Reza Nosrati
Alexander Rick Topacio & Alex Gordon
Career Simulation 2
12/21/2024

New Hire Runbook

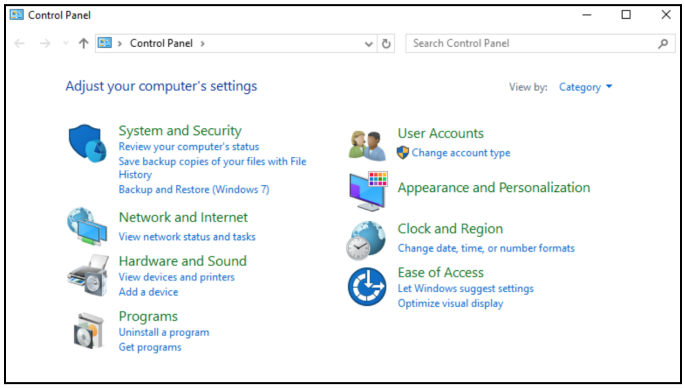
Introduction

This runbook will provide a step-by-step guide on how to set up a machine for a new hire at StackFull Software. Your tasks will consist of joining the computer to the domain, creating new users, groups, organizational units and attaching group policies among other related tasks.

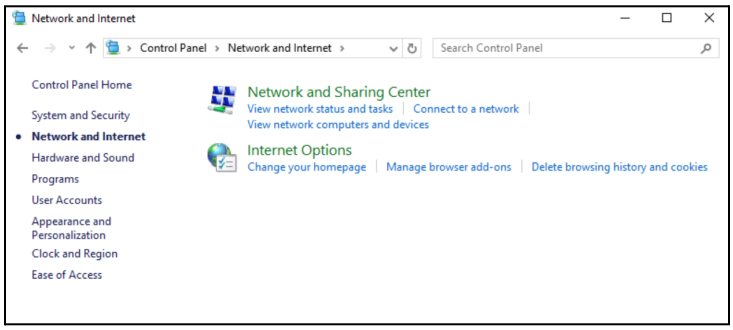
Step 1

Join the computer to the domain (the domain name is contoso.com). The username/password is administrator/PaSSw0rd. Network internet connections

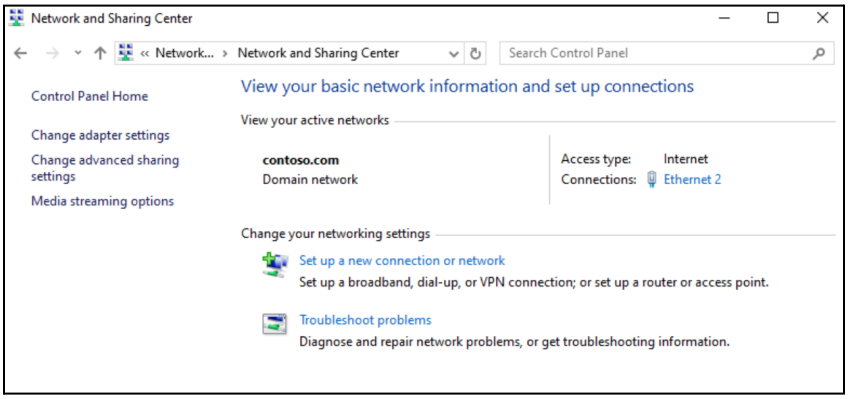
1. Open the Control Panel.



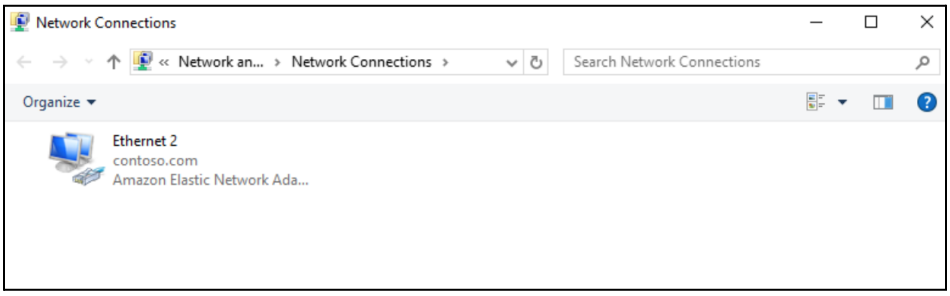
2. Click ‘Network and Internet.’



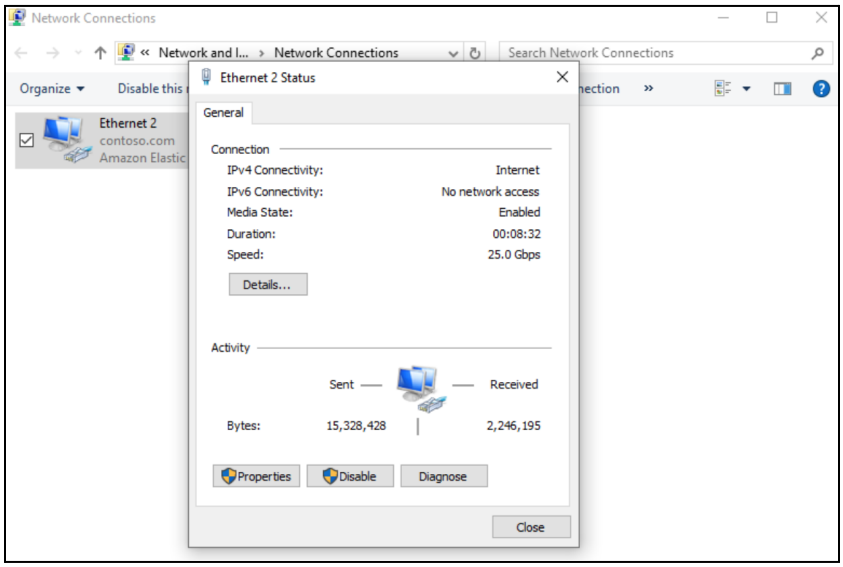
3. Click ‘Network and Sharing Center.’



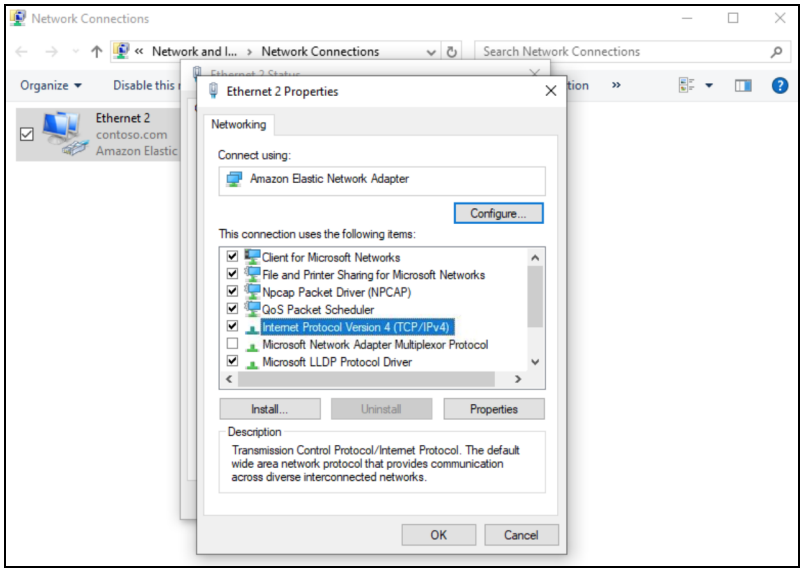
4. Click ‘Change adapter settings.’



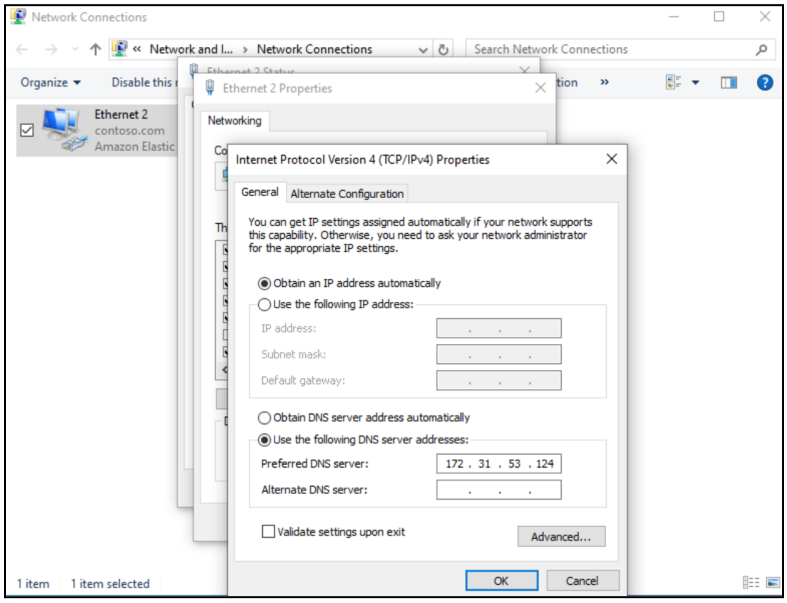
5. Double-click ‘Ethernet2.’



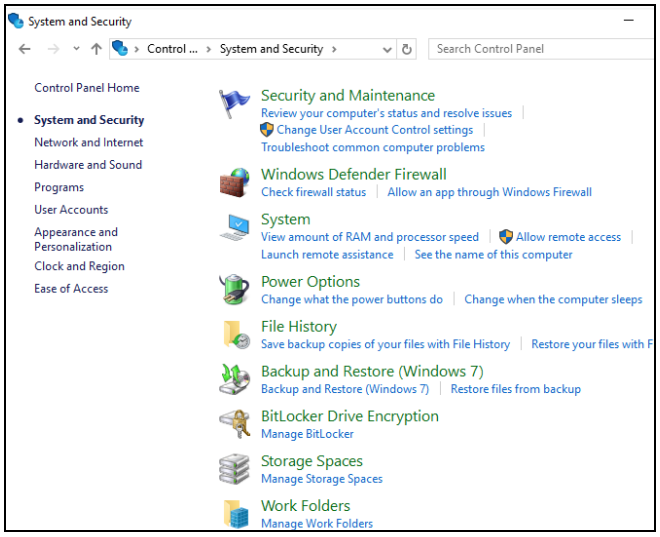
6. Click ‘Properties.’



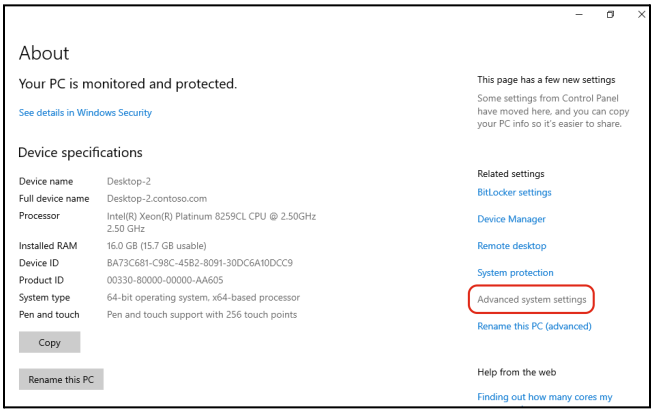
7. Click ‘Internet Protocol Version 4 (TCP/IPv4).’



