For up-to-date information on Microsoft's data processing practices, please review the Microsoft Privacy Statement. Here you can also learn about the latest tools we provide to access and control your data and how to contact us if you have a privacy inquiry.

Windows 8 and Windows Server 2012 Privacy Statement

Last updated: **August 2012**

These highlights of the full Windows 8 and Windows Server 2012 Privacy Statement ("Windows Privacy Statement") explain at a high level some of the data collection and use practices of Windows 8 and Windows Server 2012 ("Windows"). They focus on features that communicate with the Internet and aren't intended to be an exhaustive description. They don't apply to other online or offline Microsoft sites, products, or services.

This privacy statement has four sections:

- Highlights (this page)
- Statement, which is the full Windows Privacy Statement that includes links for Windows features that have their own standalone statements
- Features Supplement, which describes the features that have privacy impact in Windows 8 and Windows Server 2012
- Server Supplement, which describes the additional features that have privacy impact in Windows Server 2012

For more information on how to help protect your personal computer, your personal information, and your family online, visit our Safety and Security Center.

Your information

- Certain Windows features may ask you for permission to collect or use information from your PC, including personal information. Windows uses this information as outlined in the full Windows Privacy Statement, as well as in the Features Supplement and the Server Supplement.
- Some Windows features can, with your permission, share personal information over the Internet.
- If you choose to register your software, you'll be asked to provide personal information.
- Windows requires activation to reduce software piracy and help ensure that our customers receive the software quality they expect. Activation sends some information about your PC to Microsoft.
- You can choose to sign in to Windows with a Microsoft account, which lets you sync Windows settings and automatically sign in to apps and websites. When you create a Microsoft account, you'll be asked to provide some personal information.
- Additional details

Top of Page

Your choices

- Windows offers you a variety of ways to control how Windows features transfer information over the Internet. More information about how to control these features is in the Features Supplement and the Server Supplement.
- To help improve your experience, some features that use the Internet are turned on by default.

- Additional details

Top of Page

Uses of information

- We use the information collected to enable the features you're using or provide the services you request. We also use it to improve our products and services. In order to help provide our services, we occasionally provide information to other companies that work on our behalf. Only companies who have a business need to use the information are provided access to them. These companies are required to keep this information confidential and are prohibited from using it for any other purpose.

- Additional details

Top of Page

How to contact us

For more information about our privacy practices, go to the full Windows Privacy Statement . Or, you can write to us using our web form.

Top of Page

For up-to-date information on Microsoft's data processing practices, please review the Microsoft Privacy Statement. Here you can also learn about the latest tools we provide to access and control your data and how to contact us if you have a privacy inquiry.

Windows 8 and Windows Server 2012 Privacy Statement

Highlight | Statement | Features Supplement | Server Supplement

In this page

This statement covers Windows 8 and Windows Server 2012 ("Windows"). Certain Windows components have their own privacy statements, which are listed on the right side of this page. Privacy statements for software and services related to Windows and for prior releases are also listed there.

For information about specific features, please refer to the Features Supplement and Server Supplement.

This is a statement that focuses on features that communicate with the Internet and isn't intended to be an exhaustive list.

Collection and use of your information

The personal information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to enable the features you use and provide the services or carry out the transactions you have requested or authorized. The information may also be used to analyze and improve Microsoft products and services.

Except as described in this statement, personal information you provide won't be transferred to third parties without your consent.

We occasionally hire other companies to provide limited services on our behalf, such as for performing statistical analysis of our services. We will only provide those companies the personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Microsoft may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the software; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers, or the public.

Information collected by or sent to Microsoft by Windows 8 may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union, the European Economic Area, and Switzerland.

Top of Page

Collection and use of information about your computer

When you use software with Internet enabled features, information about your computer ("standard computer information") is sent to the websites you visit and online services you use. Standard computer information typically includes information such as your IP address, operating system version, browser version, and regional and language settings. In some cases, it may also include a hardware ID, which indicates the device manufacturer, device name, and version. If a particular feature or service sends information to Microsoft, standard computer information will be sent as well.

The privacy details for each Windows 8 feature in the Features Supplement and Server Supplement, as well as the features listed on the side of this page, describe what additional information is collected and how it is used.

Administrators can use Group Policy to modify many of the settings for the features described below. For more information, see this white paper for administrators.

Top of Page

Security of your information

Microsoft is committed to helping protect the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. For example, we store the information you provide on computer systems with limited access, which are located in controlled facilities. When we transmit highly confidential information (such as a credit card number or password) over the Internet, we protect it through the use of encryption, such as the Secure Socket Layer (SSL) protocol.

Top of Page

Changes to this privacy statement

We will occasionally update this privacy statement to reflect changes in our products, services, and customer feedback. When we post changes, we will revise the "last updated" date at the top of this statement. If there are material changes to this statement or in how Microsoft will use your personal information, we will notify you either by posting a notice of such changes prior to implementing the change or by directly sending you a notification. We encourage you to periodically review this statement to be informed of how Microsoft is protecting your information.

Top of Page

For more information

Microsoft welcomes your comments regarding this privacy statement. If you have questions about this statement, or believe that we haven't adhered to it, you can write to us using our web form.

Microsoft Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
USA

Top of Page

For up-to-date information on Microsoft's data processing practices, please review the Microsoft Privacy Statement. Here you can also learn about the latest tools we provide to access and control your data and how to contact us if you have a privacy inquiry.

Windows 8 and Windows Server 2012 Privacy Statement

In this page

Last updated: August 2012

Note that this page is a supplement to the Windows 8 and Windows Server 2012 Privacy Statement ("Windows Privacy Statement"), which has four sections:

- Highlights
- Statement, which is the full Windows Privacy Statement , and includes links to privacy statements for Windows features that have their own standalone statements
- Features Supplement (this document), which describes the features that have privacy impact in Windows 8 and Windows Server 2012
- Server Supplement, which describes the additional features that have privacy impact in Windows Server 2012

To understand the data collection and use practices relevant for a particular feature or service of Windows, you should read the full Privacy Statement and any applicable supplement or standalone statement.

Handwriting personalization—automatic learning

HomeGroup

Input Method Editor (IME)

Installation Improvement Program

Internet printing

Language preferences

Location services

Name and account picture

Network Awareness

Notifications, Lock Screen Apps, and Tile Updates

Order prints

Program Compatibility Assistant

Properties

Proximity

Remote Access connections

RemoteApp and Desktop Connections

Remote Desktop connection

Sign in with a Microsoft account

Activation

What this feature does

Activation reduces software counterfeiting, which helps ensure that Microsoft customers receive the software quality they expect. Once your software is activated, a specific product key becomes associated with the PC (or the hardware) on which your software is installed. This association prevents the product key from being used to activate the same copy of the software on multiple PCs. Some changes to your PC components or the software might require you to reactivate the software. Some changes to your PC hardware or software might require you to reactivate Windows. Activation can detect and disable activation exploits (software that circumvents or bypasses software activation). If an activation exploit is present, a software or hardware vendor might have tampered with genuine Microsoft software in order to create counterfeit copies of the software. Activation exploits may interfere with the normal operation of your system.

Information collected, processed, or transmitted

During activation, the following information is sent to Microsoft:

- The Microsoft product code (a five-digit code that identifies the Windows product you are activating).
- A channel ID or site code that identifies how the Windows product was originally obtained. For example, a channel ID or site code identifies whether the product was originally purchased from a retail store, obtained as an evaluation copy, obtained through a volume licensing program, or pre-installed by a PC manufacturer.
- The date of installation, and whether the installation was successful.
- Information that helps confirm that your Windows product key hasn't been altered.
- PC make and model.
- Version information for the operating system and software.

Sync your settings

Teredo Technology

Trusted Platform Module (TPM) Services

Update Root Certificates

Update services

Windows Customer Experience Improvement Program (CEIP)

Windows Defender

Windows Error Reporting

Windows File Association

Windows Help

Remote Assistance

Windows Search

Windows Share

Windows SmartScreen

Windows Speech Recognition

Windows Store

Windows Time Service

Windows Troubleshooting

- Region and language settings.
- A unique number called a Globally Unique Identifier (GUID) assigned to your PC.
- Product Key (hashed) and Product ID.
- BIOS name, revision number, and revision date.
- Hard drive volume serial number (hashed).
- The result of the activation check. This includes error codes and the following information about any activation exploits and related malicious or unauthorized software found or disabled:
  - The activation exploit's identifier.
  - The activation exploit's current state, such as cleaned or quarantined.
  - PC manufacturer's identification.
  - The activation exploit's file name and hash, as well as a hash of related software components that may indicate the presence of an activation exploit.
- The name and a hash of the contents of your PC's start-up instructions file. If your Windows license is on a subscription basis, information will also be sent about how your subscription works. Standard computer information is sent as well, but your PC's IP address is only retained temporarily.

Use of information

Microsoft uses the information to confirm that you have a licensed copy of the software. Microsoft doesn't use the information to contact individual consumers.

Choice and control

Activation is required and occurs automatically while you set up Windows. If you don't have a valid license for the software, you won’t be able to activate Windows.

Top of Page

Active Directory Rights Management Services (AD RMS) Client

What this feature does

Active Directory Rights Management Services (AD RMS) Client is information-protection technology that works with AD RMS enabled apps to help safeguard digital information from unauthorized use. Owners of digital information can define how recipients use the information contained in a file, such as who can open, modify, print, or take other actions with the file. In order to create or view a file with restricted permissions, your PC must be running an AD RMS enabled app and have access to an AD RMS server.

Information collected, processed, or transmitted

AD RMS uses your email address to identify you to an AD RMS server. As a result, your email address is stored on the server, and on your PC in licenses and identity certificates created by the server. Identity certificates and licenses are transferred to and from AD RMS servers when you attempt to open, print, or perform other actions on a document protected by rights management. If your PC is connected to an enterprise network, the AD RMS server is typically operated by the enterprise. If you're using Windows Live AD RMS services, the server is operated by Microsoft. To help protect your privacy, information that is sent to Microsoft AD RMS servers is encrypted.

Use of information

The license allows you to access protected files. The identity certificates are used to identify you to an AD RMS server, and allow you to protect files and to access protected files.

Choice and control

AD RMS features must be enabled through an AD RMS-capable app. By default, they aren’t enabled. You can choose to not enable or use them. However, if you don’t enable them, you won’t be able to access protected files.

Top of Page

Audit

Audit allows an administrator to configure Windows to record operating system activity in a security log that can be accessed using the Event Viewer and other apps. This log can help an administrator detect unauthorized access to the PC or resources on the PC. For example, this log can help administrators troubleshoot problems and determine whether someone has signed in to the PC, created a new user account, changed a security policy, or opened a document.

Information collected, processed, or transmitted

Administrators determine what information is collected, how long it is retained, and whether it is transmitted to other parties. The information might include personal information, such as user names or file names. For more information, contact your administrator. No information is sent to Microsoft.

Use of information

Administrators also determine how the audit information is used. Generally, the security log is used by auditors and administrators to track PC activity or to identify unauthorized access to the PC or resources on the PC.

Choice and control

Administrators determine whether this feature is enabled and how users are notified. Other users can't view the security log unless the administrator allows them to access it. You can configure Audit on your PC by opening Local Security Policy in Administrative Tools.

Top of Page

BitLocker Drive Encryption

What this feature does

BitLocker Drive Encryption helps protect your data by encrypting it, which can help prevent an unauthorized user from accessing your data. When BitLocker is enabled on a supported drive, Windows encrypts the data on the drive.

Information collected, processed, or transmitted

When BitLocker is enabled using software encryption, cryptographic keys in memory continually encrypt and decrypt data as it is read from or written to the protected drive. When BitLocker is enabled using hardware encryption, data encryption and decryption is performed by the drive.

During BitLocker setup, you can choose to print a recovery key or save it to a location on your network. If you set up BitLocker on a non-removable drive, you can also save your recovery key to a USB flash drive.

If your PC isn't joined to a domain, you can back up your BitLocker recovery key, recovery key ID, and computer name to OneDrive. To help protect your privacy, the information is sent encrypted via SSL.

You can set up BitLocker to encrypt data using a certificate stored on a smart card. When you protect a data drive using a smart card, the public key and unique identifier for the smart card are stored unencrypted on the drive. This information can be used to locate the certificate that was originally used to generate the smart card's encryption certificate.

If your PC has security hardware with at least version 1.2 of the Trusted Platform Module (TPM), BitLocker uses the TPM to provide hardware-enhanced data protection for the drive on which Windows is installed. For more information, see the Trusted Platform Module (TPM) Services section. On TPM-equipped PCs, you can also set up a personal identification number (PIN) to help add an extra layer of protection for your encrypted data. BitLocker will store this TPM-based PIN in a hashed and encrypted form on the drive.

Information collected by BitLocker isn't sent to Microsoft unless you choose to back up your recovery key to OneDrive.

Use of information

Cryptographic keys and globally unique identifiers (GUIDs) are stored in PC memory to support BitLocker operations. BitLocker recovery information allows you to access your protected data in case of hardware failures and other problems. This recovery information allows BitLocker to distinguish between authorized and

unauthorized users.

Microsoft doesn't use your individual recovery keys for any purpose. When recovery keys are sent to OneDrive, Microsoft might use aggregate data about them to analyze trends and help improve our products and services.

Choice and control

By default, BitLocker is turned off. On a removable drive, any user can turn BitLocker on or off at any time by opening BitLocker Drive Encryption in Control Panel. An administrator can turn BitLocker on or off for all drives.

If you have chosen to back up your recovery key to OneDrive, you can access or delete that key here.

Top of Page

Device discovery and setup

Windows has several features that help you discover and set up devices on your PC, including Device installation, Mobile broadband device installation, Network discovery and Wireless device pairing.

