

Course-End Project

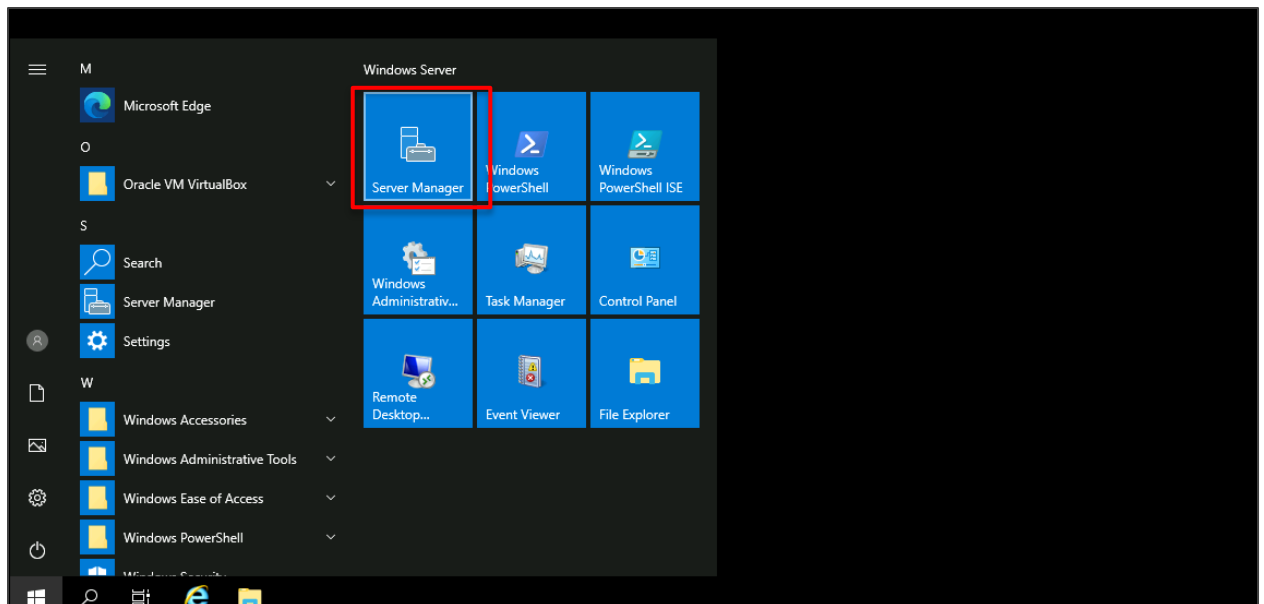
Infrastructure Security: Integrating Active Directory for Enhanced User Management and Compliance

Steps to be followed:

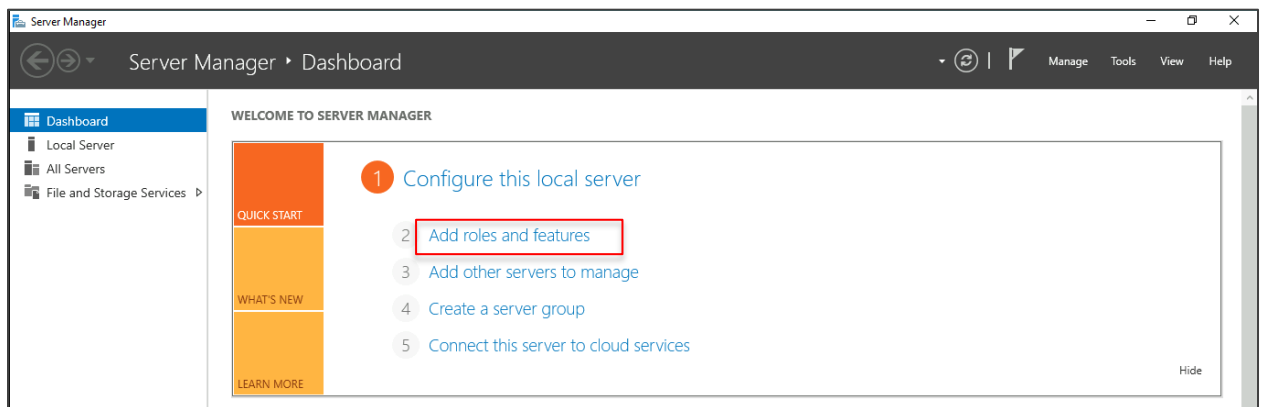
1. Setup active directory
2. Integrate client configuration
3. Create organizational units (OUs) and groups within OUs
4. Create a user management
5. Implement password policies
6. Integrate compliance and reporting

Step 1: Setup active directory

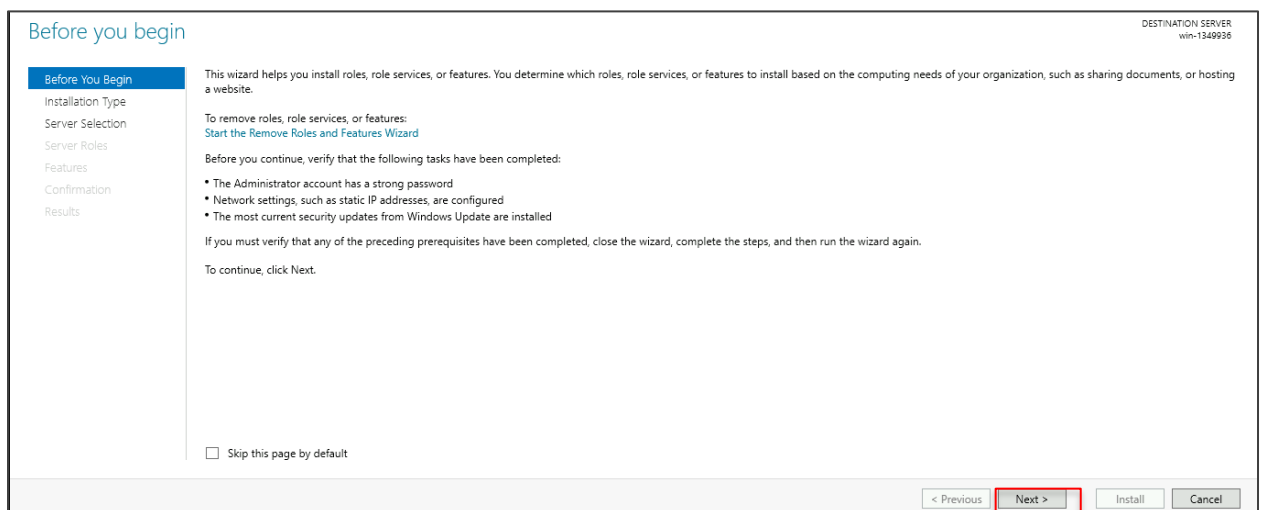
1.1 Click on Windows Key and write Server Manager. Click on **Server Manager**

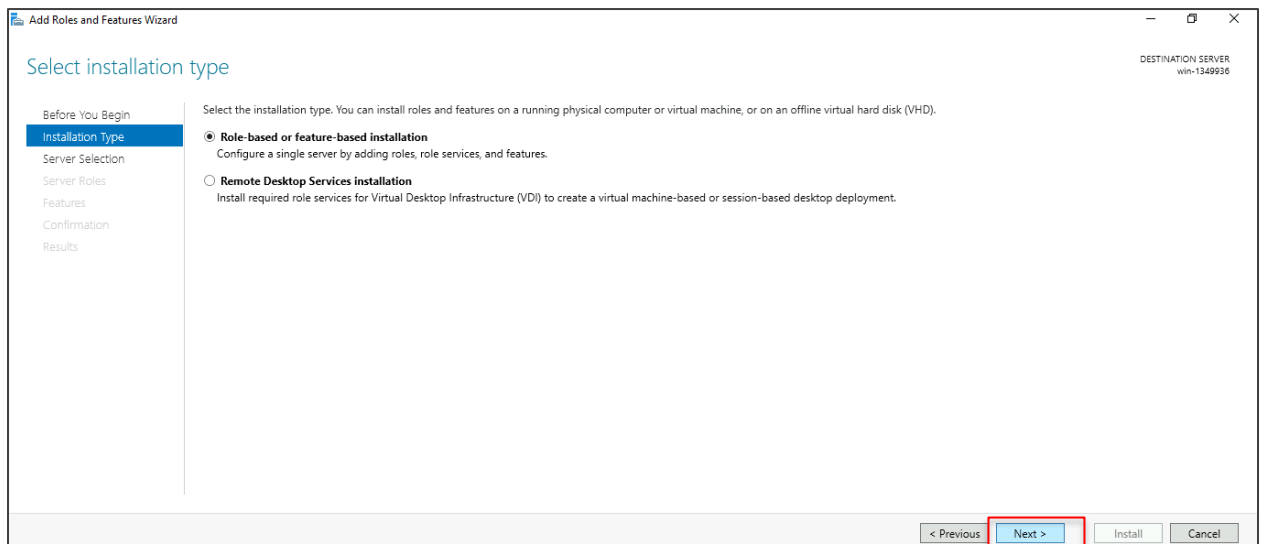


1.2 Click on **Add roles and features**

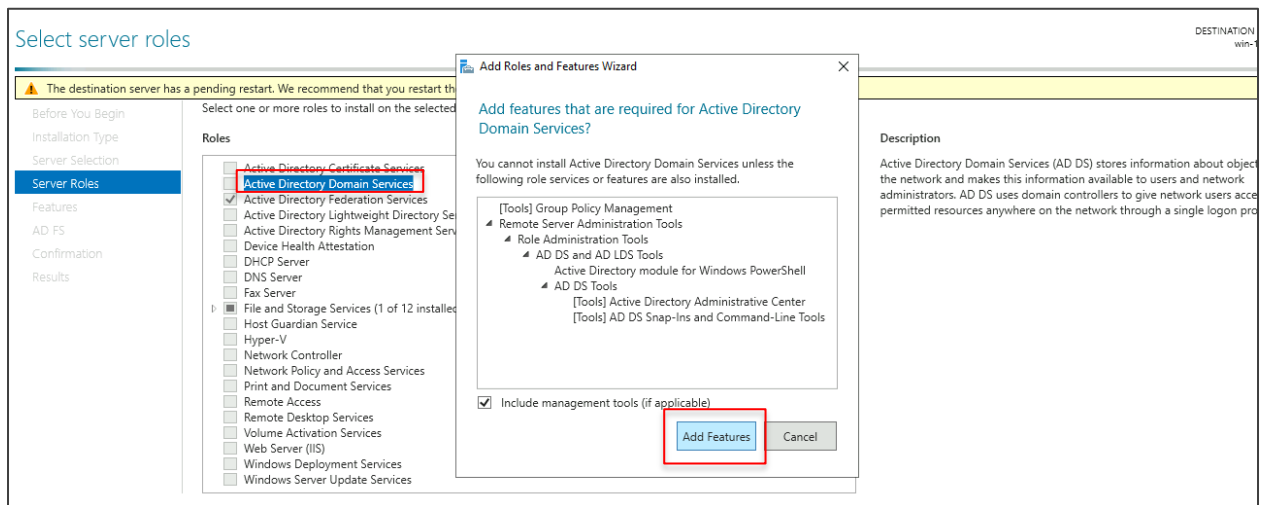


1.3 Click on **Next >**





1.4 Select **Active Directory Domain Services** then click on **Add features**



1.5 Click on Next >

Select features

DESTINATION SERVER
win-1349936

The destination server has a pending restart. We recommend that you restart the destination server before either installing or removing roles or features.

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

| Features | Description |
|--|---|
| <input type="checkbox"/> .NET Framework 3.5 Features | .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. |
| <input checked="" type="checkbox"/> .NET Framework 4.7 Features (2 of 7 installed) | |
| <input type="checkbox"/> Background Intelligent Transfer Service (BITS) | |
| <input checked="" type="checkbox"/> BitLocker Drive Encryption (Installed) | |
| <input type="checkbox"/> BitLocker Network Unlock | |
| <input type="checkbox"/> BranchCache | |
| <input type="checkbox"/> Client for NFS | |
| <input type="checkbox"/> Containers | |
| <input type="checkbox"/> Data Center Bridging | |
| <input type="checkbox"/> Direct Play | |
| <input checked="" type="checkbox"/> Enhanced Storage (Installed) | |
| <input type="checkbox"/> Failover Clustering | |
| <input checked="" type="checkbox"/> Group Policy Management | |
| <input type="checkbox"/> Host Guardian Hyper-V Support | |
| <input type="checkbox"/> I/O Quality of Service | |
| <input type="checkbox"/> IIS Hostable Web Core | |
| <input type="checkbox"/> Internet Printing Client | |
| <input type="checkbox"/> IP Address Management (IPAM) Server | |
| <input type="checkbox"/> ISNS Server service | |
| <input type="checkbox"/> LPR Port Monitor | |
| <input type="checkbox"/> Management OData IIS Extension | |

< Previous

Next >

Install

Cancel

Active Directory Federation Services (AD FS)

DESTINATION SERVER
win-1349936

Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) capabilities to authenticate a user to multiple Web applications using a single user account. AD FS helps organizations bypass the need for secondary accounts by allowing you to project a user's digital identity and access rights to trusted partners. In this federated environment, each organization continues to manage its own identities.