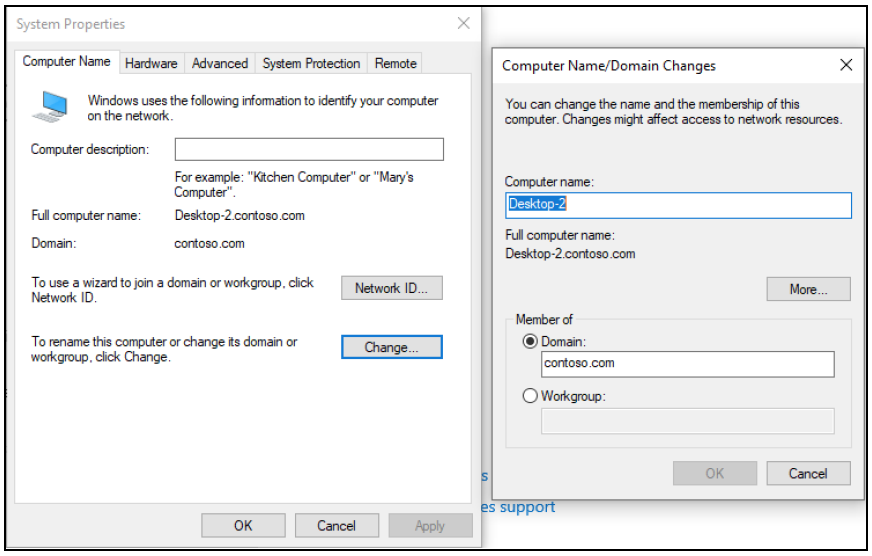
8. Enter the server’s Private IP in the “Preferred DNS server:” box (in this case: 172.31.53.124) and click “OK” to confirm changes.
9. Go back to the ‘Control Panel’ and click ‘System and Security.’



10. Now click “System,” this will bring you a new window that has “About” at the top of the page. Look under ‘Related settings’ and click ‘Advanced system settings’ (circled in red).



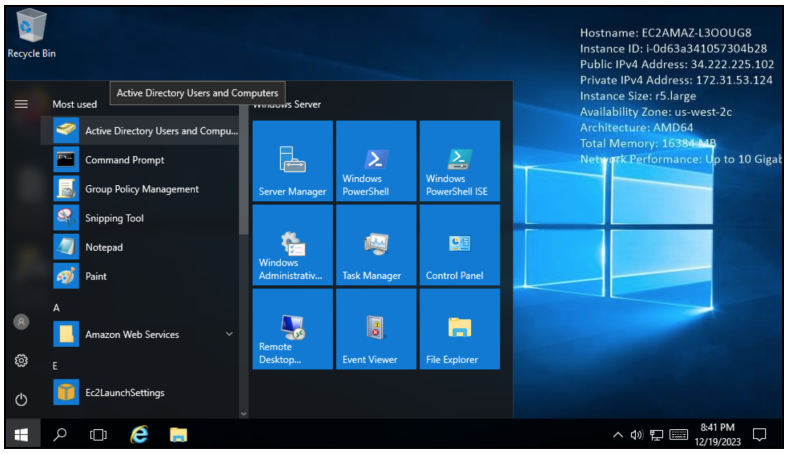
11. This will open up a new window that is titled ‘System Properties.’ Click the ‘Computer Name’ tab and then click the ‘Change…’ button. This will open another window called ‘Computer Name/Domain Changes’ and you will enter “contoso.com” in the empty box that says: “Domain:” under ‘Member of’, as seen below. Click “Ok” and then “Ok” again to confirm all changes.



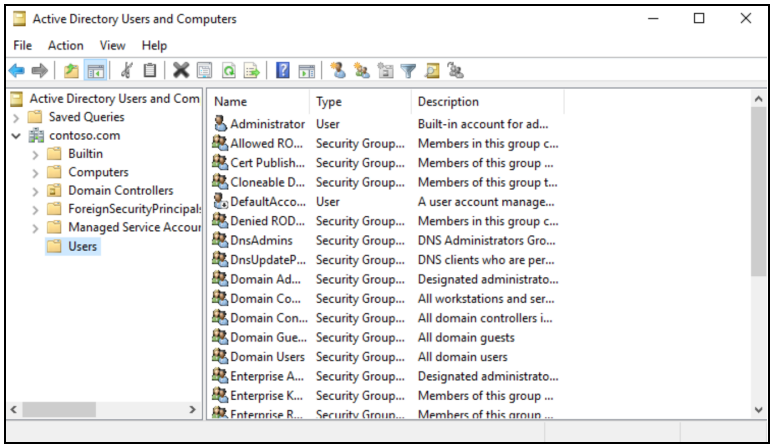
Step 2

Switch to the server. Create a user for the new hire and set a password.

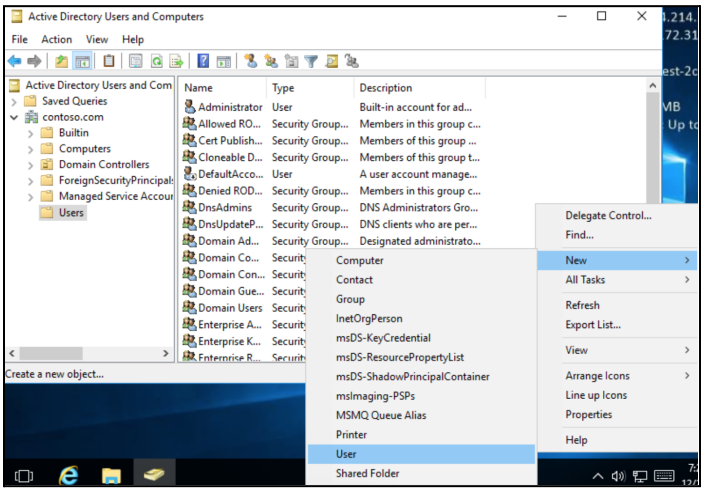
1. Switch to the server and search for ‘Active Directory Users and Computers’ in Windows search box and click it open.



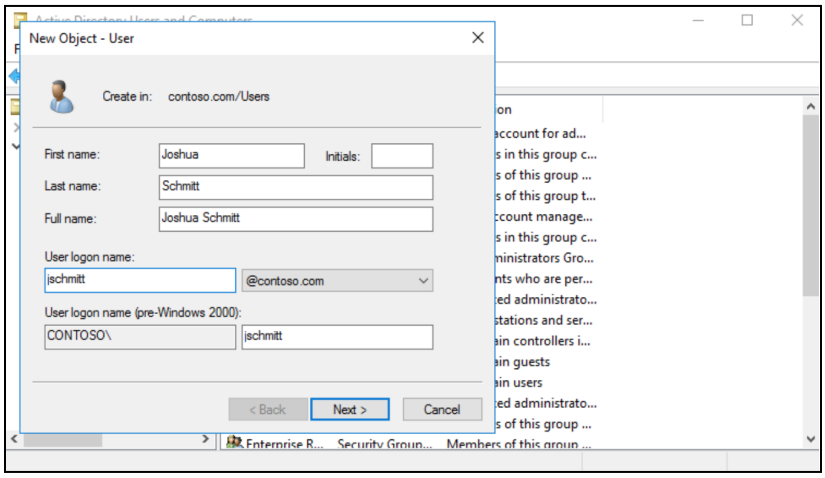
2. Click into ‘Users’ Folder on the left hand side under ‘contoso.com.’



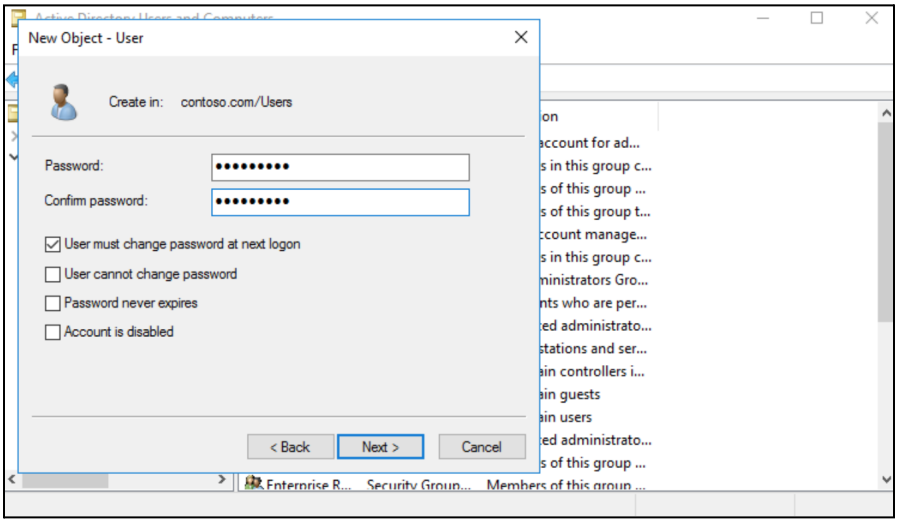
3. Right click in the white space and navigate to ‘New’ then ‘User.’



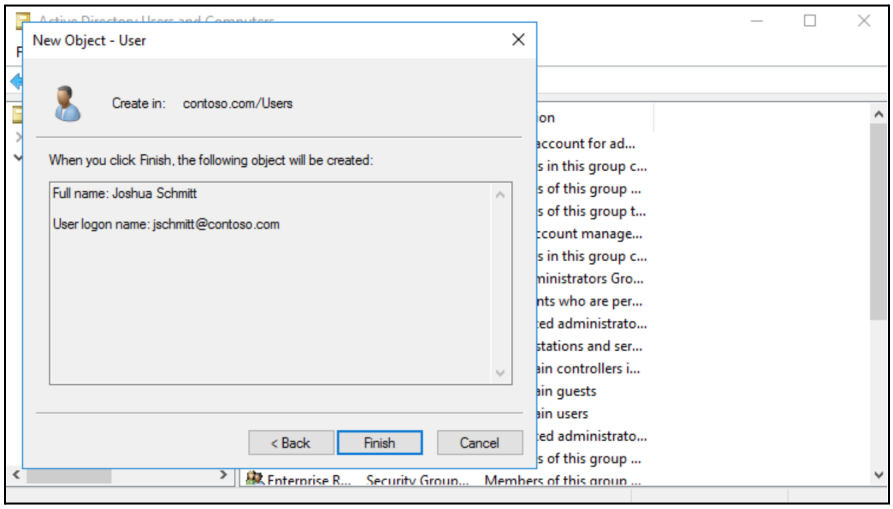
4. Enter in boxes “First name:”, “Last name:” & “User logon name:” (in this case “Joshua Schmitt”, with username jschmitt)



5. Click ‘Next>’ and enter a password in the boxes “Password:” and “Confirm password:” (in this case password1 entered). Keep the “User must change password at next logon” box checked so that the user can change when they logon.