Device installation

What this feature does

When a new device is installed on your PC, Windows can automatically search for, download, and install the device's driver software. Windows can also download information about the device, such as a description, picture, and manufacturer logo. Some devices, including certain printers, webcams, mobile broadband devices, and portable devices that sync with Windows, have an app to better enable the device’s functionality and user experience. If the device’s manufacturer has provided an app for the device, Windows can automatically download and install that app from the Windows Store if you are signed in to the Store.

Information collected, processed, or transmitted

When Windows searches for drivers, it will first check to see if an appropriate driver is already available on your PC. If not, Windows

will contact the Windows Update service online to find and download device drivers. For more about the information collected by Windows Update and how it's used, see the Update Services Privacy Statement.

To retrieve information about your device and determine whether an app is available for it, Windows sends data about the device to Microsoft, including its Device ID (for example, Hardware ID or Model ID of the device you are using), your region and language, and the date that the device information was last updated. If information or a device app is available, Windows downloads and installs it from the Windows Store. The app will be available in your Windows Store account in the list of apps you've downloaded.

Use of information

The information sent to Microsoft is used to help determine and download the appropriate device driver, information, and app for your device. Microsoft doesn't use the information to identify, contact, or target advertising to you.

Choice and control

If you choose express settings while setting up Windows, you turn on automatic downloading and installation of device drivers, information, and apps. If you choose to customize settings, you can control automatic downloading and installation of device drivers, apps and info by selecting **Automatically get device drivers, apps, and info for new devices** under Help protect and update your PC. After setting up Windows, you can change these settings in Control Panel by selecting Change device installation settings, and then selecting **No, let me choose what to do**.

You can uninstall a device app at any time without uninstalling the device, though you might need the app to use certain features of the device. You can reinstall a device app after you've uninstalled it by going to the list of apps you own in the Windows Store.

Mobile broadband device installation

What this feature does

If your PC has mobile broadband hardware provided by certain mobile operators, Windows can automatically download and install

an app that lets you manage your account and data plan with the mobile operator that provided your PC's mobile broadband hardware. Additional device information is also downloaded to help display your mobile broadband connection in network lists.

Information collected, processed, or transmitted

To determine which device information and app to download, Windows sends a portion of the hardware identifiers from your mobile broadband hardware that allows us to identify your mobile operator. To help protect your privacy, Windows doesn't send the full mobile broadband hardware identifiers to Microsoft.

If your mobile operator has provided an app to Microsoft, Windows downloads it from the Windows Store and installs it. When you open the app after it's installed, it will have access to your mobile broadband hardware, including unique hardware identifiers that the mobile operator can use to identify your account.

Use of information

Microsoft uses the part of your mobile broadband hardware's identifier that Windows sends to determine which carrier's app to install on your computer. Once installed, the app can use your mobile broadband hardware IDs. For example, a mobile operator's app might use those identifiers to look up account and plan information online. The app's use of this information will be subject to your mobile operator's privacy practices.

Choice and control

If you choose express settings while setting up Windows for the first time, Windows will automatically check for and download mobile operator apps. You can turn this feature on and off in Control Panel. For more information, see the Device Installation section above.

You can uninstall a mobile operator's app at any time without uninstalling your mobile broadband hardware.

Network discovery

What this feature does

When you connect your PC to a small private network like you might have at home, Windows can automatically discover other PCs and

shared devices on the network, and make your PC visible to others on the network. When shared devices are available, Windows can automatically connect to and install them. Examples of shared devices include printers and media extenders, but not personal devices like cameras and mobile phones.

Information collected, processed, or transmitted

When you enable sharing and connecting to devices, information about your PC, such as its name and network address, might be broadcast over the local network to allow other PCs to discover and connect to it.

In order to determine if devices connected to your network should be installed automatically, some information about the network is collected and sent to Microsoft. This information includes the number of devices on the network, the network type (for example, private network), and the types and model names of devices on the network. No personal information, such as network name or password, is collected.

Depending on your device installation settings, when Windows installs shared devices, Windows might send some information to Microsoft and install device software on your PC. For more information, see the Device Installation section.

Use of information

The information sent to Microsoft about your network is used to determine which devices on the network should be installed automatically. Microsoft doesn't use the information to identify, contact, or target advertising to you.

Choice and control

If you choose enable sharing and connect to devices when you join a network, network discovery is turned on for that network. You can change this setting for your current network by clicking the network type listed under the network's name in Network and Sharing Center.

You can choose whether to enable network discovery at all and whether to enable automatic setup of network connected devices by

selecting **Change advanced sharing settings** in Network and Sharing Center.

Wireless device pairing

What this feature does

Windows allows you to pair your PC with wireless devices that use Bluetooth or Wi–Fi Direct. Wi–Fi Direct is a wireless technology that allows devices to communicate directly with each other, without needing to connect to a Wi–Fi network.

Information collected, processed, or transmitted

When you select **Allow Bluetooth devices to find this PC in Bluetooth Settings**, Windows broadcasts your PC's name over Bluetooth to allow Bluetooth enabled devices to detect and identify your PC.

When you select **Add a device** in Devices in PC settings, Windows broadcasts your PC's name over Wi–Fi to allow Wi–Fi Direct enabled devices to detect and identify it. When you close **Add a device**, Windows stops broadcasting your PC's name over Wi–Fi.

Depending on your device installation settings, when Windows pairs with wireless devices, Windows might send some information to Microsoft and install device software on your PC. For more information, see the Device Installation section above.

Use of information

Windows broadcasts your PC's name to allow other devices to identify and connect to your PC. Your PC's name isn't sent to Microsoft.

Choice and control

To change whether Windows broadcasts your PC's name using Bluetooth, press and hold or right-click your PC in Devices and Printers in Control Panel, select **Bluetooth settings**, and then select **Allow Bluetooth devices to find this PC**. If you don't want Windows to broadcast your PC's name over Wi–Fi while adding devices, temporarily disable Wi–Fi in Wireless in PC settings before you add a device.

Top of Page

DirectAccess

What this feature does

DirectAccess enables your PC to remotely and seamlessly connect to your workplace network whenever your PC is connected to the Internet, no matter your location.

Information collected, processed, or transmitted

Each time you start your PC, DirectAccess will attempt to connect to your workplace network, whether or not you're physically located at your workplace. Once connected, your PC will download workplace policy, and you'll be able to access configured resources in the workplace network. Your workplace administrator might leverage DirectAccess connectivity to remotely manage and monitor your PC, including the websites you visit even when you aren't physically located at your workplace.

DirectAccess doesn’t send any information to Microsoft.

Use of information

Your company’s policies determine how the information collected by your workplace administrator is used.

Choice and control

DirectAccess must be configured by your workplace administrator using Group Policy. While your administrator can allow you to temporarily deactivate some elements of DirectAccess, only your workplace administrator can stop Windows from attempting to connect to your workplace for management purposes. If you or your workplace administrator removes your PC from your workplace domain, DirectAccess will no longer be able to connect.

Top of Page

Dynamic update

What this feature does

Dynamic Update enables Windows to perform a one-time check with Windows Update to get the latest updates for your PC while Windows is being installed. If updates are found, Dynamic Update automatically downloads and installs them so your PC is up to date the first time that you sign in or use it.

Information collected, processed, or transmitted

To install compatible drivers, Dynamic Update sends information to Microsoft about your PC's hardware. The types of updates Dynamic Update can download to your PC include:

- **Installation updates.** Important software updates for installation files to help ensure a successful installation.
- **In-box driver updates.** Important driver updates for the version of Windows that you're installing.

Use of information

Dynamic Update reports information to Microsoft about your PC's hardware to help identify the correct drivers for your system. For more information about how information collected by Dynamic Update is used, see the Update Services Privacy Statement.

Choice and control

When you begin installing Windows, you'll be asked whether you would like to go online to install updates.

Top of Page

Ease of Access Center

What this feature does

The Ease of Access Center enables you to turn on accessibility options and settings to help you more easily interact with the PC.

Information collected, processed, or transmitted

If you use this feature, you'll be asked to select appropriate statements.

These statements include:

- Images and text on TV are difficult to see.
- Lighting conditions make it difficult to see images on my monitor.
- I don’t use a keyboard.
- I am blind.
- I am deaf.
- I have speech impairment.

This information is saved in a non-human-readable format and stored locally on your PC.

Use of information

A set of configuration recommendations are provided to you based on the statements that you choose. This information isn’t sent to Microsoft and isn’t available to other users except you and administrators on your PC.

Choice and control

You can choose which statements you would like to select by going to Ease of Access in Control Panel. You can alter your choices at any time. You can also choose which of the recommendations you want to configure on your PC.

Top of Page

Event Viewer

What this feature does

PC users, primarily administrators, can use Event Viewer to view and manage event logs. Event logs contain information about hardware, software, and security events on your PC. You can also get information from Microsoft about events in the event logs by clicking Event Log Online Help.

Information collected, processed, or transmitted

Event logs contain event information generated by all users and

apps on the PC. By default, all users can view event log entries; however, administrators can choose to restrict access to event logs. You can access the event logs for your PC by opening Event Viewer. To learn how to open Event Viewer, see Windows Help and Support.

If you use Event Log Online Help to look up additional information about a specific event, information about the event is sent to Microsoft.

Use of information

When you use Event Log Online Help to look up information about an event, the event data sent from your PC is used to locate and provide you with additional information about the event. For Microsoft events, the event details will be sent to Microsoft. Microsoft doesn't use this information to identify, contact, or target advertising to you. For events associated with third-party apps, the information will be sent to the location specified by the third-party publisher or manufacturer. If you send information about events to third-party publishers or manufacturers, use of the information will be subject to each third party's privacy practices.

Choice and control

Administrators can choose to restrict access to Event Viewer logs. Users who have full access to event viewer logs can clear them. Unless you have previously consented to sending event information automatically when you click Event Log Online Help, you'll be asked to confirm that the information presented to you can be sent over the Internet. No event log information will be sent over the Internet unless you consent to send it. Administrators can use Group Policy to select or change the site to which event information is sent.

Top of Page

Family Safety

What this feature does

Family Safety helps parents protect their children when they use a PC. Parents can control which apps, games, and websites children are allowed to use. Parents can also set time limits and receive regular activity reports via email. Parents can manage restrictions

and view activity reports locally on the PC or online using the Microsoft Family Safety website.

Information collected, processed, or transmitted

Family Safety settings and reports of children's activity are stored on your PC. Activity reports can include info about time spent using the computer, time spent in individual apps and games, and websites visited (including attempts to view blocked sites). Administrators on the PC can change settings and view the activity report.

If online management is enabled for a child account, parents can view the child's activity report and change their settings on the Microsoft Family Safety website. A parent can allow other people to view activity reports and change settings by adding them as parents on the Microsoft Family Safety website. If the parent configuring Family Safety is signed into Windows with a Microsoft account, online management is automatically enabled.

When Family Safety is configured for a child account with online management enabled, weekly reports of the child's activity will automatically be emailed to the parent.

Use of information

Windows and the Microsoft Family Safety website use the information collected to provide the Family Safety feature. Microsoft may analyze activity log information in aggregate for data quality purposes, but we don't use this information to identify, contact, or target advertising to individual users.

Choice and control

Family Safety is turned off by default. You can access Family Safety by opening Family Safety in Control Panel. Only administrators can turn on Family Safety, and only users without administrative privileges can be monitored or restricted. Children can see their settings but can't change them. If Family Safety is turned on, the child will receive a notification that Family Safety is monitoring their account each time they sign in to Windows. If you indicate that an account is a child account during account creation, you can choose to enable Family Safety for that account.

If the administrator setting up a child's account is signed into Windows with a Microsoft account, online management is automatically enabled, and reports about the child's activity will be sent weekly. Parent accounts can be added or removed on the Microsoft Family Safety website. Anyone added as a parent on the website can view a child's activity report and change the child's Family Safety settings, even if the parent isn't an administrator on the PC the child uses.

To properly use Family Safety, only parents should be administrators of their PC, and children should not be granted administrative privileges. Please note that using this feature to monitor other users (such as adults) may violate applicable law.

Top of Page

Fax

What this feature does

The fax feature allows you to create and save fax cover pages, and to send and receive faxes using your PC and an external or a built-in fax modem or a fax server.

Information collected, processed, or transmitted

Information collected includes any personal information entered on a fax cover page, as well as identifiers contained within industry standard fax protocols such as Transmitting Subscriber ID (TSID) and Call Subscriber ID (CSID). By default, Windows uses "Fax" as the value for each identifier.

Use of information

Information entered in the sender dialog box is presented on the fax cover page. Identifiers such as the TSID and CSID might contain arbitrary text and are typically used by the receiving fax machine or PC to identify the sender. No information is sent to Microsoft.

Choice and control

Fax access is determined by your user account privileges on the PC. Unless a fax administrator changes access settings, all users can send and receive faxes. By default, all users can view the documents

that they send and any fax that is received on the PC. Administrators can see all faxed documents, sent or received, and can configure fax settings, including who has permissions to view or manage faxes, and the TSID and CSID values.

Top of Page

Handwriting personalization—automatic learning

What this feature does

Automatic learning is a handwriting recognition personalization tool that is available on PCs with touch or tablet pen. This feature collects data about the words that you use and how you write them. This helps the handwriting recognition software recognize and improve its interpretation of your handwriting style and vocabulary and also improves auto correction and text suggestions for languages without input method editors (IMEs).

Information collected, processed, or transmitted

Information collected by automatic learning is stored in the user profile for each user on the PC. The data is stored in a proprietary format that can't be read by using a text viewing app (for example, Notepad or WordPad) and is only available to other users if they are administrators on your PC.

The information collected includes:

- Text from messages you compose and calendar entries you create by using email apps (for example, Office Outlook or Windows Live Mail) including any messages that you have already sent.
- Ink that you write in Input Panel.
- Recognized text from ink that you write in Input Panel or type on on-screen keyboards.
- Alternate characters that you select to correct the recognized text.

