Understanding Device Configurations

LESSON 1

OBJECTIVE DOMAIN MATRIX

Technology Skill	Objective Domain Description	Objective Domain Number
Configuring Device Options • Understanding Microsoft Accounts • Configuring Control Panel • Configuring System Options • Changing Date and Time • Managing Devices	Configure device options	1.1
Configuring Desktop Settings • Configuring the Start Menu • Configuring User Profiles • Configuring Display Settings • Configuring Shortcuts • Understanding Group Policy	Configure desktop settings	1.2
Configuring Drive Encryption • Preparing for File Encryption • Configuring BitLocker	Configure drive encryption	1.3
Configuring Updates • Understanding Windows Update • Understanding App Updates • Understanding Device System Updates	Configure updates	1.4

KEY TERMS

Action Center
Active Directory accounts
Administrative Tools
BitLocker Drive Encryption (BDE)
Cortana
Control Panel
Computer Configuration node
decryption
device driver
Device Manager
Devices and Printers folder
domain-based accounts
Encrypting File System (EFS)
encryption
Group Policy
Group Policy objects (GPOs)
Internet Protocol Security (IPsec)
Jump List
live previews

live tiles
local user accounts
local user profile
mandatory user profile
Microsoft accounts
Microsoft Management Console (MMC)
Patch Tuesday
pin
Recycle Bin
resolution
roaming user profile
shortcut
Secure Sockets Layer (SSL)
Transport Layer Security (TLS)
Trusted Platform Module (TPM)
User Configuration node
user account
user profile
User State Migration Tool
Windows Easy Transfer
Windows Server Update Service (WSUS)
Windows Update

You work as an IT technician for the Contoso Corporation, which has hundreds of computers with a good mix between desktop computers and laptop computers. In addition, several users use smartphones and tablets to access their emails and documents. As an administrator, you need to ensure that your computers are fully functional and secure. You also need to make the machines similar to each other so that the helpdesk can support those machines.

■ Configuring Device Options

THE BOTTOM LINE

Windows 10 is a robust and flexible system that is made to work on and support a wide range of hardware. For example, Windows 10 can work on a tablet, a laptop, or a desktop computer. Windows 10 also supports mobile devices so that you can take your computer or device with you while accessing your files and programs.

The desktop (as shown in Figure 1-1) is the main screen area that you see when you first start the computer and log on to Windows. Like the top of an actual desktop, it is where you perform your work by opening and running one or more applications. It also includes the ***Recycle Bin***, which is used to recover files that have been previously deleted.

At the bottom of the desktop, you will find the Taskbar, which shows you the programs that are running and allows you to navigate between those programs. On the taskbar, you will see the Start button, which is located at the bottom-left corner.

When you click the Start button, the Windows 10 Start menu opens, as shown in Figure 1-2); the Windows 10 Start menu is a blend of the Windows 7 Start menu and the Windows 8 Start screen.

The left side of the Windows 10 Start menu displays the programs, which are used most often, and also provides access to File Explorer, Settings, Power, and All apps. When you click All Apps, all of the installed programs are shown in alphabetical order (see Figure 1-3). When you right-click an installed application, you can select Pin to Start or Pin to taskbar.

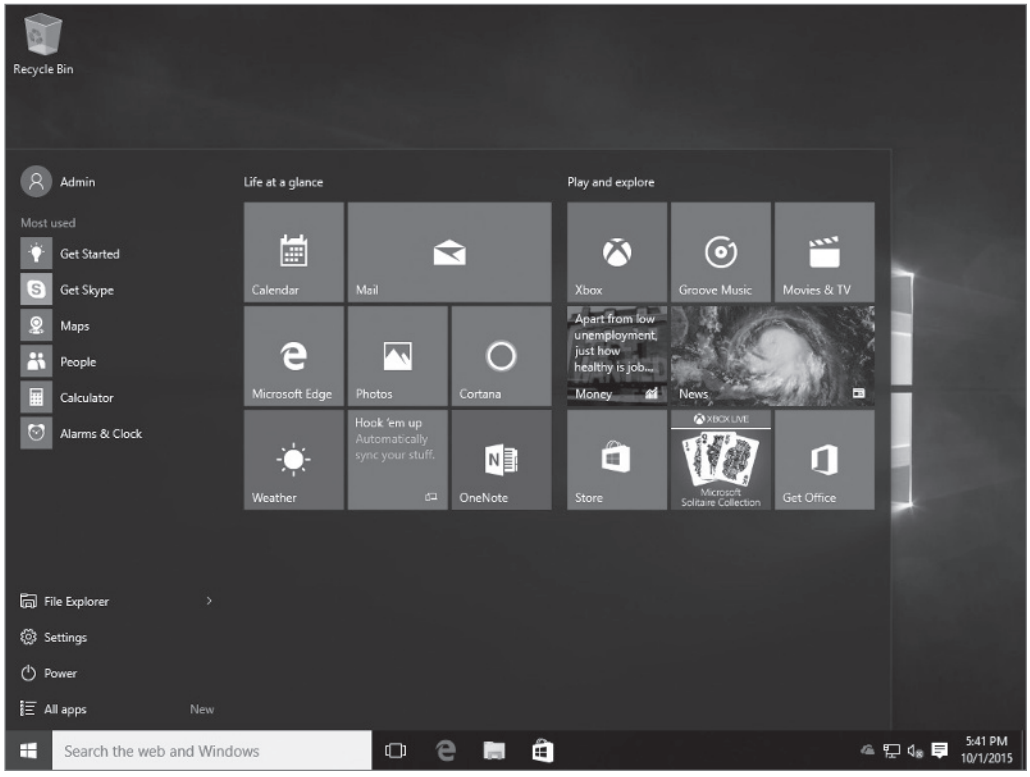
On the right side of the Windows 10 Start menu, tiles are displayed. Tiles are larger than the icons found on the Windows desktop and, unlike the static icons, they can contain dynamic content provided by the software they represent. For example, the tile for a Web browser can contain a thumbnail of the currently open Web site, while the Messaging tile can display part of your latest incoming email. Tiles in Windows 10 that contain this type of dynamic content are called ***live tiles***.

Figure 1-1

The Windows 10 Desktop

Figure 1-2

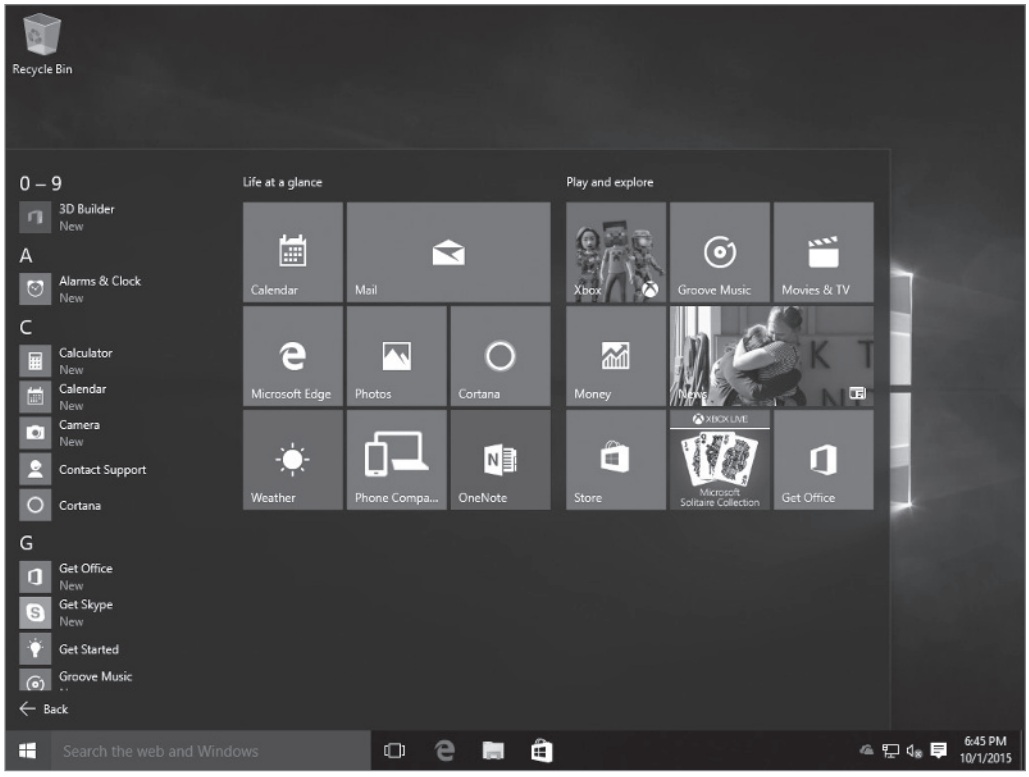
The Windows 10 Start menu



The tiles on the Start menu are configurable in a number of ways. Users can move the tiles around, change their size, change their groupings, and control whether they display live content. It is also possible to remove seldom-used tiles and add new tiles for applications, files, and shortcuts on the computer.

Figure 1-3

Accessing all Windows 10 programs



Clicking the Settings option displays the Settings application, which is based on the Modern UI interface to access common settings, as shown in Figure 1-4. These settings are organized according to the following icons:

- **System**: Allows you to configure the display, notifications and actions, Apps and features, multitasking, table mode, power and sleep options, and default apps.
- **Devices**: Provides quick access to hardware devices, such as printers.
- **Network & Internet**: Keeps track of Wi-Fi connections and allows you to configure VPN, dial-up connections, Ethernet connections, and proxy settings.
- **Personalization**: Provides settings for the background, colors, lock screen, themes, and the Start menu.
- **Accounts**: Allows you to change the profile picture and add accounts.
- **Time & language**: Allows you to configure date and time, Region and language, and Speech.
- **Ease of Access**: Provides settings for Narrator, Magnifier, high contrast, closed captions, the keyboard, and the mouse.
- **Privacy**: Allows you to configure the camera, the microphone, speech, account information, contacts, calendar, messaging, and application radio controls for Wi-Fi/Bluetooth connections.
- **Update & security**: Allows you to configure Windows Update, activate Windows, perform backups and recoveries, and configure Windows Defender.

Cortana is Microsoft's new personal assistant that will help you find things on your PC, manage your calendar, find files, chat with users, and search the Internet. To see the search results, just type the desired text in the Search the web and Windows box option. For example, Figure 1-5 shows the results for a search for "keyboard settings."

Figure 1-4

Accessing the Settings option

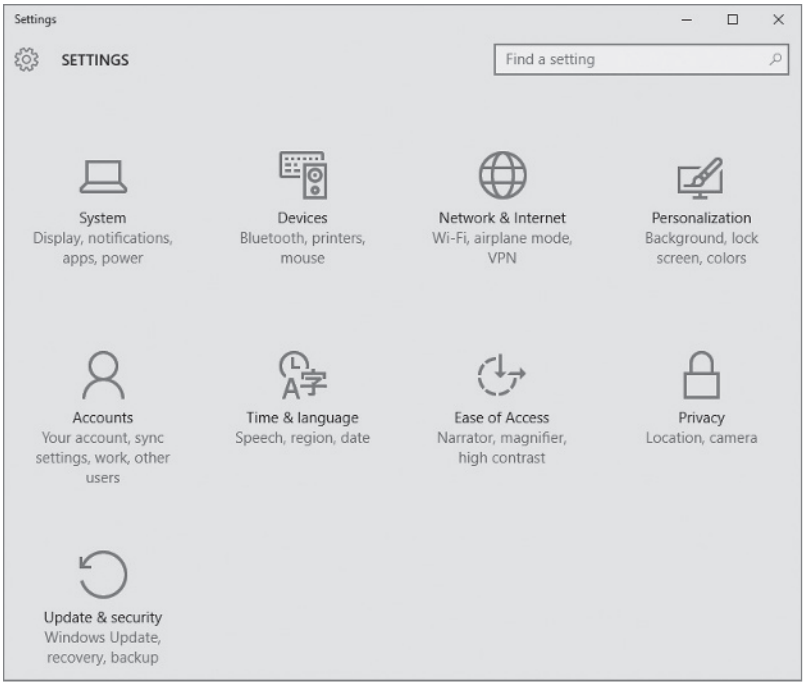
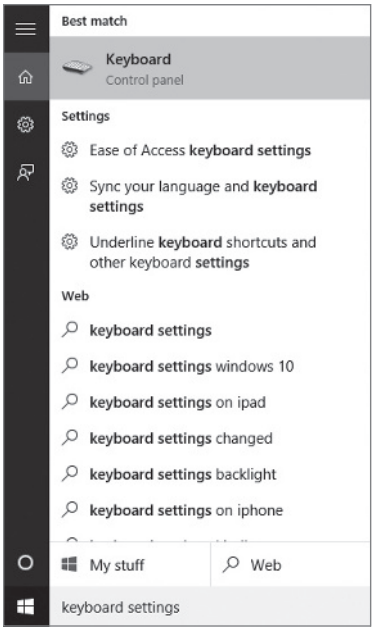


Figure 1-5

Using Cortana



USING A TOUCH SCREEN

Windows 10 can be navigated by using a pointing device (such as a mouse) or by using a touch screen. Operating a touch screen requires familiarity with certain finger gestures, such as the following:

Tap: Press a fingertip to the screen and release it. The function is identical to that of a mouse click.

Double-tap: Press a fingertip to the screen twice in quick succession on the same spot. The function is identical to that of a double mouse click.

Press and hold: Tap a location on the screen and press down for approximately two seconds. The function is the same as that of mousing over a designated spot and hovering.

Slide: Press a point on the screen and draw your finger across it without pausing. The function is the same as clicking and dragging a mouse.

Swipe: Draw a finger across the screen in the indicated direction.

Understanding Microsoft Accounts

A ***user account*** is used to identify a user or other identity on a system, which can be used in authentication, authorization, and auditing. In Windows, user accounts provide different levels of control over an organization's computers and resources.

CERTIFICATION READY
Configure device options
1.1

When working with Windows 10, there are three types of accounts:

- ***Microsoft accounts*** enable you to synchronize your desktop across multiple Windows 10 devices.
- ***Local user accounts*** are created on individual computers that are members of a workgroup to provide access to resources on that computer.
- ***Domain-based accounts***, also called ***Active Directory accounts***, are stored as objects on a domain controller and are used by the operating system to identify and authenticate the user and to grant her authorization to access specific domain resources.

When you set up a computer running Windows 10 for the first time, you have the option of creating a Microsoft account using an email address that you provide. The email address you use can come from any provider. After the account is set up, Microsoft will use it along with your password to help manage your settings across all your PCs running Windows 10. After organizing your system the way you want it (your preferred desktop background, user tiles, favorite websites in your browser, explorer settings, and so on), the information will be associated with your Microsoft account and will be stored in the cloud. Every time you log into a Windows 10 device using the account, your settings are synched from the cloud, and any changes you make are updated and available to you on the next device.

