Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**6**

**Windows 10 Security Features**

* [Chapter Introduction](javascript://)
* **6-1**[Windows 10 Security Policies](javascript://)
  + **6-1a**[Account Policies](javascript://)
  + **6-1b**[Local Policies](javascript://)
  + **6-1c**[AppLocker](javascript://)
  + **6-1d**[Software Restriction Policies](javascript://)
  + **6-1e**[Other Security Policies](javascript://)
* **6-2**[Auditing](javascript://)
* **6-3**[User Account Control](javascript://)
  + **6-3a**[Application Manifest](javascript://)
  + **6-3b**[UAC Configuration](javascript://)
* **6-4**[Malware Protection](javascript://)
  + **6-4a**[Virus and Threat Protection](javascript://)
  + **6-4b**[App & Browser Control](javascript://)
  + **6-4c**[Device Security](javascript://)
* **6-5**[Data Security](javascript://)
  + **6-5a**[Encryption Algorithms](javascript://)
  + **6-5b**[Encrypting File System](javascript://)
  + **6-5c**[BitLocker Drive Encryption](javascript://)
* **6-6**[Windows Update](javascript://)
  + **6-6a**[Servicing Branches](javascript://)
  + **6-6b**[Controlling Windows Updates](javascript://)
  + **6-6c**[Removing Windows Updates](javascript://)
  + **6-6d**[Updating Microsoft Store Apps](javascript://)
* **6-7**[Chapter Review](javascript://)
  + **6-7a**[Summary](javascript://)
  + **6-7b**[Key Terms](javascript://)
  + **6-7c**[Review Questions](javascript://)
  + **6-7d**[Case Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

Chapter Introduction

After reading this module and completing the exercises, you will be able to:

* **1**Use the Local Security Policy to secure Windows 10
* **2**Enable auditing to record security events
* **3**Configure User Account Control
* **4**Describe the malware security features in Windows 10
* **5**Implement the data security features in Windows 10
* **6**Secure Windows 10 by using Windows Update

Security is a crucial consideration for how you configure Windows 10. Computers that are not secure are susceptible to malware that can destroy data and steal passwords. Windows 10 includes many security features, most of which are enabled by default; you also have options to optimize them for your environment.

In this module, you learn how to configure security by using the Local Security Policy, including AppLocker, and how to enable auditing. You also learn about User Account Control, which requires approval to perform administrative actions. Windows Defender Antivirus, for malware protection, is covered, along with using Encrypting File System and BitLocker Drive Encryption for data encryption. Finally, using Windows Update and the new Windows 10 update processes are discussed.

Go to pg.

[**help**](javascript://)

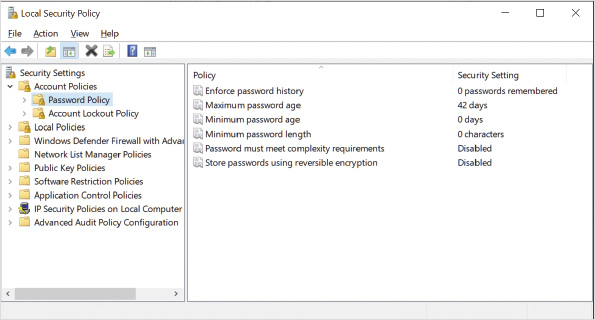
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**6-1**Windows 10 Security Policies

Windows 10 includes a [**Local Security Policy**](javascript://), shown in [Figure 6-1](javascript://), which can be used to control many facets of Windows. You can access the Local Security Policy in Administrative Tools.

**Figure 6-1Local Security Policy**



Enlarge Image

The Local Security Policy contains the following categories of settings:

* Account Policies
* Local Policies
* Windows Defender Firewall with Advanced Security
* Network List Manager Policies
* Public Key Policies
* Software Restriction Policies
* Application Control Policies
* IP Security Policies on Local Computer
* Advanced Audit Policy Configuration

The Local Security Policy is part of a larger Windows management system called Group Policy, which can be implemented on a local computer but is more commonly part of a domain-based network. A variety of tools and security templates can be used to configure and analyze security policies.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-1aAccount Policies

The Account Policies category contains the Password Policy and the Account Lockout Policy. The Account Policies in the Local Security Policy affect only local user accounts. The account policies do not affect domain accounts. To control domain accounts, the account policies must be configured at the domain level.

### Password Policy

The [**Password Policy**](javascript://) controls password characteristics for local user accounts. The available settings are:

* Enforce password history—This setting specifies the number of password changes that must occur before a password can be reused. For example, if the setting is 3, a password can be reused only every fourth time. The default value is 0 passwords remembered, and the maximum is 24 passwords remembered.
* Maximum password age—This setting is the maximum amount of time that a user can keep the same password without changing it. Forcing password changes reduces the risk of a shared or hacked password being used over an extended period of time. The default value is 42 days.
* Minimum password age—This setting is the shortest amount of time that a user can use a password before changing it. A minimum password age is often used to ensure that users do not change their password several times in quick succession to continue using a single password. The default value is 0 days, which allows passwords to be changed again immediately.
* Minimum password length—This setting is the minimum number of characters that must be in a password. In general, longer passwords are more secure. A minimum password length of 8 or 10 characters is typical for most organizations. The default value is 0 characters, which allows any password length.
* Password must meet complexity requirements—This setting applies a number of tests to a new password to ensure that it is not too easy to guess or hack. This setting is enforced when a password change is made but is not applied to existing passwords. The default value is Disabled. The complexity requirements include the following:
  + Cannot contain part of the user’s account name
  + Must be at least six characters long
  + Must contain characters meeting three of the following characteristics: uppercase characters, lowercase characters, numerals (0–9), nonalphanumeric characters (e.g., !, @, #, $)
* Store passwords using reversible encryption—This setting controls how passwords are encrypted in the Security Accounts Manager (SAM) database that stores user credentials. By default, this setting is disabled, and passwords are encrypted in a nonreversible format. Storing passwords by using reversible encryption is required for compatibility only with specific applications that require it. Enabling this option stores passwords in a less secure way and should not be enabled unless absolutely required to support a specific application.

### Account Lockout Policy

The [**Account Lockout Policy**](javascript://) is used to prevent unauthorized access to Windows 10. Using the Account Lockout Policy, you can configure an account to be temporarily disabled after a number of incorrect sign-in attempts. This prevents automated password-guessing attacks from being successful.

The settings available to control account lockouts are:

* Account lockout duration—This setting determines how many minutes an account remains locked. The default value is 30 minutes; however, this value is not configured until the Account lockout threshold has been configured.
* Account lockout threshold—This setting determines the number of incorrect sign-in attempts that must be performed before an account is locked. The default value is 0 invalid sign-in attempts, which means that account lockouts are disabled.
* Reset account lockout counter after—This setting determines within what time frame the incorrect sign-in attempts must occur to trigger a lockout. The default value is 30 minutes; however, this value is not configured until the Account lockout threshold has been configured.

**Activity 6-1**

### Implementing a Password Policy

**Time Required:**10 minutes

**Objective:**Implement a password policy that applies to local users

**Description:**A password policy is used to control the passwords that can be selected by users. One of the most effective password policy settings for increasing security is requiring complex passwords that are difficult to hack. In this activity, you configure a password policy to require complex passwords.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **local**, and then click **Local Security Policy**.

1. 3

In the Local Security Policy window, in the left pane, expand **Account Policies** and then click **Password Policy**. This shows all the password policy settings that are available to you.

1. 4

Double-click **Password must meet complexity requirements**, click **Enabled**, and then click **OK**. Now all passwords must meet complexity requirements when they are changed.

1. 5

Close all open windows.

1. 6

Press **Ctrl+Alt+Delete** and then click **Change a password**. Note that you can’t use this method to change your password if you are signed in by using a Microsoft account.

1. 7

In the Old password box, type **password**.

1. 8

In the New password and Confirm password text boxes, type **simple** and then press **Enter**. You will receive an error indicating that the new password is not acceptable due to length, complexity, or history requirements.

1. 9

Click **OK**.

1. 10

In the Old password text box, type **password**.

1. 11

In the New password and Confirm password text boxes, type **S1mpl3** and then press **Enter**. This time, the password will be changed successfully.

1. 12

Click **OK**.

**Caution**

Passwords with simple letter number substitution like S1mpl3 are still not very secure because hacking tools include that functionality. When you add numbers and symbols to make a password more complex, do your best to make it an unpredictable pattern.

Go to pg.

[**help**](javascript://)

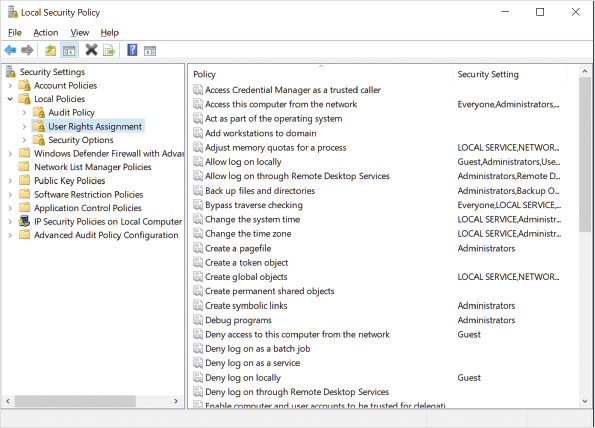
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-1bLocal Policies

Local Policies are for auditing system access, assigning user rights, and configuring specific security options. Auditing lets you track when users sign in and which resources are used. Details about auditing are covered later in this module. User rights control which system tasks a particular user or group of users can perform. The specific security options are a variety of settings that can be used to make Windows 10 more secure. [Figure 6-2](javascript://) shows some of the settings available in User Rights Assignment.

**Figure 6-2User Rights Assignment Settings**



Enlarge Image

Some of the settings available in User Rights Assignment are:

* Allow log on locally—This setting controls which users are allowed to sign in to the computer at the console but does not affect who can access the computer over the network. Administrators, Backup Operators, Guest, and Users are assigned this right by default.
* Back up files and directories—This setting controls which users are allowed to back up files, regardless of whether they have the necessary file permissions to read those files. Administrators and Backup Operators are assigned this right by default.
* Change the system time—This setting controls which users are allowed to change the system time. Administrators and Local Service are assigned this right by default.
* Load and unload device drivers—This setting controls which users are able to install and remove device drivers. Only Administrators are assigned this right by default.
* Shut down the system—This setting controls which users are able to shut down Windows 10. For a public access computer, you might restrict this right. Administrators, Backup Operators, and Users are assigned this right by default.

Some of the settings available in Security Options are:

* Devices: Prevent users from installing printer drivers—This setting controls whether standard users are allowed to install printer drivers from a shared printer. It does not affect the installation of local printer drivers. The default value is disabled, which allows all users to install network printer drivers.
* Interactive logon: Don’t display last signed-in—This setting allows you to remove the last user name from the sign-in screen. This makes sign-in more secure by not revealing user names to potential hackers. The default value is Disabled.
* Interactive logon: Message text for users attempting to log on—This setting allows you to display a message for users before they sign in. The message can be instructions about how to sign in or a warning against unauthorized use. By default, no message is displayed.
* Shutdown: Allow system to be shut down without having to log on—This setting allows you to require sign-in before allowing the system to be shut down. This is important for public access computers when you want to restrict which users can shut down the system. The default value is Enabled.

**Activity 6-2**

### Configuring a Sign-In Message

**Time Required:**10 minutes

**Objective:**Configure a warning message that appears for users before signing in

**Description:**The security policy of some organizations dictates that users are presented with a warning message about appropriate use before signing in. This warning is used to ensure that users are properly informed about organizational policies. In this activity, you configure Windows 10 with a warning message that appears before users sign in.

1. 1

If necessary, start your computer and sign in. Recall that the password has been changed to S1mpl3.

1. 2

Click the **Start** button, type **Local**, and then click **Local Security Policy**.

1. 3

In the Local Security Policy window, in the left pane, expand **Local Policies**, and then click **Security Options**.

1. 4

Scroll down and then double-click **Interactive logon: Message title for users attempting to log on**.

1. 5

In the text box, type **Acceptable Use** and then click **OK**.

1. 6

Double-click **Interactive logon: Message text for users attempting to log on**.

1. 7

In the text box, type **This computer should be used only for approved company business**. **Please see the acceptable use policy for more details.** and then click **OK**.

1. 8

Close Local Security Policy.

1. 9

Sign out and then press **Ctrl+Alt+Delete**. Notice that the warning message appears.

1. 10

Click **OK** to display the sign-in screen.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-1cAppLocker

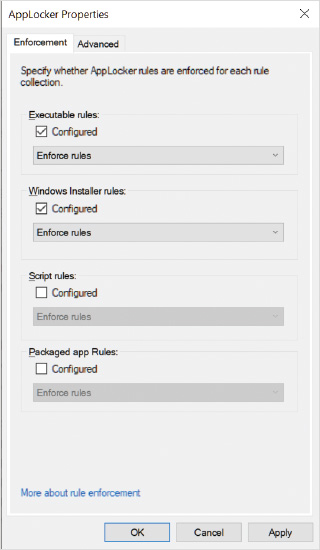
[**AppLocker**](javascript://) is used to define which programs are allowed or disallowed in the system. Its most common use is for malware prevention. Much malware installs itself by running from within a user profile. You can use AppLocker to restrict the locations that allow executables to run, thereby potentially avoiding the problem.

**Tip**

A particularly nasty type of malware is known as ransomware. Ransomware encrypts files and requires payment for a key to decrypt the files. AppLocker is an effective tool to prevent ransomware.

You can audit or enforce AppLocker rules. When you audit an AppLocker rule, an event is logged when an action matching the rule is performed, but the software is allowed to run. When you enforce an AppLocker rule, software is blocked from running. If you do not define whether rules are enforced or audited, the default is enforced. When you first implement AppLocker rules, it is a good idea to use audit rather than enforce the rules. This allows you to review the logs and verify that your rules allow all the necessary software to run. [Figure 6-3](javascript://) shows the configuration of AppLocker auditing and enforcement.

**Figure 6-3Configuring AppLocker Enforcement**



Enlarge Image

The enforcement or auditing of AppLocker rules relies on the configuration of appropriate rules and the Application Identity service. The Application Identity service must be running for AppLocker rules to be evaluated. This service is configured for Manual startup and is stopped by default. If you are implementing AppLocker rules, you should configure the Application Identity service for Automatic startup.

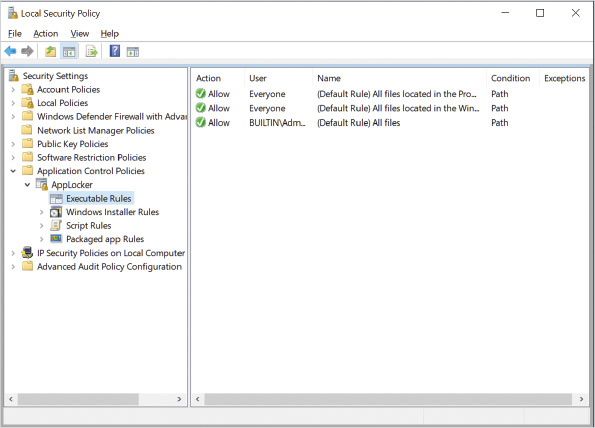
**Tip**

In a domain-based environment, you can use Group Policy to easily configure the Startup Type for the Application Identity service on multiple computers.

### Rule Collections

AppLocker rules are divided into categories called rule collections, as shown in [Figure 6-4](javascript://). Each rule collection applies to different types of files.

