Build a Directory Service Server With Active Directory

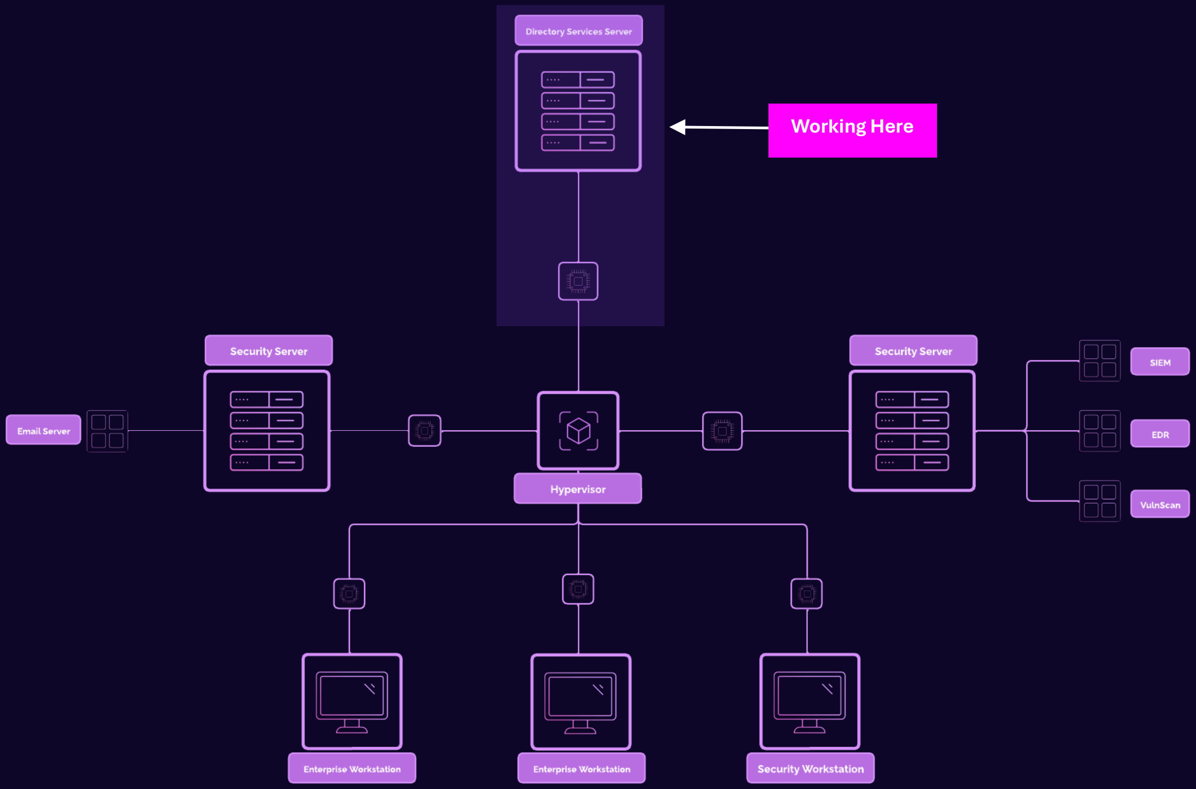
>pr0jectsecurity_

Table of Contents

Prerequisites

1. Virtualbox installed.
2. Virtual Machine with Windows 11 Server 2025 ISO has been configured and provisioned (the ISO should be attached to the new VM).

Network Topology



Active Directory Overview

What is Active Directory?

Active Directory (AD) is a directory service developed by Microsoft that manages and organizes resources in a network. It acts as a centralized database to authenticate and authorize users and devices, making it the backbone of most Windows-based enterprise environments.

Key components:

- **Authentication**: Verifies user identity using credentials like username and password.
- **Authorization**: Grants or denies access to network resources based on permissions.
- **Management**: Centralizes control over users, computers, and other resources.

Why is Active Directory Used?

Active Directory is widely used in enterprise environments to streamline and secure network management. It serves multiple purposes:

1. **Centralized Resource Management**
   AD enables administrators to manage users, devices, and permissions from a single location, reducing complexity.
2. **Scalability**
   It can handle environments ranging from small businesses to multinational corporations with millions of objects.
3. **Authentication and Authorization**
   AD provides a robust framework for verifying users and granting access to resources using security protocols like Kerberos and LDAP.
4. **Group Policy Management**
   Administrators can enforce security settings, deploy software, and manage updates across the network using Group Policy Objects (GPOs).
5. **Integration with Other Services**
   Active Directory integrates seamlessly with services like Microsoft Exchange, Azure AD, and other enterprise applications.

Active Directory Core Concepts

Active Directory Core Concepts

1. **Domains**
   - A domain is a logical grouping of objects (users, devices, etc.) that share the same database and security policies.
   - Example: `corp.local` could be a domain for an organization. `corp.project-x-dc.com` will be the domain used in this project.
2. **Domain Controllers (DCs)**

    - Servers that host the Active Directory database and perform authentication, authorization, and replication.

3. **Organizational Units (OUs)**
    - Containers within a domain used to organize objects logically.
    - Example: Separate OUs for HR, IT, and Finance.
4. **Objects**
    - Every entity in AD, such as users, computers, printers, and groups, is an object.
5. **Groups**
    - **Security Groups**: Used for managing permissions to resources.
    - **Distribution Groups**: Used for email distribution.
6. **Forest and Trees**
    - A forest is the highest-level container, encompassing multiple domains that share a common schema.
    - A tree is a hierarchy of domains within a forest.
7. **Global Catalog (GC)**
    - A distributed data repository that provides information about all objects in the forest for faster lookups.
8. **Trust Relationships**
    - Trusts enable users in one domain to access resources in another domain.

Security Implications

Active Directory is often a prime target for attackers due to its central role in managing network resources. Misconfigurations or vulnerabilities can lead to significant security risks.

1. **Common Security Threats**
    - **Credential Theft**: Techniques like *Pass-the-Hash* or *Kerberoasting* can allow attackers to escalate privileges.

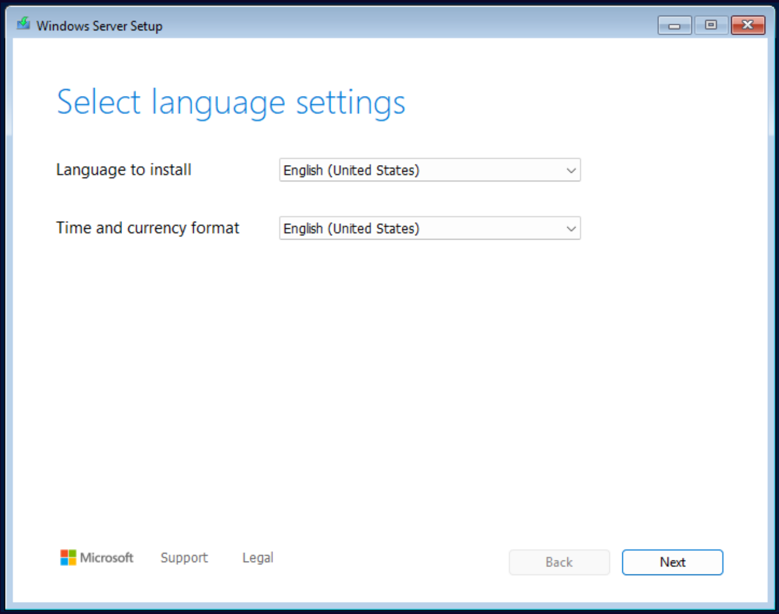
  - **Privilege Escalation**: Exploiting misconfigured permissions to gain higher access levels.
  - **Lateral Movement**: Once inside, attackers can move through the network using AD to identify valuable targets.

Many organizations are transitioning to hybrid environments using **Microsoft Entra ID** (formerly **Azure Active Directory)**, which combines on-premises and cloud-based identity management. We will be using on-premises infrastructure so we can fully control the setup, configuration, and isolation of the lab. (In addition to keep this free and avoid cloud costs!)

Setup Windows Server 2025

Step 1

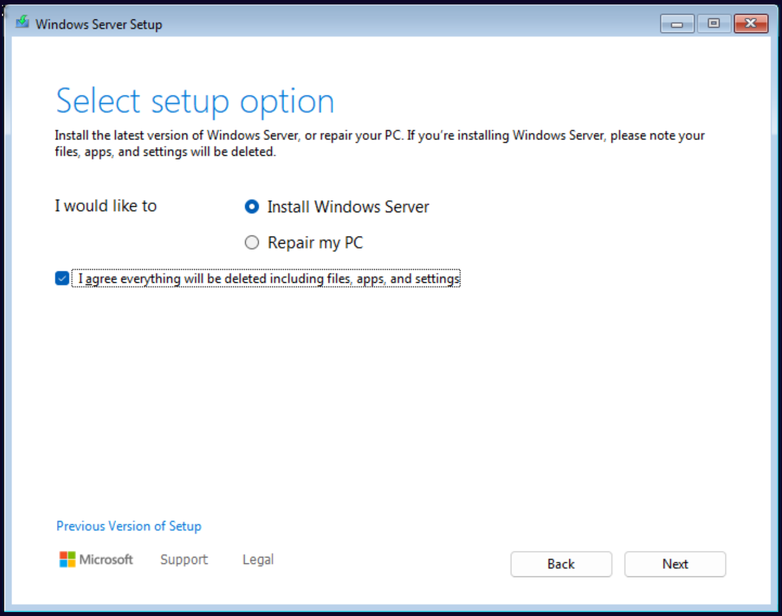
Select "Next" → "Install Windows 11" → Check the box → "Next".


Windows Server Setup

Select language settings

Language to install: English (United States)

Time and currency format: English (United States)



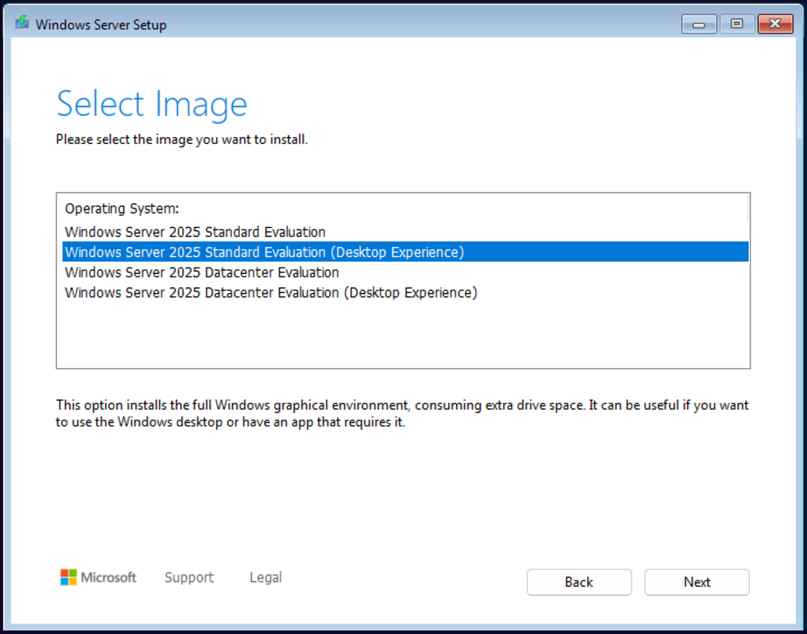
Select setup option

Install the latest version of Windows Server, or repair your PC. If you're installing Windows Server, please note your files, apps, and settings will be deleted.

I would like to ● Install Windows Server ○ Repair my PC

☑ I agree everything will be deleted including files, apps, and settings

Select “Desktop Experience”.



Select Image

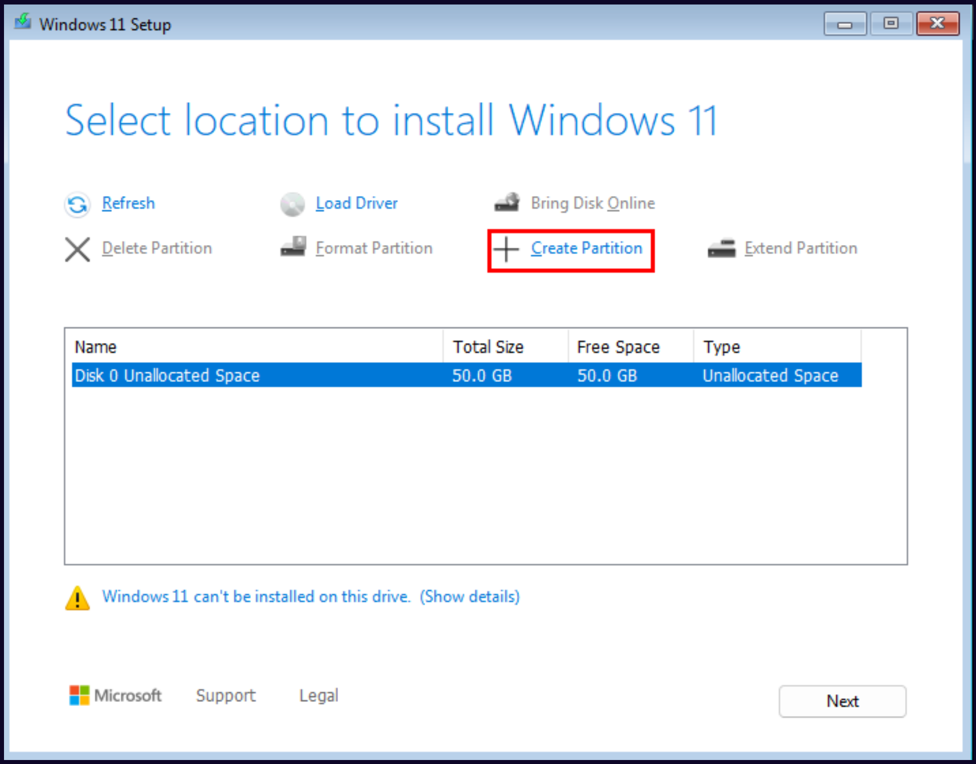
Please select the image you want to install.

Operating System:
Windows Server 2025 Standard Evaluation
Windows Server 2025 Standard Evaluation (Desktop Experience)
Windows Server 2025 Datacenter Evaluation
Windows Server 2025 Datacenter Evaluation (Desktop Experience)

This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.

Accept Microsoft’s End User License Agreement (EULA) → “Next”.

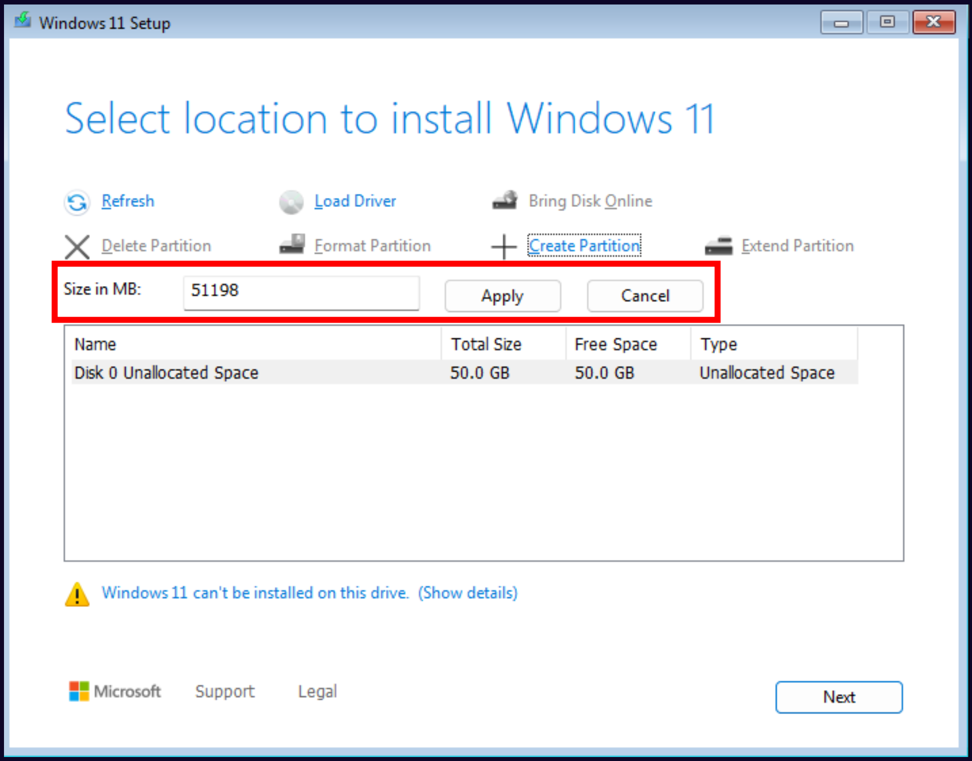
Select “Disk 0 Unallocated Space” → “Create Partition”. Use the default “Size in MB” setting → “Apply. Wait for three partitions to show up.



Select location to install Windows 11

Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	50.0 GB	50.0 GB	Unallocated Space

⚠ Windows 11 can't be installed on this drive. (Show details)



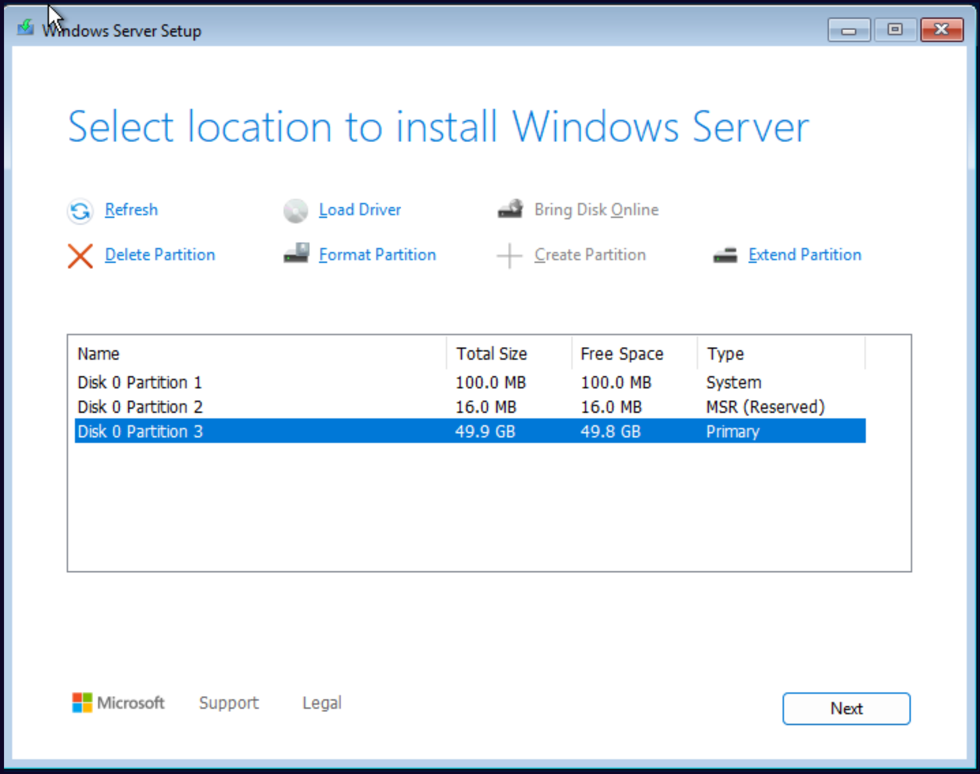
Select location to install Windows 11

Size in MB: 51198

Name	Total Size	Free Space	Type
Disk 0 Unallocated Space	50.0 GB	50.0 GB	Unallocated Space

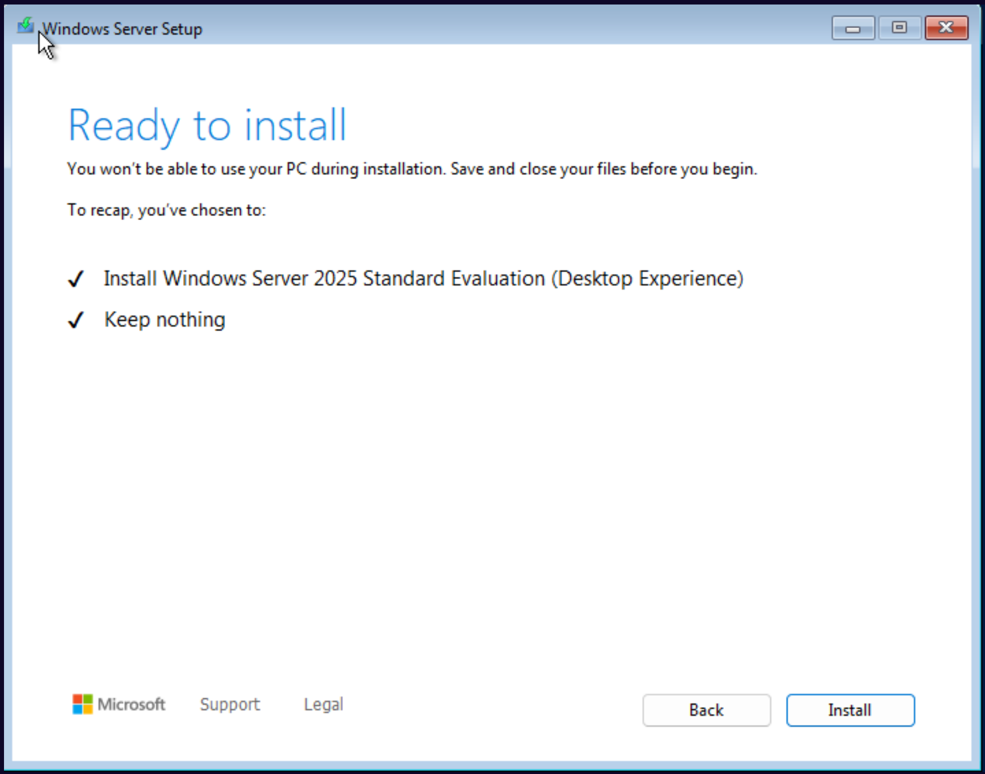
⚠ Windows 11 can't be installed on this drive. (Show details)

Select Disk 0 Partition 3 (with the largest free space). Select “Install”. Wait for Windows Server 2025 to fully install. The VM should restart.



