

17-1 Securing a Windows Personal Computer

Core 2 Objectives

- 1.2
Given a scenario, use the appropriate Microsoft command-line tool.
- 1.3
Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
- 2.5
Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
- 2.6
Given a scenario, configure a workstation to meet best practices for security.

Recall from earlier modules that securing access to computer resources involves authenticating and authorizing a user or process and accounting for what a user or process does and when the resources were being used—all of which is collectively referred to as AAA security measures. When you have a choice in the security measures 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 find the right balance between security and user convenience (see [Figure 17-1](#)).

Figure 17-1

Security measures should protect resources without hindering how users work

Also, too much security can sometimes force workers to find insecure alternatives. For example, requiring users to change their passwords weekly might result in more of them writing their passwords down to help remember them.

Note 1

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.

17-1a BIOS/UEFI Passwords

Core 2 Objective

- 2.6

Given a scenario, configure a workstation to meet best practices for security.

One example of defense in depth is requiring a power-on password as well as a Windows password to access a Windows 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 17-2](#) shows a BIOS/UEFI setup Security screen where you can set the Administrator and User passwords.

Figure 17-2

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



17-1b Securing Windows User Accounts

Core 2 Objectives

- 1.2

Given a scenario, use the appropriate Microsoft command-line tool.

- 1.3

Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).

- 2.1

Summarize various security measures and their purposes.

- 2.6

Given a scenario, configure a workstation to meet best practices for security.

When a computer is on a Windows domain, Active Directory (AD) is responsible for AAA services. For a peer-to-peer network, authentication, authorization, and accounting must happen at the local computer. As an administrator, when you first create a Windows 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 section of the module, you learn how to use Local Group Policy, Local Security Policy, and other Windows 10/11 tools to secure Windows user accounts.

Create Strong Passwords

Normally, Windows authenticates a user with a Windows password. A password needs to be a **strong password**, 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, which is guessing with 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; a long password is your best protection against a password attack because the longer the password, the more guesses it takes to discover it. After a few thousand guesses, a hacker is likely to move on.
- 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.
- It's best to not 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.

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.

Note 2

How secure is a password? Go to howsecureismypassword.net and find out how long it will take a computer to crack the password.

Rather than writing down passwords, consider storing your passwords with a password manager app such as Dashlane (dashlane.com), Sticky Password (stickypassword.com), or LastPass (lastpass.com). 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.

Don't type your passwords 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.

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, they might choose not to use a password. However, if the user travels with a laptop, always recommend that the user create a strong password.

Fingerprints, Facial Recognition, and PINs

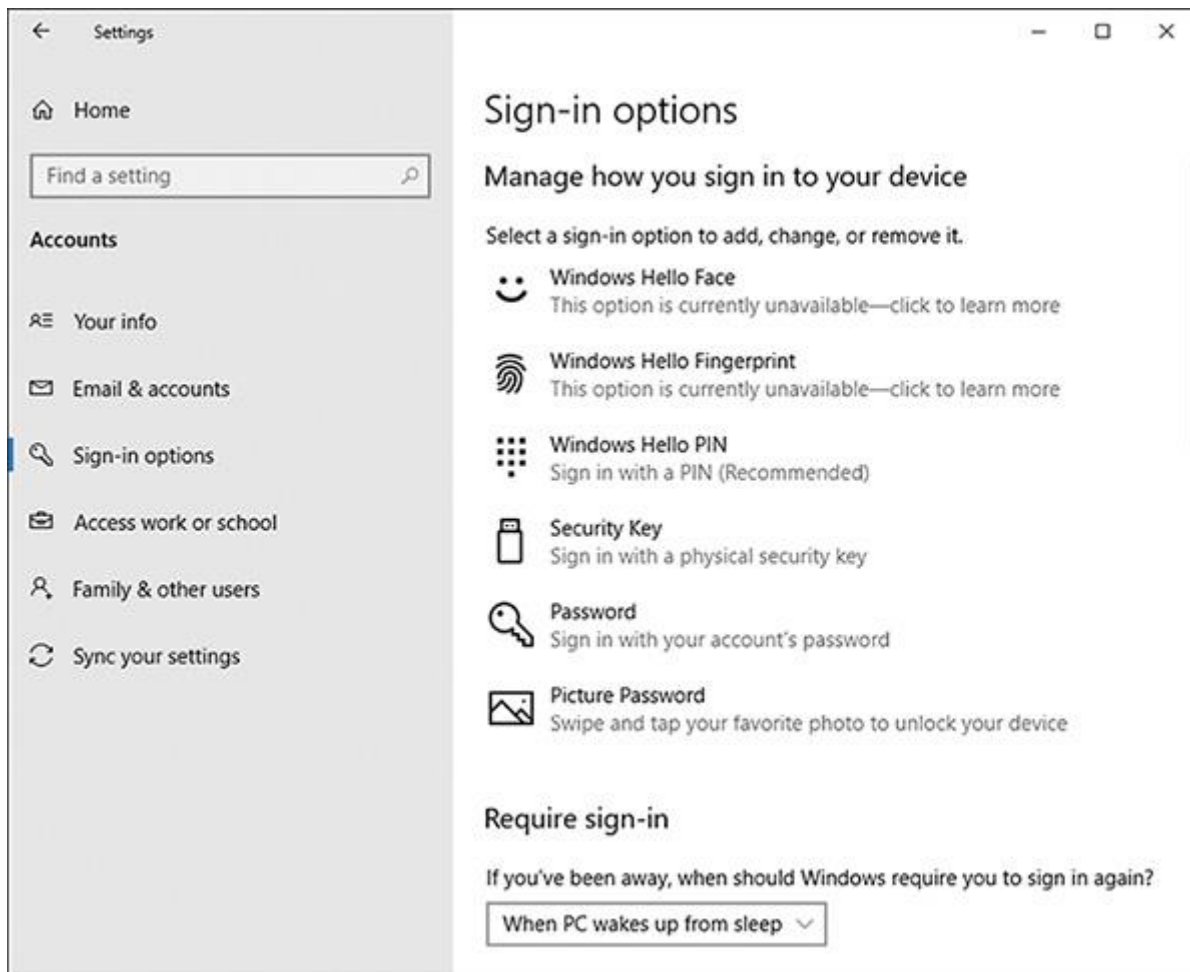
Windows account security can be further improved by configuring Windows Hello, a Windows feature that allows a user to sign in to Windows using their face, iris, fingerprint, or PIN. Captured biometric data, which is digitized, encrypted, and stored locally on the one Windows device, applies only to that one device and is never transmitted to a server. Because your Microsoft account can be used for single sign-on (SSO), when someone steals your password, they can access your Microsoft resources from any Windows device; however, your PIN works only on the one device.

To set up Windows Hello, open the **Settings** app, and select **Accounts** and **Sign-in options** (see [Figure 17-3](#)). When you select

Windows Hello Face or Windows Hello Fingerprint in this window, you are also required to set up a PIN, which can be used if signing in using your face or fingerprint is not an option, such as if you are injured or the face sensor or fingerprint sensor is not working. Face, fingerprint, and PIN sign-in don't replace the Windows password, but they are used in place of the password for this one device. If you have multiple Windows devices, you would need to set up Windows Hello on each device.

Figure 17-3

Use face recognition, fingerprint or PIN for Windows sign-in



Exam Tip

The A+ Core 2 exam expects you to know about OS login options, including passwords, PINs, fingerprints, facial recognition, and SSO.

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

Local Group Policy Editor

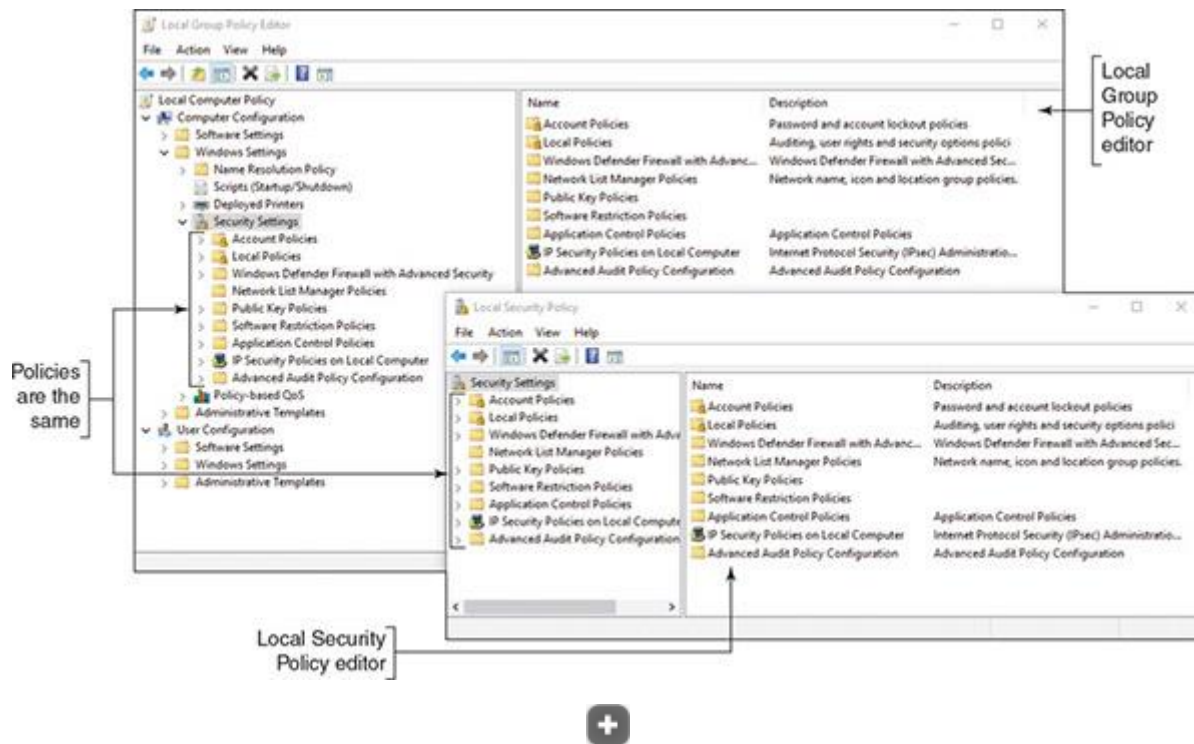
You need to be aware of three tools for managing policies that control what users and computers can do with a system or network:

- Group Policy (gpedit.msc) 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 module.
- **Local Group Policy** (gpedit.msc) contains a subset of policies in Group Policy; this subset applies only to the local Windows 10/11 computer or local user.
- **Local Security Policy** (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 a Windows 10 Administrative Tools or Windows 11 Windows 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 17-4](#) 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 17-4

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



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

- **Est. Time:** 45 minutes
- **Core 2 Objective:** 2.6

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

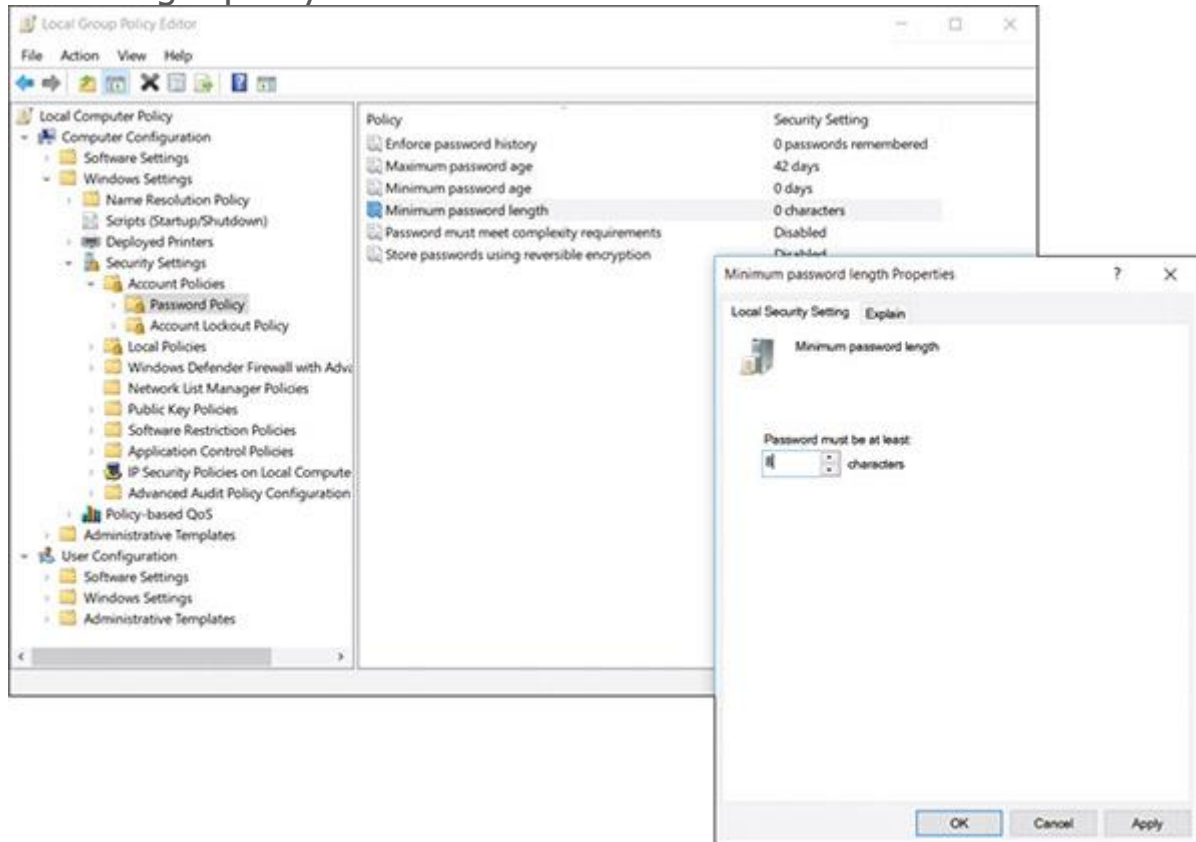
1. **1**
Sign in to Windows using an administrator account on a system that uses Windows 10/11 Pro or Enterprise.
2. **2**
To start Local Group Policy, enter the **gpedit.msc** command in the Windows search box. The Local Group Policy Editor console opens.
3. **3**
To change a policy, first use the left 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 and complexity.** 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 17-5](#)). Use the **Minimum password length** policy, and set the minimum length to at least eight characters (see the right side of [Figure 17-5](#)).

Figure 17-5

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



- **Require password complexity.** To require that passwords contain uppercase and lowercase letters, numbers, and symbols—and do not contain the user name—open the **Password must meet complexity requirements** and enable this policy.
- **Password expiration.** To require users to change their passwords frequently, open the **Maximum password age** policy, and set the age to up to 999 days. You can also set the *Minimum password age* policy so a user cannot cycle back to a favorite password immediately after they have changed it.

Note 3

For years, the security community has advised changing passwords often, but now security experts advise creating a very strong password and sticking to it unless you think the password has been compromised.

- **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, which is called tailgating. 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 a threshold for failed logon attempts.** 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.