Using a Microsoft account provides a consistent experience when working with Windows Store apps. Purchased apps will be available from each device, feeds you add will be synched across all devices, and state information will be maintained, so you can start a game or read a book and pick it up later on another device.

Microsoft accounts can be synced with a domain account, but the capability to do so depends upon Group Policy settings. Using Group Policy—covered later in this lesson—you can determine whether you want to allow the syncing of the two accounts and what information can be synced.

You can create a Microsoft account during the initial installation of the operating system or after the system is running. The following steps outline the process you can use to create the account.

CREATE A MICROSOFT USER ACCOUNT USING THE SETTINGS PROGRAM

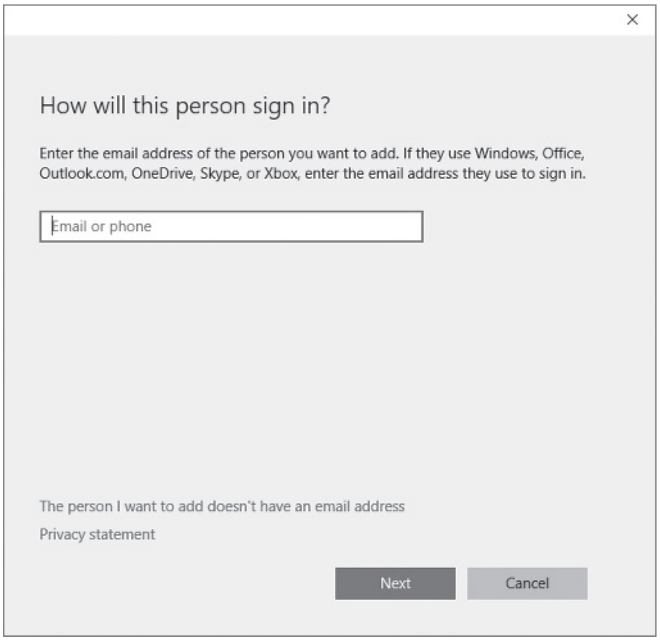
GET READY. To create the account after Windows 10 is installed using the Settings program, perform the following steps.

1. Log into the Windows 10 client computer.
2. Click the **Start** button to open the Start menu.
3. Click **Settings**.

4. Click **Accounts.**
5. Click the **Family & other users** option.
6. Click **Add someone else to this PC**.
7. On the How will this person sign in? page, to use an existing Microsoft Account, in the Email or phone text box (see Figure 1-6), type the email address you want to use. Click **Next** and then click **Finish**. If you want sign up for a new Microsoft account, click **The person I want to add doesn't have an email address**.

Figure 1-6

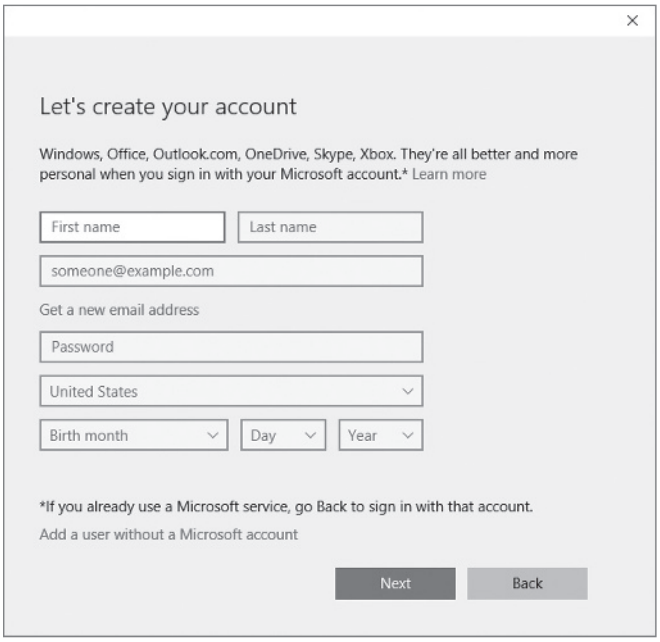
Adding a user



8. On the Let's create your account page (as shown in Figure 1-7), in the First name text box and Last name text box, type your first name and last name. In the someone@example.com text box, type the desired email address.

Figure 1-7

Creating a new account



9. In the Password text box, type the desired password.
10. In the Country text box, type the name of your country. In the remaining text boxes, type your Birth month, Day, and Year. Click **Next**.
11. On the Add security info page, in the Phone number text box, type a phone number that can receive text messages. Click **Next**.
12. On the See what's most relevant to you option, deselect one or both options, if desired:
13. Enhance my online experience by letting Microsoft Advertising use my account information
    - Send me promotional offers from Microsoft
    - By default, the account will be a standard user account. If you want to upgrade the account to an administrator, click the new account, and then click **Change account type**.
14. Change the Account type to **Administrator** and then click **OK**.
15. On the Add a user page, Click **Finish**.

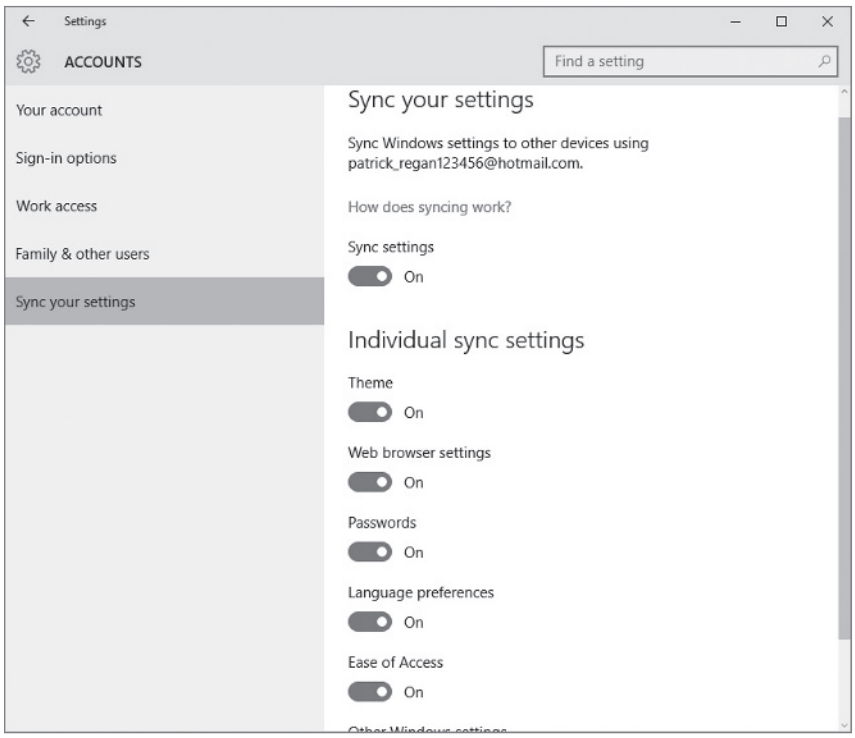
When using a logon with a Microsoft or work account in Windows 10, you can sync your PC settings—even between multiple Windows 10 machines—as long as they are connected with the same Microsoft account. Therefore, if you change the wallpaper or add a favorite shortcut in Internet Explorer, those changes will be replicated to the other machines.

The Sync feature (located under OneDrive settings, as shown in Figure 1-8) can sync many of your settings between PCs, including the following:

- Personalization settings, such as Start screen colors, background, and lock screen image
- Themes, such as the desktop background and sounds
- Ease of Access settings, such as Speech Recognition, Magnifier, On-screen Keyboard, and Narrator

Figure 1-8

Managing Sync settings in Windows 10



- Language preferences, such as keyboard settings, other input methods, and display language
- Web browser settings, such as history, pinned sites, and favorites for both versions of the browser
- Taskbar settings, such as pinned items and which side of the monitor the Taskbar is attached to
- Folder and Search settings for File Explorer
- Mouse settings
- Your accounts picture (user tile)
- Per-app notification state
- Settings for Windows Store apps, including third-party apps
- HomeGroup password

Configuring Control Panel

As with previous versions of Windows, the main graphical utility to configure the Windows environment and hardware devices is the ***Control Panel.*** It can be accessed by right-clicking the Start button and choosing Control Panel. See Figure 1-9. Of the eight categories that are listed, each category includes a top-level link, and under this link are several of the most frequently performed tasks for the category.

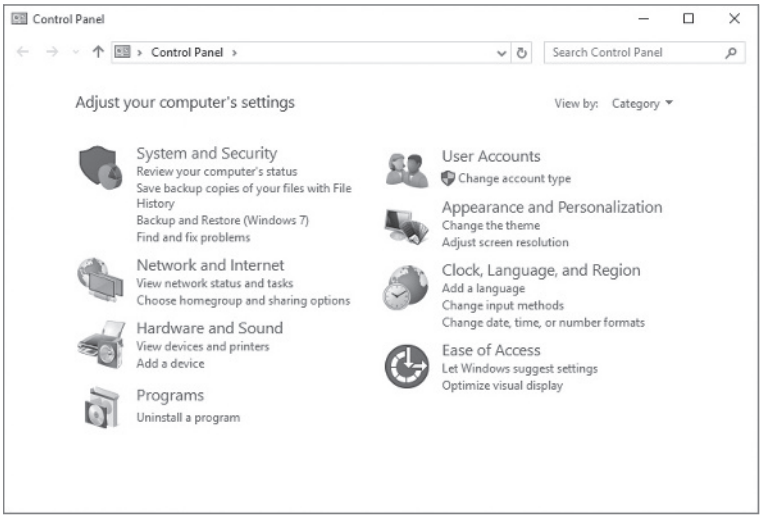
Clicking a category link provides a list of utilities in that category. Each utility listed within a category includes a link to open the utility, and under this link are several of the most frequently performed tasks for the utility.

As with current and previous versions of Windows, you can change from the default category view to classic view (large icon view or small icon view). Icon view is an alternative view that provides the look and functionality of Control Panel in Windows 2000 and earlier versions of Windows where all options are displayed as applets or icons.

The ***Microsoft Management Console (MMC)*** is one of the primary administrative tools used to manage Windows and many of the network services provided by Windows. It provides a standard method to create, save, and open the various administrative tools provided by Windows. When you open Administrative Tools, most of these programs are MMC.

Figure 1-9

Opening Control Panel



Administrative Tools is a folder in the Control Panel that contains tools for system administrators and advanced users. To access the Administrative Tools, open the Control Panel, open Administrative Tools by clicking Start, Control Panel, System and Security while in category view or double-click the Administrative Tools applet while in icon view. There is also a quick link on Windows that can be accessed by clicking the Start button.

Some common administrative tools in this folder include:

- **Component Services**: Configures and administers Component Object Model (COM) components. Component Services is designed for use by developers and administrators.
- **Computer Management**: Manages local or remote computers by using a single, consolidated desktop tool. Using Computer Management, you can perform many tasks, such as monitoring system events, configuring hard disks, and managing system performance.
- **ODBC Data Sources**: Uses Open Database Connectivity (ODBC) to move data from one type of database (a data source) to another.
- **Event Viewer**: Views information about significant events, such as programs starting or stopping or security errors that are recorded in event logs.
- **iSCSI Initiator**: Configures advanced connections between storage devices on a network.
- **Local Security Policy**: Views and edits Group Policy security settings.
- **Performance Monitor**: Views Advanced system information about the processor, memory, hard disk, and network performance.
- **Print Management**: Manages printers and print servers on a network and perform other administrative tasks.
- **Services**: Manages the different services that run in the background on your computer.
- **System Configuration**: Identifies problems that might be preventing Windows from running correctly.
- **System Information**: Shows details about your computer's hardware configuration, computer components, and software, including drivers.
- **Task Scheduler**: Schedules programs or other tasks to run automatically.
- **Windows Memory Diagnostics**: Checks your computer's memory to see whether it is functioning properly.
- **Windows PowerShell**: A task-based command-line shell and scripting language designed especially for system administration.

When you use these tools, you might assume that they are used only to manage the local computer. However, many of them can be used to manage remote computers as well. For example, you can use the Computer Management console to connect to and manage other computers, assuming you have administrative rights to the computer.

Configuring System Options

Some of the most important configuration settings for a user are the system settings within the Control Panel. These include gathering generation information about your system, changing the computer name, adding the computer to a domain, accessing the device manager, configuring remote settings, configuring startup and recovery options, and configuring overall performance settings.

To access the system settings, you can do one of the following:

- In the Control Panel, if you are in Category view, click System and Security, and then click System or click View amount of RAM and processor speed.
- In the Control Panel, if in classic view, double-click the System applet.

- Right-click Computer and choose Properties.
- Right-click the Start button and choose System.

In Windows, there are often several ways to do the same thing.

At the top of the screen, you see the Windows edition you have and the system type. If Windows comes in 64-bit, it will show 64-bit Operating System in the middle of the screen. Toward the bottom of the screen you will see the computer name and domain (if any) if Windows is activated and the Product ID. See Figure 1-10.

To help identify computers, you should name a computer with a meaningful name. This can be done within the System settings within the Control Panel. You can also add a computer to a domain or workgroup.

Every computer must have a unique computer name assigned to a network. If two computers have the same name, one or both of the computers will have trouble communicating on the network. To change the computer name, open System from the Control Panel. Then click the Change Settings option in the Computer name, domain, and workgroup settings. When the System Properties box appears with the Computer Name tab selected, click the Change button. See Figure 1-11. Any changes to the computer name or workgroup/domain name will require a reboot.

