

- 1.3.5. Troubleshooting -

As they say, stuff happens.

Although Microsoft Windows generally has become more stable and reliable over time, it will never be perfect.

Apps hang (stop responding) or crash (shut down unexpectedly).

Once in a while, a feature of Windows walks off the set without warning.

And on rare occasions, the grim BSOD ("Blue Screen of Death," more formally known as a Stop error or bugcheck) arrives, bringing your whole system to a halt.

In a fully debugged, perfect world, such occurrences would never darken your computer screen.

But you don't live there, and neither do we.

So the prudent course is to prepare for the unexpected.

That starts with enabling File History so that your documents are backed up at regular intervals and, if possible, creating periodic image backups.

But it also entails learning to use the many tools Windows provides for diagnosing errors and recovering from problems.

Getting to know your troubleshooting toolkit

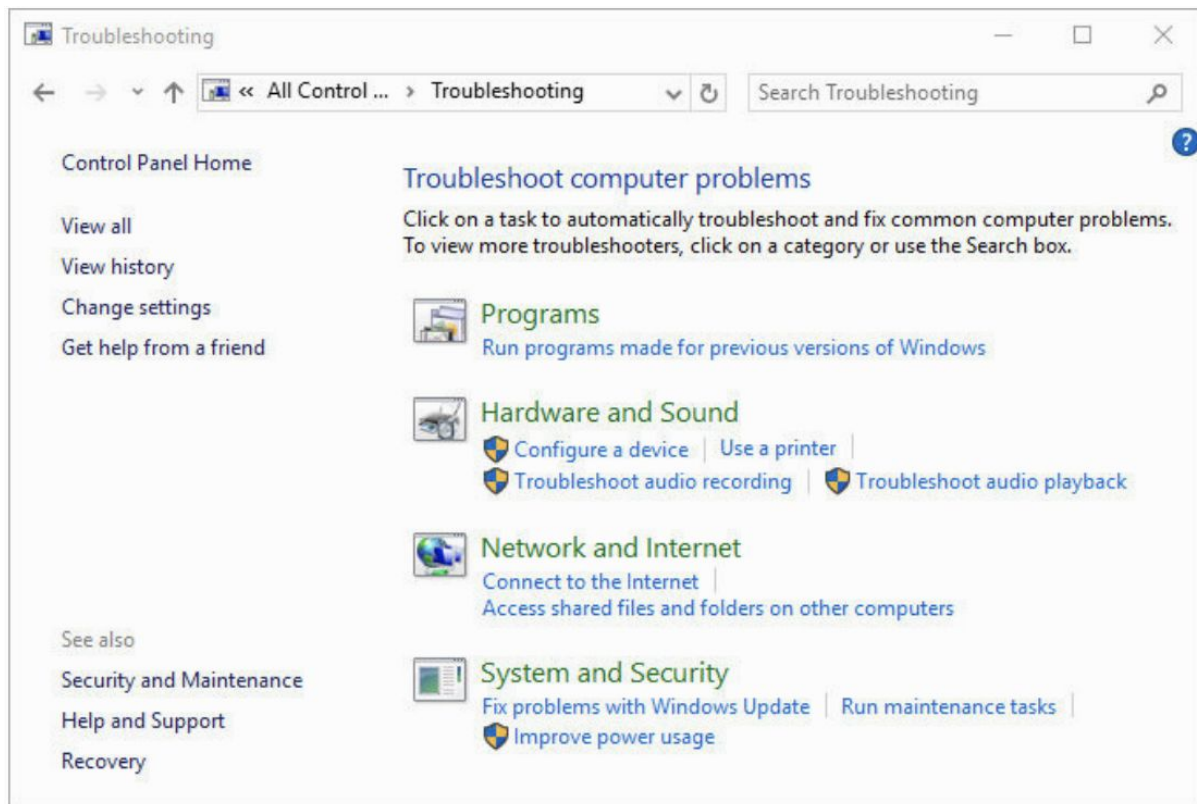
As any detective will tell you, solving a mystery requires evidence.

If your mystery involves inexplicably slow performance or crashes, you have several places to look for clues.

Built-in troubleshooters

The most obvious first step on the road to resolving performance issues is the aptly named Troubleshooting section in the classic Control Panel.

By default, it displays a list of the most commonly used troubleshooters included with Windows 10, as shown in the next picture:



Click the View All link on the left side of the Troubleshooting page to see an expanded list that includes modules for fixing more esoteric problems, such as issues with search and indexing or with the Background Intelligent Transfer Service.

There's nothing magical about any of these troubleshooters.

Their purpose is to ensure that you check the most common causes of problems, including some that might seem obvious.

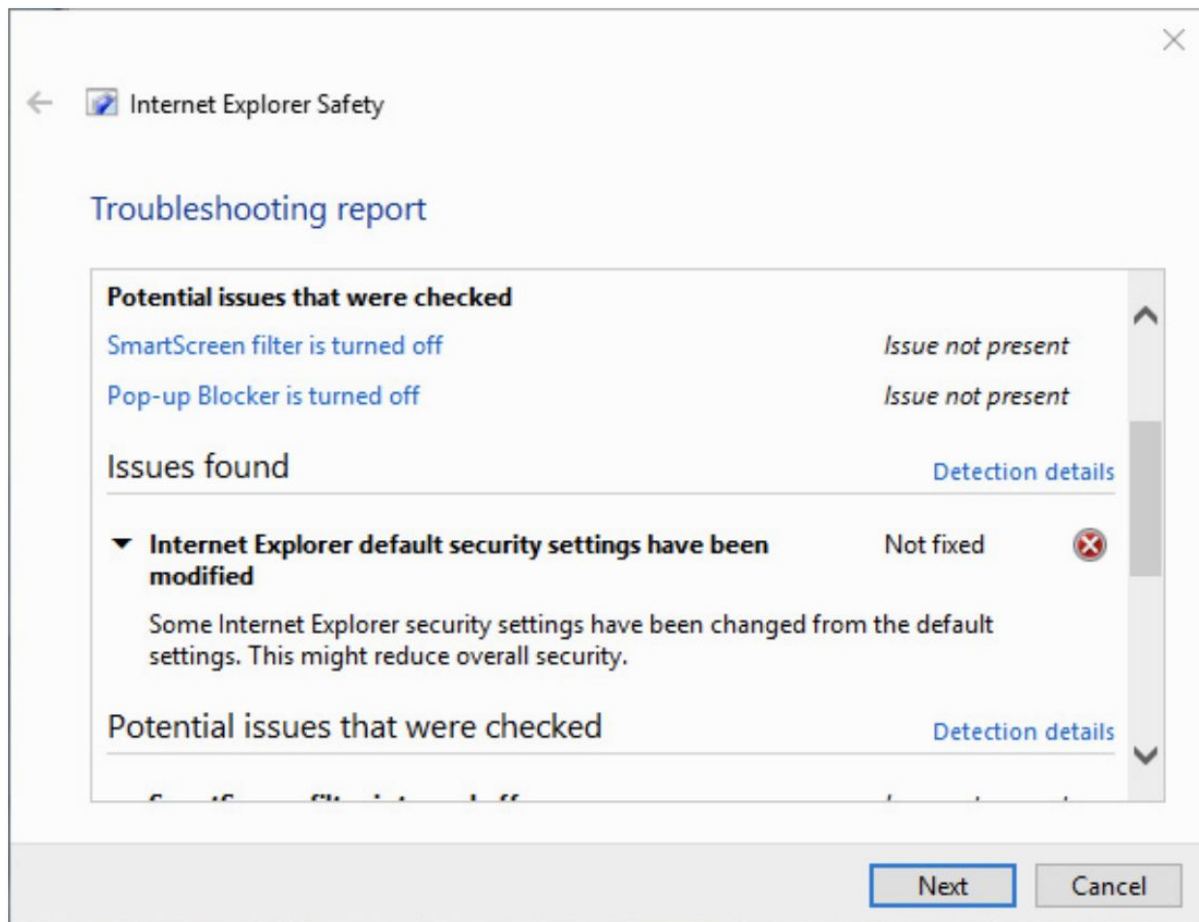
Is the network cable plugged in?

Is the printer turned on?

Running a troubleshooter can result in easy fixes for some issues; more importantly, it establishes a baseline for further troubleshooting.

A troubleshooter might lead you through several steps and ask you to check settings or connections.

At the end, it displays its results, which include a View Detailed Information link that leads to troubleshooting report similar to the one shown in the following picture:



Windows Error Reporting

Often an early indication that something is amiss is an error message informing you that an application is “not responding”—as if you hadn’t figured that out already.

If the application doesn’t come back to life, you kill the process with Task Manager and move on—ideally, without losing any data.

While all that’s happening, the Windows Error Reporting (WER) service runs continuously in the background, keeping track of software and driver installations (successful and otherwise) as well as crashes, hangs, and other system events that indicate a possible problem with Windows.

In fact, although the service and programs that enable the feature are called Windows Error Reporting, the term you’re more likely to see in Windows is problem reporting.

Microsoft provides this diagnostic information to the developers of the program that caused the error (including Microsoft developers when the issue occurs with a feature in Windows, Office, or another Microsoft program).

The goal, of course, is to improve quality by identifying problems and delivering fixes through Windows Update.

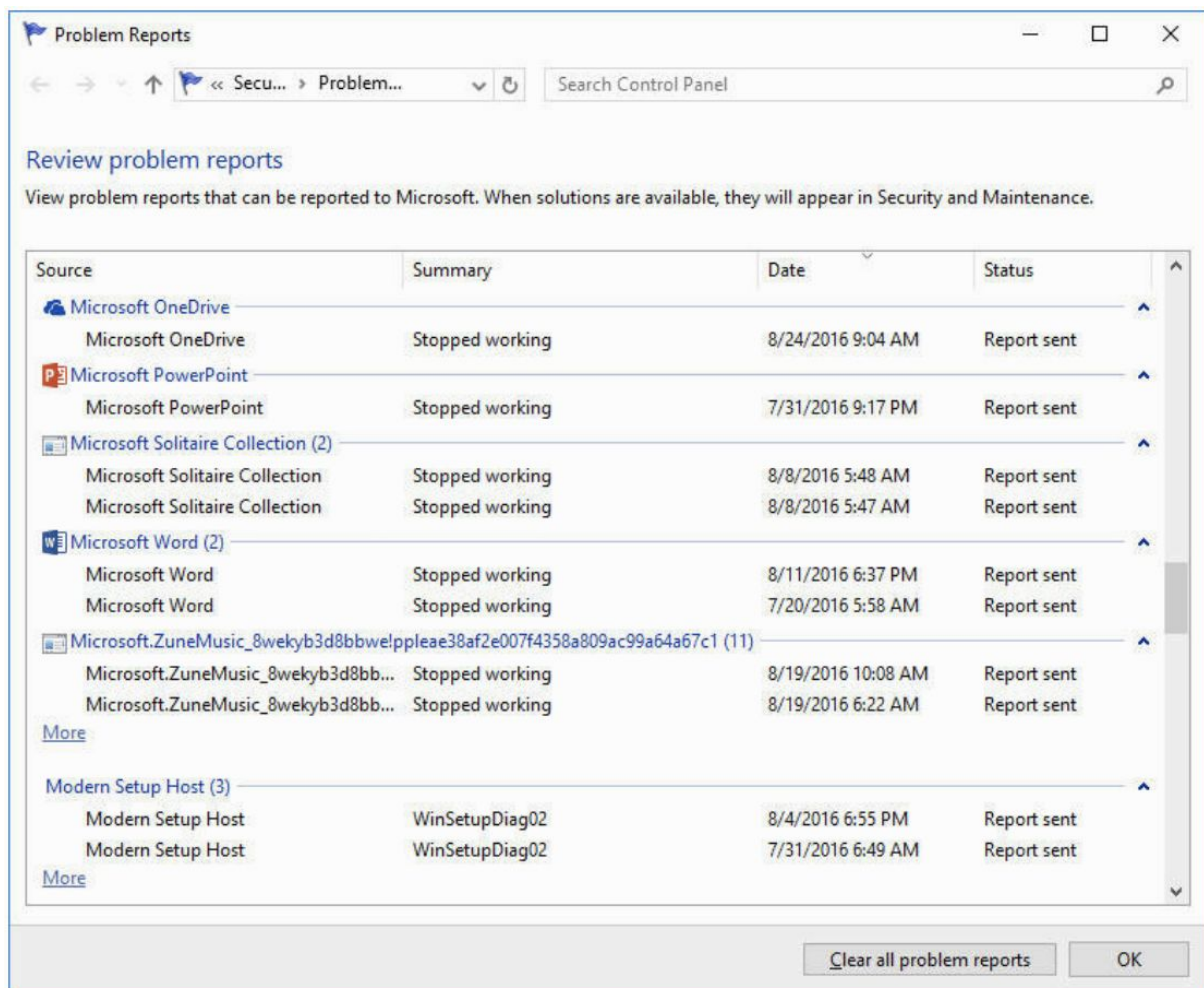
In previous versions, Windows was downright chatty about reporting crashes, successful updates, and minor speed bumps.