6. Click ‘Next>’ and confirm what you entered is correct.

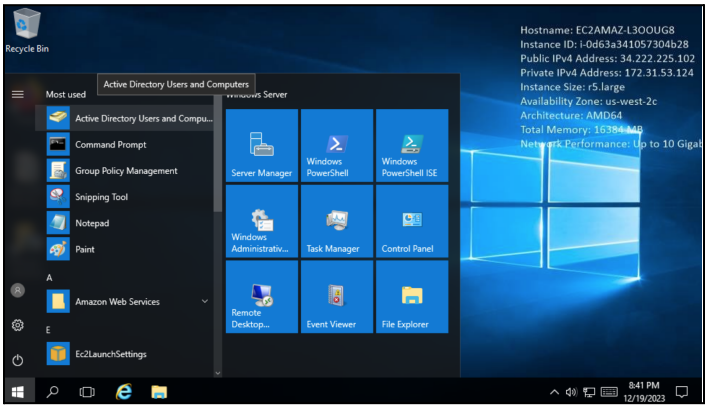


7. Then click ‘Finish,’ to confirm changes.

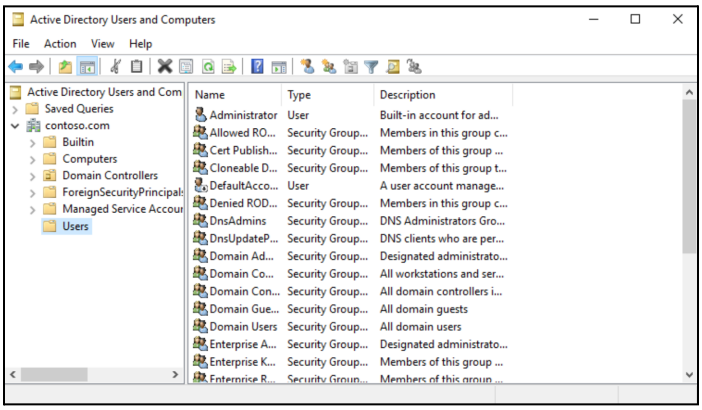
Step 3

Create a group with the department name and place the user in that group.

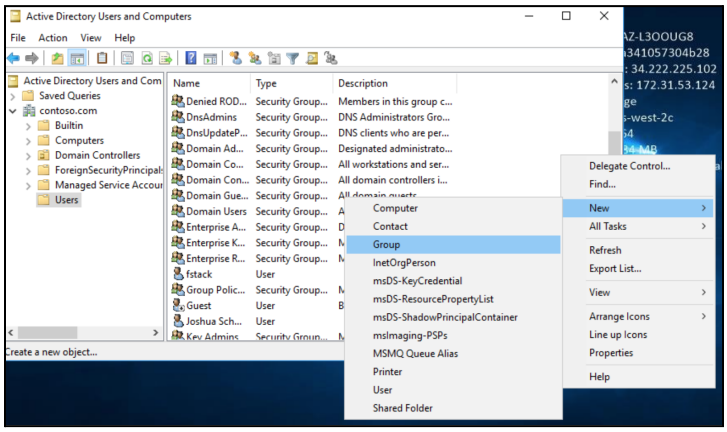
1. Search for ‘Active Directory Users and Computers’ in the Windows search box and click it open.



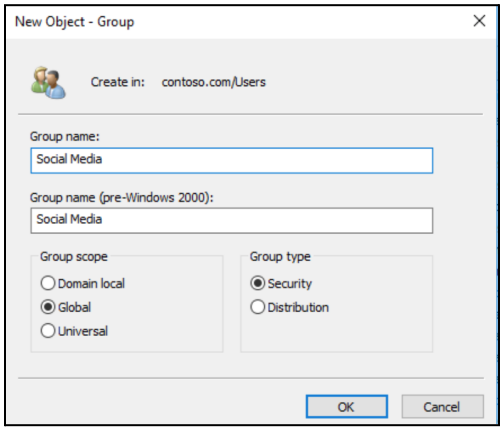
2. Click into ‘Users’ Folder on the left hand side under ‘contoso.com.’



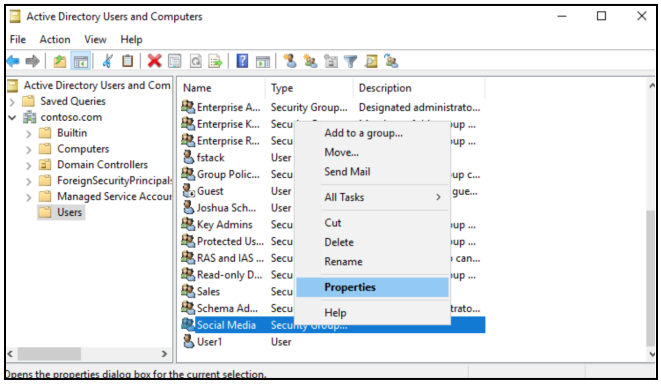
3. Right click on the empty white space once in the folder and navigate to ‘New’ then ‘Group.’



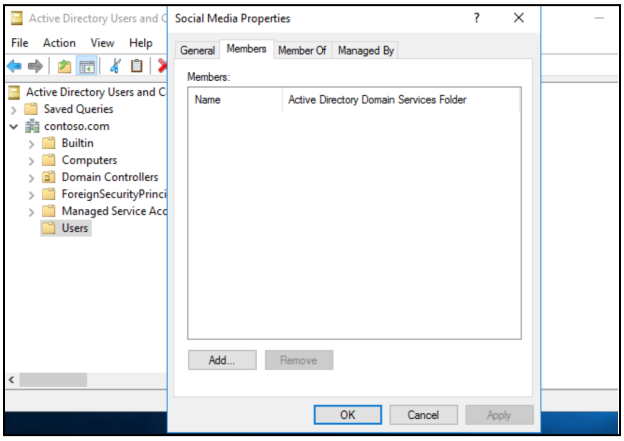
4. Enter the group name in the ‘Group name:’ box (in this instance Social Media). Click “OK” to confirm.



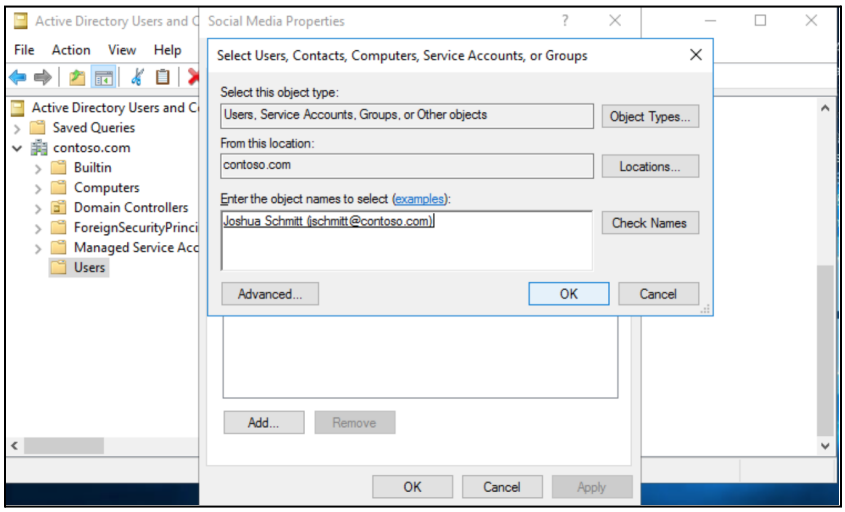
5. Right click on the newly created group (in this case “Social Media”) and click ‘Properties.’



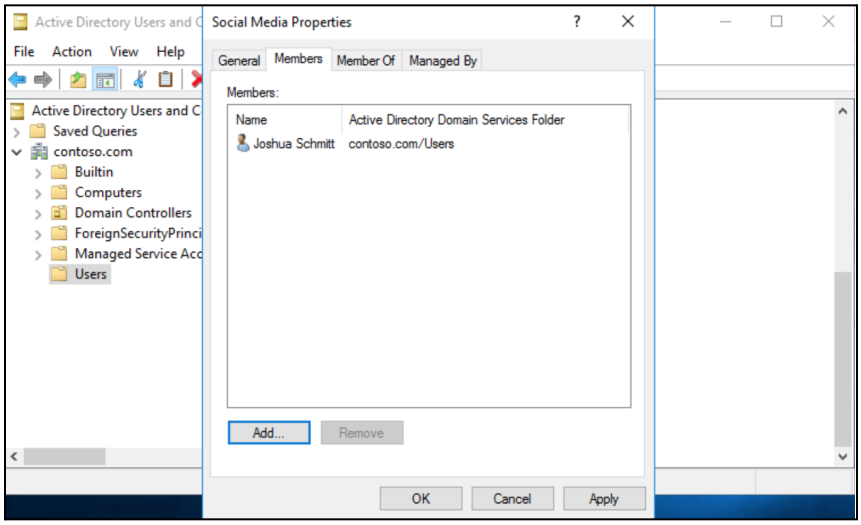
6. Click the ‘Members’ Tab and then the ‘Add…’ button.



7. In the box that says “Enter the object names to select:” enter the user you just created (in this instance ‘jschmitt’). Once entered you can click the ‘Check Names’ box to the right, which will check the (user/)name you entered and if done correctly you will see the user you created and click that. It will change and underline the official wording for the user in the box as seen below. Once finished press the “OK” button to add and confirm changes.



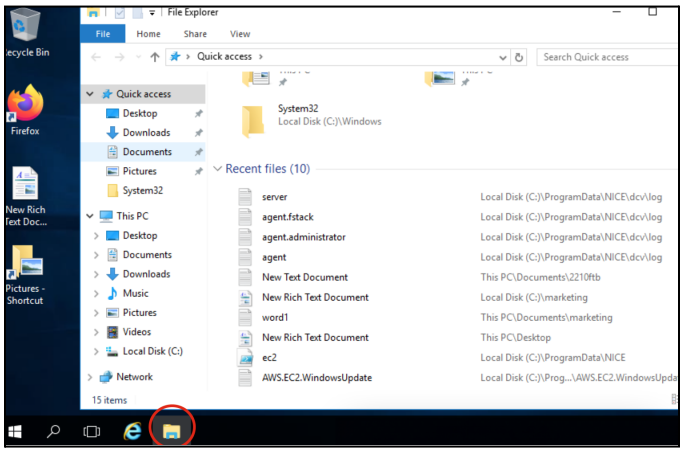
8. You should now see the user in the ‘Properties’ window. Click “OK” to end and confirm settings.