Figure 1-10

Displaying System settings

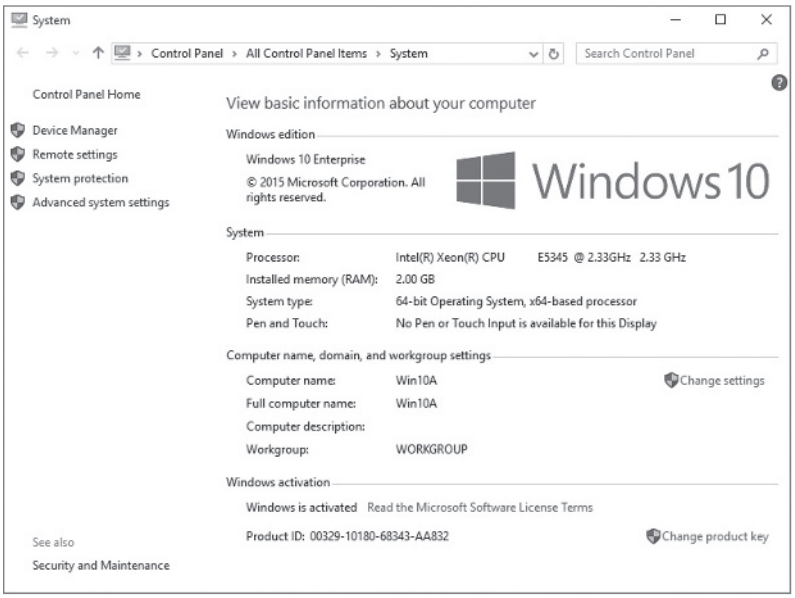
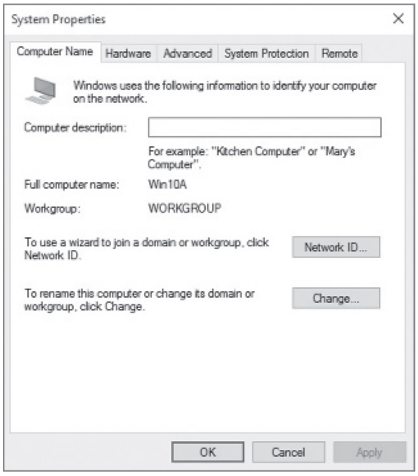


Figure 1-11

Displaying System Properties



By default, a computer is part of a workgroup. A workgroup is usually associated with a peer-to-peer network in which user accounts are decentralized and stored on each individual computer. If several users need to access the computer (while requiring unique usernames and passwords), you will need to create a user account for each user. If you want those users to access another stand-alone computer, you will have to create the same computer accounts and password on that computer as well. As you can imagine, with several computers, this can become a lot of work as you keep creating and managing accounts on each individual computer.

A domain is a logical unit of computers that define a security boundary, and it is usually associated with Microsoft's Active Directory Domain Services (AD DS). The security of the domain is generally centralized and controlled by Windows servers acting as domain controllers. As a result, you can manage the security much easier for multiple computers while providing better security.

When a computer is added to a domain, a computer account is created to represent the computer. In addition, information stored on the computer is used to uniquely identify the computer. When these items match, it shows that a computer is who it says is, which contributes to a more secure work environment.

To add the computer to the domain, open System Properties and click the Change button. You will then select the Domain option and type the name of the domain. Next, click OK. It will prompt you to log in with a domain account that has the ability to add computers to the domain. This is typically a domain administrator or account administrator. After you enter the credentials (username and password), a Welcome dialog box appears. Click OK to close the Welcome dialog box. When you close the System Properties dialog box, it will prompt you to reboot the computer.

To remove a computer from a domain, join an existing workgroup, or create a new workgroup, you select the workgroup option and type in the name of the workgroup and click OK. If you are removing yourself from the domain, you will be asked for administrative credentials so that it can delete the account from Active Directory. If you don't specify administrative credentials, it will still remove the computer from the domain, but the computer account will still remain within Active Directory.

Changing Date and Time

One of your easiest but most essential tasks is making sure that the computer has the correct date and time, which is essential for logging purposes and for security. If a secure packet is sent with the wrong date or time, the packet may be automatically denied because the date and time is used to determine if the packet is legit.

To access the date and time settings, perform one of the following steps:

- Click Clock, Language, and Region in the Control Panel while in Category view and click Set the time and date.
- Double-click Date and Time while in Icon view.
- If the date and time show in the Notification area, double-click the date and time.

To set the clock:

1. Click the Date and Time tab and then click Change date and Time.
2. Double-click the hour, minutes, or seconds, and then click the arrows to increase or decrease the value.
3. When you are finished changing the time settings, click OK.

To change the time zone, click Change time zone and click your current time zone in the drop-down list. Then click OK.

If you are part of a domain, the computer should be synchronized with the domain controllers. If you have a computer that is not part of a domain, you can synchronize with an Internet time server by clicking the Internet Time tab and selecting the checkbox next to Synchronize with an Internet time server. Then select a time server and click OK.

Managing Devices

A computer is a collection of hardware devices, each of which requires a piece of software called a device driver in order to function. Windows 10 includes a large library of device drivers, but it is still sometimes necessary to obtain them yourself.

As most people know, a PC is a collection of hardware devices, all of which are connected together and installed in a single case. Disk drives, keyboards, mice, modems, and printers are all types of devices. To communicate with the operating system running on the computer, each device also requires a software element called a ***device driver***. The device driver provides the operating system with information about a specific device.

For example, when you use a word processing application to save a file to a hard disk, the application issues a generic WriteFile function call to the operating system. The application knows nothing specific about the disk drive hardware; it just issues an instruction to store a particular file there. When the operating system processes the function call, it accesses the device driver for the hard disk drive, which provides detailed information about how to communicate with the drive. If the user selects a different target location for the file, the operating system accesses the device driver for that location, whether it's a hard drive, a floppy drive, or USB flash drive.

In most cases the information the device driver provides is integrated into the Windows interface. For example, the Properties sheet for a printer includes generic system information (see Figure 1-12), such as which port the printer is connected to and who is permitted to use it. Other tabs, and particularly the Device Settings tab, as shown in Figure 1-13, are based on hardware-specific information provided by the device driver.

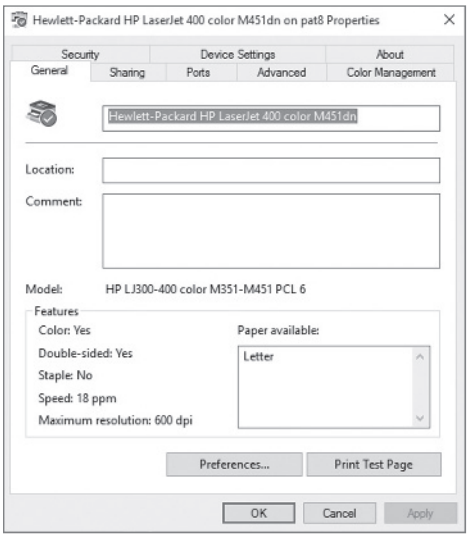
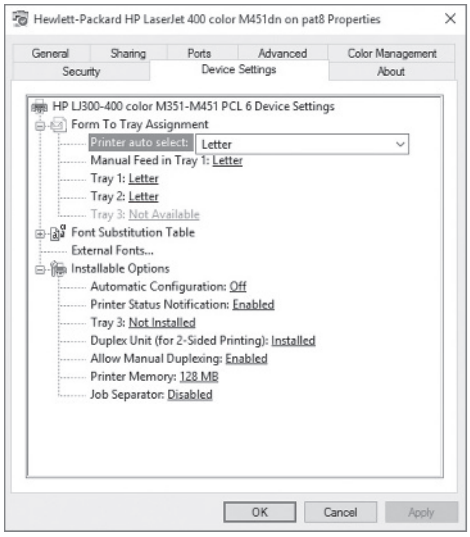


Figure 1-12

The General Settings tab of a printer's Properties sheet

Figure 1-13

The Device Settings tab of a printer's Properties sheet



In addition to providing information about a device, drivers also permit the operating system to modify the hardware configuration settings of the device. For example, when you configure a printer to print a document in landscape mode instead of portrait mode, the printer device driver generates the appropriate commend and sends it to the hardware.

The process of installing a hardware device consists primarily of identifying the device and installing a device driver for it. This process can occur during the operating system installation or at a later time, but the steps are fundamentally the same.

A major part of the Windows 10 installation process consists of identifying the devices in the computer and installing the appropriate drivers for them. The Windows 10 installation package includes hundreds of drivers for many different devices, which is why many installations finish without any user intervention. Sometimes, however, you might have to supply device drivers yourself.

USING THE DEVICES AND PRINTERS FOLDER

Windows 10, Windows includes the ***Devices and Printers folder*** to quickly allow users to see all the devices connected to the computer and to configure and troubleshoot these devices. It will also allow you to view information about the make, model, and manufacturer and give you detailed information about the sync capabilities of a mobile phone or other mobile devices.

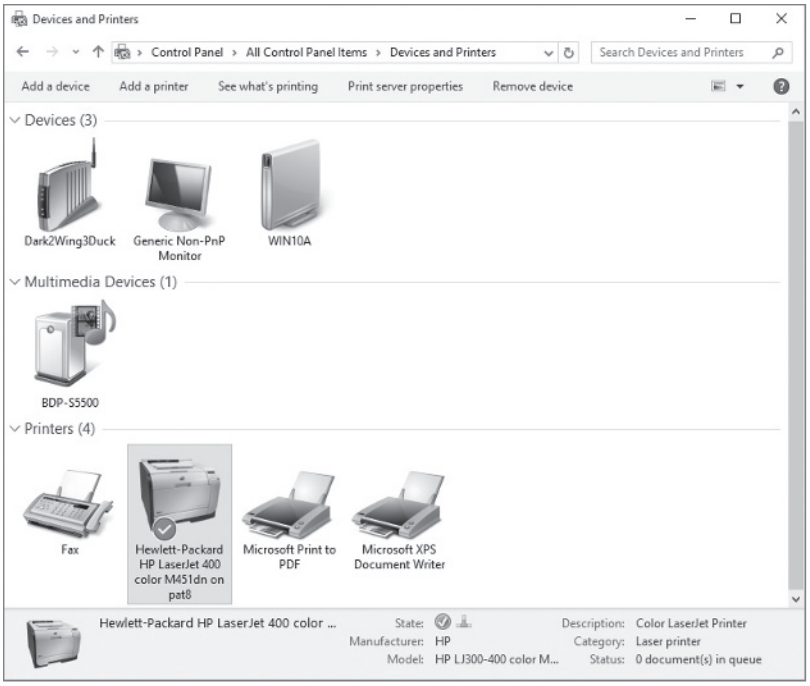
The Devices and Printers folder gives you a quick view of devices connected to your computer that you can connect or disconnect from your computer through a port or network connection. This includes mobile devices such as music players and digital cameras, USB (Universal Serial Bus) devices, and network devices. See Figure 1-14. It does not include items installed inside your computer such as internal disk drives, expansion cards, RAM and it will not display legacy devices such as keyboards and mice connected through a PS/2 or serial port.

To open the Devices and Printers folder, open the Control Panel and, under Hardware and Sound, click View devices and printers while in Category view or double-click Devices and Printers in Icon view.

When you right-click a device icon in the Devices and Printers folder, you can choose from a list of tasks that vary depending on the capabilities of the device. For example, you might be able to see what's printing on a network printer, view files stored on a USB flash drive, or open a program from the device manufacturer. For mobile devices that support the new Device Stage feature in Windows, you can also open advanced, device-specific features in Windows from the right-click menu, such as the ability to sync with a mobile phone or change ringtones.

Figure 1-14

Devices and Printers



Most PCs use USB connections for peripheral devices, and Plug and Play is an integral part of the USB standard. When you connect a printer, a camera, a scanner, or another type of device to a computer running Windows 10 using a USB port, the system usually detects it, adds it to the Devices and Printers folder and installs the appropriate device driver for it.

You can also manually install a device by selecting Add a device, which displays the Choose a device or a printer to add to this PC page.

USING DEVICE MANAGER

The Windows 10 tool for managing devices and their drivers is called ***Device Manager***. You can use Device Manager to get information about the devices installed in the computer, as well as install, update, and troubleshoot device drivers.

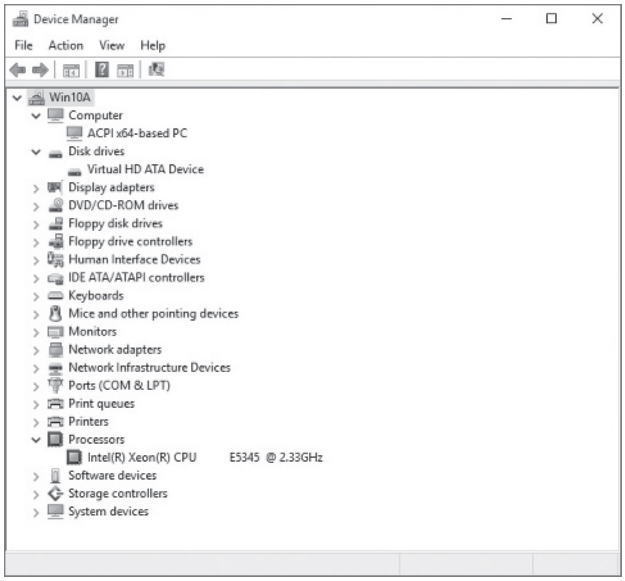
Although it is not immediately apparent, Device Manager is a snap-in for the Microsoft Management Console (MMC). This means that there are many ways that you can access Device Manager, including the following:

- Open the Hardware and Sound control panel and click the Device Manager link.
- Open the Computer Management console from the Administrative Tools program group in the System and Security control panel and click Device Manager in the scope (left) pane.
- Run the Microsoft Management Console shell application (Mmc.exe), select File > Add/Remove Snap-in, and select Device Manager from the list of snap-ins provided.
- Open the Start menu, type Device Manager or the file name of the Device Manager snap-in (Devmgmt.msc), and then execute the resulting file.
- Using Cortana, search for Device Manager and then execute the resulting file.

Each of these procedures launches the Device Manager and displays a window with an interface like that shown in Figure 1-15.

Figure 1-15

The Windows 10 Device Manager



Device Manager is capable of displaying information in the following four modes:

- **Devices by type**: Displays a list of device categories, which you can expand to show the devices in each category. This is the default Device Manager view.
- **Devices by connection**: Displays a list of the interfaces that hardware devices use to communicate with the computer. Expanding a connection shows the devices using that connection.
- **Resources by type**: Displays a list of resource types, including Direct Memory Access (DMA), Input/Output (I/O), Interrupt Request (IRQ), and Memory, which you can expand to show the resources of each type and the devices that are using them.
- **Resources by connection**: Displays a list of resource types, including Direct Memory Access (DMA), Input/Output (I/O), Interrupt Request (IRQ), and Memory, which you can expand to show the connection associated with each individual resource and the device using each connection.

To examine the properties of a device, simply locate it in the tree display and double-click it to open its Properties sheet.

The tabs on the Properties sheet vary depending on the nature of the device you select, but virtually all devices have the following four tabs:

- **General**: Displays the name of the device, its type, manufacturer, and location in the system. The Device Status box indicates whether the device is functioning and, if not, provides troubleshooting help.
- **Driver**: Displays the device driver's provider, date, version, and digital signer. The tab also provides buttons you can use to display driver details, update, roll back (used when an upgrade of a device driver fails or causes problems with a system), or uninstall the driver, and enable or disable the device.
- **Detail**: Displays extensive information about the driver and its properties.
- **Resources**: Displays the hardware resources being used by the device and indicates whether there are any conflicts with other devices in the computer.

