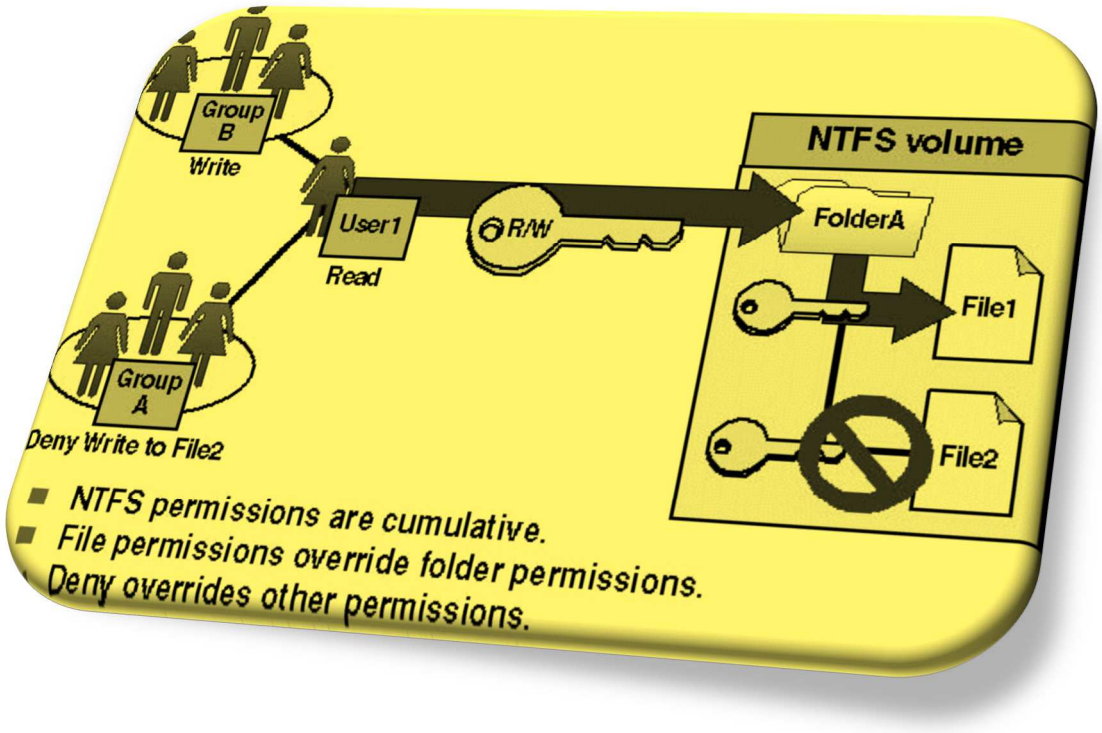
NTFS PERMISSIONS



Ana Cifuentes Romero
DW1E – 22-04-2022

Imagine we have a computer with Windows 10 for two-year courses. The first year can access two types of students: hardware and software (2 users and 1 group for the first year). The second year can access security and servers (2 users and 1 group for the second year).

The users above are standard, but we also have an advanced user called "responsible" with administrator permissions.

We want to create some folders in D:\ according to the following criteria:

- A personal folder for each user, which can only be accessed by the corresponding user. They can do everything. You only need to create the folder for one of the users, since the others are similar.
- A read-only folder for all the students called "shared". The responsible user is able to create or delete files and folders. This folder cannot be accessed by software first-year users.
- A folder only for first year students into the shared folder, where they can create files and folders, but not delete them.
- Do the same as above for second year students (into the shared folder too).

Do the following:

a) Explain the users and groups required for the computer.
b) Explain the folders we need according to the criteria above.
c) Set the NTFS permissions for all the users and groups in each folder created in part B. For the subfolders, consider two scenarios: inheritance and non-inheritance.

You can use a table similar to below.

