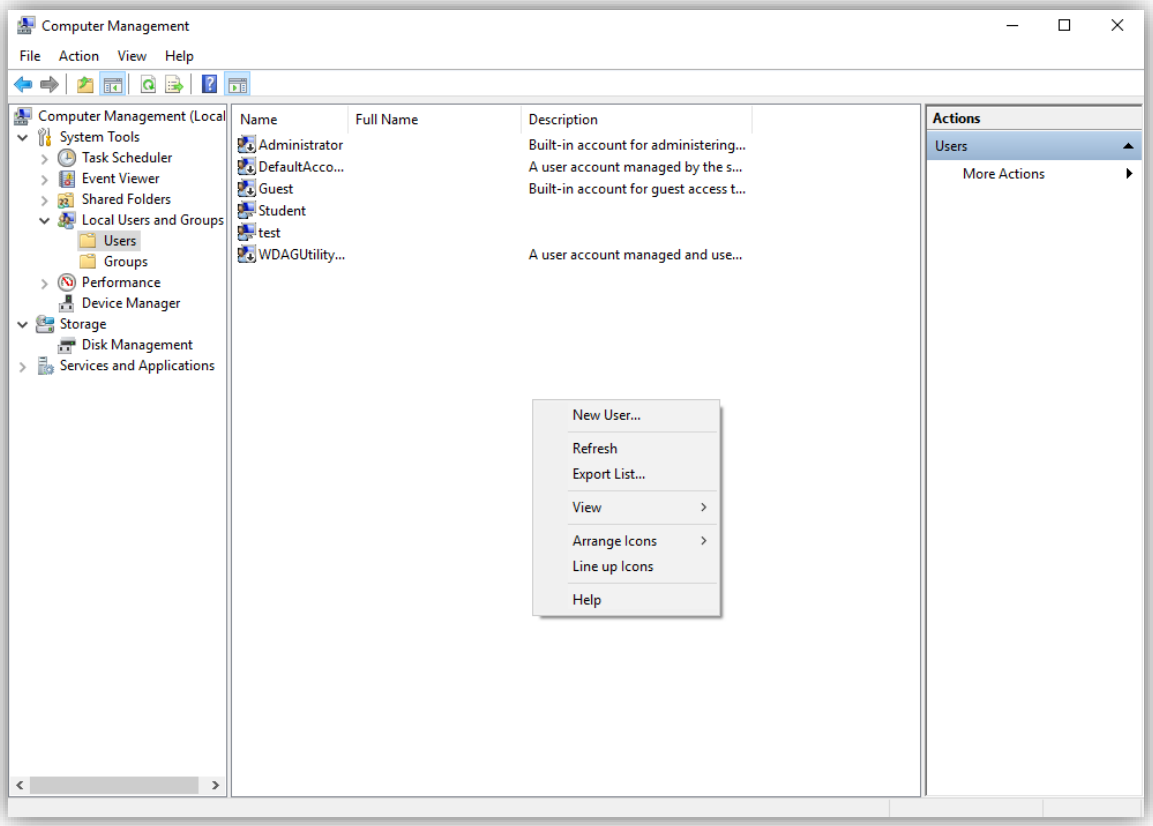
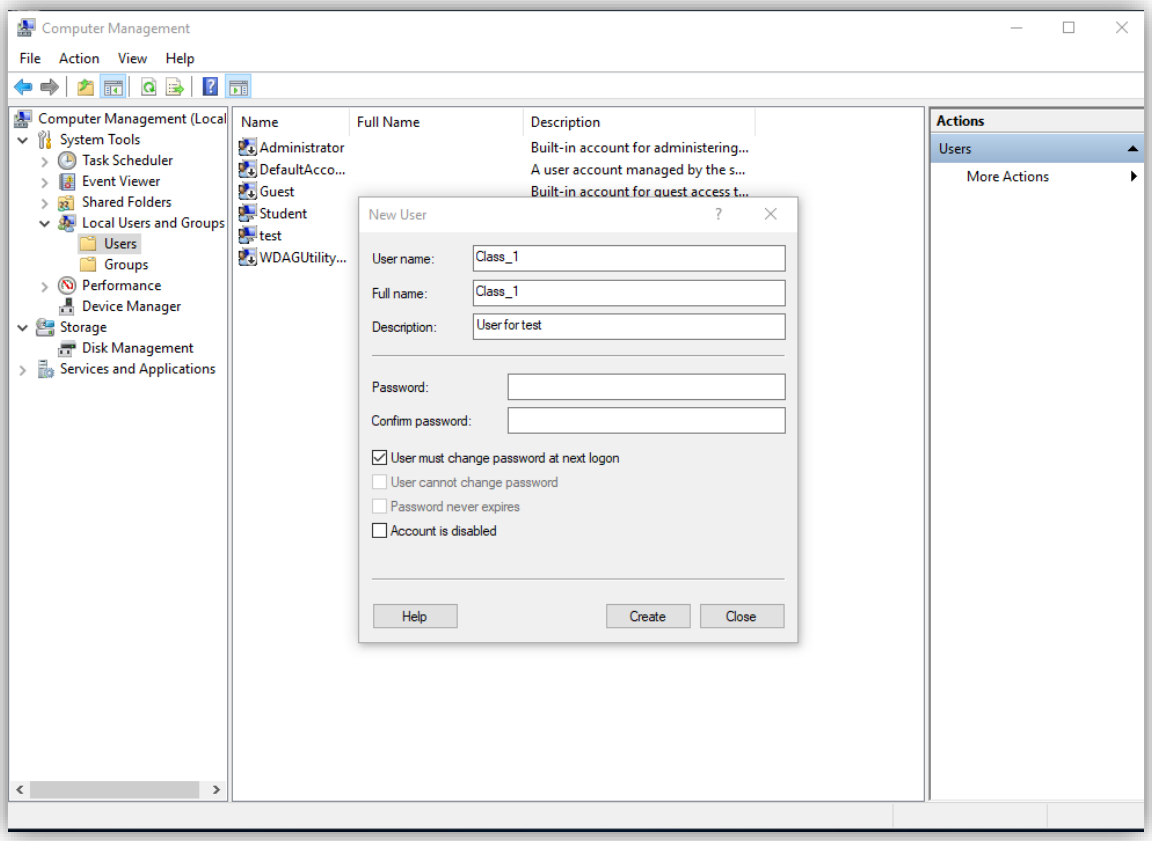
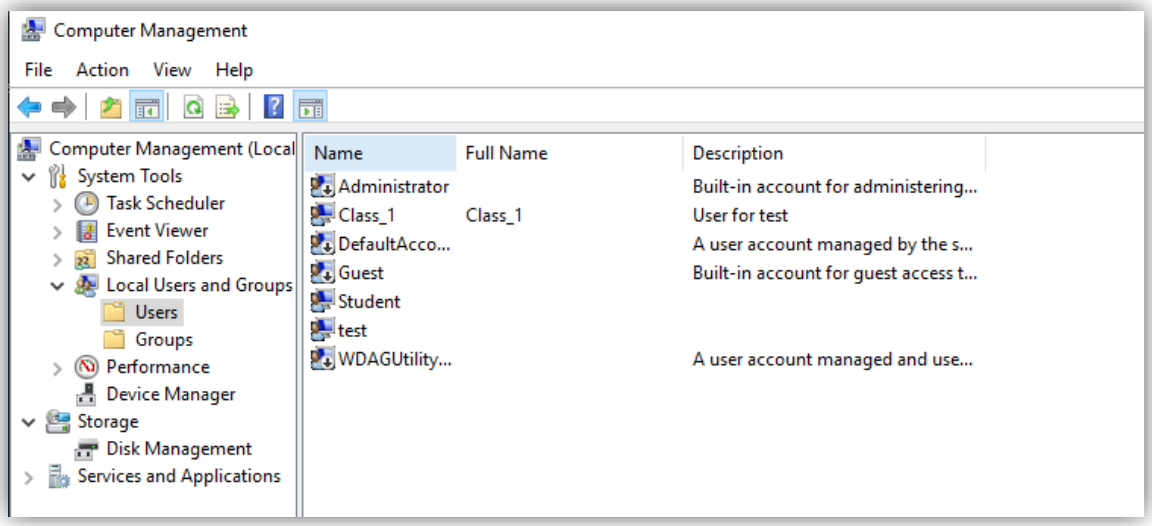
1. **Add a new standard user named “Class_1” including the description and full name. The user must change the password at the next logon.**