With Device Manager, you can disable any device in the computer, using any of the following procedures:

- Select the device and choose Disable from the Action menu.
- Right-click the device and choose Disable from the context menu.
- Open the device's Properties sheet and click the Disable button on the Driver tab.

Disabling a device does not affect the hardware in any way or uninstall the device driver; it simply renders the device inoperative until you enable it again. Obviously, you cannot disable devices that are necessary for the system to function, such as the processor, and some devices that are in use require you to restart the system before they can be disabled.

TAKE NOTE*

Disabling a device releases the hardware resources it was using back to the operating system. If you restart the computer with the device disabled, Windows might reassign those hardware resources to other devices. If you re-enable the device, the computer might allocate different hardware resources to it than it had originally.

When you update a driver using Device Manager, you can point to a location on your computer where you have already saved the new driver, or you can run a search of your computer and the Internet. To update a device driver, use the following procedure.

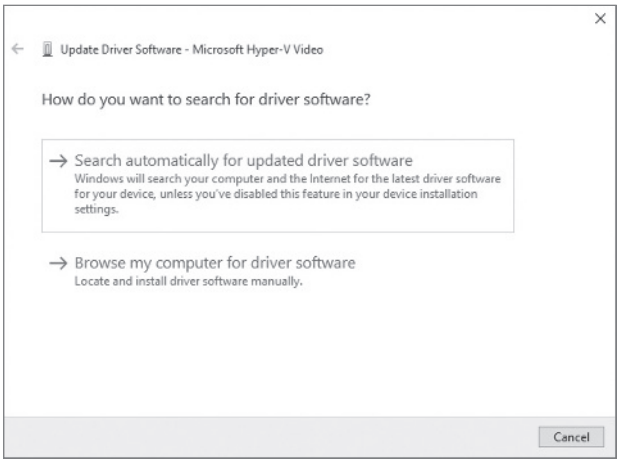
UPDATE A DEVICE DRIVER

GET READY. Log on to Windows 10 using an account with Administrator privileges.

1. Open **Device Manager** and locate the device that you want to update.
2. Double-click the device you want to update, so that its Properties sheet appears.
3. Click the **Driver** tab and then click the **Update Driver** button. The How Do You Want To Search For Driver Software? page appears, as shown in Figure 1-16.

Figure 1-16

The How Do You Want To Search For Driver Software? page



4. Click **Browse My Computer For Driver Software** to specify a location for the driver or to select from a list of installed drivers. Click **Search Automatically For Updated Driver Software** to initiate a search for a driver.
5. Click **Next** when you locate the driver you want to install. The Windows Has Successfully Update Your Driver Software page appears.
6. Click **Close**.
7. Close the Device Manager window.

When you update a device driver in Windows 10, the operating system does not discard the old driver completely. It is not uncommon for new drivers to cause more problems than they solve, and many users find that they would prefer to go back to the old version. Windows 10 makes this possible with the Roll Back feature, which you initiate by clicking the Roll Back Driver button on the Driver tab of the device's Properties sheet. This procedure uninstalls the current driver and reinstalls the previous version, returning the device to its state before you performed the most recent driver update.

Installing a new hardware device or a new device driver is a risky undertaking. There is always the possibility of a problem that, depending on the devices involved, could be trivial or catastrophic. For a peripheral device, such as a printer, a hardware misconfiguration or faulty driver would probably just cause the new device to malfunction. However, if the device involved is a graphics adapter, a bad driver could prevent the system from functioning.

TROUBLESHOOTING PROBLEM DEVICES

The ***Action Center*** (as shown in Figure 1-17) shows important notifications related to the security and maintenance of your computer. When problems occur, you will be alerted to investigate them further.

To troubleshoot hardware or driver problems, consider some of the following techniques:

- Open the Properties sheet for the device and check the Device Status box on the General tab. If the device is malfunctioning, this tab informs you of its status and enables you to launch a troubleshooter.
- Open the Device Manager and delete the device entirely. Then restart the system and allow Windows 10 to detect and install the device over again. This process will cause

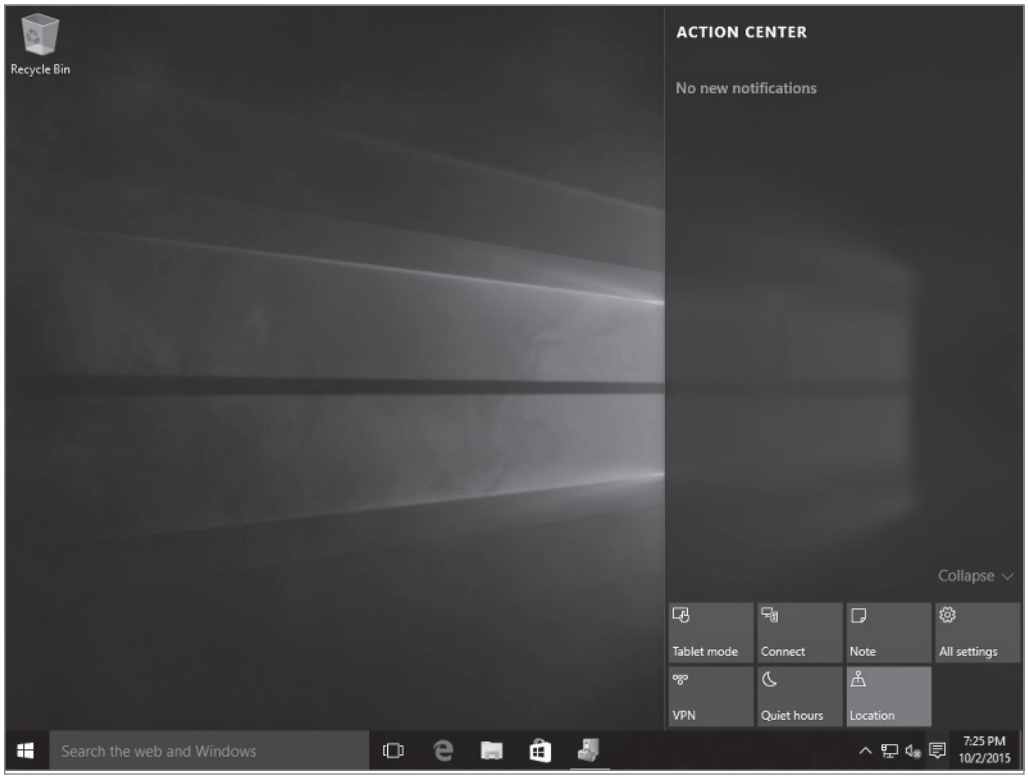


Figure 1-17
The Action Center

Windows to re-allocate hardware resources to the device, which could resolve the problem if it was caused by a hardware resource conflict.

- If the device or driver malfunction prevents the system from running properly, as in the case of a bad graphics driver that prevents an image from appearing on the screen, you can start the computer in Safe Mode by pressing the F8 key as the system starts. Safe Mode loads the operating system with a minimal set of generic device drivers, bypassing the troublesome ones, so you can uninstall or troubleshoot them.

Device Manager also displays all of the devices installed on your computer. When a device is experiencing problems, Device Manager uses symbols to provide information about the particular error condition.

When there is an issue with a device, you will see one of the following symbols (each symbol represents a specific type of problem):

- **Blue question mark inside white circle**: Driver installed; may not provide full functionality.
- **Red "X"**: device is installed in computer and is consuming resources; protected mode driver not loaded; device installed improperly.
- **Black exclamation point on yellow field**: Device in problem state; the device might be functioning; problem code will be displayed with device.
- **Blue "I" on white field**: Use automatic settings not selected for device; resource was manually selected; does not indicate a problem or disabled state.
- **Problem code**: Code explaining the problem with the device.
- **White circle with down arrow**: Device was disabled by an administrator or user.
- **Yellow warning symbol with exclamation point**: There is a problem with the device.

Windows 10 uses built-in hardware diagnostics to detect hardware problems on your computer. When problems are identified, a message appears that lets you know about the problem. If you select the message, you will be taken to the Action Center, which provides a central location to view any problems with your hardware or software.

When there is a problem, you will see two types of messages in the notification area (the bottom-right corner of your desktop):

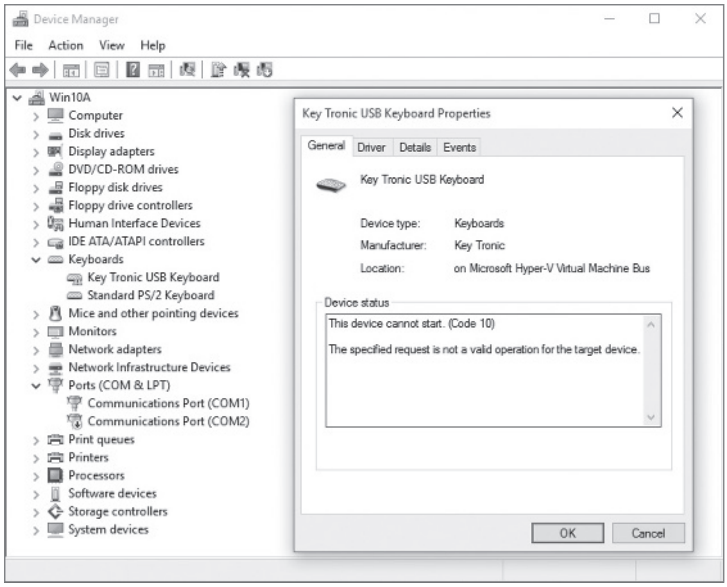
- **Red items (white flag, red circle with white x)**: These are important messages that indicate a significant problem that needs to be addressed. For example, your firewall is turned off, or spyware or antivirus applications need to be updated.
- **Yellow items**: These are messages that suggest tasks that can make your computer run better. For example, updating an application or configuring Windows Update to automatically download and install updates rather than checking with you beforehand.

How you troubleshoot a device depends upon the type of problem you encounter. For example, when you notice a device with the black exclamation point in a yellow triangle, you can double-click the device to investigate the problem further. Figure 1-18 shows that the device cannot start and the specified request is not a valid operation for the target device.

Another item of interest when troubleshooting device problems is to look for an Other Devices folder. This folder contains devices detected by Windows but lacks a driver for the device.

Figure 1-18

Troubleshooting a device



■ Configuring Desktop Settings

THE BOTTOM LINE

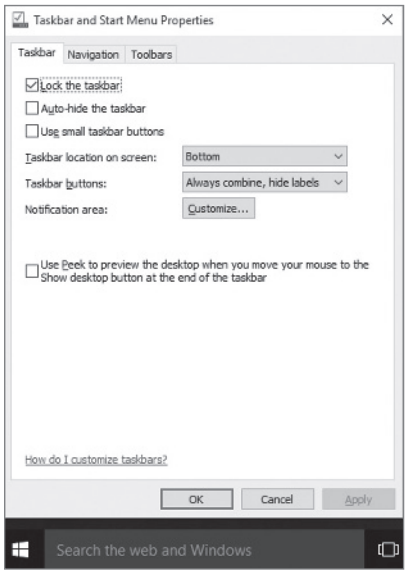
Windows desktop settings is a broad term that refers to many different settings you can configure to personalize Windows, such as the Windows theme, the desktop background, mouse clicks and pointer speeds, gadgets, shortcuts, and more. All settings are customizable—choosing the right mix will make your Windows experience more enjoyable and more productive.

CERTIFICATION READY
Configure desktop settings
1.2

The Windows desktop is a flexible, configurable part of the Windows environment. You can grab the Taskbar and move it to either side of the screen, to the top, or back to its default location at the bottom (the Taskbar must be unlocked to move it—right-click the Taskbar and, if Lock the taskbar is checked, select the box to deselect it). You can also choose which items appear in the notification area on the right side of the Taskbar by configuring the Taskbar Properties dialog box. To access this dialog box, right-click the Taskbar and choose Properties, as shown in Figure 1-19.

Figure 1-19

Opening the Taskbar and Start Menu Properties dialog box



Windows 10 has the ability to ***pin*** program shortcuts directly to the Taskbar; when you pin a program, the icon for that program displays on the Taskbar even when the program isn't running. This provides you with quick access to your frequently used programs. Shortcuts for Task View, Microsoft Edge, File Explorer, and Store appear there by default. You can unpin programs from the Taskbar as well. You'll learn about shortcuts later in the lesson.

When you open a program in Windows 10, an icon for that program displays on the Taskbar. To activate a program, just click its icon on the Taskbar. If you have several programs open at once, Windows allows you to hover the mouse pointer over an icon in the Taskbar to see a thumbnail preview of the window. This thumbnail preview is called a ***Jump List***. You can also press and hold the Alt key and then press the Tab key repeatedly to switch between windows and see ***live previews*** of the window for each open program.

Many Windows 10 desktop settings are available when you right-click a blank area of the desktop and choose Personalize. The Personalization window is shown in Figure 1-20. The main part of the window displays various themes you can use. Just click the theme of your choice and see the changes take effect immediately.

You can also change the background of any theme. Just click Background. In the Background window, open the Picture location drop-down list, and then select a picture, a solid color, or a slideshow.

When you click the Themes > Advanced sound settings, the Sound dialog box opens (see Figure 1-21). From here, you can choose different sounds to accompany Windows events, such as when you connect a device or when you close Windows. The computer's sound volume must be set at an appropriate level to actually hear the sound.

When you click the Lock screen option, you can click the Screen saver settings option to open the Screen Saver Settings dialog box (as shown in Figure 1-22). Then open the Screen saver drop-down list, select a screen saver, and click OK.

