Network Infrastructure Overview

This project simulates a **virtual enterprise network** using a home lab environment built with **Oracle VirtualBox**.
The setup includes one **Windows Server 2022** instance and two **Windows 8** workstations, all connected to the same virtual NAT network for shared internet access and internal communication.

The **Windows Server** acts as the **central management system**, hosting key services such as:

- **Active Directory Domain Services (AD DS)** for identity and access management
- **DNS** – for name resolution
- **DHCP** – for dynamic IP allocation

The two **client machines**, representing the **IT Manager** and **Sales Manager** workstations, are joined to the same virtual network segment. This allows for seamless domain integration, centralized policy enforcement and secure communication with the server.

To reflect real-world IT security principles, both workstations are configured following the **Principle of Least Privilege (PoLP)** restricting user permissions and system access so that each user can perform only the tasks necessary for their role within the organization.

Setting Up On-Premises Identity and Access Management (IAM) Using Active Directory

To manage users, groups, and access control across our virtual environment, I'll implement an on-premises **Identity and Access Management (IAM)** system using **Active Directory (AD)**.

Before proceeding, I will ensure the following prerequisites are met:

- Windows Server 2022 is fully installed and configured.
- Windows 8 client machines (IT manager and Sales PCs) are set up and connected to the same virtual network.

- A **NAT Network** (created in the previous lab) is active, and all VMs are connected to it.
  (Refer back to the **"Setting Up a Virtual Home Lab"** repository if you need a recap on configuring NAT networks in VirtualBox).

Steps to Set Up Active Directory–Based IAM

- **Install Active Directory Domain Services (AD DS)** on the Windows Server.
- **Promote the server to a Domain Controller (DC).**
- **Create a new domain forest** - for example:Bayotech.Local Or Bayotech.com
- **Create Organizational Units (OUs)** to logically structure departments (e.g., IT, Sales and HR).
- **Create Security and Distribution Groups** for role-based access control.
- **Create User Accounts** for each employee and assign them to their respective OUs and groups.
- **Update DNS Settings** on the client PCs to point to the Domain Controller's IP address.
- **Create and Configure Group Policy Objects (GPOs)** to enforce security and access policies.
- **Assign Appropriate Policies** to users and groups based on roles and responsibilities.

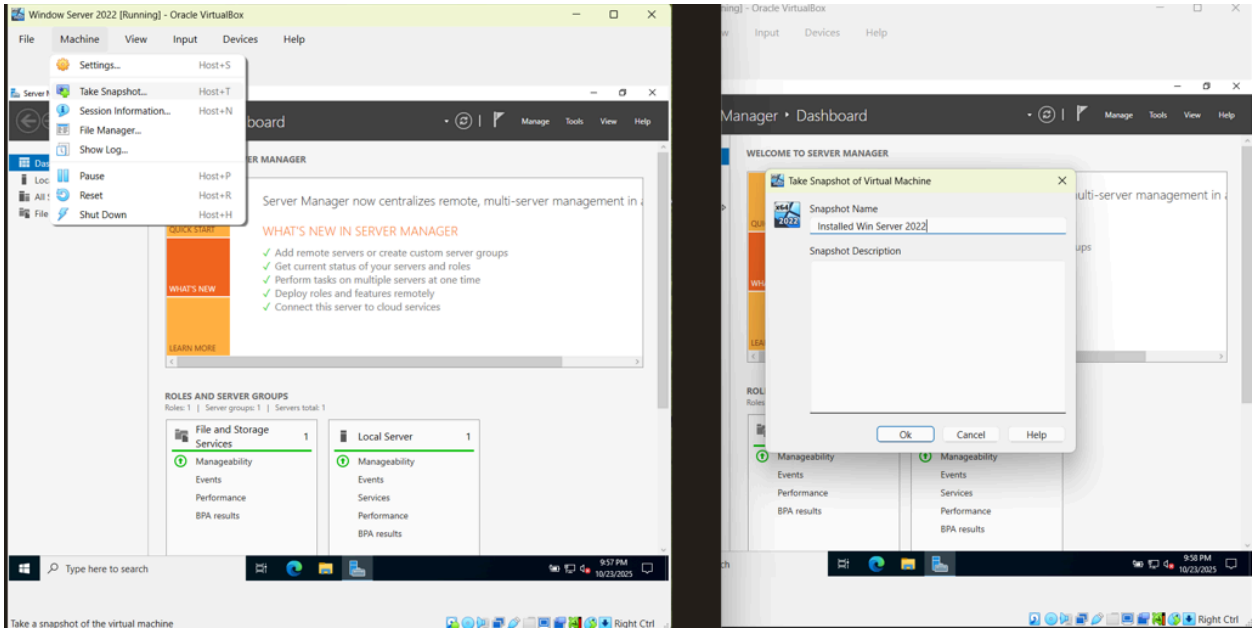
Once these steps are complete, the environment will have a fully functional Active Directory based IAM system, enabling centralized authentication, authorization, and policy management across your lab network.

Install Active Directory Domain Services (AD DS) on Windows Server

***Accessing the Windows Server VM

I will start by opening the **Windows Server VM**. Once it finishes loading, you'll be presented with the **Server Manager** dashboard, the main interface for managing server roles, features, and configurations.

Note→ (Optional) Before proceeding, **take a snapshot** of your server in VirtualBox. This snapshot serves as a restore point, if any configuration error occurs later, you can easily revert the VM to this stable state without reinstalling the OS.

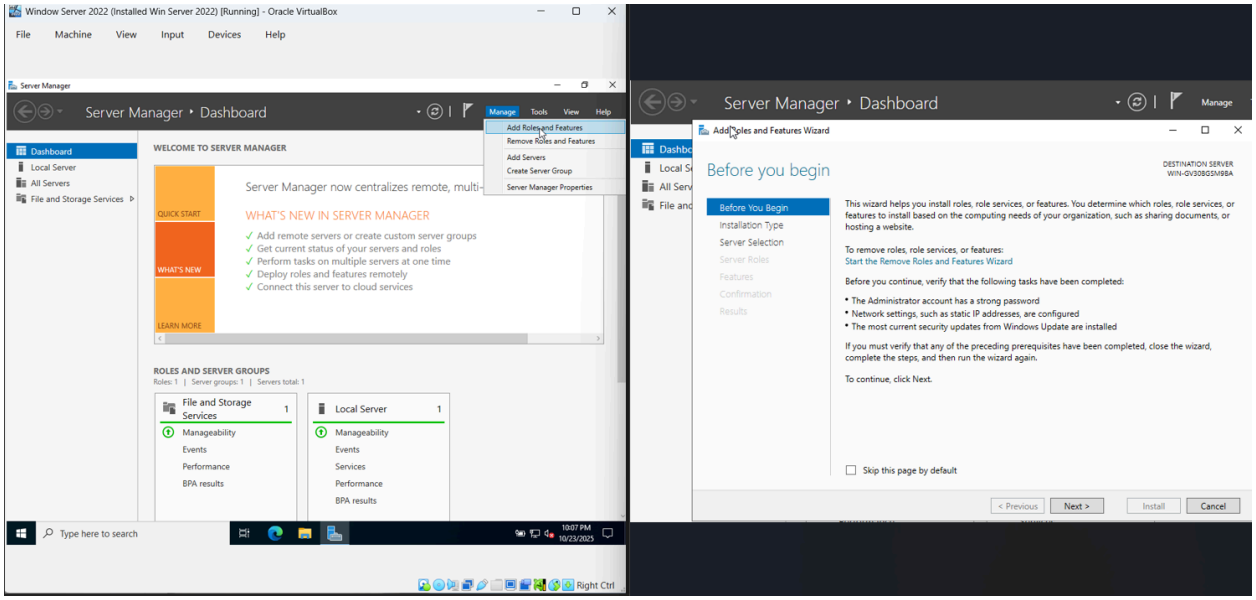


Steps in Server Manager

Once the **Server Manager** opens, wait a few moments for all services to fully load and you'll notice the status indicators changing from **red** to **green**. This confirms that the server roles and services are running properly before proceeding with any configuration.

Step 1→ Installing Active Directory Domain Services (AD DS)

- In **Server Manager**, click on **Manage → Add Roles and Features**.
- Click **Next** until the **Installation Type** page.

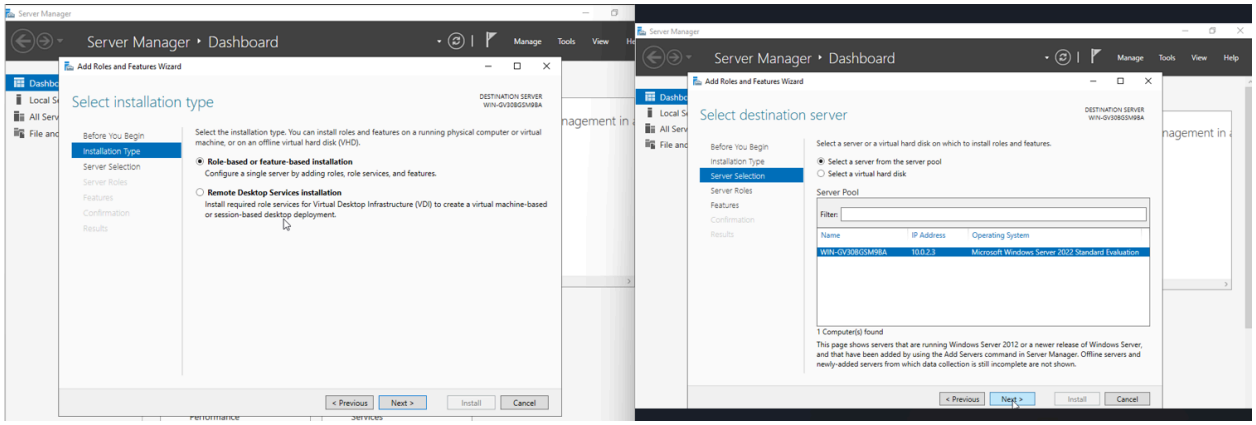


- I will be selecting **Role-based or feature-based installation**, then click **Next**.

- On the **Server Selection** page, I will choose my server from the list 'WIN-GV30BGSN9BA' (It displays my server's name and IP address).

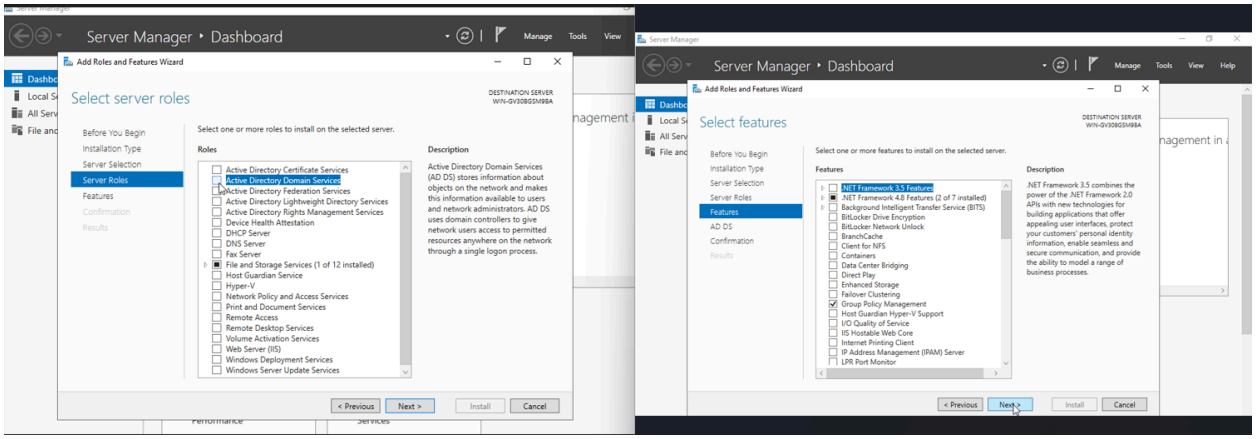
Note:-If multiple servers appear, ensure you select the correct one.

- Click **Next** to proceed to the **Server Roles** page.

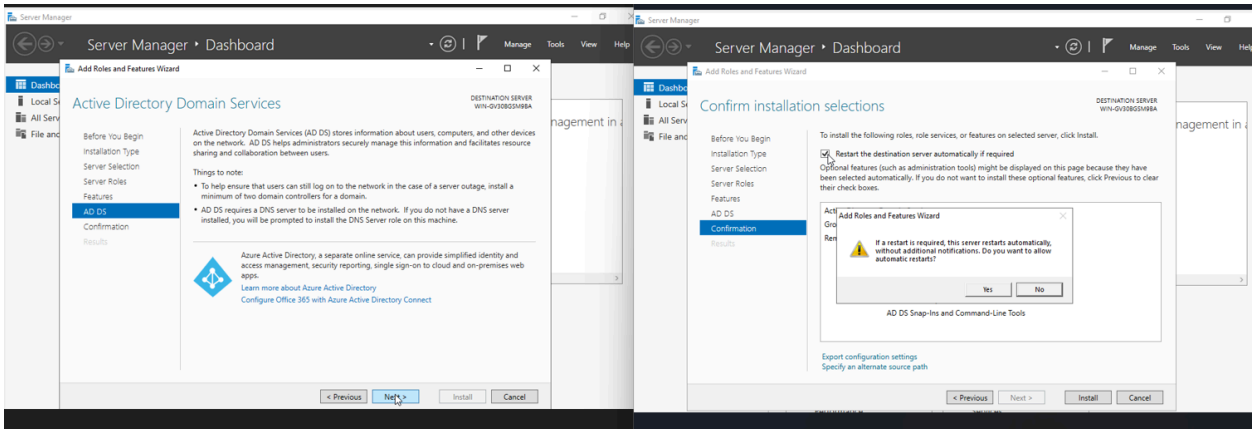


- I'll Check the box for **Active Directory Domain Services (AD DS)** ; this role enables centralized management of users, computers, and policies within a domain.

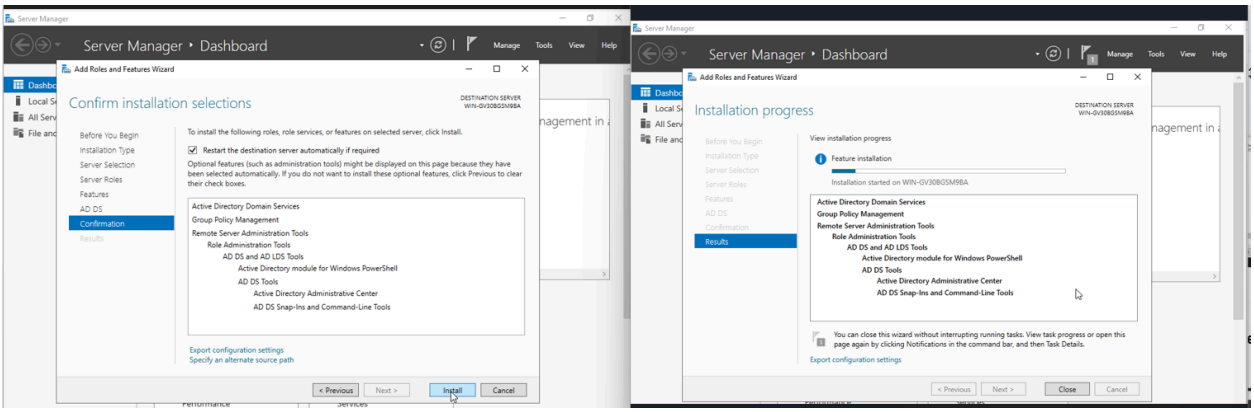
- Click **Next** through the **Features** page (leave default selections as they are).



- I'll continue clicking **Next** on the **AD DS** information page.
- On the **Confirmation** screen, I'll check **"Restart the destination server automatically if required"**, then confirm with **Yes**.

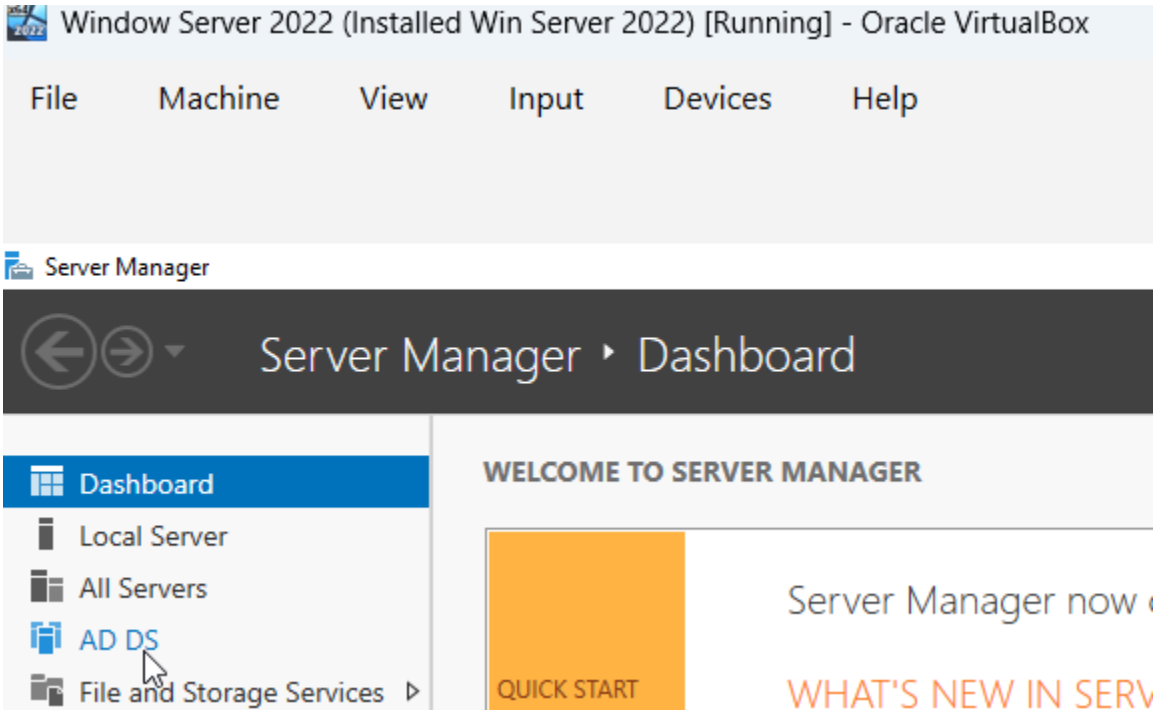


- Click **Install** to begin the installation.(Installation in progress,might take few seconds to minutes)



Note→ This process installs **Active Directory**, which acts as the backbone of my domain network, which manages authentication, permissions, and organizational policies across all connected systems.

