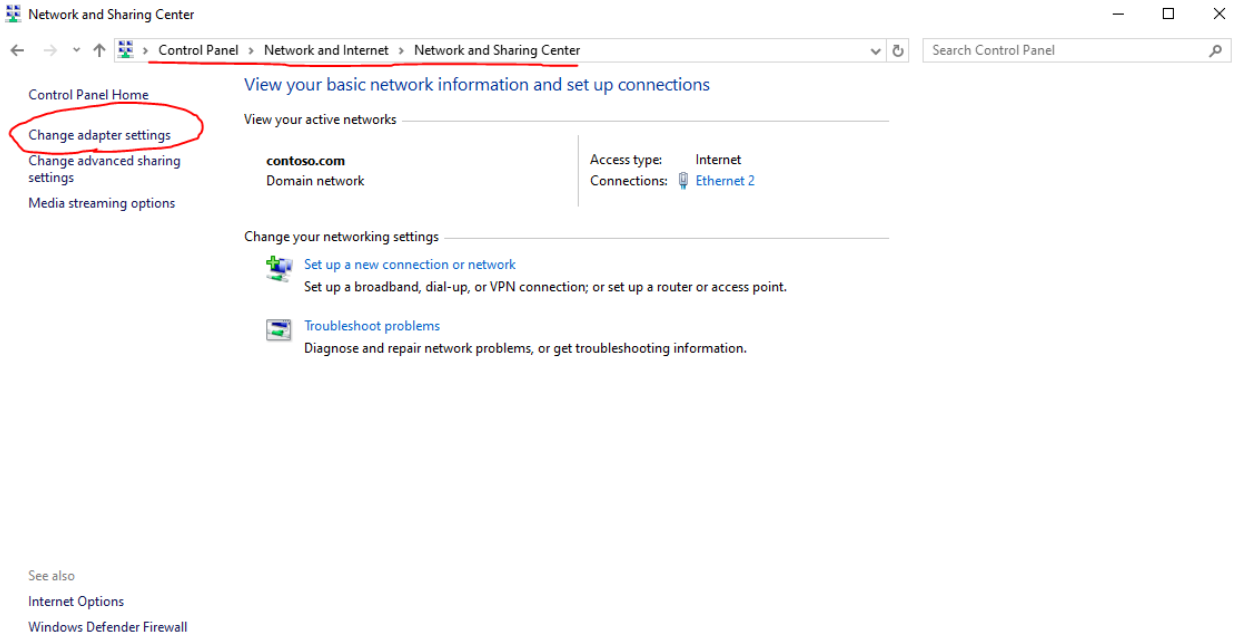
Objectives

- Join a computer to a domain
- Create a new user, group and shared folder for a new department
- Create and apply permissions to an organizational unit in the active directory based on the new department and its users
- Edit the group policy to restrict access and map the shared folder
- View the last successful login
- View the latest program installed
- Write a Powershell script that gives a list of all running services

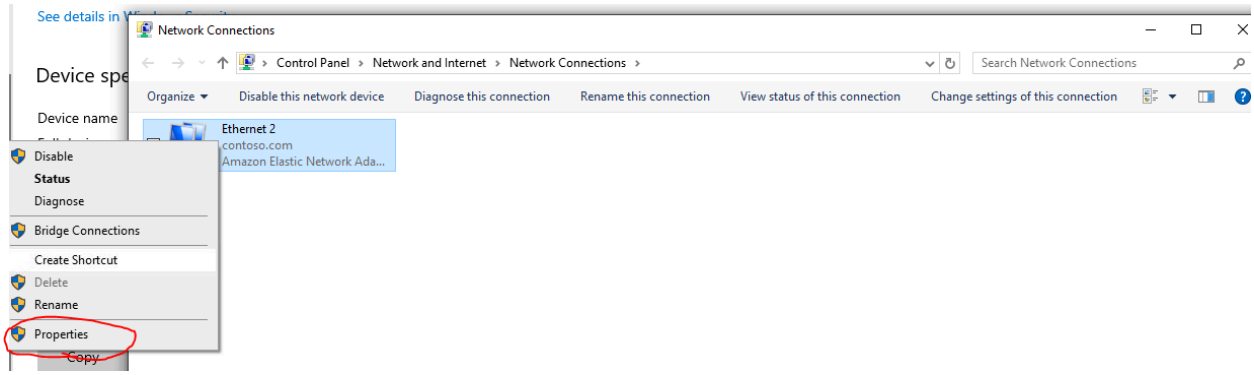
Procedures

Step 1.) Join a computer to a domain

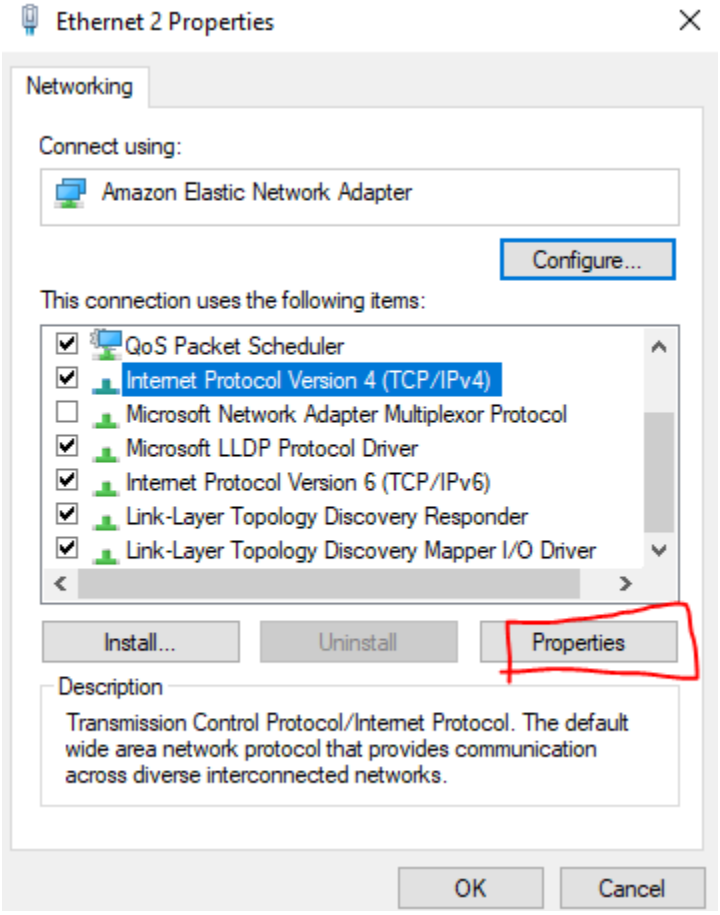
Go to the Control Panel - Network and Internet - Network and Sharing Center.



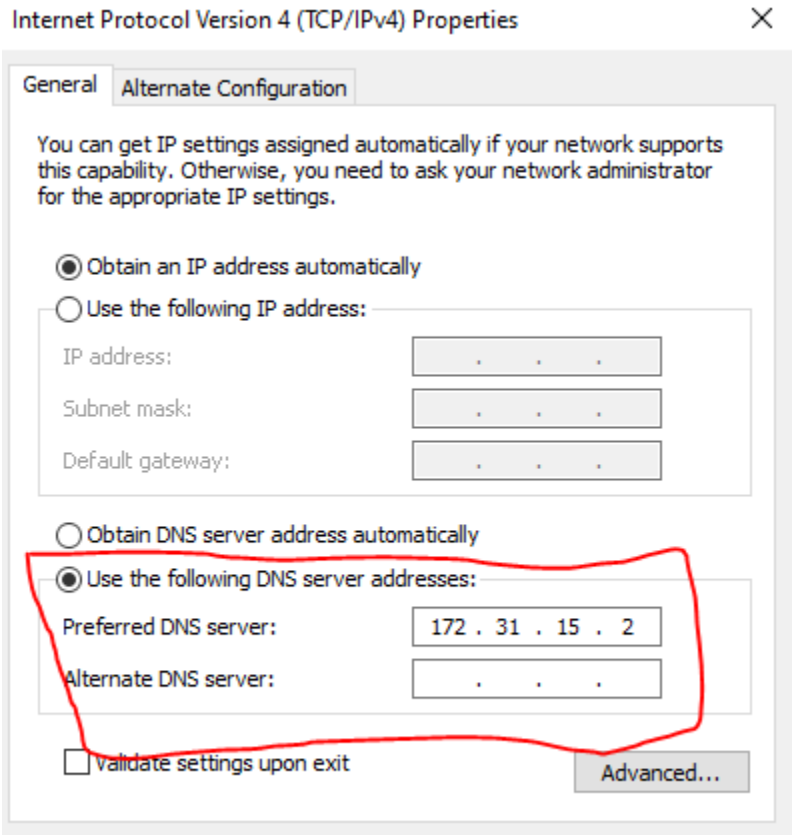
Next you will click on change adapter settings, and right click on Ethernet 2 and select properties.



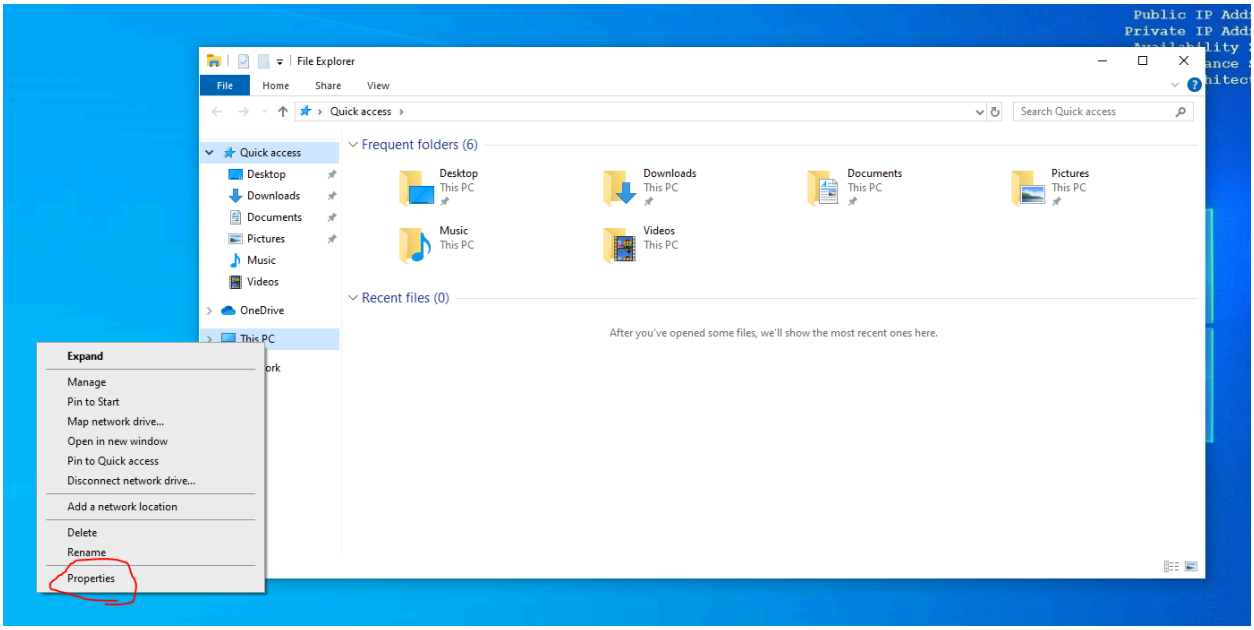
Locate the Internet Protocol Version 4 (TCP/IPv4) and select properties