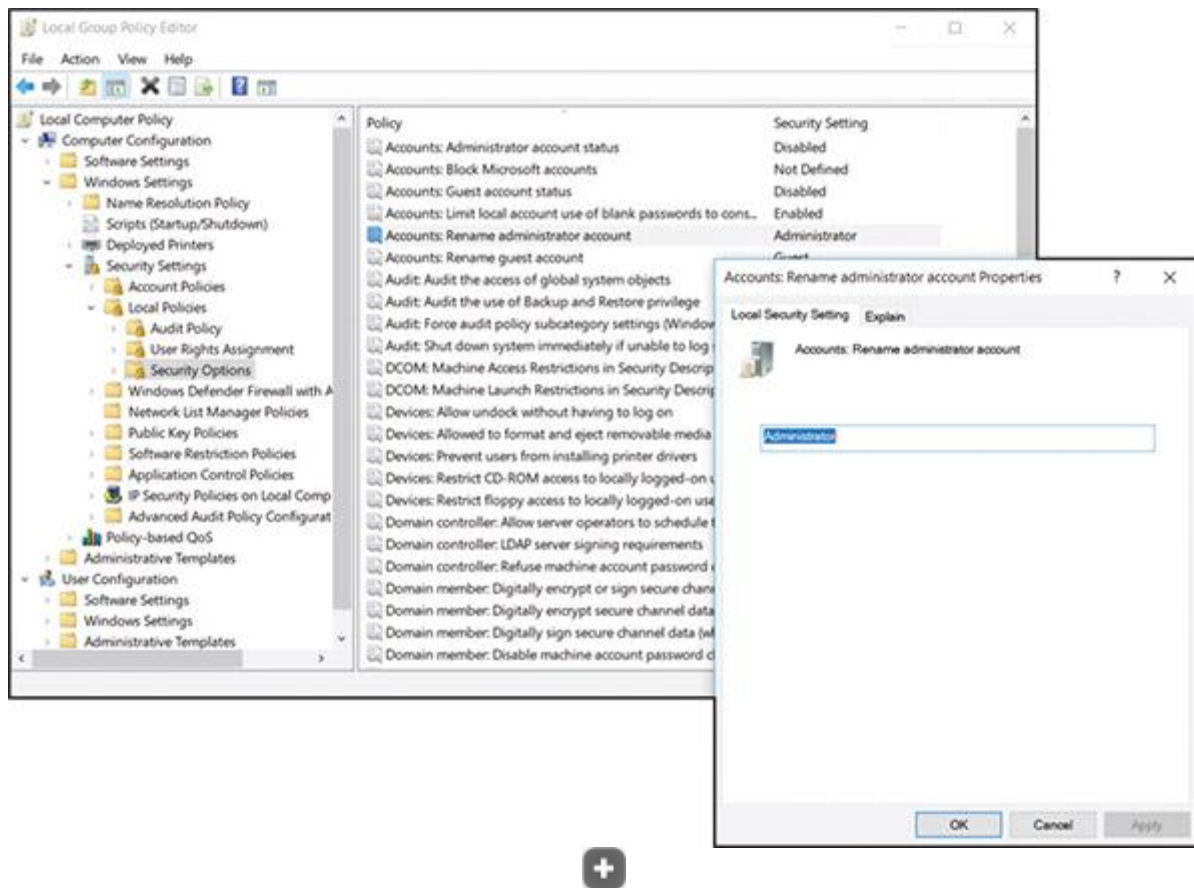
Note 4

The Properties dialog 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 17-6](#)). In the right pane, double-click **Accounts: Rename administrator account**. In the Properties dialog box for this policy (see the right side of [Figure 17-6](#)), change the name, and click **OK**. To change the name of the Guest account, use the policy **Accounts: Rename guest account**.

Figure 17-6

Use Group Policy to rename a default user account



Note 5

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 commands to activate the account and set its password:

```
net user Administrator /active:yes
```

```
net user Administrator <password>
```

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.

Note 6

When a computer is on a Windows domain managed by Active Directory, you can block a user from signing in to Windows locally, using a local account. To do that, go to the **Computer Configuration, Windows Settings, Security Settings, Local**

Policies, User Rights Assignments, and Allow log on locally policy. Remove the **Users** group from those allowed to log on locally. It's best to still allow the **Administrators** group to log on locally in case that logon is needed to troubleshoot the system.

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 some situations, 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 10/11 computer with a Microsoft account, they have 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 tiles, desktop personalization, installed apps and app settings, web browser favorites, and passwords to apps, websites, and networks.

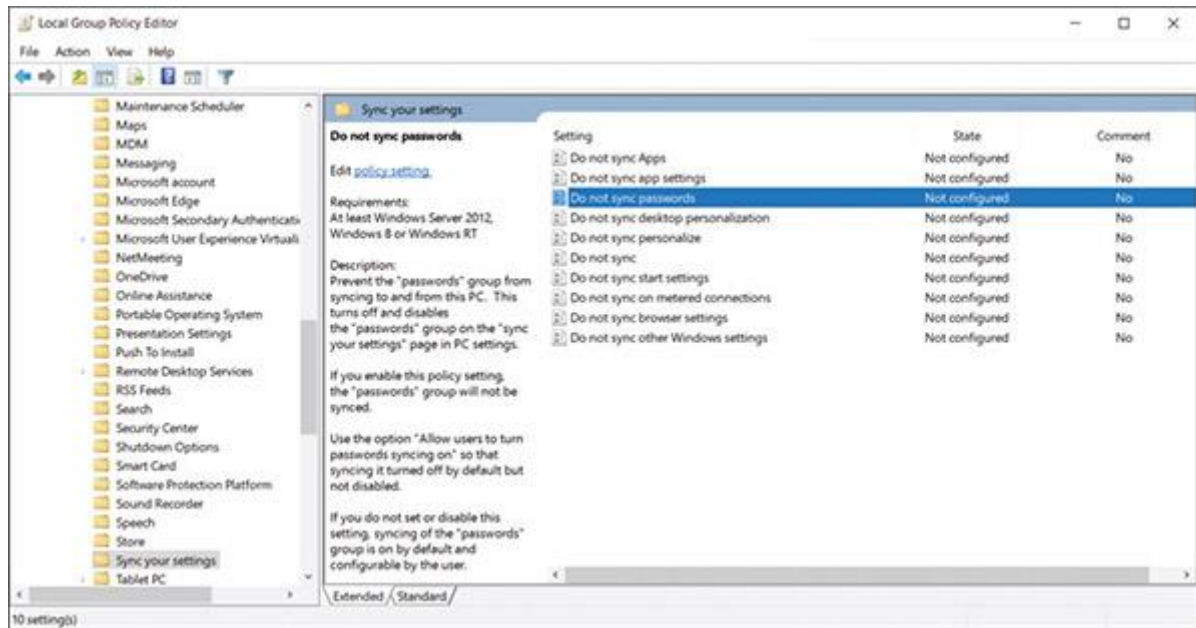
Note 7

To see and edit the sync settings available for a Microsoft account, open the Windows 10/11 **Settings** app, click the **Accounts** group, and select **Sync your settings** in the left pane.

- 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 17-7](#)). You can also block using Microsoft accounts altogether by setting the **Block Microsoft accounts** policy in the **Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options** group.

Figure 17-7

Restrict SSO authentication to online resources associated with a Microsoft account



- **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.

4. 4

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** command refreshes local group policies as well as group policies set in Active Directory on a Windows domain.

Exam Tip

The A+ Core 2 exam expects you to know how to secure a workstation in a given scenario, including managing user accounts. You need to know how to configure password length, characters, complexity, and expiration and how to restrict user permissions, configure login times, disable the guest account, set failed login attempts before lockout, set timeout screen locks, change the default administrator user account name and set its password, and disable AutoRun and AutoPlay. All these settings are done by using the Local Group Policy editor to edit these policies.

Now let's turn our attention to using encryption to secure workstation resources.

17-1c File and Folder Encryption

Core 2 Objective

- 2.5

Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

Data needs to be protected when at rest (while stored on a hard drive, flash drive, or other storage device) and in motion (while being transmitted over a network or the Internet). Encryption is an effective way to protect data, but the encryption techniques and protocols used are different depending on whether the data is at rest or in motion. In Windows, **data-at-rest encryption** can be accomplished using the Windows **Encrypting File System (EFS)**. EFS encrypts files and folders stored on drives using 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.

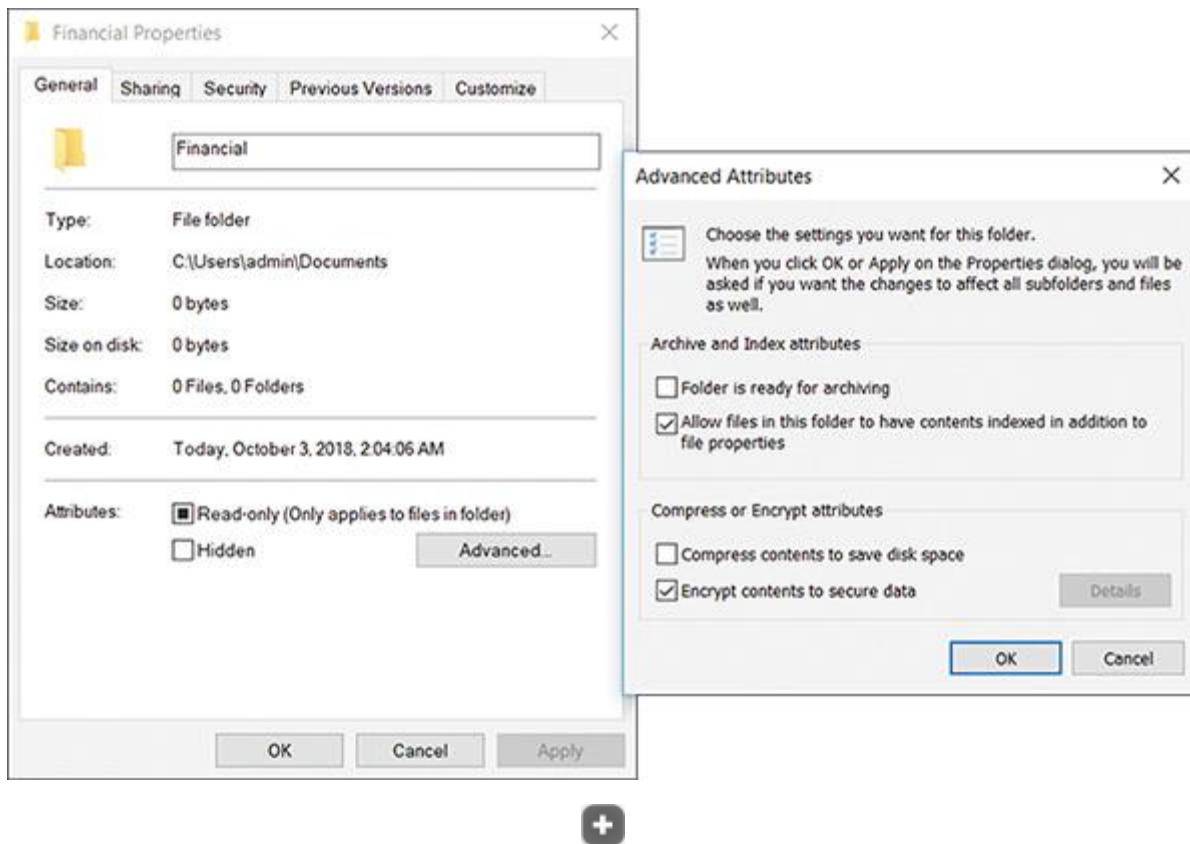
Note 8

In the module “[Network Security and Troubleshooting](#),” you learn how to encrypt data in motion on a network or the Internet.

To encrypt a folder or file, right-click it and open its **Properties** dialog box (see [Figure 17-8](#)). On the General tab, click **Advanced**. In the Advanced Attributes dialog box, check **Encrypt contents to secure data**, and click **OK**. In Explorer, encrypted file and folder names are displayed in green by default.

Figure 17-8

Encrypt a folder and all its contents



Note 9

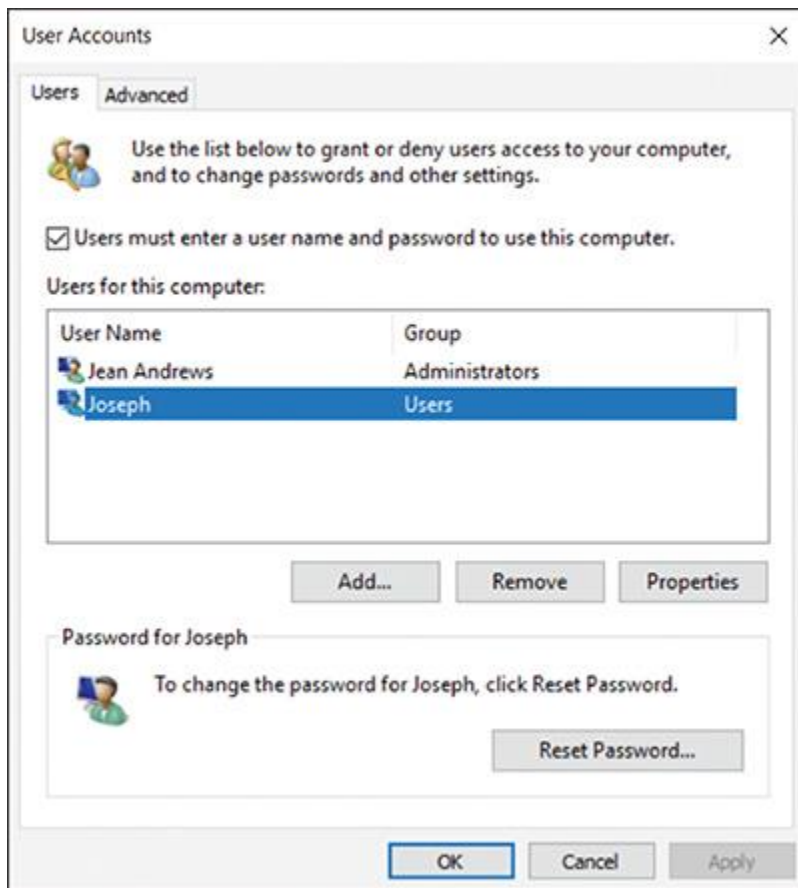
If the folder or file doesn't display in a green font in Explorer, you can change the setting by opening **Control Panel** and clicking **File Explorer Options**. On the View tab, check **Show encrypted or compressed NTFS files in color**. Click **OK**.

! Caution

If a user forgets a password, an administrator can reset the forgotten password. However, know that if an administrator resets a user password, the user will lose all their 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 tool (netplwiz.exe), as shown in [Figure 17-9](#). Select the user and click **Reset Password**. Later in the module, you learn to reset a password using the Local Users and Groups console.

Figure 17-9

Use the Network Places Wizard to reset a user password



17-1d BitLocker Encryption

Core 2 Objective

- 2.5

Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

BitLocker Drive Encryption 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**, 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.



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 and desktop 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 computer 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.) Recall that Windows 11 requires a TPM chip, version 2.0 or higher, which must be enabled before Windows 11 installs.
- **User authentication.** For Windows 10 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). The user installs the flash drive or enters a personal identification number (PIN) to unlock Windows startup. 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 their key ring or a lanyard.)
- **Computer and user authentication.** For best security, two-factor authentication is used: the TPM chip to authenticate the computer and the flash drive or PIN to authenticate the user.

Note 10

Most computers manufactured within the last five years implement TPM 2.0, which is required to run Windows 11.

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. If you decide to use BitLocker, make extra copies of the startup keys and/or PIN, and keep them in a safe location.

! Caution

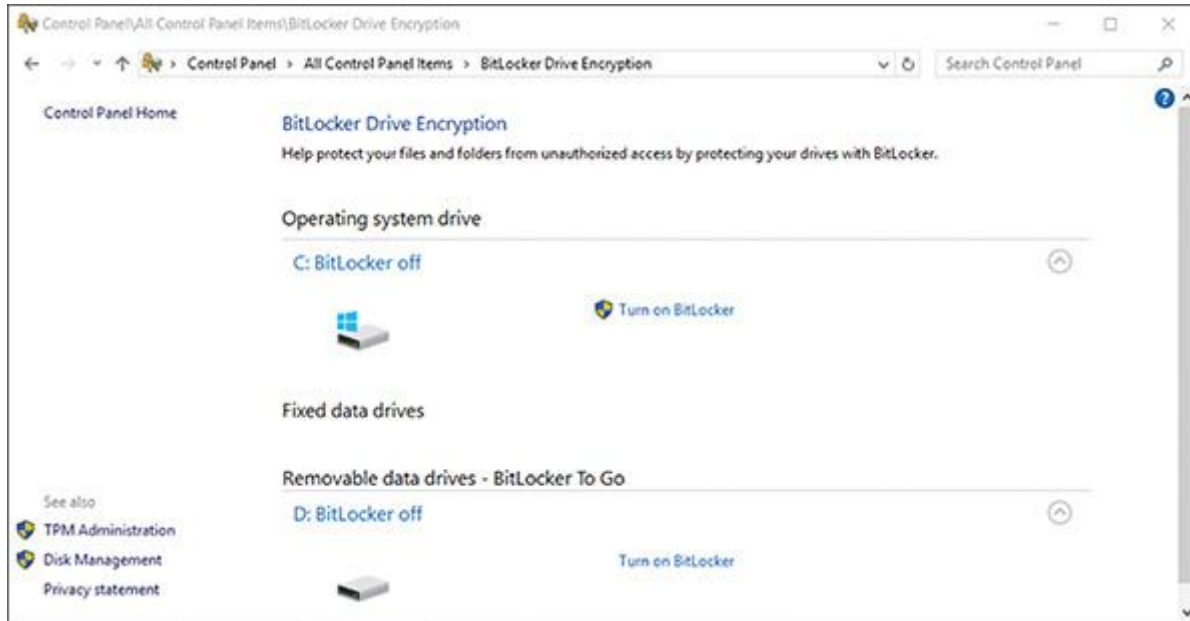
In the module "[Security Strategies](#)," you learned that some data, such as healthcare data, is regulated by the government, and organizations that are negligent in protecting it can be held legally responsible for data breaches. For this type of data, encryption and other security measures may be 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 17-10](#)). Using this window,

you can click **TPM Administration** to manage the TPM chip and turn on BitLocker or BitLocker To Go.

Figure 17-10

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



Note 11

For detailed instructions on how to set up BitLocker Drive Encryption, see the Microsoft article "BitLocker" at docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview.

17-2 Controlling Access to Folders, Files, and Printers

Core 2 Objectives

- 1.2
Given a scenario, use the appropriate Microsoft command-line tool.
- 1.3
Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
- 1.4
Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.