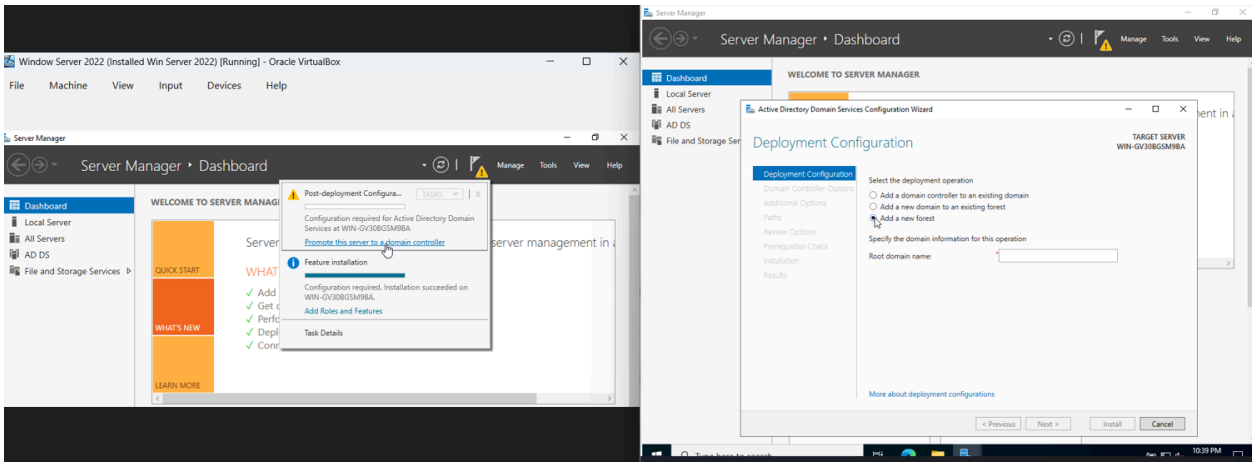
Once the installation is complete,I'll close the installation window. AD DS will be seen under the Dashboard.



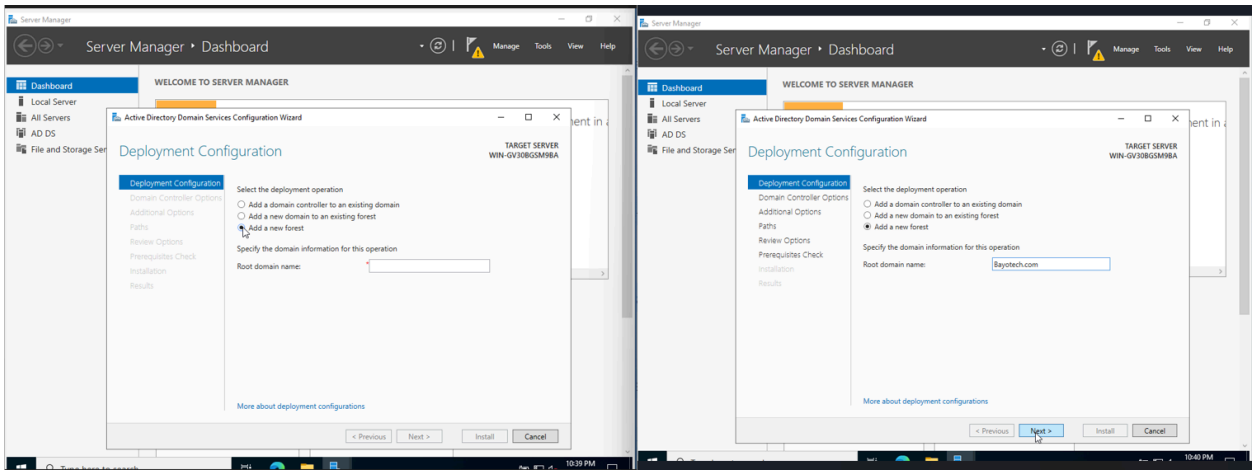
Step 2→ Promoting the Server to a Domain Controller (DC)

Once Active Directory Domain Services (AD DS) has been installed, the next step is to promote the server to a Domain Controller.

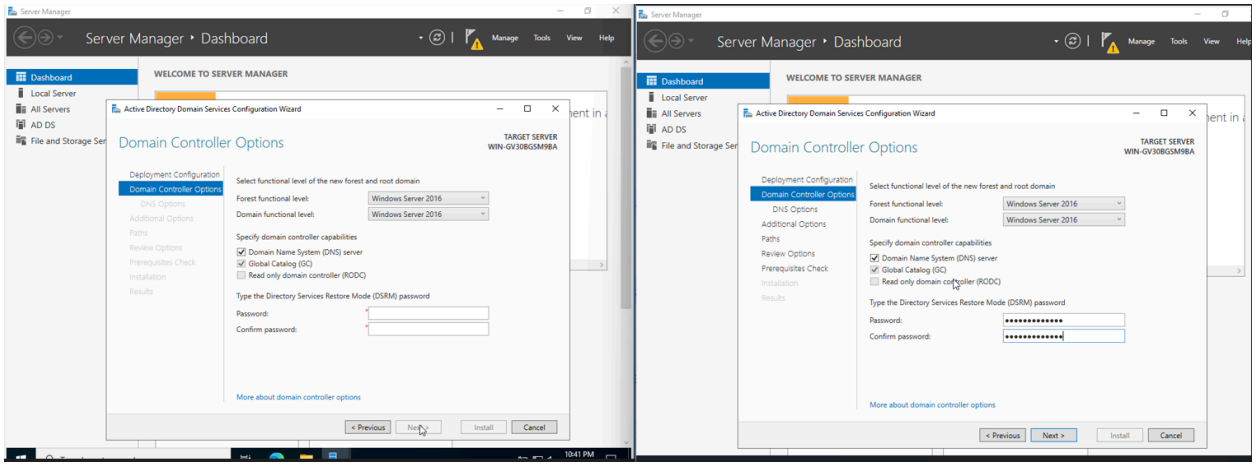
- In Server Manager,I'll click on the notification flag at the top.
- Select "**Promote this server to a domain controller.**"
- In the Deployment Configuration window, I'll choose **"Add a new forest."**



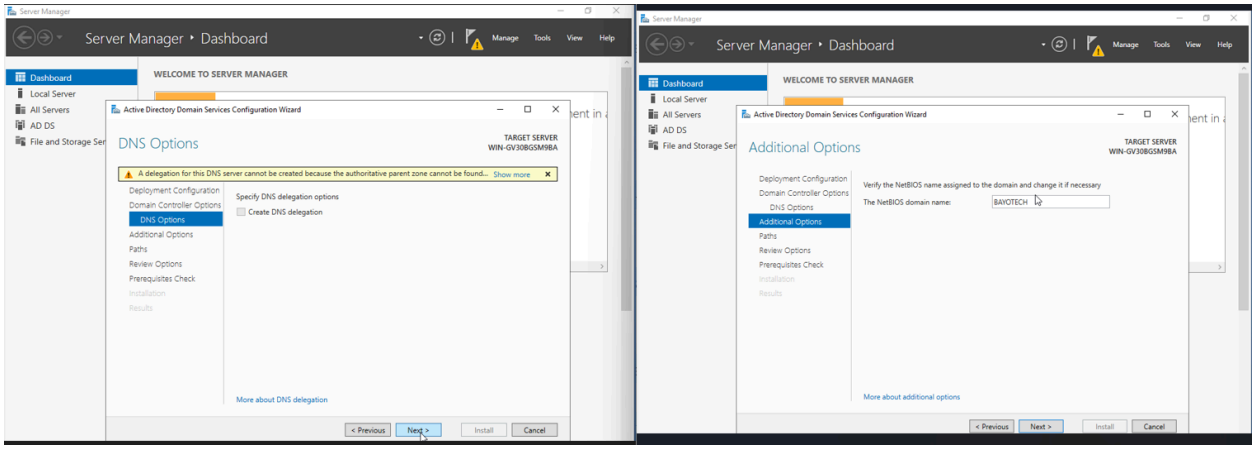
- Under Root domain name, I'll enter the name of my organization's domain for this setup, I'll use **Bayotech.com**.
- Click **Next**.



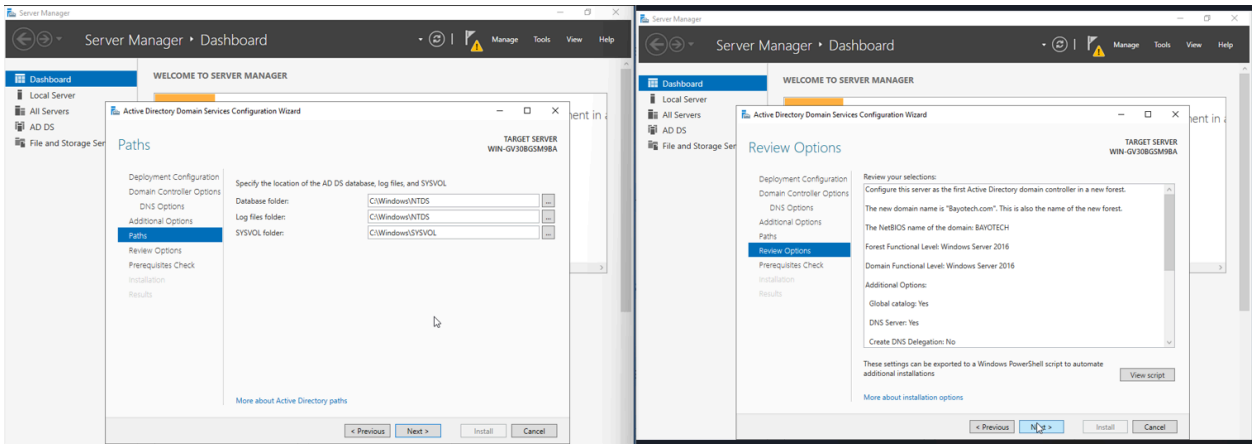
- In Domain Controller Options, I'll create and confirm a **Directory Services Restore Mode (DSRM)** password, then click **Next**.



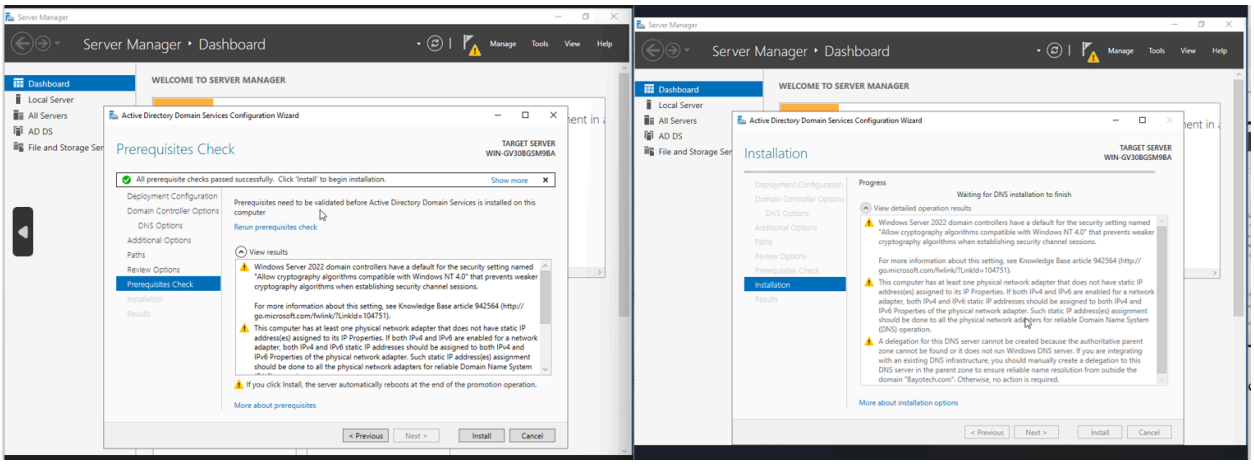
- On the DNS Options page, I'll click Next (you can leave the default settings).
- Under Additional Options,I'll verify that the **NetBIOS** domain name is automatically generated, typically in my case it is **'BAYOTECH'** then click Next.



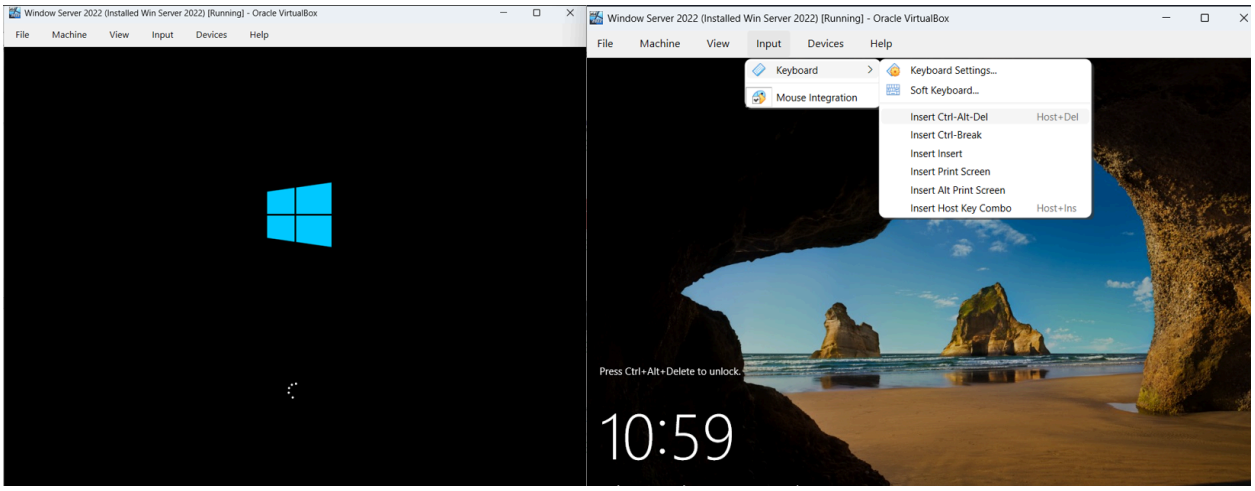
- I'll Review the Paths section (default directories are acceptable), then click **Next.**
- On the Review Options page, click **Next** to continue.



- I'll Wait for the Prerequisites Check to complete successfully, then click **Install.**



Note→ Once installation begins, the system will automatically configure the domain and restart upon completion. After rebooting, the server will now function as a Domain Controller (DC) for the **Bayotech.com domain**.

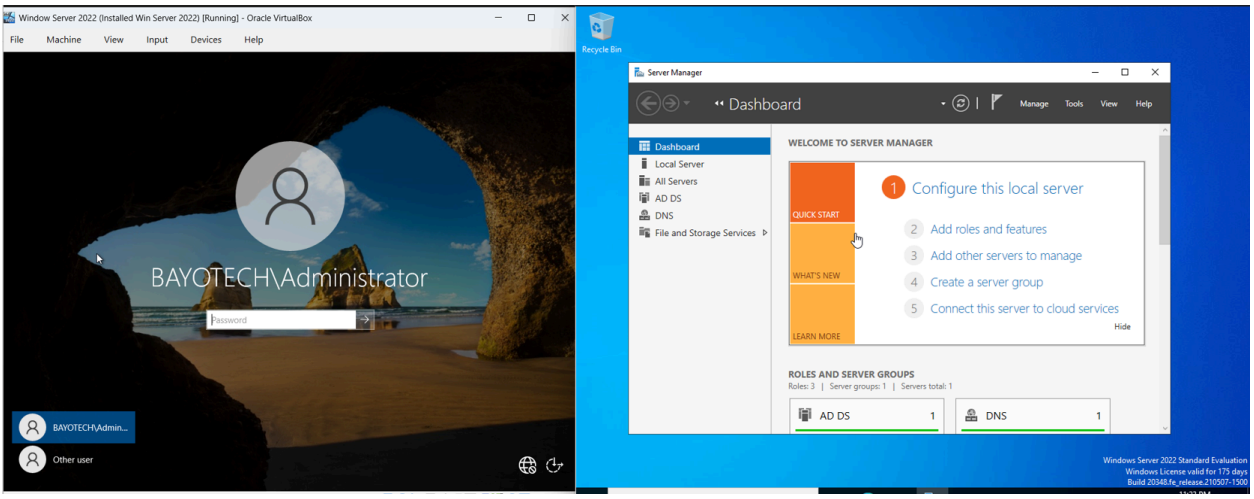


Logging In After Domain Controller Promotion

After the Active Directory installation and promotion to a Domain Controller, the server will automatically restart.

Upon reboot, I'll now need to log in using your domain credentials instead of the local administrator account. LOG IN as: **BAYOTECH\Administrator**.

Using the password I created earlier during the Active Directory configuration process. Once logged in, The server is now operating as the primary Domain Controller (DC) for the **Bayotech.com** domain.



Note → Understanding Active Directory Control

Active Directory (AD) enables centralized management and policy enforcement across all devices joined to a domain. Once a computer is connected to the domain, it adheres to the domain's policies regardless of its physical location or network connection.

For example, if a **Group Policy Object (GPO)** disables external ports (such as USB access), that restriction will apply automatically to any domain-joined computer.

In summary, the AD configuration process involves:

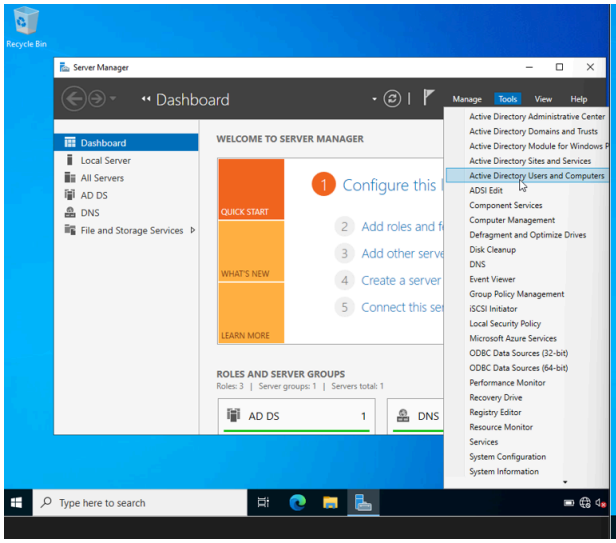
1. Installing **Active Directory Domain Services (AD DS)**
2. Creating and promoting a **Domain Controller (DC)**
3. Defining a domain (e.g., Bayotech.com)
4. Creating **Organizational Units (OUs)**, **Groups**, and **Users** to apply and manage permissions and policies efficiently.

