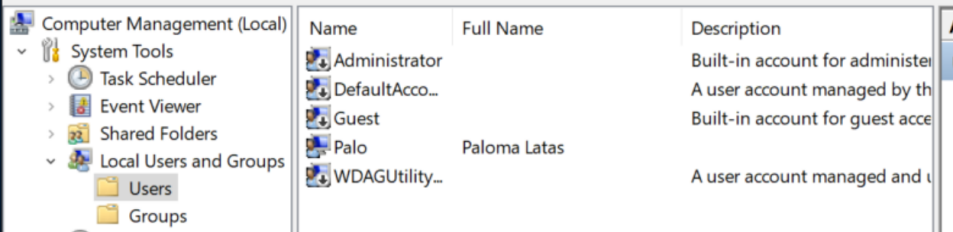
EXERCISES: Users, groups and local policies

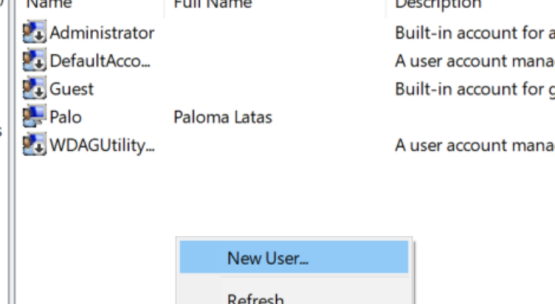
1. Add a new standard user named “Class\_1” including the description and full name.

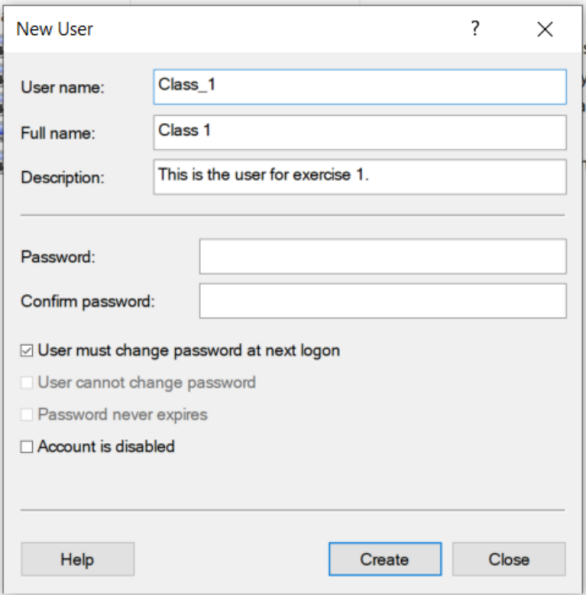
The user must change the password at next logon.

To create a new user we need to go to Computer Management>System Tools>Local users and Groups>Users



Here we right click where all the users are and we can add a new one.



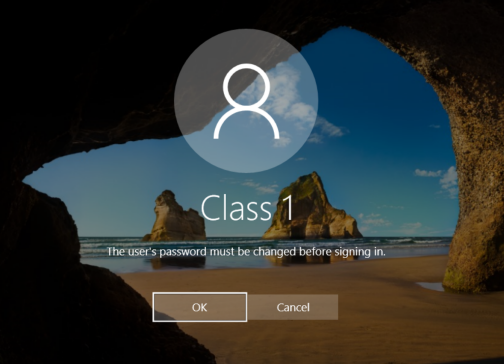


We make sure the box “user must change the password at next logon” is checked.

2. Complete the following parts about the user “Class\_1” from the previous exercise.

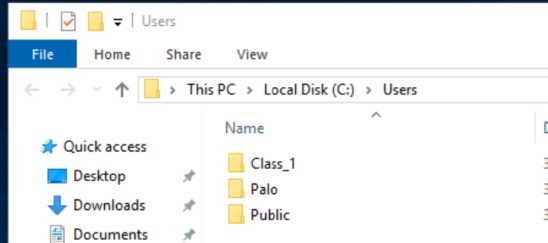
• Verify if the profile folder exists. Since we haven’t logged in as Class 1 yet the folder hasn’t been created yet.

• Log in as “Class\_1”.



• Verify if the profile folder now exists.

Now the folder exists. We can check in the users folder.



• Add a second hard drive to the virtual machine and create a folder called

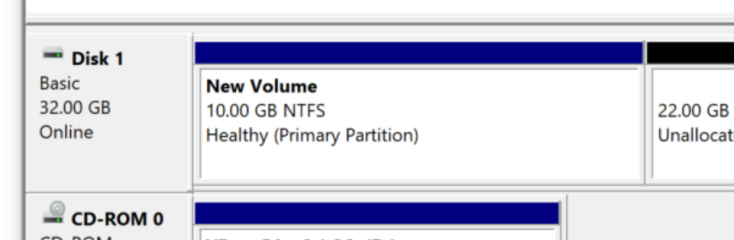
“My Documents” in F:\

• Move “Class\_1” Documents folder to the directory you have just created.

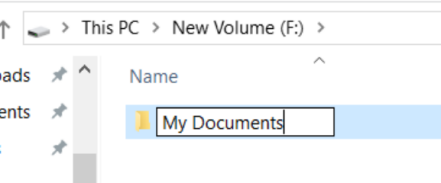
• Open “Documents” Short-cut and create a new folder. Check if this folder has

actually been created in “F:\My Documents”.

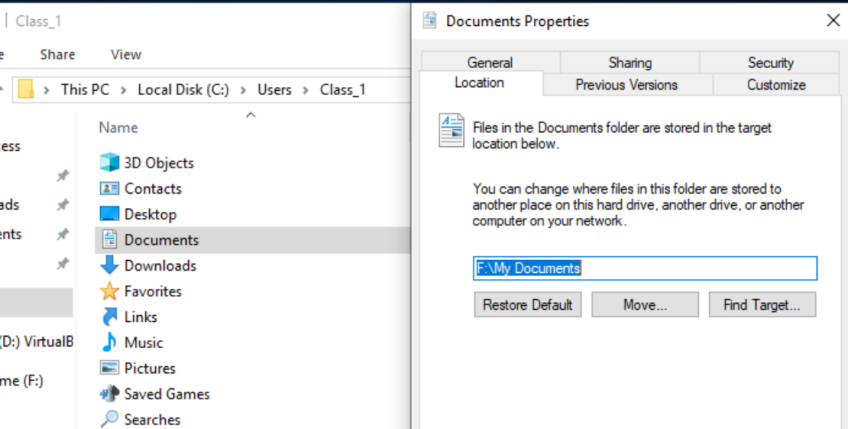
First we create the second volume.