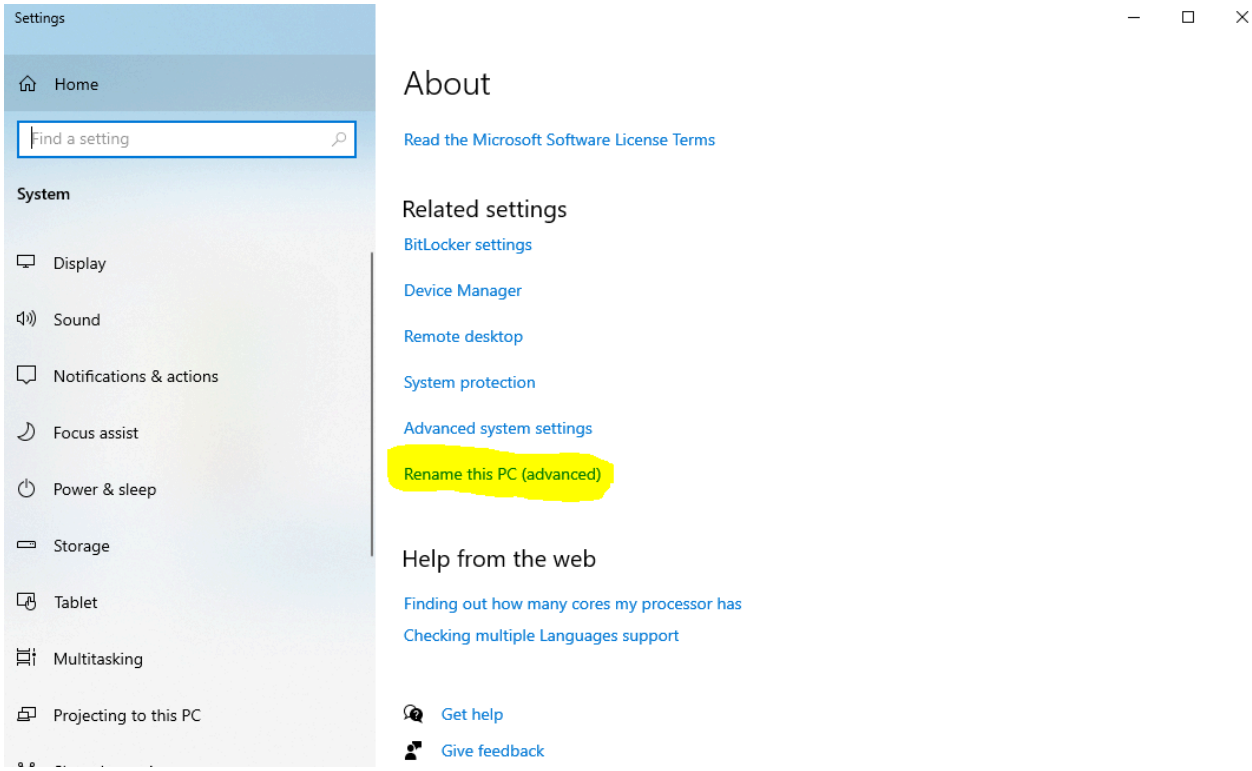
In this menu, you will want to use the Private IP of your server as the Preferred DNS Server.



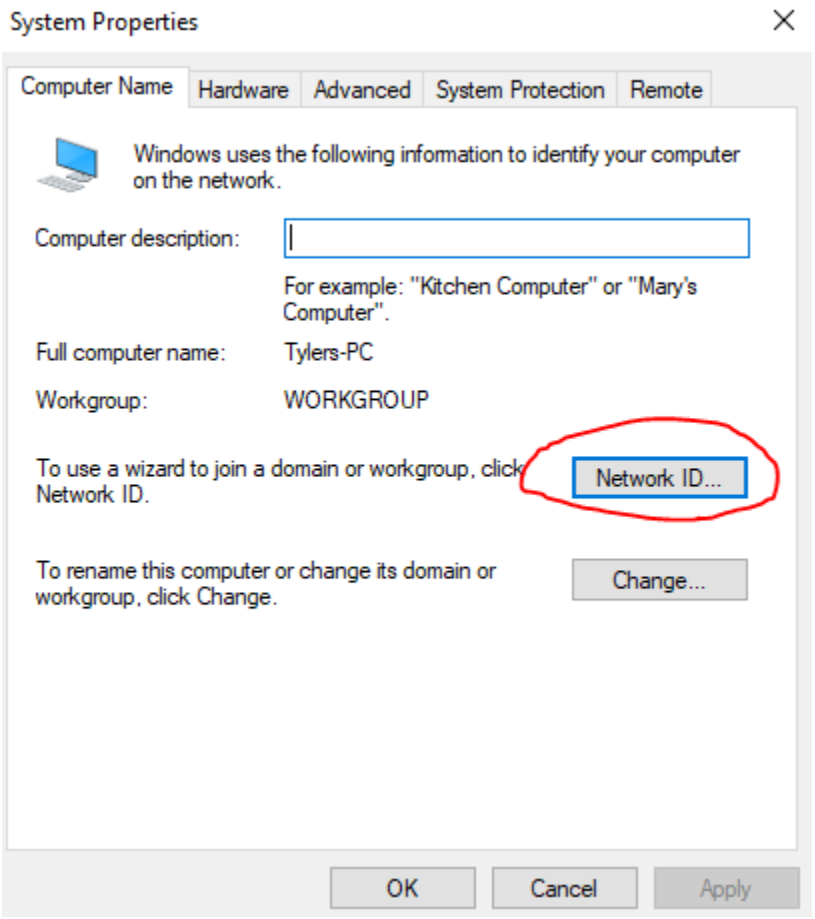
Now you will want to go to ‘This PC’ in file explorer and right click and select Properties



Here you will scroll down until you see ‘Rename This PC (advanced)’



Next, click on ‘Network ID’



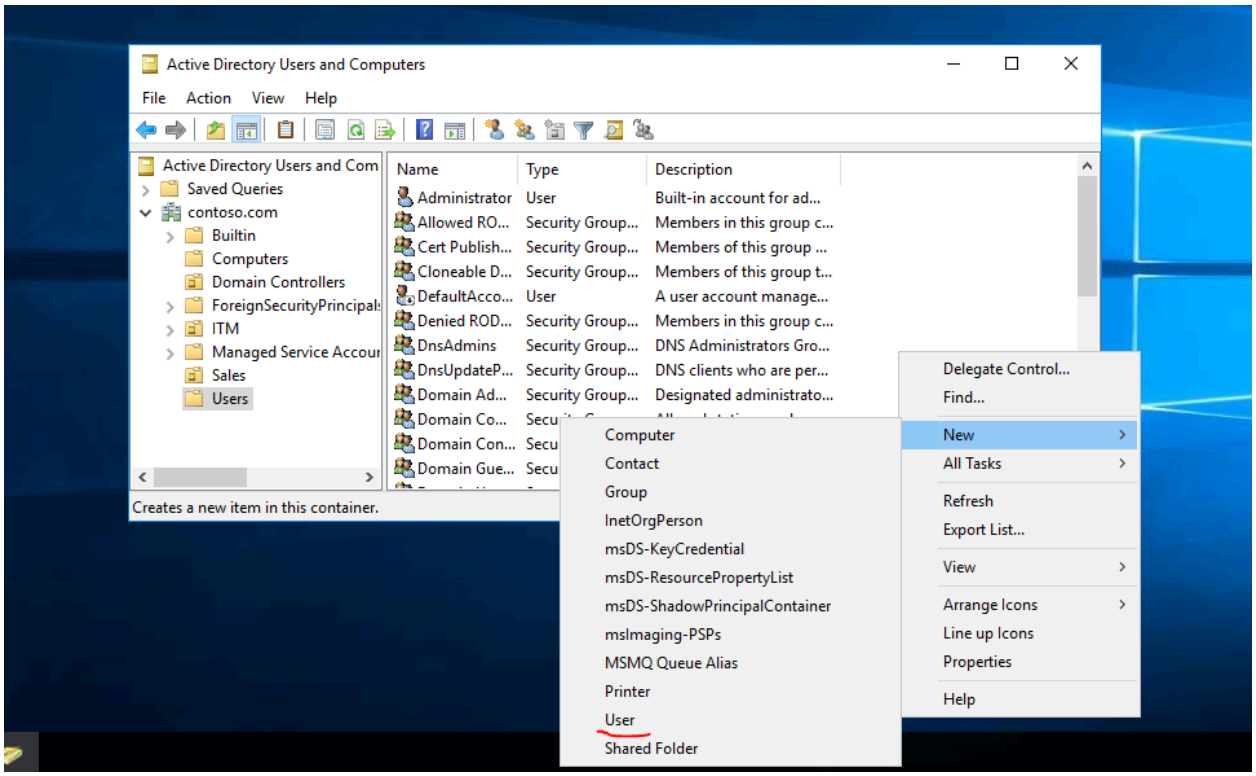
Here you will enter the username and password as well as the domain you wish to connect to

You will be asked again for your username and domain, enter the required fields and click next. Lastly, you will be prompted to enter the username and password to your domain and when input, you will be connected to the domain.

