Application Opened

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

**Chapter**

**16**

**Securing and Sharing Windows Resources**

* [Chapter Introduction](javascript://)
* **16-1**[Securing a Windows Personal Computer](javascript://)
  + **16-1a**[Using Windows to Authenticate Users](javascript://)
  + **16-1b**[Using BIOS/UEFI Passwords to Authenticate Users](javascript://)
  + **16-1c**[Securing Internet Explorer](javascript://)
  + **16-1d**[File and Folder Encryption](javascript://)
  + **16-1e**[BitLocker Encryption](javascript://)
  + **16-1f**[Windows Firewall Settings](javascript://)
* **16-2**[Controlling Access to Folders and Files](javascript://)
  + **16-2a**[Classifying User Accounts and User Groups](javascript://)
  + **16-2b**[Methods to Assign Permissions to Folders and Files](javascript://)
  + **16-2c**[How to Share Folders and Files](javascript://)
  + **16-2d**[How to Map a Network Drive or Network Printer](javascript://)
  + **16-2e**[Sync Center and Offline Files](javascript://)
  + **16-2f**[Hidden Network Resources and Administrative Shares](javascript://)
* **16-3**[Using Active Directory Domain Services](javascript://)
  + **16-3a**[Creating and Managing User Accounts in AD](javascript://)
  + **16-3b**[Group Policy Objects](javascript://)
* **16-4**[Chapter Review](javascript://)
  + **16-4a**[Chapter Summary](javascript://)
  + **16-4b**[Key Terms](javascript://)
  + **16-4c**[Thinking Critically](javascript://)
  + **16-4d**[Hands-On Projects](javascript://)
  + **16-4e**[Real Problems, Real Solutions](javascript://)
  + **16-4f**[Exam Tips](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 completing this chapter, you will be able to:

* Secure a Windows personal computer using Windows tools on the local computer
* Share and secure files and folders on a network
* Support network resources using Active Directory

In this chapter, you learn about some tools and techniques to secure the resources on a personal computer, small network, and Windows domain. Later in your career as a support technician, you can build on the skills learned in this chapter to implement even more security, such as controlling how Windows stores its passwords. However, keep in mind that even the best security will eventually fail. As a thief once said, “Locks are for honest people,” and a thief will eventually find a way to break through. Security experts tell us that security measures basically make it more difficult and time consuming for a thief to break through so that the thief gets discouraged and moves on to easier targets.

This chapter also explains how to lock down a personal computer from unauthorized access. Because security is always a huge concern when dealing with networks, you learn how to share resources on the network while protecting them from people who should not have access. Finally, you’ll learn how to use Active Directory to manage users and resources on a network.

Go to pg.

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

Application Opened

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

**16-1**Securing a Windows Personal Computer

**A+ Core 2**

* 1.4

Given a scenario, use appropriate Microsoft command line tools.

* 1.5

Given a scenario, use Microsoft operating system features and tools.

* 1.6

Given a scenario, use Microsoft Windows Control Panel utilities.

* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

* 2.2

Explain logical security concepts.

* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

* 2.7

Given a scenario, implement security best practices to secure a workstation.

When you have a choice in the security measures that you use, keep in mind two goals, which are sometimes in conflict. One goal is to protect resources, and the other goal is not to interfere with the functions of the system. A computer or network can be so protected that no one can use it, or so accessible that anyone can do whatever they want with it. The trick is to provide enough security to protect resources while still allowing users to work unhindered (see [Figure 16-1](javascript://)). Also, too much security can sometimes force workers to find insecure alternatives. For example, if you require users to change their passwords weekly, more of them might start writing their passwords down to help remember them.

**Figure 16-1**

Security measures should protect resources without hindering how users work



© Source: [iStock.com](http://istock.com/" \t "_blank)/ojogabonitoo

**Notes**

The best protection against attacks is layered protection. If one security method fails, the next might stop an attacker. When securing a workstation, use as many layers of protection as you reasonably can that are justified by the value of the resources you are protecting. These layers of defense are collectively called [**defense in depth**](javascript://).

Go to pg.

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

Application Opened

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

## 16-1aUsing Windows to Authenticate Users

**A+ Core 2**

* 1.4

Given a scenario, use appropriate Microsoft command line tools.

* 1.5

Given a scenario, use Microsoft operating system features and tools.

* 1.6

Given a scenario, use Microsoft Windows Control Panel utilities.

* 2.2

Explain logical security concepts.

* 2.5

Compare and contrast social engineering, threats, and vulnerabilities.

* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

* 2.7

Given a scenario, implement security best practices to secure a workstation.

Access to computer resources is controlled by authenticating and authorizing a user or process. A user is authenticated when he proves he is who he says he is. When a computer is on a Windows domain, Active Directory (AD) is responsible for authentication. For a peer-to-peer network, authentication must happen at the local computer. Normally, Windows authenticates a user with a Windows password.

As an administrator, when you first create an account, be sure to assign it a password. It’s best to give the user the ability to change the password at any time. In this part of the chapter, you learn how to create strong passwords and how to use Local Group Policy and Local Security Policy to control how users can authenticate to Windows.

### Create Strong Passwords

A password needs to be a [**strong password**](javascript://), which means it should not be easy to guess either by people or by computer programs using various methods, including a simple [**brute force attack**](javascript://), which tries every single combination of characters until it discovers your password.

A strong password, such as y\*3Q1693pEWJaTz1!, meets all of the following criteria:

* Use 16 or more characters, which is the best protection against a password attack.
* Combine uppercase and lowercase letters, numbers, and symbols.
* Use at least one symbol in your password.
* Don’t use consecutive letters or numbers, such as “abcdefg” or “12345.”
* Don’t use adjacent keys on your keyboard, such as “qwerty.”
* Don’t use your sign-in name in the password.
* Don’t use words in any language. Don’t even use numbers or symbols for letters (as in “p@ssw0rd”) because programs can easily guess those as well.
* Don’t use the same password for more than one system.

Studies have proven that the most secure criterion of those listed above is the length of the password. Passwords of 16 characters or more that use letters, numbers, and symbols are the most difficult to crack.

**Notes**

How secure is a password? Go to [howsecureismypassword.net](http://howsecureismypassword.net/" \t "_blank) and find out how long it will take a computer to crack the password.

In some situations, a blank Windows password might be more secure than an easy-to-guess password such as “1234.” That’s because you cannot authenticate to a Windows computer from a remote computer unless the user account has a password. A criminal might be able to guess an easy password and authenticate remotely. For this reason, if a computer is always in a protected room such as a home office and the user doesn’t intend to access it remotely, she might choose not to use a password. However, if the user travels with a laptop, always recommend that the user create a strong password.

Although it’s not recommended you write your password down, if you do write it down, keep it in as safe a place as you would the data you are protecting. Don’t send your passwords over email or chat. Change your passwords regularly, and don’t type them on a public computer. For example, computers in hotel lobbies or Internet cafés should only be used for web browsing—not for signing in to your email account or online banking account. These computers might be running keystroke-logging software put there by criminals to record each keystroke. Several years ago, while on vacation in a foreign country, I entered credit card information on a computer in a hotel lobby. Months later, I was still protesting $2 or $3 charges to my credit card from that country. Trust me. Don’t do it—I speak from experience.

**Notes**

Rather than writing down passwords, consider storing your passwords with a password manager app such as Dashlane ([dashlane.com](http://dashlane.com/" \t "_blank)), Sticky Password ([stickypassword.com](http://stickypassword.com/" \t "_blank)), or LastPass ([lastpass.com](http://lastpass.com/" \t "_blank)). These apps can keep your passwords in the cloud or on your own device, and the passwords they create are longer and stronger than those you would be able to memorize.

Next, let’s see how Local Group Policy and Local Security Policy tools can be used to enforce security best practices on a workstation.

### Local Group Policy and Local Security Policy Editors

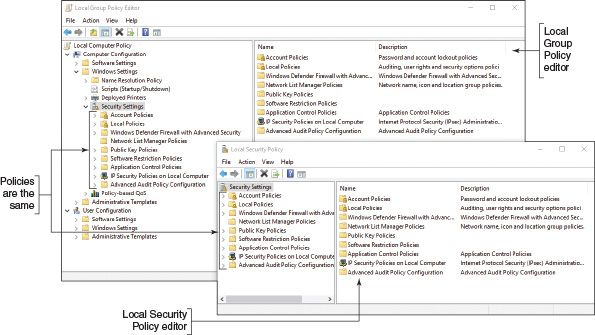
You need to be aware of three tools for policies that control what users and computers can do with a system or network:

* **Group Policy** works in Active Directory on a Windows domain to control the privileges of computers and users on the domain. You learn more about Group Policy and Active Directory later in this chapter.
* **Local Group Policy** (gpedit.msc) contains a subset of policies in Group Policy; this subset applies only to the local computer or local user.
* [**Local Security Policy**](javascript://) (secpol.msc) contains a subset of policies in Local Group Policy, which apply only to the local computer’s Windows security settings. Local Security Policy is an Administrative Tools snap-in in Control Panel.

The Local Group Policy and Local Security Policy editors are available with business and professional editions of Windows. [Figure 16-2](javascript://) shows the Local Group Policy Editor window on the left and the Local Security Policy window on the right. Notice that the Local Group Policy editor contains two major categories of policies: Computer Configuration and User Configuration. The list of policy groups selected are for the computer configuration for Windows security settings. Compare this list with the one in the Local Security Policy window; they are the same list of policies. In short, when you are working with the computer configuration in the Windows security settings group of the Local Group Policy editor, know you are working with the same group of policies you can edit when using the Local Security Policy editor.

**Figure 16-2**

The Local Security Policy editor allows you to edit a subset of policies available in the Local Group Policy editor



Enlarge Image

Now let’s see how you can use the Local Group Policy editor to secure a workstation. For example, you can set policies to require all users to have passwords. Once you have enabled a policy, a standard user of the workstation would be required to comply and would not be able to change the policy.

**Applying Concepts**

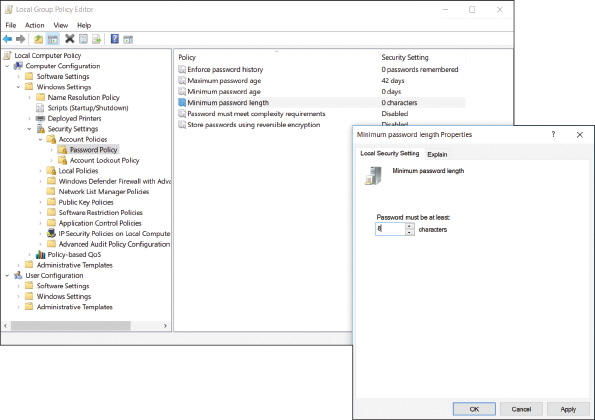
### Applying Local Security Policies

Follow these steps to set a few important policies to secure a workstation:

1. Sign in to Windows using an administrator account on a system that uses Windows 10 Pro or Enterprise, Windows 8/8.1 Professional or Enterprise, or Windows 7 Professional, Ultimate, or Enterprise.
2. To start Local Group Policy, enter the **gpedit.msc** command in the Windows 10/7 search box or the Windows 8 Run box. The Local Group Policy Editor console opens.
3. To change a policy, first use the left pane to drill down into the appropriate policy group and then use the right pane to view and edit a policy. Here are important policies you can use to secure a workstation:
   * **Require user passwords and password expiration.** To require that all user accounts have passwords, drill down to the **Computer Configuration**, **Windows Settings**, **Security Settings**, **Account Policies**, **Password Policy** group (see the left side of [Figure 16-3](javascript://)). Use the **Minimum password length** policy and set the minimum length to at least eight characters (see the right side of [Figure 16-3](javascript://)). Additionally, reduce the password expiration time frame so users must create new passwords frequently. Use the **Maximum password age** policy to require users to reset their password every 60 days. (The best practice is to set the Maximum password age in the range of 30 to 90 days.)

**Figure 16-3**

Require that each user account have a password by setting the minimum password length policy



Enlarge Image

* + **Screen lock timeout.** Windows can monitor for inactivity and run the screen saver after a set amount of time, locking the session. This prevents another person from continuing a Windows session after the user has stepped away from the computer. Drill down to the **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies**, **Security Options** group. Use the **Interactive logon: Machine inactivity limit** policy to set the number of seconds of inactivity before the screen saver runs and locks the workstation until a user signs in.
  + **Set failed logon restrictions.** Windows can be configured to lock a user account if too many incorrect logons are attempted. Drill down to the **Computer Configuration**, **Windows Settings**, **Security Settings**, **Account Policies**, **Account Lockout Policy** group. Use the **Account lockout threshold** policy to set the number of invalid logon attempts. When the number is exceeded, the account will be locked.

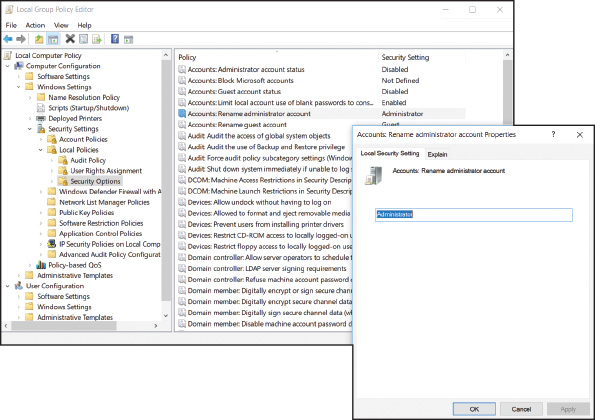
**Notes**

The Properties box for many policies offers the Explain tab. Use this tab to read more about a policy and how it works.

* + **Disable the Guest account.** For best security, the Guest account should stay disabled; you don’t want a user to accidentally enable it. To set a policy to disable the Guest account, first use the left pane to navigate to the **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies**, **Security Options** group. In the Security Options group, right-click **Accounts: Guest account status**, and select **Properties**. Change the status to **Disabled** and click **OK**.
  + **Change default user names.** A hacker is less likely to hack into the built-in Administrator account or Guest account if you change the names of these default accounts. To change the name of the Administrator account, drill down to the **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies, Security Options** group (see the left side of [Figure 16-4](javascript://)). In the right pane, double-click **Accounts: Rename administrator account**. In the Properties box for this policy (see the right side of [Figure 16-4](javascript://)), change the name and click **OK**. To change the name of the Guest account, use the policy **Accounts: Rename guest account**.

**Figure 16-4**

Use Group Policy to rename a default user account



Enlarge Image

**Notes**

The Administrator account is a built-in account that you might need in an emergency when other user accounts fail. Be sure to create a password for this account. One way to do that is to open an elevated command prompt window and enter the following command:

* + - 

For added security, open the Computer Management console and change the name of the Administrator account. Because this account and password are extremely valuable and not used very often, don’t trust your memory—keep the user account name and password in a protected and secure place.

* + **Audit logon failures.** Group Policy offers several auditing policies that monitor and log security events. You can then review these Security logs using Event Viewer. For example, to set an audit policy to monitor a failed logon event, drill down to the **Computer Configuration**, **Windows Settings**, **Security Settings**, **Local Policies**, **Audit Policy** group. Use the **Audit logon events** policy. You can audit logon successes and failures. To keep the log from getting too big, you can select **Failure** to log only these events.

All the previous policies are also found in the Local Security Policy console. The following policies are available only in Local Group Policy:

* + **Logon time restrictions.** In many cases, users should only be allowed access to a workstation during specific hours, such as during office hours. The schedule for a user’s or group’s logon hours is set through Active Directory on the domain. When logon hours set by Active Directory have expired, individual workstations can be configured to disconnect, lock, or log off the user, or to allow the user to continue the current session. To configure what happens when a user’s logon hours have expired, drill down to the **User Configuration**, **Administrative Templates**, **Windows Components**, **Windows Logon Options** group. Double-click **Set action to take when logon hours expire**. Select **Enabled** and then choose Lock, Disconnect, or Logoff. If the policy is not enabled, the user’s session will continue, but the user will not be able to log on outside of the assigned logon hours once the current session has been terminated.
  + **Disable Microsoft account resources.** Recall that a Microsoft account is a single sign-on (SSO) account, which means it provides authentication to multiple services and resources. When a user signs in to a Windows 10/8 computer with a Microsoft account, she has access to online resources such as OneDrive and OneNote and can sync settings on the computer with other computers that use the same Microsoft account. Settings include Start screen tiles, desktop personalization, installed apps and app settings, web browser favorites, and passwords to apps, websites, and networks.

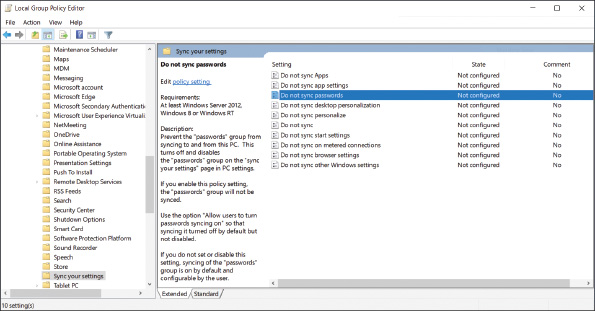
**Notes**

To see and edit the sync settings available for a Microsoft account, open the Windows 10 **Settings** app, click the **Accounts** group, and select **Sync your settings** in the left pane. In Windows 8, open the charms bar, click **Settings**, click **Change PC settings**, click **OneDrive**, and click **Sync settings**.