Use of information

The information collected is used to help improve handwriting recognition by creating a version of the recognition software that's personalized to your own style and vocabulary, and to enable auto correction and text suggestions as you type on on-screen keyboards.

The text samples are used to create an extended dictionary. The ink samples are used to help improve character recognition for each user on a PC. No information is sent to Microsoft.

Choice and control

Automatic learning is enabled by default. You can turn automatic learning on or off at any time by going to Advanced settings in Languages in Control Panel. When you turn off automatic learning, any data that has been collected and stored by automatic learning is deleted.

Top of Page

HomeGroup

What this feature does

Windows allows you to easily link PCs on your home network so that you can share pictures, music, videos, documents, and devices. It also enables PCs to stream media to devices on your home network such as a media extender. These PCs and devices are your homegroup. You can help protect your homegroup with a password, and you can choose what you want to share.

Information collected, processed, or transmitted

You can access your own files, such as pictures, videos, music, and documents, from any PC in the homegroup. When you join a homegroup, account information (including email address, display name, and picture) for all Microsoft accounts on your PC will be shared with others in the homegroup in order to enable sharing with those users.

Use of information

The information collected allows PCs in your homegroup to understand who to share content with and how to present it. No

information is sent to Microsoft.

Choice and control

You have the ability to add or remove PCs from your homegroup and decide what is shared with other homegroup members. You can create a homegroup and manage its settings by going to HomeGroup in PC settings.

Top of Page

Input Method Editor (IME)

Microsoft Input Method Editors (IMEs) are used with East Asian languages to convert keyboard input to ideograms. This section addresses several features, including IME auto-tuning and prediction, IME conversion error reporting, and IME word registration.

IME auto-tuning and prediction

What this feature does

Depending on the IME you use, and your settings, the auto-tuning and text suggestion features of IME might record words or word sequences to improve the selection of the ideograms displayed.

Information collected, processed, or transmitted

The IME auto-tuning (self-learning) and text suggestion features record a word or sequence of words and the frequency with which you use them. Auto-tuning information (excluding any digit/symbol character sequences) is stored in files for each user on a PC.

Use of information

Automatic learning and text suggestion data is used by the IME on your PC to improve the selection of ideograms displayed when you use the IME. If you choose to send this data to Microsoft, it is used to improve IME and related products and services.

Choice and control

Except for the Simplified Chinese IME (in which the prediction feature is off by default), the automatic learning and text suggestion

features are on by default in those IMEs that support them. The data collected isn't sent automatically to Microsoft. You can choose whether or not to collect or send this data in Language in Control Panel.

IME conversion error reporting

What this feature does

If errors in presenting ideograms or in converting keyboard input to ideograms occur, this feature can collect information about the errors that can help Microsoft improve its products and services.

Information collected, processed, or transmitted

IME Conversion Error Reporting collects information about IME conversion errors, such as what you typed, the first conversion or prediction result, the string you chose instead, information about the IME you use, and information about how you use it. In addition, if you use the Japanese IME, you can choose to include automatic learning information in conversion error reports.

Use of information

Microsoft uses the information to improve our products and services. Microsoft doesn’t use the information to identify, contact, or target advertising to you.

Choice and control

After a certain number of conversion errors are stored, the Mis-Conversion Report Tool will ask whether you want to send a conversion error report. You also can choose to send a conversion error report from the IME Mis-Conversion Report Tool at any time. You can view the information contained in each report before choosing whether to send it. You can also enable automatic sending of conversion error reports in IME Settings.

IME word registration

What this feature does

Depending on the IME you use, you might be able to use word registration to report unsupported words (words that might not be converted correctly to ideograms from keyboard input).

Information collected, processed, or transmitted

Registration reports can include the information you provide in the Add Word dialog box about the words being reported, and the software version number for an IME. These reports might include personal information, for example, if you add personal names using word registration. You have the opportunity to review the data being sent with each report before you choose to send it.

Use of information

Microsoft uses the information to help improve our products and services. Microsoft doesn't use the information to identify, contact, or target advertising to you.

Choice and control

Each time you create a word registration report, you're asked if you want to send this report to Microsoft. You can view the information contained in the report before choosing whether to send it.

Top of Page

Installation Improvement Program

What this feature does

This feature sends a single report to Microsoft containing basic information about your PC and how you installed Windows 8. Microsoft uses this information to help improve the installation experience and to create solutions to common installation problems.

Information collected, processed, or transmitted

The report generally includes information about your installation experience, such as the date of installation, the time it took for each installation phase to complete, whether the installation was an upgrade or a new installation of the product, version details, operating system language, media type, PC configuration, and success or failure status, along with any error codes.

If you choose to participate in the Installation Improvement Program, the report is sent to Microsoft when you're connected to the Internet. The Installation Improvement Program randomly

generates a number called a globally unique identifier (GUID) that is sent to Microsoft with the report. The GUID lets us determine which data is sent from a particular computer over time. The GUID doesn't contain any personal information and isn't used to identify you.

Use of information

Microsoft and our partners use the report to help improve our products and services. We use the GUID to correlate this data with data collected by the Windows Customer Experience Improvement Program (CEIP), a program you can choose to participate in when you're using Windows 8

Choice and control

You can choose to participate in this program when you install Windows 8 by selecting **I want to help make the installation of Windows better** .

For more information, see the Windows CEIP section.

Top of Page

Internet printing

What this feature does

Internet printing lets you print over the Internet.

Information collected, processed, or transmitted

When you print using this feature, you must first connect and authenticate yourself to an Internet print server. The information that you'll need to submit to the print server will vary depending on the level of security that the print server supports (for example, you might be asked to provide a user name and password). After you're connected, you’re presented with a list of compatible printers. If your PC doesn’t have a print driver for your selected printer, you can choose to download a driver from the print server. Because print jobs aren’t encrypted, it might be possible for others to see the content being sent.

Use of information

The information collected enables you to print using remote printers.

If you choose to use a print server hosted by Microsoft, we don’t use the information that you provide to identify, contact, or target advertising to you. If you send information to a third-party print server, use of the information will be subject to the third party's privacy practices.

Choice and control

You can enable or disable Internet printing by opening Programs and Features in Control Panel, and then selecting **Turn Windows features on or off**.

Top of Page

Language preferences

What this features does

You can add the languages you prefer to use to your language list in Windows 8. Apps and websites appear in the first language available in that list.

Information collected, processed, or transmitted

When you visit websites and install apps on your PC, your list of preferred languages is sent to the websites you visit and is available to the apps you use so they can provide content in your preferred languages.

Use of information

Your list of preferred languages is used by Microsoft’s websites and apps to provide content in your preferred languages. Microsoft doesn't use any language information to identify or contact you. Language information sent or used by third-party websites and apps is subject to the privacy practices of the third-party website or app publisher.

Choice and control

Your list of preferred languages is available to the apps you install and websites you visit. You can add or remove languages from this list in Language preferences in Control Panel. If you don’t have any languages in this list, the language you choose on the Formats tab in

Region in Control Panel will be sent to the websites you visit.

Top of Page

Location services

On PCs running Windows, "location services" refers to the Windows software and Microsoft online service that are used to determine the approximate physical location of your PC, which is provided to apps or websites that you allow to access it. The Windows Location Platform obtains location from dedicated hardware like a GPS sensor in your PC, or through software like Windows Location Provider.

Windows Location platform

What this feature does

If you choose to turn on the Windows Location Platform, apps you install from the Windows Store will be able to ask for permission to access your PC's location. Depending on your system's configuration, the platform may determine your PC's location using hardware such as a GPS sensor or software such as Windows Location Provider.

The platform doesn't prevent apps from accessing your PC's location in other ways. For example, you can install devices (such as a GPS receiver) that might send location information directly to an app and entirely bypass the platform. Regardless of your Windows Location Platform settings, online services can use your PC's IP address to determine its approximate location—usually the city your PC is in.

Information collected, processed, or transmitted

The Windows Location Platform itself doesn't transmit any information from your PC, but individual location providers (such as the Windows Location Provider) might transfer information when you use location-aware apps. Apps that are authorized to use the platform to determine your location could also transmit or store that information.

Use of information

If you enable the Windows Location Platform, authorized apps will be able to access your location and use it to give you personalized content. If you use a third-party app or location provider, its use of

your PC's location will be subject to the third party's privacy practices. Before you download a Windows Store app, you'll be able to see whether the app is location aware in the app description.

Choice and control

By choosing express settings during Windows Setup, you turn on the Windows Location Platform. If you choose to customize settings, you can control the Windows Location Platform by selecting **Turn on Windows Location Platform so apps can ask users for their location** under **Share info with apps**. The first time each Store app requests your PC's location, Windows will ask whether you want to allow that. You can control whether apps can ask for your location in Privacy in PC settings, and you can control whether an individual Store app can use your location in Permissions in the app's Settings charm.

If you use a desktop app that uses Windows Location Platform, it should ask your permission to use your PC's location, and when it accesses your PC's location, an icon will appear in the notification area to alert you that your PC's location has been accessed. Each user can control their own location settings for all apps in Privacy in PC settings. In addition, administrators can choose to turn off the Windows Location Platform for all users in Location in Control Panel.

Windows Location provider

What this feature does

The Windows Location Provider connects to the online Microsoft Location Service that helps determine your PC's approximate location based on Wi-Fi networks near your PC's or your PC's IP address.

Information collected, processed, or transmitted

When an app you've authorized to receive your location asks for it, the Windows Location Platform will ask all installed location providers (including Windows Location Provider) to determine your current location. The Windows Location Provider will first check to see if it has a list of Wi–Fi access points stored from a prior request by a location-aware app. If there isn't already a list of nearby Wi–Fi access points, or if the list is out of date, the provider sends information about nearby Wi–Fi access points and GPS information

(if available) to the Microsoft Location Service. The service returns your PC's approximate location back to Windows Location Provider, which passes the location to the Windows Location Platform, which in turn provides it to the app that requested your location. Windows Location Provider may also update its stored list of Wi–Fi access points. The Windows Location Provider maintains this list so it can determine your PC's approximate location without connecting to the Internet each time. This list of access points is encrypted when stored on disk so that apps can't directly access it.

The information that's sent about nearby Wi–Fi access points includes BSSID (the MAC address of the Wi–Fi access point) and signal strength. The GPS information includes observed latitude, longitude, direction, speed, and altitude. To help protect your privacy, Windows Location Provider doesn't send any information to uniquely identify your PC beyond the standard computer information sent with all connections to the Internet. To help protect the privacy of Wi–Fi network owners, Windows doesn't send SSIDs (Wi–Fi access point names) or hidden Wi–Fi networks. For privacy and security purposes, information sent about Wi-Fi networks is sent encrypted via SSL.

Use of information

The information is used by the Windows Location Provider to give Windows Location Platform the approximate location of your PC when an authorized app requests it.

If you choose to help improve the Microsoft Location Service, the Wi-Fi and GPS info sent to Microsoft is used to improve Microsoft's location services, which helps to improve the location services provided to your apps. Microsoft does not store any data collected from this service that could be used to identify, contact, target advertising to you, or to track or create a history of your PC's location.

Choice and control

The Windows Location Provider is used only if an authorized app has requested your PC's location. For more information about how to control whether apps can request your PC's location, see the Windows Location Platform section. If you authorize apps to request

your PC's location, the cached list of nearby Wi-Fi access point locations that are encrypted and stored by the Windows Location Provider will be deleted and replaced periodically.

If you choose express settings while setting up Windows, you choose to help improve the Microsoft Location Service. If you choose to customize settings, you can control whether to help improve the Microsoft Location Service by selecting **Help improve Microsoft services by sending some location data when location-aware apps are used** under **Send Microsoft info to help make Windows and apps better**. After setting up Windows, you can change this setting in Location Settings in Control Panel. If you choose not to help improve the service, you will still be able to use the Windows Location Provider to determine your PC's approximate location.

You can enable and disable the Windows Location Provider by opening **Turn Windows features on or off** in Control Panel. If you turn off the Windows Location Provider, you can still use other location providers (such as GPS) with Windows Location Platform.

Top of Page

Name and account picture

What this feature does

To provide personalized content, apps can request your name and account picture from Windows. Your name and account picture are displayed under Your account in Users in PC settings. If you sign in to Windows with a Microsoft account, Windows will use the name and account picture associated with that account. If you haven't chosen a picture for your account, your account picture will be a default picture provided by Windows.

Information collected, processed, or transmitted

If you allow apps to access your name and account picture, Windows will provide that information to all apps that request it. Apps might store or transmit this information.

If you sign in to Windows with a domain account, and you choose to allow apps to use your name and account picture, apps that can use

your Windows credentials will be allowed to access certain other forms of your domain account information. This information includes, for example, your user principal name (like jack@contoso.com) and DNS domain name (like corp.contoso.com\jack).

If you sign in to Windows with a Microsoft account, or if you sign in to Windows with a domain account connected to a Microsoft account, Windows can automatically sync your account picture on your PC with your Microsoft account picture.

Use of information

If you use a third-party app, how the app uses your name and account picture is subject to the third party's privacy practices. If you use a Microsoft app, the app's privacy practices will be explained in its privacy statement.

Choice and control

If you choose express settings while setting up Windows, Windows will allow apps to access your name and account picture. If you choose to customize settings, you can control access to your name and account picture by selecting **Let apps use my name and account picture** under **Share info with apps**. After setting up Windows, you can change this setting in **Privacy** in PC settings. You can change your account picture in **Personalize** in PC settings. You can also choose to allow certain apps to change your account picture.

Top of Page

Network Awareness

What this feature does

If you have a subscription plan for network access (for example, via a mobile broadband connection), this feature provides information about your subscription plan to apps and Windows features on your PC. Windows features and apps can use this information to optimize their behavior. For example, if you're on a metered data plan, Windows Update will wait to deliver lower priority updates to your

PC until you’re connected to another type of network. This feature also provides information about your network connection, such as signal strength and whether your PC is connected to the Internet.

