File Sharing – Windows Server 2022

Configured secure file sharing using Share & NTFS permissions with AGDLP group design. Demonstrated ability to manage access, enforce least privilege, and validate permissions in an Active Directory environment.

Overview

This project demonstrates the configuration of secure shared folder access in a Windows Server 2022 domain environment. Tasks included AGDLP group design, folder sharing, NTFS permissions, inheritance management, effective access testing, and network drive mapping from Windows clients.

Objectives

- Create and secure shared folders using Share + NTFS permissions
- Implement Microsoft AGDLP model (Accounts → GG → DL → Permissions)
- Remove inherited permissions and apply explicit ACLs
- Validate access using domain user accounts
- Map shared folders via GUI and command-line tools

Key Tasks Completed

- Created shared folder C:\Student_Files
- Applied Share permissions (Everyone – Full Control, for initial config)
- Applied NTFS permissions through Domain Local groups (RO, RW, M, FC)
- Removed inherited permissions and converted to explicit ACLs
- Tested access using domain users (Students vs Lecturers)
- Mapped network drives using GUI & net use command
- Implemented effective permission testing

Skills

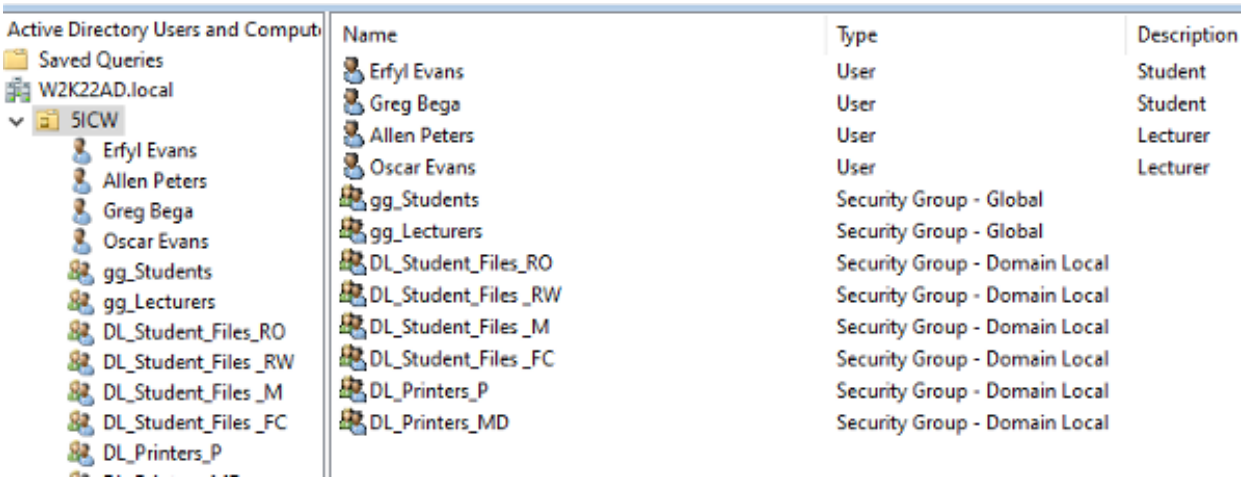
- Share & NTFS Permission Management
- Domain Local vs Global Group design (AGDLP)
- Drive Mapping (Explorer & net use)
- Print Management & Permission Delegation
- Windows Server 2022 Administration
- Group-based Permission Delegation
- Access Testing & Troubleshooting

