February 2025

GWS GROUP

WINDOWS RUNBOOK

IT PRE-ONBOARDING RUNBOOK

GWS GROUP

Prepared by: Carlos R.
Date: 02/15/2025
Version: 1.0

Overview

This runbook provides a step-by-step guide for the IT team to prepare a new hire's workstation and account before their first day. It ensures proper domain integration, security configuration, and access control following StackFull Software's IT policies.

New Hire Information
- Name: New Hire
- Role: Staff
- Department: Human Resources

Executive Summary

This IT Pre-Onboarding Runbook outlines the standardized process for preparing a new hire's workstation and account at StackFull Software. It ensures that all new employees have the necessary technology setup, security configurations, and access permissions before their first day.

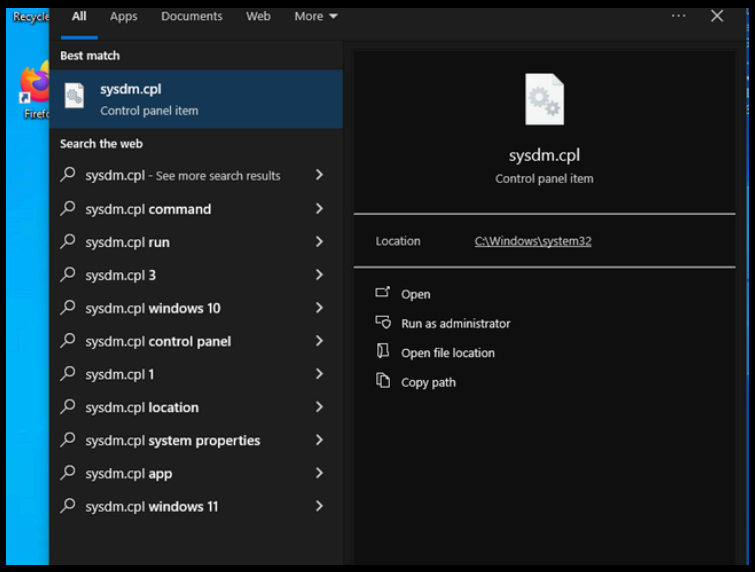
Key steps include:
- Domain Integration – Joining the new hire's computer to the contoso.com domain.
- User & Group Creation – Setting up an Active Directory user account and assigning them to a department-specific security group.
- File Share & Access Control – Creating a secure shared folder with role-based access permissions.
- Security Policies & Restrictions – Applying Group Policy Objects (GPOs) to enforce security measures, such as login messages, restricted access to CMD, and mapped network drives.
- System Auditing – Verifying login activity through Event Viewer and monitoring installed software using PowerShell.
- Automation & Monitoring – Implementing PowerShell scripts to capture running services and system configurations.

By following this runbook, the IT team ensures a secure, efficient, and repeatable onboarding process, aligning with StackFull Software's IT security and operational best practices.

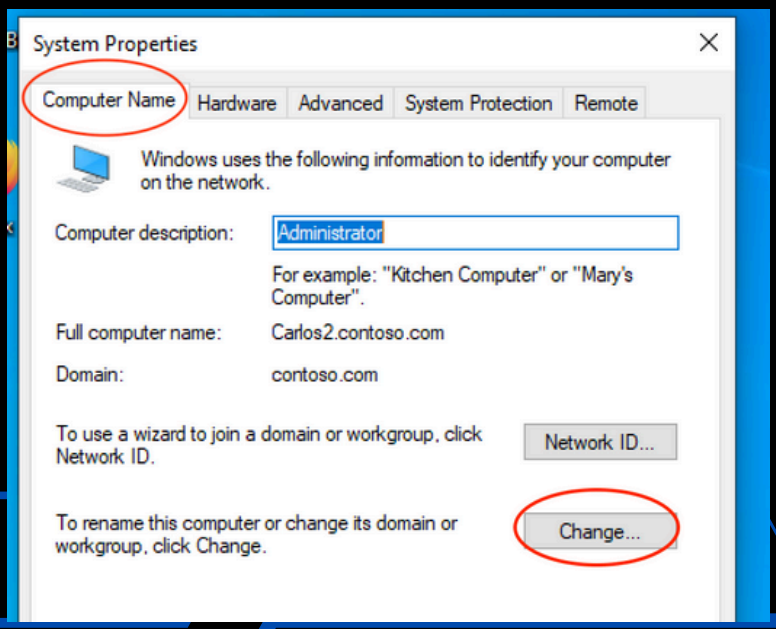
Steps to follow

Step 1: Join the Computer to the Domain

1. Log into the workstation as a local administrator.
2. Open System Properties:

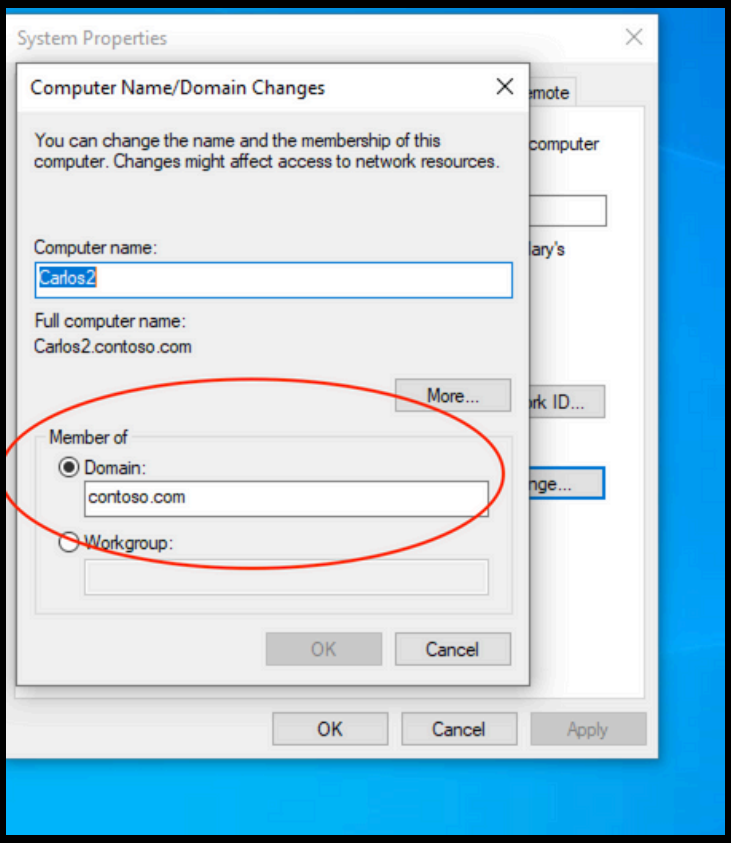


3. Click the Change button under the Computer Name tab.



Step 1 Cont.

