

Your Company

By Edvin Morales
Your City, ST 12345
(123) 456 - 7890

Onboarding New Hires

September 04, 2024

Overview

This is a standard onboarding for a new hire. Add new hires names and also roles in the company and a department . Join the new hires computer to the company domain . Create a group of the department with the user . Set up a GPO for your new group and make sure only authorized users are allowed only. A message should appear for all employees (Do not install unauthorized programs) also the run command should be disabled from the start. Check an event viewer for the last successful login .

Add new hire

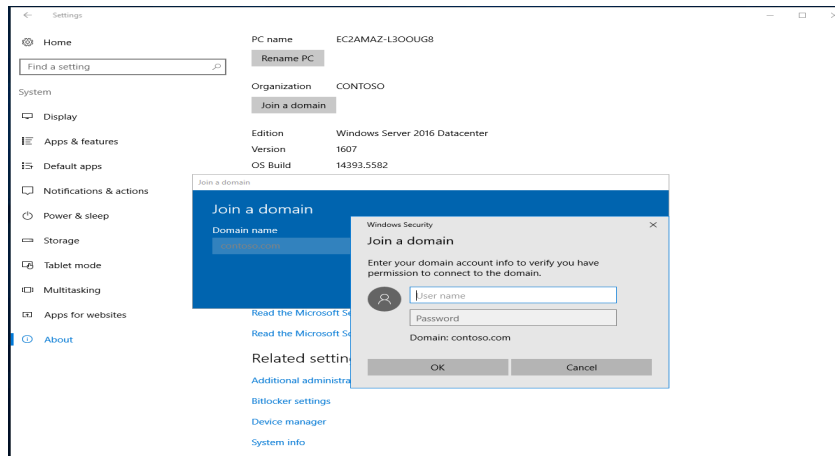
Add the new hire username and password form the gui or windows power shell. Join the new hire to the current domain . **Join the Computer to the Domain**

1. Open System Properties:

- Press **Windows + Pause/Break** or right-click on **This PC** and select **Properties**.
- Click on **Advanced system settings**.

2. Join the Domain:

- Under the **Computer Name** tab, click on **Change**.
- Select the **Domain** option and enter **contoso.com**.
- When prompted, enter the domain credentials: **administrator** as the username and **Pa\$\$w0rd** as the password.
- Restart the computer to apply the changes.



Make a group

Make a group with the department's name and place it with the user in the group. Tool can be accessed in the admin folder. **Create an OU and Place Objects in It**

1. Create an OU:

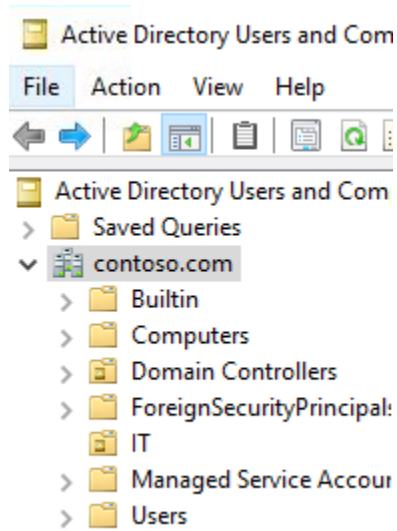
- In ADUC, right-click on the domain root (e.g., [contoso.com](#)) and select **New > Organizational Unit**.
- Name the OU after the department.

2. Move Objects into the OU:

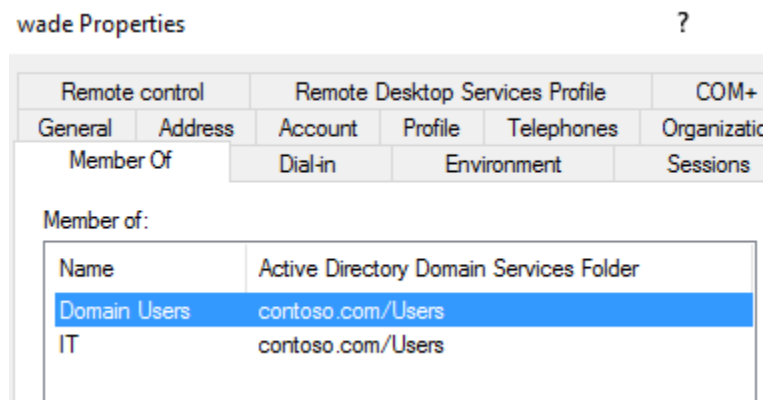
- Drag and drop the user, group, and computer into the new OU.

3. Attach a GPO to the OU:

- Open the Group Policy Management Console (GPMC).
- Right-click on the new OU and select **Create a GPO in this domain, and Link it here**.
- Name the GPO appropriately.



