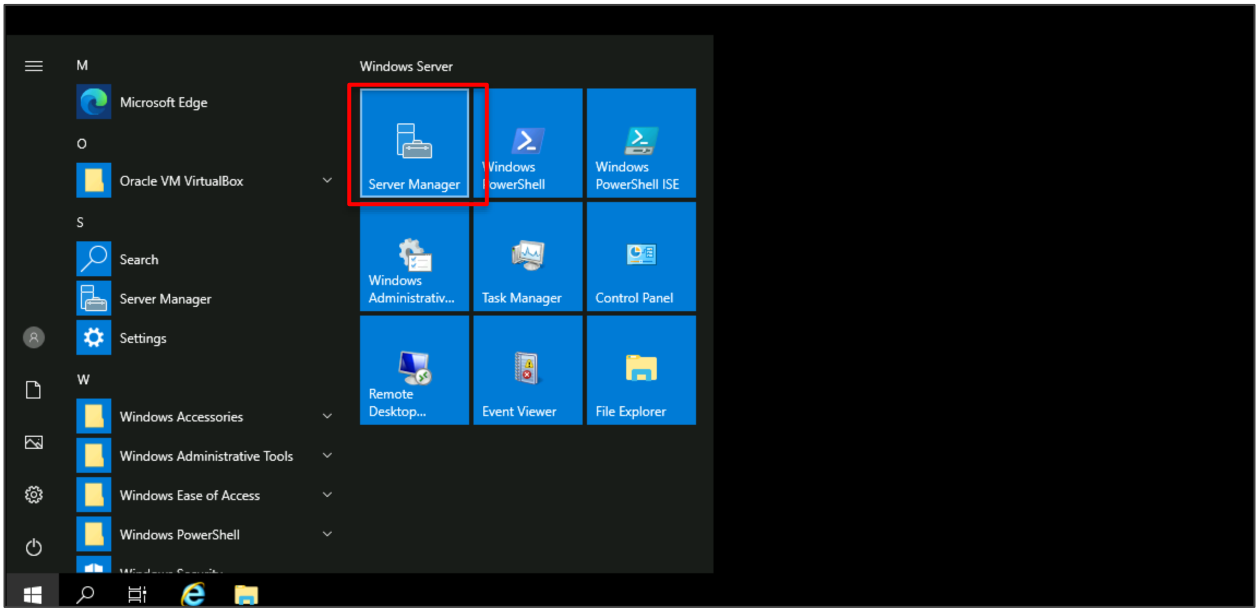
Infrastructure Security: Integrating Active Directory for Enhanced User Management and Compliance

Steps to be followed:

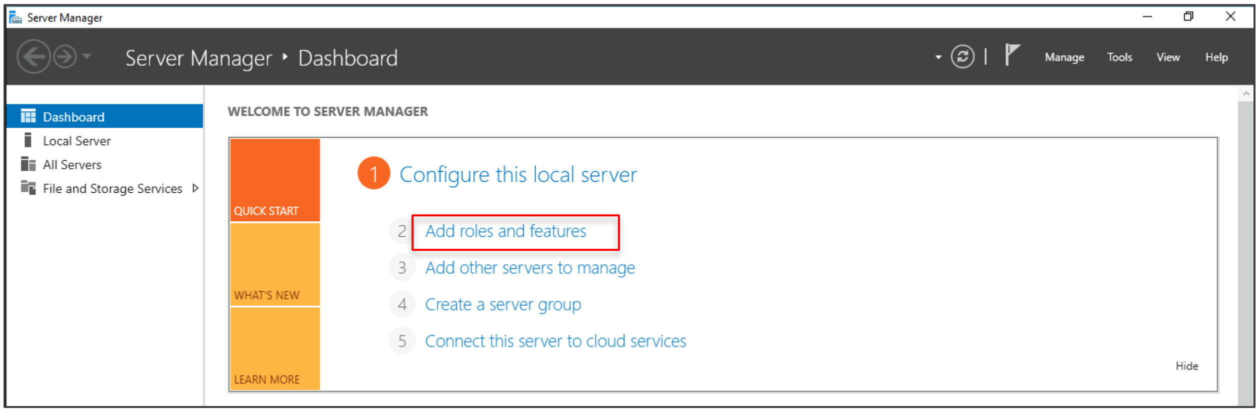
1. Setup active directory
2. Integrate client configuration
3. Create organizational units (OUs) and groups within OUs
4. Create a user management
5. Implement password policies
6. Integrate compliance and reporting

Step 1: Setup active directory

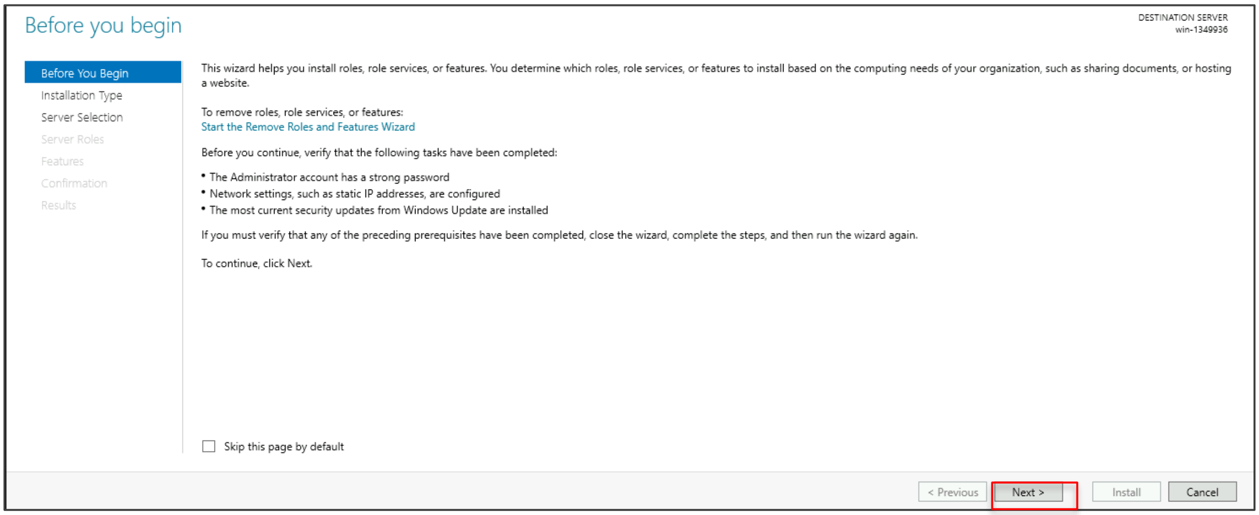
1.1 Click on Windows Key and write Server Manager. Click on **Server Manager**



1.2 Click on **Add roles and features**


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
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

1.3 Click on **Next >**



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

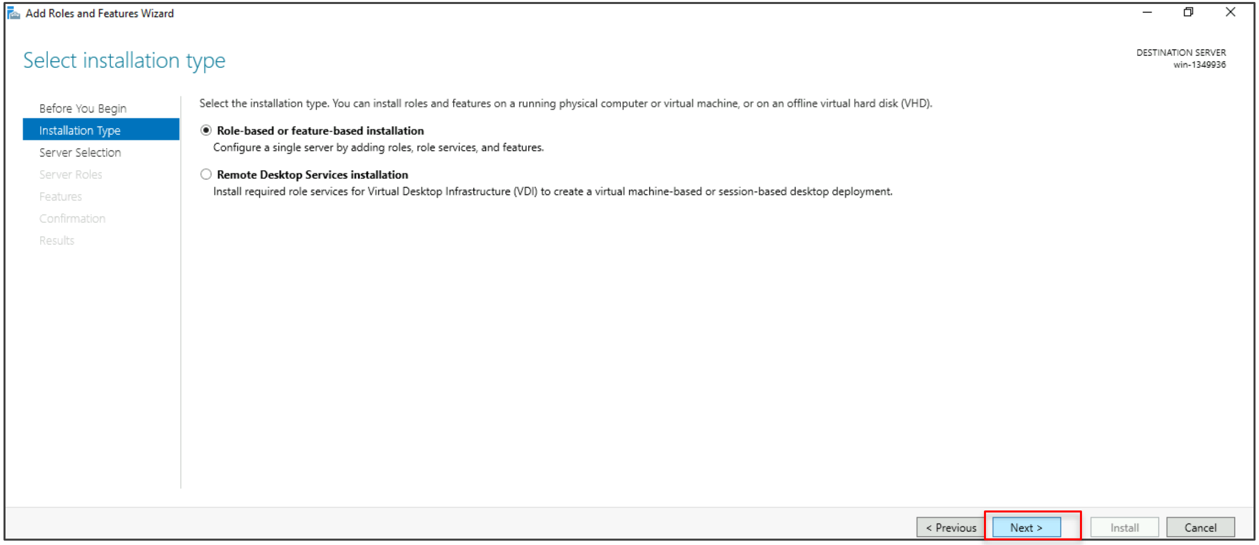
Before you continue, verify that the following tasks have been completed:

- 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



Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
win-1349936

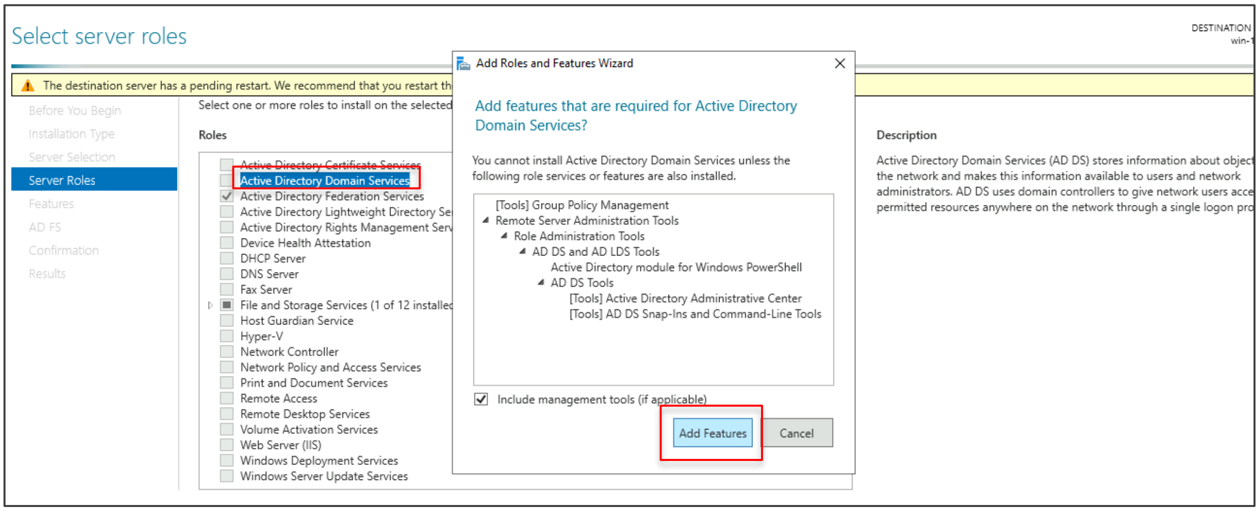
- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

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

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

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



Select server roles

DESTINATION
win-1

⚠ The destination server has a pending restart. We recommend that you restart th

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

Select one or more roles to install on the selected

Roles

□ Active Directory Certificate Services
□ Active Directory Domain Services
☑ Active Directory Federation Services
□ Active Directory Lightweight Directory Se
□ Active Directory Rights Management Serv
□ Device Health Attestation
□ DHCP Server
□ DNS Server
□ Fax Server
▨ File and Storage Services (1 of 12 installed
□ Host Guardian Service
□ Hyper-V
□ Network Controller
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services
□ Web Server (IIS)
□ Windows Deployment Services
□ Windows Server Update Services

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.

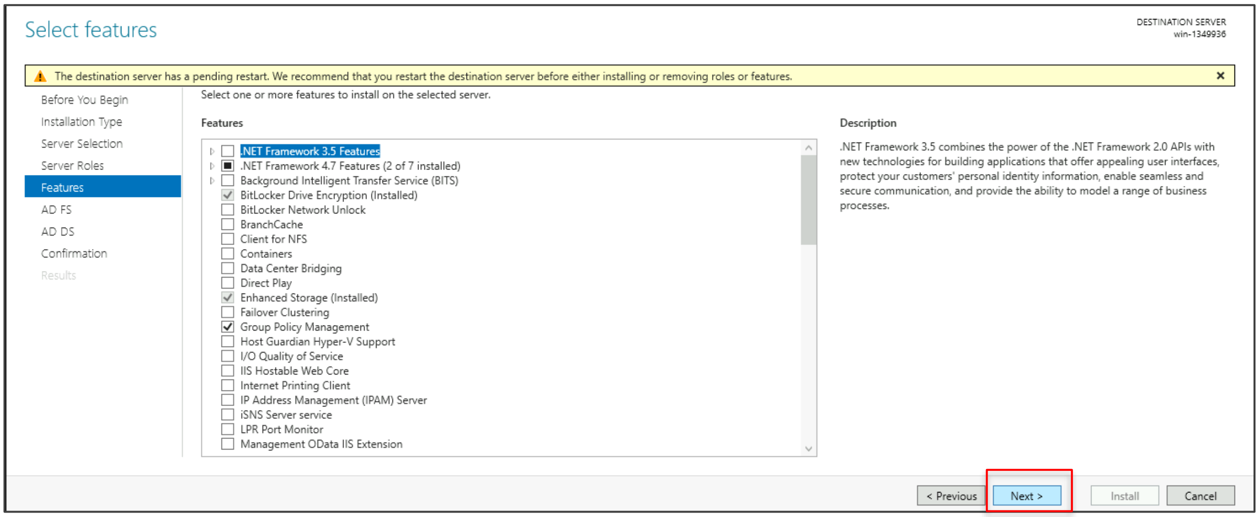
[Tools] Group Policy Management
- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
      - AD DS Tools
        - [Tools] Active Directory Administrative Center
        - [Tools] AD DS Snap-Ins and Command-Line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

☑ Include management tools (if applicable)

Description

Active Directory Domain Services (AD DS) stores information about object the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users acce permitted resources anywhere on the network through a single logon pro

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. ✕

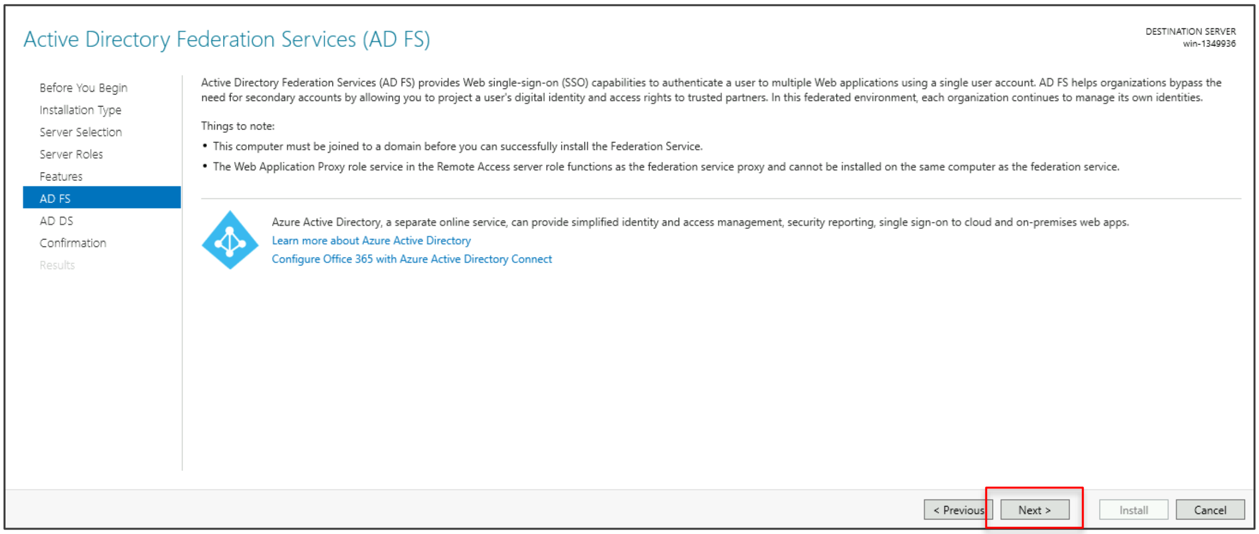
Select one or more features to install on the selected server.

