

# Handling clients and configuring Active Directory on the windows server

## Pré-requisitos:

1. Make sure windows server is having static Ip.

## OVERVIEW:

### Step 1: Install Windows Server 2019

1. Install Windows Server 2019 on the server machine that you want to use as the domain controller. Follow the on-screen instructions to complete the installation process.

### Step 2: Promote the server to a domain controller

1. Open "Server Manager" and click on "Add roles and features".
2. Follow the prompts in the "Add Roles and Features" wizard to install the "Active Directory Domain Services" role on the server.
3. After the installation is complete, click on "Promote this server to a domain controller" in the "Active Directory Domain Services Configuration Wizard" that appears after the role installation.
4. In the "Deployment Configuration" tab, select "Add a new forest" and enter the desired domain name. Click "Next".
5. Choose the forest functional level and the domain functional level for your environment. Click "Next".
6. Specify the directory services restore mode password, which will be used for recovery purposes. Click "Next".
7. Review the DNS options and click "Next".
8. Configure the NetBIOS name and click "Next".
9. Choose the desired location for the Active Directory database, log files, and SYSVOL folder. Click "Next".
10. Review the settings and click "Install" to promote the server to a domain controller.

### Step 3: Configure DNS

1. After the domain controller promotion is complete, open "Server Manager" and click on "Tools" > "DNS" to open the DNS Manager.
2. In the DNS Manager, configure the forward and reverse lookup zones for your domain.

### Step 4: Join a system to the domain

1. On the client system (e.g., Windows 10), go to System Properties by right-clicking on "This PC" > "Properties".
2. Click on "Change settings" next to "Computer name, domain, and workgroup settings".
3. In the "System Properties" window, click on the "Change" button next to "To rename this computer or join a domain".

4. Enter the domain name that you configured in Step 2 (e.g., mydomain.local) and click "OK".
5. Enter the credentials of a domain administrator account when prompted.
6. Click "OK" to join the client system to the domain.
7. Restart the client system for the changes to take effect.

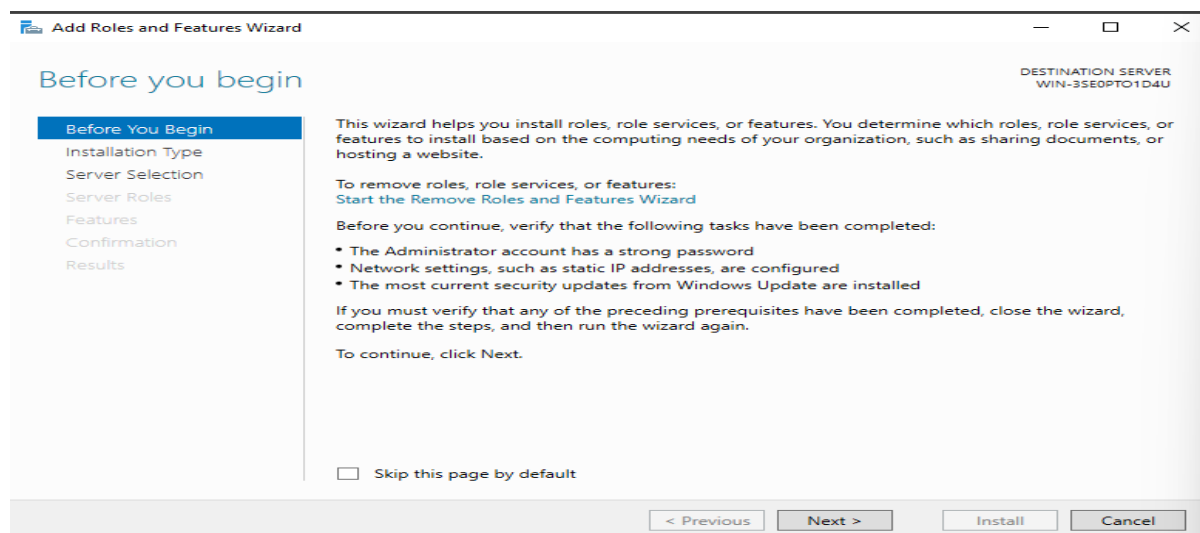
#### Step 5: Log in to the domain

1. After the client system has restarted, click on the "Other User" button on the login screen.
2. Enter the domain name and the credentials of a domain user account.
3. Click "Sign in" to log in to the domain.

