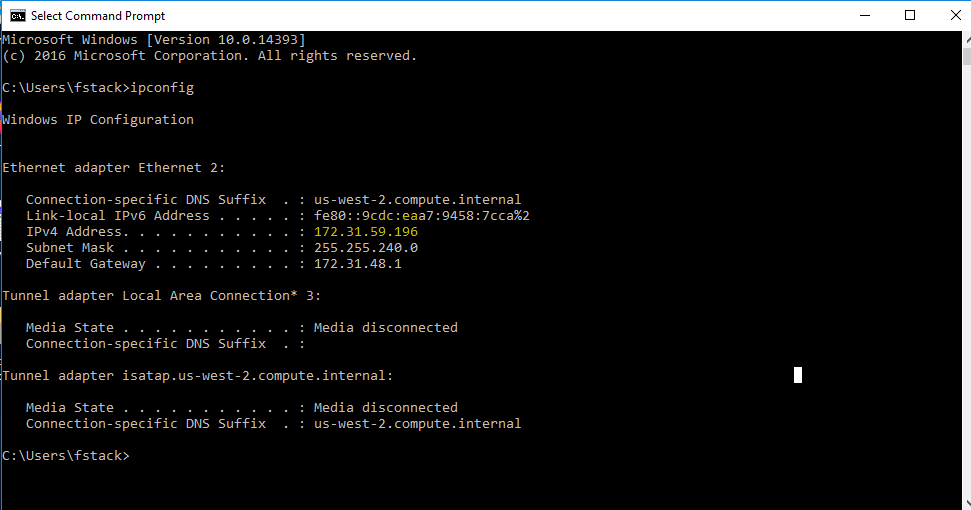
**IT Onboarding Automation & Security Configuration**

In this simulation, I put my knowledge of the Windows operating system and management techniques to the test, solving a real-life scenario based on a fictional company. 💻 Using techniques learned in the bootcamp, I carefully examined the problem, identified the best tools for the job, and documented my findings in a detailed runbook. 📝

Key objectives included performing software asset inventory functions on Windows systems, controlling account settings and passwords for domain user accounts in Active Directory, and effectively communicating technical information in a logical and coherent manner. 💬

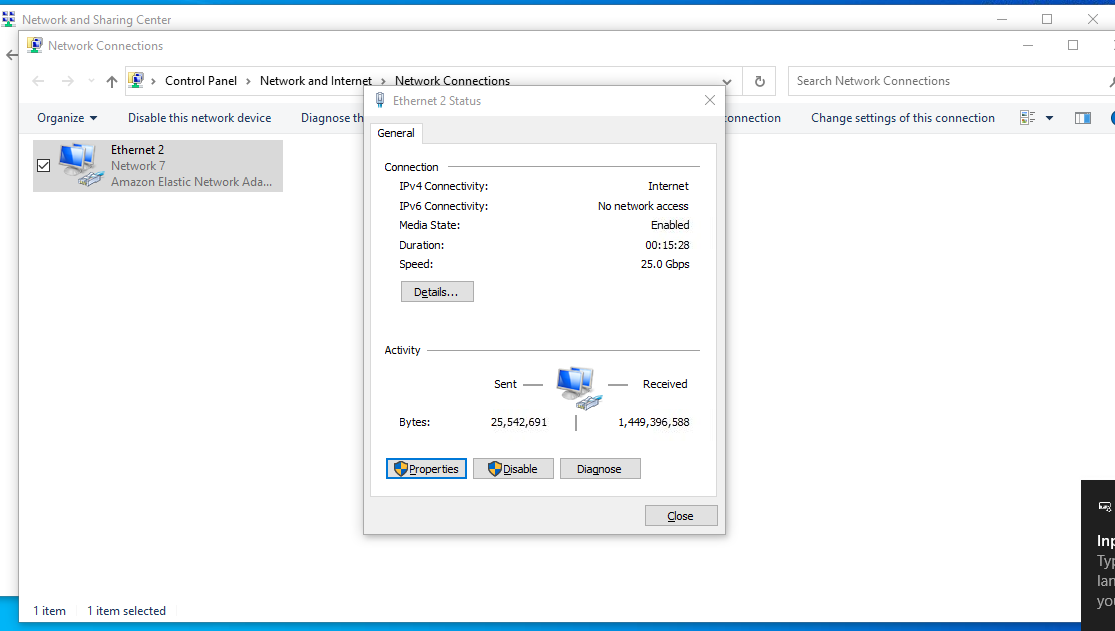
Excited to apply these skills in my future cybersecurity endeavors and beyond! 💪

**STEP 1**: In order to join the computer to the domain we need to obtain the ipv4 address to the server. We will run ipconfig on the server to obtain the ip.

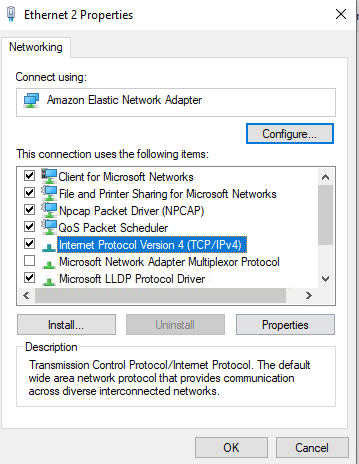


After obtaining the ip address well need to connect it.

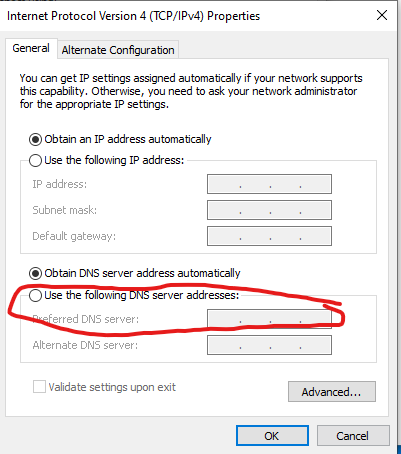
Control panel > Network and internet > Network and Sharing center> Change adapter settings.



From here we will access the properties to attach the ipv4 address,

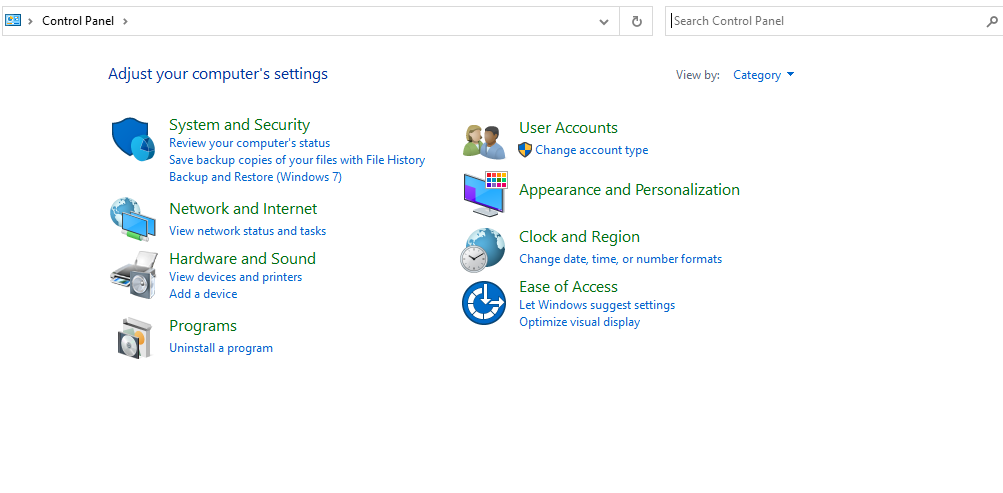


Open internet protocol version (tcp/ipv4)

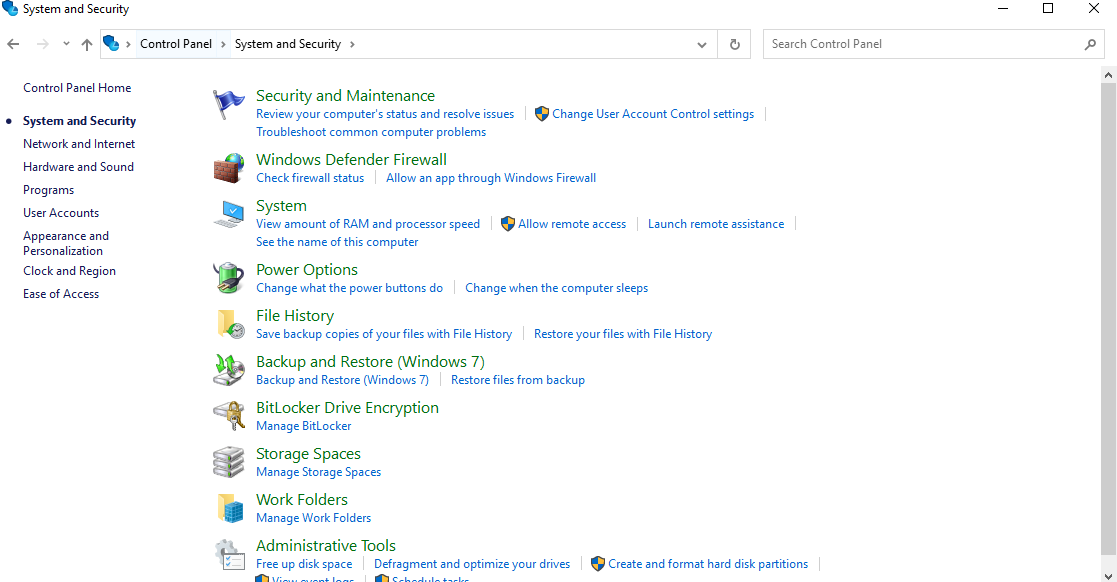


Now we will change the dns server to the ip we obtained earlier.

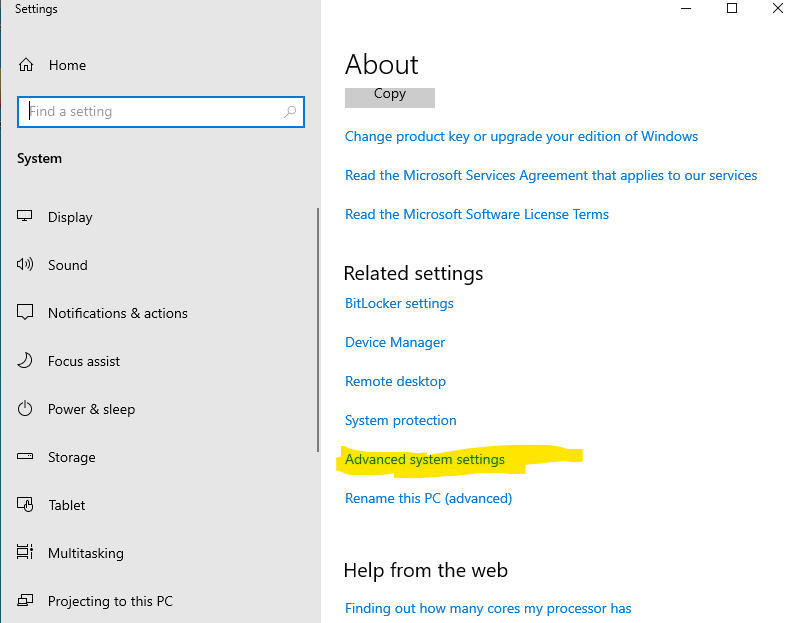
Now that we need to go back to the control panel and access the system and security folder



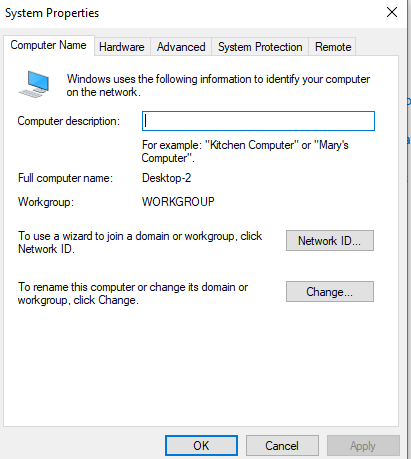
Control panel > system and security >



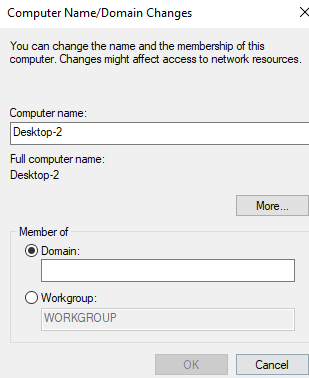
From here click on system. Control panel > system and security > system > advanced system settings (you will find this under related settings after you scroll down )



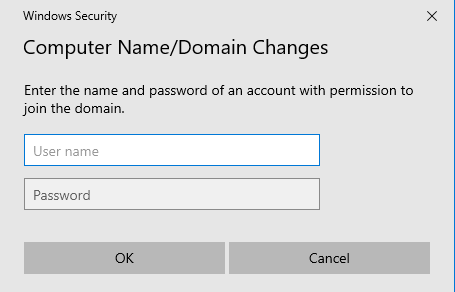
After clicking advanced system settings you will be prompted with the system properties screen.



