

FLORIDA POLY.[®]
[USER AUTHENTICATION &
AUTHORIZATION]

CIS 4367.01 Computer Security, Fall 2025

Nickolas Diaz

[Xianping Wang]

Table of Contents

Contents

Table of Contents.....	2
Abstract.....	2
Tasks.....	2
Task 1: Installing and Configuring Active Director.....	2
Task 2: Enable Complex Password Policy for All Users.....	4
Task 3: Creating University Users with Different Privileges.....	6
Task 4: Task 4: Setting Up Folder Permissions.....	7
Task 5: Verifying all settings.....	8
Conclusions.....	12
References.....	12

Abstract

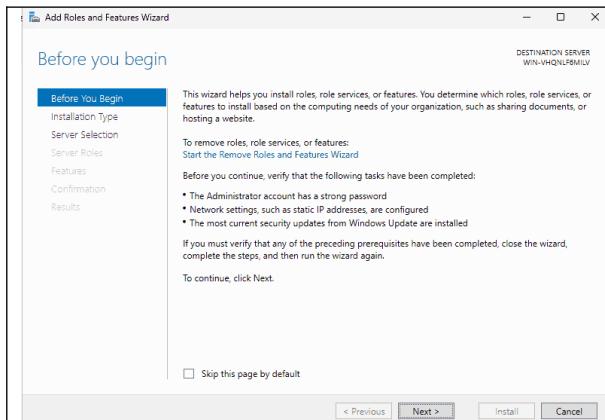
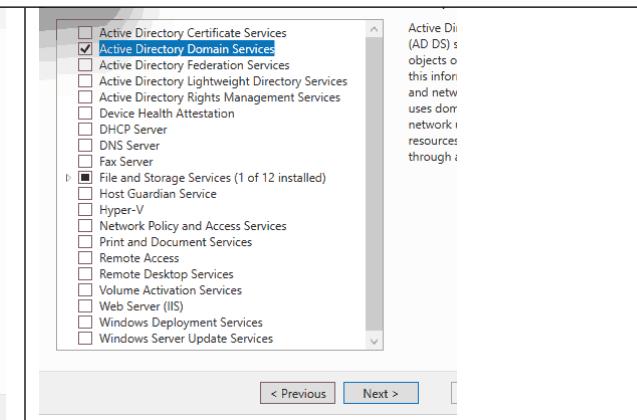
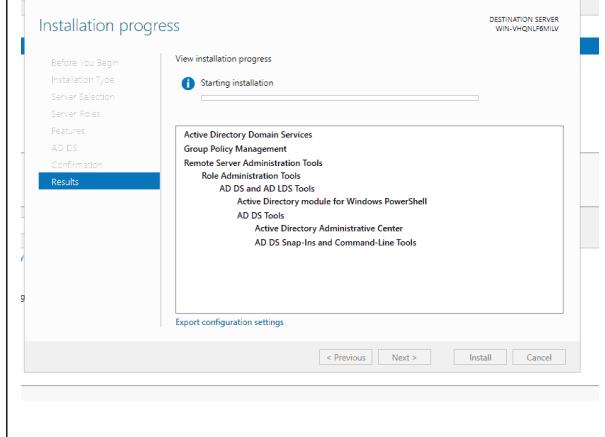
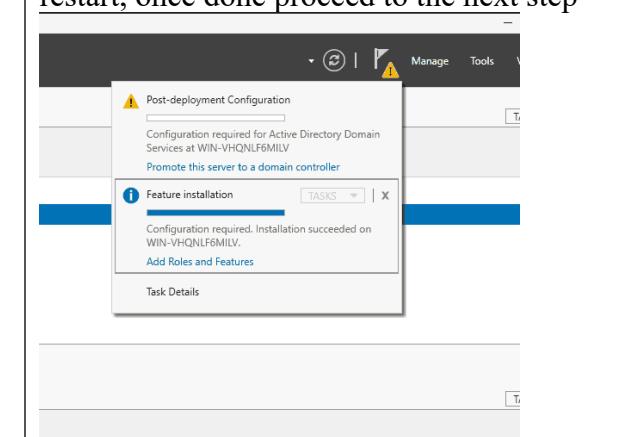
This lab will achieve setting up a domain using Active Directory on a Windows server 2025 virtual machine. It involves creating a domain service and 3 Organizational Units for each department with each department having groups such as chair, faculty and students. Each group will have their own permissions within the university such as viewing, reading or modifying files and directories within the university folder. In addition a complex password policy will be applied to the domain.

