Runbook: IT Pre-Onboarding Process for New Hires

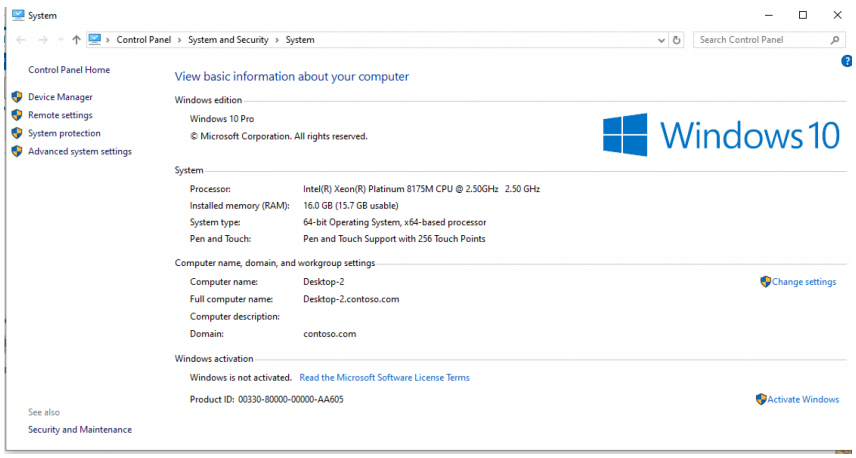
Introduction:

This runbook documents the procedure for setting up a computer and account for a new hire at StackFull Software. The process ensures that the user, computer, permissions, and policies are properly configured for a secure and functional first day.
The process includes domain joining, account creation, group assignment, shared folder setup, OU and GPO configuration, login restrictions, auditing logins, and creating PowerShell reports.
Each step below includes screenshots and detailed instructions.

Step 1: Join the computer to the domain `contoso.com`

📷 *Screenshot: Computer moved to domain (DESKTOP-2)*

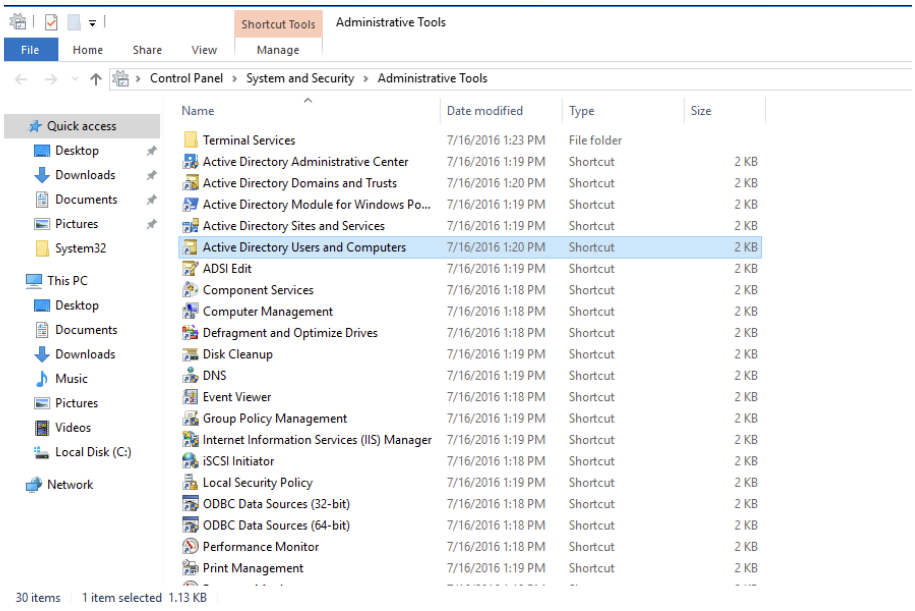
- On the client computer, open **System Properties**.
- In the Computer Name tab, click **Change…**
- Select **Domain** and enter: `contoso.com`.
- Provide credentials when prompted:
  Username: administrator
  Password: Pa$$w0rd
- Restart the computer when prompted.
- Verify in **Active Directory Users and Computers** that the computer (DESKTOP-2) now appears under the domain.



