Active Directory – Creating and Managing User Accounts, Passwords and Group Policies

Lab Overview

The purpose of this lab is to create and manage user accounts, passwords and group policies for SOA Enterprises within Active Directory. SOA Enterprises is small to medium sized business with between 30-40 employees. Its users frequently call to report issues with login, passwords and access requests. As a Tier 1 Helpdesk Technician supporting users at SOA Enterprise, it is important to resolve these issues using Active Directory to allow employees to access their user accounts and other resources. Some of the tasks performed will include:

- Creating and managing AD user accounts
- Resetting and unlocking user accounts
- Enabling/disabling accounts
- Managing group membership
- Troubleshooting common login issues
- Understanding basic AD organisational structure

Lab Environment Requirements

Required Machines

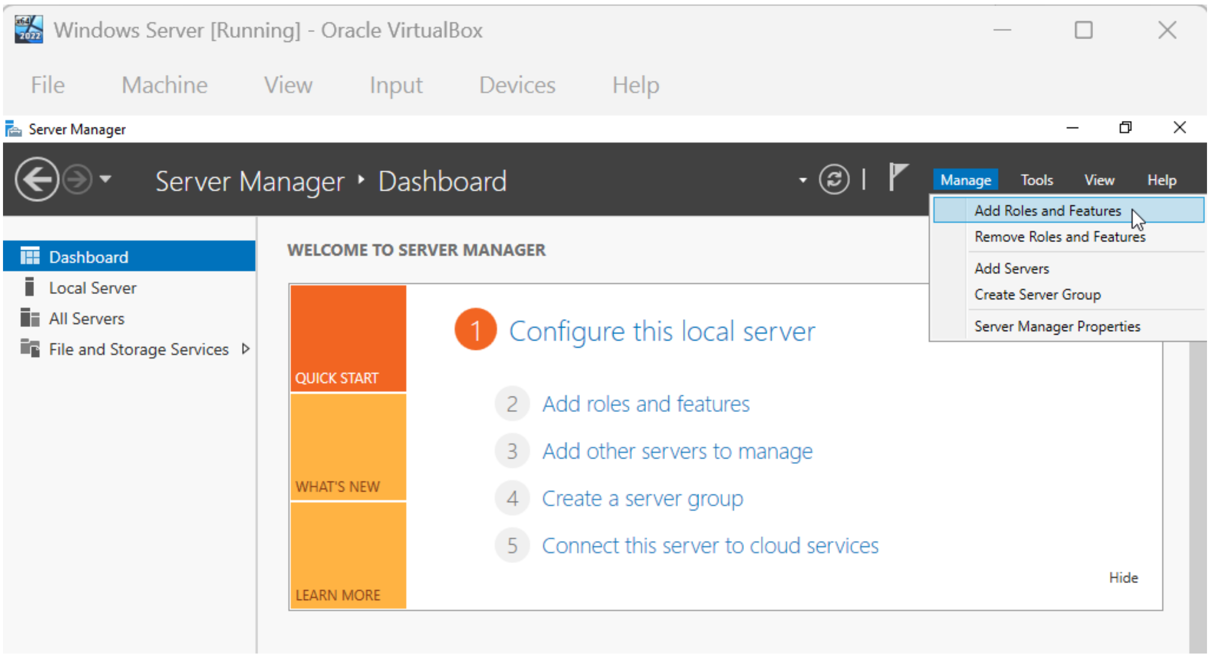
- Windows Server 2022
- Active Directory Domain Services installed.
- Domain Name example: SOA Enterprises

Tools

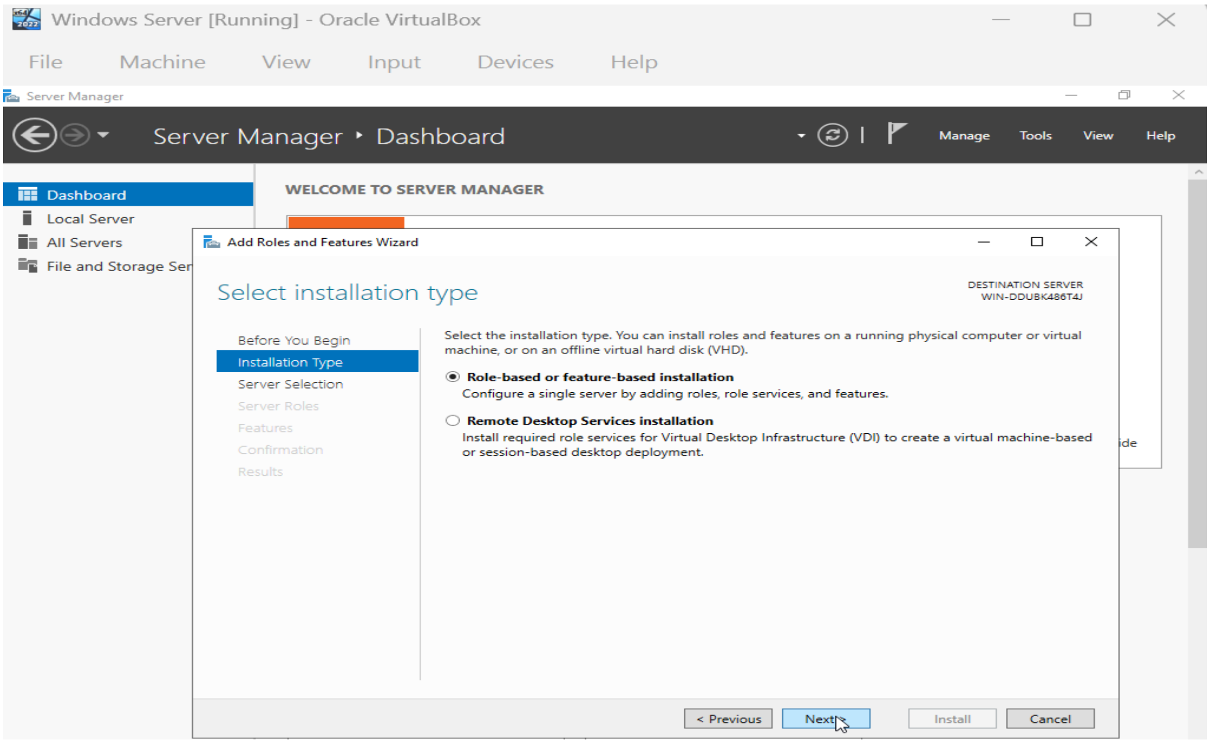
- Active Directory Users and Computers (ADUC)
- Domain Admin credentials

1. Installing Active Directory Domain services on Windows Server

Step 1) Open the Server Manager application and select 'Add Roles and Features' under the Manage tab.


Windows Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
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
Hide

Step 2) Select 'Role-based or feature-based installation' for installation type. This configures the server by adding roles, features and services and click 'Next.'

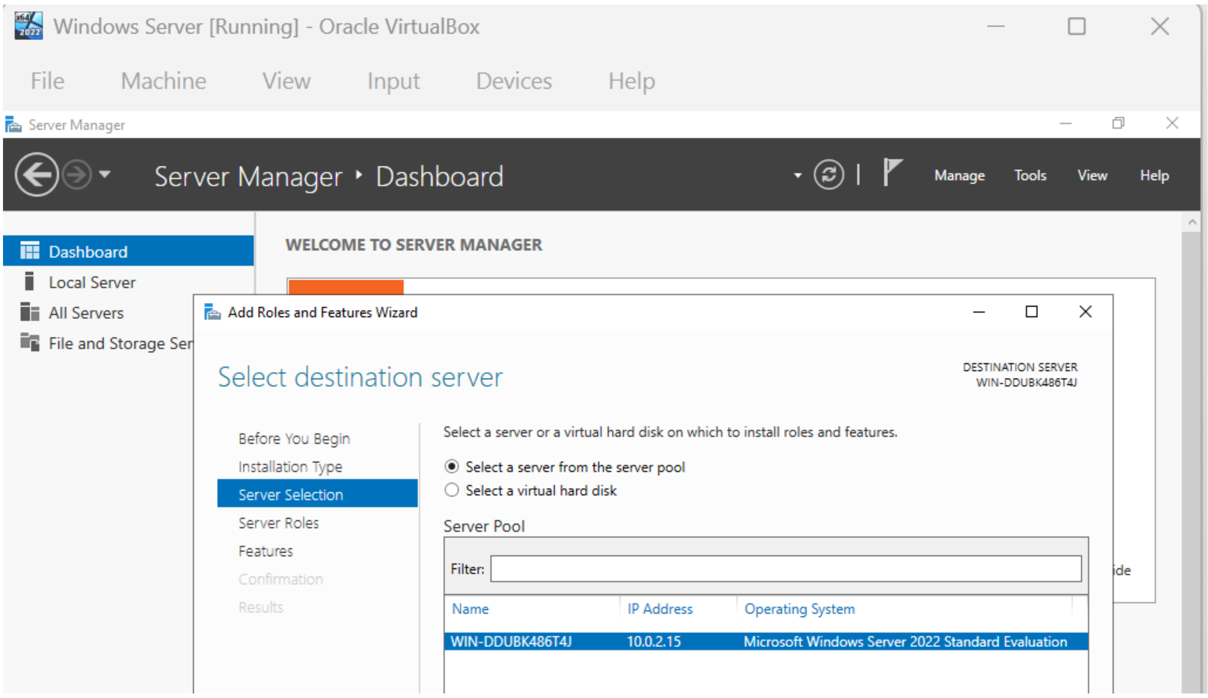


Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **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.

Step 3) Select the destination server from the server pool on which to install the roles and features.


Windows Server [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
ide
Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WIN-DDUBK486T4J

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.

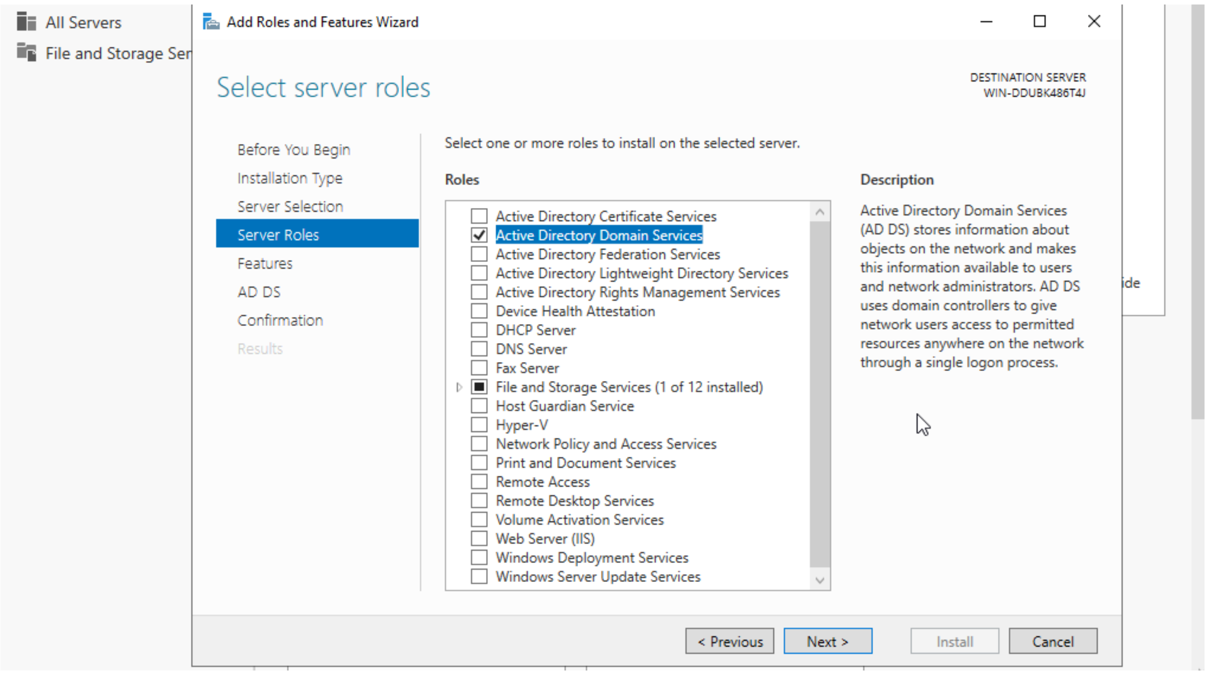
● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
WIN-DDUBK486T4J	10.0.2.15	Microsoft Windows Server 2022 Standard Evaluation

Step 4) Select 'Active Directory Domain Services' for server roles to ensure that the Active Directory role has been installed on the server. Add the services and features that are required for the Active Directory Domain Services role.



