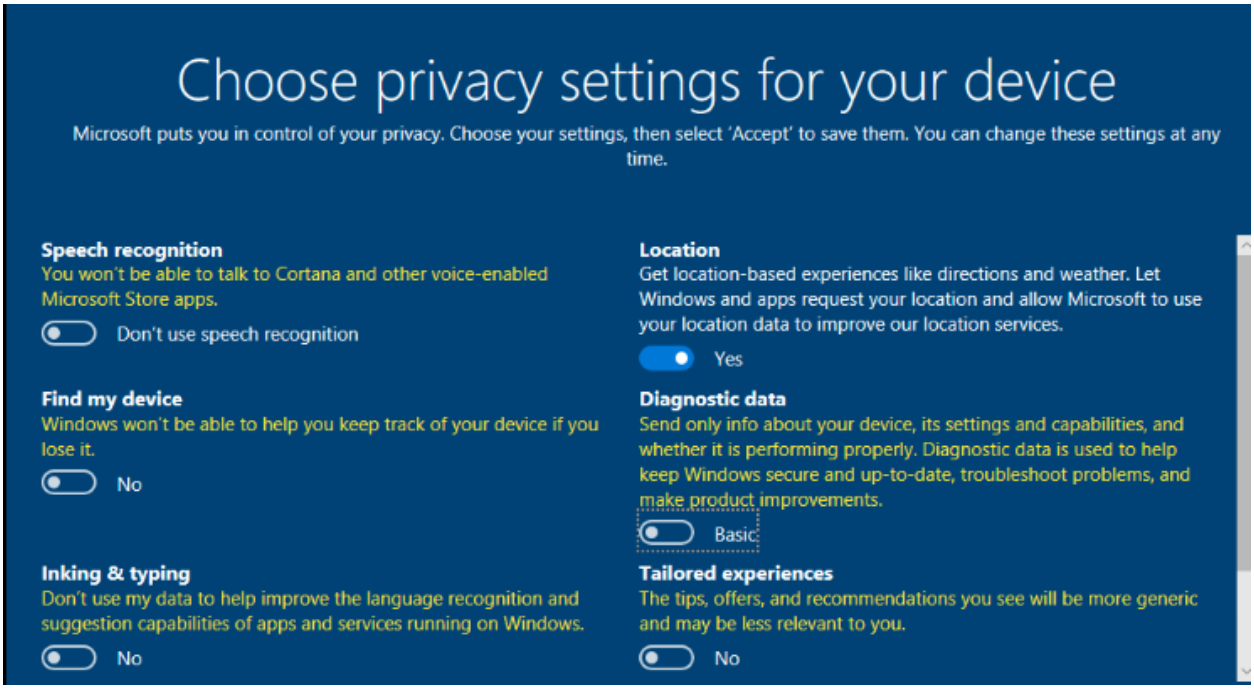
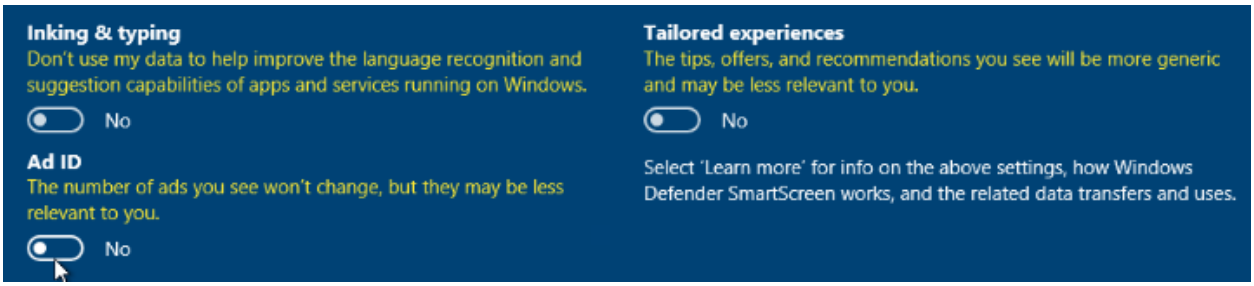
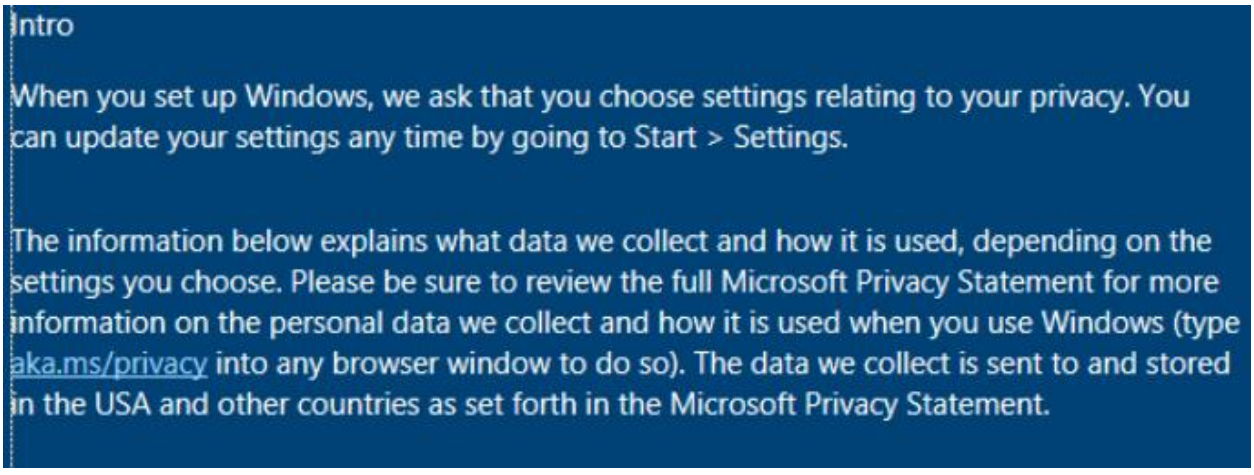