From here we want to change the computer's domain.



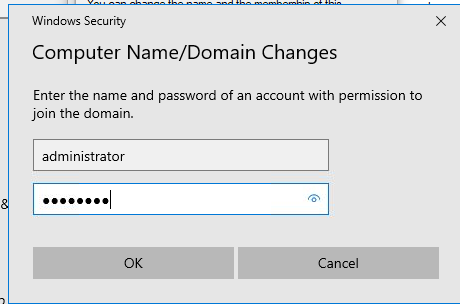
Change from workgroup to domain and then enter the provided domain : contoso.com



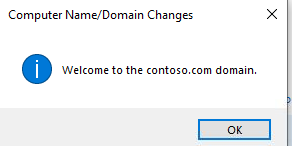
You will be prompted with a login screen, use the following credentials:

User name: Administrator

Password: Pa$$w0rd



You have now successfully connected to the contoso domain

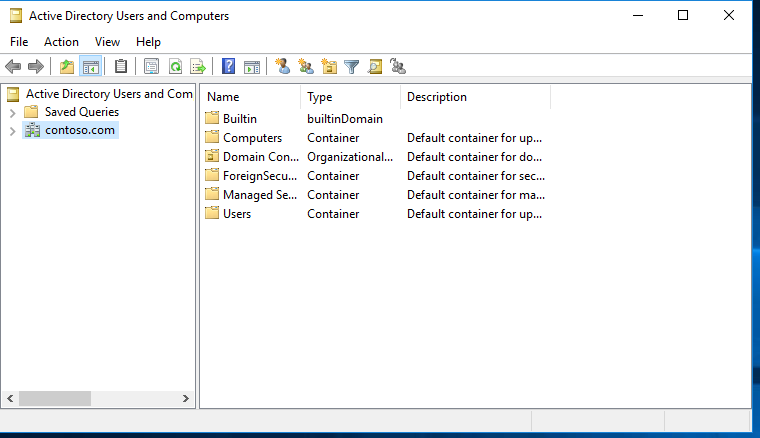


Please restart your device to apply the changes

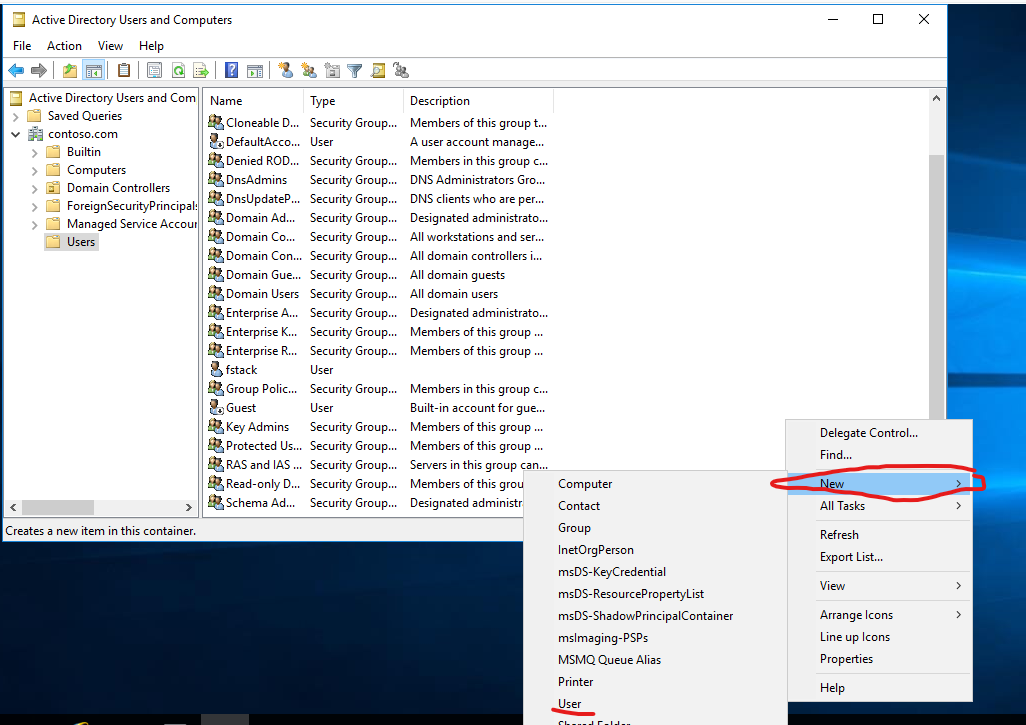
**Step 2**:

To begin step 2 we need to access the Active Directory Users and Computers

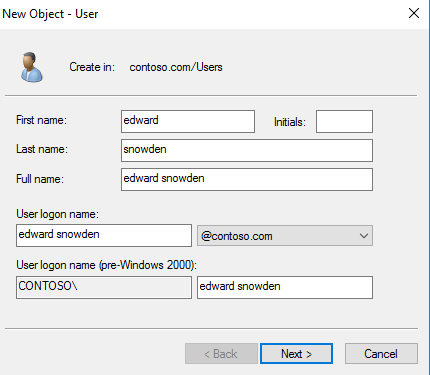
Search > Active directory users and computers



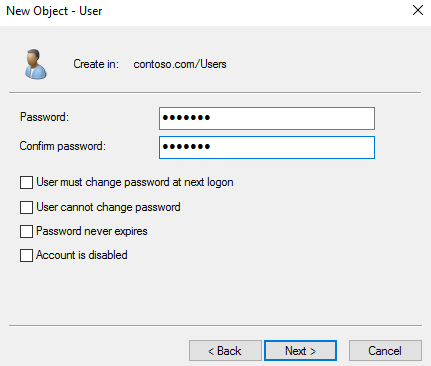
Click on users > right click inside users to create new user.



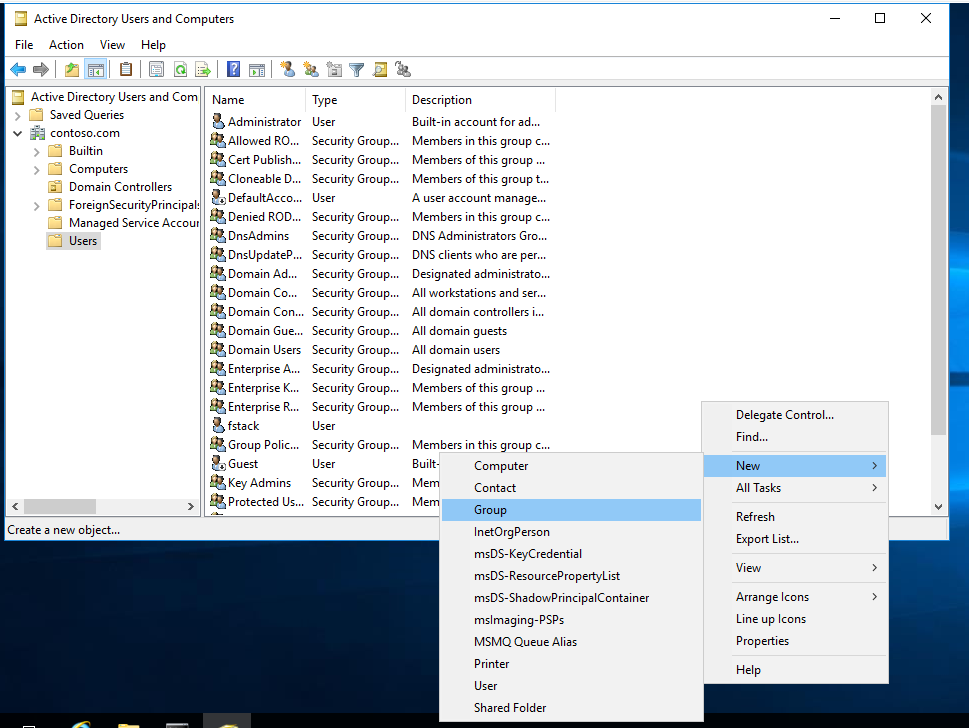
This will open the new user profile creation page. From here we can enter our new users information



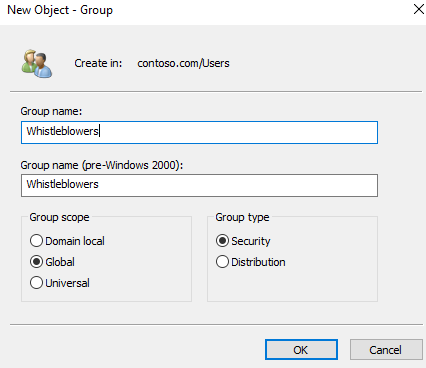
Hit next to save the user information and set password



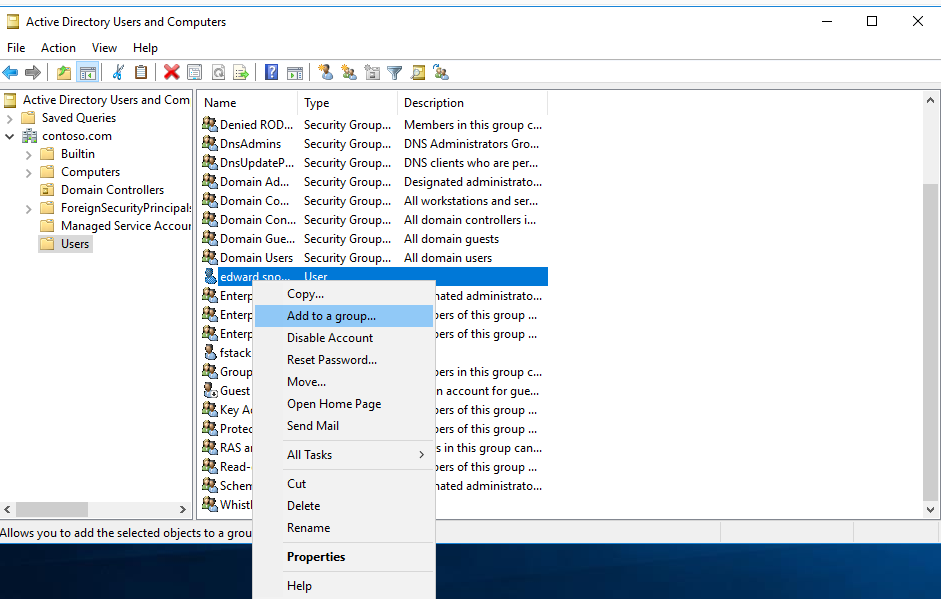
**Step 3**: Now we will begin creating a group to add our new user too using the same process as step 2 we will being in the active director users and computers but this time we will create a group instead of a user



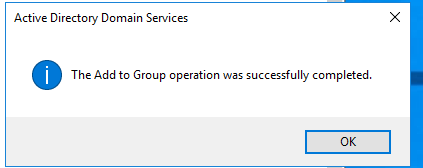
You will be prompted with a new object group creation screen. Here we will enter the new groups information.



