- 2. 3. Users, groups and permissions on Windows 10 -

- INDEX -

- Exercises -

You are going to create a new Google Document inside the "2. Windows 10" folder of your Google Drive, named:

"2. 3. Users, groups and permissions on Windows 10 - Apellidos, Nombre"

being "Apellidos, Nombre" your Last Name and Name.

Inside this Google Document you are going to copy and answer all the "Exercises" of this sub-unit.

- 2. 3. 1. Managing user accounts -

Before you can begin working with a device running Microsoft Windows 10, you must sign in with the credentials for a user account that is authorized to use that device.

User accounts are an essential cornerstone of Windows security and are key to providing a personalized user experience.

You can configure user accounts on a Windows 10 device to control access to files and other resources, and to audit system events (such as sign-ins and the use of files and other resources).

If your computer is in a secure location where only people you trust have physical access to it, you might be tempted to allow family members or co-workers to share your user account. We strongly caution against using that configuration and instead recommend that you create a user account for each person who uses the computer.

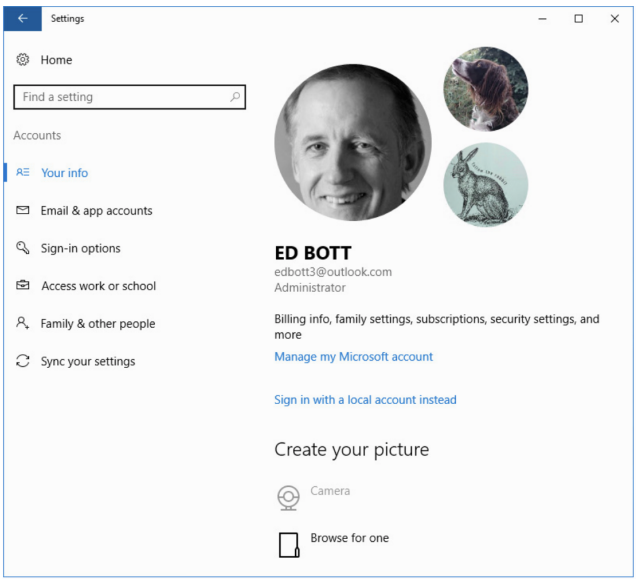
Doing so allows each account to access its own user profile and store personal files and user preferences within that profile.

Working with user accounts

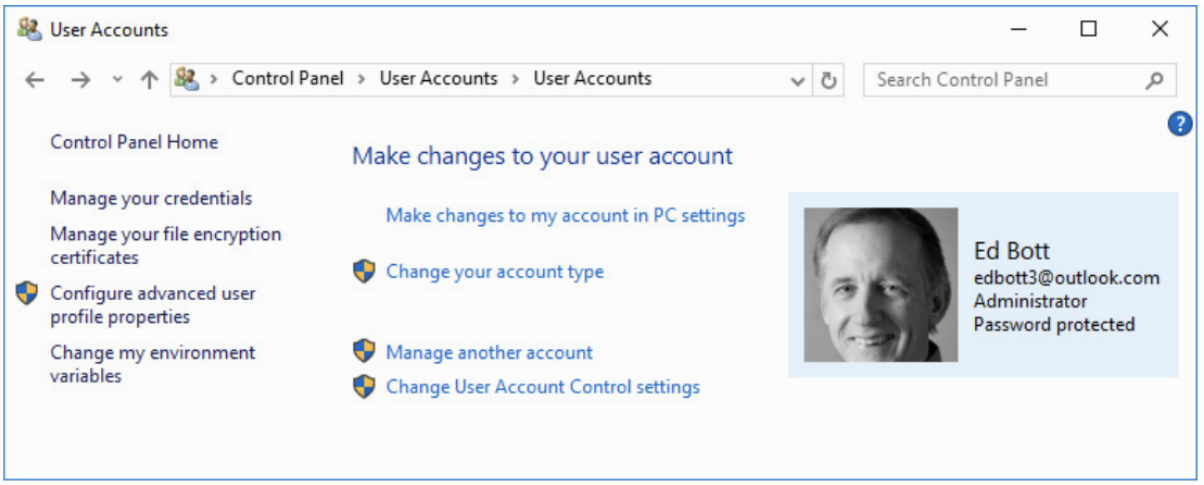
When you install Windows 10 on a new computer, the setup program creates a profile for one user account, which is an administrator account (it has full control over the computer).