Choose privacy settings for your device
Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.
Speech recognition
You won't be able to talk to Cortana and other voice-enabled Microsoft Store apps.
Don't use speech recognition
Find my device
Windows won't be able to help you keep track of your device if you lose it.
No
Inking & typing
Don't use my data to help improve the language recognition and suggestion capabilities of apps and services running on Windows.
No
Location
Get location-based experiences like directions and weather. Let Windows and apps request your location and allow Microsoft to use your location data to improve our location services.
Yes
Diagnostic data
Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up-to-date, troubleshoot problems, and make product improvements.
Basic
Tailored experiences
The tips, offers, and recommendations you see will be more generic and may be less relevant to you.
No


Inking & typing
Don't use my data to help improve the language recognition and suggestion capabilities of apps and services running on Windows.
No
Ad ID
The number of ads you see won't change, but they may be less relevant to you.
No
Tailored experiences
The tips, offers, and recommendations you see will be more generic and may be less relevant to you.
No
Select 'Learn more' for info on the above settings, how Windows Defender SmartScreen works, and the related data transfers and uses.


Intro
When you set up Windows, we ask that you choose settings relating to your privacy. You can update your settings any time by going to Start > Settings.
The information below explains what data we collect and how it is used, depending on the settings you choose. Please be sure to review the full Microsoft Privacy Statement for more information on the personal data we collect and how it is used when you use Windows (type aka.ms/privacy into any browser window to do so). The data we collect is sent to and stored in the USA and other countries as set forth in the Microsoft Privacy Statement.

Location

The Microsoft location service provides location information to Windows devices using a combination of global positioning service (GPS), nearby wireless access points, cell towers, and your IP address, depending on the capabilities of your device.

Turning on the Location setting enables certain apps, services, and Windows features to ask for permission to access and use your location data to deliver location-aware services as precisely as your device supports. When your location is used by a location-aware app or service, your location information and recent location history are stored on your device and sent to Microsoft. This data is then processed by Microsoft to remove all personally identifiable information and used in a de-identified format to improve our location services.

If you are signed in with your Microsoft account, your last known good location information is also saved to the cloud, where it is available across your devices to other apps or services that use your Microsoft account. If you are signed in with your Microsoft account but your device cannot obtain a good location on its own (such as when you are in a building or basement), apps or services can use your last known good location that is stored in the cloud.

You can turn off the Location setting and clear your device's location history at any time by going to Start > Settings > Privacy > Location. For more information about location, click here.

Find my device

Find my device uses your device's location data to help you find your device if you lose it. Find my device allows an administrator of a Windows portable device, such as a laptop or tablet, to find the location of that device from account.microsoft.com/devices. To use this feature the administrator needs to turn on the location service for the device and sign in to Windows with a Microsoft account. This feature will work for the administrator even if other users have disabled location services for themselves. When the administrator attempts to locate the device, users will see a notification in the notification center.

You can turn this off at any time by going to Start > Settings > Update & security > Find my device. For more information about find my device, click here.

