

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

Active Directory Users and Computers	Name	Type	Description
Saved Queries	Erfyl Evans	User	Student
W2K22AD.local	Greg Bega	User	Student
5ICW	Allen Peters	User	Lecturer
	Oscar Evans	User	Lecturer
	gg_Students	Security Group - Global	
	gg_Lecturers	Security Group - Global	
	DL_Student_Files_RO	Security Group - Domain Local	
	DL_Student_Files_RW	Security Group - Domain Local	
	DL_Student_Files_M	Security Group - Domain Local	
	DL_Student_Files_FC	Security Group - Domain Local	
	DL_Printers_P	Security Group - Domain Local	
	DL_Printers_MD	Security Group - Domain Local	

2. Group Nesting Example (gg_Lecturers added to DL_Student_Files_M)

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

Saved Queries

W2K16AD.local

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipal
- Managed Service Account
- Users
- 5ICW

Name	Type	Description
Allen Peters	User	Lecturer
DL_Student_...	Security Group - Domain Local	
DL_Student_...	Security Group - Domain Local	
DL_Student_...	Security Group - Domain Local	
DL_Student_...	Security Group - Domain Local	
Eryl Evans	User	Student
gg_Lecturers	Security Group - Global	
gg_Students	Security Group - Global	
Greg Bega	User	Student
Oscar Evans	User	Lecturer

gg_Lecturers

Add to a group...

Multiple Names Found

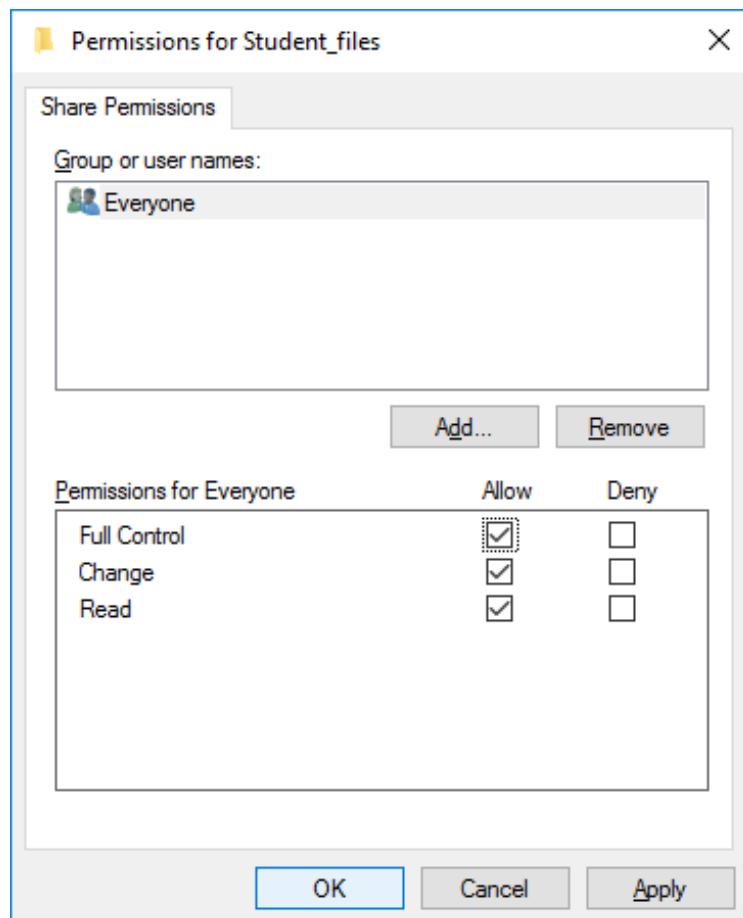
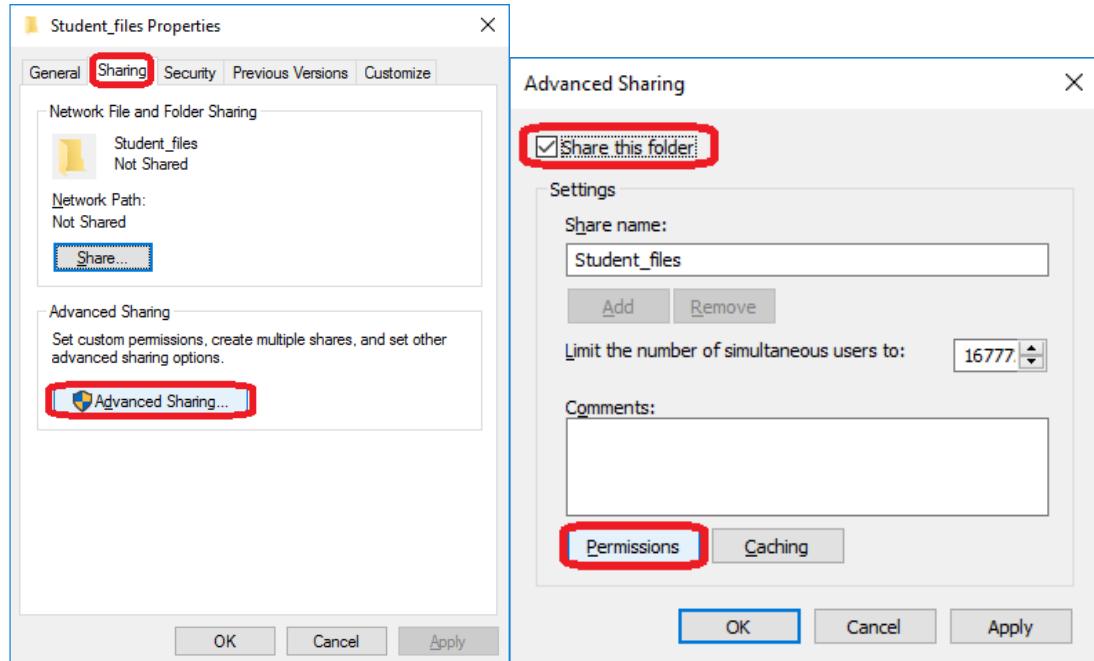
More than one object matched the name "DL". Select one or more names from this list, or, reenter the name.

