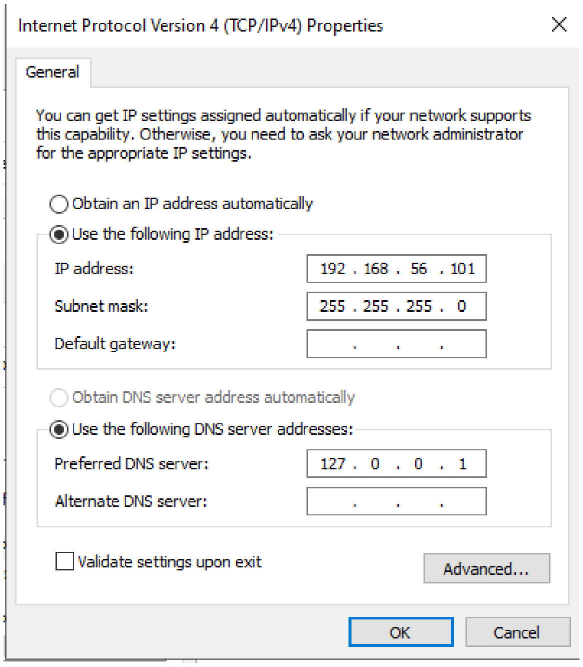
Active Directory lab by Thomas McSherry
thomas.e.mcsherry@gmail.com

Introduction

Through this exercise, I wanted to simulate various tasks and processes that I would perform while working within an Active Directory environment. First I wanted to setup and configure an Active Directory environment through an evaluation copy of Windows Server 2022, then create an OU/Groups structure with users,create/apply GPOs, join computers to this domain and simulate various tasks (Setting up shared resources and simulating a password lockout).

AD Setup and Configuration

First, I installed an evaluation copy of Windows Server 2022 on an instance of Oracle Virtualbox. The first step I took was setting up a proper static IP for the server, as well as other settings.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

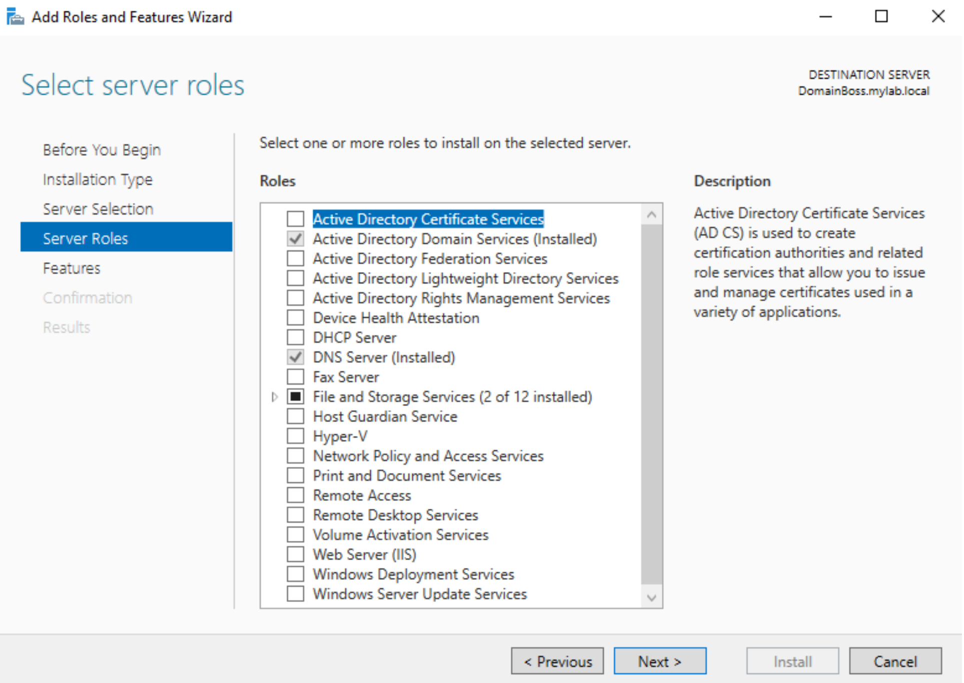
IP address: 192 . 168 . 56 . 101
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 127 . 0 . 0 . 1
Alternate DNS server: . . .

□ Validate settings upon exit

Then through Server Manager, I installed some necessary roles for this exercise



Select server roles

DESTINATION SERVER
DomainBoss.mylab.local

Select one or more roles to install on the selected server.

