- 1. 3. 4. Backup, restore, and recovery -

In the Unabridged Edition of Murphy's Law, you'll find an entire chapter of corollaries that apply to computers in general and your important data files in particular.

Murphy says, "Anything that can go wrong will go wrong."

That's certainly true of storage devices, where it's not a matter of whether they'll fail but when.

When a hard drive fails catastrophically or a solid-state drive (SSD) suddenly becomes unreadable, any data files on that device are gone, as are your Microsoft Windows installation and all your apps and settings.

Even if your hardware never lets you down, human error can wreak havoc with data.

You can press the wrong key and inadvertently delete a group of files you meant to move.

If you're not paying attention, you might absent-mindedly click the wrong button in a dialog box, saving a new file using the same name as an old one, wiping out a week's worth of work in the process.

Some of the most important new features in Windows 10 let you recover quickly from either type of disaster.

We are going to explain how to use the backup tools included with Windows 10, which allow you to prepare for the inevitable day when you need to restore a lost file (or an entire drive's worth of files).

We also explain your options for resetting Windows when the operating system becomes damaged, for whatever reason.

And finally, we offer a guide to the venerable but still useful System Restore feature.

An overview of Windows 10 backup and recovery options

Through the years, the backup and recovery tools in Windows have evolved, but their fundamental purpose has not changed.

How well you execute your backup strategy will determine how easily you're able to get back to where you were after something goes wrong—or to start over with an absolutely clean state.

When you reach into the recovery toolkit, you're hoping to perform one of the following three operations:

- Full reset. If you're selling or giving away a PC or other device running Windows 10, you can reset it to a clean configuration, wiping personal files in preparation for the new owner. Some Windows users prefer this sort of clean install when they just want to get a fresh start, minus any cruft from previous installations.
- Recovery. The "stuff happens" category includes catastrophic hardware failure, malware infection, and system corruption, as well as performance or reliability problems that can't easily be identified with normal troubleshooting. The recovery process involves reinstalling Windows from a backup image or a recovery drive.
- File restore. When (not if) you accidentally delete or overwrite an important data file or (ouch) an entire folder, library, or drive, you can call on a built-in Windows 10 tool to bring back the missing data. You can also use this same feature to find and restore earlier versions of a saved file—an original, uncompressed digital photo, for example, or a Microsoft Word document that contains a section you deleted and now want to revisit.

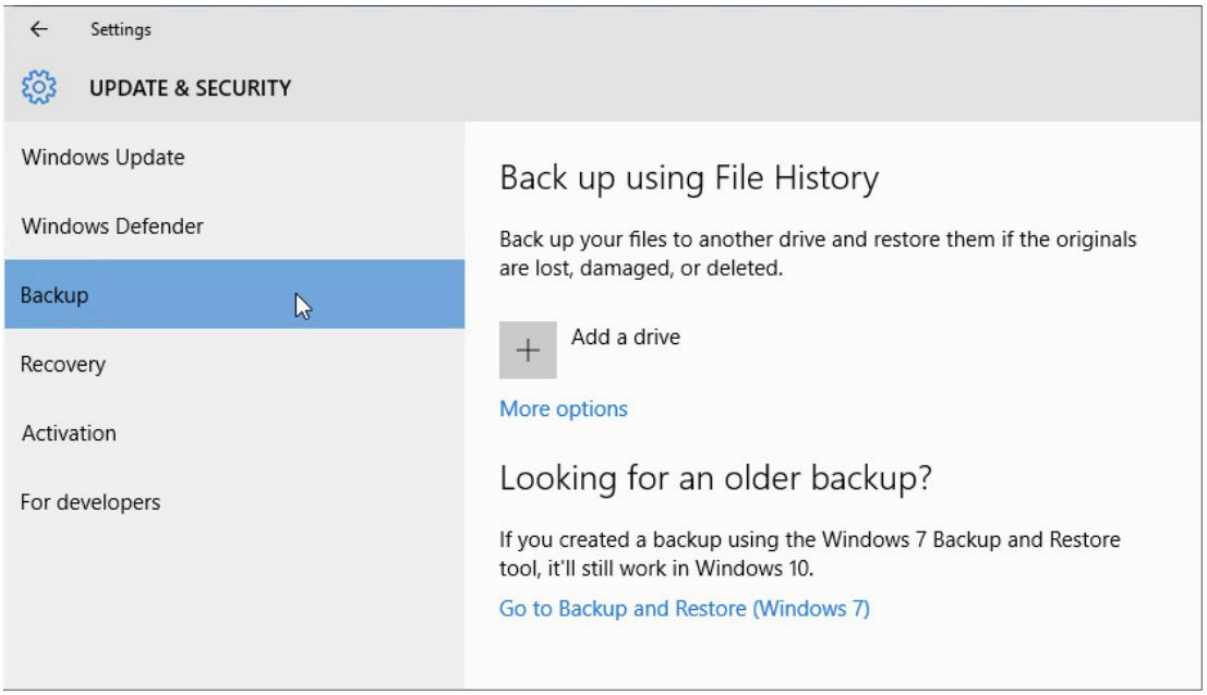
In Windows 10, the primary built-in tool for backing up files is called File History.

Its job is to save copies of your local files—every hour is the default frequency—so that you can find and restore your personal documents, pictures, and other data files when you need them.

File History has evolved since its introduction in Windows 8.

Still, it's designed to be simple and not full featured, which is why Windows 10 also includes the old-style Windows 7 Backup And Restore tool.

You'll find both backup solutions by opening Settings > Update & Security > Backup, as shown in the next picture:



Despite its advanced age, the Windows 7 backup tool can still do one impressive digital magic trick that its newer rivals can't: it can create an image of the system drive that can be restored to an exact copy of the original saved volume, complete with Windows, drivers and utilities, desktop programs, settings, and data files.

System image backups were once the gold standard of backup and are still a perfect way to capture a known good state for quick recovery.

The disadvantage of a full image backup is that it's fixed at a moment in time and doesn't capture files created, changed, or deleted since the image was created.

If your primary data files are located in the cloud or on a separate volume from the system drive, that might not be a problem.

Over the decades, the clean install has taken on almost magical properties among some Windows users.

This classic recovery option involves reinstalling Windows from installation media, installing custom drivers, rebuilding connections to network resources, restoring data files, reinstalling apps, and redoing individual preferences.

You can still follow that old-school routine if you're willing to spend the time and energy.

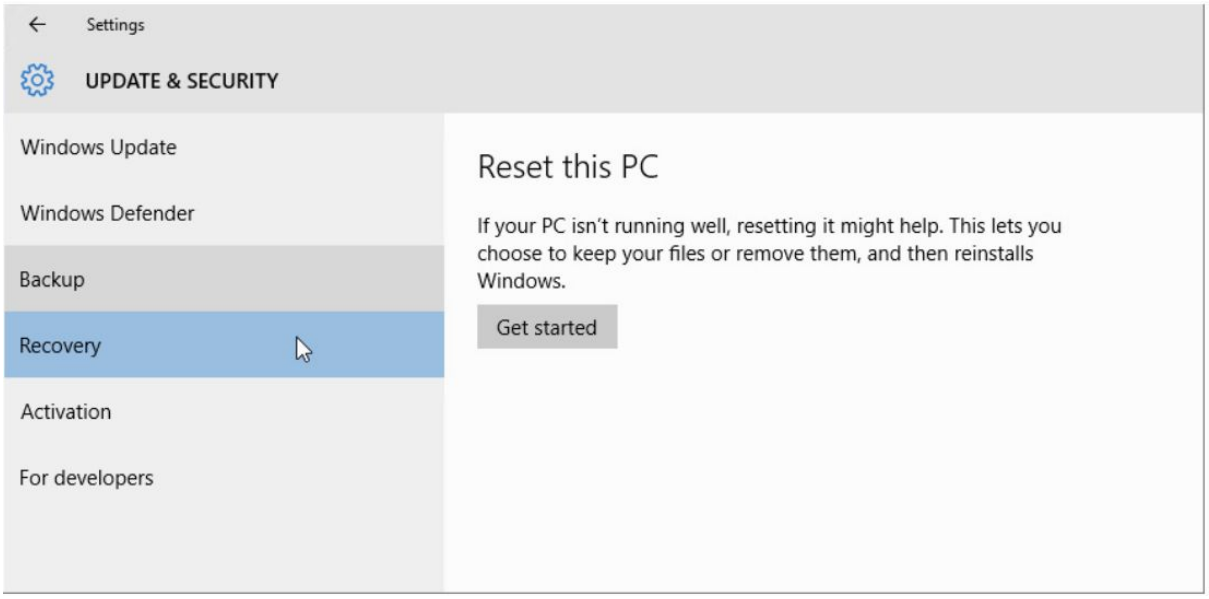
But there are faster, easier ways in Windows 10.

In Windows 8, Microsoft formally introduced a "push-button reset" feature with two options.

Windows 10 simplifies this feature under a single reset heading, which you can use to reinstall Windows with the option to keep or discard personal data files.

With this option, you can reset a misbehaving system on the fly, rolling back with relative ease to a clean, fully updated Windows 10 installation minus any third-party programs or drivers that might be causing problems.

You'll find the Reset This PC option on the Recovery page in Settings, which sits next to Backup in the Update & Security group:



Windows 10 also includes a built-in option to turn a USB flash drive into a bootable recovery drive.

Using this recovery drive, you can restore Windows, even after a complete system drive failure.

Integrating the cloud into your backup strategy

It's tempting to think of Microsoft OneDrive and other cloud-based storage services as a primary backup.

But that strategy is potentially dangerous as well.

Cloud services are generally reliable, but it's not out of the question that one might fail or be temporarily unavailable.

Moreover, online accounts can be compromised.

There are risks associated with using the cloud as your only backup medium.

And even when you think you have a backup, it might not be what you expect.

Your cloud backups of photos, for example, might be converted to a lower resolution than the original images, meaning that your only copy of a priceless photo is an inferior compressed version.

Having a complete archive of files backed up to the cloud does offer the reassurance that you can recover any or all those saved files in the event of an accident or natural disaster, such as a fire or flood, that wipes out your primary device and its separate local backup.

Given the ubiquity and relatively low cost of online storage services, in fact, it's probably prudent to keep copies of important files in two separate cloud-based services.

Just remember that those distant archives are not a replacement for comprehensive local backups on an external storage device or a networked PC.

Using File History to protect files and folders

Although you can delve into advanced settings if you dig deeply enough, File History is designed as a "set it and forget it" feature.

After you enable this backup application, it first copies all files in the backup location and then scans the file system at regular intervals (hourly, by default), looking for newly created files and changes to existing files.

Copies of each new or changed file are stored on a secondary drive, usually an external device.

You can browse the backed-up files by date and time—or search the entire history—and then restore any or all of those files to their original location or to a different folder.

But first, you have to go through a simple setup process.

Setting up File History

Although the File History feature is installed by default, it's not enabled until you designate a drive to serve as the backup destination.

This drive can be a second internal hard disk or an external storage device, such as an external hard drive, or a network location.

Caution!

Be sure you specify a File History volume that is on a separate physical drive from the one that contains the files you're backing up.

Windows will warn you, sternly, if you try to designate a separate volume on the same physical drive as your system drive.

The problem?

One sadly common cause of data loss is failure of the drive itself.

If the backups and original files are stored on the same drive, a failure wipes everything out.

Having backups on a separate physical drive allows them to remain independent.

To turn on File History for the first time, open Settings > Update & Security > Backup.

Click Add A Drive to scan for available File History drives.

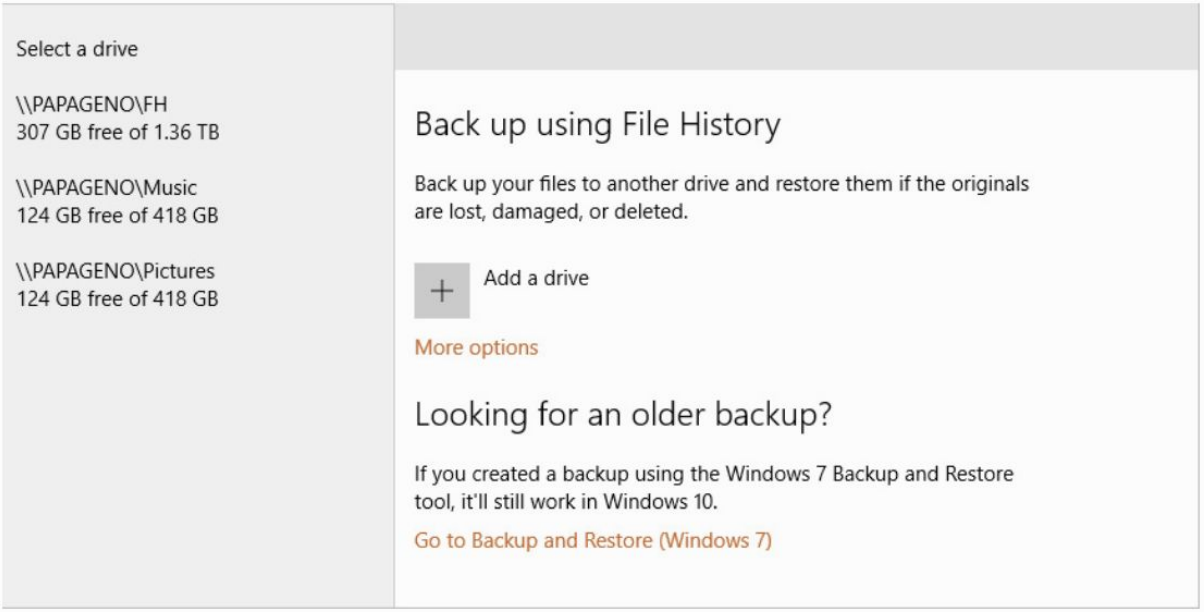
The File History wizard responds by showing you all available drives.

To add a list of network shares for which you have read/write permission, click Show All Network Locations.

This link appears after the list of available non-networked drives has been populated.

The following picture shows a system that has no attached drives but includes three network shares.

Selecting one of the available locations turns on the File History service and begins the backup process, with the backup frequency set to one hour.



When you first enable File History, it creates a full copy of all files in the locations you designated for backup.

That list contains either the default locations or your customized list.

The drive you designate as a File History drive must be either an internal or external hard drive (a category that includes SSDs).

Removable drives, such as USB flash drives, are not eligible.

The File History setup wizard will show you only eligible drives when you set up File History for the first time.

There's nothing complicated or proprietary about File History volumes:

- When you use an external drive, Windows creates a FileHistory folder, with a separate subfolder for each user. Thus, on a device that includes multiple user accounts, each user's files can be backed up separately.
- Within each user's private folder are separate subfolders, one for each device backed up. This folder arrangement allows you to use a single external drive to record File History backups on different devices.
- Each individual backup set includes two folders. The Configuration folder contains XML files and, if necessary, index files to allow speedier searches. The Data folder contains backed-up files, which are stored in a hierarchy that matches their original location.
- Backed-up files are not compressed. File names are the same as the original, with a date and time stamp appended (in parentheses) to distinguish different versions. As a result, you can browse a File History drive in File Explorer and use search tools to locate a file or folder without using the File History app.

Caution!

Files stored on a File History drive are not encrypted by default.

Anyone who has physical possession of the drive can freely read any files stored there.

If you're concerned about confidential information contained in an external File History drive, we recommend you encrypt the drive.

