

CHAPTER  
**3**

# Troubleshooting and Securing Windows 10 and Using Command Lines

**After completing this chapter, you will be able to:**

- Troubleshoot Windows 10 using the new and improved Windows 10 troubleshooting tools
- Secure data in Windows 10 and protect user privacy
- Explore the new and improved Windows 10 command line tools

**W**hen a new operating system first comes on the market, computer support technicians must quickly learn how to troubleshoot and secure it. Most of the troubleshooting and security tools you've become familiar with in Windows 8 and 7 have returned in Windows 10—and often with helpful upgrades. Windows 10 also brings more sophisticated cloud integration and syncing across devices, which, while very convenient, can present some new privacy concerns. Finally, Microsoft integrated useful Linux features into Windows 10, and, in general, further empowers command-line users.

In this chapter, you first learn to use Windows 10 tools and techniques that can help you solve a Windows startup problem and troubleshoot a corrupted Windows installation with a focus on some troubleshooting tools new to Windows 10. You'll then learn about options for protecting user privacy, and you'll explore various command-line tools, including the new Linux shell for Windows.



**Notes** Labs to accompany this chapter can be found in Appendix C at the end of this text.



**Notes** Portions of this chapter are written to follow Chapters 13, 18, and 20 in *A+ Guide to IT Technical Support*, ninth edition, or Chapters 6, 10, and 11 in *A+ Guide to Software*, ninth edition, as indicated in each section.

## STRATEGIES FOR TROUBLESHOOTING WINDOWS 10

The purpose of this part of the chapter is to introduce the troubleshooting tools new to Windows 10 and show you how to use them. For a complete discussion of how to troubleshoot a computer problem, see the main textbooks that accompany this Windows 10 text.

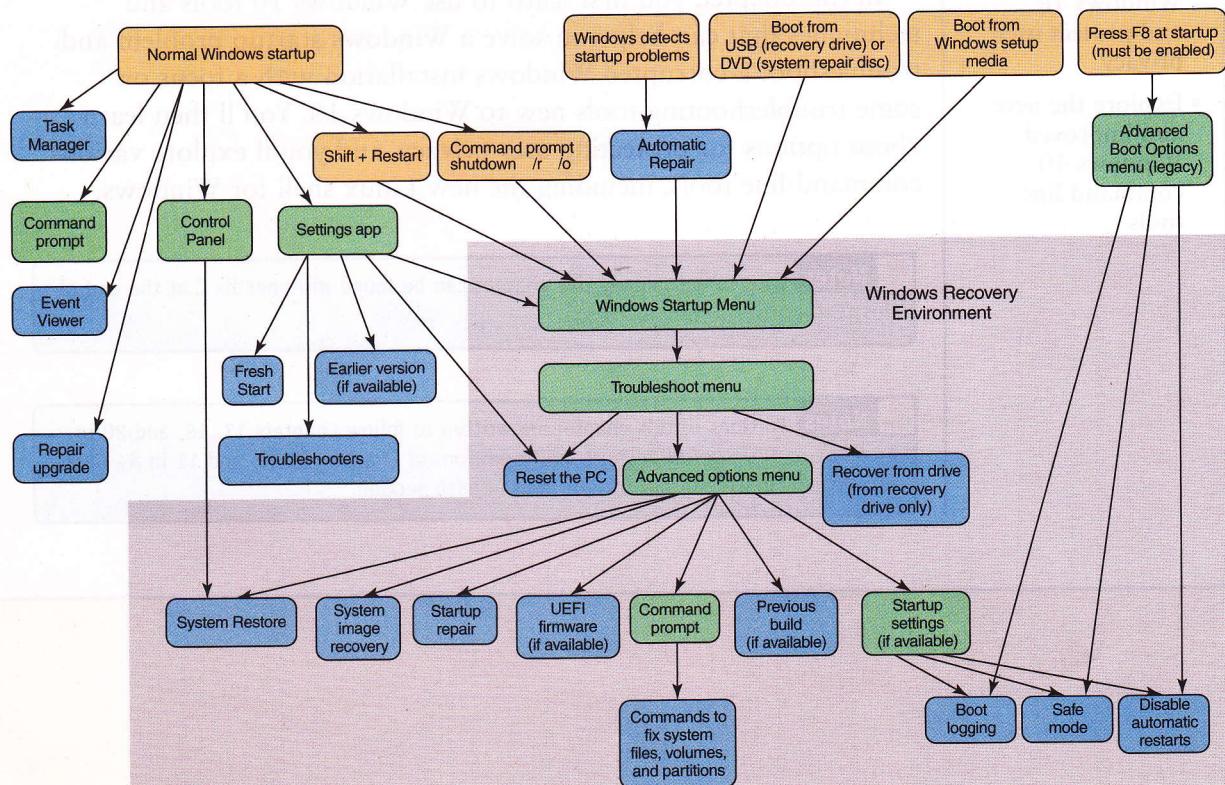


**Notes** This portion of the chapter is written to follow Chapter 13 in *A+ Guide to IT Technical Support*, ninth edition, or Chapter 6 in *A+ Guide to Software*, ninth edition.

**? To Learn More**

To learn more about troubleshooting Windows and applications, see Chapters 12 and 13 of *A+ Guide to IT Technical Support*, ninth edition, or Chapters 5 and 6 of *A+ Guide to Software*, ninth edition.

Figure 3-1 shows you the big picture of troubleshooting Windows 10. The orange boxes represent the ways to start Windows or to start the Windows Recovery Environment (Windows RE), shown as the purple area in the figure. Recall that Windows RE is an OS that offers various tools for troubleshooting problems when Windows refuses to start normally or starts with errors. The green boxes represent menus, windows, and screens that lead to the actual troubleshooting tools in blue boxes. We begin our discussion with tools available to you when Windows can start normally.



**Figure 3-1** Menus and tools to fix Windows problems and start Windows RE to get to more menus and tools to troubleshoot startup problems

### TROUBLESHOOT AFTER A NORMAL STARTUP

The following troubleshooting tools, which you can use after Windows starts normally, have not changed from Windows 8/7. Several of these tools are shown on the left side of Figure 3-1.

- ▲ **Task Manager.** Views and manages startup processes and applications and can be used to end a hung application. Task Manager also gives useful information about performance and user issues.
- ▲ **Event Viewer.** Reports all kinds of errors that happen when Windows is running and sometimes offers solutions. Windows stop errors are sometimes recorded in Event Viewer. For a stop error, right after you restart the system, examine Event Viewer for clues and possible solutions.
- ▲ **System Restore.** From Control Panel, as with Windows 8/7, you can access the System Protection dialog box to make sure System Restore is turned on or to apply a restore point when the system is giving problems. System Restore is also available in Windows RE.



**To Learn More** To learn more about creating and using restore points, see pages 460–462 in Chapter 10 of *A+ Guide to IT Technical Support*, ninth edition, or pages 124–126 in Chapter 3 of *A+ Guide to Software*, ninth edition.

- ▲ **Memory Diagnostics.** From a command prompt, use the mdsched.exe command to start the process to check memory for errors. The command also works in Windows RE.
- ▲ **System File Checker (SFC).** The sfc /scannow command, used from an elevated command prompt, checks for errors in system files and repairs them. The command also works in Windows RE.
- ▲ **Check Disk.** The chkdsk /r command detects errors and repairs a corrupted file system on the hard drive. The command also works in Windows RE.
- ▲ **Windows troubleshooters.** In the Settings app, double-click Update & security and click Troubleshoot to see a long list of troubleshooters for many common problems with hardware and software as shown in Figure 3-2. For each problem, follow the applicable troubleshooter through to a solution. There is even a troubleshooter for solving Windows Blue Screen or stop errors.

3

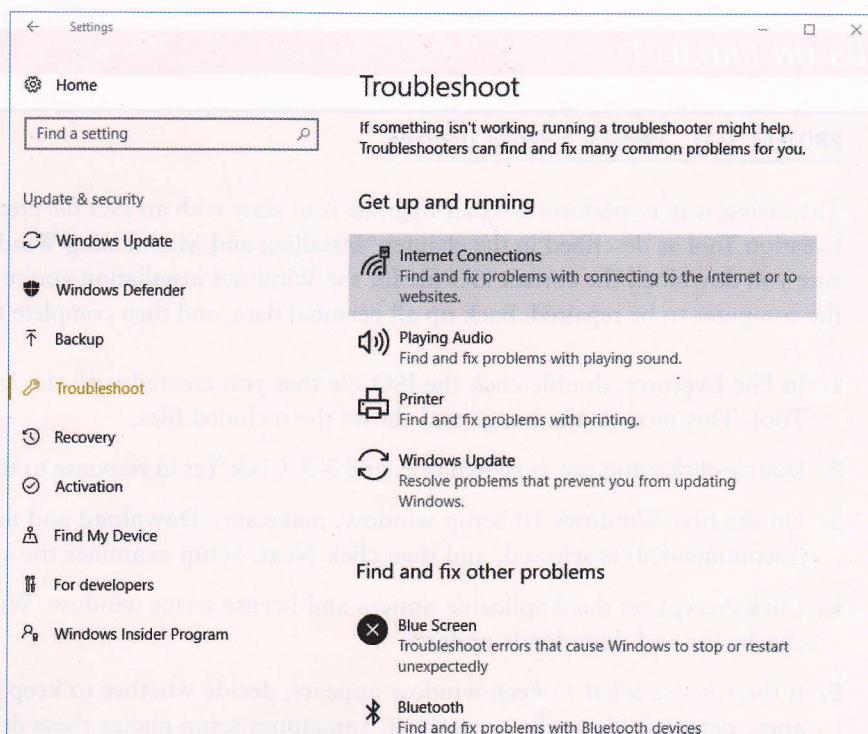


Figure 3-2 Windows 10 troubleshooters available in the Settings app

Next, we look at four troubleshooting tools that are new in Windows 10 or that have changed from Windows 8. Like the tools in the preceding list, these tools can be used after a normal Windows start. We'll start with repair upgrade, and then move on to earlier version, Fresh Start, and reset.

## REPAIR UPGRADE

If you're having problems with Windows updates or basic Windows functionality but you can still boot into Windows, you might consider performing a repair upgrade, also known as a repair install or an in-place upgrade. A **repair upgrade** is a nondestructive installation of Windows 10 over an existing Windows installation. This is not the same as a full reinstall because the Windows volume will not be reformatted. Just as with an upgrade from Windows 8 to Windows 10, you can keep personal files, apps, and Windows settings. Essentially, you trick the machine into thinking it's being upgraded while potentially repairing the Windows installation.

Keep these points in mind when doing a repair upgrade:

- ▲ Create Windows setup media, either on DVD or USB, or save an ISO file on the local hard drive.
- ▲ Make sure that you can fully boot into Windows 10. If you can't, you'll have to use a different troubleshooting tool.
- ▲ Even though all data, apps, and settings should be protected in a repair upgrade, make a backup just in case.
- ▲ Gather all product keys for all installed apps to make reinstallation of these apps easier later if necessary.



**Notes** Belarc Advisor ([belarc.com](http://belarc.com)) is a free tool that is quick and easy to use. It will produce a list of all installed apps along with their product keys if that information is available. Print a copy of the report and keep it in a safe place.

## >> HANDS-ON PROJECT

### PROJECT 3-1: Perform a Repair Upgrade

The easiest way to perform a repair upgrade is to start with an ISO file created by the Media Creation Tool as described in the chapter "Installing and Maintaining Windows 10." Make sure you download the correct ISO file for the Windows installation you're currently using on the computer to be repaired. Back up all personal data, and then complete the following steps:

1. In File Explorer, double-click the ISO file that you created with the Media Creation Tool. This mounts the image and shows the included files.
2. Double-click `setup.exe` as shown in Figure 3-3. Click **Yes** in response to the UAC dialog box.
3. On the first Windows 10 Setup window, make sure **Download and install updates (recommended)** is selected, and then click **Next**. Setup examines the system.
4. Click **Accept** on the Applicable notices and license terms window. Windows 10 Setup checks for and downloads updates.
5. If the *Choose what to keep* window appears, decide whether to keep personal files and apps, personal files only, or nothing. Sometimes setup makes these decisions for you and skips directly to the *Ready to install* window.

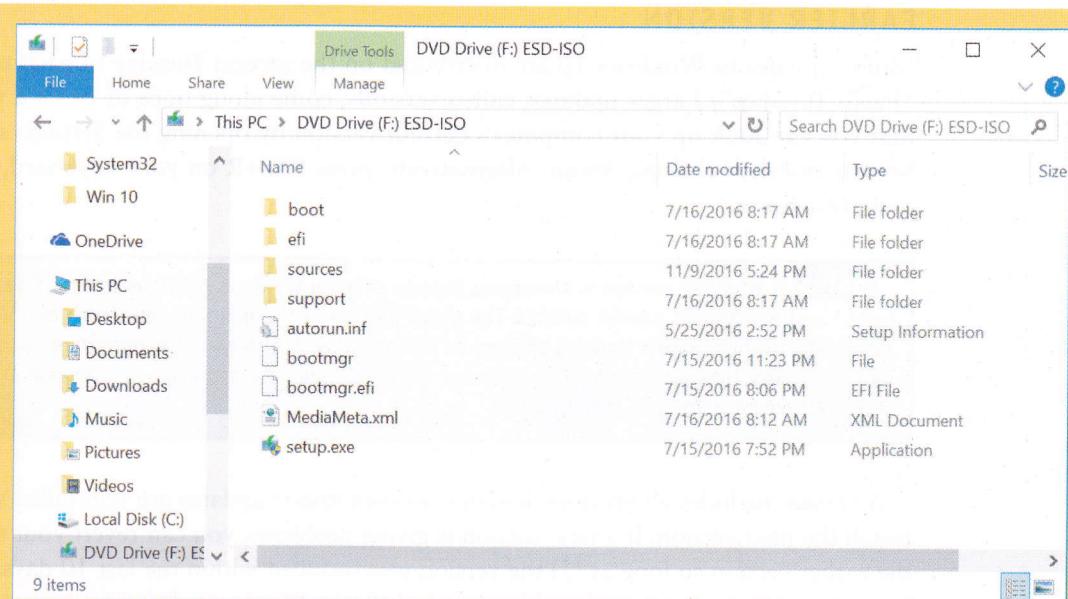


Figure 3-3 Click setup.exe to begin the repair upgrade

6. On the *Ready to install* window, make sure **Keep personal files and apps** appears and is checked as shown in Figure 3-4. If not, click **Change what to keep** and select **Keep personal files and apps**, and then click **Next** to return to the *Ready to install* window. Click **Install** to begin the installation process, which will take a while and requires several restarts. Enjoy a cup of tea or coffee while you wait.

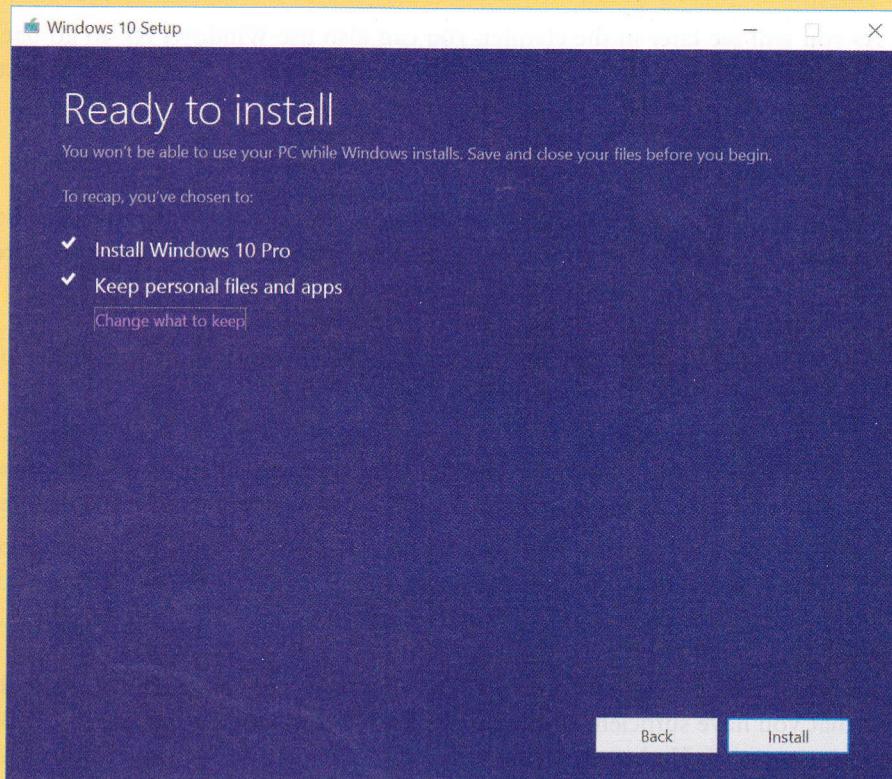


Figure 3-4 You can keep your personal files and third-party apps during a repair upgrade

7. When the lock screen appears, sign in to Windows. Once you see the desktop, all your files, apps, and settings should still be in place.

## EARLIER VERSION

Minor updates to Windows 10 are distributed on the second Tuesday of each month (called “Patch Tuesday.”) Larger updates, called **versions**, come along once or twice a year. Recall that you can look up your computer’s current version by opening the Settings app, clicking System and then clicking About. Alternatively, press Win+R on your keyboard, type winver, and press Enter.



**Notes** A Windows version is sometimes loosely called a Windows build, as in the “Creators Update build,” and is assigned a build number. The major portion of the build number (such as 15063 for build 15063.413 in the Creators Update) appears to be somewhat arbitrary and is notoriously unpredictable for future releases. However, the minor portion of the build number is more specific, in that these decimal places increment with each minor update.

A version includes all previous updates, so even minor updates are reinstalled when you install the next version. If a new version is giving problems, you can revert your system back to the earlier version so long as (1) the version was installed within the last 10 days; (2) you have not reset your computer during this time; and (3) the Windows.old folder has not been deleted.

To revert your system to the earlier version, do the following:

1. Open the Settings app, click **Update & security**, and then click **Recovery**.
2. Under *Go back to the previous version of Windows 10*, click **Get started**. If this button is grayed out, the time limit for reverting to the previous version has already passed or the Windows.old folder is missing.

As you will see later in the chapter, you can also use Windows RE to go back to a previous or earlier version. Use this method when a new version has caused the system to fail to start, such as when a critical driver is corrupted.

## FRESH START

A **Fresh Start** performs a clean installation of the most recent version of Windows 10 Home or Windows 10 Pro and is often used to remove manufacturer bloatware. Here’s what is installed, kept, and not kept with a Fresh Start:

- ▲ **Installed.** The latest generic copy of Windows, free from manufacturer bloatware, is downloaded directly from the Microsoft website.
- ▲ **Kept.** User accounts, their settings, and personal data are kept as well as some Windows settings. Microsoft apps that are natively integrated in Windows and Microsoft store apps installed by the computer manufacturer are also kept.
- ▲ **Not kept.** All apps are removed, except as stated above. A list of removed apps is displayed on the desktop after the Fresh Start completes. Be aware that you also lose any manufacturer drivers or OEM system files.

To install a fresh copy of Windows 10, first make sure you’re connected to the Internet and that you have sufficient storage space for the Windows image (about 3 GB). Open the Settings app, click **Update & security**, and then click **Recovery**. Under *More recovery options*, click **Learn how to start fresh with a clean installation of Windows** (see the left side of Figure 3-5). Click **Yes** to switch to Windows Defender Security Center, which you’ll learn more about later in this chapter. On the window shown on the right side of Figure 3-5, click **Get started** to begin the process. The tool downloads and installs a fresh copy of Windows 10. Sign in to complete setup.

