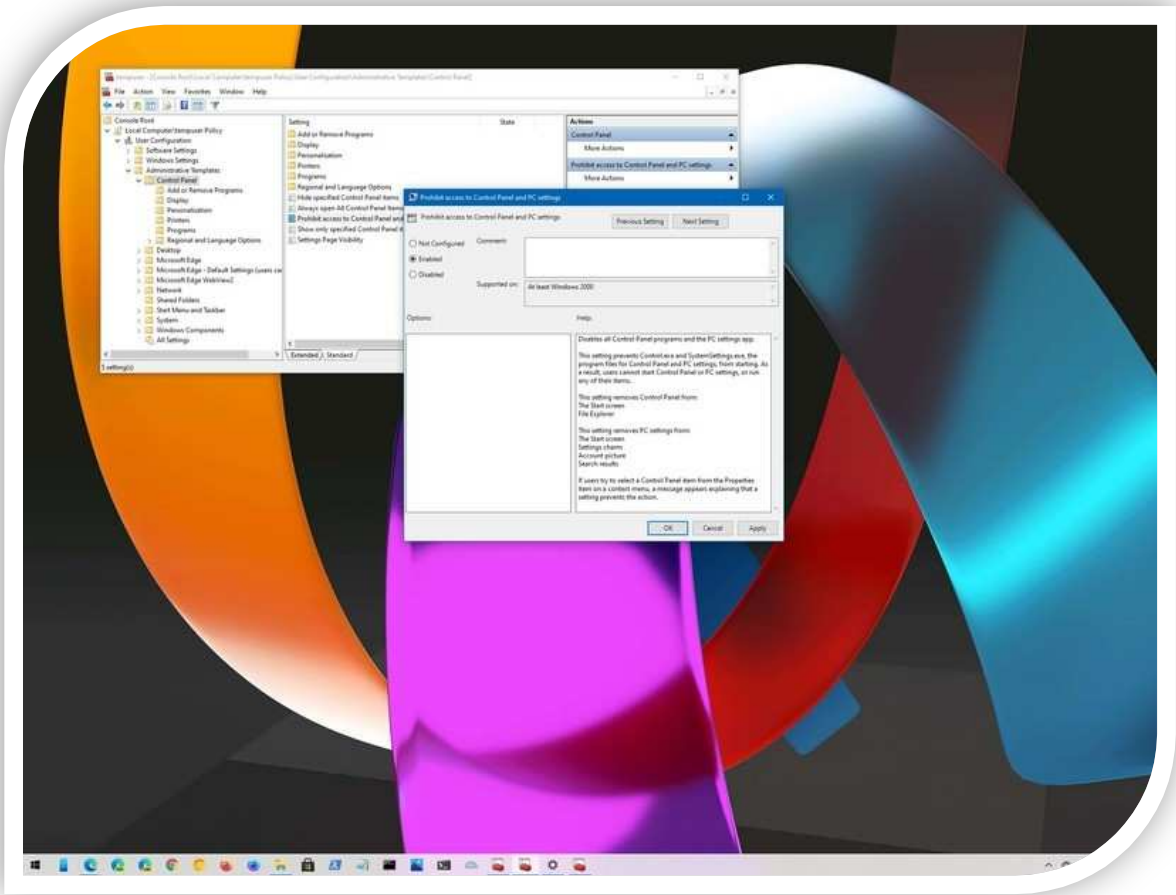
USER, GROUPS AND LOCAL POLICIES



Ana Cifuentes Romero

DW1E – 16-03-2022

INDEX

• 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”.

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.

0. Introduction.

One of the fundamental elements in the administration of a network is the control of users, groups and computers. We must therefore learn how to create, modify, organize and, if necessary, eliminate them. In addition, we will have to assign privileges for each of them, so that we can establish to what extent and under what conditions they will be able to benefit from the resources of the network.

Not always represent specific people, but can also be used as access mechanisms for certain services or applications of the local machine or even a remote computer.

A user account is an object that enables access to domain resources in two different ways:

1.- It allows to authenticate the identity of a user, because only those users who have an account in the system associated with a certain password can log in.

2.- Allows you to authorize, or deny, access to domain resources, because, once the user has logged in, they will only have access to the resources for which they have received the corresponding permissions.

Each user account has a security identifier (SID) that is unique in the domain.

Integrated accounts (are a type of user accounts that are created during installation):

When the domain is created, four new accounts are also created: **Administrator, Guest and Default**. Then, when necessary, the **Help Assistant** account is also created. These are the so-called integrated accounts and have a number of predefined rights and permissions:

Administrator: You have full control over the domain and it cannot be removed or removed from the Administrators group (although we can rename or disable it).

Guest: It is disabled by default and, although not recommended, can be enabled, for example, to allow access to users who do not yet have an account on the system or who have it disabled. By default, no password is required, although this feature, like any other feature, can be modified by the administrator.

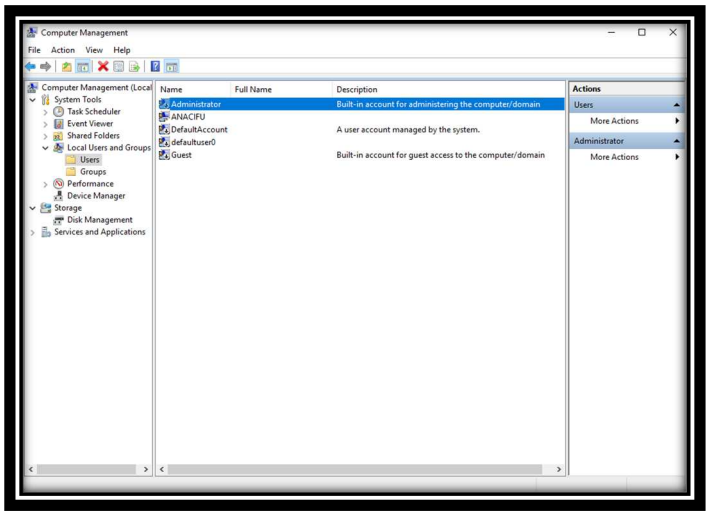
DefaultAccount: also known as Default System Managed Account (DSMA), is a built-in account introduced in Windows 10 version 1607 and Windows Server 2016.

EDefaultAccount is required to run applications manifested by multiple users (MUMA applications). MUMA apps run all the time and react to users signing in and signing in to devices. You can be granted access to resources during offline preparation, even before the account has been created. The account and group are created during the first boot of the machine within Security Account Manager. From the permission perspective, **DefaultAccount is a standard user account** (used for games, calls…).

Defaultuser0 is temporarily created and used while the system is installed. It does not belong to any user and is disabled by default. We don't know the password for the defaultuser0 account even if we want to enable it. In fact, we can delete it.

Help Assistant: Used to start Remote Assistance sessions and has limited access to the computer. It is automatically created when a remote support session is requested and deleted when support requests are no longer available.

Finally, we must bear in mind that even if the Administrator account is disabled, it can still be used to access the domain controller in safe mode.



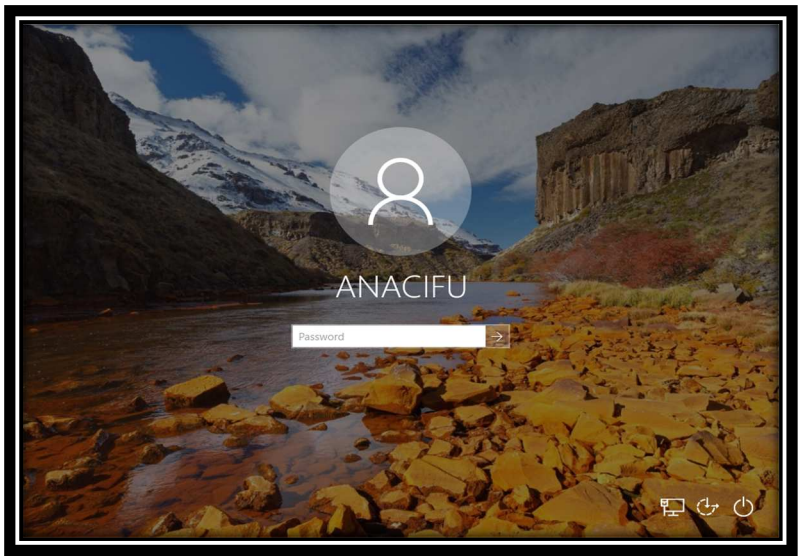
User accounts are also often identified as **security entities**:

User accounts enable individual **users** to log on to the computer and manage resources, while **groups** are used to manage resources for multiple users. The permissions and privileges you assign to user and group accounts determine which actions users can perform, as well as which computer systems and resources they can access.

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.

First thing you have to know is that is necessary to have at least one “Administrator” account. The account that you use when setting up Windows 10 is type Administrator by default (ANACIFU). However, if you add another account, it can be either Administrator or Standard. You can setup your computer with a Microsoft account, or you can skip this step and set up a local account.



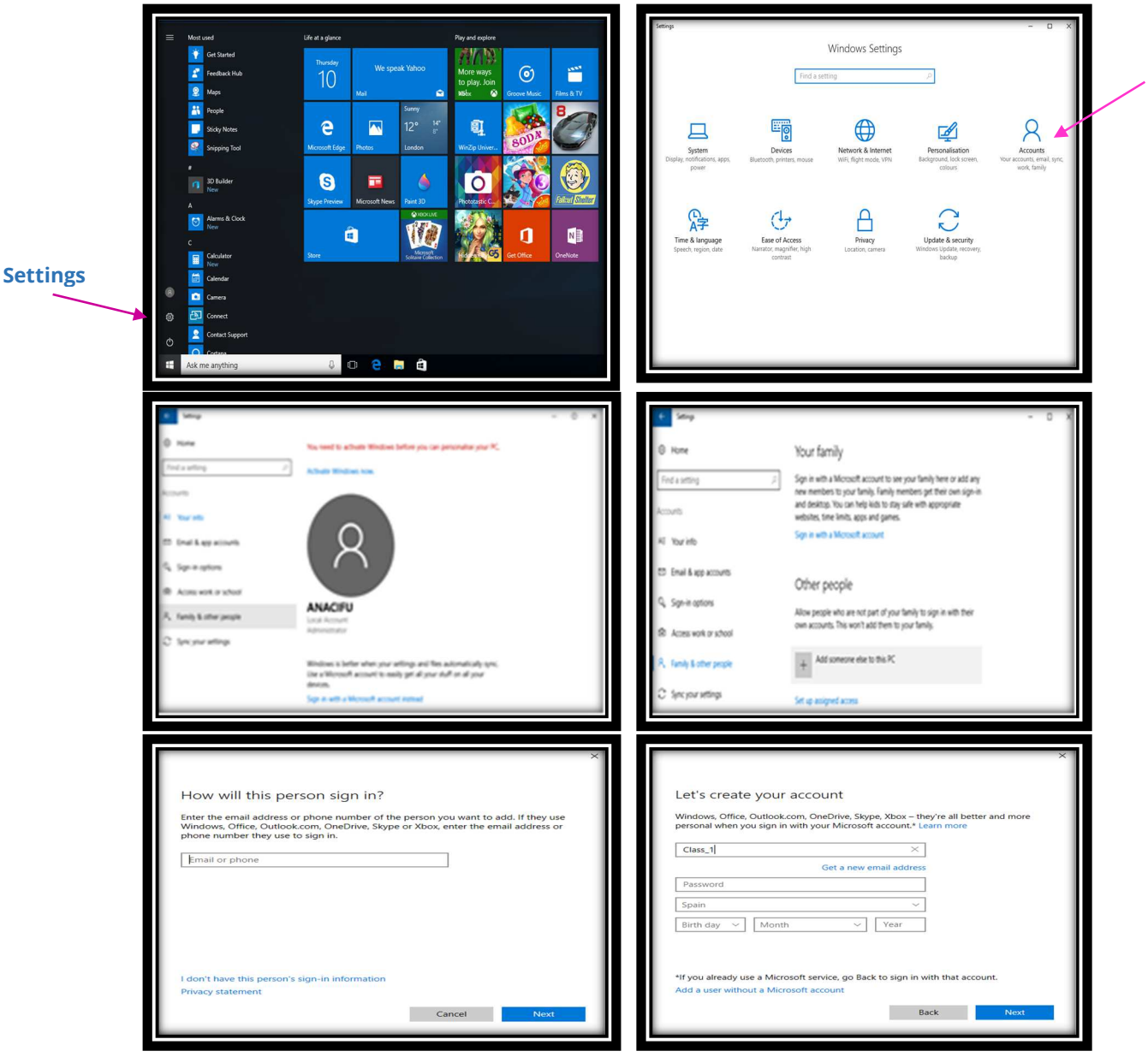
You can add an user in 4 different ways:

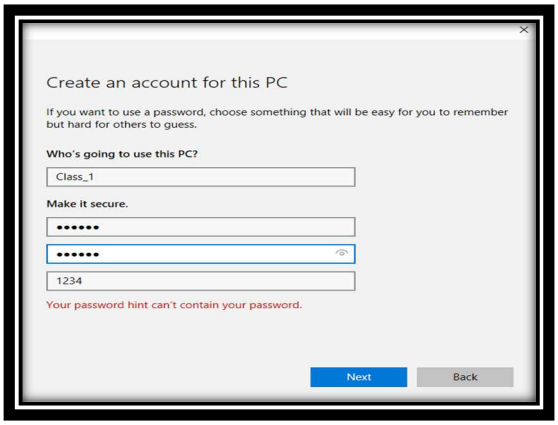
1. Create a Local User Account in Windows 10 from Settings

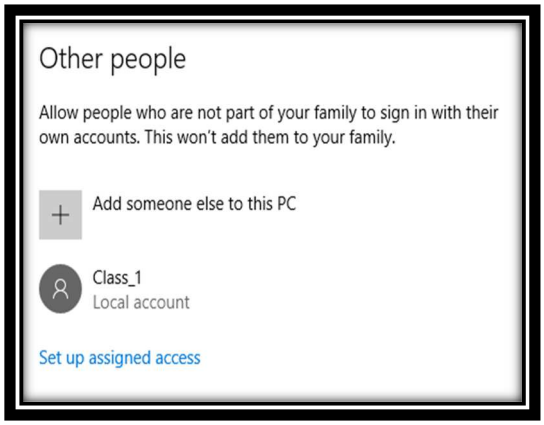
The Settings app in Windows 10 is something that you may already be familiar with. Hence, this would ideally be the most straightforward way to set up a new local user account on your computer.

1. Head to **Start > Settings** > **Accounts.**
2. Next, head over to **Family & other users** from the left pane. Now, click **Add someone else to this PC,** located under Other Users.
3. This will open a tiny window that helps you with the account setup. In typical Microsoft fashion, you will be prompted to use an online account. Select **I don't have this person's sign-in information** instead of entering an email address.

