

Active Directory Deployment & Hardening – Secure domain controller with baseline GPOs

Deployment of a Windows Server Domain Controller (Active Directory)

Company Name: CyberTech Solutions.

It includes domain setup, client configuration, OU design, group policies, and access control in an enterprise environment.

Company Structure:

CyberTech Solutions an IT services firm with the following structure:

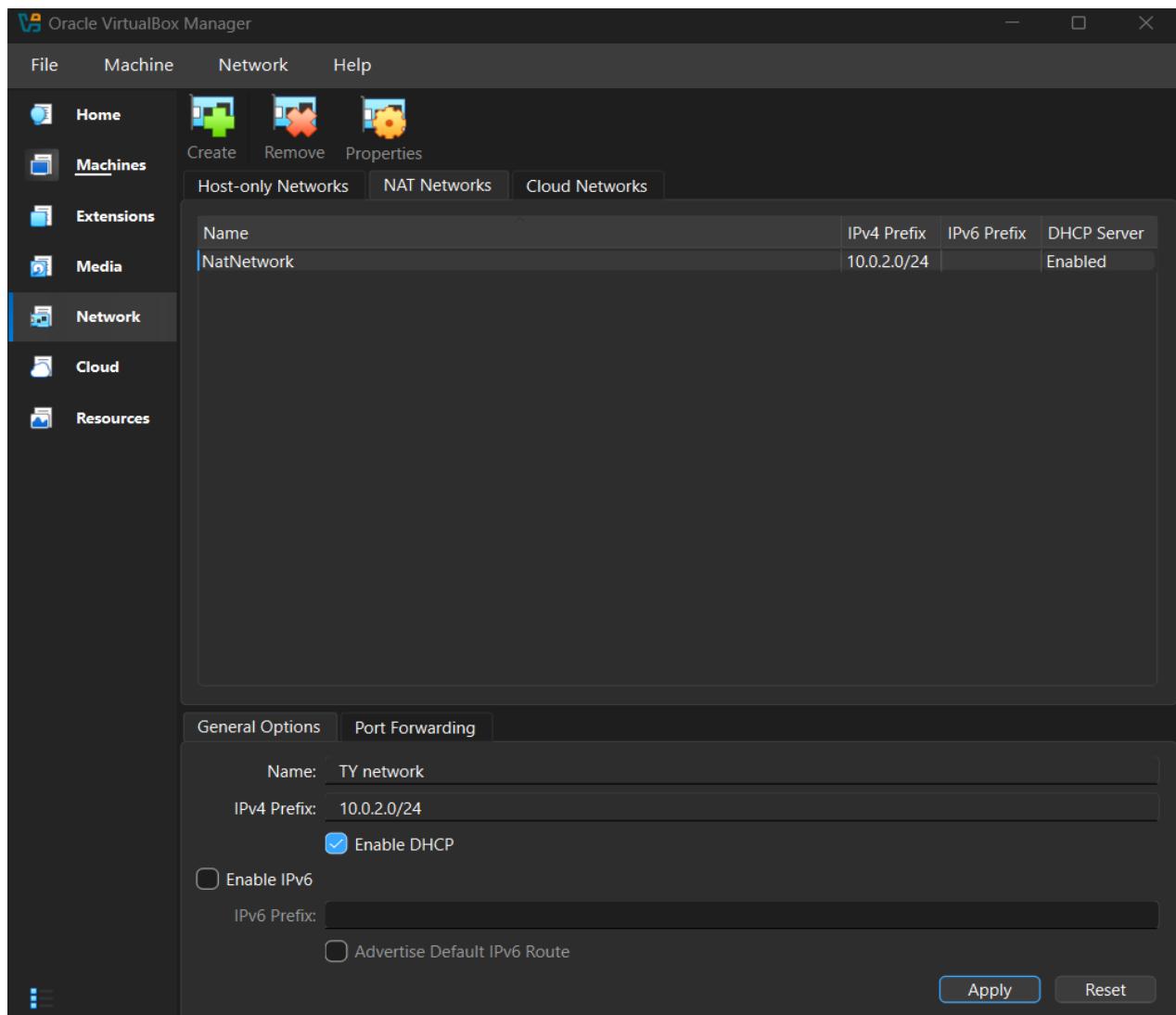
- 1 x Windows Server (AD Domain Controller)
- 1 x Windows 8 A Client PC (IT Department)
- 1 x Windows 8 B Client PC (Sales Departemnt)

Project Objectives:

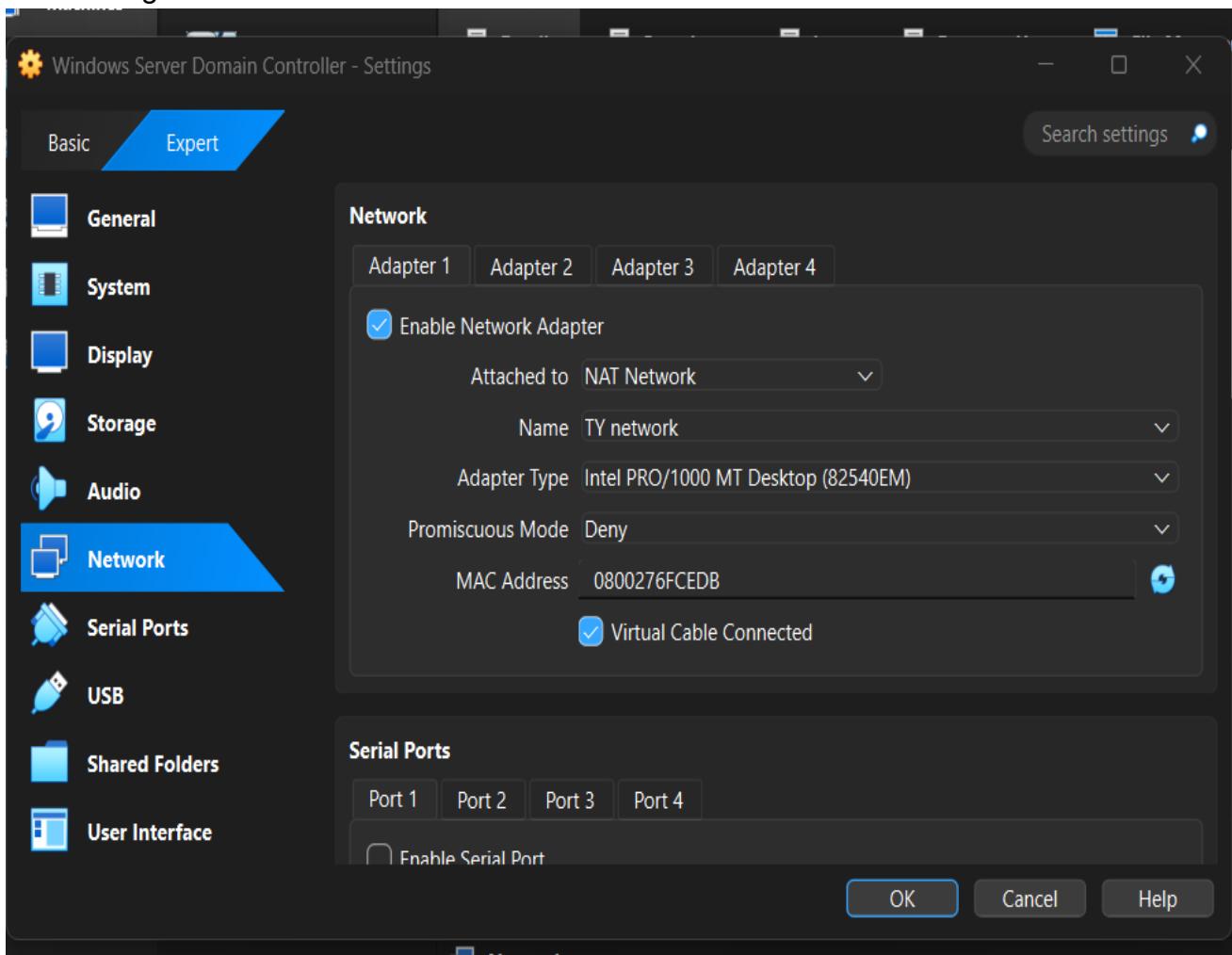
- Configure an AD Domain Controller on Windows Server
- Join client PCs to the domain
- Create Organizational Units (OUs)
- Implement basic Group Policies for access control
- Simulate a centralized IT environment.

