

- 1. 4. 1. Using advanced system management tools -

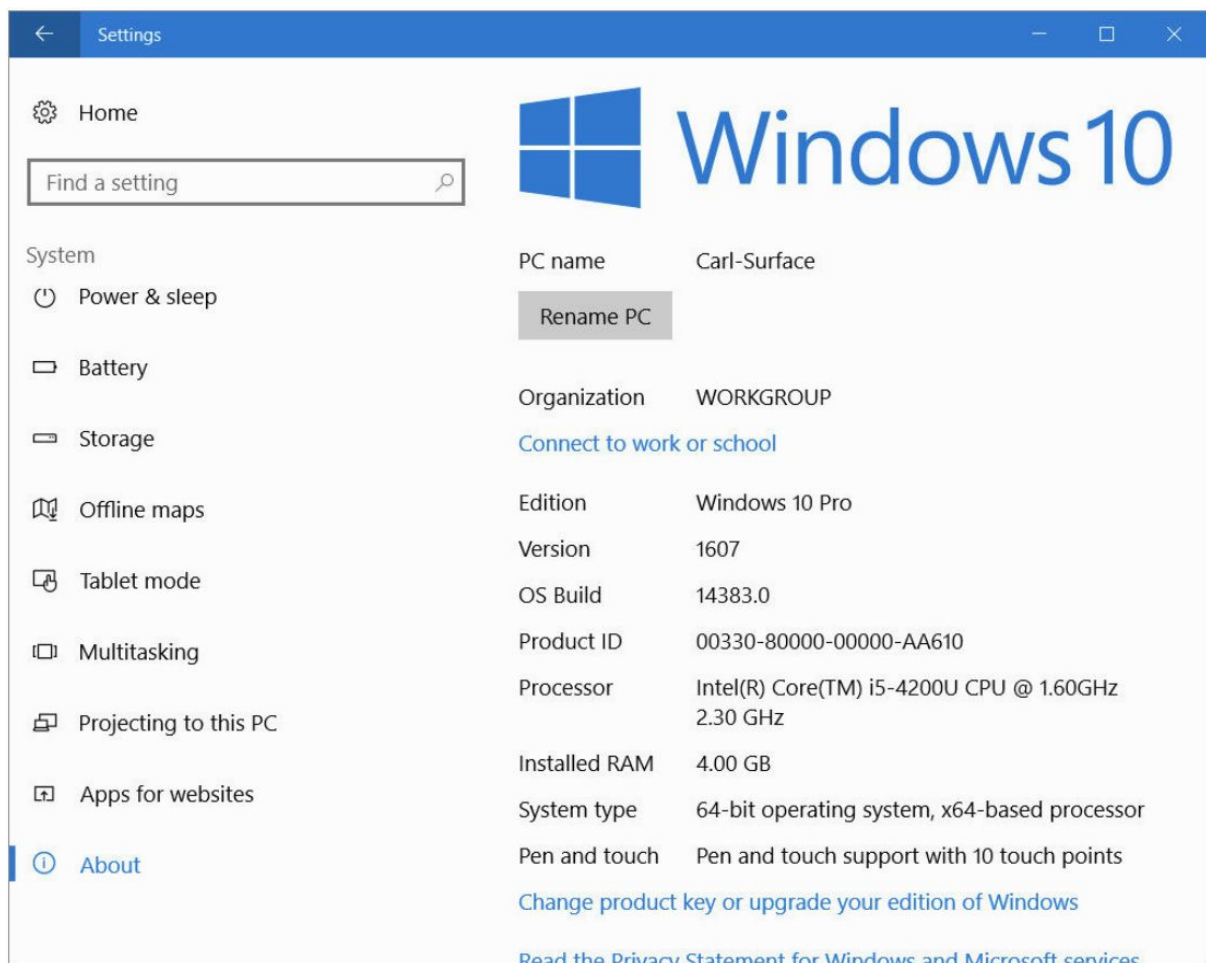
Viewing details about your system

For answers to basic questions about your operating system and computer, there's no better place to start than System, which displays the current Windows edition and whether it is a 32-bit or 64-bit version; basic system details, including processor type and installed memory; details about the computer name and network membership (domain or workgroup); and the current activation status.

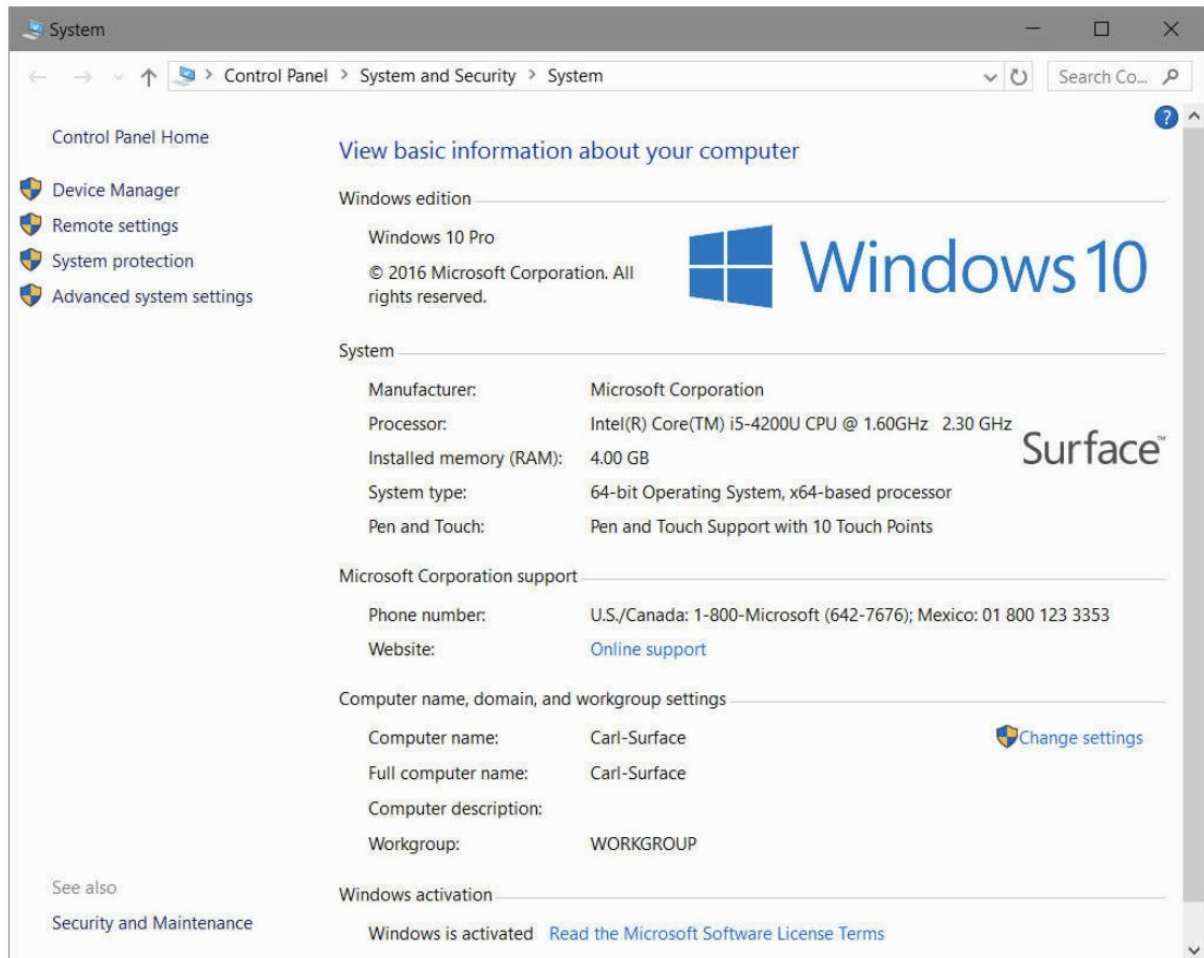
Windows 10 offers two versions of this information.

On a tablet or touchscreen-enabled system, you'll probably use the new Settings app.

Open Settings > System > About to display details like those shown in the following figure:



An alternative display that includes most of the same information is in the old-style Control Panel:



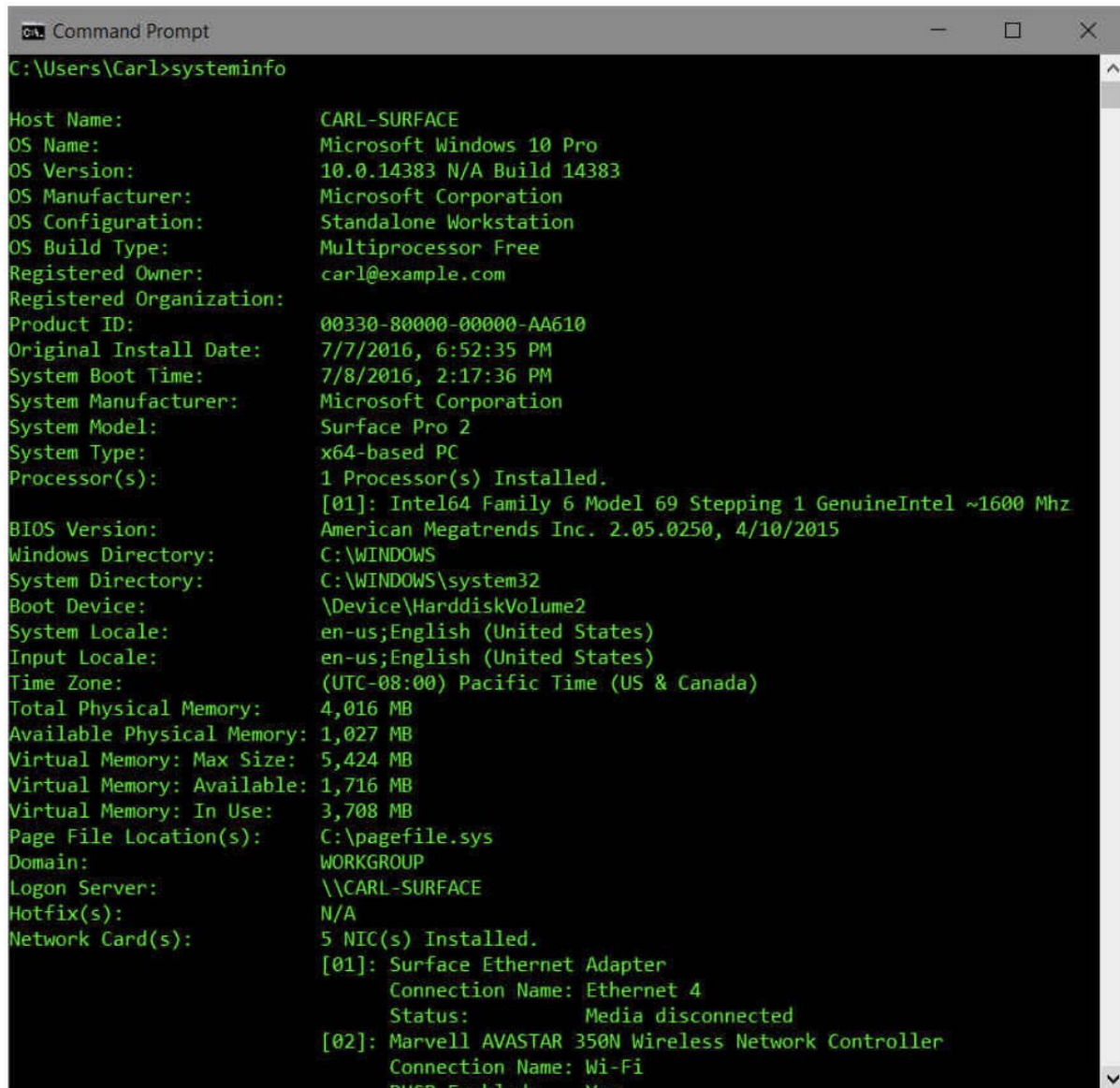
The simplest way to get to the System settings page in Control Panel is to right-click the Start button (or press Windows key+X) and then click System.