Select server roles

DESTINATION SERVER
WIN-DDUBK486T4J

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

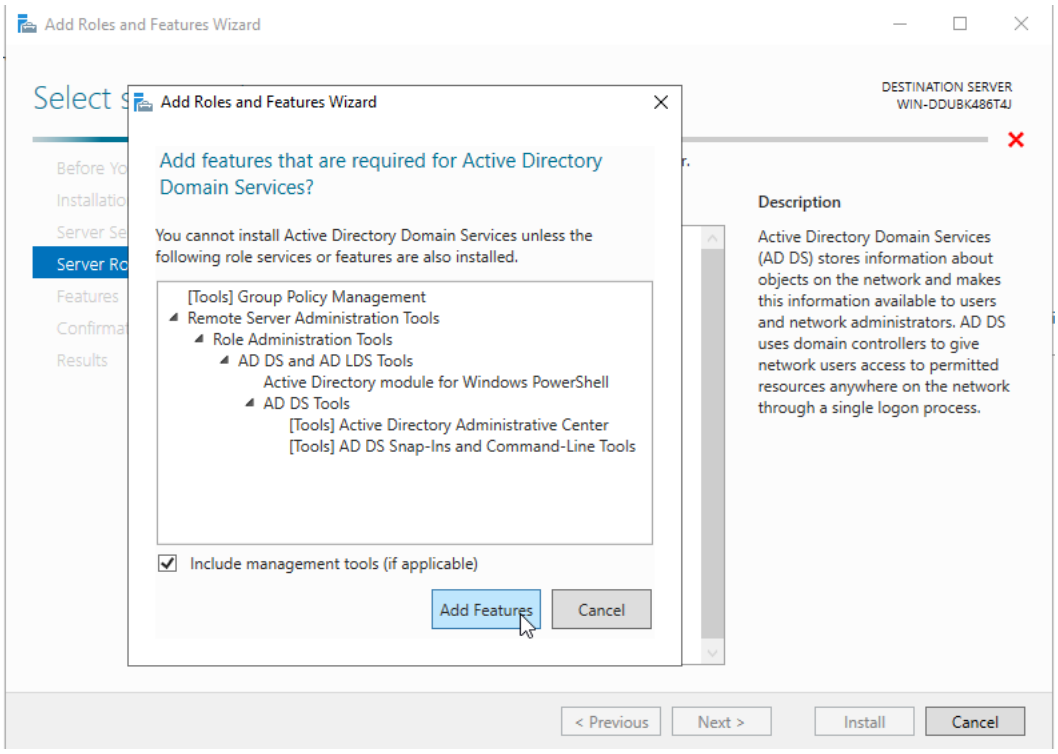
Select one or more roles to install on the selected server.

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 Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update 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.



Add Roles and Features Wizard

Add features that are required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the following role services or features are also installed.

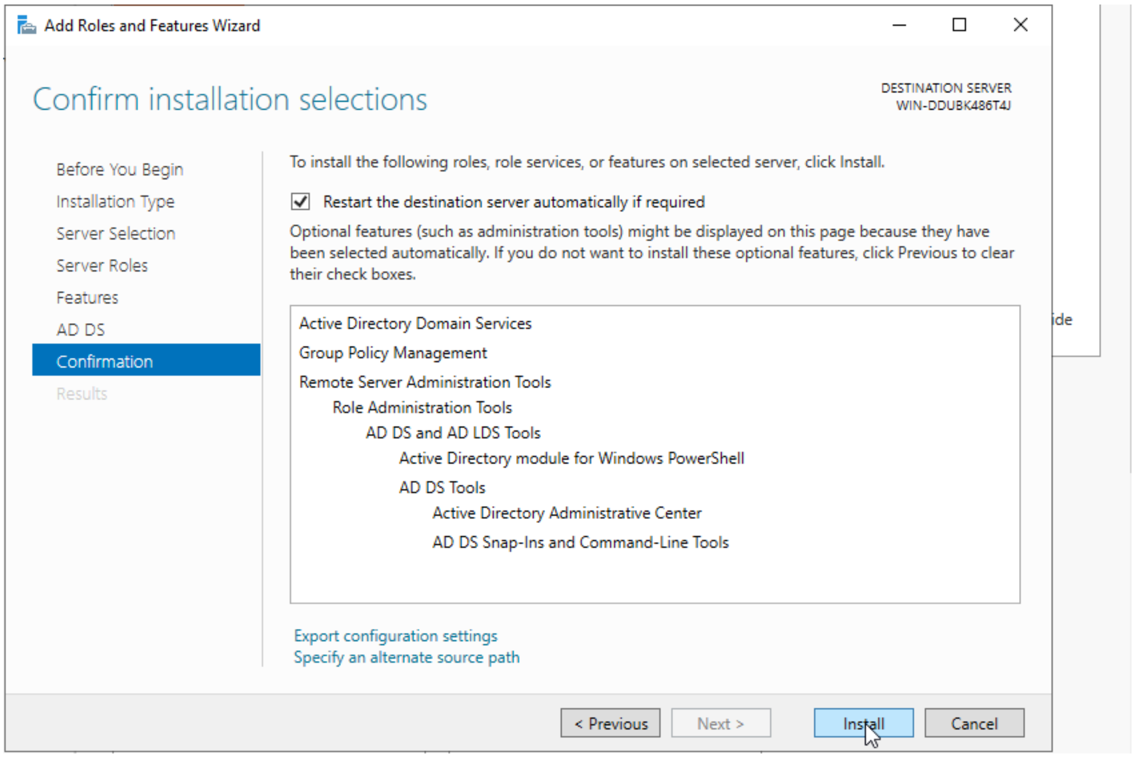
[Tools] Group Policy Management
◢ Remote Server Administration Tools
  ◢ Role Administration Tools
    ◢ AD DS and AD LDS Tools
      Active Directory module for Windows PowerShell
      ◢ AD DS Tools
        [Tools] Active Directory Administrative Center
        [Tools] AD DS Snap-Ins and Command-Line Tools

☑ Include management tools (if applicable)

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.

Step 5) Confirm the selected roles and services and click 'install'. This will restart the destination server.



Confirm installation selections

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

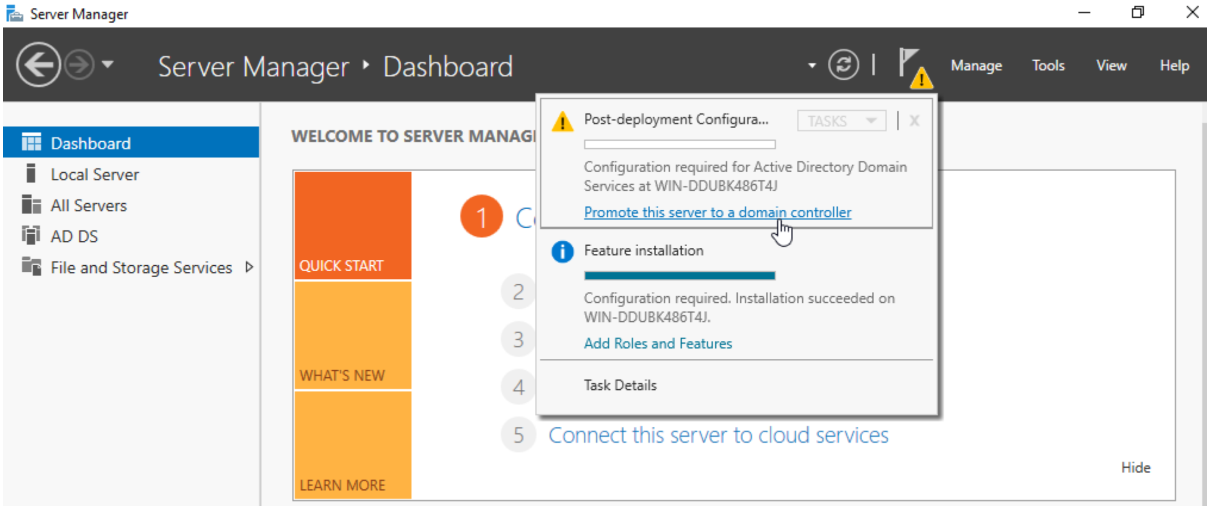
☑ Restart the destination server automatically if required

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
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

Step 6) Click on 'Promote this server to a domain controller' under Post-deployment Configuration. This will create the domain controller from the destination server.



Server Manager

Server Manager ‣ Dashboard

Post-deployment Configura...

Configuration required for Active Directory Domain Services at WIN-DDUBK486T4J

Promote this server to a domain controller

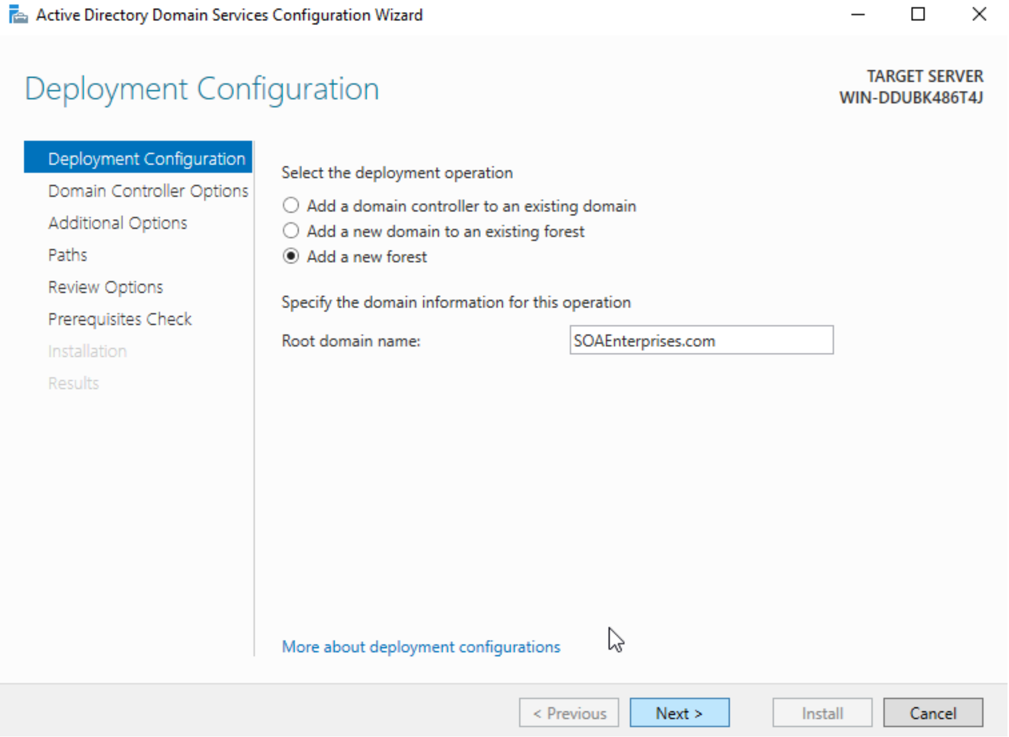
Feature installation

Configuration required. Installation succeeded on WIN-DDUBK486T4J.

Add Roles and Features

Task Details

Step 7) Select 'Add a new forest' under deployment configuration and the root domain name as 'SOAEnterprises.com'. This promotes the server to the first domain controller and creates the first domain and forest root.



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WIN-DDUBK486T4J

Select the deployment operation

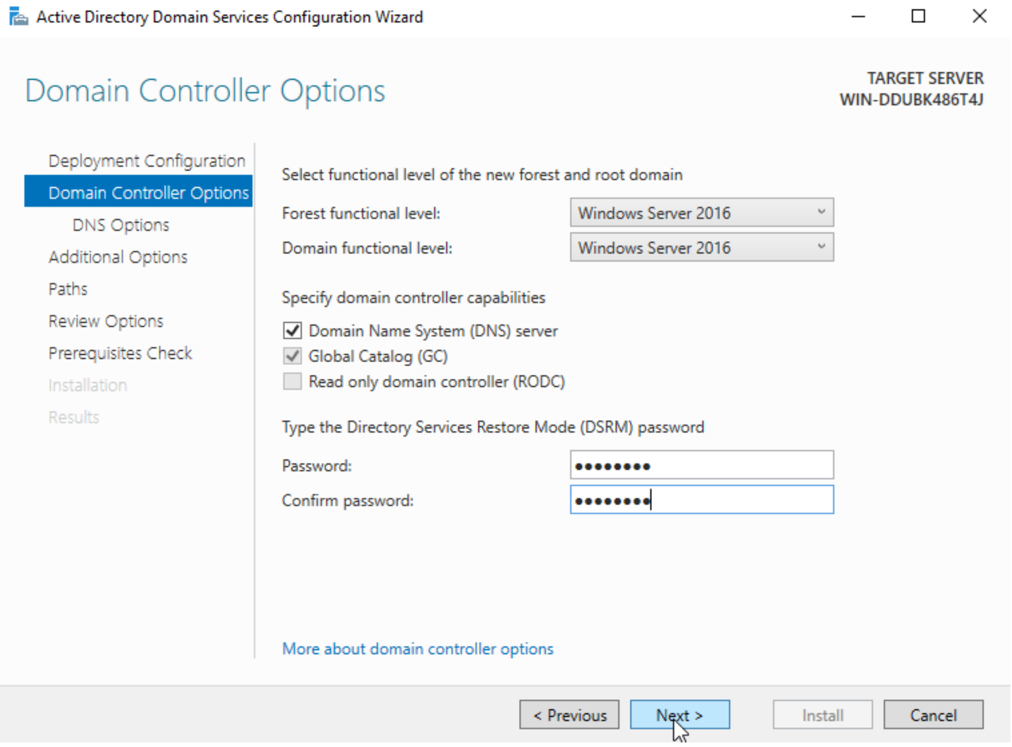
○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

Specify the domain information for this operation

Root domain name: SOAEnterprises.com

More about deployment configurations

Step 8) Enter the password for Directory Services Restore Mode (DSRM) under domain controller options.



