Check All of the Processes on Your PC for Intruders Using the Task Manager

Using the information given in this article you will be able to:

- ✓ Configure the Task Manager to your requirements,
- ✓ Clearly identify all the processes and assign corresponding programs,
- ✓ Properly close applications that are no longer working.

Every single program, service or tool that runs on your PC has one or more corresponding process. Many processes are activated during the Windows boot process, and when you launch applications, many additional processes are also started. If your computer freezes up when running a particular application, you will be asked how to proceed by a Windows error message.

If you're lucky, the message will tell you exactly which application is at fault. However, it most cases, Windows will display a cryptic message that at best just mentions a process name.

When a problem like this strikes, you should take a look in the Task Manager to check which processes are running, and look for any that are potentially suspicious. In the Task Manager you will see a list of all the processes which Windows uses to manage the services and programs running on your PC.

In this article, I'll show you which processes Windows needs and how you can control them with the help of the Task Manager.

Process Tasks and Functions in Windows

What processes do

Processes are the basic building blocks that underpin every program and service running on your PC. Every time a program is launched, a new process is started corresponding to the program, which is granted certain privileges by the operating system.

Windows responds to process problems in various ways. If a process is experiencing problems, you may see a message telling you that the program is not responding, or even a message telling you that the process has crashed. Since processes correspond to everything running on your PC, you can often spot a virus or Trojan infection by checking the running processes.

Take Control of the Processes on Your PC Using the Task Manager

Launch Task Manager

The Task Manager is the central place in Windows to manage all running processes. You can open the Task Manager by pressing the key combination and then clicking on the link shown in the Windows security window.

Alternatively, right-click on the taskbar and select **Task Manager (Start Task Manager** in 7) from the pop-up menu.

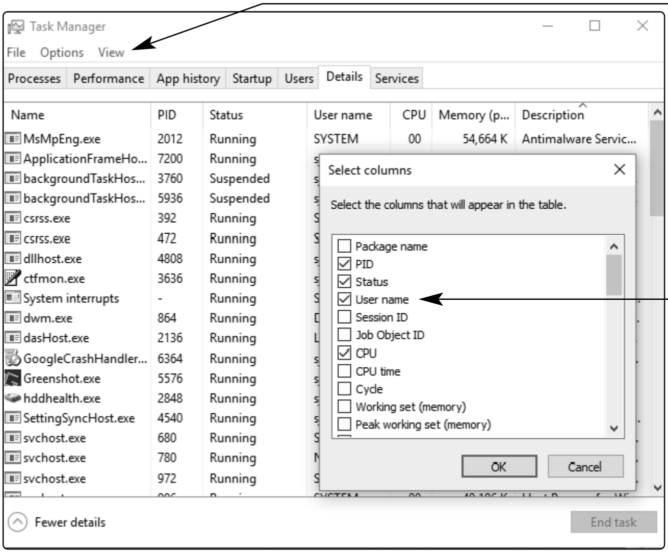
Check the processes

Click on the **Details** tab (**Processes** in Windows 7) within the Task Manager to see a list of the active processes and their relative CPU usage. The process table in the Task Manager contains all the processes that are currently running, including all applications and system services.

Change the information displayed

If you want to change the information displayed in the Task Manager, right-click the column heading and choose **Select Columns** (click **View** > **Select Columns in Windows 7**).

You can then add extra performance measurement data to the display, or remove columns that you don't need.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	PID	Status	User name	CPU	Memory (p...	Description
MsMpEng.exe	2012	Running	SYSTEM	00	54,664 K	Antimalware Servic...
ApplicationFrameHo...	7200	Running	s			
backgroundTaskHos...	3760	Suspended	s			
backgroundTaskHos...	5936	Suspended	s			
csrss.exe	392	Running	S			
csrss.exe	472	Running	S			
dllhost.exe	4808	Running	s			
ctfmon.exe	3636	Running	s			
System interrupts	-	Running	S			
dwm.exe	864	Running	D			
dasHost.exe	2136	Running	L			
GoogleCrashHandler...	6364	Running	s			
Greenshot.exe	5576	Running	s			
hddhealth.exe	2848	Running	s			
SettingSyncHost.exe	4540	Running	s			
svchost.exe	680	Running	S			
svchost.exe	780	Running	N			
svchost.exe	972	Running	S			

Select columns

Select the columns that will appear in the table.

