

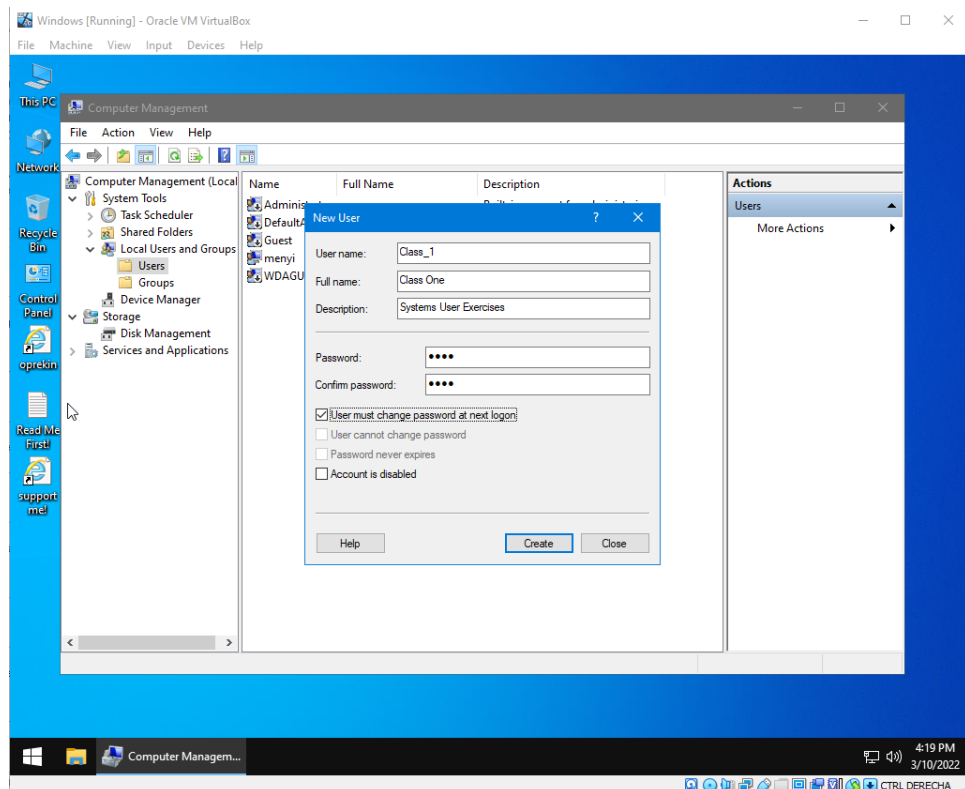
UNIT 07: Users, groups and local policies Exercises

1. Add a new standard user named "Class_1" including the description and full name.

The user must change the password at next logon.

A new user is "standard" by default and automatically belongs to "Users" group.

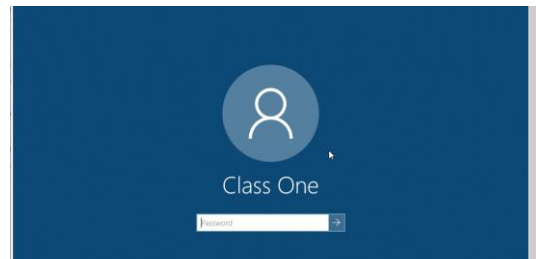
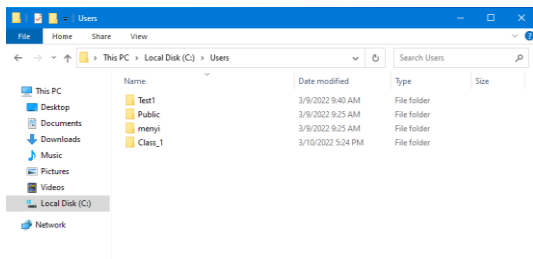
To upgrade to Administrator, first remove from "Users" and then add to "Administrators"



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

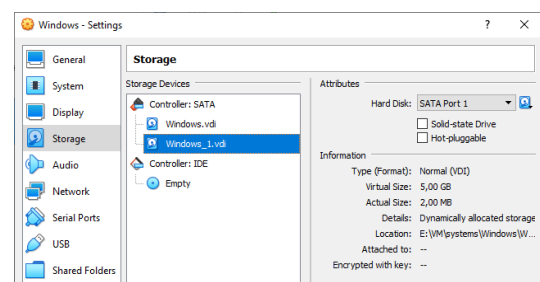
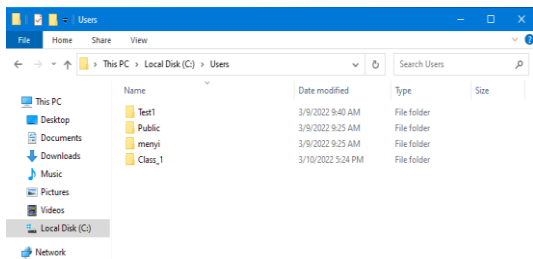
Verify if the profile folder exists. > **It doesn't exist because the profile folder is created once login**

