

NTFS Tutorial



Day 2:

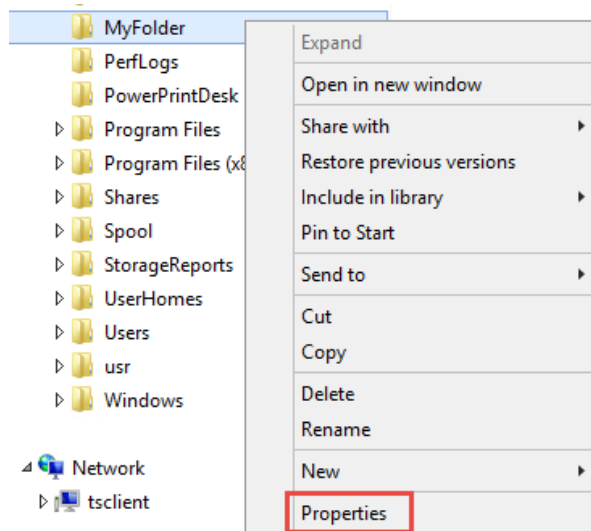
Working with Permissions

Carsten Schaefer

In previous chapters, we covered how to visualize an ACL (the current permissions of a filer or folder). Now you are going to learn how to manage these permissions. Throughout this section, we will continue to use MyFolder as our example folder.

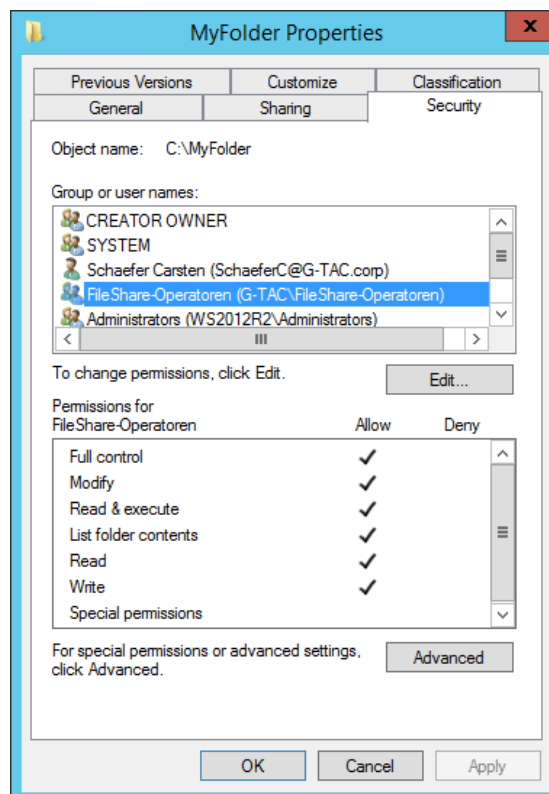
How to Assign or Remove Permissions

First, locate the folder or file you want to grant permissions to. Right click that folder. Then click on “Properties”.



