

# 0 - Windows Fundamentals 1

---

It took me a while to remember the name of the tool, but I finally remembered. We are going to be using the kali built-in tool called "xfreerdp".

```
"#sudo xfreerdp /v:IP_TO_CONNECT /u:administrator /p:letmein123!"
```

We can use other flags to make the experience smother within the xfreerdp tool, but this should get you a GUI Desktop to interact.

What encryption can you enable on Pro that you can't enable in Home?



On **Windows Pro**, you can enable **BitLocker**, which is a full disk encryption feature that is not available in the **Windows Home** edition.

## Here's why **BitLocker** stands out:

- **BitLocker** encrypts your entire drive, ensuring that all data on it is secure. If your device is lost or stolen, BitLocker prevents unauthorized access to the data by requiring proper authentication before the operating system can be accessed.
- It also supports **BitLocker To Go**, which allows encryption of external drives like USB flash drives.

In contrast, **Windows Home** only provides basic encryption through **Device Encryption** (if your hardware supports it). This feature is less robust than BitLocker:

- **Device Encryption** works in a simplified way, and it automatically encrypts the device when you sign in with a Microsoft account. However, it lacks the management and control options of BitLocker (e.g., no support for external drives, fewer encryption options).

So, the main encryption feature exclusive to **Windows Pro** is **BitLocker**, giving users more control over the security of their data compared to the Home edition.

Is encryption a key factor in deciding between the two versions for you?

Would the disk still be encrypted if the user did not sign in to the Microsoft account?

Yes, the disk can still be encrypted with BitLocker on Windows Pro even if the user does not sign in to a Microsoft account.

#### Key Details:

- BitLocker does not require a Microsoft account to function. You can manage BitLocker encryption using other methods, such as saving the recovery key locally (e.g., on a USB drive) or printing it out.
- When enabling BitLocker, you will be prompted to save a recovery key, which can be stored offline (without relying on a Microsoft account). This key is used to unlock the drive in case you forget your password or if there's a hardware change.

#### For Device Encryption (in Windows Home):

- Device Encryption typically requires you to sign in to a Microsoft account because the encryption key is stored in the cloud (linked to your Microsoft account). Without signing in, this feature will not activate automatically on most systems.

#### To summarize:

- BitLocker on Windows Pro can be fully utilized without a Microsoft account.
- Device Encryption on Windows Home usually requires a Microsoft account to function properly.

Would you like help setting up or managing BitLocker encryption?

🔊 📄 👍 🗑️ ↻

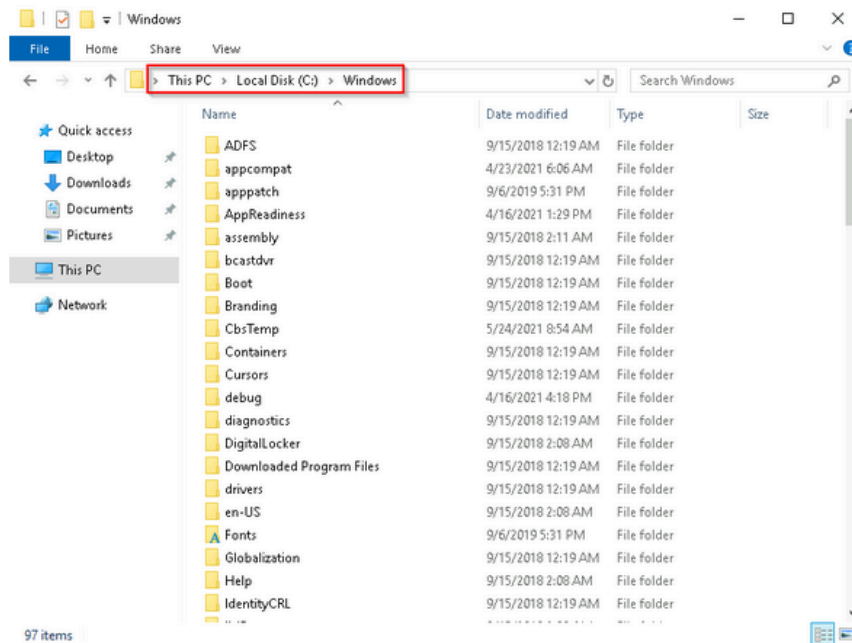
The Windows folder ( `C:\Windows` ) is traditionally known as the folder which contains the Windows operating system.