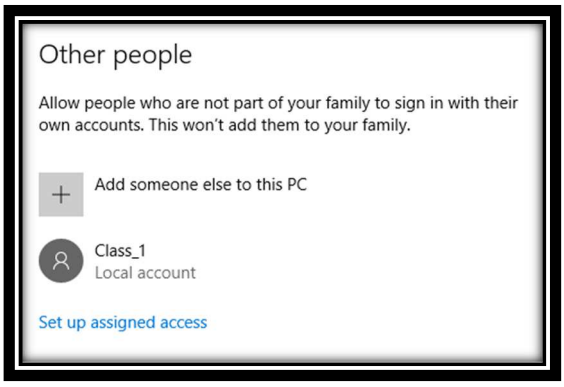
4. Windows will continue to try and get you to create a new Microsoft account. You need to click on **Add a user without a Microsoft account** instead.
5. This will bring up the account setup screen, where you'll be able to fill out all the details for your local account, including security questions that can be used for recovery if you forget the password. Once you're done, click on **Next** button and the user is created.

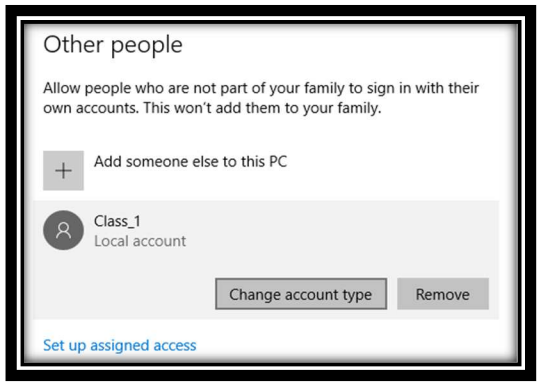




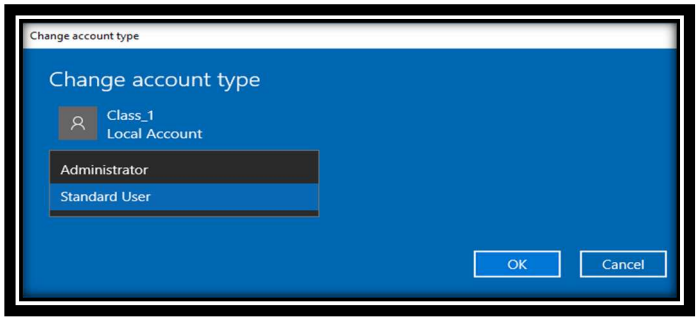


Click on user Class_1 and two options can be chosen: **"Administrator"** or **"Standard User"**.

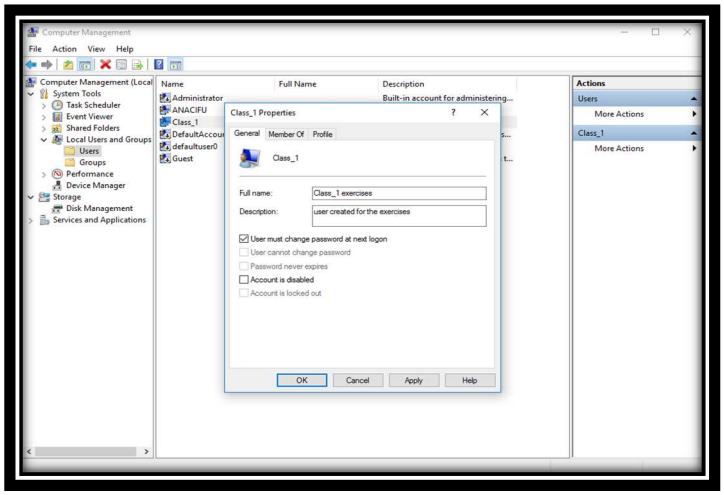


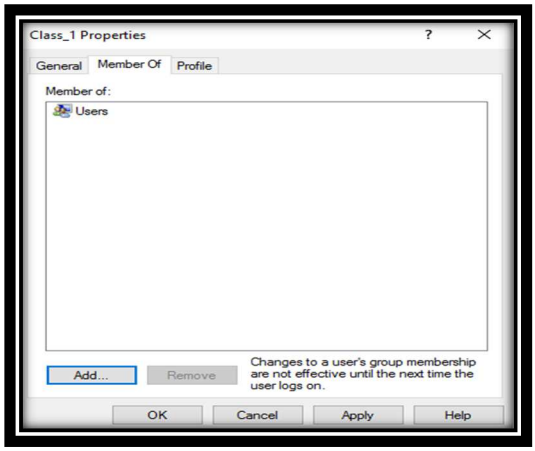


Leave the Administrator account type by default.



You have successfully created a local account at this point. If you head back to the **Family & other people** in the Account Settings menu, you'll find this new account under **Other people**. This is the only method in this list that requires you to add security questions. It can prove to be a lifesaver if you ever forget your password.



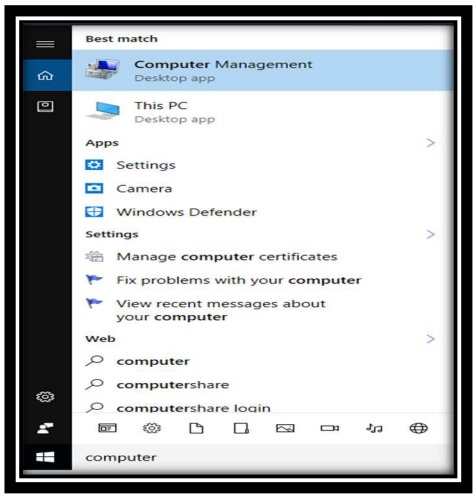


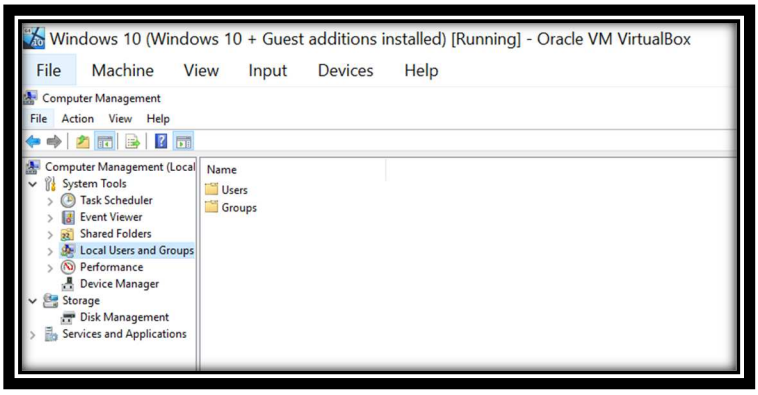
2. Make a Local User Account in Windows 10 With Computer Management.

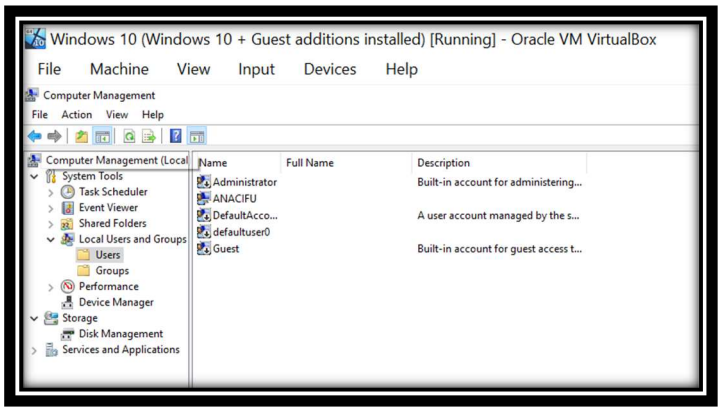
Computer Management is a built-in program that lets you access all the Windows 10 administration tools in one place. From storage management to task scheduling, you can perform many advanced operations on your PC with this app.

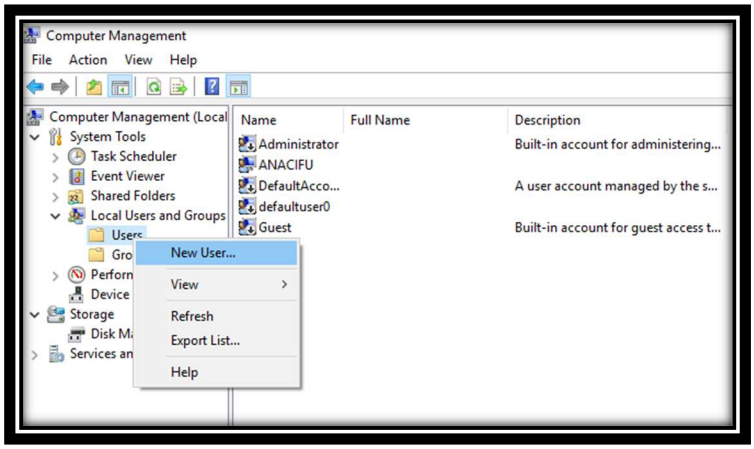
1. Find and open the Computer Management app using Windows Search. Head over to the **Local Users and Groups** section from the left pane. Here, you'll see a folder named **Users**. Right-click on this folder and choose **New User** from the context menu.
2. You know what to do next, right? Fill in your account login information and click on **Create**.

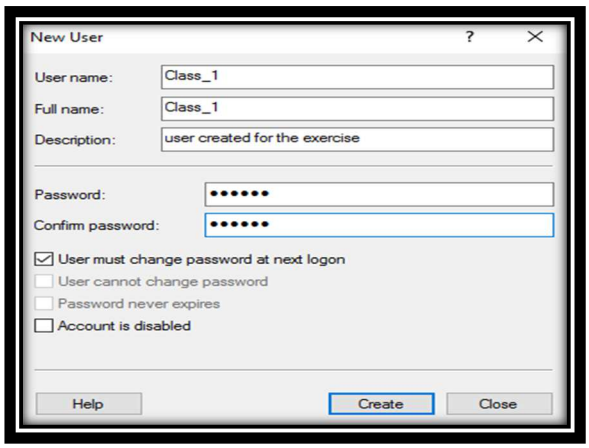
Be careful with the password you choose because there's no option to even enter a password hint here. If you forget it, there's nothing you can do other than deleting it using an administrator account.









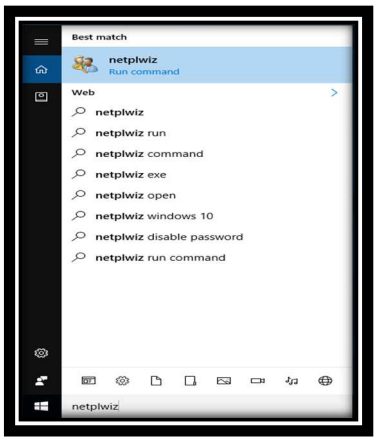


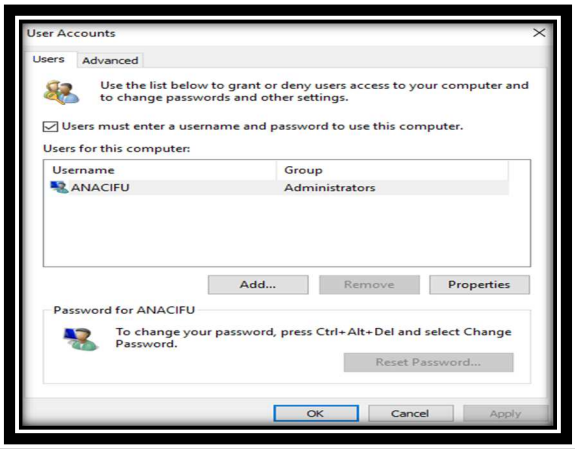
3. Set Up a Local User Account in Windows 10 With Netplwiz.

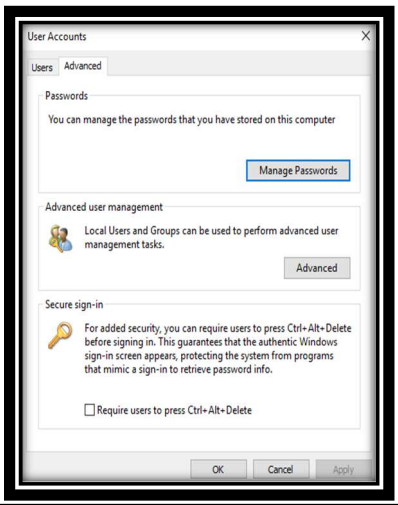
Netplwiz is basically a control panel for managing all the user accounts on a computer. In legacy versions of Windows, users relied on it to add a new user account to their PCs since a streamlined settings menu wasn't available back then. This method is still available as an option. You can use it to add or remove accounts, reset the password, change the account type, and more. To set up a local user account, follow these steps:

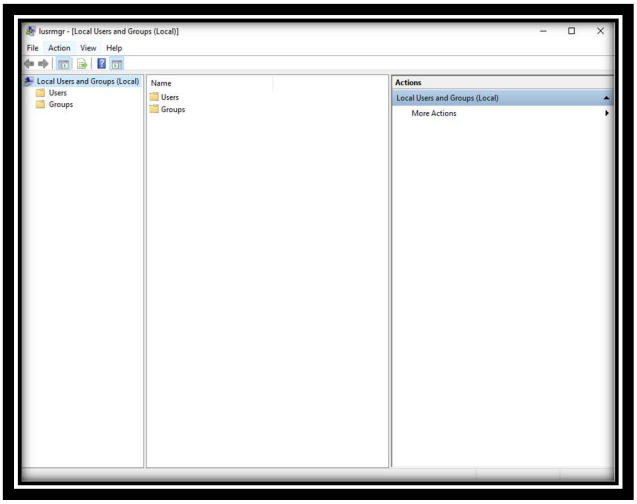
1. Type **Netplwiz** in the Start menu search field. Hit the Enter key to open the panel. Here, you'll see your primary administrator account at the top. Click on **Add** to continue.
2. You'll now see the onscreen instructions that help you set up a new user account. Here, you need to click on **Sign in without a Microsoft account** located at the bottom.
3. Next, you'll be able to select the account type. Click on **Local account** to proceed further.
4. Fill in the login details for your new account, give the desired password hint, and click on **Next** to finish setting up the account.

