IT Onboarding Runbook (Windows AD)

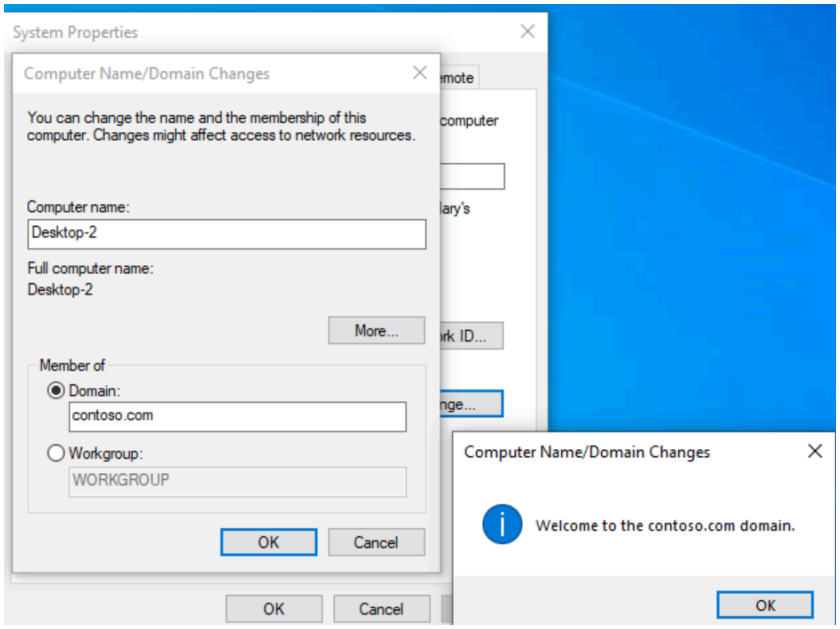
Introduction

This runbook documents the standardized process for onboarding a new hire's workstation into a Windows Active Directory environment. It covers domain integration, account setup, departmental resource configuration, Group Policy application, and verification tasks

---

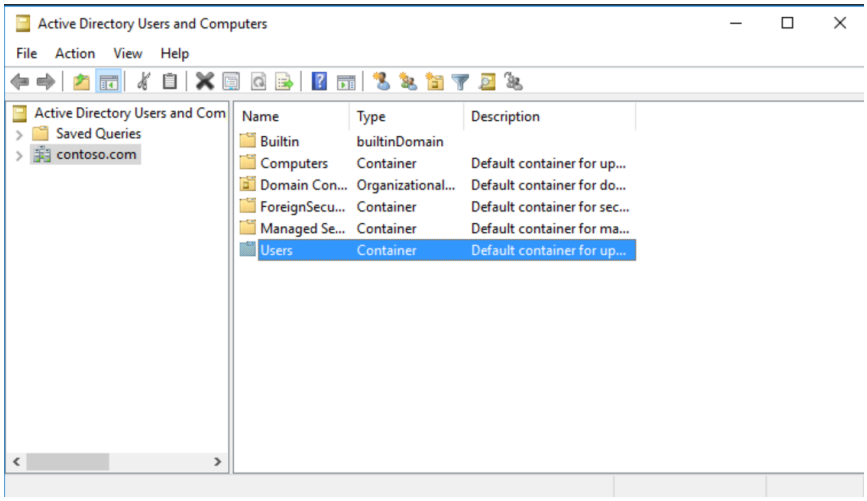
Step 1 – Join the Computer to the Domain