Folder name

	Allow					Deny				
User/Group	Full Control	Modify	Read & Execute	Read	Write	Full Control	Modify	Read & Execute	Read	Write

a) We must create one user of each type: hardware, software, security and services (for all of them you can use the default type "Users") and the user "responsible" (this is "Administrator" type). We need three groups one for the students, another for the first year (with hardware and software users) and the last one for the second year (with security and servers).

b) We need 4 folders, one for each user. Another two folders: one for first year and one for second year students. The last one we need is the shared folder.

c) NTFS permissions by using a table:

	Allow					Deny				
User/Group	Full Control	Modify	Read & Execute	Read	Write	Full Control	Modify	Read & Execute	Read	Write
hardware	X	X	X	X	X					
software	X	X	X	X	X					
security	X	X	X	X	X					
servers	X	X	X	X	X					

Shared folder (groups first and second)

	Allow					Deny				
User/Group	Full Control	Modify	Read & Execute	Read	Write	Full Control	Modify	Read & Execute	Read	Write
first			X	X						
second			X	X						
software									X	
responsible		X	X	X	X					

Firstyear folder:
With inheritance

	Allow					Deny				
User/Group	Full Control	Modify	Read & Execute	Read	Write	Full Control	Modify	Read & Execute	Read	Write
first (inherited)			X	X						
second (inherited)			X	X						
software (inherited)									X	
responsible (inherited)		X	X	X	X					
first (explicit)			X	X	X					
second (explicit)									X	

Without inheritance. We keep the user "responsible" because is the "Administrator".

	Allow					Deny				
User/Group	Full Control	Modify	Read & Execute	Read	Write	Full Control	Modify	Read & Execute	Read	Write
first			X	X	X					
responsible		X	X	X	X					

Secondyear folder:
With inheritance

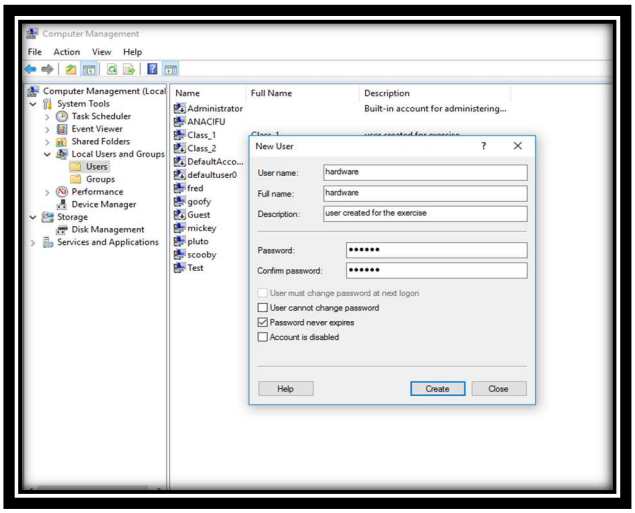
	Allow					Deny				
User/Group	Full Control	Modify	Read & Execute	Read	Write	Full Control	Modify	Read & Execute	Read	Write
first (inherited)			X	X						

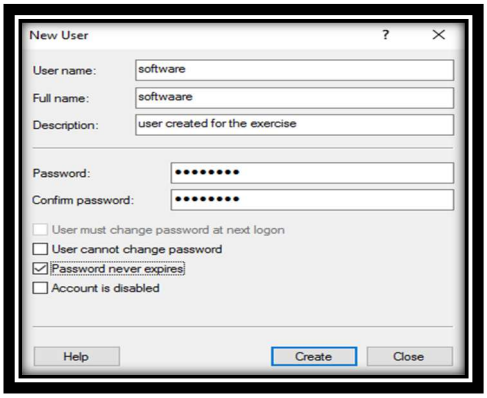
second (inherited)			X	X						
software (inherited)									X	
responsible (inherited)		X	X	X	X					
second (explicit)			X	X	X					
first (explicit)									X	