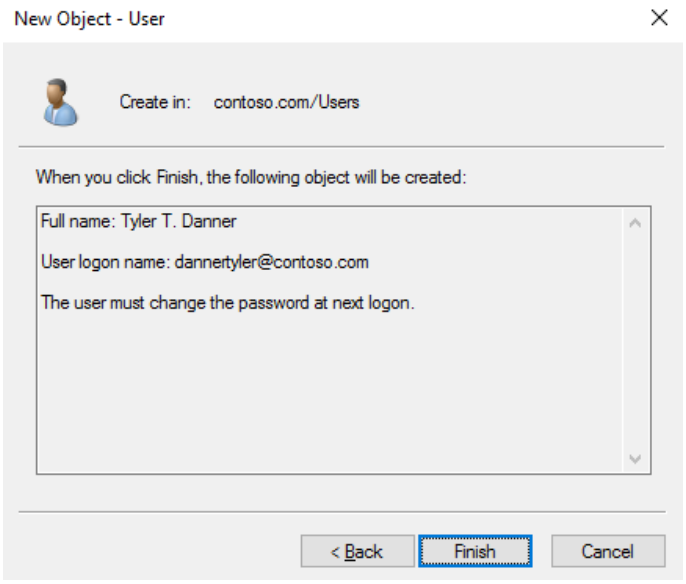
Step 2.) Create a new user, group and shared folder for a new department

Log in to the server and open the Active Directory Users and Computers

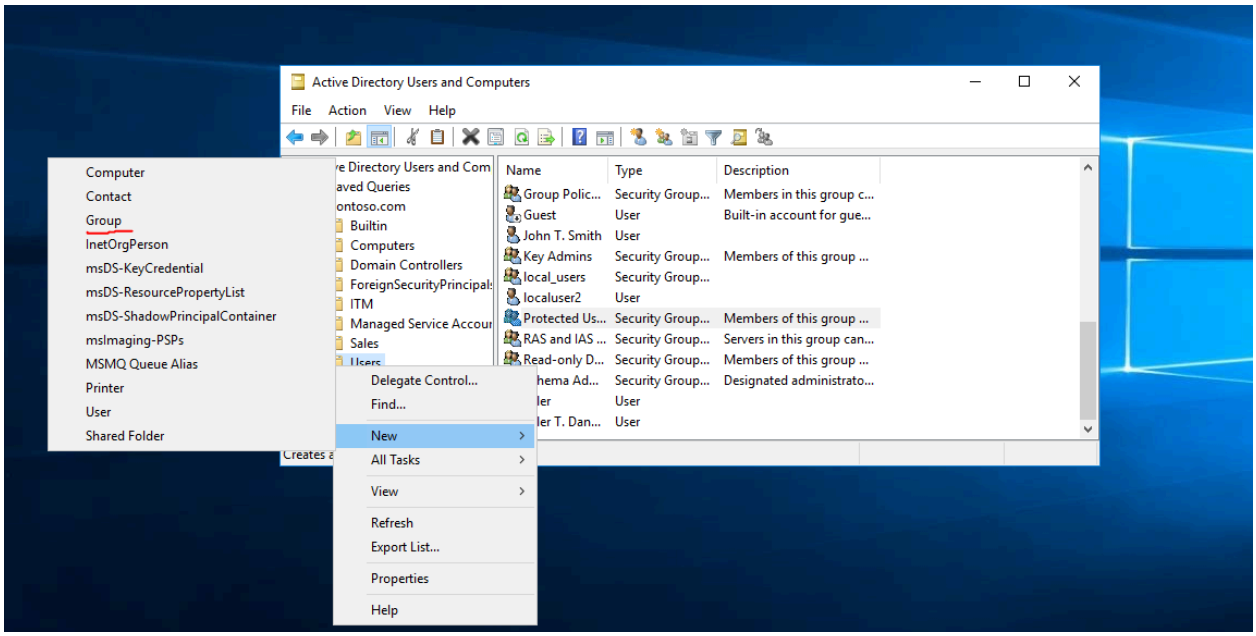
Next you will click into the Users under contoso.com, then right click, New - User



You will be prompted to enter the users first and last name, password, and their login name for the domain. Select the option to require the user to change the password on their first login.

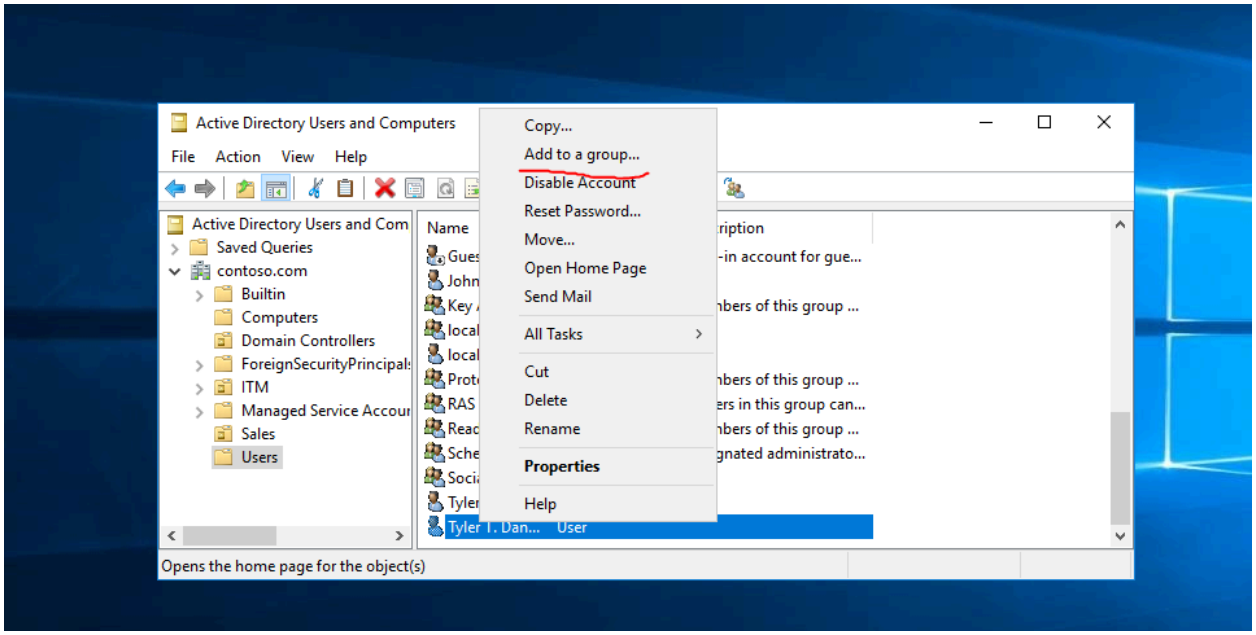


Next we will be creating a group for the new hires department. To do this, right click on the Users Organizational Unit, and select New - Group

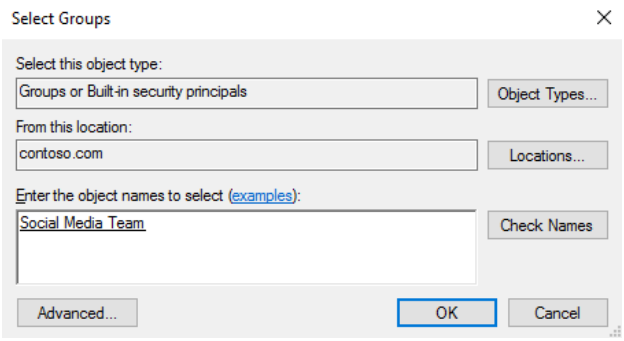


Name the group the same as the department the new hire will be working in.

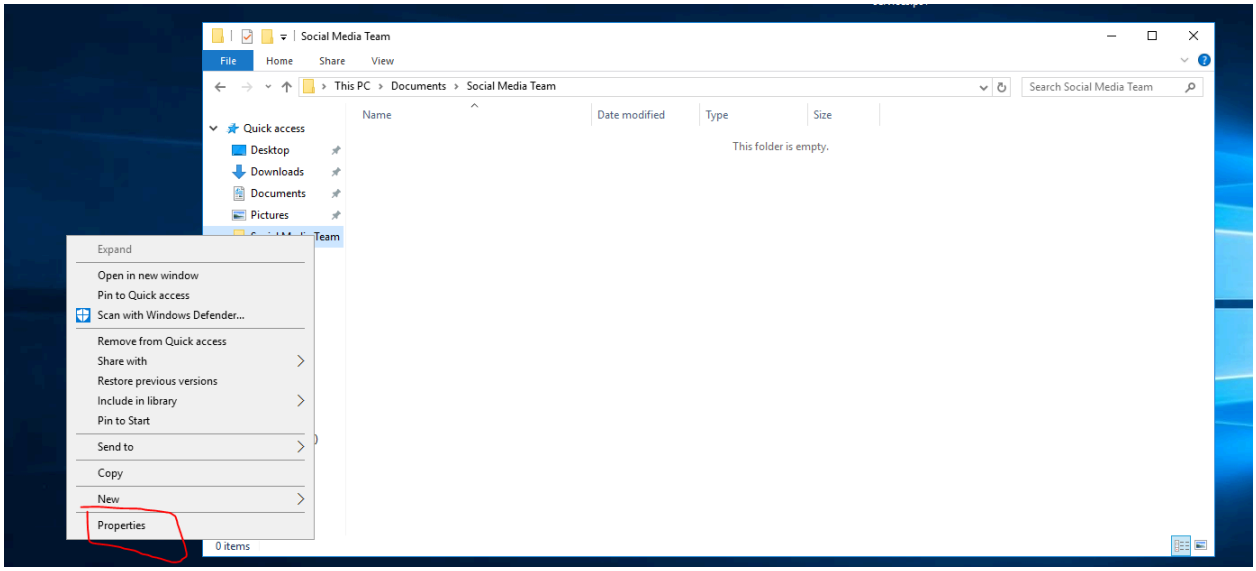
Next we will be adding the new hire into their respective group.
Right click on the new hires user we just created and click ‘Add to Group…’



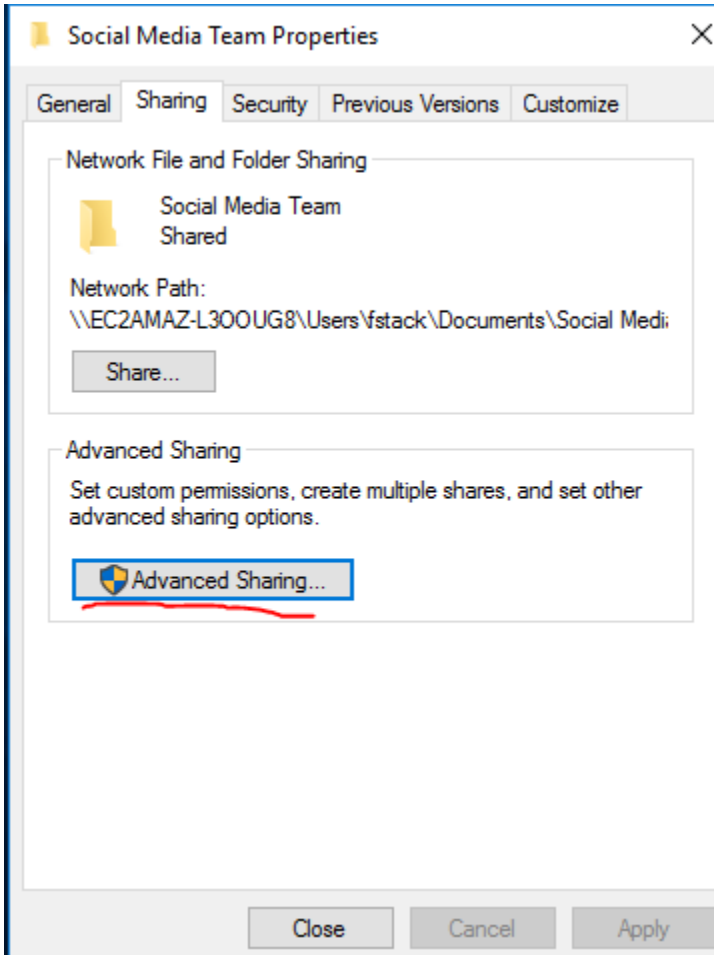
From here, you will type in the department/group that we just created and select it. Then click ok.