Select location to install Windows Server

Name	Total Size	Free Space	Type
Disk 0 Partition 1	100.0 MB	100.0 MB	System
Disk 0 Partition 2	16.0 MB	16.0 MB	MSR (Reserved)
Disk 0 Partition 3	49.9 GB	49.8 GB	Primary

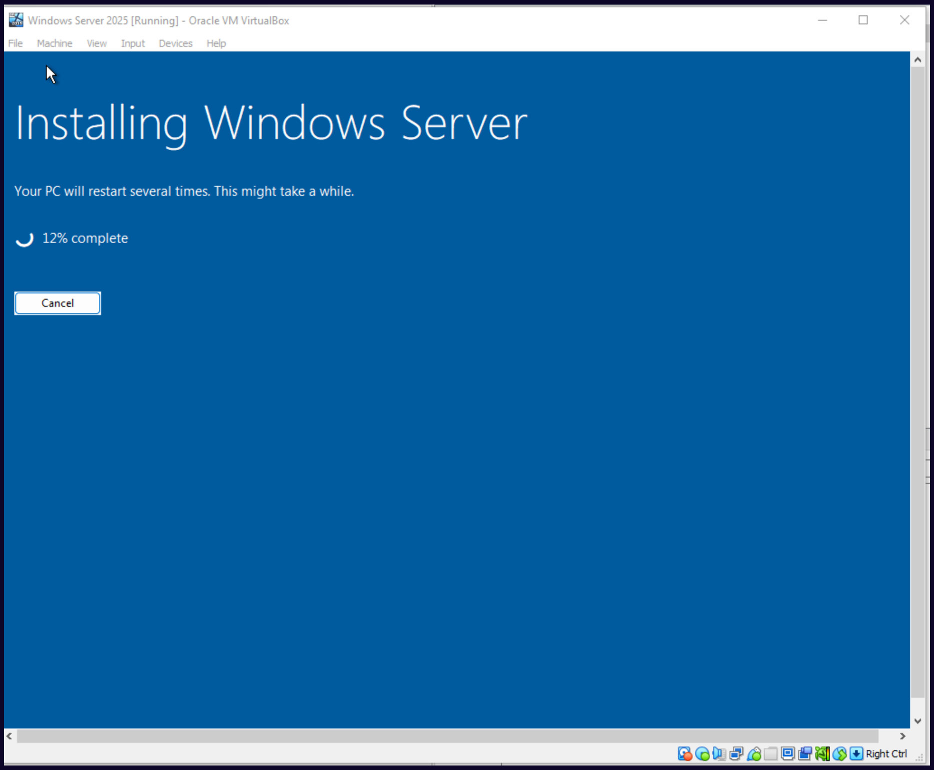


Ready to install

You won't be able to use your PC during installation. Save and close your files before you begin.

To recap, you've chosen to:

- ✓ Install Windows Server 2025 Standard Evaluation (Desktop Experience)
- ✓ Keep nothing



Installing Windows Server

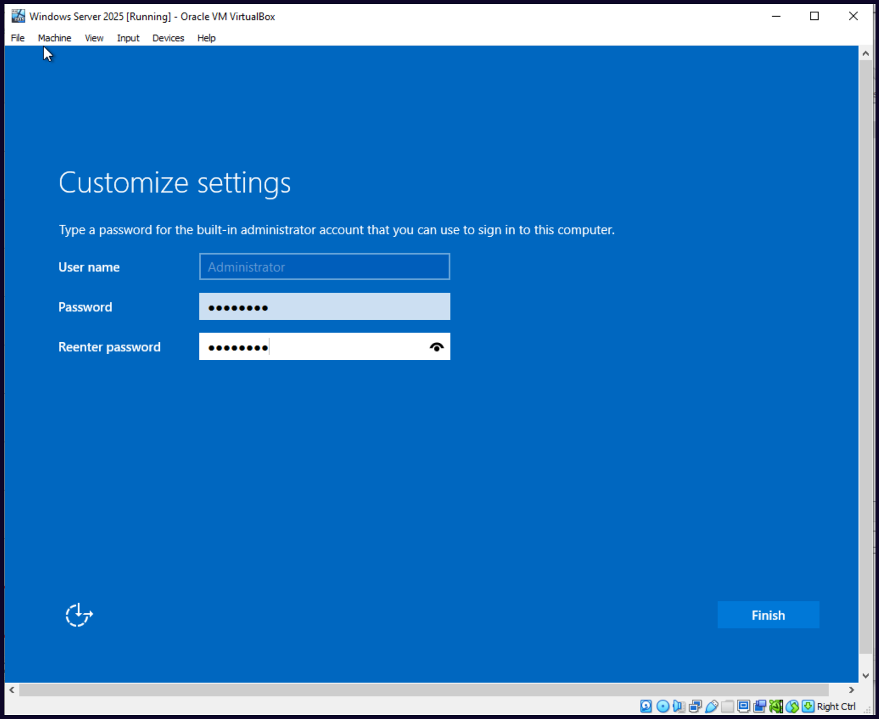
Your PC will restart several times. This might take a while.

12% complete

Step 2

Set a password for the default Administrator account. Password is (@Deeboodah1!)

👉 Refer to the "**Project Overview**" guide for more information on default usernames and passwords.



Customize settings

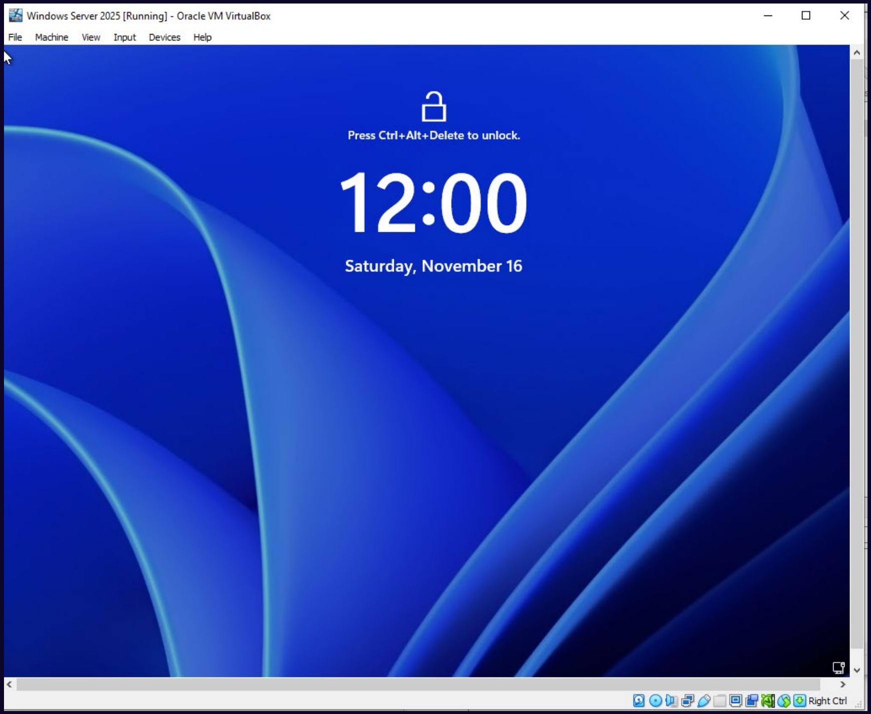
Type a password for the built-in administrator account that you can use to sign in to this computer.

User name: Administrator

Password: ••••••••

Reenter password: ••••••••

The login screen will appear.

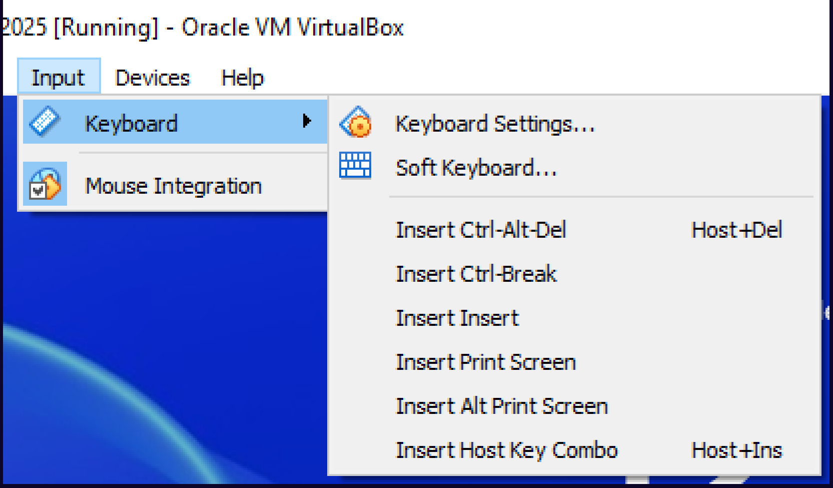


Press Ctrl+Alt+Delete to unlock.

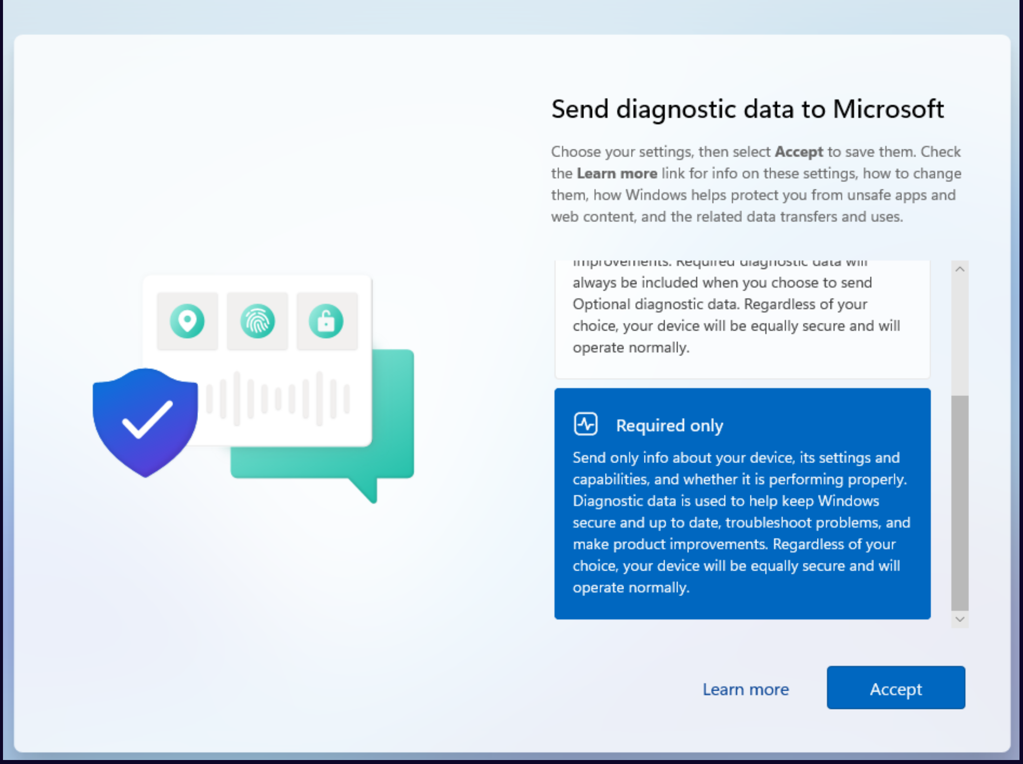
12:00

Saturday, November 16

Navigate to the top of VirtualBox, go to “Input” → “Keyboard” → “Insert Ctrl-Alt-Del” to open the login prompt.



Choose “Required only” for sending diagnostic data to Microsoft.



Send diagnostic data to Microsoft

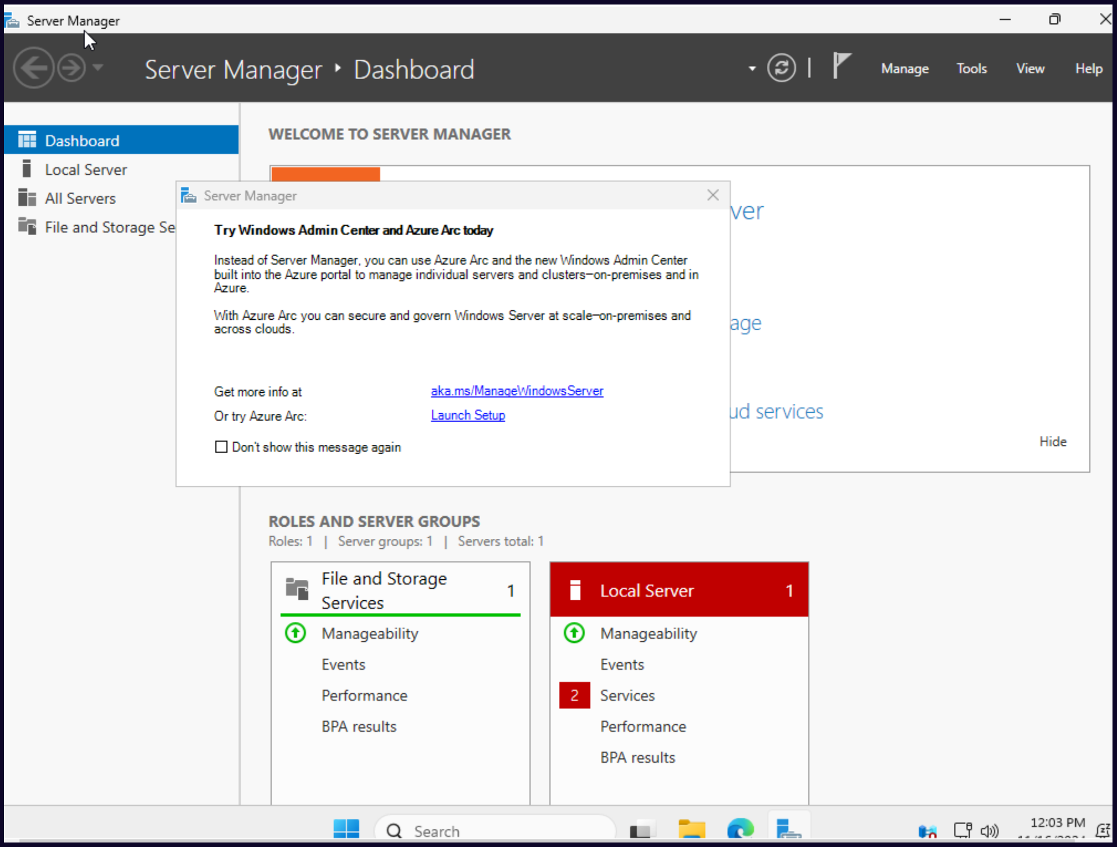
Choose your settings, then select **Accept** to save them. Check the **Learn more** link for info on these settings, how to change them, how Windows helps protect you from unsafe apps and web content, and the related data transfers and uses.

improvements. Required diagnostic data will always be included when you choose to send Optional diagnostic data. Regardless of your choice, your device will be equally secure and will operate normally.

Required only

Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements. Regardless of your choice, your device will be equally secure and will operate normally.

After signing in, you should see “Server Manager” Window. You can exit out of the dialog box to try Azure Arc.



Server Manager

Try Windows Admin Center and Azure Arc today

Instead of Server Manager, you can use Azure Arc and the new Windows Admin Center built into the Azure portal to manage individual servers and clusters—on-premises and in Azure.

With Azure Arc you can secure and govern Windows Server at scale—on-premises and across clouds.

Get more info at aka.ms/ManageWindowsServer

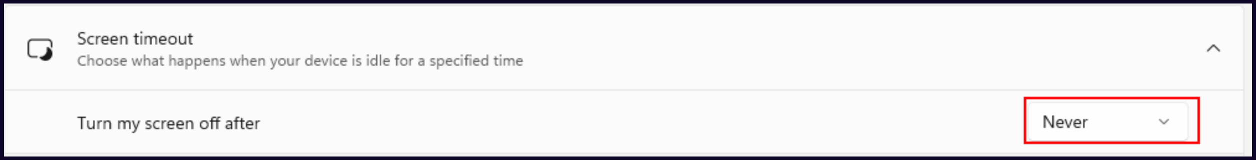
Or try Azure Arc: Launch Setup

□ Don't show this message again

Disable Default Logoff

The default time for signing out of Windows Server 2025 is 5 minutes. Let's change this.

Lookup "Settings" in the Search bar → "System" → "Power" → Select the toggle under "Screen timeout" → Select "Never".



Screen timeout
Choose what happens when your device is idle for a specified time

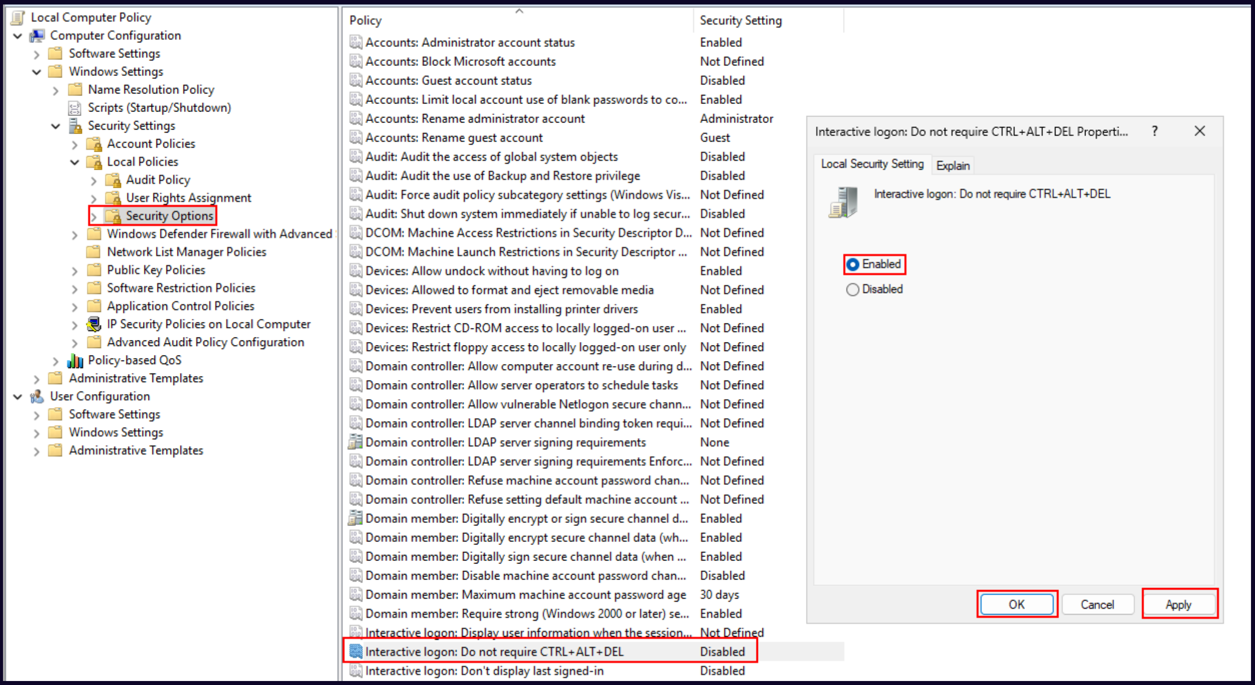
Turn my screen off after: Never

Disable CTRL + ALT + DEL

If you do not want to use the "Input" → "Keyboard" → "Insert CTRL + ALT + DEL" each time, you can disable this setting.