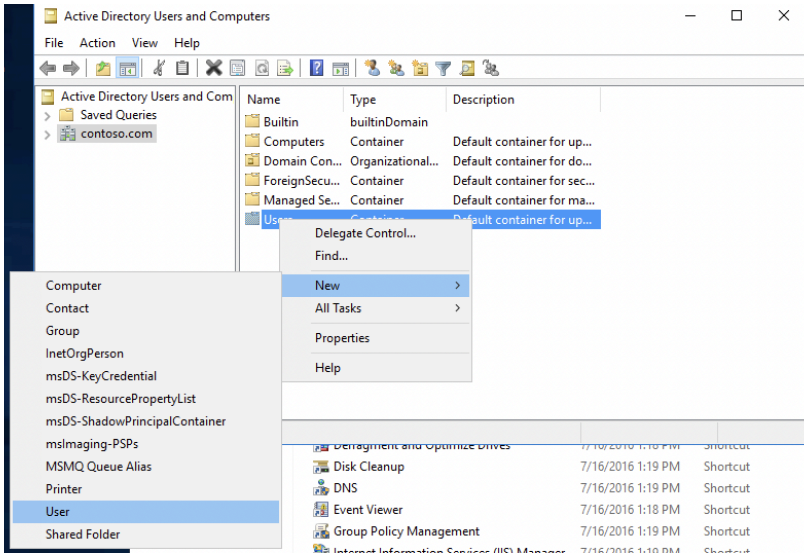
Step 2: Create a new user for the hire and set a password

📷 *Screenshot: User John Doe created and moved*

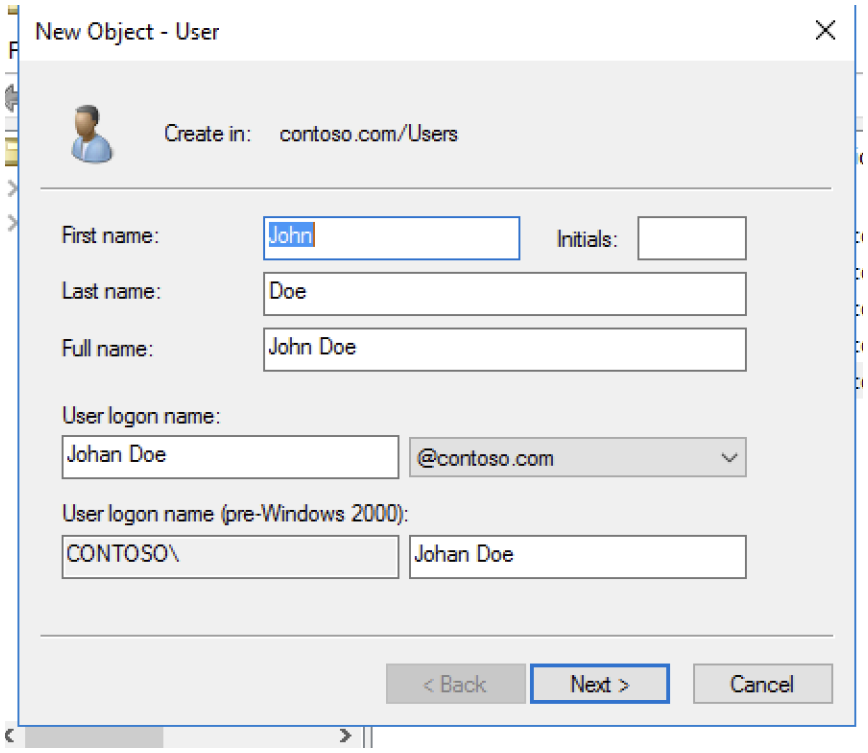
- On the server, open **Active Directory Users and Computers**.



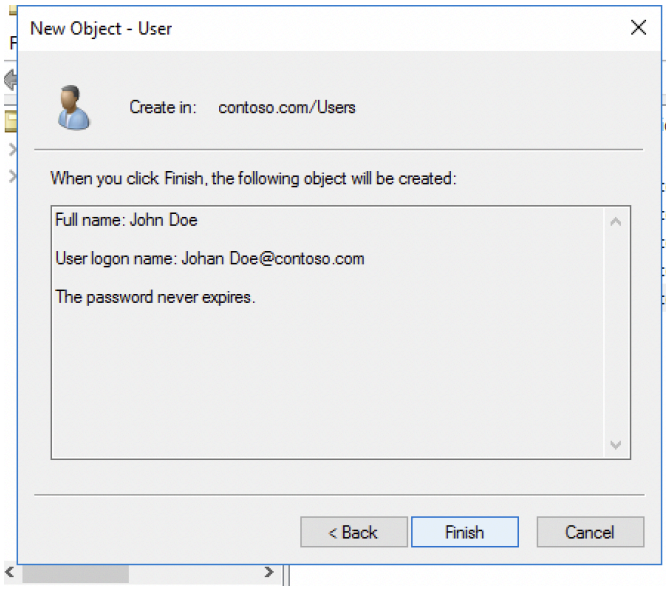
- Right-click the `Users` container, select **New → User**.



