

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

The user must change the password at next logon

The screenshot shows the Windows Computer Management interface. The left navigation pane is expanded to show 'Local Users and Groups' under 'System Tools'. The 'Users' folder is selected. A context menu is open over the 'Users' folder, with the 'New User...' option highlighted. The main pane displays a table of existing user accounts:

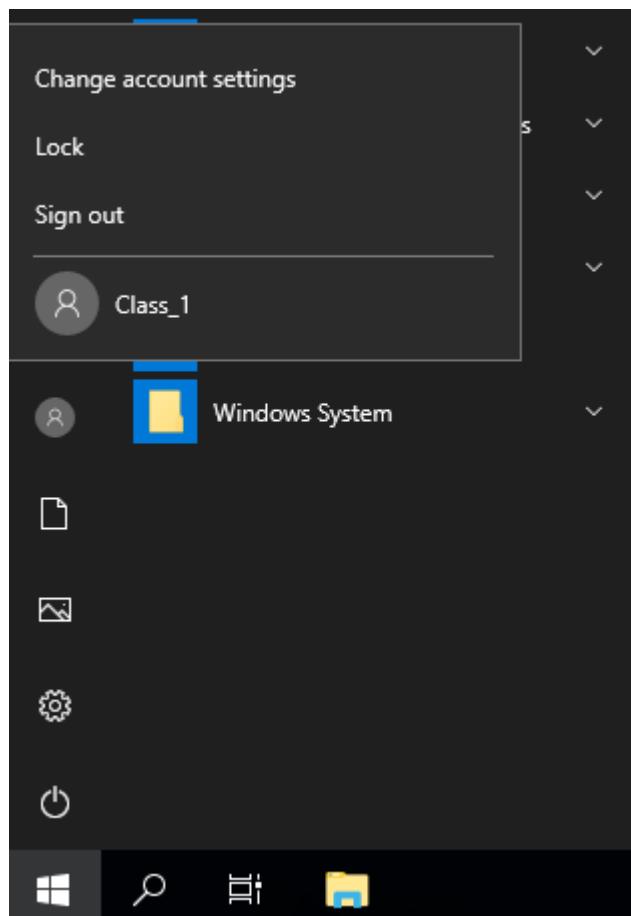
Name	Full Name	Description
Administrator		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
defaultuser0		
Guest		Built-in account for guest access t...
student		
WDAGUtility...		A user account managed and use...

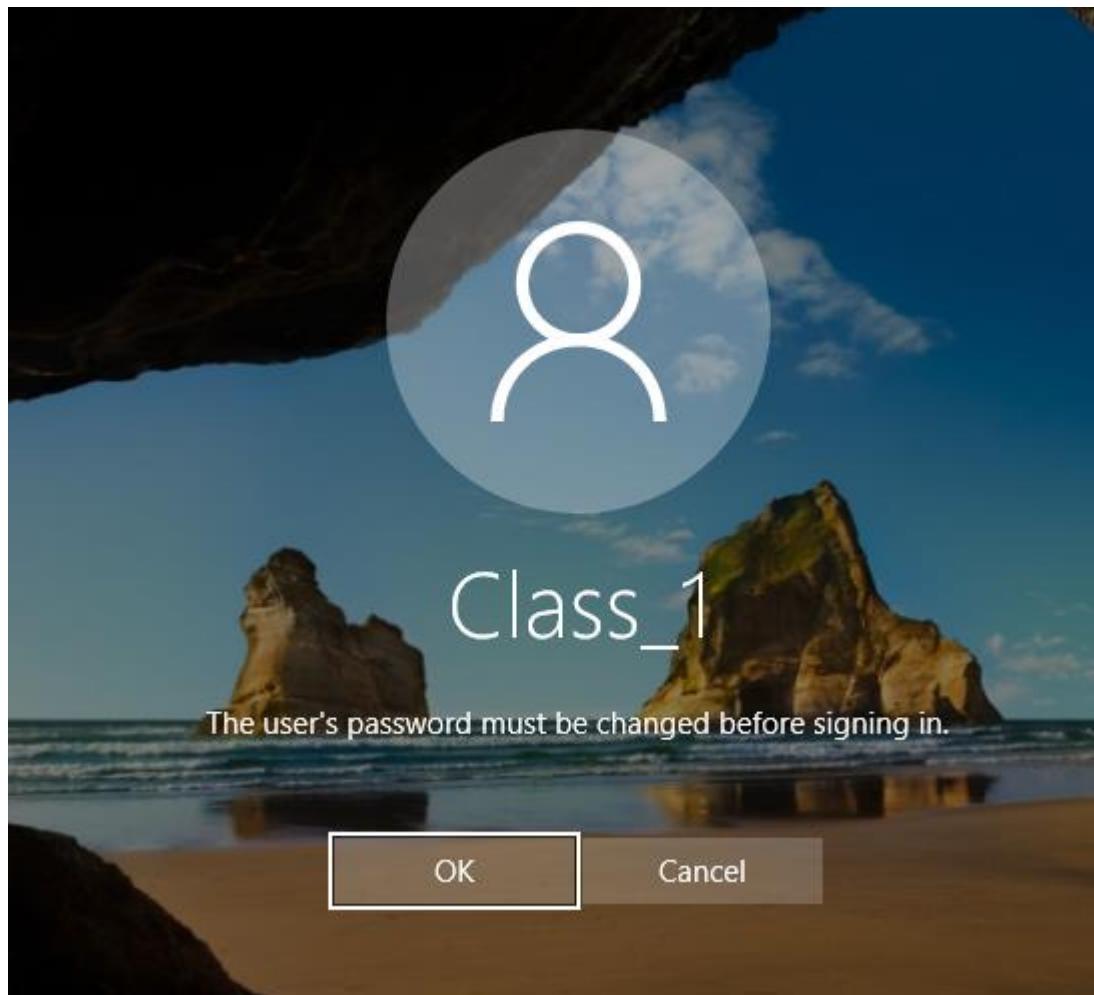
The 'Actions' pane on the right is set to 'Users'.