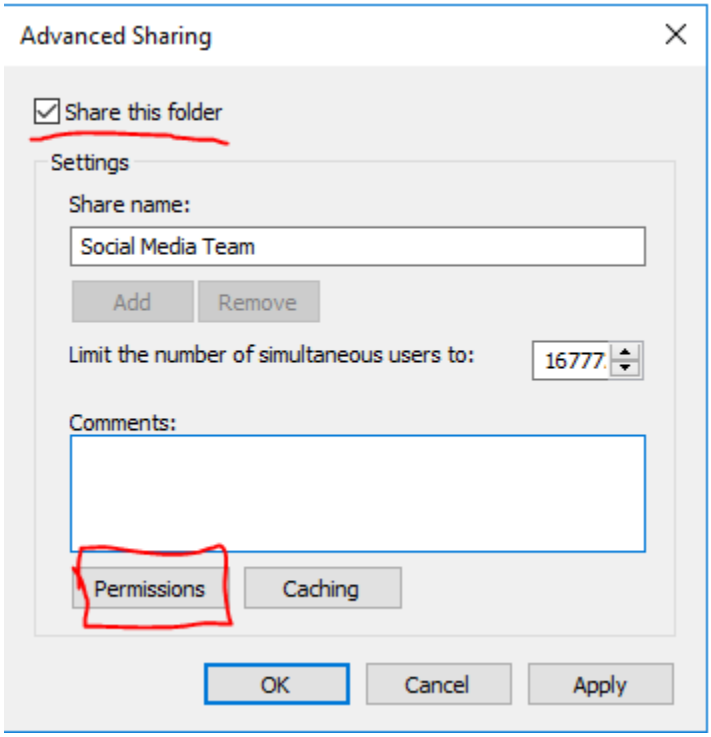
Now we will be creating a shared folder for the new group we just created.
Open file explorer and create a new folder with the name of the group/department.
Next right click on the folder and select properties.



Once in the properties, select the ‘Sharing’ tab and click on ‘Advanced Sharing’

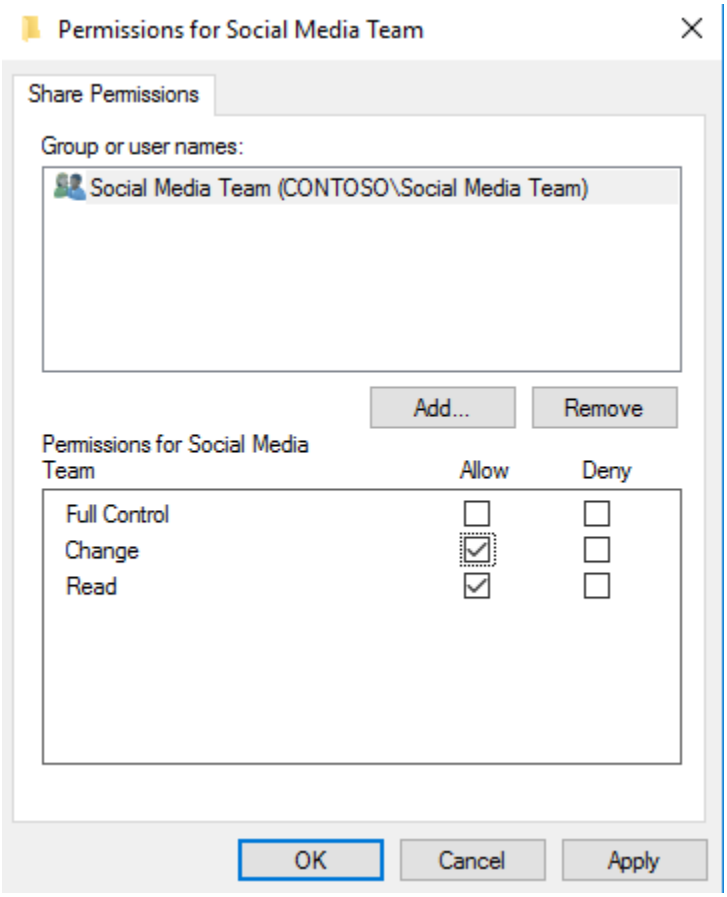


Enable the ‘Share this folder’ option and click on permissions

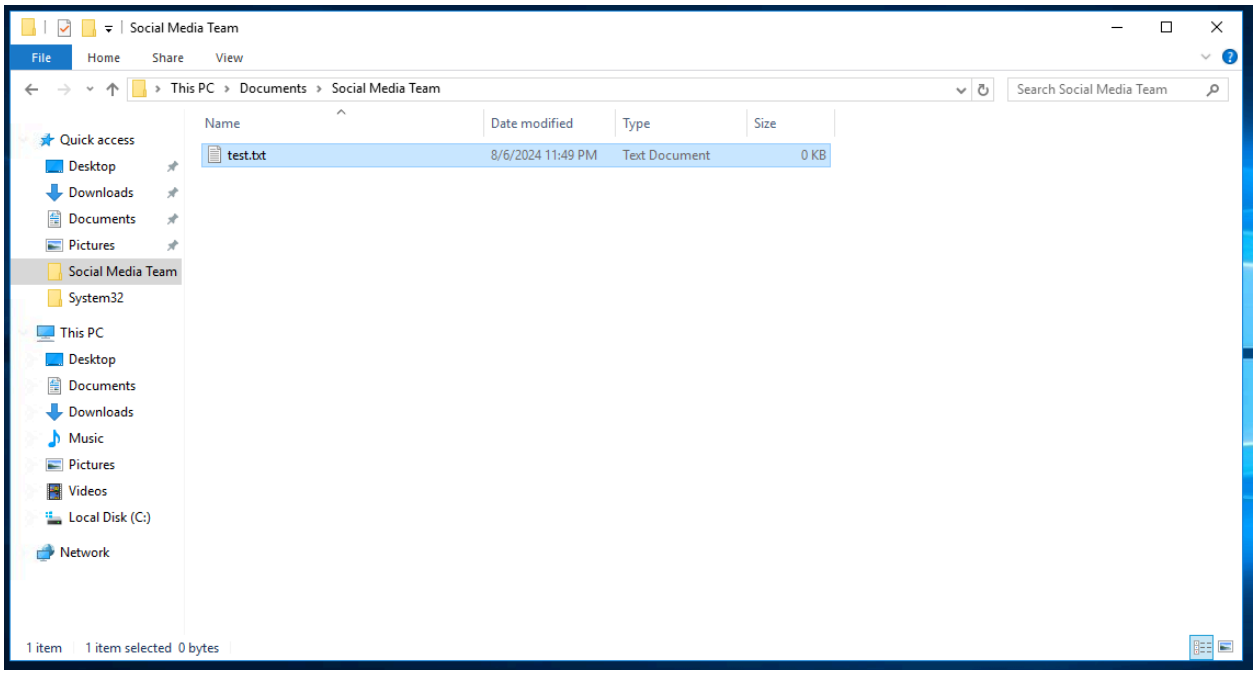


Under ‘group or user names’ remove ‘Everyone’ , then click ‘Add’ and select the group that we created for the department

Next, you need to give the group change and read permissions, so click ‘Allow’ on both.

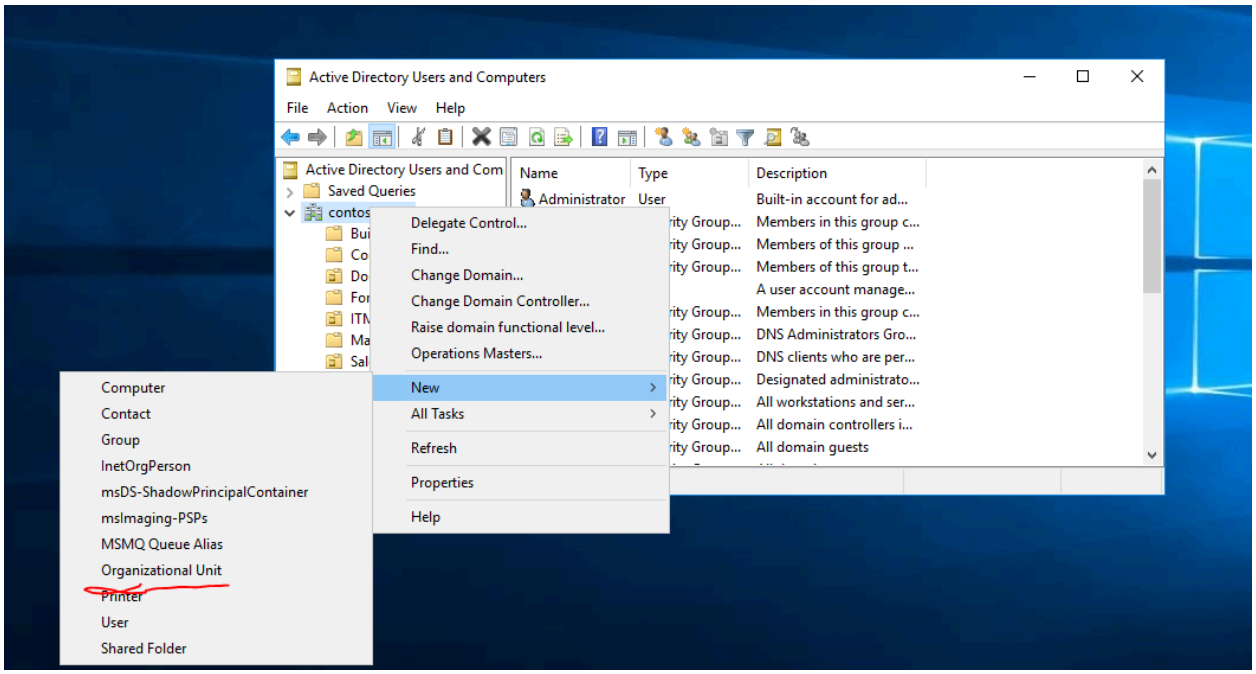


Lastly, we will create a test document to ensure we have successfully created a shared folder for the group.