- Enter the user's details (e.g., John Doe) and username.

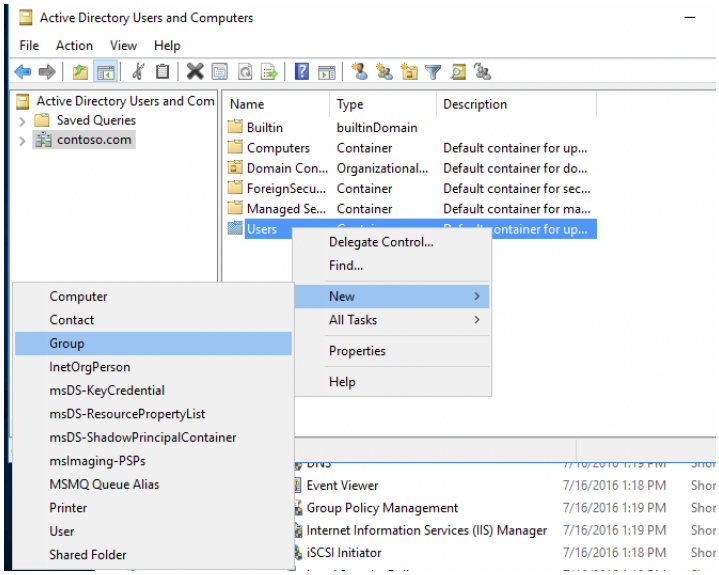


- Set an initial password and select .
- Click **Finish**.

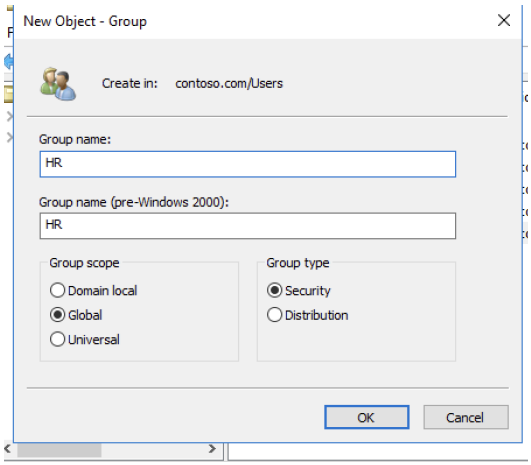


Step 3: Create a group for the department and add the user to it

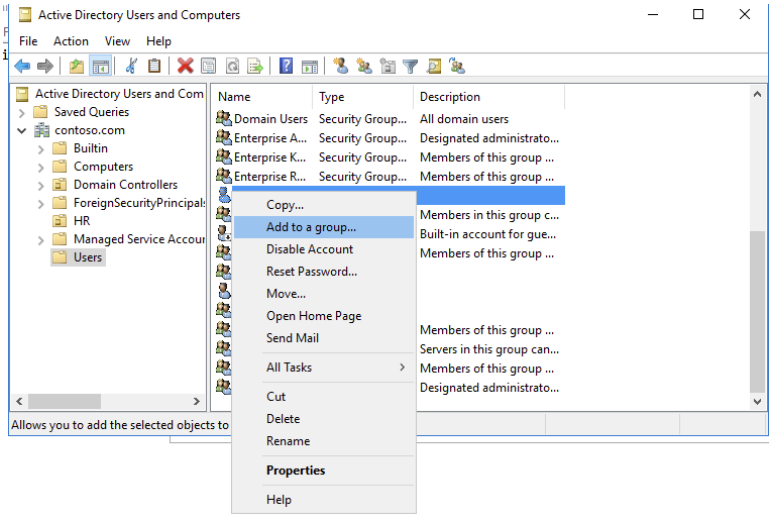
- In **Active Directory Users and Computers**, right-click the `Users` container and select **New → Group**.



- Name the group after the department (e.g., `HR`).
- Select **Global** and **Security**.