Features

- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.7 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- ☑ BitLocker Drive Encryption (Installed)
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Containers
- □ Data Center Bridging
- □ Direct Play
- ☑ Enhanced Storage (Installed)
- □ 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
- □ iSNS Server service
- □ LPR Port Monitor
- □ Management OData IIS Extension

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.



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:

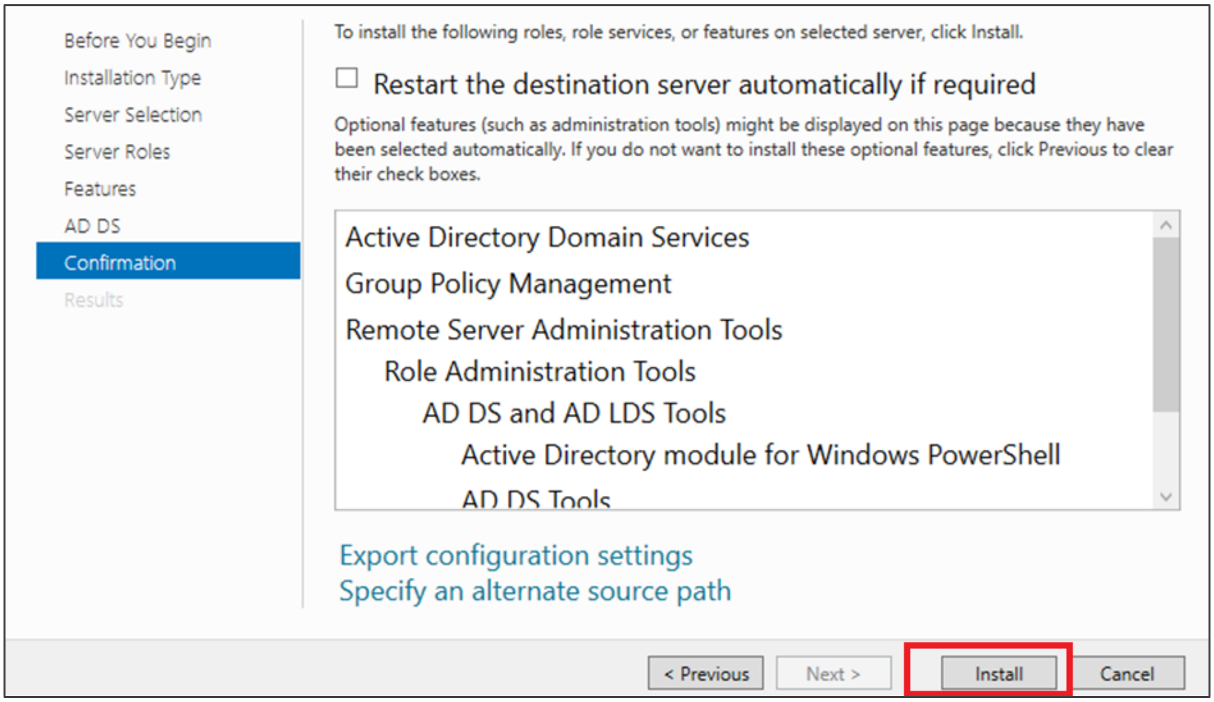
- This computer must be joined to a domain before you can successfully install the Federation Service.
- The Web Application Proxy role service in the Remote Access server role functions as the federation service proxy and cannot be installed on the same computer as the federation service.

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

1.6 Click on **Install**



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

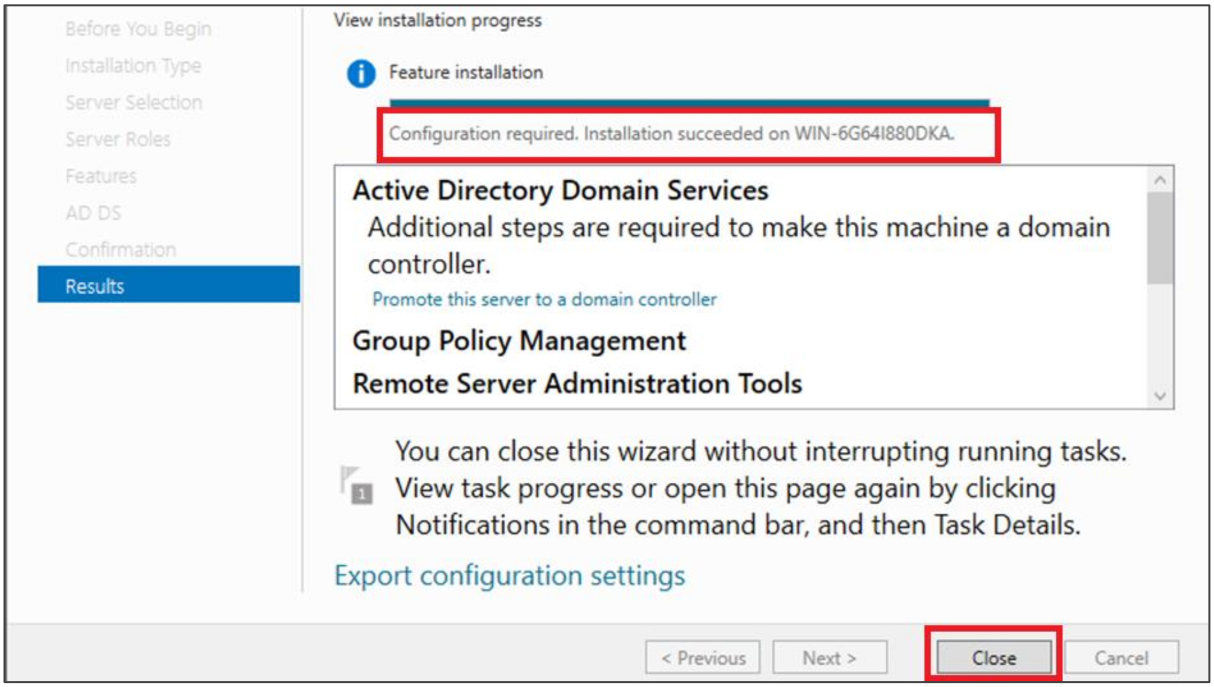
□ Restart the destination server automatically if required

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

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

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



View installation progress

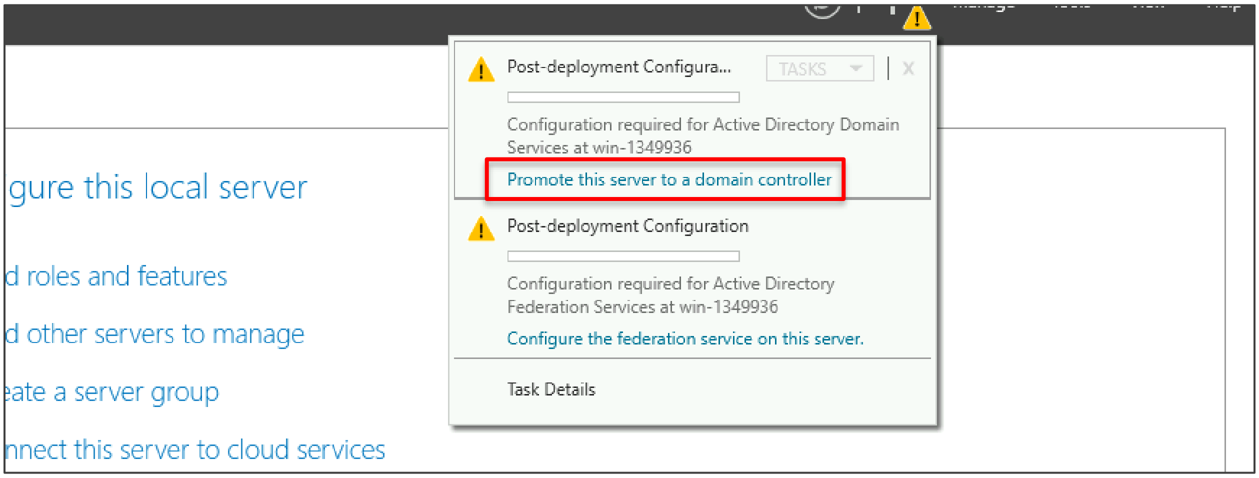
Feature installation

Configuration required. Installation succeeded on WIN-6G64I880DKA.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools

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.

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**



Post-deployment Configura...

Configuration required for Active Directory Domain Services at win-1349936

Promote this server to a domain controller

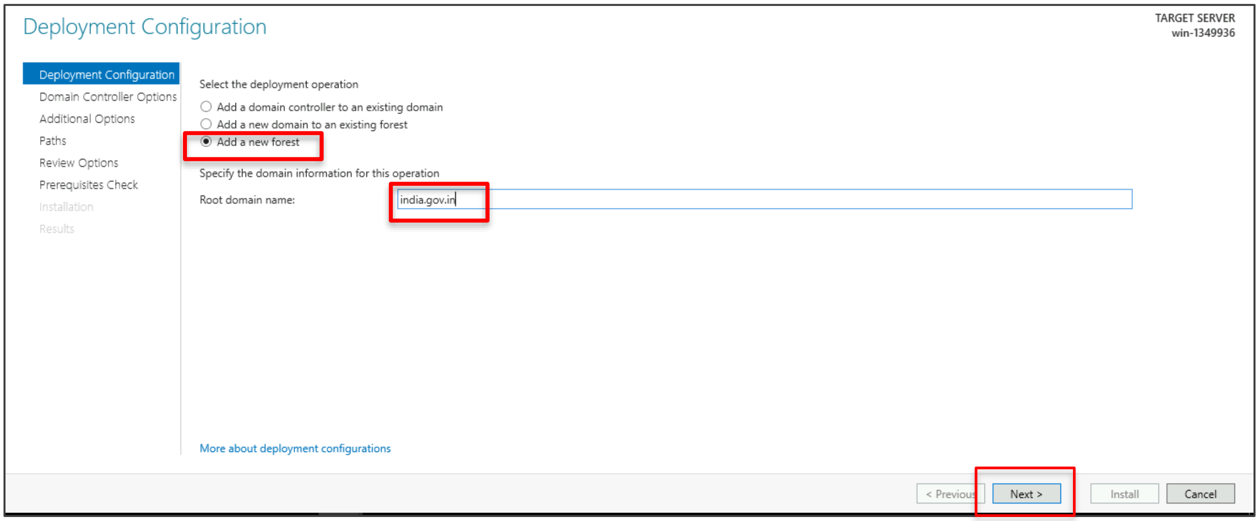
Post-deployment Configuration

Configuration required for Active Directory Federation Services at win-1349936

Configure the federation service on this server.

Task Details

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



Deployment Configuration

TARGET SERVER
win-1349936

Select the deployment operation

○ Add a domain controller to an existing domain

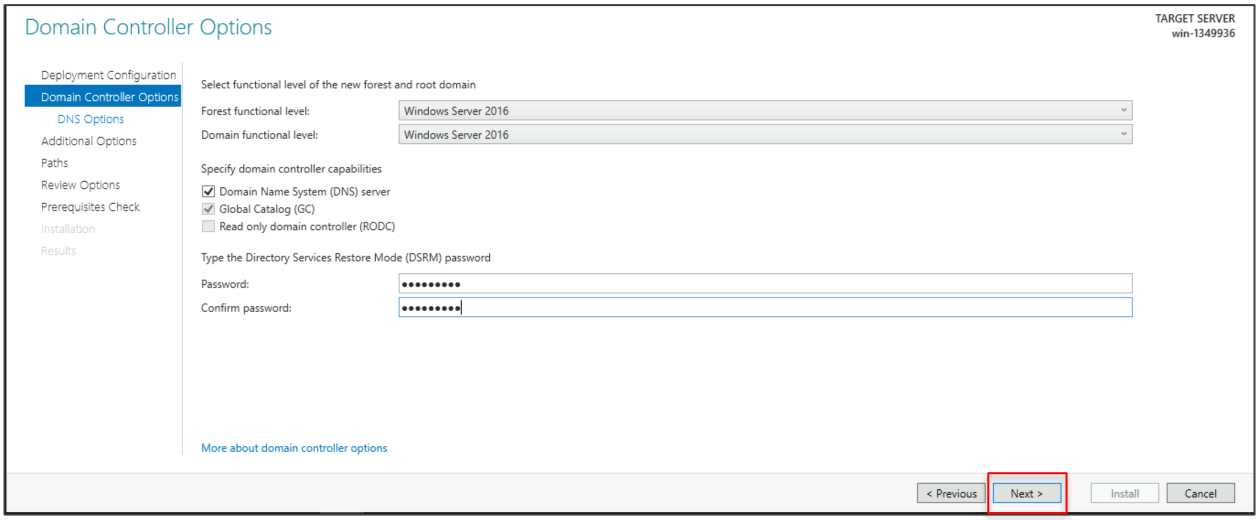
○ Add a new domain to an existing forest

● Add a new forest

Specify the domain information for this operation

Root domain name: india.gov.in

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



Domain Controller Options

TARGET SERVER
win-1349936

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)

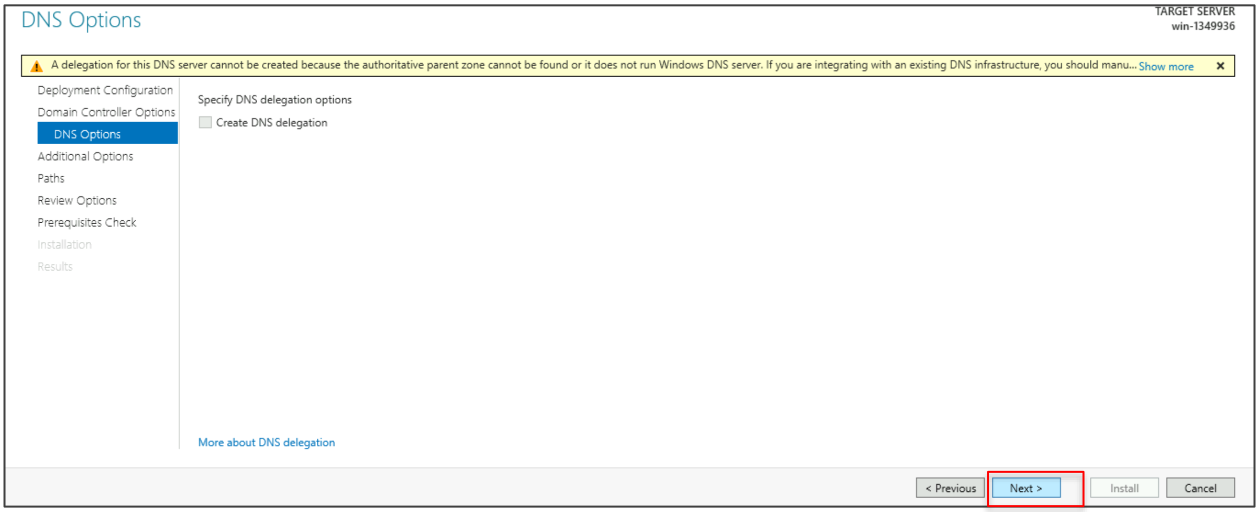
Type the Directory Services Restore Mode (DSRM) password

