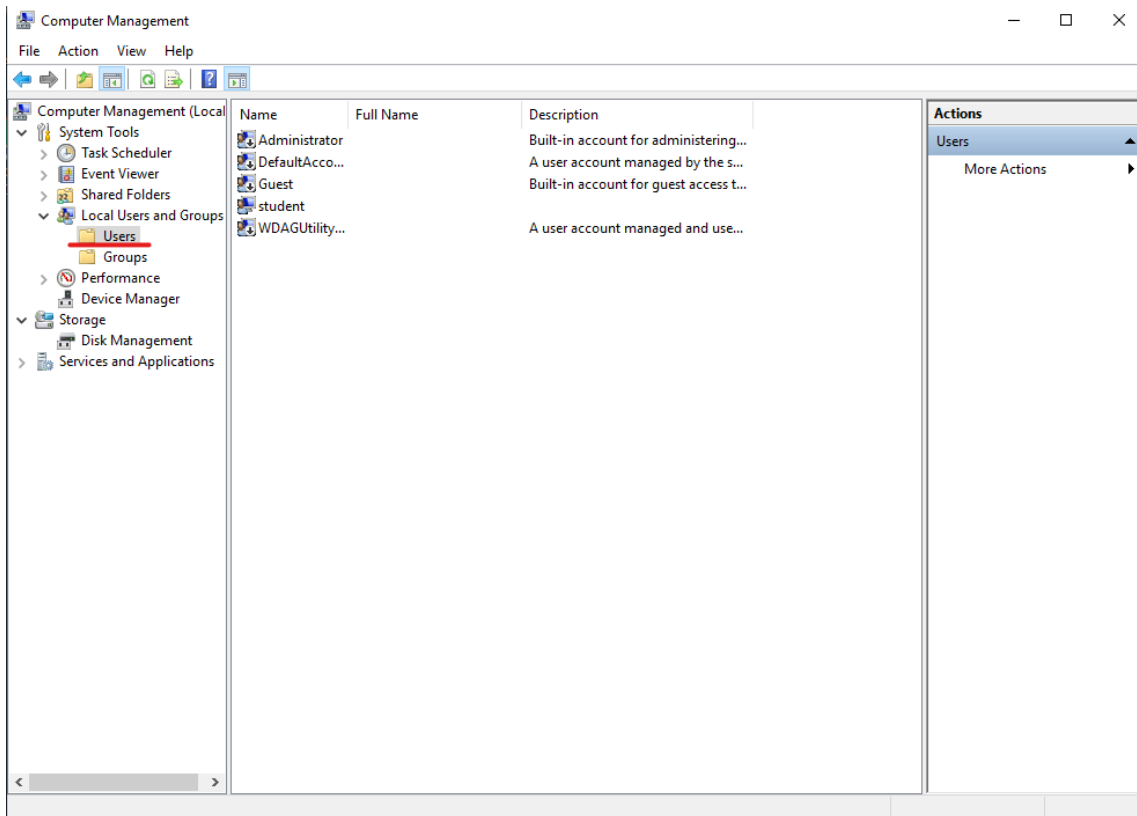


1. Add a new standard user named “Class_1” including the description and full name. The user must change the password at the next logon.

First, we will need to go to the computer management tab, then we will go to **Local users and groups**. Then we will click on the **More Actions** tab and start with the creation of a new user.



The 'New User' dialog box is shown with the following fields and options:

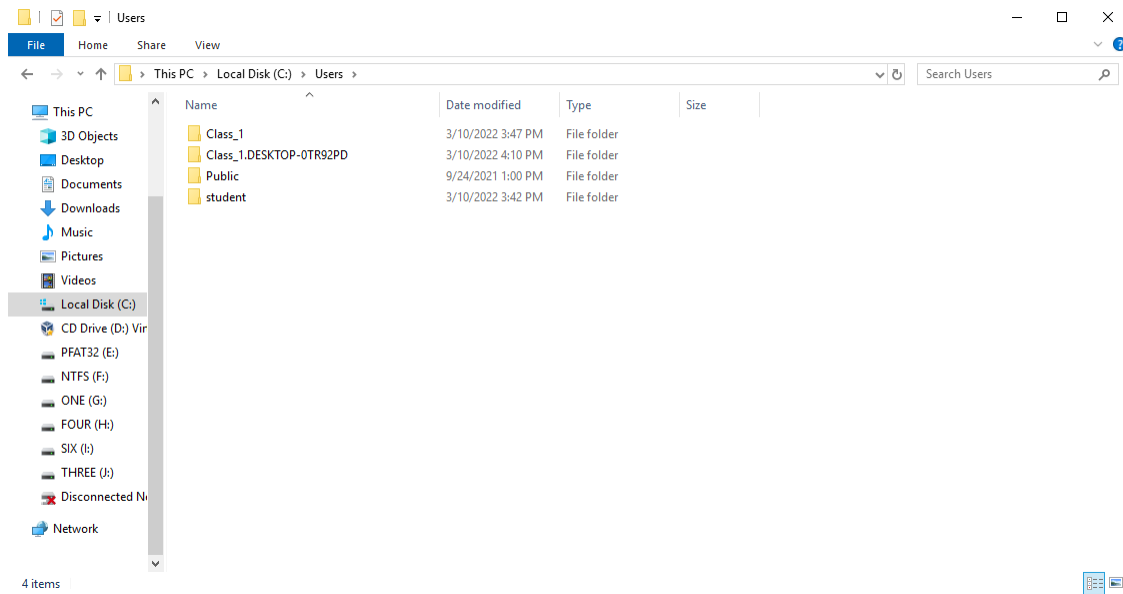
- User name:
- Full name:
- Description:
- Password:
- Confirm password:
- ☒ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled

Buttons at the bottom: Help, Create, Close.

Now we will make sure that the ‘**User must change password at next logon**’ is turned on before hitting ‘**Create**’.

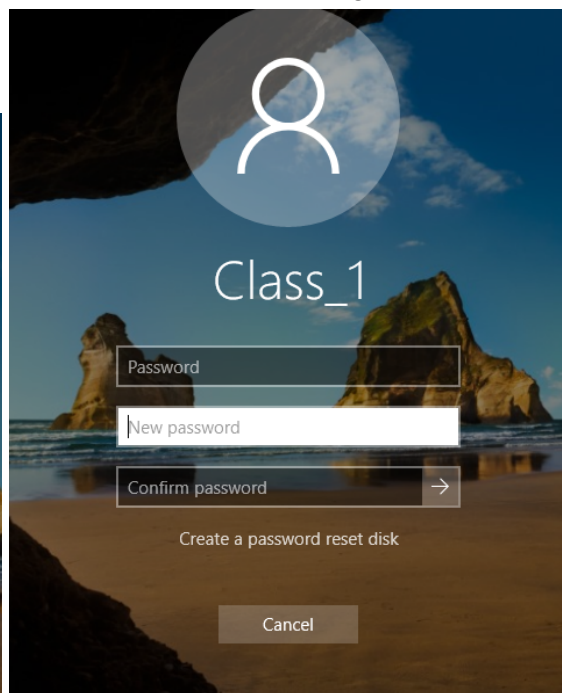
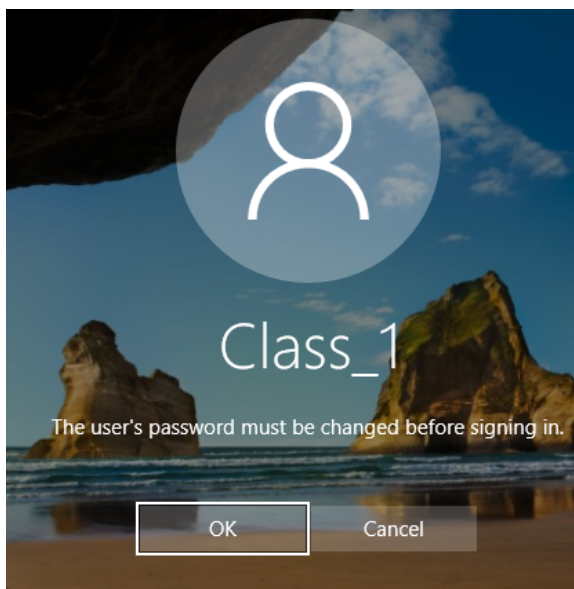
2. Complete the following parts about the user “Class_1” from the previous exercise.

-Verify if the profile folder exists.