4. Select Domain, enter contoso.com, and click OK.



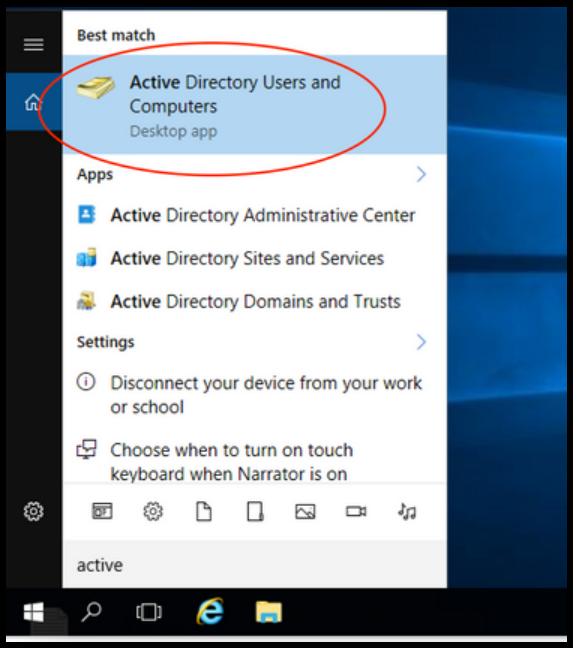
5. When prompted, enter domain administrator credentials:
   - Username: administrator
   - Password: Pa$$w0rd

6. Restart the computer to complete the process.

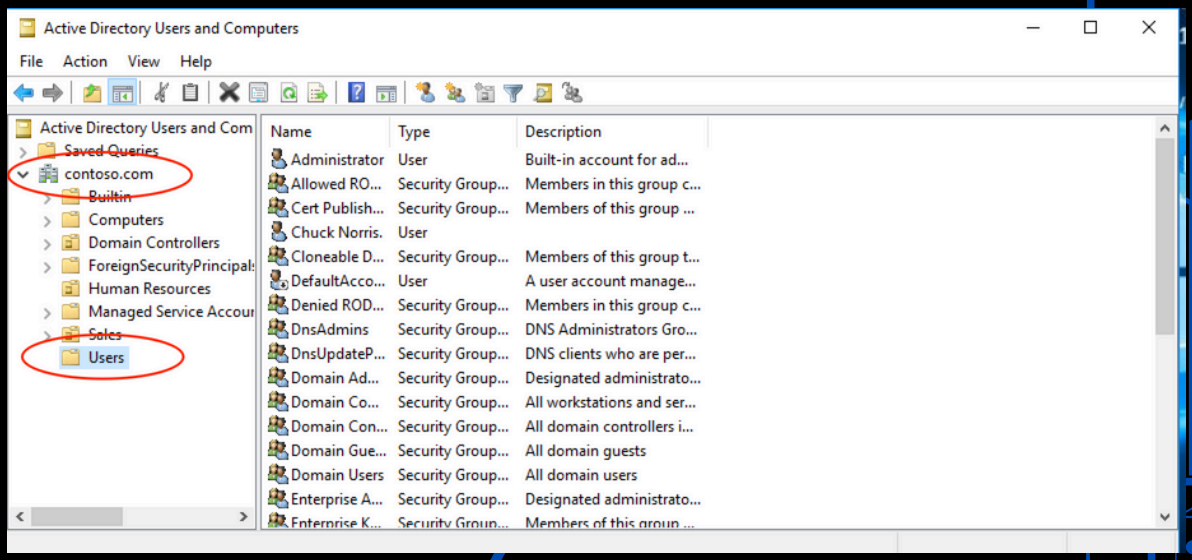
Step 2: Create a New User Account

1. Log into the server as a domain administrator.

2. Open Active Directory Users and Computers.

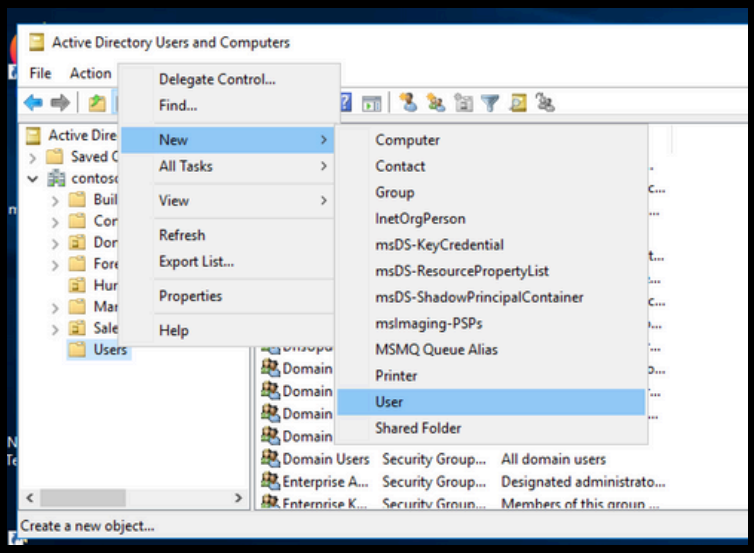


3. Navigate to contoso.com > Users.



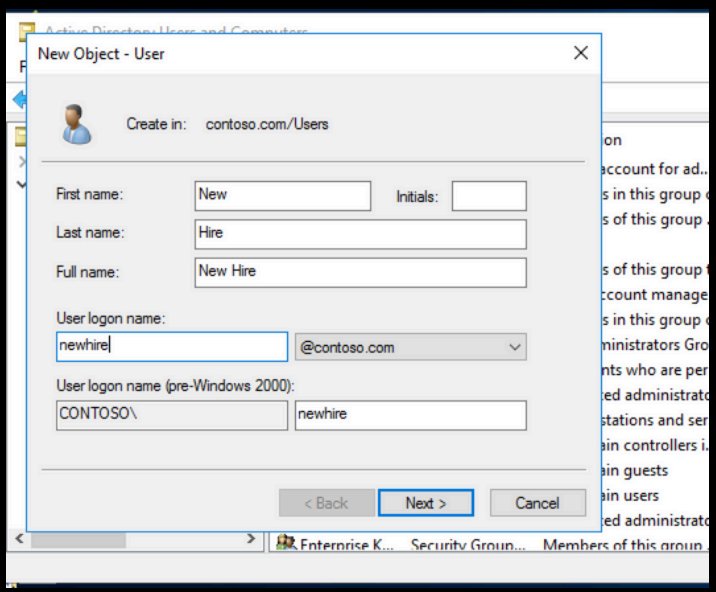
Step 2: Cont.