Domain Controller Options

TARGET SERVER
WIN-DDUBK486T4J

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

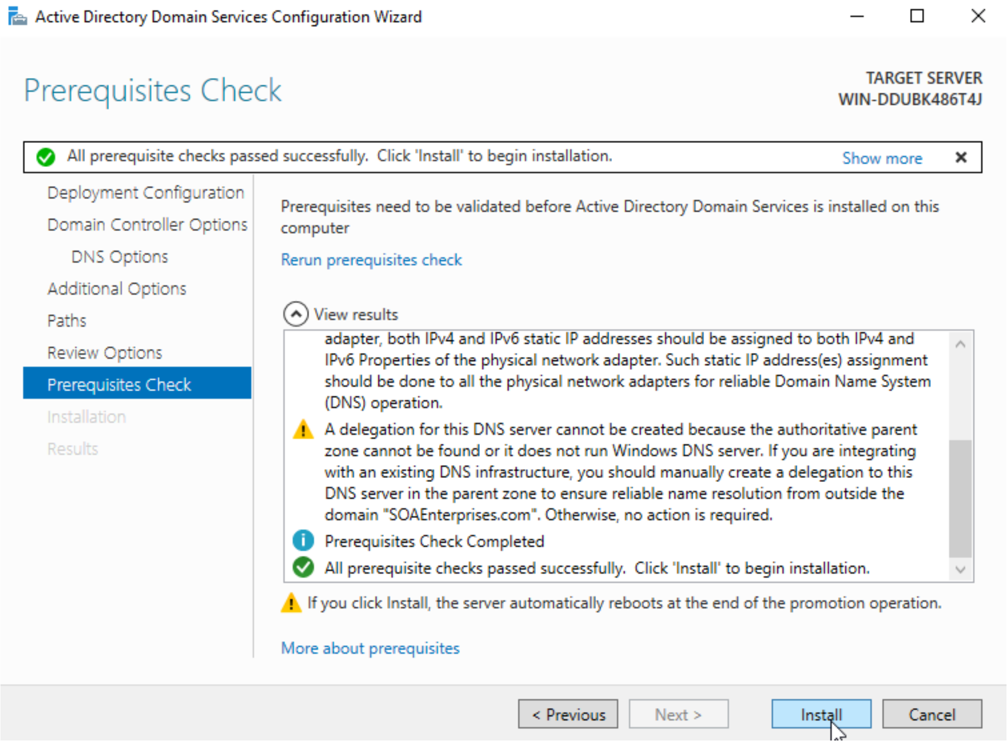
Type the Directory Services Restore Mode (DSRM) password

Password: ••••••••

Confirm password: ••••••••

More about domain controller options

Step 9) Click the ‘install’ button to start the installation once the pre-requisite check has been completed.



Prerequisites Check

TARGET SERVER
WIN-DDUBK486T4J

✓ 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

Rerun prerequisites check

View results

adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

⚠ 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 "SOAEnterprises.com". Otherwise, no action is required.

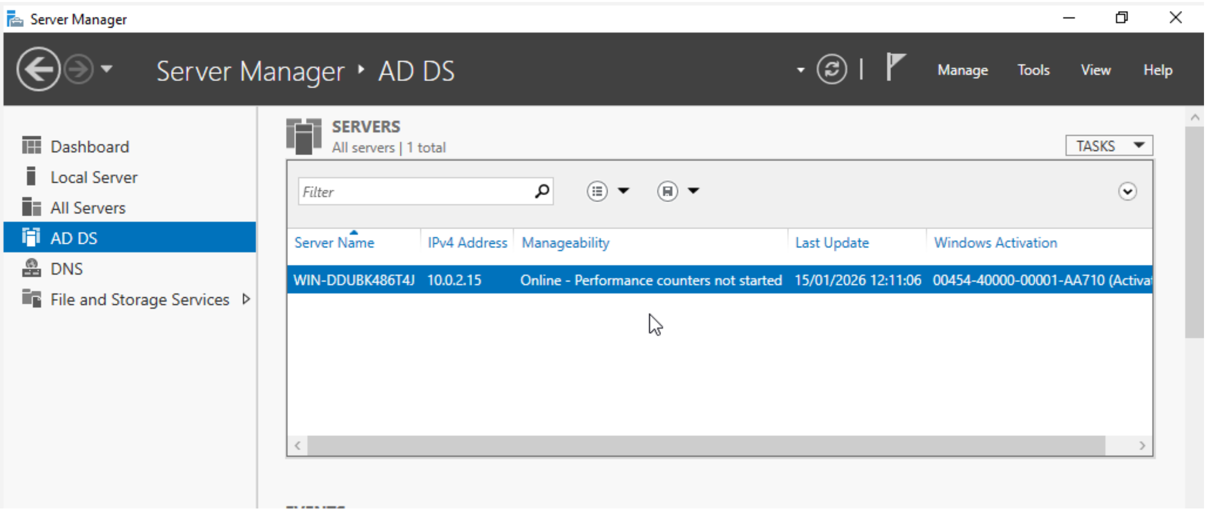
ℹ Prerequisites Check Completed

✓ 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.

More about prerequisites

Step 10) Through navigating to the Server Manager dashboard, this confirms that Active Directory Domain Services has been installed and the destination server has been promoted to domain controlled.



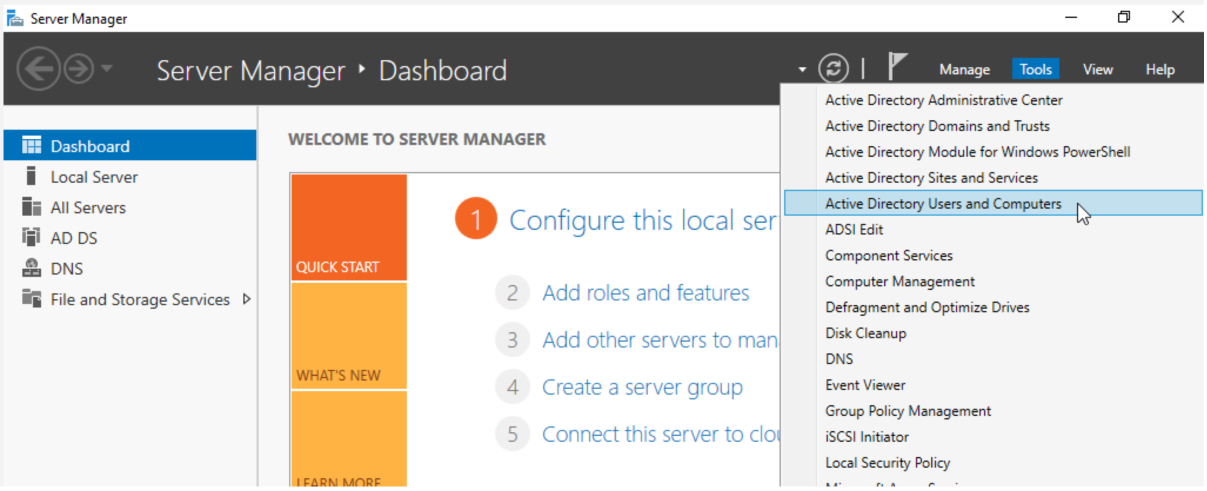
Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-DDUBK486T4J	10.0.2.15	Online - Performance counters not started	15/01/2026 12:11:06	00454-40000-00001-AA710 (Activa

Expected Outcome:

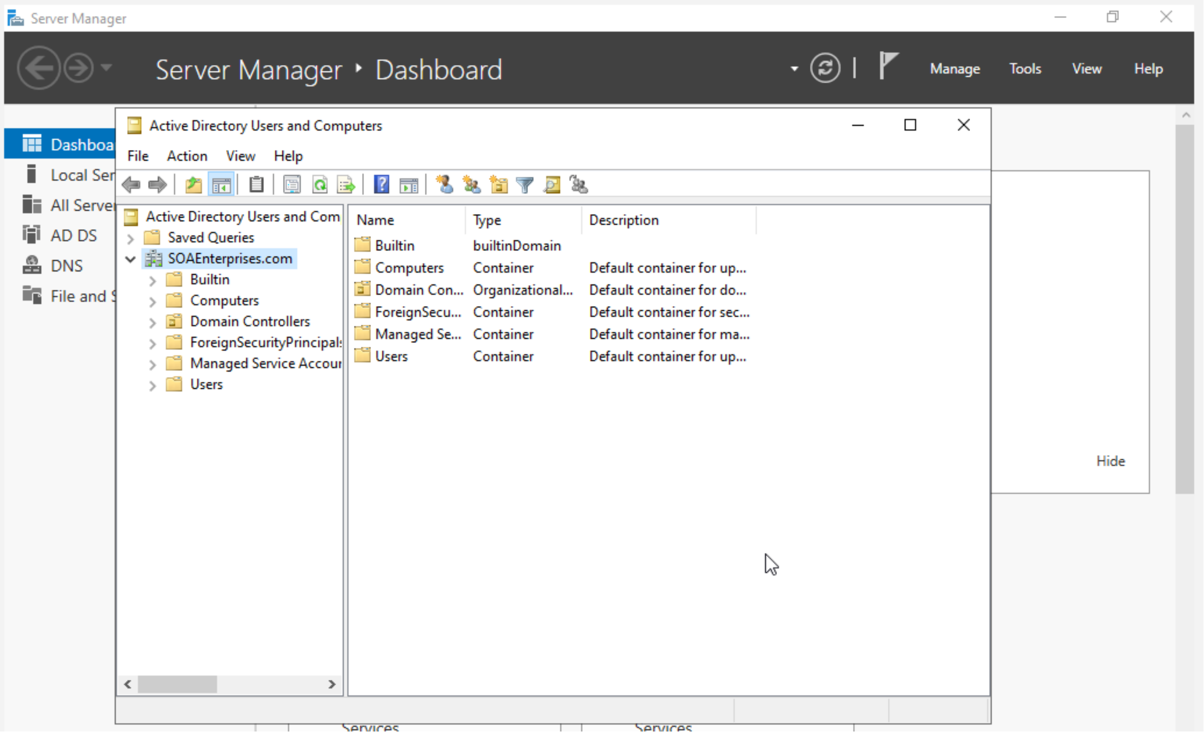
The Active Directory Domain Services role has been installed on the server, and the server has been promoted to domain controller. The first domain and forest have been created for SOA Enterprises.

2. Exploring Active Directory Structure

Step 1) Open Server Manager and click ‘Active Directory Users and Computers’ under the tools tab.

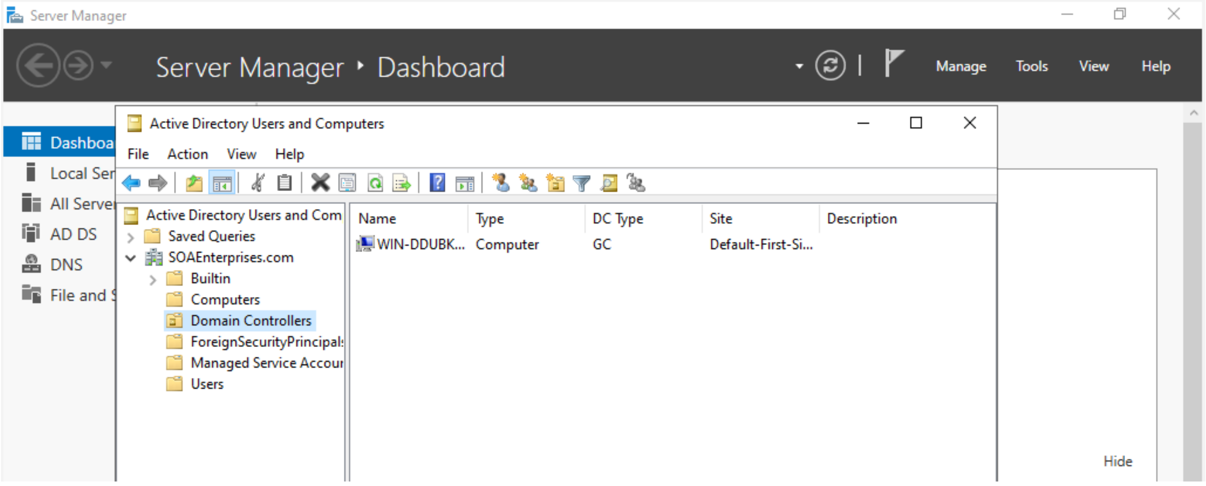

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local ser
2 Add roles and features
3 Add other servers to man
4 Create a server group
5 Connect this server to clo
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
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy

Step 2) Expand the domain ‘SOAEnterprises.com’ to view the default containers. There are multiple containers within the domain, including computers, domain controllers, managed service accounts and users.