Now we will add our users to the group

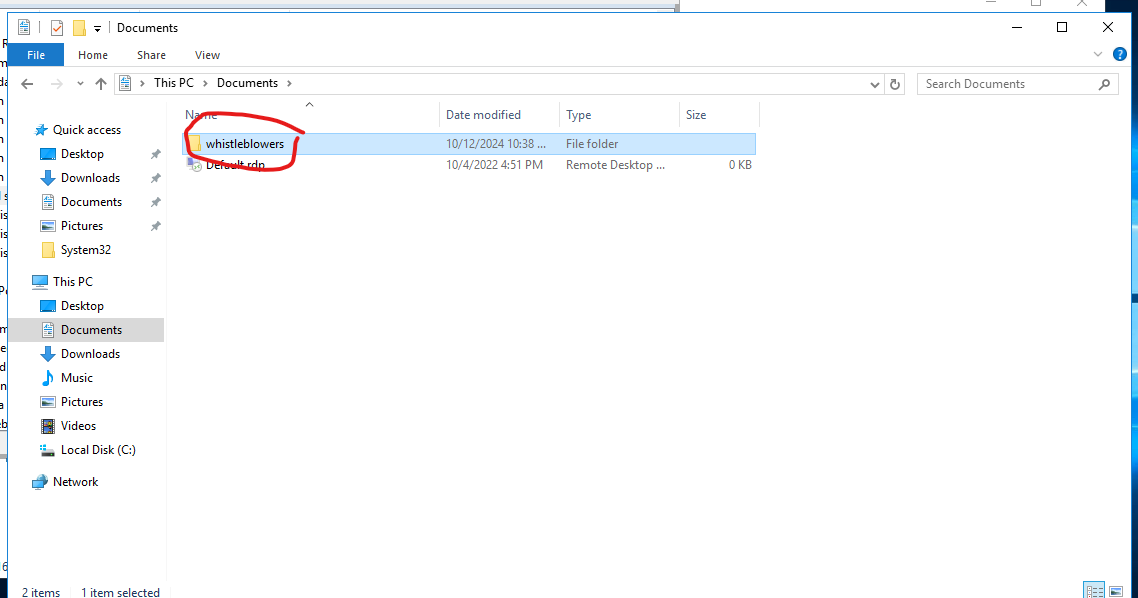


If your user was added successfully you will be presented with this screen

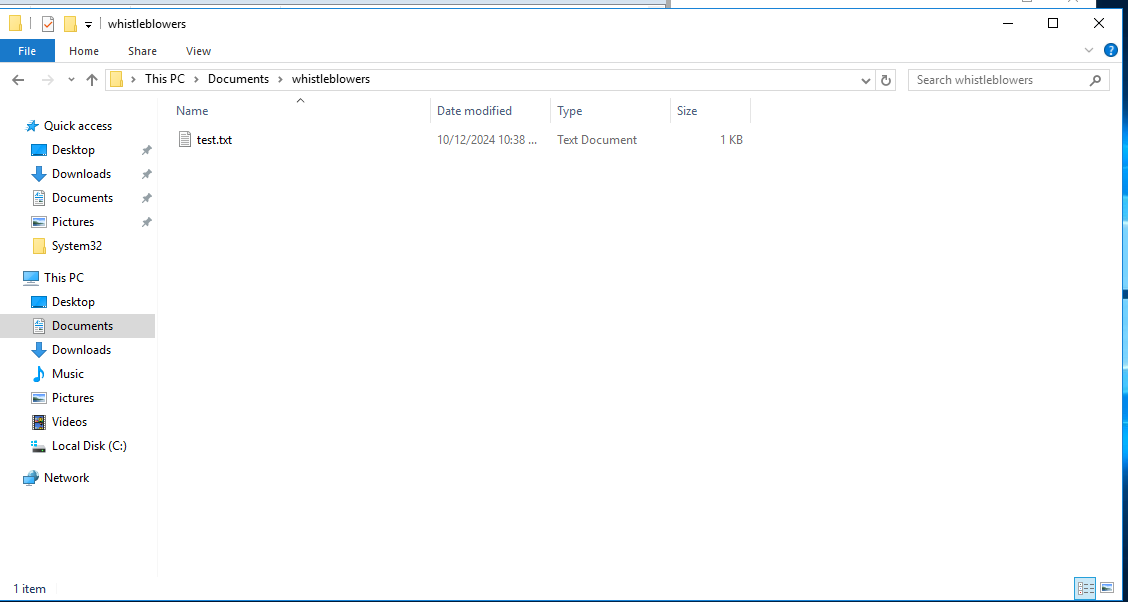


**Step 4**: Now we will create a share folder and provide the group with permissions .

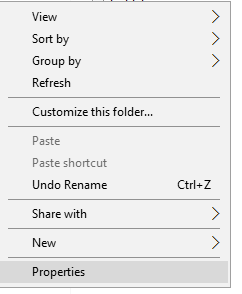
Begin by creating and empy folder and adding the departments name to it.



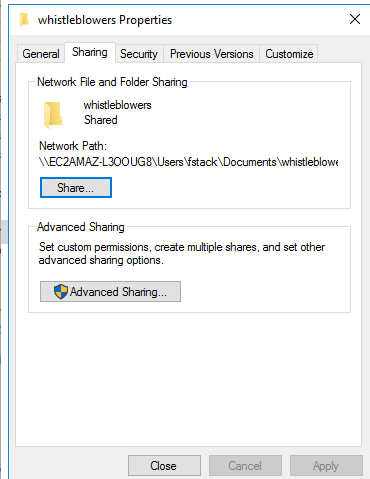
From here we will create an empty document inside the folder called test.txt



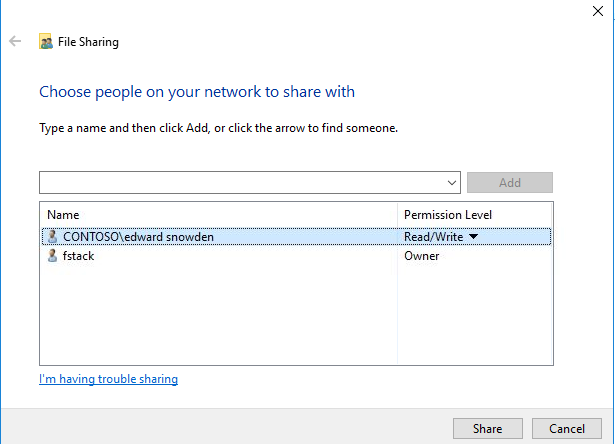
Now right click on this txt file and bring up the properties



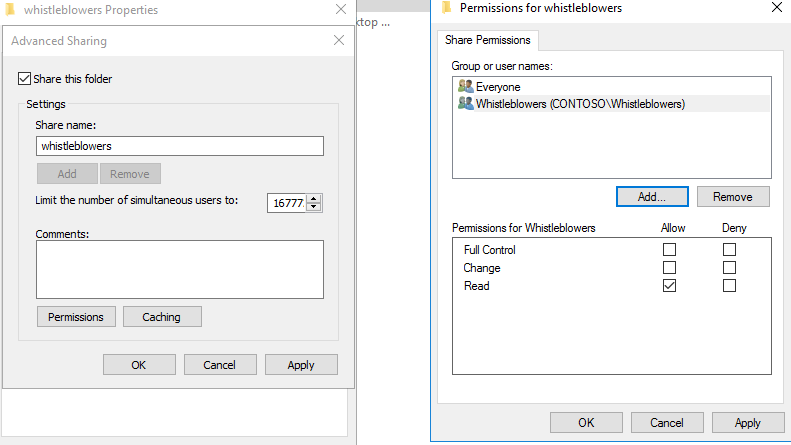
Now go to sharing > share…



Add the users you want to share the folder with and change there permission levels to read/write

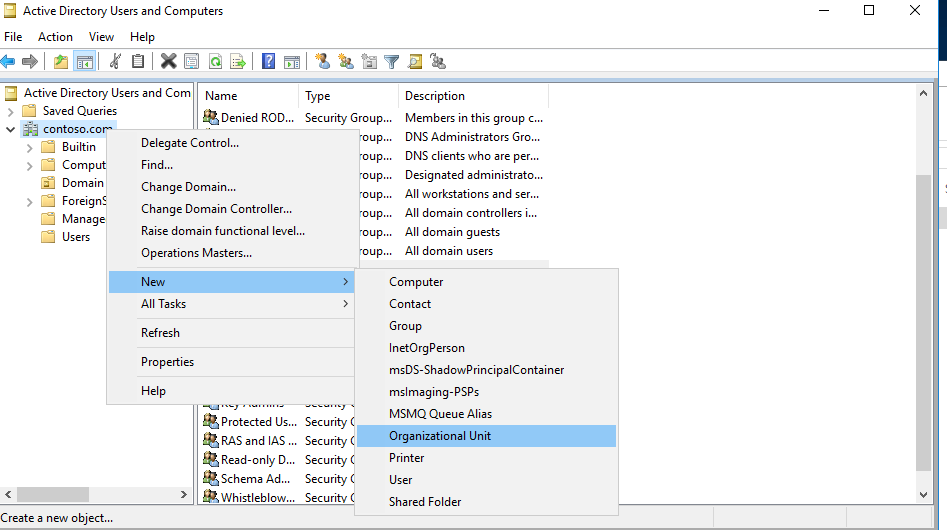


If needing to share the file with multiple users you can add the group / department using the advanced sharing setting

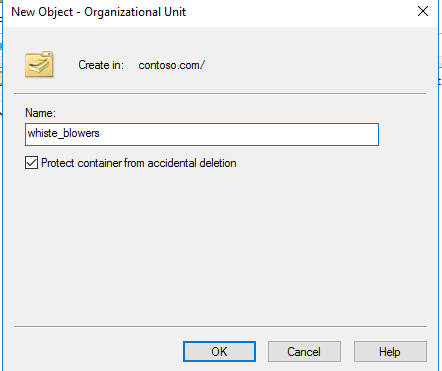


**Step 5**: Creating an OU to store our groups and users and apply group policies.

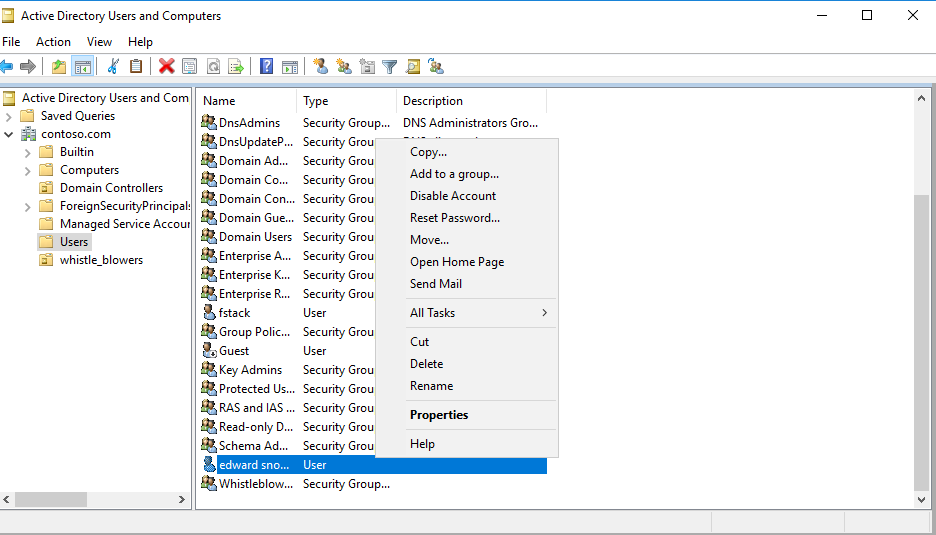
We will begin in the active directory users and computers. Take your mouse and right click on contoso.com hover over to new > organizational unit



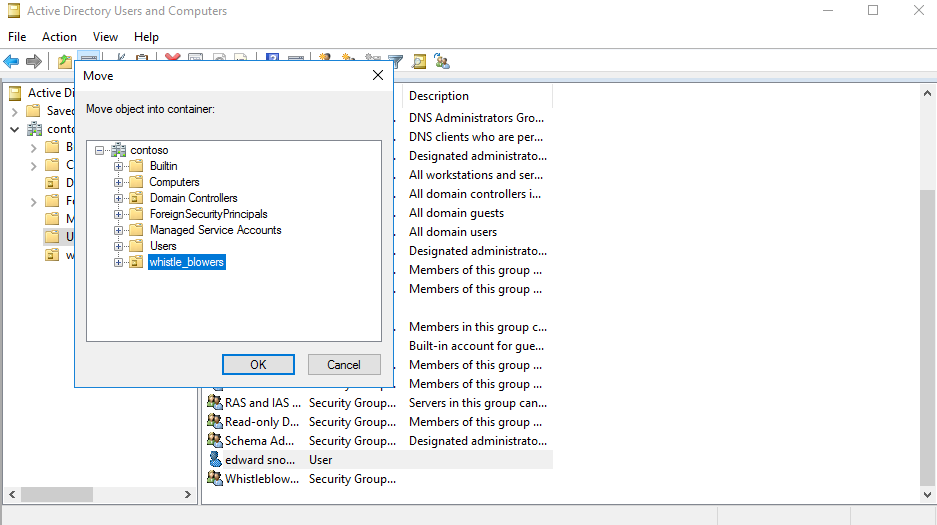
Add the departments name and then groups / users



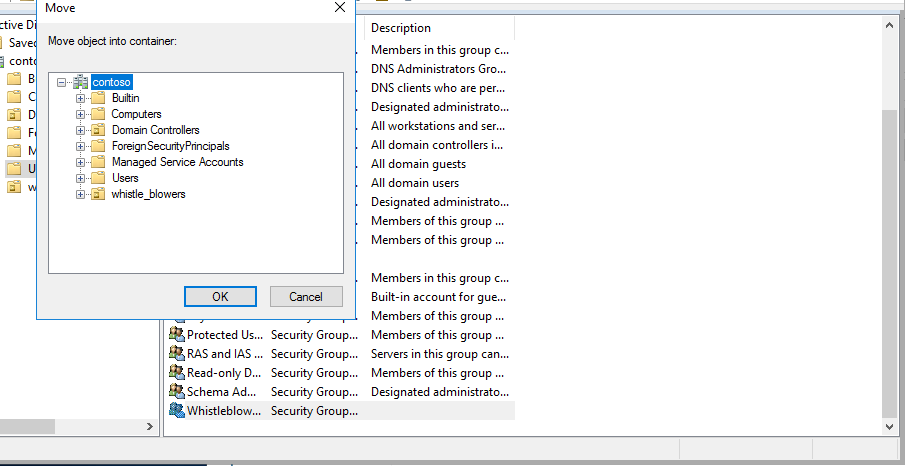
Now we will begin to move users and groups into the OU