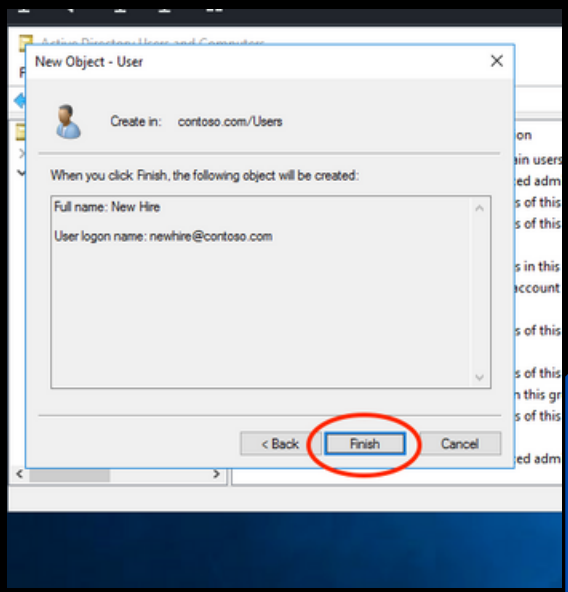
4. Right-click Users > Select New > User.



5. Enter the new hire's details:

- Username: [Insert Username]
- Password: [Insert Secure Password]
- Ensure "User must change password at next logon" is checked. Click Finish.

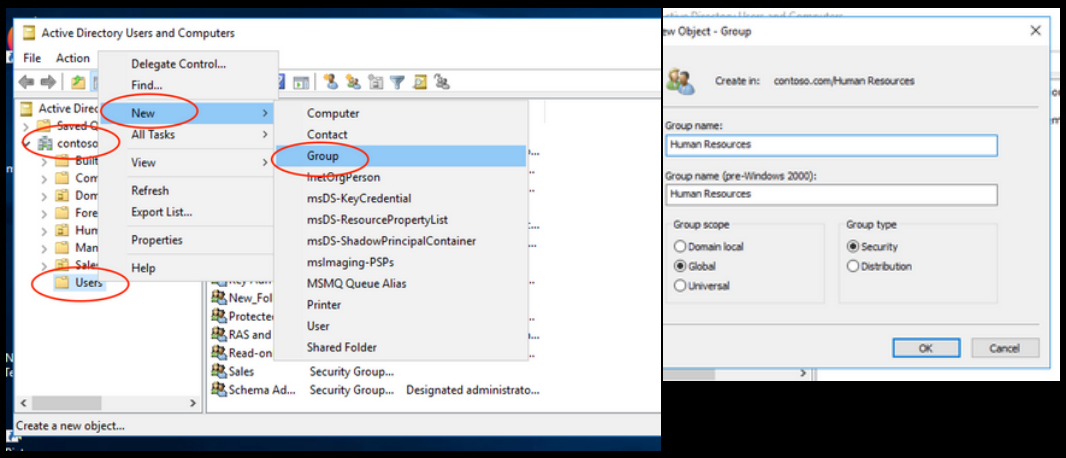




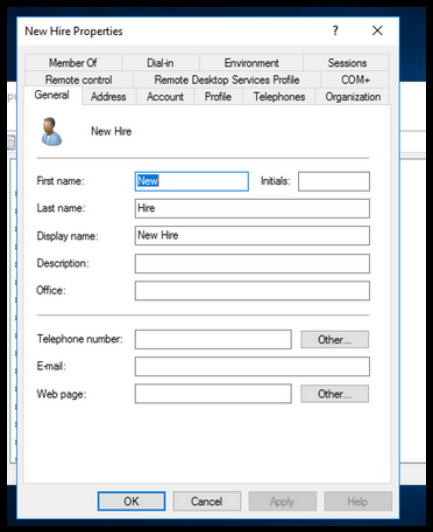
✅ Verification: The user should now appear in Active Directory.

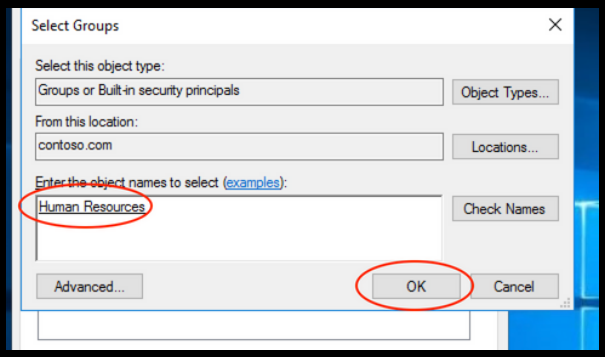
Step 3: Create a Group and Assign the User

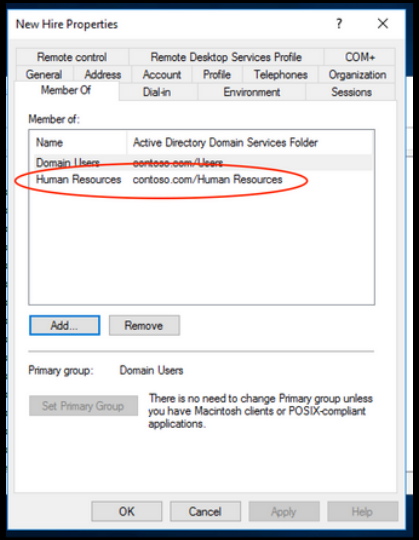
1. In Active Directory Users and Computers, navigate to contoso.com > Right-click User > Select New > Group. Then name the group based on the new hire's department (e.g., Human Resource Team).



2. Add the user to the group: Right-click the new hire's account > Properties > Member Of > Add > Select the department group. Don't forget to click apply.

