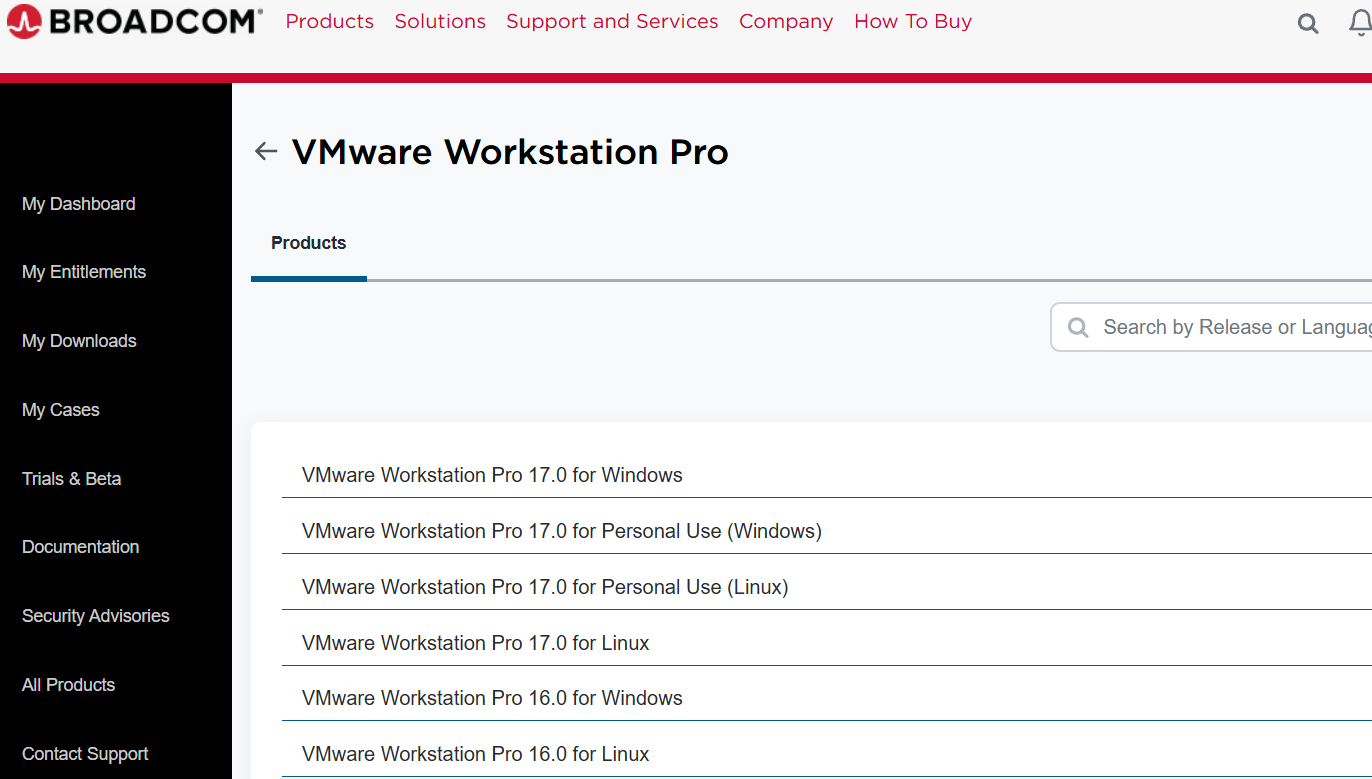
This is a Windows server that will be used to learn and practice Active Directory. My goal of this lab is to gain hands-on experience with Active Directory and have an in-depth understanding on how to manage users and troubleshoot issues within this server.

