



**Debre Berhan University  
Institute of Technology  
College of Computing  
Department of Information Technology**

**Course Name:** System and Network Administration

**Submitted By :**

**Name:** Eyob Alemayehu

**ID:** DBU1501190

**submitted to:** Dr. Samuel Asferaw

**Submission deadline:** Monday December 1, 2025

## I. Set Up Windows Workgroup System

### 1. What is a Windows Workgroup System?

A Windows Workgroup System is a peer-to-peer network model where each computer on the network is treated as an equal, or a "peer." In this model, there is no central server controlling network security and administration. Each computer maintains its own local security policy, user accounts, and resource management. It is a simple and cost-effective solution for small networks with a limited number of computers (typically 10 or fewer).

#### 1.1 How is Windows Workgroup System differing from Windows Active Directory Domain System?

Feature	Windows Workgroup System	Windows Active Directory Domain System
<b>Model</b>	Peer-to-Peer (Decentralized)	Client-Server (Centralized)
<b>User Accounts</b>	Local accounts stored on each computer. A user needs an account on every PC they access.	Centralized accounts stored on Domain Controllers. A single logon grants access to domain resources.
<b>Security &amp; Policy</b>	Local security policies managed individually on each machine.	Centralized Group Policy Objects (GPO) applied to users and computers across the entire domain.
<b>Scalability</b>	Suitable for small networks (e.g., up to 10 computers).	Designed for medium to large networks (hundreds or thousands of computers and users).
<b>Administration</b>	Administration is distributed; each user often manages their own PC.	Centralized administration by IT staff.
<b>Resource Access</b>	Users must know the password for shared resources on specific machines.	Single Sign-On (SSO) allows access to all authorized resources after domain login.

#### 1.2 Clearly show the steps in configuring Windows Workgroup System for 6 users in Windows 10 OS.

## Configuring Windows Workgroup System for 6 Users in Windows 10 OS

To configure a Windows Workgroup system for 6 users across multiple Windows 10 machines, you must ensure that all computers belong to the **same workgroup name** and that the local user accounts match on all machines for authentication.

### Step 1: Set a Common Workgroup Name

- 1. Open System Properties:** Search for Change the name of this PC or go to Settings → System → About and click Rename this PC (Advanced).
- 2. Access Change Settings:** In the "System Properties" window, under the "Computer Name" tab, click the Change... button.
- 3. Define Workgroup:**
  - Under the "Member of" section, ensure Workgroup is selected.
  - Enter the exact same workgroup name for all 6 machines (e.g., IT\_ASSIGNMENT\_GROUP).
- 4. Apply and Restart:** Click OK. You will be prompted to restart the computer. Restart all 6 PCs for the change to take effect.

### Step 2: Create Matching Local User Accounts

For peer-to-peer security in a workgroup, users must exist on the computer they are trying to access. Therefore, you must create 6 identical local user accounts with identical passwords on every Windows 10 PC:

- 1. Open User Settings:** Go to Settings → Accounts → Family & other users.
- 2. Add New User:** Click Add someone else to this PC.
- 3. Create Local Account:** Select I don't have this person's sign-in information and then Add a user without a Microsoft account.
- 4. Input Credentials:** Create the 6 required accounts, for example:
  - **Username:** User1, User2, User3, User4, User5, User6
  - **Passwords:** Set a matching, strong password for each user on all 6 computers.

### Step 3: Configure Network and Sharing Settings

This ensures the computers can see each other and share resources.

- 1. Open Network Sharing Center:** Search for Network and Sharing Center in the Control Panel.
- 2. Change Advanced Settings:** Click on Change advanced sharing settings on the left menu.
- 3. Configure Private Profile (Recommended):** Expand the Private profile:
  - Turn on Network discovery (Check the box for "Turn on automatic setup of network connected devices").
  - Turn on File and printer sharing.
- 4. Configure All Networks Profile:** Expand the All Networks profile:
  - **Public folder sharing:** Select Turn on sharing so anyone with network access can read and write files in the Public folders (Optional, but often useful).
  - **Password protected sharing:** Select Turn on password protected sharing. This is crucial, as it forces users to authenticate using the matching local accounts created in Step 2 before accessing shared files or printers.

Once these steps are completed on all 6 Windows 10 PCs, the Workgroup System is configured. The 6 users can now log into any PC locally and use their matching credentials to access shared resources (files and printers) on the other 5 computers.

### 1.3 Clearly show the steps for file sharing in Windows Workgroup System that you configured in equation 1.2.

#### Steps for File Sharing in a Windows Workgroup System

Assuming you have already configured the Windows Workgroup system (as detailed in the earlier steps, including setting a common workgroup name and creating matching local user accounts on all 6 PCs), here are the clear steps for setting up file sharing.

This procedure is performed on the host computer (the PC that has the folder you want to share).

## Step 1: Select and Open Folder Properties

1. Navigate to the folder you wish to share (e.g., a folder named Team Projects).
2. Right-click on the folder and select Properties.

## Step 2: Configure Basic Sharing

1. In the Properties window, click the Sharing tab.
2. Click the Share... button under the "Network File and Folder Sharing" section.
3. **Specify Users:** In the "Network access" window:
  - Use the drop-down menu to add the specific users who need access (e.g., **User1**, **User2**, **User3**, etc.). You must add the local accounts you created in the initial setup.
  - You can also add Everyone for simpler access, but this is less secure.
4. **Set Permissions:** For each added user/group, set the appropriate Permission Level:
  - **Read:** Users can view and open files, but cannot modify or delete them.
  - **Read/Write:** Users can view, open, modify, and delete files.
5. Click Share and then Done.

## Step 3: Configure Advanced Sharing (Optional but Recommended)

For more granular control over the share's availability, use Advanced Sharing.

1. Back in the Sharing tab of the Properties window, click Advanced Sharing.
2. Check the box for Share this folder.
3. Click the Permissions button.
4. **Define Share Permissions:** Use this window to refine access control:
  - Select the user or group (e.g., Everyone).
  - Choose the Share Permissions: Full Control (highest), Change, or Read.

• **Note:** The most restrictive permission (between the Basic Share Permission and the Advanced NTFS Security Permission) will always apply.