Things to note:

- This computer must be joined to a domain before you can successfully install the Federation Service.
- The Web Application Proxy role service in the Remote Access server role functions as the federation service proxy and cannot be installed on the same computer as the federation service.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

[Learn more about Azure Active Directory](#)

[Configure Office 365 with Azure Active Directory Connect](#)

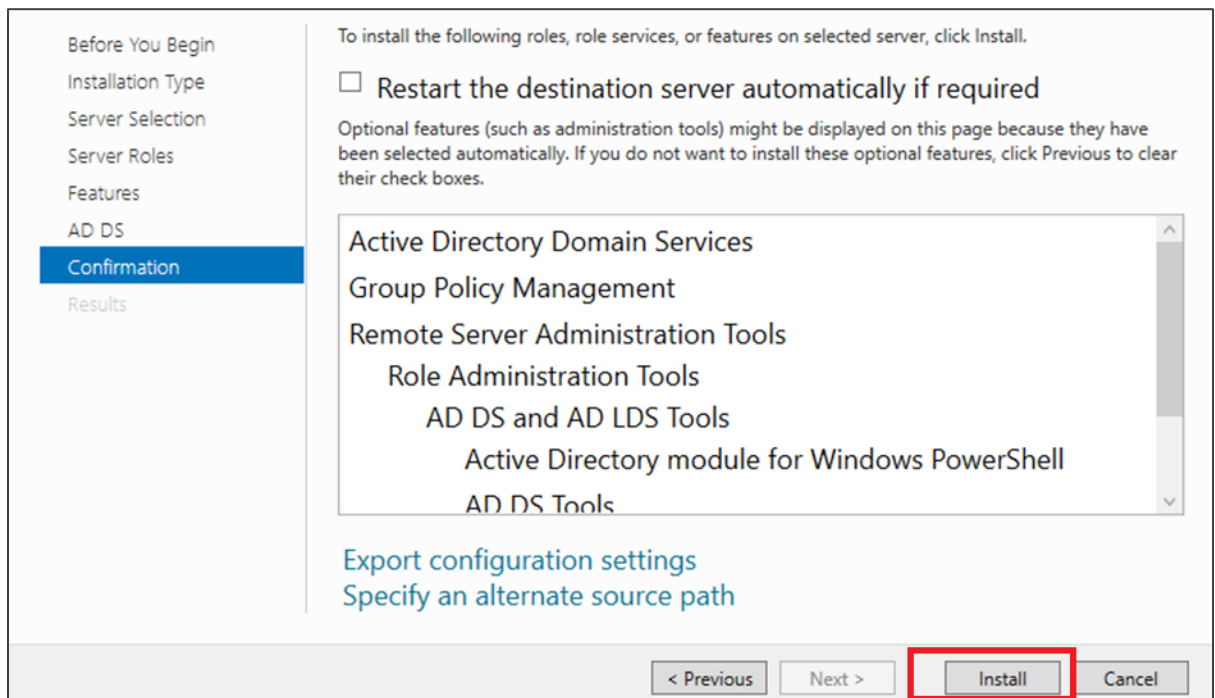
< Previous

Next >

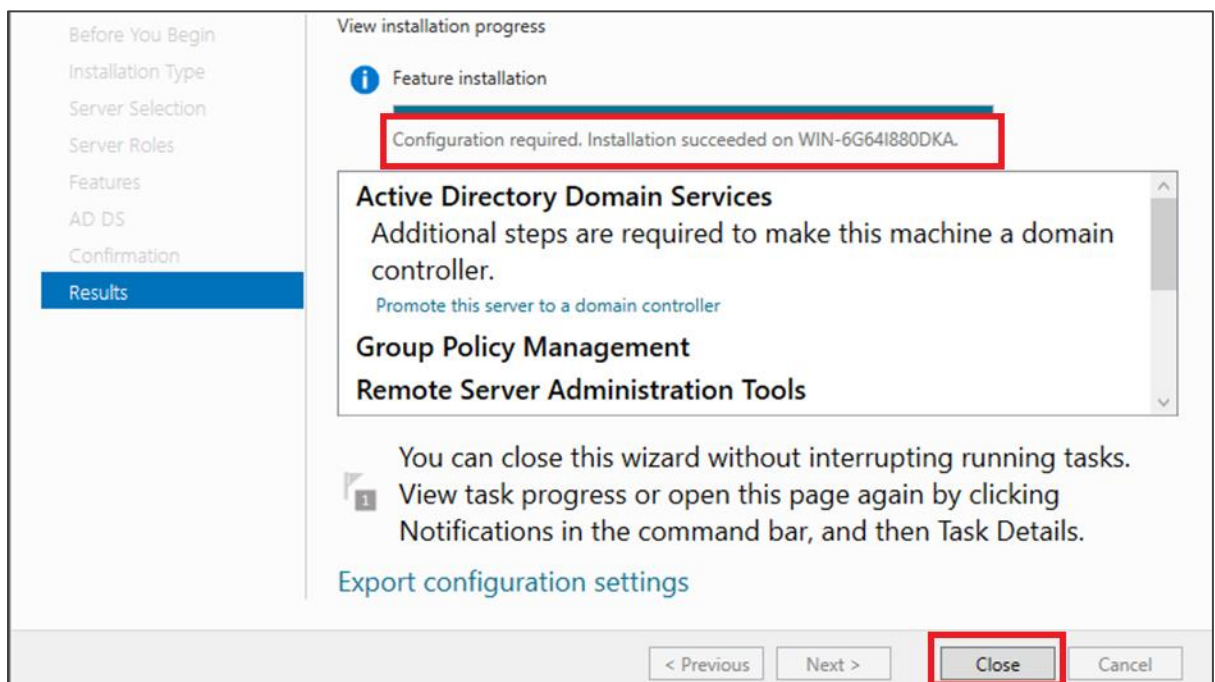
Install

Cancel

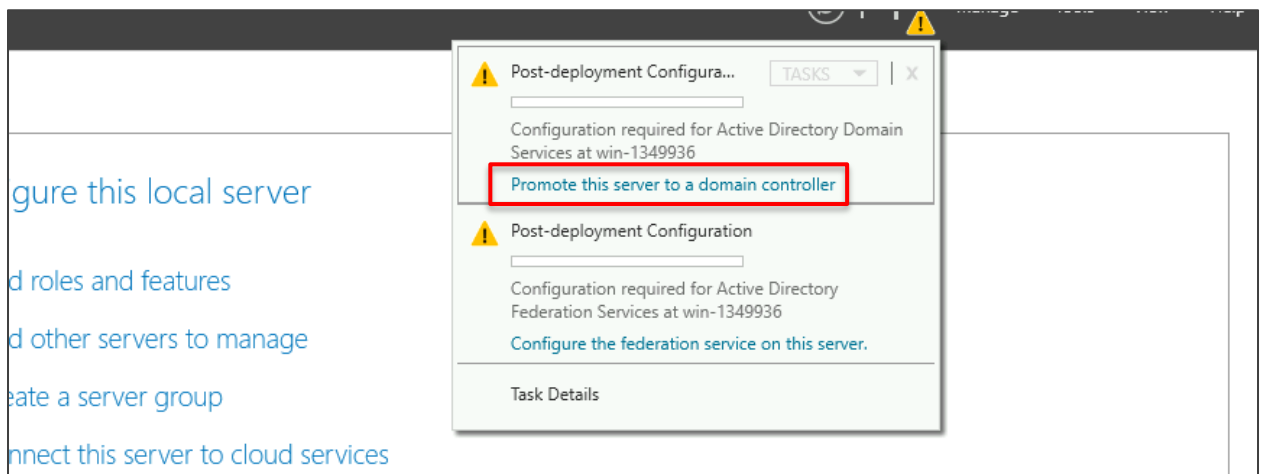
1.6 Click on **Install**



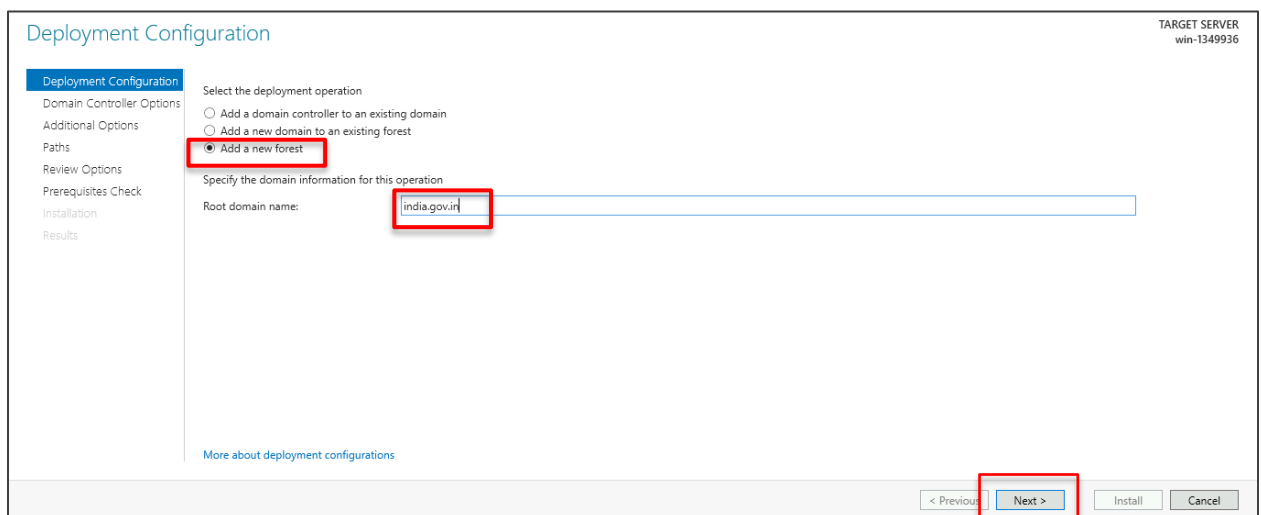
1.7 Once it is installed successfully click on **Close**



1.8 Click on the notification flag on the right side of the server manager dashboard and click on **promote this server to a domain controller**



1.9 Select **Add a new forest**. Add the **Root domain name** and click **Next**



1.10 Enter the Directory Services Restore Mode password and click **Next**

Domain Controller Options TARGET SERVER
win-1349936

Deployment Configuration
Domain Controller Options
 DNS Options
 Additional Options
 Paths
 Review Options
 Prerequisites Check
 Installation
 Results

Select functional level of the new forest and root domain

Forest functional level:

Domain functional level:

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](#)

1.11 Click **Next >**

DNS Options TARGET SERVER
win-1349936

Deployment Configuration
 Domain Controller Options
DNS Options
 Additional Options
 Paths
 Review Options
 Prerequisites Check
 Installation
 Results

Specify DNS delegation options

☐ Create DNS delegation

[More about DNS delegation](#)

⚠ 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 manu... [Show more](#) ✕

Additional Options

TARGET SERVER
win-1349936

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

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

The NetBIOS domain name:

[More about additional options](#)

< Previous

Next >

Install

Cancel

1.12 Click on **Next >** then click on **Install**

Review Options

TARGET SERVER
win-1349936

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "india.gov.in". This is also the name of the new forest.

The NetBIOS name of the domain: INDIA

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

Database folder: C:\Windows\NTDS

Log file folder: C:\Windows\NTDS

These settings can be exported to a Windows PowerShell script to automate additional installations

[More about installation options](#)

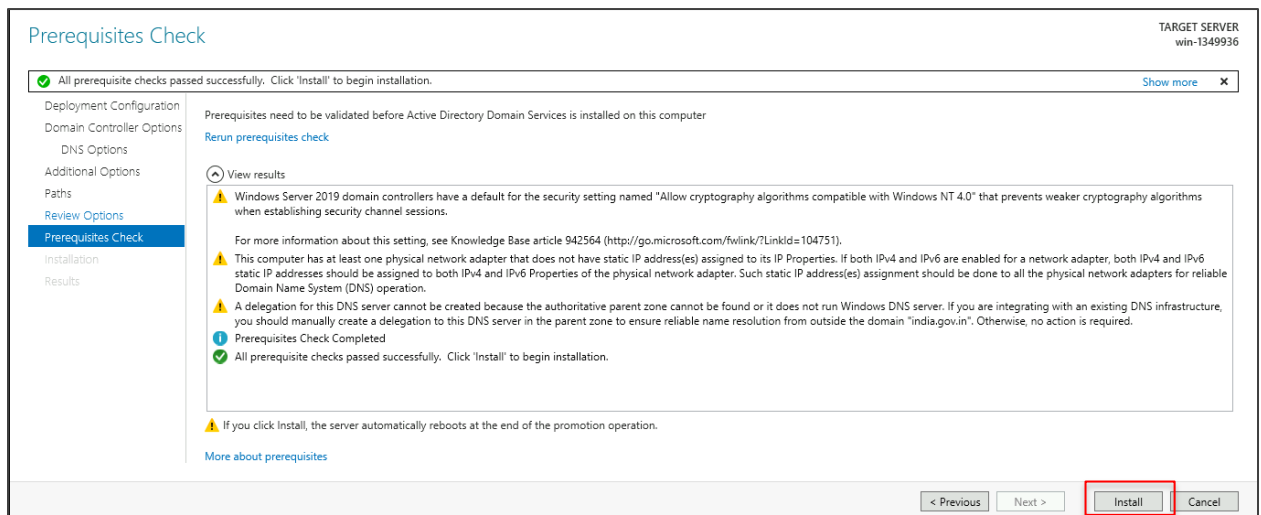
[View script](#)