- 1.6

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

- 2.5

Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

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.

Note 12

In Windows, the terms “privileges” and “permissions” have different meanings. Privileges (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 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 for user accounts and controlling permissions for folders and files. Then you learn the procedures in Windows for assigning these privileges and permissions.

17-2a Classifying User Accounts and User Groups

Core 2 Objectives

- 1.3

Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).

- 2.5

Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

In Windows, the privileges or rights assigned to a user account are established when you first create the account and decide the account type. You can later change these privileges by changing the user groups to which the account belongs. Recall from the module “[Installing Windows](#)” that user accounts can be created using the User Accounts applet in Control Panel for

any edition of Windows. For business and professional editions of Windows, you can use the **Local Users and Groups** (lusrmgr.msc) utility in the Computer Management console to create and manager users and user groups. Home editions of Windows cannot be used to manage user groups, and the Local Users and Groups utility is missing in the Computer Management console for Home editions.

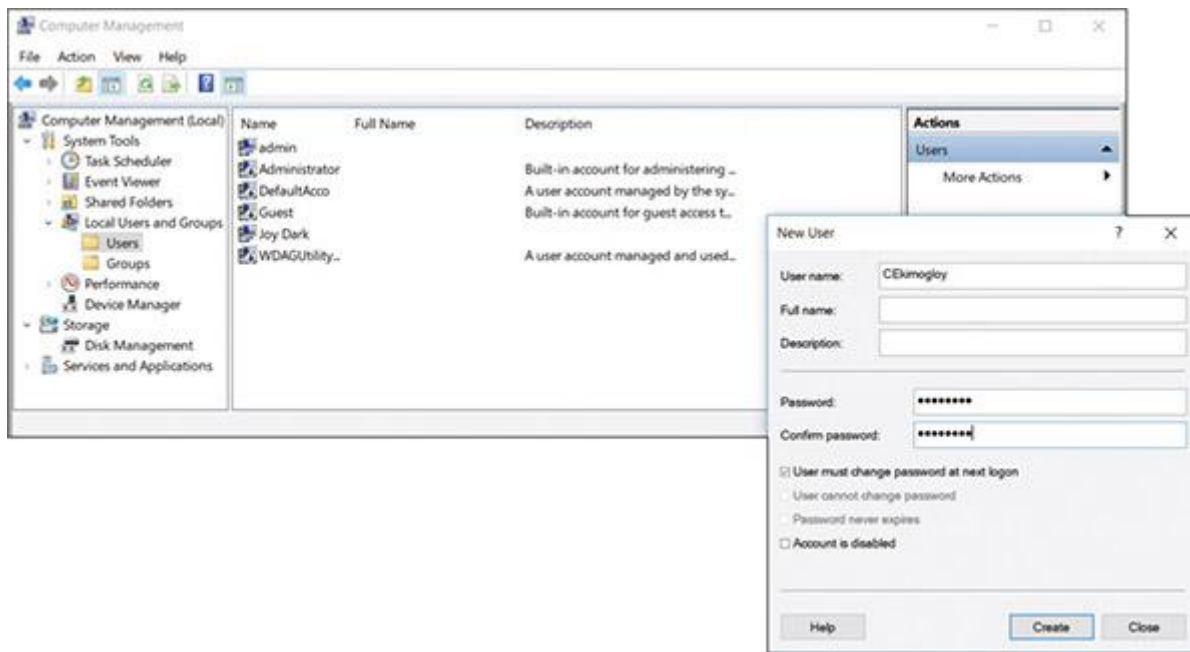
Type of User Account

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. Enter information for the new user, and click **Create** (see [Figure 17-11](#)).

Figure 17-11

Create a new user



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

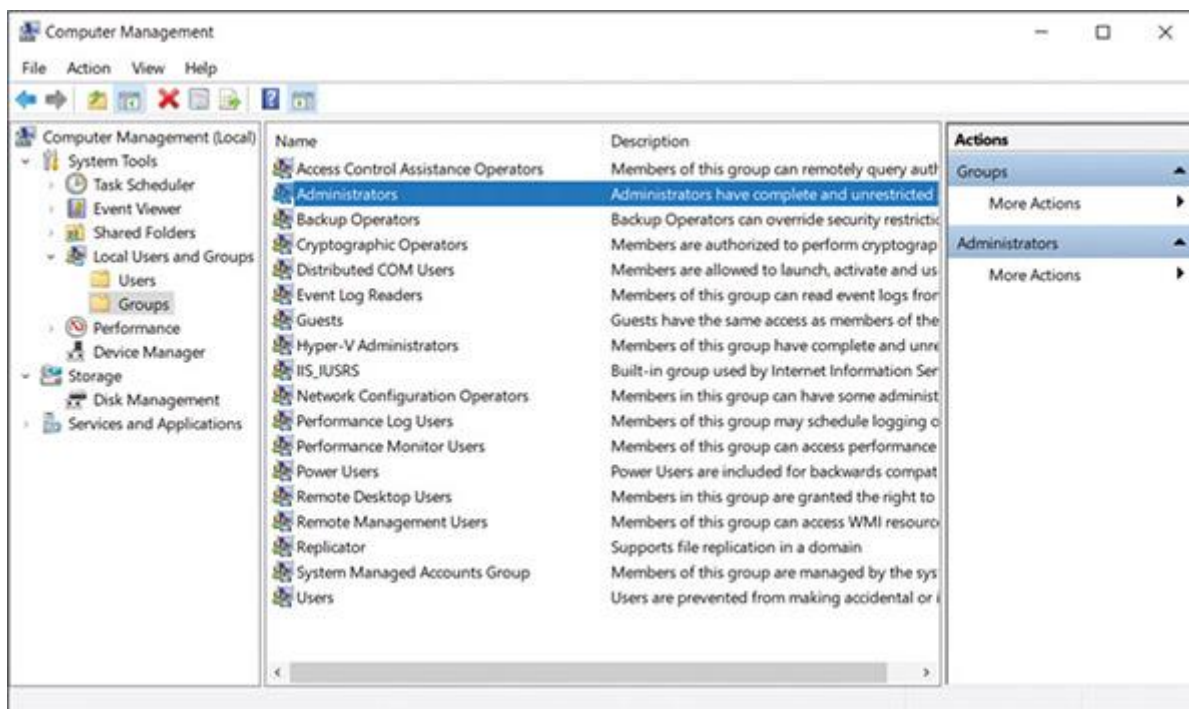
A user account can belong to one or more user groups. Windows offers several built-in user groups, and you can create your own. Here are important built-in user groups:

- **Administrators and Users groups.** By default, administrator accounts belong to the **Administrators group**, and standard user accounts belong to the **Users group**. 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** 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** 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 10/11 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 17-12](#)).

Figure 17-12

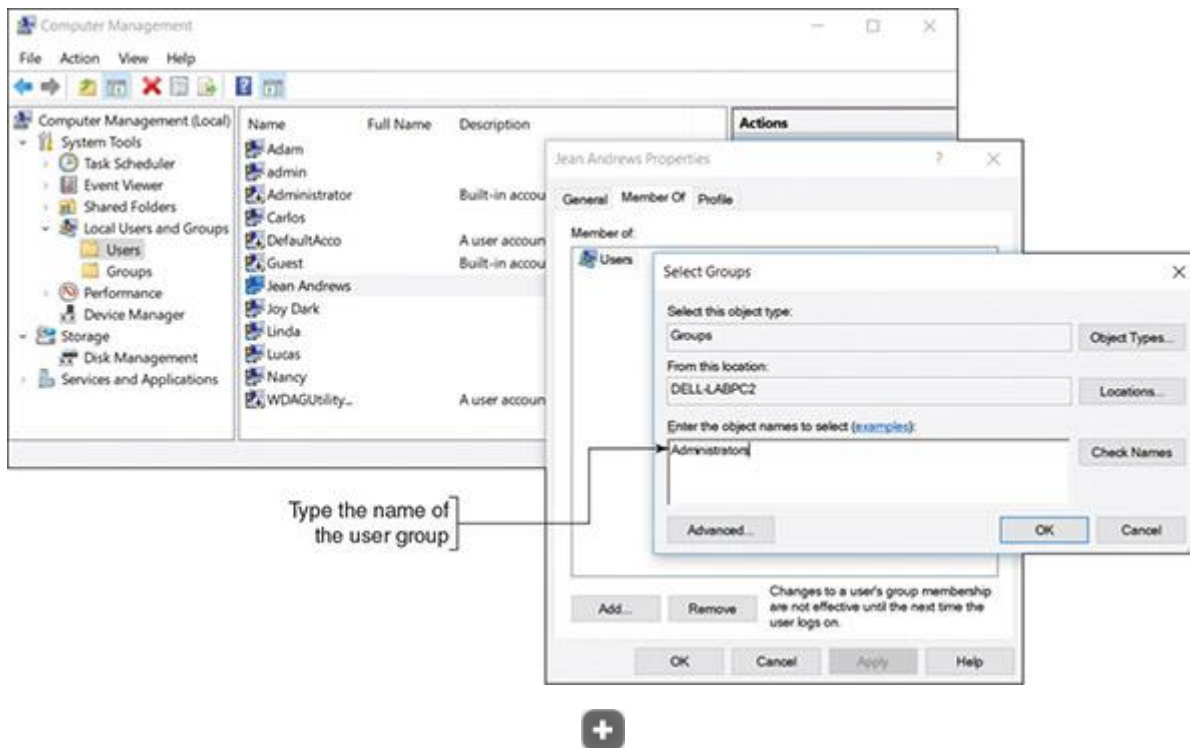
User groups installed on a system



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 17-13](#)). Right-click the user account, and select **Properties** in the shortcut menu. In the user account Properties dialog box, click the **Member Of** tab (see the middle of [Figure 17-13](#)). 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 (refer back to [Figure 17-12](#)). 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 dialog boxes.

Figure 17-13

Add a user account to a user group



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** 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** includes the Authenticated Users group as well as the Guest account. When you share a file or folder on the network, Windows gives access to the Everyone group by default.
- **Anonymous users** 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 Explorer to view shared folders and files on the remote computer, but you cannot access them.

Customized User Groups

Recall from the module “[Security Strategies](#)” that the principle of least privilege says that a person in an organization is assigned the privileges necessary to do their job and no more. One convenient way to comply with this principle is to assign privileges to user groups rather than individual users. First, create a user group based on a job description and then assign permissions to this user group. Any user account that you put in this group then acquires or inherits 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. You learn how to set all this up later in the module.

17-2b Methods to Assign Permissions to Folders and Files

Core 2 Objective

- 1.6

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

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, 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.

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.

Note 13

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 their 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.

Share Permissions and NTFS Permissions

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** 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 dialog box. Share permissions apply to a folder and its contents, but not to individual files.
- **NTFS permissions.** **NTFS permissions** apply to local users and network users and 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 dialog box. (The Security

tab is missing on the Properties dialog 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.

Inherited Permissions and Explicit Permissions

- **Inherited permissions** are permissions that are attained from a parent folder. Passing permissions from a parent object to a child is called permission propagation. When you create, copy, or move an object (file or folder) that has inherited permissions enabled into a parent folder, the new object takes on the permissions of the parent folder.
- **Explicit permissions** apply to an object (folder or file) that has inherited permissions disabled. When an object with explicit permissions is moved from one parent folder to another on the same volume, the object retains its original permissions. When an object with explicit permissions is copied from one folder to another—or moved from one volume to another—it inherits the new parent object permissions because when copied, a new object is created in the new location.



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. A project at the end of this module will help you practice this skill.

17-2c How to Share Folders and Files

Core 2 Objectives

- 1.6

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

- 2.5

Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

Now that you know about the concepts and strategies for managing users and user groups and sharing folders and files, let's look at the details of how to use Windows to set up users and user groups and assign file and folder permissions to these groups.

Applying Concepts

Creating User Groups and Folder Shares

- **Est. Time:** 45 minutes
- **Core 2 Objective:** 1.6

Makani 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. Makani 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. Makani must do the following to set up the users and data:

1. **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. **2**
Using NTFS permissions, set the permissions for the Financial and Medical folders on the file server so only the members of the appropriate group can access each folder.
3. **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 the module "[Maintaining Windows](#)").

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

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

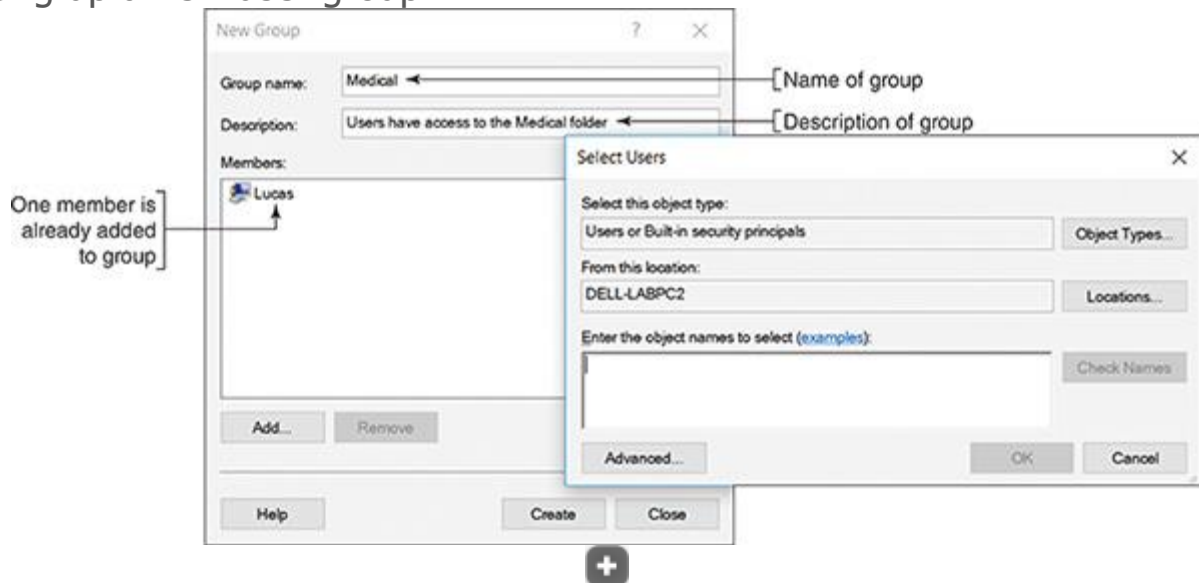
Follow these steps to create the folders, user accounts, and user groups on the file server computer that is using Windows 10/11 Pro:

1. **1**
Sign in to the system as an administrator.
2. **2**
Using an NTFS volume, create these two folders: **C:\Medical** and **C:\Financial**.

3. **3** Open 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. **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 dialog box appears. Enter the name of the group (**Medical**) and its description (**Users have access to the Medical folder**), as shown in [Figure 17-14](#).

Figure 17-14

Setting up a new user group



5. **5** 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 dialog box opens, as shown on the right side of [Figure 17-14](#). 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, their name appears under Members in the New Group dialog box, as shown in [Figure 17-14](#). To create the group, click **Create** in the New Group dialog box.
6. **6** In the same way, create the Financial group, and add Lucas, Linda, and Carlos to the group. Later, you can use the Local Users and Groups console to add or remove users from either group.
7. **7** Close the Local Users and Groups console.



Exam Tip

The A+ Core 2 exam expects you to be able to set up a user account or group and know how to add and remove users from a group.

Step 2: Set NTFS Folder Permissions For User Groups

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

1. **1**

Open **Explorer**, right-click the **Medical** folder, and select **Properties** in the shortcut menu. The Properties dialog box for the folder appears.