5. Click "OK" to close the Permissions window, and "OK" again to close Advanced Sharing.

#### **Step 4: Configure NTFS Security Permissions**

This step is vital for actual file access and is separate from the Share Permissions.

1. In the folder's Properties window, click the "Security" tab.
2. Click "Edit..." to change permissions.
3. Click "Add..." to include the domain users or groups (or the local user accounts, like User1) you wish to grant access to.
4. For the added users, check the appropriate permissions (e.g., Modify, Read & execute, Write, etc.) under "Allow".
5. Click "OK".

#### **Step 5: Access the Shared Files from a Client PC**

A user on one of the other 5 computers can now access the shared folder:

1. Open File Explorer on the client PC.
2. In the address bar, type the network path using two backslashes followed by the host computer's name (e.g., \\PC\_Host\_Name) or its IP address.
3. When prompted for credentials, the user must enter the matching local username and password (e.g., User1 and their password) that exists on the host computer (the one sharing the folder).
4. The shared folder will appear, and the user can interact with the files based on the permissions set.

### **1.4 Clearly show the steps for printer sharing in Windows Workgroup System that you configured in equation 1.2**

#### **Steps for Printer Sharing in a Windows Workgroup System**

This procedure outlines how to share a printer from one of the Windows 10 PCs (the **host computer**) so that the other 5 computers in the workgroup can use it (the **client computers**). This assumes the workgroup is already configured with a common workgroup name and matching local user accounts.

## Step 1: Share the Printer (Host Computer)

1. **Access Printer Settings:** On the computer that is physically connected to the printer, go to Settings → Devices → Printers & scanners.
2. **Manage Printer:** Select the printer you want to share and click Manage.
3. **Open Printer Properties:** Click Printer properties.
4. **Navigate to Sharing Tab:** Click the Sharing tab.
5. **Enable Sharing:** Check the box that says Share this printer.
6. **Name the Share:** Provide a clear, simple Share name (e.g., Office\_Printer). This is the name the client PCs will use to find it on the network.
7. **Optional: Additional Drivers:** If the client computers run a different architecture (e.g., one client is 32-bit while the host is 64-bit), click Additional Drivers and install the necessary drivers for those architectures.
8. Click Apply and OK. The printer is now discoverable on the workgroup network.

## Step 2: Add the Shared Printer (Client Computers)

This procedure must be repeated on each of the remaining 5 client computers.

1. **Access Printer Settings:** Go to Settings → Devices → Printers & scanners.
2. **Add a Printer:** Click Add a printer or scanner.
3. **Find Printer by Name:** After a few moments, Windows may not find it automatically. Click The printer that I want isn't listed.
4. **Select Shared Printer:** In the Add Printer wizard, Select a shared printer by name.
5. **Enter Network Path:** Type the full network path to the shared printer using the host computer's name and the share name you defined in Step 1, using the format:

*Example: \\PC\_Host\_1\Office\_Printer*

6. **Install Drivers:** Click Next. Windows will attempt to connect and install the necessary drivers.
7. **Authentication:** If prompted for credentials (due to password-protected sharing being enabled, as recommended for security):

- Enter the matching local username and password (e.g., User1 // password) that exists on the host computer.

8. **Finish:** Click Next and then Finish to complete the installation.

## II. Set Up Windows Active Directory Domain System

### 2.0 What is Windows Active Directory Domain System?

The **Windows Active Directory Domain System (AD DS)** is a **centralized, hierarchical directory service** developed by Microsoft for Windows Server operating systems. It functions as the primary security and identity backbone for corporate networks.

AD DS stores information about all network resources—including user accounts, computer accounts, shared resources, and security policies in a single, relational database. This central repository allows for a **Single Sign-On (SSO)** experience, enabling a user to authenticate once and gain authorized access to any resource across the network.

- **Key Function:** Provides centralized authentication, authorization, and management for users and devices.
- **Architecture:** Uses a **client-server** model, where dedicated servers called **Domain Controllers** manage the directory.

### 2.1 Clearly write down the steps for installing Windows Server 2022 (64 bit), Active Directory Domain Services.

This process is typically divided into three phases: OS Installation, Role Installation, and Server Promotion.

#### **phases 1: Installing Windows Server 2022 (64-bit)**

This phase sets up the base operating system on the server hardware.

**1. Boot from Installation Media:** Start the server using the Windows Server 2022 installation media (DVD or USB drive).

**2. Language and Format Selection:** Select the desired language, time, and keyboard input method. Click Next.

**3. Start Installation:** Click Install now.

**4. Edition Selection:** When prompted, choose the installation image. For a Domain Controller, selecting **Windows Server 2022 Standard (Desktop Experience)** is common, as it includes the Graphical User Interface (GUI).

**5. License Terms:** Accept the license terms and click **Next**.

**6. Installation Type:** Select **Custom: Install Windows only (advanced)** to perform a clean installation.

**7. Disk Selection:** Choose the drive or partition where you want to install the OS. Click **Next**.

**8. Completion and Password:** The installation will proceed and the server will reboot several times. Upon the first boot, set a strong password for the built-in Administrator account.

## **phases 2: Installing the Active Directory Domain Services (AD DS) Role**

After the OS is installed, you must add the AD DS software components.

- 1. Open Server Manager:** After logging in with the Administrator account, the Server Manager dashboard should open automatically.
- 2. Start Wizard:** Click **Manage** in the top-right corner, and then select **Add Roles and Features**.
- 3. Installation Type:** Select **Role-based or feature-based installation**. Click **Next**.
- 4. Server Selection:** Ensure the local server is selected. Click **Next**.
- 5. Select Server Roles:** Check the box for **Active Directory Domain Services (AD DS)**.
  - A dialog box will appear asking to install required features (like management tools). Click **Add Features**.
- 6. Confirmation and Installation:** Review the features selected, and then click **Install**. The necessary files for the AD DS role will be installed on the server.

## **phases 3: Promoting the Server to a Domain Controller**

The final phase configures the role and turns the server into a functional Domain Controller (DC).