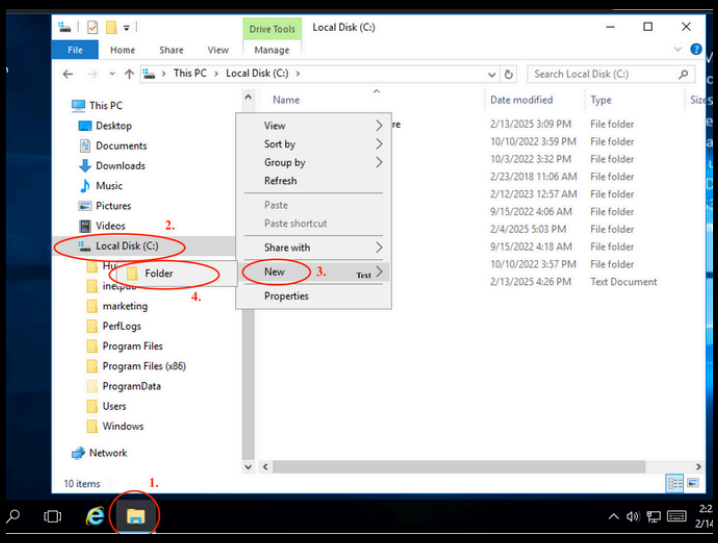


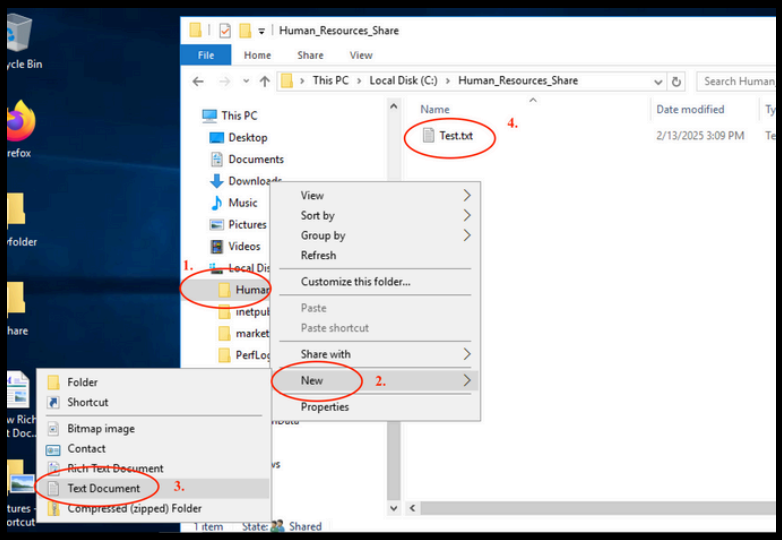




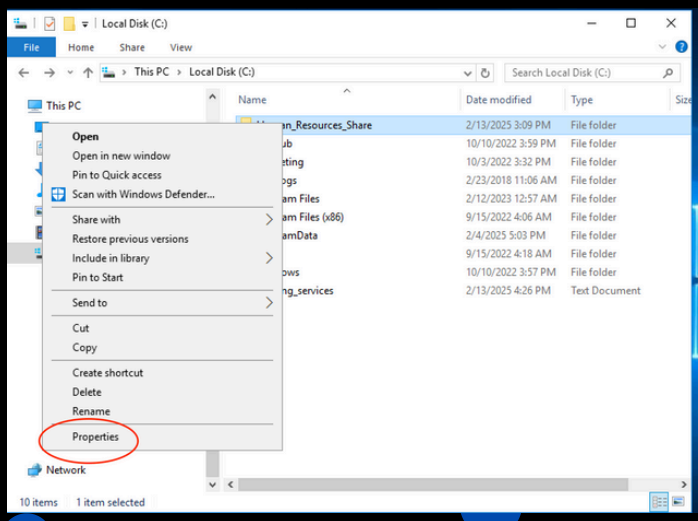
Step 4: Create a Department Share and Assign Permissions

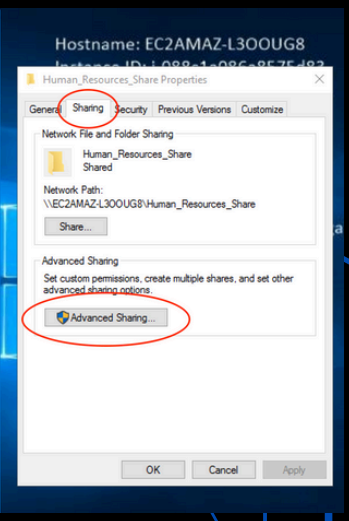
1. On the server, open File Explorer and create a folder. Then In the folder, create a text document called test.txt.





2. Right-click the folder > Properties > Sharing tab > Advanced Sharing.

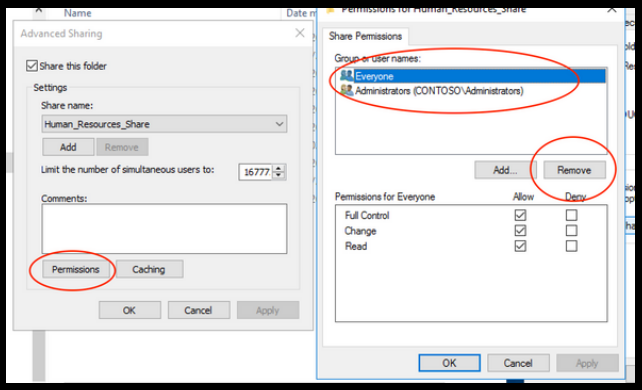


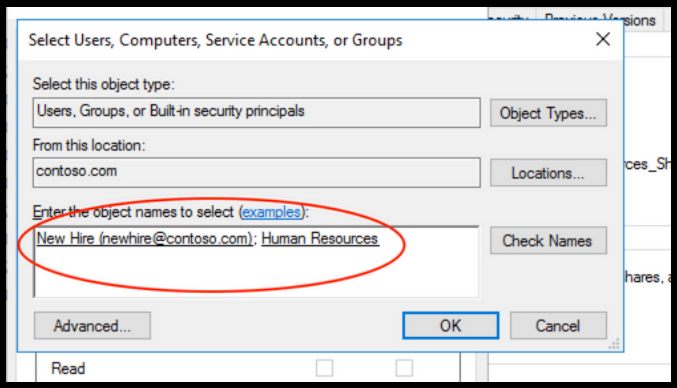


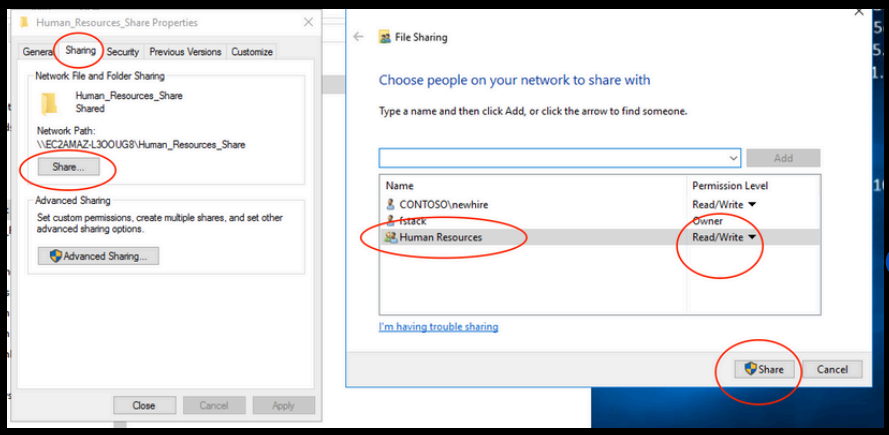
Step 4: Cont.

3. Check Share this folder > Click Permissions. Highlight and remove Everyone, then Add:

- The department group (HR Team).
- Set Read & Write permissions.