2. **2**

Click the **Security** tab (see [Figure 17-15](#)). Notice in the dialog 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 17-1](#) 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 17-15

Permissions assigned to the Medical folder

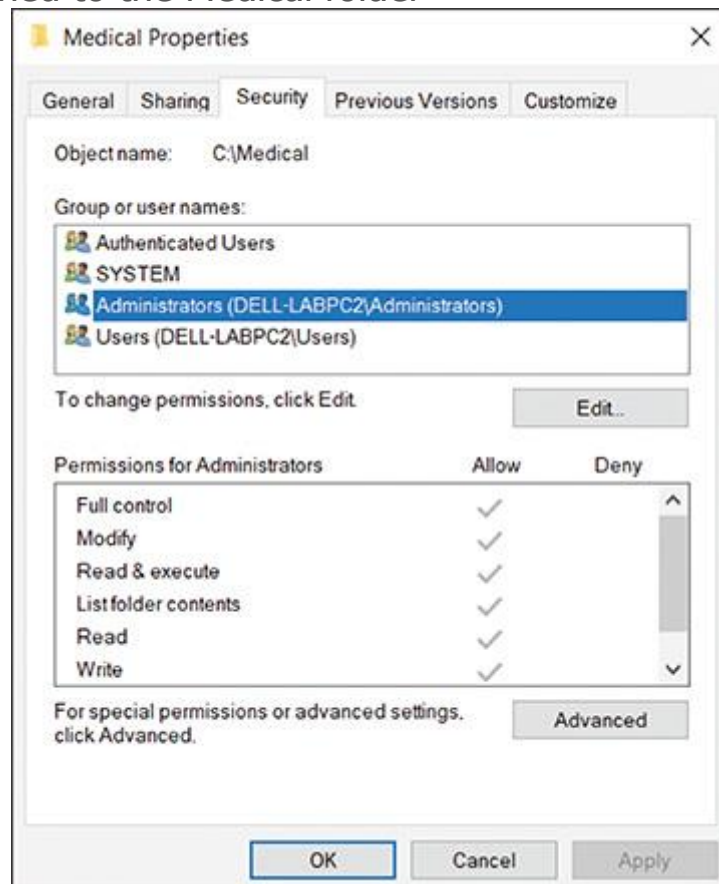


Table 17-1

Permission Levels for Files and Folders

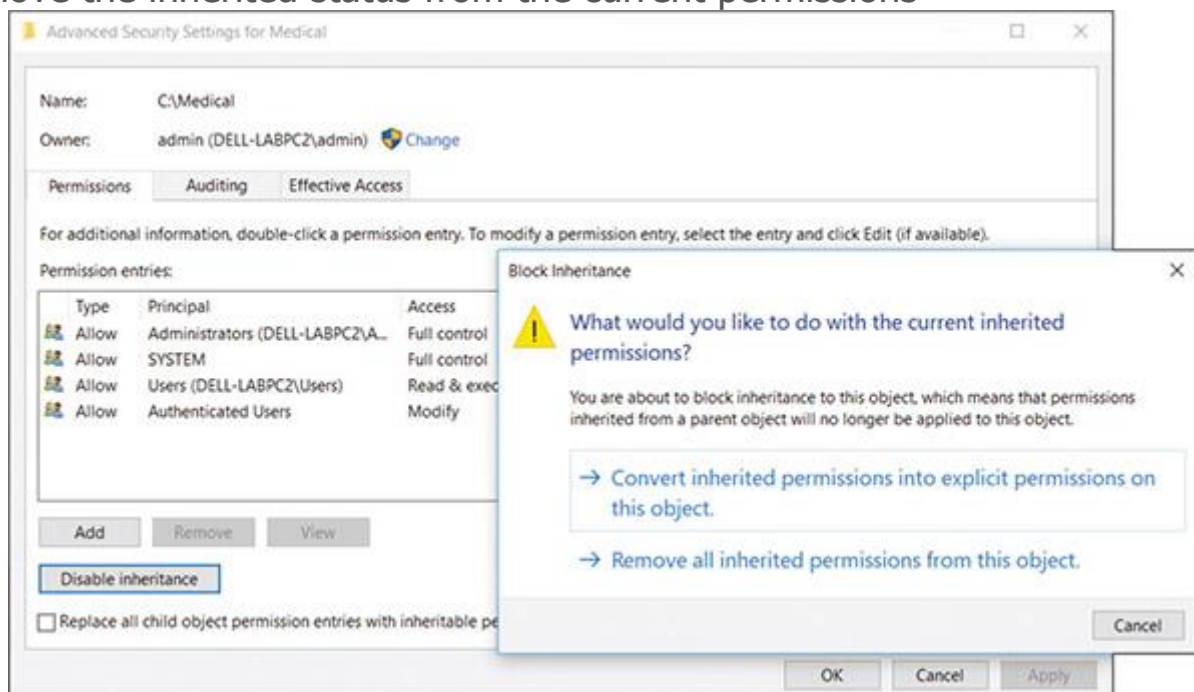
Permission Level	Description
Full control	Can read, change, delete, and create files and subfolders, read file and folder attributes, read and change permissions, and take ownership of a file or folder.
Modify	Can read, change, and create files and subfolders. Can delete the folder or file but cannot 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.

3. **3**

To remove the inherited status from these permissions so you can change them, click **Advanced**. The Advanced Security Settings dialog box appears (see the left side of [Figure 17-16](#)). Click **Change permissions** and **Disable inheritance**. The Block Inheritance dialog box appears (see the right side of [Figure 17-16](#)). 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 17-16

Remove the inherited status from the current permissions





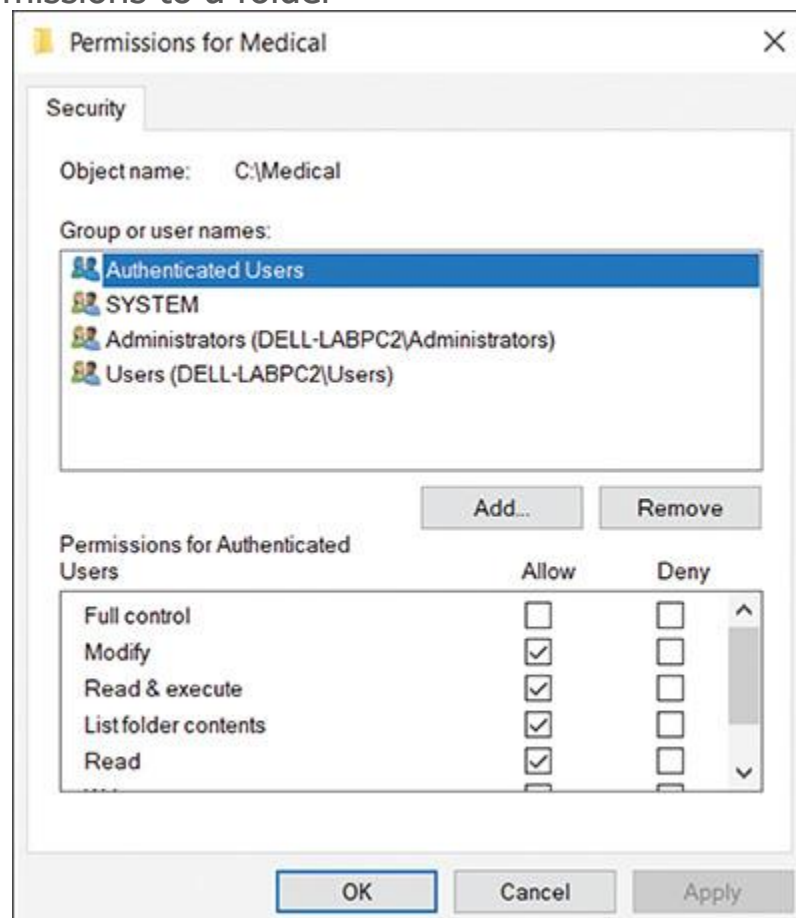
Note 14

Now that the Medical folder is using explicit permissions rather than inherited permissions, if you were to move (not copy) the folder to a new folder on the same NTFS volume, it would retain its original permissions in the new location.

4. **4**
Close the Advanced Security Settings dialog box.
5. **5**
In the Medical Properties dialog box, notice the permissions are now checked in black, indicating they are no longer inherited but rather explicit permissions and can be changed. Click **Edit** to change these permissions.
6. **6**
The Permissions dialog box opens (see [Figure 17-17](#)). 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 administrators can access the data.

Figure 17-17

Change the permissions to a folder

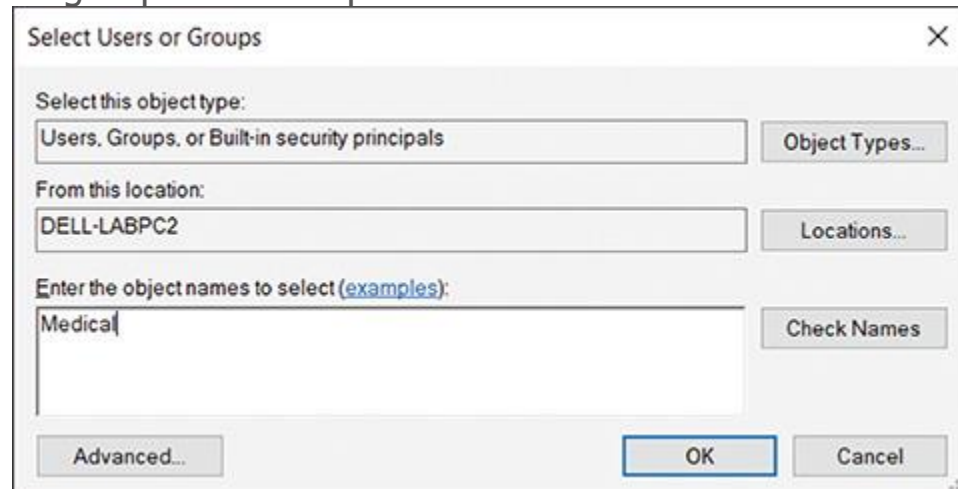


7. **7**

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 17-18](#). 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 17-18

Add a user or group to shared permissions



8. **8**
In the Permissions dialog 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 dialog box.
9. **9**
In a similar way, change the permissions of the C:\Financial folder so Authenticated Users and Users are not allowed access and the Financial group is allowed full control.

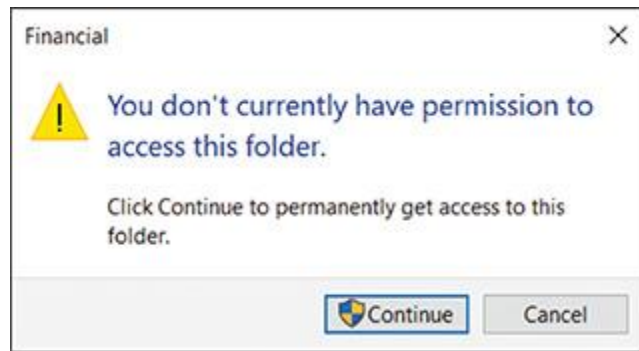
Step 3: Test, Set Share Permissions, and Go Live

It's now time to test your security measures. Never be tempted to skip testing every aspect of a new security measure. A security measure that does what you didn't intend it to do can allow in hackers or lock out wanted users. Do the following to test the NTFS permissions and implement your shared folders:

1. **1**
Test a user account in each user group to make sure the user can read, write, and delete in the folder they need 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 17-19](#) shows the dialog 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 dialog box gives you access.

Figure 17-19

Access to a folder is controlled



2. **2**

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 dialog box, and click **Advanced Sharing**.



Exam Tip

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

3. **3**

In the Advanced Sharing dialog 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 dialog 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.

4. **4**

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 dialog box.

5. **5**

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 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 17-20](#).

Figure 17-20

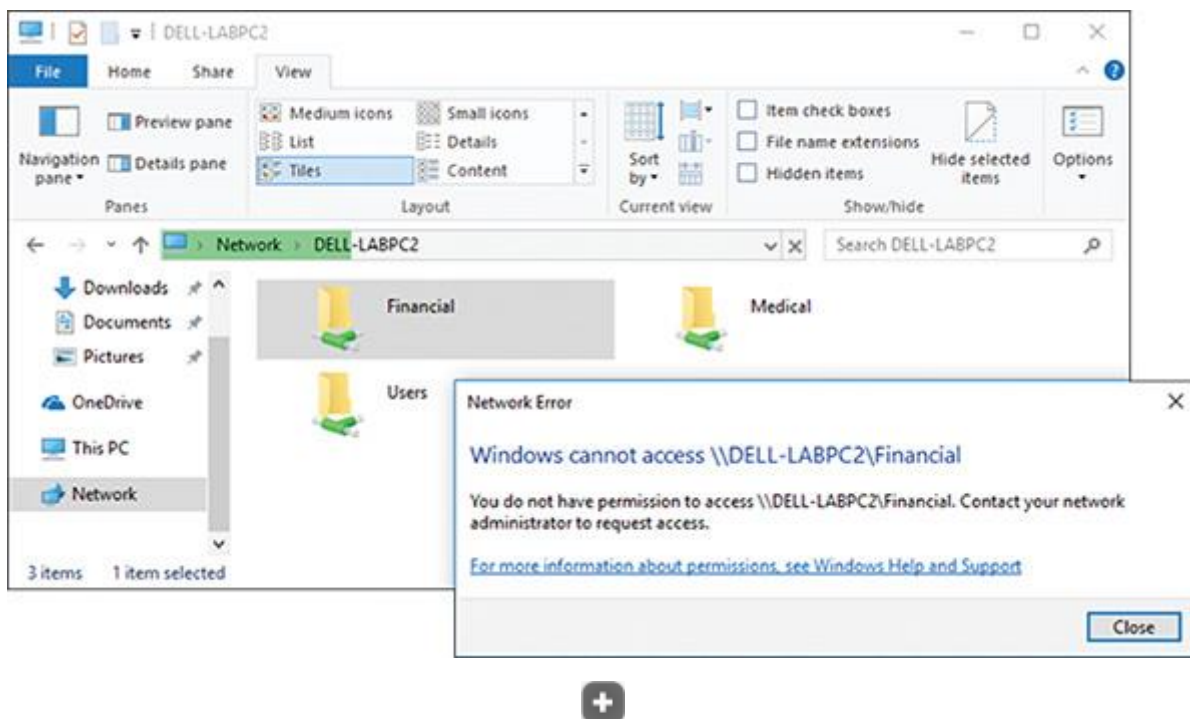
Use the computer name to access shared folders on that computer



6. **6** [Figure 17-21](#) shows the error message that appears when an unauthorized user attempts to access a network share. 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 the module "[Maintaining Windows.](#)"

Figure 17-21

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



User and Group Information with the gresult Command

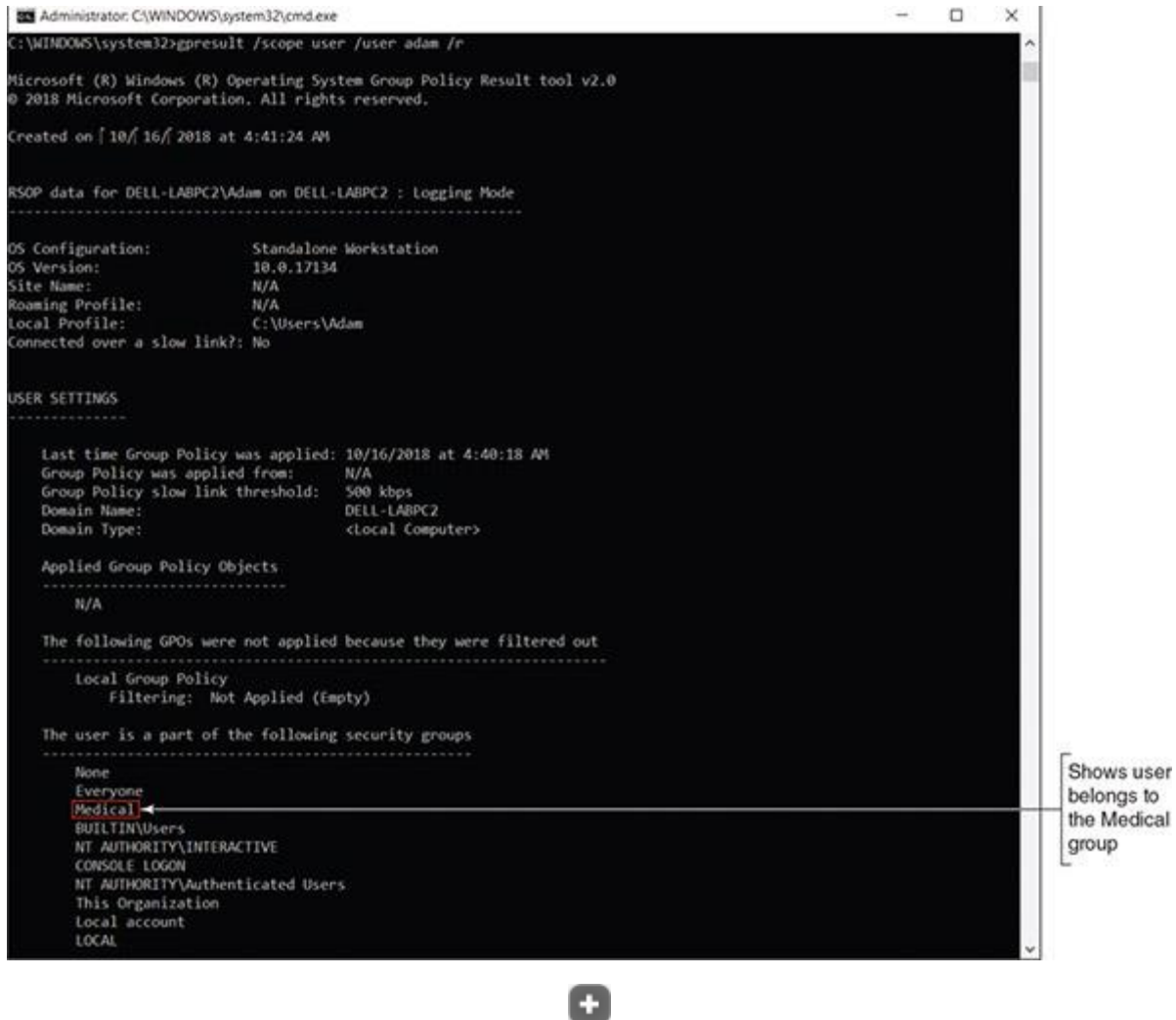
You can pull a list of all the groups a user belongs to with the **gresult** command. This information can be helpful when troubleshooting user group issues or Group Policy problems; the command displays user groups a user belongs to and all the currently applied policies set by Group Policy. To retrieve 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 17-22](#) 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 module.