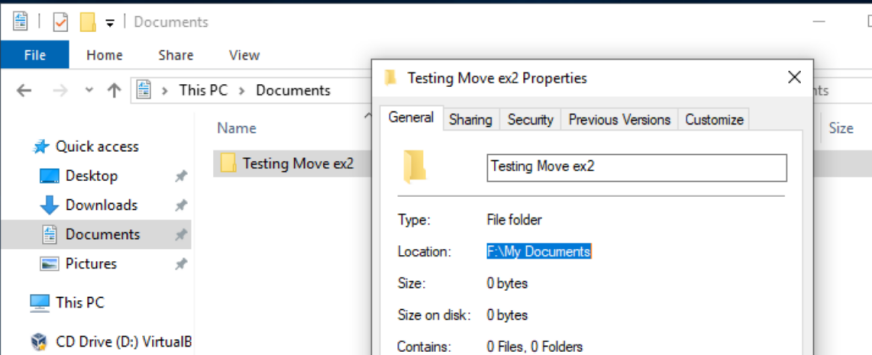
Now we create the folder “My documents” in F:\



We locate the Documents folder and click on its properties to change the location to F:\My Documents



To check that the changes are correct we create a new folder in documents and check that its location is F:\My Documents.



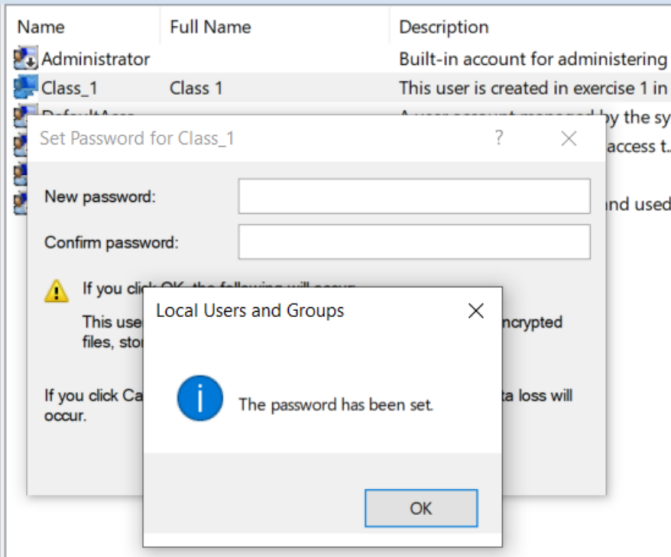
3. How do you configure a user to log in without a password and automatically when turning the computer on?

We need to check the minimum character length for a password in Local Security Policy window and there Local Securities > Account Policies> Password policy

There we can see that the minimum is 0 so that means there isn’t a password required.



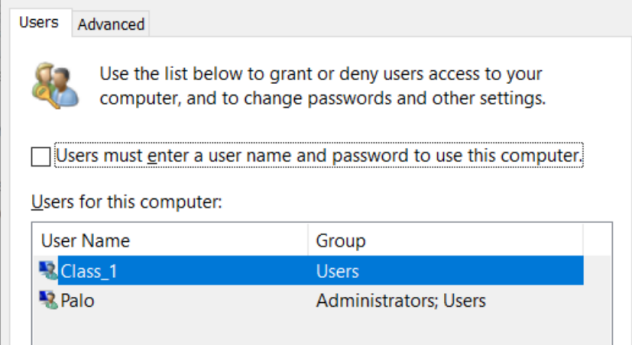
So now we can set the empty password for our user



Now we need to configure the automatic log in.

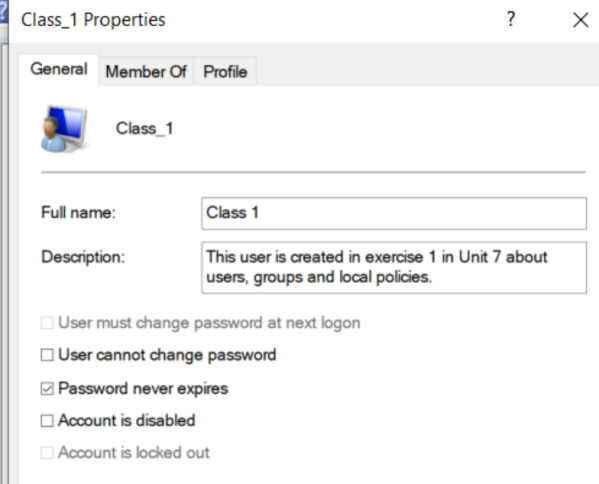
We do this using the command on the search bar.

This will open the following window in which we have to uncheck the box “Users must enter a user name and password to use this computer”

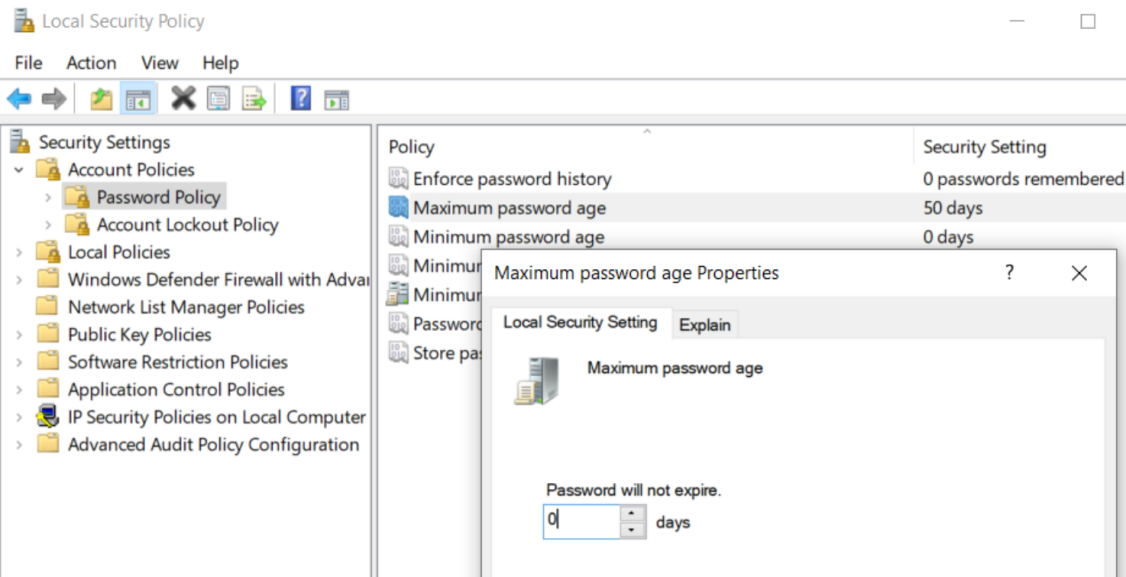


1. How do you configure a specific user so that the password never expires? How can you configure this policy for everyone?