Depending on your company’s policy, you might need to restrict access to online resources and sync settings that are linked to a user’s Microsoft account. To disable OneDrive, for example, drill down to the **Computer Configuration**, **Administrative Templates**, **Windows Components**, **OneDrive** group. Enable the **Prevent the usage of OneDrive for file storage** policy to prevent users and programs from accessing OneDrive. Additionally, in the **Windows Components** submenu, click the **Sync your settings** group and use these policies to disable syncing apps, app settings, passwords, and other Windows settings (see [Figure 16-5](javascript://)).

**Figure 16-5**

Restrict SSO authentication to online resources associated with a Microsoft account



Enlarge Image

* + **Disable AutoRun and AutoPlay.** When you attach a USB flash drive or external hard drive or insert a disc in the optical drive, Windows automatically accesses the storage media and then requests instructions for what to do next. Media files can be played automatically, which is called AutoPlay. Executable files can be run automatically, which is called AutoRun. You can disable both of these features to add yet another layer of security protection. To disable AutoPlay, drill down to the **Computer Configuration**, **Administrative Templates**, **Windows Components**, **AutoPlay Policies** group. Enable the **Turn off Autoplay** policy. To disable AutoRun, enable **Set the default behavior for AutoRun** and use the **Disabled** option.

1. When you finish setting your local security policies, close the Local Group Policy Editor console. To put your changes into effect, restart the system or open a command prompt window and enter the command **gpupdate /force**. The command might request that you restart the computer for all policies to take effect. The **[gpupdate](javascript://)** command refreshes local group policies as well as group policies set in Active Directory on a Windows domain.

**A+ Exam Tip**

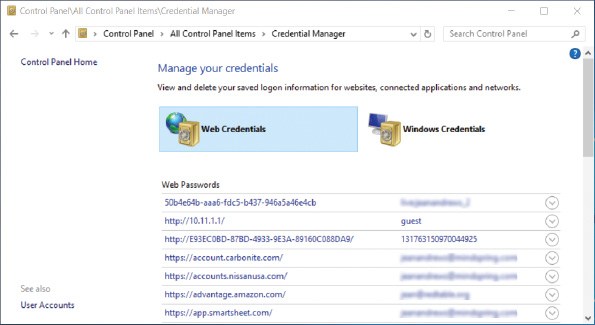
The A+ Core 2 exam expects you to know how to secure a workstation in a given scenario, including setting a strong password and configuring a workstation so that passwords will expire, knowing that a screen saver requires a password to unlock the workstation, that a logon time is restricted, and that the system locks when sign-in attempts have failed.

### Manage User Credentials

A user might need help managing the passwords and digital certificates stored on a Windows computer. To manage these user credentials, open the **Credential Manager** applet in Control Panel. The tool allows you to manage web credentials and Windows credentials (see [Figure 16-6](javascript://)). When you select a website under Web Credentials, you can edit or delete the user name and password to access the site. When you click **Windows Credentials**, you can edit and delete Windows user names, passwords, and digital certificates installed on the system. You can also use this window to install a new digital certificate in Windows.

**Figure 16-6**

Manage passwords and digital certificates in Credential Manager



Enlarge Image

Go to pg.

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

Application Opened

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

## 16-1bUsing BIOS/UEFI Passwords to Authenticate Users

**A+ Core 2**

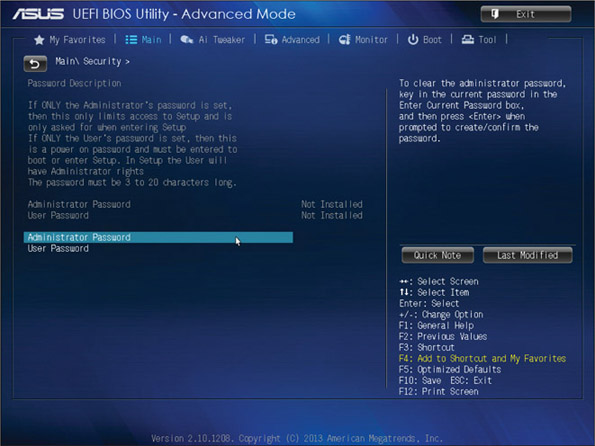
* 2.7

Given a scenario, implement security best practices to secure a workstation.

BIOS/UEFI firmware on the motherboard offers power-on passwords, which include an administrator or supervisor password (required to change BIOS/UEFI setup) and a user password (required to use the system or view BIOS/UEFI setup). Some firmware may also offer a drive lock password, which is required to access the hard drive. The drive lock password is stored on the hard drive so that it will still control access if the drive is removed from the computer and installed on another system. [Figure 16-7](javascript://) shows a BIOS/UEFI setup Security screen where you can set the Administrator and User passwords.

**Figure 16-7**

BIOS/UEFI passwords can control access to BIOS/UEFI setup and to boot the system



Enlarge Image

Source: American Megatrends, Inc.

Go to pg.

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

Application Opened

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

## 16-1cSecuring Internet Explorer

**A+ Core 2**

* 1.6

Given a scenario, use Microsoft Windows Control Panel utilities.

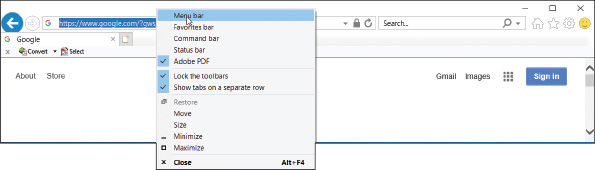
The [**Internet Options**](javascript://) dialog box can be used to secure Internet Explorer, a browser included with Windows 10/8/7. The latest release of Internet Explorer is version 11, although Windows 10 features a new browser called Microsoft Edge to eventually replace Internet Explorer. Current releases of Windows 10/8/7 come with Internet Explorer 11 installed; for an old installation of Windows, open Windows Update and find and install the Internet Explorer 11 update. You can also go to the [icrosoft.com](http://microsoft.com/" \t "_blank) website and follow links to download and install Internet Explorer 11.

Here are some tips about using Internet Explorer 11:

* **Menu bar.** To open the Internet Explorer menu bar, press the **Alt** key or right-click a blank area in the title bar and check **Menu bar** in the shortcut menu. Notice in [Figure 16-8](javascript://) that you can also add the command bar to the Internet Explorer window.

**Figure 16-8**

Access the shortcut menu from the title bar to control the Internet Explorer window



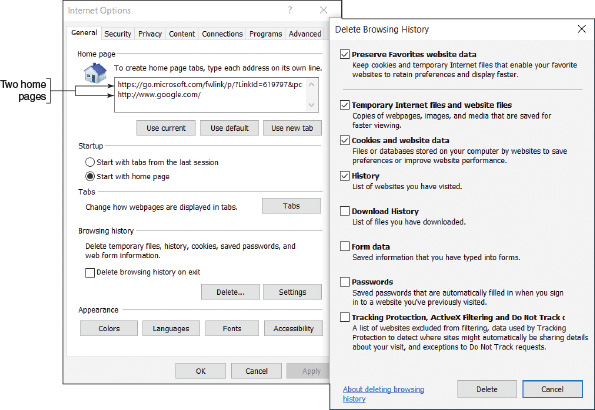
Enlarge Image

* **HTTP Secure.** Some web servers use HTTP with the SSL or TLS protocols (called HTTP Secure or HTTPS) to secure transmissions to and from the web server. Look for https and a padlock icon in the browser address box when HTTPS is used. Click the padlock to get information about the site security.
* **Repair or disable.** If you have a problem with Internet Explorer 11, try installing Windows updates, applying a restore point, or refreshing Windows 10/8. If you prefer to use a different browser, you can disable Internet Explorer 11. Open the **Programs and Features** window in Control Panel and click **Turn Windows features on or off**. In the Windows Features box, uncheck **Internet Explorer 11** and click **OK**.

Now let’s see how you can use the Internet Options box to secure Internet Explorer. To open the box, click the **Tools** icon on the right side of the Internet Explorer title bar and click **Internet options**. Another method is to press **Alt** to display the menu bar, click **Tools** in the menu, and click **Internet options**. A third method is to click **Internet Options** in the Classic view of Control Panel. The Internet Options box is shown in [Figure 16-9](javascript://).

**Figure 16-9**

Use the General tab of the Internet Options box to delete your browsing history



Enlarge Image

**Notes**

If you open the Internet Options box through Control Panel, the box is titled Internet Properties and the menus and options vary slightly.

**A+ Exam Tip**

The A+ Core 2 exam expects you to know how to use the General, Security, Privacy, Connections, Programs, and Advanced tabs in the Internet Options box.

Here are the more important tabs in the Internet Options box and how to use them:

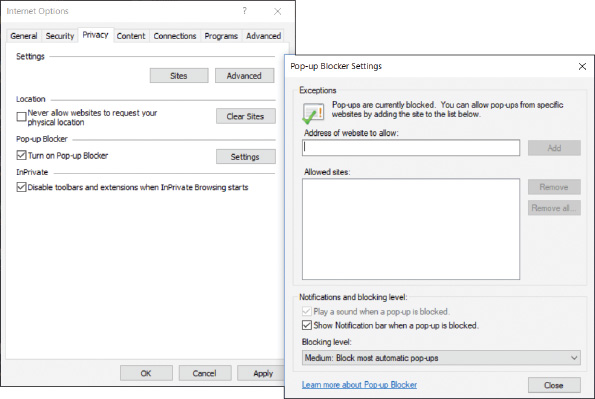
* **General tab**. Using the General tab, you can change the home page or add a second home page tab. You can also protect your identity and surfing records:
  + To delete what Internet Explorer has kept about your former browsing, click **Delete**. In the Delete Browsing History box (see the right side of [Figure 16-9](javascript://)), uncheck the first item and check all other items. (If you want to keep cookies used by websites in your Favorites list, check the first item, **Preserve Favorites website data**.) Click **Delete**.
  + For future browsing sessions, you can delete your browsing history each time you close Internet Explorer by checking **Delete browsing history on exit** on the General tab of the Internet Options box.

Internet Explorer holds a cache containing previously downloaded content in case it is requested again. The cache is stored in several folders named Temporary Internet Files. On the General tab, click **Settings** to change the maximum allowed space used for temporary Internet files and control the location of these files.

* **Security tab**. You can set a zone security level on the Security tab. For the Internet, medium-high is the default value; at this level, Internet Explorer prompts before downloading content and does not download ActiveX controls that are not signed by Microsoft. An [**ActiveX control**](javascript://) is a small app or add-on that can be downloaded from a website along with a webpage and is executed by Internet Explorer to enhance the webpage (for example, to add animation to the page). A virus can sometimes hide in an ActiveX control, but Internet Explorer is designed to catch them by authenticating each ActiveX control it downloads. To customize security settings, click **Custom level**. In the Security Settings box, you can decide exactly how you want to handle downloaded content. For example, you can disable file downloads.
* **Privacy tab**. Use the Privacy tab to block cookies that might invade your privacy or steal your identity. You can also use this tab to control the Pop-up Blocker, which prevents annoying pop-ups as you surf the web. To allow a pop-up from a particular website, click **Settings** and enter the URL of the website in the Pop-up Blocker Settings box. See [Figure 16-10](javascript://). Some pop-ups are useful, such as when you’re trying to download a file from a website and the site asks permission to complete the download.

**Figure 16-10**

Use the Privacy tab to control pop-ups and cookies



Enlarge Image

* **Connections tab**. The Connections tab allows you to configure proxy server settings and create a VPN connection. Many large corporations and ISPs use proxy servers to speed up Internet access. A web browser does not have to be aware that a proxy server is in use. However, one reason you might need to configure Internet Explorer to be aware of and use a proxy server is when you are on a corporate network and are having a problem connecting to a secured website (one using HTTP over SSL or another encryption protocol). The problem might be caused by Windows trying to connect using the wrong proxy server on the network. Check with your network administrator to find out if a specific proxy server should be used to manage secure website connections.

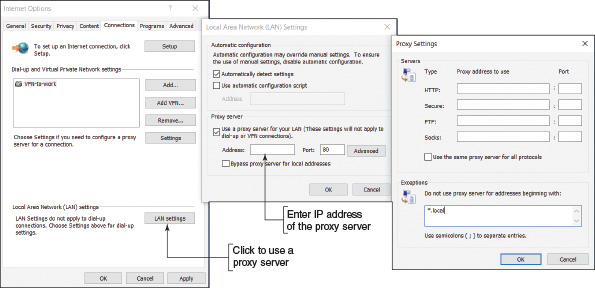
**A+ Exam Tip**

The A+ Core 2 exam expects you to know how to configure proxy settings on a client desktop.

If you need to configure Internet Explorer to use a specific proxy server, open the **Connections** tab and click **LAN settings**. In the settings box, check **Use a proxy server for your LAN** and enter the IP address of the proxy server (see [Figure 16-11](javascript://)). If your organization uses more than one proxy server, click **Advanced** and enter IP addresses for each type of proxy server on your network (see the right side of [Figure 16-11](javascript://)). You can also enter a port address for each server, if necessary. If you are trying to solve a problem of connecting to a server using HTTP over SSL or another secured protocol, use the Secure field to enter the IP address of the proxy server that is used to manage secure connections.

**Figure 16-11**

Configure Internet Explorer to use one or more proxy servers

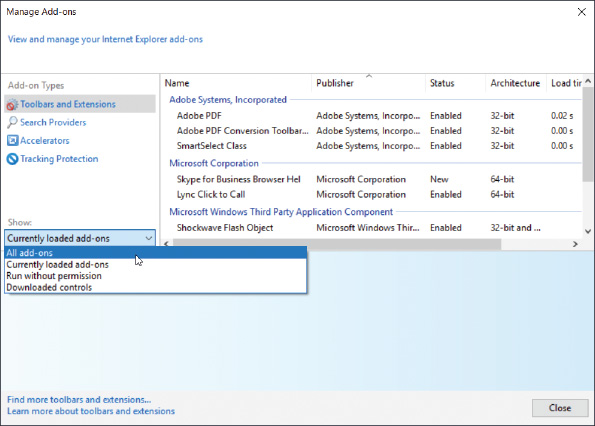


Enlarge Image

* **Programs tab**. The Programs tab is used to manage add-ons, also called plug-ins, which are small apps that help Internet Explorer to display multimedia content, manage email, translate text, or other actions. On the Programs tab, click **Manage add-ons** to open the Manage Add-ons box. See [Figure 16-12](javascript://). Here’s what you can do with this box:
  + **View all add-ons**. In the left pane under Show, you can select all add-ons installed on the computer, as shown in the figure.
  + **Enable or disable an add-on**. Select an add-on listed in the right pane to see information about it in the lower pane. To enable or disable a selected add-on, click **Enable** or click **Disable**.
  + **Delete an add-on**. Downloaded ActiveX controls can be uninstalled using this window. Select a downloaded ActiveX add-on and click **More information** in the lower pane. If the add-on has been downloaded and can be removed, the Remove button on the More information box will be available. You can also uninstall downloaded add-ons using the Programs and Features window in Control Panel.

**Figure 16-12**

Manage Internet Explorer add-ons



Enlarge Image

**Notes**

If you use Control Panel to open the Internet Options box and open the Manage Add-ons box from there, the Currently loaded add-ons option is missing in the drop-down list under Show.

* **Advanced tab**. The Advanced tab contains several miscellaneous settings used to control Internet Explorer. If you suspect problems are caused by wrong settings, use this tab to reset Internet Explorer to all default settings.

Now let’s turn our attention to securing another resource on the network: folders and files.

Go to pg.

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

Application Opened

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

## 16-1dFile and Folder Encryption

**A+ Core 2**

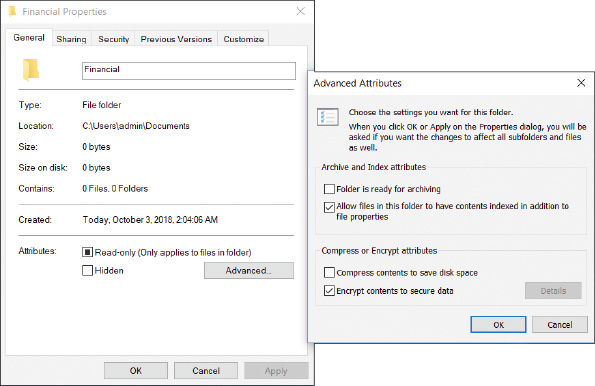
* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

In Windows, files and folders can be encrypted using the Windows [**Encrypting File System (EFS)**](javascript://). This encryption works only with the NTFS file system and business and professional editions of Windows. If a folder is marked for encryption, every file created in the folder or copied to the folder will be encrypted. An encrypted file remains encrypted if you move it from an encrypted folder to an unencrypted folder on the same or another NTFS volume. To encrypt a folder or file, right-click it and open its Properties box (see [Figure 16-13](javascript://)). On the General tab, click **Advanced**. In the Advanced Attributes box, check **Encrypt contents to secure data** and click **OK**. In File Explorer or Windows Explorer, encrypted file and folder names are displayed in green by default.