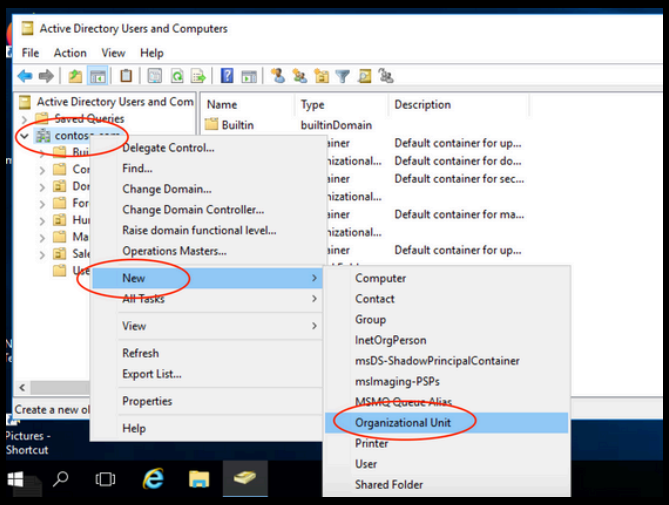




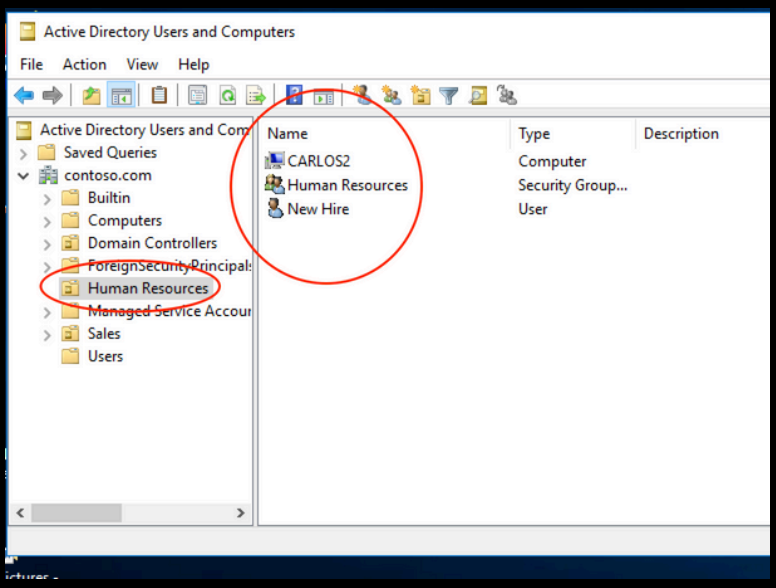
✅ Verification: Only department members can access the shared folder.

Step 5: Create an Organizational Unit (OU) and Apply Group Policy

1. Open Active Directory. Then right-click contoso.com > New > Organizational Unit (OU).



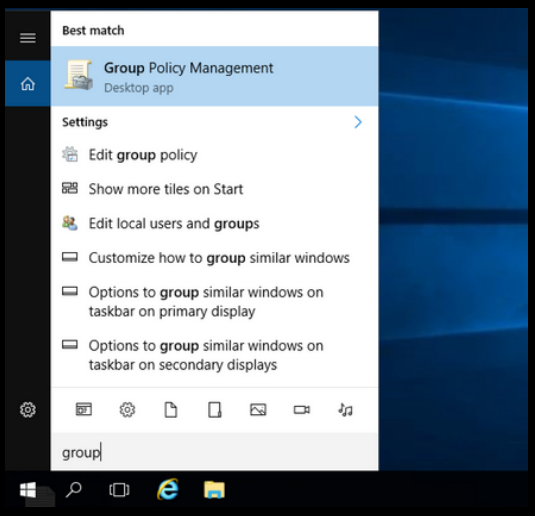
2. Name the OU based on the department (e.g., HR). Move the user, group, and computer into the new OU.
• Drag and drop the objects into the department OU.

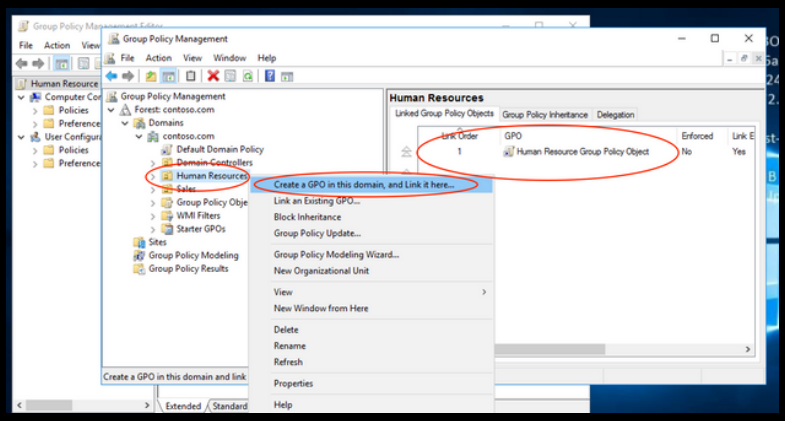


✅ Verification: The new OU contains the correct user, group, and computer.

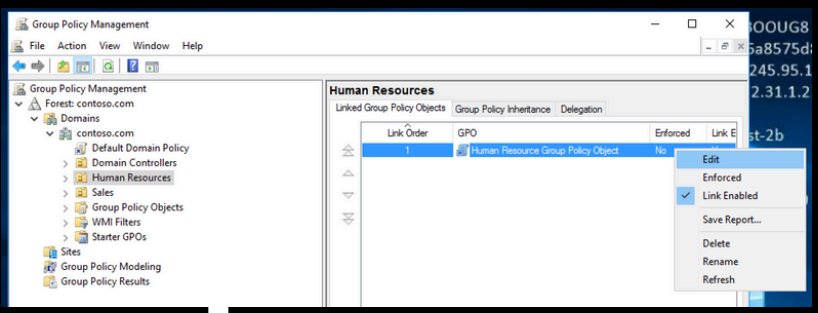
Step 6: Configure Group Policy (GPO) for Security & Access Control

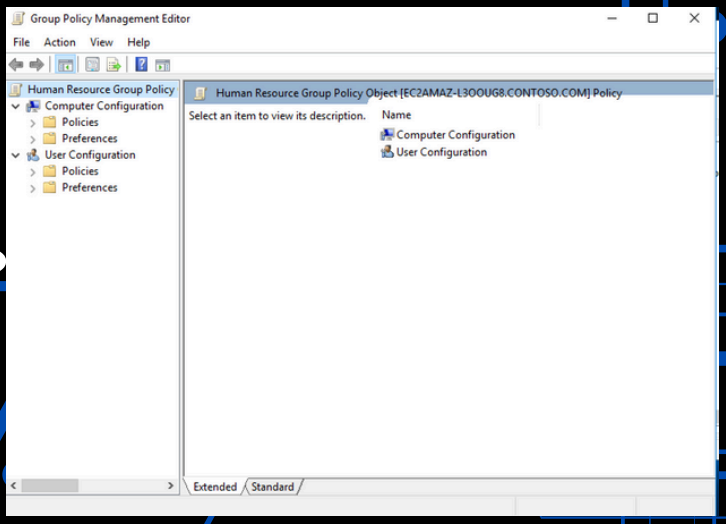
1. Open Group Policy Management. Right-click the new OU > Create a GPO in this domain.





