Windows Telemetry options

Configure Windows diagnostic data in your organization

Applies to

- Windows 10 Enterprise
- Windows 10 Mobile
- Windows Server

This article applies to Windows and Windows Server diagnostic data only. It describes the types of diagnostic data we may gather, the ways you might manage it in your organization, and some examples of how diagnostic data can provide you with valuable insights into your enterprise deployments. Microsoft uses the data to quickly identify and address issues affecting its customers.

Manage enterprise diagnostic data level

Enterprise management

Sharing diagnostic data with Microsoft is enabled by default on Windows 10, 1903 and later. Sharing this data provides many benefits to enterprises, so we do not recommend turning it off. For most enterprise

customers, simply adjusting the diagnostic data level and managing specific components is the best option.

Customers can set the diagnostic data level in both the user interface and with existing management tools. Users can change the diagnostic data level in the **Diagnostic data** setting. In the **Settings** app, in **Privacy** > **Diagnostics & feedback**. They can choose between Basic and Full. The Enhanced level will only be displayed as an option when Group Policy or Mobile Device Management (MDM) are invoked with this level. The Security level is not available.

IT pros can use various methods, including Group Policy and Mobile Device Management (MDM), to choose a diagnostic data level. If you're using Windows 10 Enterprise, Windows 10 Education, or Windows Server, the Security diagnostic data level is available when managing the policy. Setting the diagnostic data level through policy sets the upper boundary for the users' choices. To disable user choice after setting the level with the policy, you will need to use the "Configure telemetry opt-in setting user interface" group policy. The remainder of this article describes how to use group policy to configure levels and settings interface.

Manage your diagnostic data settings

Use the steps in this article to set and/or adjust the diagnostic data settings for Windows and Windows Server in your organization.

Important

These diagnostic data levels only apply to Windows and Windows Server components and apps that use the Connected User Experiences and Telemetry component. Non-Windows components, such as Microsoft Office or other 3rd-party apps, may communicate with their cloud services outside of these diagnostic data levels. You should work with your app vendors to understand their diagnostic data policy, and how you can to opt in or opt out. For more information on how Microsoft Office uses diagnostic data, see Overview of privacy controls for Office 365 ProPlus.

The lowest diagnostic data setting level supported through management policies is **Security**. The lowest diagnostic data setting supported through the Settings UI is **Basic**. The default diagnostic data setting for Windows Server is **Enhanced**.

Configure the diagnostic data level

You can configure your device's diagnostic data settings using the management tools you're already using, such as Group Policy, MDM, or Windows Provisioning. You can also manually change your settings using Registry Editor. Setting your diagnostic data levels through a

management policy sets the upper level for diagnostic data on the device.

Use the appropriate value in the table below when you configure the management policy.

Table 4

Level	Value
Security	**0**
Basic	**1**
Enhanced	**2**
Full	**3**

Note

When both the Computer Configuration policy and User Configuration policy are set, the more restrictive policy is used.

Use Group Policy to set the diagnostic data level

Use a Group Policy object to set your organization’s diagnostic data level.

1. From the Group Policy Management Console, go to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Data Collection and Preview Builds**.

2. Double-click **Allow Telemetry**.
3. In the **Options** box, select the level that you want to configure, and then click **OK**.

Use MDM to set the diagnostic data level

Use the Policy Configuration Service Provider (CSP) to apply the System/AllowTelemetry MDM policy.

Use Registry Editor to set the diagnostic data level

Use Registry Editor to manually set the registry level on each device in your organization or you can write a script to edit the registry. If a management policy already exists, such as Group Policy or MDM, it will override this registry setting.

1. Open Registry Editor, and go to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection**.
2. Right-click **DataCollection**, click New, and then click **DWORD (32-bit) Value**.
3. Type **AllowTelemetry**, and then press ENTER.
4. Double-click **AllowTelemetry**, set the desired value from the table above, and then click **OK.**

5. Click **File** > **Export**, and then save the file as a .reg file, such as **C:\AllowTelemetry.reg**. You can run this file from a script on each device in your organization.

Additional diagnostic data controls

There are a few more settings that you can turn off that may send diagnostic data information:

- To turn off Windows Update diagnostic data, you have two choices. Either turn off Windows Update, or set your devices to be managed by an on premises update server, such as Windows Server Update Services (WSUS) or Microsoft Endpoint Configuration Manager.
- Turn off **Windows Defender Cloud-based Protection** and **Automatic sample submission** in **Settings** > **Update & security** > **Windows Defender**.
- Manage the Malicious Software Removal Tool in your organization. For more info, see Microsoft KB article 891716.
- Turn off **Improve inking and typing** in **Settings** > **Privacy**. At diagnostic data levels **Enhanced** and **Full**, Microsoft uses Linguistic Data Collection info to improve language model features such as autocomplete, spellcheck, suggestions, input pattern recognition, and dictionary.