In Windows 10, most of these problem reports (including diagnostic reports sent after successful upgrades) are completely silent, but each report is logged.

You can use the history of problem reports on a system to review events and to see whether any patterns demand additional troubleshooting.

To open the Problem Reports log, type "problem reports" in the search box and then click View All Problem Reports.

The next figure shows a portion of the error history for a computer that was upgraded to Windows 10:



If more than two reports for a given heading are available, a More link appears below the group.

The number in parentheses to the right of the group heading tells you how many there are.

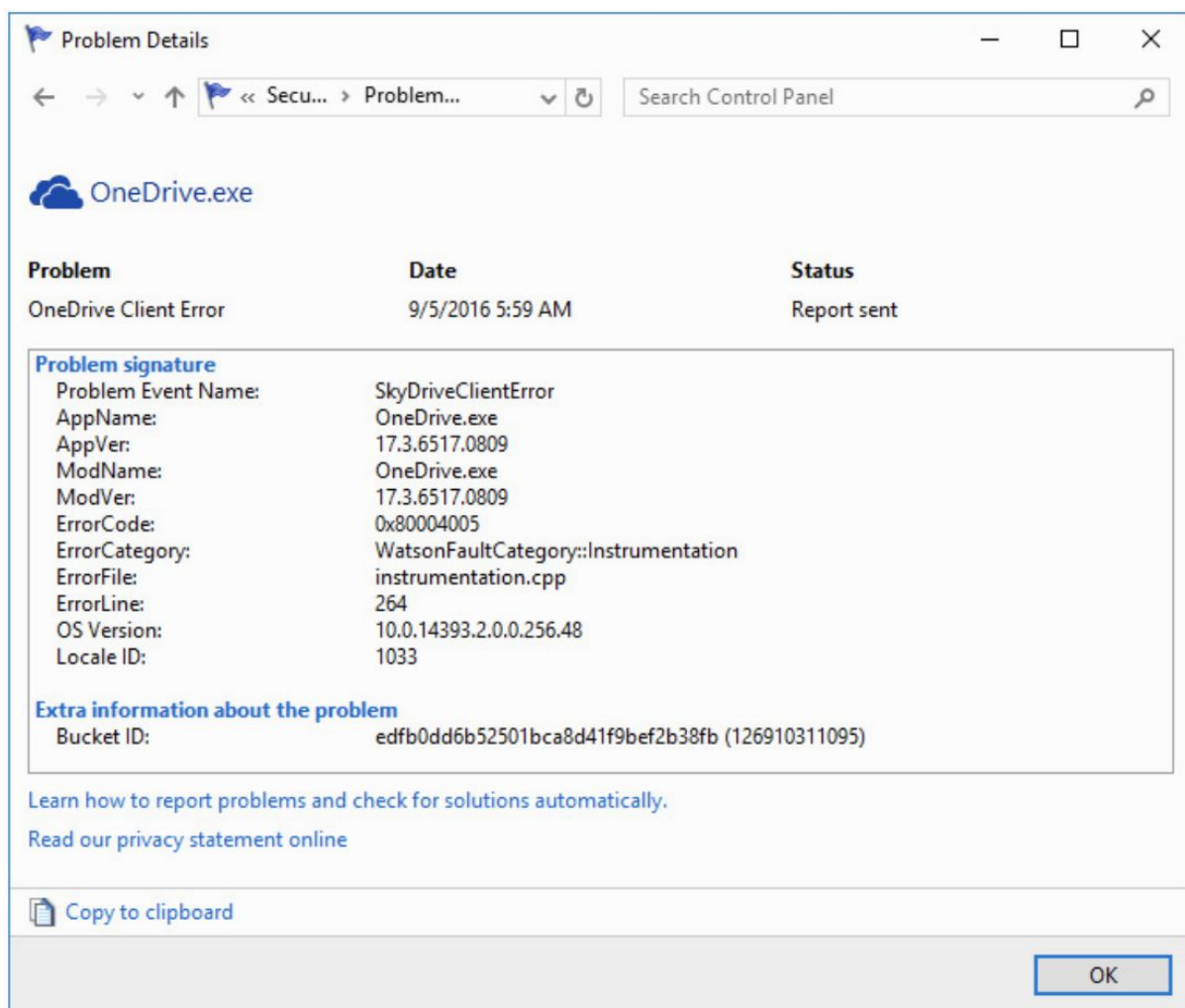
In the previous figure, for example, you can see the system has recorded 11 problems with the Groove Music app, which goes by an unwieldy name that starts with Microsoft.ZuneMusic.

If the words Solution Available appear in the Status column for an item, right-click that item and then click View Solution.

Note also that the shortcut menu includes commands to group the entries in the list of problem reports by source (which is the default view, shown in the previous picture), summary, date, or status—or you can choose Ungroup to see the entire, uncategorized list.

With the list grouped or not, you can sort by any field by clicking the field's column heading.

You can see a more detailed report about any event in this log by double-clicking the event:



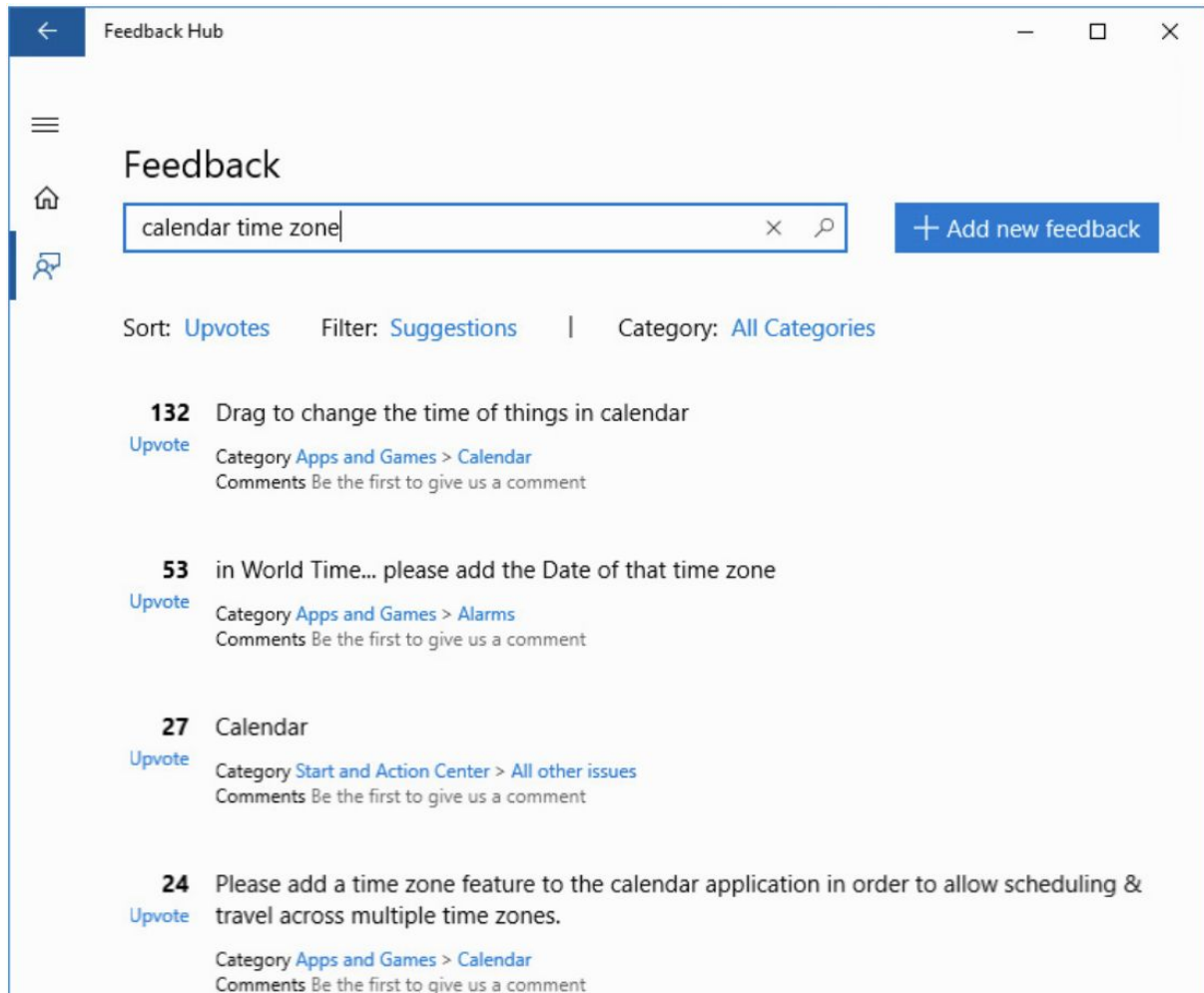
The Description field usually is written clearly enough to provide potentially useful information.

The rest of the details might or might not be meaningful to you, but they could be helpful to a support technician.

Some reports include additional details sent in a text file you can inspect for yourself.

Windows 10 also includes a Feedback app that anyone can use to send problem reports and suggestions to Microsoft.

From the app, you can search for existing feedback:



You can filter and sort the list of search results to see if your specific issue has already been reported.

If you find an existing feedback entry that describes your issue, you can add a comment and an upvote.

If you discover a new issue, feel free to create your own feedback item by clicking Add New Feedback.

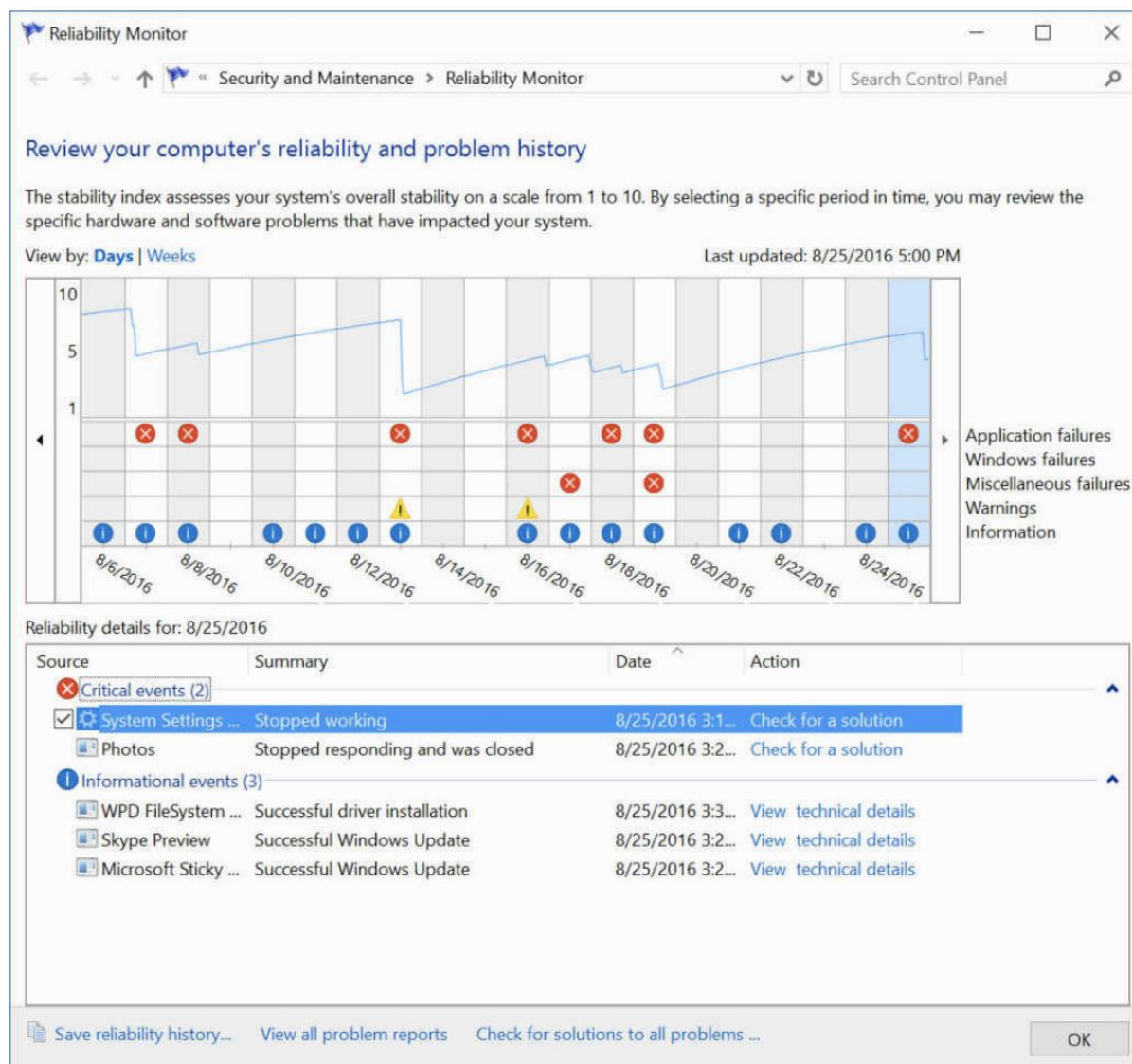
In the spirit of setting expectations, we are compelled to add that items you submit here are not the same as support tickets.