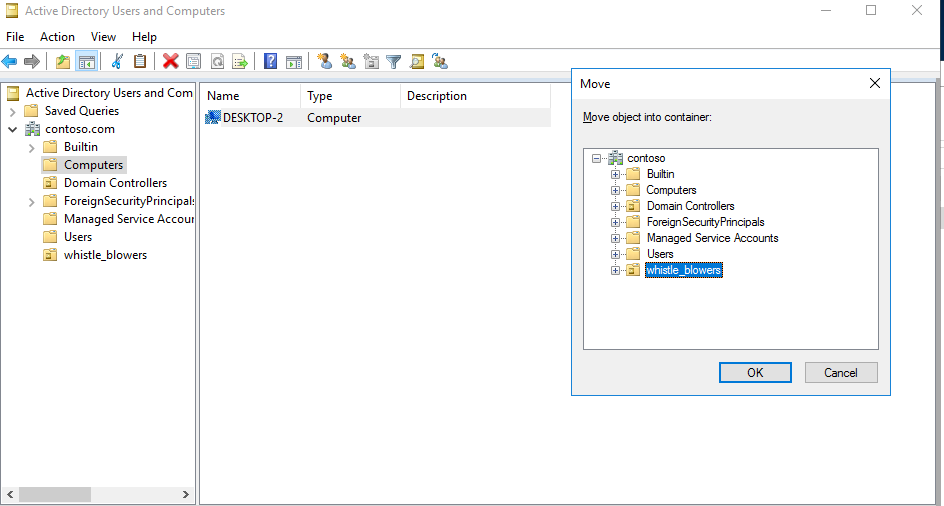
Move to new OU



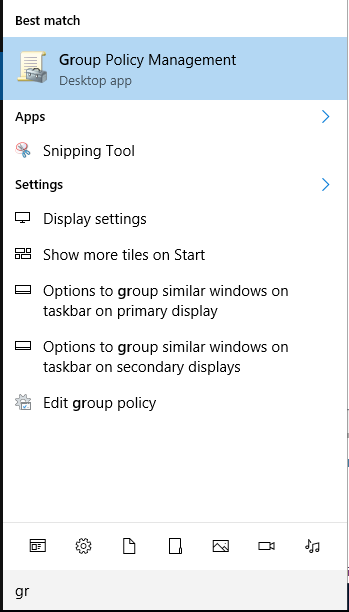
Now do the same with the group



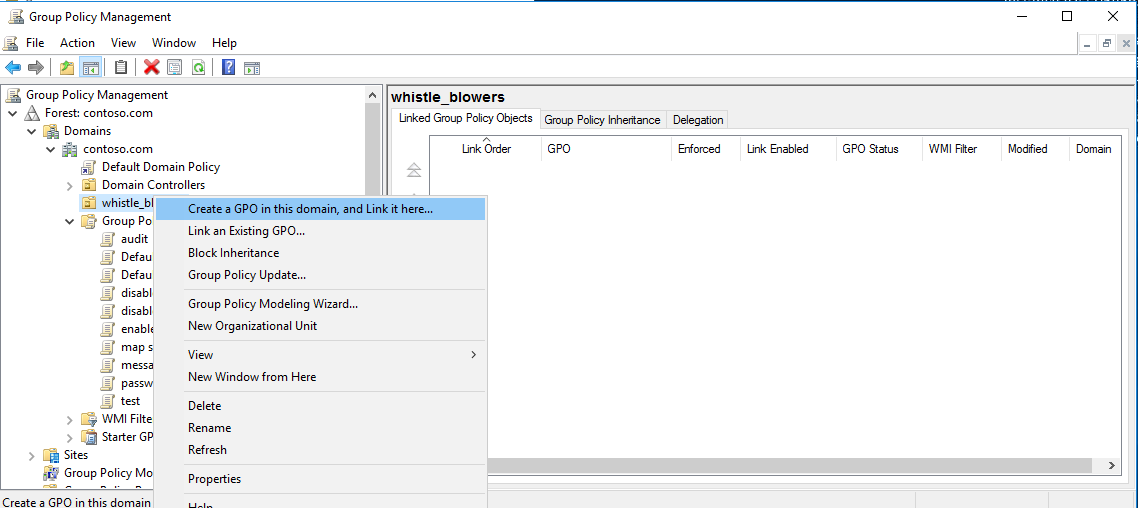
Now we'll move the computer using the same steps.



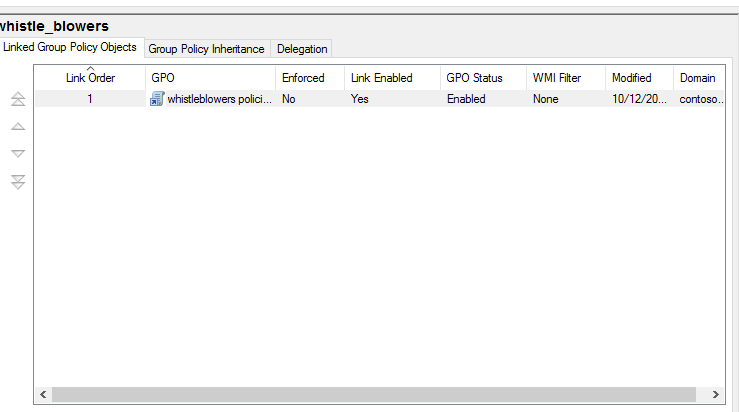
Now to attach a GPO we will navigate to the Group policy managment



From here we want to click on our organizational unit whistle\_blowers and create a gpo in this domain and link it here.

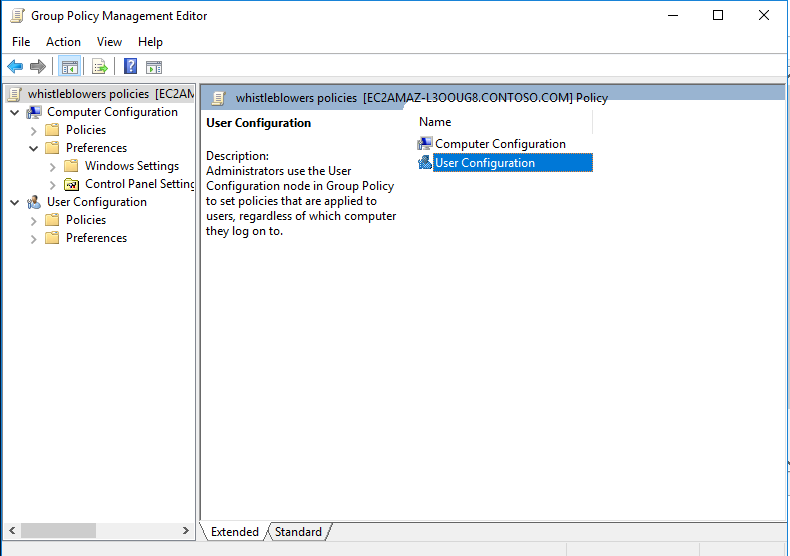


After creation it should look like this.

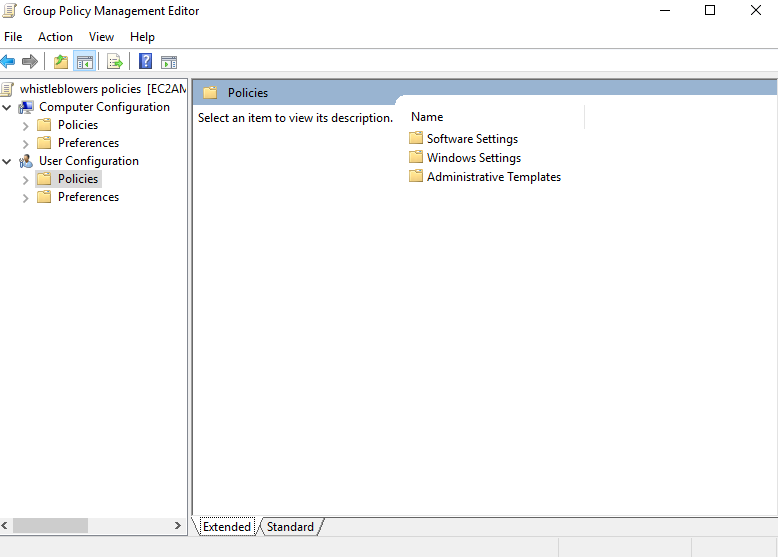


**Step 6**: Time to edit the GPO and apply some rules.

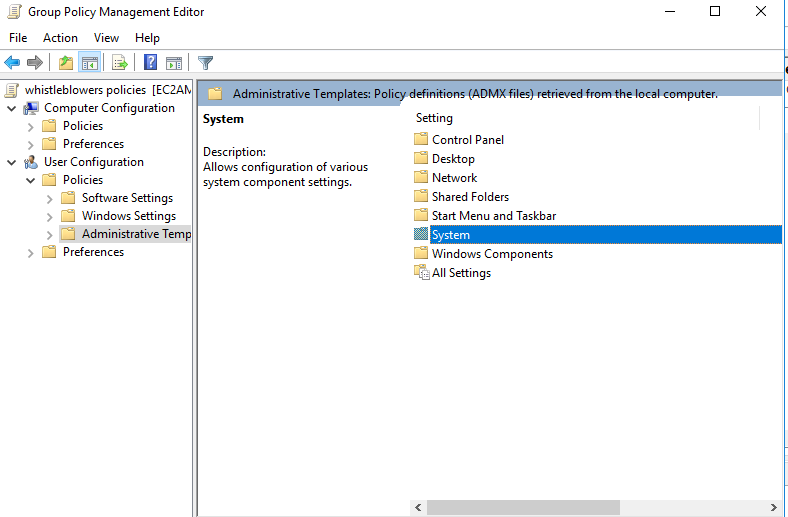
We will begin by adding a message at startup for the every computer in the OU by heading to the computer configurations