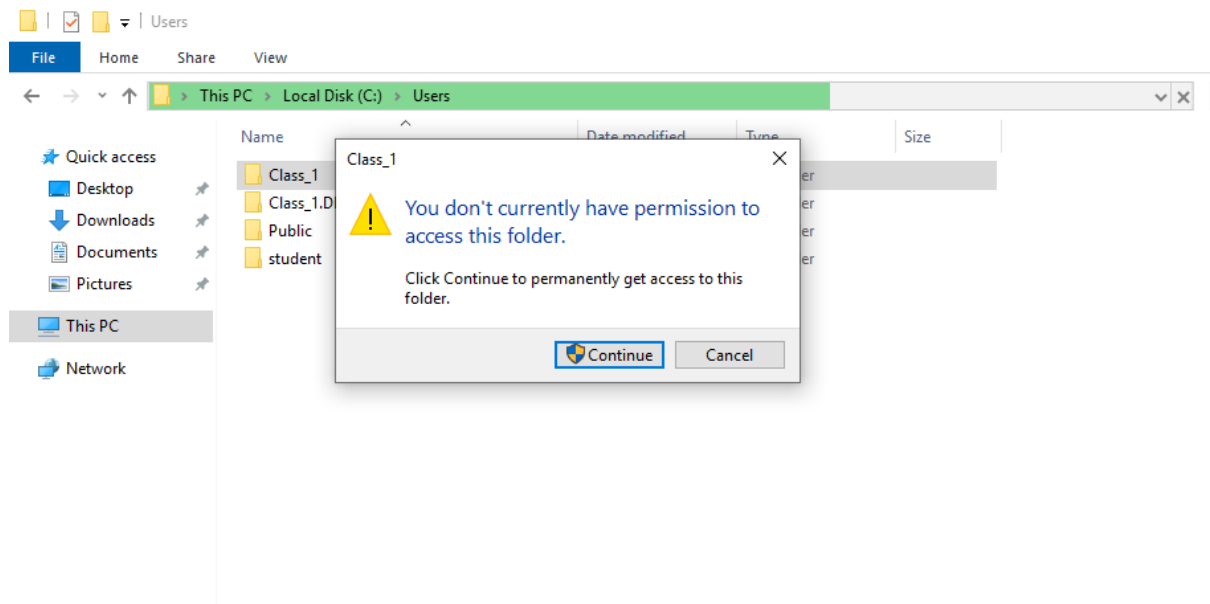
-Log in as ‘Class_1’

After signing out from ‘Student’, we will find out that if we want to login ‘Class_1’, Windows will ask us to set a password. Finally if we set a password it will let us sign in.



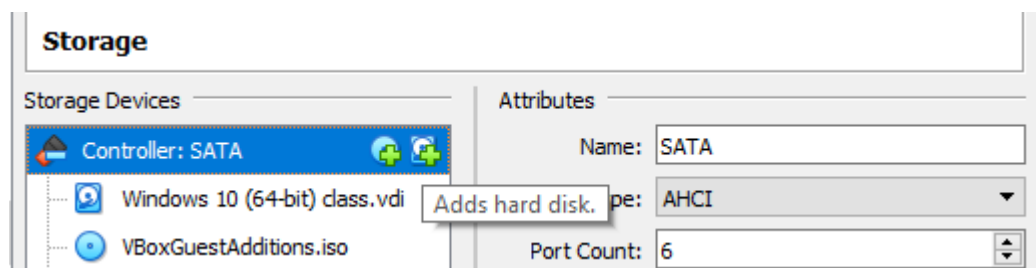
-Verify if the profile folder now exists

As we are logged in as the Class_1 user, we are not the administrator anymore and we don't have access to open the folder. But as you can see in the image below, it does recognize the user folder.

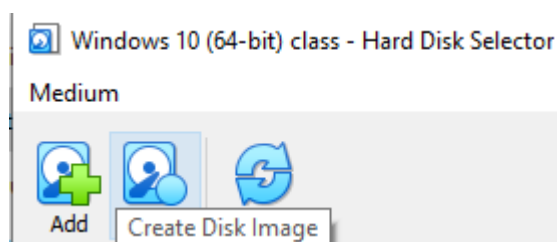


-Add a second hard drive to the virtual machine and create a folder called “My Documents” in F:

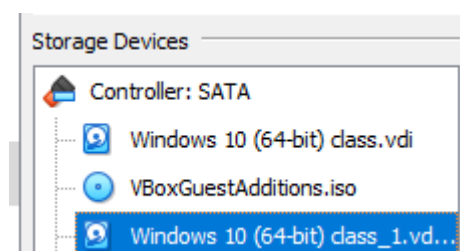
For this, we will need to shut down the virtual machine and from the VirtualBox software we will be able to create a new hard drive.



By selecting the ‘adds hard disk’ option we will add a second hard drive to the virtual machine.

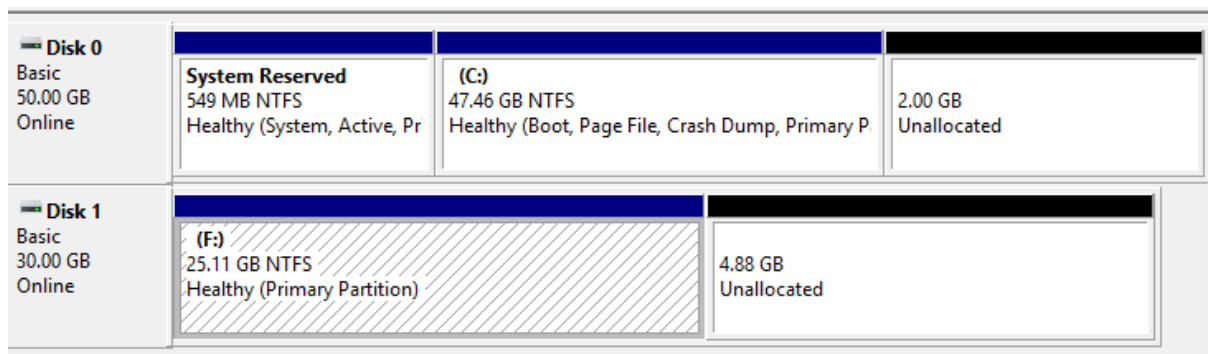
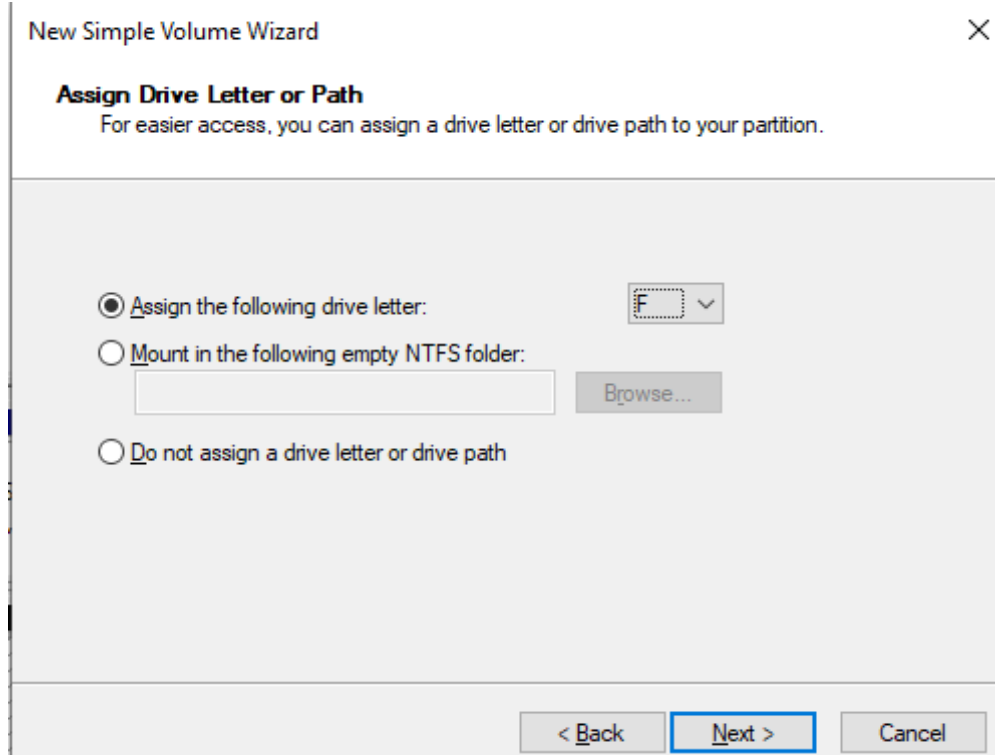
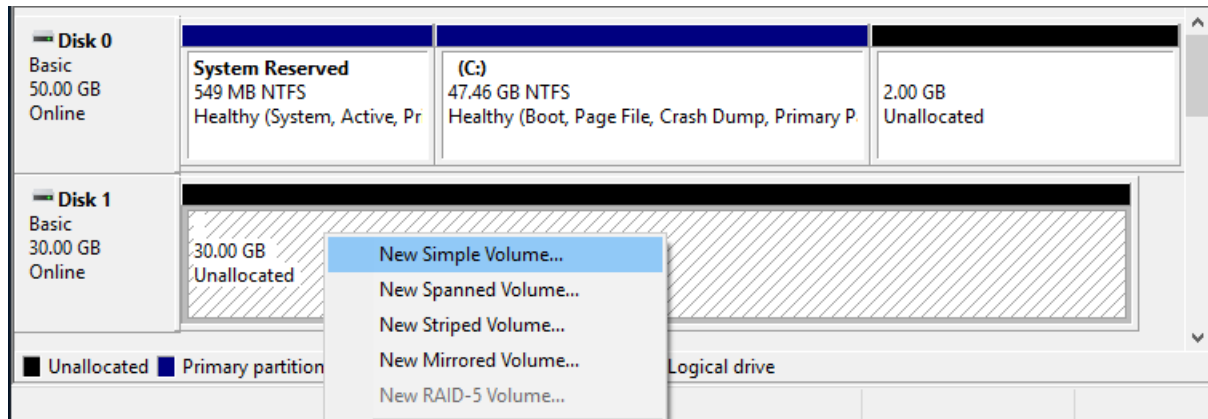


We will then proceed with the creation.