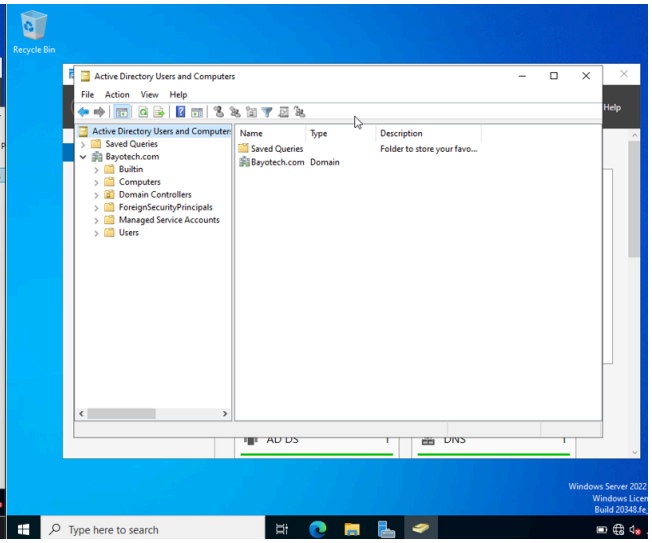
CREATING ORGANIZATION UNITS (OUs)

Once the Server Manager has fully loaded, it's time to create Organizational Units (OUs) to logically group and manage users, computers, and resources within the domain.

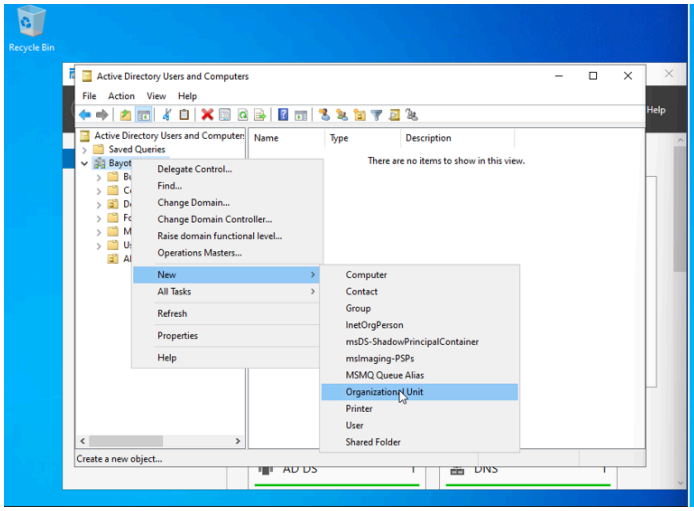
Steps→

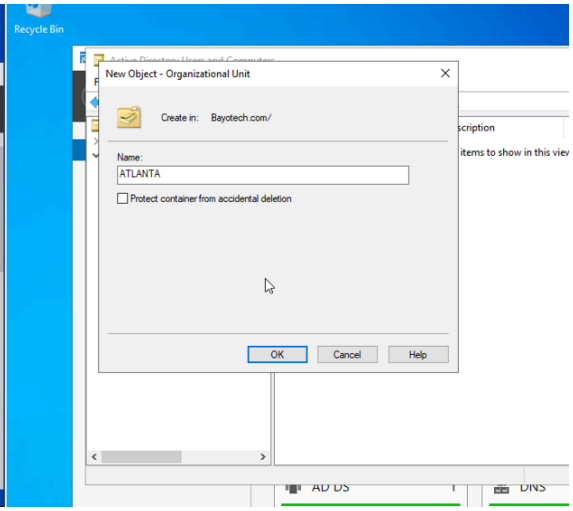
- In Server Manager, I'll navigate to the top-right menu and click **'Tools'** → '**Active Directory Users and Computers'**.
- In the left-hand panel,I'll expand the domain **'Bayotech.com'.** I can see the domain's default containers and structure.



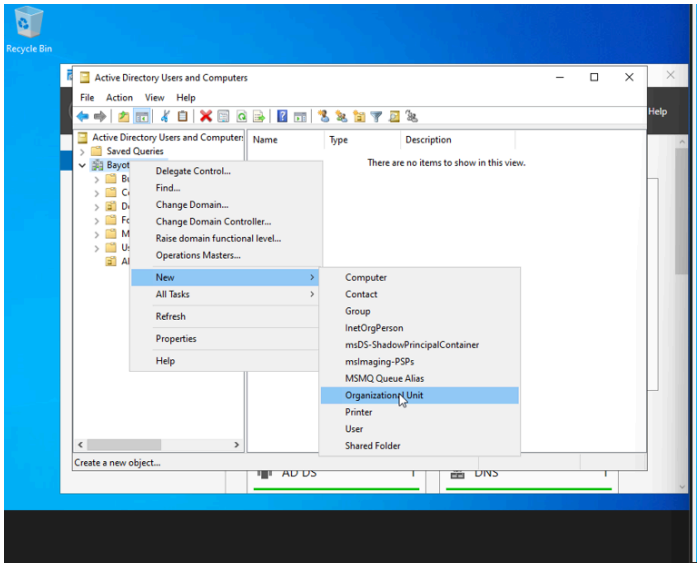


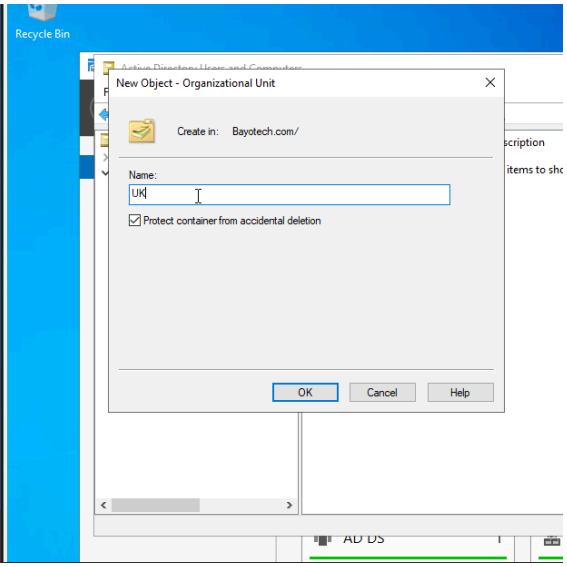
- I'll right-click on "**Bayotech.com**" → **New** → **Organizational Unit.**
- In the New Object-Organizational Unit dialog box:
  - I'll enter the name of the OU. (In this example: **Atlanta**)
  - Uncheck **"Protect container from accidental deletion"** if you want the option to remove it later.
- Click OK to create the OU.

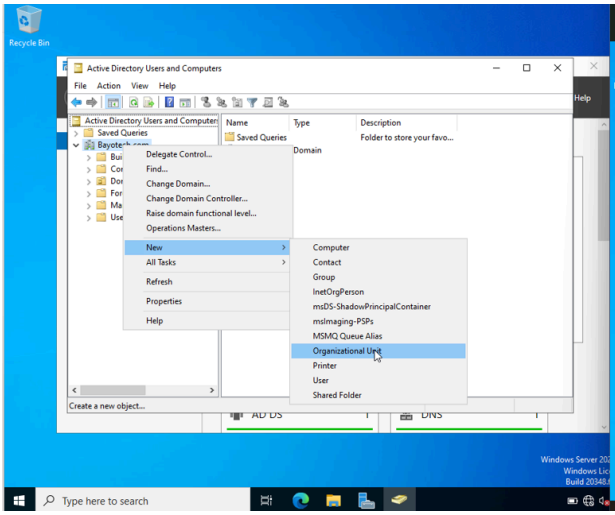


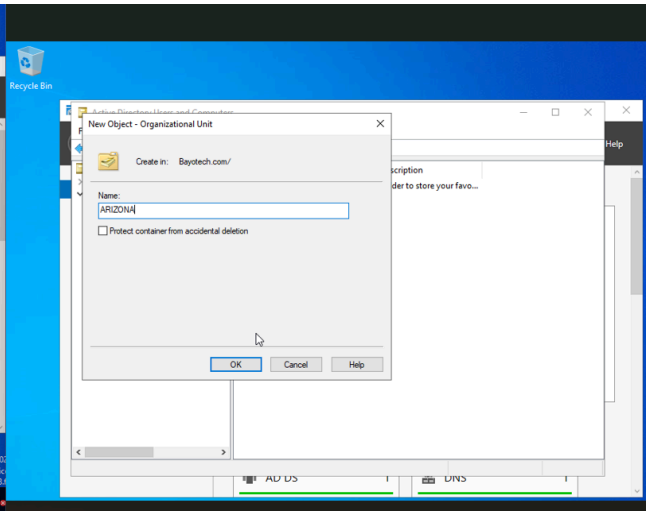


- Repeat the same process to create additional OUs ; for example, UK and Arizona to represent different branch locations or departments.







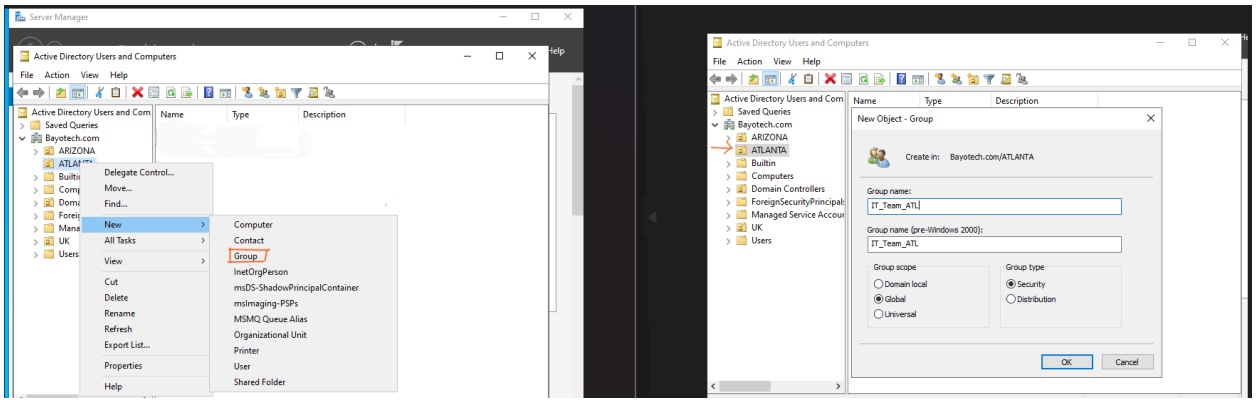


Creating Groups within Organizational Units

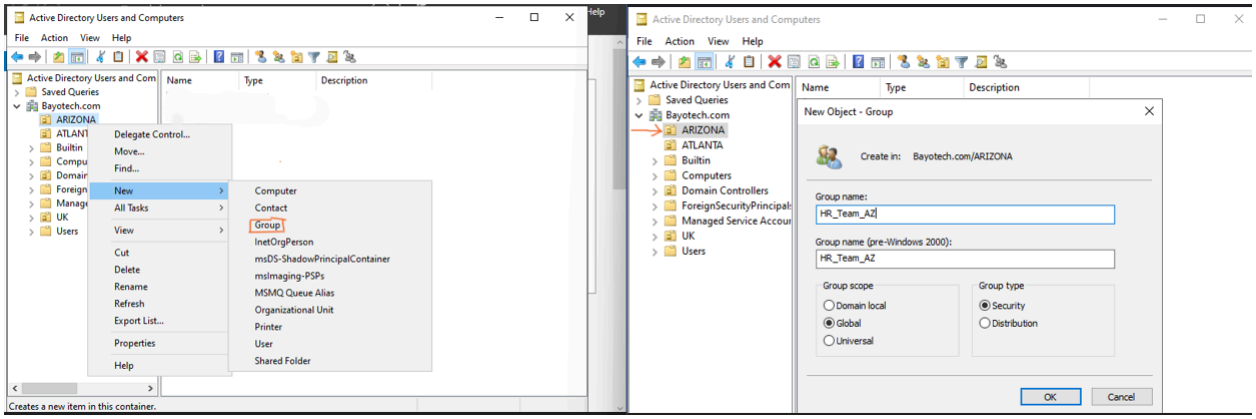
After setting up my Organizational Units (OUs), the next step is to create Groups.
Groups make it easier to manage permissions, access control, and policy assignments for multiple users at once.

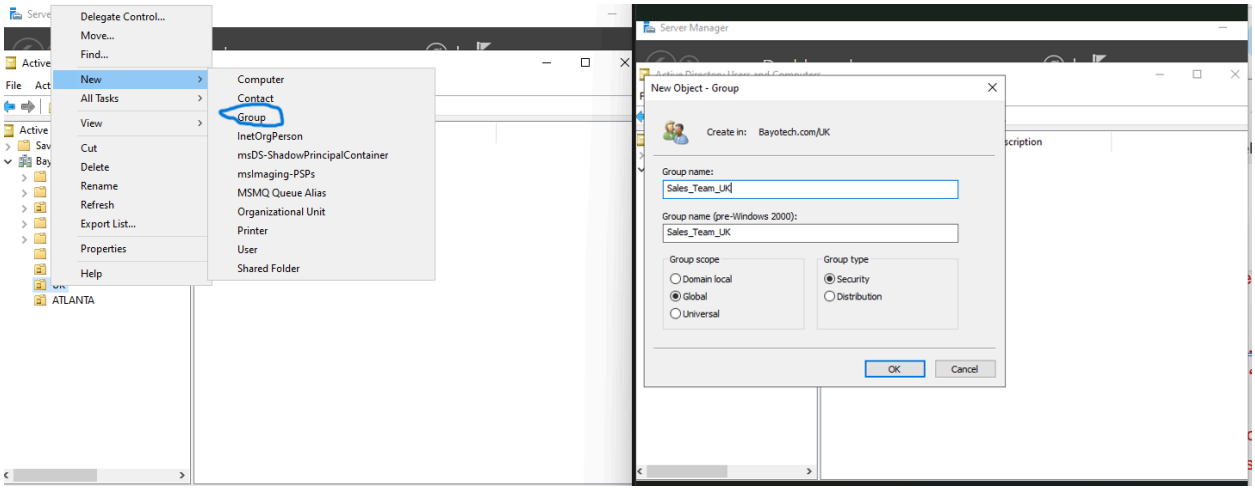
Steps→

- In Active Directory Users and Computers, I'll expand Domain **(Bayotech.com)** and navigate to the OU where I want to create the group, for example, **Atlanta.**
- I'll Right-click the **OU (Atlanta) → New → Group.**
- In the '**New Object**' Group dialog box:
    1. **Group name:** Enter a descriptive name (I am using **IT_Team_ATL**).
    2. **Group scope:** I'll Choose Global → suitable for grouping users within the same domain.
    3. **Group type:** I'll Select Security→this type of group is used to assign permissions and enforce policies.
       Click **OK** to create the group.



Repeat this process to create other groups as needed (e.g., HR_Team_AZ, Sales_Team_UK).





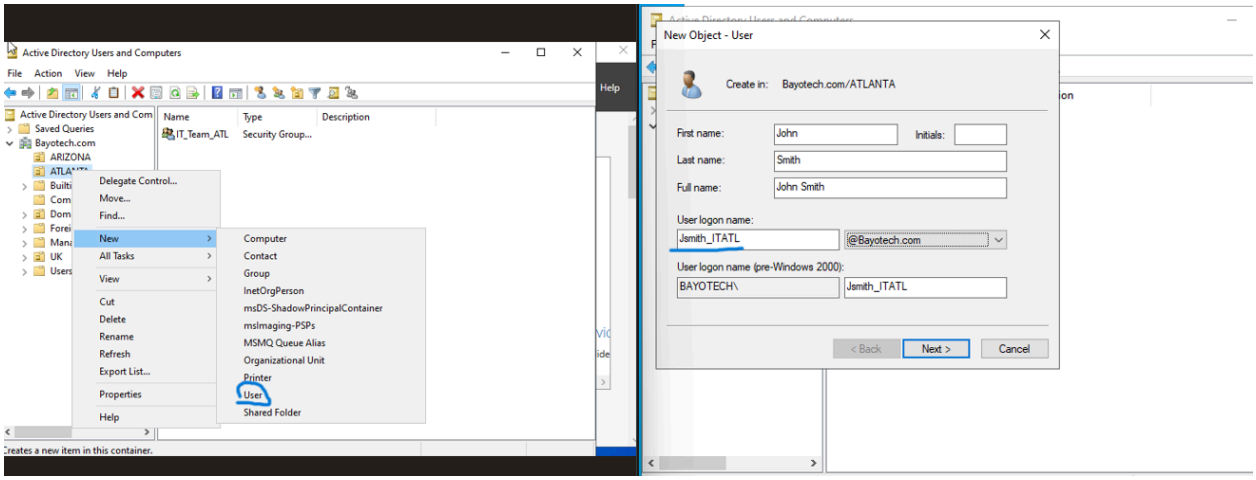
NOTE→ Organize your groups based on **function** (e.g., Sales, IT, HR) or **location** (e.g.,Atlanta,UK and Arizona,). This structure simplifies applying **Group Policies** and managing permissions efficiently across your network.