Information collected, processed, or transmitted

This feature collects Internet and intranet network connectivity information, such as the Domain Name Service (DNS) suffix of your PC, network name, and gateway address of the networks that your PC connects to. This feature also receives subscription plan information such as the amount of data remaining in the plan.

Network connectivity profiles can include a history of all networks visited and the date and time of the last connection. This feature can attempt to connect to a Microsoft server to determine whether you're connected to the Internet. The only data sent to Microsoft during network connectivity checks is standard PC information.

Use of information

If data is sent to Microsoft, it is only used to provide network connectivity status. Network connectivity status is made available to apps and features on your PC that request network connectivity information. If you use a third-party app, use of the information collected will be subject to the third party's privacy practices.

Choice and control

Network Awareness is on by default. An administrator can disable it using the Services options in Administrative Tools in Control Panel. Disabling this feature isn't recommended because it will prevent some Windows features from functioning properly.

Top of Page

Notifications, Lock Screen Apps, and Tile Updates

Windows Store apps can automatically receive content and display notifications in several ways. They can, for example, receive notifications that are displayed briefly in the corner of the screen or on app tiles if those tiles are pinned to Start. You can also receive those notifications on the lock screen if you’d like. The lock screen can display detailed or brief status for certain apps as well. App

publishers can send content to your Windows Store apps through the Windows Push Notification Service running on Microsoft servers, or the apps can download information directly from third-party servers.

Notifications

What this feature does

Windows Store apps can deliver periodic or real-time information to you that will be displayed briefly as notifications in the corner of the screen.

Information collected, processed, or transmitted

Apps can display text, images, or both in notifications. The contents of notifications can be provided locally by the app (for example, an alarm from a clock app). Notifications can also be sent from an app's online service through the Windows Push Notification Service (for example, a social network update). Images displayed in notifications may be downloaded directly from a server specified by the app publisher; when that happens, standard computer information will be sent to that server.

Use of information

Microsoft only uses notification information to deliver notifications from your apps to you. The notification can be stored temporarily by the Windows Push Notification Service before delivery to your PC. If a notification can’t be delivered immediately, it will only be stored for a few minutes before it’s deleted.

Choice and control

You can turn off notifications for all apps or for individual apps in **Notifications** in PC settings. If you turn off notifications for an app or uninstall it, the app publisher could still send updates to the Windows Push Notification Service, but those notifications won’t display on your PC.

Lock screen apps

What this feature does

Some apps can display status and notifications on the screen when your PC is locked. Lock screen apps can also perform tasks in the

background while you're not using them, such as syncing email.

Information collected, processed, or transmitted

Lock screen apps can receive status updates from the app publisher through the Windows Push Notification Service, or directly from the app publisher's (or another third party's) servers. Lock screen apps could also transmit or process other information unrelated to notifications and updates.

Use of information

Windows uses the status and notification information provided by the lock screen apps to update the lock screen.

Choice and control

After you set up Windows, the Mail, Calendar, and Messaging apps are automatically set as lock screen apps. You can add or remove these or other apps from the lock screen in Personalize in PC Settings. You can also choose one app to persistently display detailed status (for example, details for the next appointment on your calendar) on the lock screen.

You can control whether lock screen apps can display notifications on the lock screen in Notifications in PC settings.

Tile updates

What this feature does

Windows Store apps can deliver periodic or real-time information to you that will be displayed as updates to your apps' tiles in Start.

Information collected, processed, or transmitted

Store apps that are pinned to Start can update their tiles with text, images, or both. The content displayed on an app's tile can be provided locally by the app, downloaded periodically from a server specified by the app publisher, or sent from an app's online service through the Windows Push Notification Service. If tile content is downloaded directly from a server specified by the app publisher, standard computer information will be sent to that server.

Use of information

Microsoft only uses tile information to deliver tile updates from your apps to you. This information can be stored temporarily by the Windows Push Notification Service before delivery to your PC. If a tile update can't be delivered immediately, it will only be stored for a few days before it's deleted.

Choice and control

After an app has started receiving tile updates, you can turn them off by selecting the app's tile in Start and selecting **Turn live tile off** in the commands that are available for the app. If you unpin an app's tile from Start, its tile updates won't display. If you uninstall an app, the app publisher could still send updates to the Windows Push Notification Service, but they won't display on your PC.

To clear the current updates displayed on your Start tiles, swipe from the right side or point to the upper right corner of Start, tap or click **Settings**, and then tap or click **Tiles**. Tap or click the **Clear** button under **Clear personal info from my tiles**. Tile updates delivered after you clear the current updates will continue to appear.

Top of Page

Order prints

What this feature does

Order Prints enables you to send digital pictures stored on your PC or a network drive to an online photo printing service of your choice. Depending on the service, you can have your pictures printed and then delivered using postal mail or you can pick up the prints at a local store.

Information collected, processed, or transmitted

If you decide to place an order with an online photo printing service, your digital photos are sent over the Internet to the service that you selected. The file path to the digital pictures that you select (which might include your user name) might be sent to the service in order to allow the service to display and upload the images. Digital picture files might contain data about the image that was stored with the file by the camera, such as the date and time that the picture was taken or the location where the picture was taken if your camera has

GPS capabilities. The files might also contain personal information (such as captions) that might have been associated with the file through the use of digital picture management apps and Windows Explorer. For more information, see the Properties section below.

After you select an online photo printing service from Order Prints, you'll be redirected to the service's website in the Order Prints window. Information you enter on the online photo printing services website is transmitted to the service.

Use of information

The information stored in the digital picture files by the camera might be used by the online photo printing service during the printing process, for example, to adjust the color or sharpness of the image before it is printed. Information stored by digital picture management apps might be used by the online photo printing service to print as captions on the front or back of the print copy. The online photo printing services' use of this information, and other information you provide to the services, such as information you enter on their websites, will be subject to their privacy practices.

Choice and control

You can use Order Prints to choose which pictures to send and which service to use to print your pictures. Some picture management apps might be able to help you remove stored personal information before sending pictures to be printed. You might also be able to edit the properties of the file to remove stored personal information.

Top of Page

Program Compatibility Assistant

What this feature does

If an incompatibility problem is found with an app that you try to run, Program Compatibility Assistant will try to help you resolve it.

Information collected, processed, or transmitted

If an incompatibility problem is found with an app you attempt to

run, a report is generated that includes information such as the app name, app version, the needed compatibility settings, and your actions with the app so far. Problems about incompatible apps are reported to Microsoft through Windows Error Reporting or the Windows Customer Experience Improvement Program (CEIP).

Use of information

Error reports are used to provide you with responses to problems that you report for your apps. Responses contain links (when available) to the app publisher's website so you can learn more about possible solutions. Error reports created due to app failures are used to try to determine which setting to adjust when you encounter compatibility problems for the apps that you're running on this version of Windows. Information reported through CEIP is used to identify app compatibility problems.

Microsoft doesn't use any information collected through this feature to identify, contact, or target advertising to you.

Choice and control

For problems reported through Windows Error Reporting, an error report is created only when you select the option to check online for a solution. Unless you have previously consented to report problems automatically so you can check for solutions, you're asked if you want to send the error report. For more information, see the Windows Error Reporting section.

Some issues will automatically be reported through Windows CEIP if you've chosen to turn it on. For more information, see the Windows Customer Experience Improvement Program section.

Top of Page

Properties

What this feature does

Properties are file information that allow you to quickly search and organize your files. Some properties are intrinsic to the file (for example, the size of the file) while others might be specific to an app or device (for example, the settings of your camera when you took a

photo or the location data recorded by the camera for the photo).

Information collected, processed, or transmitted

The type of information stored will depend upon the type of file and the apps that use it. Examples of properties include file name, date modified, file size, author, keywords, and comments. Properties are stored in the file, and they move with the file if it is moved or copied to another location, such as a file share, or sent as an email attachment.

Use of information

Properties can help you more quickly search and organize your files. They can also be used by apps to perform app-specific tasks. No information is sent to Microsoft.

Choice and control

You can edit or remove some properties for a file by selecting the file in Windows Explorer and clicking Properties. Some intrinsic properties, such as date modified, file size, file name, and some app-specific properties can't be removed this way. For app-specific properties, you can edit or remove them only if the app used to generate the file supports these features.

Top of Page

Proximity

Near field proximity service

What this feature does

If your PC has near-field communication (NFC) hardware, you can physically tap it against another device with NFC hardware to share links, files, and other information. There are two types of proximity connections: Tap and Do and Tap and Hold. With Tap and Do, you can create a brief or long-term connection between devices over Wi–Fi, Wi–Fi Direct, or Bluetooth. With Tap and Hold, the connection is active only as long as the devices are held next to each other.

Information collected, processed, or transmitted

When you tap proximity enabled devices together, they exchange

information to establish a connection with each other. Depending on the way the devices are configured, this data can include Bluetooth and Wi–Fi network addresses, and the name of your PC.

After a connection is established, other information might be exchanged between devices, depending on the specific proximity feature or app you're using. Windows can send files, links, and other information between devices using a proximity connection. Apps that use proximity can send and receive any information they have access to. This information might be sent through your network or Internet connection, or directly through a device-to-device wireless connection.

Use of information

Network and PC information exchanged over a proximity connection is used to establish a network connection, and to identify the devices connecting to each other. Data transferred through a proximity connection initiated within an app can be used by that app in any way. No information is sent to Microsoft.

Choice and control

Near field proximity service is on by default. An administrator can disable it using the options provided in Devices and Printers in Control Panel.

Tap and Send

What this feature does

Windows Tap and Send makes it easy to share selected information with a friend standing next to you or with another one of your devices such as a mobile phone. For example, when you're in a browser, you can start Tap and Send from the Devices pane. The next device you tap will receive a link to the webpage currently being displayed. This also works with any app that supports sharing information, such as pictures, text, or files.

Information collected, processed, or transmitted

Tap and Send uses the information you're sharing and the information described in the Near field proximity service section above.

Use of information

This information is only used to create the connection between the two devices. The shared information isn't stored by Tap and Send. No information is sent to Microsoft.

Choice and control

If Near field proximity service is enabled, Tap and Send is also enabled. For more information, see the Near field proximity service section.

Top of Page

Remote Access connections

What this feature does

Remote Access connections allow you to connect to private networks using a virtual private network (VPN) connection and Remote Access Service (RAS). RAS is a component that connects a client PC (typically your PC) to a host PC (also known as a remote access server) using industry standard protocols. VPN technologies allow users to connect to a private network, such as a corporate network, over the Internet.

A Remote Access connections component, Dial-up Networking, allows you to access the Internet using a dial-up modem or broadband technology such as a cable modem or a digital subscriber line (DSL). Dial-up Networking includes dialer components such as RAS Client, Connection Manager, and RAS Phone, as well as command-line dialers like rasdial.

Information collected, processed, or transmitted

The dialer components collect information from your PC such as your user name, password, and domain name. This information is sent to the system that you're attempting to connect with. To help protect your privacy and the security of your PC, security-related information such as your user name and password are encrypted and stored on your PC.

Use of information

Dialer information is used to help your PC connect to the Internet. A remote access server might keep the user name and IP address information for accounting and compliance purposes, but no information is sent to Microsoft.

Choice and control

For non-command-line dialers, you can choose to save your password by selecting **Save this user name and password**. You can clear that option at any time to delete the previously saved password from the dialer. Because this option is turned off by default, you might be prompted to provide your password to connect to the Internet or a network. For command-line dialers like rasdial, there is no option to save your password.

Top of Page

RemoteApp and Desktop Connections

What this feature does

RemoteApp and Desktop Connections let you access apps and desktops on remote PCs that have been made available online for remote access.

Information collected, processed, or transmitted

When you enable a connection, configuration files are downloaded to your PC from the remote URL you specify. These configuration files link apps and desktops on remote PCs so that you can run them from your PC. Your PC will automatically check for and download updates to these configuration files periodically. These apps run on remote PCs, and information you enter into the apps is transmitted across the network to the remote PCs you chose to connect with.

Use of information

Updates to configuration files might include settings changes including providing you with access to new apps; however, new apps will run only if you choose to run them. This feature also sends information to the remote PCs on which the remote apps run. The use of this data by the remote apps is subject to the privacy policies of the app providers and the remote PCs' administrators. No

information is sent to Microsoft.

Choice and control

You can choose whether you want to use RemoteApp and Desktop Connections. You can add or remove RemoteApp and Desktop Connections by going to RemoteApp and Desktop Connections in Control Panel. You can add a new connection by clicking **Set up a new connection with RemoteApp and Desktop Connections**, and entering a Connection URL in the dialog box. You can also use your email address to retrieve the Connection URL. You can remove a connection and its connection files by clicking **Remove** on the connections description dialog box. If you disconnect a connection without closing all open apps, these apps will remain open on the remote PC. RemoteApp and Desktop Connections aren't shown in the Add or remove programs list in Control Panel.

Top of Page

Remote Desktop connection

What this feature does

Remote Desktop connection provides a way for you to establish a remote connection with a host PC that is running Remote Desktop Services.

Information collected, processed, or transmitted

Remote Desktop connection settings are stored in app-local storage or in a Remote Desktop Protocol (RDP) file on your PC. These settings include the name of your domain and connection configuration settings, such as remote PC name, user name, display information, local device information, audio information, clipboard, connection settings, remote app names, and session icon or thumbnail.

Credentials for these connections, Remote Desktop Gateway credentials, and a list of trusted Remote Desktop Gateway server names are stored locally on your PC. This list is stored permanently unless it is deleted by an administrator. No information is sent to Microsoft.

Use of information

Information collected by Remote Desktop connection allows you to connect to host PCs running Remote Desktop Services using your preferred settings. User name, password, and domain information are collected to allow you to save your connection settings and to enable you to double-click an RDP file or click a favorite to launch a connection without having to re-enter this information.