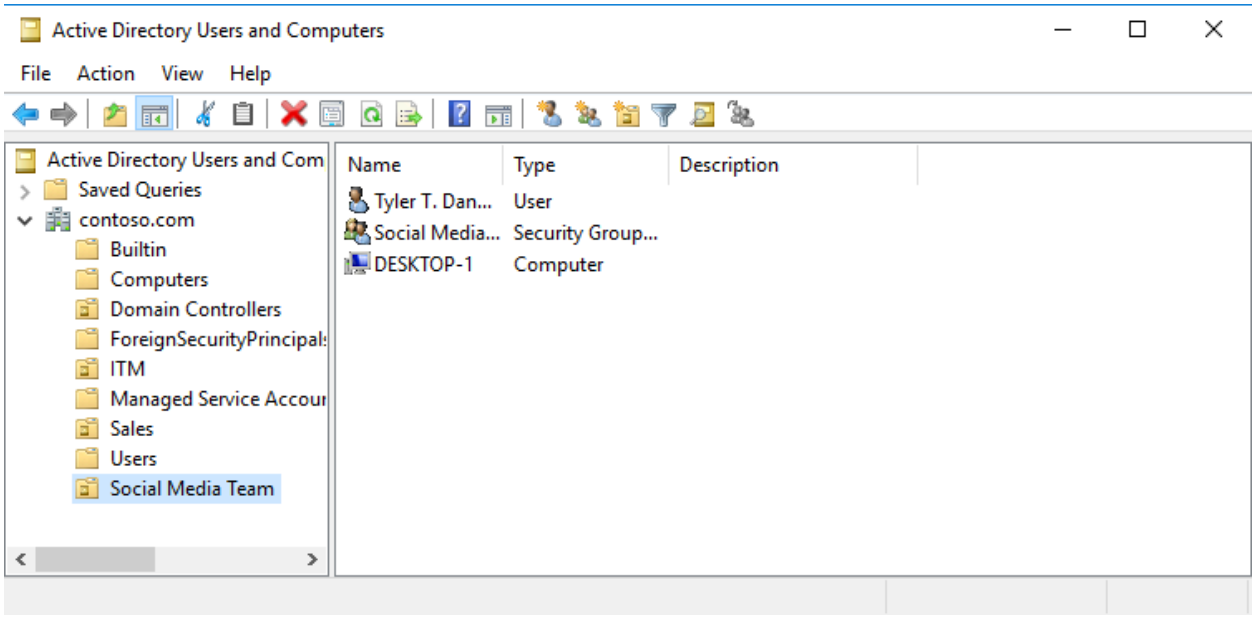


Step 3.) Create and apply permissions to an organizational unit in the active directory based on the new department and its users

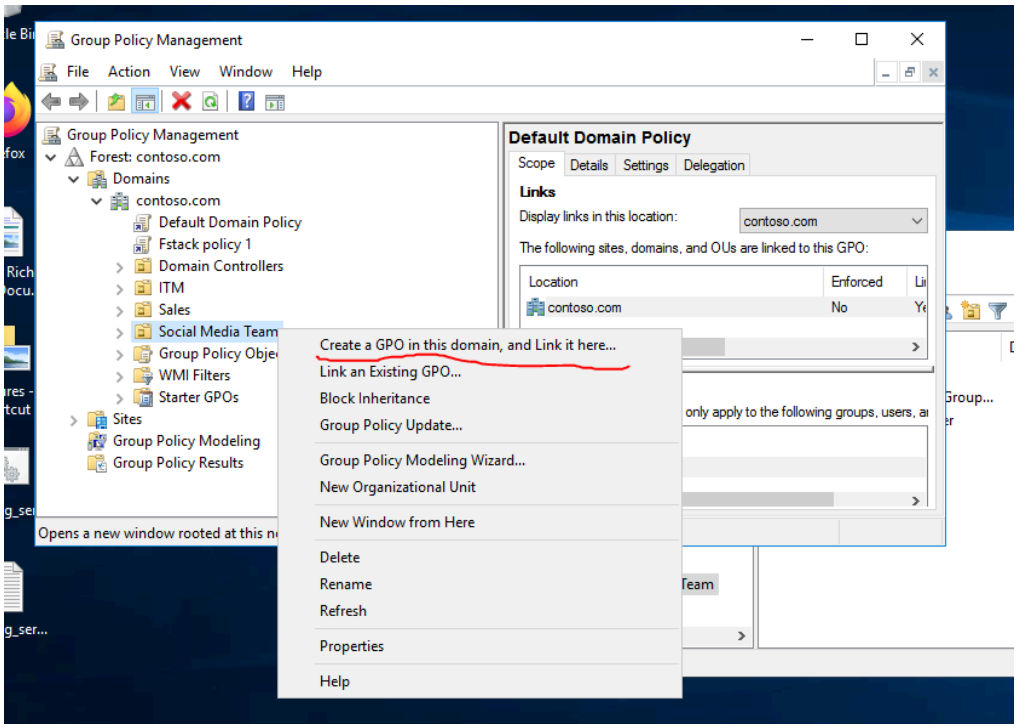
Next we will be creating an Organizational Unit and attaching a Group Policy\
Open the Active Directory, and right click on the domain. Hover over ‘New’ and then select the Organizational Unit.



Name the new organizational unit the name of the department and add the user, group and their computer. You can do this by simply dragging them from the Users OU to the New OU we just created.

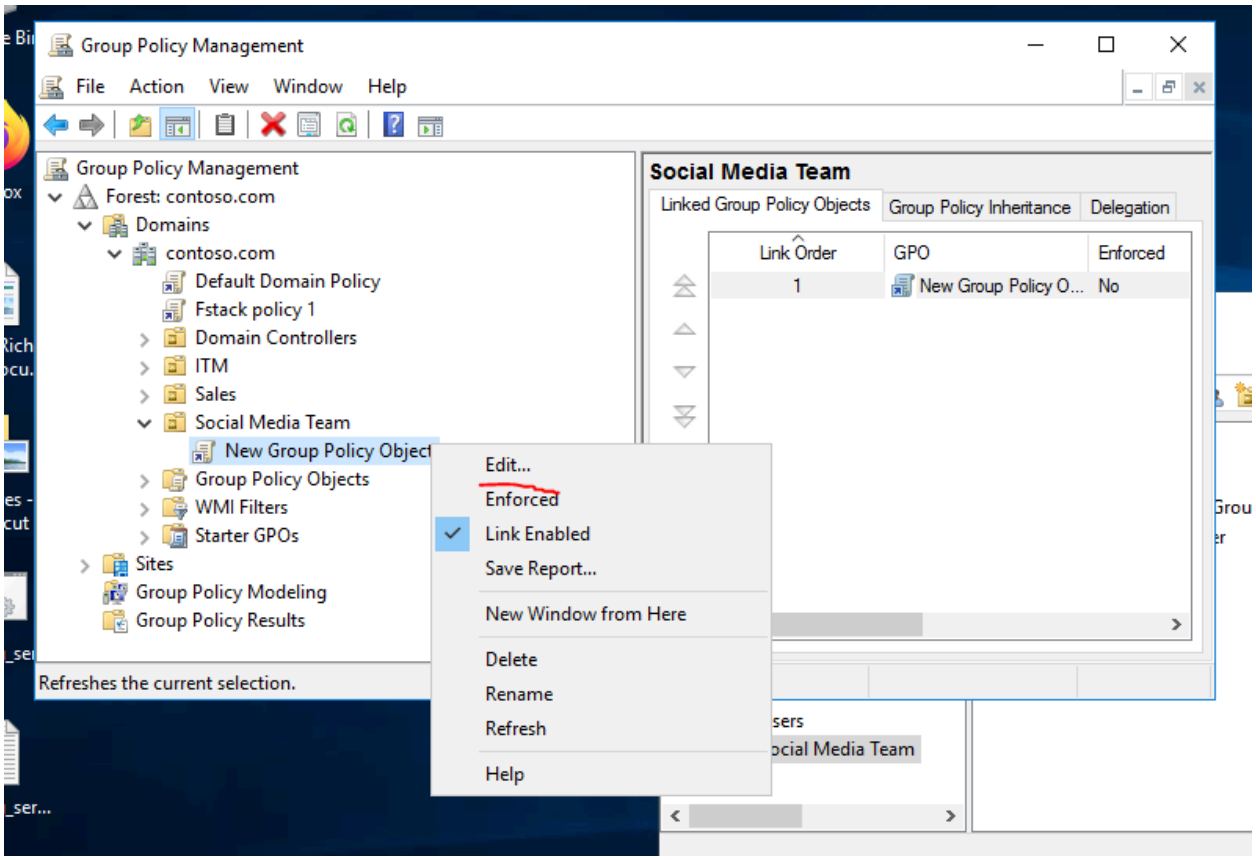


Next we will be creating the Group Policy. Open the ‘Group Policy Management’
Right click on the new OU that we just created and select ‘Create a GPO in this domain, and Link it here…’