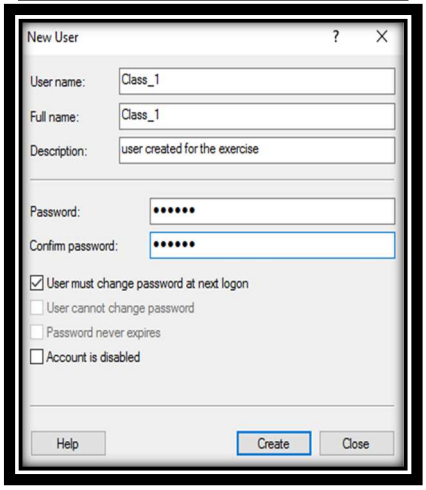
Instead of security questions, you're asked to enter a password hint in this method. This will be the only help you'll get if you ever forget your login information down the line.

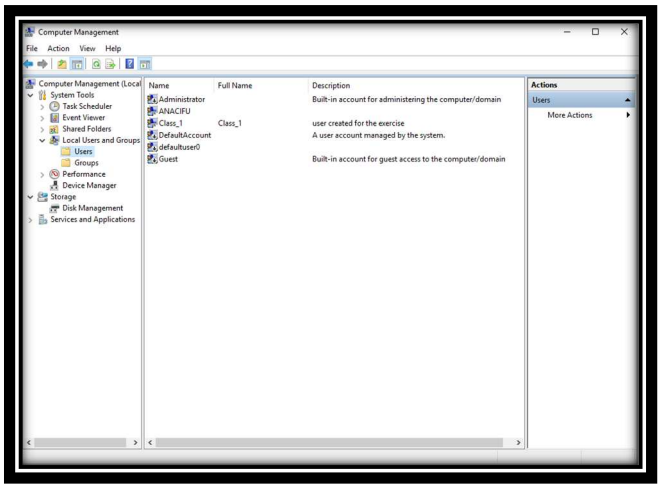




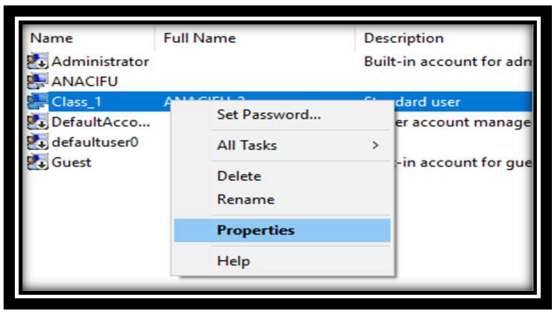


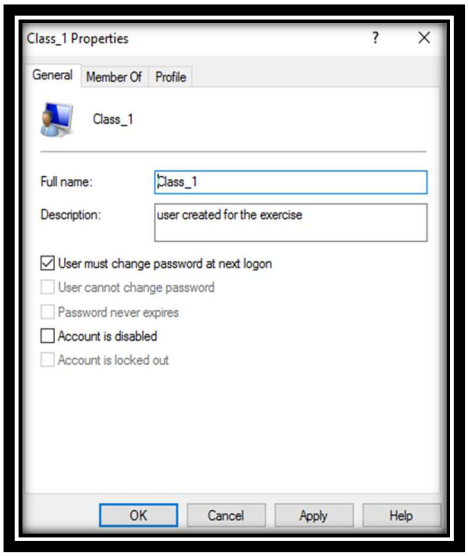






The field “Users must change password at next logon” is checked by default.





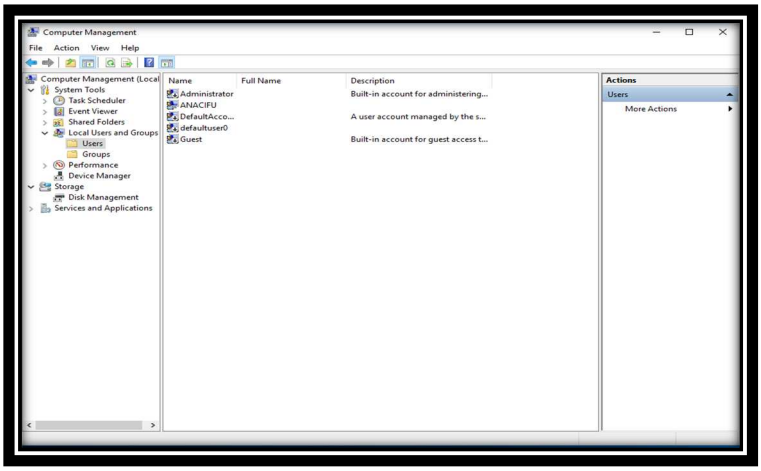
4. Use Command Prompt to Create a Local User Account

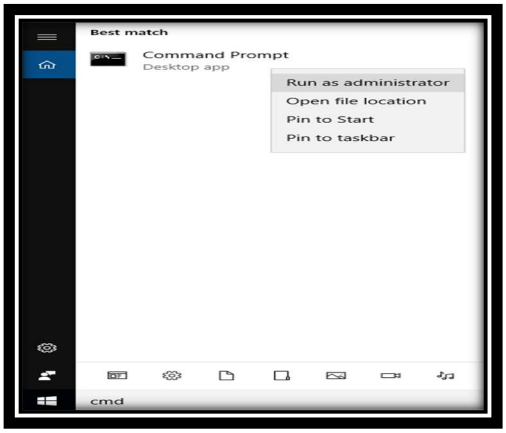
CMD or Command Prompt is a command-line interpreter that's used by tons of coders and other advanced users to perform crucial tasks on their PCs. Using CMD is arguably the fastest way to make a new local user account since all you need to do here is enter a proper line of code. You don't have to fill out too much information.

A. Type **CMD** in the Start menu search bar, and select Command Prompt as the Best match. Now, make sure to choose **Run as administrator**. If you fail to do this, you won't be allowed to make a new account.

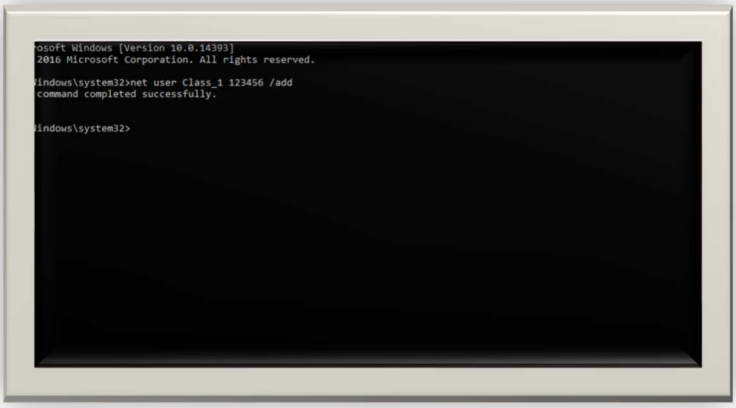
B. Now, type in the following line of code, replacing **username** and **password** in the command line to match your account requirements. Hit the Enter key.

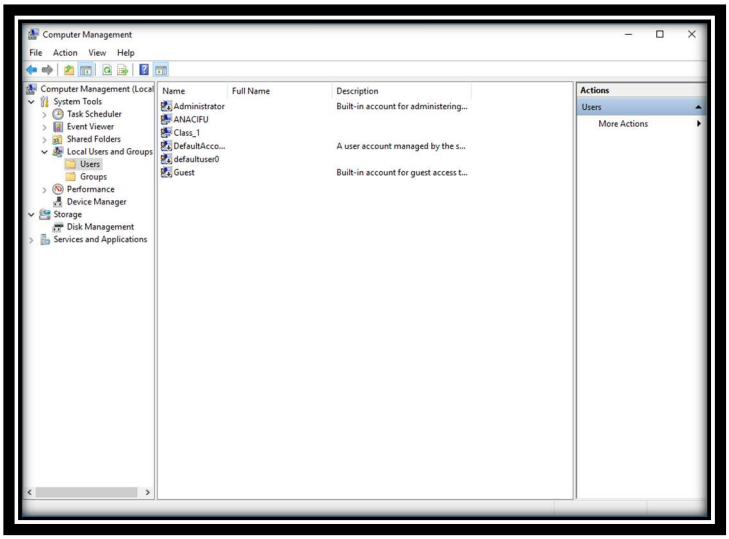
If you get a response that "The command completed successfully," it means that the account has been created. You can log out and switch to this new account right away. Since you're not prompted to retype the password for verification, you need to be extra careful not to make any typos.



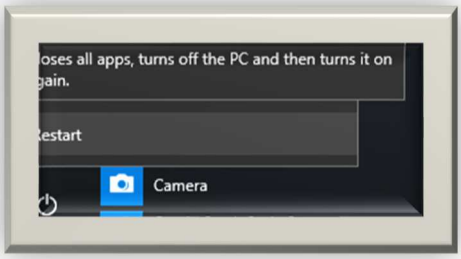


You have to write net user Class_1 123456 /add (net user [user_name] [password] /add in order to create the user.

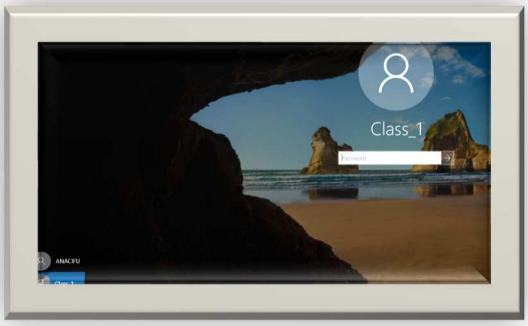




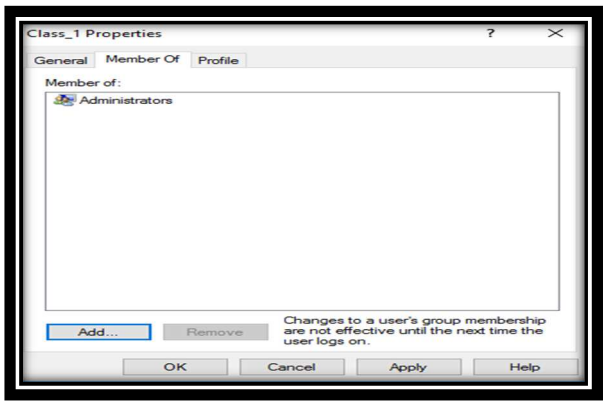
After that, you have to restart the computer to finish configuration on the user.



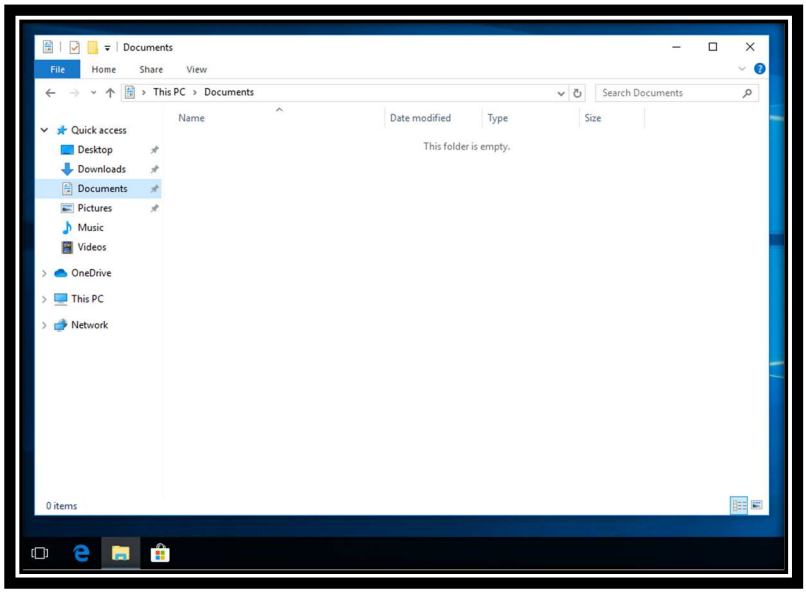
Now, when you try to enter, it asks you to change the password and once done, it allows you to access the computer.

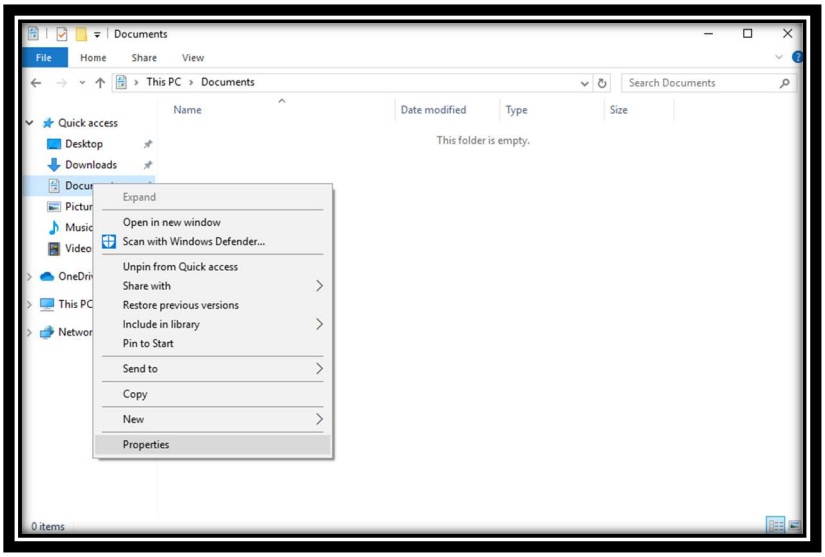


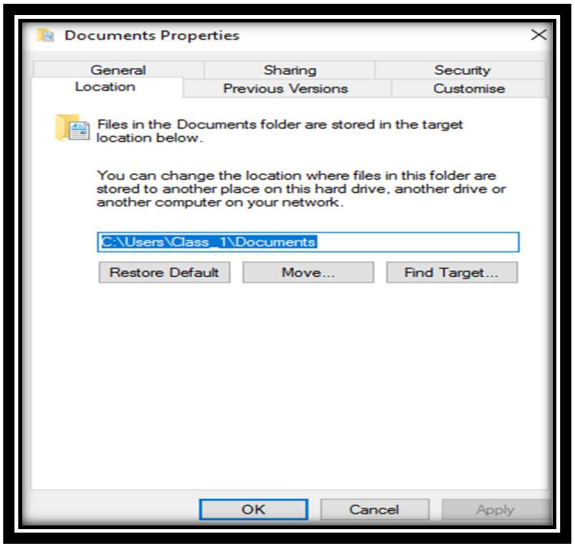
The user **Class_1** that is created as **standard** and by default becomes part of the **Users** group. Now, from "Computer Management->Local users and groups->Class_1 right-click of the mouse-> Properties you will change to the **Administrators** group, removing the Users group from Class_1 and adding the administrators group.