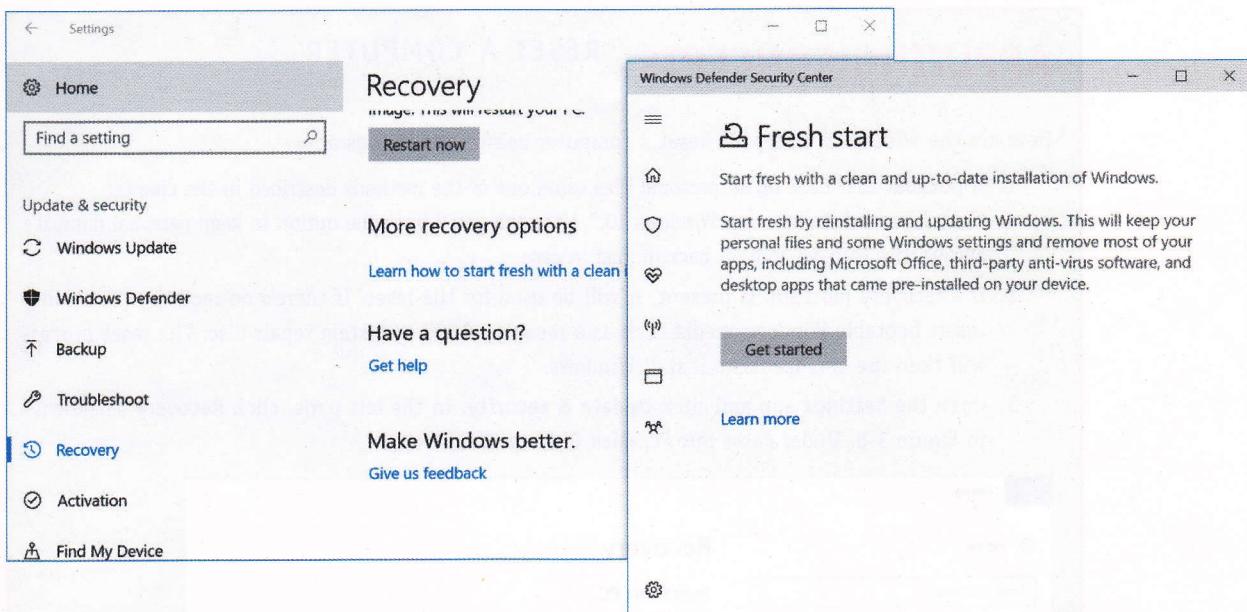


Figure 3-5 Personal files are kept when starting with a fresh copy of Windows

3

## RESET

A Windows 10 reset reinstalls Windows with the option of keeping user accounts, some Windows settings, and all personal data files. In other words, a reset is no longer considered a last-ditch effort as it was in Windows 8 and can be used earlier in the troubleshooting process. (Recall that a Windows 8 reset erases all data because it formats the Windows volume and reinstalls Windows.) If you decide to remove data files, you can also choose to clean the drive. During a reset, any apps or drivers that were installed from third-party providers will be removed, and some changes made to Windows settings will be lost. Also, if your computer has received a major update within the past ten days, you will lose the ability to revert to an earlier version of Windows. But you have the option to keep user accounts and personal files. If you're using a Microsoft account, you can choose to have many Windows settings automatically resynced to the device.



**Notes** The basic difference between the reset and Fresh Start recovery methods is that a reset uses files taken from recovery media or the recovery partition on the hard drive whereas a Fresh Start downloads a pristine, up-to-date copy of Windows from the Microsoft website. Fresh Start, therefore, gives you a cleaner reinstall or fresher start than does reset. On the other hand, a reset installs original manufacturer drivers and OEM system files, which may be needed for a customized system. Both methods are capable of retaining personal files.

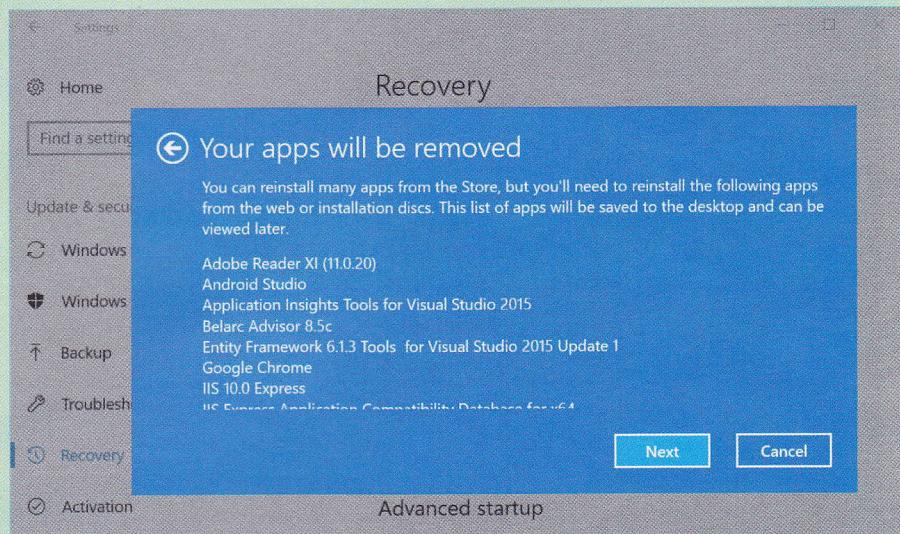


**Notes** Before performing a reset, you might want to back up any desktop apps that you've customized or use frequently. Then you can restore the backed-up versions rather than installing fresh copies. To do this, store a copy of selected apps on a flash drive using a third-party app such as CloneApp ([Mirinsoft.com](http://Mirinsoft.com)), and then restore the apps, along with their customized settings, after the Windows reset is complete.

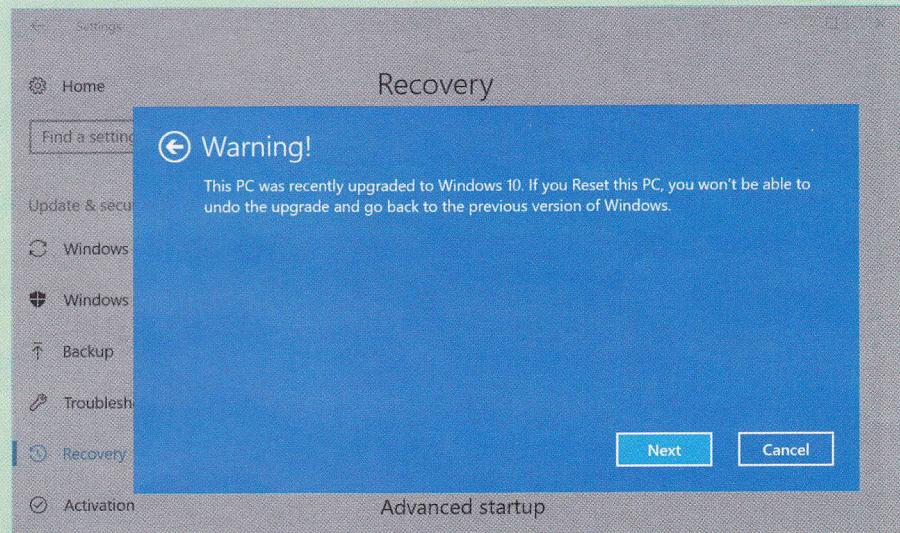
Next, you learn how to perform a reset after a normal Windows startup. Later in the chapter, you learn how to reset Windows from Windows RE when Windows refuses to start Windows normally.

**Notes** For a laptop, all-in-one, or other brand-name computer with a recovery partition present, you might see a third option on the *Choose an option* box: Restore factory settings. This option reinstalls the version of Windows that your computer came with (for example, Windows 8.1) and removes your personal files.

- a. If you click **Keep my files**, you're given a list of all apps that will be removed as shown in Figure 3-8. If you've recently updated your computer, you might see the window shown in Figure 3-9. Click **Next** and then click **Reset** to begin.



**Figure 3-8** This list of apps is saved to your desktop during the reset, and you can use it later to choose which deleted apps to reinstall



**Figure 3-9** Following a reset, you will not be able to undo an upgrade

- b. If you click **Remove everything**, you're given the option to target only the Windows drive or all drives as shown in Figure 3-10. Next, as shown in Figure 3-11, you need to choose only to remove files or remove files and also clean the drive, which will take longer but is more secure. If you've recently updated your computer, you might see the window shown in Figure 3-12. The final window, shown in Figure 3-13, confirms your selections. Click **Reset** to begin.

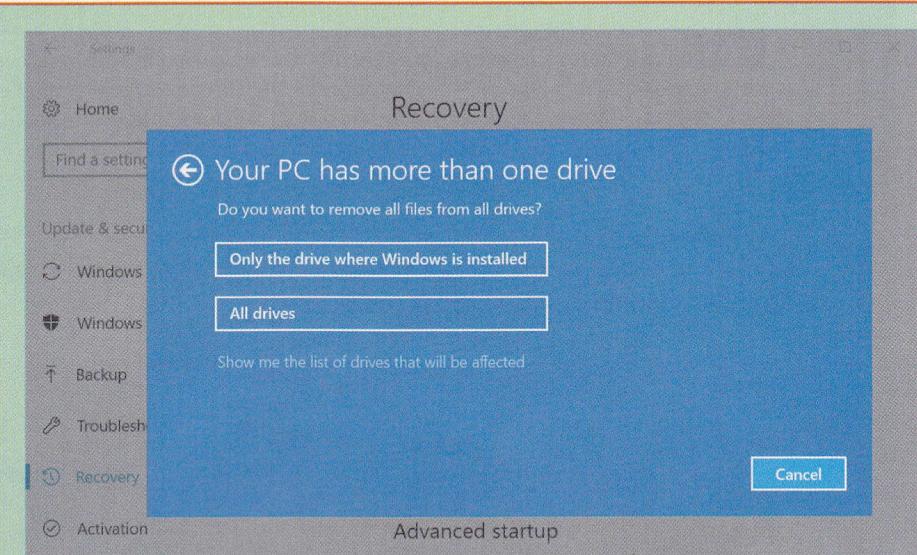


Figure 3-10 You can reset the Windows drive only or all drives

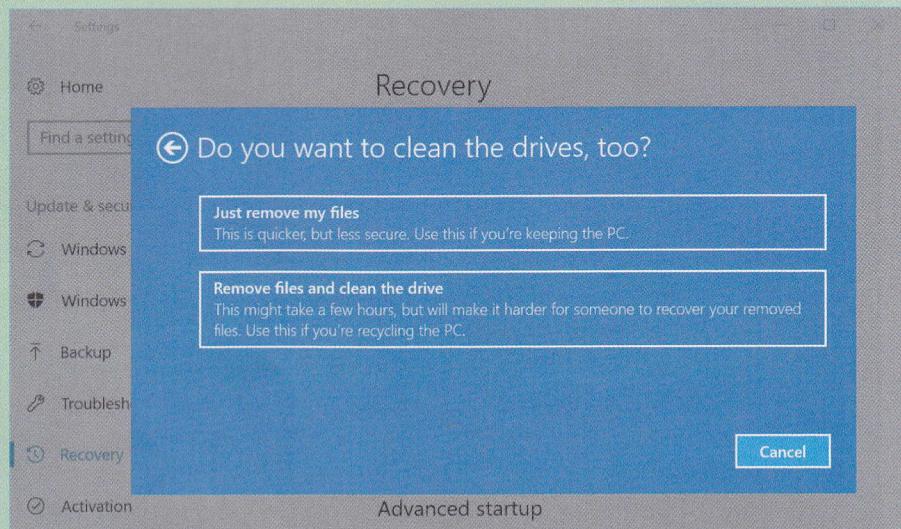


Figure 3-11 Cleaning the drives reduces the chance someone could later recover your data

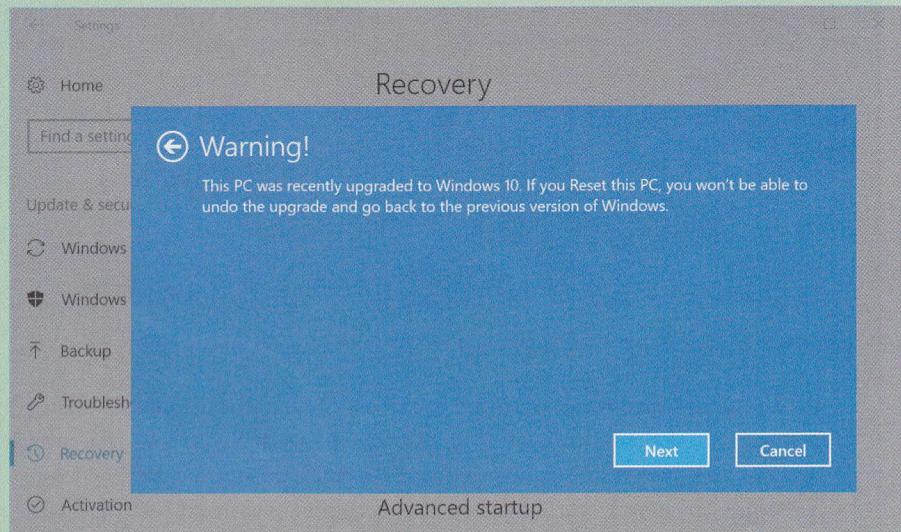


Figure 3-12 You can't return to an earlier version of Windows after resetting a computer

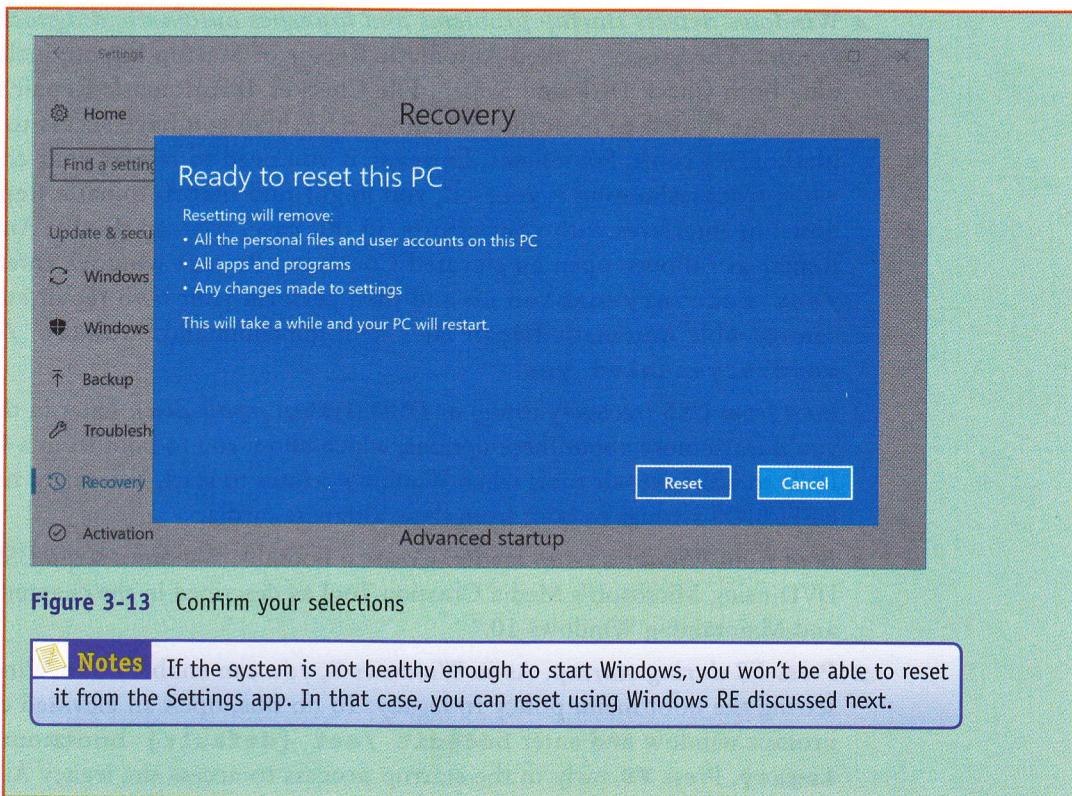


Figure 3-13 Confirm your selections



**Notes** If the system is not healthy enough to start Windows, you won't be able to reset it from the Settings app. In that case, you can reset using Windows RE discussed next.

## ACCESSING WINDOWS RECOVERY ENVIRONMENT (WINDOWS RE)

Take a look back at the purple area in Figure 3-1 that shows all the green menus and blue tasks that you can perform in Windows RE. The orange boxes in the figure show the several ways you can launch Windows RE and are described in the following list:

- ▲ **Normal Windows startup.** After Windows starts, open the Settings app and click Update & security. In the left pane, click Recovery. Under Advanced startup, click Restart now.



**Notes** Advanced startup is not available on the Recovery window in the Settings app when you are using a remote connection to the computer.

- ▲ **Shift + Restart.** From the Start menu, click the Power icon. Press and hold the Shift key and click Restart.
- ▲ **Command prompt.** In a Command Prompt window, enter `shutdown /r /o`. The /r parameter instructs the computer to restart, and the /o parameter opens Windows RE upon restart.



**Notes** You can also use the `shutdown` command to remotely shut down computers over the network.

- ▲ **Windows detects startup problems and launches automatic diagnostics and repairs.** The process, called Automatic Repair or Startup Repair, includes running both Check Disk and System File Checker. If Automatic Repair fails, you're given the option to boot into Windows RE where you have access to other troubleshooting tools. Sometimes, however, if you need to restart your computer while troubleshooting it yourself, you might find that Automatic Repair slows down or interferes with your efforts. In this case, you can disable Automatic Repair as follows: open an elevated Command Prompt window, enter `bcdedit /set recoveryenabled no` and then perform your own repair steps. You can reenable Automatic Repair later with the command `bcdedit /set recoveryenabled yes`.
- ▲ **Boot from USB (recovery drive) or DVD (system repair disc).** Later in this chapter, you'll learn more about these options, which allow you to boot from a USB drive or a DVD to access repair tools when Windows refuses to start. You might have to adjust UEFI/BIOS settings to boot from these alternate media.
- ▲ **Boot from Windows setup media.** Create a bootable Windows setup USB drive or DVD using Microsoft's Media Creation Tool as described in the chapter "Installing and Maintaining Windows 10."
- ▲ **Press F8 during startup.** As in Windows 8, you can enable F8 in Windows 10 by setting the boot menu policy to *legacy*. To do this, open an elevated command prompt window and enter `bcdedit /set {default} bootmenupolicy legacy`. Press **F8** early in the startup process to access the legacy Advanced Boot Options screen as shown in Figure 3-14. To revert to the standard boot menu policy, enter the command `bcdedit /set {default} bootmenupolicy standard`. Enable F8 before you need it as a precaution.