**Figure 16-13**

Encrypt a folder and all its contents



Enlarge Image

**Notes**

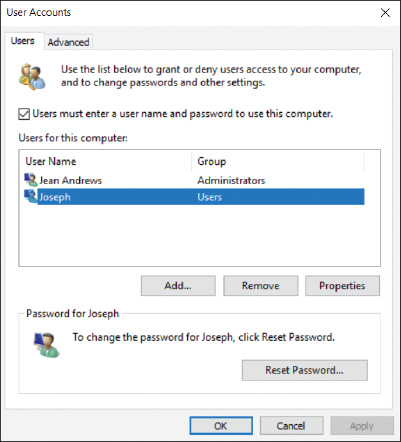
If the folder or file doesn’t display in a green font in File Explorer, you can change the setting by opening **Control Panel** and clicking **File Explorer Options**. On the View tab, check **Show encrypted or compressed NTFS files in color**. Click **OK**.

**Caution**

A user sometimes forgets a password, and an administrator can reset the forgotten password. However, know that if an administrator resets a user password, the user will lose all his EFS encrypted folders and files, personal digital certificates, and passwords stored on the computer. To reset a user password, you can use the [**Network Places Wizard**](javascript://) tool (netplwiz.exe), as shown in [Figure 16-14](javascript://). Select the user and click **Reset Password**.

**Figure 16-14**

Reset a user password



Go to pg.

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

Application Opened

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

## 16-1eBitLocker Encryption

**A+ Core 2**

* 1.6

Given a scenario, use Microsoft Windows Control Panel utilities.

* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

[**BitLocker Drive Encryption**](javascript://) in Windows professional and business editions locks down a hard drive by encrypting the entire Windows volume and any other volume on the drive and restricts access by requiring one or two encryption keys. A similar feature, [**BitLocker To Go**](javascript://), encrypts data on a USB flash drive and restricts access by requiring a password. You need to be aware of the restrictions and possible risks before you decide to use BitLocker. It’s intended to work in partnership with file and folder encryption to provide data security.

**A+ Exam Tip**

The A+ Core 2 exam expects you to know when it is appropriate to use BitLocker Drive Encryption and BitLocker To Go in a given scenario.

The three ways you can use BitLocker Drive Encryption depend on the type of protection you need and the computer hardware available:

* **Computer authentication**. Many laptop computers have a chip on the motherboard called the **TPM (Trusted Platform Module)** chip. The TPM chip holds the BitLocker encryption key (also called the startup key). If the hard drive is stolen from the laptop and installed in another computer, the data would be safe because BitLocker would not allow access without the startup key stored on the TPM chip. Therefore, this method authenticates the computer. However, if the motherboard fails and is replaced, you’ll need a backup copy of the startup key to access data on the hard drive. (You cannot move the TPM chip from one motherboard to another.)
* **User authentication**. For computers that don’t have TPM, the startup key can be stored on a USB flash drive (or other storage device the computer reads before the OS is loaded), and the flash drive must be installed before the computer boots. This method authenticates the user. For this method to be the most secure, the user must never leave the flash drive stored with the computer. (Instead, the user might keep the USB startup key on his key ring or a lanyard.)
* **Computer and user authentication**. For best security, a password can be required at every startup in addition to TPM. Using this method, both the computer and the user are authenticated. This practice is an example of **multifactor authentication (MFA)**, which uses more than one method to authenticate.

BitLocker Drive Encryption provides great security, but security comes with a price. For instance, you risk the chance your TPM will fail or you will lose all copies of the startup key. In these events, recovering the data can be messy. Therefore, use BitLocker only if the risks of using it do not outweigh the risks of stolen data. And, if you decide to use BitLocker, be sure to make extra copies of the startup key and/or password and keep them in a safe location.

**Caution**

In [Chapter 17](javascript://), you learn that some data, such as health-care data, is regulated by the government, and organizations that are negligent to protect it can be held legally responsible for data breaches. For this type of data, encryption and other security measures may be mandated by law.

To start the process of using BitLocker Drive Encryption, first go into BIOS/UEFI setup and enable the TPM chip. Then open the **BitLocker Drive Encryption** applet in Control Panel (see [Figure 16-15](javascript://)). Using this window, you can click **TPM Administration** to manage the TPM chip and turn on BitLocker or BitLocker To Go.

**Figure 16-15**

Manage BitLocker Drive Encryption, the TPM chip, and BitLocker To Go



Enlarge Image

**Notes**

For detailed instructions on how to set up BitLocker Drive Encryption, see the Microsoft Windows IT Pro Center article “BitLocker” at [docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview](http://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview" \t "_blank).

Go to pg.

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

Application Opened

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

## 16-1fWindows Firewall Settings

**A+ Core 2**

* 1.5

Given a scenario, use Microsoft operating system features and tools.

* 1.6

Given a scenario, use Microsoft Windows Control Panel utilities.

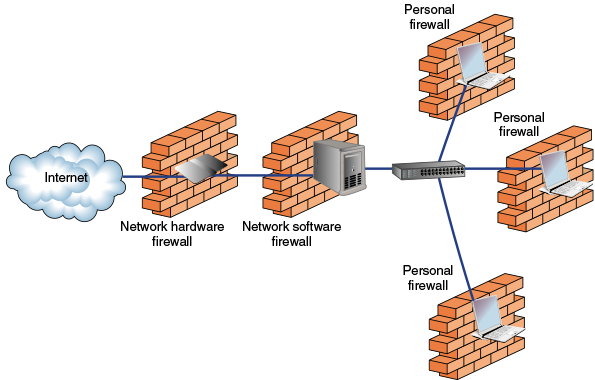
* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

Recall from [Chapter 7](javascript://) that a SOHO router can serve as a hardware firewall to protect its network from attack over the Internet. Recall that the best protection from attack is layered protection (see [Figure 16-16](javascript://)). In addition to a network hardware firewall, a large corporation might use a software firewall, also called a corporate firewall, installed on a computer that stands between the Internet and the network to protect the network. This computer has two network cards installed, and the installed software firewall filters the traffic between the two cards.

**Figure 16-16**

Three types of firewalls used to protect a network and individual computers on the network



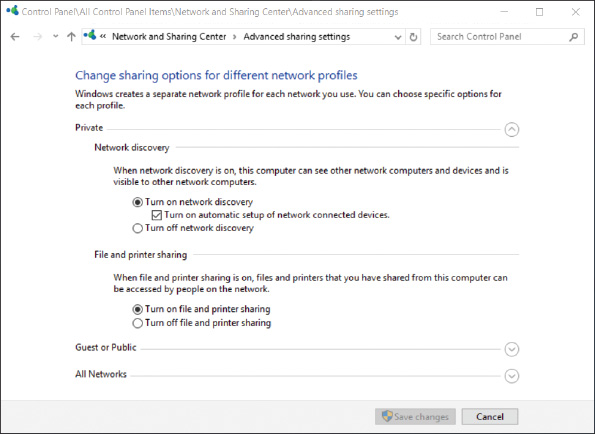
Enlarge Image

A personal firewall, also called a host firewall or application firewall, is software installed on a personal computer to protect it. A personal firewall provides redundant protection from attacks over the Internet, filters inbound traffic to protect a computer from attack from other computers on the same network, and filters outbound traffic to prevent attacks on other computers on the same network. When setting up a SOHO network or a personal computer, configure a personal firewall on each computer.

[**Windows Firewall**](javascript://) is a personal firewall that protects a computer from intrusion and from attacking other computers; it is automatically configured when you set up your security level for a new network connection. To set the security for a network connection, open the **Network and Sharing Center** in Control Panel and click **Change advanced sharing settings**. The resulting Windows 10 Advanced sharing settings window is shown in [Figure 16-17](javascript://). (Recall that for Windows 10/8, the options are private and public security, and for Windows 7, the options are home, work, and public security.)

**Figure 16-17**

Configure the security level for network connections



Enlarge Image

Later in the chapter, you learn how to share folders and printers on a private network. For folder and printer sharing to work, you need to use the Advanced sharing settings window to turn on network discovery and file and printer sharing so that Windows Firewall allows this type of network traffic.

**Applying Concepts**

### Configuring Windows Firewall

You can use the Windows Firewall window to configure even more firewall settings. Follow these steps to find out how:

1. Use one of these methods to open Windows Firewall:
   * Open the **Network and Sharing Center**. For Windows 10, click **Windows Defender Firewall** in the lower part of the left pane. For Windows 8/7, click **Windows Firewall**.
   * Open Control Panel in Classic view and click **Windows Defender Firewall**. For Windows 8/7, click **Windows Firewall**.

The Windows Defender Firewall window is shown in [Figure 16-18](javascript://). Although the Windows 8/7 Windows Firewall window looks slightly different, the windows work basically the same way.

**Figure 16-18**

Windows Defender Firewall shows the firewall is turned on to protect private and public networks

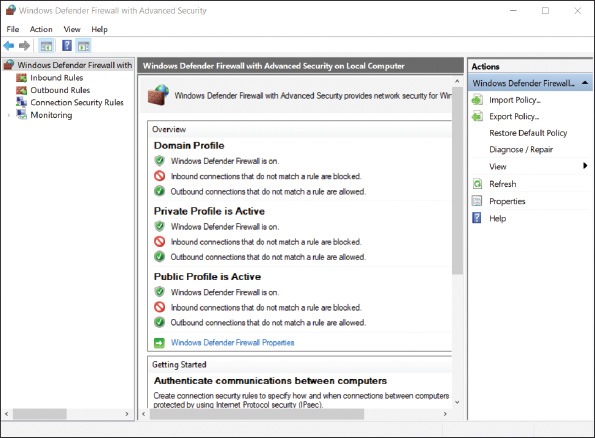


Enlarge Image

1. In general, Windows Firewall works by allowing or denying network traffic on incoming or outgoing ports. Recall that a port is a number an application on the computer uses to connect to another application on the network or Internet. Here are some basic settings you can configure in Windows Firewall:
   * Use the left pane to turn Windows Firewall on or off. When Windows Firewall is disabled (not a good idea), all traffic is allowed to pass and your computer is unprotected.
   * When Windows Firewall is enabled, all traffic is stopped unless you have specified an exception. To allow or deny a specific app access to the computer, click **Allow an app or feature through Windows Defender Firewall**. You can then select the app from a list of apps and decide how it can use the network connection.
   * To allow or deny all other types of traffic, not just those related to apps, click **Advanced settings**. On the Advanced Security window (see [Figure 16-19](javascript://)), you can click Inbound Rules or Outbound Rules to create or edit an inbound or outbound rule and control traffic. A rule can specify how port numbers, TCP/IP protocols, programs, services, computers, and remote users can use the network connection. A rule can apply to public, private, and domain networks.

**Figure 16-19**

Customize an inbound or outbound rule to control exactly what incoming or outgoing traffic is allowed through the firewall



Enlarge Image

Go to pg.

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

Application Opened

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

**16-2**Controlling Access to Folders and Files

**A+ Core 2**

* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

* 2.2

Explain logical security concepts.

* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

Responsibility for a peer-to-peer network or domain can include controlling access to folders and files for users of a local computer and for remote users accessing shared resources over the network. Managing shared resources is accomplished by

1. assigning privileges to user accounts and
2. assigning permissions to folders, files, and printers.

**Notes**

In Windows, the terms *privileges* and *permissions* have different meanings. [**Privileges**](javascript://) (also called rights) refer to the tasks an account is allowed to do in the system, such as installing software or changing the system date and time. [**Permissions**](javascript://) refer to which user accounts or user groups are allowed access to data files and folders. *Privileges are assigned to an account, and permissions are assigned to data files and folders.*

Let’s first look at the strategies used for controlling privileges to user accounts and controlling permissions to folders and files. Then you learn the procedures in Windows for assigning these privileges and permissions.

Go to pg.

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

Application Opened

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

## 16-2aClassifying User Accounts and User Groups

**A+ Core 2**

* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

* 2.2

Explain logical security concepts.

* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

Computer users should be classified to determine the privileges they need to do their jobs. For example, some users need the privilege to sign in to a system remotely and others do not. Other privileges granted to users might include the right to install software or hardware, change the system date and time, change Windows Firewall settings, and so forth. Generally, when a new employee begins work, that employee’s job description with exceptions approved by his supervisor determine what privileges the employee needs to perform his job. You, as the support technician, will be responsible to make sure the user account assigned to the employee has these privileges and no more. This approach is called the [**principle of least privilege**](javascript://).

In Windows, the privileges or rights assigned to a user account are established when you first create the account, which is when you decide the account type. You can later change these privileges by changing the user groups to which the account belongs. Recall from [Chapter 12](javascript://) that user accounts can be created using the User Accounts applet in Control Panel (in any edition of Windows) or the [**Local Users and Groups**](javascript://) utility in the Computer Management console (in business and professional editions of Windows). User accounts can be assigned to different user groups using the Computer Management console in business and professional editions of Windows. Home editions of Windows cannot be used to manage user groups.

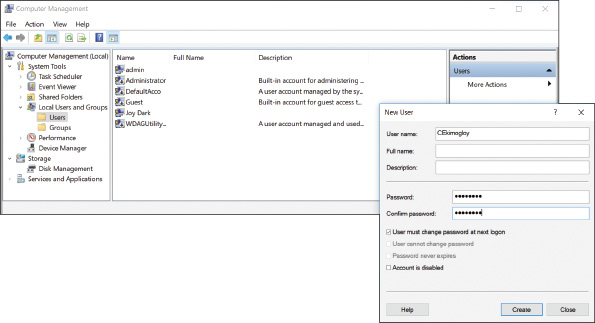
### Type of User Account

When you use the User Accounts applet in Control Panel to manage user accounts, you can choose between two account types: Administrator or Standard. When you use Local Users and Groups in Computer Management to create an account, the account type is automatically a standard user account.

To create a user account using Computer Management, first open the Computer Management console (compmgmt.msc). Under **Local Users and Groups**, right-click **Users** and select **New User** in the shortcut menu. (Windows Home editions don’t include the Local Users and Groups option in the Computer Management console.) Enter information for the new user and click **Create** (see [Figure 16-20](javascript://)).

**Figure 16-20**

Create a new user



Enlarge Image

**A+ Exam Tip**

The A+ Core 2 exam expects you to be able to compare privileges assigned to the administrator, standard user, power user, and guest user groups.

### Built-in User Groups

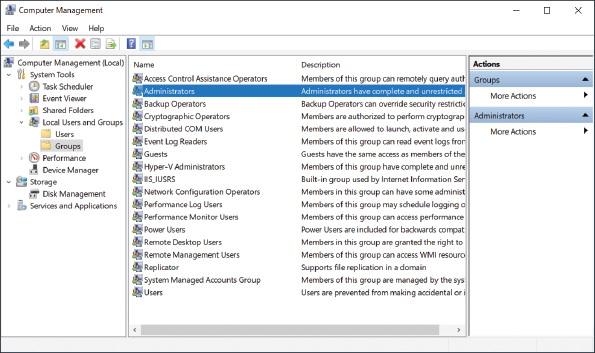
A user account can belong to one or more user groups. Windows offers several built-in user groups and you can create your own. Here are important built-in user groups:

* **Administrators and Users groups.** By default, administrator accounts belong to the [**Administrators group**](javascript://), and standard user accounts belong to the [**Users group**](javascript://). If you want to give administrator privileges to a standard user account, use the Computer Management console to add the account to the Administrators group.
* **Guests group.** The [**Guests group**](javascript://) has limited privileges on the system and is given a temporary profile that is deleted when the user signs out. Windows automatically creates one account in the Guests group named the Guest account, which is disabled by default.
* **Power Users group.** Older editions of Windows have a [**Power Users group**](javascript://) that can read from and write to parts of the system other than its own user profile folders, install applications, and perform limited administrative tasks. Windows 10/8/7 offers a Power Users group only for backward compatibility with legacy applications.

To view user groups installed on a system, open the Computer Management console. Under Local Users and Groups, click **Groups** (see [Figure 16-21](javascript://)).

**Figure 16-21**

User groups installed on a system

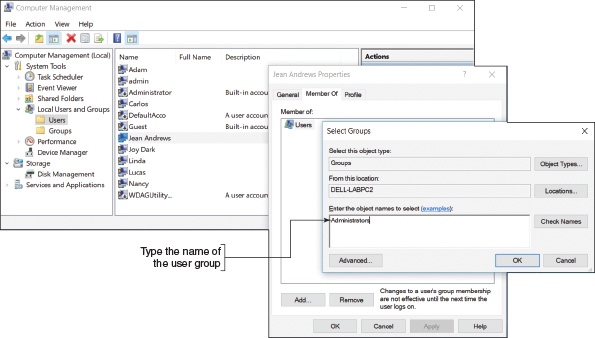


Enlarge Image

To change the groups a user account is in, click **Users** under Local Users and Groups. The list of user accounts appears in the right pane of the console window (see the left side of [Figure 16-22](javascript://)). Right-click the user account and select **Properties** in the shortcut menu. In the user account Properties box, click the **Member Of** tab (see the middle of [Figure 16-22](javascript://)). Click **Add** and enter the user group name. You must type the user group name exactly as it appears in the list of user groups that you saw earlier (see [Figure 16-21](javascript://)). To verify that the group name is correct, click **Check Names**. A verified name is underlined. (Alternately, you can click **Advanced**, click **Find Now**, and select the group name from the list of groups that appears.) Click **OK** twice to close both boxes.