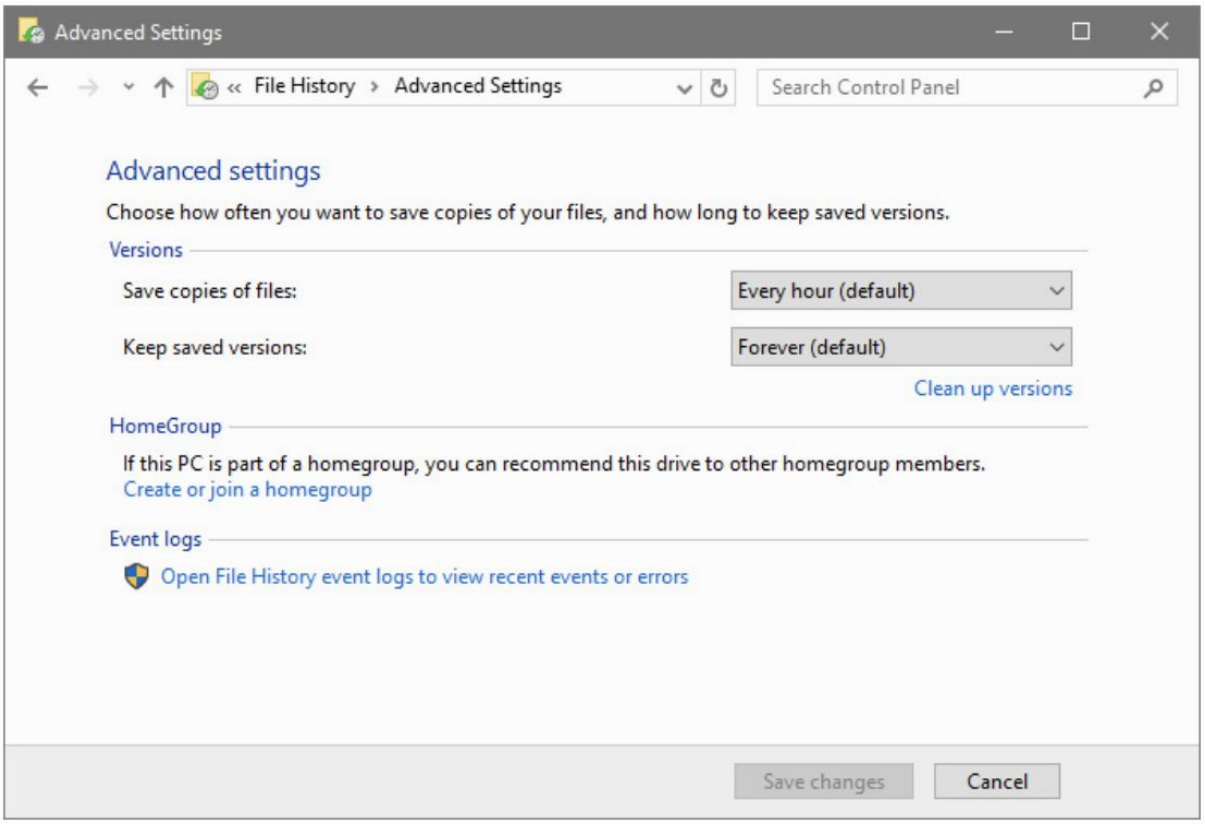
As an alternative, consider saving File History to a shared network folder for which you have appropriate permissions.

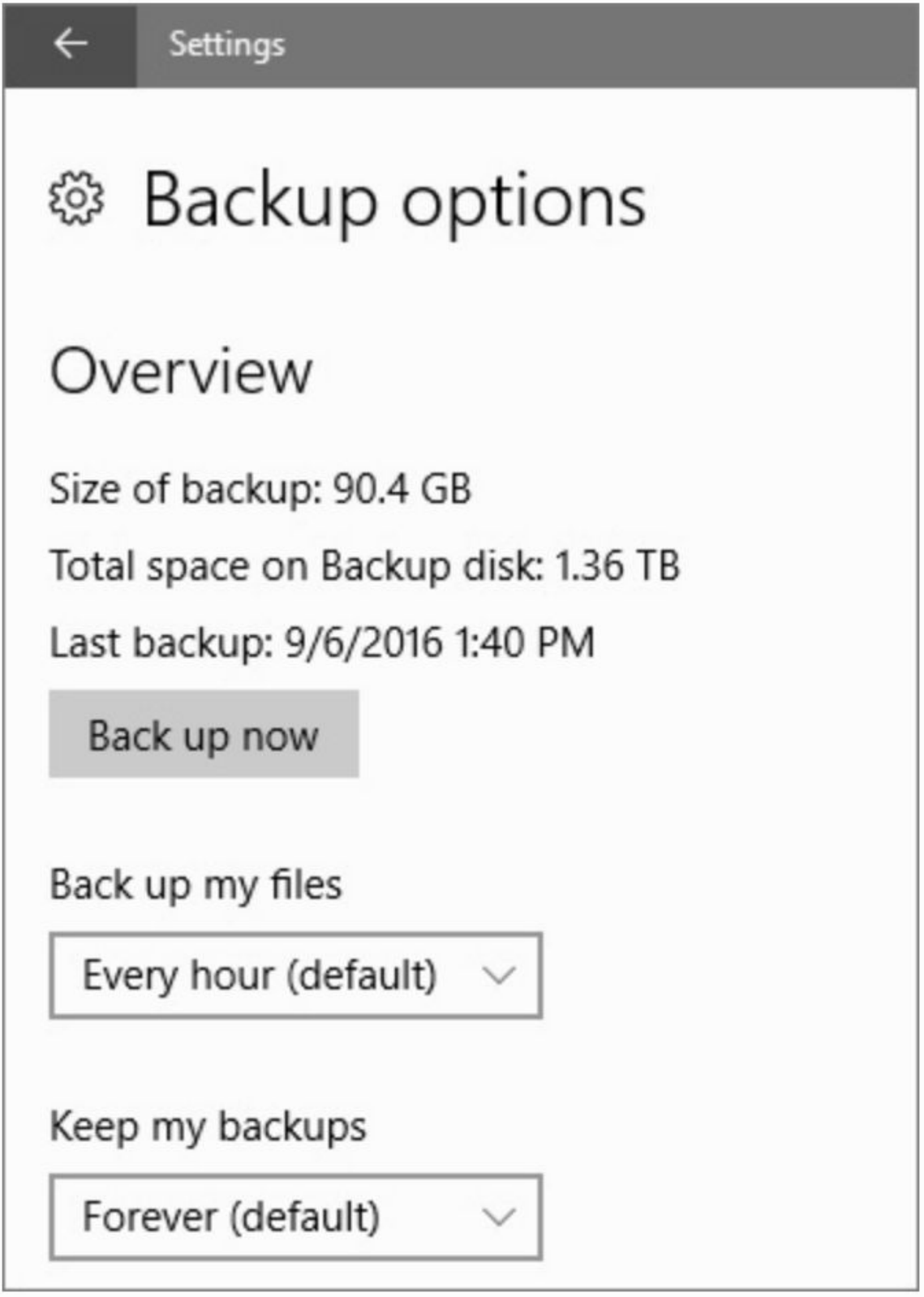
File History is yet another example of a feature caught in the transition from the classic Windows Control Panel to the new Settings app.

The overlap between old interface and new is more pronounced here than elsewhere.

From the old Control Panel (in File History, click Advanced Settings) or the new Settings app (on the Backup page, click More Options), you can change the backup interval and time period for saving backups.

The options, identical in effect but different in appearance, are shown here:


Advanced Settings
« File History › Advanced Settings
Search Control Panel
Advanced settings
Choose how often you want to save copies of your files, and how long to keep saved versions.
Versions
Save copies of files:
Every hour (default)
Keep saved versions:
Forever (default)
Clean up versions
HomeGroup
If this PC is part of a homegroup, you can recommend this drive to other homegroup members.
Create or join a homegroup
Event logs
Open File History event logs to view recent events or errors
Save changes
Cancel



By default, File History checks your designated drives and folders once an hour, saving copies of any new or changed files as part of the operation.

You can adjust this setting in either direction, choosing from nine intervals that range from every 10 minutes (if you really hate the idea of ever losing a saved file) to once daily.

File History backups are saved by default forever.

You receive a warning when your File History drive is full.

However, you can alter the Keep Saved Versions setting to 1, 3, 6, or 9 months or 1 or 2 years.

The “set it and forget it” Until Space Is Needed setting allows File History to automatically jettison old backups to make way for new ones when the drive is full.

The options in Settings and Control Panel overlap but aren’t identical.

For example, the options to share a File History drive with others in a homegroup and to quickly view File History event logs are available only in the Advanced Settings section of the classic Control Panel.

Some files are missing from File History backups

Because of the unique way File History organizes and names backed-up files, you might find that some files aren’t backed up properly.

This can happen, for example, if you append a version date and time to the name of a file, particularly if the file is deeply nested within multiple subfolders.

Those extra characters added to an already long path can cause the file name in the File History folder to exceed the maximum path limit of 260 characters.

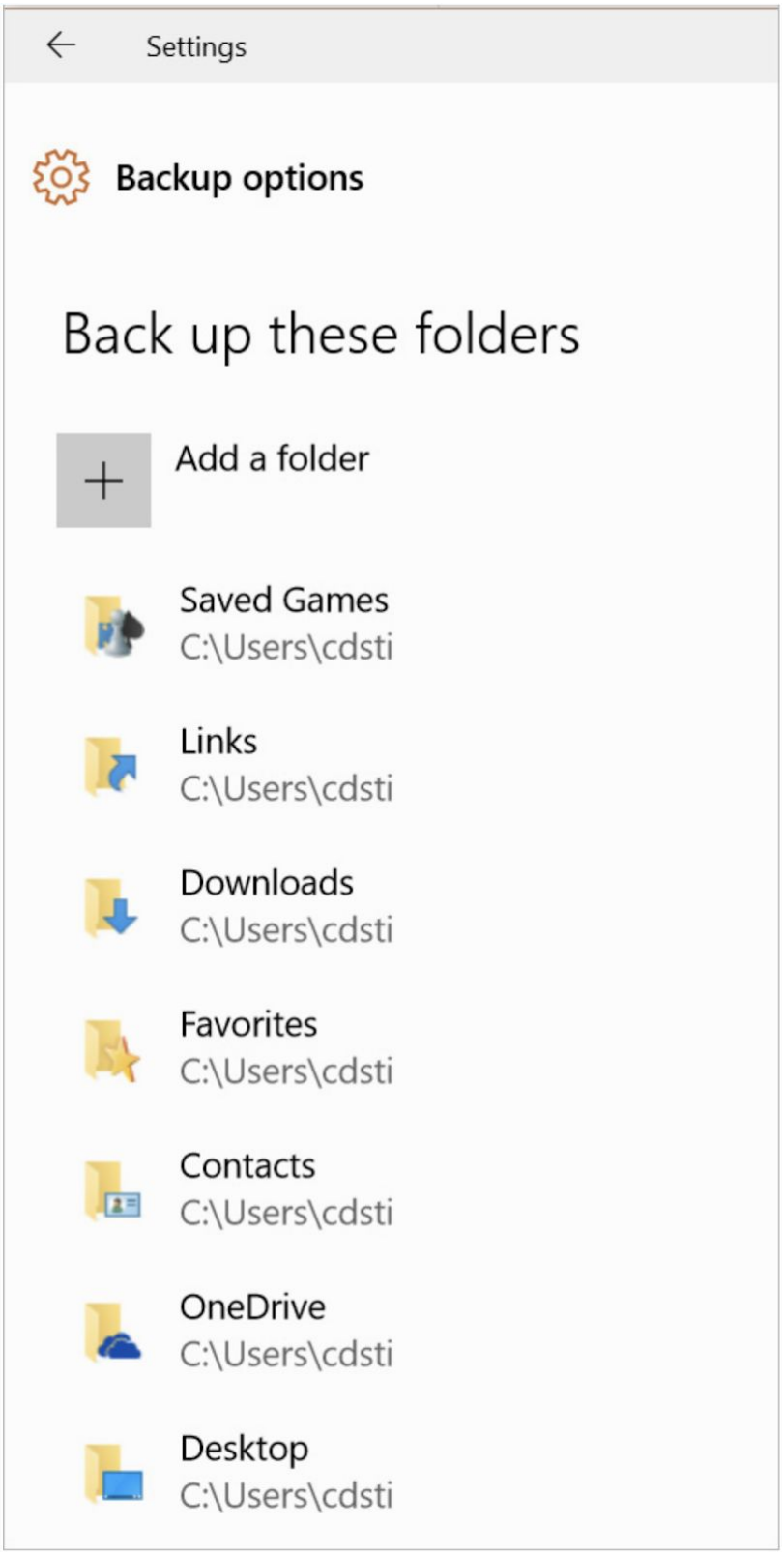
You can spot these errors easily in the File History event logs and resolve them by moving the original files or subfolders to a location with a path name that’s sufficiently shorter.

Choosing locations to back up

By default, File History backs up all folders in the current user profile (including those created by third-party apps) as well as the contents of local folders that have been added to custom libraries.

To manage the list of folders backed up by File History, open Settings > Update & Security > Backup > More Options.

Scroll down to view the folder list on the Backup Options page, as shown in the next image:

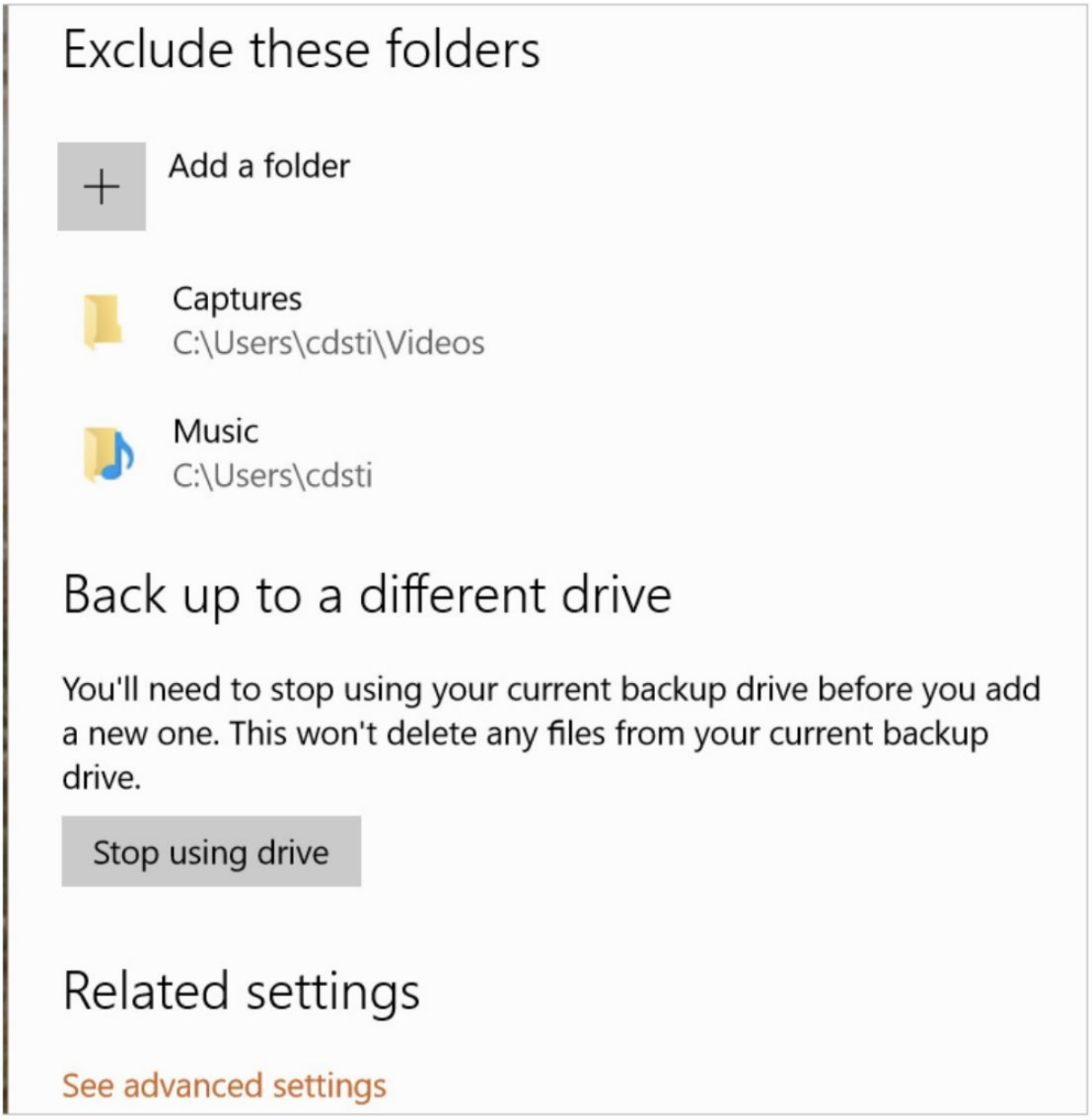


To remove any folder from this list, select its name and then click or tap Remove.

