



System Center

Applies to Windows Server 2016 Technical Preview

WINDOWS SERVER 2016 AND SYSTEM CENTER 2016 TELEMETRY

Technical Overview White Paper

May, 2016

Contents

Summary	1
Overview	1
How does Microsoft protect the security of the data?	2
Data collection	2
Data transmission	2
Data use and access	3
Data retention.....	3
What data is gathered at different telemetry levels?	3
Security level.....	4
Basic level.....	5
Enhanced level	6
Full level	6
How can enterprises manage telemetry collection?	7
Configure the operating system telemetry level	7
Use Group Policy to set the telemetry level	7
Use MDM to set the telemetry level	8
Turn off telemetry collection in System Center 2016 for the enterprise	8
Additional telemetry controls.....	8
Examples of how Microsoft uses the telemetry data.....	9
Drive higher apps and driver quality in the ecosystem	9
Reduce your total cost of ownership and downtime	9
Build features that address our customers' needs.....	9

Summary

This document provides our server and enterprise customers with the necessary information to make informed decisions about how to configure telemetry in their environments. It discusses telemetry as system data that is uploaded by the Connected User Experience and Telemetry component. In this document we will focus on the telemetry data from **Windows Server 2016** and **System Center 2016**. We will discuss how we use it to troubleshoot problems and improve our products and services. There will also be some references to Windows 10 because the underlying infrastructure in Windows Server is the same.

Note This whitepaper does not apply to System Center Configuration Manager, System Center Endpoint Protection, or System Center Data Protection Manager because those components use a different telemetry service from Windows and Windows Server.

It describes the steps that Microsoft takes to help protect the security and privacy of our customers' data, the types of telemetry we gather, and the ways an enterprise can manage its telemetry. The document also lists some examples of how telemetry can provide you with valuable insights into your enterprise deployments, and how Microsoft uses the data to quickly identify and address issues that affect its customers.

We understand that the privacy and security of our customers' information is very important. We have taken a thoughtful and comprehensive approach to customer privacy and the protection of customer data with Windows, Windows Server, and System Center. IT administrators have controls to customize features and privacy settings at any time. Our commitment to transparency and trust is clear:

- We are open with customers about the types of data we gather.
- We put enterprise customers in control—they can customize their own privacy settings.
- We put customer privacy and security first.
- We are transparent about how telemetry gets used.
- We use telemetry to improve customer experiences.

Overview

In previous versions of Windows and Windows Server, Microsoft used telemetry to check for updated or new Windows Defender signatures, check whether Windows Update installations were successful, gather reliability information through the Reliability Analysis Component (RAC) on Windows Server, and gather reliability information through the Windows Customer Experience Improvement Program (CEIP) on Windows. In Windows 10 and Windows Server 2016 Technical Preview, you can control telemetry streams by using Settings > Privacy, Group Policy, or Mobile Device Management (MDM).

Microsoft is committed to improving customer experiences in a mobile-first and cloud-first world, and it all starts with our customers. Telemetry is one critical way Microsoft is using data to improve our products and services. Telemetry gives every enterprise customer a voice that helps us shape future versions of Windows, Windows Server, and System Center. This allows us to respond quickly to your feedback, and provide new features and improved quality to our customers.

Our goal is to leverage the aggregated data to drive changes in the product and ecosystem to improve our customer experiences. We are also partnering with enterprises to provide added value from the telemetry information that is shared by their devices. Some examples include identifying outdated patches and downloading the latest antimalware signatures to help keep their devices secure, identifying application compatibility issues prior to upgrades, and gaining insights into driver reliability issues affecting other customers.

How does Microsoft protect the security of the data?

Data collection

Windows 10 and Windows Server 2016 include the Connected User Experience and Telemetry component, which uses the Event Tracing for Windows (ETW) trace logging¹ technology to gather and store telemetry events and data. The operating system and some Microsoft management solutions like System Center use the same logging technology.