If File Explorer is open, right-click This PC and click Properties to reach the same destination.

For the most exhaustive inventory of system configuration details in a no-frills text format, Windows offers three tools that provide varying levels of technical information: Systeminfo, Windows Management Instrumentation, and System Information.

Systeminfo

Systeminfo.exe is a command-line utility, installed in the Windows\System32 folder, that displays information about your Windows version, BIOS, processor, memory, network configuration, and a few more esoteric items:



```
Command Prompt
C:\Users\Carl>systeminfo

Host Name:                 CARL-SURFACE
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.14383 N/A Build 14383
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         carl@example.com
Registered Organization:
Product ID:                00330-80000-00000-AA610
Original Install Date:     7/7/2016, 6:52:35 PM
System Boot Time:         7/8/2016, 2:17:36 PM
System Manufacturer:      Microsoft Corporation
System Model:              Surface Pro 2
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                          [01]: Intel64 Family 6 Model 69 Stepping 1 GenuineIntel ~1600 Mhz
BIOS Version:              American Megatrends Inc. 2.05.0250, 4/10/2015
Windows Directory:        C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,016 MB
Available Physical Memory: 1,027 MB
Virtual Memory: Max Size: 5,424 MB
Virtual Memory: Available: 1,716 MB
Virtual Memory: In Use:    3,708 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\CARL-SURFACE
Hotfix(s):                 N/A
Network Card(s):           5 NIC(s) Installed.
                          [01]: Surface Ethernet Adapter
                              Connection Name: Ethernet 4
                              Status:          Media disconnected
                          [02]: Marvell AVASTAR 350N Wireless Network Controller
                              Connection Name: Wi-Fi
                              DHCP Enabled:    Yes
```

To run Systeminfo, open a Command Prompt window, type "systeminfo", and then press Enter.

In addition to the list format shown in the previous image, Systeminfo offers two formats that are useful if you want to work with the information in another program: Table (fixed-width columns) and CSV (comma-separated values).

To use one of these formats, append the /FO switch to the command, along with the Table or Csv parameter.

You also need to redirect the output to a file.

For example, to store comma-delimited information in a file named Info.csv, enter the following command:

systeminfo /fo csv > info.csv

Using the /S switch, you can get system information about another computer on your network.

If your user name and password don't match that of an account on the target computer, you also need to use the /U and /P switches to provide the user name and password of an authorized account.

When you've gathered information about all the computers on your network, you can import the file you created into a spreadsheet or database program for tracking and analysis.

The following command appends information about a computer named Bates to the original file you created:

systeminfo /s Bates /fo csv >> info.csv

Windows Management Instrumentation command-line utility

This tool with the extra-long name is better known by the name of its executable, Wmic.exe, which is located in the Windows\System32\Wbem folder.

Wmic provides an overwhelming amount of information about hardware, system configuration details, and user accounts.

It can be used in either of two ways.

Enter wmic from a command prompt, and the utility runs in console mode, wherein you can enter commands and view output interactively.

Alternatively, you can add global switches or aliases, which constrain the type of output you're looking for, and see the output in a Command Prompt window or redirect it to a file.

For example, use the following command to produce a neatly formatted HTML file:

wmic qfe list brief /format:htable > %temp%\hotfix.html

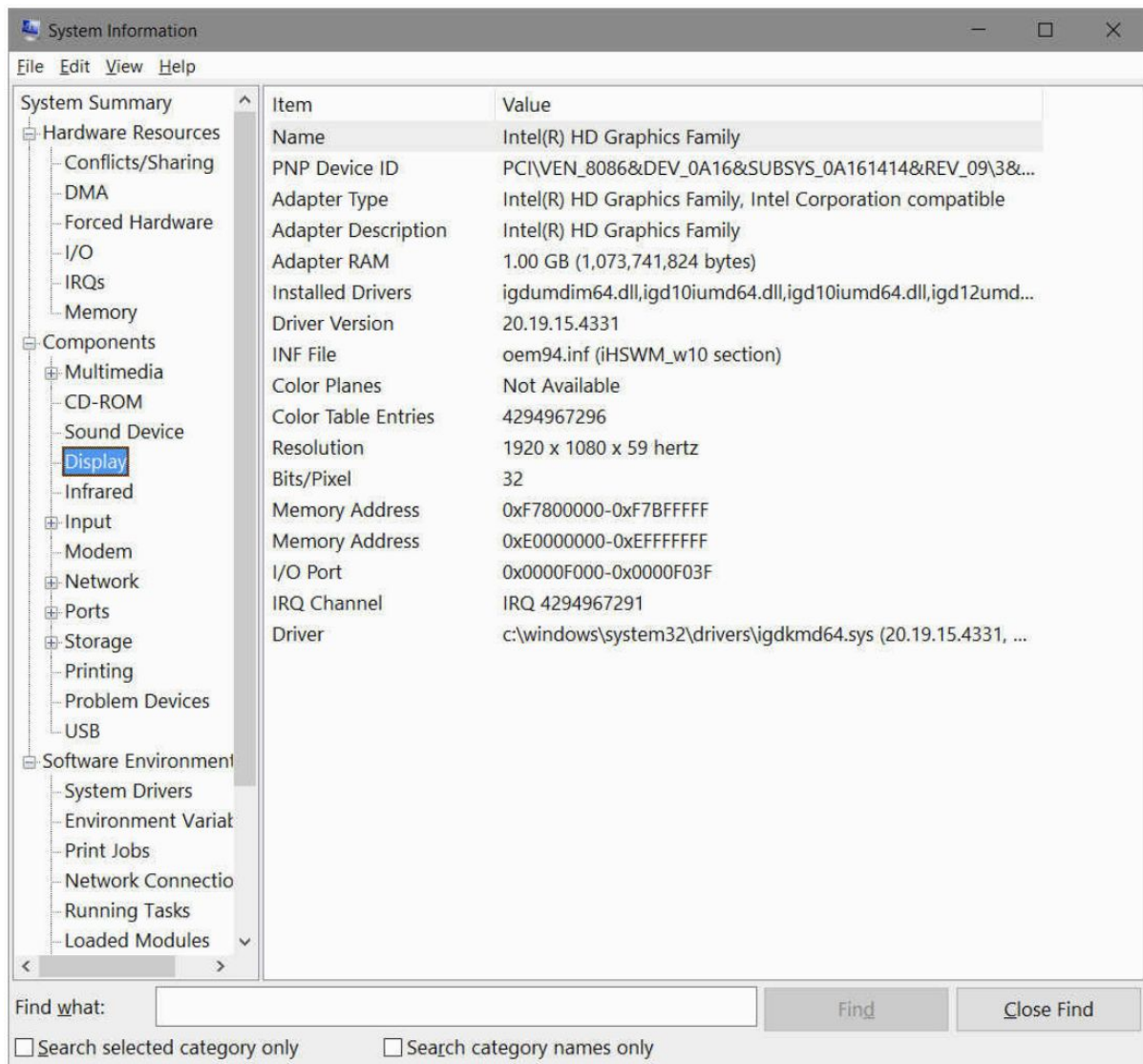
You can then open that file in a web browser to see a list of all installed updates on the current system.

To see the full syntax for Wmic, open a Command Prompt window and type wmic /? .

System Information

System Information—often called by the name of its executable, Msinfo32.exe—is a techie's paradise.

It displays a wealth of configuration information in a simple tree-and-details arrangement:



You can search for specific information, save information, view information about other computers, and even view a list of changes to your system.

To start System Information, begin typing system information in the search box or type msinfo32 at a command prompt.

You navigate through System Information much as you would through File Explorer: click a category in the left pane to view its contents in the right pane.

To search for specific information, use the Find What box at the bottom of the System Information window.

If the Find bar is not visible, press Ctrl+F, or click Edit and then clear the check box next to Hide Find.

The Find feature is basic but effective. Here are a couple of things you should know:

- Whenever you type in the Find What box to start a new search, Find begins its search at the top of the search range (which is the entire namespace unless you select Search Selected Category Only)—not at the current highlight.

- Selecting Search Category Names Only causes the Find feature to look only in the left pane. When this check box is cleared, the text in both panes is searched.

Using the System Information tool, you can preserve your configuration information—which is always helpful when reconstructing a system—in several ways:

- Save the information as an .nfo file. You can subsequently open the file (on the same computer or on a different computer with System Information) to view your saved information. To save information in this format, click File, Save. Saving this way always saves the entire collection of information.
- Save all or part of the information as a plain-text file. To save information as a text file, select the category of interest and click File, Export. To save all the information as a text file, select System Summary before you export it.
- You can print all or part of the information. Select the category of interest; click File, Print; and be sure that Selection is selected under Page Range. To print everything, select All under Page Range—and be sure to have lots of paper on hand. Depending on your system configuration and the number of installed applications, your report could top 100 pages. Even better, consider “printing” to PDF and saving the results.

Regardless of how you save your information, System Information refreshes (updates) the information immediately before processing the command.

Saving system configuration information when your computer is working properly can turn out to be useful when you have problems.