Figure 17-22

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



```
Administrator: C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>gpresult /scope user /user adam /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2018 Microsoft Corporation. All rights reserved.

Created on 10/16/2018 at 4:41:24 AM

RSOP data for DELL-LABPC2\Adam on DELL-LABPC2 : Logging Mode
-----
OS Configuration:      Standalone Workstation
OS Version:            10.0.17134
Site Name:              N/A
Roaming Profile:        N/A
Local Profile:          C:\Users\Adam
Connected over a slow link?: No

USER SETTINGS
-----
Last time Group Policy was applied: 10/16/2018 at 4:40:18 AM
Group Policy was applied from:      N/A
Group Policy slow link threshold:   500 kbps
Domain Name:                        DELL-LABPC2
Domain Type:                         <Local Computer>

Applied Group Policy Objects
-----
N/A

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups
-----
None
Everyone
Medical
BUILTIN\Users
NT AUTHORITY\INTERACTIVE
CONSOLE LOGON
NT AUTHORITY\Authenticated Users
This Organization
Local account
LOCAL
```

Shows user belongs to the Medical group

How to Use Share Permissions

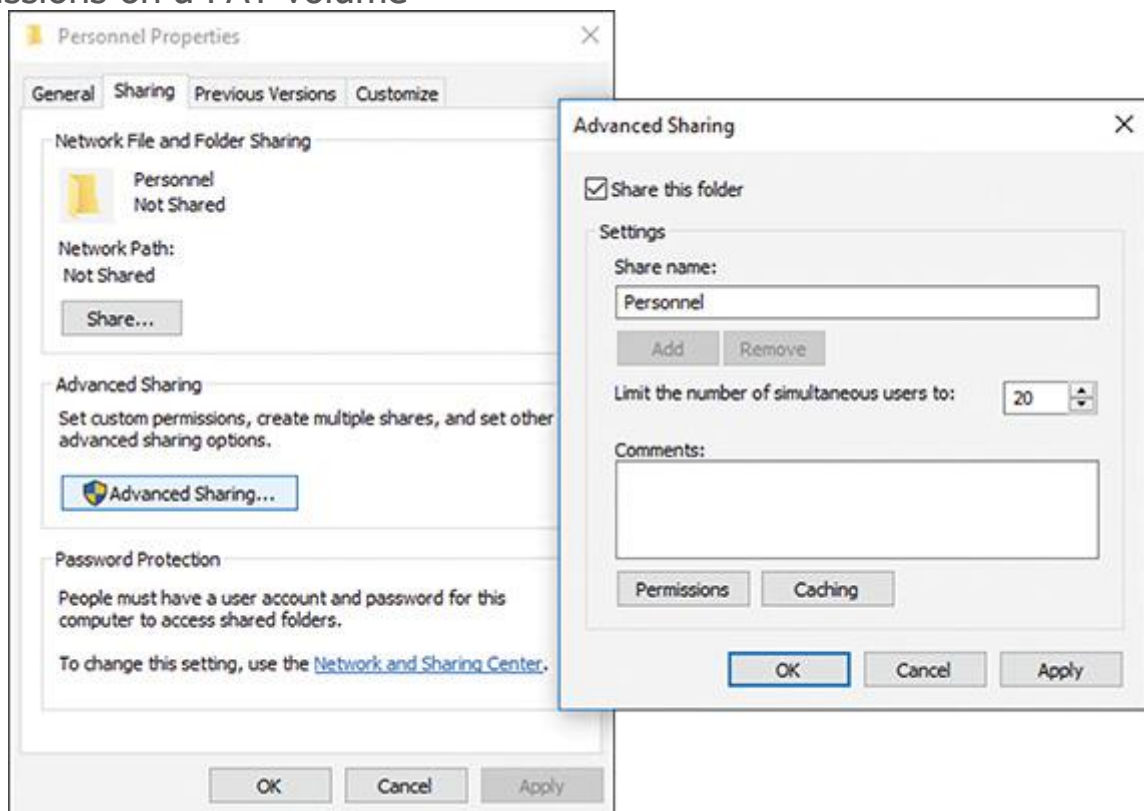
Although you can mix NTFS permissions and share permissions on the same system, life is simpler if you use one or the other. For NTFS volumes, NTFS permissions are the way to go because they can be customized better than share permissions. However, you must use share permissions on FAT volumes. To do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

1. **1**

Open the **Properties** dialog box for the folder (*Personnel* in this case). Notice in [Figure 17-23](#) 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 dialog box opens (see the right side of [Figure 17-23](#)).

Figure 17-23

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

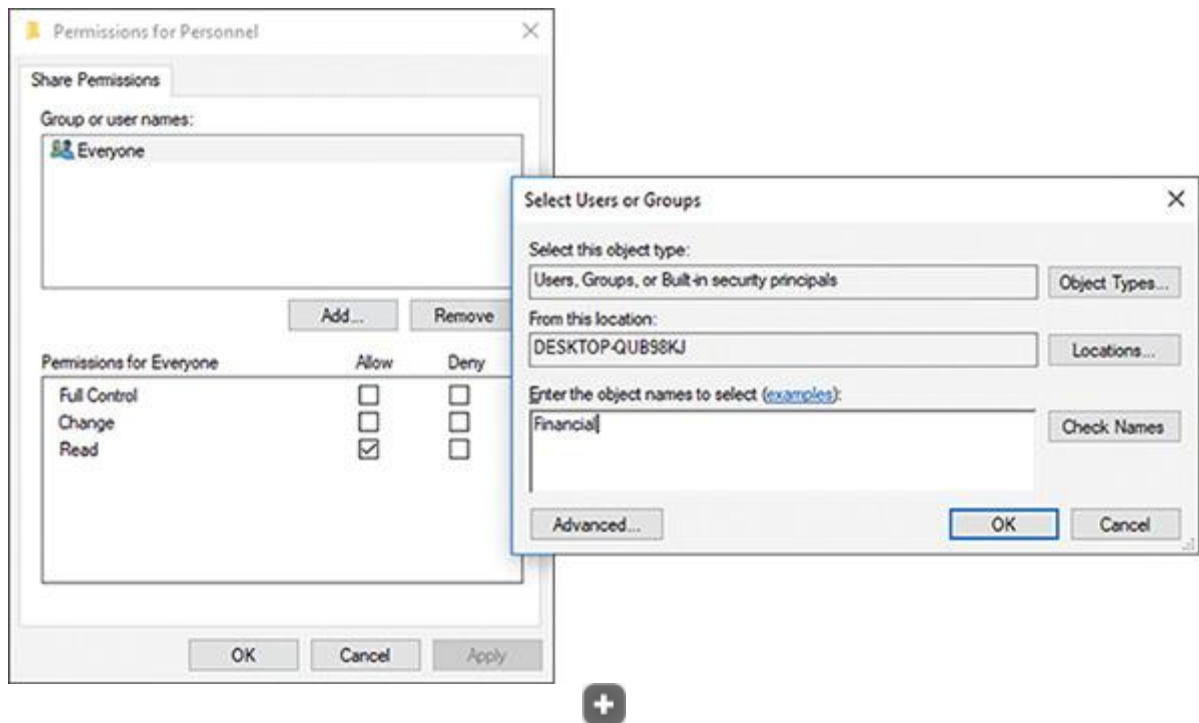


2. **2**

Check **Share this folder**. Then click **Permissions**. The Permissions dialog box opens (see the left side of [Figure 17-24](#)). Initially, the folder is shared with Everyone. Also notice that share permissions offer only three permission levels: Full Control, Change, and Read.

Figure 17-24

Add a user or user group to assign share permissions



3. **3** Click **Add**. The Select Users or Groups dialog box appears (see the right side of [Figure 17-24](#)). Enter a user account or user group and click **OK**.
4. **4** To delete the Everyone group, select it in the Permissions dialog box, and click **Remove**. Click **OK** to close each open dialog box in turn.

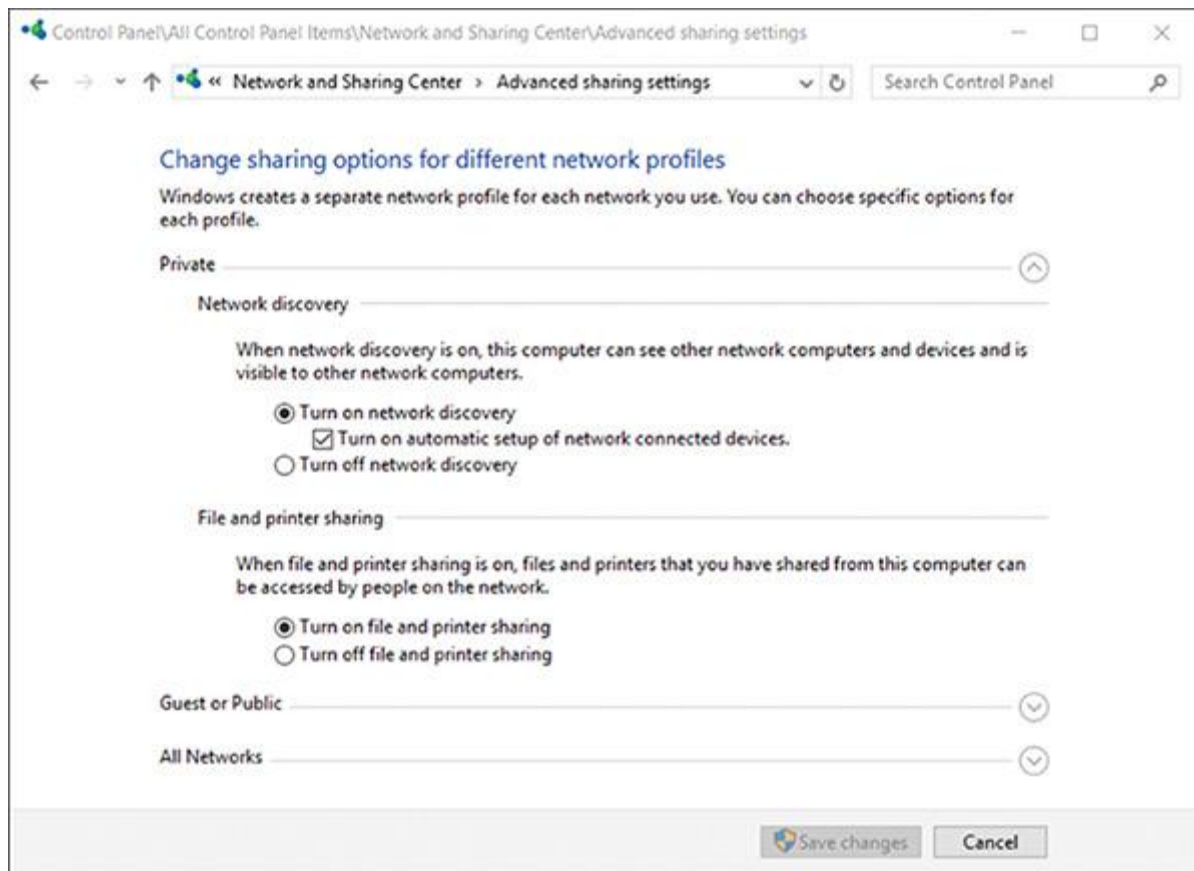
Support and Troubleshoot Shared Folders and Files

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. **1** Windows might be able to solve the problem for you. In Control Panel, click **Troubleshooting**. In the Troubleshooting window, click **Access shared files and folders on other computers**, and walk through the Shared Folders troubleshooter.
2. **2** Open the **Network and Sharing Center**. Make sure your network location is set to Private.
3. **3** In the left pane, click **Change advanced sharing settings**. The Advanced sharing settings window opens. See [Figure 17-25](#).

Figure 17-25

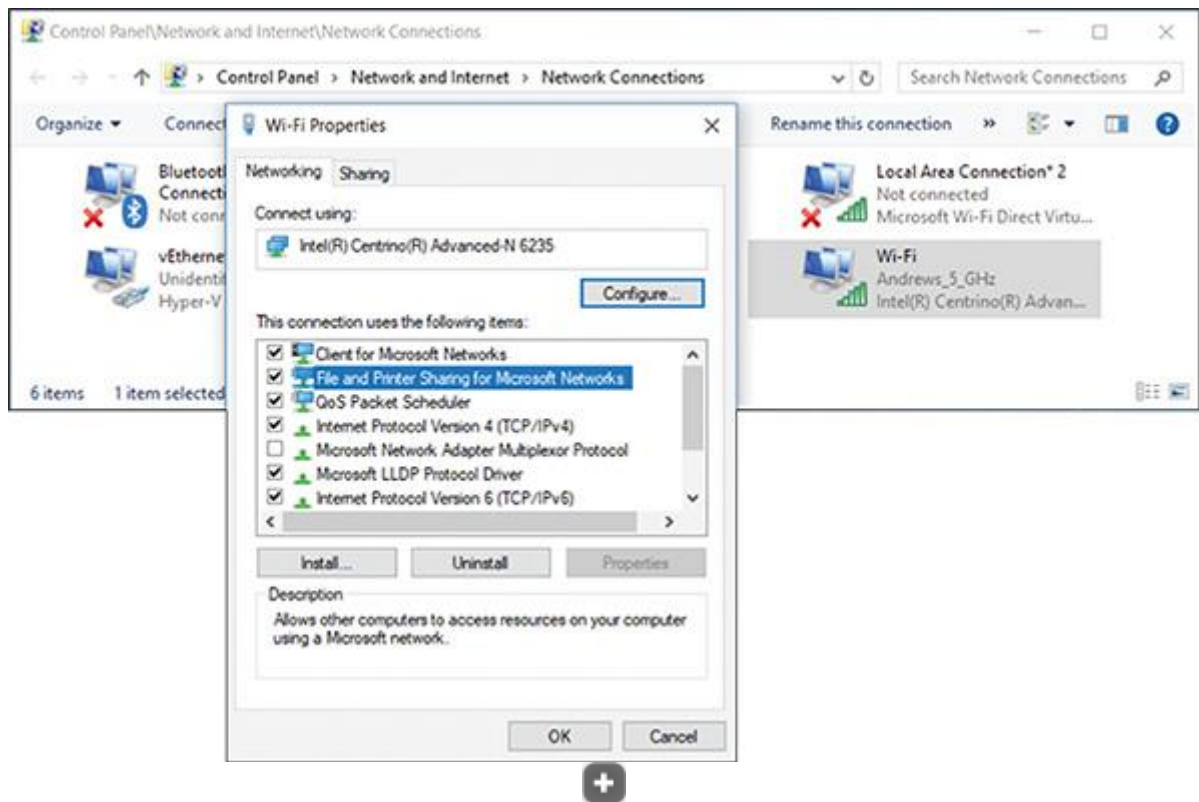
Configure the security level for network connections



4. **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**.
 - 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**.
5. **5** After you have made your changes, click **Save changes** at the bottom of the window.
6. **6** 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 dialog box, verify that **File and Printer Sharing for Microsoft Networks** is checked (see [Figure 17-26](#)).