**Figure 6-4AppLocker Rule Collections**



Enlarge Image

The rule collections are:

* Executable—These rules apply to .exe and .com files. Use these rules to control which applications users can run.
* Windows Installer—These rules apply to .msi and .msp files. Use these rules to control which users can install applications and from what locations.
* Script—These rules, which apply to .ps1, .bat, .cmd, .vbs, and .js files, are used to control which users can run scripts.
* Packaged app—These rules apply to .appx files. Use these rules to control which users can run Windows Store apps.
* DLL—These rules apply to .dll and .ocx files. Use these rules to verify that the dynamic link library (DLL) and ActiveX (OCX) files used by applications are not modified or unknown. These rules are not enabled by default due to negative performance impact.

Many Windows applications use DLL files when they are executing programs. DLL files contain code that is shared across many applications, and many DLLs are included as part of the operating system. DLL files are considered a lower risk than executable files and are not evaluated by default. Evaluating DLL files creates a significant performance impact because DLLs are accessed many times during program execution, and the DLL must be evaluated each time it is accessed. If performance is not a concern, however, you can choose to evaluate DLL files in addition to executable files to enhance security.

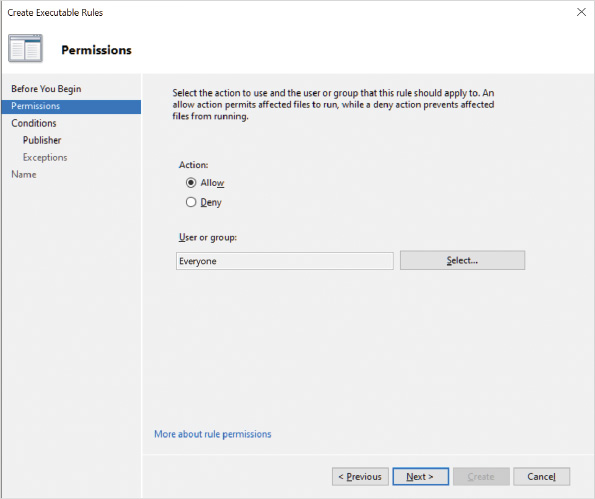
For each rule collection, you can:

* Create a New Rule—This allows you to manually specify the characteristics of a rule. To create rules in this way, you must understand the exact end results that you are trying to achieve.
* Automatically Generate Rules—This option scans your computer and creates rules that match its current configuration. In a larger corporate environment, you can create the rules on a standardized reference computer and then apply them to all computers in the organization. You should review the rules before applying them.
* Create Default Rules—This creates standardized rules for a rule collection that meets the needs of many users and organizations. Because these rules are very general, they provide less security than automatically generated rules but are usually easier to manage. The default rules created vary for each rule collection.

### Rule Permissions

Each rule contains permissions that define whether the rule allows or denies software the capability to run, as shown in [Figure 6-5](javascript://). It is important to remember that until a rule is created in a rule collection, the default permission is Allow. For example, if no executable rules are specified, all executables are allowed. As soon as a single executable rule is created, the default permission is Deny, and only specifically allowed executables can run. For example, if you create a rule that prevents users from running cmd.exe, access to all other applications without an Allow rule is prevented.

**Figure 6-5AppLocker Rule Permissions**



Enlarge Image

Permissions also define to which users the rule applies. A rule can be applied to an individual user or group but not multiple users or groups. This means it is crucially important to plan which groups to use for allowing access.

In general, the best strategy for applying rules is to begin by creating rules that allow access for larger groups of users. Then, you can restrict smaller groups or individuals with a rule that denies access, or you create an exception within the original rule. The Deny permission overrides the Allow permission when multiple rules apply for a user.

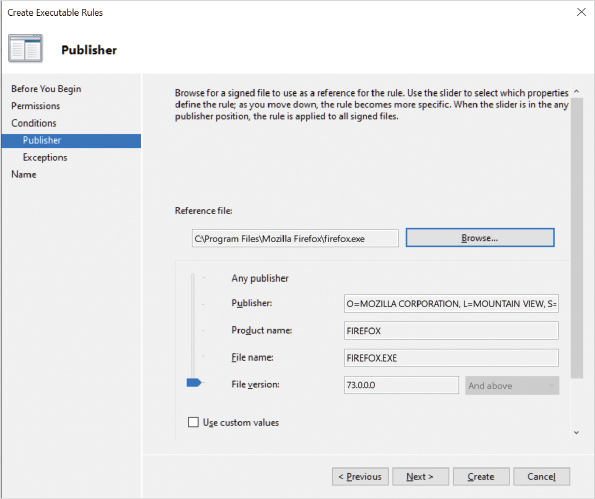
### Rule Conditions

A rule condition defines the software that is affected by the rule. The three conditions that can be used are as follows:

* Publisher
* Path
* File Hash

The Publisher rule condition, shown in [Figure 6-6](javascript://), identifies software by using a digital signature in the software. If the software is not digitally signed, you cannot use a Publisher rule condition to identify it. In that case, consider using a File Hash rule condition instead.

**Figure 6-6Publisher Rule Condition**



Enlarge Image

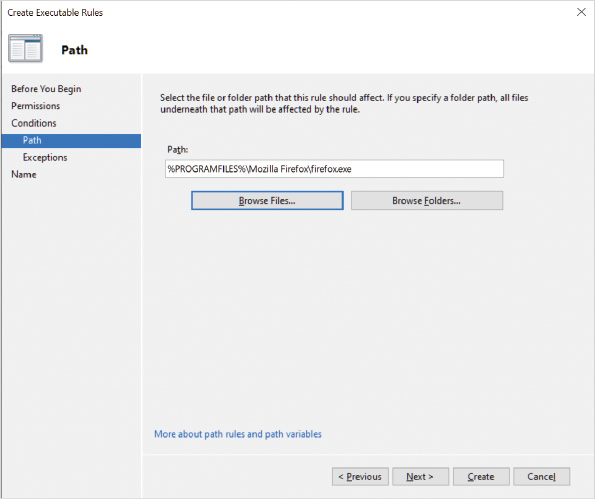
To begin configuration of a Publisher rule condition, you specify a reference file. The wizard reads the digital signature from this reference file as the basis for the condition. After a reference file has been defined, you can use the slider to select the specific information that must be matched. You can make it as specific as a particular file and file version or make it more generic and restrict it only to a specific product name or publisher. You can also define custom values that do not match the information read from the reference file.

**Tip**

If you include the file version in a publisher rule, you might need to update the rule each time you update the application. For easier maintenance, create rules that trust common publishers like Microsoft, and don’t specify further details.

The Path rule condition, shown in [Figure 6-7](javascript://), identifies software by file location. You can specify a single file or a folder path from which software can be run. This type of rule condition tends to be much less secure than a Publisher rule condition. For example, if you use a Path rule condition that allows software to be run from C:\Program Files\, any malware accidentally installed by a user and located in C:\Program Files\ can be run. At a minimum, you should avoid using Path rule conditions that allow executables to be run from file locations where standard users can copy files. Variables can be used as part of the path to simplify rule creation.

**Figure 6-7Path Rule Condition**



Enlarge Image

The File Hash rule condition generates a unique identifier for the specified files called a hash value. If the file is modified in any way, the hash value of the file no longer matches the hash value in the rule, and the software is blocked from running. If you use a File Hash rule condition, application updates will require the rule to be updated.

### Rule Exceptions

An AppLocker rule exception defines software to which the rule does not apply. In general, you use rule conditions to define a large set of software and then use exceptions to define a smaller set of software to which the rule does not apply. Similar to rule conditions, when you add an exception, it can be based on publisher, path, or file hash. You can add multiple exceptions to a single rule.

**Activity 6-3**

### Configuring AppLocker

**Time Required:**10 minutes

**Objective:**Implement AppLocker rules

**Description:**AppLocker rules can be used to limit which software is allowed to run on a workstation. An administrator can use this to prevent a particular piece of software from running or allow only specific software to run. In this activity, you create and review default AppLocker rules and audit the use of cmd.exe.

1. 1

If necessary, start your computer and sign in. Remember that the password is changed to S1mpl3.

1. 2

Click the **Start** button, type **local**, and then click **Local Security Policy**.

1. 3

In the left pane, expand **Application Control Policies** and then click **AppLocker**.

1. 4

Scroll down and notice that no rules are created by default, but they are enforced.

1. 5

Click **Executable Rules**.

1. 6

Right-click an open area in the right pane and then click **Create Default Rules**.

1. 7

Review the default rules. These rules allow administrators to run all applications and allow Everyone to run applications in C:\Program Files\ and C:\Windows\.

1. 8

Right-click an open area in the right pane and then click **Automatically Generate Rules**.

1. 9

On the Folder and Permissions screen, click **Next** to accept the default of scanning C:\Program Files\.

1. 10

On the Rule Preferences screen, read the default options that are selected and then click **Next**. Notice that the rules are being created based on digital signatures and file hashes rather than the file path.

1. 11

On the Review Rules page, click **View Rules that will be automatically created**.

1. 12

Read the rules and then click **OK**. These rules are based on the software installed on your computer.

1. 13

On the Review Rules page, click **Cancel**.

1. 14

In the left pane, right-click **Executable Rules** and then click **Create New Rule**.

1. 15

On the Before You Begin screen, click **Next**.

1. 16

On the Permissions screen, click **Deny** and then click **Next**.

1. 17

On the Conditions screen, click **Path** and then click **Next**.

1. 18

On the Path screen, in the Path box, type **C:\Windows\System32\cmd.exe** and then click **Next**.

1. 19

On the Exceptions screen, click **Next** to accept the default of no exceptions.

1. 20

In the Name box, delete the existing name, type **Deny Command Prompt**, and then click **Create**.

1. 21

In the left pane, click **Windows Installer Rules**, right-click **Windows Installer Rules**, and then click **Create Default Rules**.

1. 22

Review the default rules that are created. These rules allow Everyone to install digitally signed software and allow administrators to install any software.

1. 23

In the left pane, click **AppLocker** and then click **Configure rule enforcement**.

1. 24

Under Executable rules, select the **Configured** check box, select **Audit only** in the list, and then click **OK**.

1. 25

Close the Local Security Policy window.

1. 26

Right-click the **Start** button and then click **Computer Management**.

1. 27

Expand **Services and Applications** and then click **Services**.

1. 28

Click the **Application Identity** service, read the description, and then click the **Start** button.

1. 29

Wait a few seconds for the service to be completely initialized then click the **Start** button. Type **cmd** and then click **Command Prompt**.

1. 30

In the left pane of Computer Management, expand **Event Viewer**, expand **Applications and Services Logs**, expand **Microsoft**, expand **Windows**, expand **AppLocker**, and then click **EXE and DLL**.

1. 31

Click the **Warning** event and read the description. Notice that cmd.exe was allowed to run because it is only being audited rather than enforced. If you don’t see any events, it’s possible that the Application Identity service was not completely initialized. Close the command prompt and then repeat [Step 29](javascript://).

1. 32

In the left pane of Computer Management, scroll down and then click **Services**.

1. 33

Click the **Application Identity** service and then click **Stop**.

1. 34

Close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-1dSoftware Restriction Policies

[**Software Restriction Policies**](javascript://) are an older technology that you can use to control application usage in a fashion similar to AppLocker. Software Restriction Policies are still functional in Windows 10. If both AppLocker rules and Software Restriction Policies are defined on a Windows 10 computer, only the AppLocker rules are enforced.

AppLocker is preferred over Software Restriction Policies because it provides the following enhancements:

* Rules can be applied to specific users and groups rather than all users.
* The default rule action is Deny to increase security.
* A wizard is available to help create rules.
* You can use audit-only mode for testing that writes only events to the event log.

To use AppLocker, you must implement Windows 10 Enterprise or Windows 10 Education; however, many smaller organizations use Windows 10 Pro instead, because they receive it with new computers. For these smaller organizations that cannot use AppLocker, Software Restriction Policies offer an effective way to restrict malware from running.

**Tip**

Software Restriction Policies have been deprecated starting with Windows 10 version 1803 (March 2018). Questions about this functionality are not likely to appear on the exam.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-1eOther Security Policies

Windows Defender Firewall with Advanced Security is used to configure the firewall in Windows 10. This policy lets you configure both inbound and outbound rules for packets. In addition, you can configure specific computer-to-computer rules. In Windows 10, this area can also be used to configure IP Security (IPsec) rules.

The Network List Manager Policies are used to control how Windows 10 categorizes networks to which it is connected and how users can interact with the process. For example, unidentified networks can be automatically defined as either public or private, and the user can restrict the ability of other users to change it. These policies also control whether users can rename networks to which they connect.

Public Key Policies have settings for the [**Encrypting File System (EFS)**](javascript://), BitLocker Drive Encryption, and certificate services. You can add recovery agents for EFS files or BitLocker-encrypted drives. A recovery agent is allowed to decrypt files protected by EFS or BitLocker. More detailed information about EFS and BitLocker Drive Encryption is provided later in this module.

IP Security Policies on Local Computer are used to control encrypted network communication. By default, network communication is not encrypted. You can, however, configure encrypted network communication for certain hosts or communication on certain port numbers. This policy is deprecated in Windows 10 and is included only for backward compatibility with previous versions of Windows. When configuring IPsec rules, you should use Windows Defender Firewall with Advanced Security.

Advanced Audit Policy Configuration is a simplified way to configure advanced audit policies in Windows 10. These policies first appeared in Windows Vista but needed to be edited at a command-line level.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 6-2Auditing

[**Auditing**](javascript://) is the security process that records the occurrence of specific operating system events in the Security log. Every object in Windows 10 has audit events related to it. Log entries can be recorded for successful events or failed attempted events. For example, logging all failed sign-in attempts may warn you when an attack that might breach your security is occurring. In addition, monitoring sensitive documents for read access lets you know who is accessing the documents and when.

It is more common to use auditing to monitor access to server-based resources than resources on desktop computers. In some cases, however, you might want to know which users are signing in to a specific workstation. For example, if security logs indicate that someone was attempting unauthorized access to resources from a particular workstation, it is useful to see which user was signed in at the time.

Windows 10 has basic audit policy settings and advanced audit policy settings. Both sets of audit policy settings allow you to capture similar information, but the advanced audit policy settings have more detailed configuration options than the basic audit policy settings. Using the advanced audit policy settings allows you to limit the amount of audit data that you capture. In this way, you capture only relevant data and simplify the task of reviewing the audit logs. [Table 6-1](javascript://) describes the categories for Advanced Audit Policy settings.

**Table 6-1**

### Event Categories for Advanced Audit Policy Settings

| **Event Category** | **Description** |
| --- | --- |
| Account Logon | Tracks when users are authenticated by a computer. If a local user account is used, the event is logged locally. If a domain user account is used, the event is logged at the domain controller. Account Logon events are not audited by default. |
| Account Management | Tracks when users and groups are created, modified, or deleted. Password changes are also tracked. Success events for user management and group management are audited by default. |
| Detailed Tracking | Tracks how a computer is being used by tracking application activity. This includes identifying the creation and termination of processes, encryption events, and remote procedure call (RPC) events. No events are audited by default. |
| DS Access | This category is not relevant for Windows 10 and is not audited by default. It is used only for domain controllers. |
| Logon/Logoff | Tracks user activity events, including local and domain log-ons (sign-in) attempts, at the local computer. This category is similar to, but different from, auditing account log-on events. Signing in with a local account generates both an account log-on event and a log-on event on the local computer. Signing in with a domain account generates an account log-on event at the domain controller and a log-on event at the workstation where the sign in occurred. Success events for log off and account lockout are audited by default. Success and failure events for logon and network policy server are audited by default. |
| Object Access | Tracks access to files, folders, printers, and registry keys. Each individual object being accessed also must be configured for auditing. Files and folders can be monitored only if they are on NTFS-formatted volumes. Object access is not audited by default. |
| Policy Change | Tracks changes to user rights assignments, audit policies, and trust policies. Success events for audit policy changes and authentication policy changes are audited by default. |
| Privilege Use | Tracks when tasks are performed that require a user-rights assignment, such as changing the system time. You can define which categories of privilege use are audited; none is audited by default. |
| System | Tracks when system events occur, such as restarting the system. By default, success and failure events are audited for system integrity and other system events. Only success events are audited for security state change. |
| Global Object Access Auditing | Provides an easy way to specify that all access to files or registry keys should be audited. This avoids the need to configure auditing at the file, folder, or registry-key level after enabling auditing for object access to files or registry keys; however, this must still be used in combination with auditing enabled for object access. This category does not appear when using auditpol.exe. |

Enlarge Table

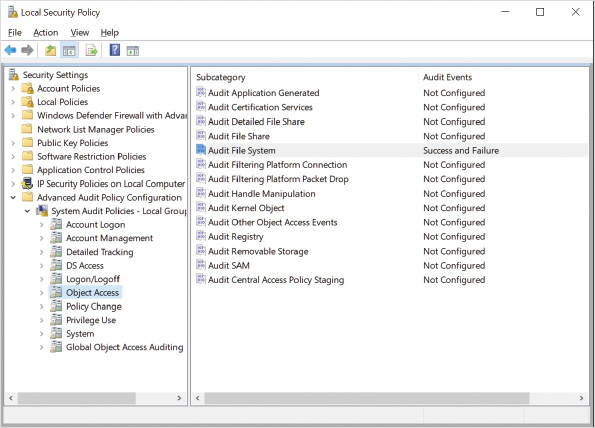
**Caution**

You should not combine basic audit policy settings and advanced audit policy settings because the results are unpredictable. To prevent conflicts, you can enable the Security Options policy setting Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.