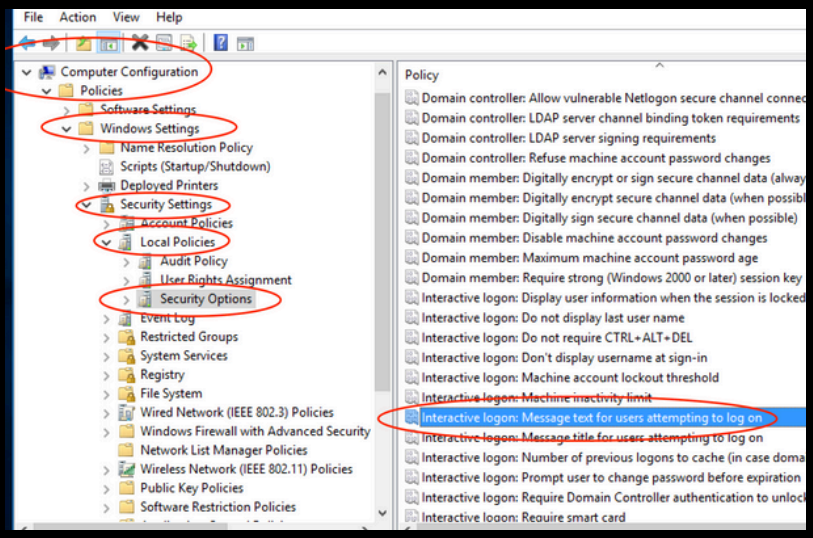
2. Edit the GPO

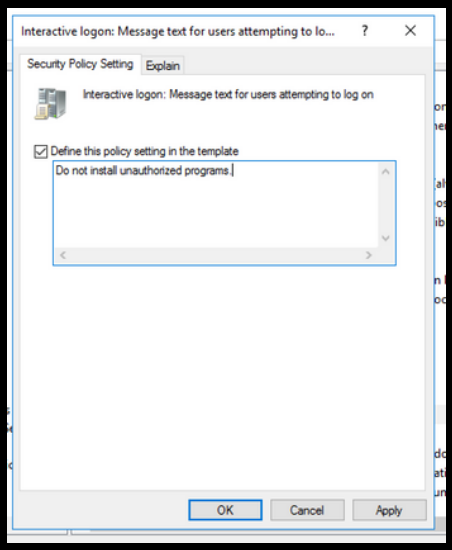


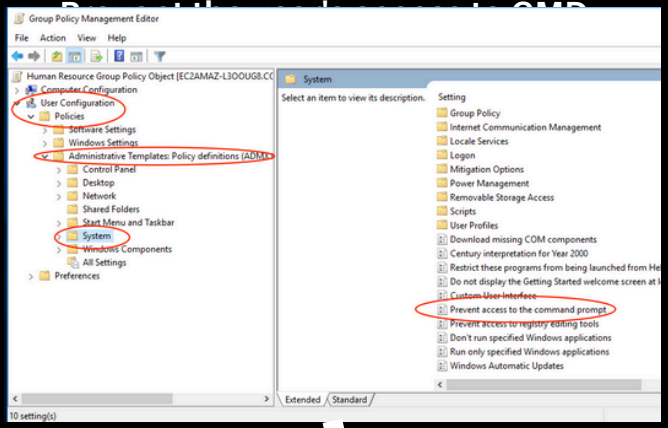


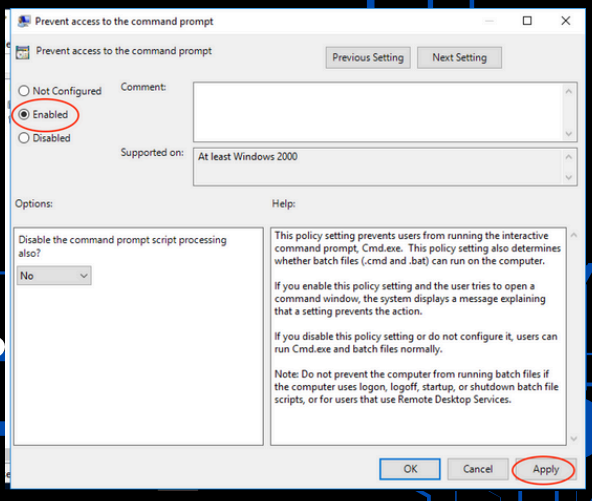
Step 6: Cont.

3. Edit the GPO and apply the following rules:
   - A message should appear whenever the computer starts (do not install unauthorized programs). In the GPE go follow this path: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options



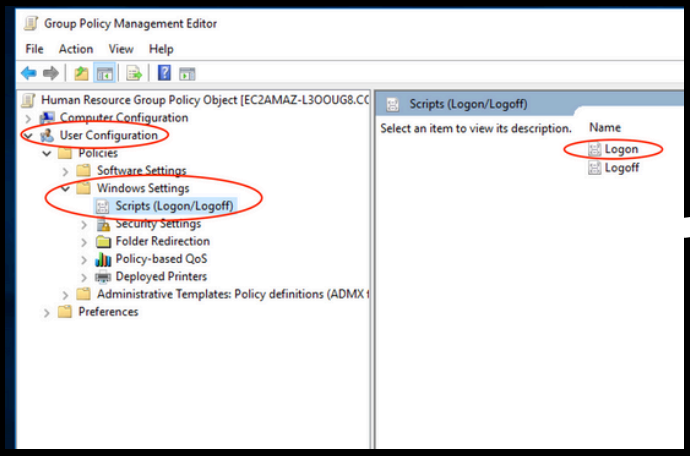


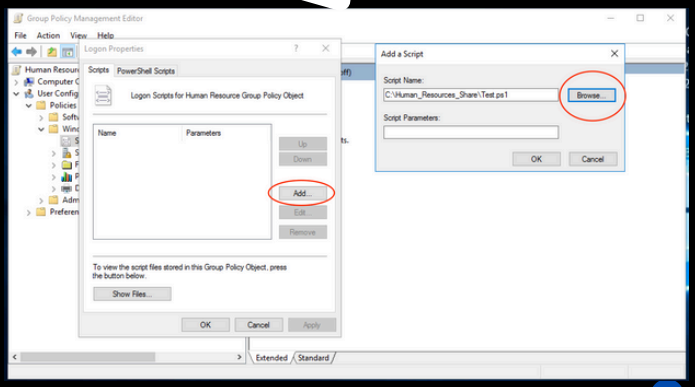




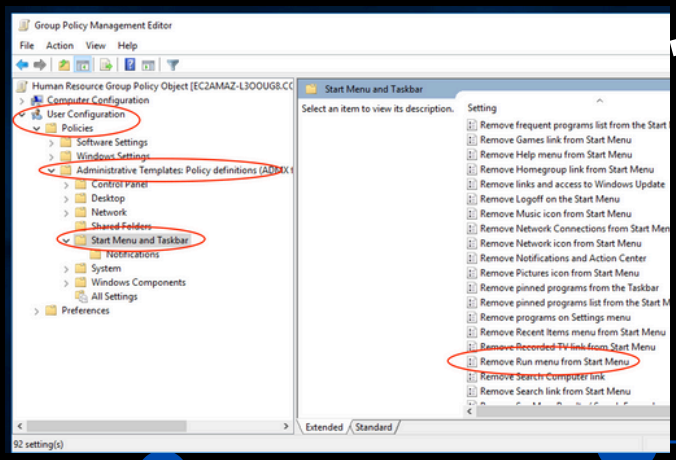
Step 6: Cont.