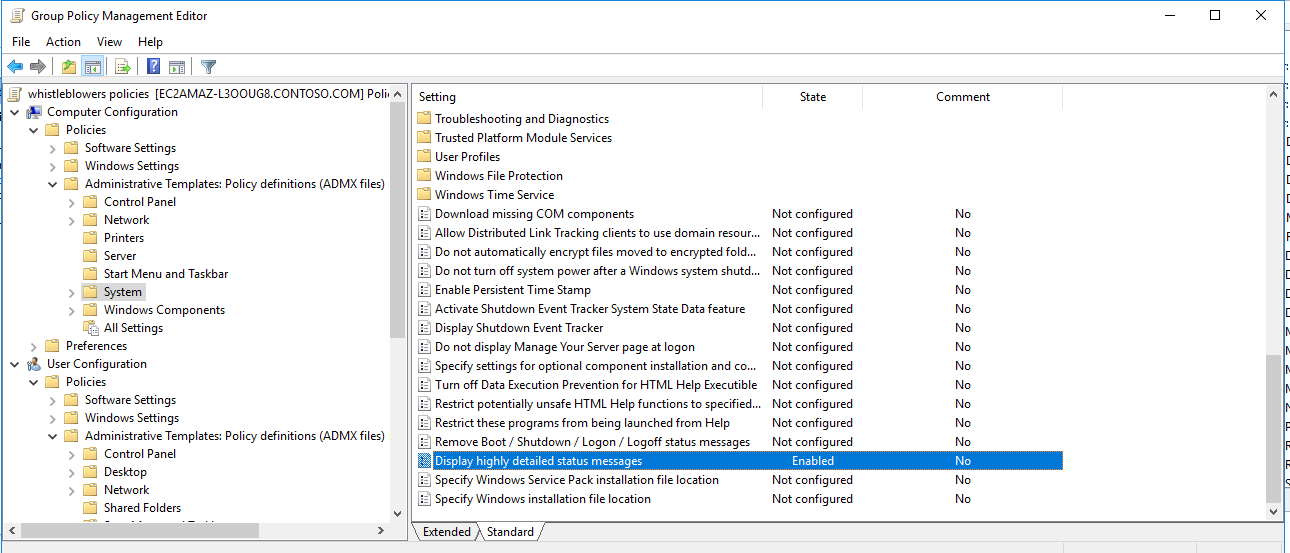


From here we go computer configuration > policies > administrative templates

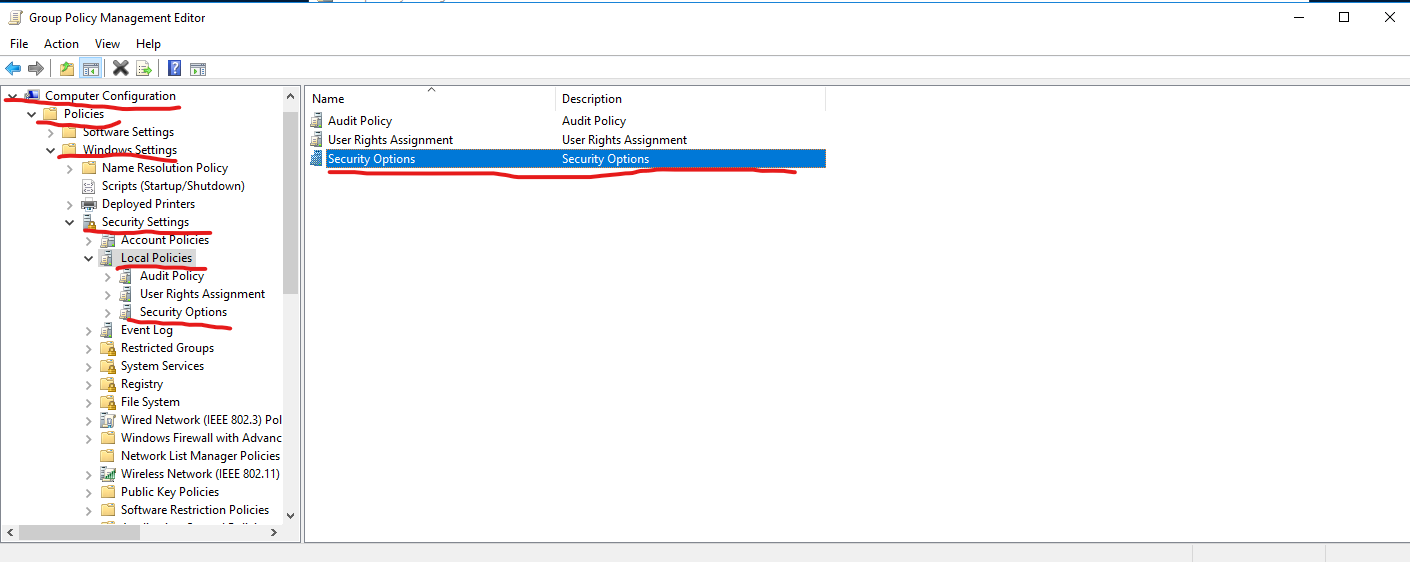


From here access the “system” folder

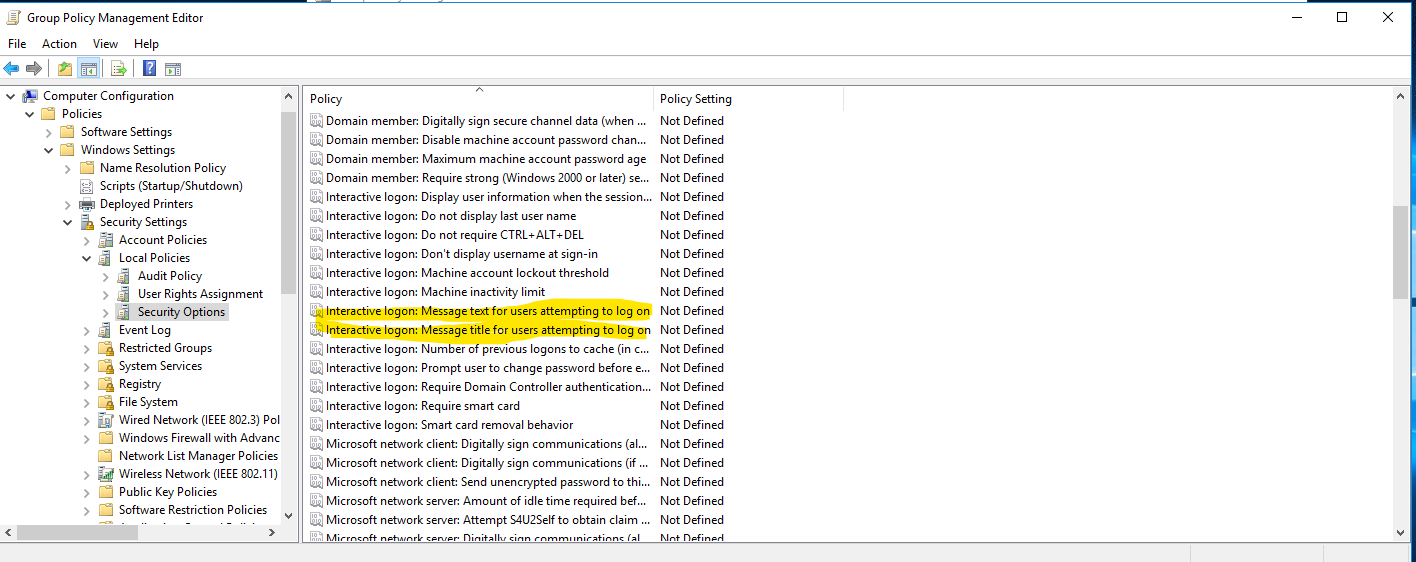
\

Find the “display highly detailed status messages and enable

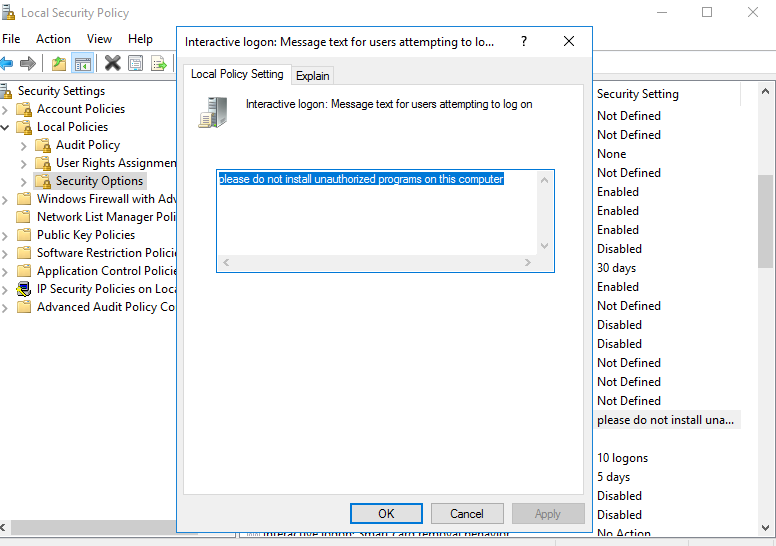
From here we will go back 2 steps to policies and access the windows settings folder to edit that message on startup. Find “interactive logon :message text for users attempting to log on” windows settings > security settings> local policies > security options



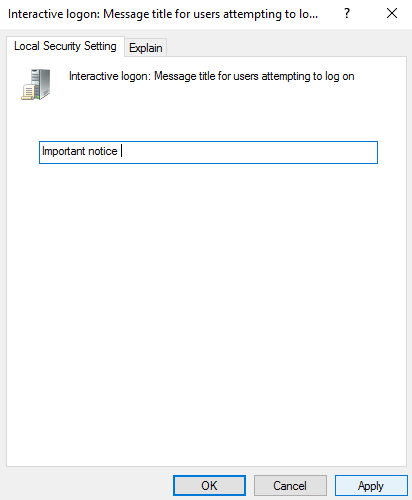
Now we find the “interactive logon: message text for users attempting to logon” we will also need the message title later on.



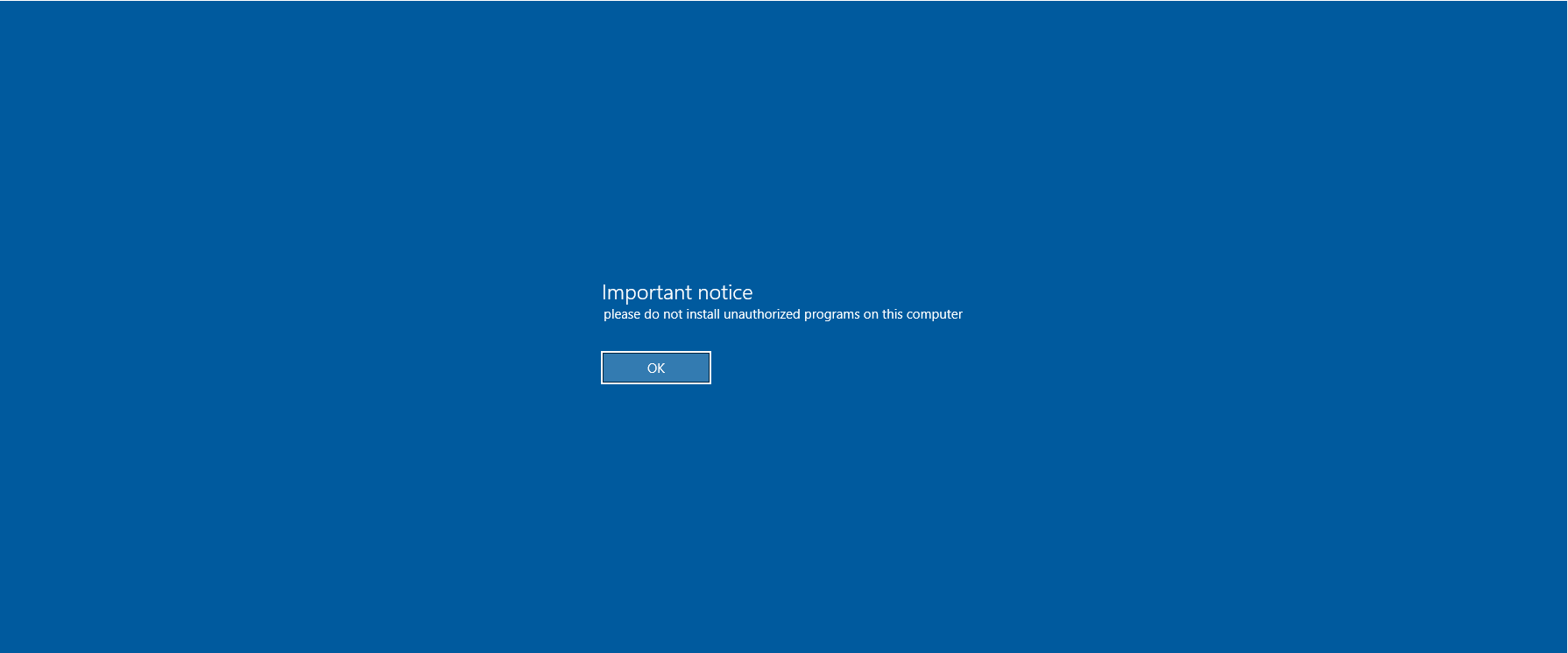
Change the message text to “please do not install unauthorized programs on this computer.



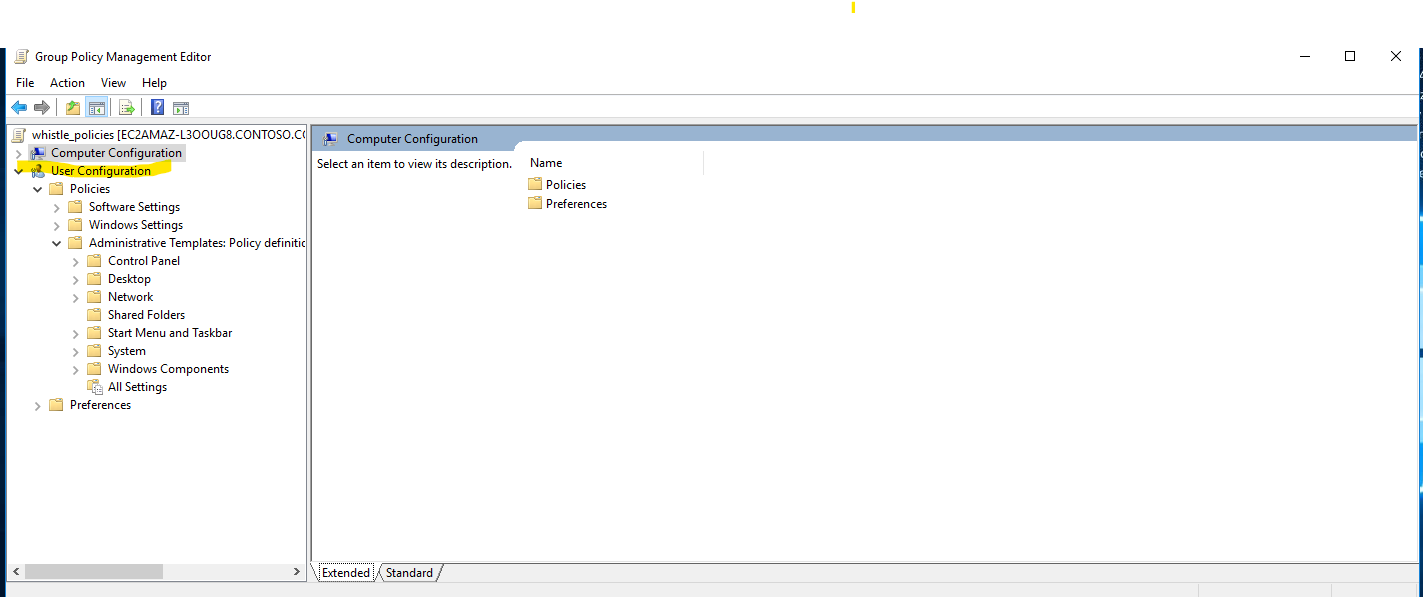
Now change the title to the interactive logon message title



