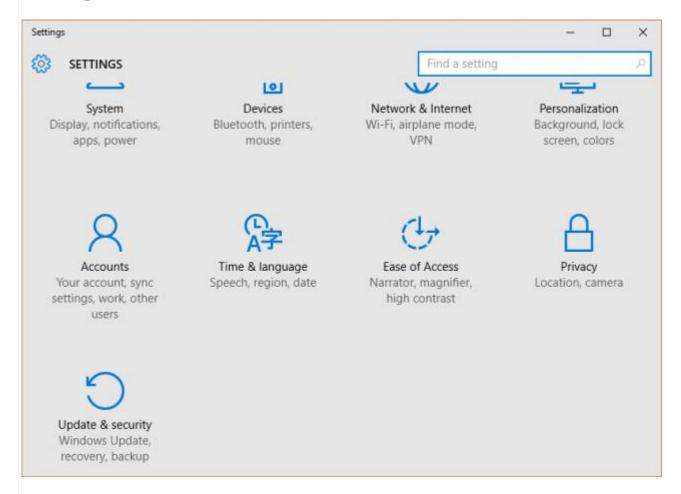
Understanding Windows 10 – A Guide to Help Get you Started

By Jim Hillier – July 14, 2015

https://davescomputertips.com/understanding-windows-10-a-guide-to-help-get-you-started/

Following an initial perusal of <u>Windows 10</u> it appeared that Microsoft included a lot of changes merely for the sake of change, presumably to help expand the gap between <u>Windows 8</u> and Windows 10. However, after spending more time working with the new operating system you will realize that statement is incorrect, and here's why.

Settings – The Windows 10 Nerve Center

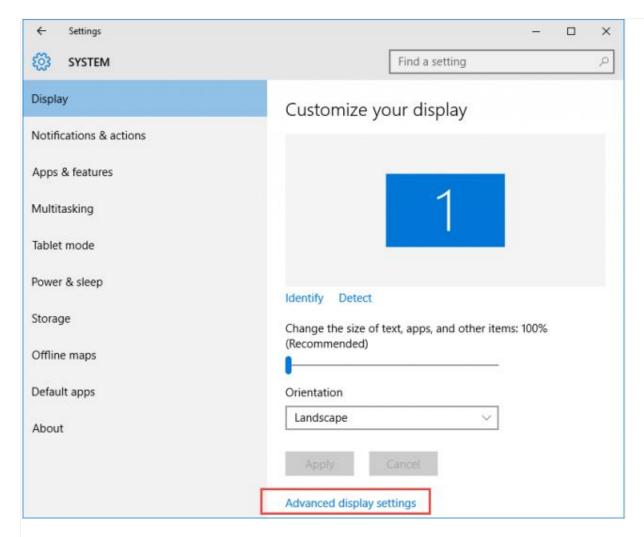


At the very heart of Windows 10 is the "Settings" menu which provides the interface for managing how the operating system displays and behaves. Consequently, a number of previously easily accessible settings/options have been moved into the Settings menus for the sake of centralization. While this may well now force users to dig a little deeper in order to locate a particular setting, I can appreciate the logic behind it, everything in one place, and no fragmentation.

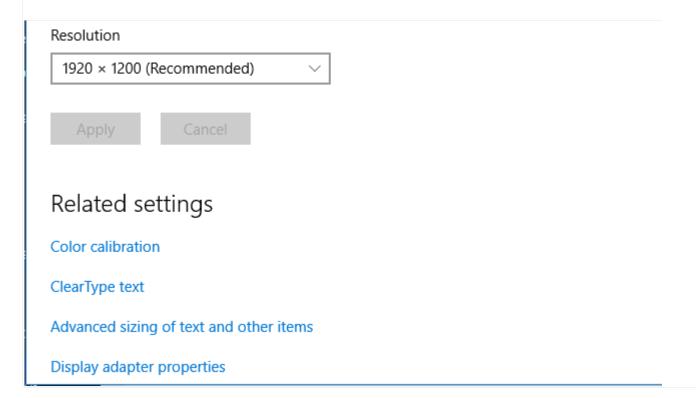
Finding "Screen Resolution in Windows 10

For example: Accessing "Screen Resolution" settings has long been a simple matter of selecting the option from the desktop right click menu. Now, in Windows 10, one needs to take a rather more convoluted path:

- 1. Click Start and then Settings
- 2. Click **System**, then click **Display**(the Display tab should open by default)
- 3. Click "Advanced display settings"



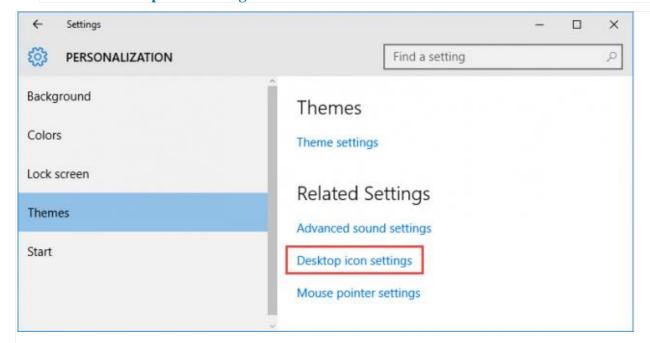
There it is!



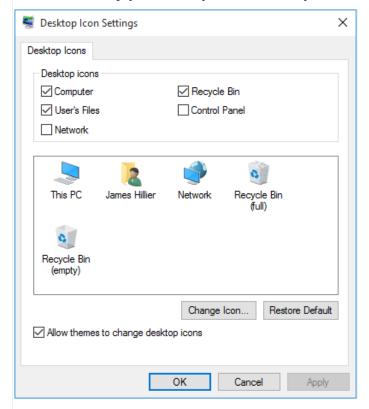
Adding Desktop Shortcuts to System Locations in Windows 10

This is another setting location that has changed and integrated into the all, encompassing Settings menu. With the extensive Win-X customizable Start Menu, and the ability to pin items to the Taskbar, desktop shortcuts are somewhat redundant in Windows 10. However, if you want to desktop shortcuts, here's how to add them:

- 1. Click Start and then Settings
- 2. Click **Personalization and then Themes**(on the left)
- 3. Click Desktop Icon Settings



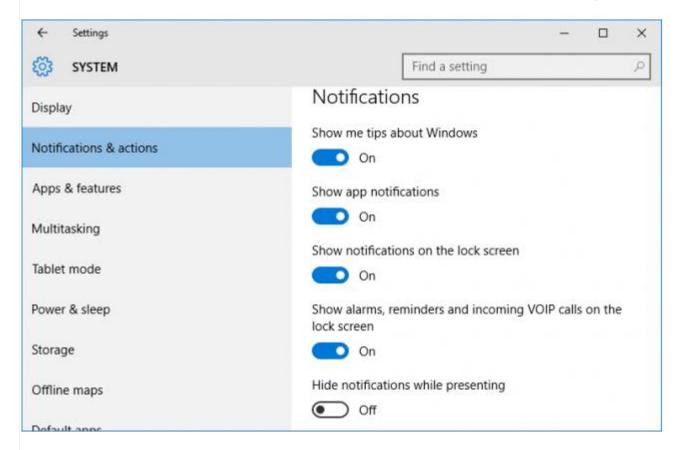
From there, simply enable any shortcuts that you want to appear on the desktop:



Bottom Line: if you're looking for a particular setting, go to the Settings menu and start to dig, it'll be there!

Windows 10 Settings "on and off Switches"

The Settings section is also where you select the "on and off" switches that let you enable and disable pretty much everything:



Look familiar? Who's copying who?

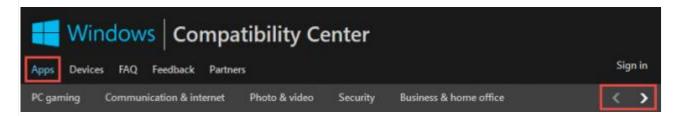
Windows 10 Automatic Updates

Forced automatic updates remain a major bone of contention among a vast number of users (and potential users). Why Microsoft assumes the right to force third party updates on its users, specifically driver updates, is unfathomable. Surely as end users, we should retain the right to decide whether to install these updates or not?

Of course, there is still a chance that Microsoft may change its tune on forcing automatic driver updates prior to delivery of the final version, and, if the volume of negative feedback holds any sway at all, perhaps they will. We live in hope!

Window Compatibility Center

When you visit <u>Windows Compatibility Center</u>, you can either search for information by entering a specific product name or utilize the top menu to browse by category:



https://www.microsoft.com/en-us/windows/compatibility/CompatCenter/Home

https://www.microsoft.com/en-us/software-download/windows10

Microsoft Accounts vs. Local Accounts in Windows 8

♠ Add a user

There are two options for signing in:

Microsoft account

Signing in to PCs with your email address lets you:

- · Download apps from Windows Store.
- · Get your online content in Microsoft apps automatically.
- Sync settings online to make PCs look and feel the same—like your browser history, accordicture, and color.

Windows 8 is more integrated with Microsoft's services than ever. When you create a user account on your computer, you'll be prompted to use a Microsoft account. Microsoft accounts are different from local user accounts, which are still available.

Microsoft accounts offer useful synchronization features, even for desktop users. However, a Microsoft account isn't mandatory if you stick to the Windows desktop – you can continue using a local user account on the desktop without any problems.

What is a Microsoft Account?

There's a good chance you already have a Microsoft account. A "Microsoft account" is a new name for Microsoft's online account system, which was previously known as Windows Live ID, Microsoft Passport, and Microsoft Wallet, among other names.

If you've ever registered for a Hotmail account or Windows Live ID; that's a Microsoft account. Microsoft accounts are now also used for other Microsoft services, including Xbox Live, Windows Phone, and Zune.

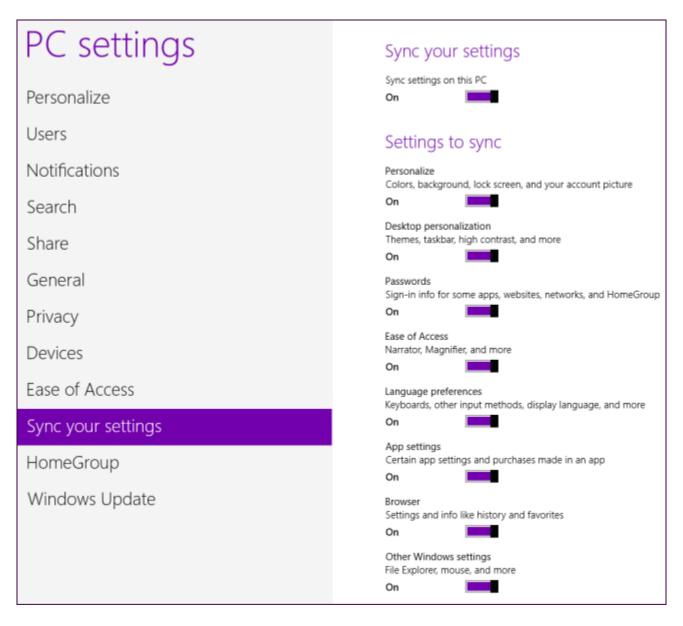
While most Microsoft accounts will probably be associated with an @hotmail.com, @outlook.com, or @live.com email address, you can create a Microsoft account linked to any email address. For example, you could have a Microsoft account linked to your @gmail.com email address.

Benefits of Using a Microsoft Account

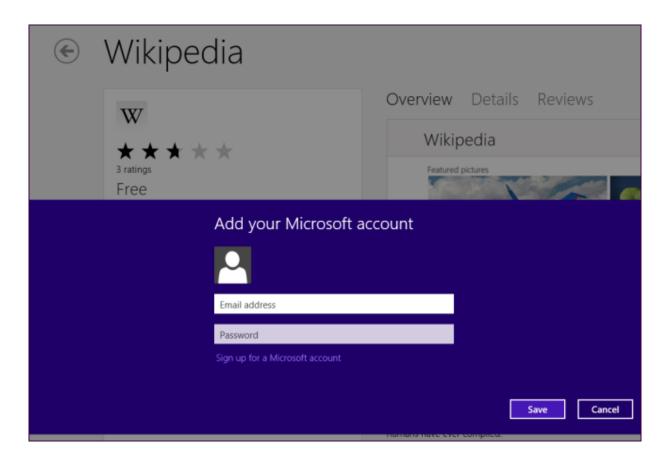
While using a Microsoft account, you'll be able to synchronize some of your PC's settings between your computers. You'll find options for controlling these settings in the PC Settings application – move your mouse to the bottom or top right corners of the screen, select the Settings charm, and click *More PC Settings* at the bottom of the Settings pane to open it.

Many settings here, such as "App settings," only apply to modern-style apps (formerly known as Metro-style apps). Other sync options, such as your account picture, desktop background, and taskbar configuration are useful to Windows desktop users that use Windows on multiple computers. After you set up Windows once, your settings will be synchronized between every computer you log into with your Microsoft account.

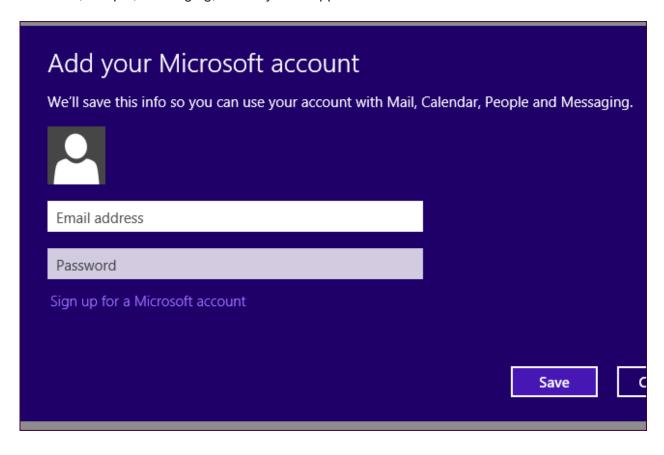
Passwords can only be synced after you trust your computer.



You can browse the Windows Store with a local user account, but you'll have to sign up for a Microsoft account if you want to download an app. The Windows Store only allows you to download Modern-style apps, though – if you only use desktop apps, this limitation won't bother you.



Many modern-style apps won't work until you log in with a Microsoft account. If you're using a local user account, you'll have to sign up for a Microsoft account if you want to use included apps like the Mail, Calendar, People, Messaging, and SkyDrive apps.

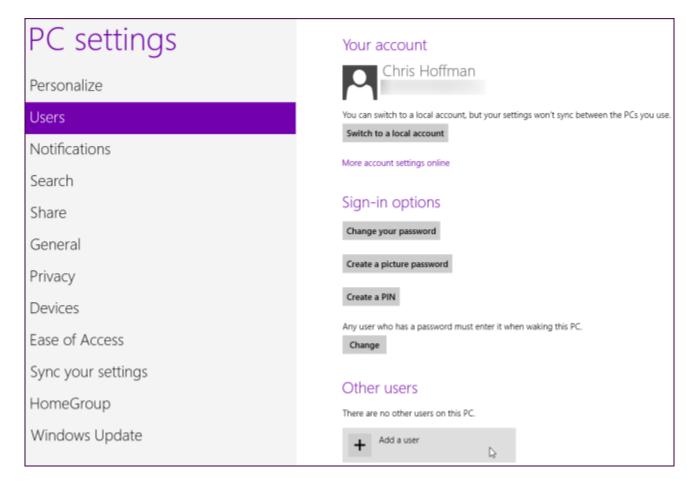


Selecting a Microsoft Account or Local Account

You can switch between a local account and Microsoft account from the PC Settings app – use the *Switch to a local account* or *Switch to a Microsoft account* button under your username.

You can also add additional users using the *Add a user* button – each additional user account can be either a Microsoft account or local account.

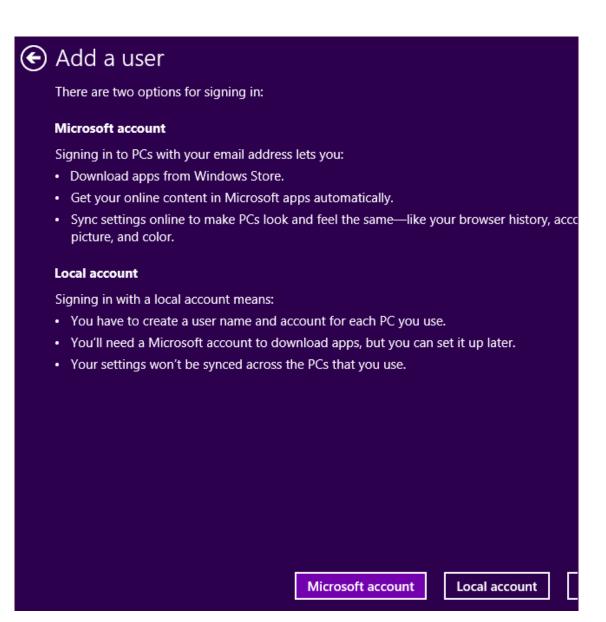
Click the *More account settings online* link here to manage your Microsoft account's security settings in a web browser. You can also access your Microsoft account summary page here.



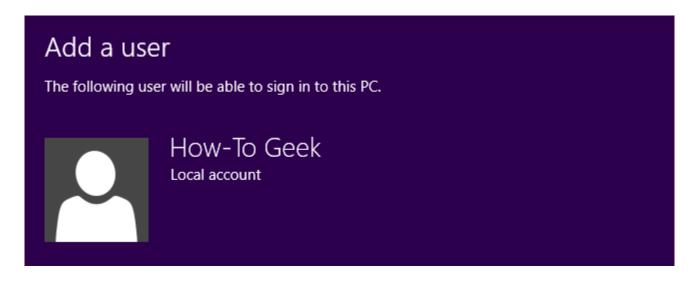
To create a local user account, you'll have to use the Sign in without a Microsoft account link hidden near the bottom of the Add a user dialog.

Add a user What email address would this person like to use to sign in to Windows? (If you know the email address they use to sign in to Microsoft services, enter it here.) Email address When you sign in to Windows with a Microsoft account, you can: Download apps from Windows Store. Get your online content in Microsoft apps automatically. Sync settings online to make PCs look and feel the same–this includes settings like browser favorites and history. Privacy statement Sign up for a new email address Sign in without a Microsoft account Next Canc

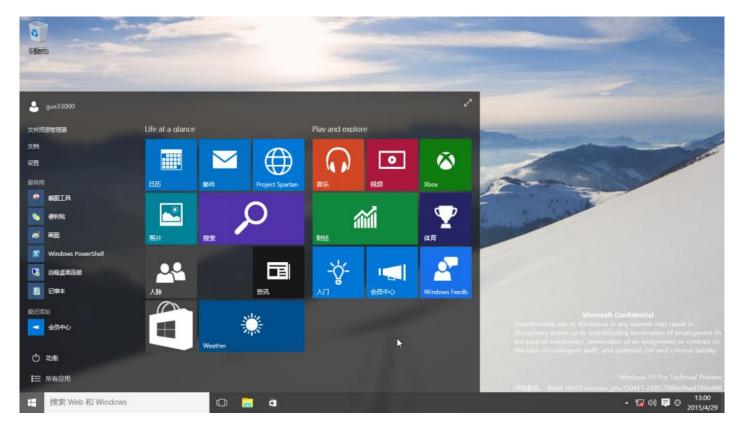
After clicking this link, you'll have to click the *Local account* button again. Even after clicking *Sign in without a Microsoft account*, the *Microsoft account* button remains highlighted. Microsoft clearly wants you to create a Microsoft account for use with Windows 8.



Local user accounts can be used normally after creation. You'll only run into limitations if you attempt to sync your settings, download modern-style apps from the Windows Store, or use certain modern-style apps that require a Microsoft account.

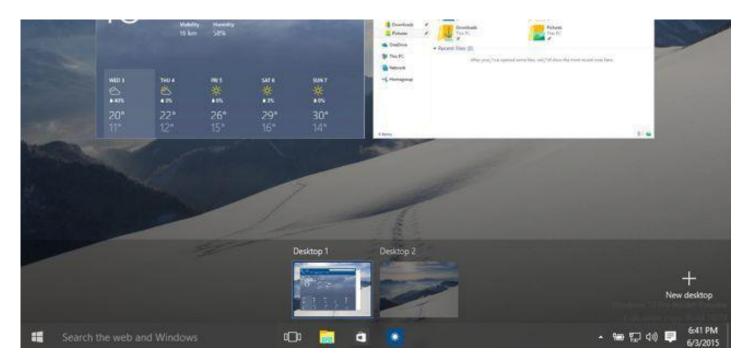


Here's What's Different About Windows 10 for Windows 8 User



What's Different about Windows 10 from Windows 8

Here's What's Different About Windows 10 for Windows 7 User



Unlike Windows 8, Windows 10 actually feels designed for a PC with a keyboard and mouse. Windows 7 users will be much more at home with Windows 10, but there are still some big changes.

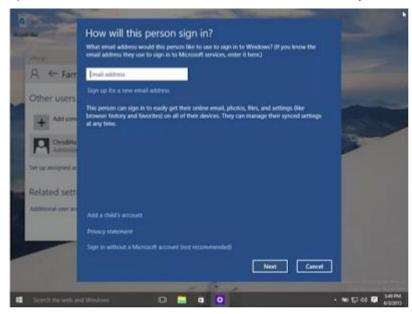
If you're a Windows 7 user, you might be surprised to see just how much has changed after you upgrade. Thankfully, there are no <u>weird hot corners</u> to learn.

Microsoft Account Integration

When you set up Windows 10, the first thing you'll be asked is whether you want to <u>log into your Windows</u> <u>system with a Microsoft account</u>. This is similar to logging into a Mac or iPhone with an Apple account, or a Chromebook or Android device with a Google account.

If you log in with a Microsoft account, many desktop settings (including your wallpaper) will sync between your PCs. You'll be automatically logged into Microsoft services like the OneDrive client integrated into Windows. A Microsoft account is mandatory to use some of the new features, like the Windows Store.

If you don't want to use a Microsoft account, that's also fine — there's a small little link that allows you to set up a traditional, local Windows account. You can easily convert it to a Microsoft account later, if you like.



The New Start Menu

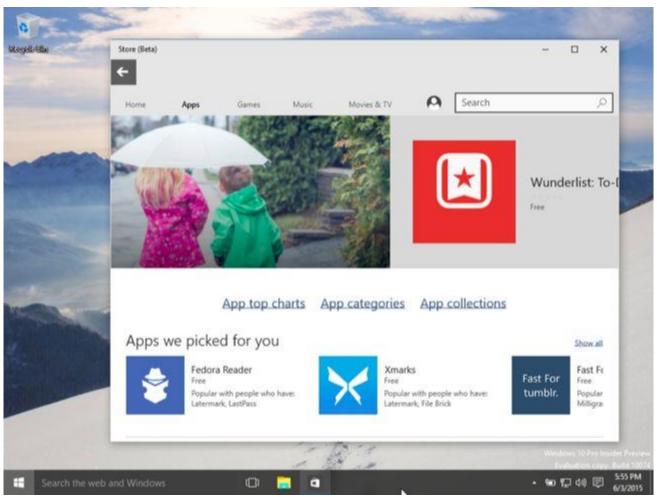
The Start menu looks very different from how it did on Windows 7. The live tiles found on Windows 8's Start screen make a return here. But, don't worry — you can remove all the live tiles if you don't like them. Just right-click them and remove them. The Start menu looks a bit different, but it has all the usual features you'd expect — a list of all your installed applications as well as power options for shutting down or restarting your PC. Move your mouse to any edge of the Start menu and you'll be able to resize it.



Universal Apps and the Windows Store

Many of the apps that come with Windows 10 are "universal apps," which are the successor to Windows 8's "Metro apps" or "Store apps." Unlike on Windows 8, these apps actually run in windows on the desktop, so you may actually be interested in using them.

To get more of these apps, you'll need to open the Store app included with Windows and download them from the Windows Store. There's no way to "sideload" these types of apps by downloading them from the Internet, although you're free to avoid them entirely and install traditional Windows desktop applications from the web. You can also mix and match traditional Windows desktop applications and new apps from the Store. They'll all run in windows on your desktop.



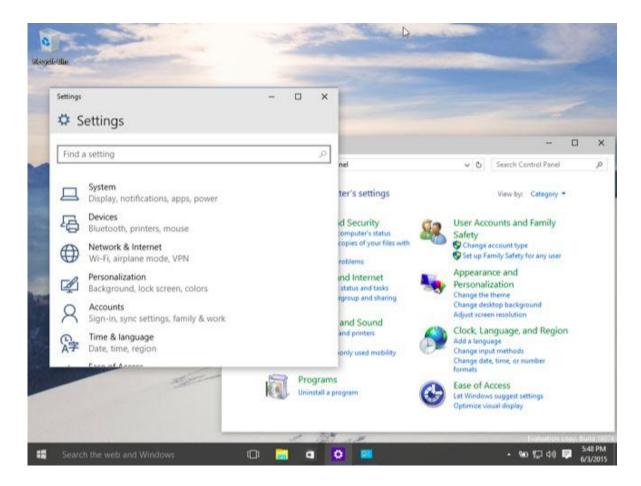
Settings App vs. Control Panel

The Settings option in the Start menu takes you straight to the new Settings app, which is evolved from the PC Settings app on Windows 8. This is designed to be a more user-friendly way to configure your computer.

However, it still doesn't contain every setting. The old Windows Control Panel is still included. Some older settings may only be available in the Control Panel, while some newer settings may only be available in the Settings app. To quickly access the Control Panel and other advanced options, you can right-click the Start button or press Windows Key + X. This menu is a useful holdover from Windows 8.

The <u>Refresh and Reset options</u> also make the leap from Windows 8 to 10. These allow you to quickly get your computer back to a like-new state without having to actually reinstall Windows.

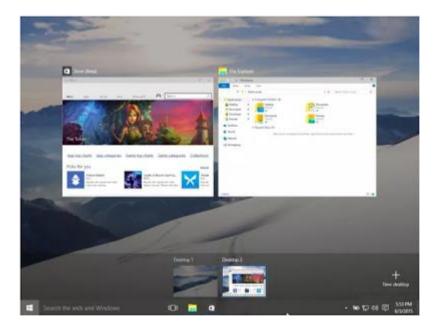
You won't be able to disable automatic Windows updates on Windows 10 Home systems. You'll need Windows 10 Professional to defer updates.



