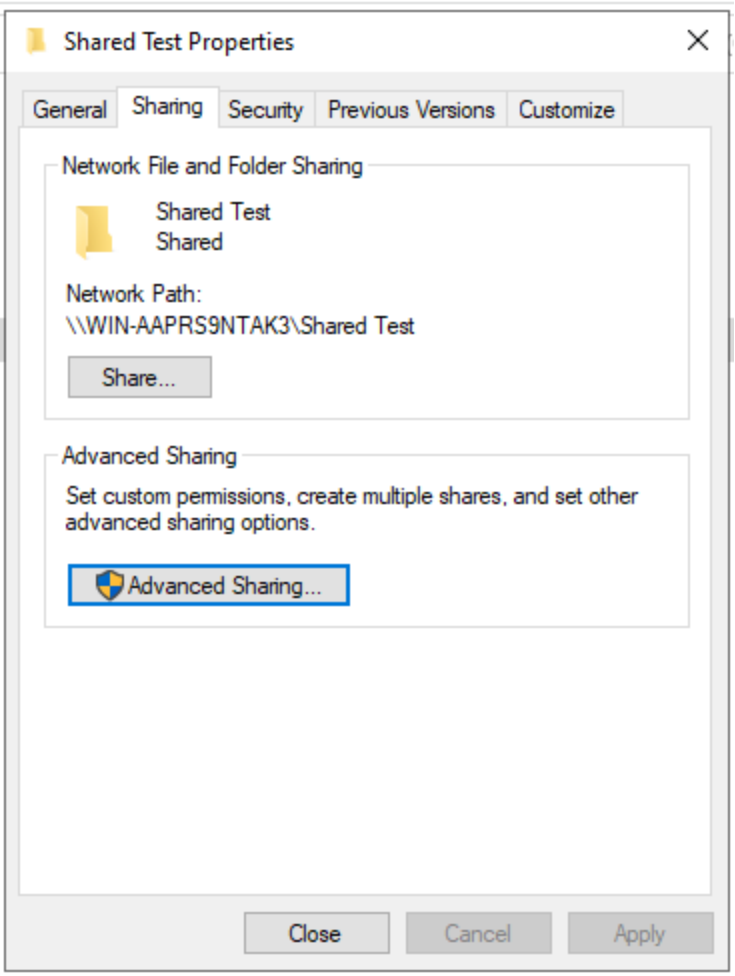
File and Folder Sharing and Access Control

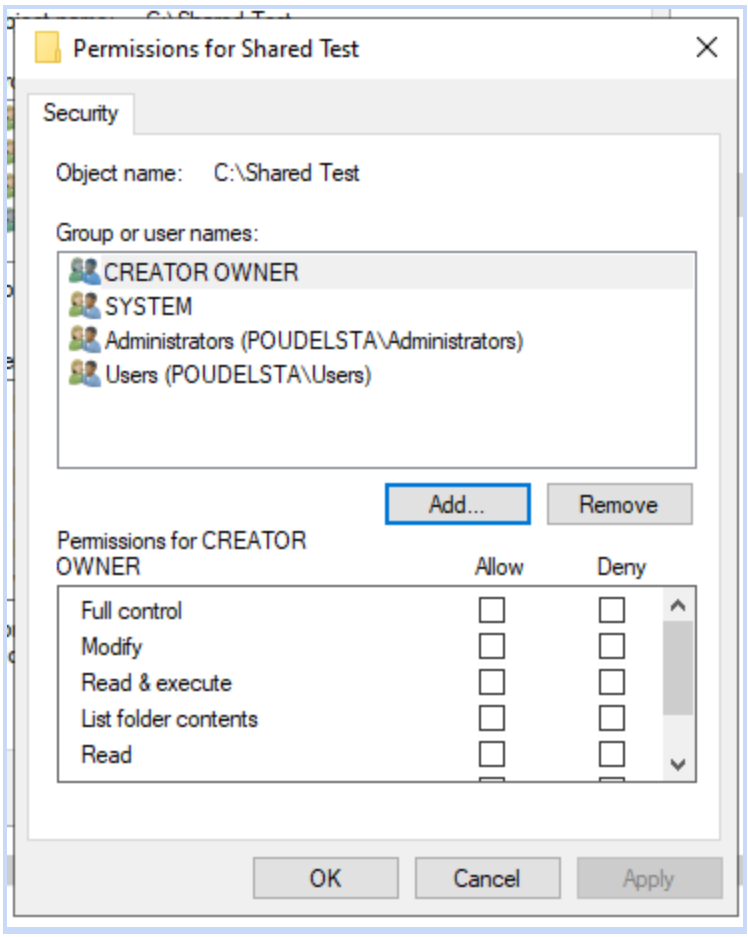
In a domain environment, there are two types of file sharing: **Local** and **Network**. Access is governed by two permission types **NTFS** and **Share** and four access control levels: **Read**, **Write**, **Execute**, and **Full Control**.