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.

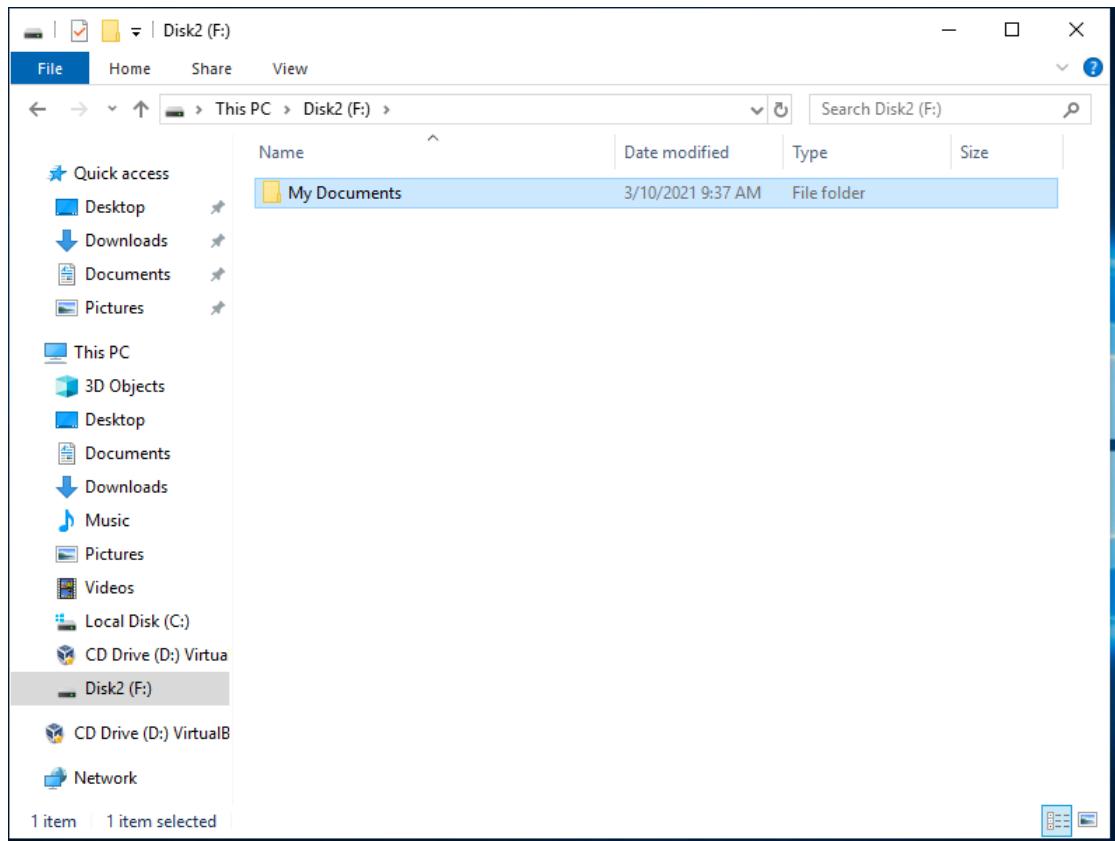
- Open “Documents” shortcut and create a new folder. Check if this folder has actually been created in “F:\My Documents”.