Creating Users and Assigning Them to Groups

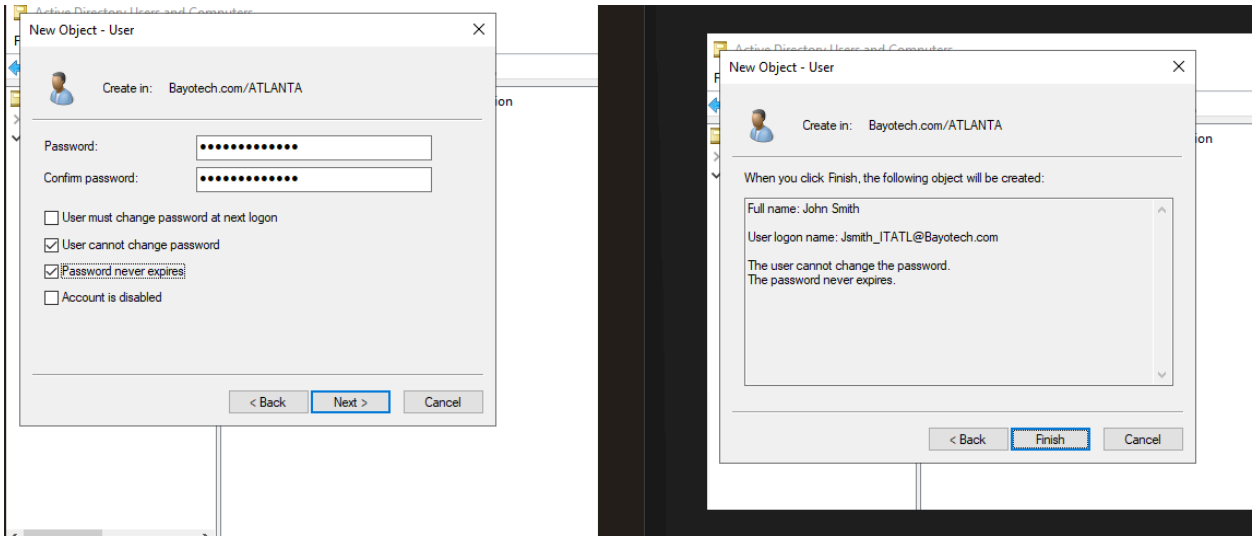
Now that the **Organizational Units (OUs)** and **Groups** are set up, the next step is to create **user accounts** and assign them to their respective groups. This step simulates real-world user management in an enterprise environment.

Steps:

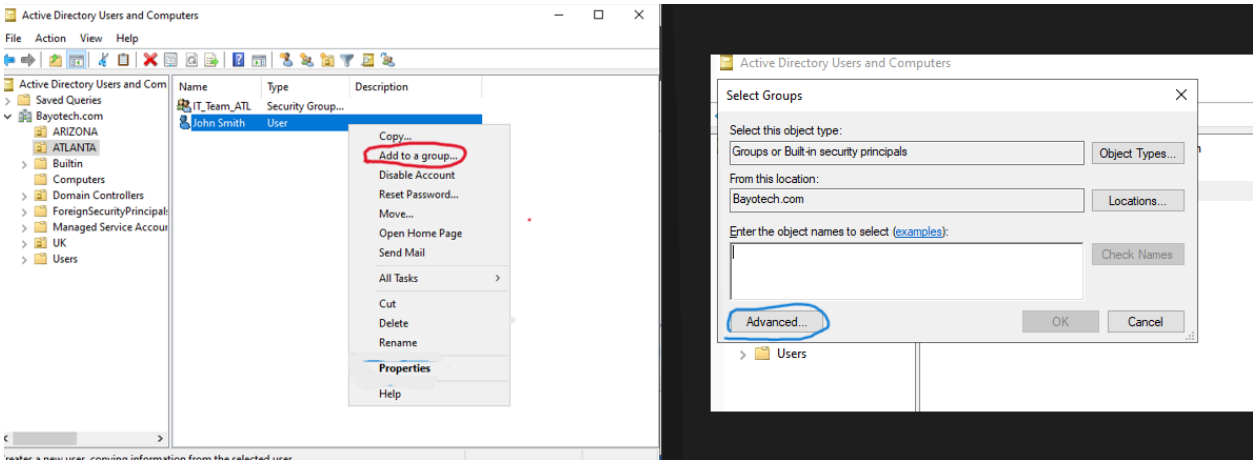
- In **Active Directory Users and Computers**,I'll navigate to the OU where the user belongs (for example, **ATLANTA**).
- Right-click the OU (**ATLANTA**) → **New** → **User**.
- In the **New Object – User** dialog box:
    - I'll Enter the First name, Last name, and User logon name (I am using- **John Smith, Userlogon:- Jsmith_ITATL)**.
    - Click **Next**.

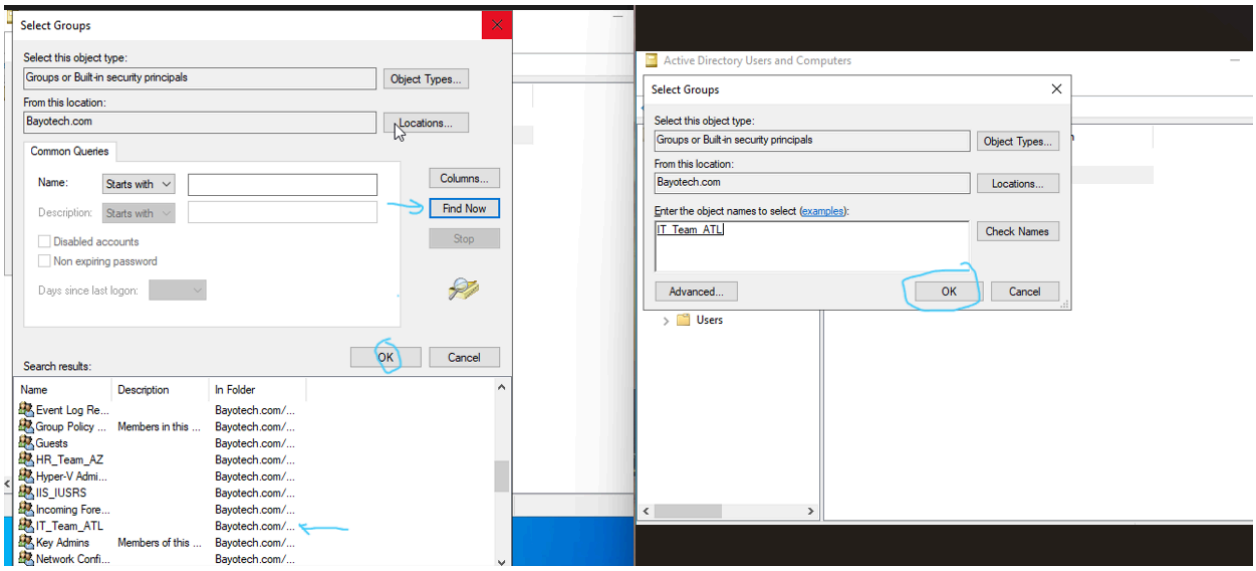


- Set a **password** for the user account.
    - You can uncheck **"User must change password at next logon"** for lab environments.
    - Optionally, check **"Password never expires"** if this is for testing or demonstration purposes.
    - Click **Next → Finish**.



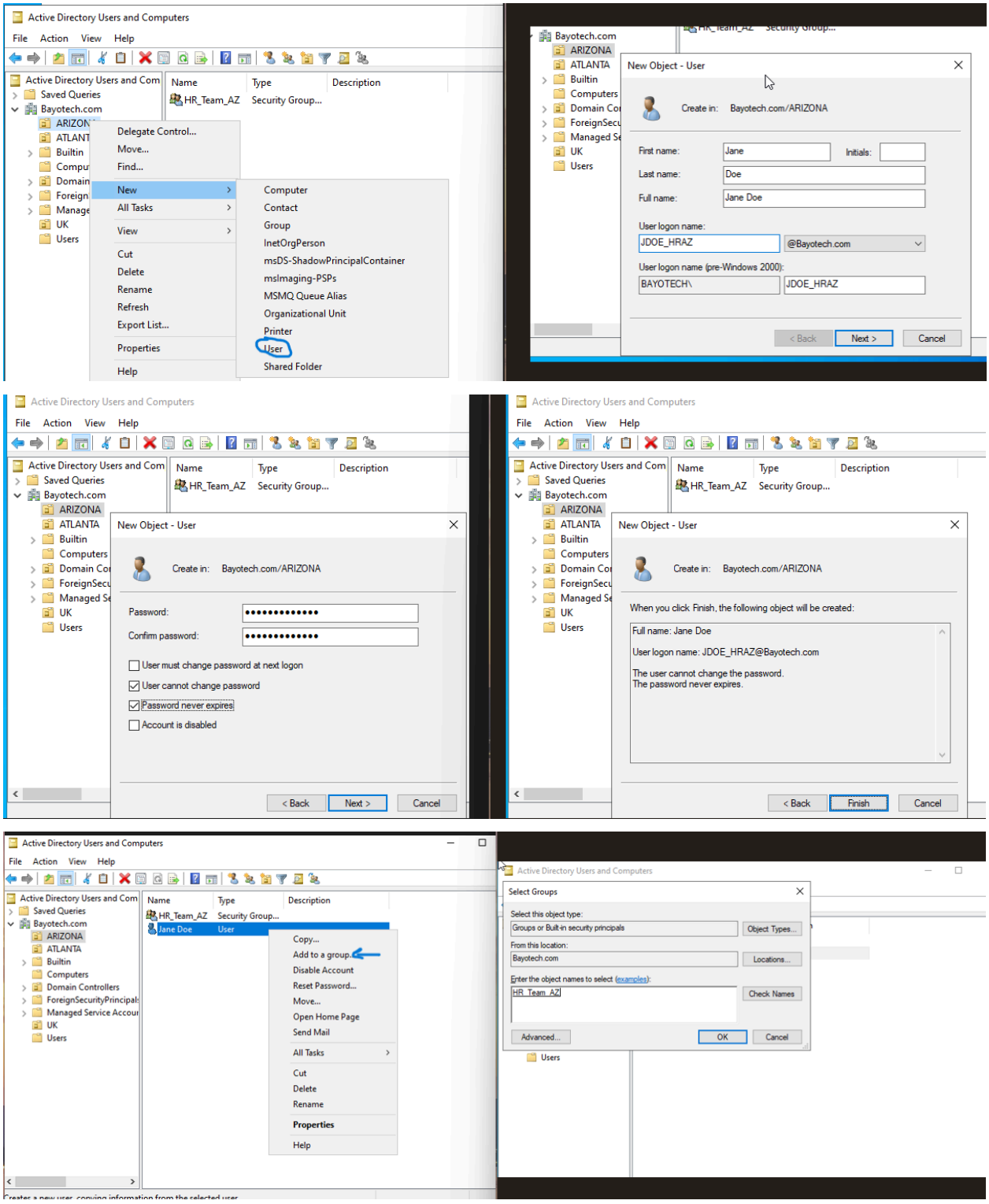
- Once the user is created, I'll right-click on the user's name → **Add to a group**.
- Click on **'Advance'** to search for a group name.
- Type the name of the group I want to add the user to **(e.g., IT_Team_ATL)** and click **OK.**



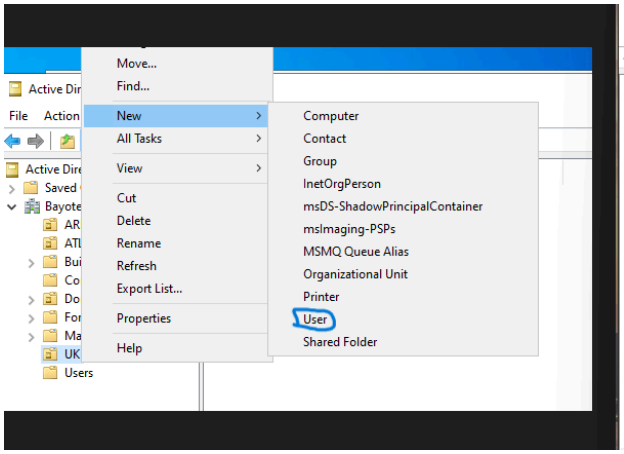


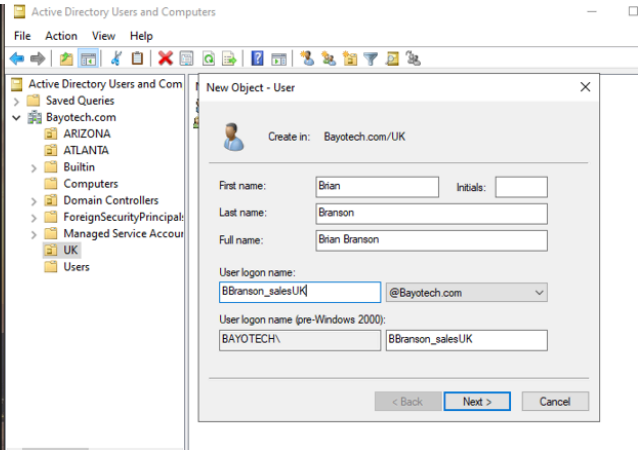
NOTE→ When Creating users within the right OUs and assigning them to specific groups ensures that Group Policies and permissions apply automatically based on their role and location.

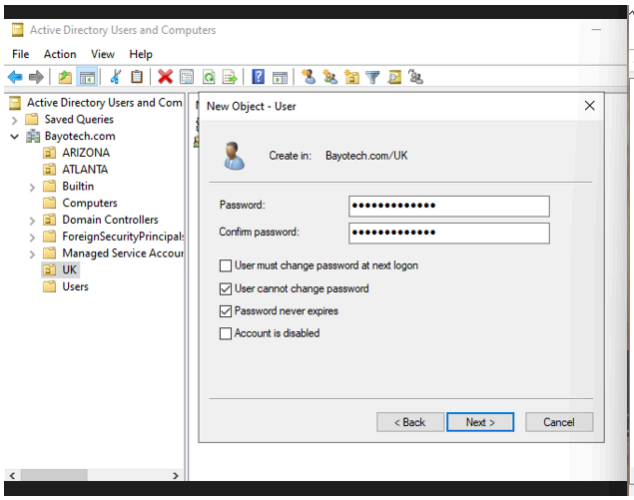
Repeat this process to create other Users as needed and Add them to the Group (e.g., User;-Jane Doe with HR_Team_AZ)

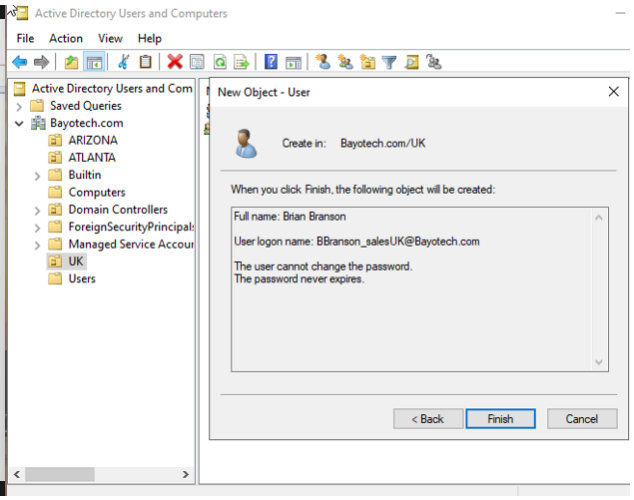


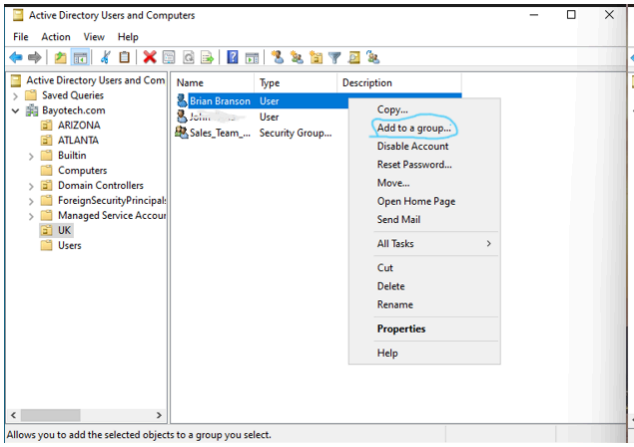
User;- Brian Branson with Sales_Team_UK.

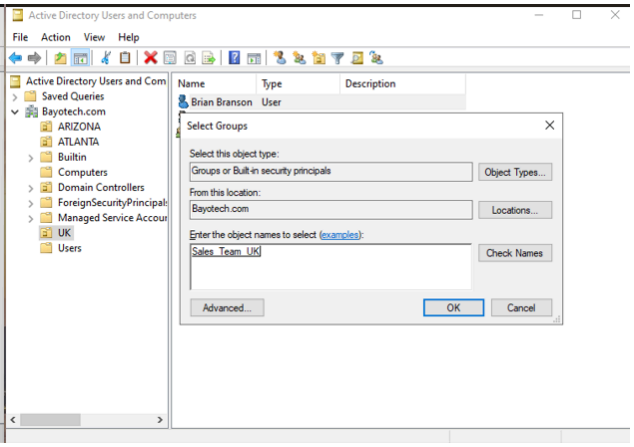

Move...
Find...
New
All Tasks
View
Cut
Delete
Rename
Refresh
Export List...
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder


Active Directory Users and Computers
File Action View Help
New Object - User
Create in: Bayotech.com/UK
First name: Brian
Initials:
Last name: Branson
Full name: Brian Branson
User logon name:
BBranson_salesUK
@Bayotech.com
User logon name (pre-Windows 2000):
BAYOTECH\
BBranson_salesUK
< Back
Next >
Cancel


Active Directory Users and Computers
File Action View Help
New Object - User
Create in: Bayotech.com/UK
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel


Active Directory Users and Computers
File Action View Help
New Object - User
Create in: Bayotech.com/UK
When you click Finish, the following object will be created:
Full name: Brian Branson
User logon name: BBranson_salesUK@Bayotech.com
The user cannot change the password.
The password never expires.
< Back
Finish
Cancel


Active Directory Users and Computers
File Action View Help
Name
Type
Description
Brian Branson User
Sales_Team_... Security Group...
Copy...
Add to a group...
Disable Account
Reset Password...
Move...
Open Home Page
Send Mail
All Tasks
Cut
Delete
Rename
Properties
Help
Allows you to add the selected objects to a group you select.


Active Directory Users and Computers
File Action View Help
Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
Bayotech.com
Locations...
Enter the object names to select (examples):
Sales_Team_UK
Check Names
Advanced...
OK
Cancel

ASSIGNING DEVICE TO NEW EMPLOYE IN ATLANTA WITH IT DEPT

Assigning a Device to a New Employee (Atlanta Office)

Now that I have created a new user account '**John Smith'** under the Atlanta Organizational Unit (OU) within the IT group, the next step is to assign and connect a device for this employee.