You won't get personal support from a Microsoft engineer or support tech, although your feedback will be considered, especially if the number of upvotes hits double or triple digits.

Reliability Monitor

Windows 10 keeps track of a wide range of system events. For a day-by-day inventory of these events, type reliability in the search box and then click the top result, View Reliability History.

That opens Reliability Monitor:



Each column in the graphical display represents events of a particular day (or week, if you click that option in the upper left corner).

Each red X along the first three lines below the graph (the various “Failures” lines) indicates a day on which problems occurred.

The “Warnings” line describes minor problems unrelated to system reliability, such as a program whose installation process didn’t complete properly.

The last line below the graph—the line marked Information—identifies days on which an app or an update was installed or removed.

You can see the details about the events of any day by clicking on the graph for that day.

Reliability Monitor retains its system stability records for one year, giving you plenty of history to review.

This history is most useful when you begin experiencing a new problem and are trying to track down its cause.

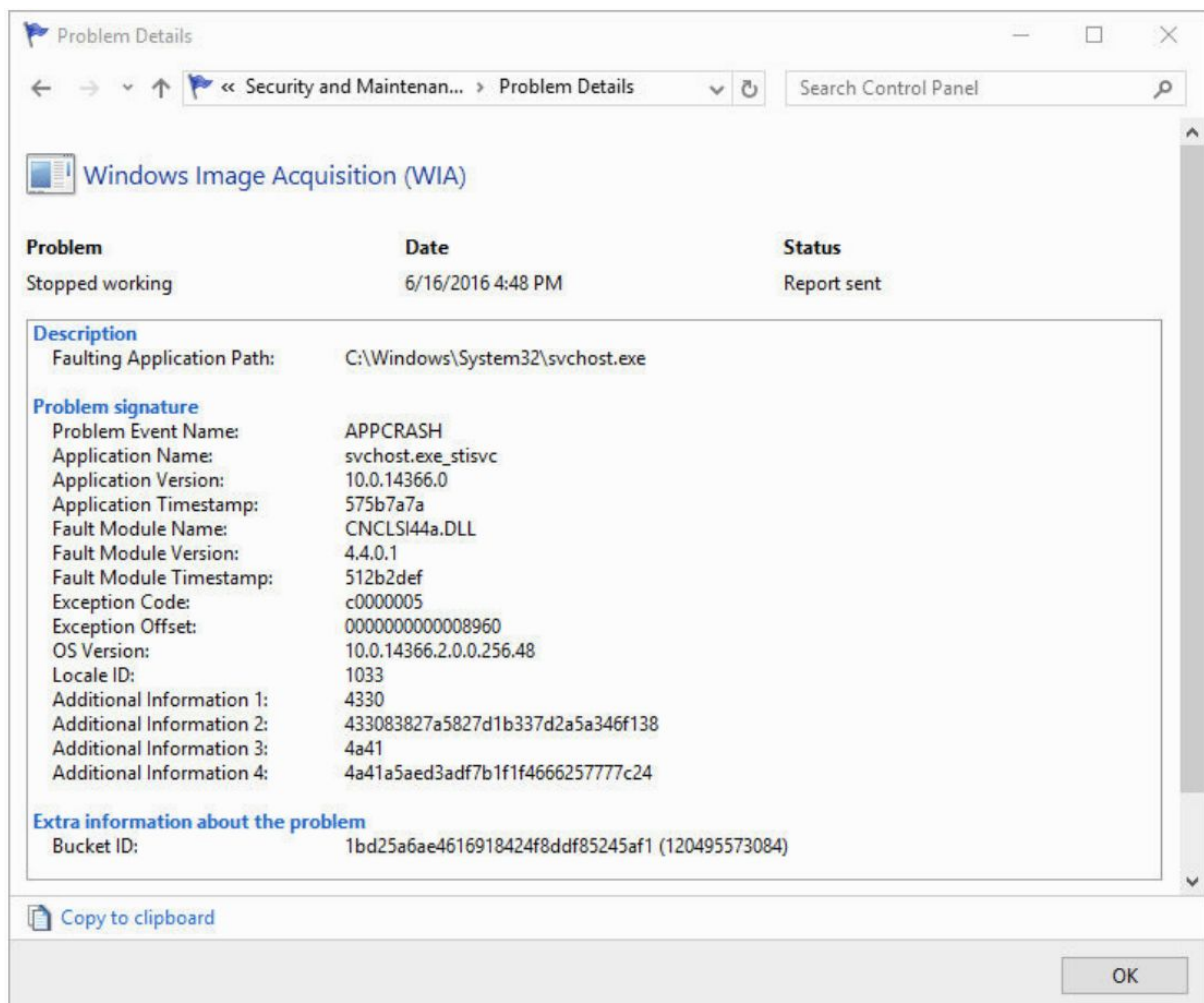
Examine the critical events for the period when the problem began, and see whether they correspond with an informational item, such as a program installation.

The alignment of these events could be mere coincidence, but it could also represent the first appearance of a long-term problem.

Conjunctions of this sort are worth examining.

If you think a new software application has destabilized your system, you can try uninstalling it.

Double-clicking any item exposes its contents, which are filled with technical details that are potentially useful, confusing, or both:



Although the various signatures and details for each such incident by themselves are probably just baffling, they're much more useful in the aggregate.

Armed with a collection of similar reports, an engineer can pin down the cause of a problem and deliver a bug fix.

If a previously common error suddenly stops appearing in the logs, chances are it was resolved with an update.

Note also that you can click the link in the Action column to take additional steps, such as searching for a solution or viewing the technical details of a particular event.

Event Viewer

In Windows, an event is any occurrence that is potentially noteworthy—to you, to other users, to the operating system, or to an application.

Events are recorded by the Windows Event Log service, and their history is preserved in one of several log files, including Application, Security, Setup, System, and Forwarded Events.

You can use Event Viewer, a Microsoft Management Console (MMC) snap-in supplied with Windows, to review and archive these event logs, as well as other logs created by the installation of certain applications and services.

You can examine the history of errors on your system by creating a filtered view of the Application log in Event Viewer.

Why would you want to do this?

The most likely reasons are to troubleshoot problems that have occurred, to keep an eye on your system to forestall problems, and to watch out for security breaches.

If a device has failed, a disk has filled close to capacity, a program has crashed repeatedly, or some other critical difficulty has arisen, the information recorded in the event logs can help you—or a technical support specialist—figure out what's wrong and what corrective steps are required.

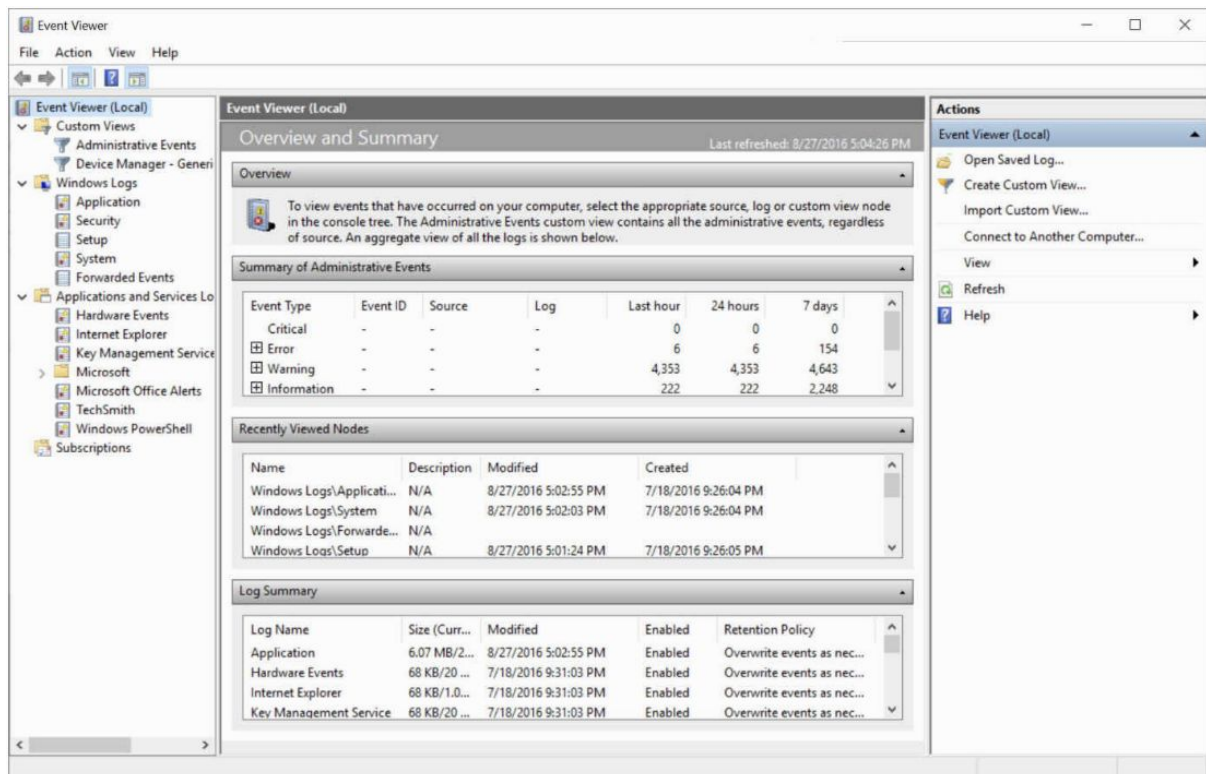
To start Event Viewer, find it by searching for event and then click Event Viewer or View Event Logs in the search results.

Alternatively, enter eventvwr.msc or eventvwr.exe in the Run box or at a command prompt.

Event Viewer requires administrator privileges for full functionality.

If you start Event Viewer while signed in as a standard user, it starts without requesting elevation.

However, the Security log is unavailable, along with some other features. To get access to all logs, right-click and choose "Run As Administrator".



When you select the top-level folder in Event Viewer's console tree, the details pane displays summary information, as shown in the previous picture.

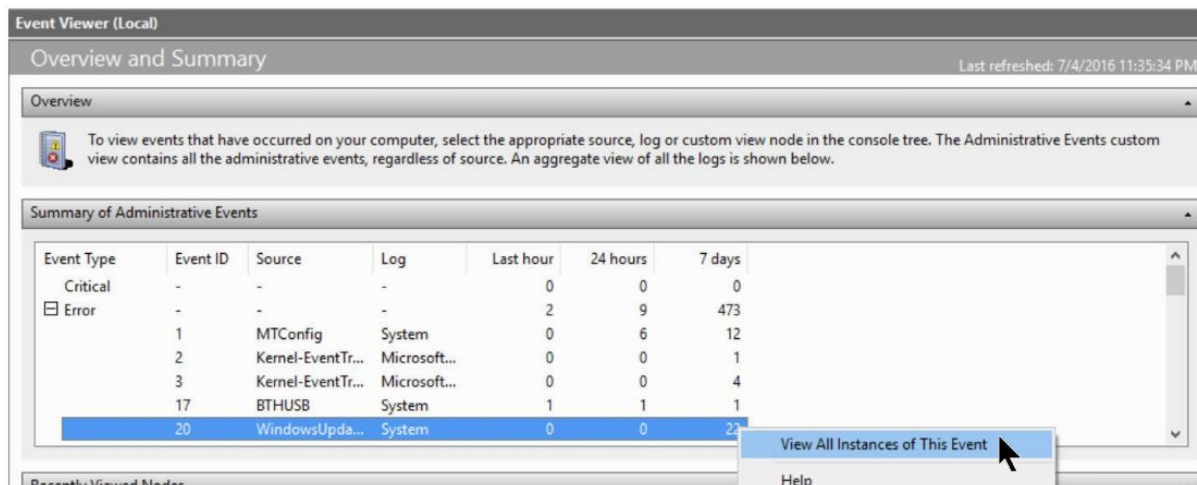
With this view, you can see at a glance whether any significant events that might require your attention have occurred in the past hour, day, or week.

You can expand each category to see the sources of events of that event type.

Seeing a count of events of various types in various time periods is interesting—but not particularly useful in and of itself.

But if, for example, you see an unusually large number of recent errors from a particular source, you might want to see the full list to determine whether a particular error needs closer examination.

To do that, you can right-click an event type or an event source under Summary Of Administrative Events, and then click View All Instances Of This Event, as shown here:



The resulting filtered list of events is drawn from multiple log files, sparing you from having to search in multiple places.

Armed with this information, you can quickly scroll through and examine the details of each one, perhaps identifying a pattern or a common factor that will help you find the cause and, eventually, the cure for whatever is causing the event.

Types of events

As a glance at the console tree confirms, events are recorded in one of several logs.

Logs are organized in the console tree in folders, and you can expand or collapse the folder tree using the customary outline controls.

The following default logs are visible under the Windows Logs heading:

- **Application.** Application events are generated by applications, including programs you install, programs that are preinstalled with Windows, apps from the Windows Store, and operating system services. Program developers decide which events to record in the Application log and which to record in a program-specific log under Applications And Services Logs.
- **Security.** Security events include sign-in attempts (successful and failed) and attempts to use secured resources, such as an attempt to create, modify, or delete a file.
- **Setup.** Setup events are generated by application installations.
- **System.** System events are generated by Windows itself and by installed features, such as device drivers. If a driver fails to load when you start a Windows session, for example, that event is recorded in the System log.
- **Forwarded Events.** The Forwarded Events log contains events gathered from other computers.