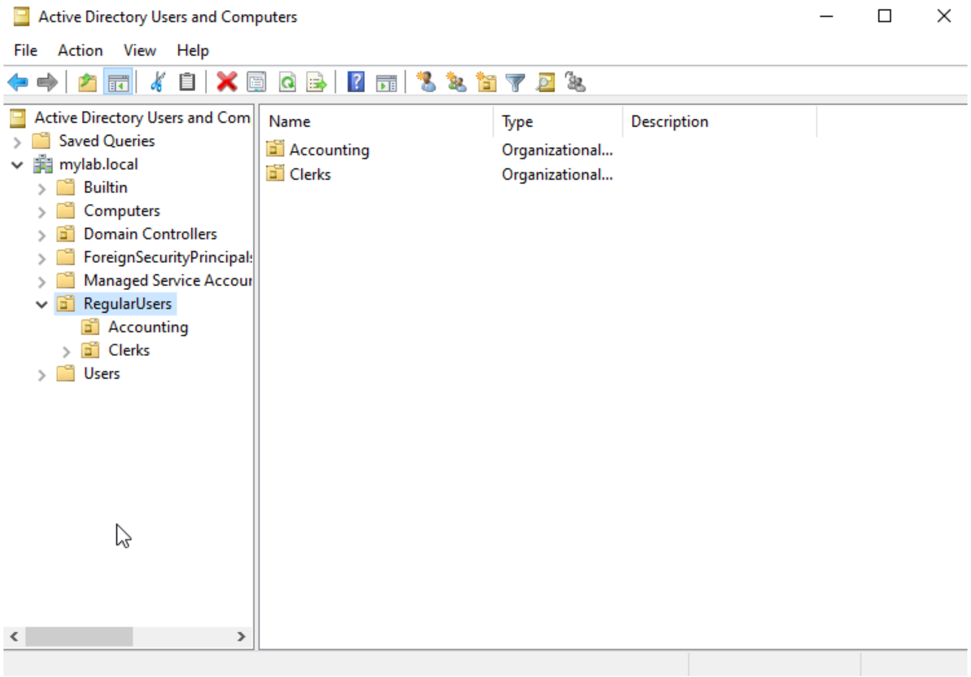
Roles

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Then within Active Directory, I created a broad OU known as RegularUsers.Within that OU I created two more, to simulate departments within an office environment.



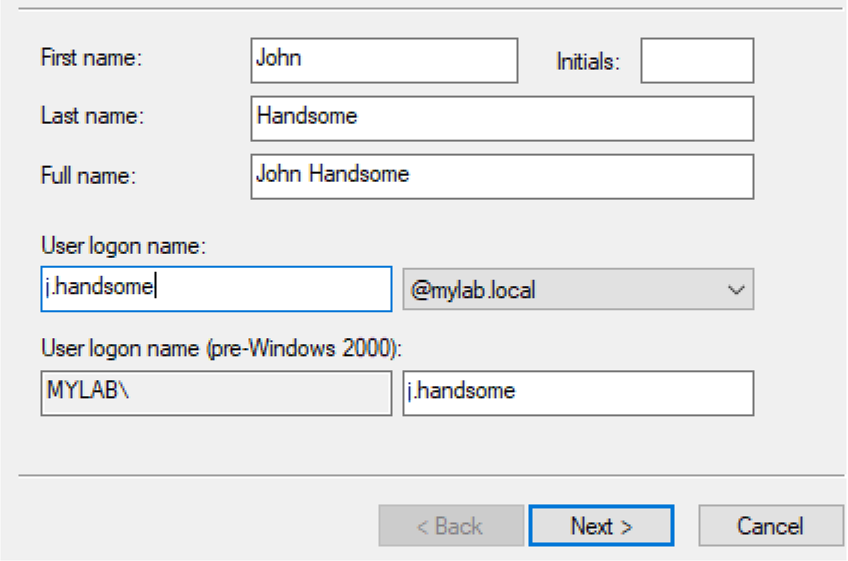
- Active Directory Users and Com
  - Saved Queries
  - mylab.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Managed Service Accour
    - RegularUsers
      - Accounting
      - Clerks
    - Users

Name	Type	Description
Accounting	Organizational...	
Clerks	Organizational...	

For purposes later on, I created appropriate groups based on the departments and added members.

User Creation + Adding to Domain

In this case, I felt it was appropriate to start off by creating a user, a RegularUser within the Accounting department.

