Windows Fundamentals Part 1

Learned:

- User Account Control prevents programs from running with elevated privileges which reduces the risk of malware.

- The Windows/System32 folder contains critical OS files and protecting it is important to prevent the system from being vulnerable.

- Monitoring the Task Manager can help identify suspicious programs that could indicate malware.

The File System

The file system used in modern versions of Windows is the **New Technology File System** or NTFS .

Before NTFS, there was **FAT16/FAT32** (File Allocation Table) and **HPFS** (High Performance File System).

You still see FAT partitions in use today. For example, you typically see FAT partitions in USB devices, MicroSD cards, etc. but traditionally not on personal Windows computers/laptops or Windows servers.

NTFS is known as a journaling file system. In case of a failure, the file system can automatically repair the folders/files on disk using information stored in a log file. This function is not possible with FAT.

NTFS

- Supports files larger than 4GB
- Set specific permissions on folders and files
- Folder and file compression
- Encryption (Encryption File System or **EFS**)

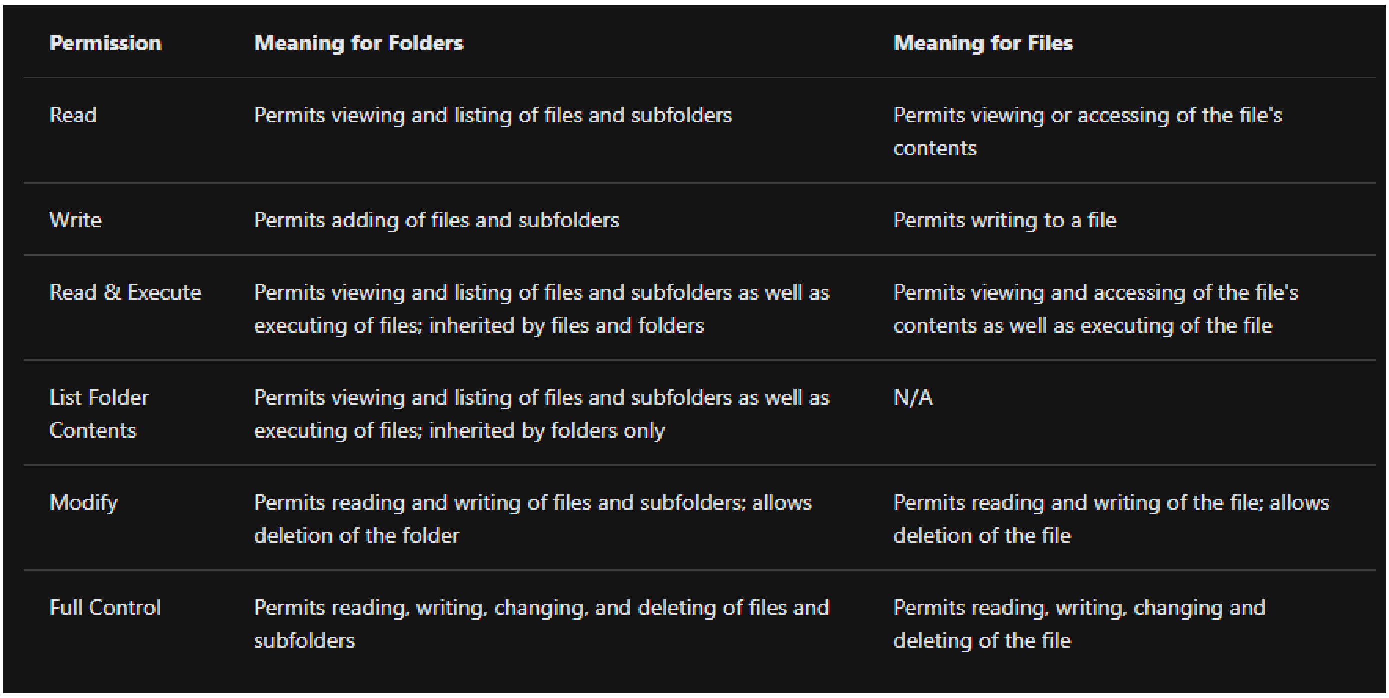
If you're running Windows You can check the Properties (right-click) of the drive your operating system is installed on, typically the C drive (C:\).

On NTFS volumes, you can set permissions that grant or deny access to files and folders.

The permissions are:

- **Full control**
- **Modify**
- **Read & Execute**
- **List folder contents**

- **Read**
- **Write**

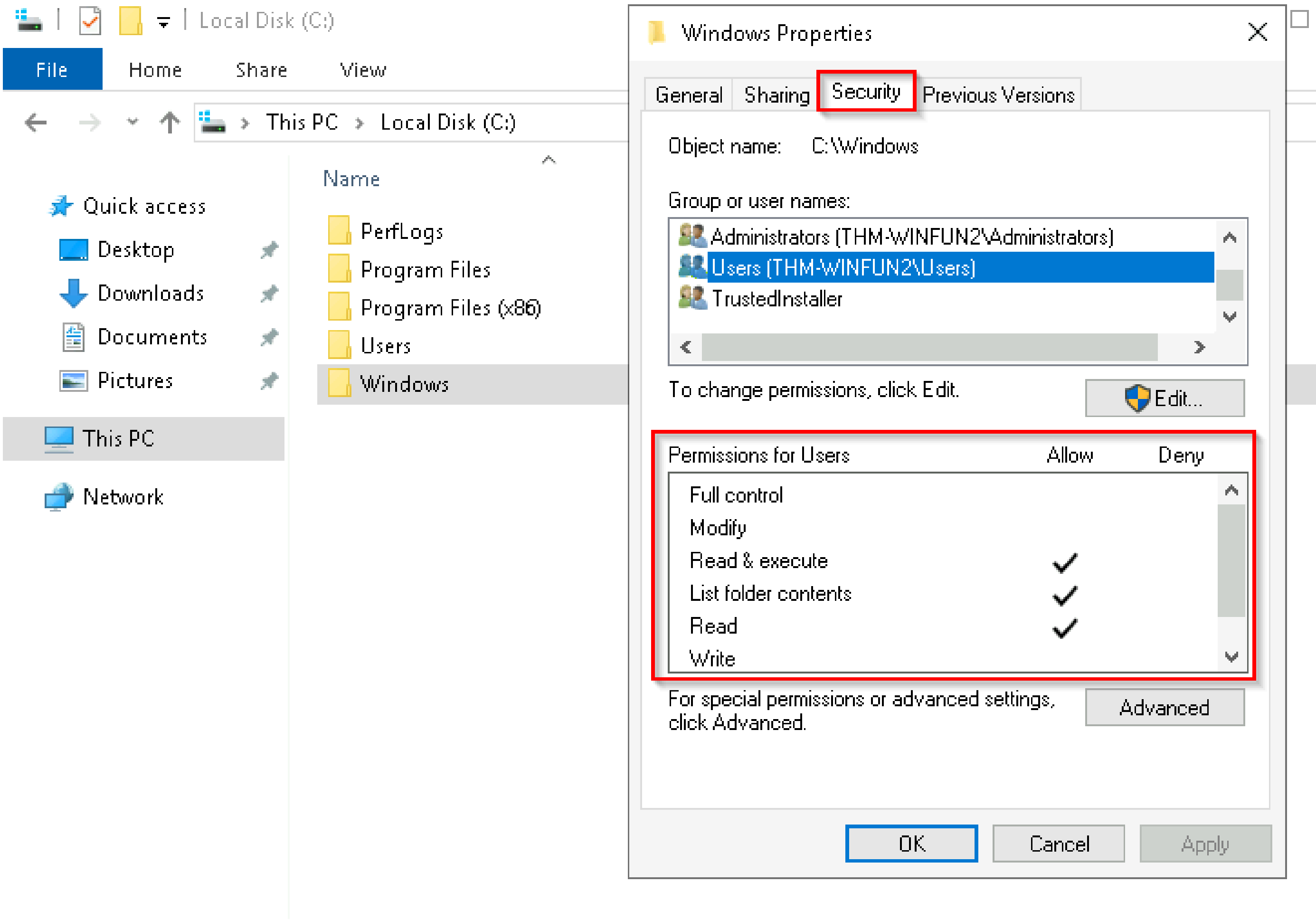


Permission	Meaning for Folders	Meaning for Files
Read	Permits viewing and listing of files and subfolders	Permits viewing or accessing of the file's contents
Write	Permits adding of files and subfolders	Permits writing to a file
Read & Execute	Permits viewing and listing of files and subfolders as well as executing of files; inherited by files and folders	Permits viewing and accessing of the file's contents as well as executing of the file
List Folder Contents	Permits viewing and listing of files and subfolders as well as executing of files; inherited by folders only	N/A
Modify	Permits reading and writing of files and subfolders; allows deletion of the folder	Permits reading and writing of the file; allows deletion of the file
Full Control	Permits reading, writing, changing, and deleting of files and subfolders	Permits reading, writing, changing and deleting of the file

How can you view the permissions for a file or folder?

- Right-click the file or folder you want to check for permissions.
- From the context menu, select `Properties` .
- Within Properties, click on the `Security` tab.
- In the `Group or user names` list, select the user, computer, or group whose permissions you want to view.

In the below image, you can see the permissions for the `Users` group for the Windows folder.



Object name: C:\Windows

Group or user names:

- Administrators (THM-WINFUN2\Administrators)
- Users (THM-WINFUN2\Users)
- TrustedInstaller

To change permissions, click Edit.

Permissions for Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.

Another feature of NTFS is **Alternate Data Streams** (**ADS**).

Alternate Data Streams (ADS) is a file attribute specific to Windows NTFS (New Technology File System).

Every file has at least one data stream (`$DATA`), and ADS allows files to contain more than one stream of data. Natively Window Explorer doesn't display ADS to the user. There are 3rd party executables that can be used to view this data, but Powershell gives you the ability to view ADS for files.

Malware writers have used ADS to hide data.

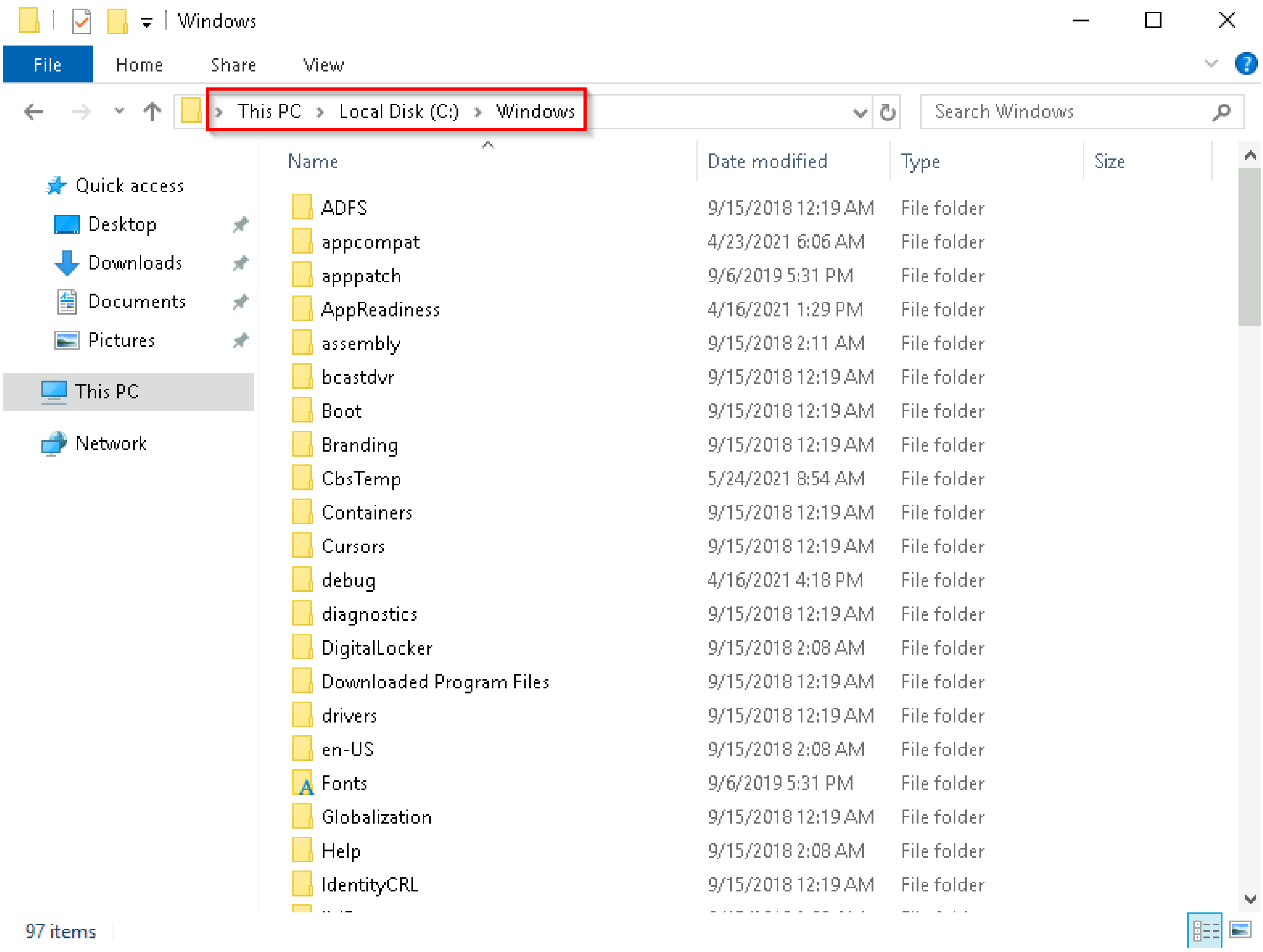
Not all its uses are malicious. For example, when you download a file from the Internet, there are identifiers written to ADS to identify that the file was downloaded from the Internet.