To add a folder from any local drive, click or tap Add A Folder and then select the location using the Select Folder dialog box.

Although the OneDrive folder is included by default in the list of folders to be backed up by File History, only files that are synced to the local drive are actually backed up.

At the end of the list is an Exclude These Folders option, shown in the next figure:



It's useful when you want to avoid filling your File History drive with large files that don't require backing up.

If you routinely put interesting but ephemeral video files into a subfolder in your Downloads folder, for example, you might choose to exclude that Videos subfolder completely from File History, while leaving the rest of the Downloads folder to be backed up.

A quicker way to exclude a folder from the backup list is simply to click it in the include list and then click the Remove button that appears:

Unfortunately, although this approach does remove folders from the list to be backed up, it does not add them to the list that appears under Exclude These Folders.

In most cases, the end result is the same.

But if the folder you remove happens to be a subfolder of an included folder, it will continue to be backed up unless you explicitly add it to the exclusion list.

When a File History drive fills up, you can either change the settings to remove old backed-up files and make room for new ones or swap in a new drive.

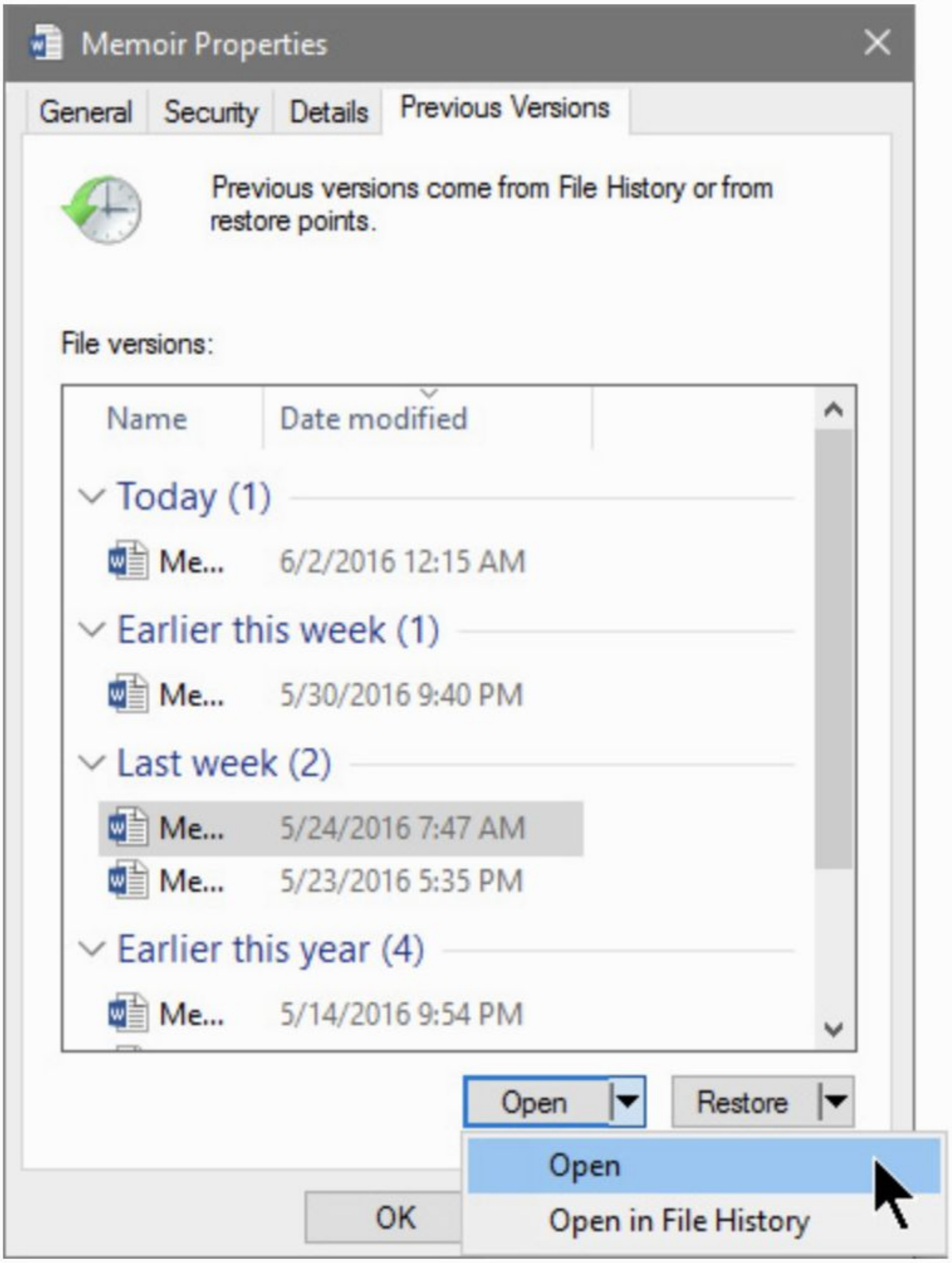
If you choose the latter option, click or tap the Stop Using Drive button on the Backup Options page, remove the old drive, and set up the new one.

Restoring files and folders

There are several ways to find and restore a backed-up file, folder, or drive.

From File Explorer, you can right-click an item, choose Properties, and then click the Previous Versions tab.

This sequence of steps generates a list of available backed-up versions sorted by date, as shown in the next picture:



The Open button at the bottom of the Previous Versions list gives you a choice of opening the selected item in its original application and opening it in the File History application; we'll say more about the File History application in a moment.

If you open the document in its original application, what you get is a read-only copy of the document.

That way, you won't accidentally overwrite the current version of the document with the older one you just opened.

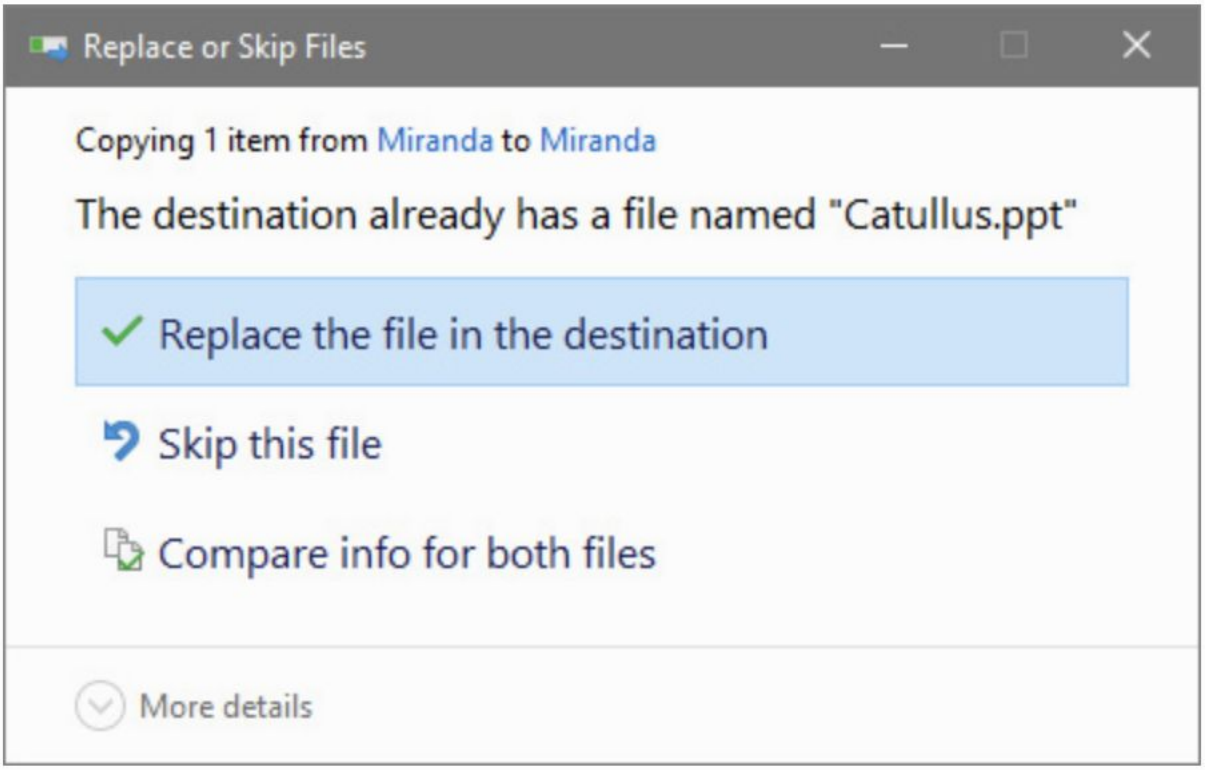
The Restore button, to the right of Open, also provides a pair of choices.

You can restore the document to its original location, or you can restore it to a new location of your choice.

If you restore to the original location and the original file still exists, you'll see the Replace Or Skip Files dialog box, which gives you an opportunity to change your mind or save the new file as a copy in the same location.

If you want to restore a copy without deleting the original, click Compare Info For Both Files and then select the check box for both the original file and the restored previous version.

The restored copy will have a number appended to the name to distinguish it from the original.



The File History app offers a distinctly different take on browsing backed-up files.

Although it resembles File Explorer in some respects, it adds a unique dimension—the ability to choose a set of saved files from a specific date and time to scan, scroll through, or search.

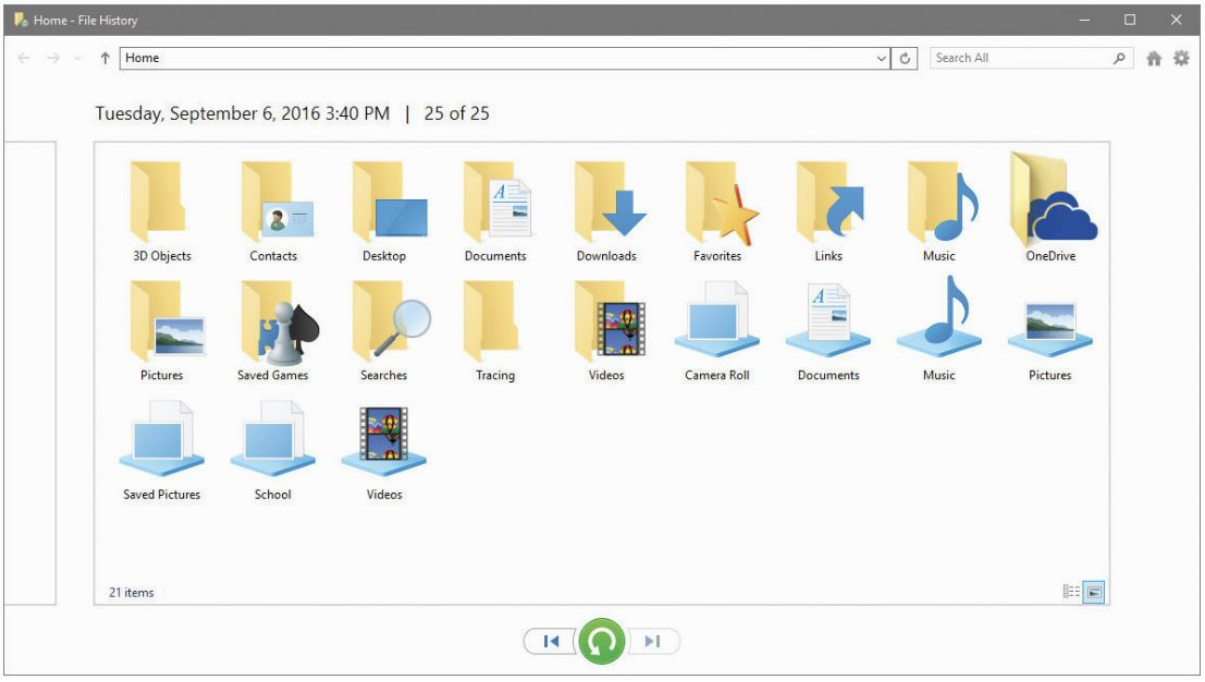
You can start the File History app in several ways:

- From the Settings app, look for Restore Files From A Current Backup, at the bottom of the Backup Options page.
- From File Explorer, select the file or folder you're interested in, and then click History, in the Open group of the ribbon's Home tab.

- From the Previous Versions tab in the Properties dialog box for a file, click Open In File History.
- Using the classic Control Panel, open File History and click Restore Personal Files in the links at the left of the settings.

The next image shows the File History app, which has an address bar, navigation controls, and a search box along the top, very much like File Explorer.

What's different are the time stamp (above the file browsing window) and three controls below the window that allow time control without the need for flux capacitors or other imaginary time-machine components.



The legend at the top of the window tells you the date and time of the currently displayed backup.

You can use controls at the bottom of the window to move between backups.

So, for example, to restore a file or folder you regret having deleted, you can move backward through the backups until you find one that includes the longed-for item and then restore it from there.

Within the backup window, you can open folders to see their contents.

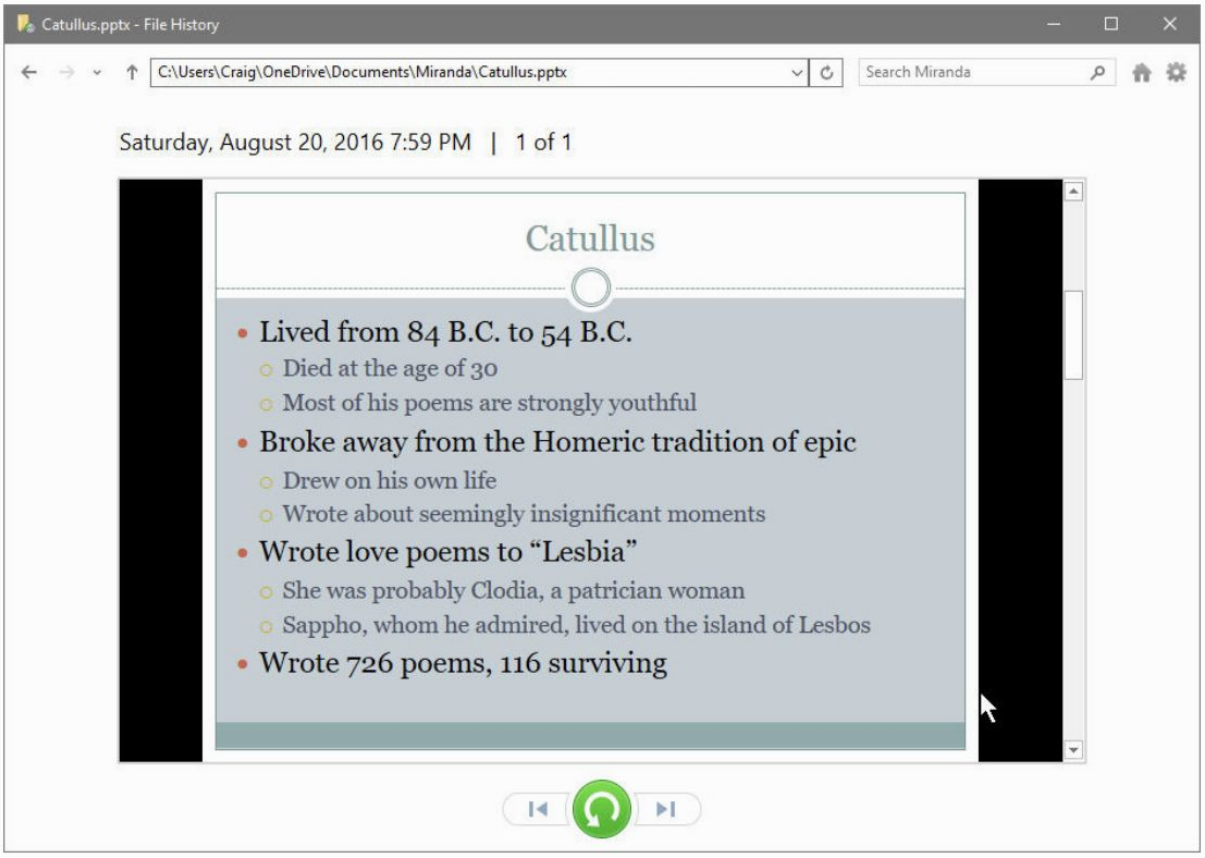
An address bar at the top, along with the invaluable up arrow beside it, lets you navigate as you might in File Explorer.