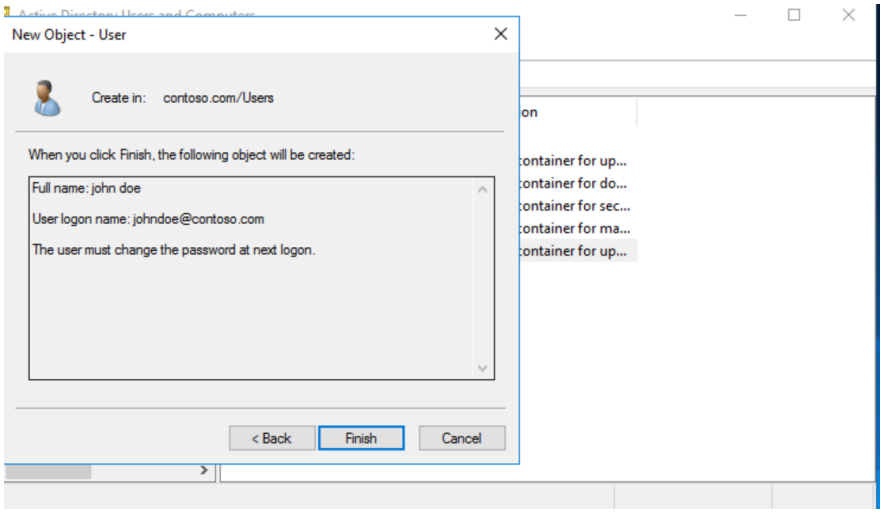
1. Log in to the workstation as a local administrator.
2. Go to **Settings → System → About → Rename this PC (Advanced)**.
3. Select **Member of domain**, type `contoso.com`, and click **OK**.
4. If an error says the domain controller cannot be contacted:
    - Go to **Control Panel → Network and Internet → Network Connections**.
    - Right-click your Ethernet adapter → **Properties** → select **Internet Protocol Version 4 (TCP/IPv4)**.
    - In the DNS server field, enter your domain controller's private IP (e.g., `192.168.1.10`).
5. Retry joining the domain, enter domain admin credentials, then reboot.



Step 2 – Create a New Hire User

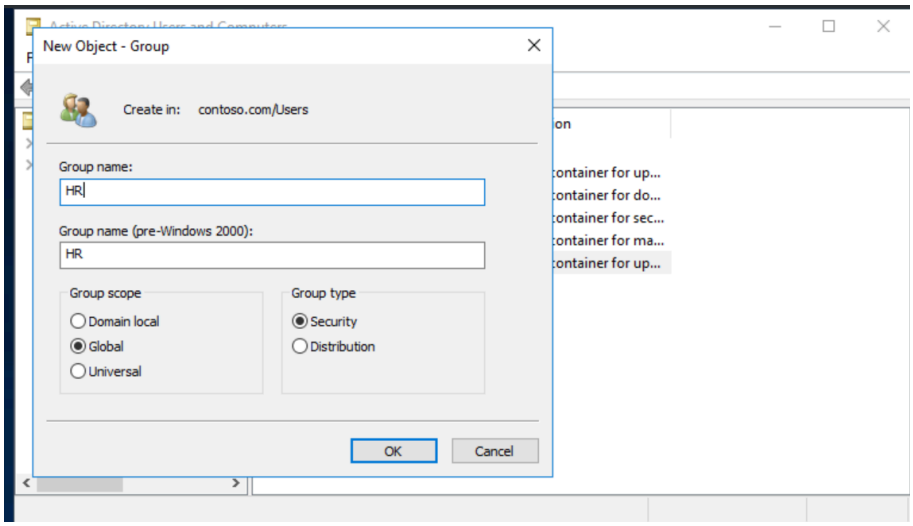
1. On the server, open **Active Directory Users and Computers (ADUC)**.
2. Select the **Users** container.
3. Right-click → **New** → **User**.
4. Enter first name, last name, and logon name.
5. Set a temporary password and check **User must change password at next logon**.
6. Click **Finish**.