## Procedure:

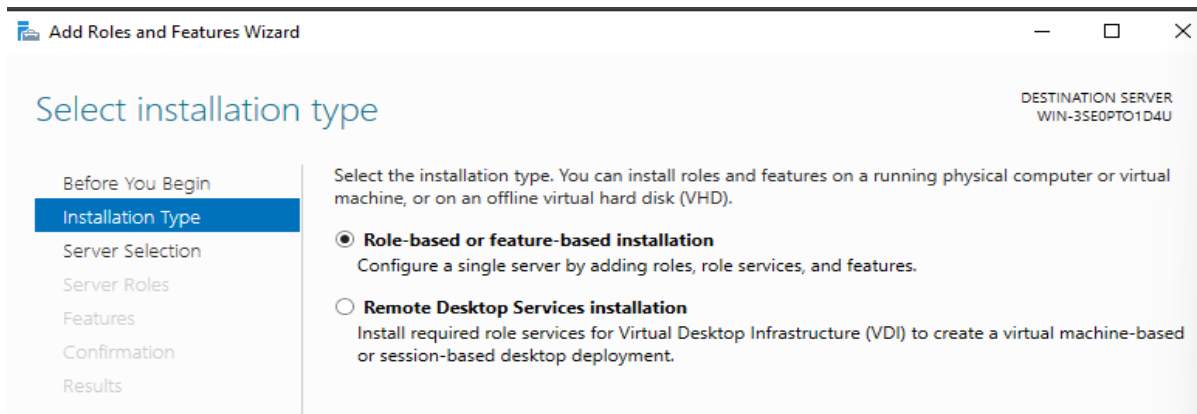
**Step 1:** When you choose "Add roles and Features" in the Windows Server Manager's Manage menu, a new window appears asking you to add the roles.

Click on Next:



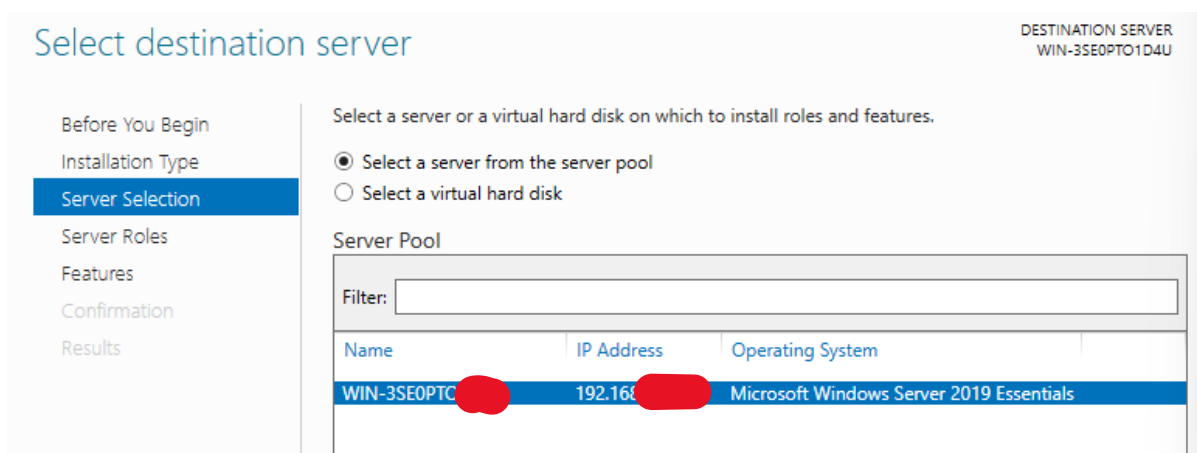
**Step 2:** As we are Installing Role-based feature so select the "Role-based or feature-based installation.

- Role-based or feature-based installation in Windows Server is a method of selectively installing only the necessary server roles or features on a Windows Server system, based on the intended use or requirements of the server. This allows for a more streamlined and efficient installation process, avoiding unnecessary software bloat. It helps to optimize system resources and security by only installing what is needed, reducing attack surface and potential vulnerabilities. This approach allows administrators to customize the server's functionality, performance, and security based on specific business needs.



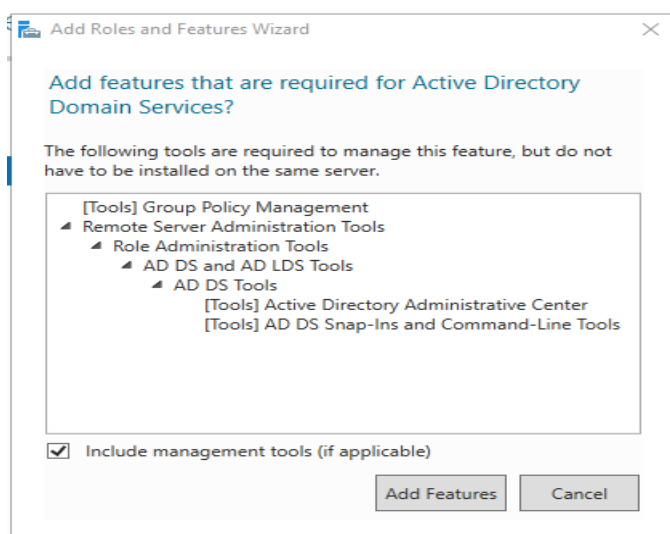
**Step 3:** We do not add features to any existing servers; instead, we create a new server and add roles to it in the server selection process.