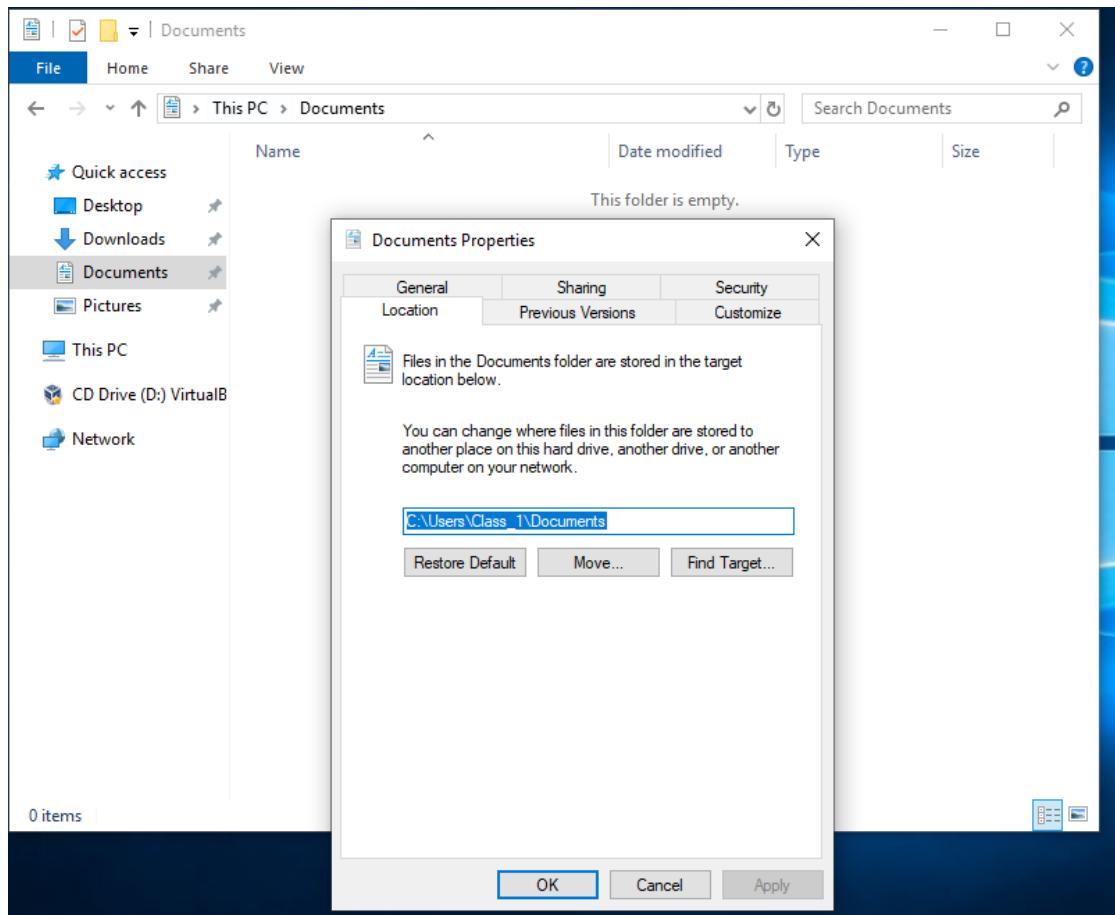


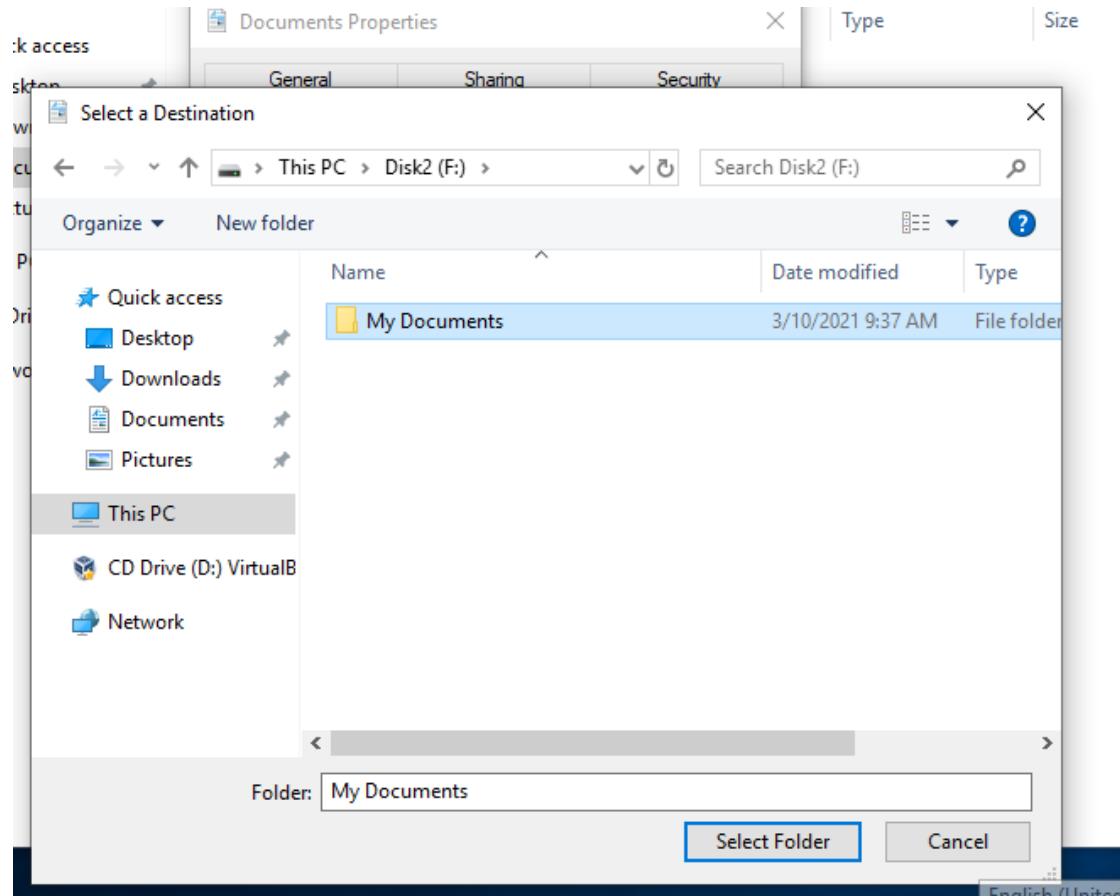