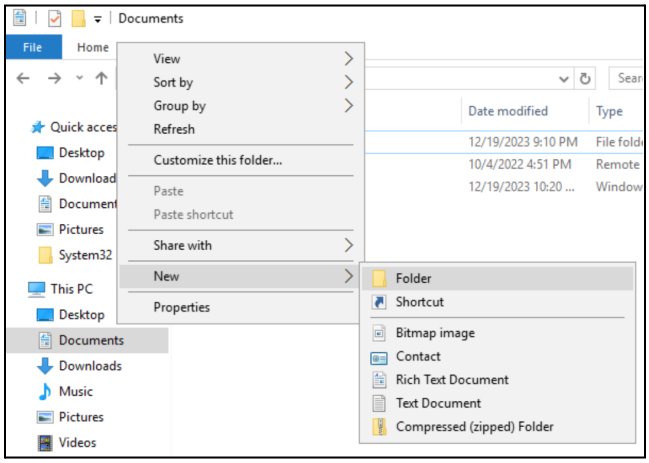
Step 4

Create a share on the server with the department name and share it only with people who belong to that department (read and write permissions). In the folder, create a text document called test.txt.

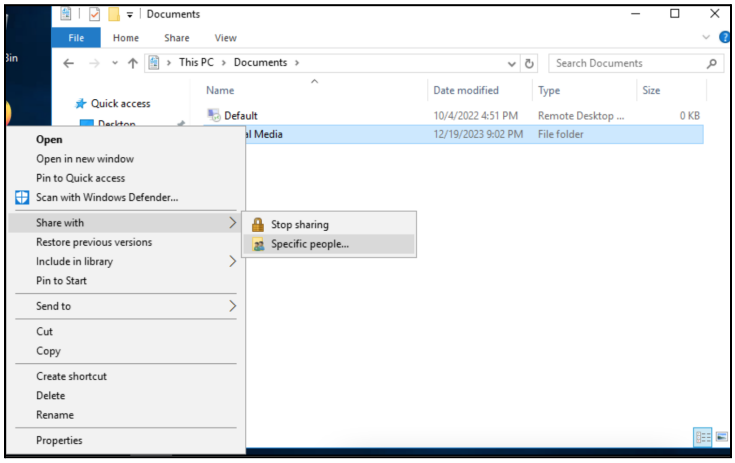
1. Click the file Explorer icon (circled in red below).



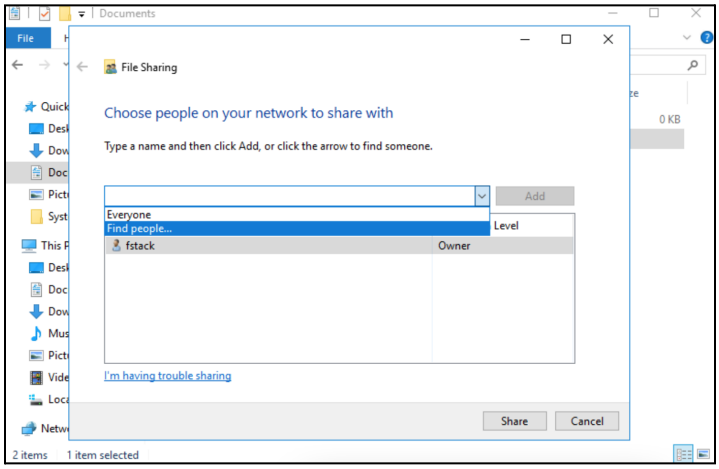
2. Once the window is open, click into ‘Documents’ on the left hand side. Right click in the empty white space in the ‘Documents’ folder and navigate to ‘New’ and then ‘Folder’. Enter the Departments name as the title for the folder (in this case Social Media).



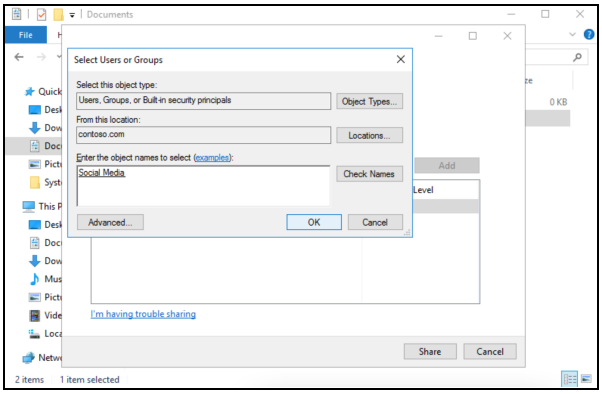
3. Now right click the folder you just created and navigate to “Share with” then “Specific people…”



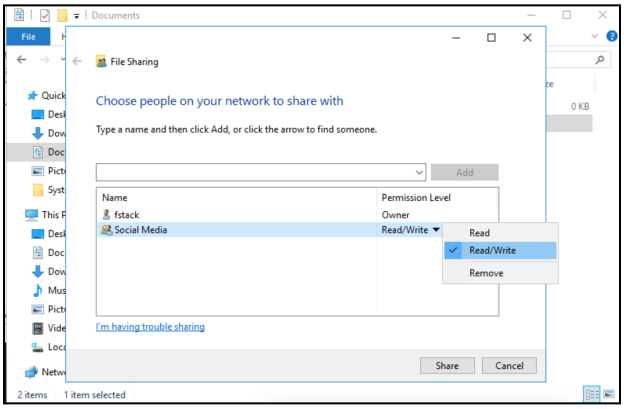
4. And then press “Find people…” in the drop down box next to ‘Add’.



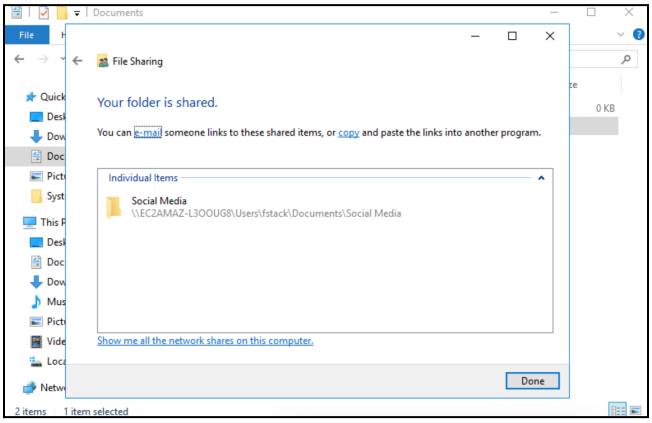
5. Type in the group name you want to share with, (in this case “Social media”) in the “Enter the object names to the select” box. Once entered you can click the “Check Names” box to the right, which will check the group you entered and if done correctly you will see the group you created and click that. It will change and underline the official wording for the group in the box as seen below. Once finished press the “OK” button to add and confirm changes.



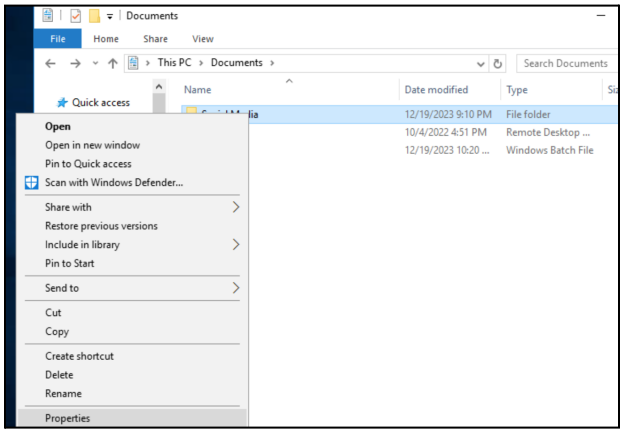
6. Now add the permissions of read and write to the group by selecting "Read/Write" in the drop down bar under "Permission Level." Click the 'Share' button once done.



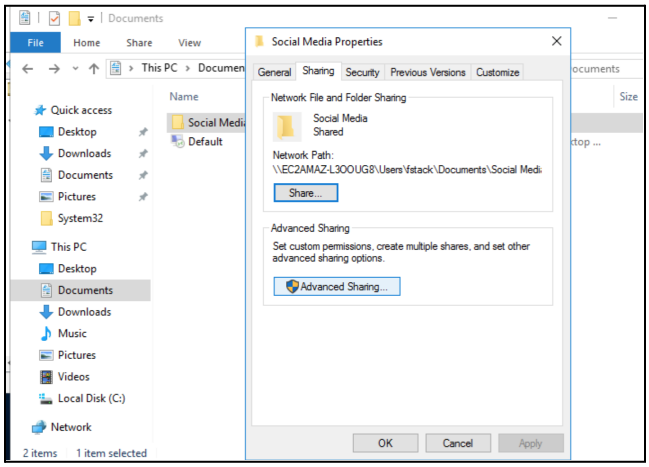
7. Your folder has now been shared. Press the "Done" button to close the file sharing window.



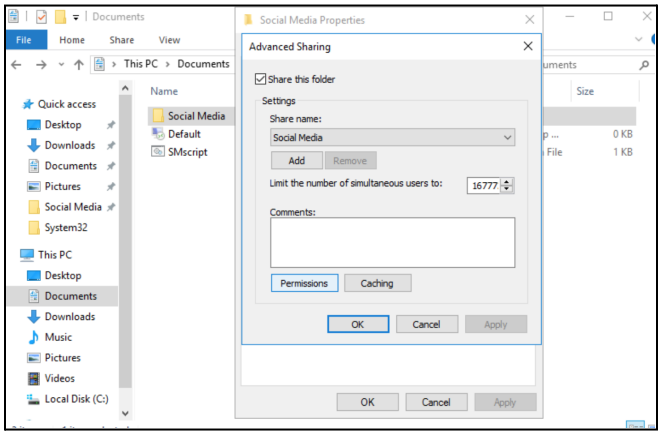
8. Now right click on the folder you just made and click ‘Properties.’



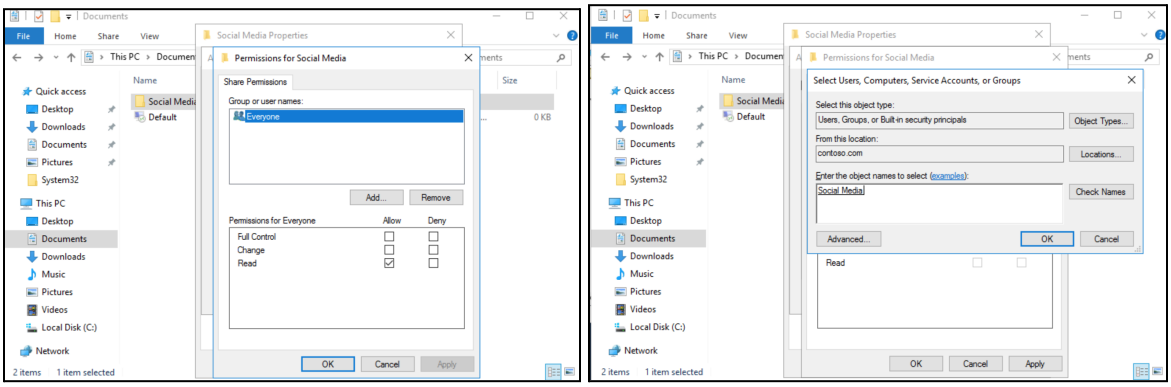
9. Once in ‘Properties’ for the folder, click the ‘Sharing’ tab.