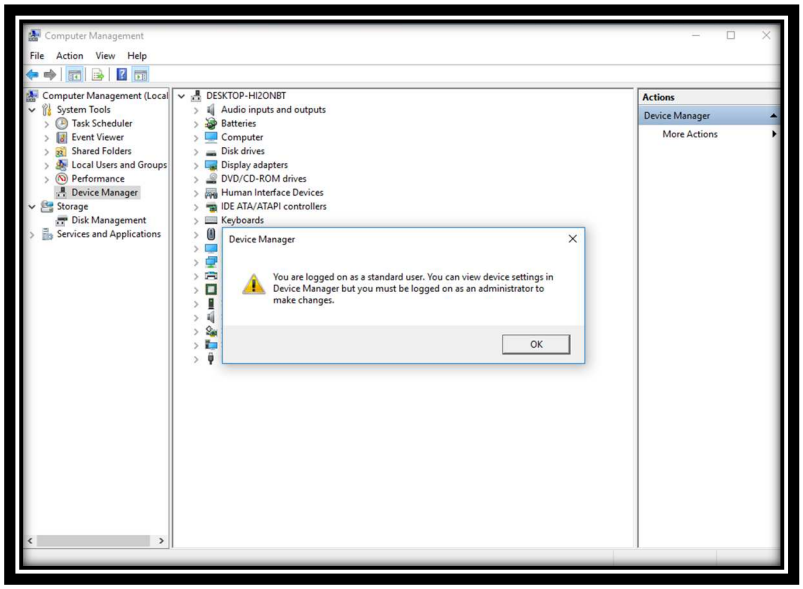


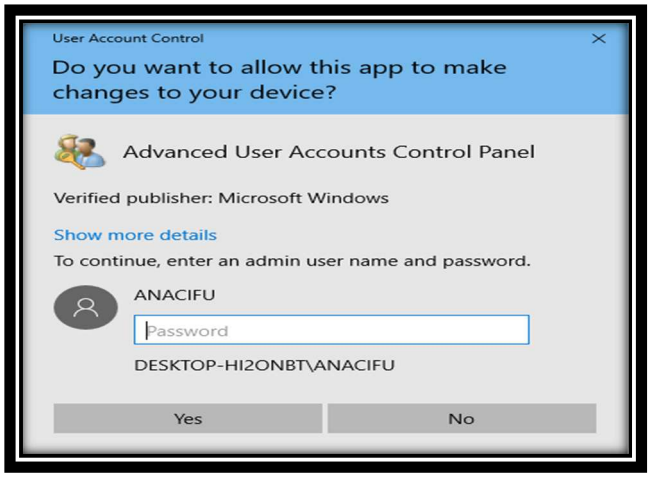

Best match
Computer Management
Desktop app
This PC
Desktop app
Apps
Settings
Camera
Windows Defender
Control Panel
Web
computer
computershare
computershare login
computer desk
computer chair
computer mouse
computer


Documents
File
Home
Share
View
This PC › Documents
Search Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
This folder is empty.
0 items


Documents
File
Home
Share
View
This PC › Documents
Search Documents
Quick access
Desktop
Downloads
Name
Date modified
Type
Size
This folder is empty.
Expand
Open in new window
Scan with Windows Defender...
Unpin from Quick access
Share with
Restore previous versions
Include in library
Pin to Start
Send to
Copy
New
Properties
0 items


Documents Properties
General
Sharing
Security
Location
Previous Versions
Customise
Files in the Documents folder are stored in the target location below.
You can change the location where files in this folder are stored to another place on this hard drive, another drive or another computer on your network.
C:\Users\Class_1\Documents
Restore Default
Move...
Find Target...
OK
Cancel
Apply

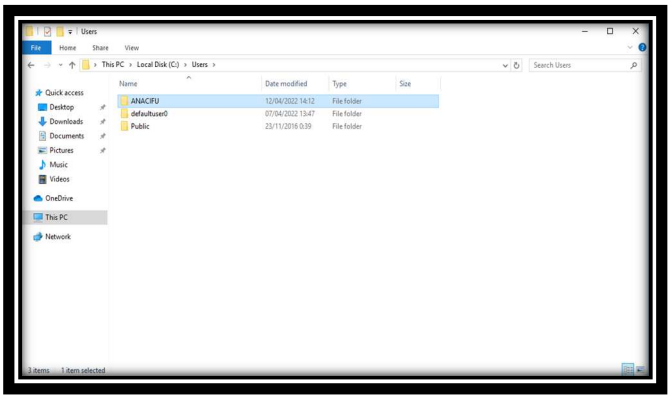

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
DESKTOP-HI2ONBT
Audio inputs and outputs
Batteries
Computer
Disk drives
Display adapters
DVD/CD-ROM drives
Human Interface Devices
IDE ATA/ATAPI controllers
Keyboards
Device Manager
You are logged on as a standard user. You can view device settings in Device Manager but you must be logged on as an administrator to make changes.
OK
Actions
Device Manager
More Actions



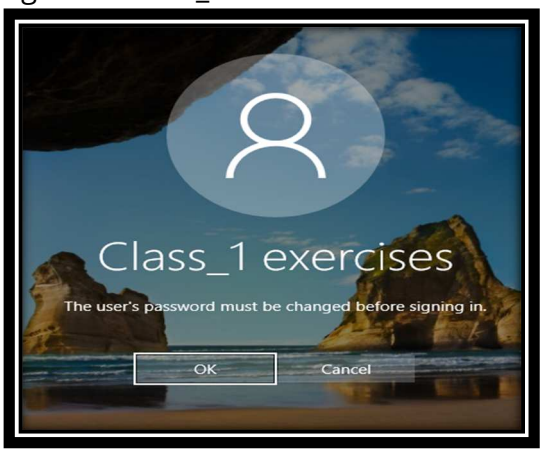
2.- Complete the following parts about the user “Class_1” from the previous exercise.

1. Verify if the profile folder exists.
2. Log in as “Class_1”.
3. Verify if the profile folder now exists.
4. Add a second hard drive to the virtual machine and create a folder called “My Documents” in F:\
5. Move “Class_1” Documents folder to the directory you have just created.
6. Open “Documents” shortcut and create a new folder. Check if this folder has actually been created in “F:\My Documents”.

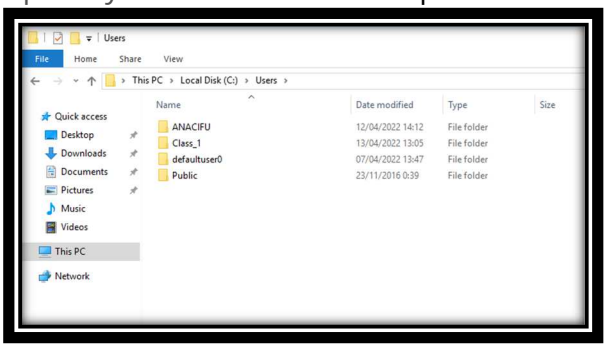
The profile folders are not created until you first log in. You can check C:\Users\Class_1. It will only exist when you log in at least once.



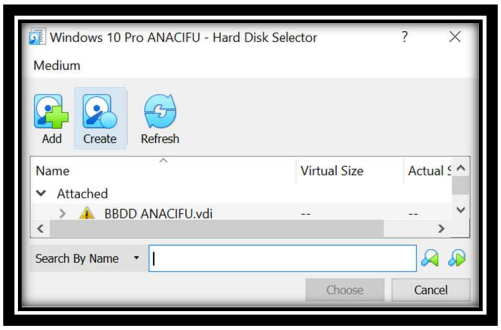
Log in as “Class_1” the first time.

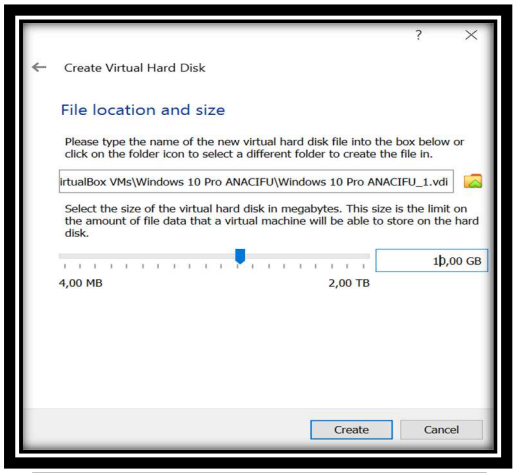


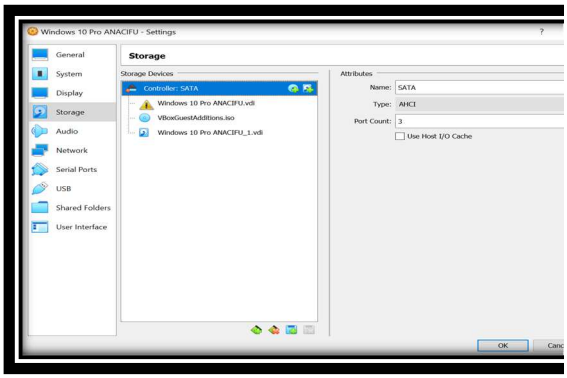
After restart the computer you can check that the profile folder now exists.

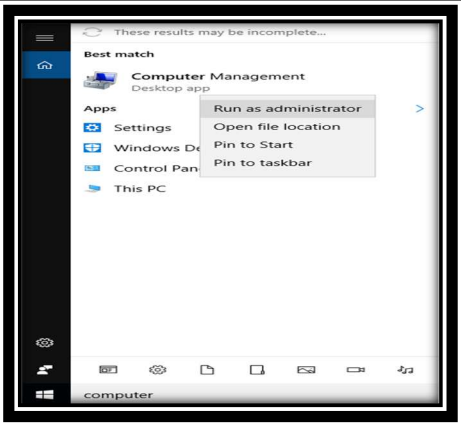


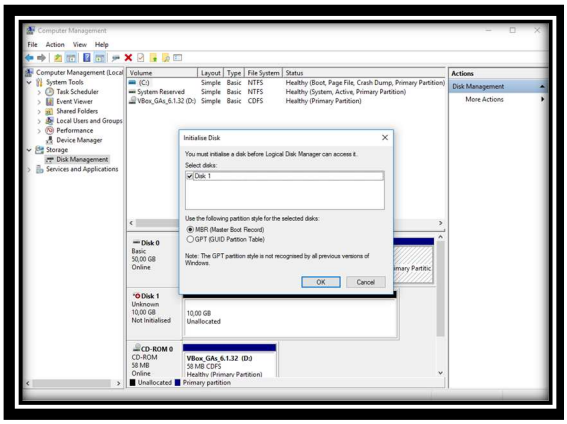
After that, we add a second hard drive to the virtual machine and create a folder called “My Documents” in F:\. Create a simple volume in the letter F. Then, you will see the new Simple volume of 10GB. You can change the name of new volume.