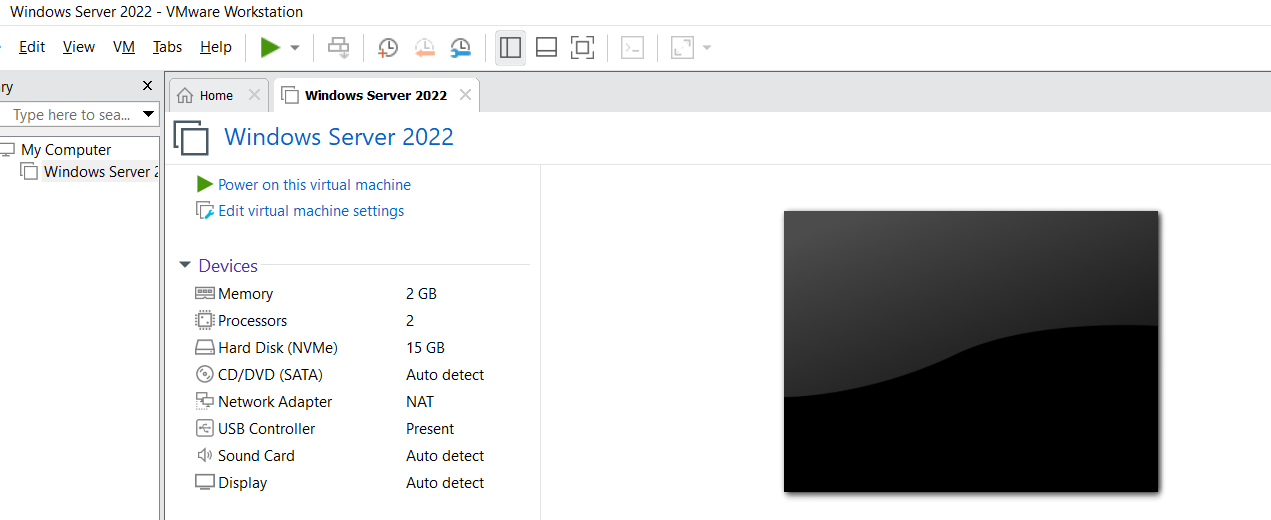
Objective: Setup an Active Directory Domain

Install a windows server into a VM, Promote the server to a Domain Controller. Create the Active Directory Domain and create Organizational Units (OU) for different departments. Create user accounts and groups within the organizational units. Finally test the GPO’s that were created on the client machine.

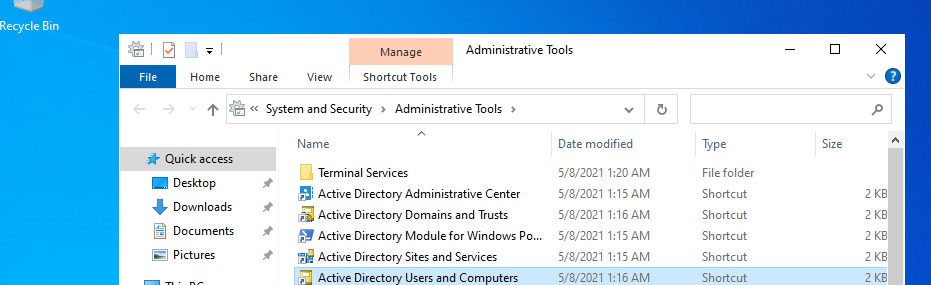
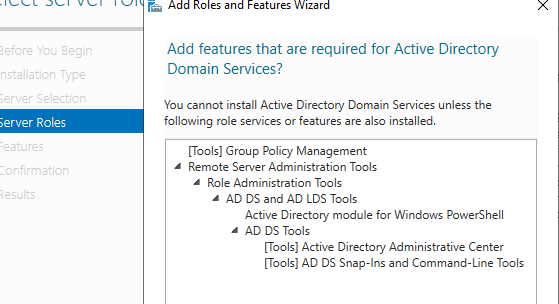
The First thing to do is create an account with Broadcom.com to get access to Vmware Workstation Pro



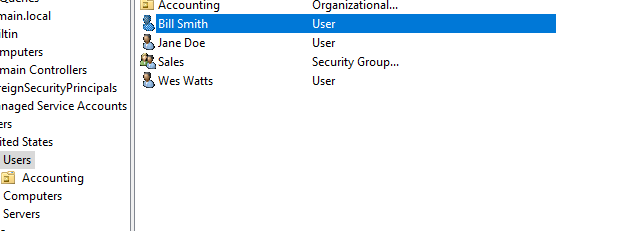
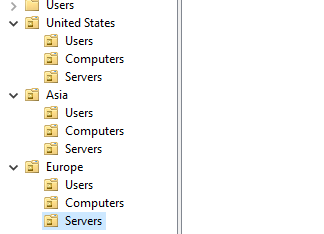
After installing Workstation, the VM has to be created and configured for this lab.