Cortana and Task View on the Taskbar

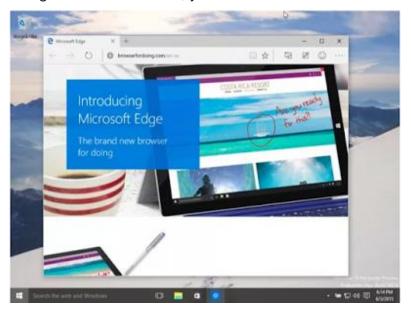
The Windows taskbar has changed a bit. In Windows 8, Microsoft removed the Start button from the taskbar and you only saw icons for your programs here. In Windows 10, the Start button isn't just back — there's a "Search the web and Windows" field that launches Microsoft's Cortana assistant and a <u>Task View button</u> that provides an overview of all your open windows and virtual desktop features.

Both of these features are enabled by default. If you'd like to disable them, you can just right-click the taskbar and choose to hide the Search and Task View options.



Edge Replaces Internet Explorer

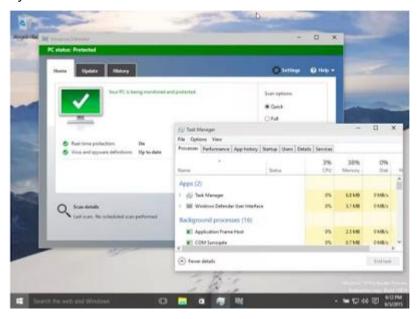
Internet Explorer is no longer the default browser, although it's still available for businesses that still need access to its older rendering engine. In its place is a modern browser named Edge. Microsoft's Edge browser should be more standards-compliant and perform better. It also no longer supports ActiveX controls, so all those old Internet Explorer toolbars and browser plug-ins will no longer function. If you've been using Internet Explorer, this is the browser you'll be using instead. If you're using Chrome or Firefox, you can install that and continue browsing normally.



Desktop and Security Improvements

Many other <u>desktop improvements from Windows 8</u> are still here, but you won't have seen them if you've been using Windows 7. The Task Manager was given an upgrade, so it's easier to see what's using your system resources and even manage startup programs without third-party software. Windows Explorer was renamed File Explorer and now has a ribbon — even if you don't like the ribbon, File Explorer offers many useful features. For example, the file-copying-and-moving dialog window is much improved and Windows can mount ISO disc image files without third-party software.

There are also many <u>security improvements from Windows 8</u>. Windows 10 includes Windows Defender by default. Windows Defender is just a renamed version of Microsoft Security Essentials, so all Windows systems have a baseline level of antivirus protection. <u>SmartScreen</u> is a reputation system that tries to block harmful and unknown file downloads from harming your computer.



These are far from the only improvements found in Windows 10. For example, you'll find a notification center and redesigned power, network, and sound icons in the system tray. Windows 10 includes Game DVR functionality for recording and streaming PC games. Microsoft has made many low-level tweaks that make Windows use less disk space, boot faster, and provide better protection against attacks.

Despite all the changes, Windows 10 is much easier to get to grips with than Windows 8 was. It's based on the familiar desktop interface, complete with a start menu and desktop windows. Windows 10 does have a "Tablet mode," but you have to enable that manually or have it automatically enabled when using tablet hardware. You aren't forced into tablet mode on typical PCs.

Get to know File Explorer's Ribbon toolbar in Windows 10

Greg Shultz explores the Ribbon toolbar in Windows 10's File Explorer for recent Windows 7 and Windows XP users.

By Greg Shultz September 11, 2015,



If you skipped Windows 8.x and have just upgraded to Windows 10 from Windows 7 or Windows XP, you're probably a little disoriented when you go to perform file management tasks. To begin with, the name of the tool has changed from Windows Explorer to File Explorer, and the file management tool has been given a slightly new user interface that features a Ribbon toolbar instead of a traditional drop-down menu system.

When I first encountered File Explorer's Ribbon toolbar, I was more than a little disconcerted by what I initially thought would be a big learning curve. However, I can now say with confidence that, once you get used to the Ribbon toolbar, you'll wonder how you ever got along without its feature set. It's truly a much more efficient navigational system.

To get started, let's take a look at the main features of File Explorer's Ribbon toolbar.

Keep in mind that while there are a host of other new features sprinkled throughout Windows 10's File Explorer that add great functionality to all the typical file management operations you are likely to perform, I won't cover them all in this article.

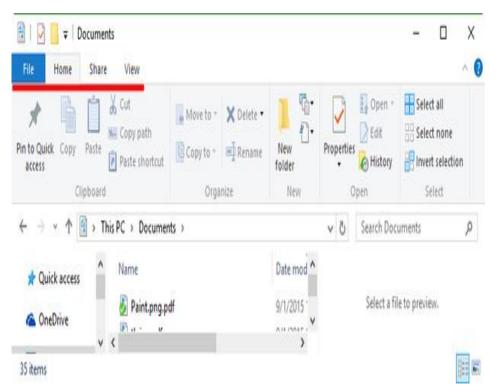
Overview

File Explorer's Ribbon contains one menu and a set of Core tabs that are always visible along with the Contextual tabs, which appear based on the type of object that you've selectedThese tabs include: a location, a folder, or a file and then provide related commands. This system of Core and Contextual tabs is designed to easily expose close to 200 different file management commands. The majority of these commands have

always existed in Windows Explorer, but they were buried in numerous nested menus, pop-ups, dialog boxes, or right-click context menus.

The Ribbon in File Explorer (**Figure A**) includes the File menu and three Core tabs titled Home, Share, and View.

Figure A

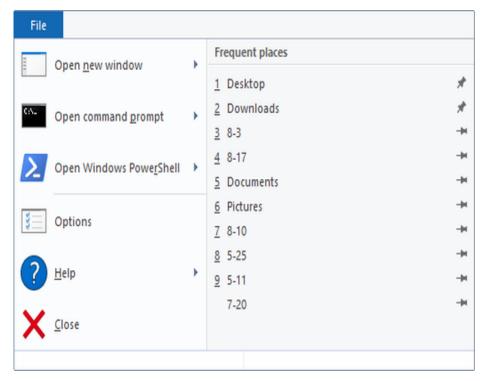


File Explorer's base Ribbon contains the File menu and three Core tabs.

File menu

As I mentioned, the Ribbon toolbar contains one menu called the File menu (**Figure B**). This menu is designed to provide you with quick access to some of the more general commands in File Explorer. When you access the File menu, you'll see a set of commands on the left side and frequent places on the right. The Frequent places show the most recently accessed folders, and this remains visible until you select a command that has a submenu. That submenu, then overlays the frequent places space and provides you with related options.

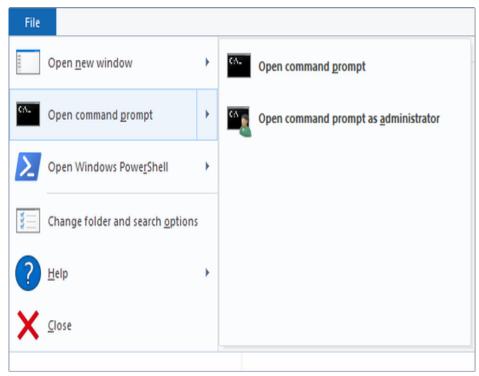
Figure B



The File menu provides access to the general commands in File Explorer

For example, when you select Open command prompt, the submenu overlays the Frequent places and shows commands to open a regular or an administrator command prompt (**Figure C**). Both of the open a command prompt window selections are targeted on the currently selected folder.

Figure C



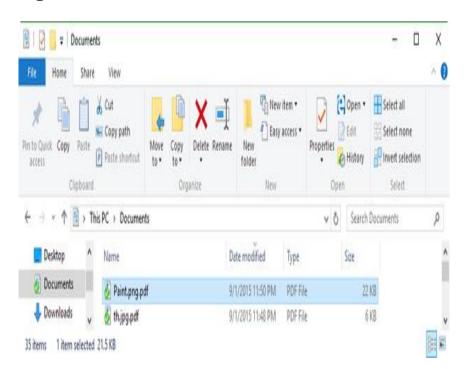
Selecting an item from the File menu displays a menu of related commands

As you can see, other commands on the File menu allow you to open a new Explorer window, open PowerShell, Change folder and search options, access Help, and close File Explorer.

Home tab

The first of the Core tabs is the Home tab (**Figure D**), and it provides you with access to the most often used file management commands. The Clipboard group includes all the standard commands, along with a very handy Copy path command. Just select a folder, click the command, and the current path is copied to the clipboard.

Figure D



The Home tab provides you with access to the main file management commands.

In the Organize group, you'll find that the Move to and Copy to commands are readily accessible rather than being hidden away on the Edit menu as they were in Windows XP/7. You'll also find that the Delete and Rename commands live in this group.

Moving down to the New group, you can create new folders and files of various types. Using the Easy access command allows you to make things easier to find by adding folders to a Library or to the Favorites, as well as by mapping a drive letter to a network location. This menu also contains items for configuring and using Offline files and folders.

In addition to the Open and Edit commands, which function just like before by launching the associated application and loading the selected file, the Open group provides you with quick access to the Properties dialog box.

The History command provides access to the File History feature. (File History is a new feature that works like a combination of Previous Versions and Windows Backup and Restore. File History continuously monitors files stored in Libraries, Desktop, Favorites,

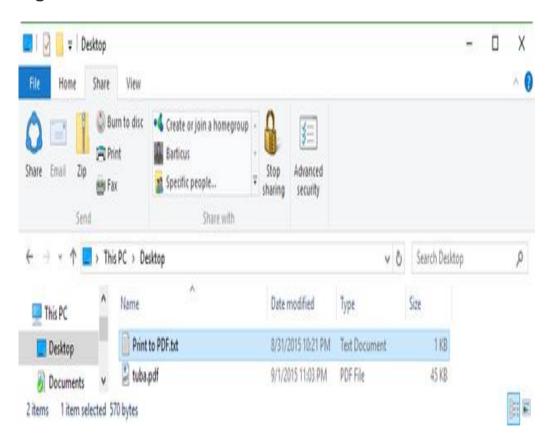
and Contacts folders, and when it detects changes in any file, it then makes a backup copy to another location—such as an external hard disk or a network drive. I'll cover File History in more detail in a future article.)

The Select group provides you with a set of commands for selecting groups of files and folders.

Share tab

The Share tab (**Figure E**) is your one-stop location for any command related to sharing files with others. For example, within the Send group, you can create a Zip file and email it. You can burn files to an optical disc, plus print or fax documents.

Figure E



The Share tab is your one-stop location for any command related to sharing files with others

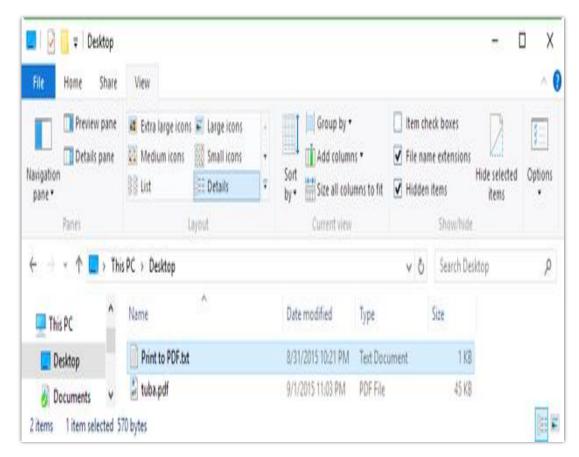
In the Share with group, you'll find a gallery that allows you to share files and folders with your home group or with specific users. The Advanced security command opens the Security tab where you can lock down sharing by setting specific permissions.

View tab

On the View tab (**Figure F**), you'll find a host of commands that you can use to configure the way you want File Explorer to display files. In the Panes group, you can configure the Navigation pane, plus enable or disable the Preview pane or the Details pane. The latter

now appears in the same space as the Preview pane rather than on the bottom of the window.

Figure F



The View tab provides you with a host of commands for configuring File Explorer's display.

The Layout group sports a live preview gallery for choosing your icon display—just hover over an option in the gallery, and the file display changes accordingly. The Current view group exposes several great commands. First, the Group by and Sort by commands give you neat ways to narrow and organize the display of your files, they're readily available. Second, when you're using the Details layout, the Add columns and Size all columns to fit commands come in real handy for getting a better look at the available file and folder details in File Explorer's display.

The Show/hide group brings several valuable items that were previously hidden in the Folder Options dialog box to light. The Item check boxes option allows you to enable the check box file selection feature. When you want to show or hide file extensions on the fly, just select the File name extensions check box. When you need to quickly see hidden files, just select the Hidden items check box. The Hide selected items command allows you to quickly set the Hidden attribute—no more going to the Properties dialog box. The Options command opens the Folder Options dialog box.

What's the Difference Between Windows 10's Express or Custom Setup?

Get going fast

Change these at any time. Select Use Express settings to:

Personalize your speech, typing, and inking input by sending contacts and calendar details, along with other associated input data to Microsoft. Let Microsoft use that info to improve the suggestion and recognition platforms.

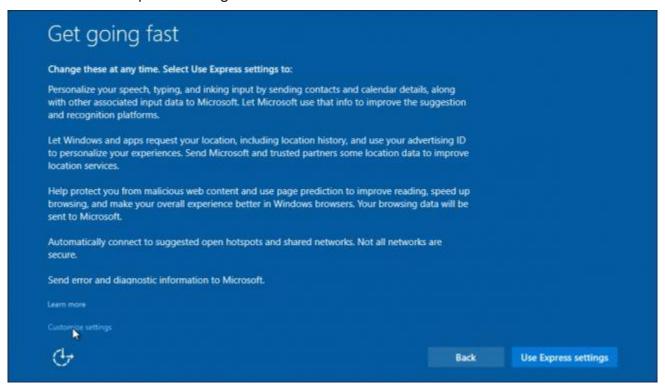
Let Windows and apps request your location, including location history, and use your advertising ID to personalize your experiences. Send Microsoft and trusted partners some location data to improve location services.

Help protect you from malicious web content and use page prediction to improve reading, speed up browsing, and make your overall experience better in Windows browsers. Your browsing data will be sent to Microsoft.

When you first set up Windows 10, Microsoft wants to rush you through the process with "Express Settings". We recommend taking a little time and stepping through the customized setup instead.

This setup process has been in place since Windows 8, and it's been our experience that most of the time users are going to just choose the easy way. There are, however, some really important privacy items you want to pay attention to.

When you see the setup screen that says "Get going fast," you should click "Customize settings" instead of "Use Express settings".



Microsoft doesn't make it obvious, but there in the lower-left corner you will see the "Customize settings" option.

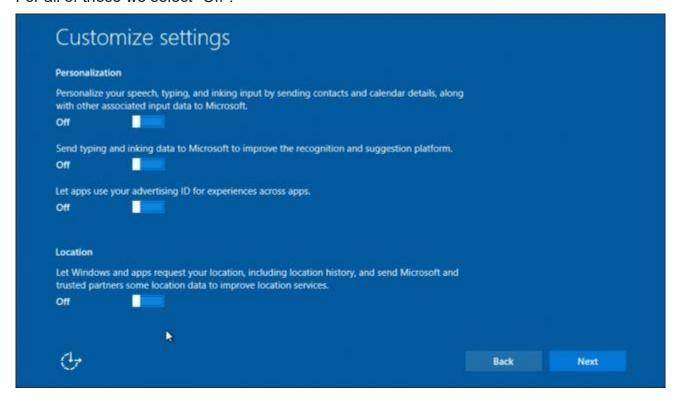
The first screen deals with Personalization and Location, the latter which <u>we've discussed in greater</u> <u>detail</u> deals with localization settings.

Fair warning, disabling many of these settings is probably going to lessen the Windows 10 experience, or at least the experience Microsoft intends. That said, let's look more closely at the kinds of information you're submitting if you willfully accept the defaults.

Personalization and Location Settings

First, with the personalization settings, you agree to send Microsoft contacts and calendar details and other "associated input data" through speech, typing, and inking input. This data is stored in the cloud so it can presumably be replicated to other Windows 10 installations when you use your Microsoft account.

You also agree to send off typing and inking data to improve recognition and suggestions, and finally, you also consent to allow apps to use your advertising ID for "experiences across apps." For all of these we select "Off".



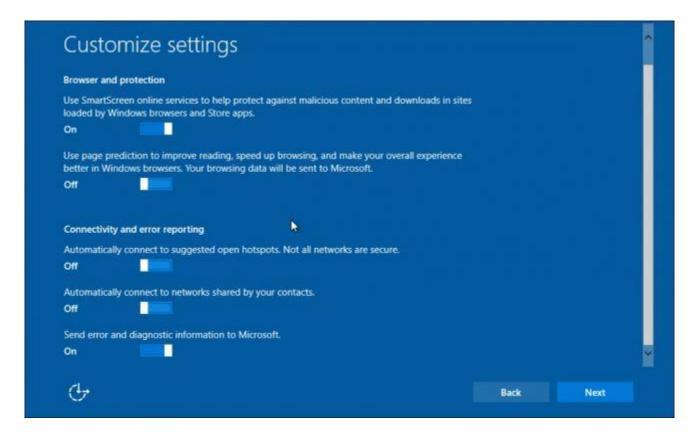
Off! Off! Off! All of it off!

As far as location data is concerned, if your computer is chained to your desk, or you've never had a need to submit your location to Microsoft, then you can most definitely turn this item "Off" as well. You can always go back later and turn it back on if it becomes a usability issue.

Browser and Protection, and Connectivity and Error Reporting Settings

The next screen deals with browser and protection settings, as well as connectivity and error reporting. It's probably a good idea to leave SmartScreen on since it is designed to protect users against "malicious content and downloads," though SmartScreen will only work with the new Edge browser.

You can leave page prediction enabled if you choose as well, but again, this is only going to work with the new Edge browser so if you use Chrome or Firefox, this setting doesn't matter. We use another browser so we turned it off.



Of the last three options, two deal with connecting to networks, we definitely believe that you should turn "Off" automatic connectivity to open hotspots, and networks shared by contacts.

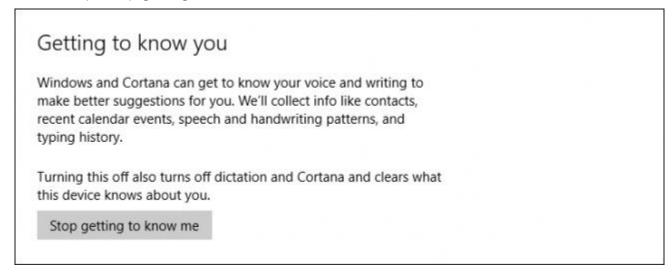
The last option "send error and diagnostic information to Microsoft" is up to you. If you don't want to share this sort of information with them, then turning it "Off" isn't going to affect your system one bit.

Turning This Stuff Off Later

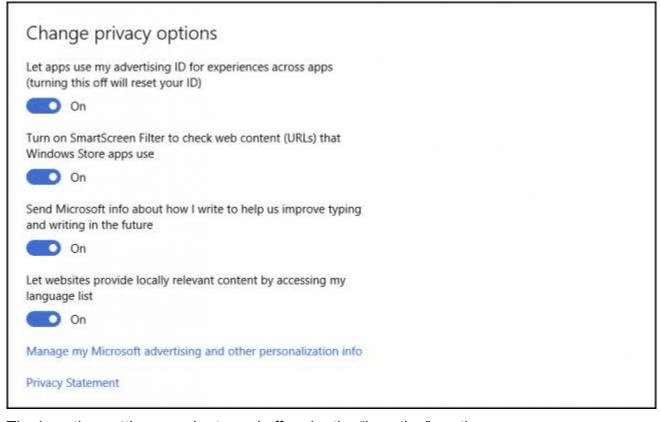
If you have chosen express settings and you want to opt out of some or all of these, all is not lost. You can still go into the settings and change things.

To turn off the first item found in the Personalization settings, you will need to open the Privacy group in Settings and then "Speech, inking, & typing".

Click or tap "Stop getting to know me".



To turn off the "advertising ID" and "send typing and inking data" options, you will need to do that in the General privacy section. You will also find the option to turn off (or on) the SmartScreen filter here.



The Location settings can be turned off under the "Location" section.

Reminder! If You Haven't yet, Turn Off Windows 10 Keylogger Now

Monday, September 07, 2015 Swati Khandelwal

Do you know? Microsoft has the power to track every single word you type or say to its digital assistant Cortana while using its newest operating system, **Windows 10**.

Last fall, we reported about a 'keylogger' that Microsoft openly put into its Windows 10 Technical Preview saying the company 'may collect voice information' as well as 'typed characters.'

It was thought that the company would include the Keylogger only within the <u>Technical Preview</u> of Windows 10, just for testing purpose. But, the thought was **wrong!**

The keylogger made its ways to <u>Windows 10 public release</u> offered by Microsoft for free due to which Windows 10 gained millions of adoption in just a few days after its first roll out back in July – but the **free upgrade is not always free**.

Yes, besides <u>various privacy issues</u>, there is a software component that tracks your inputs using your keyboard, voice, screen, mouse, and stylus, however, it is a bit more complicated than you thought.

Windows 10's Keylogger is More than Just a Keylogger

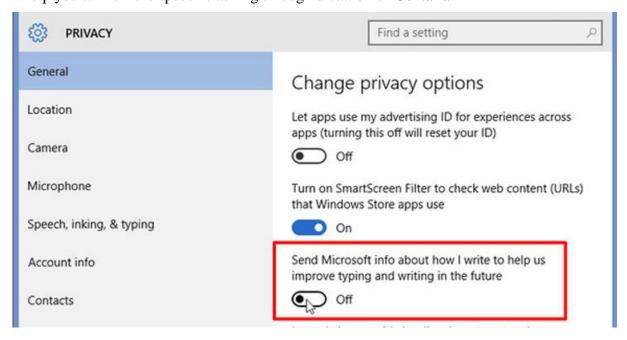
The component is not actually a keylogger it is more than that, as Microsoft openly says...

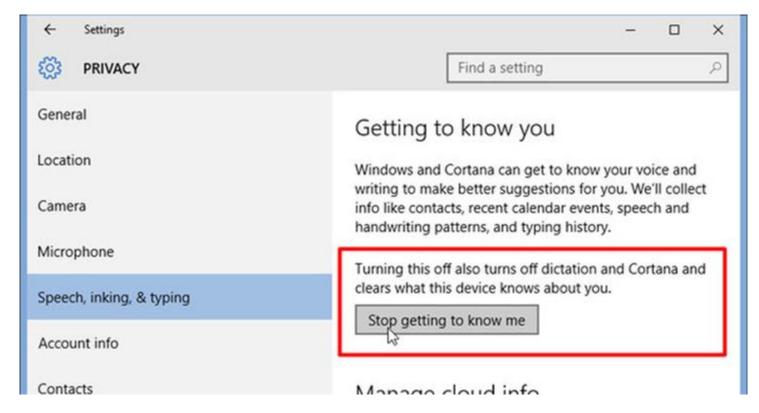
"When you interact with your Windows device by speaking, [handwriting], or typing, Microsoft collects speech, inking, and typing information, including information about your Calendar and People [contacts]..."

If that makes you feel creepy then need not to worry, because the good news is You can Turn Off this Keylogger.

Here's How You can Turn Off the Keylogger

- Click on the **Start Menu**, then open **Settings**.
- Click on **Privacy** settings, which you'll find in the very last row of the menu.
- Once you are in the Privacy menu, click on General
- Under 'Send Microsoft info about how I write to help use improve typing and writing in the future' Turn it to Off.
- Now move ahead to the 'Speech, Inking and Typing' menu and click **Stop getting to know me**. This will help you turn off the speech tracking through dictation or **Cortana**.





Due to several privacy issues built into Windows 10, Microsoft has gained a bad reputation.

Over a week ago, the company introduced Windows 10 data collecting and user behavior <u>tracking</u> <u>features to Windows 7 and Windows 8</u> as well, which is a major privacy concern for many users.

How to disable data logging in Windows 10

Here's a guide which should give you a more private, and safe experience in Windows 10. However, this is accomplished at the risk of not being able to enjoy some of Windows 10's features.

Before/During Installation

- Do **not** use *Express Settings*. Hit *Customize*, and make sure everything is turned off.
- It's strongly preferred that you use a **local account** with Windows 10.

After Installation

- Head to Settings > Privacy, and disable **everything**, unless there are some things you really need.
- While in the Privacy page, go to *feedback*, select *Never* in the first box, and *Basic* in the second box.
- Head to Settings > Update and Security > Advanced Options > Choose how updates are delivered, and turn the first switch off.
- Disable Cortana by clicking the Search bar/icon.
- **(Optional)** Disable web search in Search by going to Settings, and turning off *Search online and include web results*.
- Change the name of your PC by going to Start (or hitting the Windows key), typing *About PC*, and clicking *Rename PC*.

Slightly Complex

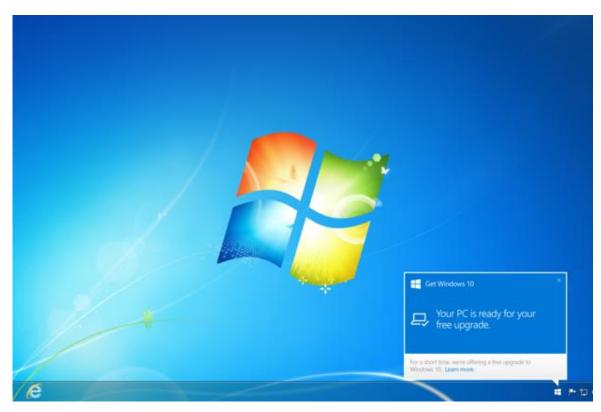
- Open up the Command Prompt by launching cmd as an administrator, and enter the following: sc delete DiagTrack
 - sc delete dmwappushservice
 - echo "" > C:\ProgramData\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-Diagtrack-Listener.etl
- Open up the *Group Policy Editor* by launching **gpedit.msc** as an administrator. Go through *Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds*. Double click *Telemetry*, hit *Disabled* and then apply. **NOTE: This only** *truly* works in the Enterprise edition, but the final step provides a decent enough workaround for Pro users.
- While still in the *Group Policy Editor*, go through *Computer Configuration > Administrative Templates > Windows Components > OneDrive*, double click *Prevent the usage of OneDrive for file storage*, hit *Enabled*, then apply.
- While still in the *Group Policy Editor*, go through *Computer Configuration > Administrative Templates > Windows Components > Windows Defender*, double click *Turn Off Windows Defender*, hit *Enabled*, then apply.
- Open up the *Registry Editor* by launching **regedit** as an administrator. Go through *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection*, select *AllowTelemetry*, change its value to 0, then apply.
- First, download the Take Ownership tweak and enable it. Then, head to the *Hosts File* by going through *C:\Windows\System32\Drivers\Etc*, take ownership of the *hosts* file, and add all of the IPs from this page into the file.

Up To You

- Replace Microsoft Edge/Internet Explorer with **Firefox**, **Chromium**, or any forks/variations of them.
- Replace Windows Media Player with VLC or MPC-HC
- Replace Groove Music with Foobar2000, Winamp, or MusicBee.
- Replace Photos/Windows Photo Viewer with ImageGlass or IrfanView.