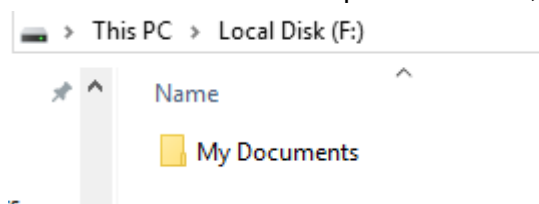


Finally we should have something like this.

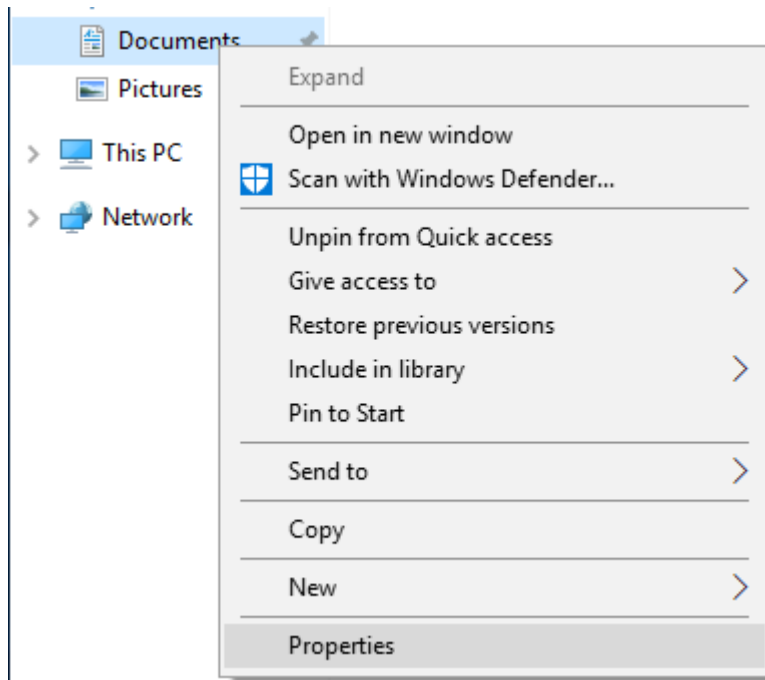
Now, in the virtual machine, we will create the disk partition 'F:'.



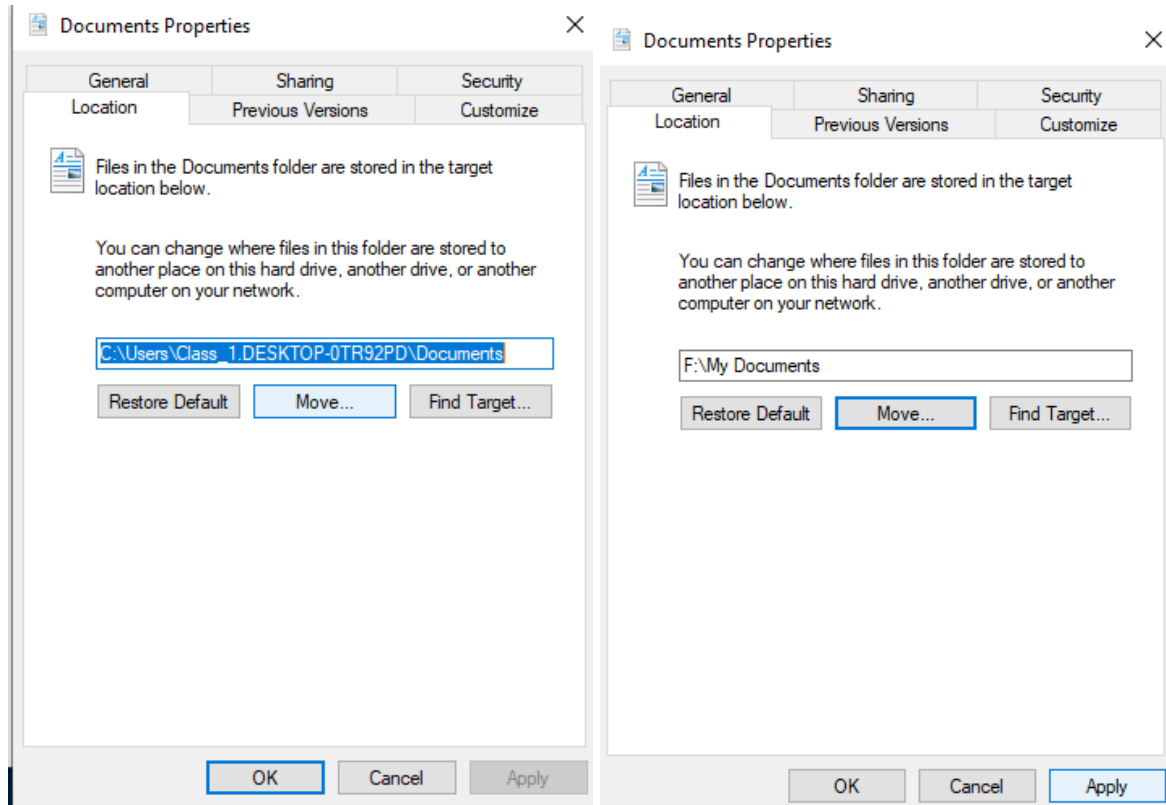
Now that we have our 'F:' partition made, we will create the 'My Documents' folder inside.



Move “**Class_1**” Documents folder to the directory you have just created.



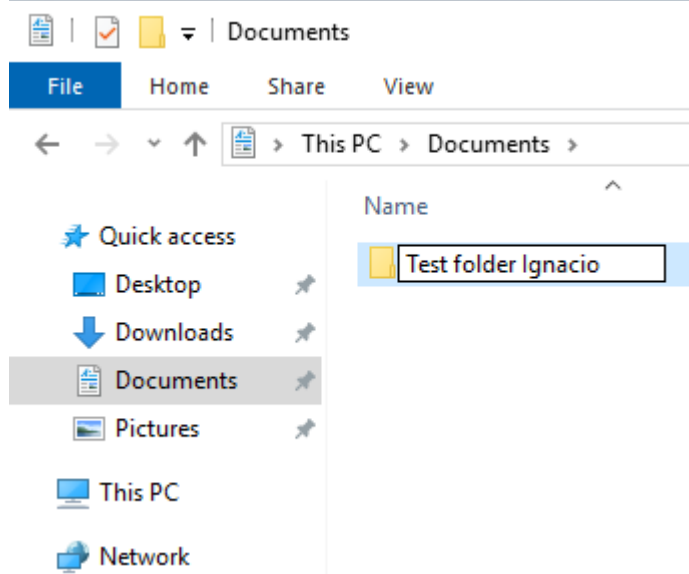
As the user ‘**Class_1**’ we will go to the **Documents** folder and select **Properties**.
Now we will go to the location tab and select the ‘**Move**’ option.



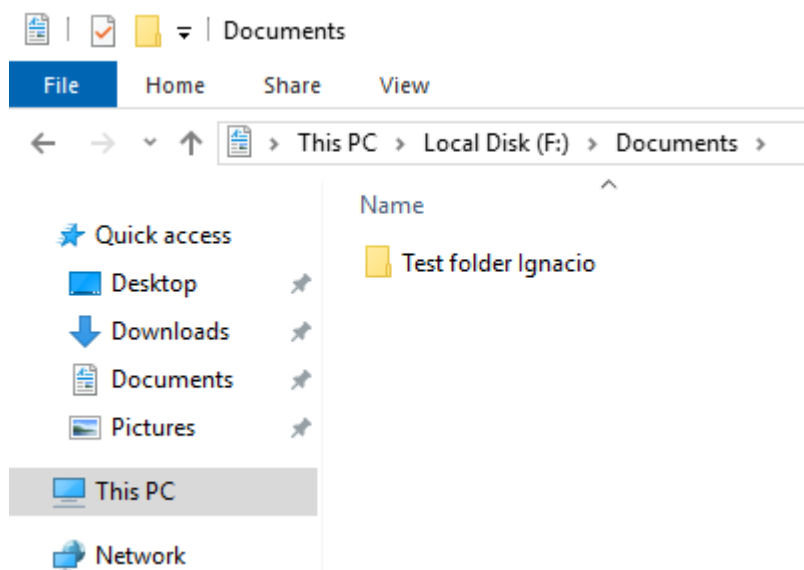
Now that we set the correct location, we will hit the ‘**Apply**’ option.