< Previous

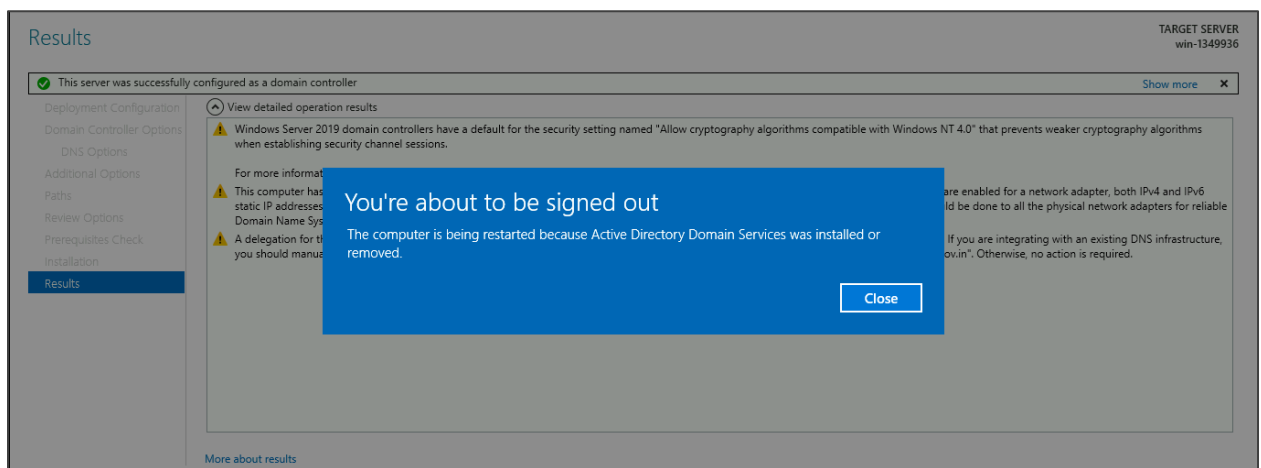
Next >

Install

Cancel

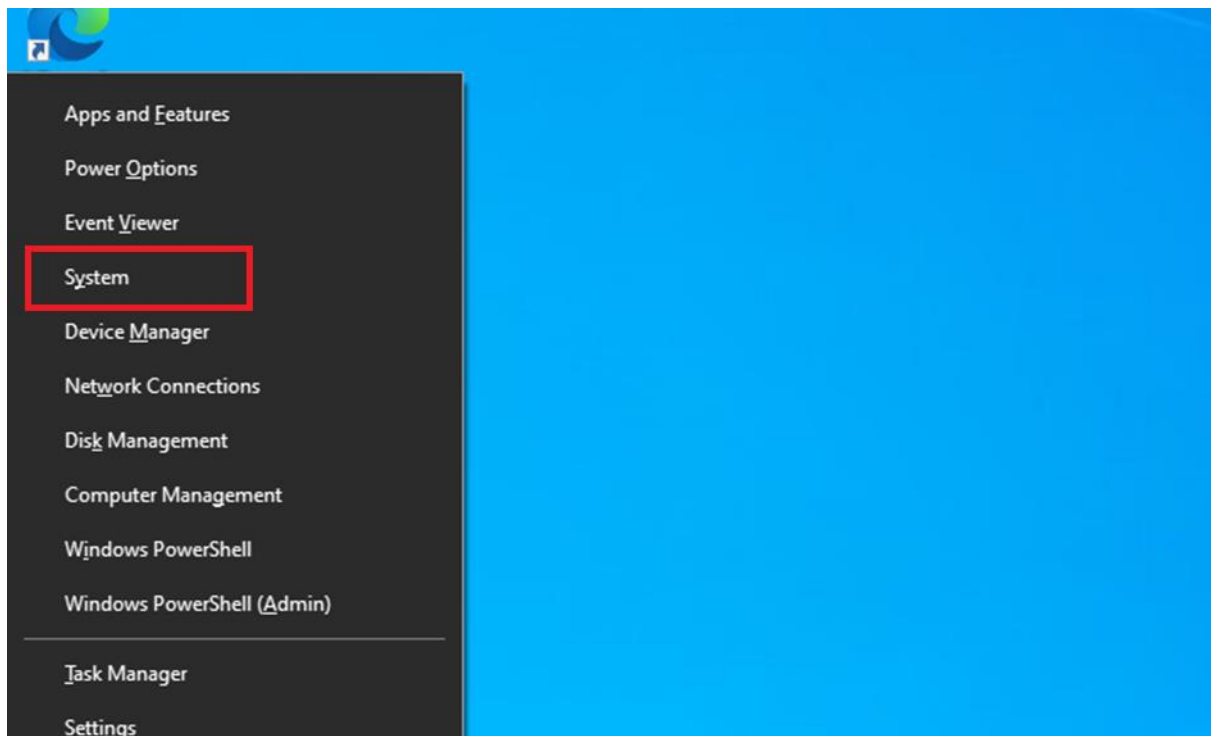


1.13 Click on Close

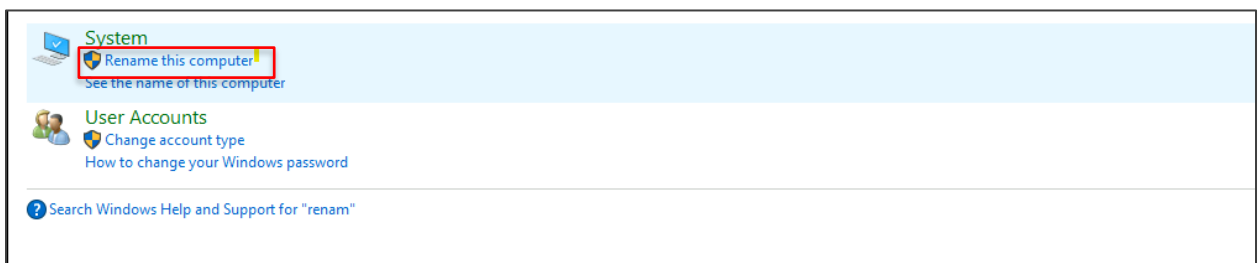


Step 2: Integrate client configuration

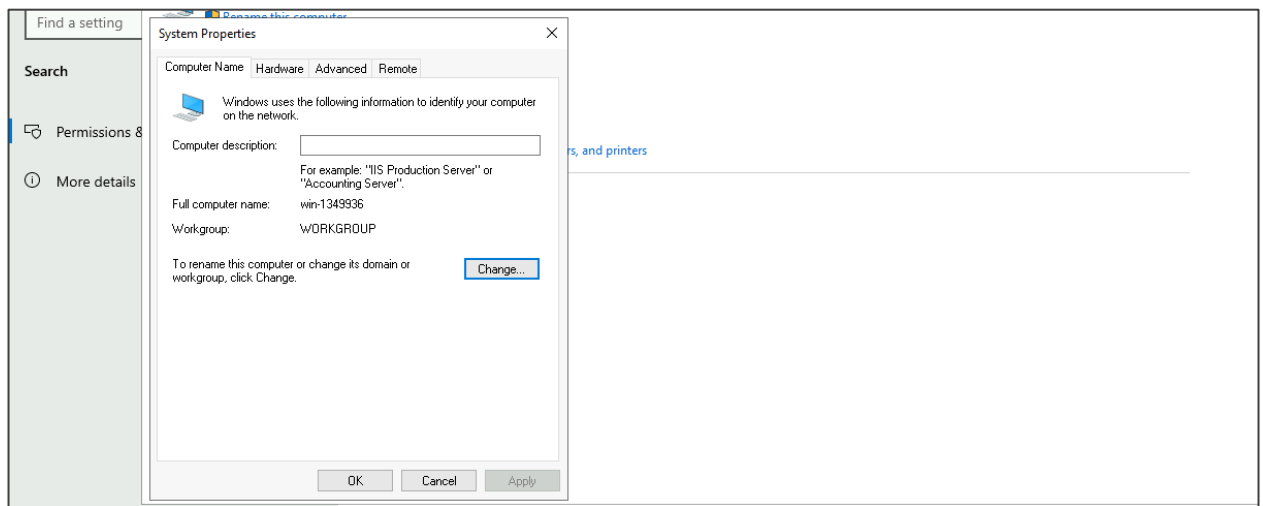
2.1 Start a Windows 10 OS and press windows+x and select the **System**



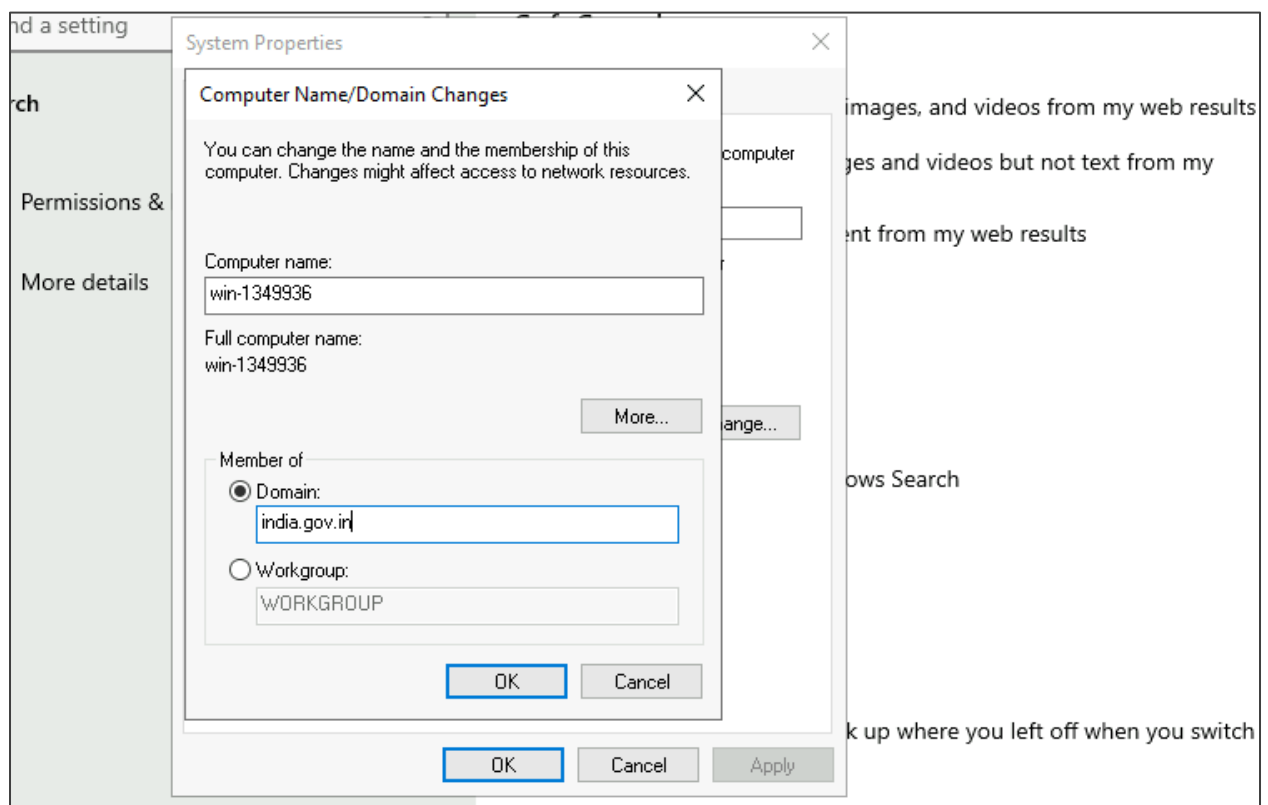
2.2 Click on **Rename this computer**



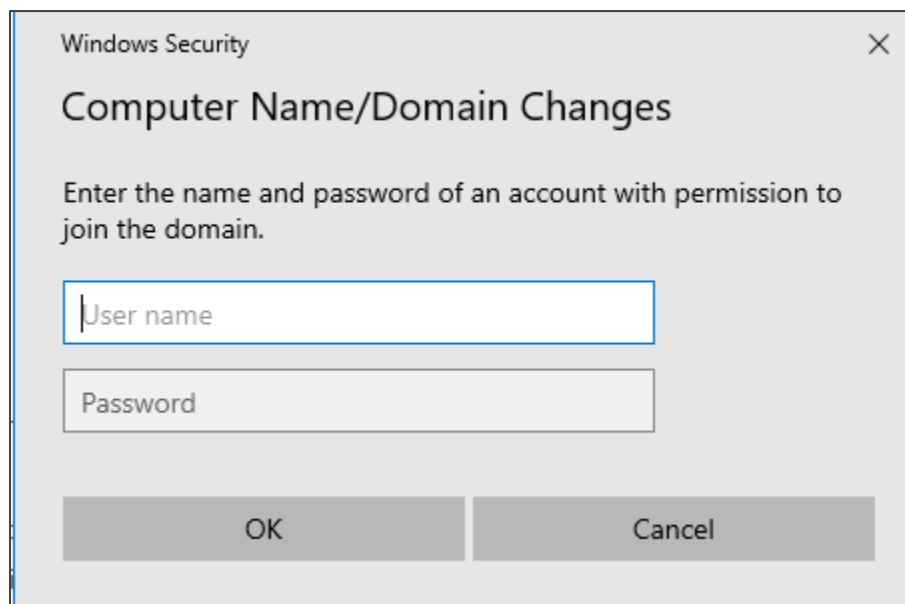
2.3 Click on **Change**



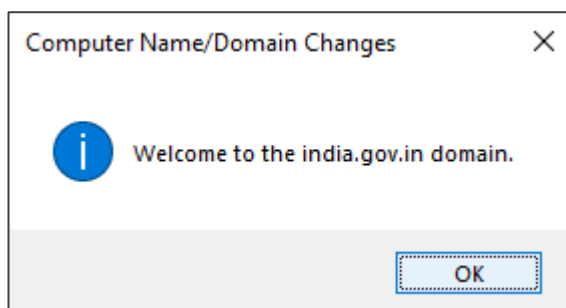
2.4 Click on **Domain** and enter the domain name you want this PC to join and click on **OK**