Tasks

Task 1: Installing and Configuring Active Director

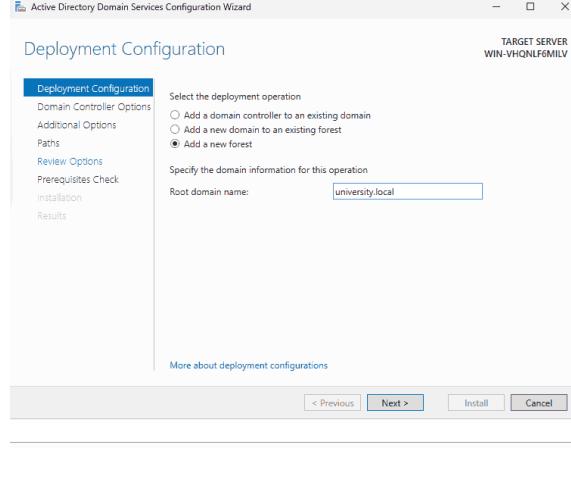
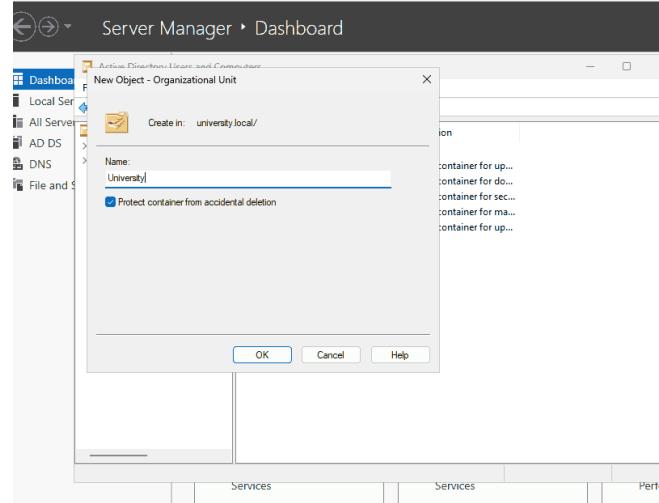
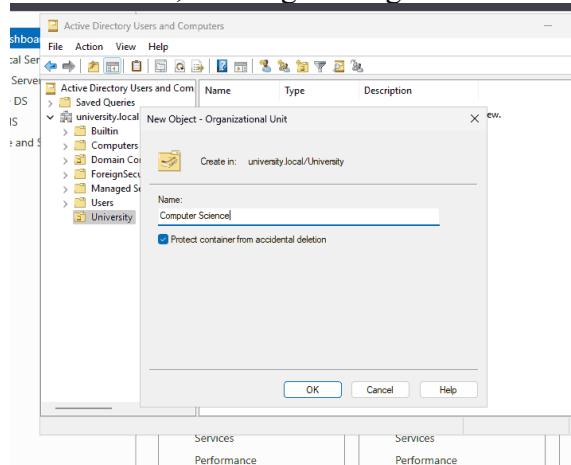
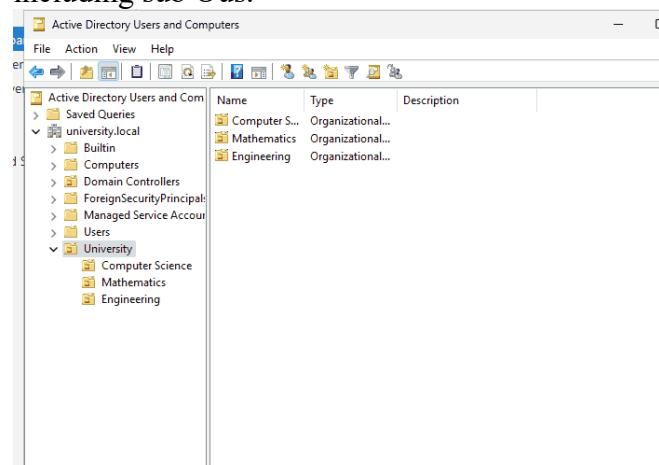
Install Active Directory Domain Service

After clicking the add roles and features from server manager, this pop-up appears	On the instalation type press Active Directory Domain Service
--	---

 <p>This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.</p> <p>To remove roles, role services, or features: Start the Remove Roles and Features Wizard</p> <p>Before you continue, verify that the following tasks have been completed:</p> <ul style="list-style-type: none"> The Administrator account has a strong password Network settings, such as static IP addresses, are configured The most current security updates from Windows Update are installed <p>If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.</p> <p>To continue, click Next.</p> <p><input type="checkbox"/> Skip this page by default</p> <p>< Previous Next > Install Cancel</p>	 <p>DESTINATION SERVER: WIN-VHQNL6MILV</p> <ul style="list-style-type: none"> <input type="checkbox"/> Active Directory Certificate Services <input checked="" type="checkbox"/> Active Directory Domain Services <input type="checkbox"/> Active Directory Federation Services <input type="checkbox"/> Active Directory Lightweight Directory Services <input type="checkbox"/> Active Directory Rights Management Services <input type="checkbox"/> Device Health Attestation <input type="checkbox"/> DHCP Server <input type="checkbox"/> DNS Server <input type="checkbox"/> Fax Server <input checked="" type="checkbox"/> File and Storage Services (1 of 12 installed) <ul style="list-style-type: none"> <input type="checkbox"/> Host Guardian Service <input type="checkbox"/> Hyper-V <input type="checkbox"/> Network Policy and Access Services <input type="checkbox"/> Print and Document Services <input type="checkbox"/> Remote Access <input type="checkbox"/> Remote Desktop Services <input type="checkbox"/> Volume Activation Services <input type="checkbox"/> Web Server (IIS) <input type="checkbox"/> Windows Deployment Services <input type="checkbox"/> Windows Server Update Services <p>< Previous Next ></p>
<h3>Go past all the options to download it</h3>	
 <p>DESTINATION SERVER: WIN-VHQNL6MILV</p> <p>View installation progress</p> <p>Starting installation</p> <p>Progress: 0%</p> <p>Active Directory Domain Services Group Policy Management Remote Server Administration Tools Role Administration Tools AD DS and AD LDS Tools Active Directory module for Windows PowerShell AD DS Tools Active Directory Administrative Center AD DS Snap-Ins and Command-Line Tools</p> <p>< Previous Next > Install Cancel</p>	<p>From here it will start downloading and restart, once done proceed to the next step</p>  <p>Post-deployment Configuration Configuration required for Active Directory Domain Services at WIN-VHQNL6MILV. Promote this server to a domain controller</p> <p>Feature installation Configuration required. Installation succeeded on WIN-VHQNL6MILV. Add Roles and Features</p> <p>Task Details</p>

Configure Active Directory Users and Computers

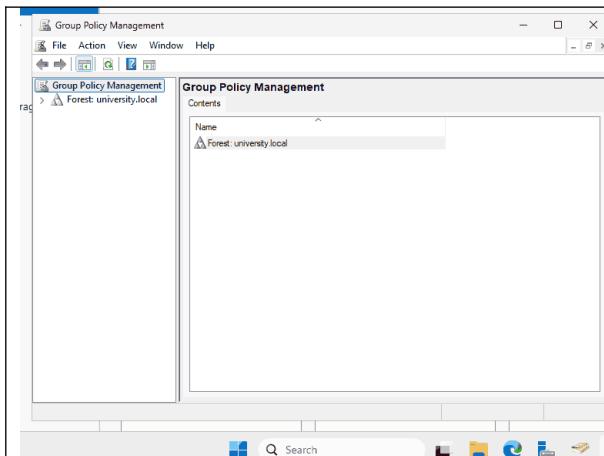
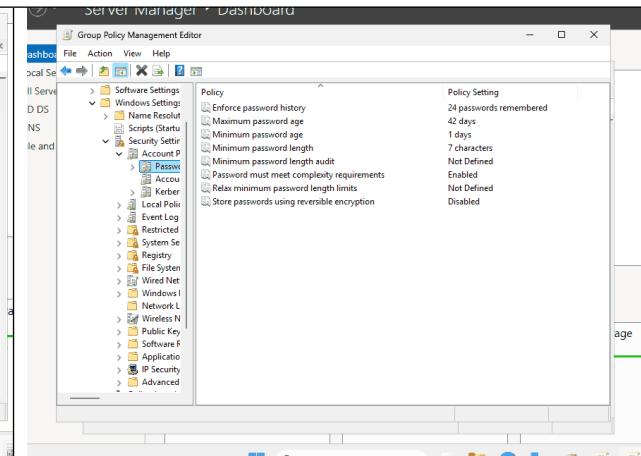
<p>Pop-up appears after clicking Active Directory Users and Computers from the server manager. In addition I added the domain university.local</p>	<p>After the domain was created I created a organizational unit called University.</p>
--	--