Computer Management/ Local Users and Groups/ Users

Right-click and choose the



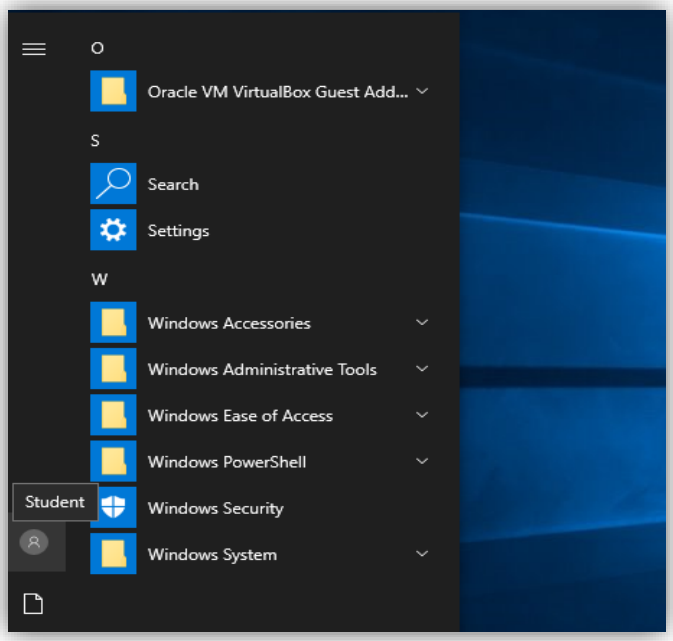




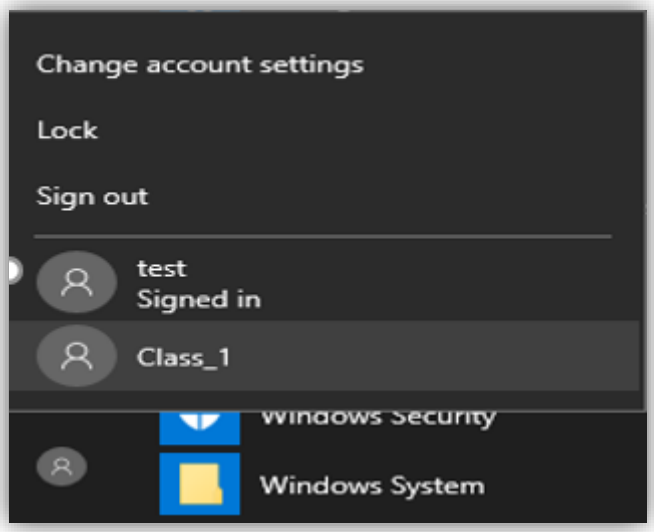
2. Complete the following parts about the user “Class_1” from the previous exercise.

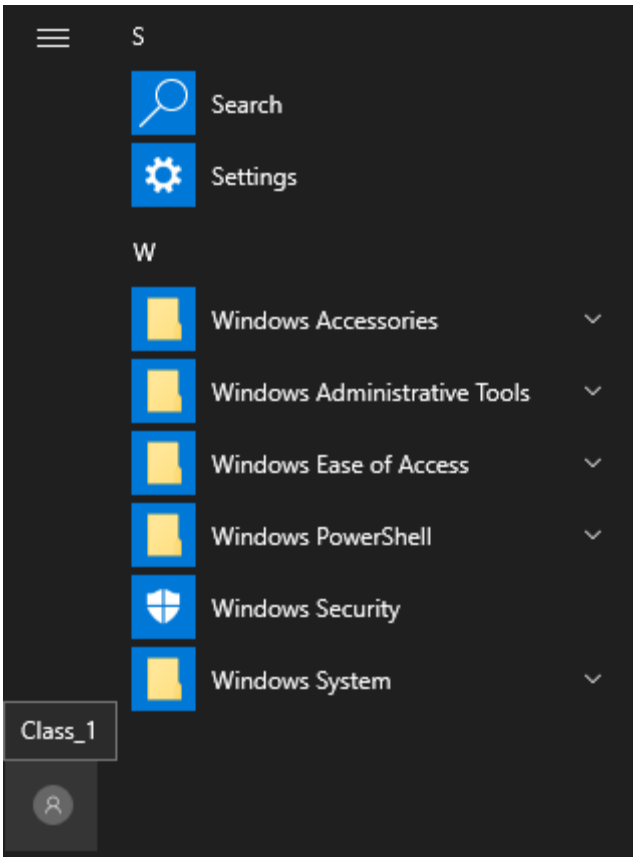
• Verify if the profile folder exists.
This folder does not exist, at this point.

- **Log in as “Class_1”.**



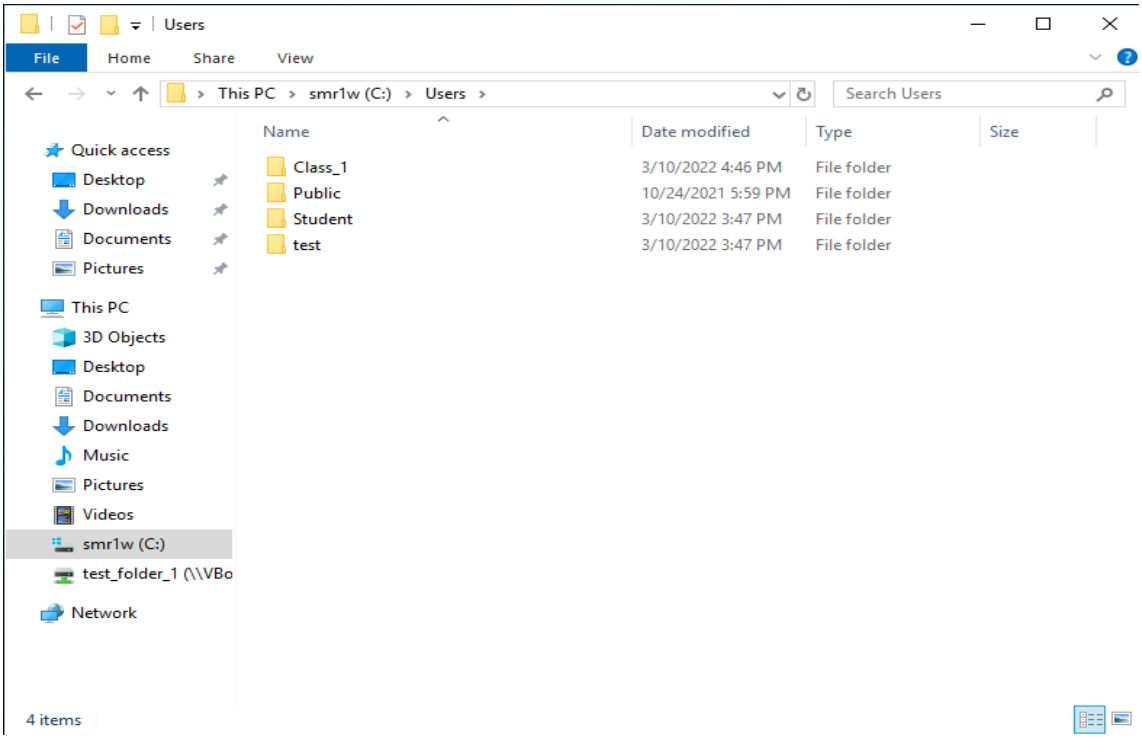
- Click on the icon and select the profile you want to log in





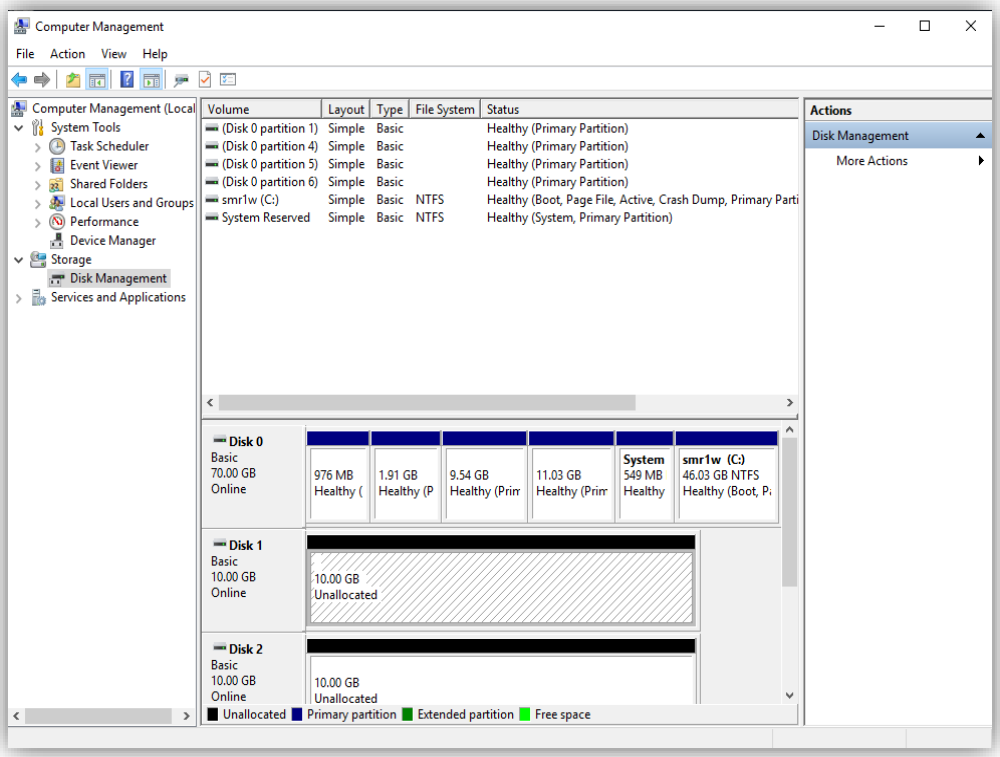
- **Verify if the profile folder now exists.**

It is necessary to log in once the folder is created.

