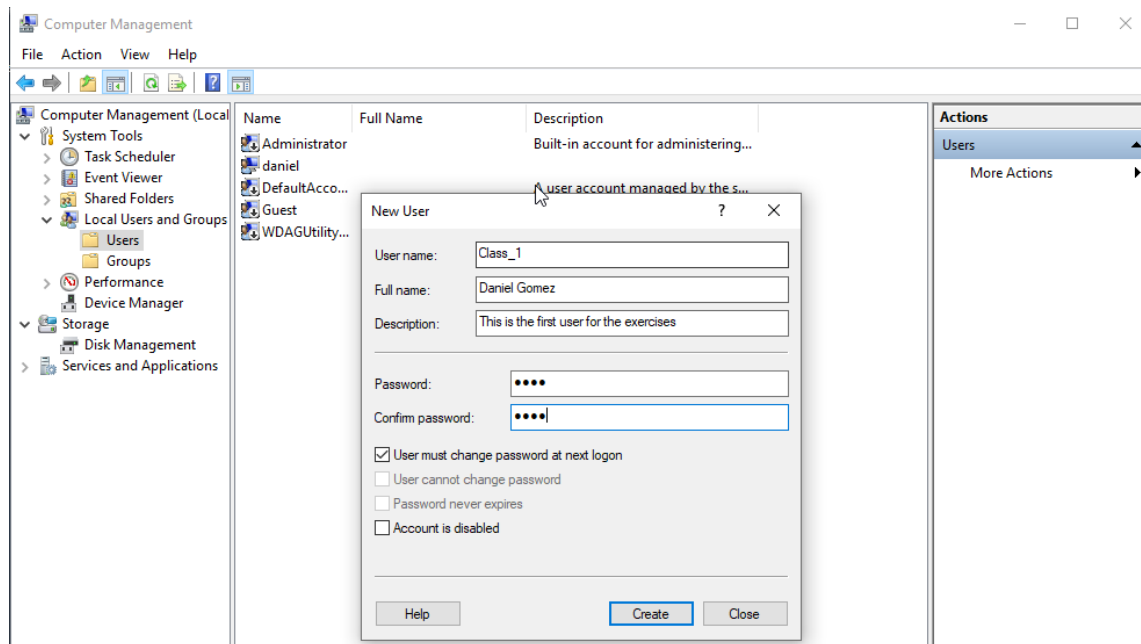


**Daniel Gómez Sánchez**

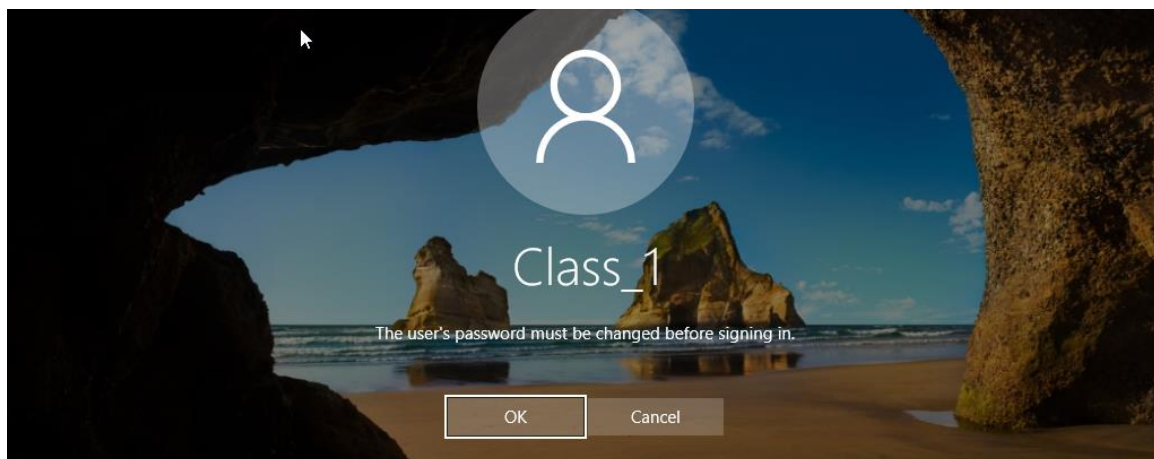
**DW1E**

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 login.