Part 1: Setting Up and Testing Shared Access

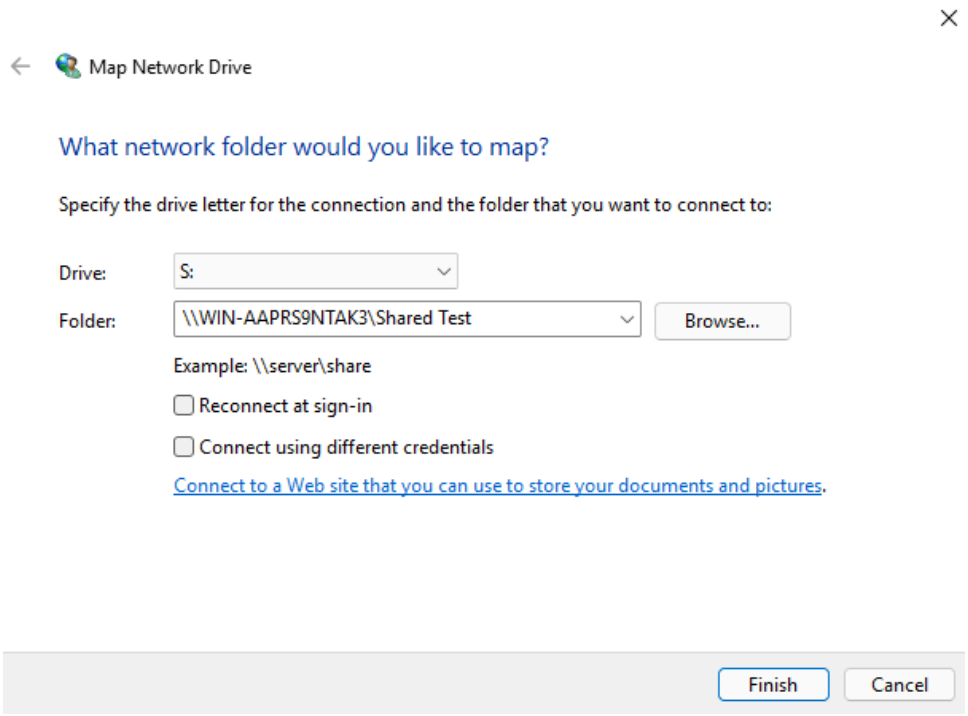
1. **Create and Configure Share Permission:**
    - We will go to our Windows Server 2022 and open File Explorer.
    - Under **"This PC"**, we will create a folder and name it **"Shared Test"**.
    - **Right-click** on the folder and click **Properties**.
    - Go to the **Sharing** tab, then click **Advanced Sharing**.
    - Check the **"Share this folder"** box, and then click **Permissions**.
    - The default permission is **Everyone** with **Read** access. We will keep this for general access.
    - Click **Add**, type domain users in the text field, and select the **Domain Users** group.
    - We will leave **Domain Users** set to **Read**. Click **Apply** and **OK**. Click **Apply** and **OK** again on the **Advanced Sharing** window.
    - **Note:** We must copy the **Network Path** (\\WIN-AAPRS9NTAK3\Shared Test), as we will use it to map the drive later.