Evidence / Screenshots

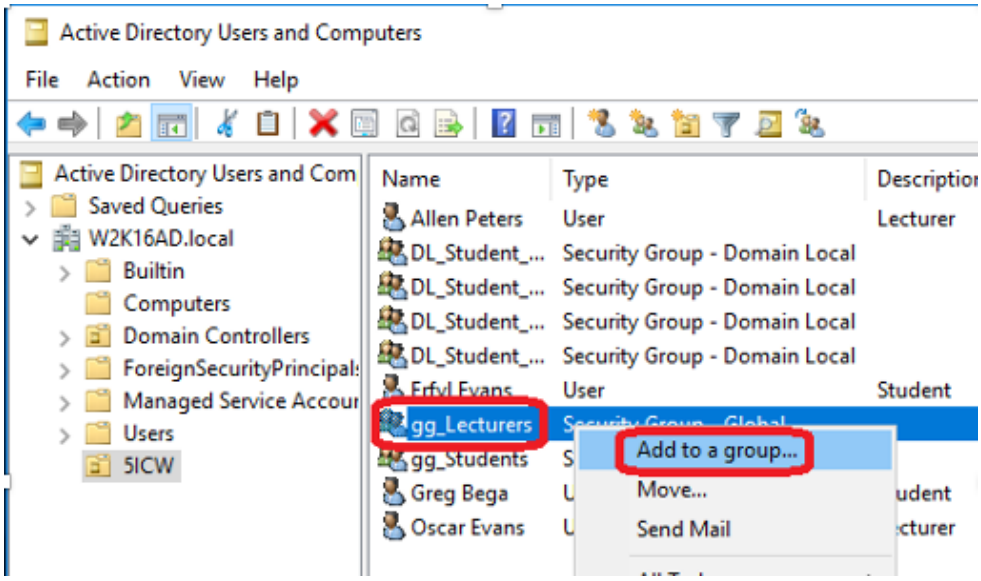
Shared Folder & Permission Structure

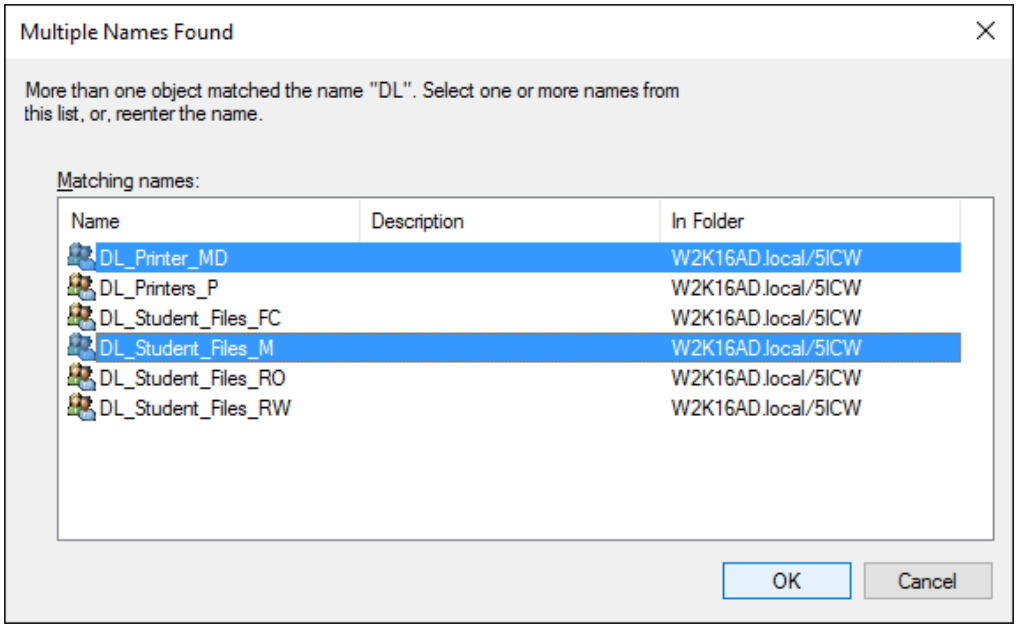
1. Domain Local Group Structure (AGDLP)