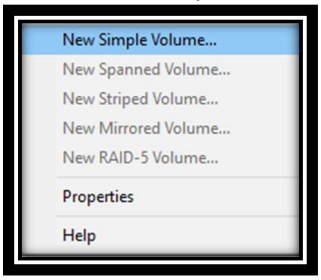


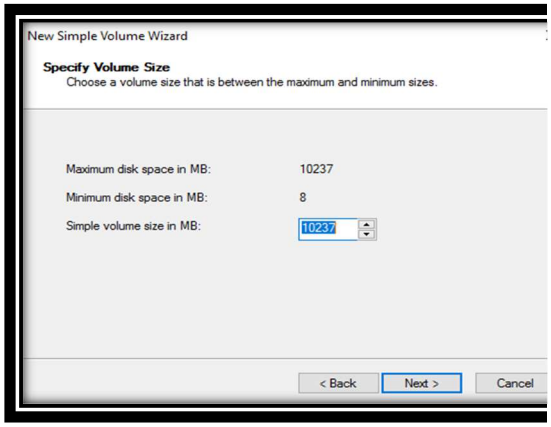


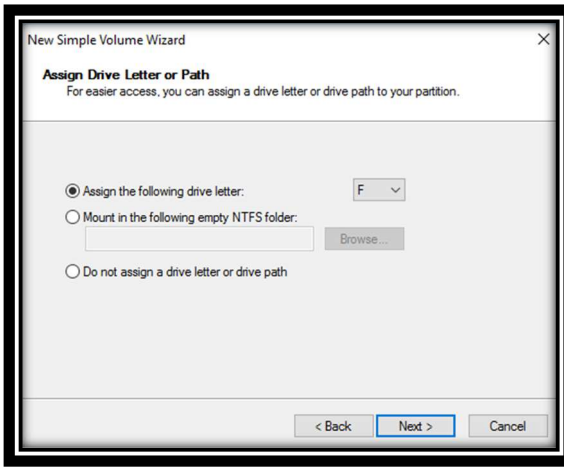


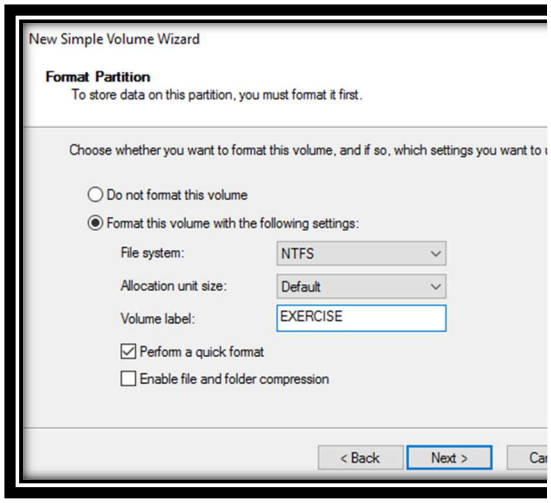


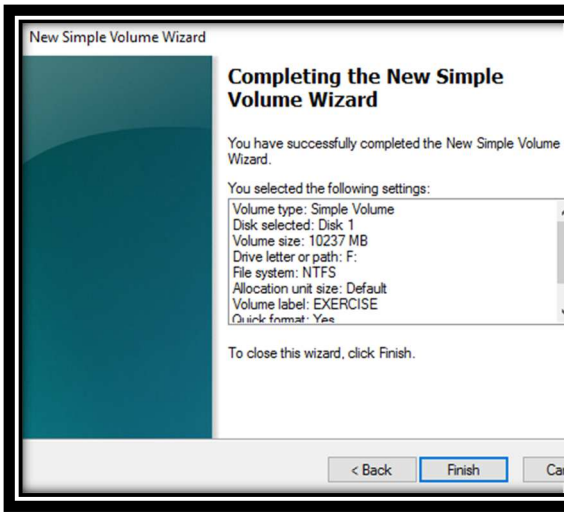
Click on unallocated space of the disk

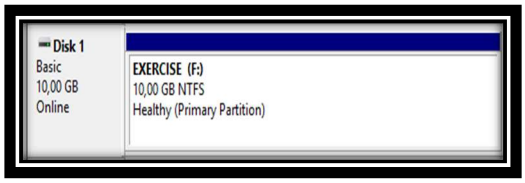




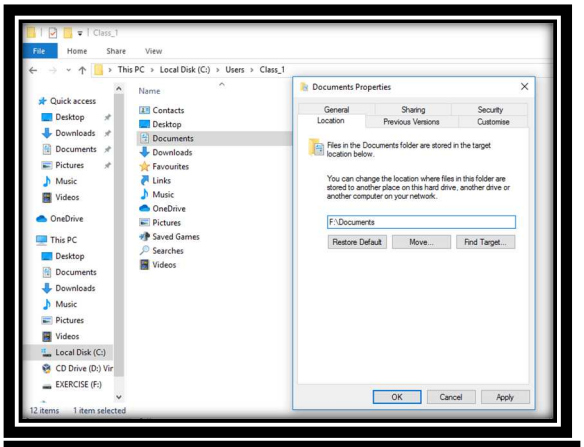


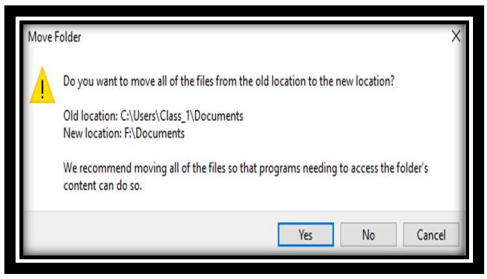


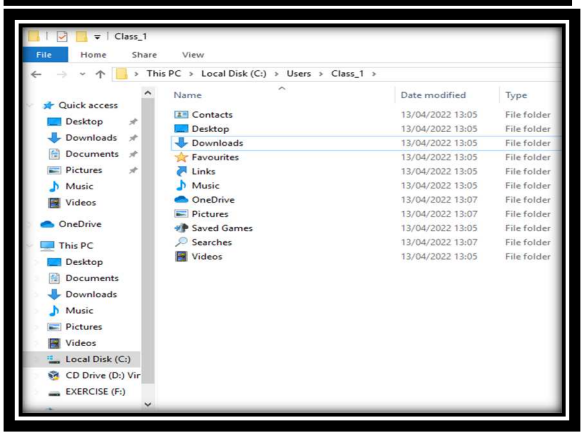


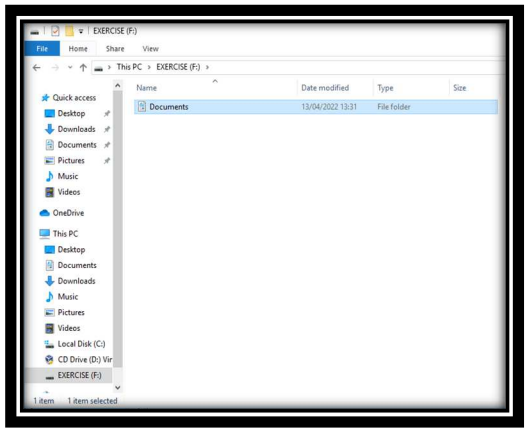


Now, we move the Class_1 user documents folder to the letter F: from File Explorer->C:\ ->Users-> Class_1 ->Documents click on this folder with right-click of the mouse -> Properties->Location->Move and choose the location in F:\



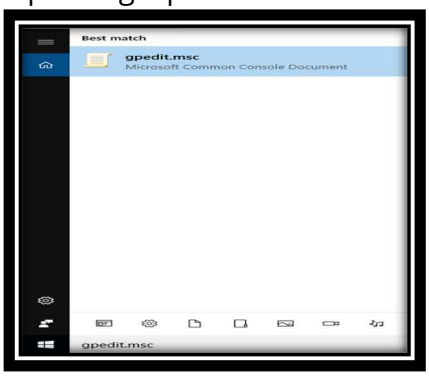


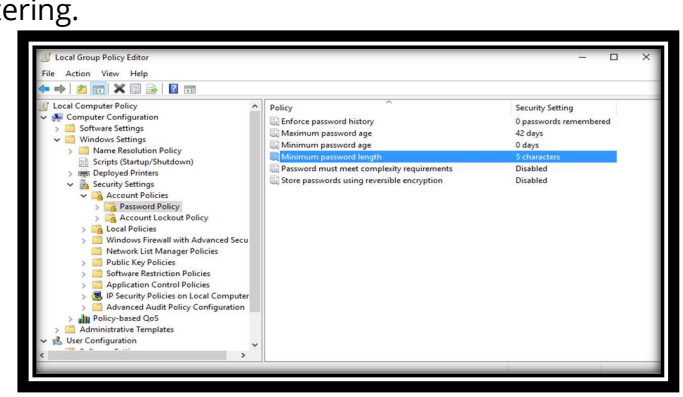


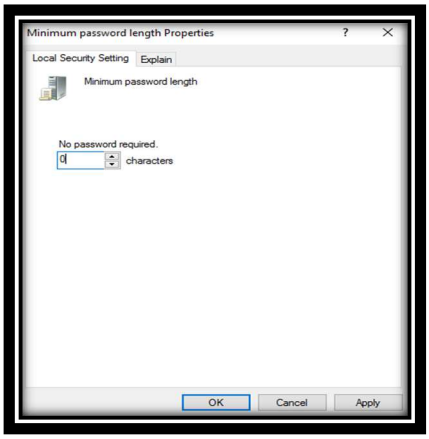


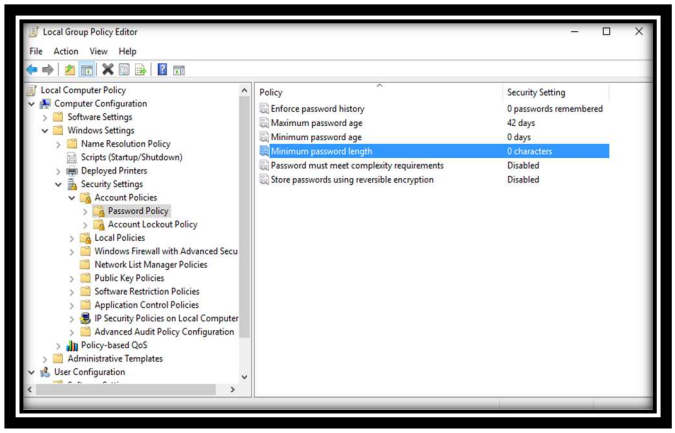
3. How do you configure a user to log in without a password and automatically when turning the computer on?

First, access with gpedit.msc to **Local Security Policy-> Security Settings->Account Policies->Password Policy**. You have to change the option **"Minimum password length"** to zero so that the user accesses automatically without requesting a password when entering.

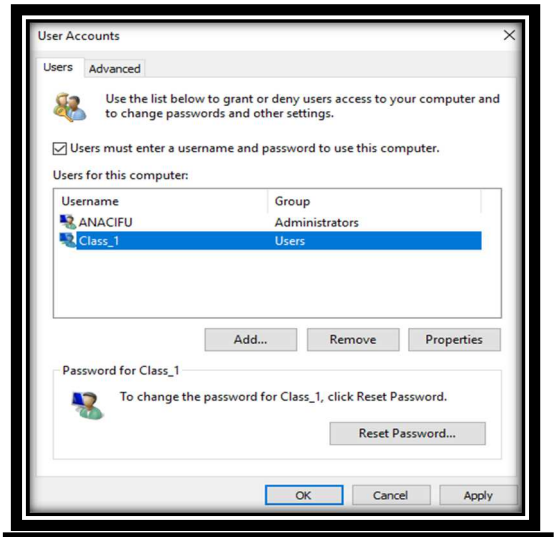


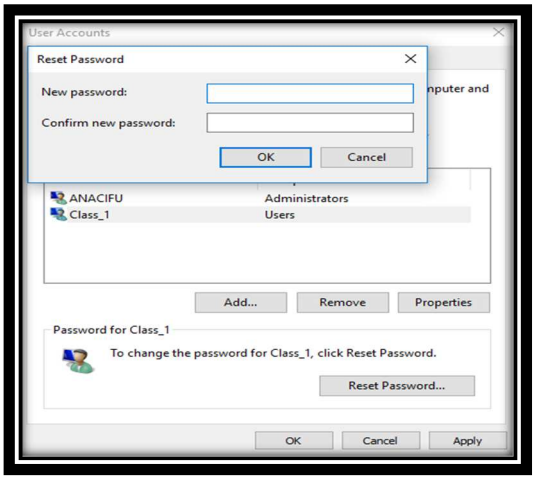


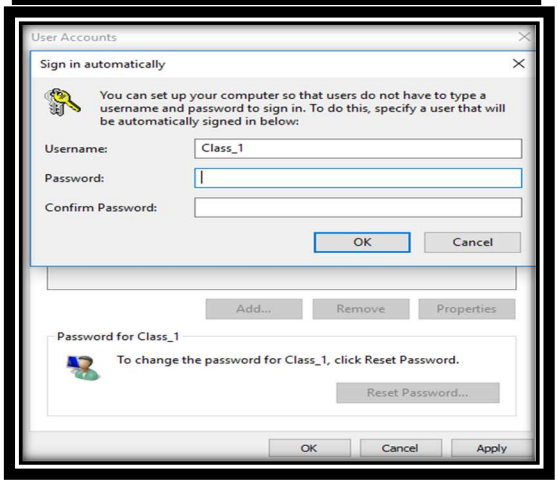




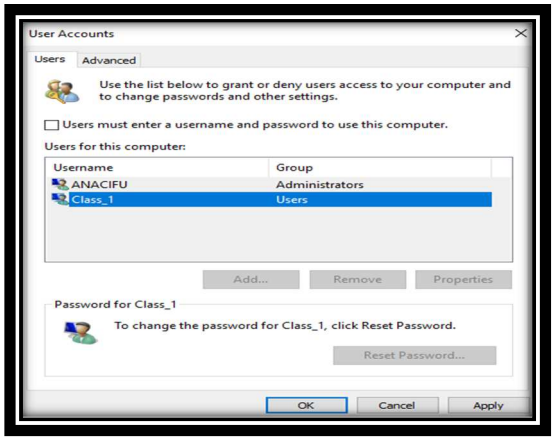
After that, with “Netplwiz” you access the Class_1 user and change the password in "Reset password" and leave it blank and when you record the change, ask again for the password and leave it blank again.



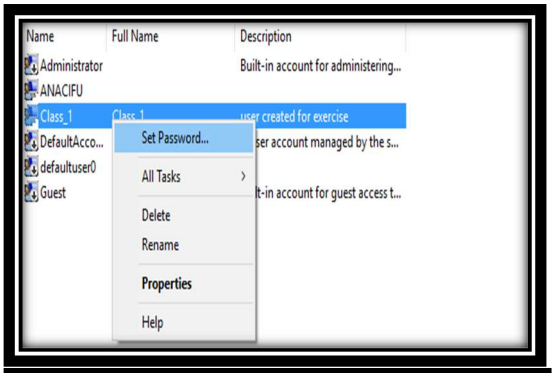


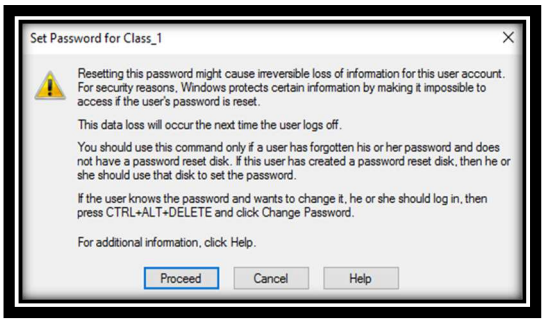


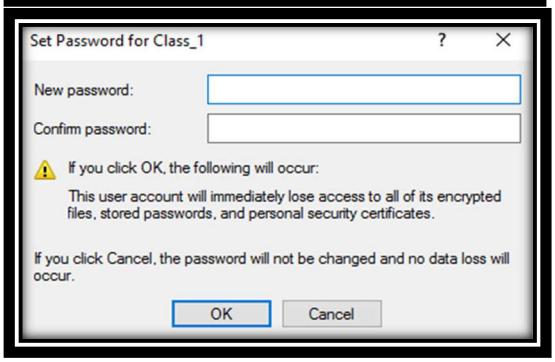
Then, unset the box “Users must enter a username and password to use this computer.

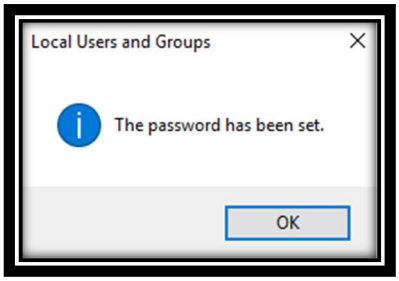


Another way to change the password from **“Computer Management”->right-click of the mouse->Set Password** and leave the password blank.

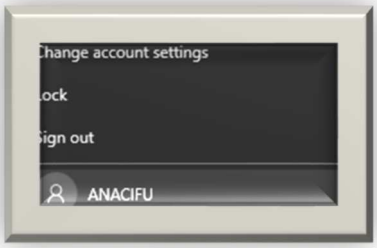






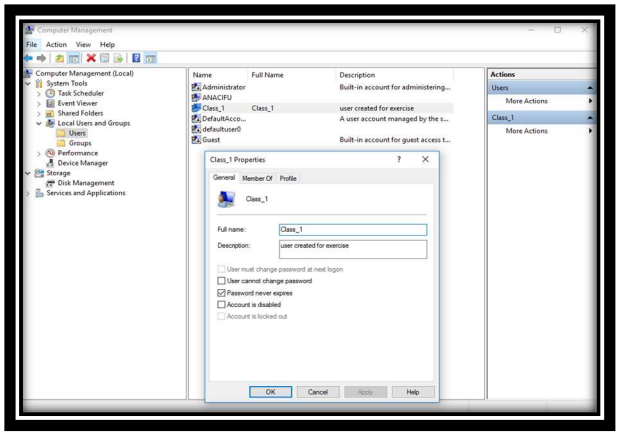


Then restart the computer and you can access to **Class_1** user without password. When you want to access to another user, you have to change it from **Start->Change Account Settings**.

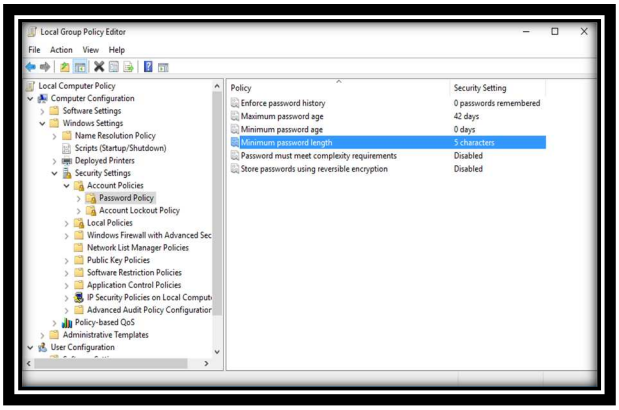


4. How do you configure a specific user so that the password never expires? How can you configure this policy for everyone?