First we have to open the Computer Management Menu, go to Local User and Groups/Users and create a new user, in this case we have to activate the user must change password at next login option.



Then when we try to login with the new user we have to change the password.

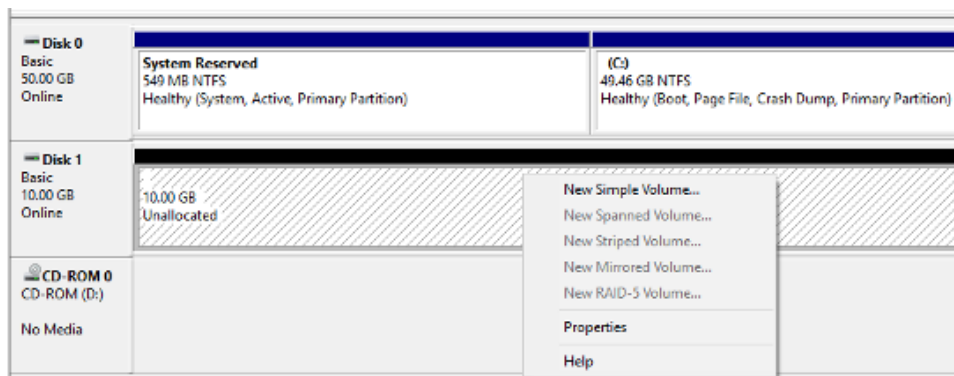
2. Complete the following parts about the user “Class\_1” from the previous exercise.

- Verify if the profile folder exists.
- Log in as “Class\_1”.

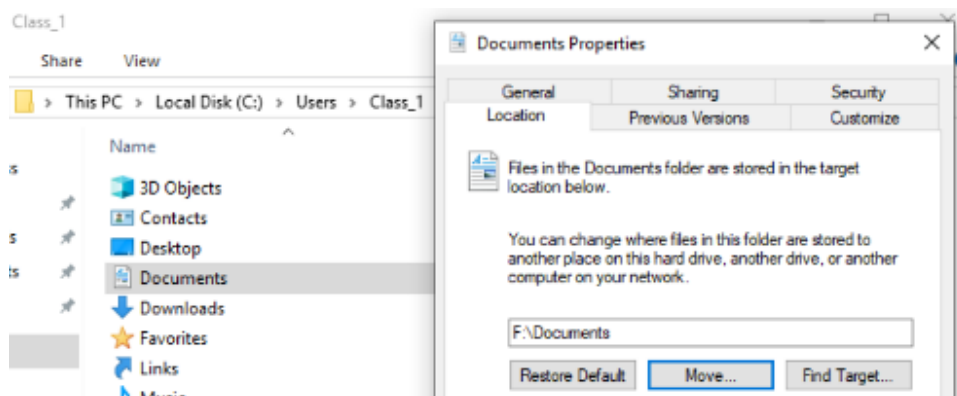
- Verify if the profile folder now exists.
- Add a second hard drive to the virtual machine and create a folder called “My Documents” in F:\
- Move “Class\_1” Documents folder to the directory you have just created.
- Open “Documents” shortcut and create a new folder. Check if this folder has actually been created in “F:\My Documents”.

The profile folders are not created until we first log in. we can check C:\Users\Class\_1. It will only exist when you log in at least once.

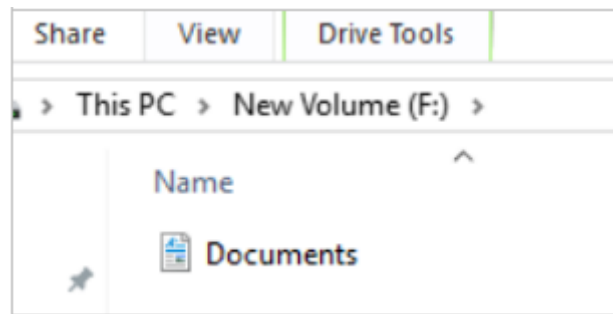
Then, we have to create a second virtual disk. And Create a simple volume in the letter F



Finally, we create a new folder in F called “Documents”






Now we can see that the folder path has changed.