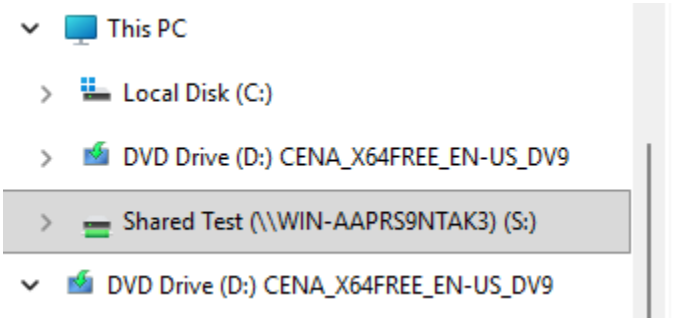
2. **Configure NTFS Permission:**
    - In the same folder **Properties** window, click the **Security** tab. This is where detailed, object-level permissions are controlled.
    - To give a specific user or group custom access, click **Edit**, and then click **Add** to find a new user or group. We can then apply specific permissions (e.g., Modify, Read & Execute) as needed.



3. **Test Mapped Network Drive (Manual Connection):**
    - We will log in to the client Windows 11 VM.
    - Open File Explorer, **right-click** on **This PC**, and select **Map network drive**.
    - We will select a drive letter (e.g., **S:** for Shared) and paste the **Network Path** copied from the server.
    - We will **uncheck** "Reconnect at sign-in" (to demonstrate the GPO fix later), and click **Finish**.



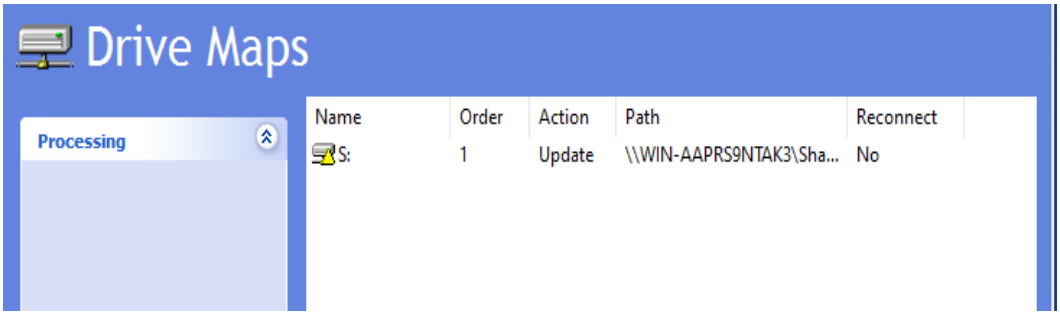
- We have successfully mapped the network drive to the Shared Test folder on the client machine.
-



- However, a crucial issue exists with this current configuration:
  i. The mapped drive we just created is a **non-persistent connection**.
  ii. If the client machine is rebooted, the network drive mapping will be lost.

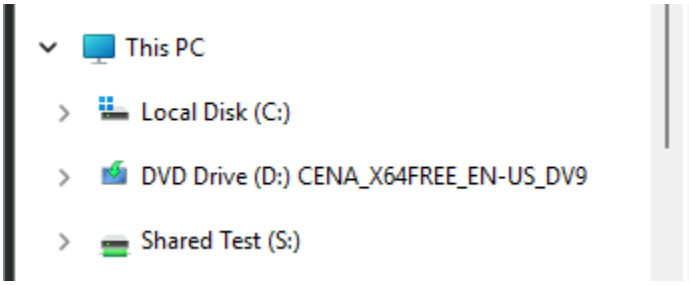
4. **Fix Persistent Mapping using GPO (User Preference):**
   - We will return to the Server and open **Group Policy Management**.
   - We will **right-click Group Policy Objects** and click **New**, naming it **Mapped Drives**.
   - **Right-click** the new GPO and click **Edit**.

- **Configuration (User Configuration Preference):** This is for users, so we navigate through **User Configuration > Preferences > Windows Settings > Drive Maps**.
- **Right-click Drive Maps > New > Mapped Drive**.
- We input the **Location** (the network path), set the **Label** to a friendly name like **Shared Test**, and select the **Drive Letter** (S:). Click **Apply** and **OK**.
-