- Select the server from the server pool
- Select the machine to configure the Active directory and click on next.

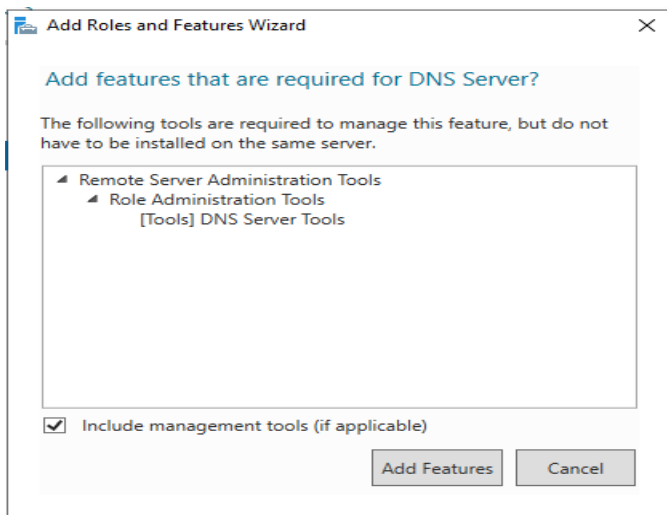


**Step 4:** Make sure you have chosen the relevant roles and need to setup them before adding the roles. As we currently deploy a new Active Directory, we must choose the

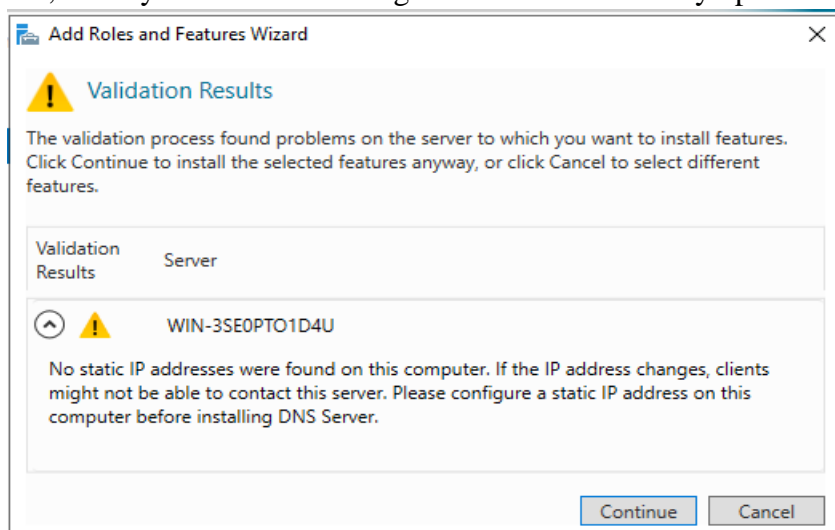
1. Active Directory Domain Service.