Look up "Local Security Policy".

Navigate to the following folder tree → Look for "Interactive logon..." → Toggle from Disabled to Enabled → "Apply" → "OK".



Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow computer account re-use during d...	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	None
Domain controller: LDAP server signing requirements Enforc...	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain controller: Refuse setting default machine account ...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Don't display last signed-in	Disabled

Interactive logon: Do not require CTRL+ALT+DEL Properti... ? ✕

Local Security Setting | Explain

Interactive logon: Do not require CTRL+ALT+DEL

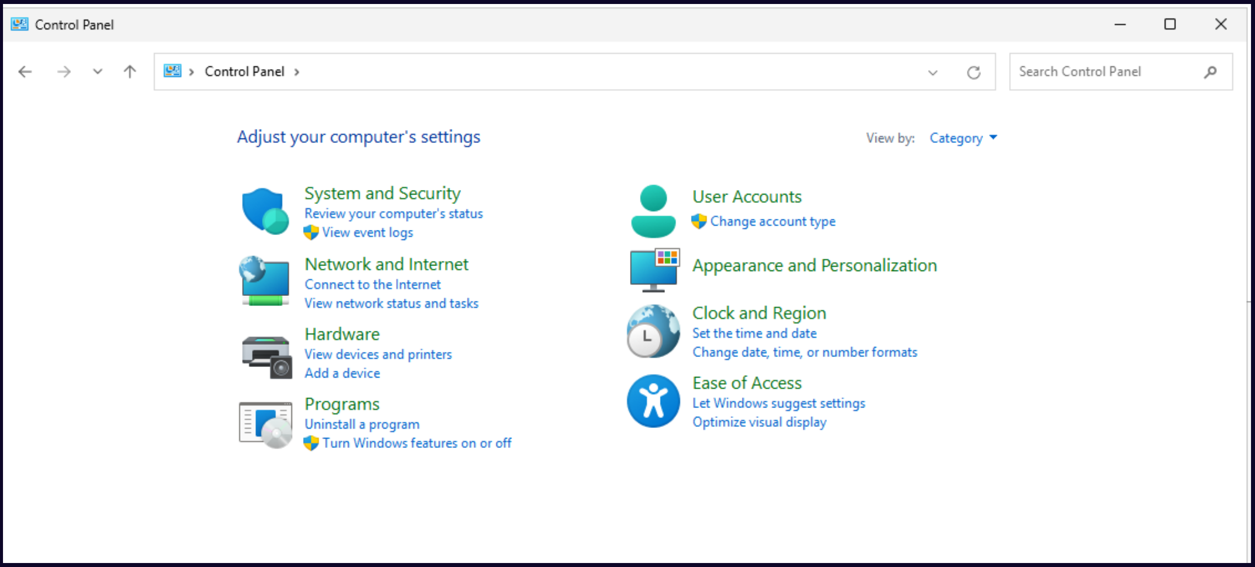
● Enabled
○ Disabled

Assign Static IP Address

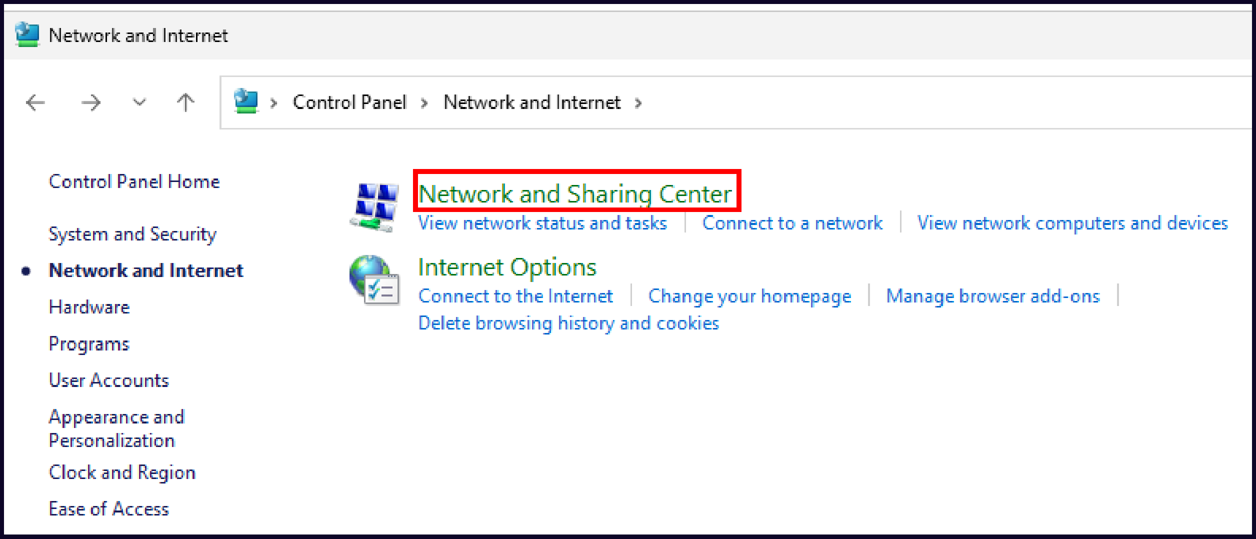
👉 Before You Start: Make sure Windows Server 2025 (`project-x-dc`) is running.

Step 1

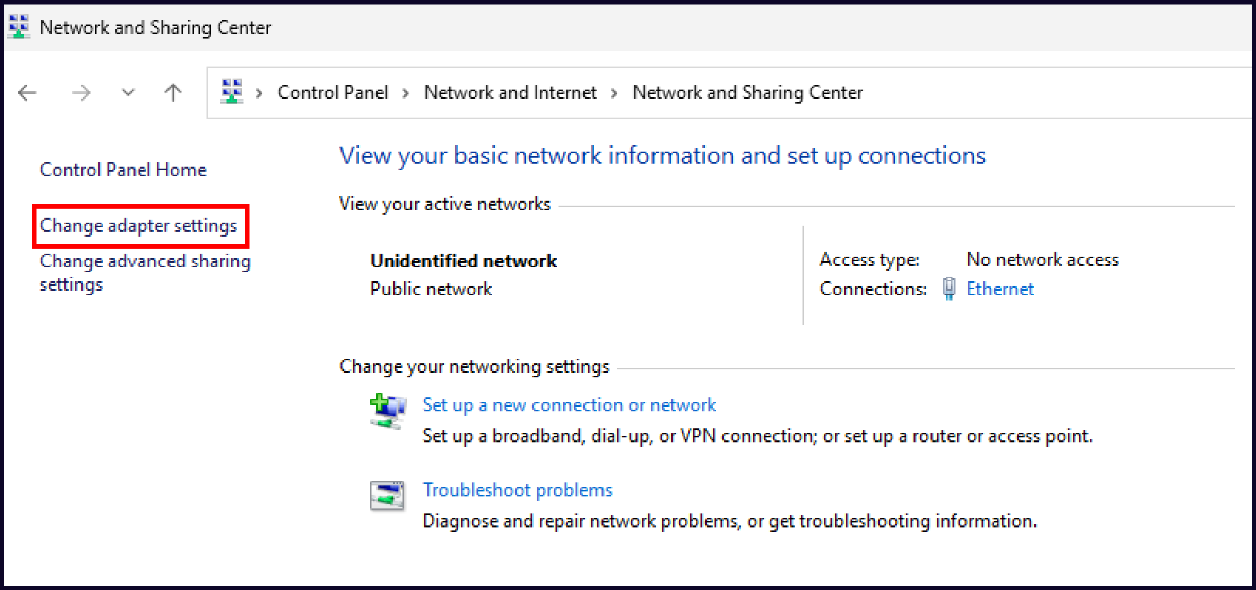
Navigate to the Control Panel (Shortcut: `Windows+X`).



Select “Network and Sharing Center”.


Network and Internet
Control Panel › Network and Internet ›
Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Network and Sharing Center
View network status and tasks | Connect to a network | View network computers and devices
Internet Options
Connect to the Internet | Change your homepage | Manage browser add-ons |
Delete browsing history and cookies

Select “Change adapter settings”.


Network and Sharing Center
Control Panel › Network and Internet › Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
Set up a new connection or network
Troubleshoot problems

View your basic network information and set up connections

View your active networks

Unidentified network
Public network

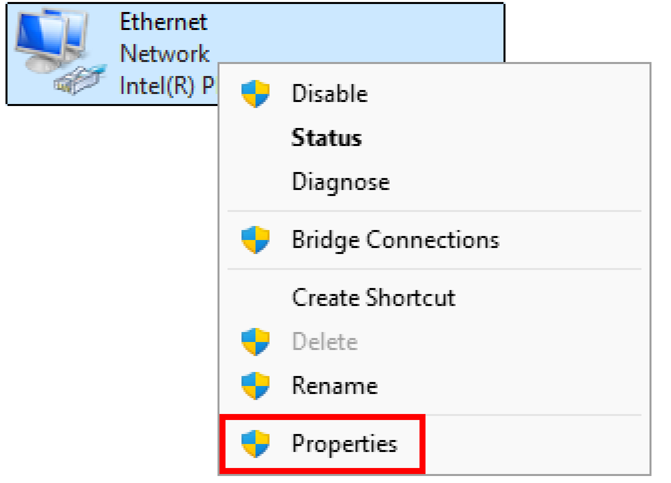
Access type: No network access
Connections: Ethernet

Change your networking settings

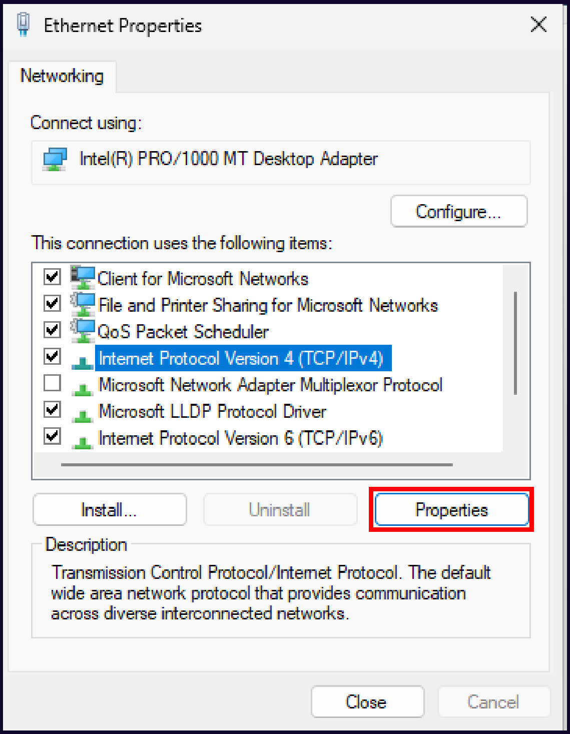
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Diagnose and repair network problems, or get troubleshooting information.

A window will pop-up with a computer icon named “Ethernet”. Right-click this icon → “Properties”.



Another box will open (yay for all the boxes we must click through 🙃). Select "Internet Protocol Version 4 (TCP/IPv4) → "Properties".



Ethernet Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

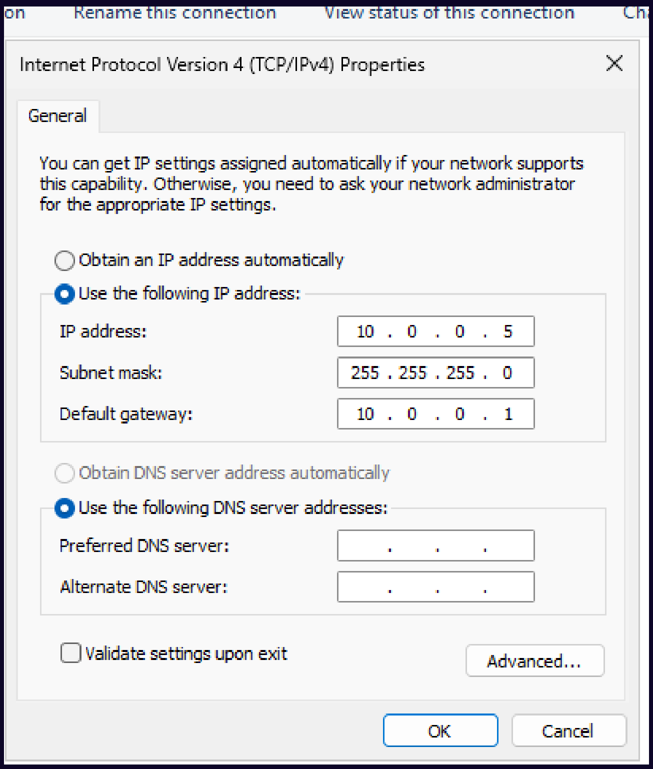
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Set this device to a static IP address. Select "OK" after finishing.

- IP address: 10.0.0.05
- Subnet mask: 255.255.255.0
- Default gateway: 10.0.0.1

👉 Refer to the "**Project Overview**" guide for more information on hostname addressing.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	10 . 0 . 0 . 5
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 0 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

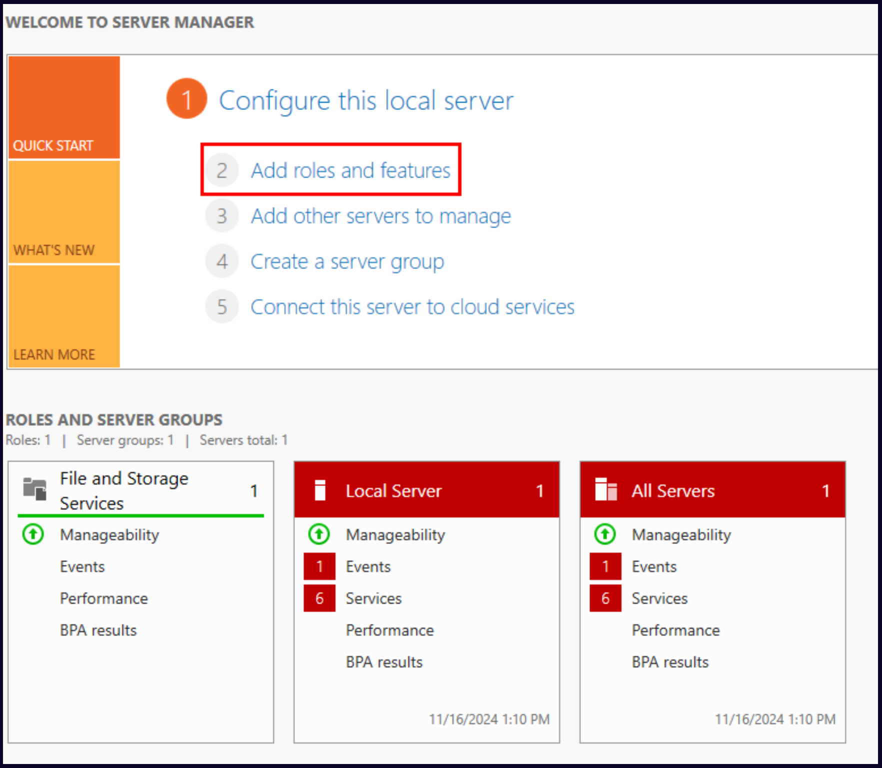
Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

Promote Active Directory to a Domain Controller

Step 1

Go back to “Server Manager” → “Add roles and features”.



WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

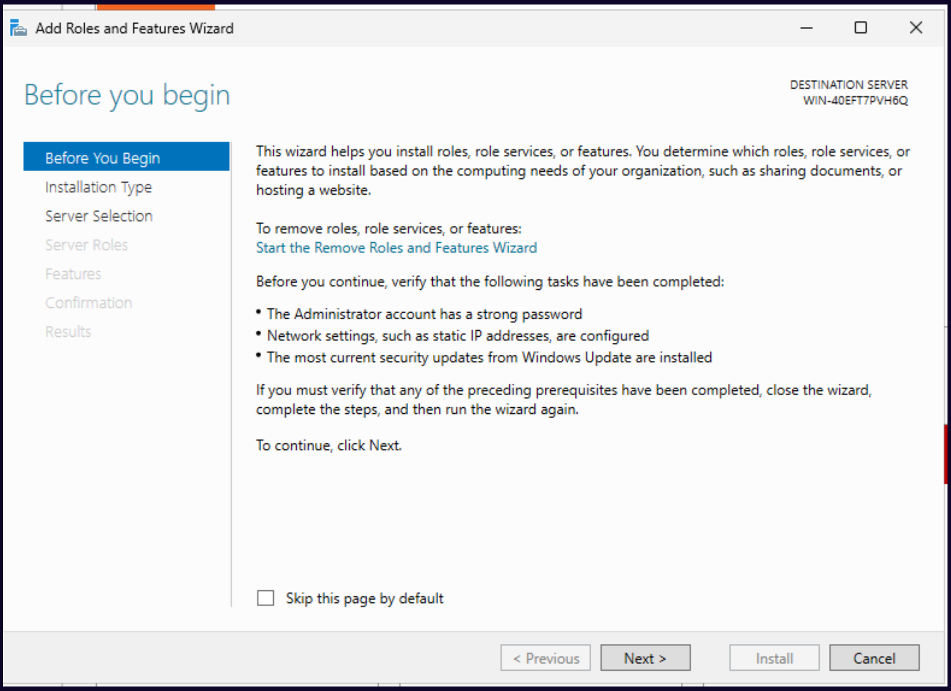
5 Connect this server to cloud services

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

File and Storage Services 1	Local Server 1	All Servers 1
Manageability	Manageability	Manageability
Events	1 Events	1 Events
Performance	6 Services	6 Services
BPA results	Performance	Performance
	BPA results	BPA results
	11/16/2024 1:10 PM	11/16/2024 1:10 PM

Select "Next" for the next 3 boxes.