Log in as "Class_1" > **Class One**



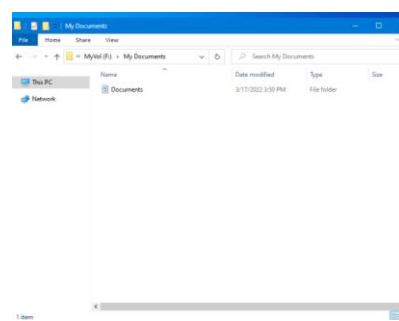
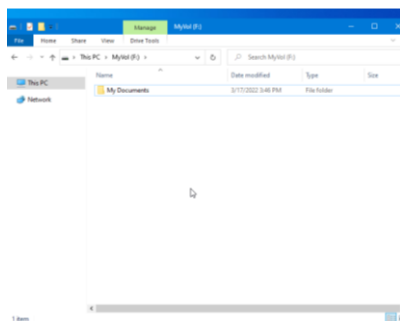
Verify if the profile folder now exists.

Add a second hard drive to the virtual machine



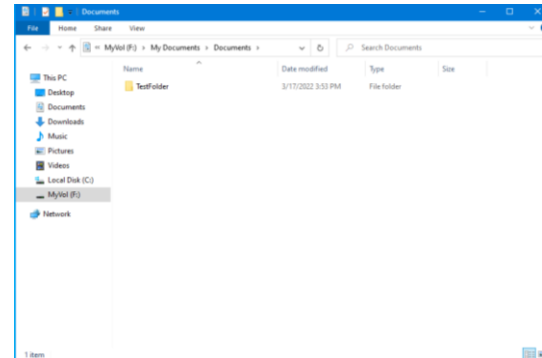
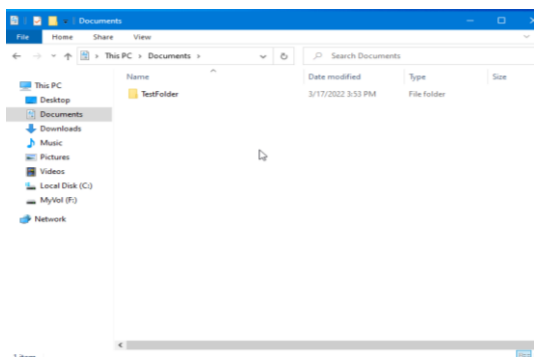
Create a folder called "My Documents" in F:\

Move "Class_1" Documents to My Documents



Open "Documents" shortcut and create a new folder

Check if this folder has actually been created in "F:\My Documents"