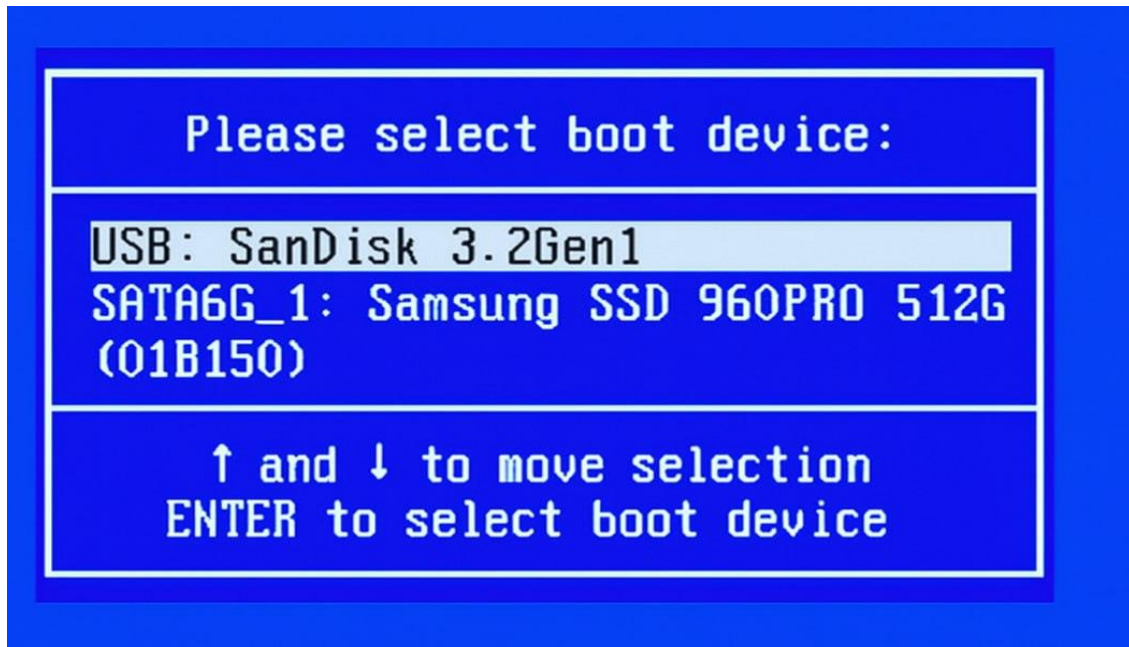
1. **Start Promotion:** After the installation completes, click the Promote this server to a domain controller link in the Server Manager notifications (flag icon).
2. **Deployment Configuration:** This is the most critical step for a new network:
  - Select **Add a new forest**.
  - Enter the **Root domain name** (e.g., companyname.local).
3. **Domain Controller Options:**
  - Set the **Forest and Domain functional levels** (use the highest available for a new installation).
  - Ensure **Domain Name System (DNS) server** and Global Catalog (GC) are checked (required for the first DC).
  - Set a strong password for the Directory Services Restore Mode (DSRM).
4. **DNS Options:** Click Next (you can generally ignore the DNS delegation warning for a new forest).
5. **NetBIOS Name:** Verify the automatically generated **NetBIOS name** and click **Next**.
6. **Paths:** Leave the default paths for the database, log files, and SYSVOL folder. Click **Next**.
7. **Review and Install:** Review all configuration settings. The system will run a prerequisites check. Once it passes, click **Install**. The server will automatically **reboot** and come up as the primary Domain Controller for the new Active Directory domain.

## 2.2 Define each terms in each step of the installation (and put the screen shoot for each step, where it is required).

### Step 1: Boot from Installation Media

**Boot from Installation Media** means starting (booting) your computer using an external device that contains the operating system installation files—**not** from the computer's internal hard drive.

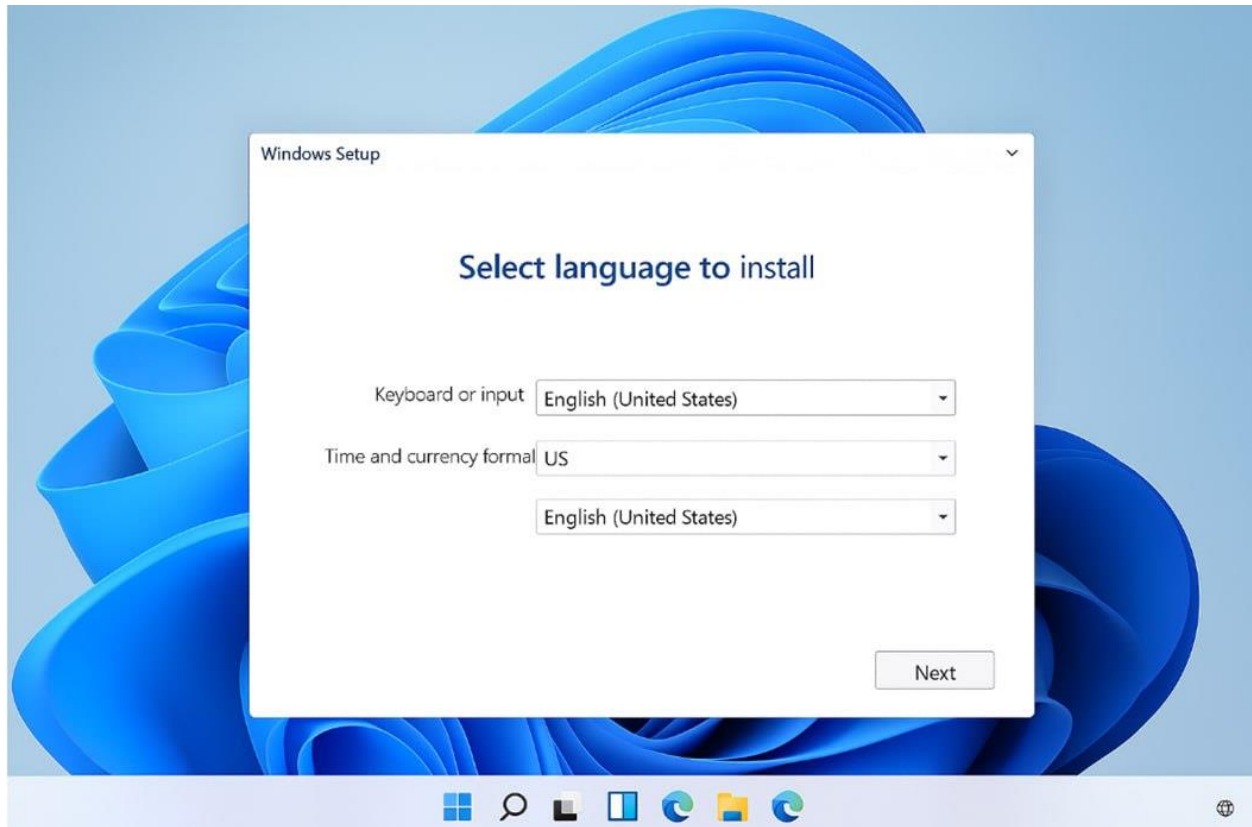
- **Boot:** The process where the computer starts and loads an operating system.
- **Installation Media:** The USB/DVD/ISO file that contains Windows Server 2022 setup files.
- **Boot Menu:** A menu that allows the user to choose what device to start the computer from.