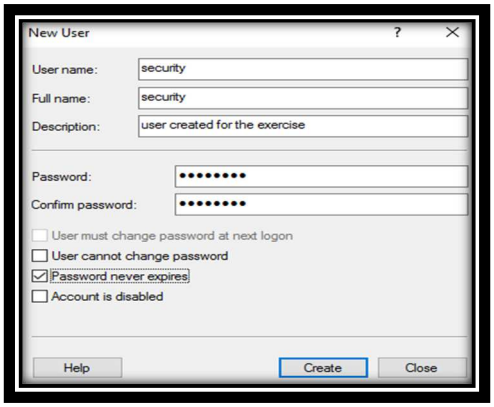
Without inheritance

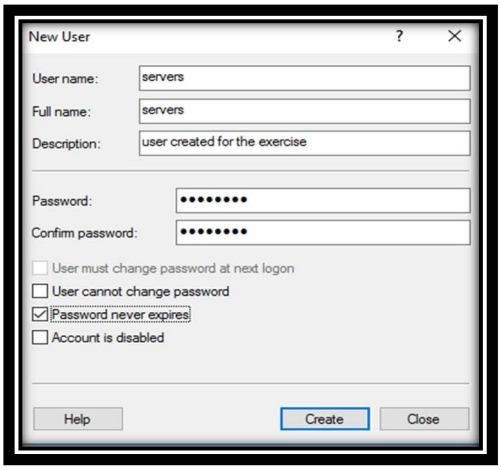
	Allow					Deny				
User/Group	**Full Control**	**Modify**	**Read & Execute**	**Read**	**Write**	**Full Control**	**Modify**	**Read & Execute**	**Read**	**Write**
second			X	X	X					
responsible		X	X	X	X					

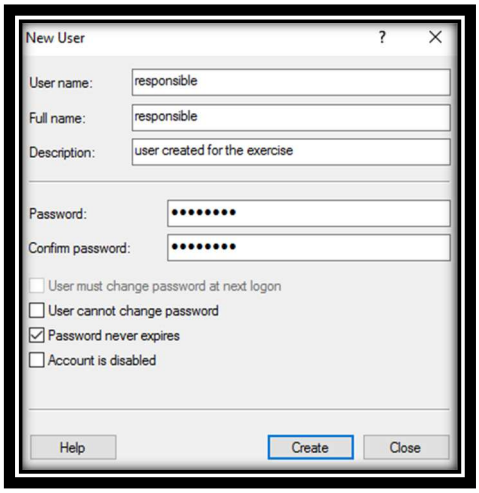
First of all , we create the users and the administrator from **"Computer Management"**.



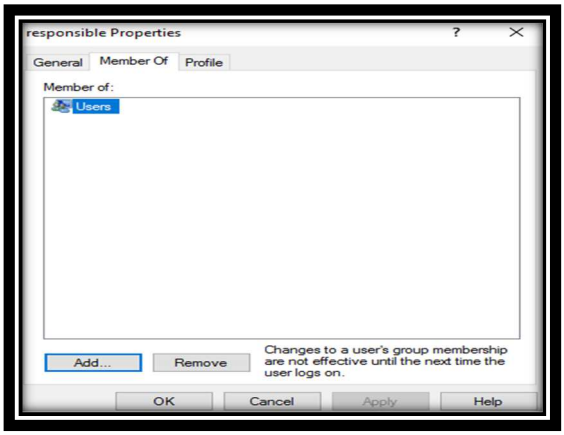


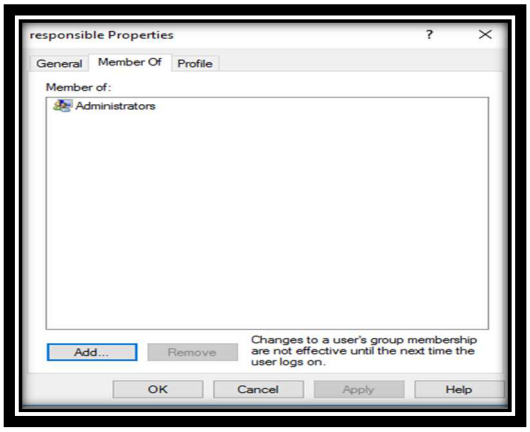




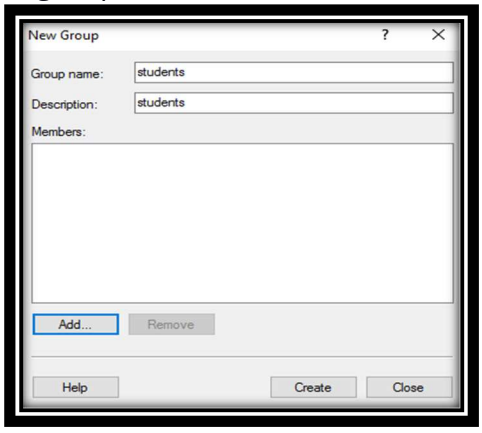


Now, again from **"Computer Management"->responsible->Properties** you have to change the type of member of the "responsible" user to **administrator** type. Remove the "Users" type and add the "Administrator" type.