Password: •••••••••

Confirm password: •••••••••

More about domain controller options

1.11 Click **Next >**



DNS Options

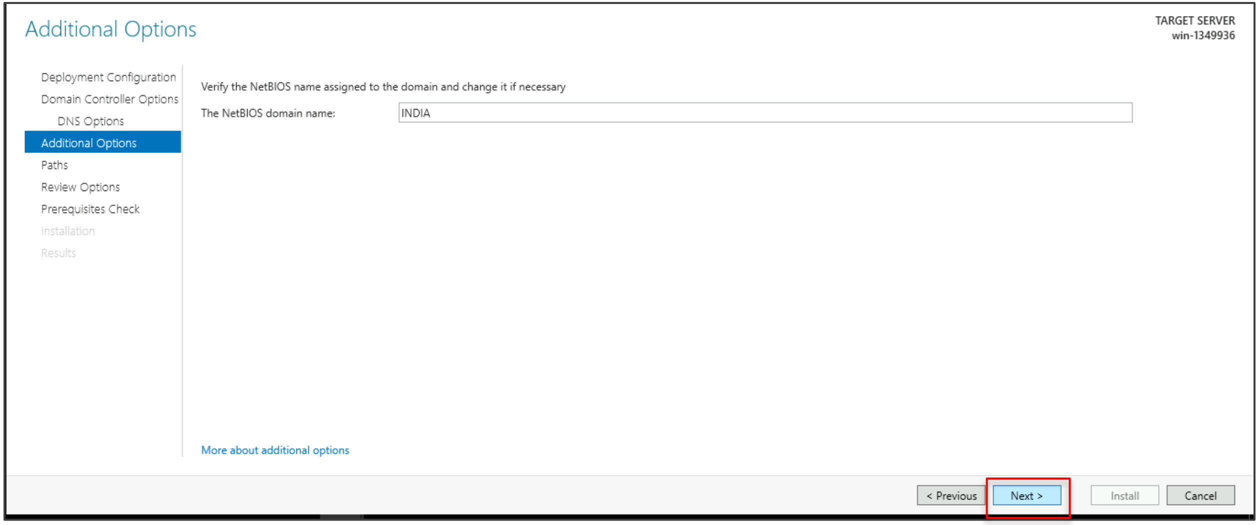
TARGET SERVER
win-1349936

⚠ 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

Specify DNS delegation options

☐ Create DNS delegation

More about DNS delegation



Additional Options

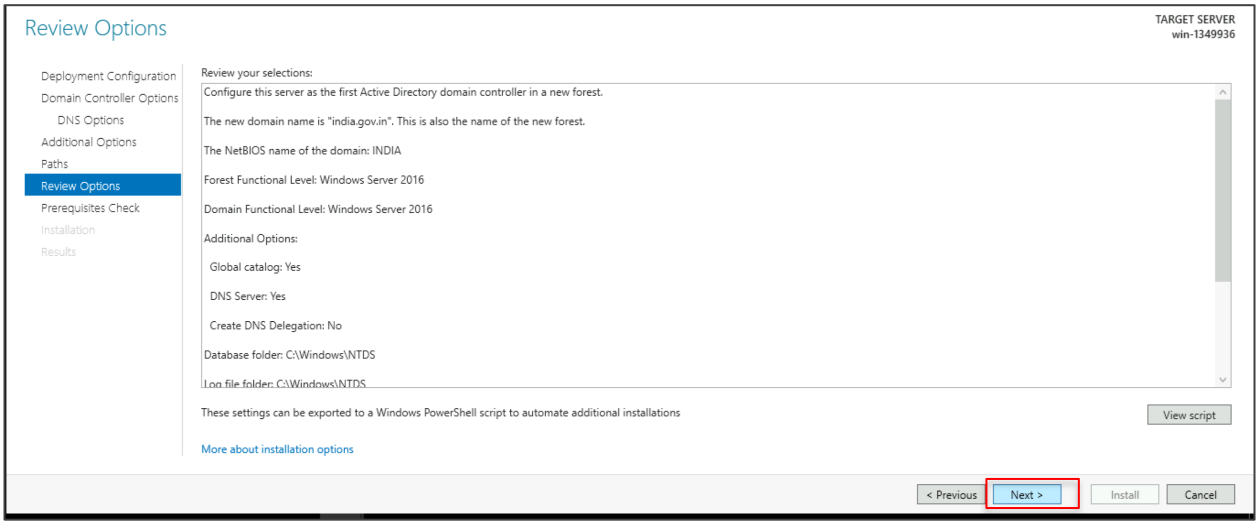
TARGET SERVER
win-1349936

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

The NetBIOS domain name: INDIA

More about additional options

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



Review Options

TARGET SERVER
win-1349936

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

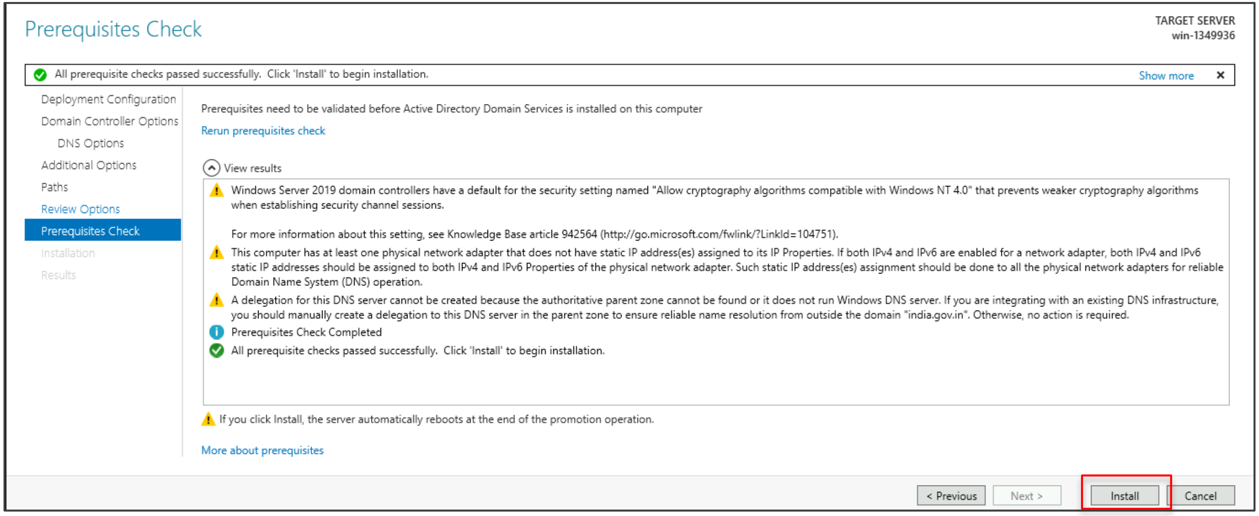
Create DNS Delegation: No

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



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

⚠ Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

⚠ This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network 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.

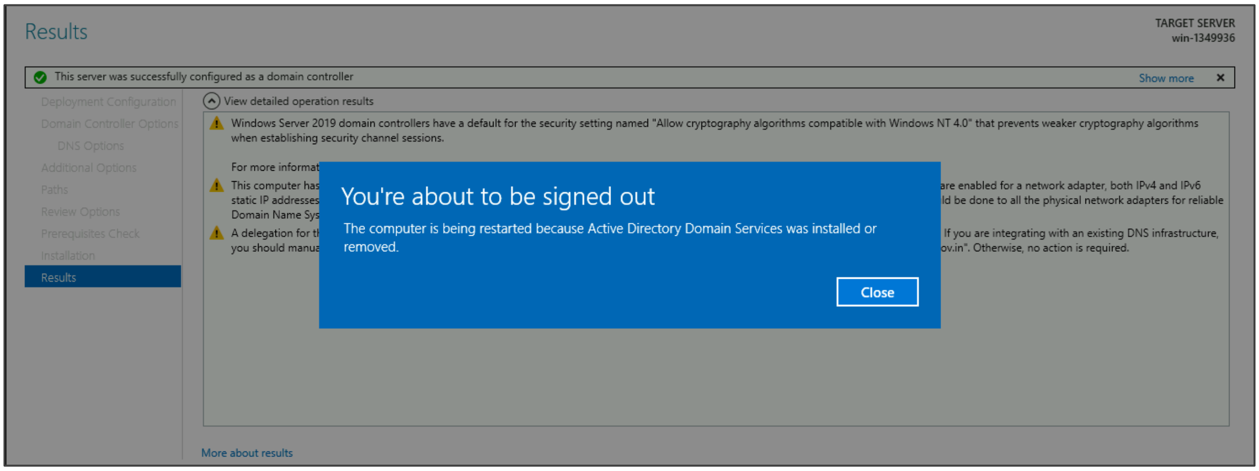
⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "india.gov.in". 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.

1.13 Click on **Close**



This server was successfully configured as a domain controller

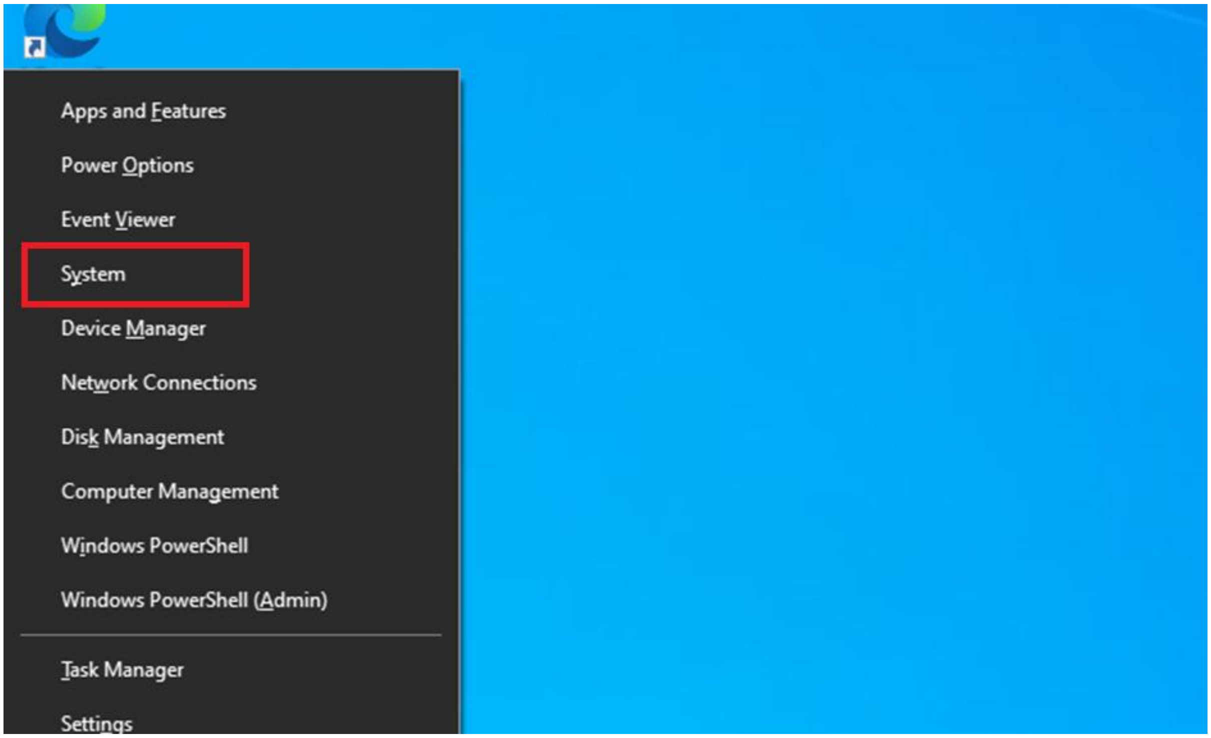
⚠ Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

You're about to be signed out

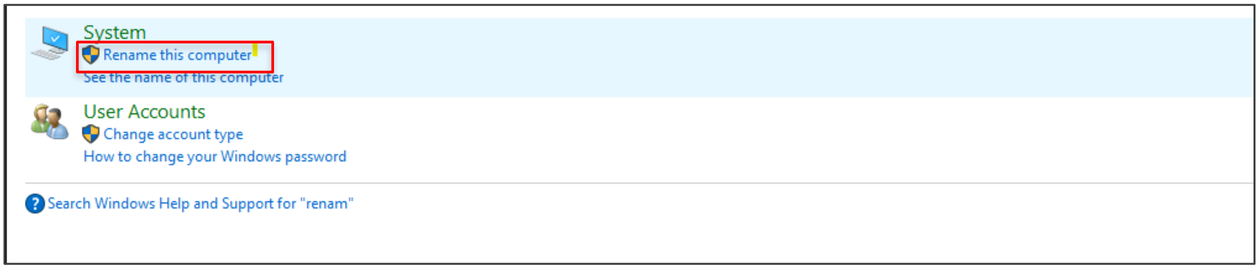
The computer is being restarted because Active Directory Domain Services was installed or removed.

Step 2: Integrate client configuration

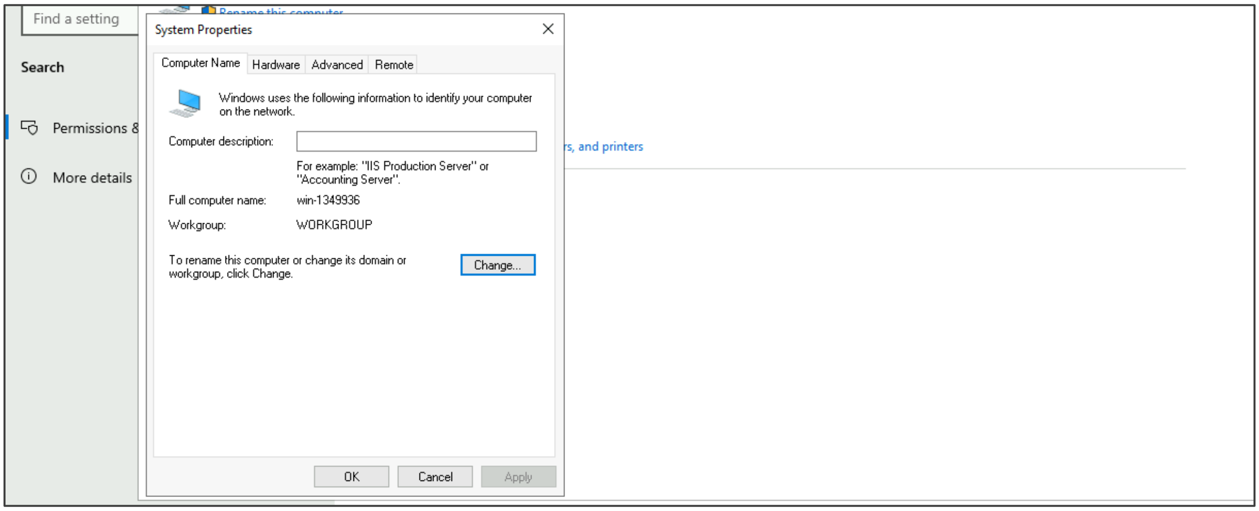
2.1 Start a Windows 10 OS and press windows+x and select the **System**



2.2 Click on **Rename this computer**


System
Rename this computer
See the name of this computer
User Accounts
Change account type
How to change your Windows password
Search Windows Help and Support for "renam"

2.3 Click on **Change**



Windows uses the following information to identify your computer on the network.