**Figure 16-22**

Add a user account to a user group



Enlarge Image

In addition to the groups you can assign to an account, Windows might automatically assign one of these built-in user groups to an account when it is determining permissions assigned to a file or folder:

* The [**Authenticated Users group**](javascript://) includes all user accounts that can access the system except the Guest account. These accounts include domain accounts (used to sign in to the domain) and local accounts (used to sign in to the local computer). The accounts might or might not require a password. When you create a folder or file that is not part of your user profile, Windows gives access to all Authenticated Users by default.
* The [**Everyone group**](javascript://) includes the Authenticated Users group as well as the Guest account. When you share a file or folder on the network (or to a homegroup in Windows 8/7), Windows gives access to the Everyone group by default.
* [**Anonymous users**](javascript://) are users who have not been authenticated on a remote computer. If you sign in to a computer using a local account and then attempt to access a remote computer, you must be authenticated on the remote computer. You will be authenticated if your user account and password match on both computers. If you signed in to your local computer with an account and password that do not match an account and password on the remote computer, you are considered an anonymous user on the remote computer. As an anonymous user, you might be allowed to use File Explorer or Windows Explorer to view shared folders and files on the remote computer, but you cannot access them.

### Customized User Groups

Use the Computer Management console or the Local Users and Groups console (lusrmgr.msc) in business and professional editions of Windows to create and manage your own user groups. When managing several user accounts, it’s easier to assign permissions to user groups rather than to individual accounts. First create a user group and then assign permissions to this user group. Any user account that you put in this group then acquires or inherits the same permissions.

User groups work especially well when several users need the same permissions. For example, you can set up an Accounting group and a Medical Records group for a small office. Users in the Accounting department and users in the Medical Records department go into their respective user groups. Then you only need to manage the permissions for two groups rather than multiple user accounts.

Go to pg.

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

Application Opened

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

## 16-2bMethods to Assign Permissions to Folders and Files

**A+ Core 2**

* 2.2

Explain logical security concepts.

* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

There are two general strategies for managing shared files and folders, also called directories, in Windows:

* **Workgroup sharing.** With workgroup sharing, all privileges and permissions are set up on each local computer so that each computer manages access to its files, folders, and printers shared on the peer-to-peer network. The local user decides which users on the network have access to which shared folder and the type of access they have.
* **Domain controlling**. If a Windows computer belongs to a domain instead of a workgroup or homegroup, all security should be managed by the network administrator for the entire network. Although individual users on workstations can share files and folders with other users in the domain, this is not considered a security best practice.

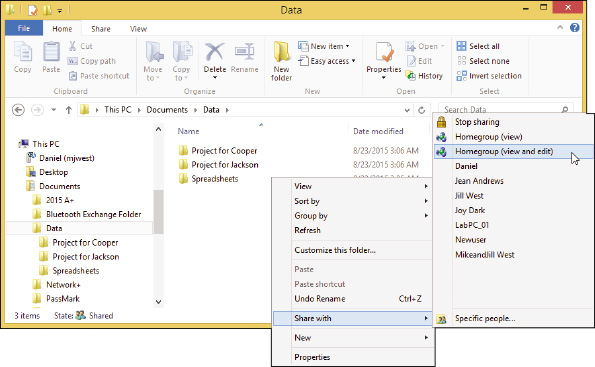
**OS Differences**

For Windows 8/7, when all users on a small network require the same access to all resources, you can use a homegroup. Folders, libraries, files, and printers shared with the homegroup are available to all users on the network whose computers have joined the homegroup. After the homegroup is set up, you can share a file or folder with the homegroup using the Sharing Wizard. To do so, right-click the item and select **Share with** in the shortcut menu. The wizard lists three general options for sharing followed by a list of specific people (see [Figure 16-23](javascript://)). Click **Homegroup (view)** or **Homegroup (view and edit)** to assign this permission to the homegroup.

Because of the lack of control over who can access a particular file or folder in a homegroup, Windows 10 Version 1803 and higher does not support homegroups.

**Figure 16-23**

Share a folder with the homegroup



Enlarge Image

On a Windows peer-to-peer network, each workstation shares its files and folders with others in the workgroup, or files and folders on a file server are shared. Here are some tips about which folders to use to hold shared data on a file server or personal computer:

* Private data for an individual user is best kept in the C:\Users folder for that user. User accounts with limited or standard privileges cannot normally access these folders because they belong to another user account. However, accounts with administrative privileges do have access.
* The C:\Users\Public folder is intended to be used for folders and files that all users share. It is not recommended that you use this folder for controlled access to data.
* For best security, create a folder that’s not in the C:\Users folder and assign permissions to that folder and its subfolders. You can allow all users access or only certain users or user groups.

Some applications can be shared with others on the network. If you share a folder that has a program file in it, a user on another computer can double-click the program file and execute it remotely on his or her desktop. This is a handy way for several users to share an application that is installed on a single computer. However, know that not all applications are designed to work this way.

Regardless of whether you are sharing to a workgroup or domain, Windows offers two methods to share a folder over the network:

* **Share permissions**. [**Share permissions**](javascript://) grant permissions only to network users, and these permissions do not apply to local users of a computer. Share permissions work on NTFS, FAT32, and exFAT volumes and are configured using the Sharing tab in a folder’s Properties box. Share permissions apply to a folder and its contents, but not to individual files.
* **NTFS permissions.** [**NTFS permissions**](javascript://) apply to local users and network users and apply to both folders and individual files. NTFS permissions work on NTFS volumes only and are configured using the Security tab in a file or folder’s Properties box. (The Security tab is missing on the Properties box of a folder or file on a FAT volume.)

Here are some tips when implementing share permissions and NTFS permissions:

* If you use both share permissions and NTFS permissions on a folder, the more restrictive permission applies. For NTFS volumes, use only NTFS permissions because they can be customized better. For FAT volumes, your only option is share permissions.
* If NTFS permissions are conflicting—for example, when a user account has been given one permission and the user group to which this user belongs has been given a different permission—the more liberal permission applies.
* [**Permission propagation**](javascript://) is when permissions are passed from parent object to child. [**Inherited permissions**](javascript://) are permissions that are attained from a parent. For example, when you create a file or folder in a parent folder, the new object takes on the permissions of the parent folder.
* When you move or copy an object to a folder, the object takes on the permissions of that folder. The exception to this rule is when you move (not copy) an object from one location to another on the same volume. In this case, the object retains its permissions from the original folder.

**Notes**

You can use the xcopy or robocopy command with parameters to change the rules for how inherited permissions are managed when copying and moving files. For more information, see the Microsoft Knowledge Base article cc733145 at [https://technet.microsoft.com/en-us/library/cc733145](https://technet.microsoft.com/en-us/library/cc733145" \t "_blank).

**A+ Exam Tip**

The A+ Core 2 exam expects you to compare NTFS and share permissions, including how allow and deny conflicts are resolved with each and what happens to permissions when you move or copy a file or folder.

Go to pg.

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

Application Opened

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

## 16-2cHow to Share Folders and Files

**A+ Core 2**

* 1.5

Given a scenario, use Microsoft operating system features and tools.

* 1.6

Given a scenario, use Microsoft Windows Control Panel utilities.

* 2.2

Explain logical security concepts.

* 2.6

Compare and contrast the differences of basic Microsoft Windows OS security settings.

Now that you know about the concepts and strategies for sharing folders and files, let’s look at the details of how to use Windows to manage user privileges and file and folder permissions.

**Applying Concepts**

### Creating User Accounts with Data Access

Nicole is responsible for a peer-to-peer network at a medical doctor’s office. Four computers are connected to the small company network; one of these computers acts as the file server for the network. Nicole has created two classifications of data, Financial and Medical. Two workers (Nancy and Adam) require access to the Medical data, and two workers (Linda and Carlos) require access to the Financial folder. In addition, the doctor, Lucas, requires access to both categories of data. Nicole must do the following to set up the users and data:

1. Create folders named Financial and Medical on the file server. Create five user accounts, one each for Lucas, Nancy, Adam, Linda, and Carlos. All the accounts belong to the Windows standard user group. Create two user groups, Financial and Medical.
2. Using NTFS permissions, set the permissions for the Financial and Medical folders on the file server so that only the members of the appropriate group can access each folder.
3. Test access to both folders using test data and then copy all real data into the two folders and subfolders. Set up a backup plan for the two folders, as you learned to do in [Chapter 13](javascript://).

Let’s look at how each of these three steps is done.

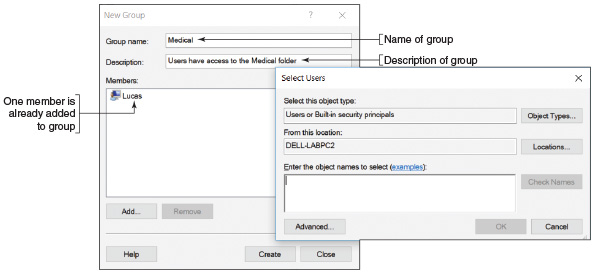
### Step 1: Create Folders, User Accounts, and User Groups

Follow these steps to create the folders, user accounts, and user groups on the file server computer that is using Windows 10 Pro:

1. Sign in to the system as an administrator.
2. Using an NTFS volume, create these two folders: **C:\Medical** and **C:\Financial**.
3. Open the Computer Management console or the Local Users and Groups console and create user accounts for **Lucas**, **Nancy**, **Adam**, **Linda**, and **Carlos**. The account types are automatically standard user accounts.
4. To create the Medical user group, right-click **Groups** under Local Users and Groups and select **New Group** in the shortcut menu. The New Group box appears. Enter the name of the group (**Medical**) and its description (**Users have access to the Medical folder**), as shown in [Figure 16-24](javascript://).

**Figure 16-24**

Setting up a new user group



Enlarge Image

1. Add all the users who need access to medical data (Lucas, Adam, and Nancy). To add members to the Medical group, click **Add**. The Select Users box opens, as shown on the right side of [Figure 16-24](javascript://). Under Enter the object names to select, enter the name of a user. Click **Check Names** to verify the user. Click **OK**. As each user is added, his or her name appears under Members in the New Group box, as shown in [Figure 16-24](javascript://). To create the group, click **Create** in the New Group box.
2. In the same way, create the Financial group and add Lucas, Linda, and Carlos to the group. Later, you can use the Computer Management console to add or remove users from either group.
3. Close the Computer Management console.

**A+ Exam Tip**

The A+ Core 2 exam expects you to be able to set up a user account or group and know how to change the group to which an account is assigned.

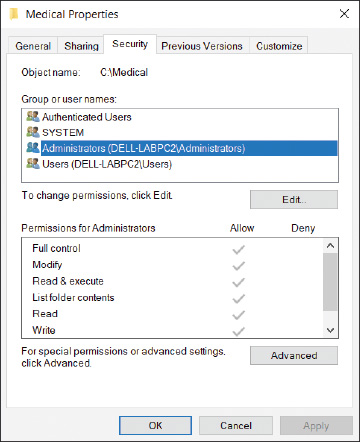
### Step 2: Set NTFS Folder Permissions for User Groups

Follow these steps to set the NTFS permissions for the two folders:

1. Open File Explorer or Windows Explorer, right-click the **Medical** folder, and select **Properties** in the shortcut menu. The Properties box for the folder appears.
2. Click the **Security** tab (see [Figure 16-25](javascript://)). Notice in the box that Authenticated Users, SYSTEM, Administrators, and Users all have access to the C:\Medical folder. When you select a user group, the type of permissions assigned to that group appears in the Permissions area. [Table 16-1](javascript://) explains the more significant types of permission. Note that the Administrators group has full control of the folder. Also notice the checks under Allow are dimmed. These permissions are dimmed because they have been inherited from the parent object. In this case, the parent object is Windows default settings.

**Figure 16-25**

Permissions assigned to the Medical folder



**Table 16-1**

### Permission Levels for Files and Folders

| **Permission Level** | **Description** |
| --- | --- |
| Full control | Can read, change, delete, and create files and subfolders, read file and folder attributes, read and change permissions, and take ownership of a file or folder. |
| Modify | Can read, change, and create files and subfolders. Can delete the folder or file but cannot delete subfolders and their files. Can read and change attributes. Can view permissions but not change them. Cannot take ownership. |
| Read & execute | Can read folders and contents and run programs in a folder. (Applies to both files and folders.) |
| List folder contents | Can read folders and contents and run programs in a folder. (Applies only to folders.) |
| Read | Can read folders and contents. |
| Write | Can create a folder or file and change attributes but cannot read data. This permission is used for a drop folder, where users can drop confidential files that can only be read by a manager. For example, an instructor can receive student homework in a drop folder. |

Enlarge Table

**Notes**

For a thorough discussion of how permissions work, see the Microsoft Knowledge Base article cc783530 at [https://technet.microsoft.com/en-us/library/Cc783530(v=WS.10).aspx](https://technet.microsoft.com/en-us/library/Cc783530(v=WS.10).aspx" \t "_blank).

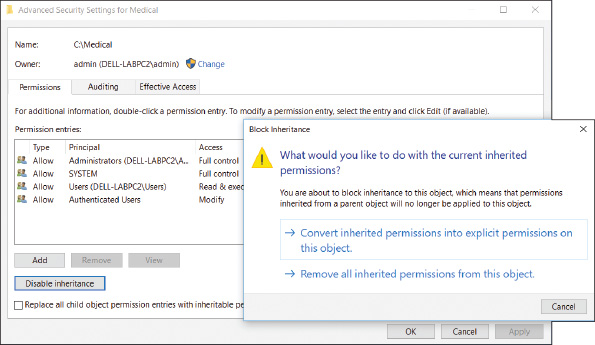
**A+ Exam Tip**

The A+ Core 2 exam expects you to know that NTFS permissions can be customized better than share permissions.

1. To remove the inherited status from these permissions so you can change them, click **Advanced**. The Advanced Security Settings box appears (see the left side of [Figure 16-26](javascript://)). Click **Disable inheritance**. The Block Inheritance box appears (see the right side of [Figure 16-26](javascript://)). To keep the current permissions but remove the inherited status placed on them, click **Convert inherited permissions into explicit permissions on this object**. Click **Apply**.

**Figure 16-26**

Remove the inherited status from the current permissions



Enlarge Image

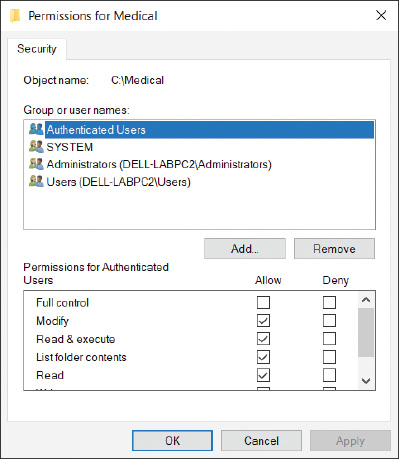
**OS Differences**

To remove the inherited status of folder permissions in Windows 7, open the Advanced Security Settings box and click **Change Permissions**. In the new Advanced Security Settings box, you can now uncheck **Include inheritable permissions from this object’s parent**. A Windows Security warning box appears. To keep the current permissions but remove the inherited status placed on them, click **Add**.

1. Close the Advanced Security Settings box.
2. In the Medical Properties box, notice the permissions are now checked in black, indicating they are no longer inherited permissions and can be changed. Click **Edit** to change these permissions.
3. The Permissions box opens (see [Figure 16-27](javascript://)). Select the **Authenticated Users** group and click **Remove**. Also remove the **Users** group. Don’t remove the SYSTEM group, which gives Windows the access it needs. Also, don’t remove the Administrators group. You need to leave that group as is so that administrators can access the data.

**Figure 16-27**

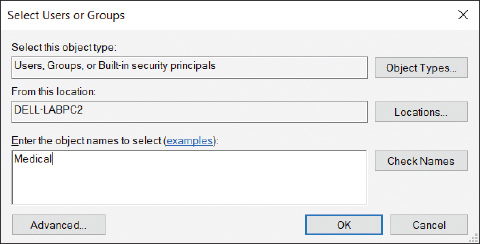
Change the permissions to a folder



1. To add a new group, click **Add**. The Select Users or Groups box opens. Under Enter the object names to select, type **Medical**, as shown in [Figure 16-28](javascript://). Click **Check Names** to verify the group. Click **OK**. The Medical group is added to the list of groups and users for this folder.

**Figure 16-28**

Add a user or group to shared permissions



1. In the Permissions box, make sure the **Medical** group is selected. Under Permissions for Medical, check **Allow** under Full control to give that permission to this user group. Click **OK** twice to close the Properties box.
2. In a similar way, change the permissions of the C:\Financial folder so that Authenticated Users and Users are not allowed access and the Financial group is allowed full control.

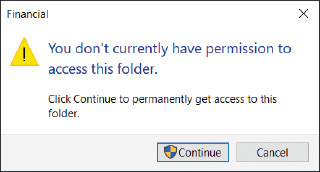
### Step 3: Test, Set Share Permissions, and Go Live

It’s now time to test your security measures. Do the following to test the NTFS permissions and implement your shared folders:

1. Test a user account in each user group to make sure the user can read, write, and delete in the folder he needs but cannot access the other folder. Put some test data in each folder. Then sign in to the system using an account you want to test and try to access each folder. [Figure 16-29](javascript://) shows the box that appears when an unauthorized user attempts to access a local folder. When you click **Continue**, entering an administrator password in the resulting UAC box gives you access.