2.5 Login with an administrator account on Windows Server 2022

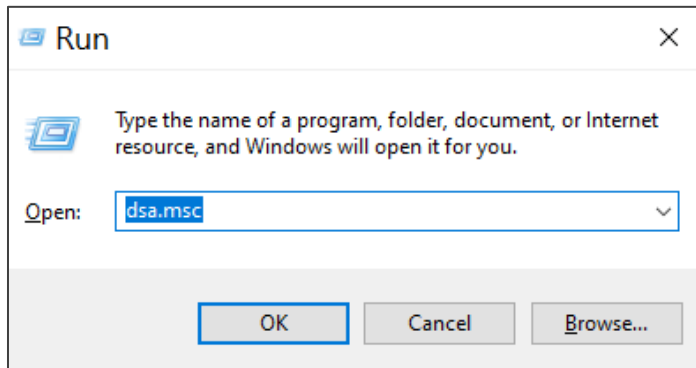


2.6 Upon successful login, the current system will join the domain, click on **OK**

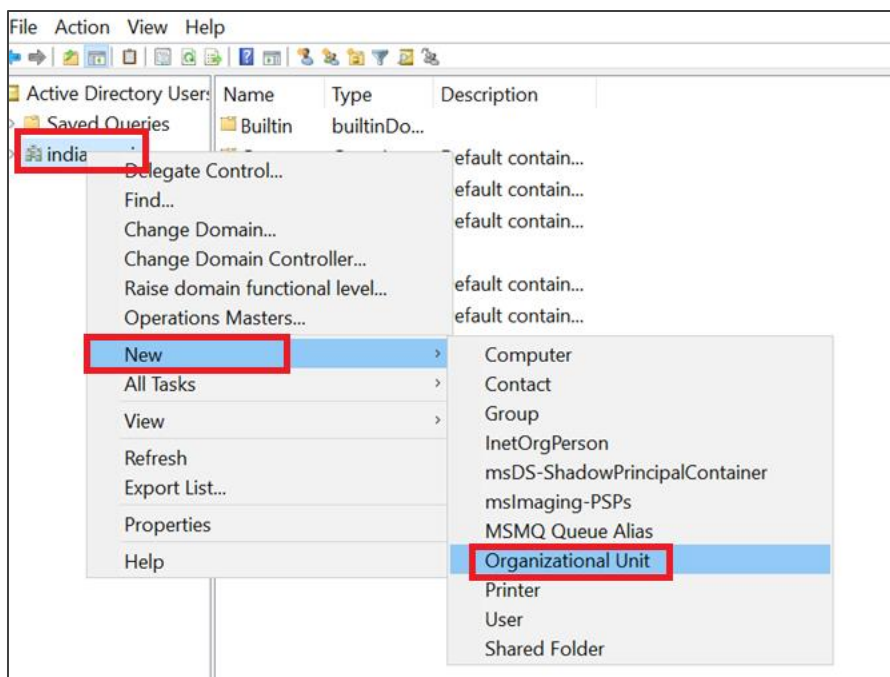


Step 3: Create organizational units (OUs) and groups within OUs

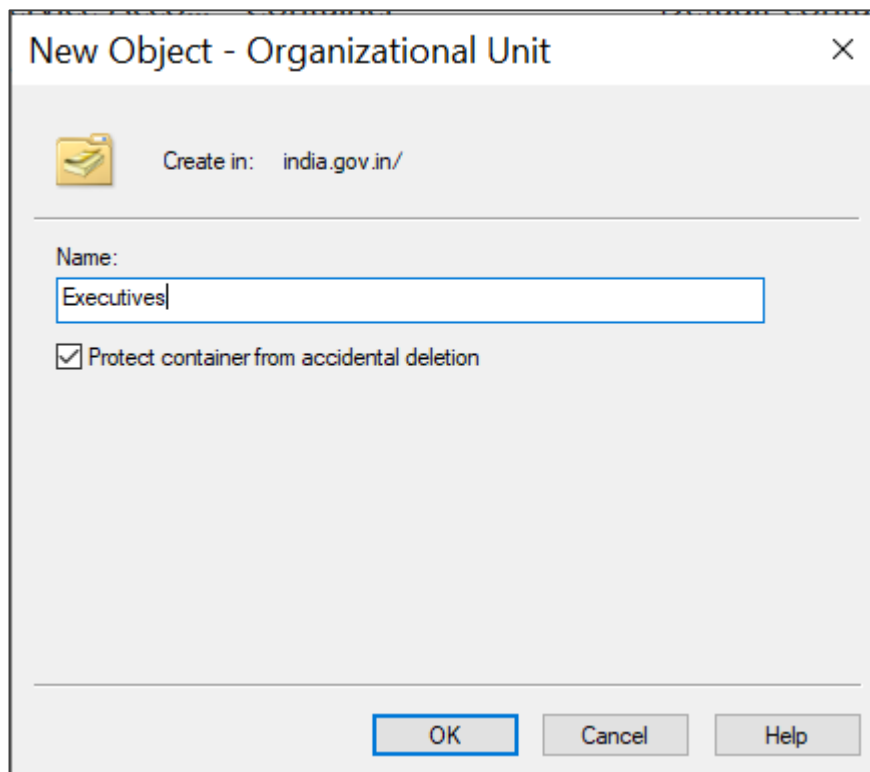
3.1 Press windows + r and type **dsa.msc**



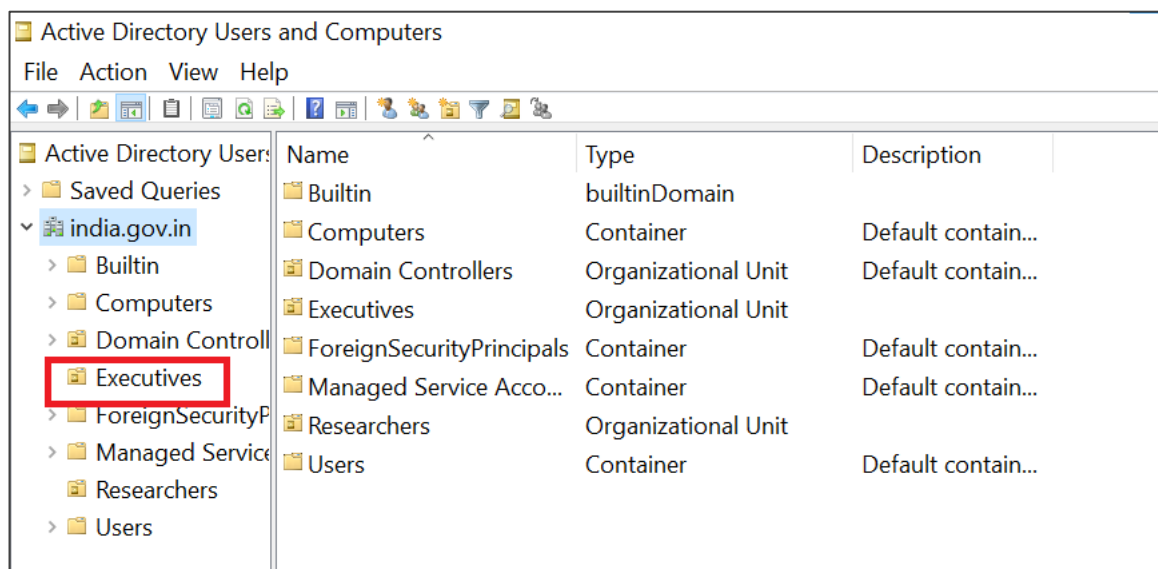
3.2 Right click on the domain **india.gov.in** and click on **New** and **Organizational Unit**



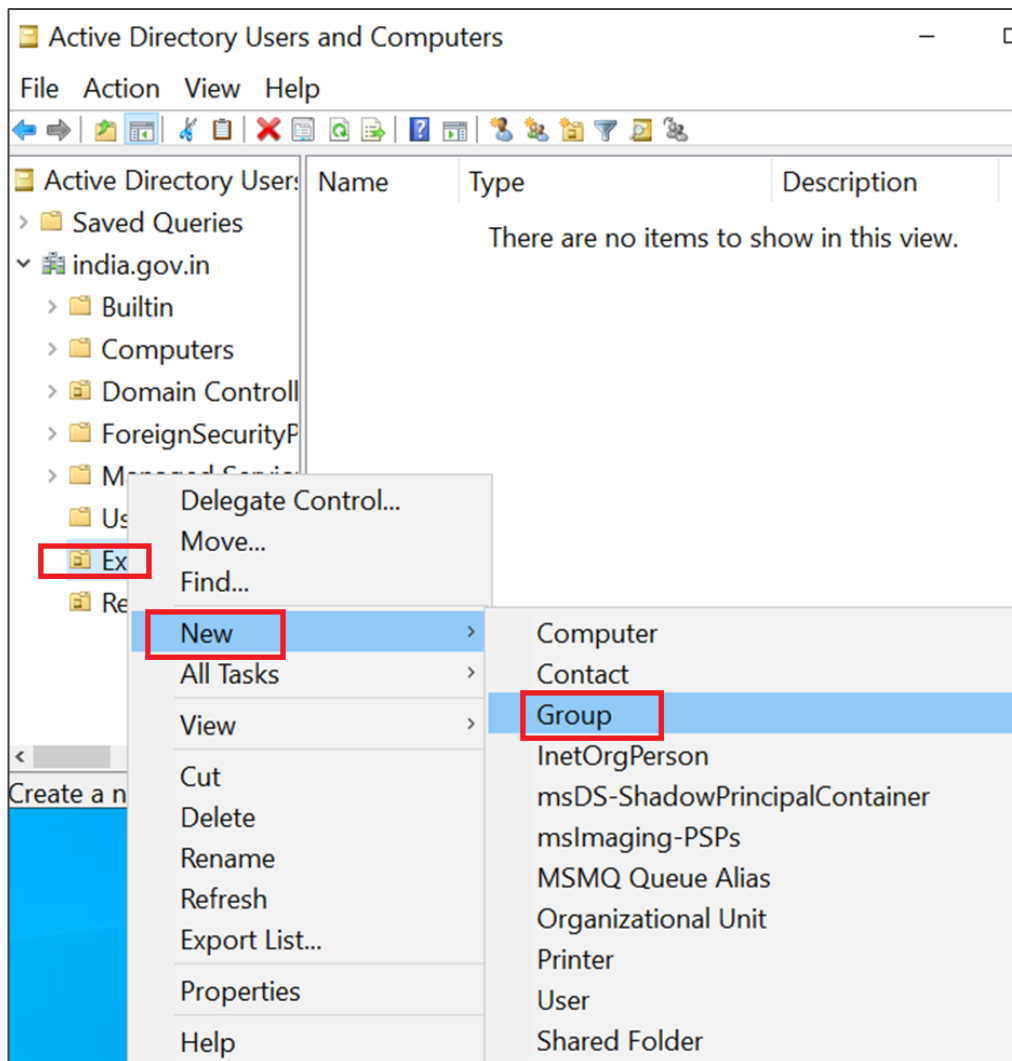
3.3 Write the **Name** of the OU to be created, then click on **OK**



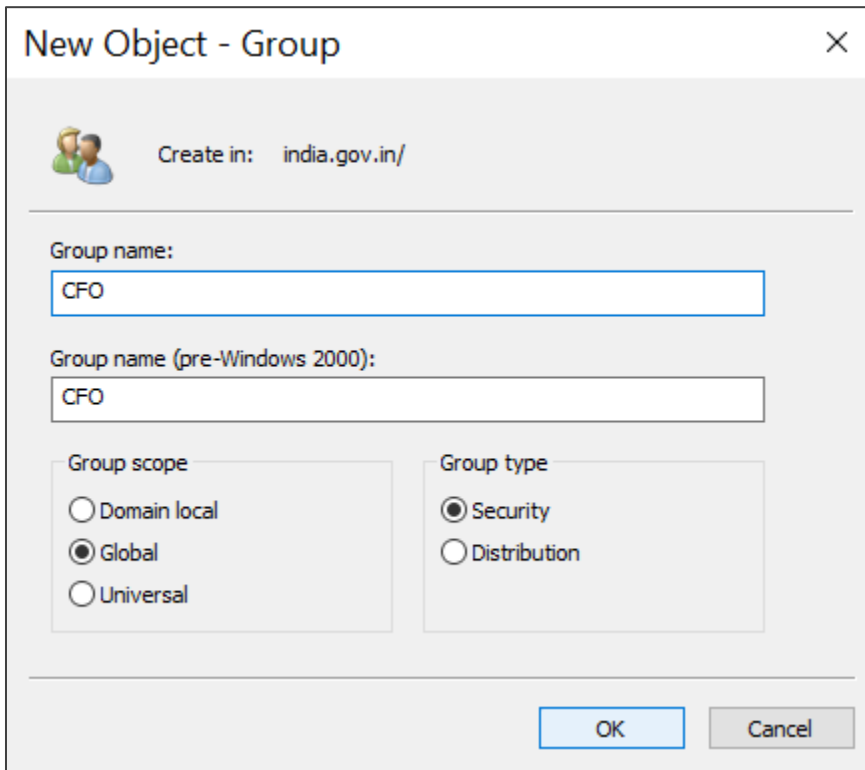
Executives OU is visible in the left tree pane:



3.4 Right Click on the **Executives** OU, click on **New**, and select **Group**



3.5 Write the **Group name** as **CFO** and click on **OK**



New Object - Group

Create in: india.gov.in/

Group name:
CFO

Group name (pre-Windows 2000):
CFO

Group scope

- ☐ Domain local
- ☒ Global
- ☐ Universal

Group type

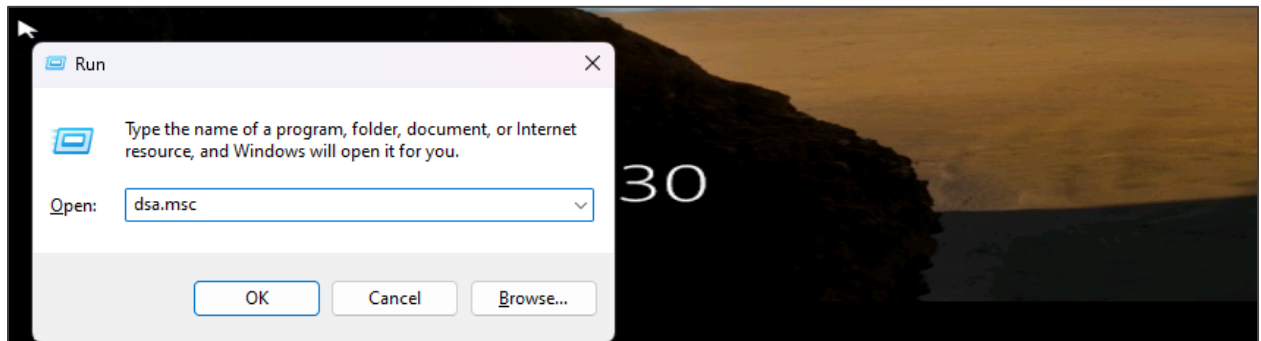
- ☒ Security
- ☐ Distribution

OK Cancel

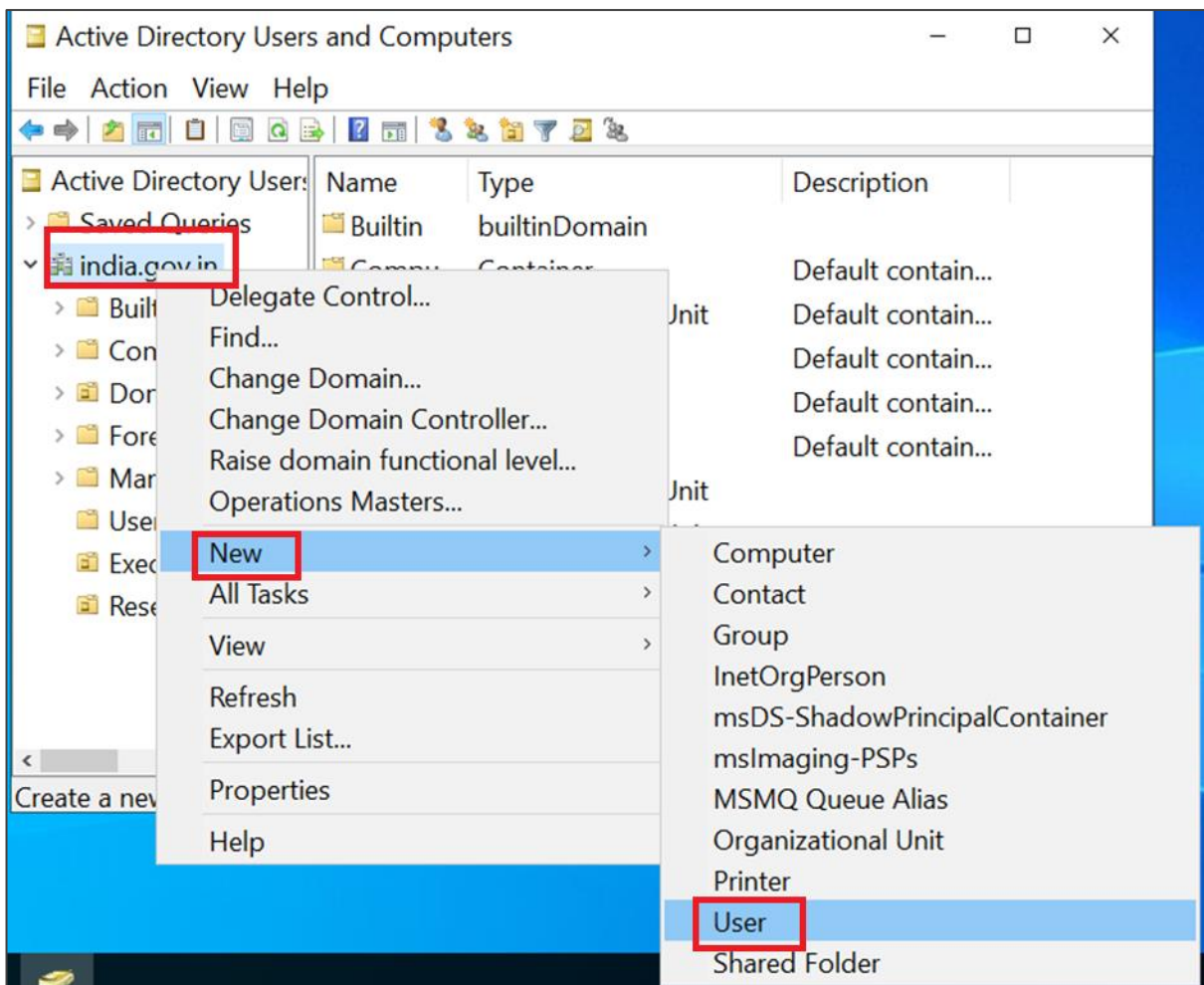
Note : Similarly create other groups.

Step 4: Create a user management

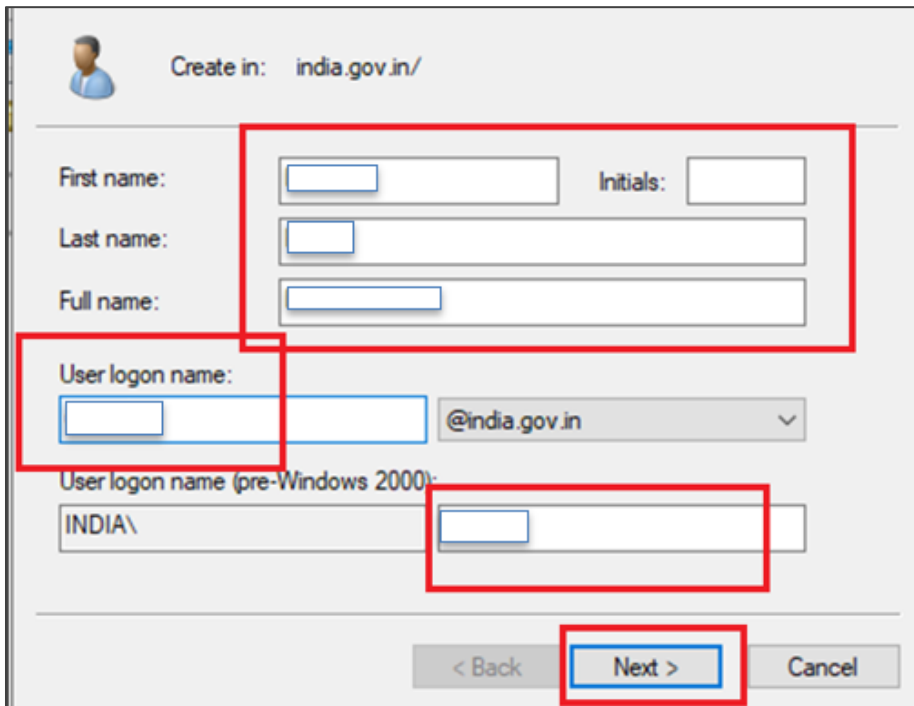
4.1 Press windows+r and type **dsa.msc**



4.2 Right click on domain **india.gov.in**, select **New**, and click on **User**



4.3 Enter the details of the user, choose a username, and click **Next**



Create in: india.gov.in/

First name: Initials:

Last name:

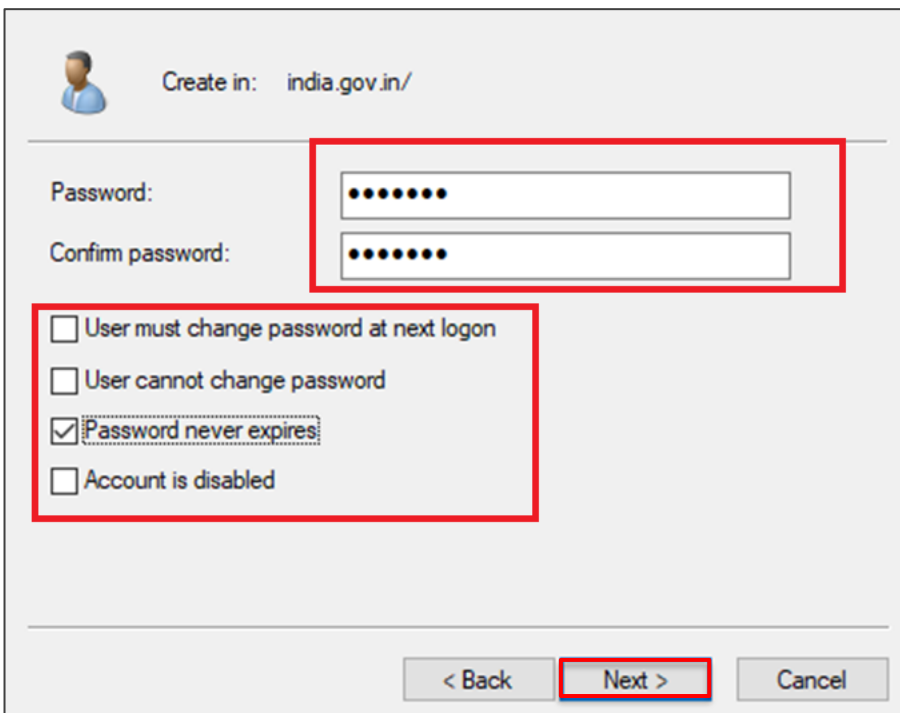
Full name:

User logon name: @india.gov.in

User logon name (pre-Windows 2000): INDIA\

< Back **Next >** Cancel

4.4 Enter the password to be set for the user and select the appropriate checkbox for the user and click **Next**, then click on **Finish**



Create in: india.gov.in/

Password:

Confirm password:

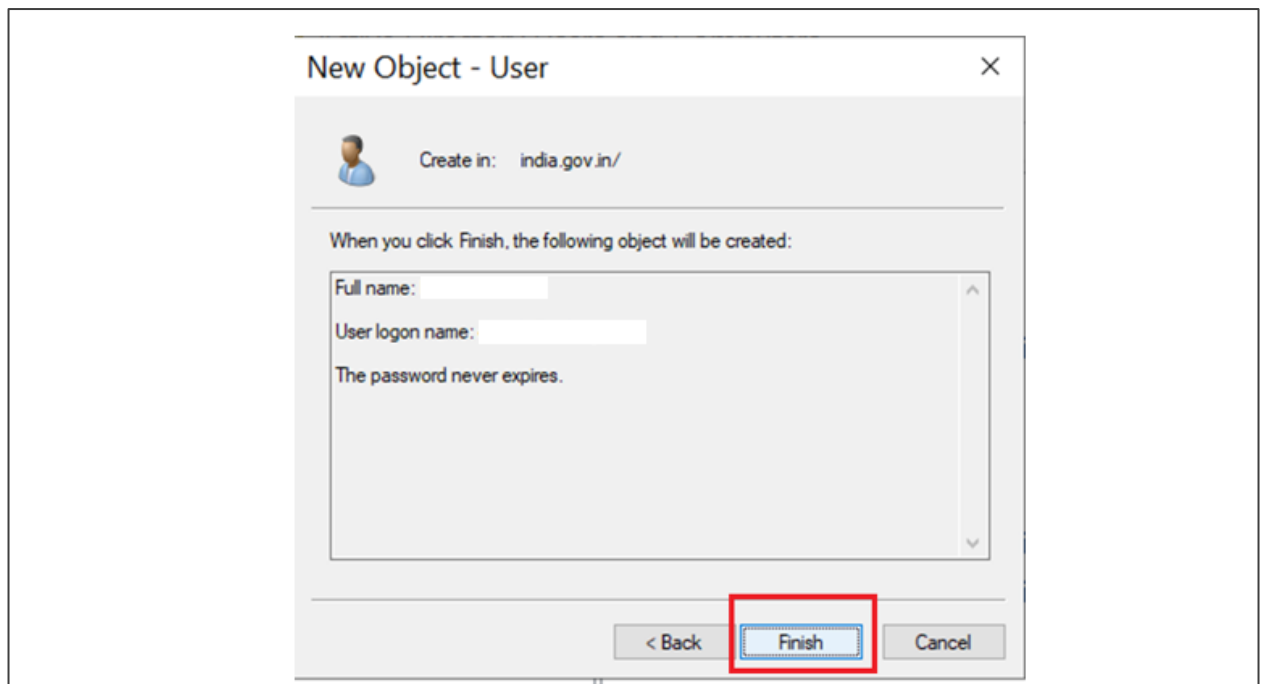
☐ User must change password at next logon