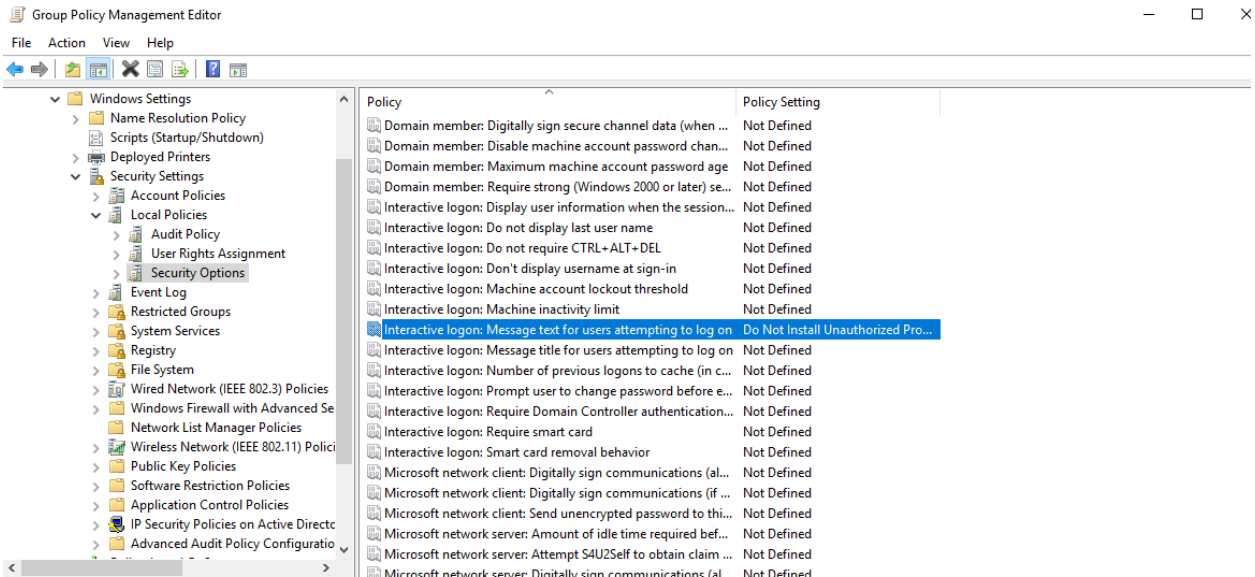


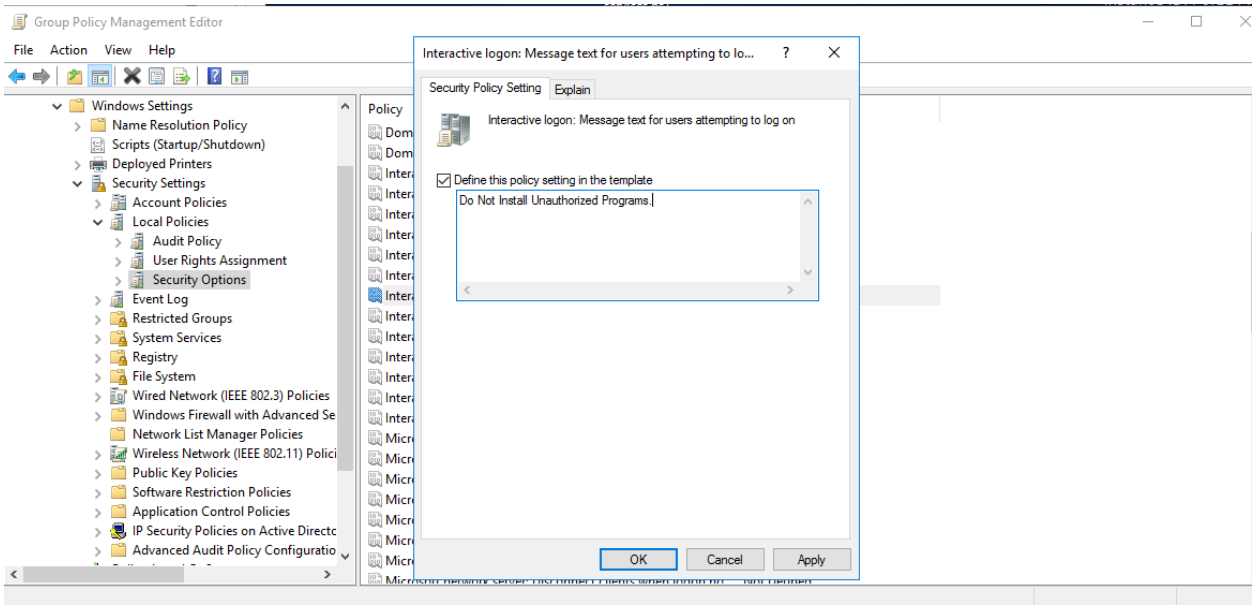
Step 4.) Edit the group policy to restrict access and map the shared folder

Next we will right click on the New Group Policy Object we just created under the OU of the department, and select ‘Edit’

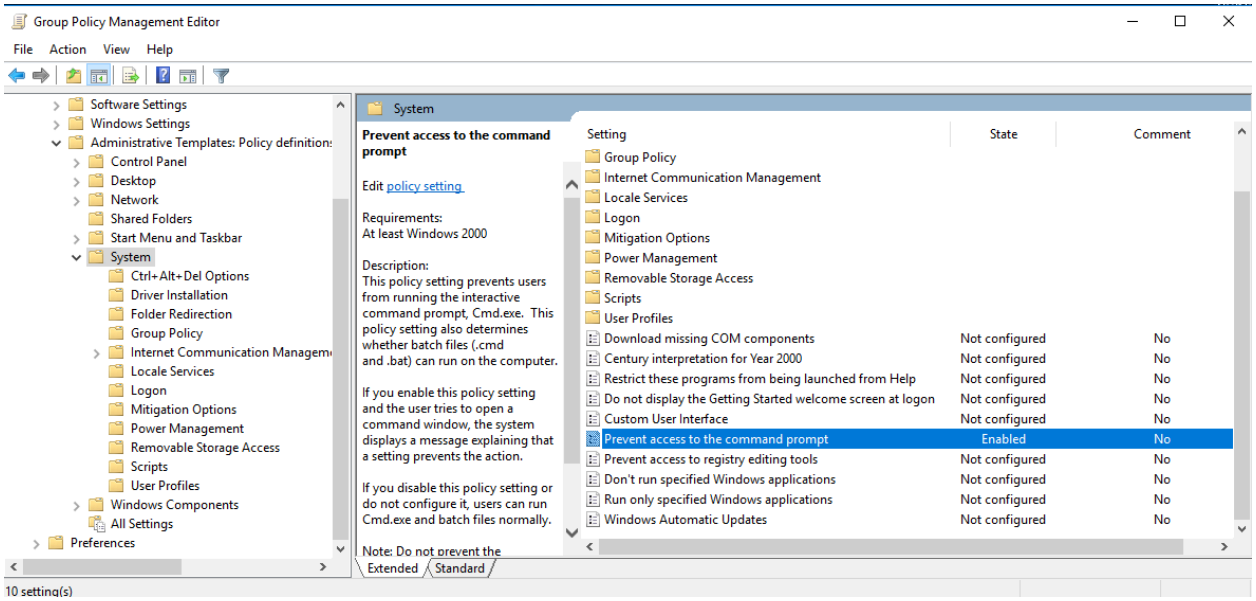


Our first policy we need to apply is a startup message that states “Do not install unauthorized programs”
To do this we will go to
Computer Configuration - Policies - Windows Settings - Security Settings - Local Policies - Security Options . Here you will find ‘ Interactive Logon: Message text for users attempting to log on”
Define the policy and apply your changes.





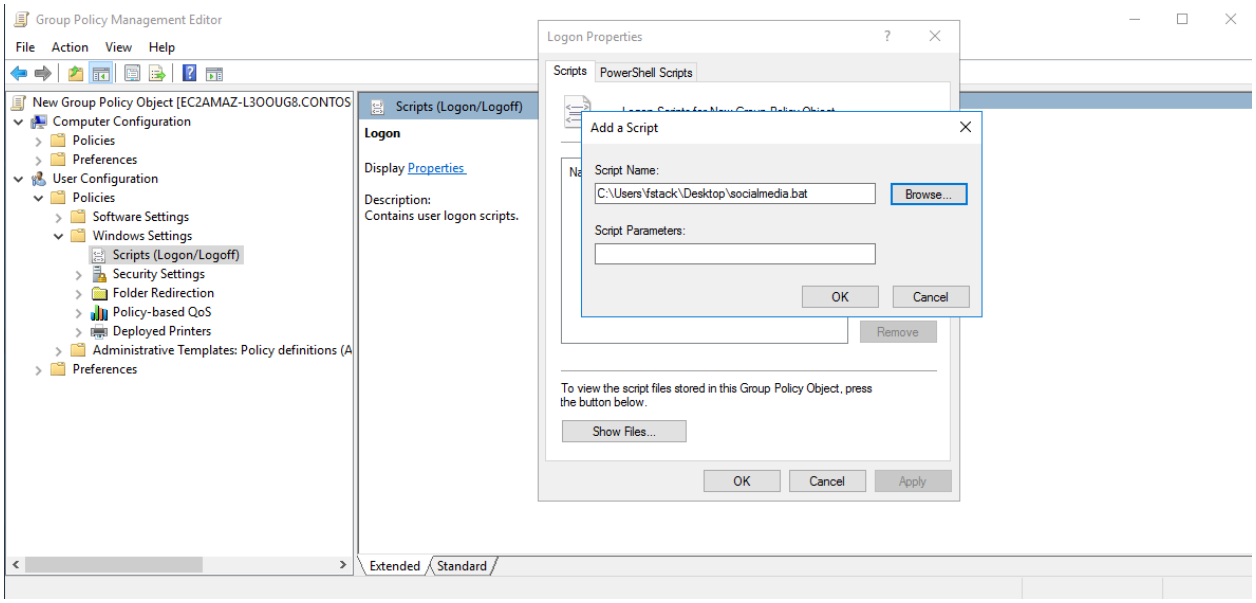
Our next policy to enforce is to prevent the user from using the Command Prompt. While in the group policy management editor, navigate User Configuration - Policies - Administrative Templates - System and enable Prevent access to the command prompt.



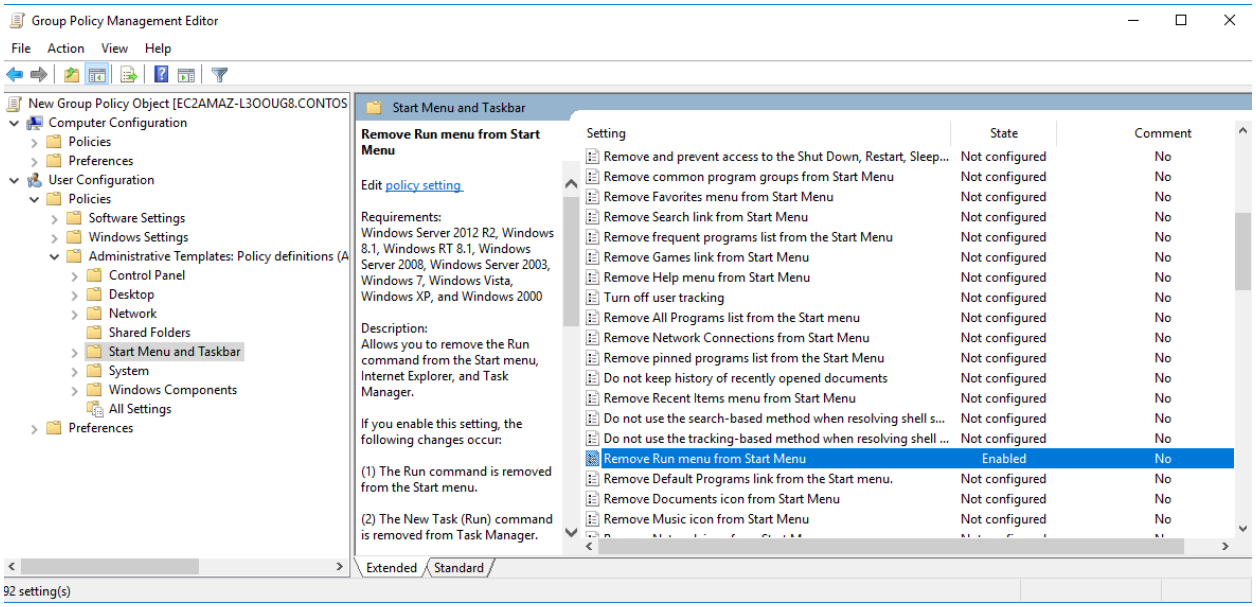
Our third policy is to write and apply a script that to the users login to map the share we created earlier. This can be done by creating a text document and entering ‘ Net Use (File Path of Shared Folder) ‘ and saving this and a .bat file.