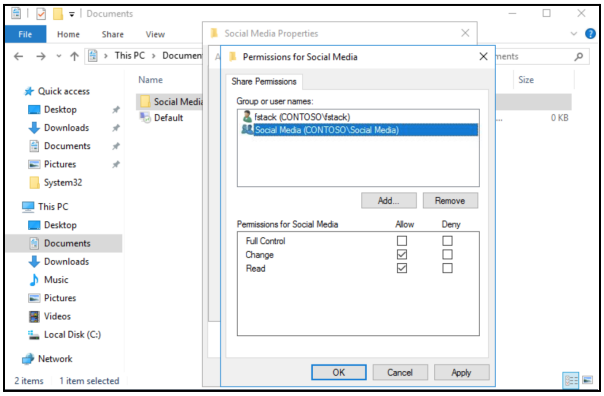
10. Click the ‘Advanced Sharing…’ button which will open a new window and then click the ‘Permissions’ button.



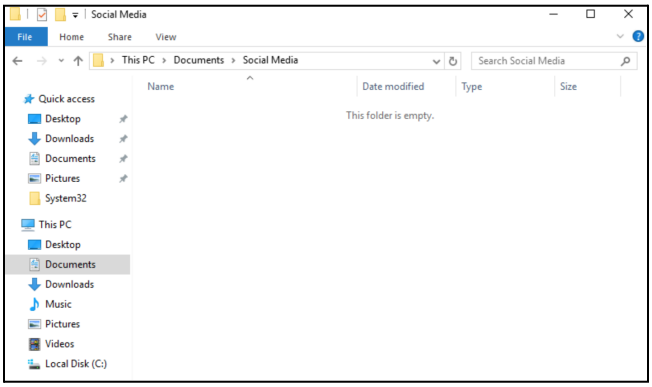
11. Now add the Department group (in this case ‘Social Media’) by clicking the ‘Add…’ button.



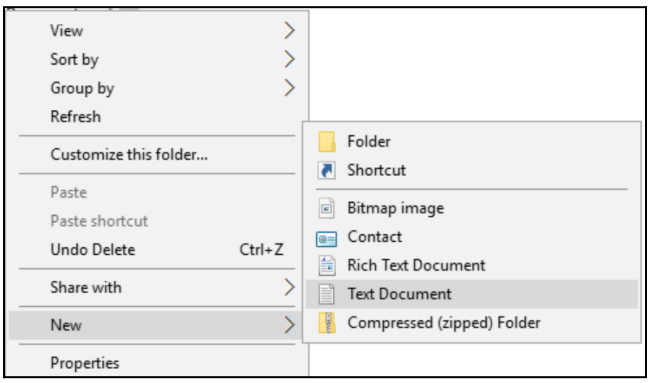
12. Set the Permissions so that the ‘Change’ and ‘Read’ boxes are checked for your Department Group and then click “OK” to confirm changes.



13. Now double-click into the group folder (in this case ‘Social Media’), there should be nothing in there.



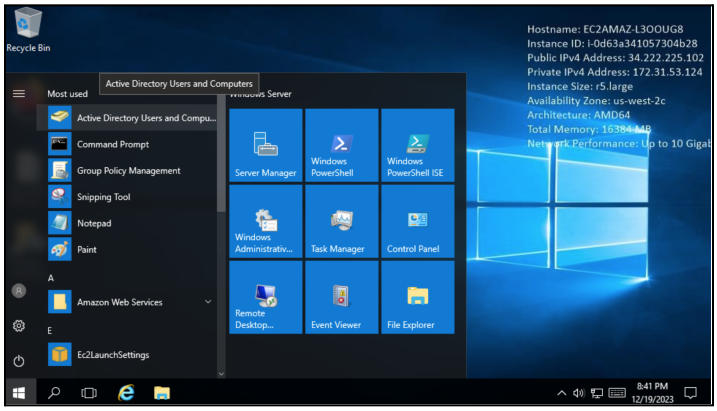
14. Right click in the white space in the folder and navigate to ‘New’ and then ‘Text Document’ and title it “test.txt.”



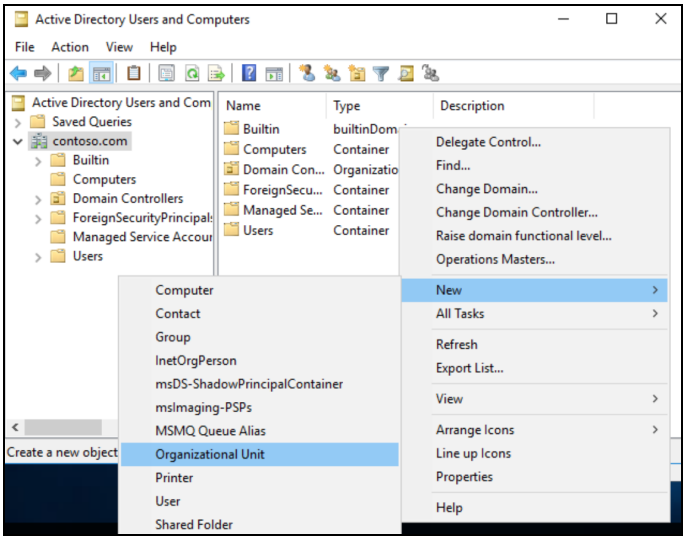
Step 5

Create an OU (organizational unit) with the department’s name and place the user, group, and computer in the OU. Attach a GPO (group policy object) to the OU you created.

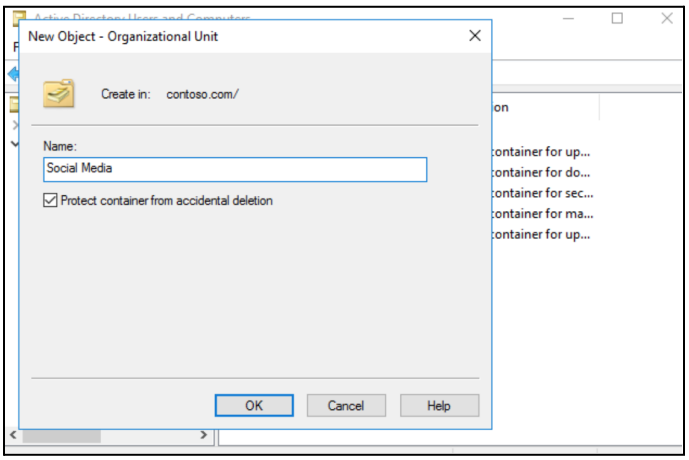
1. Search for ‘Active Directory Users and Computers’ in the Windows search box and click it open.



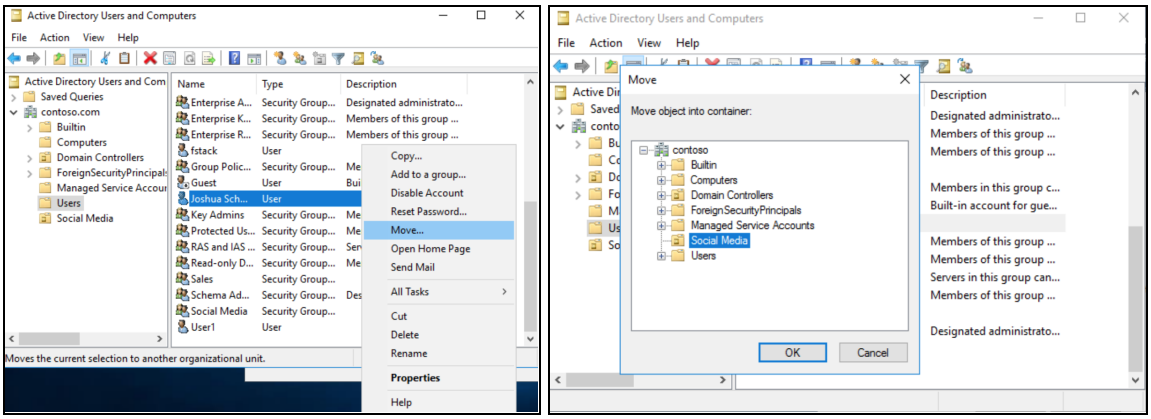
2. In “Active Directory Users and Computers,” click ‘contoso.com’. Once in the domain folder right click and navigate to ‘New’ then ‘Organizational Unit’.

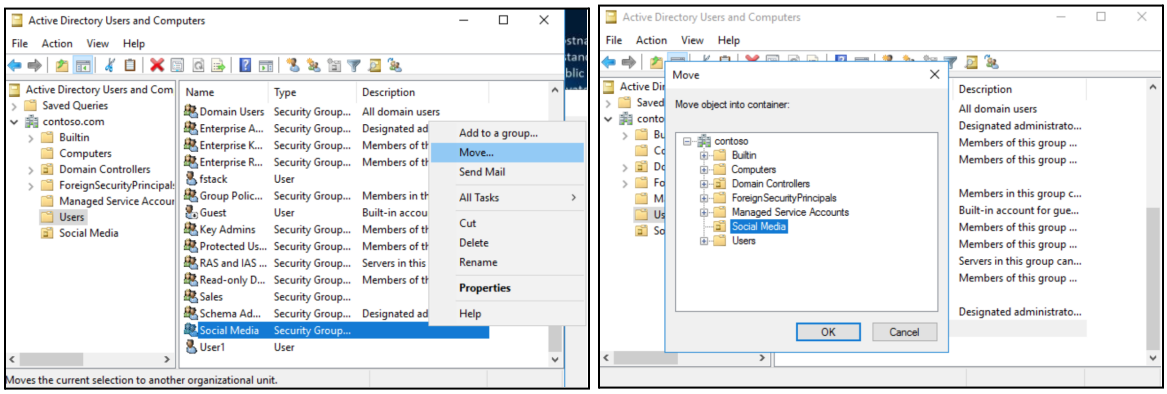


3. Enter the department's name (in this case ‘Social Media’) in the “Name:” box and press “OK” once finished.

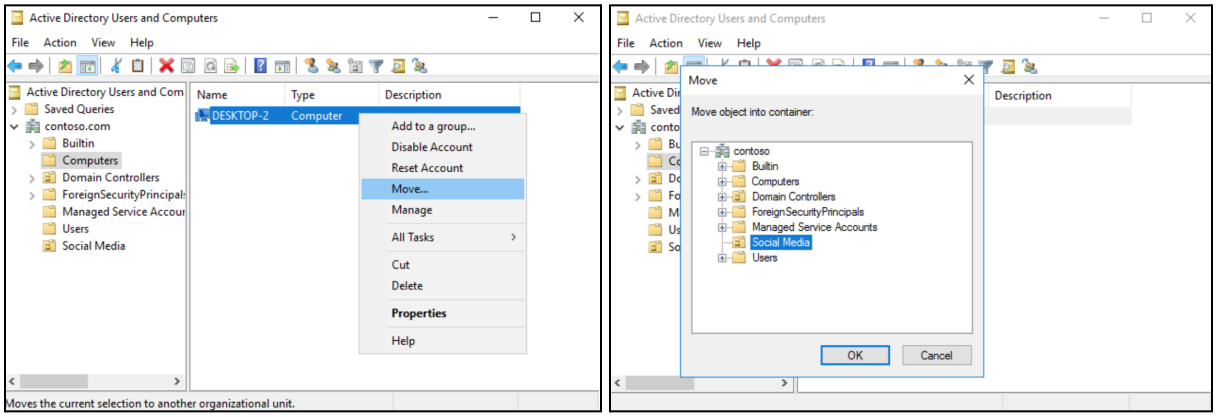


4. Click back into the Users folder and right click on the user you previously created and the group you previously created (in this case ‘Joshua Schmitt’ and ‘Social Media’) and click “Move…” to the OU you just created.