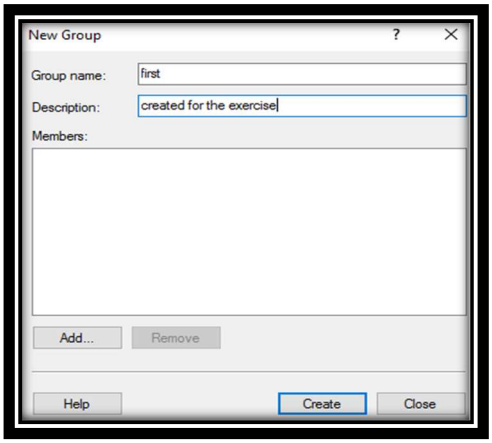


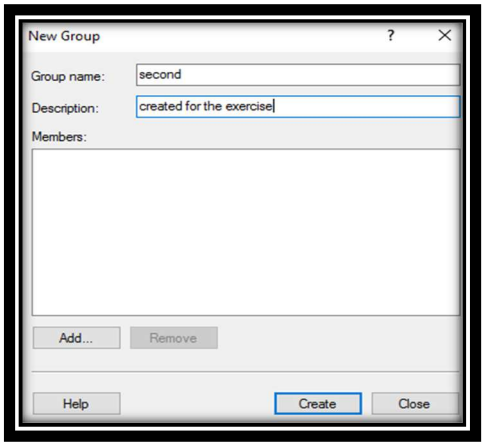


Now, we can create a new group for the students.

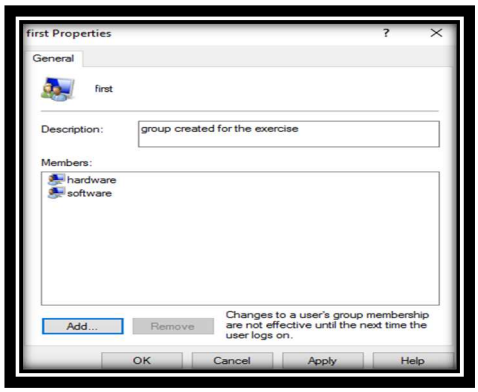


a) Then, we need to create two groups: one for the first year (with hardware and software users) and the second one for the second year (with security and servers).

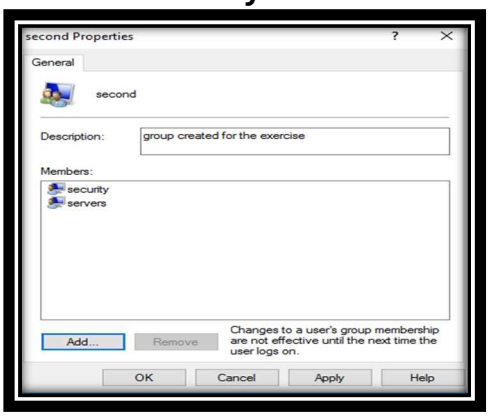




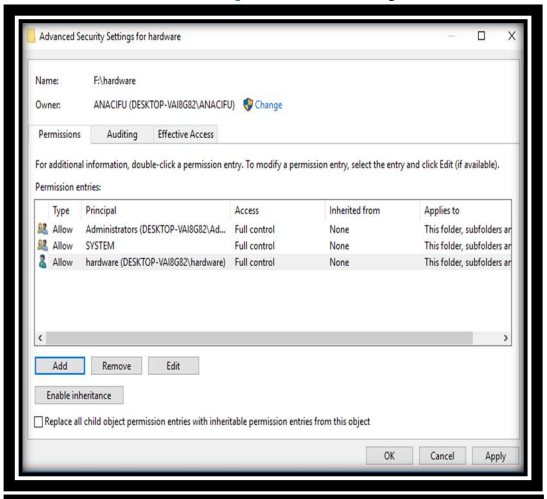
In the **"first"** group we include **hardware** and **software** users.