MyFolder Properties

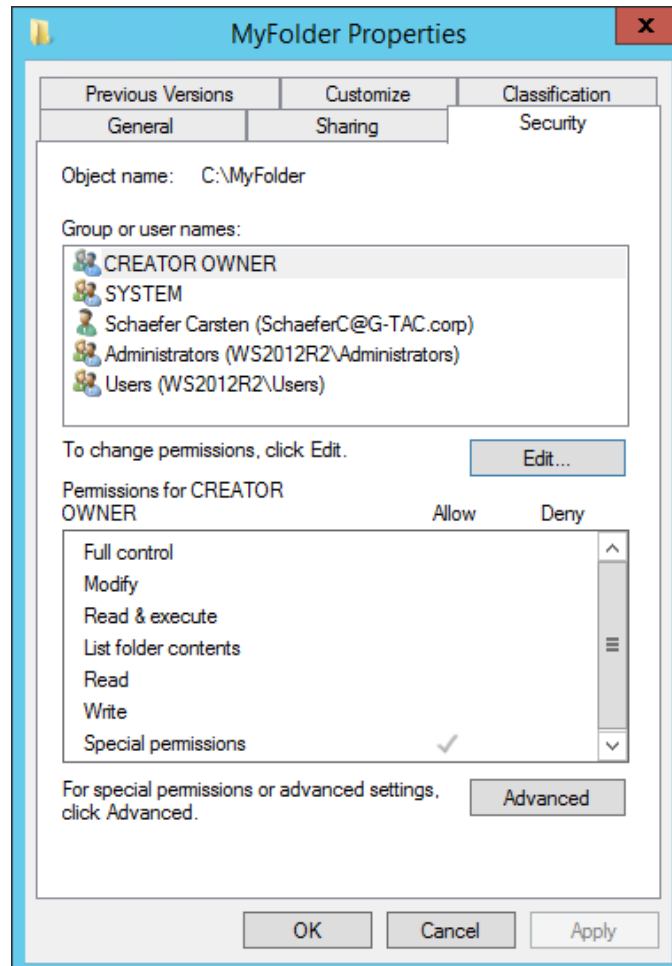
Click on the security tab to view the ACL for the folder. Under “Groups or user names” click the “Edit” button.



MyFolder ACL properties page

To remove a user, simply click on that user and press the “Remove” button followed by the “OK” button.

To add a user, click the “Add” button:

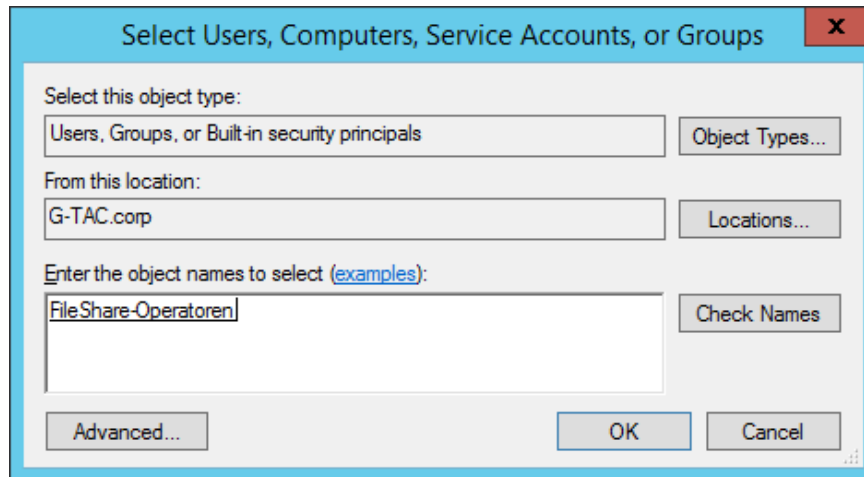


MyFolder permissions properties page

Now you can select the User/Groups you wish to grant access to MyFolder. The options within the “Select Users or Groups” form are as follows:

- Object Types: Allows you to filter what type of object you want to assign, in order to narrow your search.
- Locations: If you are on a Windows Network, you can choose between the local computer or Active Directory to search for network users in your organization.

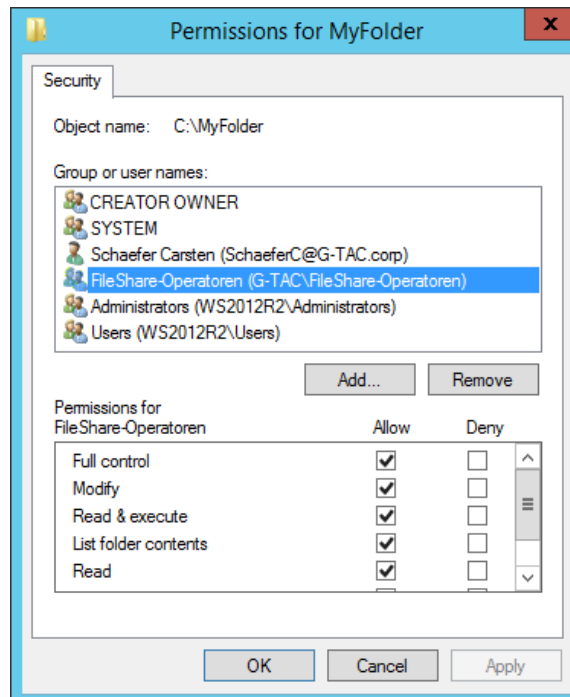
For our example, we are going to type “FileShare-Operatoren” in the “Enter the object names to select” textbox and then click the “Check Names” button, followed by the “OK” button.