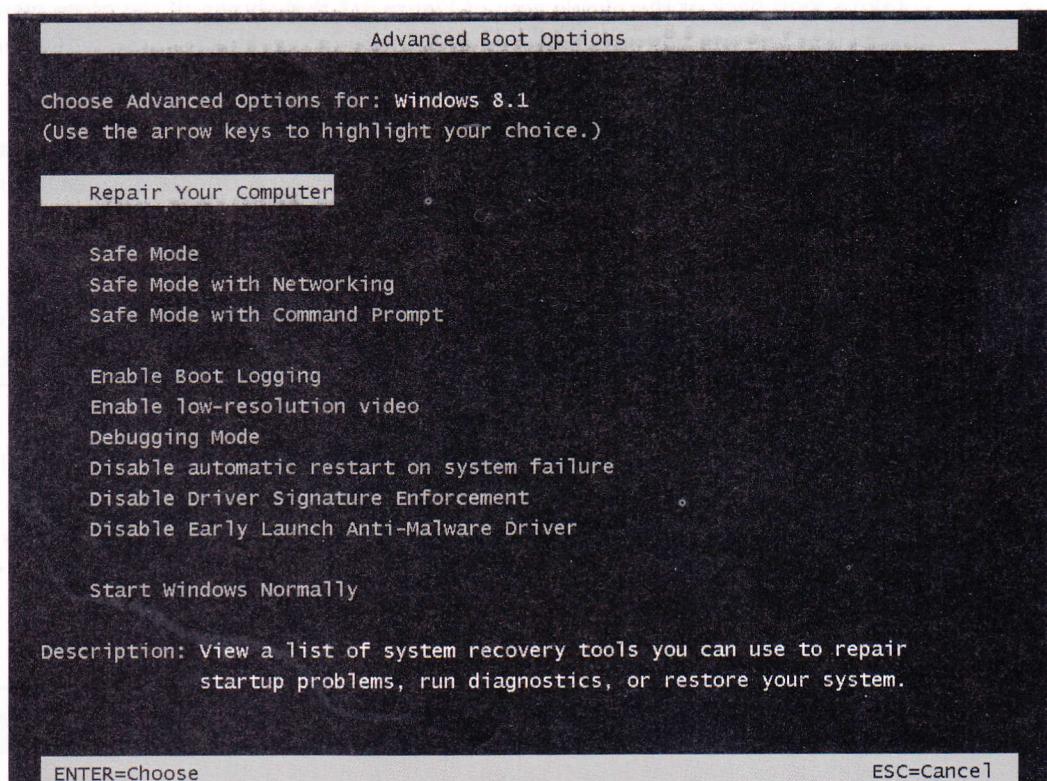
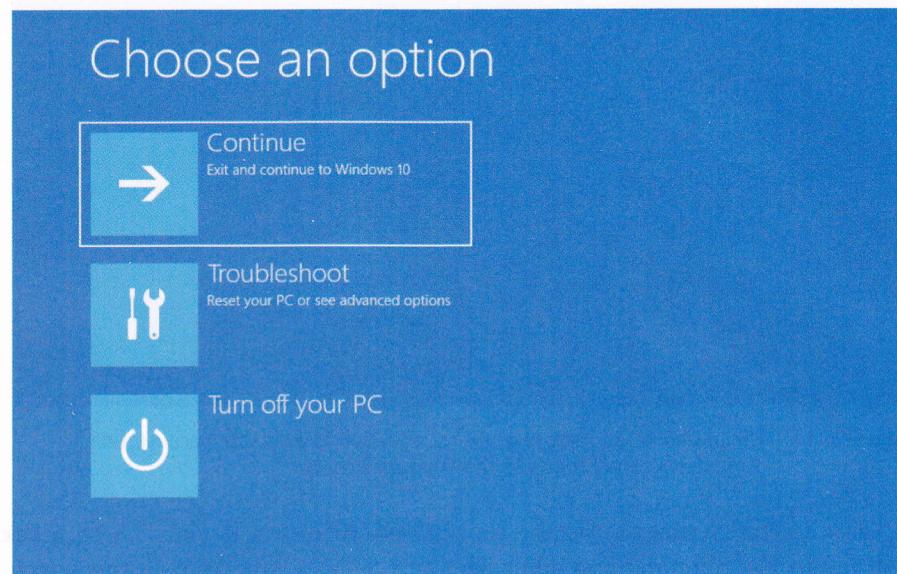


Figure 3-14 Use the Advanced Boot Options menu to troubleshoot difficult startup problems

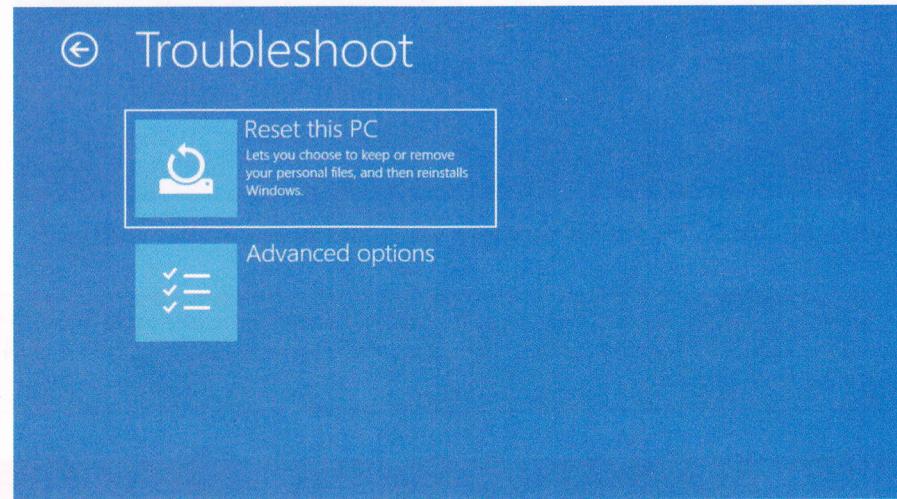
## MENU SCREENS IN WINDOWS RE

Regardless of how you launched Windows RE, when it launches, the first screen you see is called the Windows Startup Menu or the *Choose an option* screen shown in Figure 3-15.



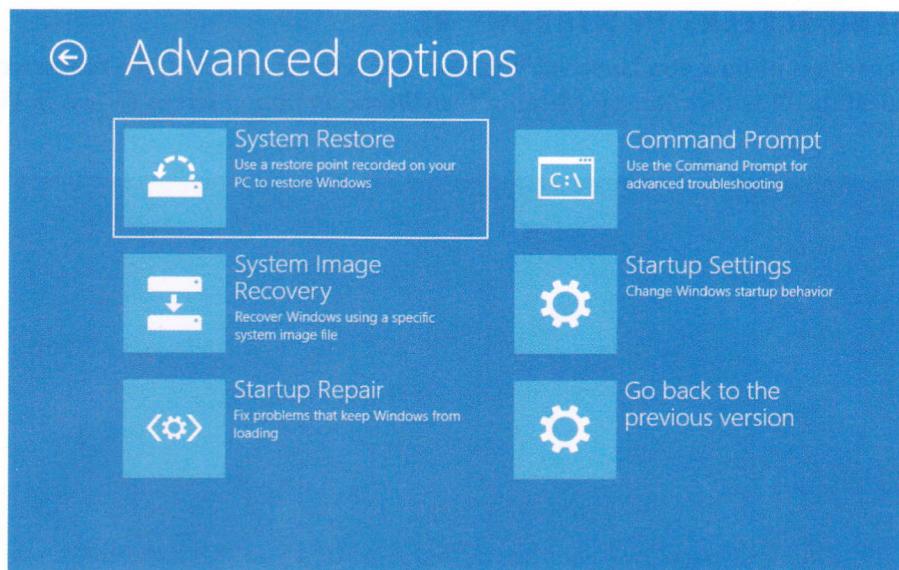
**Figure 3-15** The Windows Startup Menu is the first screen you see when entering Windows RE

Looking back at Figure 3-1, you can see how the Windows Startup Menu green box leads you to more menu screens. Click **Troubleshoot** to see the **Troubleshoot** menu screen in Figure 3-16.



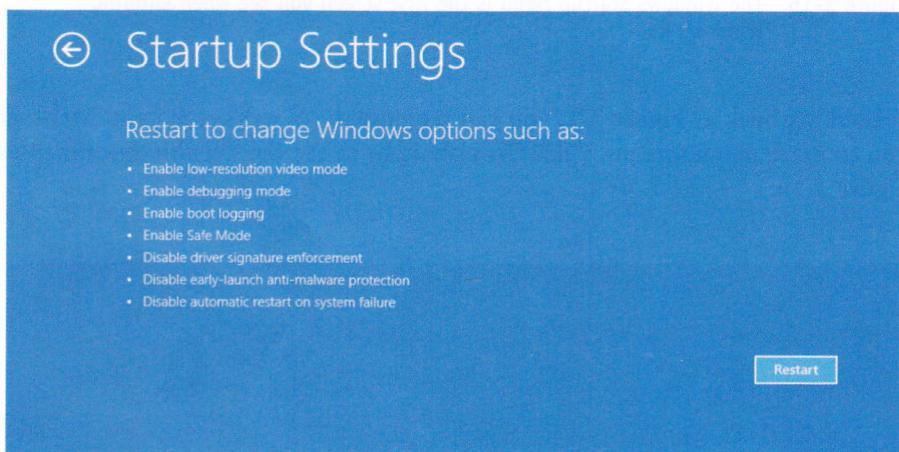
**Figure 3-16** You can reset the computer from the Troubleshoot screen

Click **Advanced options** to see the Advanced options screen in Figure 3-17. You can get to a command prompt by clicking Command Prompt where you can enter various commands to troubleshoot and solve problems. The Startup Settings option on the Advanced options screen is included on the screen only if Windows RE is accessed through the Settings app.



**Figure 3-17** The option to go back to a previous version is available because this computer recently received the Creators Update

Click **Startup Settings** to see the startup options shown in Figure 3-18. Clicking **Restart** will restart the computer and implement any changes you make on this screen.



**Figure 3-18** The Startup Settings menu gives you options for how Windows starts up

**To Learn More** To learn more about the Startup Settings menu, see pages 606–610 in Chapter 13 of *A+ Guide to IT Technical Support*, ninth edition, or pages 270–274 in Chapter 6 of *A+ Guide to Software*, ninth edition.

## >> HANDS-ON PROJECT

### PROJECT 3-2: Use the bcdedit Command

Making changes to the Boot Configuration Data (BCD) store can affect how your Windows system boots, which can often be helpful when troubleshooting startup problems. Use the bcdedit command to manually edit the BCD. Be sure to make a copy of the BCD before you edit it.

To practice using the **bcdedit /export** command, complete the following steps:

1. Open an elevated Command Prompt window. Enter the command **bcdedit /export C:\BCDBackup** to create a backup copy of the BCD store on the C: drive (or change the drive letter for a different drive). Open File Explorer and confirm your BCD backup file has been created as shown in Figure 3-19.

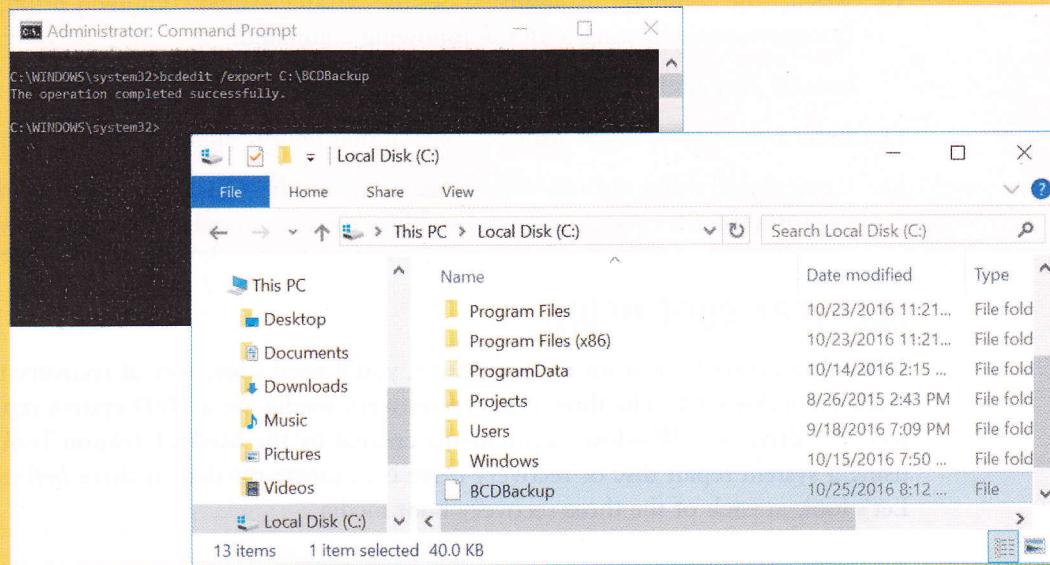


Figure 3-19 Specify the file path and filename where the BCD backup should be saved



**Notes** If you later need to use the backup copy of the BCD store, enter the command **bcdedit /import C:\BCDBackup**, using the correct path and filename for your backup copy of the BCD store.

2. Enter the command **bcdedit /enum** to display the current contents of the BCD store. Copy and paste this data to a text document for later reference. Save the document to your desktop and name it **BCDStore**.



**Notes** The default parameter on the **bcdedit** command is **/enum**, so entering **bcdedit** by itself produces the same command output.

3. Locate the *recoveryenabled* setting in the Windows Boot Loader section of the BCD store. Is Automatic Repair enabled or disabled on your system?
4. Reverse this setting using the appropriate command:  
To disable Automatic Repair, enter **bcdedit /set recoveryenabled no**  
To enable Automatic Repair, enter **bcdedit /set recoveryenabled yes**
5. Enter **bcdedit /enum** again to confirm the setting has been changed. Then revert to the original setting using the appropriate command.
6. Locate the *bootmenupolicy* setting in the Windows Boot Loader section. What setting is currently selected?

7. If necessary, change this setting to Legacy by entering the following command:  
**bcdeedit /set {default} bootmenupolicy legacy**
8. Enter **bcdeedit /enum** again to confirm that *bootmenupolicy* has been set to Legacy.
9. Restart your computer and attempt to use F8 to reach the legacy Advanced Boot Options screen. Did it work?
10. Restart the computer normally. If desired, at an elevated command prompt, revert the *bootmenupolicy* setting with the following command:  
**bcdeedit /set {default} bootmenupolicy standard**
11. Enter **bcdeedit /enum** again to confirm that *bootmenupolicy* has been set to Standard.
12. Compare all other settings with those shown in the BCDDStore text document saved on your desktop. If everything matches, close the Command Prompt window.

## RECOVERY BOOT MEDIA

If Windows can't boot from the hard drive, you'll need some sort of recovery media to launch Windows RE. The three types of recovery media are a DVD system repair disc, a USB recovery drive, and Windows setup media created by the Media Creation Tool. The key to using a system repair disc or recovery drive is to create the disc or drive *before* it is needed. Let's look at each of the three recovery boot media.



**Notes** All boot media is bit-specific. Use 32-bit media to repair a 32-bit Windows installation and 64-bit media to repair a 64-bit installation.

### SYSTEM REPAIR DISC

A system repair disc is a bootable DVD with Windows repair tools that can start the system and fix problems. Using the DVD requires an optical drive.

The system repair disc was an integral backup tool for Windows 7, was an option but hidden in Windows 8, and has resurfaced in Windows 10 in Control Panel on the *Backup and Restore (Windows 7)* window (see Figure 3-20). To use a system repair disc, boot the system from the disc and select your keyboard layout. Then Windows RE is launched.

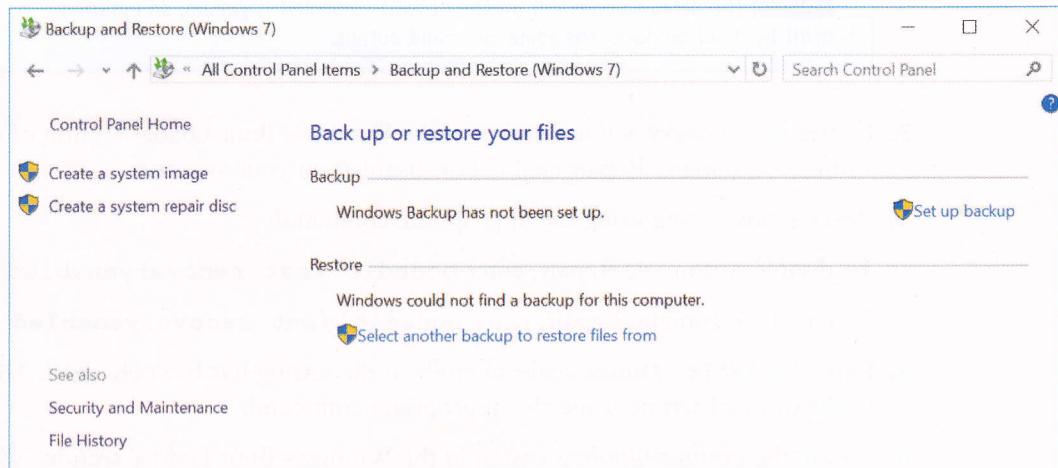
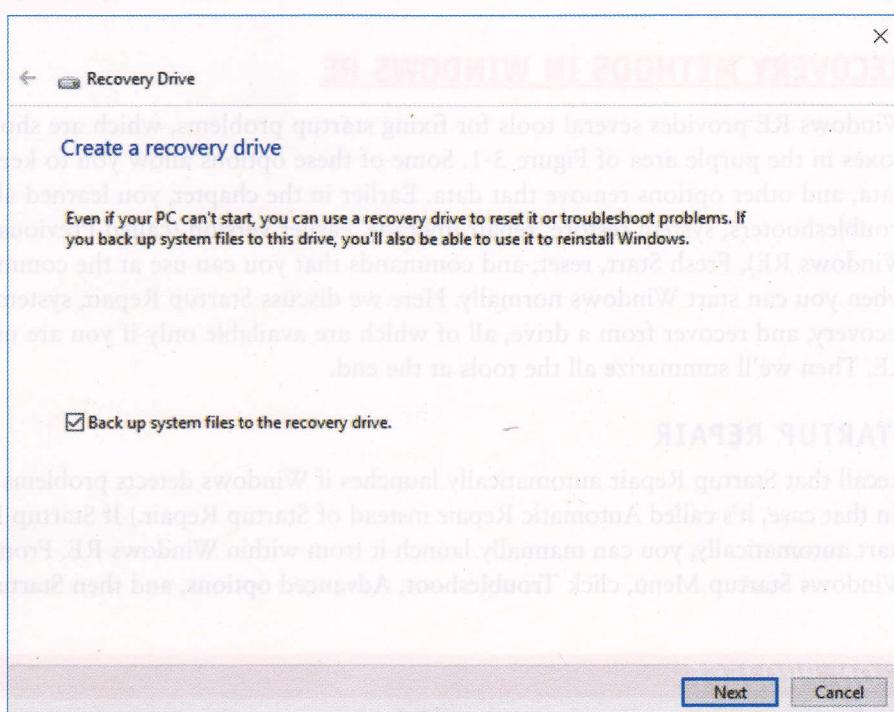


Figure 3-20 Create a system image or a system repair disc from Control Panel

**To Learn More** To learn more about creating a system repair disc, see page 601 in Chapter 13 of *A+ Guide to IT Technical Support*, ninth edition, or page 265 in Chapter 6 of *A+ Guide to Software*, ninth edition.

## RECOVERY DRIVE

A recovery drive is a bootable USB flash drive that can access Windows repair tools and is handy when you need to repair a computer that doesn't have an optical drive. When you create a recovery drive, you can choose to back up system files as shown in Figure 3-21. For a laptop, all-in-one, or other brand-name computer, these system files include OEM system files and drivers created by the manufacturer and stored on a recovery partition. If you include the system files on the recovery drive, you have the option of reinstalling Windows from the recovery drive which Microsoft documentation calls **recover from a drive**. The process deletes personal files and third-party apps and drivers, reinstalls manufacturer drivers, and restores settings to original manufacturer settings. You can use a recovery drive to repair a computer other than the one on which it was created. However, system files included on a recovery drive may not be compatible with all computers.



**Figure 3-21** Back up system files to the recovery drive so you can reinstall Windows later

To be used as a recovery drive, the USB flash drive needs to have at least 1 GB storage. If you plan to back up system files to the drive, you'll need 8 GB to 16 GB of storage on the drive. Also keep in mind that all data on the drive will be erased. Do the following to create a recovery drive:

1. Open Control Panel and click Recovery. Click Create a recovery drive, and click Yes in the UAC dialog box.
2. Choose whether to include system files (refer back to Figure 3-21), and then click Next. For a brand-name computer, these system files include OEM files if they are available.