On a specific user we only have to click on its properties, from the users and groups in the computer management menu, and check the box that says “password never expires”.

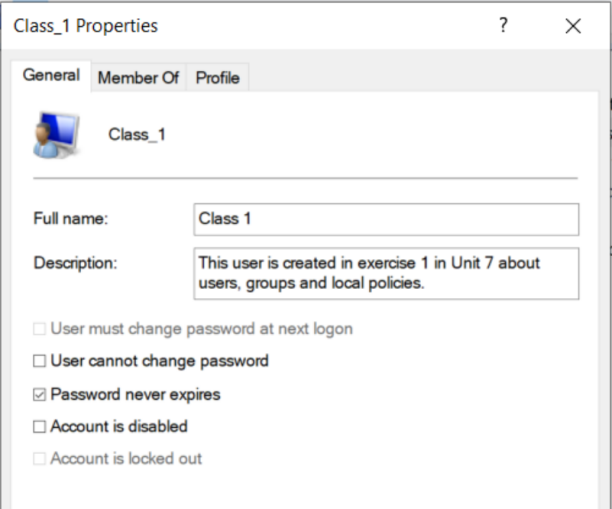


And for every user we need to go to Local Security Policy window and there Local Securities > Account Policies> Password policy and change the “maximum password age” to 0.



5. When can you use a locked account?

An account will be locked when the maximum attempts of introducing a password has been reached. So we can either wait for the reset time to pass, or we can unlock it from an administrator account.

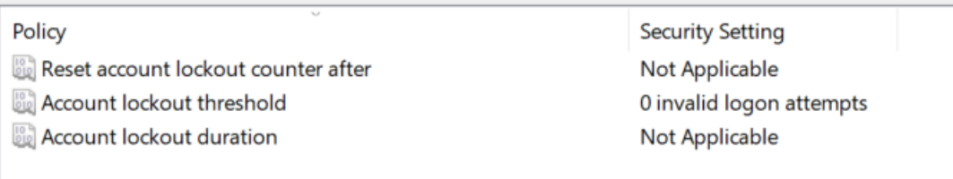


We would need to uncheck last box that says “Account is locked out”. In this case it is faded because the account is not actually locked out.

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?

The reset account lockout counter after cannot be larger than the account lockout duration because it would simply be of no effect. So it needs to be a smaller or equal value.

If account local threshold was 0 we wouldn’t be able to change the other two policies.



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-

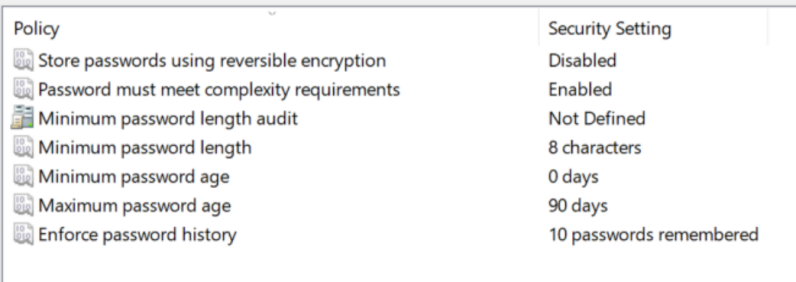
alphanumeric characters.

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

• All the passwords expire after 3 months.

This changes can be made in Local Security Policy window and there Local Securities > Account Policies> Password policy

There we need to change , minimum password length, maximum password age, password history, and complexity requirements. The menu should look like this.



1. 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.

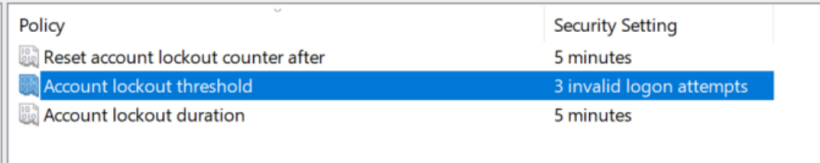
• Lock the user again.

• Wait for 5 minutes.

• Type the right password and check if the user is able to log in.

These changes have to be done in Local Security Policy>Security Settings> Account Policies>Account Lockout Policies.

There we change the policies according to the exercise



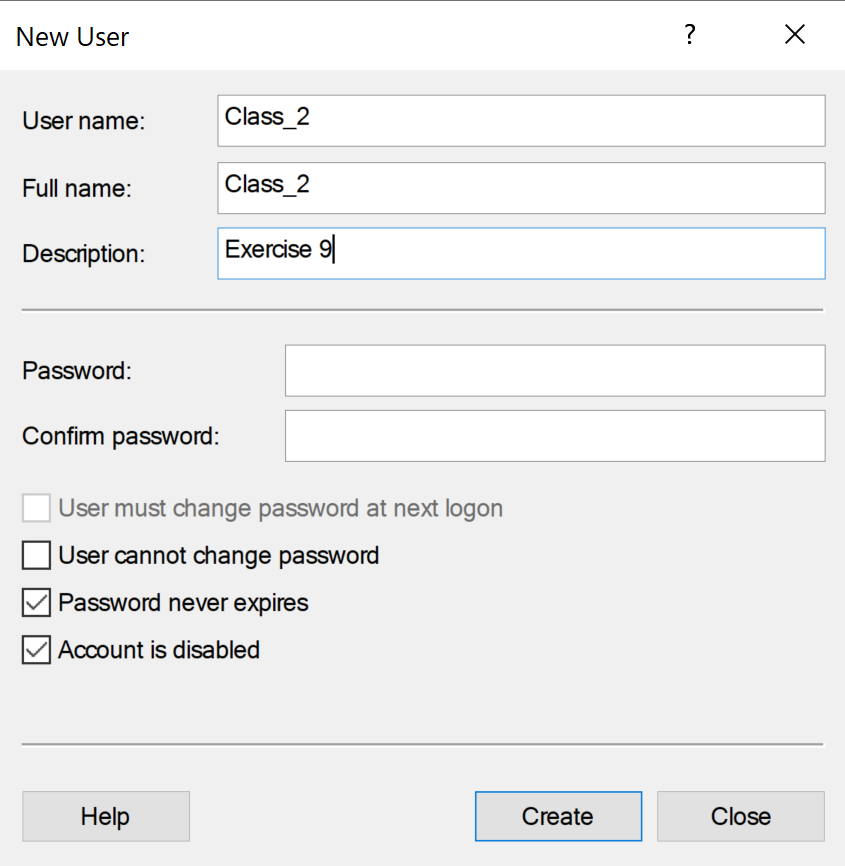
9. Add a new group name “Class” and complete the following:

• Add the user “Class\_1” to the group “Class”.