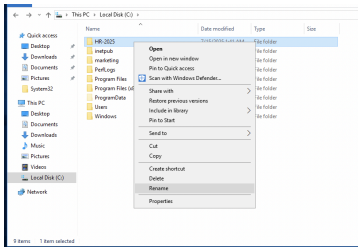


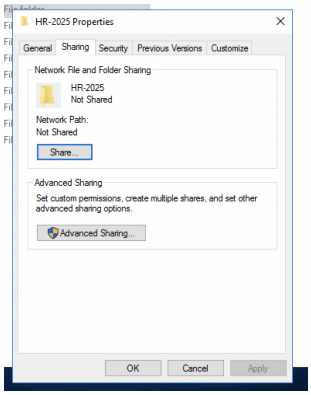
- Click **OK**.
- Right-click the user, select **Add to a group…**, and add them to the HR group.



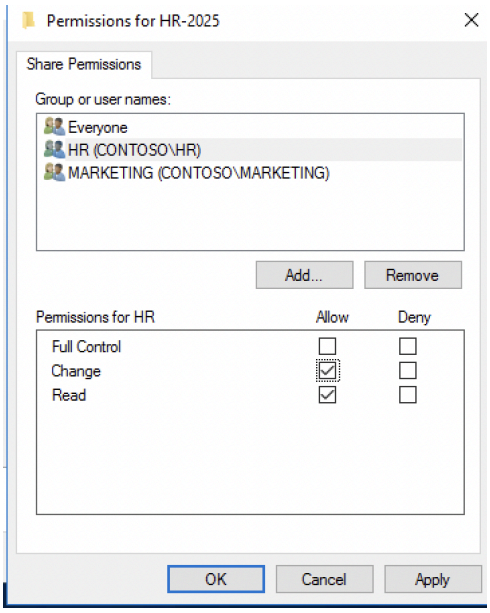
Step 4: Create and share a folder with the department group

- On the server, create a folder (e.g., `HR-2025`) on a shared drive.
- Right-click the folder, select **Properties** → **Sharing** → **Advanced Sharing…**.





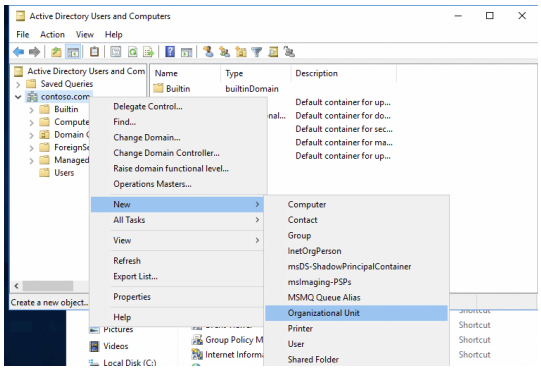
- Click **Permissions…**
- Remove unnecessary groups and add `HR (CONTOSO\HR)` with:
    - **Allow: Change and Read**
    - **Deny: none**



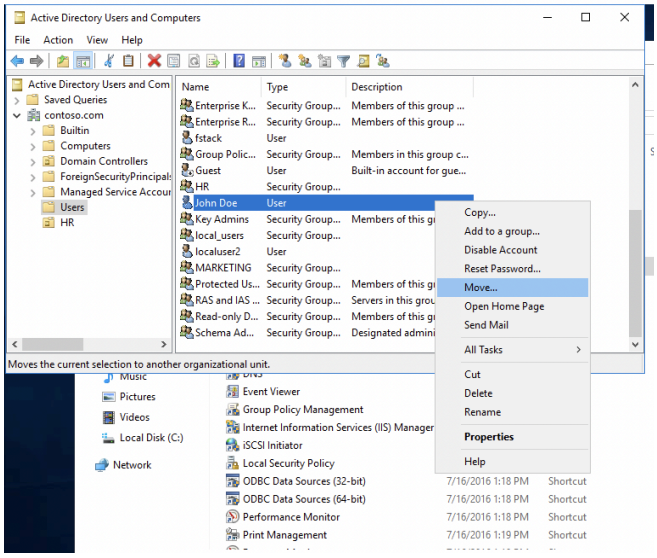
- Click **OK**.
- Inside the folder, create a text file named `test.txt`.