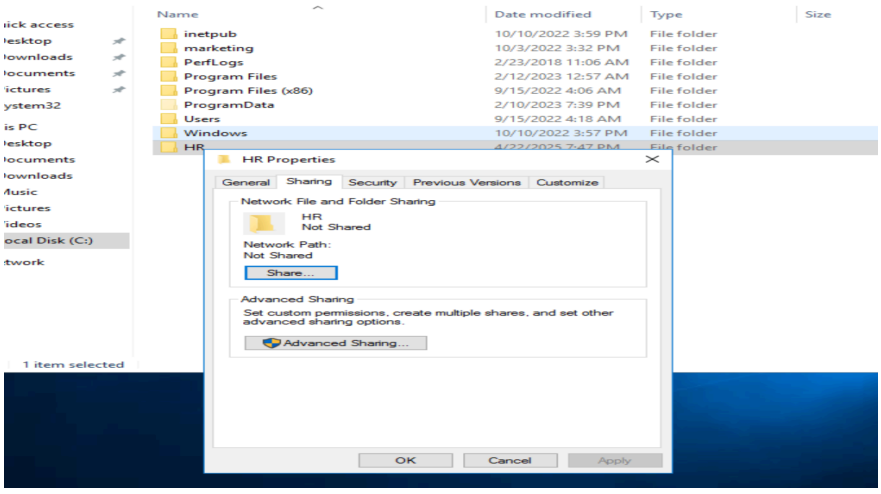
Step 3 – Create Department Group and Add User

1. In ADUC, right-click **Users** → **New** → **Group**.
2. Name it after the department (e.g., Sales).
3. Right-click the new hire's user → **Add to a group…** → enter the group name.