Step 2: Choose Language, Time, and Keyboard

**Terms:**

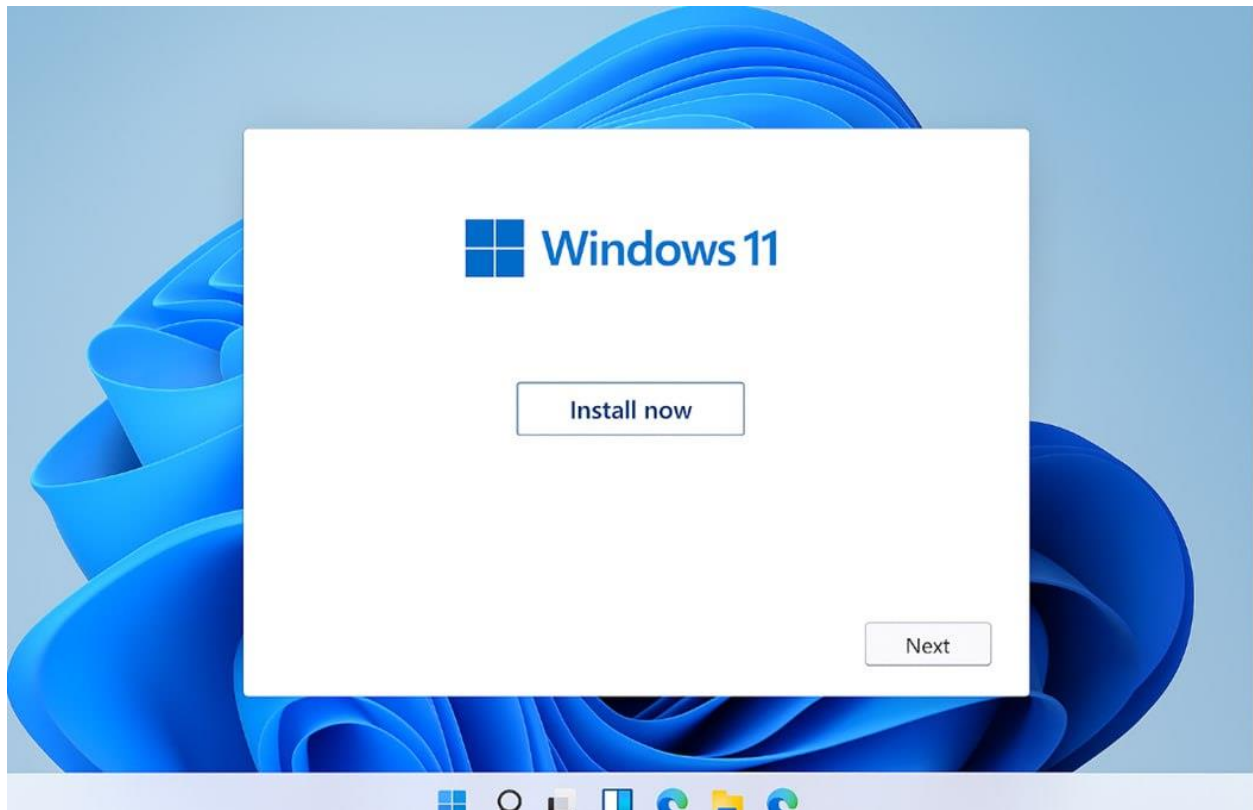
- **Language to Install:** The language Windows Server will use.
- **Time and Currency Format:** Controls how date, time, and currency appear.
- **Keyboard Input Method:** Determines how your keyboard types (e.g., US, UK).



Step 3: Click Install Now

**Terms:**

- **Install Now:** A button that starts the Windows Server installation process.
- **Setup Wizard:** A guided interface that helps you through the installation.



#### Step 4: Select Windows Server Edition

##### Terms:

- **Windows Server 2022 Standard/Datacenter:**  
Different versions of the server operating system with different features.
- **Desktop Experience:**  
Includes the normal GUI (Graphical User Interface). Without it, the server is only command-line.