Computer description:

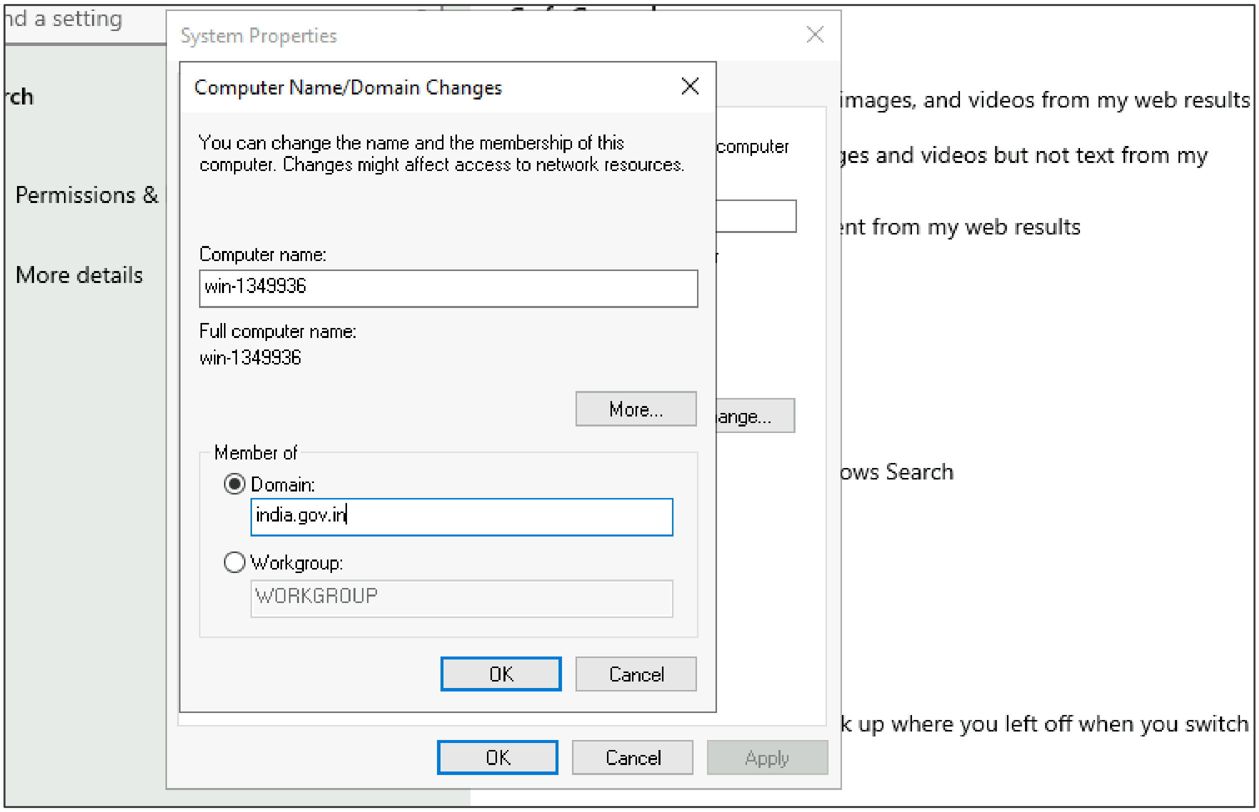
For example: "IIS Production Server" or "Accounting Server".

Full computer name: win-1349936

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

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


nd a setting
rch
Permissions &
More details
System Properties
images, and videos from my web results
computer
ges and videos but not text from my
nt from my web results
ange...
ows Search
k up where you left off when you switch
Computer Name/Domain Changes
More...
OK
Cancel
OK
Cancel
Apply

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: win-1349936

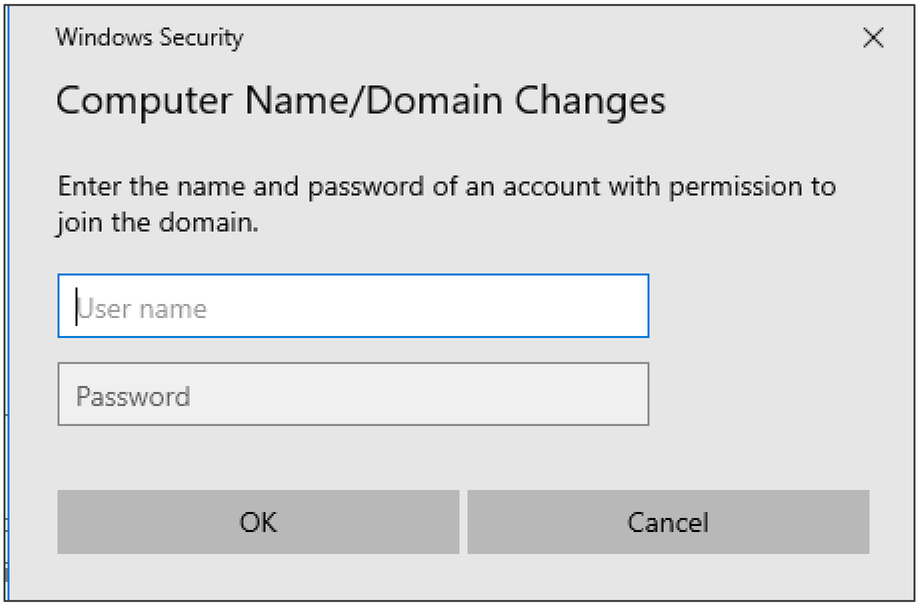
Full computer name: win-1349936

Member of

● Domain: india.gov.in

○ Workgroup: WORKGROUP

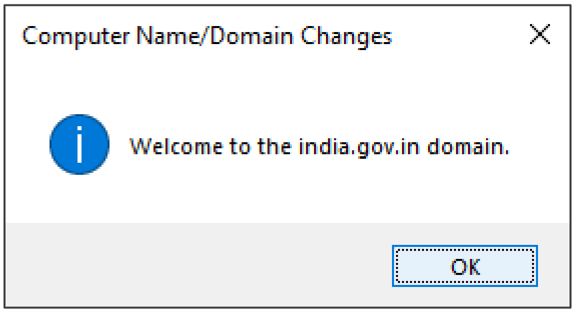
2.5 Login with an administrator account on Windows Server 2022


Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

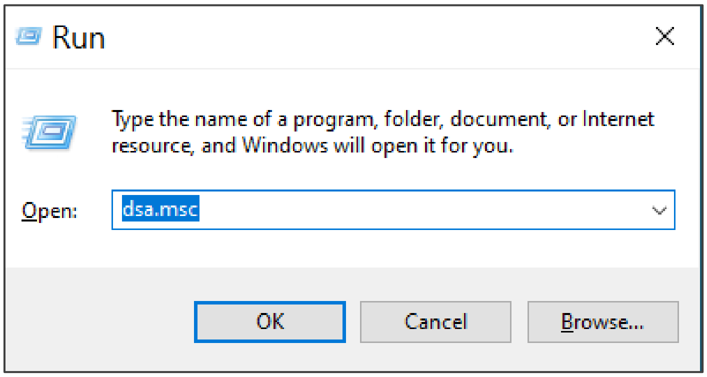
2.6 Upon successful login, the current system will join the domain, click on **OK**


Computer Name/Domain Changes

Welcome to the india.gov.in domain.

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

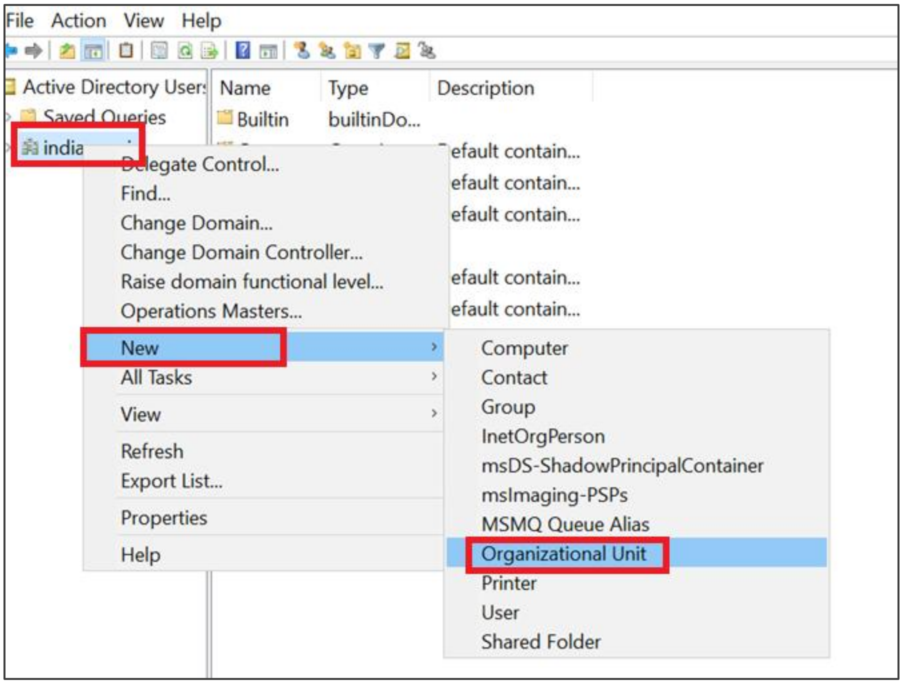
3.1 Press windows + r and type **dsa.msc**


Run

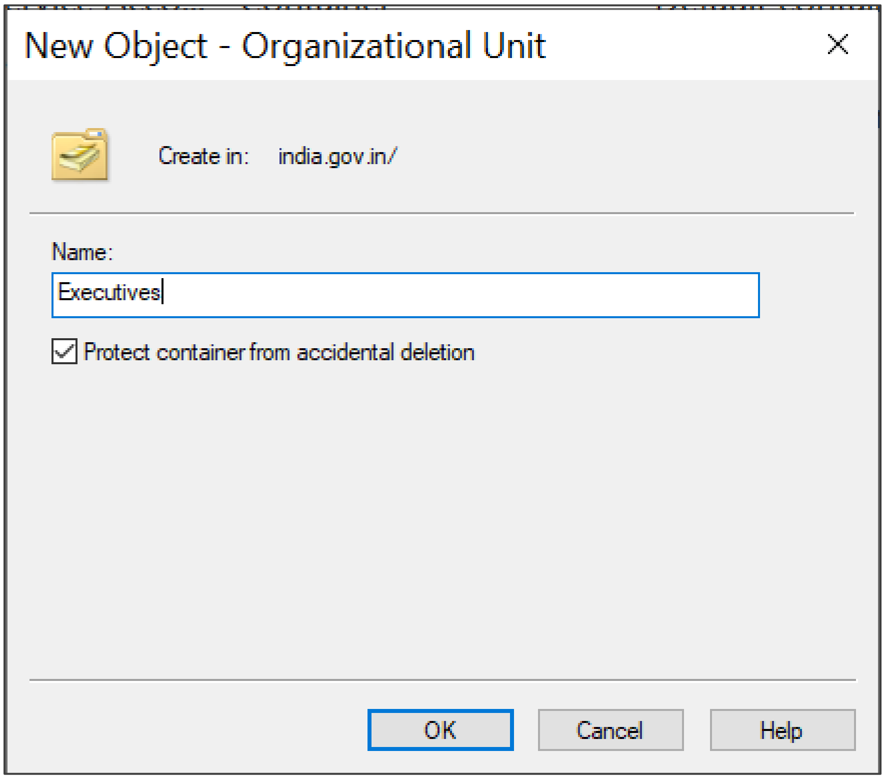
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: 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**

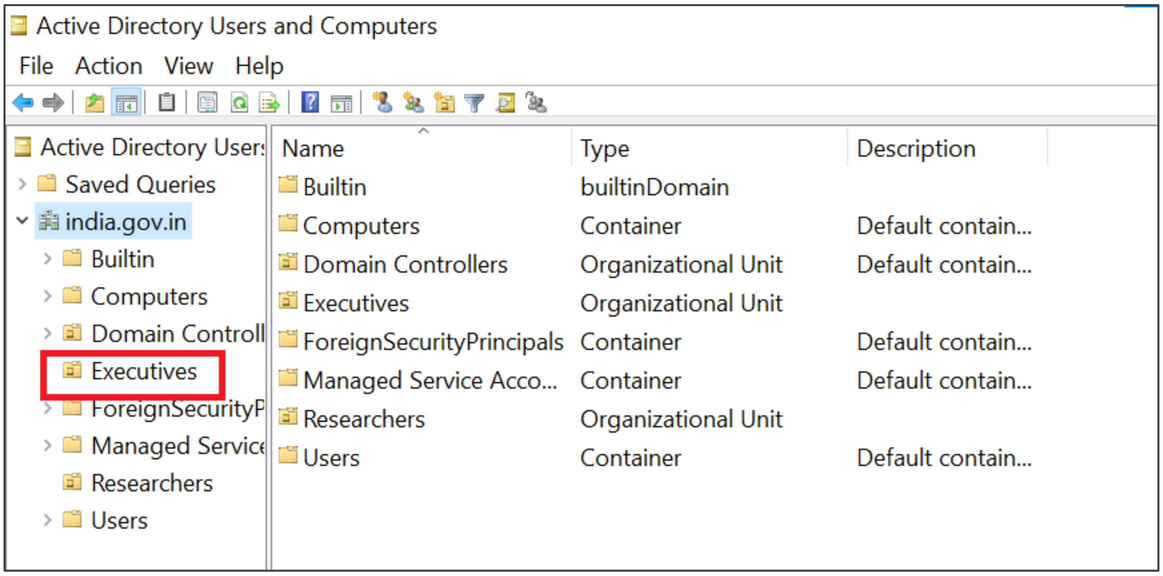


Create in: india.gov.in/

Name: Executives

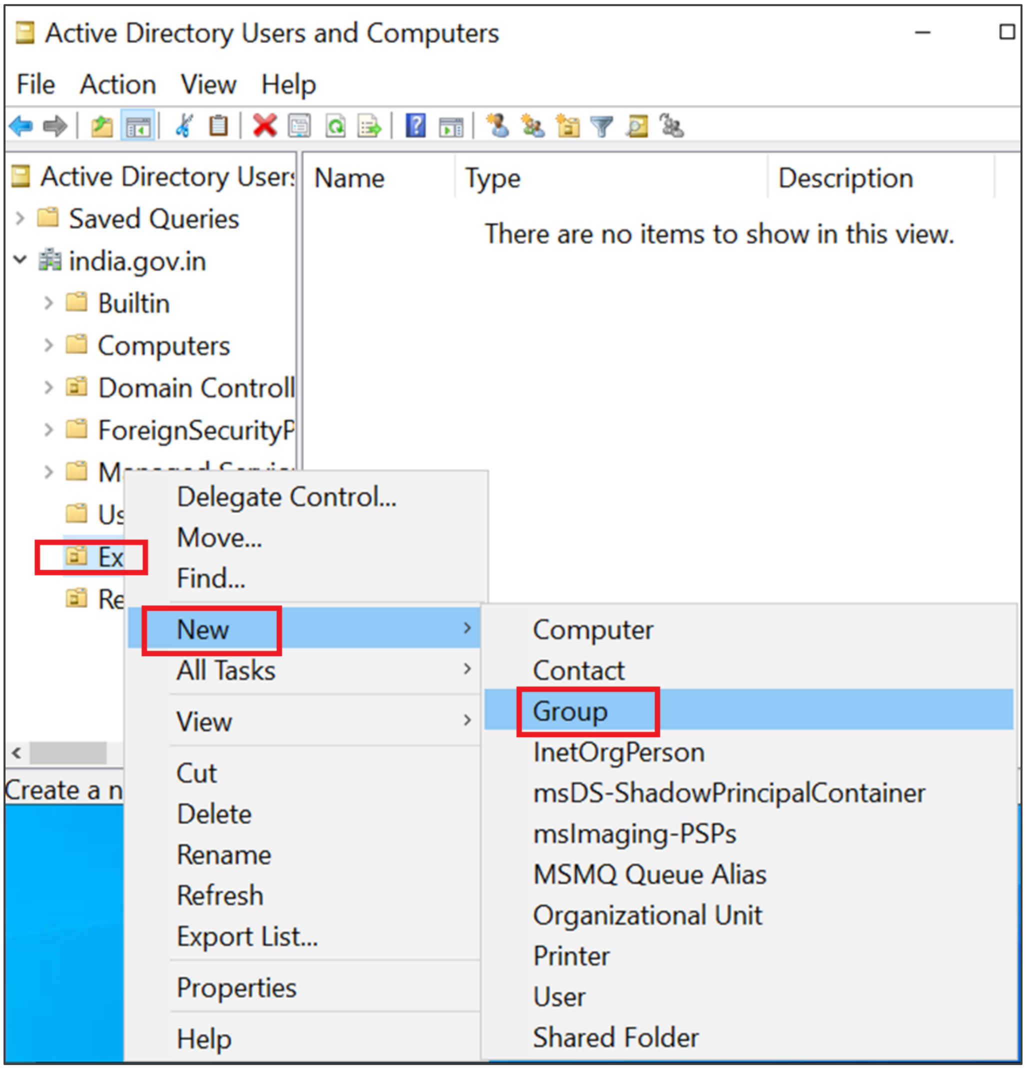
☑ Protect container from accidental deletion