The folder doesn't have to reside in the C drive necessarily. It can reside in any other drive and technically can reside in a different folder.

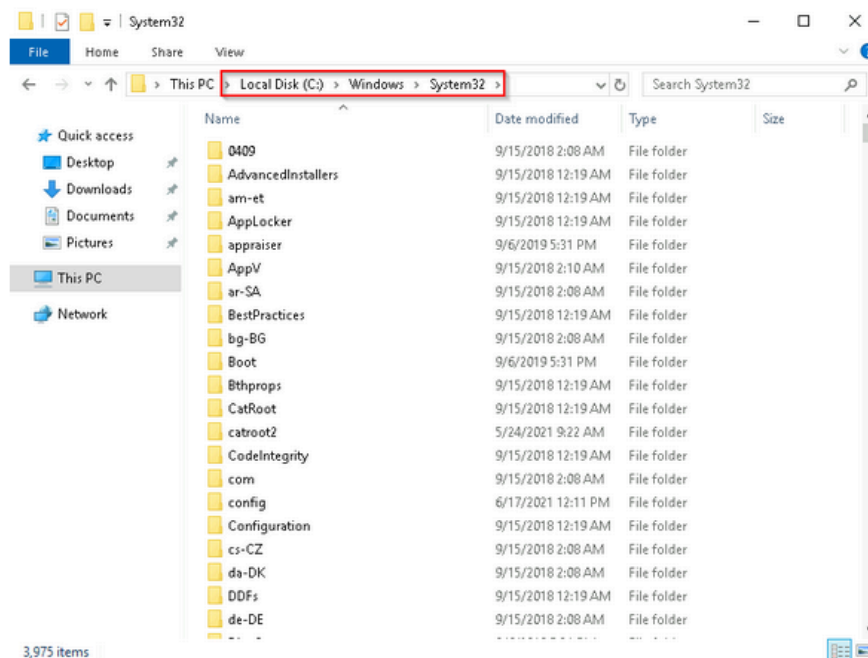
This is where environment variables, more specifically system environment variables, come into play. Even though not discussed yet, the system environment variable for the Windows directory is `%windir%`.

Per Microsoft, "Environment variables store information about the operating system environment. This information includes details such as the operating system path, the number of processors used by the operating system, and the location of temporary folders".

There are many folders within the 'Windows' folder. See below.



One of the many folders is **System32**.



The System32 folder holds the important files that are critical for the operating system.

You should proceed with extreme caution when interacting with this folder. Accidentally deleting any files or folders within System32 can render the Windows OS inoperational. Read more about this action [here](#).

**Note:** Many of the tools that will be covered in the Windows Fundamentals series reside within the System32 folder.

User accounts can be one of two types on a typical local Windows system: **Administrator** & **Standard User**.

The user account type will determine what actions the user can perform on that specific Windows system.

- An Administrator can make changes to the system: add users, delete users, modify groups, modify settings on the system, etc.
- A Standard User can only make changes to folders/files attributed to the user & can't perform system-level changes, such as install programs.

You are currently logged in as an Administrator. There are several ways to determine which user accounts exist on the system.

One way is to click the **Start Menu** and type **Other User**. A shortcut to **System Settings > Other users** should appear.



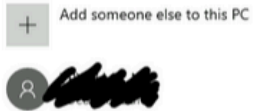
If you click on it, a Settings window should now appear. See below.

## Other users

### Other users



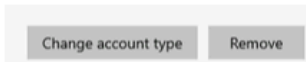
## Other users



Since you're the Administrator, you see an option to **Add someone else to this PC**.

**Note:** A Standard User will not see this option.

Click on the local user account. More options should appear: **Change account type** and **Remove**.



Click on Change account type. The value in the drop-down box (or the highlighted value if you click the drop-down) is the current account type.