Under the Applications And Services Logs heading, you'll find logs for individual applications and services.

The difference between this heading and the Windows Logs heading is that logs under Applications And Services record events related only to a particular program or feature, whereas the logs that appear under Windows Logs generally record events that are systemwide.

If you expand the Microsoft entry under Applications And Services Logs, you'll find a Windows subfolder, which in turn contains a folder for each of hundreds of features that are part of Windows 10.

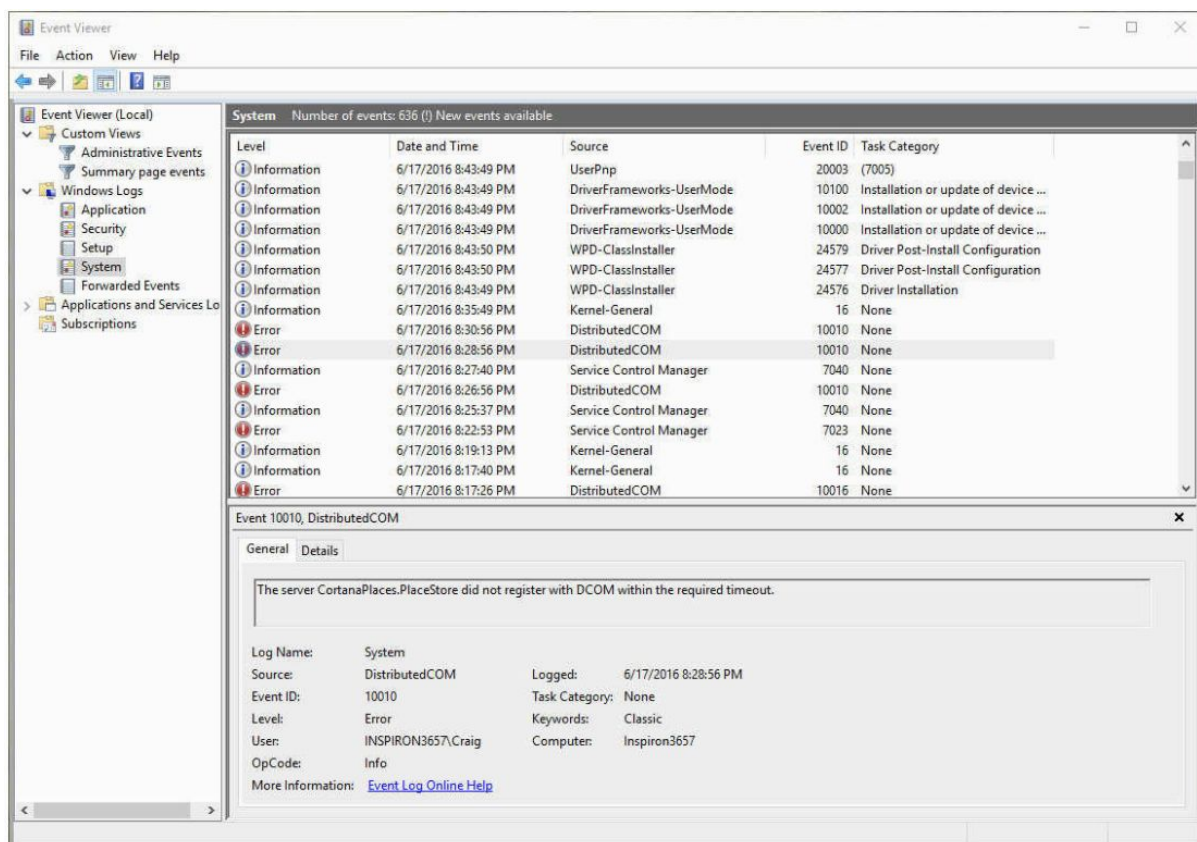
Each of these folders contains one or more logs.

Viewing logs and events

When you select a log or a custom view from the console tree, the details pane shows a list of associated events, sorted (by default) in reverse chronological order, with each event occupying a single line.

A preview pane below the list displays the contents of the saved event record.

The next image shows one such listing from the System log:



Events in most log files are classified by severity, with one of three entries in the Level field: Error, Warning, or Information.

- Error events represent possible loss of data or functionality. Examples of errors include events related to a malfunctioning network adapter and loss of functionality caused by a device or service that doesn't load at startup.
- Warning events represent less significant or less immediate problems than error events. Examples of warning events include a nearly full disk, a timeout by the network redirector, and data errors on local storage.
- Other events that Windows logs are identified as Information events.

The Security log file uses two different icons to classify events: a key icon identifies Audit Success events, and a lock icon identifies Audit Failure events.

Both types of events are classified as Information-level events; "Audit Success" and "Audit Failure" are stored in the Keywords field of the Security log file.

The preview pane shows information about the currently selected event.

Drag the split bar between the list and preview pane up to make the preview pane larger so that you can see more details, or double-click the event to open it in a separate dialog box that includes Next and Previous buttons and an option to copy the event to the Clipboard.

The information you find in Event Viewer is evidence of things that happened in the past.

Like any good detective, you have the task of using those clues to help identify possible issues.

One hidden helper, located near the bottom of the Event Properties dialog box, is a link to more information online.

Clicking this link opens a webpage that might provide more specific and detailed information about this particular combination of event source and event ID, including further action you might want to take in response to the event.

Customizing the presentation of tabular data in Event Viewer

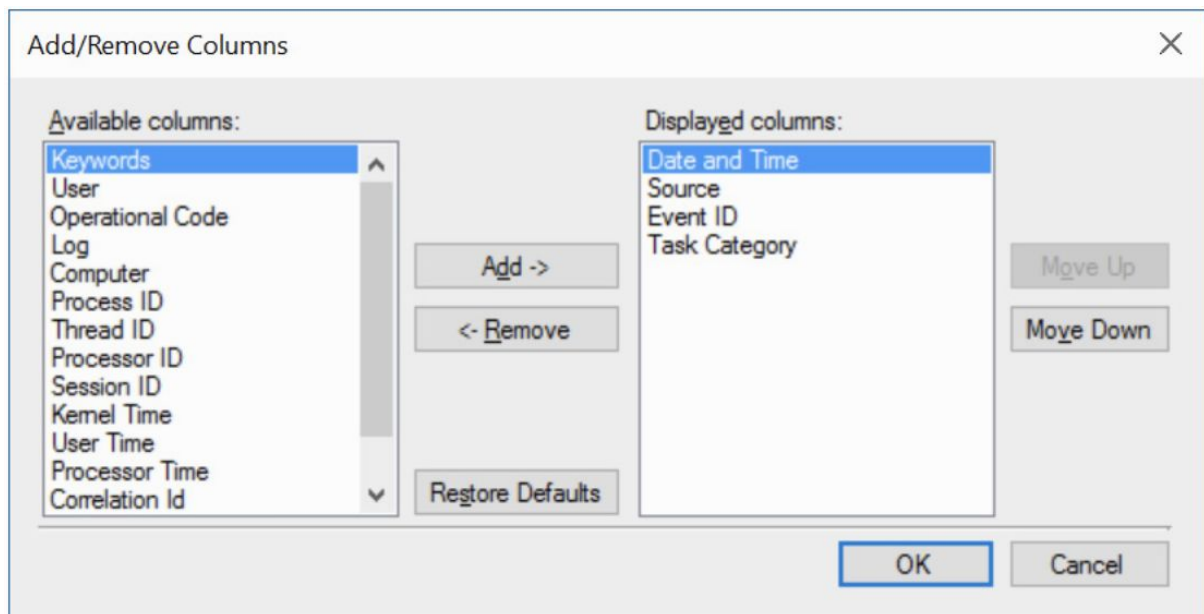
If you have passing familiarity with Details view in File Explorer, you'll feel right at home with the many tabular reports in Event Viewer.

You can change a column's width by dragging its heading left or right.

You can sort on any column by clicking its heading; click a second time to reverse the sort order.

Right-click a column heading and choose Add/Remove Columns to make more or fewer columns appear.

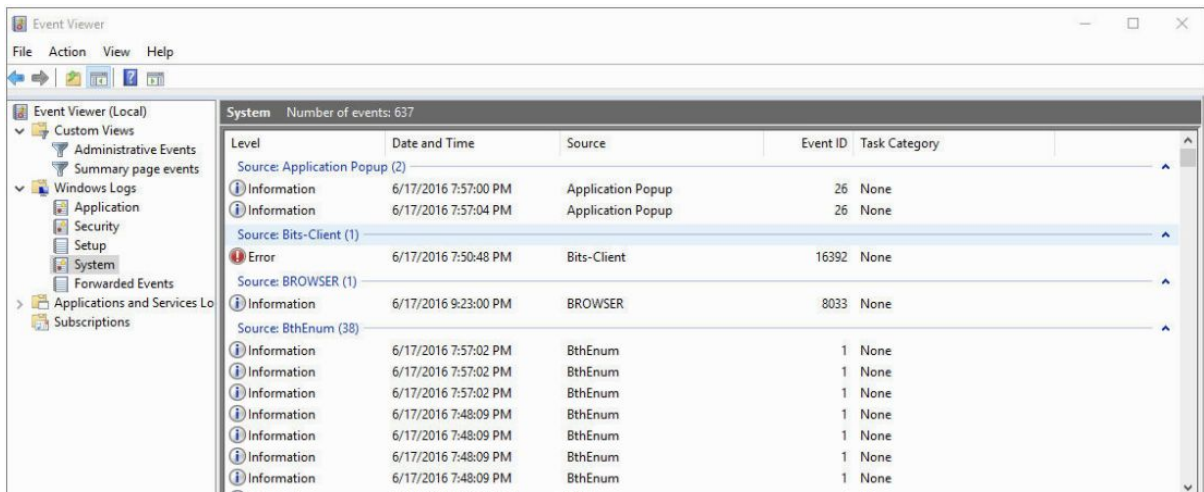
As you'll see, the choices are many:



As with files and folders in File Explorer, you also have the option to group events in Event Viewer.

To do that, right-click the column heading by which you want to group and then click Group Events By This Column.

Here, for example, we grouped by Source:



Filtering the log display

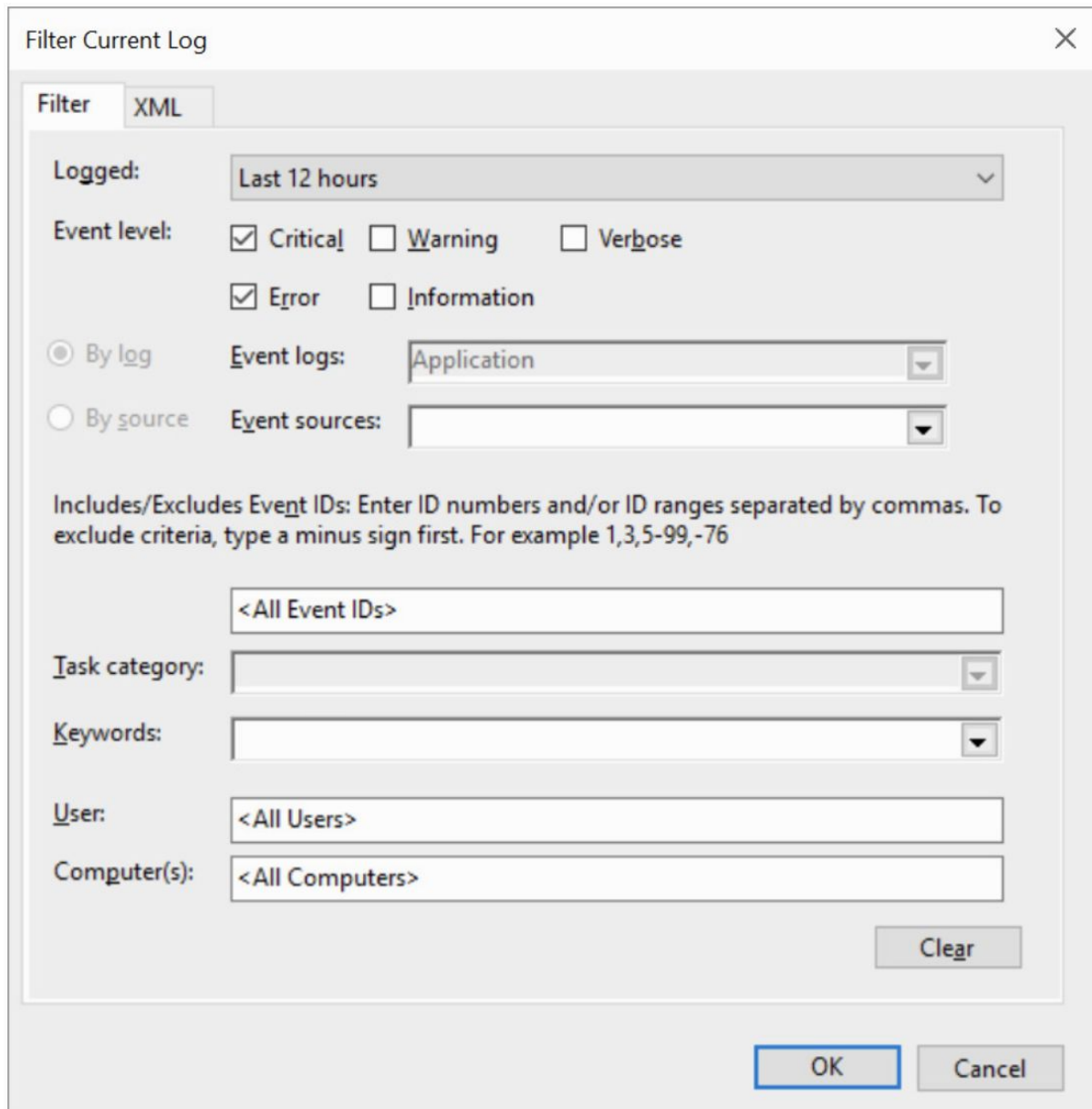
As you can see from a cursory look at your System log, events can pile up quickly, obscuring those generated by a particular source or those that occurred at a particular date and time.