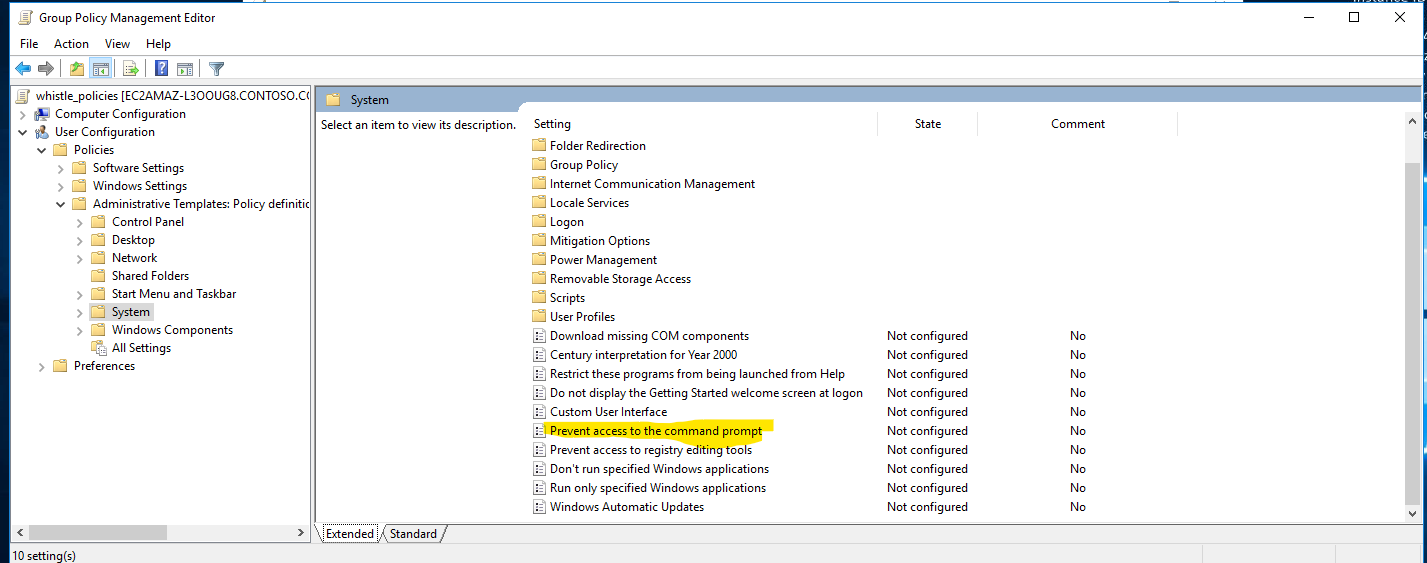
Now anytime users boot up their computer they will be prompted with the important message



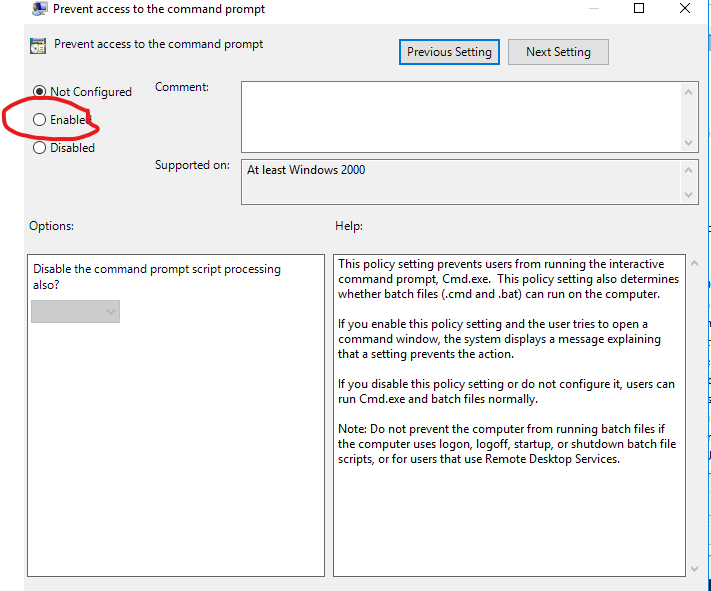
Now in the same gpo we will restrict our users access to the cmd prompt . head to the users configuration



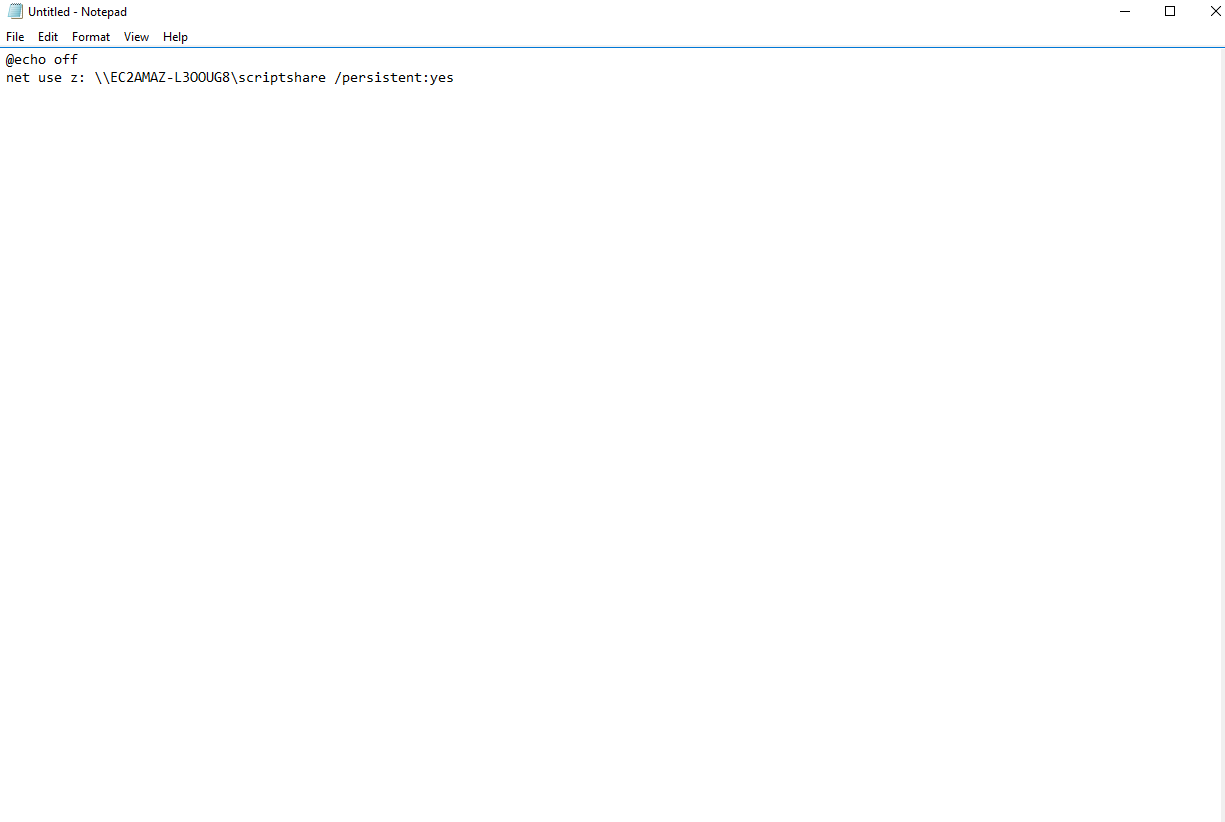
From here follow the path user configuration > policies > administrative templates > system . here you will see the policy to “prevent access to the command prompt”

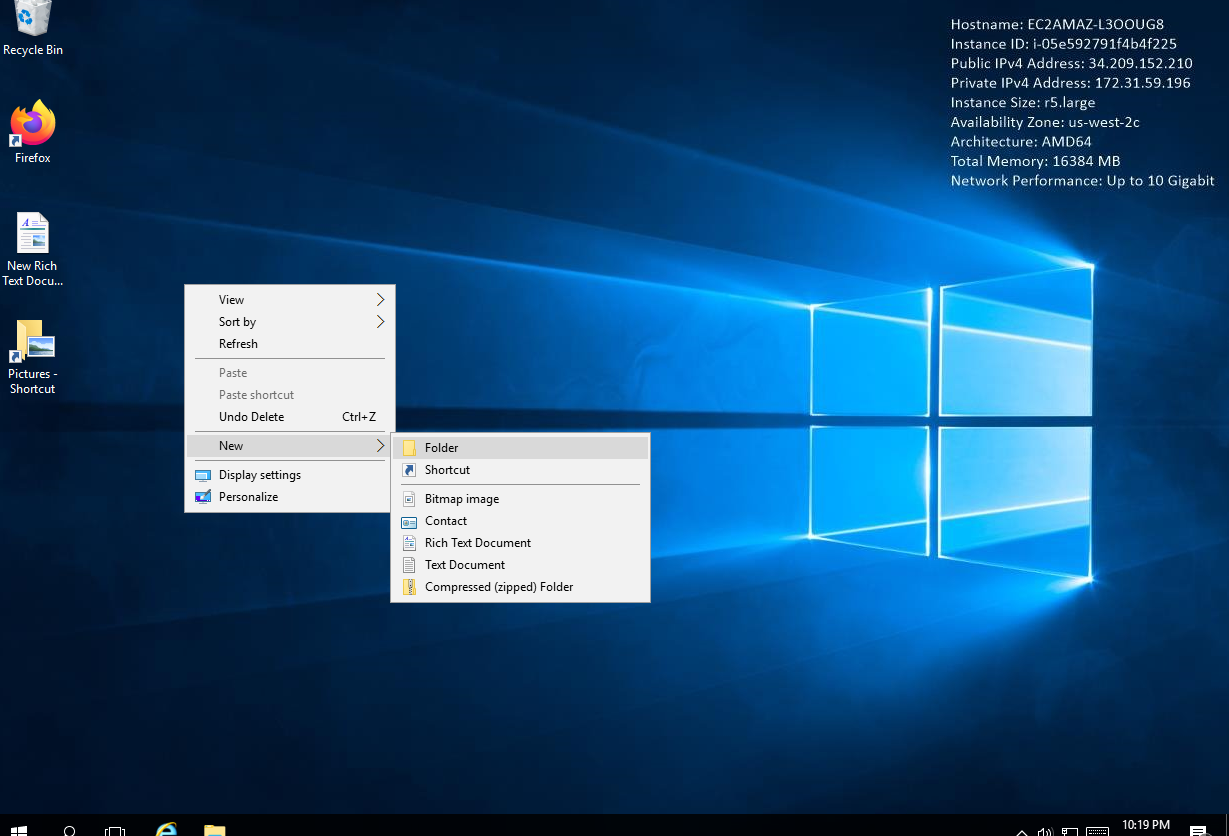


Double click inside the the policy and enable it \* if we also want to disable command prompt script processing change the dropdown tab to yes\*

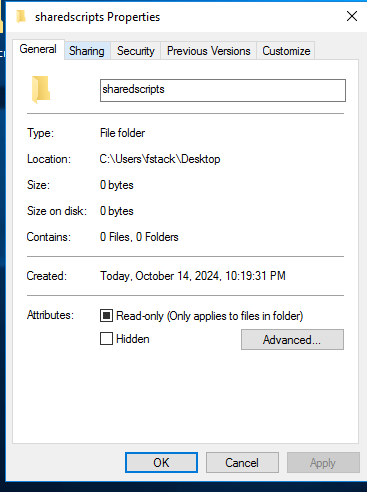


Now we need to create a bat script to map the shared folder. Begin with notepad and enter the following,

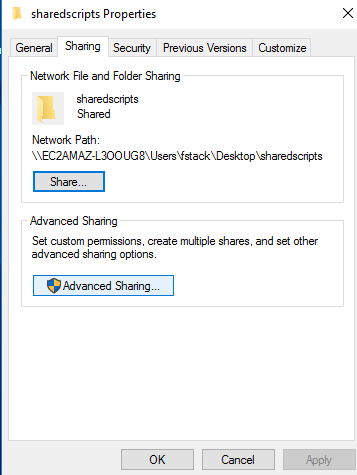


Now we need to save the script as sharedfolder.bat and save it in a shared folder so that it can be accessed. We will begin by creating a shared folder and changing the permissions to allow access by the users. 