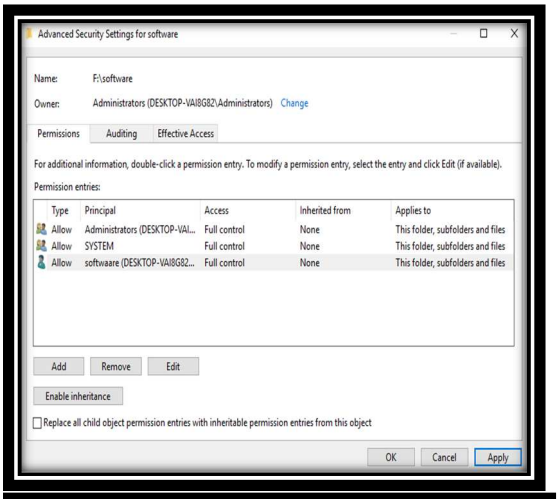


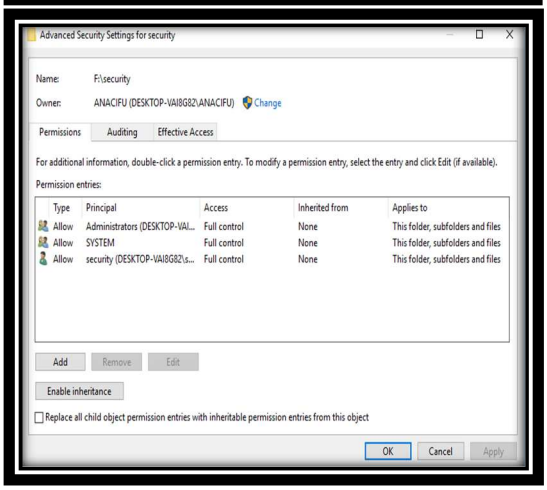
In the **"second"** group we include **security** and **servers** users.

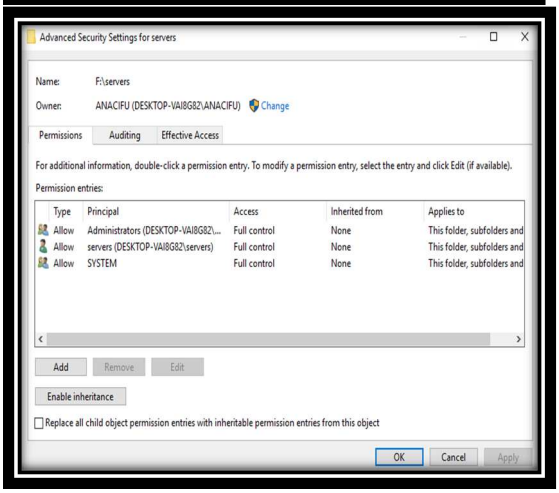


Now, from **File explorer->F:** you have to create all four folders with “full control”.

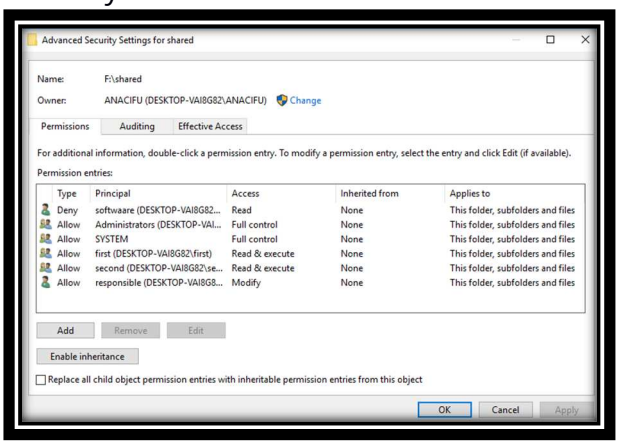




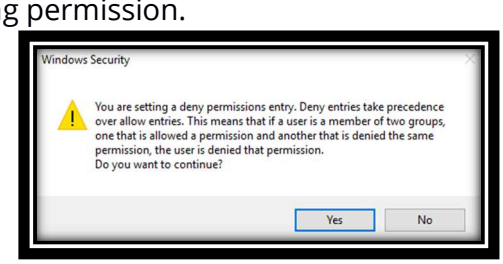




Now, we create a read-only folder for all the students called “shared”. The responsible user is able to create or delete files and folders. This folder cannot be accessed by software first-year users.