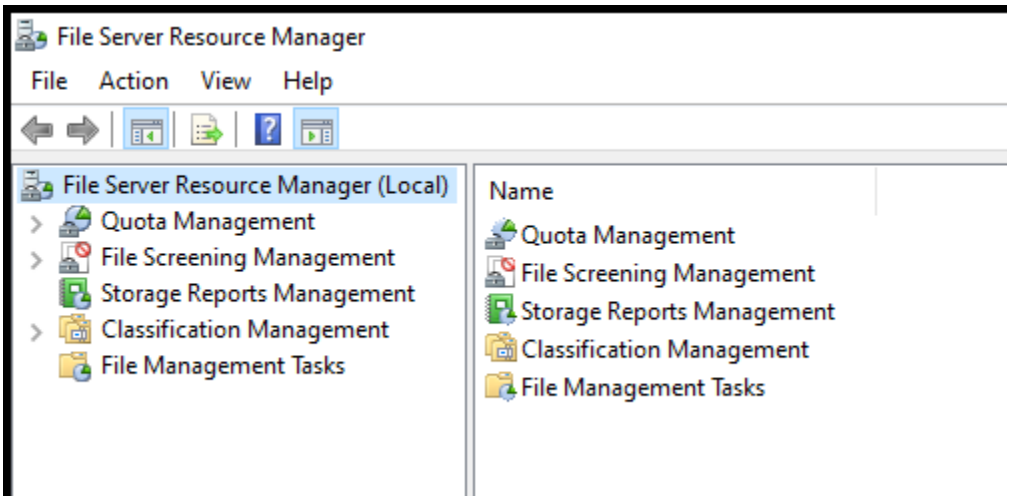
- **Linking:** We will drag and drop the **Mapped Drives** GPO onto the **Retail_Branches > Users** OU.

- On the client machine, we open Command Prompt and type gpupdate /force, then reboot the computer. Upon re-logging in, we will verify the File Explorer now shows the persistent drive mapped with the friendly label **Shared Test**.



Implementing Quotas and File Screening (FSRM)

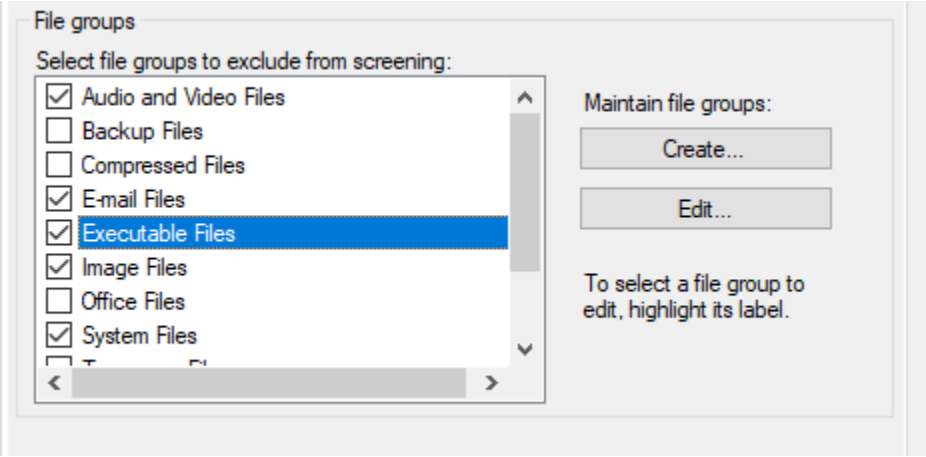
To manage storage efficiently, we will use **File Server Resource Manager (FSRM)**, found under **Windows Administrative Tools** on the server.



1. **Set Up Quota Management:**
    - Quotas set a maximum storage limit on a folder to prevent users from maximizing disk space.
    - We will expand **Quota Management** and **right-click** on **Quotas**, then select **Create Quota**.
    - We will browse to the **Shared Test** folder.
    - We will select **Define custom quota properties** and click **Custom Properties**. We can choose a limit (e.g., 10 GB) and set a **Hard Quota** (stopping users from exceeding the limit).
    - Under **Notification thresholds**, we will click **Add**. We can set a threshold (e.g., 80% usage) and check the box to send an email notification to an administrator or IT distribution list, and to the user.

2. **Set Up File Screening Management:**
    - File screening is used to block or allow specific file types (e.g., blocking video files from a document share).

- We will **right-click File Screens** and select **Create File Screen**.
- We will browse the path again and select the **Shared Test** folder.
- We will select **Define Custom file screen properties** and click **Custom Properties**.
- In the **Settings** tab, we will select which file groups to **allow** or **block**. We will configure it to **allow** only **Text Files** and **Office Files**. Click **OK**.



- This creates an templet for us as well. And we can see thaat C:\\Shared Test allowing Officeand text Files.