Windows / System32 Folders

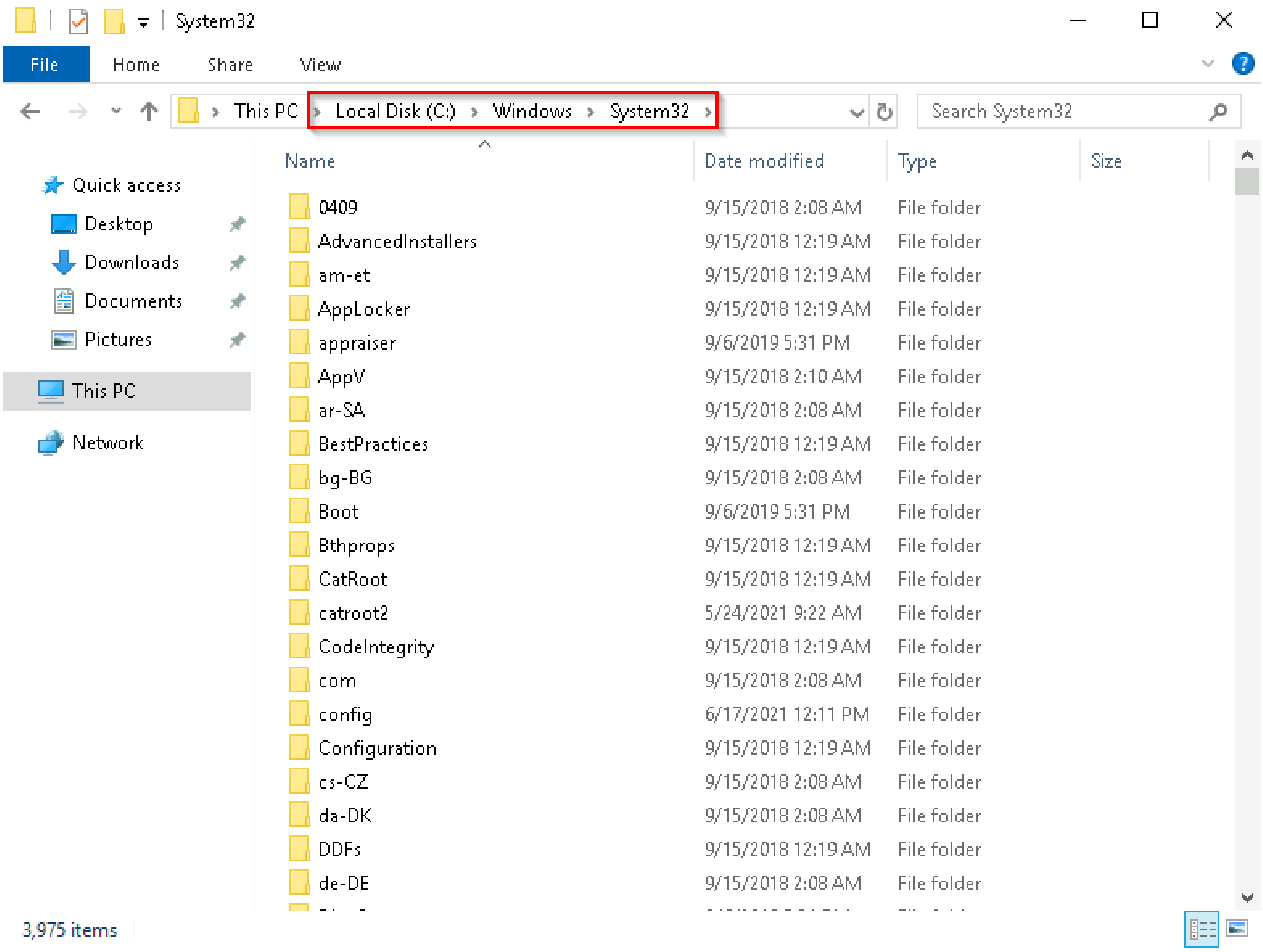
The Windows folder (`C:\Windows`) is traditionally known as the folder which contains the Windows operating system.

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%` .



Name	Date modified	Type	Size
ADFS	9/15/2018 12:19 AM	File folder	
appcompat	4/23/2021 6:06 AM	File folder	
apppatch	9/6/2019 5:31 PM	File folder	
AppReadiness	4/16/2021 1:29 PM	File folder	
assembly	9/15/2018 2:11 AM	File folder	
bcastdvr	9/15/2018 12:19 AM	File folder	
Boot	9/15/2018 12:19 AM	File folder	
Branding	9/15/2018 12:19 AM	File folder	
CbsTemp	5/24/2021 8:54 AM	File folder	
Containers	9/15/2018 12:19 AM	File folder	
Cursors	9/15/2018 12:19 AM	File folder	
debug	4/16/2021 4:18 PM	File folder	
diagnostics	9/15/2018 12:19 AM	File folder	
DigitalLocker	9/15/2018 2:08 AM	File folder	
Downloaded Program Files	9/15/2018 12:19 AM	File folder	
drivers	9/15/2018 12:19 AM	File folder	
en-US	9/15/2018 2:08 AM	File folder	
Fonts	9/6/2019 5:31 PM	File folder	
Globalization	9/15/2018 12:19 AM	File folder	
Help	9/15/2018 2:08 AM	File folder	
IdentityCRL	9/15/2018 12:19 AM	File folder	



Name	Date modified	Type	Size
0409	9/15/2018 2:08 AM	File folder	
AdvancedInstallers	9/15/2018 12:19 AM	File folder	
am-et	9/15/2018 12:19 AM	File folder	
AppLocker	9/15/2018 12:19 AM	File folder	
appraiser	9/6/2019 5:31 PM	File folder	
AppV	9/15/2018 2:10 AM	File folder	
ar-SA	9/15/2018 2:08 AM	File folder	
BestPractices	9/15/2018 12:19 AM	File folder	
bg-BG	9/15/2018 2:08 AM	File folder	
Boot	9/6/2019 5:31 PM	File folder	
Bthprops	9/15/2018 12:19 AM	File folder	
CatRoot	9/15/2018 12:19 AM	File folder	
catroot2	5/24/2021 9:22 AM	File folder	
CodeIntegrity	9/15/2018 12:19 AM	File folder	
com	9/15/2018 2:08 AM	File folder	
config	6/17/2021 12:11 PM	File folder	
Configuration	9/15/2018 12:19 AM	File folder	
cs-CZ	9/15/2018 2:08 AM	File folder	
da-DK	9/15/2018 2:08 AM	File folder	
DDFs	9/15/2018 12:19 AM	File folder	
de-DE	9/15/2018 2:08 AM	File folder	

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.

