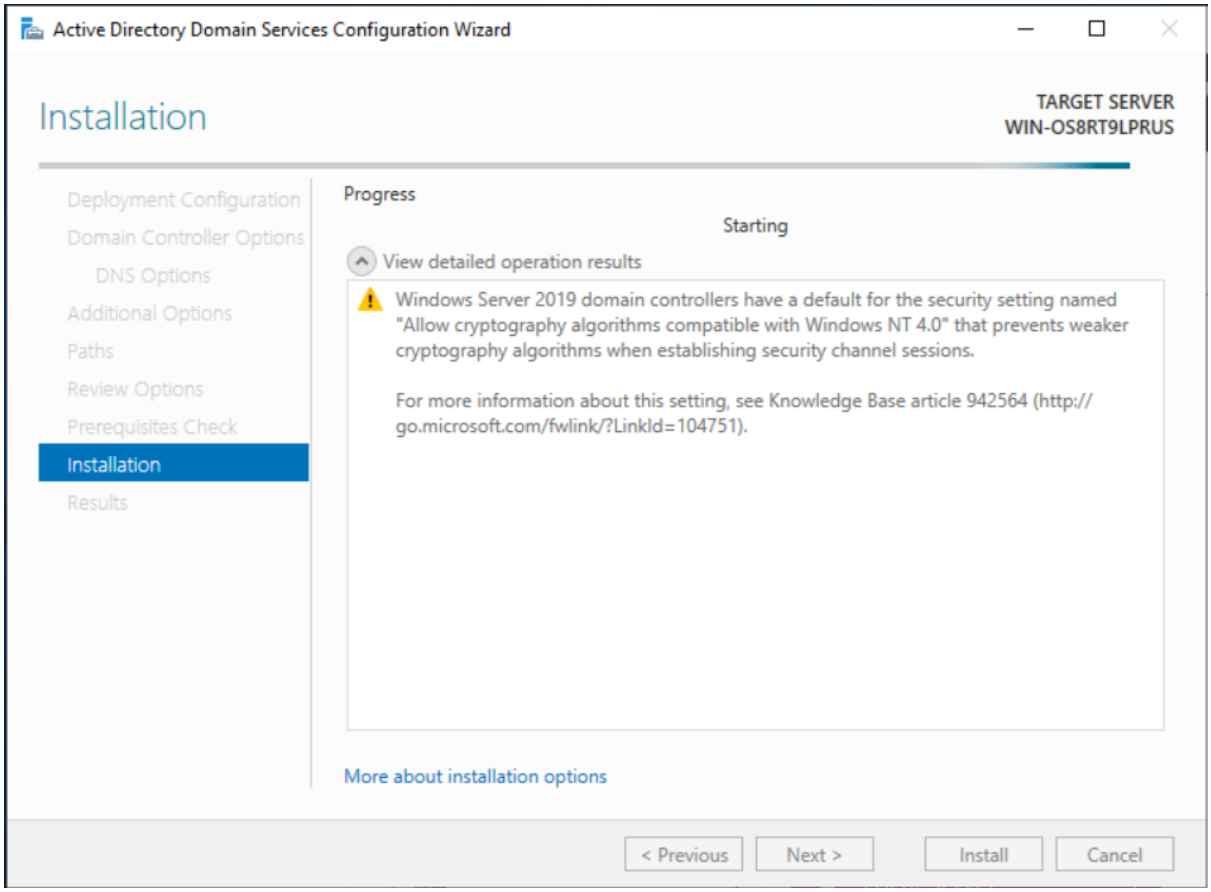
6.Click "Next".



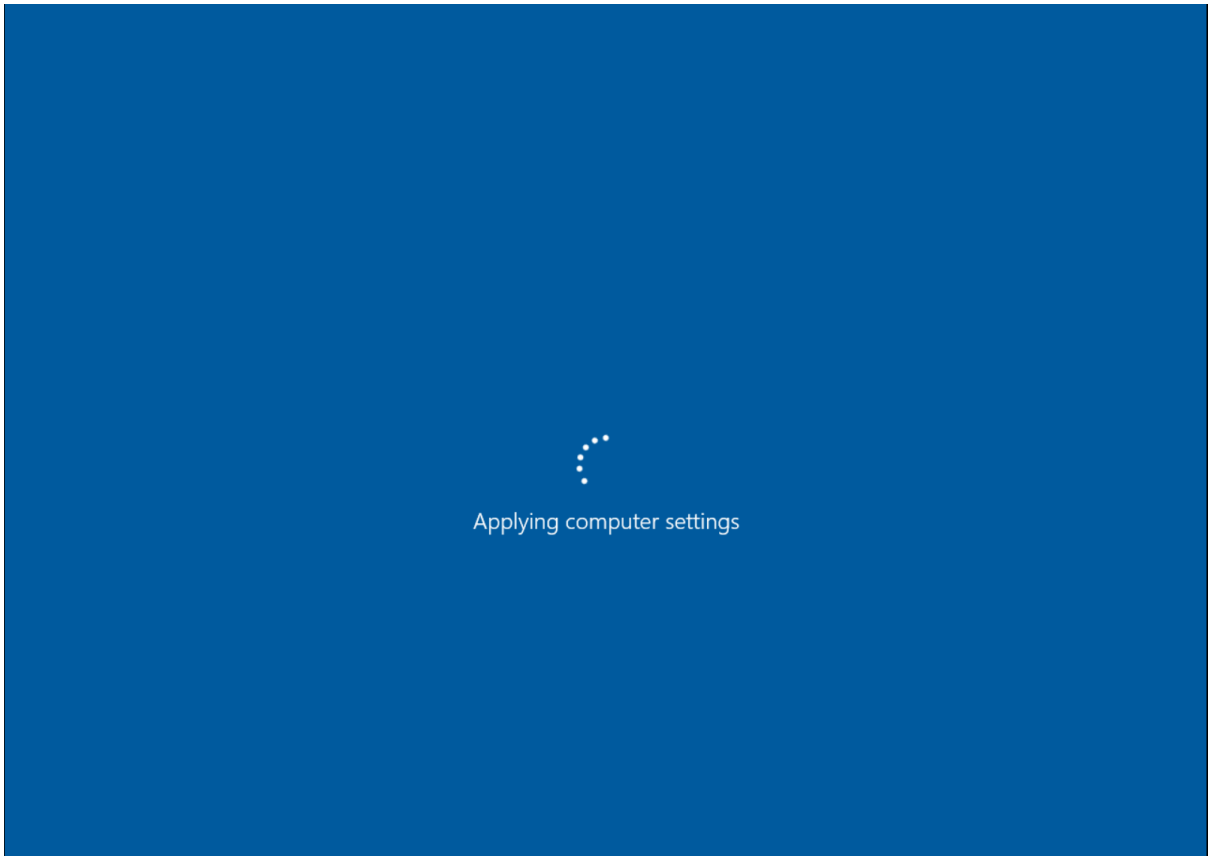
7.Select "Install".



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

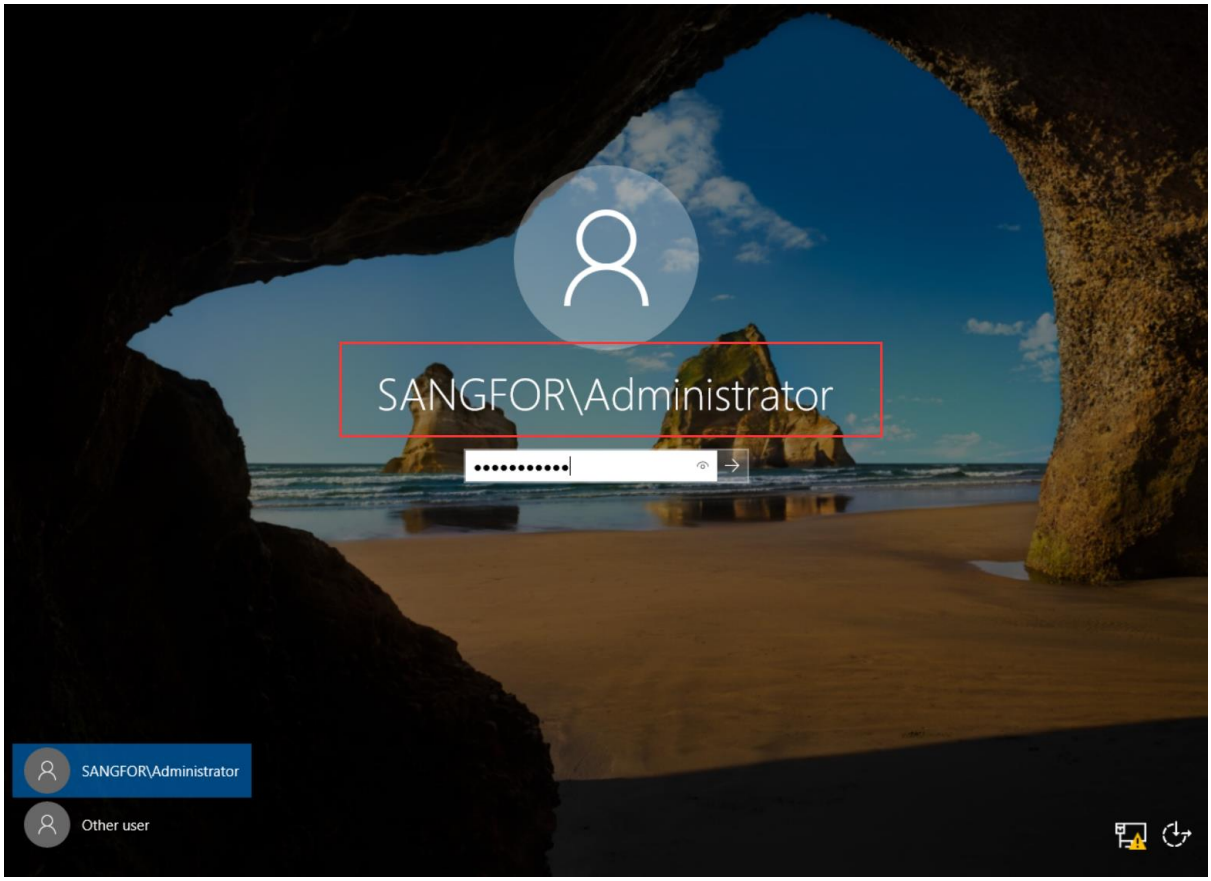


9. After the installation is complete, Windows Server will automatically restart.



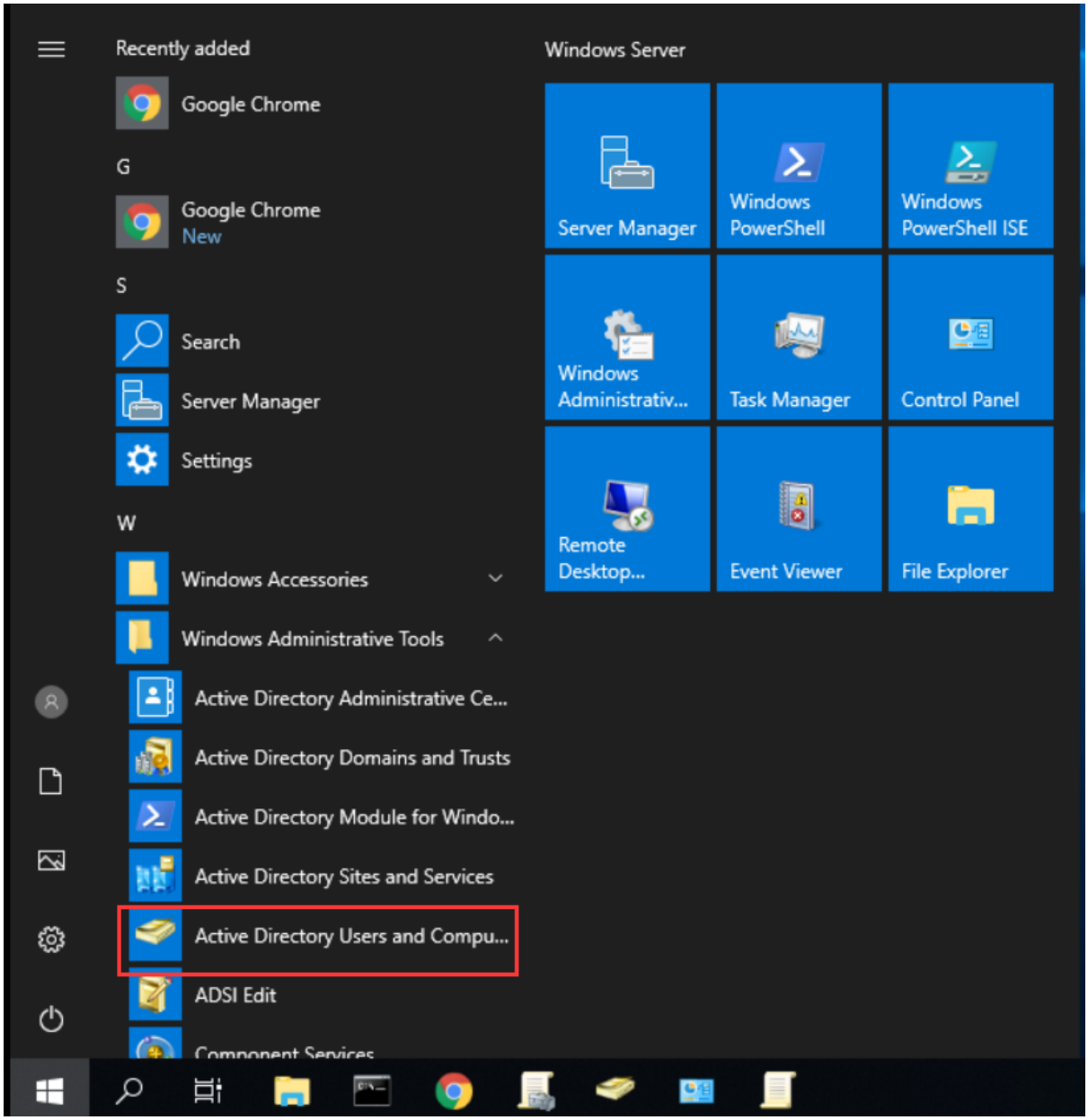
10. After the Windows Server restarts, you can see on the login page that the default local administrator

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.