Add Roles and Features Wizard

Before you begin

DESTINATION SERVER
WIN-40EFT7PVH6Q

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

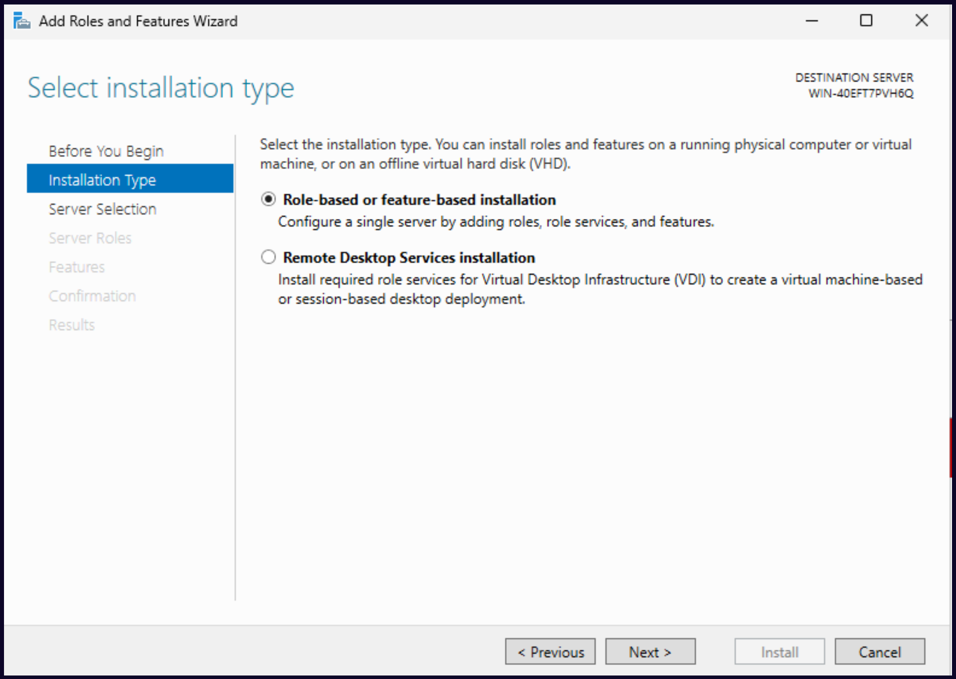
Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default



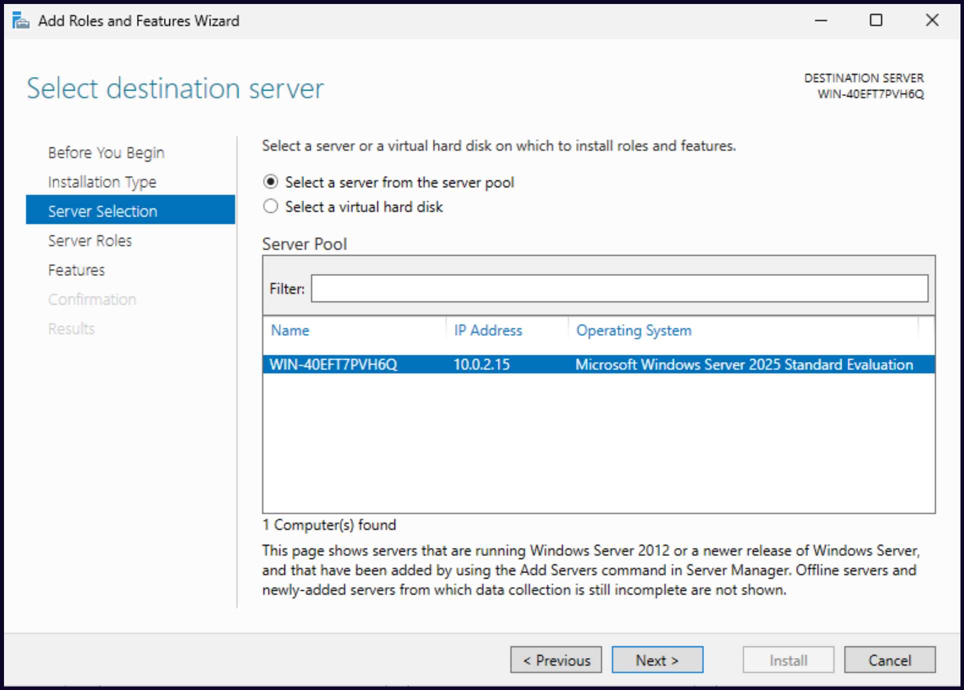
Select installation type

DESTINATION SERVER
WIN-40EFT7PVH6Q

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.



Select destination server

DESTINATION SERVER
WIN-40EFT7PVH6Q

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

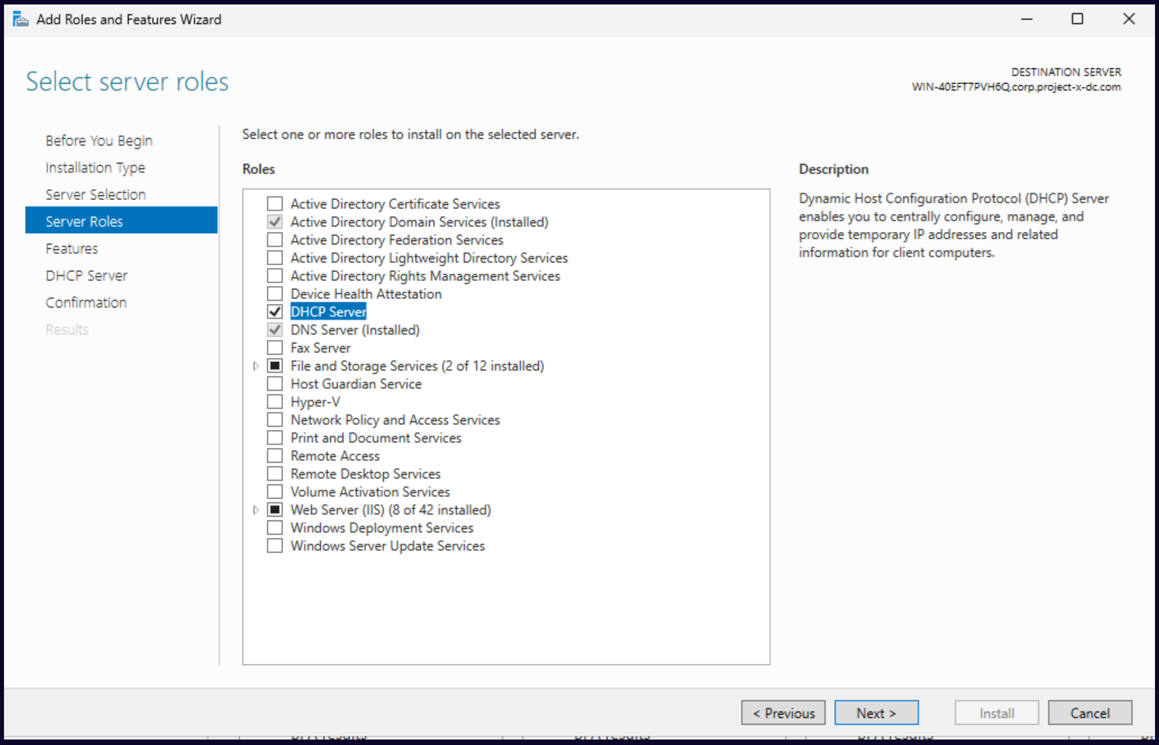
Filter:

Name	IP Address	Operating System
WIN-40EFT7PVH6Q	10.0.2.15	Microsoft Windows Server 2025 Standard Evaluation

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.

Select “Active Directory Domain Services)”, “DHCP Server”, “DNS Server”, File and Storage Services” and “Web Server (IIS)”.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-40EFT7PVH6Q.corp.project-x-dc.com

- Before You Begin
- Installation Type
- Server Selection
- **Server Roles**
- Features
- DHCP Server
- Confirmation
- Results

Select one or more roles to install on the selected server.

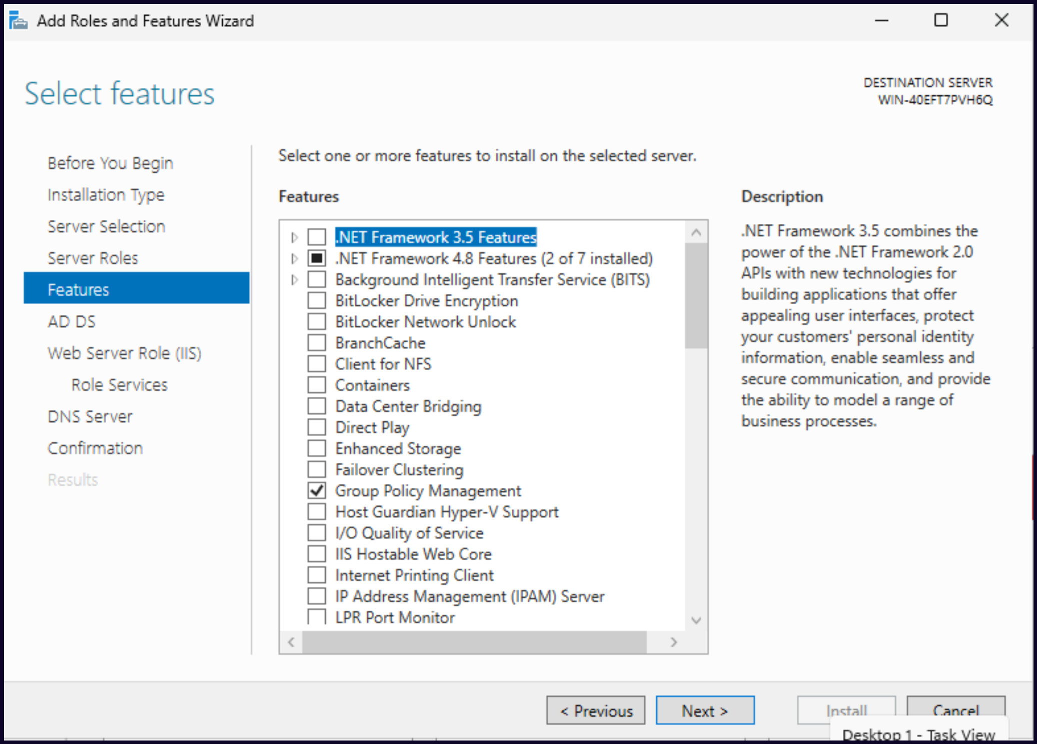
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- ☑ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (8 of 42 installed)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.

Leave the defaults, select "Next".



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-40EFT7PVH6Q

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- **Features**
- AD DS
- Web Server Role (IIS)
  - Role Services
- DNS Server
- Confirmation
- Results

Select one or more features to install on the selected server.

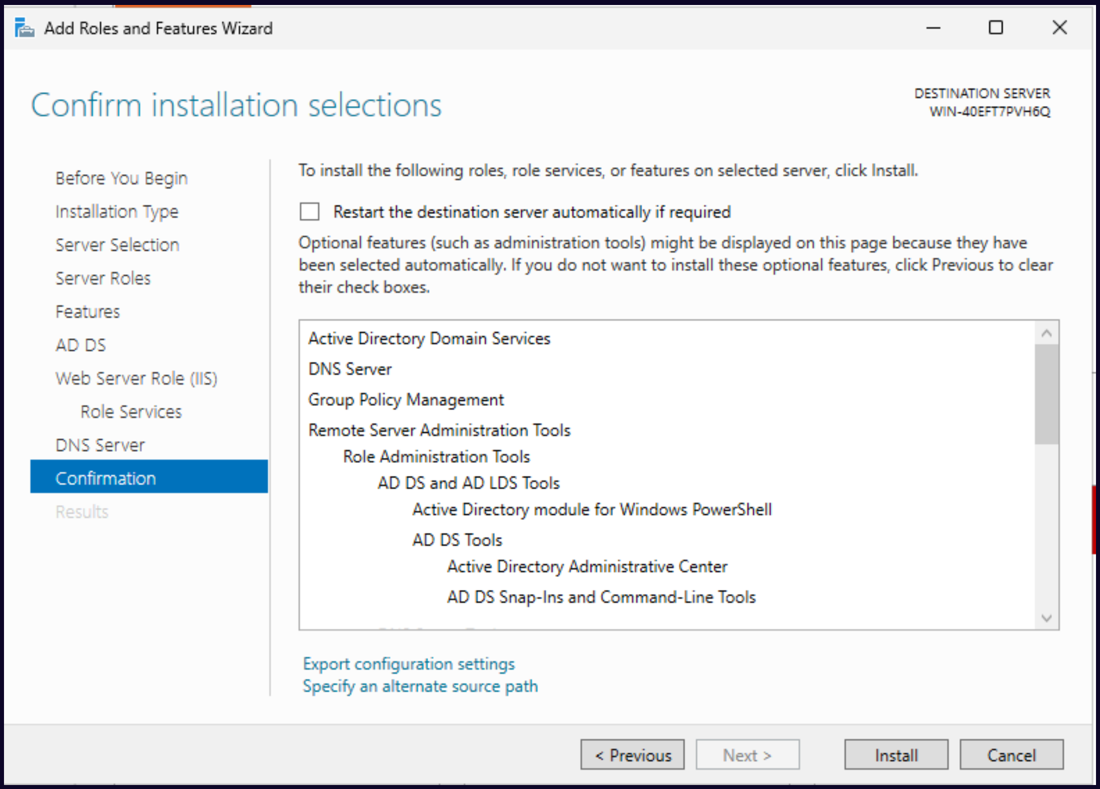
Features

- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.8 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management
- □ Host Guardian Hyper-V Support
- □ I/O Quality of Service
- □ IIS Hostable Web Core
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ LPR Port Monitor

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Select "Next" until you get to the Confirmation tab. Select "Install".



Confirm installation selections

DESTINATION SERVER
WIN-40EFT7PVH6Q

To install the following roles, role services, or features on selected server, click Install.

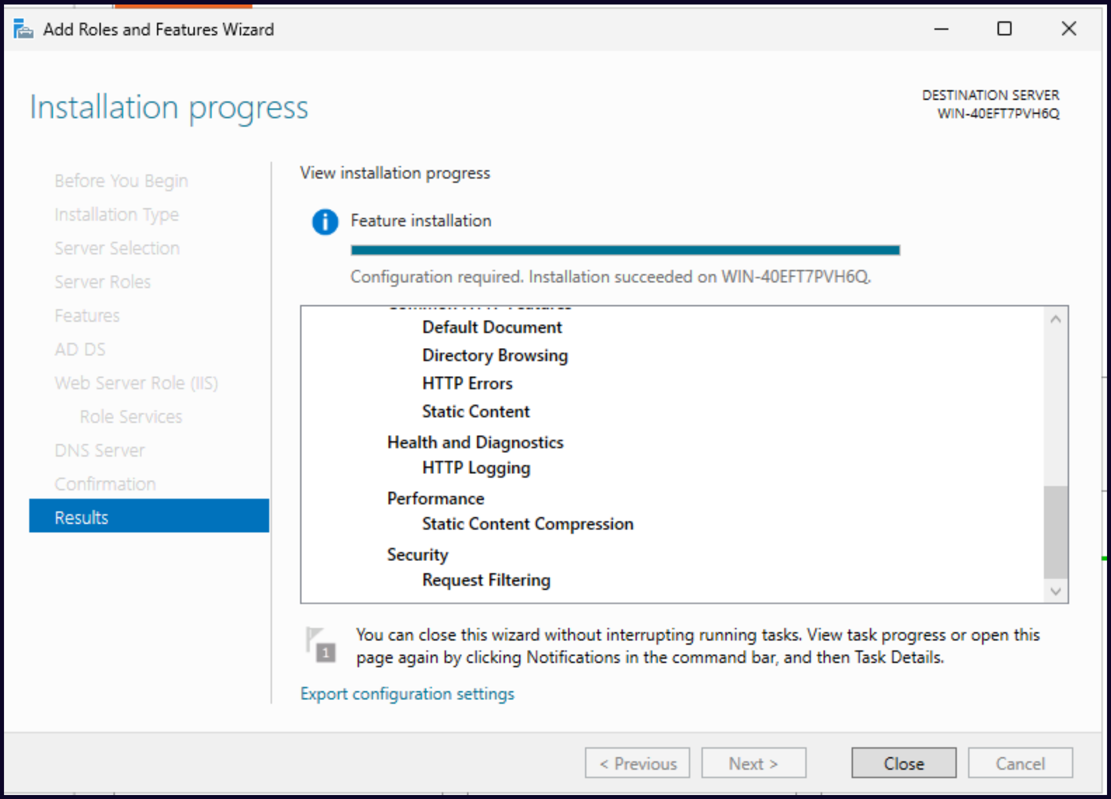
□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

```
Active Directory Domain Services
DNS Server
Group Policy Management
Remote Server Administration Tools
    Role Administration Tools
        AD DS and AD LDS Tools
            Active Directory module for Windows PowerShell
            AD DS Tools
                Active Directory Administrative Center
                AD DS Snap-Ins and Command-Line Tools
```

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

You can close the dialogue box while the features are installed.



Installation progress

DESTINATION SERVER
WIN-40EFT7PVH6Q

View installation progress

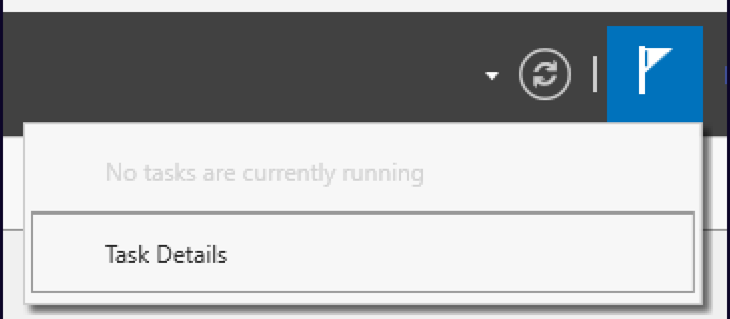
Feature installation

Configuration required. Installation succeeded on WIN-40EFT7PVH6Q.

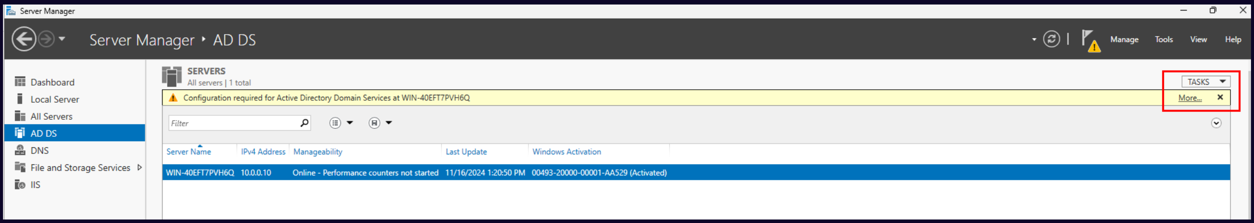
```
        Default Document
        Directory Browsing
        HTTP Errors
        Static Content
    Health and Diagnostics
        HTTP Logging
    Performance
        Static Content Compression
    Security
        Request Filtering
```

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

You will see a message in the notifications section of “Server Manager” when all of the features have been installed.


No tasks are currently running

A message notification will appear for configuring Active Directory, Select “More”.

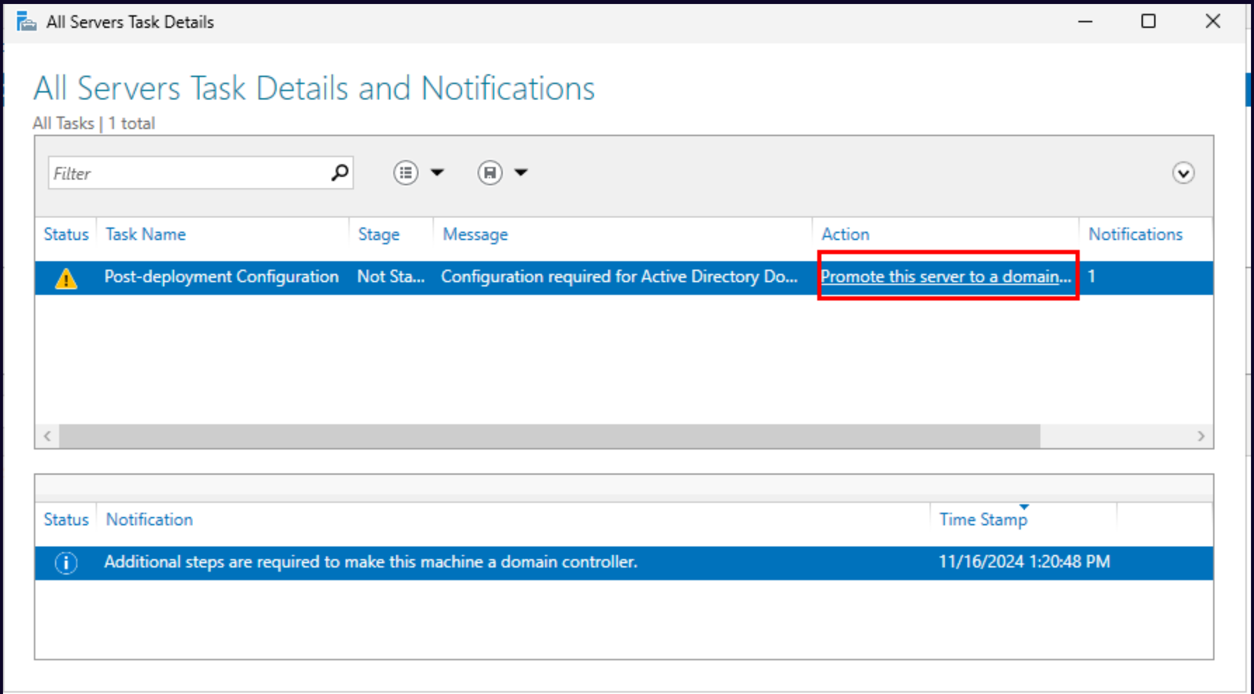


SERVERS
All servers | 1 total

⚠ Configuration required for Active Directory Domain Services at WIN-40EFT7PVH6Q

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-40EFT7PVH6Q	10.0.0.10	Online - Performance counters not started	11/16/2024 1:20:50 PM	00493-20000-00001-AA529 (Activated)

Select “Promote this server to a domain”.