Comparing your computer’s current configuration with a known good baseline configuration can help you spot possible problem areas.

You can open multiple instances of System Information to display the current configuration in one window and a baseline configuration in another.

Save the configuration in OneDrive, and you’ll be able to retrieve the information even after a hard-disk replacement.

Managing services

A service is a specialized program that performs a function to support other programs.

Many services operate at a low level (by interacting directly with hardware, for example) and need to run even when no user is signed in.

For this reason, they’re often run by the System account (which has elevated privileges) rather than by ordinary user accounts.

For the most complete view of services running on your computer, use the Services console.

You can also view running services and perform limited management functions by using Task Manager.

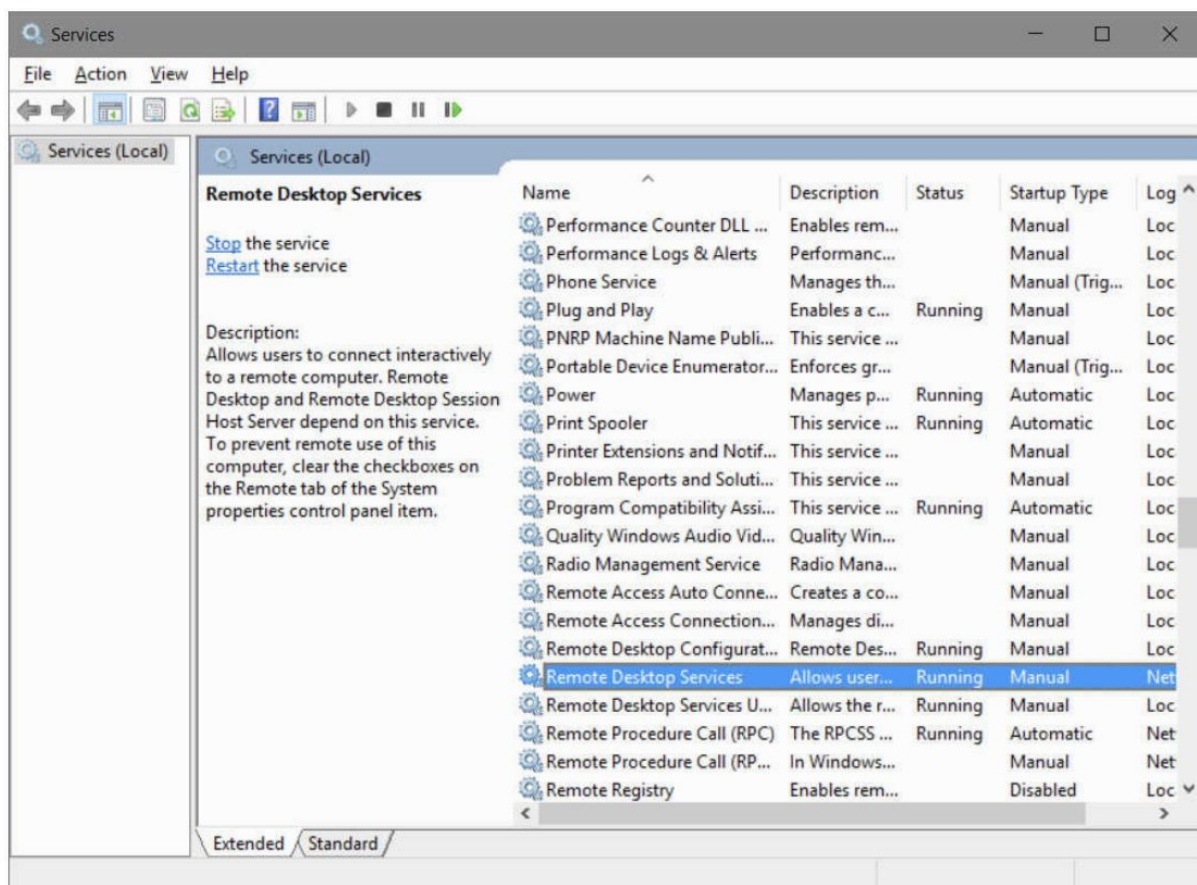
Using the Services console

You manage services with the Services snap-in (Services.msc) for Microsoft Management Console.

To view this snap-in, type "services" in the search box and then click the Services desktop app at the top of the results list.

You must have administrator privileges to gain full functionality in the Services console.

Running it as a standard user, you can view service settings, but you can't start or stop most services, change the startup type, or make any other configuration changes:



The Extended and Standard views in the Services console (selectable by clicking a tab near the bottom of the window) have a single difference: the Extended view provides

descriptive information of the selected service in the space at the left edge of the details pane.

This space also sometimes includes links for starting, stopping, or pausing the selected service.

Unless you need to constrain the console display to a small area of your screen, you'll probably find the Extended view preferable to the Standard view.

The Services console offers plenty of information in its clean display.

You can sort the contents of any column by clicking the column title, as you can with similar lists.

To sort in reverse order, click the column title again.

In addition, you can do the following:

- Start, stop, pause, resume, or restart the selected service, as described in the following section.
- Display the properties dialog box for the selected service, in which you can configure the service and learn more about it.

Most essential services are set to start automatically when your computer starts, and the operating system stops them as part of its shutdown process.

A handful of services that aren't typically used at startup are set with the Automatic (Delayed Start) option, which starts the associated service two minutes after the rest of startup completes, making the startup process smoother.

The Trigger Start option allows Windows to run or stop a service as needed in response to specific events; the File History service, for example, doesn't run unless you enable the File History feature.

But sometimes you might need to manually start or stop a service.

For example, you might want to start a seldom-used service on the rare occasion when you need it.

Because running services requires system resources such as memory, running them only when necessary can improve performance.

On the other hand, you might want to stop a service because you're no longer using it.

A more common reason for stopping a service is because it isn't working properly.

For example, if print jobs get stuck in the print queue, sometimes the best remedy is to stop and then restart the Print Spooler service.

If a service allows pausing, try pausing and then continuing the service as your first step instead of stopping the service.

Pausing can solve certain problems without canceling jobs in process or resetting connections.

Starting and stopping services

Not all services allow you to change their status.

Some prevent stopping and starting altogether, whereas others permit stopping and starting but not pausing and resuming.

Some services allow these permissions to only certain users or groups.

For example, most services allow only members of the Administrators group to start or stop them.

Which status changes are allowed and who has permission to make them are controlled by each service's discretionary access control list (DACL), which is established when the service is created on a computer.

To change a service's status, select it in the Services console.

Then click the appropriate link in the area to the left of the service list (if you're using the Extended view and the link you need appears there).

Alternatively, you can use the Play/Pause/Stop controls on the toolbar or right-click and use the corresponding command.

You can also change a service's status by opening its properties dialog box and then clicking one of the buttons on the General tab.

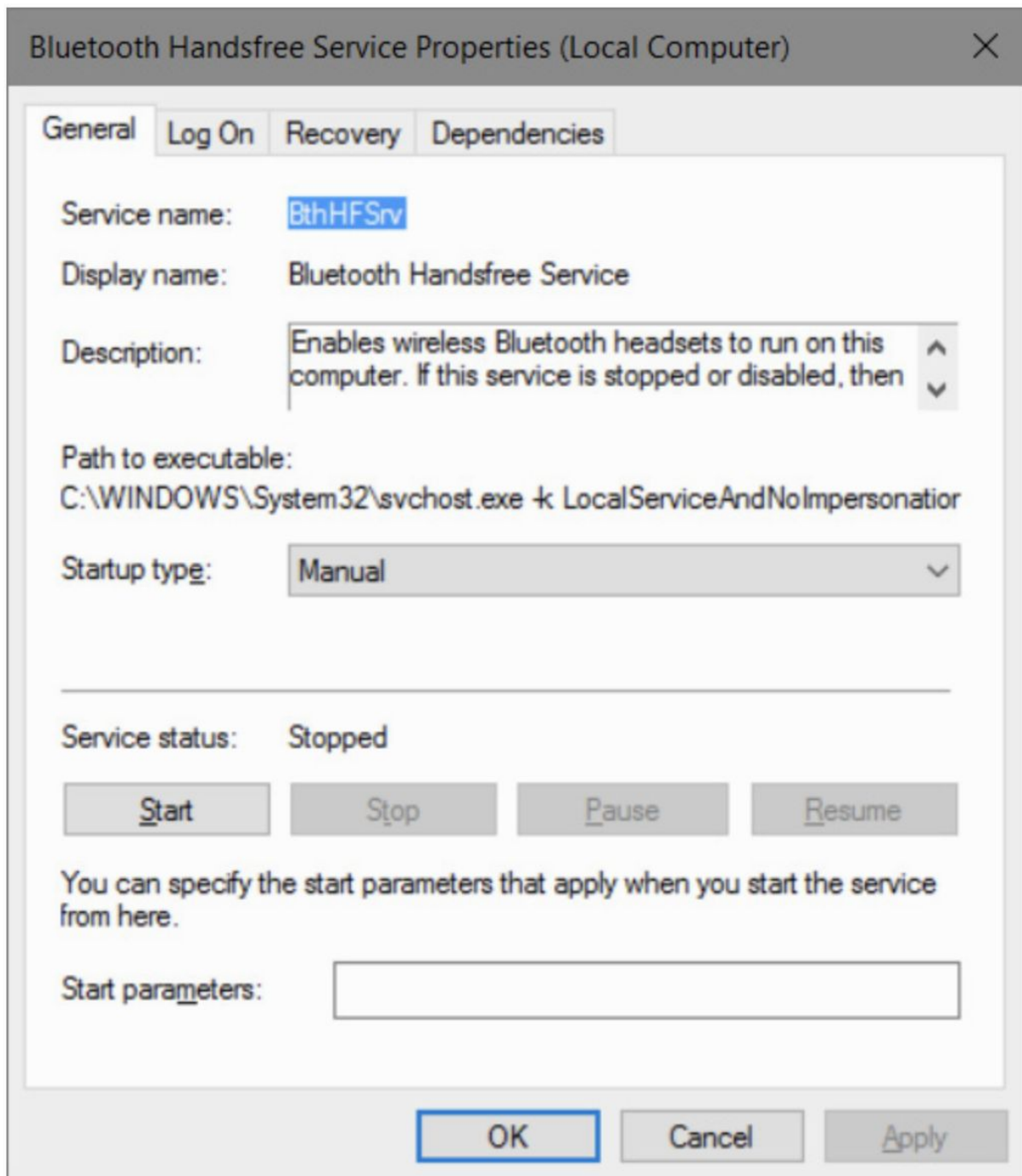
Taking the extra step of opening the properties dialog box to set the status has only one advantage: you can specify start parameters when you start a service by using this method.