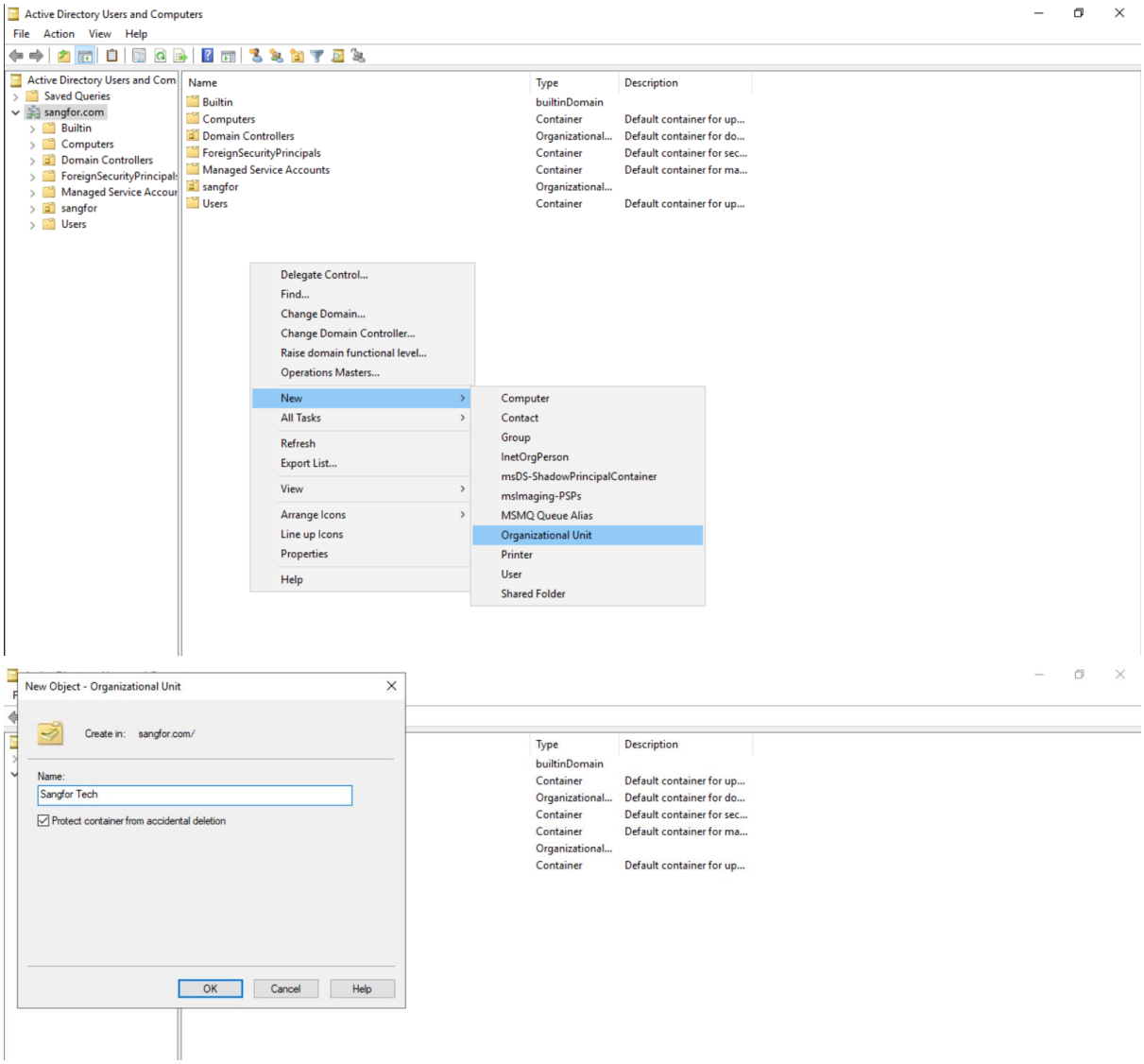


2.3 Create usernames and passwords for other users in the domain

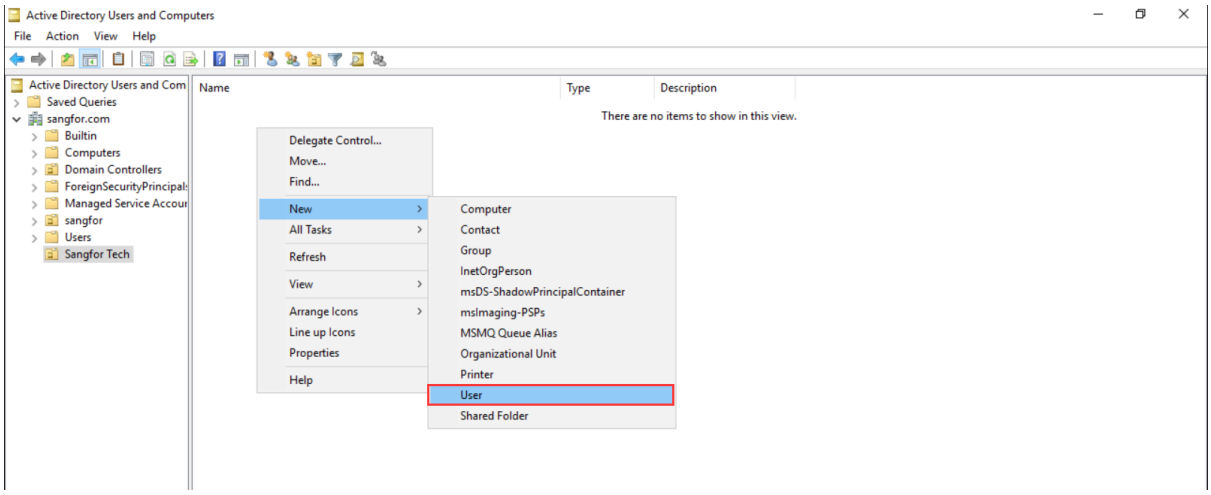
1.Open "Active Directory Users and Computers".

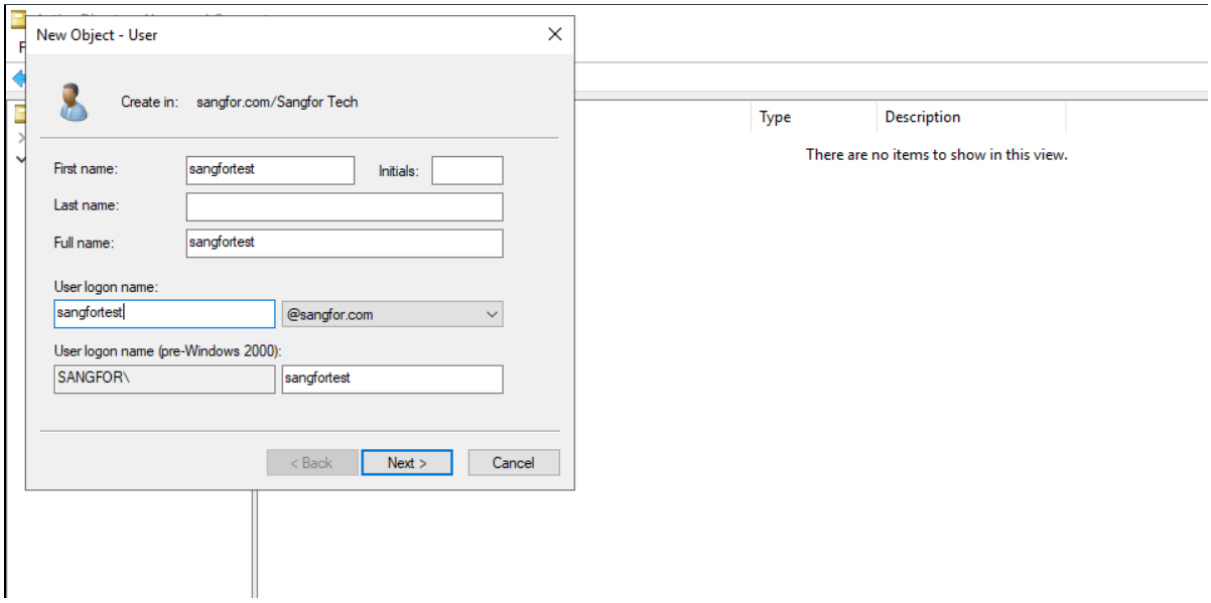


2. In order to facilitate the management of users according to the company's organizational structure, a logical container is created here to represent a department. For example, create a department called Sangfor Tech.

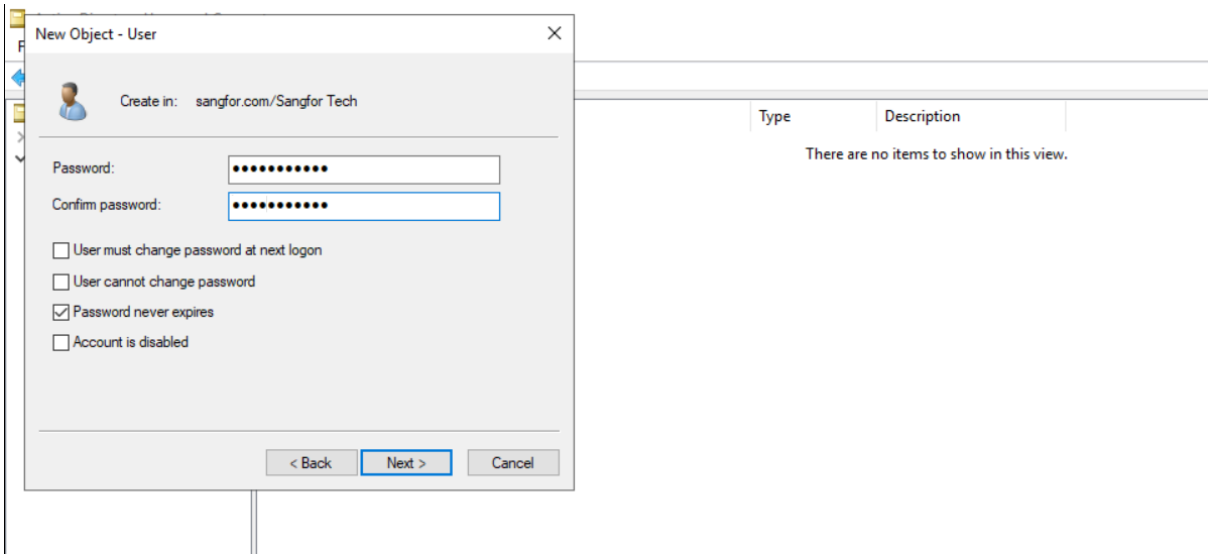


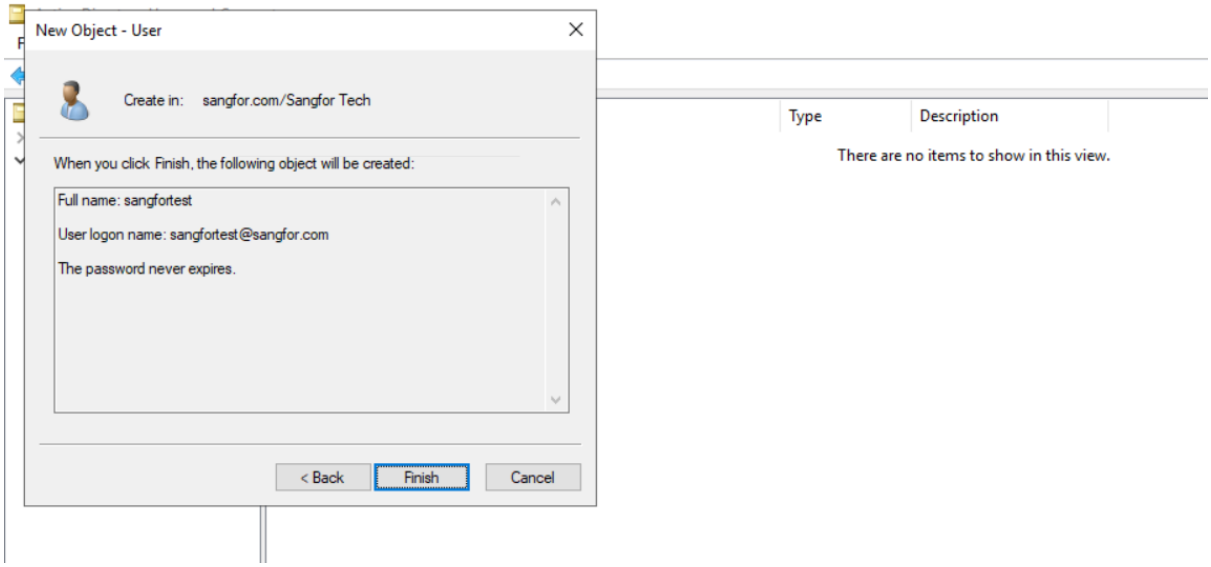
3. Create a user in the container, for example called sangfortest.