As with File Explorer, you can use the search box in the upper right to narrow the results by file type, keyword, or file contents.

Because file names rarely provide enough detail to determine whether a specific file is the one you're looking for, File History has a preview function.

Double-click a file to show its contents in the File History window.

The following figure shows one such preview of a PowerPoint presentation, with the full path and file name in the address bar and a scroll bar along the right for moving through the document in the preview window.

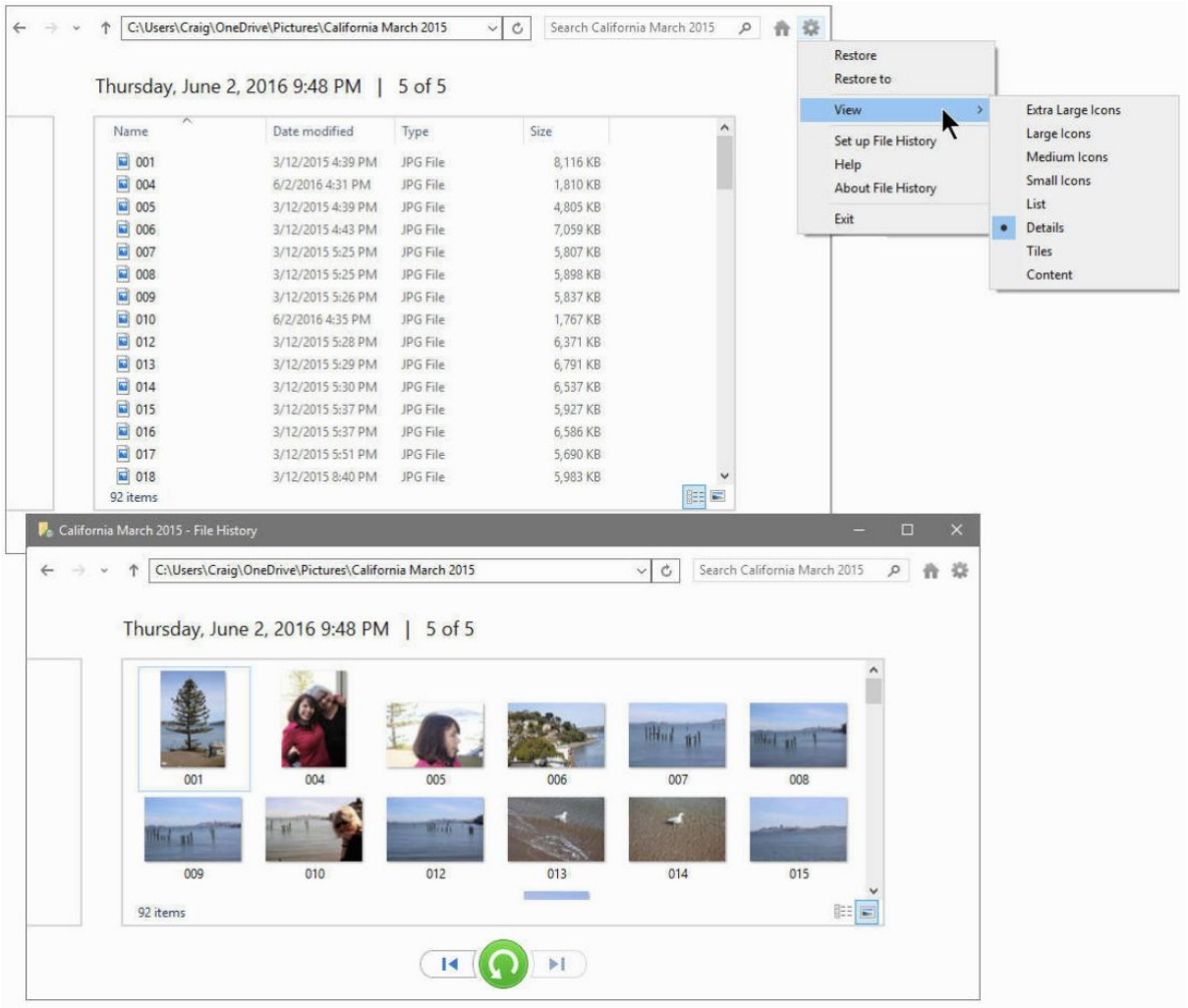


The option to restore entire folders is especially useful when you're switching to a new PC.

After you complete one last backup on your old PC, plug the File History drive into your new PC, and then use the big green Restore button to copy your backed-up files to corresponding locations on the new PC.

As with File Explorer, you can change the view of files in the File History browsing window.

By using the two shortcuts in the lower right corner, you can quickly switch to Details or Large Icons view, although you have a total of eight predefined views, available from the well-hidden shortcut menu shown in the next picture.



Recovering files and folders from an older backup

What if you need to recover documents from a File History drive that's no longer in use?

No problem.

In File Explorer, open the old File History drive and navigate to the files you need.

You might need to go through several layers of subfolders to get there.

Your previously backed-up files will have dates and times appended to their original names to help you decide which to resurrect.

Copy the files you want to restore, using a destination folder of your choosing; rename the files, if desired, to remove the date and time stamp.

Using the Reset option to recover from serious problems

One of the signature features of Windows 8 was a feature that turned out to be quietly revolutionary: a way for any user, even one without technical skills, to reset Windows to its original configuration using a Refresh or Reset command.

Windows 10 significantly refines that capability under a single Reset command.

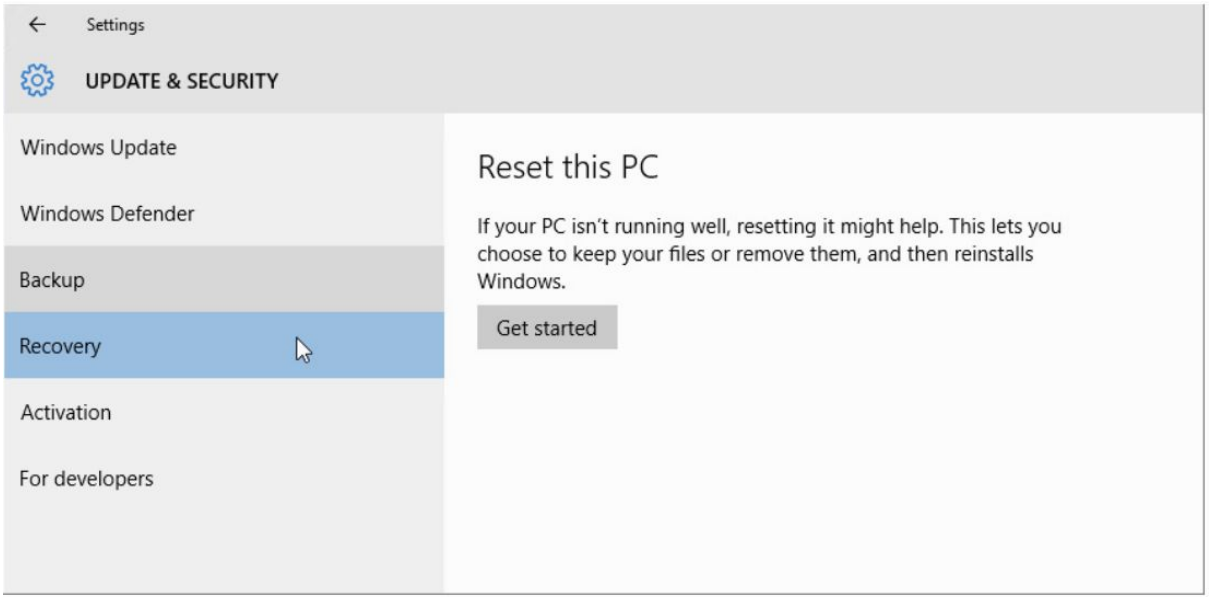
The most important change eliminates the need to have a disk-hogging OEM recovery image in a dedicated partition at the end of the hard drive.

In Windows 10, that recovery image and its associated partition are no longer required.

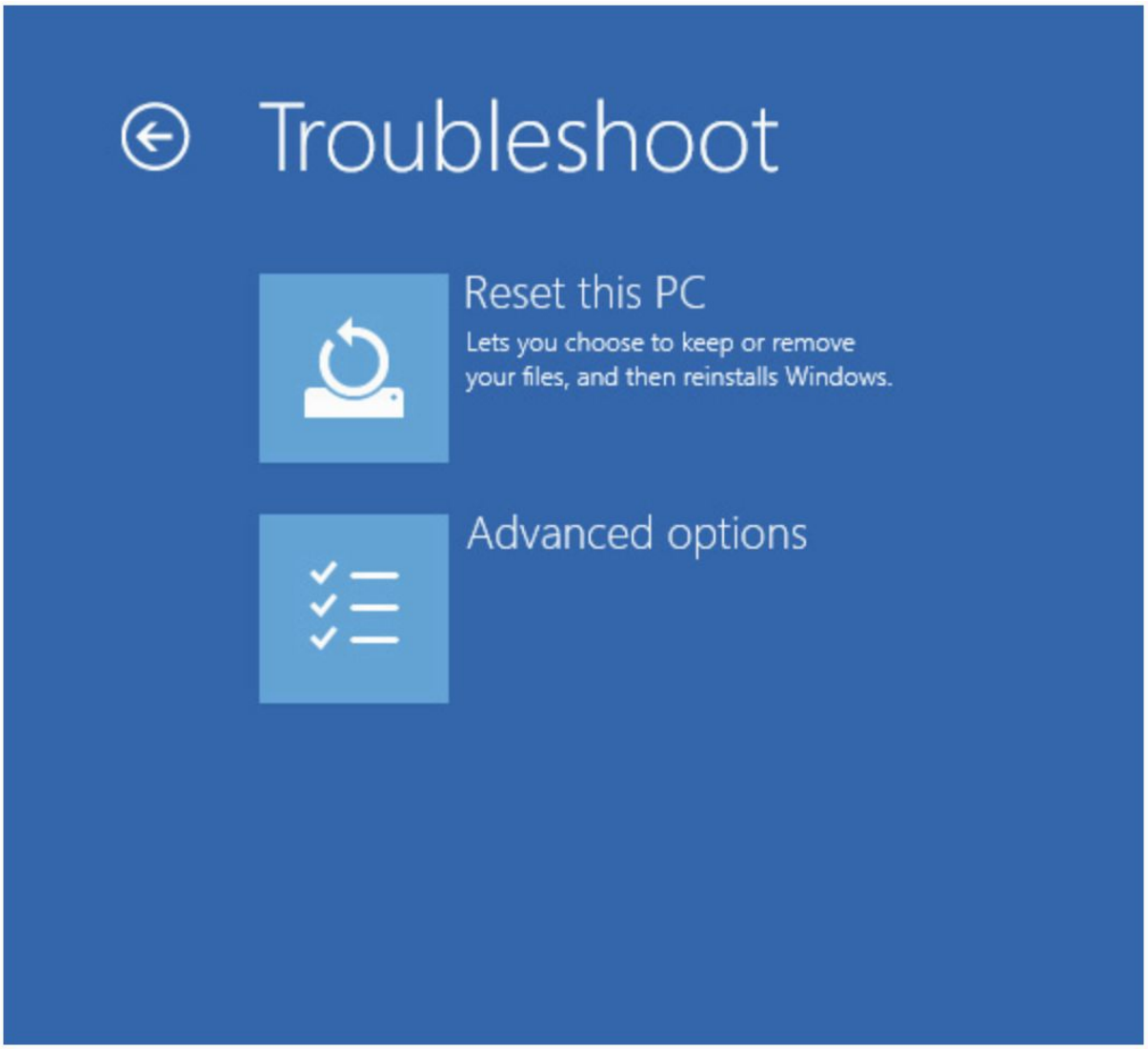
Instead, Windows 10 accomplishes recovery operations by rebuilding the operating system to a clean state using existing system files.

This push-button reset option has the same effect as a clean install, without the hassles of finding drivers and without wiping out potentially valuable data.

The Reset This PC option is at the top of the list on the Recovery page in Settings:



It's also the featured choice on the Troubleshoot menu when you restart in the Windows Recovery Environment, as shown in the next picture:



When you reset a PC, Windows 10 and its drivers are restored to the most recent rollup state.

The reset PC includes all updates except those installed in the last 28 days, a design that allows recovery to succeed when a freshly installed update is part of the problem.

For PCs sold with Windows 10 already installed, any customized settings and desktop programs installed by the manufacturer are restored with the Windows 10 reset.

These customizations are saved in a separate container, which is created as part of the OEM setup process.

All Windows apps included with Windows 10 by default (Photos, Weather, Groove Music, Mail, and Calendar, for example) are restored, along with any Windows apps that were added to the system by the OEM or as part of an enterprise deployment.

App updates are downloaded and reinstalled via the Store automatically after recovery.

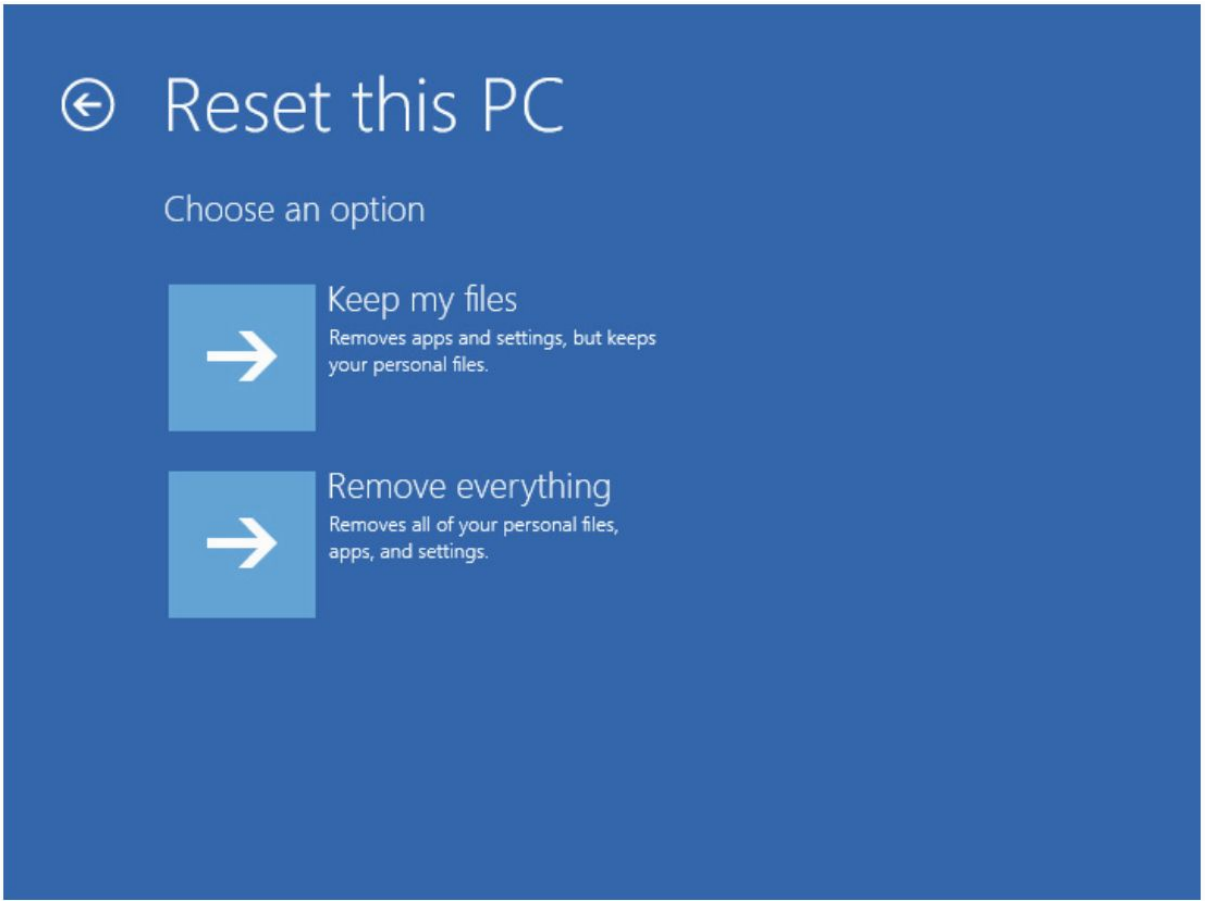
Windows desktop programs are not restored and must be manually reinstalled.