	
<p>In the organizational unit I created three sub-OUs called Computer Science, Mathematics, and Engineering</p> 	<p>This is the tree view of the organizational unit, including sub OUs.</p> 

Task 2: Enable Complex Password Policy for All Users

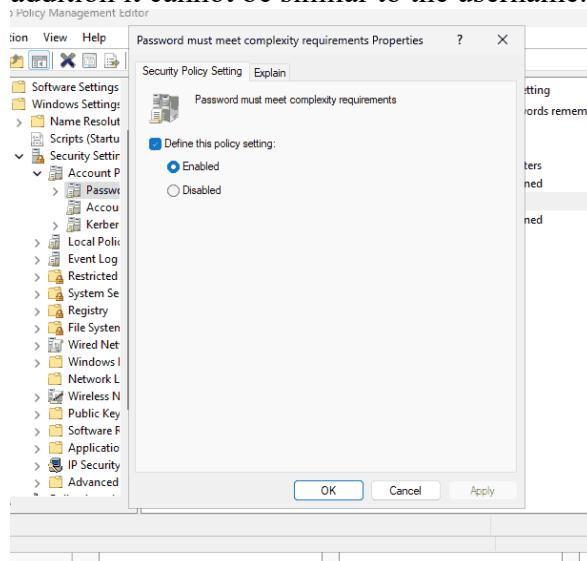
First I headed to Group Policy Management, I typed gPMC.msc in the terminal to open it.

From Group Policy Management > Forest > Domains > university.local > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy, is the location of the password complexity settings.

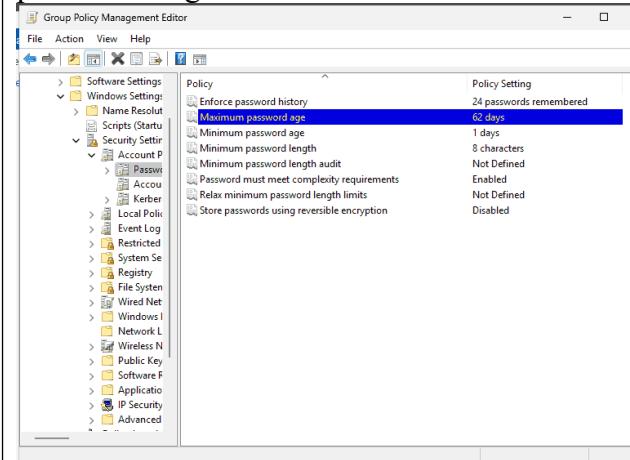
The screenshot shows the Windows Group Policy Management interface. On the left, the 'Group Policy Management' window displays the 'Contents' pane with 'Name' and 'Forest: university.local'. On the right, the 'Group Policy Management Editor' window shows the 'Policy' section under 'Account Policies'. The 'Password must meet complexity requirements' policy is selected, showing its properties: 'Policy Setting' is 'Enabled', '24 passwords remembered' is '42 days', '1 days' is '7 characters', 'Not Defined' is 'Enabled', 'Not Defined' is 'Not Defined', and 'Disabled' is 'Disabled'.

Clicking the password must meet complexity requirements, this pop-up shows, click enable to force the OU to have secure passwords, passwords have to use uppercase lowercase numbers Non-alphabetic characters and be up to 8 characters, in addition it cannot be similar to the username.



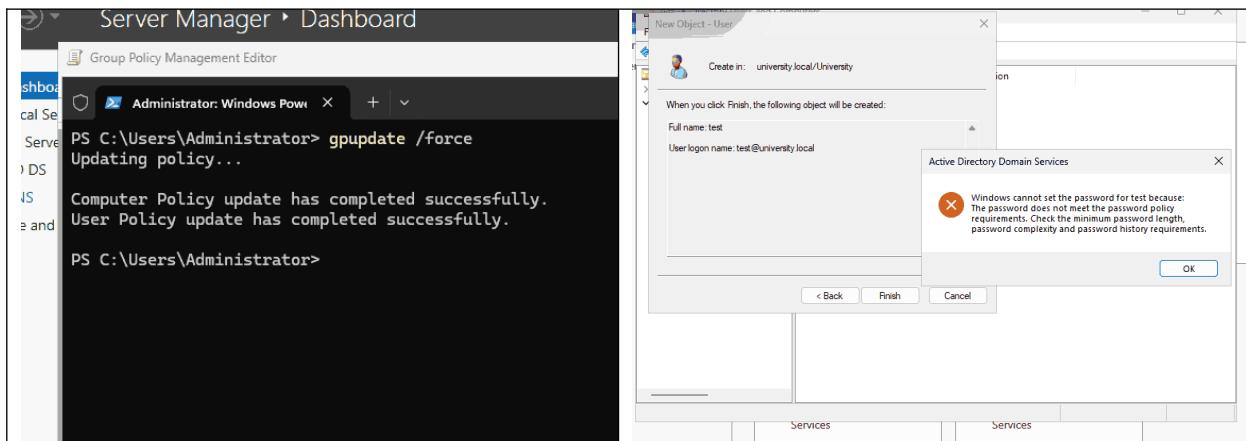
Lastly in order to make these policies take affect the command gpupdate /force is used.