Matching names:

Name	Description	In Folder
DL_Printer_MD		W2K16AD.local/5ICW
DL_Printers_P		W2K16AD.local/5ICW
DL_Student_Files_FC		W2K16AD.local/5ICW
DL_Student_Files_M		W2K16AD.local/5ICW
DL_Student_Files_RO		W2K16AD.local/5ICW
DL_Student_Files_RW		W2K16AD.local/5ICW

OK Cancel

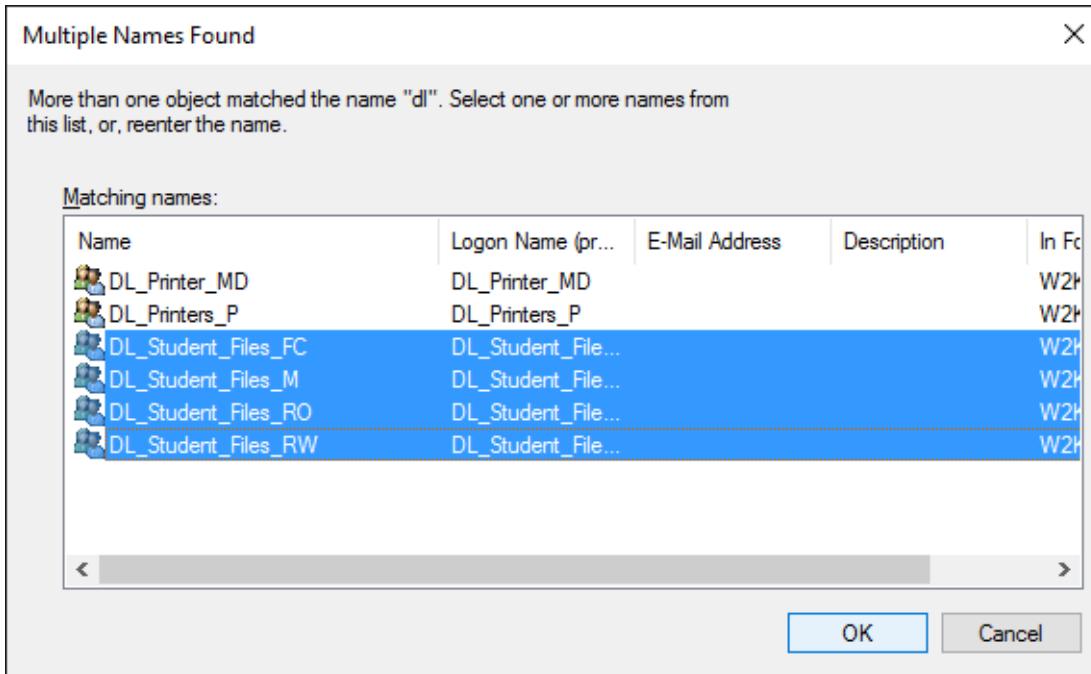
3. Shared C:\Student_Files with initial Full Control via Share Permissions