Figure 1-20

The Windows 10 Personalization window

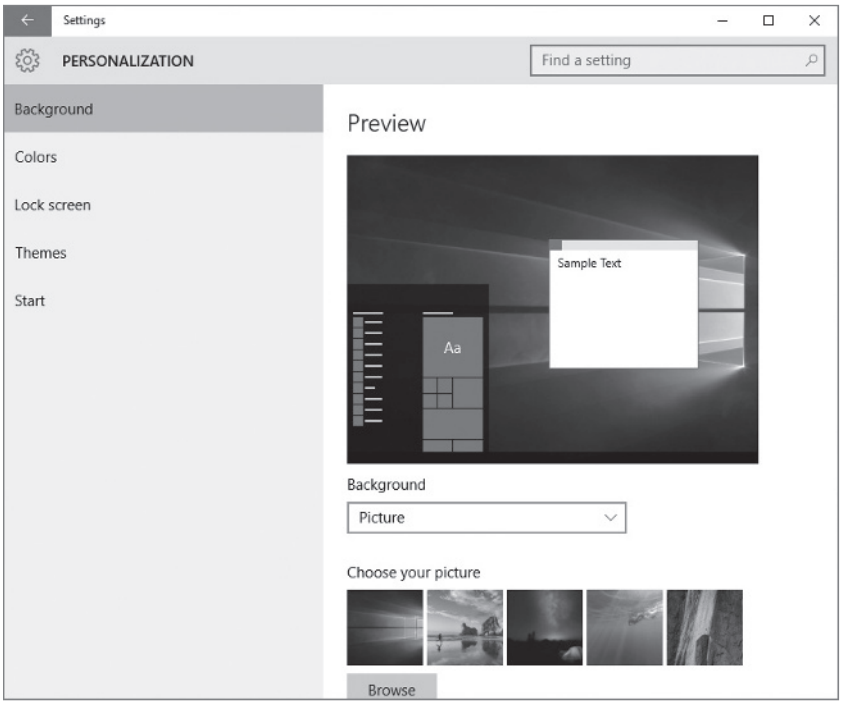


Figure 1-21

The Sound dialog box

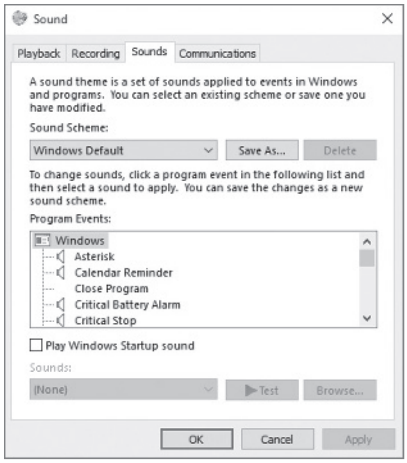
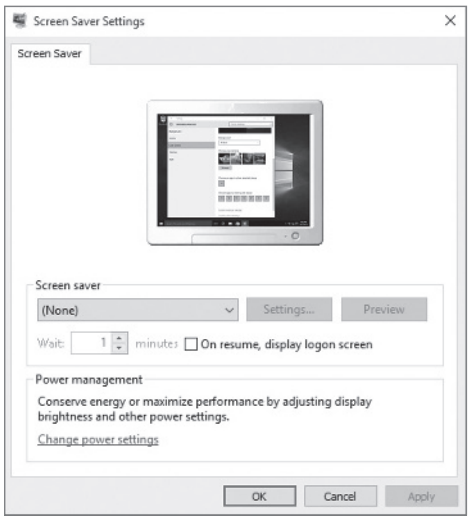


Figure 1-22

Configuring the screen saver



Configuring the Start Menu

Windows 10 uses the Modern UI/Metro style that utilizes the Start menu. The Start menu contains a list of applications and Desktop programs via pinned tiles. The pinned tiles have different sizes and colors. In addition, you can pin folders to the new Start screen.

To pin an item to the Start screen, find a program or file by using the All apps option, by using Cortana, or by using File Explorer. Then right-click the program, application or folder and choose Pin to Start in App bar or popup menu. Some tiles allow for additional actions. For example, when you pin This PC to the Start menu, you can quickly open Computer Management or System Properties or you can connect/disconnect network drives.

Configuring User Profiles

A ***user profile*** is a series of folders, associated with a specific user account that contain personal documents, user-specific registry settings, Internet favorites, and other personalized information—everything that provides a user's familiar working environment. On a Windows 10 computer, user profiles are stored in the Users folder, within subfolders named for the user accounts.

On computers running Windows 10, user profiles automatically create and maintain the desktop settings for each user's work environment on the local computer in a folder beneath C:\Users. The system creates a new user profile for each user logging on at the computer for the first time.

Each user folder contains a separate user profile for that person. A typical user profile consists of the following folders, some of which are hidden, plus a hidden registry file:

- AppData
- Contacts
- Desktop
- Downloads
- Favorites
- Links
- My Documents
- My Music
- My Pictures
- My Videos
- Saved Games
- Searches

When a user logs on at the workstation using a local or domain account, the system loads that individual's profile and uses it throughout the session until the user logs off. During the session, the My Documents folder in the user's profile becomes the operative My Documents folder for the system, as do all the other folders in the profile.

There are three main types of user profiles, as follows:

- ***Local user profile***: A profile that Windows automatically creates when each user logs on at the computer for the first time. The local user profile is stored on the computer's local hard disk.
- ***Roaming user profile***: A copy of a local user profile that is stored on a shared server drive, making it accessible from anywhere on the network.
- ***Mandatory user profile***: A roaming profile that users cannot change. Administrators use mandatory user profiles to enforce particular desktop settings for individuals or for a group of users. A fourth variation, called a super-mandatory profile, requires the user to access the server-based profile or the logon fails.

USING ROAMING PROFILES

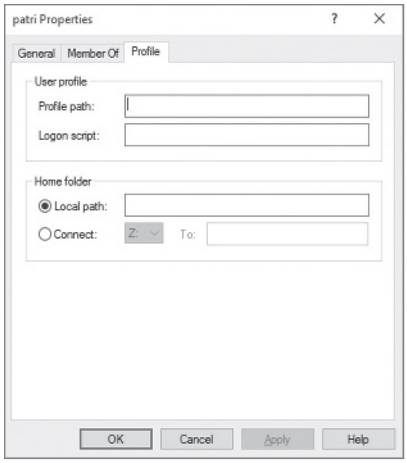
To support users who work at multiple computers on the same network, administrators can create roaming user profiles.

A roaming user profile is simply a copy of a local user profile that is stored on a network share (to which the user has appropriate permissions), so that the user can access it from any computer on the network. No matter which computer a user logs on from, he or she always receives the files and desktop settings from the profile stored on the server.

To enable a user to access a roaming user profile, rather than a local profile, you must open the user's Properties sheet to the Profile tab, as shown in Figure 1-23, and type the location of the roaming profile in the Profile Path field.

Figure 1-23

The Profile tab of a user's Properties sheet



Then, the next time the user logs on, Windows 10 accesses the roaming user profile in the following manner:

1. During the user's first logon, the computer copies the entire contents of the roaming profile to the appropriate subfolder in the Users folder on the local drive. Having the roaming user profile contents stored on the local drive enables the user access to the profile during later logons, even if the server containing the roaming profile is unavailable.
2. The computer applies the roaming user profile settings to the computer, making it the active profile.
3. As the user works, the system saves any changes he or she makes to the user profile to the copy on the local drive.
4. When the user logs off, the computer replicates any changes made to the local copy of the user profile back to the server where the roaming profile is stored.
5. The next time the user logs on at the same computer, the system compares the contents of the locally stored profile with the roaming profile stored on the server. The computer copies only the roaming profile components that have changed to the copy on the local drive, which makes the logon process shorter and more efficient.

You should create roaming user profiles on a file server that you back up frequently, so that you always have copies of your users' most recent profiles. To improve logon performance for a busy network, place the users' roaming profiles folder on a member server instead of a domain controller.

USING MANDATORY USER PROFILES

A mandatory user profile is simply a read-only roaming user profile. Users receive files and desktop settings from a server-based profile, just as they would with any roaming profile, and they can modify their desktop environments while they are logged on. However, because the profile is read-only, the system cannot save any profile changes back to the server when the users log off. The next time the user logs on, the server-based profile will be the same as during the previous logon.

Windows 10 downloads the mandatory profile settings to the local computer each time the user logs on. You can assign one mandatory profile to multiple users who require the same desktop settings, such as a group of users who all do the same job. Because the profile never changes, you do not have to worry about one user making changes that affect all of the other users. Also, a mandatory profile makes it possible to modify the desktop environment for multiple users by changing only one profile.

To create a mandatory user profile, rename the Ntuser.dat file in the folder containing the roaming profile to Ntuser.man. The Ntuser.dat file consists of the Windows 10 system registry settings that apply to the individual user account and contains the user environment settings, such as those controlling the appearance of the desktop. Renaming this file with a .man extension makes it read-only, preventing the client computers from saving changes to the profile when a user logs off.

MIGRATING USER PROFILES

There are two basic methods for deploying Windows 10 to a client while retaining the user profile settings: upgrade and migration. In an upgrade, you install Windows 10 on the computer running an earlier operating system. Windows 10 overwrites the old OS, but all of the user profiles already on the computer remain in place. In a migration, you copy the user profile information from the old operating system to some temporary medium and transfer it to a new, clean installation of Windows 10.

Microsoft provides the following two tools for migrating files and settings to new computers:

- ***Windows Easy Transfer***: Designed for the migration of a single computer, Easy Transfer is a wizard-based utility that makes it possible to migrate user profile information for multiple users from one computer to another.
- ***User State Migration Tool***: Designed for large-scale enterprise deployments, the User State Migration Tool is a command-line utility that can migrate profile information for multiple users on multiple computers.

In the following sections, you will learn the procedure for using Windows Easy Transfer to migrate user profile settings from a Windows 7 workstation, a Windows 8/8.1 workstation, or a Windows 10 workstation to a new Windows 10 workstation. You will also learn some basic facts about using the User State Migration Tool.

Configuring Display Settings

Windows 10 has several display settings, but you're most likely to modify the resolution, color depth, and font size most often. You can modify each setting to suit a particular application.

When you right-click the desktop and choose Display Settings, the Display page opens. This is where you can change the orientation and the size of the text and apps, as shown in Figure 1-24.

To open the screen resolution window (as shown in Figure 1-25), click the Advanced display settings option. This is where you choose which monitor to use (if your computer is connected to two or more monitors) and whether to display content in a landscape orientation or a portrait orientation. You can also configure settings to connect a projector to your computer. Three other important display settings you might want to adjust for specific purposes are resolution, color depth, and font size.

Resolution refers to the number of pixels that create the "image," that is, everything you see on the screen. ***Resolution*** has a horizontal value and a vertical value, such as 1200 x 768 or 1600 x 900. The Windows desktop expands itself to fit whatever resolution you select, so you always have a full background. Similarly, the Taskbar stretches across the bottom of the screen, regardless of the resolution you choose.

You might need to change a computer's screen resolution for a variety of reasons, such as when you're accommodating a visually impaired user or when you're using an external projector.

Figure 1-24

Opening the Display Settings page

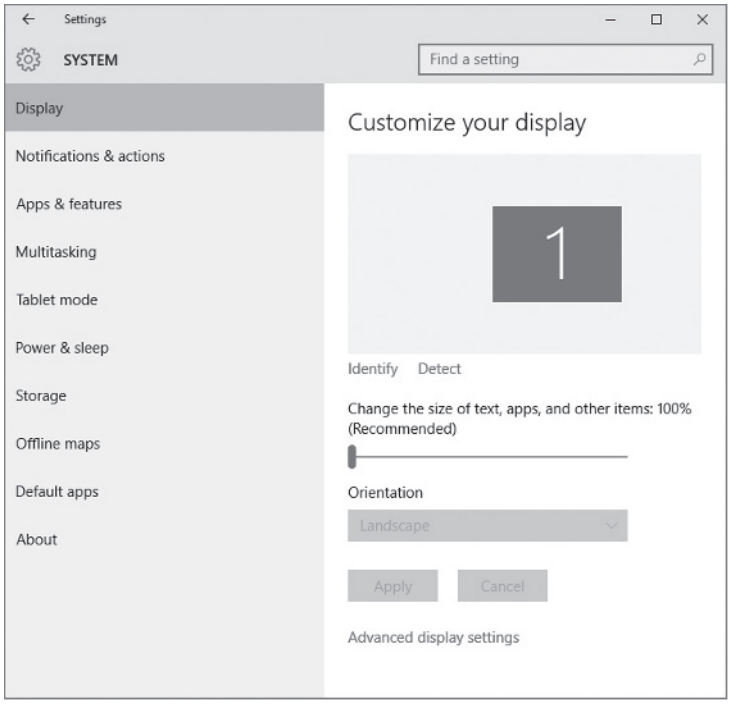
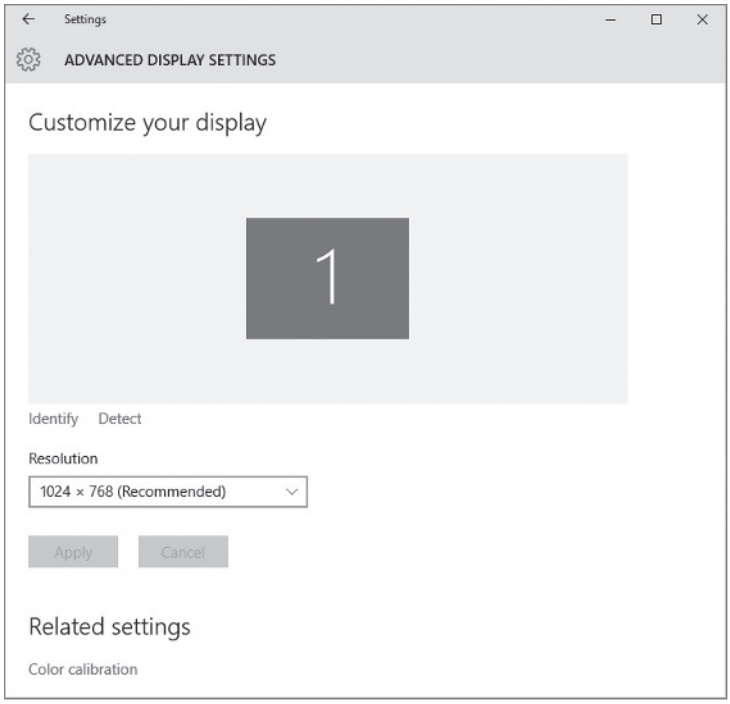


Figure 1-25

The Advanced Display Settings page



Your computer's monitor has a minimum and a maximum resolution it can display, so Windows 7 gives you a range of resolutions to choose from.

Screen fonts are usually measured in dots per inch (dpi). You can enhance the appearance of your desktop by adjusting font size dpi to improve the readability of pixelated or illegible fonts.

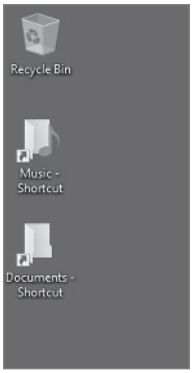
Configuring Shortcuts

Shortcuts are icons you can click to start a program or go to a location without requiring any extra steps. Shortcuts save time because you don't have to use several keystrokes or click several menus or commands.