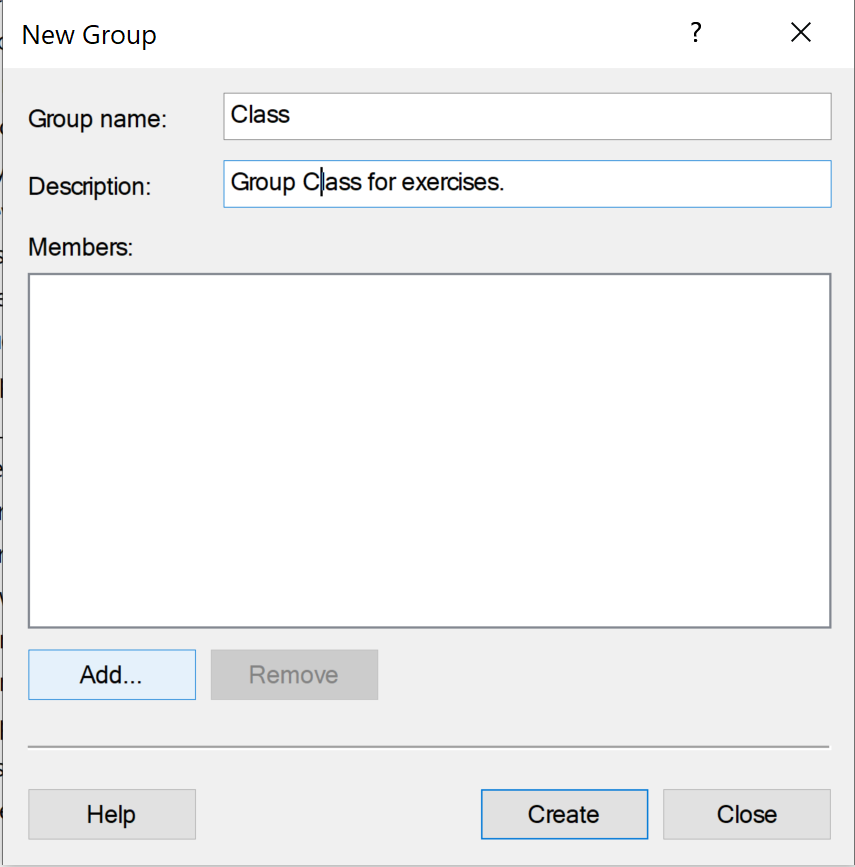
• Create a guest user called “Class\_2”, initially disabled that cannot change

the password. Then, add the user to “Class”.

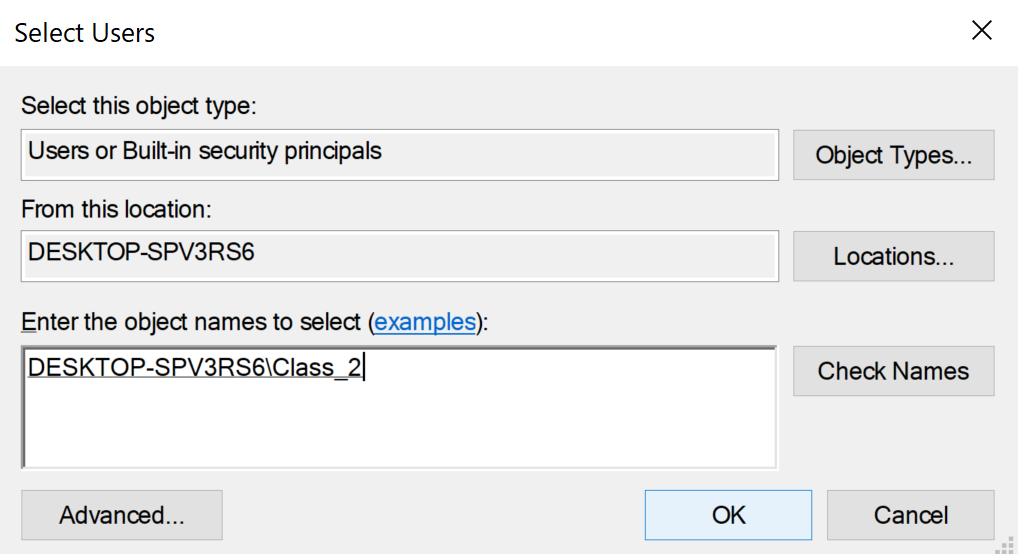
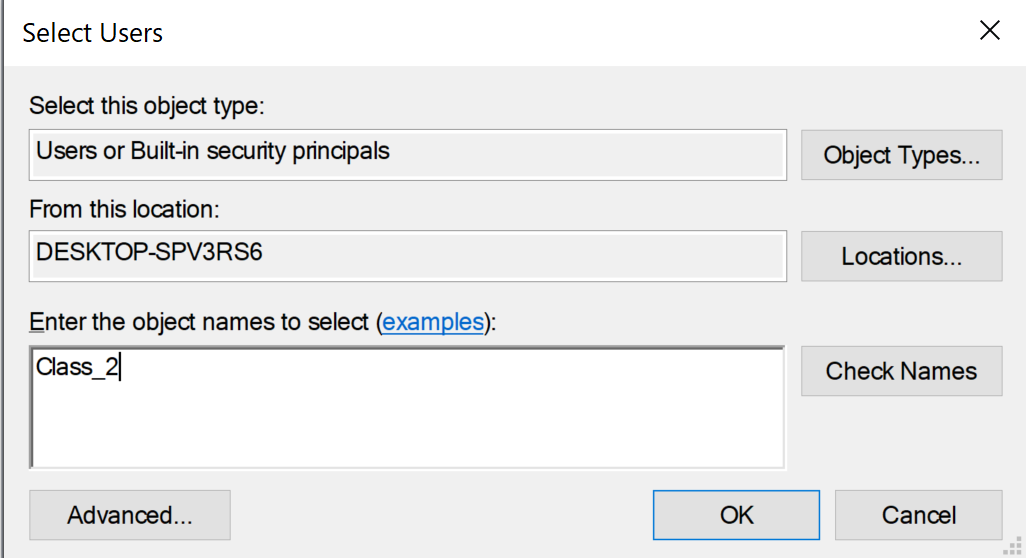
We create Class\_2, we need to check the two bottom boxes in order to match the requirements of the exercise.



Now we create the Class group.



