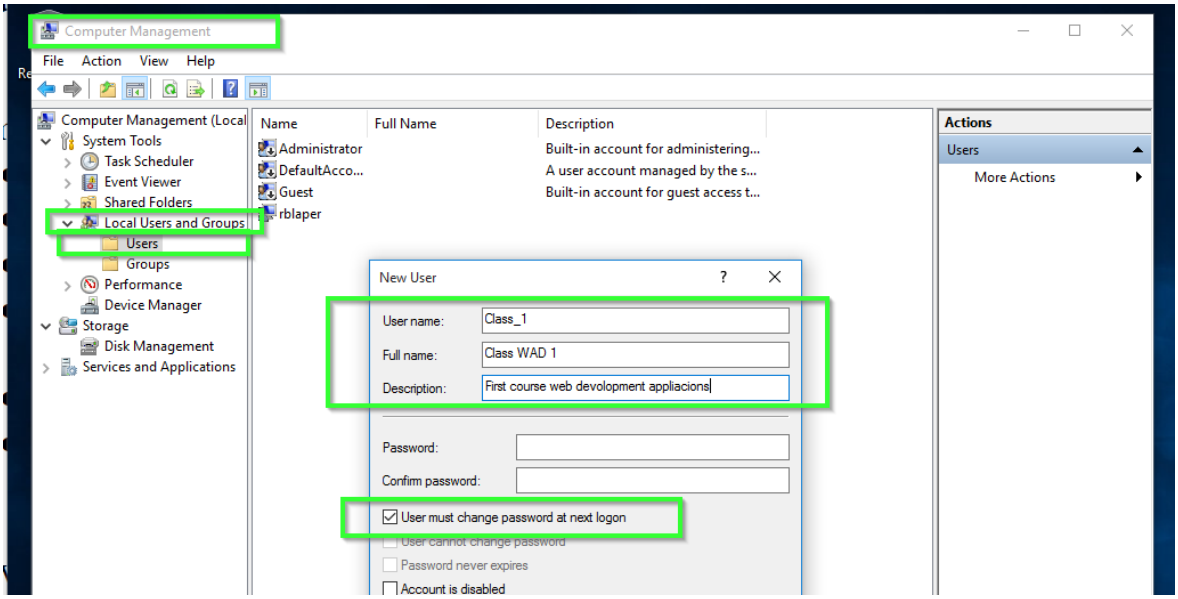
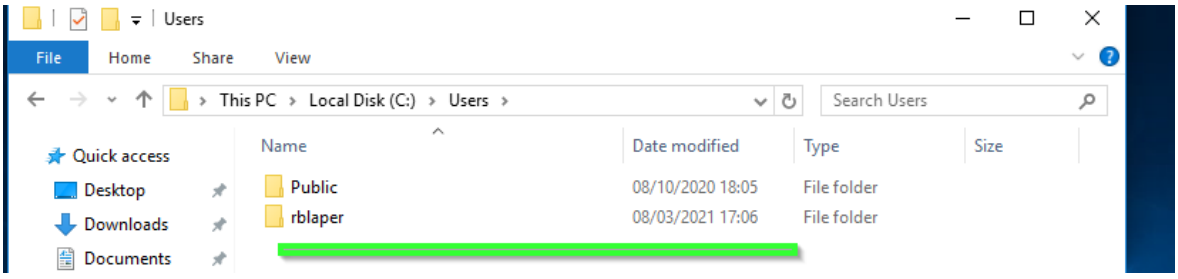
EXERCISES: Users, groups and local policies in Windows 10 x64.

1. **Add a new standard user named "Class_1" including the description and full name. The user must change the password at next logon.**

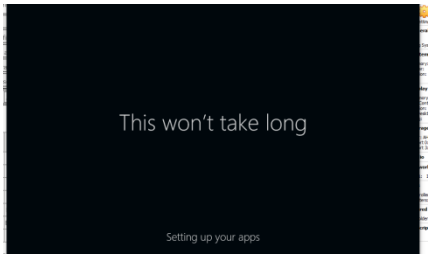


2. **Complete the following parts about the user "Class_1" from the previous exercise.**

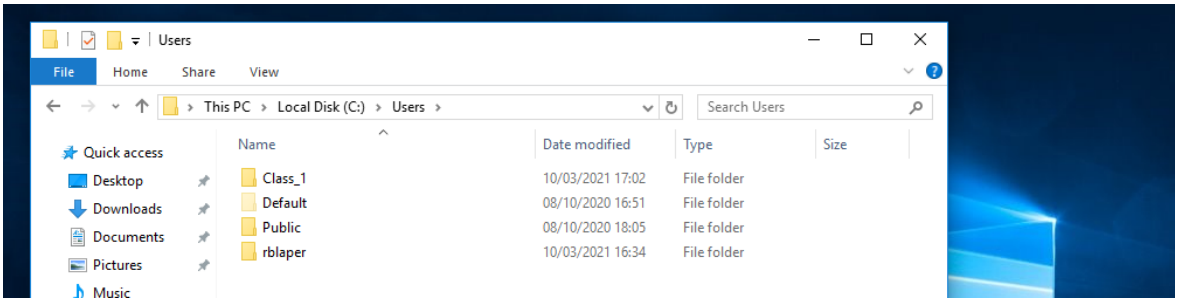
- Verify if the profile folder exists.