3. Windows reports the size USB flash drive needed. Insert a flash drive. Windows inspects the size of the drive, and, if the drive is large enough, you see it listed among available devices. Select the drive and click **Next**. Click **Create** to begin the process. It will take a while to complete.

**? To Learn More** To learn more about creating a recovery drive, see pages 599–601 in Chapter 13 of *A+ Guide to IT Technical Support*, ninth edition, or pages 263–265 in Chapter 6 of *A+ Guide to Software*, ninth edition.

## MEDIA CREATION TOOL

Another option for a computer that can't boot is to use the Media Creation Tool on a working computer to create a bootable Windows setup ISO file, DVD, or flash drive, and then use that media to access Windows RE or reinstall Windows on the broken computer. Recall that you learned how to use the Media Creation Tool in the chapter “Installing and Maintaining Windows 10” of the text.

Now that you know how to launch Windows RE from within Windows or by using other bootable media, let's look at the tools available in Windows RE to repair a system.

## RECOVERY METHODS IN WINDOWS RE

Windows RE provides several tools for fixing startup problems, which are shown in the blue boxes in the purple area of Figure 3-1. Some of these options allow you to keep personal data, and other options remove that data. Earlier in the chapter, you learned about Windows troubleshooters, system restore, repair upgrade, earlier version (called Previous build in Windows RE), Fresh Start, reset, and commands that you can use at the command prompt when you can start Windows normally. Here we discuss Startup Repair, system image recovery, and recover from a drive, all of which are available only if you are using Windows RE. Then we'll summarize all the tools at the end.

### STARTUP REPAIR

Recall that Startup Repair automatically launches if Windows detects problems while starting. (In that case, it's called Automatic Repair instead of Startup Repair.) If Startup Repair doesn't start automatically, you can manually launch it from within Windows RE. From the initial Windows Startup Menu, click **Troubleshoot**, **Advanced options**, and then **Startup Repair**.

### >> HANDS-ON PROJECT

#### PROJECT 3-3: Use Startup Repair

When Startup Repair attempts to fix the system, it creates a log file with information about the steps taken during the repair process. If Startup Repair doesn't fix the system, you can use the log file to investigate the problem and perhaps manually fix it. Do the following to practice using Startup Repair and examine its log file:

1. Use the Settings app in Windows to launch Windows RE. From the initial Windows Startup Menu, click **Troubleshoot**, **Advanced options**, and then **Startup Repair**.
2. Diagnostics of the system are made and the location of the log file displays on screen. Note the path and name of the file. The default location of the log file is

C:\Windows\System32\LogFiles\SRTSRTTrail.txt. Click **Advanced options**. You are returned to the Windows Startup Menu.

3. To view the log file from the Windows RE command prompt, click **Troubleshoot** and click **Command Prompt**.
4. In the Command Prompt window, enter the command **c:** to access the hard drive. (Or a different drive depending on the log file location reported in Step 2.)
5. Use this command to go to the directory where the log file is located: **cd \Windows\System32\LogFiles\SRT**
6. To use NotePad to view the file contents, enter this command: **notepad.exe SRTTrail.txt**
7. In the log file, look for information about a failed test.

**To Learn More** To learn more about Startup Repair, see pages 602–606 in Chapter 13 of *A+ Guide to IT Technical Support*, ninth edition, or pages 266–270 in Chapter 6 of *A+ Guide to Software*, ninth edition.

3

## SYSTEM IMAGE RECOVERY

You learned how to create a system image in the chapter “Installing and Maintaining Windows 10.” System image recovery tends to be an all-or-nothing recovery option where you replace the entire contents of a hard drive with whatever operating system state and personal data are saved in the system image. It recovers all personal files, system files, and installed apps that were in place at the time the system image was most recently created or updated. If your system image is updated regularly, this option could work very well for you when repairing or replacing hardware, such as a failed hard drive. However, if a software-related problem has been building for a while, a recently updated system image won’t necessarily fix the root of the problem.

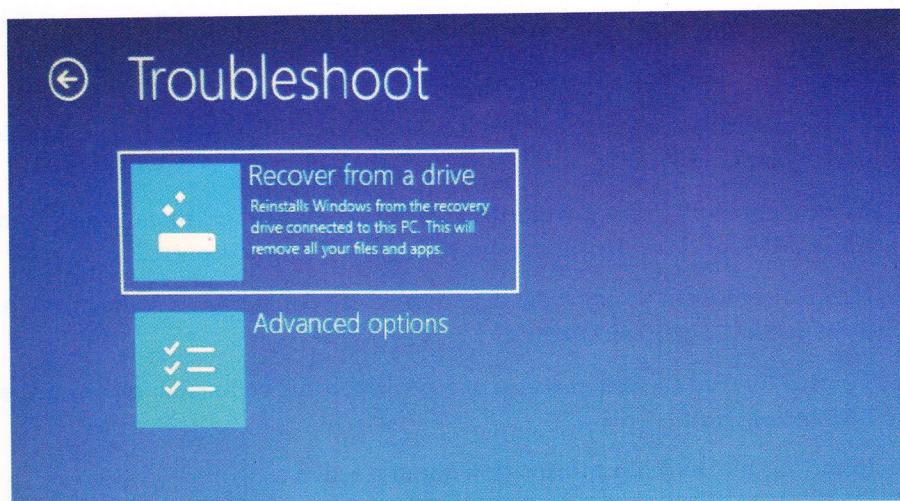
To recover Windows using a system image file, reboot the computer into Windows RE, click **Troubleshoot**, **Advanced options**, and **System Image Recovery**.

**To Learn More** To learn more about creating and using system images, see page 464 in Chapter 10 of *A+ Guide to IT Technical Support*, ninth edition, or pages 128 in Chapter 3 of *A+ Guide to Software*, ninth edition.

## RECOVER FROM A DRIVE

If you create a recovery drive before encountering a problem, you can use the recovery drive to access Windows RE and its recovery options. If you back up system files to the recovery drive, you can use the drive to reinstall Windows. You’ll lose all personal data files and installed apps if you recover Windows from the system files on the recovery drive.

When you boot from the recovery drive, choose your keyboard layout and then click **Troubleshoot**. You’ll see the screen shown in Figure 3-22. *Advanced options* takes you to the familiar Advanced options screen shown earlier in Figure 3-17 (except you won’t see Startup Settings as an option). To reinstall Windows from the recovery drive, click **Recover from a drive**.



**Figure 3-22** When you boot from a recovery drive, you're given the option to recover Windows from the drive if you saved system files to that drive

Table 3-1 summarizes all the Windows recovery methods discussed in this part of the chapter along with their respective functions and unique features. The methods are listed from least to most invasive.

Method	Function	Location	Unique Features
Startup Repair	Repairs files required for startup	Windows RE	Does not affect personal data, installed apps, or Windows settings
Earlier version or Previous build	Reverses major updates	Settings app or Windows RE	Can be used within 10 days after a major update
Repair upgrade	Repairs Windows installation	ISO file in File Explorer	Installs a new copy of Windows over the existing copy without disrupting personal files, installed apps, or Windows settings
System Restore	Reverses changes to Windows	System window or Windows RE	Applying a restore point can lose some user settings, applications installed, and other events done after the restore point was created. User data is not affected.
System Image Recovery	Copies entire system image from a previously stored backup image	Windows RE	Includes all personal files and installed apps
Reset*	Reinstalls Windows	Settings app or Windows RE	Can preserve personal data; uses OEM system files on computer if available
Fresh Start	Installs a clean copy of Windows	Settings app	Eliminates OEM bloatware; downloads Windows from Microsoft website
Recover from a drive	Reinstalls Windows	Recovery drive, if system files are included	Removes all personal files and installed apps

\*Some computer manufacturers provide a Push-Button Reset option that preserves all apps and Windows settings during the reset.

**Table 3-1** Recovery methods in Windows 10

## SUMMARY OF TROUBLESHOOTING STRATEGIES

Now that you've seen the new Windows 10 troubleshooting and recovery methods, let's look at strategies for using them. Here's a list of what to do and when:

1. Before anything goes wrong, take time to create a system repair disc, recovery drive, or installation media, and, if appropriate, a system image.

2. Show every user you support how to use File History to back up their personal data and how to restore files from backups. Don't forget to ask the user to practice restoring a file or folder so he or she is comfortable with recovering lost data.
3. When troubleshooting a startup problem, follow procedures to interview the user, back up important data or verify you have current backups, research and identify any error messages, and determine what has recently changed that might be the source of the problem. These troubleshooting skills work about the same way no matter which OS you're supporting.

 **To Learn More** To learn more about troubleshooting Windows startup problems, see Chapter 13 of *A+ Guide to IT Technical Support*, ninth edition, or Chapter 6 of *A+ Guide to Software*, ninth edition.

4. When troubleshooting an unknown startup problem in Windows 10, follow these steps, which are listed in the least intrusive order:
  - a. **Restart.** Restart the system and, if Windows detects a startup issue, it will attempt to fix its own problems.
  - b. **Repair.** Use the Startup Repair option on the Advanced options screen (refer to Figure 3-17).
  - c. **Restore.** Use System Restore on the Advanced options screen.
  - d. **Reset.** Use the *Reset your PC* option on the Troubleshoot screen (refer to Figure 3-16). You can choose whether to keep your data files, or to completely start over with a new installation of Windows 10.
  - e. **Recover from a drive.** If you saved system files to a recovery drive (refer to Figure 3-21), reinstall Windows from this drive. Personal data, apps, and settings will be lost.
  - f. **Reinstall.** Use the Media Creation Tool on a working computer to create installation media with a new copy of Windows. Personal data, apps, and settings will be lost, and you might need to reinstall drivers for various devices.

3

## PROVIDE REMOTE ASSISTANCE: QUICK ASSIST

Sometimes technicians are called upon to assist users remotely. In Windows 10, you have two options to remotely assist a user: Remote Assistance and the new Quick Assist. As an improvement on Remote Assistance, Quick Assist does not require an emailed invitation, it works in all versions of Windows 10, and it's more universally compatible with existing network hardware configuration. Using Quick Assist, the computer of the person receiving assistance becomes the host computer and the computer of the technician providing assistance becomes the client computer. For Quick Assist to work, both computers must be running Windows 10, the technician providing assistance must have a Microsoft account, and the person receiving the connection must agree to it by entering a code generated by the technician's client computer.



**Notes** Remote Desktop Connection, a similar remote connection app that is also built into Windows, is still available in Windows 10.



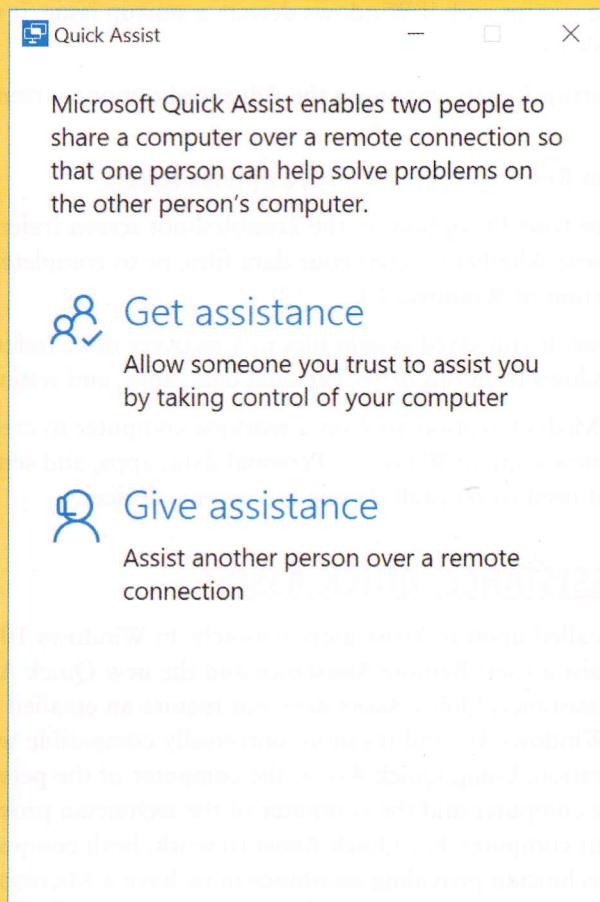
**To Learn More** To learn more about Remote Assistance and Remote Desktop, see pages 815–822 in Chapter 17 of *A+ Guide to IT Technical Support*, ninth edition, or pages 427–434 in Chapter 9 of *A+ Guide to Software*, ninth edition.

**>> HANDS-ON PROJECT****PROJECT 3-4:** Use Quick Assist

To complete this project, you need to work with a partner, with one person acting as a technician giving assistance, and the other acting as a person getting assistance. Quick Assist is designed to help people who are not in the same location to work together. So if you and your partner are working on two computers in the same room, pretend you are actually working in remote locations. Perform the steps and then change roles and repeat, so you both have the chance to give and get assistance.

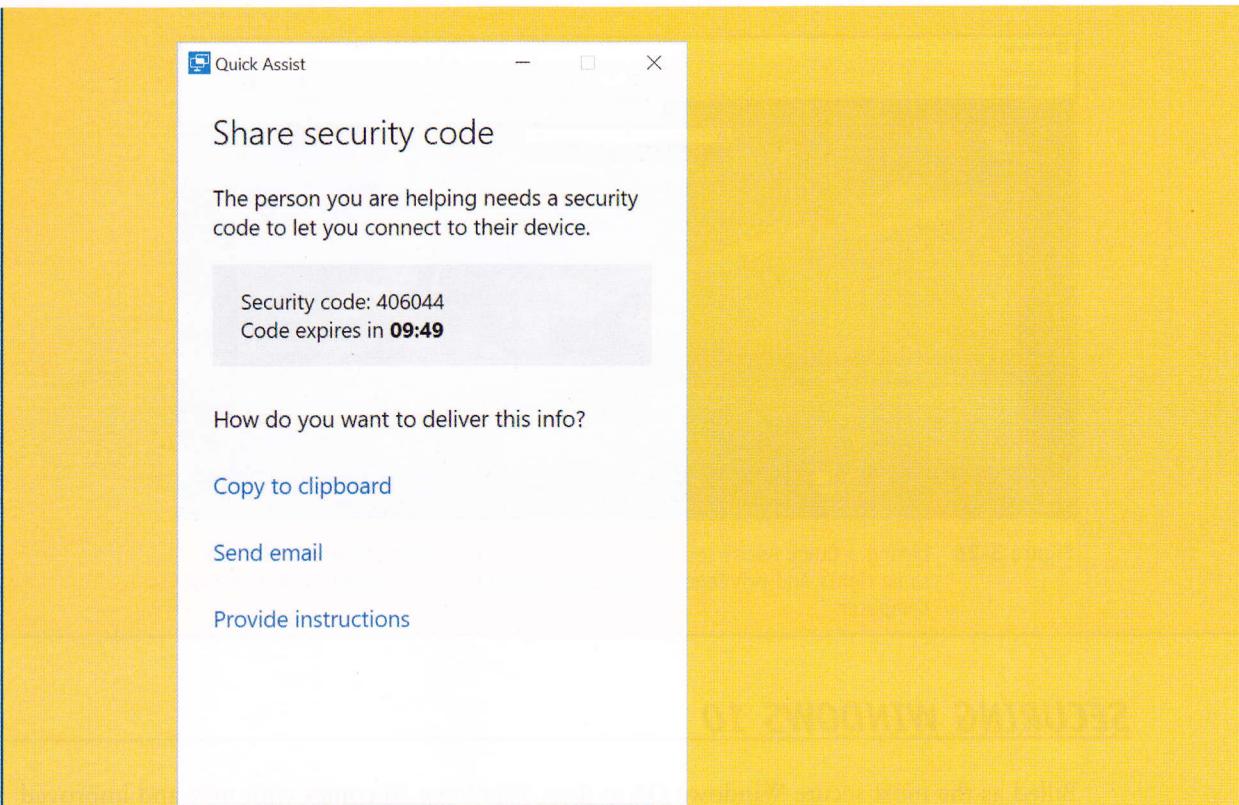
As a technician giving help, follow these steps:

1. Click Start and type Quick Assist, or open the Windows Accessories folder in the Start menu. Click Quick Assist to open the app shown in Figure 3-23.



**Figure 3-23** Request or offer assistance via a remote connection

2. Click **Give assistance**, and sign in with your Microsoft account if necessary. You'll see a 6-digit security code that is valid for 10 minutes as shown in Figure 3-24.
3. Do one of the following to share this information with the person you're assisting:
  - ▲ **Copy to clipboard.** Paste the security code and instructions into an email or chat app.
  - ▲ **Send email.** Use Quick Assist to send the security code and instructions directly by email.



3

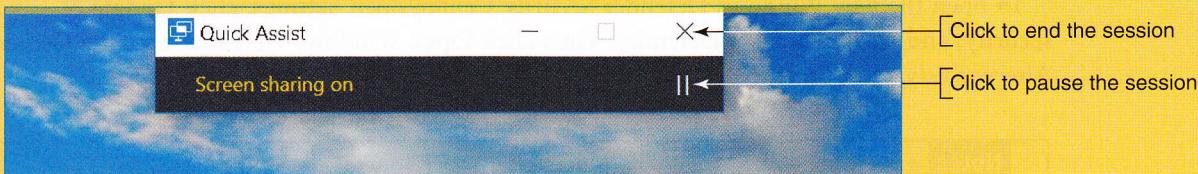
**Figure 3-24** Send instructions and the security code to the person receiving assistance

▲ **Provide instructions.** Read the instructions and security code on your screen as you talk the other person through the connection process.

As the person getting assistance, complete these steps:

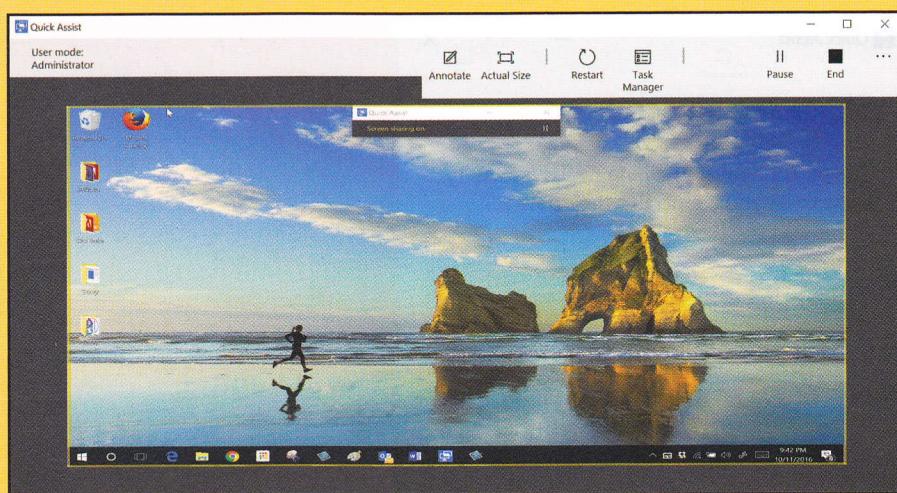
1. Open the Quick Assist app as described in Step 1 above.
2. To request assistance, click **Get assistance**. Next, enter the code provided by the technician, which you might receive in an email, via a chat app, or over the phone. Click **Submit**.
3. Click **Allow** to give permission for the technician to have access to your computer.

After the connection is established, a toolbar appears at the top of the host computer screen with options for pausing or disconnecting (see Figure 3-25).



**Figure 3-25** The person receiving assistance maintains control of the screen-sharing session

The technician on the client computer sees the host computer's screen along with a toolbar (see Figure 3-26) for adjusting the display and interacting with the other computer. Notice the technician can end the session by clicking End.