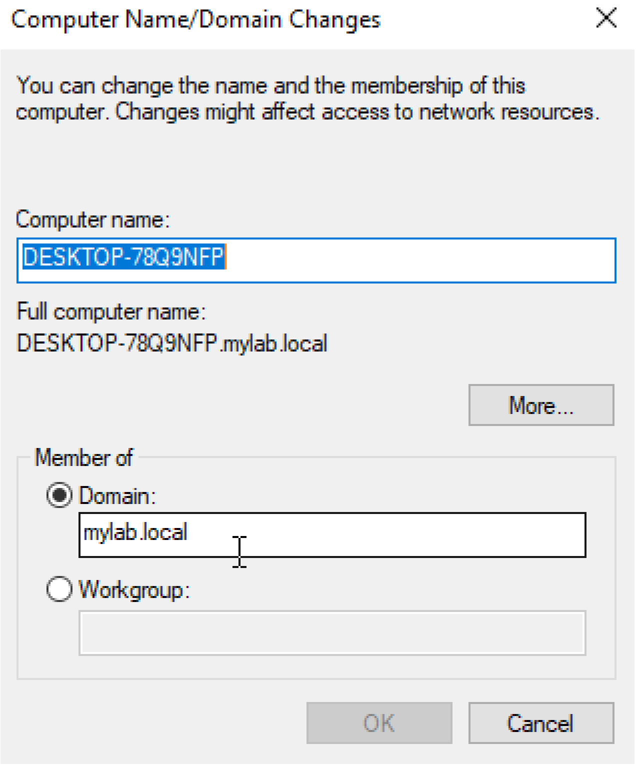


First name: John
Initials:
Last name: Handsome
Full name: John Handsome

User logon name:
j.handsome @mylab.local

User logon name (pre-Windows 2000):
MYLAB\ j.handsome

After the creation of this account, I installed an instance of Windows 10 Enterprise on a separate VM running in tandem with the WIndows Server instance. I then joined this instance to the Domain, and successfully logged into the John Handsome account.



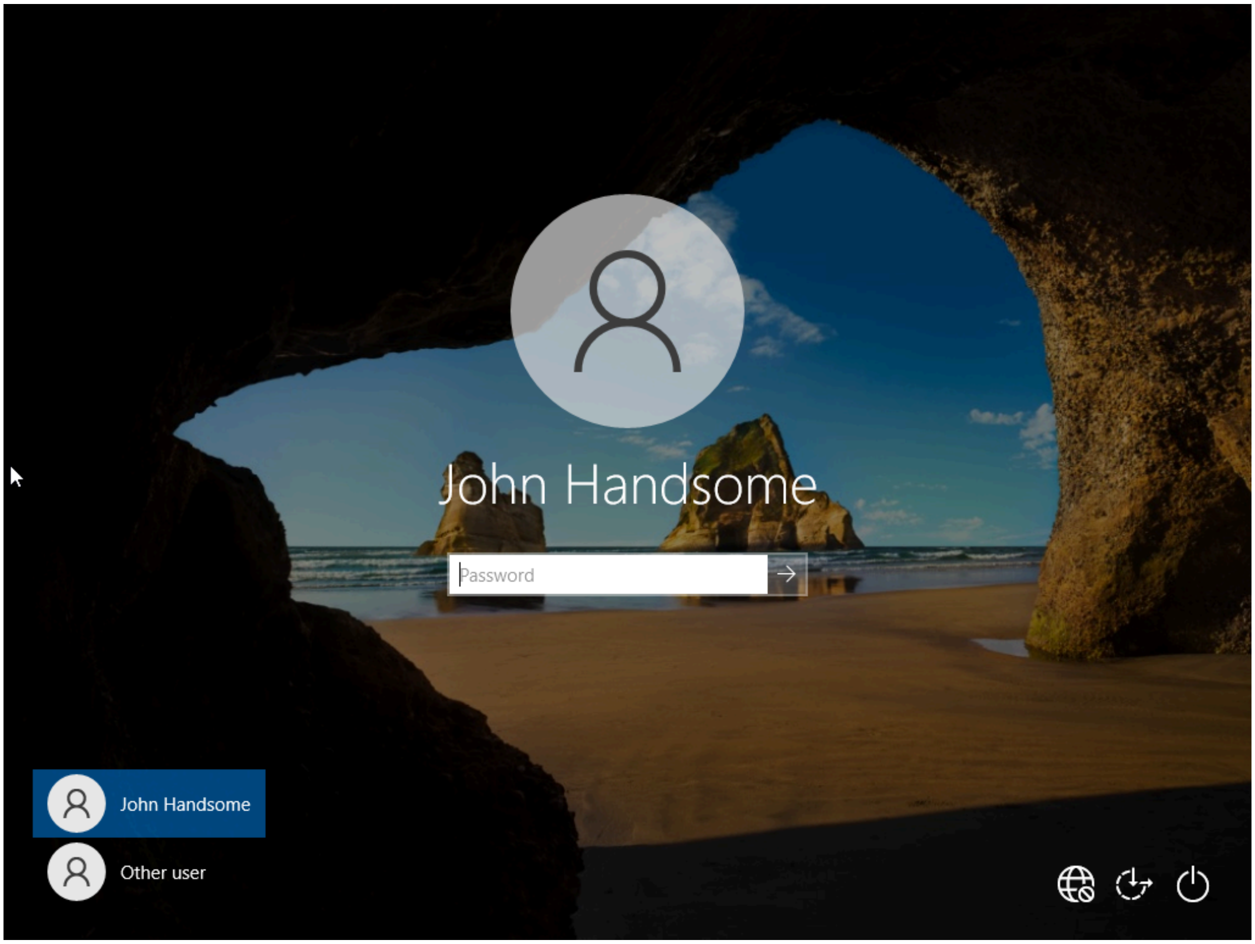
Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
DESKTOP-78Q9NFP