See Screenshots below for walkthrough:

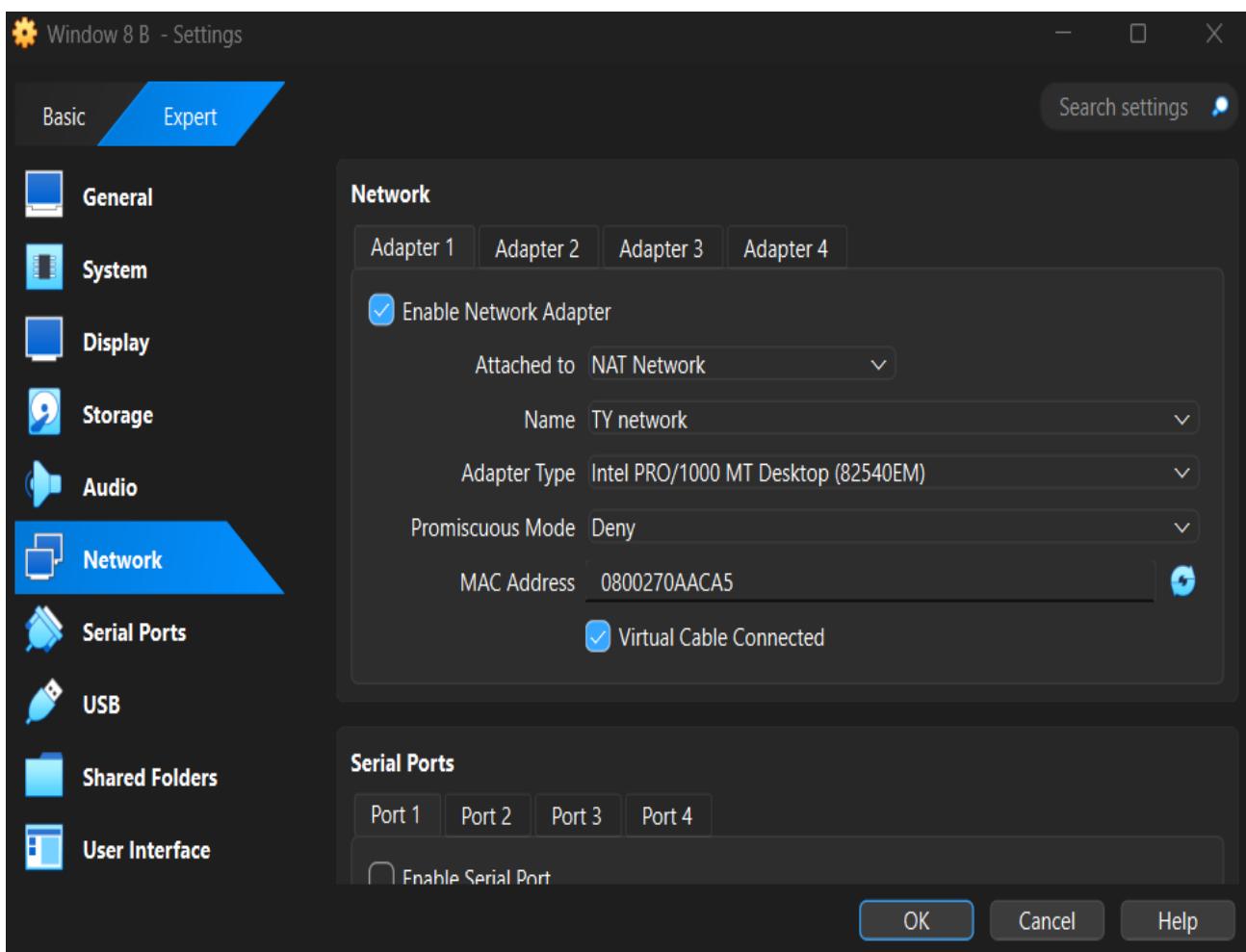
Network creation in VM



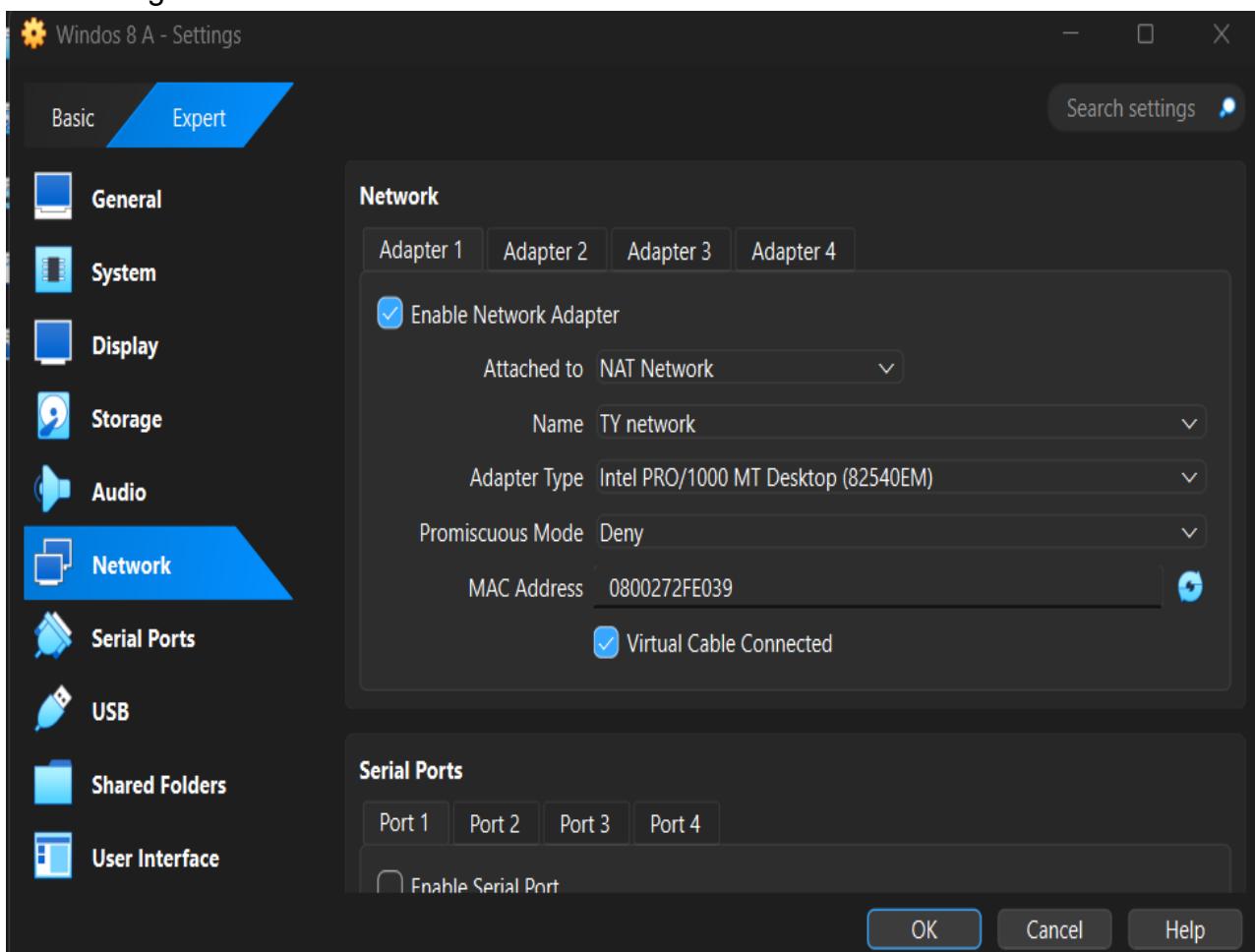
Connecting Network to WIndos Server domain