Note

Microsoft does not intend to gather sensitive information, such as credit card numbers, usernames and passwords, email addresses, or other similarly sensitive information for Linguistic Data Collection. We guard against such events by using technologies to identify and remove sensitive information before linguistic data is sent from the user's device. If we determine that sensitive information has been inadvertently received, we delete the information.

Diagnostic data levels

These levels are available on all desktop and mobile editions of Windows 10, except for the **Security** level, which is limited to Windows 10 Enterprise, Windows 10 Education, Windows 10 Mobile Enterprise, Windows 10 IoT Core (IoT Core), and Windows Server.

Security level

The Security level gathers only the diagnostic data info that is required to keep Windows devices, Windows Server, and guests protected with the latest security updates. This level is only available on Windows Server, Windows 10 Enterprise, Windows 10 Education, Windows 10 Mobile Enterprise, and Windows IoT Core editions.

Note

If your organization relies on Windows Update for updates, you shouldn't use the **Security** level. Because no Windows Update information is gathered at this level, important information about update failures is not sent. Microsoft uses this information to fix the causes of those failures and improve the quality of our updates.

Windows Server Update Services (WSUS) and Microsoft Endpoint Configuration Manager functionality is not affected at this level, nor is diagnostic data about Windows Server features or System Center gathered.

The data gathered at this level includes:

- **Connected User Experiences and Telemetry component settings**. If general diagnostic data has been gathered and is queued, it is sent to Microsoft. Along with this diagnostic data, the Connected User Experiences and Telemetry component may download a configuration settings file from Microsoft's servers. This file is used to configure the Connected User Experiences and Telemetry component itself. The data gathered by the client for this request includes OS information, device id (used to identify what specific device is requesting settings) and device class (for example, whether the device is server or desktop).

- **Malicious Software Removal Tool (MSRT)** The MSRT infection report contains information, including device info and IP address.

  Note

  You can turn off the MSRT infection report. No MSRT information is included if MSRT is not used. If Windows Update is turned off, MSRT will not be offered to users. For more info, see Microsoft KB article 891716.

- **Windows Defender/Endpoint Protection**. Windows Defender and System Center Endpoint Protection requires some information to function, including: anti-malware signatures, diagnostic information, User Account Control settings, Unified Extensible Firmware Interface (UEFI) settings, and IP address.

  Note

  This reporting can be turned off and no information is included if a customer is using third-party antimalware software, or if Windows Defender is turned off. For more info, see Windows Defender.

  Microsoft recommends that Windows Update, Windows Defender, and MSRT remain enabled unless the enterprise uses alternative solutions such as Windows Server Update Services, Microsoft Endpoint Configuration Manager, or a third-party antimalware

solution. Windows Update, Windows Defender, and MSRT provide core Windows functionality such as driver and OS updates, including security updates.

For servers with default diagnostic data settings and no Internet connectivity, you should set the diagnostic data level to **Security**. This stops data gathering for events that would not be uploaded due to the lack of Internet connectivity.

No user content, such as user files or communications, is gathered at the **Security** diagnostic data level, and we take steps to avoid gathering any information that directly identifies a company or user, such as name, email address, or account ID. However, in rare circumstances, MSRT information may unintentionally contain personal information. For instance, some malware may create entries in a computer's registry that include information such as a username, causing it to be gathered. MSRT reporting is optional and can be turned off at any time.

Basic level

The Basic level gathers a limited set of data that's critical for understanding the device and its configuration. This level also includes the **Security** level data. This level helps to identify problems that can occur on a specific hardware or software configuration. For example, it can help determine if crashes are more frequent on devices with a

specific amount of memory or that are running a specific driver version. The Connected User Experiences and Telemetry component does not gather diagnostic data about System Center, but it can transmit diagnostic data for other non-Windows applications if they have user consent.

This is the default level for Windows 10 Education editions, as well as all desktop editions starting with Windows 10, version 1903.

The normal upload range for the Basic diagnostic data level is between 109 KB - 159 KB per day, per device.