Select Users or Groups prompt

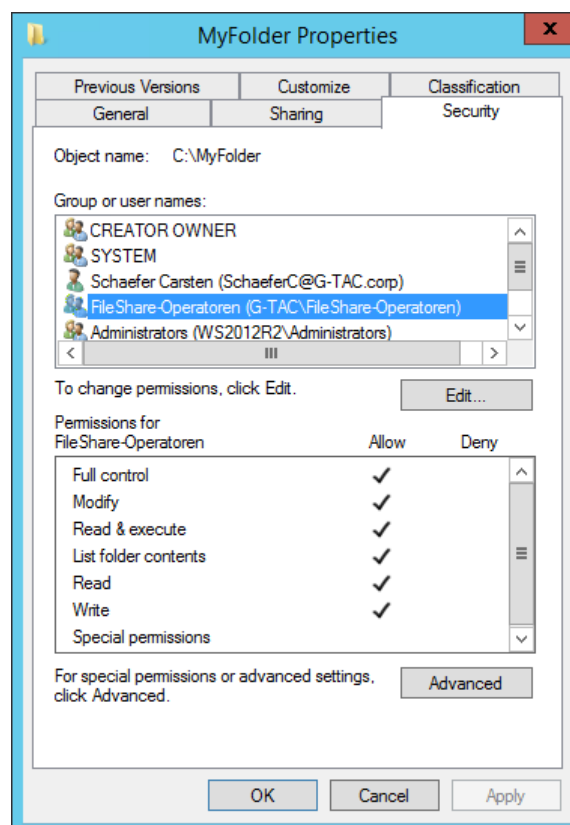
“FileShare-Operatoren” now appears on the “Permissions for MyFolder” page. Here you can choose which permissions to grant the user. Once you assign these permissions, click the “OK” button. For this exercise, we assigned the “Full Control” permission to the user from the “FileShare-Operatoren” group. You can also deny permissions using the “Deny” column.

As a reminder, we do not recommend denying permissions to users. Instead, it is best to control user access through the groups which they belong to.



Assigning permissions to the FileShare-Operatoren group

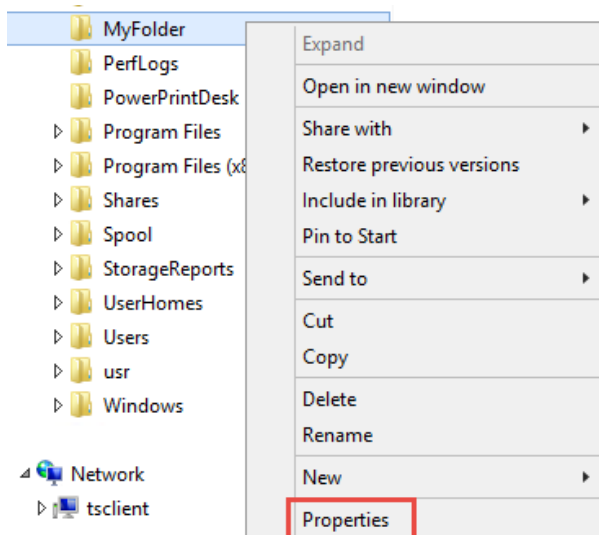
Group now has “Full Control” permissions within the ACL.