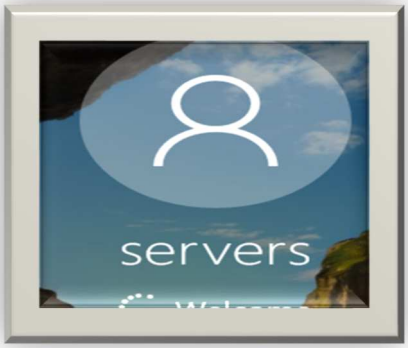


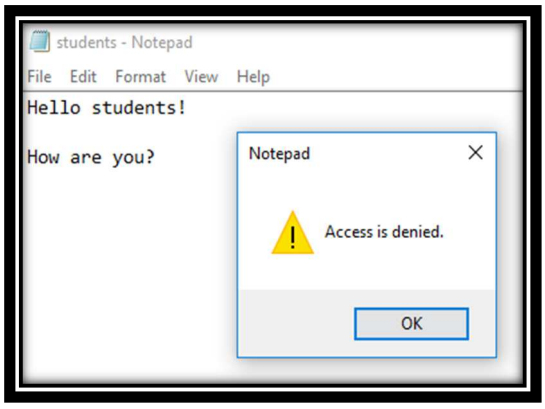
This screen informs that when denying permissions to a user, if he has allow the permissions in another group, I will take into account the most restrictive so will deny the corresponding permission.



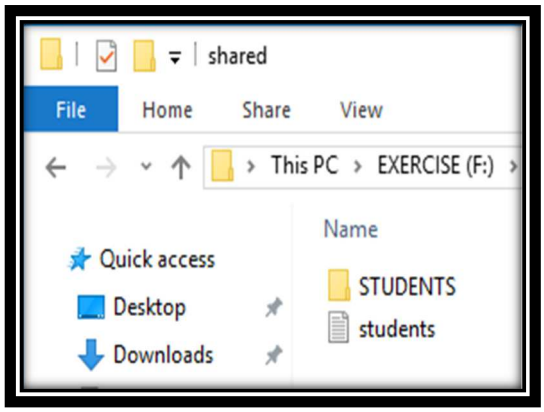
After including all this information, we restart the computer.

Now, we are check that the shared folder is only for read.

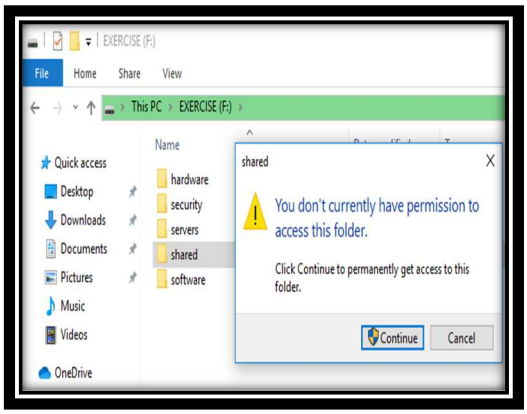




Now, we are check that the **responsible** user is able to create or delete files and folders.

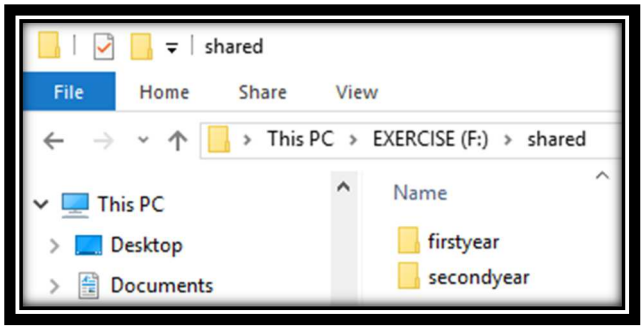


Then, we are check that the **software** user cannot access to **shared** folder.