4. NTFS Permissions (Security Tab)

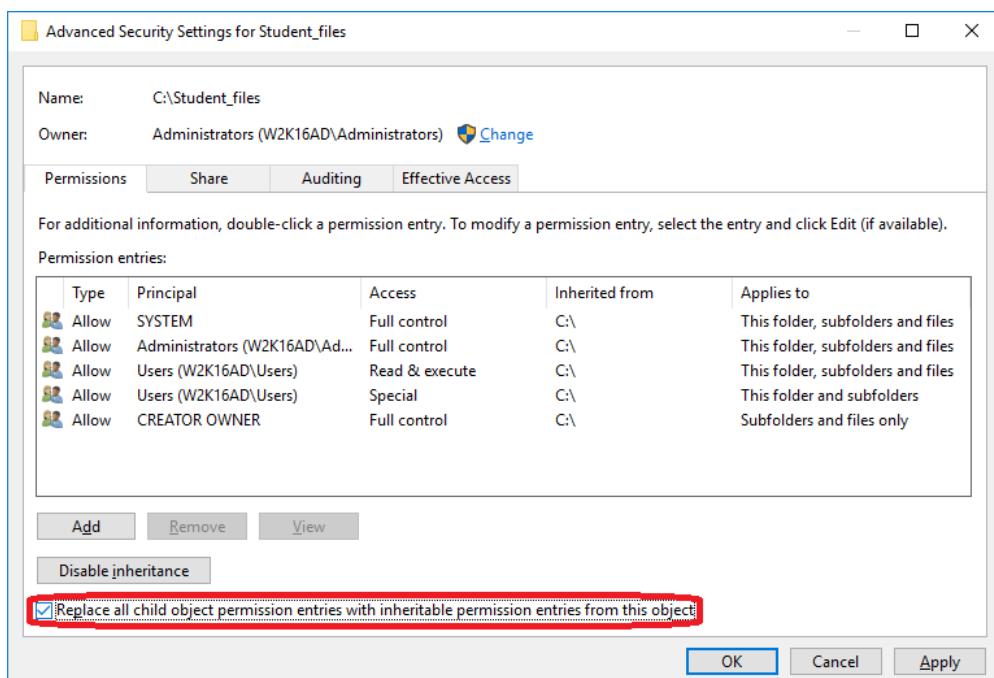
Applied NTFS permissions using Domain Local groups

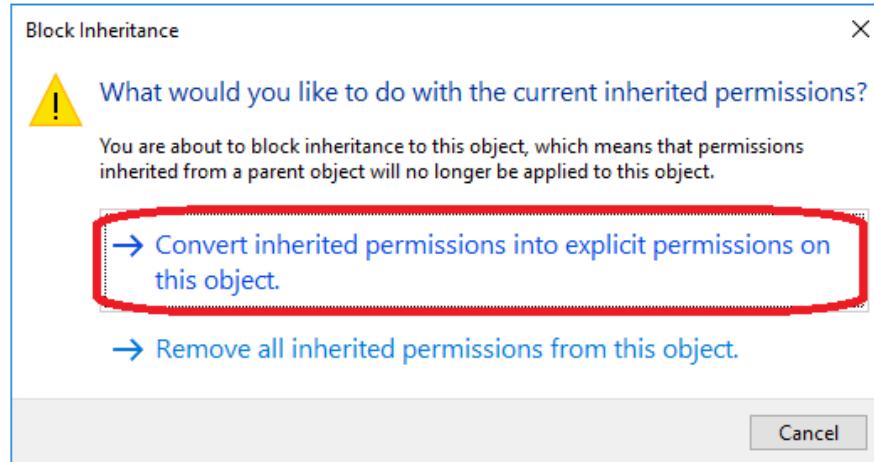
RO = Read & Execute / RW = Read, Write / M = Modify / FC = Full Control