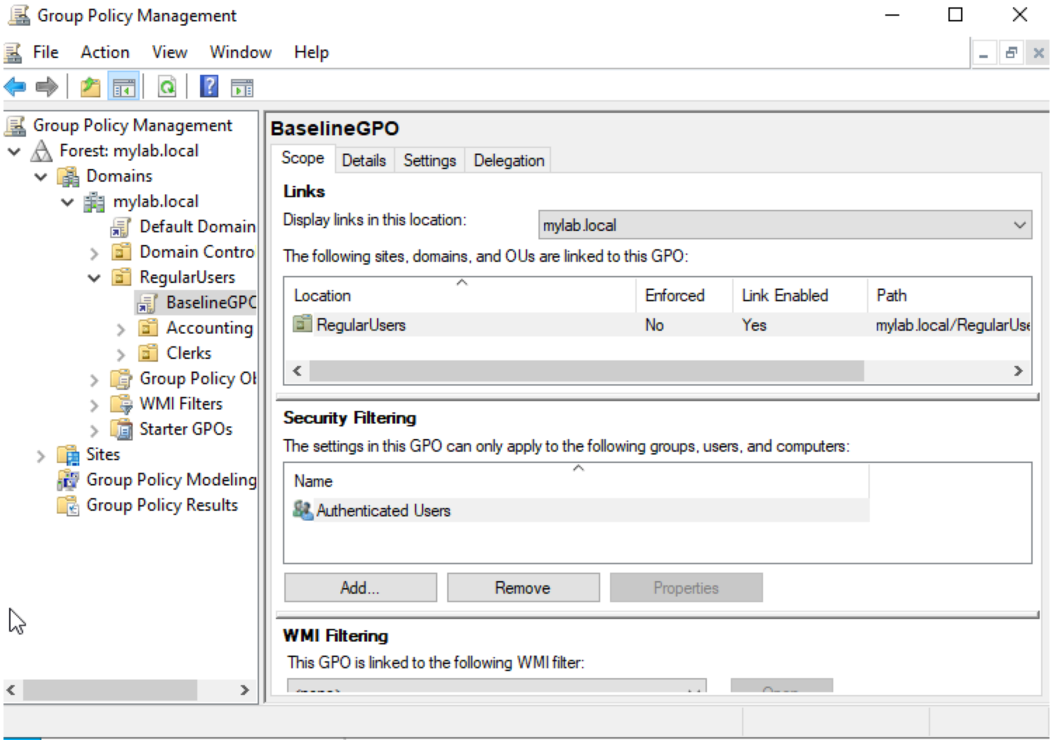
Full computer name:
DESKTOP-78Q9NFP.mylab.local

Member of
● Domain:
mylab.local
○ Workgroup:



Testing GPO Configuration
I wanted to create a good baseline GPO, restricting control panel and settings access for the RegularUsers OU. Also too curious about the interaction, I wanted to make sure that it worked within the Accounting OU, under the RegularUsers OU.

Within Group Policy Management, I set this up by applying it to the RegularUsers OU.



BaselineGPO

Links

Display links in this location: mylab.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
RegularUsers	No	Yes	mylab.local/RegularUs