Created security groups for file access based on Microsoft best practices

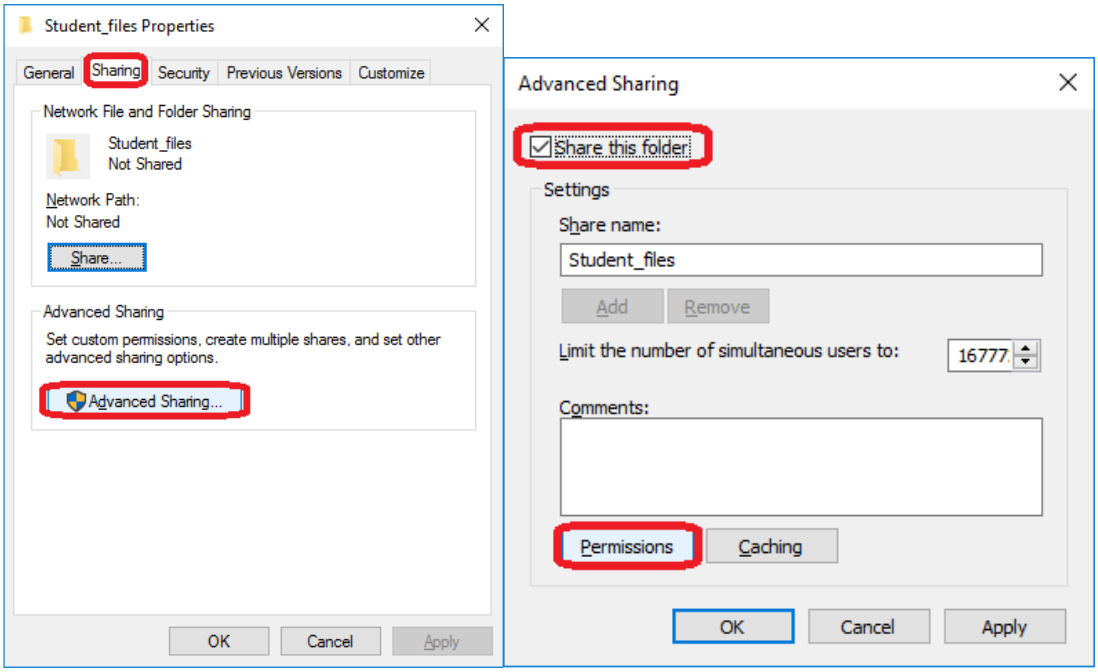


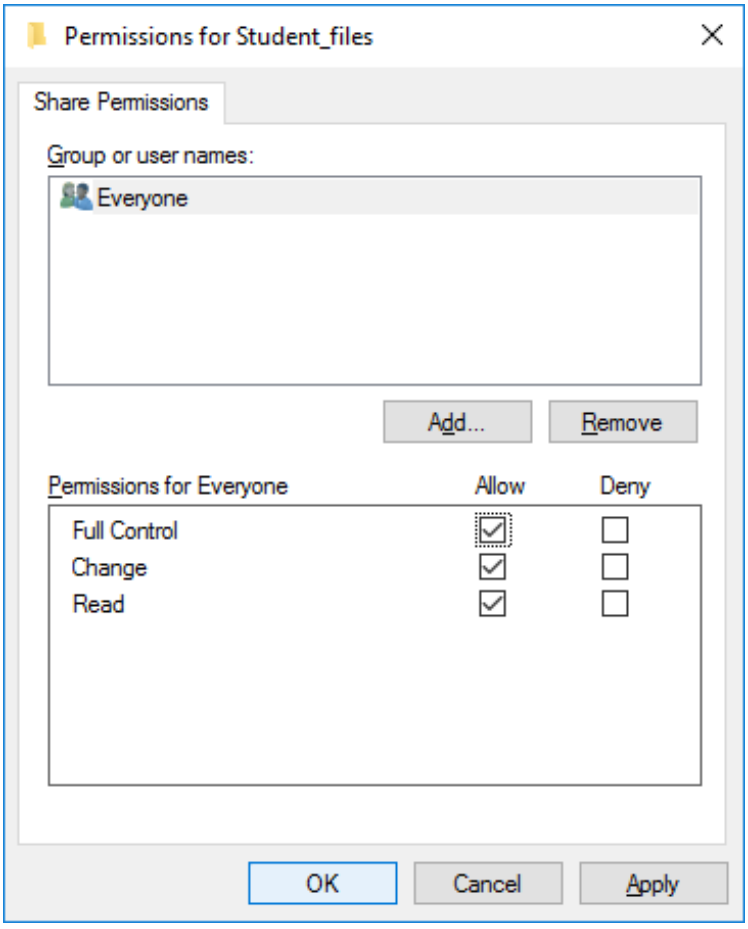
2. Group Nesting Example (gg_Lecturers added to DL_Student_Files_M)