Sorting and grouping can help you to find that needle in a haystack, but to get the hay out of the way altogether, use filtering.

With filtering, you can select events based on multiple criteria; all other events are hidden from view, making it much easier to focus on the items you currently care about.

To filter the currently displayed log or custom view, click Filter Current Log or Filter Current Custom View in the Action pane on the right.

A dialog box like the one shown in the next figure appears:



The image shows a 'Filter Current Log' dialog box with a close button (X) in the top right corner. It has two tabs: 'Filter' (selected) and 'XML'. The 'Filter' tab contains several sections:

- Logged:** A dropdown menu currently set to 'Last 12 hours'.
- Event level:** Four checkboxes: 'Critical' (checked), 'Warning' (unchecked), 'Verbose' (unchecked), and 'Error' (checked). 'Information' is also unchecked.
- By log:** A radio button that is selected, followed by an 'Event logs:' dropdown menu set to 'Application'.
- By source:** A radio button that is unselected, followed by an 'Event sources:' dropdown menu.
- Includes/Excludes Event IDs:** A text box containing '<All Event IDs>'. Above this box is a descriptive text: 'Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76'.
- Task category:** A dropdown menu.
- Keywords:** A dropdown menu.
- User:** A text box containing '<All Users>'.
- Computer(s):** A text box containing '<All Computers>'.

At the bottom right of the dialog, there is a 'Clear' button. At the very bottom, there are 'OK' and 'Cancel' buttons.

To fully appreciate the flexibility of filtering, click the arrow by each filter.

You can, for example, filter events from the past hour, 12 hours, day, week, month, or any custom time period you specify.

In the Event Sources, Task Category, and Keywords boxes, you can type text to filter on (separating multiple items with commas), but you'll probably find it easier to click the arrow and then click each item you want to include in your filtered view.

In the Includes/Excludes Event IDs box, you can enter multiple ID numbers and number ranges, separated by commas; to exclude particular event IDs, precede their number with a minus sign.

Click OK to see the filtered list.

If you think you'll use the same filter criteria again, click Save Filter To Custom View in the Action pane on the right.

To restore the unfiltered list, in the Event Viewer window, click Clear Filter.

Dealing with Stop errors

If Windows has ever suddenly shut down, you've probably experienced that sinking feeling in the pit of your stomach.

When Windows 10 encounters a serious problem that makes it impossible for the operating system to continue running, it does the only thing it can do, just as every one of its predecessors has done in the same circumstances.

It shuts down immediately and displays an ominous text message whose technical details begin with the word STOP.

Because a Stop error typically appears in white letters on a blue background, this type of message is often referred to as a blue-screen error or the Blue Screen of Death (BSOD).

When a Stop error appears, it means there is a serious problem that demands your immediate attention.

Windows 10 collects and saves a variety of information in logs and dump files, which a support engineer or developer armed with debugging tools can use to identify the cause of Stop errors.

Customizing how Windows handles Stop errors

When Windows encounters a serious error that forces it to stop running, it displays a Stop message and then writes debugging information to the page file.

When the computer restarts, this information is saved as a crash dump file, which can be used to debug the specific cause of the error.

You can customize two crucial aspects of this process by defining the size of the crash dump files and specifying whether you want Windows to restart automatically after a Stop message appears.

By default, Windows automatically restarts after a Stop message and creates a crash dump file optimized for automatic analysis.

That's the preferred strategy in response to random, isolated Stop errors.

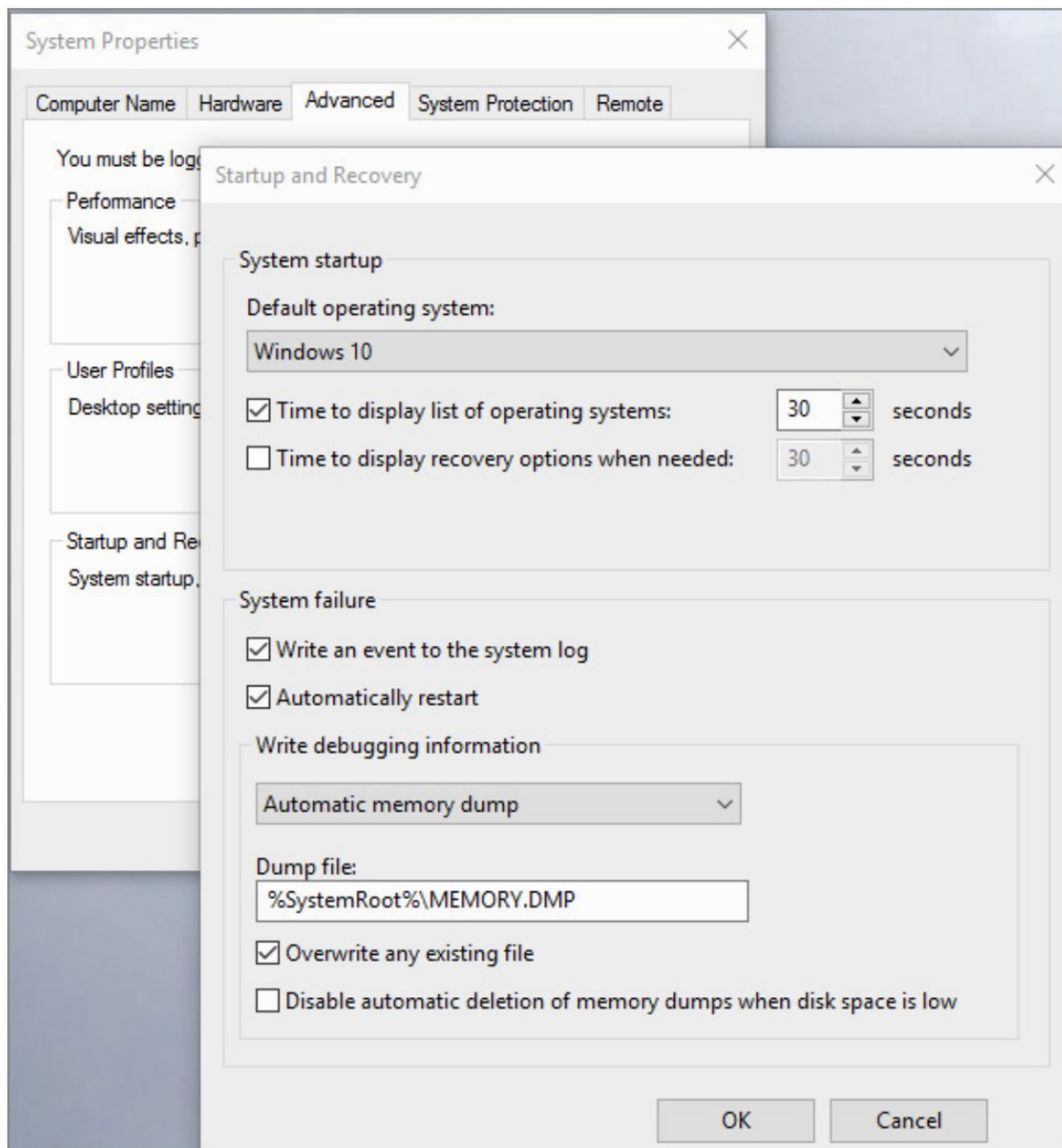
But if you're experiencing chronic Stop errors, you might have more troubleshooting success by changing these settings to collect a more detailed dump file and to stop after a crash.

To make this change, type "advanced" in the search box and then click View Advanced System Settings in the results list.

Or, in the Run or search box, type the undocumented command "systempropertiesadvanced" and press Enter.

On the Advanced tab of the System Properties dialog box, under Startup And Recovery, click Settings.

Adjust the settings under the System Failure heading:



If you want Windows to pause at the Stop error message page, clear the Automatically Restart check box and click OK.

From the same dialog box, you can also define the settings for crash dump files.

By default, Windows sets this value to Automatic Memory Dump, which saves a kernel memory dump after a crash.

This option includes memory allocated to kernel-mode drivers and programs, which are most likely to cause Stop errors.

Because this file does not include unallocated memory or memory allocated to user-mode programs, it usually will be smaller in size than the amount of RAM on your system.

The exact size varies, but in general you can expect the file to be no larger than one-third the size of installed physical RAM, and much less than that on a system with 16 GB of RAM or more.

The crash files are stored in %SystemRoot% using the file name Memory.dmp.

If your system crashes multiple times, each new dump file replaces the previous file.

If disk space is limited or you're planning to send the crash dump file to a support technician, you might want to consider setting the system to store a small memory dump (commonly called a mini dump).

A small memory dump contains just a fraction of the information in a kernel memory dump, but it's often enough to determine the cause of a problem.

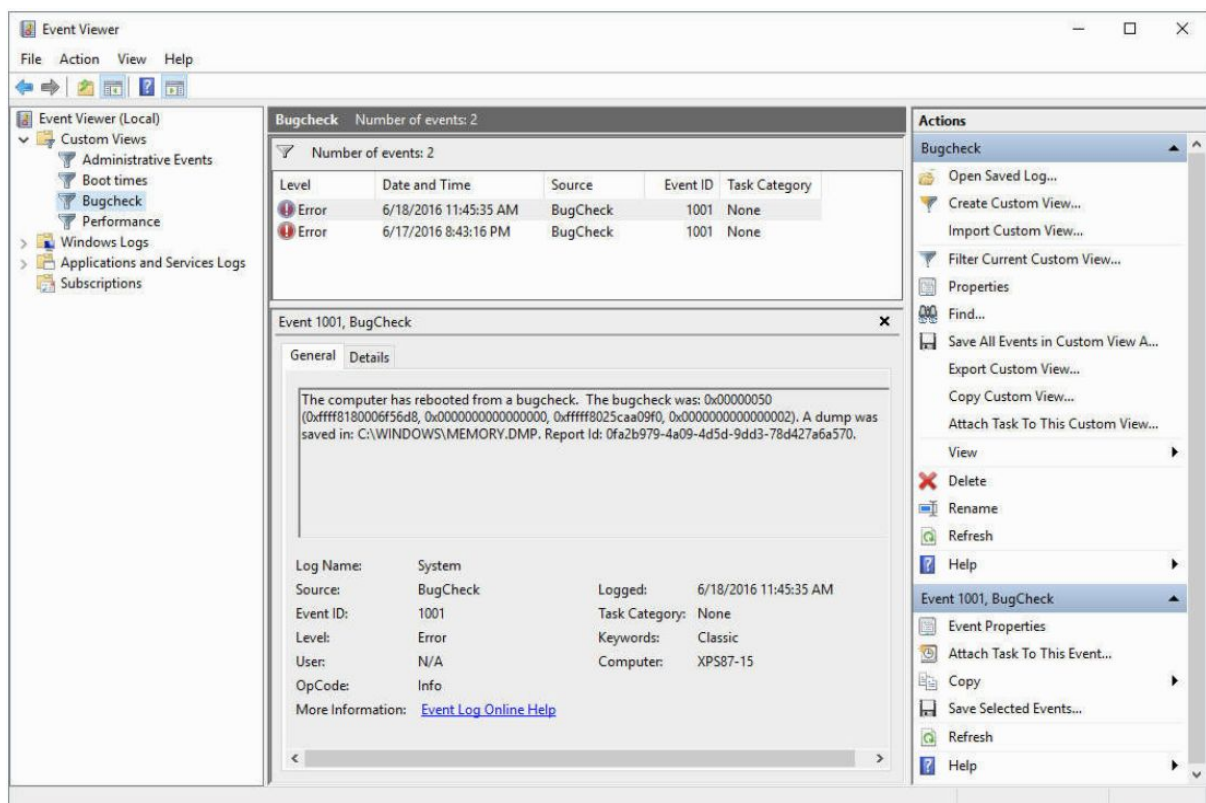
What's in a Stop error

The exact text of a Stop error varies according to what caused the error.

But the format is predictable.

Don't bother copying down the error code from the blue screen itself.

