Deploy Office Telemetry Dashboard

In this article

View contributors to this article by accessing the link Below

https://docs.microsoft.com/en-us/DeployOffice/compat/deploy-telemetry-dashboard

Applies to: *Office 365 ProPlus, Office 2019, and Office 2016*

This article helps you deploy the five components of Office Telemetry Dashboard: the dashboard itself, the processor, the agent, the database, and a shared folder. Ensure that you review Plan a deployment of Office Telemetry Dashboard for topology, scalability, and hardware guidance before you deploy these components.

Important

- Office Telemetry Dashboard is an on-premises tool that collects inventory, usage, and health data about the Office documents and solutions, such as add-ins, used in your organization. The data is primarily designed to help your organization with application compatibility testing.
- Data collected for Office Telemetry Dashboard is stored in a SQL Server database controlled by your organization and the data collected is ***not*** sent to Microsoft. For more information, see Data collected by the agent for Office Telemetry Dashboard.
- Data collected for Office Telemetry Dashboard is different than Office diagnostic data, which can be sent to Microsoft. For more information about Office diagnostic data, see Overview of privacy controls for Office 365 ProPlus.
- Settings used to manage Office Telemetry Dashboard have no impact on Office diagnostic data and vice versa. For more information about managing Office diagnostic data, see Use policy settings to manage privacy controls for Office 365 ProPlus.

Office Telemetry Dashboard

Office Telemetry Dashboard is an Excel workbook that is configured to connect to a database. Office Telemetry Dashboard is installed together with Office 365 ProPlus, Office Professional

Plus 2019, Office Professional Plus 2016, and Office Standard 2016. To view Office Telemetry Dashboard, you must have Excel 2019 or Excel 2016 installed.

After Office is installed, you can start Office Telemetry Dashboard by using one of the procedures in the following table:

How to start Office Telemetry Dashboard

Table 1

Operating system	**How to start Office Telemetry Dashboard**
Windows 10, Windows Server 2008 R2, Windows Server 2008, or Windows 7 with Service Pack 1	From the **Start** menu, choose **All Programs**, then **Microsoft Office 2016 Tools**, then **Telemetry Dashboard for Office 2016**.
Windows 8.1 or Windows 8	On the **Start** screen, type **Telemetry Dashboard** and then choose it from the search results.
Windows Server 2012 R2 or Windows Server 2012	Swipe in from the right edge to show the charms and then choose **Search** to see all the apps that are installed on the computer. Next, choose **Telemetry Dashboard for Office 2016**.

For Office 365 ProPlus and Office 2019, look for **Telemetry Dashboard for Office** under **Microsoft Office Tools**.

SQL Server

SQL Server must be deployed before you can configure Office Telemetry Dashboard. You don't have to have an existing database, but you do have to install or have access to one of these versions of SQL Server:

- SQL Server 2016 or SQL Server 2016 Express
- SQL Server 2014 or SQL Server 2014 Express
- SQL Server 2012 or SQL Server 2012 Express
- SQL Server 2008 R2 or SQL Server 2008 R2 Express Edition
- SQL Server 2008 or SQL Server 2008 Express Edition
- SQL Server 2005 or SQL Server 2005 Express Edition

The **Getting started** worksheet in Office Telemetry Dashboard provides a link to download SQL Server 2014 Express. If you don't have SQL Server already installed, follow the steps in To download and install SQL Server 2014 Express. Be sure to review the following guidelines before you install SQL Server 2014 Express.

- Ensure that the computer meets the hardware and software requirements for SQL Server 2014. This is especially important if you are planning an all-in-one configuration for testing because SQL Server has additional requirements, such as installing Windows service packs that aren't required for Office Telemetry Dashboard. These requirements are described in Hardware and Software Requirements for Installing SQL Server 2014.

- For local installations, you must run Setup as an administrator. If you install SQL Server from a remote shared folder, you must use a domain account that has read and execute permissions on the remote shared folder. For more information, see Install SQL Server 2014 from the Installation Wizard (Setup).