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

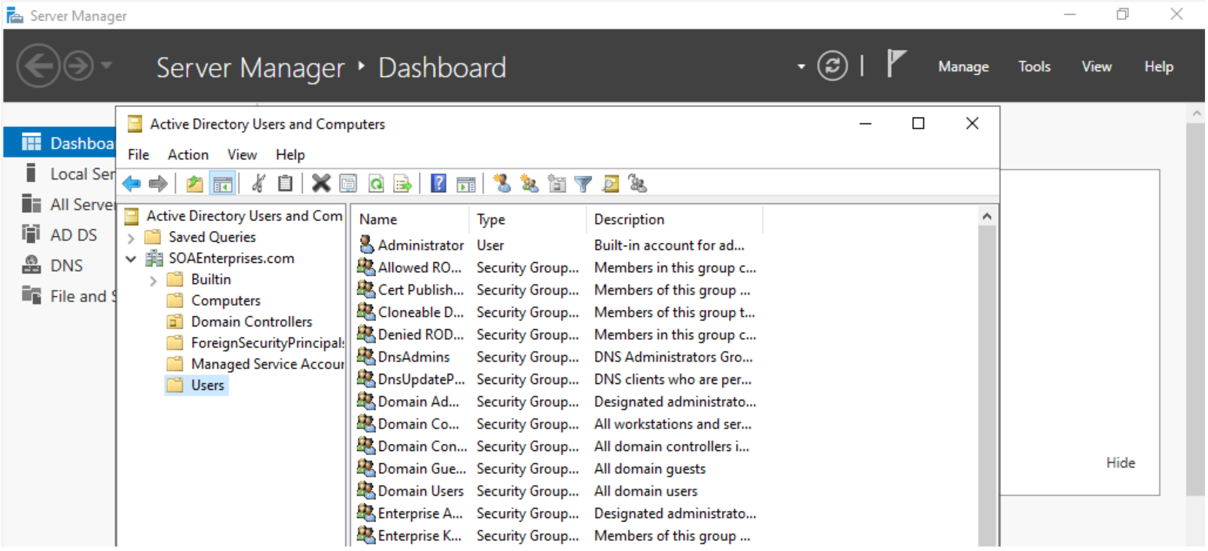
Step 3) The domain controllers container shows one domain controller which is the server that was recently promoted.



- Active Directory Users and Com
  - Saved Queries
  - SOAEnterprises.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Managed Service Accour
    - Users

Name	Type	DC Type	Site	Description
WIN-DDUBK...	Computer	GC	Default-First-Si...	

Step 4) The users container shows all the default users that were created and their assigned groups.



- Active Directory Users and Com
  - Saved Queries
  - SOAEnterprises.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Managed Service Accour
    - Users

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...
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 ...

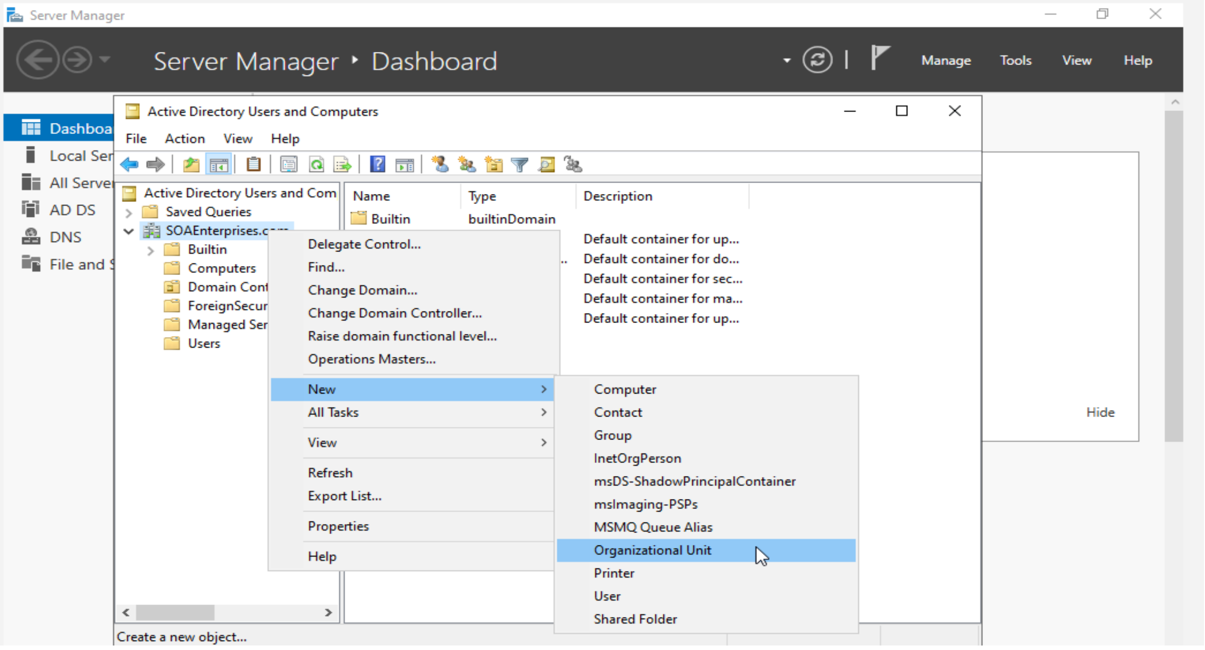
Expected Outcome:

The Active Directory Users and Computers tab has been successfully explored and can understand where information about users, computers and domain controllers can be located.

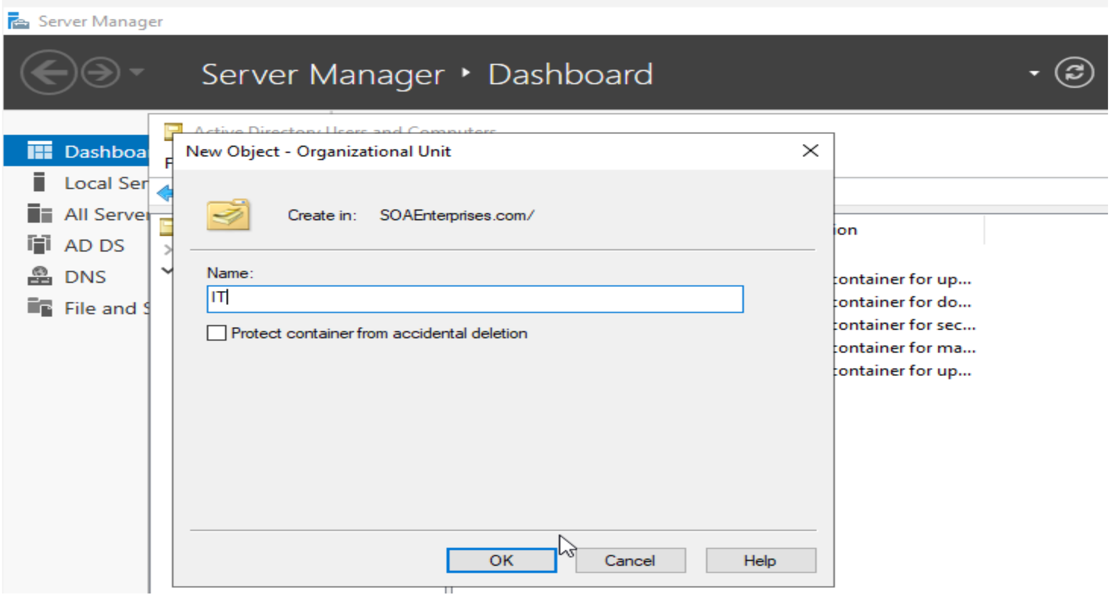
3. Creating Organisational Units within a Domain

SOA Enterprises wants to organise their users by departments. For this exercise, the organisational units will be created for three departments, including IT, HR and Marketing.

Step 1) Navigate to Active Directory Users and Computers and right-click on the 'SOAEnterprise.com' domain and select 'New > Organisational Unit.'



Step 2) Enter the name of the Organisational Unit as 'IT' and click the 'OK.' Repeat this step for the HR and Marketing departments.

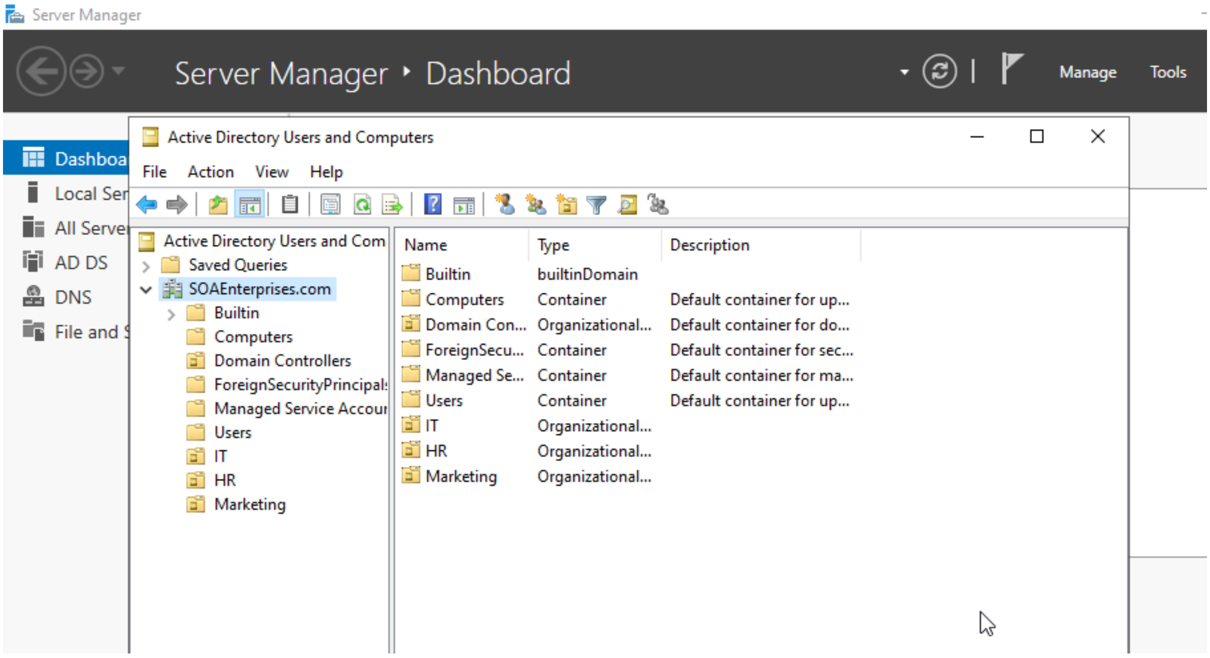


Create in: SOAEnterprises.com/

Name: IT

□ Protect container from accidental deletion

Step 3) The organizational units have been created for IT, HR and Marketing departments and can be viewed in the SOA Enterprises domain.



Active Directory Users and Com
- Saved Queries
- SOAEnterprises.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal:
  - Managed Service Accour
  - Users
  - IT
  - HR
  - Marketing

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...
IT	Organizational...	
HR	Organizational...	
Marketing	Organizational...	