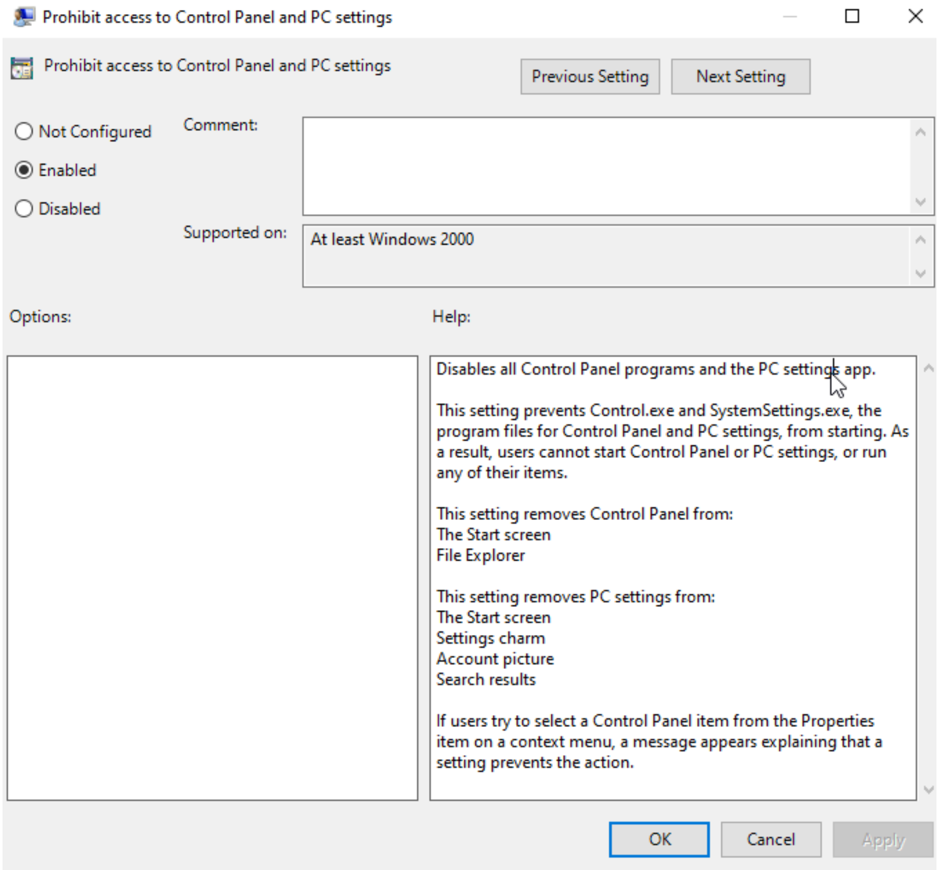
Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:



Prohibit access to Control Panel and PC settings

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Help:

Disables all Control Panel programs and the PC settings app.

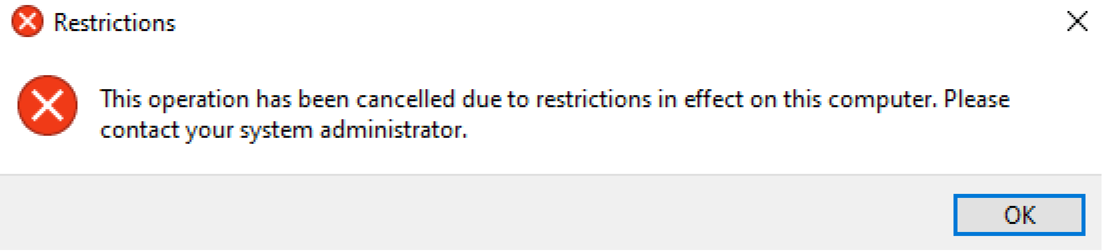
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:
The Start screen
File Explorer

This setting removes PC settings from:
The Start screen
Settings charm
Account picture
Search results

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.

After setting this up, I logged into the John Handsome account and attempted to access the Control Panel, confirming the success of the GPO application.

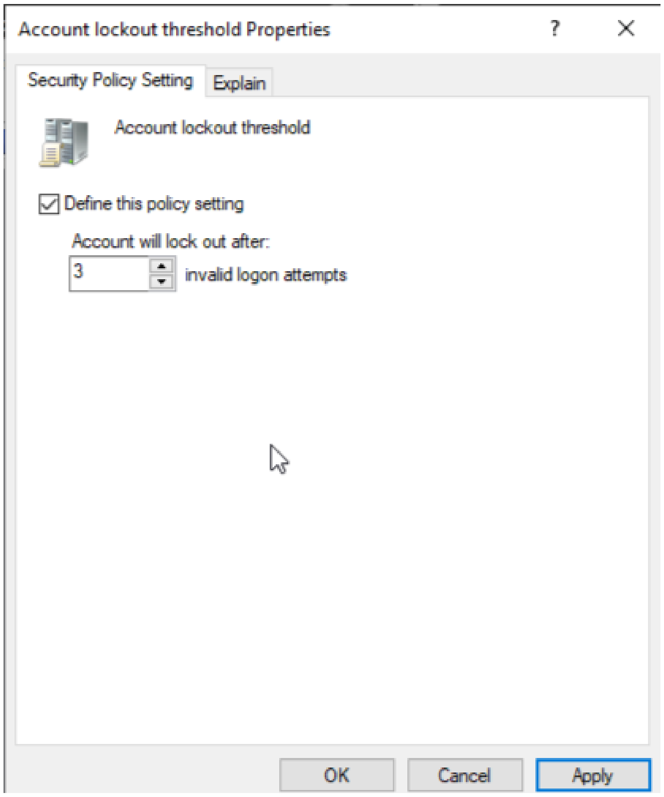


This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

Account Lockout Simulation

First, I had to change the default settings so after a couple of incorrect password attempts, a User would be locked out of their account. In case if user credentials were compromised, I feel that a time-based lockout would be inappropriate.