After signing in for the first time, you can go to Settings > Accounts to create new user accounts and make routine changes to existing accounts.

The Your Info page provides an overview of your account, similar to the one shown in the next figure:



You'll find some account-related settings under the User Accounts heading in the old-school Control Panel, which is shown in the following figure. Several of these settings duplicate functions that are available in Settings > Accounts.

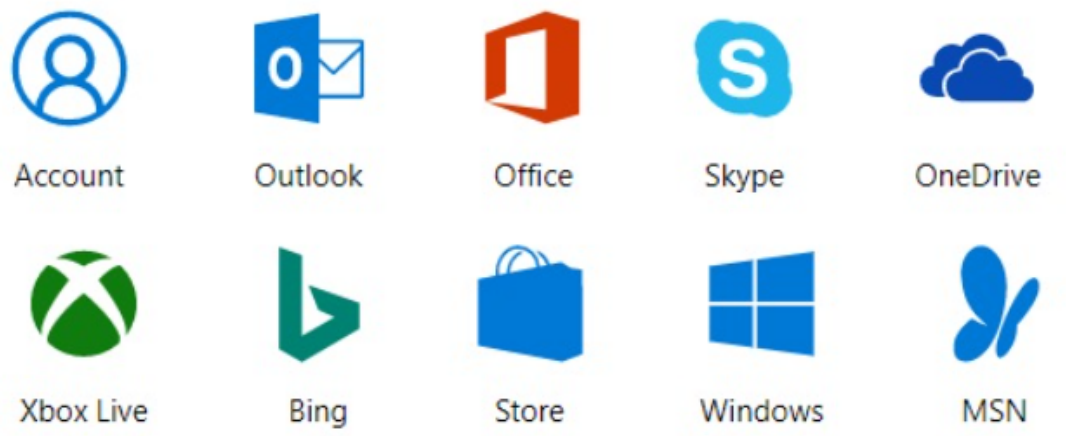


Choosing an account type

Windows 10 supports four different account types.

1. Microsoft account

A Microsoft Account is the modern name given to the Identity system that provides authentication and authorization to Microsoft's consumer services.



You do not need a Microsoft address to create a Microsoft account; you can set up a Microsoft account using an existing email address from any domain and any email provider.

The biggest advantage of signing in with a Microsoft account is synchronizing PC settings between multiple computers.

2. Local account

A local account is one that stores its sign-in credentials and other account data on your PC. A local account works only on a single computer. It doesn't require an email address as the user name, nor does it communicate with an external server to verify credentials.

This type of account was the standard in Windows for decades. Microsoft recommends the use of a Microsoft account rather than a local user account, but some folks have privacy and data security concerns about storing personal information on the servers of a large corporation.

You can switch between using a Microsoft account and a local account by going to Settings, Accounts.

3. Azure Active Directory account

The third type of account, available during initial setup of Windows 10 Pro, Enterprise, or Education, is a work or school account using Azure Active Directory.

Azure AD offers some of the advantages of a Microsoft account, including support for two-factor authentication and single sign-on to online services, balanced by the capability of network administrators to impose restrictions using management software.

These accounts are most common in medium-size and large businesses and schools.

4. Active Directory domain account

In organizations with Windows domains running Active Directory services, administrators can join a PC to the domain, creating a domain machine account.

This option is available only with Windows 10 Pro, Enterprise, or Education editions.

After this step is complete, any user with a domain user account can sign in to the PC and access local and domain-based resources.

Default local user accounts

The default local user accounts are built-in accounts that are created automatically when the operating system is installed. The default local user accounts can't be removed or deleted.