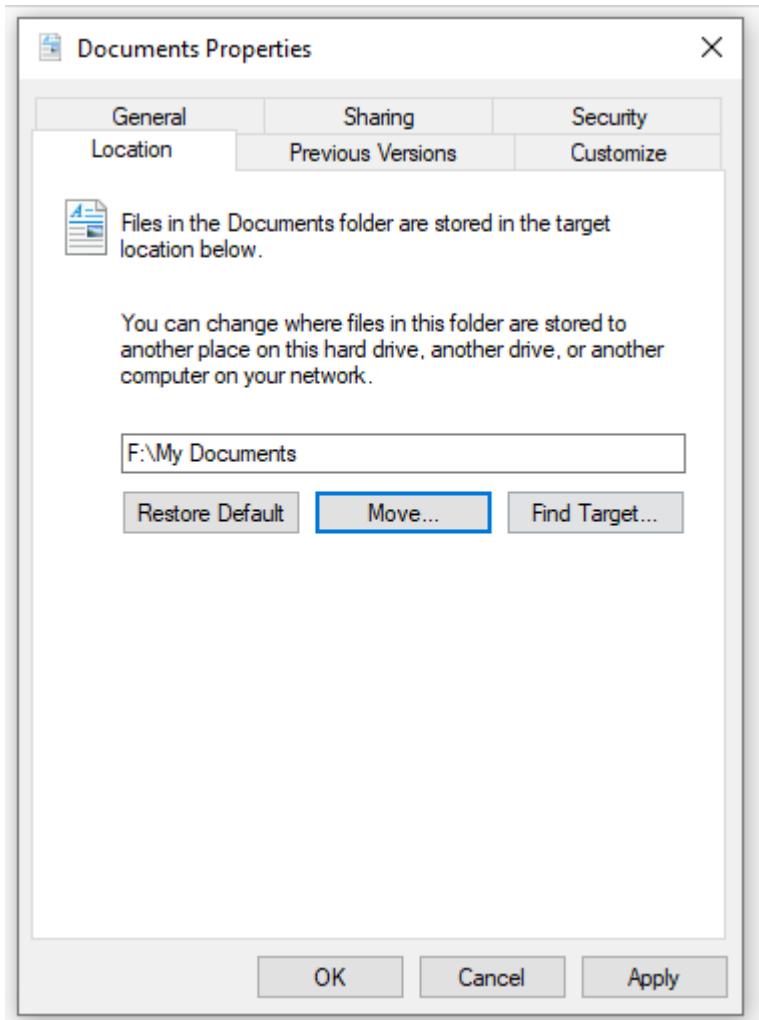
▼ Devices and drives (3) —————

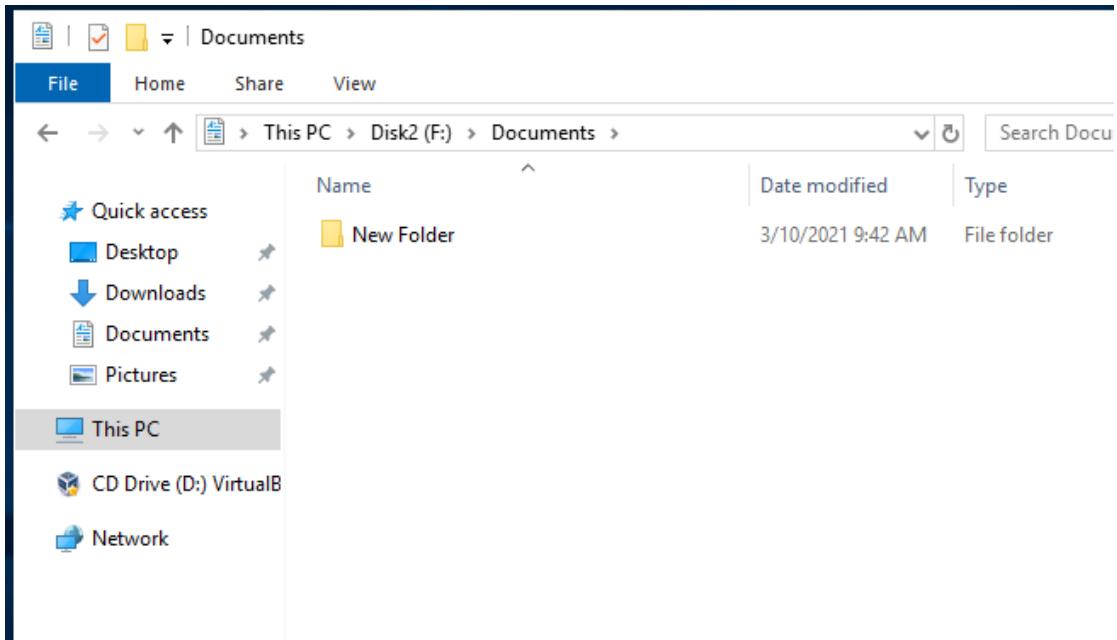
	<b>Local Disk (C:)</b>	
	<b>Disk2 (F:)</b>	
	9.95 GB free of 9.99 GB	