Instead, look through Event Viewer for an event with the source BugCheck, as shown in the example in the next image:

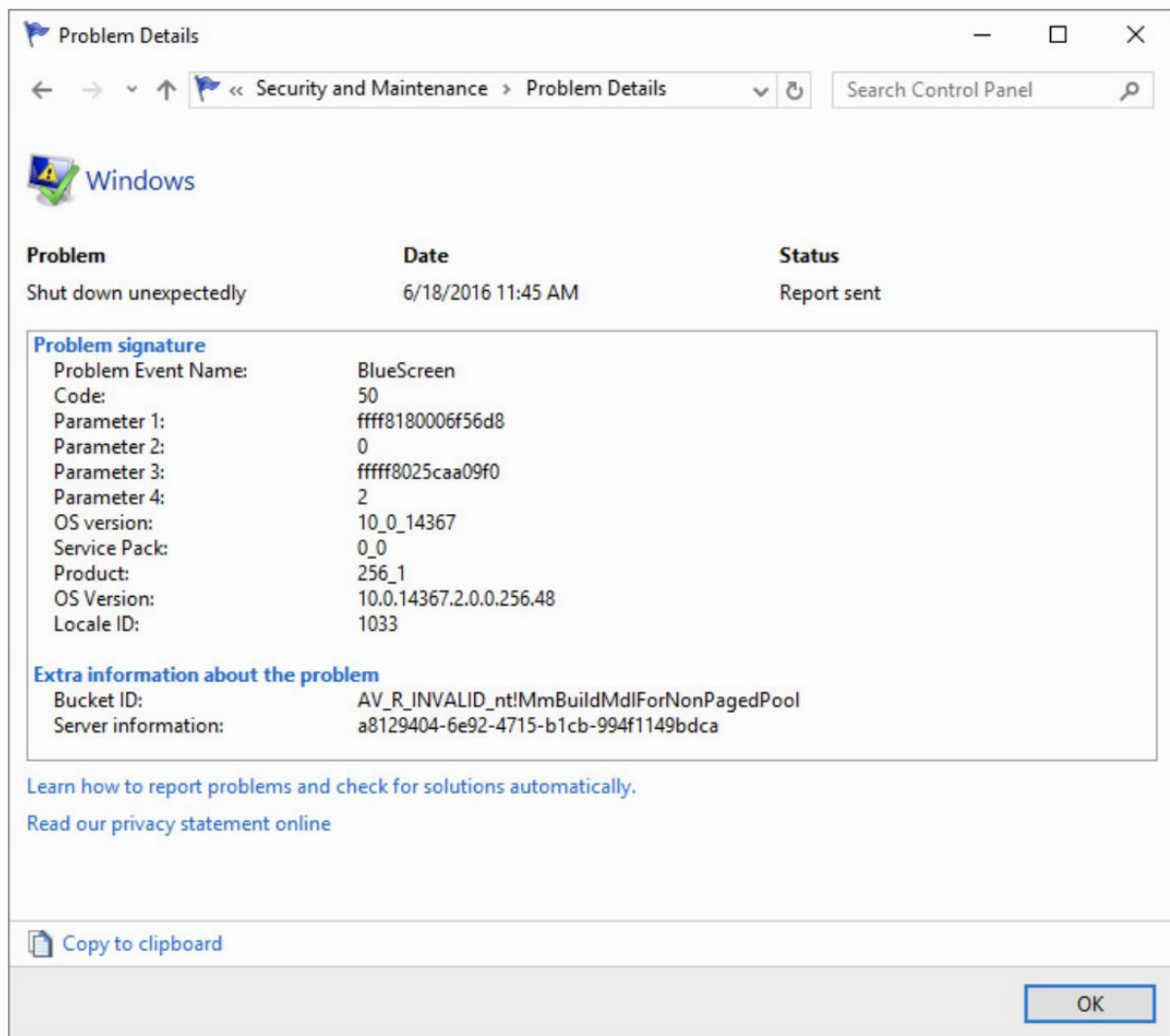


You can gather important details from the bugcheck information, which consists of the error number (in hexadecimal notation, as indicated by the 0x at the beginning of the code) and up to four parameters that are specific to the error type.

Windows 10 also displays the information in Reliability Monitor, under the heading Critical Events.

Select the day on which the error occurred, and double-click the “Shut down unexpectedly” entry for an event with Windows as the source.

That displays the bugcheck information in a slightly more readable format than in Event Viewer, as shown next, even using the term BlueScreen as the Problem Event Name:



For a comprehensive and official list of what each error code means, see the MSDN “Bug Check Code Reference” at <https://bit.ly/bug-check-codes>.

A code of 0x00000144, for example, points to problems with a USB 3 controller, whereas 0x0000009F is a driver power state failure.

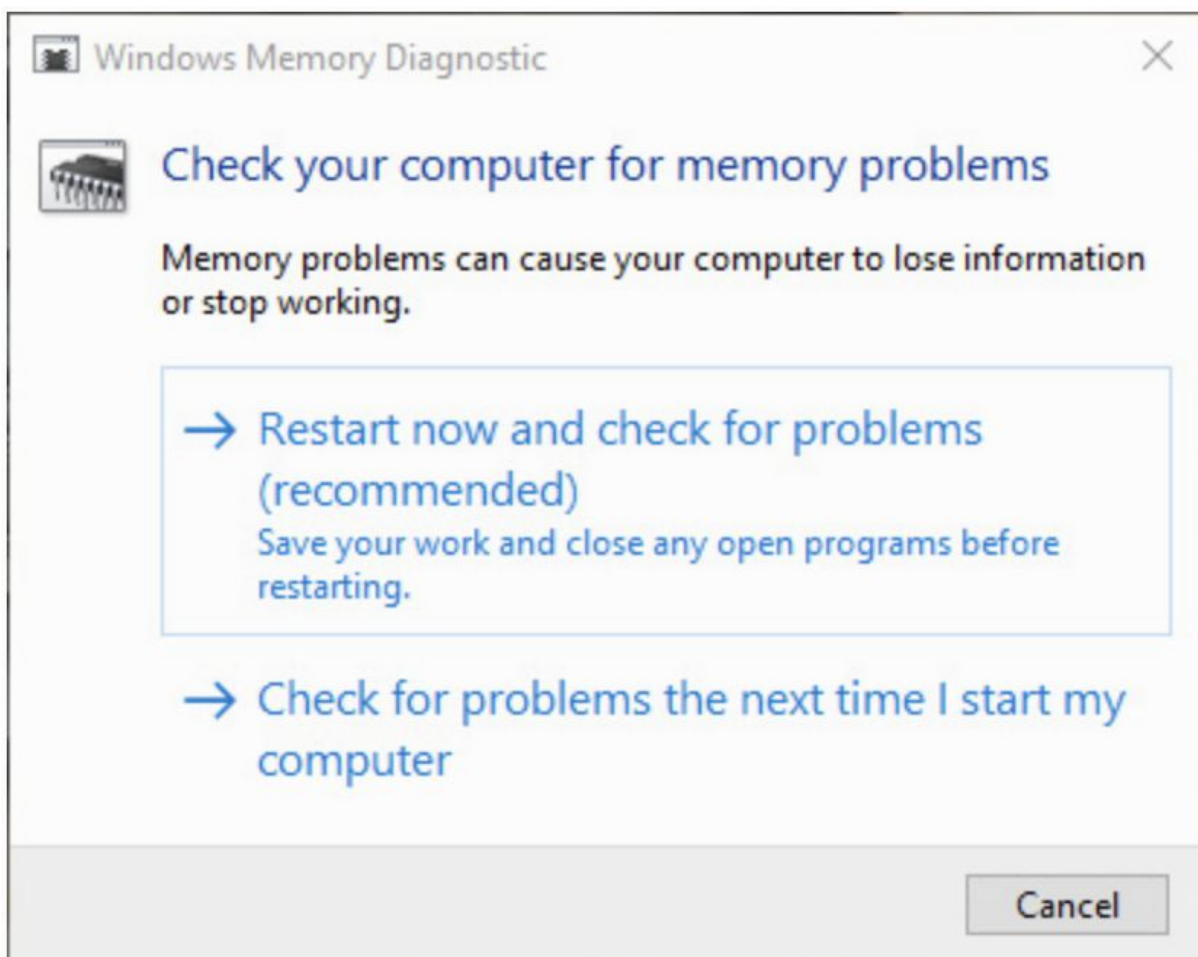
Our favorite is 0xDEADDEAD, which indicates a manually initiated crash.

In general, you need a debugger or a dedicated analytic tool to get any additional useful information from a memory dump file.

Isolating the cause of a Stop error

If you experience a Stop error, don't panic. Instead, run through the following troubleshooting checklist to isolate the problem and find a solution:

- Don't forget to rule out hardware problems. In many cases, software is the victim and not the cause of blue-screen errors. Common hardware failures such as a damaged hard disk or a corrupted solid state disk (SSD), defective physical RAM, an overheated CPU chip, or even a bad cable can result in Stop errors. If the errors seem to happen at random and the message details vary each time, there's a good chance you're experiencing hardware problems.
- Check your memory. Windows 10 includes a memory diagnostic tool you can use if you suspect a faulty or failing memory chip. To run this diagnostic procedure, type memory in the search box and click Windows Memory Diagnostic in the search results. This tool, shown here, requires a restart to run its full suite of tests, which you can perform immediately or defer until your next restart.



- Look for a driver name in the error details. If the error message identifies a specific file name and you can trace that file to a driver for a specific hardware device, you might be able to solve the problem by disabling, removing, or rolling back that driver to an earlier version. The most likely offenders are network interface cards, video adapters, and disk controllers.
- Ask yourself, “What’s new?” Be suspicious of newly installed hardware and software. If you added a device recently, remove it temporarily and see whether the problem goes away. Take an especially close look at software in the categories that install services or file-system filter drivers; these hook into the core operating system files that manage the file system to perform tasks such as scanning for viruses. This category includes backup programs, multimedia applications, antivirus software, and DVD-burning utilities. You might need to permanently uninstall or update the program to resolve the problem.
- Search Microsoft Support. Make a note of the error code and all parameters. Search Microsoft Support using both the full and short formats. For instance, if you’re experiencing a `KMODE_EXCEPTION_NOT_HANDLED` error, use `0x1E` and `0x0000001E` as your search keywords.
- Check your system BIOS or firmware. Is an update available from the manufacturer of the system or motherboard? Check the BIOS or firmware documentation carefully; resetting all BIOS options to their defaults can sometimes resolve an issue caused by overtweaking.
- Are you low on system resources? Stop errors are sometimes the result of a critical shortage of RAM or disk space. If you can start in Safe Mode, check the amount of physical RAM installed and look at the system and boot drives to see how much free disk space is available.
- Is a crucial system file damaged? To reinstall a driver, restart your computer in Safe Mode. (See the following section.) If your system starts in Safe Mode but not normally, you very likely have a problem driver. Try running Device Manager in Safe Mode and uninstalling the most likely suspect. Or run System Restore in Safe Mode. If restoring to a particular day cures the problem, use Reliability Monitor to determine what changes occurred on or shortly after that day.

Troubleshooting in Safe Mode

In earlier times, holding down the F8 key while restarting gave you the opportunity to start your system in Safe Mode, with only core drivers and services activated.

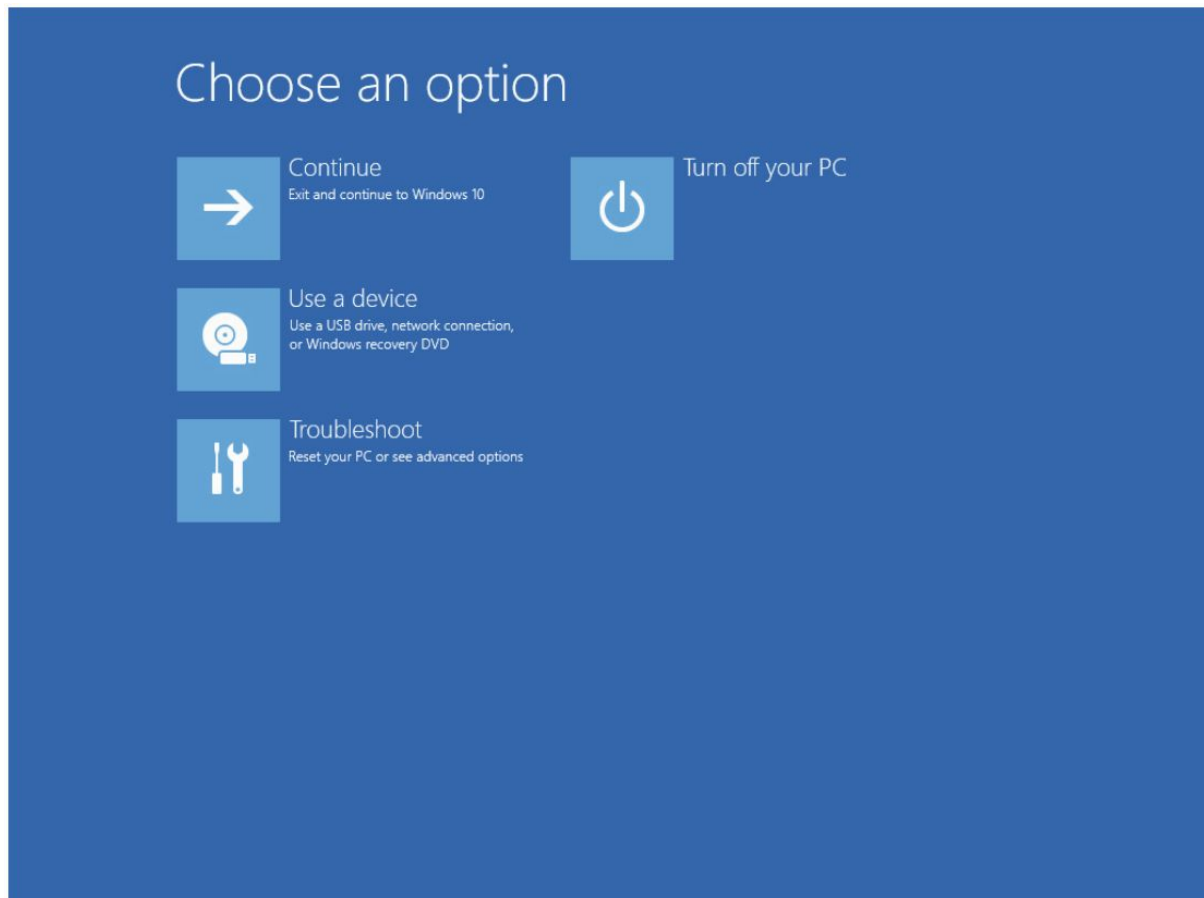
On modern hardware, with UEFI firmware, that’s no longer possible.