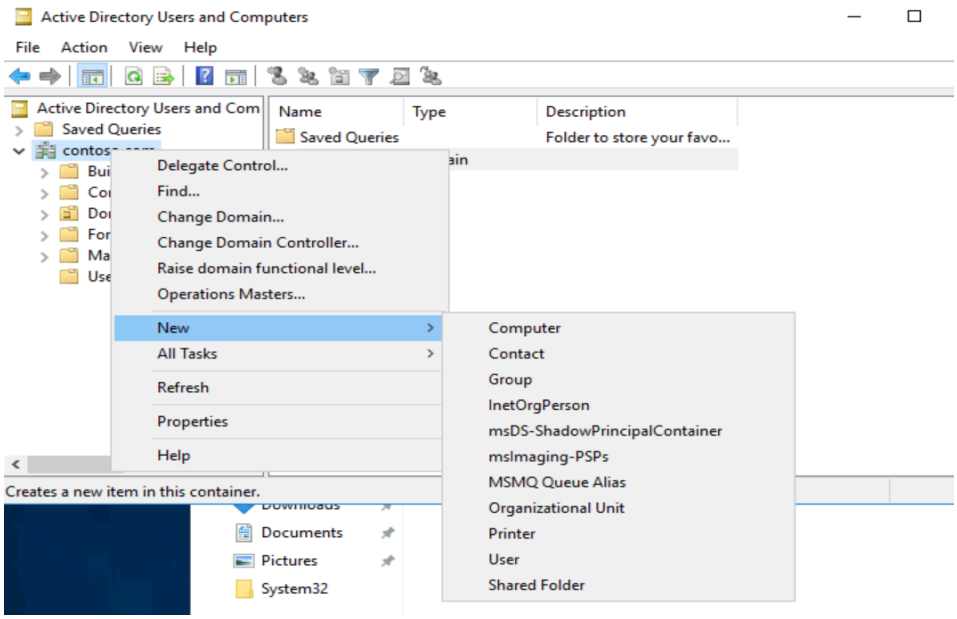
Step 4 – Create Departmental Share

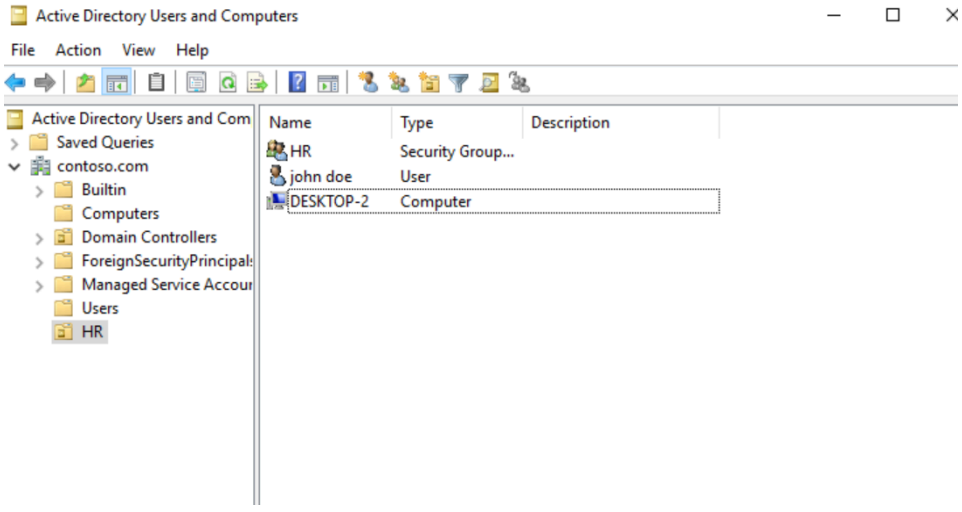
1. On the server, create `C:\Shares\Sales`.
2. Right-click folder → **Properties** → **Sharing** → **Advanced Sharing**.
3. Share with the department group (Allow: Read, Change).
4. In **Security** tab, grant the group **Modify**.
5. Create `test.txt` inside.



Step 5 – Create OU and Move Objects

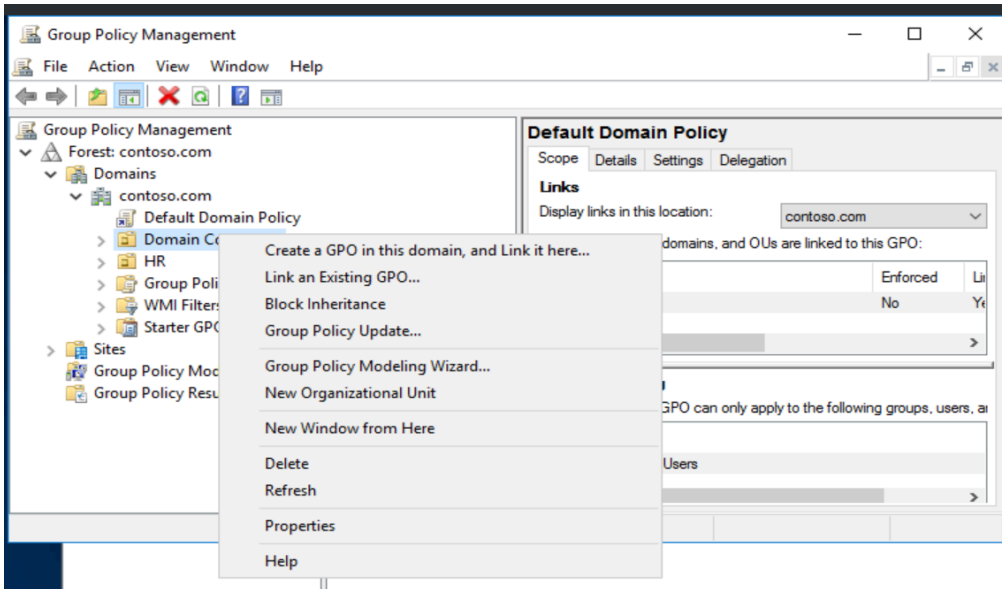
1. In ADUC, right-click domain root → **New** → **Organizational Unit** → name it after the department.
2. Move the new hire's user, group, and computer objects into the OU.