**Figure 16-29**

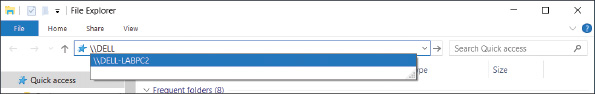
Access to a folder is controlled



1. Now that NTFS permissions are set correctly for each local and network user, you are ready to allow access over the network. To do that, both NTFS and share permissions must allow network access. (Share permissions apply only to network access, not local access.) The best practice is to allow full access using share permissions and restrictive access using NTFS permissions. Remember that the most restrictive permissions apply. To allow full access using share permissions, click the **Sharing** tab of each folder’s properties box, and click **Advanced Sharing**.
2. In the Advanced Sharing box, check **Share this folder** if it is not already checked. Then click **Permissions**. To add a new group, click **Add**. The Select Users or Groups box opens. Under Enter the object names to select, type **Everyone** and click **OK**. The Everyone group is added to the list of groups and users for this folder.
3. With **Everyone** selected, check **Allow** under Full control to give that permission to the Everyone user group. Click **OK** twice and then close the Properties box.
4. Now that you have the security settings in place for one computer, go to each computer on the network and create the user accounts that will be using this computer. Then test the security and make sure each user can or cannot access the \Financial and \Medical folders as you intend. To access shared folders, you can drill down into the Network group in File Explorer or Windows Explorer. Another method is to type the IP address (for example, **\\192.168.1.112**) or computer name (for example, **\\DELL-LABPC2**) in the address bar of the Explorer window, as shown in [Figure 16-30](javascript://).

**Figure 16-30**

Use the computer name to access shared folders on that computer

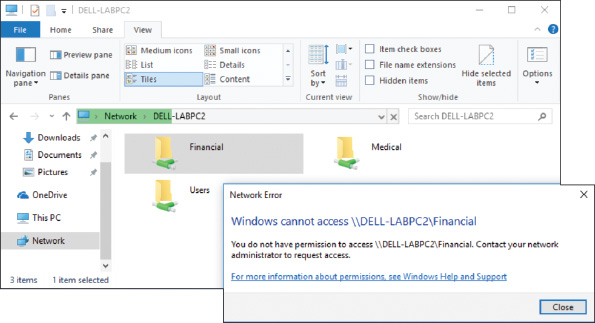


Enlarge Image

1. [Figure 16-31](javascript://) shows the error message that appears when an unauthorized user attempts to access a network resource. After you are convinced the security works as you want it to, copy all the company data to subfolders in these folders. Check a few subfolders and files to verify that each has the permissions you expect. Also, don’t forget to implement the backup procedures on the file server, as you learned in [Chapter 13](javascript://).

**Figure 16-31**

When a remote user is denied access to a network resource, there is no opportunity to provide access from this screen



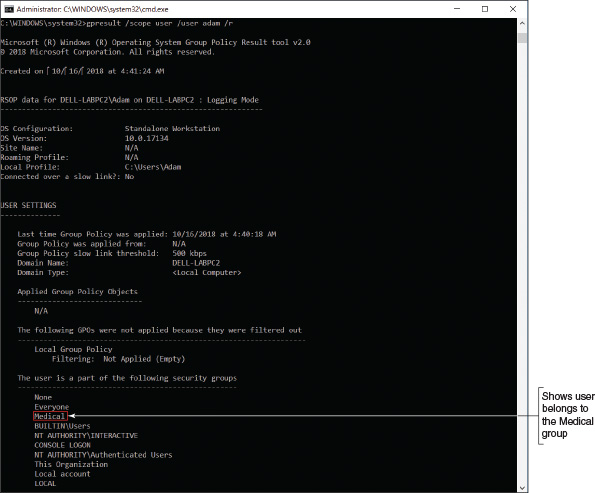
Enlarge Image

### User and Group Information with the Gpresult Command

You can pull a list of all the groups a user belongs to with the **[gpresult](javascript://)** command. This information can be helpful when troubleshooting user group issues or Group Policy problems; the command displays user groups a user belongs to and all the currently applied policies set by Group Policy. To retrieve information about a user other than the one signed in, open an elevated command prompt window and enter the command **gpresult /scope user /user** username **/r**. [Figure 16-32](javascript://) shows output for the user Adam; you can verify that he belongs to the Medical group. You learn more about the gpresult command later in this chapter.

**Figure 16-32**

The /r parameter requests a summary of the gpresult information instead of more verbose (/v) output



Enlarge Image

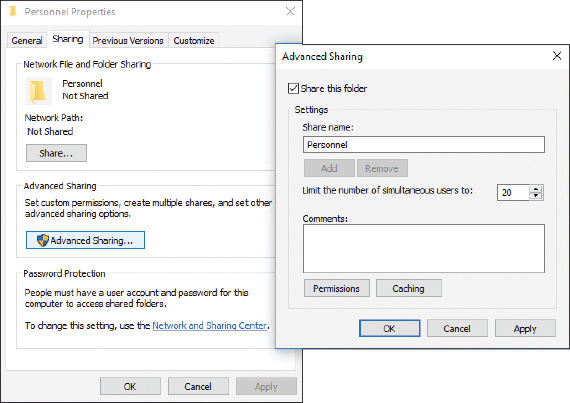
### How to Use Share Permissions

Although you can mix NTFS permissions and share permissions on the same system, life is simpler if you use one or the other. For NTFS volumes, NTFS permissions are the way to go because they can be customized better than share permissions. However, you must use share permissions on FAT volumes. To do so, follow these steps:

1. Open the Properties box for the folder (Personnel in this case). Notice in [Figure 16-33](javascript://) that the Security tab is missing because the folder is on a FAT volume. Select the **Sharing** tab and click **Advanced Sharing**. The Advanced Sharing box opens (see the right side of [Figure 16-33](javascript://)).

**Figure 16-33**

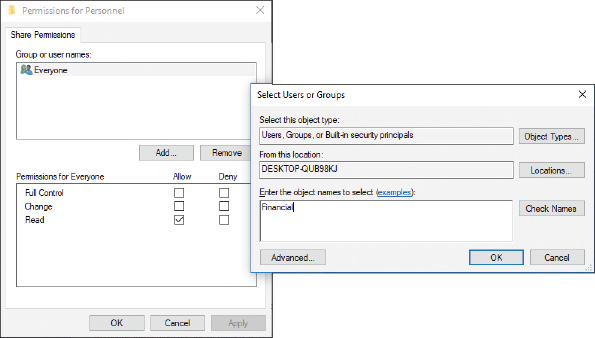
Use the Sharing tab of a folder Properties box to set up share permissions on a FAT volume



1. Check **Share this folder**. Then click **Permissions**. The Permissions box opens (see the left side of [Figure 16-34](javascript://)). Initially, the folder is shared with Everyone. Also notice that share permissions offer only three permission levels: Full Control, Change, and Read.

**Figure 16-34**

Add a user or user group to assign share permissions



Enlarge Image

1. Click **Add**. The Select Users or Groups box appears (see the right side of [Figure 16-34](javascript://)). Enter a user account or user group and click **OK**.
2. To delete the Everyone group, select it in the Permissions box and click **Remove**. Click **OK** to close each open box in turn.

### Support and Troubleshoot Shared Folders and Files

You have just seen how to set up user groups and folder permissions assigned to these groups. If you have problems accessing a shared resource, follow these steps:

1. Windows might be able to solve the problem for you. In Control Panel, click **Troubleshooting**. The Troubleshooting window presents a list of troubleshooters for addressing problems in the categories of Programs, Hardware and Sound, Network and Internet, or System and Security. Click **Access shared files and folders on other computers** and walk through the Shared Folders troubleshooter.
2. Open the Network and Sharing Center. Make sure your network location is set to Private (Home or Work for Windows 7).
3. In the left pane, click **Change advanced sharing settings**. The Advanced sharing settings window opens (refer back to [Figure 16-17](javascript://)).
4. Verify that the settings here are the default settings for a Private network profile:
   * Select **Turn on network discovery** and make sure **Turn on automatic setup of network connected devices** is checked.
   * Select **Turn on file and printer sharing**.

**A+ Exam Tip**

The A+ Core 2 exam expects you to know the difference between a shared printer and a network printer. A printer installed locally on a computer can be shared with other computers. This is different from a network printer, which is accessed by each networked computer directly through the network.

**OS Differences**

If you want a Windows 8/7 computer to access Homegroup resources, select **Allow Windows to manage homegroup connections (recommended)** under HomeGroup connections.

If you are using NTFS permissions along with less restrictive share permissions to share resources on a network, disable homegroup sharing, which can cause conflicts.

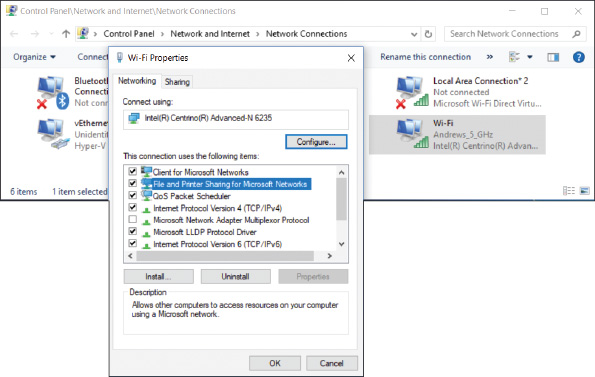
* + If you want to share the Public folder to the network, go to the Public folder sharing section under All Networks and select **Turn on sharing so anyone with network access can read and write files in the Public folders.**
  + If you want the added protection of requiring that all users on the network must have a valid user account and password on this computer, select **Turn on password protected sharing**.

After you have made your changes, click Save changes at the bottom of the window.

1. In the Network and Sharing Center, click **Change adapter settings**. The Network Connections window appears. Right-click the network connection icon and select **Properties** in the shortcut menu. In the Properties box, verify that **File and Printer Sharing for Microsoft Networks** is checked (see [Figure 16-35](javascript://)).

**Figure 16-35**

Verify that the properties for the network connection are set for sharing resources over the connection



Enlarge Image

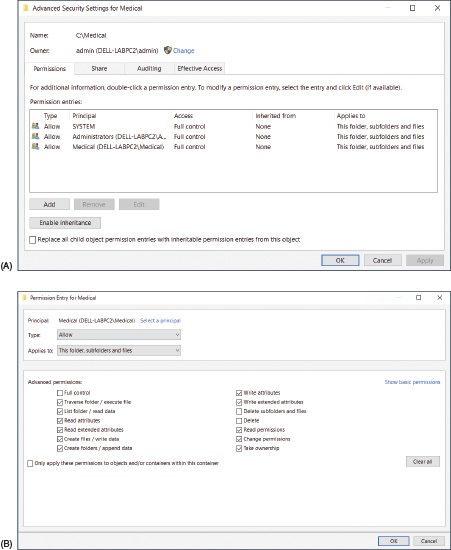
1. The user account name and password on the remote computer must match the user account and password on the host computer. If these accounts and passwords don’t match, the user is considered an anonymous user and is denied access to resources shared on the remote computer. To verify that account names and passwords match, open the Computer Management console, where you can view user account names, create new accounts, and set passwords.

Here are a few tips about managing shared folders and files:

* **Use advanced permissions settings**. If you need further control of the permissions assigned to a user or group, click **Advanced** on the Security tab of a folder’s Properties box. The Advanced Security Settings box appears (see [Figure 16-36A](javascript://)). You can see that the Medical user group was given full control. To change these permission details, double-click the user group. In this example, the Medical group is being edited. The Permission Entry box opens (see [Figure 16-36B](javascript://)). On Windows 10/8 systems only, click **Show advanced permissions**.

**Figure 16-36**

Advanced permissions settings



Enlarge Image

Detailed permissions can now be changed. For example, to prevent users in the Medical group from deleting the Medical folder, its subfolders, and its files, uncheck **Delete subfolders and files** and uncheck **Delete**. Click **OK** to close each box. The resulting change means that users of the Medical group cannot delete or move a file or folder. (They can, however, copy the file or folder.)

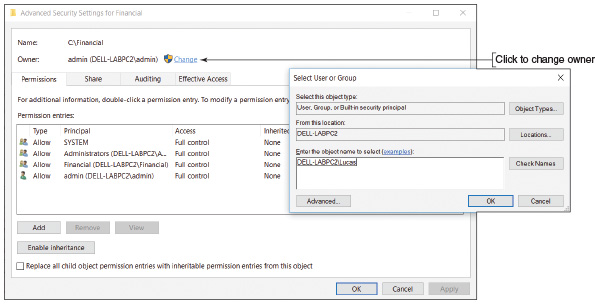
**A+ Exam Tip**

The A+ Core 2 exam expects you to be able to implement permissions so that a user can copy but not move a file or folder and understand how to apply Allow and Deny permissions.

* **Manage permissions using the parent folder.** When a subfolder is created, it is assigned the permissions of the parent folder. Recall that these inherited permissions appear dimmed. The best way to change inherited permissions is to change the permissions of the parent object. In other words, to change the permissions of the C:\Financial\QuickBooks folder, change the permission of the C:\Financial folder. Changing permissions of a parent folder affects all its subfolders.
* **Check the effective permissions.** Permissions manually set for a subfolder or file can override inherited permissions. Permissions that are manually set are called explicit permissions. When a folder or file has inherited an explicit permission set, it might be confusing to know exactly which permissions are in effect for the file or folder. To find out, see the Advanced Security Settings box. (Look back at [Figure 16-36A](javascript://).) NTFS permissions are reported on the Permissions tab and share permissions are reported on the Share tab. Use the Effective Access tab (for Windows 7, the tab is called Effective Permissions) to get a detailed report of resources available to a particular user.
* **Take ownership of a folder.** The owner of a folder always has full permissions for the folder. If you are having a problem changing permissions and you are not the folder owner, try taking ownership of the folder. To do that, click **Advanced** on the Security tab of the folder’s Properties box. The Advanced Security Settings box appears. Next to the name of the owner, click **Change**. You can then enter the name of the new owner (see [Figure 16-37](javascript://)). Click **Check Names** to confirm the name is entered correctly and click **OK** twice.

**Figure 16-37**

Change the owner of a folder



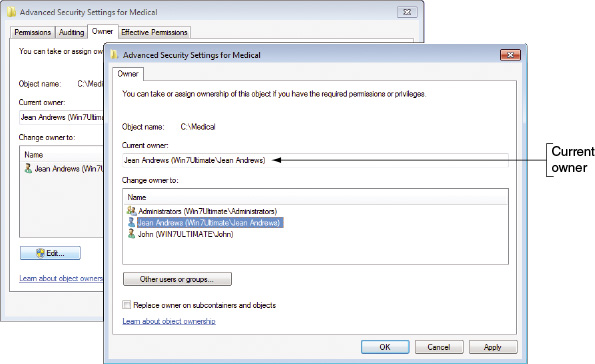
Enlarge Image

**OS Differences**

To change the owner of a folder in Windows 7, open the Advanced Security Settings box, click the **Owner** tab, then click **Edit**. Select a user from the Change owner to list (see [Figure 16-38](javascript://)) and click **Apply** to make that user the new owner. If a user is not listed, click **Other users or groups** and add the user. Close the Advanced Security Settings box and the Properties box, and reopen the Properties box for the change to take effect.

**Figure 16-38**

Change the owner of a folder in Windows 7



Enlarge Image

* **Use only one workgroup**. It is not necessary that all computers belong to the same workgroup in order to share resources. However, performance improves when they are all in the same workgroup.
* **Require passwords for all user accounts.** Don’t forget that for best security, each user account needs a password. In a workgroup, the policy to require that all accounts have passwords is set using Local Group Policy. On a domain, Group Policy is used.
* **Use a mapped network drive.** For the convenience of remote users, map network drives for shared folders that are heavily used. How to do that is coming up next.

Go to pg.

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

Application Opened

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

## 16-2dHow to Map a Network Drive or Network Printer

**A+ Core 2**

* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

A [**network share**](javascript://) is one of the most powerful and versatile methods of communicating over a network. A network share makes one computer (the client) appear to have a new hard drive, such as drive E:, that is really hard drive space on another host computer (the server). The client computer creates and saves a shortcut associated with a drive letter that points to the host computer’s shared folder or drive. This is called [**mapping**](javascript://) the drive. This client/server arrangement is managed by a Windows component, the [**Network File System (NFS)**](javascript://), which makes it possible for files on the network to be accessed as easily as if they are stored on the local computer. NFS is a type of distributed file system (DFS), which is a system that shares files on a network. Even if the host computer uses a different OS, such as macOS or Linux, the network share still functions. In addition to mapping a network drive, you can also map a network printer to a computer.

**Notes**

A network-attached storage (NAS) device provides hard drive storage for computers on a network. Computers on the network can access this storage using a mapped network drive.