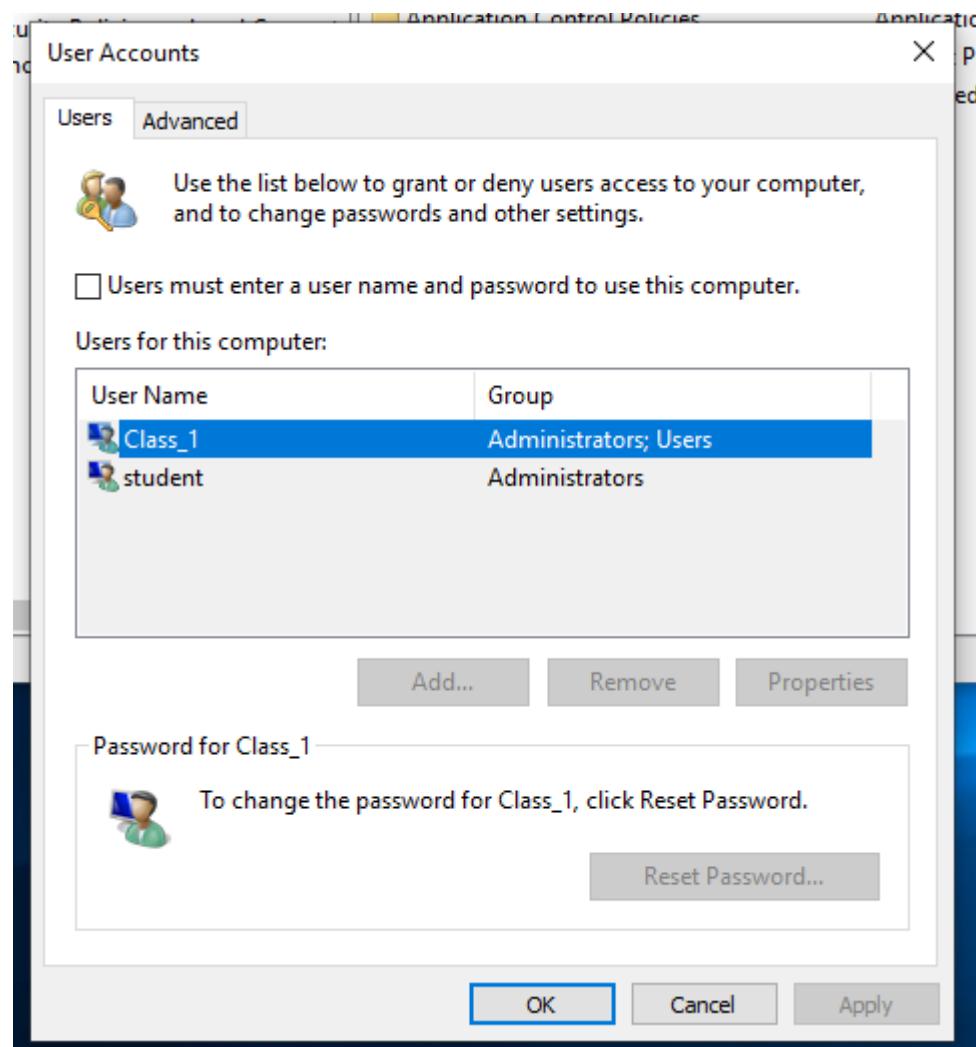


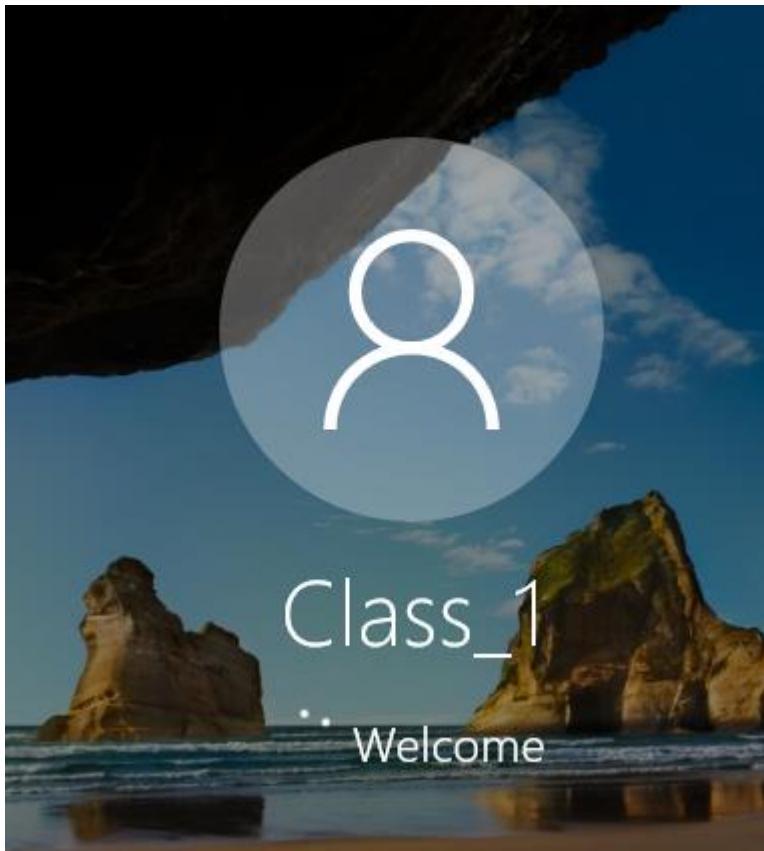




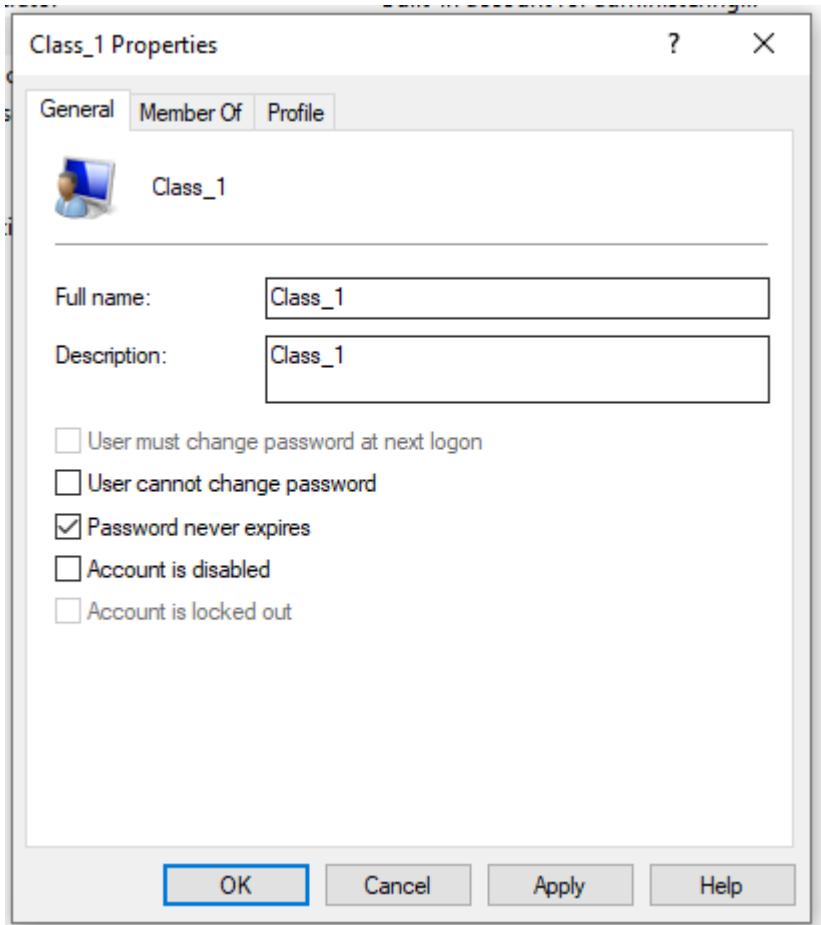


3. How do you configure a user to log in without a password and automatically when turning the computer on?





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



The screenshot shows the 'Local Security Policy' snap-in window. The left pane shows a tree view of security settings: 'Security Settings' > 'Account Policies' (which includes 'Password Policy' and 'Account Lockout Policy') > 'Local Policies' (which includes 'Audit Policy', 'User Rights Assignment', 'Security Options', 'Windows