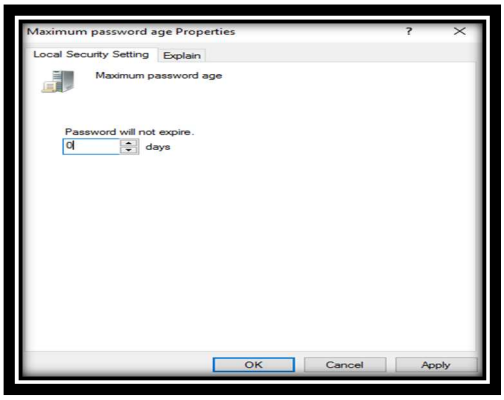
To do this, you have to go to Computer Management, choose an user and select the check box “Password never expires” for one user.

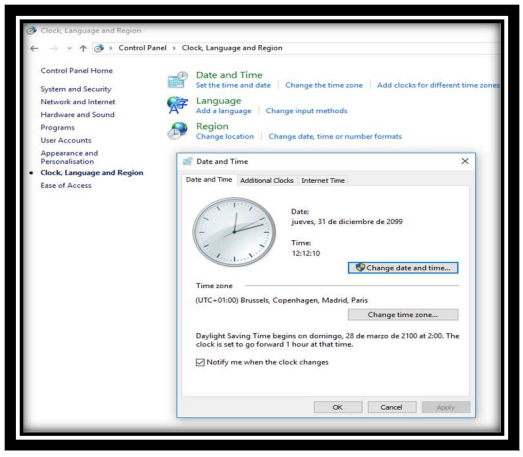


After that, gpedit.msc->Local Computer Policy->Local Settings->Password policy and change the 5 characters password to cero for every user.



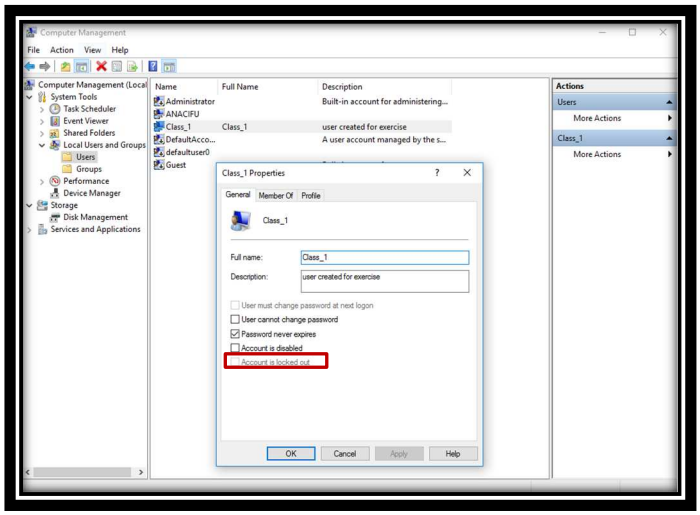
Now, I show you how to keep the password until you do not make another change. Also, and in a less orthodox way, I will demonstrate that the password does not change ever. You have to change the date of the computer and Windows 10 in the virtual machine to the maximum possible (31-12-2099), restart the computer on that maximum date and check that it does not change.





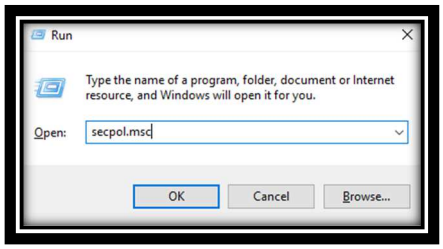
5. When can you use a locked account?

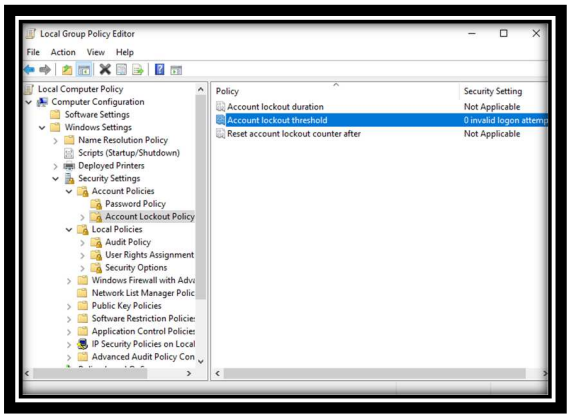
If you have entered a wrong password too many times or, in the case of shared computers, a person has tried to log in with your password, but with a user that was not yours. For safety, these actions can cause the user account to lock. And, to unlock the account, you need to turn to an administrator and perform a number of configurations.



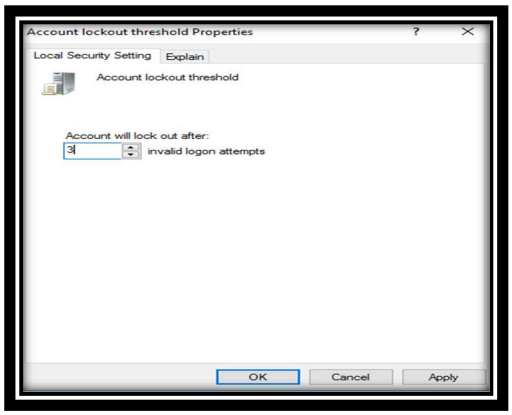
The first thing we are going to do is limit the number of failed login attempts because otherwise, you would never get to block an account.

Press the Windows + R key, then type secpol.msc and press Enter to open the Local Security Policy. Then go to **Security Settings> Account Policies> Account Blocking Policy**.

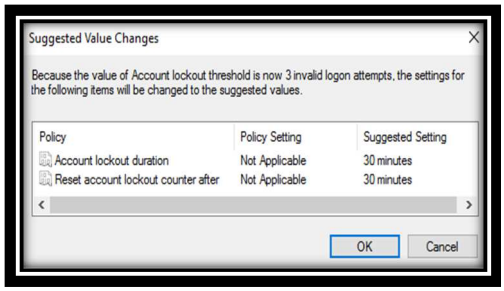


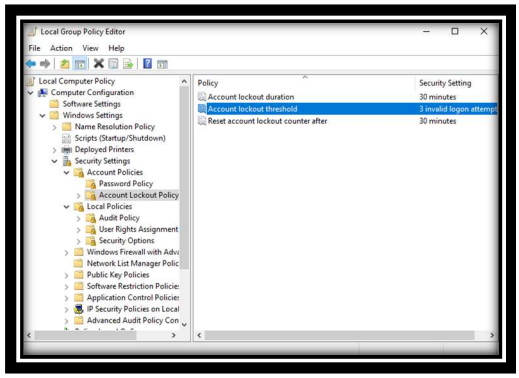


Account Lock Threshold: The account lock threshold policy determines the number of failed login attempts that will cause a user's account to be blocked. A blocked account cannot be used until it is reset or until the number of minutes specified in the account lock duration policy settings expires. You can set a value of 1 to 999 failed login attempts or you can specify that the account will never be blocked by setting the value to 0. If the account's lock threshold is set to a number greater than zero, the duration of the account lock must be greater than or equal to the value of Reset the account lock counter later. Click on **"Apply"** button.



Now, the account lock threshold value is now 3 invalid login attempts.
The default setting is 30 minutes. Close everything and restart your PC to save changes. Click on **"OK"** button.

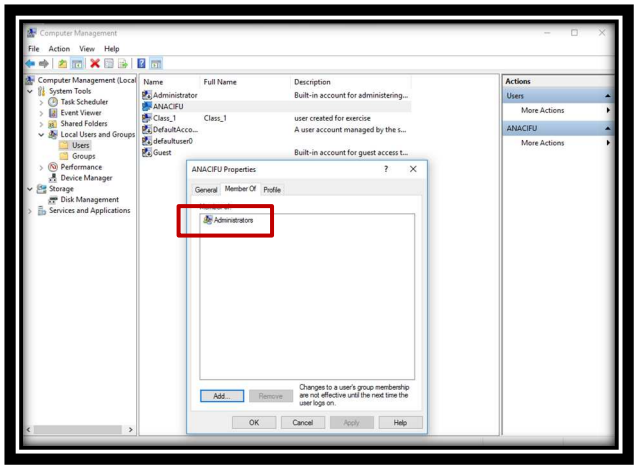


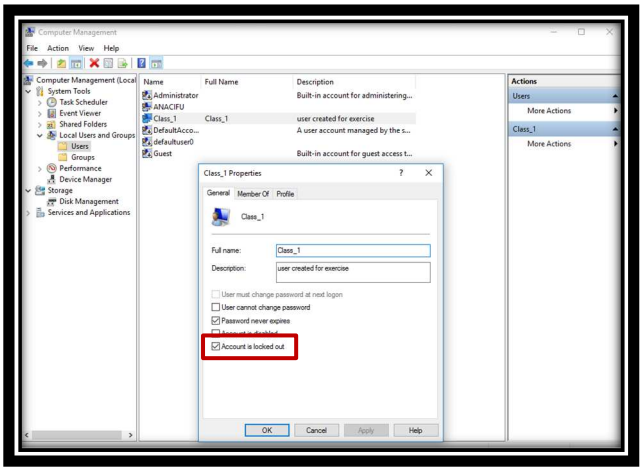


Now, after three attempts, the account is locked.

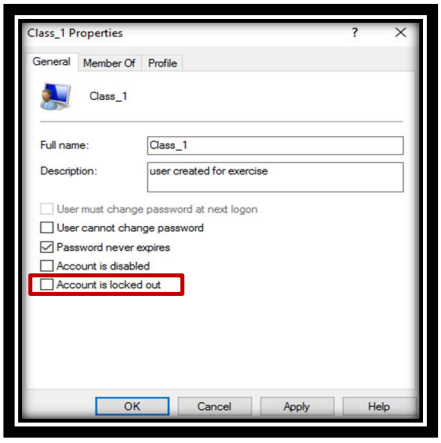
When the account is blocked, we can wait 30 minutes for it to unlock automatically or we will directly unlock it from an administrator account.

Now let's check that the ANACIFU user is an administrator and that the Class_1 user is locked.

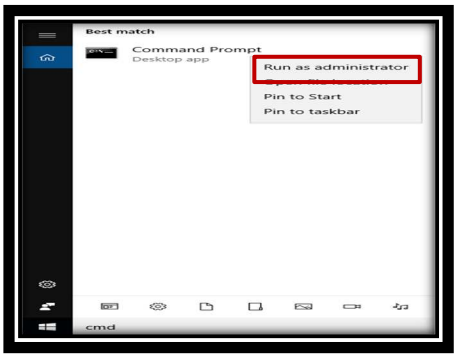




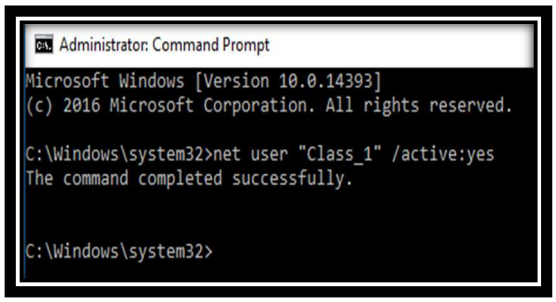
Just uncheck this box, apply the changes and you're done. We just have to log out with the user we have and restart it with the one that was locked.



If we do not want to use the previous user manager, then there is another way to do it: from CMD. To do this, we will also need a working user account, with Administrator permissions, to unlock the Windows account.
To achieve this, we just need to click with the right mouse button on the entry corresponding to the CMD search. Once we see the options that appear we only have to click on the Run as administrator.



When we have opened this window, we must execute the following command, changing «user» by the name of the user we want to unlock, between quotes and respecting upper and lower case: **"net user "user" /active:yes"**-> **net user "Class_1" /active:yes**. Once done, we will be able to close the CMD window, log out and start again with the user that was locked.



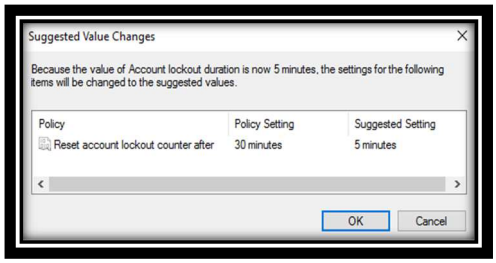
6. Imagine you define an "Account lockout threshold" of 3 and "Account lockout duration" of 5. What would be the valid values of "Reset account lockout counter after"? What if "Account lockout threshold" value were 0?

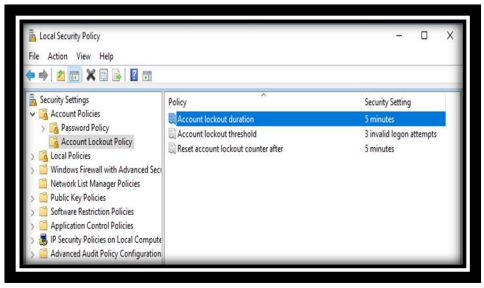
   Account Lock Duration: The account lock duration policy determines the number of minutes that a blocked account remains locked before it is automatically unlocked. The available range is from 1 to 99,999 minutes. A value of 0 specifies that the account will be locked until an administrator unlocks it explicitly. If the **account lock threshold** is set to a number greater than zero, the **account lock duration** must be greater than or equal to the value of **Rertart the account lock counter after**.

   Restart the account lock counter after: The Account Lock Counter Reset after policy settings determines the number of minutes that must elapse from the time a user fails to connect before the failed connection attempts counter is reset to 0. If the **Account Lock Threshold** is set to a number greater than zero, this reset time must be less than or equal to the value of the **account lock duration**.

   This means that if the **"Account Lock Threshold"** is set to a number greater than zero, this reset time must be less than or equal to the value of the **account lock duration**.

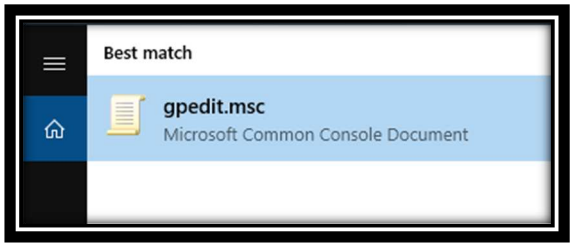
   If **"Account lockout threshold"** value were 0, no other policies could be set as accounts would not be blocked because there is no limit the number of failed login attempts.