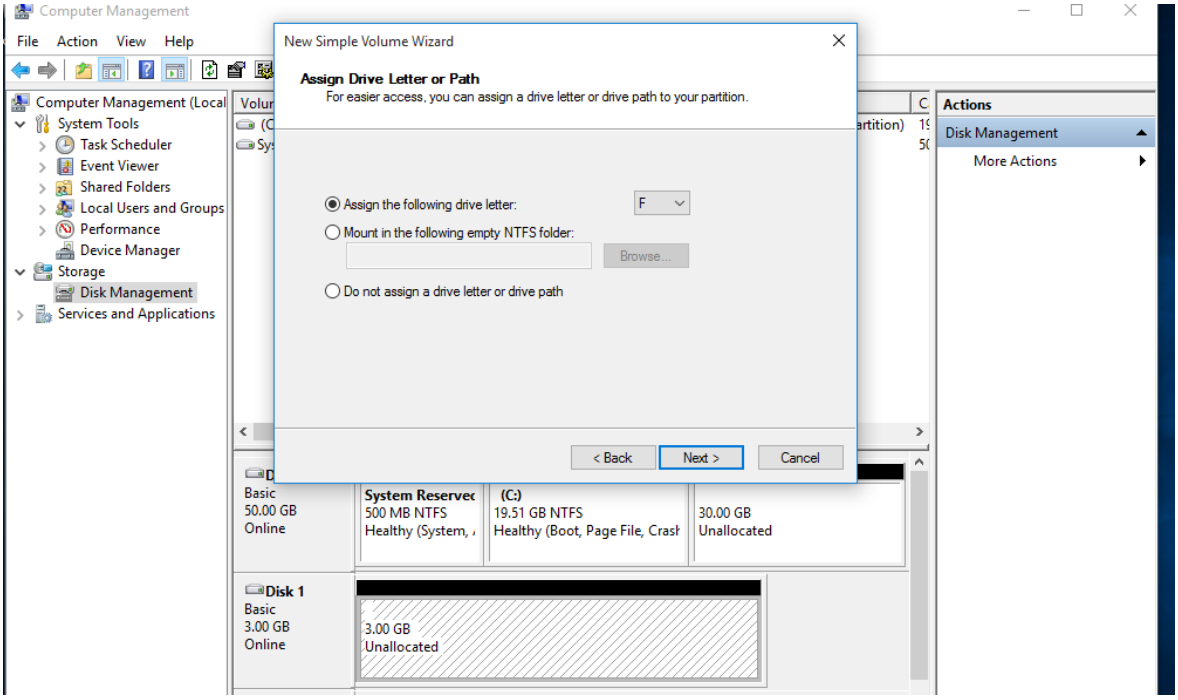
- Log in as "Class_1".



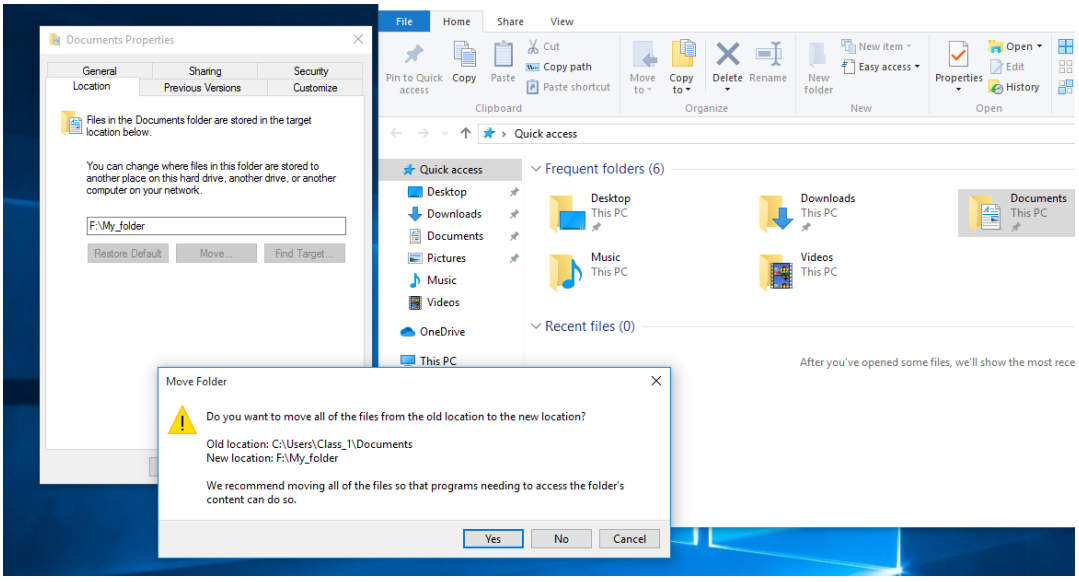
- Verify if the profile folder now exists.

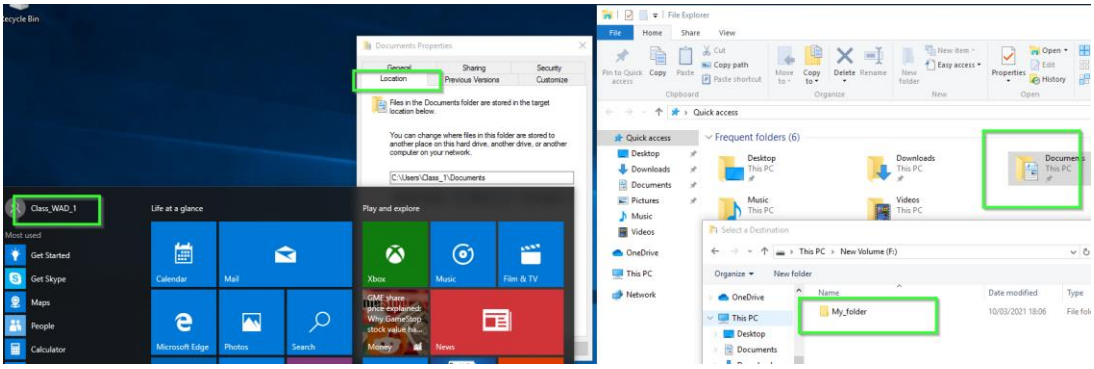


- Add a second hard drive to the virtual machine and create a folder called “My Documents” in F:\