I then edited the Default Domain Policy, navigated to Security Settings > Account Policies > Account Lockout Policy > Account lockout threshold and set the attempt amount to 3.



Account lockout threshold

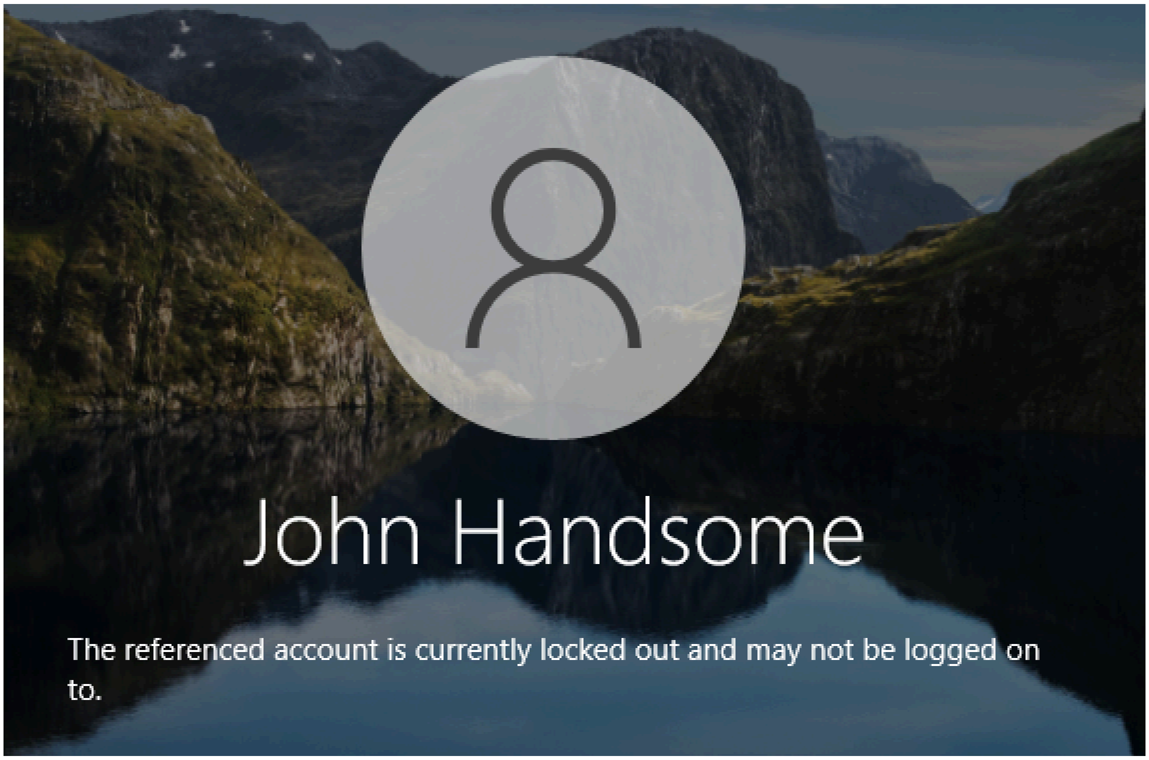
☑ Define this policy setting

Account will lock out after:

3 invalid logon attempts

Within the lockout policy, I then changed the lockout duration to 0, so the account could only be unlocked via an administrator.

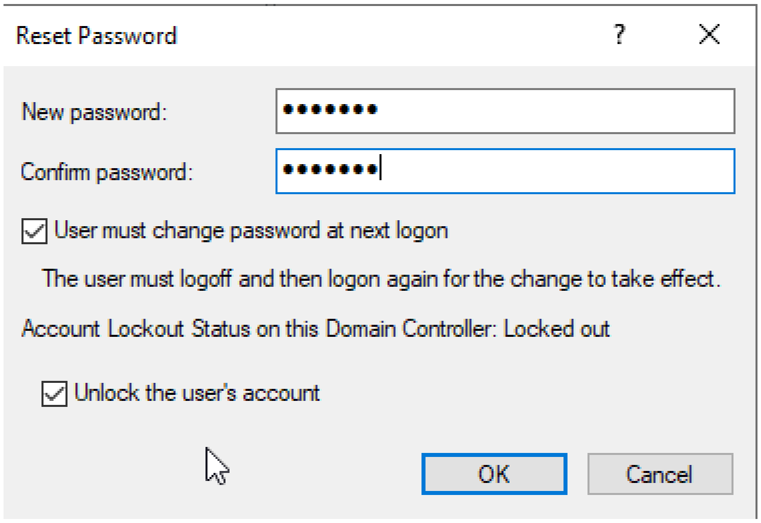
To test this, I inputted an incorrect password 3 times on the John Handsome account.