1. Operating system features and some management applications are instrumented to publish events and data. Examples of management applications include Virtual Machine Manager (VMM), Server Manager, and Storage Spaces.
2. Events are gathered by using public operating system event logging and tracing APIs.
3. You can configure the telemetry level by using an MDM policy, Group Policy, or registry settings.
4. The Connected User Experience and Telemetry component transmits telemetry data over HTTPS to Microsoft and uses certificate pinning.

Data transmission

All telemetry data is encrypted using SSL and uses certificate pinning during transfer from the device to Microsoft.

Endpoints

The Microsoft Data Management service routes data back to our protected cloud storage. Only Microsoft personnel with a valid business justification are permitted access.

The Connected User Experience and Telemetry component connects to the Microsoft Data Management service at v10.vortex-win.data.microsoft.com.

The Connected User Experience and Telemetry component also connects to settings-win.data.microsoft.com to download configuration information.

[Windows Error Reporting](https://watson.telemetry.microsoft.com) connects to watson.telemetry.microsoft.com.

[Online Crash Analysis](https://oca.telemetry.microsoft.com) connects to oca.telemetry.microsoft.com.

¹ About TraceLogging - [https://msdn.microsoft.com/en-us/library/dn904632\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/dn904632(v=vs.85).aspx)

Data use and access

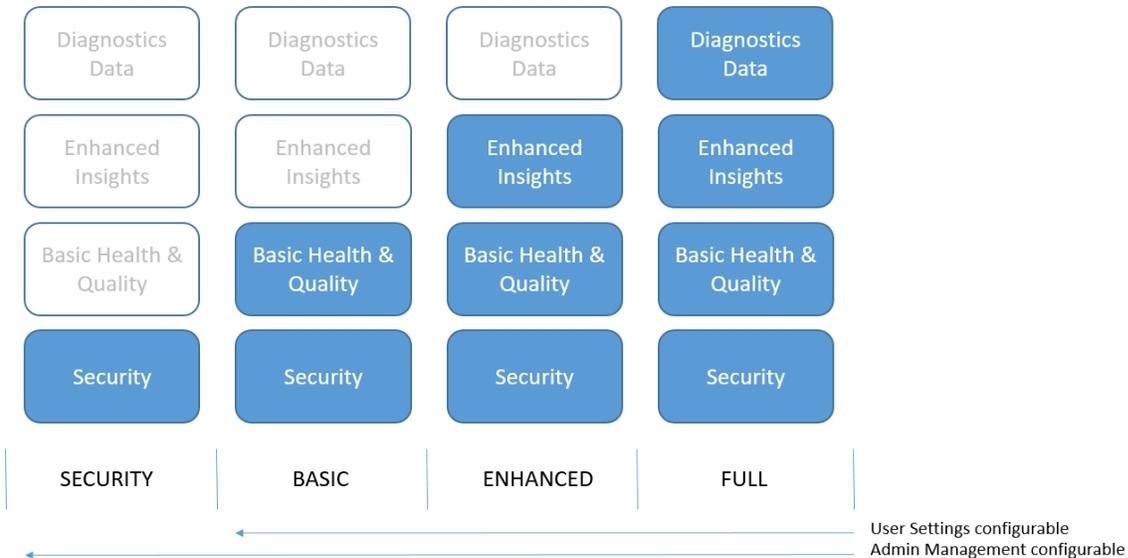
Data gathered from telemetry is used by Microsoft teams primarily to improve our customer experiences, and for security, health, quality, and performance analysis. The principle of least privileged guides access to telemetry data. Only Microsoft personnel with a valid business need are permitted access to the telemetry data. Microsoft does not share personal data of our customers with third parties, except at the customer's discretion or for the limited purposes described in the Privacy Statement². We do share business reports with OEMs and third party partners that include aggregated, anonymized telemetry information. Data sharing decisions are made by an internal team including privacy, legal, and data management.