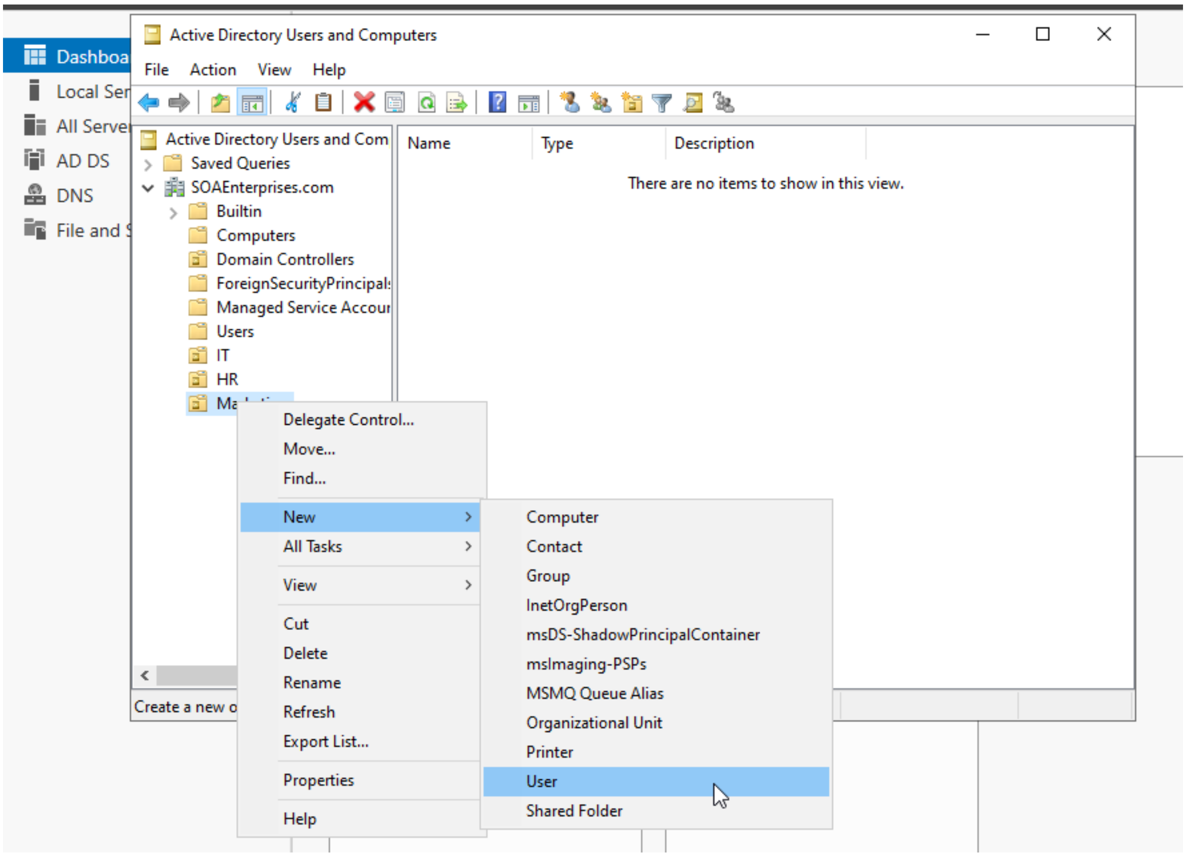
Expected Outcome:

The organizational units have successfully been created for the IT, HR and Marketing departments. This creates a clean organizational unit structure for user management.

4. Creating a New User Account

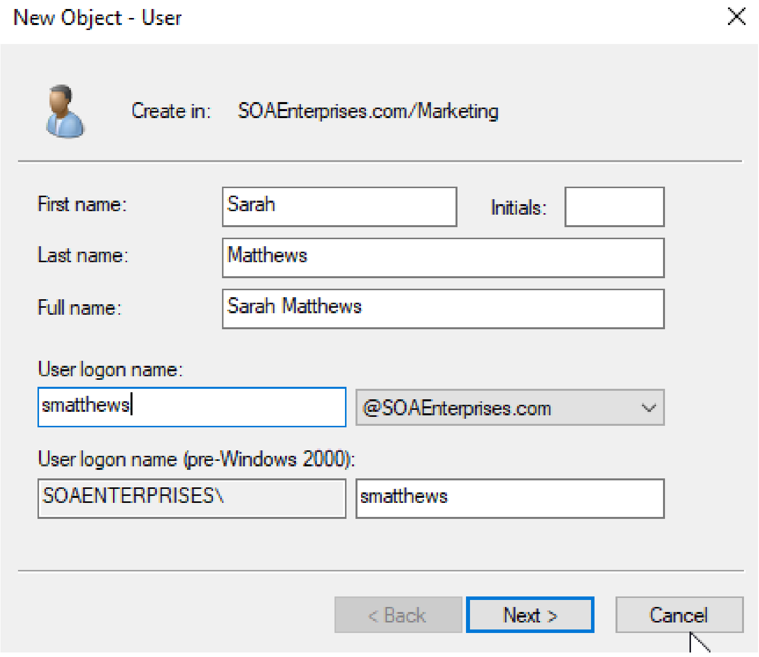
A new employee, Sarah has joined the marketing department within SOA Enterprises. This exercise will demonstrate how to create a new user account within the marketing organizational unit.

Step 1) Right-click on the 'Marketing' organisational unit and select 'New > User.'



Step 2) Enter the following details for the new user and click ‘next’:

- First name: Sarah
- Last name: Matthews
- Username: smatthews



New Object - User

Create in: SOAEnterprises.com/Marketing

First name: Sarah

Initials:

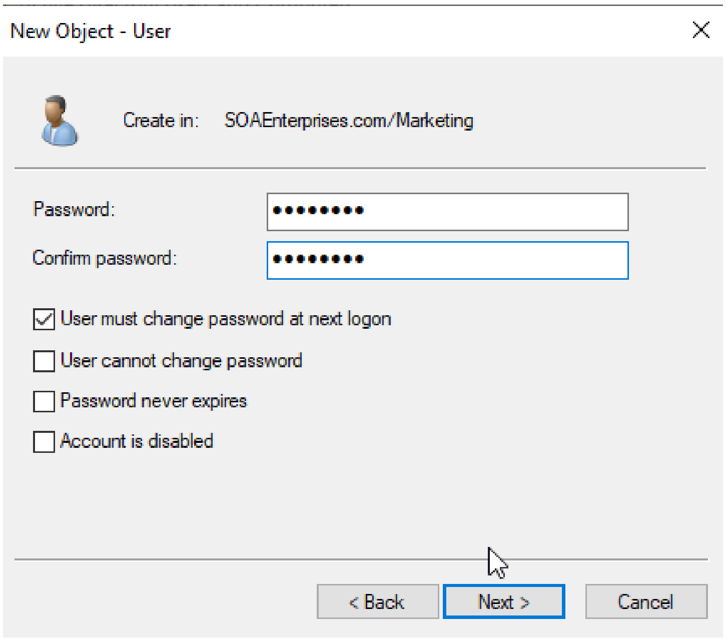
Last name: Matthews

Full name: Sarah Matthews

User logon name: smatthews @SOAEnterprises.com

User logon name (pre-Windows 2000): SOAENTERPRISES\ smatthews

Step 3) Create a password for the new user and check ‘User must change password at next logon.’ This allows the user to change their password once logged in.



New Object - User

Create in: SOAEnterprises.com/Marketing

Password: ••••••••

Confirm password: ••••••••

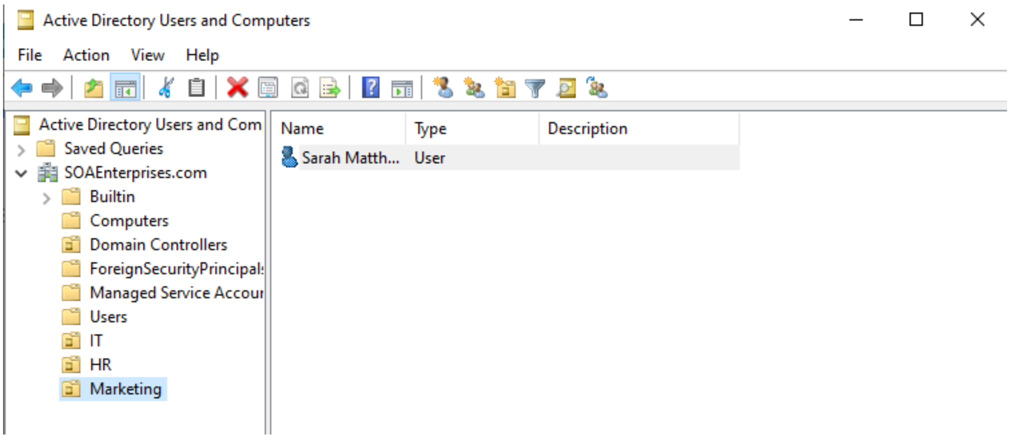
☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

Step 4) This confirms that a new user, Sarah Mattthews has been created and added to the Marketing department.



Name	Type	Description
Sarah Matth...	User	

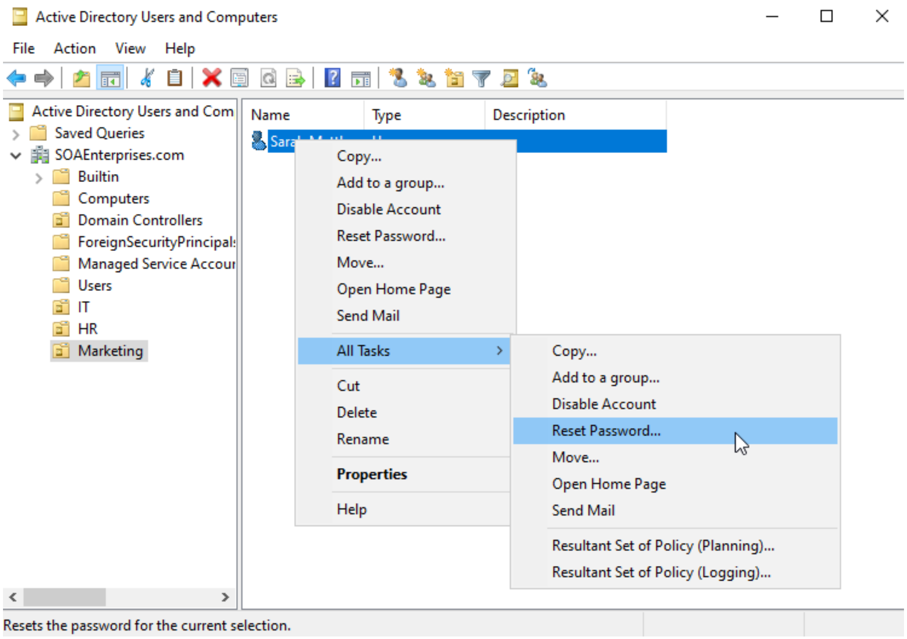
Expected Outcome:

The user account for the new employee has been successfully created and added to the marketing department.

5. Resetting a User's Password

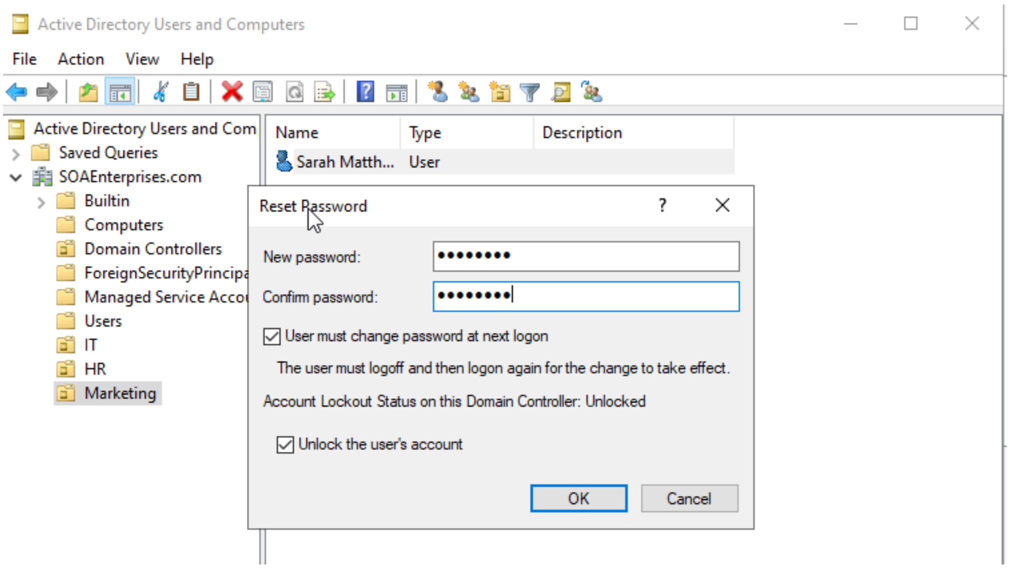
An employee from the marketing department, Sarah Mattehews has submitted a support request to the helpdesk to reset her password. This exercise will demonstrate how to reset a users' password within Active Directory.

Step 1) Right-click on 'smatthews' and select 'Reset Password' under the 'All Tasks' option.



Resets the password for the current selection.

Step 2) Set a temporary password and Check ‘User must change password at next logon.’