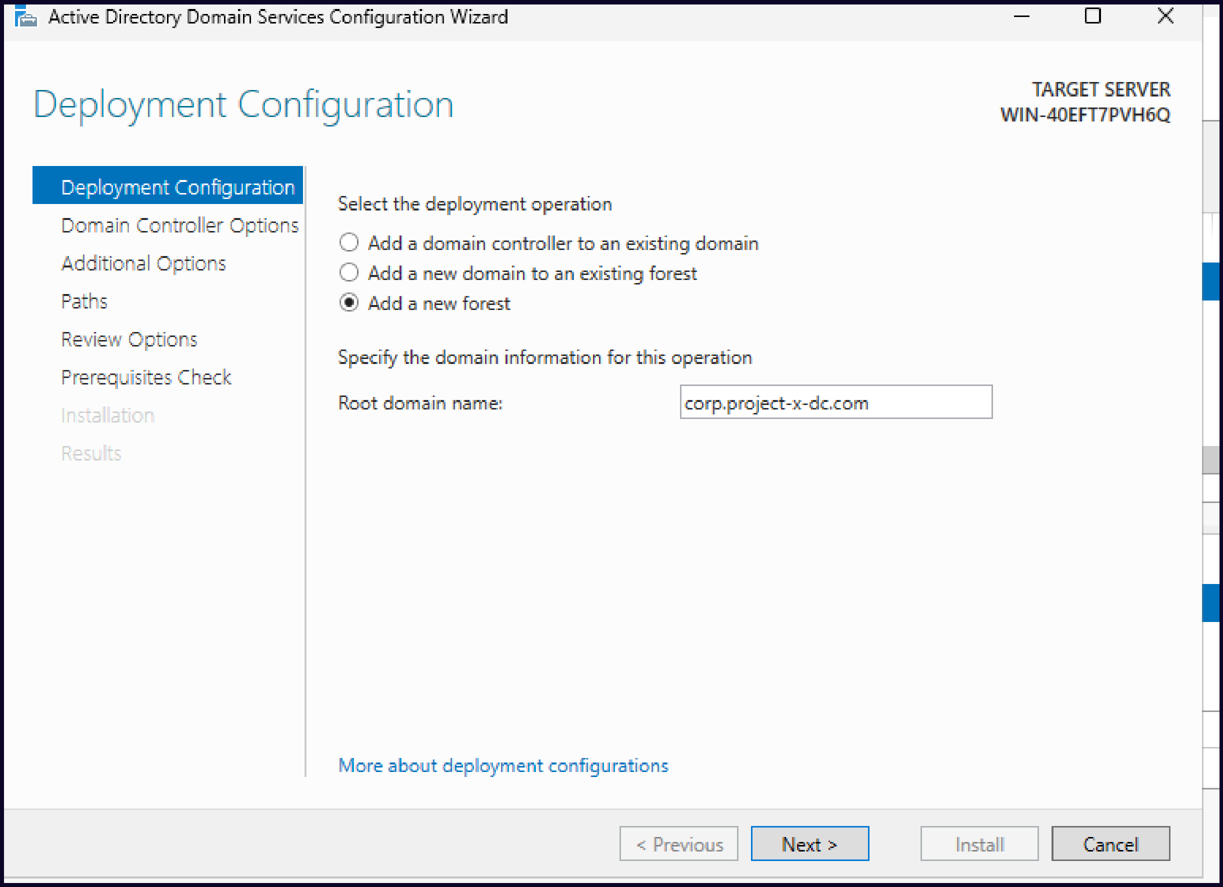


All Servers Task Details and Notifications
All Tasks | 1 total

Status	Task Name	Stage	Message	Action	Notifications
⚠	Post-deployment Configuration	Not Sta...	Configuration required for Active Directory Do...	Promote this server to a domain...	1

Status	Notification	Time Stamp
ⓘ	Additional steps are required to make this machine a domain controller.	11/16/2024 1:20:48 PM

Select “Add a new forest”. Then enter a root domain name, `corp.project-x-dc.com`.



Deployment Configuration

TARGET SERVER
WIN-40EFT7PVH6Q

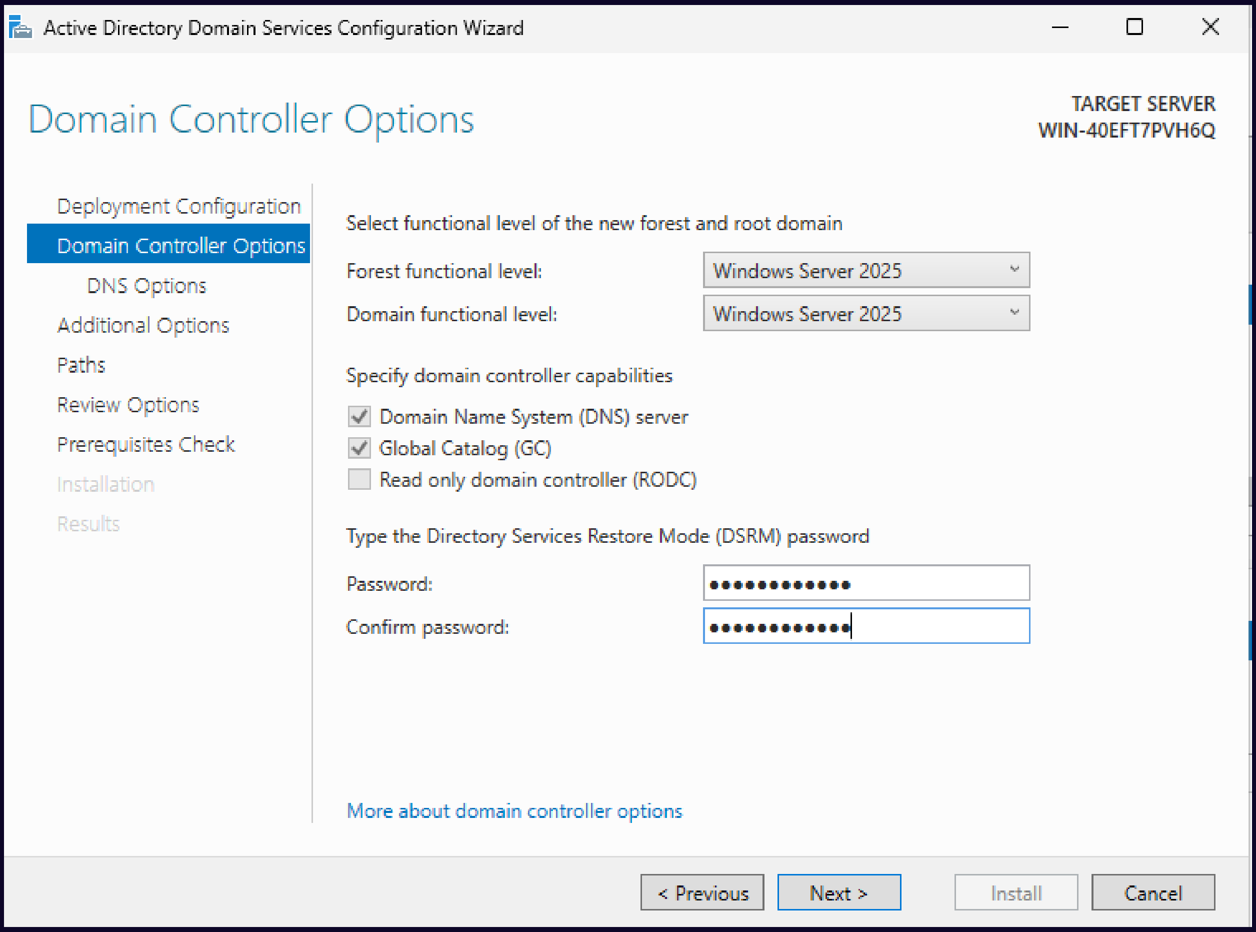
Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: corp.project-x-dc.com

Leave the default options, for the Directory Services Restore Mode (DSRM) password, use the Administrator password (`@Deeboodah1!`). Select Next.



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WIN-40EFT7PVH6Q

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2025

Domain functional level: Windows Server 2025

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

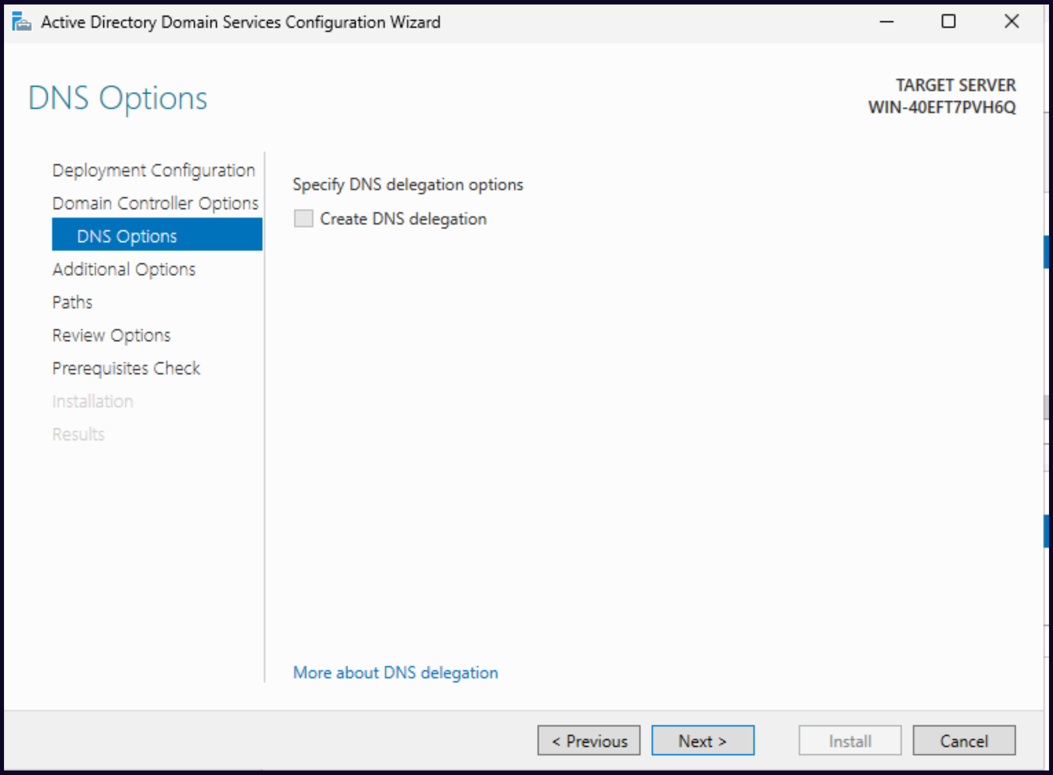
Type the Directory Services Restore Mode (DSRM) password

Password: •••••••••••••

Confirm password: •••••••••••••

More about domain controller options

Leave the “Create DNS delegation” box blank → “Next”.



Active Directory Domain Services Configuration Wizard

DNS Options

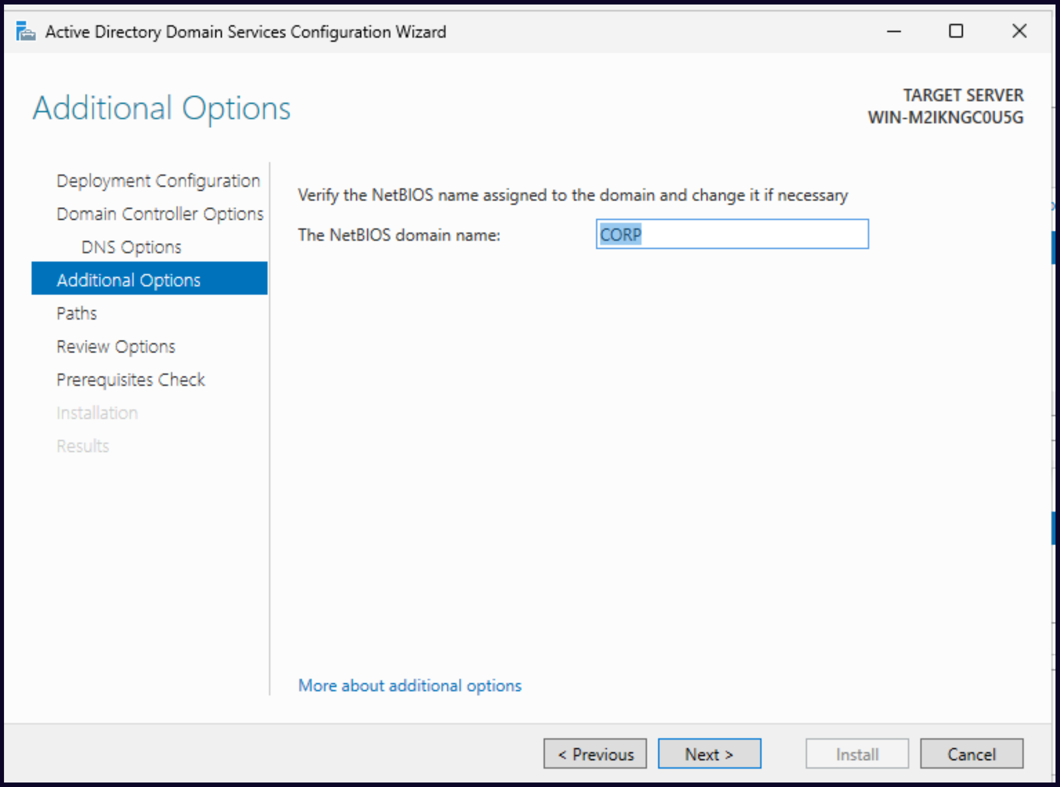
TARGET SERVER
WIN-40EFT7PVH6Q

Specify DNS delegation options

□ Create DNS delegation

More about DNS delegation

Leave the NetBIOS CORP, proceed with all other defaults until getting to the check screen.



Active Directory Domain Services Configuration Wizard

Additional Options

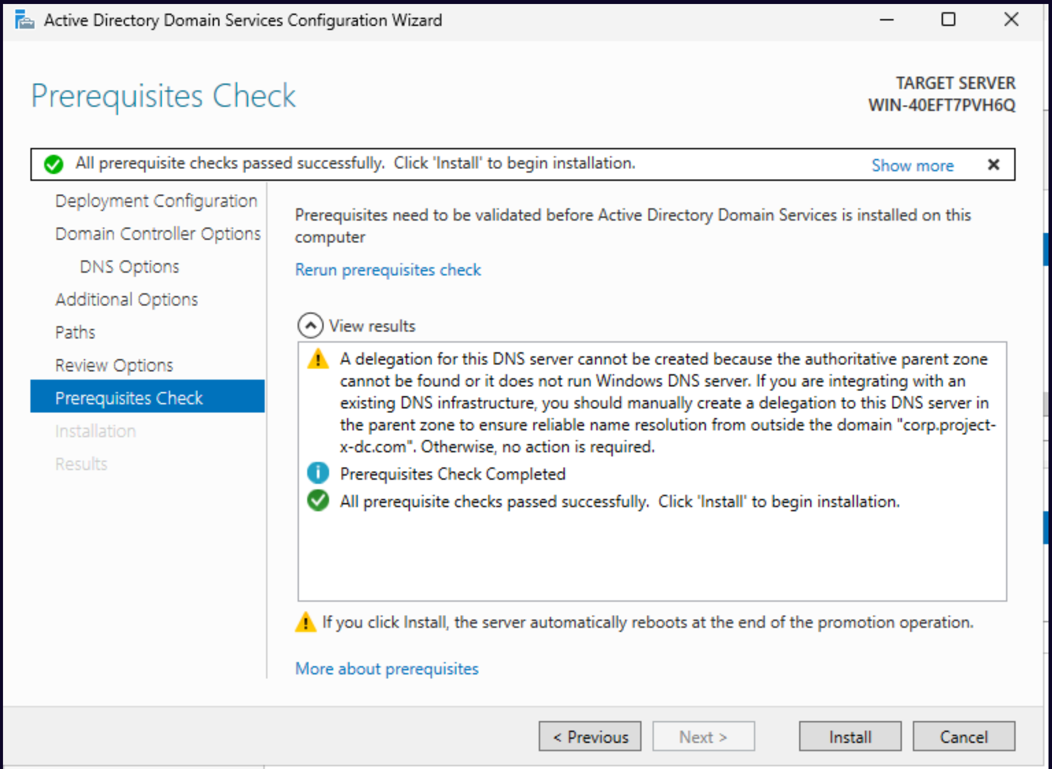
TARGET SERVER
WIN-M2IKNGC0U5G

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: CORP

More about additional options

A few checks will be run through. Allow the wizard to finish, then select “Install”. Let the server restart.



Prerequisites Check

TARGET SERVER
WIN-40EFT7PVH6Q

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation.

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

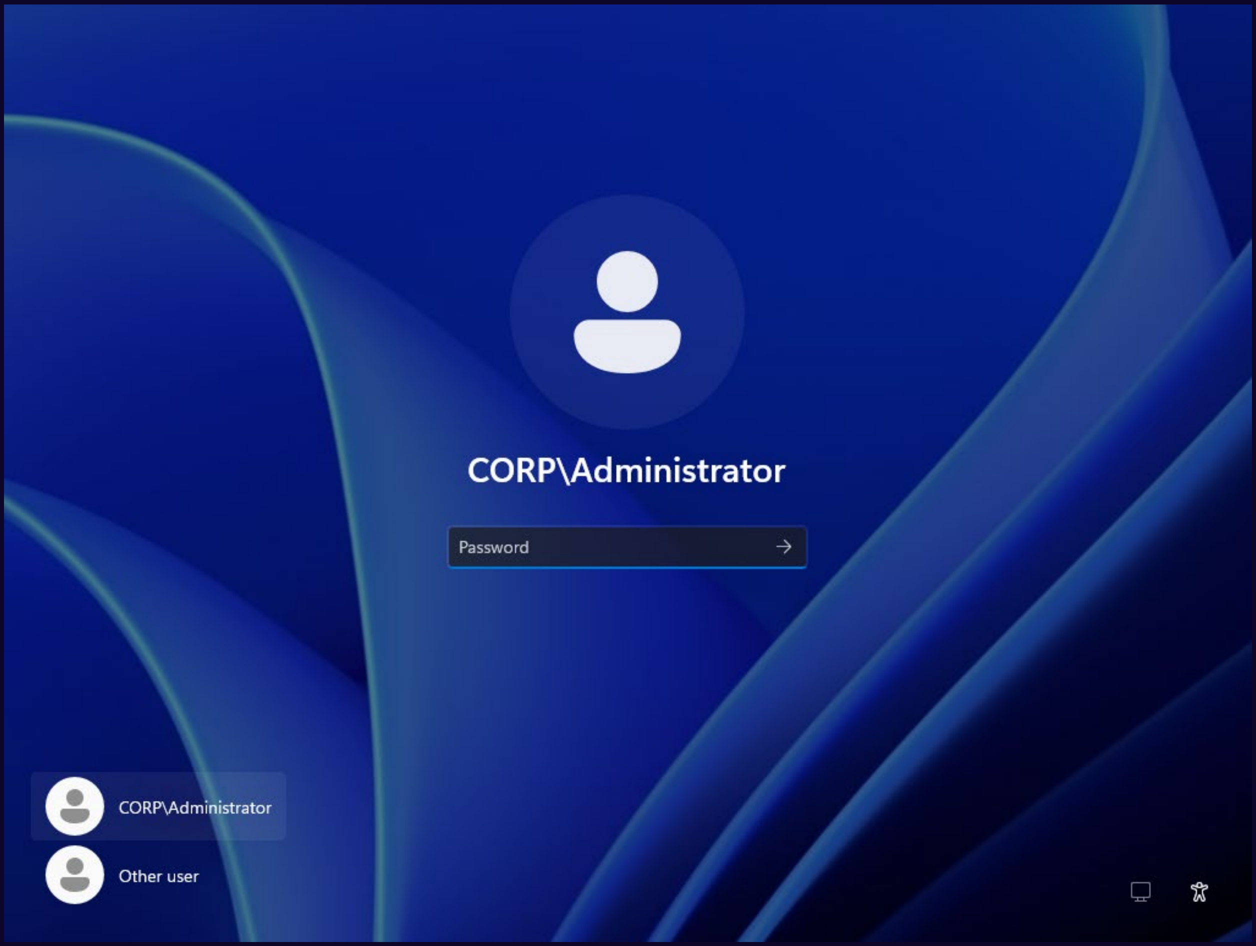
⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "corp.project-x-dc.com". Otherwise, no action is required.