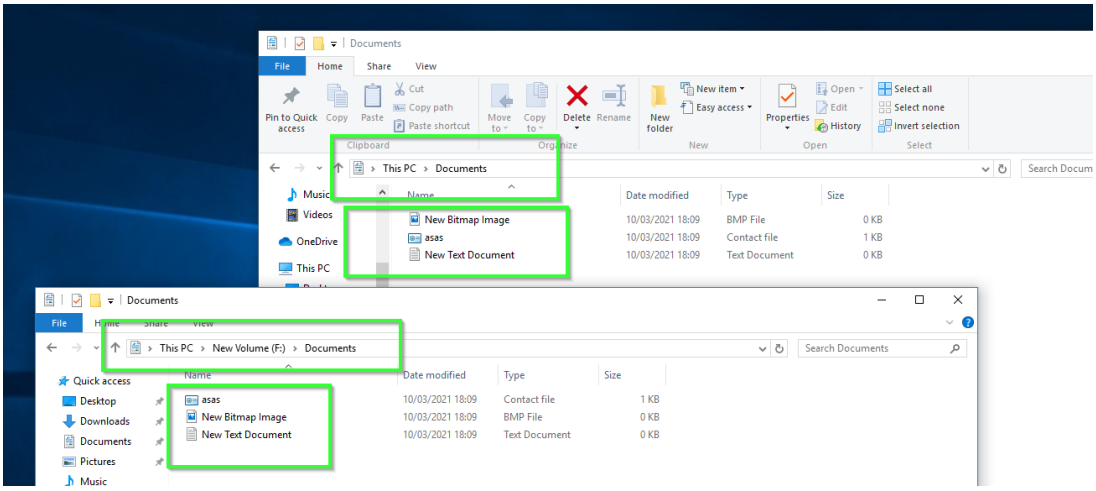


- Move “Class_1” Documents folder to the directory you have just created.





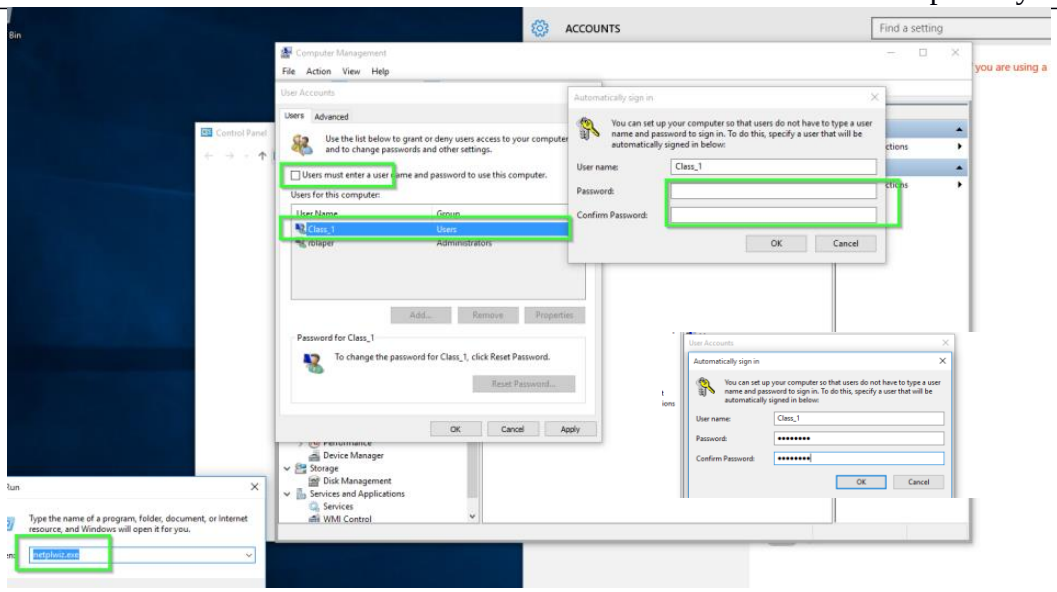
- Open “Documents” shortcut and create a new folder. Check if this folder has actually been created in “F:\My Documents”.



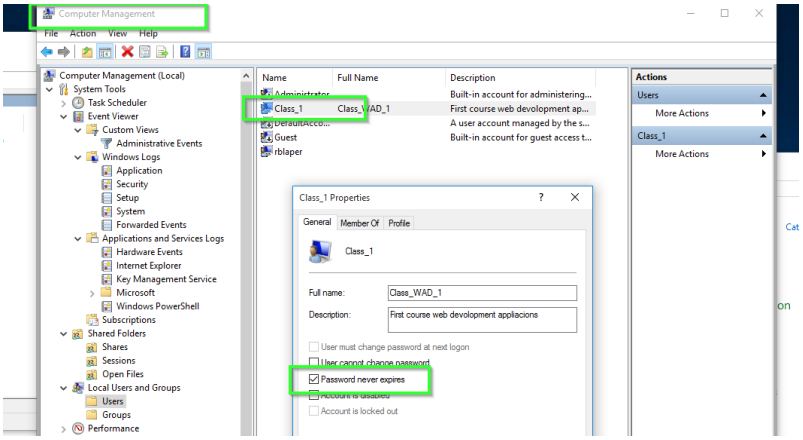
3. How do you configure a user to log in without a password and automatically when turning the computer on?

netplwiz.exe is an Advanced User Accounts Control Panel. It is a little tool that can be used for accounts administration (changing the username or accessing the user credentials, make windows to auto login)

netplwiz.exe



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



Yes

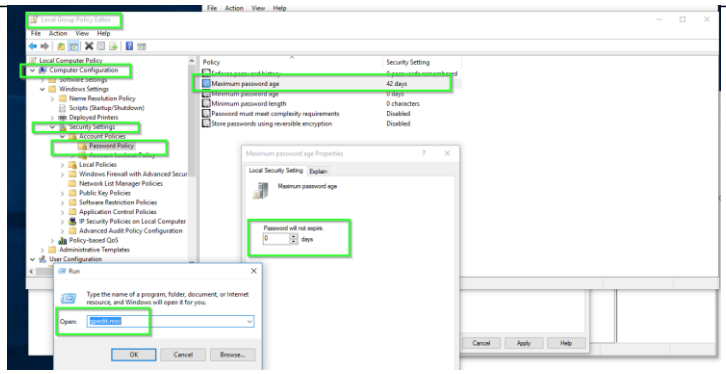
Throw gpedit or secpol

Group Policy Editor (gpedit.msc) and the Local Security Policy (secpol.msc) both are Windows tools used for system security policies administration on systems (for editing registry policies). secpol.msc is a subcategory of gpedit.msc. **gpedit** policies apply to the computer and users in the domain universally and are often set by the system administrator from a central location, whereas **secpol**, set policies relevant to a particular local machine only.