Basic auditing is enabled through the Local Security Policy or by using Group Policy. The [**audit policy**](javascript://) for basic auditing is located in the Local Policies node of the Local Security Policy.

Advanced auditing is enabled through the Local Security Policy, by using Group Policy, or by using auditpol.exe. The tool auditpol.exe provides the most accurate view of which Advanced Audit Policy settings are applied. [Figure 6-8](javascript://) shows the Advanced Audit Policy settings in the Local Security Policy.

**Figure 6-8Advanced Audit Policy**

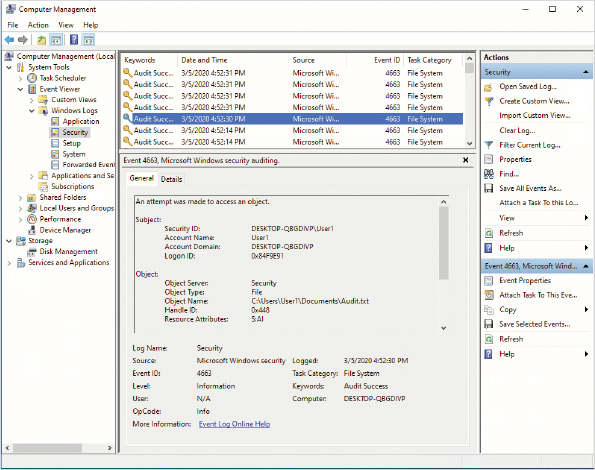


Enlarge Image

The default configuration for the Advanced Audit Policy settings can be viewed only by using the auditpol.exe utility. If you review the configuration in the Local Security Policy, it appears that no settings are enabled. Be aware that after you enable settings in the Local Security Policy, the default configuration is lost and does not return if the Advanced Audit Policy settings are removed from the Local Security Policy. Refer to [Table 6-1](javascript://) for the default configuration for the Advanced Audit Policy settings.

After the audit policy is configured, the audited events are recorded in the Security log that is viewed by using Event Viewer. Event Viewer is available as part of the Computer Management MMC console or as a stand-alone MMC console in Administrative Tools. Security events are listed by selecting the Windows Security log, as shown in [Figure 6-9](javascript://).

**Figure 6-9Windows Security Log**



Enlarge Image

**Activity 6-4**

### Auditing File Access

**Time Required:**15 minutes

**Objective:**Audit file modification for users

**Description:**In a corporate environment, it is useful to track all the users who have modified sensitive files. You can use auditing to track file modification. In this activity, you enable auditing of file modification creation, configure a file to be audited, and view user modification of that file.

1. 1

If necessary, start your computer and sign in. Remember that the password is changed to S1mpl3.

1. 2

Right-click the **Start** button and then click **Windows PowerShell (Admin)**.

1. 3

In the User Account Control dialog box, click **Yes**.

1. 4

At the Windows PowerShell prompt, type **auditpol /get /category:\*** and then press **Enter**. This displays a list of all the advanced audit policy settings and their configurations.

1. 5

Read the list of policy settings that are enabled. This is the default configuration for Windows 10. Notice that below Object Access, File System auditing is not enabled. After you enable policy settings in the local security policy, these settings are removed, and only the settings explicitly applied in the policy are effective.

1. 6

Close the Windows PowerShell prompt window.

1. 7

Click the **Start** button, type **local**, and then click **Local Security Policy**.

1. 8

In the left pane, expand **Local Policies** and then click **Audit Policy**. Review the list of categories for basic auditing and notice that none is enabled in the local security policy.

1. 9

In the left pane, expand **Advanced Audit Policy Configuration**, expand **System Audit Policies - Local Group Policy Object**, and then click **Object Access**.

1. 10

Double-click **Audit File System**. This option enables auditing for file access.

1. 11

In the Audit File System Properties dialog box, select the **Configure the following audit events** check box and then select the **Success** and **Failure** check boxes.

1. 12

Click the **Explain** tab, read the explanation, and then click **OK**. The system is now able to track successful file access when users have permission to access a file and unsuccessful file access when users do not have permission to access a file; however, auditing must still be enabled for the individual files.

1. 13

Close Local Security Policy, and close all open windows.

1. 14

On the taskbar, click **File Explorer** and then click **Documents**.

1. 15

Right-click an open area in the **Name** column, point to **New**, and then click **Text Document**.

1. 16

Type **Audit** and then press **Enter**.

1. 17

Right-click **Audit**, click **Properties**, and then click the **Security** tab.

1. 18

In the Audit Properties dialog box, click **Advanced** and then click the **Auditing** tab. Notice that auditing information is protected by UAC.

1. 19

Click **Continue** to open the auditing information. Notice that no auditing is configured by default.

1. 20

Click **Add**, click **Select a principal**, type **Everyone**, click **Check Names**, and then click **OK**. This configures auditing to track access by all users. You can limit auditing to certain users or groups.

1. 21

In the Type box, select **All**. This configures auditing of successful and failed access.

1. 22

Below Basic permissions, select the **Full control** check box. This configures auditing to track all changes to the file.

1. 23

Click **OK** three times to close all open dialog boxes.

1. 24

Double-click **Audit** to open the file and then add some content to the file.

1. 25

Click **File** on the menu bar, click **Exit**, and then click **Save**.

1. 26

Close the File Explorer window.

1. 27

Right-click the **Start** button and then click **Computer Management**.

1. 28

In the left pane, expand **Event Viewer**, expand **Windows Logs**, and then click **Security**. This displays all the events in the security log.

1. 29

Right-click **Security** and then click **Filter Current Log**.

1. 30

In the Event sources box, select **Microsoft Windows security auditing**.

1. 31

In the <All Event IDs> box, type **4663** and then click **OK**. Notice that multiple events are listed. These events were generated by editing the file.

1. 32

Starting with the first event, read the Account Name identified in the event. Continue down until the Account Name referenced is Userx. Read the description of the event. The description indicates that a file was written by Userx, where x is the number assigned to you; the file opened was Audit.txt; and the program used to write the file was notepad.exe.

1. 33

Close the Computer Management window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**6-3**User Account Control

[**User Account Control (UAC)**](javascript://) is a feature that makes running applications more secure. Security is enhanced by reducing the need to sign in and run applications using administrator privileges. Reducing the use of administrative privileges makes it less likely that malicious software can adversely affect Windows 10.

In some organizations, all user accounts are configured as administrators on the local workstations. This is done to ensure that users are able to perform any local maintenance tasks that may be required, such as installing printers or software. In Windows 10, major efforts have been put forth to ensure that most common tasks do not require administrative privileges; however, even if users are still given administrative privileges, UAC increases security.

When UAC is enabled and an administrative user signs in, the administrative user is assigned two access tokens. One access token includes standard user privileges and the other access token includes administrative privileges. The standard user access token is used to launch the Windows 10 user interface; therefore, all applications started by using the user interface also start with standard user privileges. This approach keeps any malicious software from having access to restricted areas, like system files.

Admin Approval Mode ensures that the access token with administrative privileges is used only when required. When you use an application that requires administrative privileges, you are prompted to continue or cancel running the program with administrative privileges. If you select to continue, the program is run using the access token with administrative privileges. The Application Information Service is responsible for launching programs by using the access token with administrative privileges.

When UAC is enabled and a standard user signs in, the user is assigned only one access token with standard user privileges. If the user attempts to run an application that requires administrative privileges, the user is prompted to supply credentials for a user with administrative privileges.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-3aApplication Manifest

Newer Windows applications use an application manifest to describe the structure of an application. The application manifest file identifies required DLL files and whether they are shared. The file can also include information about UAC. To trigger the privilege elevation prompt for an application that requires administrative privileges, an entry must be included in the application manifest.

Applications that are not designed for Windows 10 and that require administrative privileges do not properly request elevated privileges, which generates an error. You can eliminate this error by using the Application Compatibility Toolkit.

Go to pg.

[**help**](javascript://)

Application Opened

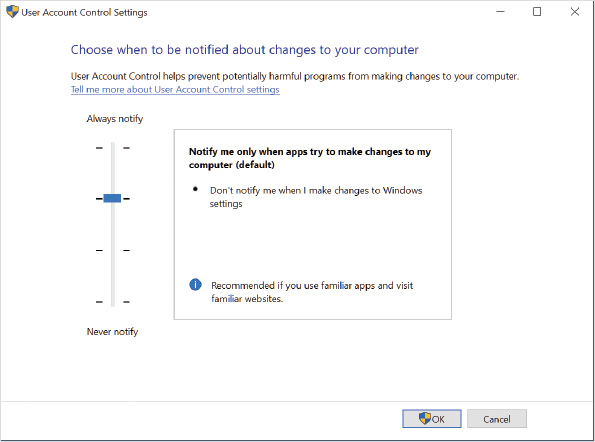
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-3bUAC Configuration

Windows 10 limits the number of UAC prompts presented to administrative users with a default configuration that does not prompt if the user initiated the action. If a program initiates the action, a UAC prompt is still presented; however, you can modify the default configuration as shown in [Figure 6-10](javascript://). Four options are available, as listed below:

* Always notify me—This setting is equivalent to the configuration in Windows Vista in which even administrative users are prompted every time an administrative task is attempted.
* Notify me only when apps try to make changes to my computer—Administrative users are prompted only when a program attempts to perform an administrative task. When the administrative task is initiated by the user, a prompt is not displayed. This is the default setting.
* Notify me only when apps try to make changes to my computer (do not dim my desktop)—This setting is the same as the default setting except that when the UAC prompt is displayed, the screen is not dimmed.
* Never notify me—This setting disables UAC and is not recommended because UAC is an important security feature.

**Figure 6-10UAC Settings**



Enlarge Image

For advanced configuration, UAC is configured by using either the Local Security Policy or Group Policy. The policy settings for configuring UAC are listed in [Table 6-2](javascript://). The default settings for UAC work well for most scenarios. Carefully consider the ramifications before you modify the advanced configuration settings for UAC.

**Table 6-2**

### UAC Configuration Options

| **Option (User Account Control)** | **Description** |
| --- | --- |
| Admin Approval Mode for the built-in Administrator account | Used to enable or disable Admin Approval Mode for the built-in administrator account. The default configuration is disabled. |
| Allow UIAccess application to prompt for elevation without using secure desktop | Used to allow UIAccess programs, such as Remote Assistance, to automatically disable the screen dimming that normally occurs when a UAC prompt is displayed. This is a less secure configuration but can speed up screen drawing over slow connections. This is disabled by default. |
| Behavior of the elevation prompt for administrators in Admin Approval Mode | Used to configure the elevation prompt for Administrators only. The default configuration is to prompt for consent for non-Windows binaries; however, you can also configure a prompt for administrative credentials instead of a simple approval or you can disable the prompt. Entirely disabling the prompt effectively disables UAC for administrators because applications can then request elevation to administrative privileges and are automatically approved. Applications still run with standard user privileges until they request elevation. |
| Behavior of the elevation prompt for standard users | Used to configure the elevation prompt for standard users only. The default configuration is to prompt for credentials. You can also select Automatically deny elevation requests, in which case the user must manually use the Run as administrator option to elevate the privileges of the application. |
| Detect application installations and prompt for elevation | Used to automatically detect whether an application is being installed and generate a prompt to elevate privileges. The default configuration is enabled. If this option is disabled, many legacy application installations will fail. |
| Only elevate executables that are signed and validated | Used to limit privilege elevation to only applications that are digitally signed. The default configuration is disabled, which allows older unsigned applications that require administrative privileges to be elevated. |
| Only elevate UIAccess applications that are installed in secure locations | Used to force applications using the UIAccess integrity level in their application manifest to be located from a secure location. Secure locations are C:\ProgramFiles\ and C:\Windows\System32\ and their subfolders. The default configuration is enabled. |
| Run all administrators in Admin Approval Mode | Used to limit all user processes to standard user privileges unless they are elevated to administrator privileges. The default configuration is enabled. When this option is disabled, UAC is disabled for administrators and standard users. |
| Switch to the secure desktop when prompting for elevation | Used to secure communication between the elevation prompt and other processes. When enabled, the UAC elevation prompt is limited to communication with processes that are part of Windows 10. This prevents malware from approving elevation. The default configuration is enabled. |
| Virtualize file and registry write failures to per-user locations | Used to enable non-UAC compliant applications to run properly. Applications that write to restricted areas are silently redirected to space in the user profile. The default configuration is enabled. |

Enlarge Table

**Activity 6-5**

### Configuring UAC

**Time Required:**5 minutes

**Objective:**Identify the differences in simplified UAC settings

**Description:**In most cases, UAC with the default configuration makes using a computer more secure for administrative users because many tasks performed by administrative users do not need administrative privileges, such as reading email or researching on the Internet. The default configuration does not prompt administrative users for approval when they initiate the action. In some cases, however, you might want administrators to be prompted so that they realize they are performing an administrative task. In this activity, you review how the simplified UAC settings modify the user experience.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **local**, and then click **Local Security Policy**.

1. 3

Expand **Local Policies** and then click **Security Options**.

1. 4

Scroll down to the bottom of the list of security options and read the options available for User Account Control.

1. 5

Close Local Security Policy.

1. 6

Click the **Start** button and then click **Settings**.

1. 7

In the Settings window, in the Find a setting box, type **uac** and then click **Change User Account Control settings**.

1. 8

In the User Account Control Settings dialog box, move the slider up to **Always notify** and then click **OK**.

1. 9

Click **Yes** to allow the changes. Notice that you are prompted by UAC because a program is changing the setting. Also notice that the screen is dimmed (hidden) when you are prompted by UAC which indicates that the secure desktop is being used.

1. 10

In the Find a setting box, type **uac** and then click **Change User Account Control settings**. Notice that this time you are prompted to elevate.

1. 11

In the User Account Control dialog box, click **Yes**.

1. 12

In the User Account Control Settings dialog box, move the slider down to **Notify me only when apps make changes to my computer (do not dim my desktop)** and then click **OK**.

1. 13

Click **Yes** to allow the changes.

1. 14

Click the **Start** button, type **diskpart**, and then press **Enter**. Notice that a UAC dialog box appears, but the desktop is not dimmed. Secure desktop is not being used.

1. 15

In the User Account Control dialog box, click **No**.

1. 16

In the Find a setting box, type **uac** and then click **Change User Account Control settings**.

1. 17

Move the slider back to the default setting and then click **OK**.

1. 18

Click **Yes** to approve the change.