Other setting to modify are password history 24 previous passwords this means that you cannot reuse any passwords, Password age how long to get a new password and lastly password length which is 8



The screenshot shows the 'Group Policy Management Editor' window with the 'Policy' section. The 'Maximum password age' policy is selected, highlighted in blue. Other policies listed include 'Enforce password history' (24 days), 'Minimum password age' (1 day), 'Minimum password length' (8 characters), 'Minimum password length audit' (Not Defined), 'Relax minimum password length limits' (Not Defined), and 'Store passwords using reversible encryption' (Disabled).

This is demonstrating the password complexity requirements in this case username and password were similar.



Task 3: Creating University Users with Different Privileges

Create Users

6 users were created for each department, the Chair, 2 Faculty, and 3 Students
Here is the Computer Science department

This screenshot shows the 'Active Directory Users and Computers' snap-in. The navigation pane on the left shows the tree structure: Active Directory Users and Computers > Saved Queries > university.local > Builtin > Computers > Domain Controllers > ForeignSecurityPrincipals > Managed Service Accounts > University > Computer Science > Engineering > Mathematics > Users. The main pane displays a table of users under 'Computer Science': CS_Chair, CS_Faculty1, CS_Faculty2, CS_Faculty3, CS_Student1, CS_Student2, and CS_Student33.

Here is the Mathematics department

This screenshot shows the 'Active Directory Users and Computers' snap-in. The navigation pane on the left shows the tree structure: Active Directory Users and Computers > Saved Queries > university.local > Builtin > Computers > Domain Controllers > ForeignSecurityPrincipals > Managed Service Accounts > University > Computer Science > Engineering > Mathematics > Users. The main pane displays a table of users under 'Mathematics': MA_Chair, MA_Faculty1, MA_Faculty2, MA_Faculty3, MA_Student1, MA_Student2, and MA_Student33.

Here is the Engineering department

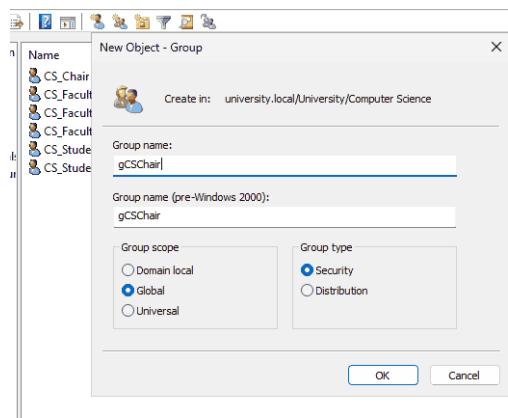
This screenshot shows the 'Active Directory Users and Computers' snap-in. The navigation pane on the left shows the tree structure: Active Directory Users and Computers > Saved Queries > university.local > Builtin > Computers > Domain Controllers > ForeignSecurityPrincipals > Managed Service Accounts > University > Computer Science > Engineering > Mathematics > Users. The main pane displays a table of users under 'Engineering': EG_Chair, EG_Faculty1, EG_Faculty2, EG_Faculty3, EG_Student1, EG_Student2, EG_Student3, and EG_Student33.

The provost user on top of the University

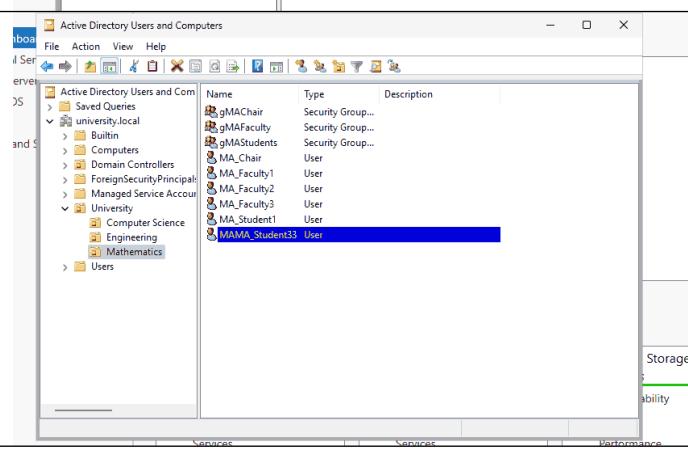
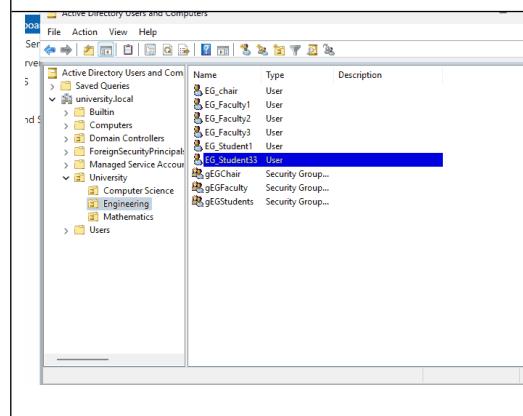
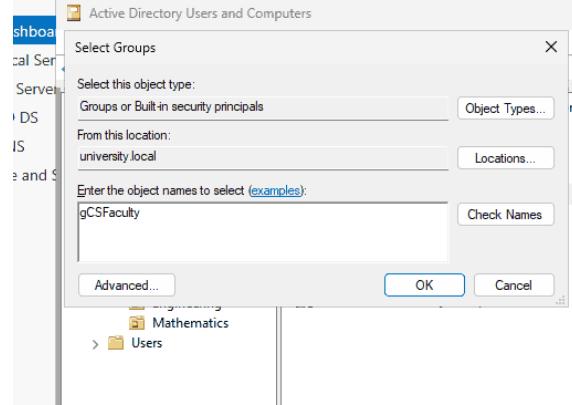
This screenshot shows the 'Active Directory Users and Computers' snap-in. The navigation pane on the left shows the tree structure: Active Directory Users and Computers > Saved Queries > university.local > Builtin > Computers > Domain Controllers > ForeignSecurityPrincipals > Managed Service Accounts > University > Computer Science > Engineering > Mathematics > Users. The main pane displays a table of users under 'Users': provost.