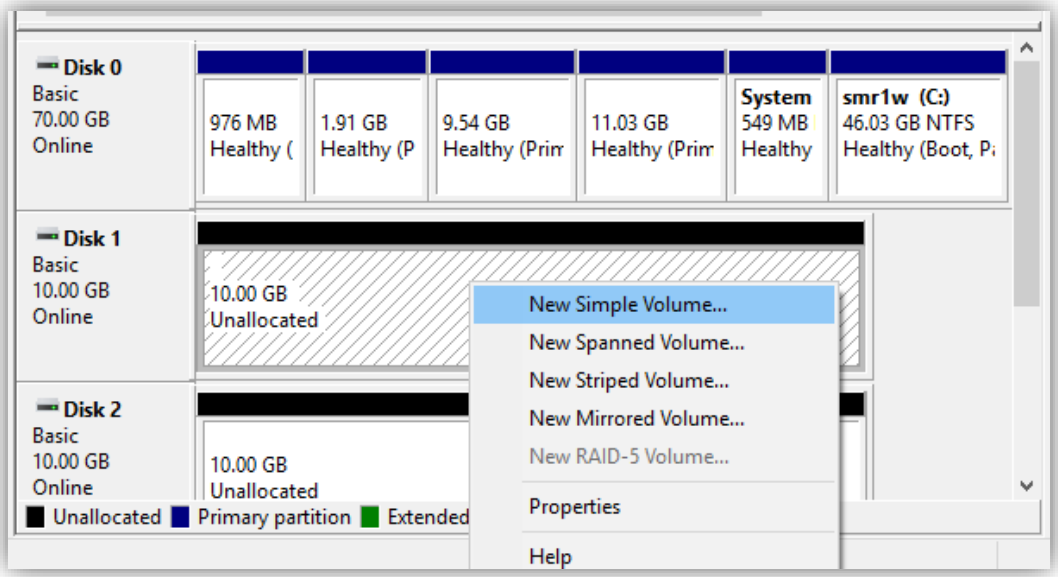


• Add a second hard drive to the virtual machine and create a folder called "My Documents" in F:

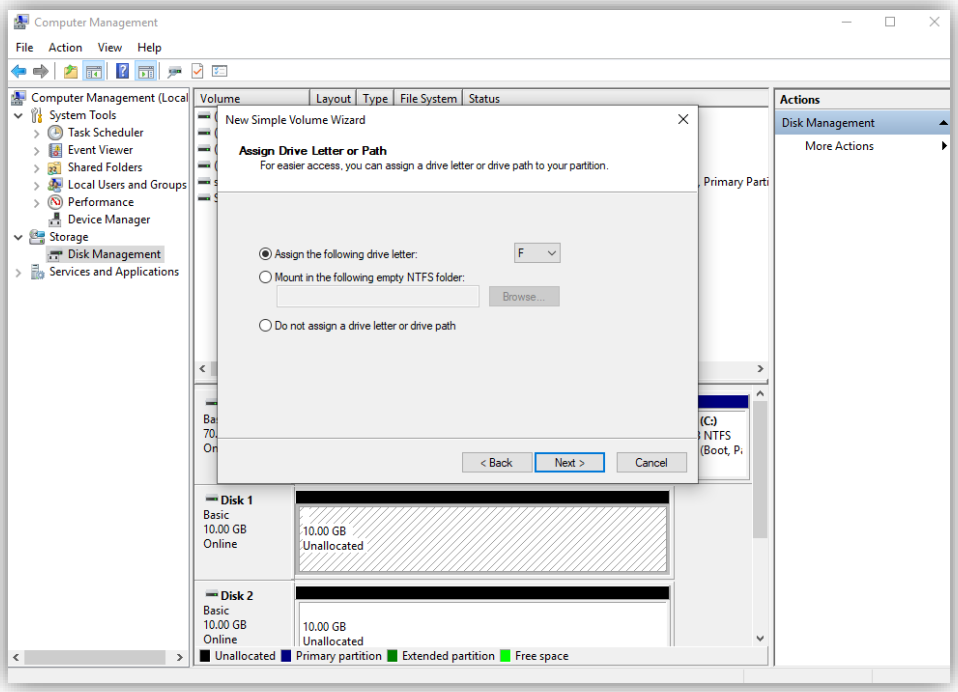
First of all, we need to create a simple volume.