1. 19

Close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**6-4**Malware Protection

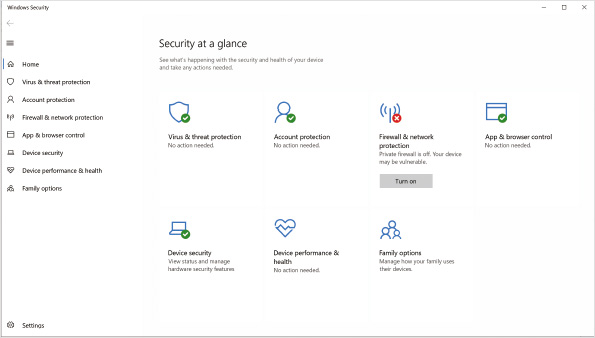
[**Malware**](javascript://) (malicious software) is unwanted software on a computer that you did not choose to install. As the name indicates, this software performs actions you don’t approve.

Some of the things malware can do include:

* Sending spam from your computer to the Internet
* Capturing user names and passwords for websites, including online banking
* Stealing personal information for identity theft
* Allowing others to remotely control your computer and use it as a launching point for illegal activities
* Using your processor to mine digital currency

Windows Security, shown in [Figure 6-11](javascript://), is a console that brings together most security settings, including those related to malware. The Home screen displays the status of security services. A green check mark indicates that everything is working properly. A yellow warning exclamation sign indicates that you should review the status of the service and might need to perform an action. A red x indicates that an error with the services needs to be fixed.

**Figure 6-11Windows Security**



Enlarge Image

Windows Defender Advanced Threat Protection (ATP) is the collection of features that protects Windows 10 from malware, and you can configure anti-malware features from within Windows Security.

Other functionality in Windows Security includes:

* *Account protection*—This screen provides links to configure sign-in options and dynamic lock.
* *Firewall & network protection*—This screen provides status information about Windows Defender Firewall and links to configure Windows Defender Firewall.
* *Family options*—For home users, this screen provides links to configure family settings for Microsoft accounts. Once enabled, you can set limits on specific accounts that restrict access to websites and limit screen time. You can also obtain weekly activity reports to monitor activity.

Go to pg.

[**help**](javascript://)

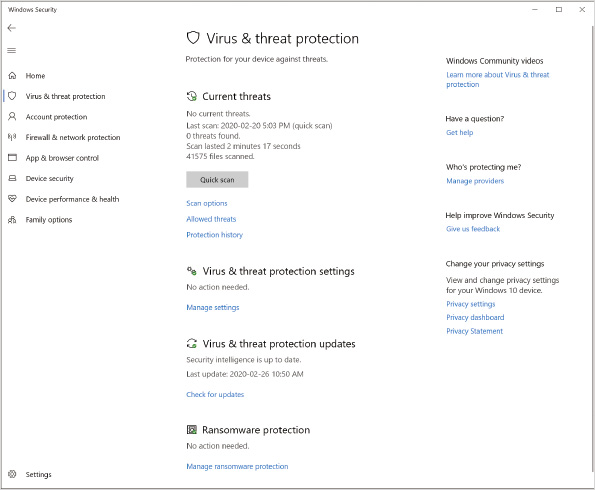
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-4aVirus and Threat Protection

The Virus & threat protection screen, shown in [Figure 6-12](javascript://), provides the settings for managing traditional anti-malware scanning in [**Windows Defender Antivirus**](javascript://). The anti-malware scanning provided by Windows Defender Antivirus is as good as that found in third-party anti-malware software. Home users typically don’t need to buy additional anti-malware software.

**Figure 6-12Virus & Threat Protection Screen**



Enlarge Image

In an enterprise environment, you might choose to use third-party anti-malware software, not because that software detects and removes malware better than Windows Defender Antivirus, but because it offers better management capabilities. Most corporate anti-malware software has a centralized console for distributing signature updates and monitoring computers. Windows Defender Antivirus provides no centralized monitoring or control. Consequently, it is best suited to small environments.

**Tip**

Microsoft does provide centralized monitoring for Windows Defender Antivirus as part of Microsoft Configuration Manager Endpoint Protection enterprise management software and Microsoft Intune cloud service.

### Scanning

Real-time scanning constantly monitors activity on your computer. It monitors actions, files that are being downloaded, and disk activity. The goal of real-time scanning is to detect malware before it executes on your computer. For example, if you run a program that contains malware, real-time scanning identifies the malware when the file is read from disk and prevents it from executing. It will also quarantine the file.

**Tip**

If you are performing a disk-intensive activity, temporarily disabling real-time scanning can increase overall storage performance.

On-demand scanning is used to identify malware that is already present on your computer. A quick scan looks for malware in the most common locations. When a quick scan is running, user performance is not affected. A full scan looks at the entire disk system and running processes to find malware. This type of scan is more complete, but it might affect system performance. A full scan is typically performed when you think that malware is on your computer. You can run a custom scan if you want to check a specific folder or file for malware.

Some malware is capable of hiding itself when resident in memory and avoiding detection. In some cases, the malware is capable of restarting itself after infection and remaining undetectable by anti-malware software, such as Windows Defender Firewall. For this type of malware, you need to do an offline scan where Windows is not running so that the malware is not in memory. For this scenario, use Windows Defender Offline. Windows Defender Offline restarts your computer and performs a scan while your installation of Windows 10 is not running. You can run a Windows Defender Offline scan manually or it might be suggested when Windows Defender Antivirus detects malware.

Windows 10 automatically runs scheduled scans in the background. This is important to detect malware that has been saved to disk before malware definitions were updated. A default schedule is in place for running quick scans and remediation scans (full scan), but you can configure your own schedule by using the Set-MpPreference cmdlet or by using Group Policy. No graphical interface is available for configuring scheduled scans.

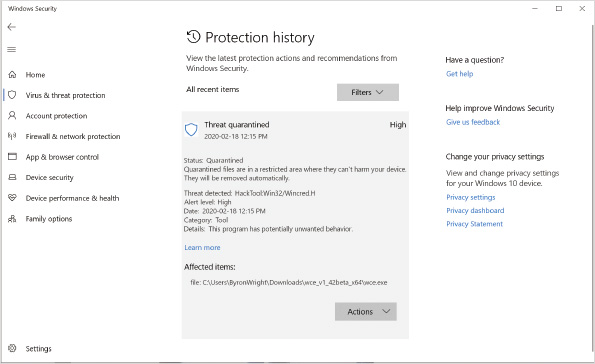
### Definitions

Windows Defender Antivirus uses definitions to identify known and potential malware. The definitions should be updated regularly to ensure you can detect the most recent malware. By default, definitions are updated automatically by Windows Update; however, you also have the option to manually update the definitions on the Virus & threat protection screen.

### Protection History

In Windows Defender, you can view the history of items that were detected. In the list of detections, you can expand the event, as shown in [Figure 6-13](javascript://). Expanding the event allows you to read more information about what was detected and the action subsequently performed by Windows Defender Antivirus.

**Figure 6-13Protection History Screen**



Enlarge Image

Sometimes antivirus software can be overly aggressive and quarantine files that you legitimately want to use and access. This is common with tools that analyze Windows security or scan the network. On the Actions button, you can restore a quarantined file that appears as a false positive. Alternatively, after you’ve verified that the file was a threat, you can remove it using the Actions button.

**Tip**

If you identify a false positive detection and allow a program to run, it is listed in Allowed threats.

In most cases, only a few items should be listed in the protection history; however, if you have an unfortunate event (or a few of them) and many items are listed in the protection history, you can use filtering to identify the items you want to view. The Filters button lets you view items based on recommendations, quarantined items, cleaned items, blocked actions, and severity.

### Virus and Threat Protection Settings

Windows Defender Antivirus has a very limited set of configuration options available in the Update & security settings. In most cases, you want to leave these options at the default setting. The settings you can configure are:

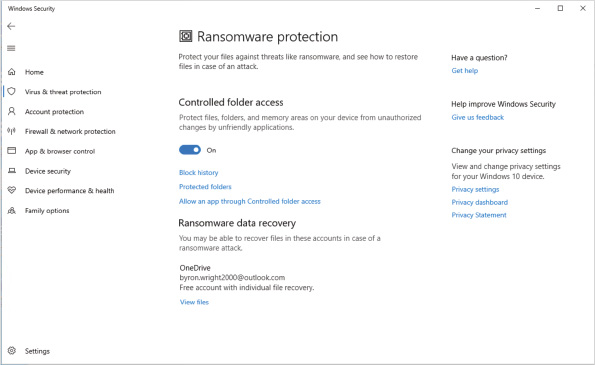
* Real-time protection—Unless you have a specific need to disable real-time protection, you should leave this on. If you are copying a large number of files, disabling real-time protection might speed up the copying process. Also, if you are trying to download a file that you know is safe, and Windows Defender is seeing the file as a false positive, you can temporarily disable real-time scanning.
* Cloud-based protection—This option allows Windows Defender Antivirus to communicate with Microsoft to report malware and scanning activity on your computer. This information is used by Microsoft to improve Windows Defender Antivirus. Cloud-based protection is enabled by default.
* Automatic sample submission—When this option is enabled, samples of detected malware are sent back to Microsoft for further analysis. This is particularly important for malware identified by heuristics. Heuristics identifies malware based on pattern of behavior instead of signature. After submission to Microsoft, the malware signature can be included in definitions. Automatic sample submission is enabled by default.
* Tamper protection—When this option is enabled, applications can’t modify Windows Defender Antivirus settings. This helps to prevent malware from evading Windows Defender Antivirus by adding an exclusion or disabling real-time protection.
* Exclusions—Some applications, such as databases, might not run properly when real-time scanning is performed on them. In such a case, you can create an exclusion for specific files or folders. No exclusions are configured by default.
* Notifications—You control which events generate notifications. By default, you get notified when Windows Defender Antivirus completes a scan, finds a threat, blocks a file, or blocks an action.

### Ransomware Protection

Losing all the data files on a computer is one of the most devastating events that can occur for a computer user. Ransomware is a type of malware that encrypts files and makes them unusable unless you pay a fee to the hacker(s). The charge to decrypt might be a few hundred dollars or thousands of dollars. It’s better to protect yourself than to pay the ransom.

To protect your computer against ransomware, Windows 10 includes [**controlled folder access**](javascript://), shown in [Figure 6-14](javascript://). You can specify folders that applications are not allowed to access. This doesn’t prevent you from opening a data file using Word or Excel, but it does stop unknown applications from modifying or deleting files. If you have a trusted application that is blocked by controlled folder access, you can allow it.

**Figure 6-14Ransomware Protection Screen**



Enlarge Image

### Group Policy Configuration

The user interface for configuring Windows Defender offers very few options. If you need fine-grained control over Windows Defender, you can use Group Policy. In a domain-based environment, the Group Policy settings can be easily deployed to multiple computers. The Group Policy settings for Windows Defender are located in Computer Configuration\Administrative Templates\Windows Components\Windows Defender Antivirus. Each of the settings is documented in the Group Policy editor.

### Windows PowerShell Configuration

The graphical interface for managing Windows Defender Antivirus does not give you all the available management options. To view and modify the detailed configuration settings for a local instance of Windows Defender Antivirus, you can use Windows PowerShell cmdlets. You can use Windows PowerShell scripts to configure multiple computers, but Group Policy is better suited for that task. [Table 6-3](javascript://) lists some of the cmdlets for managing Windows Defender Antivirus.

**Table 6-3**

### Windows PowerShell Cmdlets for Managing Windows Defender Antivirus

| **Cmdlet** | **Description** |
| --- | --- |
| Get-MpPreference | Views the current configuration settings for Windows Defender Antivirus |
| Set-MpPreference | Modifies the settings for Windows Defender Antivirus |
| Get-MpComputerStatus | Views the current status of Windows Defender Antivirus |
| Get-MpThreat | Views threats that have been detected by Windows Defender Antivirus; this identifies the threat but not the specific incident information |
| Get-MpThreatDetection | Views incident information, such as time of the incident, where threats have been detected by Windows Defender Antivirus |
| Remove-MpThreat | Removes active threats; in most cases Windows Defender Antivirus removes threats by default and the cmdlet is not required |
| Start-MpScan | Starts a Windows Defender Antivirus scan |
| Start-MpWDOScan | Starts a Windows Defender offline scan |
| Update-MpSignature | Updates definitions for Windows Defender Antivirus |

**Activity 6-6**

### Using Windows Defender Antivirus

**Time Required:**10 minutes

**Objective:**Use Windows Defender Antivirus to prevent spyware on a computer

**Description:**Windows Defender Antivirus is used to prevent malware installation and remove malware. You can test the functionality of anti-malware software by using the EICAR anti-malware test file. The test file has a specific text string that all anti-malware software detects but poses no risk of a malware infection. In this activity, you test real-time scanning and on-demand scanning.

1. 1

If necessary, start your computer and sign in.

1. 2

On the taskbar, click **Microsoft Edge**.

1. 3

In the Search or enter web address box, type [www.eicar.org](http://www.eicar.org/" \t "_blank) and then press **Enter**.

1. 4

On the Eicar website, click the **DOWNLOAD ANTI MALWARE TESTFILE** icon in the upper-right corner and then click **DOWNLOAD** in the left navigation menu.

1. 5

On the Download page, scroll down and below the Download area using the secure, SSL enabled protocol https heading, click **eicar\_com.zip** and then click **Save**. You should be notified that Windows Defender detected malware and deleted it.

1. 6

Leave the Microsoft Edge window open for later in this activity.

1. 7

Click the **Start** button and then click **Settings**.

1. 8

In the Settings window, click **Update & Security** and then click **Windows Security**.

1. 9

On the Windows Security screen, click **Virus & threat protection**.

1. 10

In the Windows Security window, below Virus & threat protection settings, click **Manage settings**.

1. 11

Click the **Real-time protection** switch to turn it **Off**. If necessary, click **Yes** in the User Account Control prompt to confirm the action.

1. 12

In Microsoft Edge, click **eicar\_com.zip** and then click **Save**.

1. 13

Click **Open folder** and verify that the file is downloaded.

1. 14

In the Windows Security window, click the **Real-time protection** switch to turn it **On**. Notice that the eicar\_com.zip file is not detected immediately because the file hasn’t been accessed yet.

1. 15

In the left navigation pane, click **Virus & threat protection** and then click **Scan options**.

1. 16

On the Scan options screen, click **Custom scan** and then click **Scan now**.

1. 17

In the Select Folder dialog box, browse to **Local Disk (C:)**, select the **Users** folder, and then click **Select Folder**.

1. 18

When the scan is complete, the EICAR test file is shown as a detected threat. Click **Virus:DOS/EICAR\_Test\_File** to view the details.

1. 19

Click **See details** and then click **Yes** in the User Account Control prompt.

1. 20

Read the detailed information about the EICAR test file and then click **OK**.

1. 21

Click **Start actions** to apply the default action.

1. 22

Close all open windows.

1. 23

Click the **Start** button, type **PowerShell**, right-click **Windows PowerShell**, and then click **Run as administrator**.

1. 24

In the User Account Control dialog box, click **Yes**.

1. 25

At the Windows PowerShell prompt, type **Get-MpThreat** and then press **Enter**. Read the threat information.

1. 26

At the Windows PowerShell prompt, type **Get-MpThreatDetection** and then press **Enter**. Read the threat detection information.

1. 27

At the Windows PowerShell prompt, type **Get-MpPreference** and then press **Enter**. Read the configuration information.

1. 28

At the Windows PowerShell prompt, type **Get-MpComputerStatus** and then press **Enter**. Read the status information.

1. 29

Close the Windows PowerShell window.

Go to pg.