To apply the script we just created when a user logs on, navigate from the group policy management editor User Configuration - Windows Settings - Scripts (Logon/Logoff) - Logon

You will need to browse your files and select the script you just created and apply.

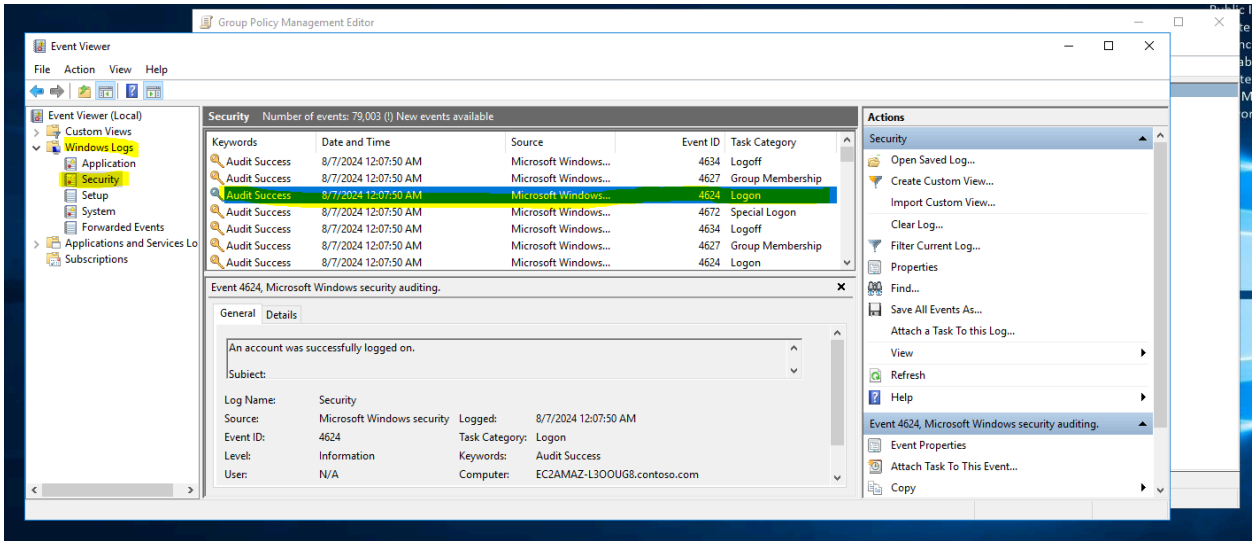


Our last group policy will be to disable the run command. While still in the group policy management editor, navigate User Configuration - Policies - Administrative Templates - Start Menu and Taskbar. There you find Remove Run menu from Start Menu, select enable.



Step 5.) View the last successful login

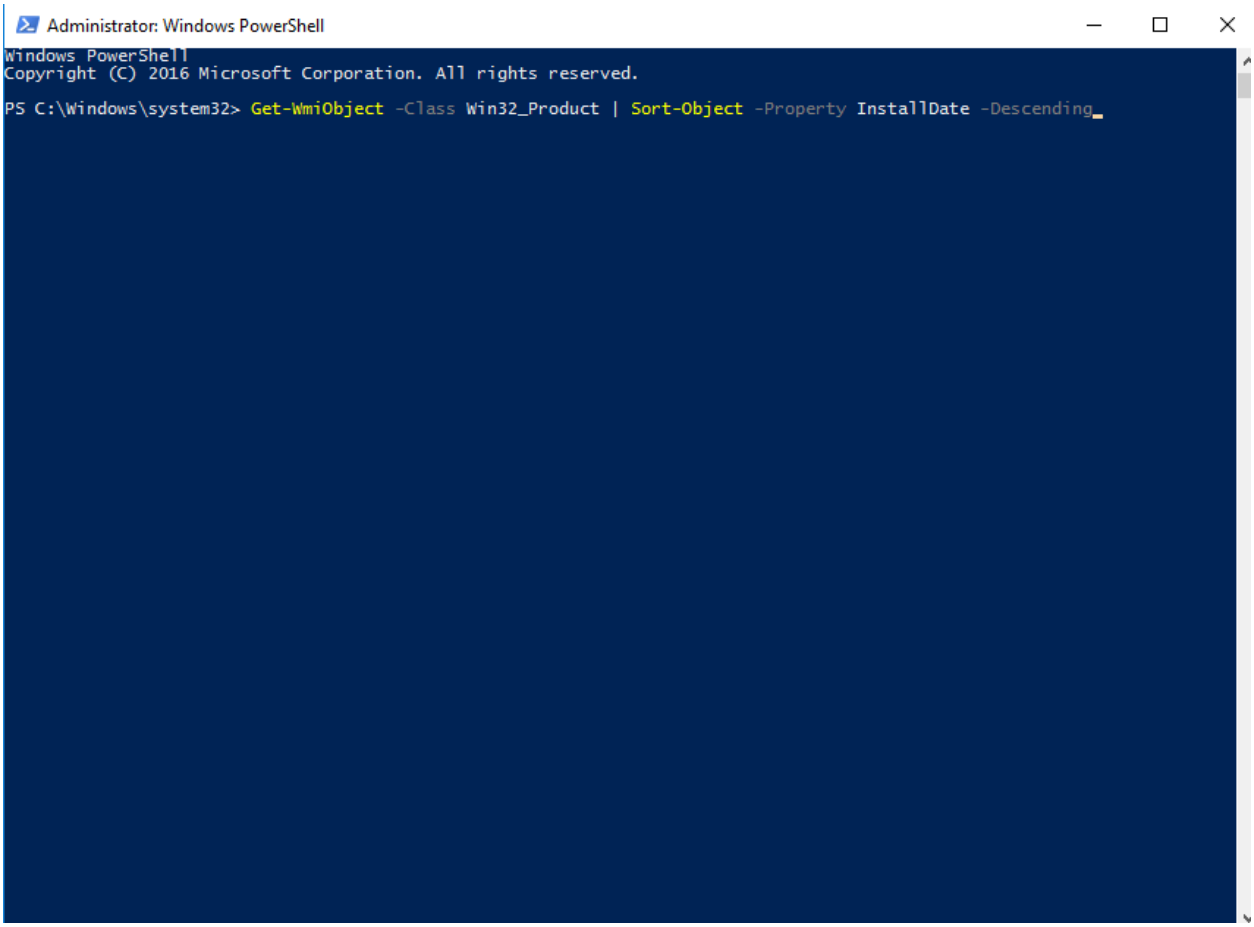
To view the last successful login we will be using Event Viewer. With Event Viewer open, navigate to Windows Logs - Security

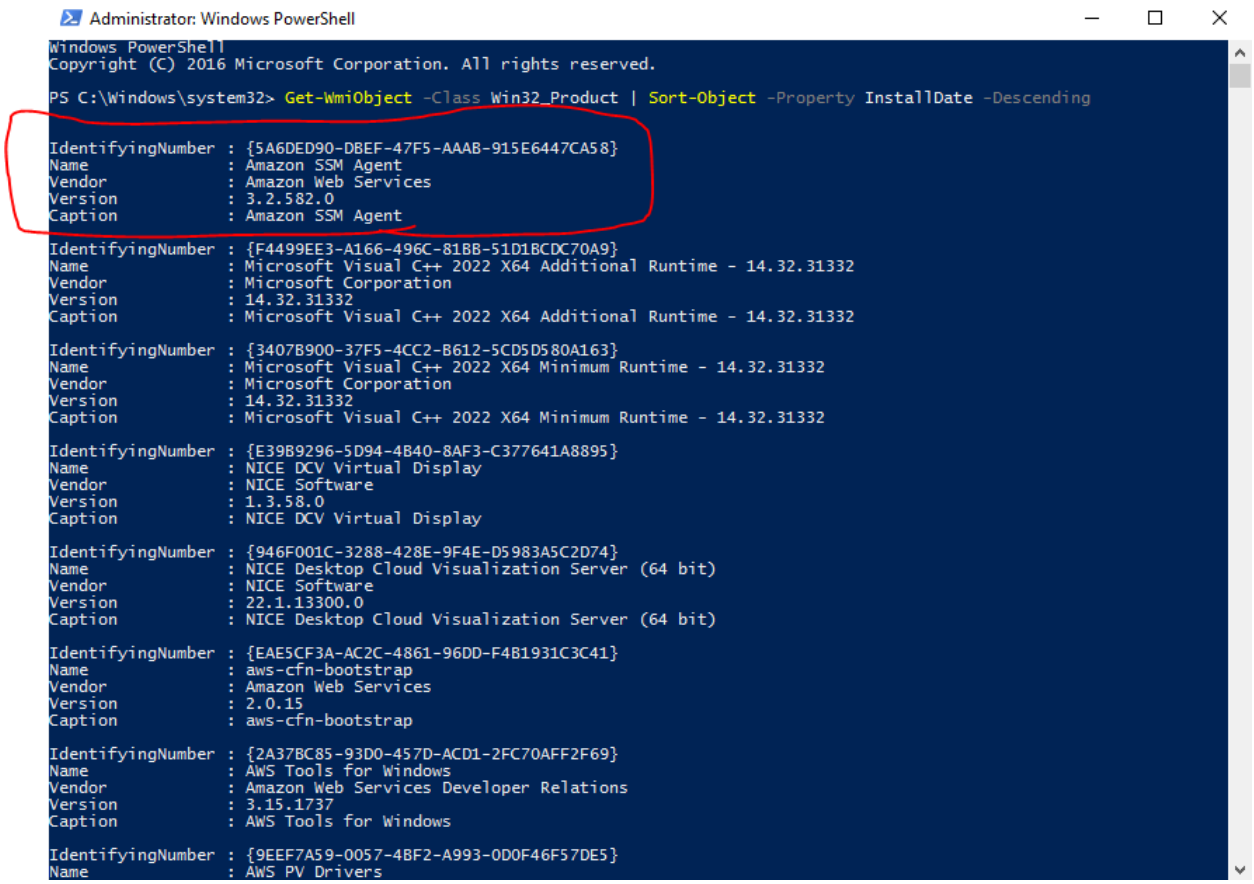


Step 6.) View the latest program installed

To view the latest program installed we will be using powershell. Run Powershell as an Administrator, and execute the following command: *Get-WmiObject -Class Win32_Product | Sort-Object -Property InstallDate -Descending*