I then was able to download the Active Directory Tools onto this server using the ISO download from Windows

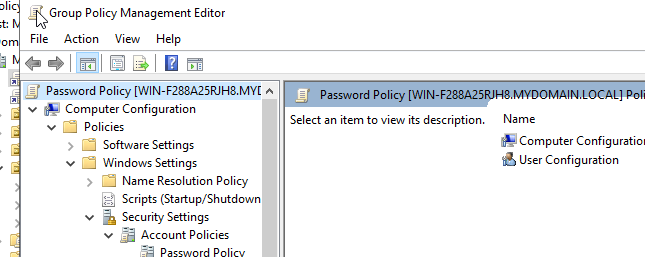


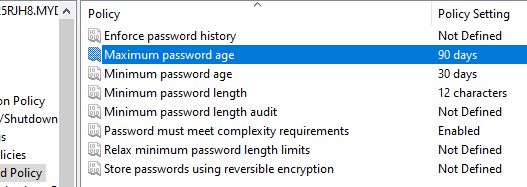
Created OUs with users, computers and servers to start populating the server with accounts that will be used for this lab



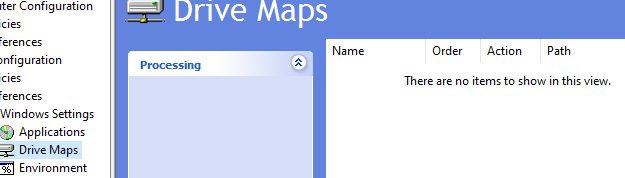
Established Group Policy Object (GPO) using the Group Policy Management Console (GPMC) into this server that consists of Password policy, Drive Mapping, Desktop Wallpaper Policy, Control Panel Restriction Policy, Account lockout Policy, and Disable USB Storage Policy

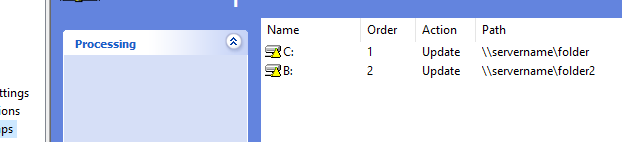
Using the GPM, I navigated over to the Password policies to edit this policy to create a policy that enforces good password practices



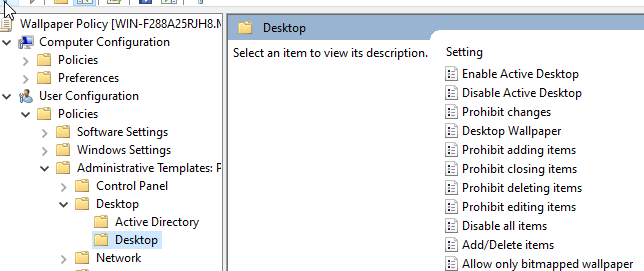


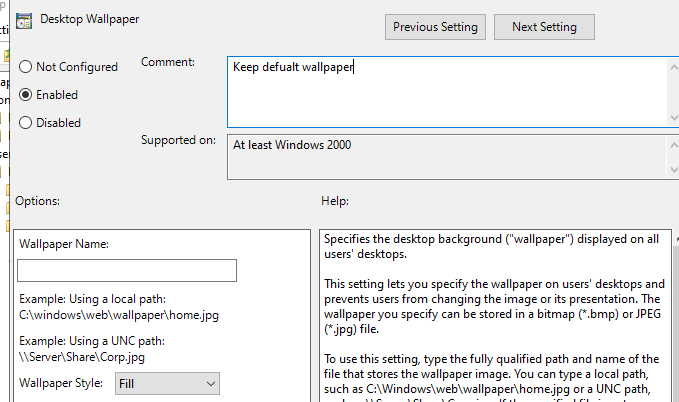
Next was to map Drives using the GPM so users can access and edit their shared files



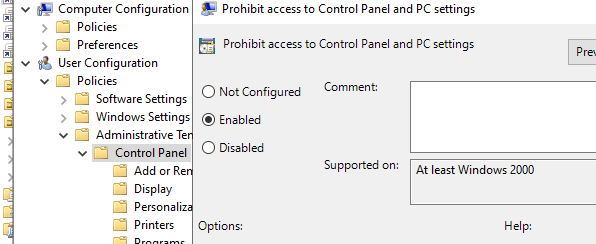


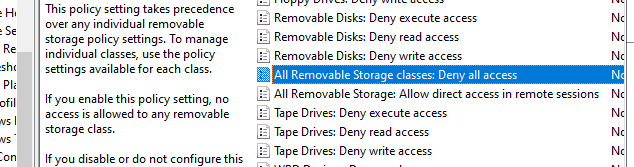
Created a Wallpaper policy so that users do not have the ability to change their desktop wallpapers