Figure 17-26

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



7. **7**

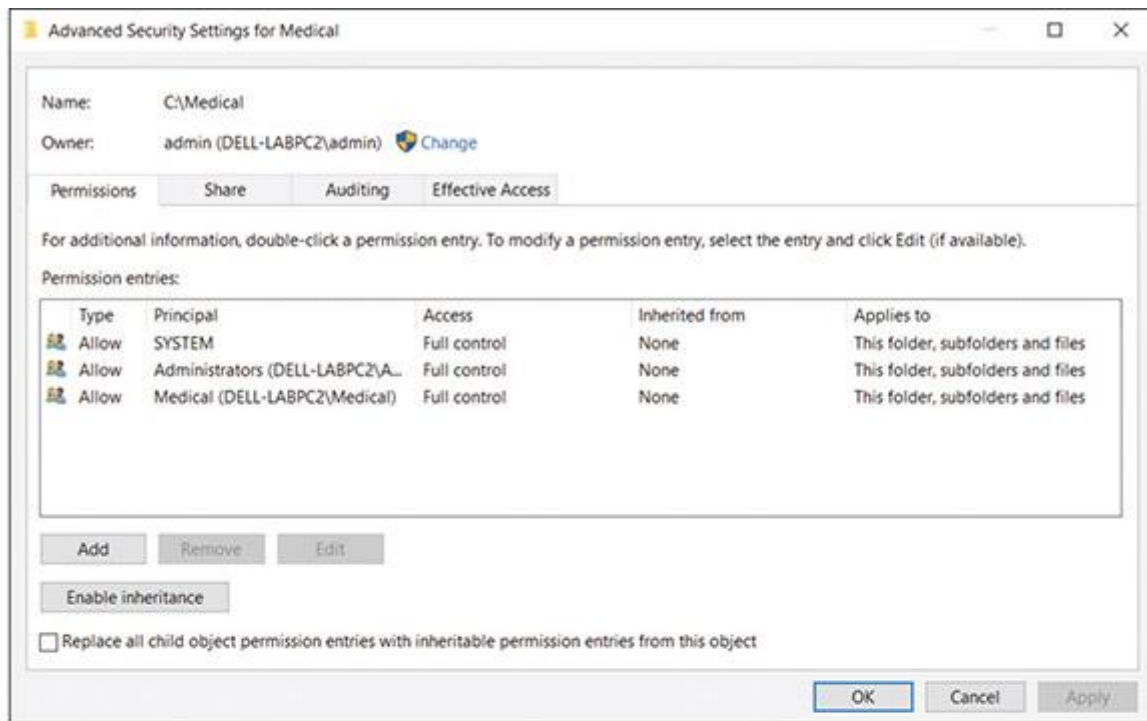
The user account name and password on the remote computer must match the user account and password on the host computer. If these accounts and passwords don't match, the user is considered an anonymous user and is denied access to resources shared on the remote computer. To verify that account names and passwords match, open the **Local Users and Groups** console, where you can view user account names, create new accounts, and set or reset passwords.

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

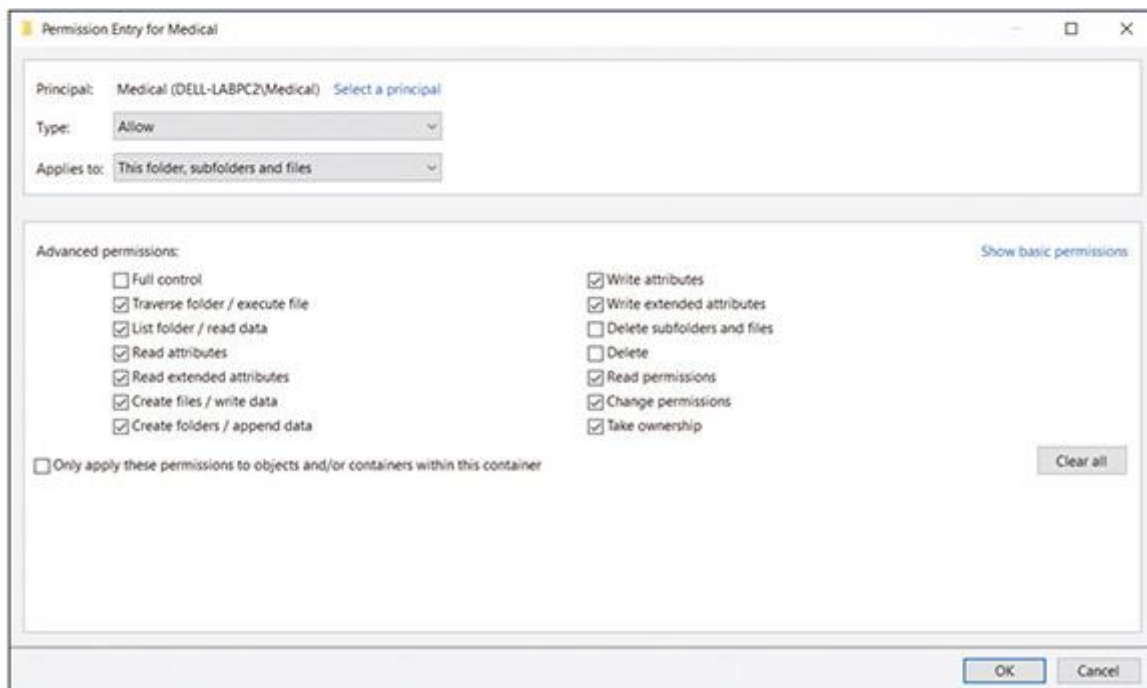
- **Use advanced permissions settings.** If you need further control of the permissions assigned to a user or group, click **Advanced** on the Security tab of a folder's Properties dialog box. The Advanced Security Settings dialog box appears (see [Figure 17-27A](#)). You can see that the Medical user 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 dialog box opens. Click **Show advanced permissions** to see these advanced permissions, as shown in [Figure 17-27B](#).

Figure 17-27

Advanced permissions settings



(A)



(B)



- 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 dialog 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.)



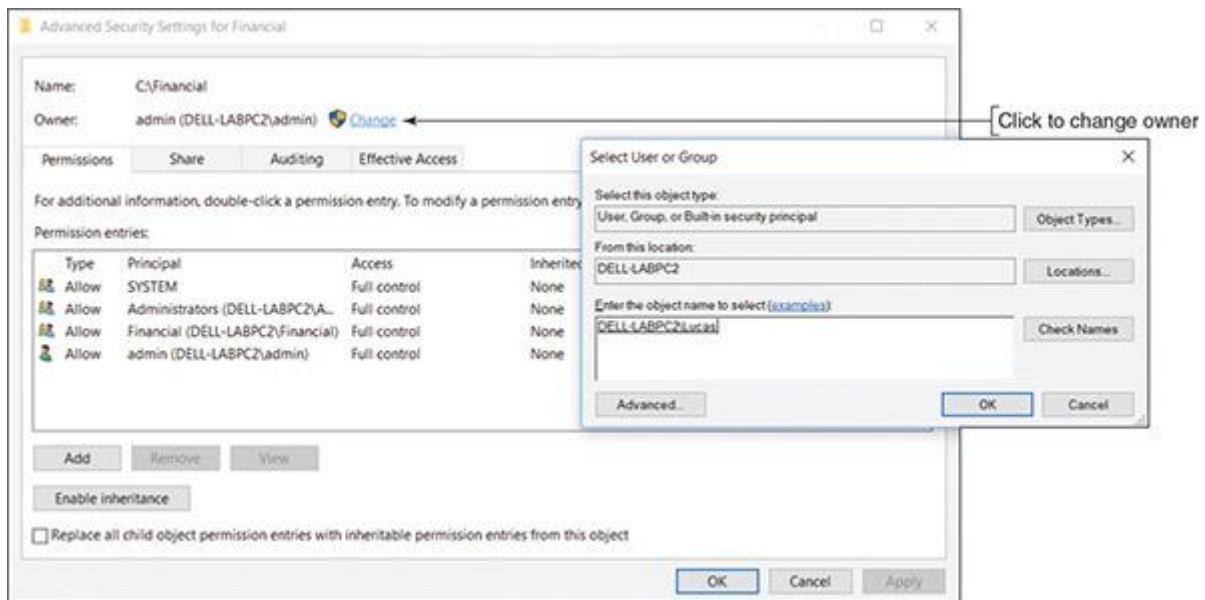
Exam Tip

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 to 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.** Explicit permissions can be manually set for a subfolder or file, which overrides inherited permissions. When a folder or file has inherited and explicit permission set, it might be confusing to know exactly which permissions are in effect. To find out, see the **Advanced Security Settings** dialog box. (Refer back at [Figure 17-27A](#).) NTFS permissions are reported on the Permissions tab and share permissions are reported on the Share tab. (If the Share tab is missing, share permissions are not set.) Use the Effective Access tab 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 dialog box. The Advanced Security Settings dialog box appears. Next to the name of the owner, click **Change**. You can then enter the name of the new owner (see [Figure 17-28](#)). Click **Check Names** to confirm the name is entered correctly, and click **OK** twice.

Figure 17-28

Change the owner of a folder



- **Use only one workgroup.** On a peer-to-peer network, it's 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 the network path to access a shared folder.** To access shared folders on the network in the Explorer navigation bar or in a command prompt window, type the **network path** to the share as two backslashes, the computer name, one backslash, and the folder name, as shown in [Figure 17-29](#) for Explorer and in a command line in [Figure 17-30](#).

Figure 17-29

Network path to a shared folder using the Explorer navigation bar

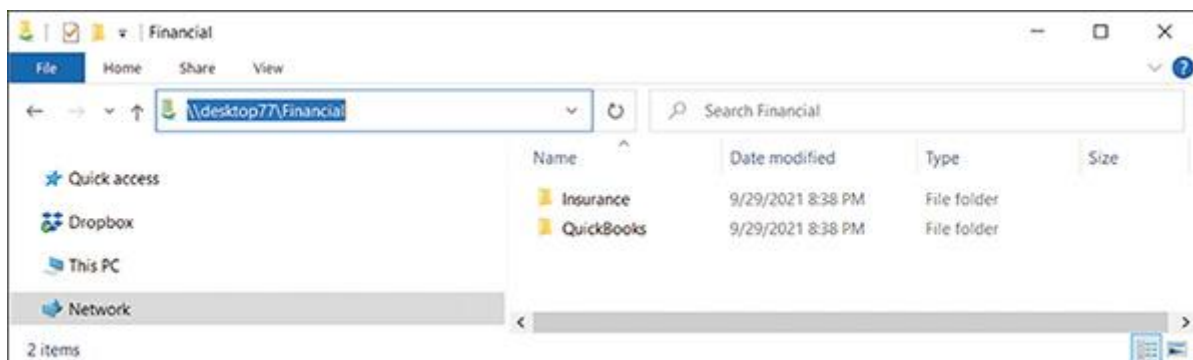
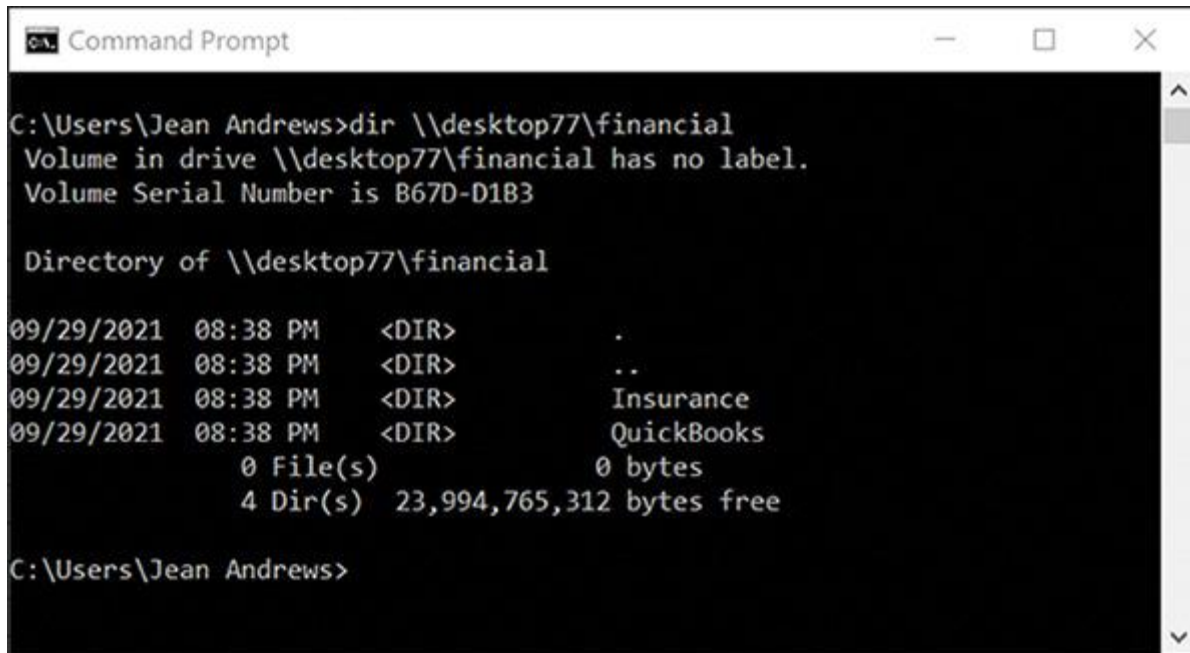


Figure 17-30

Network path to a shared folder using a command line



```
Command Prompt

C:\Users\Jean Andrews>dir \\desktop77\financial
Volume in drive \\desktop77\financial has no label.
Volume Serial Number is B67D-D1B3

Directory of \\desktop77\financial

09/29/2021  08:38 PM    <DIR>          .
09/29/2021  08:38 PM    <DIR>          ..
09/29/2021  08:38 PM    <DIR>          Insurance
09/29/2021  08:38 PM    <DIR>          QuickBooks
               0 File(s)                0 bytes
               4 Dir(s) 23,994,765,312 bytes free

C:\Users\Jean Andrews>
```

- **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.

17-2d How to Map a Network Drive or Network Printer

Core 2 Objective

- 1.6

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

A **mapped drive**, also called a **network share**, is one of the most powerful and versatile methods of communicating over a network. A mapped drive 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** the drive. In addition to mapping a network drive, you can also map a network printer to a computer.

Note 15

By default, this client/server arrangement is managed by the Windows Server Message Block (SMB) protocol, which you first learned about in the Core 1 module “[Networking Fundamentals](#).” Alternately, Windows can use the Network File System (NFS) protocol, which is compatible with Linux and UNIX file sharing on the network. Linux and UNIX also support Windows SMB via the Samba application. You learn more about Samba in the module “[Linux and Scripting](#).” Regardless of which protocol is used, host computers using different OSs—such as Windows, macOS, or Linux—can still share network resources.

Applying Concepts

Mapping a Network Drive and Network Printer

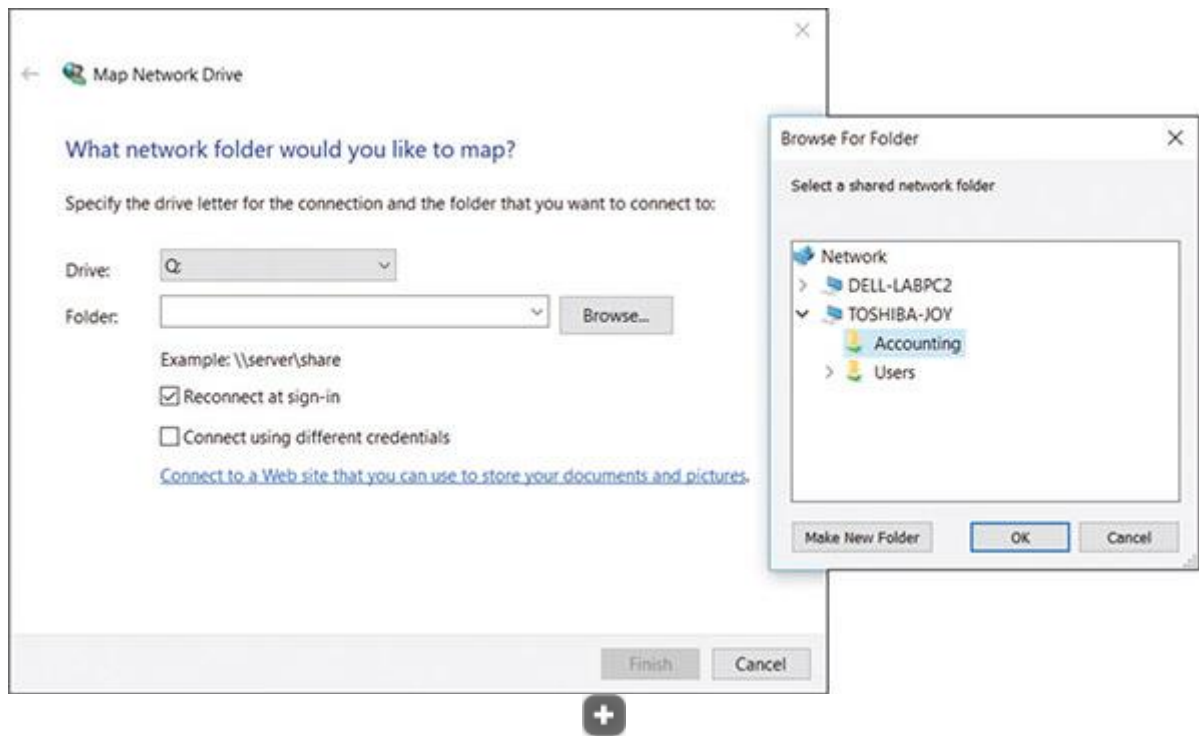
- **Est. Time:** 30 minutes
- **Core 2 Objective:** 1.6

To set up a network drive, follow these steps:

1. **1**
On the host computer, share the folder or entire volume to which you want others to have access.
2. **2**
On the remote computer that will use the network drive, open **Explorer**. In the left pane, click **This PC**. For Windows 10, at the top of the window, click the **Computer** tab, and click **Map network drive**. For Windows 11, at the top of the window, click the ... *See more* icon, and select **Map network drive**.)
3. **3**
The Map Network Drive dialog box opens, as shown on the left side of [Figure 17-31](#). Select a drive letter from the drop-down list.