Likewise, any previously purchased Windows apps are discarded and must be reinstalled from the Store.

Resetting a PC isn't something you do accidentally.

The process involves multiple confirmations, with many opportunities to bail out if you get cold feet or realize that you need to do just one more backup before you irrevocably wipe the disk.

The first step offers you the option to keep your personal files or remove everything, as shown in the next picture:



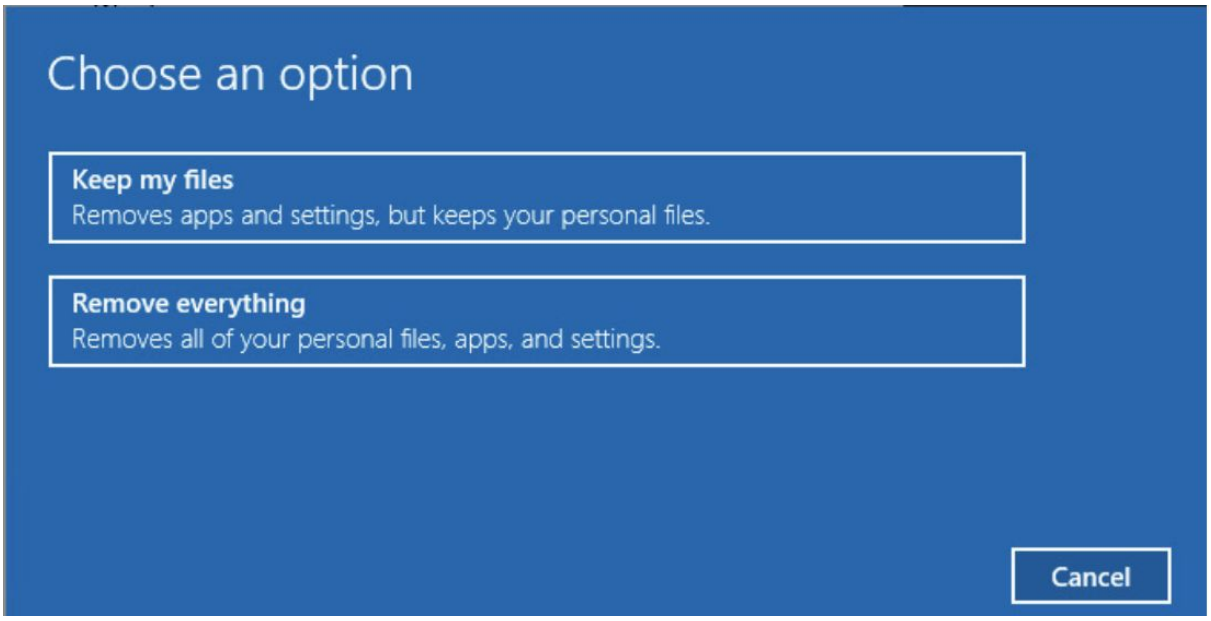
If you're performing the reset operation in preparation for selling or donating your computer, you'll probably want to use the second option.

Otherwise, choose the first option to retain your personal files.

If you're removing everything, the reset process also includes an option to scrub data from the drive so that it cannot easily be recovered using disk utilities.

As the explanatory text in the next figure makes clear, the Remove Files And Clean The Drive option can add hours to the process.

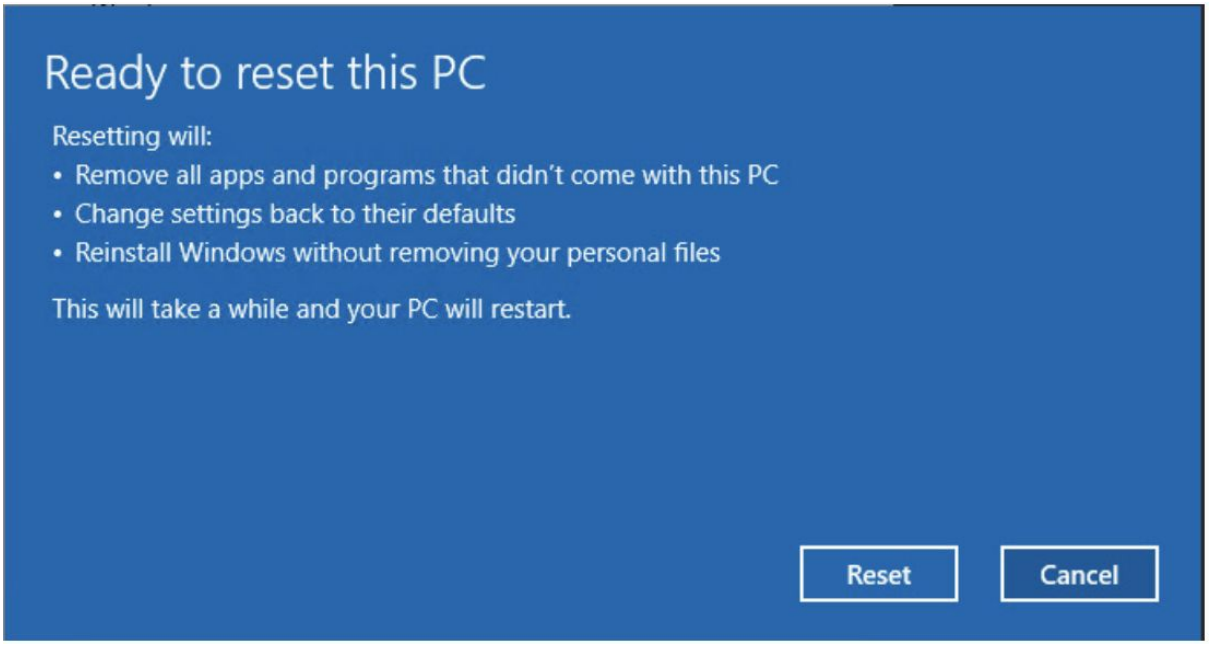
Note that this option, while thorough, is not certified to meet any government or industry standards for data removal.



If you made it this far through the process, you have only one more confirmation to get through.

That dialog box, shown in the next image, shows the choices you made, with one last Cancel option.

To plunge irreversibly ahead, click Reset:



The reset option is a tremendous time-saver, but it's not all-powerful.

Your attempts to reset Windows can be thwarted by a handful of scenarios:

- If operating system files have been heavily corrupted or infected by malware, the reset process will probably not work.
- If the problem is caused by a cumulative update that is more than 28 days old, the reset might not be able to avoid that problem.

- If a user chooses the wrong language during the out-of-box-experience (OOBE) phase on a single-language Windows version (typically sold in developing countries and regions), a complete reinstallation might be required.

If the reset option doesn't work, it might be time for a more drastic solution: reinstalling with the assistance of a recovery drive.

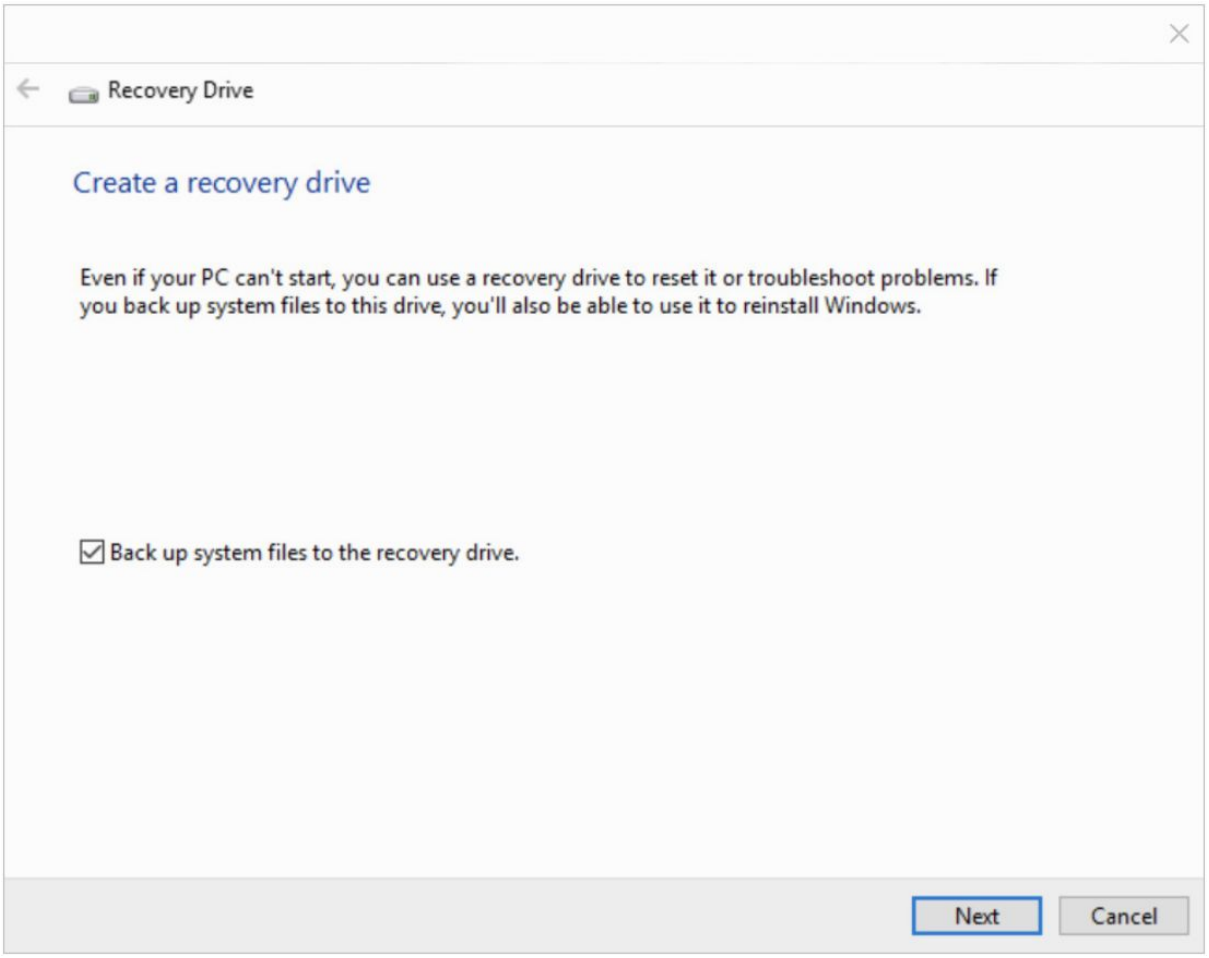
Creating and using a recovery drive

Windows 10 includes the capability to turn a USB flash drive into a recovery drive you can use to perform repairs or completely reinstall Windows.

The Recovery Media Creator creates a bootable drive that contains the Windows Recovery Environment.

To get there, open Control Panel, search for Recovery, and select Create A Recovery Drive.

If you select the Back Up System Files To The Recovery Drive check box, as shown in the following image, the utility creates a bootable drive that can be used to fully restore Windows, skipping most of the setup process.



To use the recovery drive, configure your PC so that you can boot from the USB flash drive.

That process, which is unique for many machines, might involve tapping a key or pressing a combination of buttons such as Power+Volume Up when restarting.

If you see the Recover From A Drive option when you restart, congratulations—the system has recognized your recovery drive and you are (fingers crossed) a few minutes away from being back in business.

The menu that appears when you start from a recovery drive allows you to repair a PC that has startup issues.

Choose Troubleshoot to get to the Advanced Options menu, where you can choose to perform a startup repair, use System Restore to undo a problematic change, or open a Command Prompt window to use system tools such as DiskPart from the command line.

Creating and restoring a system image backup

We recommend the Windows Backup program for the one task it does exceptionally well: use it to make a system image backup that can re-create a complete PC configuration, using a single drive or multiple drives.

Restoring that system image creates a perfect copy of the system configuration as it existed on the day that system image was captured.

You don't need to install, update, and activate Windows; reinstall all your applications; and then configure your applications to work the way you like.

Instead, you boot into the Windows Recovery Environment, choose an image file to restore, and then complete the process by restoring from your latest file backup, which is likely to be more recent than the image.

The image files that Windows Backup creates are largely hardware independent, which means that—with some limitations—you can restore your backup image to a new computer of a different brand and type.

Just be prepared to jump through some activation hoops on the new PC.

Use a system image to save your custom configuration

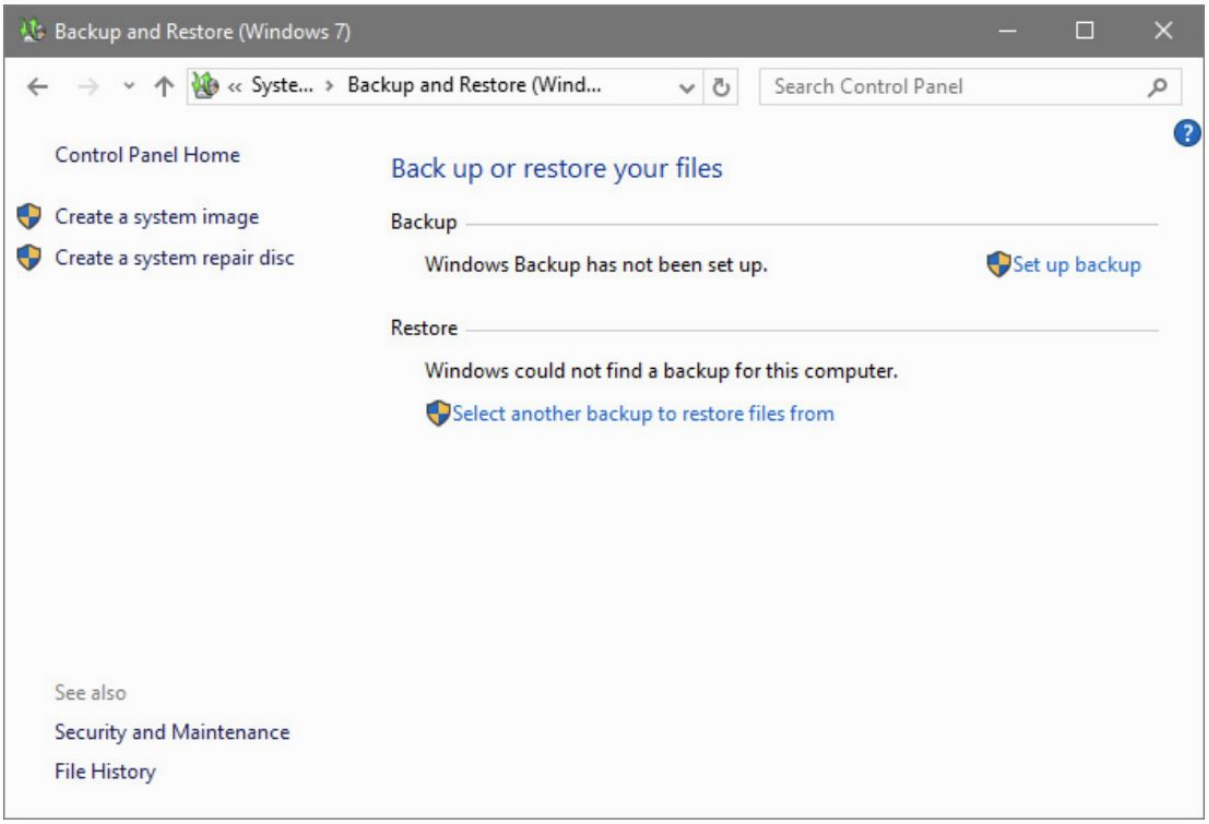
The single greatest use for a system image backup is to clean up an OEM configuration, leaving Windows intact, removing unwanted software, and installing your favorite apps.