Choice and control

You can choose if you want to use Remote Desktop connection. If you use it, your RDP files and Remote Desktop connection favorites contain information required to connect to a remote PC, including the options and settings that were configured when the connection was automatically saved. You can customize RDP files and favorites, including files for connecting to the same PC with different settings. To modify saved credentials, open Credential Manager in User accounts in Control Panel.

Top of Page

Sign in with a Microsoft account

What this feature does

A Microsoft account (formerly known as Windows Live ID) is a single email address and password you can use as your sign-in info to sign in to apps, sites, and services from Microsoft and select Microsoft partners. You can sign up for a Microsoft account in Windows or on Microsoft websites that require you to sign in with a Microsoft account.

You can choose to sign in to Windows with a Microsoft account or choose to connect your local or domain account to a Microsoft account. If you do this, Windows can help make your PCs look and feel the same by automatically syncing settings and info in Windows and Microsoft apps. If you go to the sign-in page of those websites, it will also automatically sign you in to websites that use Microsoft accounts to sign in.

Information collected, processed, or transmitted

When you enter an email address to use as a Microsoft account while setting up your PC or in Users in PC settings, Windows sends the email address to Microsoft to determine if there's already a Microsoft account associated with that email address. If you already use that email address as a Microsoft account, you can use it and the password for the Microsoft account to sign in to Windows. If you don't already have enough security info for your Microsoft account, we might first ask you for additional security info such as a mobile phone number that we can use to verify the account is yours if you have trouble signing in to your account. If you don't have a Microsoft account, you can create one using any email address.

Each time you sign in to Windows with a Microsoft account while your PC is connected to the Internet, Windows verifies your email address and password with Microsoft's servers. When you are signed in to Windows with your Microsoft account or with a domain account connected to your Microsoft account:

- Certain Windows settings will sync between the PCs that you sign in to with a Microsoft account. For more information about what settings are synced and how to control them, see the Sync your settings section.

- Microsoft apps that use a Microsoft account for authentication (like Mail, Calendar, Photos, People, Messaging, OneDrive, Microsoft Office, and other apps) can automatically begin downloading your info (for example, the Mail app will automatically download the messages sent to your Outlook.com or Hotmail.com address if you have one).

- Web browsers can automatically sign you in to websites that you sign in to with your Microsoft account (for example, if you visit OneDrive.com you may be automatically signed in without needing to reenter your Microsoft account password).

Windows will ask your permission before allowing third-party apps to use profile information or other personal information associated with your Microsoft account. If you sign in to Windows with a domain account connected to a Microsoft account, the settings and info you choose will sync with your domain account, and you'll automatically be signed in to apps and websites as described above. Because

domain administrators are able to access any information on your PC, they will also be able to access any settings and info you have chosen to sync with other PCs through your Microsoft account. This can include settings such as name, account picture, and browser history. For more information about what settings are synced and how to control them, see the Sync your settings section.

Use of information

When you create a new Microsoft account in Windows, we use the information you provide to create and help secure the account. For example, the security info you provide (like your phone number or alternate email address) is only used if you can't sign in to your account. When you're signed in to Windows with a Microsoft account, Windows uses your Microsoft account info to sign you in to apps and websites automatically. To learn more about the privacy impact of having a Microsoft account, read the privacy statement displayed when you choose Sign up for a new email address. For information about how individual Microsoft apps use information associated with your Microsoft account, see the apps' own privacy statements. You can find the privacy statement for a Microsoft app in the app's Settings charm or About dialog.

Choice and control

When you sign in to Windows with a Microsoft account, some settings are synced automatically. To learn how to change which Windows settings are synced or to stop syncing, see the Sync your settings section. To learn more about the data collected by Microsoft apps that use a Microsoft account for authentication, read their privacy statements. You can find the privacy statements for the Windows Live apps (Mail, Calendar, Photos, People, Messaging, OneDrive) at go.microsoft.com/fwlink/?LinkId=257483, and for Microsoft Office at go.microsoft.com/fwlink/?LinkId=257484. You can also find an app's privacy statement in the app's Settings charm or About dialog.

You don't have to sign in to Windows with a Microsoft account. When you add a user to your PC while setting up your PC or in **Users** in PC settings, you can choose to use a local account or a Microsoft account. You can switch to a local account or Microsoft

account at any time in **Users** in PC settings. If you sign in to Windows with a domain account, you can connect or disconnect your Microsoft account at any time in **Users** in PC settings.

When you use InPrivate Browsing in Internet Explorer, you won't be automatically signed in to websites that use Microsoft accounts.

Top of Page

Sync your settings

What this feature does

When you sign in to Windows with a Microsoft account, Windows syncs some of your settings and info with Microsoft servers to make it easier to have personalized experiences across multiple PCs. After you've signed into a PC with a Microsoft account, when you sign into another PC with the same Microsoft account for the first time, Windows will download and apply the settings and info you choose to sync from your other PCs. Settings you choose to sync will automatically update on Microsoft servers and your other PCs as you use them.

Information collected, processed, or transmitted

If you choose to sign in to Windows with a Microsoft account, Windows syncs certain settings with Microsoft servers. These settings include:

- Language preferences
- Ease of Access preferences
- Personalization settings such as your account picture, lock screen image, background, and mouse settings
- Settings for Windows Store apps
- Spell checker and IME dictionaries
- Web browser history and favorites
- Saved app, website, and network passwords

To help protect your privacy, all synced settings are sent encrypted

via SSL. Some of these settings won't sync on your PC until you add your PC to your Microsoft account as a trusted PC.

If you sign in to Windows with a domain account connected to a Microsoft account, settings and info you have chosen will sync to your domain account. Passwords that you save while signed into Windows with a domain account connected to a Microsoft account will never be synced. Because domain administrators are able to access any information on your PC, they will also be able to access any settings and info, including your browsing history, that you have chosen to sync with other PCs through your Microsoft account.

Use of information

Windows 8 uses these settings and info to provide the syncing service. Microsoft doesn't use your synced settings and info to identify, contact, or target advertising to you.

Choice and control

When you sign in to Windows with a Microsoft account, Sync your settings will be turned on. You can choose to sync your settings, and control what is synced, by going to **Sync your settings** in PC settings. If you sign in to Windows with a domain account and you choose to connect that account to a Microsoft account, Windows will ask which settings you want to sync before connecting your Microsoft account.

Top of Page

Teredo Technology

What this feature does

Teredo Technology (Teredo) allows PCs and networks to communicate over multiple networking protocols.

Information collected, processed, or transmitted

Each time you start your PC, Teredo will attempt to locate a public Internet Protocol version 6 (IPv6) service on the Internet. This occurs automatically when your PC is connected to a public or private network, but doesn’t occur on managed networks such as

enterprise domains. If you use an app that requires Teredo to use IPv6 connectivity, or if you configure your firewall to always enable IPv6 connectivity, then Teredo will periodically contact the Microsoft Teredo service over the Internet. The only information sent to Microsoft is standard PC information and the name of the service requested (for example, teredo.ipv6.microsoft.com).

Use of information

The information sent from your PC by Teredo is used to determine if your PC is connected to the Internet and if it can locate a public IPv6 service. Once the service is located, information is sent to maintain a connection with the IPv6 service.

Choice and control

Using the netsh command line tool, you can change the query that the service sends over the Internet to use non-Microsoft servers instead, or you can turn it off. For detailed instructions, see the "Internet Protocol Version 6, Teredo, and Related Technologies" section of this technical white paper.

Top of Page

Trusted Platform Module (TPM) Services

What this feature does

The Trusted Platform Module (TPM) is security hardware built into some PCs that, if present and provisioned, enables your PC to take full advantage of advanced security features. Windows features that use the TPM include BitLocker Drive Encryption, Virtual Smart Card, Secure Boot, Windows Defender, and TPM Based Certificate Storage.

Information collected, processed, or transmitted

By default, Windows takes ownership of the TPM and stores the full TPM owner authorization information so it's only available to the Windows administrators. Limited authorization values are created to perform typical administrative actions and standard user actions and are managed by Windows.

The TPM Management Console allows you to interactively provision the TPM and save the TPM owner authorization value to external

media like a USB flash drive after the TPM has been provisioned. A saved file contains the TPM owner authorization information for the TPM. The file also contains the PC name, operating system version, creation user, and creation date information to assist you in recognizing the file.

In a domain environment, the full TPM owner password can be configured by the domain administrator to be stored in Active Directory under a TPM object when the TPM is provisioned.

Each TPM has a unique cryptographic Endorsement Key that it uses to indicate its authenticity. The Endorsement Key can be created and stored in the TPM by your PC's manufacturer, or for older PCs, Windows might need to trigger creation of the Endorsement Key inside the TPM. The private portion of the Endorsement Key is never exposed outside of the TPM, and once it has been created, it usually can't be reset. An Endorsement Key Certificate will be stored in the TPM of most Windows 8 computers. The Endorsement Key Certificate indicates that the Endorsement Key exists in a hardware TPM. The certificate is useful for remote verifiers to confirm the TPM conforms to the TPM specifications. The Endorsement Key Certificate is usually signed by the TPM manufacturer or the platform manufacturer.

Use of information

Once the TPM is initialized, apps can use the TPM to create and help secure additional unique cryptographic keys. For example, BitLocker Drive Encryption uses the TPM to help protect the key that encrypts the drive.

If you choose to save the TPM owner password to a file, the additional PC and user information saved inside this file helps you to identify the matching PC and TPM. The TPM endorsement key is used by Windows during TPM initialization to encrypt your TPM owner authorization value before sending it to the TPM. Windows doesn’t transmit cryptographic keys outside of your PC. Windows does provide an interface for third-party apps like antimalware software to use the Endorsement Key for certain TPM scenarios, such as Measured Boot with Attestation. For antimalware software the endorsement key and the endorsement key certificate are useful

to confirm boot measurements are provided by a TPM from a specific manufacturer. By default, only administrators or apps with administrative rights can use the TPM endorsement key.

Choice and control

Users or administrators opt in to using the TPM by turning on a Windows feature or running an app that uses the TPM.

You can choose to clear the TPM and reset it to factory defaults. Clearing the TPM removes owner information, and with the exception of the endorsement key, all TPM-based keys or cryptographic information that apps might have created when the TPM was in use.

Top of Page

Update Root Certificates

What this feature does

Certificates are used primarily to verify the identity of a person or device, authenticate a service, or encrypt files. Trusted root certification authorities are the organizations that issue certificates. Update Root Certificates contacts the online Windows Update service to see if Microsoft has added a certification authority to its list of trusted authorities, but only when an app is presented with a certificate issued by a certification authority that isn't directly trusted (a certificate that isn't stored in a list of trusted certificates on your PC). If the certification authority has been added to the Microsoft list of trusted authorities, its certificate will automatically be added to the list of trusted certificates on your PC.

Information collected, processed, or transmitted

Update Root Certificates sends a request to the online Windows Update service that asks for the current list of root certification authorities in the Microsoft Root Certificate Program. If the untrusted certificate is on the list, Update Root Certificates obtains that certificate from Windows Update and places it in the trusted certificate store on your PC. The information transferred includes the names and cryptographic hashes of root certificates.

For more information about Windows Update and your privacy, read the Update Services Privacy Statement.

Use of information

The information is used by Microsoft to update the list of trusted certificates on your PC. Microsoft doesn't use this information to identify, contact, or target advertising to you.

Choice and control

Update Root Certificates is enabled by default. Administrators can configure Group Policy to disable the Update Root Certificates on a PC.

Top of Page

Update services

What this feature does

Update services for Windows includes Windows Update and Microsoft Update:

- **Windows Update** is a service that provides you with software updates for Windows software and other supporting software, such as drivers supplied by device manufacturers.
- **Microsoft Update** is a service that provides you with software updates for Windows software, as well as other Microsoft software such as Microsoft Office.

Information collected, processed, or transmitted

If you choose to get important software updates for your PC, the Windows Malicious Software Removal Tool (MSRT) might be included with these updates. MSRT checks PCs for infections by specific, prevalent malicious software ("malware") and helps remove any infections found. If the software runs, it will remove the malware listed on the Microsoft Support website. During a Malware check, a report will be sent to Microsoft with specific information about malware detected, errors, and other information about your PC. For more information, read the Windows Malicious Software Removal Tool privacy statement .

To learn what other information Update Services collects, see the Update Services privacy statement.

Use of information

This MSRT information is used to help improve our antimalware and other security products and services. No information in the MSRT reports will be used to identify or contact you.

To learn how Update Services uses other information, see the Update Services privacy statement.

Choice and control

If you choose express settings while setting up Windows, you turn on the Update Services and set Windows Update to install updates automatically. If you choose to customize settings, you can control the Update Services in **Windows Update** under **Help protect and update your PC**. After Windows installs, you can change settings for the Update Services in Control Panel. For more information, see the Update Services privacy statement.

If you have chosen to check for and install important updates, and receive MSRT as part of these updates for your PC, you can disable the software's reporting functionality by following these instructions on Microsoft Support.

Top of Page

Windows Customer Experience Improvement Program (CEIP)

What this feature does

Windows Customer Experience Improvement Programs (CEIP) can collect information about how you use your apps, your PCs, connected devices, and Windows. It can also collect information about performance and reliability problems that might occur. If you choose to participate in Windows CEIP, Windows will send this data to Microsoft, and will also periodically download a file to collect more relevant information about how you use Windows and apps. CEIP reports are sent to Microsoft to help improve the features our customers use most often, and to create solutions to common problems.

Information collected, processed, or transmitted

CEIP reports can include information such as:

- Configuration information. including information such as how many processors are in your PC, the number of network connections in use, screen resolutions for display devices, and which version of Windows is running.

- Performance and reliability information, including information such as how quickly an app responds when you click a button, how many problems you experience with an app or a device, and how quickly information is sent or received over a network connection.

- App use information, including information about the features you use most often, such as how frequently you open apps, how often you use Windows Help and Support, which services you use to sign in to apps, and how many folders you typically create on your desktop.