MyFolder ACL after assigning permissions to FileShare-Operatoren

How to Assign Special Permissions

First, locate the folder or file you want to grant permissions to. Right click that folder. Then click on “Properties”.

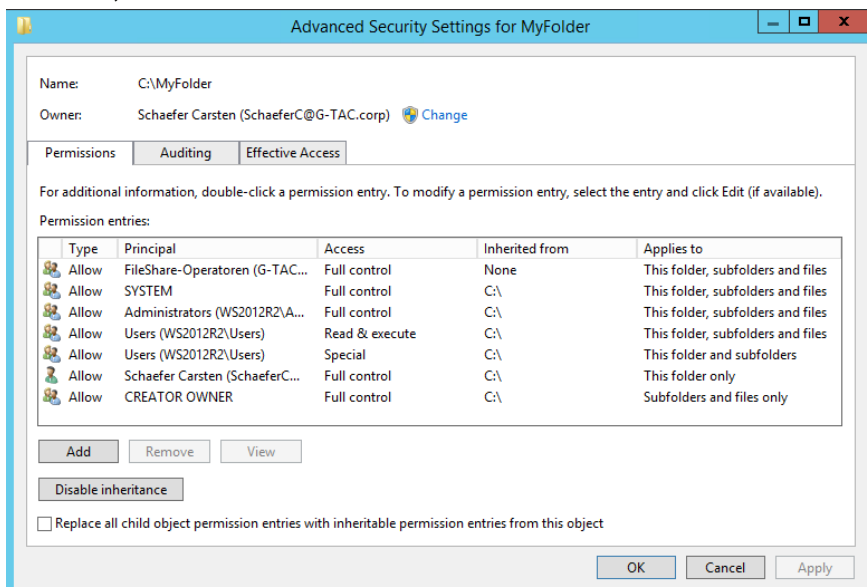


MyFolder properties

Click on the security tab to view the ACL for the folder. Then click on “Advanced”.

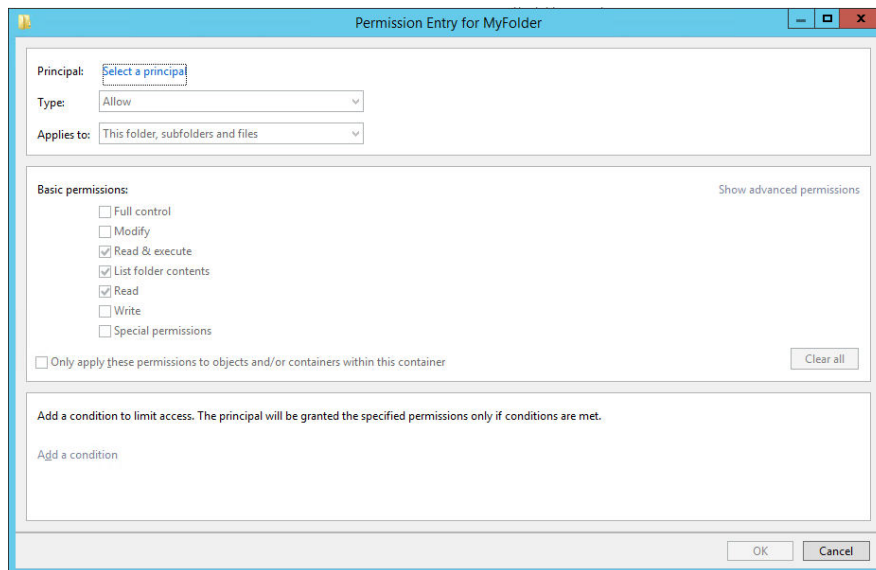
This is the “Advanced Security Settings” tab, which changed in Windows Server 2012 to provide an interface that is easier to understand and manage.

In the permissions tab, click on the “Add” button.