Being able to return to a baseline configuration quickly is a trick that IT pros learned long ago as a way of deploying Windows in large organizations.

By mastering the system image backup feature, you can accomplish the same result even in an environment with a few PCs instead of a thousand.

Creating a system image backup

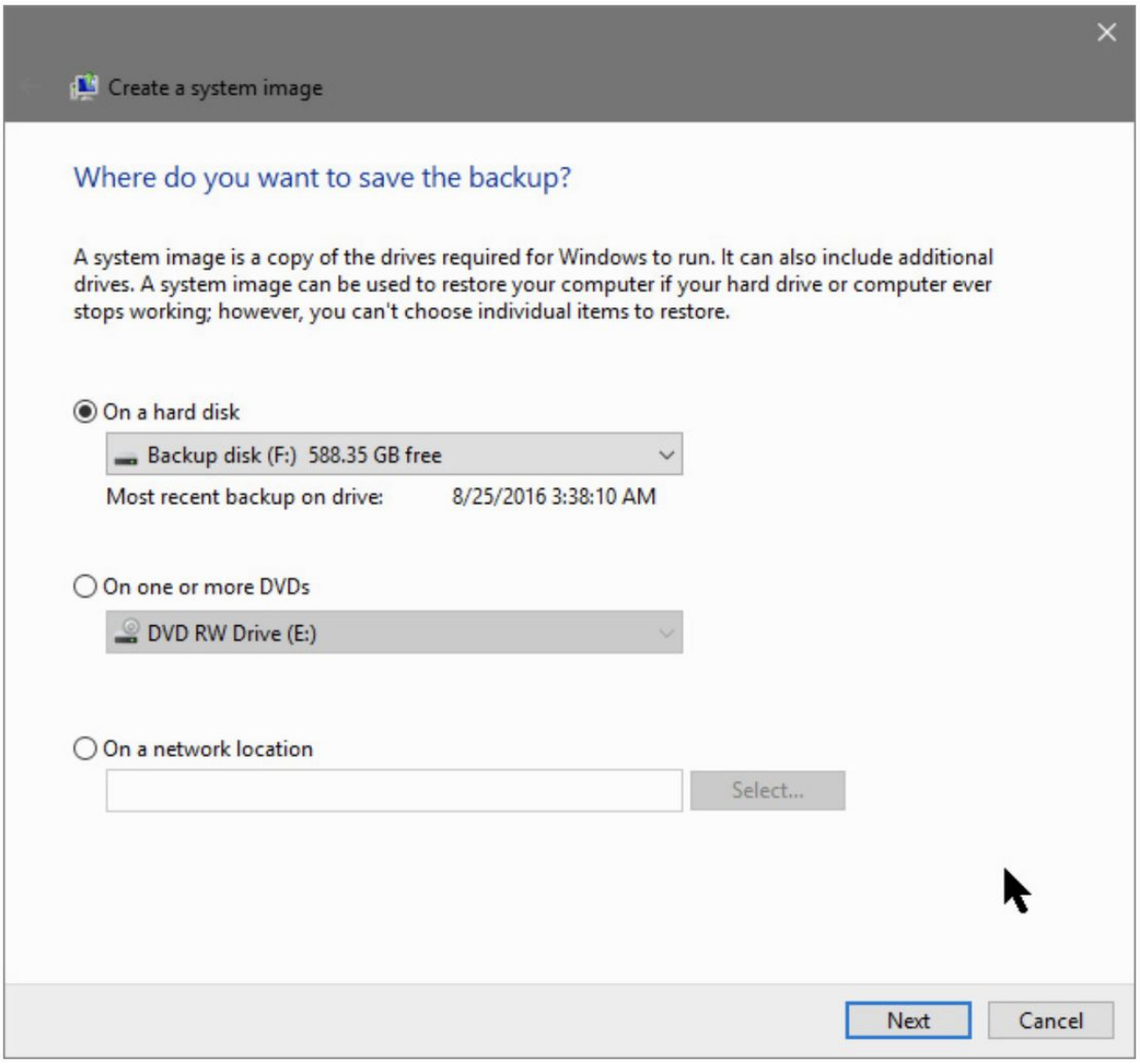
Type "backup" in the search box to find the Windows 7 Backup And Restore (Windows 7) tool, shown in the next picture:



Ignore the options in the center of that window, and instead click the "Create A System Image" link at the left side of the window.

That opens the efficient "Create A System Image" wizard.

The first step asks you to define a destination for your system image, as shown in the next image:



The ideal destination for a system image backup is a local hard disk, internal or external.

If the Windows Backup program detects a drive that qualifies, it suggests that destination in the list of hard disks at the top of the dialog box.

The second option lets you choose a DVD writer as the target for the backup operation.

You'll need to supply two, three, and maybe more blank discs to store the image backup.

Although this option might have made sense in a bygone era, it's downright quaint today.

Most new PCs don't even include a DVD drive, making backups stored on that media inconvenient at best and potentially useless.

Even when a DVD drive is available, a single corrupted disc in the series can ruin the whole backup.

If you try to choose a removable drive that is not a hard drive, such as a USB flash drive or SD card, Windows Backup will return this error message: “The drive is not a valid backup location.”

In its conventional backup role, Windows Backup can save data files on just about any storage medium.

System image backups, however, must be saved on a hard disk, a DVD, or a network location.

When you create a system image backup, the resulting image file stores the complete contents of all selected drives during its first backup.

If the backup target is a local (internal or external) hard drive, subsequent backup operations store only new and changed data.

Therefore, the subsequent, incremental backup operation typically runs much faster, depending on how much data has been changed or added since the previous image backup operation.

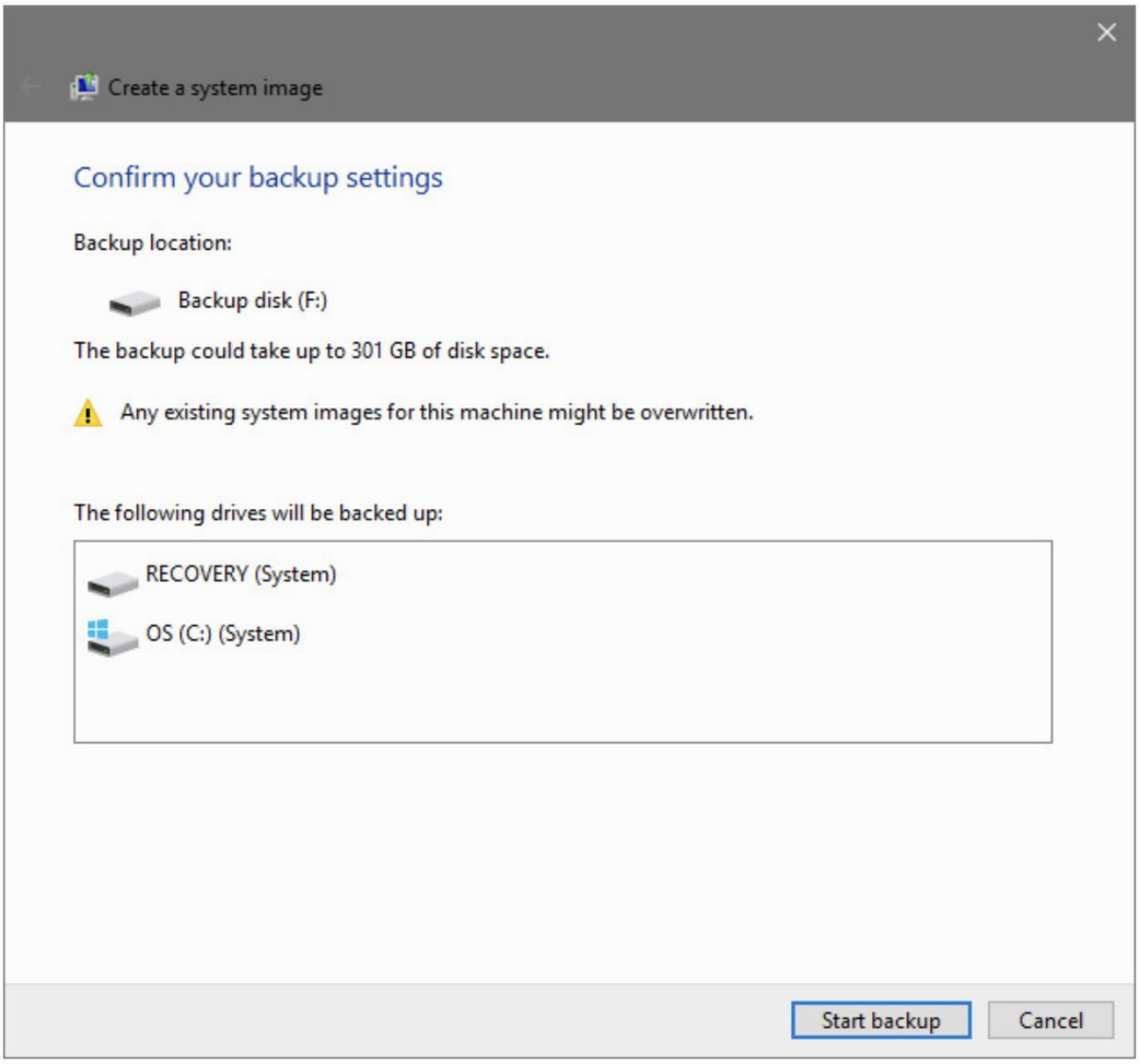
If you choose a shared network folder as the backup destination, you can save only one image backup.

Any subsequent image backup wipes out the previous image backup.

If you have multiple hard drives, Windows displays a dialog box like the one shown in the following figure, in which you choose the volumes you want to include in the backup.

By default, any volume that contains Windows system files is selected.

If other drives are available, you can optionally choose to include them in the image backup as well.



The disk space requirements for an image-based backup can be substantial, especially on a well-used system that includes lots of user data files.

Windows Backup estimates the amount of disk space the image will use (as shown in the previous image) and will warn you if the destination you choose doesn't have sufficient free disk space.

After you confirm your settings, click Start Backup to begin the process of building and saving your image.

System images are stored in virtual hard disk (.vhd) format.

Although the data is not compressed, it is compact because the image file does not include the hard drive's unused space and some other unnecessary files, such as hibernation files, page files, and restore points.

Incremental system image backups on a local drive are not written to a separate folder.

Instead, new and updated files (actually, the changed blocks in those files) are written to the same .vhd file.

The older blocks are stored as shadow copies in the .vhd file, allowing you to restore any previous version.

The final step of the image backup process offers to help you create a system repair disc on a writable CD or DVD.

This option might be useful for an older PC, but it's redundant if you already created a recovery drive as described in the previous section.

Save multiple image backups on a network

If you specify a shared network folder as the destination for an image backup, beware of the consequences if you try to reuse that location for a subsequent backup of the same computer.

If the backup operation fails for any reason, the older backup will be overwritten, but the newer backup will not be usable.

In other words, you'll have no backup.

You can avoid this risk by creating a new subfolder in the shared network folder to hold each new image backup.

The disadvantage, of course, is that each image file will occupy as much space as the original disk, unlike an incremental image backup on an external hard drive, which stores only the changed data.

Restoring a system image backup

The system image capabilities in Windows Backup are intended for creating an emergency recovery kit for a single PC.

In that role, they function exceptionally well.

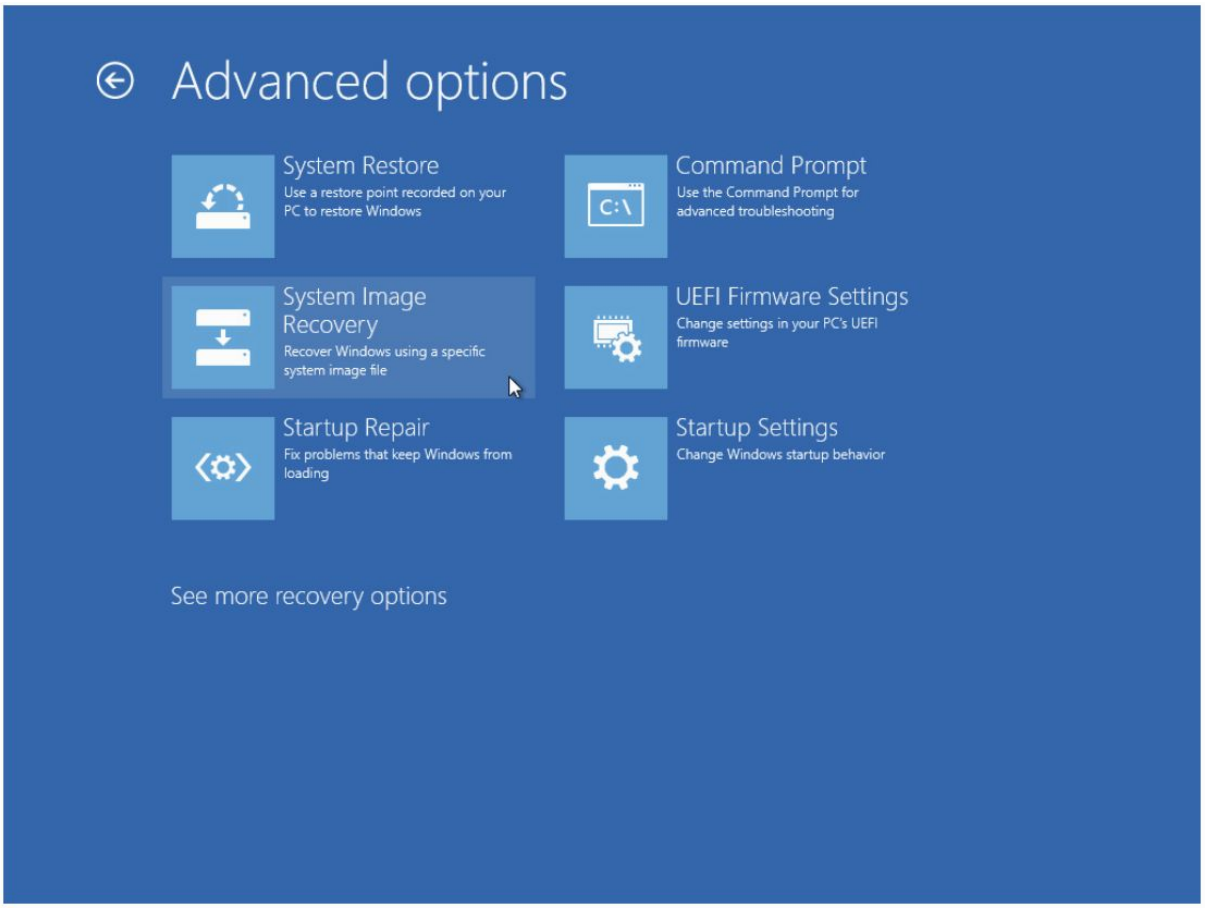
If your hard drive fails catastrophically, or if you want to wipe your existing Windows installation and start with a clean custom image you created a few weeks or months ago, you've come to the right place.

Your options (and potential gotchas) become more complex if you want to use these basic image backup and restore tools to work with a complex set of physical disks and partitions, especially if the disk layout has changed from the time you created the original image.

We assume you created an image backup of your system disk and want to restore it to a system that is essentially the same (in terms of hardware and disk layout) as the one you started with.

In that case, you can restart your computer using a recovery drive or a Windows 10 installation drive and then choose the "Repair Your Computer" option.