Connecting Network to windows 8 b network

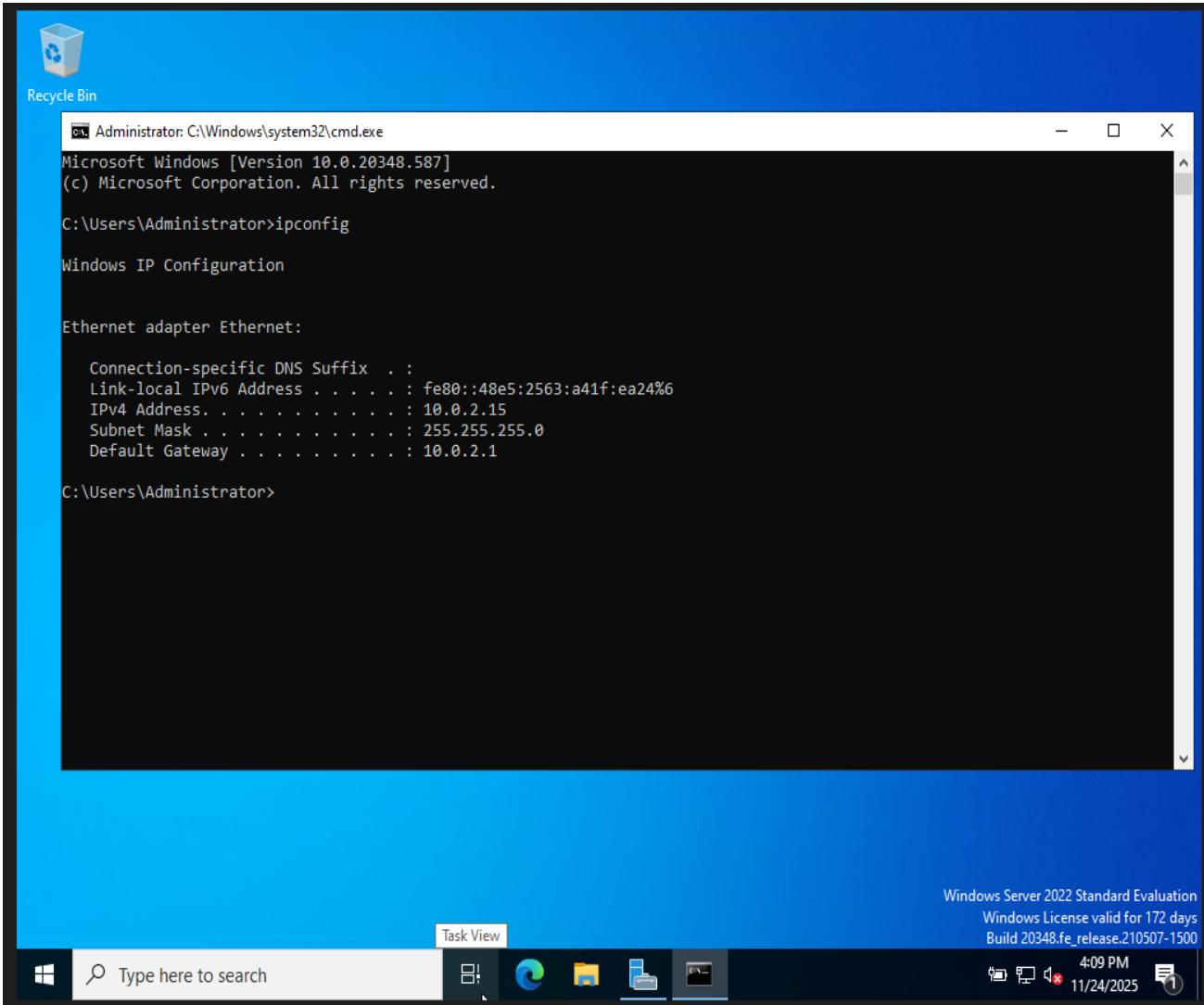


Connecting Network to windows 8 A network

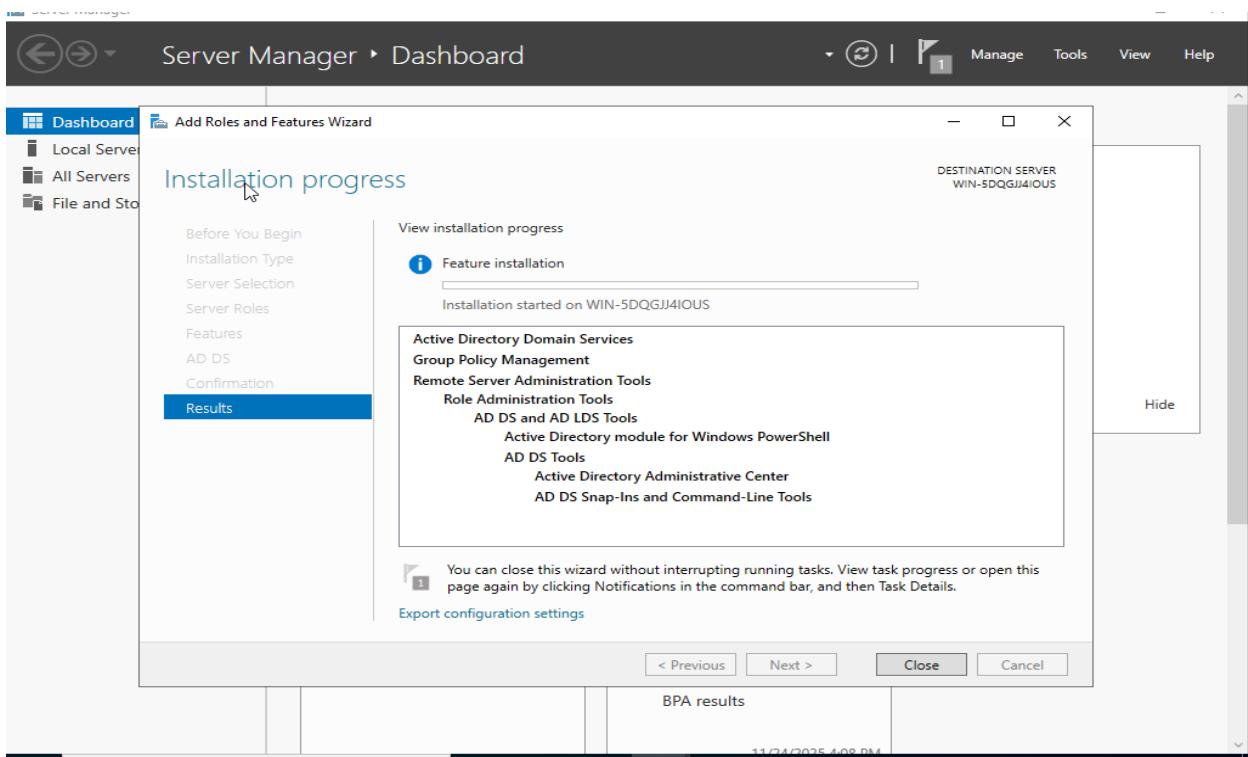


Confirming Server IP – 10.0.2.15

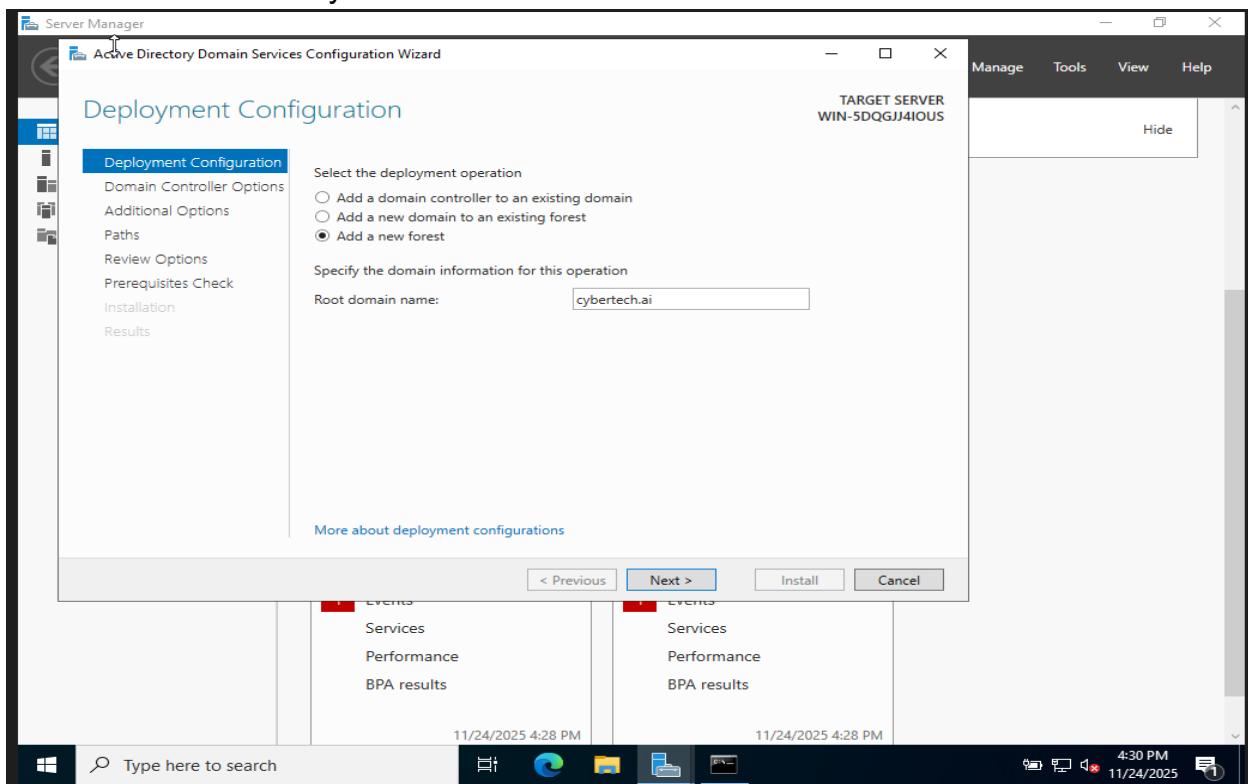
Subnet Mask- 255.255.255.0



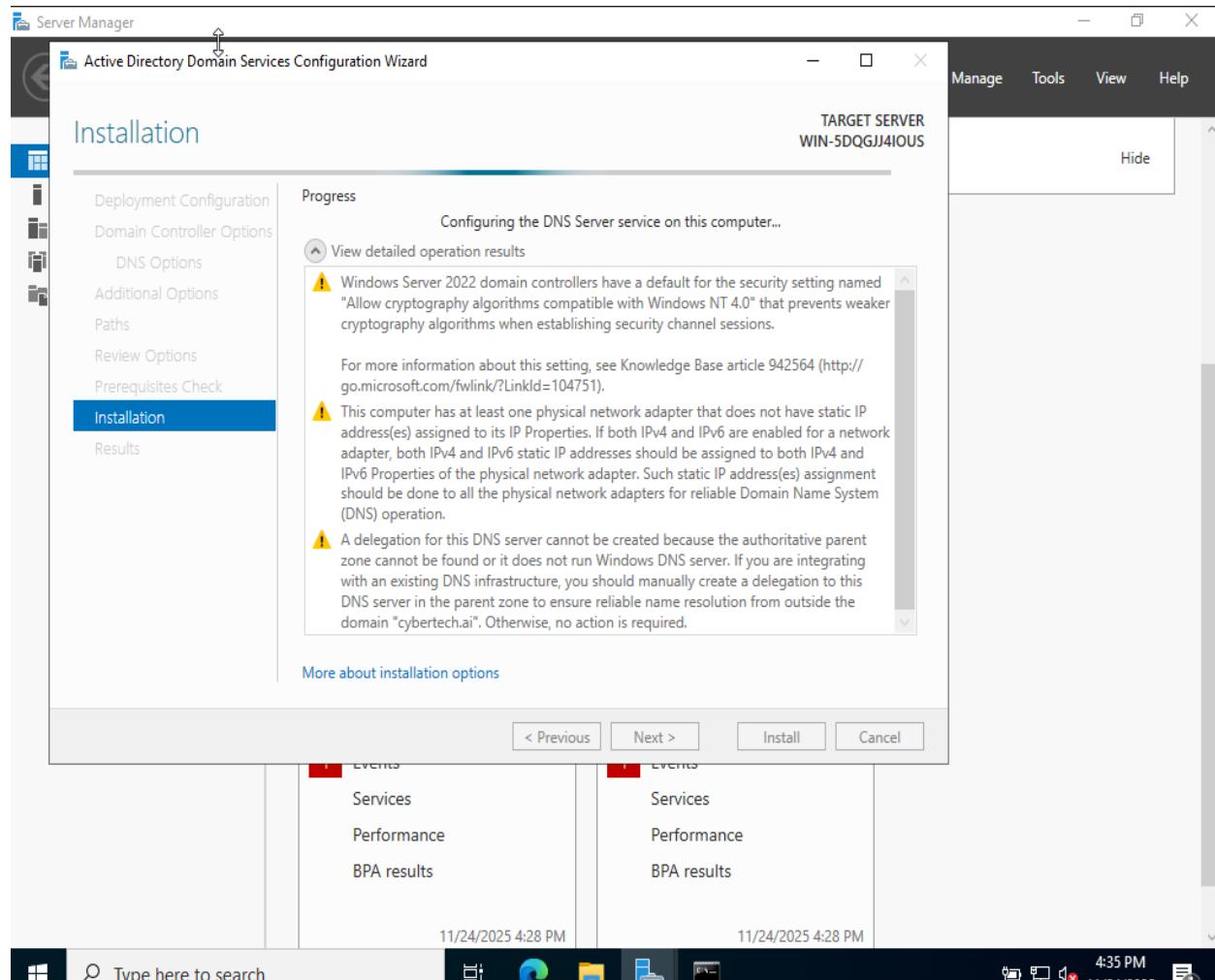
Installation of Active directory



Root domain name – cybertech.ai



DNS installation



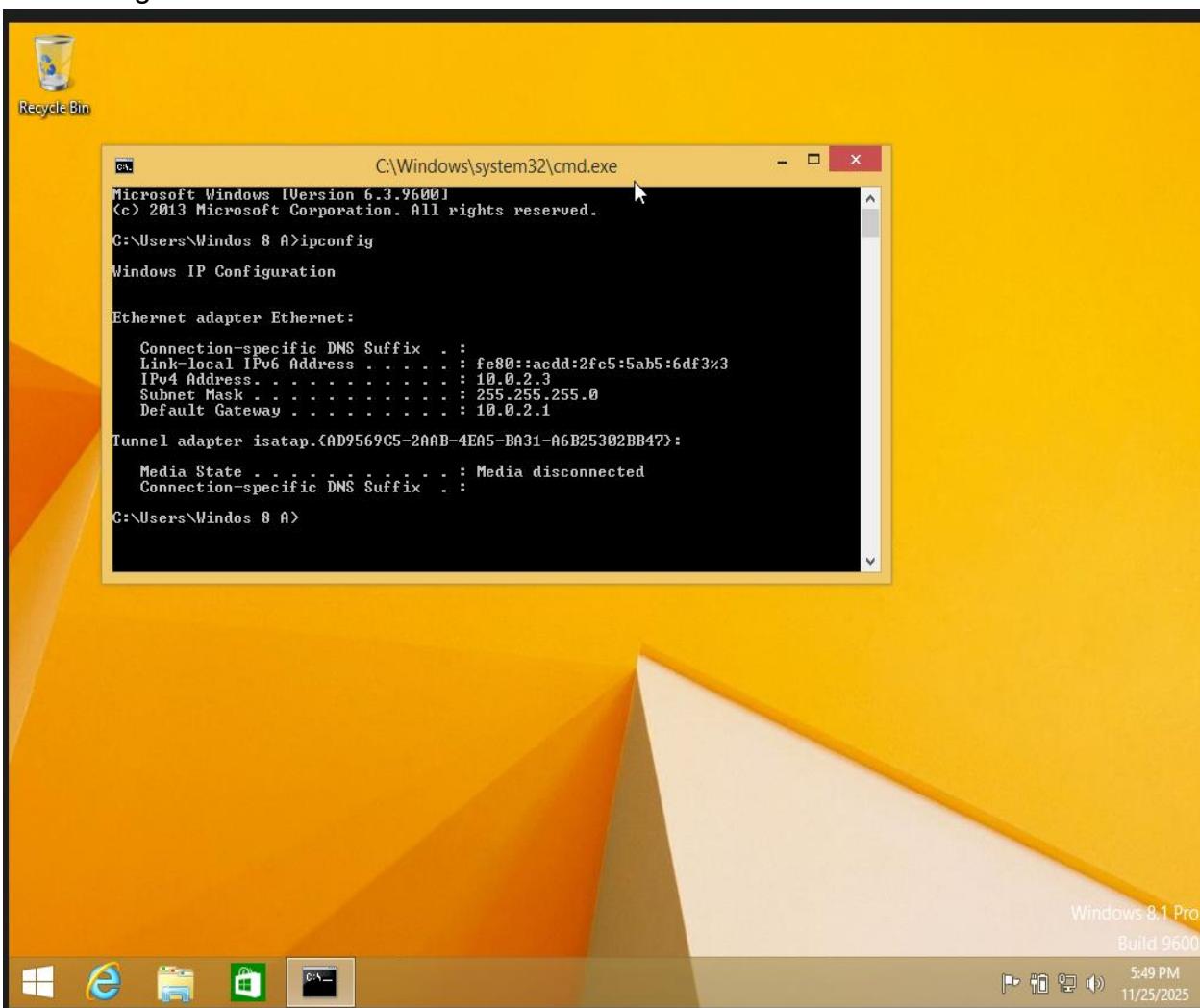
Creating organization unit, groups, users and roles.

The screenshot shows the Windows Server Manager interface. The left navigation pane lists 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage Services'. The main content area is titled 'Active Directory Users and Computers' and displays a tree view of the domain structure under 'cybertech.ai'. The tree includes 'Saved Queries', 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'HR', 'IT department' (which is expanded to show 'Managed Service Account', 'Procurement', 'Sales', and 'Users'), and 'System Administrators'. To the right of the tree is a table showing user and group details:

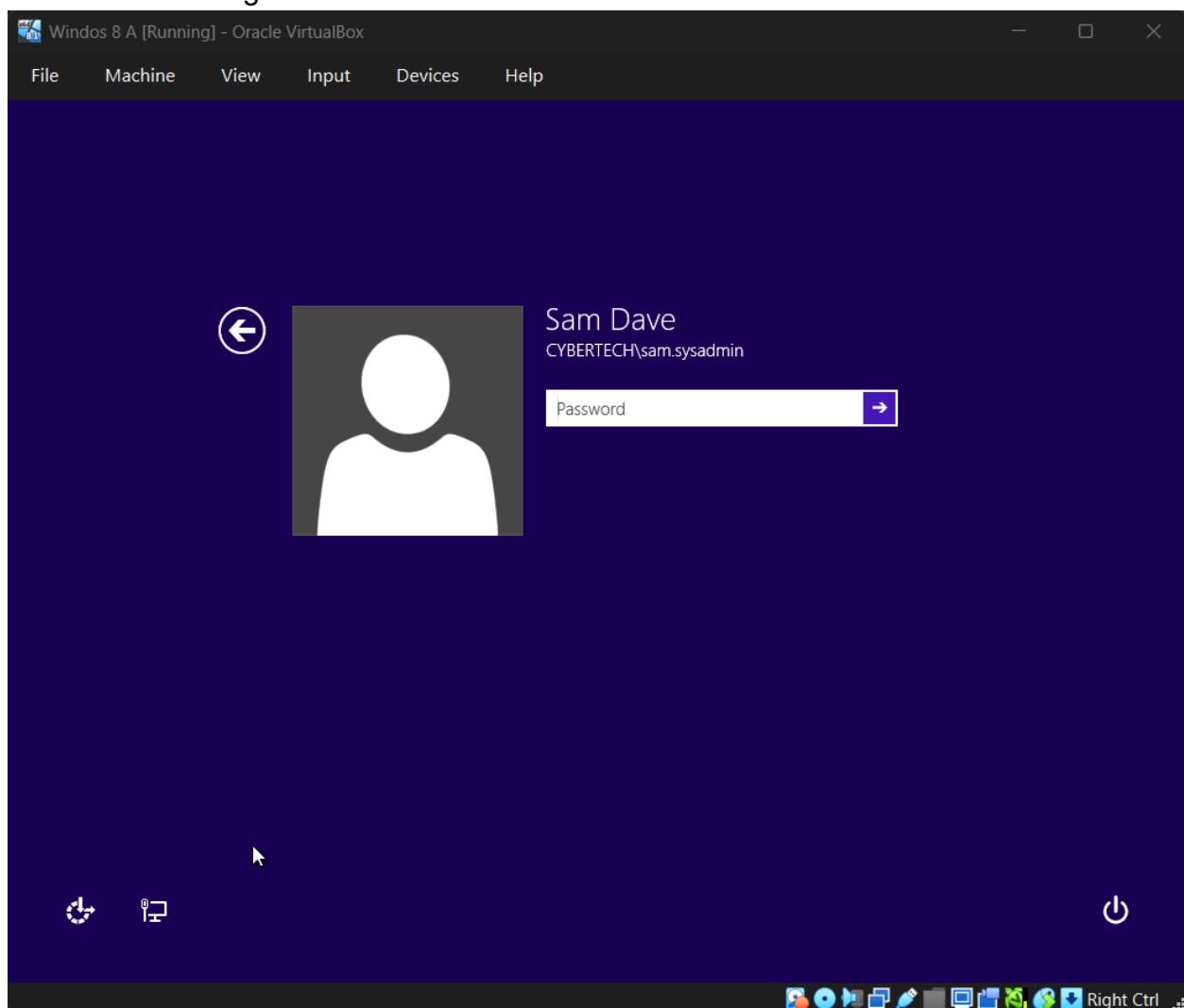
Name	Type	Description
Jay Thomson	User	
Programmer	Security Group...	
Sam Dave	User	
System Admin...	Security Group...	