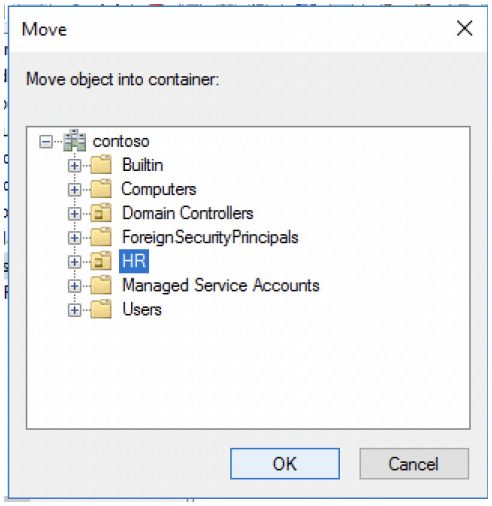
5: Create an Organizational Unit (OU) and place all objects

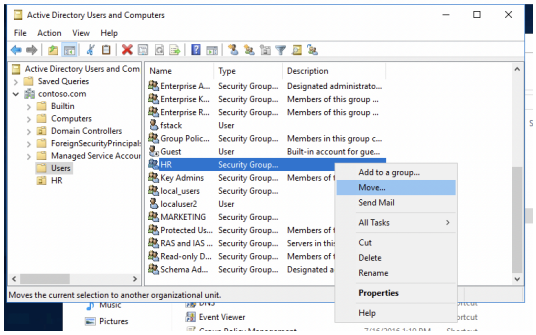
- In **Active Directory Users and Computers**, right-click the domain and select **New → Organizational Unit**.

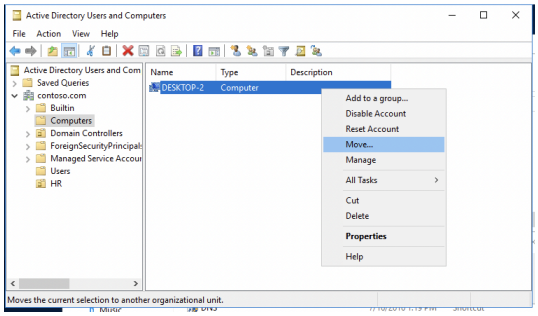


- Name it HR.
- Click **OK**.
- Move the John Doe user, HR group, and DESKTOP-2 computer into the HR OU.





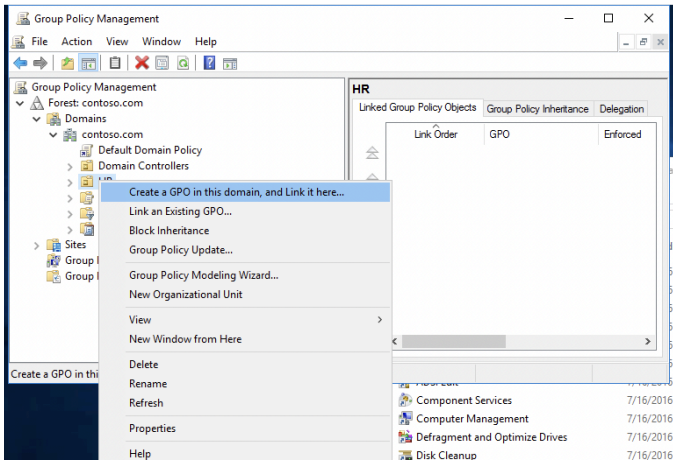


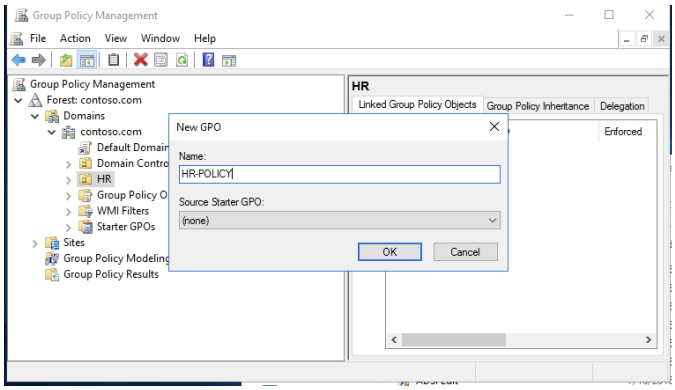


Step 6: Create and edit a Group Policy Object (GPO) with required settings

Create and link GPO:

- Open **Group Policy Management Console**.
- Right-click the HR OU and select **Create a GPO in this domain, and Link it here…**