ℹ Prerequisites Check Completed

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation.

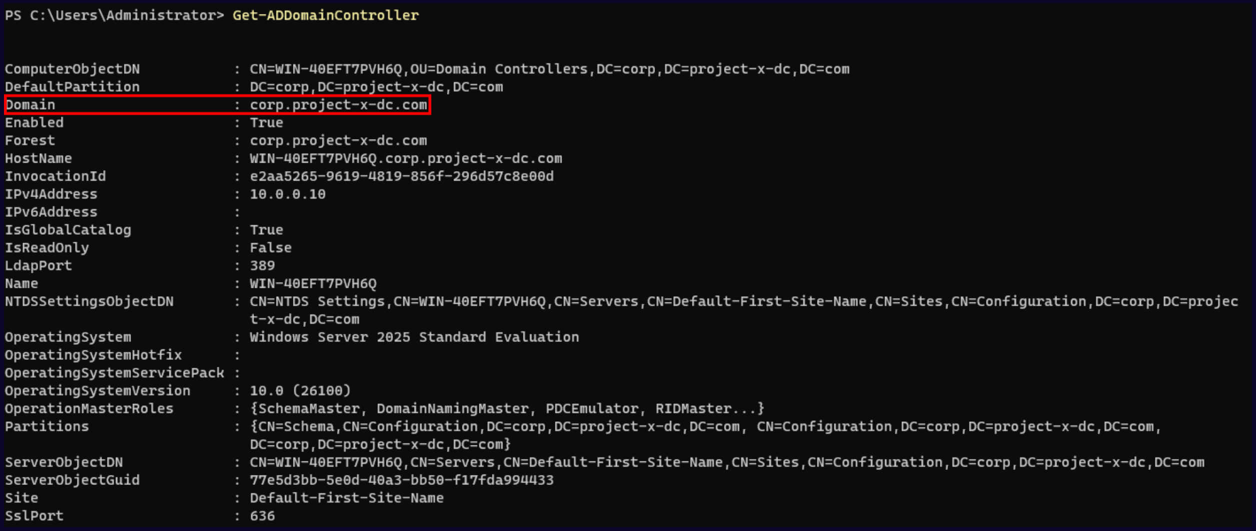
⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

You can now login under the `CORP\Administrator` domain.



To verify this Server is apart of the domain, open a new PowerShell session, type in:

```
Get-ADDomainController
```

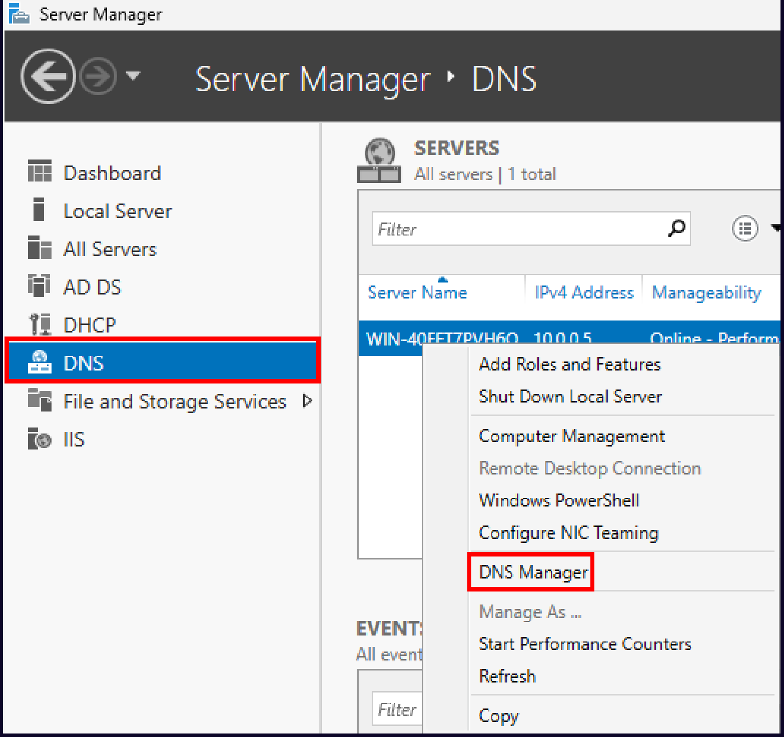


```
PS C:\Users\Administrator> Get-ADDomainController


ComputerObjectDN           : CN=WIN-40EFT7PVH6Q,OU=Domain Controllers,DC=corp,DC=project-x-dc,DC=com
DefaultPartition           : DC=corp,DC=project-x-dc,DC=com
Domain                     : corp.project-x-dc.com
Enabled                    : True
Forest                     : corp.project-x-dc.com
HostName                   : WIN-40EFT7PVH6Q.corp.project-x-dc.com
InvocationId               : e2aa5265-9619-4819-856f-296d57c8e00d
IPv4Address                : 10.0.0.10
IPv6Address                :
IsGlobalCatalog            : True
IsReadOnly                 : False
LdapPort                   : 389
Name                       : WIN-40EFT7PVH6Q
NTDSSettingsObjectDN       : CN=NTDS Settings,CN=WIN-40EFT7PVH6Q,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=corp,DC=projec
                             t-x-dc,DC=com
OperatingSystem            : Windows Server 2025 Standard Evaluation
OperatingSystemHotfix      :
OperatingSystemServicePack :
OperatingSystemVersion     : 10.0 (26100)
OperationMasterRoles       : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
Partitions                 : {CN=Schema,CN=Configuration,DC=corp,DC=project-x-dc,DC=com, CN=Configuration,DC=corp,DC=project-x-dc,DC=com,
                             DC=corp,DC=project-x-dc,DC=com}
ServerObjectDN             : CN=WIN-40EFT7PVH6Q,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=corp,DC=project-x-dc,DC=com
ServerObjectGuid           : 77e5d3bb-5e0d-40a3-bb50-f17fda994433
Site                       : Default-First-Site-Name
SslPort                    : 636
```

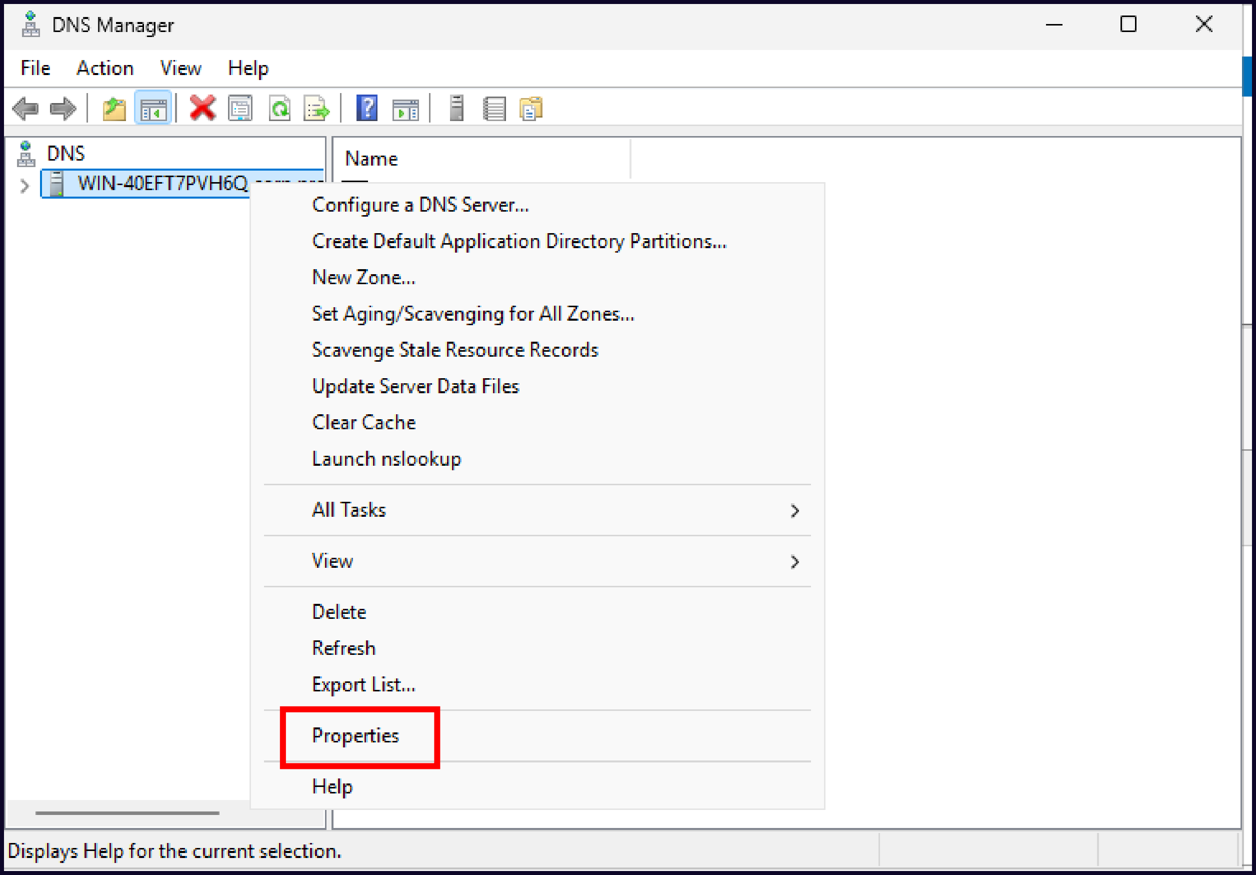
Setup DNS For Internet Access

Step 1

Go to “Server Manager” → DNS → Select the Server → Right-click → “DNS Manager”.

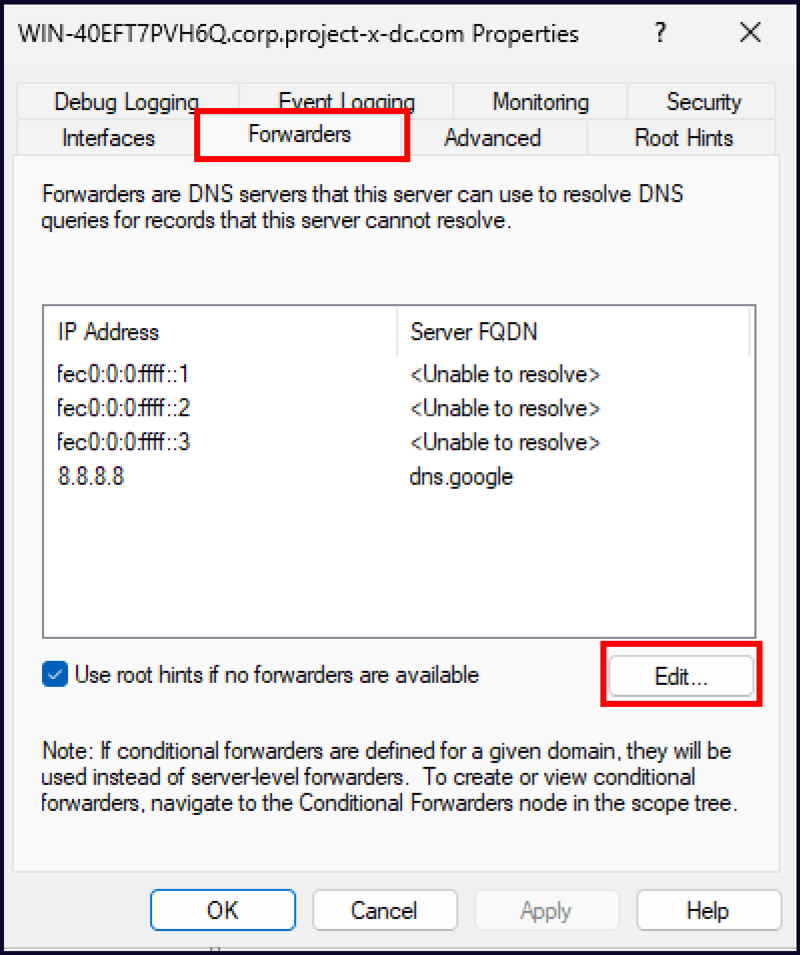


DNS Manager will appear → Right-click the domain → “Properties”.



Displays Help for the current selection.

Select the “Forwarders” tab → “Edit”.



WIN-40EFT7PVH6Q.corp.project-x-dc.com Properties

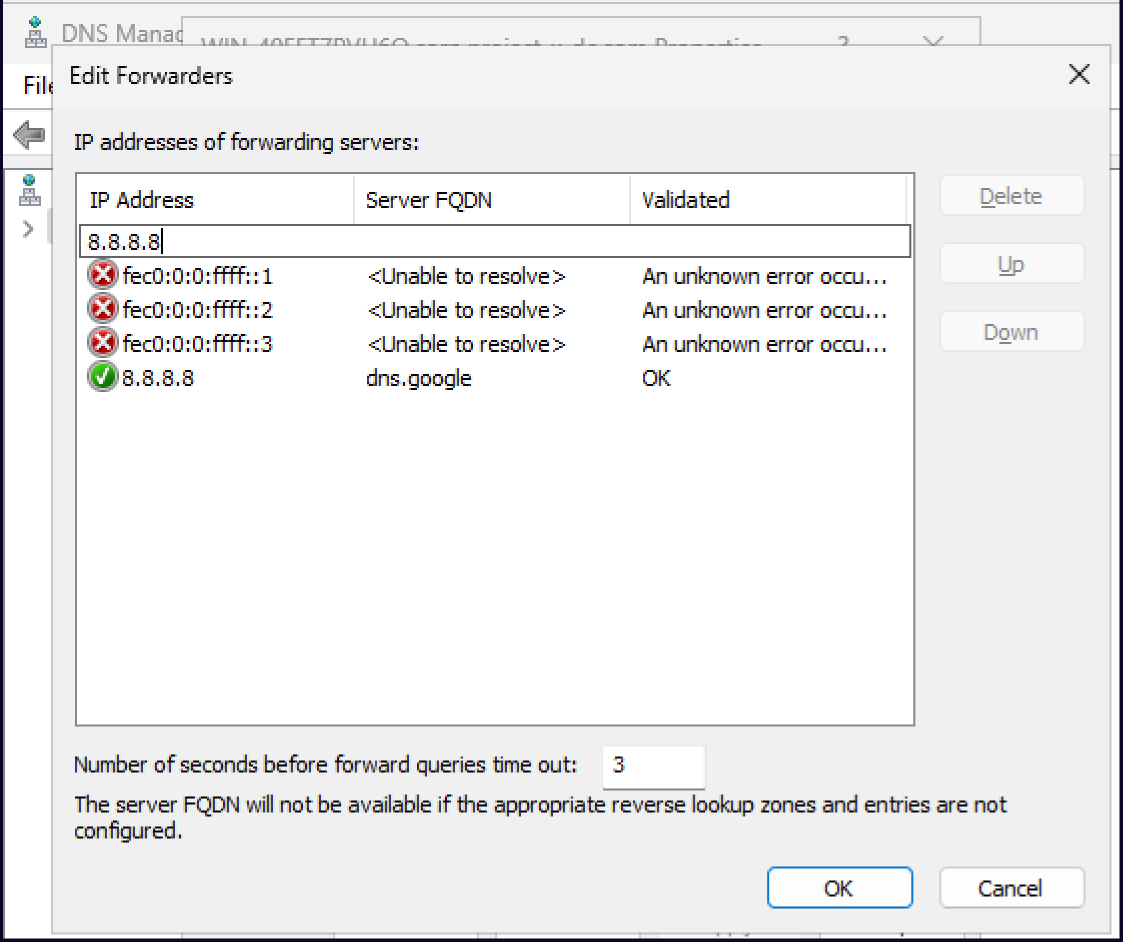
Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

IP Address	Server FQDN
fec0:0:0:ffff::1	<Unable to resolve>
fec0:0:0:ffff::2	<Unable to resolve>
fec0:0:0:ffff::3	<Unable to resolve>
8.8.8.8	dns.google

☑ Use root hints if no forwarders are available

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

Add in “8.8.8.8” → Select “OK”. This will allow us to still use the Internet from Windows Server 2025.