Microsoft is Auto-Downloading Windows 10 to PCs, Even If You Don't Want it

Friday, September 11, 2015 Swati Khandelwal



Microsoft wholeheartedly wants you to upgrade to Windows 10. So much that even if you have not opted-in for Windows 10 upgrade, you will get it the other way. *Surprised?*

If you have Windows Update enabled on your PCs running Windows 7 or Windows 8.1, you'll notice a large file between **3.5GB** and **6GB has** mysteriously been downloaded to your computer in the background.

The huge file is actually linked to Windows 10 installation that Microsoft is reportedly downloading on Windows 7 and Windows 8.1 computers even if users have not opted into the upgrade.

The news comes days after it was disclosed that Microsoft is installing *Windows 10's data collecting and user behavior tracking features* onto Windows 7 and 8.1 machines.

With this latest automatic Windows 10 installation, Microsoft is not only consuming your storage space but also <u>using your Internet bandwidth</u> for unrequested files, as the Windows 10 installer downloads up to 6 gigabytes, depending on which Windows version you are using.

According to the latest report published by the <u>Inquirer</u>, a number of users running Windows 7 or 8.1 complained that a large folder called '<u>\$Windows.~BT</u>' has been dropped in their system that tries to install Windows 10 every time they boot up their PCs.

Here's the Kicker:

Microsoft, which released its newest Windows 10 operating system earlier this summer, admitted that it was downloading the unwanted files on users' computers.

The Redmond technology firm said in a statement:

"For individuals who have chosen to receive automatic updates through Windows Update, we help upgradable devices get ready for Windows 10 by downloading the files they'll need if they decide to upgrade." Now, this is insane.

Microsoft mentioned many times that it plans to deploy Windows 10 on over 1 Billion devices worldwide, but upgrading users' computers without their awareness is a bad practice.

Moreover, the practice is problematic for users with slow or metered Internet connections.

Check If Microsoft is Downloading Windows 10 without Your Awareness:

- Open and Check the drive Windows is installed on.
- Look for the folder \$Windows.~BT (it is hidden folder so enable the option to view hidden files)
- If it exists, Windows installation files have already been downloaded without your permission

Also from Computer-World

"For those who have chosen to reserve their upgrade of Windows 10 and those that have Windows Update automatic updates enabled, we may help customers prepare their devices for Windows 10 by downloading the files necessary for future installation," a spokeswoman said in a Sept. 11 email response to several questions. "This does result in a smoother upgrade experience and ensures the customer's device has the latest software."

Earlier that same day, Microsoft had asserted, "This is an industry practice that reduces time for installation and ensures device readiness," when it confirmed accounts that Windows 7 and Windows 8.1 users had found <u>large amounts of data representing the Windows 10 upgrade on their PCs</u> even though they had not requested the free upgrade.

Some applications *do* pre-load updates in the background (<u>Google's Chrome</u> is one example, <u>Mozilla's Firefox</u> another), before triggering the program install at the next launch, but operating systems have never taken that tack.

Although Microsoft's retreat from the industry-practice claim was minor in itself, it was more notable for another reason: As the latest instance in a cycle of company to customer communication omissions and missteps.

Those have ranged from difficulty explaining who would get the free Windows 10 upgrade and who would not. Ultimately, Microsoft decided that it would not amnesty customers running counterfeit copies of older editions and a months-long wait before it announced that users would receive updates and upgrades free of charge for a decade, to an under-explained new feature that shares upload bandwidth to provide for others faster downloads and a mandatory data collection practice that gives Redmond telemetric information on how the OS and applications are used and run.

Also irksome was Microsoft's installation of a nag-and-notification app on virtually all consumergrade Windows 7 and Windows 8.1 devices and on some business PCs as well that pitched Windows 10 and asked users to "reserve" a copy prior to, and after as well, the July 29 launch.

Microsoft *did* publicize the Get Windows 10 app on June 1, the same day it began triggering it on most devices, but that was several months after <u>word circulated of the practice</u>.

It did nothing of the sort before starting to pre-load the OS upgrade on Windows 7 and 8.1 machines whose owners had *not* reserved a copy. While the rationale may have made sense within Microsoft - whether for the expressed purpose of speeding up the upgrade process, as it claimed last week, or with an implied agenda of boosting adoption, which smacked of duplicity to some it struck a nerve with the power users whom Microsoft has traditionally relied on as its ambassadors.

"This was a Big mistake on Microsoft's part. If people didn't opt-in for the upgrade, they should not have to download it," opined Adam Forcount in a comment appended to *Computerworld*'s story last week about the background upgrade downloading practice. "This kind of behavior from Microsoft is extremely disheartening. If I had wanted someone else to decide how I should use my computer, I would have bought an <u>Apple</u> product."

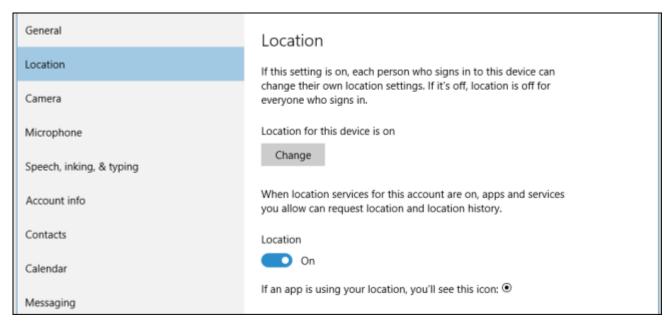
Here are link to article(s)

http://www.computerworld.com/article/2984312/microsoft-windows/microsofts-decision-to-pre-load-windows-10-upgrade-sans-consent-is-ill-advised.html

and

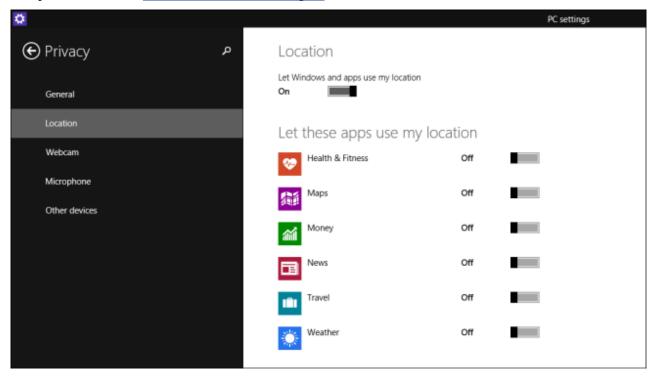
http://www.computerworld.com/article/2983633/microsoft-windows/microsoft-pushes-windows-10-upgrade-to-pcs-without-user-consent.html

How to Disable or Configure Location Tracking in Windows 10



Windows 10 includes a whole bunch of new privacy settings, all are important in their own right, but perhaps none so much as the location settings. If you're privacy-conscious, you will definitely want to investigate them further.

As a whole Windows 10's privacy settings, at least in the most current build, are a lot more extensive and comprehensive than its Windows 8.1 counterpart.



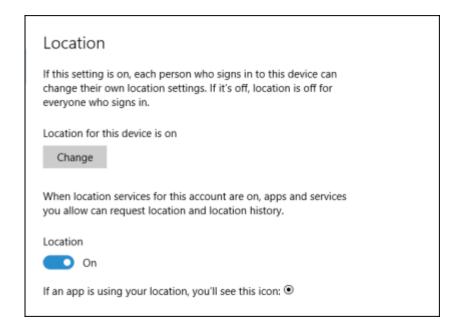
Windows 8.1's Privacy settings are fairly lacking. There's some basic stuff here but nothing like we should expect to find on a modern operating system.

One of the most important aspects of any set of privacy options will be the location items, because those are going to tie you and your device to a place, revealing where you are and where you have been. Luckily, Windows 10 includes a better set of location-oriented privacy settings, which we want to discuss in greater detail today.

Disabling Location Globally or Individually

The first and most important difference between Windows 8.1 and Windows 10 is that in the latter, you can now disable location either globally, so it is disabled for all user accounts on that device, or individually, meaning each user can set their own location settings.

First, open up the Settings in Windows 10 and click on the Privacy group. To turn off location just for that account, you can click the button under "Location" to "Off".



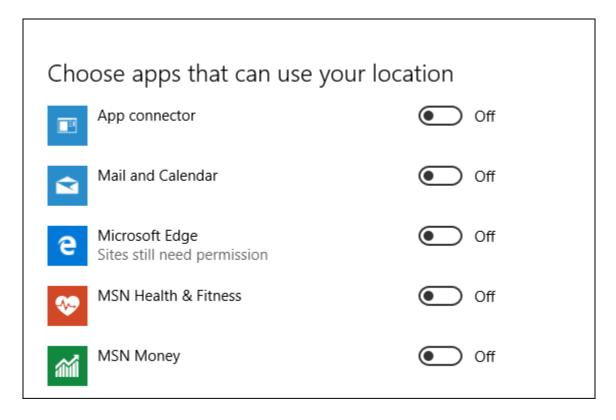
If you want to turn off location for the entire device, however, you want to click the "Change" button, which will then open a new window so you can turn off the "Location for this device".

If you decide to leave location on, then there are further options you need to check, First there's your "Location history". History is stored a "limited time" for the need of certain apps and services that rely on it.

To clear the history on your device, simply click the appropriate button.

Location history When location is on, the locations obtained to meet the needs of your apps and services will be stored for a limited time on the device. Apps that have access to these stored locations will appear below. Clear history on this device Clear Learn more about location settings Privacy Statement

Below the clear history option are the apps that actually poll your location when you use them. This is no different than on Windows 8.1, and you simply need to go through and click "Off" or "On" any apps you want to disallow or grant (respectively) permission to access your location.



Finally, there's a new "Geofencing" option. If you don't know what geofencing is, you're in luck because we have a great article that explains it.

On Windows 10, if you have an app that is using your location for geofencing, it will show up under the heading. You can then prevent apps from using your location for geofencing by turning them off.

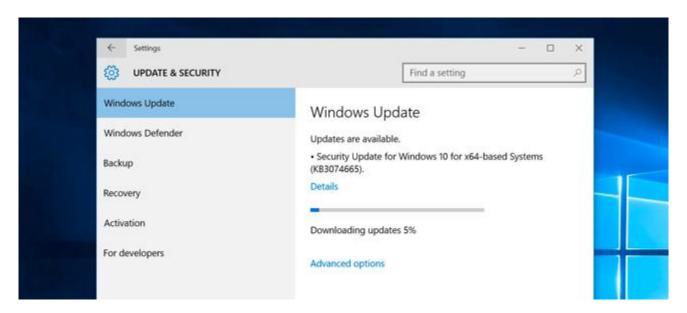
Geofencing

A geofence is a boundary around a place of interest, and apps can use your location to see if you're crossing in and out of one. To stop apps from using your location for geofencing, turn off location for those apps.

None of your apps are currently using geofencing.

So that's it for Windows 10's location settings. Microsoft has obviously given it more time and thought than in Windows 8.1.

What You Need to Know About Windows Update on Windows 10



Windows Update has seen a lot of <u>changes on Windows 10</u>. The biggest is a more aggressive approach to getting everyone up-to-date, but Windows 10 will also use Bit Torrent-style peer-to-peer downloads for updates.

Many of the included applications on Windows 10 like Microsoft Edge browser and all those other "universal apps" will be automatically updated through the Windows Store, which is separate from Windows Update.

The Control Panel Interface is Gone

Windows 8 offered dual interfaces for Windows Update — one in the PC Settings app, and one in the older Control Panel. Windows 10 retains most of the old Control Panel, but the Windows Update interface has been removed.

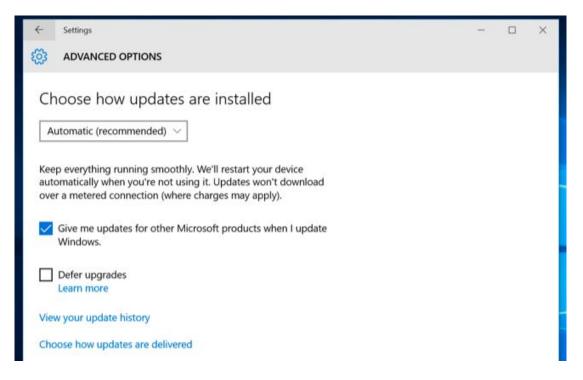
Instead, you'll find Windows Update in the new Settings app under Update & security. This is the only interface for Windows Update in Windows 10.

Updates Install Automatically, and You Can't Choose Which

Visit the Windows Update interface and you'll just find a single button — "Check for updates." Click this button and Windows will check for available updates. If it finds any, it will automatically download and install them. Windows will also check for updates in the background and automatically download and install them.

Unlike on previous versions of Windows, there's no way to select individual updates you want to download. All updates — from security updates and Wi

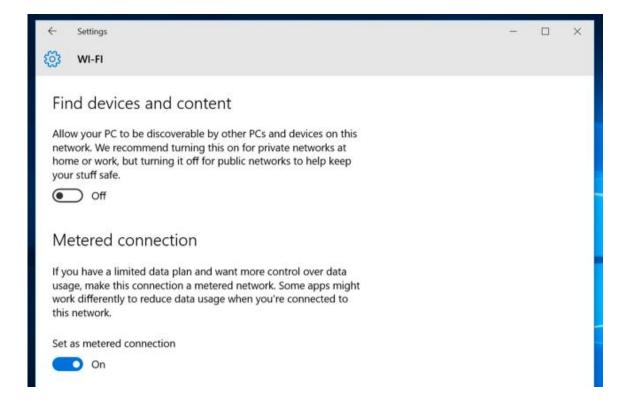
The only option you can control is to select the "Advanced options" link and uncheck "Give me updates for other Microsoft products when I update Windows." This will allow you to disable updates for Microsoft Office and other Microsoft programs.



Windows 10 Won't Download Updates on Metered Connections

Windows won't download updates on connections you mark as "<u>metered</u>." This ensures Windows won't waste valuable tethering data or other mobile data on updates that can wait until it reaches a solid, unrestricted Wi-Fi network. To prevent Windows from downloading updates on a specific connection, first connect to that WI-Fi network.

Next, open the WI-Fi settings panel and select "Network settings," or open the Settings app and select "Network & Internet." Scroll down in the list of Wi-Fi networks and select "Advanced options." Activate the "Set as metered connection" option here. This only affects the current WI-FI network you're connected to. Windows will remember the setting for this specific network in the future.



Professional Editions of Windows 10 Can Delay Feature Updates

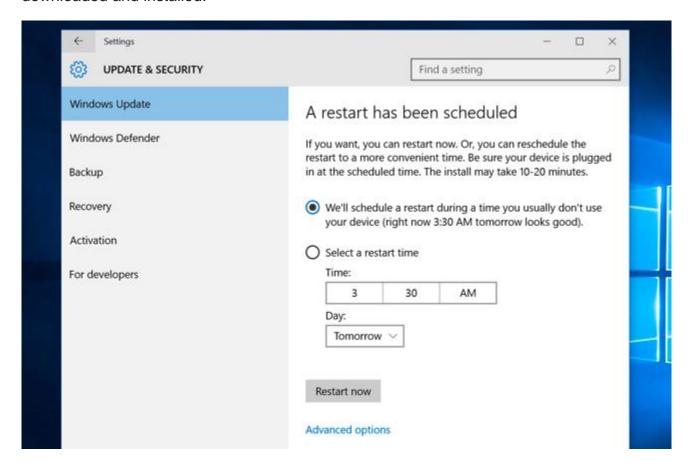
Home users can't delay upgrades at all, but <u>Professional editions of Windows 10</u> get a "Defer upgrades" option in the Advanced options interface. If you enable this, you'll still receive security updates automatically. Windows 10 will put off downloading feature updates for several months until they've had plenty of time to be tested on home PCs.

This is designed to make business PCs a bit more stable and allow system administrators to test new feature updates before they reach their users. If you upgrade to Windows 10 Professional, you could enable this option yourself. But, either way, you'll get those feature updates, it will just happen a few months later.

You Can Choose When to Reboot

Click the "Advanced options" link in the Windows Update interface and you'll only find two "Choose how updates are installed" options. You can pick "Automatic," which is the default and Windows will automatically download updates, install them, and schedule a reboot for a time when you aren't using your PC.

You can also choose "Notify to schedule restart," which will prevent your PC from automatically rebooting without your confirmation. But, either way, those updates will be automatically downloaded and installed.



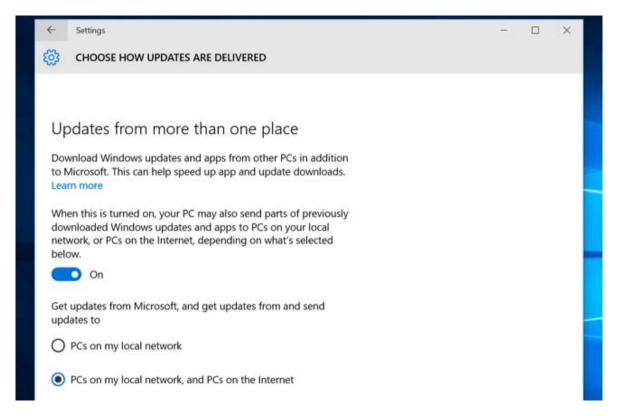
Peer-to-Peer Downloads for Updates are Enabled, Even Over the Internet

To speed up updating, Windows now uses peer-to-peer downloads for updates. For example, if you have several Windows PCs at home, you don't necessarily have to download the same update several times. Instead, the first PC to update would download it and the other PCs could download it from the first PC.

You can control whether peer-to-peer downloads are enabled from the "Choose how updates are delivered" link under "Advanced options" here.

By default, Windows 10 enables peer-to-peer downloads over the Internet as well, and your PC will use some of your upload bandwidth sending those Windows updates to other PCs. You can disable this by selecting only "PCs on my local network" here.

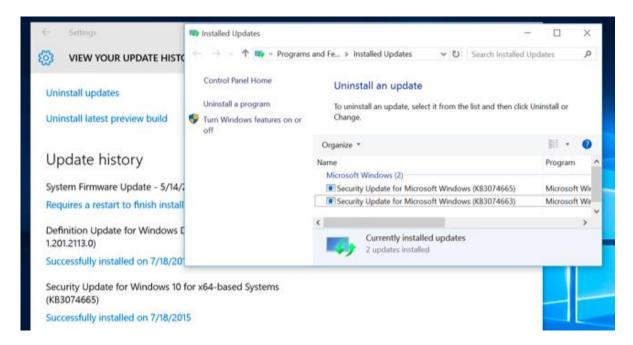
If you run Disk Cleanup and clean up the Windows Update files lying around on your PC to free up space, your PC won't be able to provide peer-to-peer downloads because the files won't be available.



You Can View Your Update History and Uninstall Updates

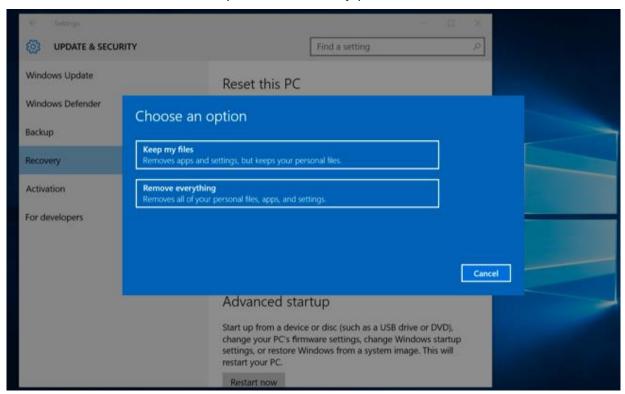
If there is a problem with your PC, you can uninstall problematic updates afterwards. To view your update history, open the Windows Update interface, select "Advanced options," and select "View your update history." You'll see a list of updates, and you can select "Uninstall updates" to view a list of updates you can uninstall.

Microsoft will probably continue rolling out major updates to Windows 10 in the form of "builds" that contain all previous updates. This means that you'll be unavailable to avoid updates forever, just as you'd have to accept an update when it appeared in a service pack on previous versions of Windows — assuming you wanted to upgrade to that service pack.



Windows Won't Have to Update Again After You Reset Your PC

When you use the <u>"PC Reset" feature found in Windows 10</u> to restore your PC, you won't have to re-download every single Windows update that's ever been released. Instead, the new PC Reset feature will give you a fresh, up-to-date Windows system. You won't need to spend hours updating and rebooting over and over, which is a huge improvement from Windows 8's Refresh and Reset features and the manufacturer-provided recovery partitions on Windows 10.



Microsoft also plans on making more use of the "build" system going forward. While small security updates will come as individual updates, major upgrades to Windows 10 that include new features will likely arrive as "builds." A Windows 10 PC can upgrade directly to a new build, which means that old cycle of downloading updates and rebooting four or five times to ensure you have all the old updates on an out-of-date PC won't be necessary

How to Stop Windows 10 From Uploading Updates to Other PCs Over the Internet



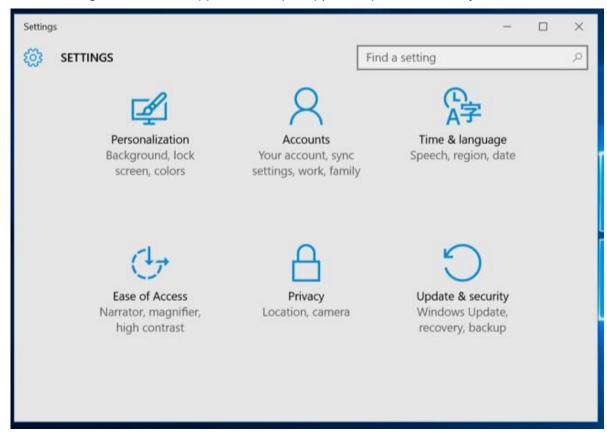
Windows 10 includes a new peer-to-peer download feature for updates and Windows Store apps. By default, Windows will automatically use your PC's Internet connection to upload updates, hiding the option to disable this five clicks deep in the operating system.

You can continue to use peer-to-peer updates on your local network, but you may not want to waste upload bandwidth to help reduce Microsoft's bandwidth bills. This is especially true if you have <u>data caps on your</u> Internet connection.

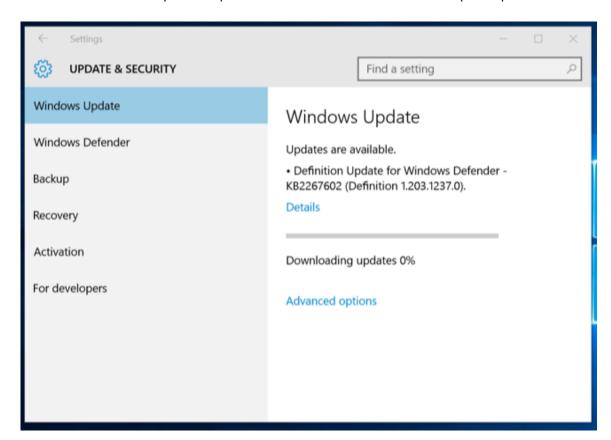
Disable the Uploads

You'll find this setting where all the <u>other Windows Update settings</u> now exist. Open it by clicking the Start button and selecting "Settings" at the bottom-left corner of the Start menu.

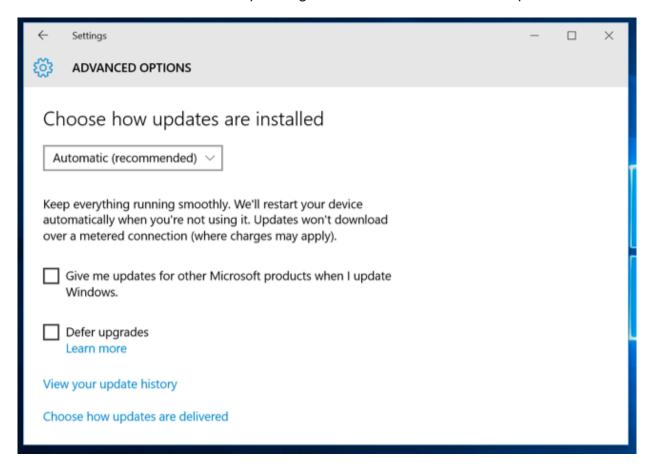
In the Settings window that appears click (or tap) the "Update & security" icon.



Click the "Advanced options" option at the bottom of the Windows Update pane.

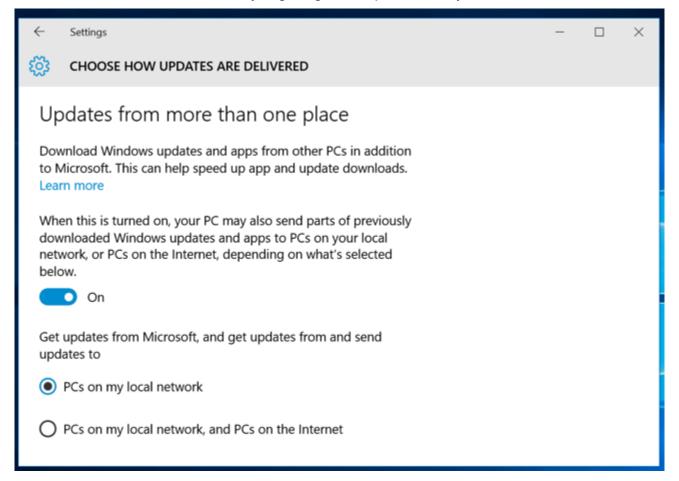


Scroll down to the bottom of this pane again and select "Choose how updates are delivered."



Select the option you prefer under "Updates from more than one place." We recommend just selecting "PCs on my local network" here.

- Off: This disables the peer-to-peer update feature entirely. Updates will only be downloaded from Microsoft's servers, and won't be uploaded to anywhere.
- PCs on my local network: This is the best option. With this enabled, you'll benefit from peer-to-peer updates on your home or work network. This means faster downloads and less download bandwidth used. You'll only have to download the updates once and they'll be shared amongst all your PCs. Your PC will never upload updates over the Internet.
- PCs on my local network, and PCs on the Internet: This option is the default, although it probably shouldn't be. With this enabled, Windows 10 will upload updates from your PC to other computers over the Internet. These computers would normally just download updates from Microsoft, but Microsoft will save on bandwidth because they're getting some updates from your Internet connection.