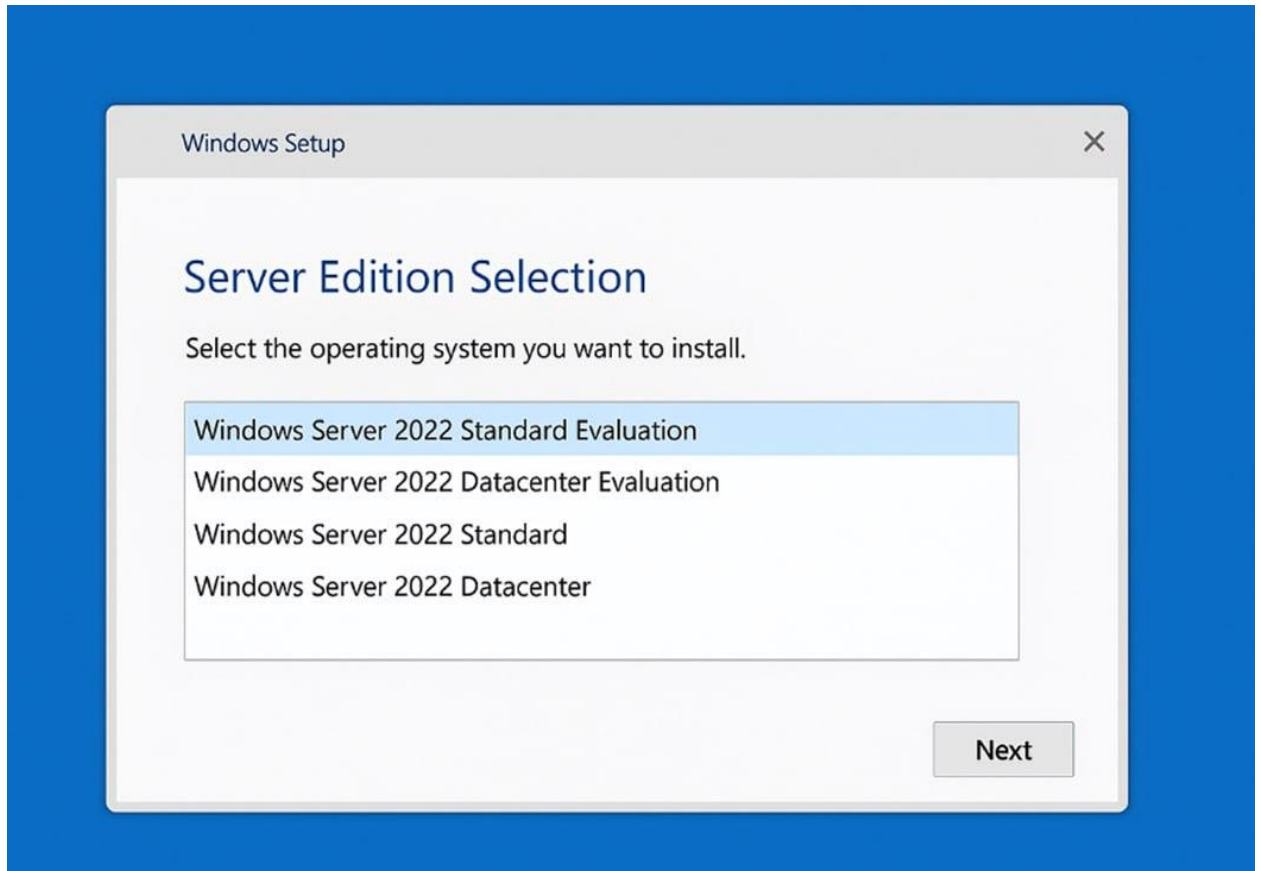
##### Server Edition Selection

This screen allows you to choose which version of Windows Server 2022 you want to install.

- **Datacenter (Desktop Experience):**  
Full GUI version with advanced features for large organizations and virtualization.
- **Standard (Server Core):**  
Minimal installation without GUI; uses command-line only.

- **Datacenter (Server Core):** Minimal version with advanced datacenter features; recommended for enterprise environments.

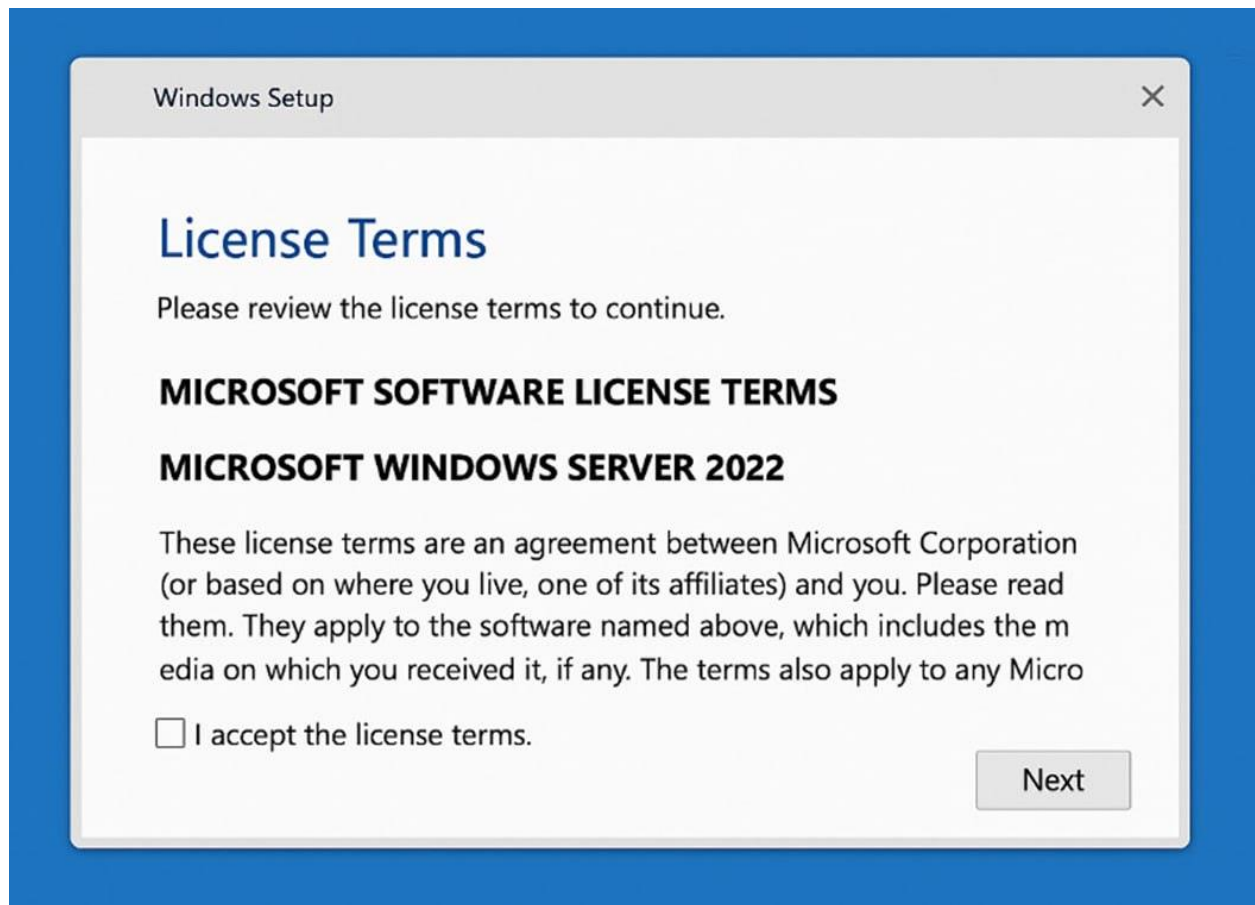
Choose the edition that fits your needs and click **Next**.



