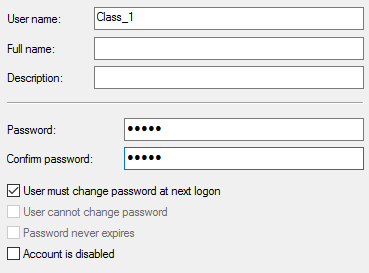
Users, groups and local policies

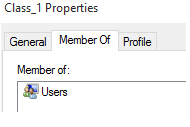
1. Add a new standard user named “Class\_1” including the description and full name. The user must change the password at next logon.



You can add a user from Computer Management 🡪 Users 🡪 New User but also from Settings 🡪 Accounts 🡪 Family & Other Users

The box “User must change password at next logon” is checked by default.

A new user is also standard by default and belongs to Users.



1. 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.

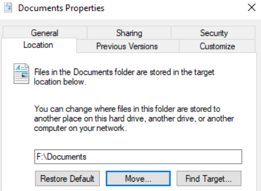
Open “Documents” shortcut and create a new folder. Check if this folder has actually been created in “F:\My Documents”.

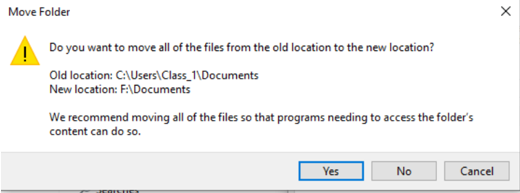
The profile folders are not created until you log in.

To add a second hard drive, create a simple volume in the letter F.

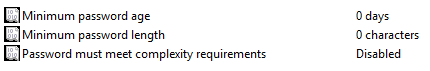


Then, create a new folder called “Documents”. To change the location right clicking on the folder from the tab “Location”

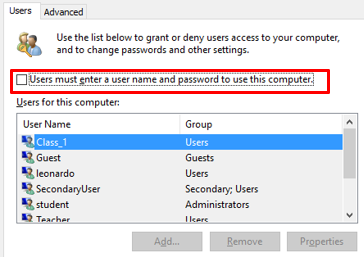




1. How do you configure a user to log in without a password and automatically when turning the computer on?



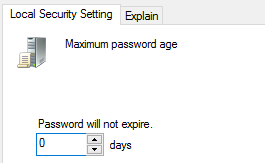
Configuring password settings from Computer Management



This way it automatically logs in.

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

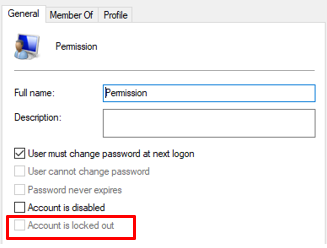
On Local security policies, set Maximum Password Age to 0 days.



To configure this for specific users, from Computer Management check the box “Password never expires”.

1. When can you use a locked account?

You can unlock an account as administrator from computer management



1. 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 won’t be able to set the other policies.

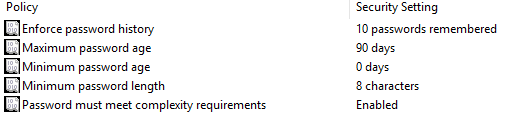
1. Configure the system according to the following criteria:

• 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.



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.

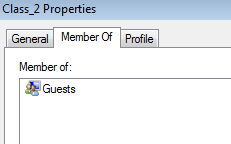


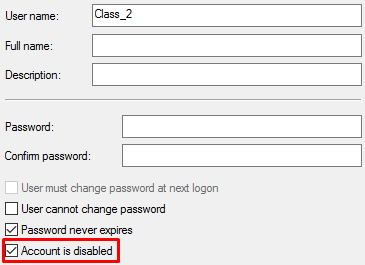
1. Add a new group name “Class” and complete the following:

• 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”.

From Computer Management we create Class\_2, which will be added to Guests groups and removed from Users



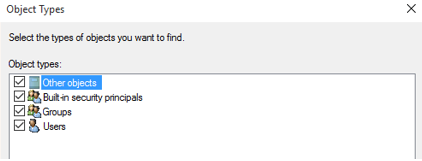


Then in Groups we create a group called “Class” and add users to it

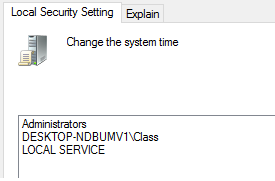
1. Modify the user rights so “Class\_1” and “Class\_2” will be able to “Change the system time”

Local security policies 🡪 User rights assignment 🡪 Change the system time

You cannot add groups by default and you need to check “Groups” in “Object types”

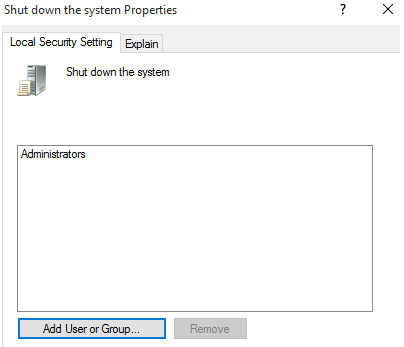


Then we add the group to the policy



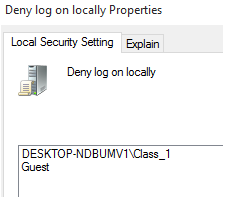
1. Modify the user rights so that only the administrator users can “Shut down the system”

Remove all users except the administrators from the policy below.



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

Local security policies 🡪 User rights assignment 🡪 Deny log on as locally. All the standard users will be able to log in except Class\_1



1. 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.

If we delete Test from the group Users we won’t be able to log in