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

Now we will create a new folder in the Documents folder.

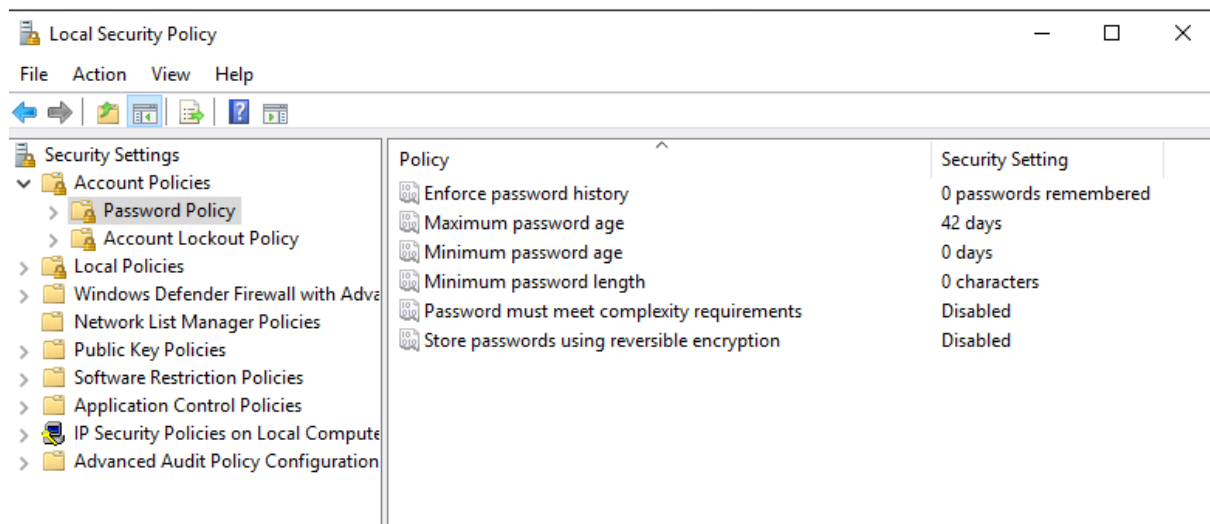


As you can see in the image below the test folder successfully created in the **F:\My Documents** directory.

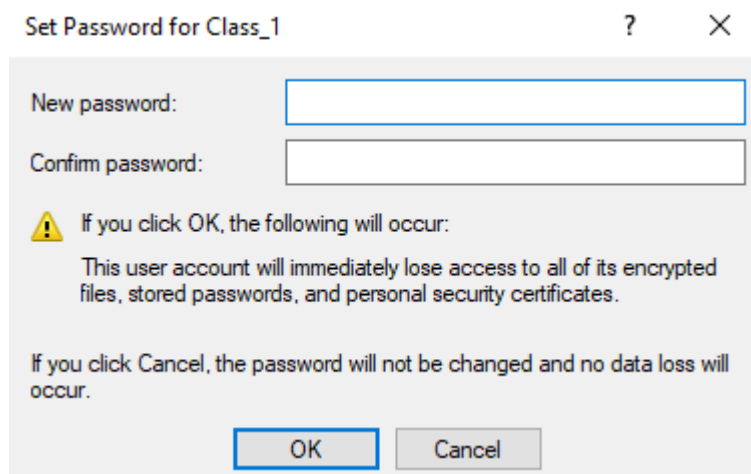


3. How do you configure a user to log in without a password and automatically when turning the computer on?

For this exercise we will need to go into the **Administrative tools** and select the **Local security policy** tab, then we will check that the **Minimum password age** says **0 days**, the **Minimum password length** says **0 chars** and the **Password must meet complexity requirements** is **disabled**.



Now we will go to the same tab as exercise one (**Computer Management**) and from there we will set the password of our user to 'blank'.



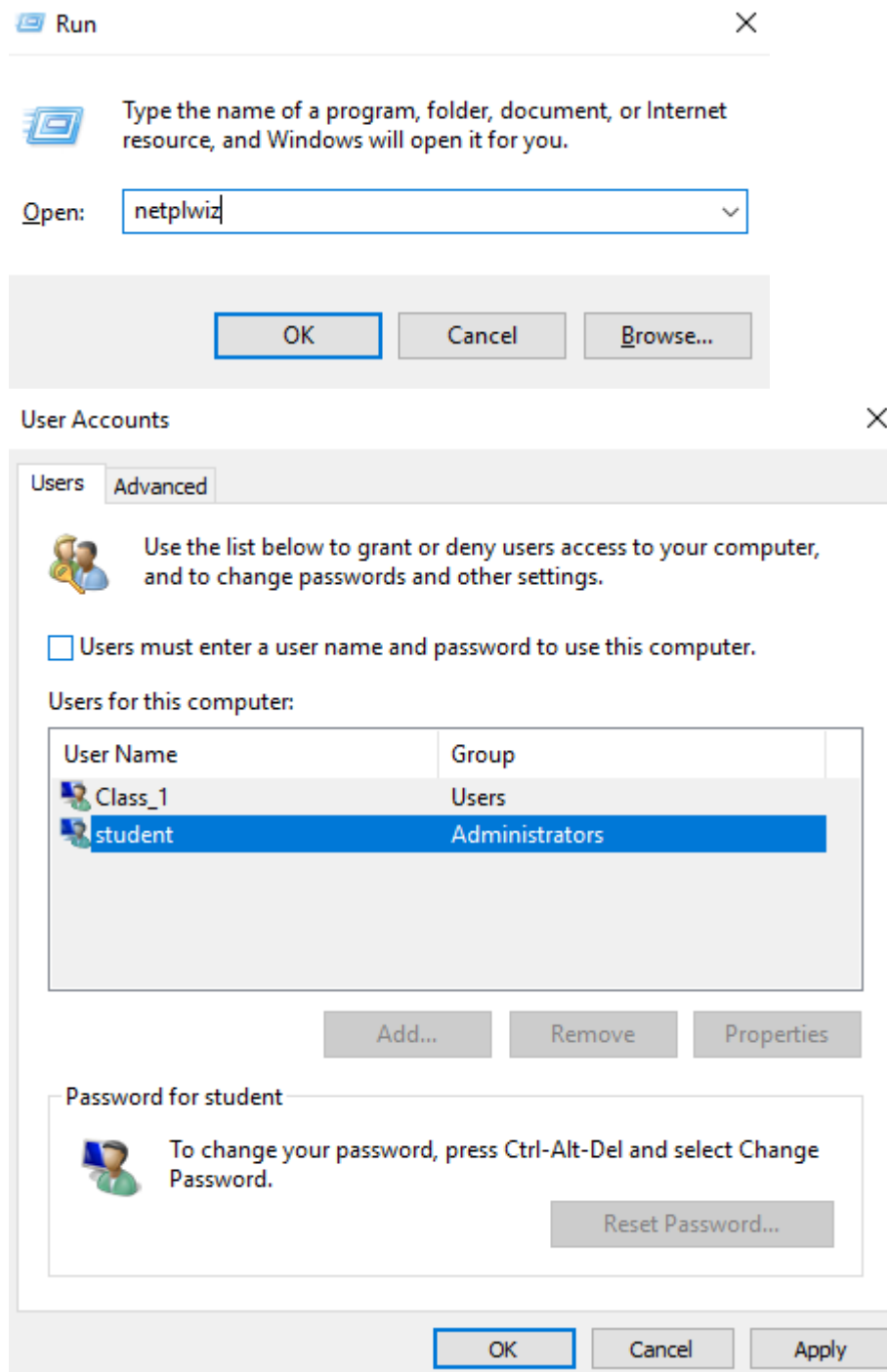
Local Users and Groups



The password has been set.