Create Security Groups

This is the pop-up for creating a new group



9 groups were created, gCSChair, gCSFaculty, gEGStudent, gEGChair, gEGFaculty, gEGStudent, gMAChair, gMAFaculty, gMAStudent, and the appropriate users were put in the group.

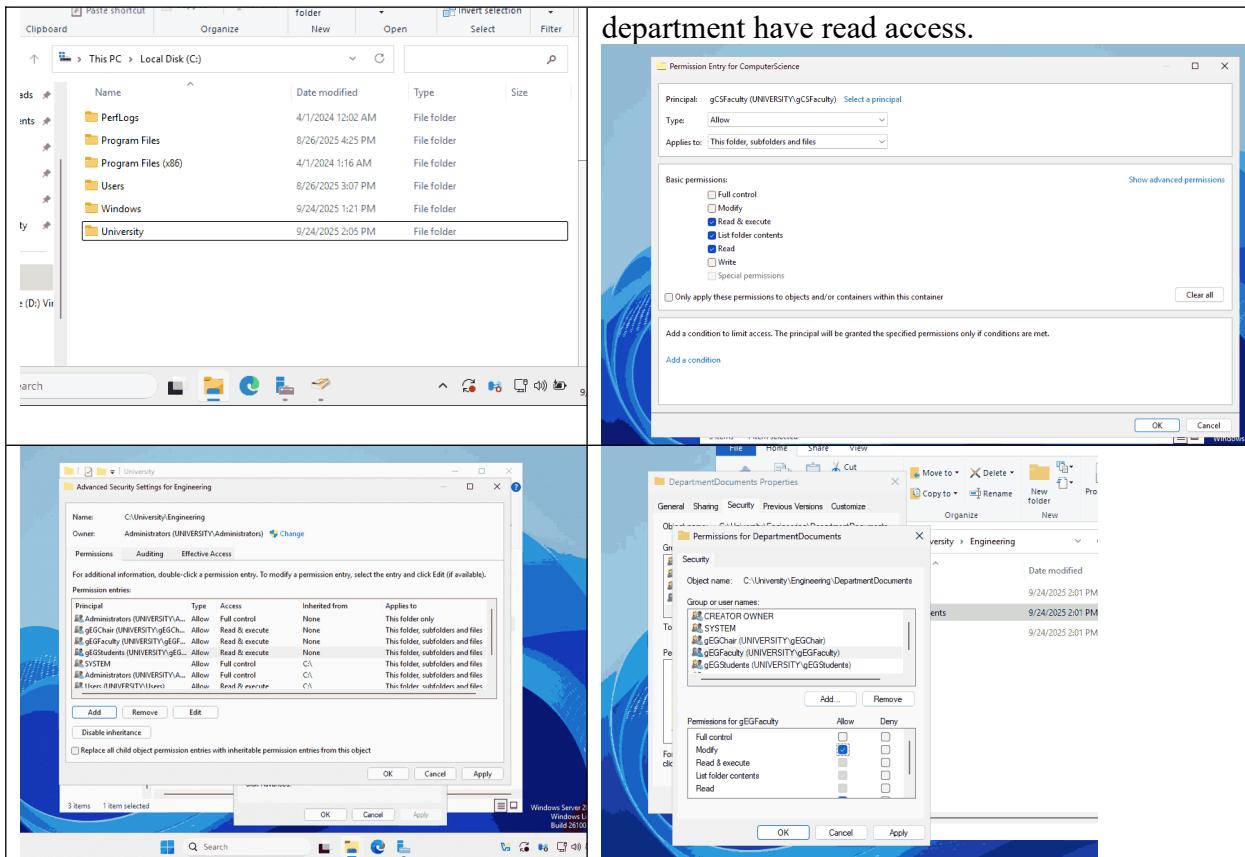


Task 4: Task 4: Setting Up Folder Permissions

Create Departmental Folders and assign permissions

Created the University document and the subfolders for each department, which are announcements, departmentDocuments, and SharedResources

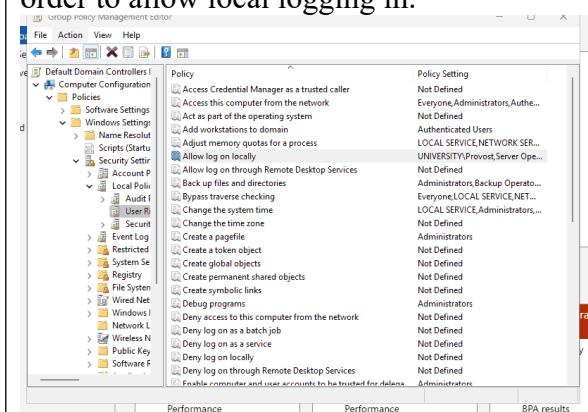
Used the powershell scripts to assign all the positions. The provost users as the owner and The chair has write access for their department folder, the Faculty write access for DepartmentDocuments and SharedResources and Students have write access for just the SharedResources. Lastly All users inside the



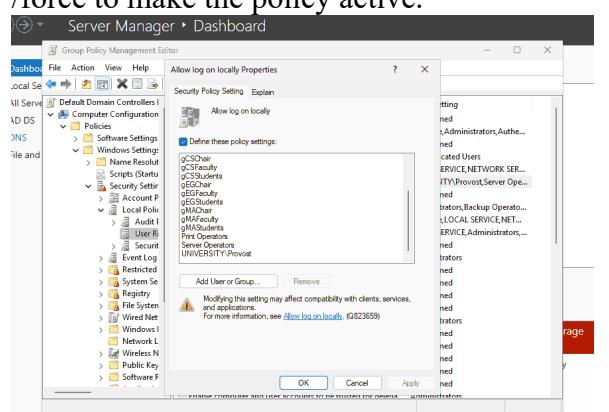
Task 5: Verifying all settings

Enable local logon of domain users onto the domain controller

Opened Group Policy Management Editor, in order to allow local logging in.