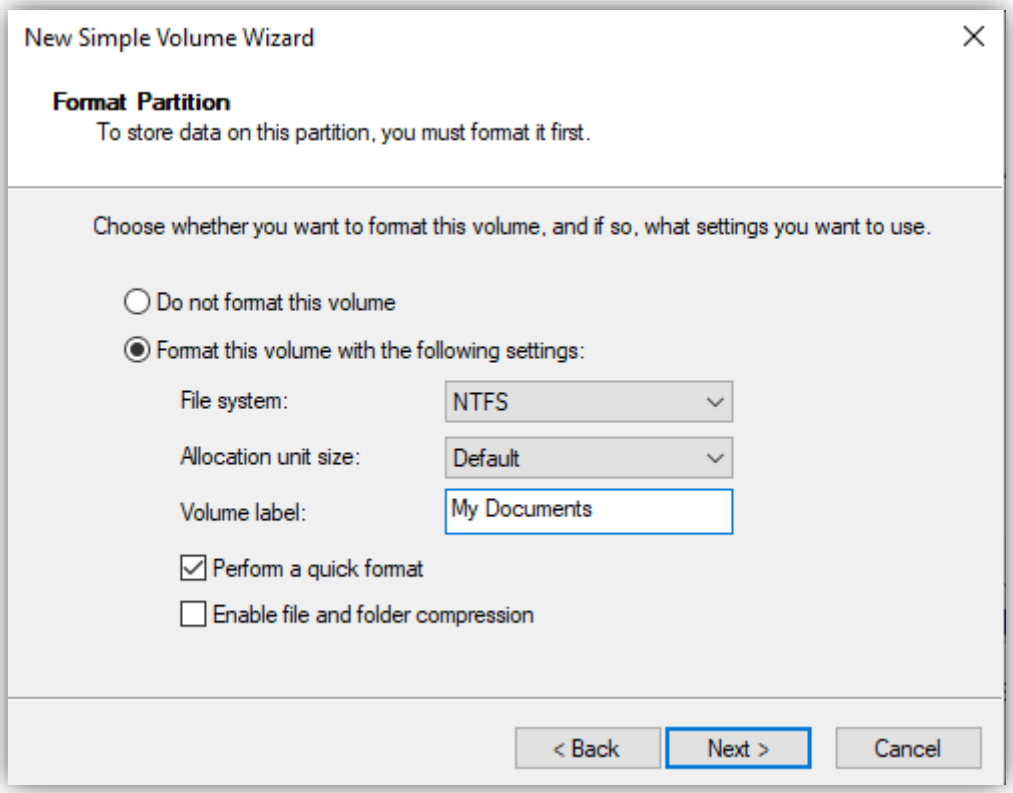


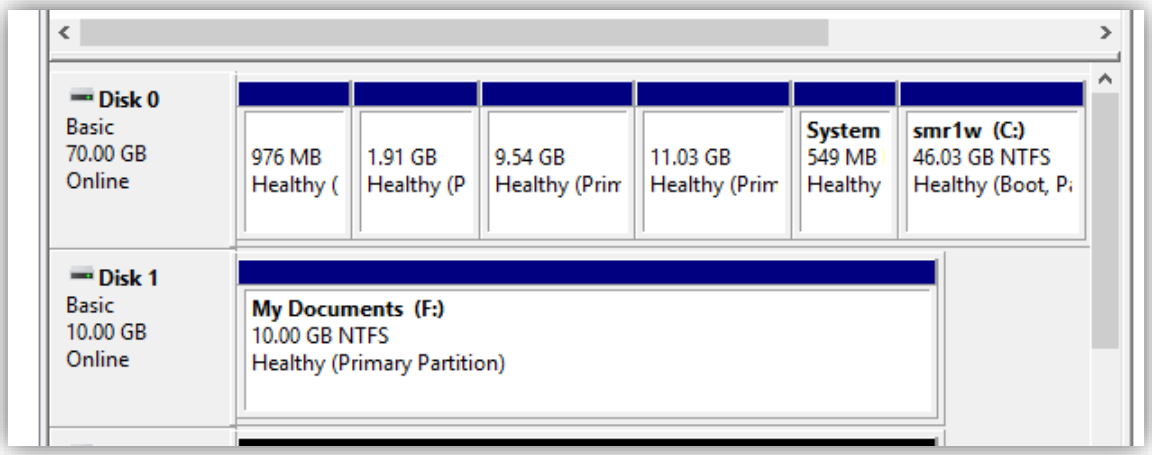
Right-click on the unallocated space and click on new simple volume:



Assign the letter that you want, in this case F:

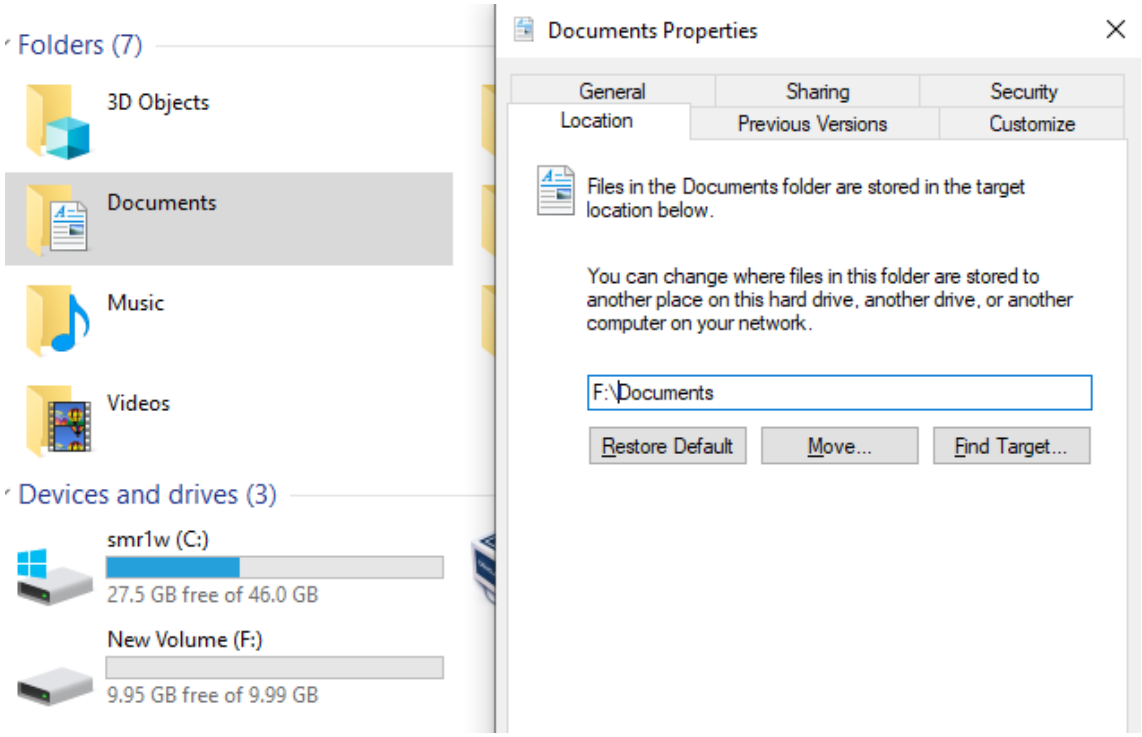

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Volume Layout Type File System Status
Actions
Disk Management
More Actions
New Simple Volume Wizard
Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.
Assign the following drive letter: F
Mount in the following empty NTFS folder:
Browse...
Do not assign a drive letter or drive path
< Back Next > Cancel
Disk 1
Basic
10.00 GB
Online
10.00 GB
Unallocated
Disk 2
Basic
10.00 GB
Online
10.00 GB
Unallocated
Unallocated Primary partition Extended partition Free space

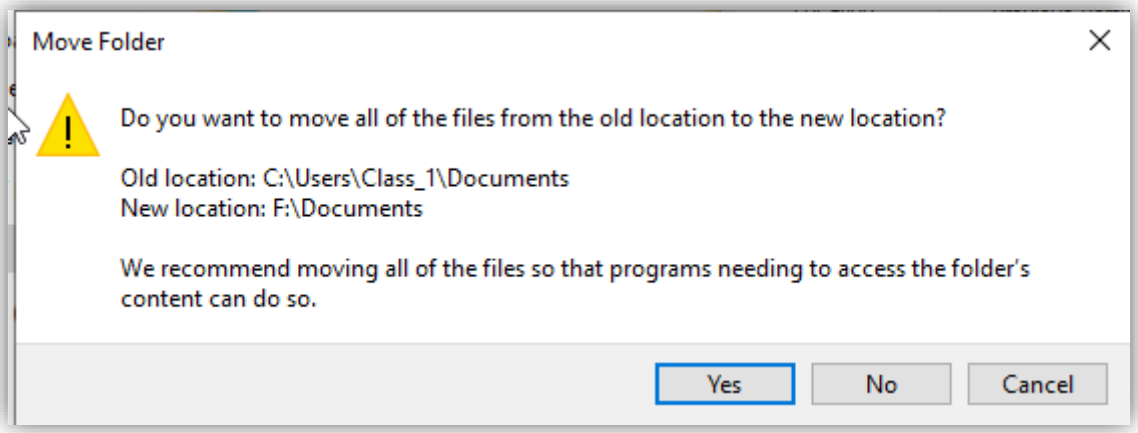

New Simple Volume Wizard
Format Partition
To store data on this partition, you must format it first.
Choose whether you want to format this volume, and if so, what settings you want to use.
Do not format this volume
Format this volume with the following settings:
File system: NTFS
Allocation unit size: Default
Volume label: My Documents
Perform a quick format
Enable file and folder compression
< Back Next > Cancel



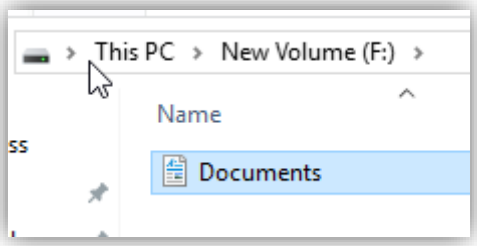
- **Move "Class_1" Documents folder to the directory you have just created.**

In order to do this, go to documents properties, and from location move to the new location, in this case, F:\Documents



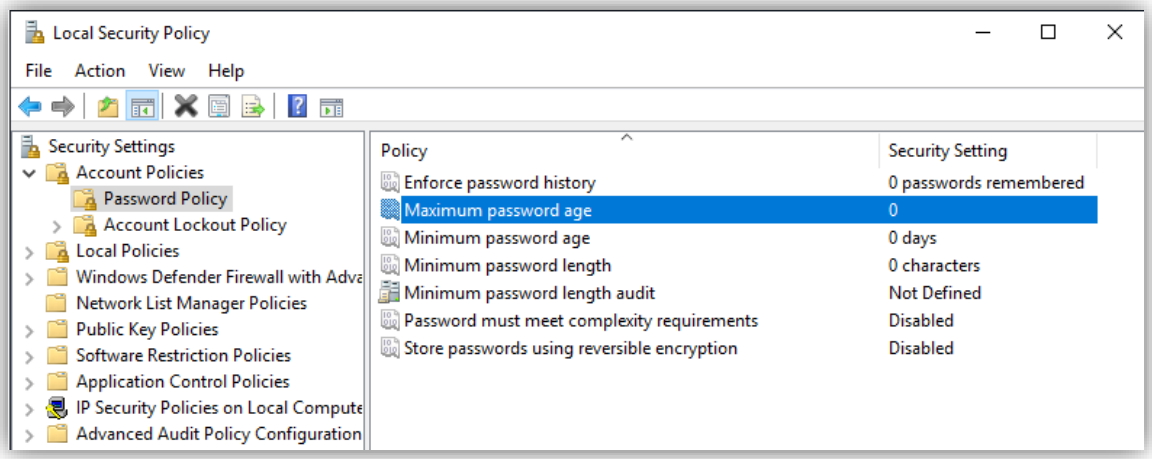


• Open “Documents” shortcut and create a new folder. Check if this folder has actually been created in “F:\My Documents”.