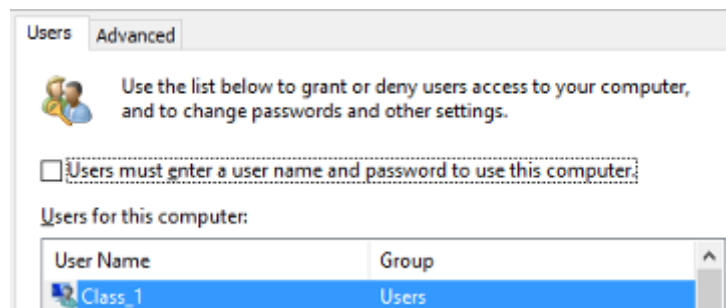


3. How do you configure a user to log in without a password and automatically when turning the computer on?

First we have to configurate the password policy like: "Minimum password length: 0" and "Passwords must meet complexity requirements: disabled"

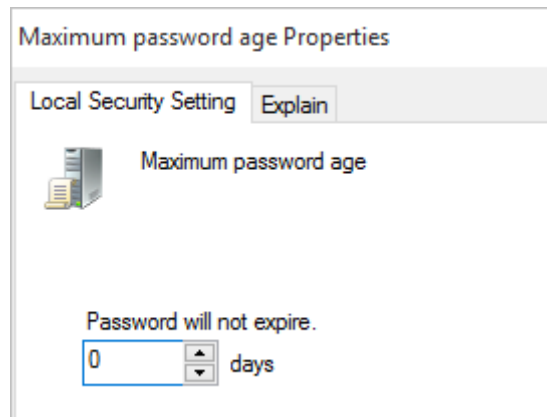
	Minimum password age	0 days
	Minimum password length	0 characters
	Password must meet complexity requirements	Disabled

Then we have to uncheck the option that requires to set a password the first time we log in.

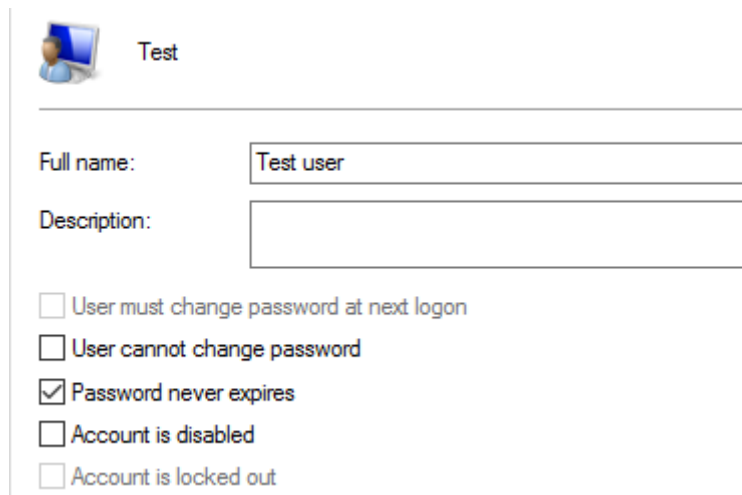


1. How do you configure a specific user so that the password never expires?      How can you configure this policy for everyone?

We have to go to: Local security policies -> Maximum password age = 0. This way, the password for every user will never expire.

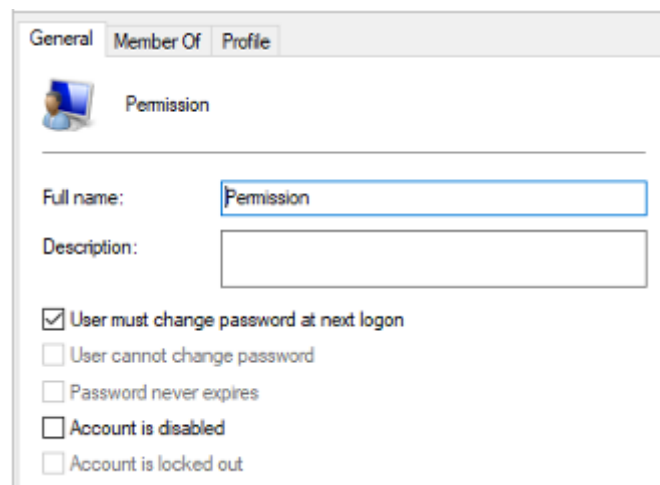


Also, from Computer Management, the “Password never expires”. This way only affects to specific users.