Defender Firewall with Adv...', 'Network List Manager Policies', 'Public Key Policies', 'Software Restriction Policies', 'Application Control Policies', 'IP Security Policies on Local Computer', and 'Advanced Audit Policy Configuration'). The right pane displays a table of policies and their settings:

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

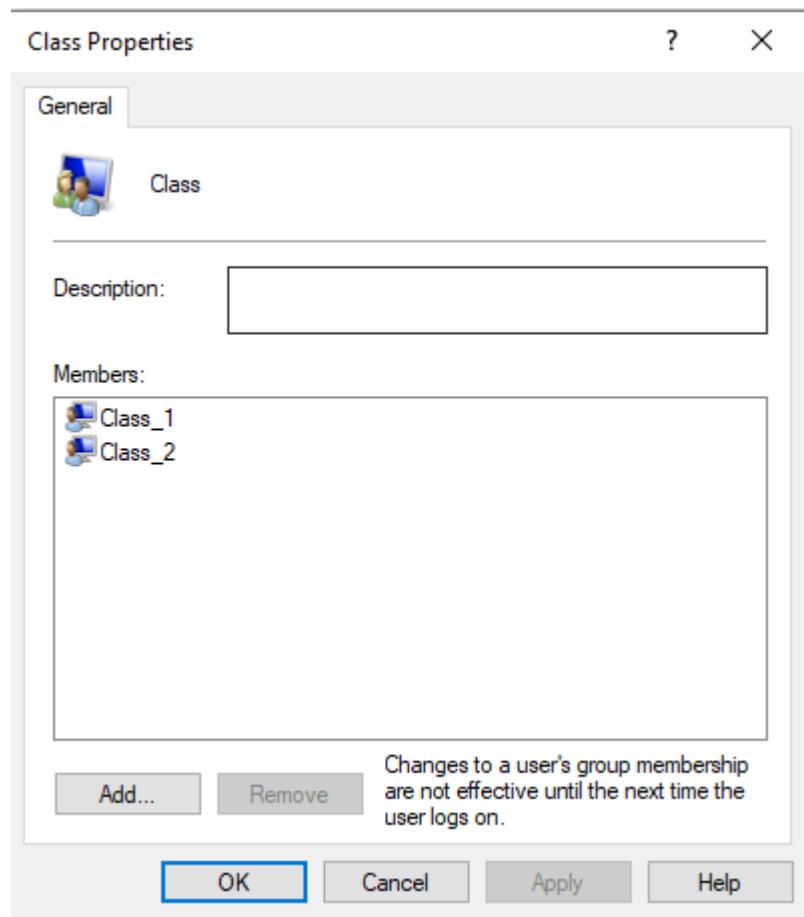
##### 5. When can you use a locked account?

We can wait until the user automatically unlocks (if the locked state is temporally) or go to the user properties with the administrator account and deselect account locked checkbox.

