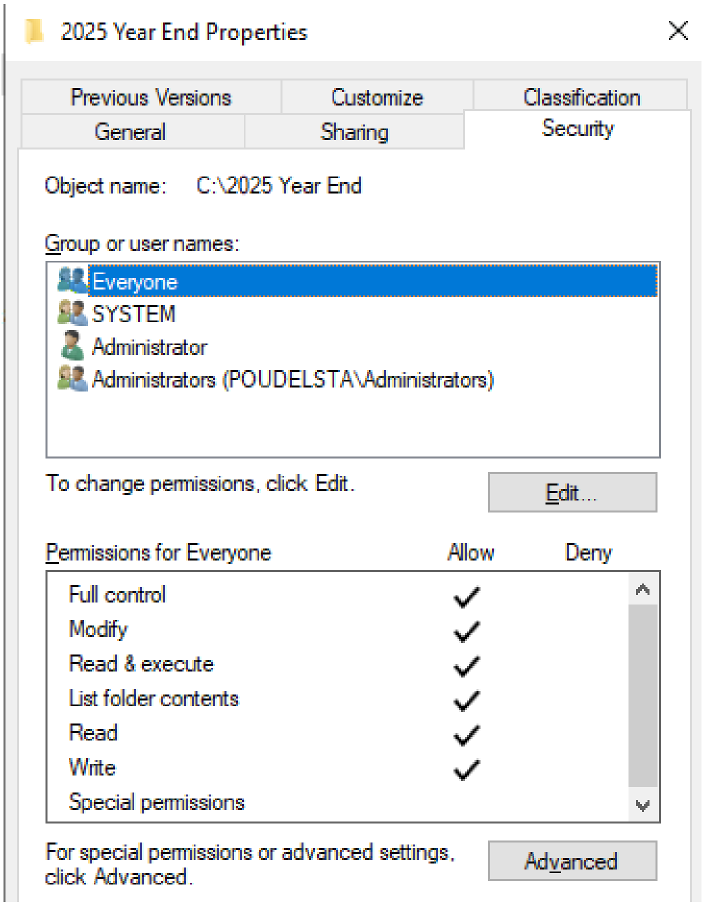
Advanced Permissions: Inheritance and Explicit Deny

Part 1: Effective Permissions and Inheritance Control

This scenario demonstrates how to override inheritance and explicitly apply permissions, ensuring only authorized groups have access to sensitive files.

1. **Preparation (Group and Folders):**
   - In **AD Users and Computers**, we will create a security group named **Year End Audit** (Group type: Security, Scope: Global).
   - We will open **File Explorer** and create the following folder structure on the Local Disk (C:):
     - **2025 Year-End** (Parent Folder)
     - **Audit Report** (Subfolder 1 - Sensitive)
     - **Year-End Review** (Subfolder 2 - General)

2. **Set Up Full Control on Parent Folder:**
   - **Right-click** on the **2025 Year-End** folder and go to **Properties**.
   - **Sharing Tab:** Click **Share**, add the **Everyone** group, and ensure they have **Read/Write** access. Click **Share**, then **Done**.
   - **Security (NTFS) Tab:** Click **Edit**, and ensure the **Everyone** group is listed and has **Full Control**. Click **Apply** and **OK**.
   - **Result:** Both subfolders (**Audit Report** and **Year End Review**) now inherit **Full Control** permission for **Everyone**.



Object name: C:\2025 Year End

Group or user names:

- Everyone
- SYSTEM
- Administrator
- Administrators (POUDELSTA\Administrators)

To change permissions, click Edit.