5. When can you use a locked account?

After the lockout duration or the logon failed attempts are reset. The administrator is also able to unlock an account from computer management. The checkbox will be automatically enabled.








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”.

If “Account lockout threshold” were 0, you would not be able to set the other policies, as you cannot lock a password.

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 nonalphanumeric characters.
- The system stores the last 10 passwords for each user.
- All the passwords expire after 3 months.

Policy	Security Setting
 Enforce password history	10 passwords remembered
 Maximum password age	90 days
 Minimum password age	0 days
 Minimum password length	8 characters
 Password must meet complexity requirements	Enabled

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.

 Account lockout duration	5 minutes
 Account lockout threshold	3 invalid logon attempts
 Reset account lockout counter after	5 minutes

General Member Of Profile

Permission

Full name: Permission

Description:

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

☐ Account is locked out

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".

New User ? X

User name: Class\_2

Full name:

Description:

Password:

Confirm password:

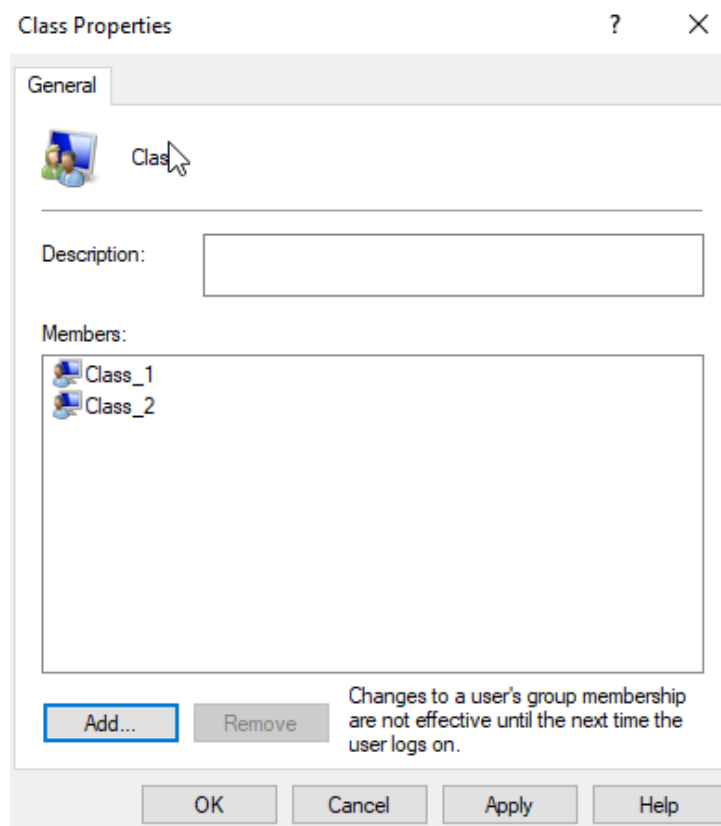
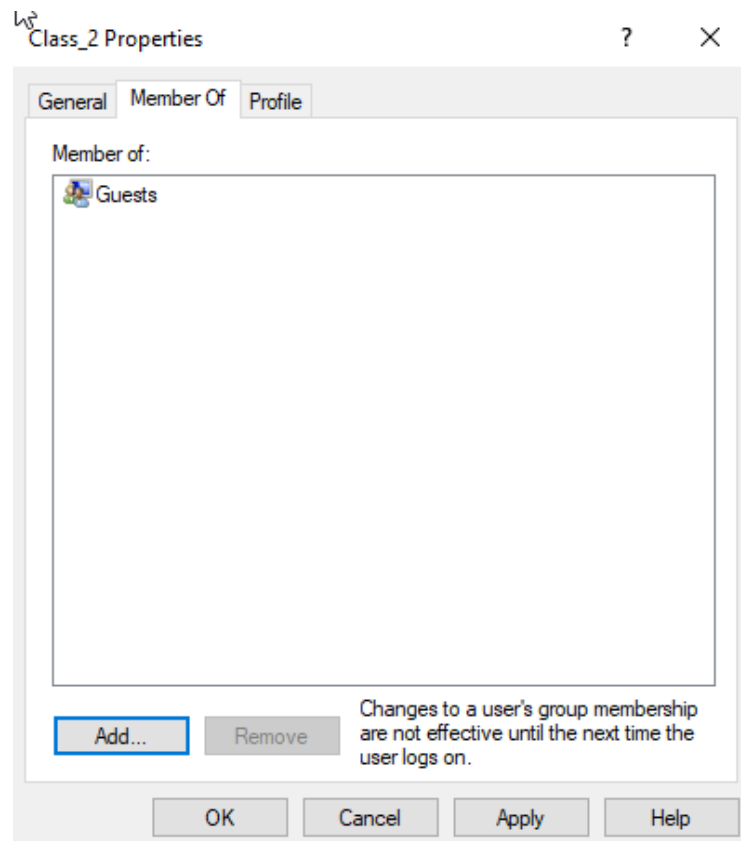
☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