[**help**](javascript://)

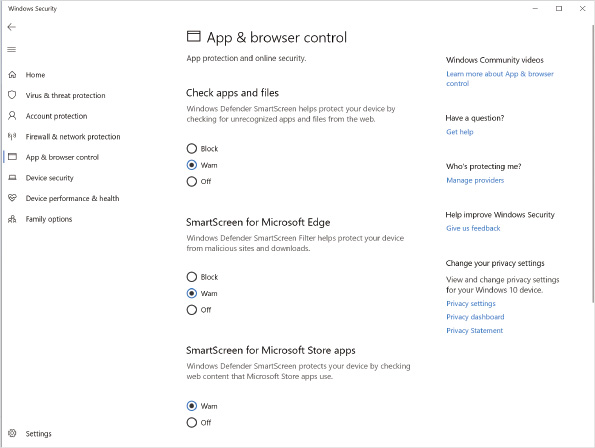
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-4bApp & Browser Control

Because the Internet is one of the primary sources of malware, it’s important that access to the Internet is monitored for malware. [**Windows Defender Smartscreen**](javascript://) is included in Windows 10 to monitor unrecognized apps and files, malicious websites, and web content downloaded by Microsoft Store apps. For these options, you can configure content to be blocked, a warning displayed, or no action (off), as shown in [Figure 6-15](javascript://).

**Figure 6-15App & Browser Control Screen**



Enlarge Image

Not all malware will be detected by Windows Defender Smartscreen because it identifies known malicious files. Malware developers are constantly developing new methods to exploit Windows 10. [**Windows Defender Application Guard**](javascript://) can mitigate some malware risk by running Microsoft Edge in an isolated browsing environment. The isolated browsing environment is a Hyper-V enabled container that is in a separate environment from the operating system. This prevents an unknown exploit from affecting the operating system and infecting Windows 10. It also prevents the exploit from accessing credentials currently in use.

Windows 10 Pro includes Windows Defender Application Guard, but you need to configure it for each device. To centrally manage Windows Defender Application Guard by using management software, such as Microsoft Intune, you need to use Windows 10 Enterprise or Windows 10 Education. You also need to have a computer that supports Hyper-V virtualization.

Known exploit mitigation techniques can be enabled or disabled in Windows 10. Many of them are enabled by default because they generally do not cause application compatibility issues. For example, Data Execution Prevention (DEP), which ensures that code is not run from data-only memory, is on by default. Other mitigations are not enabled by default because they can cause compatibility issues; because of this, you should evaluate your applications before enabling the mitigation.

In addition to system-level exploit protection mitigations, you can configure application-specific settings. If you have one application that is not compatible with a mitigation, you can disable the mitigation for that specific application and enable the mitigation and the system level.

**Note 1**

For a description of exploit protection mitigations, see Customize exploit protection at [https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/customize-exploit-protection](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/customize-exploit-protection" \t "_blank).

You can deploy customized mitigation settings to multiple computers by using an XML file with the customized mitigation settings. First, you configure a reference computer with the customized settings and then export those settings as an XML file. You can export the XML file from exploit-protection settings or by using the Get-ProcessMitigation cmdlet with the -PolicyFilePath parameter. You can import the XML file on a destination computer by using the Set-ProcessMitigation cmdlet or by using the Use a common set of exploit protection settings setting in Group Policy. After you import the XML file, you can view the settings in Windows Security.

Go to pg.

[**help**](javascript://)

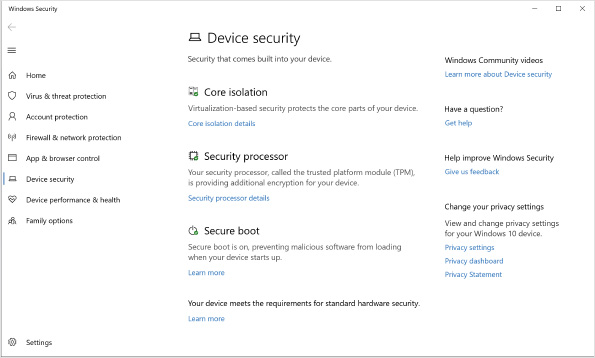
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-4cDevice Security

The content on the Device security screen, shown in [Figure 6-16](javascript://), in Windows Security varies depending on the capabilities of your computer. The options supported by your computer automatically appear if applicable.

**Figure 6-16Device Security Screen**



Enlarge Image

Core isolation includes memory protection techniques that are available only if your computer supports Hyper-V virtualization. Memory integrity enforces the requirement for code running kernel mode to be trusted. Memory access protection prevents drive-by direct memory access (DMA) attaches that can occur when hot-plug PCI devices are connected via Thunderbolt 3 ports. Memory access protection is enabled automatically if your computer has a Thunderbolt 3 port.

Security processor contains the settings for the trusted platform module (TPM) in your computer. You can use this area to view information about the TPM, including the manufacturer and TPM specification version. If you want to view error messages or clear the TPM to default settings, select the Security processor troubleshooting link.

**Caution**

Data encryption keys are often stored in the TPM. Make sure you back up TPM data before you clear it back to default settings.

Secure boot is a system that ensures the integrity of files used early in the Windows 10 startup process. If startup files are modified, Windows 10 will not start in order to ensure that malware is not being loaded. Newer computers using UEFI firmware support using secure boot.

At the bottom of the Device security screen is a status message about the support your computer has for standard hardware security, including the following:

* Your device meets the requirements for standard hardware security—When you see this message, your device supports memory integrity and core isolation. Your device also has a TPM-meeting specification version 2.0, secure boot enabled, DEP enabled, and UEFI memory attributes table (MAT).
* Your device meets the requirements for enhanced hardware security—When you see this message, your device meets the requirements for standard hardware security and has memory integrity enabled.
* Your device exceeds the requirements for enhanced hardware security—When you see this message, your device meets the requirements for enhanced hardware security and has System Management Mode (SMM) protection turned on. SMM protection monitors operating system memory and ensures that it is not modified.
* Standard hardware security not supported—When you see this message, at least one of the requirements for standard hardware security is not met.

Often, when a computer does not meet the requirements for standard hardware security, it is due to the TPM configuration. It is common for lower-end computers to not include a TPM. Older computers also might not have a TPM that is specified as version 2.0.

UEFI firmware configuration can also prevent a computer from meeting standard hardware security requirements. Most newer computers have UEFI firmware that supports secure boot and UEFI MAT. Sometimes, however, the UEFI firmware is configured to run in BIOS-compatibility mode, which doesn’t support secure boot or UEFI MAT. Also, you might need to enable secure boot in the UEFI firmware. Secure boot might not be enabled by default.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**6-5**Data Security

The most basic level of data security in Windows 10 is NTFS permissions. NTFS permissions stop signed-in users from accessing files and folders for which they do not have read or write permission; however, NTFS permissions are effective in protecting data only when the original operating system is running.

You can work around NTFS permissions and gain access to data in several ways. The following are two examples:

* You can start a computer from a USB drive or DVD and run Linux with an NTFS driver. Linux with an NTFS driver can read NTFS-formatted partitions and ignore the security information. This allows you to copy or modify data on the NTFS-formatted volume even without a valid user name.
* You can attach a hard drive from one Windows 10 computer to another. Local administrators always can take ownership of files and then read or modify them. When you move a hard drive, the local administrators of the new system can take ownership of files and then read or modify them.

As you can see, it is relatively easy to work around NTFS permissions when you have physical access to the computer. NTFS permissions are a reliable method of securing data when files are accessible only over a network, but not when there is physical access to the computer storing the files. This makes NTFS permissions excellent for servers, which are typically physically secured, but not as effective for desktop computers and laptops. Laptops are particularly at risk because they are more often lost or stolen.

To secure data on desktop computers and laptops, encryption is required. Windows 10 includes Encrypting File System (EFS) and BitLocker Drive Encryption to encrypt files.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-5aEncryption Algorithms

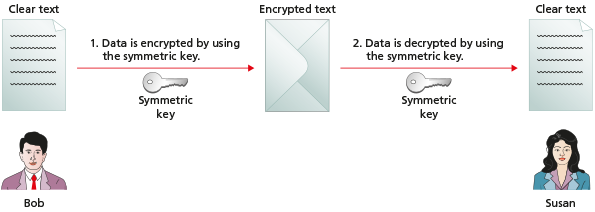
Encryption is the process of taking data and rendering it unreadable. In most cases, encryption is a two-way process; first, data is encrypted to make it unreadable, then it is decrypted to make it readable again. The process for encrypting data uses an algorithm. For computerized encryption of data, algorithms are math formulas that scramble the data into an unreadable format.

Different types of encryption algorithms are suited to different purposes. Some algorithms are faster than others and best suited to encrypting large volumes of data. Other algorithms require two separate keys for encryption and decryption and are well suited to operations performed by two separate users or processes.

### Symmetric Encryption

A [**symmetric encryption algorithm**](javascript://) uses the same key to encrypt data and decrypt data. This is very similar to how a deadbolt lock works. When you leave your house, you lock the door with your key; when you return, you unlock the door with the same key. [Figure 6-17](javascript://) shows Bob and Susan accessing encrypted data by using the same key.

**Figure 6-17Symmetric Encryption**



Enlarge Image

In computerized encryption, the key is a long number that is extremely difficult to guess. The longer the key, the harder it is to guess. One of the most common key lengths for symmetric encryption is 128 bits. Data that is symmetrically encrypted with a 128-bit key will take years to decrypt by guessing the key. Other solutions offer stronger encryption, with longer keys of 4096 bits or more.

Symmetric encryption is strong and fast, which makes it well suited to encrypting large volumes of data, such as that contained in files. Most file encryption is done with a symmetric encryption algorithm. Both EFS and BitLocker Drive Encryption use symmetric encryption to secure data.

The biggest problem with symmetric encryption is securing the key. Anyone who has a copy of the encryption key can decrypt the data. In [Figure 6-17](javascript://), both Bob and Susan need to have a copy of the same symmetric key. EFS and BitLocker Drive Encryption both use different methods to secure the key.

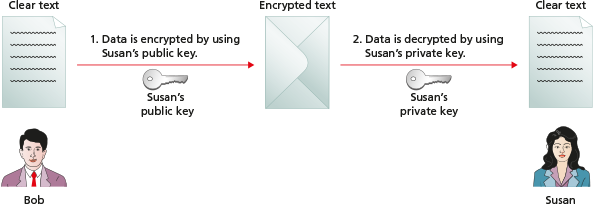
### Asymmetric Encryption

An [**asymmetric encryption algorithm**](javascript://) uses two related, but unique, keys to encrypt and decrypt data. Data encrypted by one key is decrypted by the other key. This is similar to an electronic safe, where one person has a code that allows him or her to deposit money, but the other person has a code that allows him or her to remove money from the safe.

The keys used in asymmetric encryption are part of a digital certificate. Digital certificates are obtained from certificate authorities (sometimes also called certification authorities). Some of the better-known certificate authorities are Comodo, Digicert, and Let’s Encrypt. Companies can also generate their own digital certificates internally. Most server operating systems, including Windows Server 2019, have certificate authority functionality as an option.

The digital certificate from a certification authority contains a public key and a private key. The public key is meant to be known to other people. The private key is protected and known only to you. By using both keys, encrypted data can be sent securely without the risk of transferring a symmetrical key. For example, in [Figure 6-18](javascript://), Bob is encrypting data for Susan. When Bob performs the encryption, he uses Susan’s public key. Then, Susan—and only Susan—can decrypt the data by using her private key because only Susan has the private key.

**Figure 6-18Asymmetric Encryption**



Enlarge Image

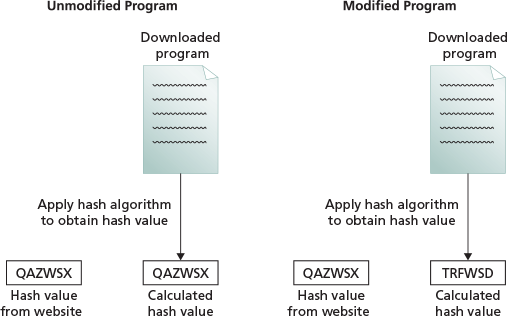
Asymmetric encryption requires more processing power and is less secure than symmetric encryption. This makes asymmetric encryption unsuitable for large volumes of data. Asymmetric encryption is typically used to encrypt small amounts of data. Many systems for encrypting data use symmetric encryption to encrypt the data and then use asymmetric encryption to protect just the symmetric key because a symmetric key is relatively small compared to the data it has encrypted.

### Hashing

[**Hashing algorithms**](javascript://) are used for a very different purpose than symmetric and asymmetric encryption algorithms. A hashing algorithm is one-way encryption, which means that it encrypts data, but the data cannot be decrypted.

Hashing is used to uniquely identify data rather than prevent access to data. Sometimes, hash values for data are referred to as fingerprints. When you download software, some websites give you an MD5 value for the file. MD5 is a hashing algorithm. The MD5 value is the unique value that is created when the MD5 hashing algorithm is run on the downloadable software. You can verify that the software has not been modified or corrupted by verifying the MD5 value after you download the software. If the software has been changed in any way, the MD5 value is also changed. [Figure 6-19](javascript://) shows how a hash value is used to verify that software has not been modified.

**Figure 6-19Hash Encryption**



Hashing algorithms are also used for storing passwords. The passwords entered by users are not actually checked. The operating system verifies that the hash value of the password entered by the user matches the hash value that is stored for the user’s password. When passwords are stored only as a hash value, it is impossible to decrypt the password. The password can be guessed only by brute force (trying all possible combinations).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-5bEncrypting File System

EFS is a technology that was first included with Windows 2000 Professional. It encrypts individual files and folders on a volume. This makes it suitable for protecting data files and folders on workstations and laptops; however, it can also be used to encrypt files and folders on network servers. This section focuses on encrypting local files.

To encrypt a file or folder by using EFS, the file or folder must be located on an NTFS-formatted partition. FAT- and FAT32-formatted partitions cannot hold EFS-encrypted files. FAT and FAT32 file systems are not capable of holding the information required to decrypt the files.

When a file is encrypted, the data in the file is encrypted using a symmetrical key that is randomly generated for that specific file. The symmetrical key is then encrypted by asymmetric encryption, based on user-specific keys. This protects the symmetrical key from unauthorized users.

To use EFS, users must have a digital certificate with a public key and a private key. Unless specifically configured otherwise, users do not have a digital certificate by default. If a user encrypts a file and does not have a digital certificate, Windows 10 generates a certificate automatically. The public key from the digital certificate is used to encrypt the symmetrical key that encrypted the file. Only the user who encrypted the file is able to decrypt the symmetrical key because only that user has access to the private key required to decrypt the symmetrical key. The EFS encryption and decryption process is shown in [Figure 6-20](javascript://).

**Figure 6-20EFS Encryption and Decryption Process**



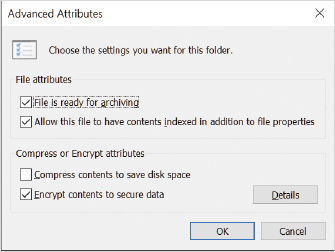
Enlarge Image

**Tip**

User certificates are stored in the user profile.

From the user perspective, encryption is a file attribute, like compression, hidden, or read-only. To encrypt a file, a user needs to access the Advanced Attributes of the file, as shown in [Figure 6-21](javascript://).

**Figure 6-21Advanced Attributes of a File**



**Tip**

Files that are encrypted cannot also be compressed.

Files can also be encrypted using the cipher command-line utility. Cipher is useful for scripting or making changes to many files at once. For more information about cipher options, run cipher with the /? switch from a command prompt.

### Lost Encryption Keys

If a user loses the certificate that secures an EFS key, the encrypted file is unrecoverable with the default configuration. The encrypted file can be recovered only if the user has backed up the EFS certificate or if a recovery certificate has been created and installed.

The following are some ways EFS certificates may be lost:

* The user profile is corrupted.
* The user profile is deleted accidentally.
* The user is deleted from the system.
* The user password is reset.