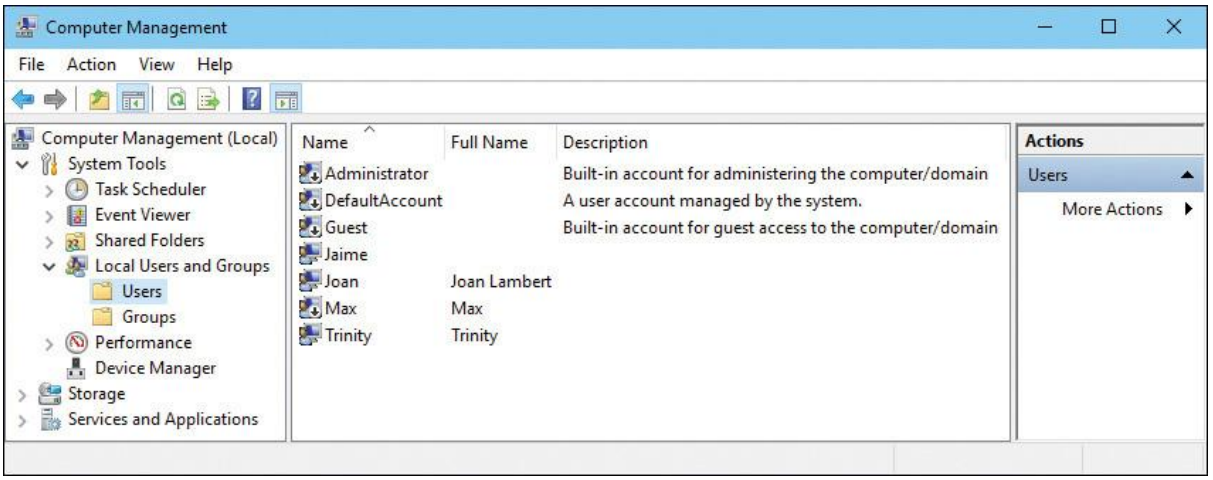
- **Administrator**: It is a user account for system administration. Every computer has an Administrator account that can't be deleted. Windows setup disables the built-in Administrator account.
- **Guest**: this account lets occasional or one-time users, who don't have an account on the computer, temporarily sign in. By default, the Guest account is

disabled and has a blank password. It's a best practice to leave the Guest account disabled, unless its use is necessary.

Other default local user accounts include HelpAssistant and DefaultAccount. There are also default local system accounts, such as SYSTEM, NETWORK SERVICE or LOCAL SERVICE.

Managing local users with the Computer Management console

You can manage local users (creating, deleting, modifying, etc.) from the Computer Management console. You can find a link to this console in the Quick Link menu (Windows + X).



- 2. 3. 2. Managing local groups -

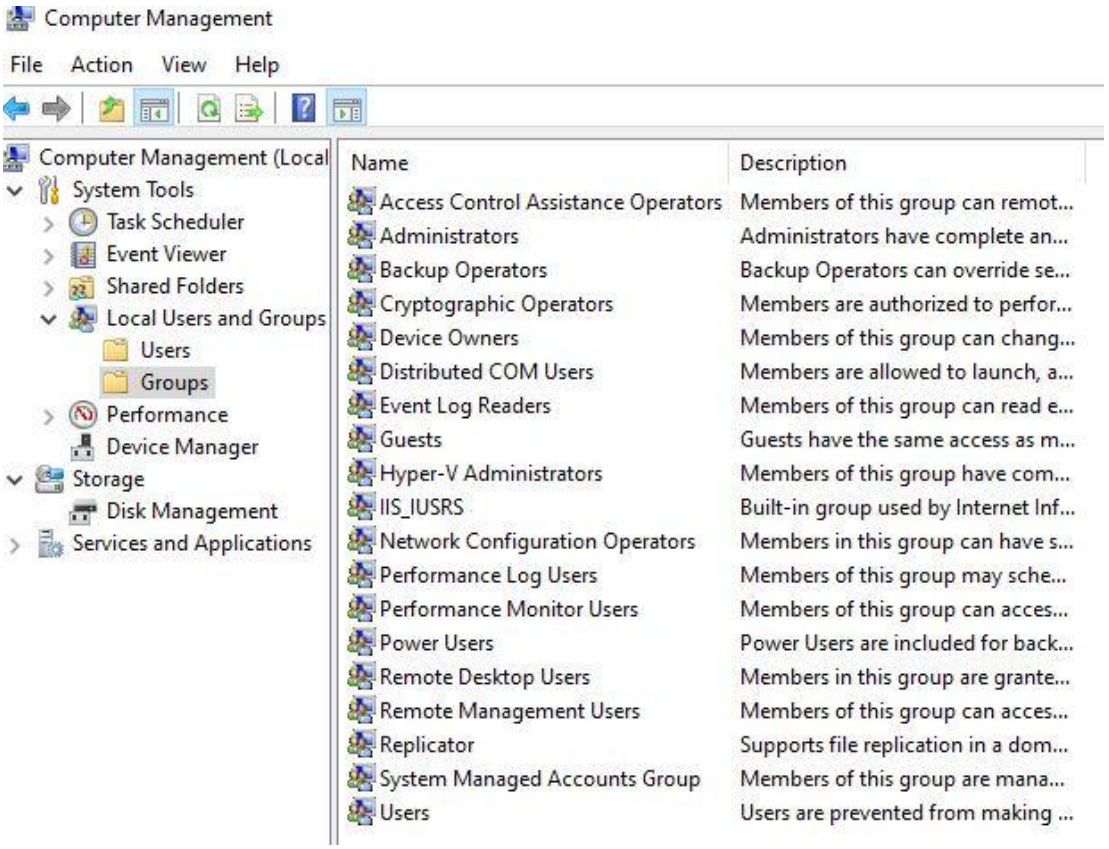
A group is a collection of user accounts and other groups that you can manage as a single unit.