- Gpedit: it is a graphical user interface Windows module for editing registry entries. This tool makes the administration of registry of policies easier, because they are located in many places.
- Secpol; it is a Windows module used for administration of system settings, as well. It is a smaller than gpedit and used to administer a subgroup of entries

Summarizing, gpedit.msc is broader than the secpol.msc, the last one is focused more on security related registry entries.

win key + r **secpol | gpedit**

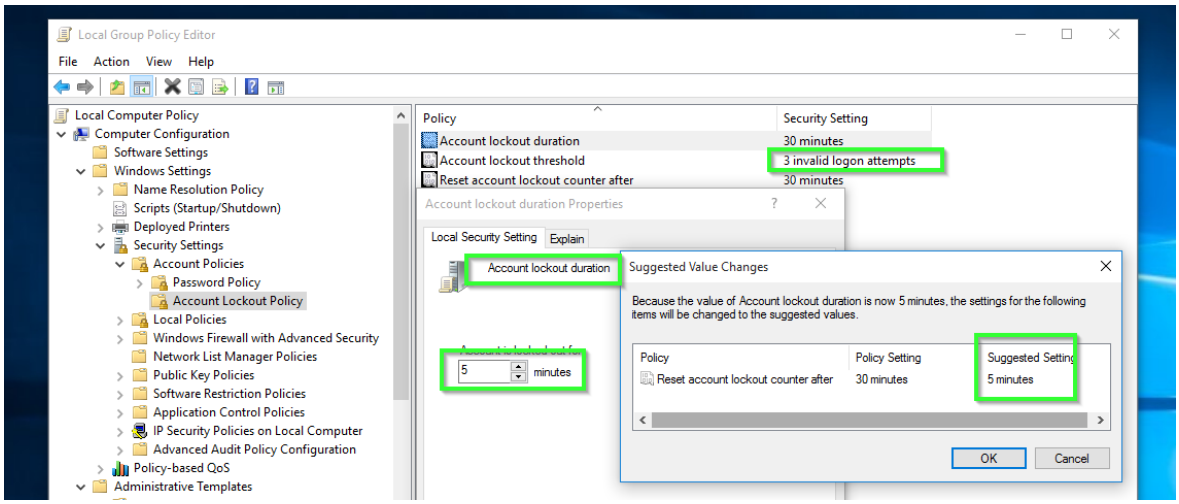


5. When can you use a locked account?

A locked account cannot be used until the administrator reset it or until the number of minutes specified by the Account lockout duration policy setting expires.

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?

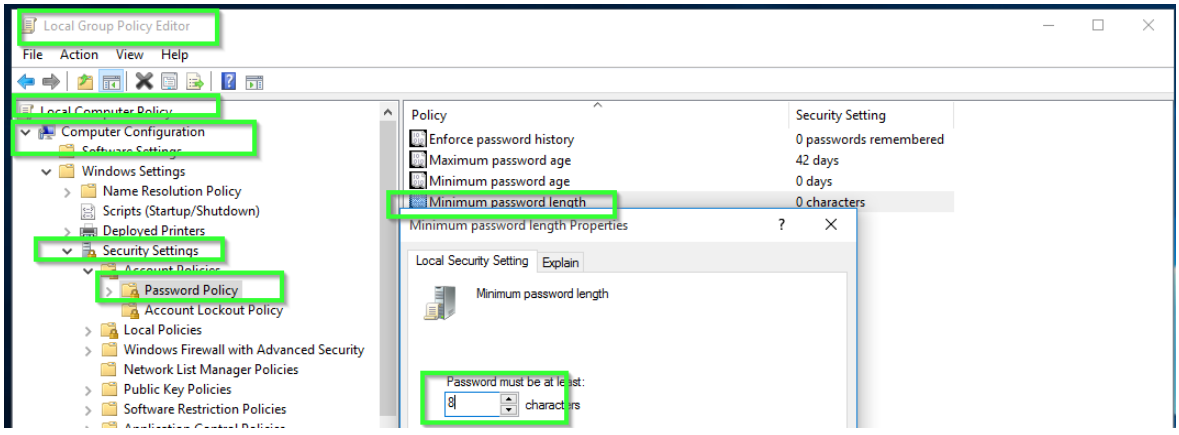
At least 5 minutes.



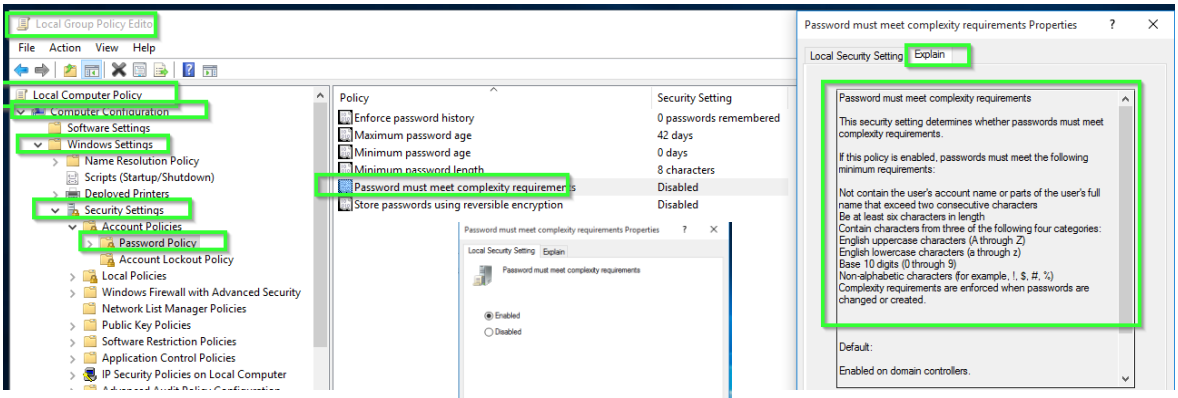
By setting the value to 0, the account will never be locked

