Windows File Sharing Scenarios

File System Permissions

- **Explicit Permissions:**
    - Directly assigned and customized for individual files or folders (objects).
    - **Always** take priority over inherited permissions.
- **Inherited Permissions:**
    - Automatically passed down from a parent folder to its children.
    - An object inherits the permissions set on its parent by default.

Network Access Methods

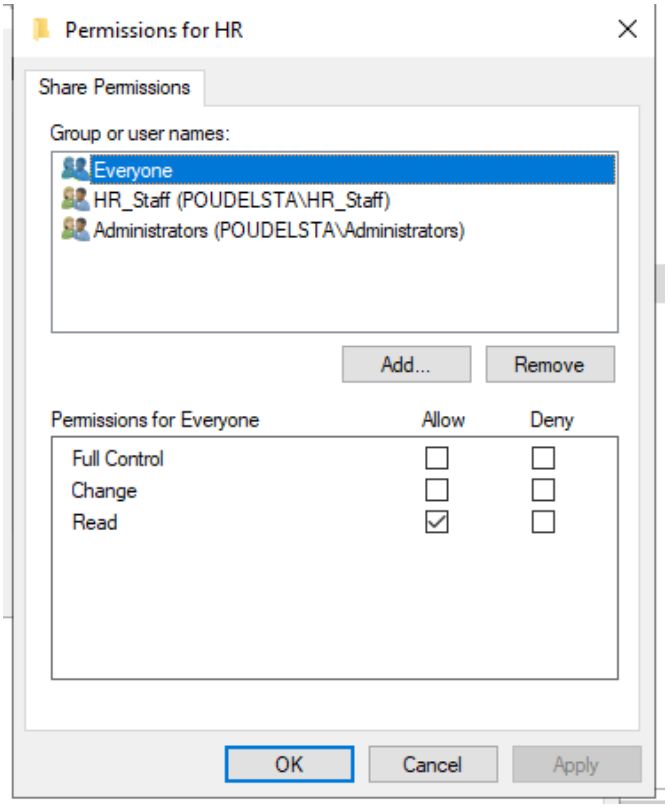
- **Mapped Drive (Persistent Access):**
    - A network share assigned to a local drive letter on the user's computer (e.g., Z:).
    - Connections can be configured to **persist** across reboots.
- **Network Path (Direct Access):**
    - The shared folder is accessed directly using its specific UNC path (e.g., \\ServerName\ShareName).
    - Connections are often **non-persistent** (temporary access).

We must remember the cardinal rule of network access: **The Explicit permission is the most restrictive permission between the Share permission and the NTFS permission.**

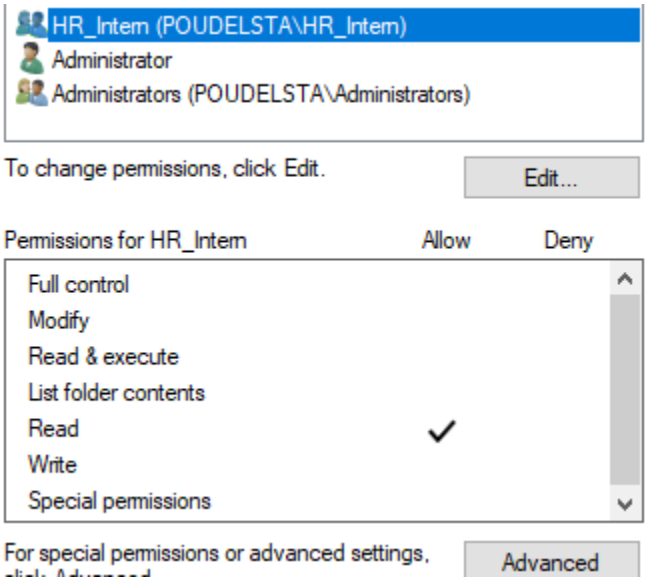
Scenario 1: HR Staff Read/Write Access

1. **Create Folder:** On the server, we will create an **HR** folder on the Local Disk (C:).

2. **Shared Permission:**
    - Go to **Properties > Sharing tab > Share...**.
    - We will find the **HR_Staff** group (we created this in AD) and set their permission to **Read/Write**. Click **Share**, then **Done**.
    - Next, go to **Advanced Sharing > Permissions**. We will give **HR_Staff Full Control**. We will change **Everyone** to **Read**.



3. **NTFS Permission (Security Tab within the HR properties):**
    - We will click **Edit**, then **Add**, and search for and select **HR_Staff**.
    - We will ensure **HR_Staff** has **Read** and **Write** permissions, and we will check the desired boxes (e.g., **Modify** and **Read & Execute**).