Reset Password

New password: ••••••••

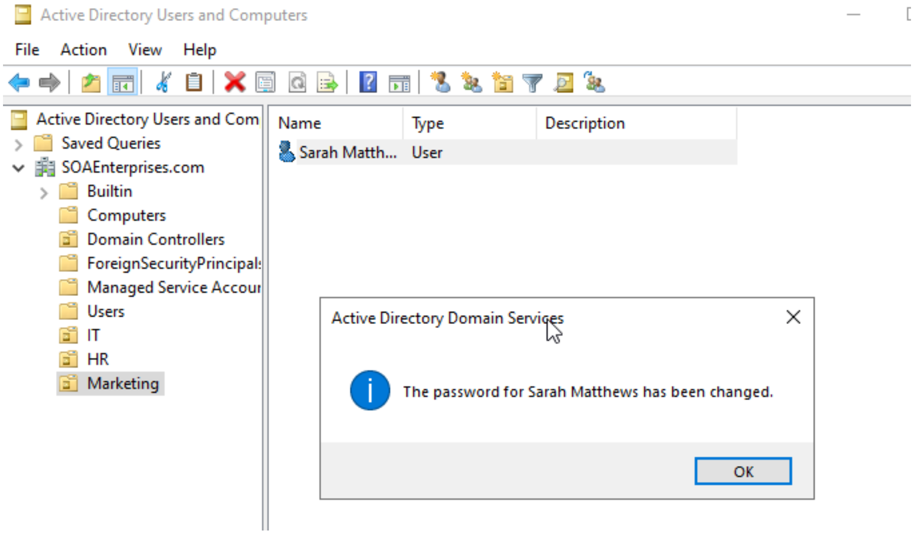
Confirm password: ••••••••

☑ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

Account Lockout Status on this Domain Controller: Unlocked

☑ Unlock the user's account



Active Directory Domain Services

The password for Sarah Matthews has been changed.

An email was sent to Sarah Matthews following the password reset to notify her of the temporary password.

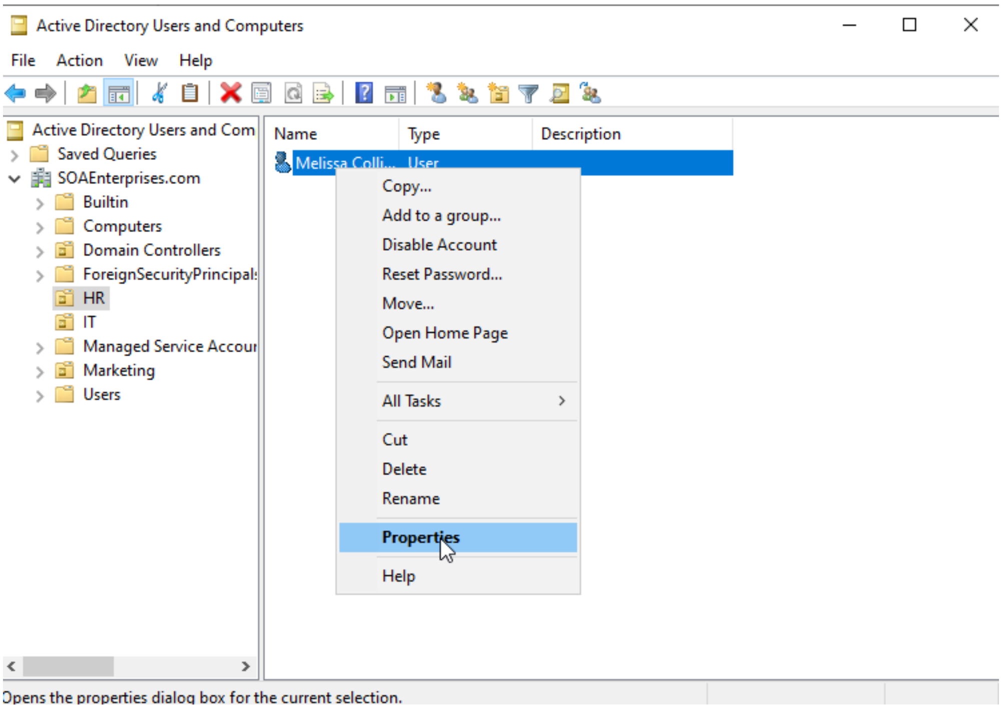
Expected Outcome:

The user’s password was successfully reset in Active Directory, and the user is able to login and reset the password.

6. Unlocking a Locked Account

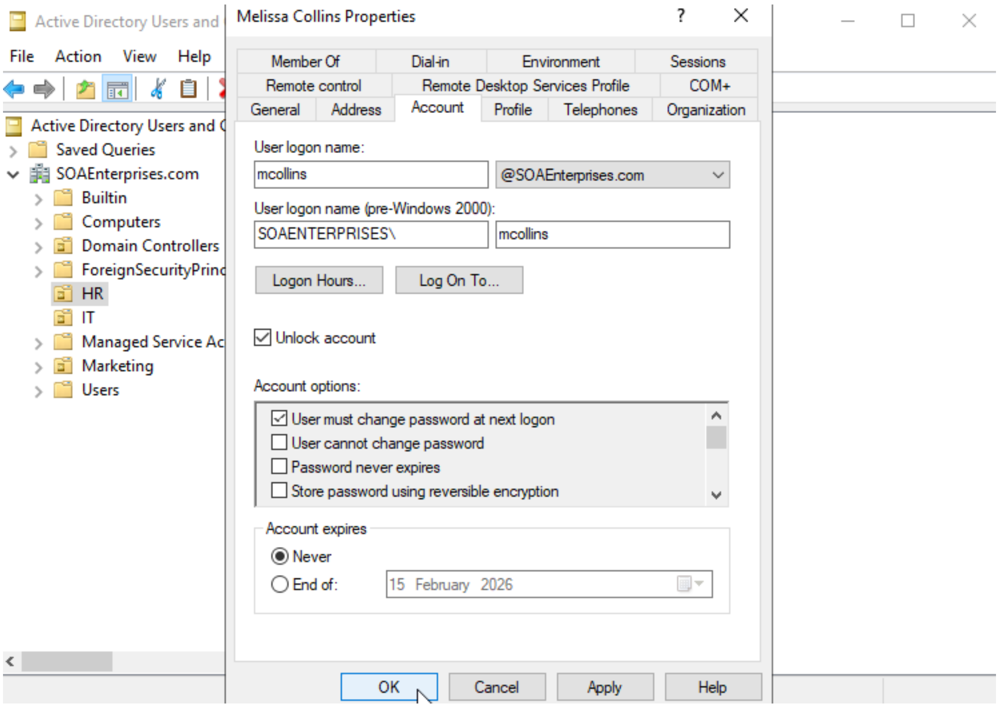
An employee from the HR department, Melissa Collins has entered the incorrect password too many times and has been locked out of their user account. This exercise will show how to unlock a user's account.

Step 1) Right-click on 'mcollins' and select 'Properties.'



Opens the properties dialog box for the current selection.

Step 2) In properties select the 'Account' tab and check 'Unlock Account' and click 'OK.'



User logon name:
mcollins @SOAEnterprises.com

User logon name (pre-Windows 2000):
SOAENTERPRISES\ mcollins

☑ Unlock account

Account options:
☑ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Store password using reversible encryption

Account expires
● Never
○ End of: 15 February 2026

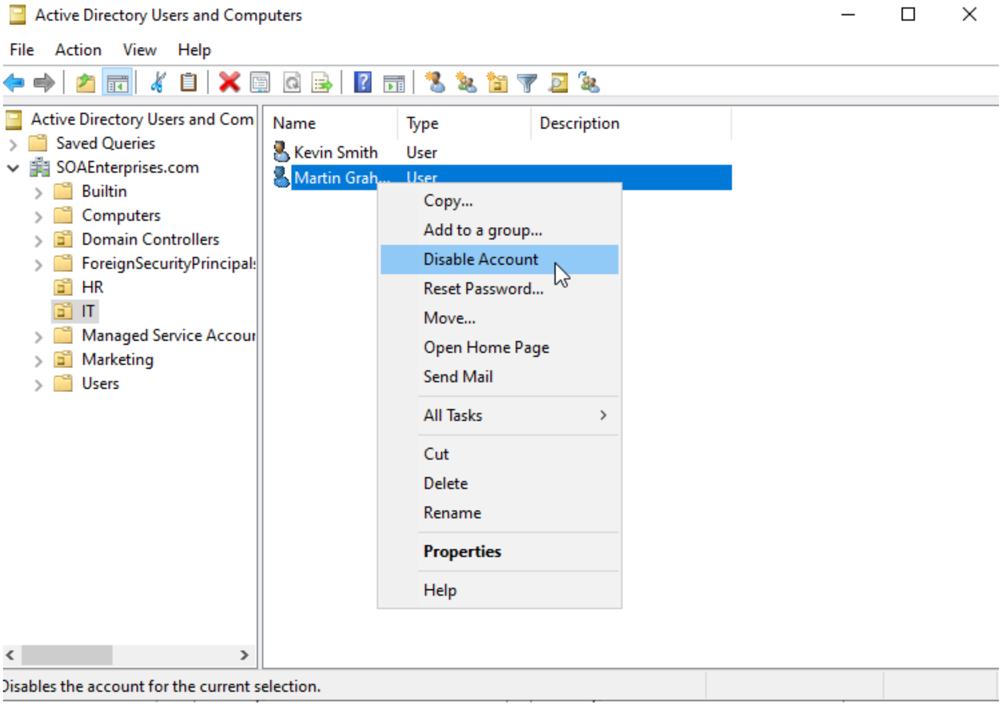
Expected Outcome:

Melissa Collins was able to login into her user account and change her password at the next logon.

7. Disable and Enable a User Account

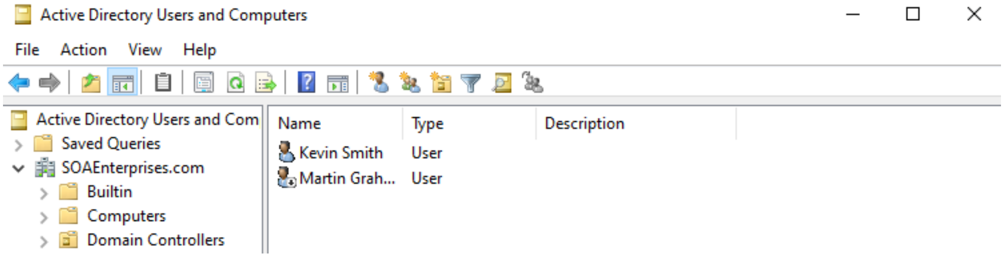
An employee from the IT department, Martin Graham retires from SOA Enterprises and would need his user account disabled. This exercise will show to disable and enable user accounts from Active Directory.

Step 1) Right-click on 'Martin Graham' and select 'Disable Account.'

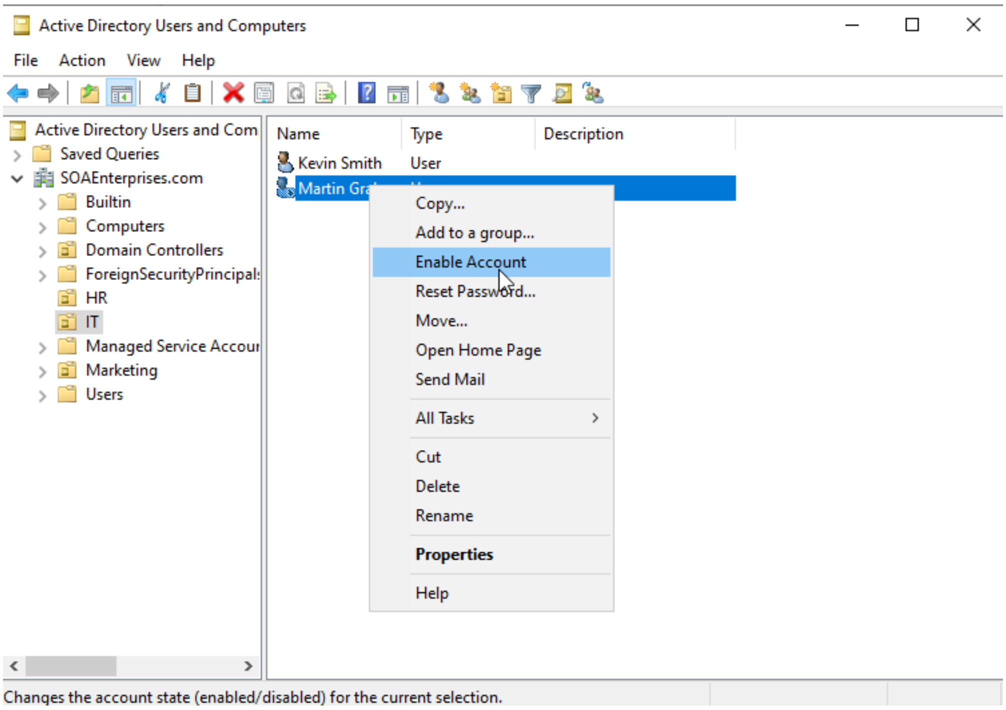


Disables the account for the current selection.

