

Protecting Important Folders From Accidental Move or Erasing

The Problem

It's happened to all of us but it happens more frequently at work where there are a lot of other people sharing folders and files. An important deadline has arrived and you've put in exhausting hours on a grant or proposal that could bring in much needed revenue for your department or project. You go to open the file to print or submit and it's gone. In fact, the entire folder in which you and your team has been in and out of during the weeks has disappeared.

You call your technology staff and they spend two hours searching. Once, you remember, they finally found a lost folder tucked away under some obscure unrelated folder. After a long time looking your techs report that your file must have been erased and they'll have to try server tape backups to perhaps retrieve your file. But will that backup file include all the changes you put in yesterday? Will they be able to extract the file from one of the backups in time for you to send your proposal by 11 a.m.?

Where do these files go? Who erases them? Who moves entire folders containing very important files around and aimlessly drops them into other folders? Who does this to us? 🤪

The answer is, (*are you sitting down?*), **you or your colleagues**, unless you have a mean-spirited psychopath on your staff who is hell-bent-to-leather to ruin your life, cause your nervous breakdown and deprive your company from getting that one grant that was needed to make payroll. 🐱

It's not that space invaders are invisibly hovering above our company, channeling our minds to erase these files or move the folders they're in. Files getting deleted and entire folders getting moved or deleted happens out of (1) carelessness with dragging and dropping files and folders with one's mouse, or (2) hitting delete when a file or folder is highlighted but while you are not focused enough to know it is selected – maybe because you have scrolled down and what is highlighted is no longer able to be seen on your screen. These sloppy or computer-novice actions happen when you are overtired, non-focused and are not fully present in the work that is before you.

“*That's the way I am all the time*” you quietly mutter under your breath. 🤪

Well there are approximately 100,000 deaths in hospitals each year because of mistakes, but technology is being put in place to turn that around, these days, with electronic medical records and e-prescribing which doesn't permit conflicting drugs or wrong dosages go through the order system. We now can do the same thing with computer files and folders that are deemed important.

The Remedy

Thanks to Steve Lahnen, we have a new methodology to protect important folders and the files within them from being erased or moved. In fact, a user can't delete a file or move it or its folders elsewhere, even if they intentionally tried. This goes even for files that they created, opened, edited or saved themselves in the folder with these controls on it.

Here is how it is done, and this is just a quick summary of the detailed instructions and screen shots that follow for your network administrator.

1. First, you **sit down with your management team** and determine if a department or workgroup needs a special protected folder for extremely important work. This work or project files are definitely NOT every day work – memos to colleagues, letters and to-do lists. The reason you don't want every day work in one of these especially controlled folders is because once you create a file in this special "Vault" folder, you can't erase it. It stays there until an administrator erases it. That's why the management team has to decide what file or files is a "do-not-erase-under-any-circumstances" kind of file.

Consider, for this special "Vault" folder, work for grants, proposals, special data that gets worked on by a number of people. Very definitely you would want to keep your production database in one of these "Vault" folders. You would name a folder with a common naming scheme so that it is clear that this is known as a special secure folder. We name ours with the word "Vault" added. For instance, "Grant Vault" or "Production Database Vault."

2. Next, you **create a group (or groups) in your server's active directory to which you will later assign restrictions for certain folders**. People in one of these groups can access anywhere else in the company's data files they normally do but if they have permission to go into one of these "Vault" folders for the purpose of that folder, the restrictions placed on them (from being in one of these particular groups) prohibits them from deleting files, folders or moving the files or folders from where they are. They **can** open, view, edit and save but they **can't** delete or move things by accident or otherwise.

Administrator Folder Permissions Instructions

1. Creating Your Groups

Create your list of groups in *Active Directory* that have something to do with the users or tasks into which you'd put users as members. Let's say you have 3 company sites named by the street they are on. Let's say you have a company site named **Genesee, Riley and Delaware**. Those could be the names of 3 groups needing need to access a database for their site's work. Let's also say that you have other users who help write grants. That group could be called **Grants**. So you start with this list of named security groups on your server:

Examples of Groups You Could Create on the Server for Department or Tasks:

1. Genesee
2. Riley
3. Delaware
4. Grants
5. Experiment Group (create this just for practicing the setup of this kind of protected vault folder)