To download and install SQL Server 2014 Express

1. In Office Telemetry Dashboard, on the **Getting started** worksheet, under **1. Set up prerequisites**, choose the link to download and install SQL Server 2014 Express with Tools. Choose the 32-bit or 64-bit edition, as appropriate. Or use this link: Microsoft SQL Server 2014 Express.
2. The setup process for SQL Server 2014 Express takes a while to download and extract files. Accept the various prompts and wait for the first page of SQL Server 2014 Express, which is named the **SQL Server Installation Center**, to appear after extraction is completed. Then, follow these steps:
    1. In the SQL Server Installation Center, choose **New SQL Server stand-alone installation or add features to an existing installation**.
    2. In the SQL Server 2014 setup wizard, read the license terms, accept them, and then choose **Next**.
    3. On the **Feature Selection** page, accept the default settings. Choose **Next**.
    4. On the **Instance Configuration** page, create a named instance (for example, use the name "teledash"). Choose **Next**.
    5. On the **Server Configuration** page, accept default service accounts. Choose **Next**.
    6. On the **Database Engine Configuration** page, accept the default authentication mode (Windows authentication mode). Your user account is displayed as a SQL Server administrator. (Warning: Don't use Mixed Mode because Office Telemetry Dashboard doesn't support SQL Server authentication.) Choose **Next**.
    7. On the **Error Reporting** page, select the check box if you want to send error reports to Microsoft. Otherwise, just choose **Next**.
    8. Wait for the installation process to finish, and then exit the wizard and the SQL Server Installation Center.

Office Telemetry Processor

Office Telemetry Processor runs on one or more computers and collects inventory, usage, and health data from the shared folder and imports the data to the database. The processor is installed as a Windows service named "Office Telemetry Processor" and the processor supports Transport Layer Security (TLS) 1.2.

Important

If the computers that run the processor and the shared folder pair, and the SQL database aren't joined to a domain, you must install these components by using the script that is described in Quickly set up Office Telemetry Dashboard on a workgroup or domain-joined computer.

The processor generates error logs in a file that is named dperrorlog.txt. It is located in a hidden folder at %systemroot%\ServiceProfiles\NetworkService\AppData\Local\Temp.

Each computer on which you install the processors and database must also run the latest version of the Universal C Runtime (CRT) for the version of Windows running on the computer. For information, see Update for Universal C Runtime in Windows.

We recommend the following operating systems for computers that run the processor:

For production environments: For best performance, we recommend these operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

For test or small production environments: You can use computers that run Windows 10, Windows 8.1, Windows 8, and Windows 7 with Service Pack 1 in test environments and in small production environments. There is a limit of 20 concurrent connections for client operating systems, but in small environments, the agent randomization setting should minimize any chance of more than 20 agents connecting at one time.

Ensure that you have the following available before you run the wizard to set up the processor.

- **SQL Server instance name.** The example used earlier is "teledash."
- **SQL database.** A new database will be created if you don't specify an existing database.
- **Permissions to create a shared folder, or the UNC path of an existing shared folder.** The wizard that sets up the processor can create a shared folder if it has permissions to do so. If you specify an existing shared folder, any existing NTFS and shared folder permissions are overwritten with permissions set by the wizard.
- **Permissions to create a database (sysadmin role in SQL Server).** To create and configure a new database, the account that runs the wizard to set up the processor must be a domain account that is a member of the sysadmin server-level role on the SQL Server. For ongoing use of Office Telemetry Dashboard, membership in the sysadmin role isn't required and can be removed after the database is created. You can also use an existing database.
- **At least 11 GB of hard disk space.** This disk space is needed to temporarily store data that is collected from users.