☐ User cannot change password

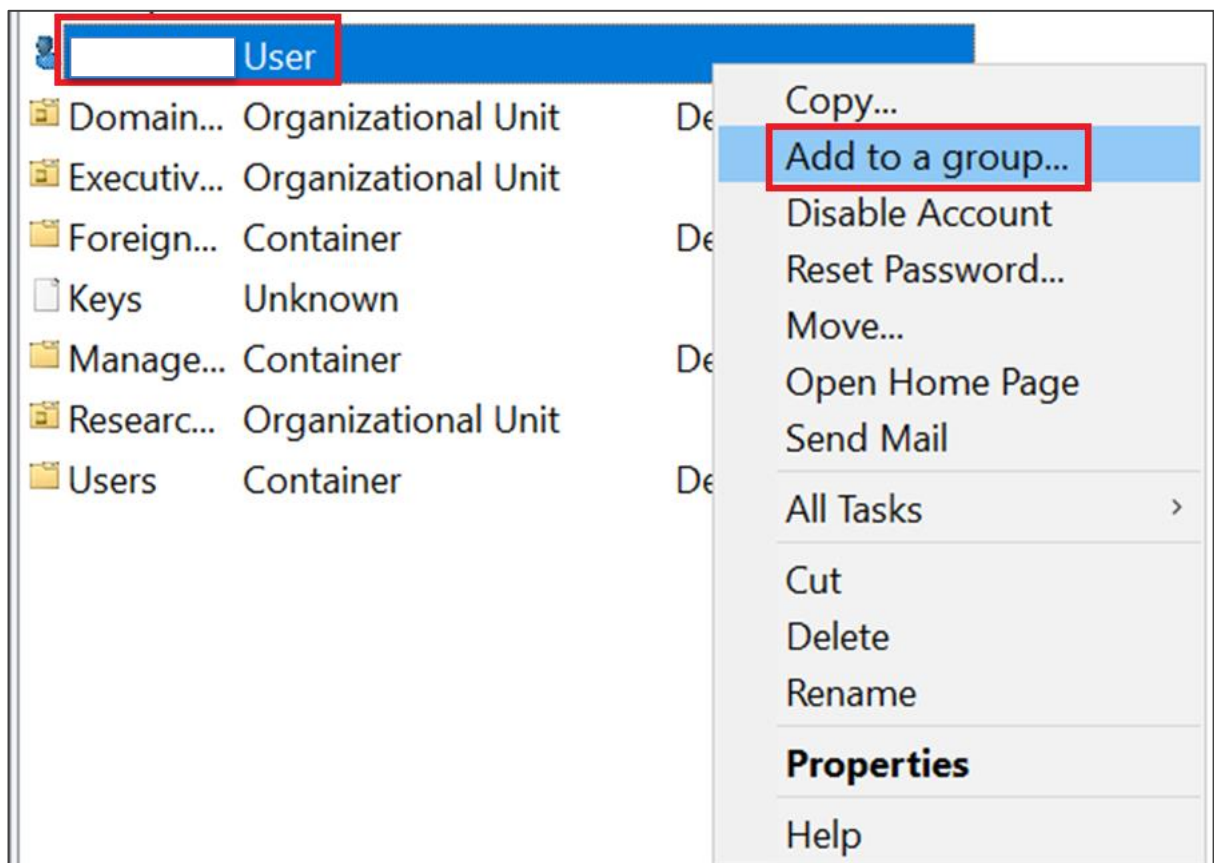
☒ Password never expires

☐ Account is disabled

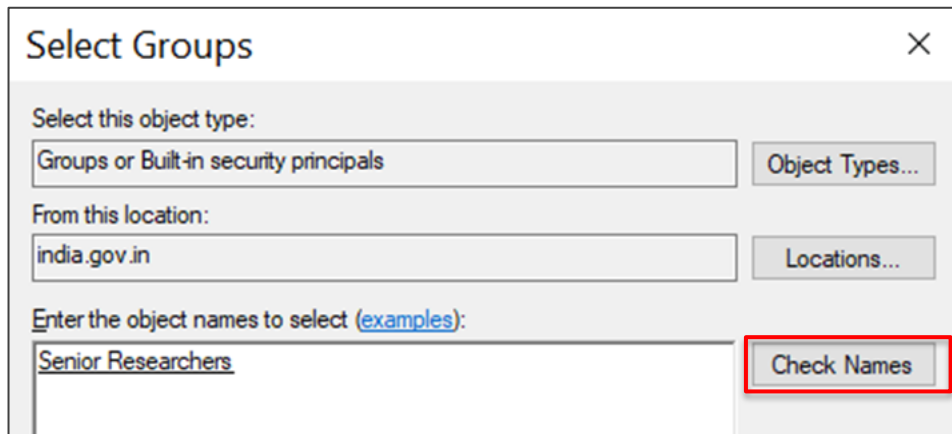
< Back **Next >** Cancel



4.5 Right click on the user created and select **Add to a group**



4.6 Write **Senior Researchers** in the textbox and click on **Check Names**



Select Groups

Select this object type:

Groups or Built-in security principals

Object Types...

From this location:

india.gov.in

Locations...

Enter the object names to select (examples):

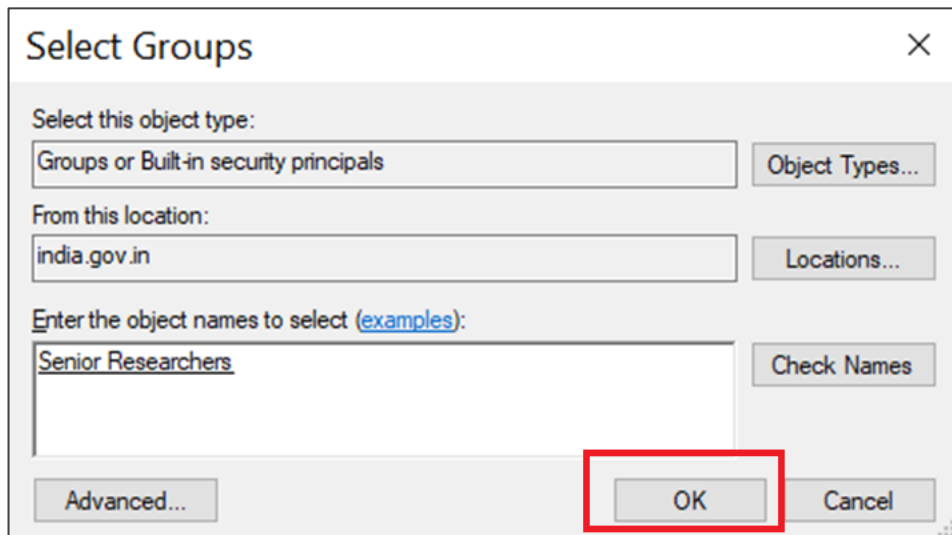
Senior Researchers

Check Names

4.7 Select the **Senior Researcher** group and click **OK**

| Name | Description | In Folder |
|------------------|-------------|---------------------|
| Senior Resear... | | india.gov.in/Res... |

4.8 Select the tab Member Of and click on **OK**



Select Groups

Select this object type:

Groups or Built-in security principals

Object Types...

From this location:

india.gov.in

Locations...

Enter the object names to select (examples):

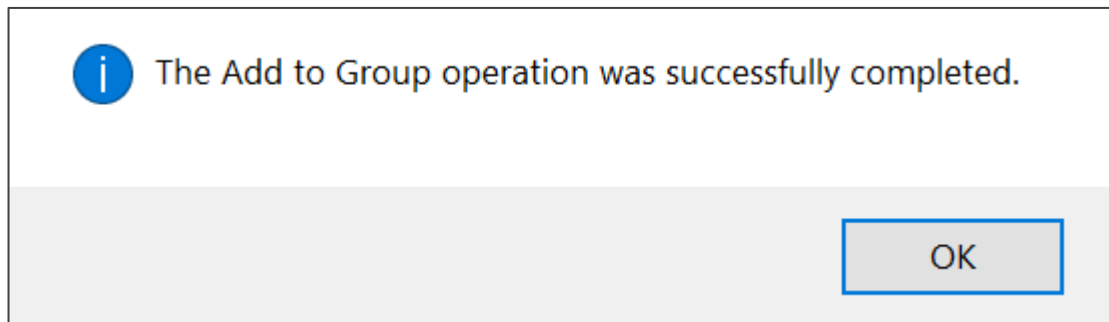
Senior Researchers

Check Names

Advanced...

OK

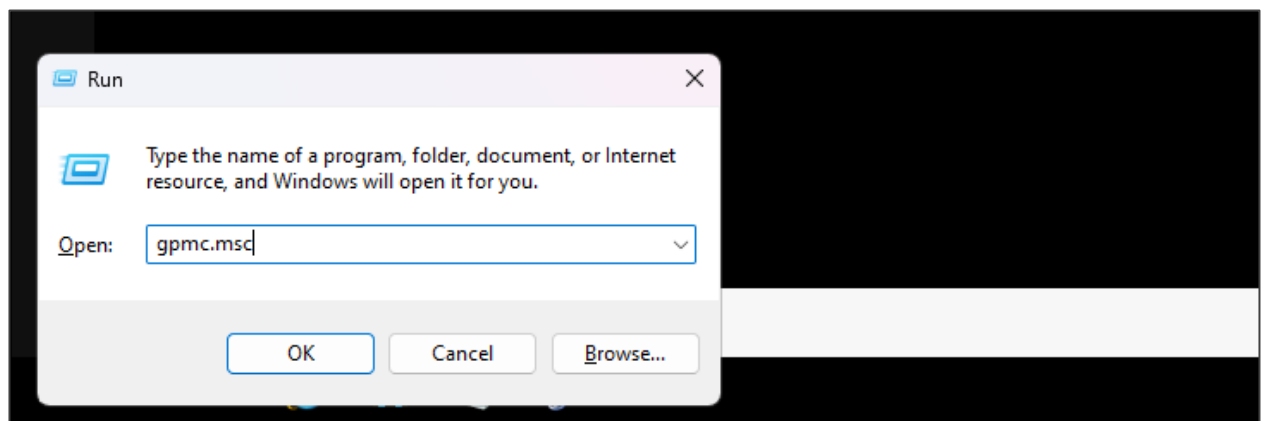
Cancel



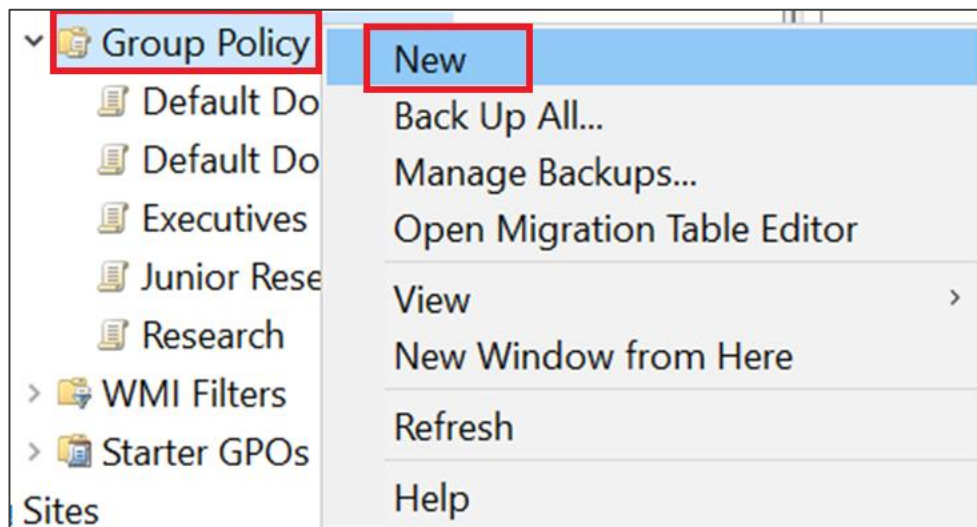
The user has been successfully added to the group Senior Researchers.