Speech recognition

Windows provides both a device-based speech recognition feature (available through the Windows Speech Recognition Desktop app) and a cloud-based speech recognition service, in regions where Cortana is available. To learn what languages and regions speech currently supports, search for "Cortana's regions and languages" in any browser or in the search bar. Turning on the Speech recognition setting allows Microsoft to collect and use your voice recordings to provide you with cloud-based speech recognition services in Cortana, in the Mixed Realty Portal, in supported Microsoft Store apps, dictation in Windows, and over time in other parts of Windows. The voice data is used in the aggregate to help improve our ability to correctly recognize all users' speech.

You can turn this off at any time in Start > Settings > Privacy > Speech, inking & typing. If you later allow Cortana to access information such as calendar and contacts data, your speech recognition experience can be personalized so that it works better for you. Note that you can always use device-based speech recognition by typing "Windows Speech Recognition" in the search bar and running the Windows Speech Recognition Desktop app. For more information about speech recognition, click here.

Diagnostics

There are two levels of diagnostic data: Basic and Full. Microsoft uses diagnostic data to keep Windows secure and up-to-date, troubleshoot problems, and make product improvements as described in more detail below. Regardless of your selection your device will be just as secure and operate normally. This data is transmitted to Microsoft and stored with one or more unique identifiers that can help us recognize an individual user on an individual device and understand the device's service issues and use patterns.

Basic diagnostic data is information about your device, its settings and capabilities, and whether it is performing properly. This the minimum level of diagnostic data needed to help keep your device reliable, secure and operating normally.

Full diagnostic data includes all data collected with Basic, along with information about the websites you browse, how you use apps and features, plus additional information about device health, device usage and enhanced error reporting. At Full, Microsoft also collects the memory state of your device when a system or app crash occurs (which may unintentionally include parts of a file you were using when a problem occurred). While your device will be just as secure and operate normally if you choose the Basic level of diagnostics, the additional information we collect at Full makes it easier for us to identify and fix issues and make product improvements that benefit all Windows users.

Some of the data described above may not be collected from your device even if your diagnostic data setting is set to Full. Microsoft minimizes the volume of data we collect from all devices by collecting some of the data at the Full level from only a small percentage of devices (sample). By running the Diagnostic Data Viewer tool, you can see an icon which indicates whether your device is part of a sample and also which specific data is collected from your device. Instructions for how to download the Diagnostic Data Viewer tool can be found at Start > Settings > Privacy > Diagnostics & feedback.

Specific data items collected in Windows diagnostics are subject to change to give Microsoft flexibility to collect the data needed for the purposes described. For example, to ensure Microsoft can troubleshoot the latest performance issue impacting users' computing experience or update a Windows 10 device that is new to the market, Microsoft may need to collect data items that were not collected previously. For a current list of data types collected at both levels of diagnostics, see https://go.microsoft.com/fwlink/?linkid=865126 or see https://go.microsoft.com/fwlink/?linkid=865125 for the current list of data collected at Basic.

We use Basic diagnostic data to keep Windows devices up-to-date. Microsoft uses:

Basic error information to help determine whether problems your device is experiencing can be addressed by the update process;

Information about your device, its settings and capabilities, including applications and drivers installed on your device, to ascertain whether your device is ready for and compatible with the next operating system or app release and ready for update;

Logging information from the update process itself to understand how well your device's updates are proceeding through the stages of downloading, pre-installation, post-installation, post-reboot and setup;

Data about the performance of updates on all Windows devices to assess the success of an update's deployment and to learn device characteristics (e.g., hardware, peripherals, settings and applications) that are associated with the success or failure of an update; and

Data about which devices have had upgrade failures and why to determine whether to offer the same upgrade again.

We use both levels of diagnostic data (Basic and Full) to troubleshoot issues to help keep Windows, and related products and services, reliable and secure.

Microsoft uses Basic data to:

Comprehend the immense number of hardware, system and software combinations customers use;

Analyze issues based on specific hardware, system and software combinations and identify where problems or issues occur with a specific or limited set of devices;

Determine whether an app or process experiences a performance issue (e.g., the app crashes or hangs) and when a crash-dump file is created on the device (crash dumps themselves are collected at Full); and

Understand the effectiveness and fix problems with the diagnostic transmission system itself.

Microsoft uses the additional data collected at Full to help spot and fix problems more quickly. We use:

Information about app usage to understand what the user was doing in an app that caused a problem in conjunction with what we learn about the impact of other apps or processes running on a device;

Information about device health, such as battery level or how quickly applications respond to input, to better understand the data we collect about application performance issues and make corrections; and

Information contained in enhanced error reporting and crash dumps to better understand the data related to the specific conditions under which an error or crash occurred.