Windows 10 provides a set of default groups at installation, but It also provides an option to create groups. Default groups include:

- **Administrators**: members of this group have complete control over the system. They can perform tasks like installing software, modifying system settings, and managing other users.
- **Users**: standard user accounts belong to this group. They have limited system-wide access and can use most software and change system settings that don't affect other users.

You can use groups to simplify administration by assigning permissions on a resource to a group, rather than to individual users. Assigning permissions to a group assigns the same access to the resource to all members of that group.

You can only manage local groups from the Computer Management console. There, you can create and delete groups, and also manage group membership.



- 2. 3. 3. Exercises: Managing users and groups -

In the following exercises include screenshots in order to show that you have completed the task. You must also include the answers to the questions.

1. With your local account, create a PIN, sign out from Windows, and login using the PIN.
2. With your local account, create a Picture Password, sign out from Windows, and login using the Picture Password.
3. Using Settings, create a new local account. As the account username you can choose the first name of a classmate. Set the password “alumno”.
4. Login with the new user. Does he have the same desktop background as the initial user? Why?
5. Try creating a new user using the new account. You can do it? Why? How could you solve it?
6. Create a new Microsoft account on your Windows 10 using your @iesdoctorbalmis.com email (https://account.microsoft.com). Try to login with your new user.
7. Switch to your original user (the one created during the installation) and open the Computer Management console. Locate your three users and include the groups they belong to.
8. Unlock Administrator user and try to login with this account.
9. Create a fourth user from the Computer Management console (using another classmate's name and the same password used previously). Make sure the password never expires.
10. Check the user’s folders under C:\Windows\Users. Is there a folder for the last user created? Why?
11. Login with the new user and check the user's folder again.
12. Switch to your original user and create the groups Designers and Developers.
13. Your original account and the account created at exercise 3 must belong to the Designers group. The other two accounts (Microsoft account and the account created at exercise 9) must belong to the Developers group.

- 2. 3. 4. Managing permissions -

Permissions are a key component of the Windows 10 security architecture that you can use to manage the process of authorizing users to access resources on a computer.

Permissions enable the owner of each resource to control who can perform an operation or a set of operations on the resource. The owner of a resource always has the ability to read and change permissions on the resource. By default, in Windows 10, the owner is the creator of the resource.

Permissions can be granted to a user or to a group. All members of a group inherit permissions granted to the group.

NTFS Permission	Folders	Files
Read	Open files and subfolders	Open files
List Folder Contents	List contents of folder, traverse folder to open subfolders	Not applicable
Read and Execute	Not applicable	Open files, execute programs
Write	Create subfolders and add files	Modify files
Modify	All the above + delete	All the above
Full Control	All the above + change permissions and take ownership, delete subfolders	All the above + change permissions and take ownership

Granting and Denying Permissions

A permission is authorization to perform an operation on a specific resource, such as a file. Permissions can be granted by owners, and by anyone with the permission to grant permissions, which normally includes administrators on the system.