3. Shared C:\Student_Files with initial Full Control via Share Permissions

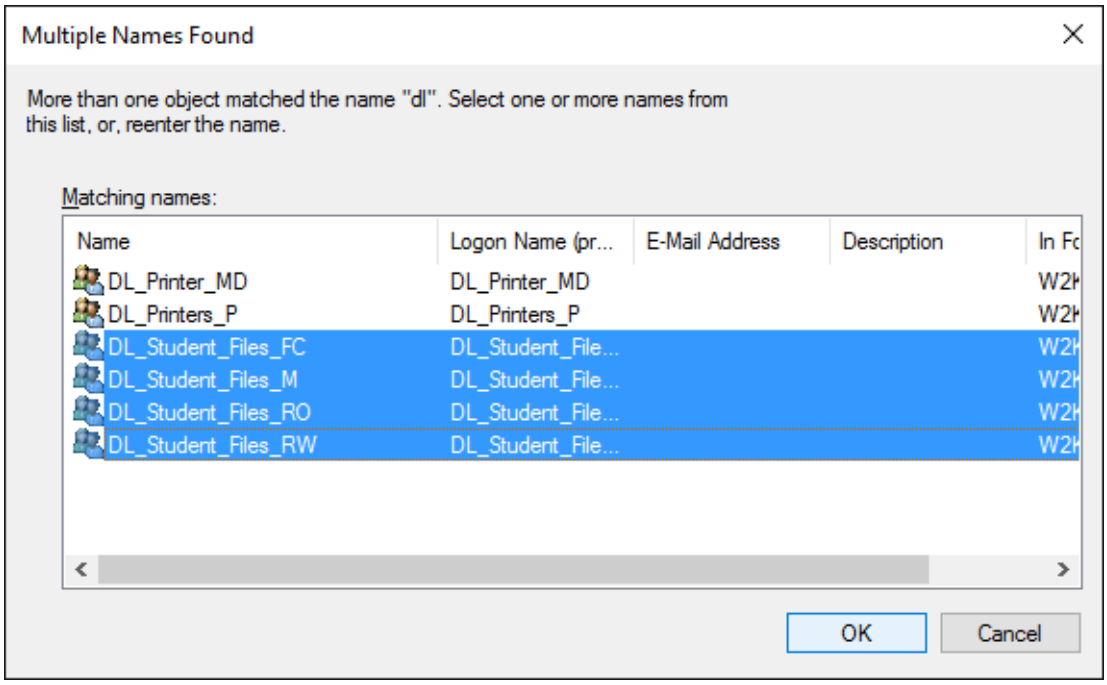




4. NTFS Permissions (Security Tab)

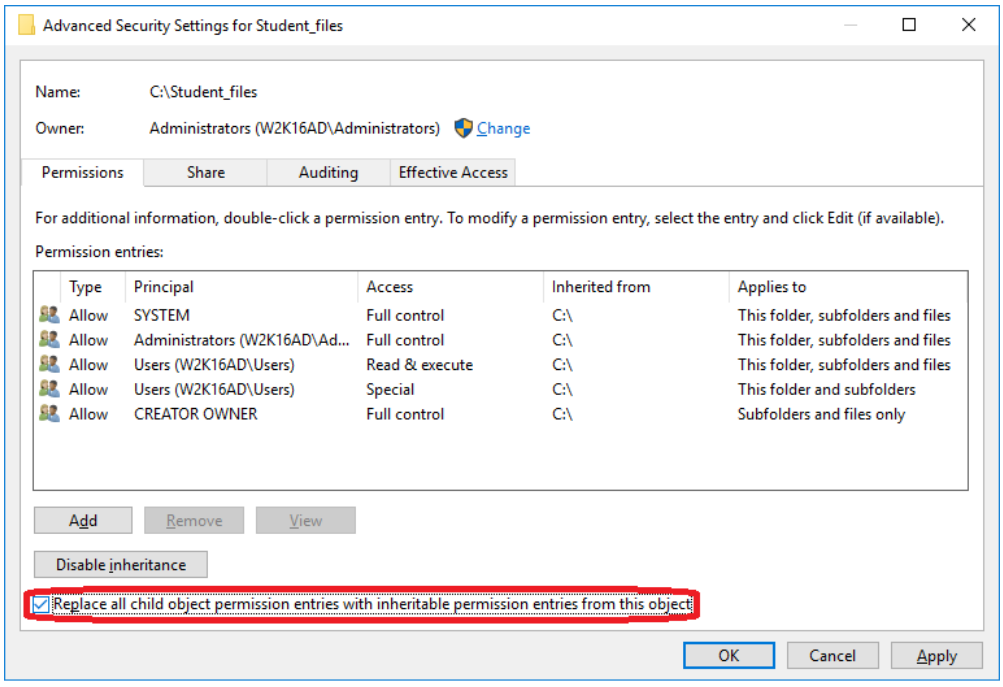
Applied NTFS permissions using Domain Local groups