Set a login password for this user.



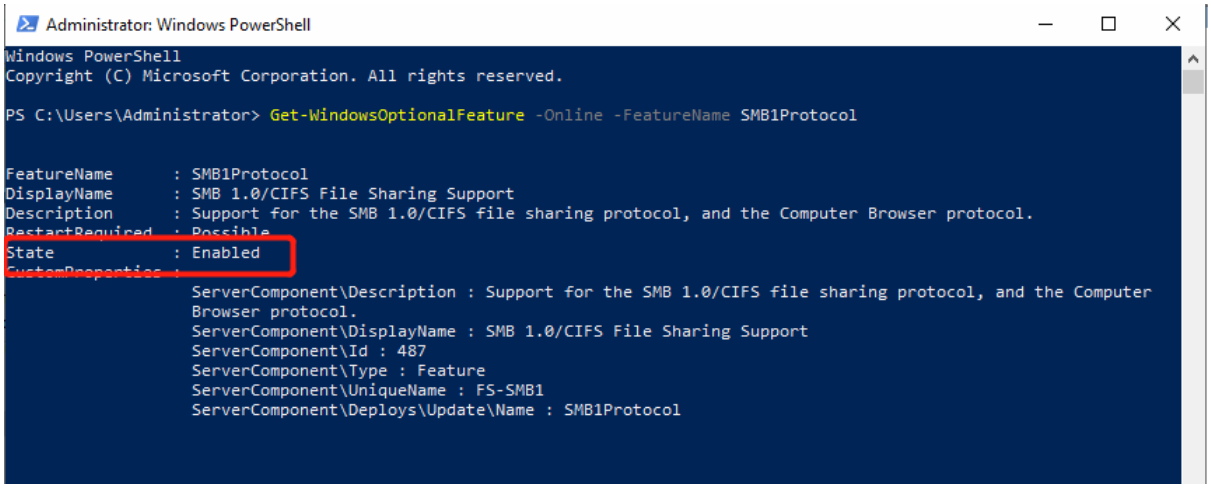


2.4 Enable SMBv1 of Windows Server

The interaction between IAM and Windows Server requires the use of the SMBv1 protocol, and some Windows Servers disable the SMBv1 protocol by default, so you need to manually enable it.

1. Open Powershell with administrator permission.

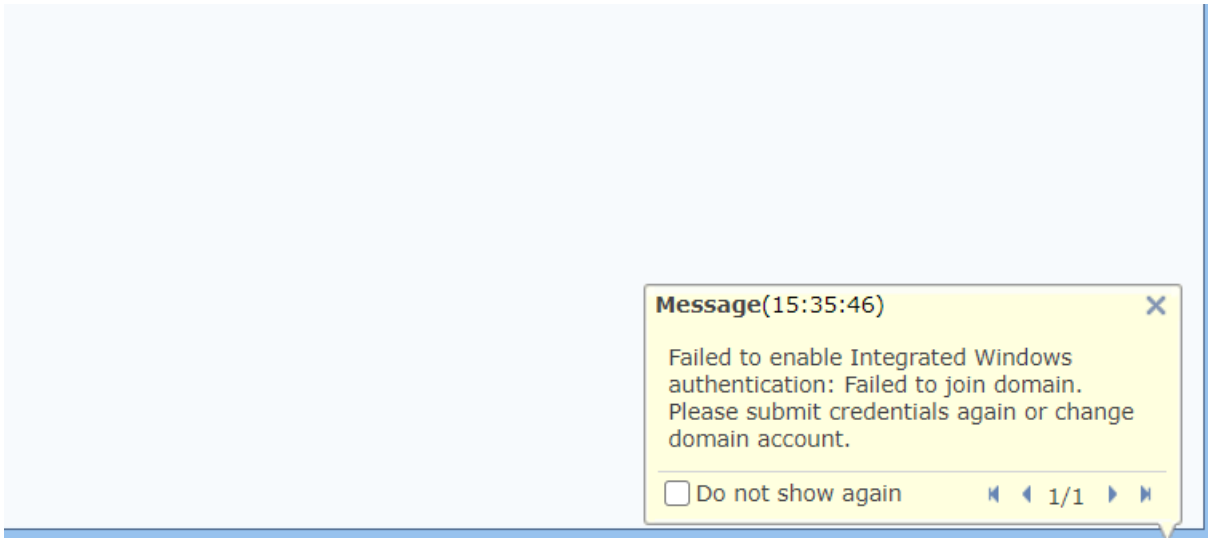
2.Use **Get-WindowsOptionalFeature –Online –FeatureName SMB1Protocol** command to check the SMBv1 Status.



3. Use **Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol** command to enable SMBv1, then the windows server will restart to apply the function.

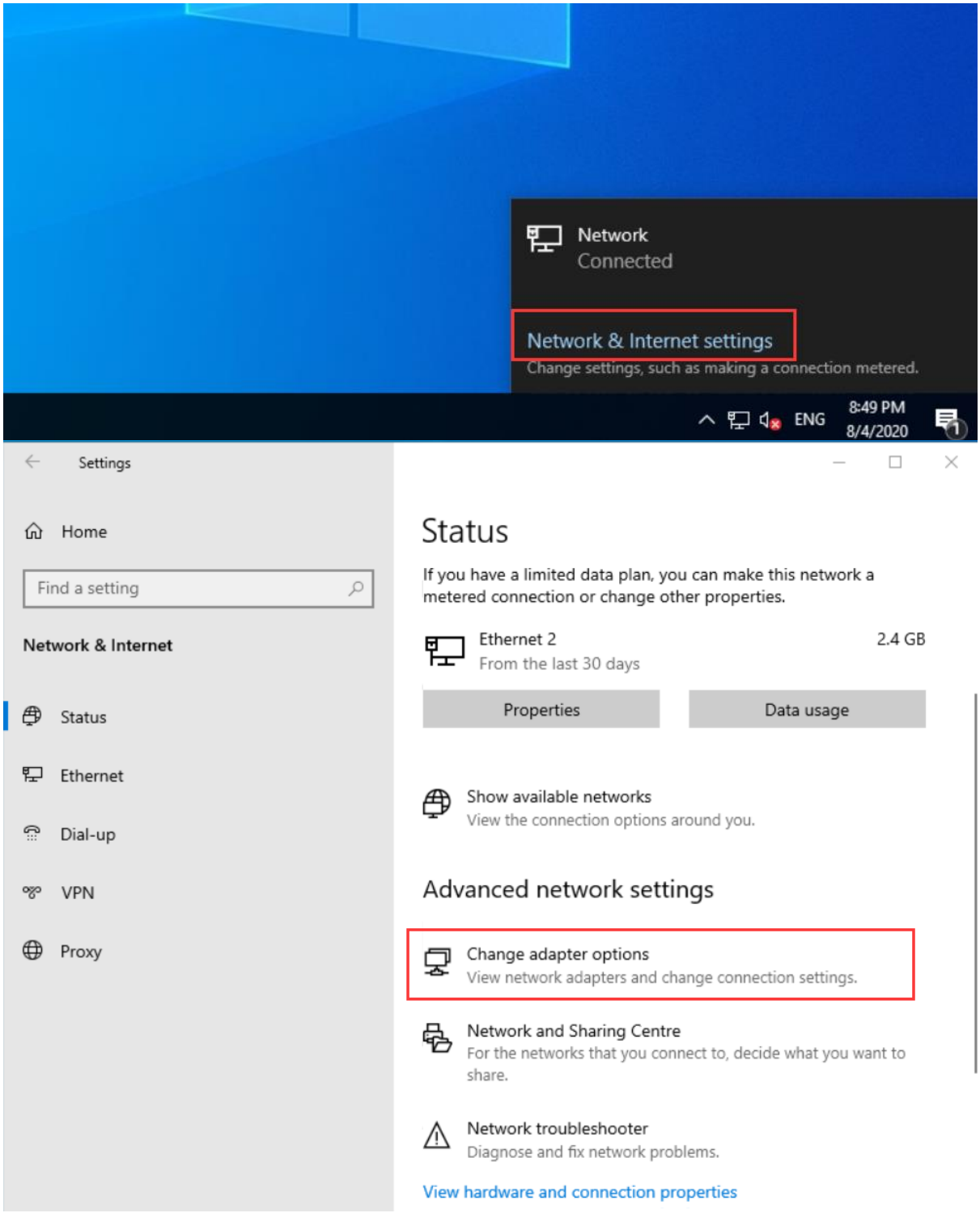
4. For more method of each version of windows server, you can look Microsoft Website for more details.

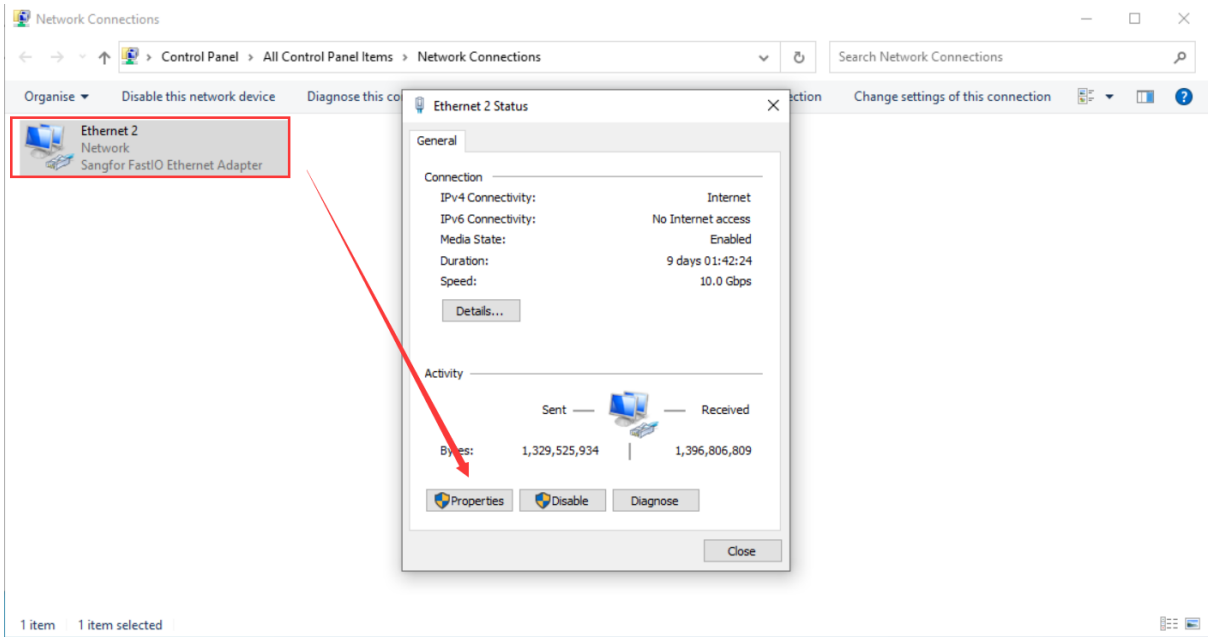
5.If you not enable the SMBv1, it will show following error.