We use the Basic level of diagnostic data to improve Windows. We use the Full level of diagnostic data to improve Windows and related products and services.

Microsoft uses Basic data for product improvement in the context of keeping your Windows device up-to-date and secure; problem-solving; accessibility; reliability; performance; enhancing existing Windows features; compatibility of apps, drivers, and other utilities; privacy; and energy efficiency.

Microsoft uses Basic data for this purpose as follows:

Information about customers' devices, peripherals, and settings (and their configurations) is used to prioritize product improvements by determining which improvements will have the greatest positive impact to the most Windows 10 users; and

Information about which apps are installed on devices is used to prioritize app-compatibility testing and feature improvements for the most popular apps.

Additional data collected at Full is used to help make even more meaningful improvements to Windows and related products and services:

App usage information helps us prioritize app-compatibility testing and make feature improvements to apps and features that are used the most;

Information about the impact of device characteristics, configuration and app usage on device health (for example on battery life) is used to analyze and make changes that improve the performance of Windows devices; and

Aggregate information about browsing history in Microsoft browsers is used to tune Bing's search algorithms to provide more effective search results.

We don't use any Windows diagnostic data to provide personalized experiences or promote products or services to you unless you let us do so with the separate Tailored experiences setting with diagnostic data (described below).

You can adjust your diagnostic data collection level at any time in Start > Settings > Privacy > Feedback & diagnostics. For more information about diagnostics, click here.

Inking and Typing recognition

If you choose to send data to Microsoft to improve inking and typing recognition, Microsoft will collect samples of the content that you type or write to improve features such as handwriting recognition, autocompletion, next word prediction and spelling correction in the many languages used by Windows customers. When Microsoft collects Inking and Typing diagnostic data, it is divided into small samples and processed to remove unique identifiers, sequencing information, and other data (such as email addresses and numeric values) which could be used to reconstruct the original content or associate the input to the user.

You can turn this off at any time in Start > Settings > Privacy > Diagnostics & feedback. For more information about Inking and typing data, click here.

Tailored experiences with diagnostic data

If you choose to turn on tailored experiences, we will use your Windows diagnostic data (Basic or Full as you have selected) to offer you personalized tips, ads and recommendations to enhance Microsoft products and services for your needs. If you have selected Basic as your diagnostic data setting, personalization is based on information about your device, its settings and capabilities, and whether it is performing properly. If you have selected Full, personalization is also based on information about the websites you browse, how you use apps and features, plus additional information about device health. However, we do not use the content of crash dumps for personalization when we receive such data from users who have selected Full.

Tailored experiences include suggestions on how to customize and optimize Windows; and recommendations for and offers of Microsoft and third-party products and service, features, apps, and hardware for your Windows experiences. For example, to help you get the most out of your device, we may tell you about features you may not know about or that are new. If you are having a problem with your Windows device, you may be offered a solution. You may be offered a chance to customize your lock screen with pictures, or to be shown more pictures of the kind you like, or fewer of the ones you don't. If you stream movies in your browser, you may be recommended an app from the Microsoft Store that streams more efficiently. Or, if you are running out of space on your hard drive, Windows may recommend you try OneDrive or purchase hardware to gain more space.

You can turn this off at any time in Start > Settings > Privacy > Diagnostics & feedback. For more information about tailored experiences with diagnostic data, click here.

Relevant ads

Windows generates a unique advertising ID for each user on a device, which application developers and advertising networks can use to provide more relevant advertising in apps. When the advertising ID is enabled, apps can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. Thus, app developers (and the advertising networks they work with) can associate personal data they collect about you with your advertising ID and use that personal data to provide more relevant advertising and other personalized experiences across their apps.

You can turn this off at any time in Start > Settings > Privacy. Please note that turning advertising ID off will not reduce the number of ads you see, but it may mean that ads are less interesting and relevant to you. Turning it back on will reset the advertising ID. For more information about relevant ads, click here.

Windows Defender SmartScreen

Windows Defender SmartScreen sends data to Microsoft about the websites you visit and files you download to warn you and help protect you and your device from unsafe web content or malicious software. Since we strive to protect you when using our services and those of third parties, we turn Windows Defender SmartScreen on by default.

You can turn Windows Defender SmartScreen off at any time by going to Start > Windows Defender Security Center > App & browser control. For more information about Windows Defender SmartScreen, click here.