**Figure 3-26** During a Quick Assist session, the technician providing assistance has the same rights and privileges as the user account that is signed in on the host computer

## **SECURING WINDOWS 10**

Billed as the most secure Windows OS to date, Windows 10 comes with new and improved security features. In the chapter “Survey of Windows Features and Support Tools” you learned about Windows Hello, which uses biometric authentication or a second device to sign you in to Windows. Let’s look at some other security improvements in Windows 10.



**Notes** This portion of the chapter is written to follow Chapter 18 in *A+ Guide to IT Technical Support*, ninth edition, or Chapter 10 in *A+ Guide to Software*, ninth edition.

### **WINDOWS DEFENDER SECURITY CENTER**

Windows Defender received an extensive overhaul with the Windows 10 Creators Update. Defender is no longer limited to anti-malware functions and is now integrated with Windows Firewall. In addition, it provides single-point access to device performance, app control, and family protection features. When you attempt to configure options for these features, Defender will often redirect you to other parts of Windows (such as Control Panel). But still, it’s helpful to know that you can always start in Defender. In future updates to Defender, you can expect to find access to additional settings.

To open the new Windows Defender Security Center, open Settings, click Update & security, and click Windows Defender. Then click Open Windows Defender Security Center. Alternatively, click Start, type Defender, and click Windows Defender Security Center.



**Notes** A third way to access Windows Defender Security Center is to show the hidden icons in the system tray on the taskbar and double-click the shield icon (see Figure 3-27).

The Windows Defender Security Center home screen (see Figure 3-28) gives a quick overview of your device’s status. Click Virus & threat protection to see a scan and threat

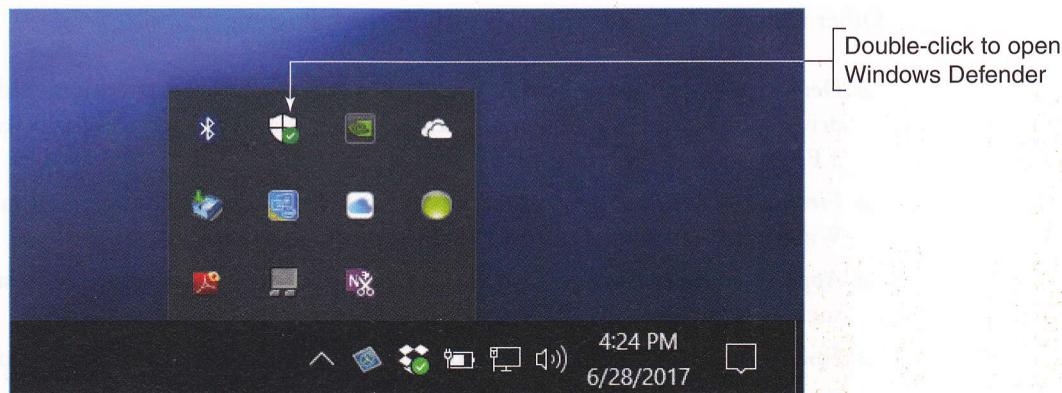


Figure 3-27 Defender is a hidden icon in the system tray

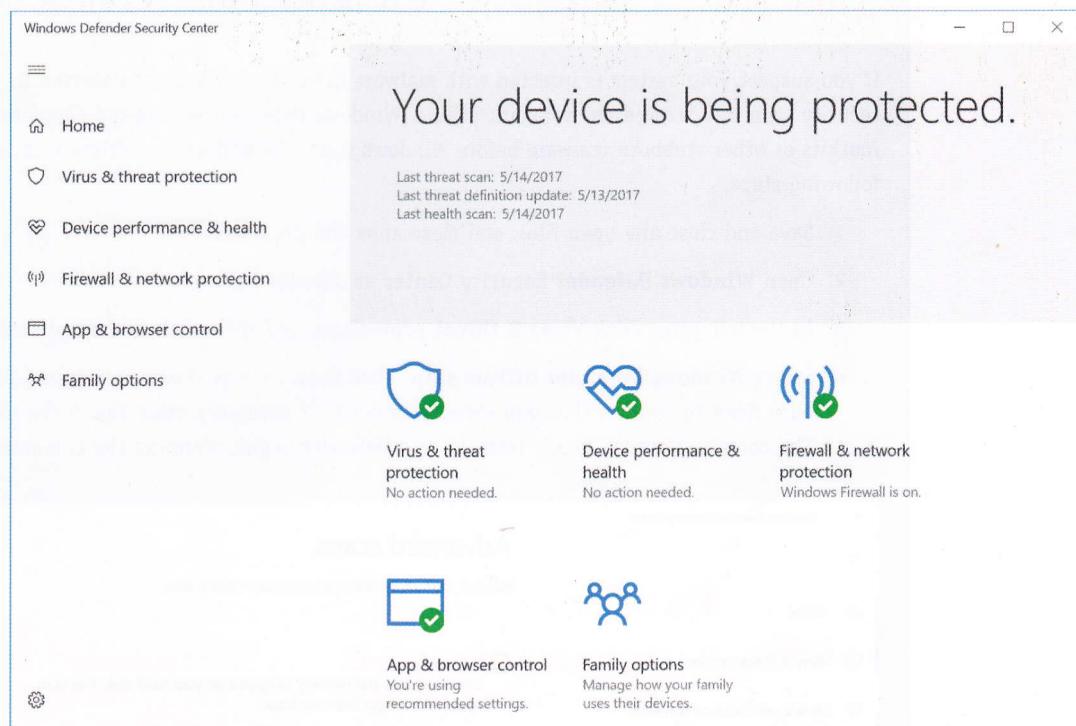


Figure 3-28 The new Windows Defender Security Center

history report or to initiate a new scan. Click **Advanced scan** to see a new option called **Windows Defender Offline**. An offline scan gives Windows an edge in removing rootkits and stubborn malware by running a scan in a trusted environment. It restarts your computer and scans the system before Windows loads. Windows Defender Offline was available as a download to bootable media for Windows 8, but it's much more accessible and easier to use in Windows 10.

Back on the *Virus & threat protection* screen, click **Virus & threat protection settings** to see setting options for Windows Defender Antivirus. New with Windows 10 is cloud-based protection. This feature allows Windows to share information with Microsoft about potential threats to your computer. This screen gives you the option to turn cloud-based protection off as well as to adjust other configuration options.

Other menus in the security center include the following:

- ▲ **Device performance & health.** Lists issues that might need attention, such as updates, drivers, or battery life (when applicable). This is also the screen where you can initiate a Fresh Start as discussed earlier in this chapter.
- ▲ **Firewall & network protection.** Gives limited options for changes and takes you to Windows Firewall in Control Panel for more detailed adjustments.
- ▲ **Apps & browser control.** Lets you set up SmartScreen settings for browsers and apps, such as warning or blocking when downloading files from the Web.
- ▲ **Family options.** Provides a link to the Microsoft website for making changes to parental controls and monitoring other Windows devices.

## APPLYING CONCEPTS

### USE WINDOWS DEFENDER OFFLINE

If you suspect your system is infected with malware but Defender has not detected it, you can run a security scan in a trusted environment offline. Windows Defender restarts the computer and looks for rootkits or other stubborn malware before Windows starts. To perform an offline scan, complete the following steps:

1. Save and close any open files, and close apps and programs.
2. Open **Windows Defender Security Center** as described above.
3. In the left pane, click **Virus & threat protection**, and then click **Advanced scan**.
4. Select **Windows Defender Offline scan**, click **Scan now** as shown in Figure 3-29, and then click **Scan** to confirm that you saved your work. If necessary, click **Yes** in the UAC dialog box. The computer automatically restarts, and Defender begins scanning the computer.

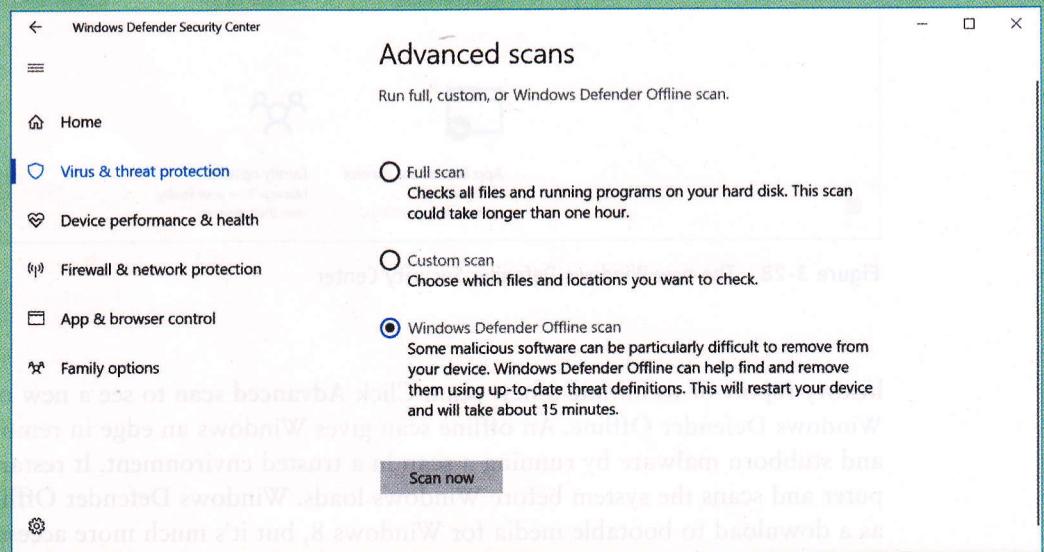


Figure 3-29 Be sure to close open files and apps before running Windows Defender Offline

5. After the scan is complete, and the computer restarts again, sign in.
6. To view the scan log, open **Windows Defender Security Center** again. Click the **Virus & threat protection** and click **Scan history**. If any threats are discovered by the scan, they'll be listed here.

## WINDOWS 10 SECURITY TECHNOLOGIES

BitLocker has been around since Windows Vista. With Windows 10, several changes were made under the hood to close loopholes and increase security of data stored under BitLocker encryption:

- ▲ Windows 10 BitLocker gives you two encryption options:
  - ▲ Legacy-compatible encryption primarily designed for removable devices that might need to be decrypted by older versions of Windows.
  - ▲ New and more secure encryption for encrypting installed storage devices.
- ▲ BitLocker is only available on Windows 10 Pro, Enterprise, and Education editions.

Like Windows 8.1, Windows 10 also includes an encryption tool related to BitLocker named **Device Encryption**. This tool can protect the system boot volume on a Windows 10 Home system. If the device's hardware qualifies, the first time an administrator signs in with a Microsoft account, the system automatically encrypts the system boot volume in the background without user intervention. Most desktop computers do not meet these requirements, but many tablets do. This helps make Windows 10 much more secure for these portable devices.

**To Learn More** To learn more about BitLocker, see pages 869–870 in Chapter 18 of *A+ Guide to IT Technical Support*, ninth edition, or pages 481–482 in Chapter 10 of *A+ Guide to Software*, ninth edition.

**Virtualization-based security (VBS)**, a new feature for Windows 10, uses the virtualization technology in Hyper-V to increase security of critical system components. For VBS to work, a 64-bit OS must be installed and UEFI Secure Boot enabled. Basically, VBS creates a virtualized container to hold key system processes and system data. The contents of these protected containers can only be changed through privileged access, making it more difficult for hackers to make system-level changes that would aid their intrusion efforts.

VBS enables two additional Windows 10 security features: Device Guard and Credential Guard, both of which are only available in Enterprise and Education editions. **Device Guard** restricts the applications allowed to run on a device to those included on an organization's whitelist (a list of allowed applications). **Credential Guard** uses Secure Boot and virtualization technology to store credentialing secrets, especially domain credentials, and the services that use those credentials run in an isolated virtual environment.



**Notes** VBS, Device Guard, and Credential Guard all require UEFI Secure Boot to work. UEFI requires a GPT partitioning system on the hard drive. Windows 10 includes the new **mbr2gpt.exe** command that converts an MBR partitioning system to GPT without affecting data on the drive.

## **SECURITY OPTIONS IN THE SETTINGS APP**

As a computer's security increases, its convenience generally decreases. The Settings app provides many options for finding the balance that works for you. Next, we'll explore some of the more significant security-related settings in the Settings app.

### **NETWORK & INTERNET SETTINGS**

By definition, networked computers share information with each other. The Network & Internet menu helps you determine how easily your computer will connect with a network and how accessible your data is to other computers on the network.

In the **Settings** app, click **Network & Internet**. Click each of the following items in the left pane to review security options on that screen:

- ▲ **Status.** Click **Sharing options** to change your network profile. This takes you to Control Panel where you can decide whether to treat the network as a private, guest, or public network for features such as network discovery, file and printer sharing, and HomeGroup connections.
- ▲ **Wi-Fi.** This screen allows you to manage the computer's network connection as well as some other important Wi-Fi options:
  - ▲ **Wi-Fi services** automatically connects your Windows 10 device to open Wi-Fi hotspots included in its crowdsourced database. Wi-Fi services selects from available hotspots by considering the strength of the Internet connection, the number of other Microsoft Wi-Fi services users connected to those hotspots, your past use of any available hotspots, and the strength and quality of the Wi-Fi signal at your location. You must sign in with a Microsoft account to use Wi-Fi services, although it might be turned on by default. In that case, you can click the slider button to turn it off.
  - ▲ **Hotspot 2.0**, also called HS 2.0 or Wi-Fi Certified Passpoint, is a mobile device authentication technology standardized by the Wi-Fi Alliance that allows easier transition between public Wi-Fi hotspots and between Wi-Fi and cellular networks. One purpose of this technology is to reduce the load on some cellular networks. As you roam into and between hotspots that support HS 2.0, your device can seamlessly authenticate to each network without requiring you to manually sign in to every new network. Ultimately, the goal is to make roaming into and out of Wi-Fi networks as carefree as switching between cellular networks is now.

### **PRIVACY SETTINGS**

When you use a Microsoft account with Windows 10, Microsoft keeps information about your account and activities on its servers, which Microsoft claims helps them provide the most valuable experience for their customers. This information, called **telemetry**, is considered by some to be an invasion of personal privacy. Therefore, the Settings app gives you options to limit what Microsoft keeps while maintaining functionality.

On the **Settings** app home screen, click **Privacy**. Click each of the following items in the left pane to review security options on that screen:

- ▲ **General.** These privacy options affect what data Microsoft and other apps can collect about a user's activity on the device. Notice one setting in particular: advertising ID. Your **advertising ID** is linked to your Microsoft account and collects information to personalize advertising. The data stored on Microsoft's servers can include browsing and search histories, a list of apps you download, location history, writing and speech patterns, contacts, calendar events, and device usage. Microsoft uses this data to provide interest-based advertising, which can show up both in your browser and

in Windows Store apps. Turning the advertising ID off opts you out of receiving these personalized ads, but it does not necessarily prevent the data from being collected.

- ▲ **Location.** At the top of this list is the option to turn location services on or off. You can also set a default location and clear location history for the device. Scroll farther down on the screen to set location permissions for specific apps.
- ▲ **Camera, Microphone, Notifications, Account info, Contacts, Calendar, Call history, Email, Messaging, Radios (such as Bluetooth), and Other devices.** Each of these screens provides a list of apps allowed to access each feature. You can disable all apps from using each of these tools, or grant access for specific apps.



**Notes** It's notoriously easy for an experienced hacker to access a device's camera and disable the light indicating the camera is in use so that you don't know your camera has been hijacked. For optimal security, cover your webcam with a piece of tape or sticky note when you're not using it.

- ▲ **Speech, inking, & typing.** Voice, writing style, speech patterns, handwriting, and typing style are all unique to each person. By collecting data on these behavioral patterns, Windows and Cortana can better predict your needs and preferences. To turn this off, and also disable dictation features, click **Stop getting to know me**.
- ▲ **Feedback & diagnostics.** To minimize data sent to Microsoft, select **Never** under **Feedback frequency**, and select **Basic** under **Diagnostic and usage data**. Here's a brief description of the diagnostic and usage data options:
  - ▲ **Basic.** This information is required for Windows to function. It includes information about your device, installed apps, and Windows errors.
  - ▲ **Full.** This option includes basic information as well as advanced diagnostic features and snapshots that might include personal data and parts of files that are open when the information is collected. Microsoft states that this data is not used to personalize advertising on your device.
- ▲ **Background apps.** You might want to disable apps you never use to prevent them from draining your battery or exchanging data in the background. If you're not sure what a particular app is, do an online search to determine whether it provides helpful services for you.



**Notes** Find out more about what personal data Microsoft collects and what they do with that data at [privacy.microsoft.com/en-us/privacystatement](http://privacy.microsoft.com/en-us/privacystatement).



**Notes** Additional privacy settings for Microsoft accounts are available at the website [choice.microsoft.com](http://choice.microsoft.com).

## UPDATE & SECURITY SETTINGS

The *Update & security* menu in the Settings app gives you access to the new Windows Defender Security Center, discussed earlier in this chapter. A couple of additional settings address options for sharing system update files and locating a lost device.

On the Settings app home screen, click **Update & security**. Click each of the following items in the left pane to review security options on that screen:

- ▲ **Windows Update.** Recall that Windows shares parts of pending updates with other computers in the interest of speeding up these downloads. You can choose not to

participate in this sharing, or restrict sharing to computers on your local network. To access these settings, on the *Update & security* pane click **Windows Update**. Click **Advanced options** and then click **Choose how updates are delivered**.

- ▲ **Find My Device.** Device location can be especially helpful if you've lost your device or if it's fallen into the wrong hands. However, this also means that the device's location is reported to Microsoft on a regular basis. It's up to you to decide whether this resource is worth the compromise on privacy. To ring, lock, or erase a phone, or to see any Windows device's location on a map, go to [account.microsoft.com/devices](http://account.microsoft.com/devices). Sign in if necessary, using the same account that is signed in to the device. Click a device and choose from the available options for that device.

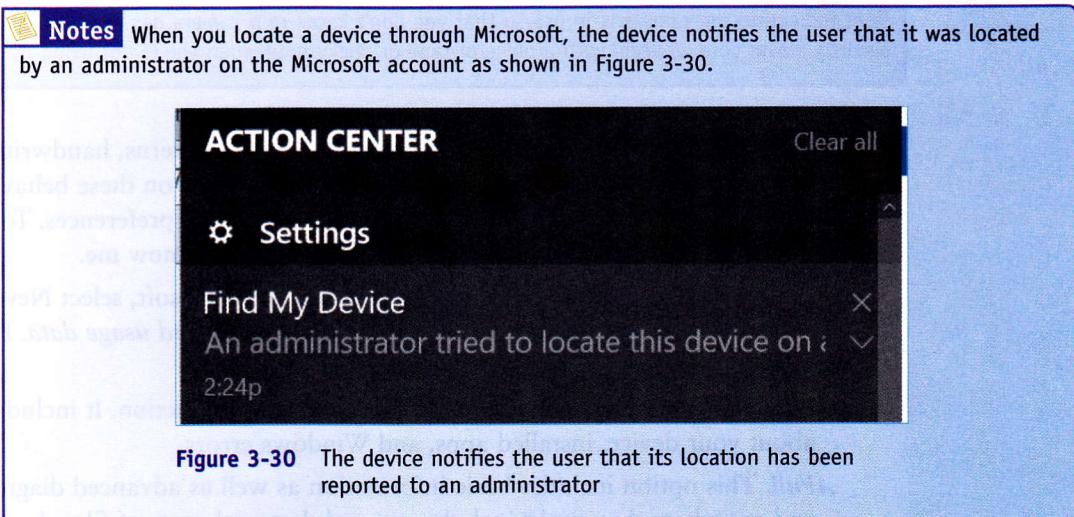


Figure 3-30 The device notifies the user that its location has been reported to an administrator

## SECURITY OPTIONS IN CORTANA

As you learned in the chapter “Survey of Windows Features and Support Tools” of this text, Cortana is the Windows digital assistant. To provide personalized assistance, Cortana has to collect a great deal of information about the user, such as speech and handwriting patterns, search history, usage statistics, and more. Some people are uncomfortable with the amount of data being collected and saved on Microsoft’s servers. You can’t completely turn Cortana off because it is essentially the Windows search app. However, you can better secure Cortana by adjusting its access to certain types of data.