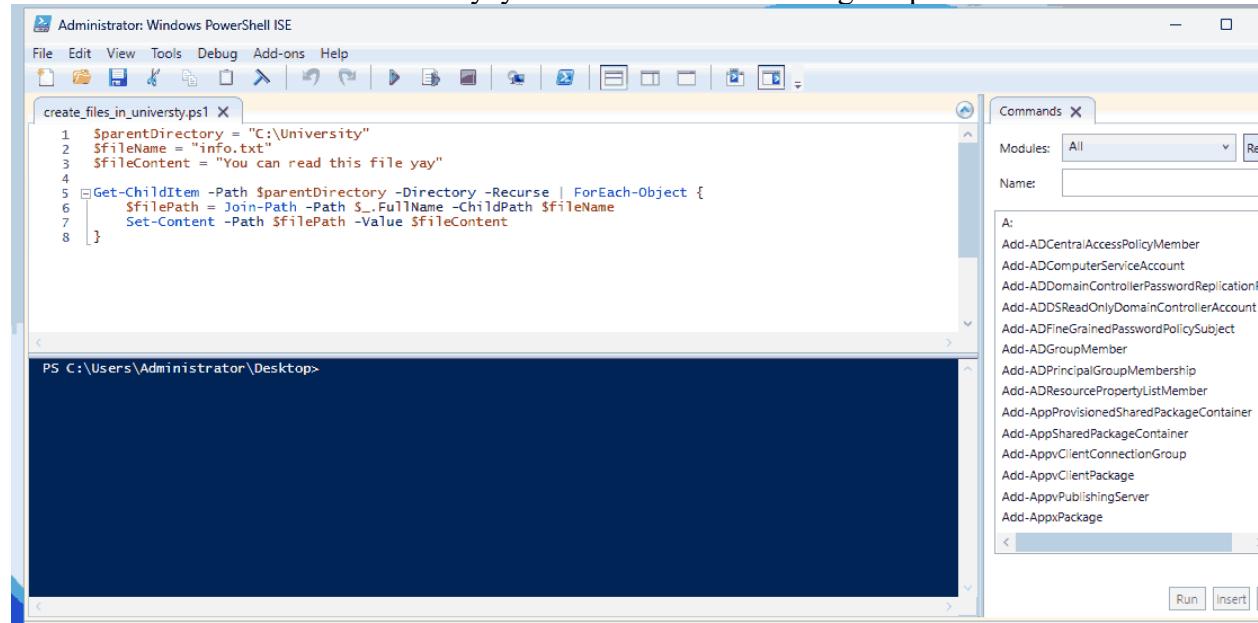


Added all the groups in and did a gpupdate /force to make the policy active.



Verifying all settings

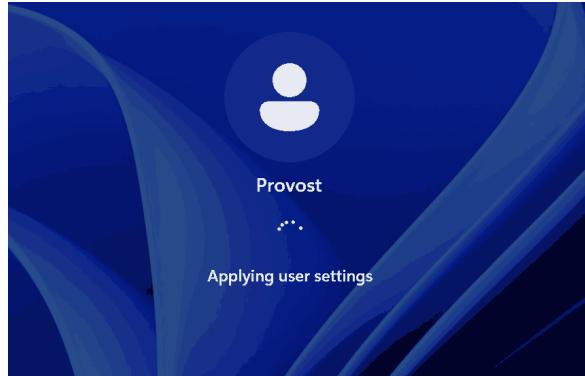
I created a script that creates a file for each directory in the University folder, all of them have the contents “You can read this file yay”. This is easier for testing the permissions of each folder.