Executives OU is visible in the left tree pane:



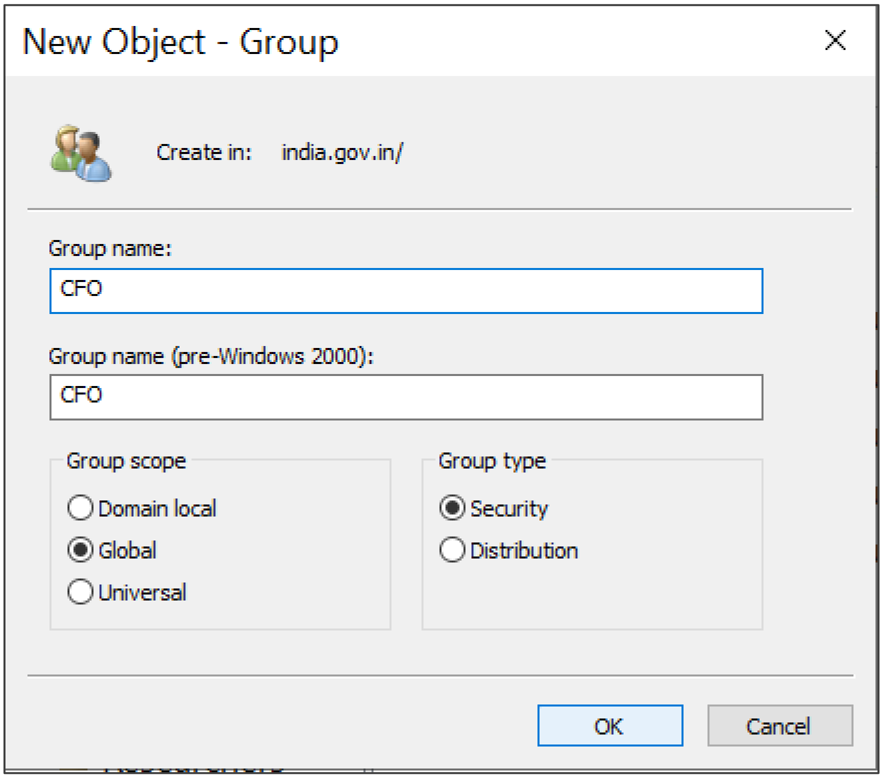
Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default contain...
Domain Controllers	Organizational Unit	Default contain...
Executives	Organizational Unit	
ForeignSecurityPrincipals	Container	Default contain...
Managed Service Acco...	Container	Default contain...
Researchers	Organizational Unit	
Users	Container	Default contain...

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



There are no items to show in this view.

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

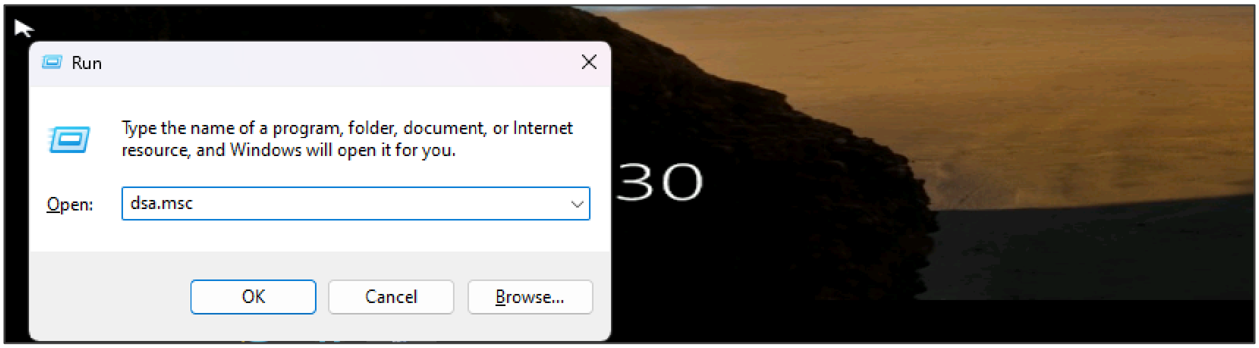
Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Note : Similarly create other groups.

Step 4: Create a user management

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

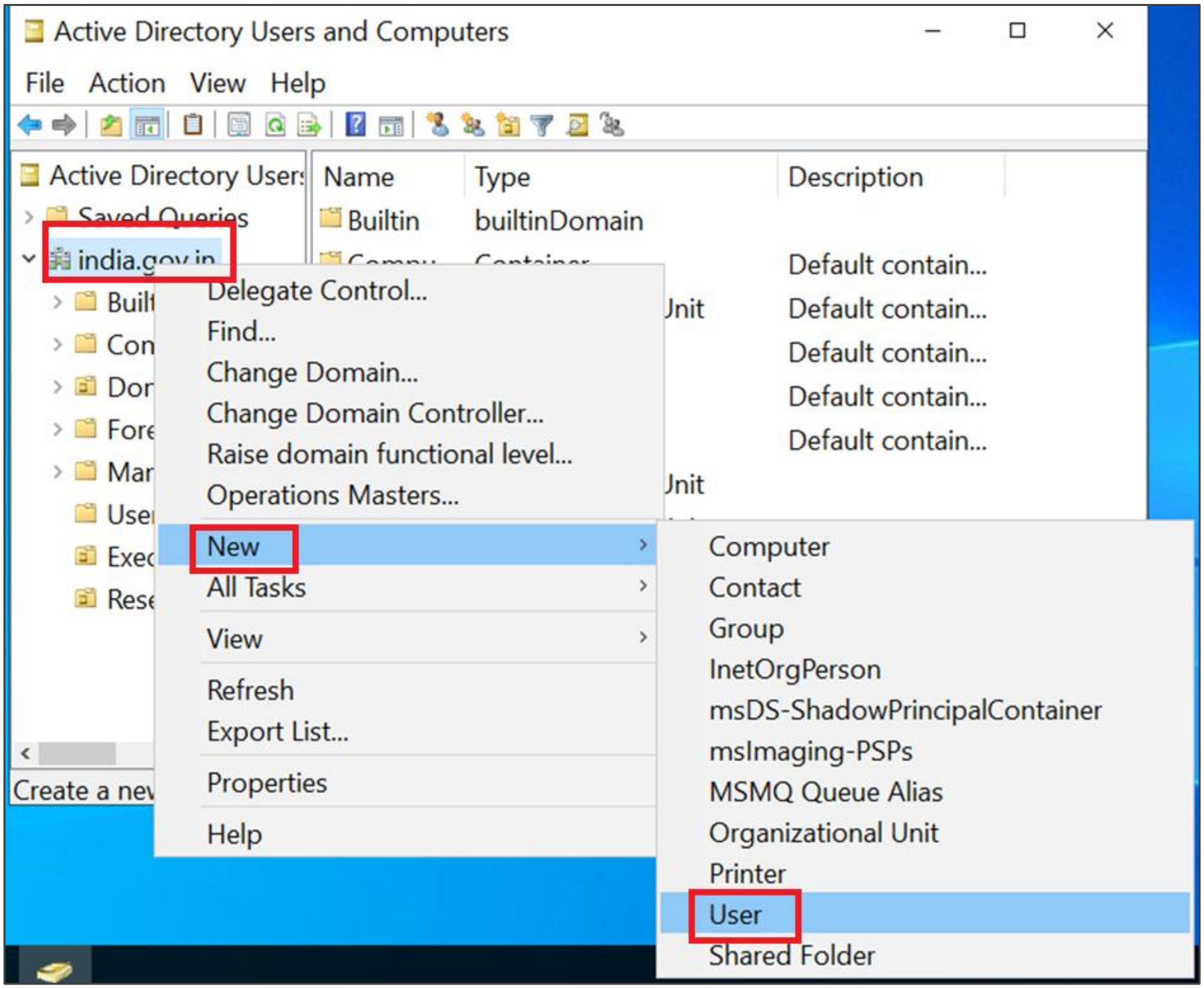


Run

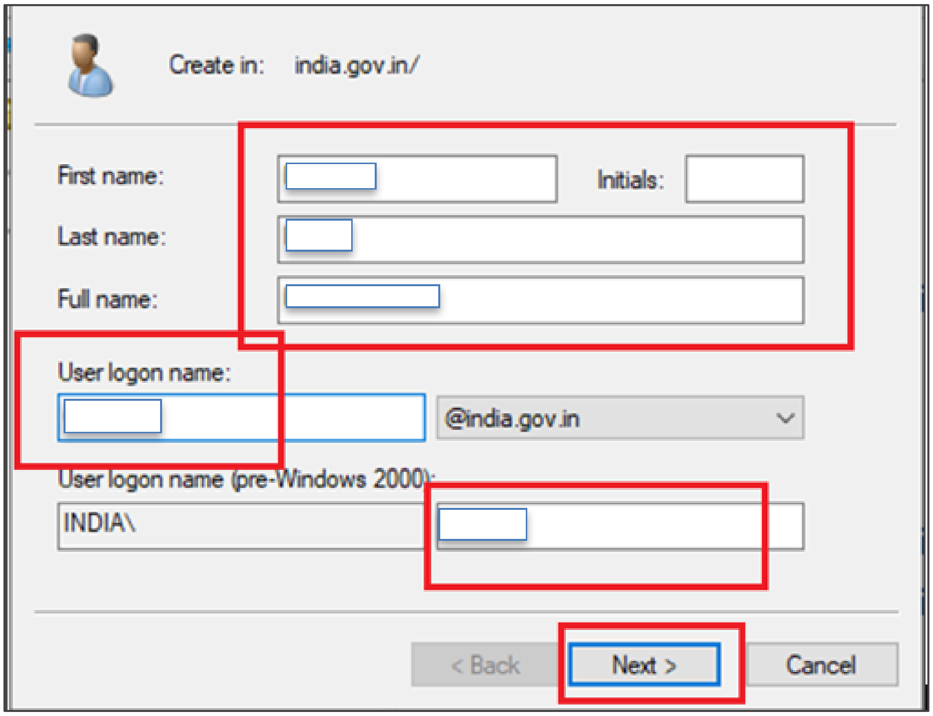
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: 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:

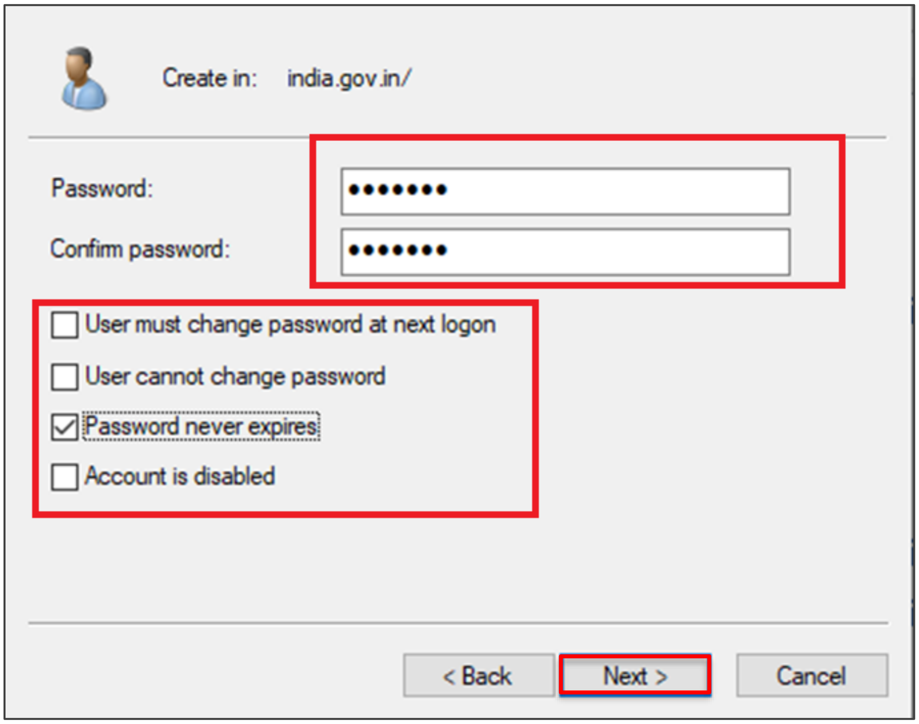
Last name:

Full name:

User logon name: @india.gov.in

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

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: •••••••

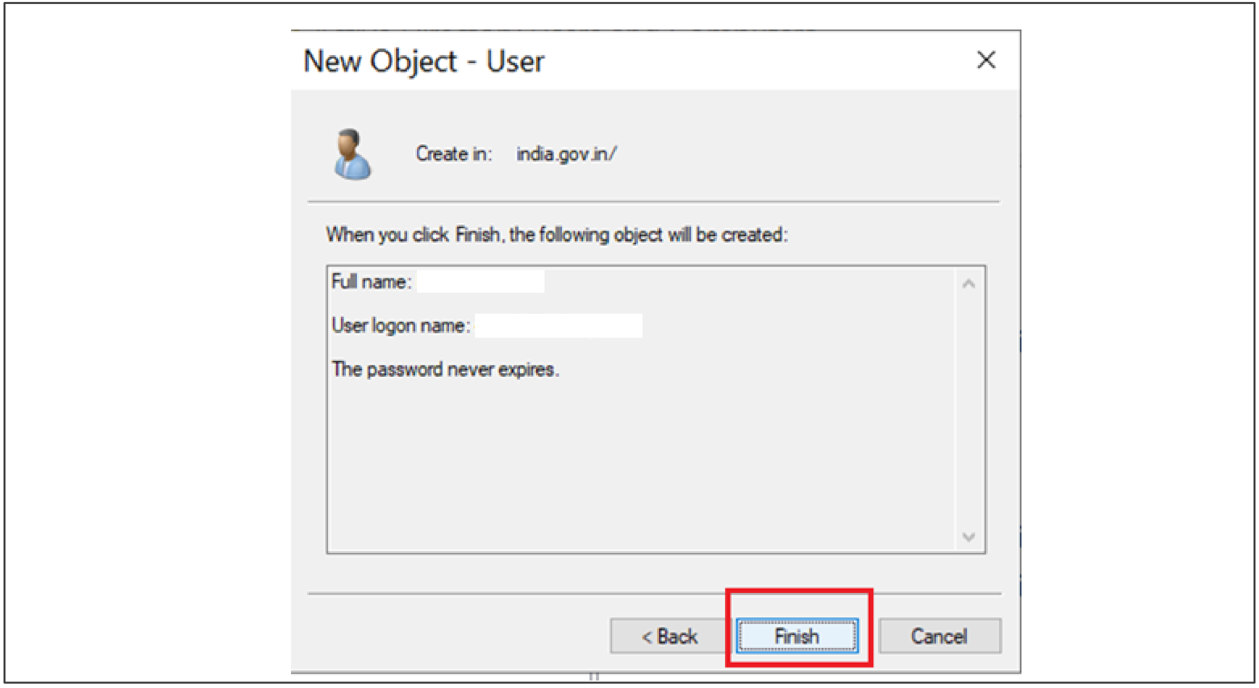
Confirm password: •••••••

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled



Create in: india.gov.in/

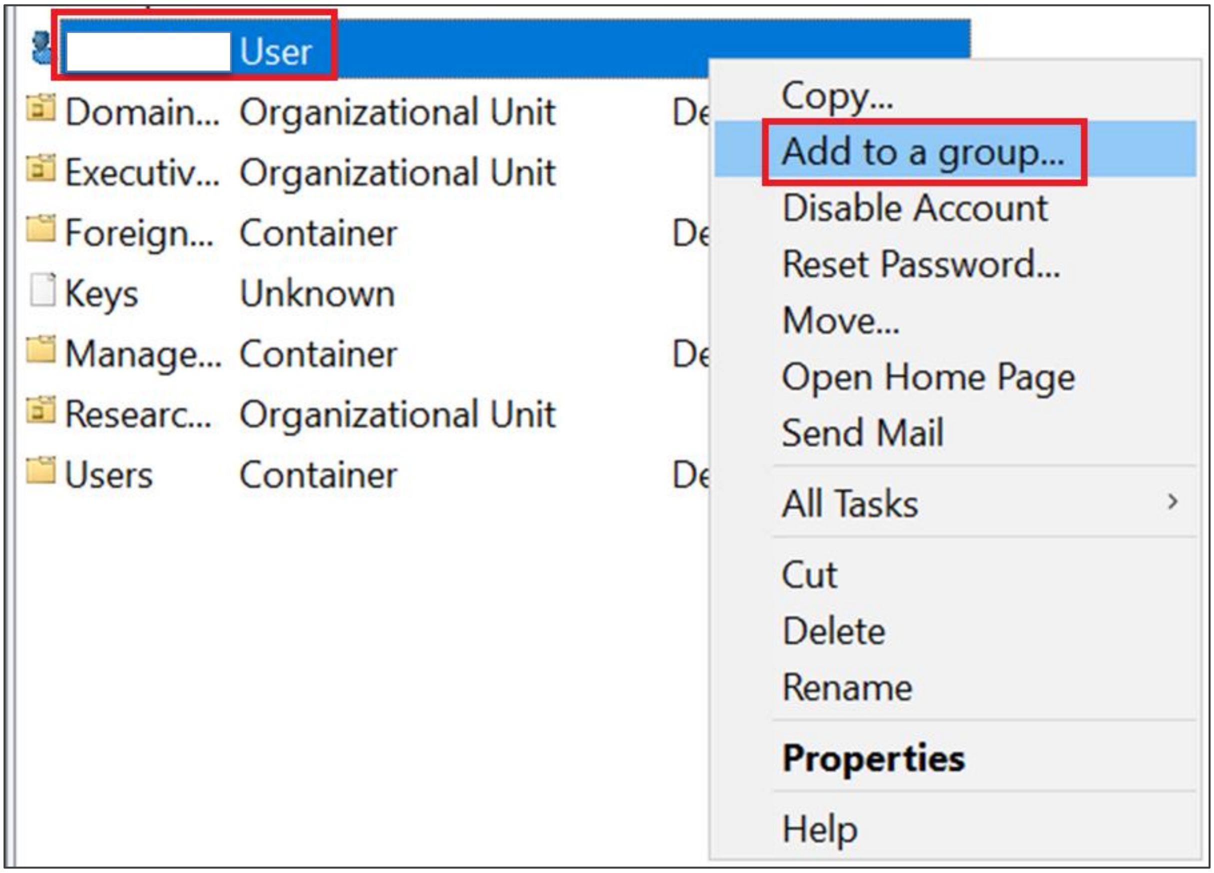
When you click Finish, the following object will be created:

Full name:

User logon name:

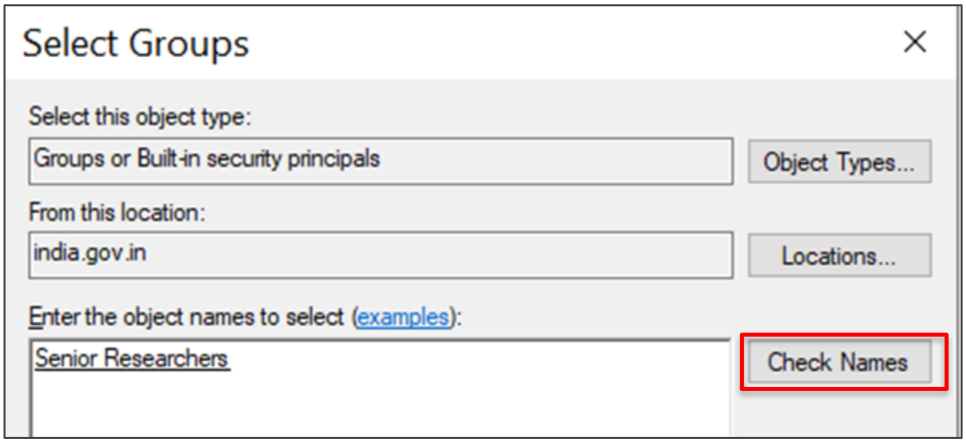
The password never expires.

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



	User	
Domain...	Organizational Unit	De
Executiv...	Organizational Unit	
Foreign...	Container	De
Keys	Unknown	
Manage...	Container	De
Researc...	Organizational Unit	
Users	Container	De

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



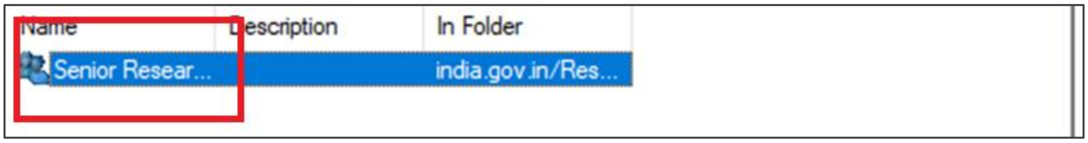
Select Groups

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

From this location:
india.gov.in

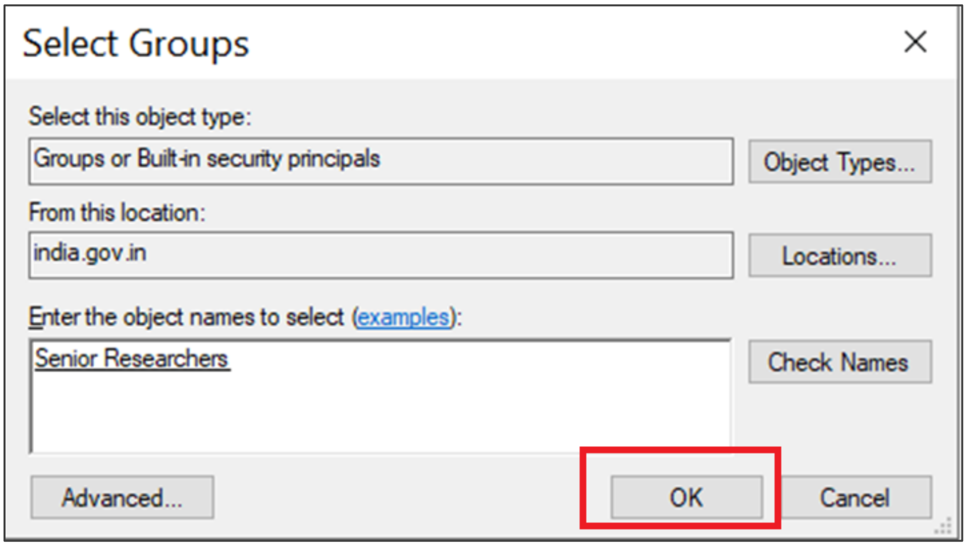
Enter the object names to select (examples):
Senior Researchers

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**

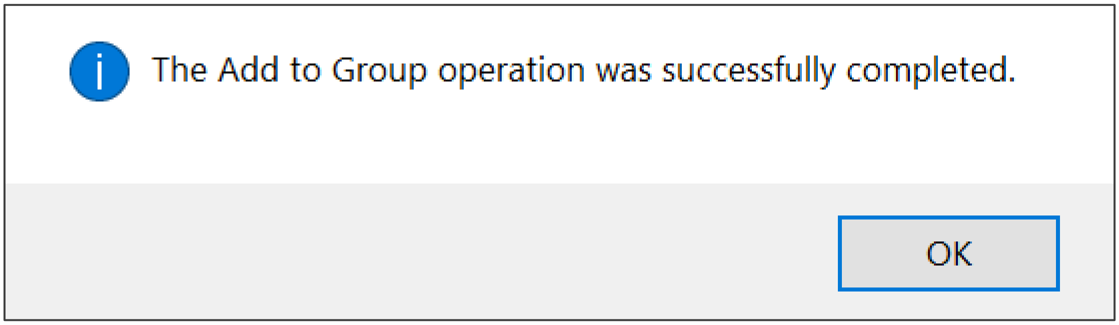


Select Groups

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

From this location:
india.gov.in

Enter the object names to select (examples):
Senior Researchers

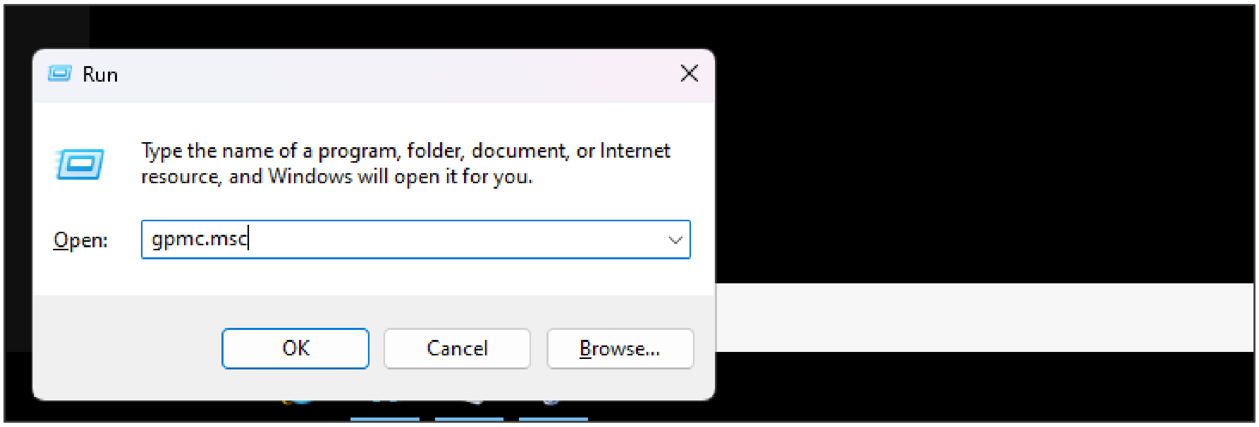


The Add to Group operation was successfully completed.

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

Step 5: Implement password policies

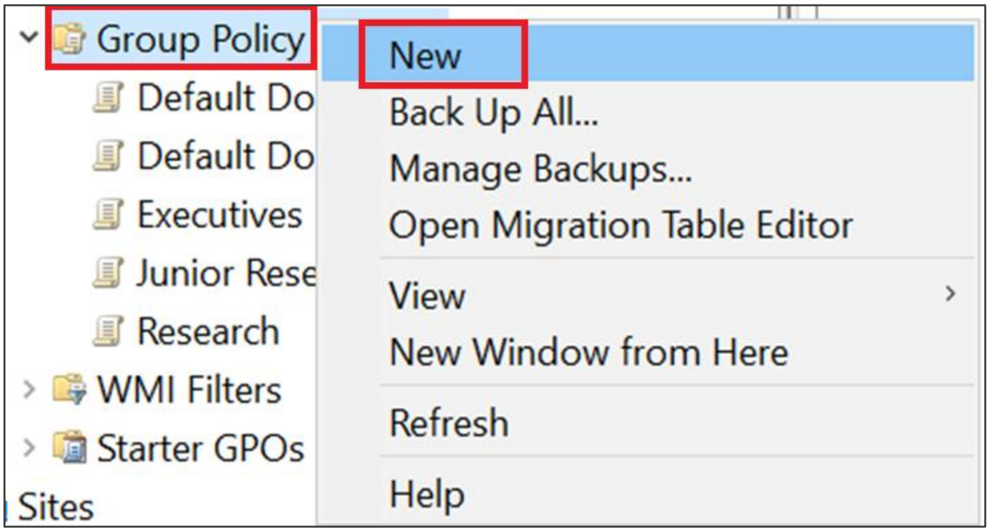
5.1 After signing in to Windows 10 client system using newly created domain user press windows+r and type **gpmc.msc** and click **OK**



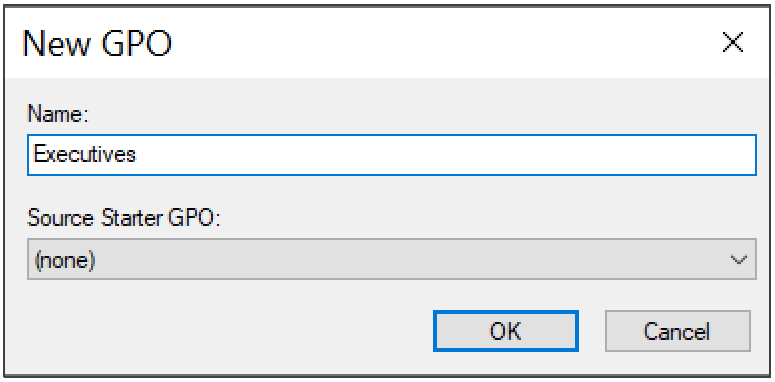
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpmc.msc