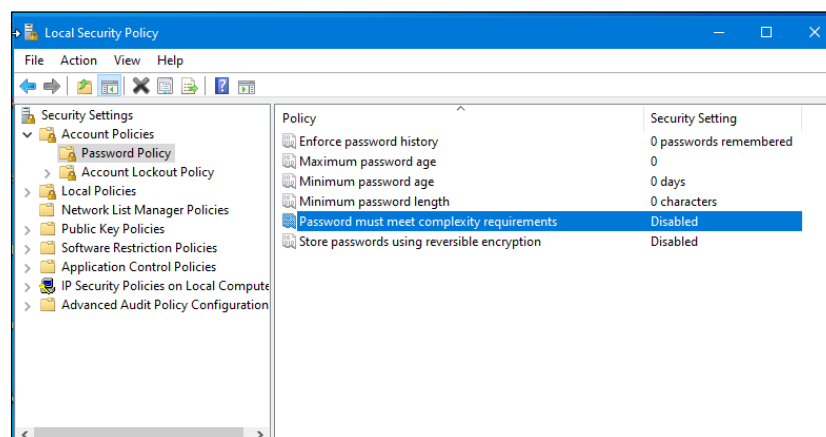


3. How do you configure a user to log in without a password and automatically when turning the computer on?

First, change password settings as indicated from

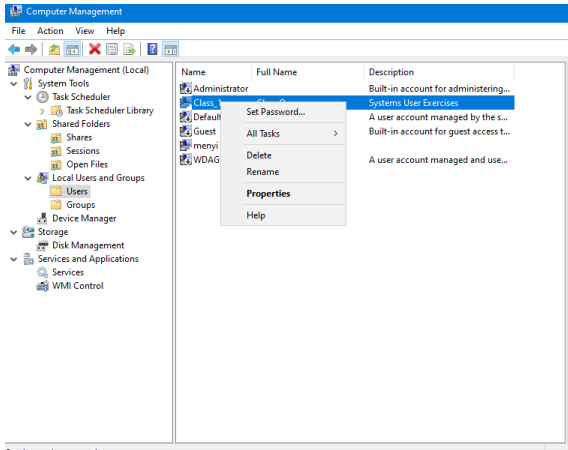
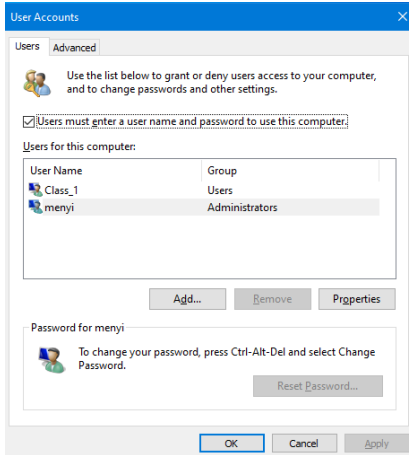
Administrative Tools > Local Security Policy > Account Policies > Password Policy

- Minimum password age = 0 days
- Minimum password length = 0 characters.
- Password must meet complexity requirements = Disabled



Then, set up an empty password from Computer Management and finally unset “Users must enter a user name and password to use this computer” from Users.

This way, a user can automatically log in without password

	
Local Users and Groups to change password	Open this window > Start > run > netplwiz

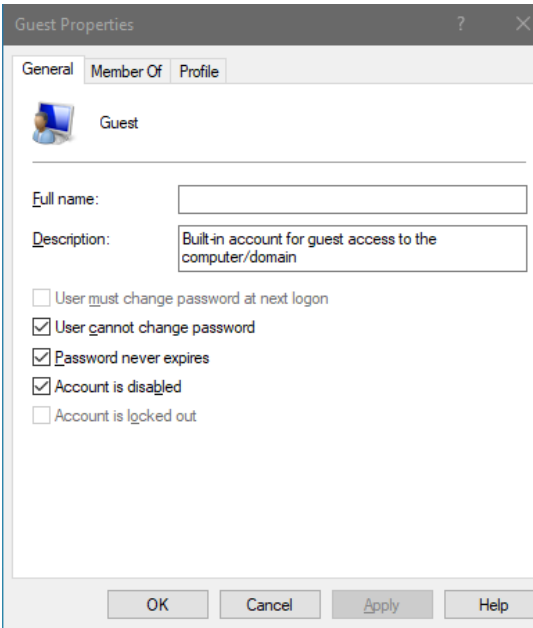
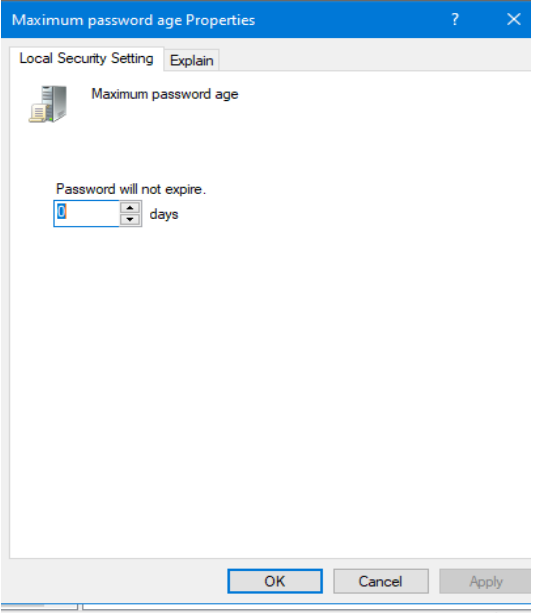
4. How do you configure a specific user so that the password never expires?

By setting the Maximum password age of the specified user to 0.

From Computer Management > User and Groups

How can you configure this policy for everyone?

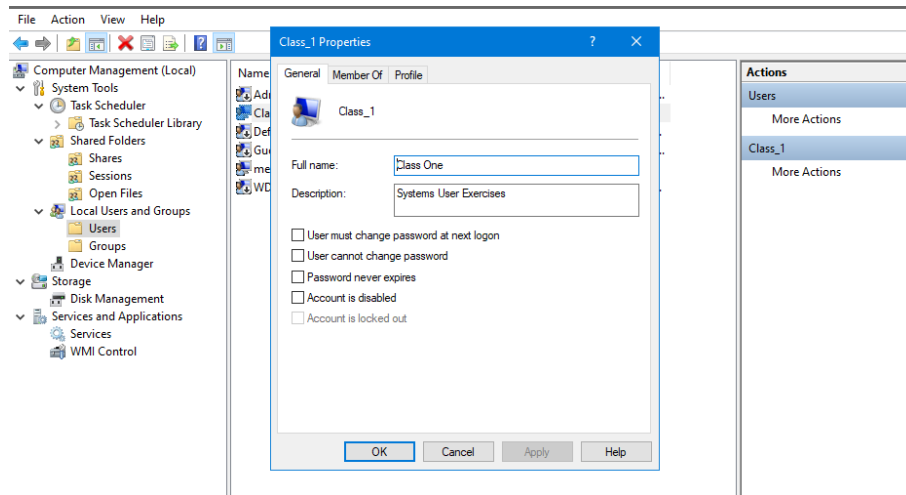
By setting Maximum password age parameter to 0 from Local security policies