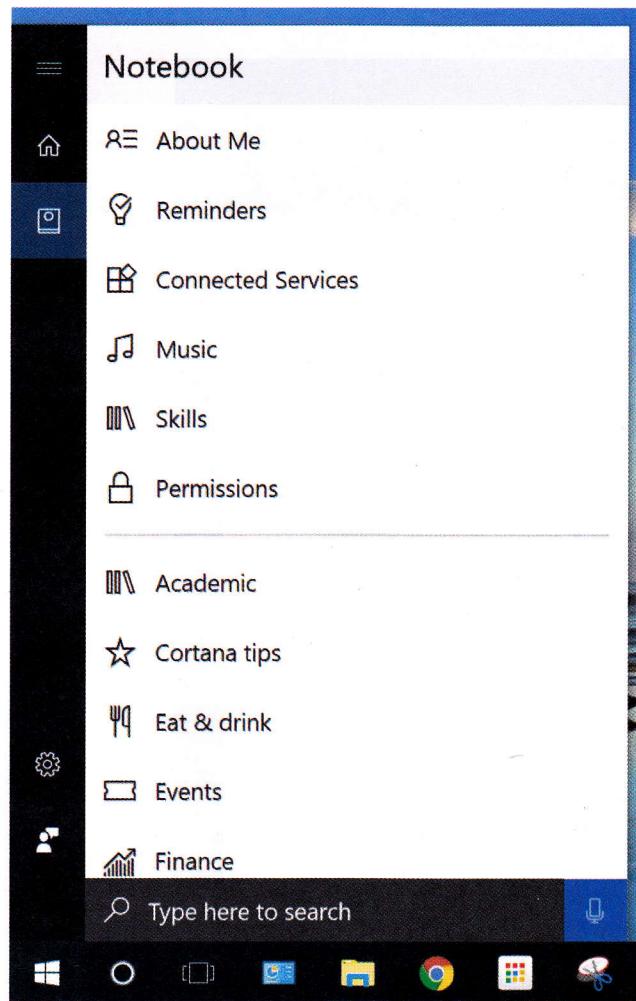
To change some of Cortana’s basic settings, click the Cortana search box in the taskbar, and then click the **Settings** icon in the left pane. Some options of particular interest include the following:

- ▲ **Lock screen.** Making Cortana available on your lock screen means that someone could use Cortana even without being able to sign in to your device. The more Cortana learns about you, the more of a privacy risk this becomes. You also have a separate option of whether to let Cortana access your calendar, email, and other data from the lock screen.
- ▲ **My device history.** Your historical data from other devices can be synced between devices. Click **Clear my device history** to remove this information.

At the bottom of the Cortana Settings menu, click **Other privacy settings** to open the Privacy menu in the Settings app, which you learned about earlier in this chapter. Return to

the Cortana settings menu, and then click **Learn more about Cortana & Search** to visit the Microsoft website where you can read about Cortana's privacy options.

If you're signed in to Cortana with a Microsoft account, additional settings are available. Click the **Cortana** search box in the taskbar, and then click the **Notebook** icon in the left pane (see Figure 3-31). If this is the first time you've viewed your Notebook, click **Personalize**. Some options of interest include the following:

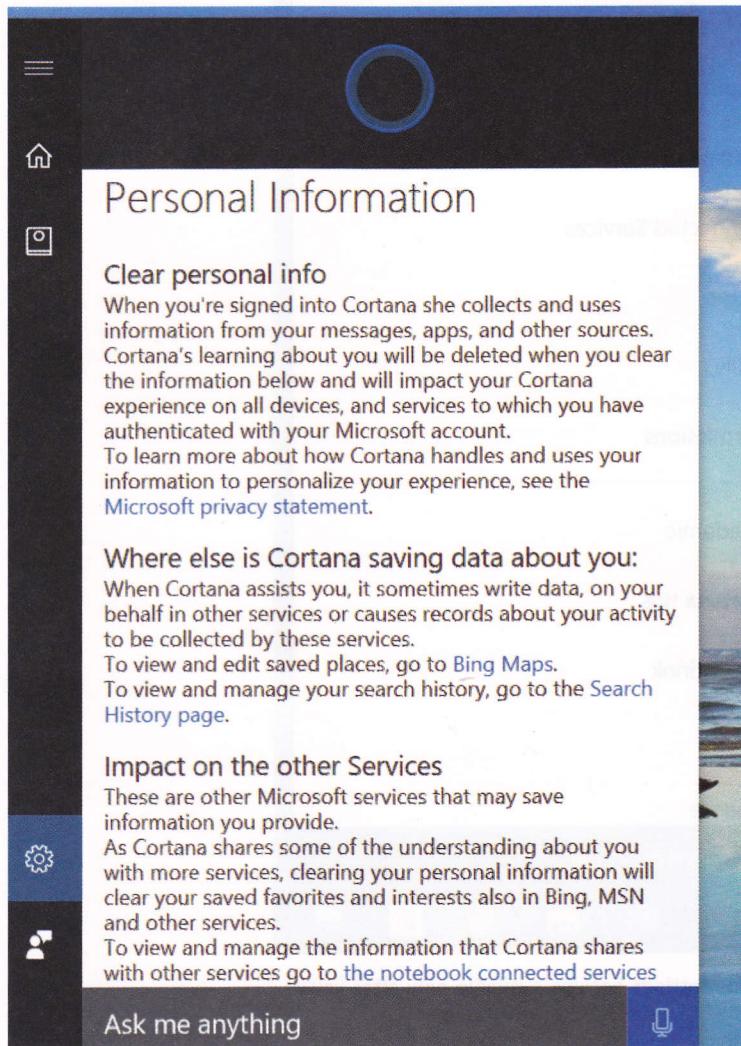


**Figure 3-31** Some settings become available only after you've signed in with a Microsoft account

- **About Me.** This item gives you the option to sign out of Cortana. To do so, click your Microsoft account. On the next screen, click your Microsoft account again, and then click **Sign out**.
- **Permissions.** Use the Permissions screen to enable or disable data collection for location, contacts, email, calendar, communication history including text messages, and browsing history.
- **Areas of interest.** To disable an area of interest, click the item you want to change and set the slider button to off.

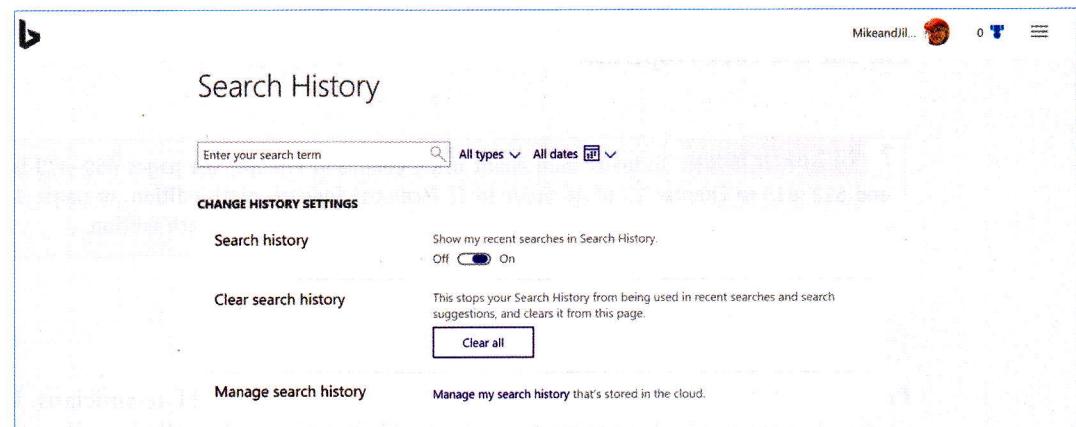
 **Notes** Read more about Cortana and your privacy at [privacy.microsoft.com/en-us/windows-10-cortana-and-privacy](https://privacy.microsoft.com/en-us/windows-10-cortana-and-privacy).

Cortana also stores information about you on Bing's servers. To access this information and adjust those settings, click the Cortana icon in the taskbar, and then click the Settings icon. Click **Change what Cortana knows about me in the cloud**. This opens the Personal Information screen, as shown in Figure 3-32, where you'll find a few links of interest.



**Figure 3-32** View or clear information Cortana has saved about you in the cloud

- ▲ Click **Bing Maps** to view, edit, or remove your saved places, such as home or work.
- ▲ Click **Search History page** to view, manage, or remove items in your Bing search history. On Bing's search history page, you can click **CHANGE HISTORY SETTINGS** to adjust these settings as shown in Figure 3-33.
- ▲ Scroll to the bottom of Cortana's Personal Information screen and click **Clear** to delete what Cortana knows about you.



**Figure 3-33** Use this screen to search your history or to stop saving this data



**Notes** Explore Bing privacy settings related to your Cortana use at [bing.com/account/personalization](http://bing.com/account/personalization).

## WINDOWS 10 COMMAND-LINE INTERFACES

3

As you become more comfortable with command-line interfaces, you'll find they can be more flexible and convenient than a graphical interface, especially for those commands you use frequently. Microsoft continues to make significant improvements to command-line options in Windows, including increased emphasis on PowerShell and the addition of a Linux shell. The three command-line interfaces (CLI) offered by Windows 10 are the Command Prompt, PowerShell, and Linux shell interfaces. First, let's look at changes made to Command Prompt and PowerShell, and then we'll see how the Linux shell works in Windows 10.



**Notes** This portion of the chapter is written to follow Chapter 20 in *A+ Guide to IT Technical Support*, ninth edition, or Chapter 11 in *A+ Guide to Software*, ninth edition.

### POWERSHELL AND COMMAND PROMPT

Both PowerShell and Command Prompt function about the same in Windows 10 as they did in Windows 8. However, PowerShell was restructured under the hood to reduce its **attack surface**—that is, how vulnerable it is to an attack. In addition, new commands and parameters have been added to both PowerShell and Command Prompt as well as some options for user interaction.

Here are a few of the changes Windows 10 made to both PowerShell and Command Prompt:

- ▲ **Full screen mode.** New to Windows 10, you can maximize the Command Prompt or PowerShell window so it takes up the entire screen.
- ▲ **Opacity.** When working with multiple windows in a limited display space, you can reduce the opacity (transparency) of the Command Prompt or PowerShell window so you can see one window while working in another.
- ▲ **Ctrl key shortcuts.** Ctrl key shortcuts, such as Ctrl+C (copy), Ctrl+V (paste), Ctrl+A (select all), and Ctrl+F (find) can now be enabled in Command Prompt and PowerShell windows.

To access opacity, Ctrl key shortcuts, and other features for either utility, right-click the title bar and click **Properties**.

 **To Learn More** To learn more about using Command Prompt, see pages 469–479 in Chapter 10 and 612–613 in Chapter 13 of *A+ Guide to IT Technical Support*, ninth edition, or pages 133–143 in Chapter 3 and pages 276–277 in Chapter 6 of *A+ Guide to Software*, ninth edition.

## POWERSHELL CMDLETS

PowerShell skills are becoming increasingly important for all IT technicians. In this part of the chapter, we look at some basic PowerShell commands, called **cmdlets** (pronounced “command-lets”), as a starting point to help you warm up to PowerShell.

 **To Learn More** To learn more about Windows PowerShell, see pages 479 in Chapter 10 of *A+ Guide to IT Technical Support*, ninth edition, or pages 143 in Chapter 3 of *A+ Guide to Software*, ninth edition.

Native PowerShell cmdlet syntax almost always starts with a verb followed by a noun and connected with a hyphen, as in *verb-noun*. For example, consider the cmdlet `Get-ChildItem`. The *Get* verb defines the action and the *ChildItem* noun defines the object of that action. “Get” simply means to retrieve something; an item is a file or folder, and “ChildItem” is any item within another item. So the cmdlet `Get-ChildItem` retrieves items in one or more specified locations, similar to how `dir` works at the Command Prompt. `Set`, `Copy`, and `Remove` are other verb options. Other noun options include `Help`, `Location`, `Content`, `Process`, and `Service`. With this information, you can deduce several helpful cmdlets as shown in Table 3-2.

Cmdlet	Description
<code>Get-Item</code>	Retrieves files and folders
<code>Get-Process</code>	Retrieves the processes running on a computer
<code>Set-Location</code>	Changes the current working location to a specified location
<code>Copy-Item</code>	Copies an item to a specified location
<code>Remove-Item</code>	Deletes an item
<code>Get-Verb</code>	Shows a list of all cmdlet verbs
<code>Get-Verb *-Location</code>	Shows a list of all cmdlet verbs available for a specific noun, where the asterisk is a wild card in place of any verb attached to the noun <i>Location</i>
<code>Get-Command</code>	Shows a list of all available cmdlets

Table 3-2 Common PowerShell cmdlets

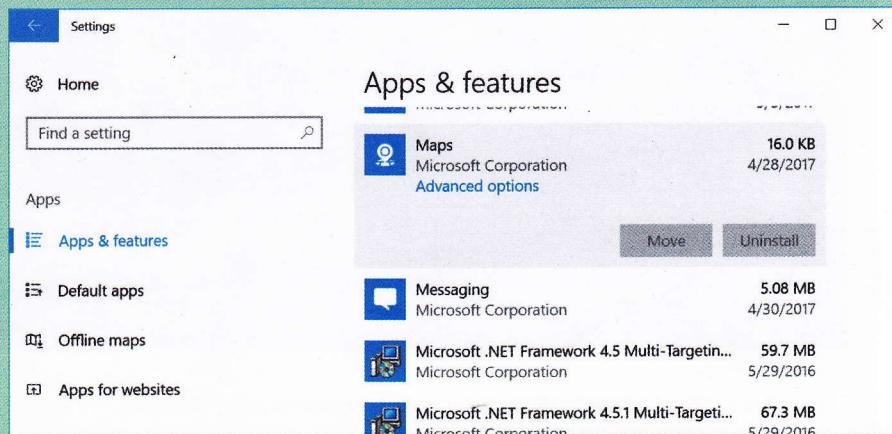
 **Notes** PowerShell cmdlets are not case sensitive. You can type `Get-Item` or `get-item` and you'll get the same result.

## APPLYING CONCEPTS USE POWERSHELL

As you learned earlier in this chapter, Fresh Start allows you to install a clean copy of Windows and can be used to remove manufacturer-installed apps, which are sometimes referred to as bloatware. However, even a clean copy of Windows comes with several apps that you might not want and that cannot be removed through the Settings app. For example, you might not want Xbox installed on a computer you use for work. An alternative to the Settings app is to use PowerShell to uninstall unwanted apps.

Complete the following steps to install an app from the Windows Store and then remove it using PowerShell:

1. Open the **Windows Store** and find a simple app to install, such as Dropbox. Click **Get** to download and install the app. Close the Windows Store.
2. Open the **Settings** app and click **Apps**.
3. Scroll down to the app you just installed. In most cases, you can use this window to remove the app, but some apps can't be uninstalled from here. For example, as shown in Figure 3-34, the **Uninstall** button is grayed out for the Maps app.



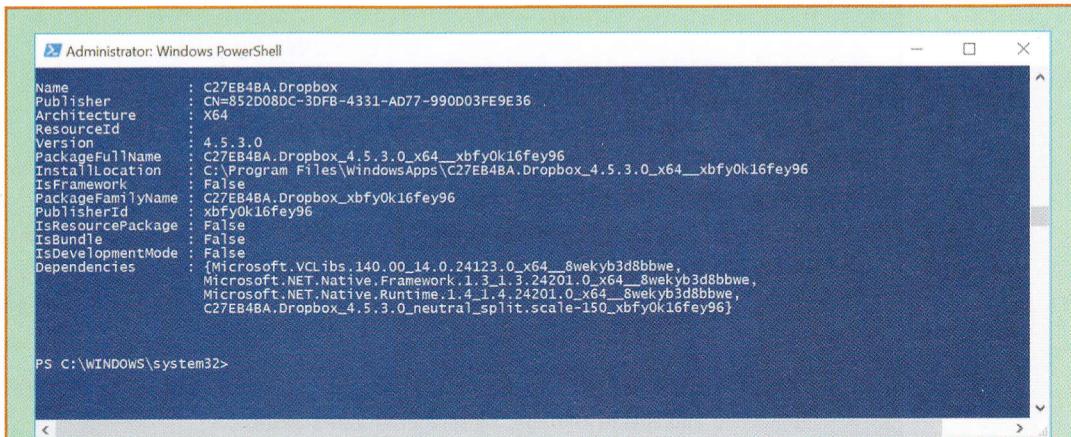
**Figure 3-34** Some apps cannot be uninstalled from the Settings window

4. Open an elevated PowerShell window. To do this, right-click **Start** and click **Windows PowerShell (Admin)**. If needed, click **Yes** in the UAC dialog box.

**Notes** By default, Windows 10 with the Creators Update lists Windows PowerShell in the Quick Launch menu instead of Command Prompt. You can use the Settings app to change this setting. Click **Personalization** and then click **Taskbar**. Scroll down and turn the slider button to **Off** under *Replace Command Prompt with Windows PowerShell in the menu when I right-click the start button or press Windows key+X*.

Regardless of which app is listed in the Quick Launch menu, both Command Prompt and PowerShell can be accessed in the All apps list on the Start menu. You might also want to pin one or both to your taskbar.

5. Enter **Get-AppxPackage** to see a list of all apps installed for the current user. Wade through and find the entry for the app you just installed. (It's most likely at the bottom of the list since you just installed it.) For example, Figure 3-35 shows Dropbox installed on the system.