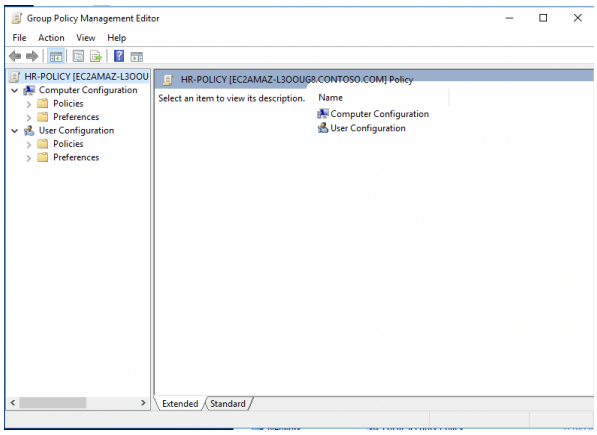




- Name it: `HR-POLICY`.
- Click **OK**.

Edit GPO:

- Right-click `HR-POLICY` and select **Edit…**.

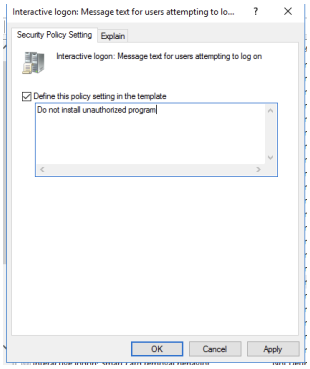


Display message at startup:

- Navigate to:
  `Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options`

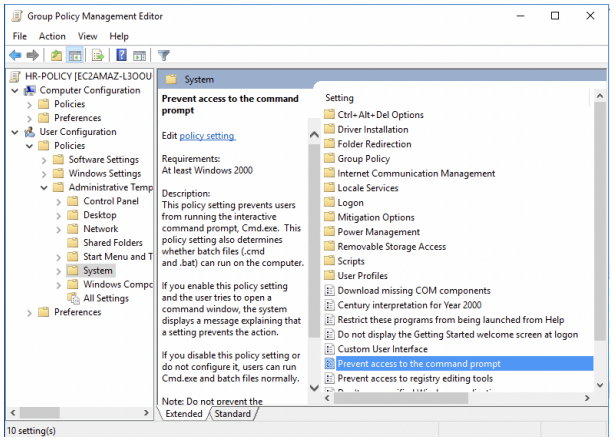
- Find **Interactive logon: Message text for users attempting to log on**.

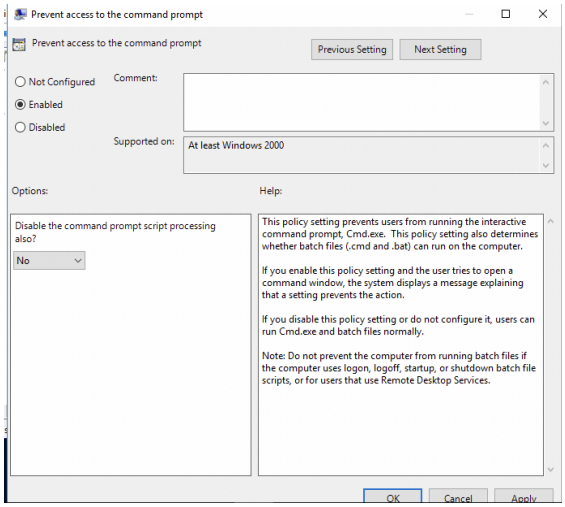
- Edit the setting and enter:
  `Do not install unauthorized programs.`



Prevent access to the Command Prompt:

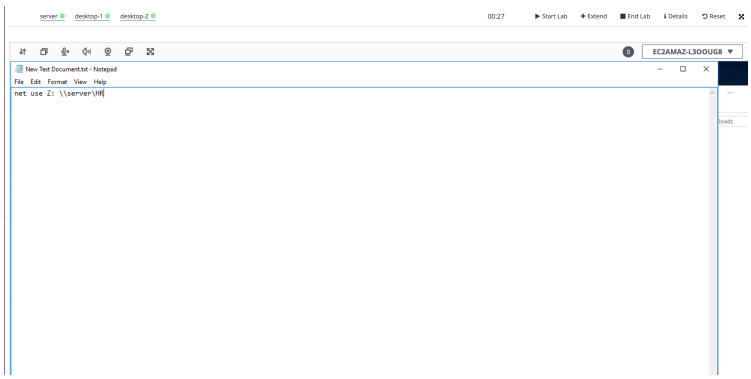
- Navigate to:
  `User Configuration → Policies → Administrative Templates → System`
- Double-click **Prevent access to the command prompt**.
- Select **Enabled** and ensure the script processing option is set to `No`.
- Click **OK**.