User Accounts, Profiles, and Permissions

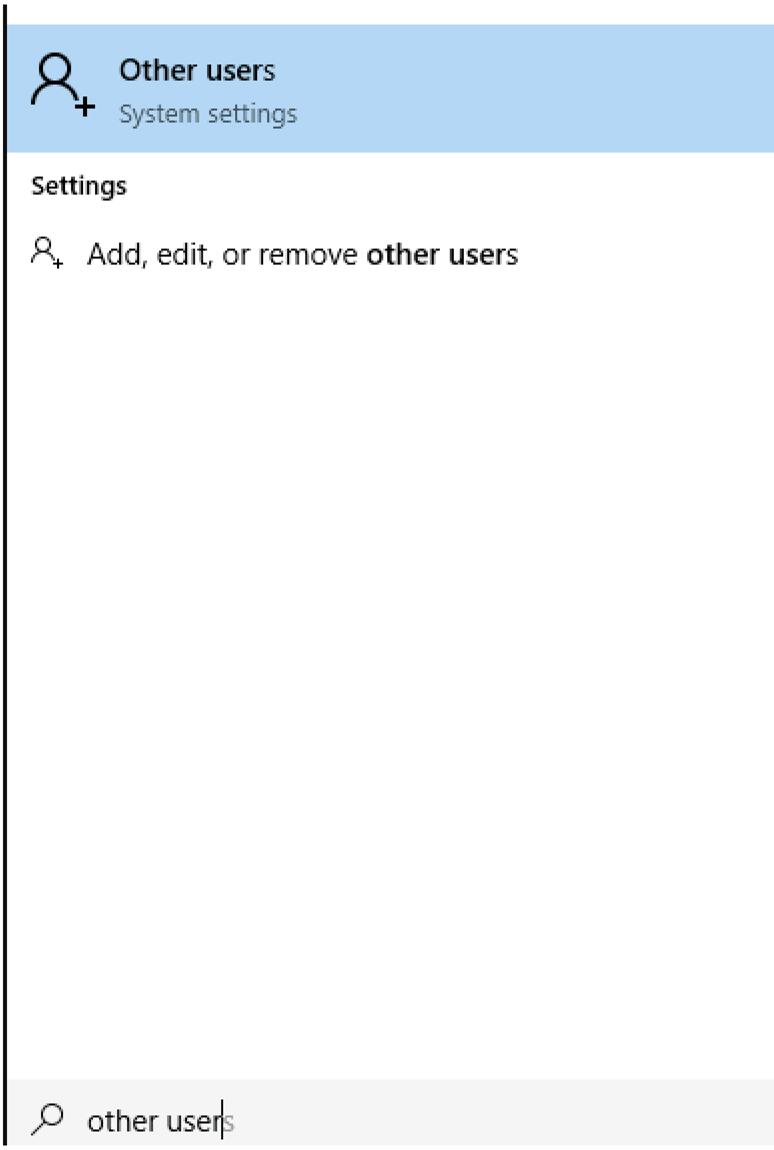
User accounts can be one of two types on a typical local Windows system: **Administrator** & **Standard User**.

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.

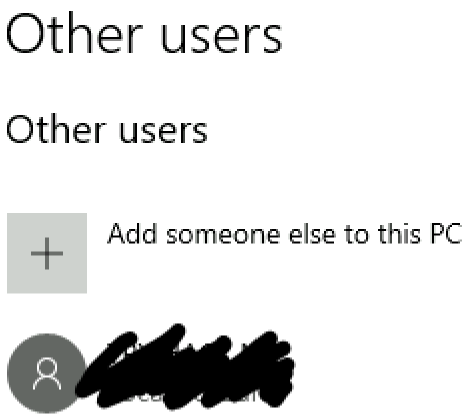
You are currently logged in as an Administrator. There are several ways to determine which user accounts exist on the system.

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



other users

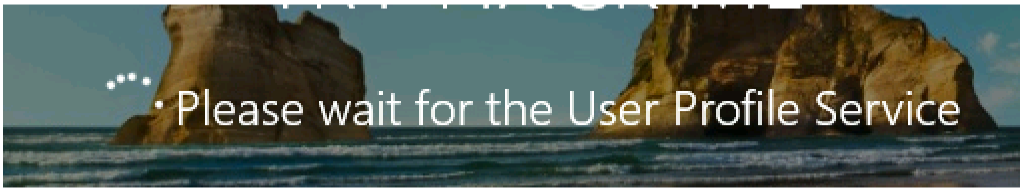
If you click on it, a Settings window should now appear. See below.



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.

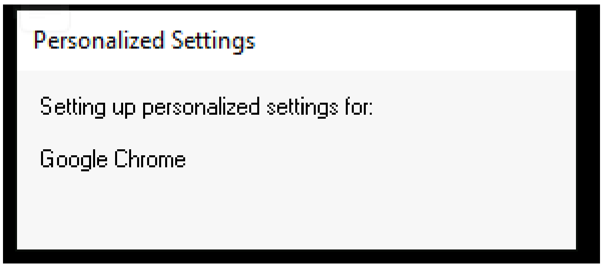
For example, the user profile folder for the user account Max will be C:\Users\Max.

The creation of the user's profile is done upon login. When a new user account logs in 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.



Please wait for the User Profile Service

Once logged in, the user will see a dialog box indicating that the profile is in creation.



Personalized Settings

Setting up personalized settings for:

Google Chrome

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

- Desktop
- Documents
- Downloads
- Music
- Pictures

Another way to access this information 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 will open items quickly.

In 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.