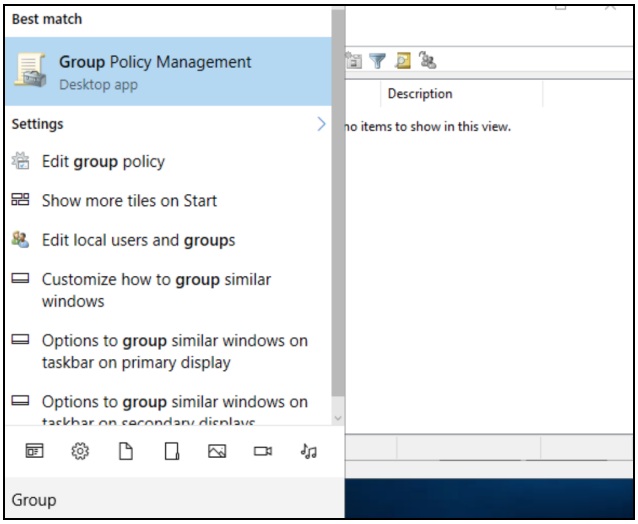




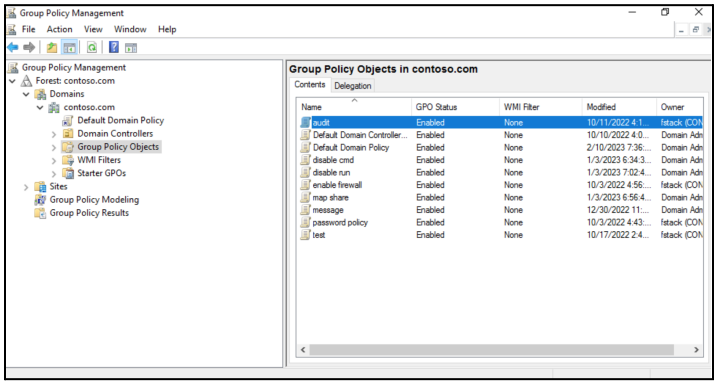
5. Now click into the ‘Computers’ folder (under contoso.com) and right click ‘DESKTOP-2’ and ‘Move…’ into the OU.



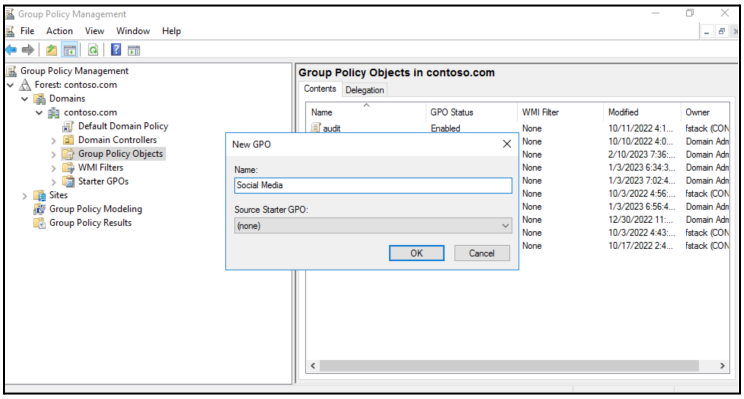
6. Now go to the ‘Group Policy Management’ app from the ‘Control Panel.’



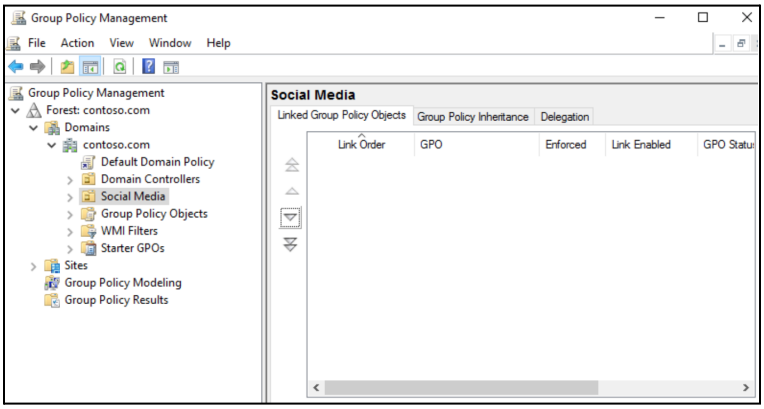
7. Click the ‘Group Policy Objects’ folder on the left hand side.



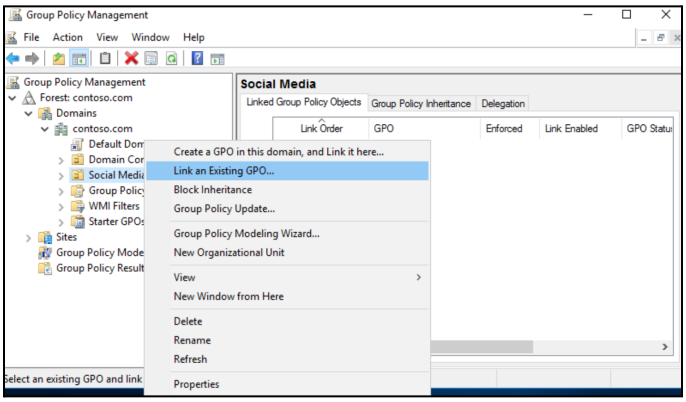
8. Right click in the blank white space in the ‘Group Policy Objects’ folder and click “New” and enter the department name in the “Name:” box (in this case Social Media) and click “OK” once finished.



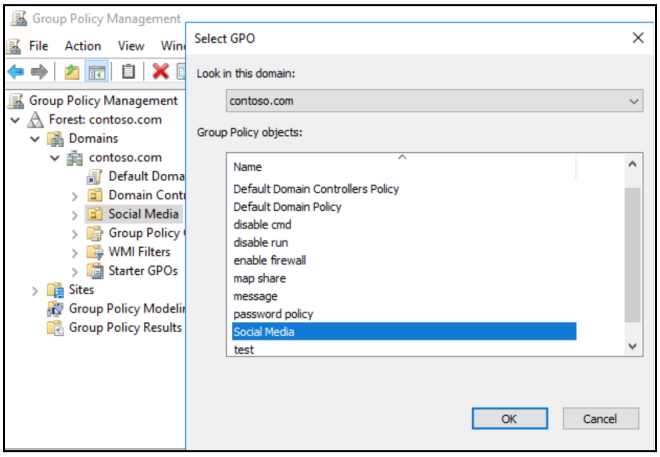
9. Now that you made it, click the OU you created (in this case ‘Social Media’).



10. Right click the OU name (‘Social Media’) and navigate to and click “Link an Existing GPO…”



11. Click the GPO you just created and then click “OK”. Your GPO is now connected to your OU.

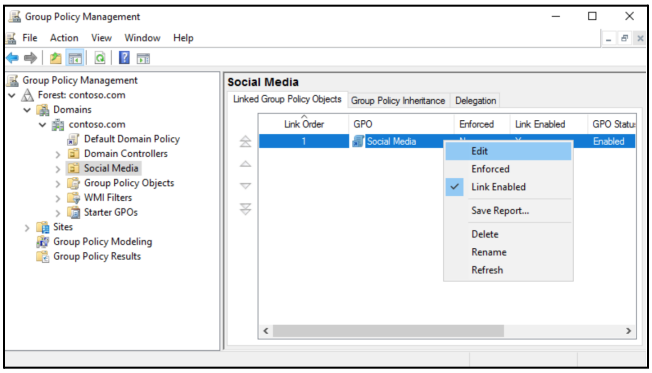


Step 6

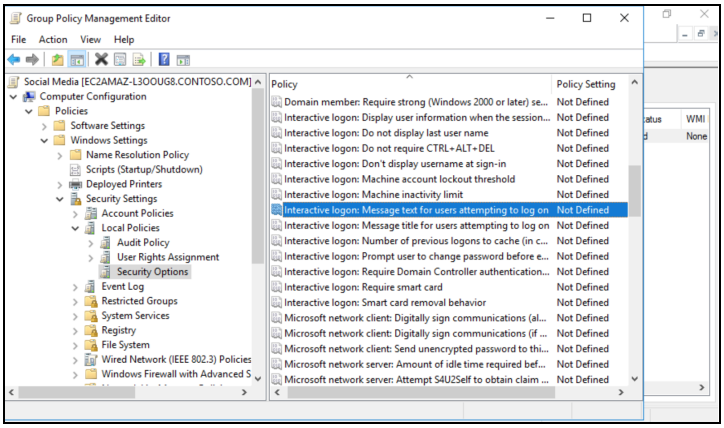
Edit the GPO and apply the following rules:

- A message should appear whenever the computer starts (do not install unauthorized programs).
- Prevent the user's access to CMD.
- Add script to the user's login to map the share you created.
- Disable the run command from the start menu.

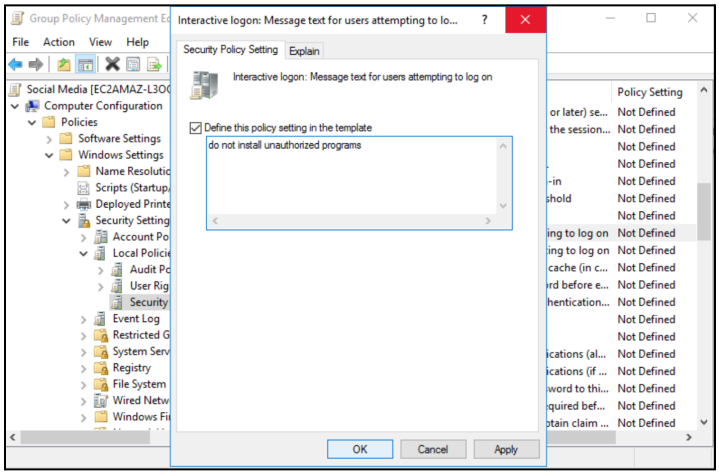
1. To add a message when the computer starts: Right click the GPO under the Department's OU and click 'Edit.'



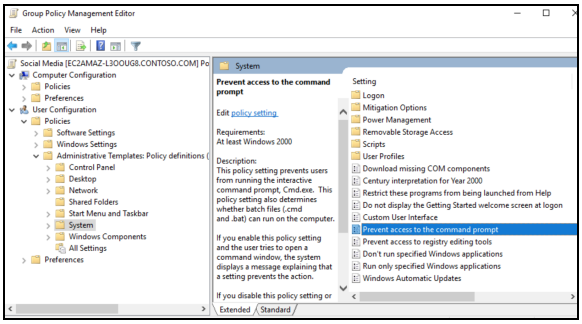
2. On the left hand side under the Department's GPO (in this case Social Media) navigate to 'Computer Configuration,' to 'Policies,' to 'Windows Settings,' to 'Security Settings,' to 'Local Policies,' to 'Security Options' and click 'Security Options.' You will then scroll to the Policy "Interactive logon: Message text for users attempting to log on" and click that.