IP addresses of forwarding servers:

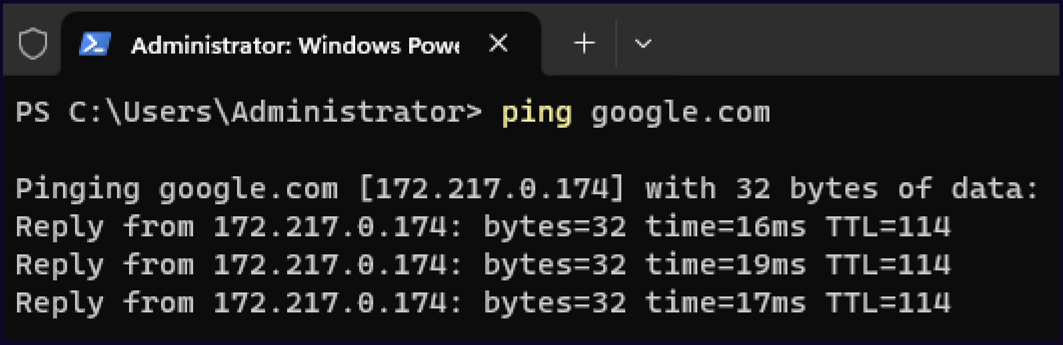
IP Address	Server FQDN	Validated
8.8.8.8		
✗ fec0:0:0:ffff::1	<Unable to resolve>	An unknown error occu...
✗ fec0:0:0:ffff::2	<Unable to resolve>	An unknown error occu...
✗ fec0:0:0:ffff::3	<Unable to resolve>	An unknown error occu...
✓ 8.8.8.8	dns.google	OK

Number of seconds before forward queries time out: 3

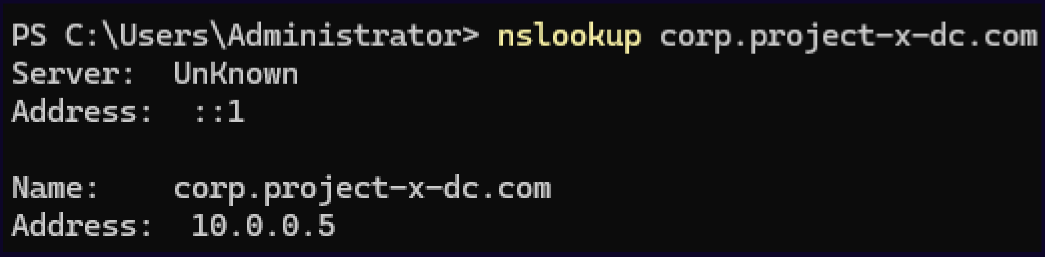
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

Open a PowerShell session. Enter:

```
ping google.com

nslookup corp.project-x-dc.com
```



```
PS C:\Users\Administrator> ping google.com

Pinging google.com [172.217.0.174] with 32 bytes of data:
Reply from 172.217.0.174: bytes=32 time=16ms TTL=114
Reply from 172.217.0.174: bytes=32 time=19ms TTL=114
Reply from 172.217.0.174: bytes=32 time=17ms TTL=114
```

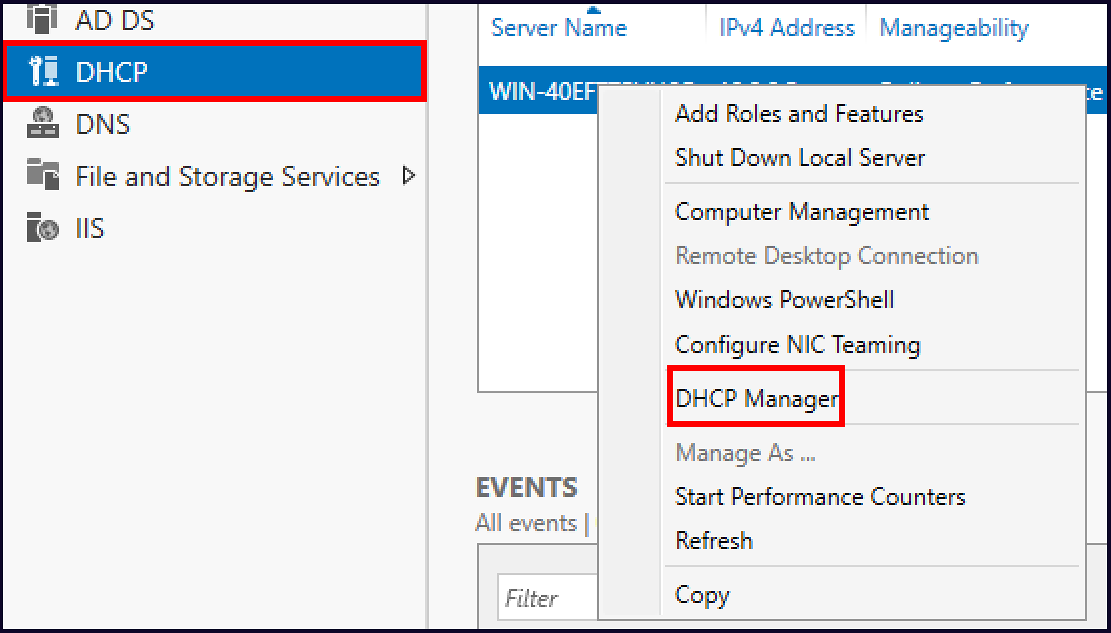


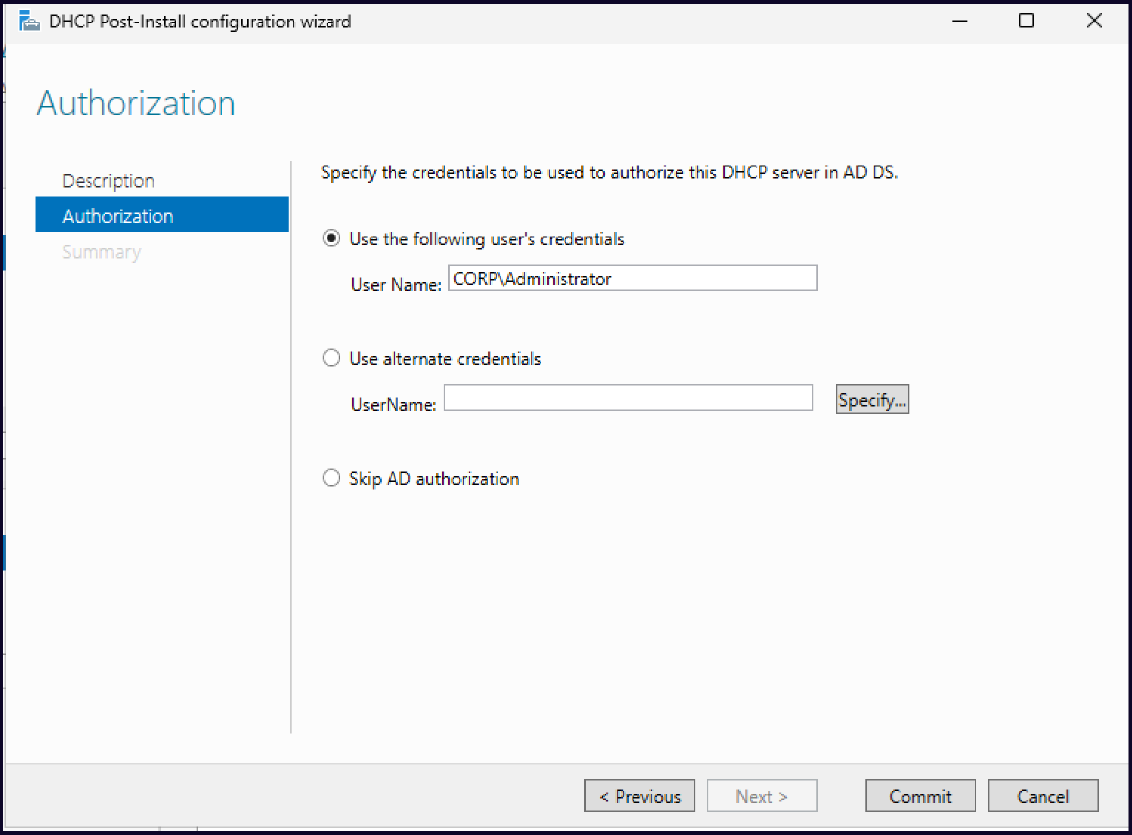
```
PS C:\Users\Administrator> nslookup corp.project-x-dc.com
Server:  UnKnown
Address:  ::1

Name:    corp.project-x-dc.com
Address:  10.0.0.5
```

Setup DHCP

Step 1

Navigate to “DHCP” → “DHCP Manager”.





DHCP Post-Install configuration wizard

Authorization

Specify the credentials to be used to authorize this DHCP server in AD DS.

● Use the following user's credentials

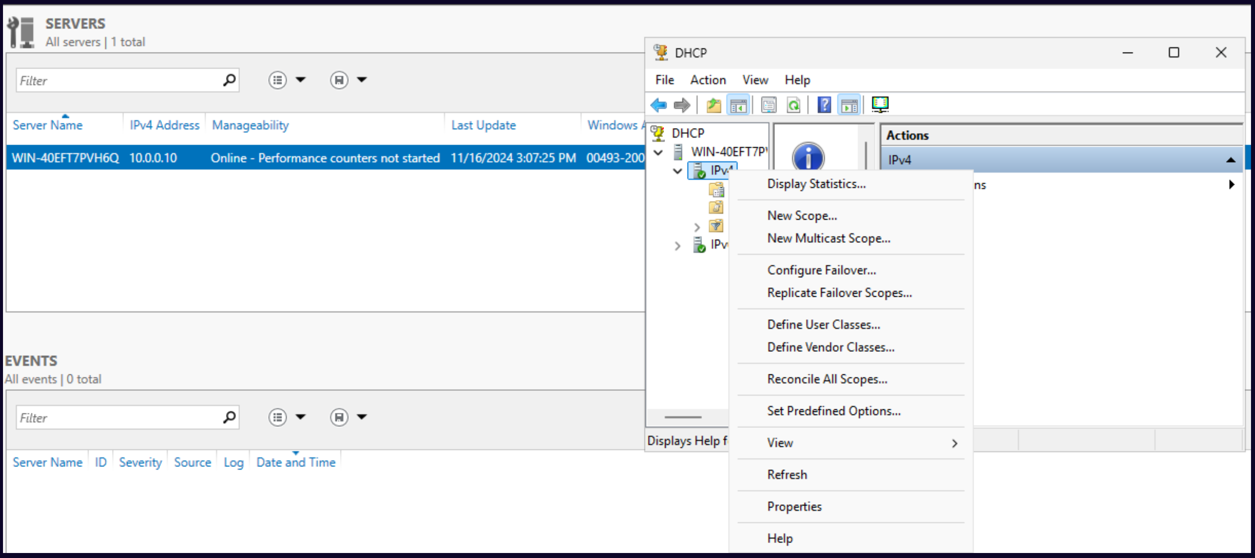
User Name: CORP\Administrator

○ Use alternate credentials

UserName:

○ Skip AD authorization

Navigate to “IPv4” → “New Scope”.



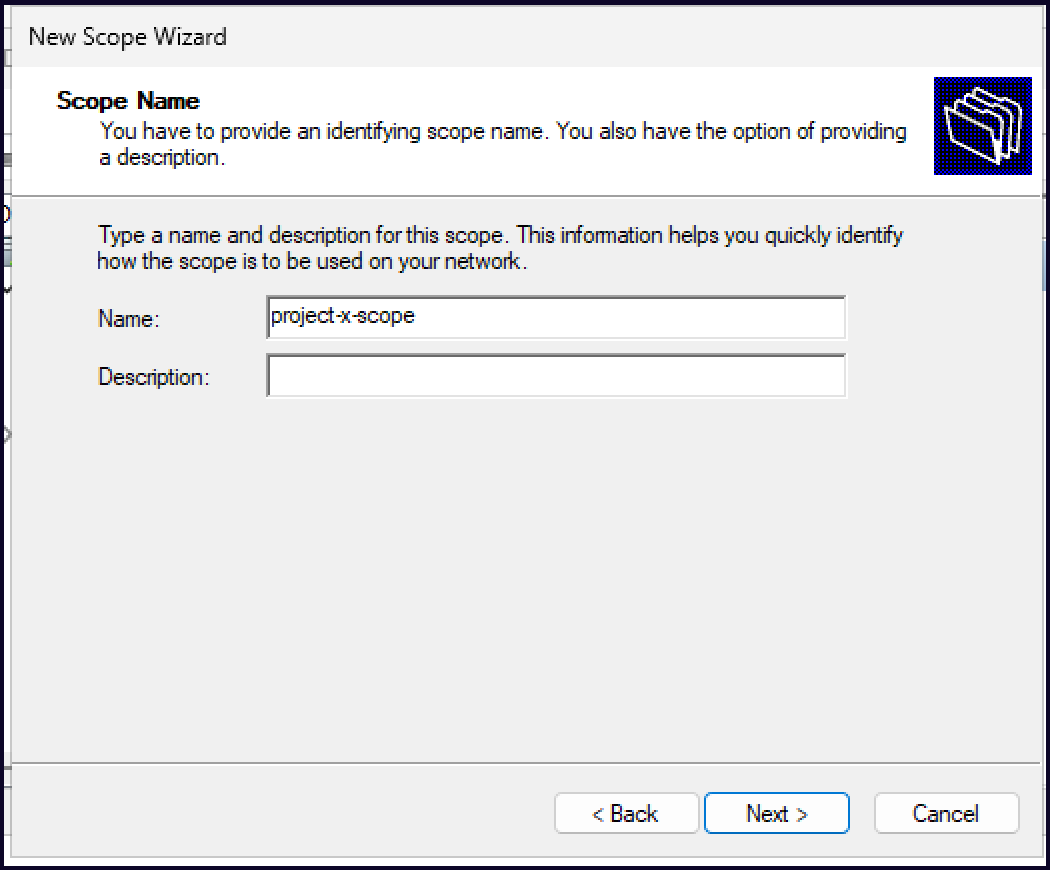
SERVERS
All servers | 1 total

Server Name	IPv4 Address	Manageability	Last Update	Windows A
WIN-40EFT7PVH6Q	10.0.0.10	Online - Performance counters not started	11/16/2024 3:07:25 PM	00493-200

EVENTS
All events | 0 total

Server Name	ID	Severity	Source	Log	Date and Time

Add project-x-scope.



New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: project-x-scope

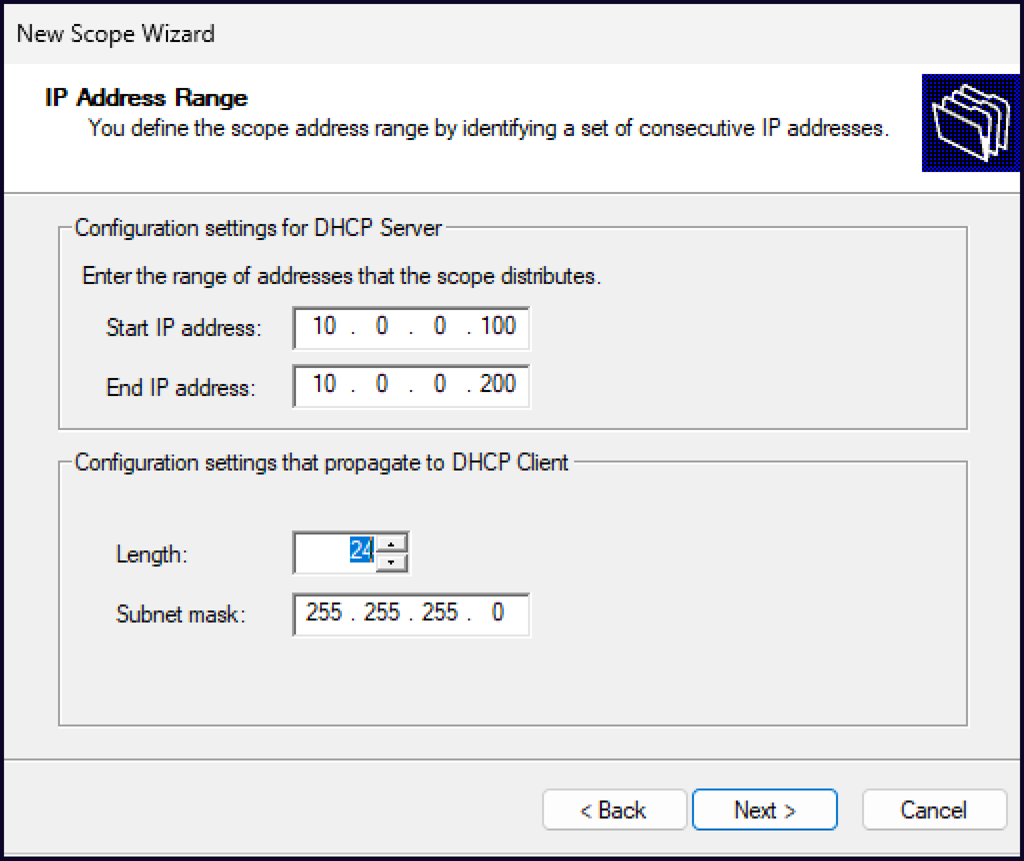
Description:

Enter the following addresses for leasing. Select “Next”. And

Start IP address: 10.0.0.100

End IP address: 10.0.0.200

Subnet mask: 255.255.255.0


New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 10 . 0 . 0 . 100

End IP address: 10 . 0 . 0 . 200

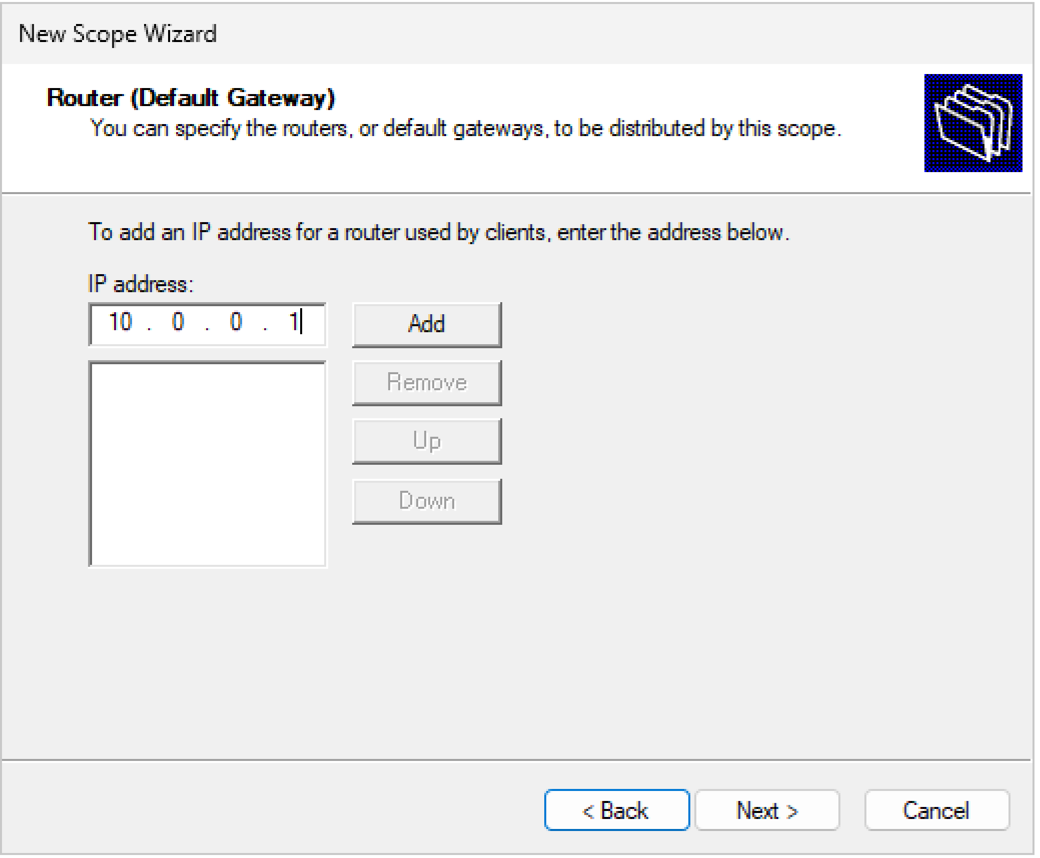
Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Run through all the defaults (don’t worry about excluding IP addresses or lease expiration).

Add 10.0.0.1 for the Router IP.



New Scope Wizard

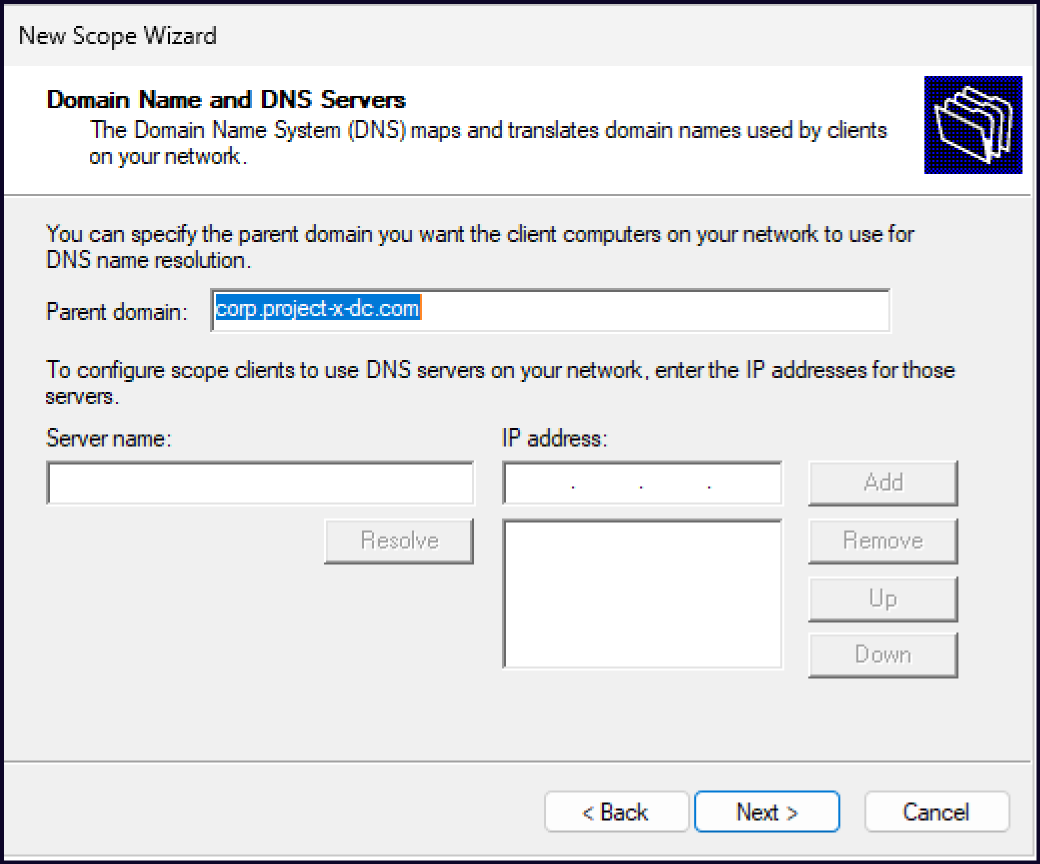
Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address: 10 . 0 . 0 . 1

Keep default.