**Applying Concepts**

### Mapping a Network Drive and Network Printer

To set up a network drive, follow these steps:

1. On the host computer, share the folder or entire volume to which you want others to have access.
2. On the remote computer that will use the network drive, open File Explorer. In the left pane, click **This PC**. At the top of the window, click the **Computer** tab and click **Map network drive**. (Alternately, you can right-click a folder you see shared on the network and click **Map network drive**.)

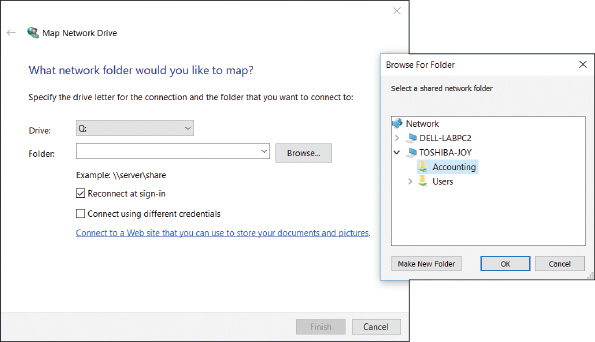
**OS Differences**

On a remote computer running Windows 7, open Windows Explorer and press **Alt** to display the menu bar. Click the **Tools** menu and select **Map network drive**.

1. The Map Network Drive dialog box opens, as shown on the left side of [Figure 16-39](javascript://). Select a drive letter from the drop-down list.

**Figure 16-39**

Mapping a network drive to a host computer



Enlarge Image

1. Click the **Browse** button and locate the shared folder or drive on the host computer (see the right side of [Figure 16-39](javascript://)). Click **OK** to close the Browse For Folder dialog box, and click **Finish** to map the drive. The folder on the host computer now appears as one more drive in Explorer on your computer.

**Notes**

When mapping a network drive, you can type the path to the host computer rather than clicking the Browse button to navigate to the host. To enter the path, open the Map Network Drive dialog box and use two backslashes followed by the name of the host computer, followed by a backslash and the drive or folder to access on the host computer. For example, to access the Projects folder on the computer named Win8, enter **\\Win8\Projects** and then click **Finish**.

If a network drive does not work, go to the Network and Sharing Center and verify that the network connection is good. You can also use the net use command to solve problems with mapped network drives. You learned about the net use command in [Chapter 7](javascript://).

**Notes**

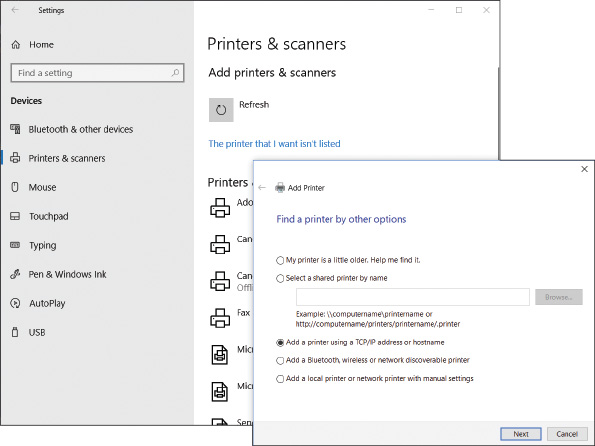
A host computer might be in sleep mode or powered down when a remote computer attempts to make a mapped drive connection at startup. To solve this problem, configure the host computer for Wake-on-LAN, as you learned in [Chapter 7](javascript://).

Recall from [Chapter 14](javascript://) that you can connect a network printer to a server and the server can share the printer on the network. The Print Management console can be used to manage all shared printers on the network from a single workstation. You can also map a network printer directly to your computer, eliminating a print server or printer sharing from the process. Here’s how:

1. In Windows 10, open the **Settings** app, select the **Devices** group, and then click **Printers & scanners**. A list of installed printers and scanners appears. Click **Add a printer or scanner**. Windows searches for available printers and scanners, but probably will not find the network printer. Click **The printer that I want isn’t listed**. In the Add Printer box (see [Figure 16-40](javascript://)), select **Add a printer using a TCP/IP address or hostname** and click **Next**.

**Figure 16-40**

Select a network printer identified by its IP address or host name



Enlarge Image

1. Enter the printer’s IP address and click **Next**. Windows searches the network for the printer. If it finds the printer, the installation proceeds and you can select the printer manufacturer and model. Alternately, you can provide printer drivers that you can download to your computer. After the printer is installed, be sure to print a test page.

**OS Differences**

To install a network printer for Windows 8/7 systems, open **Control Panel** in Classic view and click **Devices and Printers**. Click **Add a printer**. Windows 8/7 will most likely find and list the network printer. Be sure to select a printer that shows its IP address; otherwise, you are connecting to a computer that has shared the printer to the network. If the printer doesn’t appear in the list, click **The printer that I want isn’t listed**, enter the name of the printer or its IP address, and click **Next**.

If you have problems mapping to a network printer, download the printer drivers from the website of the printer manufacturer and follow the manufacturer’s directions to install the printer.

Go to pg.

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

Application Opened

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

## 16-2eSync Center and Offline Files

**A+ Core 2**

* 1.6

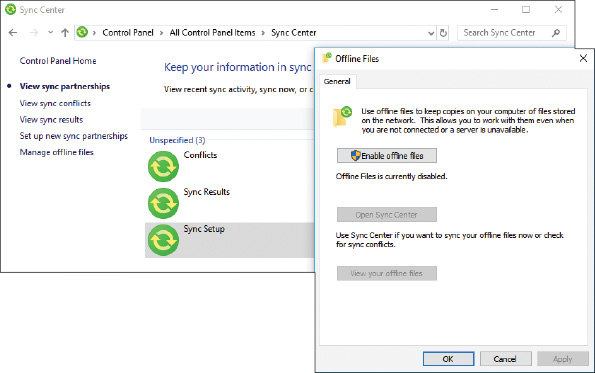
Given a scenario, use Microsoft Windows Control Panel utilities.

[**Sync Center**](javascript://), an applet in Control Panel, allows two computers to sync the contents of a shared folder or volume. When you set up a folder to work offline, your computer can work with the folder even when your computer is not connected to the remote computer that holds the share because Sync Center keeps a copy of the files on the local computer. Later, when the computer reconnects to the network, Sync Center can sync up the local and remote files, resolving any conflicts that might have happened if files were edited at both locations. Follow these steps to use Sync Center:

1. Go to **Control Panel** and open **Sync Center**. The Sync Center window appears (see [Figure 16-41](javascript://)). To enable offline files, click **Manage offline files**. In the box that appears, click **Enable offline files** and click **OK**. You must restart the computer.

**Figure 16-41**

Enable offline files so you can use Sync Center

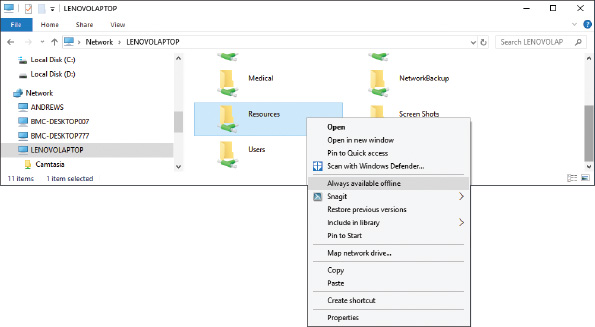


Enlarge Image

1. Using File Explorer or Windows Explorer, right-click a shared folder on the network and click **Always available offline** (see [Figure 16-42](javascript://)). Alternately, you can select the folder, open the **Home** menu, click **Easy access**, and click **Always available offline**.

**Figure 16-42**

Configure a network share as an offline folder

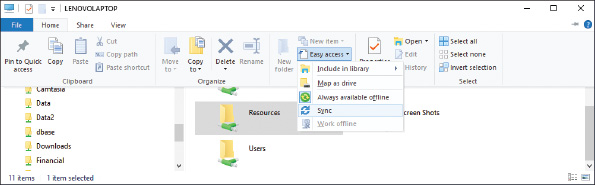


Enlarge Image

1. The folder will sync on your computer and the remote computer. (On your computer, offline files are stored in the C:\Windows\CSC folder.) When your network connection is slow or disconnected, you can continue to use the folder on your computer.
2. Later, when your computer and the remote computer are connected, you can force a manual sync of the files in the folder. In File Explorer, select the folder, open the **Home** menu, click **Easy access**, and click **Sync**. See [Figure 16-43](javascript://).

**Figure 16-43**

Manually force an offline folder to sync with the network share



Enlarge Image

**Notes**

OneDrive is cloud storage associated with your Microsoft account and stored in the Microsoft Cloud. To make OneDrive folders available offline when you are not connected to the Internet, right-click a folder in OneDrive and click **Always available offline**.

Go to pg.

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

Application Opened

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

## 16-2fHidden Network Resources and Administrative Shares

**A+ Core 2**

* 1.8

Given a scenario, configure Microsoft Windows networking on a client/desktop.

* 2.6

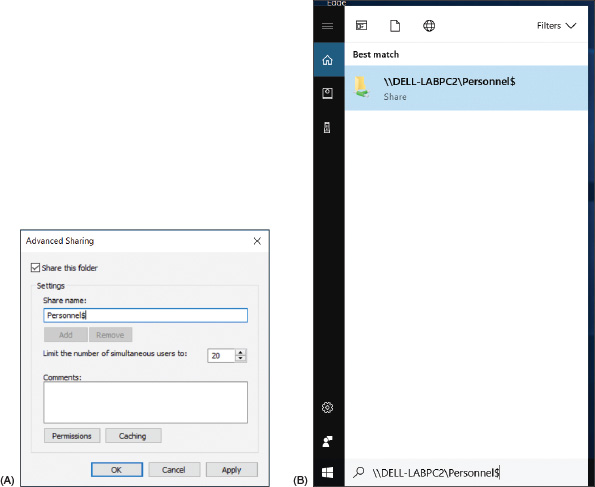
Compare and contrast the differences of basic Microsoft Windows OS security settings.

Sometimes your goal is to ensure that a folder or file is not accessible from the network or by other users, or is secretly shared on the network. When you need to protect confidential data from users on the network, you can do the following:

* **Disable File and Printer Sharing**. If no resources on the computer are shared, use the Network and Sharing Center to disable File and Printer Sharing for Microsoft Networks.
* **Hide a shared folder**. If you want to share a folder but don’t want others to see the shared folder in File Explorer or Windows Explorer, add a $ to the end of the share name in the Advanced Sharing box, as shown in [Figure 16-44A](javascript://). This shared and hidden folder is called a [**hidden share**](javascript://). Others on the network can access the folder only when they know its name. For example, to access a shared folder named Personnel$ on the computer named DELL-LABPC2, a user must enter \\**DELL-LABPC2**\**Personnel$** in the search box (see [Figure 16-44B](javascript://)) on the remote computer and press **Enter**. The user on the remote computer can also search for the hidden share’s location using the search box in File Explorer or Windows Explorer.

**Figure 16-44**

(A) A $ at the end of the share name hides the share unless the exact name is used to locate it; (B) access a hidden, shared folder on the network by searching for its exact name



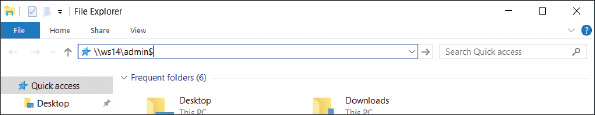
Enlarge Image

So far in this chapter, you have learned about folders and files on a computer that are shared with other users on the network; these shares are called [**local shares**](javascript://). For computers that belong to a domain, you need to be aware of another way folders are shared, called administrative shares. [**Administrative shares**](javascript://) are folders shared by default that administrator accounts at the domain level can access. You don’t need to manually share these folders because Windows automatically does so by default. Two types of administrative shares are:

* **The %systemroot% folder**. Enter the path **\\computername\admin$** to access the %systemroot% folder (most likely the C:\Windows folder) on a remote computer in order to work with that computer’s system folders and files. For example, to connect to the ws14 workstation shown in [Figure 16-45](javascript://), the entry in the Explorer address bar is **\\ws14\admin$**. The authenticate box appears; enter **Administrator** as the user name and the password to the Administrator account. The admin$ administrative share is called the [**Remote Admin share**](javascript://).

**Figure 16-45**

Access an administrative share on a domain



Enlarge Image

* **Any volume or drive**. To access the root level of any volume or drive on the network, enter the computer name and drive letter followed by a $—for example, **\\ws14\C$**.

**A+ Exam Tip**

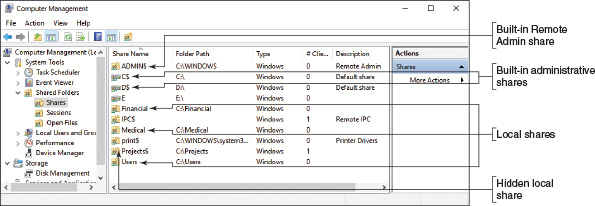
The A+ Core 2 exam expects you to understand the difference between administrative shares and local shares.

**Notes**

To see a list of all shares on a computer, open the Computer Management console and drill down to **System Tools**, **Shared Folders**, **Shares** (see [Figure 16-46](javascript://)).

**Figure 16-46**

Use the Computer Management console to view all shares



Enlarge Image

**Caution**

When supporting a workgroup, you might be tempted to share all the drives on all computers so that you can have easy access remotely. However, using local shares in this way is not a good security practice. Don’t share the \Windows folder or an entire drive or volume on the network. These local shares appear in everyone’s Explorer window. You don’t want your system files and folders exposed like this.

Go to pg.

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

Application Opened

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

**16-3**Using Active Directory Domain Services

**A+ Core 2**

* 2.2

Explain logical security concepts.

* 2.7

Given a scenario, implement security best practices to secure a workstation.

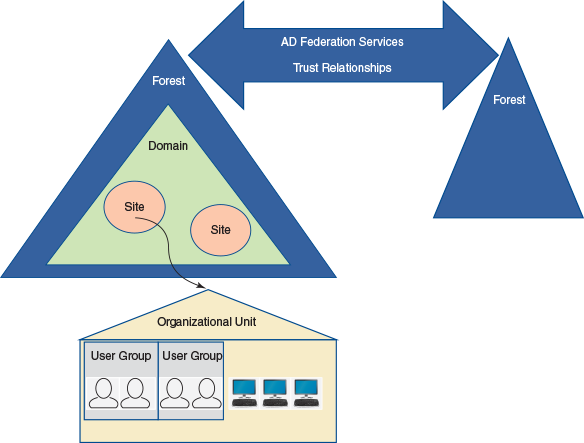
**Active Directory (AD)** is a suite of services and databases provided by Windows Server that is used to manage Windows domains, including access to the domain and what users and computers can do in the domain. AD incorporates five groups of services:

* [**Active Directory Domain Services (AD DS)**](javascript://) authenticates accounts and authorizes what these accounts can do.
* AD Certificate Services (AD CS) secures identities of services, computers, and users.
* AD Federation Services (AD FS) secures trust relationships with outside organizations.
* AD Rights Management Services (AD RMS) secures data.
* AD Lightweight Directory Services (AD LDS) secures applications.

Active Directory organizes resources in a top-down hierarchical structure, as shown in [Figure 16-47](javascript://). Users and resources of a company or school managed by AD are organized into a [**forest**](javascript://) (the entire enterprise), which contains a domain (for example, [mycompany.com](http://mycompany.com/" \t "_blank)). For a few very large enterprises, domains can contain subdomains (for example, [mycompany.com](http://mycompany.com/" \t "_blank) and [mycompany-dev.com](http://mycompany-dev.com/" \t "_blank)), but in most situations, a forest contains only a single domain. Domains can contain sites (for example, a New York branch office and a San Francisco branch). Domains are also organized into organizational units and sub-organizational units.

**Figure 16-47**

The Active Directory organizational structure

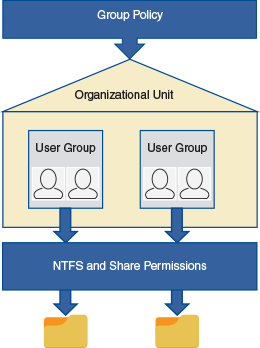


An [**organizational unit (OU)**](javascript://) is created to make it easier for technicians to assign privileges to users and computers in the OU; privileges are assigned using policies created by Group Policy. These policies are contained in [**Group Policy Objects (GPOs)**](javascript://) that are applied to each user and computer in the OU.

An OU also can contain user groups, which contain users. Permissions assigned to folders work much the same way as they do in Windows 10/8/7. NTFS and share permissions are assigned to a folder on a server in the domain by assigning permissions to a user group, and the users in this group inherit these assigned permissions. In summary, managing resources in AD revolves around the tools shown in [Figure 16-48](javascript://).

**Figure 16-48**

Group policies apply to OUs, and NTFS and share permissions apply to folders to control access to the resources in a domain



In this chapter, we focus on the skills an IT technician needs to manage user accounts with Active Directory Domain Services, including creating, resetting, unlocking, enabling, and disabling user accounts and resetting user account passwords. You also learn how Group Policy can be used to assign privileges to an OU and the groups and users in the OU.

Go to pg.

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

Application Opened

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

## 16-3aCreating and Managing User Accounts in AD

**A+ Core 2**

* 2.2

Explain logical security concepts.