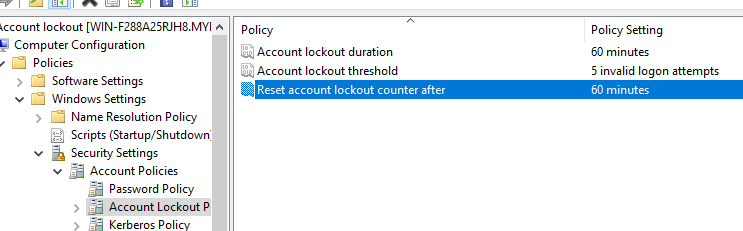


Created a policy that will restrict user accessing the control panel

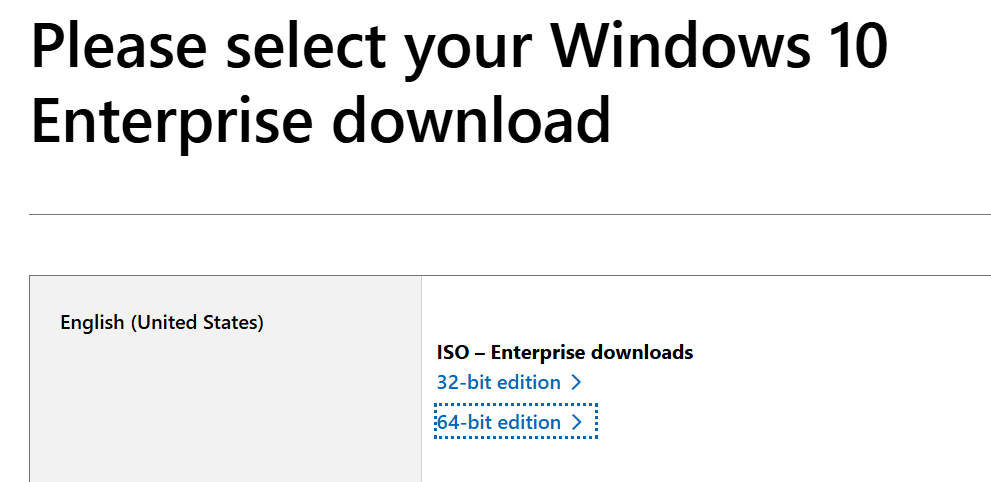


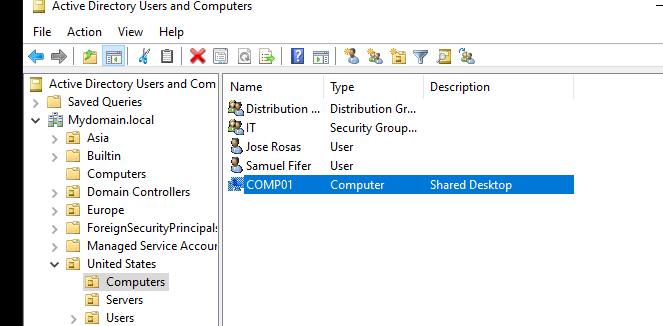
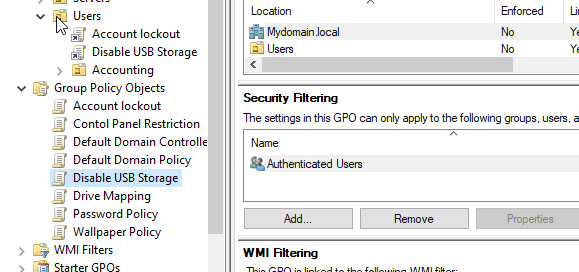
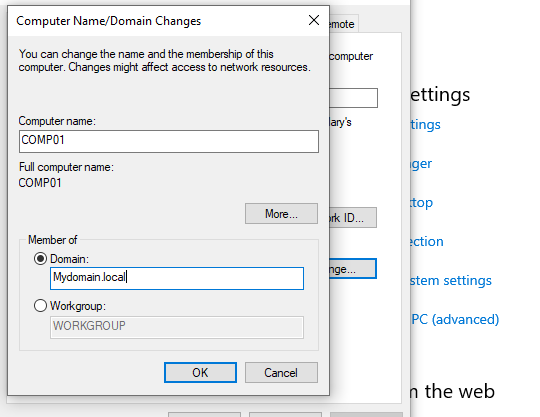
I created a policy that will disable USB storage to prevent users from using USB storage devices.