To add members we click on add.



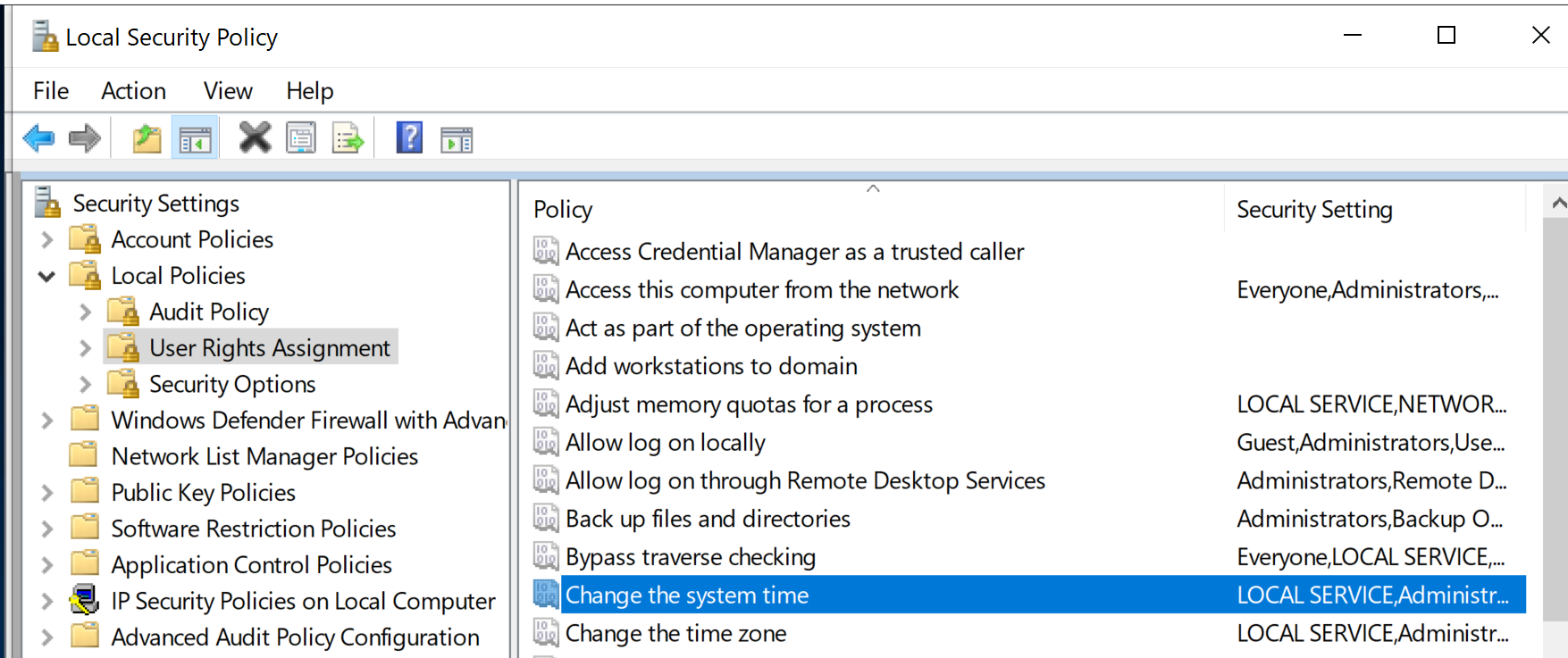
Now that the users are on the members list we click on OK and its done.

Computer systems 2

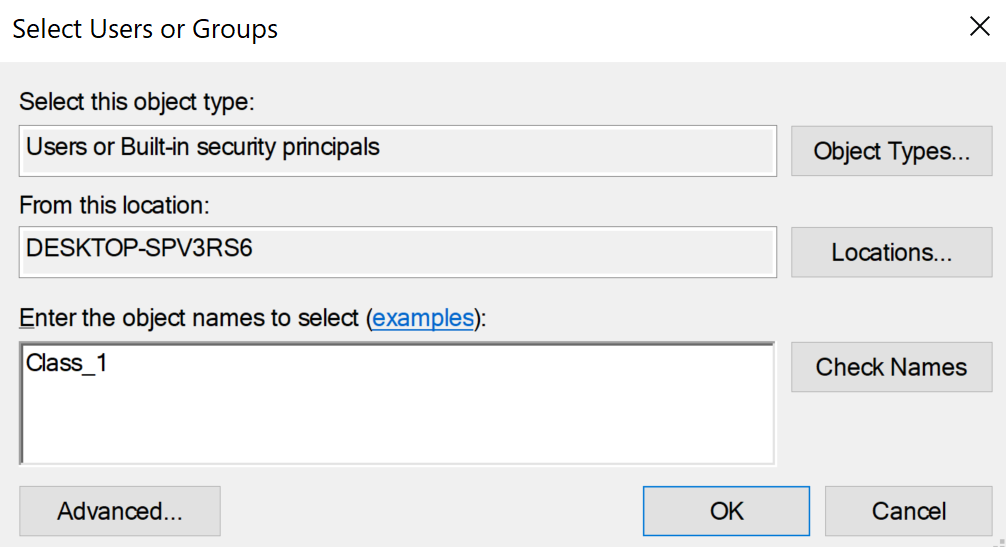
10. Modify the user rights so “Class\_1” and “Class\_2” will be able to “Change the system time”.

For this exercise we need to go to Local Security Policies>Security Settings>Local Policies>User Rights Assignment

There we need to look for Changing System Time

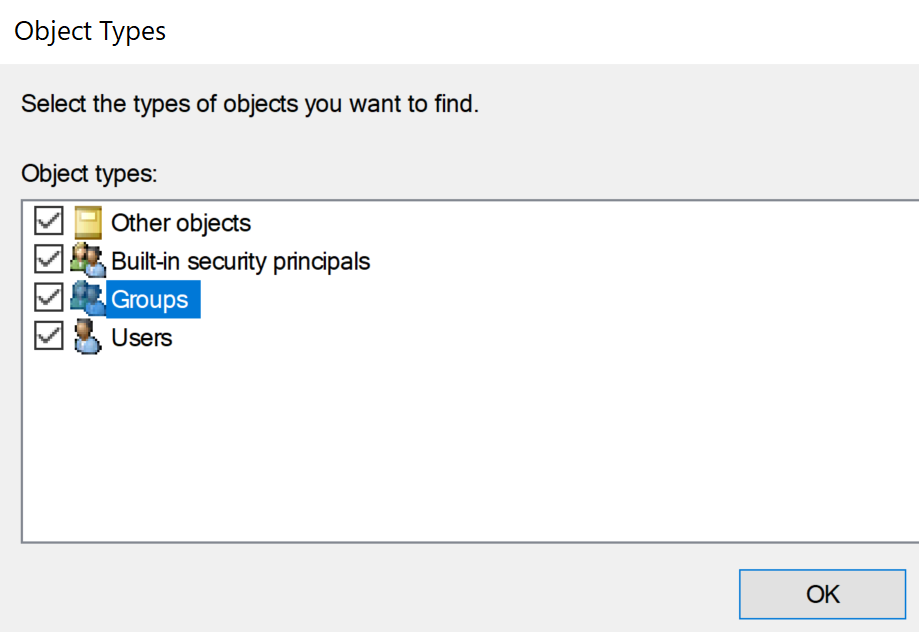


We right click on it and click on Properties>Add User or Group And follow the same process when creating a Group. We write the names of the users, check them and add them.