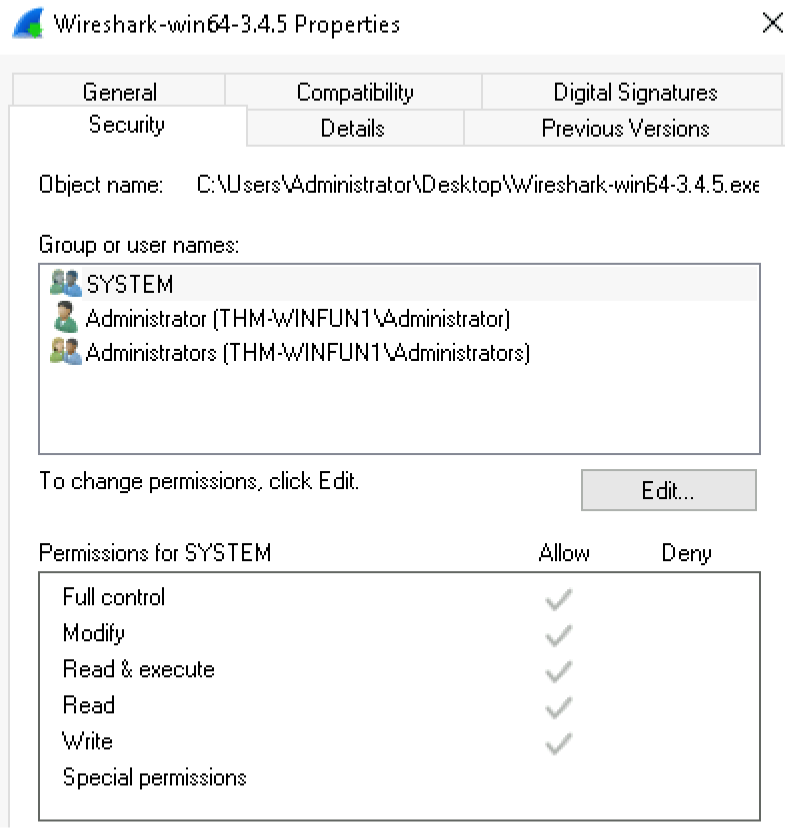
User Account Control

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. 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).

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.

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



Object name: C:\Users\Administrator\Desktop\Wireshark-win64-3.4.5.exe

Group or user names:

SYSTEM
Administrator (THM-WINFUN1\Administrator)
Administrators (THM-WINFUN1\Administrators)

To change permissions, click Edit.

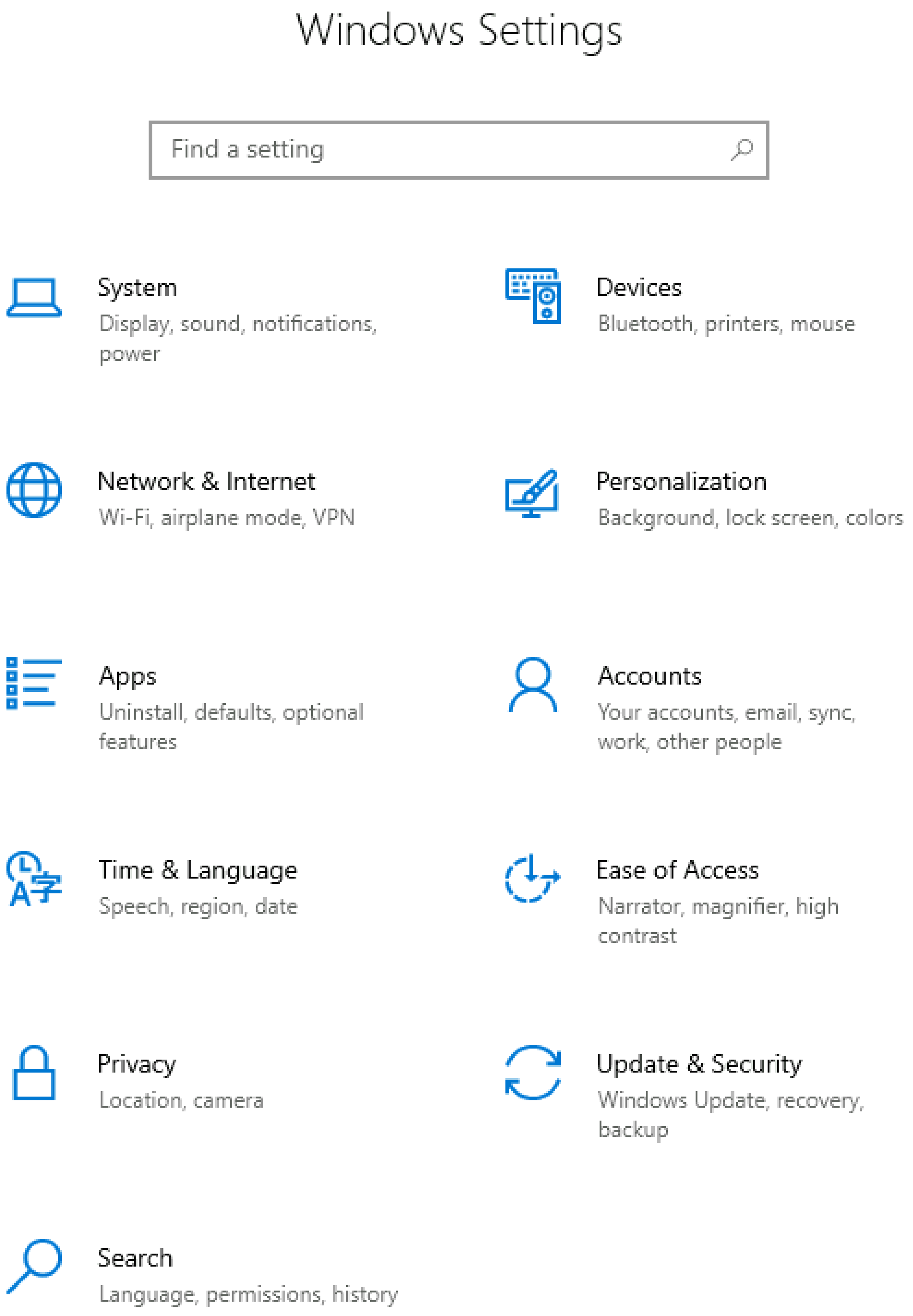
Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

Settings and Control Panel

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 :