An icon is a small, visual symbol of a computer resource, such as a program, folder, file, or drive. To access an actual computer resource, click or double-click its icon. Some icons are located on the desktop, others are in the Start menu, and still others might appear in the list of files and folders in Windows Explorer.

A ***shortcut*** (see Figure 1-26) is an icon or link that gives you quick access to an original resource. The links you see in Control Panel are also considered shortcuts. Because a shortcut only points to a resource, deleting a shortcut does not delete the actual item. You can usually distinguish a shortcut icon from the original item it refers to because the shortcut has a small arrow in the shortcut icon's lower-left corner.

Figure 1-26
Shortcut icons



If you regularly access a particular folder, for example, you can create a shortcut to that folder on the desktop. Whenever you want to open that folder, double-click the icon instead of launching Windows Explorer and navigating to the folder to open it.

CREATE AND DELETE A SHORTCUT

GET READY. To create a folder shortcut on the desktop, perform the following steps.

1. In File Explorer, point to the folder for which you want to create a shortcut.
2. Right-click the folder and choose **Send To > Desktop (create shortcut)**.
3. To delete a shortcut icon:
4. Right-click it, choose **Delete**, and then click **OK**. The shortcut is removed and sent to the Recycle Bin.

Understanding Group Policy

Group Policy is one of the most powerful features of Active Directory that controls the working environment for user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment. For example, you can use Group Policy to specify how often a user must change his password, set the desktop background image and screensaver on a person's computer, or configure spell-checking so that it is required before a user can send an email.

There are literally thousands of settings that can be used to restrict certain actions, make a system more secure, or standardize a working environment. A setting can control a computer registry, NTFS security, an audit and security policy, software installation, folder redirection, offline folders, or log on and log off scripts. Group Policy is one of the most powerful features of Active Directory that controls the working environment for user accounts and computer accounts. Group Policy (see Figure 1-27) provides the centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment. As each server version is released, Microsoft usually adds additional parameters.

Group Policy objects (GPOs) are collections of user and computer settings, including the following:

- **System settings**: Application settings, desktop appearance, and behavior of system services.
- **Security settings**: Local computer, domain, and network security settings.
- **Software installation settings**: Management of software installation, updates, and removal.
- **Scripts settings**: Scripts for when a computer starts or shuts down and for when a user logs on and off.
- **Folder redirection settings**: Storage for users' folders on the network. For example, the *Redirect to the local user profile location* option will move the location of the folder to the local user profile under the Users folder.

APPLYING GROUP POLICY

Group Policy can be set locally on a workstation or set at different levels (site, domain, or organizational unit) within Active Directory. Generally speaking, you will not find as many settings locally as you will at the site, domain, or OU level. When group policies are applied, they are applied in the following order:

1. Local
2. Site
3. Domain
4. OU

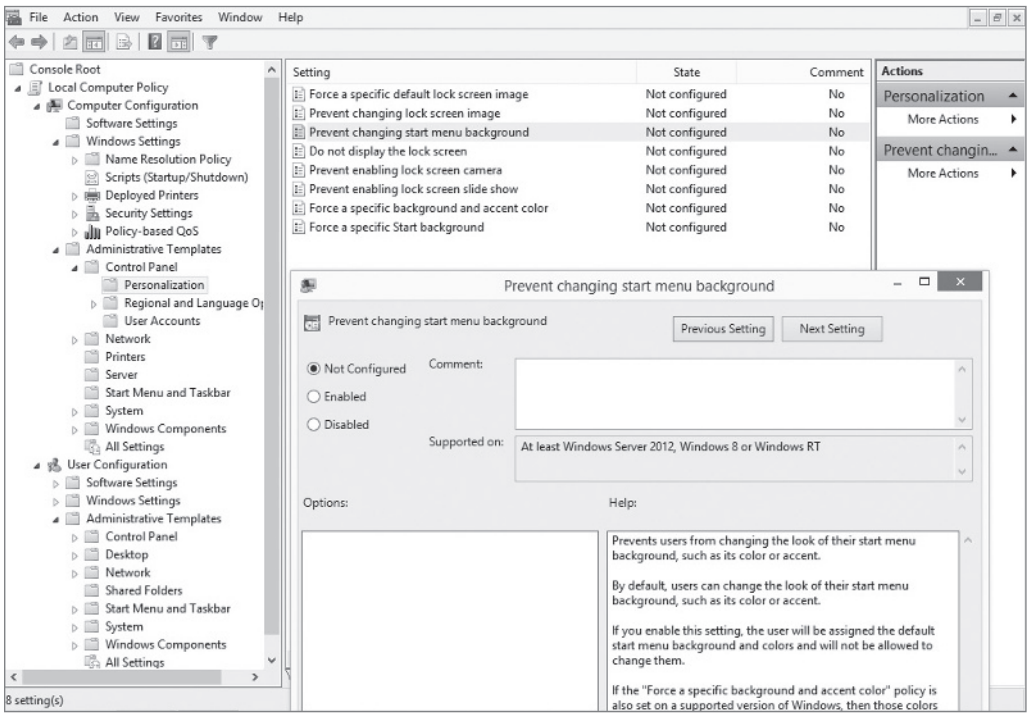
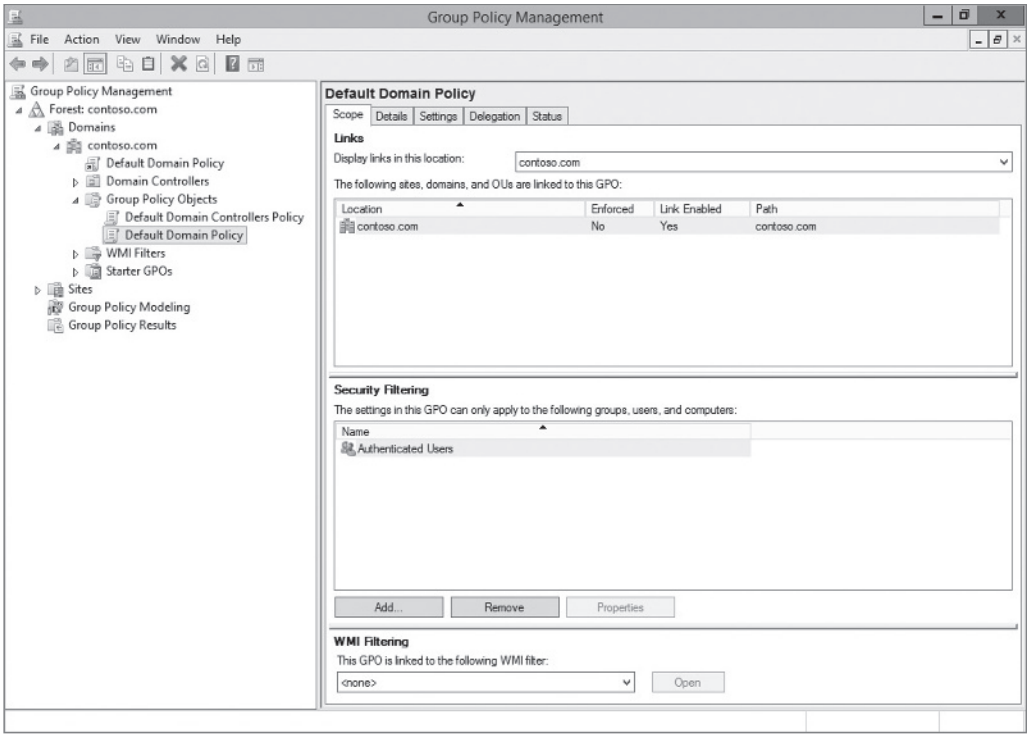


Figure 1-27

Group Policy Editor

Figure 1-28

The Group Policy Management Console



If you configure a Group Policy setting at the site, domain, or OU level and that setting contradicts a setting configured at the local policy level; the local policy setting will be overridden. Generally speaking, if you have a policy setting that conflicts with a previous executed setting, the more recent executed setting remains in effect (see Figure 1-28).

ACCESS THE LOCAL GROUP POLICY EDITOR

GET READY. You can open the Local Group Policy Editor by using gpedit.msc at a command line or by using the Microsoft Management Console (MMC). To open the Local Group Policy Editor from the command line, perform the following steps.

1. Open MMC by clicking **Start**, clicking in the Start Search box, typing mmc, and then pressing Enter.)
2. On the **File** menu, click **Add/Remove Snap-in**.
3. In the Add or Remove Snap-in dialog box, click **Group Policy Object Editor**, and then click **Add**.
4. In the Select Group Policy Object dialog box, click **Browse**.
5. Click **This computer** to edit the Local Group Policy object, or click **Users** to edit Administrator, Non-Administrator, or per-user Local Group Policy objects.
6. Click **Finish**.

Most times, you only need to access the security settings that you found in the local policy. This can be done by opening the Local Security Policy from Administrative Tools.

CONFIGURING GROUP POLICY SETTINGS

There are thousands of settings available with group policies. In addition, as each version of Windows is released, new settings are added to allow administrators to configure new technology that has been added to Windows, provide control that was not available previously, or provide more granular control.

As discussed, group policies are organized according to computer settings (contained in the Computer Configuration node) and user settings (contained in the User Configuration node). The ***Computer Configuration*** node contains settings that are applied to the computer regardless of who logs on to the computer. By default, computer settings are applied when the computer is started. The ***User Configuration*** node contains settings that are applied when the user logs on. Group policy settings are refreshed every 90 minutes with a random delay of 30 minutes (giving a random range between 90 minutes and 120 minutes). On domain controllers, group policies get refreshed every five minutes.

Starting with Windows Server 2008, the Computer Configuration and User Configuration nodes are divided into Policies and Preferences nodes. Policies include the traditional settings that were available with earlier versions of Windows, but also have many new settings that were not available previously. Preferences allow you to configure additional Windows settings that were not available previously and they allow more control on how the settings are applied to the clients.

Computer Configuration\Policies can be organized according to the following nodes:

- **Software Settings**: Contains only one node, Software installation, which allows you to install and maintain software within your organization.
- **Windows Settings**: Allows you to configure Windows settings, including Name Resolution Policy, Scripts (Startup/Shutdown), Security Settings, and Policy-Based QoS nodes.
- **Administrative Templates**: Contains registry-based Group Policy settings that are used to configure the computer environment, such as the Control Panel, Printers, System, and Windows components.

Software Configuration\Policies can be divided into the following nodes:

- **Software Settings**: Contains only one node, Software installation, which allows you to install and maintain software within your organization.
- **Windows Settings**: Allows you to configure Windows settings, including Scripts (Logon/Logoff), Security Settings, Folder Redirection, and Policy-Based QoS nodes.
- **Administrative Templates**: Contains registry-based Group Policy settings that are used to configure the user environment, such as the Control Panel, Printers, System, and Windows components.

USING ADMINISTRATIVE TEMPLATES

Windows 10 includes thousands of Administrative Template policies, which contain registry-based policy settings that are used to configure the user and computer environment. For example, to configure the user's desktop image or a default screen saver, you would use an Administrative Template policy.

Administrative Templates can be located under both Computer Configuration and User Configuration. The requirements for an Administrative Template setting, such as which operating system supports the setting and the description of the feature, are displayed:

- On the Extended tab when you click to select an Administrative Template setting
- When you double-click an Administrative Template setting

When configuring Administrative Templates, there are three states:

- **Not Configured**: The registry key is not modified or overwritten.
- **Enabled**: The registry key is modified by this setting.
- **Disabled**: The Disabled settings undo a change made by a prior Enabled setting.

If you want to undo the group policy, removing the group policy does not necessarily remove the setting from a computer that has the setting configured with a GPO. In these cases, you

need to change the policy to Disabled (or create a second policy) and is applied to the computer and/or user. After the policy is applied, the policy can be removed. The policy can also be manually removed using the registry editor (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies and HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies).

Some Administrative Templates will be used to configure a setting such as specifying a desktop image or specifying a screen saver. Although these settings are configured with group policies, some of these settings can be changed while the computer is running. However, when the group policy is reapplied, the setting will revert back to the setting defined with the GPO. Other settings will used to lock down a computer so that users cannot modify a setting or hide the setting from the user.

CONFIGURE THE DESKTOP BACKGROUND IMAGE WITH GROUP POLICIES

GET READY. To configure the desktop background image with group policies, perform the following steps.

1. Open the **Group Policy Management Editor** for the GPO you want to configure.
2. Navigate to **User Configuration\Policies\Administrative Templates\Desktop\Desktop**.
3. Double-click **Desktop Wallpaper**. The Desktop Wallpaper dialog box opens.
4. Click **Enabled**.
5. In the Wallpaper Name text box, type the path and name of an image file.
6. Click **OK** to close the Desktop Wallpaper dialog box. The Desktop Wallpaper shows as Enabled.
7. Close the Group Policy Management Editor window.

■ Configuring Drive Encryption

THE BOTTOM LINE

Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, that file remains encrypted when the file is stored on disk. ***Decryption*** is the process of converting data from encrypted format back to its original format. You can use encryption to help protect files on a computer.

CERTIFICATION READY
Configure drive encryption
1.3

Today, newer versions of Windows offer two file encrypting technologies: Encrypting File System (EFS) and BitLocker Drive Encryption. EFS protects individual files or folders; BitLocker protects entire volumes.

Preparing for File Encryption

Encrypting File System (EFS) can encrypt files on an NTFS volume and those files cannot be used unless the user has access to the keys required to decrypt the information. By default, when you encrypt a file with EFS, the file or folder turns green to show that the file is encrypted.

After a file has been encrypted, you do not have to manually decrypt an encrypted file before you can use it. Instead, you work with the file or folder just like any other file that is not encrypted. When you open a file that is encrypted with EFS, the file is automatically

decrypted as needed. When you save the file, it is automatically decrypted. However, if another user tries to access the same file, he cannot open it because he does not have the proper key to open the file.

EFS uses an encryption key to encrypt the data, which is stored in a digital certificate. The first time a user encrypts a file or folder, an encryption certificate and key are created and bound to the user account. The user who creates the file is the only person who can read it. As the user works, EFS encrypts the files using a key generated from the user's public key. Data encrypted with this key can be decrypted only by the user's personal encryption certificate, which is generated using a private key.

CONFIGURING EFS

To encrypt or decrypt a folder or file, enable or disable the encryption attribute just as you set any other attribute, such as read-only, compressed, or hidden. If you encrypt a folder, all files and subfolders created in the encrypted folder are automatically encrypted. Microsoft recommends that you encrypt at the folder level. You can also encrypt or decrypt a file or folder using the Cipher command.