## Step 5: Accept the License Terms

### Terms:

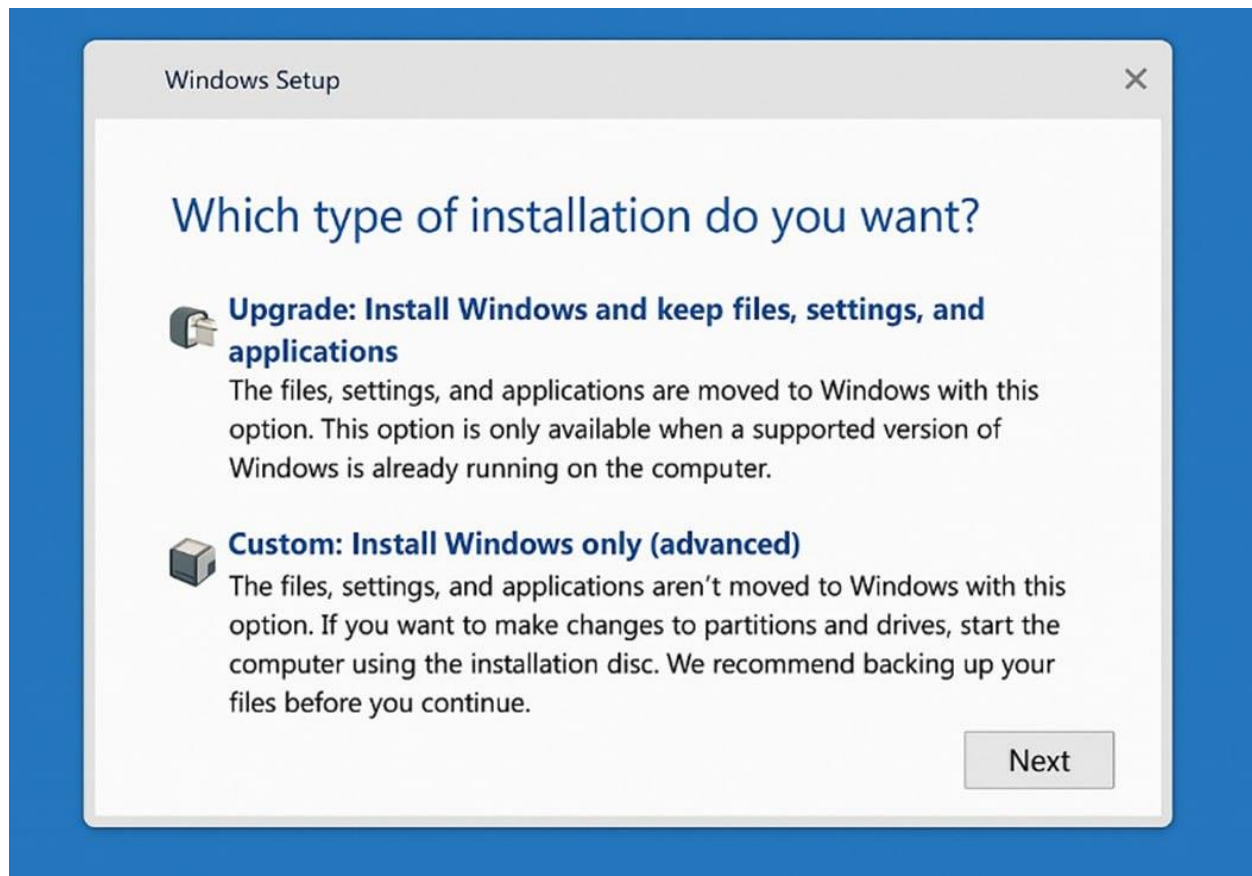
- **License Agreement:**  
Legal rules that you must agree to before installing the software.
- **I Accept the License Terms:**  
Confirms that you agree to Microsoft's terms.