Figure 17-31

Mapping a network drive to a host computer



4. **4** Click the **Browse** button, and locate the shared folder or drive on the host computer (see the right side of [Figure 17-31](#)). 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.

Note 16

When mapping a network drive, you can type the network 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 type the network path—for example, `\\FILESERVER\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 learn about the net use command in the module “[Network Security and Troubleshooting](#).”



Core to Core

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 the Core 1 module “[Networking Fundamentals](#).”

Note 17

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.

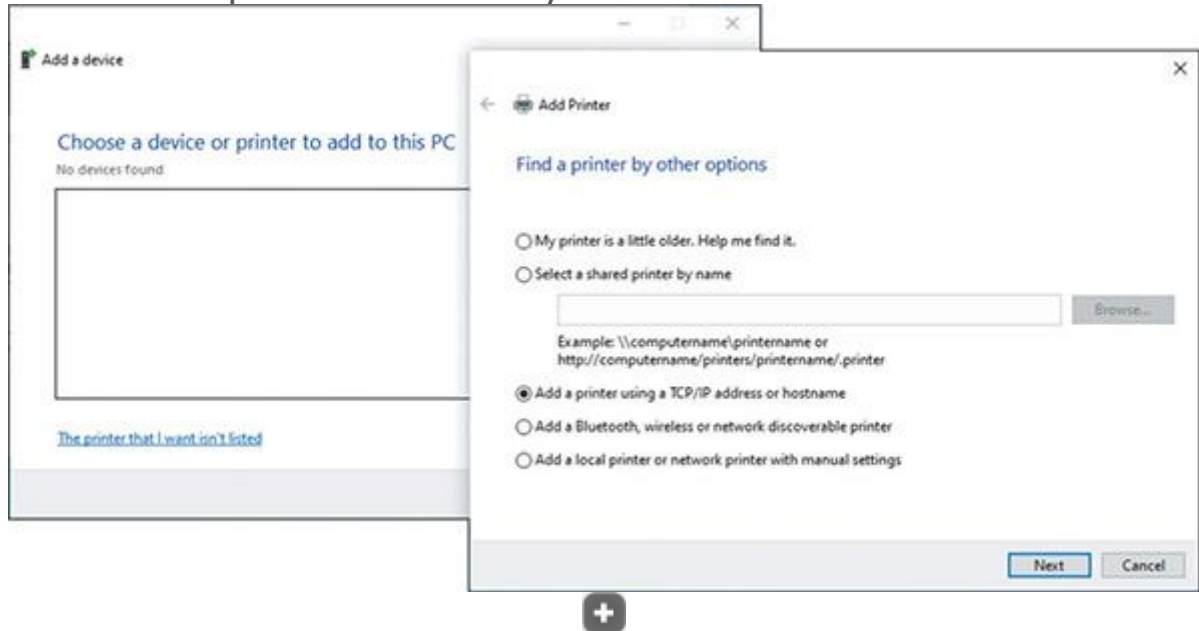
To install a network printer, follow these steps:

1. **1**

In Control Panel in classic view, open the **Devices and Printers** applet, and click **Add a printer**. Windows searches for available printers. If the printer is not found, click **The printer that I want isn't listed**. See the left side of [Figure 17-32](#).

Figure 17-32

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



2. **2**

In the Add Printer dialog box (see the right side of [Figure 17-32](#)), select **Add a printer using a TCP/IP address or hostname**, and click **Next**.

3. **3**

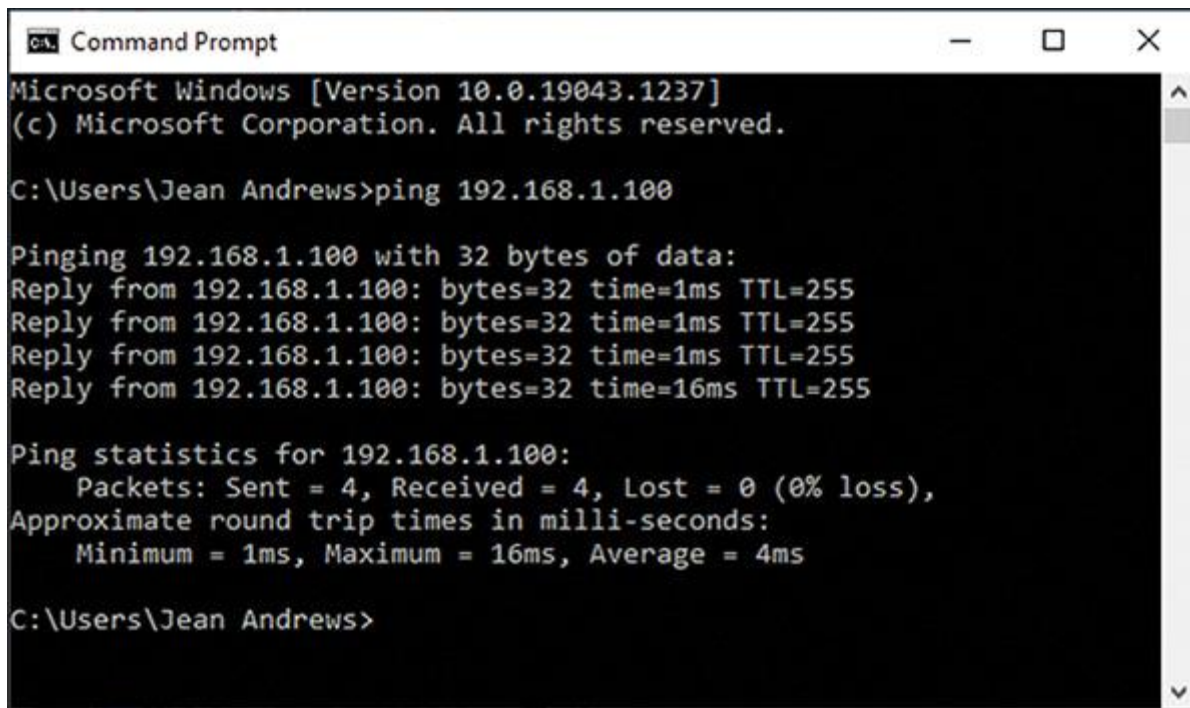
Enter the printer's IP address or hostname, and click **Next**. Windows searches the network for the printer. If it finds the printer, the installation proceeds, and you can select the printer manufacturer and model and then name the printer (for example, CanonInHallway). Alternately, you can provide printer drivers that you can download to your computer. After the printer is installed, be sure to print a test page.

If you have problems installing a network printer, do the following:

- To verify the printer is online and you know its IP address, open a command prompt window and use the ping command, as shown in [Figure 17-33](#).

Figure 17-33

Ping a printer to verify it is online and the IP address is correct

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The text inside shows the Windows version as 10.0.19043.1237 and copyright for Microsoft Corporation. The user is at the prompt "C:\Users\Jean Andrews>". They have entered the command "ping 192.168.1.100". The output shows four successful replies from 192.168.1.100 with 32 bytes of data, times of 1ms, 1ms, 1ms, and 16ms, and a TTL of 255. Ping statistics show 4 packets sent and received with 0% loss, and round trip times of 1ms minimum, 16ms maximum, and 4ms average. The prompt "C:\Users\Jean Andrews>" is shown again at the bottom.

```
Microsoft Windows [Version 10.0.19043.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Jean Andrews>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=1ms TTL=255
Reply from 192.168.1.100: bytes=32 time=1ms TTL=255
Reply from 192.168.1.100: bytes=32 time=1ms TTL=255
Reply from 192.168.1.100: bytes=32 time=16ms TTL=255

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 4ms

C:\Users\Jean Andrews>
```



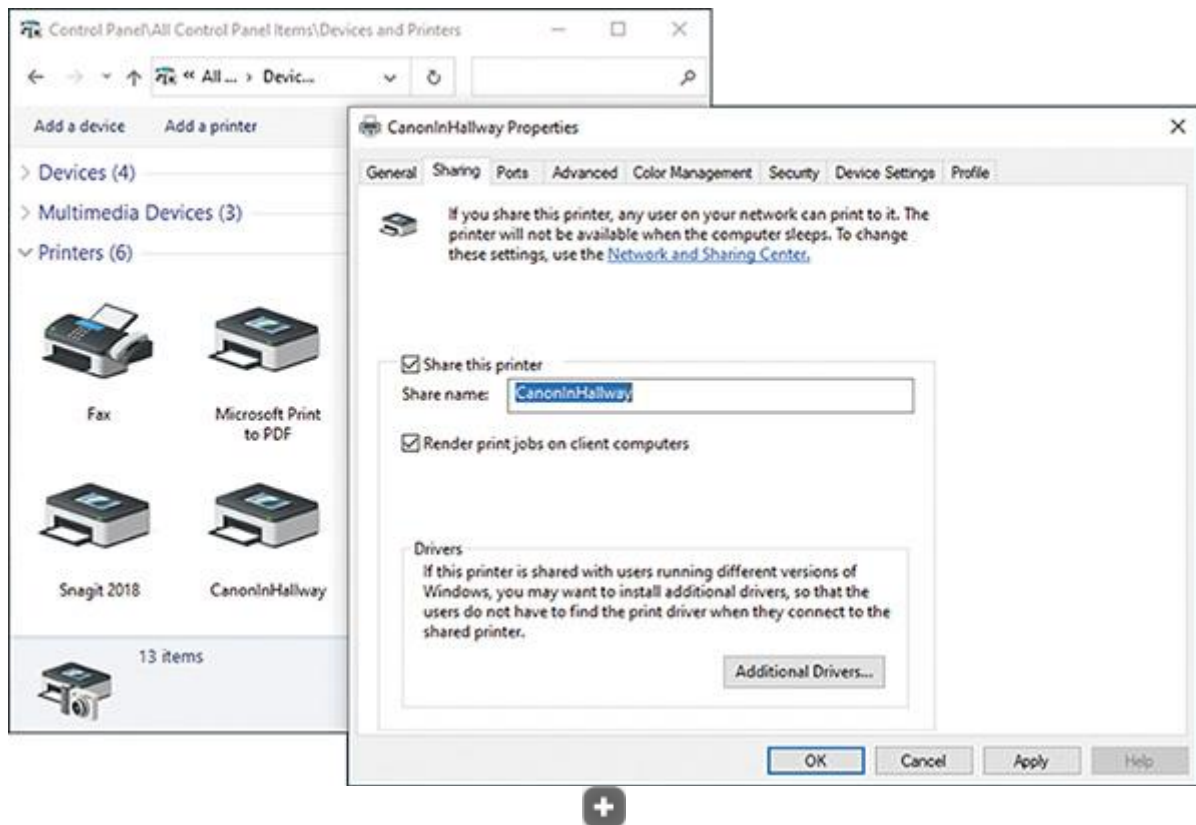
- Download the printer drivers from the website of the printer manufacturer, and follow the manufacturer's directions to install the printer.

After you have installed a local printer, you can share it with others on the network. Follow these steps:

1. **1**
In the Devices and Printers window, right-click the printer, and click **Printer properties**.
2. **2**
In the Properties dialog box, click the **Sharing** tab, and check **Share this printer**. See [Figure 17-34](#). You can change the Share name and decide whether print jobs are to be rendered (produced) on this computer or client computers. Click **Apply**. The two-person share icon appears beside the printer in the Devices and Printers window.

Figure 17-34

Share a local printer to the network



Other computers on the network can now see the printer in their Explorer window when they drill down into resources shared by the computer. To install the printer on a client computer, right-click the printer and click **Connect**.



Core to Core

More information about managing shared printers is covered in the Core 1 module [“Supporting Printers.”](#)



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.

17-2e Hidden Network Resources and Administrative Shares

Core 2 Objective

- 1.6

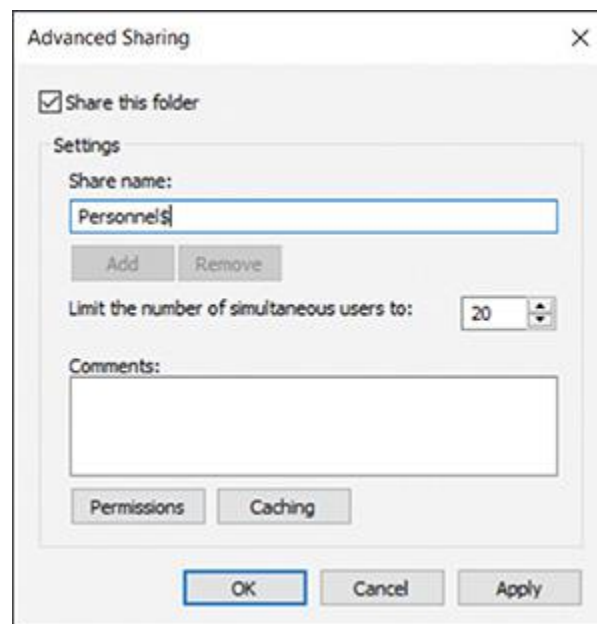
Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Sometimes you may need to secretly share a file or folder on the network or ensure that a folder or file is not visible or accessible from the network or by other users. 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 Explorer, add a \$ to the end of the share name in the Advanced Sharing dialog box, as shown in [Figure 17-35](#). This shared and hidden folder is called a **hidden share**. Others on the network can access the folder only when they know its network path. For example, to access a shared folder named Personnel\$ on the computer named Desktop77, a user must enter \\Desktop77\Personnel\$ in the Explorer navigation bar.

Figure 17-35

A \$ at the end of the share name hides the share unless the exact name is used in a network path to locate it

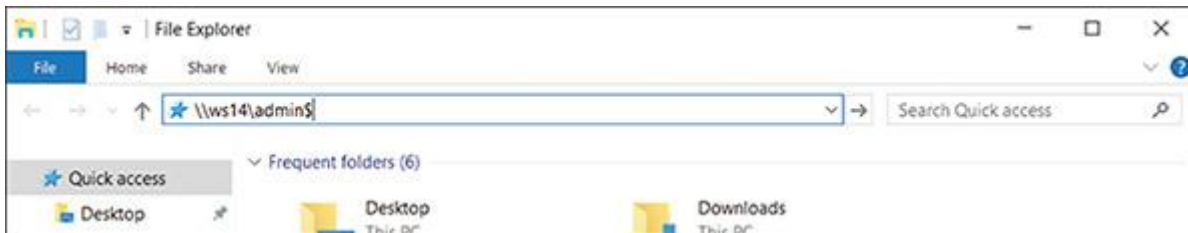


So far in this module, you have learned about folders and files on a computer that are shared with other users on the network; these shares are called **local shares**. For computers that belong to a domain, you need to be aware of another way folders are shared, called administrative shares. **Administrative shares** 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. The following are two types of administrative shares:

- **The %systemroot% folder.** Enter the path `\\computername\admin$` to access the %systemroot% folder (most likely the C:\Windows folder) on a remote computer in order to work with that computer's system folders and files. For example, to connect to the ws14 workstation shown in [Figure 17-36](#), the entry in the Explorer navigation bar is `\\ws14\admin$`. The authenticate dialog 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**.

Figure 17-36

Access an administrative share on a domain



- **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$`.



Exam Tip

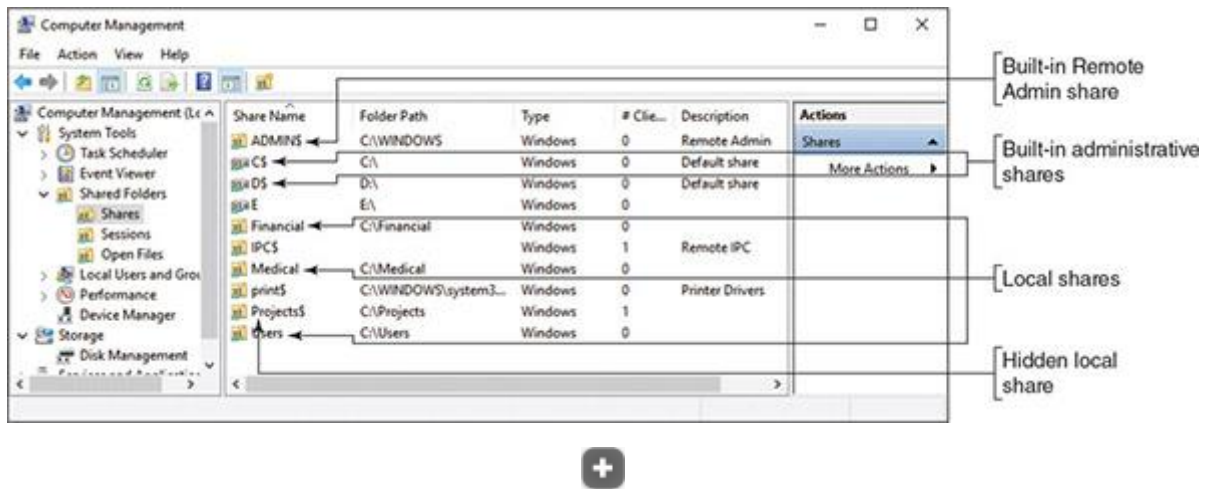
The A+ Core 2 exam expects you to understand the difference between administrative shares and local shares.