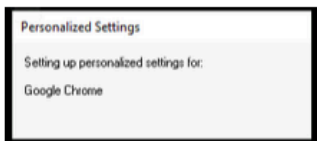
When a user account is created, a profile is created for the user. The location for each user profile folder will fall under is C:\Users.

For example, the user profile folder for the user account Max will be C:\Users\Max.

The creation of the user's profile is done upon initial login. When a new user account logs in to a local system for the first time, they'll see several messages on the login screen. One of the messages, User Profile Service, sits on the login screen for a while, which is at work creating the user profile. See below.



Once logged in, the user will see a dialog box similar to the one below (again), indicating that the profile is in creation.



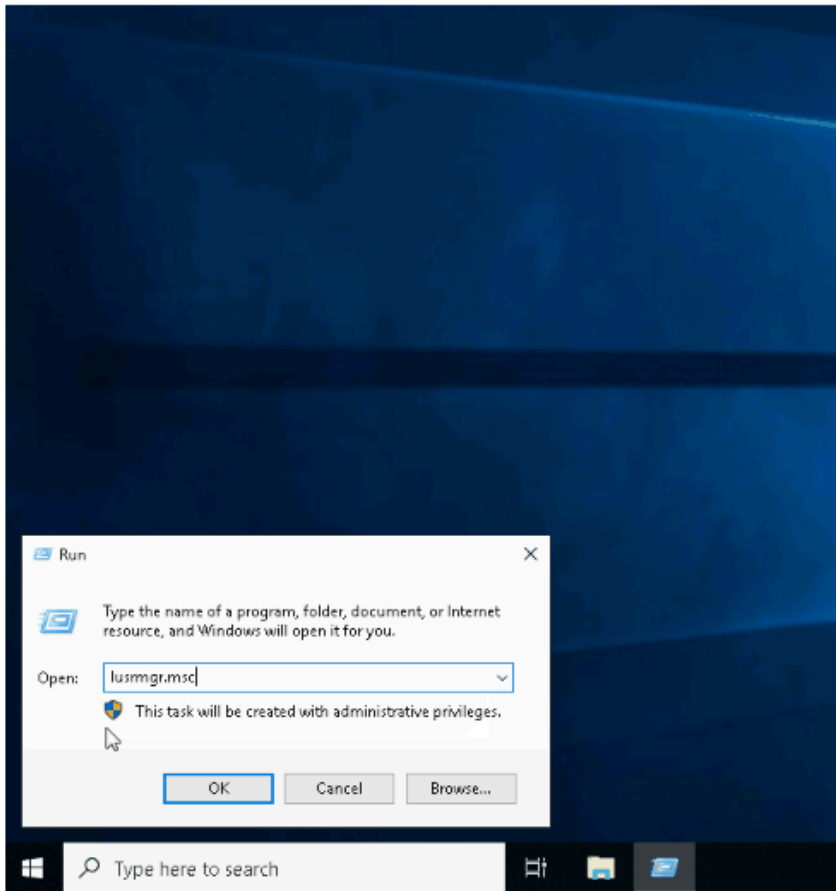
Each user profile will have the same folders; a few of them are:

Each user profile will have the same folders; a few of them are:

- Desktop
- Documents
- Downloads
- Music
- Pictures

Another way to access this information, and then some, is using **Local User and Group Management**.

Right-click on the Start Menu and click **Run**. Type **lusrmgr.msc**. See below



**Note:** The Run Dialog Box allows us to open items quickly.

Back to lusrmgr, you should see two folders: **Users** and **Groups**.

Back to lusrmgr, you should see two folders: **Users** and **Groups**.

If you click on Groups, you see all the names of the local groups along with a brief description for each group.

Each group has permissions set to it, and users are assigned/added to groups by the Administrator. When a user is assigned to a group, the user inherits the permissions of that group. A user can be assigned to multiple groups.

**Note:** If you click on **Add someone else to this PC** from **Other users**, it will open **Local Users and Management**.

The large majority of home users are logged into their Windows systems as local administrators. Remember from the previous task that any user with administrator as the account type can make changes to the system.

A user doesn't need to run with high (elevated) privileges on the system to run tasks that don't require such privileges, such as surfing the Internet, working on a Word document, etc. This elevated privilege increases the risk of system compromise because it makes it easier for malware to infect the system. Consequently, since the user account can make changes to the system, the malware would run in the context of the logged-in user.