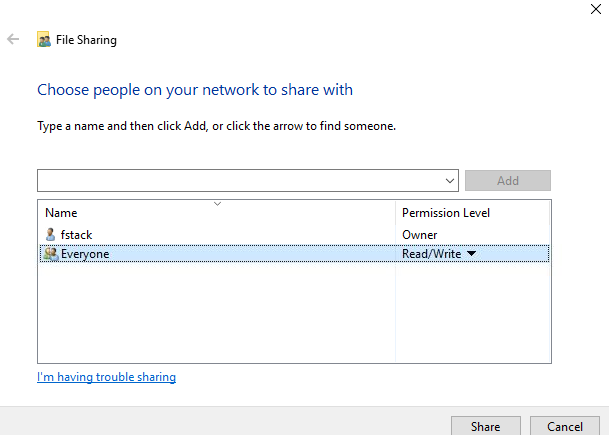
Now go into the sharing settings

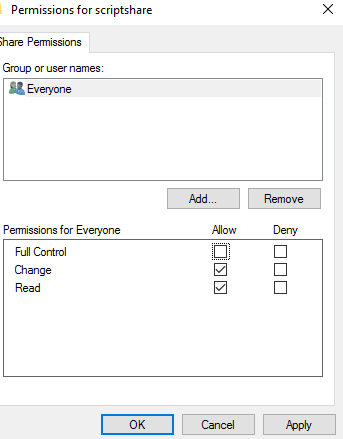


Now click on the advanced sharing options

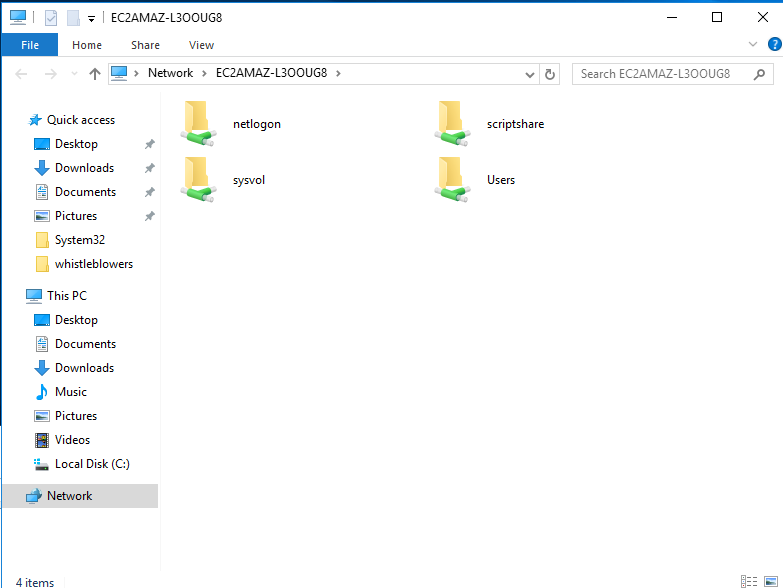


Give permissions to the folder

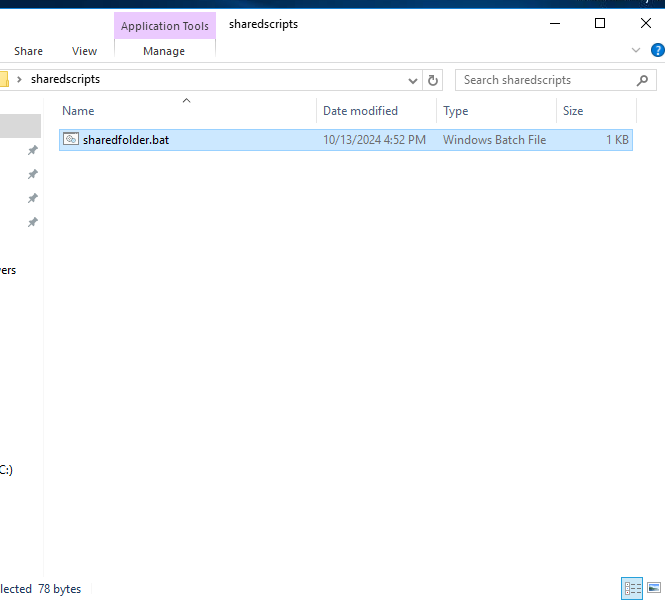




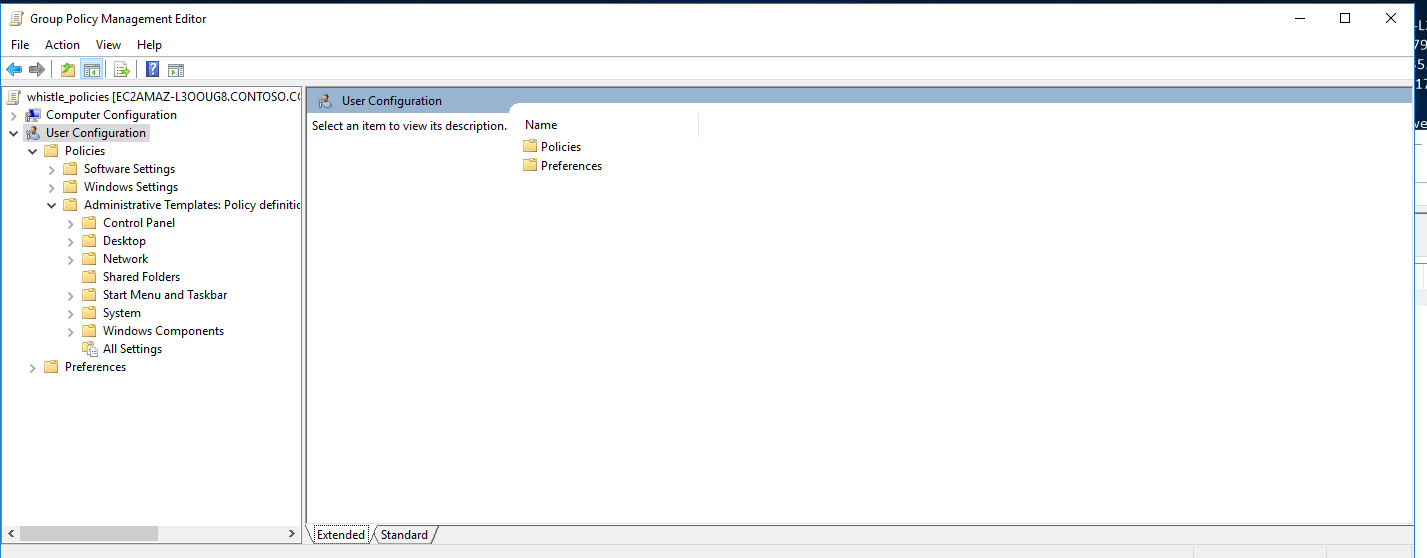
Now when you check network you should see our shared folder “scriptshare”



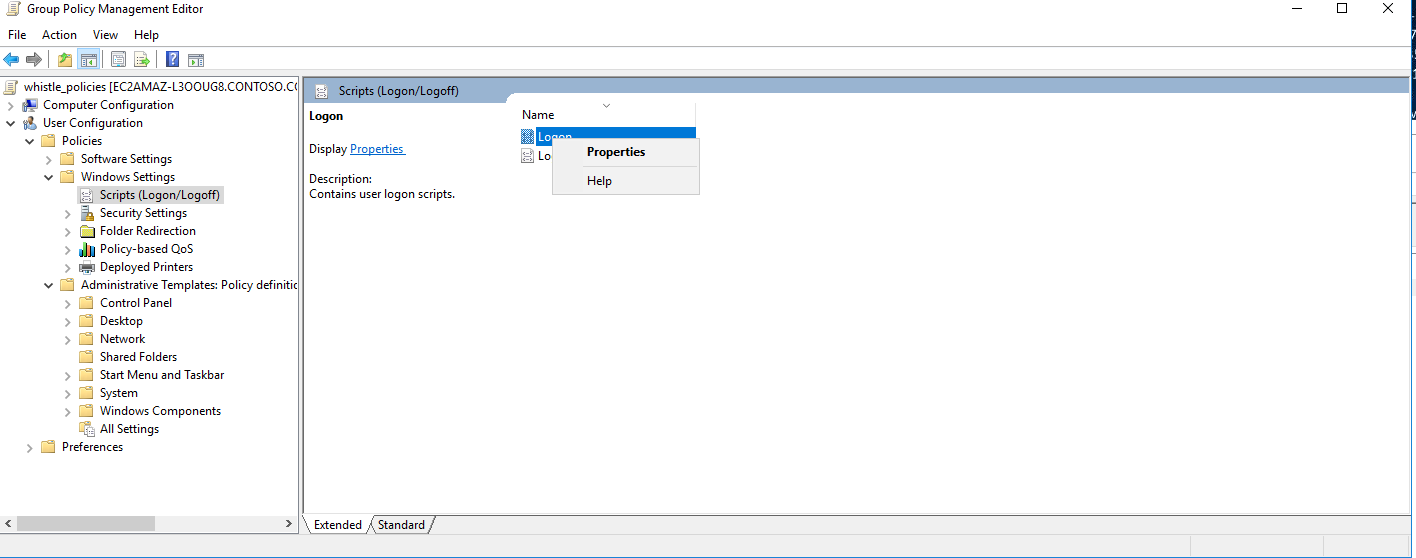
Now we need to copy the bat script into our shared folder



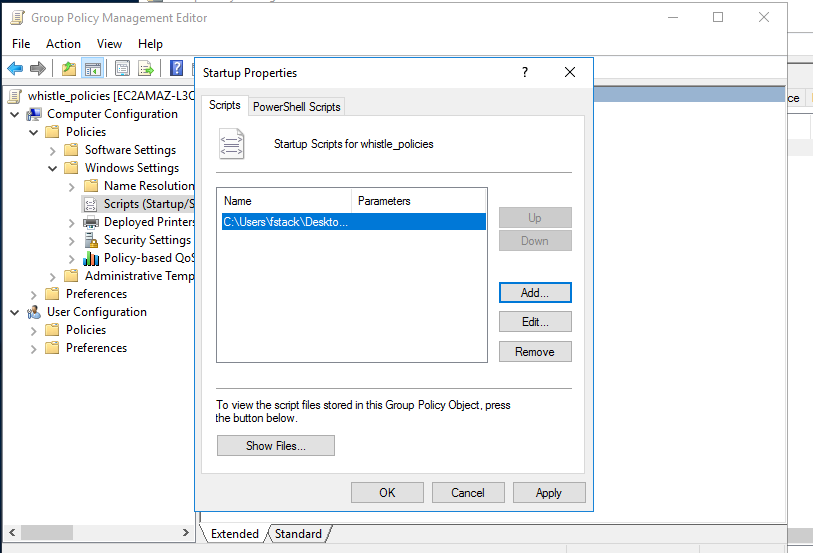
Now we need to apply the script to our GPO. User configuration > policies > windows settings > scripts



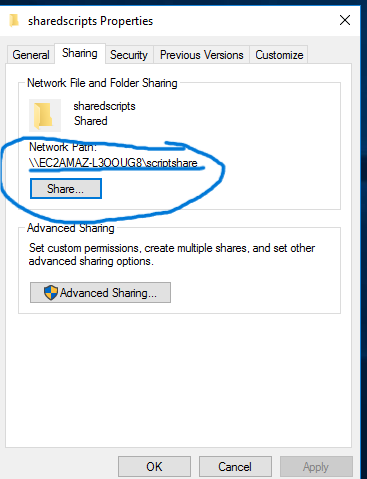
From here open up the properties.

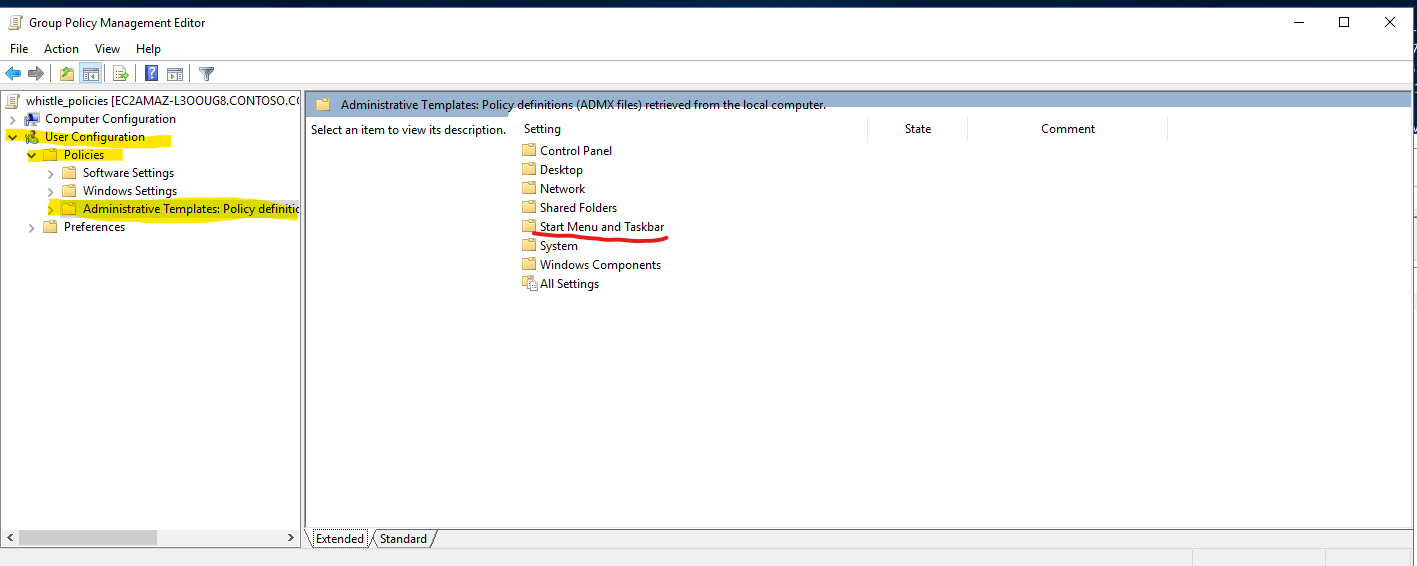


Click “add” and insert the script we created earlier.