User Accounts in Control Panel provides an option for you to manage your file encryption certificates that allows you to view, create, and back up certificates used for EFS. You can also configure EFS to use a certificate on a smart card and update previously encrypted files to use a new EFS certificate. After a certificate is backed up, it can be used whenever required. This certificate can be imported back into a new user profile or even to a different user.

**Tip**

You can back up and import EFS certificates by using the Certificates snap-in in a Microsoft Management Console.

Creating a recovery certificate allows the files encrypted by all users to be recovered if required. When a recovery certificate is in place, the symmetric key for all files is stored twice. The first copy of the symmetric key is encrypted by using the public key of the user encrypting the file. The second copy of the symmetric key is encrypted by using the public key of the recovery certificate.

The steps for creating and using a recovery certificate are as follows:

1. 1

Create the recovery certificate—This is done by running cipher with the /r:filename option, where filename is the name of the recovery certificate.

1. 2

Install the recovery certificate—This is done by importing the recovery certificate into the local security policy as a data recovery agent. After this point, all newly encrypted files will include a symmetric key that is accessible to a user using the recovery certificate.

1. 3

Update existing encrypted files—This is done by running cipher with the /u option. Encrypted files can be updated only by a user who is able to decrypt the files. This means that multiple users might need to update files. Updating encrypted files adds an extra encrypted copy of the symmetric key that is accessible to a user using the recovery certificate.

To recover files, you import the recovery certificate into a user profile using the Certificates MMC snap-in. After the recovery certificate is imported, that user can decrypt any files necessary.

In a domain-based environment, the recovery certificate is deployed by using Group Policy rather than individually on each computer. To do this, navigate to Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypting File System, right-click Encrypting File System, and then click Add Data Recovery Agent. A wizard then guides you through the process of importing the certificate that will be used as a data recovery agent.

### Sharing Encrypted Files

In a domain-based environment, it is easy to store encrypted files on a server and access them from multiple workstations or share them with other users. The necessary certificates are automatically created and stored on the remote server, and the files are encrypted and shared. On workstations that are part of a workgroup or local users in a domain, the process takes more work.

For a single user to work with encrypted files on multiple computers, follow these steps:

1. 1

Encrypt the file on the first computer.

1. 2

Export the EFS certificate, including the private key from the first computer.

1. 3

Import the EFS certificate, including the private key on the second computer.

1. 4

Open the encrypted file on the second computer.

To share encrypted files with other users, follow these steps:

1. 1

Export the EFS certificate of the first user but do not include the private key.

1. 2

Import the EFS certificate of the first user into the profile of the second user as a trusted person.

1. 3

The second user encrypts the file and shares it with the first user. A copy of the symmetric key is encrypted with the public key of each user.

**Tip**

In an environment without an internal certificate authority, the EFS certificate for a user is created automatically the first time he or she encrypts a file.

Encrypted files are typically not shared within a workgroup because of the complex process required. Sharing encrypted files is more common among domain users where no additional configuration is required.

### Moving and Copying Encrypted Files

The encryption of files and folders behaves differently than NTFS permissions and compression when files and folders are moved and copied. When files and folders are copied, they always take on the NTFS permissions or compression attribute of the folder they are copied into; however, this is not the case for encrypted files.

The following rules apply for moving and copying encrypted files:

* An unencrypted file copied or moved to an encrypted folder becomes encrypted.
* An encrypted file copied or moved to an unencrypted folder remains encrypted.
* An encrypted file copied or moved to a FAT or FAT32-formatted volume becomes unencrypted if you have access to decrypt the file. If you do not have access to decrypt the file, you receive an access-denied error.

**Activity 6-7**

### Using EFS

**Time Required:**10 minutes

**Objective:**Use EFS to encrypt and protect files

**Description:**EFS is used to encrypt individual files and folders. After a file is encrypted, only authorized users are able to read the data in the file. In this activity, you encrypt a file and test it to ensure that only authorized users can decrypt the file.

1. 1

If necessary, start your computer and sign in.

1. 2

On the taskbar, click **File Explorer**.

1. 3

In the File Explorer window, navigate to **C:\Users\Public\Public Documents\**.

1. 4

Right-click an open area in the **Name** column, point to **New**, and then click **Text Document**.

1. 5

Type **encrypt** as the file name and then press **Enter**.

1. 6

Double-click **encrypt** to open it and then type a line of text.

1. 7

Click **File** on the menu bar, click **Exit**, and then click **Save**.

1. 8

Right-click an open area in the **Name** column, point to **New**, and then click **Text Document**.

1. 9

Type **other** as the file name and then press **Enter**.

1. 10

Double-click **other** to open it and then type a line of text.

1. 11

Click **File** on the menu bar, click **Exit**, and then click **Save**.

1. 12

Right-click **encrypt** and then click **Properties**.

1. 13

Click the **Advanced** button, select the **Encrypt contents to secure data** check box, and then click **OK**.

1. 14

Click **OK**, click **Encrypt the file only**, and then click **OK**. Notice that the file encrypt now has a lock icon to indicate that it is encrypted.

1. 15

Close the File Explorer window.

1. 16

Switch the user to **Bob**.

1. 17

On the taskbar, click **File Explorer**.

1. 18

In File Explorer, navigate to **C:\Users\Public\Public Documents\**.

1. 19

Double-click **other**. Notice that you are able to open and read this file.

1. 20

Exit Notepad.

1. 21

Double-click **encrypt**. You receive an error indicating that access is denied because the file is encrypted.

1. 22

Click **OK** to close the error dialog box and then exit Notepad.

1. 23

Sign out as **Bob**.

**Activity 6-8**

### Recovering Lost Encryption Keys

**Time Required:**10 minutes

**Objective:**Back up and restore an EFS encryption key

**Description:**A lost EFS encryption key means that an encrypted file cannot be accessed. To avoid this problem, you can back up the encryption key of a user. If a user’s encryption key is backed up, you can restore it and then the user regains access to his or her files. In this activity, you back up and restore the encryption key for a user.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **control** and then click **Control Panel**.

1. 3

Click **User Accounts** and then click **User Accounts**.

1. 4

In the left pane, click **Manage your file encryption certificates**.

1. 5

Click **Next** to start the Manage your file encryption certificates wizard.

1. 6

Click **Next** to accept the default certificate.

1. 7

If necessary, click **Back up the certificate and key now**.

1. 8

To set the Backup location, click the **Browse** button, type **CertBak**, and then click **Save**. The default location is your Documents directory. Typically, you would save the backed-up certificate on removable storage and keep it in a secure location.

1. 9

In the Password and Confirm password boxes, type **password** and then click **Next**. It is important to secure the backup with a password because it contains your private key.

1. 10

Click **Next** to skip updating encrypted files with a new key.

1. 11

Click **Close**.

1. 12

Click the **Start** button, type **mmc**, and then press **Enter**.

1. 13

Click **Yes** to start the Microsoft Management Console.

1. 14

Click **File** on the menu bar and then click **Add/Remove Snap-in**.

1. 15

In the Available snap-ins area, click **Certificates** and then click **Add**.

1. 16

Click **Finish** to accept managing certificates for your user account and then click **OK**.

1. 17

In the left pane, expand **Certificates—Current User**, expand **Personal**, and then click **Certificates**.

1. 18

In the middle pane, right-click the **Userx** certificate, and then click **Delete**. If multiple certificates appear, delete all of them.

1. 19

Read the warning message about losing the ability to decrypt files and then click **Yes**.

1. 20

Sign out and sign in again. This clears the certificate from memory.

1. 21

On the taskbar, click **File Explorer**.

1. 22

In File Explorer, below Recent files, double-click **encrypt**. You should receive an error indicating that access is denied because the file is encrypted.

1. 23

Click **OK** to close the error dialog box and then exit Notepad.

1. 24

Click the **Start** button, type **mmc**, and then press **Enter**.

1. 25

Click **Yes** to start the Microsoft Management Console.

1. 26

Click **File** on the menu bar and then click **Add/Remove Snap-in**.

1. 27

In the Available snap-ins area, click **Certificates** and then click **Add**.

1. 28

Click **Finish** to accept managing certificates for your user account and then click **OK**.

1. 29

In the left pane, expand **Certificates - Current User** and then click **Personal**.

1. 30

Right-click **Personal**, point to **All Tasks,** and then click **Import**.

1. 31

Click **Next** to start the Certificate Import Wizard.

1. 32

Click the **Browse** button, change the file type to **Personal Information Exchange (\*.pfx,\*.p12)**, click **CertBak**, and then click **Open**.

1. 33

Click **Next**.

1. 34

In the Password box, type **password**.

1. 35

Select the **Mark this key as exportable. This will allow you to back up or transport your keys at a later time.** check box and then click **Next**.

1. 36

Click **Next** to accept the default certificate location, click **Finish**, and then click **OK**. Now you have a personal certificate again.

1. 37

Close the MMC and then click **No** to saving the console settings.

1. 38

In the File Explorer window, double-click **encrypt**. Now you are able to open the file because you have restored the certificate that contains your private key. Your public key was used to encrypt the symmetrical key that was used to encrypt the file.

1. 39

Close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

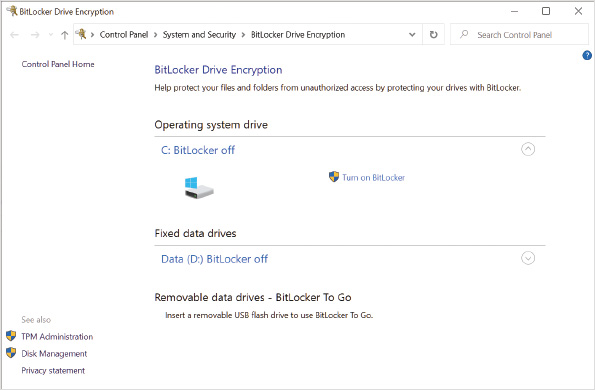
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-5cBitLocker Drive Encryption

[**BitLocker Drive Encryption**](javascript://) is a data encryption feature included with Windows 10 that addresses some of the shortcomings of EFS. EFS is designed to encrypt only specified files. Some files, such as the operating system files, cannot be encrypted by using EFS. In addition, in some cases it might be possible to introduce low-level software that is able to steal EFS certificates.

When you use BitLocker Drive Encryption, an entire volume is encrypted. This protects not only your data, but also the operating system. Protecting the operating system ensures that additional software is not placed on the drive when the operating system is shut down. [Figure 6-22](javascript://) shows the screen used to enable BitLocker Drive Encryption.

**Figure 6-22BitLocker Drive Encryption**



Enlarge Image

BitLocker Drive Encryption is designed to be used with a TPM. A TPM is part of the motherboard in a computer and is used to store encryption keys and certificates. Not all computers have a TPM module, and you should verify whether a TPM is present when buying a newer computer. BitLocker Drive Encryption can be used on computers without a TPM, in which case the encryption keys are stored on a USB drive or you need to enter a PIN at startup.

When a TPM is used, BitLocker Drive Encryption has two modes:

* TPM only—In this mode, the user is not aware that BitLocker is activated because the keys stored in the TPM are automatically used to start Windows 10. This option protects data from offline modification but does not add any extra protection to the boot process to prevent password guessing.
* Startup key—In this mode, the user must supply a startup key to boot Windows 10. The startup key can be configured on a USB drive or as a PIN entered by the user. This adds extra protection because password guessing to sign in to the operating system cannot be performed without first obtaining the startup key.

**Caution**

Requiring users to enter a startup PIN adds security, but it also entails one more item for users to remember. TPM-only configuration results in fewer help desk calls and is still quite secure.

### BitLocker Hard Drive Configuration

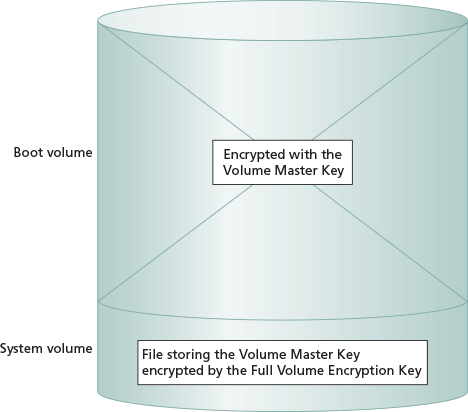
To use BitLocker Drive Encryption, a hard drive must be divided into two partitions. One partition is used as the operating system volume. The operating system volume is the volume that is encrypted. This volume is the C: drive that contains both the operating system and user data.

The second required volume is the system volume. The system volume is not encrypted and contains the necessary files to boot the operating system. This volume must be at least 300 MB and formatted as an NTFS volume. Windows 10 automatically creates this volume as part of the installation process unless you specifically prevent it.

### BitLocker Encryption Keys

BitLocker uses two keys to protect data. The [**Volume Master Key (VMK)**](javascript://) is used to encrypt the data on the operating system volume. The VMK is then encrypted using a [**Full Volume Encryption Key (FVEK)**](javascript://)**.** This multiple-key method for data encryption makes it faster to change the encryption key. Changing the VMK would require re-encrypting all the data, which is time consuming. Changing the FVEK requires re-encrypting only the VMK, which is very fast. [Figure 6-23](javascript://) illustrates how the encryption keys are used to protect data.

**Figure 6-23BitLocker Encryption Keys**



Accessing BitLocker-encrypted data is seamless for the user. A filter driver is used by Windows 10 to encrypt and decrypt data transparently as it is accessed from the hard drive. All data saved on the operating system volume is encrypted, including the paging files and hibernation file. Although a slight decrease in disk performance occurs, it should not be noticeable to users in most circumstances. Microsoft claims that BitLocker has a performance impact of less than 10%.

**Activity 6-9**

### Enabling BitLocker Drive Encryption

**Time Required:**15 minutes

**Objective:**Enable BitLocker Drive Encryption

**Description:**BitLocker Drive Encryption encrypts the contents of a hard drive so that unauthorized users cannot gain access to it. This is typically implemented in mobile computers. For the best experience, you should use a computer with a TPM; however, you can enable BitLocker on computers without a TPM. In this activity, you encrypt the C: drive of a computer without a TPM.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **mmc**, and then press **Enter**.

1. 3

Click **Yes** to start the Microsoft Management Console.

1. 4

Click **File** on the menu bar and then click **Add/Remove Snap-in**.

1. 5

In the Available snap-ins area, click **Group Policy Object Editor**, and then click **Add**.

1. 6

Click **Finish** to edit the Local Computer Group Policy object and then click **OK**.

1. 7

Expand **Local Computer Policy**, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, expand **BitLocker Drive Encryption**, and then click **Operating System Drives**.

1. 8

Double-click **Require additional authentication at startup**.

1. 9

In the Require additional authentication at startup window, click **Enabled**.

1. 10

Select the **Allow BitLocker without a compatible TPM (requires a password or startup key on a USB flash drive)** check box and then click **OK**.

1. 11

Close the MMC and then click **No** to saving the settings.

1. 12

Click the **Start** button and then click **Settings**.

1. 13

In the Find a setting box, type **BitLocker** and then click **Manage BitLocker**.

1. 14

In the BitLocker Drive Encryption window, for the C: drive, click **Turn on BitLocker**.

1. 15

On the Choose how to unlock your drive at startup screen, click **Enter a password**.

1. 16

On the Create a password to unlock this drive screen, in the Enter your password and Reenter your password boxes, type **password** and then click **Next**.

1. 17

On the How do you want to back up your recovery key screen, click **Print the recovery key**.

1. 18

In the Print window, click **Microsoft Print to PDF** and then click **Print**.

1. 19

In the Save Print Output As window, in the File name box, type **BitLocker** and then click **Save**.

1. 20

On the How do you want to back up your recovery key screen, click **Next**.

1. 21

On the Choose how much of your drive to encrypt screen, click **Encrypt used disk space only (faster and best for new PC’s and drives)** and then click **Next**.

1. 22

On the Choose which encryption mode to use screen, click **New encryption mode (best for fixed drives on this device)** and then click **Next**.

1. 23

On the Are you ready to encrypt this drive screen, click **Continue**.