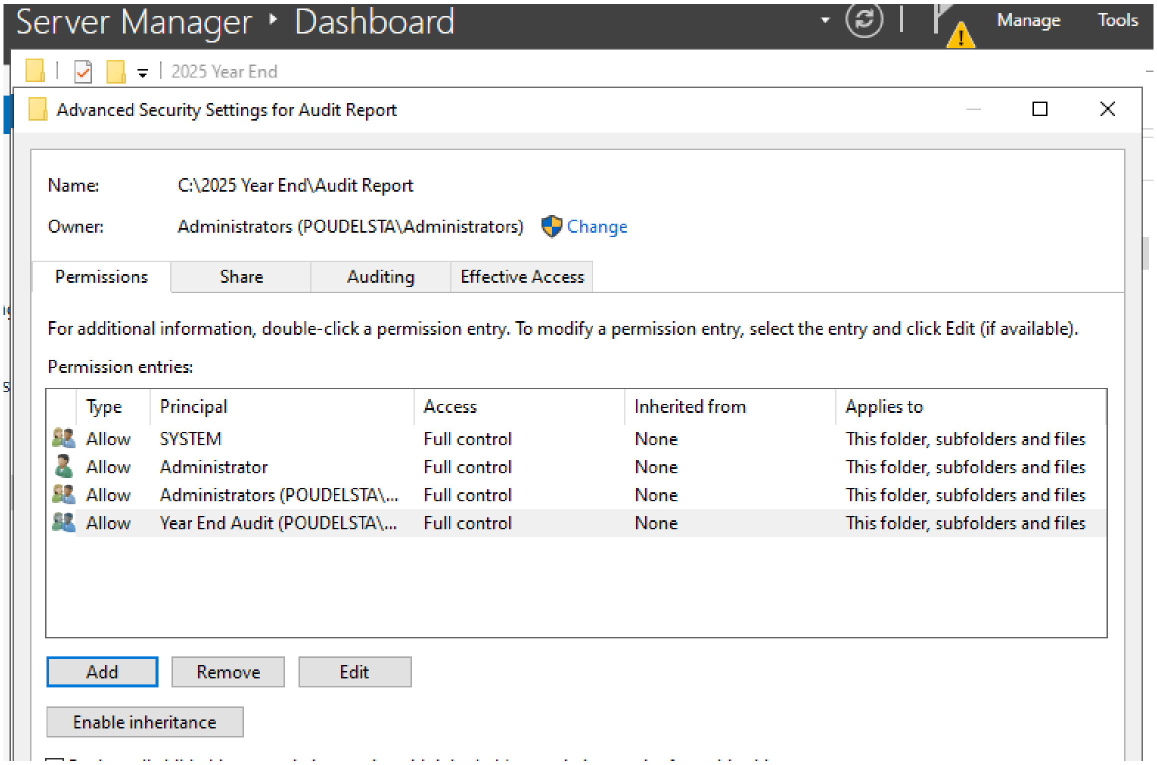
Permissions for Everyone	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

3. **Disable Inheritance on Sensitive Folder (Audit Report):**
   - Our goal is to restrict the **Audit Report** subfolder so only the **Year-End Audit** group has access.
   - **Right-click** the **Audit Report** subfolder and go to **Properties > Security tab > Advanced**.
   - Click **Disable inheritance**.
   - In the pop-up window, select the first option: **"Convert inherited permissions into explicit permissions on this object."**

4. **Apply Explicit Permissions:**
   - In the **Advanced Security Settings** window:
     - Select the **Everyone** entry and click **Remove**.
     - Click **Add**, click **Select a principal**, and input the **Year End Audit** group.
     - Under "Basic permissions," check the **Full control** box. Click **OK**.

- **Verification:** The permission list now shows only **Year End Audit**, **Administrator**, and **SYSTEM** with explicit permissions. Click **Apply** and **OK**.