	
---	--

5. When can you use a locked account?

Once the lockout duration has ended or the logon failed attempts are reset.

Also, the administrator is able to unlock the account from Computer Management, the corresponding checkbox will be automatically enabled when opening the window.



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 was 0?

Reset account lockout counter after must be less or equal to “Account lockout duration”

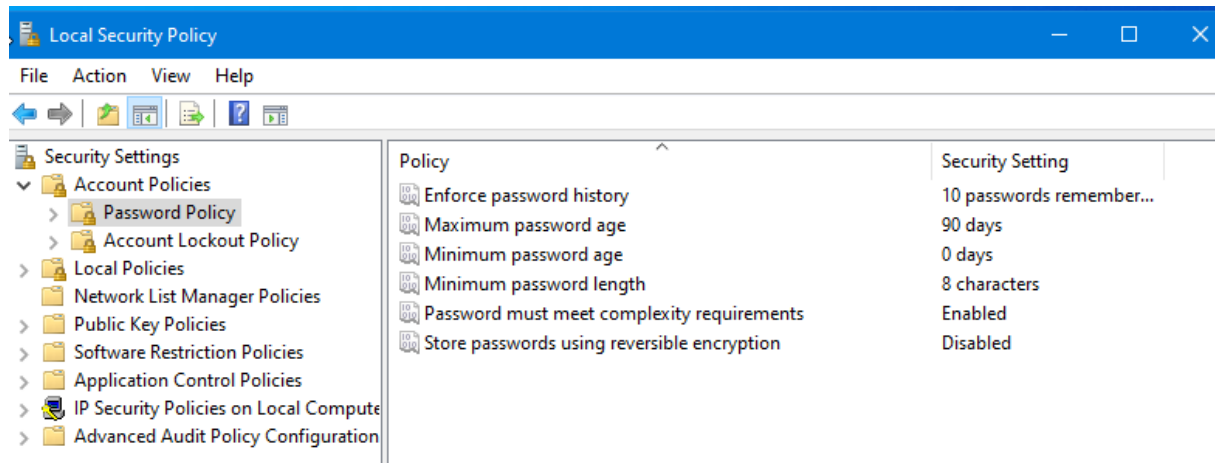
therefore you won't be able to set any other policy once

the “Account lockout threshold” has been set to 0

7. Configure the system according to the following criteria,

From Local Security Policy > Security Settings > Account Policy > Password Policy

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



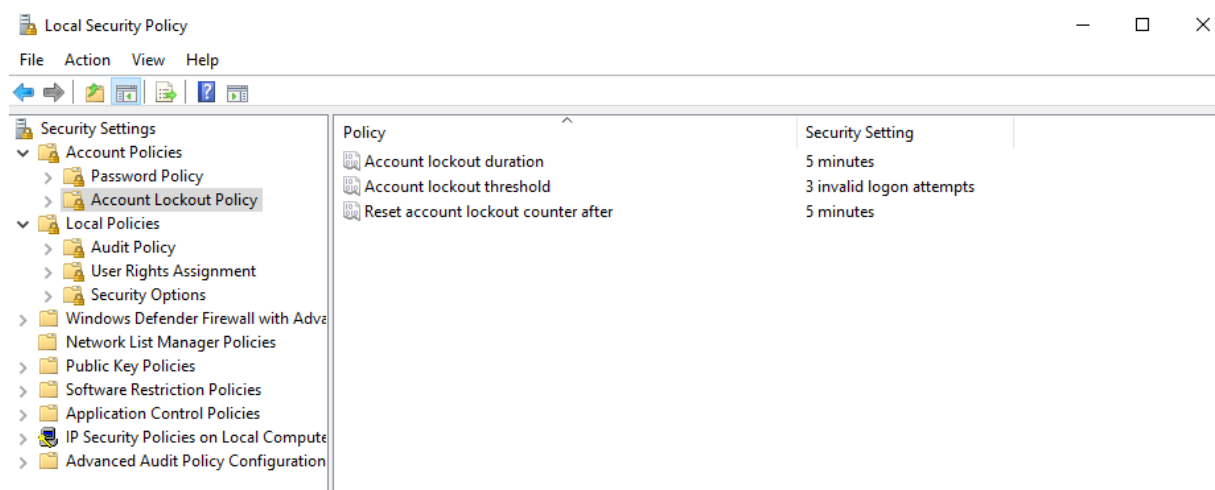
8. Configure the user "Class_1" to be locked after 3 invalid logon attempts.