5. Inheritance Removed / Explicit Permissions

Disabled inheritance and converted inherited permissions to explicit entries





6. Inheritance Removed / Explicit Permissions

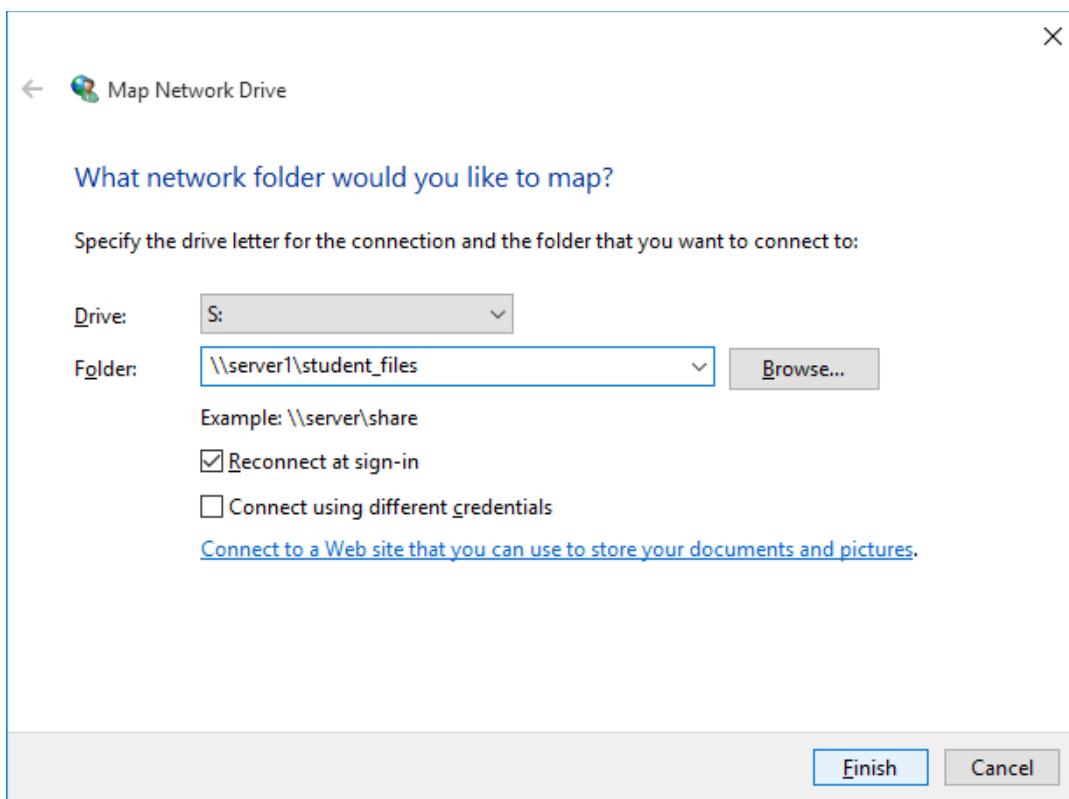
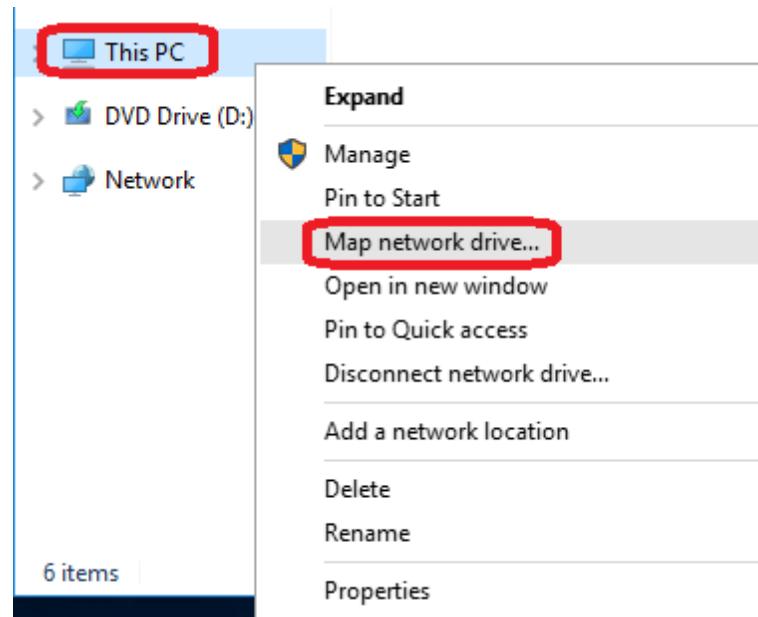
Tested effective permissions using user EEvans (Read only)