Advanced Security Settings for Audit Report

Name: C:\2025 Year End\Audit Report

Owner: Administrators (POUDELSTA\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

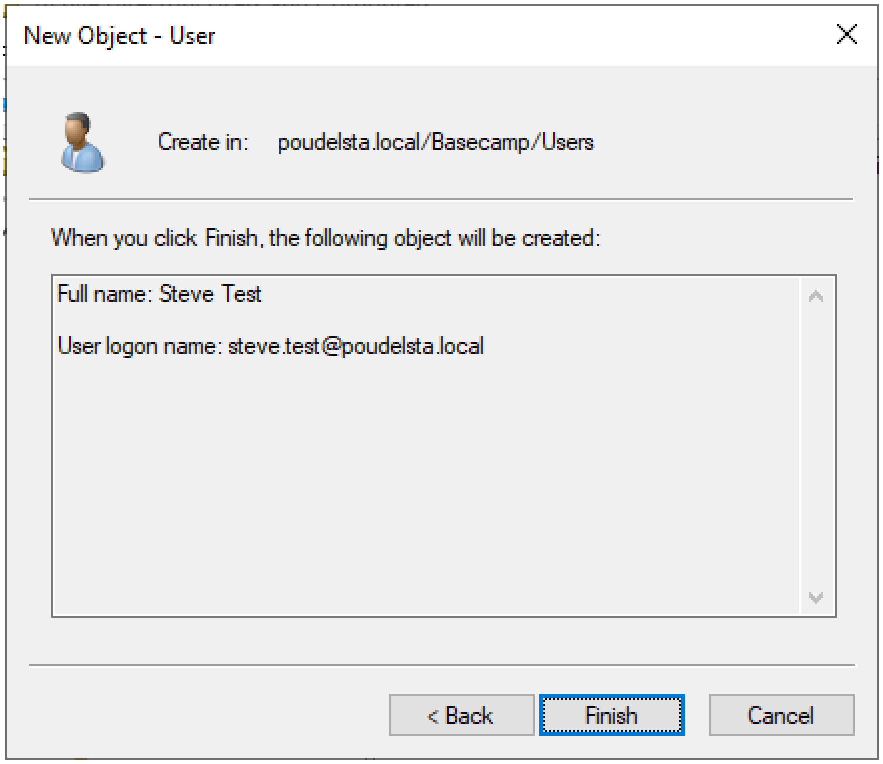
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrator	Full control	None	This folder, subfolders and files
Allow	Administrators (POUDELSTA\...	Full control	None	This folder, subfolders and files
Allow	Year End Audit (POUDELSTA\...	Full control	None	This folder, subfolders and files

Part 2: Implementing Explicit Deny in NTFS Permissions

This scenario demonstrates the rule that **Explicit Deny** overrides any other permission, including **Full Control Allow**.

1. **Preparation (User and Folders):**
   - In **AD Users and Computers**, we will create a test user named **Steve Test** and ensure they are a member of the **IT Admin** group (a group that has **Allow** permissions).



New Object - User

Create in: poudelsta.local/Basecamp/Users

When you click Finish, the following object will be created:

Full name: Steve Test

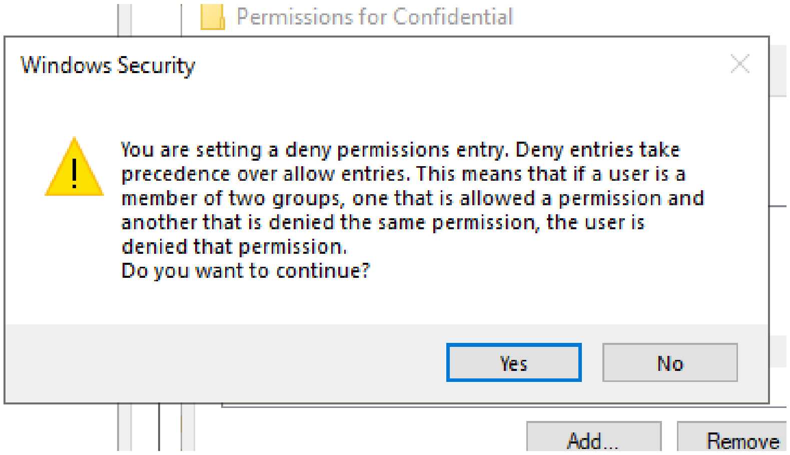
User logon name: steve.test@poudelsta.local

- We will create a new folder called **IT Project** and create two subfolders inside it: **Confidential** and **Material**.