If the user is locked out, it will be able to type the password again in 5 minutes.

Login as Class_1 > Run as Administrator Local Security Policy >

Security Settings > Account Policies > Account Lockout Policy

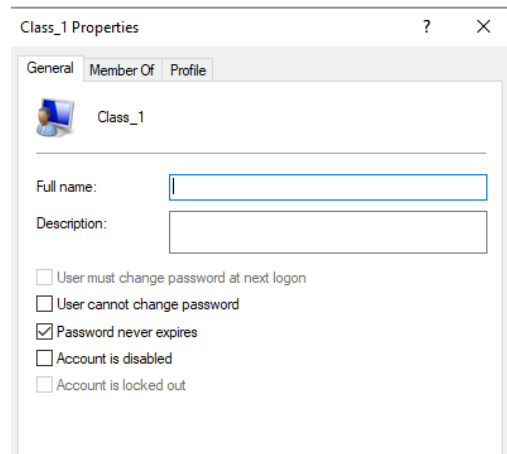
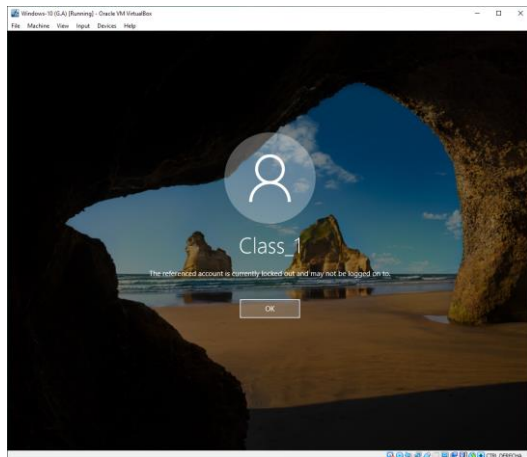
Set first "Account lockout threshold" then "Account lockout duration" also set "Reset account lockout counter", this reset time must be less than or equal to the "Account lockout duration"



Complete the following steps:

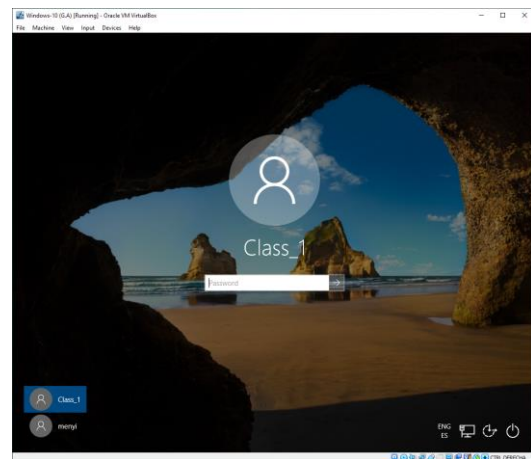
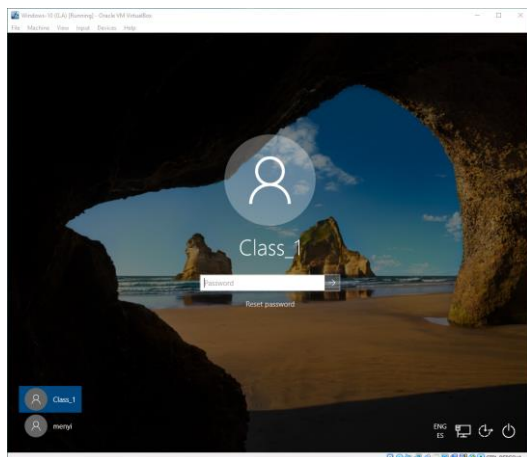
Lock the user