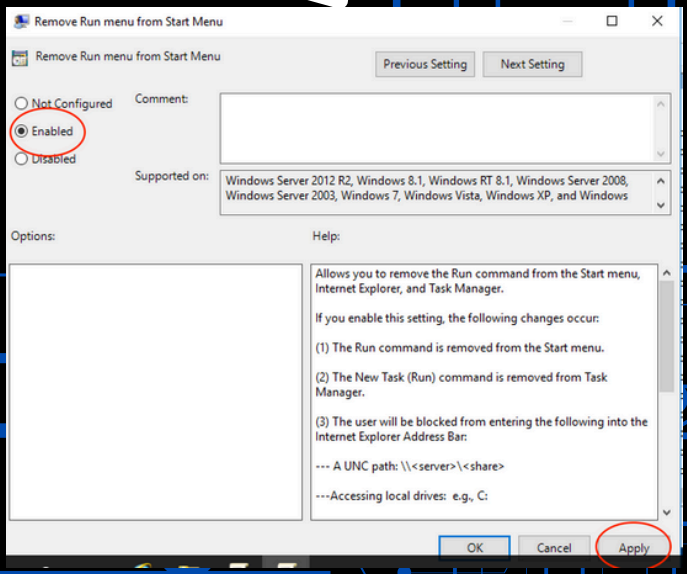
- Add script to the user's login to map the share you created.





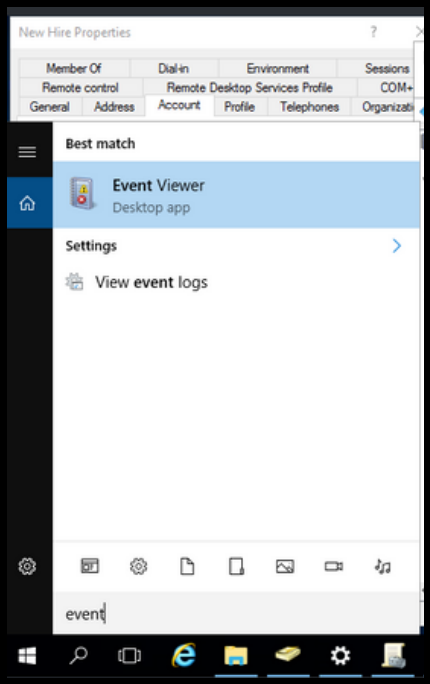
- Disable the run command from the start menu.

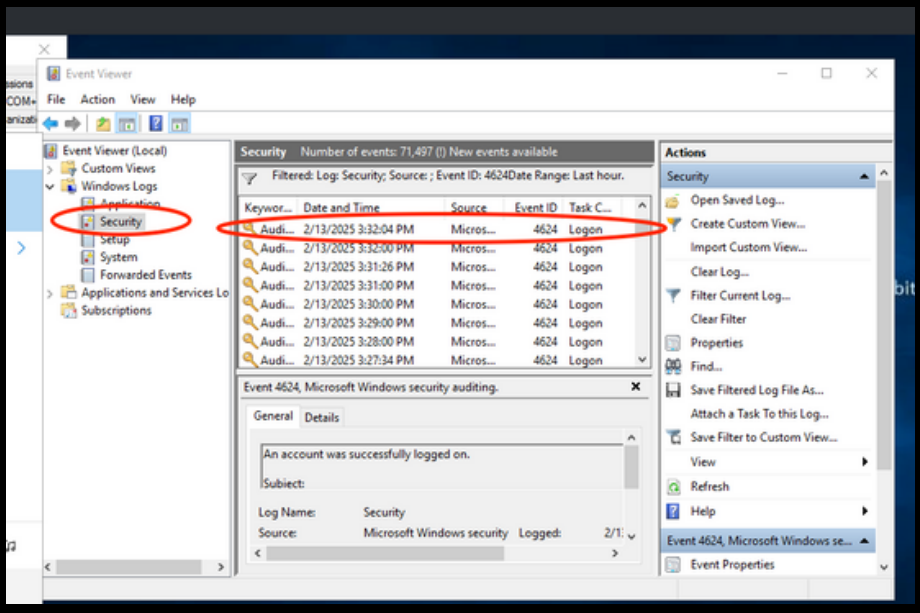


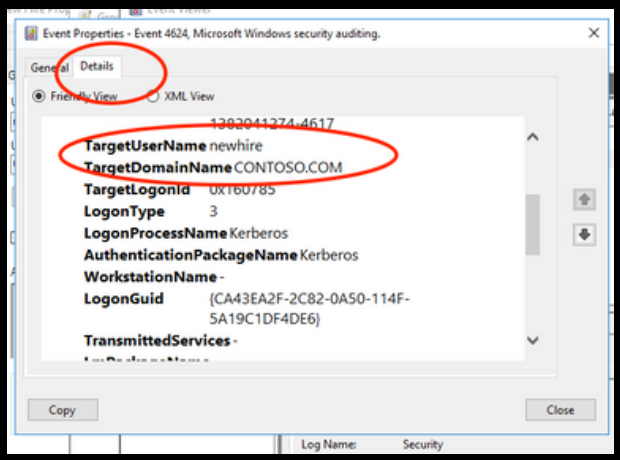


Step 7: Check Last Successful Login in Event Viewer

1. Open Event Viewer, then review the most recently installed programs.





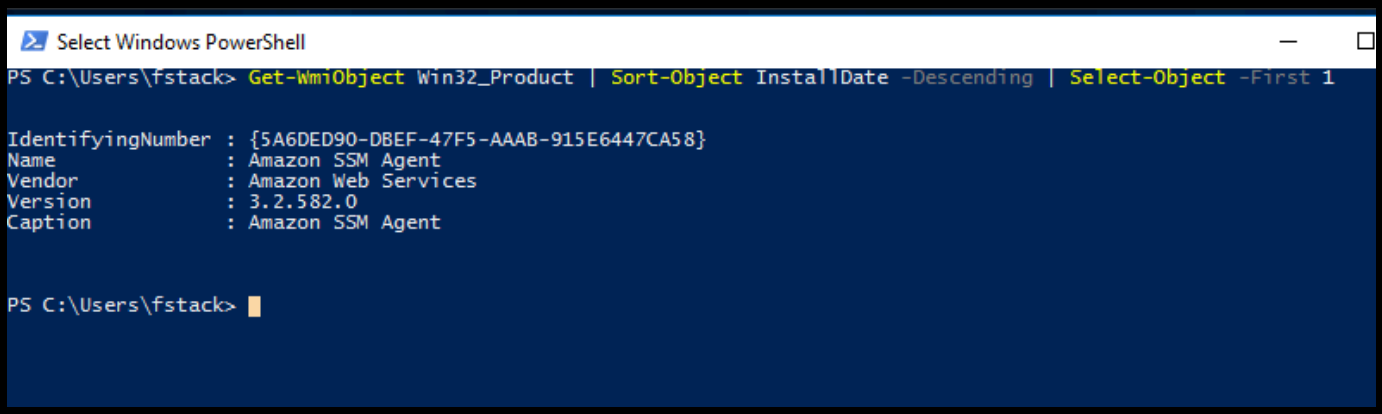


✅ Verification: Confirm the latest installed program is logged.