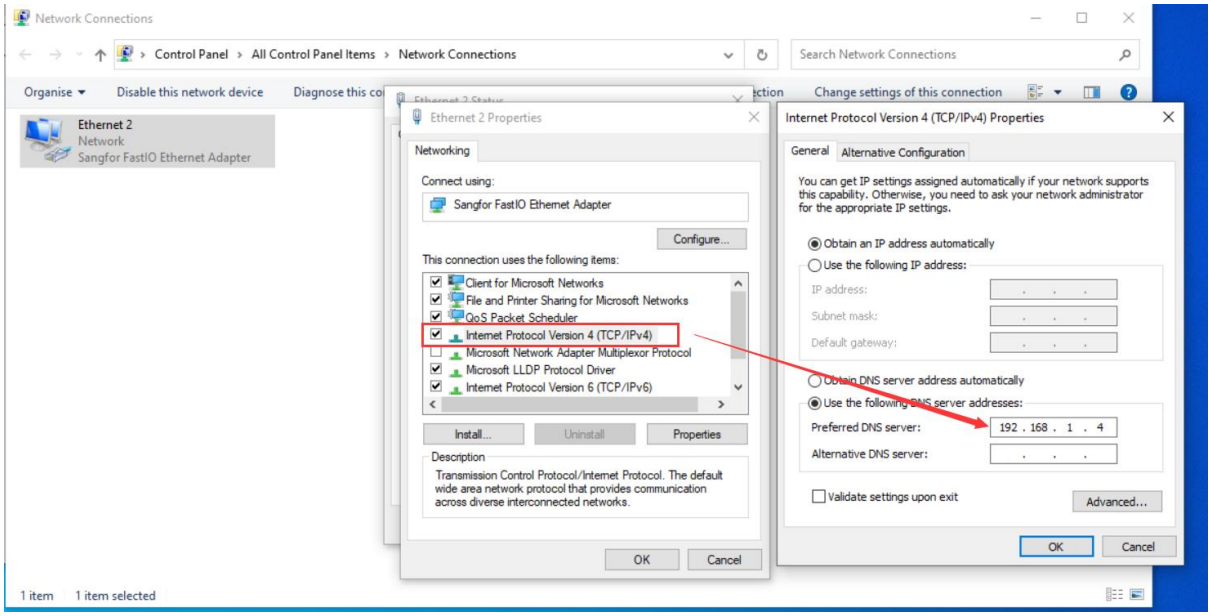


2.5 Join the PC to the domain

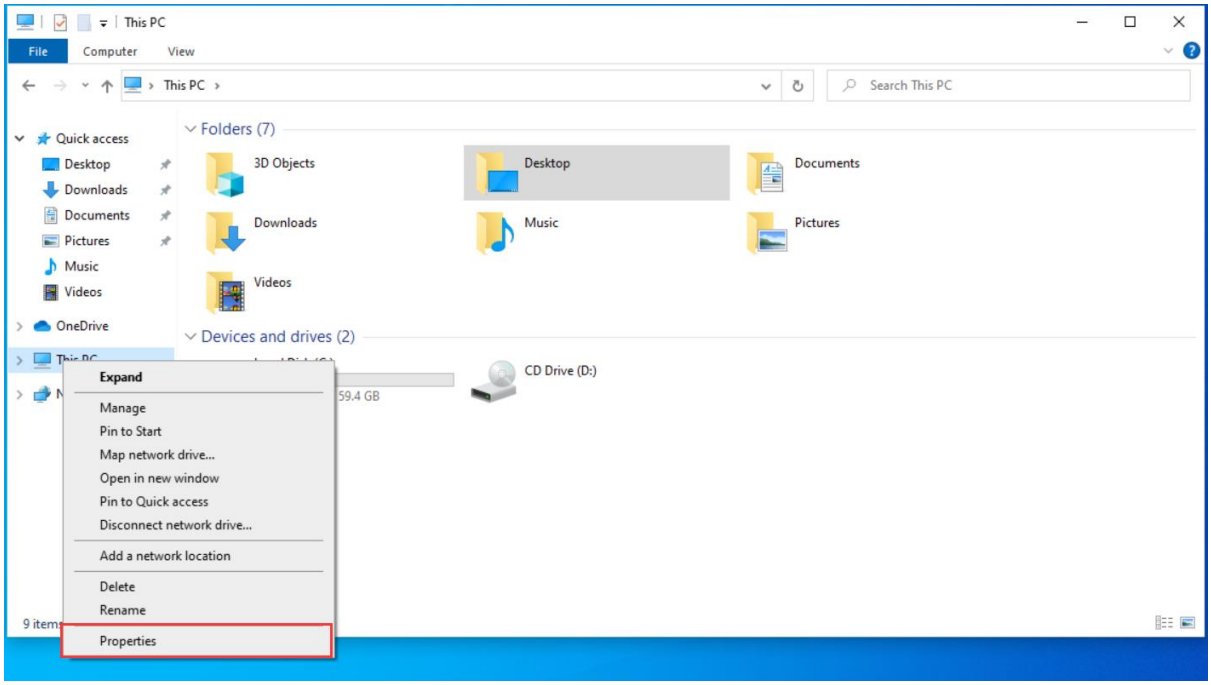
1. Configure the PC's network card, and configure DNS as the IP of the domain control server: 192.168.1.4

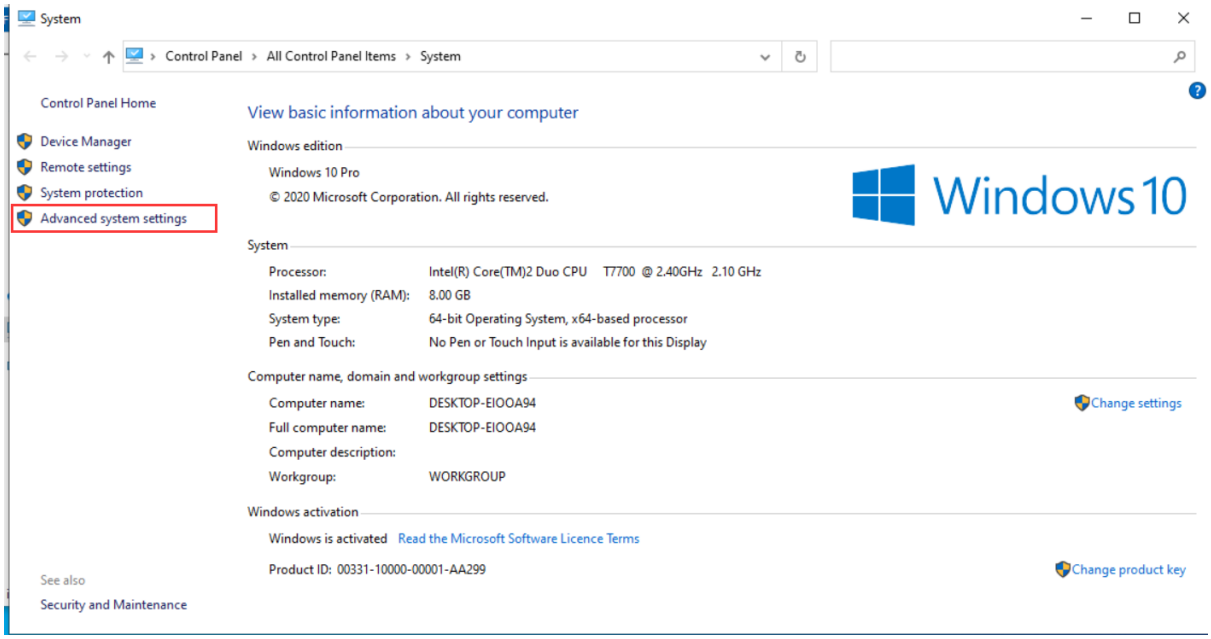

Network
Connected
Network & Internet settings
Change settings, such as making a connection metered.
ENG
8:49 PM
8/4/2020
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
Status
If you have a limited data plan, you can make this network a metered connection or change other properties.
Ethernet 2
From the last 30 days
2.4 GB
Properties
Data usage
Show available networks
View the connection options around you.
Advanced network settings
Change adapter options
View network adapters and change connection settings.
Network and Sharing Centre
For the networks that you connect to, decide what you want to share.
Network troubleshooter
Diagnose and fix network problems.
View hardware and connection properties

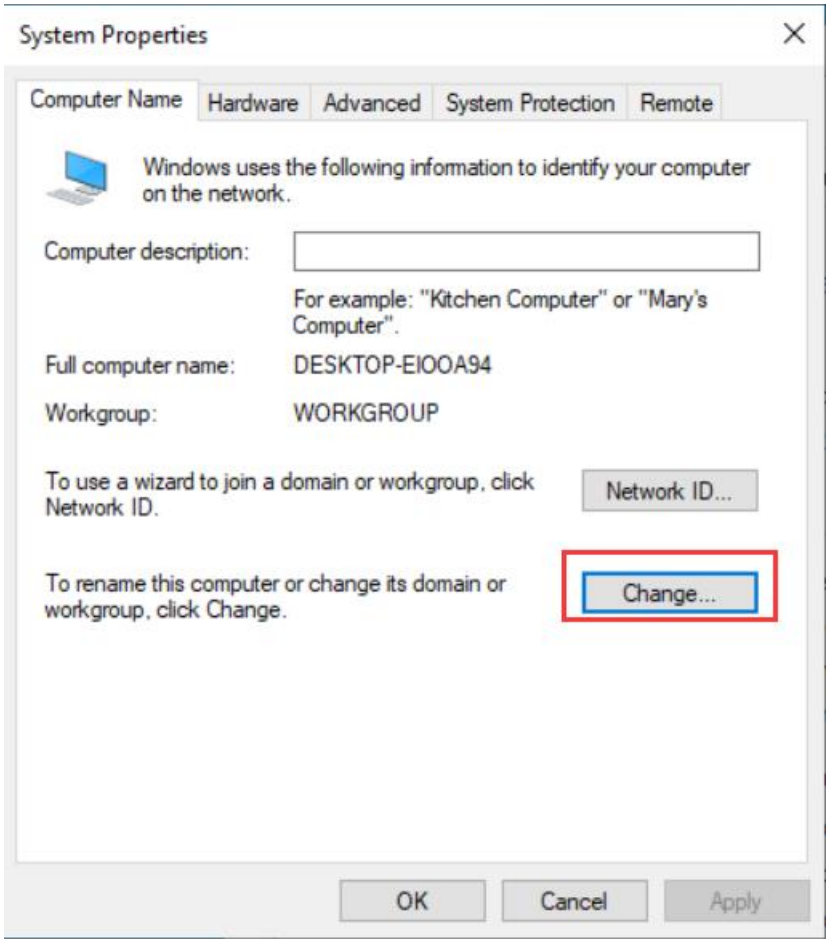


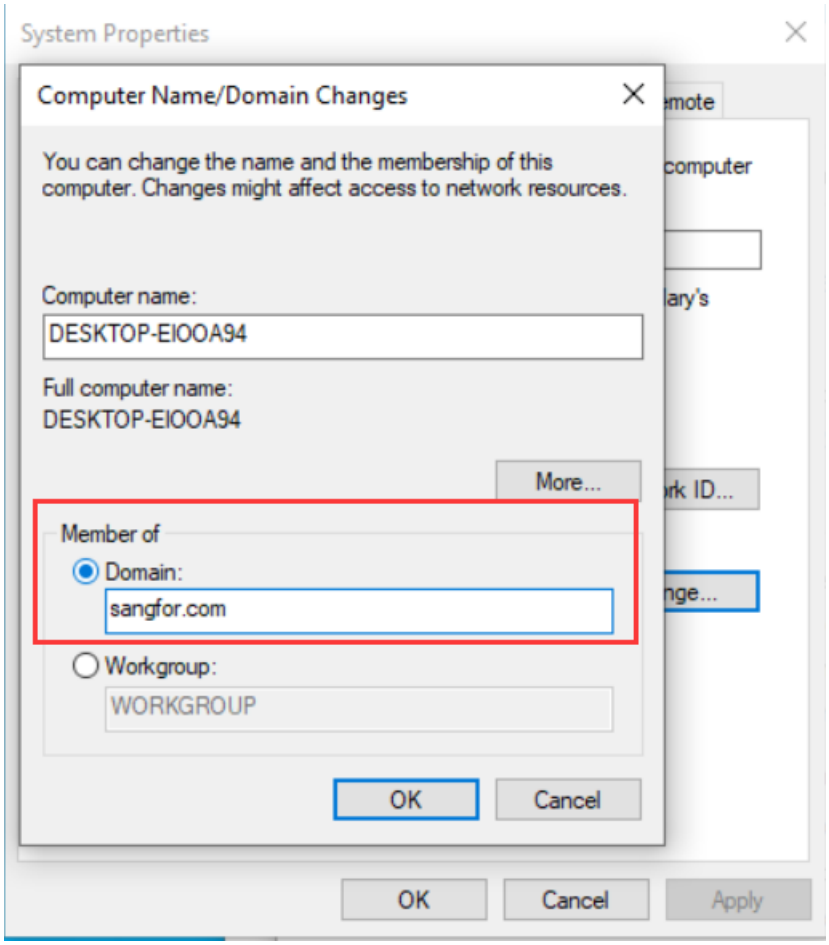


2. Join the PC to the domain.

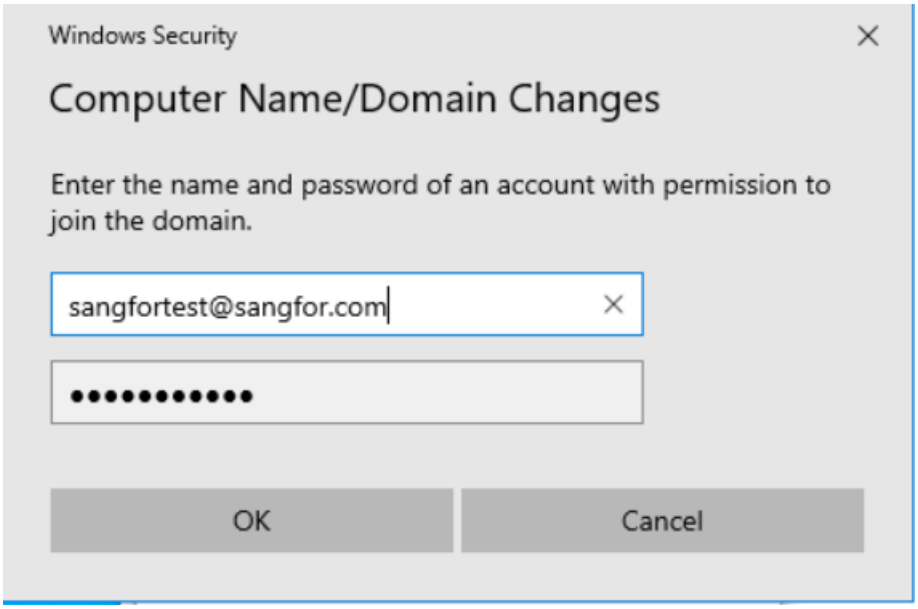

This PC
File
Computer
View
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (2)
CD Drive (D:)
59.4 GB
Expand
Manage
Pin to Start
Map network drive...
Open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