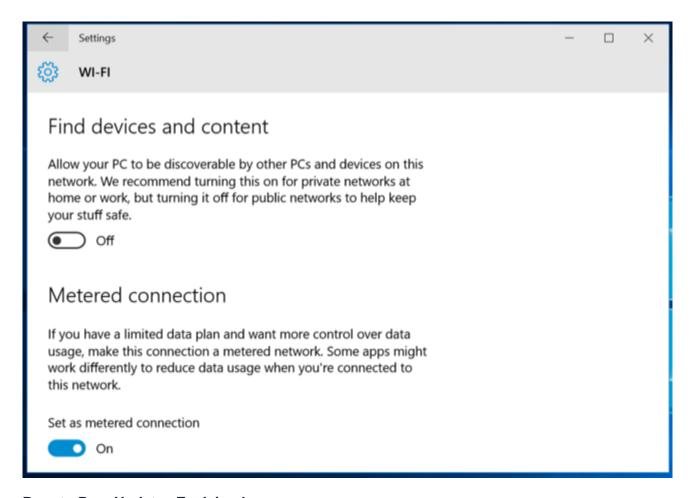


You Can Also Set Your Connection as Metered

You could also set your current Wi-Fi connection as "metered." When you set a connection as metered, you're telling Windows it's a connection with restricted data — such as a mobile data connection or <u>a Wi-FI hotspot from a smartphone you're tethered to</u>. Windows won't upload updates on a metered connection — it won't even automatically download Windows updates.

To set your current Wi-FI network as a metered connection, open the Settings app and navigate to Network & Internet > Wi-Fi > Advanced options. Activate the toggle under "Set as metered connection." The current Wi-Fi network will become a metered connection.

This isn't necessary if you've already disabled peer-to-peer updates in general. It will also prevent your Windows 10 PC from sharing updates with other computers on the same local network.



Peer-to-Peer Updates Explained

Peer-to-peer updates are actually a great feature — on your local network. Download the update once and all your computer can share it. Bandwidth on your local network should be plentiful. This actually saves you both time and reduces how much data you have to download, as you won't have to download the updates five times if you have five Windows 10 PCs at home.

Microsoft <u>acquired</u> Pando Networks back in 2013. Pando Networks was a peer-to-peer media distribution company, and used a modified form of BitTorrent to distribute data. It hasn't been confirmed, but Microsoftwatchers believe Windows 10's peer-to-peer downloads are based on this technology. As with <u>BitTorrent</u>, Microsoft states "the download is broken down into smaller parts" and "Windows uses the fastest, most reliable download source for each part of the file." In Bit Torrent parlance, Windows 10 is "seeding" updates on your PC's Internet connection with the default setting.

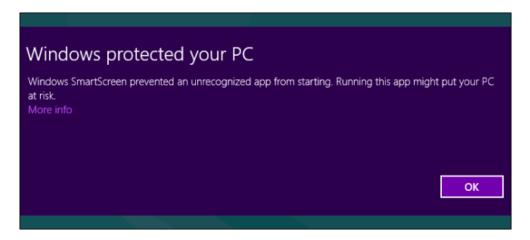
Windows 10 isn't the first software product to play this game. A variety of PC game companies, notably Blizzard Entertainment, distribute games and patches with a peer-to-peer downloader that uses Bit Torrent in the background to speed up downloads, sharing your Internet connection with other people downloading. However, these are generally more conspicuous, it isn't a hidden feature enabled in the background that's always running.

If Microsoft servers are being slammed, the distributed nature of the updates can ensure they reach more people faster. This will also help Microsoft save on bandwidth bills, as they're passing on some of the upload bandwidth they'd need to pay for to their customers' Internet connections.

According to Microsoft, this feature is named "Windows Update Delivery Optimization." Microsoft says it also uses your computer's Internet connection to upload universal apps you've downloaded to other PCs over the Internet, so it isn't just about Windows updates. This isn't made clear in the Settings app itself, but only on Microsoft's website.

For more information, consult the official Windows Update Delivery Optimization FAQ on Microsoft's website.

How the SmartScreen Filter Works in Windows 10



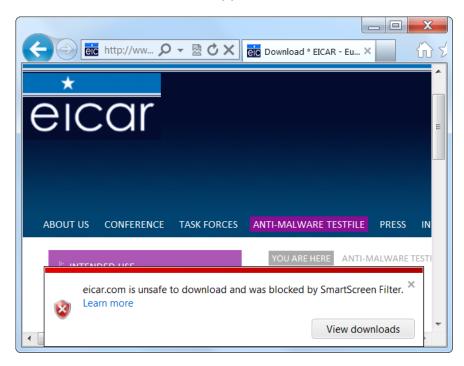
Windows 8 includes a SmartScreen filter that prevents unknown/malicious programs from running. SmartScreen is part of Internet Explorer 9 and 11 and is now integrated into the operating system. SmartScreen is a useful security feature that will help prevent bad applications from running, but it may occasionally prevent a legitimate application from running. SmartScreen reports some information to Microsoft, so it may have some privacy implications.

How SmartScreen Works

By default, Windows 10 sends information about every application you download and install to Microsoft. Microsoft's servers make an assessment of the application. If the application is legitimate and fairly popular, such as Mozilla Firefox or iTunes, Windows 10 will run the application.

If SmartScreen doesn't know about an application, whether it's malware or just a program that few people use, Windows 10 will prevent the application from running. It also prevents known-bad programs from running.

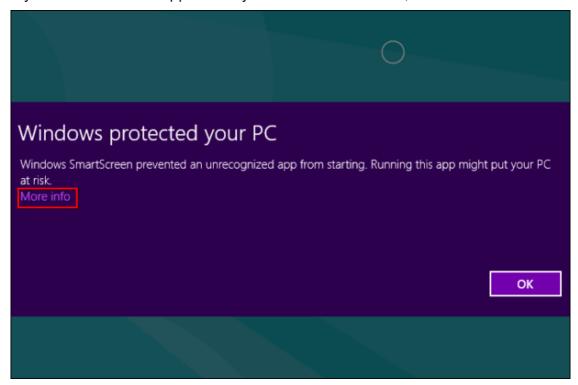
When you download an application, Internet Explorer's SmartScreen filter contacts Microsoft to determine whether the download should be allowed. With Windows 10, this is now integrated into Windows itself. If you download an application with another browser, such as Firefox or Chrome, SmartScreen will check the application.



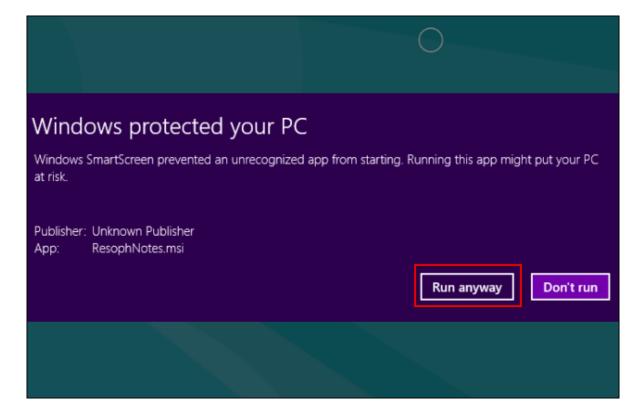
Running an Unrecognized Application

When you try to launch an application SmartScreen doesn't recognize, it will display a message saying it "protected your PC" by preventing the application from running. It's good to be cautious if you encounter this message. However, some legitimate applications may be considered unrecognized.

If you're sure that an application you want to use is safe, click the More info link.



Click Run anyway and Windows will allow the application to run, bypassing the SmartScreen filter.

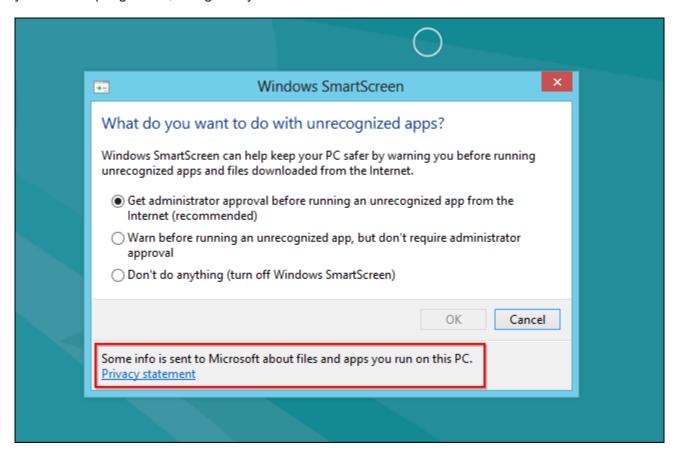


Privacy Concerns

Because SmartScreen reports information about each application you run to Microsoft to check whether the application should be run or not, it's been singled out in the media as a potential privacy problem.

SmartScreen sends several pieces of data to Microsoft when you run a program. The information includes the file name of the application you attempt to run, along with a hash of the application's contents. This hash is compared to Microsoft's database. If it matches a known good application, such as iTunes, it's allowed to run. (For more information about the exact data sent to Microsoft, read this post on the Within Windows blog.)

When you attempt to run an application on Windows 10, Microsoft will know the file name of the application you're attempting to run, along with your IP address.



However, Microsoft has <u>responded to these concerns</u>, saying they're not building a database of programs linked to specific users:

"We can confirm that we are not building a historical database of program and user IP data. Like all online services, IP addresses are necessary to connect to our service, but we periodically delete them from our logs. As our privacy statements indicate, we take steps to protect our users' privacy on the backend. We don't use this data to identify, contact or target advertising to our users and we don't share it with third parties."

SmartScreen is a useful security feature that can help prevent less-experienced users from running applications they shouldn't run. However, you can disable the SmartScreen filter if you don't want to use it

30 Ways Your Windows 10 Computer Phones Home to Microsoft

Windows 10 phones home more than any other version of Windows before it. Along with Windows 10, Microsoft released a new privacy policy and services agreement containing <u>45 pages of legalese</u>. If Google wrote these, Microsoft might say you were being "Scroogled."

Like it or not, Microsoft isn't alone here. What Windows 10 is doing has become common and normal across the web, Android, iOS, and other modern platforms. Microsoft is hoovering up all the data it can get to better target ads, personalize the operating system, and improve its software and services.

Editor's Note: almost everything is sending back data to somewhere for instance, if you are using Chrome, everything you search for is sent back to Google. Ad networks are tracking you on every website (including this one). Facebook and Amazon have ad systems that border on creepy. We're not necessarily condemning Microsoft with this article, but with all the recent interest in privacy and Windows 10, we decided to build a list of all the things being sent back in Windows 10 and let you decide what you think.

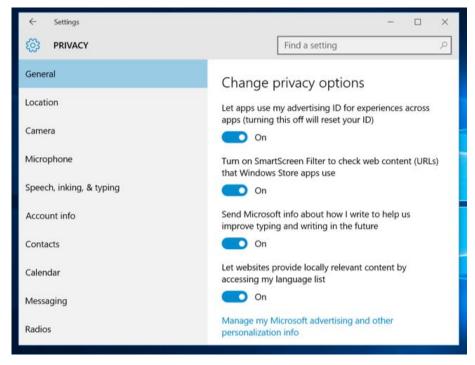
You can actually change many of these options right after the installation process if you <u>select "Customize settings" instead of "Use express settings."</u> However, most people will probably click right through and use the express settings. This activates a lot of features that share data with Microsoft.

You'll find a lot of these features <u>under Privacy in the new Settings app</u>. (Click the Start button, click Settings, and select Privacy.) Some of the options here simply control which apps have access to different data — for example, which apps can control your webcam. Others allow you to set system-wide privacy options.

Under General, you'll find:

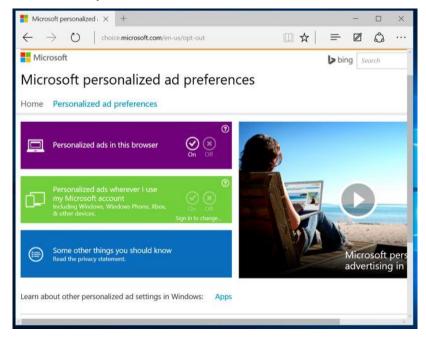
- 1. Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)

 This enables a unique advertising ID that you can be tracked with across different "Windows Store", or universal, apps. Microsoft can track your use of apps and show you targeted ads across different apps.
- 2. Turn on the SmartScreen Filter to check web content (URLs) that Windows Store apps use This enables the SmartScreen filter in universal apps. As we point out below, it's also enabled in File Explorer itself, Microsoft Edge, and Internet Explorer with different settings.
- 3. Send Microsoft info about how I write to help us improve typing and writing in the future This is related to the "Speech, inking, & typing" settings below. With it enabled, information about how you type and write is sent to Microsoft's servers.
- 4. Let websites provide locally relevant content by accessing my language list
 Websites you access can see the languages you have installed on your system and choose to serve you
 in your preferred language with this option enabled.



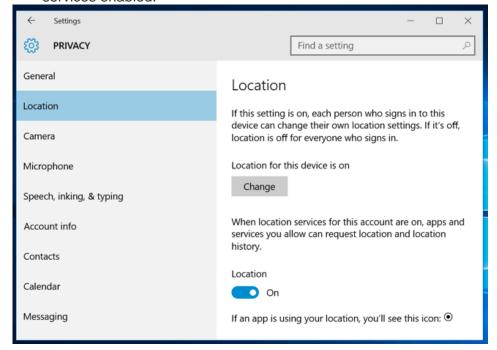
You'll see a "Manage my Microsoft advertising and other personalization info" link at the bottom here. Click it, and then click over to "Personalized ad preferences" on the web page that appears. You can also access this page at https://choice.microsoft.com/en-us/opt-out.

- **5. Personalized ads in this browser** This option is specific to each individual browser you use, and controls whether Microsoft will show you personalized ads in that browser.
- **6. Personalized ads wherever I use my Microsoft account** This option is tied to your Microsoft account and controls whether you see personalized ads on Windows, Windows Phone, Xbox, and other devices you use a Microsoft account on.



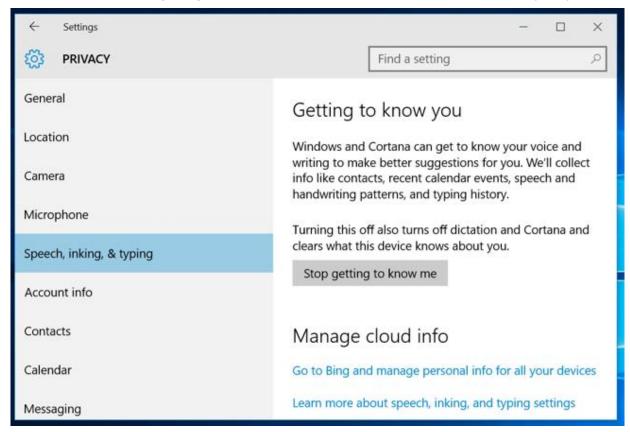
The Location screen activates location services. This isn't mentioned on the Location Settings window itself, but the custom setup screen states this will also "send Microsoft and trusted partners some location data to improve location services."

• 7. Location and location history – Your location is shared with individual apps that you choose to share it with. Location history is also available to apps, and stored only on your local device and just for 24 hours. But apparently some data is shared with Microsoft and its trusted partners if you have location services enabled.

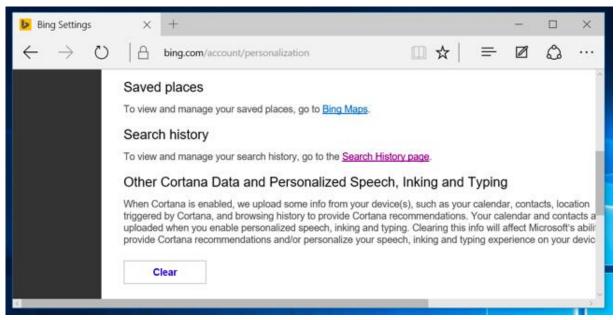


The "Speech, inking, & typing" section covers a surprising amount of data:

• **8. Speech, inking, & typing** – Windows and Cortana can "get to know you" by logging your voice, writing, contacts, calendar events, speech and handwriting pattern, and typing history. You can tell Windows to "Stop getting to know me" from here. This clears data stored only on your Windows device.

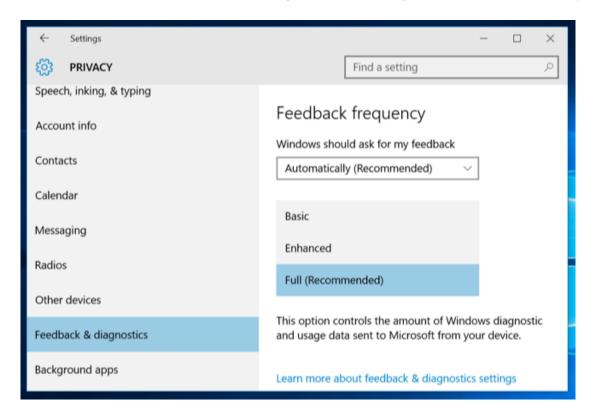


9. Speech, inking, & typing in the cloud – Click the "Go to Bing and manage personal info for all your devices" option to clear personalization data stored on Microsoft's servers tied to your Microsoft account. This link takes you to the https://bing.com/account/personalization page. Use the "Clear" button under "Other Cortana Data and Personalized Speech, Inking and Typing" section to clear this data.



The "Feedback & diagnostics" setting has a surprising option. What's especially surprising is Windows 10 won't actually let you disable this option.

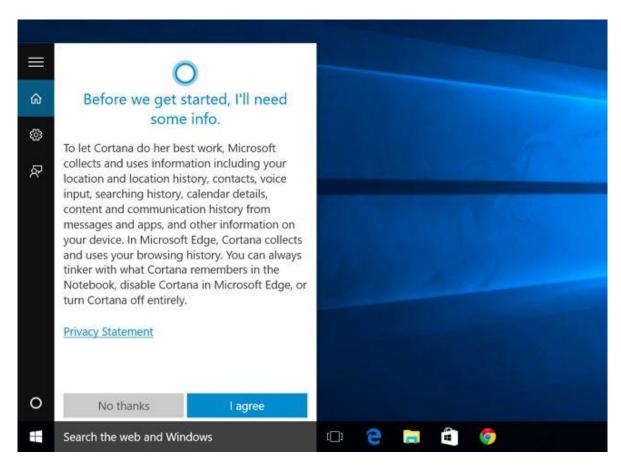
• 10. Diagnostic and usage data – By default, Windows 10 will send "Full" diagnostic and usage data to Microsoft. This seems to be Microsoft's new telemetry system codenamed "Asimov." You can select only Enhanced or Basic diagnostic and usage data. You can only disable this on Enterprise editions of Windows, and that requires changing the "Allow Telemetry" option in the group policy editor. This change doesn't even work on Professional edition of Windows. Yes, you can set the option to "0" which would normally disable it, but the Group Policy editor states that the "0" setting is ignored except on Enterprise versions of Windows. Instead, setting the option to "0" just sends "Basic" telemetry data.



Cortana and Bing Search

Obviously, when you use Microsoft's built-in Cortana assistant, Cortana requires a lot of your information to function.

- 11. Cortana As you can see when you enable <u>Cortana</u>, Cortana will collect and use "location and location history, contacts, voice input, searching history, calendar details, content and communication history from messages and apps, and other information on your device." Cortana also captures your browsing history from the Microsoft Edge web browser. Cortana as a whole requires sharing a lot of data with Microsoft, just as Google Now and Siri do with Google and Apple.
- 12. Bing Search in the Start Menu Even if you've disabled Cortana, searches you make in the new Start menu will also return <u>search suggestions from Bing</u> and the Windows Store. This means Microsoft sends your Start menu search queries to their servers unless you disable the Bing integration.



Device Encryption and Your BitLocker Recovery key

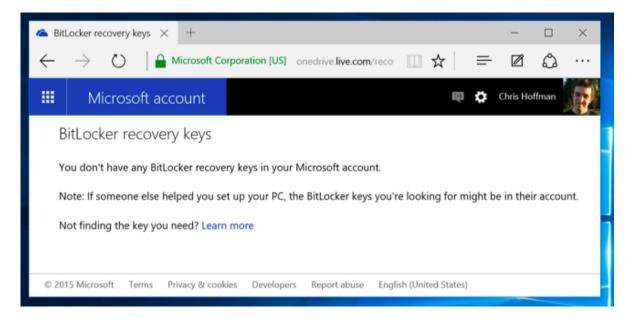
Here's Why Windows 8.1's Encryption Doesn't Seem to Scare the FBI

The FBI isn't happy about the latest versions of iOS and Android using encryption by default. FBI director James Comey... [Read Article]

This part carries forward from Windows 8.1. If you buy a new device and it has the required hardware as most new Windows 8.1 and 10 devices do <u>it's automatically encrypted with BitLocker-like encryption known</u> as "device encryption."

• 13. Device encryption's BitLocker recovery key — This actually only automatically happens if you use a Microsoft account. And, if you do, it will upload your encryption recovery key to Microsoft's servers. This means that you can get access if you ever lose it, but it also means that Microsoft or anyone who can get the key from Microsoft — such as a government — can decrypt your encrypted files. Of course, this is still an upgrade over the previous situation where all Windows Home devices were unencrypted. In that case, anyone could read their data.

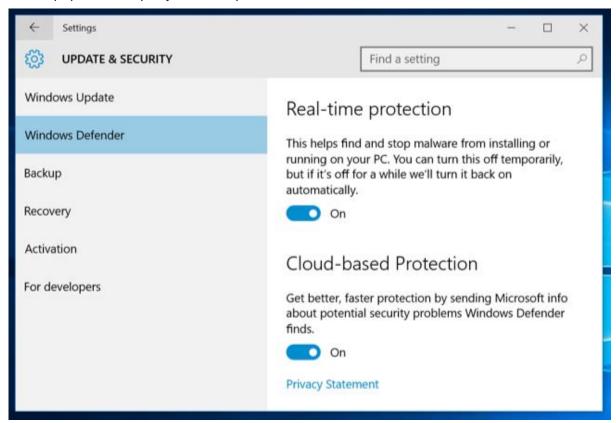
You can avoid this by not logging in with a Microsoft account, but then your device won't be encrypted at all. If you'd rather not do this, you can upgrade to a Professional edition of Windows and use the standard BitLocker feature. BitLocker will ask if you want to store your recovery key with Microsoft for safekeeping, but that's optional. You can find these keys at https://onedrive.live.com/recoverykey.



Windows Defender

Windows 10 includes the Windows Defender antivirus, and it's enabled right out of the box. This is the successor to the Microsoft Security Essentials antivirus that was available for free on Windows 7. Settings for this are available under Update & security > Windows Defender in the Settings app. Windows Defender will automatically enable real-time protection. Even if you turn it off, it's only temporary it will turn that real-time antivirus protection back on later. The only real way to turn it off is to install a third-party antivirus. Windows Defender won't run if another antivirus is running.

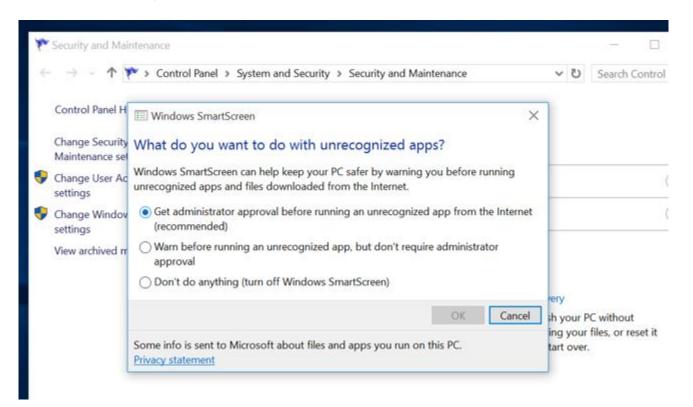
- **14. Cloud-based Protection** Cloud-based antivirus protection "sends Microsoft info about potential security problems Windows Defender finds."
- **15. Sample submission** This helps improve Windows Defender's protection "by sending MIcrosoft malware samples" that Windows Defender finds. Both of these features are similar to the features found in popular third-party antivirus products, and can be disabled.



SmartScreen Application-Checking

Windows 10 also includes the SmartScreen filter introduced in Windows 8. When you run an application downloaded from the Internet, SmartScreen checks in with Microsoft's servers to check that application's reputation. If it's a known-good application, Windows 10 will run it normally. If it's a known-bad application, Windows 10 will warn you and get your permission before running it.

• 16. Windows SmartScreen in File Explorer – These settings can be controlled from the old Control Panel. To access them, open the Start menu, type "smartscreen", and click "Change SmartScreen settings." This will take you to the System and Security > Security and Maintenance window in the Control Panel. Click the "Change Windows SmartScreen settings" link and you'll be able to disable SmartScreen, if you like.

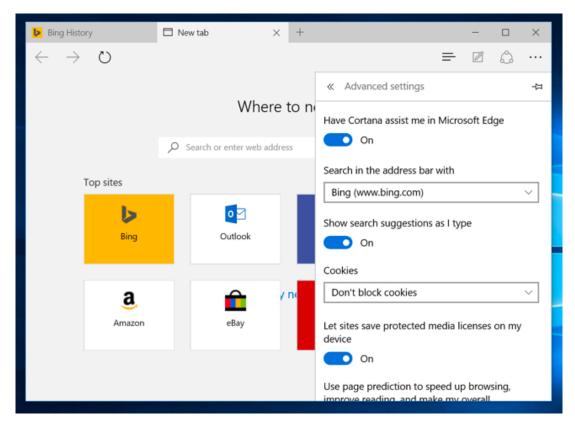


Microsoft Edge

SmartScreen and Cortana are also part of <u>Microsoft Edge</u>, Windows 10's new web browser. You'll find the privacy related options under the menu in Edge — select Settings and then select "View advanced settings."

- 17. Have Cortana assist me in Microsoft Edge When Cortana is enabled in Microsoft Edge, Cortana will track your browsing history and other information, saving it.
- **18. Show search suggestions as I type** When you start typing in the address bar, your typing will be sent to your search engine Bing unless you <u>change the search engine</u> and it will return search suggestions. This means Bing will see your typing even if you're typing a web address directly. All modern browsers, aside from Firefox with its separate address bar and search box, work this way.
- 19. Help protect me from malicious sites and downloads with the SmartScreen filter Like Google Safe Browsing in Chrome and Firefox, Edge uses a filter to help block dangerous sites.

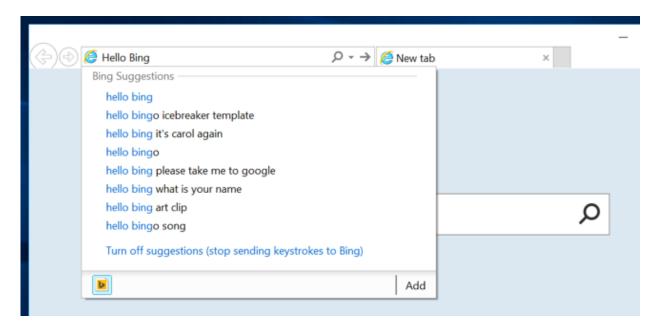
If you choose to save other types of data in Edge, it will be synced online with your Microsoft account.