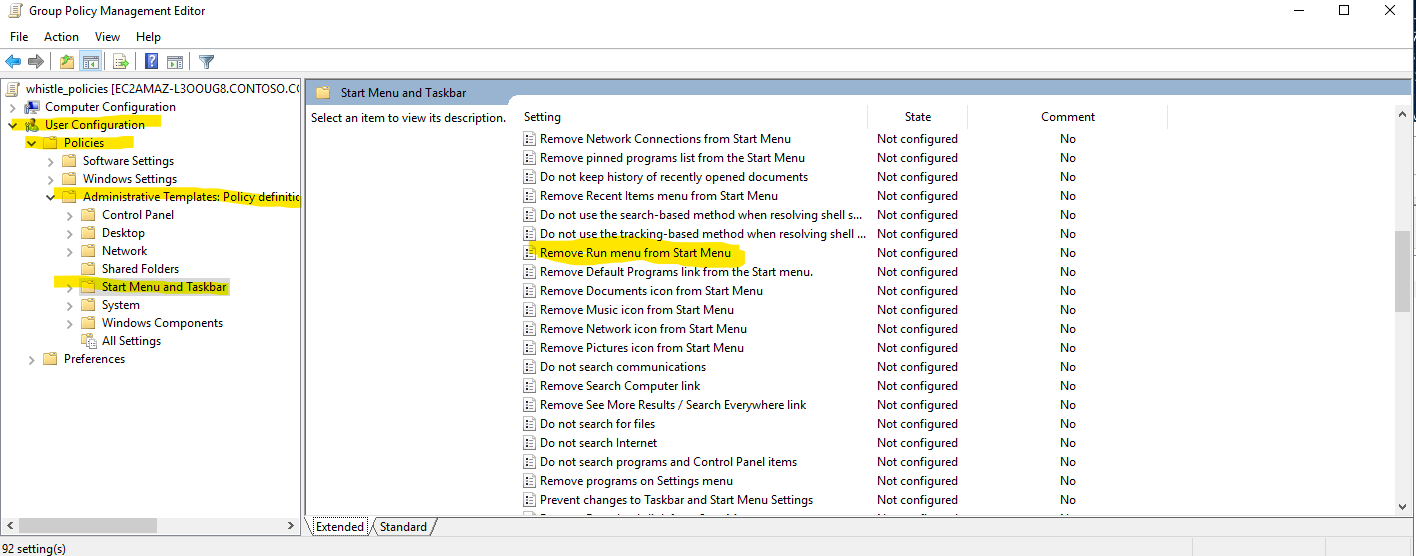


\*\*\*\*make sure to use the shared network path and not the :C drive \*\*\*\*\*\*\*\*\*

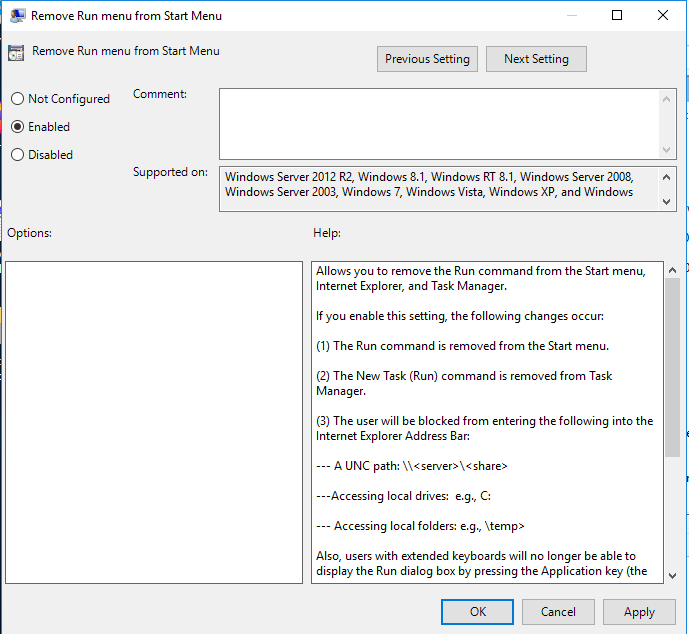


Apply the settings and ok. Now for our final step in this policy we need to disable the run command. In the same GPO we will head back to the user configuration > policies > administrative templates > start menu taskbar.

From here find the setting “remove run menu from start menu”

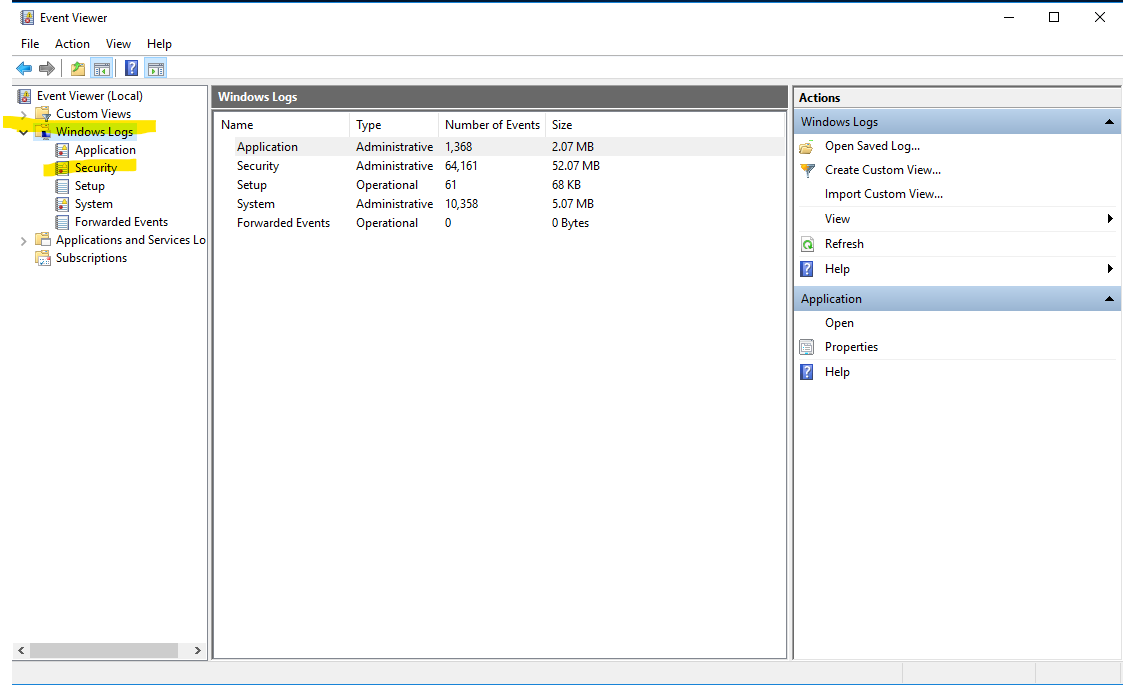


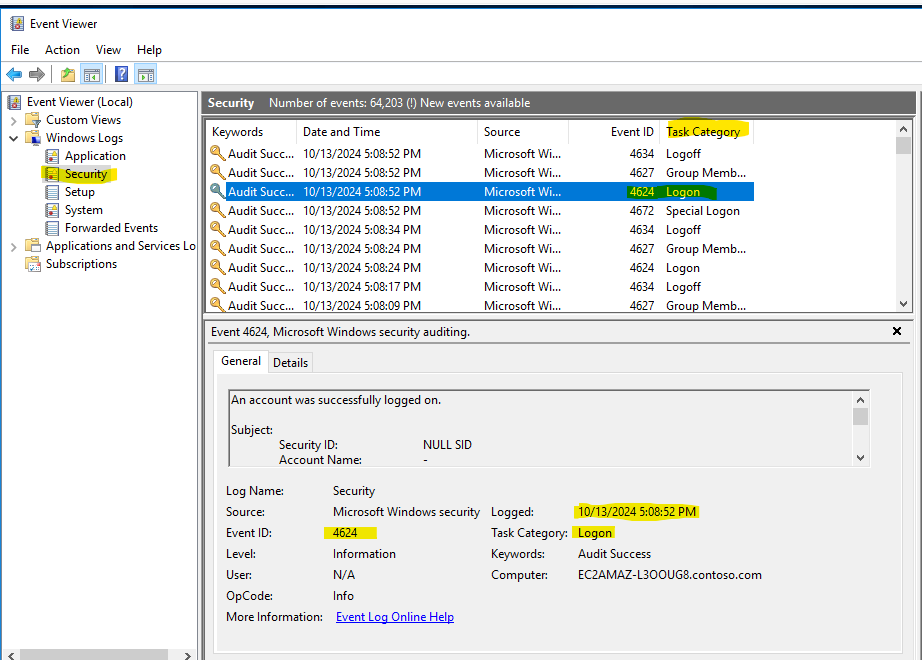
Click enabled , apply and then ok



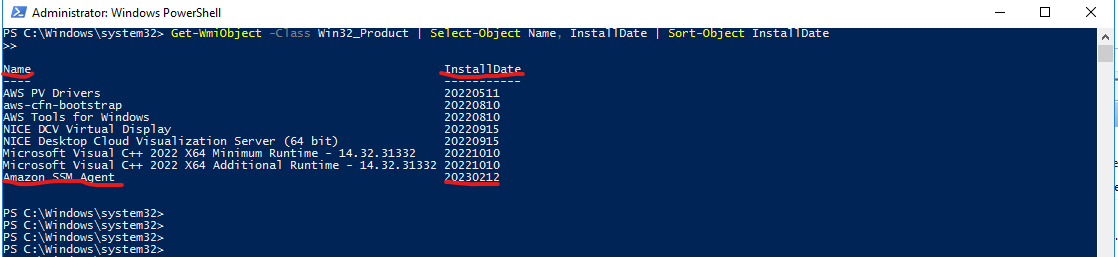
We have now successfully modified our GPO. To test everything has applied you can run a gpupdate on the server and then login to the accounts to verify the changes

**Step 7**:Check the Event Viewer on the server machine. We will begin by running event viewer and heading to windows logs> security . here we will find security related events including logons.



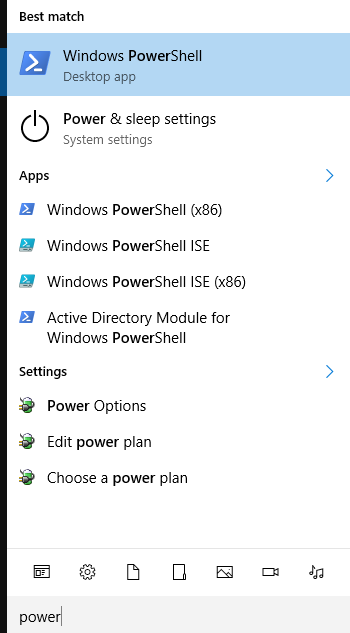
Here we can see the task category “logon” and an event id 4624 which shows us a successful login. 

**Step 8**: Use PowerShell to check what the latest program installed on the computer was. We will begin by launching elevated powershell.once inside power shell we will enter the following command to list all programs installed by their dates. Get-WmiObject -Class Win32\_Product | Select-Object Name, InstallDate | Sort-Object InstallDate



Here we can see the “amazon ssm agent” was installed 12/02/2023

Step 9:Write a PowerShell script that gives a list of all running services and puts it in a file named running\_services.txt. We will begin by opening powershell



From here we need to enter our script

– Get a list of all running services

$runningServices = Get-Service | Where-Object { $\_.Status -eq 'Running' }

–Target desired properties

$runningServices | Select-Object DisplayName, Status, Name | Format-Table -AutoSize

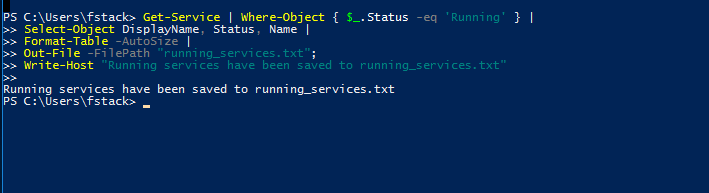
– Export the running services to a text file

$runningServices | Select-Object DisplayName, Status, Name | Out-File -FilePath "running\_services.txt"

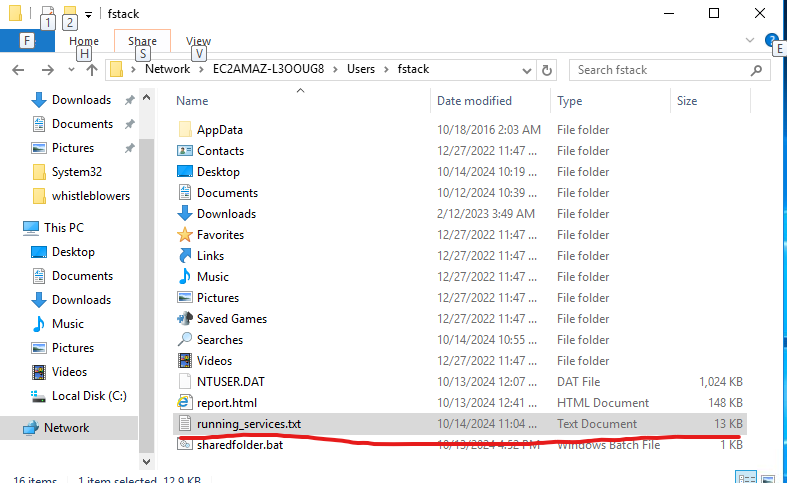
Now we can pipe this entire command into powershell and run it.

Get-Service | Where-Object { $\_.Status -eq 'Running' } | Select-Object DisplayName, Status, |

Format-Table -AutoSize | Out-File -FilePath "running\_services.txt";



Now we can observe the saved txt file



And if we pop inside well see all the running services saved as txt file