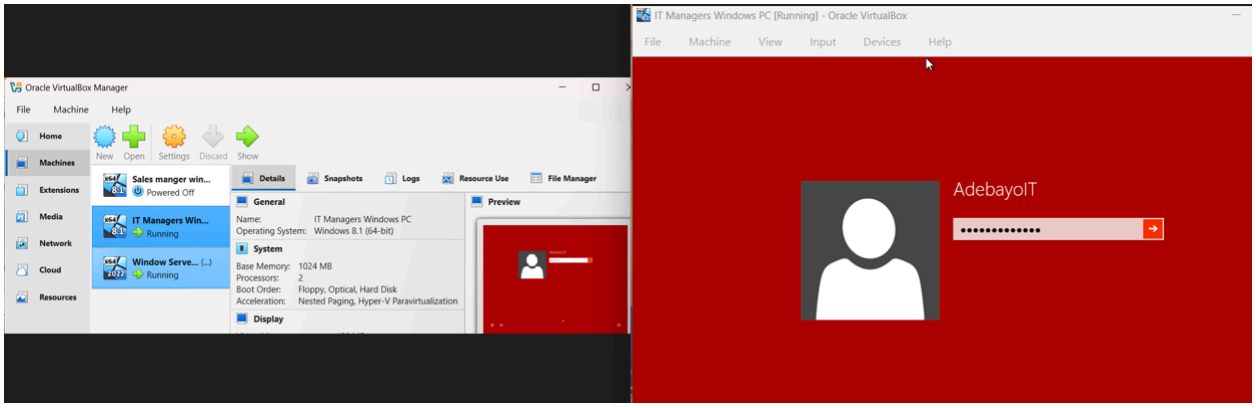
This process involves joining the user's computer to the domain, allowing domain policies, permissions, and configurations to apply automatically.

Joining John Smith's Device to the Domain Controller (Windows Server 2022)

Now that I've created the user **John Smith** under the **OU Atlanta → IT**, the next step is to **join his workstation (Windows 8 PC)** to the **Bayotech.com** domain managed by the Windows Server 2022 Domain Controller, Follow the steps below:

STEP 1→ Power On the User Device

Start the **Windows 8 workstation** (From the VirtualBox) that will be assigned to **John Smith**. This device will be joined to the **domain controller** so that it can receive domain policies and configurations.

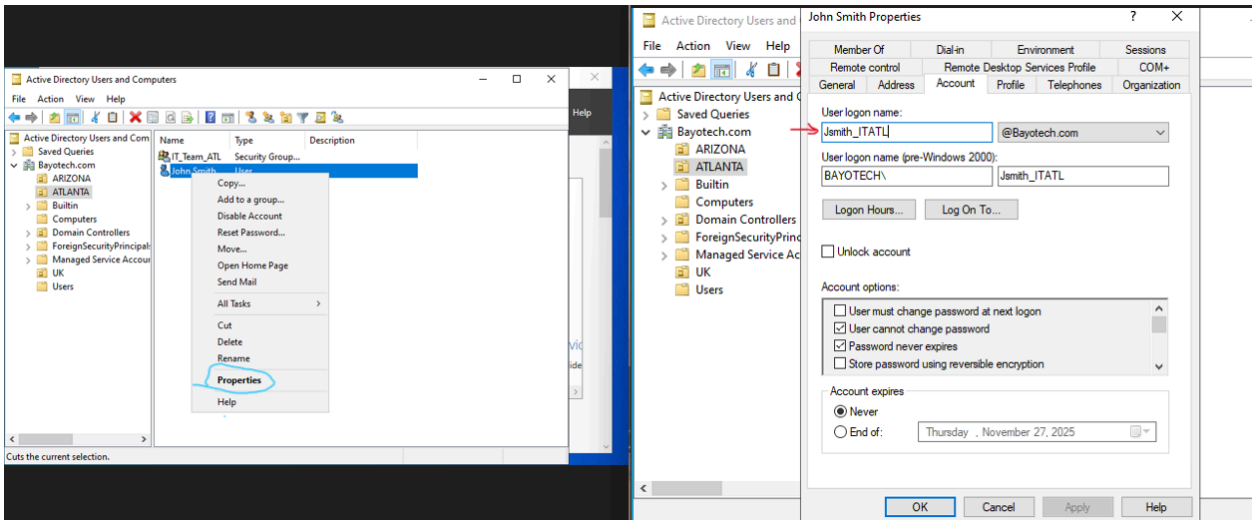


STEP 2→Verify User Account Details

On the Windows Server (Domain Controller):

- I'll Open **Active Directory Users and Computers (ADUC)**.
- Locate and **right-click** the user **John Smith → Properties → Account**.
- Note the **User logon name**, it should appear as:Jsmith_ITATL@Bayotech.com

Note → This confirms the user's domain credentials that will be used when logging into the assigned workstation after it's joined to the domain.

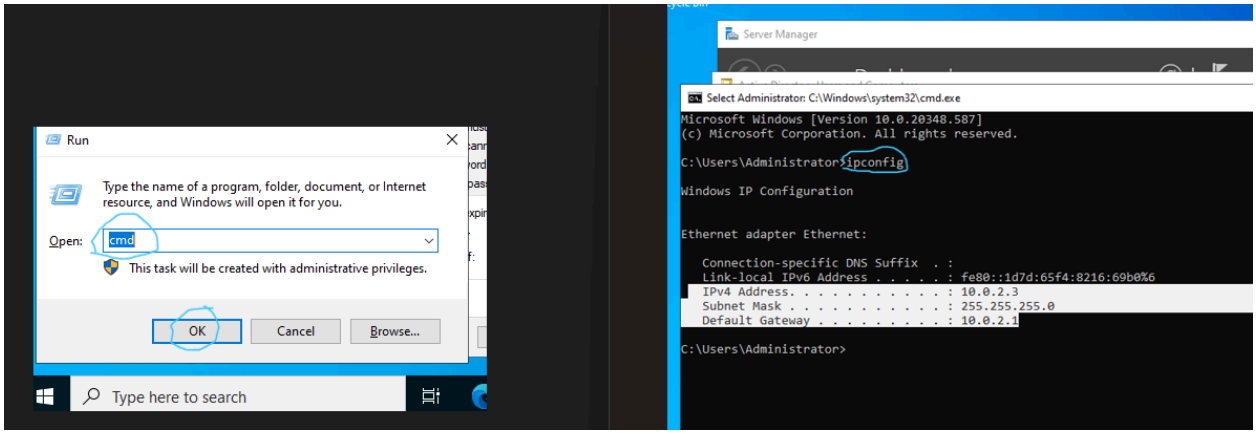


STEP 3→ Check the Server and Workstation IP Addresses

Before joining the workstation to the domain, verify the IP configuration of both the Windows Server and the Sales Windows PC to ensure they're on the same network.

On the Windows Server:

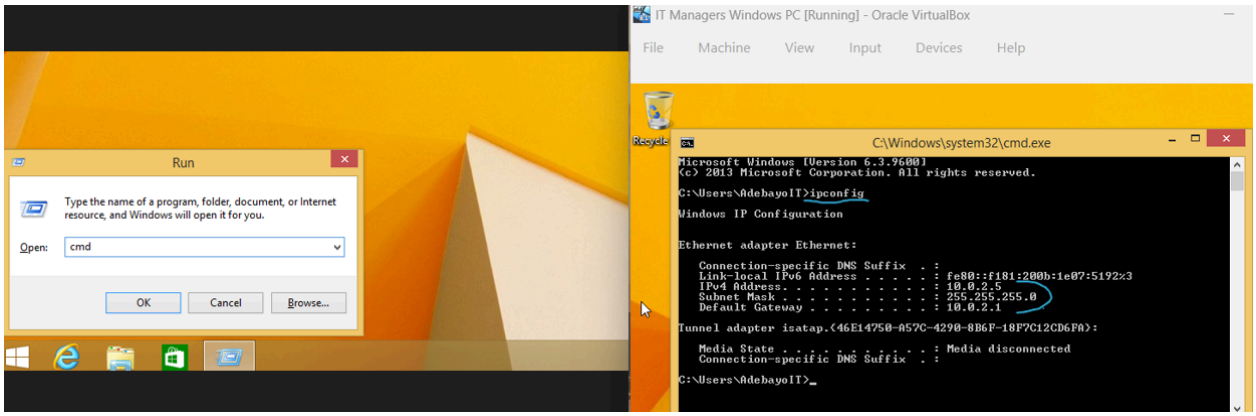
- Press **Win + R**, type **'cmd'**, and press **'Enter'** to open the **Command Prompt**.
- Type **'ipconfig'** and press **'Enter'**.
- Note down the I**Pv4 Address, Subnet Mask, and Default Gateway** ,this identifies my server's network settings.



On the Sales Windows PC:

Repeat the same process ,Open Command Prompt and run **`ipconfig`** to view the **PC's network details.**

NOTE→Ensure that both systems are on the **same subnet** and that the **server's IP** will later be used as the **DNS address** for the client PC. This step is crucial for successful domain joining.



STEP 4→ Test Network Connectivity Between the Workstation and Server

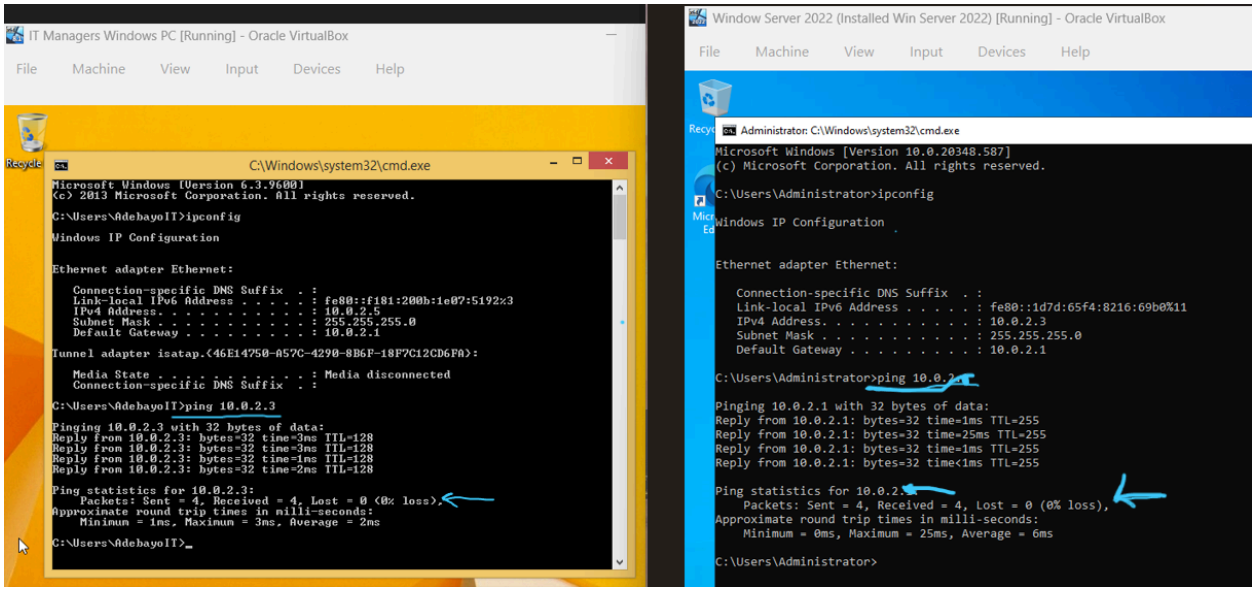
I will verify that the **IT Manager Windows PC** (assigned to John) can communicate with the **Windows Server** over the network.

- On the IT manager Windows PC, while still on the Command Prompt from **Step 3,** I'll type the following command (replace the IP with my server's actual address):`ping 10.0.2.3` and press '**Enter'**.

- **On the Server PC,** Repeat the same process, while still on the **Command Prompt** on the Windows Server ping the **IT Manager PC's IP address**. By command:`ping 10.0.2.5`

NOTE→ If the **Packets Sent** and **Packets Received** values match, it confirms successful communication meaning the workstation and the server are on the same network and can exchange data.A successful PING confirms that the client can reach the domain controller, allowing me to proceed with **joining the PC to the domain**.

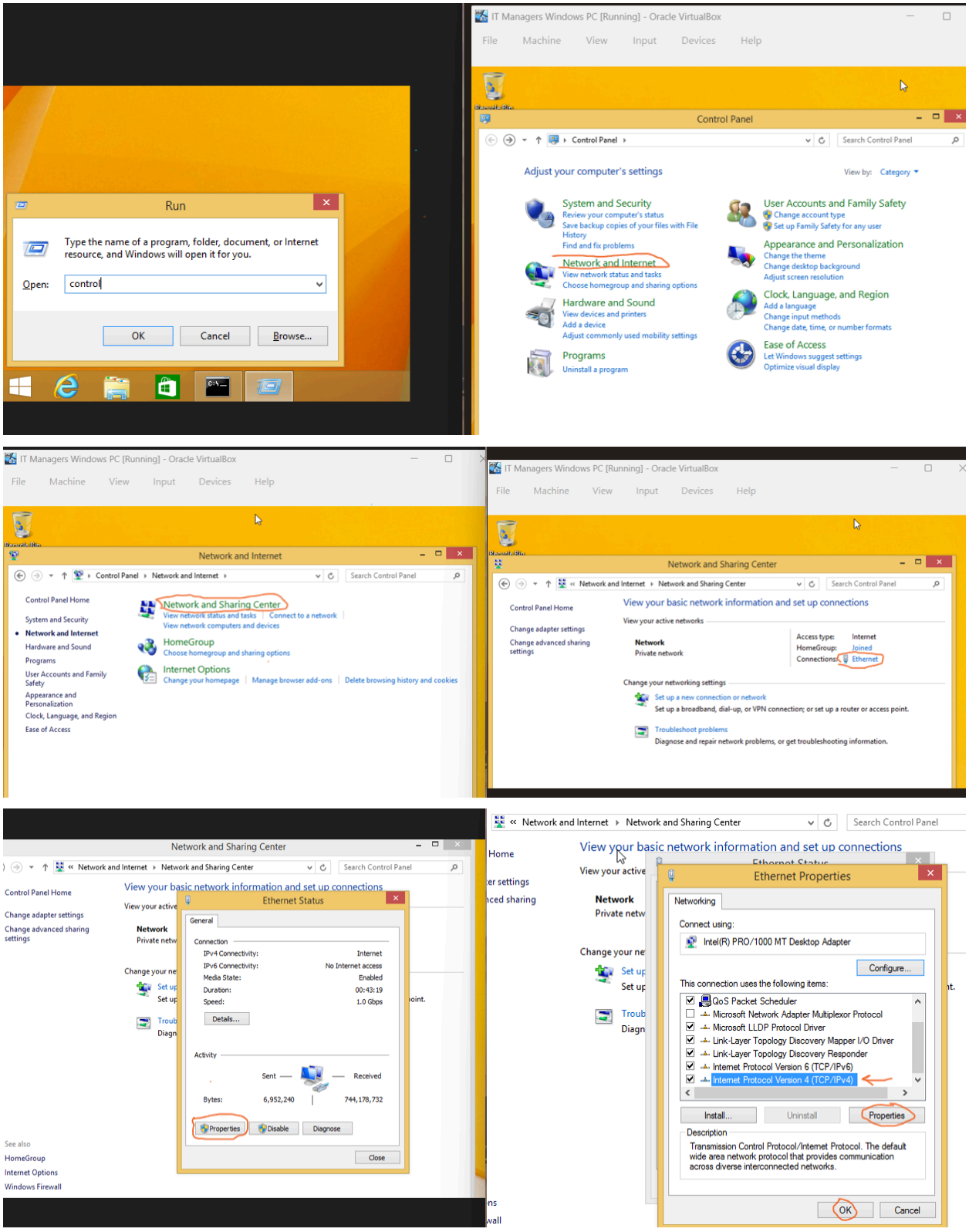
If the **ping fails**, verify that both devices are on the same **NAT network** in VirtualBox and that **Windows Firewall** isn't blocking **ICMP** (ping) requests.



STEP 5→Configure the Network Settings on the IT Managers PC

To allow the IT manager PC to communicate with the Domain Controller (Server), I need to configure its network and DNS settings bellow;

- Press **'Win + R'**, type '`control`', and press **'Ok'** to open the 'Control Panel'.
- Navigate to **'Network and Internet'** → **'Network and Sharing Center'**.
- Click on **'Ethernet'** (My active network connection).
- In the Ethernet Status window, click **'Properties'.**
- Scroll down and select **'Internet Protocol Version 4 (TCP/IPv4)'** → click **'Properties'**.



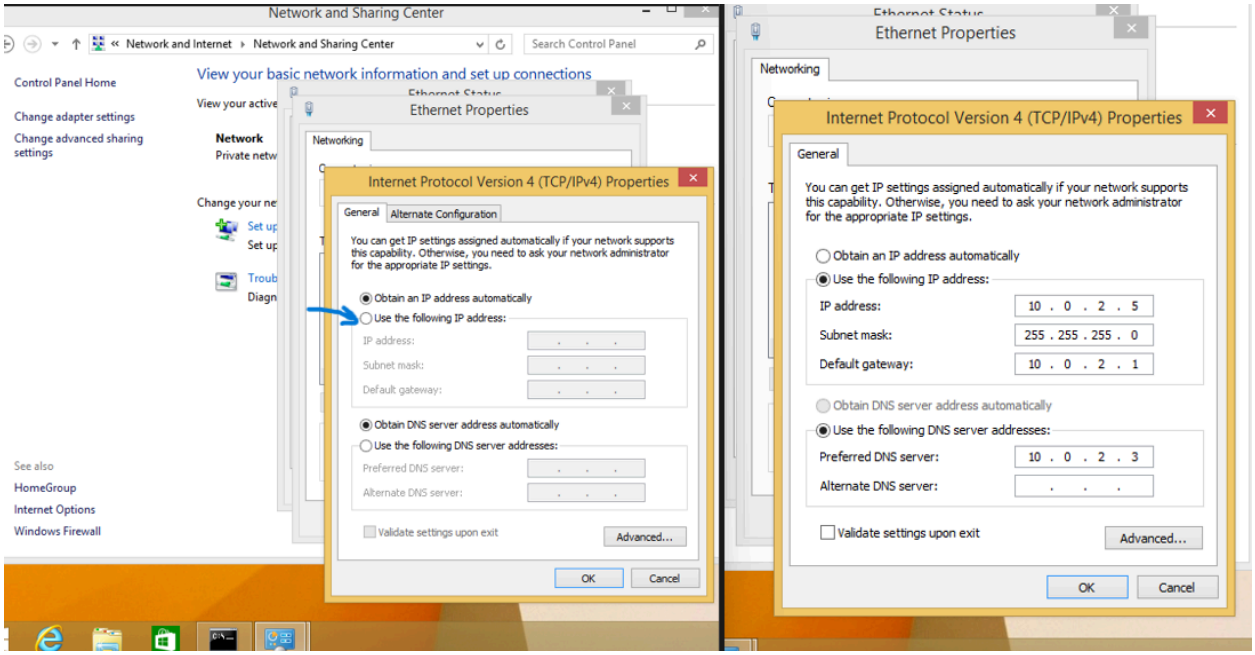
Configure the IP Settings:

- Choose '**Use the following IP address'** (Static configuration).
- Enter the following values (based on your network setup):
    - **IP address**: the same as the IT Manager's IP from your earlier `ipconfig` test.
    - **Subnet mask:** as displayed in the same output.
    - **Default gateway:** the network's gateway (often your VirtualBox NAT gateway).