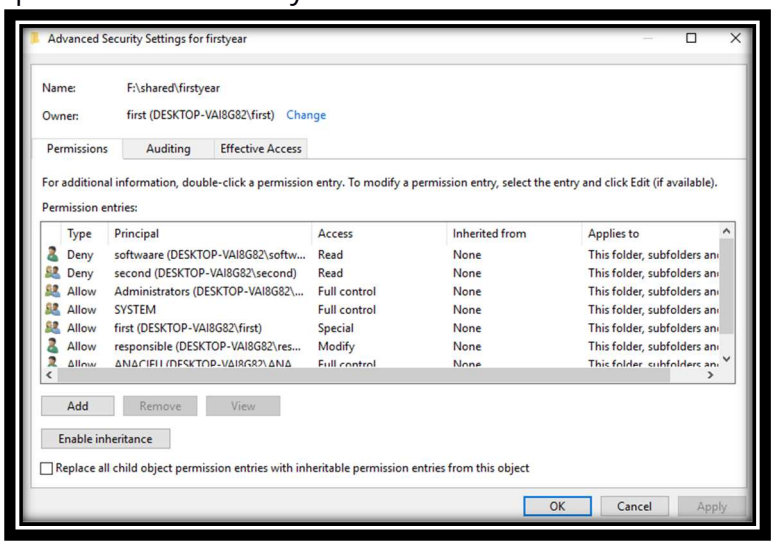


A folder only for first year students into the shared folder. They can create files and folders but not delete them and second year students will not be able to access.

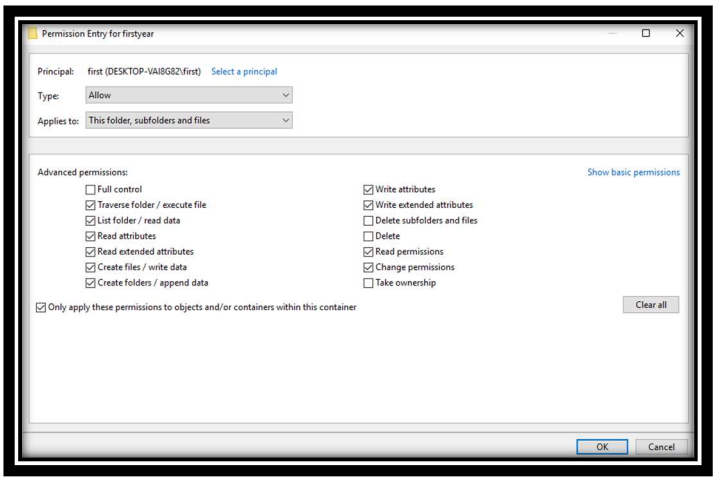
For the subfolder consider two scenarios: inheritance and non-inheritance. The **responsible** user has permissions as **administrator**. Optional change ownership to corresponding user.



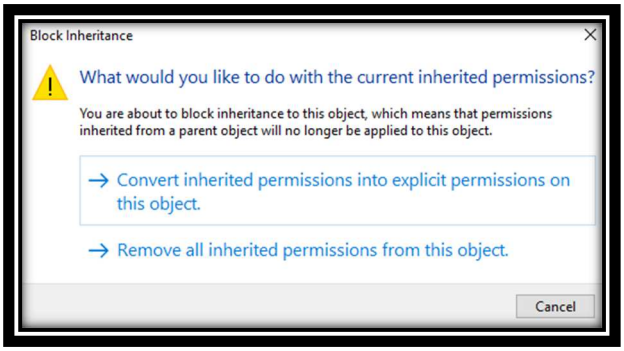
Those are the permissions for firstyear folder.



Mark the option “Only apply these permissions to objects and/or containers within this container.