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



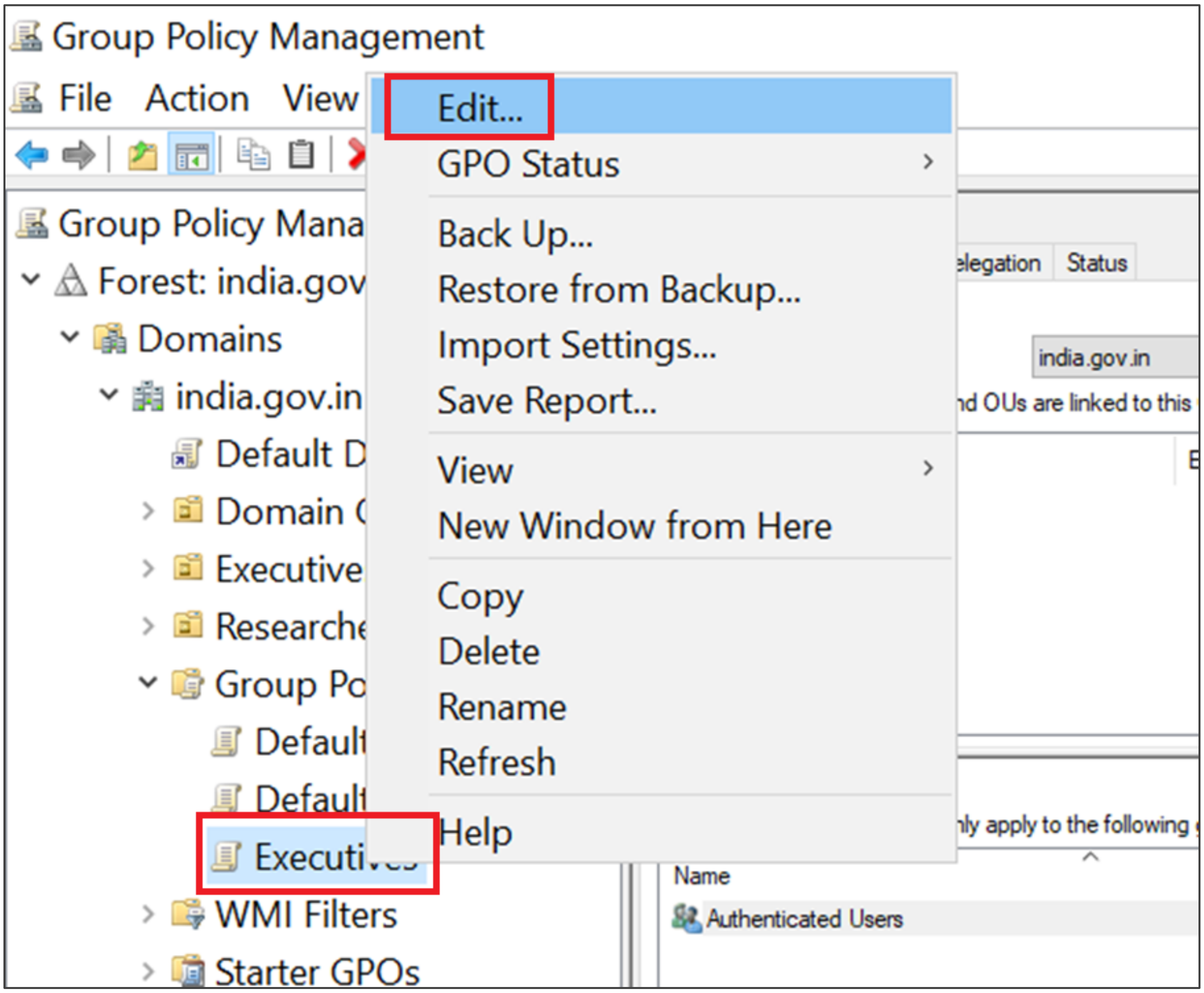
5.3 Write the **Name** of the group policy as **Executives** and click on **OK**



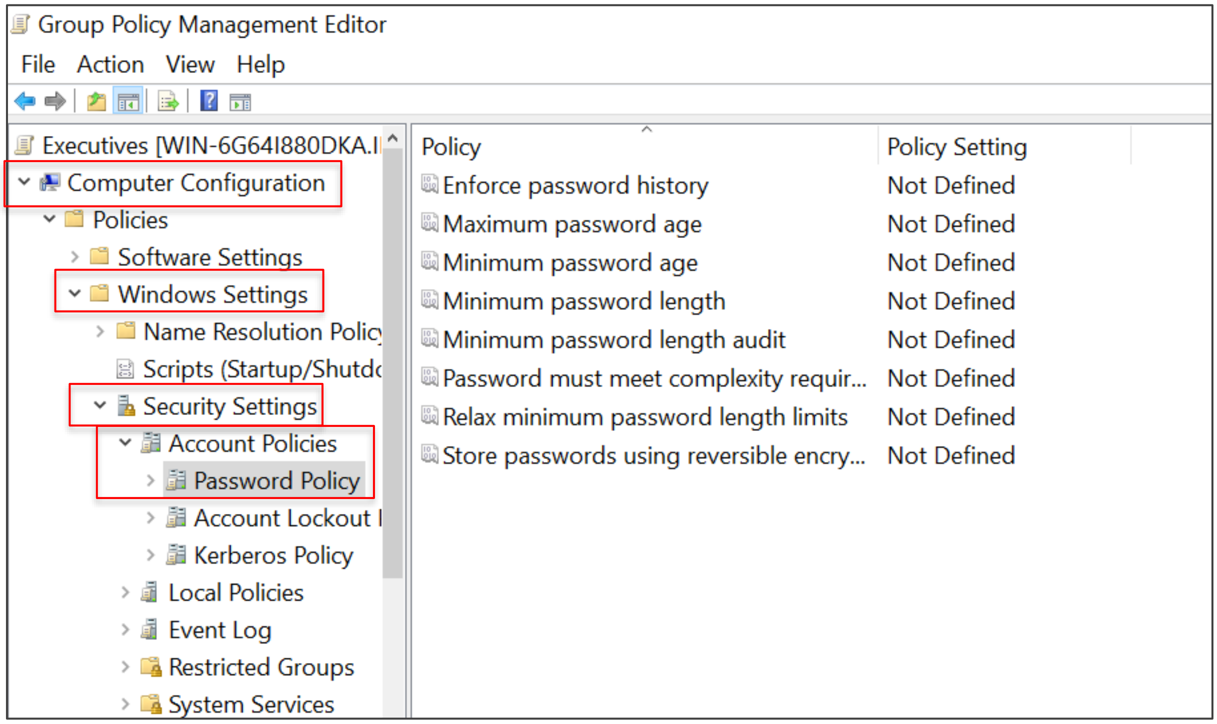
Name: Executives

Source Starter GPO: (none)

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

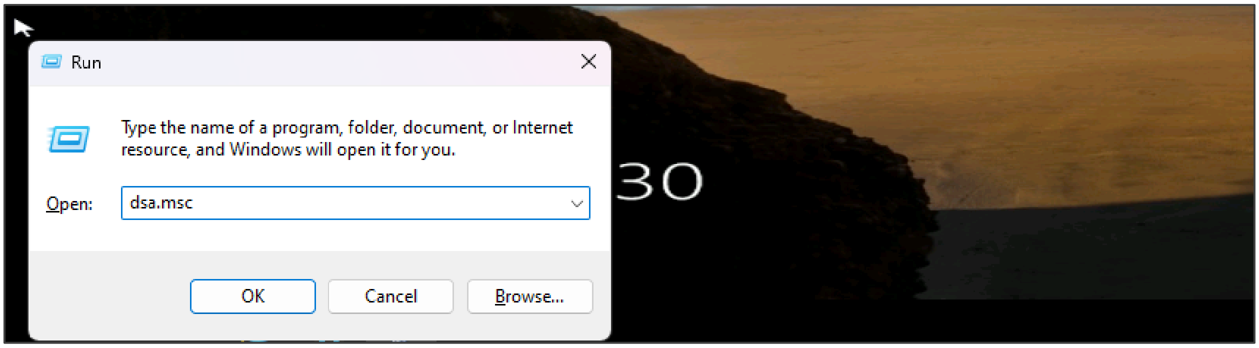


5.5 Navigate to **Computer Configuration**>**Windows Settings**>**Security Settings**>**Account Policies**>**Password Policy**



Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Minimum password length audit	Not Defined
Password must meet complexity requir...	Not Defined
Relax minimum password length limits	Not Defined
Store passwords using reversible encry...	Not Defined

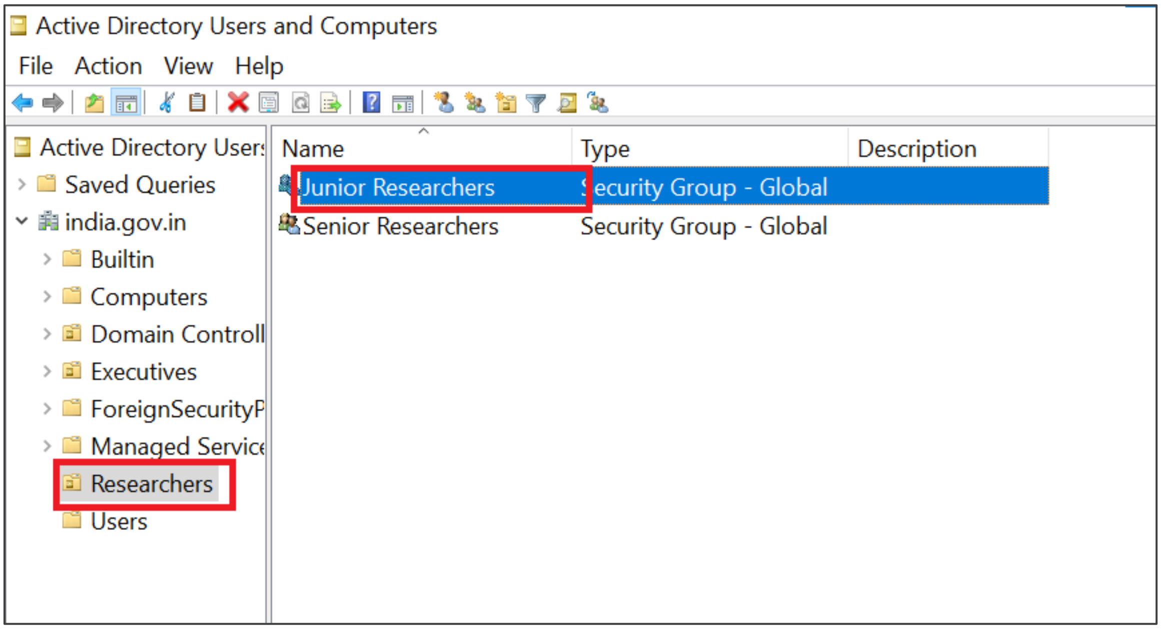
5.6 press windows+r and type **dsa.msc** and click **OK**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: dsa.msc

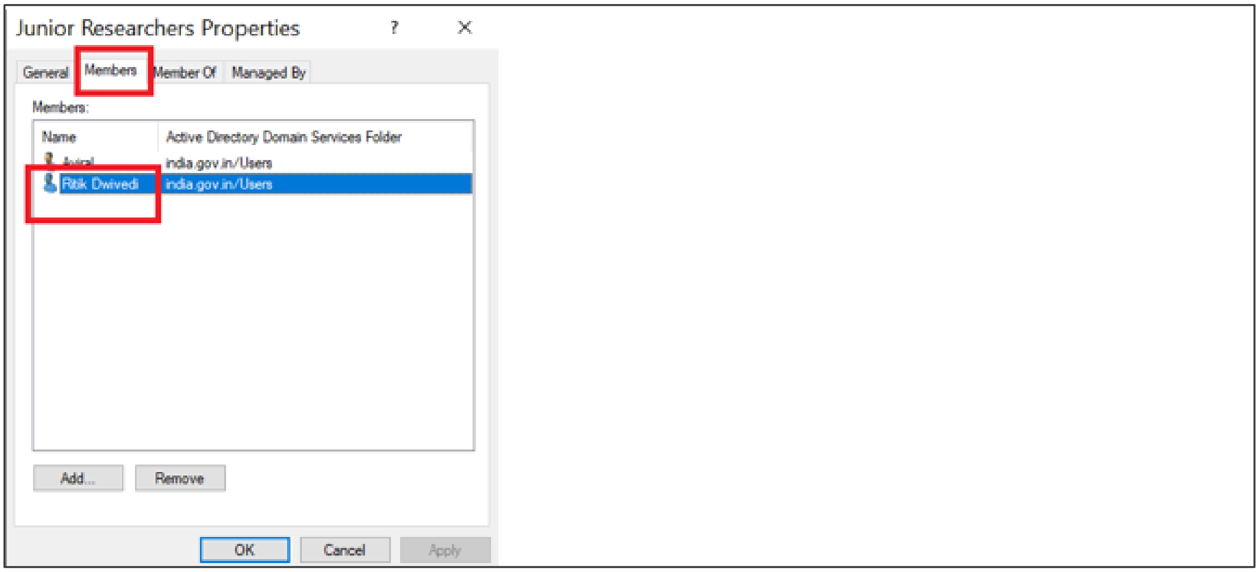
5.7 Double click on **Researchers** and then double click on **Junior Researchers**



Active Directory Users
- Saved Queries
- india.gov.in
  - Builtin
  - Computers
  - Domain Controll
  - Executives
  - ForeignSecurityP
  - Managed Service
  - Researchers
  - Users

Name	Type	Description
Junior Researchers	Security Group - Global	
Senior Researchers	Security Group - Global	

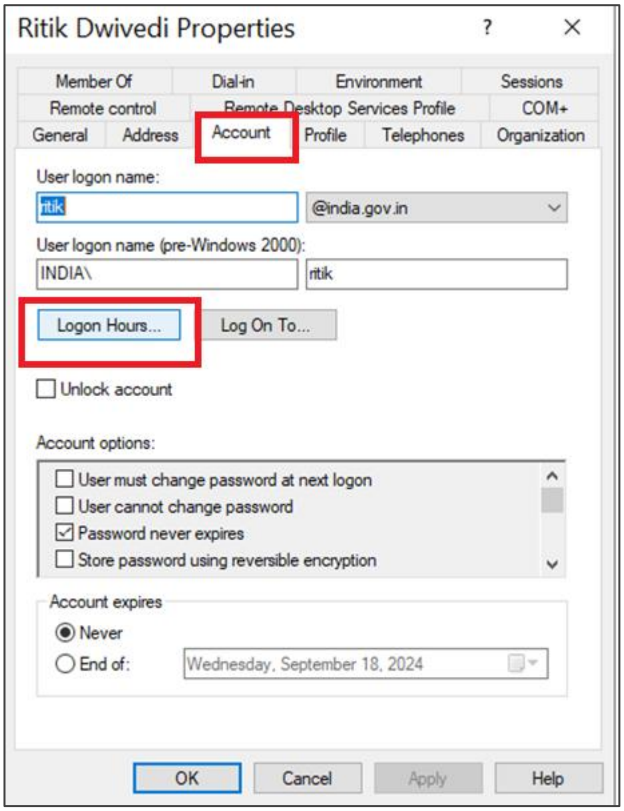
5.8 Click on **Members** and double click on Ritik Dwivedi



Members:

Name	Active Directory Domain Services Folder
Aviral	india.gov.in/Users
Ritik Dwivedi	india.gov.in/Users