Set the DNS Server:

- Under '**Use the following DNS server addresses**', enter the server's IP address **`10.0.2.3`.** Click **'Ok'** to apply the changes.

Using a **static IP** ensures consistent connectivity to the domain controller, which is recommended for lab environments.

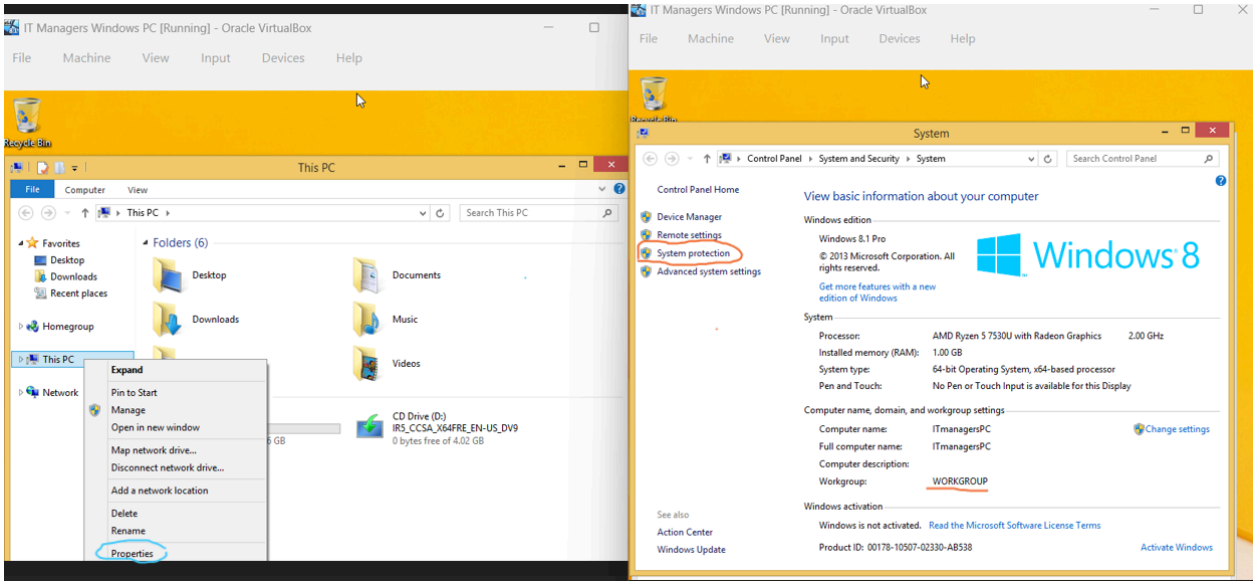


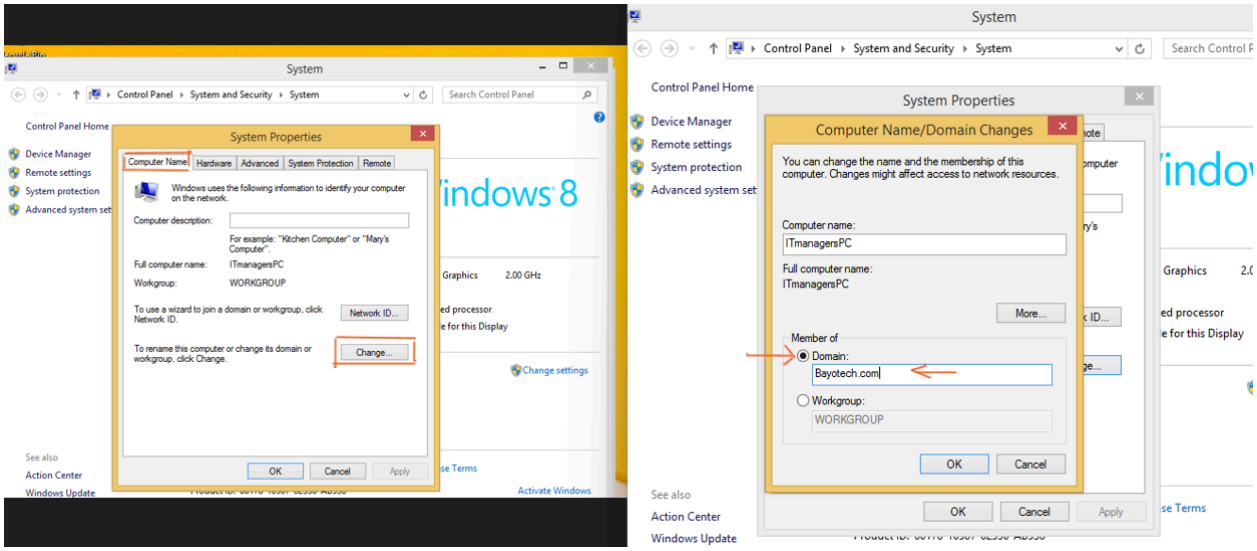
STEP 6→ Join the IT Managers PC to the Domain

Now that the network and DNS settings are configured, the next step is to join the IT Managers PC to the **Bayotech.com** domain below;

- I'll open **File Explorer** on the **IT Managers PC** → Right-click on **'This PC'** → select **'Properties'.**
- In the **'System'** window, I'll click on **'System Protection'** in the left panel.

- In the System Properties dialog box, navigate to the '**Computer Name**' tab.
- I'll click on **'Change'** in front of "**To rename this computer or change its domain or workgroup, click Change**".



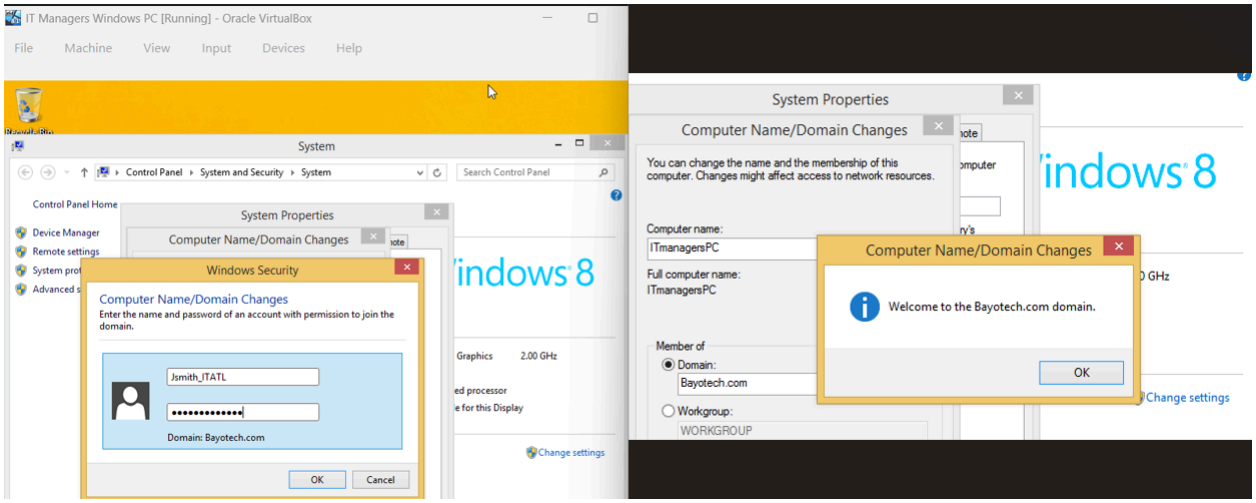


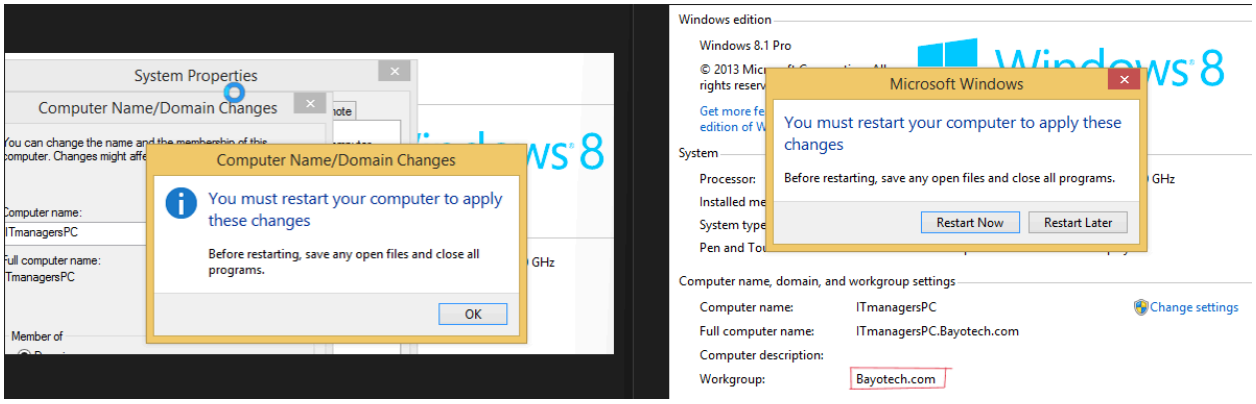
Join the Domain:

- In the **Computer Name/Domain Changes** window:
  - Under '**Member of**', select '**Domain**'.
  - I'll enter the domain name: Bayotech.com → Click **'Ok'**
- When prompted with Windows Security, I entered the credentials of the user I created in Active Directory:

- Username: **Jsmith_ITATL**
- Password: (the password I configured earlier)

Upon successful configuration , a message appears: **Welcome to the Bayotech.com domain**
Click OK, and I was prompted to restart the PC to apply the domain changes.





After Restart:
I Log in using the domain credentials: **BAYOTECH\Jsmith_ITATL**
This confirms that the device has successfully joined the **Bayotech.com** domain and is now under centralized management via **Active Directory**

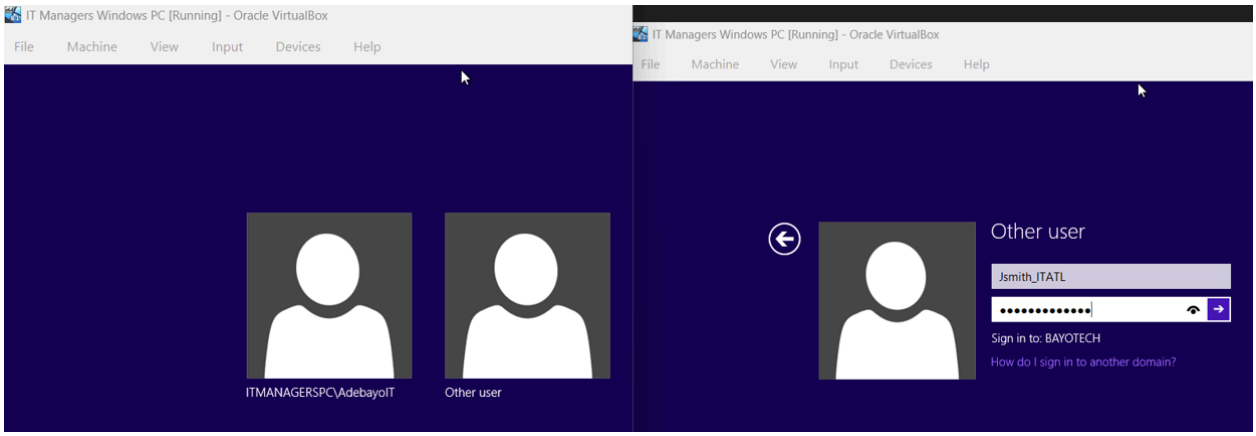
Using the Assigned PC

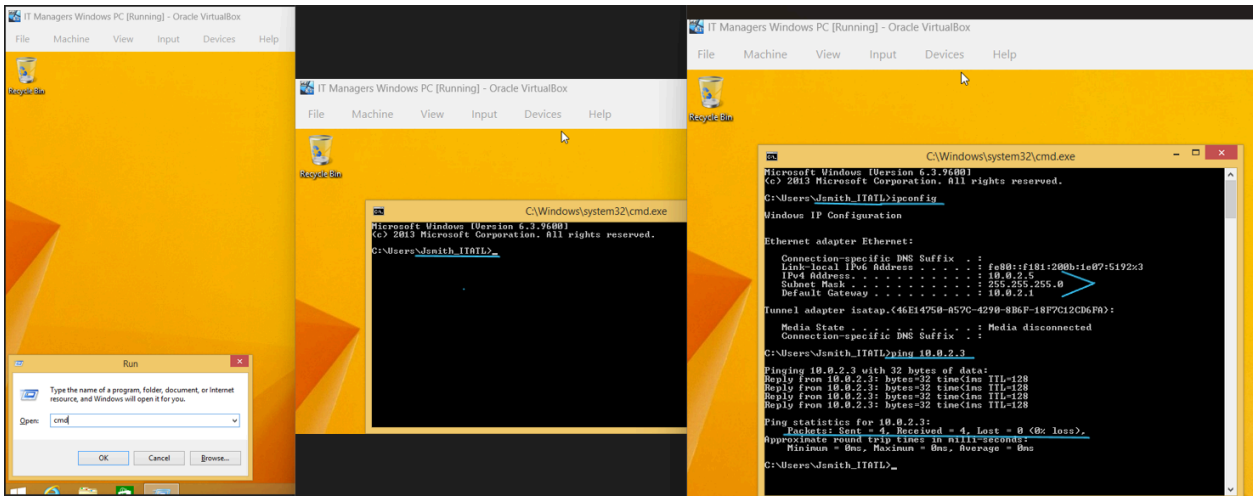
- Upon restarting the IT Managers PC, the system name will appear as **'ITManagersPC\AdebayoIT'**. I Click the back arrow on the login screen and select **'Other User'** to switch accounts.

- When prompted, I enter the credentials for the assigned user to sign in to the Domain **“Bayotech’**,for example, **John Smith** using the format;

  Username:- **Jsmith_ITATL

  **Password:- [xxxxxxxx]
- After successfully logging in as **John Smith,** I open the Command Prompt (**Win + R → type cmd → Enter**).
- I notice the prompt now displays the username logon for **John Smith** as **‘Jsmith_ITATL’**, confirming that I am logged into the domain account.
- I run the command **‘ipconfig’** to verify that the PC is still configured with the correct static IP address assigned earlier.
- Next,I’ll run a **ping test** using the server’s IP address (e.g., **ping 10.0.2.3**) to ensure that communication between the **ITManager PC** and the **server** remains active and stable.



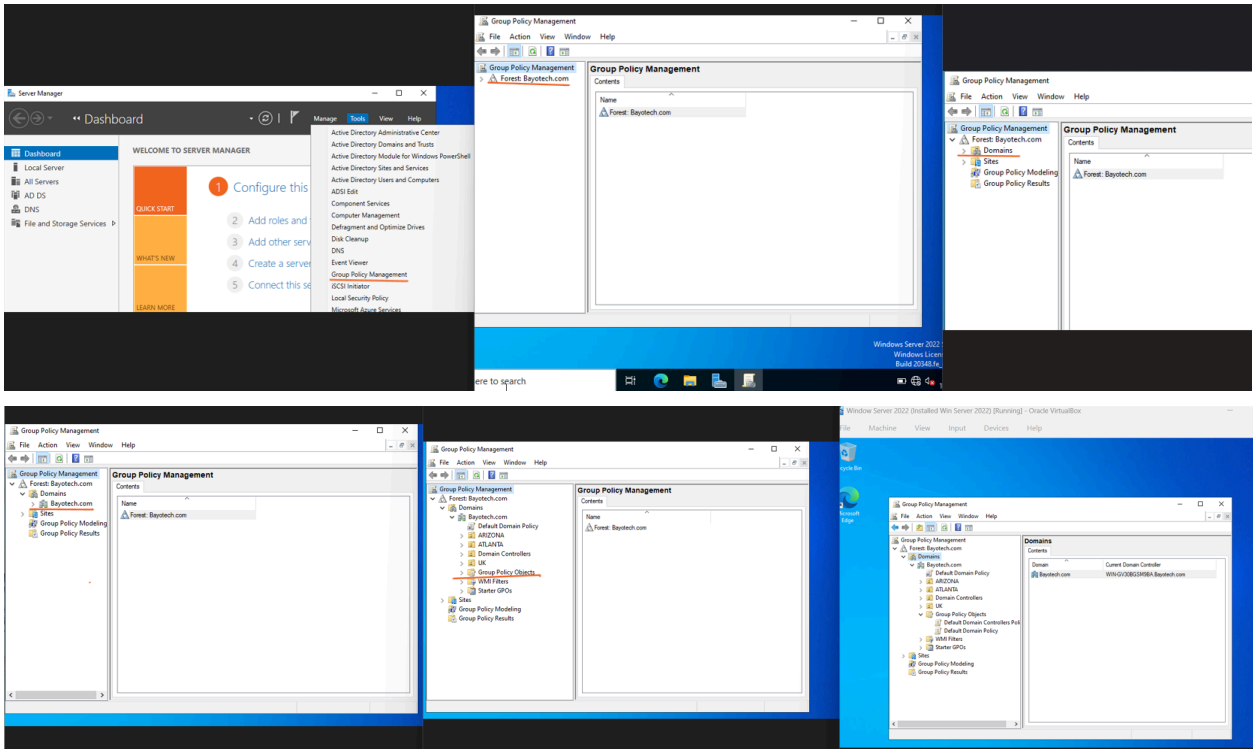


Assigning Group Policies (GPOs) to Users and Computers

After successfully adding users and computers to the Active Directory domain, the next step is to **assign Group Policies (GPOs)**. Group Policies allow administrators to centrally manage user and computer settings such as password requirements, desktop restrictions, software installation permissions and more.