Data retention

Microsoft believes in and practices information minimization. We strive to gather only the information that we need, and we store it for as long as it's needed to provide a service or for analysis. Much of the information about how the operating system and apps are functioning is deleted within 30 days. Other information, such as error reporting data, may be retained longer.

What data is gathered at different telemetry levels?

This section illustrates and explains the different telemetry levels in Windows 10 and Windows Server 2016. These levels are available on all editions of Windows Server 2016. The following figure shows a comparison of the telemetry levels:



The telemetry levels are cumulative and can be categorized into four levels:

² Windows Server prerelease: <http://windows.microsoft.com/en-us/windows/preview-privacy-statement>
System Center prerelease: <http://go.microsoft.com/fwlink/?LinkID=623851&clcid=0x409>

- **Security:** Information that's required to help keep the OS and System Center secure, including data about the Connected User Experience and Telemetry component settings, the Malicious Software Removal Tool (MSRT), and Windows Defender.
- **Basic:** Basic device information, including: quality-related data, app compatibility, app usage data, and data from the **Security** level.
- **Enhanced:** Additional insights, including: how the OS, System Center, and apps are used, how they perform, advanced reliability data, and data from both the **Basic** and **Security** levels.
- **Full:** All data necessary to identify and help to fix problems, plus data from the **Security**, **Basic**, and **Enhanced** levels.

Security level

The **Security** level gathers only the telemetry data that is required to keep Windows devices, Windows Server, and guests secure with the latest security updates. This level is available on all Windows Server 2016 editions and only on Windows 10 Enterprise, Windows 10 Education, Windows 10 Mobile Enterprise, and 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 System Center Configuration Manager functionality is not affected at this level, nor is telemetry data about Windows Server features or System Center gathered.

The data gathered at this level includes:

- **Connected User Experience and Telemetry component settings:** If data has been gathered and is queued to be sent, the Connected User Experience and Telemetry component downloads its settings file from Microsoft servers. 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 such as device information and IP address.
Note: You can turn off the MSRT³ 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.
- **Windows Defender/Endpoint Protection:** Windows Defender and System Center Endpoint Protection require 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.

³ About MSRT: <http://support.microsoft.com/en-us/kb/890830>

Microsoft recommends that Windows Update, Windows Defender, and MSRT remain enabled unless the enterprise uses alternative solutions such as WSUS, System Center 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 telemetry settings and no Internet connectivity, you should set the telemetry 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** telemetry level, and we avoid gathering any information that directly identifies a company or user, such as a name or email address. 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, which would cause 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 is critical for understanding the system and its configuration. This level includes the **Security** level information. This level helps to identify problems that can occur on a particular device hardware or software configuration. For example, it can help determine if crashes are more frequent on devices with a specific amount of memory or a particular network driver version. The Connected User Experience and Telemetry component does not gather telemetry data about System Center, but it can transmit telemetry for non-Windows apps if they have user consent.

The data gathered at this level includes:

- **Basic device information:** Helps provide an understanding about the types and configurations of native and virtualized Windows Server 2016 instances in the ecosystem, including:
 - Machine attributes, such as the OEM, model, and BIOS date
 - Networking attributes, such as the number and speed of network adapters
 - Processor and memory attributes, such as the number of cores, architecture, memory size, and firmware version
 - Virtualization attributes, such as Second Level Address Translation (SLAT) support and the guest operating system
 - OS attributes, such as the edition and virtualization state
 - Storage attributes, such as the number of drives, type, speed, and size
- **Connected User Experience and Telemetry component quality metrics:** Helps provide an understanding about how the Connected User Experience and Telemetry component is functioning, including percent 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. An example is the count of crashes in the operating system on a particular hardware configuration or with a specific driver version.