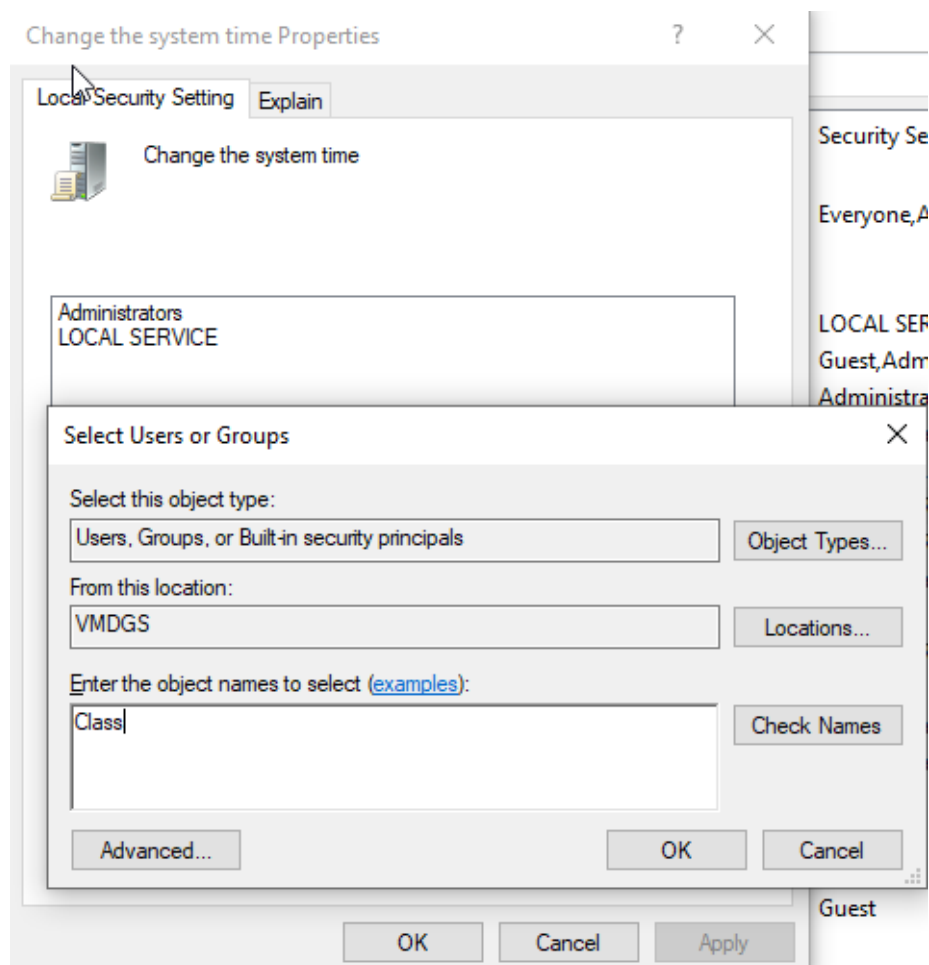
☒ Account is disabled

Help Create Close

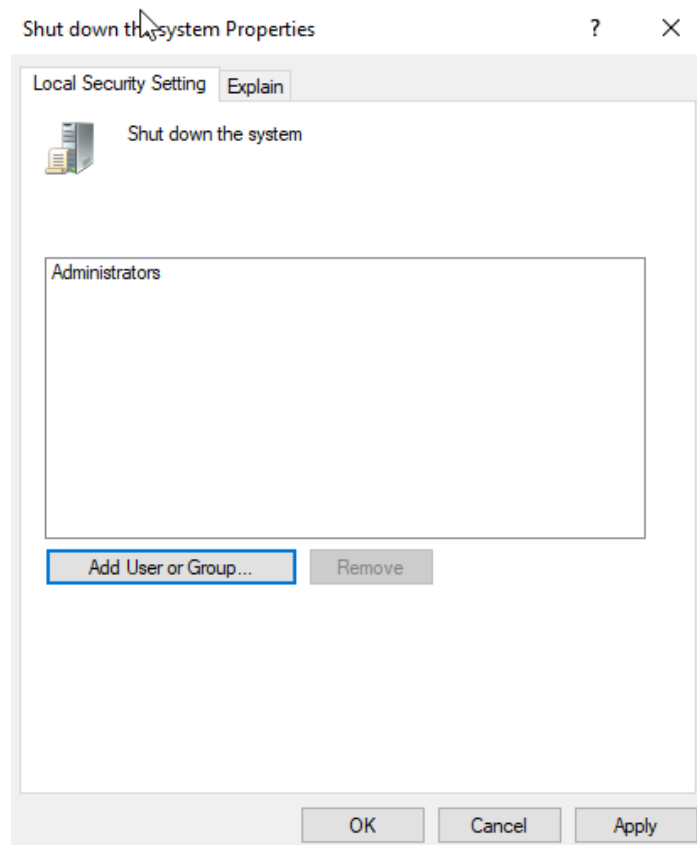


10. Modify the user rights so "Class\_1" and "Class\_2" will be able to "Change the system time".

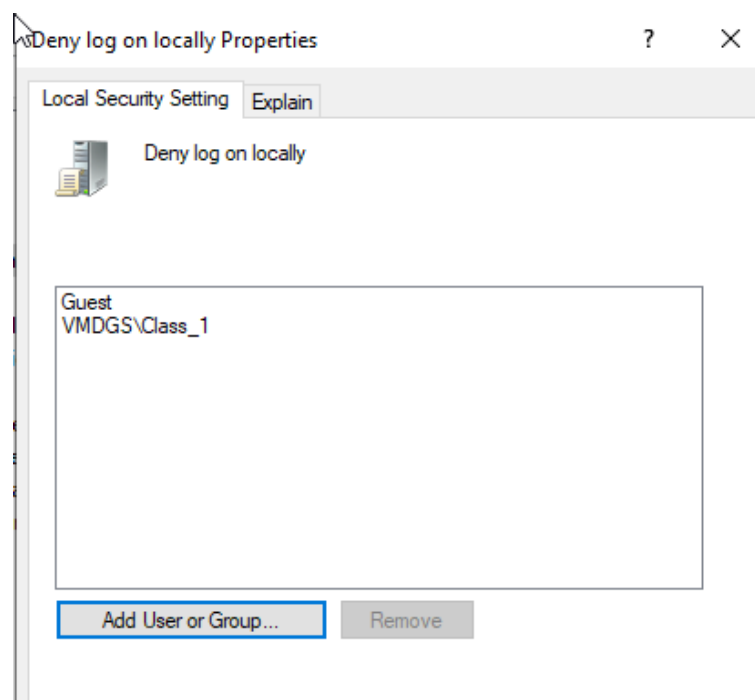




11. Modify the user rights so that only the administrator users can “Shut down the system”



12. Suppose all the standard users are able to log in. How can we deny log on to the specific user "Class\_1"?



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.

A valid password, needs to have: " (uppercase, lowercase, numbers, non-alphanumeric characters, minimum length 8...)

If we deleted "Test" from the group "Users", we would not be able to log in due to test doesn't belong to any of the groups that are allow to log in.