Safe Mode is still available, but you have to work a little harder to get there.

If you can start Windows and get to the sign-in screen, you can then click the Power button in the lower right corner of that screen.

Clicking Restart while holding down Shift takes you to the Windows Recovery Environment, where you can take various actions, including restoring Windows from an image backup (if one is available), running System Restore to revert to a saved Restore Point, and resetting your PC.

When you first arrive in the Windows Recovery Environment, the following menu appears:



To get to Safe Mode, click Troubleshoot in this menu, and then click Advanced Options.

On the Advanced Options menu that appears, click Startup Settings, and then click Restart.

You will then see the Startup Settings menu:

Startup Settings

Press a number to choose from the options below:

Use number keys or functions keys F1-F9.

- 1) Enable debugging
- 2) Enable boot logging
- 3) Enable low-resolution video
- 4) Enable Safe Mode
- 5) Enable Safe Mode with Networking
- 6) Enable Safe Mode with Command Prompt
- 7) Disable driver signature enforcement
- 8) Disable early launch anti-malware protection
- 9) Disable automatic restart after failure

Press F10 for more options

Press Enter to return to your operating system

In Safe Mode, you can access certain essential configuration tools, including Device Manager, System Restore, and Registry Editor.

If Windows appears to work properly in Safe Mode, you can safely assume there's no problem with the basic services.

Use Device Manager, Driver Verifier, and Event Viewer to try to Figure out where the trouble lies.

If you suspect that a newly installed device or program is the cause of the problem, you can remove the offending software while you're running in Safe Mode.

Use Device Manager to uninstall or roll back a hardware driver; use Control Panel to remove a desktop program or utility.

Then try restarting the system normally to see whether your changes have resolved the problem.

If you need access to network connections, choose the Safe Mode With Networking option, which loads the base set of Safe Mode files and adds drivers and services required to start Windows networking.

The third Safe Mode option, Safe Mode With Command Prompt, loads the same stripped-down set of services as Safe Mode, but it uses the Windows command interpreter (Cmd.exe) as a shell instead of the graphical Windows Explorer (Explorer.exe, which also serves as the host for File Explorer).

This option is unnecessary unless you're having a problem with the Windows graphical interface.

The default Safe Mode also provides access to the command line.

Press Windows key+R, and then type `cmd.exe` in the Run dialog box.

The six additional choices on the Startup Settings menu are of use in specialized circumstances:

- **Enable Boot Logging.** With this option enabled, Windows creates a log file that lists the names and status of all drivers loaded into memory. To view the contents of this file, look for `Ntbtlog.txt` in the `%SystemRoot%` folder. If your system is hanging because of a faulty driver, the last entry in this log file might identify the culprit.
- **Enable Low-Resolution Video.** This option starts the computer in 640-by-480 resolution using the current video driver. Use this option to recover from video problems that are caused not by a faulty driver but by incorrect settings, such as an improper resolution or refresh rate.
- **Disable Driver Signature Enforcement.** Use this option if Windows is refusing to start because you installed an unsigned user-mode driver. Windows will start normally, not in Safe Mode. Note that you cannot disable the requirement for signed kernel-mode drivers.
- **Disable Early Launch Antimalware Protection.** This is one of the core security measures of Windows 10 on a UEFI-equipped machine. Unless you're a security researcher or a driver developer, we can't think of any reason to disable this important security check.
- **Disable Automatic Restart After Failure.** Use this option if you're getting Stop errors (blue-screen crashes) and you want the opportunity to see the crash details on the Stop error screen instead of simply pausing there before restarting.

Connecting to another computer with Quick Assist

With Quick Assist, an inconspicuous new tool introduced with Windows 10, you can connect to another computer to give or receive assistance.

If you are the helper, you can see the other computer's screen on your system, run diagnostic tools such as Task Manager, edit the remote system's registry, and even use a stylus to annotate the remote display.

With roles reversed, you can let another user troubleshoot problems on your own system and help you find your way out of difficulty.

The technology behind Quick Assist is not new.

In the guise of Windows Remote Assistance, it was present in versions of Windows dating back to Windows XP and Windows Server 2003.

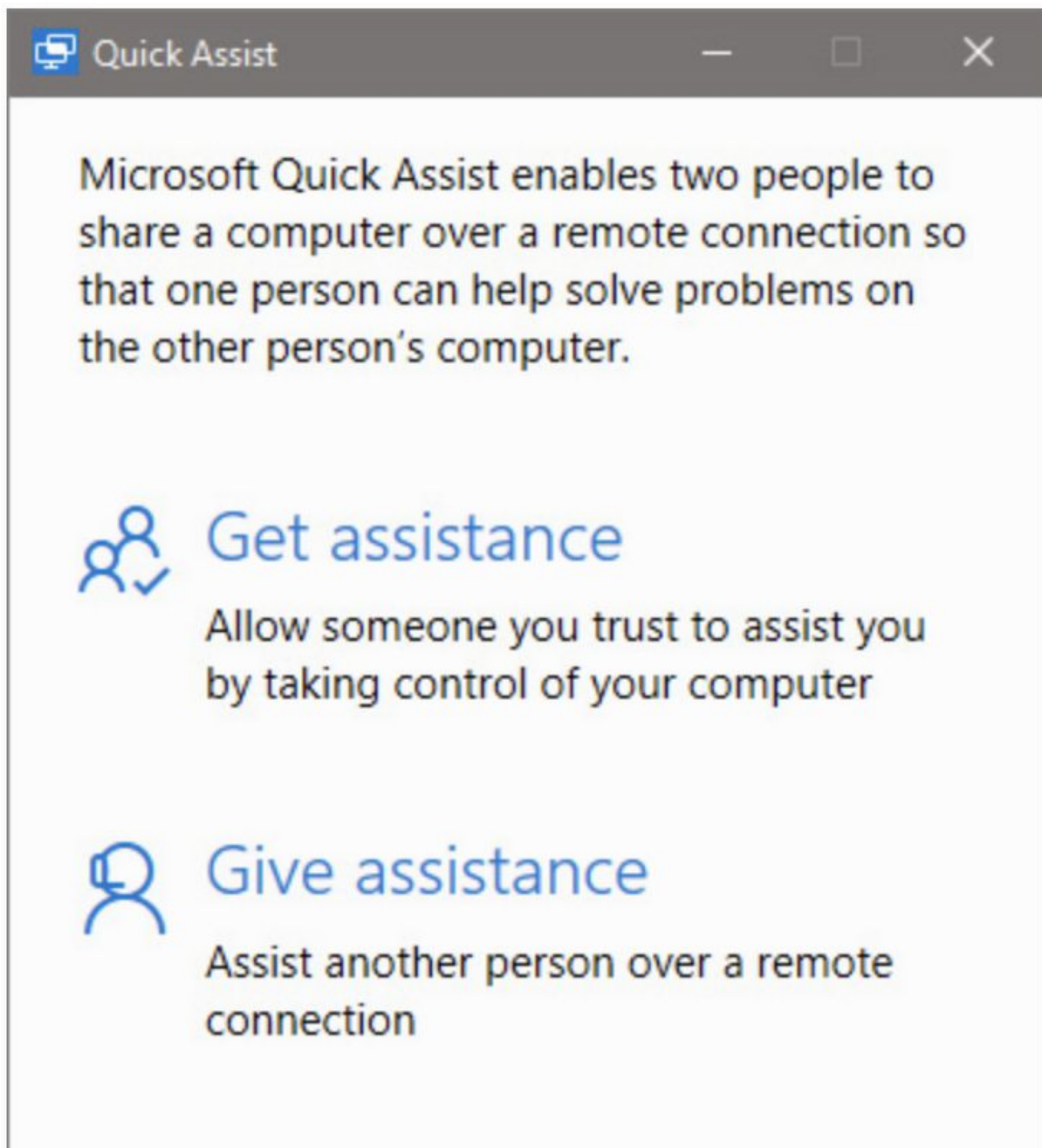
But earlier incarnations were complex and difficult to use.

With Quick Assist, Windows 10 provides a simpler if less ambitious tool, one that a novice in need of help can use with ease.

Two ground rules apply: the computer giving assistance must be able to sign in with a Microsoft account (Quick Assist will prompt for one if the user is signed in using a local account), and both systems have to be running Windows 10, version 1607 or later.

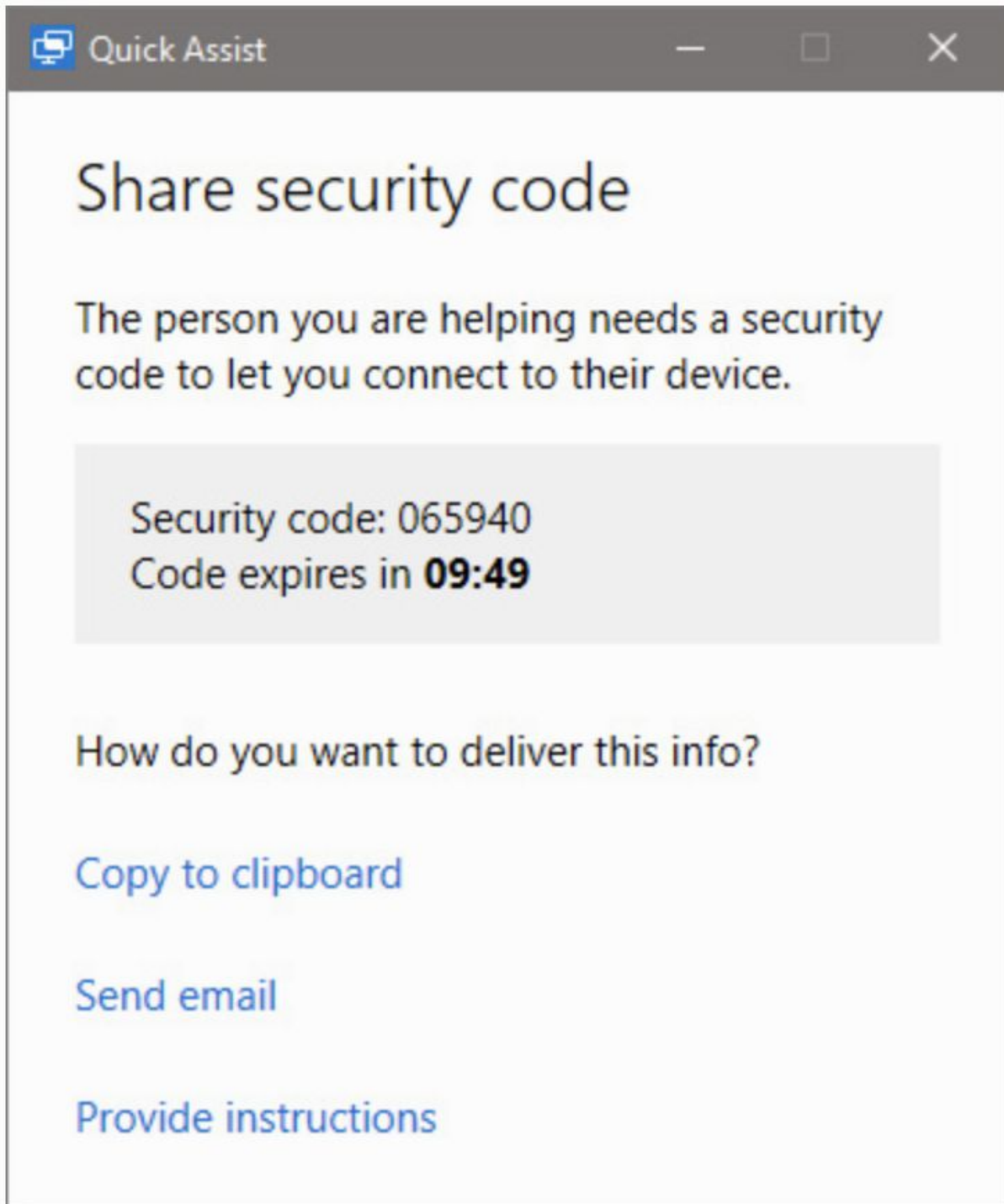
The simplest way to run Quick Assist is to start typing quick in the Search box.