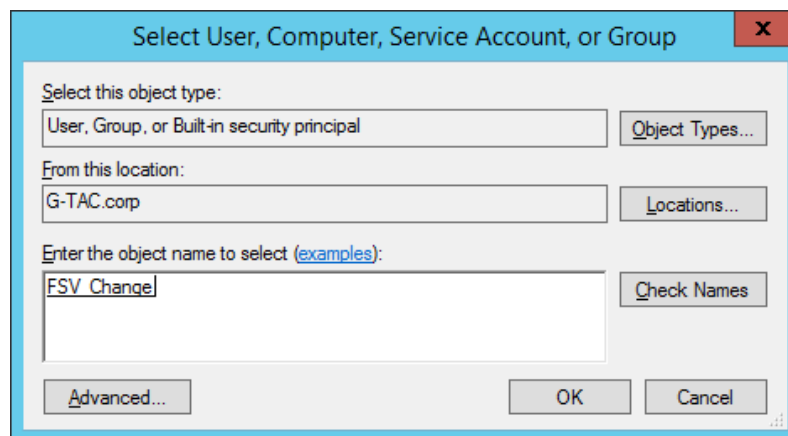
Advanced Security Settings for MyFolder

On the permissions entry page, click on “Select a principal”.



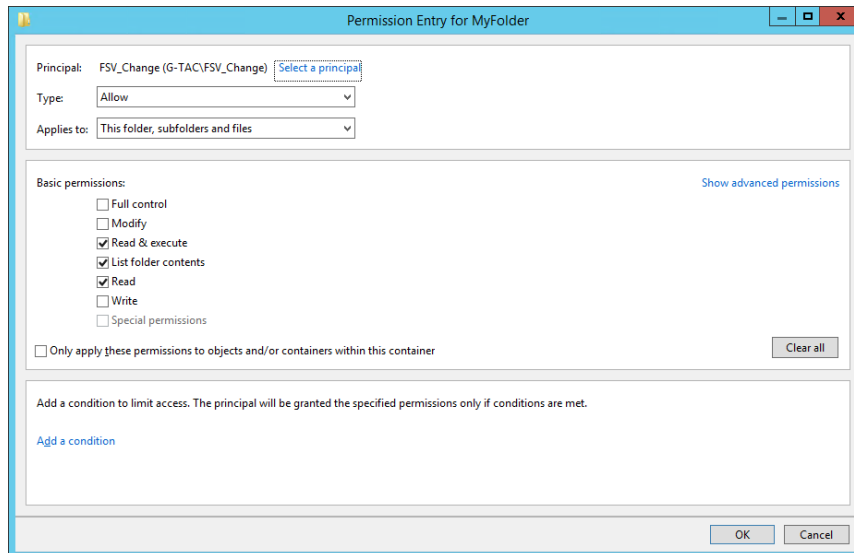
Permission Entry property page for MyFolder

Choose the user or group you want to grant special permissions to. We will use group “FSV_Change” for our example. Then click the “OK” button.