Internet Explorer

Internet Explorer is still around, although it's not the default browser.

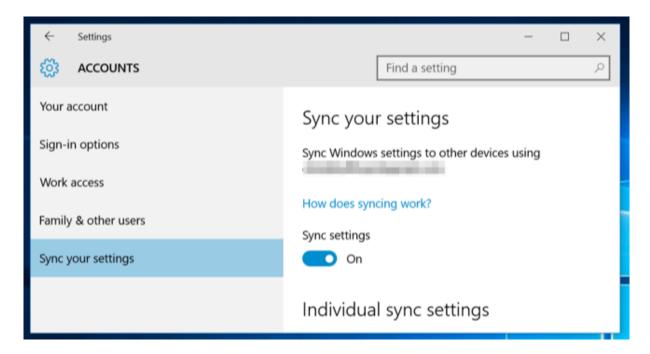
- **20. SmartScreen** Internet Explorer also uses SmartScreen, and this can be controlled by clicking the gear menu, pointing to Safety, and selecting Turn off SmartScreen filter.
- 21. Enable Suggested Sites This is an older feature and isn't enabled by default. It is still offered under the Advanced list of settings under Internet Options window. This little known feature of Internet Explorer has been around awhile, and it uploads your browsing history to Microsoft if you enable it.
- **22. Bing Suggestions** As in Edge, anything you type in the address bar is sent to Microsoft's Bing search engine to provide you with search suggestions unless you change search engines or click "Turn off suggestions (stop sending keystrokes to Bing)" after typing in the address bar.



Microsoft Account and Sync

Windows 10 recommends you sign in with a Microsoft account, just like Windows 8. This allows you to log in with the same account you use for other Microsoft services like Outlook.com, Office 365, OneDrive, Skype, MSN, and other services. This also enables a lot of online features in Windows 10, like access to the Windows Store and many included apps that require a Microsoft account, OneDrive file access in File Explorer, and various sync features. You can choose to use a local user account if you prefer.

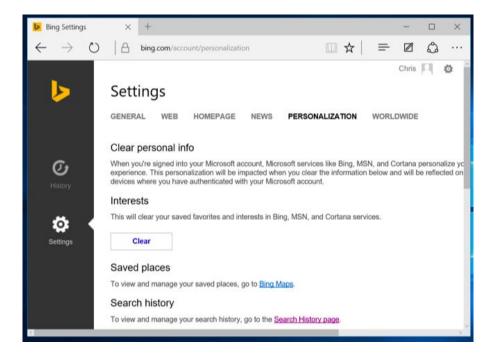
- 23. Sync settings A variety of Windows settings such as your saved passwords and web browser data are synced by default if you sign in with a Microsoft account. These options are available under Settings > Accounts > Sync your settings.
- **24. Devices you've logged in from** Microsoft will keep track of devices you've logged into with your Microsoft account. You can view this list at https://account.microsoft.com/devices.



Personal history and interests

Microsoft tells you: "When you're signed into your Microsoft account, Microsoft services like Bing, MSN, and Cortana personalize your experience."

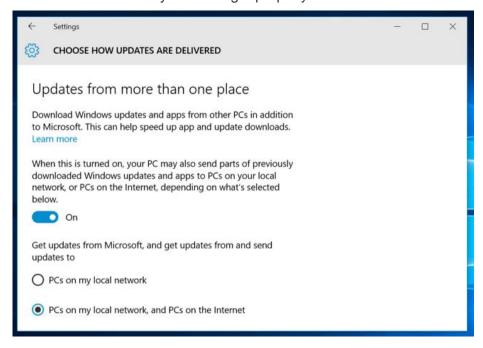
- **25. Personal history and interests** You can clear personal info and "interests" in Bing, MSN, and Cortana from the https://bing.com/account/personalization page.
- **26. Bing search history** Search using Windows 10's Start menu and the Bing search in Edge and you'll build up a Bing search history tied to your Microsoft account. You can view and clear this history from https://bing.com/profile/history.



Windows Update, Store, and Activation

<u>Windows Update</u> uses your upload bandwidth by default to upload Windows Updates to other users. These settings can be controlled under Settings > Update & security > Windows Update > Advanced options > Choose how updates are delivered. You can make Windows only share updates with PCs on your local network, not the entire Internet.

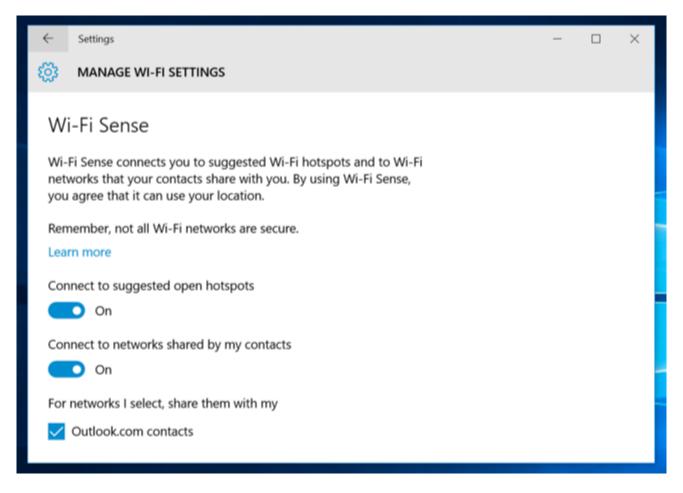
- 27. Windows Update Windows 10 Home requires that you install security, driver, and feature updates automatically, and you can only <u>prevent Windows 10 from automatically downloading updates</u> by setting your device's connection as a metered connection or upgrading to Windows 10 Pro. Thankfully, there is at least a way to block updates you don't want.
- 28. Windows Store The Windows Store will automatically check in with Microsoft and download new versions of included universal apps like Microsoft Edge. Even Cortana and the Start menu can be updated via the Windows Store.
- **29. Windows Activation** Windows still includes <u>Windows Activation</u>, which checks in with Microsoft's servers to ensure you're using a properly licensed and activated version of Windows.



Wi-Fi Sense

<u>The Wi-Fi sense feature</u> is enabled by default, and it will automatically connect to suggested open hotspots and networks your Outlook.com, Skype, and Facebook contacts have shared with you.

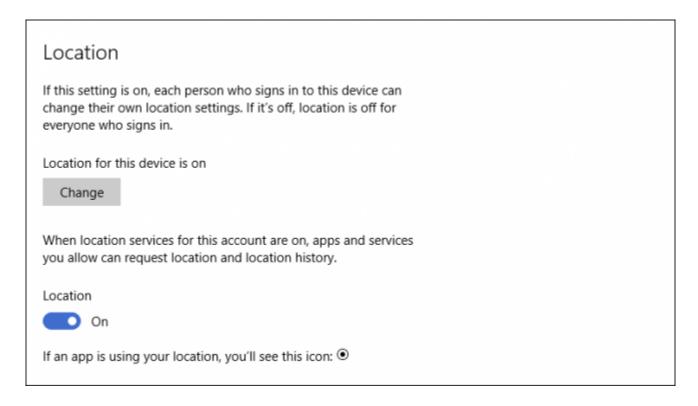
• 30. Wi-Fi Sense – These options can be controlled under Settings > Wi-Fi > Manage Wi-Fi settings. Note that Windows 10 won't actually share your Wi-Fi network's passphrase with anyone else unless you choose to manually share that individual network. However, if you give a friend access to your passphrase and they connect and click the Share option, they could share it with their entire network of Facebook, Skype, and Outlook.com email contacts and give them access to your Wi-Fi network.



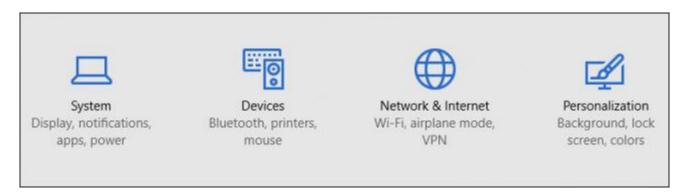
This is just a conservative list, and probably isn't complete. There are many other ways Windows 10 arguably phones home. Windows 10 includes apps for a variety of Microsoft services: Cortana, Bing, Outlook.com, OneDrive, Groove Music, MSN, and Xbox. Each of these services may have its own privacy policy and store data about you in a different place if you use them.

And, again, this isn't unusual in this day and age. Whether you love it or hate it — actually, it's more like you're indifferent to it or hate it — many operating systems and services now function this way. What's new here is Windows is jumping on board. Many of these features were already present in Windows 8/1, too.

But Microsoft could certainly do a better job of putting these options in a single place and better explaining them, though. They're scattered not just across Windows 10's interface, but across a variety of different Microsoft websites.



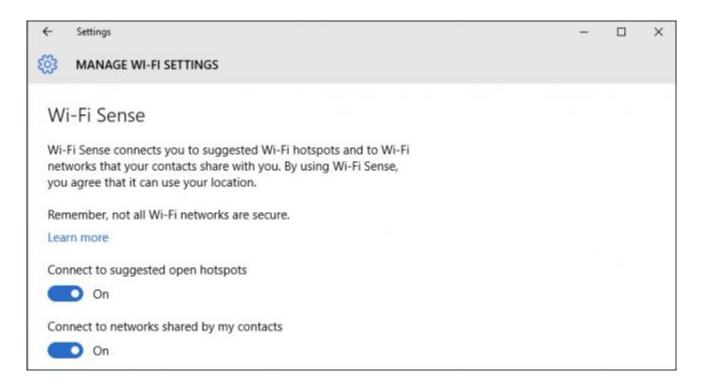
Those connectivity settings can be adjusted later by opening the "Network & Internet" settings.



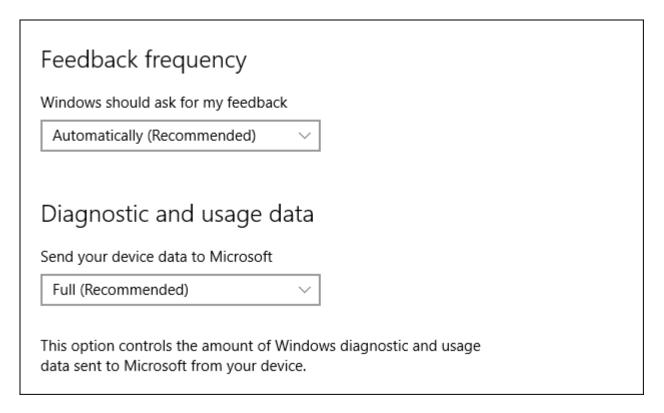
Tap or click "Wi-Fi" and then (if necessary) scroll down to "Manage Wi-Fi settings".



Tap or click "Off" the two options shown in the screenshot.



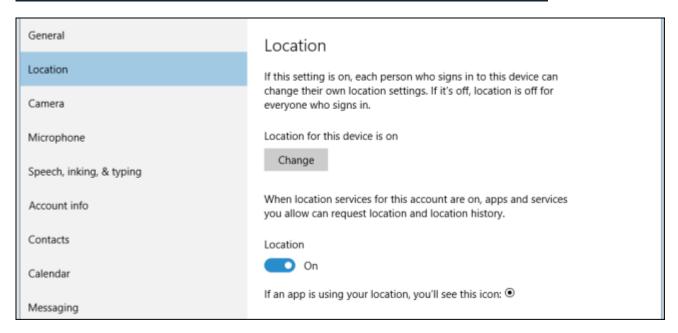
Finally, there's one more spot in the privacy settings called "Feedback & diagnostics" where you can adjust the final option in the customized setup.



With that, you will have undone anything turned on in the express setup. We urge you to pay careful attention to other things in the privacy settings, and we'll pay a closer look at those in an upcoming article.

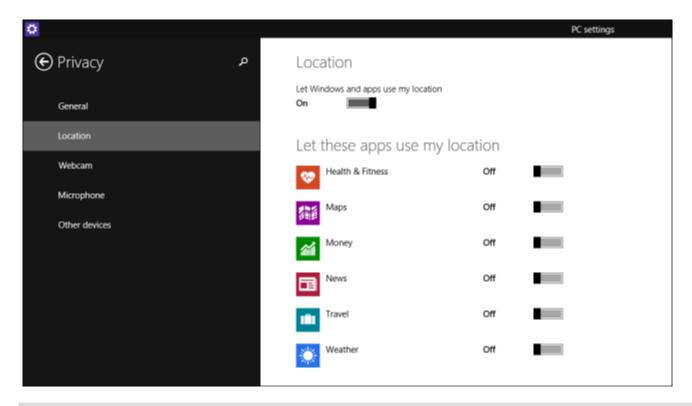
If you're just now setting up Windows 10 on your computer, do yourself a favor and take a few minutes to go through the customized install. Chances are fairly good you're going to want to turn off at least a couple of the items found in it.

How to Disable or Configure Location Tracking in Windows 10



Windows 10 includes a whole bunch of new privacy settings, all are important in their own right, but perhaps none so much as the location settings. If you're privacy-conscious, you will definitely want to investigate them further.

As a whole Windows 10's privacy settings, at least in the most current build, are a lot more extensive and comprehensive than its Windows 8.1 counterpart.



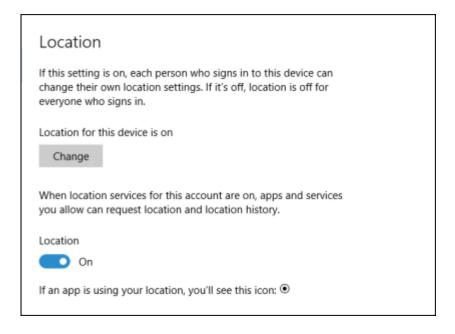
Windows 8.1's Privacy settings are fairly lacking. There's some basic stuff here but nothing like we should expect to find on a modern operating system.

One of the most important aspects of any set of privacy options will be the location items, because those are going to tie you and your device to a place, revealing where you are and where you have been. Luckily, Windows 10 includes a better set of location-oriented privacy settings, which we want to discuss in greater detail today.

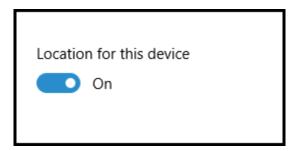
Disabling Location Globally or Individually

The first and most important difference between Windows 8.1 and Windows 10 is that in the latter, you can now disable location either globally, so it is disabled for all user accounts on that device, or individually, meaning each user can set their own location settings.

First, open up the Settings in Windows 10 and click on the Privacy group. To turn off location just for that account, you can click the button under "Location" to "Off".



If you want to turn off location for the entire device, however, you want to click the "Change" button, which will then open a new window so you can turn off the "Location for this device".

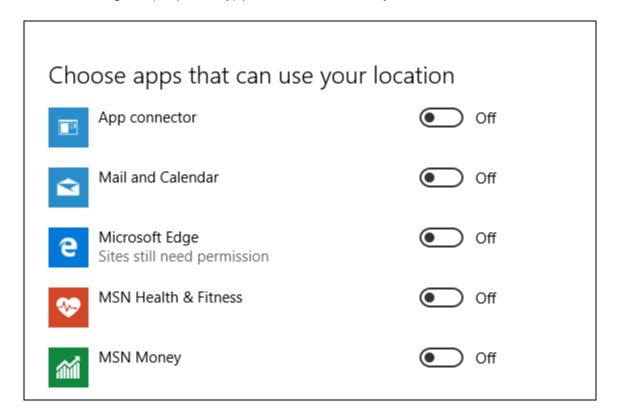


If you decide to leave location on, then there are further options you need to check out. First of all there's your "Location history". History is stored for a "limited time" for the need of certain apps and services that rely upon it.

To clear the history on your device, simply click the appropriate button.

Location history When location is on, the locations obtained to meet the needs of your apps and services will be stored for a limited time on the device. Apps that have access to these stored locations will appear below. Clear history on this device Clear Learn more about location settings Privacy Statement

Below the clear history option are the apps that actually poll your location when you use them. This is no different than on Windows 8.1, and you simply need to go through and click "Off" or "On" any apps you want to disallow or grant (respectively) permission to access your location.



Finally, there's a new "Geofencing" option. If you don't know what geofencing is, you're in luck because <u>we have a great article that explains it</u>.

On Windows 10, if you have an app that is using your location for geofencing, it will show up under the heading. You can then prevent apps from using your location for geofencing by turning them off.

Geofencing

A geofence is a boundary around a place of interest, and apps can use your location to see if you're crossing in and out of one. To stop apps from using your location for geofencing, turn off location for those apps.

None of your apps are currently using geofencing.

So that's it for Windows 10's location settings. Microsoft has obviously given it more time and thought than in Windows 8.1.

It's important to note and understand, however, these location settings will only apply to apps appearing in the "Choose apps that can use your location" list and any other apps, whether a browser or other desktop program, may still be able to pinpoint your location using your IP address and other basic information. In those cases, you will need to adjust each app's privacy settings accordingly.

HTG Explains: What Geofencing Is (and Why You Should Be Using It)

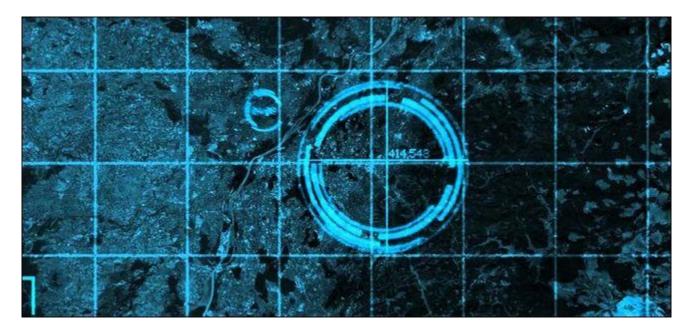


The term is popping up more frequently in news articles, appearing in product manuals, and highlighted as a feature in tons of mobile applications, but what exactly is geofencing? Read on as we explain what it is, why it's appearing in more productions and applications, and how you can benefit from using it.

What Is Geofencing?

Geofencing is the use of the Global Positioning System (GPS) satellite network and/or local radio-frequency identifiers (such as Wi-Fi nodes or Bluetooth beacons) to create virtual boundaries around a location. The geofence is then paired with a hardware/software application that responds to the boundary in some fashion as dictated by the parameters of the program.

While geofence-based hardware and software solutions have been around for decades, the early systems were limited largely to those willing to invest in expensive custom hardware for specific use cases. One of the early commercial uses of geofencing was in the livestock industry wherein a handful of cattle in a herd would be equipped with GPS units and if the herd moved outside of geographic boundaries (the geofence) set by the rancher then the rancher would receive an alert. Similar systems were deployed to safeguard and monitor company vehicle fleets wherein if a company vehicle left the zone it was assigned to managers at the company would be notified.



That's all very interesting but as someone not running a cattle farm or a delivery fleet you're probably asking yourself "How does this apply to me? Your title said I should be using geofencing!" So how *does* it apply to you?

The widespread adoption of smartphones has put a GPS/Wi-Fi/Bluetooth radio in the pockets of millions of consumers and ushered in an age of incredibly cheap and ubiquitous geolocation markers that has pushed geofencing from an expensive commercial practice into the realm of consumer application. What used to be a very costly tool for very specific applications is now free for developers to include in their software as the consumer already has the necessary hardware. As a result geofencing capabilities are popping up in everything from shopping lists to smart home control packages.

In other words, there's a whole world of geofencing potential around you worth tapping into. Your smartphone is capable of reminding you to pick up the dry cleaning when you're near the dry cleaners, of turning down the thermostat when you drive away from your house, and all other manner of handy location-based tricks.

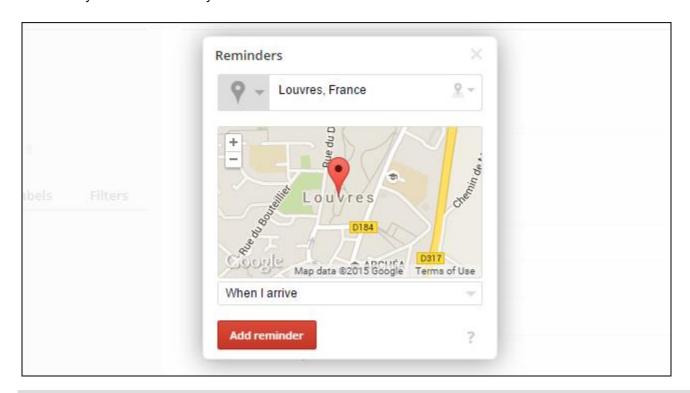
Now that we have a clearer picture of what geofencing is, let's take a look at real-world applications you can start using today.

Geofencing in Application

Geofencing has crept into a wide range of applications over the last few years and has improved everything from to-do lists to household management. The following examples are merely that, examples culled from a wide range of available applications intended to highlight the diverse ways in which application developers are using geofencing. If you have a favorite app we've failed to mention here, by all means jump into the comments at the bottom and share the app.

Productivity

One of the most frustrating things, in regard to productivity and getting stuff done, is remembering you need to do something when you're not in the right place to do it. If the dry cleaner is on the way home from work then it's useful to have the process of leaving work trigger a reminder to get the dry cleaning. If you need files off a certain computer at work then it's useful to have the reminder trigger when you arrive at work the next day. You keep forgetting to buy that adapter at the hardware store? Set a location-based reminder so the next time you're in the store you won't leave without it.



Stealing the Mona Lisa? Better set a geo-located reminder.

These kind of location-aware triggers and reminders are built into a large number of popular productivity apps. Cross-platform todo list app Todoist supports location-based reminders on both iOS and Android. Popular cross-platform service RememberTheMilk also supports location-based reminders. iPhone users who just need simple reminders without the complexity of a full task management system can also just attach a location to any item in the Reminders app.

Smarthome Control

Smarthome control is an area where geofencing really shines. After all what says "The future is now!" more than approaching your home and having the lights turn on as you walk towards the door?

That's not even a vaporware suggestion either as off-the-shelf products such as <u>the previously reviewed</u> <u>Philips Hue system</u> have smartphone-based geofencing built right in. You can instruct the Hue to turn your lights on and off as you come and go and/or even have them apply custom scenes to different areas of your house.

You can enjoy similar home/away detection with your heating and cooling thanks to <u>a handy iOS app</u>

<u>Skylark</u> that pairs with both Nest and Honeywell smart thermostats. Android users can use IFTTT scripts or the Nest component in <u>the Life360 app</u> to do the same.

Security

There are a bunch of clever applications for geofencing when it comes to mobile and computer security. Android 5.0, for example, <u>has a handy feature wherein you can disable device locking if you are within range of the "home" Wi-Fi node</u>: No more constantly unlocking your phone when you're just sitting around on your couch playing with it during commercial breaks.

You can also set up a miniature geofence around your computer that automatically locks your computer when your phone (and it's corresponding bluetooth radio) move away from the computer. We detail <a href="https://example.com/hore/blue-computer-blue-comp

Family Tracking

If you have a busy family that you want to keep tabs on (like getting an alert when your kid gets home from school and forgets to call you), there are handy geofence-based solutions like the aforementioned <u>Life360</u> <u>application</u>, available for both iOS and Android, that makes it dead simple to set up zones with corresponding notifications.



Apple's <u>Find My Friends</u> app for iOS 8.0+, seen above, offers similar functionality with the ability to check locations and set location-aware alerts.

Roll Your Own with IFTTT

<u>IFTTT</u> (IF This Then That) is a recipe system that allows you to create recipes like "If I'm leaving my office turn the air conditioner on at home" or "if I'm in the house after 9AM on a weekday text my boss that I'm stuck in traffic" or whatever other recipe you can cook up.

IFTTT supports native location tracking for both Android and iOS through the official IFTTT application. To see sample recipes that take advantage of the location tracking, check out the iOS location channel and the Android location channel.

While using IFTTT is certainly more complicated than, say, using the simple geofencing built right into the Hue smart bulb system it offers a huge degree of flexibility as nearly any of the tens of thousands of IFTTT recipes can be adapted to work with the location app on your phone.

The Future of Geofencing

Although still unfamiliar to many people geofencing is a natural extension of our desire for our devices to do more (and to do more automatically) and to decrease the friction with which interact with our environment.

As devices become increasingly sophisticated and more elements of our home, vehicles, and workplace enter the ever growing stable of "Internet of things" objects expect to see geofencing applied to more and more devices and environments.

This increased integration could yield all sorts of novelties like workstations that power down when their owners leave for the building, coffee pots that turn on in the morning when the first coffee drinkers arrive, attic fans that whirl to life to suck in cool evening air as you drive home, garage doors that open automatically as you round the bend, and all manner of little changes that leave the computers to worry about the trivial bits while we get to focus on things more interesting than wondering if we locked the back door properly.

Windows 10 is Great, Except for the Parts That Are Terrible



<u>Windows 10 is a great upgrade</u>. Microsoft paid a lot of attention to the feedback they ignored while developing Windows 8, and it shows. Unfortunately, some parts of Windows 10 are inexplicably bad and hostile to users.

While Windows 10 as a whole shows Microsoft listening to feedback, parts of it show the same old Microsoft that dug its feet in and announced products like the original Xbox One and Windows 8 without appearing to care about many users.

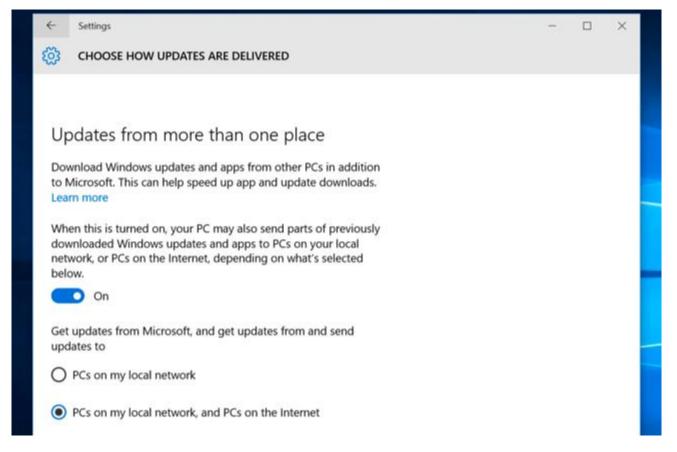
It Uses Your Upload Bandwidth without Even Telling You

By default, <u>Windows 10 automatically uploads Windows updates</u> and apps from the Windows Store to other PCs over the Internet. This is a great feature when restricted to the local network, but Microsoft opts everyone into the Internet part of it by default, using your upload bandwidth for something that doesn't help you.

Worse yet, there's no indication this is happening unless you read about it online, find your Internet connection slow, or get contacted by your Internet service provider because you're using up your limited upload bandwidth.