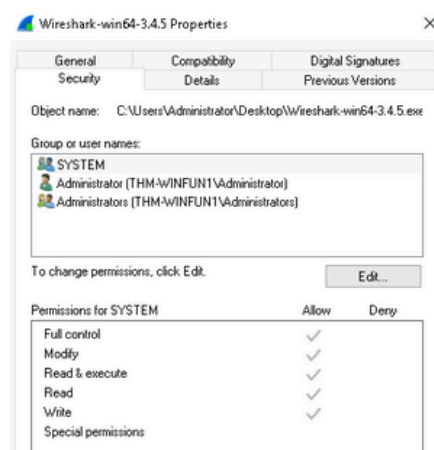
To protect the local user with such privileges, Microsoft introduced **User Account Control (UAC)**. This concept was first introduced with the short-lived [Windows Vista](#) and continued with versions of Windows that followed.

**Note:** UAC (by default) doesn't apply for the built-in local administrator account.

How does UAC work? When a user with an account type of administrator logs into a system, the current session doesn't run with elevated permissions. When an operation requiring higher-level privileges needs to execute, the user will be prompted to confirm if they permit the operation to run.

Let's look at the program on the account you're currently logged into, the built-in administrator account—Right-click to view its Properties.

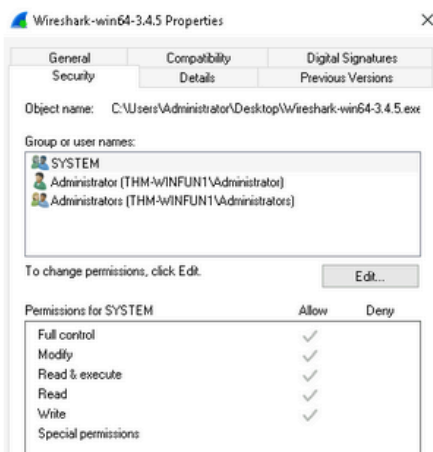
In the Security tab, we can see the users/groups and their permissions to this file. Notice that the standard user is not listed.



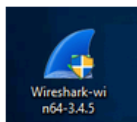
Log in as the standard user and try to install this program. To do this, you can remote desktop into the machine as the standard user account.

**Note:** You have the username and password for the standard user. It's visible in `lusrmgr.msc`.

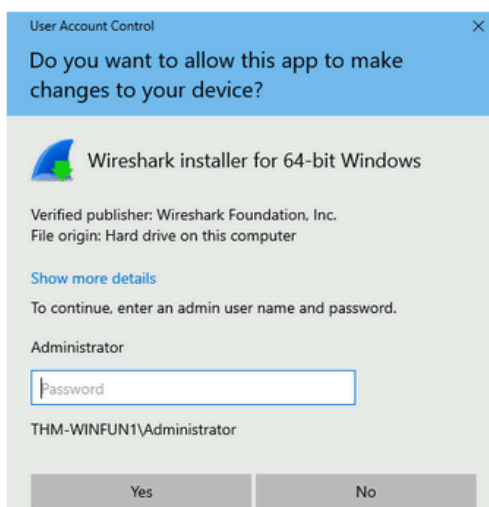
Before installing the program, notice the icon. Do you see the difference? When you're logged in as the standard user, the shield icon is on the program's default icon. See below.



This shield icon is an indicator that UAC will prompt to allow higher-level privileges to install the program.



Double-click the program, and you'll see the UAC prompt. Notice that the built-in administrator account is already set as the user name and prompts the account's password. See below.



After some time, if a password is not entered, the UAC prompt disappears, and the program does not install.

This feature reduces the likelihood of malware successfully compromising your system. You can read more about UAC [here](#).