Step 2) The icon next to the user's name 'Martin Graham' has changed to indicate the account has been disabled.

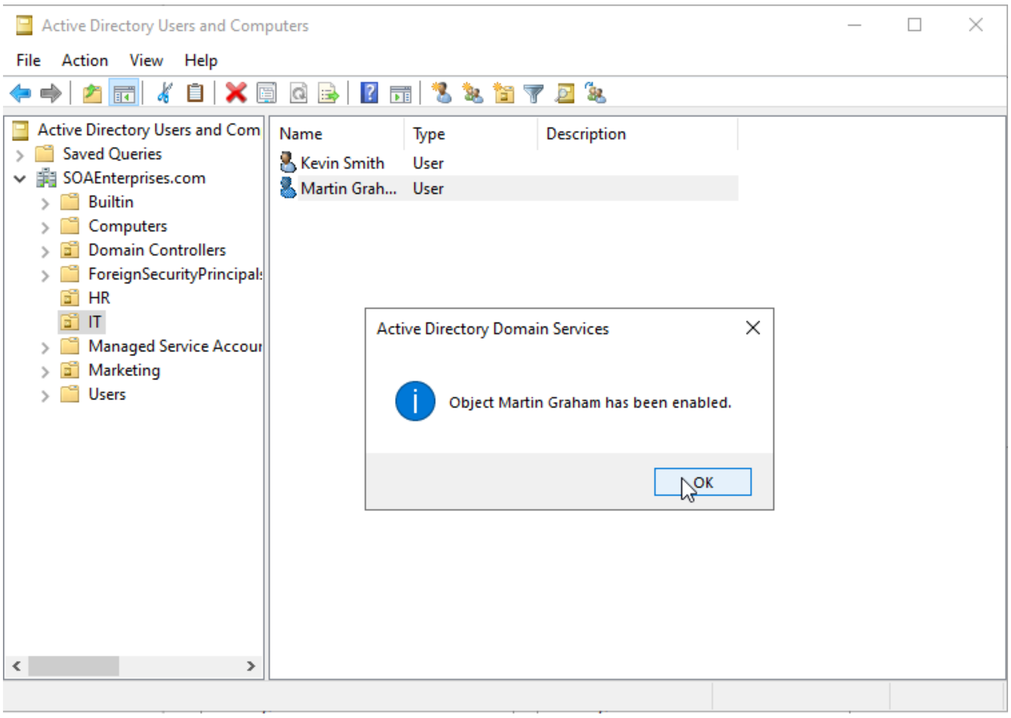


Step 3) To enable the user account after disabling it, right click on the user and select ‘Enable Account.’



Changes the account state (enabled/disabled) for the current selection.

Step 4) The user has been enabled once again, and the icon has been changed.



Active Directory Domain Services

Object Martin Graham has been enabled.

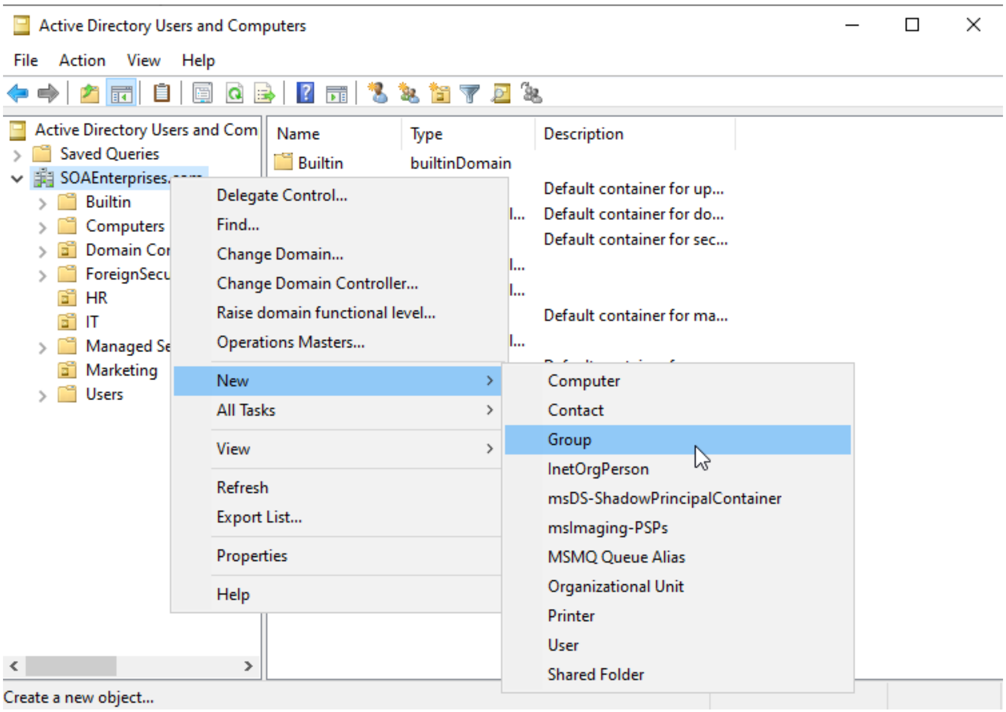
Expected Outcome:

The user account ‘Martin Graham’ was successfully disabled and re-enabled.

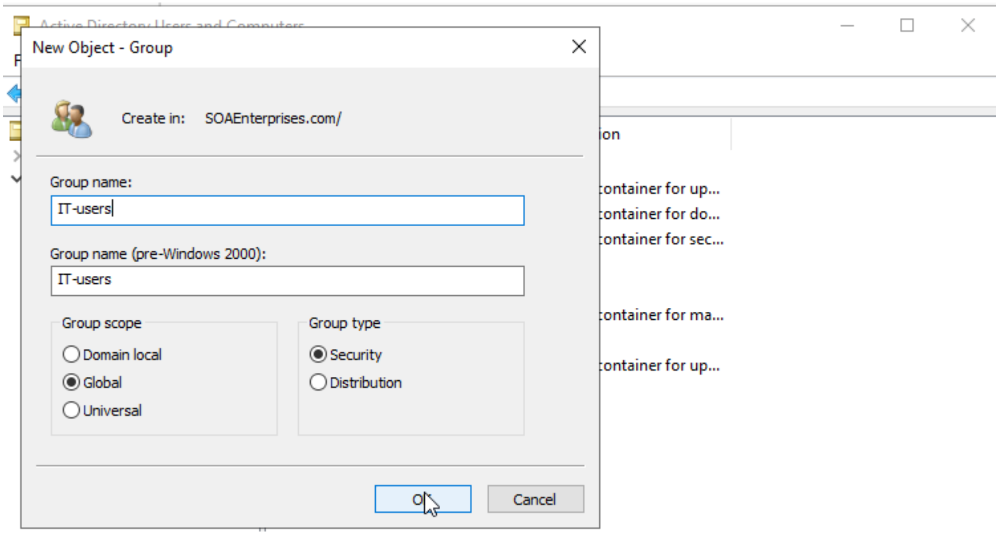
8. Group Membership Management

An employee from the HR department, Melissa Collins needs access to the IT shared folder. For this exercise, a security group called IT-users will be created and Melissa Collins will be added to the group.

Step 1) Right-click on 'SOAEnterprises' and select 'group' under the 'New' option.



Step 2) Create a new group called 'IT-users' and select 'Security' as the group type and 'Global' as the group scope.


New Object - Group

Create in: SOAEnterprises.com/

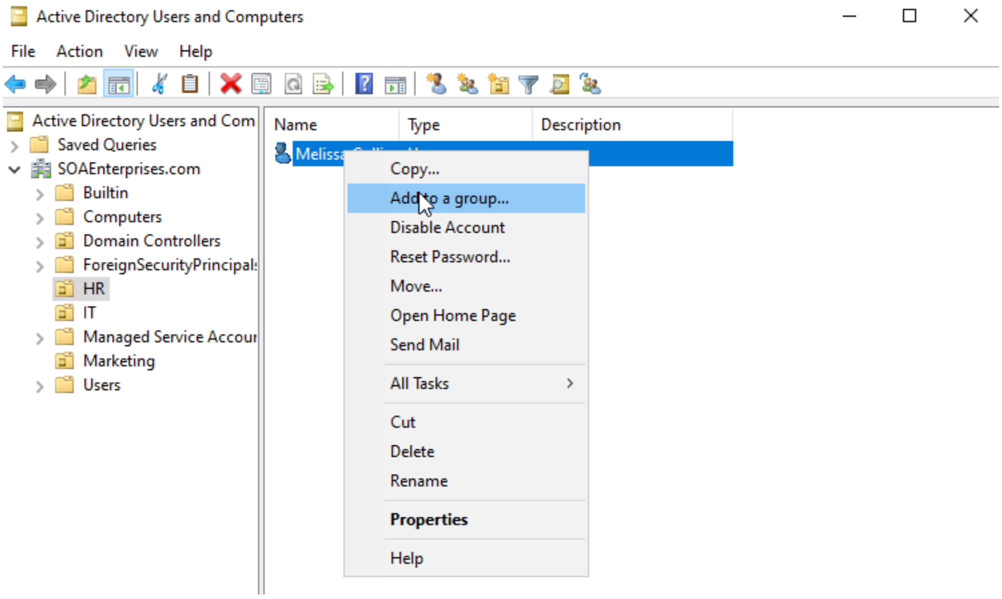
Group name: IT-users

Group name (pre-Windows 2000): IT-users

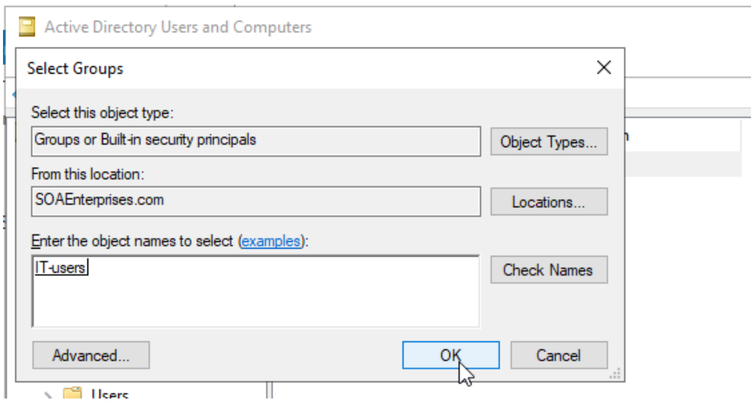
Group scope: ○ Domain local ● Global ○ Universal

Group type: ● Security ○ Distribution

Step 3) Right-click on ‘Melissa Collins’ and select ‘Add to a group.’



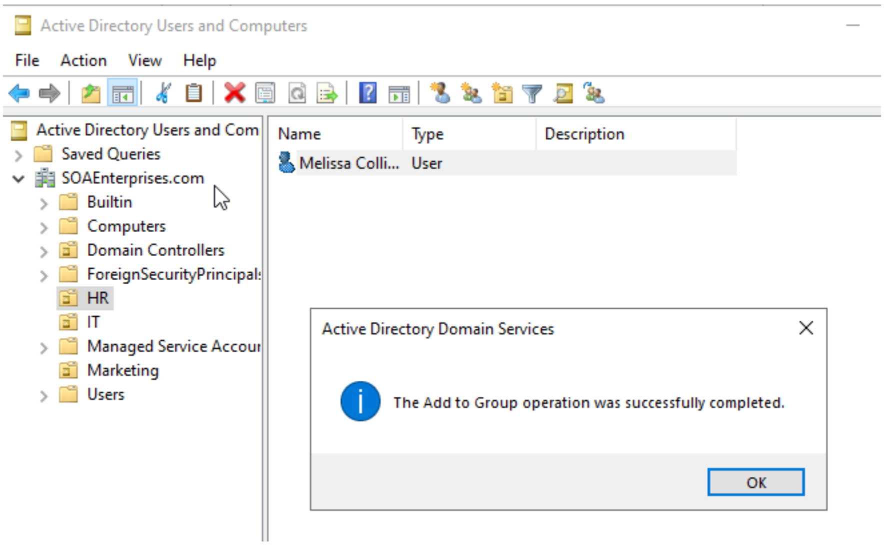
Step 4) Select the IT-users group by entering the group name into object names and click ‘OK.’