* 2.7

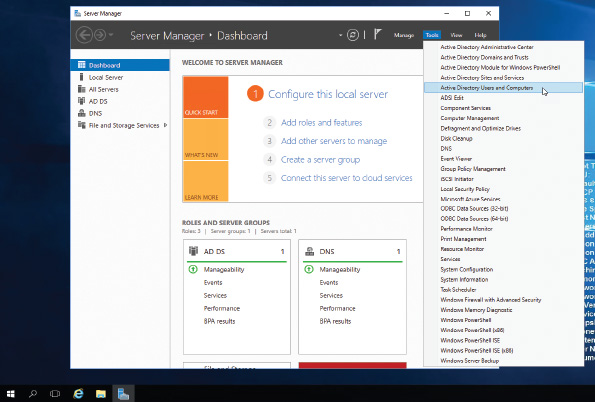
Given a scenario, implement security best practices to secure a workstation.

Before we discuss how to manage a user account on a Windows domain, let’s pause to see how you can access Domain Services on the domain controller to get to the tools you need. You’ll need a local administrator account for a Windows Server computer that is a domain controller. Then you can use one of these methods to access the domain controller:

* **Sitting at the computer**. While physically seated at the Windows Server computer, sign in to Windows Server with an administrator account. Then click **Start** and click **Server Manager** in the Start menu. The Server Manager console is shown in [Figure 16-49](javascript://) with the Tools menu open. The [**Server Manager**](javascript://) console contains the tools used to manage Active Directory and is included in Windows Server. It can also be installed in Windows 10.

**Figure 16-49**

The Windows Server desktop with the Server Manager console showing the Tools menu



Enlarge Image

* **Remote access to Windows Server**. You can use Remote Desktop from anywhere on the Internet to connect to a Windows Server computer, sign in, and open Server Manager. How to use Remote Desktop is covered in [Chapter 13](javascript://). Recall that Remote Desktop requires the host computer to have a static IP address; you can expect a domain controller to have one.
* **AD Administrative Center and PowerShell**. Administrative Center is an interface for managing Active Directory. In Windows 10/8/7, you can download and install Remote Server Administrative Tools (RSAT) from [microsoft.com](http://microsoft.com/" \t "_blank). Administrative Center is one of the tools in this package. Many PowerShell cmdlets apply to Active Directory. To use PowerShell to manage Active Directory, you must first execute the cmdlet **Import-Module ActiveDirectory**, which installs the AD cmdlets.

**Notes**

If you don’t have access to Active Directory and a Windows domain to practice the skills in this part of the chapter, you can follow the steps in [Real Problem 16-2](javascript://) at the end of this chapter to set up your own Windows domain in Windows Server using the free Google Cloud Platform at cloud.google.com.

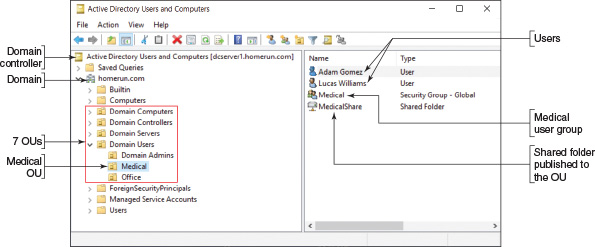
### Use Server Manager and Create a New User

Let’s get started learning to use Server Manager. In Server Manager, follow these steps to view the OU structure and create a new user:

1. Sign in to Windows Server with an administrator account and open **Server Manager**.
2. Click **Tools** (refer back to [Figure 16-49](javascript://)) and click **Active Directory Users and Computers**. (The utility is also available in Control Panel under Administrative Tools.) The Active Directory Users and Computers window displays. [Figure 16-50](javascript://) shows the sample domain [homerun.com](http://homerun.com/" \t "_blank), which belongs to our fictitious company, Homerun Sports Medicine, Inc.

**Figure 16-50**

Users, computers, and OUs in the domain



Enlarge Image

There are seven OUs currently in the domain:

* + Domain Controllers is a default OU created when the domain was created. It contains all the domain controllers managing Active Directory. Our controller is named dcserver1.
  + Domain Computers, Domain Servers, and Domain Users were created by the system administrator directly under the [homerun.com](http://homerun.com/" \t "_blank) domain so that appropriate policies can more easily be applied to these OUs.
  + Domain Users contains three OUs: Domain Admins, Medical, and Office.
  + The Medical OU is selected, and you can see it contains two users, one user group, and one shared folder. (If you drill down into the Medical user group, you can see that Adam Gomez and Lucas Williams are members of the group.) It’s okay to give a user group the same name as an OU, but it can sometimes get confusing, depending on the situation.

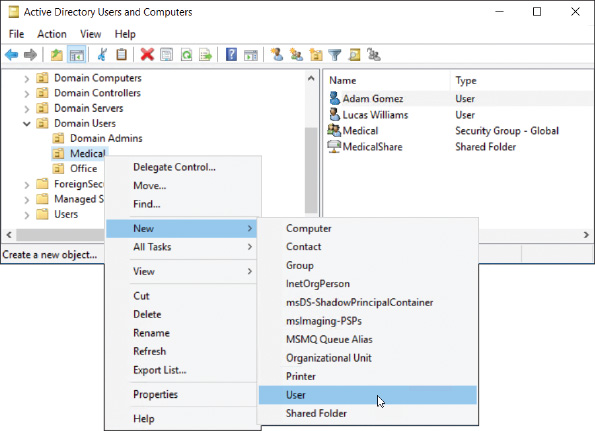
**Notes**

To share a folder in Active Directory, first set the folder’s NTFS and share permissions for the user group, as you learned to do earlier in the chapter. Then, to publish the folder in AD, right-click the OU to which you want to include the folder, click **New**, click **Folder**, and point to the folder. The folder is published in AD and can be found by users signed in to the domain on client computers.

1. To add a new user, right-click the OU to which you want to add the user, point to **New**, and click **User** (see [Figure 16-51](javascript://)).

**Figure 16-51**

Right-click the OU to create a new user

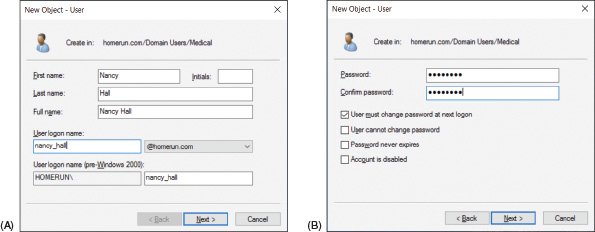


Enlarge Image

1. Enter the user’s first name, last name, and user name (see [Figure 16-52A](javascript://)). Click **Next**. On the next screen, decide how to handle the password (see [Figure 16-52B](javascript://)).

**Figure 16-52**

To create a new user, (A) enter a name and logon name, and (B) decide how to handle the password



Enlarge Image

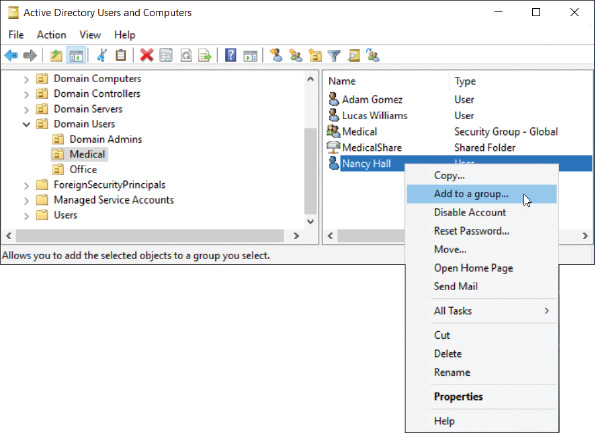
Here are the best practices for these password options:

* + Always require a password.
  + By default, the password you enter must meet AD’s complexity requirements: It must have at least eight lowercase and uppercase letters, numbers, and symbols, and it cannot contain any three consecutive letters in the user name or display name.
  + The best practice is to require the user to change the password at next logon.
  + Don’t check Password never expires. It’s a good idea for the user to occasionally change the password.
  + Notice you can select Account is disabled. This might be appropriate when you are setting up an account well in advance of the account actually being used.

1. Click **Next** and click **Finish**. The account is created. To confirm that the account is created in the correct OU, click the OU; the account should be listed in the right pane.
2. After the account is created, you can add it to an existing user group. Right-click the user account and click **Add to a group** (see [Figure 16-53](javascript://)).

**Figure 16-53**

Add the user account to an existing user group

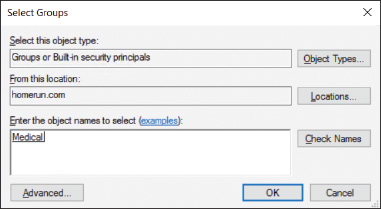


Enlarge Image

1. Type the group name and click **Check Names**. Windows verifies the name of the group and confirms it by underlining the name. Click **OK** (see [Figure 16-54](javascript://)).

**Figure 16-54**

Type the user group name and click Check Names



**Notes**

To create a new user group, right-click the OU where you want to add the group, click **New**, and click **Group**. You can then name the group.

Recall that users belong to user groups and users and user groups belong to OUs. When a policy is applied to an OU, it is applied to all users and user groups in the OU. When folder permissions are assigned to a user group, they are assigned to all users in the user group.

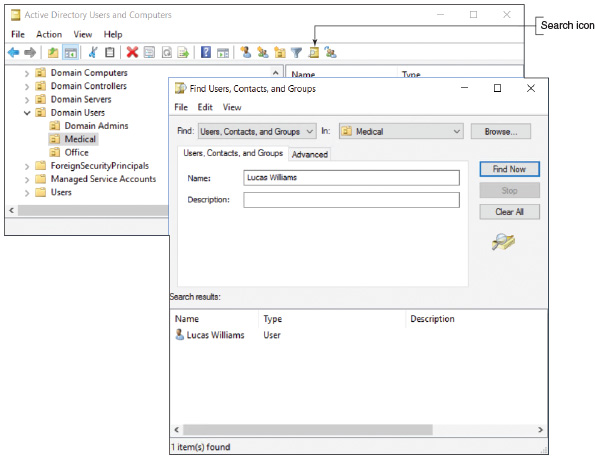
### Manage Accounts and Passwords

An account might get locked after too many failed attempts to sign in. If the user says she knows the password but the account is locked, do the following to unlock the account:

1. An enterprise domain is likely to have hundreds if not thousands of user accounts. Do one of the following to locate the account:
   * If you don’t know where to find the account, you can use the search utility. Click the search icon in the Active Directory Users and Computers window (see [Figure 16-55](javascript://)).

**Figure 16-55**

Search for a user account



Enlarge Image

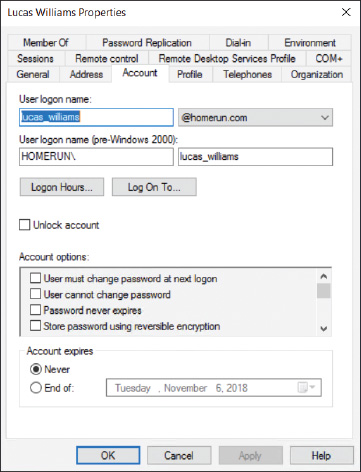
At the top of the Find Users, Contacts, and Groups box, notice you can filter the search using the drop-down menus. Enter the name of the account and click **Find Now**. Double-click the account in the list of matches that appears. The account’s Properties box appears.

* + If you know where to find the account, drill down to it, right-click it, and select **Properties**.

1. In the Properties box for the account, select the **Account** tab (see [Figure 16-56](javascript://)), check **Unlock account**, and click **Apply**. The user should then be able to sign in.

**Figure 16-56**

Unlock a locked account

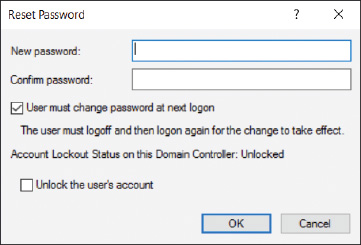


Follow these steps to reset a forgotten password and disable, enable, or delete an account:

1. Locate the account and right-click it. In the shortcut menu, click **Reset Password** (refer back to [Figure 16-53](javascript://)). In the Reset Password box (see [Figure 16-57](javascript://)), enter a new password twice. It’s a good idea to leave the User must change password at next logon box checked. If the account has been locked, check **Unlock the user’s account**. Click **OK**.

**Figure 16-57**

Reset the user password



1. In the account’s shortcut menu in [Figure 16-53](javascript://), note the options to disable and delete an account. When you click **Disable Account**, the user cannot sign in, but the account’s user profile still exists and you can later enable the account using the same shortcut menu. Click **Delete** to delete the account, which deletes the user profile. You can also disable and enable an account and designate when an account will expire using options on the Account tab of the user’s Properties box.

**Notes**

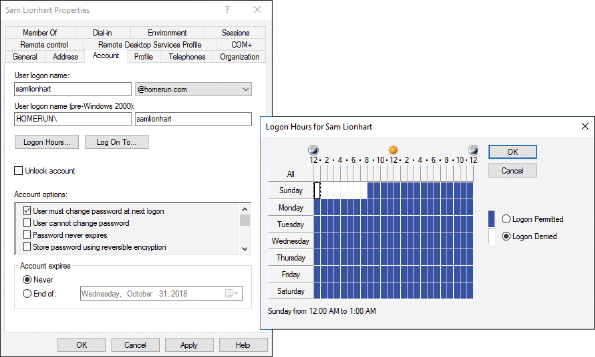
The user account is considered an object in Active Directory. When you delete an AD object, it goes to the Active Directory Recycle Bin, where it can be recovered until the Recycle Bin is emptied.

Here are a few other tips to help you manage accounts in Active Directory:

* **Disable the Guest account**. In Active Directory, the Guest account is disabled by default. For best security, leave the account disabled. If you find the Guest account enabled, right-click it and select **Disable Account**.
* **Logon time restrictions**. By default, a user can sign in to AD at any time. Suppose, however, that midnight to 8:00AM every Sunday is restricted for routine maintenance. To set logon time restrictions, open the user’s Properties box, select the **Account** tab, and click **Logon Hours** (see [Figure 16-58](javascript://)). Click an hour and then click **Logon Denied**. Notice that in [Figure 16-58](javascript://), midnight to 8:00AM on Sunday is denied.

**Figure 16-58**

Logon time restrictions



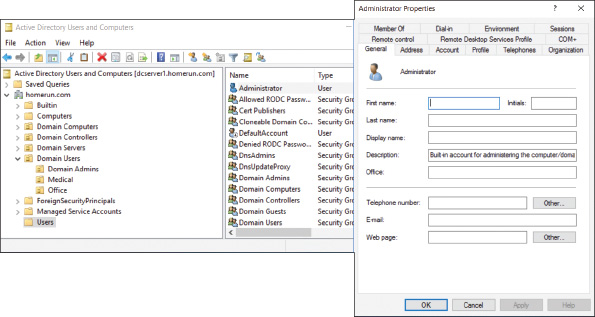
Enlarge Image

* **Timeout and screen lock**. On the Sessions tab of the user’s Properties box, you can limit how long a session remains disconnected before it ends (never or up to 2 days), how long an active session stays up (never or up to 2 days), and how long an idle session stays up. After you have made your selections, click **Apply** to save changes.
* **Administrator password**. Before AD Domain Services can be configured to be a domain controller on the network, the Administrator account on its computer must have a strong password (including lowercase and uppercase letters, numbers, and symbols). To manage the properties of the Administrator account, open **Users** in the **Active Directory Users and Computers** window, right-click **Administrator**, and click **Properties**. See [Figure 16-59](javascript://). To change the password of the Administrator account, you can use the following command in an elevated command prompt window in Windows Server:



**Figure 16-59**

Manage the properties of the Administrator account



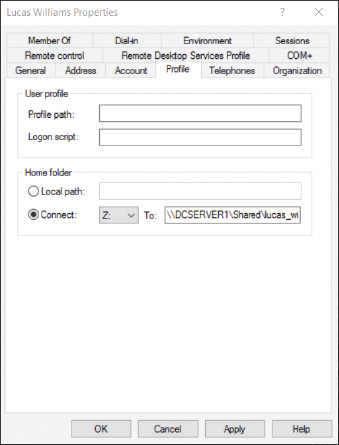
Enlarge Image

* **Home folder**. The [**Home folder**](javascript://) is the default folder that is presented to the user whenever she is ready to save a file. On a peer-to-peer network, the Home folder in Windows is normally the Documents folder in the user profile at C:\Users\username\Documents. Active Directory is able to change this Home folder location to a share on the network, which is called [**folder redirection**](javascript://). Two reasons to apply folder redirection to the Home folder are:
  + On a domain, a user might sign in to different computers. When his Home folder is stored on the network, it’s always available and does not need to be copied to each computer he uses.
  + It’s easier for backups to be maintained when all Home folders are on a network server rather than on individual workstations. In an organization, individual workstations are generally not backed up regularly, but servers on the network are backed up at least every night.

To see if a user’s Home folder is on his local computer or on the network, select the **Profile** tab of the user’s Properties box (see [Figure 16-60](javascript://)). For this user, the Home folder is in a network share.

**Figure 16-60**

This user’s Home folder is contained in a network share



**Notes**

Many corporations are beginning to use cloud services rather than managing data on their premises. One way to do this is to set up OneDrive in the Microsoft cloud for each user in the Windows domain. Users are then encouraged to use their OneDrive for personal files rather than their Home folders stored on a network share.