To install the Office Telemetry Processor

1. On the computer where you want to install the processor, install the latest version of the CRT. For more information, see Update for Universal C Runtime in Windows.
2. In Office Telemetry Dashboard, on the **Getting started** worksheet, choose the installation link under **2. Install Telemetry Processor**. Select the x86 or x64 version that's the same as the Windows operating system architecture where the processor will run.
3. Optionally, you can use the links in Office Telemetry Dashboard to save the .msi file to another computer and run the Setup program there. This step is required if you are installing processors on separate computers.
4. Choose **Next** and then choose **Yes** to accept the User Account Control prompt to install the processor. Choose **Finish**, which starts the **Office Telemetry Processor settings** wizard.
5. Choose **Yes** to accept the prompt, and then choose **Next**.
6. Type the name of the SQL Server instance, and then choose **Connect**.
7. Type the name of a new database, choose **Create**, and then choose **Next**.
8. Choose **Yes** to create database permissions and the database role.
9. Do one of the following on the **Shared Folder** page:
   - Specify the UNC path of an existing shared folder, and then choose **Next**. Choose **Yes** to allow the wizard to set the appropriate permissions.
   - To create a new shared folder on the local computer, choose **Browse**. Navigate to the location where you want to create the shared folder. Open the shortcut menu for the parent folder (right-click it), point to **New**, and then choose **Folder**. Type the name of the new folder, ensure that you choose the folder again to select it, and then choose **Select Folder**. Choose **Next**, and then choose **Yes** to allow the wizard to share the folder and set the appropriate permissions.
10. Accept the default option to sign up for the Customer Experience Improvement Program, or choose the option not to sign up for the program at this point, and then choose **Next**.
11. Choose **Finish** to exit the wizard.

Database used by Office Telemetry Dashboard

The database, which was created by the **Office Telemetry Processor settings** wizard, is ready to be configured and connected to Office Telemetry Dashboard.

To connect to the database

1. In Office Telemetry Dashboard, on the **Getting started** worksheet, under **5. Connect to the database to view telemetry data**, choose **Connect to Database**.
2. Specify the name of the SQL Server and SQL database that you specified during the installation of the processor.

When the connection is established, many new worksheets are added to the workbook. They won't contain data until you deploy and enable the agents.

To grant other administrators permission to access the database

- You can use the Telemetry Dashboard Administration Tool (Tdadm) on the computer that is running SQL Server to allow other administrators to view data in Office Telemetry Dashboard. You don't have to run this for your own account if you created a database when you installed the processor. Update the values for dbserver, dbname, and domain\user as needed.

- `tdadm.exe -o permission -databaseserver dbserver -databasename dbname -add domain\user`
-

For more information about Tdadm, see the Tdadm wiki.

For more information about how to configure the reporting threshold in the database to help protect user privacy, see Manage the privacy of data monitored by Office Telemetry Dashboard. If you have problems connecting to the database, see Troubleshooting Office Telemetry Dashboard deployments.

If your data (for example, file names, solution names, user names, computer names, or tag values) includes supplementary characters (surrogate pairs), use the following SC collations that are available in SQL Server to support better handling of the characters.

- Version 90 Windows collations, such as Chinese_PRC_Stroke_90
- Version 100 Windows collations, such as Latin1_General_100_CI_AS_SC

For more details about collation settings, see the documentation for the version of SQL Server that you are using.

Office Telemetry Agent

The following information and instructions will help you learn more about how to deploy and enable the Office Telemetry Agent.

Deploying the agent

The agent is built into Office 365 ProPlus, Office 2019, Office 2016, and Office 2013 and doesn't have to be deployed separately. If your organization has any of the following versions of Office, you must deploy the Office 2019 or Office 2016 agent to these clients.

- Office 2003
- Office 2007
- Office 2010

For computers that are running Office 2013 and you have the Office 2013 agent installed on the computer, there are several additional considerations:

- You can monitor computers running Office 2013 from the Office 2019 or Office 2016 Office Telemetry Dashboard. In order for this to work, the computer must also be running the Office 2013 agent. The agent must be configured to point to the Office 2019 or Office 2016 Office Telemetry Dashboard.
- You cannot use an Office 2019 or Office 2016 agent with Office 2013. The Office 2019 or Office 2016 agent will not be able to read events from an Office 2013 installation.
- Once you have upgraded a computer to Office 2019 or Office 2016, you can continue to run the old Office 2013 agent. The agent will continue to report data to the Office 2013 Office Telemetry Dashboard. At the same time, the new Office 2019 or Office 2016 agent that was installed when you upgraded to Office 2019 or Office 2016 will provide the same data to the Office 2019 or Office 2016 Office Telemetry Dashboard. This may use up valuable computer and network bandwidth resources. We recommend you disable the Office 2013 agent once you are ready to move to Office 2019 or Office 2016 Office Telemetry Dashboard.
- When you install the Office 2019 or Office 2016 agent, it does not overwrite the Office 2013 agent. Instead, you need to disable the Office 2013 agent. You disable the agent by using Group Policy. For more information on the Group Policy settings you use to disable the agent, see Enabling and configuring the agent.
- We recommend that you do not deploy the Office 2019 or Office 2016 agent on computers that are only running Office 2013.

In order to run the agent, client computers must run one of the following versions of Windows (either 32-bit or 64-bit):

- Window 10
- Windows 8.1
- Windows 8
- Windows 7 with Service Pack 1
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

The agent might not work correctly on Windows service packs that are no longer supported by Microsoft. We recommend that you verify that your service pack is supported on the Microsoft Product Lifecycle Search website before you install the agent.

The computer running the agent must also run the latest version of the Universal C Runtime (CRT) for the version of Windows. For information, see Update for Universal C Runtime in Windows.

To deploy the Office 2019 or Office 2016 agent to Office 2010, Office 2007, and Office 2003 clients

1. In Office Telemetry Dashboard, on the **Getting started** worksheet, under **3. Deploy Telemetry Agent**, choose the appropriate link (x86 or x64) to save the agent .msi file to a specified location.
2. Using your preferred method, deploy the .msi file to client computers that you want to monitor. Be sure to match the x86 or x64 version of the agent to the architecture of the Windows operating system that is running on the client, not the Office client architecture.

   For client local installations, you must run the .msi file as an administrator. You can deploy the MSI package silently by using the /quiet parameter with the MSI. Refer to the MSI help for the full set of available parameters.

   For large-scale deployments, you can deploy Telemetry Agent by using Microsoft Endpoint Configuration Manager.

Enabling and configuring the agent

To enable and configure the agent, you can edit the registry on each monitored client computer in small or test environments. For production environments that contain hundreds or thousands of client computers, you can use Group Policy administrative templates. Two settings, AgentInitWait and AgentRandomDelay, are configurable only in the registry.

- Use the registry to enable and configure the agent
- Use Group Policy to enable and configure the agent

Use the registry to enable and configure the agent

The easiest way to update the registry on a single client is to run a .reg file that sets the registry values that enable the agent to collect and upload data. You can create this .reg file by copying one of the following examples to a text file, updating the required fields, saving the file as agent.reg and then running it from an elevated command prompt. In the .reg file, ensure that you specify the UNC path of the shared folder to which the agent uploads the data. Optionally, you can update the <TAG> fields so you can easily identify the collected data in your organization, such as by department, location, or deployment group.

The following example sets the default settings that are needed to enable the agent. AgentInitWait and AgentRandomDelay are set to their default values, which are appropriate for production deployments.

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\osm]
"CommonFileShare"="\\\\<SERVERNAME>\\<SHARENAME>"
"Tag1"="<TAG1>"
"Tag2"="<TAG2>"
"Tag3"="<TAG3>"
"Tag4"="<TAG4>"
"AgentInitWait"=dword:00000258
"Enablelogging"=dword:00000001
"EnableUpload"=dword:00000001
```

```
"EnableFileObfuscation"=dword:00000000
"AgentRandomDelay"=dword:000000F0
```

The code in the following example enables Office Telemetry Dashboard to begin uploading data immediately by setting AgentInitWait and AgentRandomDelay to their smallest values. Use this example only in test deployments.

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\osm]
"CommonFileShare"="\\\\<SERVERNAME>\\<SHARENAME>"
"Tag1"="<TAG1>"
"Tag2"="<TAG2>"
"Tag3"="<TAG3>"
"Tag4"="<TAG4>"
"AgentInitWait"=dword:00000001
"Enablelogging"=dword:00000001
"EnableUpload"=dword:00000001
"EnableFileObfuscation"=dword:00000000
"AgentRandomDelay"=dword:00000000
```

You can distribute registry updates to multiple client computers by putting a .reg file in a shared folder and instructing users to run the file, or you can add a command to the users' logon script to automatically import the .reg file when users log on. Use the syntax in the following example to start the .reg file from a logon script:

```
%windir%\regedit.exe /s <PATH>\<NAME>.reg
```

For more information about how to use .reg files, see How to add, modify, or delete registry subkeys and values by using a registration entries (.reg) file.