1. 24

Restart your computer.

1. 25

On the BitLocker screen, in the Enter the password to unlock this drive box, type **password** and then press **Enter**.

1. 26

Sign in to your computer.

1. 27

Right-click the **Start** button and then click **Windows PowerShell (Admin)**.

1. 28

In the User Account Control dialog box, click **Yes**.

1. 29

At the Windows PowerShell prompt, type **manage-bde -status** and then press **Enter**. This shows the percentage of encryption completed.

1. 30

At the Windows PowerShell prompt, type **Get-Command | \*BitLocker\*** and then press **Enter**. This displays the Windows PowerShell cmdlets available for managing BitLocker.

1. 31

At the Windows PowerShell prompt, type **Get-BitLockerVolume** and then press **Enter**. This provides status information about the BitLocker encrypted volume.

1. 32

Close the Windows PowerShell prompt window.

### BitLocker Network Unlock

One potential issue with BitLocker-encrypted systems is maintenance. If TPM and a PIN are required for startup, it prevents remote maintenance. For example, if a wake-on-LAN is used to start a computer remotely, it remains at the BitLocker screen waiting for the PIN to be entered, which means an administrator cannot remotely control it and updates cannot be installed. To resolve this issue, [**BitLocker Network Unlock**](javascript://) allows computers to start automatically when connected to the corporate network.

When Network Unlock is enabled, the computer requests a certificate from the network during startup. A Windows Deployment Services (WDS) server provides a certificate capable of unlocking BitLocker. This functionality is possible only if the computer has UEFI firmware. BIOS firmware is not supported for Network Unlock.

**Note 2**

For detailed information about enabling Network Unlock, see BitLocker: How to enable Network Unlock at [https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-enable-network-unlock](https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-enable-network-unlock" \t "_blank).

### Recovering BitLocker-Encrypted Data

When BitLocker Drive Encryption is enabled, a recovery password is generated automatically. The recovery password is a random number that you can save to a USB drive or folder, display on the screen, or print. It is important to keep the key in a secure location because it can be used to access data on the BitLocker-encrypted volume.

Windows 10 also provides an option to configure a data recovery agent for BitLocker. Like a data recovery agent for EFS, a data recovery agent for BitLocker can access BitLocker-encrypted data even if a user forgets the PIN or password. In domain-based environments, this is configured by importing a certificate for a data recovery agent into Group Policy at Computer Configuration\Windows Settings\Security Settings\Public Key Policies.

In domain-based environments, you have the option to store the recovery password for BitLocker-encrypted drives in Active Directory. When this option is enabled, the recovery password is stored as an attribute of the computer object in Active Directory. You can also configure BitLocker to not allow encryption unless the recovery password is successfully stored in Active Directory. In a Group Policy object, enable Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista) in Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption.

The recovery password is required when the normal decryption process for BitLocker Drive Encryption is unable to function. The most common reasons that the recovery password is required are:

* Modified boot files—If one of the boot files on the system volume is modified, BitLocker Drive Encryption stops the system from starting because the operating system has experienced tampering.
* Lost encryption keys—If the TPM has a problem, and the encryption keys stored in it are lost or corrupted, the encrypted volume cannot be decrypted normally. The recovery password is also required if the encryption keys are stored on a USB drive that is lost or erased.
* Lost or forgotten startup PIN—If the requirement for a startup PIN is selected and the user forgets the startup PIN, the recovery password is required to access the encrypted data.

The recovery process is as follows:

1. Turn on the computer.
2. Enter the BitLocker Drive Encryption Recovery Console.
3. Provide the recovery password by inserting a USB key or typing it in.
4. The computer restarts and boots normally.

### Disabling BitLocker Drive Encryption

If you no longer need BitLocker Drive Encryption, you can turn it off or disable it. Turning off BitLocker Drive Encryption decrypts all the data on the hard drive and makes it readable again. After BitLocker Drive Encryption is turned off, the drive can be moved to another computer and read by other operating systems.

Disabling BitLocker Drive Encryption does not decrypt the files on the volume. Instead, BitLocker Drive Encryption stores the FVEK as a clear key, which effectively removes the data protection associated with using BitLocker Drive Encryption. A clear key is one that is not encrypted or protected in any way. Disabling BitLocker Drive Encryption is not sufficient for other operating systems to read the BitLocker-encrypted data.

**Activity 6-10**

### Recovering a BitLocker-Encrypted Drive

**Time Required:**20 minutes

**Objective:**Recover a BitLocker-encrypted drive

**Description:**BitLocker Drive Encryption protects your data from anyone who might steal your computer; however, it can also render your data unavailable if the keys in the TPM are corrupted or you forget a startup password. In this activity, you recover the C: drive of a computer after forgetting the password.

1. 1

If necessary, start your computer and sign in.

1. 2

On the taskbar, click **File Explorer**, and below Recent files, double-click **BitLocker**.

1. 3

Read the contents of BitLocker.pdf. This content should be stored in a safe location that is not on the encrypted drive.

1. 4

Print a copy of BitLocker.pdf so that you can use it later in this activity to recover the drive. If you do not have access to a printer, copy the recovery key on a piece of paper. If you are working with a virtual machine, you can take a screenshot.

1. 5

Restart your computer.

1. 6

On the BitLocker screen, press **Esc** to enter BitLocker Recovery.

1. 7

On the BitLocker recovery screen, in the Enter the recovery key for this drive box, type the recovery key from BitLocker.pdf and then press **Enter**.

1. 8

Sign in to your computer.

1. 9

Click the **Start** button and then click **Settings**.

1. 10

In the Find a setting box, type **BitLocker** and then click **Manage BitLocker**.

1. 11

For the C: drive, click **Suspend protection**.

1. 12

In the BitLocker Drive Encryption dialog box, click **Yes**.

1. 13

Restart your computer and then sign in. Notice that you did not need to enter the password even though the drive is still encrypted.

1. 14

Click the **Start** button and then click **Settings**.

1. 15

In the Find a setting box, type **BitLocker** and then click **Manage BitLocker**.

1. 16

For the C: drive, click **Turn off BitLocker**.

1. 17

In the BitLocker Drive Encryption dialog box, click **Turn off BitLocker**.

1. 18

Close all open windows.

### BitLocker To Go

Windows 10 includes [**BitLocker To Go**](javascript://) as a method for protecting data on removable storage, such as USB drives. When you choose to enable removable storage for BitLocker To Go, you are prompted for how the storage will be unlocked. This process for unlocking the encryption keys is different for BitLocker To Go because you must be able to unlock the removable drive on multiple computers.

The options for unlocking removable storage are:

* Use a password to unlock the drive—When this option is selected, you enter a password that protects the encryption key for the data. When you take the removable storage to another computer, you are prompted for the password before getting access to the data on the removable drive.
* Use my smart card to unlock the drive—When this option is selected, you identify a smart card that will protect the encryption key for the data. When you take the removable storage to another computer, you must provide the smart card and the PIN for the smart card before getting access to the data on the removable drive. This method is the most secure, but the second computer must have a smart card reader, which is not common.

When you enable BitLocker To Go for a removable drive, you are prompted to save or print the recovery key, just as you are when you enable BitLocker for a fixed hard drive.

BitLocker To Go can be enabled for a device only when using Windows 10 Pro, Enterprise, or Education editions, although any edition of Windows 10 can view or modify data encrypted by BitLocker To Go. This means you can configure Windows To Go on a USB drive at work with Windows 10 Pro and use the encrypted data on your home computer running Windows 10 Home.

BitLocker To Go can be configured to automatically unlock a protected drive when it is connected to a specific computer when a particular user is signed in. This simplifies access to the drive when used in a trusted environment, but still prompts for a password when the protected drive is used in another location.

Many BitLocker and BitLocker To Go settings can be managed through Group Policy. For example, you can force all removable storage to be encrypted with BitLocker To Go.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**6-6**Windows Update

Scheduling automatic updates with [**Windows Update**](javascript://) is the most important security precaution you can take with Windows 10. The vast majority of exploits used by viruses, worms, and other malware are addressed by updates available from Microsoft. Often, computers are vulnerable to many of these threats only because the necessary updates have not been applied.

When a Windows security flaw is found by a security company or an ethical hacker, the flaw is reported to Microsoft. The person or company that found the flaw does not release their findings until Microsoft has created and released an update to fix the problem, which typically takes a few weeks or months.

After the update has been released, the person or company that found the flaw releases detailed information about the flaw. Microsoft releases the information on their website, as well. Malware creators then begin to create software that takes advantage of the flaw. Computers that do not apply patches in a timely way are still vulnerable to malware using the flaw. In contrast, computers that are updated regularly are not vulnerable.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-6aServicing Branches

Microsoft has fundamentally changed the update process in Windows 10. In previous versions of Windows, Microsoft released security updates for varying service pack levels, which made it difficult for Microsoft to test and verify compatibility. Microsoft now releases updates for specific builds of Windows 10 only for a specified period of time. Before the end of the support period, a new build is released and computers upgrade to the new build, which then gets new updates until the next build is released.

The three distinct servicing branches are:

* Windows Insider Preview Branch—This branch is updated at irregular intervals depending on when Microsoft has a new preview ready for release. Consider this branch beta software. Windows Insider Preview should be used only on test computers if you want an early look at new features. You need to join the Windows Insider Program to use this service branch.
* Semi-Annual Channel—Approximately every six months, Microsoft releases [**feature updates**](javascript://) that include new functionality in Windows 10. These releases have a version number that identifies when it was released. For example, version 1909 was released in September of 2019.
* Long Term Servicing Branch—This branch is a specific edition of Windows 10 that does not receive feature updates. Windows Updates are provided for Long Term Servicing Branch for 10 years. This is meant for controlled environments, such as equipment controllers, where changes cannot be tolerated.

Microsoft provides monthly updates that include fixes and security updates for the Semi-Annual Channel releases for 18 months. This allows organizations to keep Windows 10 in a supported state if they choose to skip a feature update to avoid a change in their environment. For Enterprise and Education editions of Windows 10, updates are provided for 30 months, which provides additional time for testing and controlled deployment.

**Tip**

Feature updates for early versions of Windows 10 took 30–45 minutes to install on many devices. Starting with version 1909, feature updates can be incremental and take only a few minutes to install.

Go to pg.

[**help**](javascript://)

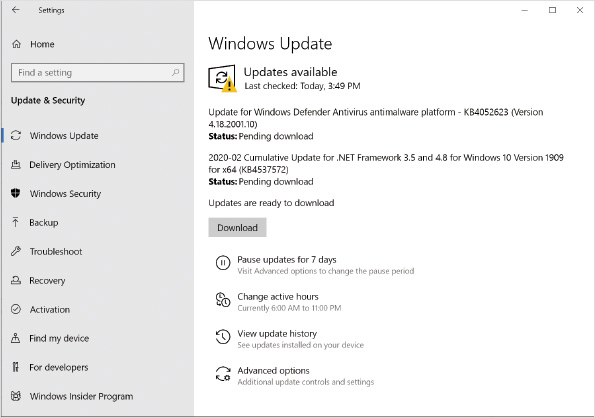
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-6bControlling Windows Updates

The default configuration of Windows Update uses the Semi-Annual Channel and installs updates automatically when they are available. When updates are available, they are listed in Windows Update, as shown in [Figure 6-24](javascript://). You have the option to check for updates immediately, but typically this is not required. You also have the option to view your update history there. Viewing the update history can be useful when trying to identify if a recent update introduced instability.

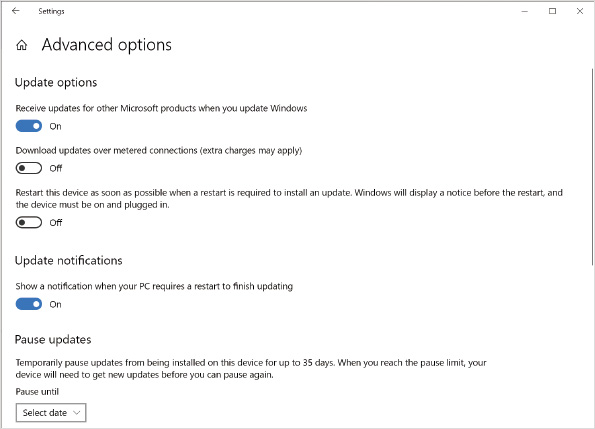
**Figure 6-24Windows Update Screen**



Enlarge Image

In the settings for Windows Update, you can view the active hours defined for your computer. When you define active hours, your computer will not be automatically restarted during those active hours. You can change these active hours to match when you use the device so that it doesn’t restart when you want to use it. You can also turn on the Automatically adjust active hours for this device based on activity option that automatically sets the active hours based on when the device is typically used. Other advanced options are shown in [Figure 6-25](javascript://).

**Figure 6-25Advanced Options for Windows Update**



Enlarge Image

In the Advanced options, you can configure additional settings, such as:

* Receive updates for other Microsoft products when you update Windows—In most cases, you will want to leave this option on to get updates for a wide variety of Microsoft products. Malware is capable of taking advantage of flaws in multiple products, not just the operating system.
* Download updates over metered connections—This option is off by default and should generally remain off. On metered connections you usually have a limited amount of data and usage, and additional costs might be incurred. For example, you probably don’t want to download large windows updates when your laptop is tethered to your mobile phone for data.
* Restart this device as soon as possible when a restart is required to install an update—This option is off by default and should generally remain off. When you enable this option, your computer will restart after an update is installed, even if it is during active hours. Windows displays a notice that the restart will happen. If your device is on battery power, a restart is not performed.
* Show a notification when your PC requires a restart to finish updating—When this option is on, a notification is displayed in the system tray to indicate that a system restart is required after an update is installed. This gives users an option to restart during active hours if they want to. This option is on by default.
* Pause updates—You can pause updates for up to 35 days by selecting an allowed date. When the pause is completed, pending updates must be installed before you can pause again. This option is typically used when you have identified an update that you think will cause problems on your computer.

### Windows Update for Business

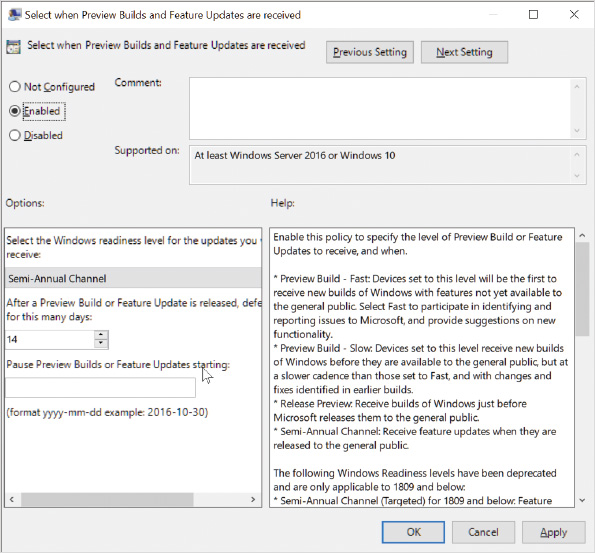
To allow more detailed control of update delivery to computers in a business environment, you can use [**Windows Update for Business**](javascript://). Windows Update for Business allows you to defer feature updates and quality updates by up to 365 days. By default, each update type is deferred for 7 days. Delaying update installation provides additional time to determine if new updates cause any problems with your computers. Windows Update for Business is not available for Windows 10 Home.

The purpose of Windows Update for Business is to create separate groups of computers that perform updates at different times. The first group is the testers in the organization. If the testers group finds a problem, you can pause updates to everyone else until the issue is resolved.

In a domain-based network, you can apply Windows Update for Business settings by using Group Policy. You can create multiple configurations to apply different settings to different sets of computers. The Windows Update for Business Group Policy settings are located in Computer Configuration\Administrative Templates\Windows Components\Windows Update\Windows Update for Business. The available settings are:

* Manage preview builds—Use this setting to allow or disallow Windows Insider versions of Windows 10.
* Select when Preview Builds and Feature Updates are received—Use this setting, shown in [Figure 6-26](javascript://), to define how long Feature Updates are delayed. You can also pause Feature Updates until a specified date.