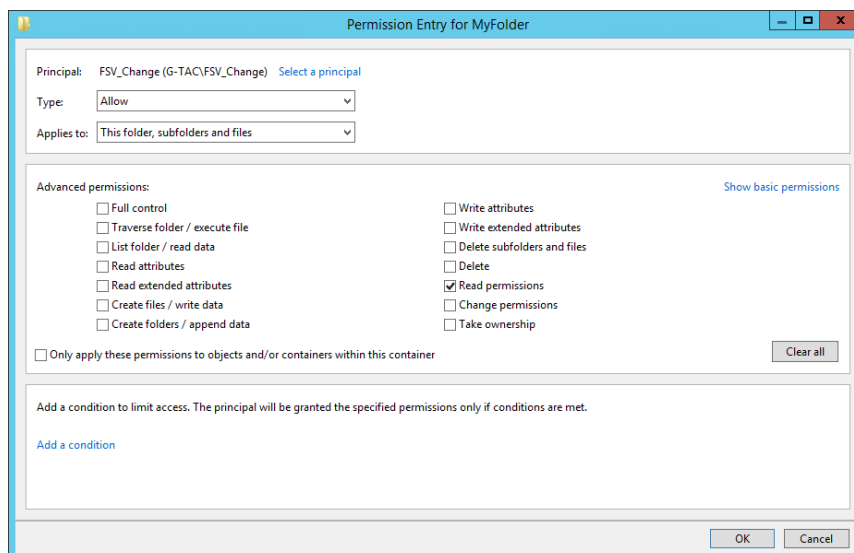
Select User or Group prompt

Once you have selected your user or group, by default, you are presented with the list of basic permissions. To see the list of advanced permissions, click on “Show advanced permissions”.



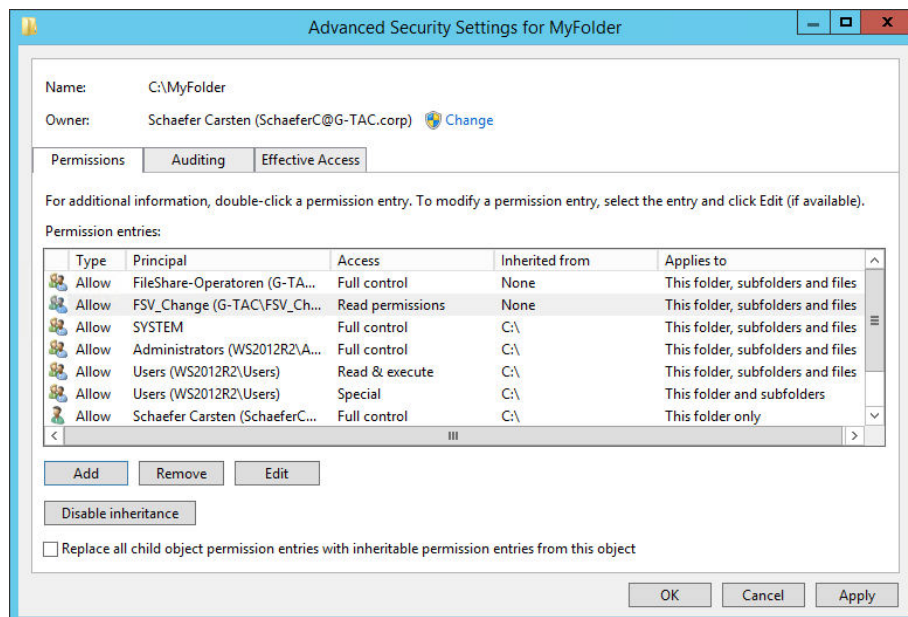
Enabling advanced permissions in the Permission entry for the MyFolder property page

Select the proper advanced permissions for the user and click the “OK” button. For more details about each advanced permission type, please refer to the previous chapter.



Choosing advanced permissions for FSV_Change

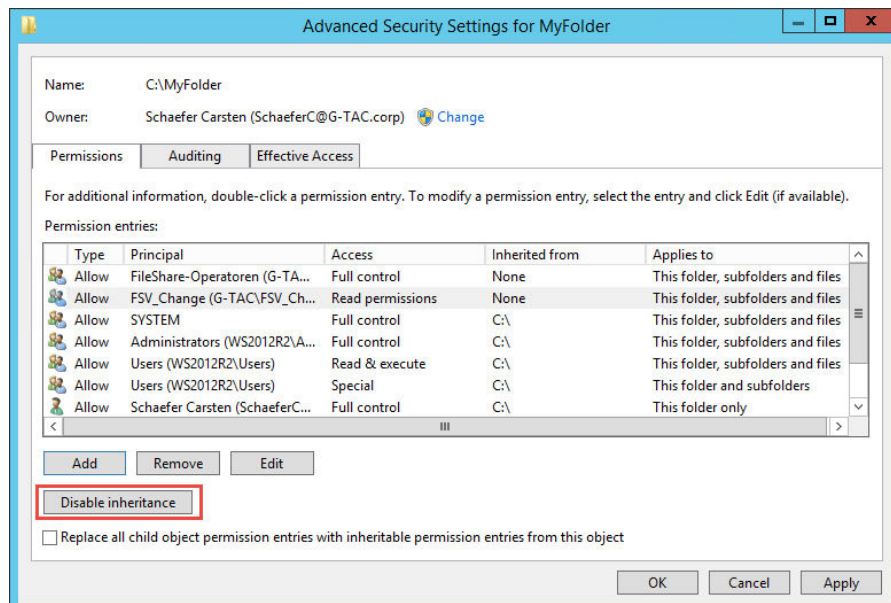
You will now see the advanced permissions assigned on the “Advanced Security Settings” page. Click the “OK” button to complete the process.