New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

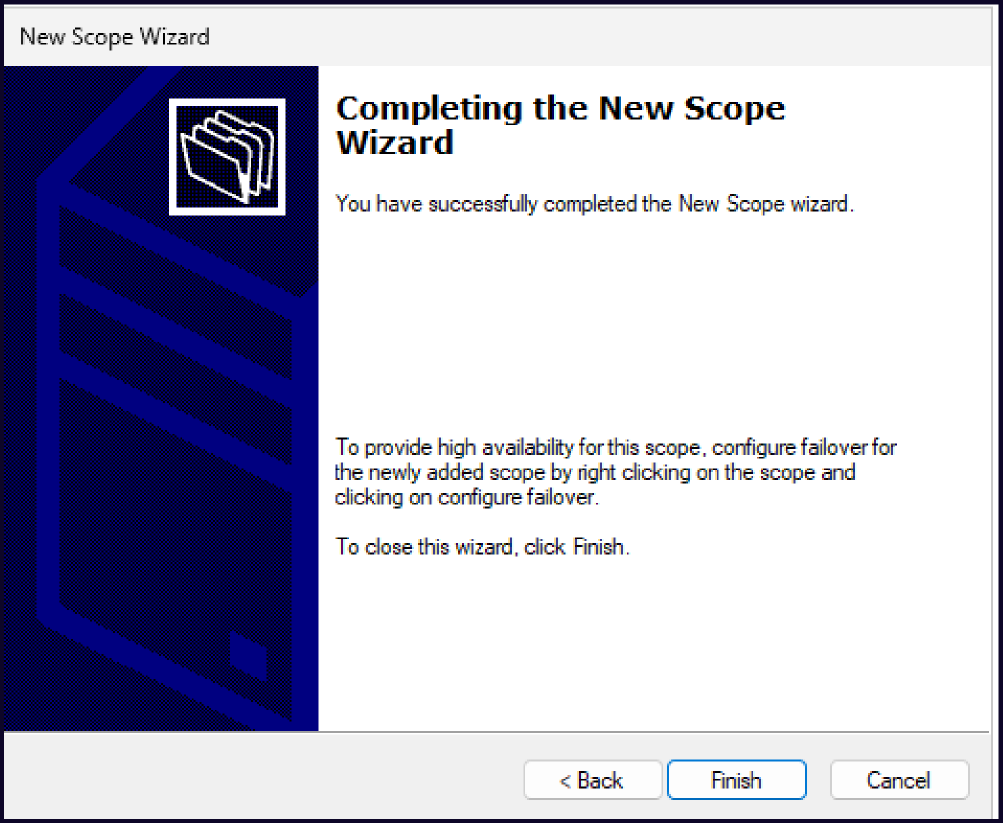
Parent domain: corp.project-x-dc.com

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address: . . .

Run through all the other dialogue box defaults, until finished.



New Scope Wizard

Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

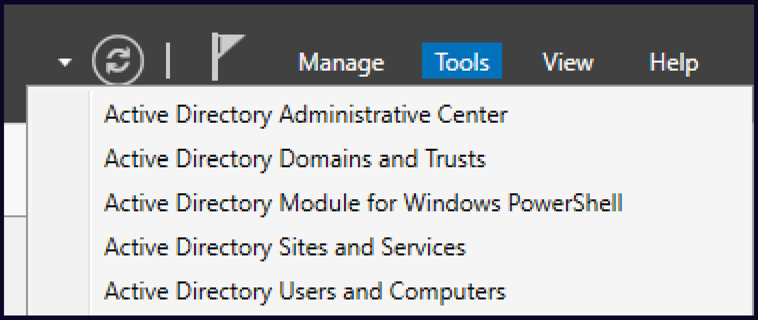
To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

To close this wizard, click Finish.

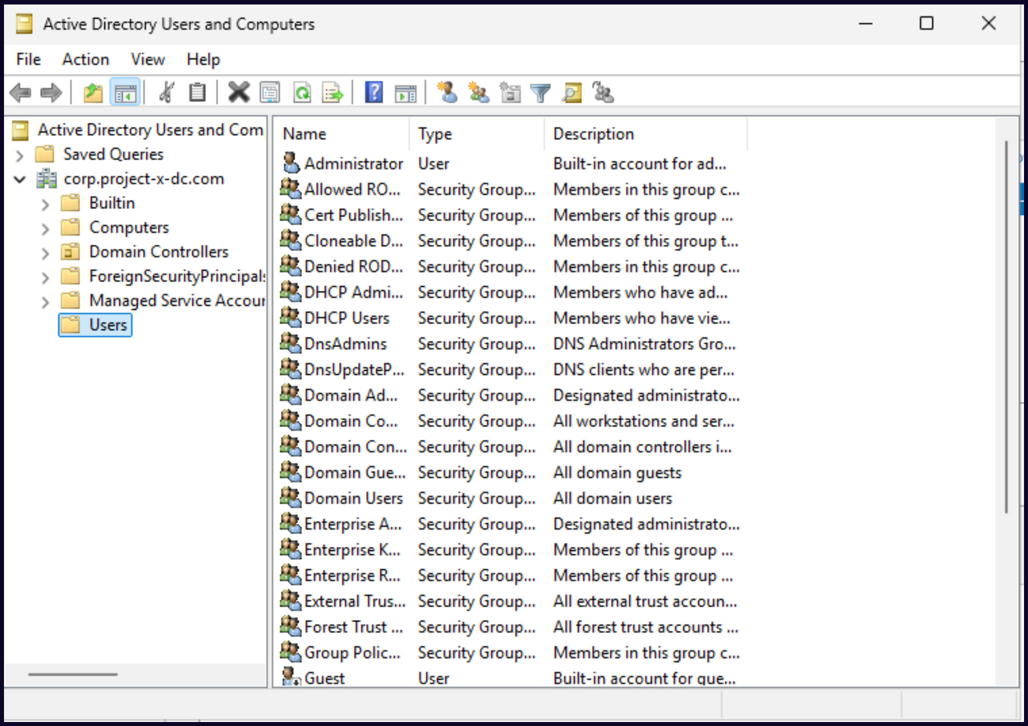
Add User Accounts in Active Directory

Step 1

Navigate to “Server Manager” → “Tools” → “Active Directory Users and Computers”.

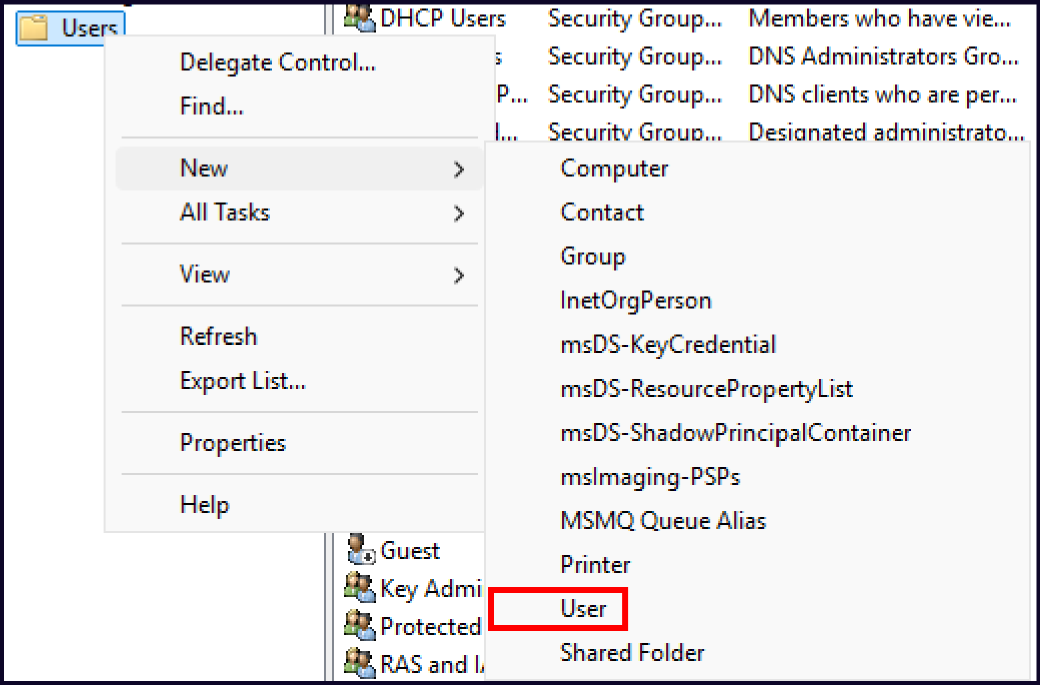


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers



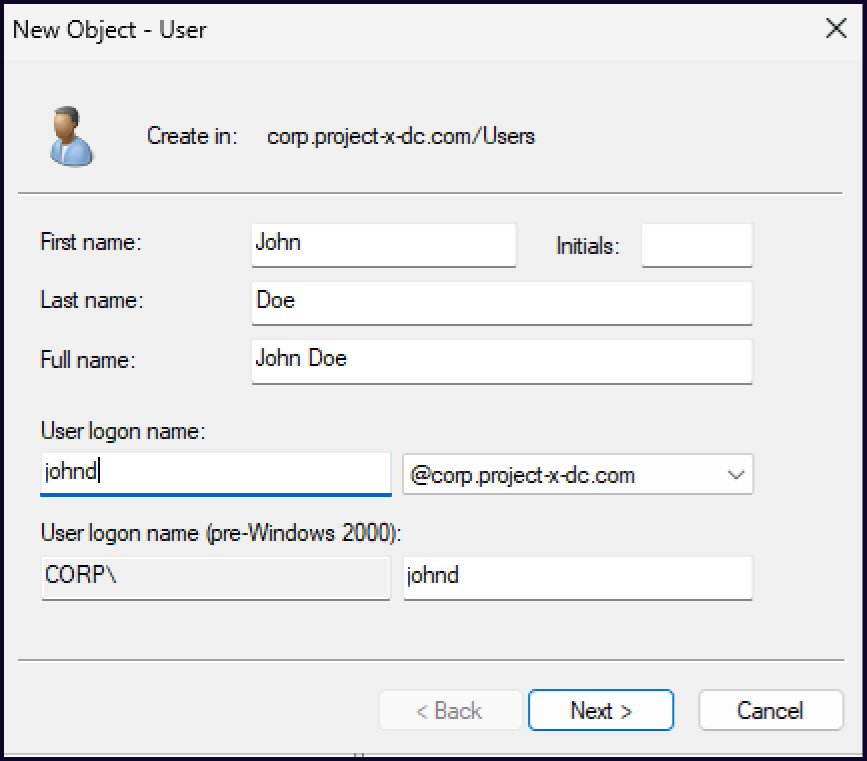
Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DHCP Admi...	Security Group...	Members who have ad...
DHCP Users	Security Group...	Members who have vie...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
External Trus...	Security Group...	All external trust accoun...
Forest Trust ...	Security Group...	All forest trust accounts ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...

Navigate to “Users” → “New” → “User”.



Add in the user information.

👉 Refer to the “Project Overview” guide for more information on default usernames and passwords.



New Object - User

Create in: corp.project-x-dc.com/Users

First name: John

Initials:

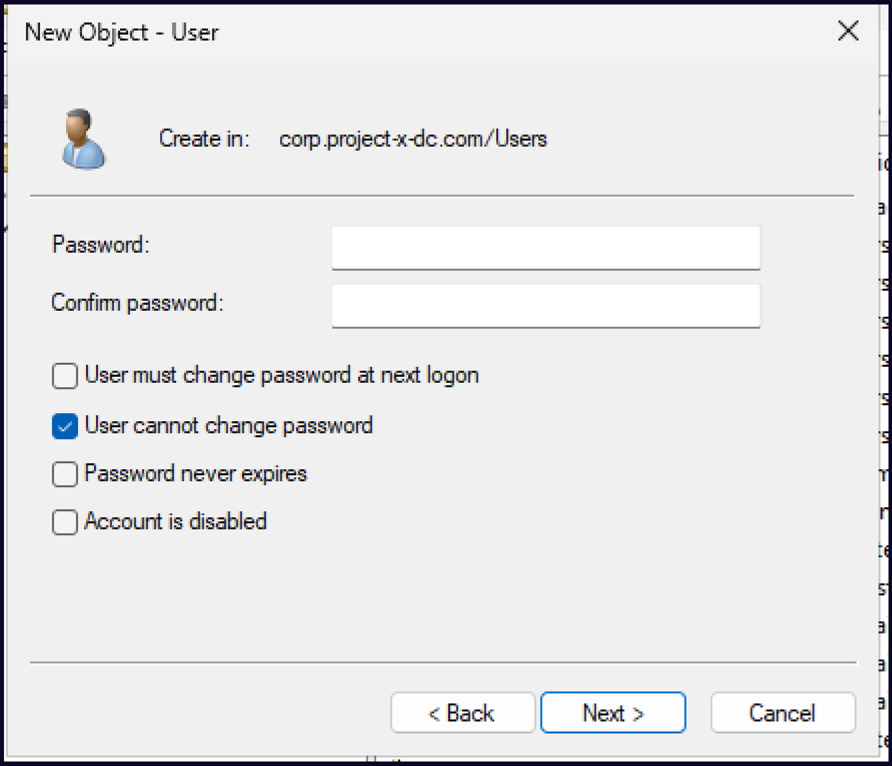
Last name: Doe

Full name: John Doe

User logon name: johnd @corp.project-x-dc.com

User logon name (pre-Windows 2000): CORP\ johnd

Select “User cannot change password” → “Next”. Run through all default configuration settings.



New Object - User

Create in: corp.project-x-dc.com/Users

Password:

Confirm password:

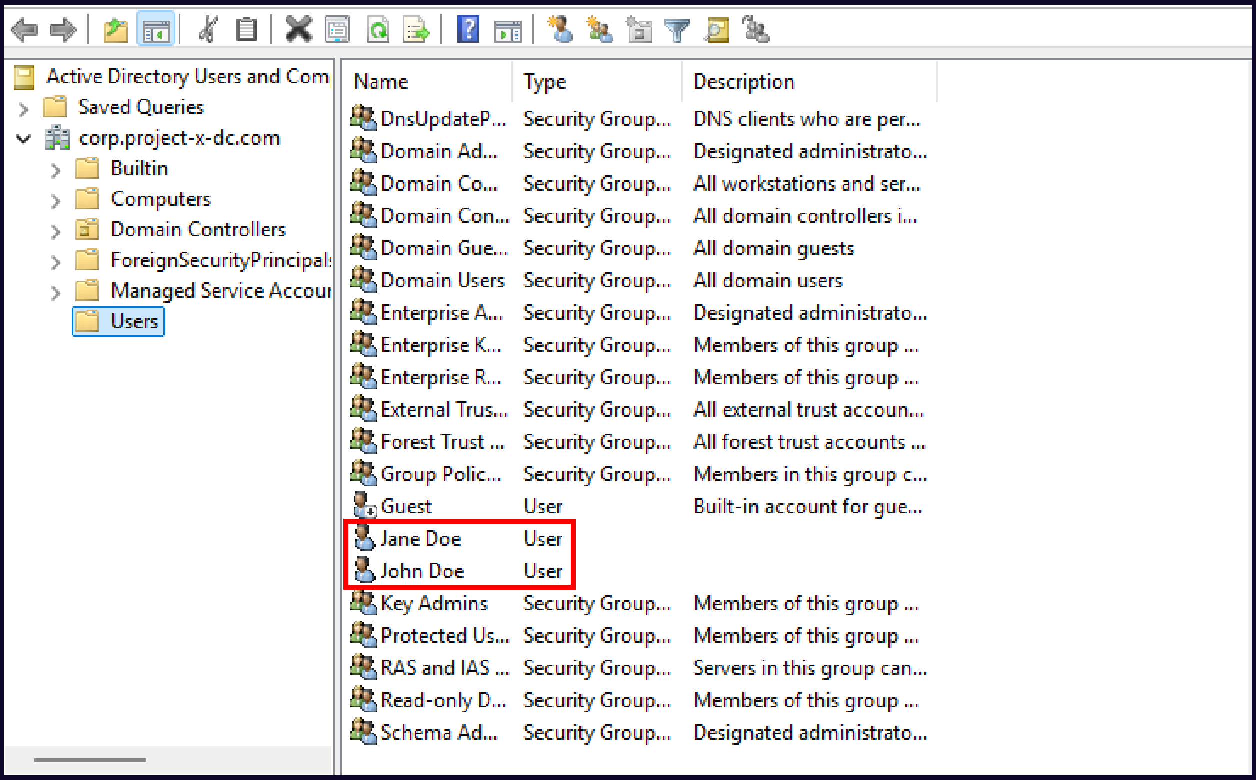
□ User must change password at next logon

☑ User cannot change password

□ Password never expires

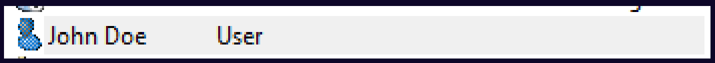
□ Account is disabled

You will see the new users created. Succes!



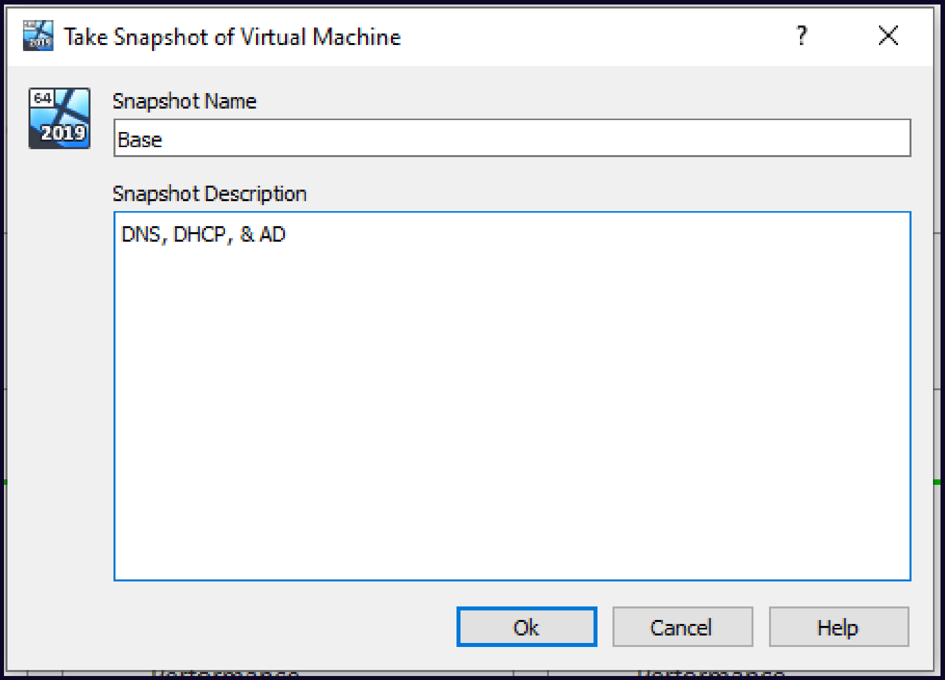
Active Directory Users and Com
- Saved Queries
- corp.project-x-dc.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal:
  - Managed Service Accour
  - Users

Name	Type	Description
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
External Trus...	Security Group...	All external trust accoun...
Forest Trust ...	Security Group...	All forest trust accounts ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Jane Doe	User	
John Doe	User	
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...



John Doe User

📷 Take Snapshot!



Take Snapshot of Virtual Machine

Snapshot Name: Base

Snapshot Description: DNS, DHCP, & AD

>projectsecurity_