This is a rare requirement.

Configuring services

To review or modify the way a service starts up or what happens when it doesn't start properly, view its properties dialog box.

To do that, double-click the service in the Services console:



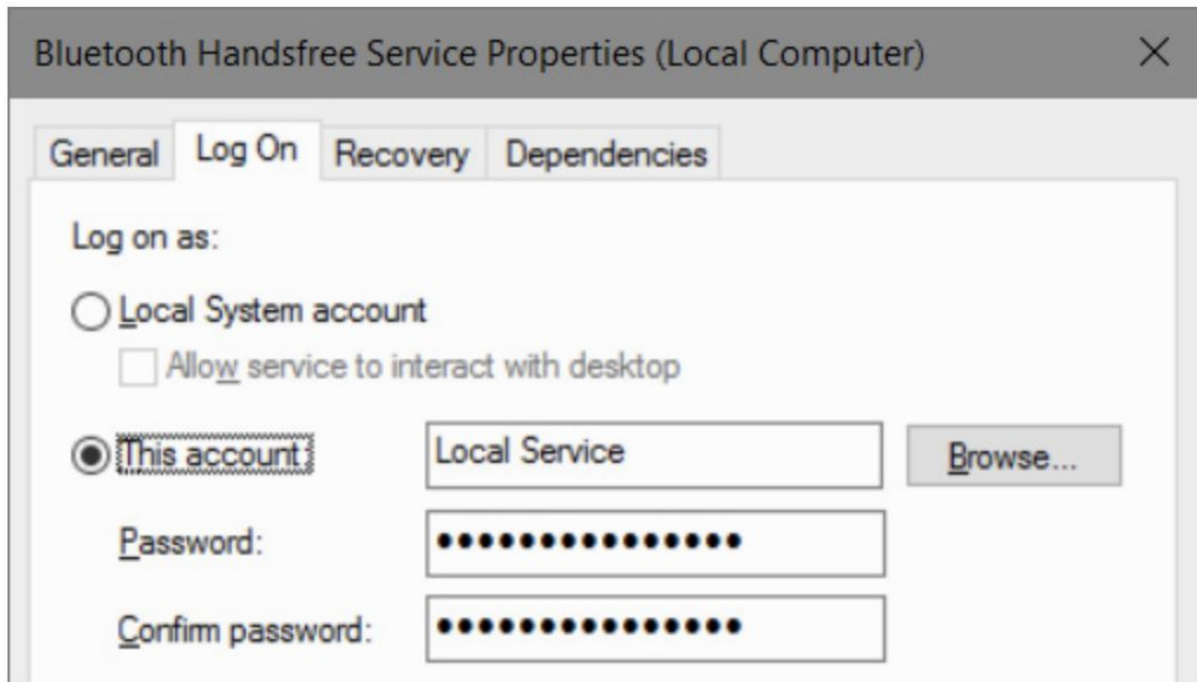
Setting startup options

On the General tab of the properties dialog box, you specify the startup type:

- Automatic (Delayed Start). The service starts shortly after the computer starts in order to improve startup performance and user experience.
- Automatic. The service starts when the computer starts.
- Manual. The service doesn't start automatically at startup, but it can be started by a user, program, or dependent service.

- Disabled. The service can't be started.

You'll find other startup options on the Log On tab of the properties dialog box:



Specifying recovery actions

For various reasons—hardware not operating properly or a network connection being down, for example—a service that's running smoothly might suddenly stop.

By using settings on the Recovery tab of the properties dialog box, you can specify what happens if a service fails.

The next picture, for example, shows the default settings for the Bluetooth Handsfree service:

The screenshot shows the 'Bluetooth Handsfree Service Properties (Local Computer)' dialog box with the 'Recovery' tab selected. The dialog has four tabs: 'General', 'Log On', 'Recovery', and 'Dependencies'. The 'Recovery' tab contains the following settings:

- Select the computer's response if this service fails.** (with a link to 'Help me set up recovery actions')
- First failure:** Restart the Service (dropdown menu)
- Second failure:** Restart the Service (dropdown menu)
- Subsequent failures:** Take No Action (dropdown menu)
- Reset fail count after:** 0 days (text input)
- Restart service after:** 2 minutes (text input)
- ☐ **Enable actions for stops with errors.** (with a button 'Restart Computer Options...')
- Run program** section:
 - Program:** (text input) with a 'Browse...' button
 - Command line parameters:** (text input)
 - ☐ **Append fail count to end of command line (/fail=%1%)**

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

You might want to perform a different action the first time a service fails than on the second or subsequent failures.

The Recovery tab enables you to assign a particular response to the first failure, the second failure, and all subsequent failures, from among these options:

- Take No Action. The service gives up trying. In most cases, the service places a message in the event log. Use of the event log depends on how the service was programmed by its developers.
- Restart The Service. The computer waits for the time specified in the Restart Service After box to elapse and then tries to start the service.

- **Run A Program.** The computer runs the program you specify in the Run Program box. For example, you could specify a program that attempts to resolve the problem or one that alerts you to the situation.
- **Restart The Computer.** Drastic but effective, this option restarts the computer after the time specified in the Restart Computer Options dialog box elapses. In that dialog box, you can also specify a message to be broadcast to other users on your network, warning them of the impending shutdown.

Viewing dependencies

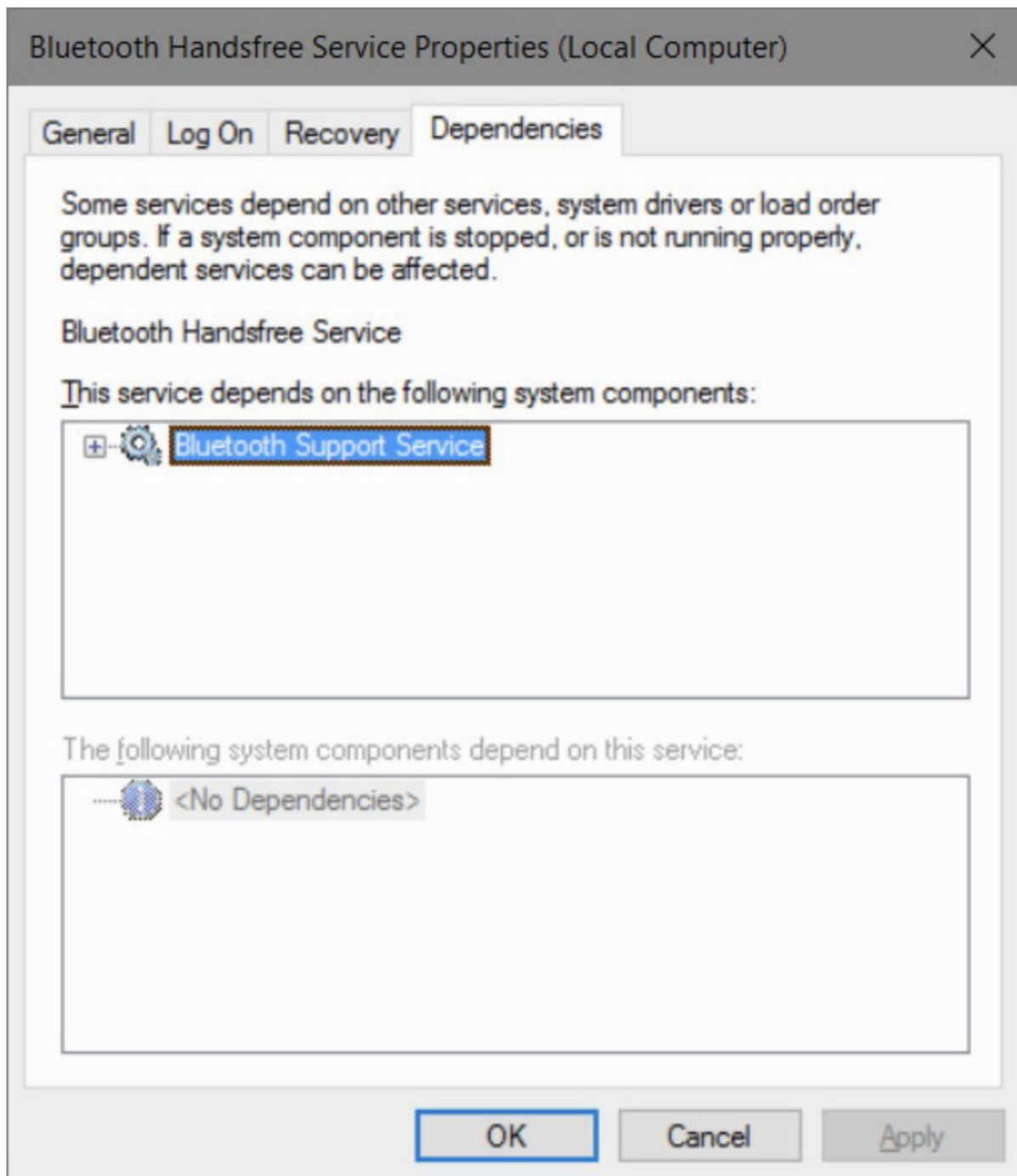
Many services rely on the functions of another service.

If you attempt to start a service that depends on other services, Windows first starts the others.

If you stop a service upon which others are dependent, Windows also stops those services.

Before you either start or stop a service, therefore, it's helpful to know what other services your action might affect.