CEIP reports also contain information about events (event log data) on your PC from up to seven days prior to the time you decide to participate in CEIP. Since most users decide to participate in CEIP within several days of setting up Windows, Microsoft uses this information to analyze and improve the Windows setup experience.

This information is sent to Microsoft when you're connected to the Internet. CEIP reports don’t intentionally contain contact information, such as your name, address, or phone number; however, some reports might unintentionally contain individual identifiers, such as a serial number for a device that is connected to your PC. Microsoft filters the information contained in CEIP reports to try to remove any individual identifiers that they might contain.

CEIP randomly generates a number called a globally unique identifier (GUID) that is sent to Microsoft with every CEIP report. The GUID lets us determine which data is sent from a particular computer over time. The pre-installed Microsoft apps licensed with Windows may create their own unique identifiers for use with CEIP, which could be based on information from your Microsoft account.

CEIP will also periodically download a file to collect more relevant information about the way you useWindows and apps. This file helps Windows collect additional information to help Microsoft create solutions for common problems and better understand usage patterns of Windows and apps.

Use of information

Microsoft uses CEIP information to improve our products and services, as well as third-party software and hardware designed for use with these products and services. We might also share CEIP information, with Microsoft partners so they can improve their products and services, but the information shared is in aggregated form and can't be used to identify, contact, or target advertising to you.

We use the GUID to distinguish how widespread the feedback we receive is and how to prioritize it. For example, the GUID allows Microsoft to distinguish between one customer experiencing a problem one hundred times and one hundred customers experiencing the same problem once. Microsoft doesn't use the information collected by CEIP to identify or contact you.

Choice and control

If you choose express settings while setting up Windows, you turn on Windows CEIP: Windows and the Microsoft apps licensed with Windows will be able to send CEIP reports for all users on your PC. If you choose to customize settings, you can control CEIP by selecting **Participate in the Customer Experience Improvement Program to help improve Microsoft software and services** under **Send Microsoft info to help make Windows and apps better**. After setting up Windows, administrators can change this setting in Action Center in Control Panel.

For more information, see the CEIP frequently asked questions online.

Top of Page

Windows Defender

Windows Defender looks for malware and other potentially unwanted software on your PC. It includes the Microsoft Active Protection Service and History features.

Microsoft Active Protection Service

What this feature does

The Microsoft Active Protection Service (MAPS) antimalware community is a voluntary, worldwide community including Windows Defender users. Through MAPS, users can send information about malware and other potentially unwanted software to Microsoft in a report. MAPS can help protect your PC by automatically downloading new signatures for newly-detected malware.

Information collected, processed, or transmitted

MAPS reports include information about potential malware files, such as file names, cryptographic hash, software publisher, size, and date stamps. In addition, MAPS might collect full URLs to indicate the origin of the files. These URLs might occasionally contain personal information such as search terms or data entered in forms. Reports might also include the actions you took when Windows Defender notified you that the potentially unwanted software was detected. MAPS includes this information to help Microsoft gauge how effectively Windows Defender can detect and remove malware and potentially unwanted software, and to attempt to identify new malware.

Reports are automatically sent to Microsoft when:

- Windows Defender detects software that hasn’t been analyzed for risks yet.
- Windows Defender detects changes to your PC by software that hasn't been analyzed for risks yet.
- Windows Defender takes action on malware upon detection (as part of its automatic remediation).
- Windows Defender completes a scheduled scan and automatically takes action on software that it detects based on your settings.

You can join MAPS with a basic or an advanced membership. If you choose to enable MAPS while setting up Windows, you join with a basic membership. Basic membership reports contain the information described in this section. Advanced membership reports are more comprehensive and might occasionally contain personal information from, for example, file paths and partial memory dumps. These reports, along with reports from other Windows Defender users who are participating in MAPS, help our researchers discover new threats more rapidly. Malware definitions are then created, and then these updated definitions are made available to all users through Windows Update.

If you join MAPS with a basic or an advanced membership:

- Microsoft might request a sample submission report. This report contains specific files from your PC that Microsoft suspects might be potentially unwanted software. The sample report is used for further analysis. You'll be asked each time if you want to send this sample submission report to Microsoft.

- If Windows Update has not been able to obtain updated signatures for Windows Defender for a period of time, Windows Defender will attempt to use MAPS to download signatures from an alternate download location.

To help protect your privacy, all information sent to MAPS is sent encrypted via SSL.

Use of information

Reports sent to MAPS are used to improve Microsoft software and services. The reports might also be used for statistical, testing, or analytical purposes, and for generating definitions. MAPS doesn’t intentionally collect personal information. To the extent that MAPS might unintentionally collect any personal information, Microsoft won’t use the information to identify, contact, or target advertising to you.

Choice and control

If you choose express settings while setting up Windows, you turn on MAPS. If you choose to customize settings, you can control MAPS

by selecting **Help Microsoft respond to malicious apps and malware by joining Microsoft Active Protection Service** under **Send Microsoft info to help make Windows and apps better**. After setting up Windows, you can change your MAPS membership or settings, including turning off MAPS, in the Tools menu in Windows Defender.

History feature

What this feature does

The History feature provides a list of all apps on your PC that Windows Defender detects and the actions that were taken when the apps were detected.

In addition, you can view a list of apps that Windows Defender doesn't monitor while they are running on your PC (these are called allowed items). You can also view apps that Windows Defender prevents from running until you choose to remove them or allow them to run again (these are called quarantined items).

Information collected, processed, or transmitted

The list of software that Windows Defender detects, the actions that you and other users take, and the actions that Windows Defender takes automatically are stored on your PC. All users can view the history in Windows Defender to see malware and other potentially unwanted software that has attempted to install itself or run on the PC, or that has been allowed to run by another user. For example, if you learn about a new malware threat, you can check the History to see if Windows Defender has prevented it from infecting your PC. No information is sent to Microsoft.

Choice and control

History lists can be deleted by an administrator.

Top of Page

Windows Error Reporting

What this feature does

Windows Error Reporting helps Microsoft and Microsoft partners

diagnose problems in the software you use and provide solutions. Not all problems have solutions, but when solutions are available, they are offered as steps to solve a problem you've reported or as updates to install. To help prevent problems and make software more reliable, some solutions are also included in service packs and future versions of the software.

Information collected, processed, or transmitted

Many software products are designed to work with Windows Error Reporting. If a problem occurs in one of these products, you might be asked if you want to report it.

Windows Error Reporting collects information that is useful for diagnosing and solving a problem that has occurred, such as where the problem happened in the software or hardware, the type or severity of the problem, files that help describe the problem, basic software and hardware information, or possible software performance and compatibility problems. If you use Windows to host virtual machines, error reports sent to Microsoft might include information about virtual machines.

Windows Error Reporting also collects information about apps, drivers, and devices to help Microsoft understand and improve app and device compatibility. Information about an app might include the name of the app's executable files. Information about devices and drivers might include the names of devices you've installed on your PC and the executable files associated with those devices' drivers. Information about the company that published an app or driver might be collected.

If you choose to enable automatic reporting while setting up Windows, the reporting service will automatically send basic information about where problems occur. Some error reports might unintentionally contain personal information. For example, a report that contains a snapshot of PC memory might include your name, part of a document you were working on, or data that you recently submitted to a website. If a report is likely to contain this type of information, Windows will ask if you want to send this information, even if you've enabled automatic reporting. Reports including files and data might be stored on your PC until after they have been sent

or deleted.

After you send a report, the reporting service might ask you for more information about the problem that occurred. If you choose to provide your phone number or email address in this information, your error report will be personally identifiable. Microsoft might contact you to request additional information to help solve the problem you reported.

Windows Error Reporting randomly generates a number called a globally unique identifier (GUID) that is sent to Microsoft with every error report. The GUID lets us determine which data is sent from a particular computer over time. The GUID doesn't contain any personal information.

To help protect your privacy, the information is sent encrypted via SSL.

Use of information

Microsoft uses information about errors and problems reported by Windows users to improve Microsoft products and services, as well as third-party software and hardware designed for use with these products and services. We use the GUID to determine how widespread the feedback we receive is and how to prioritize it. For example, the GUID allows Microsoft to distinguish between one customer experiencing a problem one hundred times and one hundred customers experiencing the same problem once.

Microsoft employees, contractors, vendors, and partners might be provided access to relevant portions of the information collected, but they're only permitted to use the information to repair or improve Microsoft products and services, or third-party software and hardware designed for use with Microsoft products and services. If an error report contains personal information, Microsoft doesn't use the information to identify, contact, or target advertising to you. However, if you choose to provide contact information as described above, we may use this information to contact you.

Choice and control

If you choose express settings while setting up Windows, Windows Error Reporting will automatically send basic reports to check for

solutions to problems online. If you choose to customize settings, you can control Windows Error Reporting by selecting **Use Windows Error Reporting to check for solutions to problems** under **Check online for solutions to problems**. After setting up Windows, you can change this setting in Action Center in Control Panel.

For more information, see the Microsoft Error Reporting Service privacy statement .

Top of Page

Windows File Association

What this feature does

Windows File Association helps users associate file types with specific apps. If you try to open a file type and it doesn't have an app associated with it, Windows will ask if you want to use Windows File Association to find an app for the file, which includes searching the Windows Store for a compatible app. Apps that are typically associated with the file name extension are displayed.

Information collected, processed, or transmitted

If you choose to use Windows File Association, the file name extension (for example, docx or pdf) and your PC display language are sent to Microsoft. The rest of the file name isn't sent to Microsoft. When a file association is made with a particular app, a unique identifier for the app is sent to identify the default app for each file type.

Use of information

When you submit a file name extension, the service returns a list of the apps that Microsoft is aware of that can open files of that extension. Unless you choose to download and install an app, no file type associations will change.

Choice and control

When you try to open a file type without an associated app, you can choose whether to use Windows File Association. No file association information is sent to Microsoft unless you decide to use the service.

Top of Page

Windows Help

Windows Online Help and Support

What this feature does

Windows Online Help and Support, when turned on, allows you to get the most up-to-date help and support content available when you're connected to the Internet.

Information collected, processed, or transmitted

When you use Windows Online Help and Support, your help search queries are sent to Microsoft, as well as your requests for help content when a link is clicked. Windows sends some information about your PC's configuration to help find more relevant help content. Windows Online Help and Support also uses standard web technologies like cookies.

Use of information

Microsoft uses the information to return help topics in response to your search queries, to return the most relevant results, to develop new content, and to improve existing content. We use the information about your PC's configuration to display appropriate help content for that configuration. We use cookies and other web technologies to make it easier to navigate help content and to help us better understand how users use Windows Online Help.

Choice and control

Online Help and Support is turned on by default. To change this setting, tap or click the **Settings** icon at the top of the Help and Support window, and then select or clear **Get online Help**. To clear the cookies used by Windows Help, open Internet Options in Control Panel, click or tap the **Delete** button under **Browsing history**, select **Cookies and website data**, and click or tap **Delete**. If you choose to block all cookies (in the Privacy section of Internet Options), Windows Help won't set any cookies.

Help Experience Improvement Program

What this feature does

The Help Experience Improvement Program helps Microsoft identify trends in the way our customers use Windows Online Help and Support so that we can improve our search results and the relevancy of our content.

Information collected, processed, or transmitted

HEIP sends Microsoft information about the version of Windows that your PC is running and about how you use Windows Help and Support, including queries you enter when you search Windows Help and Support and any ratings or feedback on the Help topics presented to you. When you search, browse, or provide any ratings or feedback on the Help topics presented to you, this information will be sent to Microsoft.

HEIP randomly generates a number called a globally unique identifier (GUID) that is sent to Microsoft with every HEIP report. The GUID lets us determine which data is sent from a particular machine over time. The GUID doesn't contain any personal information. The GUID is separate from the GUIDs used by Windows Error Reporting and Windows CEIP.

Use of information

The data collected is used to identify trends and usage patterns so that Microsoft can improve the quality of content we provide and the relevance of our search results. We use the GUID to determine how widespread the issues we receive are and how to prioritize them. For example, the GUID allows Microsoft to distinguish between one customer experiencing an issue one hundred times and one hundred customers experiencing the same issue once.

The Help Experience Improvement Program does not intentionally collect any information that could be used to personally identify you. If you type such information into the search or feedback boxes, the information will be sent, but Microsoft doesn't use this or other information collected to identify, contact, or target advertising to you.

Choice and control

If you choose express settings while setting up Windows, you join the Help Experience Improvement Program. If you choose to customize settings, you can control Help Experience Improvement Program settings by selecting **Help improve Windows Help content by sending info to the Help Experience Improvement Program** under **Send Microsoft info to help make Windows and apps better**. After setting up Windows, you can change this setting in Windows Help and Support.

Top of Page

Remote Assistance

What this feature does

You can use Remote Assistance to invite someone to connect to your PC and help you with a PC problem, even if that person isn't nearby. After connecting, the other person can view your PC. With your permission, the other person can use his or her mouse and keyboard to control your PC and show you how to fix a problem.

Information collected, processed, or transmitted

Remote Assistance creates an encrypted connection between the two PCs over the Internet or the local network. When someone uses Remote Assistance to connect to your PC, that person can see your desktop and any open documents, including any visible private information. In addition, if you allow the other person to control your PC with his or her mouse and keyboard, that person can do things like delete files or change settings. After a connection is made, Remote Assistance will exchange contact information including user name, PC name, and account picture. A session log file maintains a record of all Remote Assistance connections.

Use of information

The information is used to establish an encrypted connection and to provide the other person access to your desktop. No information is sent to Microsoft.

Choice and control

Before you allow someone to connect to your PC, close any open

apps or documents that you don't want the other person to see. If at any time you feel uncomfortable about what that person is seeing or doing on your PC, press the Esc key to end the session. You can disable session logging and contact information exchange by clearing these options in Remote Assistance settings.

