Windows 10 Privavcy Settings

Article URL
Windows 10 Privavcy Settings

Author
SecurityHome.eu

Published: 09 September 2015

Last updated on 20 September 2015.

Â

Privacy settings in the Control Panel

You access privacy settings through the Control Panel, which is now called Settings in Windows 10. (keyboard shortcut: Windows-I). Another method is to tap the Windows key, which opens the Start menu, and then click the Settings button.

Before we start flipping switches, a word of warning: although you may be tempted to disable everything that reduces your privacy, doing so may impair or disable certain apps and interactions between apps.

Clicking the Privacy button opens a window with two panes. On the left is a category list, and on the right are the settings for the category that you're looking at. In the General pane, there are four settings: advertising ID, SmartScreen, handwriting recognition, and language.

Advertising ID

identifies your Web behavior to deliver targeted ads. It works like this: if you open the Windows 10 Travel app and also the Calendar app, Microsoft can use that info to show you ads for Expedia or Southwest Airlines, for example. That's assuming the app uses ads to begin with. You won't start seeing banner ads when you open the calculator, but Microsoft Edge (which replaces Internet Explorer as your default Web browser in Windows 10) may run these tailored ads when you go to Bing or Outlook.com.
Advertising ID communicates no personal information about you. It's a sort of beacon to deliver targeted ads showing something that you might want to buy. In theory, if the ads are more relevant to you, you're more likely to click them, which helps both the advertiser and the people selling the ad space, and maybe you, too, if you get a better shopping experience. But if you prefer to disable advertising ID, you can do so in the General pane. Note that disabling it does not block ads, only Microsoft's ability to target ads.

The SmartScreen filter is a layer that Microsoft Edge and Internet Explorer use to help protect you from dangerous or suspicious websites. The filter does this in three ways.
One, it analyzes the website for questionable behaviors, like opening fake pop-up windows or redirecting you

to other websites.

Two, SmartScreen checks the Web address against a list Microsoft maintains of websites that are known to be fraudulent. SmartScreen is a helpful tool, so we recommend leaving it on.

The third setting helps improve handwriting recognition by sending Microsoft data about how you write. It doesn't send what you actually write. This setting will be grayed out if Windows 10 does not detect a stylus. Since it's not sending personally identifiable info, we don't see the harm in leaving it on.

The language setting helps websites detect which language you're using so they can deliver regional info, like maybe a Dow Jones stock ticker for users of US English or rugby scores for users of UK English. The setting also helps websites understand where its users are coming from, which can help them figure out what kind of content or user experience to create.

The Location pane

If you are using an administrator account, as you will be by default, then you will see the option to disable location info for all user accounts on that device. Below that is a toggle for the specific account that is currently logged in, which will be grayed out if location services are disabled for everyone. Location can be used to let Windows 10 apps display region-specific info like weather and sports scores, or to show you map locations and shopping choices in your area. If you disable this setting, you can still enter your location info manually -- it just won't be sent automatically.

Some apps will use your device's Bluetooth or Wi-Fi functions to determine your location even when your location setting is disabled. You can toggle that feature on and off in the Radios pane (in the list to the left). Bluetooth and Wi-Fi will still function, just without location info.

Camera and microphone

As you've probably guessed, these two sections have a toggle that disables your device's webcam and mic. You can also toggle for specific apps, including pre-installed apps designed by Microsoft and other apps . If you purchased this device from a system builder like Dell, Acer, Toshiba, or Lenovo, they may have some pre-installed apps as well.

A Windows 10 app gets camera and microphone permissions by default if it wants it, regardless of how likely it is to use it, so we recommend checking these settings periodically if you're leaving your webcam enabled. Generally, you should only give webcam and mic access when you know you'll use them in that app, such as Skype. Note that disabling your webcam and mic in Settings may not prevent malware from secretly re-enabling it. You might want to put a piece of black tape over your webcam lens when you're not using it.

Speech, inking, and typing

The speech section is where you toggle Cortana's speech recognition, among other things. Cortana is like Apple's Siri or google now, but it works on the desktop as well as on mobile devices. You can use speech recognition to dictate a text message to send to someone in your contacts list. Enabling the speech setting also improves handwriting recognition and search suggestions that are made as you type.

Contacts, Calendar, Messaging, and Radios

These next four sections work roughly the same: there's a toggle to turn the function off altogether, and a list of apps that you can toggle on an individual basis. If no apps are listed, none are asking for those permissions.

If you're not using Cortana, and if you're using Gmail and Google Hangouts instead of a Windows 10 mail app or chat app, you can probably turn all of this off without much negative impact.

Other Devices

Windows 10 tells you a little about how the functions in the Other Devices section operate. But the company doesn't say much about what those functions will actually be used for; instead, it tells you to go to each app's website and look at the app's specific settings to figure that out.
As we are not sure what it does, it is probably not a bad idea to disable it.

Feedback & Diagnostics

Feedback & Diagnostics helps Microsoft improve how Windows 10 works. The feedback function controls a small notification bubble that sometimes pops up in the lower right-hand corner of the screen, asking you to rate a particular program or function in Windows 10. Unfortunately, Microsoft has tied diagnostic and usage data together, but you can still limit sharing to basic error info by going with the Basic option. The Enhanced setting sends Microsoft info about often and how long you use certain apps but also gives the company more diagnostic info for troubleshooting and for developing system updates.

The Full setting may send Microsoft personally identifiable information, such as the contents of a document you were working on when you experienced a crash. Microsoft states that it will not use this info "to identify, contact, or target advertising to you," but the potential privacy breach is pretty serious, so we recommend not using the Full setting, even though it sends a large amount of diagnostic info that helps Microsoft improve its apps and system updates. In fact, if this device is provided by your employer, the Full setting may be forbidden by company policy. If not, it arguably should be.

Background apps

Unlike the other categories, this one does not have a global toggle; each app must be toggled individually.
If you use the Windows 10 calendar to keep track of events, then you'll probably want to let that run in the background.
We have disabled most apps, but you have to descide yourself what apps can run in the background.

Managing Wi-Fi Sense

Windows 10 does some unusual things with Wi-Fi that you should familiarize yourself with. Go back to the home window of Settings, click Network & Internet, scroll the right-hand side of the window to the bottom, and click Manage Wi-Fi Settings.

There are two important choices to make here. First is the decision to connect to suggested open hotspots. Since public Wi-Fi is a popular avenue for hackers to tamper with connected devices, we recommend leaving that off. The other setting enables network sharing. Users of Skype, Outlook.com, and Facebook can share access to their Wi-Fi network with people on their friends lists. In turn, you can share this access privilege with your friends on Facebook, Skype, and Outlook.com, depending on what boxes you check when you enable network sharing.

Note that we say "access privilege" instead of "password." Your Wi-Fi password remains unknown to others using this system. However, making access to your home Wi-Fi as shareable as a tweet is pretty inadvisable from a security perspective, so we'd recommend that you never check any of those three boxes.