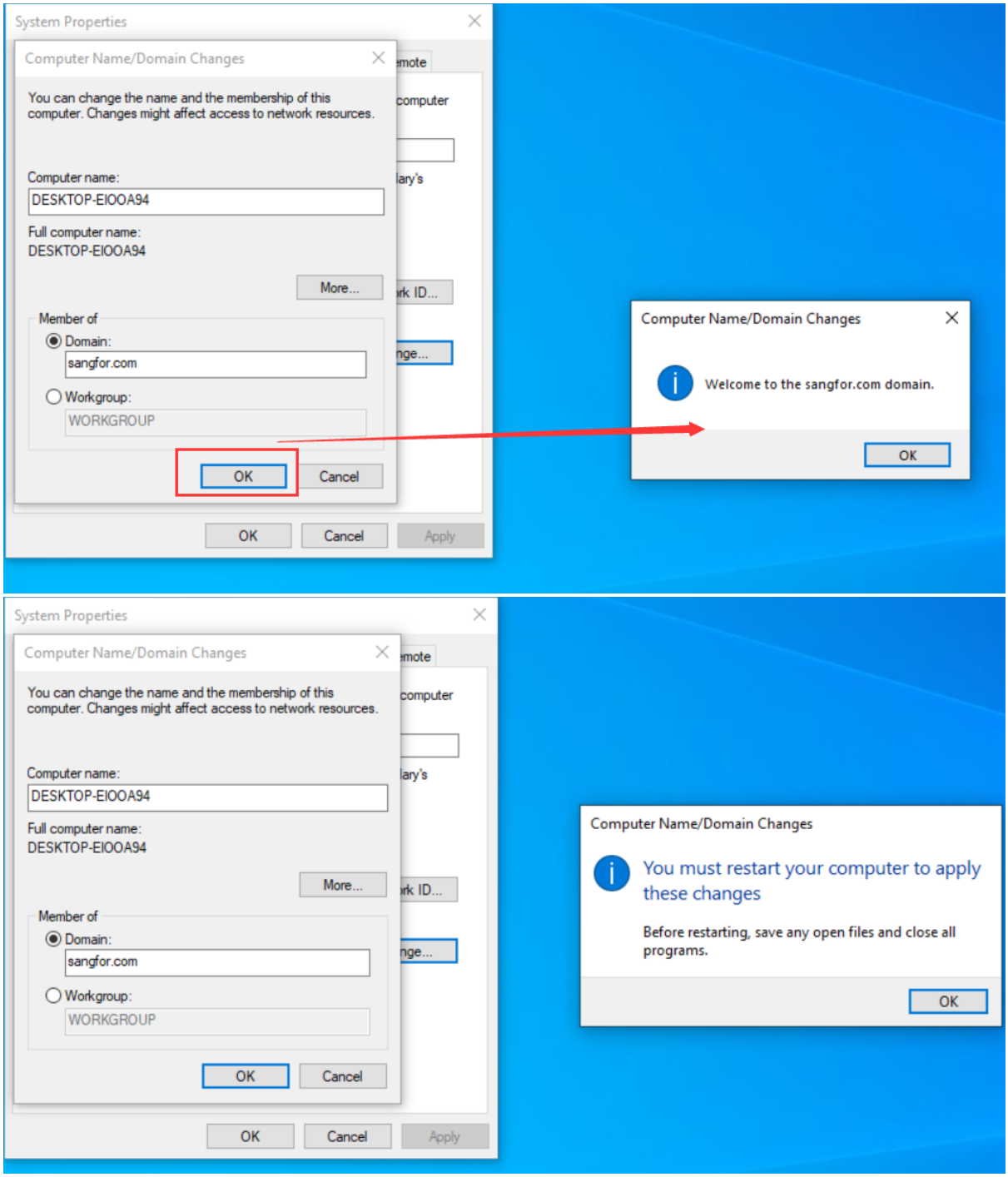

System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "Kitchen Computer" or "Mary's Computer".
Full computer name:
DESKTOP-EIOOA94
Workgroup:
WORKGROUP
To use a wizard 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

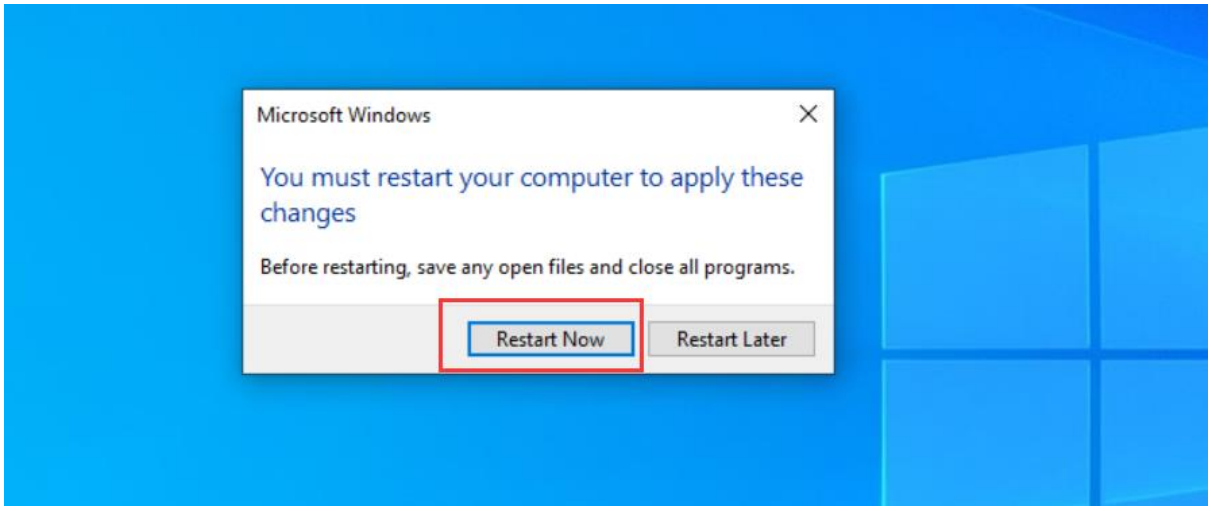


3. In the process of joining the domain, you need to verify your identity, just use the sangfortest user created on the AD domain control 192.168.1.4 for testing.

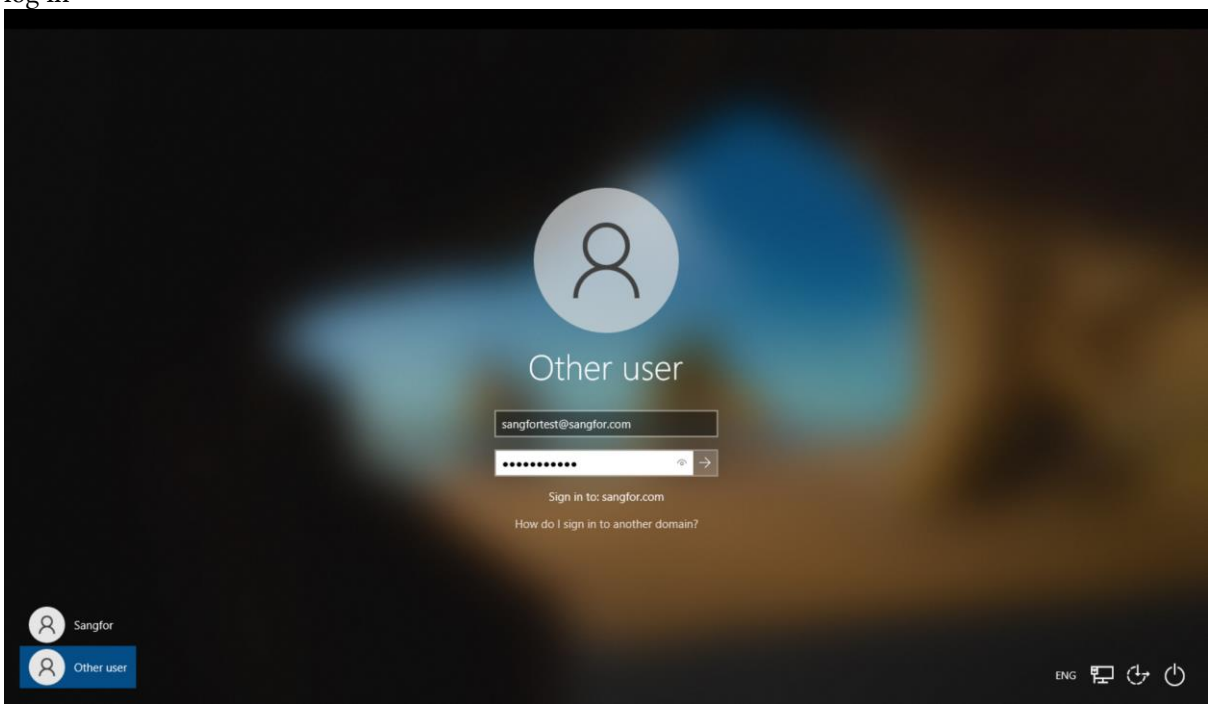


4. After successfully joining the domain, you need to restart the PC.


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
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
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



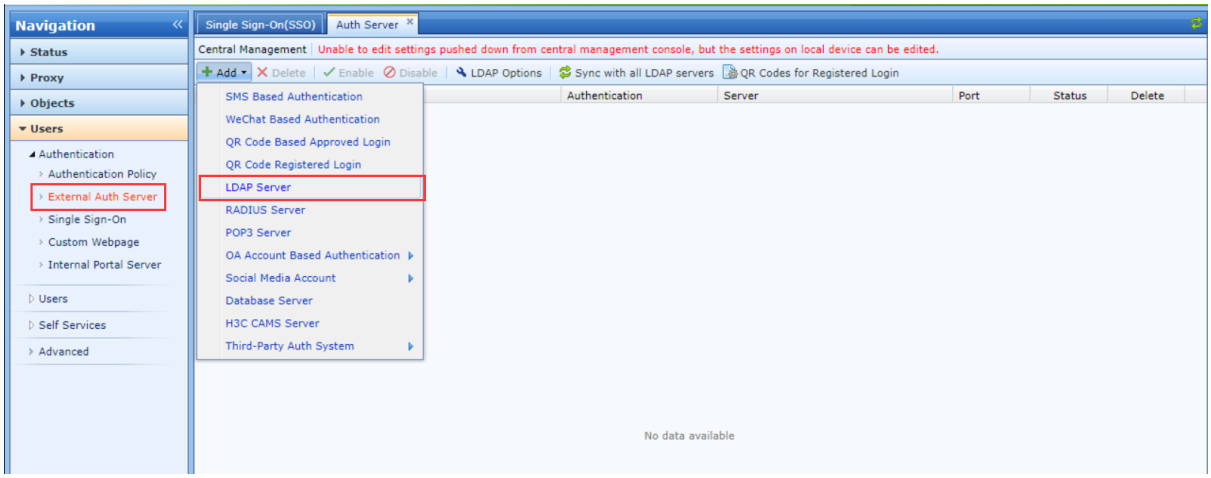
5. After restarting, you can see the login page of the PC, choose to use the domain account sangfortest to log in