* **Logon scripts**. A logon script is a list of commands stored in a script file that is performed each time a user signs in to Windows. In Active Directory, logon scripts are normally stored on the domain controllers in a network share named Netlogon. Types of logon scripts supported by Active Directory include Windows batch files (.bat file extension), VBScript files (.vbs file extension), and PowerShell scripts (.ps2 file extension). After the script file is stored in the Netlogon share, select the **Profile** tab in the user’s Properties box. See [Figure 16-60](javascript://). Under Logon script, enter the name of the script file along with its file extension.

Normally, when you want to change a setting for a single user, you use the user’s Properties box, as just explained. If you need to change settings for all the users in an OU, the best tool to use is Group Policy because these policies affect multiple users.

Go to pg.

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

Application Opened

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

## 16-3bGroup Policy Objects

**A+ Core 2**

* 2.2

Explain logical security concepts.

* 2.7

Given a scenario, implement security best practices to secure a workstation.

Group Policy can be used on the domain controller to create Group Policy Objects, which contain policies that apply to an OU. These OU policies apply to users, computers, shared folders, and printers in the OU.

Using Group Policy to manage GPOs is beyond the scope of this text. However, let’s take a quick look at how you would get started to create and edit a GPO.

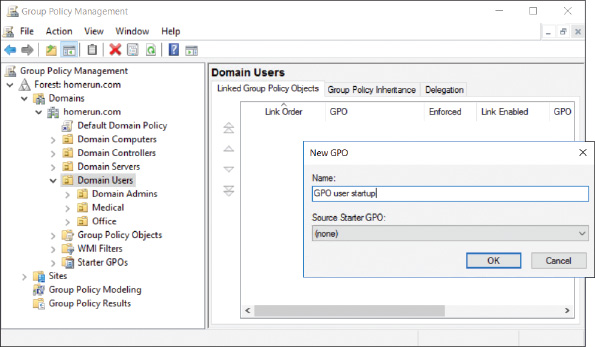
### Create and Edit a GPO

You learned earlier that you can use the user account Properties box to set a logon script for a single user. Here is how to create a GPO to set a policy to run a startup script for all users in the domain or an OU:

1. In the Server Manager window, click **Tools** and click **Group Policy Management**. (The tool is also available in Administrative Tools in Control Panel.)
2. In the Group Policy Management window (see [Figure 16-61](javascript://)), drill down into the OUs to find the one to which you want to apply the GPO. Right-click the OU and click **Create a GPO in this domain, and Link it here**. You can then name the GPO, as shown in the figure, and click **OK**.

**Figure 16-61**

Create a new GPO for the Domain Users OU

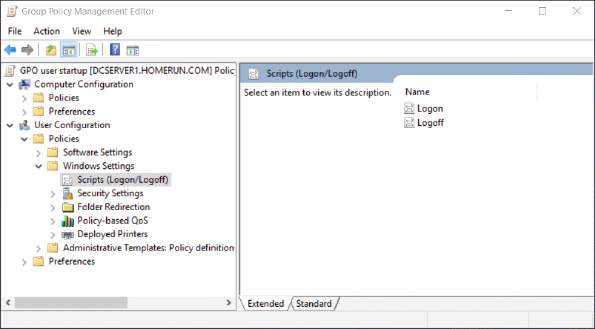


Enlarge Image

1. The new GPO appears in the list under the OU and in the Group Policy Objects list. To display details about the GPO, click it and click **OK**. The GPO details display in the right pane with the Settings tab selected.
2. To edit a GPO, right-click it in the left pane and click **Edit**. The Group Policy Management Editor window opens so you can edit the GPO. You can see the GPO name at the top of the left pane of the editor (see [Figure 16-62](javascript://)).

**Figure 16-62**

Drill down into the policies to find the ones you need



Enlarge Image

1. Just as with Local Group Policy, policies apply to either the computer or the user. You can drill down into the Computer Configuration or User Configuration policies and find and set the ones you want. For example, to add a login script for all users in the OU to which the GPO belongs, drill down in the **User Configuration**, **Policies**, **Windows Settings**, **Scripts (Logon/Logoff)** group, as shown in [Figure 16-62](javascript://).
2. When you’re done setting policies, close the GPO editor to return to the Group Policy Management window.
3. GPO updates are automatically pushed down to clients on the domain in the same site in just a few minutes. On a client computer, just as with Local Group Policy, you can use the **gpupdate /force** command to apply new policies to the client.

### Which Policy Wins

Sometimes policies overlap or conflict. Here is the order in which policies are applied; the last policy to be applied wins:

1. **Local**. All local policies are applied first. As you learned earlier, Local Group Policy on the local computer can create policies that apply to the local computer or users.
2. **Site**. Policies for sites are applied next.
3. **Domain**. Policies for a domain are applied next.
4. **OU**. Policies for an OU are applied next and then policies for sub-OUs are applied next.
5. **Enforced**. Policies that are tagged as Enforced policies are applied last and always win over other policies.

**Notes**

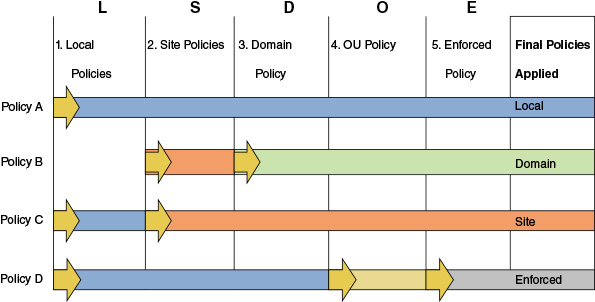
To tag a GPO as Enforced, right-click the GPO in the Group Policy Management window and click **Enforced**.

Where there is a conflict of policies, the last policy applied wins. It’s important to remember the order in which policies are applied, and the acronym LSDOE (usually pronounced “LS-doe”) can help: Local, Site, Domain, OU, and Enforced.

[Figure 16-63](javascript://) shows what can happen when there are conflicting policies. In the figure, you see that policies A, B, C, and D are applied; to understand which policy is applied at each level, follow the diagram from left to right. First, notice that local policy A wins because policy A does not exist at the site, domain, OU, or enforced level. For policy B, domain policy B wins over site policy B. For policy C, site policy C wins over local policy C. Although OU policy D would have won over local policy D, the OU policy D was not applied because it was overridden by enforced policy D. Therefore, the resultant policies are local policy A, domain policy B, site policy C, and enforced policy D.

**Figure 16-63**

Resulting policies applied when conflicting policies exist



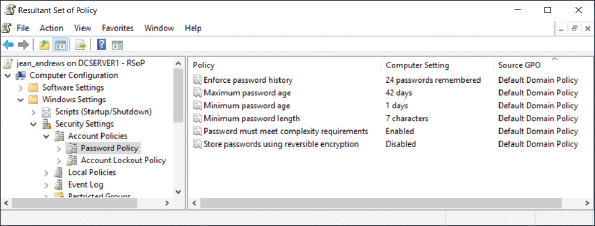
Enlarge Image

To find out the resulting policies for the computer or user, do one of the following:

* In a command prompt window, enter the **rsop.msc** command. The [**Resultant Set of Policy (RSoP)**](javascript://) window opens, where you can drill down to see the policies set for the computer or user. For example, [Figure 16-64](javascript://) shows the RSoP for the Password Policy.

**Figure 16-64**

The Resultant Set of Policy for the Password Policy

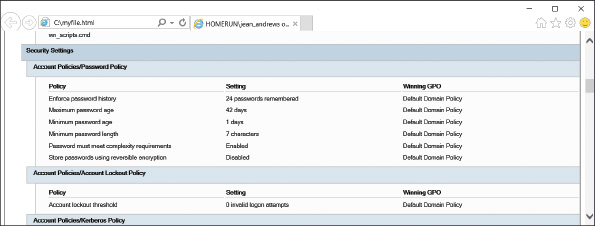


Enlarge Image

* In a command prompt window, enter the **gpresult /v** command, which displays the policies currently applied to the computer and user. The report is very long; you can save it to an HTML file so you can later search it. For example, use this command: **gpresult /h C:\myfile.html**. To view the file, double-click it in File Explorer. The HTML file opens in Internet Explorer. [Figure 16-65](javascript://) shows a snip of the file that includes the Password Policy.

**Figure 16-65**

The gpresult output displayed as an HTML file in Internet Explorer



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

## 16-4a**Chapter Summary**

### Securing a Windows Personal Computer

* A long password is a strong password.
* Use Local Group Policies (gpedit.msc) and Local Security Policies (secpol.msc) to secure a Windows computer.
* The Internet Options dialog box is used to manage many Internet Explorer settings. Proxy settings are managed using the Connections tab, and add-ons are managed using the Programs tab.
* Encrypting File System (EFS) encrypts files and folders on an NTFS file system. BitLocker Drive Encryption encrypts an entire volume on a hard drive. Both are available on business and professional editions of Windows.

### Controlling Access to Folders and Files

* Access to folders and files on a network is controlled by assigning privileges to user accounts and assigning permission to folders and files.
* Apply the principle of least privilege when assigning privileges to users. You can change the privileges of an account by adding it to or removing it from a user group.
* You can create customized user groups to make it easier to manage privileges to multiple user accounts.
* Two ways to share files and folders on the network are to use workgroup sharing and domain controllers. With workgroup sharing, you can use share permissions and/or NTFS permissions. For Windows 8/7, when all users on a small network require the same access to all resources, you can use a Windows 8/7 homegroup. Peer-to-peer networks use local shares, and a Windows domain supports administrative shares. You can also hide network resources so that a user must know the name of the resource to access it.
* A mapped network drive makes it easier for users to access drives and folders on the network.

### Using Active Directory Domain Services

* Active Directory (AD) is a suite of services and databases provided by Windows Server that is used to manage Windows domains.
* Active Directory organizes resources in a top-down hierarchical structure. A forest contains a domain. Domains can contain sites. Domains are also organized into organizational units (OUs) and sub-organizational units.
* Managing resources in AD revolves around the OU, user groups, and NTFS and share permissions. Group Policies apply to OUs, and NTFS and share permissions apply to folders to control access to the resources in a domain.
* Active Directory is able to change the Home folder location to a share on the network, which is called folder redirection.
* The order in which group policies are applied are: local, site, domain, OU, and enforced. Where there is a conflict in policies, the last policy applied wins.

Go to pg.

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

Application Opened

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

# Chapter Review

## 16-4b**Key Terms**

For explanations of key terms, see the Glossary for this text.

* **Active Directory (AD)**
* [**Active Directory Domain Services (AD DS)**](javascript://)
* [**ActiveX control**](javascript://)
* [**administrative shares**](javascript://)
* [**Administrators group**](javascript://)
* [**Anonymous users**](javascript://)
* [**Authenticated Users group**](javascript://)
* [**BitLocker Drive Encryption**](javascript://)
* [**BitLocker To Go**](javascript://)
* [**brute force attack**](javascript://)
* [**defense in depth**](javascript://)
* [**Encrypting File System (EFS)**](javascript://)
* [**Everyone group**](javascript://)
* [**folder redirection**](javascript://)
* [**forest**](javascript://)
* [**gpresult**](javascript://)
* [**gpupdate**](javascript://)
* **Group Policy**
* [**Group Policy Object (GPO)**](javascript://)
* [**Guests group**](javascript://)
* [**hidden share**](javascript://)
* [**Home folder**](javascript://)
* [**inherited permissions**](javascript://)
* [**Internet Options**](javascript://)
* **Local Group Policy**
* [**Local Security Policy**](javascript://)
* [**local shares**](javascript://)
* [**Local Users and Groups**](javascript://)
* [**mapping**](javascript://)
* **multifactor authentication (MFA)**
* [**Network File System (NFS)**](javascript://)
* [**Network Places Wizard**](javascript://)
* [**network share**](javascript://)
* [**NTFS permissions**](javascript://)
* [**organizational unit (OU)**](javascript://)
* [**permission propagation**](javascript://)
* [**permissions**](javascript://)
* [**Power Users group**](javascript://)
* [**principle of least privilege**](javascript://)
* [**privileges**](javascript://)
* [**Remote Admin share**](javascript://)
* [**Resultant Set of Policy (RSoP)**](javascript://)
* [**Server Manager**](javascript://)
* [**share permissions**](javascript://)
* [**strong password**](javascript://)
* [**Sync Center**](javascript://)
* **TPM (Trusted Platform Module)**
* [**Users group**](javascript://)
* [**Windows Firewall**](javascript://)

Go to pg.

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

Application Opened

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

# Chapter Review

## 16-4c**Thinking Critically**

These questions are designed to prepare you for the critical thinking required for the A+ exams and may use content from other chapters and the web.

1. Your organization has set up three levels of classification for data accessed by users on a small network:
   * Low security: Data in the C:\Public folder
   * Medium security: Data in a shared folder that some, but not all, user groups can access
   * High security: Data in a shared and encrypted folder that requires a password to access. The folder is shared only to one user group.

Classify each of the following sets of data:

* + Directions to the company’s Fourth of July party
  + Details of an invention made by the company president that has not yet been patented
  + Résumés presented by several people applying for a job with the company
  + Payroll spreadsheets
  + Job openings at the company

1. You work in the Accounting department and have been using a network drive to post Excel workbook files to your file server as you complete them. When you attempt to save a workbook file to the drive, you see the error message: “You do not have access to the folder ‘J:\’. See your administrator for access to this folder.” What should you do first? Second? Explain the reasoning behind your choices.
   * Ask your network administrator to give you permission to access the folder.
   * Check File Explorer to verify that you can connect to the network.
   * Save the workbook file to your hard drive.
   * Using File Explorer, remap the network drive.
   * Reboot your PC.
2. Which type of server can function as a firewall?
   * Mail server
   * Proxy server
   * Print server
   * FTP server
3. What is the command to launch each of the following tools?
   * Local Group Policy
   * Local Security Policy
   * Computer Management console
   * Local Users and Groups console
   * Resultant Set of Policy (RSoP)
4. What hardware component is needed to set up BitLocker Encryption so that you can authenticate the computer?
5. Where in Group Policy can you locate the policy that requires a smart card to be used to authenticate a user to Windows?
   * Computer Configuration, Windows Settings, Security Settings, Local Policies, Biometrics
   * Computer Configuration, Administrative Templates, System, Logon
   * Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options
   * User Configuration, Administrative Templates, System, Logon
6. You open a folder Properties box to encrypt the folder, click Advanced, and discover that Encrypt contents to secure data is dimmed. What is the most likely problem?
   * Encryption has not been enabled. Use the Computer Management console to enable it.
   * You are not using an edition of Windows that supports encryption.
   * Most likely a virus has attacked the system and is disabling encryption.
   * Encryption applies only to files, not folders.
7. You have shared a folder, C:\DenverCO, with your team. The folder contains information about your company branch in Denver, Colorado. Your company decides to reorganize into zones, so you move the folder as a subfolder in the folder G:\Zone3. When your team members try to access G:\Zone3\DenverCO, they get an error message saying they have been denied access. What happened to the permissions when you moved the folder to its new location?
8. What command do you enter in the Explorer search box to access the Remote Admin share on the computer named Fin?
9. In your organization, each department has a folder on a shared drive. Your boss frequently copies the folder to his local computer to run reports. You have noticed that the folder for your department keeps disappearing from the shared drive. You discover that the folder isn’t being deleted and often gets moved into a random, nearby folder. You suspect that coworkers in other departments are being careless with their mouse clicks while accessing their own folders on the shared drive and are dragging and dropping your department folder into other folders without noticing. How can you prevent this folder from being moved, but still allow it to be copied? What steps do you take?
10. If you are having a problem changing the permissions of a folder that was created by another user, what can you do to help solve the problem?
11. When setting up OUs in a new domain, why might it be useful to put all computers in one OU and all users in another?
    * It will be easier to inventory computers in the domain.
    * It will help organize users into user groups.
    * An OU must contain either users or computers, but not both.
    * Policies generally apply to either computers or users.
12. You have set up a user group named Accounting and have put all employees in the Accounting department in this group, which has been given permission to use the Financial folder on a file server. You are now asked to create a subfolder under Financial named Payroll. Megan, the payroll officer, is the only employee in the Accounting department allowed to access this folder. What is the best way to configure the new share?
    * Assign Megan read/write permissions to the Payroll folder, and explain to your boss that it is not a best practice to give only one employee access to an important folder.
    * Assign Megan read/write permissions to the Payroll folder.
    * Create a new user group named Payroll, put Megan in the group, and assign the group read/write permissions to the Payroll folder.
    * Ask your boss to allow you to put the folder outside of the Financial folder so you can assign a new user group read/write permissions to this folder that will not conflict with the Accounting user group.
13. Which of the following is true about NTFS permissions and share permissions? Select all that apply.
    * Share permissions do not work on an NTFS volume.
    * NTFS permissions work only on an NTFS volume.
    * If share permissions and NTFS permissions are in conflict, NTFS permissions win.
    * If you set NTFS permissions but do not set share permissions, NTFS permissions apply.
14. Which security features are available on Windows 10 Home? Select all that apply.
    * Local Group Policy
    * NTFS permissions
    * Active Directory
    * Internet Options

Go to pg.

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