Windows Settings

Find a setting

System
Display, sound, notifications, power

Devices
Bluetooth, printers, mouse

Network & Internet
Wi-Fi, airplane mode, VPN

Personalization
Background, lock screen, colors

Apps
Uninstall, defaults, optional features

Accounts
Your accounts, email, sync, work, other people

Time & Language
Speech, region, date

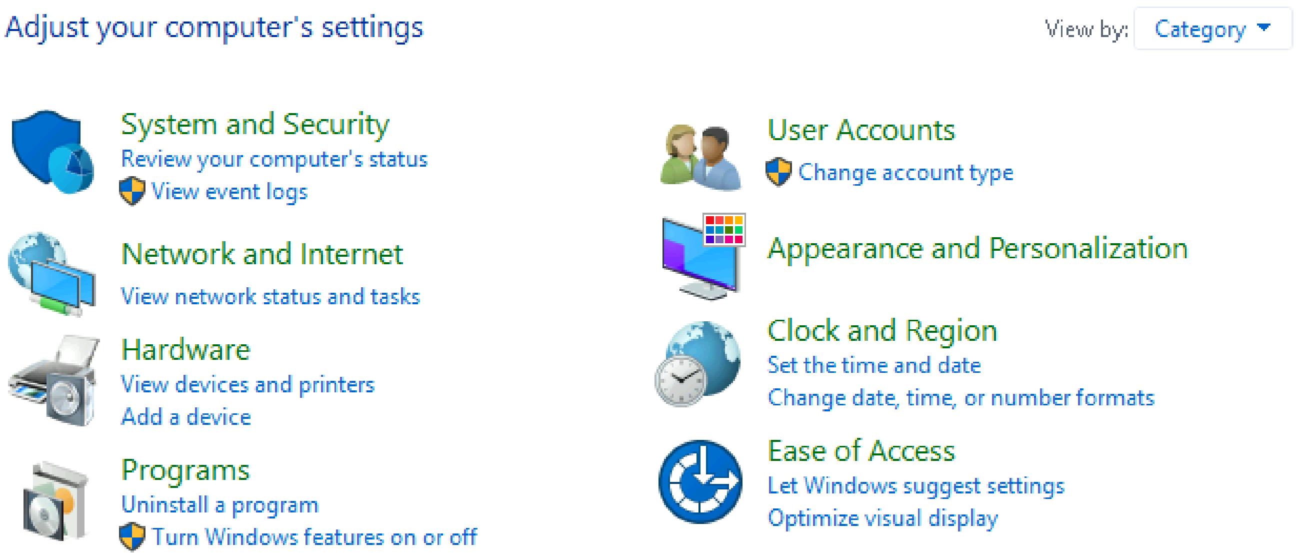
Ease of Access
Narrator, magnifier, high contrast

Privacy
Location, camera

Update & Security
Windows Update, recovery, backup

Search
Language, permissions, history

Control Panel :



Adjust your computer's settings

View by: Category

System and Security
Review your computer's status
View event logs

Network and Internet
View network status and tasks

Hardware
View devices and printers
Add a device

Programs
Uninstall a program
Turn Windows features on or off

User Accounts
Change account type

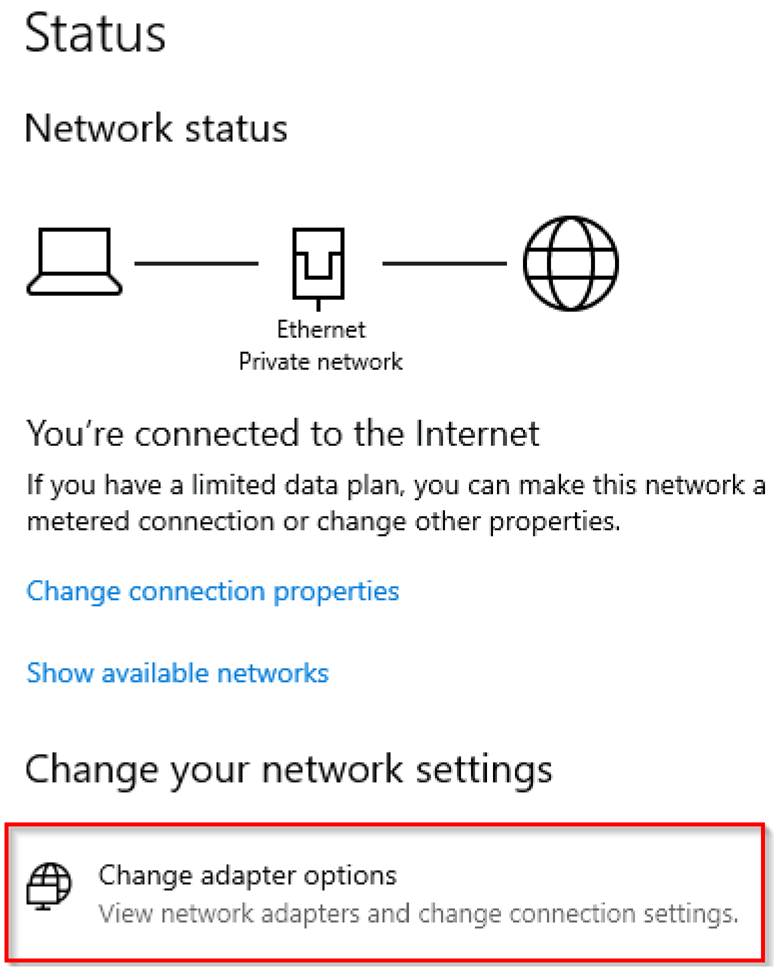
Appearance and Personalization

Clock and Region
Set the time and date
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

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.