Scenario 2: Finance Team Exclusive Access

1. **Folder Creation:** We will create a **Finance** folder on the server.

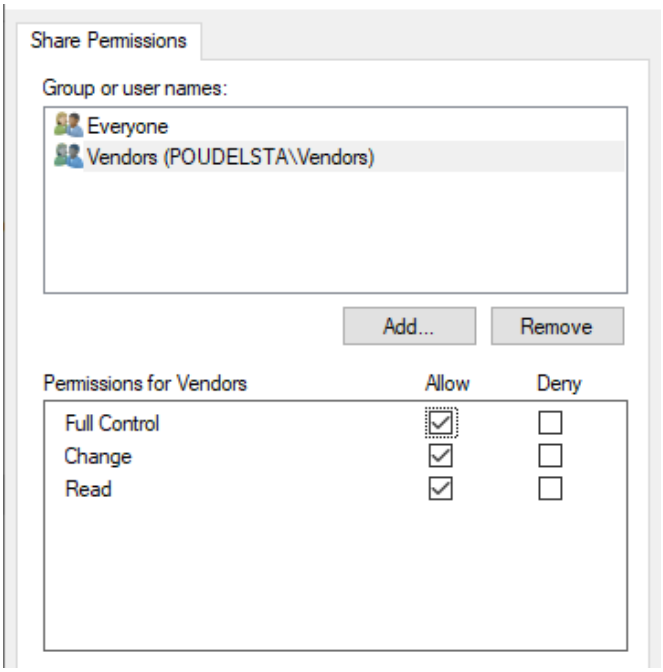
2. **Shared Permission (Exclusion):**
    - Go to **Properties > Sharing tab > Advanced Sharing > Permissions**.
    - We will **uncheck Read** for the **Everyone** group to block general access.
    - We will click **Add**, find **Finance_Staff**, and give them **Full Control**.

3. **NTFS Permission (Exclusion):**
    - Go to the **Security** tab. We will click **Edit > Add**, and select **Finance_Staff**.
    - We will give **Finance_Staff Full Control**. This ensures that only members of this group can access the folder.

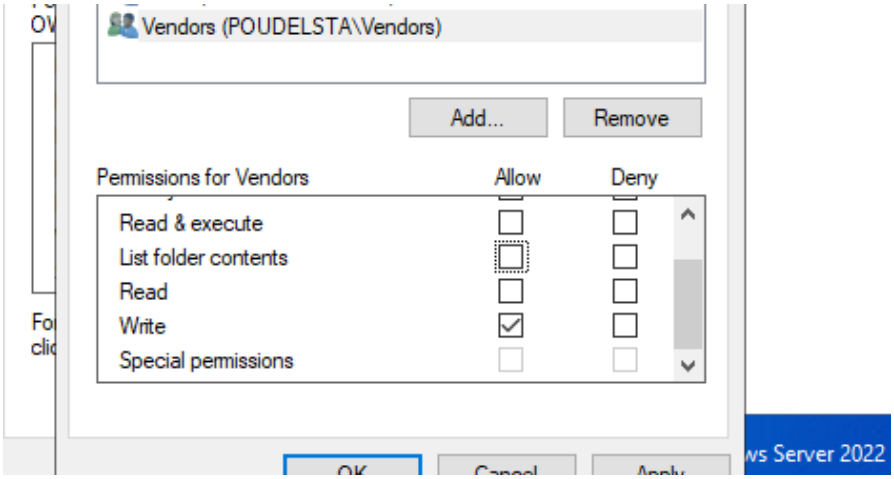
Scenario 3: Vendor Upload Folder (Write-Only)

1. **Folder Creation:** We will create a **VendorFiles** folder.

2. **Shared Permission (Full Access):**
    - Go to **Properties > Sharing tab > Advanced Sharing > Permissions**.
    - We will click **Add**, find the **Vendors** group, and give them **Full Control**. (This is done so the NTFS permission can be the restrictive factor.)



3. **NTFS Permission (Restrictive):**
    - Go to the **Security** tab. Click **Edit > Add**, and select the **Vendors** group.
    - We will **allow only the Write** permission, removing all other permissions (like Read, List folder contents, etc.). This ensures vendors can upload (Write) but cannot see or modify existing files (Read/Modify).