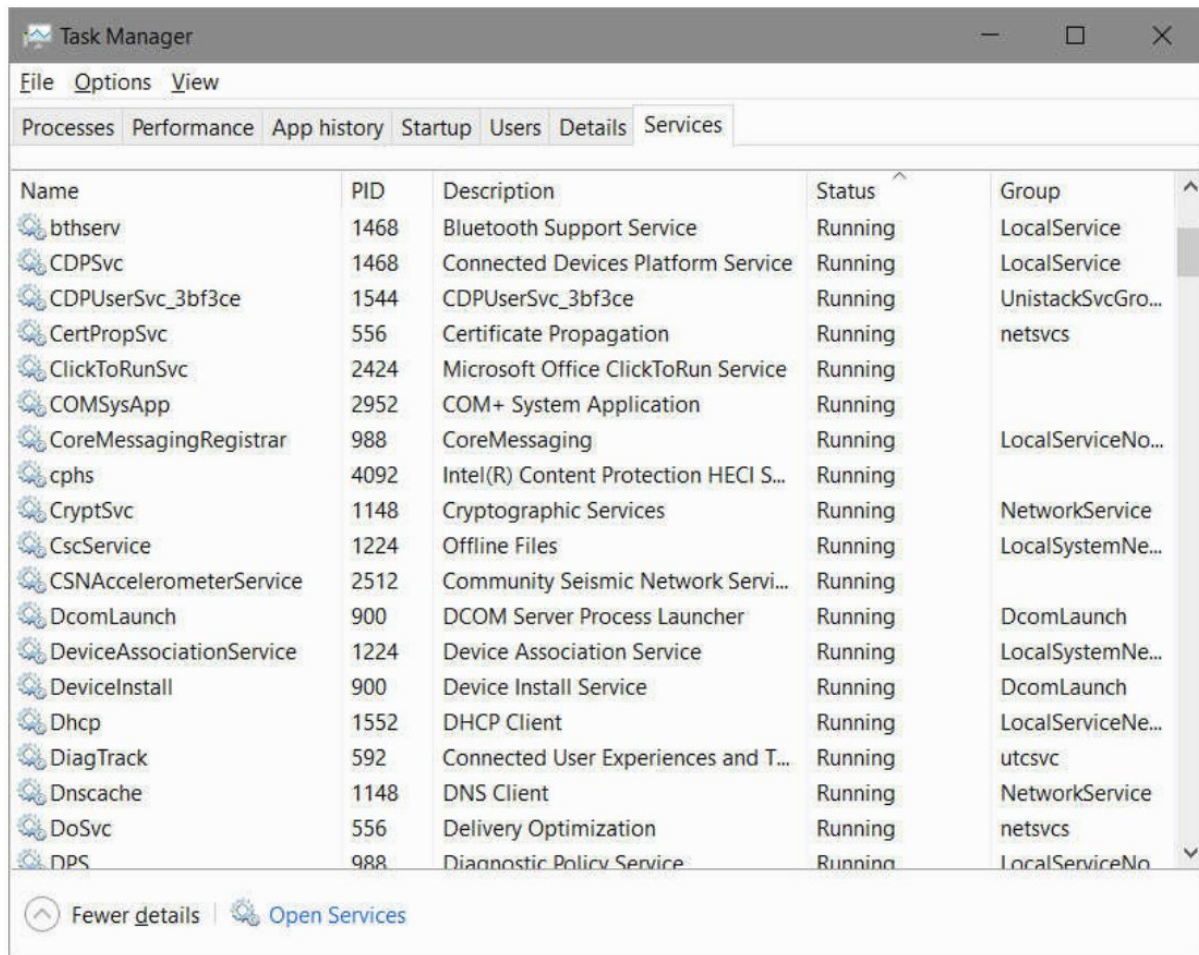
To obtain that information, go to the Dependencies tab of a service's properties dialog box:



Managing services from Task Manager

Using the Services tab in Windows Task Manager, you can start and stop services and view several important aspects of the services, both running and available, on your computer.

You can also use this tab as a shortcut to the Services console.



To start, stop, or restart a service, right-click its name on the Services tab and then click Start, Stop, or Restart.

Using the Services tab, you can also associate a running service with its process identifier (PID) and then further associate that PID with other programs and services being run under that PID.

For example, the previous picture shows a couple of services running with PID 1468.

Right-clicking one of the services with PID 1468 gives you two options: one to stop the service and one called Go To Details.

Clicking the latter option opens the Details tab in Task Manager with the particular process (typically, Svchost.exe) highlighted.

Editing the Windows registry

The Windows registry is the central storage location that contains configuration details for hardware, system settings, services, user customizations, applications, and every detail—large and small—that makes Windows work.

Although it's convenient to think of the registry as a monolithic database, its contents are actually stored in multiple locations as separate hive files, alongside logs and other support files.

Some of those hive files are read into memory when the operating system starts; hive files that contain user-specific settings are stored in the user profile and are loaded when a new user signs in.

You can't work with hive files directly.

Windows 10 is designed in such a way that direct registry edits by end users are generally unnecessary.

When you change your configuration by using the Settings app or Control Panel, for example, Windows writes the necessary updates to the registry for you.

Likewise, when you install a new piece of hardware or a new program, the setup program makes the required registry changes; you don't need to know the details.

On the other hand, because the designers of Windows couldn't provide a user interface for every conceivable customization you might want to make, sometimes working directly with the registry is the only way to make a change.

Even when it's not the only way, it might be the fastest way.

Removing or modifying registry entries is occasionally a crucial part of troubleshooting and repair as well.

Windows includes a registry editor you should know how to use—safely.

Caution!

An incorrect registry modification can render your system unbootable and in some cases might require a complete reinstall of the operating system.

Use Registry Editor at your own risk.

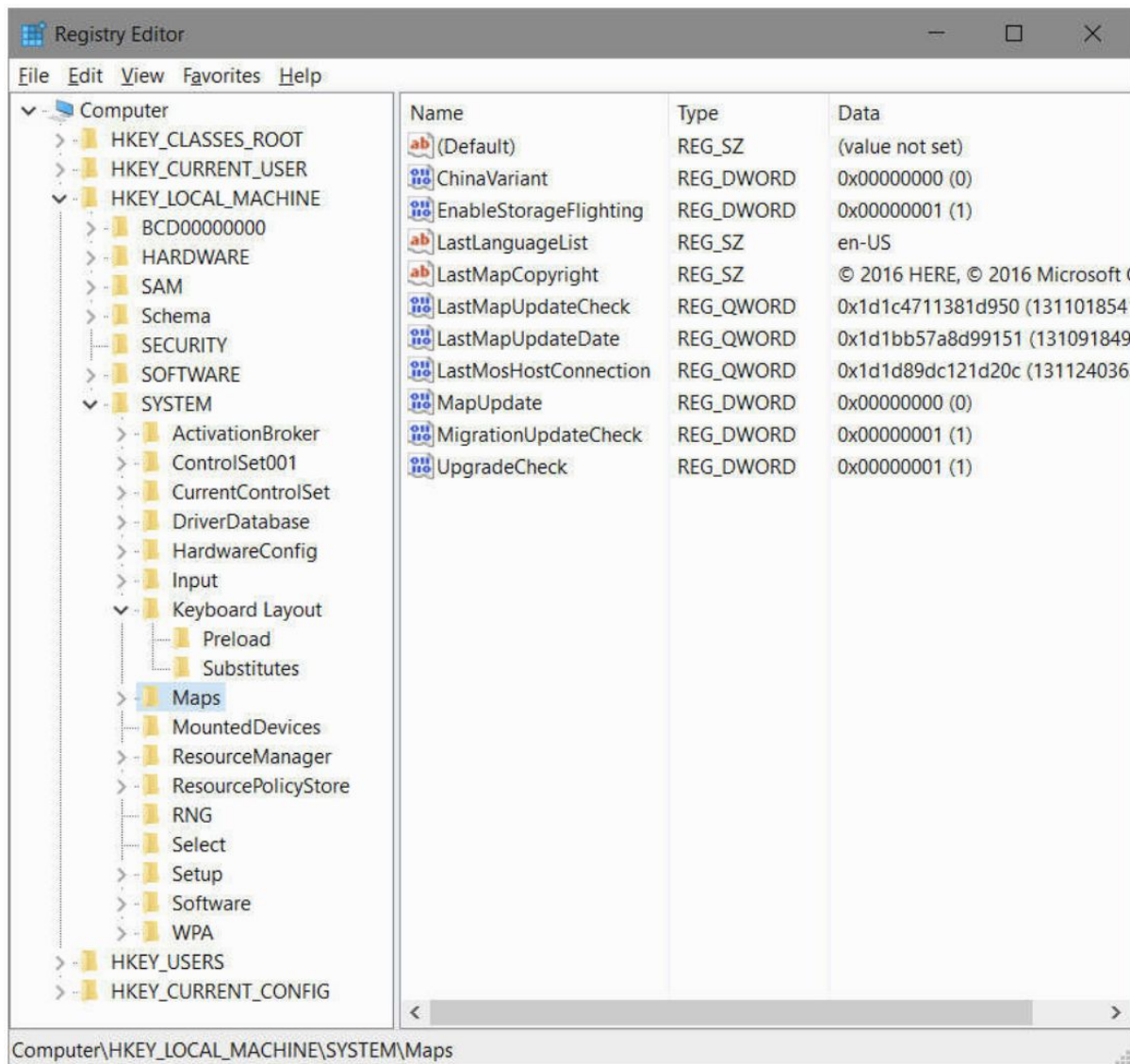
Understanding the Registry Editor hierarchy

Registry Editor (Regedit.exe) offers a unified view of the registry's contents as well as tools for modifying its contents.

You won't find this important utility on the All Apps list, however, and it doesn't show up when you type its name in the search box.

To start Registry Editor, you must use the name of its executable file, Regedit.exe, or type "regedit" at a command prompt.

The next figure shows a collapsed view of the Windows 10 registry, as seen through Registry Editor:



The Computer node appears at the top of the Registry Editor tree listing.

Beneath it, as shown here, are five root keys: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, and HKEY_CURRENT_CONFIG.

For simplicity's sake and typographical convenience, you can abbreviate the root key names as HKCR, HKCU, HKLM, HKU, and HKCC, respectively.

Root keys, sometimes called predefined keys, contain subkeys.

Registry Editor displays this structure in a hierarchical tree in the left pane.

In the previous figure, for example, HKLM is open, showing its top-level subkeys.

Subkeys, which we call keys for short, can contain subkeys of their own, which can be expanded as necessary to display additional subkeys.

The status bar at the bottom of the Registry Editor window shows the full path of the currently selected key: HKLM\System\Maps, in the previous figure.

The contents of HKEY_LOCAL_MACHINE define the workings of Windows itself, and its subkeys map neatly to several hives we mentioned at the start of this section.

HKEY_USERS contains an entry for every existing user account (including system accounts), each of which uses the security identifier, or SID, for that account.

The remaining three predefined keys don't exist, technically.

Like the file system in Windows—which uses junctions, symlinks, and other trickery to display a virtual namespace—the registry uses a bit of misdirection (implemented with the REG_LINK data type) to create these convenient representations of keys that are actually stored within HKEY_LOCAL_MACHINE and HKEY_USERS:

- HKEY_CLASSES_ROOT is merged from keys within HKLM\Software\Classes and HKEY_USERS\sid\Classes (where sid is the security identifier of the currently signed-in user).
- HKEY_CURRENT_USER is a view into the settings for the currently signed-in user account, as stored in HKEY_USERS\sid (where sid is the security identifier of the currently signed-in user).
- HKEY_CURRENT_CONFIG displays the contents of the Hardware Profiles\Current subkey in HKLM\SYSTEM\CurrentControlSet\Hardware Profiles.