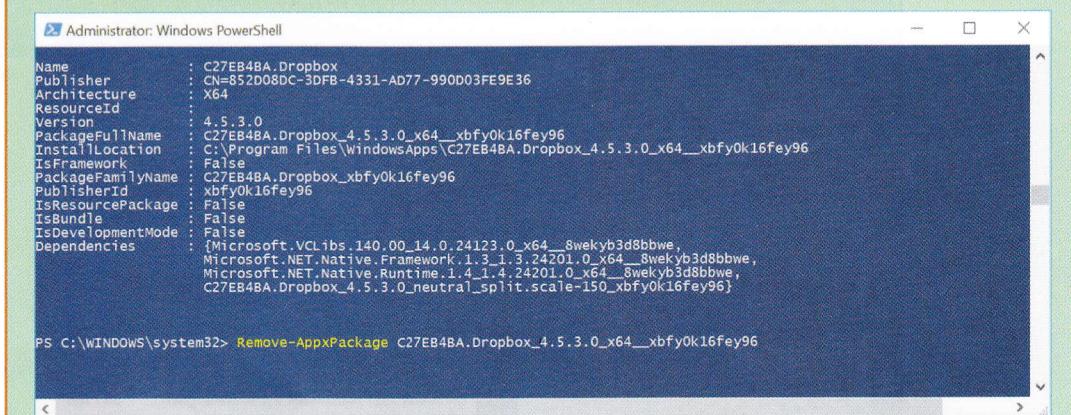


```
Administrator: Windows PowerShell
Name : C27EB4BA.Dropbox
Publisher : CN=852D08DC-3DFB-4331-AD77-990D03FE9E36
Architecture : X64
ResourceId : 4.5.3.0
PackageFullName : C27EB4BA.Dropbox_4.5.3.0_x64_xbfy0k16fey96
InstallLocation : C:\Program Files\windowsApps\C27EB4BA.Dropbox_4.5.3.0_x64_xbfy0k16fey96
IsFramework : False
PackageFamilyName : C27EB4BA.Dropbox_xbfy0k16fey96
PublisherId : xbfy0k16fey96
IsResourcePackage : False
IsBundle : False
IsDevelopmentMode : False
Dependencies : {Microsoft.VCLibs.140.00_14.0.24123.0_x64_8wekyb3d8bbwe,
Microsoft.NET.Native.Framework.1.3.1_3.24201.0_x64_8wekyb3d8bbwe,
Microsoft.NET.Native.Runtime.1.4_1.4.24201.0_x64_8wekyb3d8bbwe,
C27EB4BA.Dropbox_4.5.3.0_neutral_split.scale-150_xbfy0k16fey96}

PS C:\WINDOWS\system32>
```

**Figure 3-35** Find the app you just installed

6. Select and copy the text for the PackageFullName field of the app to be removed. Enter the command `Remove-AppxPackage <PackageFullName>` as shown in Figure 3-36.



```
Administrator: Windows PowerShell
Name : C27EB4BA.Dropbox
Publisher : CN=852D08DC-3DFB-4331-AD77-990D03FE9E36
Architecture : X64
ResourceId : 4.5.3.0
PackageFullName : C27EB4BA.Dropbox_4.5.3.0_x64_xbfy0k16fey96
InstallLocation : C:\Program Files\windowsApps\C27EB4BA.Dropbox_4.5.3.0_x64_xbfy0k16fey96
IsFramework : False
PackageFamilyName : C27EB4BA.Dropbox_xbfy0k16fey96
PublisherId : xbfy0k16fey96
IsResourcePackage : False
IsBundle : False
IsDevelopmentMode : False
Dependencies : {Microsoft.VCLibs.140.00_14.0.24123.0_x64_8wekyb3d8bbwe,
Microsoft.NET.Native.Framework.1.3.1_3.24201.0_x64_8wekyb3d8bbwe,
Microsoft.NET.Native.Runtime.1.4_1.4.24201.0_x64_8wekyb3d8bbwe,
C27EB4BA.Dropbox_4.5.3.0_neutral_split.scale-150_xbfy0k16fey96}

PS C:\WINDOWS\system32> Remove-AppxPackage C27EB4BA.Dropbox_4.5.3.0_x64_xbfy0k16fey96
```

**Figure 3-36** The PackageFullName field must be typed exactly; therefore, it's easiest to copy and paste

7. Enter the command `Get-AppxPackage` to confirm the app was removed. Also check the Settings app to make sure the app is no longer listed there.
8. Enter `exit` to close the PowerShell session.

Here are some other basic cmdlet features you should know:

- ▲ **Aliases for Command Prompt commands.** An **alias** is a nickname or shortcut for a cmdlet. For convenience, many of the commands you're accustomed to using in a Command Prompt window also work in PowerShell. These Command Prompt commands are defined as aliases for native PowerShell cmdlets. For example, one default alias for `Get-ChildItem` is `dir`. Therefore, you can enter `dir` in PowerShell to execute the `Get-ChildItem` cmdlet. Note that an alias applies only to the referenced command and does not include parameters or values (such as a filename) that might be used by the command.

**Notes** You can create your own aliases using the `Set-Alias` and `New-Alias` cmdlets. For example, `Set-Alias show Get-ChildItem` assigns the alias `show` to the cmdlet `Get-ChildItem`.

- ▲ **List aliases.** The cmdlet `Get-Alias` shows all the available aliases in the current session, including the default aliases and other aliases you created during the session.

- ▲ **Help.** To find the cmdlet assigned to a specific alias, use the Help cmdlet (also called Get-Help). For example, enter **Help dir** to see the output shown in Figure 3-37. Here you can see that dir is an alias for Get-ChildItem.

```

Windows PowerShell
PS C:\Users\jill west> help dir

NAME
    Get-ChildItem

SYNTAX
    Get-ChildItem [[-Path] <string[]>] [[-Filter] <string>] [-Include <string[]>] [-Exclude <string[]>] [-Recurse]
    [-Depth <uint32>] [-Force] [-Name] [-UseTransaction] [-Attributes {ReadOnly | Hidden | System | Directory |
    Archive | Device | Normal | Temporary | SparseFile | ReparsePoint | Compressed | Offline | NotContentIndexed |
    Encrypted | IntegrityStream | NoScrubData}] [-Directory] [-File] [-Hidden] [-ReadOnly] [-System]
    [<CommonParameters>]

    Get-ChildItem [[-Filter] <string>] -LiteralPath <string[]> [-Include <string[]>] [-Exclude <string[]>] [-Recurse]
    [-Depth <uint32>] [-Force] [-Name] [-UseTransaction] [-Attributes {ReadOnly | Hidden | System | Directory |
    Archive | Device | Normal | Temporary | SparseFile | ReparsePoint | Compressed | Offline | NotContentIndexed |
    Encrypted | IntegrityStream | NoScrubData}] [-Directory] [-File] [-Hidden] [-ReadOnly] [-System]
    [<CommonParameters>]

ALIASES
    gci
    ls
    dir

REMARKS
    Get-Help cannot find the Help files for this cmdlet on this computer. It is displaying only partial help.
    -- To download and install Help files for the module that includes this cmdlet, use Update-Help.
    -- To view the Help topic for this cmdlet online, type: "Get-Help Get-ChildItem -Online" or
    go to http://go.microsoft.com/fwlink/?LinkId=113308.

PS C:\Users\jill west>

```

**Figure 3-37** Dir, gci, and ls are all aliases for Get-ChildItem



**Notes** At the bottom of Figure 3-37 a message informs the user that the Help files for the cmdlet are not available on the computer. This is because you must install the PowerShell help files to access them. To do this, open an elevated PowerShell window. Type **Update-Help** and press **Enter**. The process will take a few minutes. When you return to the PowerShell prompt, enter **Help dir** again to see how much additional information you have access to.

- ▲ **Parameters.** The current version of PowerShell in Windows 10, as of the Creators Update, is 5.1. A new parameter as of PowerShell 5.0 is the **-Depth** parameter on the Get-ChildItem cmdlet. This parameter allows you to specify how many layers to search in the targeted location to retrieve child items. To use this parameter, you must also use the **-Recurse** parameter, which instructs PowerShell to retrieve items within child items (such as files within folders) at the targeted location. For example, **Get-ChildItem -Recurse -Depth 2** delivers a list of items in the current folder, that folder's child folders, and folders within those child folders, but no deeper than two child layers of folders. The following Hands-On Project will help you understand how this works.

## >> HANDS-ON PROJECT

### PROJECT 3-5: Explore the Get-ChildItem Cmdlet

Complete the following steps to practice using parameters with the Get-ChildItem cmdlet:

1. Open a PowerShell window. By default, you begin at the home directory of your user account.
2. Enter the cmdlet **Get-ChildItem**. This produces a list of files and folders in your user's home directory.
3. By adding the **-recurse** parameter, you can retrieve a list of files and folders that also shows the contents of those folders. To do this, enter the cmdlet **Get-ChildItem -recurve**.

If you have many files and folders stored in your user account, it might take a while for this output to scroll by on your screen. Press **Ctrl+C** to stop the output.

4. Instead of listing all the contents of all of the folders in your user account, you might want to limit the depth of that information to only one or two layers. Here's where the **-depth** parameter comes in. Enter the cmdlet **Get-ChildItem -recurse -depth 1** and compare the output this time to the extensive output you received in the previous step.
5. You can also limit the search to only certain types of files in a particular location. Here, let's combine the **-recurse** parameter with the **-include** parameter to list all the **.jpg** and **.png** files in your Pictures folder. Using your own username, enter the cmdlet **Get-ChildItem -recurse c:\users\username\Pictures\\*.\* -include \*.jpg,\*.png** as shown in Figure 3-38. This instructs Windows to search the Pictures folder and its subfolders for files of any name and type, but to list only those files with the **.jpg** or **.png** file type. (The **-exclude** parameter would show all file types *except* those listed in the cmdlet.)

Mode	LastWriteTime	Length	Name
-a---	5/8/2017 2:23 PM	135052	22_systemNEW.png
-a---	5/10/2017 2:30 PM	85474	52_developNEW.png
-a---	12/4/2016 12:12 PM	630870	A_TV01.png
-a---	5/26/2017 1:13 PM	103779	fireplace.jpg
-a---	5/8/2017 9:11 PM	103204	freshstart01.png
-a---	5/26/2017 1:11 PM	235659	front porch.jpg
-a---	5/26/2017 1:12 PM	178792	garden.jpg
-a---	5/26/2017 1:13 PM	99910	gardenwindow.jpg
-a---	11/7/2016 2:40 PM	31282	image.png
-a---	11/22/2016 7:30 PM	73096	iso.png
-a---	11/18/2016 9:52 AM	40407	project03.PNG
-a---	11/7/2016 2:44 PM	71133	repair.png
-a---	5/26/2017 1:12 PM	195451	snowyhouse.jpg
-a---	5/26/2017 1:11 PM	84984	stainedglasswindow.jpg
-a---	10/2/2016 9:45 AM	109920	updateoptions1.png
-a---	10/23/2016 1:16 PM	25119	wrap.png
-a---	5/26/2017 1:12 PM	143421	Zackonbike.jpg

**Figure 3-38** The **-recurse** parameter shows the contents of listed folder, and the **-include** parameter limits the output to only the file types given in the cmdlet

6. The output of a cmdlet can be piped, or fed for immediate use, into another cmdlet in the same entry. Suppose you want to sort those picture files by size rather than by filename. Enter the cmdlet **Get-ChildItem -recurse c:\users\username\Pictures\\*.\* -include \*.jpg,\*.png | Sort-Object length**. By default, this shows the files in ascending order.
7. To sort in descending order instead, specify the **-descending** parameter: **Get-ChildItem -recurse c:\users\username\Pictures\\*.\* -include \*.jpg,\*.png | Sort-Object length -descending**.

## UBUNTU BASH ON WINDOWS

In response to customer feedback, Microsoft built a Linux shell into Windows 10 that provides a shell prompt to enter Linux commands. Note that this shell is not a VM, and it's not a fully separate operating system, but rather a shell that allows users to interact with underlying Windows functions and system files. The new shell requires a Windows component, **Windows Subsystem for Linux (WSL)**, to support it. WSL installs a subset of the Ubuntu distribution of Linux, which is one of the most popular distributions. By default, Ubuntu provides Bash, which is its most popular shell. This shell is called **Bash on Ubuntu on Windows**, Bash on Windows, or Ubuntu Bash. (It's possible to install other Ubuntu shells

by using switcher software in PowerShell.) Many Linux commands work in WSL running Ubuntu Bash.

WSL runs on any 64-bit Windows 10 system with the Anniversary Update build 14393 or later. You must first turn on Developer Mode, and then enable the Windows Subsystem for Linux (Beta) feature. As its name suggests, this feature is still in beta as Microsoft continues to resolve many bugs and gaps in compatibility.

**To Learn More** To learn more about Linux distros and commands, see pages 972–985 in Chapter 20 of *A+ Guide to IT Technical Support*, ninth edition, or pages 530–543 in Chapter 11 of *A+ Guide to Software*, ninth edition.

## APPLYING CONCEPTS

### ENABLE WINDOWS SUBSYSTEM FOR LINUX (WSL) AND INSTALL UBUNTU BASH

Complete the following steps to enable Windows Subsystem for Linux and install Ubuntu Bash on a Windows 10 system:

1. First, turn on Developer Mode.
  - a. Open the **Settings** app and click **Update & security**. In the left pane, scroll down and click **For developers**.
  - b. Select **Developer mode** as shown in Figure 3-39. Click **Yes** to turn on Developer Mode and close the Settings app.

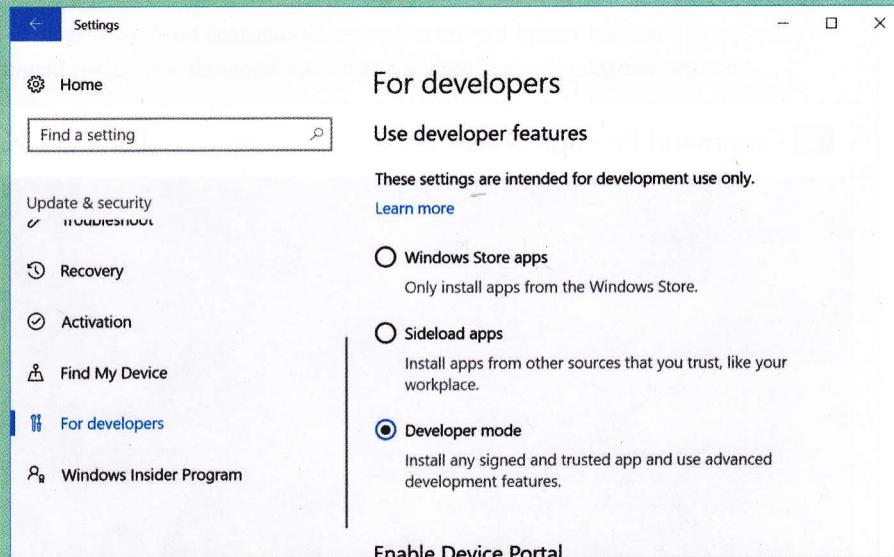
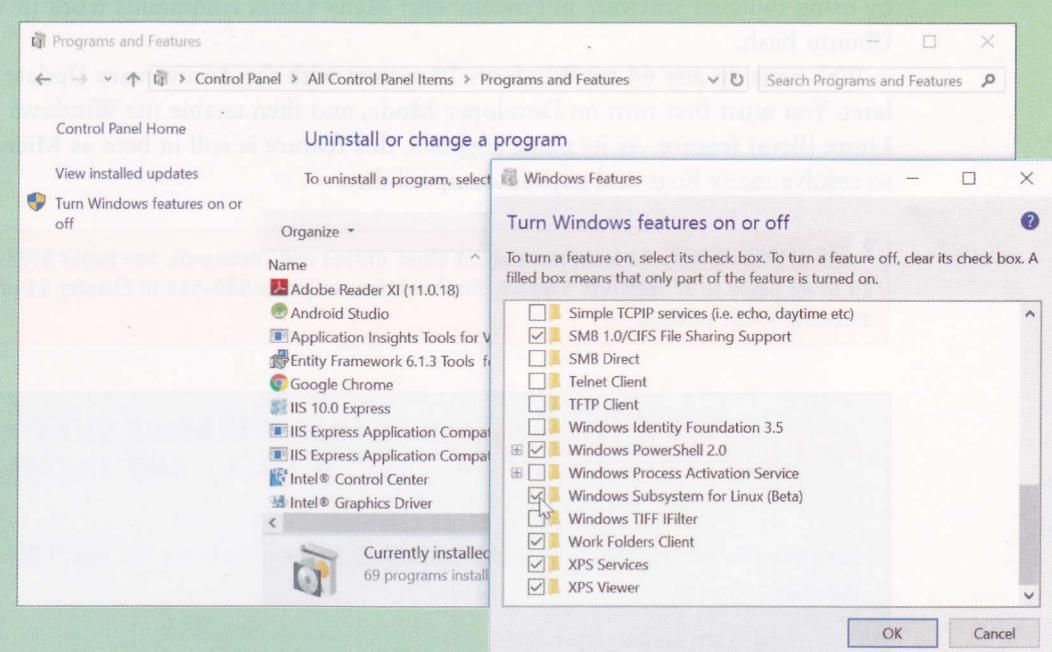


Figure 3-39 Turn on Developer Mode from the Settings app

2. Enable Windows Subsystem for Linux.
  - a. Open **Control Panel** and click **Programs and Features**. In the left pane, click **Turn Windows features on or off**.

**Notes** To open the *Turn Windows features on or off* window, you can also click **Start**, begin typing **turn Windows**, and then click **Turn Windows features on or off**.

- b. Scroll down and click **Windows Subsystem for Linux (Beta)** as shown in Figure 3-40. Click **OK**.



**Figure 3-40** Turn on the Windows Subsystem for Linux (Beta) feature

- c. Restart the computer when the changes are complete to finish enabling Windows Subsystem for Linux.
3. Install and run Bash on Ubuntu on Windows from the command prompt.
  - a. Open a Command Prompt window and enter the command **bash** (see Figure 3-41). Note that the first time you enter the bash command, Windows downloads and installs Ubuntu on Windows.

```
C:\Users\Jill West>bash
-- Beta feature --
This will install Ubuntu on Windows, distributed by Canonical
and licensed under its terms available here:
https://aka.ms/uowterms

Type "y" to continue: y
Downloading from the Windows Store... 100%
Extracting filesystem, this will take a few minutes...
Please create a default UNIX user account. The username does not
need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: JillWest
Enter new UNIX password:
```

**Figure 3-41** The first time you enter the bash command, Windows will download and install Ubuntu on Windows

- b. Enter **y** to accept the installation terms. Bash on Ubuntu on Windows downloads from the Windows Store, and then is extracted, and installed. This might take several minutes.
- c. Enter a new UNIX username at the prompt. This username can be different from your Windows username.

- d. Enter a password at the next prompt. The cursor will not move as you type the password. Re-enter the password at the next prompt.
- e. After the installation is complete, Windows switches to the Bash on Ubuntu environment with its shell prompt within the Command Prompt window as shown in Figure 3-42.

```

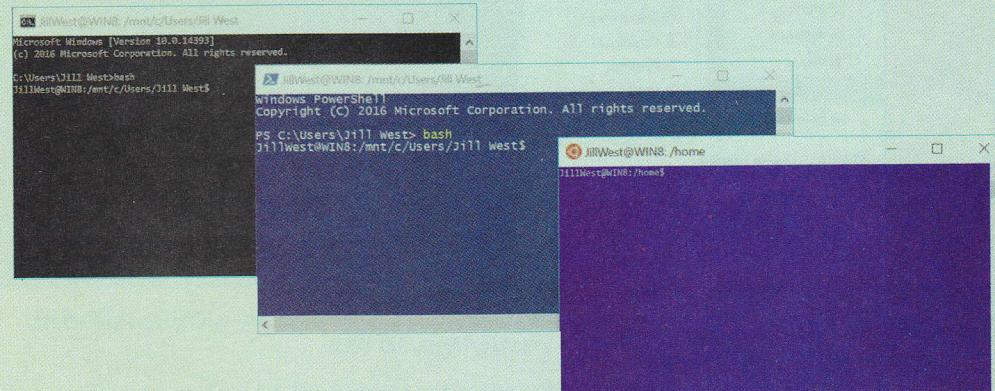
C:\JillWest@WIN8: /mnt/c/Users/Jill West
C:\Users\Jill West>bash
-- Beta feature --
This will install Ubuntu on Windows, distributed by Canonical
and licensed under its terms available here:
https://aka.ms/uowterms

Type "y" to continue: y
Downloading from the Windows Store... 100%
Extracting filesystem, this will take a few minutes...
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: JillWest
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Installation successful!
The environment will start momentarily...
Documentation is available at: https://aka.ms/wsldocs
JillWest@WIN8:/mnt/c/Users/Jill West$
```

3

**Figure 3-42** Bash on Ubuntu on Windows is installed and provides a shell prompt

- f. You can continue to interact with the Ubuntu Bash from the Command Prompt window, or you can open Bash on Ubuntu on Windows in a separate window. To do this, click **Start**, and then click **Bash on Ubuntu on Windows** in the Start menu. You can also open Bash from within PowerShell. See Figure 3-43 to compare the three windows.