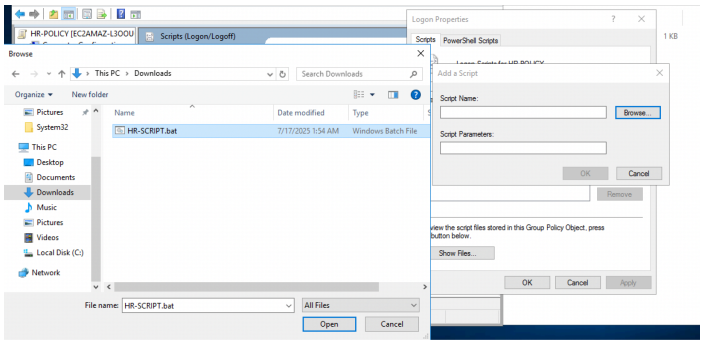


Add logon script to map the HR share:
Open Notepad and write:

```
net use Z: \\server\HR
```



- Save the file as `HR-SCRIPT.bat`.



- In the GPO Editor, navigate to:
  `User Configuration → Policies → Windows Settings → Scripts (Logon/Logoff)`

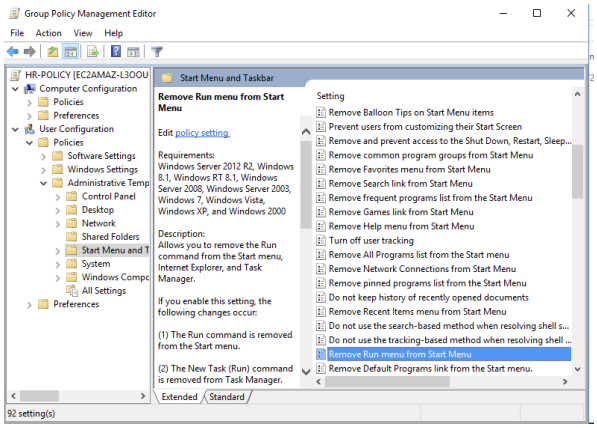
- Double-click **Logon**, click **Add… → Browse…**, and select `HR-SCRIPT.bat`.

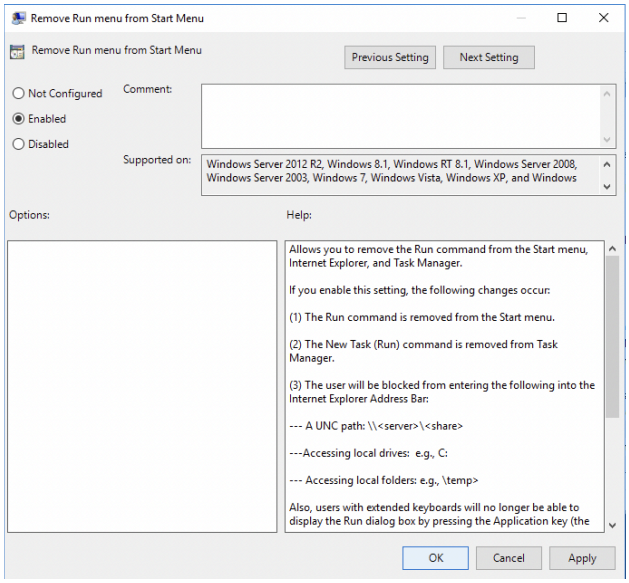
- Click **OK**.

Disable Run command from the Start Menu:

- Navigate to:
  `User Configuration → Policies → Administrative Templates → Start Menu and Taskbar`

- Double-click **Remove Run menu from Start Menu**.