The program should quickly appear at the top of the search results. Both parties run the program in this manner, and both see the following:

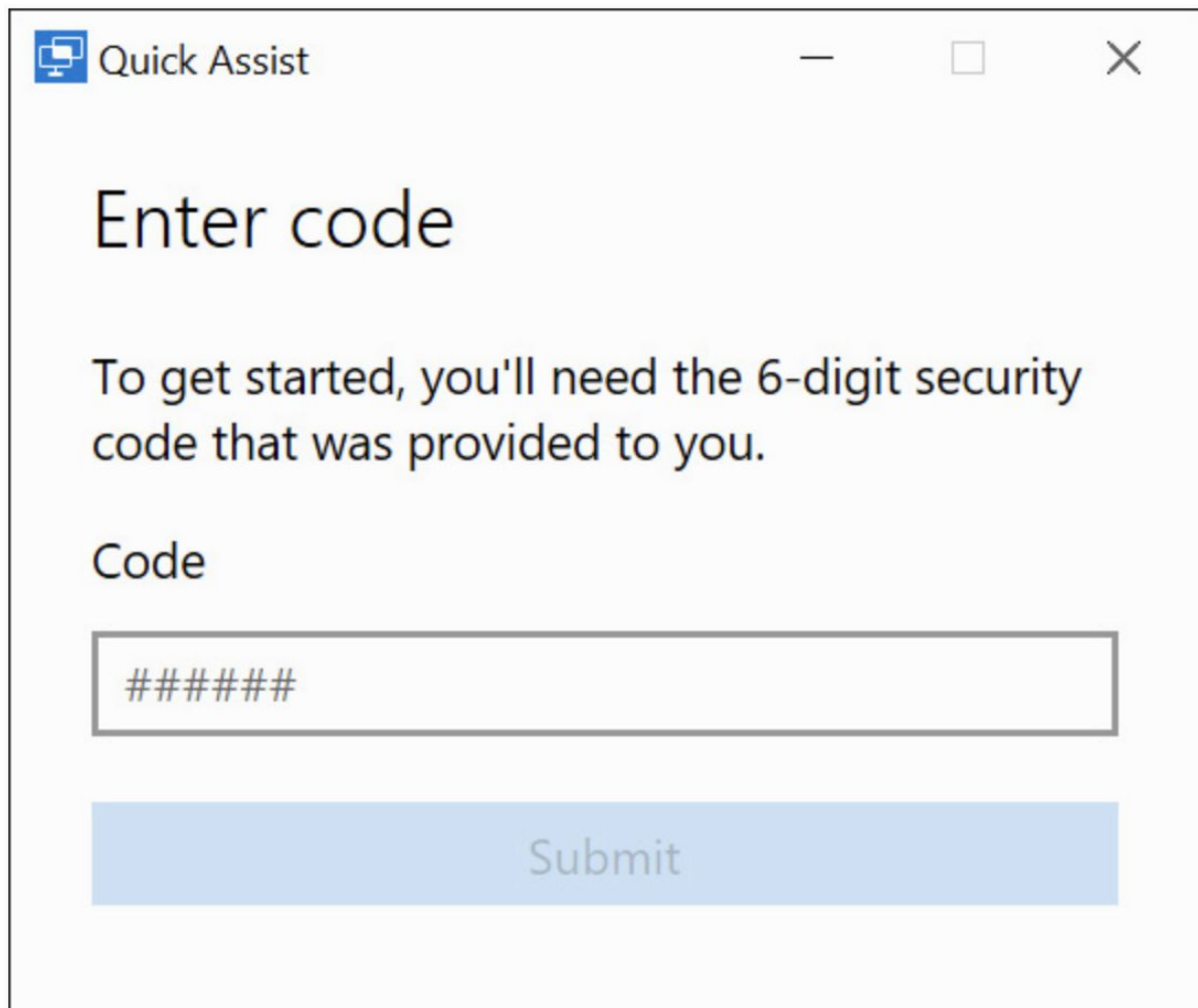


The user needing help clicks Get Assistance; the helper clicks Give Assistance.

The helper is then given a six-digit security code:



The user to be assisted sees the following:



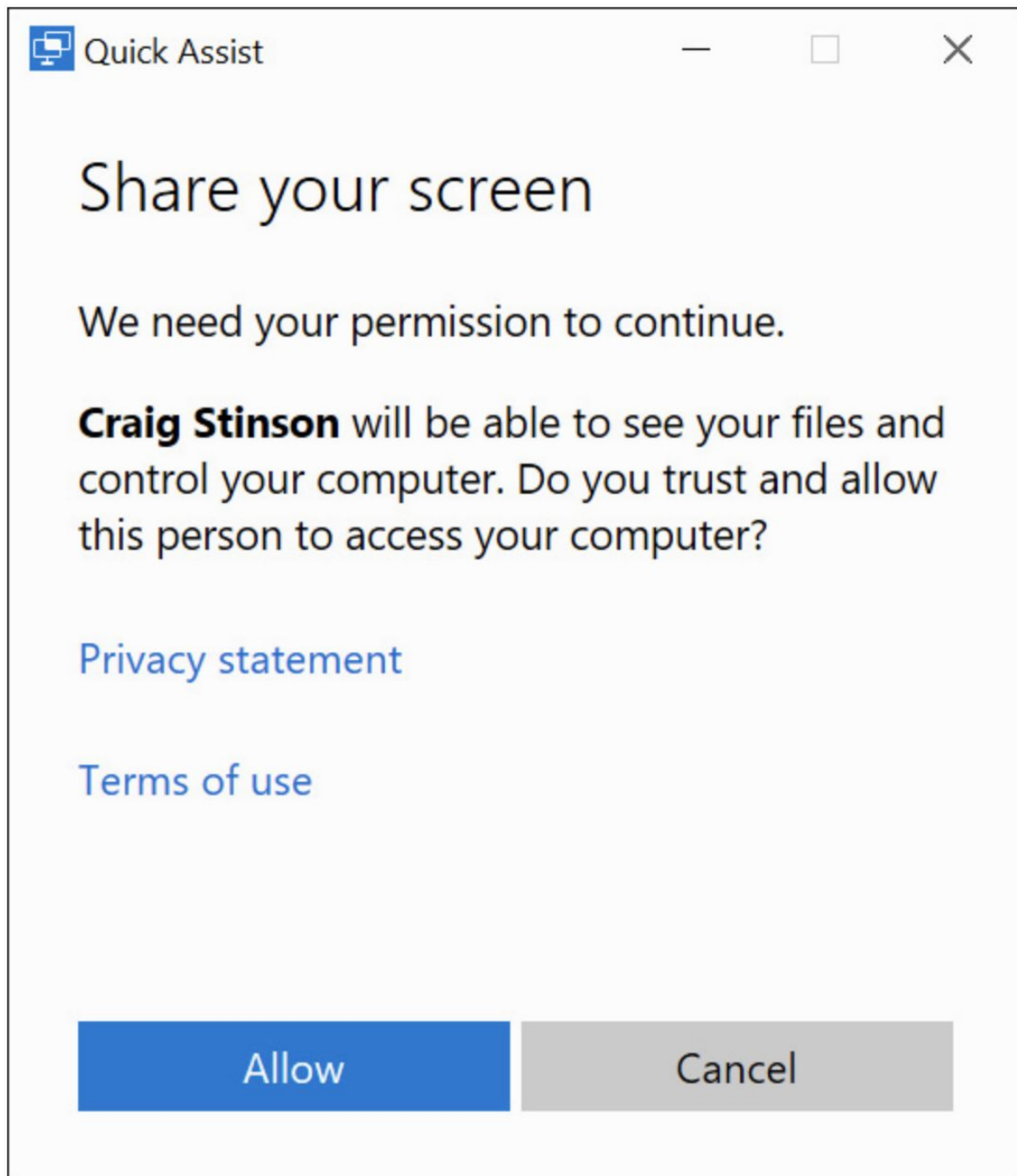
The image shows a Windows-style window titled "Quick Assist". Inside the window, the text "Enter code" is displayed in a large font. Below it, a message states: "To get started, you'll need the 6-digit security code that was provided to you." Underneath this message, the word "Code" is written. Below "Code" is a text input field containing six hash symbols (#####). At the bottom of the window is a large blue button labeled "Submit".

If you're the helper, you have 10 minutes to communicate the security code to your friend or colleague.

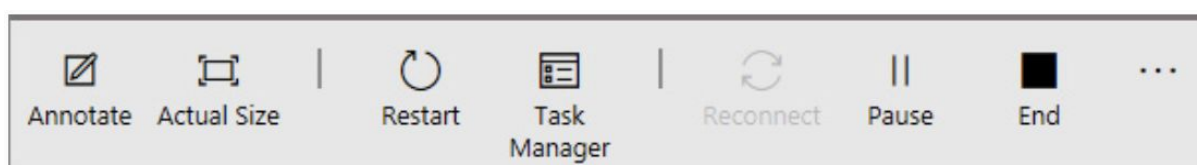
You can use the Send Email link to do this, but it's probably simpler to use the phone.

The two of you are likely to want to be in touch via phone in any case.

When the code has been delivered and entered, the user to be helped must give permission to make his system visible:



With permission granted, the helper sees the other system on his or her own display. A toolbar appears as well, at the top of the helper's screen:



From left to right, the buttons are as follows:

- Annotate opens a second toolbar with pen tools. The helper can use stylus or mouse to make freehand annotations on the other screen. These are erased at the end of the session.
- To accommodate systems of differing resolutions, the remote system is sized to fit the helper system. The Actual Size button switches from fitted to actual.
- The Restart button restarts the remote system. The connection between the two systems is reinstated after the remote system logs back on; no additional exchange of security code is required.
- The Task Manager button lets you display that invaluable utility on the remote system. Pressing Ctrl+Shift+Esc launches the helper's own Task Manager, not that of the remote computer.
- The Reconnect button is there to help you reestablish connection in the event the connection is broken.
- The Pause button, which changes to Resume when used, gives you a means of taking time out. Either party can pause. During the pause, the systems remain connected, but the remote system is not visible to the helper.
- The End button terminates the connection. Either party can also terminate by clicking the usual close button in the upper right corner of the screen.

- Exercises - 1. 3. 5. Troubleshooting -

Open the following Google Document that you have created in a previous sub-unit:

"1. 3. System maintenance and troubleshooting - Apellidos, Nombre"

being "Apellidos, Nombre" your Last Name and Name.

Inside this Google Document you are going to copy and answer all the "Exercises" of this sub-unit:

1. Go to the Control Panel and search for "Troubleshooting" until you see "Troubleshoot computer problems". Test the different trouble-shooters: Programs, Hardware and Sound, Network and Internet, System and Internet.
2. Go to Settings -> Privacy -> Feedback & diagnostics. Check your settings there. Click on "Give us feedback about the Feedback Hub survey notifications": a new app will be opened -> "Feedback Hub" ("Centro de opiniones" in Spanish). Select "Category:" "All categories". Search for a term (for example, "USB") and read some Feedback comments.
3. Type "reliability" in the Windows search box and then click the top result, "View reliability history". That opens "Reliability Monitor". Search for red "X" ("Failures") and click on them and open the details in order to check which problem happened.
4. Type "event" in the Windows search box and then click the top result, "Event Viewer". On the left open the "Windows Logs" and click on the different categories: Application, Security, Setup, System, Forwarded Events. On those categories, sort the events using the "Level" column, and look for "Error" (in red color) events: open some of them and read the messages inside those errors. On the right ("Actions") use the "Filter Current Log" to select in "Event Level" only "Error" and "Critical".
5. Close all the programs and documents of your virtual machine. In the Windows 10 search box search for "memory" and open the "Windows Memory Diagnostic" app. Select "Restart now and check for problems".
6. You are going to restart your virtual machine in "Safe Mode". In order to do so, firstly "Sign out" from your current Windows user. Secondly, in the sign in screen, click the "Shut down" button on the lower right corner. Click the "Shift" key and select "Restart" in the menu. In the next screen, select "Troubleshoot". In the next screen, select "Advanced options". In the next screen, select "Start-up Settings". In the next screen, click on the "Restart" button. In the next screen, named "Startup Settings", select the option "4) Enable Safe Mode". With Windows 10 started in "Safe Mode", open the "Device Manager" and "Event Viewer" to try to figure out where a possible problem would be.

7. Type “quick” in the Windows search box and then click on “Quick Assist”. You have to do this exercise with a partner: first “Get assistance” and later “Give assistance”. Use the “Annotate” feature to make freehand annotations on the other screen.