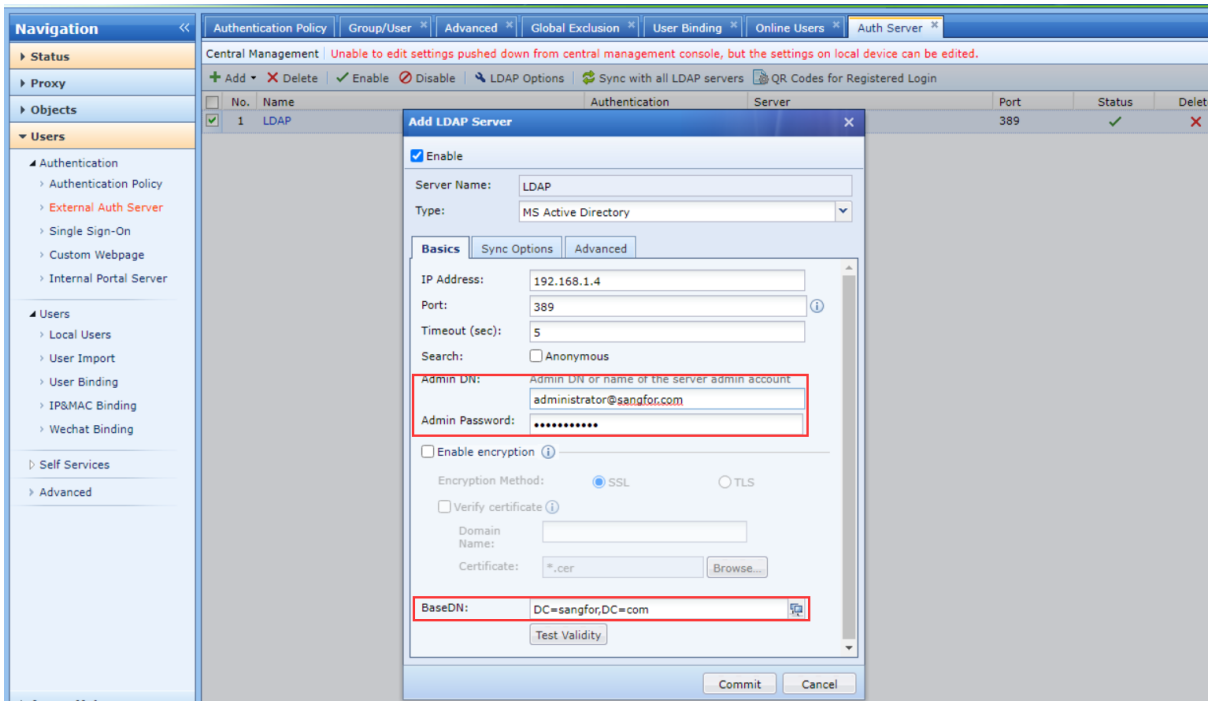
Chapter 3 How to Configure IAM

3.1 Add LDAP server

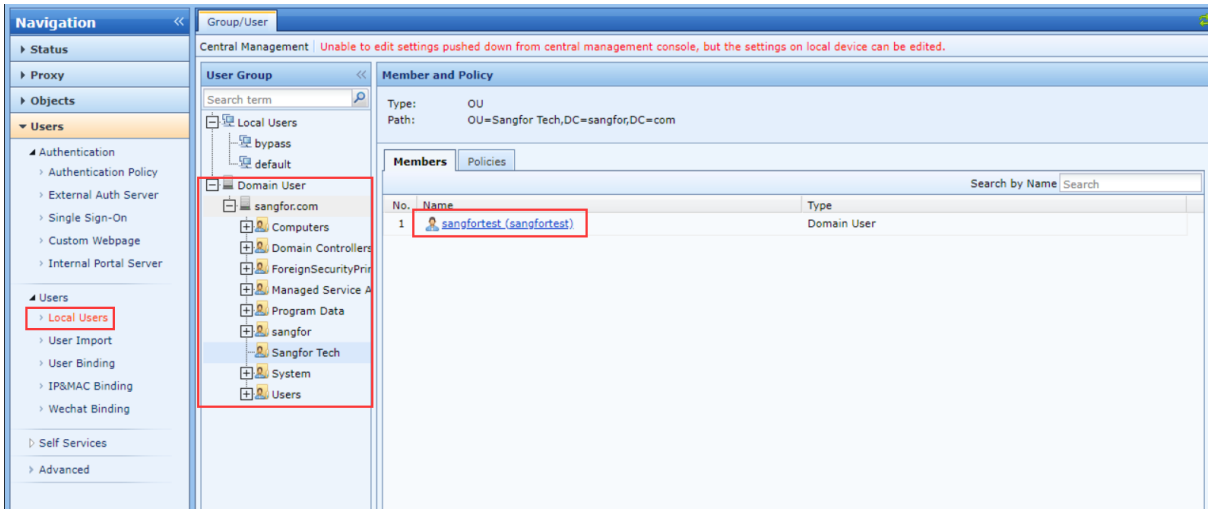
1. Add Microsoft AD server on IAM.



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.

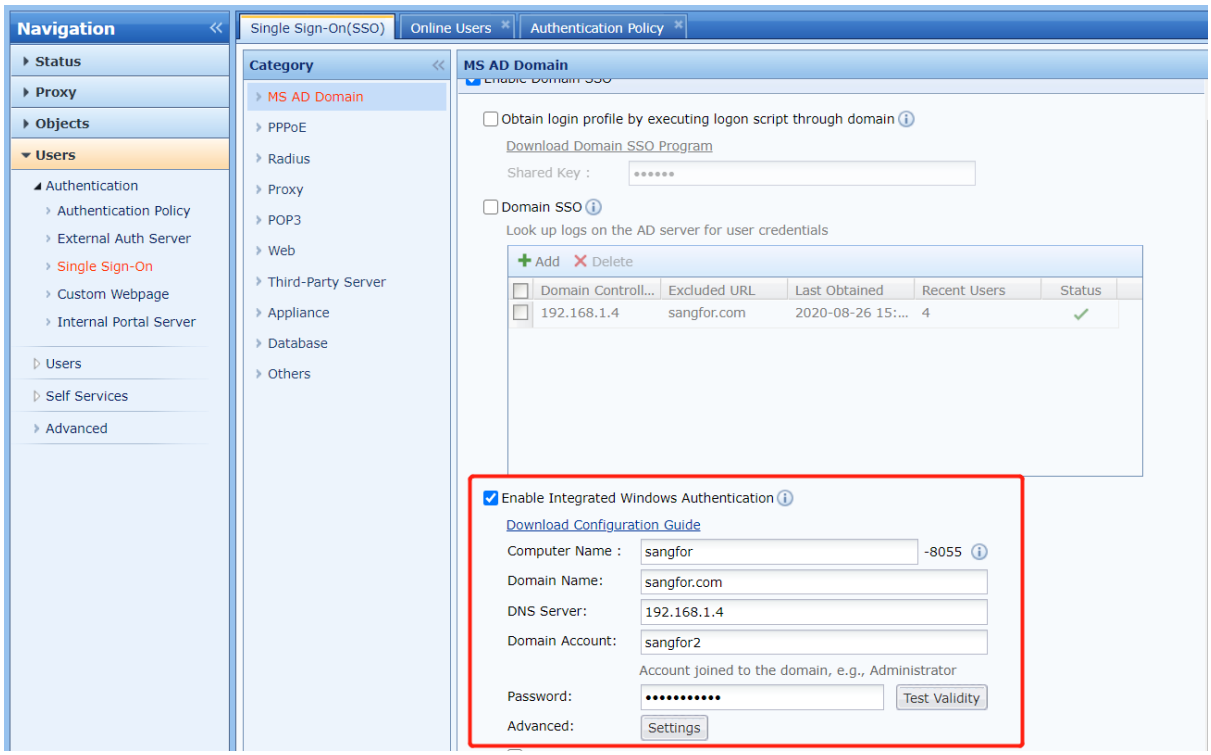


3. If IAM and AD can interact normally, then in the local user, you can see that IAM has obtained the domain user information of the AD server, including the sangfortest user we created before.

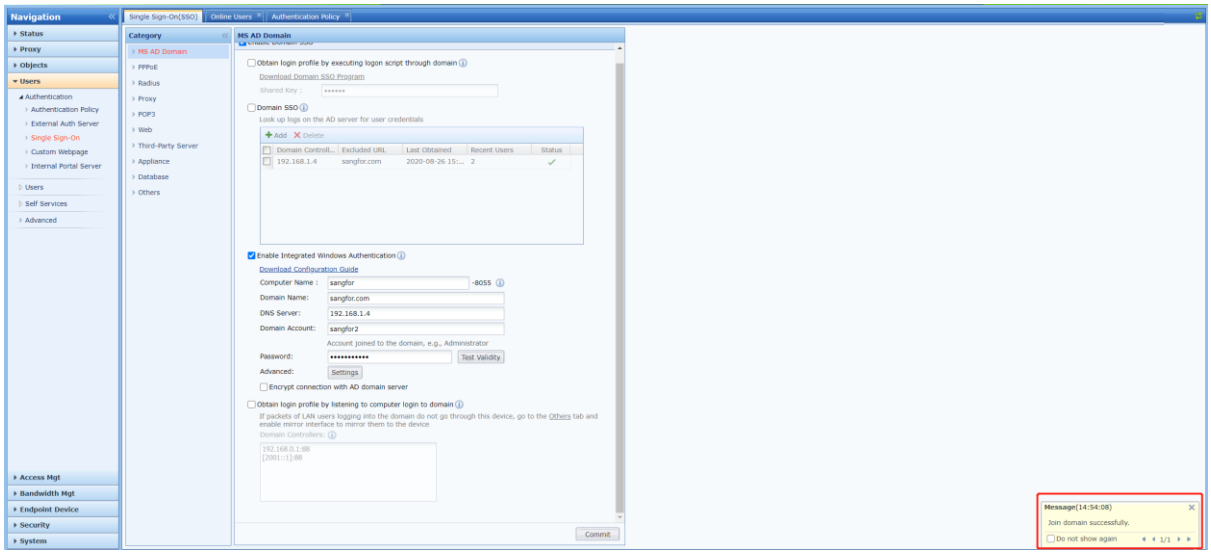


3.2 Configure Integrated Windows Authentication SSO

1. Turn on "Domain SSO" and turn on IWA. Here you need to configure Integrated Windows Authentication.

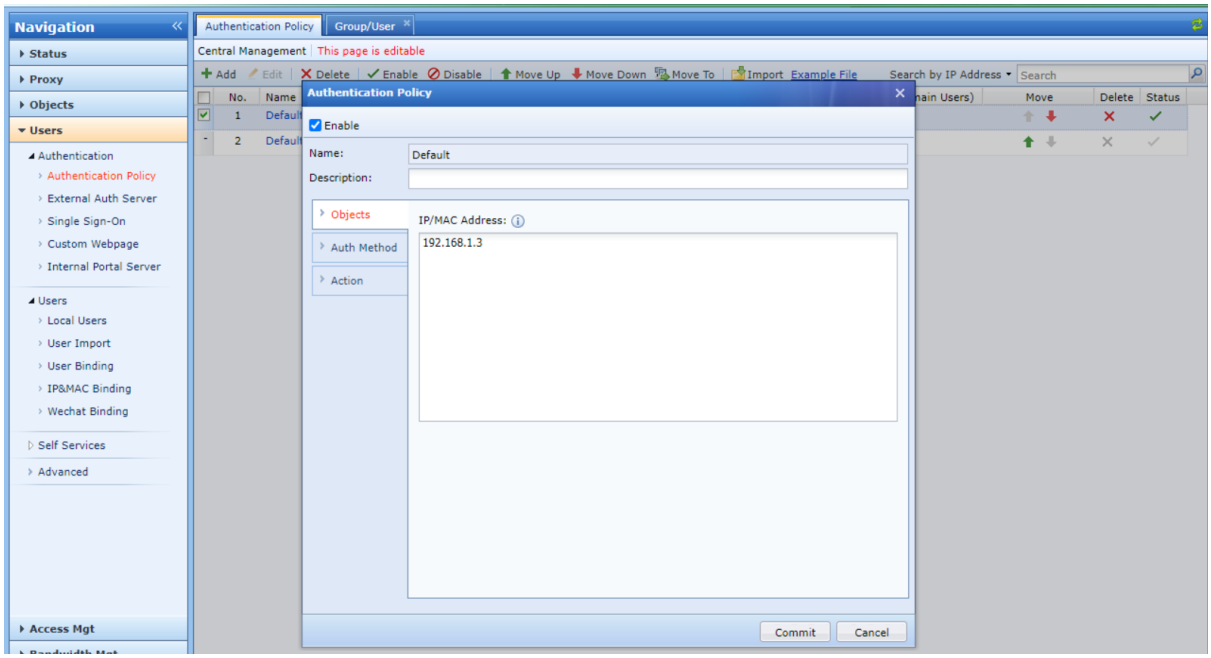


If you can see the prompt " Join domain successfully. " in the lower right corner, which means the IAM has been joined to Windows Server successfully.