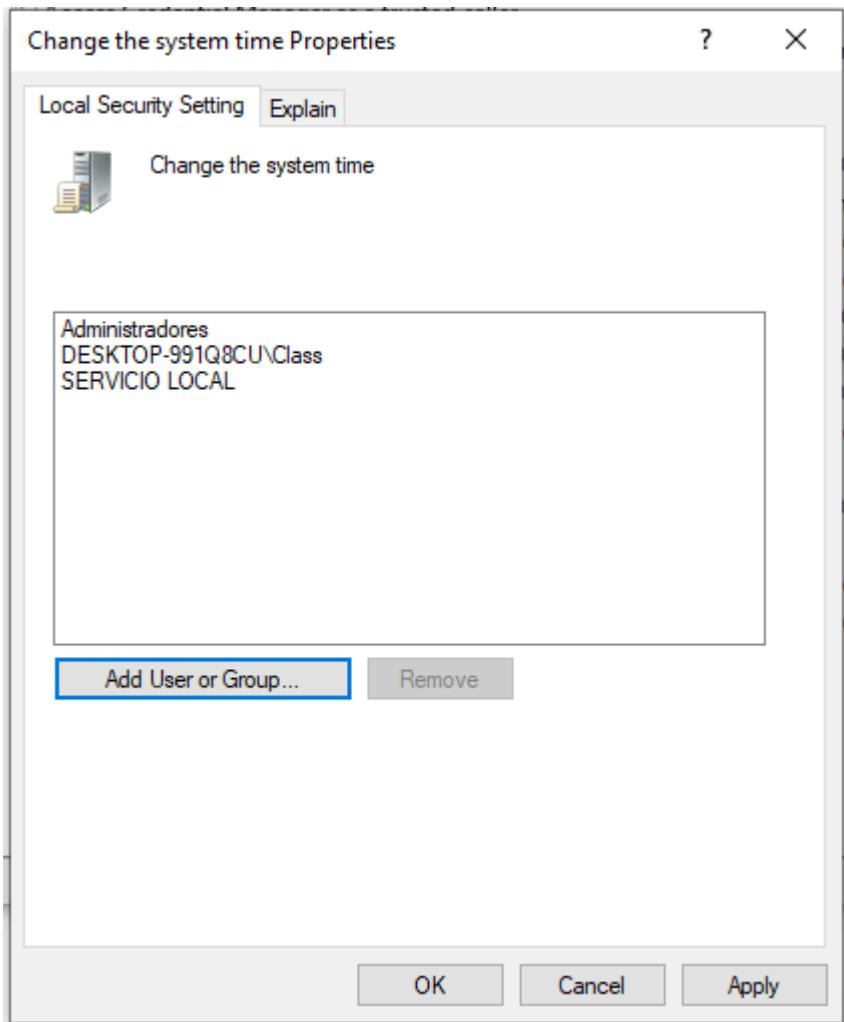
6. Imagine you define an “Account lockout threshold” of 3 and “Account lockout duration” of 5. What would be the valid values of “Reset account lockout counter after”? What if “Account lockout threshold” value was 0?

7.

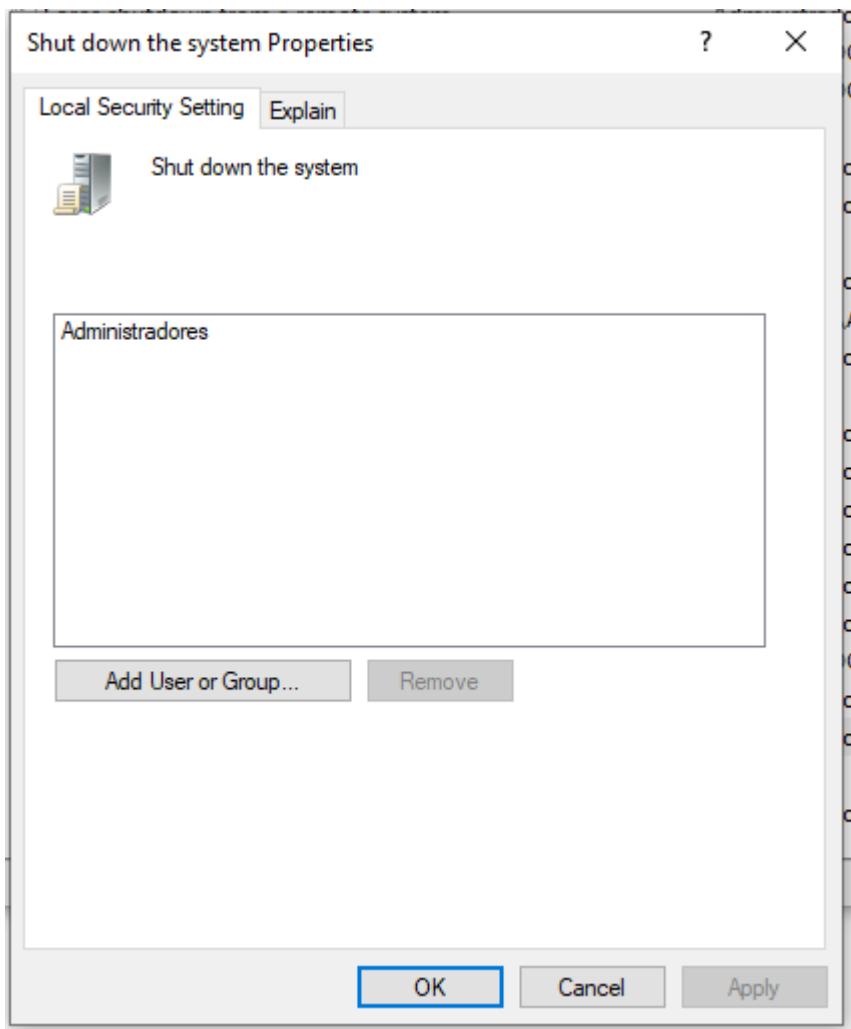
9.



10.



11.



12.

We can deny to log if we deny to log to all the users of Class group.

13.

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	8 characters
Minimum password length audit	1 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Enabled