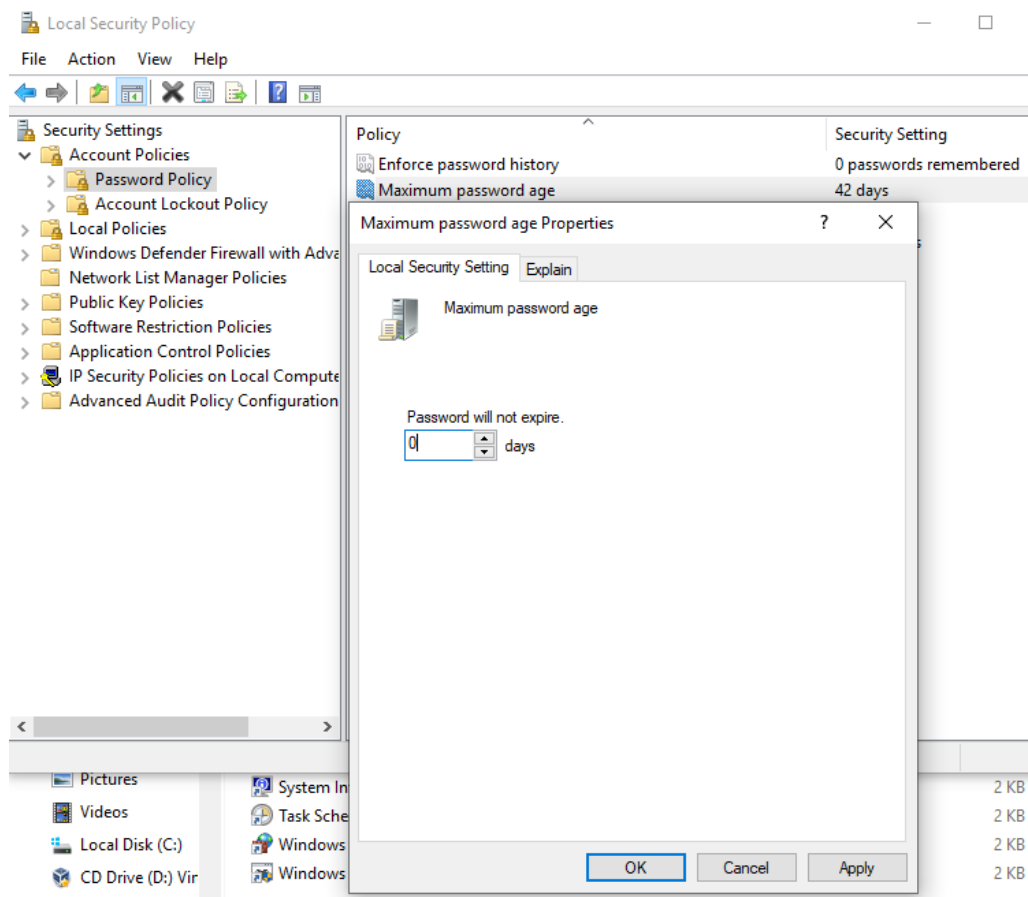
OK

Finally we will type 'netplwiz' in the alt+r tab in windows. This will open the User Accounts window in which we will disable the '**Users must enter a user name and password to use this computer**'.

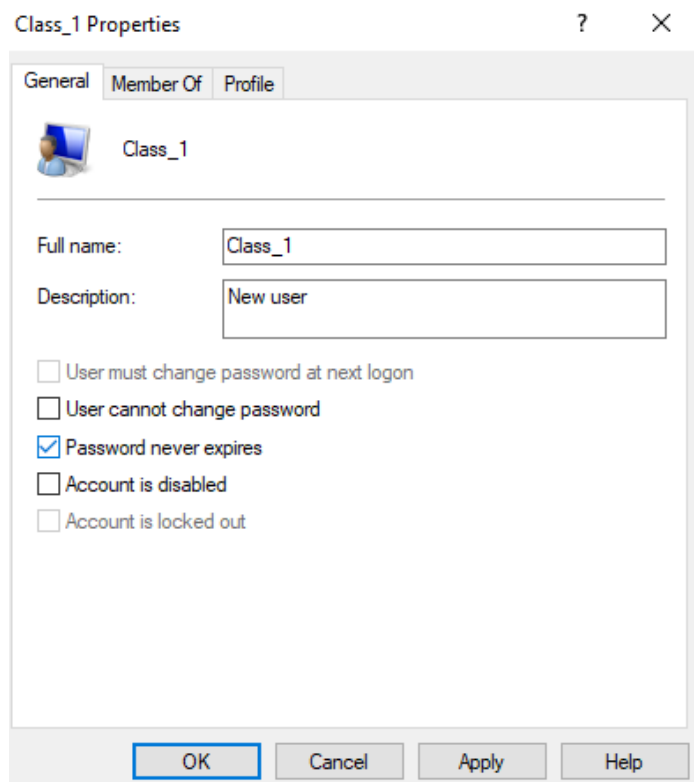


4. How do you configure a specific user so that the password never expires? How can you configure this policy for everyone?

If we want to configure the system so that the local password never expires, we will go to the Local security policies and then set the Maximum password age to '0'.



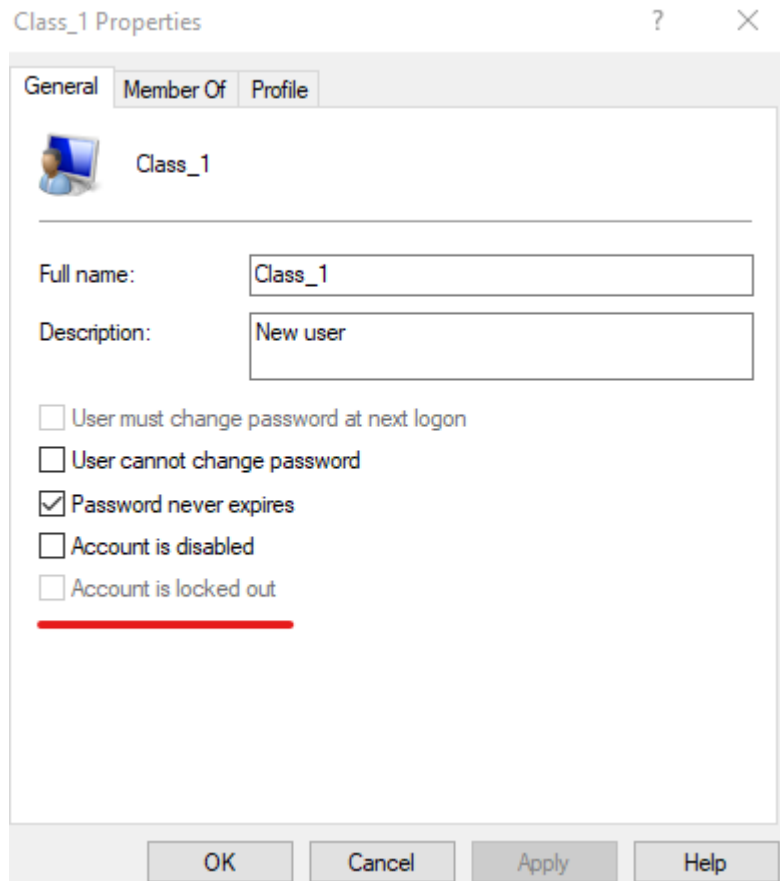
Finally from the **Computer Management** tab we can set that the **password never expires** in the user properties., which will only affect specific users.



5. When can you use a locked account?

You will be able to use the locked account when the lockdown is over.

Also, the administrator will be able to unlock the account from the **Computer Management** tab when the properties of said user are accessed.



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 the “Account lockout threshold” value were 0?

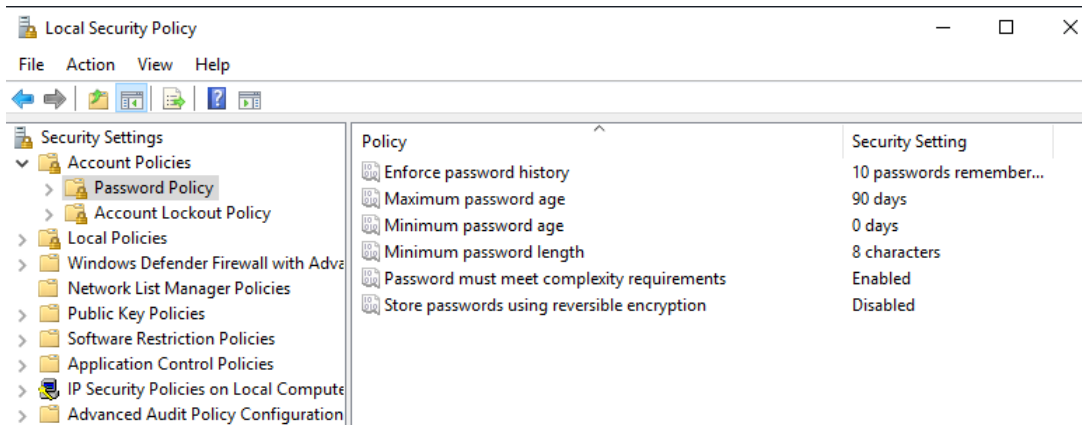
The valid values of ‘Reset account lockout counter after’ will be the inferior or equal to the ones in ‘Account lockout duration’.

If the ‘Account lockout threshold’ value were 0 you would not be able to set the other policies as the account cannot be locked.

7. Configure the system according to the following criteria:

- **All the passwords must have at least 8 characters.**
- **All the passwords must contain uppercase, lowercase, numbers and non-alphanumeric characters.**
- **The system stores the last 10 passwords for each user.**
- **All the passwords expire after 3 months**

To insert this type of settings we will need to go into the **Local Security Policy** tab.