John Handsome

The referenced account is currently locked out and may not be logged on to.

Dealing with this case in a workplace environment, I’m aware the best general practice is to contact the user, and ask if it was their doing. After that the correct thing to do would be to reset the password and give them a new one that they would then change after logging on. This is done by right-clicking on the user in AD and selecting Reset Password.



Reset Password

New password: •••••••

Confirm password: •••••••

☑ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

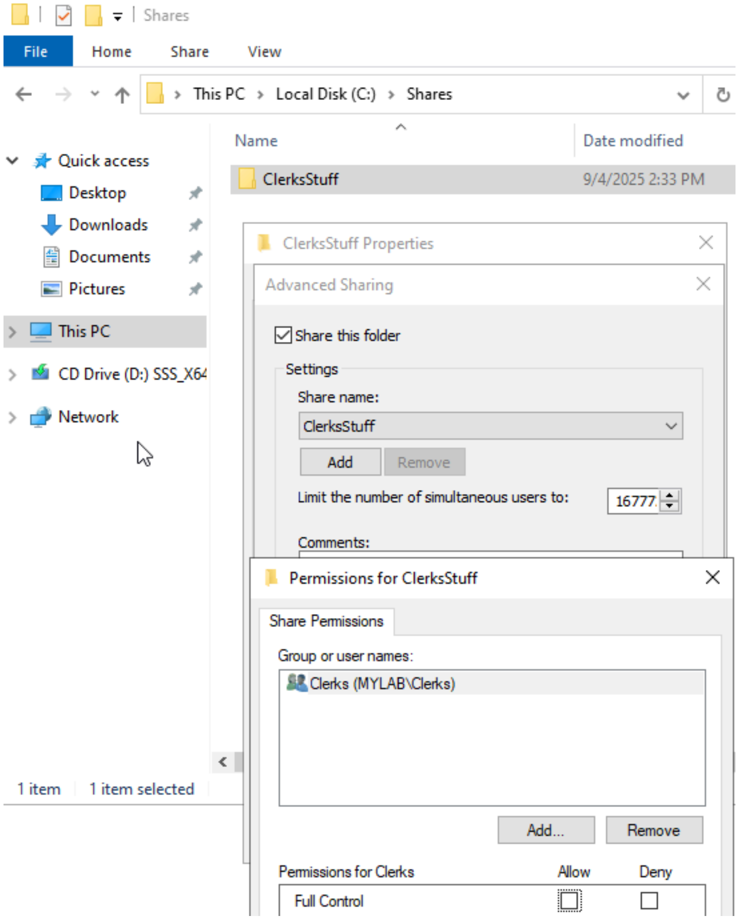
Account Lockout Status on this Domain Controller: Locked out

☑ Unlock the user's account

Then, just to be sure I inputted the new password to verify if the appropriate prompt would come up to change the password.

Mapping a Network Drive

For this exercise I wanted to create a network drive that only users under the Clerks group could access. In the C drive of my domain controller I created a folder and configured sharing.



Name	Date modified
ClerksStuff	9/4/2025 2:33 PM

Advanced Sharing

☑ Share this folder

Settings

Share name: ClerksStuff

Limit the number of simultaneous users to: 16777

Comments:

Permissions for ClerksStuff

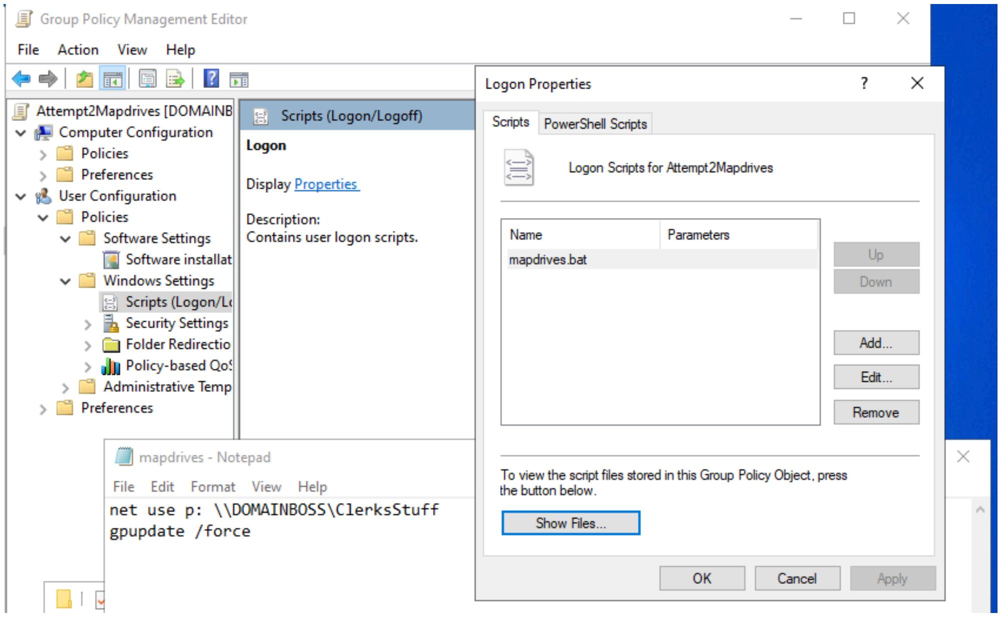
Share Permissions

Group or user names:

Clerks (MYLAB\Clerks)

Permissions for Clerks	Allow	Deny
Full Control	□	□

Under the Clerks OU, I created a GPO with a condition on Logon where it does a couple of commands via a script.



Description:
Contains user logon scripts.

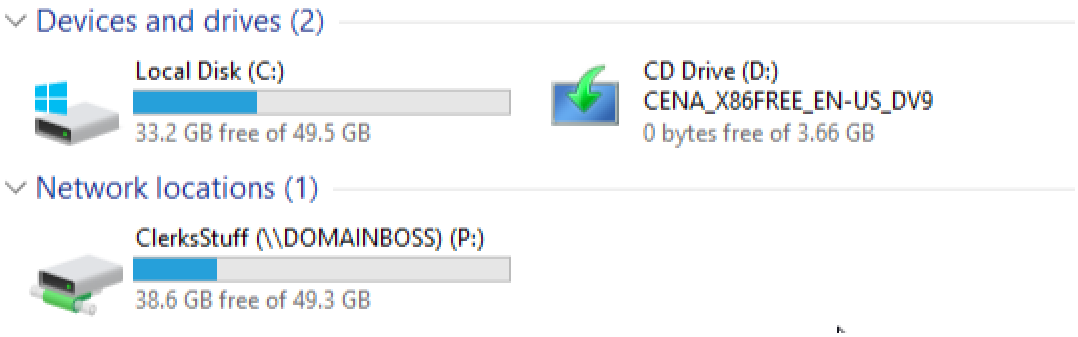
Logon Scripts for Attempt2Mapdrives

Name	Parameters
mapdrives.bat	

To view the script files stored in this Group Policy Object, press the button below.

```
net use p: \\DOMAINBOSS\ClerksStuff
gpupdate /force
```

Then, I logged onto a Clerks account to verify that it was there.


Devices and drives (2)

Local Disk (C:)
33.2 GB free of 49.5 GB

CD Drive (D:) CENA_X86FREE_EN-US_DV9
0 bytes free of 3.66 GB

Network locations (1)

ClerksStuff (\\DOMAINBOSS) (P:)
38.6 GB free of 49.3 GB

Conclusion

In summary, I deployed an Active Directory environment using Windows Server 2022, and joined computers using Windows 10 to the domain, setup OUs and groups, as well as creating relevant GPOS. To simulate potential day-to-day actions in the workplace, I simulated a password reset and mapped a network drive. Going through this exercise, I had various issues and setbacks that I had to troubleshoot through online research. This helped me get a good idea for the standard AD workflow, and going through the troubleshooting process helped me refine my own personal process.

Conclusion

Despite the increase of cloud for common business applications in this day and age, Active Directory is still incredibly relevant and the backbone of many systems. Setting up Windows Server 2022, and joining a Windows Client showed many steps of configuring users and access. The configuration and testing of OUs, groups and GPOs allowed me to understand how users/devices are structured within a network, and how privileges are provisioned. The simulation of an end-user password reset allowed me to gain knowledge of common tasks, and how this very common ticket is solved. On another note, mapping a shared network drive showed the steps of how AD is utilized to manage business-related resources within an environment. Overall, this exercise allowed me to grasp fundamentals of Active Directory and how networks are managed in a business setting, while specifically testing these actions allowed me to gain knowledge on common troubleshooting steps/knowledge that are very relevant within help desk.