At the bottom, there are two status cards: 'File and Storage Services' (green) and 'Local Server' (red). The 'Local Server' card shows 1 item, Manageability (green), and 2 Events (red). The taskbar at the bottom includes the Start button, a search bar, and system icons.

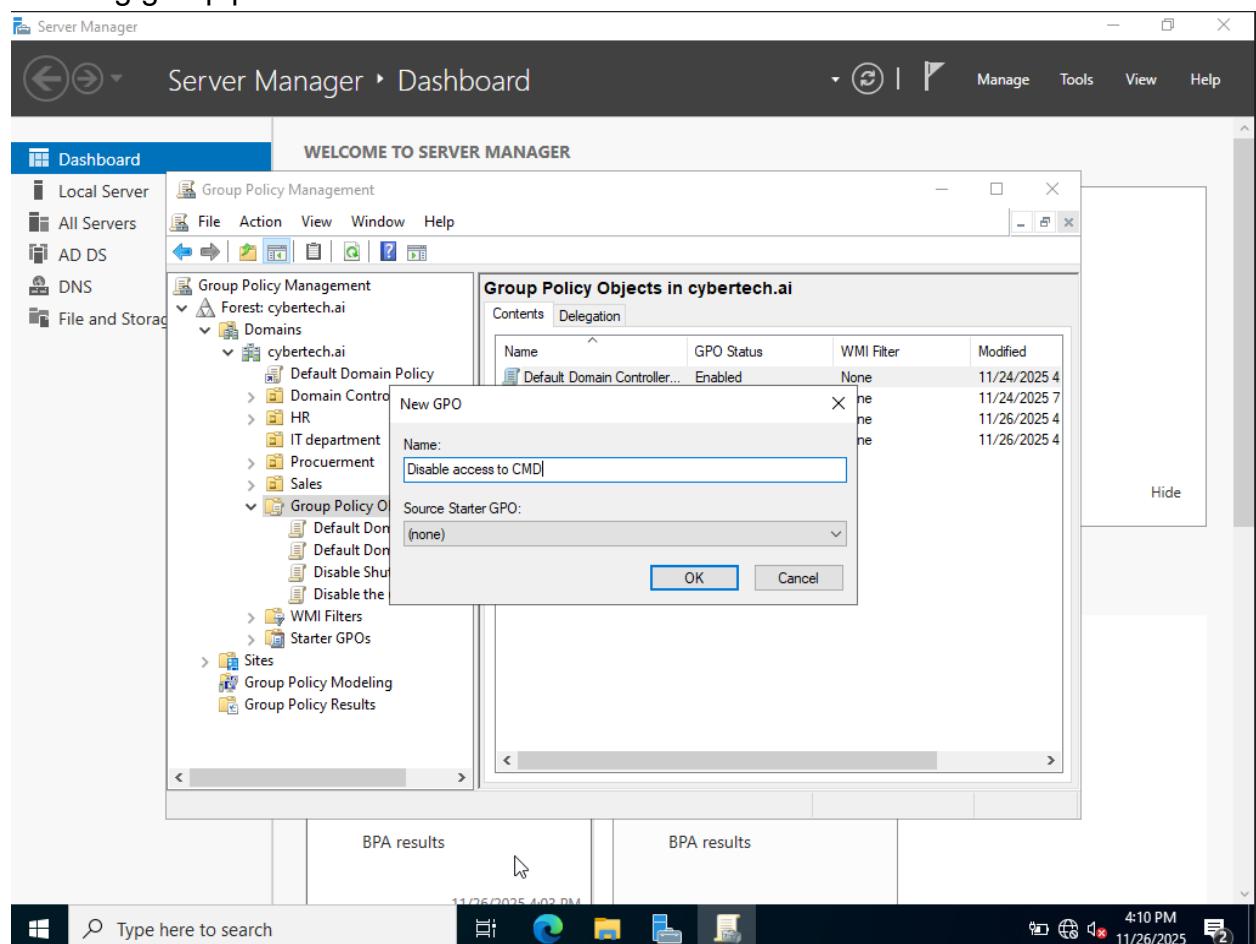
Confirming IP for windows 8 A



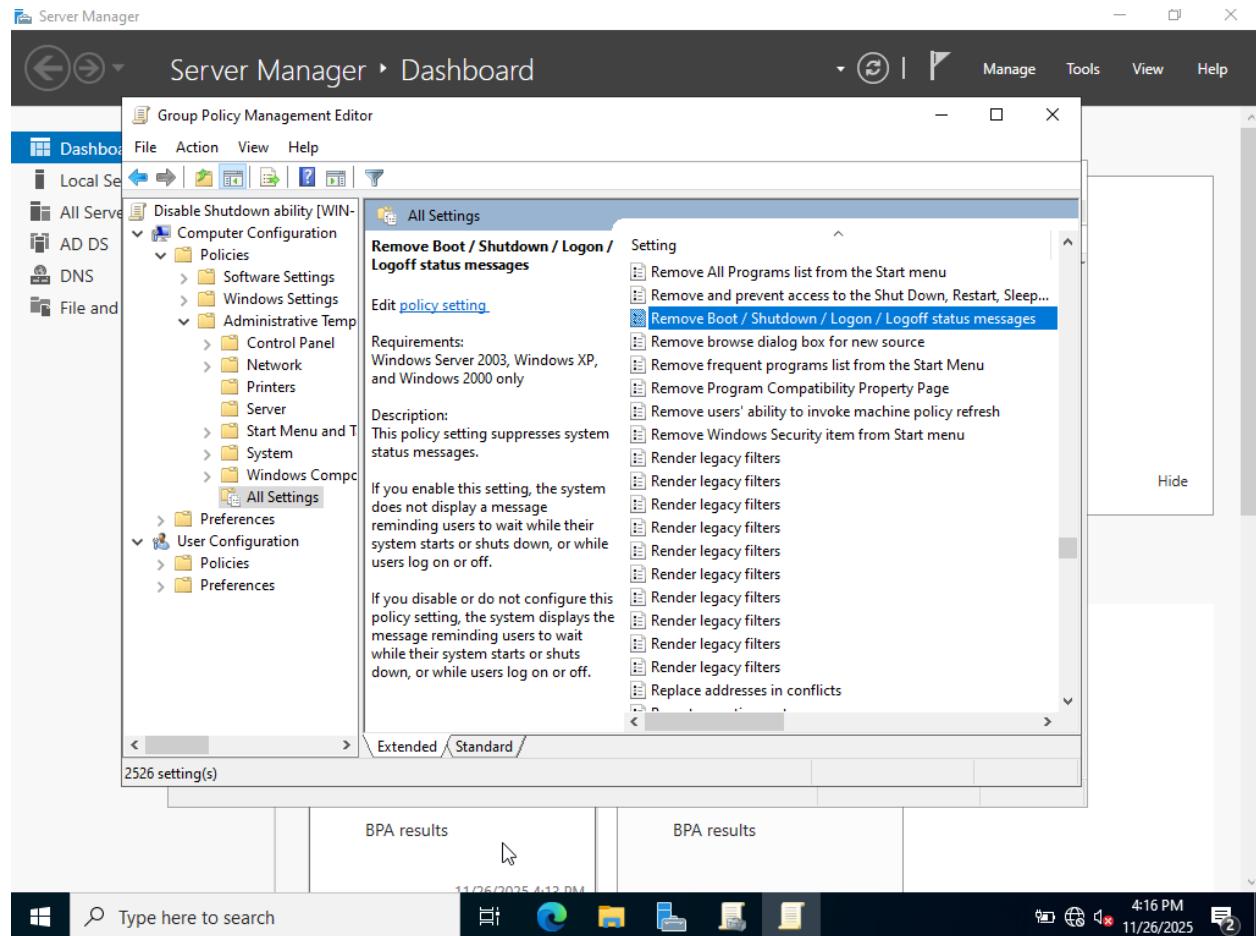
Windows 8 A assigned to User Sam



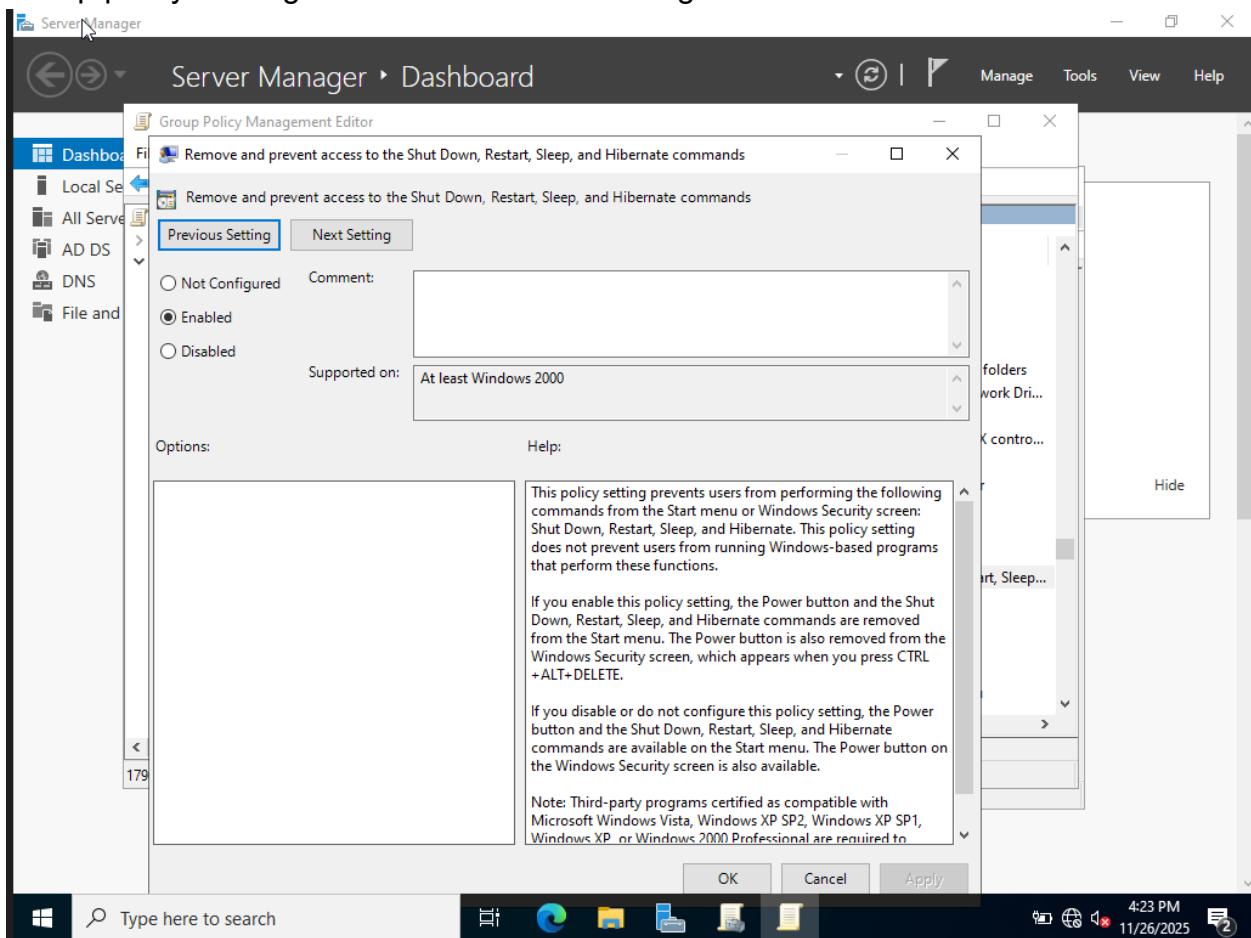
Creating group policies in AD – Disable access to CMD



Group policy management editor on Computer configuration



Group policy management editor on User configuration



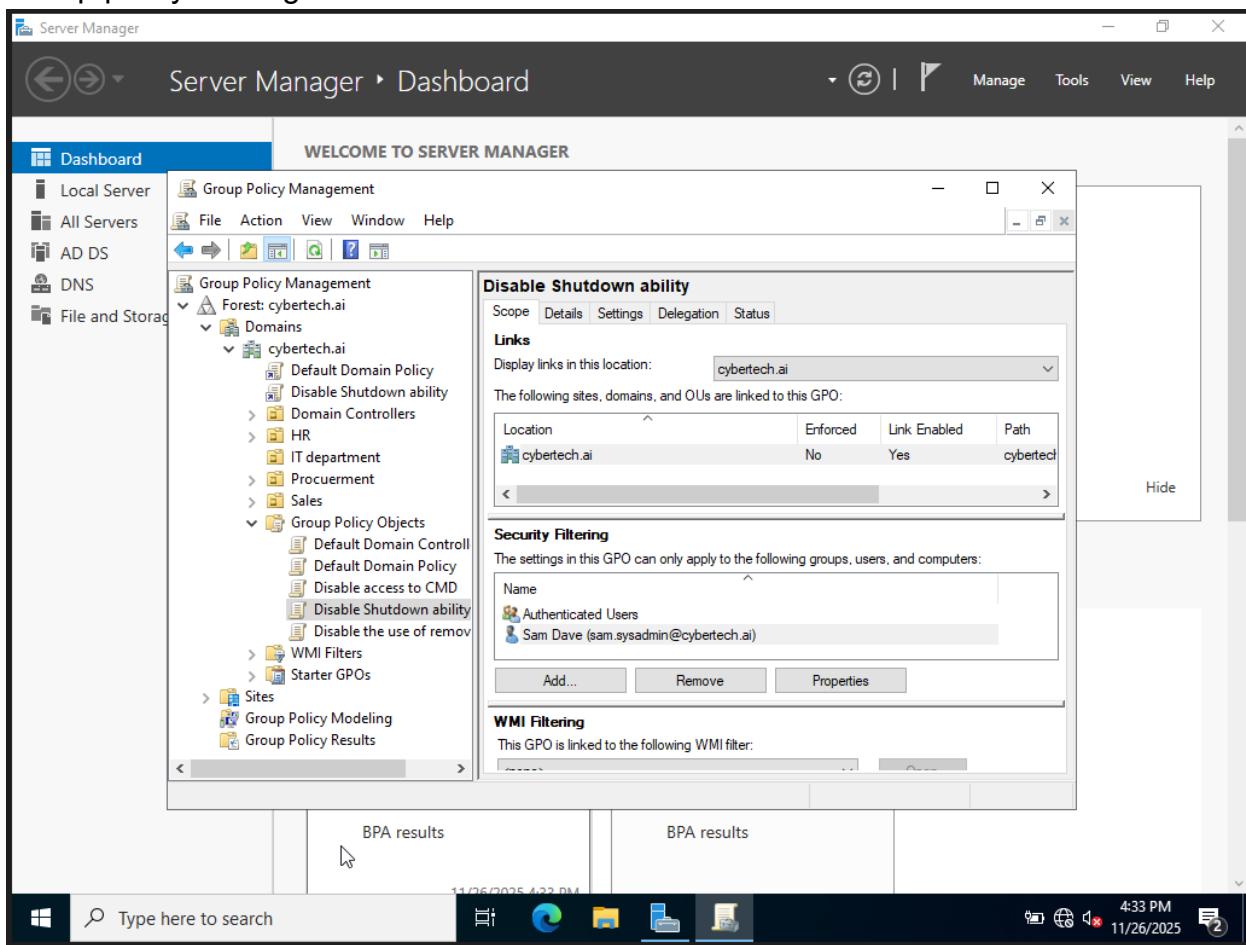
Group policy management details

The screenshot shows the Windows Server Manager interface. The left navigation pane includes links for Local Server, All Servers, AD DS, DNS, and File and Storage. The main content area is titled "WELCOME TO SERVER MANAGER" and displays the "Group Policy Management" section. A tree view under "Group Policy Management" shows the "Forest: cybertech.ai" and its "Domains" (cybertech.ai, HR, IT department, Procurement, Sales). Under "cybertech.ai", there are "Group Policy Objects" (Default Domain Controller, Default Domain Policy, Disable access to CMD, Disable Shutdown ability, Disable the use of removable media, WMI Filters, Starter GPOs), "Sites" (Group Policy Modeling, Group Policy Results), and "Group Policy Results". A specific GPO, "Disable Shutdown ability", is selected and detailed in the right-hand pane. The "Details" tab is active, showing the following information:

Disable Shutdown ability	
Data collected on: 11/26/2025 4:25:33 PM	
General	
Domain	cybertech.ai
Owner	CYBERTECH\Domain Admins
Created	11/26/2025 4:09:26 PM
Modified	11/26/2025 4:23:10 PM
User Revisions	1 (AD), 1 (SYSVOL)
Computer Revisions	1 (AD), 1 (SYSVOL)
Unique ID	{D3C79E69-B046-4120-A340-AD5781C40628}
GPO Status	Enabled

The status bar at the bottom indicates the time as 4:26 PM and the date as 11/26/2025.