View of advanced permissions set for user Schaeferc

How to Disable Inheritance

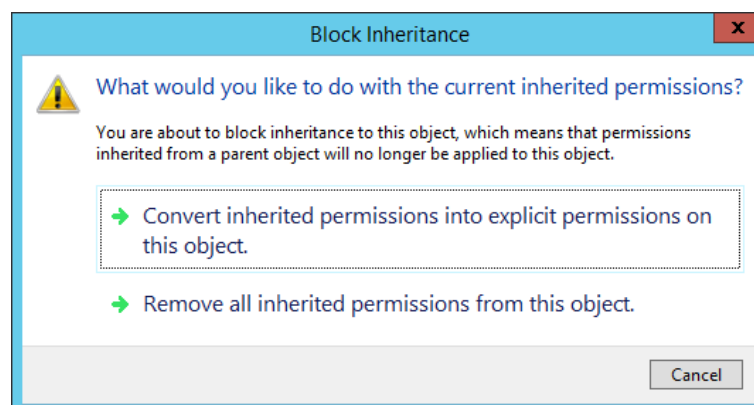
You can disable inheritance for any given file or folder by going to the Security tab within the properties of that file/folder and clicking on “Advanced” followed by “Disable inheritance”.



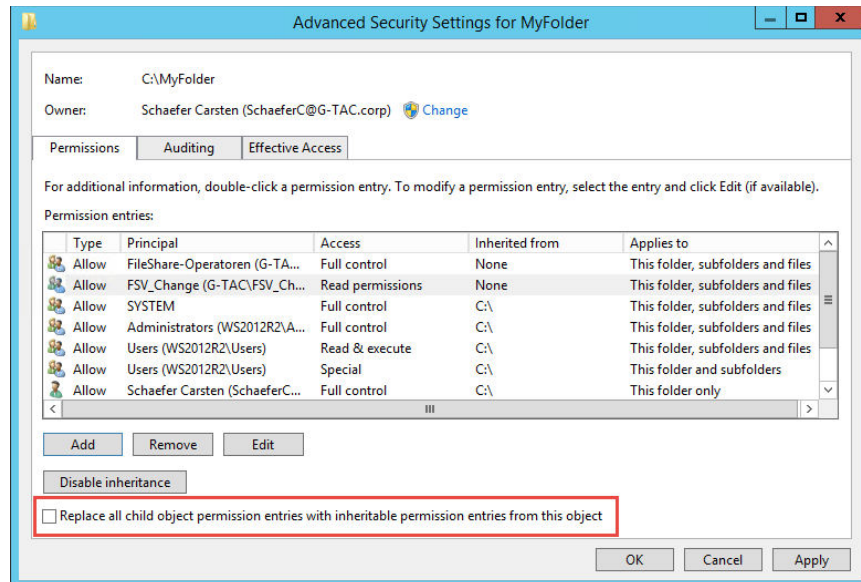
Disabling inheritance and replacing child object permissions in the Advanced Security Settings tab

In next step you have to choose one of the following options. The first option “Convert inherited permissions into explicit permissions on this object” will copy all inherited permissions and set them explicitly on this level. This would be the same as if you set all of these permissions manually.