The data gathered at this level includes:

- **Basic device data**. Helps provide an understanding about the types of Windows devices and the configurations and types of native and virtualized Windows Servers in the ecosystem. Examples include:
    - Device attributes, such as camera resolution and display type
    - Internet Explorer version
    - Battery attributes, such as capacity and type
    - Networking attributes, such as number of network adapters, speed of network adapters, mobile operator network, and IMEI number
    - Processor and memory attributes, such as number of cores, architecture, speed, memory size, and firmware

    - Virtualization attribute, such as Second Level Address Translation (SLAT) support and guest operating system
    - Operating system attributes, such as Windows edition and virtualization state
    - Storage attributes, such as number of drives, type, and size
- **Connected User Experiences and Telemetry component quality metrics**. Helps provide an understanding about how the Connected User Experiences and Telemetry component is functioning, including % of uploaded events, dropped events, and the last upload time.
- **Quality-related information**. Helps Microsoft develop a basic understanding of how a device and its operating system are performing. Some examples are the device characteristics of a Connected Standby device, the number of crashes or hangs, and application state change details, such as how much processor time and memory were used, and the total uptime for an app.
- **Compatibility data**. Helps provide an understanding about which apps are installed on a device or virtual machine and identifies potential compatibility problems.
    - **General app data and app data for Internet Explorer add-ons**. Includes a list of apps that are installed on a native or virtualized instance of the OS and whether these apps function correctly after an upgrade. This app data includes

the app name, publisher, version, and basic details about which files have been blocked from usage.

  - **Internet Explorer add-ons**. Includes a list of Internet Explorer add-ons that are installed on a device and whether these apps will work after an upgrade.
  - **System data**. Helps provide an understanding about whether a device meets the minimum requirements to upgrade to the next version of the operating system. System information includes the amount of memory, as well as information about the processor and BIOS.
  - **Accessory device data**. Includes a list of accessory devices, such as printers or external storage devices, that are connected to Windows PCs and whether these devices will function after upgrading to a new version of the operating system.
  - **Driver data**. Includes specific driver usage that's meant to help figure out whether apps and devices will function after upgrading to a new version of the operating system. This can help to determine blocking issues and then help Microsoft and our partners apply fixes and improvements.

- **Microsoft Store**. Provides information about how the Microsoft Store performs, including app downloads, installations, and

updates. It also includes Microsoft Store launches, page views, suspend and resumes, and obtaining licenses.

Enhanced level

The Enhanced level gathers data about how Windows and apps are used and how they perform. This level also includes data from both the **Basic** and **Security** levels. This level helps to improve the user experience with the operating system and apps. Data from this level can be abstracted into patterns and trends that can help Microsoft determine future improvements.

This level is needed to quickly identify and address Windows and Windows Server quality issues.

The normal upload range for the Enhanced diagnostic data level is between 239 KB - 348 KB per day, per device.

The data gathered at this level includes:

- **Operating system events**. Helps to gain insights into different areas of the operating system, including networking, Hyper-V, Cortana, storage, file system, and other components.
- **Operating system app events**. A set of events resulting from Microsoft applications and management tools that were downloaded from the Store or pre-installed with Windows or

Windows Server, including Server Manager, Photos, Mail, and Microsoft Edge.

- **Device-specific events**. Contains data about events that are specific to certain devices, such as Surface Hub and Microsoft HoloLens. For example, Microsoft HoloLens sends Holographic Processing Unit (HPU)-related events.
- **Some crash dump types**. All crash dump types, except for heap dumps and full dumps.

If the Connected User Experiences and Telemetry component detects a problem on Windows 10 that requires gathering more detailed instrumentation, the Connected User Experiences and Telemetry component at the **Enhanced** diagnostic data level will only gather data about the events associated with the specific issue.

Full level

The Full level gathers data necessary to identify and to help fix problems, following the approval process described below. This level also includes data from the Basic, Enhanced, and Security levels.

Additionally, at this level, devices opted in to the Windows Insider Program will send events, such as reliability and app responsiveness. that can show Microsoft how pre-release binaries and features are performing. These events help us make decisions on which builds are

flighted. All devices in the Windows Insider Program are automatically set to this level.

If a device experiences problems that are difficult to identify or repeat using Microsoft's internal testing, additional data becomes necessary. This data can include any user content that might have triggered the problem and is gathered from a small sample of devices that have both opted into the **Full** diagnostic data level and have exhibited the problem.

However, before more data is gathered, Microsoft's privacy governance team, including privacy and other subject matter experts, must approve the diagnostics request made by a Microsoft engineer. If the request is approved, Microsoft engineers can use the following capabilities to get the information:

- Ability to run a limited, pre-approved list of Microsoft certified diagnostic tools, such as msinfo32.exe, powercfg.exe, and dxdiag.exe.
- Ability to get registry keys.
- All crash dump types, including heap dumps and full dumps.

Note

Crash dumps collected at this diagnostic data level may unintentionally contain personal data, such as portions of memory from a documents, a web page, etc.