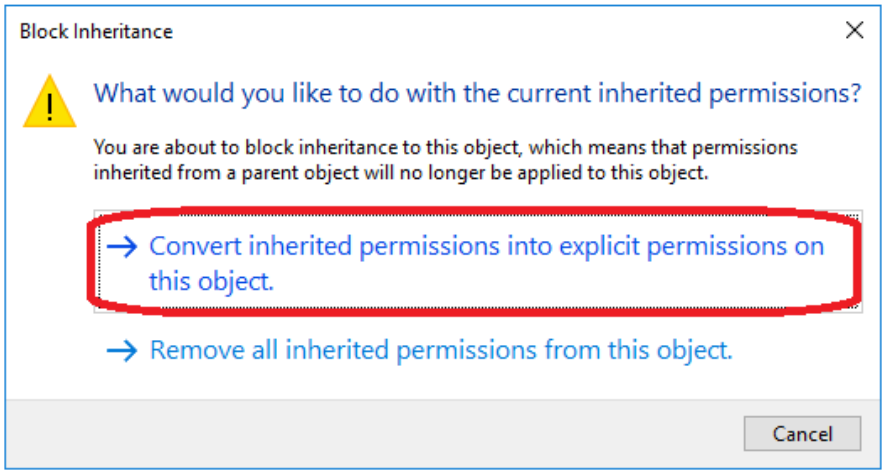
RO = Read & Execute / RW = Read, Write / M = Modify / FC = Full Control



5. Inheritance Removed / Explicit Permissions

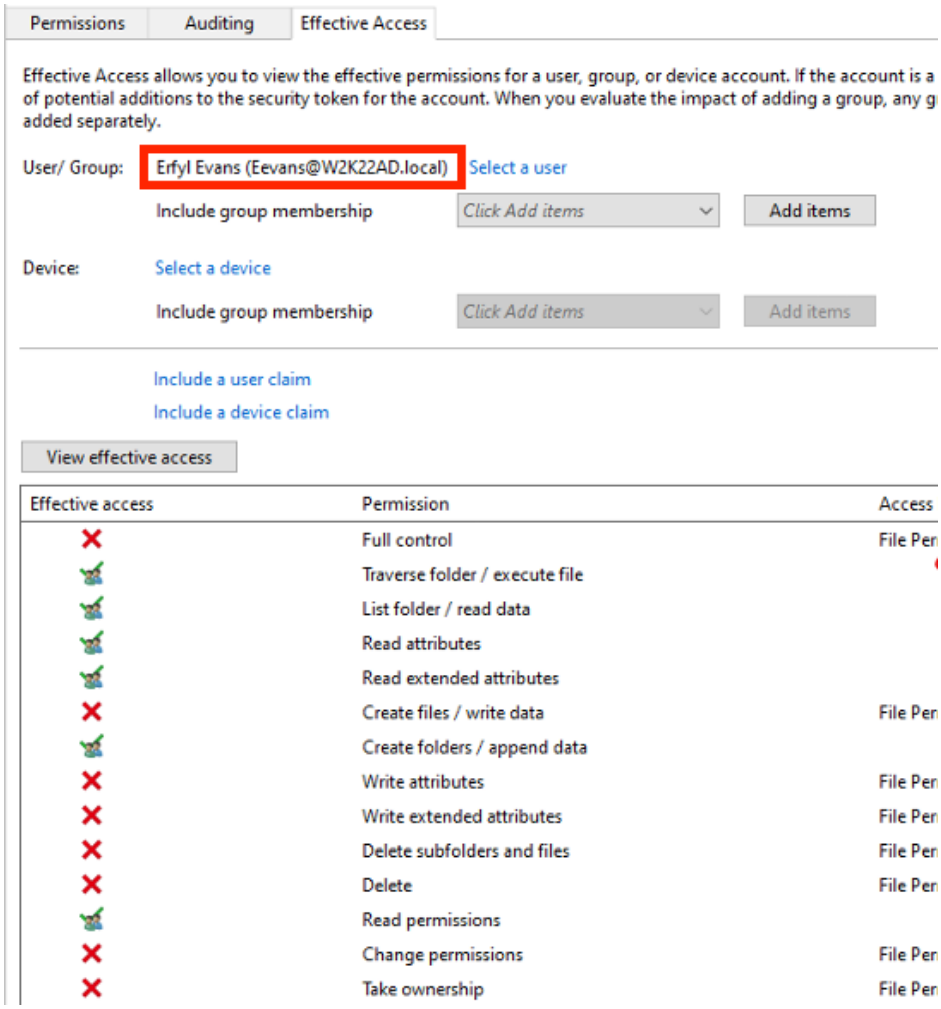
Disabled inheritance and converted inherited permissions to explicit entries