Unlock the user. Is the user able to log in? Yes



Lock the user again. Wait for 5 minutes

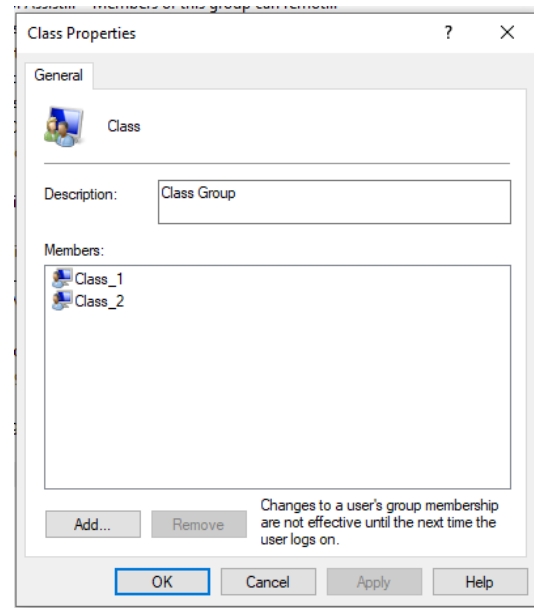
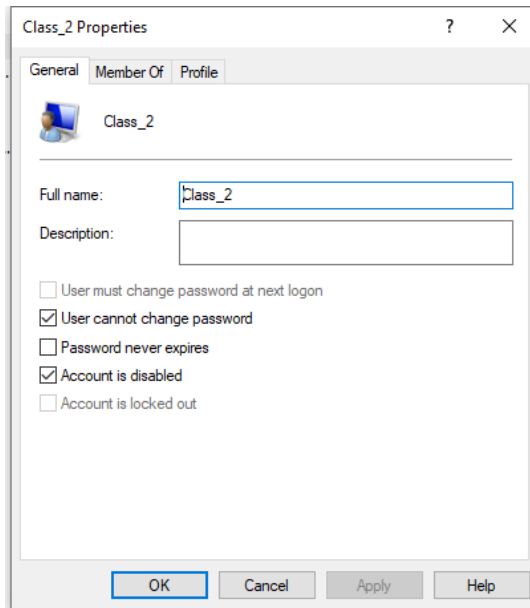
Enter password. Is the user able to log in? Yes



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

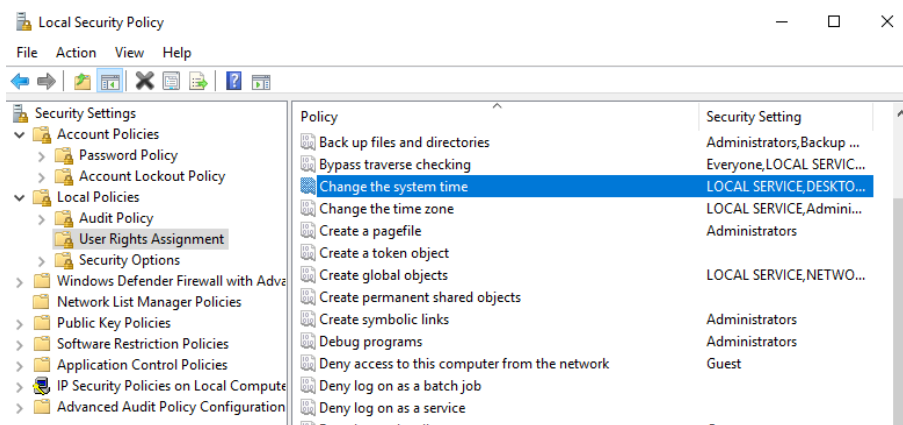
- a. Add the user "Class_1" to the group "Class"
- b. Create a guest user called "Class_2", initially disabled that cannot change the password.

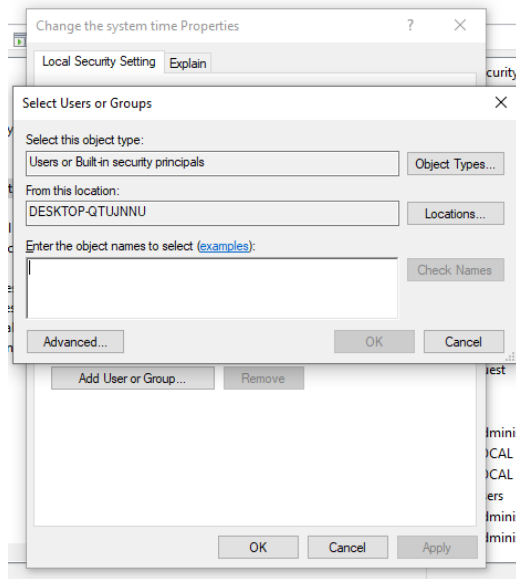
Then, add the user to "Class"