7. Configure the system according to the following criteria:

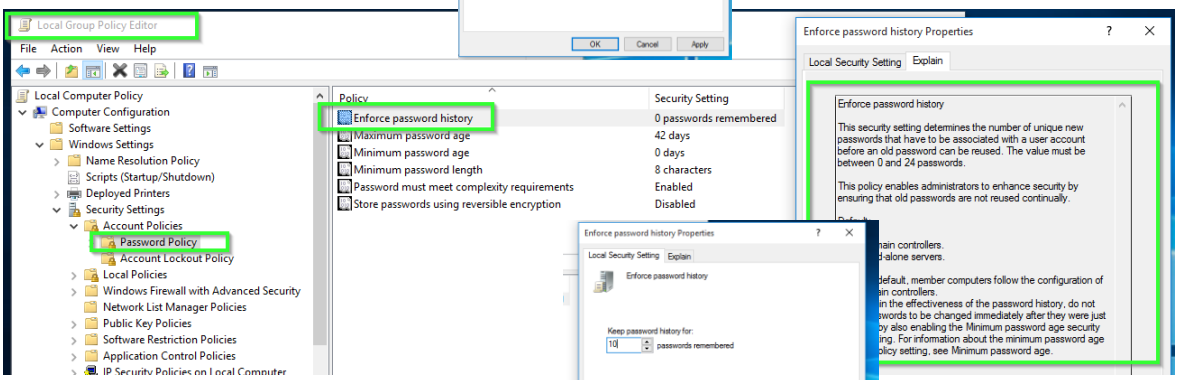
- **All the passwords must have at least 8 characters.**



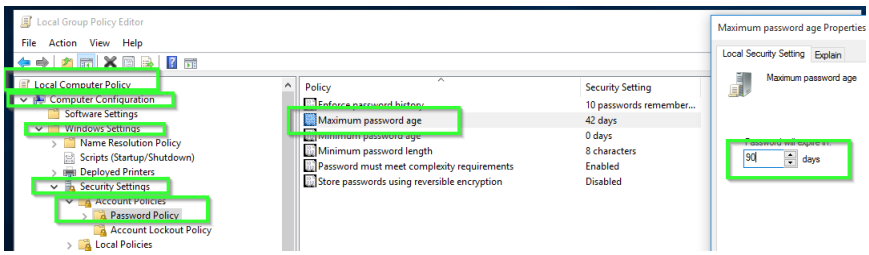
- **All the passwords must contain uppercase, lowercase, numbers and non- alphanumeric characters.**



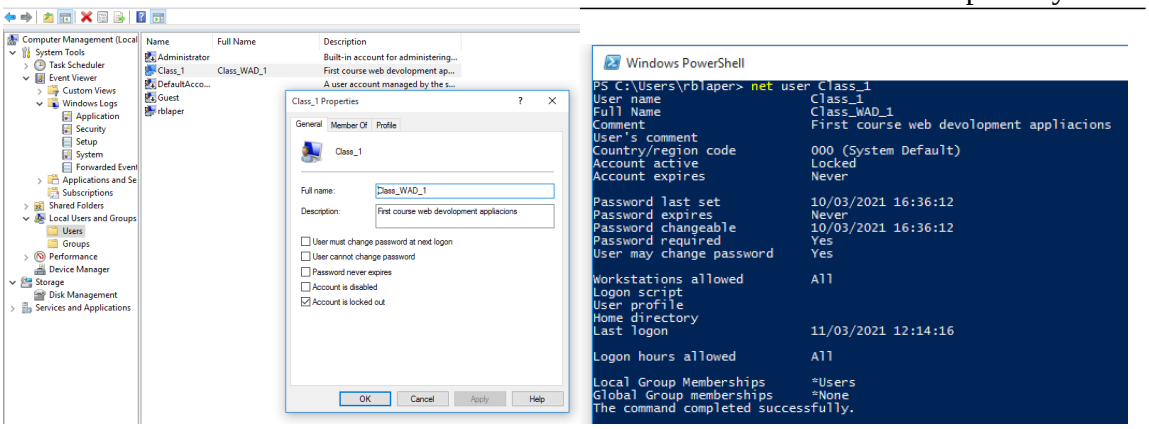
- **The system stores the r each user.**



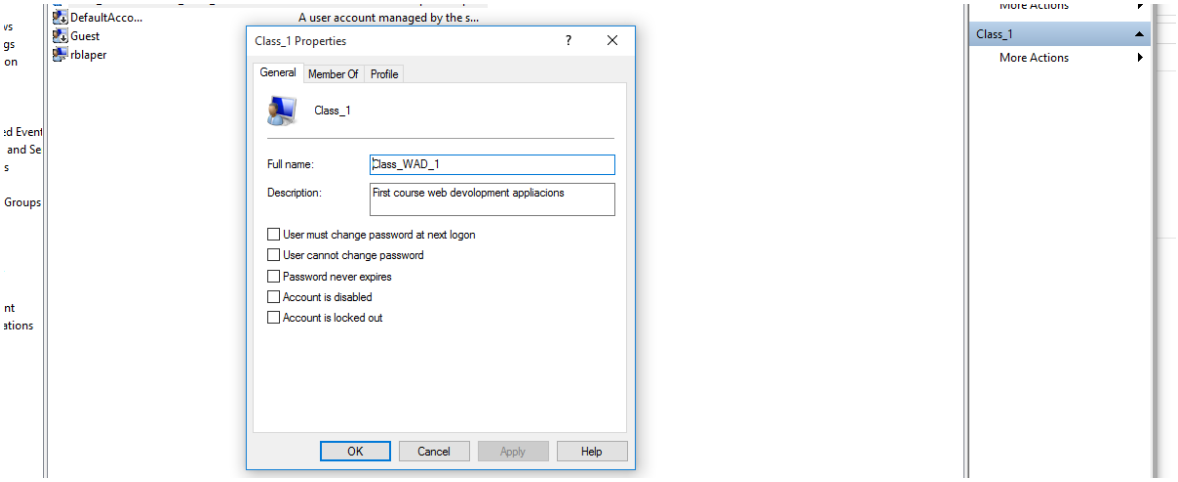
- **All the passwords expire after 3 months.**



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. Complete the following steps:**
   - **Lock the user.**