If you own an object, you can grant any user or group any permission on that object, including the permission to take ownership.

When permission to perform an operation is not explicitly granted, it is implicitly denied. But permissions can also be explicitly denied.

Explicit denials are usually used to exclude a subset from a larger group that has been given permission to perform an operation.

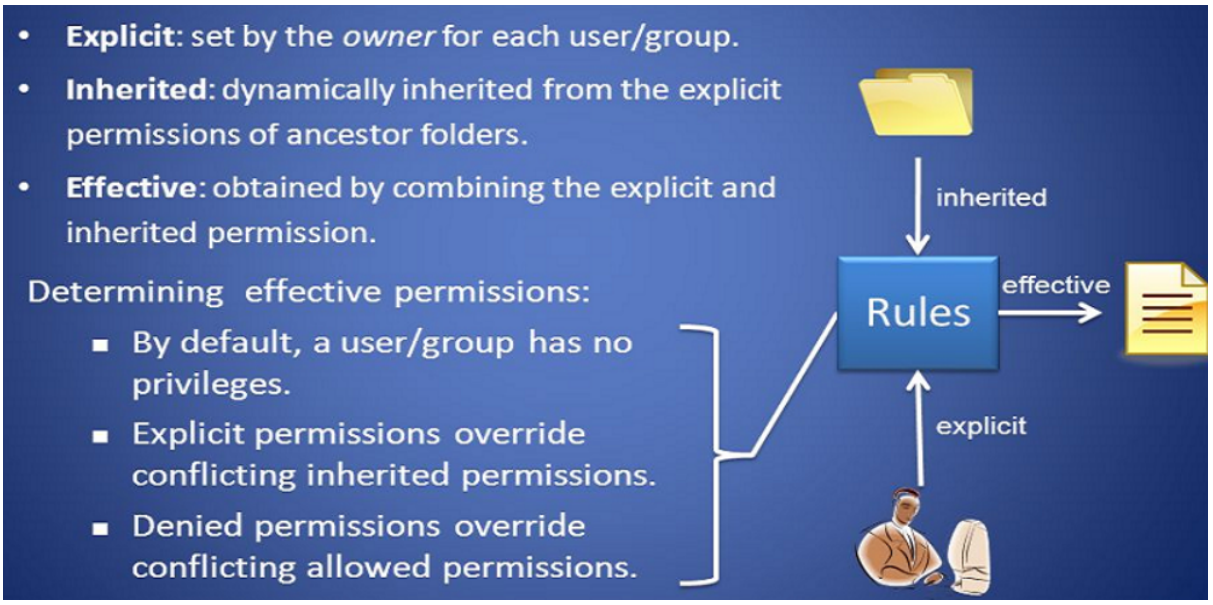
Note that use of explicit denials increases the complexity of the authorization policy and can create unexpected errors. Though it is sometimes necessary, you can and should avoid the use of explicit denies in most cases.

Each permission that a resource's owner grants to a particular user or group is stored as an ACE (Access Control Entry) in a Discretionary Access Control List (DACL) that is part of the object's security descriptor.

Explicit vs. Inherited Permissions

There are two types of permissions:

- Explicit permissions are those that are set by default when the resource is created or by user action.
- Inherited permissions are those that are propagated to a child resource from a parent resource.By default, resources inherit the permissions from their container when they are created.



- 2. 3. 5. Exercises: Managing file and folder permissions -

In the following exercises include screenshots in order to show that you have completed the task. You must also include the answers to the questions.

1. Using your original user, create the folders HTML, CSS and JS under C:\.
2. Check the permissions assigned to the new folders. Are they explicit or inherited?
3. Check who is the owner of those folders.
4. Removes the Users and Authenticated Users groups from the permissions of the three directories. Explain everything you had to do to achieve it.
5. Set the permissions of the three folders following these instructions:
    a. Users in the Designers group should have Modify permissions on HTML and CSS folders.
    b. Users in the Developers group should have Modify permissions on the JS folder.
    c. Users in the Developers group should be able to read HTML and CSS folders, but not to write in.
    d. The user with a Microsoft account should not access the CSS folder under any circumstances, regardless of the groups to which they belong.
6. Login with your four users, and verify that they have the correct permissions on all the three folders.