Choose Advanced Options and then select System Image Recovery, as shown in the next picture:



If the backup deities are smiling, you should see a dialog box proposing the most recent available system image backup.

If you're restoring the most recent image backup to the same system on which it was originally created and the backup is stored on an external hard drive attached to the computer, your job is easy.

Verify that the date and time and other details of the image match the one you want to restore, and then click Next to continue.

If the image file you're planning to restore from is on a network share or if you want to use a different image, choose Select A System Image and then click Next.

You'll see a dialog box that lists additional image files available on local drives.

Select the correct file, and click Next to select an image created on a specific date if more than one is available.

If the image file you're looking for is in a shared network folder, click the Advanced button and then click Search For A System Image On The Network.

Enter the network location that contains your saved image, along with a user name and password that have authorized access to that location.

Restoring an image backup completely replaces the current contents of each volume in the image file.

The restore program offers to format the disk or disks to which it is restoring files before it begins the restore process; if you have multiple drives or volumes and you're nervous about wiping out valuable data files, it offers an option to exclude certain disks from formatting.

The important point to recognize about restoring a system image is that it replaces the current contents of system volumes with the exact contents that existed at the time of the image backup you select.

That means your Windows system files and registry will be returned to healthy (provided the system was in good shape when you performed your most recent backup and that no hardware-related issues have cropped up since then).

Whatever programs were installed when you backed up your system will be restored entirely.

All other files on the restored disk, including your documents, will also be returned to their prior states, and any changes made after your most recent backup will be lost.

The main hardware limitation for restoring a system image backup is that the target computer must have at least as many hard drives as the source system, and each drive must be at least as big as its corresponding drive in the source system.

This means, for example, that you can't restore a system image from a system that has a 500-GB hard drive to a system with a 256-GB SSD, even if the original system used far less than 256 GB of drive space.

Keep in mind also that on a system with multiple hard drives, the BIOS determines which one is the bootable drive, and this is the one on which Windows will restore the image of your system volume.

You have no choice in the matter, aside from reconnecting the drives or, if your BIOS permits it, selecting a different bootable drive.

If your new computer meets the space requirements, restoring a system image should work.

This is true even when the source and target computers use different disk controllers.

Similarly, other differences—such as different graphics cards, audio cards, processors, and so on—shouldn't prevent you from restoring a system image to a different computer, because hardware drivers are isolated from the rest of the image information and are rebuilt as part of the restore process.

You might need to reactivate Windows because of hardware changes.

Caution!

If you keep your documents on the same volume as your system files, restoring a system image is likely to entail the loss of recent work—unless, of course, you have an up-to-date file backup or you have the good fortune to have made an image backup almost immediately before your current troubles began.

The same is true if you save documents on a volume separate from your system files but have included that data volume in your image backup.

If you have documents that have not been backed up, you can avoid losing recent work by copying them to a disk that will not be affected by the restore process—a USB flash drive, for example, or some other form of removable media.

You can use the Command Prompt option in the Windows Recovery Environment to copy these documents.

If you do have a recent file backup, you can restore files after you restore the image backup and your system is running again.

Your backup folders are “empty”

If you use File Explorer to browse to the folder containing your system image backup, when you rest the mouse pointer over a folder name, the pop-up tip might identify it as an “Empty folder.”

Alarmed, you right-click the folder and choose Properties, only to find that the folder apparently contains 0 bytes, 0 files, and 0 folders.

Don’t worry.

This is the normal condition when your backups are stored on an NTFS volume because, by default, only the System user account has permission to view the files.

That’s a reasonable security and reliability precaution, which prevents you or another user from inadvertently deleting a key backup file.

If you’re confident in your ability to work safely with backup files in their native format, the solution is simple: double-click the folder name.

Follow the prompts, including a User Account Control (UAC) consent dialog box, to permanently add your user account to the folder’s permissions list, giving you Full Control access to the folder.

Configuring system protection options

The System Restore feature has been part of Windows since the turn of the twenty-first century.

It’s a relatively minor part of the recovery toolkit now, but it can be useful for quickly undoing recent changes that introduced instability.

When System Restore is enabled, the Volume Shadow Copy service takes occasional snapshots of designated local storage volumes.

These snapshots occur before Windows Update installs new updates and when supported software installers run.

You can also create snapshots manually—a sensible precaution before you make system-level changes.

System Restore snapshots take note of differences in the details of your system configuration—registry settings, driver files, third-party applications, and so on—allowing you to undo changes and roll back a system configuration to a time when it was known to work correctly.

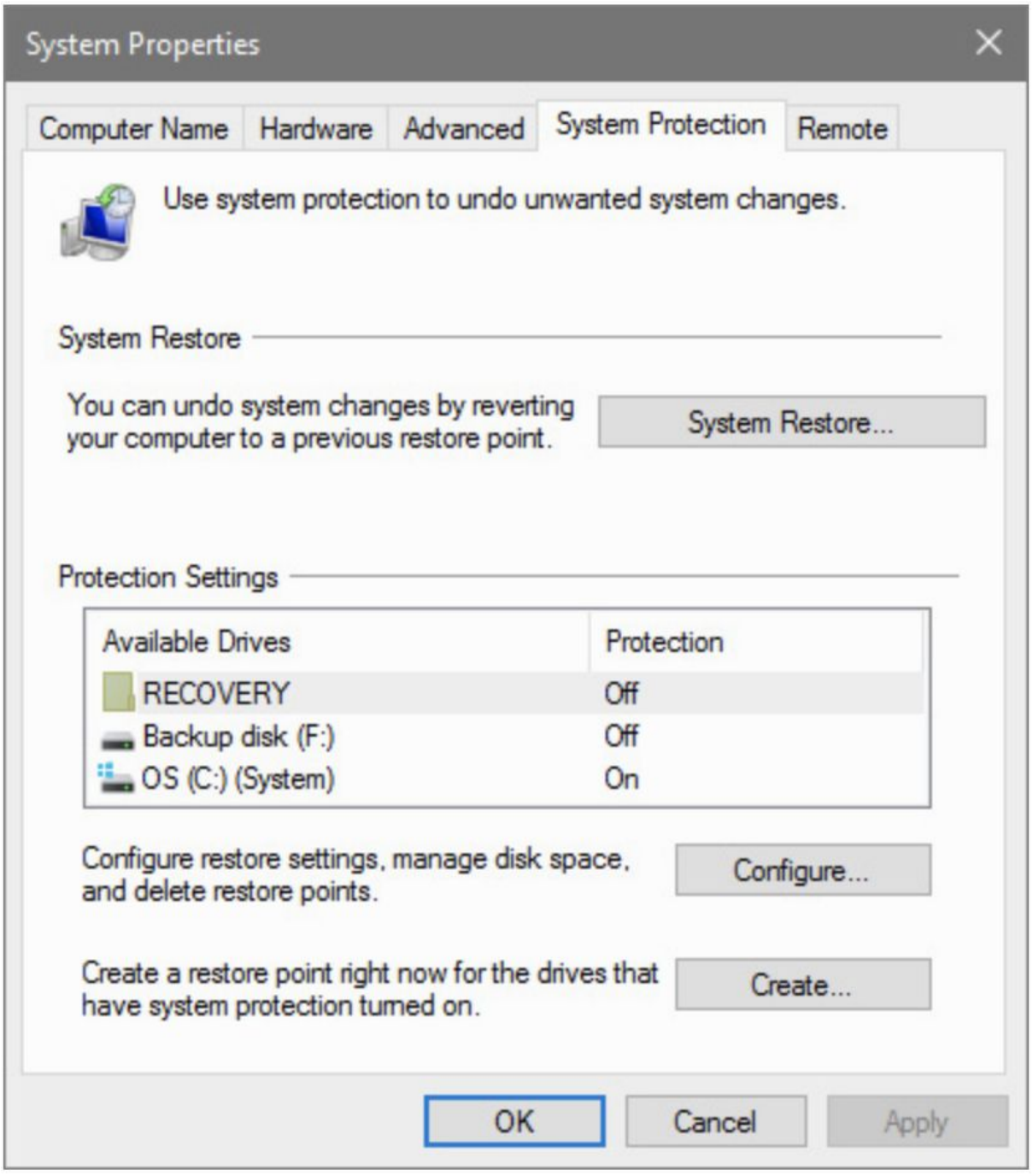
Note that System Restore monitors all files it considers system-related, which includes executable files and installers.

If you download the latest version of a favorite utility and store it in your Downloads folder, it will be removed if you roll back to a System Restore checkpoint from before it was downloaded.

To check the status of System Protection, start typing System Protection in the search box and follow the "Create A Restore Point" link to the System Protection tab of the System Properties dialog box in Control Panel.

There you’ll find a list of internal and external NTFS-formatted drives.

The value under Protection Settings indicates whether restore points are being created automatically for each drive.

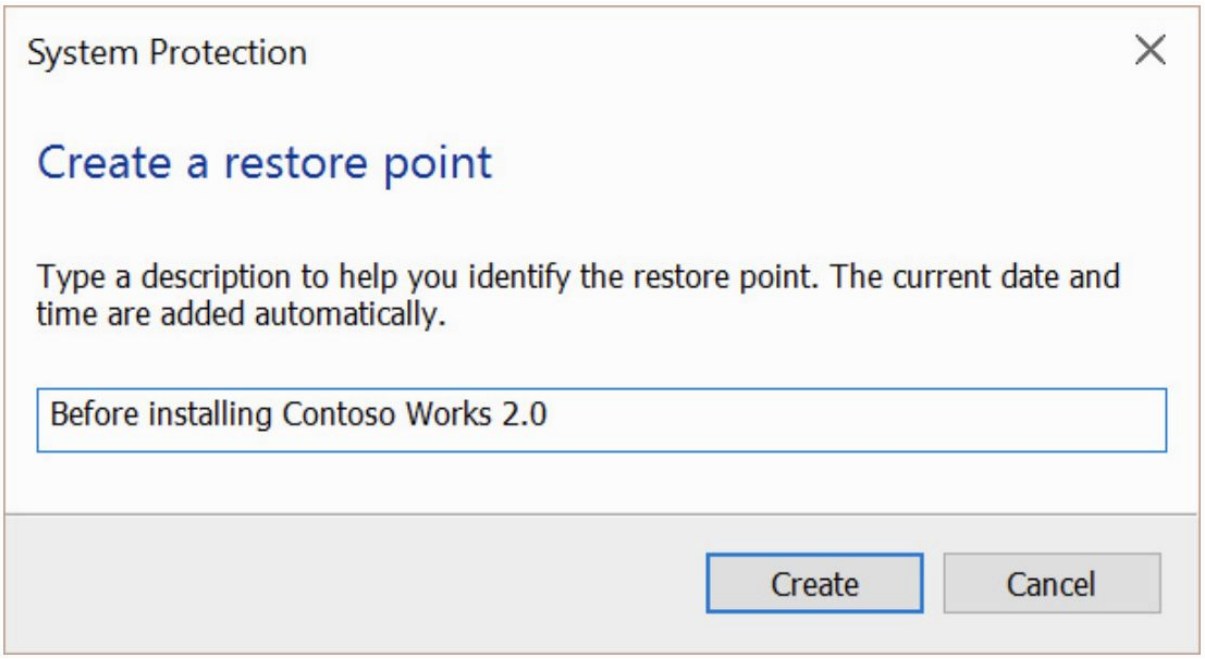


Using the System Properties dialog box, you can enable or disable automatic monitoring for any local drive.

By design, system protection is fully enabled for the system drive and is disabled for all other local drives.

You can also manually create a restore point at any time for all drives that have system protection enabled.

Click the "Create" button at the bottom of the System Protection tab to open the "Create A Restore Point" dialog box shown in the next picture:



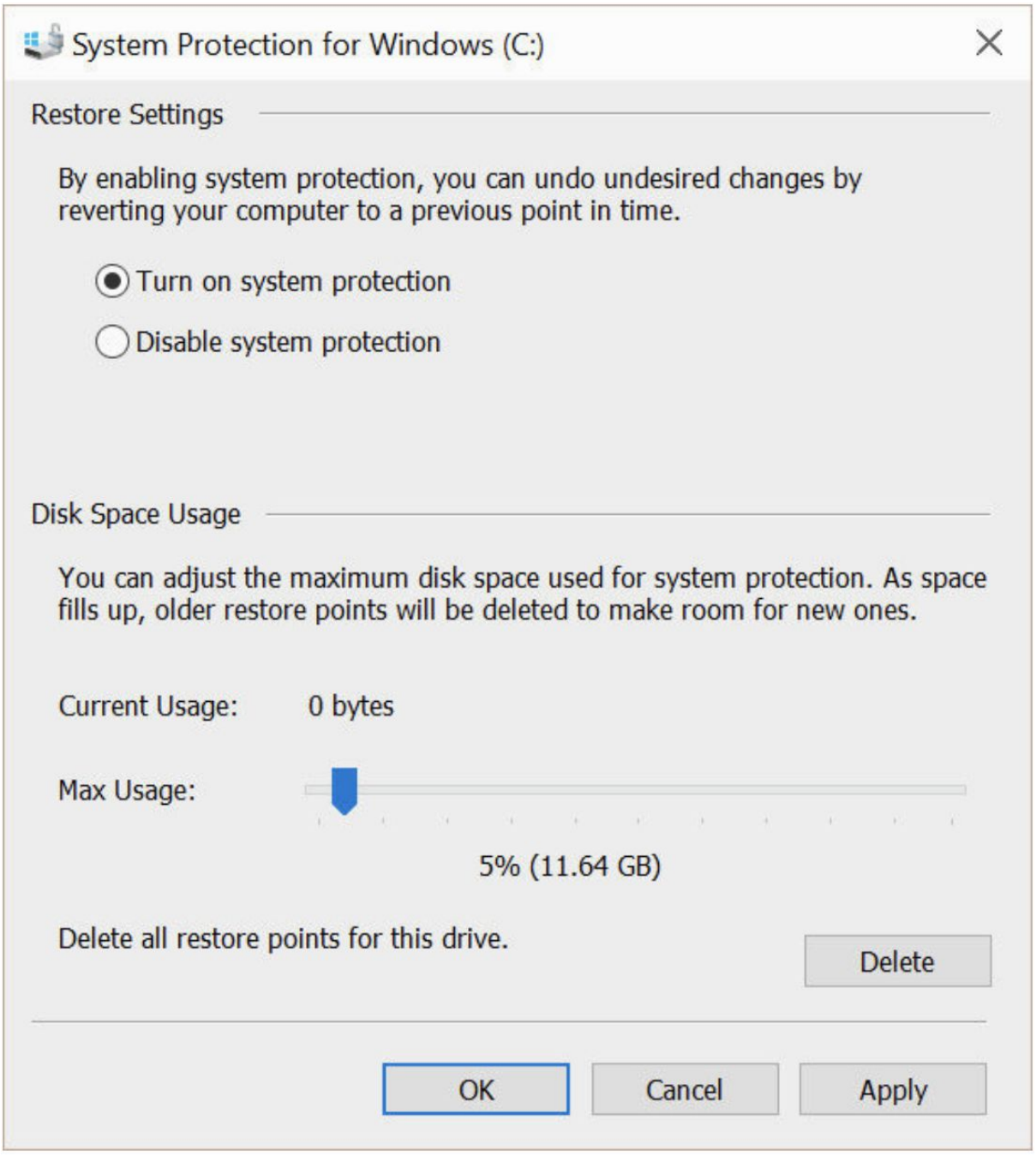
Enter a meaningful description.

You can't leave the box blank, although you can tap the spacebar to leave that box effectively blank.

Then click "Create" to enter the descriptive text.

To turn system protection on or to adjust the amount of space it uses, select a drive from the Available Drives list and then click "Configure".

That opens the dialog box shown in the following figure:



The information under the Disk Space Usage heading shows both the current usage and the maximum amount of space that will be used for snapshots before System Protection begins deleting old restore points to make room for new ones.