The following tables describe each registry value.

Note

If you're not an administrator, you'll have to edit the registry under HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\OSM. These changes can be overwritten by policy settings that are located in HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\OSM.

Agent registry settings under HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\OSM

Table 2

Value name	Type	Value description and data	Required or optional
enablelogging	REG_DWORD	Enables runtime logging and static scanning. This allows the agent to collect data.	Required

Table 2

Value name	**Type**	**Value description and data**	**Required or optional**
		Value: 1 = Enable logging and agent 0 = Disable logging and agent Default = 0 (Disable logging & agent)	
enableupload	REG_DWORD	Turns on the data uploading feature in the agent so that the agent can periodically upload data to the shared folder that is specified in CommonFileShare. **Value:** 0 = Do not upload 1 = Upload Default = 0 (Do not upload)	Required
commonfileshare	REG_SZ	Specifies the UNC path of the shared folder for storing data. **Value:** \\server\share	Required
tag1 tag2 tag3 tag4	REG_SZ	Adds custom tags to the data that is sent by the agent. If you enable this policy setting, the specified custom tags are shown in Office Telemetry Dashboard, where you can filter the collected data by the tag name. You can replace **tag1**, **tag2**, **tag3**, and **tag4** with custom strings to categorize and filter the collected data (for example, replace **tag1** with a department name, replace **tag2** with the location of the users, and so on). **Value:** *tag1* *tag2* *tag3* *tag4*	Optional
enablefileobfuscation	REG_DWORD	Configures the agent to disguise, or obfuscate, certain file properties that are reported in data.	Optional

Table 2

Value name	**Type**	**Value description and data**	**Required or optional**
		If you enable this policy setting, the agent obfuscates the file name, file path, and title of Office documents before uploading data to the shared folder. You can learn more about file obfuscation and other privacy settings for Office Telemetry Dashboard in Manage the privacy of data monitored by Office Telemetry Dashboard. **Value:** 0 = Do not obfuscate 1 = Obfuscate Default = 0 (No obfuscation)	
AgentInitWait	REG_DWORD	**IMPORTANT:** To avoid affecting network or client performance, decrease this value in test environments only. Adjusts the time that the agent waits before it scans a client and uploads data to the shared folder. If this value doesn't exist, the default wait time is 10 minutes (600 seconds). In test environments, you can specify 1 second to remove the delay for testing Windows 7 with Service Pack 1 and earlier clients. We recommend that you set this to at least 60 seconds for computers that run Windows "8." **Value:** *x* = Wait time in seconds	Optional
AgentRandomDelay	REG_DWORD	**IMPORTANT:** To avoid affecting network or client performance, decrease this value in test environments only. Adjusts the maximum random delay, in minutes. The agent randomly waits between 0 and **AgentRandomDelay** minutes, in addition to the **AgentInitWait** value, before it starts to scan or upload data. If this value doesn't exist, the agent waits between 0 minutes to 240	Optional

Table 2

Value name	**Type**	**Value description and data**	**Required or optional**
		minutes. In test environments, you can specify 0 to remove the random delay for testing. **Value:** *x* = Random delay in minutes	

Agent registry settings under HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\OSM\preventedapplications

Table 3

Value name	**Value type**	**Value description and data**	**Required or optional**
accesssolution olksolution onenotesolution pptsolution projectsolution publishersolution visiosolution wdsolution xlsolution	REG_DWORD	Prevents data for specific Office applications from being reported to Office Telemetry Dashboard. You can learn more about this registry setting in [Manage the privacy of data monitored by Office Telemetry Dashboard](). **Value:** 1 = Prevent reporting 0 = Allow reporting Default = 0 (Allow reporting)	Optional