Step 5: Implement password policies

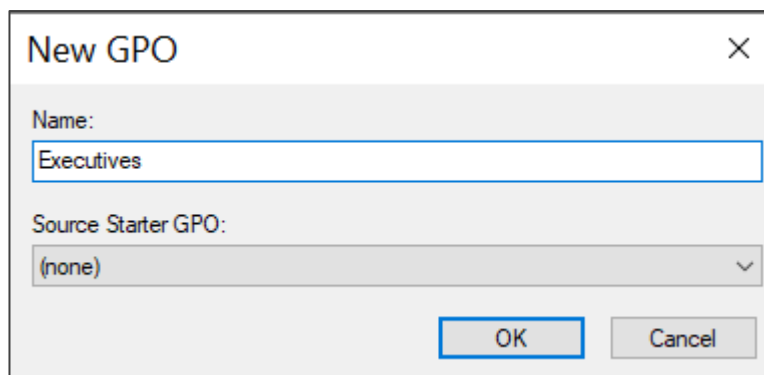
5.1 After signing in to Windows 10 client system using newly created domain user press windows+r and type **gpmc.msc** and click **OK**



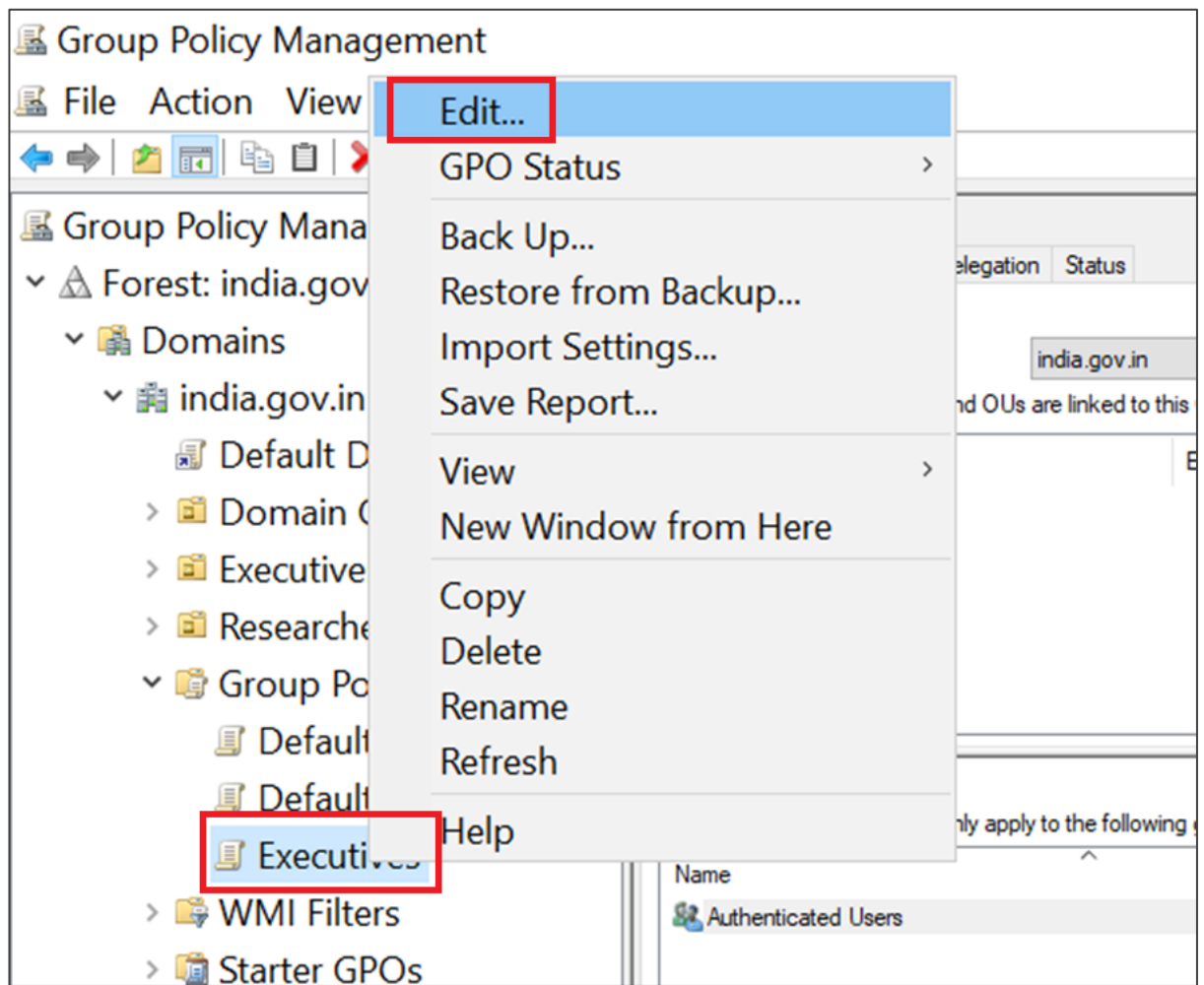
5.2 Right-click on **Group Policy Objects** and click **New**



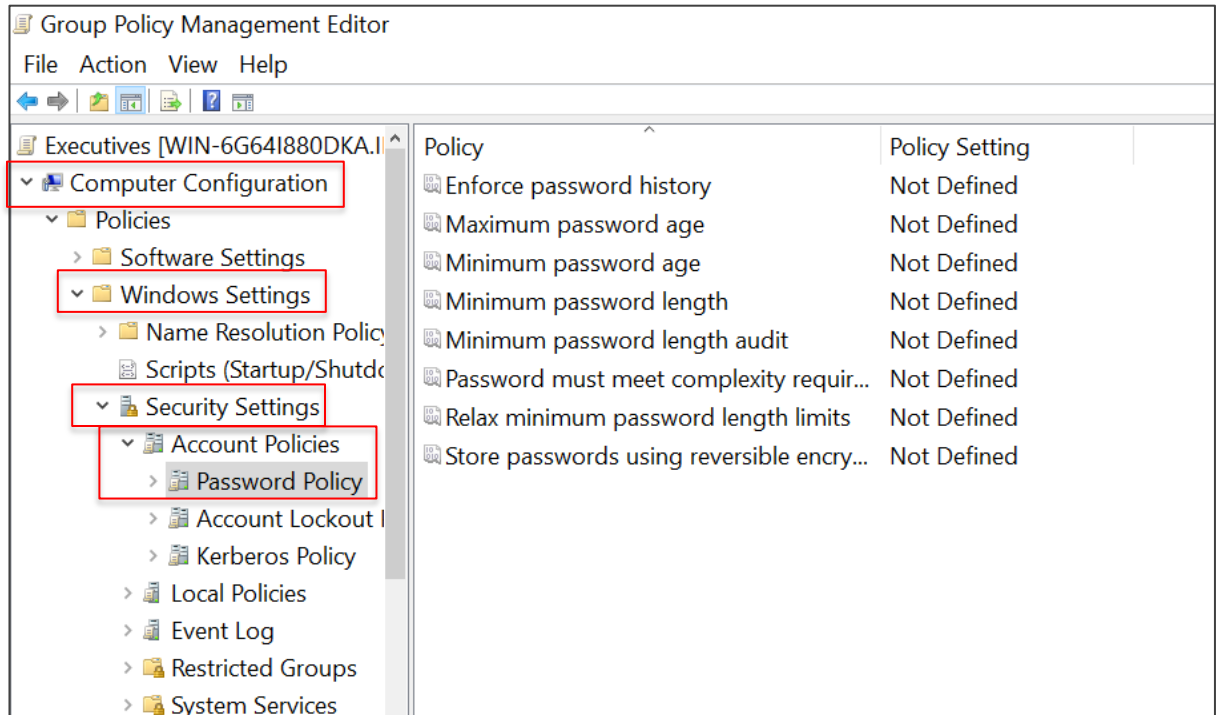
5.3 Write the **Name** of the group policy as **Executives** and click on **OK**



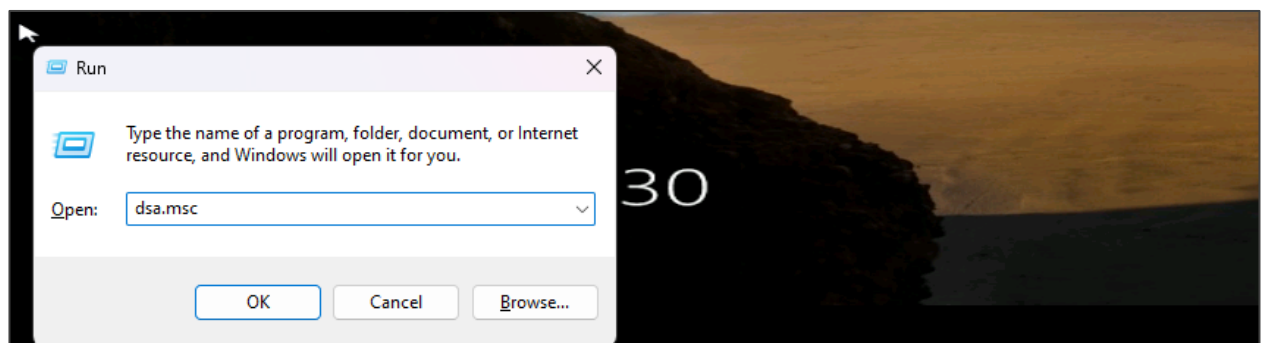
5.4 Right-click on the newly created object and click **Edit**



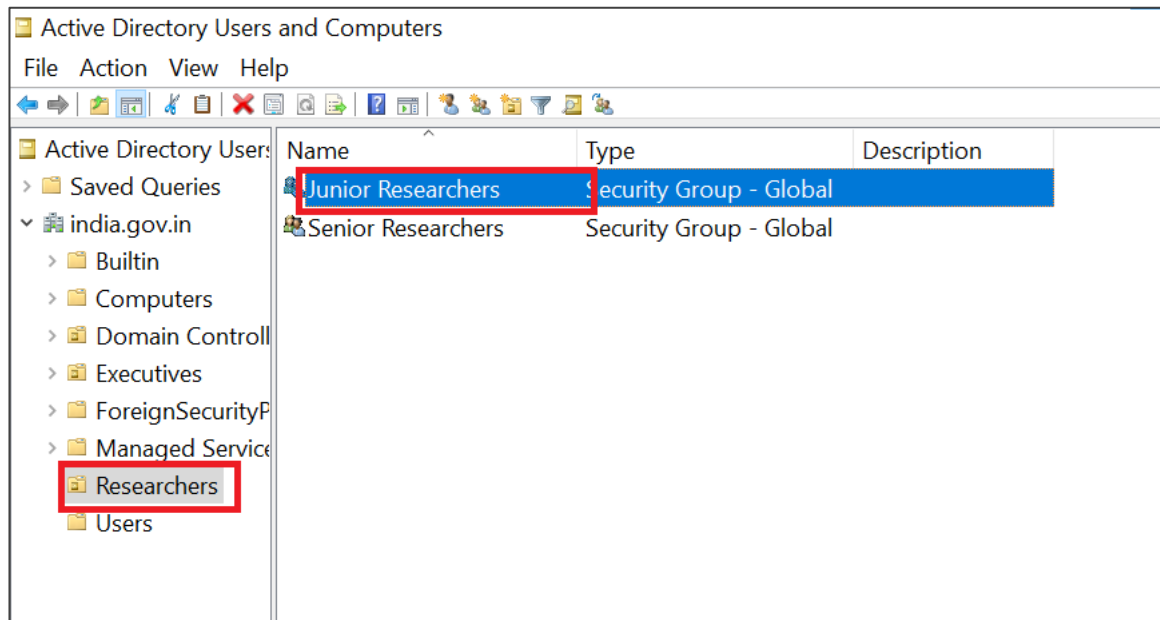
5.5 Navigate to **Computer Configuration>Windows Settings>Security Settings>Account Policies>Password Policy**



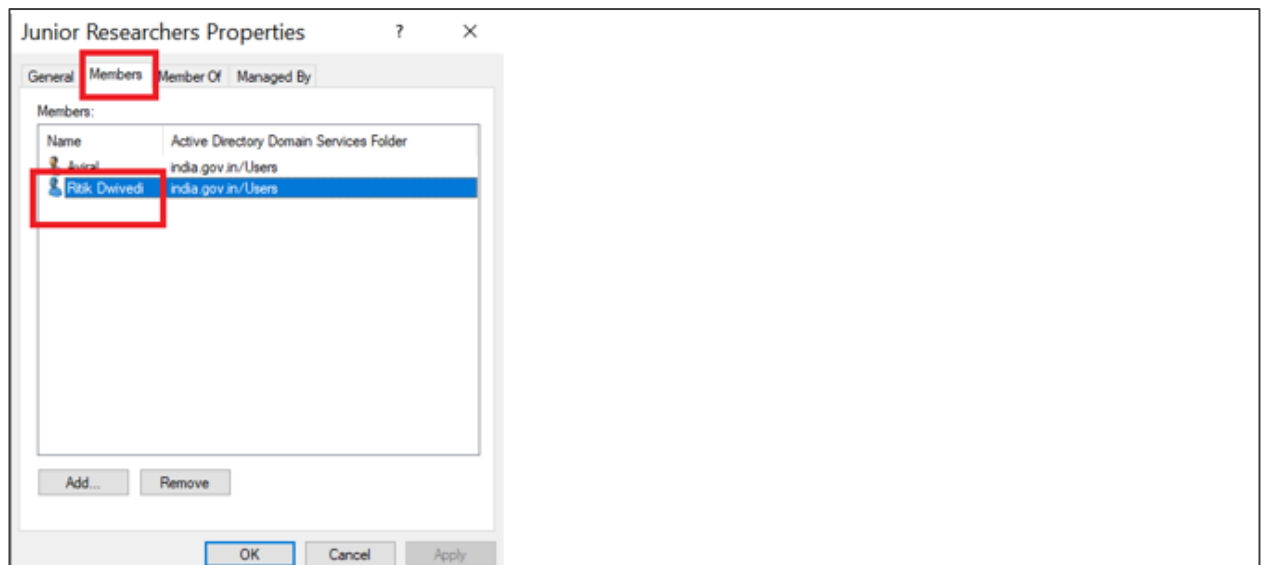
5.6 press windows+r and type **dsa.msc** and click **OK**



5.7 Double click on **Researchers** and then double click on **Junior Researchers**



5.8 Click on **Members** and double click on Ritik Dwivedi



5.9 Click on **Account** and select **Logon Hours**, then set logon hours between 7:00 AM to 7:00 PM

Ritik Dwivedi Properties

Member Of: Remote control, Dial-in, Environment, Sessions, Remote Desktop Services Profile, COM+

General Address **Account** Profile Telephones Organization

User logon name: rtik @india.gov.in

User logon name (pre-Windows 2000): INDIA\ rtik

Logon Hours... Log On To...