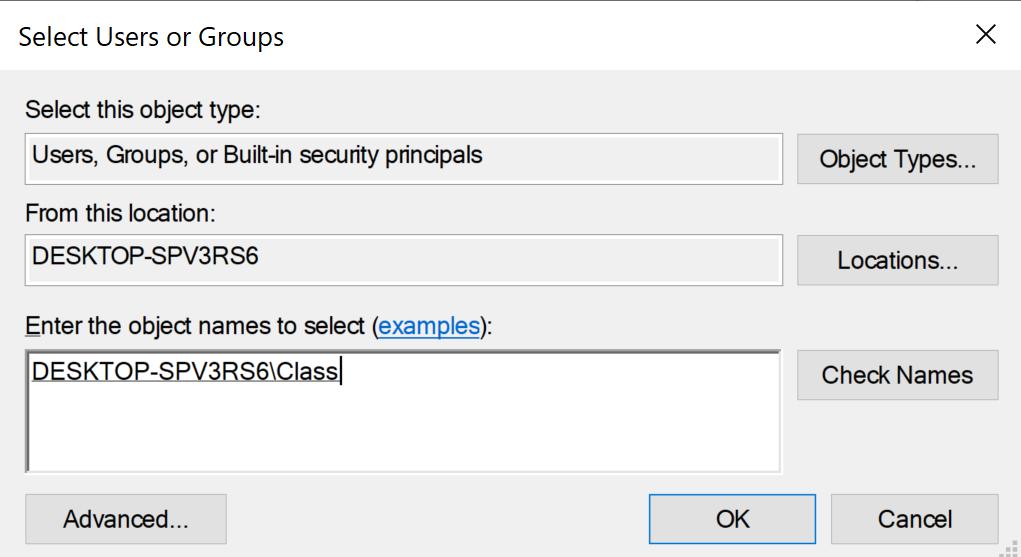


Also, since both the users we need to add form the group Class we can directly add this group instead.

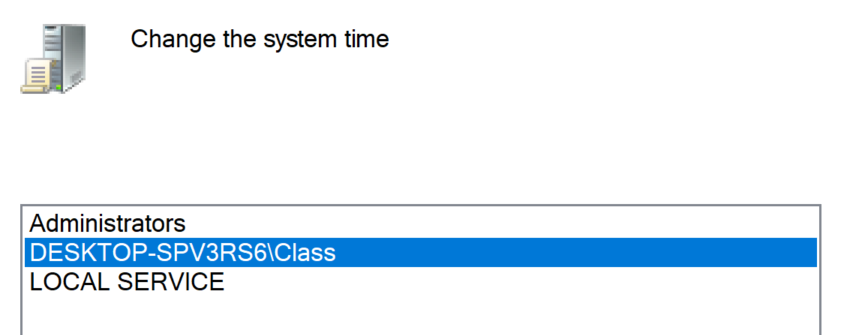
We need to make sure that directly adding groups is allowed and we check it in Object types.



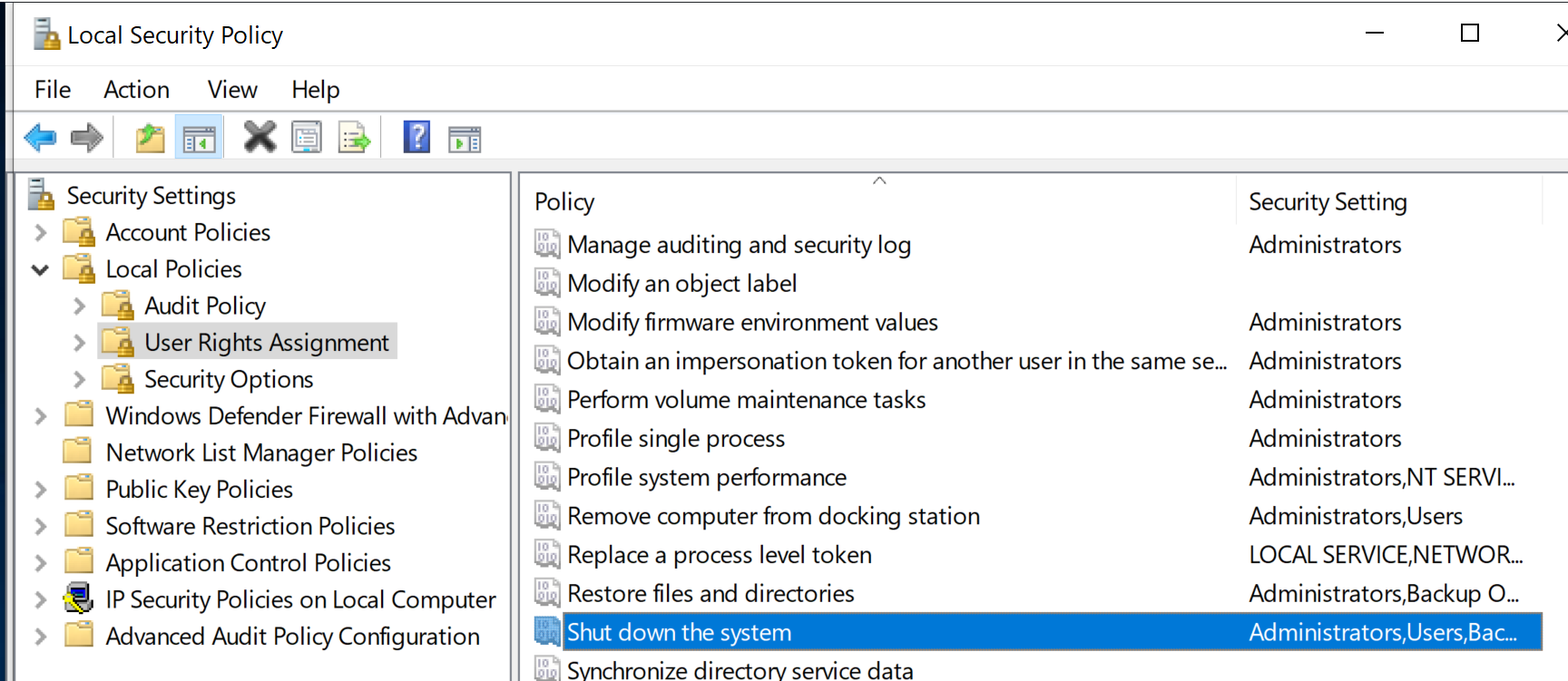
Now we can add Class the way we know.