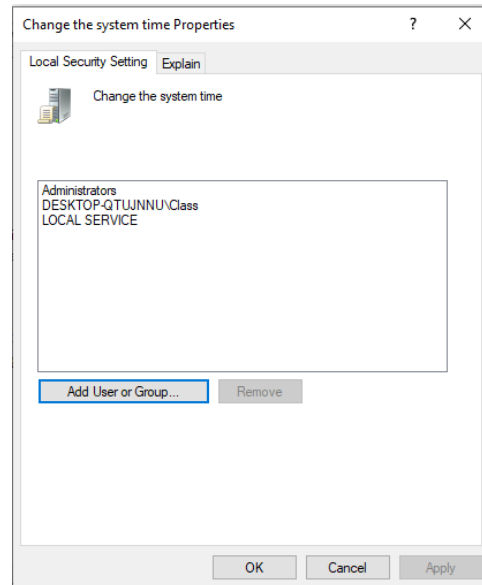
10. Modify the user rights so "Class_1" and "Class_2" will be able to "Change the system time"

From **Local Security Policy > Local Policy > User Rights Assignment > Change the System time**





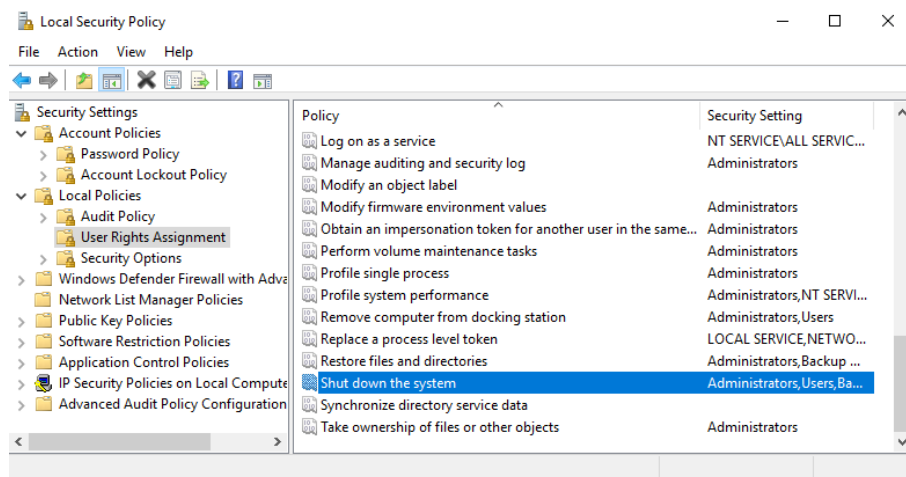
Add User or Group ...

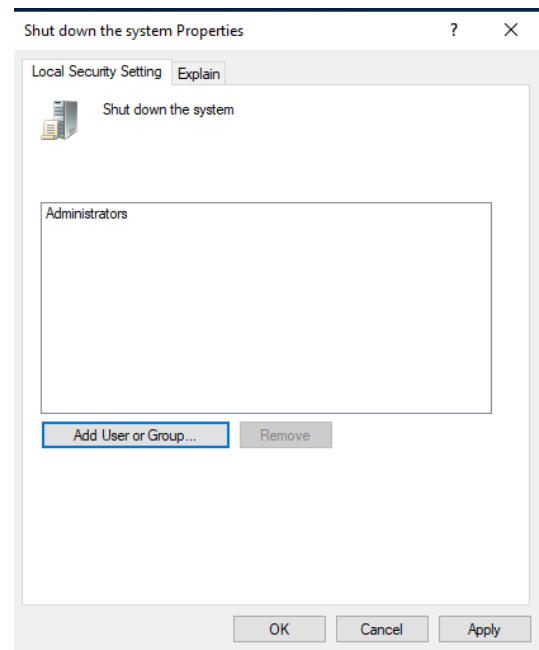
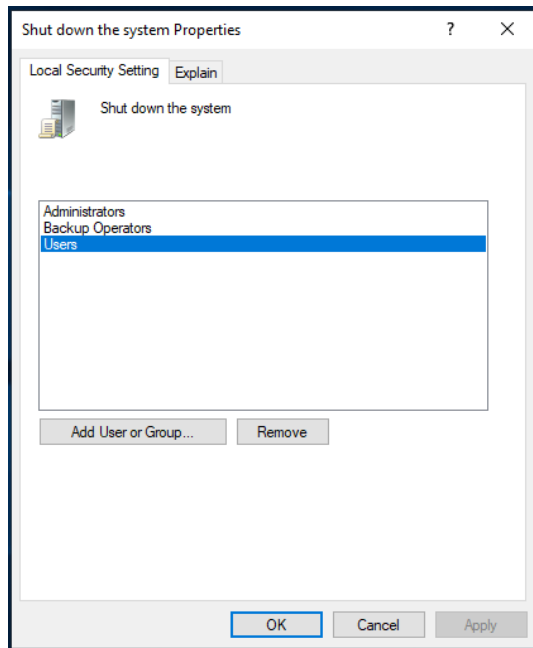


Select Class group or User one by one

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

From **Local Security Policy > Local Policy > User Rights Assignment > Shut down the system**