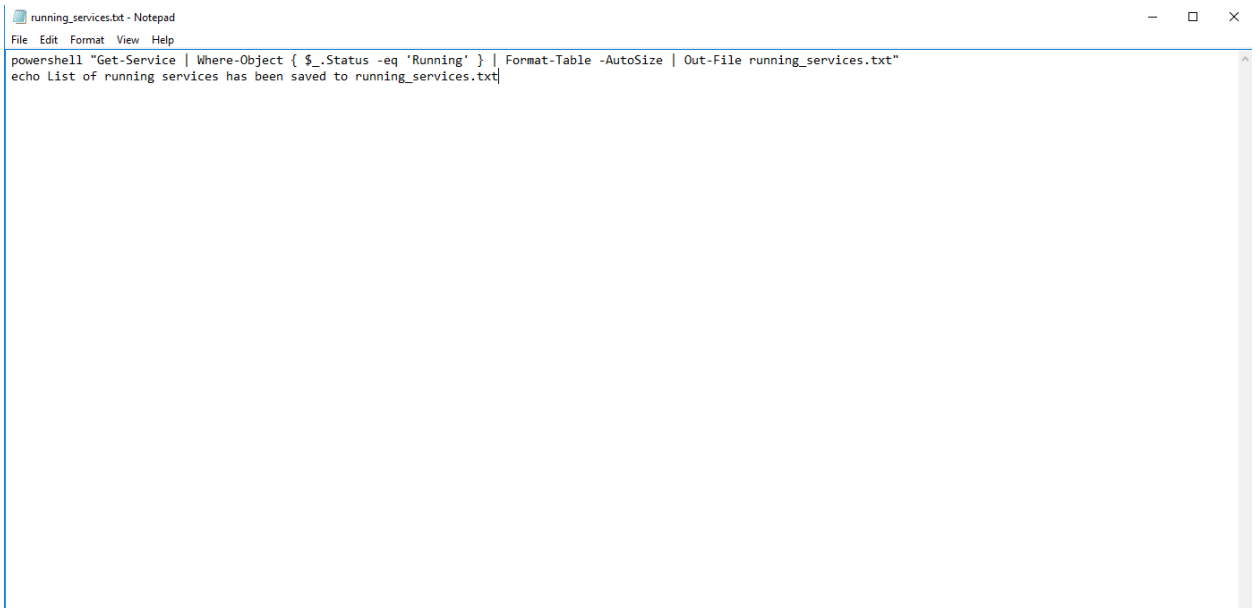
This command will provide you with a list of System32 programs and will list them in descending order based on their install date. This means the top option will be the latest installed.



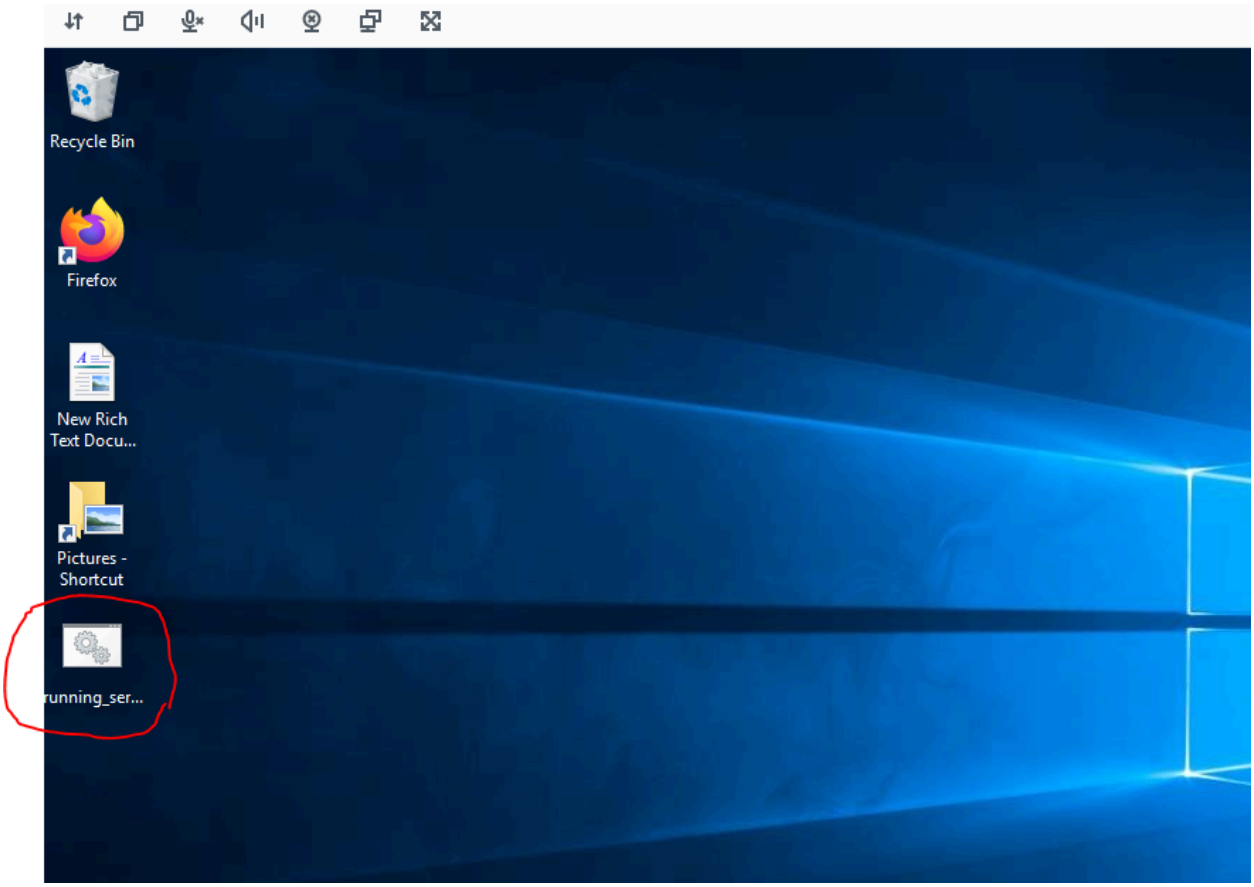


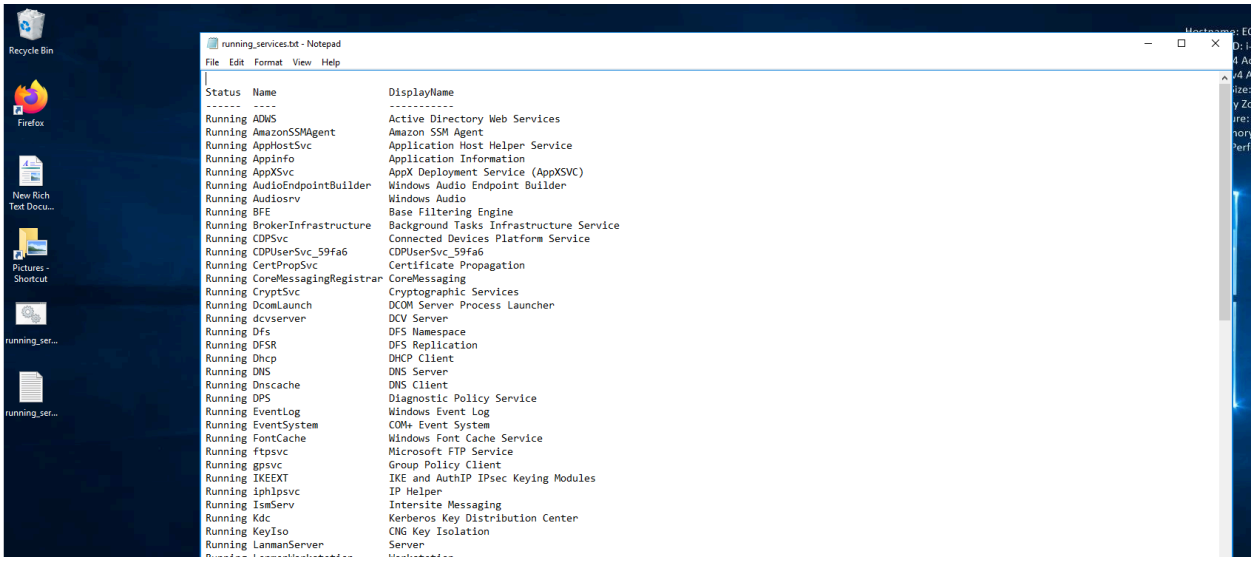
Here we can see the latest installed program. (Amazon SSM Agent)

Step 7.) Write a Powershell script that gives a list of all running services To do this, open a new text document and write the following script:



Be sure to save this as a .bat file to turn it into a script. Then double click the script to run it.


Recycle Bin
Firefox
New Rich Text Docu...
Pictures - Shortcut
running_ser...


running_services.txt - Notepad
File Edit Format View Help
Status Name DisplayName
Running ADWS Active Directory Web Services
Running AmazonSSMAgent Amazon SSM Agent
Running AppHostSvc Application Host Helper Service
Running Appinfo Application Information
Running AppXSvc AppX Deployment Service (AppXSVC)
Running AudioEndpointBuilder Windows Audio Endpoint Builder
Running Audiosrv Windows Audio
Running BFE Base Filtering Engine
Running BrokerInfrastructure Background Tasks Infrastructure Service
Running CDPSvc Connected Devices Platform Service
Running CDPUserSvc_59fa6 CDPUserSvc_59fa6
Running CertPropSvc Certificate Propagation
Running CoreMessagingRegistrar CoreMessaging
Running CryptSvc Cryptographic Services
Running DcomLaunch DCOM Server Process Launcher
Running dcvserver DCV Server
Running Dfs DFS Namespace
Running DFSR DFS Replication
Running Dhcp DHCP Client
Running DNS DNS Server
Running Dnscache DNS Client
Running DPS Diagnostic Policy Service
Running EventLog Windows Event Log
Running EventSystem COM+ Event System
Running FontCache Windows Font Cache Service
Running ftpsvc Microsoft FTP Service
Running gpsvc Group Policy Client
Running IKEEXT IKE and AuthIP IPsec Keying Modules
Running iphlpsvc IP Helper
Running IsmServ Intersite Messaging
Running Kdc Kerberos Key Distribution Center
Running KeyIso CNG Key Isolation
Running LanmanServer Server