☐ 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: Wednesday, September 18, 2024

OK Cancel Apply Help

12 • 2 • 4 • 6 • 8 • 10 • 12 • 2 • 4 • 6 • 8 • 10 • 12

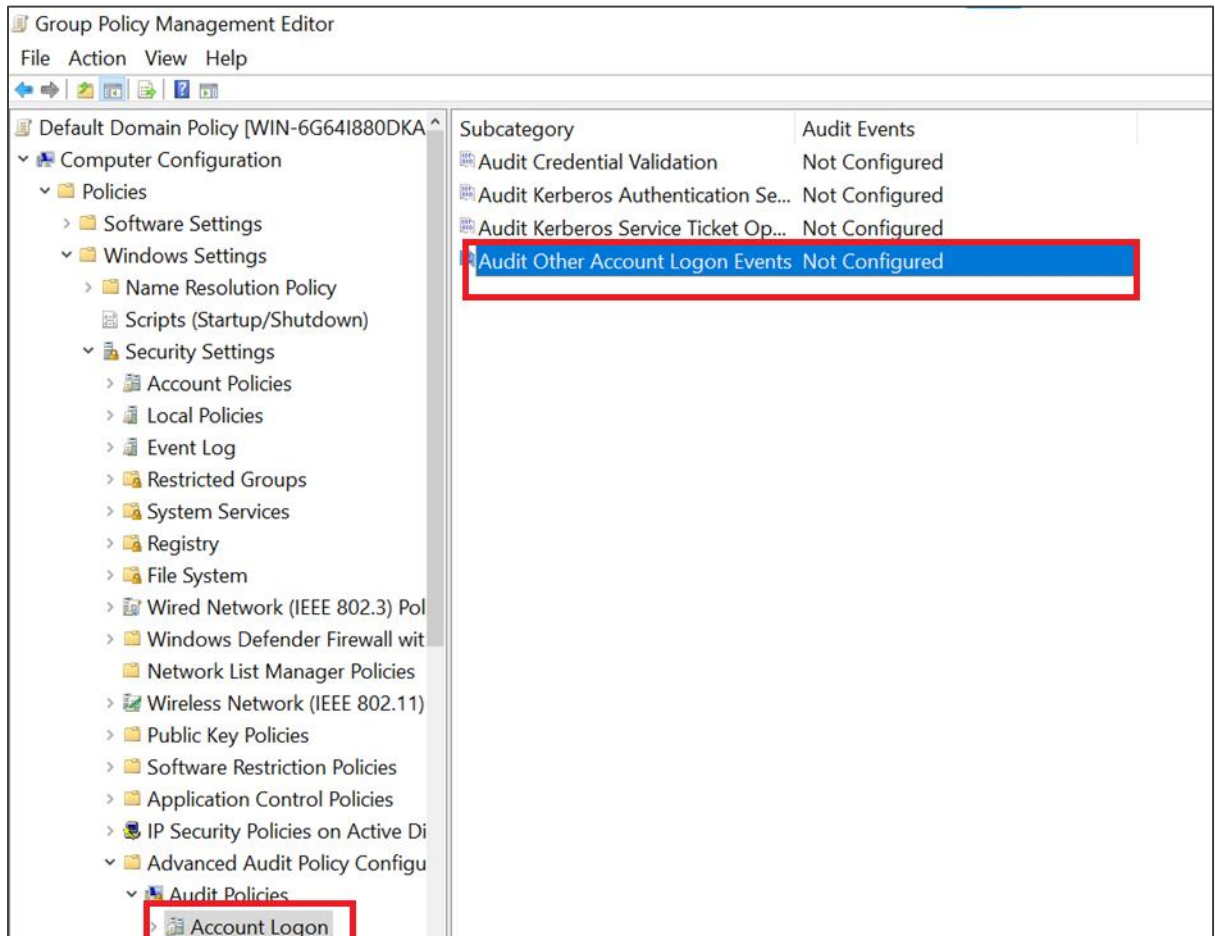
OK Cancel

| All | | | | | | | | | | | | | | | | | | | | | |
|-----------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Sunday | | | | | | | | | | | | | | | | | | | | | |
| Monday | | | | | | | | | | | | | | | | | | | | | |
| Tuesday | | | | | | | | | | | | | | | | | | | | | |
| Wednesday | | | | | | | | | | | | | | | | | | | | | |
| Thursday | | | | | | | | | | | | | | | | | | | | | |
| Friday | | | | | | | | | | | | | | | | | | | | | |
| Saturday | | | | | | | | | | | | | | | | | | | | | |

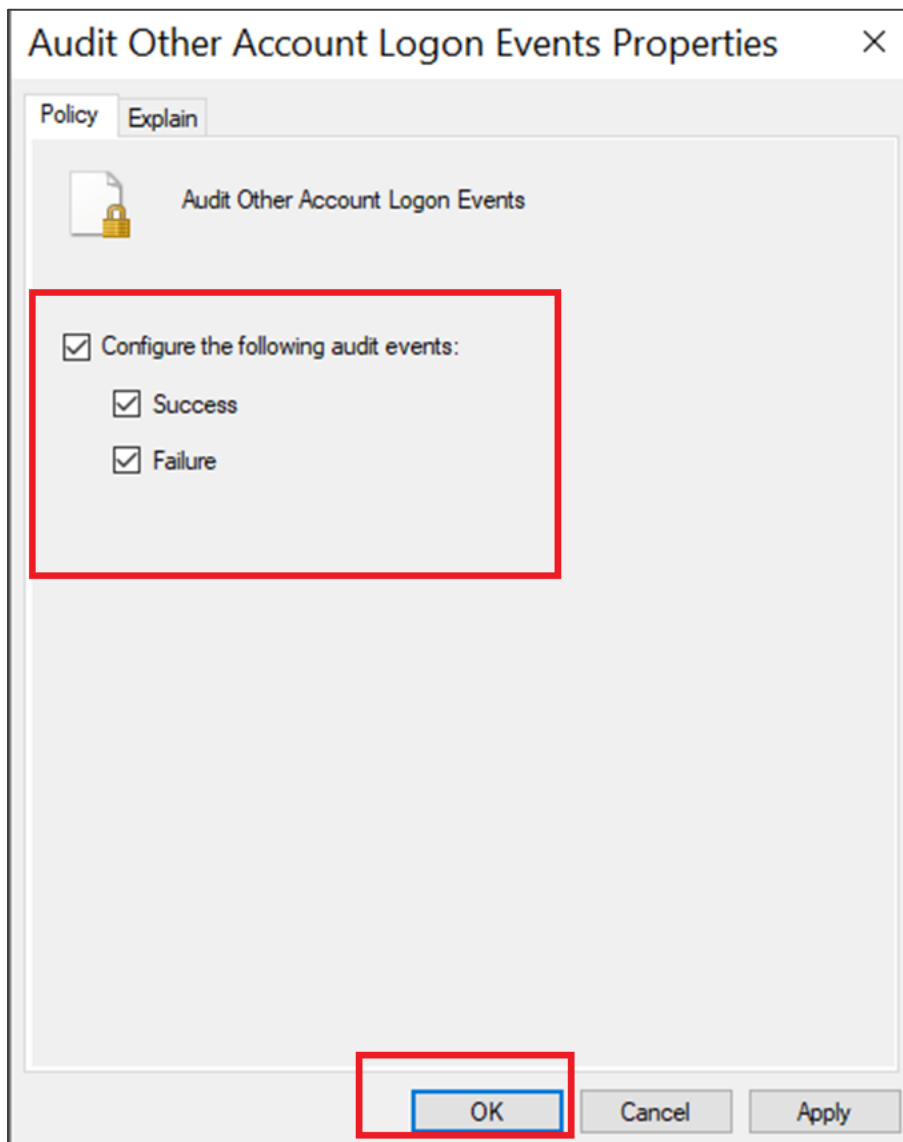
☒ Logon Permitted
☐ Logon Denied

Sunday through Saturday from 7:00 AM to 7:00 PM

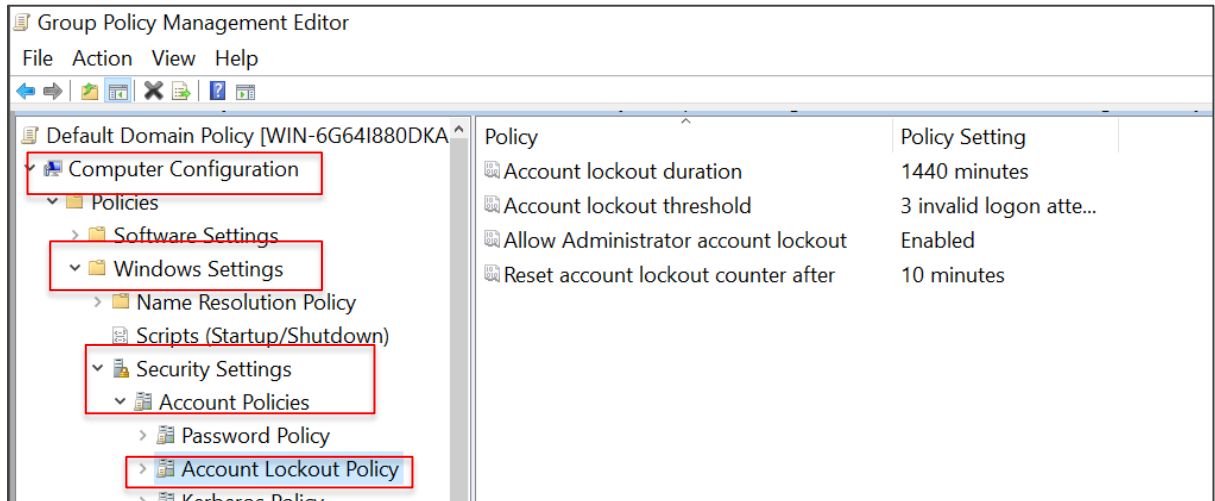
5.10 Now navigate to **Computer Configuration>Windows Setting>Security Settings>Advanced Audit Policy Configuration> Audit Policies> Account Logon**, then click on **Audit other Account Logon Events Not Configured**



5.11 Select both **Success** and **Failure** and click on **OK**

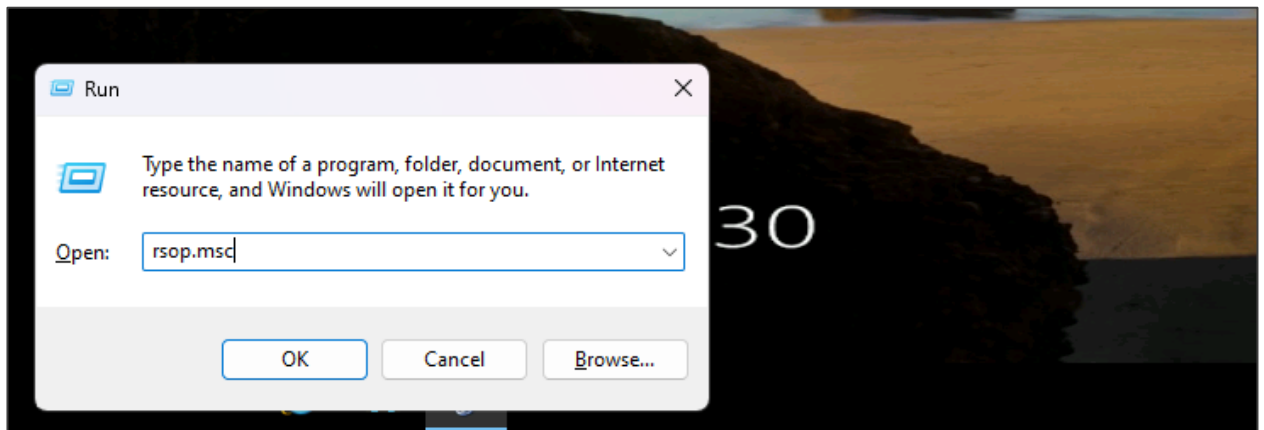


5.12 Navigate to **Computer Configuration>Windows Settings>Security Settings>Account Policies>Account Lockout Policy**




Step 6: Integrate compliance and reporting

6.1 Press windows+r and type **rsop.msc** to generate resultant set of policy (RSOP):



Resultant Set of Policy is being processed...

This Microsoft Management Console contains the RSoP snap-in defined below.

 Starting with Microsoft Windows Vista Service Pack 1 (SP1), the Resultant Set of Policies (RSoP) report does not show all Microsoft Group Policy settings. To see the full set of Microsoft Group Policy settings applied for a computer or user, use the command-line tool gpresult.

Please wait while it is processed.

| Selection | Settings |
|----------------------------------|-----------------------|
| Mode | Logging |
| User name | INDIA\Aviral |
| Display user policy settings | Yes |
| Computer name | INDIA\WIN-6G64I880DKA |
| Display computer policy settings | Yes |

Progress:

By completing these steps, you have successfully integrated Active Directory to enhance user management and compliance within your organization. This integration not only streamlines administrative tasks but also fortifies security protocols.