2. DNS Server.

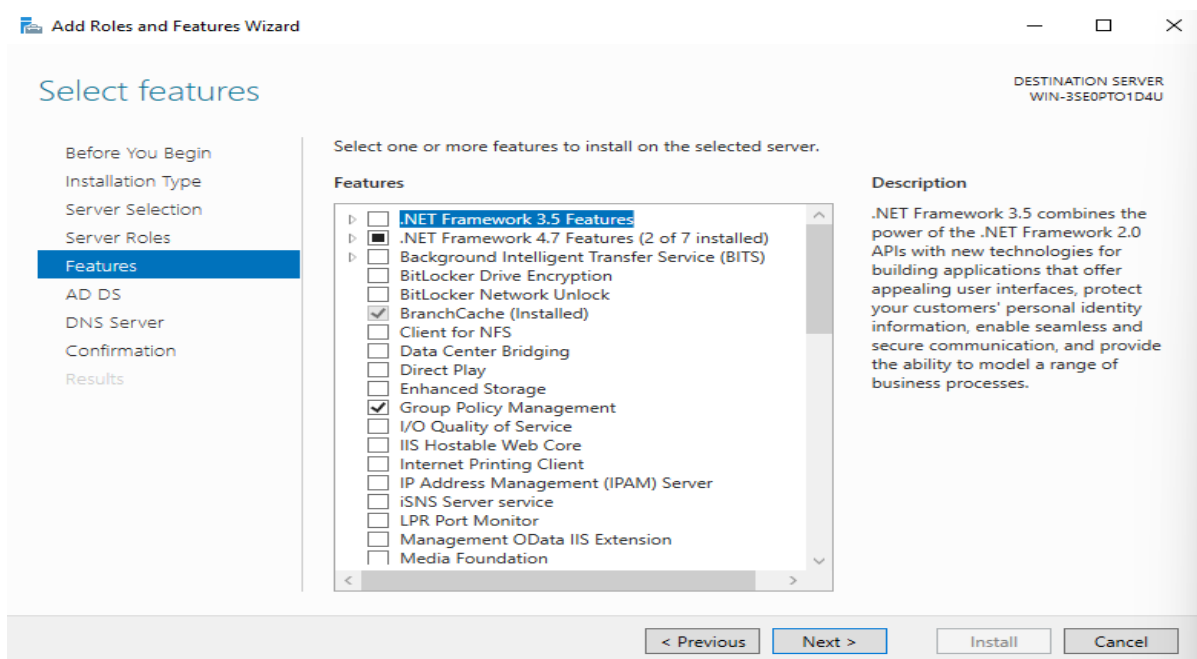


We must supply a static IP in order to operate the Server, as we indicated earlier in the prerequisites. If not, modify the network settings so that the server may operate without interruption.

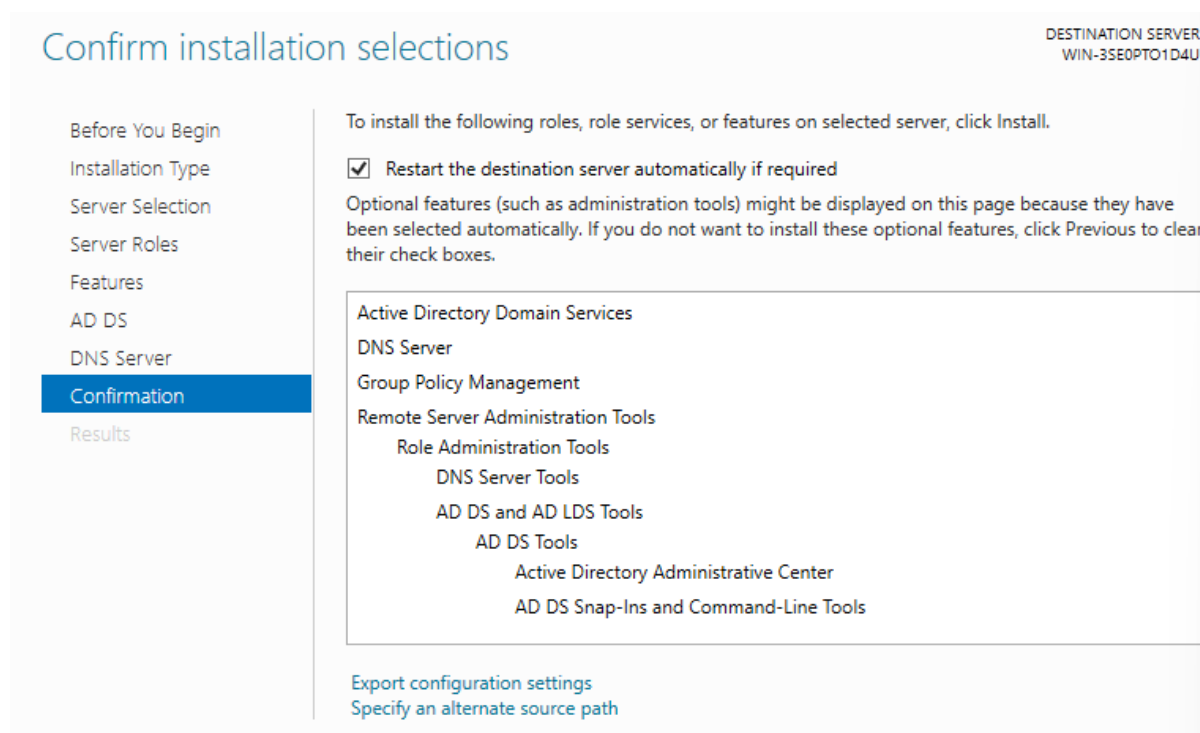


Static IP Error:

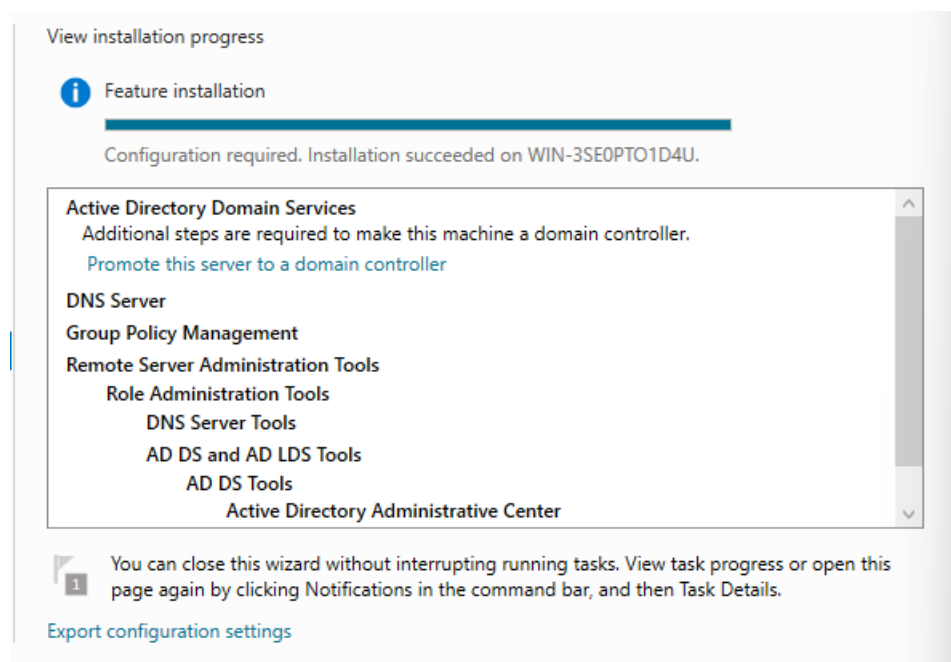
**Step 5:** In the features menu leave it as it is and click on next.



**Step 6 :** View the features in confirmation, select the option to automatically restart the Destination, make the appropriate adjustments, and click Install.



**Step 7:** As we can see, after a successful installation, the server needs to be promoted to a domain controller. Choose it to elevate the server to domain controller status.



**Step 8:** Because it is our primary domain controller, we must choose "Add a new forest" in the deployment operation.

Note: You can choose from the remaining two alternatives based on your needs if you already have a domain and wish to set the current server to that server.

➤ In the Domain section provide a Domain Controller name

Note: Domain name should need with (dot) extension. ex (Naveen.com, lab.in ...etc)

Deployment Configuration

TARU  
WIN-3SI

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

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: ai.vitap

**Step 9:** In the step 9 you can customize the Forest function level and Domain functional level.

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: 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: \*

By default I'm going with current top functional level windows server 2016 . And provide an password for the Directory Service Restore Mode.

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: 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: .....

**Step 10:** Click next once we can see that the NetBIOS domain name matches the name we entered for the root domain name.

## Additional Options

TARGET SERVER  
WIN-3SE0PT01D4U

- 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:

**Step 11:** You can change the database directories, log files, and SYSVOL folder under the paths sections. Click Next after leaving everything at its default state.

## Paths

TARGET SERVER  
WIN-3SE0PT01D4U

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

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:

 ...

Log files folder:

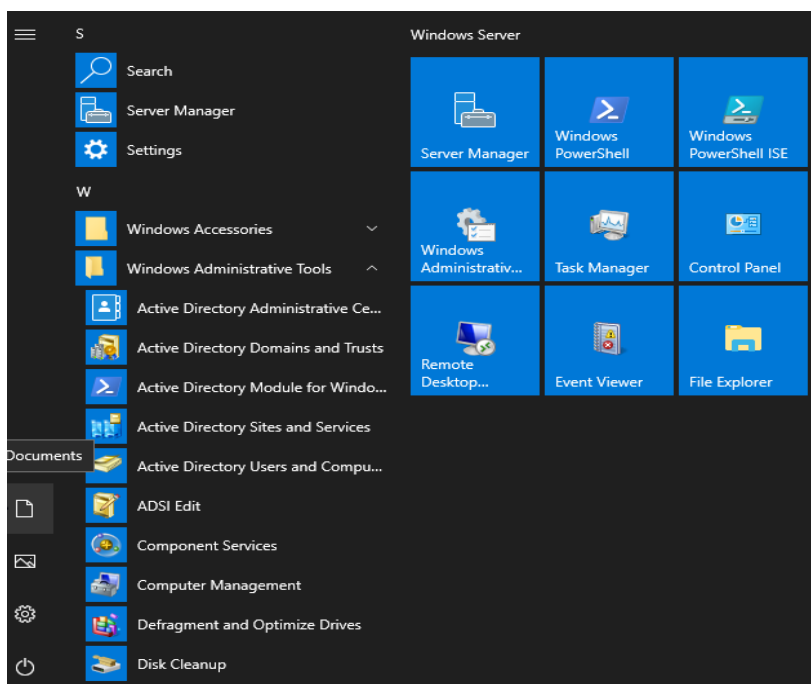
 ...