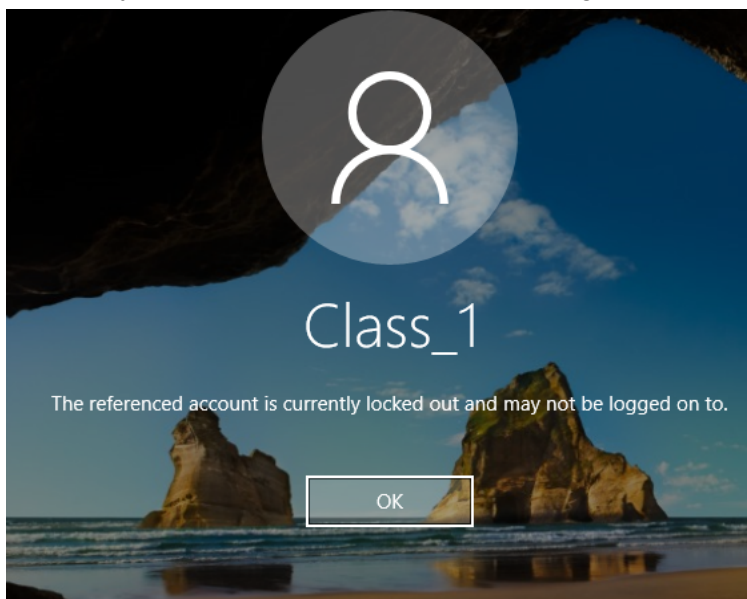
8. Configure the user “Class_1” to be locked after 3 invalid logon attempts. If the user is locked out, it will be able to type the password again in 5 minutes. Complete the following steps:

- **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.**

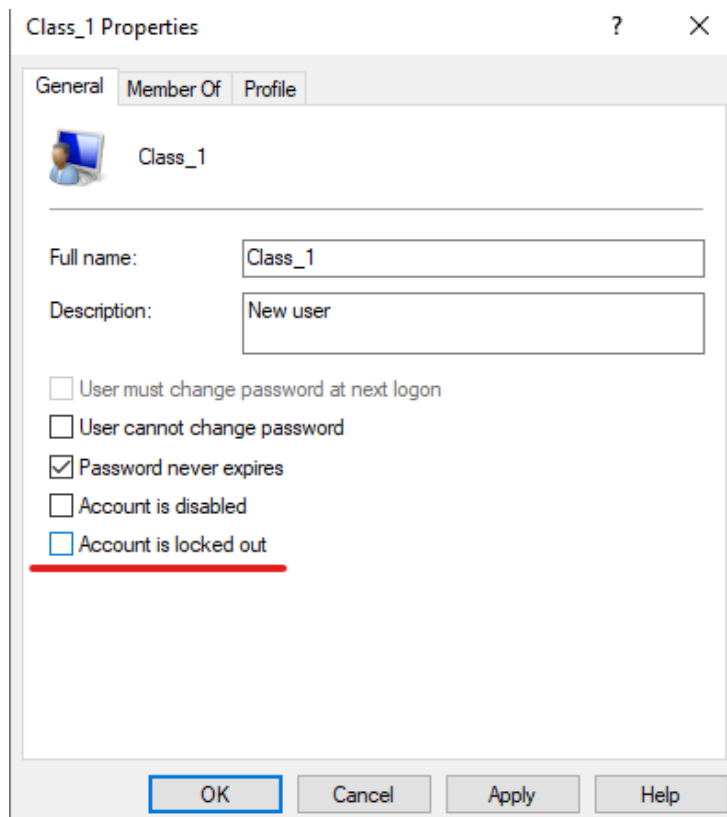
From the ‘**Account Lockout Policy**’ tab we will be able to change the setting to those asked.

Policy	Security Setting
Account lockout duration	5 minutes
Account lockout threshold	3 invalid logon attempt
Reset account lockout counter after	5 minutes

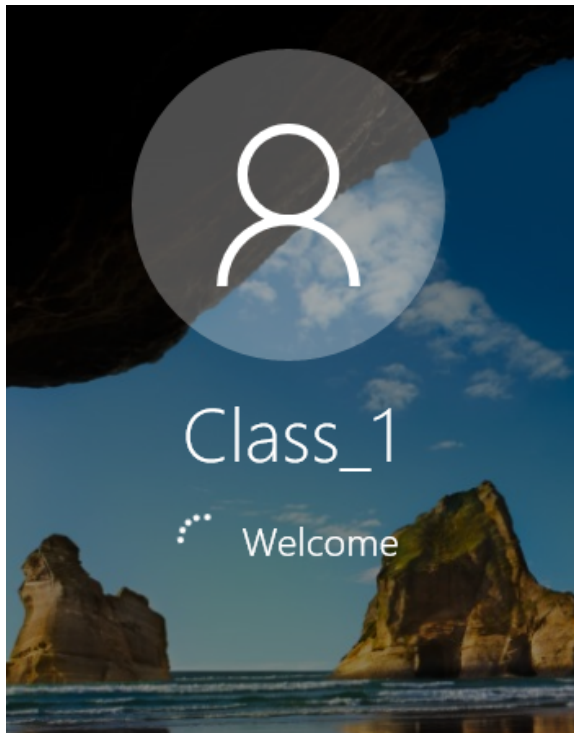
Next, In order to lock the **Class_1** user we need to type anything except the password we previously set a total of 3 times before locking out.



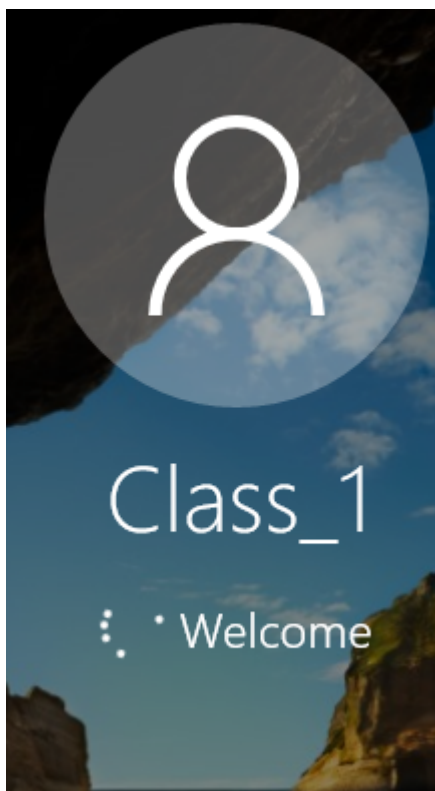
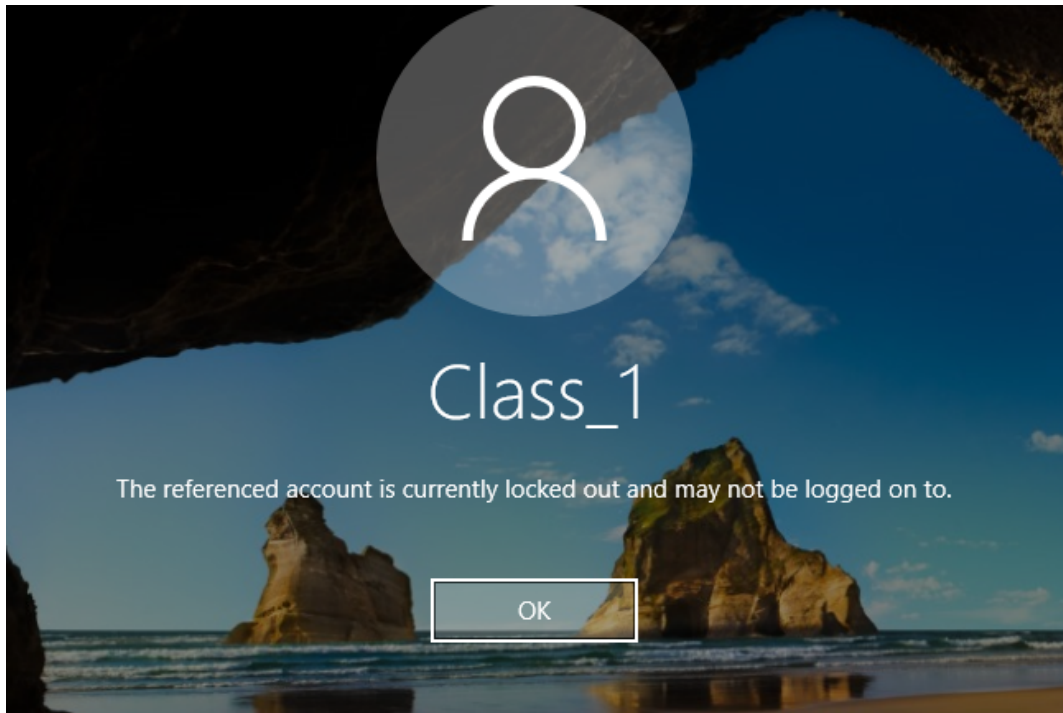
Now we will sign in as the administrator user and go to the **Computer Management** tab. Then we will go to the user Class_1 properties and disable the '**Account is locked out**' option.