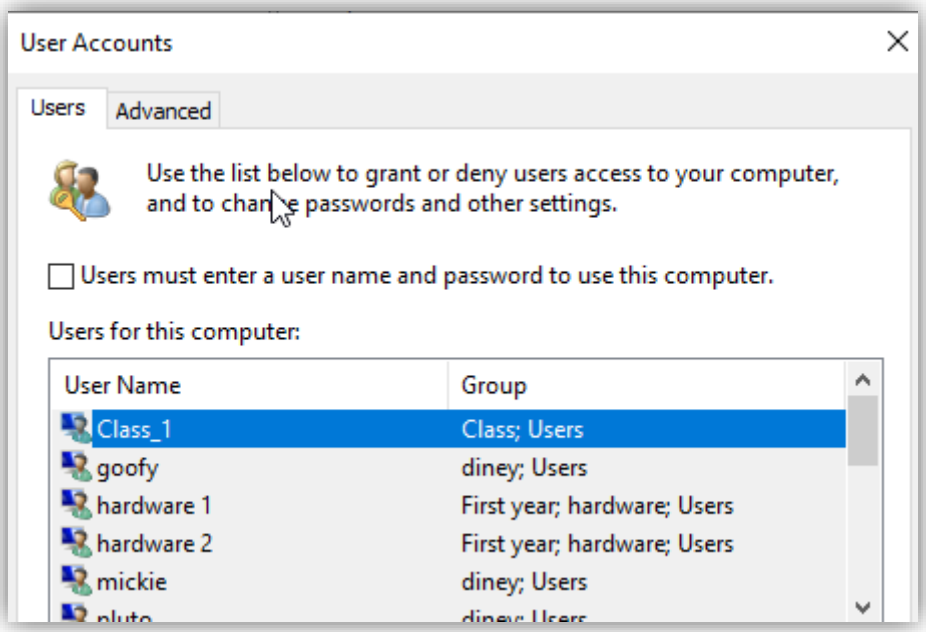
3. How do you configure a user to log in without a password and automatically when turning the computer on?

In order to do this, it is necessary to set the minimum length and the complexity requirement like the screen below.



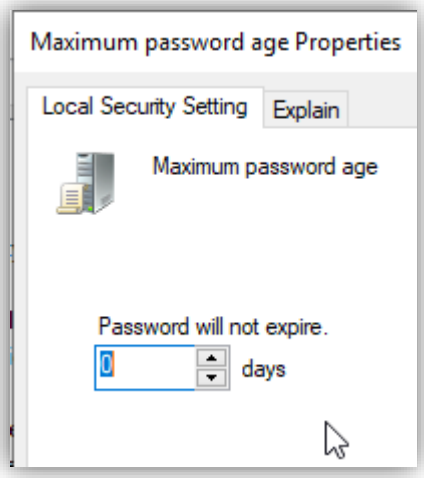
With this configuration, you can create a new user in the same way as in the exercise before, without a password, and for enter automatically when turning

the computer on, you must type “netplwiz”, and uncheck the option shown below.



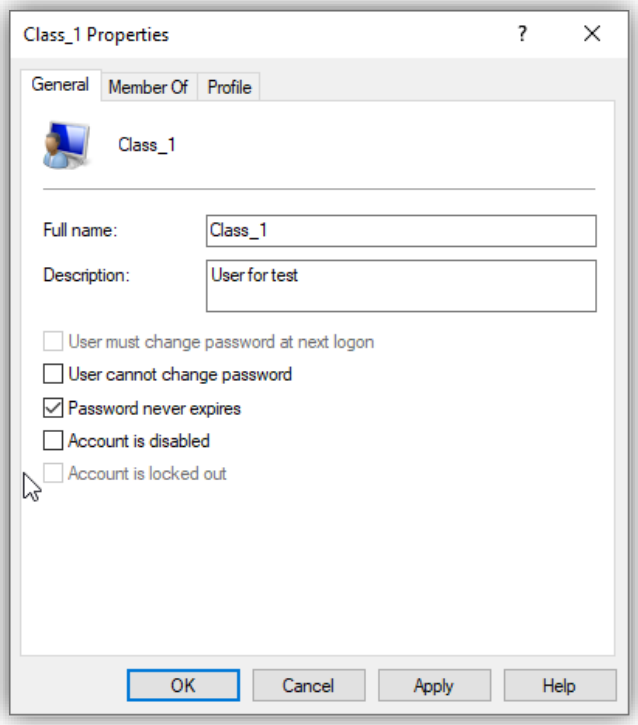
4. How do you configure a specific user so that the password never expires? How can you configure this policy for everyone?

You need to go to the Local Security Setting and set the maximum password age in zero days.



5. When can you use a locked account?

Even if the user is locked for logon failed attempts, the administrator can unlock it from computer management.



6. Imagine you define an "Account lockout threshold" of 3 and "Account lockout duration" of 5. What would be the valid values of "Reset account lockout counter after"? What if "Account lockout threshold" value were 0?

Reset account lockout counter after must be less or equal to "Account lockout duration".
A value of 0 specifies that the account will be locked out until an administrator explicitly unlocks it.

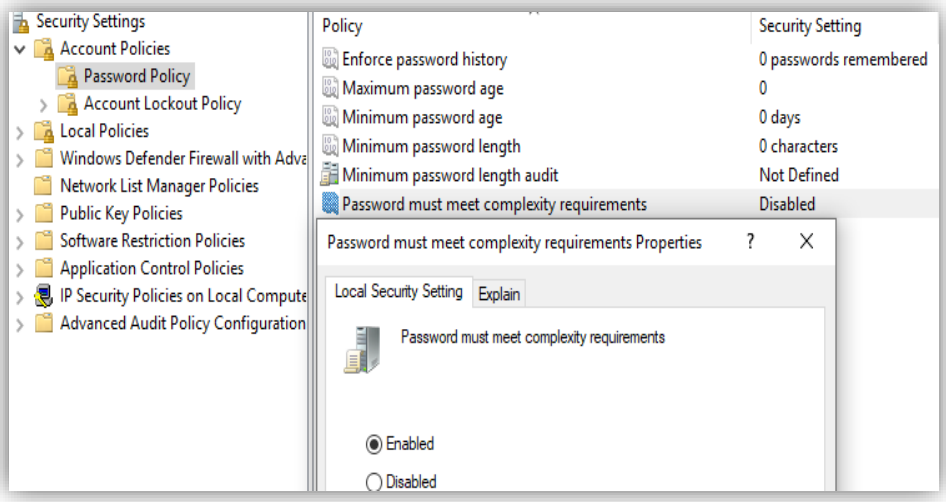
7. Configure the system according to the following criteria:

• All the passwords must have at least 8 characters.

Go to Local security policy/Account policies/password policy/minimum password length.

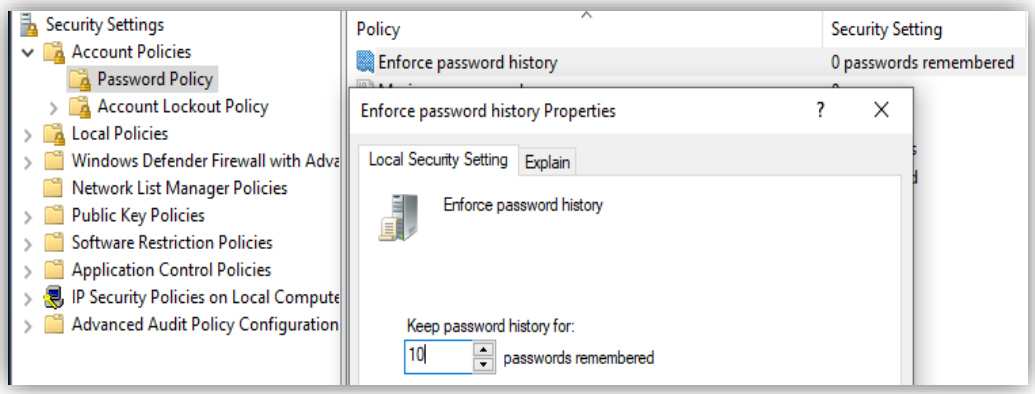
• All the passwords must contain uppercase, lowercase, numbers and nonalphanumeric characters.