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
create_files_in_university.ps1 X
1 $parentDirectory = "C:\University"
2 $fileName = "info.txt"
3 $fileContent = "You can read this file yay"
4
5 Get-ChildItem -Path $parentDirectory -Directory -Recurse | ForEach-Object {
6     $filePath = Join-Path -Path $_.FullName -ChildPath $fileName
7     Set-Content -Path $filePath -Value $fileContent
8 }
```

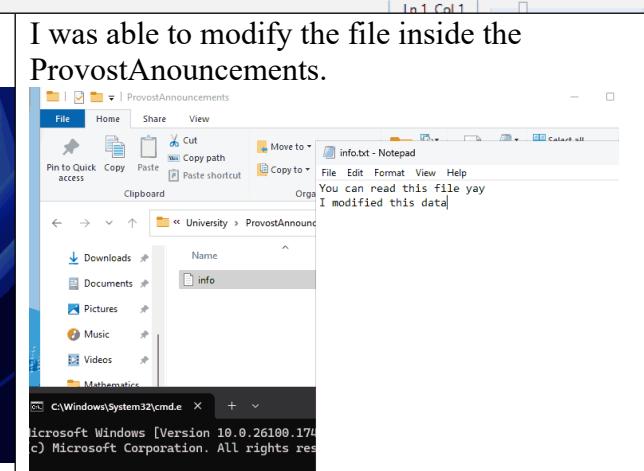
PS C:\Users\Administrator\Desktop>

Signed out of Administrator and logged in to Provost.

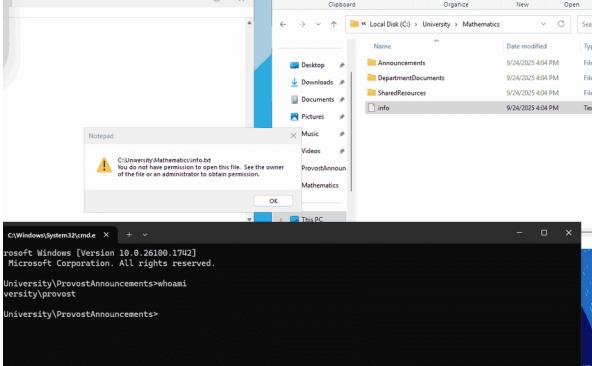
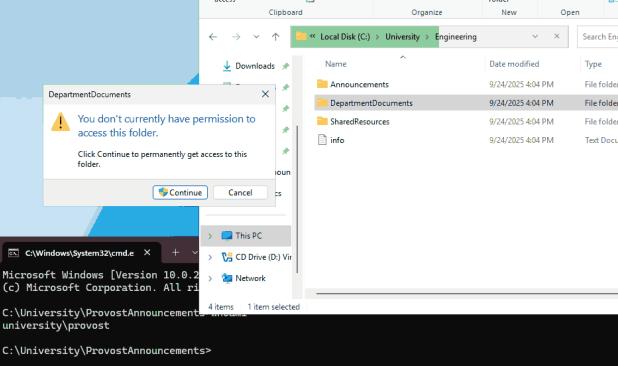
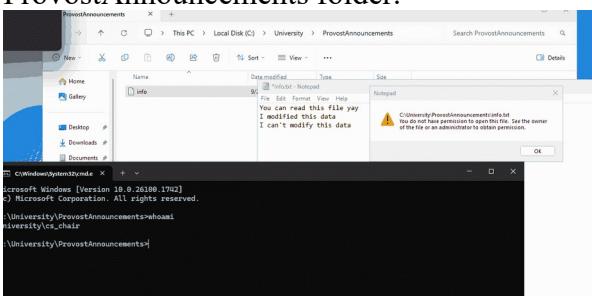
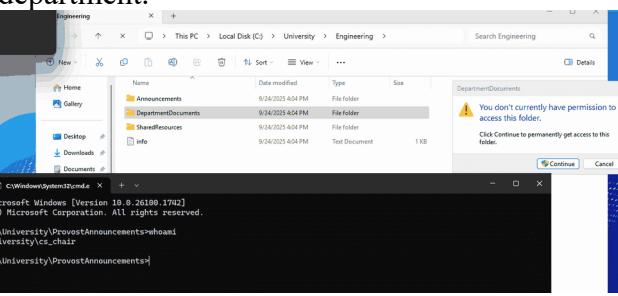
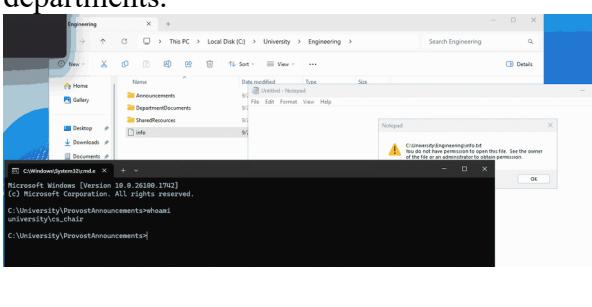
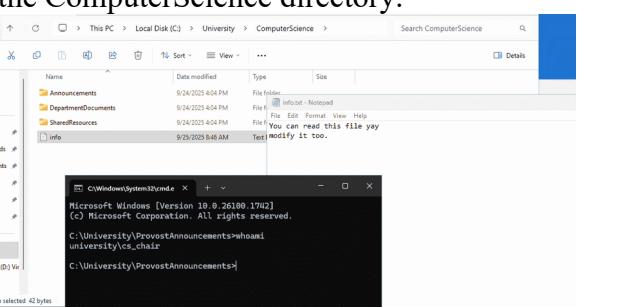
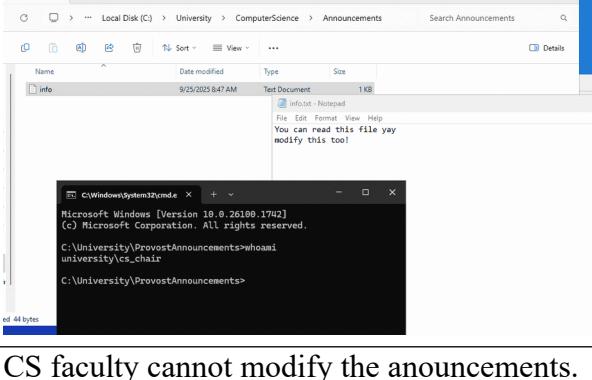
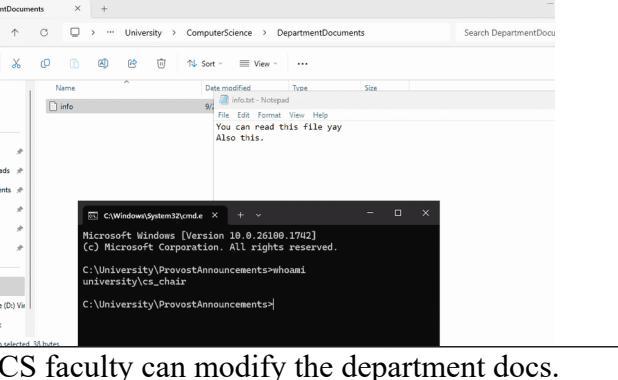


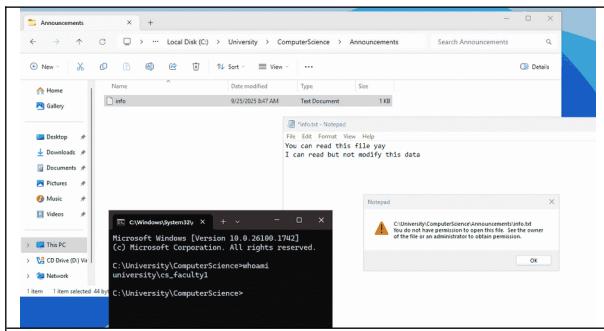
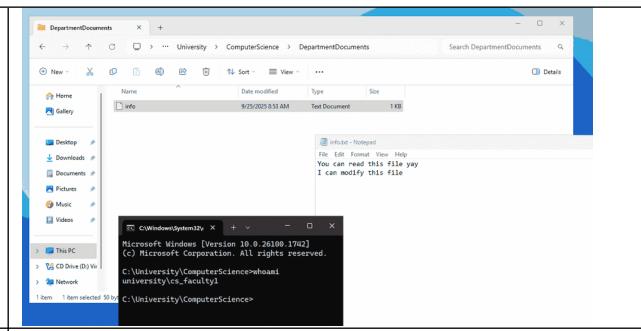
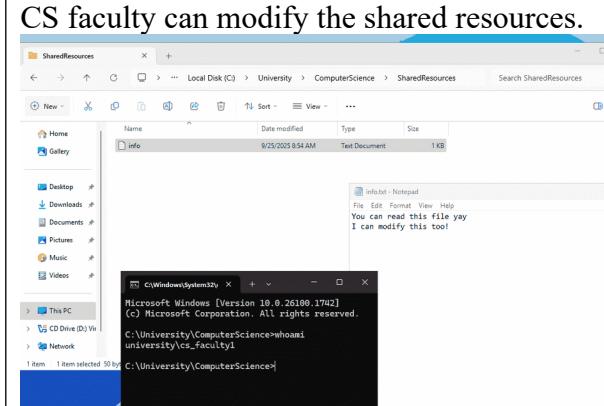
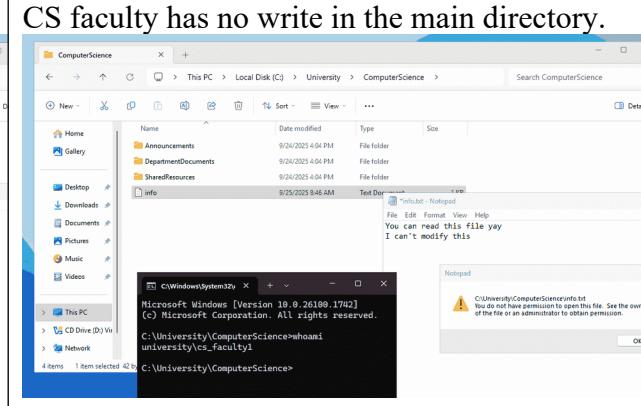
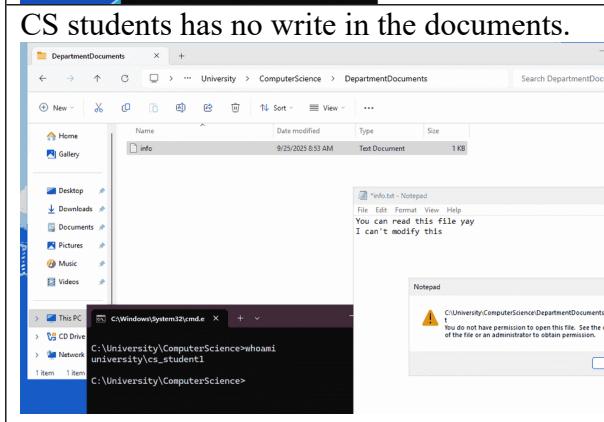
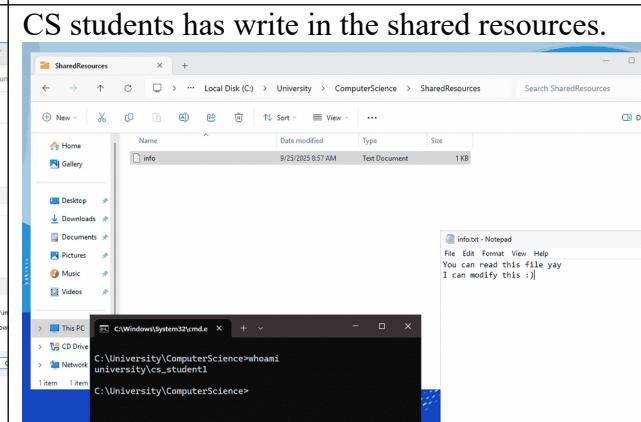
The provost user does not have read permissions for any of the departments.

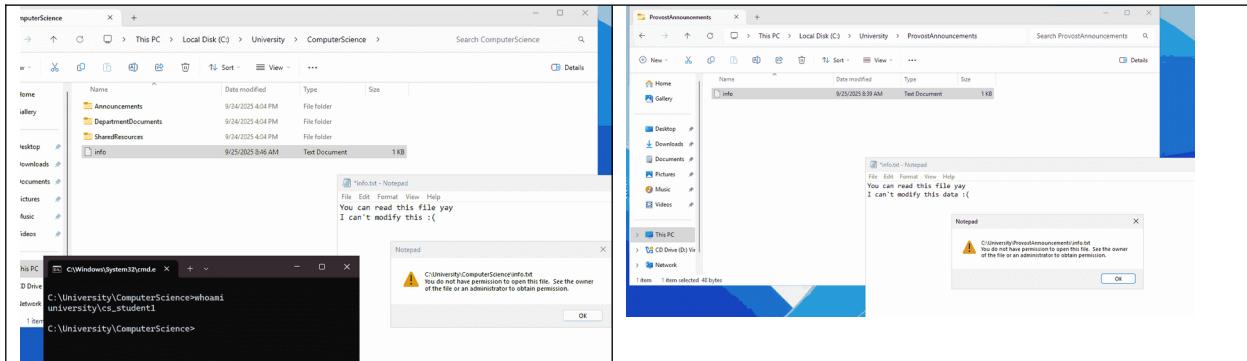
I was able to modify the file inside the ProvostAnnouncements.



The provost user does not have file listing for any of the subfolders in the departments.

	
<p>The CS chair cannot modify the ProvostAnnouncements folder.</p> 	<p>The CS chair does not have access in any other department.</p> 