Any changes you make to keys and values in these virtual keys have the same effect as though you had edited the actual locations.

The HKCR and HKCU keys are generally more convenient to use.

Registry values and data types

Every key contains at least one value.

In Registry Editor, that obligatory value is known as the default value.

Many keys have additional values.

The names, data types, and data associated with values appear in the right pane.

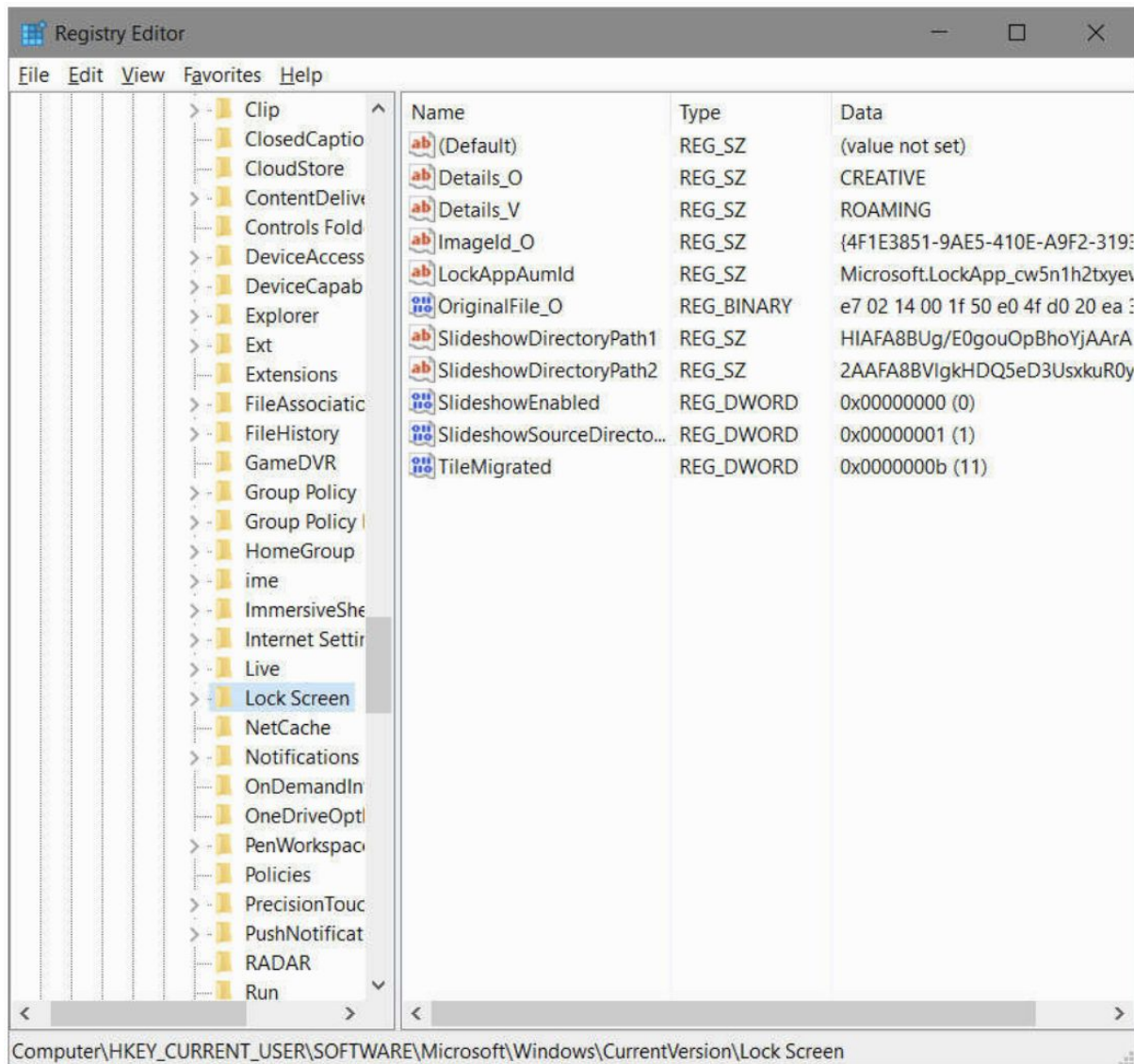
The default value for many keys is not defined.

You can think of an empty default value as a placeholder—a slot that could hold data but currently does not.

All values other than the default always include the following three components: name, data type, and data.

The next image, for example, shows customized settings for the current user's lock screen.

Note the full path to this key in the bottom of the Registry Editor window.



The SlideshowEnabled value (near the bottom of the list) is of data type REG_DWORD.

The data associated with this value (on the system used for this figure) is 0x00000000. The prefix 0x denotes a hexadecimal value. Registry Editor displays the decimal equivalent of hexadecimal values in parentheses after the value.

The registry uses the following data types:

- REG_SZ The SZ indicates a zero-terminated string. This variable-length string can contain Unicode as well as ANSI characters. When you enter or edit a REG_SZ value, Registry Editor terminates the value with a 00 byte for you.
- REG_BINARY The REG_BINARY type contains binary data—0s and 1s.

- REG_DWORD This data type is a “double word”—that is, a 32-bit numeric value. Although it can hold any integer from 0 to 232, the registry often uses it for simple Boolean values (0 or 1) because the registry lacks a Boolean data type.
- REG_QWORD This data type is a “quadruple word”—a 64-bit numeric value.
- REG_MULTI_SZ This data type contains a group of zero-terminated strings assigned to a single value.
- REG_EXPAND_SZ This data type is a zero-terminated string containing an unexpanded reference to an environment variable, such as %SystemRoot%.

Backing up and restoring parts of the registry

The two most important things to know about Registry Editor are that it copies your changes immediately into the registry and that it has no Undo command.

Registry Editor doesn't wait for you to issue a File, Save command (because it has no such command) before making changes in the registry files.

And after you alter some bit of registry data, the original data is gone forever—unless you remember it and restore it yourself or unless you have some form of backup you can restore.

Registry Editor, therefore, is a tool to be used sparingly and cautiously; it should not be left open when not in use.

Before you make any changes to the registry, consider using System Restore to set a restore point, which includes a snapshot of the registry as it currently exists.

Taking this precaution allows you to roll back any ill-advised changes.

In addition, you can use the Export command in Registry Editor to back up the branch of the registry where you plan to work.

Registry Editor can save all or portions of your registry in any of the four different formats described here:

- Registration Files. The Registration Files option creates a .reg file, which is a text file that can be read and edited in Notepad or a similar program. A .reg file can be merged into the registry of a system running any version of Windows. When you merge a .reg file, its keys and values replace the corresponding keys and values in the registry. By using .reg files, you can edit your registry “offline” and add your changes to the registry without even opening Registry Editor. You can also use .reg files as an easy way to share registry settings and copy them to other computers.
- Registry Hive Files. The Registry Hive File format saves a binary image of a selected portion of the registry. You won't be able to read the resulting file (although you can choose one of the text-file options if that's what you need to do), but if you need to restore the keys you worked on, you can be confident

that this format will do the job correctly. Registry Hive File is the format of choice if you want to create a backup before working in Registry Editor. That's because when you import a registry hive file, it restores the entire hive to exactly the way it was when you saved it. (The .reg file types, when merged, restore all the saved keys and values to their original locations, which repairs all deletions and edits. But the process does not remove any keys or values you added.) Note, however, that a registry hive file has the potential to do the greatest damage if you import it to the wrong key; see the caution in the following section.

- Win9x/NT4 Registration Files. The Win9x/NT4 Registration Files option also generates a .reg file, but one in an older format used by earlier versions of Windows. The principal difference between the two formats is that the current format uses Unicode and the older format does not. We can't think of a real-world scenario in which you would actually want to use this legacy format.
- Text Files. The Text Files option, like the Registration Files option, creates a file that can be read in Notepad or another text editor. The principal advantage of this format is that it cannot accidentally (or intentionally) be merged into the registry. Thus, using this option is a good way to create a record of your registry's state at a particular time. Its disadvantage, relative to the .reg file format, is the size of the files it creates. Text files are considerably larger than corresponding .reg files, and they take longer to create.

To export all or part of a registry hive, select a key in the left pane, and then on the File menu, click Export.

Easier yet: Right-click a key and click Export.

In the Save As Type list in the Export Registry File dialog box, select one of the four file types.

Under Export Range, select Selected Branch.

The resulting file includes the selected key and all its subkeys and values.

If you need to restore the exported hive from a registry hive file, select the same key in the left pane of the Registry Editor window, click Import on the File menu, and specify the file.

You'll see a confirmation prompt letting you know that your action will overwrite (replace) the current key and all its subkeys.

This is your last chance to make sure you're importing the hive into the right location, so take a moment to make sure you selected the correct key before you click Yes.

If you saved your backup as a .reg file, you use the same process to import it.

As an alternative, you can double-click the .reg file in File Explorer without opening Registry Editor.

Unlike with a registry hive file, however, the complete path to each key and value is stored as part of the file and it always restores to the same location.

This approach for recovering from registry editing mishaps is fine if you did not add new values or subkeys to the section of the registry you're working with; it returns existing data to its former state but doesn't alter the data you added.

Caution!

Importing a registry hive file replaces the entire contents of the selected key with the contents of the file—regardless of its original source.

That is, it wipes out everything in the selected key and then adds the keys and values from the file.

When you import, be absolutely certain you selected the correct key.

You used a registry cleaner and your system is no longer working properly

The registry is often inscrutable and can appear messy.

Misguided attempts at cleanup can cause unexpected problems that are nearly impossible to troubleshoot, which explains why Microsoft is so insistent with its warnings that improper changes to the registry can prevent your computer from operating properly or even booting.

We've never found a so-called registry cleaner that justifies the risk it inevitably entails.

If you find yourself with a misbehaving system after using a registry cleaner, use the Reset option to recover your system and start over.

And this time, don't bother to install that unnecessary utility.

Browsing and editing with Registry Editor

Because of the registry's size, looking for a particular key, value, or data item can be daunting.

In Registry Editor, the Find command (on the Edit menu and also available by pressing Ctrl+F) works in the forward direction only and does not wrap around when it gets to the end of the registry.

If you're not sure where the item you need is located, select the highest level in the left pane before issuing the command.

If you have an approximate idea where the item you want is located, you can save time by starting at a node closer to (but still above) the target.