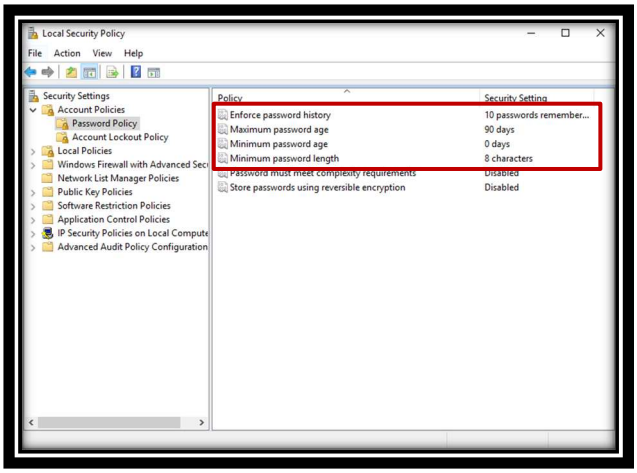


7. Configure the system according to the following criteria:
    1. All the passwords must have at least 8 characters.
    2. All the passwords must contain uppercase, lowercase, numbers and non-alphanumeric characters.
    3. The system stores the last 10 passwords for each user.
    4. All the passwords expire after 3 months.

The first thing we need to do is to log in with **“gpedit.msc”** to the **“Local Security Policy”**.



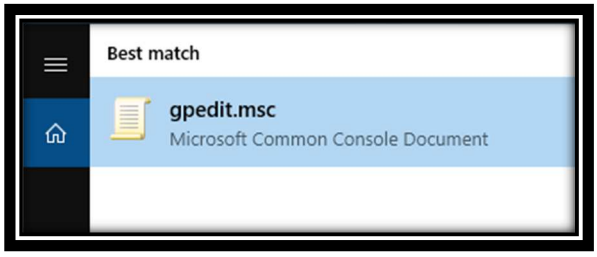
Then, we must change **“Enforce password history”** from 0 to 10 passwords, **“Maximum password age to 90 days”** and **“Minimum password length”** to 8 characters.



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:
    1. Lock the user.
    2. Unlock the user as administrator and check if the user is able to log in.
    3. Lock the user again.
    4. Wait for 5 minutes.
    5. Type the right password and check if the user is able to log in.

The first two steps are the same as those already performed in exercise 5.

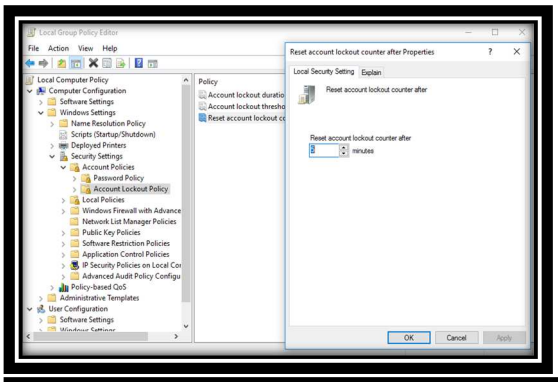
Now, next thing we need to do is to log in with **"gpedit.msc"** to the **"Local Security Policy"** and change its policies.

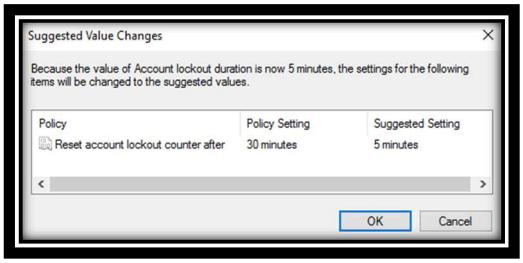


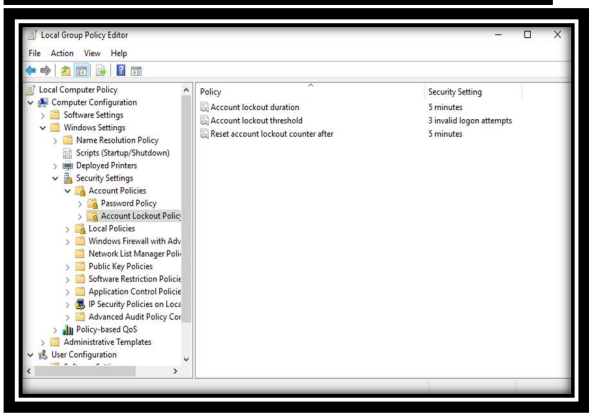
Now, we change the **"Account lockout threshold"** policy to 3 attempts and the **"Reset Account Lockout Counter After"** policy to 5 minutes.

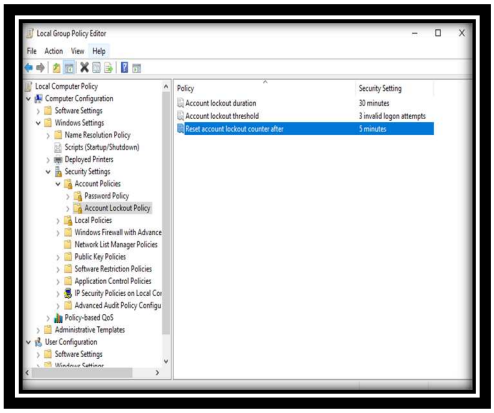
I have made the change on three occasions and in one of them the policy **"Account Lock Duration"** has been automatically changed to 5 minutes and in the next two it has stayed in 30 minutes. Both cases are correct because if the **"Account Lock**

Threshold” is set to a number greater than zero, the **“Duration of the Account Lock”** must be *greater than or equal* to the value of **“Reset the account lock counter later”**.







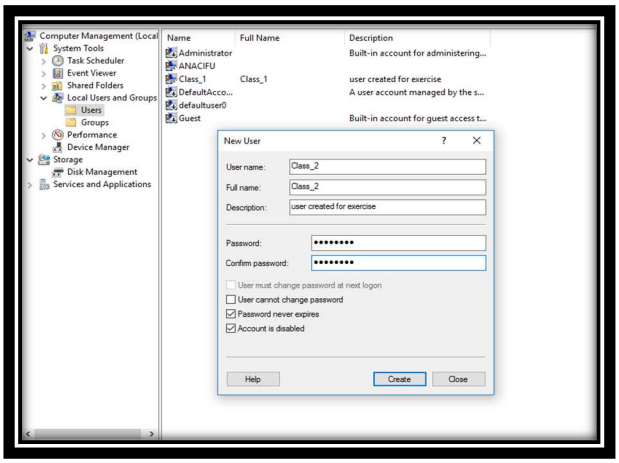


Now, after three attempts, the account is locked.

After five minutes of waiting, we enter the correct password and Windows is accessed through this user.

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

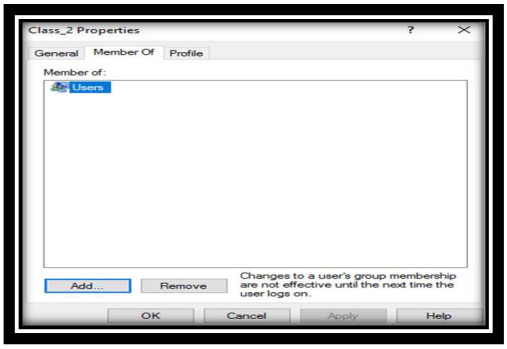
The first step is to create the Class_2 user with the requested features.

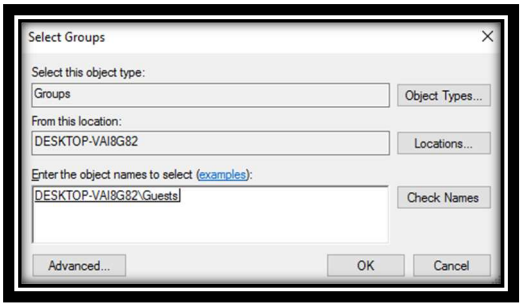


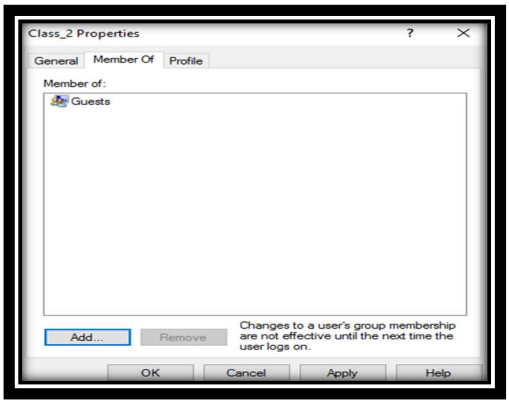
Once created, place the cursor over the newly created user, right-click of the mouse and choose properties to change the user type.

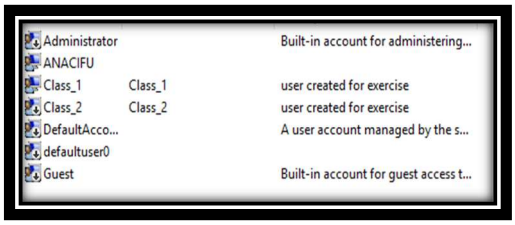
Now the Users type is removed clicking on **“Remove”** button. Then, in order to create the new user type, click on **“Add”** button, the next screen click on **“Advanced”**

button, on the next screen click on **"Find Now"** button and choose the Guests group and click on the **"OK"** button to finish.



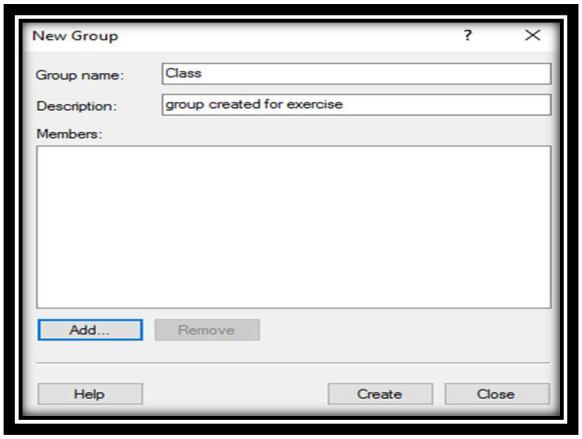


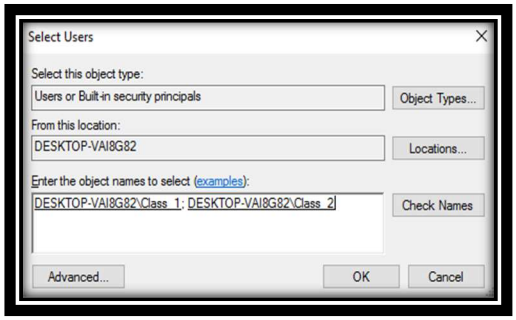


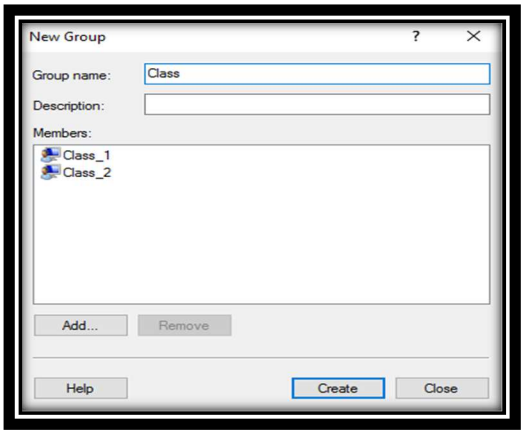


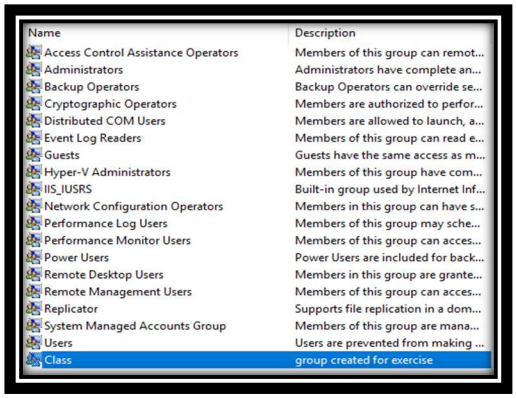
Once created, place the cursor over the groups folder, right-click of the mouse and choose properties to create the group Class.

Then, in order to create the new group, click on **"Add"** button, the next screen click on **"Advanced"** button, on the next screen click on **"Find Now"** button and choose the users you want add to the group and click on the **"Create"** button to finish.



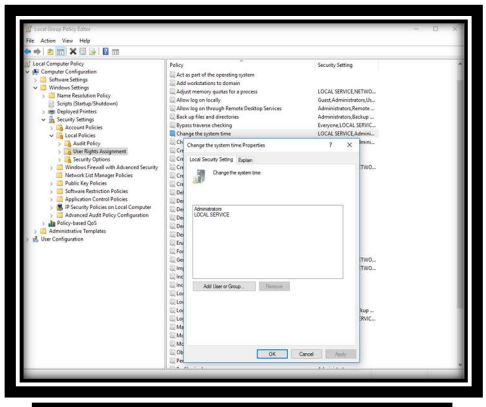


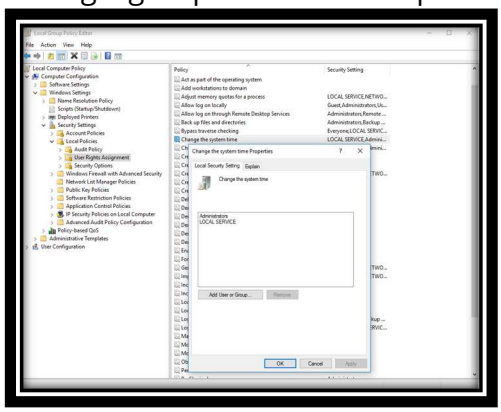


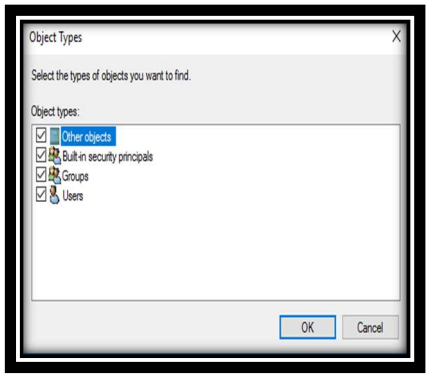


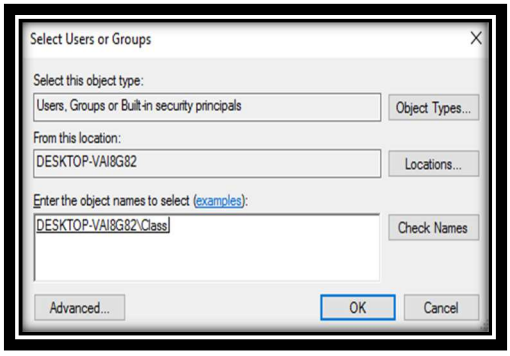
10. Modify the user rights so “Class_1” and “Class_2” will be able to **“Change the system time”**.