To adjust the maximum amount of disk space available for volume snapshots, click the System Protection tab in the System Properties dialog box, select a drive letter from the list of available drives, click Configure, and move the Max Usage slider to the value you prefer.

For drives greater than 64 GB in size, you can choose any value between 1 percent and 100 percent.

If you're concerned about disk space usage and you're confident you won't need to use any of your currently saved restore points, you can click the Delete button in the lower right corner under the Disk Space Usage heading to remove all existing restore points without changing other System Protection settings.

Rolling back to a previous restore point

After you configure System Protection, it runs silently and automatically, making as-needed snapshots of your system configuration.

The System Restore utility provides controlled access to snapshots created by the System Protection feature.

It can't perform miracles—it won't bring a dead hard drive back to life, unfortunately—but it can be a lifesaver in any of the following situations:

- You install a program that conflicts with other software or drivers on your system. If uninstalling the program doesn't cure the problem, you can restore your system configuration to a point before you installed the program. That should remove any problematic files or registry settings that were left behind by the uninstaller.
- You install one or more updated drivers that cause performance or stability problems. Rather than using the Roll Back Driver command in Device Manager, use System Restore to replace the new, troublesome driver (or drivers) with those that were in place the last time you saved a restore point.
- Your system develops performance or stability problems for no apparent reason. This scenario is especially likely if you share a computer with other family members or coworkers who have administrator accounts and are in the habit of casually installing untested, incompatible software and drivers. If you know the system was working properly on a certain date, you can use a restore point from that date, undoing potentially harmful changes made since then and, if all goes well, returning your system to proper operation.

Caution!

Don't count on System Restore to protect you from viruses, worms, Trojan horses, and other malware.

Use Windows Defender or a reliable and up-to-date third-party antivirus program.

The quickest way to get to System Restore is to type "rstrui" at a command prompt.

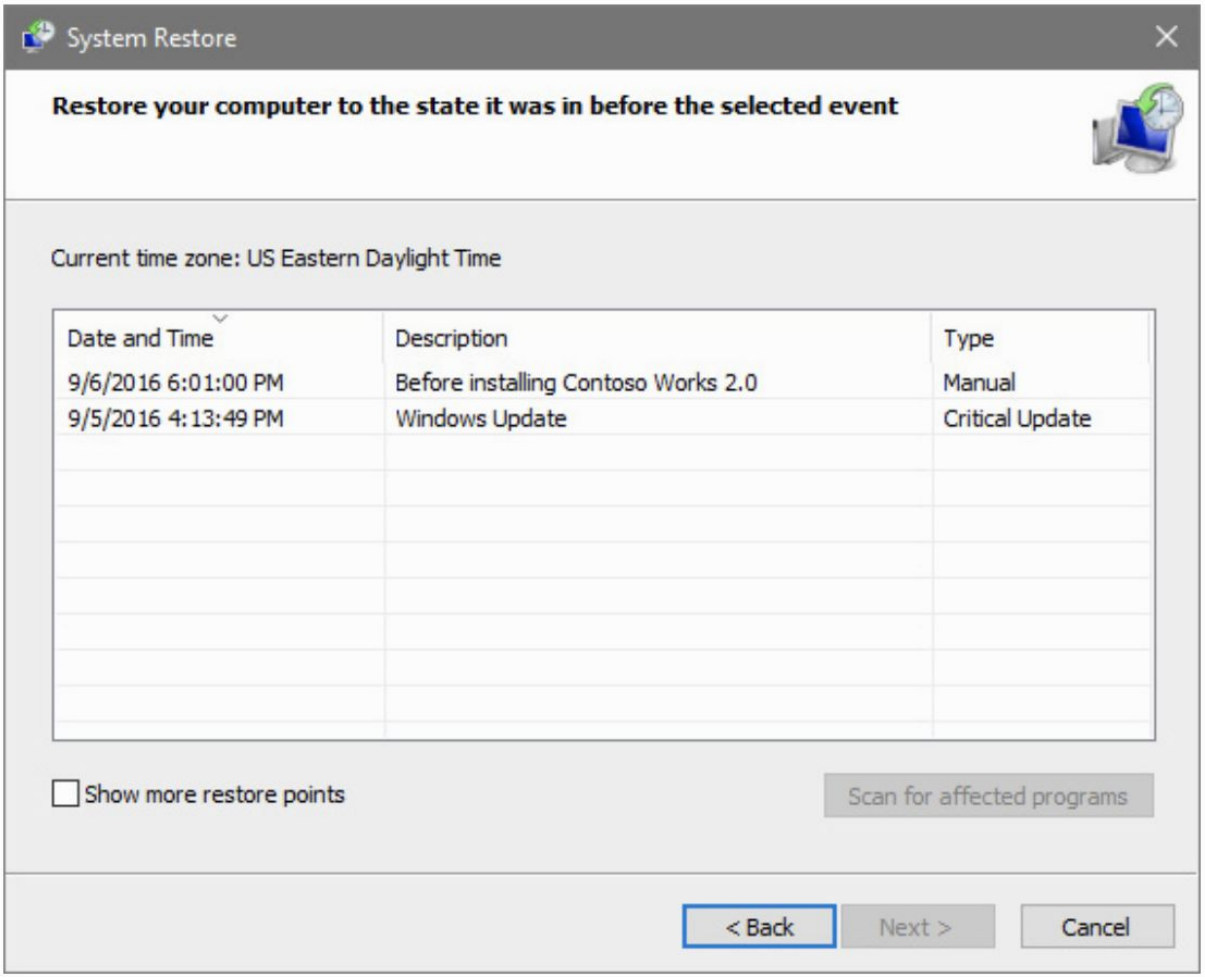
You can also click System Restore on the System Protection tab of the System Properties dialog box to find this well-hidden feature.

If you're running under a standard user account, you'll need to enter an administrator's credentials in a UAC dialog box to continue.

When the System Restore wizard appears, it might recommend the most recent restore point.

To see a complete list of available restore points, select Show More Restore Points and click Next.

That displays a list of recent restore points, as shown in the next image:



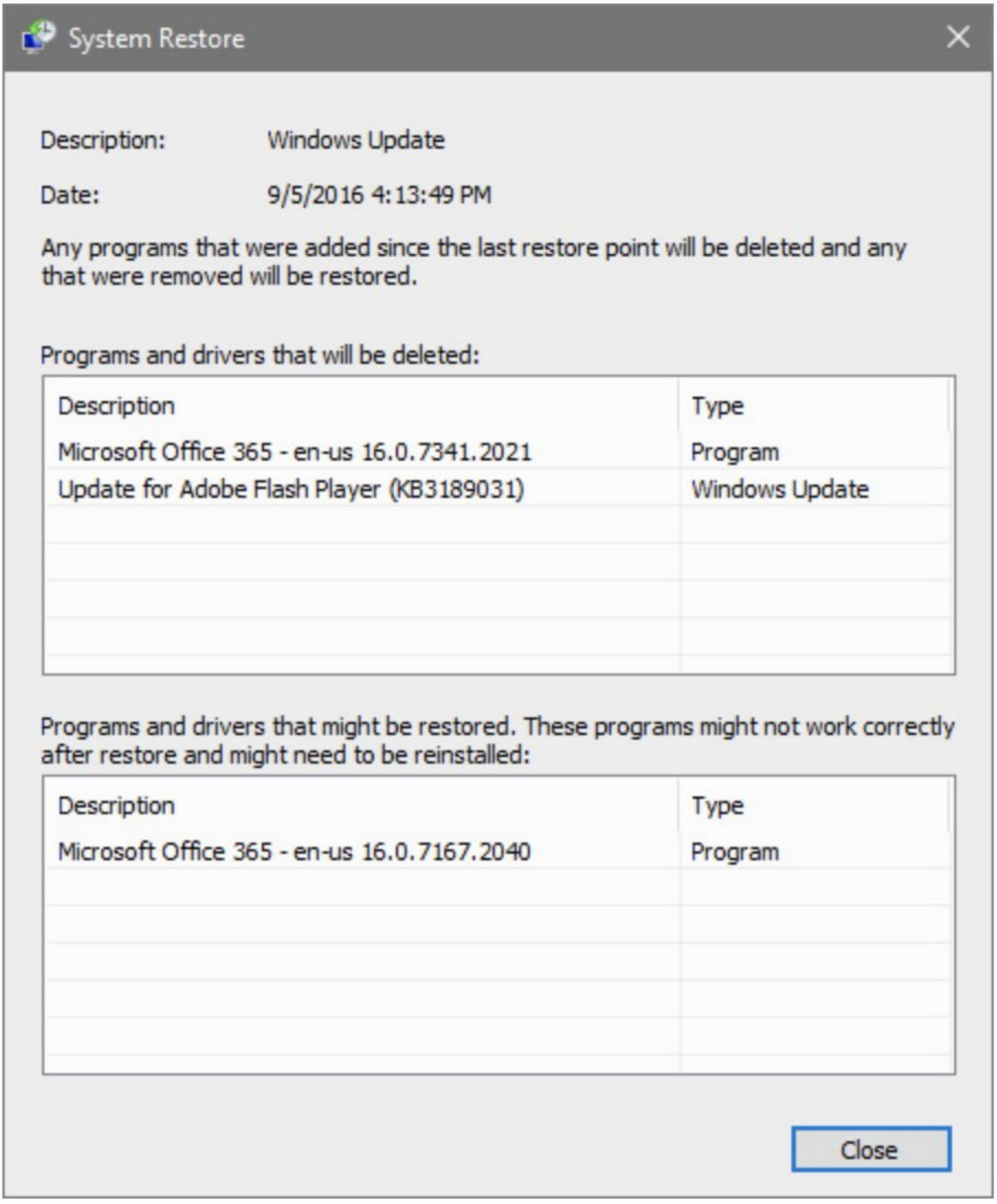
If the restore point you're looking for is older than the oldest entry in the list, select Show More Restore Points to see the full list.

What impact will your choice of restore points have?

To see a full list of programs and drivers that will be deleted or restored, select the restore point you're planning to use, and then click Scan For Affected Programs.

That displays a dialog box like the one shown in the next picture, highlighting every change you made since that restore point was created.

Note that this list does not warn you about any executable files that might be deleted from your Desktop, Downloads, or other folders.



After selecting a restore point, click Next to display a series of confirmation dialog boxes.

After you successfully convince the system that, yes, you really want to do this, it creates a new restore point and then begins replacing system files and registry settings with those in the restore point you selected.

As part of the process, your computer will restart and various messages will appear, all counseling patience and asking you not to interfere with the goings-on.

When System Restore reinstates a previously saved configuration using a restore point, your data files—documents, pictures, music files, and the like—are not tampered with in any way.

The only exception is if you or a program created or saved a file using file-name extensions from the list of monitored extensions, as described in the previous section.

Before System Restore begins the process of returning your system to a previous restore point, it creates a new restore point—making it possible for you to return to the present if this time machine doesn't meet your expectations.

When the process is complete, do some testing to see whether the restoration fixed the problem you were encountering.

If it has not and you want to return the system to the state it was in before you restored it, retrace your steps to System Restore.

At or near the top of the list of available restore points, you will find one labeled Undo: Restore Operation.

Choose that one and you're back where you started.

System Restore do's and don'ts

You don't have to be a science-fiction aficionado to appreciate the hazards of time travel.

Here are some to be aware of:

- If you create a new user account and then use System Restore to roll back your system configuration to a point before the new account was created, the new user will no longer be able to sign in, and you will receive no warning. The good news is that the new user's unencrypted documents will be intact.
- System Restore does not uninstall programs, although it does remove executable files, dynamic-link libraries (DLLs), and registry entries created by the installer. To avoid having orphaned program shortcuts and files, view the list of programs and drivers that will be affected when you return to the restore point you're about to roll back to. If you don't want the program anymore, uninstall it in the normal way before running the restore operation. If you want to continue using the program, reinstall it after the restore is complete.
- Any changes made to your system configuration using the Windows Recovery Environment are not monitored by System Protection. This can produce unintended consequences if you make major changes to system files and then roll back your system configuration with System Restore.
- Although you can restore your system to a previously saved restore point from the Windows Recovery Environment, you cannot create a new restore point from that location. As a result, you cannot undo a restore operation that you perform by starting from the Windows Recovery Environment. You should use

System Restore in this mode only if you are unable to start Windows normally to perform a restore operation.

- Vocabulary -

- thwarted: estropeado / boicoteado.
- unabridged : íntegro / estricto.

- Exercises - 1. 3. 4. Backup, restore, and recovery -

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 Settings -> Update & Security -> Recovery -> Get started. Which two options do you have?
2. Go to Settings -> Update & Security -> Backup -> Back up using File History -> Add a drive: select the “BACKUP” volume of one of the new hard drives that you have added in the previous exercises. Check if the File History Back up is made, and navigate through the new folders in the “BACKUP” volume.
3. Go to Settings -> Update & Security -> Backup -> Back up using File History -> More options -> Back up my files: “Daily”, and Keep my backups: “Until space is needed”. Check which folders are going to be back up in the “Back up these folders” section.
4. Go to Settings -> Update & Security -> Backup -> Back up using File History -> More options -> Restore files from a current backup: and check the File History app. You will need some days of backing up files after enabling File History in order to see different dates in the File History app.
5. When you reinstall Windows 10 using the “Reset this PC” feature, you can choose two different options. Which parts of Windows 10 are restored (kept) and which parts are not restored (deleted) in each of those two options?
6. Go to the Control Panel. In the search box write: “recovery drive” and click on “Create a recovery drive”. Select the “Back up system files to the recovery drive” check box. Insert a USB flash drive of at least 8 GB and create the recovery drive there. Be careful: all the data of the USB flash drive will be deleted!
7. Turn your Windows 10 virtual machine off. Add a new 60 GB hard drive in Virtual Box (“dynamic”). Turn your virtual machine on. Open “Disk Management”. Create one NTFS volume (“quick format”) of 60 GB in this new hard drive: labelled “W10-BACKUP” and with the “X” drive letter).
8. Go to Control Panel -> System and Security -> Back up and Restore (Windows 7) -> Create a system image -> One a hard disk: “W10-BACKUP” (the “X” drive letter) -> Next -> Start Backup.
9. Create a new virtual machine named “Windows 10 Restored” with 4 GB of RAM. Add a new 60 GB hard drive in Virtual Box (“dynamic”), because the C: ("WINDOWS") partition that you have made the image backup has 50 GB, so this new hard drive has to have at least 50 GB. Later, add the existing hard

drive: previously labelled “W10-BACKUP”. You are going to boot the new virtual machine into the Windows Recovery Environment. Start it with the Windows 10 installation ISO (in the virtual CD/DVD reader) or with the “recovery drive” USB flash drive inserted in the USB reader. Choose: Repair your computer -> Advanced options -> System Image Recovery. Reinstall the new virtual machine with the Windows 10 system image that you have created before. In the new virtual machine, eject the Windows 10 installation ISO (from the virtual CD/DVD reader). Start the new virtual machine and check that you have “cloned” your Windows 10: look for the user, password, desktop, user files, etc. If your new virtual machine does not start properly, turn it off, and check in "Configuración" -> "Almacenamiento" -> "Controlador: SATA" if the first hard drive is the new 60 GB hard drive that you have just restored the Windows image to. If you want to have Internet connection in the "cloned" Windows 10, you have to change the network adapter of your virtual machine in Virtual Box, from "NAT" to "Bridged" ("Adaptador puente"). Also remember to disconnect the “W10-BACKUP” hard drive from "Configuración" -> "Almacenamiento" -> "Controlador: SATA".

10. Write “System Protection” in the Windows 10 search box and follow the “Create A Restore Point” link to the System Protection tab. Select your “C:” drive and click on the “Configure…” button. Select “Turn on system protection”, put “Max Usage” to “5%” and click “OK”.
11. On the previous “System Protection” tab, click on the “Create…” button in order to create manually a Restore Point.
12. Type “rstrui” at a Command Prompt -> Next. See your different Restore Points. Select one Restore Point and click the “Next” button in order to restore your Windows 10 to that previous Restore Point. After restarting, check that the restored Windows 10 is working properly.