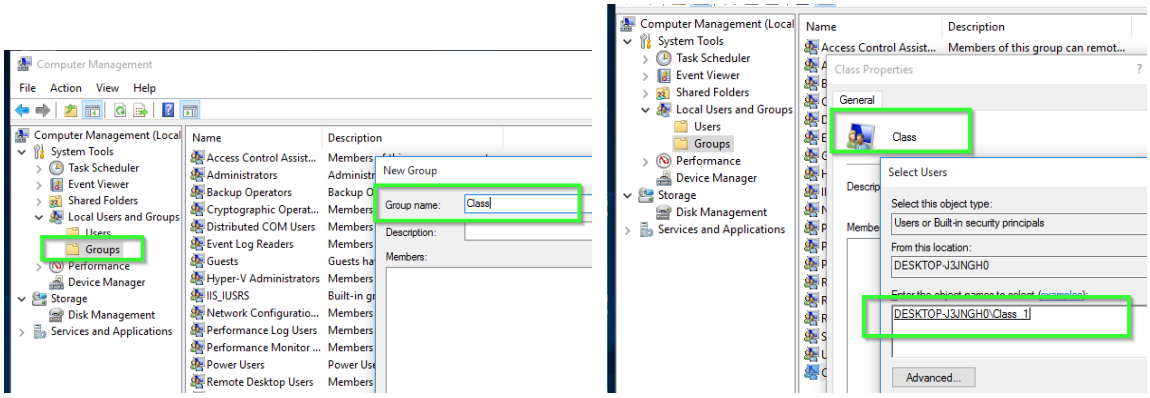


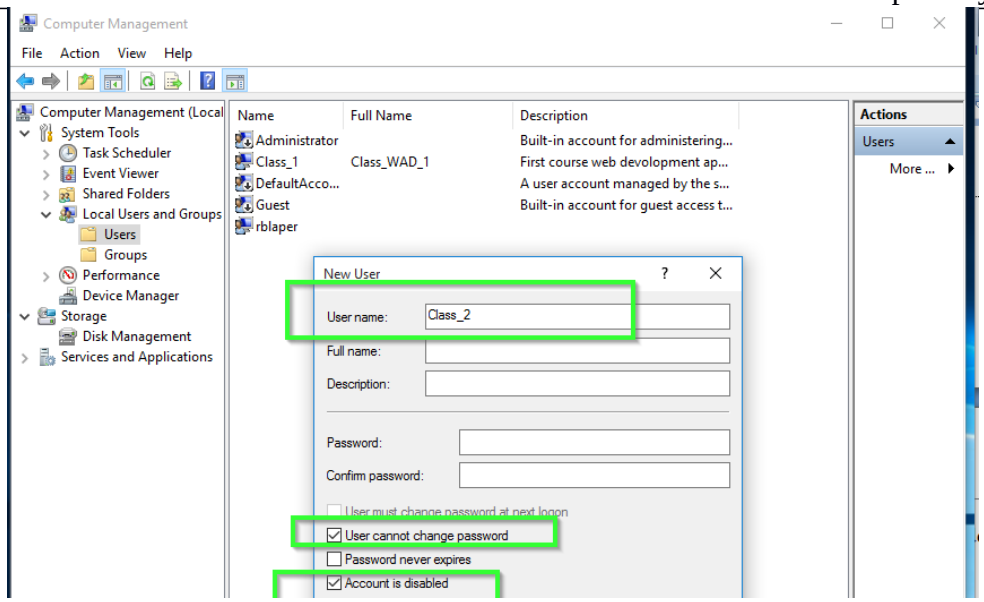
- **Unlock the user as administrator and check if the user is able to log in.**



- **Lock the user again.**
- **Wait for 5 minutes.**
- **Type the right password and check if the user is able to log in.**

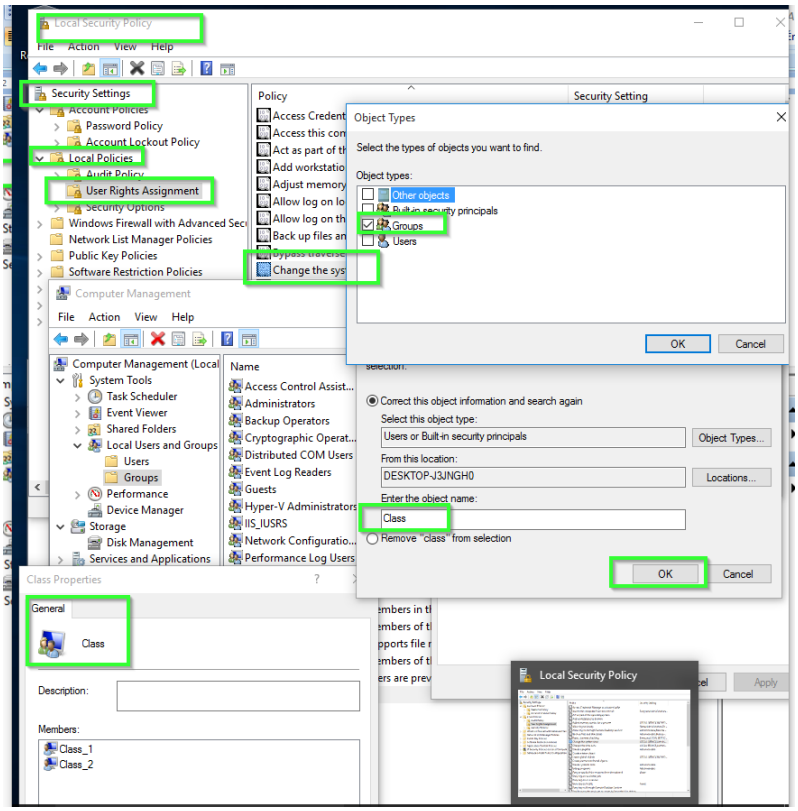
9. **Add a new group name "Class" and complete the following:**
   - **Add the user "Class_1" to the group "Class".**
   - **Create a guest user called "Class_2", initially disabled that cannot change the password. Then, add the user to "Class".**