**Figure 6-26Windows Update for Business Group Policy setting**



Enlarge Image

* Select when Quality Updates are received—Use this setting to define how long Quality Updates are delayed. You can also pause Quality Updates until a specified date.

The standard Windows Update process can also be modified to use Windows Server Update Services (WSUS). WSUS provides greater control over the update process by allowing individual updates and upgrades to be approved for delivery to groups of computers. When WSUS is used, the Defer Upgrades and Updates setting is not used.

### Delivery Optimization

Delivery optimization allows Windows Updates to be delivered among Windows 10 devices rather than all devices downloading the updates from Microsoft. This can reduce network data consumption when Internet speed is limited or data caps are in place.

By default, this setting is on, but it is limited to computers on the local network. You have the option to allow sharing with computers on the Internet also, but most organizations won’t allow this due to security concerns.

An activity monitor for delivery optimization allows you to see download and upload statistics. You can verify how much data has been sent and received from Microsoft, computers on the local network, and computers on the Internet.

If you think that delivery optimization for Windows updates is causing network problems, rather than disabling it, you can implement bandwidth limits for uploading and downloading updates. These are configured in the advanced options within delivery optimization.

Go to pg.

[**help**](javascript://)

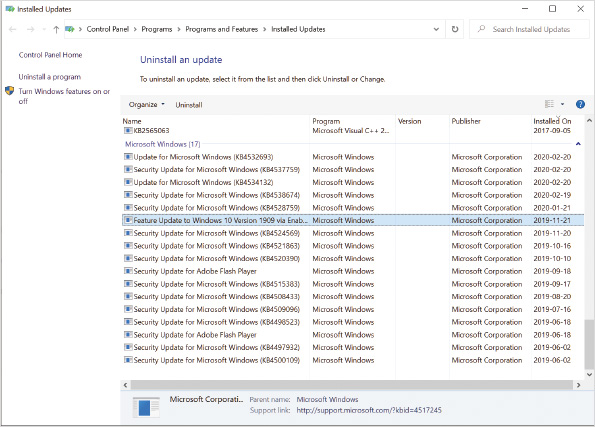
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-6cRemoving Windows Updates

If you believe that a Windows update is causing a problem on your computer, you can remove it. The simplest way to remove an update is through the graphical interface, shown in [Figure 6-27](javascript://), which you can access through Control Panel or the update history in Settings. The Uninstall an update screen categorizes updates by product, such as Microsoft Windows or Adobe Acrobat Reader. To remove an update, you select the update and then click Uninstall.

**Figure 6-27Uninstall an Update Screen**



Enlarge Image

In a larger environment, you might want to script a solution for removing an update from computers. This is faster than manually visiting many computers. To do this, you can use the Windows Update Standalone Installer (wusa.exe). This tool can install or remove Windows Updates from the command prompt or a Windows PowerShell prompt; however, you need to specify the KB number of the update.

You can identify the KB number of an update from the title of the update in update history or on the Uninstall an update screen. At a Windows PowerShell prompt, you can use the Get-HotFix cmdlet. You can also use the command wmic qfe list at a command prompt or in the Windows PowerShell window.

**Activity 6-11**

### Protecting Your Computer by Using Windows Update

**Time Required:**5 minutes

**Objective:**Protect your computer by configuring Windows Update

**Description:**One of the simplest methods for protecting your computer from malware that uses known exploits is regular installation of patches and security updates. For better stability in a business environment, you can configure Windows Update for Business to delay Windows Updates for a few days. In this activity, you view available options and configure Windows Update.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button and then click **Settings**.

1. 3

In the Settings window, click **Update & Security**. This screen indicates whether Windows 10 is up to date or not.

1. 4

Click **Change active hours** and read the available options.

1. 5

On the Change active hours screen, click the **Back** button in the upper-left corner.

1. 6

Click **Advanced options** and read all the available options.

1. 7

Scroll down to the Choose when updates are installed area, specify **30** days for feature updates, and then specify **5** days for quality updates.

1. 8

Click **Delivery Optimization** and read the available options.

1. 9

Click **Advanced options**, read the available options, and then click the **Back** button.

1. 10

Click **Activity monitor** and review the statistics.

1. 11

Click the **Back** button three times or until you are on the Windows Update screen and then click **View update history**.

1. 12

Scroll down and read the list of updates. Notice that categories for Feature Updates, Quality Updates, Driver Updates, Definition Updates, and Other Updates are listed. If your installation of Windows 10 is new, no updates might be installed.

1. 13

At the top of the View update history screen, click **Uninstall updates**. You can remove updates from this window.

1. 14

Close all open windows.

1. 15

Click the **Start** button, type **PowerShell**, and then click **Windows PowerShell**.

1. 16

At the Windows PowerShell prompt, type **Get-HotFix** and then press **Enter**. Read the results of this command.

1. 17

At the Windows PowerShell prompt, type **wmic qfe list** and then press **Enter**. Read the results of this command.

1. 18

At the Windows PowerShell prompt, type **wusa.exe /?** and then press **Enter**.

1. 19

In the Windows Update Standalone Installer dialog box, read the help information and then click **OK**.

1. 20

Close the Windows PowerShell window.

Go to pg.

[**help**](javascript://)

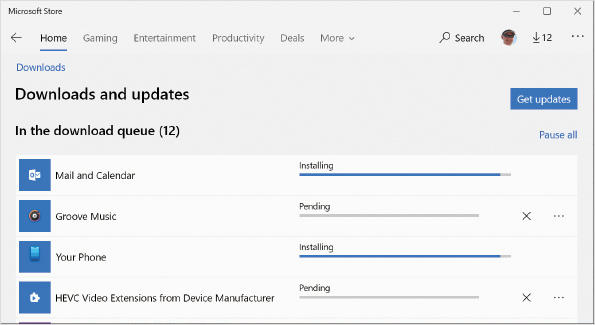
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 6-6dUpdating Microsoft Store Apps

Microsoft Store apps are not updated by using Windows Update. Windows Store apps are updated through the Microsoft Store. To access settings related to Microsoft Store app updates, click the Start button, start the Microsoft Store app, and then click the Downloads and updates icon in the upper-right corner. From the Downloads and updates screen, shown in [Figure 6-28](javascript://), you can check for updates, download all updates, or download specific updates.

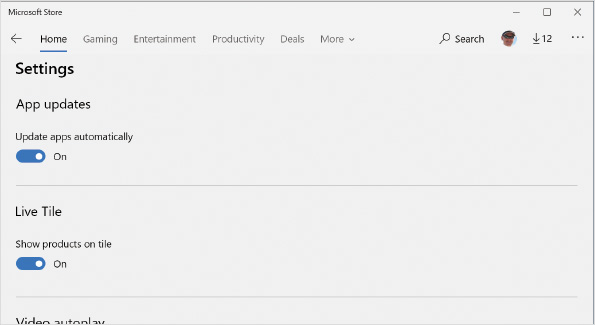
**Figure 6-28Windows Store Downloads and Updates**



Enlarge Image

If you select Settings from the menu in the upper-right corner, you can turn on or off automatic updates for Microsoft Store apps, as shown in [Figure 6-29](javascript://). Update apps automatically is on by default which is the preferred option in most scenarios.

**Figure 6-29Microsoft Store Settings**



Enlarge Image

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 6-7a**Summary**

* The Local Security Policy in Windows 10 is used to configure a wide variety of security settings. Account policies control password settings and account lockout settings. Local policies configure auditing, user rights, and other security options. Software restriction policies and AppLocker control what software is allowed to run on a computer. Other security policies configure Windows Defender Firewall and EFS certificates and encrypt network communication.
* Auditing is used to record specific operating system events to the security log. Event categories that can be configured are Account Logon, Account Management, Detailed Tracking, DS Access, Logon/Logoff, Object Access, Policy Change, Privilege Use, System, and Global Object Access.
* User Account Control (UAC) increases security by allowing users to sign in and perform their jobs with standard user accounts. UAC also limits administrators to standard user privileges until administrative privileges are required by using Admin Approval Mode.
* Windows 10 includes multiple anti-malware technologies. Windows Defender Antivirus monitors memory and the file system for malware with real-time, scheduled, and on-demand scanning. Windows Defender Smartscreen monitors content downloaded from the Internet. Device Security monitors and configures system-level anti-malware configuration settings, such as memory protection.
* Encrypting File System (EFS) protects individual files by encrypting them. Only the person who encrypted a file can decrypt it, unless that file has been properly shared. A recovery certificate can be used to decrypt files if the certificate is configured.
* BitLocker Drive Encryption is used to encrypt an entire volume. To use BitLocker Drive Encryption, the hard drive must contain at least two partitions. BitLocker Drive Encryption also protects the operating system from being modified. BitLocker To Go allows removable storage to be encrypted.
* Windows Update is used to ensure that updates are applied to Windows 10 as they are made available. Windows 10 uses the semiannual channel update of Windows 10 by default, but it can be configured to use Windows Insider Preview Branch. You can delay installation of updates by using Windows Update for Business.
* Microsoft Store apps are updated by the Microsoft Store instead of Windows Update. Microsoft Store apps are automatically updated by default.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 6-7b**Key Terms**

* [**Account Lockout Policy**](javascript://)
* [**AppLocker**](javascript://)
* [**asymmetric encryption algorithm**](javascript://)
* [**audit policy**](javascript://)
* [**auditing**](javascript://)
* [**BitLocker Drive Encryption**](javascript://)
* [**BitLocker Network Unlock**](javascript://)
* [**BitLocker To Go**](javascript://)
* [**controlled folder access**](javascript://)
* [**Encrypting File System (EFS)**](javascript://)
* [**feature updates**](javascript://)
* [**Full Volume Encryption Key (FVEK)**](javascript://)
* [**hashing algorithms**](javascript://)
* [**Local Security Policy**](javascript://)
* [**malware**](javascript://)
* [**password policy**](javascript://)
* [**Software Restriction Policies**](javascript://)
* [**symmetric encryption algorithm**](javascript://)
* [**User Account Control (UAC)**](javascript://)
* [**Volume Master Key (VMK)**](javascript://)
* [**Windows Defender Antivirus**](javascript://)
* [**Windows Defender Application Guard**](javascript://)
* [**Windows Defender Smartscreen**](javascript://)
* [**Windows Update**](javascript://)
* [**Windows Update for Business**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 6-7c**Review Questions**

1. Which security feature in Windows 10 prevents malware by limiting user privilege levels?
   1. Windows Defender Antivirus
   2. User Account Control (UAC)
   3. Microsoft Security Essentials
   4. Service SIDs
2. Which of the following passwords meet complexity requirements? (Choose all that apply.)
   1. passw0rd$
   2. ##$$@@
   3. ake1vyue
   4. a1batr0$$
   5. A%5j
3. Which password policy setting should you use to prevent users from reusing their passwords too quickly?
   1. Maximum password age
   2. Minimum password age
   3. Minimum password length
   4. Password must meet complexity requirements
   5. Store passwords using reversible encryption
4. Which Account Lockout Policy setting is used to configure the time frame in which incorrect logon attempts must be conducted before an account is locked out?
   1. Account lockout duration
   2. Account lockout threshold
   3. Reset account lockout counter after
   4. Account lockout release period
5. The  local policy controls the tasks users are allowed to perform.
6. Which type of AppLocker rule condition can uniquely identify any file regardless of its location?
   1. Publisher
   2. Hash
   3. Network zone
   4. Path
7. You must configure a certificate authority on your network to use EFS. True or False?
8. How would you create AppLocker rules if you wanted to avoid updating the rules when most software is already installed?
   1. Manually create rules for each application.
   2. Automatically generate rules.
   3. Create default rules.
   4. Download rule templates.
9. Evaluating DLL files for software restrictions has a minimal impact on performance because of caching. True or False?
10. To which event log are audit events written?
    1. Application
    2. Security
    3. System
    4. Audit
    5. Advanced Audit
11. A(n)  is used to describe the structure of an application and trigger UAC when required.
12. What are you disabling when you configure UAC to not dim the desktop?
    1. Admin Approval Mode
    2. file and registry virtualization
    3. user-initiated prompts
    4. secure desktop
13. Which type of encryption is the fastest, strongest, and best suited to encrypting large amounts of information?
    1. symmetric
    2. 128-bit
    3. asymmetric
    4. hash
    5. public key
14. To encrypt a file by using EFS, the file must be stored on an NTFS-formatted partition. True or False?
15. How can you recover EFS-encrypted files if the user profile holding the digital certificate is accidentally deleted? (Choose all that apply.)
    1. Restore the file from backup.
    2. Restore the user certificate from a backup copy.
    3. Another user that has access to open the file can decrypt it.
    4. Decrypt the file by using the recovery certificate.
    5. Decrypt the file by using the EFS recovery snap-in.
16. Which of the following is not true about BitLocker Drive Encryption?
    1. BitLocker Drive Encryption requires at least two disk partitions.
    2. BitLocker Drive Encryption is designed to be used with a TPM.
    3. Two encryption keys are used to protect data.
    4. Data is still encrypted when BitLocker Drive Encryption is disabled.
    5. You must use a USB drive to store the startup PIN.
17. BitLocker Drive Encryption is user aware and can be used to protect individual files on a shared computer. True or False?
18. How long are quality updates provided for a specific version of Windows 10 Pro?
    1. 6 months
    2. 12 months
    3. 18 months
    4. 24 months
    5. 30 months
19. Which command-line tool can be used to remove Windows Updates?
    1. Remove-HotFix
    2. wusa.exe
    3. wmic qfe
    4. wuauclt.exe
    5. Updates can be removed only from the graphical interface.
20. Which setting should you configure to minimize data usage from downloading Windows Updates each time you travel and tether your laptop to your mobile phone for data connectivity?
    1. Pause updates for 7 days.
    2. Delay installation of feature updates for 14 days in Windows Update for Business.
    3. Limit bandwidth utilization in delivery optimization.
    4. Turn off Download updates over metered connections.
    5. Disable the Windows Update service.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 6-7d**Case Projects**

**Case Project 6-1**

### Virus Prevention

Buddy’s Machine Shop’s computers have been infected with a virus for the second time in six months. Several computers cannot run antivirus software with real-time scanning (even Windows Defender Antivirus) because it interferes with specialized software used to fabricate machine parts from blocks of metal. What can you do to mitigate the risk of viruses infecting the computers?

**Case Project 6-2**

### Controlling Windows Updates

Angela’s Printing Services has 50 Windows computers that are used for various purposes, such as graphical design and general office productivity. All computers are running Windows 10 Pro with the default settings for Windows Update. Last month an update caused an unexpected problem with critical printing software. How should Windows Update be configured to minimize the risk of problems from future updates?

**Case Project 6-3**

### Data Encryption

The salespeople at Hyperactive Media sales all use laptop computers so that they can have easy access to important data on the road. The salespeople regularly take customer lists and other sensitive company information with them; unfortunately, a laptop occasionally is lost or stolen. Which data encryption features in Windows 10 can prevent hard drive data from being used after a laptop is stolen? Which features would you implement and why?

**Case Project 6-4**

### Enterprise Virus Protection

You are the new system administrator for Precision Accounting Services, which has 45 computers on its network running Windows Defender Antivirus. All the computers have access to the Internet and update antivirus definitions as required.

Last week, several users received an email with a link to an executable file stored on a cloud-based file sharing service. One user was tricked into downloading and running the malware. This malware was detected by Windows Defender Antivirus, but it couldn’t be removed from memory while running. The user didn’t understand the malware detection messages and didn’t inform you. This created a security risk because the malware ran for an extended period and began accessing network file shares. How can you prevent this in the future?

Go to pg.

[**help**](javascript://)