It could appear as an option in the custom setup process or a note about it could appear somewhere, but it doesn't — it just works in the background. You have to find a special option hidden five clicks deep in the operating system to disable it.

This potentially helps everyone download updates faster. it's basically like BitTorrent for Windows updates. But many people, especially outside the USA, have connections with upload data caps. Microsoft is saving some money on bandwidth bills by using customers' Internet connections, without telling them.



Few Options for Automatic Updates Hurt People on Limited Internet Connections

Windows 10 forces all home PCs to automatically download and install updates. That's good in one way, as it keeps home Windows systems secure.

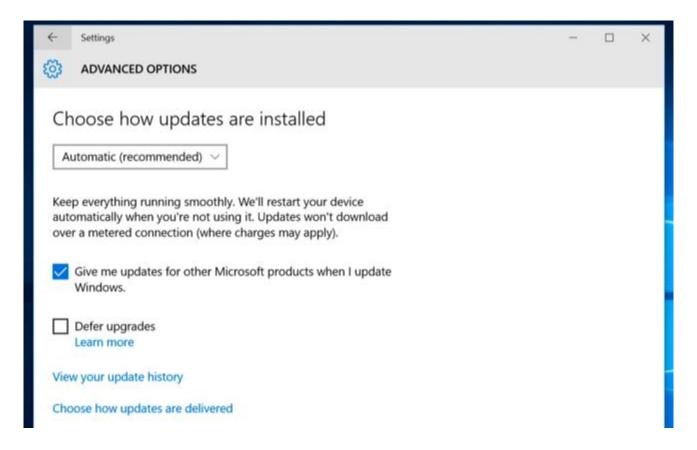
But there's a big problem with this: It's not implemented in a respectful way. You can only configure the time Windows reboots — not when it downloads updates.

Many people — again, especially outside the USA, but also in more remote or rural areas in the US — have Internet connections with bandwidth caps. They can't necessarily download hundreds of megabytes of updates every single week. Some people have unlimited bandwidth during certain hours only — perhaps during the middle of the night. Windows 10 provides no way to tell Windows to only download updates during these uncapped hours.

The one solution to this for home users is setting a connection as "metered." Microsoft says you should set every connection with a data cap as a metered connection. This will give you control over when you download updates.

There's just one big problem: Microsoft doesn't let you set a wired Ethernet connection as a metered connection. If your home Internet service provider has data caps and you're hooked up via a normal Ethernet connection, there's no way to <u>restrict those Windows Updates</u> without shelling out \$100 for the Professional edition of Windows 10.

This is reminiscent of the original Xbox One, which demanded a nearly always-on Internet connection. Microsoft just assumes all its users have broadband Internet connections without any data caps and doesn't seem to understand the connections many people have to deal with.



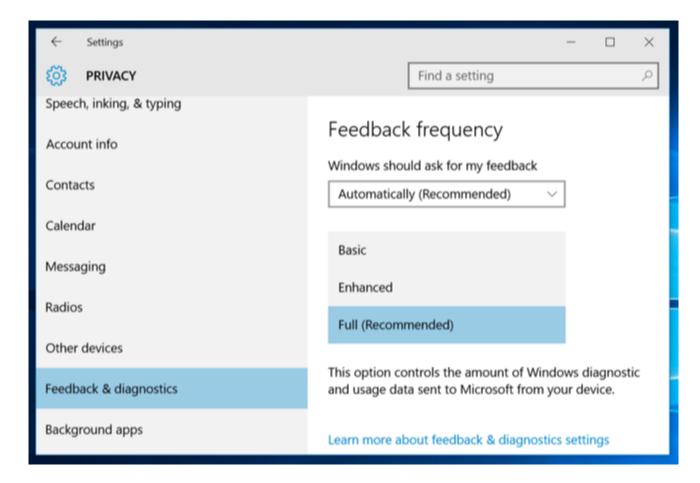
People Are Upset About Privacy, and Microsoft Isn't Communicating Well

Windows 10 is currently under a firestorm of controversy — even now being discussed in the mainstream media — over privacy concerns. Windows 10 is a big shift from Windows 7 and includes many more features that phone home to the mothership. Some of these can't even be disabled. For example, the telemetry feature can only be disabled entirely on Enterprise versions of Windows.

Microsoft should be explaining this a lot better and making it simpler to understand. We<u>categorized 30 different privacy settings located all across Windows 10's interface</u> and the web, some of which offered confusingly vague explanations. Had Microsoft arranged these options in a better way with more explanation, they at least could have dulled some of the criticism. We feel a lot of the criticism is overblown, but Microsoft isn't helping itself by remaining silent.

Worse yet, Microsoft is charging onwards despite criticism. Updates to Windows 7 and 8.1 <u>add the telemetry service from Windows 10</u>, making Windows users sticking with older versions of Windows for privacy reasons upset.

"By applying this service, you can add benefits from the latest version of Windows to systems that have not yet upgraded," says Microsoft's patch note. That's just a ridiculous explanation — Microsoft may be getting some benefit out of collecting telemetry data, but the average Windows 7 or 8 user isn't getting a "benefit from the latest version of Windows" after the telemetry service is installed.

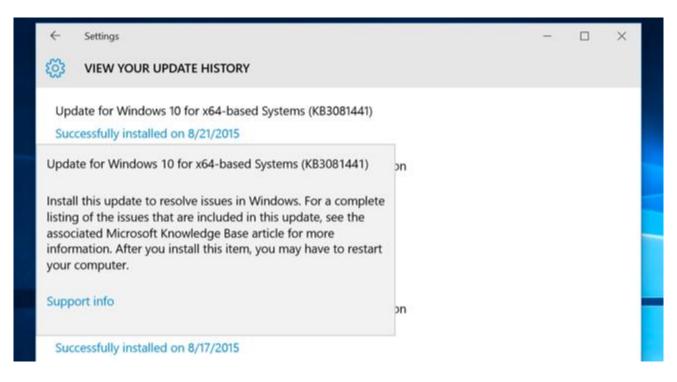


Microsoft Won't Give You Patch Notes; Deal With It

Microsoft is charging ahead with their vision of Windows as a service, planning to constantly update Windows 10 with new features going forward. Faced with all these constant updates, you — or businesses concerned about change — might want to see what these updates actually do.

But Microsoft <u>has no plans</u> to actually provide any patch notes so you can figure out what they're changing. Microsoft might occasionally provide information about big changes if they feel like it, but that's it. There are now reports that Microsoft may provide some patch notes to enterprises, but that would be it.

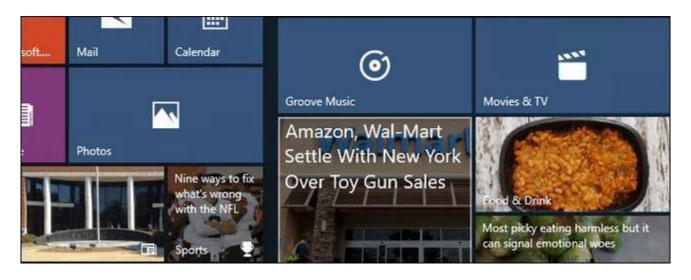
Microsoft is planning on updating Windows 10 on a continual basis with more than just security and bug fixes Microsoft will update Windows 10 with new features, changes, low-level modifications, and more. But Microsoft isn't willing to actually inform their customers what's changing.



The Start Menu is Flashy but is Missing Basic Functionality

After years of using Windows 8 and then 8.1, any Start menu at all seems like a huge upgrade. But Windows 10's Start menu actually isn't all that great when you compare it to Windows 7's. Microsoft added flashy live tiles and removed useful features. It may not work as well as it used to, but it does bombard you with information about hamburgers and Lady Gaga and football when you open it.

There's no way to pin apps you regularly use to the left side of the Start menu, for example. Worse yet, the Start menu now works in an entirely different way. It only supports 500 entries and will break after you add more than 500 shortcuts, just not displaying shortcuts to applications you've installed. They won't be accessible via the Start menu's search feature, either. That's just sloppy and shows Microsoft is more worried about making a flashy live tile Start menu than a tool that will actually be robust in the real world for the PC users who need it most.



Metro Apps Are Still Practically Unusable

Thom Holwerda from OSNews <u>writes</u> that Windows 10 is only well reviewed because it's free and because reviewers haven't forced themselves to use only those Metro apps, now called universal apps.

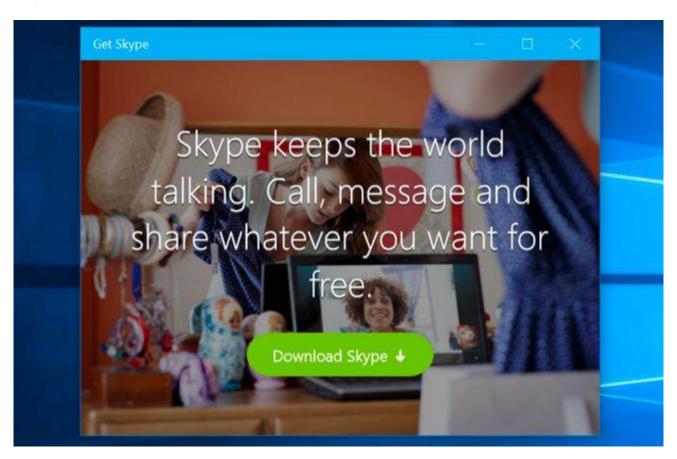
You'll still be mostly using desktop apps if you want a good experience on Windows 10. Even Microsoft themselves don't seem confident about universal apps. Microsoft unceremoniously killed the universal version of Skype a month before Windows 10 was out, they want you to use the desktop Skype app instead. The Metro versions of Office 2016 are all called "Mobile" versions to encourage you to not use them and get the traditional desktop apps instead.

Even apps that are seeing a lot of development aren't quite there yet. Microsoft Edge has a lot of issues, even when doing something as simple as dragging a tab out of a window.

Remember, Windows 8 came out in 2012. It's been three years, and those Metro/universal apps still aren't compelling. Really, Microsoft was working on the Metro platform for years before Windows 8 was released, so Microsoft's best and brightest have had 5-6 years to release some awesome apps and show everyone how it's done. Instead, we have the Skype team going back to the desktop app and the Office team telling people not to use the universal apps on PCs. Those universal apps are just meant for smartphones and small tablets — that's what the Office team at Microsoft is telling us.

Maybe they'll be more successful once developers can simply port their iPad apps to the Windows Store. Unfortunately for Microsoft, most PC users probably won't want to use iPad apps on their desktop.

Windows 10 includes "Get Skype" and "Get Office" apps, which are literally just universal apps that just tell you to download the desktop apps. Microsoft is also using these ads to <u>spam Windows 10 users with ads</u>, so they do have another function.



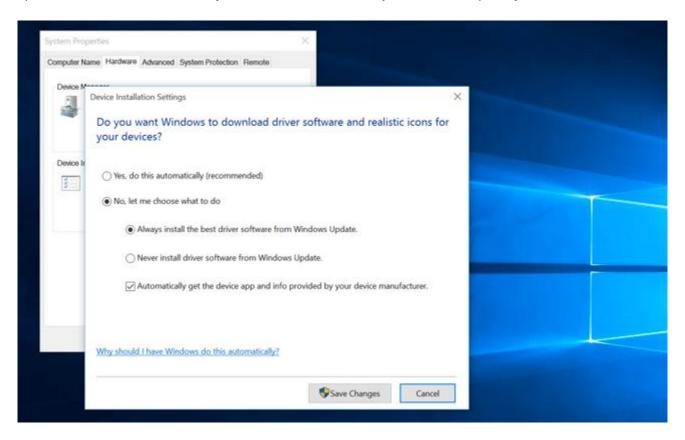
Mandatory Driver Updates Can Break Some Systems

Mandatory driver updates are another issue. Rather than just pushing out Microsoft's own Windows updates to everyone, Microsoft is forcing you to install the latest drivers it thinks will work on your computer. There's no way to opt out of these drivers if they don't work for your hardware. Install your own custom drivers and Windows Update will repeatedly install its own drivers over your own custom ones.

There's still a "Do you want Windows to download driver software" setting buried in Windows that claims it will stop Windows Update from installing drivers, but it doesn't actually work. Microsoft didn't bother removing it, though, which just confuses everyone.

The only way to get around this is by <u>blocking individual driver updates with a special tool you have to download from Microsoft's website</u>. But you'll get new drivers when a newer version appears in Windows Update.

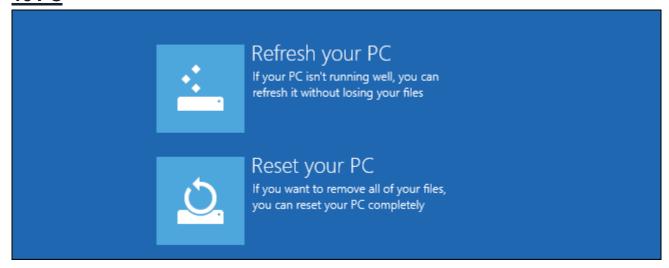
Mandatory security updates are one thing, but Microsoft should allow PC users to have control over their specific hardware drivers if they need it — even if this is just a hidden option you have to enable.



These are just a few of the ways Windows 10 falls flat on its face. There are certainly others. The continued separation between the Settings and Control Panel apps is silly. The white titlebars are ugly to many people and a sad step back from the colorful Windows 8, although Microsoft seems to be realizing their mistake and adding color choice back in.

And people who depended on the unique placeholder files functionality in Microsoft OneDrive on Windows 8.1 will be disappointed to find it's been completely removed in Windows 10.

Everything You Need to Know About Refreshing and Resetting Your Windows 8 or 10 PC



Windows users regularly reinstall Windows (or restore from a recovery partition) to fix system problems. Windows 8 or 10 include easier-to-use "Refresh" and "Reset" options that quickly restore Windows to a fresh, factory default configuration.

Just as mobile devices have an integrated "reset to factory defaults" option, so does Windows 8 or 10. You can even create your own refresh image or access these options if your computer can't boot.

The Difference between Refresh and Reset

Windows 8 or 10 have two factory reset options, named Refresh and Reset. Both reset your computer to a fresh, factory default sate. Refresh preserves your files and installed Modern programs, while Reset removes everything on your system.

When you Refresh your PC:

Windows will save your personal files, personalization settings, and Modern apps installed from the Windows Store.

- Windows will reset your PC settings.
- Windows will remove all installed desktop programs. A list of the removed programs will be saved to your desktop.

By resetting your computer settings and removing all desktop programs, Windows can "refresh" your PC so it's more like a fresh install without deleting your personal files.

Refresh your PC

Here's what will happen:

- Your files and personalization settings won't change.
- Your PC settings will be changed back to their defaults.
- Apps from Windows Store will be kept.
- Apps you installed from discs or websites will be removed.
- A list of removed apps will be saved on your desktop.

When you Reset your PC, Windows will remove everything. Think of this like doing a complete Windows reinstall and formatting your hard drive.

Reset your PC

Here's what will happen:

- · All your personal files and apps will be removed.
- Your PC settings will be changed back to their defaults.

Should You Refresh or Reset your PC?

If you're experiencing problems with your computer and want to fix them, you should try refreshing your PC first. Windows will restore system files and desktop programs to their default state, saving all your important personal files (and Modern apps, if you use them.)

If you want to reset your computer to its factory default state – particularly useful if you're getting rid of the computer and want to remove your personal data, or if you just want a clean start — you should reset your PC instead.

Refresh your PC without affecting your files

If your PC isn't running well, you can refresh it without losing your photos, music, videos, and other personal files.

Get started

Remove everything and reinstall Windows

If you want to recycle your PC or start over completely, you can reset it to its factory settings.

Get started

Under the Hood

Microsoft has explained what's actually going on under the hood here. When you reset your PC:

The PC boots into Windows RE, the Windows Recovery Environment

Windows RE erases and formats the Windows partitions before installing a fresh copy of Windows 8 or 10.

The PC restarts into the new copy of Windows.

When you refresh your PC, the same steps occur. However, before erasing your Windows partition, Windows RE scans the hard drive for your files, settings, and Modern apps. It places them aside, installs a fresh copy of Windows, and puts them back where they were found.

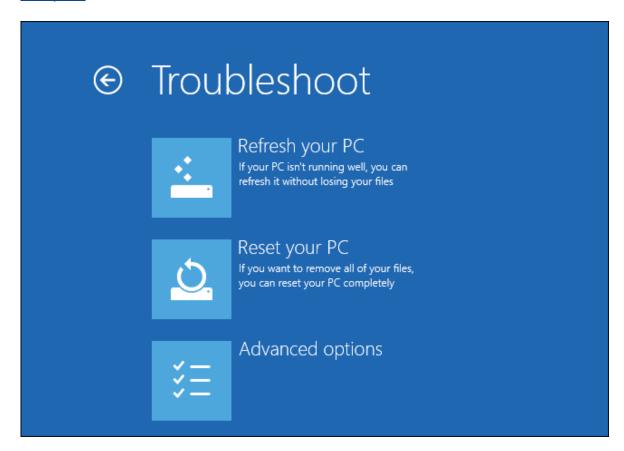
Both refresh and reset involve a fresh installation of Windows, which is why your desktop programs aren't saved.

Note that it's always a good idea to have backup copies of your files. If something goes wrong, you wouldn't want to lose the only copy.

How to Refresh or Reset

If your computer is still working properly, you can <u>refresh or reset it from the PC Settings application within Windows</u>. For Windows 10, go to Settings, Update and Security, and then Recovery.

If your computer is not booting properly, you can refresh or reset it from the boot options menu. We've covered <u>several ways to access this menu</u>. Once you've accessed it, <u>use the Refresh your PC or Reset your PC option</u>.



Creating Your Own Refresh Image

Refreshing your PC removes all your desktop programs. If you always install some critical desktop programs, you'll have to reinstall them every time you refresh your computer. To save time, you can create a custom refresh image after installing the programs you use. They'll be saved and will come back every time you refresh your computer.

Read More: How to Create a Custom Refresh Image in Windows 8

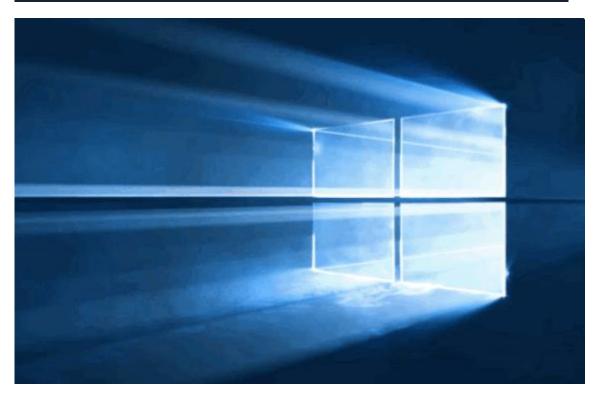
```
Administrator: Command Prompt (Admin)

C:\Windows\system32\recimg /createimage C:\CustomRefreshImages\Image1
Source 0S location: C:
Recovery image path: C:\CustomRefreshImages\Image1\install.wim
Creating recovery image. Press [ESC] to cancel.
Initializing
100%
Creating snapshot
100%
Mriting image
100%
Registering image
100%
Recovery image creation and registration completed successfully.

C:\Windows\system32>
```

The refresh and reset features help quickly reinstall Windows. Even for experienced users, the refresh and reset processes are faster than reinstalling Windows the old-fashioned way.

Should You Upgrade to the Professional Edition of Windows 10?



However you're getting Windows 10 — either with the free upgrade offer or on a new PC — you're probably getting Windows 10 Home. You can pay to upgrade that Windows 10 Home system to Windows 10 Professional — but should you?

If you already had a Professional edition of Windows 7 or Windows 8.1, don't worry. The free upgrade offer will give you Windows 10 Professional. Otherwise, you'll need to shell out some money if you want the below extra features.

The Windows 10 Pro Pack Upgrade Costs \$99

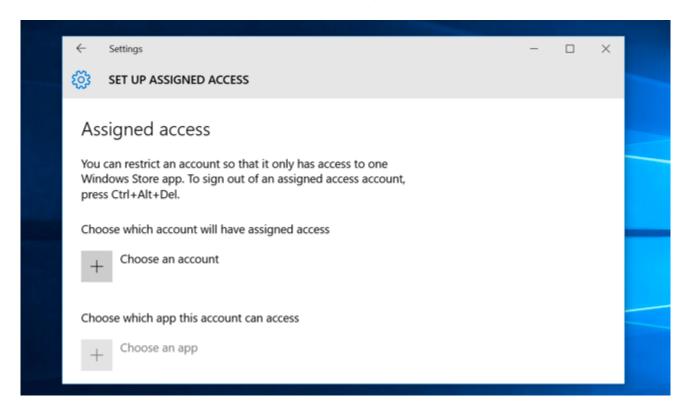
This works similarly to the Windows 8 Pro Pack. From within Windows 10 itself, you have the option of paying Microsoft another \$99. If you do, your Windows 10 Home system will be upgraded to a Windows 10 Professional system with no Windows reinstall required. All the extra features in Windows 10 Professional will be unlocked. With Windows 8.1, this was also sold as a physical card with a code on it, so you can probably buy it in stores, too.

Unsurprisingly, most of the features included here are intended for businesses and power users in general. Microsoft called the base edition of Windows 8 "Windows 8" and the Professional version "Windows 8 Professional." With Windows 10, they're back to "Windows 10 Home" and "Windows 10 Professional," which is certainly clearer.

Microsoft is no longer offering Windows Media Center as a paid upgrade — that's discontinued. Media Center devotees will want to stick with older versions of Windows or try a Windows Media Center alternative.

Assigned Access 8.1

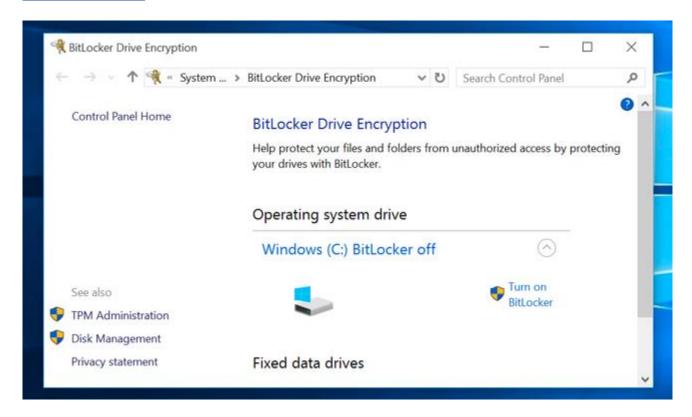
<u>The Assigned Access feature</u> was added in Windows 8.1, so that's probably why Microsoft is still calling it "Assigned Access 8.1." This option allows you to lock a user account down to automatically load a specific universal app and run only that application. It's ideal for kiosk-type PCs — you could have it automatically load a web browser and restrict users to that, for example.



BitLocker and EFS

<u>Microsoft's BitLocker disk encryption technology</u> is still restricted to the Professional version of Windows, so you'll need to pay up if you want to use the most powerful and integrated disk-encryption tool on Windows. BitLocker allows you to encrypt internal drives and external USB drives. You can even <u>create encrypted container files</u>. The <u>Encrypting File System (EFS) feature</u> is similar — powerful encryption features aren't offered in the Home edition.

The Home edition does offer <u>Device Encryption</u>, which is automatically enabled on new PCs. However, it doesn't provide many options — Device Encryption only works if you sign in with a Microsoft account on a new PC with the appropriate hardware. Even then, <u>it always uploads your encryption recovery key to Microsoft's servers.</u>



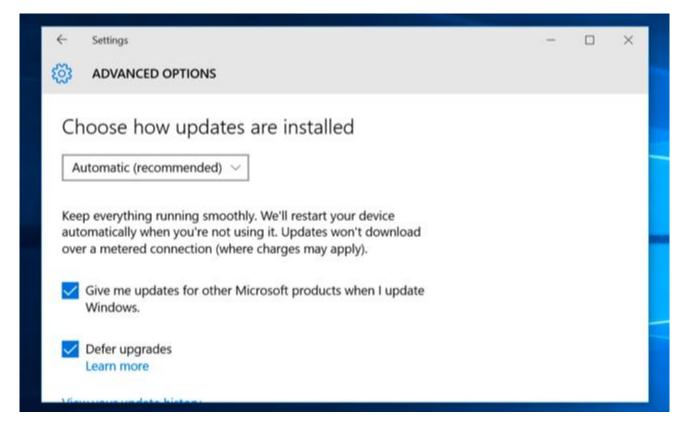
Business Store and Private Catalog

With Windows 10, businesses can create a private section of the Windows 10 Store for their organization. Users can browse the business's private catalog and install apps specifically approved by their organization. Businesses can also buy Store apps in bulk and deploy them to their own devices. This requires at least the Professional edition of Windows 10.

Current Branch for Business

<u>Windows 10 doesn't allow you to disable Windows Update</u> and delay installing feature updates. Microsoft wants those Windows systems to be always up-to-date. Windows 10 Home users aren't able to put off installing feature updates at all. Windows 10 Professional users can put off installing these updates by being on the "Current branch for business," a more conservative approach to updates. By the time these systems

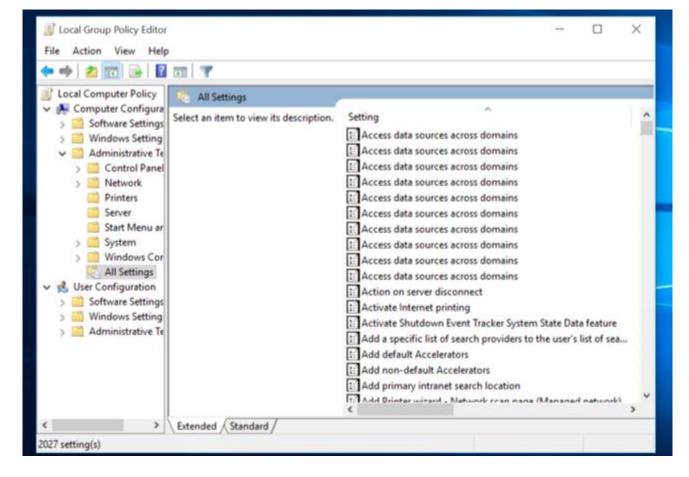
get Windows 10 updates, they will have been beta-tested by millions of Windows 10 Home users. By default, Windows 10 Professional still uses the faster approach to updates.



Domain Join, Group Policy, and Microsoft Azure Active Directory Join

If you want to join a domain or manage your PC via group policy, these will continue to require the Professional edition of Windows. Generally, these are only features used on business networks, not on your home network. However, the Local Group Policy Editor will remain off-limits to you and you won't be able to tweak group policy settings on a Home version of Windows 10, just as on previous editions of Windows.