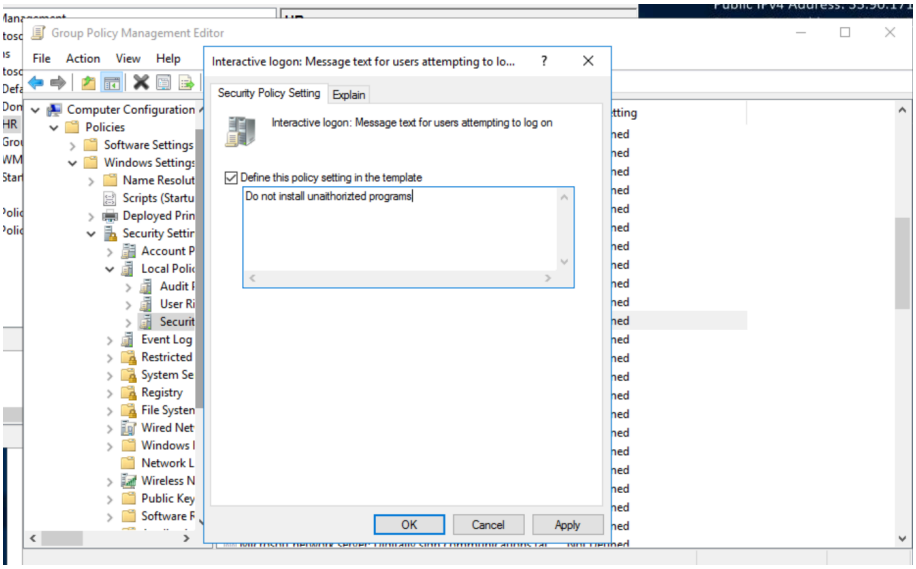


Step 6 – Apply GPO to OU

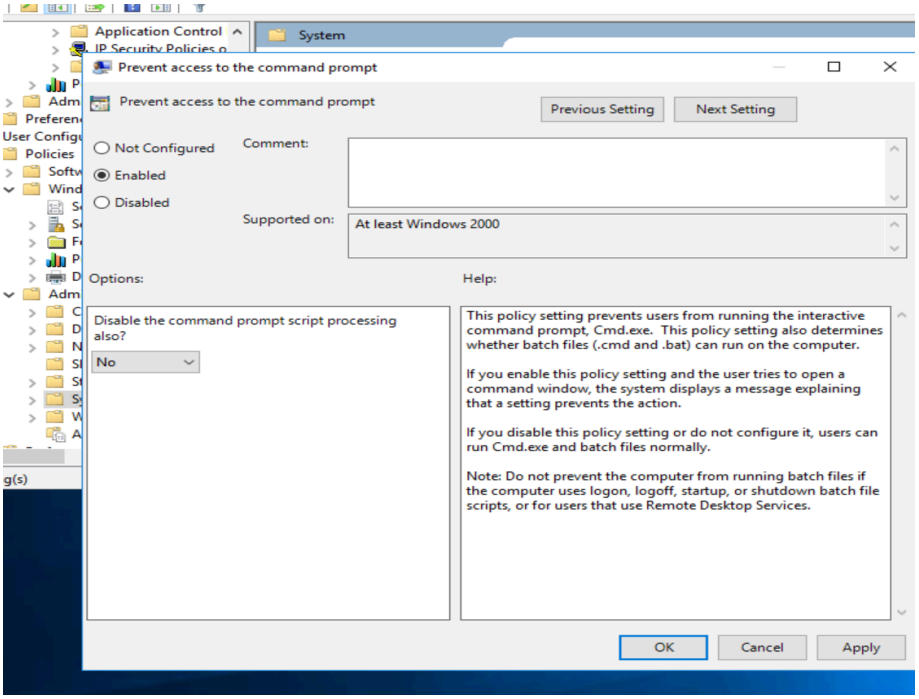
1. In **Group Policy Management**, create and link a new GPO to the OU.