Now, in order to disable inheritance, click on the **“Disable Inheritance”** button. You will be asked to convert legacy permissions to explicit permissions or delete all inherited permissions. If you are not sure, choose to convert them. The following screenshot shows what happens when you choose to delete legacy permissions. Only explicit permissions remain.



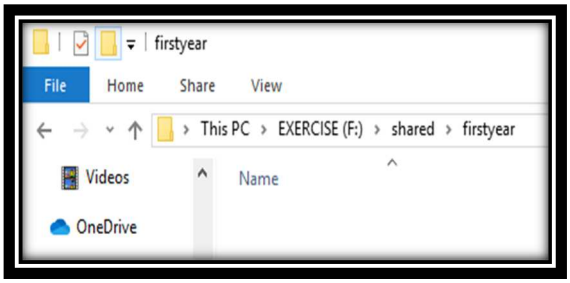
Click the Enable Inheritance button. Inheritance permissions will be added to the current permissions list.
Explicit permissions are those that are set by default on nonchild objects when the object is created, or by user action on nonchild, nonmajor, or child objects.

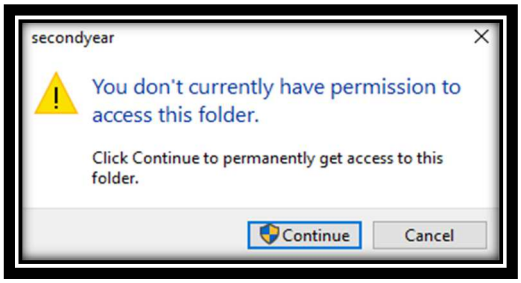
Inherited permissions are permissions that propagate to an object from a parent object. Legacy permissions facilitate the task of managing permissions and ensure that permissions are consistent across all objects within a given container.

By default, objects inside a container inherit permissions from that container when objects are created. For example, when you create a folder named MyFolder, all subfolders and files created within MyFolder automatically inherit permissions from

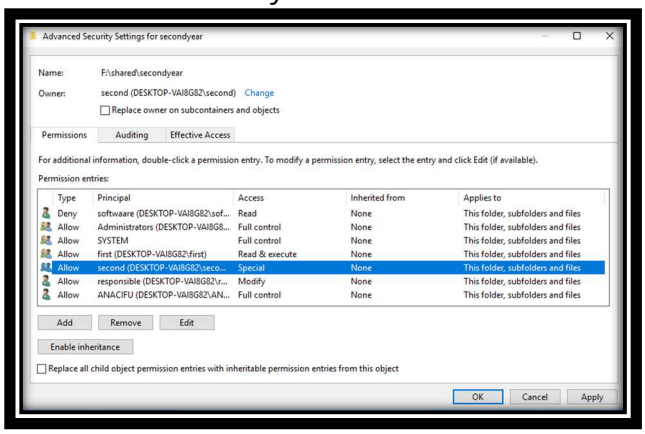
that folder. Therefore, MyFolder has explicit permissions, while all subfolders and files it contains have inherited permissions.

Hardware and **software** students are able to access to the firstyear folder but do not have access to the secondyear folder.

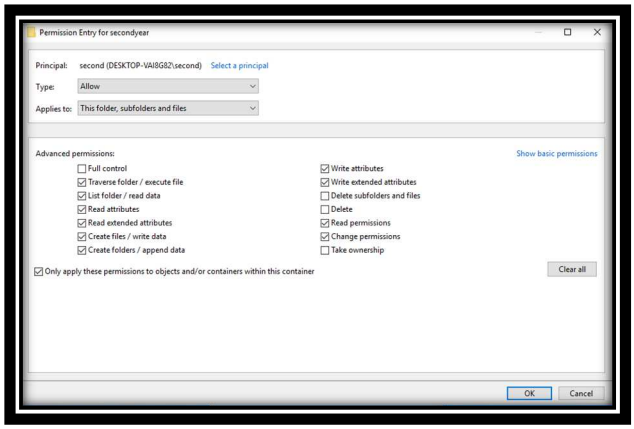




Those are the permissions for secondyear folder.



Mark the option “Only apply these permissions to objects and/or containers within this container.



Security and **servers** students are able to access to the secondyear folder but do not have access to the firstyear folder.