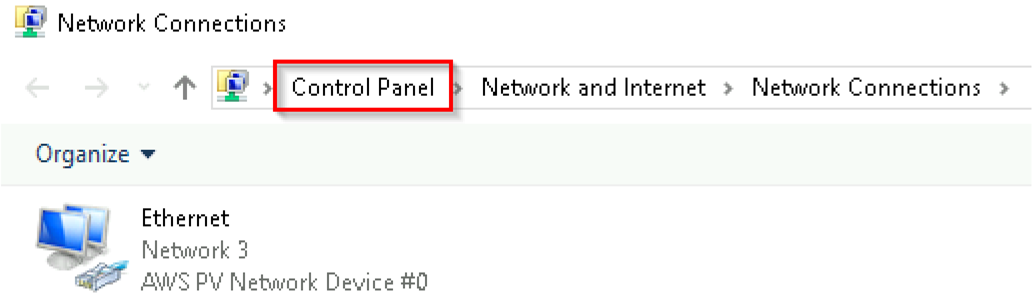
Change connection properties

Show available networks

Change your network settings

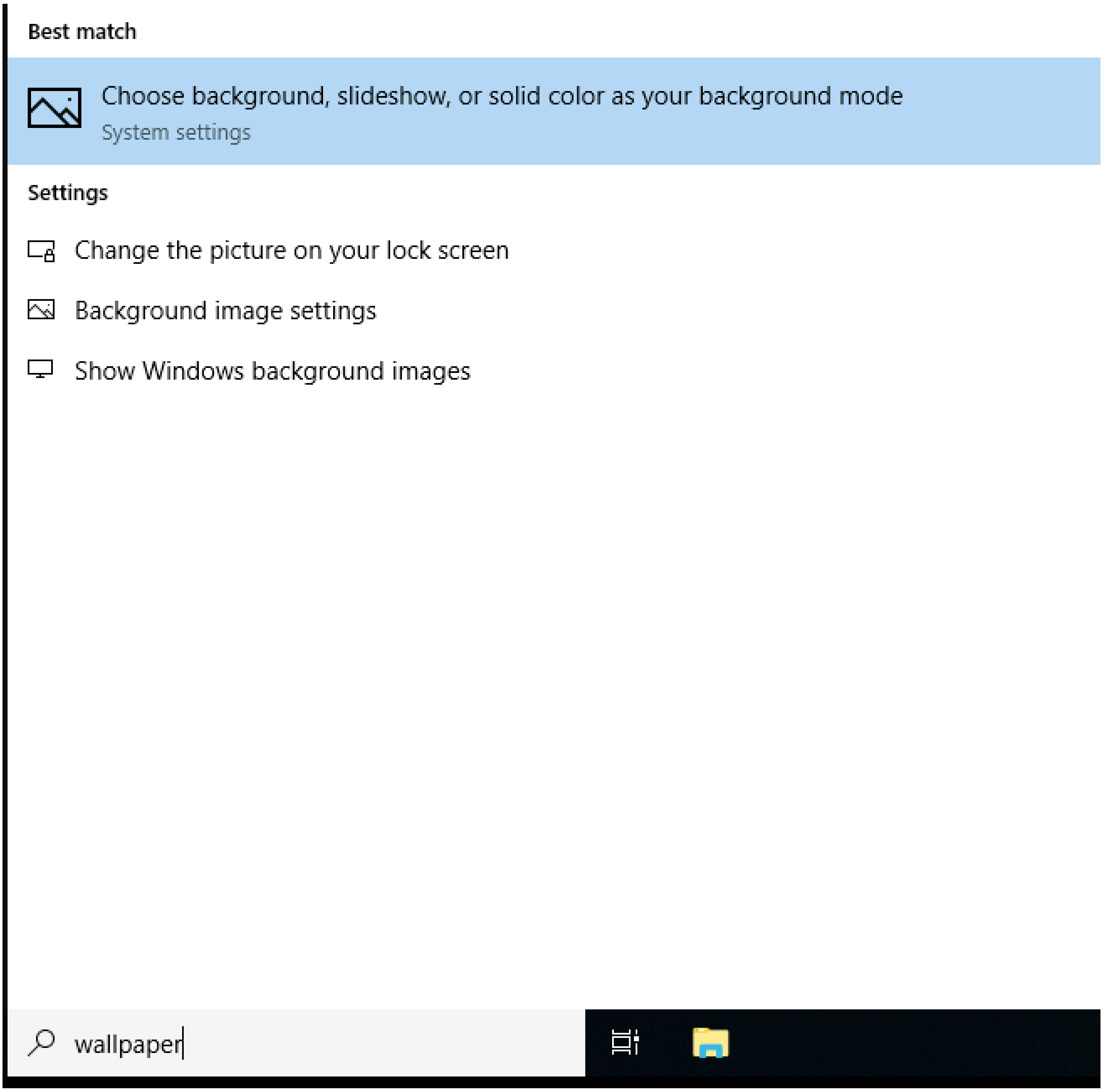
Change adapter options
View network adapters and change connection settings.

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

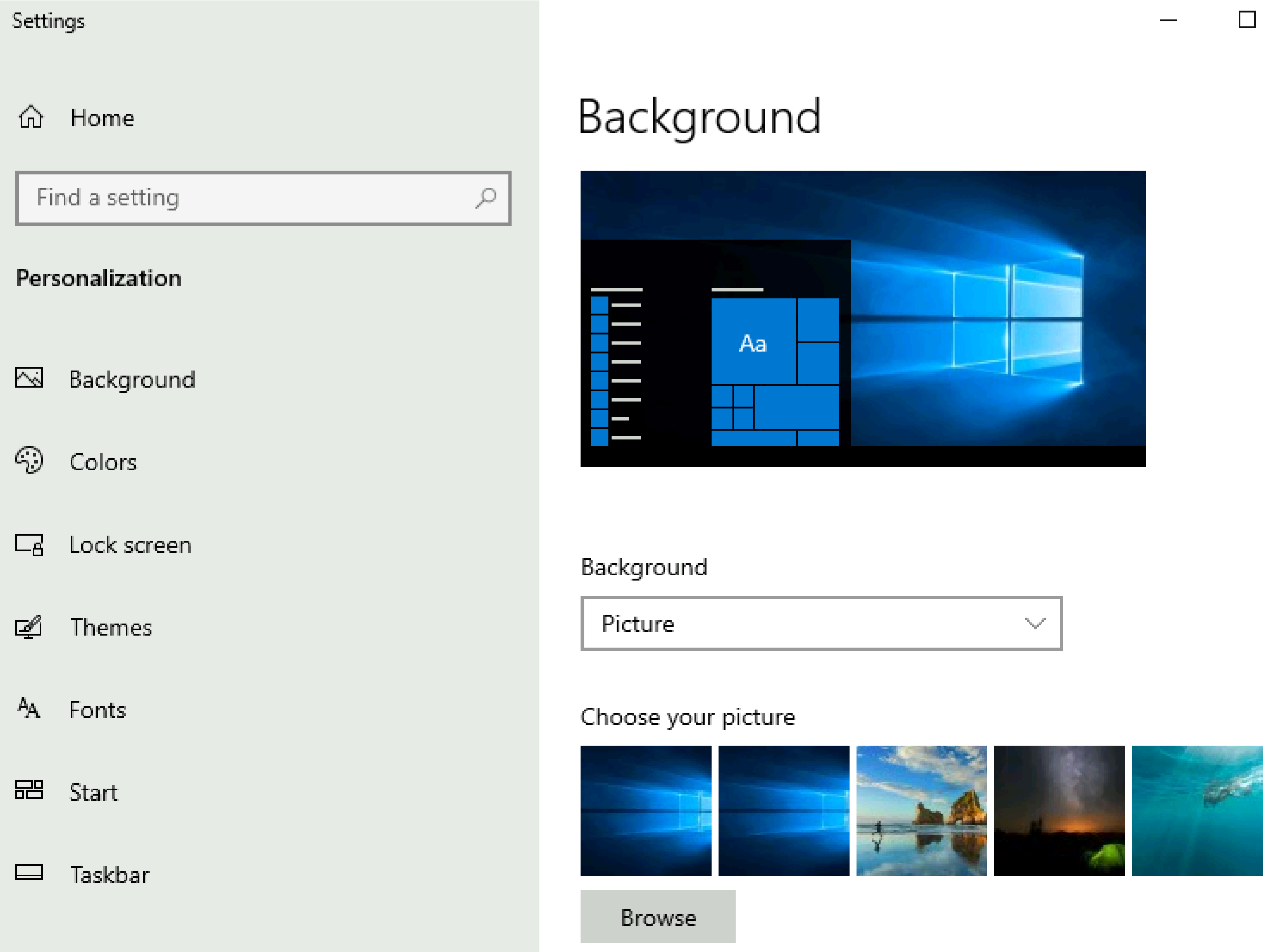


If you're unclear which to open if you wish to change a setting, use the Start menu and search for it.