I can now see the **Group Policy Management Console (GPMC)** displaying the forest that was created **"Bayotech.com."**

To apply a policy to the domain; I'll Expand the **Forest: Bayotech.com** —> Expand **Domains** —>Expand the created domain **"Bayotech.com"** —>(Within this structure, you'll find several components, including:Default Domain Policy ,Domain Controllers ,Organizational Units (OUs) ,Group Policy Objects (GPOs) ,WMI Filters ,Starter GPOs))



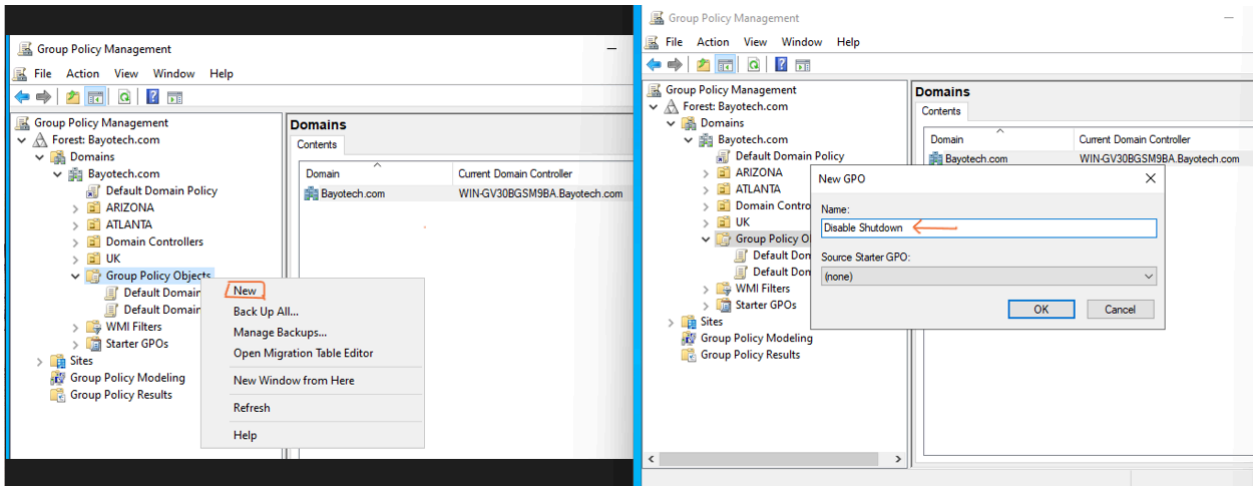
Steps to Assign a Group Policy (GPO)

Step 1→ To Create a New Policy

- I'll right-click on '**Group Policy Objects**'.

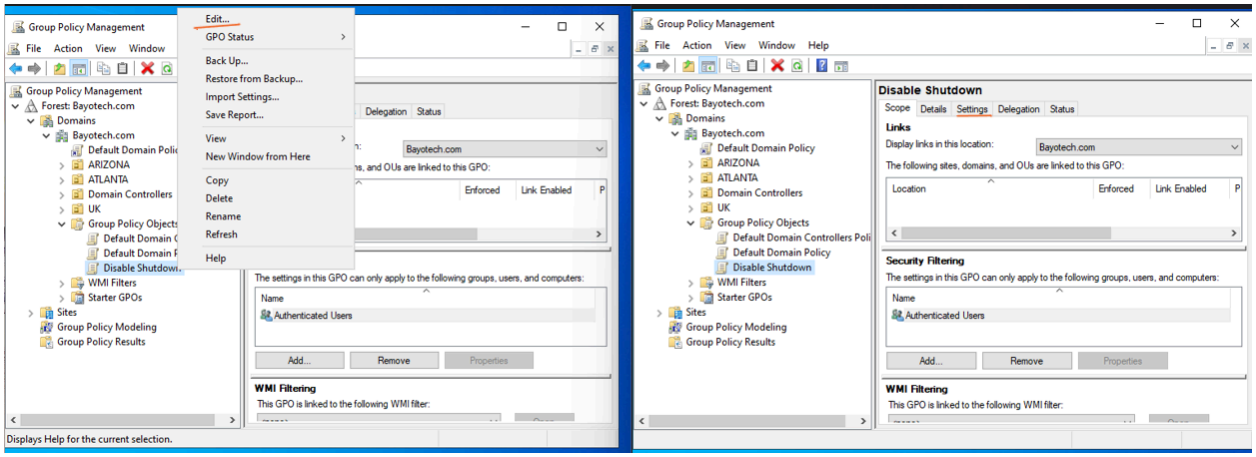
- Click **‘New’**→ Enter a name for the policy for example,**‘Disable Shutdown’**--> Click **‘Ok’**.

NOTE→ The policy has only been created ,it has not yet been applied. At this stage, the GPO is empty, meaning no specific settings or rules (such as disabling shutdown) have been configured within it yet.



Step 2→ Editing the Newly Created GPO

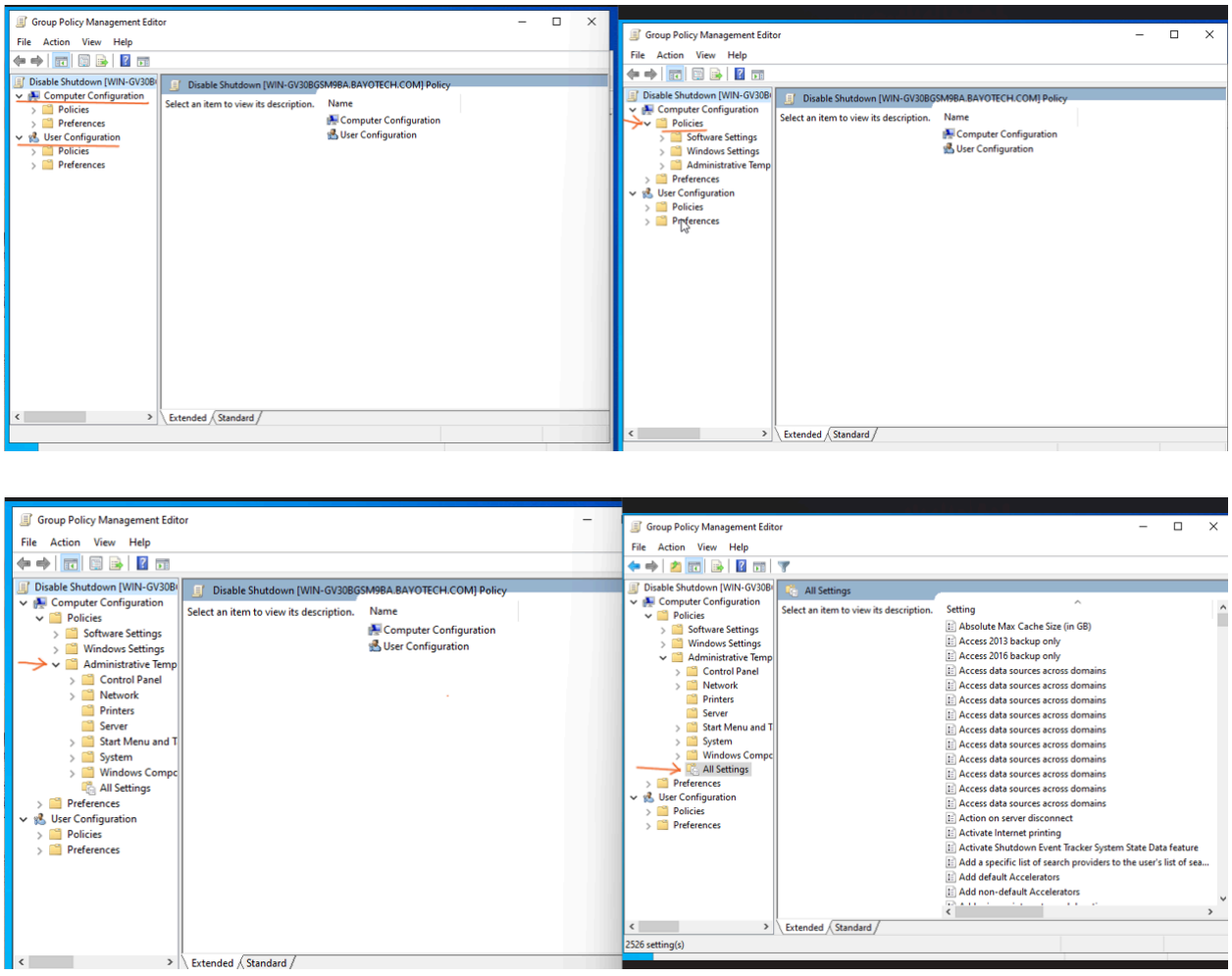
- I’ll right-click on the newly created GPO **‘Disable shutdown’** and select **‘Edit’.** (This opens the Group Policy Management Editor, allowing me to configure and add specific settings that define how the policy functions.)
- The editor displays two main sections: **‘Computer Configuration’** and **‘User Configuration’**.
    - To ensure the policy applies correctly, settings can be configured under both **Computer Configuration** (for all machines) and **User Configuration** (for individual users).

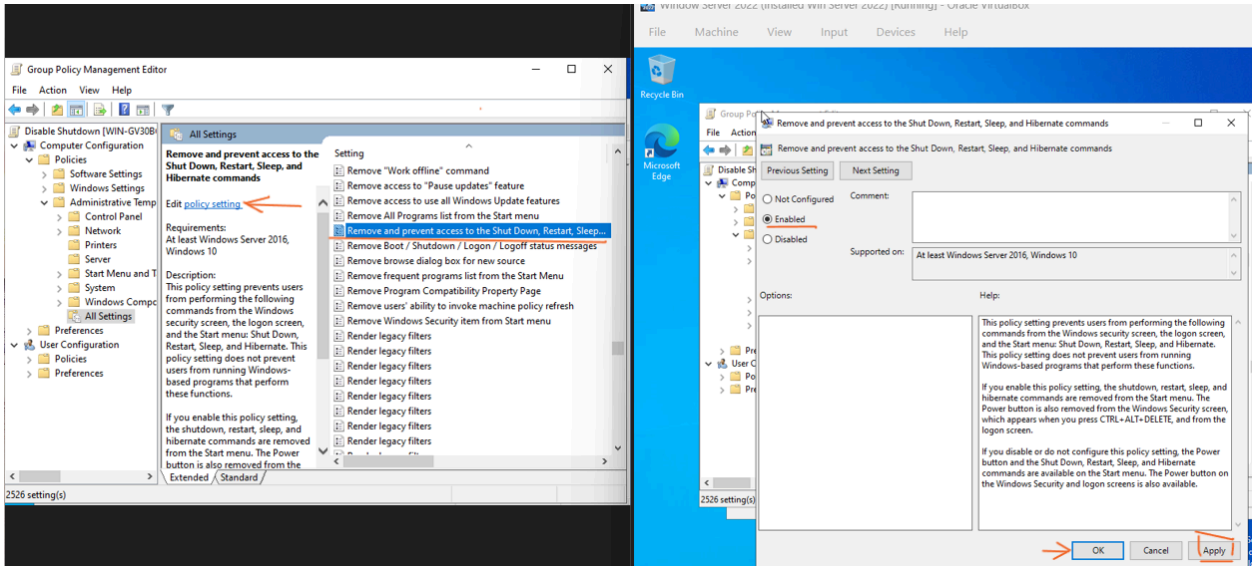


Step 3→ Configuring the “Disable Shutdown” Policy

Start with the **Computer Configuration** section:

- Expand **Policies → Administrative Templates → All Settings**.(This displays a list of available settings, Click the **Settings** column header to sort them alphabetically for easier navigation).
- Locate and double-click **“Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands.”** (This is the policy I would be implementing).
- In the **Policy Settings** window, select **Enabled**. Click **Apply**, then **OK** to save the configuration.

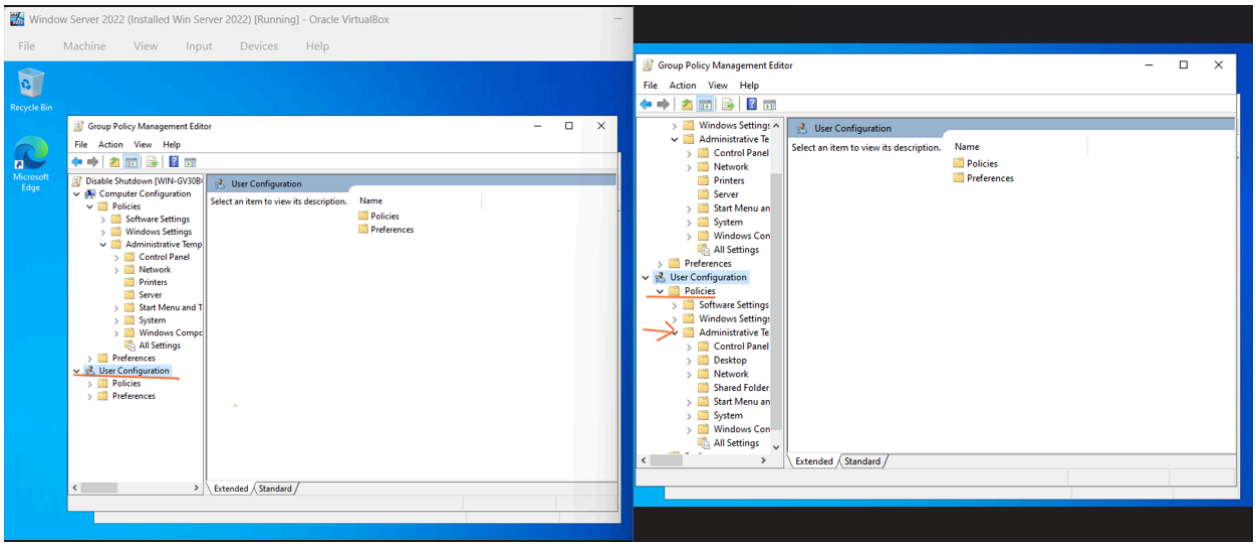


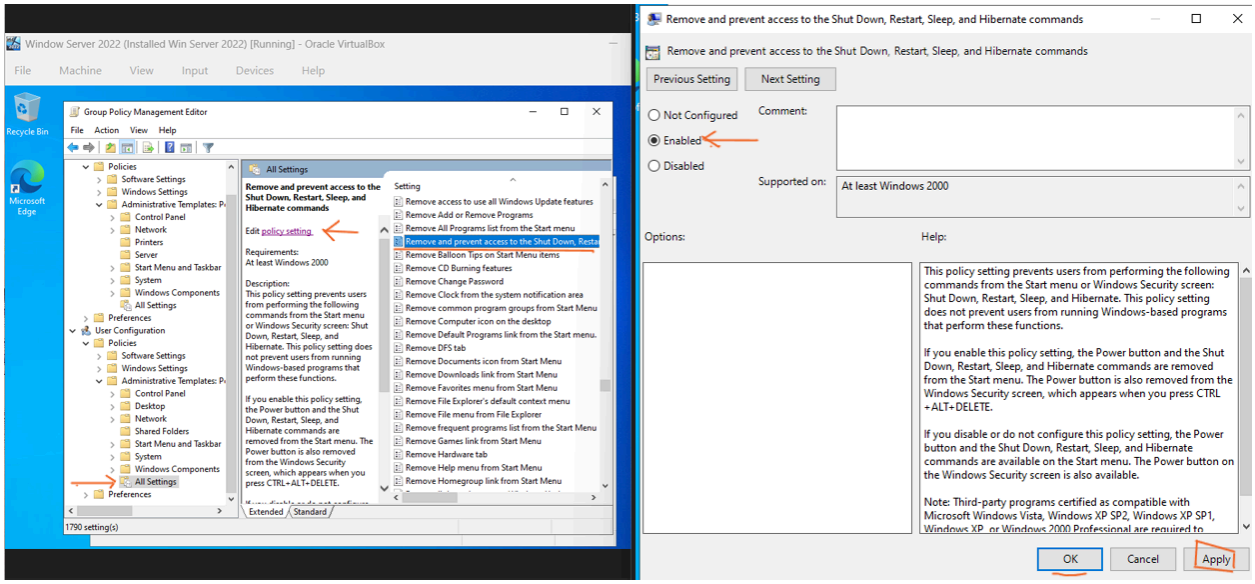


Next→ Applying the Policy to User Configuration

Repeat the same process under User Configuration:

- Expand '**User Configuration' → 'Administrative Templates' → 'All Settings'**.
- Locate and select the same policy (**"Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands"**) → click to open the '**Policy Settings window'**.
- Select **'Enabled'**, then click **'Apply'** and **'Ok'** to save the changes.



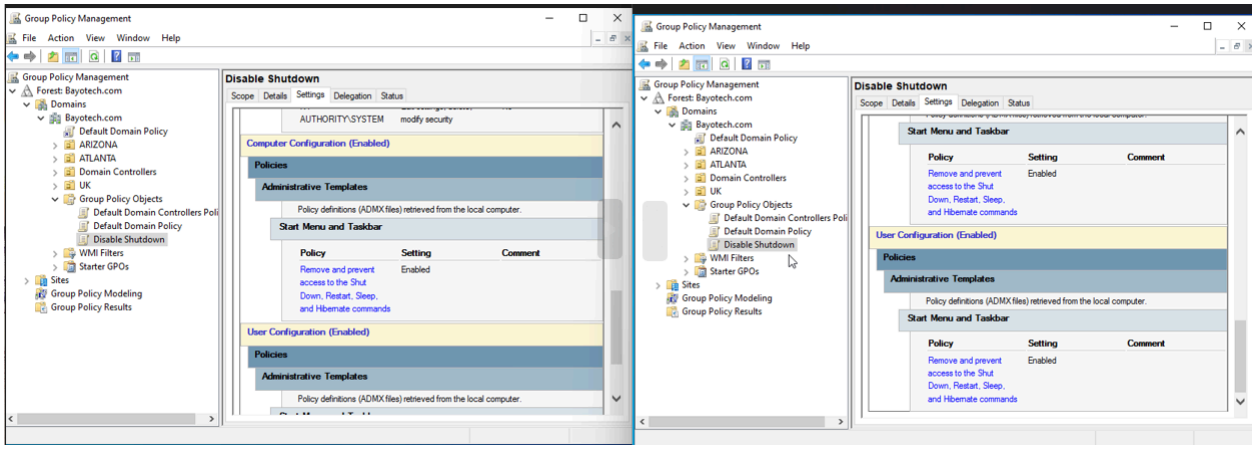


Note: The policy has now been successfully enabled under both **Computer Configuration** and **User Configuration**, ensuring that shutdown and restart options are restricted for all users and systems within the domain.