Go to Local security policy/Account policies/password policy/password must meet complexity requirements.



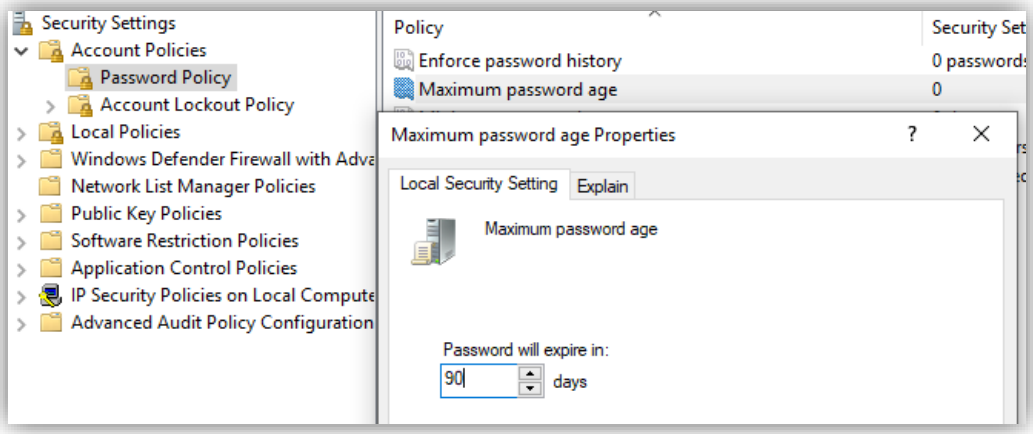
• The system stores the last 10 passwords for each user.

Go to Local security policy/Account policies/password policy/Enforce password history.



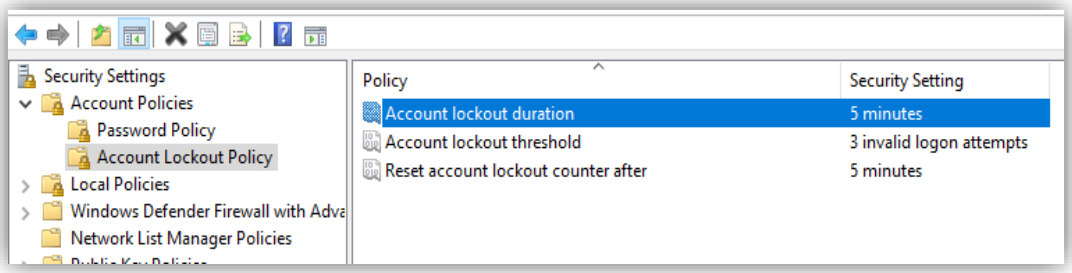
• All the passwords expire after 3 months.

Go to Local security policy/Account policies/password policy/maximum password age.



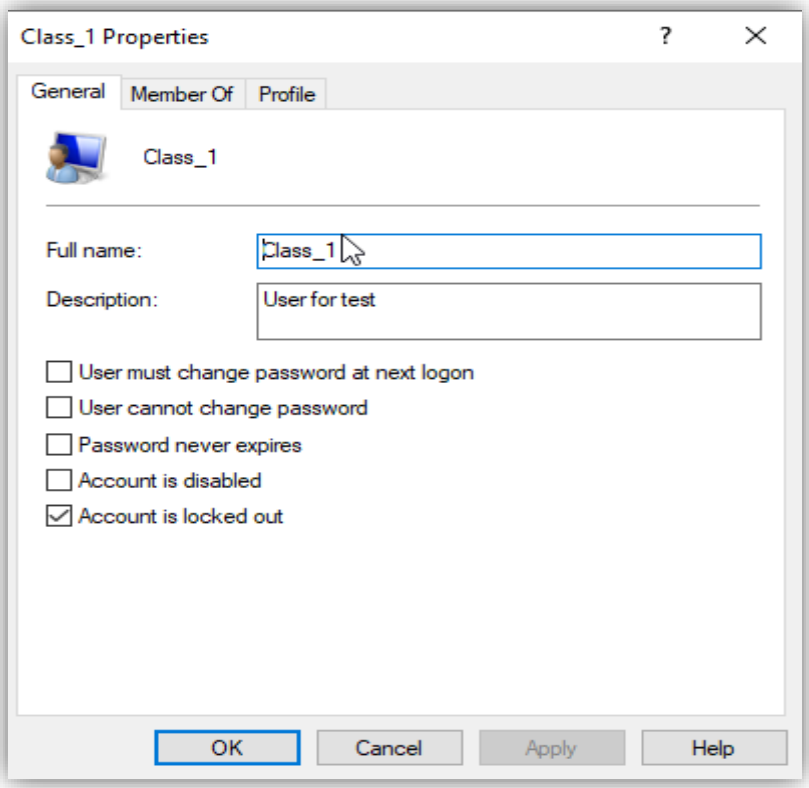
8. Configure the user "Class_1" to be locked after 3 invalid logon attempts. If the user is locked out, it will be able to type the password again in 5 minutes. Complete the following steps:
• Lock the user. • Unlock the user as administrator and check if the user is able to log in. • Lock the user again. • Wait for 5 minutes. • Type the right password and check if the user is able to log in.

In the picture below, we can see how we have to configure the security setting to have the requirements asked for this exercise.



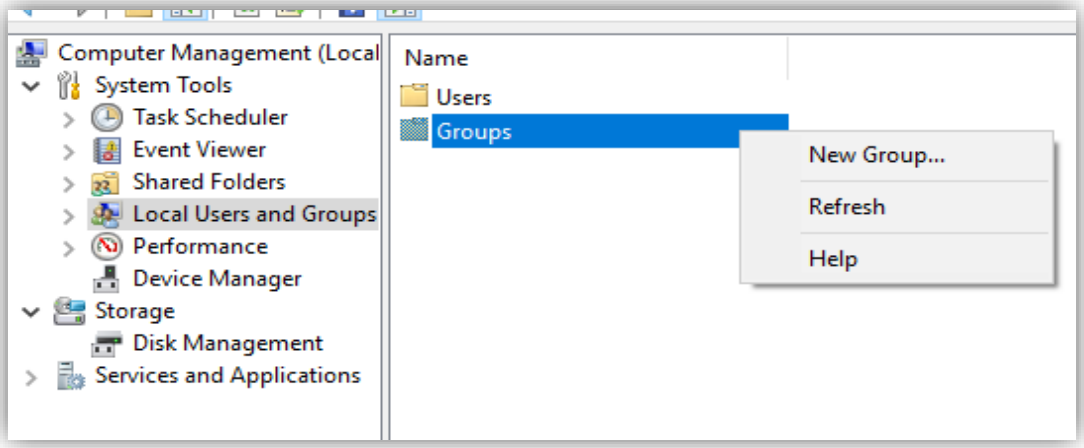
After three attempts the user is locked:

Then we can unlock the user from the administrator. Go to computer management and select the user who you need to unlock, uncheck the “Account is locked out” and press ok.

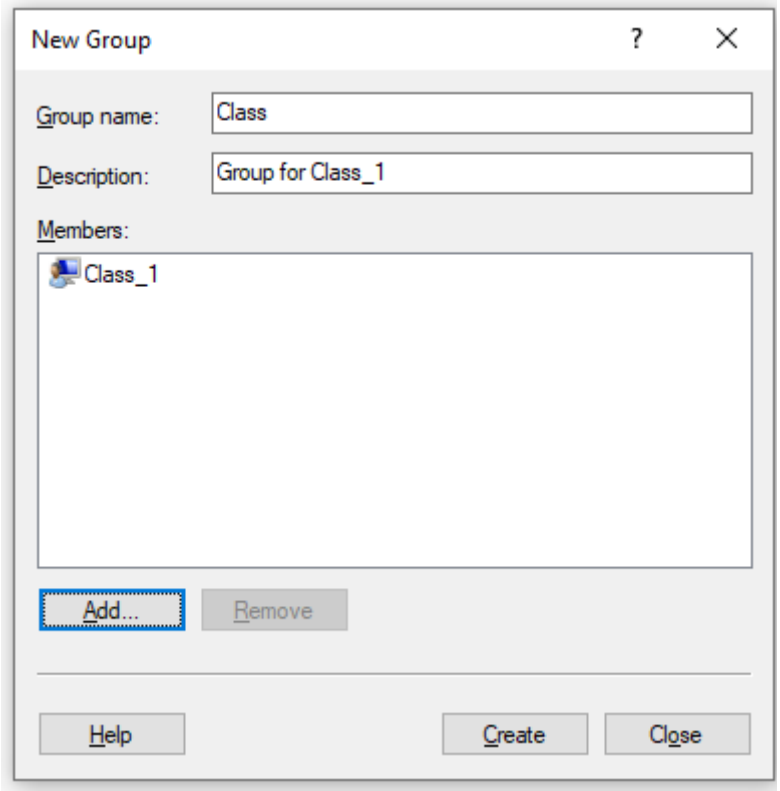


9. Add a new group name “Class” and complete the following: • Add the user “Class_1” to the group “Class”. • Create a guest user called “Class_2”, initially disabled that cannot change the password. Then, add the user to “Class”.