Organizations using Microsoft's Azure AD service can have their Windows 10 devices sign directly into Azure active directory rather than signing in with a Microsoft account or a traditional Windows domain with a local server. This requires the employee choose the "This device belongs to my organization" option during the set-up process and sign in with their Azure AD credentials.



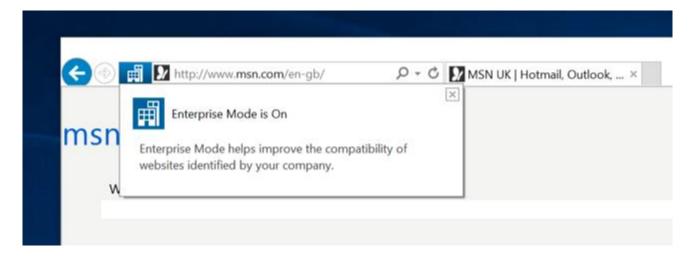
Enterprise Data Protection

Enterprise Data Protection (EDP) is a new feature in Windows 10. For devices containing both personal data belonging to an employee and work data belonging to an organization, EDP allows businesses to mark specific universal apps as having privileged corporate data and protect it. That data can be separately encrypted and even remotely wiped without affecting the user's own data. Enterprises can also audit and track the usage of this data.

For example, an email app could be marked as containing sensitive email and the data protected and audited. If an employee quits, the organization can remotely wipe that email app of all data without touching the rest of the sy

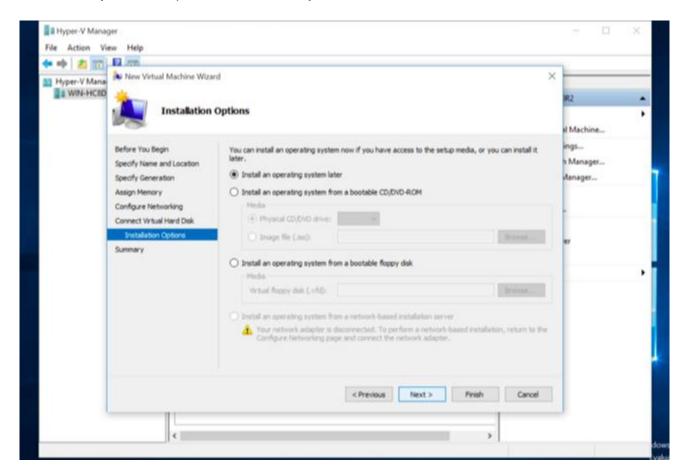
Internet Explorer 11 is still included in Windows 10, although <u>Microsoft's Edge browser</u> is the default. Professional editions of Windows get <u>the "Enterprise Mode" feature in Internet Explorer</u>, which essentially allows you to force Internet Explorer 11 to behave more like Internet Explorer 8. This is only really useful if you're using ancient websites — usually internal business websites — that don't work properly in modern browsers. This option must first be enabled in group policy before you can access it.

All editions of Windows 10 include Internet Explorer 11 for compatibility with older websites. This feature is just an extra perk.



Hyper-V

Windows 10 offers <u>a built-in virtual machine solution known as Hyper-V</u>. This was previously a Windows Server feature that made the jump to desktop versions of Windows with Windows 8. Like VirtualBox and VMware, Hyper-V allows you to create and run virtual machines, allowing you to run operating systems in windows on your desktop. This feature is only included with Professional editions of Windows.



Remote Desktop

Like previous versions of Windows, Windows 10 Home offers a client for connecting to Remote Desktop servers, but not the Remote Desktop server itself. To host a Remote Desktop server using Windows 10's

built-in Remote Desktop feature, you'll need Windows 10 Professional. However, there are many<u>other</u> remote-desktop solutions that don't require Windows 10 Professional and are easier to set up.

Windows Update for Business

This is a tool that allows network administrators to better control when Windows Update occurs on devices on their network. For example, they can set specific devices to perform updates first in a "wave" of updates that goes out. They can configure maintenance windows to define exactly when updates should and should not occur — during normal business hours, for example. Peer-to-peer delivery of Windows Updates can occur over a business network between remote offices.

The Enterprise and Education editions of Windows 10 offer more features still, although you can't get them without a volume license. For example, they offer Windows To Go for installing and running Windows 10 from a USB flash drive and AppLocker for locking down the applications that can run on your computer.

Here's Why Windows 8.1's Encryption Doesn't Seem to Scare the FBI



The FBI isn't happy about the latest versions of iOS and Android using encryption by default. FBI director James Comey has been blasting both Apple and Google. Microsoft is never mentioned — but <u>Windows 8.1</u> uses encryption by default, too.

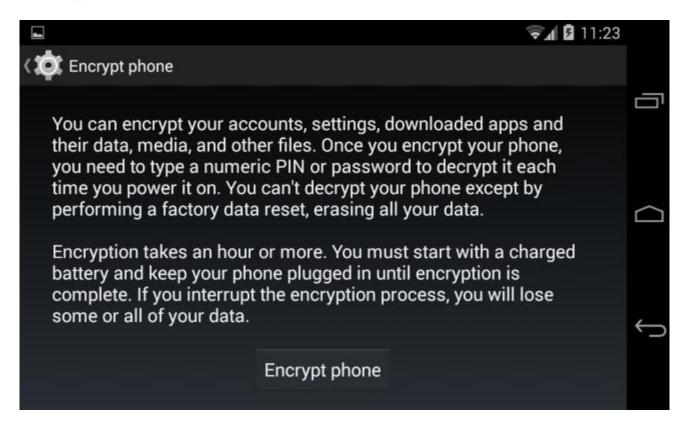
The FBI doesn't seem worried about Windows 8.1's default "device encryption" feature. Microsoft's encryption works a bit differently — Microsoft holds the keys and could hand them over to the FBI.

Why the FBI is Blasting Apple and Google

FBI directory James Comey <u>has said</u> Apple and Google are creating "a black hole for law enforcement." Encryption "threatens to lead us all to a very dark place," according to the FBI.

The latest versions of Apple's iOS and Google's Android automatically encrypt a smartphone or tablet's storage by default. Previously, this was just an option most users wouldn't enable. Because of the way encryption works, only a person who knows the key can decrypt it and access the unencrypted files. If Apple or Google received a warrant — or some sort of secret "national security letter" — they wouldn't be able to decrypt the files even if they wanted to. They don't have the encryption key. (A national security letter is a secret order that may contain a "nondisclosure" requirement, preventing the person who received the national security letter from ever talking about it for the rest of their life under threat of criminal prosecution.)

This is the main issue for the FBI — encryption that prevents thieves from accessing your data after they steal your device is fine. However, the FBI wants to have a way to force Apple or Google to provide access to the encrypted data. In other words, they want Apple and Google to have a key they can use to gain access to the encrypted data.



Windows 8.1's Device Encryption Gives Microsoft a Key

New Windows 8.1 devices ship with something called "device encryption" enabled by default. This is different from the BitLocker encryption feature, which is only available in more expensive <u>Professional editions of Windows</u> and not enabled by default.

If you have a supported device, the device's storage comes pre-encrypted — but it uses an empty encryption key. When you sign in with a Microsoft account, the encryption is activated and a recovery key is uploaded to

Microsoft's servers. (If you sign in on a <u>domain</u>, the recovery key is uploaded to Active Directory Domain Services, so your business or school has it instead of Microsoft.) If you use a local account, there's no way to enable the device encryption.

In other words, device encryption can only be used if you upload a recovery key to Microsoft's servers (or to your organization's domain server). If a thief stole your device, they wouldn't be able to gain access. However, if law enforcement were to send a warrant (or a secret national security letter) to Microsoft, Microsoft would be forced to give the government your recovery key.

This is exactly what the FBI wants from Apple and Google — they want them to hold a recovery key they can disclose. Apple and Google are digging in, but Microsoft already gave the FBI what they wanted.

How will this person sign in?

What email address would this person like to use to sign in to Windows? (If you know the email address they use to sign in to Microsoft services, enter it here.)

Email address

Sign up for a new email address

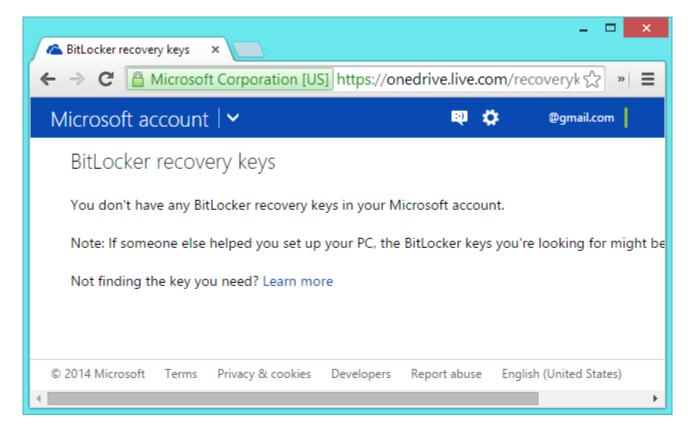
This person can sign in to easily get their online email, photos, files, and settings (like browser history and favorites) on all of their devices. They can manage their synced settings at any time.

Microsoft May Have Other Reasons, But...

Now, this isn't *all* about providing a backdoor for the FBI. Average Windows users who forget their password will be able to get a recovery key from their Microsoft account by going through a password reset process. They'd just have to visithttp://windows.microsoft.com/recoverykeyand sign in with the same Microsoft account — using an account recovery procedure if they can't remember the password. Typically, encryption can't be bypassed — if a user forgot their password, they'd lose access to all the files on their computer. Microsoft seems to consider this unacceptable.

But this is all a bit weird. There's no way to enable device encryption without uploading a recovery key somewhere — not even a hidden power user option. This is very unusual for encryption — Android and iOS certainly don't do it this way. BitLocker offers to back up your recovery key to your Microsoft account, but this part isn't mandatory. It's one of many different ways to create a backup of your recovery key — unlike with the default device encryption.

Even ignoring law enforcement access, this makes the encryption weaker. Someone could go through the password reset process in your Microsoft account to gain access to your encrypted files. We've previously seen people abuse password reset procedures with <u>social-engineering tricks</u> to gain access to other people's accounts. It's just less secure.



Law Enforcement Can Get Everything, Anyway

If the FBI wants to get access to text messages and phone calls, they can get it from the cellular carriers. If the FBI wants to get access to emails, social media posts, and files stored in cloud storage, they can get it by contacting the associated web services — yes, even Google and Apple would have to respond and hand over users' data.

The US and other countries even have massive secret databases containing logs of who's called who.

They're even trying to monitor all the traffic on the web and shove it into a database so it can be queried later.

Whatever sensitive data is protected via encryption is probably available elsewhere. Even with iOS and Android, devices are set to upload data to Apple's iCloud and Google various services. That uploaded data could be gotten from their servers with a warrant or national security letter.

Pass a Law If It's So Important

There's a way for the FBI to actually get these backdoors — the government would just have to pass a low mandating backdoors for law enforcement. Currently, implementing encryption with no backdoors for law enforcement is completely legal in the US. The FBI actually gave up on pushing for such a law:

"The F.B.I. has abandoned a component of its original proposal that would have required companies that facilitate the encryption of users' messages to always have a key to unscramble them if presented with a court order. Critics had charged that such a law would create back doors for hackers. The current

proposal would allow services that fully encrypt messages between users to keep operating, officials said."

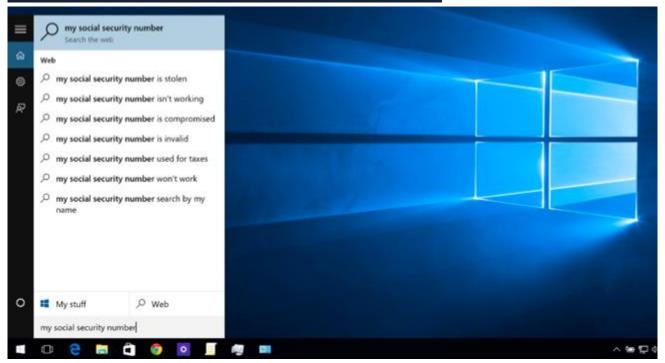
If it's so dangerous to allow encryption without a backdoor, why did the FBI give up on it? Probably because they know they'd lose. But, if the FBI's current rhetoric is anything to go by, we could see such a law start to take form again.



Overall, device encryption is still a useful feature in Windows. Encrypting files but allowing the FBI to gain access is still an improvement over not encrypting those files. The encryption at least prevents thieves from gaining access. Let's not mince words: Device encryption is good. It's better than the complete lack of default encryption Windows used to offer, even with this concern.

However, Microsoft's means of allowing law enforcement to access encrypted files is something that's flown under the radar. It's particularly relevant when we see Apple and Google digging in and refusing to enable this covert access. Apple and Google can't provide law enforcement with access to your encrypted data, but Microsoft can.

How to Disable Bing in the Windows 10 Start Menu



Windows 10, by default, sends everything you search for in the Start Menu to their servers to give you results from Bing search — so you better make sure that you don't type anything private into your own PC's Start Menu. Or, you could just disable the Bing integration in the Start Menu.

It's worth noting that Android's default search and even iOS will also send your search results to their servers to try and get more relevant results — but somehow it seems different when you're on your personal computer in your house trying to search through your personal files.

We're definitely glad that they included a way to easily disable the web integration — it's just worth noting that if you want to use Cortana, you don't have any choice in whether the Start Menu uses Bing, so you're going to have to disable Cortana to disable the web integration.

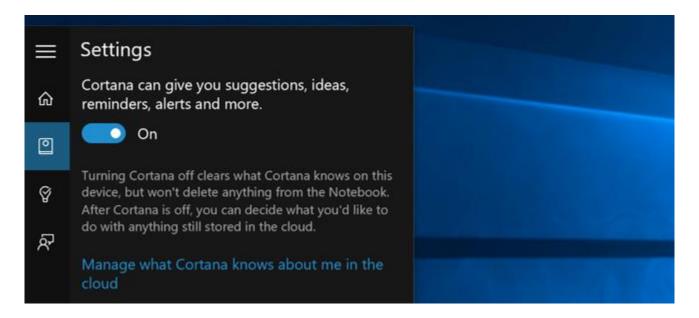
How to Disable Bing Integration in the Start Menu

Luckily Bing is really easy to disable, and you'll just need to get to the Cortana search settings screen — the easiest way to do this is to type "cortana settings" into the Start Menu and choose the "Cortana & Search settings" item.

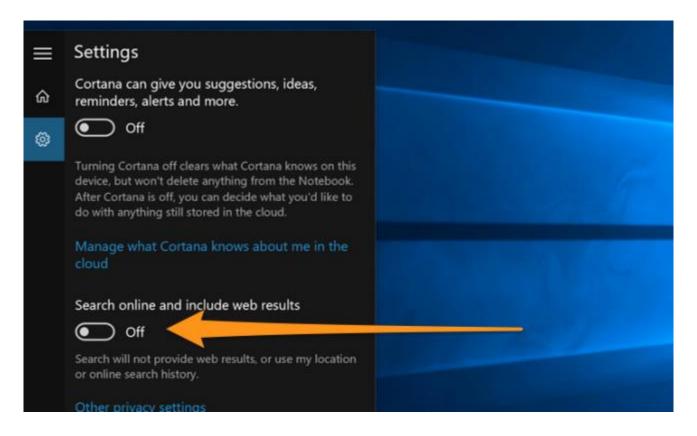


This will bring up the settings dialog, which is going to look different depending on whether you've already disabled Cortana or not.

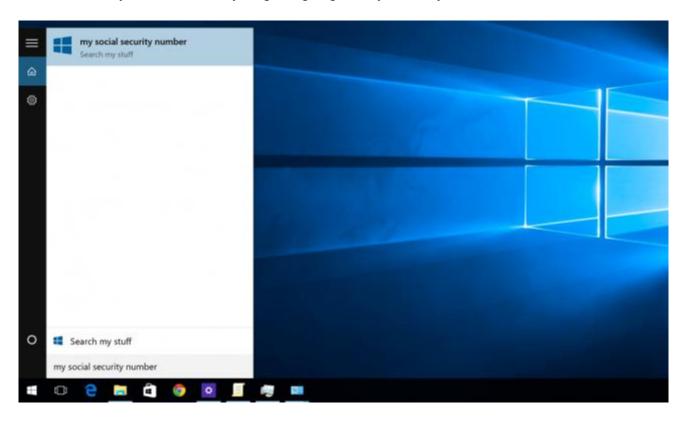
If you want to disable the Bing integration, you're going to also have to disable Cortana — so flip that switch to Off.



Now that you've disabled Cortana, the rest of the dialog will change and you'll see an option for "Search online and include web results", which you are going to want to disable as well — this is how you actually disable Bing from the Start Menu.



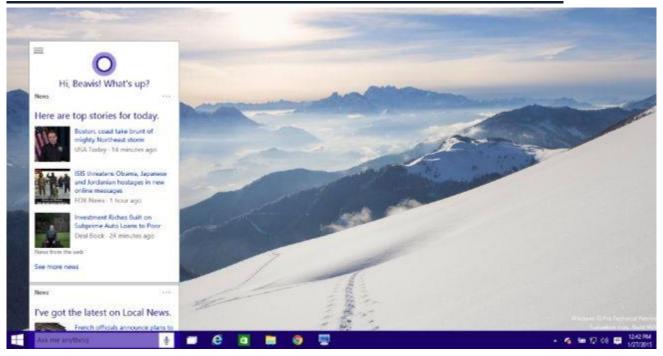
And now when you search for anything, it's going to only search your own PC.



Notice how clean it is now — and it says "Search my stuff" instead of "Search the web".

Note that If you want to <u>disable the Search box from the Taskbar</u>, you'll need to right-click it and choose the Hidden option.

How to Hide the Cortana Search Box on the Windows 10 Taskbar



One of the most talked about features in the latest version of Windows 10 was the Cortana personal assistant that is integrated directly into the taskbar. But what if you don't want to waste all that taskbar space?

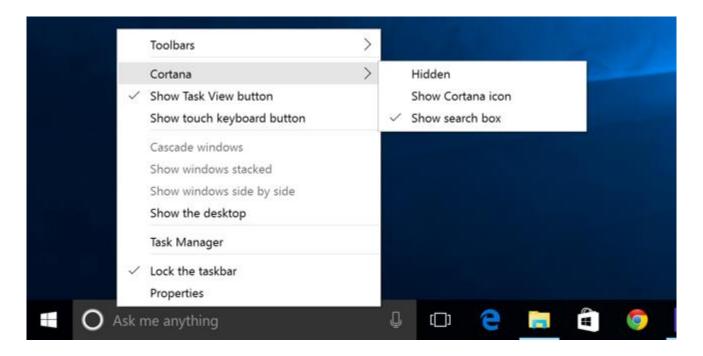
Luckily they not only provide a way to remove the search box from the taskbar, but you can change it into an icon, or you can remove it entirely and then it'll show up on the taskbar only when you open the Start Menu (so you can still search for your apps).

We're not entirely sure if we like the idea of a digital assistant as part of Windows, but if you're using the preview, we recommend that you test it out at least to give it a chance. If you don't like it, then you can disable it and make the search box revert back to the Windows 8.x behavior where it searches your apps as well as the web.

Removing the Cortana Search Box from the Taskbar

Note that hiding the search box doesn't actually disable Cortana — keep reading below for instructions on how to do that. This will simply hide the box from the Taskbar.

Simply right-click on any empty space on the taskbar, go to Search, and then change "Show search box" to either "Show Cortana icon" or "Hidden".



If you change it to an icon, it'll show a circle like you can see below.

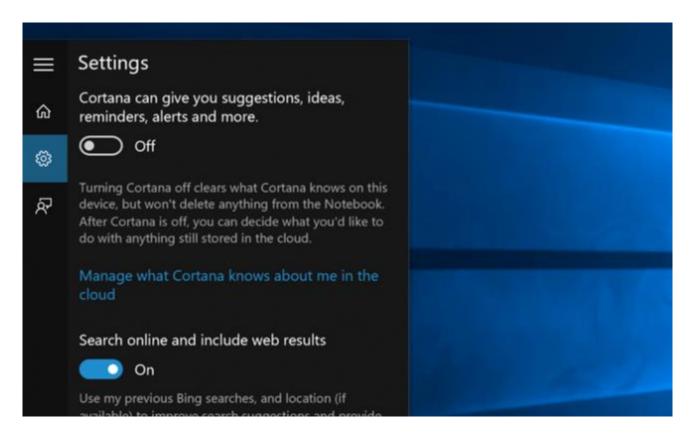


And if you disable it entirely, it'll be removed from the taskbar. You can also hide that Task View button while you are at it by just right-clicking and unchecking the box — although we'll say that the new task switcher is pretty nice.

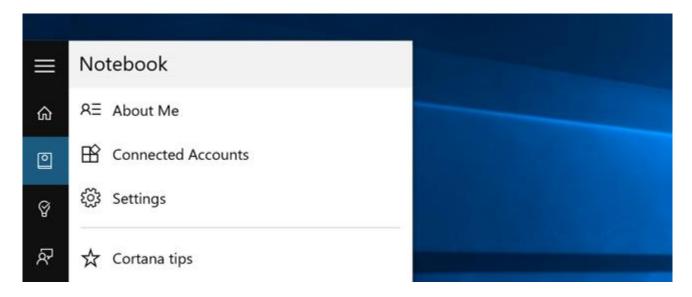


Disabling Cortana

If you haven't enabled Cortana, you'll see the top of the box that looks like this when you click on the Search box and then click the Settings icon. Note that Cortana is Off. You can also turn off the online search and including Bing results when you search the Start Menu by flipping that switch off as well.



If you have already enabled Cortana, the settings dialog changes completely and is hidden beneath the Notebook icon — from here you can click on Settings and get to the screen above.



Once you disable Cortana and Bing, you can then hide the icon.

It's really nice that you can turn it off — we'd have probably preferred that Bing stay out of our Start menu in the first place though.

How to Remove Cortana from the Windows 10 Taskbar



Cortana is the latest digital personal assistant to make its way into a market already dominated by Apple and Google. Cortana officially arrives for the desktop in Windows 10. That's largely a good thing, though it's still important to know how to reduce Cortana's presence.

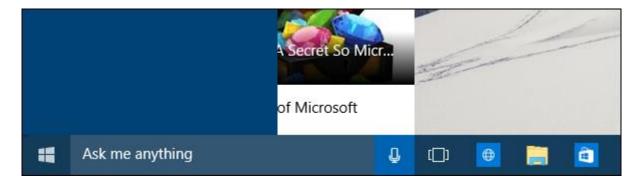
In case you hadn't heard, Cortana is Microsoft's version of the same kind of voice-activated (if desired) computer assistant you've come to expect from "Ok Google" and Siri. You can for example <u>say, "Hey Cortana"</u> and ask it for the weather or sport scores or see how your stocks are doing.

So far the buzz about Cortana is generally positive and <u>we are looking forward to it</u>. For Windows, it seems like an idea whose time has come. It especially makes sense when you consider that Microsoft wants to fit Windows 10 onto more tablet-like devices, so being able to just tell your computer what you want will be more efficient and easier than using a touch keyboard all the time.

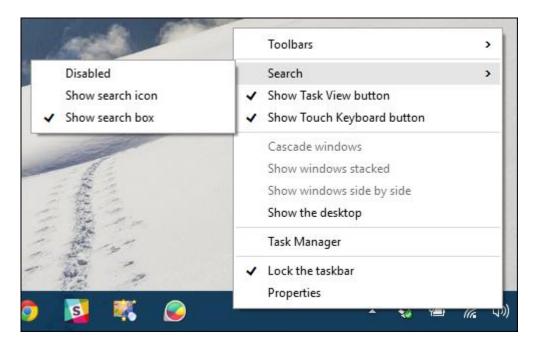
On Windows 10, Microsoft has integrated Cortana right into the taskbar, which is fine since Google has no problem slapping its search feature on Android's home screen.



Unlike Android, however, Windows 10 easily allows you to change how much space Cortana takes up on the taskbar. By default, it appears as a search bar that says "Ask me anything".



It's not ugly or detracting but it is rather wide and for folks with smaller displays, it might take up too much screen real estate. Luckily, if you right-click on a blank spot on the taskbar, you can scroll up to "Search" and change how much space Cortana occupies.



Here, we've just elected to show the search icon, which is just a simple circle.



Finally, if you just want Cortana off your taskbar completely, then you can just disable it.



Note, however, this will not turn Cortana off. If you have it, for example, set up to listen for your voice, then even if you remove Cortana from the taskbar, it will still respond when you say "Hey Cortana".

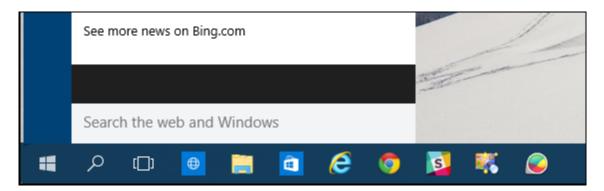
To completely turn Cortana off, as in, it will no longer work, respond, or collect information, then you first need to open the Cortana search feature and click on the gear icon along the left-hand edge.



This will open the settings where you can turn "Hey Cortana" on or off, change your name, or, most importantly, turn the whole thing off right at the very top where it says "Cortana can give you suggestions, ideas, reminders, alerts, and more."

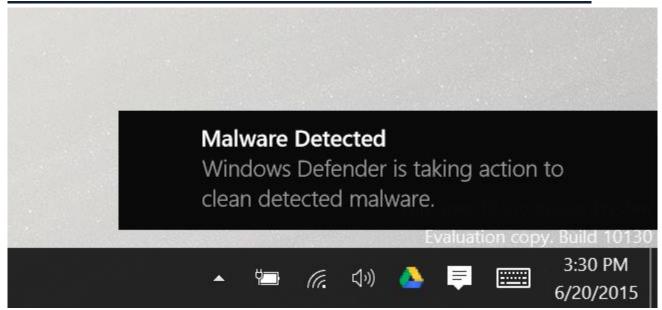


Once disabled, Cortana will revert to the traditional Windows search feature, indicated on the taskbar by a magnifying glass. When you click on it, it will instead let you "Search the web and Windows" (via Bing).



You can still change the way search appears on your task bar, however, electing to show the search box, the icon, or disable (remove) it altogether. If you do decide you want to disable it, you can still access search through the old keyboard shortcut "Windows + S".