As you can see in the image below, the **Class_1** user has been unlocked and is able to be logged into again if we type the correct password.



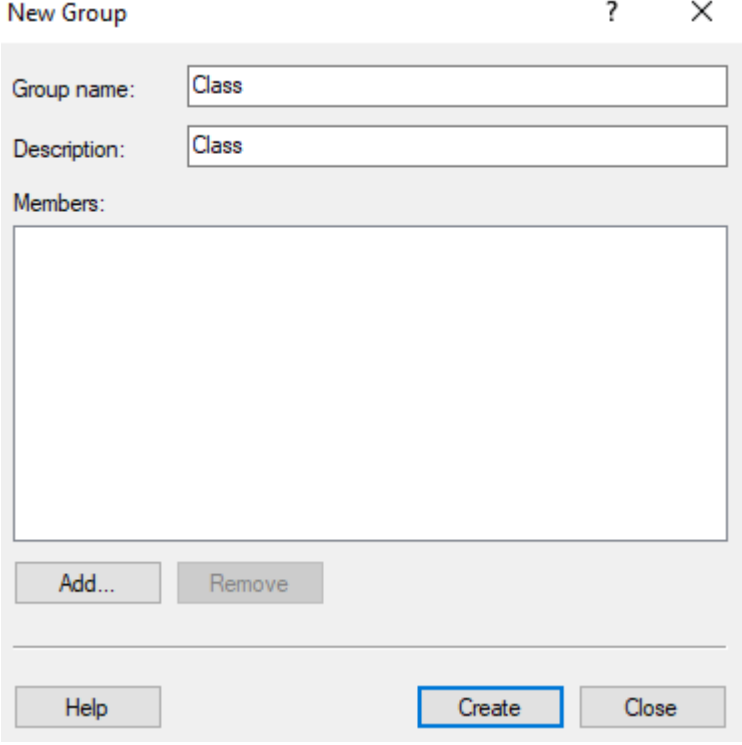
If we lock the **Class_1** user again and **wait 5 minutes**, we will be able to sign in again as 3 minutes is the account lockout duration.



9. Add a new group name “Class” and complete the following:

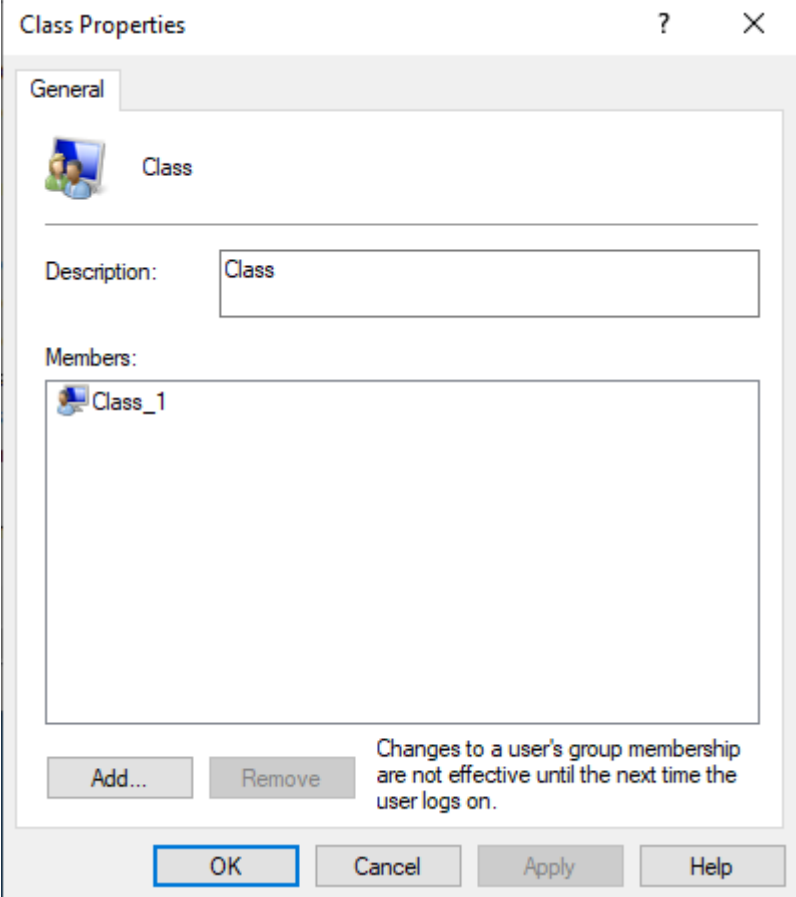
- Add the user “Class_1” to the group “Class”.
- Create a guest user called “Class_2”, initially disabled that cannot change the password. Then, add the user to “Class”.

To create a new group we will go to the **Computer Management** tab and select '**create group**' by hitting right click on the '**Groups**' folder:



The 'New Group' dialog box is shown. It has a title bar with a question mark and a close button. The 'Group name' field contains 'Class'. The 'Description' field contains 'Class'. Below these is a 'Members' list box, which is currently empty. At the bottom of the list box are 'Add...' and 'Remove' buttons. At the bottom of the dialog are 'Help', 'Create' (highlighted with a blue border), and 'Close' buttons.

Now we go into the group folder and select the **Class** group. Then we will be able to add any user to the group by hitting the '**add**' button.



The 'Class Properties' dialog box is shown. It has a title bar with a question mark and a close button. The 'General' tab is selected. The 'Class' icon is shown next to the group name 'Class'. The 'Description' field contains 'Class'. Below this is a 'Members' list box containing 'Class_1'. At the bottom of the list box are 'Add...' and 'Remove' buttons. A note at the bottom right of the list box states: 'Changes to a user's group membership are not effective until the next time the user logs on.' At the bottom of the dialog are 'OK' (highlighted with a blue border), 'Cancel', 'Apply', and 'Help' buttons.

To create another user we will go to the **Users** tab, right-click and hit the **new user** option. Then we will set that the **password never expires** as well as **disabling** the user.

New User ? X

User name:

Full name:

Description:

Password:

Confirm password:

☐ User must change password at next logon

☒ User cannot change password


☒ Password never expires

☒ Account is disabled

And finally we will add the user **Class_2** to the **Class** group.



Class Properties ? X

General

 Class

Description:

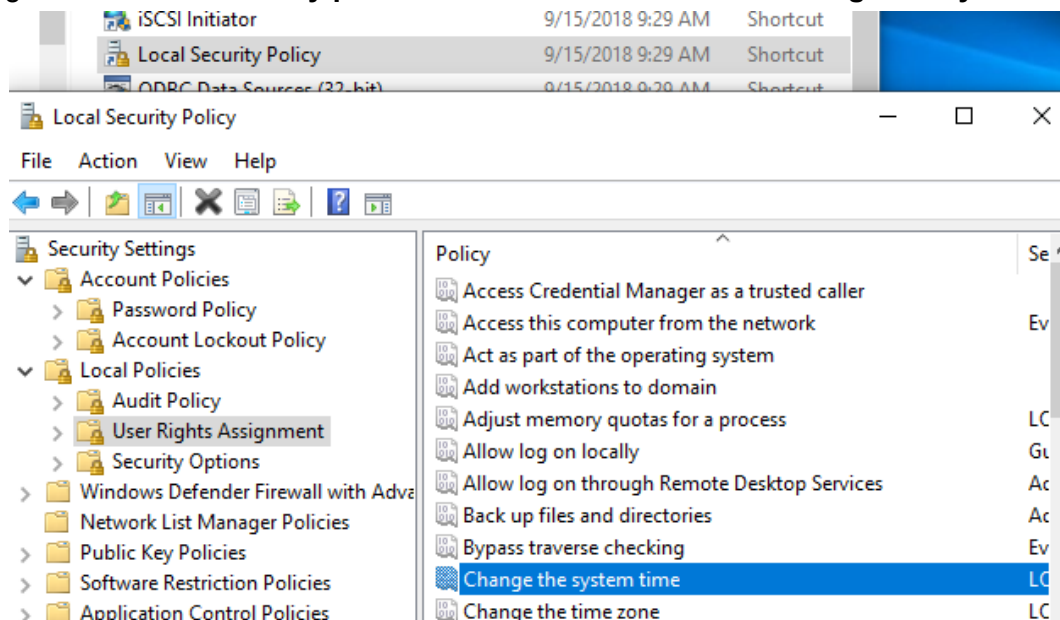
Members:

 Class_1
 Class_2

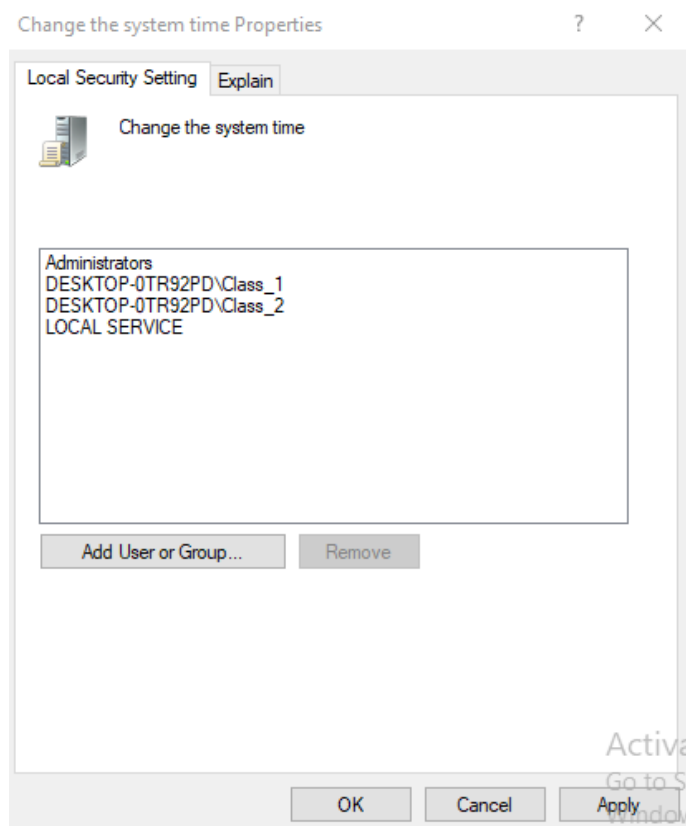
Changes to a user's group membership are not effective until the next time the user logs on.

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

If we want to modify the user rights so the user can change the system time you will need to go to the **Local security policies tab**. Then we will hit the ‘**Change the system time**’ tab.

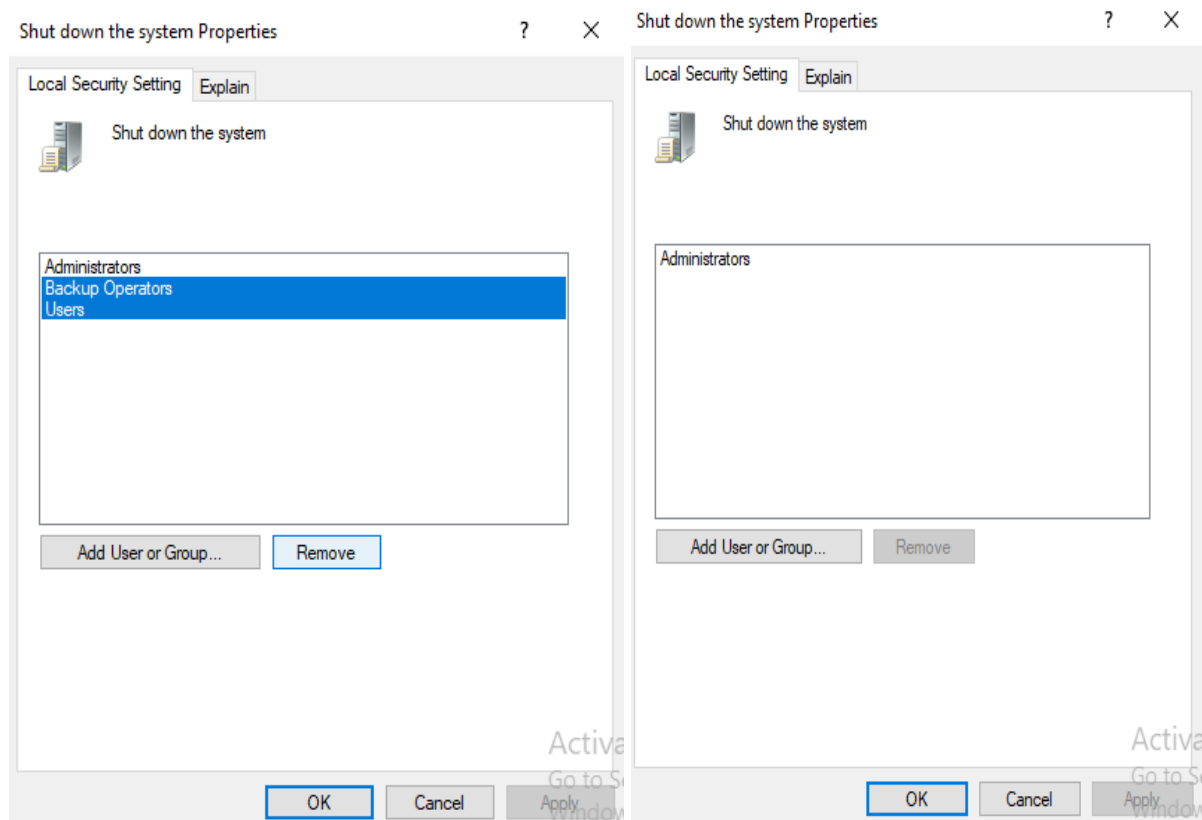


Now we will add the users Class_1 and Class_2.



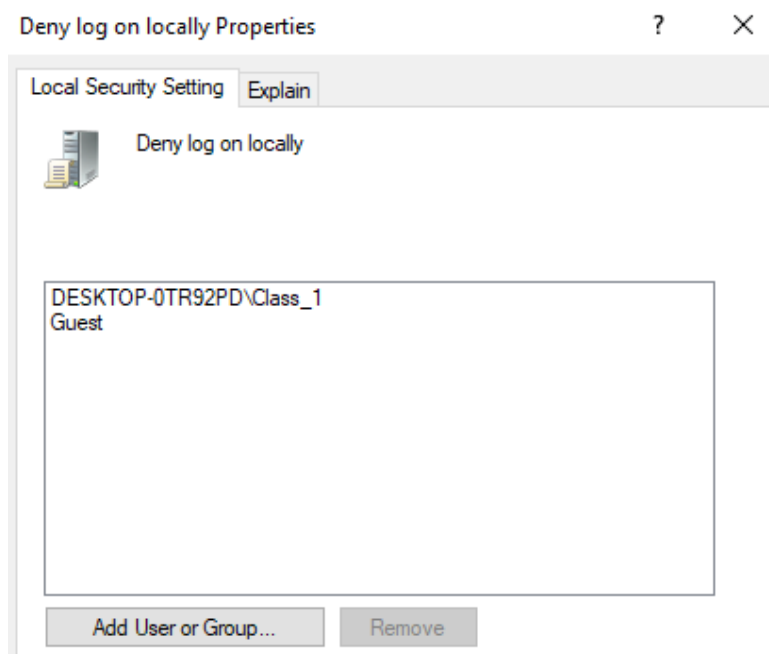
11. Modify the user rights so that only the administrator users can “Shut down the system”.

To modify the users so that only the **admin** can **shut down** we will need to go to the **Local security** tab and select the ‘**Shut down the system Properties**’ tab in the ‘**User right assignments**’ folder. From here, we will remove everything except the administrator.



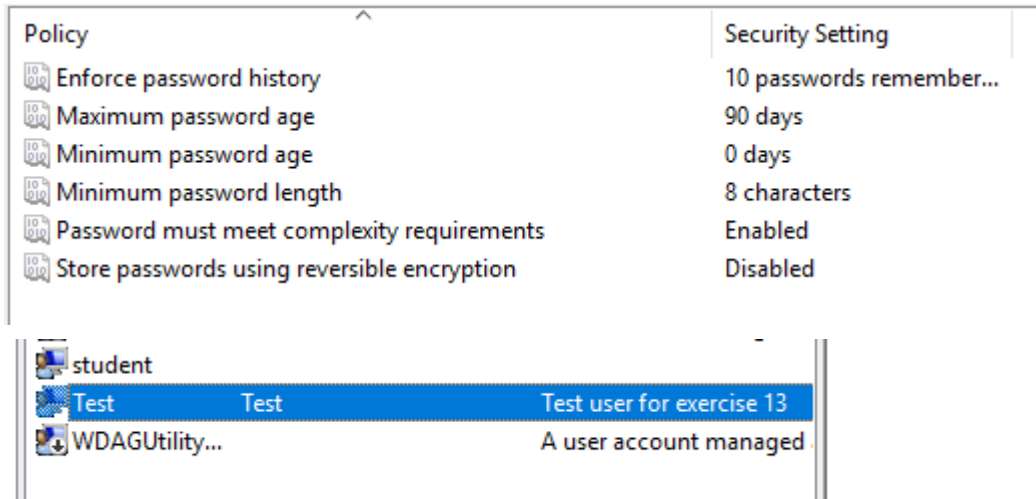
12. Suppose all the standard users are able to log in. How can we deny log on to the specific user “Class_1”?

To **deny log on** to **Class_1** we will need to go to the ‘**User Right Assignment**’ inside the **Local Security Policy** tab and find the ‘**Deny log on locally**’ setting. From here we will simply add the user **Class_1** to the list.



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.

First we will need to create the ‘**Test**’ user according to the policies of exercise 7.



Then we will go to the **Groups** and select **Users**. From here we will be able to **remove** the **Test** user. As you can see in the image below, you cannot log in the **Test** user as the system does not recognize it anymore.