Agent registry settings under HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\OSM\preventedsolutiontypes

Table 4

Value name	**Value type**	**Value description and data**	**Required or optional**
agave appaddins comaddins documentfiles templatefiles	REG_DWORD	Prevents data for specific solutions from being reported to Office Telemetry Dashboard. However, the solution type is still reported. You can learn more about this registry setting in [Manage the privacy of data monitored by Office Telemetry Dashboard](). **Value:**	Optional

Table 4

Value name	Value type	Value description and data	Required or optional
		1 = Prevent reporting 0 = Allow reporting Default = 0 (Allow reporting)	

Use Group Policy to enable and configure the agent

You can also use Group Policy to enable and configure agents. Download the Administrative Template files (ADMX/ADML) for Office from the Microsoft Download Center. The policy settings that are listed in the following table are available in the path **User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Telemetry Dashboard**.

Agent policy settings

Table 5

Setting name	Description	Required or optional
Turn on telemetry data collection	Turns on the data collection features in Office that are used by Office Telemetry Dashboard and Office Telemetry Log. By default, data collection is disabled in Office.	Required
Turn on data uploading for Office Telemetry Agent	Turns on the data uploading feature in the agent so that the agent can periodically upload data to a shared folder. By default, data uploading is disabled.	Required
Specify the UNC path to store Office telemetry data	Specifies the Uniform Naming Convention (UNC) path of a shared folder to which the agent sends data.	Required
Specify custom tags for Office telemetry data	Adds custom tags to the data that is sent by the agent. If you enable this policy setting, the specified custom tags are shown in Office Telemetry Dashboard, where you can filter the collected data by the tag name. You can specify any string that you want to categorize and filter the collected data (for example, department name, title of user, and so on).	Optional
Turn on privacy settings in Office Telemetry Agent	Configures the agent to disguise, or obfuscate, certain file properties that are reported in data. If you enable this policy setting, the agent obfuscates the file name, file path, and title of Office documents before uploading data to the shared folder. You can learn more about file obfuscation and other privacy settings for Office Telemetry Dashboard in Manage the	Optional

Table 5

Setting name	Description	Required or optional
	privacy of data monitored by Office Telemetry Dashboard.	
Office applications to exclude from Office Telemetry Agent reporting	Prevents data for specific Office applications from being reported to Office Telemetry Dashboard.	Optional
Office solutions to exclude from Office Telemetry Agent reporting	Prevents data for specific Office solutions from being reported to Office Telemetry Dashboard.	Optional

Triggering data collection manually

When a user logs in to an Office client, the agent waits 10 minutes to allow other logon processes to be completed, and then waits a randomized number of minutes up to 4 hours (or the max delay that is set for the AgentRandomDelay registry value) to avoid client computers sending data to network at the same time. After this initial scan, the agent scans and collects data every 8 hours.

If you want to trigger the data collection manually and see data uploaded immediately to Office Telemetry Dashboard, set the following registry values as described in the earlier table:

For computers that run Windows 7 with Service Pack 1 and earlier

- AgentInitWait: 1
- AgentRandomRelay: 0

For computers that run Windows 8 and later

Because user logon is faster in Windows 8 and later versions of Microsoft Windows, we recommend setting AgentInitWait to at least 60 seconds to ensure that the network connection is ready after the user logs on.

- AgentInitWait: 60
- AgentRandomRelay: 0

To trigger a scan manually, use one of the following procedures.

To trigger scanning and data collection on Windows clients

1. Ensure that the computer is connected to an AC power supply.
2. In Task Scheduler on the client computer, expand **Task Scheduler Library**, expand **Microsoft**, and then choose **Office**.

3. Right-click **OfficeTelemetryAgentLogOn**, and then choose **Run**.

Frequently asked questions about Office Telemetry Dashboard

Q: What happens if a client computer is disconnected for some time?