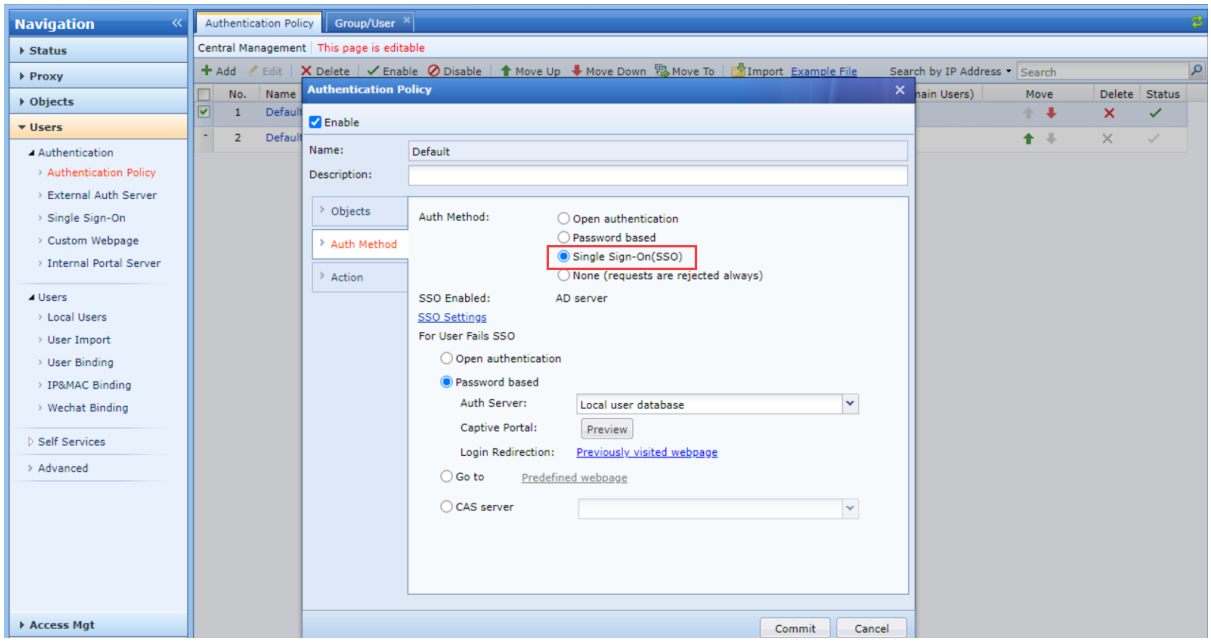


3.3 Configure authentication policy on IAM

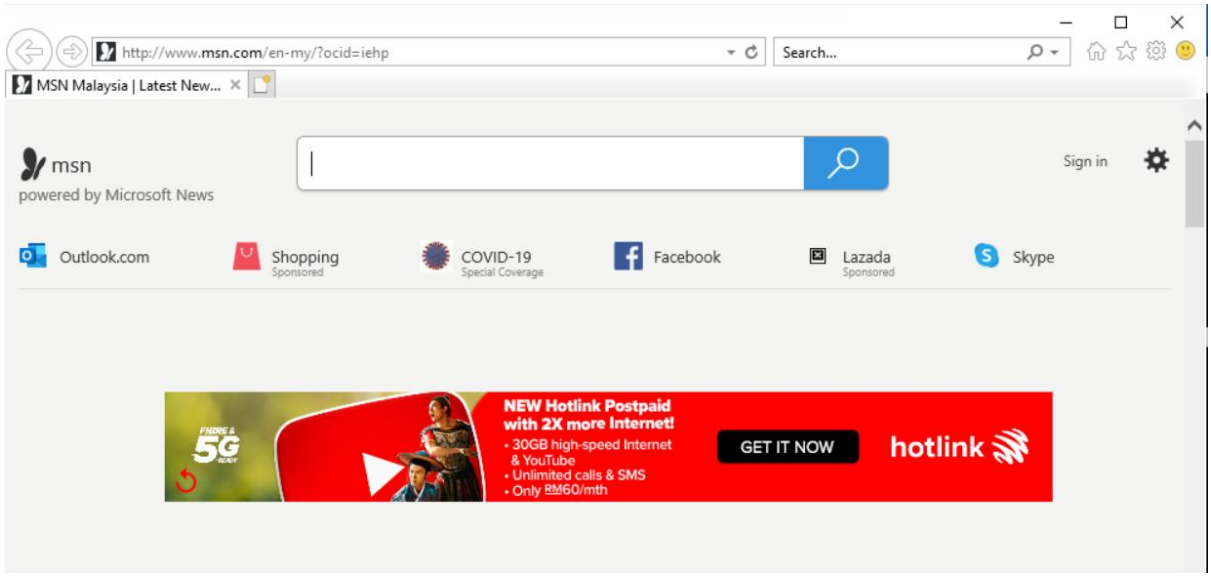
1. Set the scope of the authentication policy, that is, which IP should match the authentication policy.

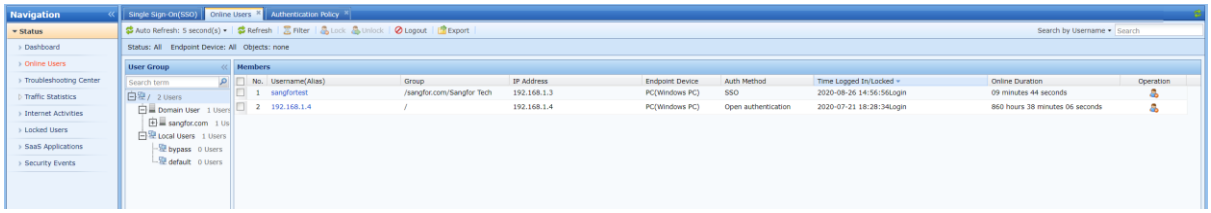


2. Select the authentication method as "SSO".



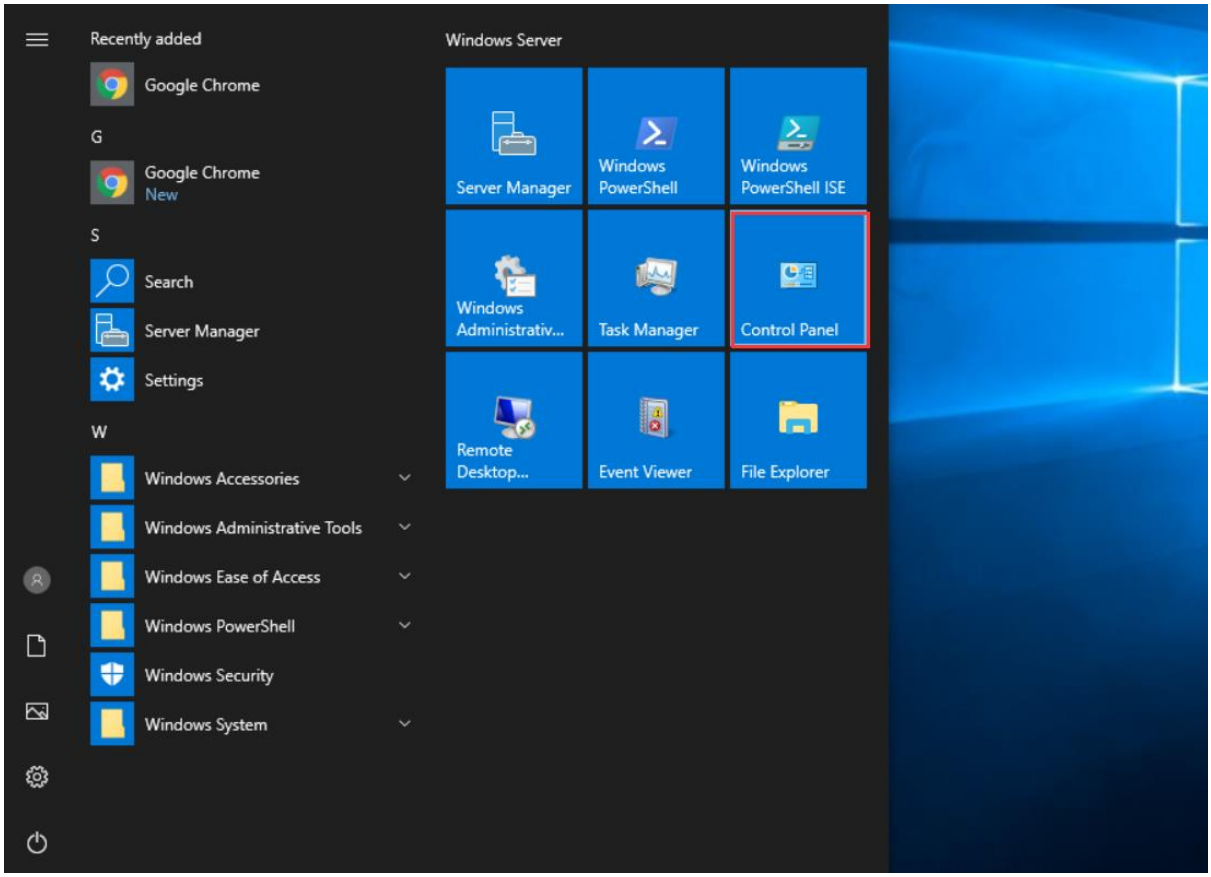
3. Restart the test PC192.168.1.3 and log in to the PC with a domain account. After you enter desktop, you must open Internet Explore and access http website, then you can see that PC192.168.1.3 is online and the authentication method is SSO on the IAM.