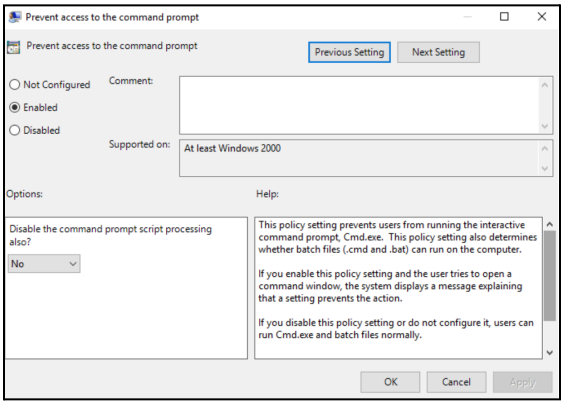
3. Once opened, under the ‘Security Policy Setting’ tab in the empty box that says “Define this policy setting in the template,” enter: “do not install unauthorized programs.” And click “OK” once finished.



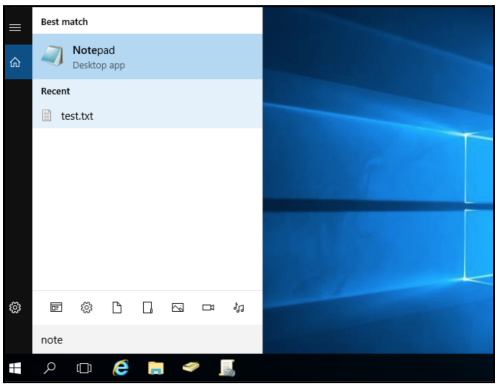
4. Now to prevent the user’s access to CMD: Still in the ‘Group Policy Management Editor’ window navigate to ‘User Configuration,’ to ‘Policies,’ to ‘Administrative Templates,’ to clicking on ‘System’. There under ‘Setting’ you should see a policy setting that says, “Prevent access to the command prompt.”



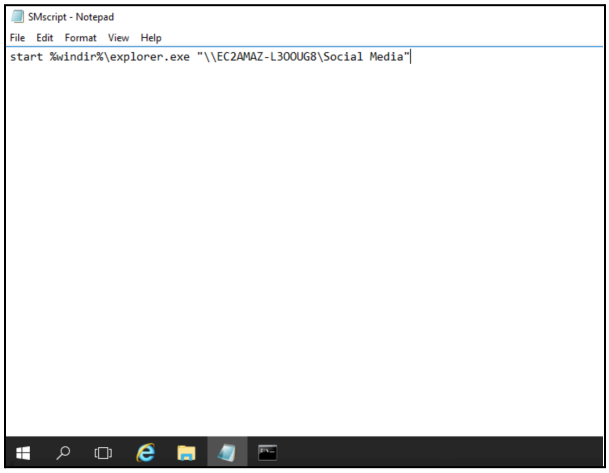
5. Double click the policy setting (“Prevent access to the command prompt”) and a window will open. Once in, click “Enabled” (a black dot will be in the circle next to it now) and then click “OK” to confirm changes.



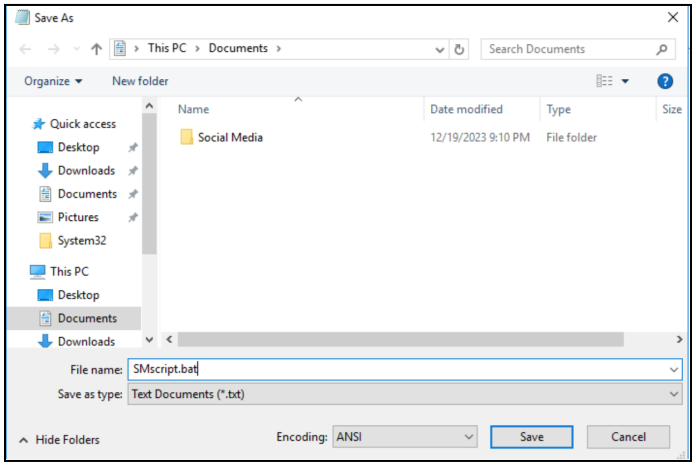
6. Now add a script to the user's login to map the share you created. First open up the notepad app from the Control Panel.



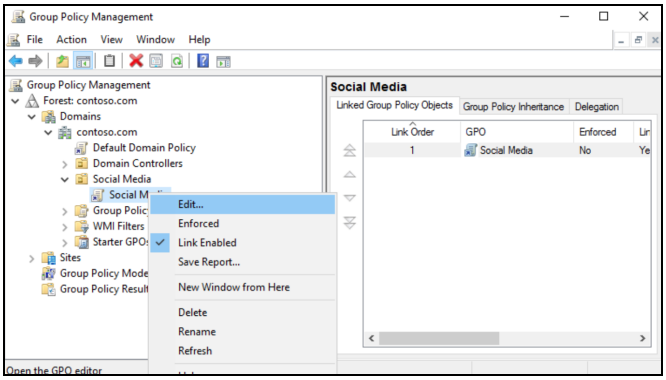
7. Once in, write this: start %windir%\explorer.exe "\\EC2AMAZ-L3OOUG8\Social Media" (Replace “Social Media” with the user’s Department name).



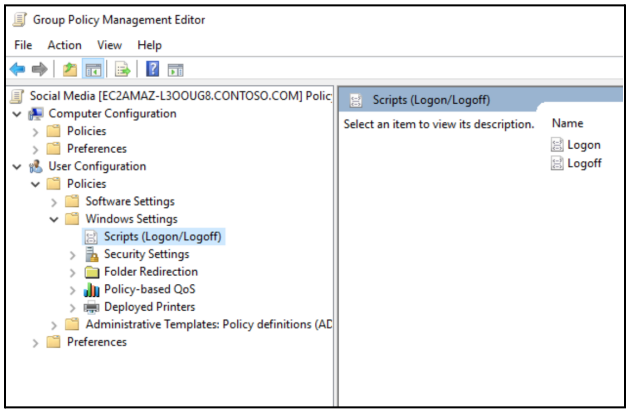
8. Now save the script as a “.bat” file (so in this instance the file will be named “SMscript.bat”) and save in Documents.



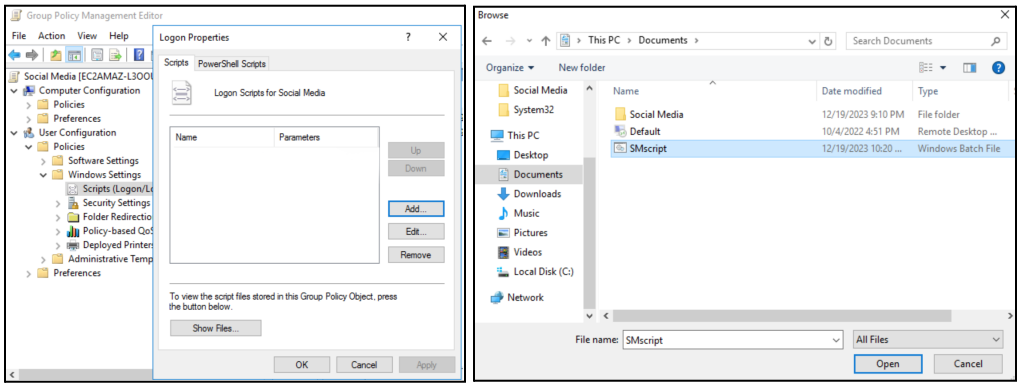
9. Now that you have made a “.bat” file with the script, you must connect it to the GPO. Go back to the “Group Policy Management” window and under the Department’s OU (in this case Social Media), right click the GPO and select ‘Edit…’



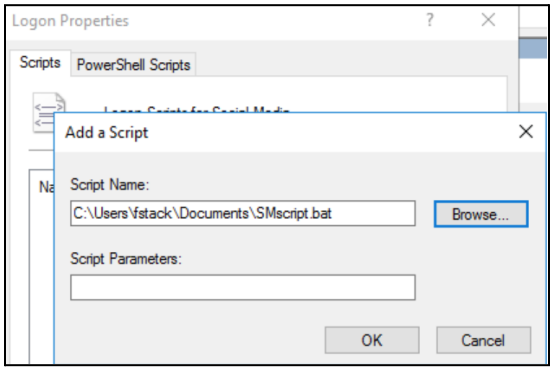
10. This will open up a new window called ‘Group Policy Management Editor’ and on the left hand side navigate the folders from ‘User Configuration,’ to ‘ Windows Settings,’ to Scripts (Logon/Logoff).



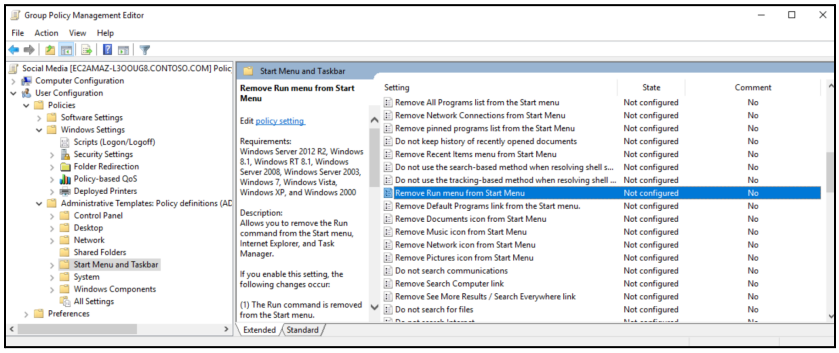
11. Double Click “Logon”. Under the Logon Properties click the ‘Add…’ button and then search for the “.bat” script you just created (in this instance “SMscript.bat” is saved in ‘Documents’), click ‘Open’ once found.



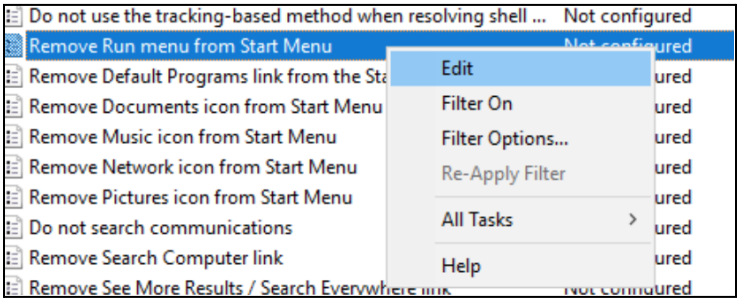
12. You will now see the script name in the ‘Add a Script’ Window and click “OK” to confirm.