Top of Page

Windows Search

What this feature does

Windows Search provides you with a quick and consistent entry point to search for apps, settings, files, or content within apps.

Information collected, processed, or transmitted

When you use Windows Search, the characters you type in the search field (as you type them) and the final search query you submit are only supplied to Windows and any app you're searching in, so Windows or the app can provide search suggestions and show search results. Windows stores search queries and data about how often you search in the apps.

Use of information

Windows uses the stored previous searches to provide search suggestions in the Search pane. The information stored about how often you search in apps is used to sort the list of searchable apps in the Search pane in order of frequency. If you search within a third-party app, use of the information collected will be subject to the third party's privacy practices. If you search within a Microsoft app, the app's privacy practices will be explained in its privacy statement.

Choice and control

Windows stores this information by default. You can disable the storage of this information or delete all of your stored previous searches in Search in PC settings.

Top of Page

Windows Share

What this feature does

Windows Share lets you share content between Windows Store apps that support sharing. It also lets you share content with your friends.

Information collected, processed, or transmitted

When sharing, the source app passes content to the target app only after you select the target in the Share pane. If the source app hasn't implemented sharing, you'll have the option to share an image of whatever appears on the screen. So that you can access them more easily, target apps and people that you frequently share content with will appear in a list in the Share pane. No information is sent to Microsoft.

Use of information

The information stored about how often you share with target apps and people that you frequently share content with is used to sort the list in the Share pane in order of frequency. If you share information with a third-party app, use of the information collected will be subject to the third party's privacy policy. If you share with a Microsoft app, the app's privacy practices will be explained in its privacy statement.

Choice and control

By default, Windows stores information about your use of Windows Share. You can disable the storage of this information or delete all of the stored targets in Share in PC settings.

Top of Page

Windows SmartScreen

What this feature does

Windows SmartScreen helps keep your PC safe by checking files and apps with Microsoft before you open or run them to help protect you from potentially unsafe files and apps. Windows will ask you what you want to do if a file or app is unknown or potentially unsafe before it is opened.

Information collected, processed, or transmitted

If you choose to use this feature, information about some of the apps you use and some of the files you download from the Internet will be sent to Microsoft. This information might include a file name, file identifier ("hash"), and digital certificate information along with standard PC information and the Windows SmartScreen filter version number. To help protect your privacy, the information sent to Microsoft is encrypted via SSL.

Windows SmartScreen randomly generates a number called a globally unique identifier (GUID) that is sent to Microsoft with your SmartScreen usage data. The GUID lets us determine which data is sent from a particular PC over time. The GUID doesn't contain any personal information.

Use of information

Microsoft uses the information described above to provide warnings to you about potentially unsafe files and apps. We also use the information to analyze performance of the feature and to improve the quality of our products and services. We use the GUID to determine how widespread the feedback we receive is and how to prioritize it. For example, the GUID allows Microsoft to distinguish between one customer experiencing a problem one hundred times and one hundred customers experiencing the same problem once. Microsoft doesn't use the information to identify, contact, or target advertising to you.

Choice and control

If you choose express settings while setting up Windows, you turn on Windows SmartScreen. If you choose to customize settings, you can control Windows SmartScreen by selecting **Use Windows SmartScreen Filter to check files and apps with Microsoft** under **Help protect your privacy and your PC**. After setting up Windows, you can change this setting in Action Center in Control Panel.

Top of Page

Windows Speech Recognition

What this feature does

Windows Speech Recognition provides speech recognition within Windows and for any apps that choose to use it. Windows Speech Recognition increases its accuracy by learning how you use language, including the sounds and words you like to use.

Information collected, processed, or transmitted

Windows Speech Recognition stores a list of words and their pronunciations on your PC. Words and pronunciations are added to this list using the Speech Dictionary, and by using Windows Speech Recognition to dictate and correct words.

When the Windows Speech Recognition document review feature is enabled, text from Microsoft Office Word documents (with doc or docx file name extensions) and email (from email folders other than Deleted Items or Junk Mail) on your PC and on any connected file shares included in your Windows search index locations is collected and stored in one-, two-, or three-word fragments. One-word fragments include only words you have added to custom dictionaries, and two- or three-word fragments include only words found in standard dictionaries.

All collected information is stored in your personal speech profile on your PC. Speech profiles are stored for each user, and users aren't able to access the profiles of other users on your PC. However, administrators can access any profile on your PC. The profile information isn't sent to Microsoft unless you choose to send it when asked by Windows Speech Recognition. You can review the data before it is sent. If you choose to send this information, acoustic adaptation data that was used to adapt to your audio characteristics is also sent.

If you complete a speech training session, Windows Speech Recognition will ask you whether you wish to send your speech profile information to Microsoft. You can review the information before it's sent. This information might include recordings of your voice while you completed the training session and the other information from your personal speech profile.

Use of information

Windows Speech Recognition uses words from the speech profile to

convert your speech to text. Microsoft uses personal speech profile information to improve our products and services. We don't use this information to identify, contact, or target advertising to you.

Choice and control

You can choose whether to run Windows Speech Recognition. If you run Windows Speech Recognition, the document review feature is on by default. You can choose to change your document review settings the first time you run Windows Speech recognition. You can change your document review settings or delete personal speech profiles (and most document review information) by going to Speech Recognition in Control Panel and clicking **Advanced speech options**. You can also use the Change existing words option in the Speech Dictionary to delete words that you've added to your speech profile. However, deleting your personal speech profile doesn't delete words added through the Speech Dictionary.

You can control the locations that document review will collect word fragments from by modifying the locations included in your Windows search index. To view or modify what locations are included in your Windows search index, open Indexing Options in Control Panel.

At the end of any training session you'll be given the choice whether to send your training and other profile information to Microsoft. You can also send information when Windows Speech Recognition is launched by right-clicking **Microphone**, and then clicking **Help improve speech recognition**. In either case, you can view all data files before they are sent, and can choose not to send them.

Top of Page

Windows Store

The Windows Store lets you find, manage, and install apps for your PC. The sections below describe how the Store's features, and the apps you obtain through the Store, could impact your privacy, and what you can do to control that.

Store app and service

What this feature does

The Store lets you find and install apps for your PC. It also keeps track of the Store apps you've installed, so you can get updates for them and install them on more than one PC.

Information collected, processed, or transmitted

To find and install apps, you must sign in to the Store with a Microsoft account. This gives the Store access to information in your Microsoft account profile, such as your name, email address, and account picture. The Store collects and associates the following additional information with your Store account:

- Payments to the Store. Information about what you bought, how much you paid, and how you paid when buying apps or making in-app purchases with your Store account.

- Apps you've installed. The list of apps you've installed, the license policy for each app (permanent license or limited-time trial), and a list of purchases you made with your Store account within each app. In addition to storing this information online with your Store account, the Store stores licensing information on your PC for each app you install. This information identifies you as the owner of the license.

- PCs you've installed apps on. The make, model, and computer name of each PC you install apps on, along with a number that uniquely identifies the PC. This number is generated based on the PC's hardware configuration, and doesn't contain any information about you.

- Ratings, reviews, and problem reports. Once you've installed an app, you can write a review or leave a rating for it in the Store. Your Microsoft account is associated with these ratings. If you write a review, the name and picture from your Microsoft account will be published with your review.

- Store preferences. Preferences you set for viewing apps in the Store, such as whether to only display apps that are available in your native language.

You can choose to store your payment information, such as a credit card number, with your Store account. For security purposes, this

information is transmitted over SSL, and all but the last four digits of your credit card number are stored encrypted.

The Store collects some information about your copy of Windows, to determine whether it was sold at retail, is an evaluation copy, is subject to a volume licensing program, or was preinstalled by your PC's manufacturer. When you first connect to the Store, a list of all the apps preinstalled on your PC is sent to the Store, which then associates licenses for those apps with your Store account.

The Store automatically checks for updates to your apps, and it can notify you when new updates are available. To provide updates, the Store sends the following information to Microsoft:

- A list of all the apps installed from the Store by all users on your PC
- The licensing information for each app, including the owner of each license
- Your Windows Update and/or Microsoft Update configuration settings, such as whether you want updates automatically downloaded or installed.
- The successes, failures, and errors you experience when updating apps from the Store.
- Globally Unique Identifier (GUID) – a randomly generated number that doesn't contain any personal information. GUIDs are used to identify individual PCs without identifying the user.
- BIOS name, revision number, and revision date – information about the set of essential software routines that test your hardware, start the operating system on your computer, and transfer data among hardware devices connected to your computer.

As you browse the Store and use apps from it, Microsoft collects some information to help us understand usage patterns and trends, similar to the way many websites analyze their visitors' browsing data. None of this activity data is used to identify or contact you.

Use of information

Microsoft uses your contact information to send you email necessary to provide the Store services, such as receipts for apps you buy. It uses your payment information to let you pay for purchases; if you choose to store this information, you won't need to enter it every time. Microsoft uses information about your purchases to operate the Store and provide customer support.

The Store keeps track of all the apps you've installed. You can use the Store to manage the list of devices you've installed apps on, and customer support can also help you manage this information. Once you install an app, you'll always be able to see it in your Store purchase history, even if you choose to uninstall it. The Store also uses this list to help enforce the limit on the number of PCs you can install apps on, as described in the Windows Store terms of use. When you write a review for an app, the name and account picture associated with your Windows account will be published next to the review in the Store. If you report a problem with an app, the problem report is made available to Store representatives to assess and take action on. They might use your name and the email address associated with your Store account to contact you, if necessary, when they review the report.

When there are updates available to apps you've installed, a notification will display in the Store, and the Store's app tile will indicate the number of available updates. You can then view the list of available updates and choose which ones to install. Updated apps might use different Windows capabilities than the previous versions, which could give them access to different resources on your PC. You can see the updated lists of capabilities on the App Description pages linked to from the page listing available updates.

The Store uses the information it collects about your copy of Windows to determine how Windows was installed on your PC (for example, whether your PC's manufacturer preinstalled it). This information allows the Store to let you access apps provided exclusively by that manufacturer for its customers. It is also used to provide information to Microsoft (and in aggregate to the manufacturer, in some cases) about Windows usage patterns.

Microsoft uses some app purchase and usage data in aggregate to

learn how people use the Store (for example, how users find the apps they install). Microsoft might share some of these aggregate statistics with app developers. Microsoft doesn't share any of your personal information with app developers. We use the browsing and usage data collected by the Store to better understand how people use the Store, and to improve Store features and services.

Choice and control

If you choose to use the Store, the information described in this section will be sent to Microsoft as described above.

If you want to remove a review that you have published for an app, go to the app description in the Store, edit your review, and delete all the text.

Permission for Store apps

What this feature does

Many apps you install from the Windows Store are designed to take advantage of specific hardware and software features of your PC. For example, a photo app might need to use your webcam, and a restaurant guide might need to know your location to provide nearby recommendations.

Information collected, processed, or transmitted

Here’s a list of features that apps must disclose they use:

- Your Internet connection. Allows the app to connect to the Internet.
- Incoming connections through a firewall. Allows the app to send information to or from your PC through a firewall.
- A home or work network. Allows the app to send information between your PC and other PCs on the same network
- Your pictures, videos, music, or documents libraries. Allows the app to access, change, or delete files in your libraries. This includes access to any additional data embedded in these files, such as location information in photos.
- Removable storage. Allows the app to access, add, change, or

delete files on an external hard drive, USB flash drive, or portable device.

- Your Windows credentials. Allows the app to use your credentials to authenticate and provide access to a corporate intranet.
- Certificates stored on your PC or a smart card. Allows the app to use certificates to securely connect to organizations like banks, government agencies, or your employer.
- Your PC's text messaging feature. Allows the app to send and receive text messages.
- Your webcam and microphone. Allows the app to take pictures and record audio and video.
- Your location. Allows the app to determine your approximate location based on a GPS sensor or network information.
- Your PC's near-field communication feature. Allows the app to connect to other nearby devices that the same app is running on.
- Your portable devices. Allows the app to communicate with devices like your mobile phone, digital camera, or portable music player.
- Your information on a portable device. Allows the app to access, add, change, or delete contacts, calendars, tasks, notes, status, or ringtones on your portable device.
- Your mobile broadband account. Allows the app to manage your mobile broadband account.

You'll see the features an app uses listed on its App Description page. If you install an app, Windows will allow it to use these features, except for location, text messaging, and webcam and microphone, which are considered especially sensitive. When an app requests access to one of these sensitive features for the first time, Windows will ask you whether you want to allow the app to use it. You can change whether the app can use it at any time.

Use of information

Each app's use of these features will be subject to its developer's privacy practices. If an app uses one of the sensitive features described above, a link to the app publisher's privacy statement will be available on its App Description page in the Store.

Choice and control

You can see what features an app requires in the Store before installing the app. Windows will ask whether you want to allow or deny access to the most sensitive of these features—location, text messaging, webcam, and microphone—before the first time each app uses them.

When you look at an app's App Description page in the Windows Store, there will be an abbreviated list of the features used by the app at the bottom of the left column. You can see the full list on the Details page of the App Description. After you install an app, you can see the full list of features it uses at any time, and control its access to the especially sensitive ones. To do this, open the app, click or tap the Settings charm, and then select **Permissions**.

Help improve the Windows Store by sending URLs for web content that apps use

What this feature does

Some apps you get from the Store are like websites and might expose your computer to potentially unsafe software, such as malware. If you choose to turn this feature on, it collects information about the web content used by these apps to help Microsoft diagnose potentially unsafe behavior. For example, we might use this information to remove an app from the Store.

Information collected, processed, or transmitted

If you choose to send information about the web content used by your apps, Microsoft will collect information about the URLs and types of content that these apps access when you use them. This can help us identify which of these apps are receiving content from harmful or unsafe websites. Reports sent to Microsoft include information such as the name or identifier of the app, the full URLs of addresses the app accesses, and full URLs that indicate the

location of any JavaScript that the app accesses. Windows generates a number called a globally unique identifier (GUID) that is sent to Microsoft with each report. The GUID lets us determine which data is sent from a particular computer over time. The GUID doesn't contain any personal information and isn't used to identify you.