- **Compatibility data:** Helps provide an understanding about which apps are installed on a system and virtual machine, and identifies potential compatibility problems.
 - **General app data:** 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.
 - **App usage data:** Includes how an app is used, including how long an app is used for, when the app has focus, and when the app is started.
 - **System data:** Helps provide an understanding about whether a system meets the minimum requirements to upgrade to the next OS version. 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 external storage devices, that are connected to Windows systems and whether these devices will function after upgrading to a new version of the OS.
 - **Driver data:** Includes specific driver usage that is meant to help figure out whether apps and systems will function after upgrading to a new version of the OS. This data can help determine blocking issues and then help Microsoft and our partners apply fixes and improvements.

Enhanced level

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

This is the default level on all Windows Server 2016 and System Center 2016 editions. It is the minimum level that is required to quickly identify and address OS and System Center customer quality issues.

The data gathered at this level includes:

- **OS events:** Help to gain insights into different areas of the OS, including networking, Hyper-V, storage, file system, and other components.
- **OS app events:** Result from Microsoft applications and management tools that were installed with or on Windows Server (for example, Server Manager and System Center).
- **Some crash dump types.** All crash dump types, except for heap dumps and full dumps.

Full level

The **Full** level gathers data necessary to identify and help fix problems. This level also includes data from the **Security**, **Basic**, and **Enhanced** levels.

If systems experience 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. It is gathered from a small randomly selected set of systems that have both opted into the **Full** telemetry level and have exhibited the problem. Data sharing decisions are made by an internal team including privacy, legal, and data management.

How can enterprises manage telemetry collection?

We do not recommend that you turn off telemetry in your organization because valuable functionality may be impacted, but we recognize that in some scenarios this may be required. Use the steps in this section to turn off telemetry for Windows 10, Windows Server 2016, and System Center 2016.

Important: These telemetry levels only apply to Windows, Windows Server, System Center components, and apps that use the Connected User Experience and Telemetry component. Non-Windows components, such as Microsoft Office or other third-party apps, may communicate with their cloud services outside of these telemetry levels. You should work with your app vendors to understand their telemetry policy, and how you can opt in or opt out. For more information on how Microsoft Office uses telemetry, see [Overview of Office Telemetry](#)⁴.

Customers can turn off System Center telemetry collection. The default is on at the **Enhanced** level. The data gathered at this level represents what is collected by default when System Center telemetry is turned on. However, setting the operating system telemetry level to **Basic** turns off System Center telemetry, even if the System Center telemetry switch is turned on.

The lowest telemetry setting level that is supported on Windows Server 2016 through management policies is **Security**. The lowest telemetry setting that is supported through the Settings UI is **Basic**. The default telemetry level for all Windows Server 2016 editions is **Enhanced**.

Configure the operating system telemetry level

You can configure your OS telemetry settings using the management tools you are already using, such as Group Policy, MDM, or Windows Provisioning. You can also manually change your settings using Registry Editor. Setting your telemetry levels through a management policy overrides any device level settings.

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

Value	Level	Data gathered
0	Security	Security data only.
1	Basic	Security data, and Basic Health and Quality data.
2	Enhanced	Security data, Basic Health and Quality data, and Enhanced Insights.
3	Full	Security data, Basic Health and Quality data, Enhanced Insights and Advanced Reliability data, and Diagnostics data.

Table 1: Telemetry levels and data types

Use Group Policy to set the telemetry level

Use a Group Policy object to set your organization's telemetry level.

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

⁴ Overview of Office Telemetry: <https://technet.microsoft.com/library/jj863580.aspx>

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 telemetry level

Use the Policy Configuration Service Provider (CSP)⁵ to apply the `System/AllowTelemetry` MDM policy.

Use Registry Editor to set the telemetry level

Use Registry Editor to manually set the registry level on each device in your organization, or 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\Microsoft\Windows\CurrentVersion\Policies\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** and 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 or virtual machine (VM) in your organization.