Permissions	Auditing	Effective Access
<p>Effective Access allows you to view the effective permissions for a user, group, or device account. If the account is a member of a group, the permissions for that group are included. If the account is a member of multiple groups, the permissions for all groups are included.</p> <p>User/ Group: Erfyl Evans (Eevans@W2K22AD.local) Select a user</p> <p>Device: Select a device</p> <p>Include group membership Click Add items Add items</p> <p>Include a user claim</p> <p>Include a device claim</p> <p>View effective access</p>		
Effective access	Permission	Access
	Full control	File Pen
	Traverse folder / execute file	File Pen
	List folder / read data	File Pen
	Read attributes	File Pen
	Read extended attributes	File Pen
	Create files / write data	File Pen
	Create folders / append data	File Pen
	Write attributes	File Pen
	Write extended attributes	File Pen
	Delete subfolders and files	File Pen
	Delete	File Pen
	Read permissions	File Pen
	Change permissions	File Pen
	Take ownership	File Pen

7. Drive Mapping Verification

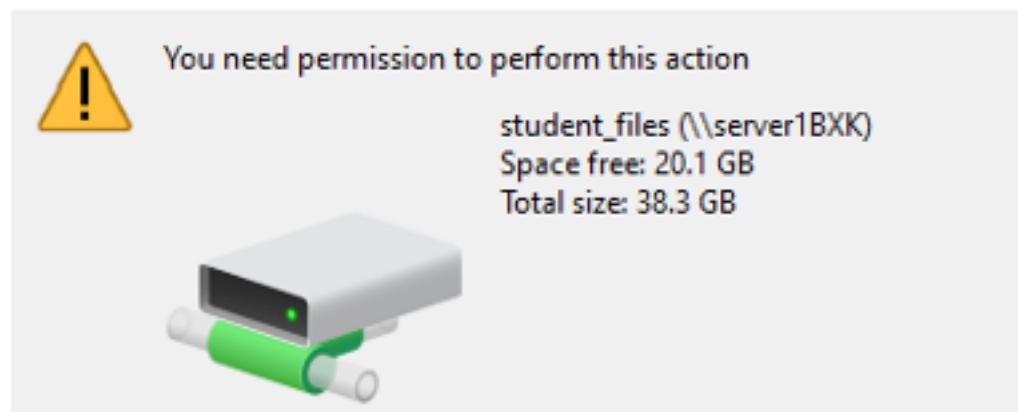
Mapped share as S:\ (student) and L:\ (lecturer)

Verified write access difference between accounts

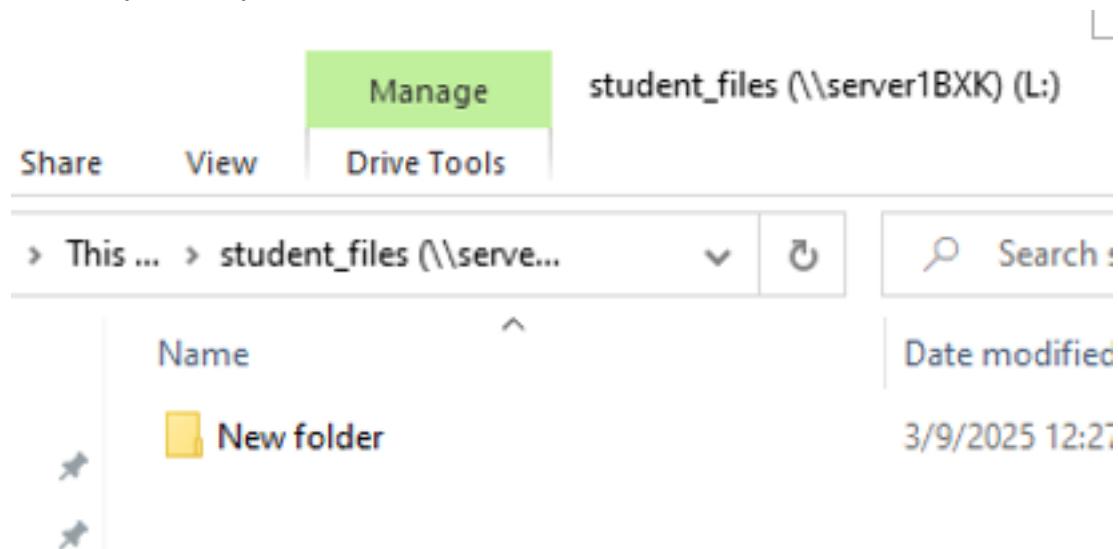


Eevans (Student)

Destination Folder Access Denied



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.