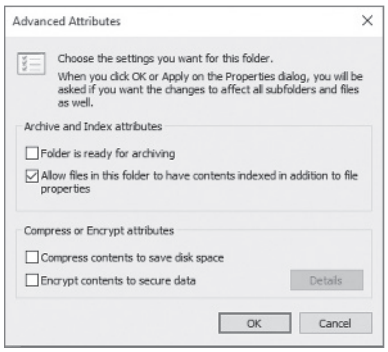
ENCRYPT A FOLDER OR FILE USING EFS

GET READY. To encrypt a folder or file, perform the following steps.

1. Right-click the folder or file you want to encrypt and choose **Properties**. The Properties dialog box opens.
2. Click the **General** tab, and then click **Advanced**. The Advanced Attributes dialog box appears (see Figure 1-29).

Figure 1-29

The Advanced Attributes dialog box



3. Select the **Encrypt contents to secure data** checkbox.
4. Click **OK** to close the Advanced Attributes dialog box.
5. Click **OK** to close the Properties dialog box.
6. If you encrypt a file in an unencrypted folder, a warning appears. If you want to encrypt only the file, select **Encrypt the file only** and then click **OK**. If you want to encrypt the folder and all content in the folder, select the **Encrypt the file and its parent folder (recommended)** option. Click **OK**.
7. If you encrypt a folder, a message prompts you to confirm the changes. If you want to encrypt only the folder, select **Apply changes to this folder only**. If you want to apply to all folders, select **Apply changes to this folder, subfolders and files**. Click **OK** to close the **Confirm Attribute Changes** dialog box.

DECRYPT A FOLDER OR FILE

GET READY. To decrypt a folder or file, perform the following steps.

1. Right-click the folder or file you want to decrypt and choose **Properties.** The Properties dialog box opens.
2. Click the **General** tab and then click **Advanced**. The Advanced Attributes dialog box opens.
3. Clear the **Encrypt contents to secure data** checkbox.
4. Click **OK** to close the Advanced Attributes dialog box.
5. Click **OK** to close the Properties dialog box.
6. When you are prompted to confirm the changes, click **OK**. When you want to decrypt only the folders, select **Apply changes to this folder only**. When you want to apply to all folders, select **Apply changes to this folder, subfolders and files**.

When working with EFS, keep the following in mind:

- You can encrypt or compress NTFS files only when using EFS; you can't do both. If the user marks a file or folder for encryption, that file or folder is uncompressed.
- If you encrypt a file, it is automatically decrypted if you copy or move the file to a volume that is not an NTFS volume.
- Moving unencrypted files into an encrypted folder automatically causes those files to be encrypted in the new folder.
- Moving an encrypted file from an EFS-encrypted folder does not automatically decrypt files. Instead, you must explicitly decrypt the file.
- Files marked with the System attribute or that are in the root directory cannot be encrypted.
- Remember that an encrypted folder or file does not protect against the deletion of the file, listing the files or directories. To prevent deletion or listing of files, use NTFS permissions.
- Although you can use EFS on remote systems, data that is transmitted over the network is not encrypted. If encryption is needed over the network, use ***SSL/TLS (Secure Sockets Layer/Transport Layer Security)*** or IPsec. SSL/TLS uses a digital certificate to encrypt a web page such as when you access an https:// website using a browser. ***Internet Protocol Security (IPsec)*** is a protocol suite that secures IP communications by authenticating and encryption each IP packet of a communication session.

Configuring BitLocker

Unlike EFS, BitLocker allows you to encrypt the entire volume. Therefore, if a drive or laptop is stolen, the data is still encrypted even if the thief installs it in another system for which he is an administrator.

BitLocker Drive Encryption (BDE) is the feature in Windows since Windows Vista and Windows Server 2008 that can use a computer's ***Trusted Platform Module (TPM)***, which is a microchip that is built into a computer. It is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft. BitLocker Drive Encryption can use a TPM to validate the integrity of a computer's boot manager and boot files at startup, and to guarantee that a computer's hard disk has not been tampered with while the operating system was offline. BitLocker Drive Encryption also stores measurements of core operating system files in the TPM.

TAKE NOTE*

For workstations, BitLocker is a feature of Windows 7 Enterprise, Windows 7 Ultimate, Windows 8/8.1 Pro, Windows 8/8.1 Enterprise, Windows 10 Pro, and Windows 10 Enterprise. It is not supported on other editions of Windows.

The system requirements of BitLocker are as follows:

- Because BitLocker stores its own encryption and decryption key in a hardware device that is separate from your hard disk, you must have one of the following:
  - A computer with TPM. If your computer was manufactured with TPM version 1.2 or higher, BitLocker stores its key in the TPM.
  - A removable USB memory device, such as a USB flash drive. If your computer doesn't have TPM version 1.2 or higher, BitLocker stores its key on the flash drive.
- Your computer must have at least two partitions: a system partition (containing the files needed to start your computer and must be at least 350 MB for computers running Windows 10) and an operating system partition (containing Windows). The operating system partition is encrypted and the system partition remains unencrypted so that your computer can start. If your computer doesn't have two partitions, BitLocker creates them for you. Both partitions must be formatted with the NTFS file system.
- Your computer must have a BIOS that is compatible with TPM and supports USB devices during computer startup. If this is not the case, you need to update the BIOS before using BitLocker.

TAKE NOTE*

BitLocker is not commonly used on servers, but may become more common in the future as BitLocker has been improved to work on failover cluster volumes and Storage Area Networks (SANs). Instead, most organizations use physical security for servers (such as locked server room and/or server rack that can be accessed only by a handful of people) to prevent the computer and drives from being stolen.

Instead, BitLocker is more commonly used with mobile computers and, to a lesser extent, desktop computers. However, it takes a domain infrastructure with Windows servers to get the most benefits from BitLocker and the management of systems running BitLocker.

BitLocker supports NTFS, FAT16, FAT32 and ExFAT on USB, Firewire, SATA, SAS, ATA, IDE, and SCSI drives. It does not support CD File System, iSCSI, Fiber Channel, eSATA, and Bluetooth. BitLocker also does not support dynamic volumes; it supports only basic volumes.

BitLocker has five operational modes for OS drives, which define the steps involved in the system boot process. These modes, in descending order from most secure to least secure, are as follows:

- **TPM + startup PIN + startup key**: The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a personal identification number (PIN) and insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.
- **TPM + startup key**: The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.
- **TPM + startup PIN**: The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a PIN before the system can unlock the BitLocker volume and complete the system boot sequence.
- **Startup key only**: The BitLocker configuration process stores a startup key on a USB flash drive, which the administrator must insert each time the system boots. This mode

does not require the server to have a TPM chip, but it must have a system BIOS that supports access to the USB flash drive before the operating system loads.

- **TPM only**: The system stores the BitLocker volume encryption key on the TPM chip, and accesses it automatically when the chip has determined that the boot environment is unmodified. This unlocks the protected volume and the computer continues to boot. No administrative interaction is required during the system boot sequence.

When you use BitLocker on fixed and removable data drives that are not the OS volume, you can use one of the following:

- Password
- Smart card
- Automatic Unlock

When you enable BitLocker using the BitLocker Drive Encryption control panel, you can select the TPM + startup key, TPM + startup PIN, or TPM only option. To use the TPM + startup PIN + startup key option, you must first configure the Require additional authentication at startup Group Policy setting, found in the Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives container.

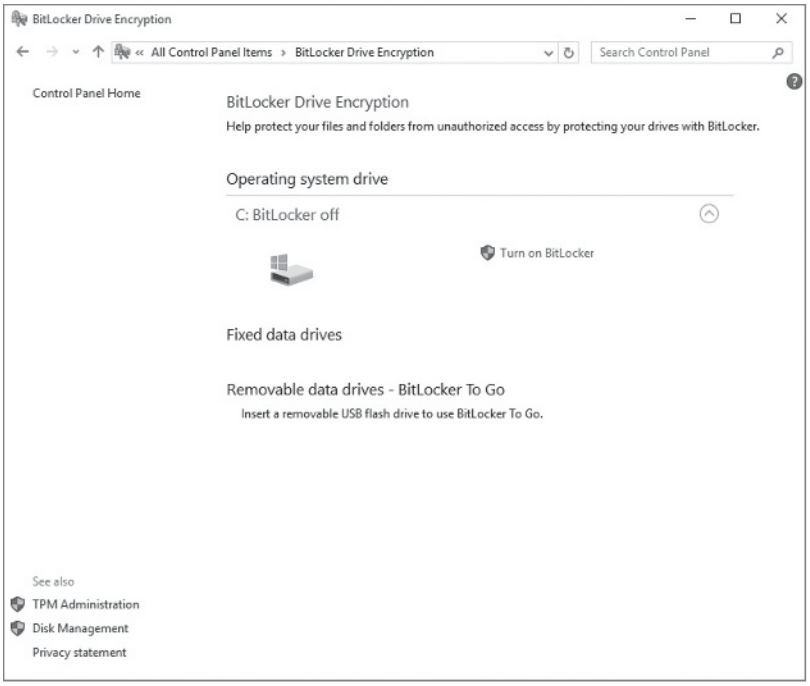
DETERMINE WHETHER YOU HAVE TPM

GET READY. To find out whether your computer has TPM security hardware, perform the following steps.

1. Open the **Control Panel**.
2. Click **System and Security** and click **BitLocker Drive Encryption**. The BitLocker Drive Encryption window opens (see Figure 1-30).

Figure 1-30

The BitLocker Drive Encryption window



3. In the left pane, click **TPM Administration**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

The TPM Management on Local Computer snap-in tells you whether your computer has the TPM security hardware. If your computer doesn't have it, you'll need a removable USB memory device to turn on BitLocker and store the BitLocker startup key that you need whenever you start your computer.

If your computer does not have TPM and you need to encrypt the C drive with BitLocker, you will have to set the Allow BitLocker without a compatible TPM option to Require additional authentication at startup using a GPO. This setting is located at Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives. Double-click the Require additional authentication at startup setting, select Enabled, and select the Allow BitLocker without a compatible TPM option. Click OK to save the new setting.

TURN ON BITLOCKER

GET READY. To turn on BitLocker for the C drive on a computer running Windows 10, perform the following steps.

1. Click **Start** and then click the **Control Panel**.
2. Click **System and Security** and then click **BitLocker Drive Encryption**. The BitLocker Drive Encryption window opens.
3. Click **Turn on BitLocker** for the volume that you want to encrypt. A BitLocker Drive Encryption (X:) window opens.

MORE INFORMATION

If your computer has a TPM chip, Windows provides a TPM Management console that you can use to change the chip's password and modify its properties.

4. On the Choose how you want to unlock this drive page, select **Enter a password**. Type a password in the Enter your password text box and the Reenter your password text box. Click **Next**.
5. On the How do you want to back up your recovery key? page, click **Save to a file**.
6. In the Save BitLocker recovery key as dialog box, click **Save**.
7. After the file is saved, make sure the key is stored in a safe place. Then click **Next**.
8. On the Are you ready to encrypt this drive page, the *Run BitLocker system check* option is already selected. Click **Continue**.
9. When a message indicates the computer must be restarted, click **Restart now**.

When the encryption process is complete, you can open the BitLocker Drive Encryption Control Panel to ensure that the volume is encrypted or to turn off BitLocker, such as when you want to perform a BIOS upgrade or other system maintenance.

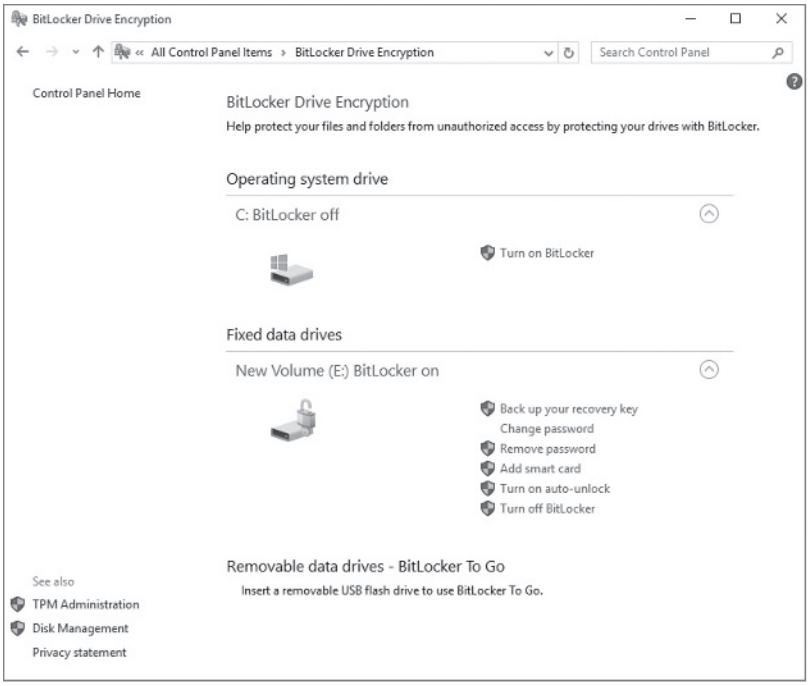
The BitLocker Control Panel applet enables you to recover the encryption key and recovery password at will. Figure 1-31 shows the following options available after you use BitLocker to encrypt a drive:

- Back up your recovery key
- Change password
- Remove password
- Add smart card
- Turn on auto-unlock
- Turn off BitLocker

You should consider carefully how to store this information, because it allows access to the encrypted data. It is also possible to escrow this information into Active Directory.

Figure 1-31

The BitLocker applet options for a BitLocker-encrypted volume



Standard users can change the password or PIN if they know the current PIN or password. By default, a user has five attempts to type the current PIN or password. When this happens, the administrator has to reset the volume PIN or password or the system needs to be rebooted. To make sure that password or PIN is not too easy to guess, you can define how complex the password is by using a group policy. To define the complexity, enable and configure the Configure use of passwords for fixed data drives settings found in Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\.

■ Configuring Updates

THE BOTTOM LINE

Intruders and some viruses, worms, rootkits, spyware, and adware gain access to a system by exploiting security holes in Windows, Internet Explorer, Microsoft Office, or other software applications. Therefore, the first step you should take to protect yourself against malware is to keep your system up to date with the latest service packs, security patches, and other critical fixes.

Microsoft routinely releases security updates on the second Tuesday of each month, commonly known as ***Patch Tuesday***. However, in the future, Microsoft might release patches as soon as they become available.

Because computers are often used as production systems, you should test any updates to make sure they do not cause problems for you. Although Microsoft performs intensive testing, occasionally problems do occur, either as a bug or as a compatibility issue with third-party software. Therefore, always be sure you have a good backup of your system and data files before you install patches so that you have a back-out plan if necessary.