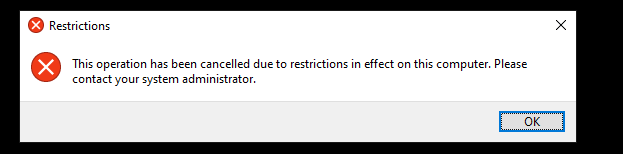
Created an Account Lockout Policy to prevent access from a brute force attack



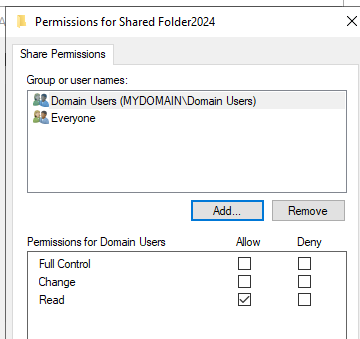
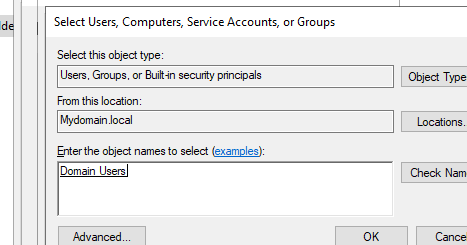
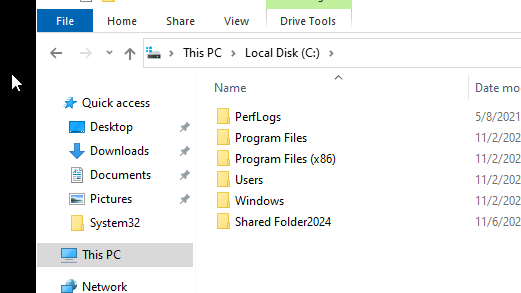
I implemented another VM with Windows 10 to connect to the windows server/domain to test out the GPO’s. After configuring the DNS settings I was then able to successfully connect both VM’s. Then I was able to add the GPO’s to the OU’s and added the desktop to the respective OU. After I tried to use the control panel on the user desktop and was met with an error, which means that the GPO worked successfully.

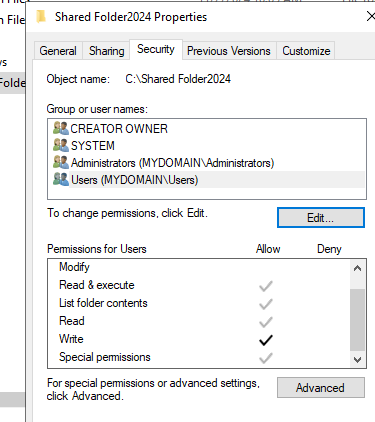


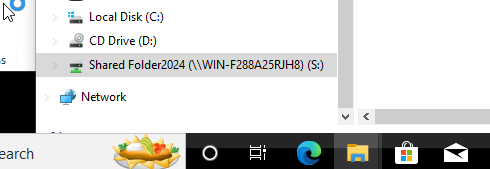




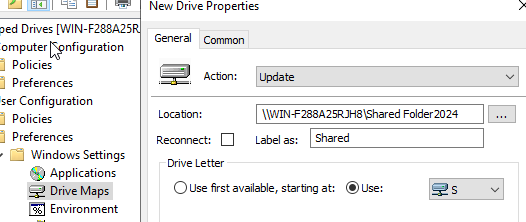
Setting up File services and file sharing to learn how to manage network resources and permissions. I created shared folders with the appropriate permissions. Also the NTFS and share permissions to allow domain users access.





I then logged into the domain user account to see if it has access to the shared folder by mapping the network drives.