Step 8: Check Recently Installed Programs with PowerShell

1. Open PowerShell as Administrator & review the most recently installed programs.

2. Run the following command:
Get-WmiObject -Class Win32_Product | Sort-Object InstallDate | Select-Object -Last 5 | Format-Table Name, InstallDate



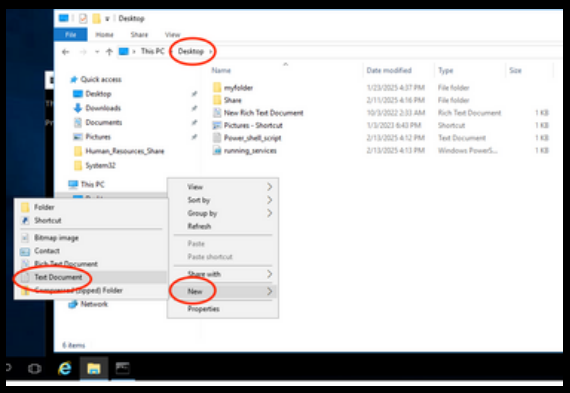
✅ Verification: Confirm the latest installed program is logged.

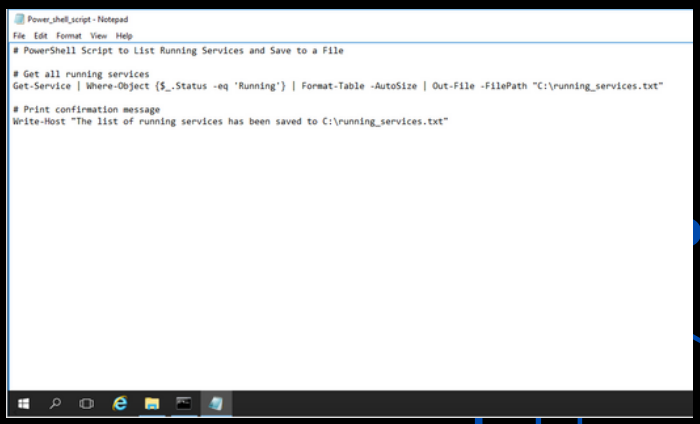
Step Step 9: PowerShell Script to List Running Services

Write a PowerShell script that gives a list of all running services and puts it in a file named running_services.txt.

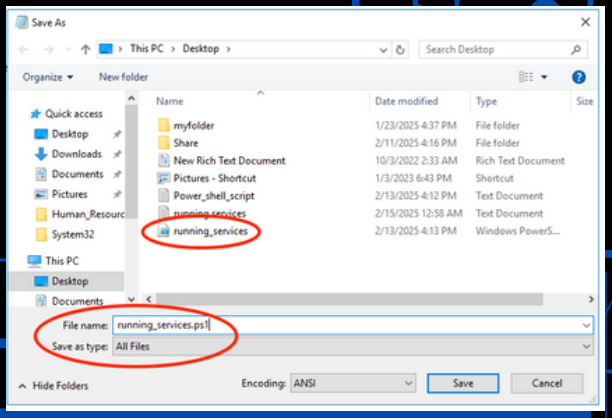
1. Open Notepad and paste the following script:

```
# PowerShell Script to List Running Services and Save to a File

# Get all running services
Get-Service | Where-Object {$_.Status -eq 'Running'} | Format-Table -AutoSize |
Out-File -FilePath "C:\running_services.txt"

# Print confirmation message
Write-Host "The list of running services has been saved to
C:\running_services.txt"
```

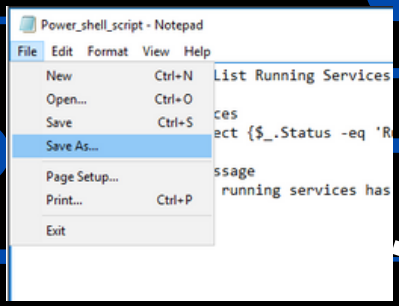




2. Save the Script as a .ps1 File
- Click File > Save As....
- In the Save As window:
- Choose a location (e.g., Desktop).
- Set File name: running_services.ps1
- Change Save as type: to All Files.



3. Click Save.



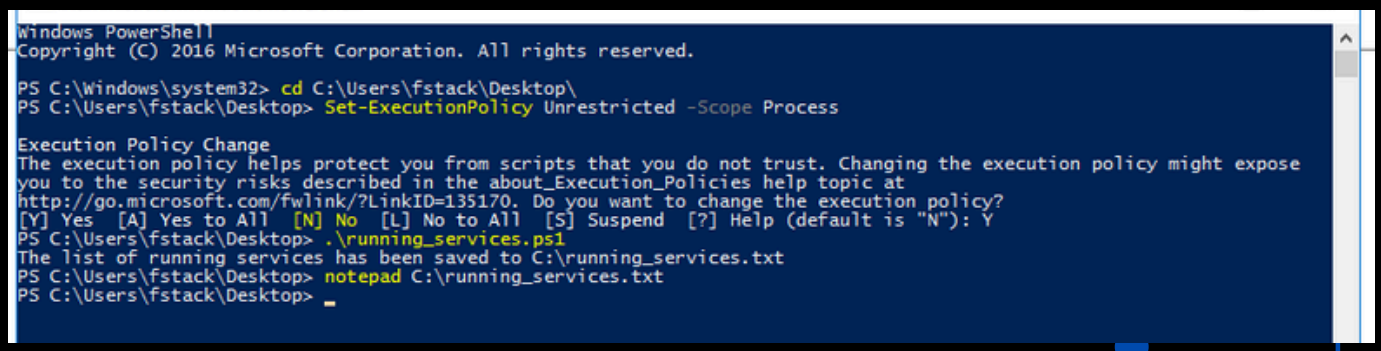
Step Step 9: Cont

Run the PowerShell Script
1. Open PowerShell as Administrator.

2. Navigate to the Desktop (or where you saved the script):
cd C:\Users\fstack\Desktop

3. Allow script execution (if required): Set-ExecutionPolicy Unrestricted -Scope Process

Type Y and press Enter if prompted.
4. Run the script:
.\running_services.ps1



4. Verify the Output File
Open File Explorer and navigate to C:\.
Locate and open running_services.txt.
It should immediately pop up once the command is run. It will look like the image on the right.