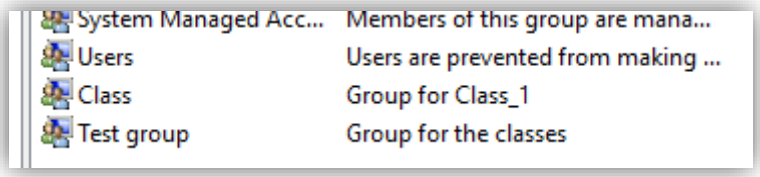
Go to Computer Management\System Tools\Local Users and Groups\Groups, click on Local Users and Groups, and then right-click on Groups



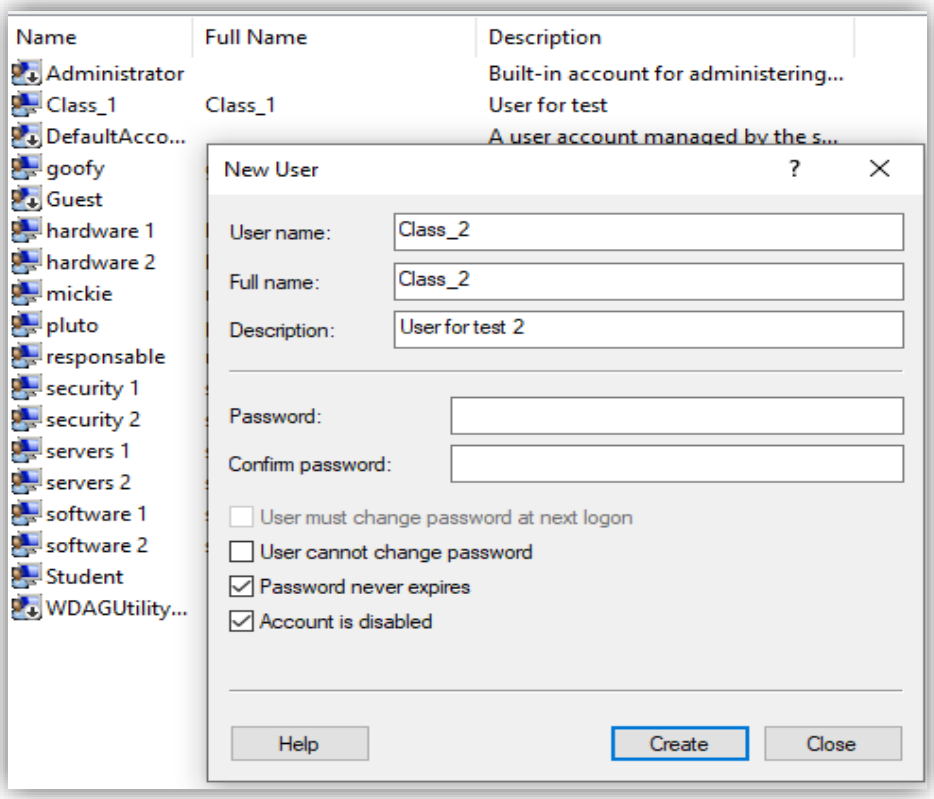
After that you have to click on new group and add the user you want to include throw the Add option.



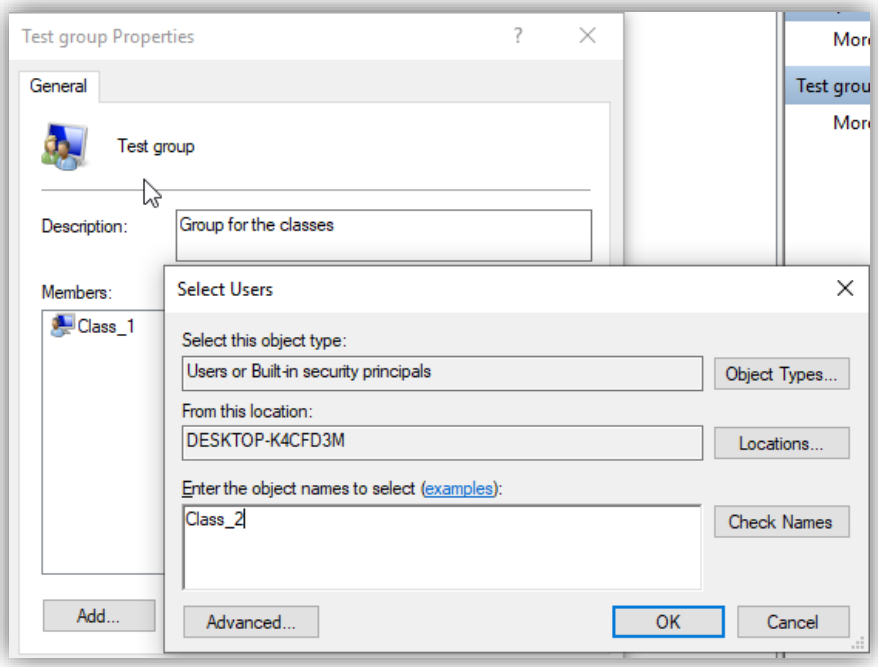
Then the group is created.



Create a new user from computer management:

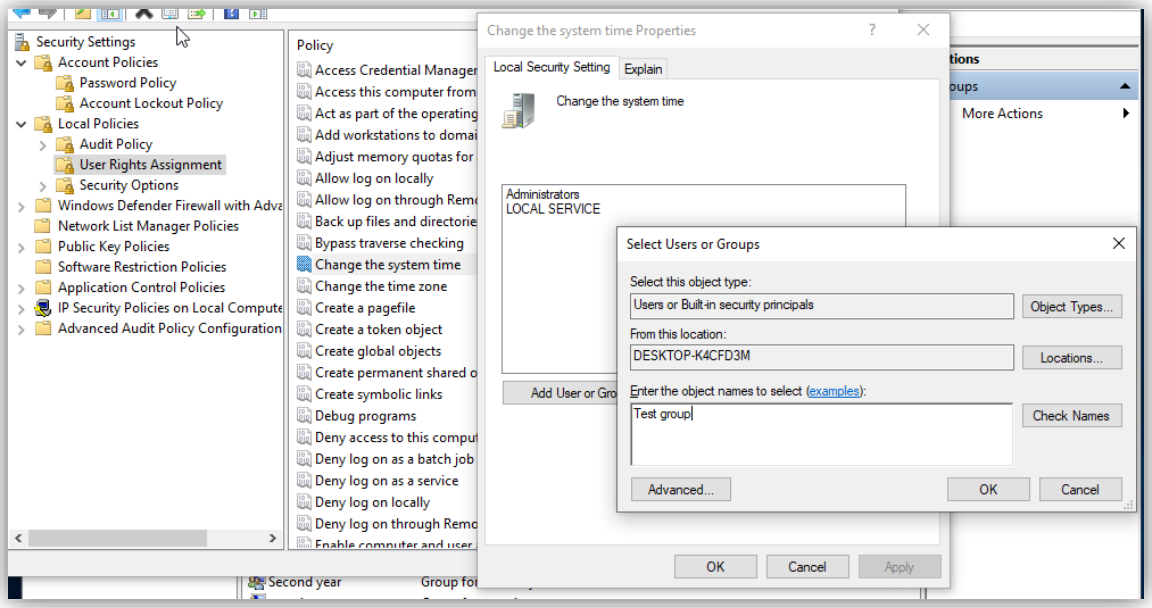


Now add the user to the previous group created:

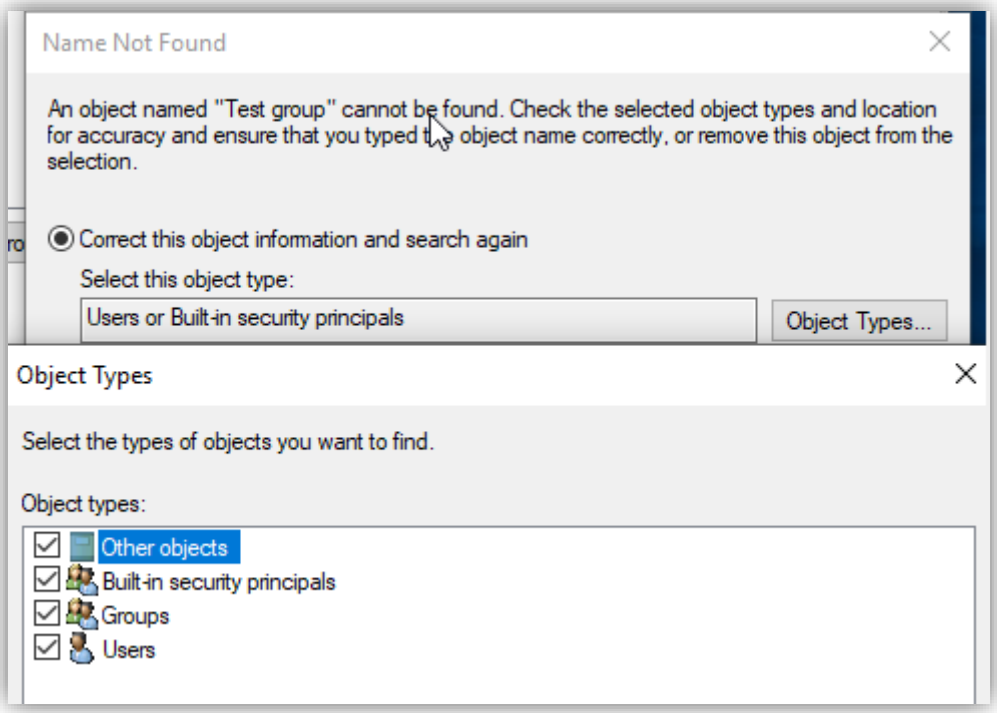


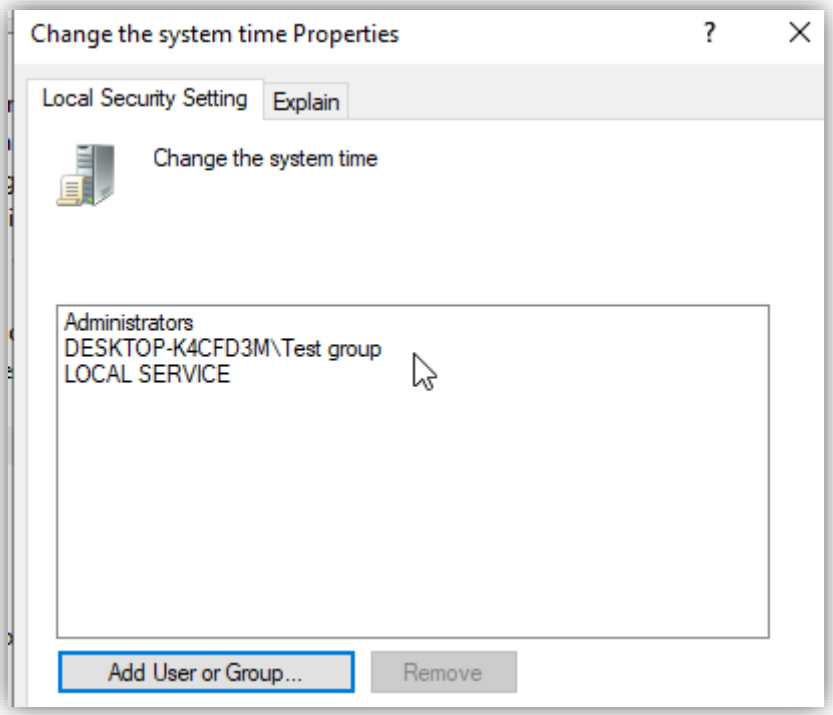
10. Modify the user rights so "Class_1" and "Class_2" will be able to "Change the system time".

For this proposal, go to Local security policy/Local policies/User rights assignment/change the system time, and add the group.



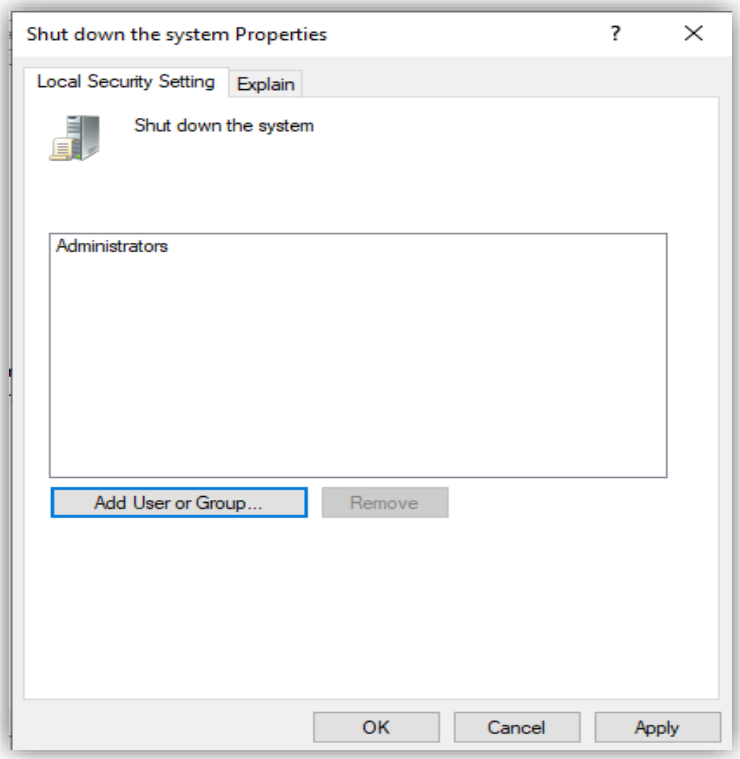
Then check names and add the type group from object types:





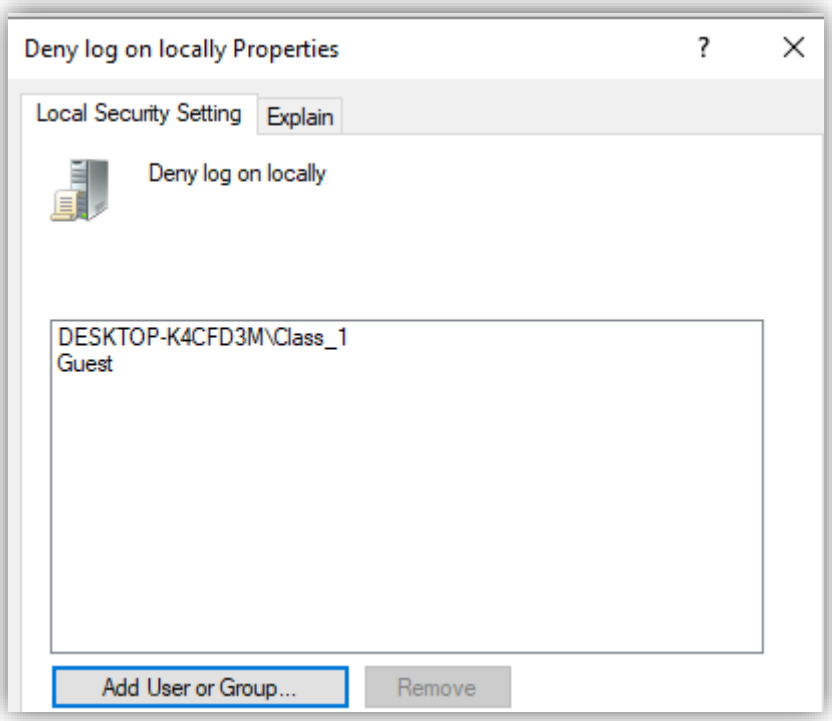
11. Modify the user rights so that only the administrator users can “Shut down the system”

It is necessary to remove all the users, except the administrators, from the policy below:



12. Suppose all the standard users are able to log in. How can we deny log on to the specific user “Class_1”?

Go to Local security policies/user rights assignment and Deny log on as locally.



13. Overall, add a new user called "Test" according to the requirements in exercise 7. What if we deleted "Test" from the group "Users"? Try to log in and explain what happens.

It is necessary to set a valid password with non-alphanumeric characters, a minimum length of 8, uppercase, lowercase, numbers, being a valid password "Local_123".

If we delete the test from the group users, the Test user cannot be able to log in. This is because the user doesn´t belong to any groups that are able to log in.