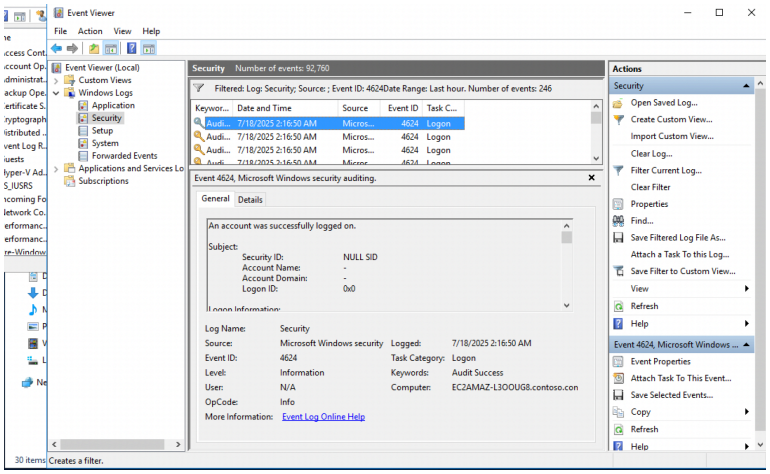




- Select **Enabled** and click **OK**.

Step 7: Verify last successful login for the user in Event Viewer

- Open **Event Viewer** on the server.
- Navigate to: `Windows Logs → Security`.
- Search or filter for Event ID `4624`.



- Verify the details of the most recent successful login for the user.

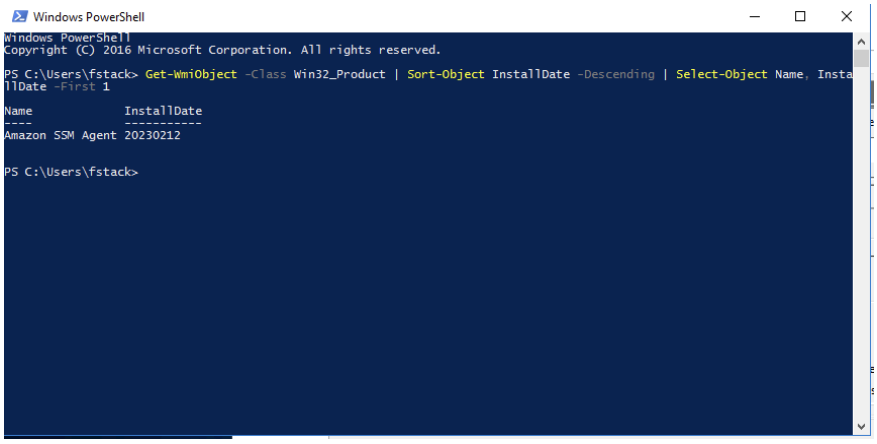
Step 8: Use PowerShell to find the most recently installed program

- Open PowerShell.

Run the following command:

powershell
CopyEdit

```
Get-WmiObject -Class Win32_Product | Sort-Object InstallDate
-Descending | Select-Object Name, InstallDate -First 1
```



- Review the output for the most recently installed software.

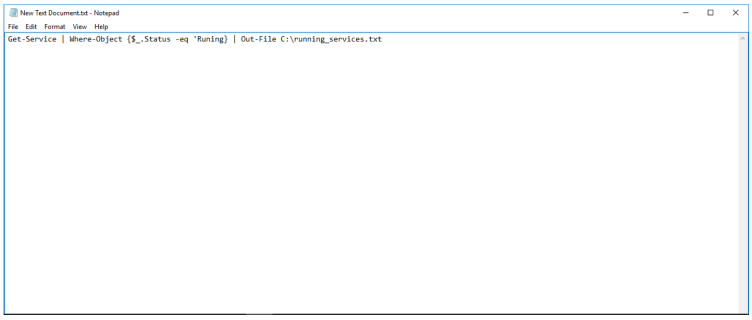
Step 9: Write and run PowerShell script to list running services

Write script:

Open Notepad and write:

powershell
CopyEdit

```
Get-Service | Where-Object {$_.Status -eq 'Running'} | Out-File C:\running_services.txt
```



- Save as `ListRunningServices.ps1`.

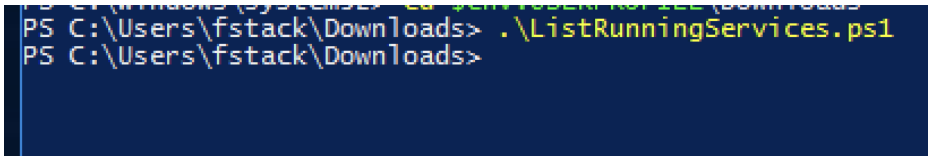
Run script:

- Open PowerShell and navigate to where the script is saved.

Run:

powershell
CopyEdit

```
.\ListRunningServices.ps1
```



Verify output:

- Open `C:\running_services.txt` and confirm that it lists all currently running services with `Status`, `Name`, and `DisplayName`.