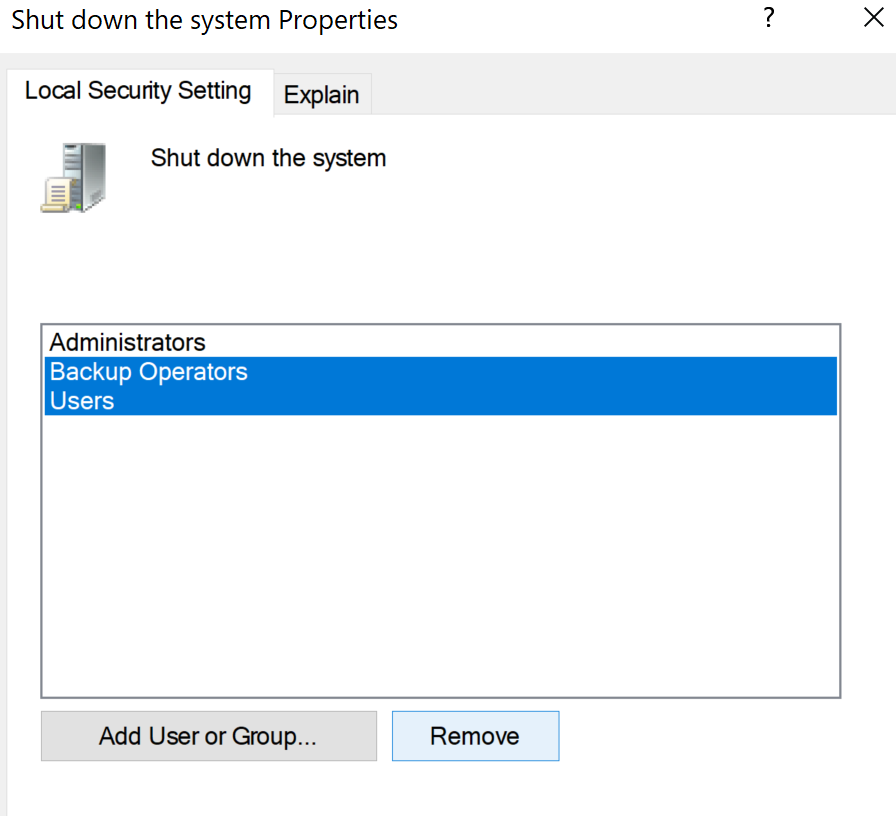
As we can see it is now added.

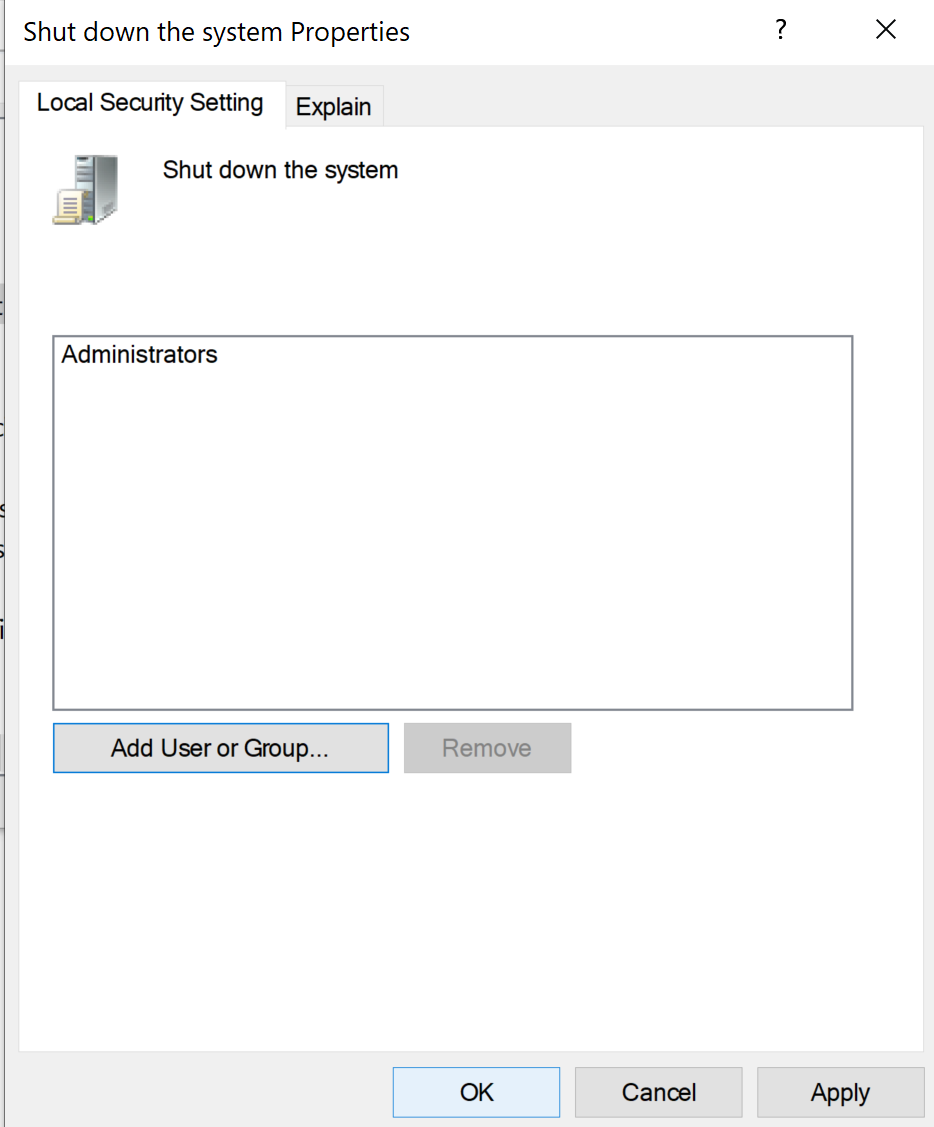


1. Modify the user rights so that only the administrator users can “Shut down the system”

In the same menu as the previous exercise we now look for ‘Shut down the System’.