SYSVOL folder:

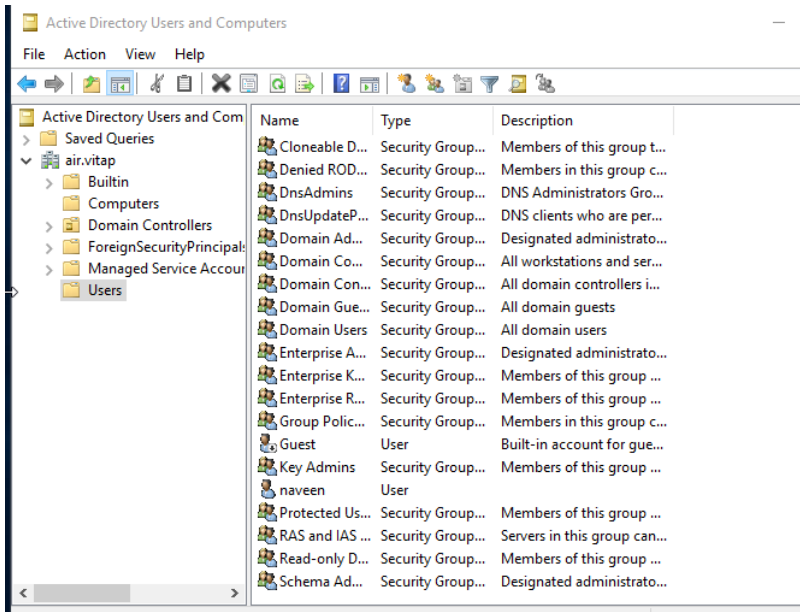
 ...

## Adding the user to the active directory

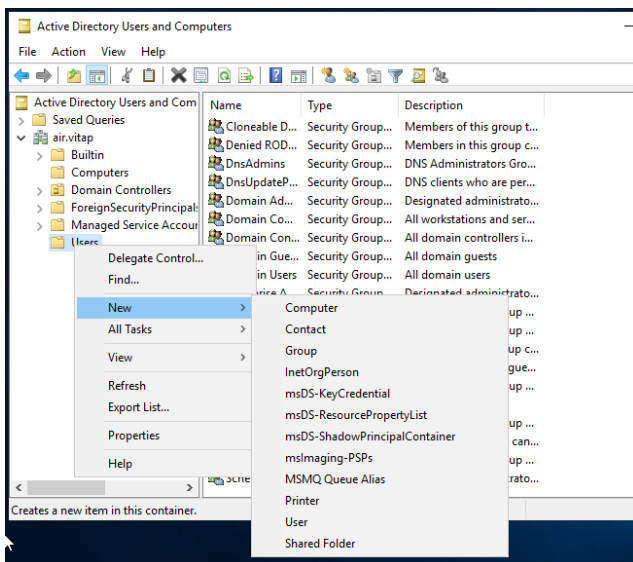
**Step 1:** Select the Active Directory users and the computers by launching the Windows Administrator tool.



**Step 2:** Click on the group folder that is located under the previously created active directory.



**Step 3:** As we can see, the active directory contains all of the users. A user account that uses single sign-on must be created. Therefore, right-click on it and choose "add new user."



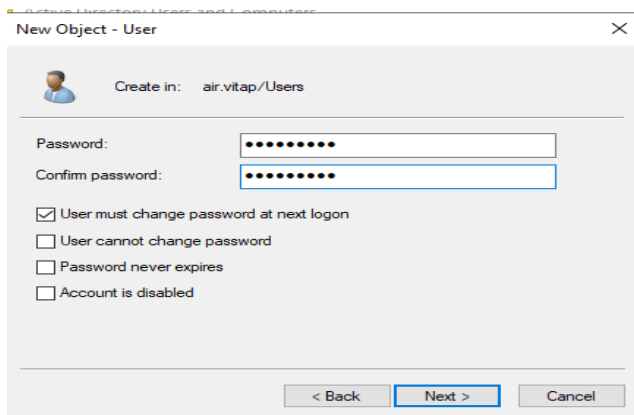
We can create new User or we can create a Group.

- Provide the necessary details of the users and click on next.