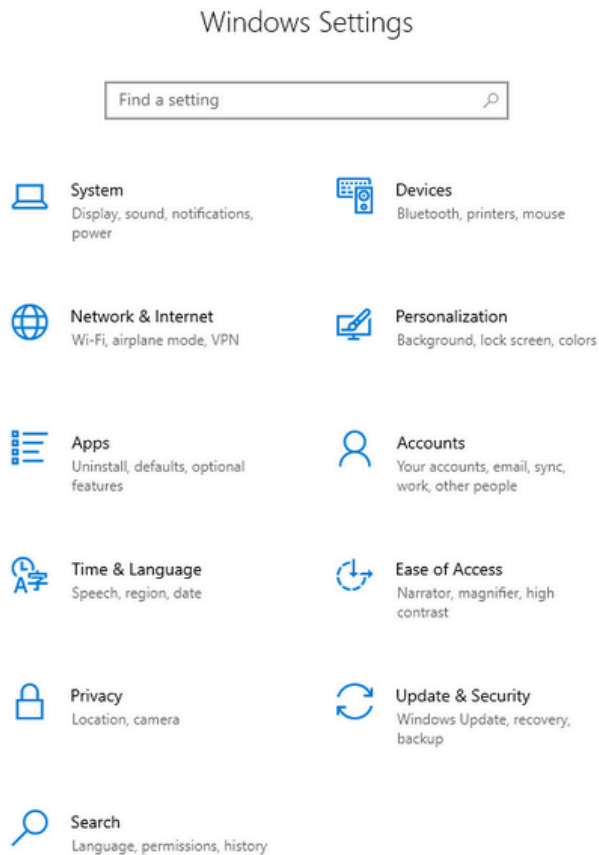
On a Windows system, the primary locations to make changes are the Settings menu and the Control Panel.

For a long time, the Control Panel has been the go-to location to make system changes, such as adding a printer, uninstall a program, etc.

The Settings menu was introduced in Windows 8, the first Windows operating system catered to touch screen tablets, and is still available in Windows 10. As a matter of fact, the Settings menu is now the primary location a user goes to if they are looking to change the system.

There are similarities and differences between the two menus. Below are screenshots of each.

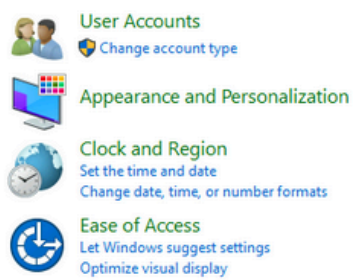
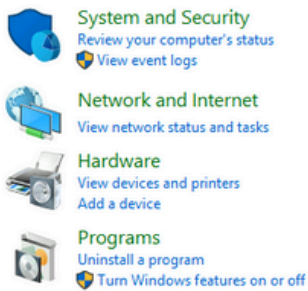
#### Settings:



## Control Panel:

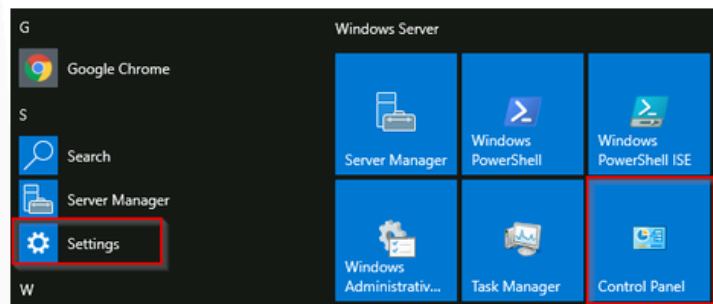
Adjust your computer's settings

View by: Category ▾



**Note:** The icons for Settings might be different in the version of Windows on your personal device.

Both can be accessed from the Start Menu. See below.

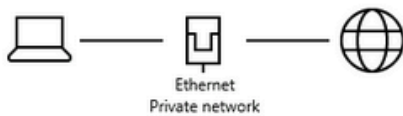


Control Panel is the menu where you will access more complex settings and perform more complex actions. In some cases, you can start in Settings and end up in the Control Panel.

For example, in Settings, click on **Network & Internet**. From here, click on **Change adapter options**.

# Status

## Network status




### You're connected to the Internet

If you have a limited data plan, you can make this network a metered connection or change other properties.