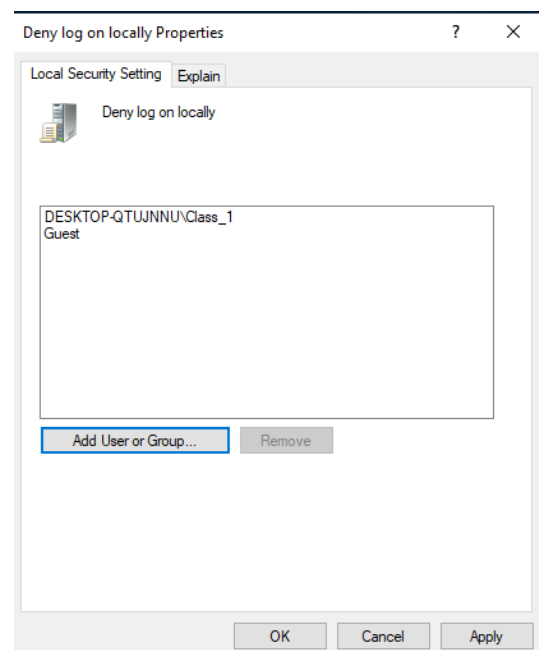
Remove all groups but Administrators

Only Administrators groups has permission

12. Suppose all the standard users are able to log in.

How can we deny log on to the specific user "Class_1"?

From **Local Security Policy > Local Policy > User Rights Assignment > Deny log on locally**

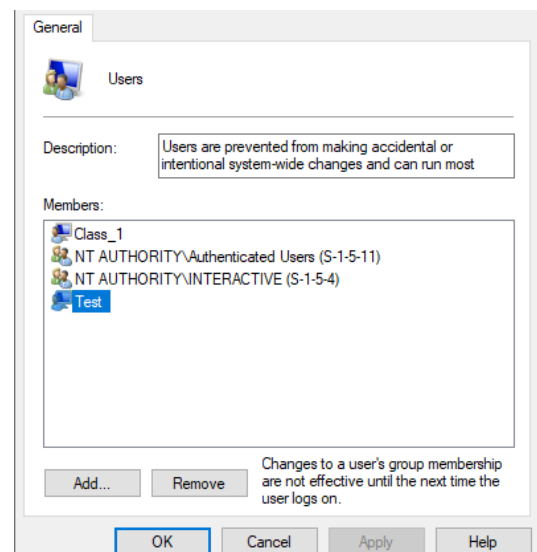
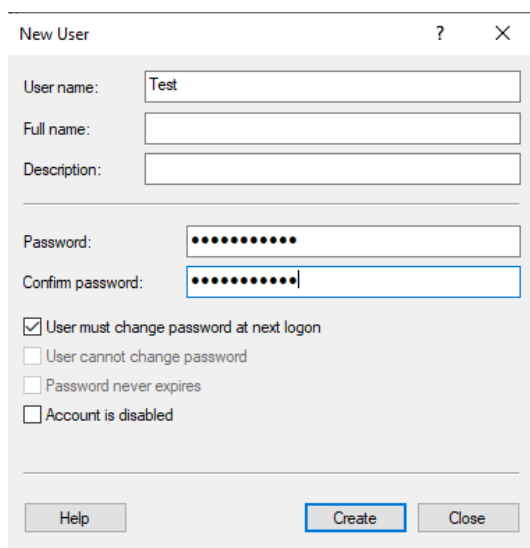
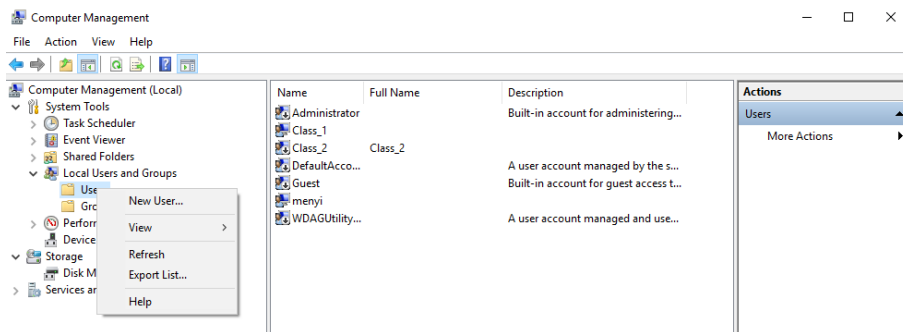


Add User Class_1

Guest group and Class_1 user are denied to log

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.

From **Computer Management > Local User and Groups > Users > New user**



New user

Remove Test from Users group

Test user is not be able to log in, because the Deny log on locally policy set before.
After removing, Test user doesn't belong to any group and therefore has no permission