A: If a monitored client is disconnected, or if the shared folder is temporarily unavailable, data is still collected locally on the client. When the connection is restored, the backlog of information is delivered to the shared folder.

Q: How much data is transferred during each transfer?

A: The amount varies according to the number of files that are used and solutions installed. Here are estimates for how much data the agent sends for different versions of Office:

- Earlier versions of Office send approximately 50 KB for every upload.
- Office 2013 and later send approximately 64 KB of data for every upload.

The amount transferred can be larger when the interval is set to longer than the default or when the data sits idle on the local computer for long periods of time. Note that actual file content isn't transferred; only metadata about the files is transferred.

Q: What is the performance impact of installing and running the agent?

A: The agent is transparent to the user and performs low-impact tasks, such as inspecting content from MRU and specific local registry settings. The agent doesn't actively scan files. The agent does account for monitor power state and network status to avoid affecting client performance.

Q: How can I re-initialize an agent?

A: The agent is stored locally on the client computer at %localappdata%\Microsoft\Office\16.0\Telemetry. You can delete the contents of this folder to reinitialize the computer and start a fresh discovery. Note that this is a per-user data location.

Q: How frequently is data sent to the shared folder?

A: Data is transferred from the client to the shared folder when users log on and every 8 hours while the user is logged in. You can adjust this interval in Task Scheduler.

Q: What is the format of the collected data?

A: Collected data is stored and transferred in binary format to optimize the storage and data transfer requirements.

Q: If I change the custom labels after I deploy the agents, when will the new labels be updated in the database?

A: Only files that are in the Most Recently Used list will have their labels updated in the database. This will occur the next time the agent sends usage data. For files that are not in the Most Recently Used list, they will continue to show the old labels in the database until the user opens the file and the agent uploads usage data.

Troubleshooting Office Telemetry Dashboard deployments

The following table describes some symptoms that you might encounter after you deploy Office Telemetry Dashboard and its components.

Troubleshooting Office Telemetry Dashboard deployments

Table 6

Issue	Description	Resolution
Office Telemetry Processor settings wizard fails	The wizard fails with the message "The Telemetry Processor settings wizard can only run on computers that are joined to a domain. Join the computer to a domain and run the wizard again."	The computers that run the processor, shared folder, and SQL database must be joined to a domain so that the appropriate security settings can be configured. Ensure the computer or computers are in trusted domains. You can install these components on a single workgroup computer or domain-joined computer by using the script that is described in the blog post [Quickly set up Office Telemetry Dashboard on a workgroup or domain-joined computer]().
Office Telemetry Processor settings wizard fails	The processor is using the wrong SQL Server instance.	If there are two or more instances of SQL Server, ensure that you point to the correct SQL Server instance by using the format *Servername\SQLServerinstance* during the processor setup.
Office	The agent	Check the registry path and value for the CommonFileShare,

Table 6

Issue	Description	Resolution
Telemetry Dashboard shows no data	isn't uploading data and the Msoia.exe process isn't running in Task Manager.	EnableLogging, and EnableUpload registry values. These are described in Enabling and configuring the agent, earlier in this article.
Office Telemetry Dashboard shows no data	The agent isn't scanning or uploading data. The Msoia.exe process runs in Task Manager for a long time.	By default, the agent has an initial wait timer and randomization feature to avoid uploading large amounts of data at the same time as other agents and affecting network bandwidth. Update the AgentInitWait and AgentRandomDelay registry values to remove this delay in test environments. Otherwise the upload process can be delayed for up to 4 hours and 10 minutes. These registry values are described in Enabling and configuring the agent, earlier in this article. You can learn how to trigger scanning and uploading in Triggering data collection manually.
Office Telemetry Dashboard shows no data	The agent doesn't upload data. The Msoia.exe process runs in Task Manager for a long time.	Verify the network connection between the agent and the shared folder. Verify that the computer is joined to a domain. The shared folder is configured to allow access only to users who are authenticated within the domain. The agent continues to try to upload data after the upload has failed. When using the default registry values, the agent continues to run as a process in Task Manager for up to 4 hours and 10 minutes (max). To adjust registry values, see Enabling and configuring the agent, earlier in this article. You can learn how to trigger scanning and uploading in Triggering data collection manually.
Office Telemetry Dashboard shows no data	The agent task doesn't seem to be working.	Check the information in the **Last Run Result** column in Task Scheduler. If the operation succeeds, it shows return code 0. If the agent cannot upload data to the shared folder, the message "The network name cannot be found" appears in the **Last Run Result** column. This is the only error that the agent logs in the **Last Run Result** column. If other errors are listed, they were caused by other reasons or the scheduled task didn't run.
Office Telemetry Dashboard shows no data	The processor isn't working. There are many	Verify the network connection between the processor and the shared folder. Was the processor configured by the **Office Telemetry Processor settings** wizard? The permissions on the shared folder can vary, depending on the processor location and the database. Run the **Office Telemetry Processor settings** wizard again from the shortcut on the desktop.