The second option “Remove all inherited permissions from this object” will remove any permissions. You must be aware that you have to set permissions now by your own. Otherwise no permissions will be set on this folder anyway.



When administrators and users start changing permissions regularly, some files or folders can become inaccessible to users and groups that should have access. For this reason, you can, at any time, go back to the default inherited state by choosing “Replace all child object permission entries with inheritable permission entries from this object” as seen in next image.



How to Override Folder Permissions with File Permissions

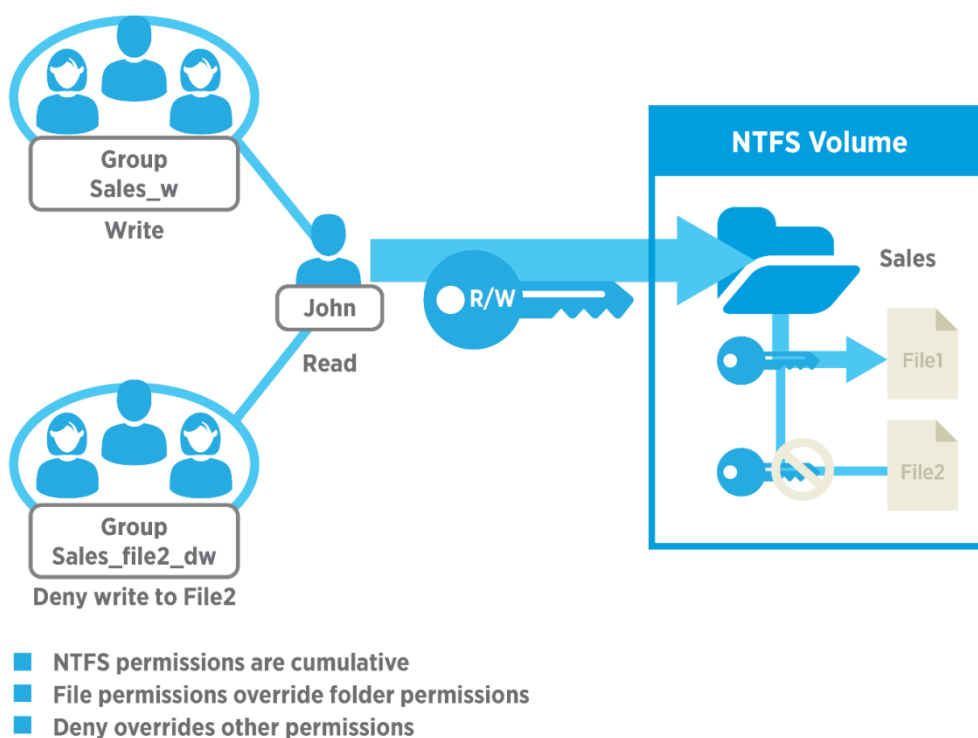
It is possible to override access to a file within a folder that you do not have access to. In our example, let's say that you do not have access to "MyFolder", but there is a specific file within MyFolder called "MyFile" that you need access to. You can receive access to only this specific file if you use the "Bypass Traverse Checking" security setting permission.

Bypass Traverse Checking is a setting that is assigned through Group Policy Settings. Therefore, we won't cover it in detail in this article.

How to Override Folder Permissions with Deny Permission

It is possible to override any permissions with a Deny Permission. In our example, let's say that you do have modify access to "MyFolder" because of your membership in a specific security group, and you are a member of a group that is denying permissions to a specific file in that folder, you will not get access to this file.

Denying permissions overrides any other permissions a user might have. Consider, this is not the recommended method of controlling access to resources.



Example with Deny Permissions

In Figure above, John is member of Group Sales_W and Group Sales_File2_DW. For folder Sales John will inherit Write permissions from Group Sales_W. And John will inherit Deny Write permissions for File2 from Group Sales_File2_DW.

The results are: John can read and write to File1. He can also read File2, but cannot write to this file because he is a member of Group Sales_File2_DW, which grants Deny Write permission to this file.