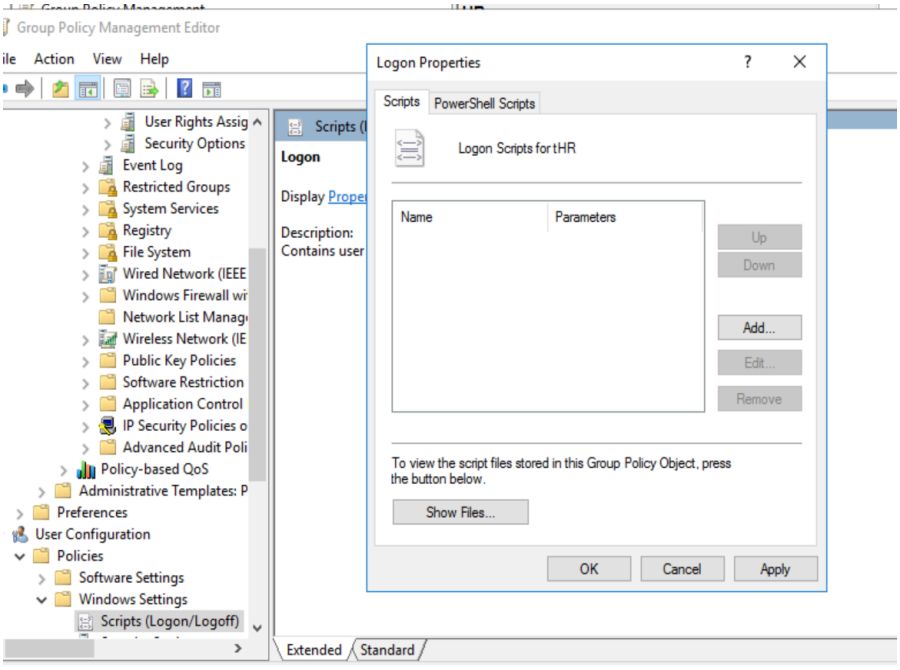
2. Edit the GPO to configure:
   - **Startup message**: Computer Config → Policies → Windows Settings → Security Settings → Local Policies → Security Options → set Interactive logon message.



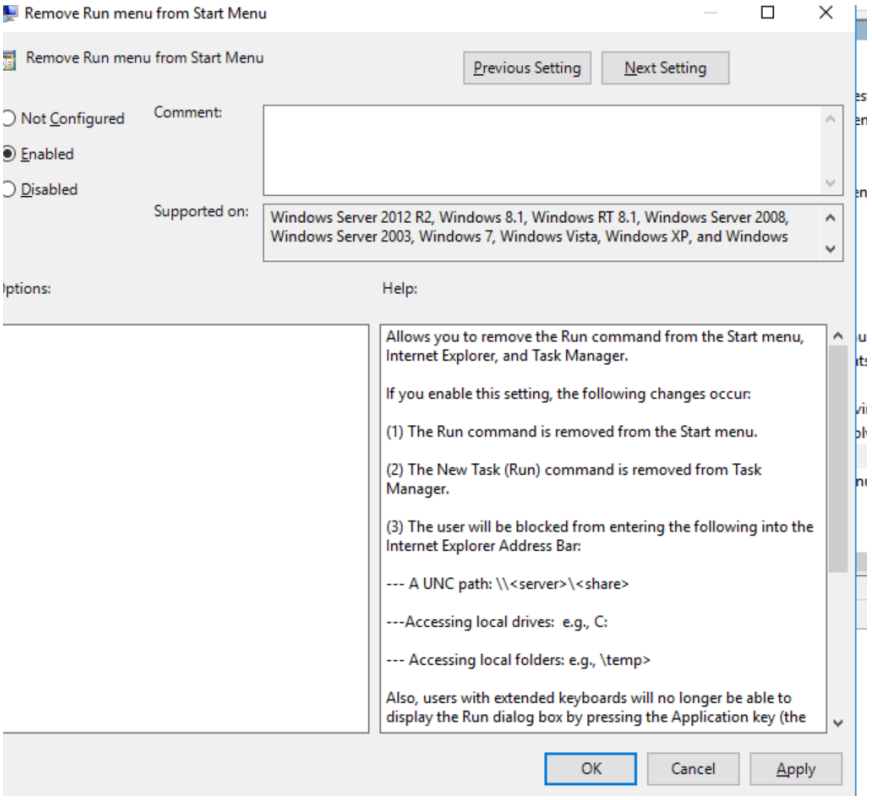
- **Disable Command Prompt**: User Config → Administrative Templates → System → Prevent access to the command prompt → Enabled.