Table 6

Issue	**Description**	**Resolution**
	folders and files in the shared folder.	
Office Telemetry Dashboard shows no data	The processor is working but there are many folders and files under in the Failed folder under the shared folder.	The processor processes the files in the shared folder to the database one time per minute. If the processor fails to process the files three times, it will move the failed files to the Failed folder. See the processor log (%windows%\ServiceProfiles\NetworkService\AppData\Local\Temp\dperrorlog.txt) for more information.
Office Telemetry Dashboard shows no data	The processor isn't working because of SQL Server authentication settings.	Check the authentication type for SQL Server. Office Telemetry Dashboard doesn't support SQL authentication. You must use Windows authentication.
Office Telemetry Dashboard shows no data	The processor isn't working because of firewall issues between the processor and the database.	If there is a firewall between Office Telemetry Dashboard and the database, check whether the SQL port is enabled in the firewall configuration. The default port for SQL Server is 1433. See Configure a Windows Firewall for Database Engine Access for more information.
Office Telemetry Dashboard shows no data	The processor isn't working because of firewall issues between the	If there is a firewall between Office Telemetry Dashboard and the database, check whether the SQL port is enabled in the firewall configuration. The default port for SQL Express isn't a fixed value. Check the port number in the SQL Configuration Manager and add the port to the firewall configuration. See Configure a Windows Firewall for Database Engine Access for more information.

Table 6

Issue	Description	Resolution
	processor, the database, and SQL Express.	
Office Telemetry Dashboard shows no data	The processor isn't working.	See the processor log (%windows%\ServiceProfiles\NetworkService\AppData\Local\Temp\dperrorlog.txt) for more information.
Office Telemetry Dashboard can't connect to the database	Office Telemetry Dashboard shows an error message that states it can't connect to the database because of SQL Server permissions.	Check the permission role for Office Telemetry Dashboard. Add the user to the td_readonly role by using OSQL, SQLCMD, Enterprise Manager, or the Telemetry Dashboard Administration Tool (Tdadm). See Database used by Office Telemetry Dashboard earlier in this article for more information.
Office Telemetry Dashboard can't connect to the database	Office Telemetry Dashboard shows an error message that states it can't connect to the database.	If there are two or more instances of SQL Server, ensure that the **Data connection settings** dialog box in Office Telemetry Dashboard uses the correct SQL Server instance in the format *Servername\SQLServerinstance*.
Office Telemetry Dashboard can't connect to the	Office Telemetry Dashboard shows an error message that states it	If the SQL Server is SQL Express, ensure that the SQL Server instance name is correct. The default instance name for SQL Express differs from SQL Server, for example: *Servername\SQLExpress*.

Table 6

Issue	Description	Resolution
database	can't connect to the database.	
Office Telemetry Dashboard can't connect to the database	Office Telemetry Dashboard shows an error message that states it can't connect to the database.	If the SQL Server default collation is case-sensitive (for example, the Japanese version of SQL Server is case-sensitive by default), ensure that you entered a case-sensitive database name in the **Data connection settings** dialog box in Office Telemetry Dashboard.