2. Create a pretend user for this experiment

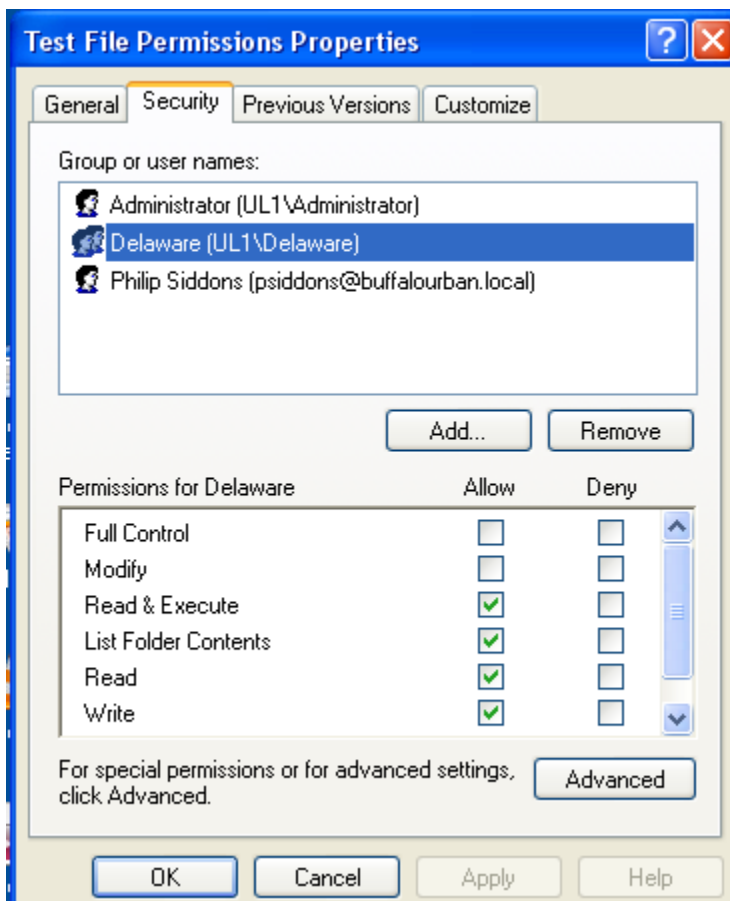
You could create a user named "Fake User" with a password that is easy for you to remember during this experiment.

3. **Create an Experimental Folder To Practice Assigning Permissions** such as:

F:\Test Vault

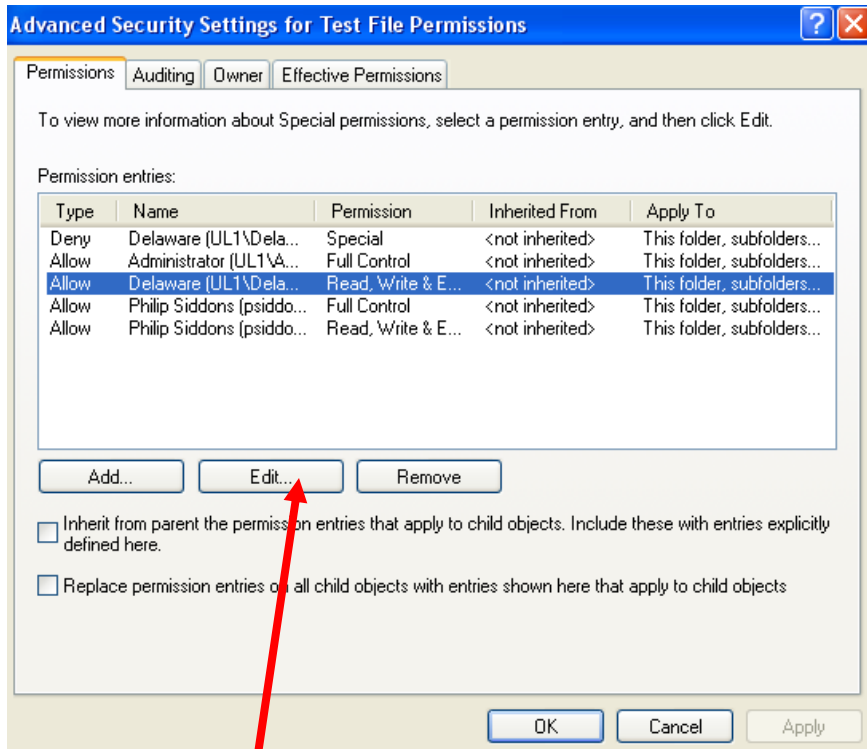
4. **Assign the permissions** to this Experimental **Test Vault** folder in order to practice assigning permissions. Follow the screen shots below for guidance.

In this folder, assign permissions to a group as follows (this case, the experimental group is the **Delaware** Group). It is highlighted in the screen below because it was added using the **Add** button and it appears in the Group or user names list along with (in this example) Administrator and Philip Siddons. Be sure the group for which you want to set permissions is highlighted (as is the **Delaware** group below):



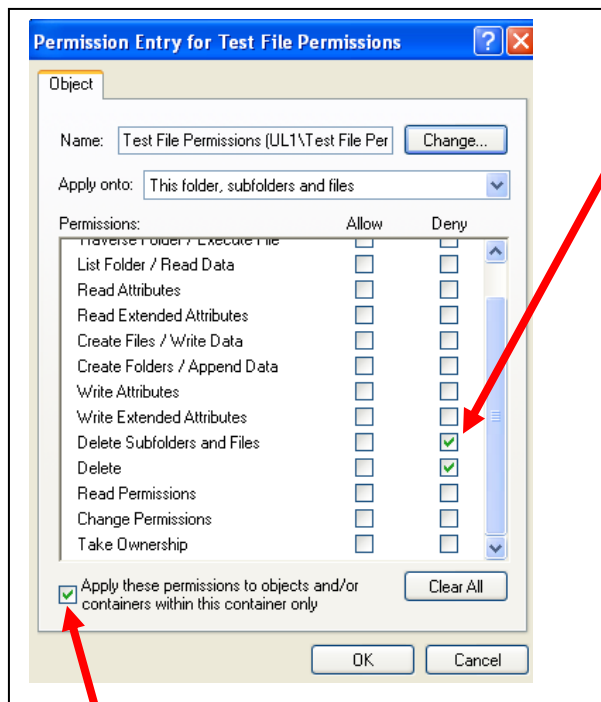
After assigning the above four permissions (in the “Allow” column), click on the **Advanced** button.