After you locate an item of interest, you can put it on the Favorites list to simplify a return visit.

Open the Favorites menu, click Add To Favorites, and supply a friendly name (or accept the default).

If you're about to close Registry Editor and know you'll be returning to the same key the next time you open the editor, you can skip the Favorites step because Registry Editor always remembers your last position and returns to that position in the next session.

Registry Editor includes a number of time-saving keyboard shortcuts for navigating the registry:

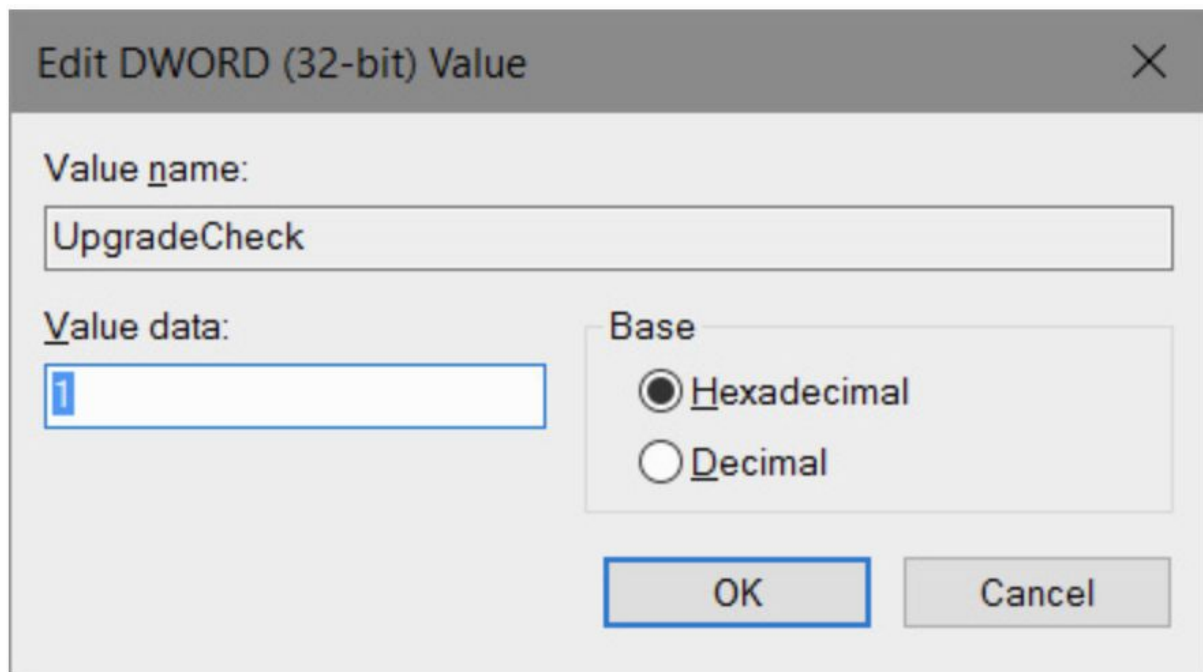
- To move to the next subkey that starts with a particular letter, simply type that letter when the focus is in the left pane; in the right pane, use the same trick to jump to the next value that begins with that letter.
- To open a key (revealing its subkeys), press the Right Arrow key.
- To move up one level in the subkey hierarchy, press the Left Arrow key; a second press collapses the subkeys of the current key.
- To move to the top of the hierarchy, press Home.
- To quickly move between the left and right panes, use the Tab key.
- In the right pane, press F2 to rename a value, and press Enter to open that value and edit its data.

Once you are comfortable using these keyboard shortcuts, you'll find it's usually easier to zip through the subkey hierarchy with a combination of arrow keys and letter keys than it is to open outline controls with the mouse.

Changing data

You can change the data associated with a value by selecting a value in the right pane and pressing Enter or by double-clicking the value.

Registry Editor pops up an edit window appropriate for the value's data type:



Adding or deleting keys

To add a key, select the new key's parent in the left pane, open the Edit menu, point to New, and click Key.

The new key arrives as a generically named outline entry, exactly the way a new folder does in File Explorer.

Type a new name.

To delete a key, select it and then press Delete.

Adding or deleting values

To add a value, select the parent key, open the Edit menu, and point to New.

On the submenu that appears, click the type of value you want to add. A value of the type you select appears in the right pane with a generic name.

Type over the generic name, press Enter twice, enter your data, and press Enter once more.

To delete a value, select it and press Delete.

Using the Reg command

One expert-level option is to use the Reg command in a Command Prompt window or in a batch file or script.

Type `reg /?` to see the full list of eligible arguments for the reg command (query, add, export, import, and so on).

Each of those variants has its own syntax help.

Try "**reg add /?**" to see the correct syntax for adding a value.

Using .reg files to automate registry changes

The .reg files created by the Export command in Registry Editor are plain text, suitable for reading and editing in Notepad or any similar editor.

Therefore, they provide an alternative method for editing your registry.

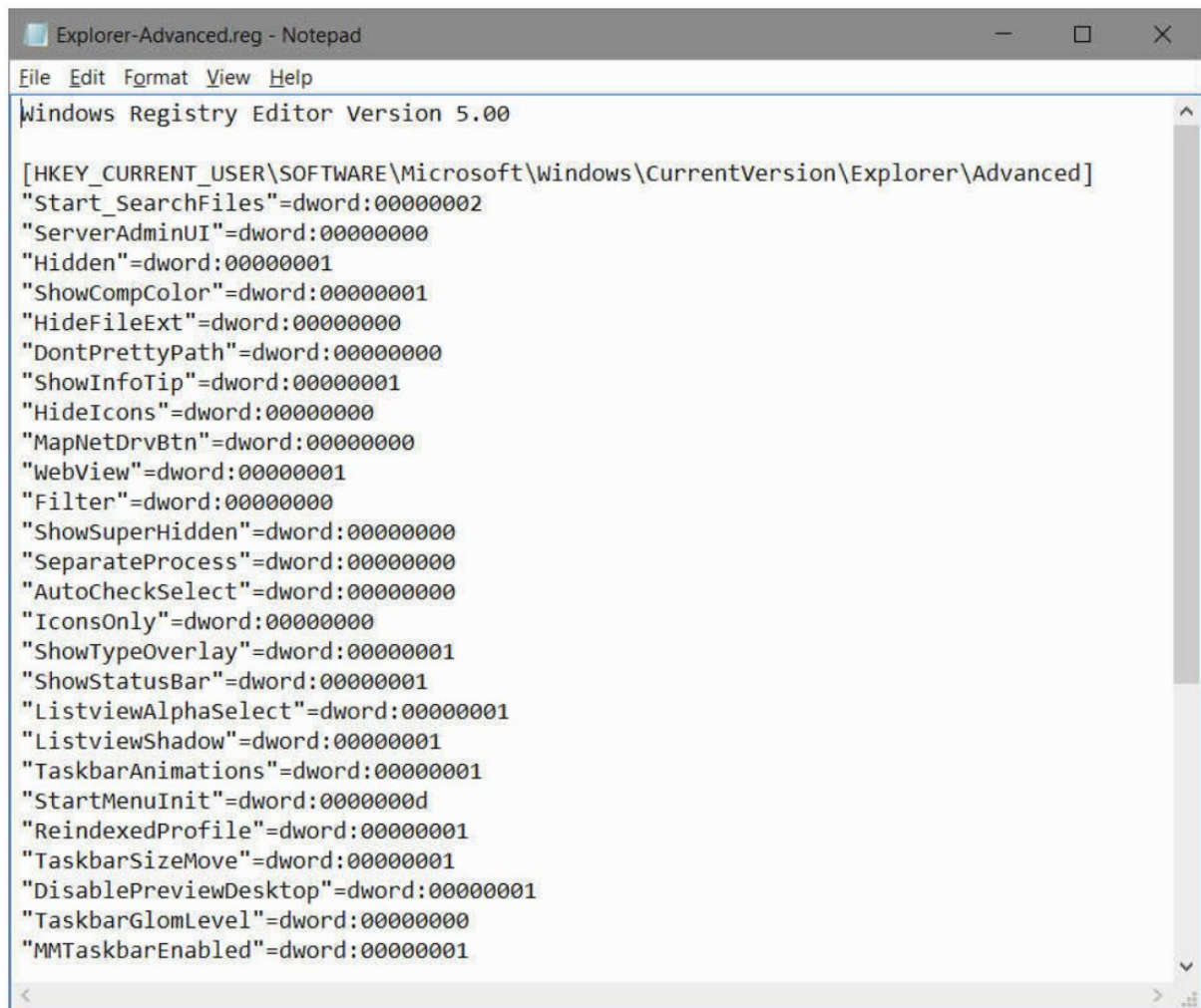
You can export a section of the registry, change it offline, and then merge it back into the registry.

Or you can add new keys, values, and data to the registry by creating a .reg file from scratch and merging it.

A .reg file is particularly useful if you need to make the same changes to the registry of several computers.

You can make and test your changes on one machine, save the relevant part of the registry as a .reg file, and then transport the file to the other machines that require it.