6. Inheritance Removed / Explicit Permissions

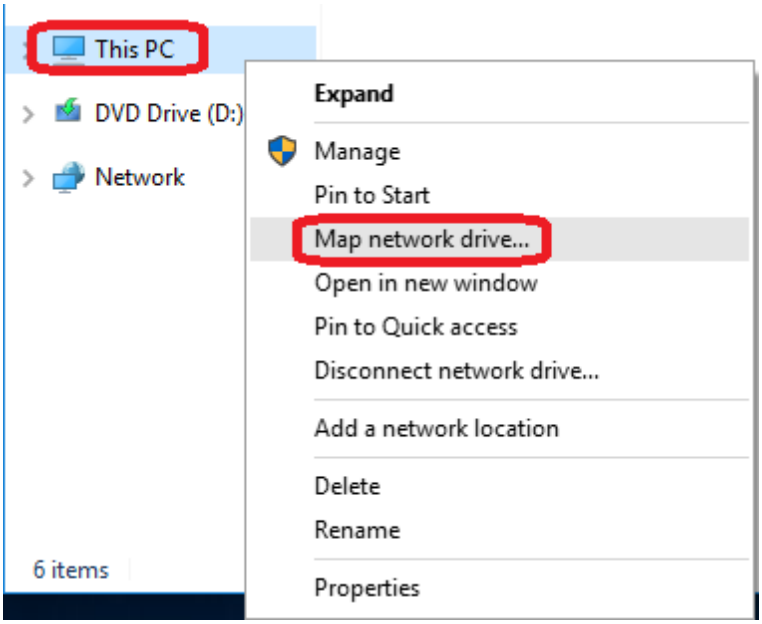
Tested effective permissions using user EEvans (Read only)