- ☐ Package name
- ☑ PID
- ☑ Status
- ☑ User name
- ☐ Session ID
- ☐ Job Object ID
- ☑ CPU
- ☐ CPU time
- ☐ Cycle
- ☐ Working set (memory)
- ☐ Peak working set (memory)

Click View > Select Columns...

... and select the performance measurement data that you require

You can personally configure which information you would like the Task Manager to display in Windows 7

The Task Manager options

The following table lists all the Task Manager's data column options and what they mean:

Process information	Description
PID (Process Identifier)	The ID number assigned to the process by Windows.
CPU Usage (CPU in Windows 8.1)	The percentage of time that the process threads have occupied the processor since the last update.
CPU Time	The total time in seconds that the process has occupied the CPU since it was launched.

Process information	Description
Memory – Private Working Set	The amount of space that the process occupies in main memory (measured in KB).
Memory – Working Set Delta	Changes in the memory load since the last update (in KB). Unlike the System Monitor tool, the Task Manager can show negative values.
Page Faults	Shows how often data is moved from the hard drive page file to RAM because it was not present in memory. This value is accumulated from the point in time when the process was launched.
PF Delta (Page Faults Delta in Windows 7)	Change in the number of page faults since the last update.
Paged Pool (Memory – Paged Pool in Windows 7)	The amount of memory that the process is using in the paging file (in KB). The paging file is an extension to the system RAM that allows data that spills out of the main RAM to be saved to the slower hard drive.
NP Pool (Memory – Non Paged Pool in Windows 7)	The extent of the main RAM (system memory) that is used by the process in KB. This is the data in the main memory that hasn't spilled over to the hard drive.
Base Priority	The base priority of the process determines the order in which processor time is allocated to the threads of the process. Each process is assigned a priority when it starts. The higher the priority, the greater the amount of processor time that is allocated to the process. You can change the priority of a process in the Task Manager, if you have a program that you want to use more of your system resources than the other software running on your machine.

Process information	Description
Handles	The number of object handles in the object table of the process.
Threads	The number of active threads belonging to a process.

How to Find Out More About Processes on Windows

How to identify Windows processes

Whereas some programs can be easily identified from their process name (taskmgr.exe for the Task Manager or Iexplore.exe for Internet Explorer, for example), other important Windows processes hide behind cryptic names.

A summary of important processes

The following table shows you which programs are hiding behind which process names, and whether they can be safely terminated using the Task Manager:

Process	Can be ended?	Description
Csrss.exe	No	This is the part of the Win32 subsystem that is responsible for user mode. Csrss stands for Client/Server Run Time Subsystem. It is responsible for console windows and creating and deleting process threads.
Explorer.exe	Yes	This is the user interface which takes care of displaying components such as the taskbar, desktop and so on, and gives you access to your programs and files. This process is not as important for normal Windows operation as you might think, and can be closed (and relaunched) using the Task Manager.
Idle process	No	This is an individual thread that is run on every processor. It deals with the usage of processor time

Process	Can be ended?	Description
		when it is not being used by other processes or threads.
Lsass.exe	No	This is the local authentication server. It creates the process that is responsible for the authentication of users by the login service.
Mstask.exe	No	This is the task scheduler service that automatically launches processes at a time configured by you.
Services.exe	No	This is the management process for system services. The launch and shutdown of services, as well as all usual interactions with services, are all managed by it.
Smss.exe	No	This is the Session Manager process which is the subsystem responsible for opening user sessions.
Spoolsv.exe	No	This is the print queue service which is responsible for the management of all printing and faxing jobs initiated by the user.
Svchost.exe	No	This is a general process which serves as a host for other processes that are launched by DLLs. That's why you will find multiple instances of this process running in the Resource Monitor. Using the TaskList.exe tool, you can view which processes can use Svchost.exe. Launch the tool by typing **tasklist /SVC** at the Command Prompt.
System	No	The majority of threads initiated by the kernel are run in the form of system processes.
Taskmgr.exe	Yes	This is the process that runs the Task Manager.
Winlogon.exe	No	This process is responsible for the management of user log-on and log-off.
Winmgmt.exe	No	Winmgmt.exe is a core component of client management subsystem.