How to Use the Built-in Windows Defender Antivirus on Windows 10



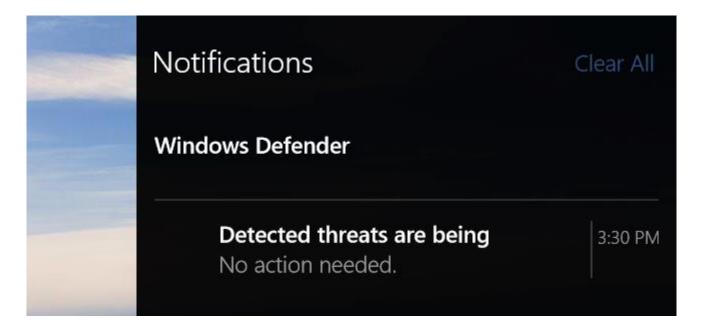
<u>Windows 10 has built-in real-time antivirus</u>, just as Windows 8 did. It automatically runs in the background, ensuring all Windows users have a baseline level of antivirus protection. Windows 10 won't complain at you to install an antivirus, as Windows 7 did.

If you've used Microsoft Security Essentials on Windows 7 or previous versions of Windows, this is the same basic product. It was renamed to "Windows Defender" in Windows 8 and integrated into Windows itself.

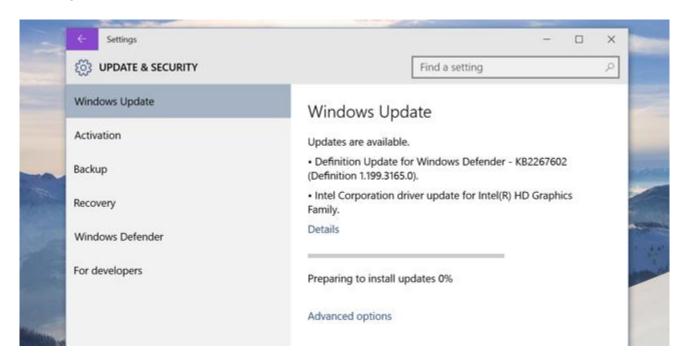
Automatic Scans and Updates

Like other anti-malware applications, Windows Defender automatically runs in the background, scanning files when they're accessed and before you open them.

You don't really have to think about Windows Defender at all. It will only pop up and inform you when it finds malware. It won't even ask you what you want to do with the malicious software it finds — it will clean it up and quarantine the files automatically. You'll see a "Malware detected" notification saying "Windows Defender is taking action to clean detected malware" or "Detected threats are being cleaned." It'll appear in the notification center, too.



Antivirus definition updates will automatically arrive through <u>Windows Update</u> and be installed like any other system update. These types of updates don't require rebooting your computer. You don't need to worry about updating Windows Defender.

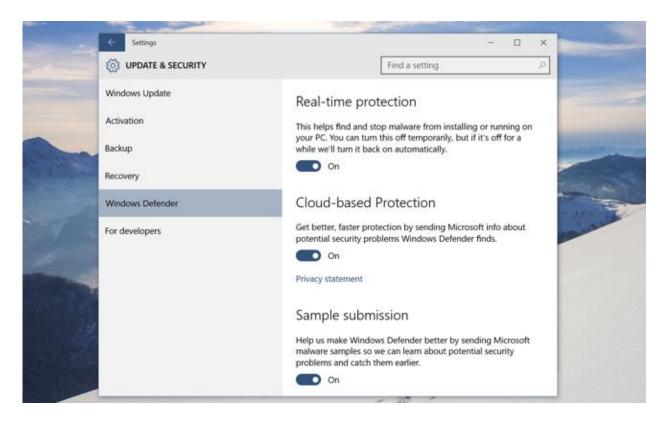


Configuration and Exclusions

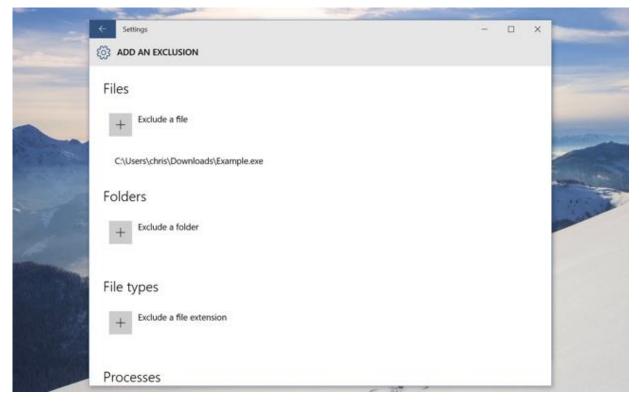
Windows Defender settings are now integrated into Windows 10's new Settings app. To access it, open the Start menu and select Settings. Choose the "Update & security" category and select Windows Defender.

By default, Windows Defender automatically enables real-time protection, cloud-based protection, and sample submission. Real-time protection ensures Windows Defender automatically finds malware by scanning your system in real time. You could disable this for a short period of time if necessary for performance reasons, but Windows Defender will automatically re-enable real-time protection to keep you

safe later. Cloud-based protection and sample submission allow Windows Defender to share information about threats and the actual malware files it detects with Microsoft.



You can also set Exclusions from here — scroll down and select "Add an exclusion." Exclusions can be specific files, folders, file types, and processes. If the antivirus is dramatically slowing down a certain application you know is safe by scanning it, this can speed things up again. Be careful to<u>use exclusions sparingly and smartly</u> — these reduce your PC's security because they tell Windows Defender not to look in certain places.

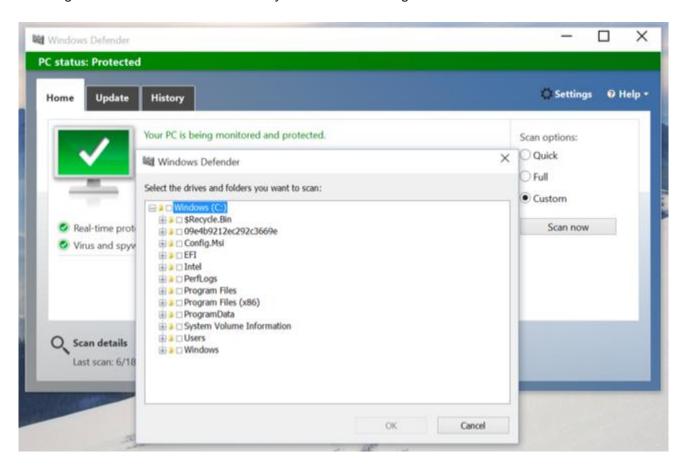


Manual Scans

Scroll down to the Version info section at the bottom of the Windows Defender pane in the Settings window and click "Use Windows Defender" to access the Windows Defender desktop app interface. If you've used Microsoft Security Essentials before, you'll immediately recognize this. (We can probably expect Microsoft to move more of the options here to the Windows Defender pane in the Settings app over time.)

From this window, you can initiate a quick scan, full system scan, or a custom scan of specific folders. For example, you could connect an external hard drive to your computer and perform a Custom scan to scan that entire drive for malware.

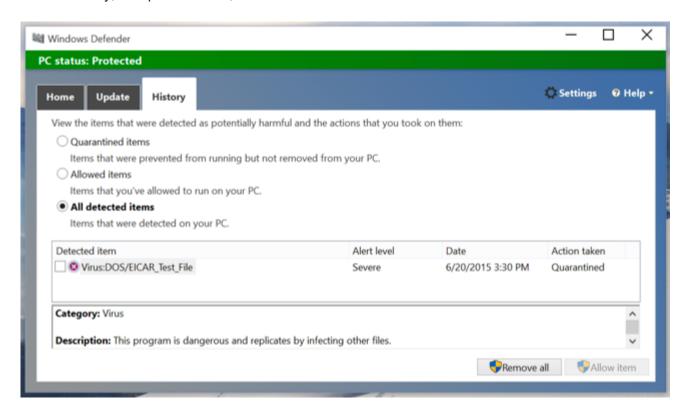
You shouldn't have to regularly perform manual antivirus scans. Windows Defender scans everything in the background anyway, and there's even a scheduled task in Windows that automatically scans your computer on a regular basis. This feature is mostly useful for scanning external media and network locations.



Viewing Quarantined Malware

If Windows Defender informs you that it's blocked malware, you can view the blocked malware from the Windows Defender desktop app. Click the "use Windows Defender" link in the Settings app to access Windows Defender, and then click over to the History tab. Click "View details" to view detected malware. You can see the name of the malware and when it was found and quarantined.

From here, you can remove the malware to delete it entirely from your PC or allow the supposedly malicious file to run. You should only do this if you're absolutely sure the detected malware is a <u>false positive</u>. If you're not absolutely, 100 percent sure, don't allow it to run.



What if You Install Another Antivirus?

Windows 10 will automatically disable Windows Defender if you install another anti-malware program. It won't continue performing real-time scans, so it won't interfere with your other antivirus. Try to open the Windows Defender settings pane with another antivirus installed and you'll find every option grayed out. Click the "Use Windows Defender" link and you'll be informed Windows Defender has been disabled. Windows Defender will pop-up and say "This app has been turned off and isn't monitoring your computer."

If you uninstall the other antivirus, Windows Defender will kick into gear once again and take over, providing antivirus protection.

Whichever antivirus product you prefer, it's good that every single new Windows installation going forward will come with built-in antivirus protection. <u>The Malicious Software Removal Tool</u> Microsoft occasionally delivers through Windows Update is no substitute for a proper anti-malware application.

Antivirus Slowing Your PC Down? Maybe You Should Use Exclusions









Protecting your computer with an antivirus solution is par for the course when you're dealing with a Windows PC, but unfortunately it slows you down at the same time. Here's how to improve your performance, at least a little bit.

We're not going to sit here and tell you to go without antivirus, since that would be irresponsible. What we're going to do today is explain how you can exclude certain folders with write-heavy operations to speed up your PC without putting yourself into extra danger.

Note: Before you start excluding any files, you keep in mind that changing any of the default security settings could be risky, and you should probably close the browser tab and run away. Or maybe print off the article and burn it. Also, the image is by xkcd

What Files Should You Exclude?

The general idea is that if you have some applications that are writing to the hard drive constantly, you should probably exclude the folders they are writing or reading from, as long as those applications are trusted and safe.

For example, if you're using a virtual machine, which does both reads and writes from the hard drive on a fairly constant basis, you should make sure your antivirus application is not scanning those files and folders. Here's a few examples of some things you may consider excluding:

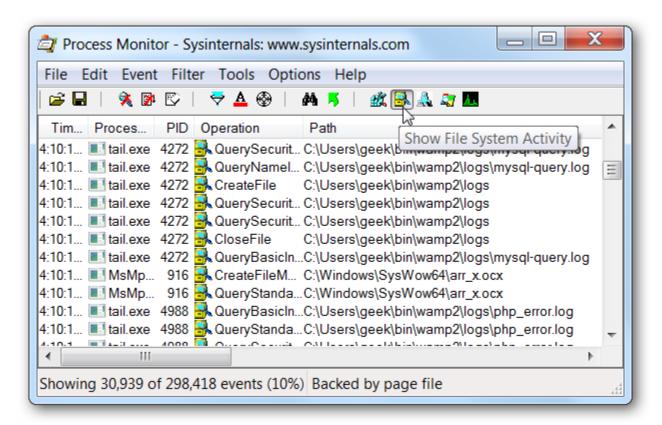
- **Virtual Machine Directories:** If you're using VMware or VirtualBox, you should make sure those locations are excluded. This is actually what prompted this article, and probably the only *significant* performance boost out of the things we're mentioning.
- **Subversion / TortoiseSVN Folders:** Have you ever tried to do a big checkout of a source control project and had it fail? There's a good chance that it's conflicting with your antivirus application. *This one has personally happened to me.*
- Personal Photo/Video Folders: Got you have a massive library of photos or videos that you've taken with your digital camera? As long as you only use this location for files copied from your SD card, there's no reason to be scanning it and slowing your PC down while doing photo editing.
- Legitimate Music Folders: If you're downloading music from shady sources, this does not apply. If you've ripped your own CDs or downloaded from somewhere legitimate like Amazon, then you can safely exclude your music folder.

• Windows Update Folders: This actually comes straight out of a <u>Microsoft KB article</u>—you'll notice that they don't recommend it, because they can't do that in case somebody writes a special virus for the purpose of suing them, but the same principle applies.

Other Scenarios

There's a nearly infinite number of applications and scenarios for everybody's PC, so it's hard to say exactly what is going to work on your PC—but there's a way you can figure it out for yourself using <u>Process Monitor</u>, the great tool from Sysinternals at Microsoft.

Just open up Process Monitor, and then "uncheck" all of the little icons on the right-hand side of the toolbar, leaving only the "Show File System Activity" one checked. At this point you'll see loads and loads of items in the list, with every access to the file system.



You can use this data to figure out which applications are constantly reading and writing to the hard drive, and then based on the safety of those files, you can choose whether or not to exclude them.

Don't Exclude File Types, Exclude Folders

When you exclude a filename or file extension, you are telling your antivirus software to completely ignore those files anywhere on your system, which could cause a security problem. It's a much better bet to exclude a particular folder that you know is safe, like your virtual machine folders.

Always Scan Files from the Internet

I'll start by saying this should go without saying... which always seems to be said anyway... but you should make absolutely certain to scan any files that come from anywhere on the internet, and *especially* when those files come from torrents or other similar sources rife with viruses.

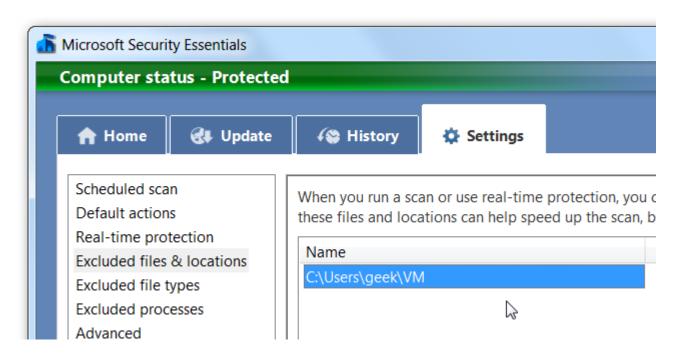
All Antivirus Applications Work Differently

The next thing to mention is that not every antivirus application is going to work the same way—for instance, by default, AVG only scans a specific set of file extensions, and files with no extensions. There's no way to tell—without benchmarking, at least—whether excluding folders will make a performance difference if they don't scan those extensions.

Some other anti-virus applications, however, don't limit themselves to specific file types, so you'll need to dig into the settings for your particular application.

Excluding Files from Microsoft Security Essentials

Microsoft Security Essentials makes it real simple to exclude files—just head into the Settings, choose Excluded files & locations on the left-hand side, and then add folders into the list on the right-hand side.



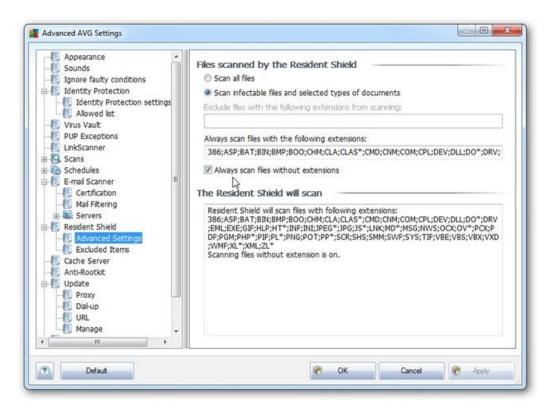
You'll probably notice that MSE doesn't slow your system down very much anyway.

Excluding Files from AVG Anti-Virus

As we mentioned earlier, AVG works a little differently—if you head into Tools -> Advanced settings...



Then head to Resident Shield -> Advanced Settings to see the list of file types that are currently being scanned. You'll notice that AVG always scans files with no extensions, which shouldn't normally pose a problem, but depending on the applications you're using there might be a problem.



You can switch to the Resident Shield -> Excluded Items to add in folders or specific files to exclude from scanning.

We're not going to cover every other antivirus application, but they all pretty much work the same. Also, we prefer Microsoft Security Essentials.

Funny Related Story



About 10 years ago, when I was still fairly new at the vaporware company I was working for at the time, the <u>ILOVEYOU worm</u> attacked our email system, crushing our Microsoft Exchange server with an overload of emails, and then the worst possible thing happened—our email server became corrupted. The IT staff ran the recovery tools, which fixed the problem and all was well... for a few hours until it became corrupted again. And again.

After a couple days of this problem, I finally popped my head in the door and asked to take a look. Sure enough, the problem became very clear within minutes.

That's right. You guessed it...

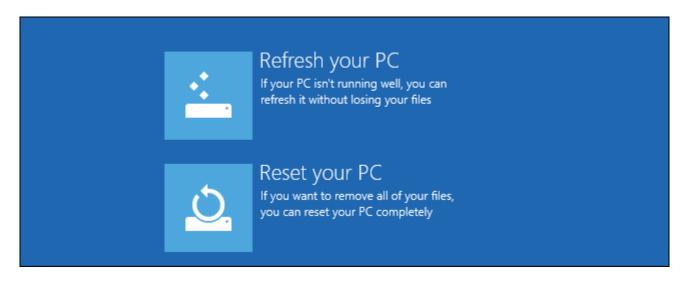
They had installed the desktop edition of Norton Antivirus on the email server, and they didn't exclude the database folder for Exchange. Virus-laden emails came into the Exchange database, and then Norton proceeded to rip them right out of the database itself, corrupting the files badly in the process.

Of course, I removed Norton and proceeded to grab a reputable antivirus plugin for Microsoft Exchange, which cleaned the emails the proper way, and all was well. Until the brilliant IT person installed Norton again. *sigh* At least I got a promotion out of it.

Wrapping Up: Use This Tip At Your Own Risk

Just to wrap up, and as we said earlier, forget that you read this article, and if you get a virus don't blame us. This especially applies if you're not really sure what you're doing—this probably isn't something you should mess with.

Everything You Need to Know About Refreshing and Resetting Your Windows 8 or 10 PC



Windows users regularly reinstall Windows (or restore from a recovery partition) to fix system problems. Windows 8 or 10 include easier-to-use "Refresh" and "Reset" options that quickly restore Windows to a fresh, factory default configuration.

Just as mobile devices have an integrated "reset to factory defaults" option, so does Windows 8 or 10. You can even create your own refresh image or access these options if your computer can't boot.

The Difference between Refresh and Reset

Windows 8 or 10 have two factory reset options, named Refresh and Reset. Both reset your computer to a fresh, factory default sate. Refresh preserves your files and installed Modern programs, while Reset removes everything on your system.

When you Refresh your PC:

- Windows will save your personal files, personalization settings, and Modern apps installed from the Windows Store.
- Windows will reset your PC settings.
- Windows will remove all installed desktop programs. A list of the removed programs will be saved to your desktop.

By resetting your computer settings and removing all desktop programs, Windows can "refresh" your PC so it's more like a fresh install without deleting your personal files.

Refresh your PC

Here's what will happen:

- · Your files and personalization settings won't change.
- Your PC settings will be changed back to their defaults.
- Apps from Windows Store will be kept.
- Apps you installed from discs or websites will be removed.
- A list of removed apps will be saved on your desktop.

When you Reset your PC, Windows will remove everything. Think of this like doing a complete Windows reinstall and formatting your hard drive.

Reset your PC

Here's what will happen:

- All your personal files and apps will be removed.
- Your PC settings will be changed back to their defaults.

Should You Refresh or Reset Your PC?

If you're experiencing problems with your computer and want to fix them, you should try refreshing your PC first. Windows will restore system files and desktop programs to their default state, saving all your important personal files (and Modern apps, if you use them.)

If you want to reset your computer to its factory default state – particularly useful if you're getting rid of the computer and want to remove your personal data, or if you just want a clean start — you should reset your PC instead.

Refresh your PC without affecting your files

If your PC isn't running well, you can refresh it without losing your photos, music, videos, and other personal files.

Get started

Remove everything and reinstall Windows

If you want to recycle your PC or start over completely, you can reset it to its factory settings.

Get started

Under the Hood

Microsoft has explained what's actually going on under the hood here. When you reset your PC:

- 1. The PC boots into Windows RE, the Windows Recovery Environment
- 2. Windows RE erases and formats the Windows partitions before installing a fresh copy of Windows 8 or 10.
- 3. The PC restarts into the new copy of Windows.

When you refresh your PC, the same steps occur. However, before erasing your Windows partition, Windows RE scans the hard drive for your files, settings, and Modern apps. It places them aside, installs a fresh copy of Windows, and puts them back where they were found.

Both refresh and reset involve a fresh installation of Windows, which is why your desktop programs aren't saved.

Note that it's always a good idea to have backup copies of your files. If something goes wrong, you wouldn't want to lose the only copy.

How to Refresh or Reset

If your computer is still working properly, you can <u>refresh or reset it from the PC Settings application within</u> Windows. For Windows 10, go to Settings, Update and Security, and then Recovery.

If your computer is not booting properly, you can refresh or reset it from the boot options menu. We've covered <u>several ways to access this menu</u>. Once you've accessed it, <u>use the Refresh your PC or Reset your PC option</u>.



Creating Your Own Refresh Image

Refreshing your PC removes all your desktop programs. If you always install some critical desktop programs, you'll have to reinstall them every time you refresh your computer. To save time, you can create a custom refresh image after installing the programs you use. They'll be saved and will come back every time you refresh your computer.

Read More: How to Create a Custom Refresh Image in Windows 8

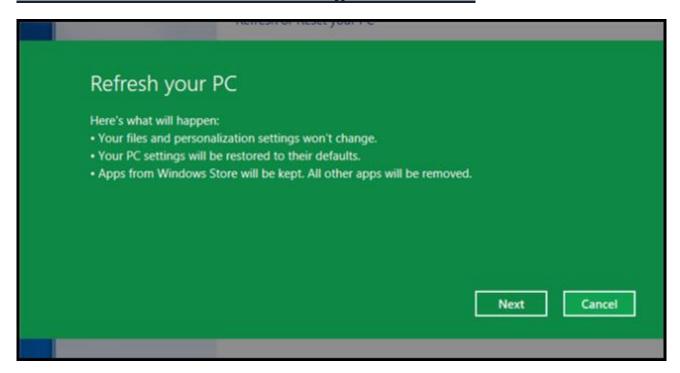
```
Administrator: Command Prompt (Admin)

C:\Windows\system32\recimg \rangle createimage C:\CustomRefreshImages\Image1 Source 0S location: C:
Recovery image path: C:\CustomRefreshImages\Image1\install.wim
Creating recovery image. Press [ESC] to cancel.
Initializing
100%
Creating snapshot
100%
Mriting image
100%
Registering image
100%
Recovery image creation and registration completed successfully.

C:\Windows\system32\rangle
```

The refresh and reset features help quickly reinstall Windows. Even for experienced users, the refresh and reset processes are faster than reinstalling Windows the old-fashioned way.

How to Create a Custom Refresh Image in Windows 8

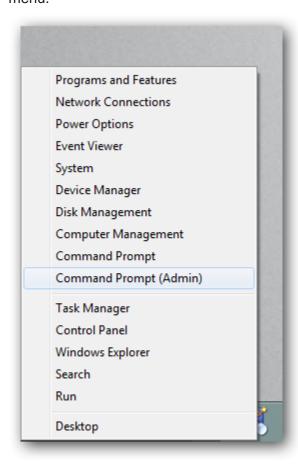


We have already shown you how to use the Refresh and Reset features in Windows 8, now we are back to show you how you can create a custom refresh image. This means next time you refresh your Windows 8 PC, you can use a custom image instead of the one that shipped with your PC.

When you refresh your PC, all of your files including Metro applications downloaded from the Windows store are kept. This is great, but unfortunately, all your non-metro applications and PC settings are removed. If you are like me and have a lot of non-metro apps this can be very annoying, but you can fix this by creating a refresh image that already has your apps installed and your settings tweaked.

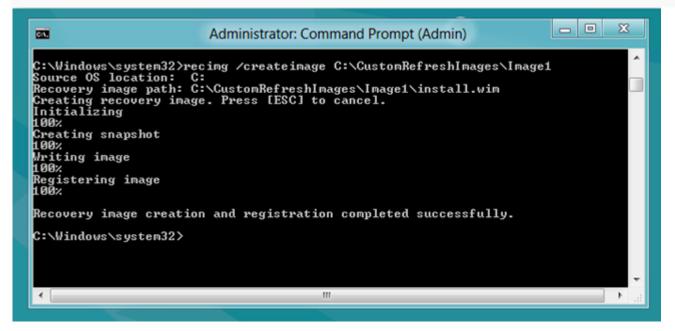
Creating A Custom Refresh Image

Right-click the bottom left corner of your screen and select Command Prompt (Admin) from the context menu.



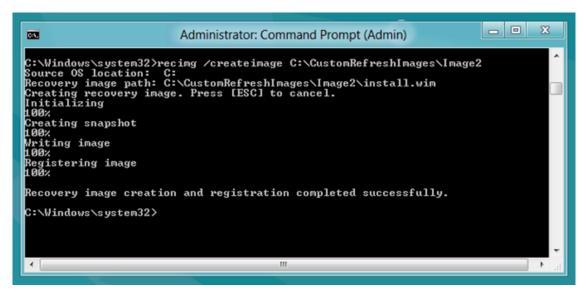
To create a custom refresh image we use the recimg.exe utility.

recimg /createimage C:\CustomRefreshImages\Image1



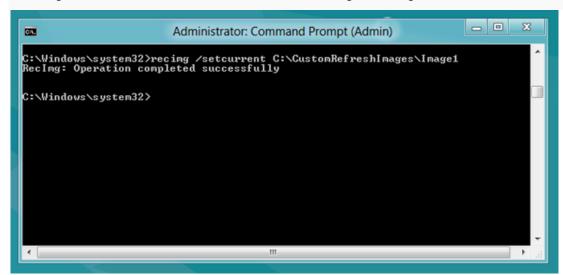
The reason we are using a subfolder on our drive is that you can actually create multiple refresh images and switch between them, to create another image we could do the following:

recimg /createimage C:\CustomRefreshImages\Image2

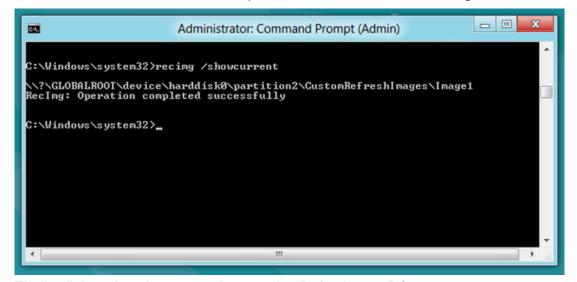


When you create an image using the /createimage parameter, the image you create is automatically set as the default refresh image. If you have multiple refresh images you can choose the active image by using the /setcurrent parameter.

recimg /setcurrent C:\CustomRefreshImages\Image1



You can also use the /showcurrent parameter to show the active image.



That's all there is to it, now you just need to Refresh your PC.