## Step 6: Choose Installation Type (Custom)

### Terms:

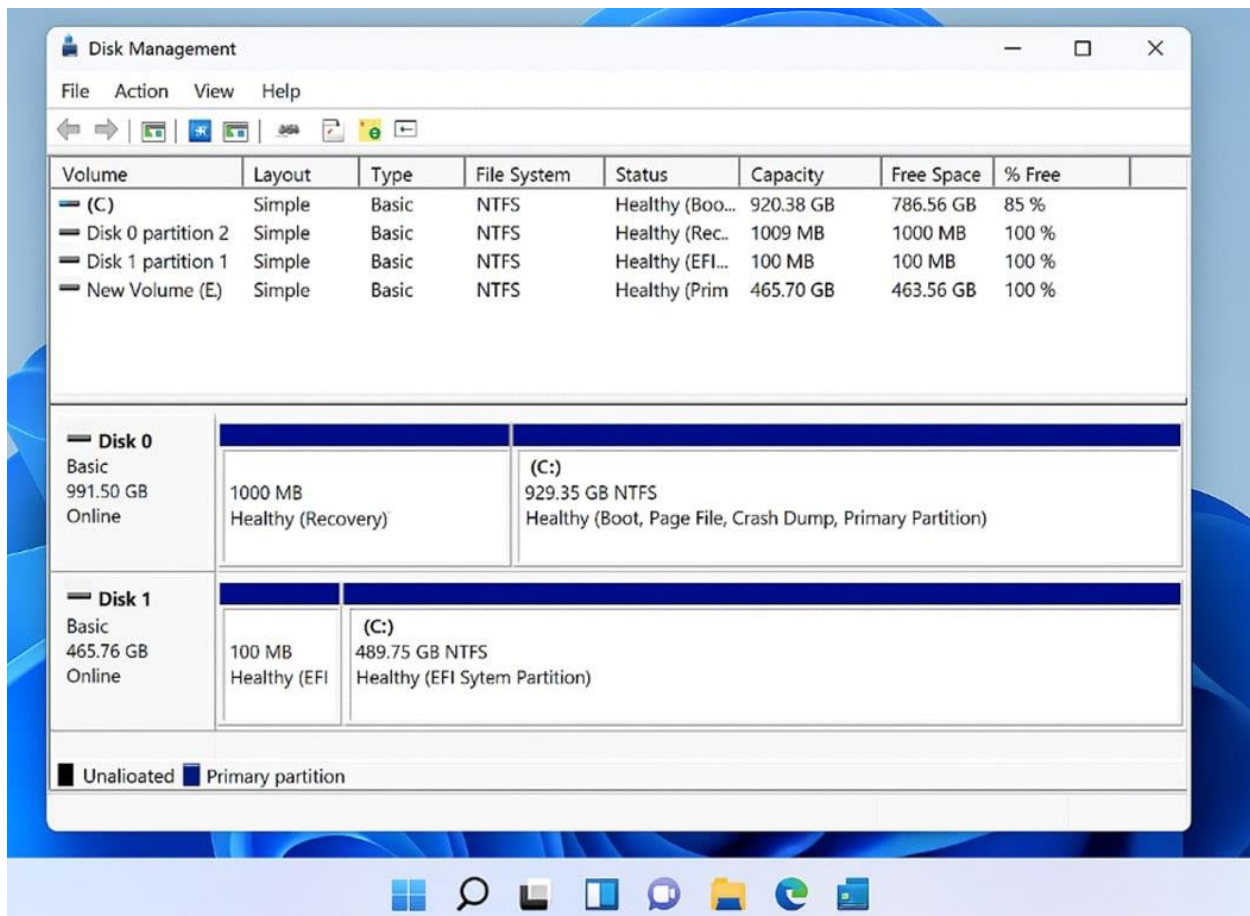
- **Custom Installation:**  
Installs Windows Server as a fresh copy.
- **Upgrade Installation:**  
Updates an old version without deleting files (not recommended for servers).
- **Advanced Options:**  
Allows you to choose partitions manually.



## Step 7: Select Disk / Partition

### Terms:

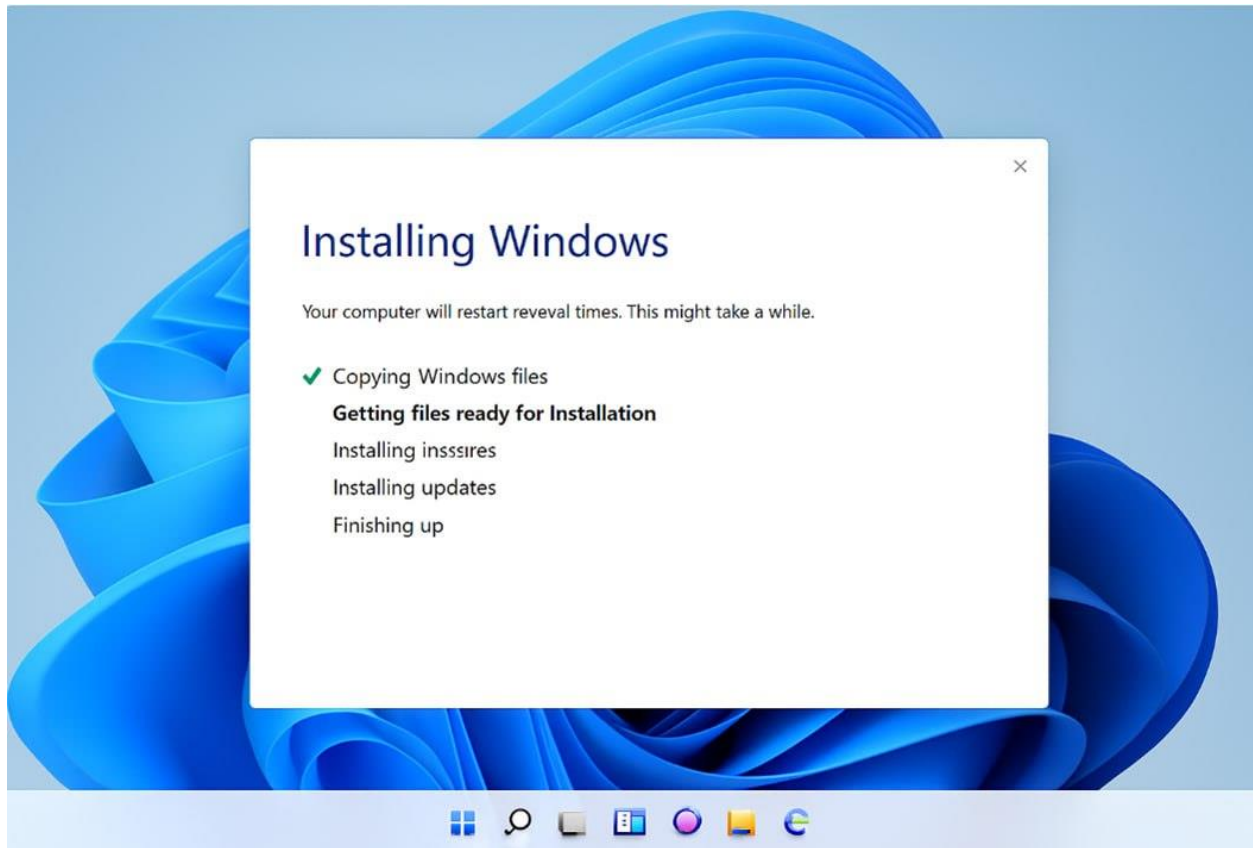
- **Drive:** The storage device (SSD/HDD) where Windows will be installed.
- **Partition:** A divided section of the drive used to store files.
- **Format:** Prepares the disk for installation.