<p>The CS Chair cannot read any file in other departments.</p> 	<p>The CS chair can read and write everything it the ComputerScience directory.</p> 
<p>The CS Chair can write the announcements.</p> 	<p>The CS chair can modify the Department Docs.</p> 
<p>CS faculty cannot modify the announcements.</p>	<p>CS faculty can modify the department docs.</p>

	
<p>CS faculty can modify the shared resources.</p> 	<p>CS faculty has no write in the main directory.</p> 
<p>CS students has no write in the documents.</p> 	<p>CS students has write in the shared resources.</p> 
<p>CS students has no write in main directory.</p>	<p>CS students no write in the announcements.</p>



Conclusions

The lab taught me a lot on how active directory works on windows. I learned how to create OUs and domains, how to create groups and users, configuring their permissions, so that they have either read, write or full permissions for each folder. I have learned how secure passwords policies work and enable them. I have learned about the group policy editor and how they can contain settings for the organization such as local login and password policies. I have delved into PowerShell scripting and how they can automate the process of creating users/groups and setting their permissions. Lastly, I have learned how to verify the permissions of each folder knowing who has access and what they can do with them. The output of the lab is a working windows server domain with the users and groups with the retrospective folders for them.

References

<https://github.com/ufidon/comsec/blob/main/labs/lab03/README.md>