To help protect your privacy, the information sent to Microsoft is encrypted. Information that might be associated with a webpage that these apps access, such as search terms or data you entered into apps, might be included. For example, if you look up a word in a dictionary app, the word you look up might be included in the information sent to Microsoft as part of the full address accessed by the app. Microsoft filters these addresses to try to remove personal information where possible.

Use of information

Microsoft periodically reviews the information sent to help detect apps that might be interacting with unsafe web content, such as harmful web addresses or scripts. We might use this information to take action against potentially harmful apps. Addresses of web content can unintentionally contain personal information, but this information isn't used to identify, contact, or target advertising to you. We use the GUID to determine how widespread the feedback we receive is and how to prioritize it. For example, the GUID allows Microsoft to distinguish between potentially unsafe behavior occurring 100 times on a single PC, and the same behavior occurring once on each of 100 PCs.

Choice and control

If you choose express settings while setting up Windows, Windows will send information about the web content used by your apps from the Store built using JavaScript. If you choose to customize settings, you can control this setting by selecting **Help improve Windows Store by sending URLs for web content that apps use** under **Send Microsoft info to help make Windows and apps better** . After installation, you can change this setting in Privacy in PC settings.

Top of Page

Windows Time Service

What this feature does

The Windows Time service automatically synchronizes your PC's time with a time server on a network.

Information collected, processed, or transmitted

The service connects to a time server over the Internet or a local network using the industry standard Network Time Protocol. By default, this service synchronizes with time.windows.com once a week. No information other than standard PC information is sent to the time server.

Use of information

Information is used by the Windows Time service to automatically synchronize the local PC's time.

Choice and control

The Windows Time service is turned on by default. You can turn this feature off or choose your preferred time source by going to Date and Time in Control Panel, choosing the Internet Time tab, and clicking **Change Settings**. Turning off Windows Time Service has no direct effect on apps or other services, but without a reliable time source, the local PC's clock might get out of sync with other PCs on the network or Internet. Apps and services that depend on time might fail or stop working correctly if there is a significant time discrepancy between networked PCs.

Top of Page

Windows Troubleshooting

What this feature does

Windows Troubleshooting allows you to diagnose and fix common problems on your PC.

Information collected, processed or transmitted

After running a troubleshooting pack, the results are saved to your PC. These results might contain personal information, such as your

user name or the name of a device. Windows Troubleshooting can help you search for problem solutions in Windows Help and Windows communities online. Keywords associated with the problem will be sent to Microsoft to help find a solution. For example, if your printer isn't working properly and you look for help, the words "printer," "print," and "printing" are sent to Microsoft.

Use of information

Microsoft uses the information collected from Windows Troubleshooting to help solve problems our users encounter.

Choice and control

If you choose express settings during Windows setup, Windows Troubleshooting will search for online troubleshooting packs by default. To change these settings, To delete Troubleshooting results, go to Troubleshooting in Control Panel. Click **View history**, select a result, and then click **Delete**.

Top of Page

For up-to-date information on Microsoft's data processing practices, please review the Microsoft Privacy Statement. Here you can also learn about the latest tools we provide to access and control your data and how to contact us if you have a privacy inquiry.

Windows 8 and Windows Server 2012 Privacy Statement

In this page

Last updated: **August 2012**

This page is a supplement to the Windows 8 and Windows Server 2012 Privacy Statement ("Windows Privacy Statement"). The Privacy Statement includes four sections:

- Highlights
- Statement, which is the full Windows Privacy Statement that includes links for Windows features that have their own stand-alone statements
- Features Supplement, which describes the features that have a privacy impact in Windows 8 and Windows Server 2012
- Server Supplement (this document), which describes the additional features that have privacy impact in Windows Server 2012

To understand the data collection and use practices relevant for a particular feature or service of Windows, you should read the full Windows Privacy Statement and any applicable supplement. In addition, you should read this white paper for administators.

User Access Logging

What this feature does

User Access Logging (UAL) collects and aggregates records of client requests of server roles (both user and device requests) and installed products (if registered with UAL) on the local server. This data—in the form of IP addresses, user names, and in some cases, host names and/or virtual machine identities—is stored in the local Extensible Storage Engine (ESE) databases and is only accessible by administrators. UAL has a WMIv2 provider and associated Windows PowerShell cmdlets for retrieving user access data that is intended for offline customer Client Access License (CAL) entitlement management, where actual records of unique client requests are critical.

Information collected, processed, or transmitted

IP addresses, user names, and in some cases, host names (if DNS role is installed), and virtual machine identities (if Hyper–V role is installed) are collected locally on the server when UAL is turned on. No collected data is sent to Microsoft.

Use of information

UAL data is made available to administrators through local ESE databases, the WMI provider, and Windows PowerShell cmdlets. Windows does not make use of this data outside of the UAL feature itself.

Choice and control

UAL is enabled by default. The UAL service can be stopped and started while the server is running. To disable UAL permanently, open Windows PowerShell, type Disable-UAL, and restart the server. An administrator can delete all historical data collected, by first stopping the service, disabling UAL, then deleting all files in the folder %SystemRoot%\System32\LogFiles\SUM\.

Top of Page

Server Manager

What this feature does

Server Manager is a management tool that enables an administrator to monitor either one or multiple servers, and to view general or role-specific status—to perform management tasks and access other server management tools.

Information collected, processed, or transmitted

Server Manager collects the following types of information from a server the administrator manages:

- **General server information:** NetBios name and fully qualified domain name (FQDN), account credentials entered in the "Manage as" feature, IPv4 address, IPv6 address, manageability status, description, operating system version, type, last update, processors, memory, cluster name, cluster object type, activation status, SKU, operating system architecture, manufacturer, Customer Experience Improvement Program (CEIP) configuration, and Windows Error Reporting (WER) configuration.

- **Events:** ID, severity, source, log, date, and time for each event from Windows and other logs that the administrator chooses.

- **All services:** name, status, and start type.

- **Server role information:** Best Practice Analyzer (BPA) results for roles that are installed on the server.

- **Performance information:** samples for performance counters, and notifications for CPU usage and available memory.

Use of information

This information is stored in Server Manager and is not sent to Microsoft. It is displayed in Server Manager to help administrators monitor systems.

Choice and control

An administrator can opt in or out of collecting data from any server

except the local server by adding or removing the server in Server Manager. An administrator can explicitly provide credentials to connect to a remote server. Server Manager asks for the administrator to explicitly consent to store the credentials locally in Server Manager, and the administrator can delete these credentials at any time.

Top of Page

Active Directory Federation Services

What this feature does

Active Directory Federation Services (AD FS) is an enterprise-ready federation and single-sign-on solution for local or other network-based applications. AD FS helps administrators enable users to collaborate across organizations and to easily access applications on local or other networks, while maintaining application security. AD FS uses a security token service that uses Active Directory Domain Services (AD DS) to authenticate users and issue them security tokens using various protocols. The token is digitally signed and contains claims about the user, which come from each or any combination of AD DS, Lightweight Directory Access Protocol (LDAP), SQL Server, or a custom store.

Information collected, processed, or transmitted

A user’s credentials are collected when the user authenticates with AD FS. The credentials are immediately sent to Active Directory Domain Services for authentication, and AD FS doesn't store them locally. The user’s attributes in Active Directory Domain Services might be used to generate outgoing claims, depending on the claim rules that an AD FS administrator has configured. Outgoing claims will be sent to trusted partners that an AD FS administrator has established a trust relationship with. No information is sent to Microsoft.

Use of information

Microsoft won’t have access to this information. This information is intended for use by the customer only.

Choice and control

Use AD FS if you want AD FS to collect or send data to trusted partners.

Top of Page

IP Address Management

What this feature does

IP Address Management (IPAM) enables server administrators to track the IP address, host name, and client identifier (such as the MAC address in IPv4 and DUID in IPv6) of computers or devices on a network with user logon information.

Information collected, processed, or transmitted

The IPAM server collects audit logs and events from DHCP servers, domain controllers, and network policy servers, and then locally stores the IP address, host name, client identifier, and user name of the logged-on user. A server administrator can search the collected logs based on IP address, client identifier, host name, and user name using the IPAM console. None of this information is sent to Microsoft.

Use of information

Microsoft doesn't have access to this information. This information is intended for use by the customer only.

Choice and control

IPAM is not installed by default and must be installed by the server administrator. After IPAM is installed, IP address auditing is automatically enabled. To disable IP address auditing on a server where IPAM is installed, start Task Scheduler on the IPAM server, browse to Audit Task under Microsoft\Windows\IPAM, and then disable the task.

Top of Page

Unified Remote Access

What this feature does

Unified Remote Access allows remote users to connect to a private network, such as a corporate network, over the Internet. Unified Remote Access uses DirectAccess to provide remote client computers running Windows 8 with uninterrupted and transparent connectivity to corporate networks. It also provides Remote Access Service (RAS) functionality, which is traditional VPN services, including site-to-site local or other network connectivity.

Information collected, processed, or transmitted

FFor Unified Remote Access user monitoring, the DirectAccess server stores the details of remote users connecting to the private network. This includes information such as host name of the remote user, Active Directory user name, and public IP address of the remote client (if the client is behind network address translation (NAT), it will be the public IP address). This data can also be stored in the Windows Internal Database (WID)/RADIUS servers, only with administrator consent. Only a DirectAccess administrator (a domain user with a local administrator account) accessing a server can access and view this information.

Use of information

This information will be used by the administrator for troubleshooting client connectivity and also for audit or compliance purposes. No information is sent to Microsoft.

Choice and control

Remote client monitoring is enabled by default and cannot be disabled. The monitoring data is stored in the WID/RADIUS servers only if an administrator has configured accounting to use any of these options. If an administrator has not configured accounting, none of this information will be stored. An administrator can also configure accounting on a remote access server to not store user name and IP address information.

Top of Page

Remote Desktop Services

What this feature does

Remote Desktop Services (RDS) provides a platform to help companies implement a centralized desktop strategy, manage desktops and application, and improve flexibility and compliance while improving data security.

Information collected, processed, or transmitted

For RDS user monitoring, the Remote Desktop Session Host server stores information about remote users connecting to RDS resources. This includes information such as host name of the remote user, Active Directory user name, and public IP address of the remote client (if client is behind network address translation (NAT), it will be the public IP address). This data is stored automatically in the Windows Internal Database (WID)/SQL servers when users connect. No information is sent to Microsoft. Only a domain user who has a local administrator account can access and view this information.

Use of information

This information will be used by the administrator for troubleshooting client connectivity and also for internal audit or compliance purposes. No information is sent to Microsoft.

Choice and control

Client monitoring is enabled by default and cannot be disabled. The monitoring information is stored in the WID/SQL server.

Top of Page

Windows Customer Experience Improvement Program (CEIP) and Windows Error Reporting (WER)

What this feature does

For more information about these features, see the Features Supplement tab or this white paper for administators.

Information collected, processed, or transmitted

To learn about the specific information that is collected, processed, and transmitted by these features, please see CEIP and WER on the Features Supplement tab.

Use of information

To learn about how we use information that is collected by these features, see CEIP and WER on the Features Supplement tab.

Choice and control

CEIP is off by default, and WER is set by default to prompt you before sending crash reports to Microsoft. You can turn CEIP on and off from Server Manager and Control Panel, and by using command-line methods of control. WER can be controlled by using command-line methods only.

To turn CEIP on or off using the Control Panel, click **System and Maintenance**, and click **Problem Reports and Solutions**. Then, in the left pane, under See also, click **Customer Experience Improvement Settings** for the option to turn CEIP on or off.

Server Manager controls

Local server

- Enable CEIP
  Open Server Manager and select **Local Server**. Click the Customer Experience Improvement Program link, select **Yes, I want to participate in the CEIP** in the dialog box, and then click **OK.**

- Disable CEIP
  Open Server Manager and select **Local Server**. Click the Customer Experience Improvement Program link and select **No, I don't want to participate** in the dialog box, and then click **OK.**

- Enable WER
  Open Server Manager and select **Local Server**. Click the Windows Error Reporting link, select **Yes, automatically send summary reports**, and then click **OK**.

- Disable WER
  Open Server Manager and select **Local Server**. Click the Windows Error Reporting link, select **select I don't want to participate, and don't ask me again**, and then click **OK**.

Multi-machine

- Enable CEIP
  Open Server Manager and select **All Servers**. In the Servers tile, select all servers (Ctrl+A), right-click and select **Configure Windows Automatic Feedback** . On the Customer Experience Improvement Program tab, select **Yes, I want to participate (Recommended)**. Apply this setting to all servers by selecting the check box next to Server Name in the Select Servers control, and then click **OK**.

- Disable CEIP
  Open Server Manager and select All Servers. In the Servers tile, select all servers (Ctrl+A), right-click and select **Configure Windows Automatic Feedback** . On the Customer Experience Improvement Program tab, select **No, I don't want to participate**. Apply this setting to all servers by selecting the check box next to Server Name in the Select Servers control, and then click **OK.**

- Enable WER
  Open Server Manager and select **All Servers**. In the Servers tile, select all servers (Ctrl+A), right-click and select **Configure Windows Automatic Feedback** . On the Windows Error Reporting tab, select **Yes, automatically send summary reports (Recommended)**. Apply this setting to all servers by selecting the check box next to Server Name in the Select Servers control, and then click **OK**.

- Disable WER
  Open Server Manager and select **All Servers**. In the Servers tile, select all servers (Ctrl+A), right-click and select **Configure Windows Automatic Feedback** . On the Windows Error Reporting tab, select **No, I don't want to participate**. Apply this setting to all servers by selecting the check box next to Server Name in the Select Servers control, and then click **OK**.

Top of Page