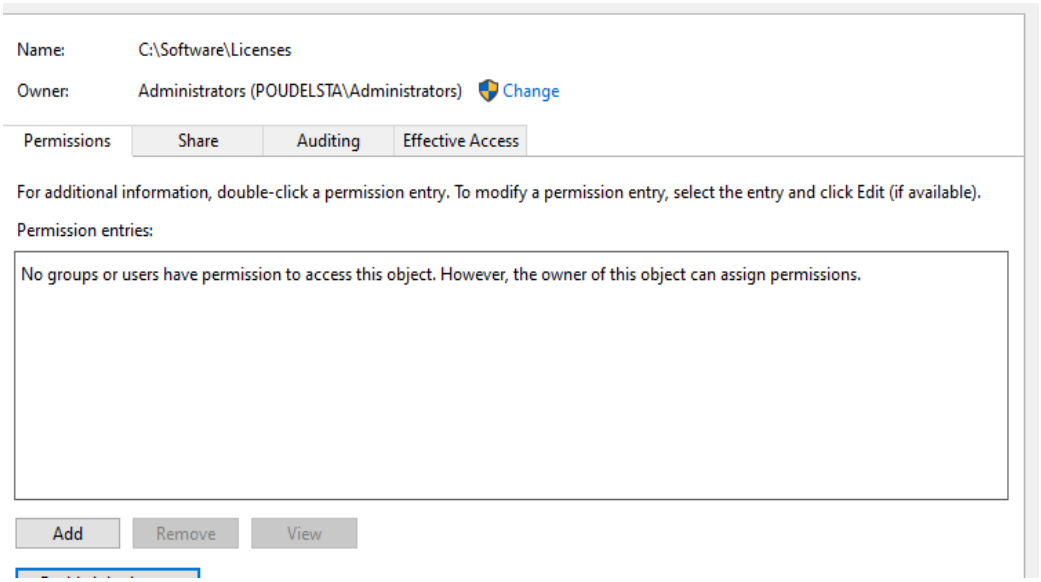


Scenario 4: Senior IT Staff Exclusive Subfolder Access

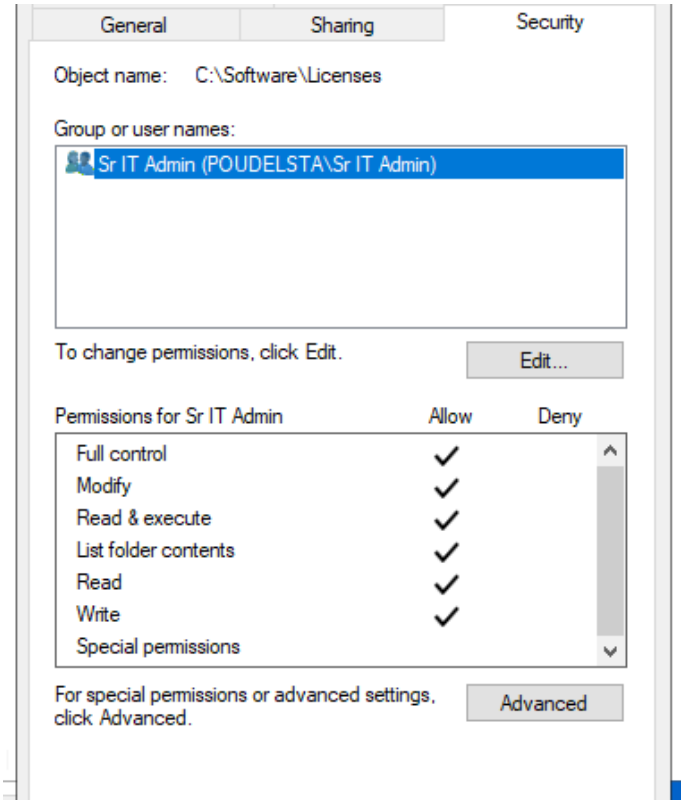
1. **Folder Creation:** We will create a parent folder named **Software Repository** and a subfolder named **Licenses** inside it.

2. **Shared Permission (Parent Folder):**
    - On the **Software Repository** folder, we will go to **Advanced Sharing > Permissions**. We will add the **IT Team** group and grant them **Full Control**.

3. **NTFS Permission (Subfolder Inheritance Removal):**
    - **Note:** For the subfolder, we only need to change the NTFS permissions, as it will inherit the Share permission from the parent.
    - **Right-click** the **Licenses** subfolder and go to **Properties > Security tab**.
    - Click **Advanced**, and then click **Disable inheritance**.
    - When prompted, we will choose **"Remove all inherited permissions from this object."** (This locks out everyone, including the IT Team.)



    - We will click **Edit**, **Add**, and select the **Sr IT Admin** group. We will grant them **Full Control** over this subfolder, ensuring only they have access.


General
Sharing
Security
Object name: C:\Software\Licenses
Group or user names:
Sr IT Admin (POUDELSTA\Sr IT Admin)
To change permissions, click Edit.
Edit...
Permissions for Sr IT Admin
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
Special permissions
For special permissions or advanced settings, click Advanced.
Advanced