Select this object type:
Groups or Built-in security principals

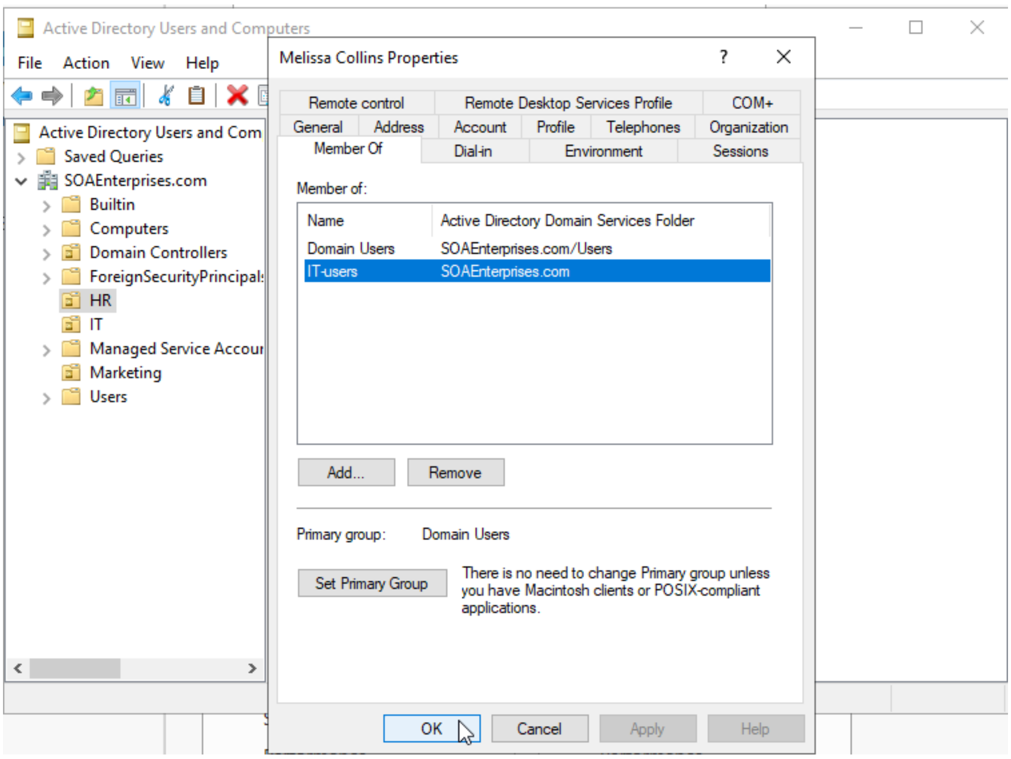
From this location:
SOAEnterprises.com

Enter the object names to select (examples):
IT-users



The Add to Group operation was successfully completed.

Step 5) Verify the user account has been added to the group by right clicking on Melissa Collins and selecting 'Properties.' Click on the 'Member of' tab to display the groups that the user is a member of. This confirms that the user account has been added to the IT-users group.



Member of:

Name	Active Directory Domain Services Folder
Domain Users	SOAEnterprises.com/Users
IT-users	SOAEnterprises.com

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

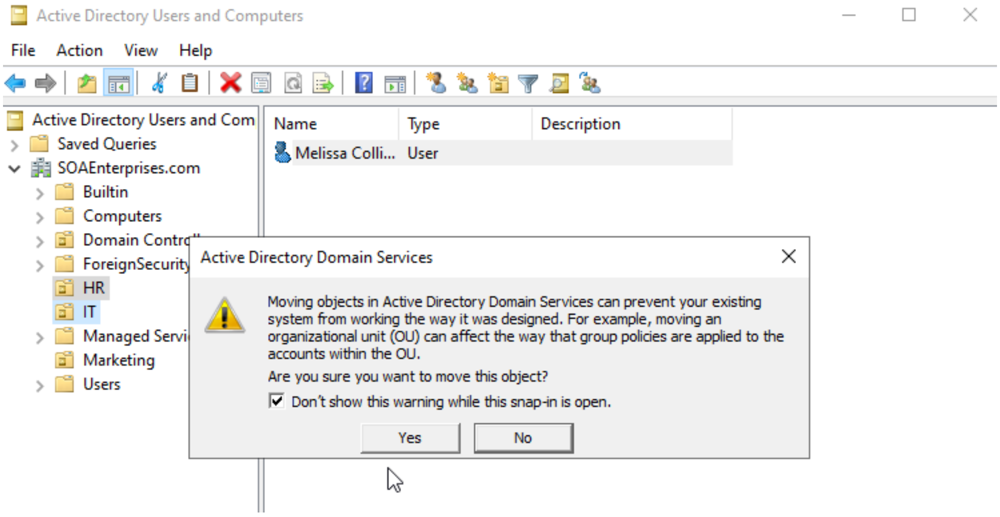
Expected Outcome:

The user account 'Melissa Collins' inherits permissions for the IT-users group via group membership.

9. Move Users between Organisational Units

An employee from the HR department, Melissa Collins has transferred to the IT department. This exercise will show how to manage this change by moving users from one organisation to another.

Step 1) Click on 'Melissa Collins' from the HR organisational unit to the IT organisational unit.



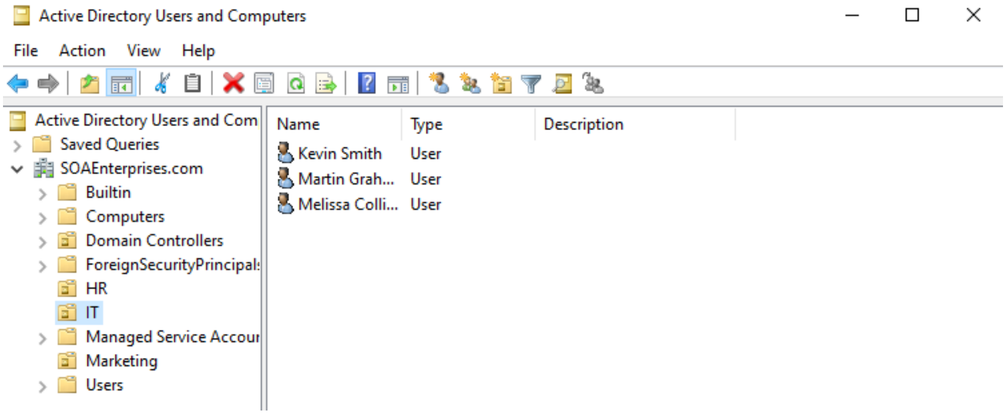
Active Directory Domain Services

Moving objects in Active Directory Domain Services can prevent your existing system from working the way it was designed. For example, moving an organizational unit (OU) can affect the way that group policies are applied to the accounts within the OU.

Are you sure you want to move this object?

☑ Don't show this warning while this snap-in is open.

Step 2) Confirm that Melissa Collins is now part of the IT organisational unit.



Name	Type	Description
Kevin Smith	User	
Martin Grah...	User	
Melissa Colli...	User	

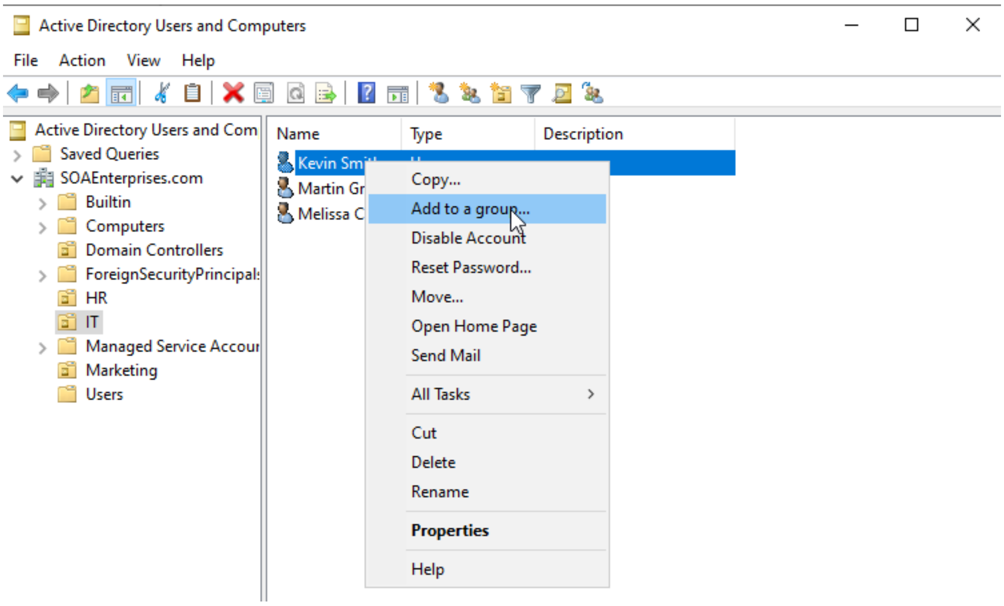
Expected Outcome:

The user account 'Melissa Collins' has moved from the HR to IT organisational unit and is now managed under the correct department.

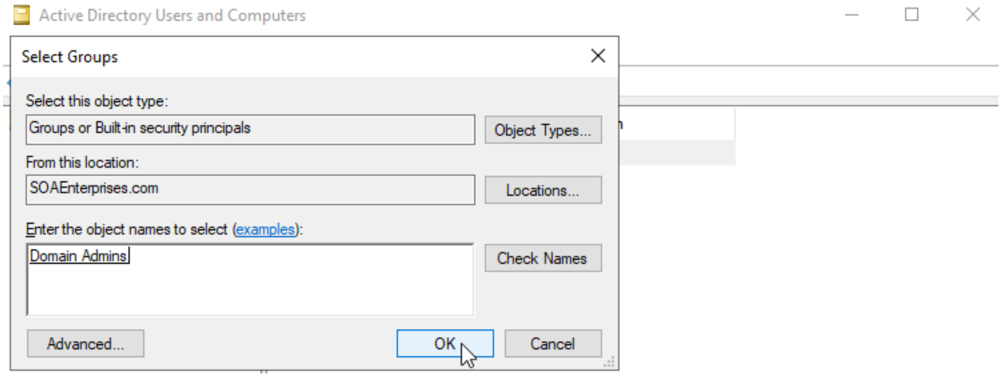
10. Troubleshooting Login Issues

An employee, Kevin Smith from the IT department want to access the Domain Controller but lacks the administrative privileges. This exercise will demonstrate how to resolve this issue by adding Kevin Smith to the Domain Admins group.

Step 1) Right-click on ‘Kevin Smith’ and select 'Add to a group.’



Step 2) Select the Domain Admins group by entering the groups name into object name and click ‘OK.’

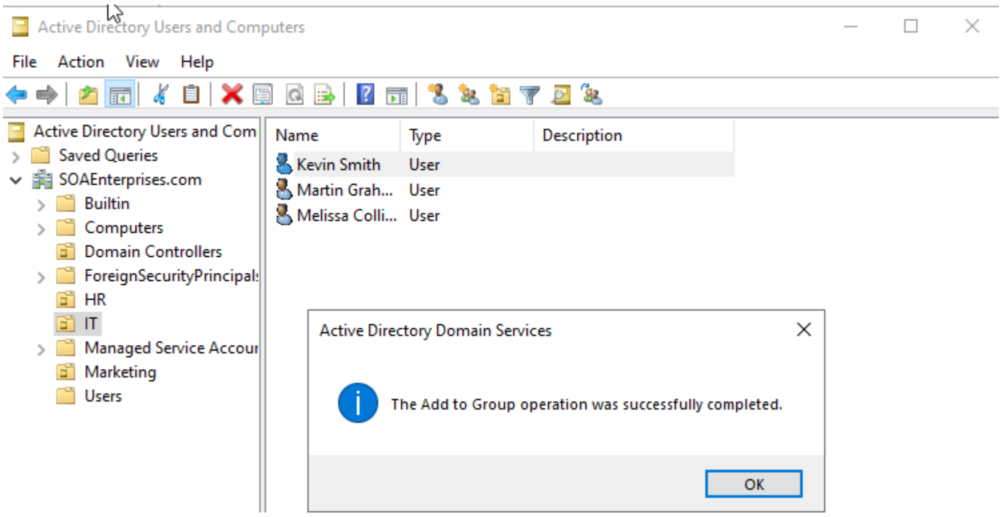


Select this object type:
Groups or Built-in security principals

From this location:
SOAEnterprises.com

Enter the object names to select (examples):
Domain Admins

Step 3) The user account 'Kevin Smith' from the IT department has successfully added to the Domain Admins group and can access the domain controller.



Name	Type	Description
Kevin Smith	User	
Martin Grah...	User	
Melissa Colli...	User	

Active Directory Domain Services

The Add to Group operation was successfully completed.

The group membership for the Domain Admins group should be assigned carefully and only to those with the necessary right and privileges to perform their job roles.