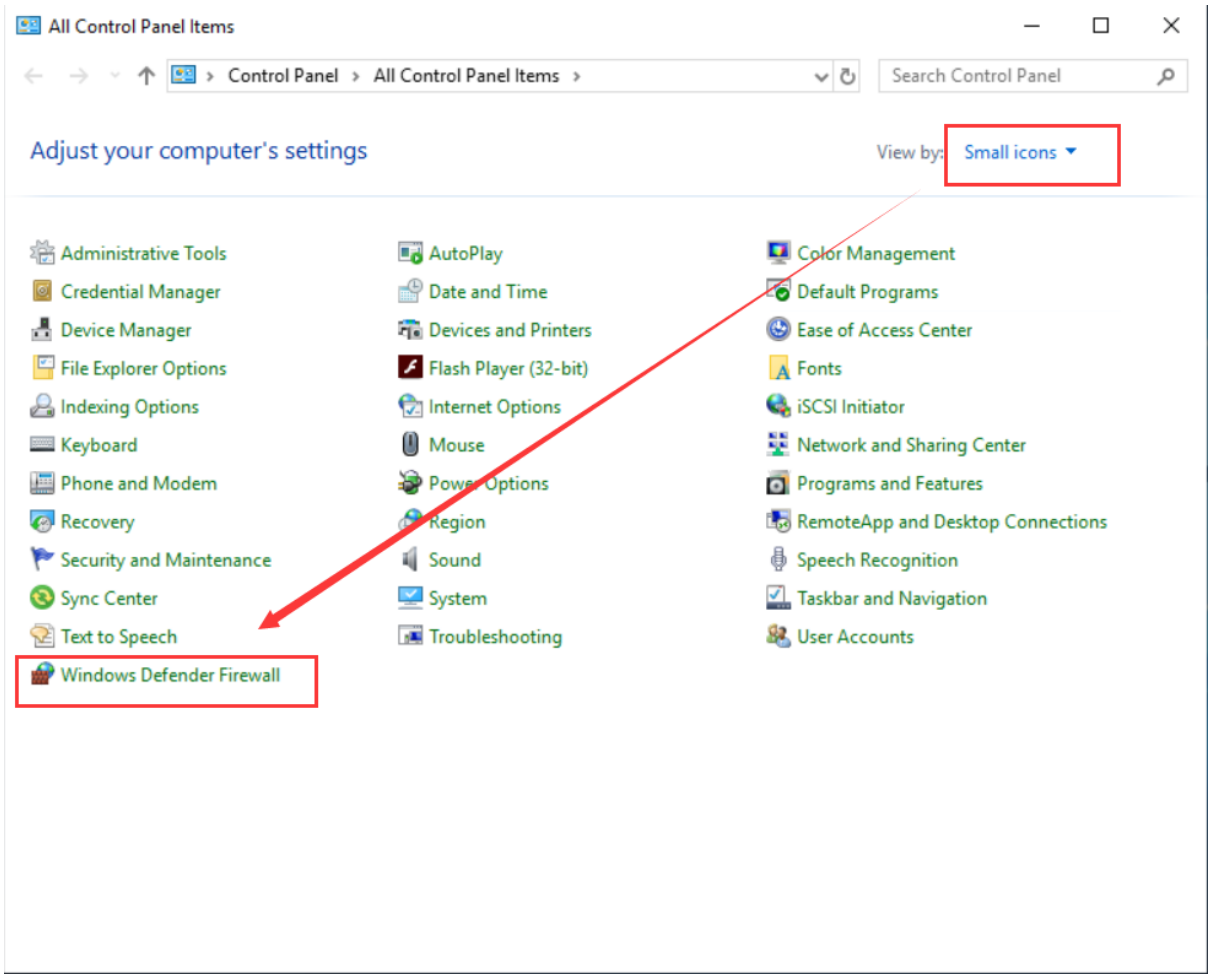


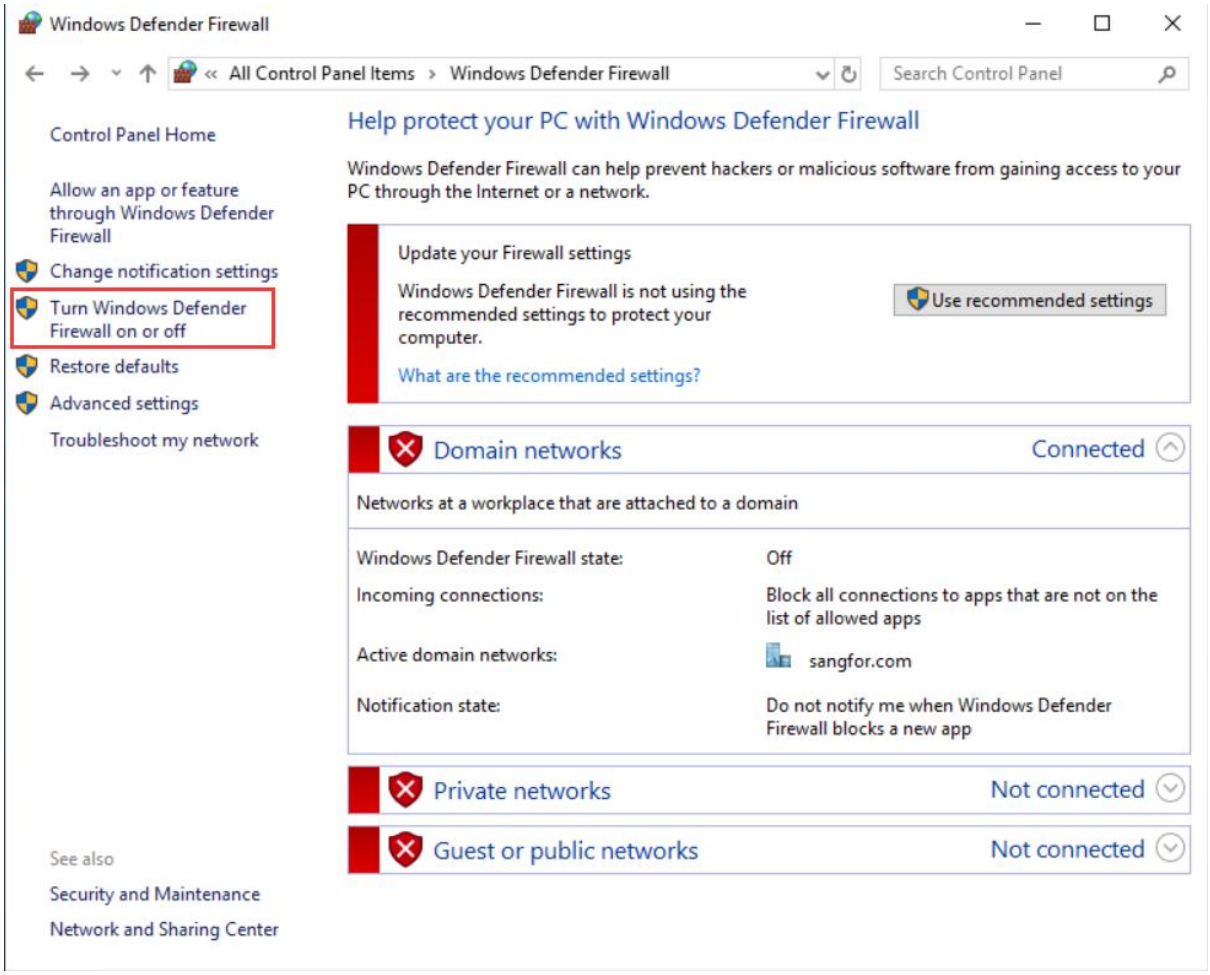


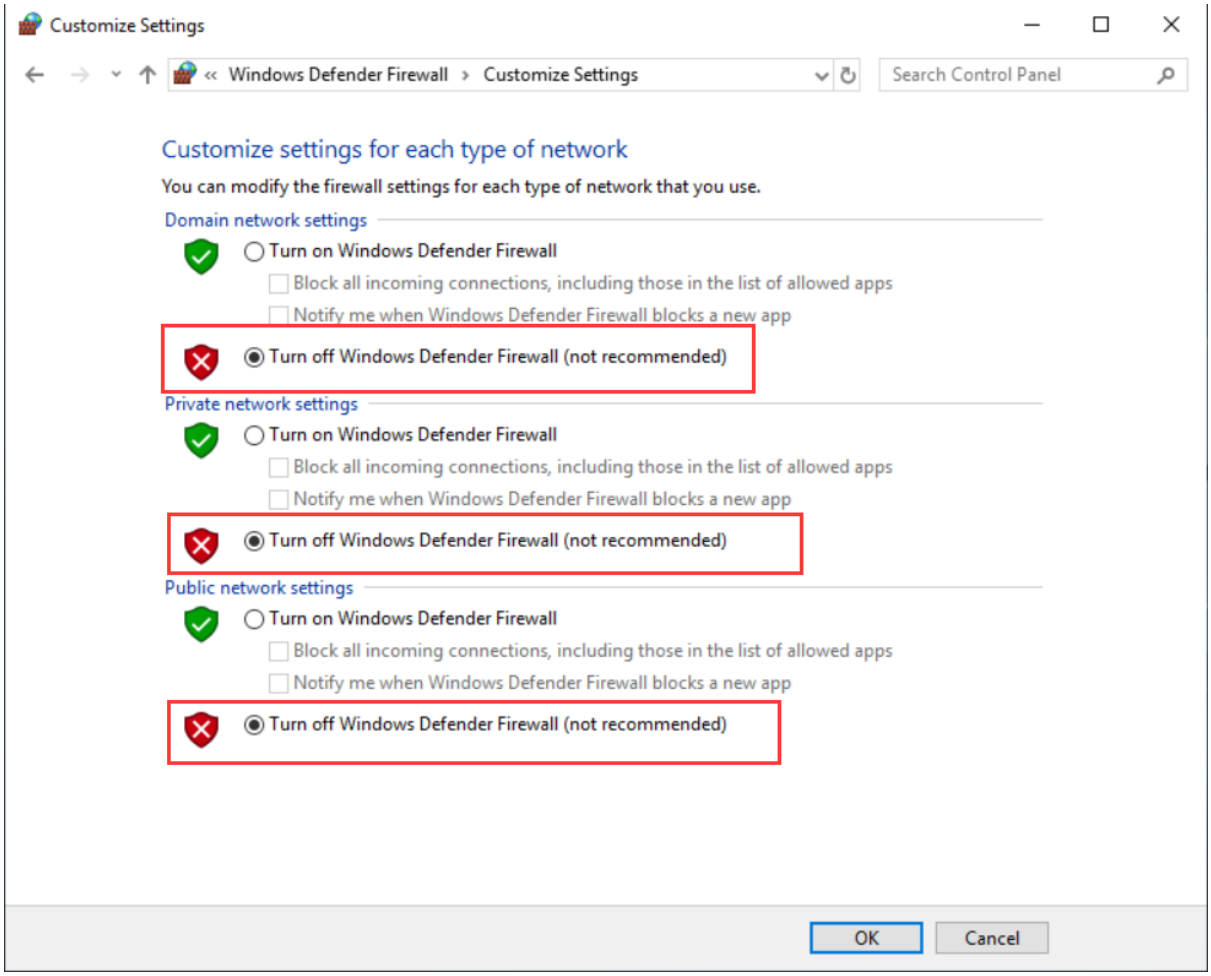
Chapter 4 Precautions

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 unable to obtain relevant data from AD Server.

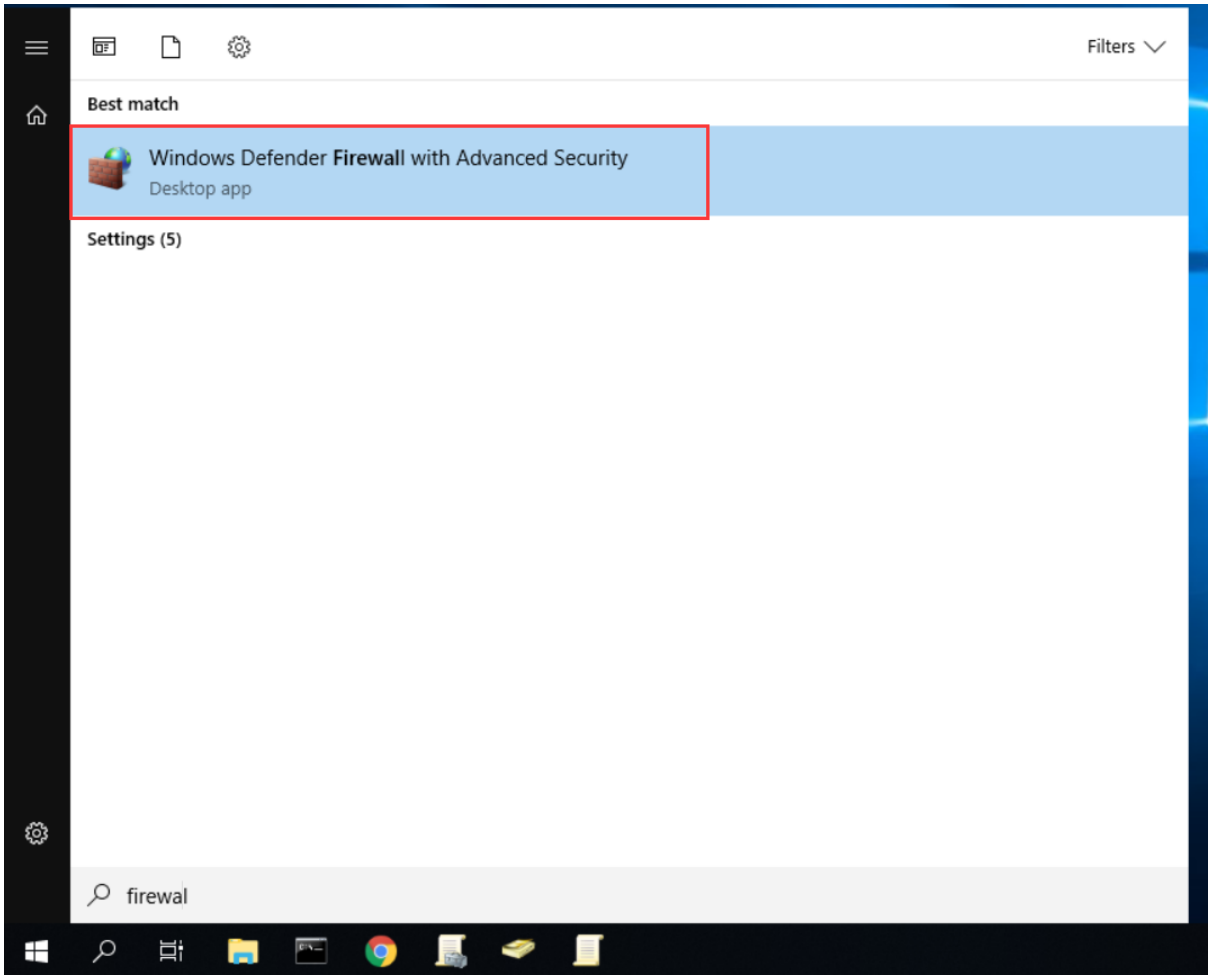

Recently added
Google Chrome
G
Google Chrome
New
S
Search
Server Manager
Settings
W
Windows Accessories
Windows Administrative Tools
Windows Ease of Access
Windows PowerShell
Windows Security
Windows System
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

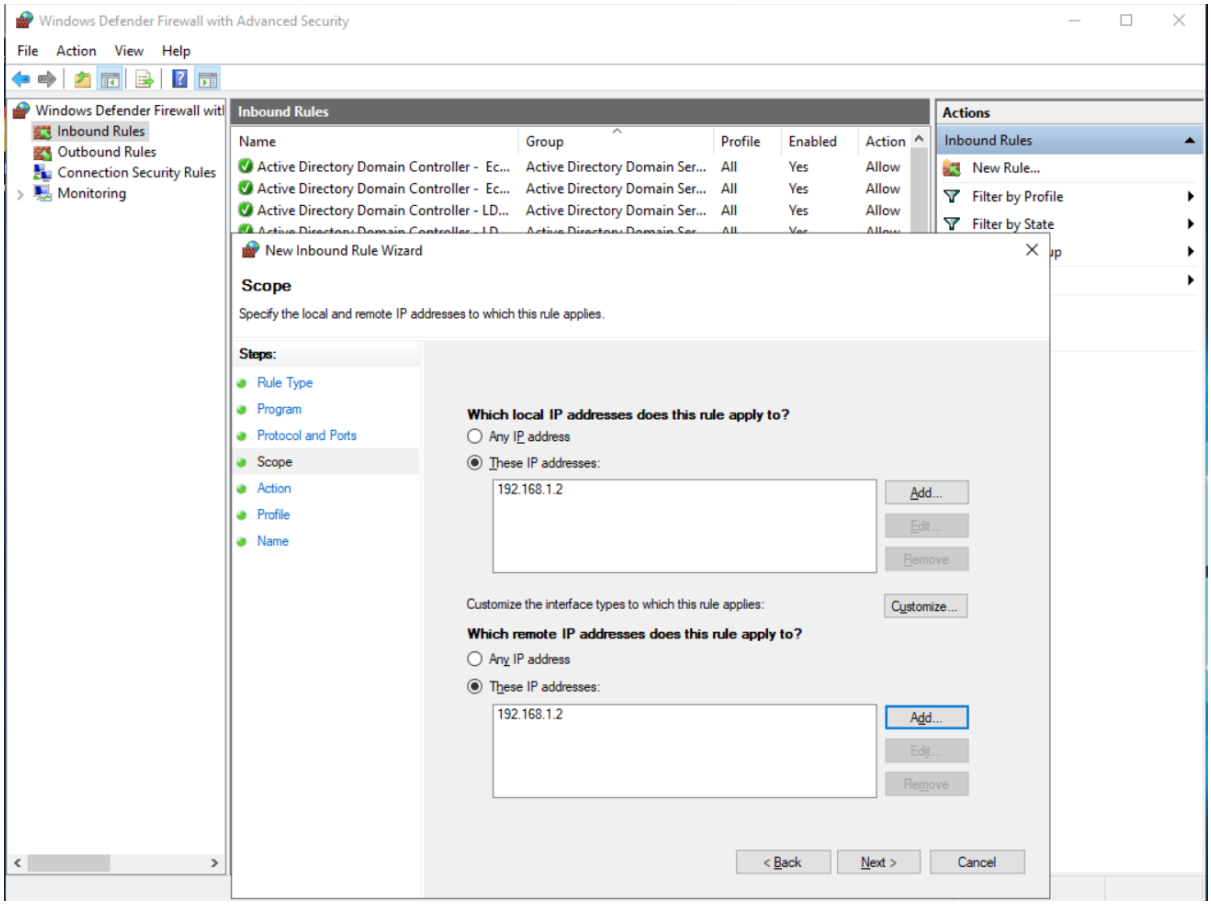

All Control Panel Items
Control Panel › All Control Panel Items ›
Search Control Panel
Adjust your computer's settings
View by: Small icons
Administrative Tools
Credential Manager
Device Manager
File Explorer Options
Indexing Options
Keyboard
Phone and Modem
Recovery
Security and Maintenance
Sync Center
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