Verifying the Policy Settings

To confirm that the policy has been successfully configured:

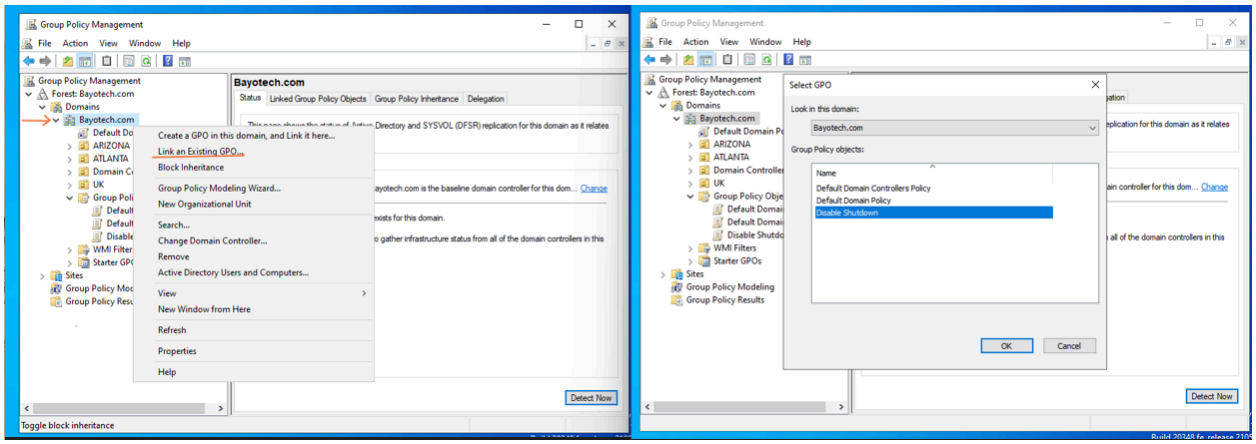
- Click on the **created GPO**.
- Navigate to the **Scope** tab, then select **Settings**.(If an error message appears, simply ignore it and reopen the **Settings** tab.)
- Scroll down to locate '**Computer Configuration**' see the newly applied policy listed there. Continue scrolling to find **User Configuration**, where the same policy should also appear.



Step 4→ Linking the GPO to the Domain

Right-click on **“Bayotech.com”** → select **“Link an Existing GPO”**
This option allows me to link the policy I created to the domain. (Note: In Active Directory, multiple domains can exist, so be sure you’re selecting the correct one.)

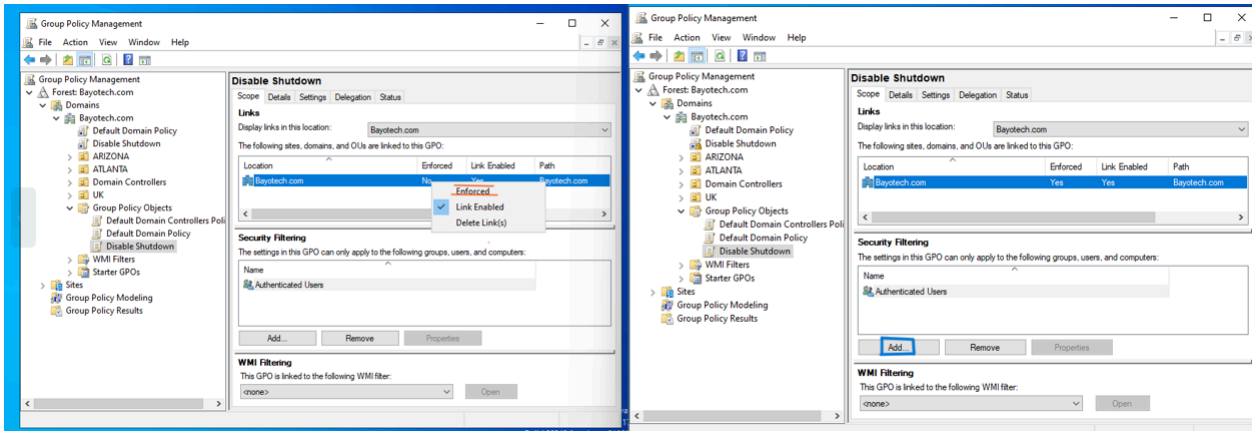
A list of all available GPOs will appear, select the policy you created (in this case, **“Disable Shutdown”**) → click **OK** to link it.



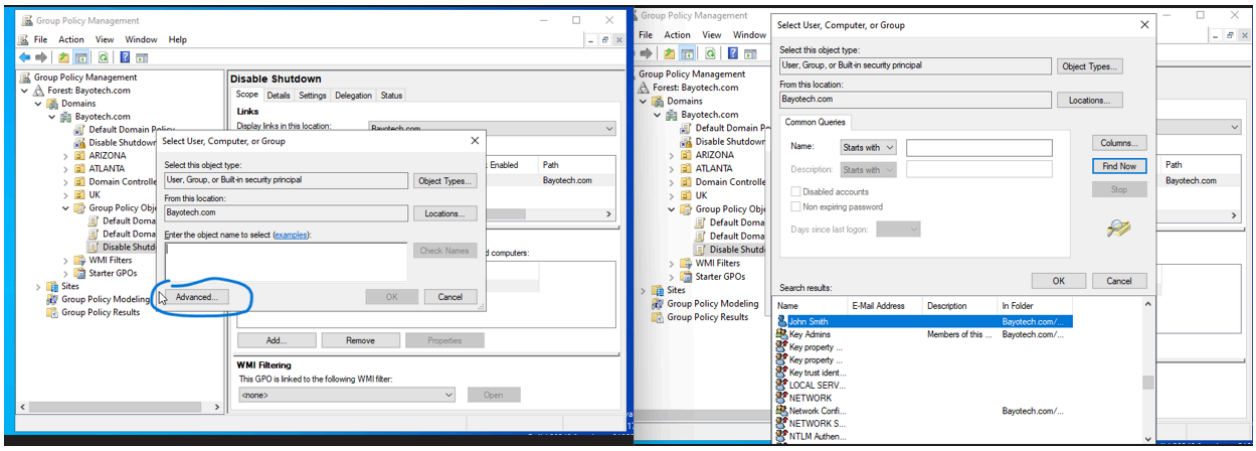
Enforcing and Assigning the GPO to a User

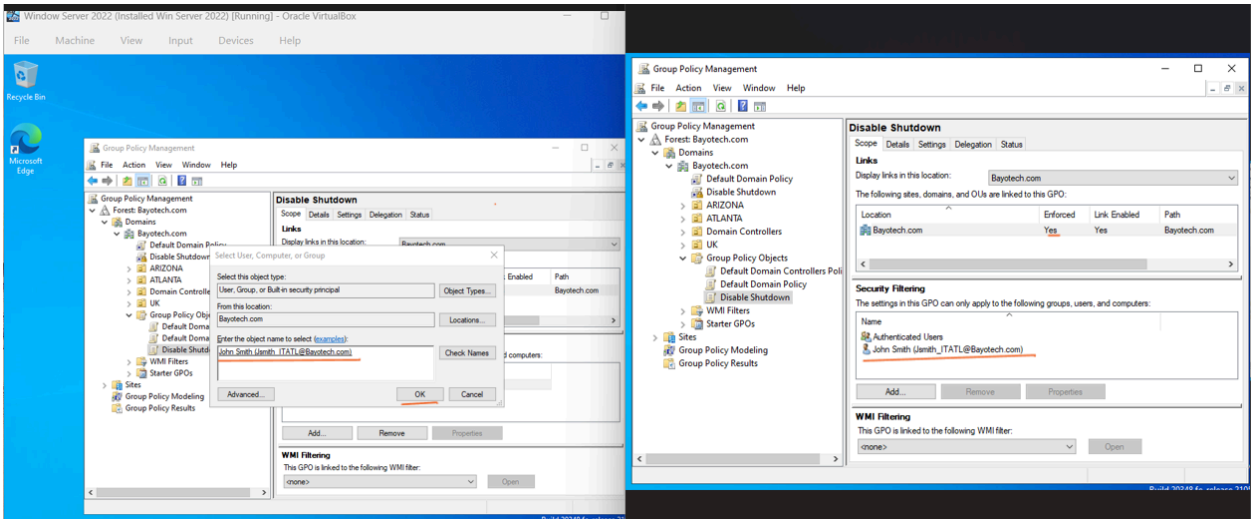
Click on the **created policy** to open its settings, then select the **“Scope”** tab.

- Under **“Links”**, navigate to the domain ‘Bayotech.com’. In the **“Enforced”** column, right click on it to change the value from **“No”** to **“Yes.”** by clicking **‘Enforced’**
- Next, under **‘Security Filtering’** click **“Add.”**



- In the pop-up window, select **'Advanced'**→ click **'Find Now'** to display all available users.
- Locate and select the user you want the policy applied to in this case, **"John Smith."** and Click **OK** to confirm.

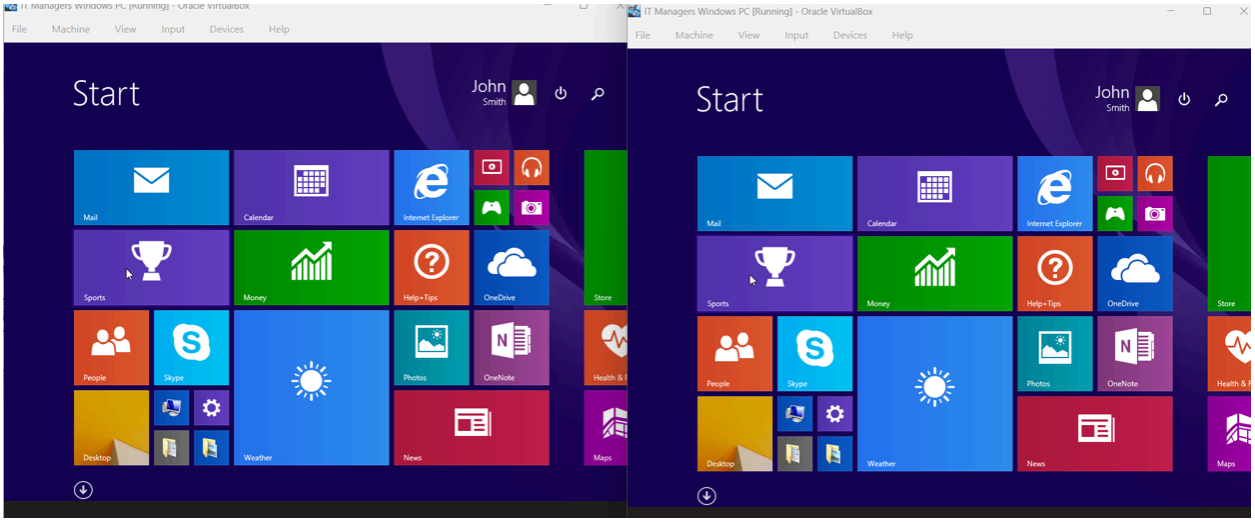




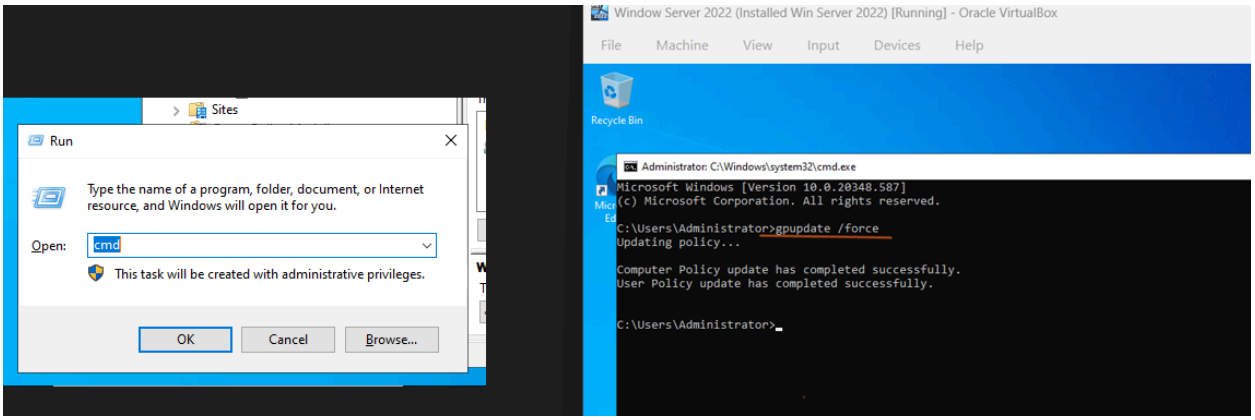
NOTE → The **"Disable Shutdown"** policy is now enforced and specifically applied to the user **John Smith** within the domain.

Applying and Verifying the Group Policy

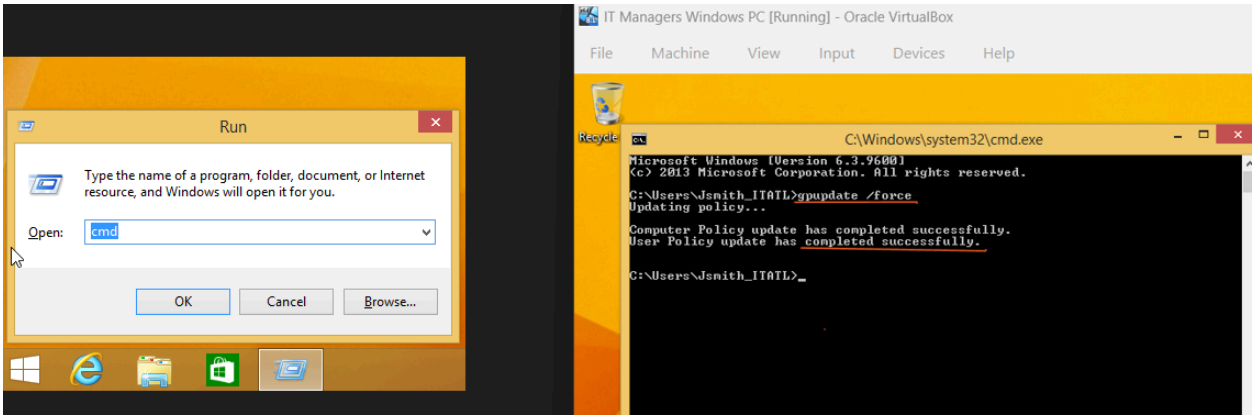
When I log into **John Smith's computer**, I notice that the PC can still be shut down. This means the new Group Policy hasn't been applied yet.



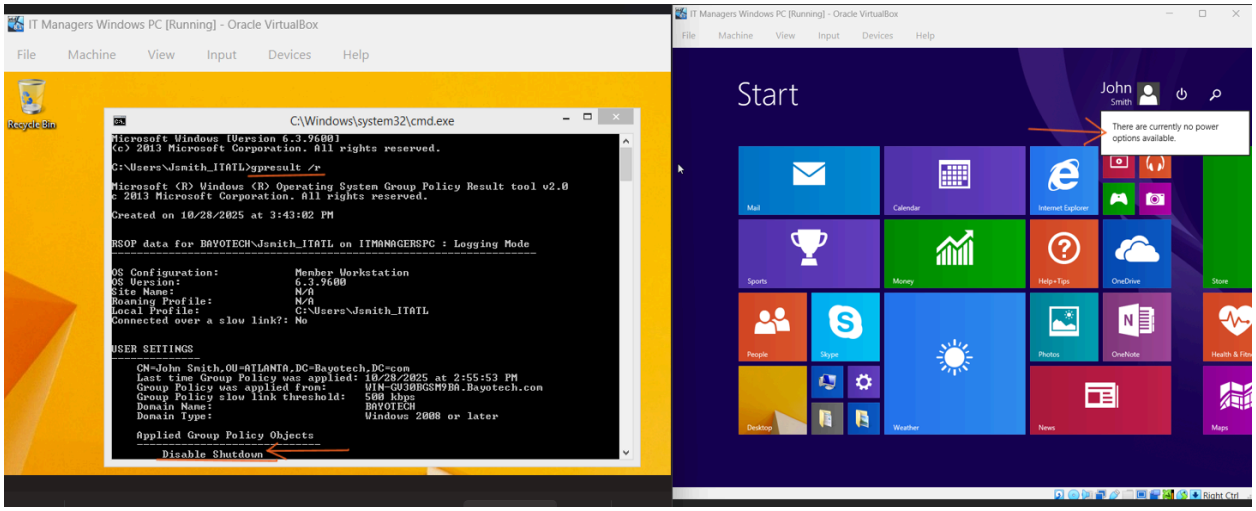
To enforce the policy: I went back to the **server PC** → press **Win + R** → type '`cmd`' →enter the command '`gpupdate /force`' to refresh and apply the latest Group Policy settings on the server.



I'll repeat the same '`gpupdate /force`' command on **John Smith's PC** to ensure the updated policy is synchronized.



After the update completes, I return to **John Smith's PC** and verify that the **shutdown options are now disabled**, confirming that the policy has been successfully implemented.



Summary

This lab demonstrates how Active Directory (AD) and Group Policy Objects (GPOs) play a critical role in an organization's cybersecurity posture. By centralizing user and device management, AD allows administrators to enforce least-privilege access, standardize security configurations, and reduce the attack surface across the enterprise.

Implementing the "Disable Shutdown" policy illustrates how security controls can be deployed remotely and consistently, preventing unauthorized system changes and improving operational resilience.

This hands-on exercise reinforces key cybersecurity principles ; access control, configuration management, and policy enforcement . Showing how proper IAM practices form the foundation of a secure, compliant network environment.