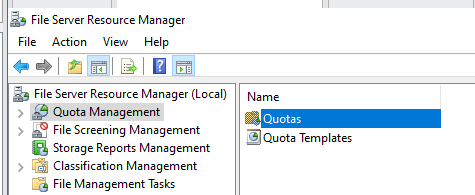
I then realized that this is not the best way for persistence. The network sharing option was better that way the file always gets mapped to the user every time they login I went back into the windows server to create a new GPO

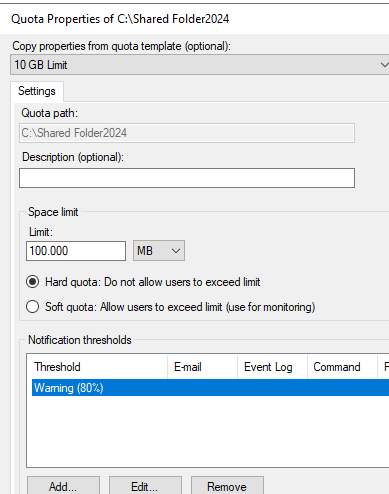
I then added this GPO to the users.

I then logged into the user machine to see if the shared file was successful

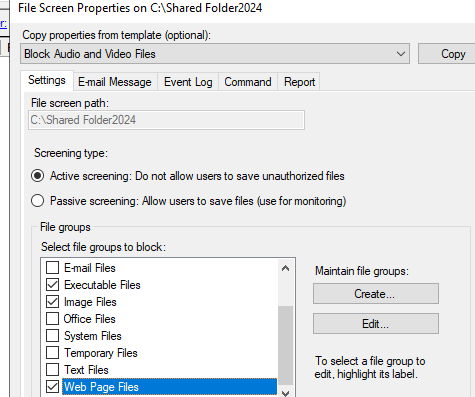


Using the File Server Resource Manager I was able to configure the quota to manage the storage. I set the limit to 10GB with a threshold of around 80% to send an email to IT informing them that the folder is almost full.

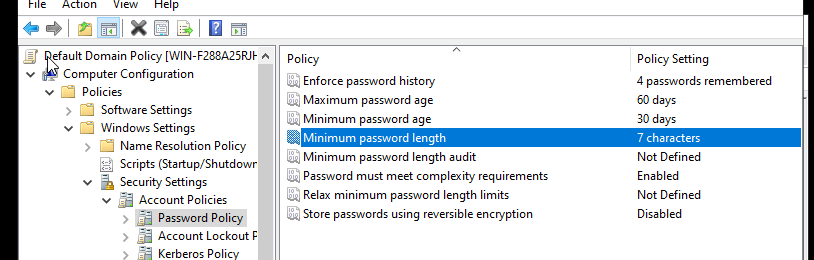




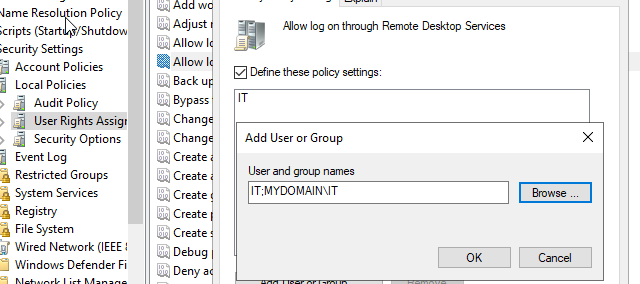
Configured the file types by using the File Screening Management to restrict certain file types to prevent the folders from filling up easily.



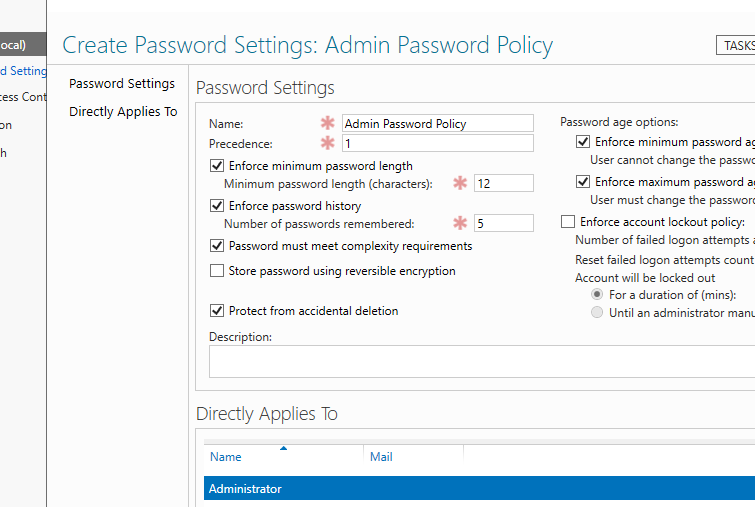
Now it's time to configure the security policy to enhance security on all user desktops. This will include password policies for users. I configured the password policy setting to have standard requirement for user to create their password for the next time they login.