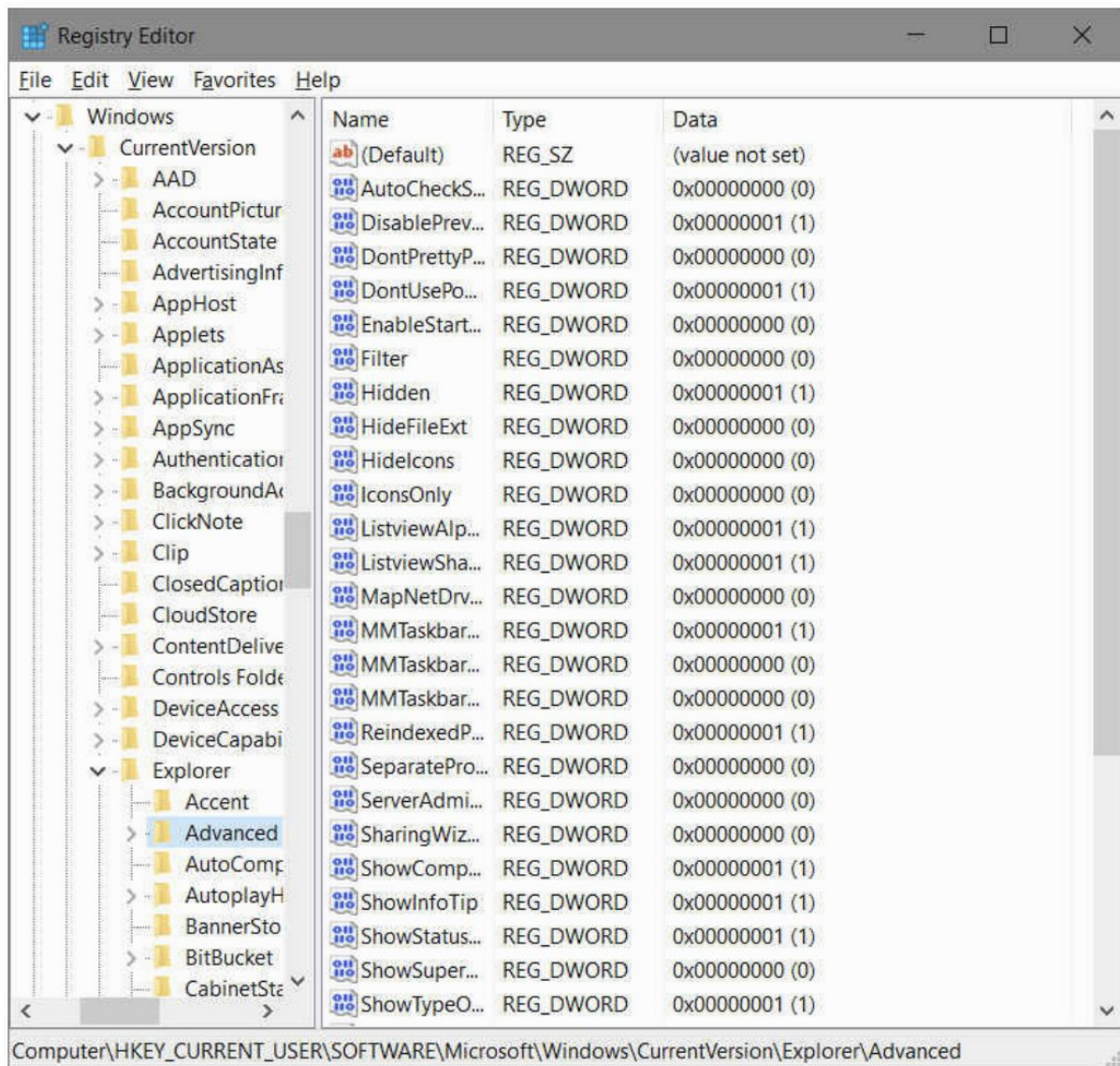
The next image shows a .reg file:



```
Explorer-Advanced.reg - Notepad
File Edit Format View Help
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"Start_SearchFiles"=dword:00000002
"ServerAdminUI"=dword:00000000
"Hidden"=dword:00000001
"ShowCompColor"=dword:00000001
"HideFileExt"=dword:00000000
"DontPrettyPath"=dword:00000000
"ShowInfoTip"=dword:00000001
"HideIcons"=dword:00000000
"MapNetDrvBtn"=dword:00000000
"WebView"=dword:00000001
"Filter"=dword:00000000
"ShowSuperHidden"=dword:00000000
"SeparateProcess"=dword:00000000
"AutoCheckSelect"=dword:00000000
"IconsOnly"=dword:00000000
"ShowTypeOverlay"=dword:00000001
"ShowStatusBar"=dword:00000001
"ListViewAlphaSelect"=dword:00000001
"ListViewShadow"=dword:00000001
"TaskbarAnimations"=dword:00000001
"StartMenuInit"=dword:0000000d
"ReindexedProfile"=dword:00000001
"TaskbarSizeMove"=dword:00000001
"DisablePreviewDesktop"=dword:00000001
"TaskbarGlomLevel"=dword:00000000
"MMTaskbarEnabled"=dword:00000001
```

In this case, the file was exported from the
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced key, shown in
the next figure:



Using Microsoft Management Console

Microsoft Management Console (MMC) is an application that hosts tools for administering computers, networks, and other system components.

By itself, MMC performs no administrative services.

Rather, it acts as the host for one or more modules, called snap-ins, which do the useful work.

MMC provides user-interface consistency so that you or the users you support see more or less the same style of application each time you need to carry out some kind of computer management task.

A combination of one or more snap-ins can be saved in a file called a Microsoft Common Console Document or, more commonly, an MMC console.

Creating snap-ins requires expertise in programming.

You don't have to be a programmer, however, to make your own custom MMC consoles.

All you need to do is run MMC, start with a blank console, and add one or more of the snap-ins available on your system.

Alternatively, you can customize some of the MMC consoles supplied by Microsoft or other vendors simply by adding or removing snap-ins.

You might, for example, want to combine the Services console with the Event Viewer console, the latter filtered to show only events generated by services.

You might also want to include a link to a website that offers details about services and service-related errors.

Or perhaps you would like to simplify some of the existing consoles by removing snap-ins you seldom use.

MMC consoles use, by default, the file-name extension .msc, and .msc files are associated by default with MMC.

Thus, you can run any MMC console by double-clicking its file name in a File Explorer window or by entering the file name at a command prompt.

Windows 10 includes several predefined consoles; the most commonly used ones, described in the following table, can be easily found by typing their name in the search box:

Console name (file name)	Description
Computer Management (Compmgmt.msc)	Includes the functionality of the Task Scheduler, Event Viewer, Shared Folders, Local Users And Groups, Performance Monitor, Device Manager, Disk Management, Services, and WMI Control snap-ins, providing control over a wide range of computer tasks.
Certificate Manager (Certmgr.msc)	Uses the Certificates snap-in to view and manage security certificates for the current user. A similar console, Certlm.msc, manages certificates on the local machine.
Device Manager (Devmgmt.msc)	Uses the Device Manager snap-in to enable administration of all attached hardware devices and their drivers. See Chapter 13, "Hardware," for more information on configuring hardware.
Disk Management (Diskmgmt.msc)	Uses the Disk Management snap-in for configuring disk volumes and partitions. For details, see Chapter 14.
Event Viewer (Eventvwr.msc)	Uses the Event Viewer snap-in to display all types of logged information. See "Event Viewer" in Chapter 17 for details.
Hyper-V Manager (Virtmgmt.msc)	Uses the Hyper-V Manager snap-in to provide an environment for creating, modifying, and running virtual machines. See Chapter 22, "Running virtual machines with Hyper-V," for details.
Local Users and Groups (Lusrmgr.msc)	Uses the Local Users and Groups snap-in to manage local user accounts and security groups. For more information, see "User accounts and security groups" in Chapter 6.
Performance Monitor (Perfmon.msc)	Uses the Performance Monitor snap-in to provide a set of monitoring tools. See Chapter 15, "System maintenance and performance," for details.
Print Management (Printmanagement.msc)	Uses the Print Management snap-in for managing printers and print jobs.
Services (Services.msc)	Uses the Services snap-in to manage services in Windows. For details, see "Managing startup programs and services" in Chapter 15 and "Managing services," earlier in this chapter.
Task Scheduler (Taskschd.msc)	Uses the Task Scheduler snap-in for managing tasks that run automatically. For details, see "Using Task Scheduler" in Chapter 19.
Trusted Platform Module (TPM) Management (Tpm.msc)	Displays information about and enables configuration of a computer's TPM chip.
Windows Firewall With Advanced Security (Wf.msc)	Uses the Windows Firewall With Advanced Security snap-in to configure rules and make other firewall settings. For details, see "Advanced tools for managing Windows Firewall" in Chapter 7.

- Vocabulary -

- hive: colmena.
- hive (registry): a hive is a logical group of keys, subkeys, and values in the Windows registry.

- Exercises - 1. 4. Windows 10 for experts and IT pros -

You are going to create a new Google Document inside the "1. Windows Client" folder of your Google Drive, named:

"1. 4. Windows 10 for experts and IT pros - Apellidos, Nombre"

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

Share this Google Document with the teacher (jorge@iesdoctorbalmis.com) with "Edit" permissions.

Inside this Google Document you are going to answer to the exercises of the following sub-units:

- 1. 4. 1. Using advanced system management tools
- 1. 4. 2. Automating tasks and activities
- 1. 4. 3. Advanced networking
- 1. 4. 4. Managing Windows 10 in business
- 1. 4. 5. Running virtual machines with Hyper-V

- Exercises - 1. 4. 1. Using advanced system management tools -

Open the following Google Document that you have just created:

"1. 4. Windows 10 for experts and IT pros - 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:

1. Open Settings -> System -> About in order to display your system details, like PC name, Organisation, Windows Edition, Version, Processor, Installed RAM, System type...
2. Open a Command Prompt window and type "systeminfo". In that Command Prompt, type "systeminfo /fo csv > info.csv", and then open the "info.csv" file

with a SpreadSheet program (LibreOffice Calc, Microsoft Excel, Google Drive Sheets).

3. Open a Command Prompt window, type "wmic qfe list brief /format:htable > hotfix.html" and then open the "hotfix.html" file with a web browser to see which Windows Updates your computer has installed.
4. Type "system information" in the Windows search box in order to open the System Information desktop program. Navigate through System Information clicking a category in the left pane to view its contents in the right pane. Save the System Information as an .nfo file.
5. Type "services" in the Windows search box in order to open the Services desktop program. Click on the "Extended" tab below. Look for the "File History Service" and Stop it. Then, Start it again. Open the Properties of the "File History Service" and check the different tabs: General, Log On, Recovery and Dependencies.
6. Open a Command Prompt window and type "regedit". Check the different keys of the Windows Registry.
7. Do a backup of your Windows Registry exporting it in .reg and Registry Hive Files.
8. Disable the Action Center using the Registry. Navigate to the HKEY_CURRENT_USER \ SOFTWARE \ Policies \ Microsoft \ Windows \ Explorer registry key. If you don't have an "Explorer" key, then you'll have to create one manually: right click on the "Windows" key -> "New" -> "Key". Name that new key "Explorer" . Then right-click on the "Explorer" key, select New -> DWORD (32-bit), and name the new DWORD as DisableNotificationCenter. Right-click the DisableNotificationCenter value, select Modify, and enter "1" as its value. Restart your PC and the Action Center should no longer bother you. Do note, however, that this also disables notifications in general, so you'll need to factor that into whether or not you go through with this tweak. If you want to go back and see the Action Center, just enter "0" as the value of the previous entry of the registry.
9. Use the Windows search box in order to open some of the MMCs (Microsoft Management Consoles): Compmgmt.msc, Devmgmt.msc, Diskmgmt.msc, Eventvwr.msc, Lusrmgr.msc, Printmanagement.msc, Services.msc, etc.