[Change connection properties](#)

[Show available networks](#)

## Change your network settings

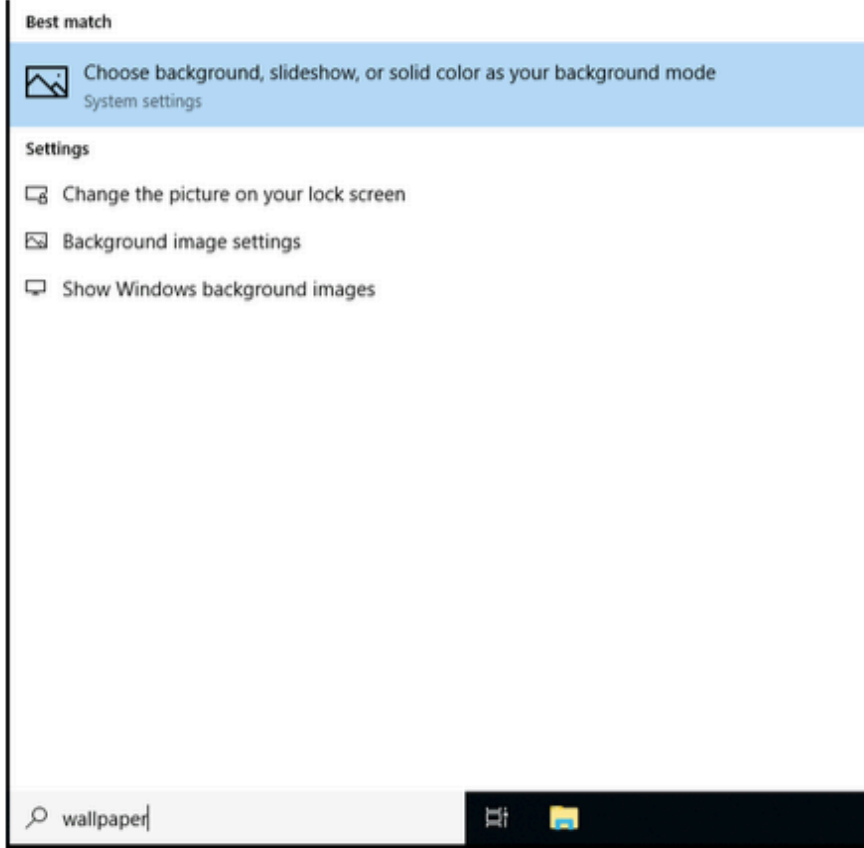
**Change adapter options**  
View network adapters and change connection settings.

Notice that the next window that pops up is from the Control Panel.