Here, select the name of the group name on which that you are editing permissions. (Again, in this example, the **Delaware** group is highlighted.)



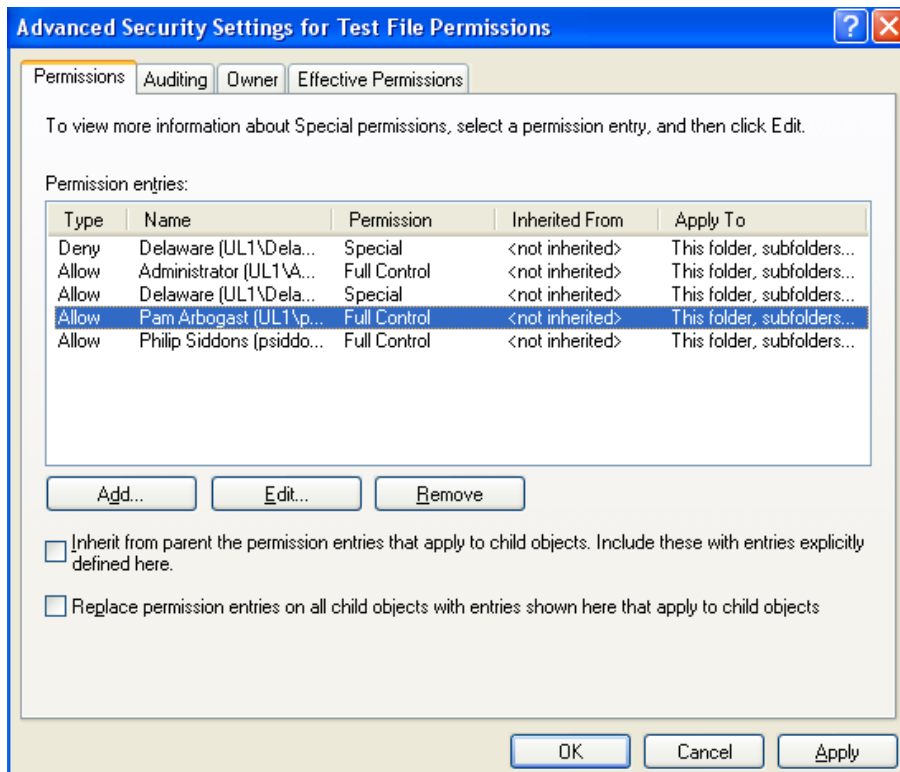
Now choose the **Edit** button

Make sure these two items are checked in the **Deny** column (**Delete Subfolders and Files** and **Delete**):

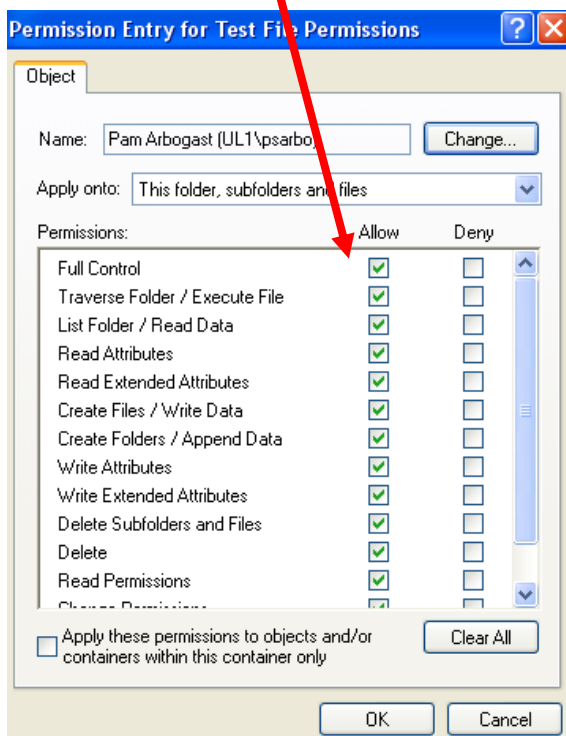


Check the check box in the bottom left next to “Apply these permissions to objects and/or containers within this container only.” Click the **OK** button, . . .

Make sure an administrator has full access to the folder. In this case, notice that Pam Arbogast has full access:



In this case, Pam Arbogast is an administrator so after she is added as a user in this permissions list, click the **Edit** button and give her full control of the folder.



Now, any file created or even saved by someone in the **Delaware** group can't be erased by that Delaware group user or anyone else in that Delaware group. The files can't even be renamed. It can only be deleted by someone with the Full Control permissions in that folder, such as an Administrator.

Press the OK button.