Group policy management attached to a user in OU



Group policy update on Sever in CMD

The screenshot shows a Windows Server desktop environment. A Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe" is open, displaying the output of the command "gpupdate /force". The output shows the process of updating computer and user policies successfully. Below the Command Prompt is a Task Manager window showing performance-related tabs like Events, Services, Performance, and BPA results. The Performance tab is currently selected. At the bottom is the Windows taskbar with a search bar, pinned icons for File Explorer, Edge, and File History, and the system tray showing the date and time (11/26/2025 4:38 PM) and a notification icon.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

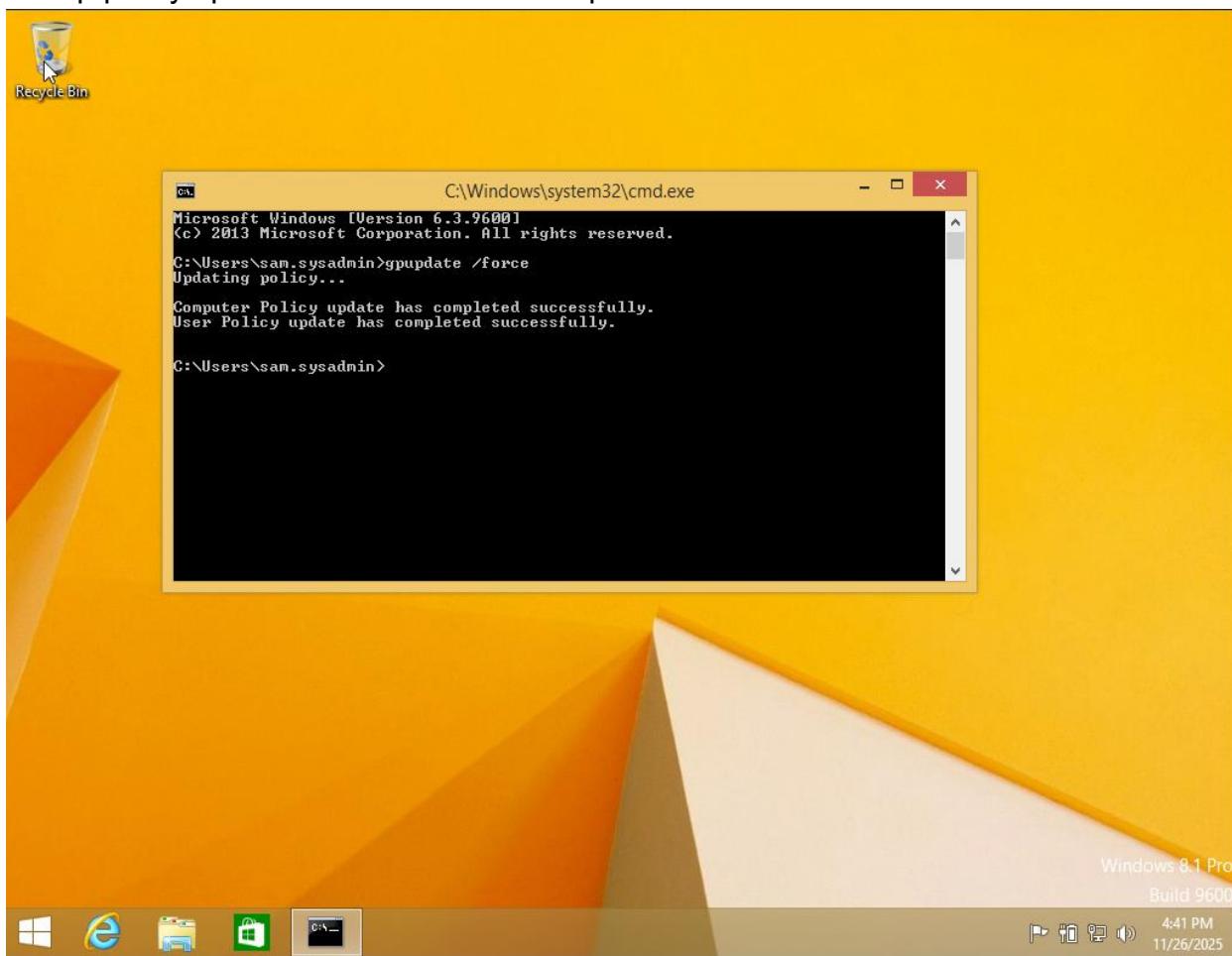
C:\Users\Administrator>
```

Events
Services
Performance
BPA results

Events
Services
Performance
BPA results

Type here to search 11/26/2025 4:38 PM 4:38 PM 11/26/2025

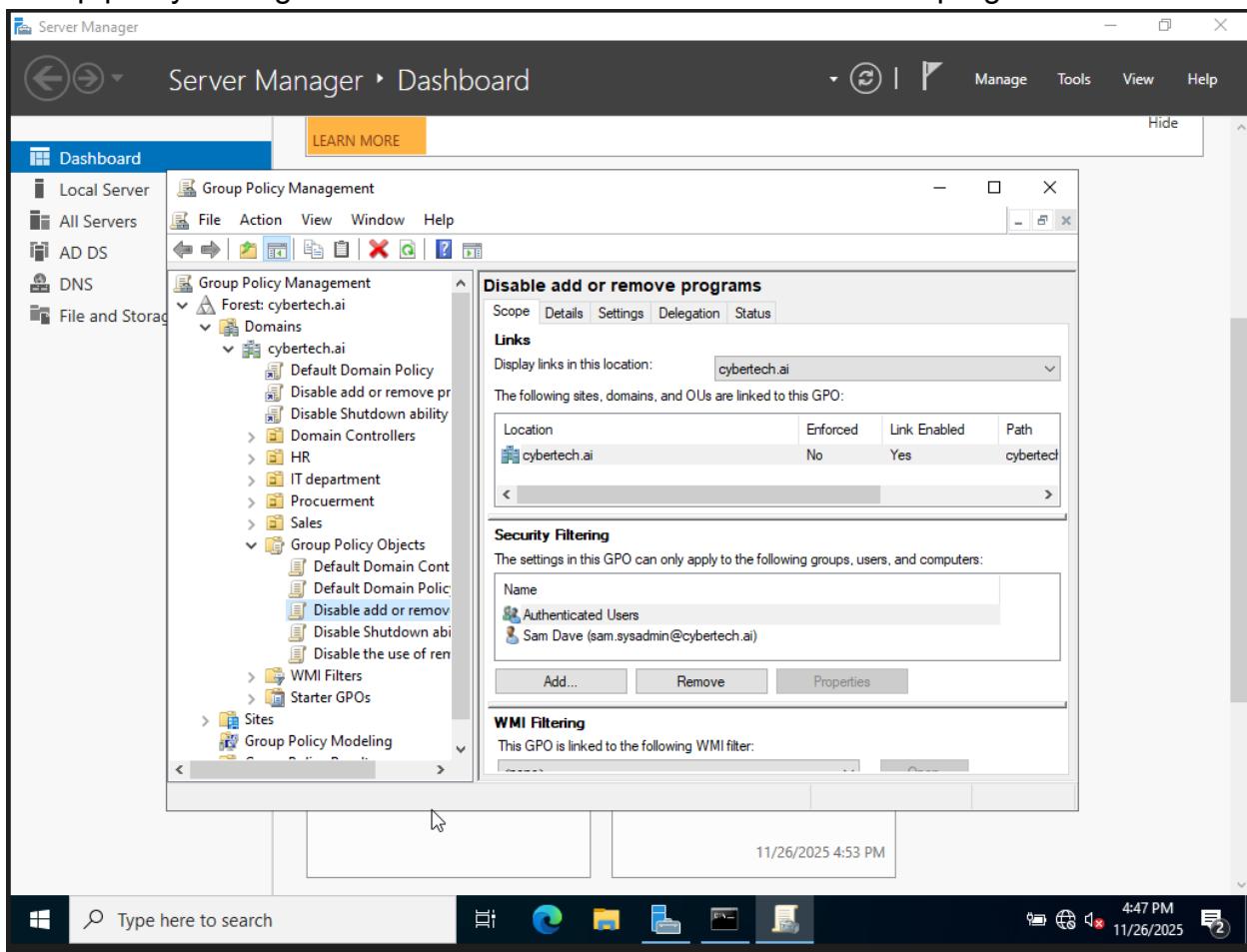
Group policy update on Win 8 A user computer



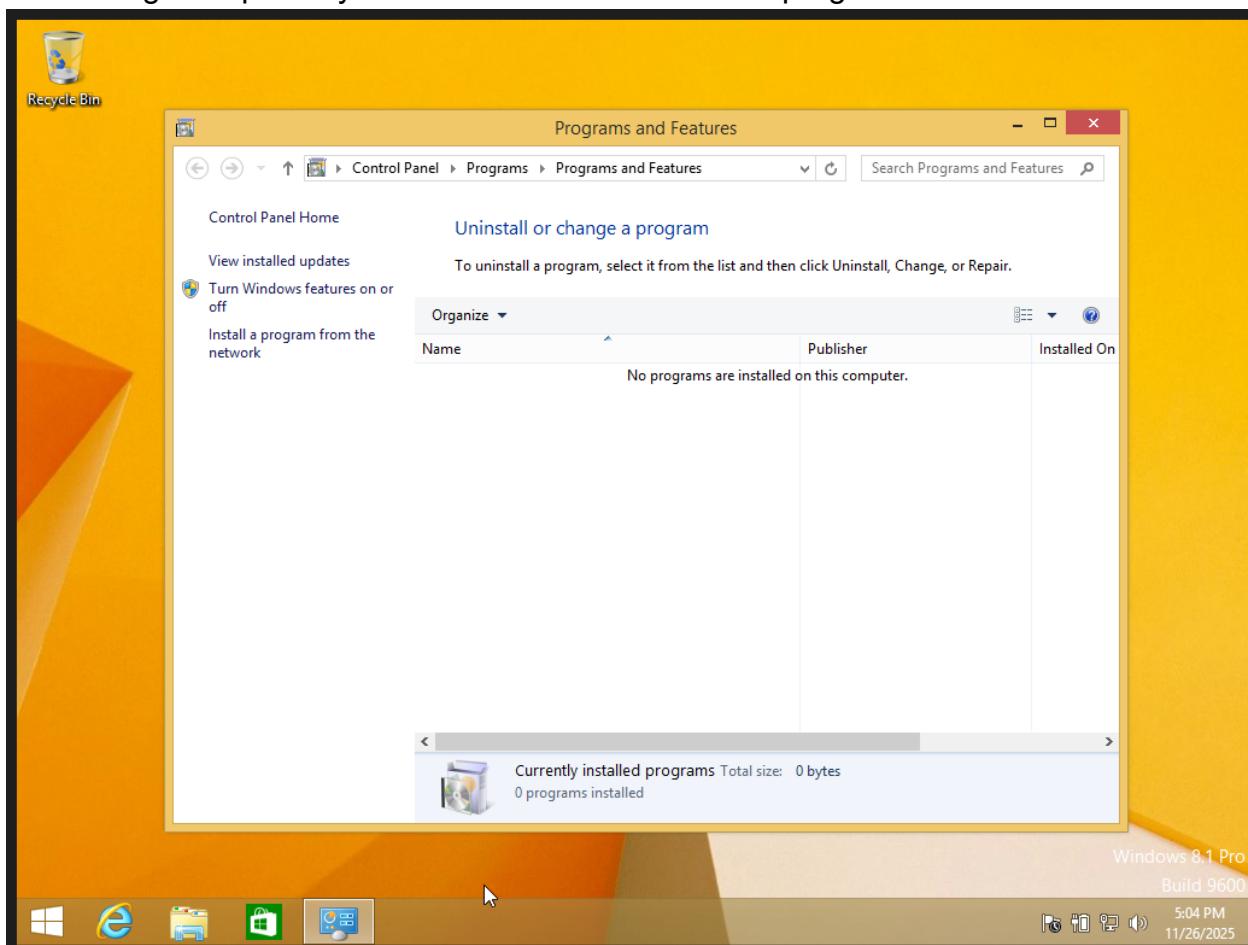
Confirming the Group Policy is effective



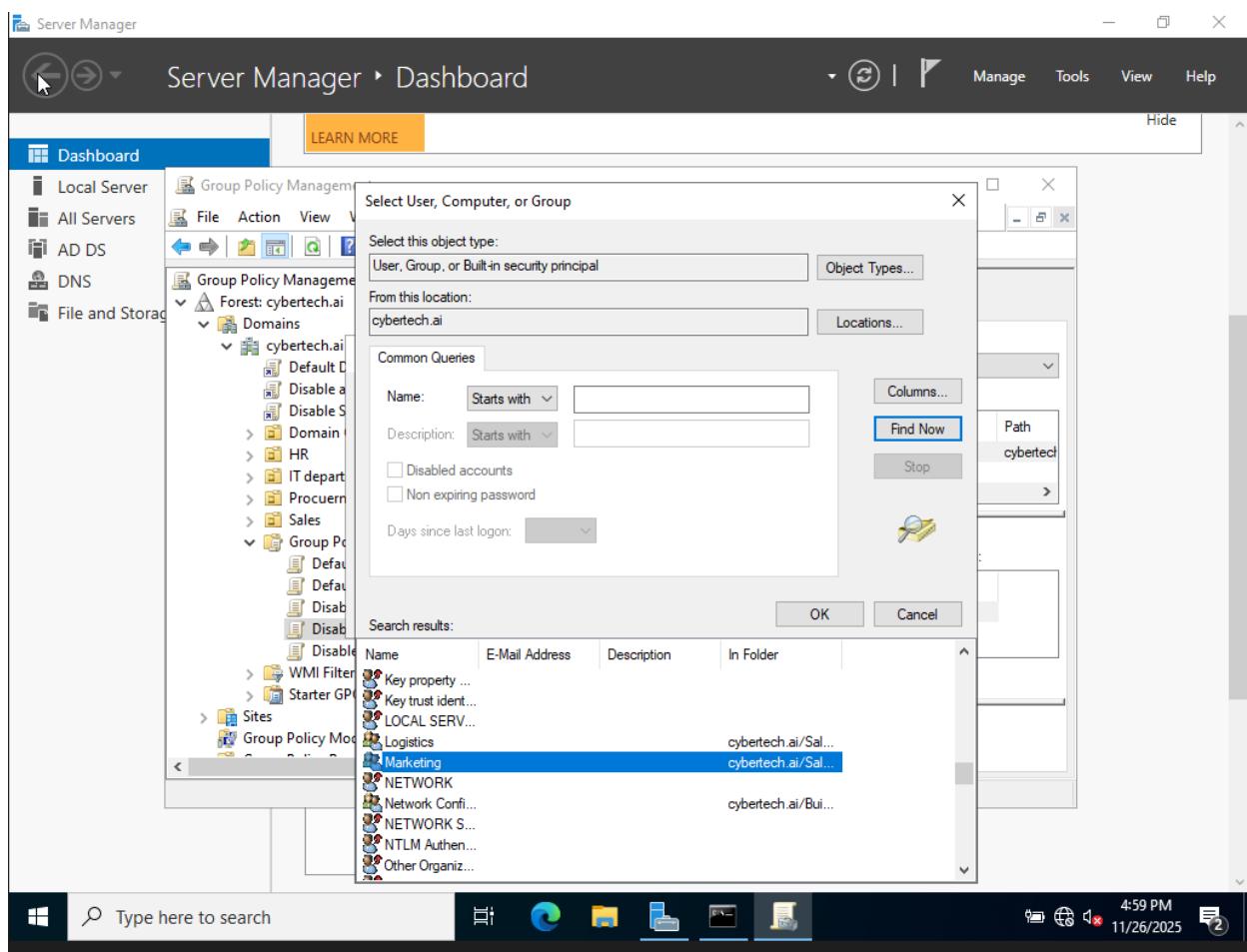
Group policy management is attached to a user to add or remove programs



Confirming Group Policy is effective for add or remove program



Group Policy Management for marketing department



Group Policy Management for marketing2