Connect to server



Message pop up

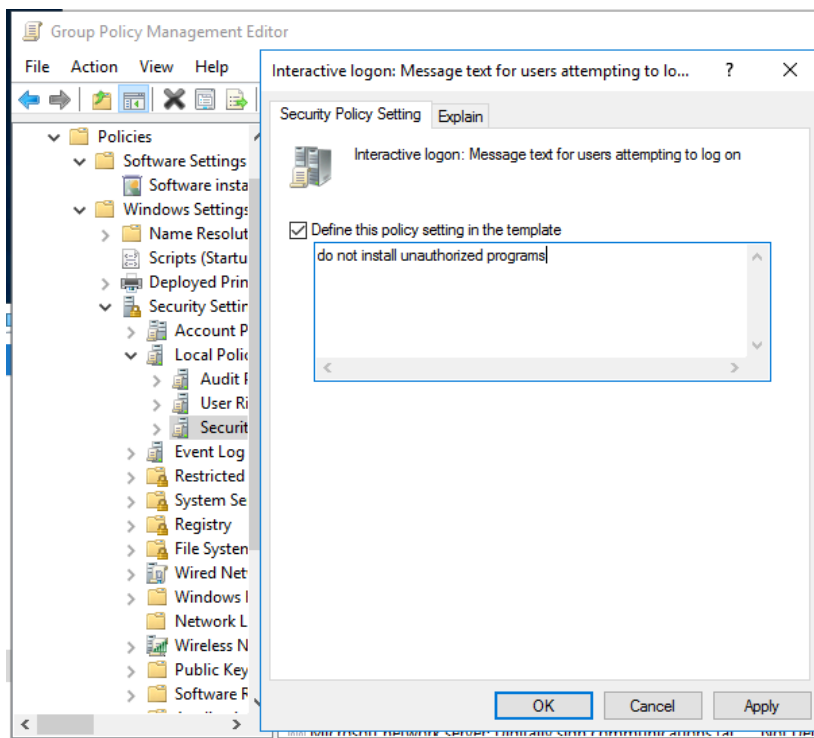
Go to GPO and add the message that pops up on login. Have to use the GPManager go to window settings and under windows settings and enable the message pop up. **Step 6: Edit the GPO with Specific Rules**

1. **Open Group Policy Management Editor:**

- Right-click the newly created GPO and select **Edit**.

2. **Configure a Startup Message:**

- Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**.
- Configure **Interactive logon: Message text for users attempting to log on** and **Interactive logon: Message title for users attempting to log on**.



Server Share

Share a folder server side with the new hire and only people who belong with read and write permissions

1. Create a Shared Folder:

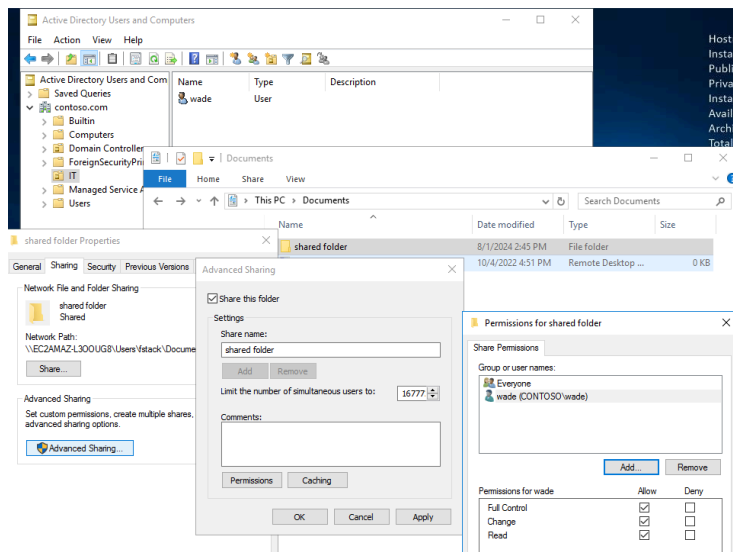
- On the server, create a new folder with the department name.
- Right-click on the folder and select **Properties**.
- Go to the **Sharing** tab and click **Advanced Sharing**.
- Check **Share this folder** and give it a share name.

2. Set Permissions:

- Click on **Permissions**.
- Remove **Everyone** and add the group you created in Step 3.
- Set the group's permissions to **Read** and **Write**.

3. Create a Test File:

- In the shared folder, create a text document named **test.txt**.

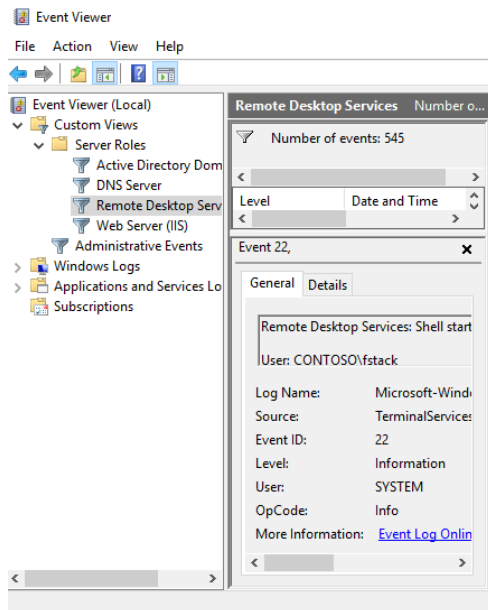


Look at the event finder

Make sure your domain is connected to your event finder to check for the last successful login

Check Event Viewer for Last Successful Login

1. **Open Event Viewer:**
 - On the server, open Event Viewer ([eventvwr.msc](#)).
2. **Navigate to Security Logs:**
 - Expand [Windows Logs](#) and select [Security](#).
3. **Filter and Find Last Successful Login:**
 - Use the [Filter Current Log](#) option to filter by Event ID [4624](#) (successful login).
 - Note the details of the last successful login for your user.