To change the users rights, you have to go to **Local Security policy**, then change **User Right Assingment** and set the security policy by **adding** the Class group and taking into account that in the option **"Objetc types"** has to be checked the box of the groups since being a group we need this option.

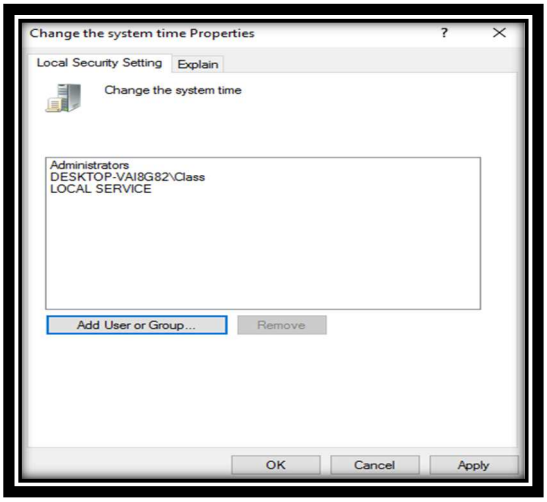




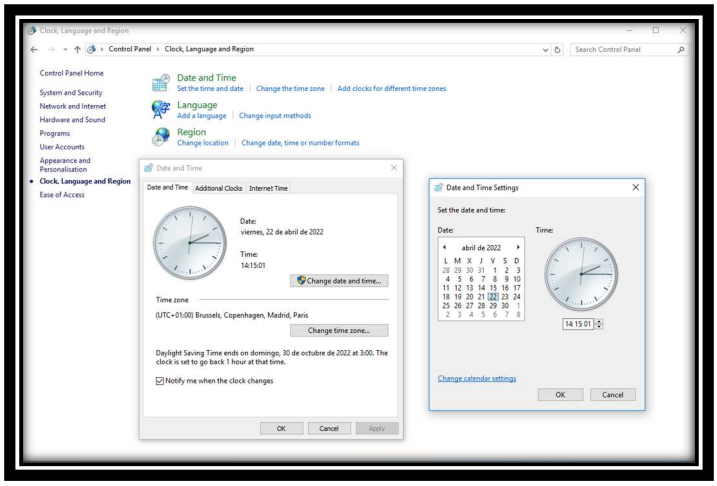




Right-click on the right “Change the system time” and add the group Class

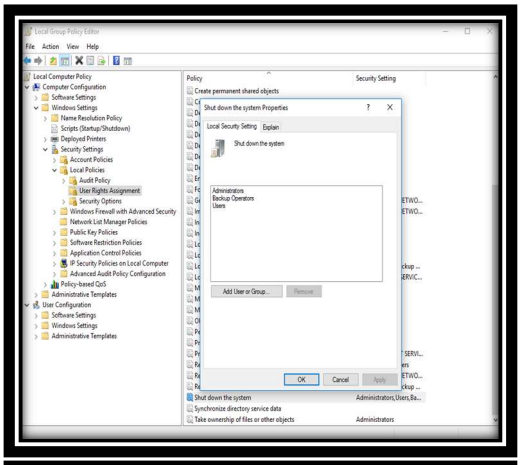


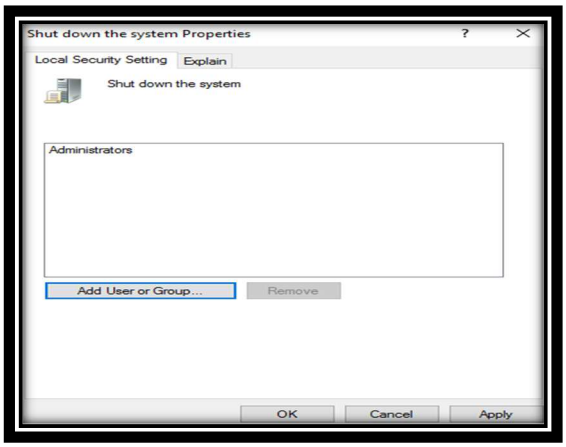
Then, restart the computer and check one of the users

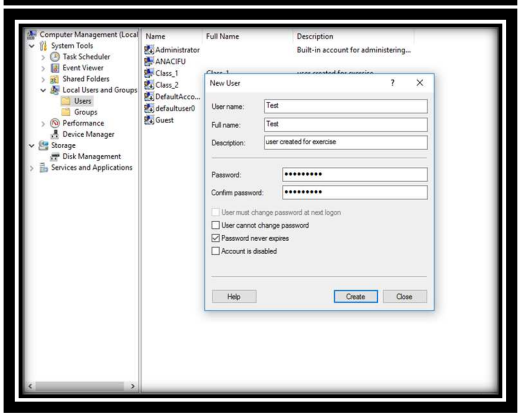


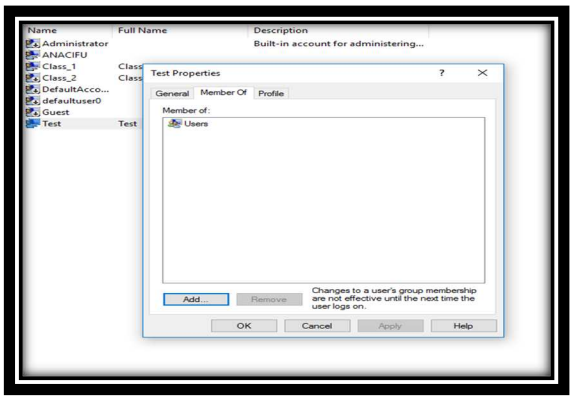
11. Modify the user rights so that only the administrator users can “Shut down the system”.

From **Local Security Policy-> right-click->Shut down the system** and delete all the users except “Administrators”. Then you can create a user in order to check that this policy is working.



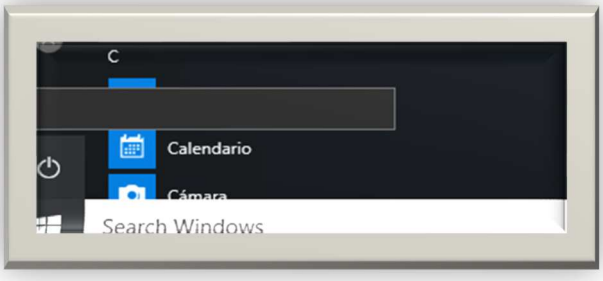

Shut down the system Properties
Local Security Setting
Explain
Shut down the system
Administrators
Add User or Group...
Remove
OK
Cancel
Apply




Name
Full Name
Description
Administrator
Built-in account for administering...
ANACIFU
Class_1
Class_2
DefaultAcco...
defaultuser0
Guest
Test
Test Properties
General
Member Of
Profile
Member of:
Users
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help

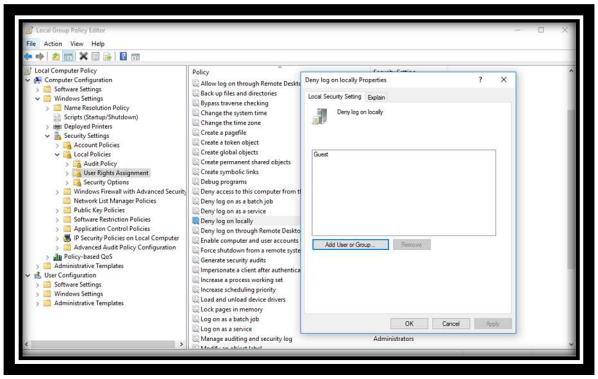

Test
Welcome

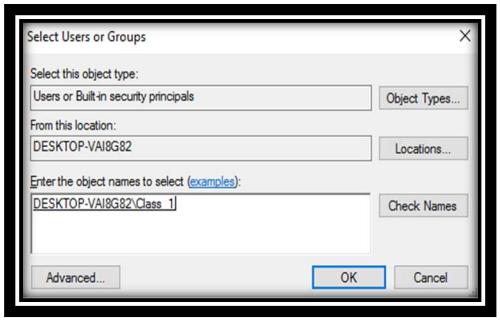

etting things ready – please don't turn off your P

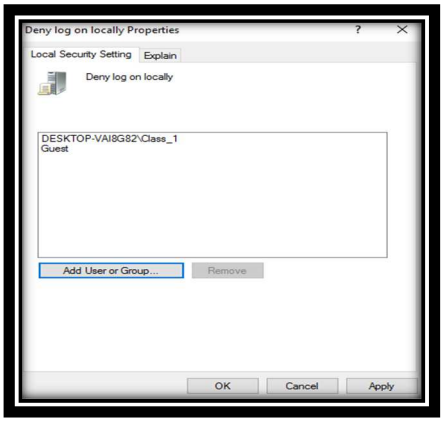

C
Calendario
Cámara
Search Windows

12. Suppose all the standard users are able to log in. How can we deny log on to the specific user “Class_1”?

From Local security policies->User rights assignment, we can set the policy “Deny log on as locally”, add the user Class_1 to the list. This way all the standard users except “Class_1” are able to log in. After that, restart the computer and we can check the users that can log on.

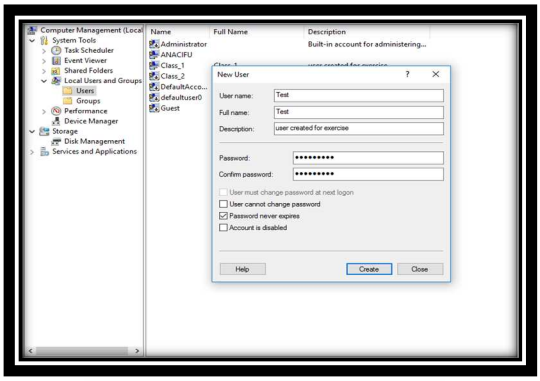


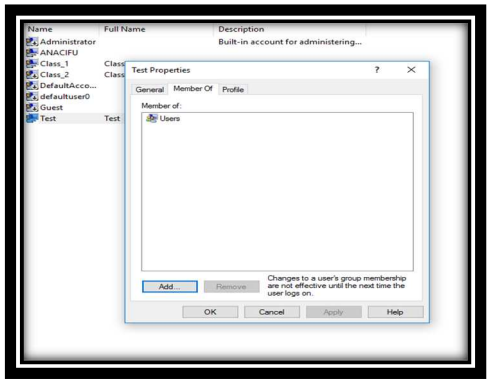




13. Overall, add a new user called “Test” according to the requirements in exercise 7. What if we deleted “Test” from the group “Users”? Try to log in and explain what happens.

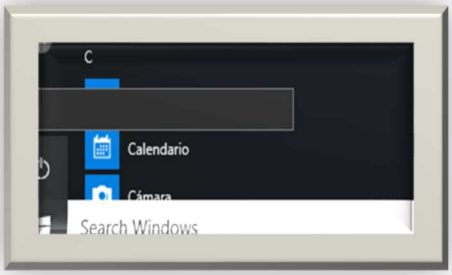
We create a user called “Test” with the password 12345-AC according to the requirements for this user. After that, from “Computer Management”->Properties we delete the group Users for this user. Then, we restart the computer and we check that the user “Test” does not belong to any of the authotised to log on, we are not able to log in and we have to log on with another user.

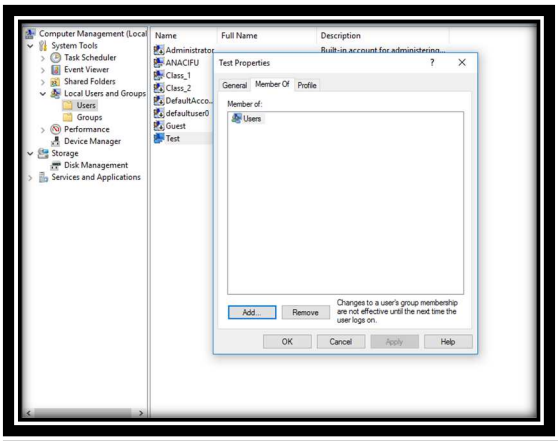

Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
Built-in account for administering...
ANACIFU
Class_1
Class_2
DefaultAcco...
defaultuser0
Guest
New User
User name:
Test
Full name:
Test
Description:
user created for exercise
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Help
Create
Close

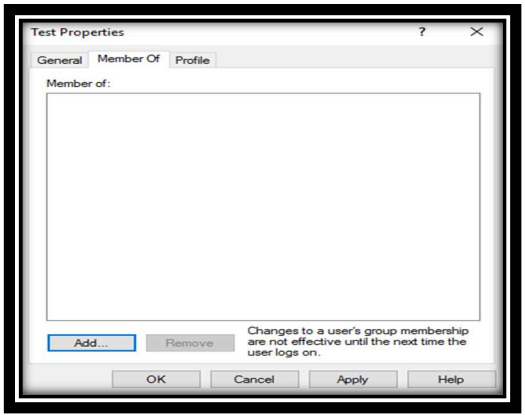

Name
Full Name
Description
Administrator
Built-in account for administering...
ANACIFU
Class_1
Class_2
DefaultAcco...
defaultuser0
Guest
Test
Test Properties
General
Member Of
Profile
Member of:
Users
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help

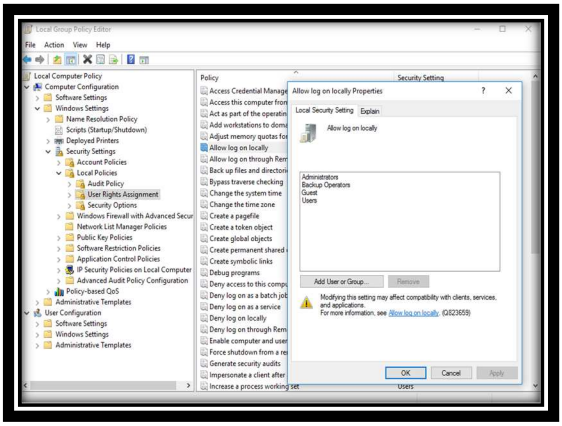

Test
Welcome


etting things ready – please don't turn off your


C
Calendario
Cámara
Search Windows


Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Full Name
Description
Administrator
ANACIFU
Class_1
Class_2
DefaultAcco...
defaultuser0
Guest
Test
Test Properties
General
Member Of
Profile
Member of:
Users
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help


Test Properties
General
Member Of
Profile
Member of:
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help


Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secur
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Policy
Security Setting
Allow log on locally Properties
Local Security Setting
Explain
Allow log on locally
Administrators
Backup Operators
Guest
Users
Add User or Group...
Remove
OK
Cancel
Apply


ANACIFU