The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'air.vitap/Users'. The 'First name' field contains 'cyber', and the 'Initials' field is empty. The 'Last name' field is empty. The 'Full name' field contains 'cyber'. The 'User logon name' field contains 'cyber', and the domain dropdown is set to '@air.vitap'. The 'User logon name (pre-Windows 2000)' field contains 'AIR\cyber'. The 'Next >' button is highlighted.

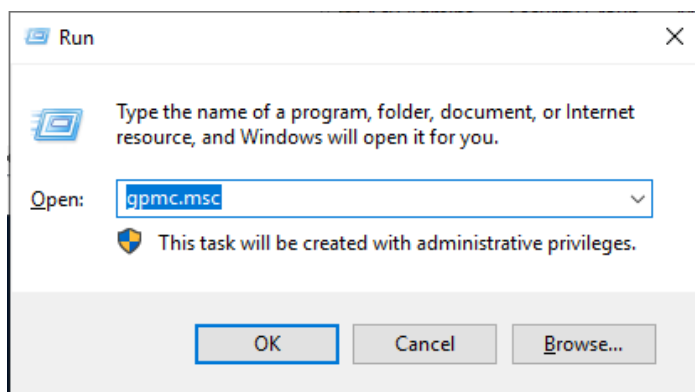


**Step 4:** You can choose whether the user needs to change their password, if you want to prevent them from doing so, or if you want to preserve their current password as their permanent one in the password management system.

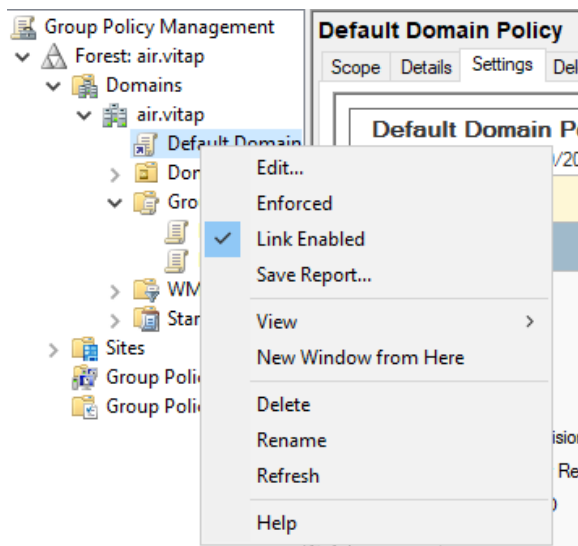


Password length is not complexity to handle that issue is an exception that the server active directory throws when setting up the password.

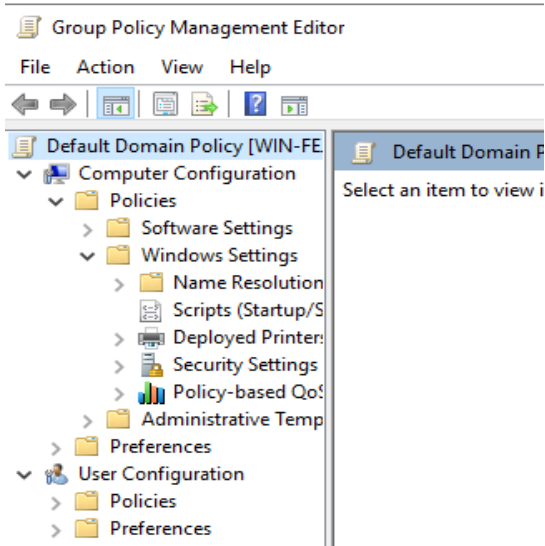
- Click on start > type run> type gpmmc.msc



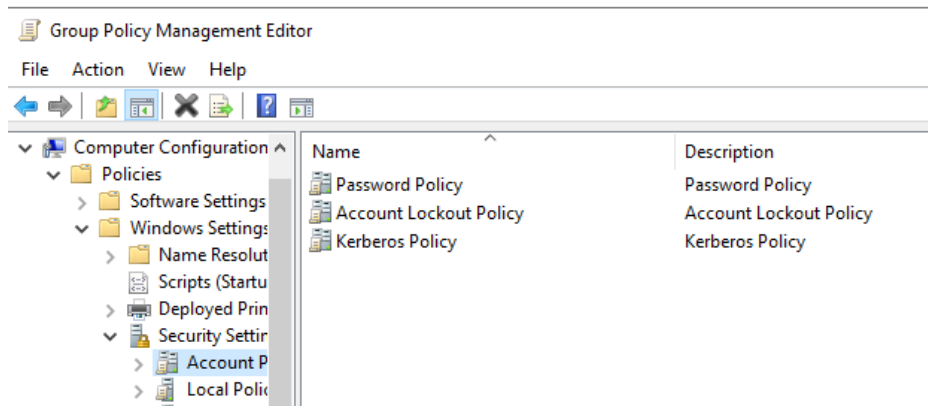
- Under the forest, retrieve to the Default Domain policy right click on it and select edit