Install Checker

Check the Latest Installed Program with PowerShell

1. Open PowerShell:

- On the computer, open PowerShell as an administrator.

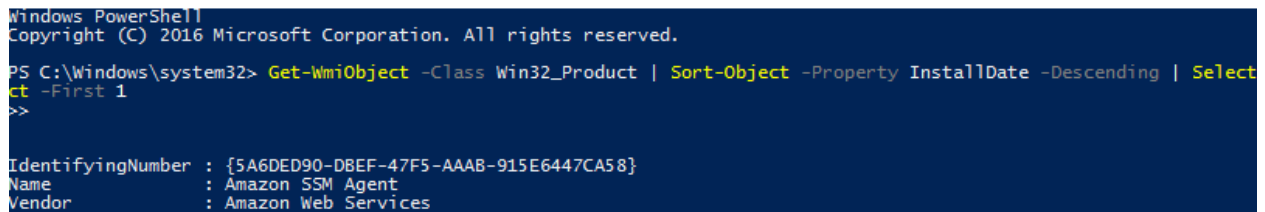
2. Check the Latest Installed Program:

- Run the following command to get the latest installed program:

powershell

Copy code

```
Get-WmiObject -Class Win32_Product | Sort-Object -Property InstallDate  
-Descending | Select-0
```



```
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
  
PS C:\Windows\system32> Get-WmiObject -Class Win32_Product | Sort-Object -Property InstallDate -Descending | Select-Object -First 1  
>>  
  
IdentifyingNumber : {5A6DED90-DBEF-47F5-AAAB-915E6447CA58}  
Name               : Amazon SSM Agent  
Vendor             : Amazon Web Services
```

PowerShell Script to List Running Services

1. Create the PowerShell Script:

Open a text editor and write the following script:

powershell

Copy code

```
Get-Service | Out-File -FilePath C:\running_services.txt
```

- Save the script with a `.ps1` extension.

2. Run the Script:

- Open PowerShell as an administrator and execute the script:

powershell

Copy code
`.\path\to\your\script.ps1`

Overview

Congratulations on successfully adding a new hire to the company domain! This runbook has guided you through the essential steps to ensure that the new employee is integrated into our network securely and efficiently. Below is a summary of the key actions performed and important points to remember.

Summary of Actions Performed

1. **Join Computer to the Domain:**
 - Joined the new hire's computer to the company domain (contoso.com) using the credentials provided.
2. **User Account Creation:**
 - Created a new user account for the new hire and set a secure initial password.
3. **Group Assignment:**
 - Created a department-specific group and added the new hire to this group for appropriate access rights.
4. **Shared Resources Configuration:**
 - Set up a department-specific shared folder and configured permissions to ensure only authorized users have read and write access.
 - Created a test document (test.txt) in the shared folder to verify access.
5. **Organizational Unit (OU) Setup:**
 - Created an Organizational Unit (OU) for the department.
 - Moved the new user account, department group, and computer object into the new OU.
 - Linked a Group Policy Object (GPO) to the OU.
6. **Group Policy Configuration:**
 - Configured GPO settings to:

- Display a startup message warning against unauthorized software installation.
- Prevent access to the Command Prompt (CMD).
- Add a login script to map the shared folder.
- Disable the Run command from the Start menu.

7. Event Viewer Check:

- Verified the last successful login of the new user using Event Viewer on the server.

8. PowerShell Operations:

- Used PowerShell to check the latest installed program on the new hire's computer.
- Wrote a PowerShell script to list all running services and saved it to running_services.txt.

Key Points to Remember

- **Security:** Ensure that all security policies and procedures are followed to maintain the integrity and security of the company domain.
- **Documentation:** Document any deviations or specific configurations made during the setup for future reference.
- **Support:** Provide the new hire with necessary support and resources to get acquainted with their system and access rights.
- **Monitoring:** Regularly monitor user activities and access rights to ensure compliance with company policies.

Next Steps

- **Ongoing Support:** Check in with the new hire to ensure they have access to all required resources and address any issues they might face.
- **Training:** Encourage the new hire to participate in IT security and domain usage training.
- **Feedback:** Gather feedback from the new hire regarding the setup process to identify areas for improvement.

Final Thoughts

Adding a new hire to the company domain is a crucial task that ensures they have the necessary access to perform their job functions while maintaining the security and integrity of our network. By following this runbook, you have ensured a smooth and secure integration for the new employee.

Thank you for your diligence and attention to detail throughout this process. Your efforts contribute significantly to the seamless onboarding experience and the overall security posture of our organization.