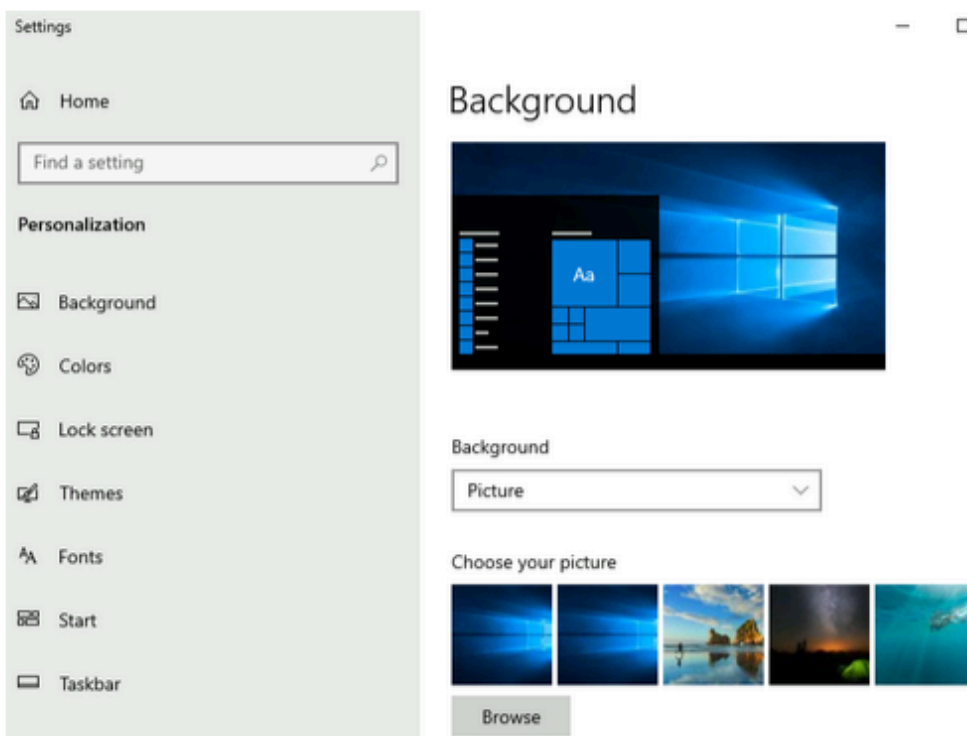


If you're unclear which to open if you wish to change a setting, use the Start menu and search for it.

In the example below, the search was 'wallpaper.' Notice that few results were returned.



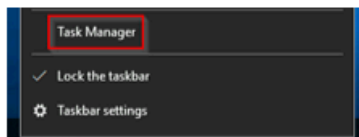
If we click on the Best match, a window to the Settings menu appears to make changes to the wallpaper.



The last subject that will be touched on in this module is the **Task Manager**.

The Task Manager provides information about the applications and processes currently running on the system. Other information is also available, such as how much **CPU** and **RAM** are being utilized, which falls under **Performance**.

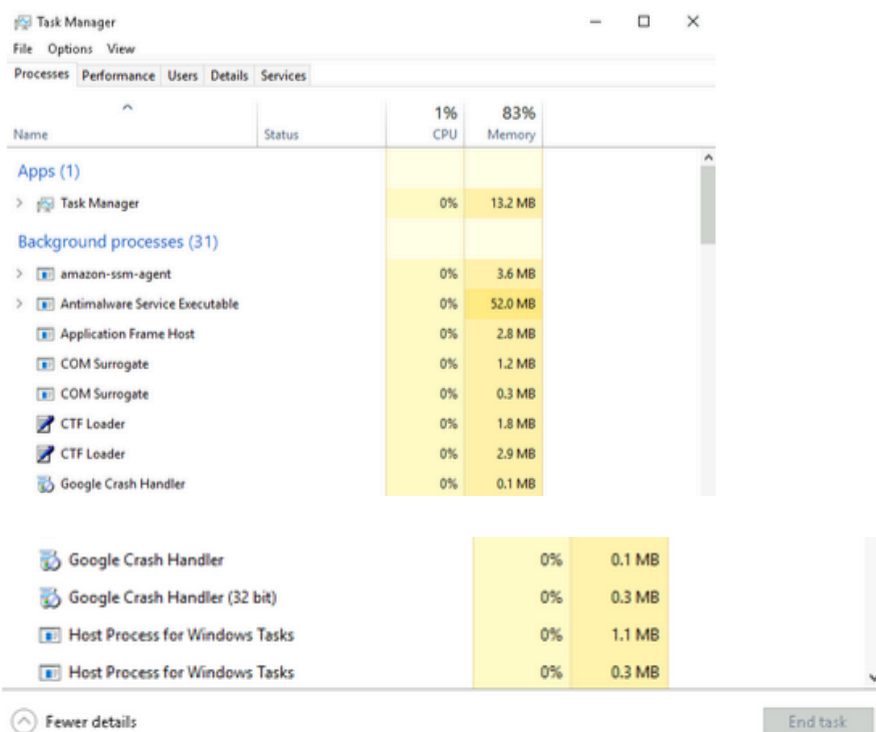
You can access the Task Manager by right-clicking the taskbar.



Task Manager will open in Simple View and won't show much information.



Click on **More details**, and the view changes.



You can refer to this [blog post](#) for more detailed information about the Task Manager.

If you wish to learn more about the core Windows processes and what each process is responsible for, visit the [Core Windows Processes](#) room.

The keyboard shortcut to open Task Manager in Windows is:

`Ctrl + Shift + Esc`

This will immediately bring up the Task Manager window. Alternatively, you can also use:

`Ctrl + Alt + Delete`

and then select Task Manager from the menu that appears.

<https://www.howtogeek.com/405806/windows-task-manager-the-complete-guide/>