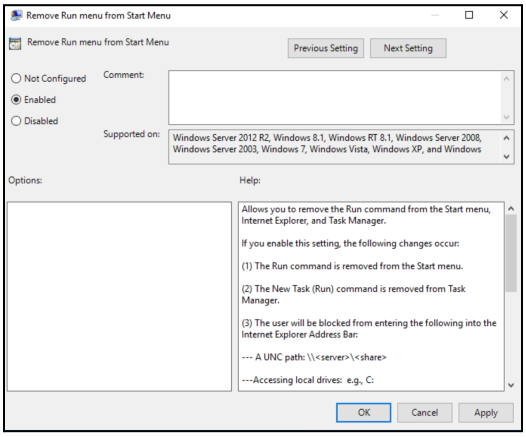
13. Now you must Disable the run command from the start menu. Still in the ‘Group Policy Management Editor’ on the left-hand side navigate from ‘User Configuration,’ to ‘Windows Settings,’ to ‘Administrative Templates:,” to clicking “Start Menu and Taskbar.”



14. Scroll under ‘Setting’ until you find “Remove Run menu from Start Menu.” Once found, right click ‘Edit.’



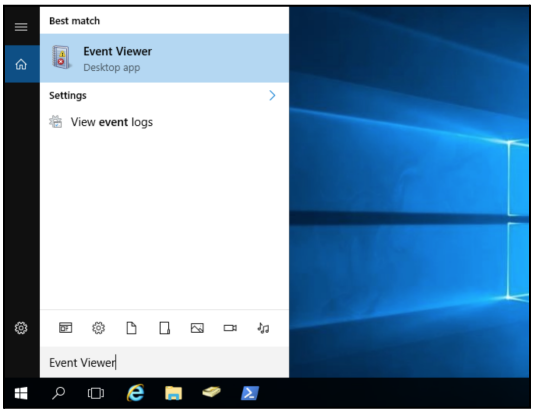
15. This will take you to a new window for “Remove Run menu from Start Menu.” Click the “Enabled” button (so there is a black dot on it) and click “OK” to confirm.



Step 7

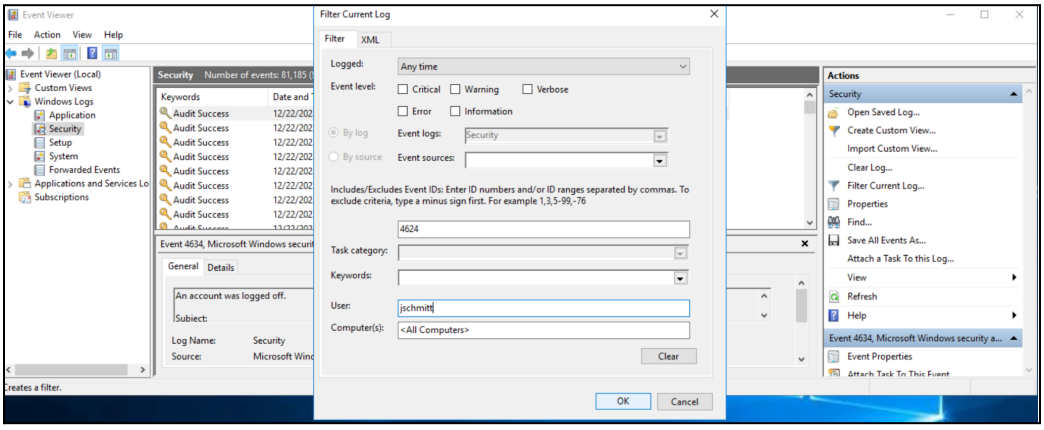
To check the Event Viewer on the server and find the last successful login from the user created, follow these steps:

1. Go to ‘Event Viewer’ from the ‘Control Panel,’ right click and press “Open as an Administrator.”



2. On the left hand side, navigate to ‘Windows Logs’ and then click ‘Security.’ On the right hand side of the window under ‘Actions,’ click ‘Filter Current Log…” A new window will open and you will enter ‘4624’ (an event ID that generates when a logon session is created) in the box that says ‘<All Event IDs>’ and the user

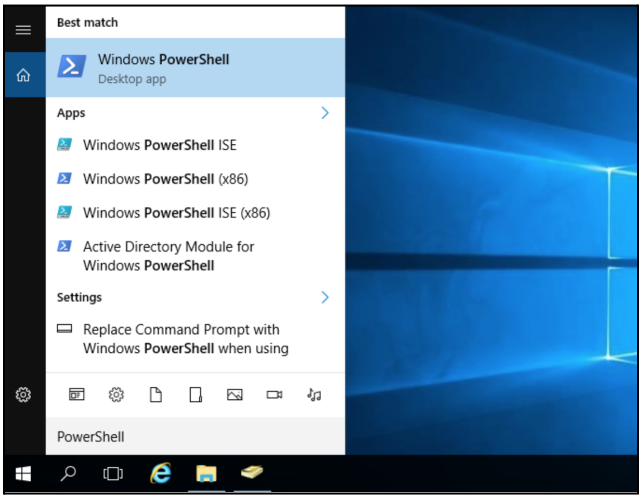
you are looking for, in this instance ‘jschmitt.’ Then click ‘OK’ and your results will populate.



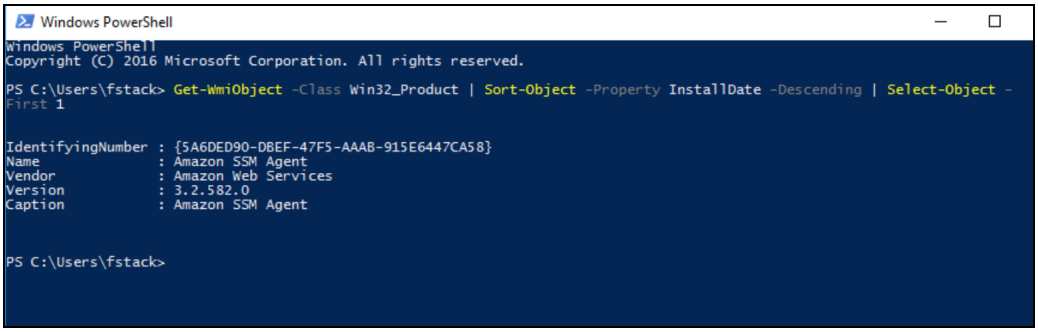
Step 8

To use PowerShell to find the latest program installed follow these steps:

1. Open up ‘PowerShell.’



2. Type in: Get-WmiObject -Class Win32_Product | Sort-Object -Property InstallDate -Descending | Select-Object -First 1

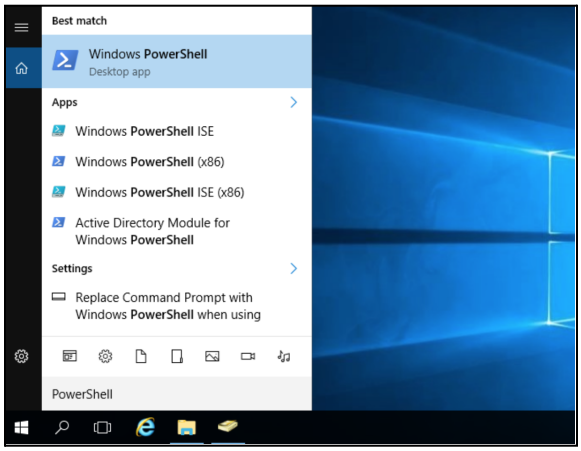


3. The latest installed program will populate.

Step 9

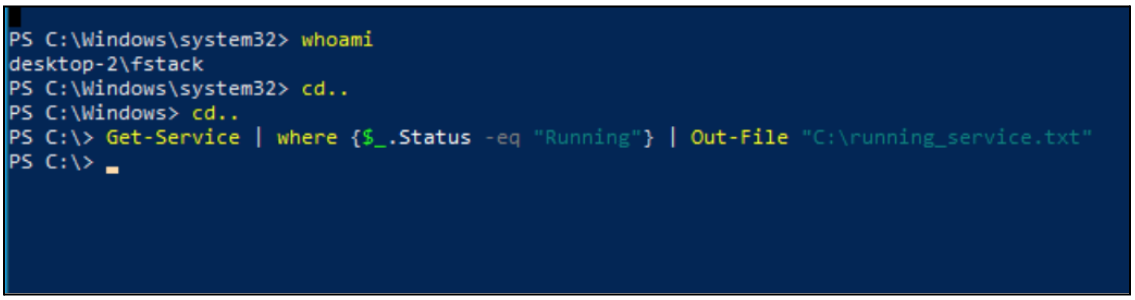
Write a PowerShell script that gives a list of all running services and puts it in a file named running_services.txt.

1. To do this, open up ‘PowerShell.’

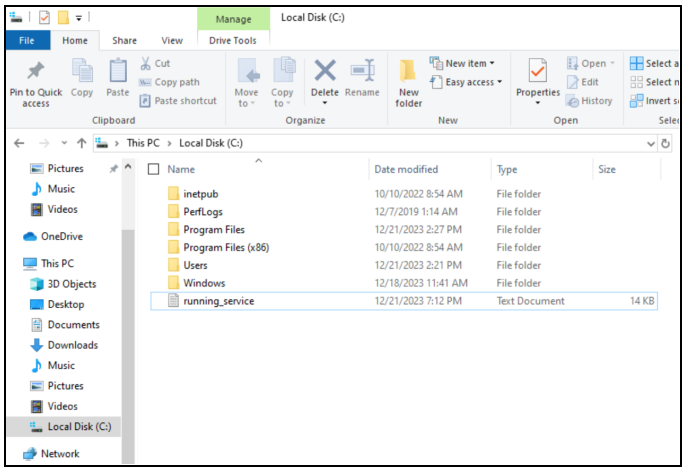


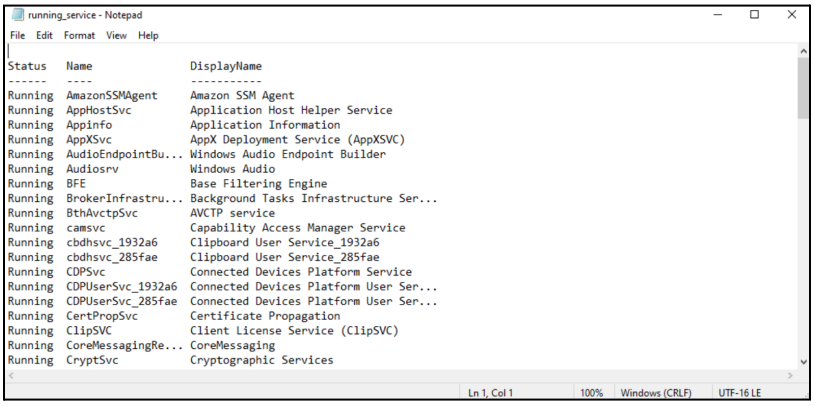
2. In there, ‘cd..’ until you get to ‘C:\’ and type this code into the powershell:

   Get-Service | where {$_.Status -eq “Running”} | Out-File “C:\running_service.txt”



3. Once ran you can go to the C drive and confirm your file was made.





4. You did it and have completed this runbook, well done!