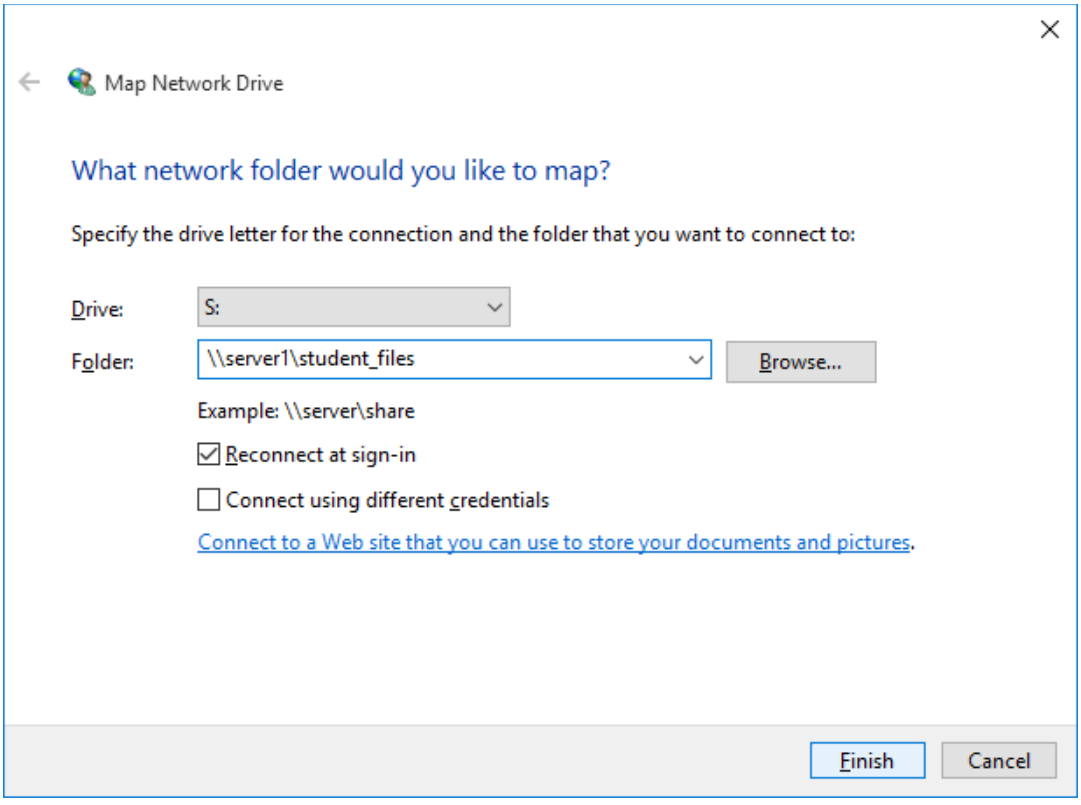


7. Drive Mapping Verification

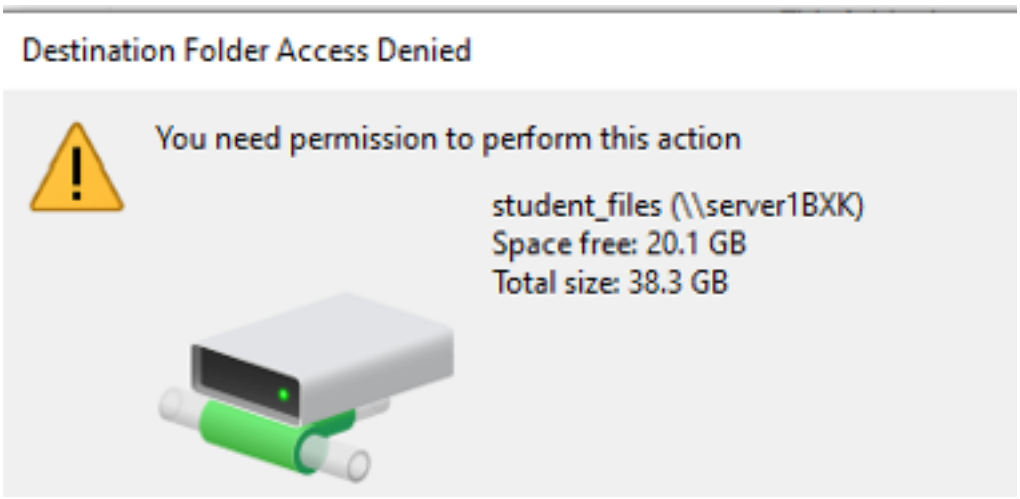
Mapped share as S:\ (student) and L:\ (lecturer)

Verified write access difference between accounts

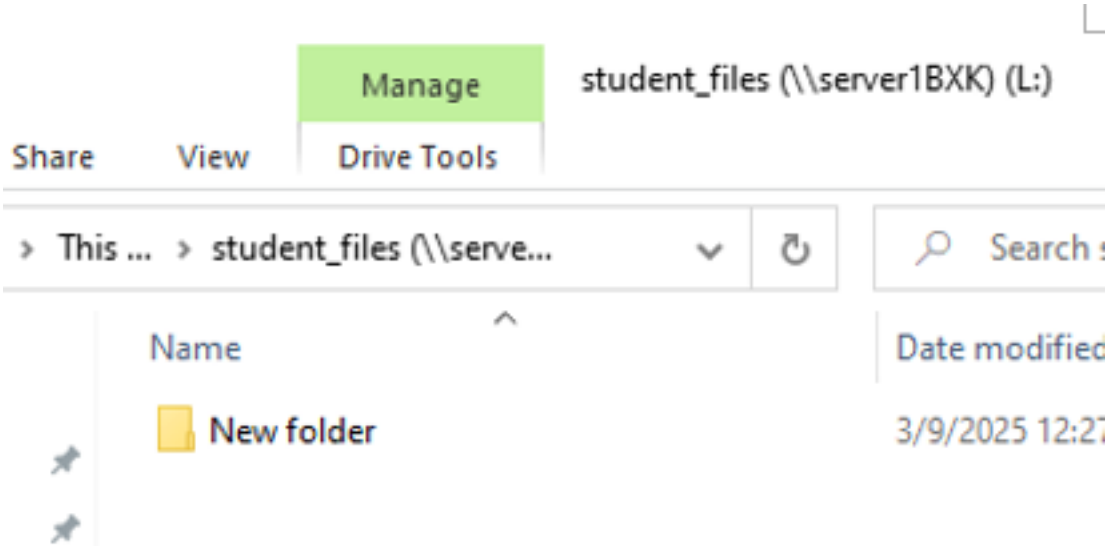




Eevans (Student)



APeters (Lecturer)



Summary

This lab demonstrates secure file sharing and access control using Active Directory, NTFS permissions, and the AGDLP model. By separating user groups from permission groups and applying explicit ACLs, the environment follows real enterprise standards for security and manageability.