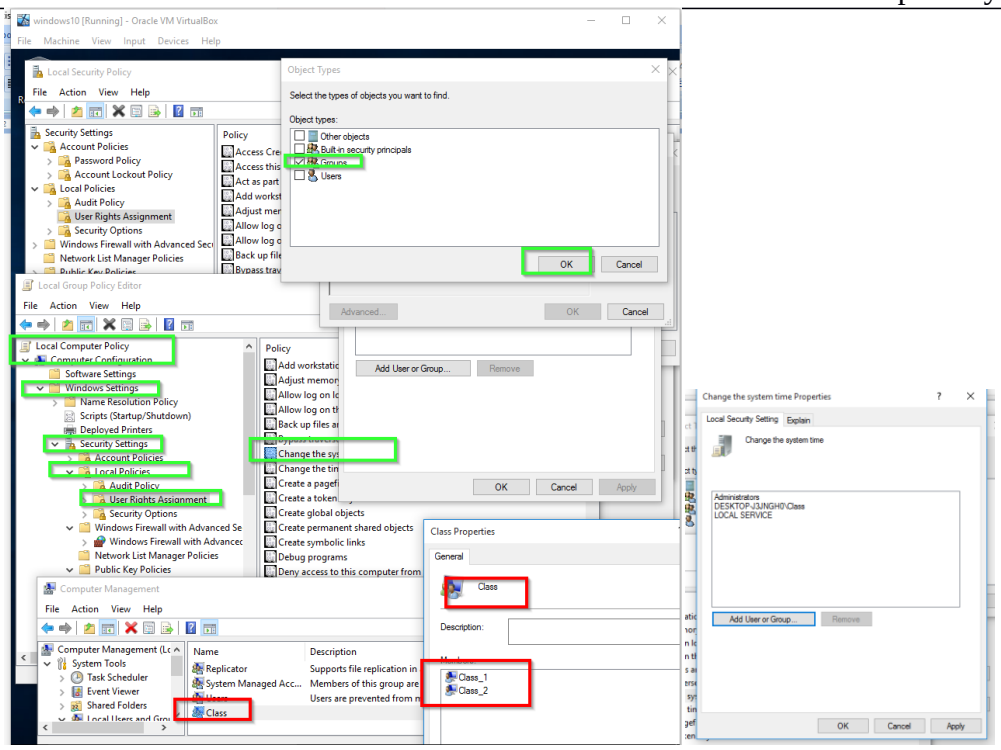




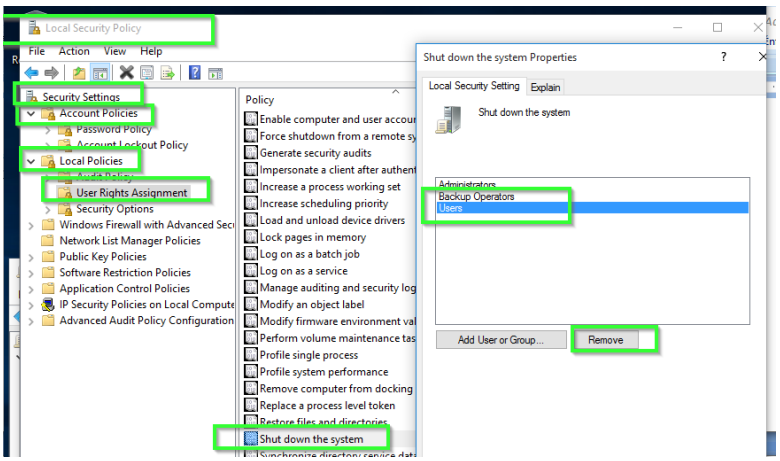
10. **Modify the user rights so "Class_1" and "Class_2" will be able to "Change the system time".**