The screenshot shows the Windows Server Manager interface with the 'Group Policy Management' tool open. The left navigation pane lists 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and Storage'. The main pane displays the 'Group Policy Management' interface for the 'cybertech.ai' domain. The 'Disable Shutdown ability' GPO is selected. The 'Links' section shows a single link to the 'cybertech.ai' domain. The 'Security Filtering' section lists the 'Marketing' group under 'Name'. The 'WMI Filtering' section indicates no WMI filter is applied.

Location	Enforced	Link Enabled	Path
cybertech.ai	No	Yes	cybertech

Links
Display links in this location: cybertech.ai
The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
cybertech.ai	No	Yes	cybertech

Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users
Marketing (CYBERTECH\Marketing)
Sam Dave (sam.sysadmin@cybertech.ai)

WMI Filtering
This GPO is linked to the following WMI filter:
<none>

Group Policy update for policy

The screenshot shows a Windows Server 2022 desktop environment. At the top is the Server Manager dashboard. Below it is a command prompt window titled 'Administrator: C:\Windows\system32\cmd.exe'. The window displays the output of running 'gpupdate /force' multiple times, showing successful completion of Computer and User Policy updates. The taskbar at the bottom includes the Start button, a search bar, pinned icons for File Explorer, Edge, File History, Task View, and Printers, and a system tray with network, battery, and clock icons.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

BPA results 11/26/2025 4:58 PM

BPA results 11/26/2025 4:58 PM

5:02 PM 11/26/2025