**Figure 3-43** Bash on Ubuntu can be accessed from Command Prompt, PowerShell, or its own app, Bash on Ubuntu on Windows

At this point, most of the Linux commands you've become familiar with will work as usual at the Ubuntu shell prompt. The commands interact with the underlying Windows system files, and changes to those files can be monitored through other Windows tools.



**Notes** Linux commands are case sensitive. If you enter `Ifconfig`, you'll get an error message.

## &gt;&gt; HANDS-ON PROJECT

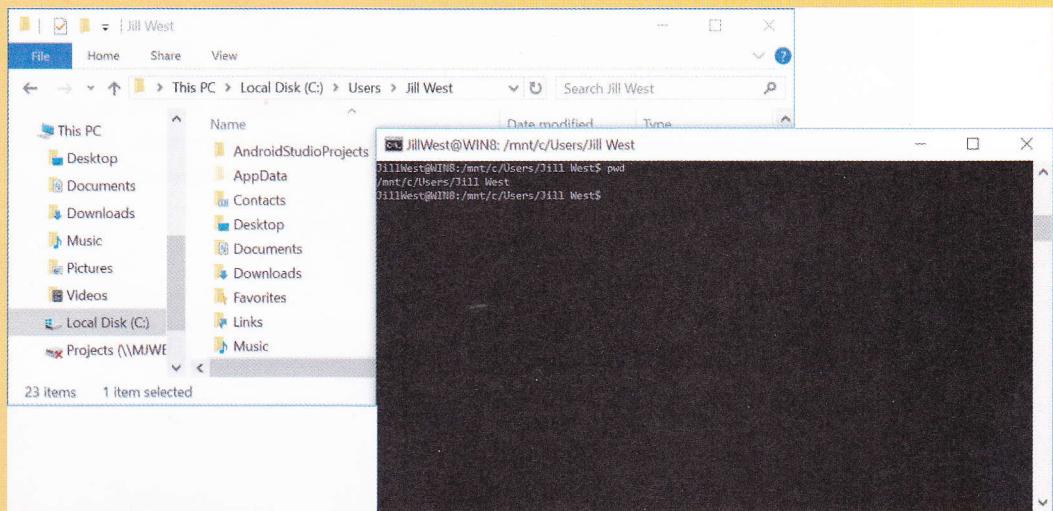
**PROJECT 3-6:** Use Ubuntu Bash on Windows

Let's see how commands entered through the Ubuntu Bash affect Windows files. This project assumes you have already enabled Windows Subsystem for Linux and installed the Bash on Ubuntu on Windows software. Complete the following steps:



**Notes** Many of these steps correspond with the Hands-On Project on page 981 in Chapter 20 of the *A+ Guide to IT Technical Support*, ninth edition, or on page 539 in Chapter 11 of the *A+ Guide to Software*, ninth edition. If you have the available resources, consider completing these projects at the same time on side-by-side computers to compare the results when using Ubuntu on a VM versus Bash on Ubuntu on Windows.

1. Open a Command Prompt window. Type **bash**, and press **Enter**.
2. At the Ubuntu shell prompt, enter the command **pwd** to see the full path of the current directory. Note that in the Ubuntu environment, the C: drive is referred to as /mnt/c. In a second window, open File Explorer and navigate to the current user's home directory. In Figure 3-44, in the Ubuntu window, the command output indicates the current directory is on drive C: in user Jill West's folder. File Explorer shows the same location.



**Figure 3-44** On this computer, the current user's home directory is C:\Users\Jill West, which in Ubuntu is /mnt/c/Users/Jill West

3. At the Ubuntu shell prompt, enter the command **ls -l** to see a list of files and directories in the current directory. Compare the information in the File Explorer window with the data listed in the Ubuntu window. What differences do you notice?
4. At the Ubuntu shell prompt, enter the command **mkdir mydir**. In File Explorer, confirm that a new folder named mydir has been created.
5. At the Ubuntu shell prompt, enter the command **cd mydir** to go to the directory you just created. In File Explorer, double-click the mydir folder to open it.
6. At the Ubuntu shell prompt, enter the command **touch myfile** to create a blank file named myfile in the current directory. In File Explorer, confirm the new file myfile has been created.
7. At the Ubuntu shell prompt, enter the command **ls** to list current directory contents as shown in Figure 3-45.

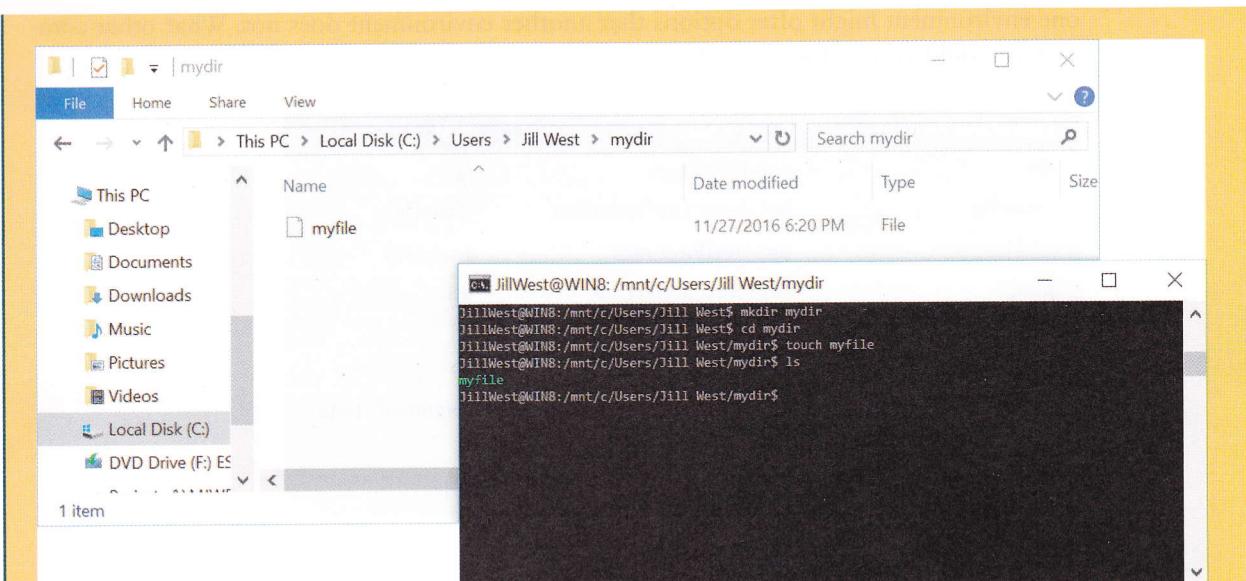


Figure 3-45 File Explorer reflects all the directory and file changes made at the Ubuntu shell prompt

8. At the Ubuntu shell prompt, enter the command `cd ..` to move up one level in the directory tree. In File Explorer, return to the user's home directory.
9. At the Ubuntu shell prompt, enter the command `cd /home` to change to the home directory. Enter the command `ls` to examine the contents of the home directory. Where do you think this directory is located in File Explorer?
10. At the Ubuntu shell prompt, enter the command `ping 127.0.0.1` to ping the loopback address. Press `Ctrl+C` to stop the output.
11. At the Ubuntu shell prompt, enter the command `ifconfig` to display TCP/IP configuration data. How many network interfaces are listed?
12. At the Ubuntu shell prompt, enter the command `man ifconfig` to display the Ubuntu Manual for the ifconfig command. What option is used to show all interfaces, including those that are down? Press `Q` to exit.
13. At the Ubuntu shell prompt, enter the command `lsb_release -a` to see information about the current Linux distro. What release is your computer using? What is its codename?
14. At the Ubuntu shell prompt, enter the command `exit` to log out of Ubuntu and return to the Windows command prompt.

On a normal Ubuntu system, you can use `sudo` before a command to execute the command with administrative privileges. However, in the WSL environment, Ubuntu only has the same privileges as the hosting command prompt. To run Ubuntu with administrator privileges, open Bash from an elevated command prompt or, in the Start menu, right-click **Bash on Ubuntu on Windows**, select **More**, and click **Run as administrator**.

It might seem like you're learning three different languages when you try switching between Command Prompt, PowerShell, and Linux. Table 3-3 gives a quick look at some of the most familiar commands in Command Prompt, allowing you to compare them to similar commands in PowerShell and Linux. Keep in mind that each command will function differently in its respective environment and also will offer various options and limitations. What's really interesting is to explore the extent of these differences and learn how a command in

one environment might offer options that another environment does not. What other commands would you add to this list?

Command Prompt	PowerShell	WSL
<code>dir</code>	<code>Get-ChildItem</code>	<code>ls</code>
<code>ipconfig</code>	<code>Get-NetIPConfiguration</code>	<code>ifconfig</code>
	<code>Get-NetIPAddress</code>	<code>iwconfig</code>
<code>ping</code>	<code>Test-NetConnection</code>	<code>ping</code>
<code>cd</code>	<code>Set-Location</code>	<code>cd</code>
<code>tasklist</code>	<code>Get-Process</code>	<code>ps</code>
<code>help command</code> <code>command /?</code>	<code>Get-Help command</code>	<code>command -help</code>
<code>exit</code>	<code>Exit</code>	<code>exit</code>

Table 3-3 Common commands in three CLIs

## >> CHAPTER SUMMARY

### Strategies for Troubleshooting Windows 10

- ▲ Tools for troubleshooting Windows after it starts normally include Task Manager, Event Viewer, System Restore, Memory Diagnostics, System File Checker, Check Disk, Windows troubleshooters, repair upgrade, earlier version, Fresh Start, and Windows reset.
- ▲ Windows RE can be used to troubleshoot problems that prevent Windows from starting or starting with errors.
- ▲ Windows RE can be launched from the Settings app, Start menu Power icon, command prompt, or by pressing F8 at startup (if F8 is enabled). In addition, Windows RE may launch automatically if Windows detects a problem at startup and you can use boot media to launch Windows RE.
- ▲ Three types of boot media can launch Windows RE and recover the system: a system repair disc, a recovery drive, and installation media created by the Media Creation Tool.
- ▲ In Windows RE, to fix a Windows startup problem, you can use Startup Repair, system restore, system image recovery, reset Windows, recover from a drive, or return to a previous build (or version). Some of these options allow you to keep personal data, and other options remove that data.
- ▲ When troubleshooting a startup problem, follow this procedure: interview the user, back up important data or verify you have current backups, research and identify any error messages, and determine what has recently changed that might be the source of the problem.
- ▲ As an improvement on Remote Assistance, Quick Assist does not require an emailed invitation, works in all versions of Windows 10, and is more universally compatible with existing network hardware configuration.

### Securing Windows 10

- ▲ The new Windows Defender Security Center includes the option to perform an offline scan, which gives Windows an edge in removing rootkits and stubborn malware by running a scan in a trusted environment.
- ▲ Virtualization-based security (VBS), a new feature of Windows 10, uses Hyper-V technology to increase security by isolating critical system components in a virtual environment.

- ▲ The Settings app provides many options for users to determine how accessible a computer's data is on a network, what personal information Microsoft can collect and retain, and how Windows updates are installed.
- ▲ Cortana's settings can be adjusted to control how much access Cortana has to certain types of user data.

## Windows 10 Command Line Interfaces

- ▲ Windows 10 adds new commands and parameters for both PowerShell and Command Prompt as well as some new options for interacting with the windows presenting these utilities to users.
- ▲ Many of the commands used in Command Prompt also work in PowerShell as aliases, or nicknames, for PowerShell cmdlets. Native PowerShell cmdlets almost always conform to the syntax *verb-noun*.
- ▲ In response to customer feedback, Microsoft built a Linux shell into Windows 10 that works like the Ubuntu Bash shell. This shell is not a VM, and it's not a fully separate operating system, but rather a shell for users to interact with underlying Windows functions and system files.

### >> KEY TERMS

3

**advertising ID** – An identification number linked to an individual's Microsoft account for the purpose of collecting information on that user's activities to personalize advertising.

**alias** – A nickname for a PowerShell cmdlet.

**attack surface** – The extent of attack vulnerability for a device, software, or network.

**Bash on Ubuntu on Windows** – A Linux shell that translates Linux commands into compatible Windows commands that interact directly with underlying Windows system files and functions. Also called Bash on Windows or Ubuntu Bash.

**cmdlet** – A PowerShell command.

**Credential Guard** – A security feature that uses Secure Boot and virtualization technology to store credentialing secrets, especially domain credentials, where the services that use those credentials run in an isolated virtual environment.

**Device Encryption** – An encryption tool similar to BitLocker that can protect the system boot volume on a Windows 10 Home system if an administrator signs in with a Microsoft account and if the device's hardware meets certain requirements.

**Device Guard** – A security feature that restricts the applications allowed to run on a device to those included on an organization's whitelist.

**Fresh Start** – A recovery method that performs a clean installation of the most recent version of Windows 10 Home or Windows 10 Pro.

**Hotspot 2.0** – A mobile device authentication technology standardized by the Wi-Fi Alliance that allows easier transition between public Wi-Fi hotspots and between Wi-Fi and cellular networks. Also called HS 2.0 or Wi-Fi Certified Passpoint.

**mbr2gpt.exe** – A command new to Windows 10 Creators Update that converts an MBR partitioning system to GPT without losing data on the drive.

**recover from a drive** – Phrase used to refer to the process of reinstalling Windows from system files stored on a recovery drive. The files may include OEM system files and manufacturer drivers specific to the computer that was used to create the drive.

**repair upgrade** – A non-destructive installation of Windows 10 over an existing Windows installation.

**telemetry** – Information collected about users' activities on a Windows device.

**version** – A large Windows update that includes all previous updates.

**Virtualization-based security (VBS)** – A new feature in Windows 10 that uses virtualization technology in Hyper-V to increase security around critical system components.

**Wi-Fi services** – A wireless connection management feature that automatically connects a Windows 10 device to open Wi-Fi hotspots included in its crowdsourced database.

**Windows Defender Offline** – An option in Windows Defender Security Center that runs a scan in a trusted environment, giving Windows an edge in removing rootkits and stubborn malware.

**Windows Subsystem for Linux (WSL)** – A subsystem or component of Windows designed to support Ubuntu on Windows. The component must first be enabled and is currently considered in beta (not fully tested).

**>> REVIEWING THE BASICS**

1. Which app in Windows can be used to restart a computer into Windows RE?
2. What are the three types of bootable recovery media?
3. Which repair tool is the least invasive, repair upgrade or system restore? Why?
4. Can a recovery drive be used to recover Windows using OEM device drivers installed in the system? System image recovery? Reset?
5. What physical media can the Media Creation Tool use to create bootable installation media from the ISO file it provides?
6. Where is the Startup Repair log file stored when Windows setup installs Windows on the C: drive?
7. Which recovery method is a non-destructive installation of Windows 10 over an existing Windows installation?
8. Which recovery method performs a clean installation of the most recent version of Windows 10 Home or Windows 10 Pro downloaded directly from the Microsoft website?
9. What encryption tool can protect the system boot volume on a Windows 10 Home system if an administrator signs in with a Microsoft account and if the device's hardware meets certain requirements?
10. Which three Windows 10 editions include BitLocker?
11. Device Guard and Credential Guard are supported by what security technology?
12. Which Windows app can be used to manage the telemetry that Microsoft collects?
13. What data source does Wi-Fi services use to select the best Wi-Fi hotspot for a connection?
14. What website allows you to ring, lock, or erase your Windows phone or to see any of your Windows devices' locations on a map?
15. Lately your computer has taken a long time to boot up, and you sometimes notice unusual error messages during startup. What new feature in the Windows Defender Security Center can you use to run a scan in a trusted environment?
16. You've been playing with PowerShell and created a few new aliases that are easy for you to remember. What is the PowerShell cmdlet that will list all the aliases available for the current PowerShell session?
17. Which PowerShell cmdlet gives the same results as the cd command used at the Command Line?
18. What shell does Windows Subsystem for Linux install by default?
19. You're trying to repair a friend's computer that is experiencing some glitches in Windows. He and his wife both use the computer regularly, and although the data is backed up, it would be a hassle to restore all the files along with several apps and customized Windows settings. Currently, you're trying to decide whether to reset the computer, perform a Fresh Start, or recover the system from the recovery drive that your friend created about a week ago. Which of these recovery methods will allow you to retain user accounts, user settings, and user data?
20. Will the Microsoft Office application suite installed on a computer be lost when you use the *Recover from a drive* method to recover the system? The Reset method? The Fresh Start method?

**>> THINKING CRITICALLY**

1. Which backup tool and media should you use to keep an up-to-date copy of the entire Windows volume?
- System image on multiple DVDs
  - Windows Backup on a network location
  - File History on a flash drive
  - System image on a network location
2. Suppose you are about to donate a Windows 10 computer to a school. What should you do before the computer goes out the door?
- Delete the Windows folder, and then perform a Windows 10 upgrade.
  - Copy all your data to an external storage device, and then perform a repair upgrade.
  - Copy all your data to an external storage device, and then reset Windows without keeping personal data.
  - Delete all your data on the hard drive, and then apply a restore point.
3. Which option on the Advanced options screen is available only when you restart the computer in Windows RE rather than from bootable media such as a recovery drive?
- System Restore
  - System Image Recovery
  - Startup Repair
  - Command Prompt
  - Startup Settings
4. Which of the following is a PowerShell cmdlet that will change the current directory?
- Get-ChildItem
  - Get-Location
  - Move-Item
  - Set-Location

3

**>> REAL PROBLEMS, REAL SOLUTIONS****REAL PROBLEM 3-1: Perform a Clean Boot**

When troubleshooting Windows problems, you might want to perform a clean boot to eliminate processes and services from launching at startup that might be the source of the problem or be causing a conflict with other programs. For more details about performing a clean boot, see the Microsoft Knowledge Base article 929135 at [support.microsoft.com/en-us/kb/929135](http://support.microsoft.com/en-us/kb/929135). Do the following to practice performing a clean boot:

1. Use the System Configuration (msconfig) utility to disable all non-Microsoft services. Use Task Manager to disable all startup processes.
2. Restart the computer. Note any changes or error messages you see during startup.
3. Return the startup process to start as usual. Restart the computer to verify all works as it should.

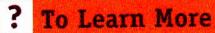
**REAL PROBLEM 3-2:** Use NTFS Permissions to Share Files and Folders

When learning to support a new edition of Windows, your skills supporting previous editions will come in handy. This text assumes you already know how to support Windows 8. Apply these Windows 8 skills to set up NTFS permissions and share permissions to share files and folders between two computers on a local network. In doing so, you'll see that Windows 8 and Windows 10 have much in common. Using two Windows 10 computers, do the following. As you work, write down each step you take in a log:



**Notes** If you are working alone with only one computer, you can use two virtual machines installed in a hypervisor on your computer to do this Real Problem.

1. On Computer 1 and Computer 2, set the network security to Private.
2. On Computer 1, sign in as an administrator and create two folders: C:\Financial and C:\Medical. Put a text file in each folder.
3. On Computer 2, create three new standard user accounts: John, Maria, and Jose.
4. Set up NTFS permissions, and share permissions so the following points are true.
  - ▲ When John is signed in to Computer 2, he can read and write to the Financial and Medical folders on Computer 1.
  - ▲ When Maria and Jose are signed in to Computer 2, they can read and write to the Medical folder, but they are not allowed access to the Financial folder on Computer 1.
5. Be sure to test your permissions by signing in to Computer 2 using the John, Maria, and Jose accounts and making sure all settings work as they should.
6. Compare the log of steps you kept with the log kept by another student. Look for differences and note them.



**To Learn More** The skills used in this problem were not covered in the chapter because they work fundamentally the same way in Windows 8 and Windows 10. To learn more about how to share files and folders on a network, start at page 825 in Chapter 17 of *A+ Guide to IT Technical Support*, ninth edition, or page 437 in Chapter 9 of *A+ Guide to Software*, ninth edition.