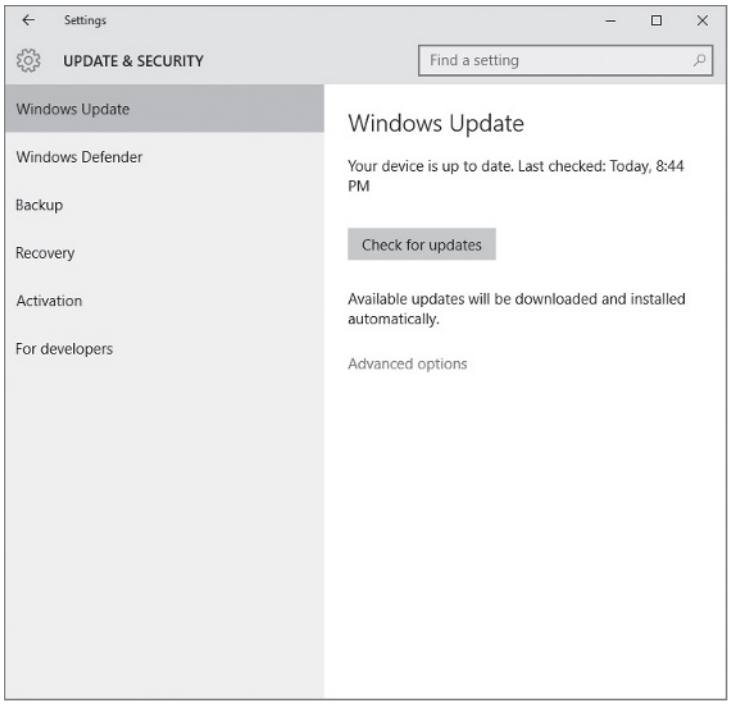
CERTIFICATION READY
Configure updates
1.4

Understanding Windows Update

Windows Update provides your Windows 10 users with a way to keep their computers current by checking a designated server. The server provides software that patches security issues, installs updates that make Windows and your applications more stable, fixes issues with existing Windows programs, and provides new features. The server can be hosted by Microsoft or it can be set up and managed in your organization by running the Windows Server Update Services (WSUS) or Configuration Manager.

When you first install Windows 10, you can choose how you want Windows Update to function. On a Windows 10 computer, you can open Settings and click Update & security to open the Windows Update page (see Figure 1-32).

Figure 1-32
The Windows Update page



By clicking Advanced options, you can configure for Automatic updates, give updates for other Microsoft products when Windows is updated, defer upgrades, and view your update history (as shown in Figure 1-33).

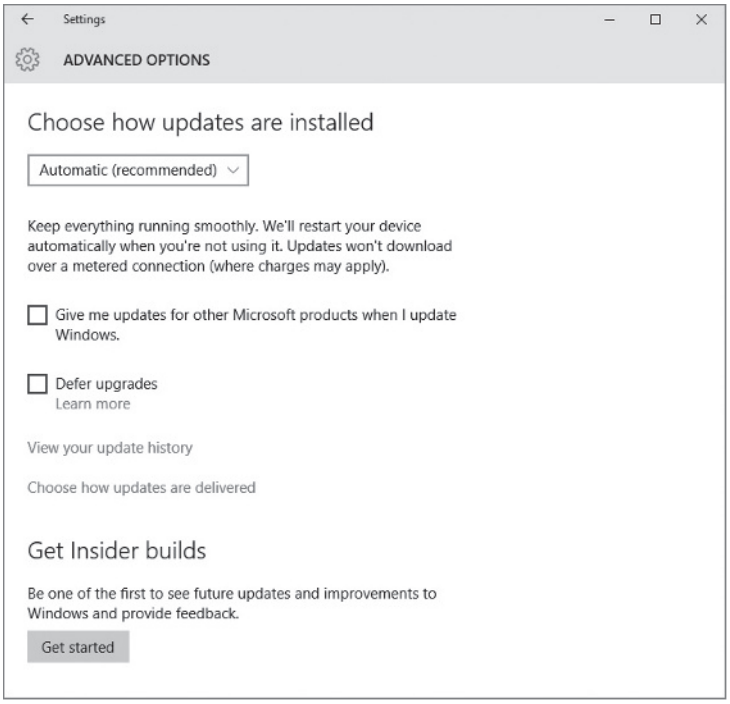
If your computer is part of an enterprise infrastructure, the enterprise organization might automatically configure the update settings via a local Group Policy or a domain-based Group Policy for your user and/or computer account. Group Policy settings related to Windows Update can be found in the following locations:

- Computer Configuration > Policies\Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates
- User Configuration > Policies > Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates

For corporations, you can also use ***Windows Server Update Service (WSUS)*** or System Center Configuration Manager to keep your systems updated. Smaller organizations might use WSUS or cloud-based services such as Microsoft Intune to keep systems up-to-date. The advantage of using one of these systems is that it allows you to test the patch, schedule the

Figure 1-33

The Windows Update Advanced Options page

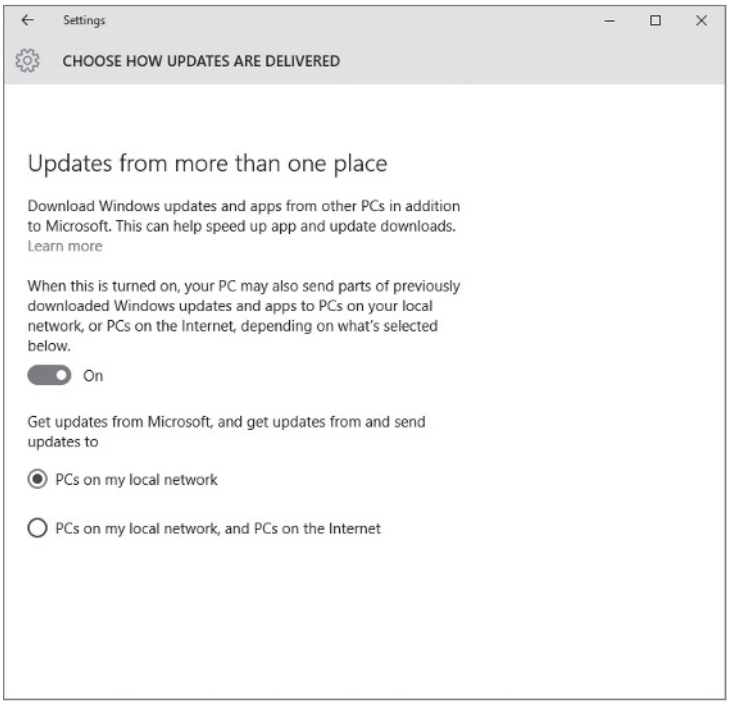


updates, and prioritize client updates. Once you determine a patch is safe, you can enable it for deployment.

If you click the Choose how updates are delivered option, the Updates from more than one place page displays (see Figure 1-34). Unless you are part of a corporation that is using WSUS or Configuration Manager, you must use your Internet connection to retrieve updates from Microsoft. Starting with Windows 10, you can enable the Updates from more than one place option, which also allows you to get updates from other computers on the same network as your local computer and from computers on the Internet.

Figure 1-34

The Updates from more than one place page



Understanding App Updates

As applications became more sophisticated, they were provided more access so that they could do more on a system. Unfortunately, it was not long before these apps became targets of intruders and malware. To fix problems with applications and to keep a system or device secure, you need to keep applications current with the latest updates.

For Microsoft applications, you can find Microsoft updates using Windows Update, WSUS, Configuration Manager, or Microsoft Intune. To enable updates for Microsoft applications, you can click Change settings and then select the Give me updates for other Microsoft products when I update Windows option.

Some non-Microsoft products also release regular updates. Some of these applications (such as Adobe products, and Java) have mechanisms that will automatically check for updates and notify you that updates are available or they will automatically install those updates.

Understanding Device System Updates

For all intents and purposes, mobile devices (including smart phones and tablets) are computers that can run a wide range of applications. Since these devices usually contain personal and corporate information, these devices are also targets of intruders and malware. Therefore, you need to keep the operating system and the applications up-to-date so that security patches can be applied as they are released.

Applications on smart phones and tablets are usually updated through stores such as Microsoft Store, Google Play, and iTunes. Fortunately, these stores offer mechanisms to notify you when updates are available and to automatically install these updates as they become available. For example, for Windows 10 store the live tile for the Store app change to indicate the number of app updates that were available, launch the Store app, click the updates link, select all the updates, click Install. By default, Windows 10 has been automated, whereas these updates are automatically downloaded and installed as soon as they are available with no user interaction.

SUMMARY SKILL MATRIX

In this lesson you learned:

- Windows 10 is a robust and flexible system that is made to work on and support a wide range of hardware. For example, Windows 10 can work on a tablet, a laptop, or a desktop computer. Windows 10 also supports mobile devices so that you can take your computer or device with you while accessing your files and programs.
- Microsoft accounts enable you to synchronize your desktop across multiple Windows 10 devices.
- A user account is used to identify a user or other identity on a system, which can be used in authentication, authorization, and auditing. In Windows, user accounts provides different levels of control over the organization's computers and resources. Microsoft accounts enable you to synchronize your desktop across multiple Windows 10 devices.
- A computer is a collection of hardware devices, each of which requires a piece of software called a device driver in order to function. Windows 10 includes a large library of device drivers, but it is still sometimes necessary to obtain them yourself. Device Drivers are managed by the Devices and Printers folder and Device Manager.

- Group Policy is one of the most powerful features of Active Directory that controls the working environment for user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and user settings in an Active Directory environment.
- Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk. Decryption is the process of converting data from encrypted format back to its original format. To help protect files on a computer, you can use encryption.
- Today, newer versions of Windows offer two file encrypting technologies: Encrypting File System (EFS) and BitLocker Drive Encryption. EFS protects individual files or folders; BitLocker protects entire volumes.
- Intruders and some viruses, worms, rootkits, spyware, and adware gain access to a system by exploiting security holes in Windows, Internet Explorer, Microsoft Office, or other software applications. Therefore, the first step you should take to protect yourself against malware is to keep your system up to date with the latest service packs, security patches, and other critical fixes.

■ Knowledge Assessment

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. _____ enable you to synchronize your desktop across multiple Windows 10 devices.
2. A _____ is a series of folders, associated with a specific user account that contains personal documents and settings.
3. The _____ is a microchip that is built into a computer.
4. To protect computers against intruders and malware, you must _____.
5. A Windows application that has dynamic content can be viewed at any time from _____.
6. The primary configuration tool for Windows is the _____.
7. Computer Management, Event Viewer, and GPO Editor are based on the _____.
8. For a device to operate in Windows, you must install a _____.
9. _____ is the process of converting data into a format that cannot be read by another user.
10. The _____ shows important notifications related to the security and maintenance of your computer.

Multiple Choice

Circle the letter that corresponds to the best answer.

1. Which of the following are types of user accounts used in Windows 10? (Choose all that apply)
   a. Domain-based accounts
   b. Local user accounts
   c. Microsoft accounts
   d. Computer centric accounts

2. In Windows 10, how can you minimize network traffic when downloading Windows updates?
   a. You can enable file caching.
   b. You can enable the WriteFile function.
   c. You can enable the Updates from more than one place option.
   d. You can enable Internet Sharing.

3. Which of the following is the best place to manage printers and print drivers?
   a. Device Manager
   b. Devices and Printers folder
   c. Print Manager
   d. Print Configuration Tool

4. In Device Manager, which of the following indicates that a device is not functioning properly?
   a. A red "X
   b. A blue question mark inside white circle
   c. A black exclamation point on yellow field
   d. A white circle with down arrow
   e. A yellow warning symbol with exclamation point

5. Which type of profile allows a user within a corporation to use the same user profile no matter what computer that user accesses?
   a. Local user profile
   b. Persistent user profile
   c. Roaming user profile
   d. Mandatory user profile

6. Which of the following allows you to encrypt an entire volume on a mobile computer?
   a. EFS
   b. DFS
   c. SSL
   d. BitLocker

7. You have updated the device driver for a network adapter, but now the adapter is not being recognized. What should you do?
   a. Check to see if there is a newer driver
   b. Roll back the driver
   c. Reinstall Windows
   d. Run Windows update

8. You want to configure several computers to use the same desktop background and screensaver settings. What is the best way to ensure that all systems are compliant with these settings?
   a. Use Group Policy
   b. Manually configure the systems
   c. Modify the registry
   d. Generate roaming profiles

9. What is the easiest way to ensure all of your computers include the newest Windows updates while still ensuring that those updates do not cause any problems for the users?
   a. Use Task Scheduler
   b. Use WSUS
   c. Use Windows updates
   d. Use GPOs

10. You install an application and now the system does not boot properly. What should you do?
    a. Roll back the application
    b. Reinstall the application
    c. Run Windows Update
    d. Boot the system into safe mode

True / False

Circle T if the statement is true or F if the statement is false.

T F 1. To see the version of Windows, the name of the computer, and the amount of memory, you can open System Properties.

T F 2. To keep a computer secure, you need only to install all new Windows updates.

T F 3. You have applications on your Windows phone that you downloaded from the Microsoft Store. The best way to keep these applications up-to-date is to visit the Windows Update website.

T F 4. The most effective way to protect a document is to use NTFS permissions.

T F 5. For a large organization, you should use Microsoft accounts to manage rights and permissions.

■ Case Projects

Scenario 1-1: Syncing Settings

You own a small business, and to make it easier for you to work whenever needed, you have a desktop computer at home, a desktop computer at your office location, and a laptop—and all machines are running Windows 10. Describe how to ensure that all of the settings are the same for all machines.

Scenario 1-2: Distributing Windows Updates Across a Network

You support Richman Investments, a brokerage firm that employs 20 brokers. Each broker has his own client computer, and the firm has a server running Windows Server. All of the client computers are configured identically.

Over the past six months, some Windows updates have caused the computers to hang, leaving the brokers without computers to conduct business. How can you ensure that the Windows updates that install on client computers will not cause usability issues?

Scenario 1-3: Protecting Laptop Computers

Henry, a traveling salesperson at your company, left his laptop at the airport on his last trip. The laptop was never recovered. His new laptop arrived yesterday and you installed Windows 10 Enterprise and productivity applications and restored data from a backup. What should you do to the laptop to protect all programs and data on the computer in the event of loss or theft?

Scenario 1-4: Standardizing a User's Work Environment

You administer a network in which many of the computers are shared among users and people often use different computers based on where they work. Therefore, you need to configure the following:

- Users must be able to access all documents that they store in their Documents and Desktop folders.
- Users should also have an application installed so that they can clock in and out.

How can you accomplish this?