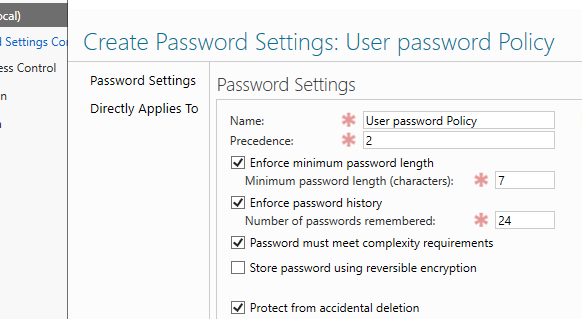


Also created a new policy for User Rights to assign and restrict certain rights for users.



Using the Active Directory Administrative Center I was able to create a fine grain password policy that will allow user to have a standard password requirement while admin accounts will have a more stringent requirement





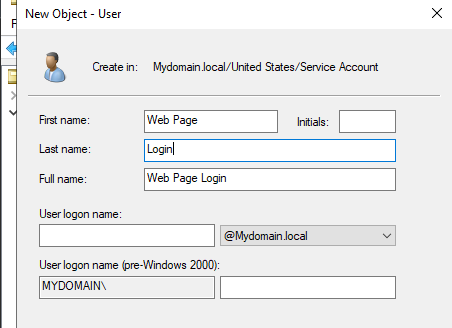
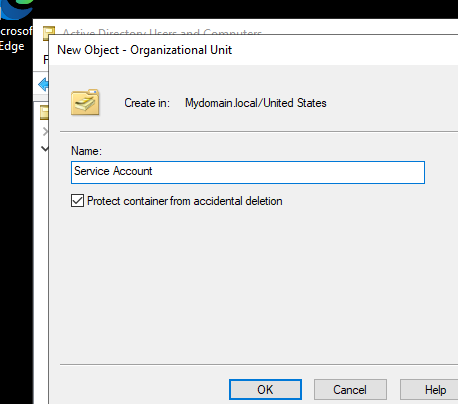
I was also able to implement a service account using Sysinternals tools to help manage it. This is something that some companies use in their business i.e (kiosk, digital menu) and wanted to learn more about it.

Purpose: Setup a single purpose computer that displays a specific webpage

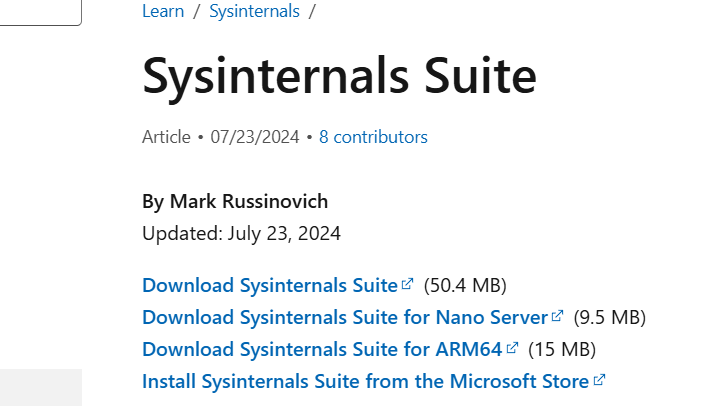
Objective:

* Use a service account as login account
* Account should login when computer reboots
* Web browser should startup automatically once logged in and in full screen mode
* Configure the computer to always be ON
* Restrict Logon for Service account

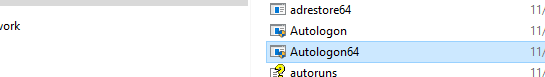
First I created an Organizational Unit named “Service Account” with a user