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



User logon name: ritik @india.gov.in

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

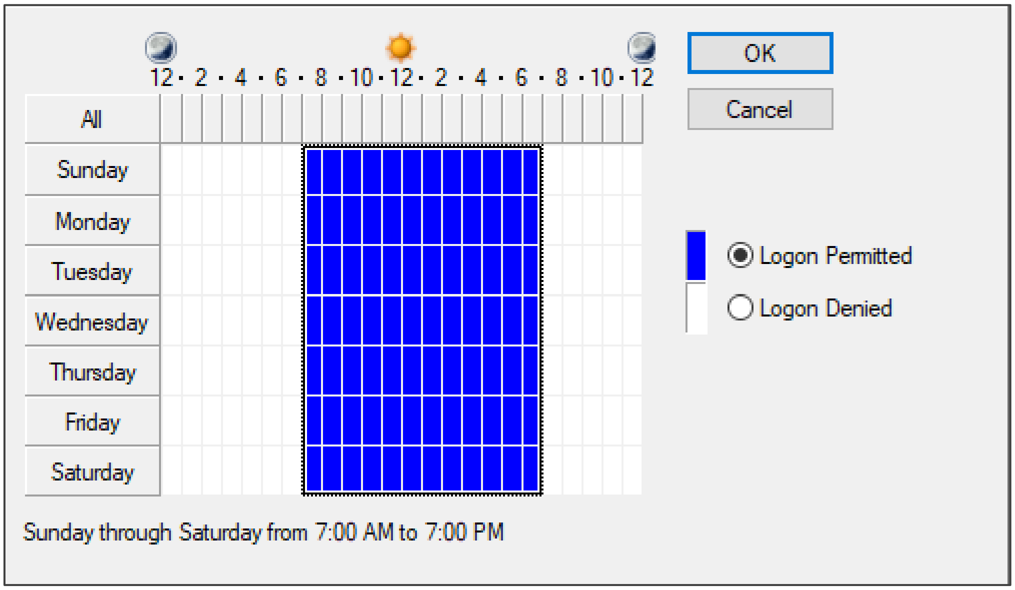
□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

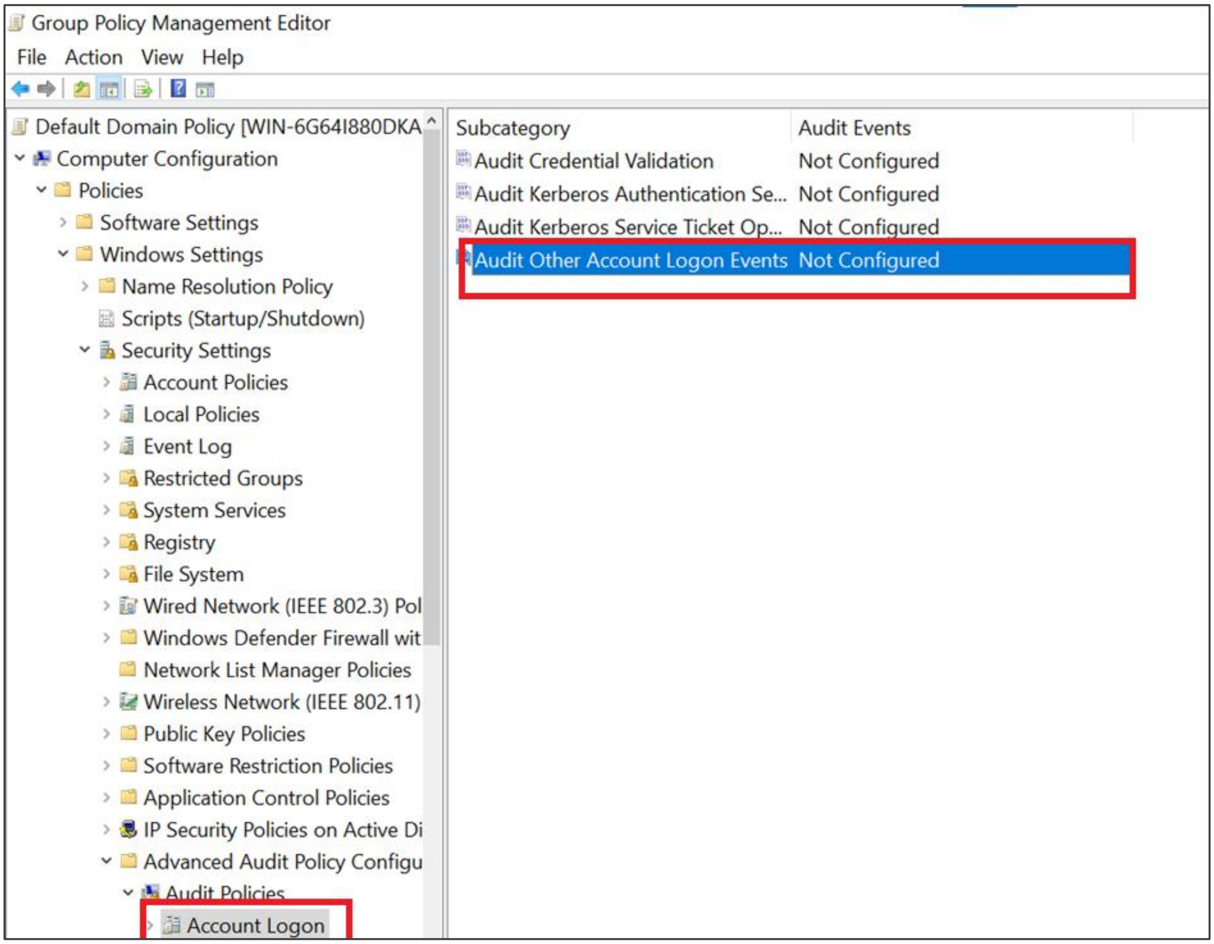
● Never
○ End of: Wednesday, September 18, 2024



● Logon Permitted
○ Logon Denied

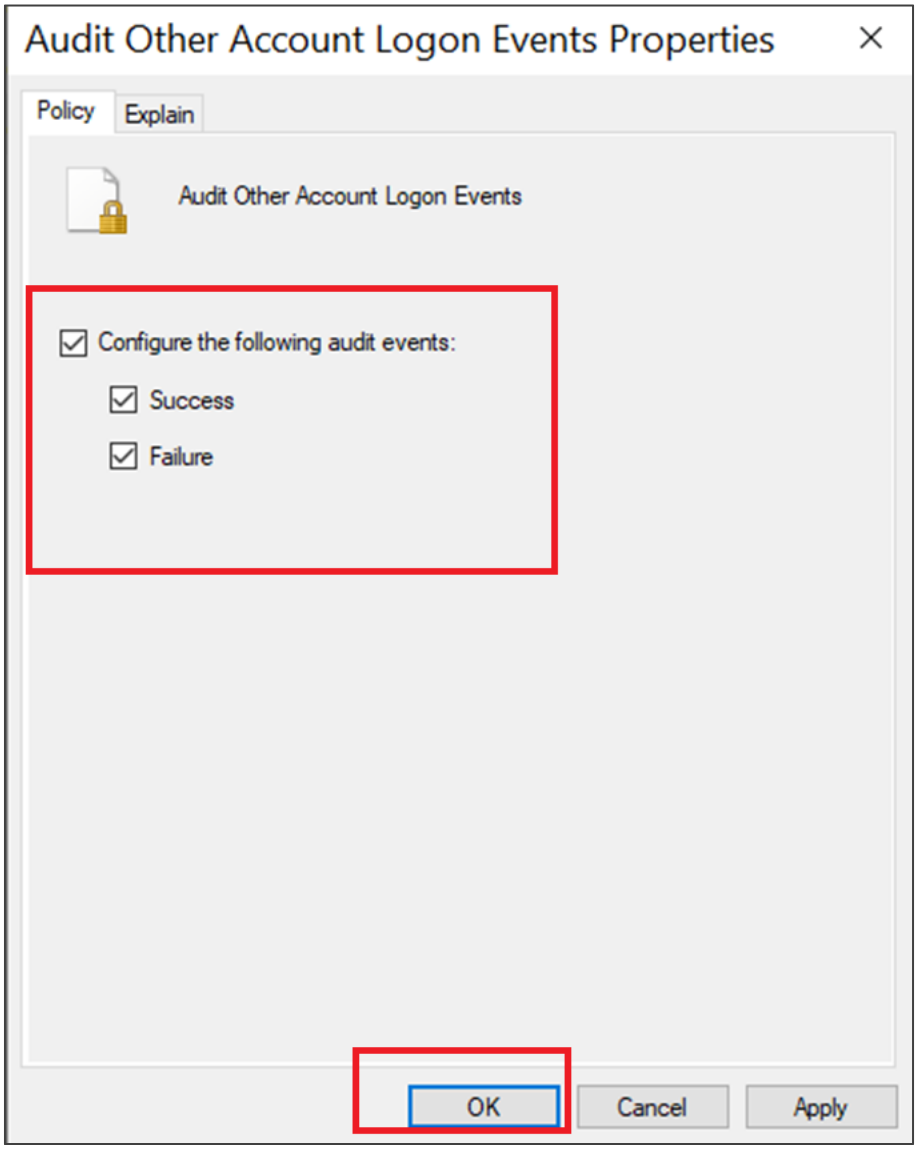
Sunday through Saturday from 7:00 AM to 7:00 PM

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**


Group Policy Management Editor
File Action View Help
Default Domain Policy [WIN-6G64I880DKA
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Pol
Windows Defender Firewall wit
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Di
Advanced Audit Policy Configu
Audit Policies
Account Logon

Subcategory	Audit Events
Audit Credential Validation	Not Configured
Audit Kerberos Authentication Se...	Not Configured
Audit Kerberos Service Ticket Op...	Not Configured
Audit Other Account Logon Events	Not Configured

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



Audit Other Account Logon Events Properties

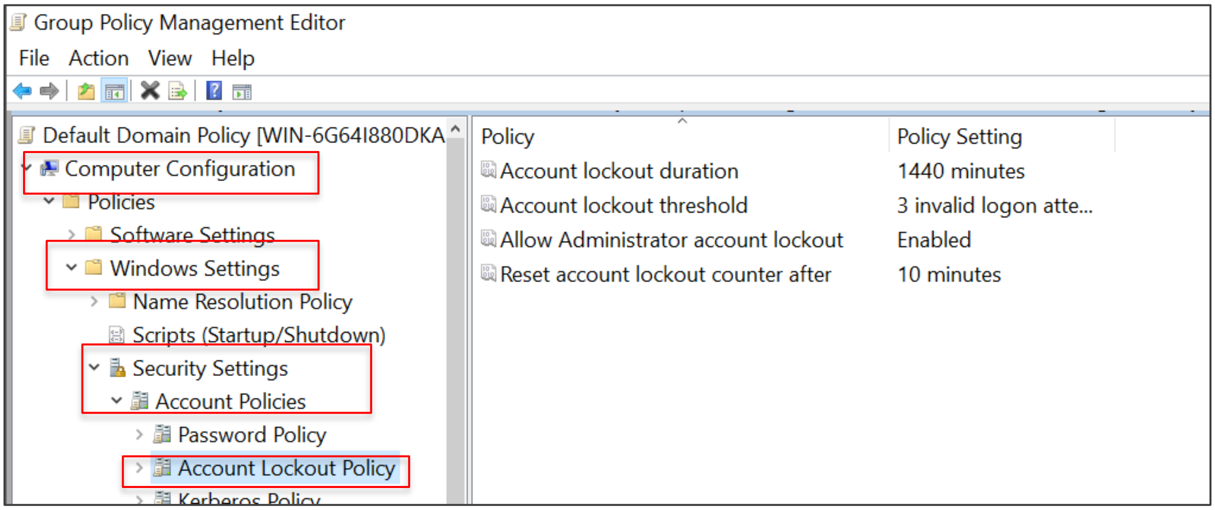
Audit Other Account Logon Events

☑ Configure the following audit events:

☑ Success

☑ Failure

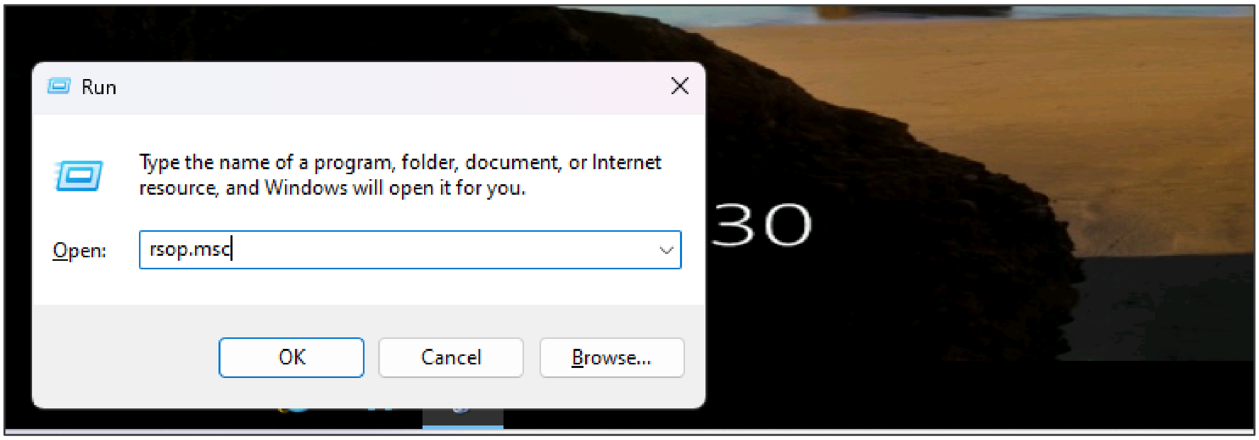
5.12 Navigate to **Computer Configuration**>**Windows Settings**>**Security Settings**>**Account Policies**>**Account Lockout Policy**



Policy	Policy Setting
Account lockout duration	1440 minutes
Account lockout threshold	3 invalid logon atte...
Allow Administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

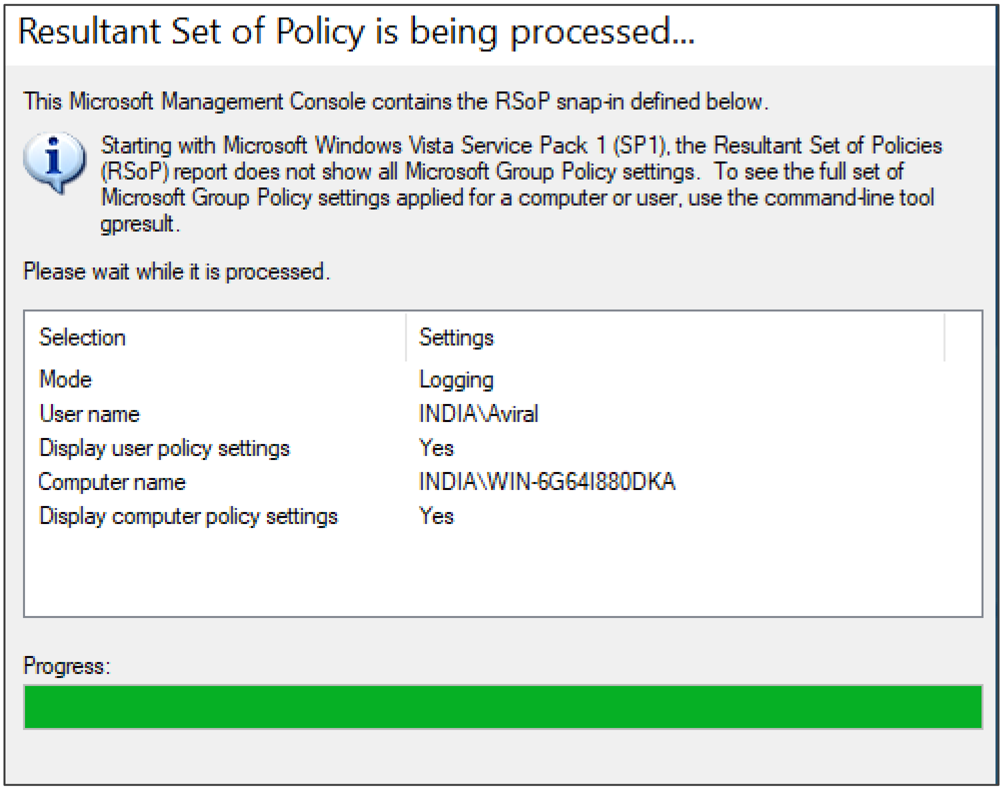
Step 6: Integrate compliance and reporting

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



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: rsop.msc



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.