Turn off telemetry collection in System Center 2016 for the enterprise

For System Center 2016 Technical Preview 4, IT administrators can reduce the flow of System Center telemetry to zero by following these steps:

- Turn off telemetry by going into the System Center UI Console settings workspace.
- For Service Management Automation and Service Provider Foundation instructions on how to turn off telemetry, see Microsoft Knowledge Base article# 3096505⁶.

Additional telemetry controls

In Windows Server 2016, there are additional telemetry controls to reduce the flow of Windows telemetry data:

- Change the default telemetry level from **Enhanced** to **Security**.
- Turn off Windows Update, or set the machines to be managed by an on premise update server such as WSUS⁷ or System Center Configuration Manager⁸.
- Turn off **Windows Defender Cloud based Protection** and **Automatic sample submission** in **Settings > Update & Security > Windows Defender**. If a third-party antimalware service is installed, Windows Defender (and its telemetry) should automatically shut off.

⁵ Configuration Service Provider: [https://msdn.microsoft.com/library/windows/hardware/dn904962\(v=vs.85\).aspx](https://msdn.microsoft.com/library/windows/hardware/dn904962(v=vs.85).aspx)

⁶ Microsoft KB: [3096505](https://support.microsoft.com/en-us/kb/3096505) How to disable telemetry for Service Management Automation and Service Provider Foundation (<https://support.microsoft.com/en-us/kb/3096505>)

⁷ About Windows Server Update Services (WSUS): <https://technet.microsoft.com/library/hh852345.aspx>

⁸ System Center Configuration Manager: <https://technet.microsoft.com/en-us/library/dn965439.aspx>

- Turn off the MSRT infection report as described in the Microsoft Knowledge Base article “Deployment of the Microsoft Windows Malicious Software Removal Tool in an enterprise environment.”⁹

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

Examples of how Microsoft uses the telemetry data

Drive higher apps and driver quality in the ecosystem

Telemetry plays an important role in helping us quickly identify and fix critical reliability and security issues in our customers' deployments and configurations. Insights into the telemetry data that we gather help us quickly identify crashes or hangs associated with a certain application or driver on a given configuration, like a particular storage type (for example, SCSI) or a memory size.

For System Center, job usages and statuses can also help us enhance the job workload and the communication between System Center and its managed products. Microsoft's ability to get this data from customers and drive improvements into the ecosystem helps raise the bar for the quality of System Center, Windows Server applications, Windows apps, and drivers. Real-time data about Windows Server and Windows installations reduces downtime and the cost associated with troubleshooting unreliable drivers or unstable applications

Reduce your total cost of ownership and downtime

Telemetry provides a view of which features and services customers use most. For example, the telemetry data provides us with a heat map of the most commonly deployed Windows Server roles, most used Windows features, and which ones are used the least. This helps us make informed decisions about where we should invest our engineering resources to build a leaner operating system.

For System Center, understanding the customer environment for management and monitoring will help drive the support compatibilities matrix, such as host and guest OS. This can help you use existing hardware to meet your business needs and reduce your total cost of ownership. It can also help to reduce the downtime that is associated with security updates.

Build features that address our customers' needs

Telemetry also helps Microsoft to better understand how customers deploy components, use features, and use services to achieve their business goals. Getting insights from that data helps us prioritize our engineering investments in areas that can directly impact our customers' experiences and workloads.

Some examples include customer usage of containers, storage, and networking configurations that are associated with Windows Server roles like Clustering and Web. Another example is to find out when CPU hyper-threading is turned off and what the resulting impact is. We use the insights to drive

⁹ Microsoft KB: [891716](http://support.microsoft.com/kb/891716) Deployment of the Microsoft Windows Malicious Software Removal Tool in an enterprise environment. (<http://support.microsoft.com/kb/891716/>)

improvements and intelligence into some of our management and monitoring solutions. This helps customers to diagnose quality issues and save money by making fewer support calls to Microsoft.