Again we click on it and select the ones we want to remove, everyone except Administrators.



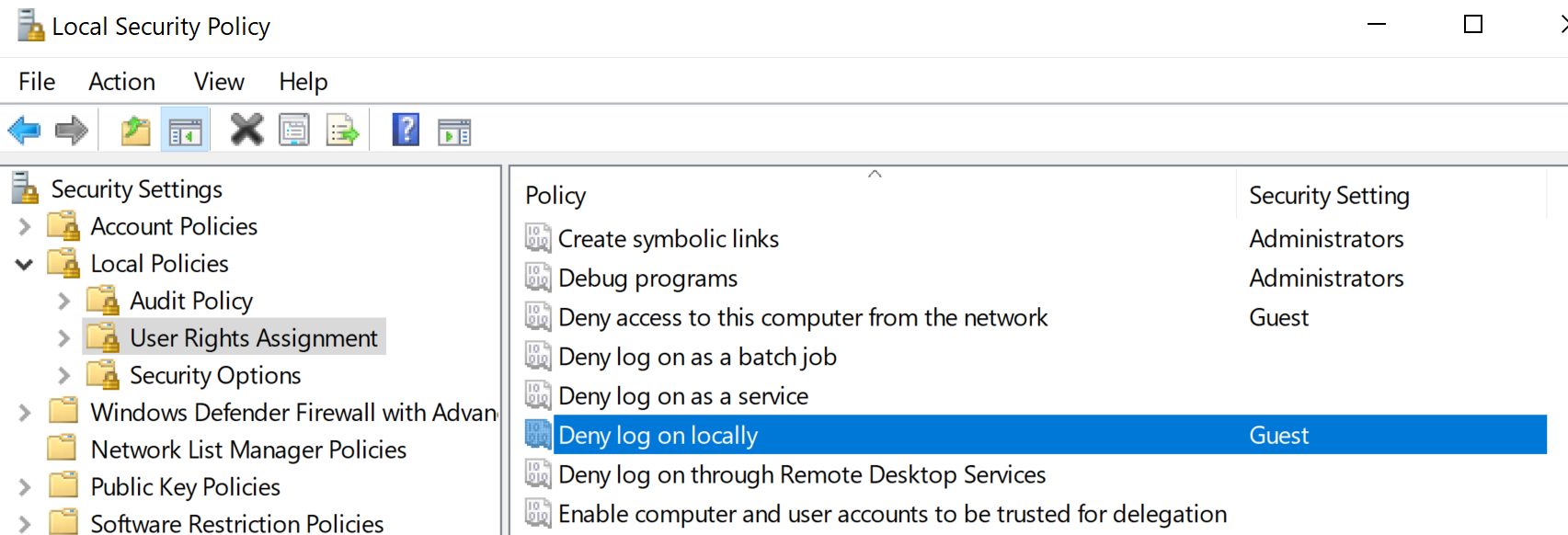


We click on ok to save the changes and finish.

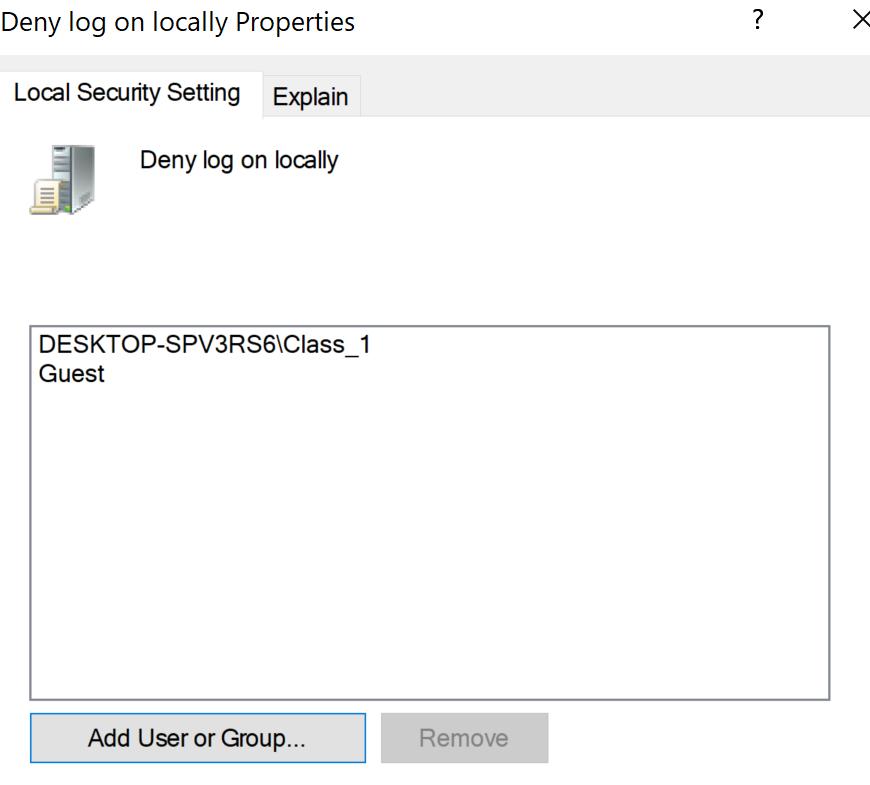
12. Suppose all the standard users are able to log in. How can we deny log on to the

specific user “Class\_1”?

Again in the same menu in Local Security Policy we look for ‘Deny log on locally’



We follow th same process as before and add Class\_1 to the list

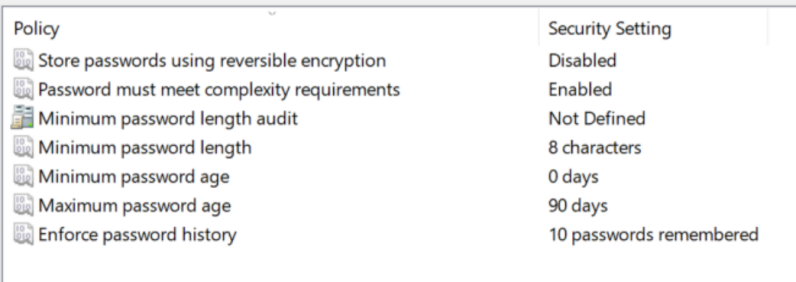


Now Class\_1 will not be able to log in.

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.

This were the requirements for exercise 7:



So when creating user Test we have to create a password that meets said requirements.

I used Paloma\_890 .