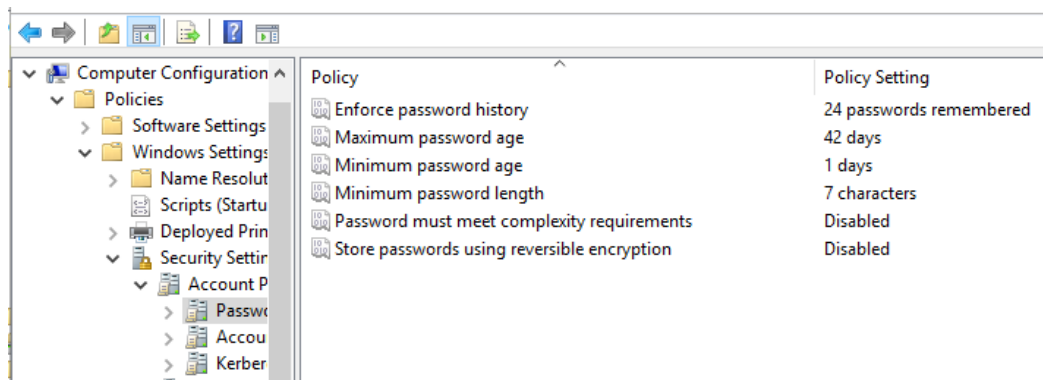
- Under the Computer configuration retrieve to the path  
Computer configuration > Policies > Windows Settings > Security Settings



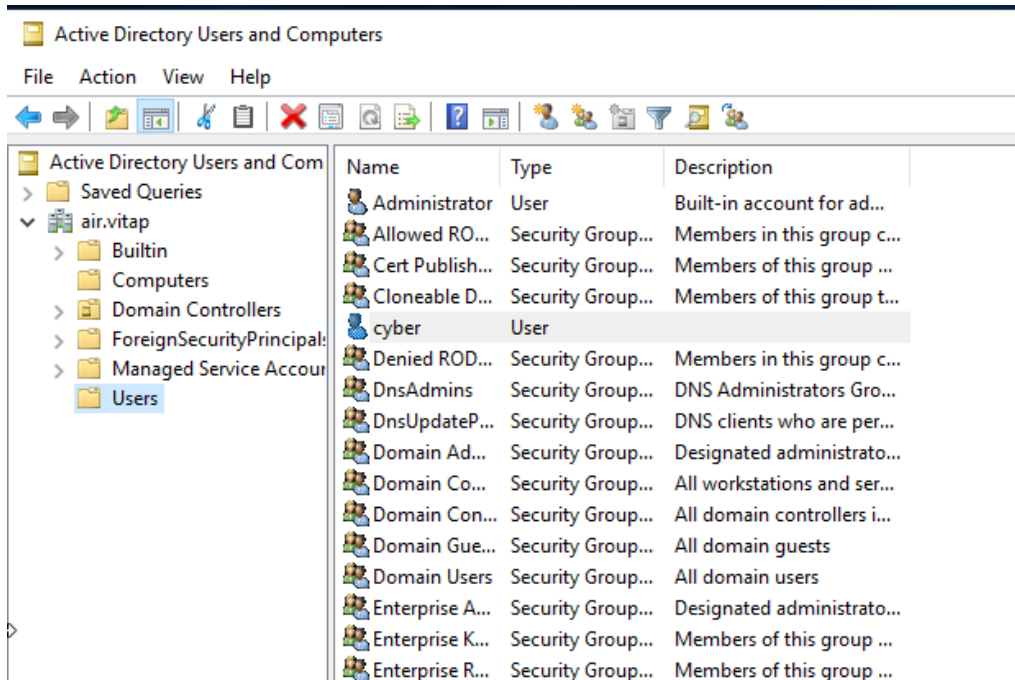
- Under the security policies select the Account policies and select the Password policy



- Now under the policies Disable the Password must meet complexity requirements



**Step 5:** create the user account and save it. As you can see, cyber was used to create the user account.



Adding the system to the Active directory.

Pre-requisites:

- Firstly, to add the system to the active directory domain we need know the DNS on the active directory
- For that check the DNS of the active directory
- Add the Active directory IP as the DNS server of the windows system which need to be added under network configuration.

Step 1: Open the System which you want to add to the active Directory domain and go to system settings.

- Click on about and select advance system settings.
- Edit system name.
- Under domain section Give the credentials of domain then the system will add and automatically restart.

*Handwritten signature*