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


Best match
Choose background, slideshow, or solid color as your background mode
System settings
Settings
Change the picture on your lock screen
Background image settings
Show Windows background images
wallpaper

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



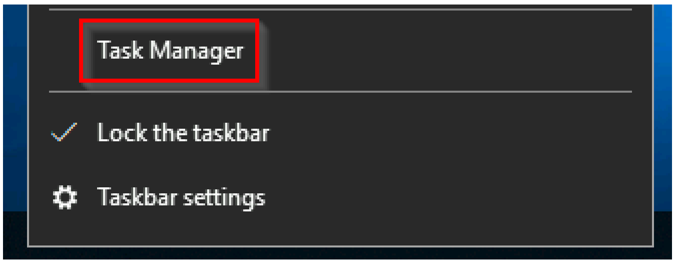
Background

Picture

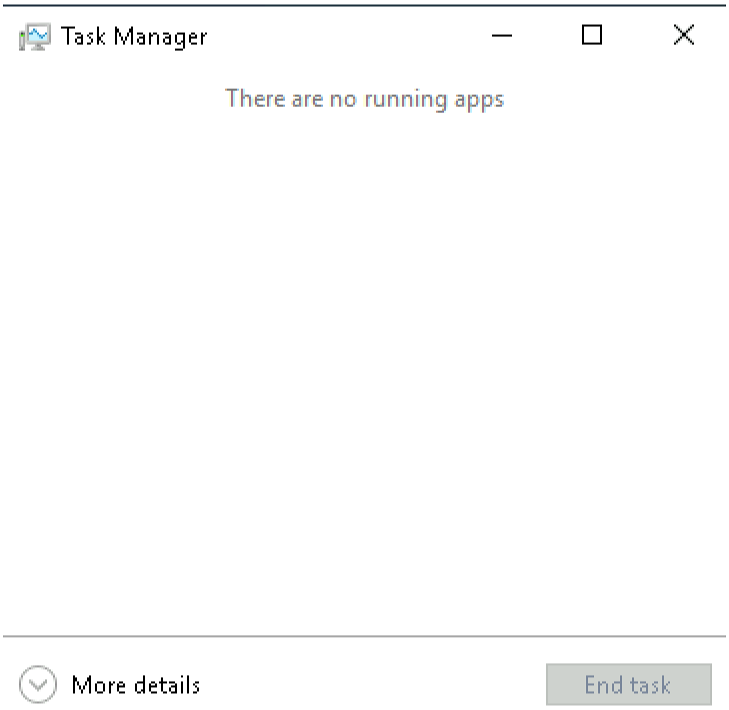
Task Manager

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.

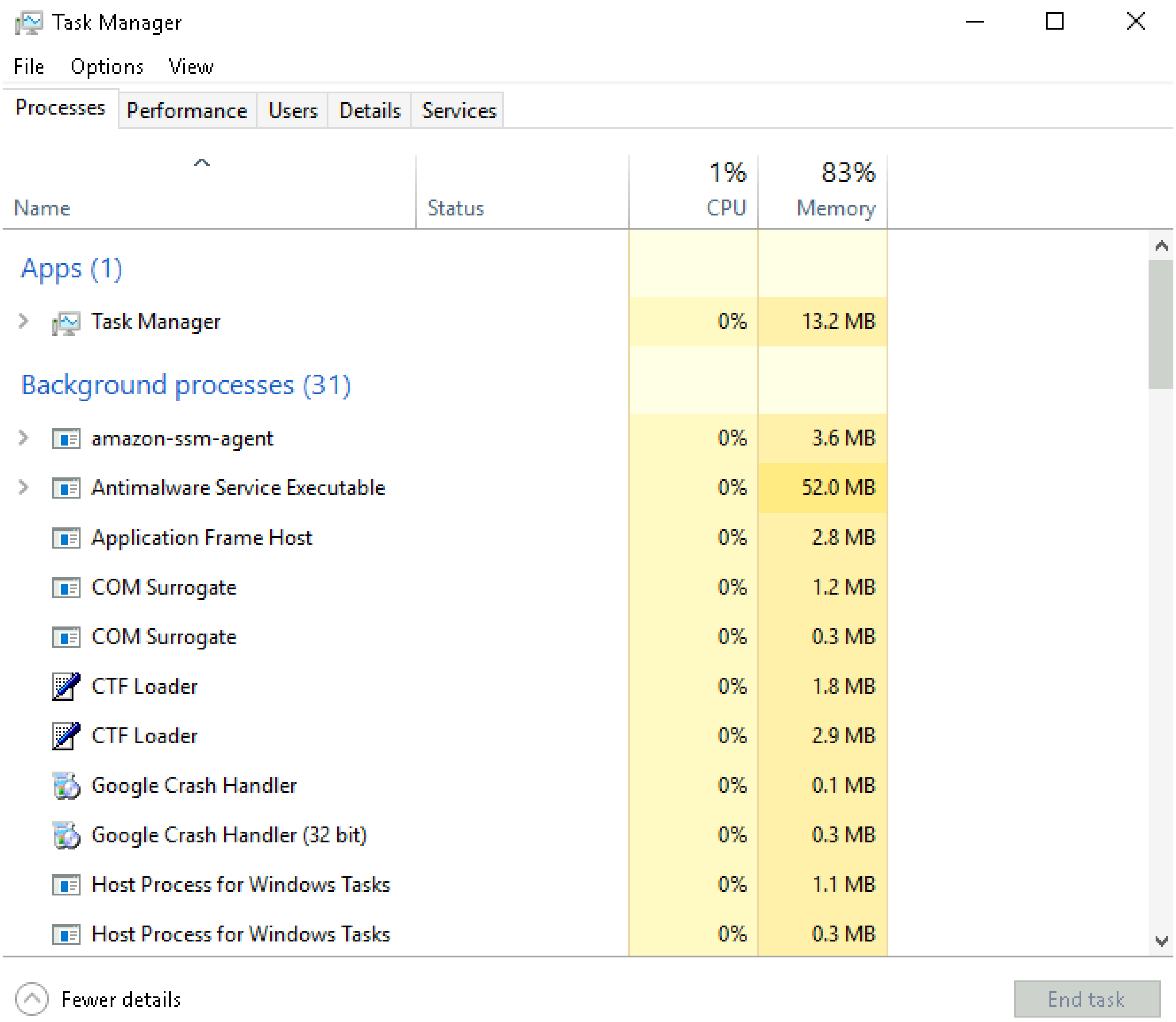


Task Manager will open in Simple View and won't show much information.



There are no running apps

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



Name	Status	1% CPU	83% Memory
Apps (1)			
Task Manager		0%	13.2 MB
Background processes (31)			
amazon-ssm-agent		0%	3.6 MB
Antimalware Service Executable		0%	52.0 MB
Application Frame Host		0%	2.8 MB
COM Surrogate		0%	1.2 MB
COM Surrogate		0%	0.3 MB
CTF Loader		0%	1.8 MB
CTF Loader		0%	2.9 MB
Google Crash Handler		0%	0.1 MB
Google Crash Handler (32 bit)		0%	0.3 MB
Host Process for Windows Tasks		0%	1.1 MB
Host Process for Windows Tasks		0%	0.3 MB