2. **Set Up Read/Write Allowance on Parent Folder:**
   - **Right-click IT Project** and go to **Properties**.
   - **Sharing Tab:** Click **Share**, add the **IT Admin** group, and give them **Read/Write** access.
   - **Security (NTFS) Tab:** Ensure the **IT Admin** group has **Allow** permissions (e.g., Modify, Read & Execute).
   - **Result:** The **Confidential** subfolder inherits these **Allow** permissions for **Steve Test** (via membership in **IT Admin**).

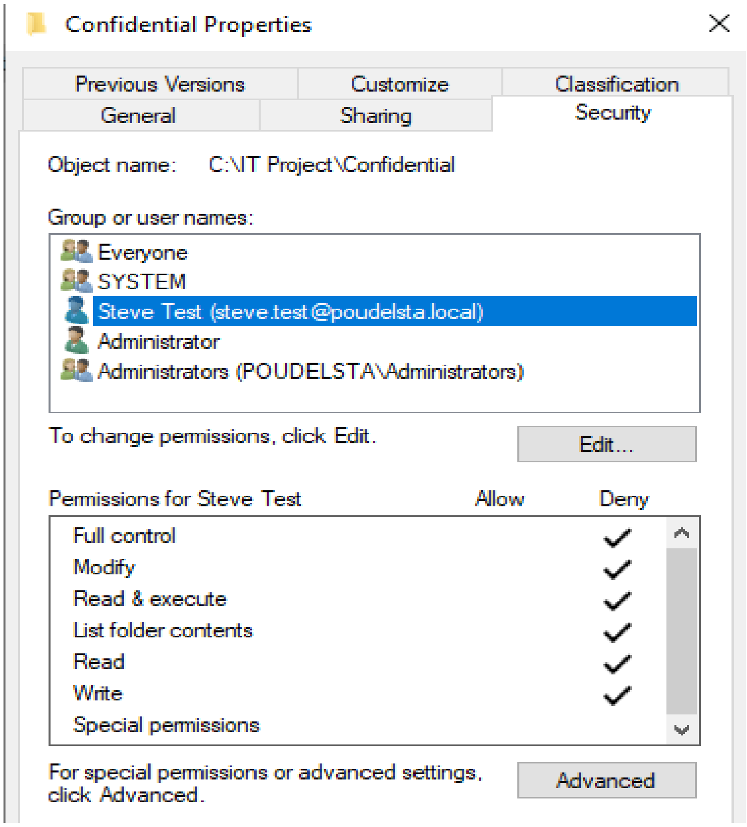
3. **Explicitly Deny Access to Subfolder:**
   - We will **right-click** the **Confidential** subfolder and go to **Properties > Security tab**.
   - Click **Edit**, and then click **Add**.
   - Input the username **Steve Test** and click **OK**.

- On the permission list, select **Steve Test**. In the "Deny" column, check the box for **Full control**.
- **Warning:** A Windows Security warning will appear, reminding us that **Deny entries take precedence over Allow entries**. Click **Yes**.



You are setting a deny permissions entry. Deny entries take precedence over allow entries. This means that if a user is a member of two groups, one that is allowed a permission and another that is denied the same permission, the user is denied that permission.
Do you want to continue?

- **Verification:** If **Steve Test** attempts to access the **IT Project** folder, they will be granted access. If they try to open the **Confidential** subfolder, they will be explicitly denied, even though their group membership grants them full access.



Object name: C:\IT Project\Confidential

Group or user names:
Everyone
SYSTEM
Steve Test (steve.test@poudelsta.local)
Administrator
Administrators (POUDELSTA\Administrators)

To change permissions, click Edit.

Permissions for Steve Test	Allow	Deny
Full control		✓
Modify		✓
Read & execute		✓
List folder contents		✓
Read		✓
Write		✓
Special permissions		

For special permissions or advanced settings, click Advanced.