## Step 8: Windows Installs Files

### Terms:

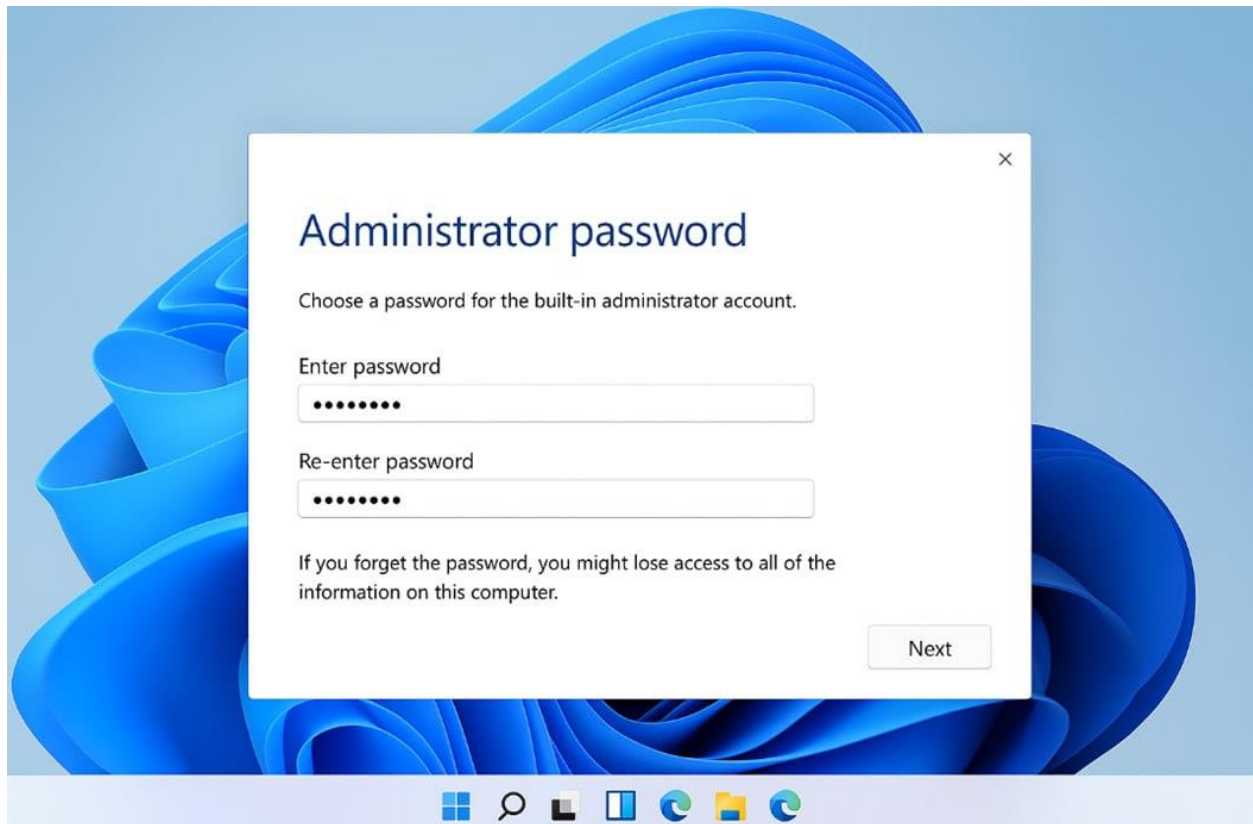
- **Copying Files:** Moves installation files to the hard drive.
- **Installing Features:** Adds Windows Server components.
- **Reboot:** Automatically restarts the system to continue installation.



## Step 9: Set Administrator Password

### Terms:

- **Administrator Account:** The highest-level account with full control over the server.
- **Strong Password:** A secure password required by Windows Server (complexity rules apply).



## Step 10: Log In to Windows Server

### Terms:

- **Ctrl + Alt + Delete:** The keyboard shortcut to access the login screen.
- **Sign In Screen:** Where you type your username and password.

## 2.3 Write the steps to create AD Users and User Groups.

### Steps to Create AD Users and User Groups

#### Pre-Step: Accessing Active Directory Users and Computers (ADUC)

1. Log in to your Domain Controller (Windows Server 2022).
2. Open Server Manager.

3. Click Tools in the top-right corner.
4. Select Active Directory Users and Computers from the drop-down menu.
5. In the left pane, expand your domain (e.g., contoso.local).

### **Step 1: Create an Organizational Unit (OU) (Optional, but Recommended)**

Creating an Organizational Unit (OU) is a best practice for organizing users and applying specific Group Policies to them without affecting the entire domain.

1. In the ADUC console, right-click on your domain name (e.g., contoso.local).
2. Select New → Organizational Unit.
3. Enter a descriptive name for the OU, such as IT\_Staff or Administrative\_Users.
4. Click OK.

### **Step 2: Create a New AD User Account**

1. In the ADUC console, right-click on the new OU you created (e.g., IT\_Staff) or the default Users container.
2. Select New → User.
3. Fill in User Identification Details:
  - First name:
  - Last name:
  - Full name:
  - User logon name:
4. Click Next.
5. Set Password and Options:
  - Enter and confirm a strong initial password.
  - Select the appropriate password policy options:
    - User must change password at next logon: (Standard security practice).
    - User cannot change password: (Used for highly controlled or service accounts).

- Password never expires: (Used for service accounts).
- Account is disabled: (For creating accounts ahead of time).

6. Click Next and then Finish

### **Step 3: Create a New AD Security Group**

Groups are used to bundle users together to simplify access control and policy application. Security groups are used to assign permissions.

1. In the ADUC console, right-click on the appropriate container (usually the same OU as the users, e.g., IT\_Staff).
2. Select New → Group.
3. Fill in Group Details:
  - Group name: IT\_Admins\_Global
  - Group scope: Define where this group can be applied. The most common for user groups is Global.
    - Global: Can contain members from its own domain and grant access to resources in any domain in the forest.
  - Group type: Select Security (to assign permissions to files, printers, etc.).
4. Click OK

### **Step 4: Add the User to the Group**

1. In the ADUC console, locate and double-click the newly created group (e.g., IT\_Admins\_Global) to open its properties.
2. Go to the "Members" tab.
3. Click the "Add..." button.
4. In the selection window, type the user's logon name.
5. Click "Check Names" to verify the user exists, and then click OK.
6. Click Apply and OK to close the group properties member and inherits all permissions assigned to the IT\_Admin