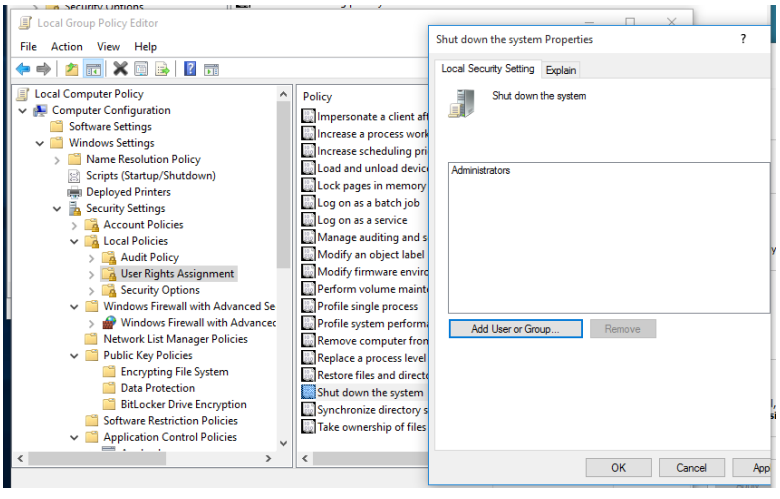
win key + r **secpol | gpedit**





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

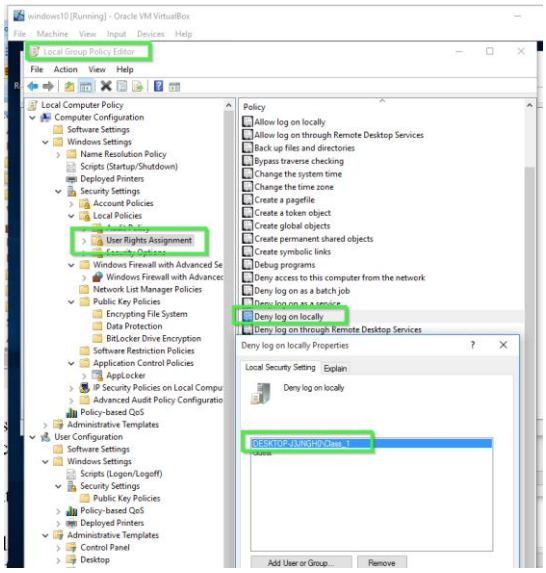


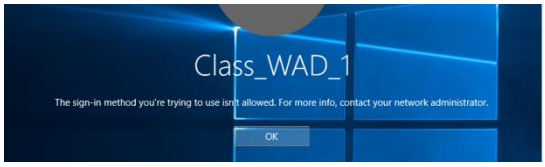


12. Suppose all the standard users are able to log in. How can we deny log on

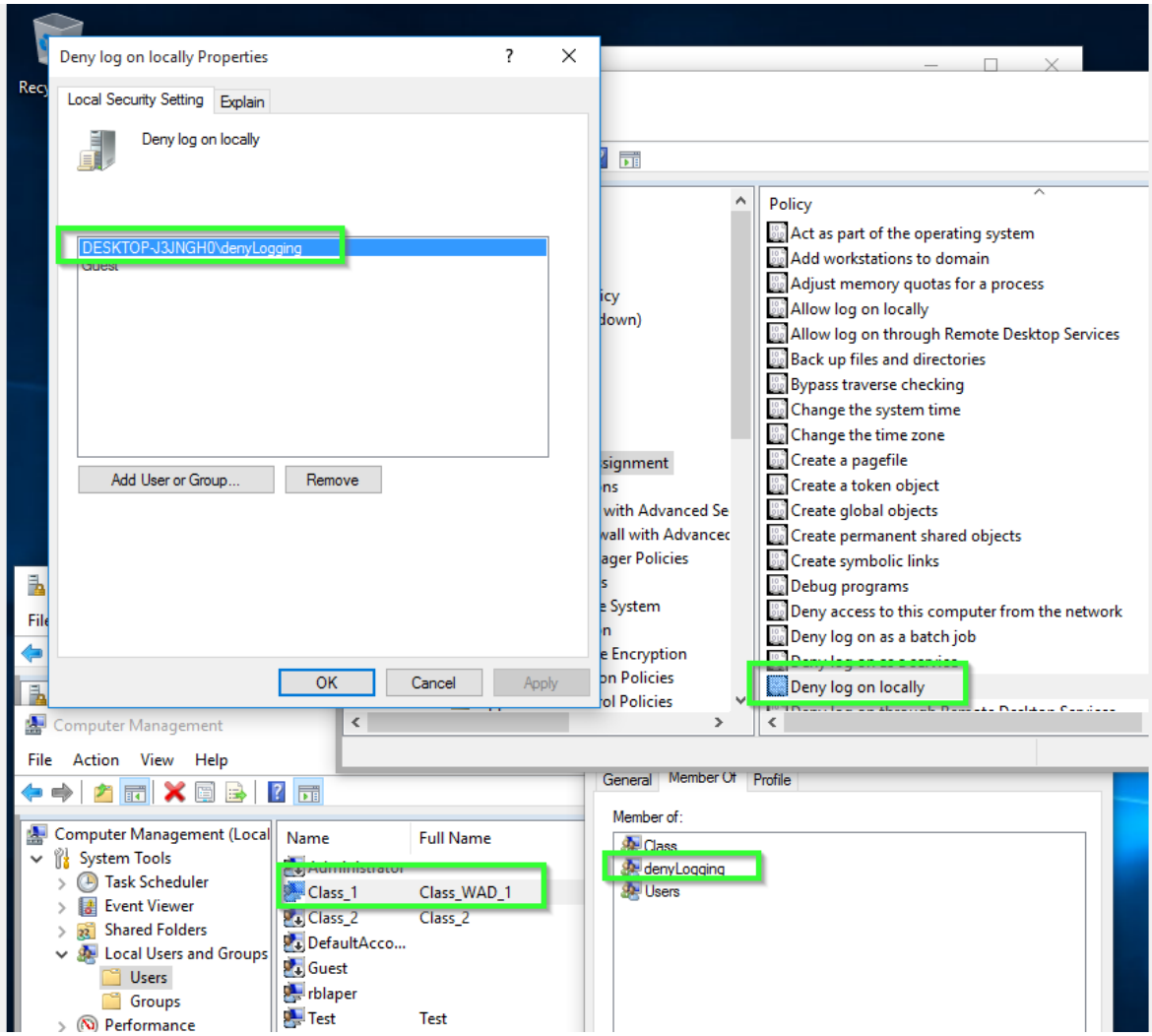
to the specific user “Class_1”?

At user or group level



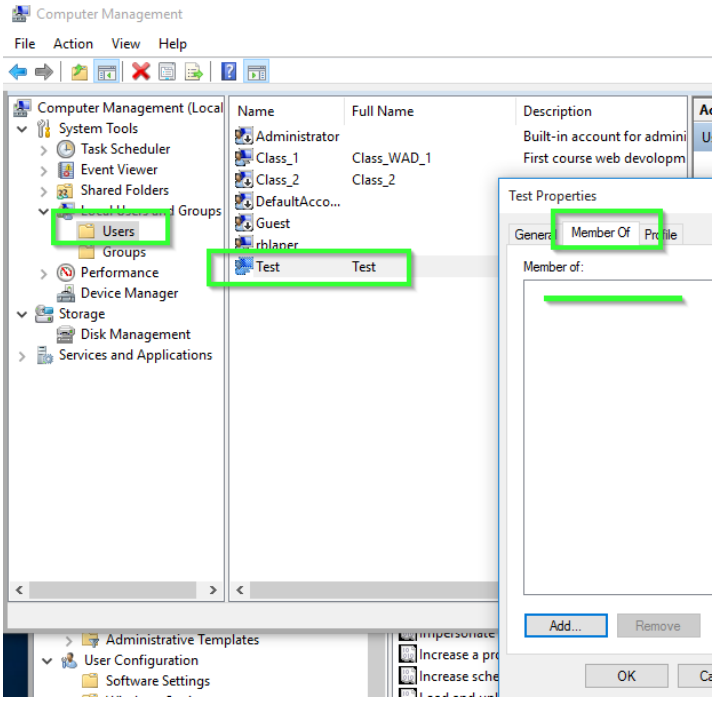


Or at group level. Add group and deny logging throw policies



13. **Overall, add a new user called “Test” according to the requirements in**

exercise 7. What if we deleted "Test" from the group "Users"? Nothing. **Try to log in and explain what happens.** The user is not offered to log



Referencias:

https://networksandservers.blogspot.com/2017/05/gpedit-vs-secpol.html
http://solution.rf.gd/harismuntazir/718/windows-most-useful-and-most-unknown-commands-part-i/?i=1