- **Logon script**: User Config → Windows Settings → Scripts (Logon) → add `map-drive.bat`:
  net use S: \\SRV-FILE01\Sales /persistent:yes



- **Remove Run menu**: User Config → Administrative Templates → Start Menu and Taskbar → Remove Run menu from Start Menu → Enabled.

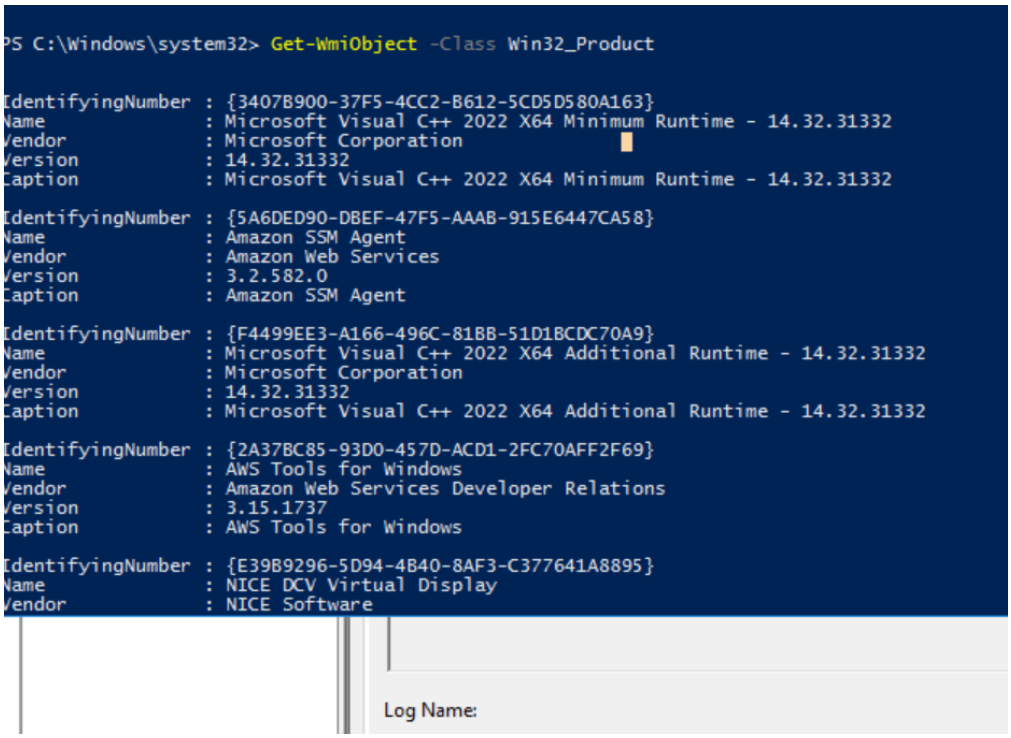


Step 7 – Verify Successful Logon

1. On the server, open **Event Viewer** → **Windows Logs** → **Security**.
2. Filter for **Event ID 4624** and the new hire's username.
3. Confirm logon type and timestamp.

Step 8 – Check Latest Installed Program

1. On the workstation, open **PowerShell**.
2. Run:
   Get-WmiObject Win32_Product | Sort-Object InstallDate -Descending | Select-Object -First 1
3. Review the output for the most recent installation.



Step 9 – Export Running Services

1. On the workstation, open **PowerShell**.
2. Run:
   Get-Service | Where-Object {$_.Status -eq 'Running'} | Out-File C:\Temp\running_services.txt
3. Check `C:\Temp\running_services.txt` for the list of running services.