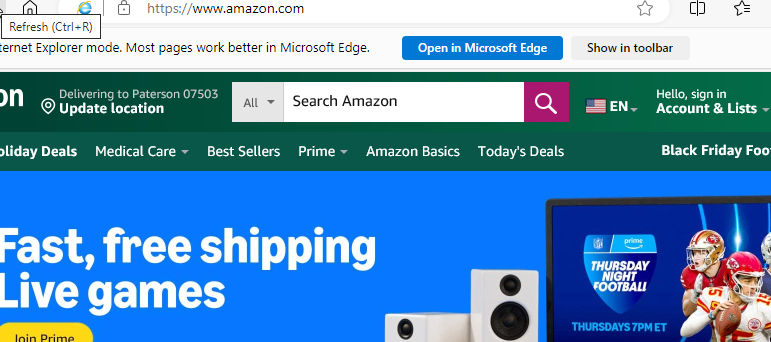
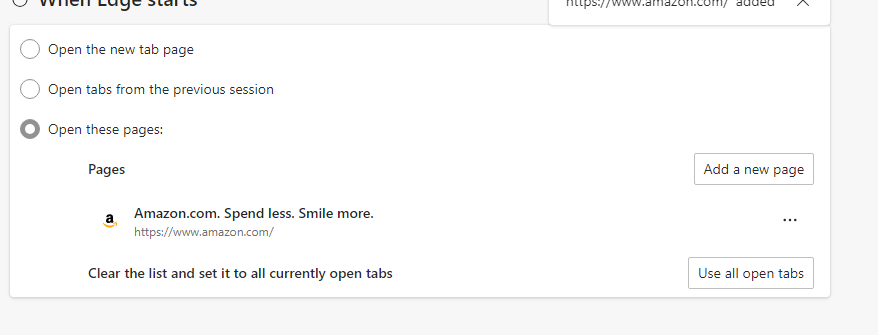
Downloaded the Sysinternals ISO onto my windows client machine



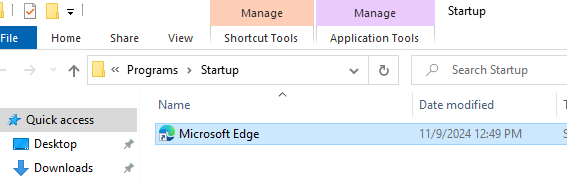
Used Autologon64 tool to configure the machine to successfully auto login after rebooting



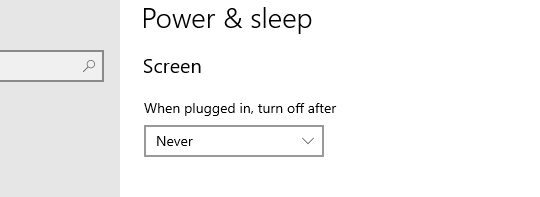
Setting up the browser to display the webpage every time the machine boots up. I chose Amazon.com to display each time.



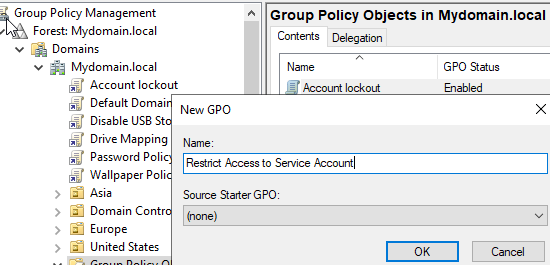
Added microsoft Edge to the startup so it displays right after a reboot

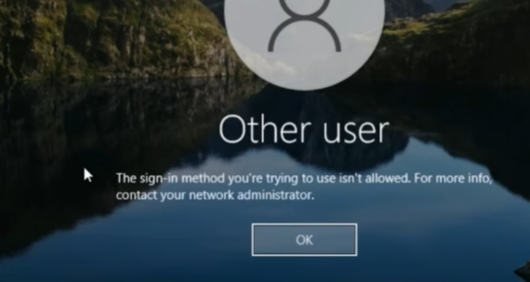


Changed the sleep mode to never so the machine stays on 24/7 while no one is touching it



On my Domain server I created a new Gpo for the service account to restrict standard users to login to this account. Once I updated the service account, I tried logging in with a user account and was met with an error message. This lets me know that the GPO that restricts users from logging in to this account was successful.





This lab has taught me so much about Active directory.I knew nothing going into this lab and came out with learning very important skills and knowledge about Active Directory. For example creating OU’S,GPO’S, resetting passwords, file management, managing and creating users. Going through this lab has made me realize the importance of managing users through AD. I was also able to experience what an IT professional does on a daily basis while using AD. I noticed a common issue in the workplace is password resets as users forget their passwords or lock themselves out. I repeated the process of resetting passwords so that I can become accustomed to this process. Although there is much to learn about AD I feel I've learned very important aspects and look forward to learning more ways to solve issues using Active Directory to become well rounded so better solve issues.