Note 18

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 17-37](#)).

Figure 17-37

Use the Computer Management console to view all shares



! 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.

17-3 Using Active Directory Domain Services

Core 2 Objective

• 2.1

Summarize various security measures and their purposes.

Recall that 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:

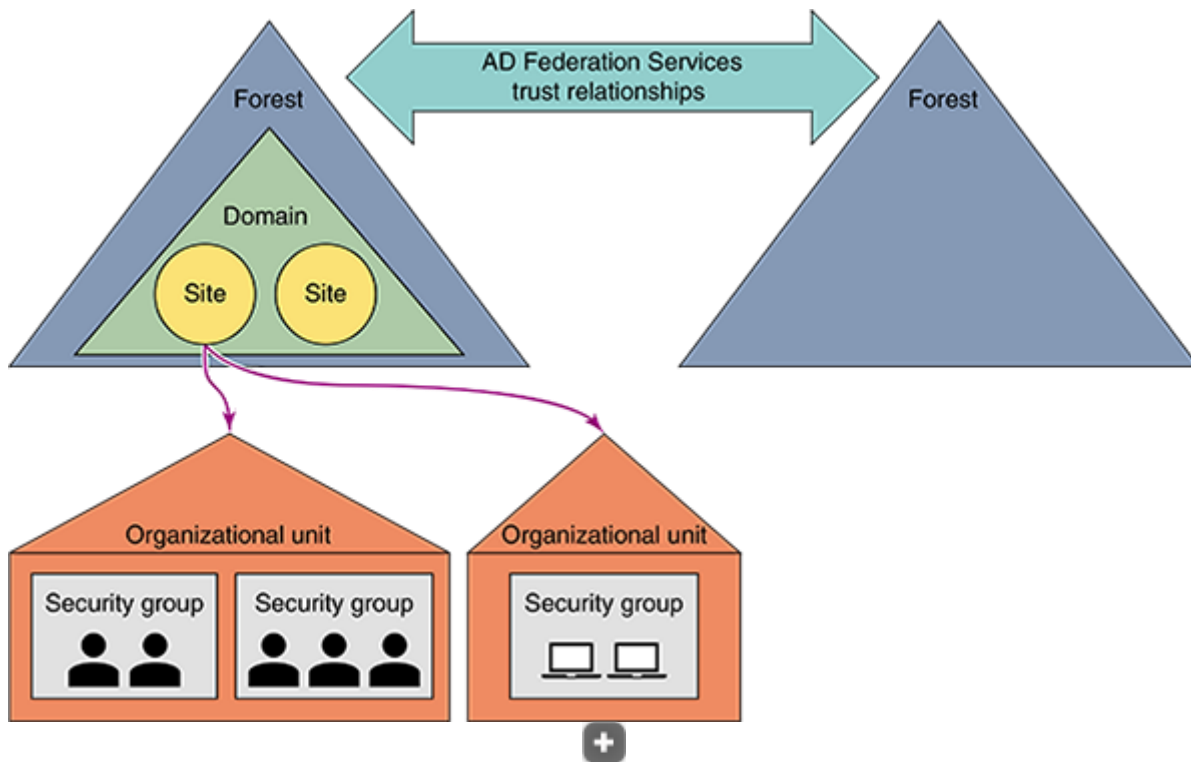
- **Active Directory Domain Services (AD DS)** authenticates accounts and authorizes what these accounts can do.
- AD Certificate Services (AD CS) secures identities of services, computers, and users.
- AD Federation Services (AD FS) secures trust relationships with outside organizations.
- AD Rights 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 17-38](#). Users and resources of a company or school managed by AD are organized into a **forest** (the entire enterprise), which contains a domain (for example, [mycompany.com](#)). For a few very large

enterprises, domains can contain subdomains (for example, mycompany.com and mycompany-dev.com), 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 and sites are also organized into various organizational units.

Figure 17-38

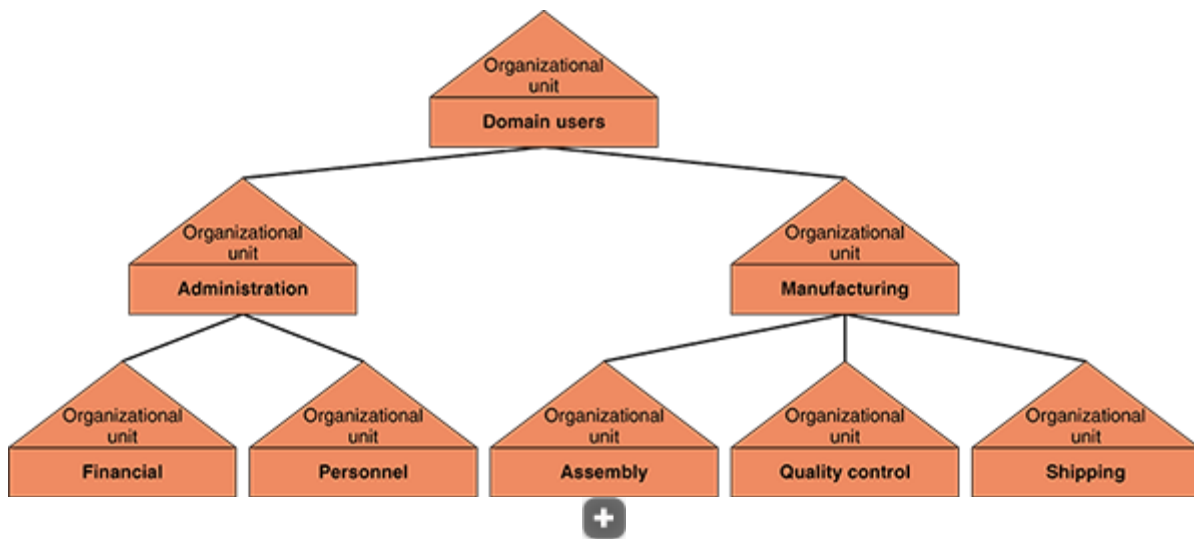
The Active Directory organizational structure



Organizational units (OU) are created to make it easier for technicians to assign privileges to users and computers that are assigned to an OU. In general, an administrator creates an OU tree to follow the job descriptions within an organization. For example, [Figure 17-39](#) shows the Domain Users OU includes everyone in the company. Other OUs are created based on job responsibilities. Although it is possible to put users and computers in the same OU, it is not recommended because generally their privileges are very different.

Figure 17-39

Organizational units structured to follow the organization of a company



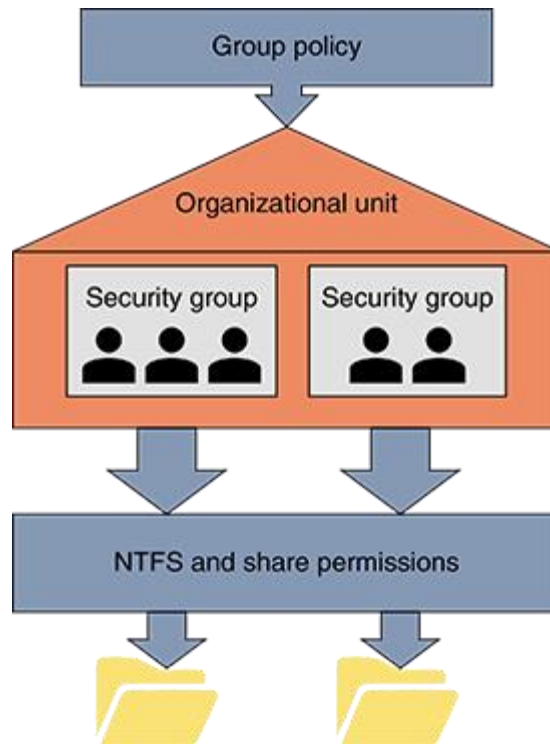
An OU can contain groups of users or computers called **security groups**, which are similar to user groups in a Windows workgroup except a security group can include a computer or a user.

Privileges are assigned to OUs using policies created by Group Policy. These policies are contained in **Group Policy Objects (GPOs)** that are applied to the OU and, by inheritance, to each security group, user, and computer in the OU.

Permissions assigned to folders work much the same way as they do in Windows 10/11. NTFS and share permissions are assigned to a folder on a server in the domain by assigning permissions to an OU or security group, and the users in this OU or group inherit these assigned permissions. In summary, managing resources in AD revolves around the tools shown in [Figure 17-40](#).

Figure 17-40

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



In this module, 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; resetting user account passwords; and managing login scripts. You also learn how Group Policy can be used to assign privileges to an OU and the security groups and users in the OU.

17-3a Creating and Managing User Accounts in AD

Core 2 Objective

- 2.1

Summarize various security measures and their purposes.

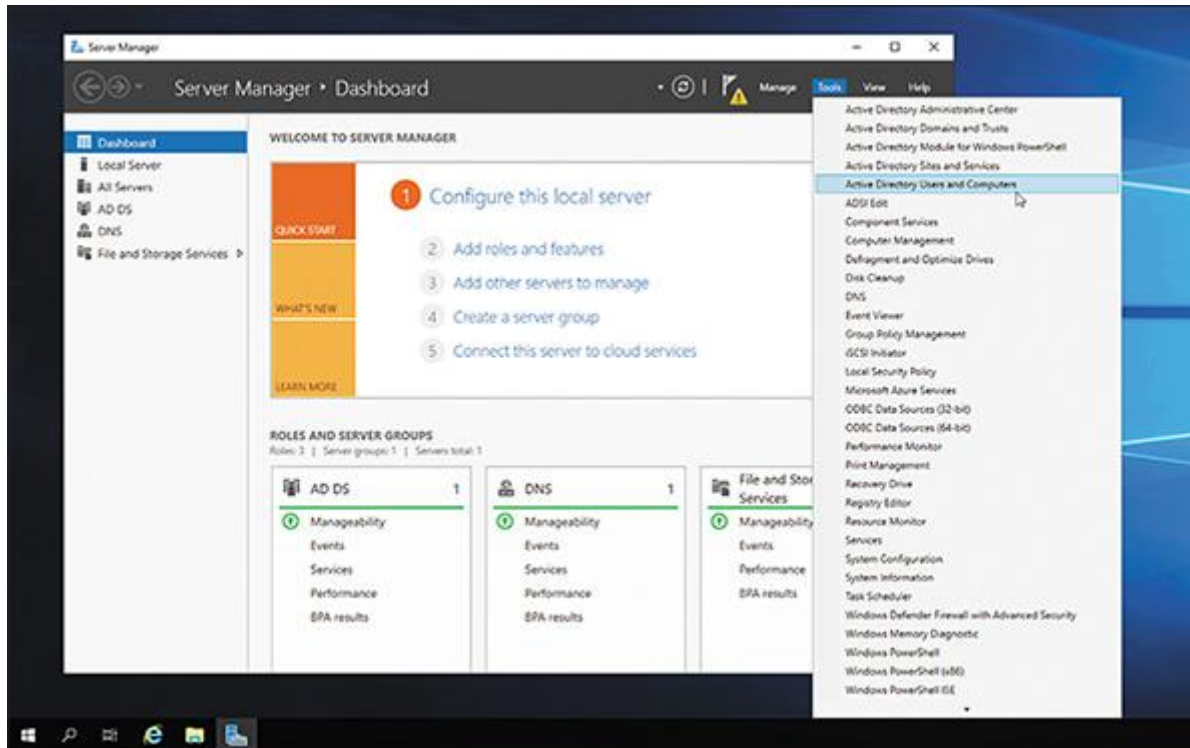
Before we discuss how to manage a user account on a Windows domain, let's pause to see how you can access Domain Services on the domain controller to get to the tools you need. You'll need a local administrator account for a Windows Server computer that is a domain controller. Then you can use one of 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 17-41](#) with the Tools menu open. The **Server Manager** console contains the tools used to

manage Active Directory and is included in Windows Server. It can also be installed in Windows 10/11.

Figure 17-41

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



- **Remote access via Remote Desktop.** You can use Remote Desktop from anywhere on the Internet to connect to a Windows Server computer, sign in, and open Server Manager. Details about Remote Desktop are covered in the module “[Network Security and Troubleshooting](#),” and you get a first look at it in a project at the end of this module. Remote Desktop is included in Windows 10/11 Pro and Enterprise editions.
- **Remote access via Windows Admin Center.** Windows Admin Center is a console you download and install for free in Windows 10/11. It works inside a browser and contains various tools for remotely managing Windows Server.

Note 19

If you don’t have access to Active Directory and a Windows domain to practice the skills in this part of the module, you can follow the steps in [Real Problem 17-2](#) at the end of this module to set up your own Windows domain in Windows Server using the free Google Cloud Platform at cloud.google.com.

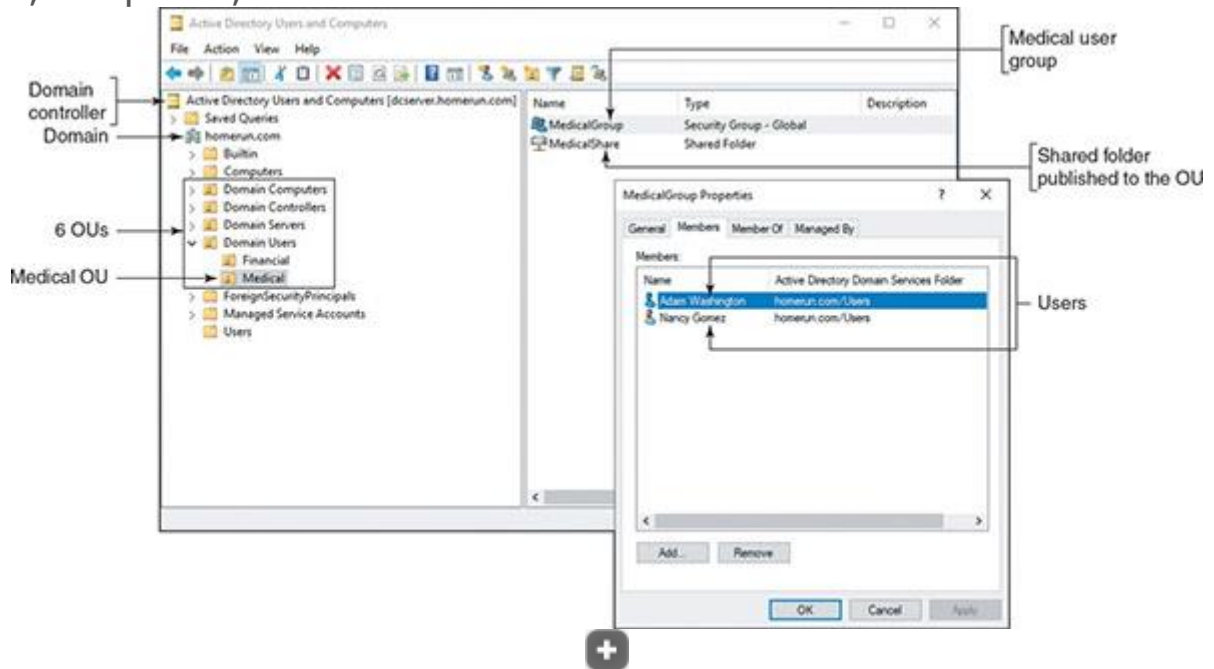
Use Server Manager and Create a New User

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. **1** Sign in to Windows Server with an administrator account, and open **Server Manager**.
2. **2** Click **Tools** (refer back to [Figure 17-41](#)), 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 17-42](#) shows the sample domain [homerun.com](#), which belongs to our fictitious company, Homerun Sports Medicine, Inc.

Figure 17-42

Users, computers, and OUs in the domain



There are six 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 dcserver.
- Domain Computers and Domain Servers OUs were created by the system administrator directly under the [homerun.com](#) domain so appropriate policies can more easily be applied to the computers assigned to these OUs.
- Domain Users OU was created directly under the [homerun.com](#) domain, and all users will be assigned to this OU. Domain Users contains two OUs: Financial and Medical. Each of these OUs contains a security group, and every new user will be assigned to one of these two security groups.

- In [Figure 17-42](#), note the Medical OU is selected, and it contains the MedicalGroup security group and one shared folder. (You can give an OU and a security group the same name, but to avoid confusion, use different names.)

3. **3**

Double-click the **MedicalGroup** to view its Properties dialog box. Click the **Members** tab to see that Nancy Gomez and Adam Washington are members of the group, as shown in [Figure 17-42](#).

Note 20

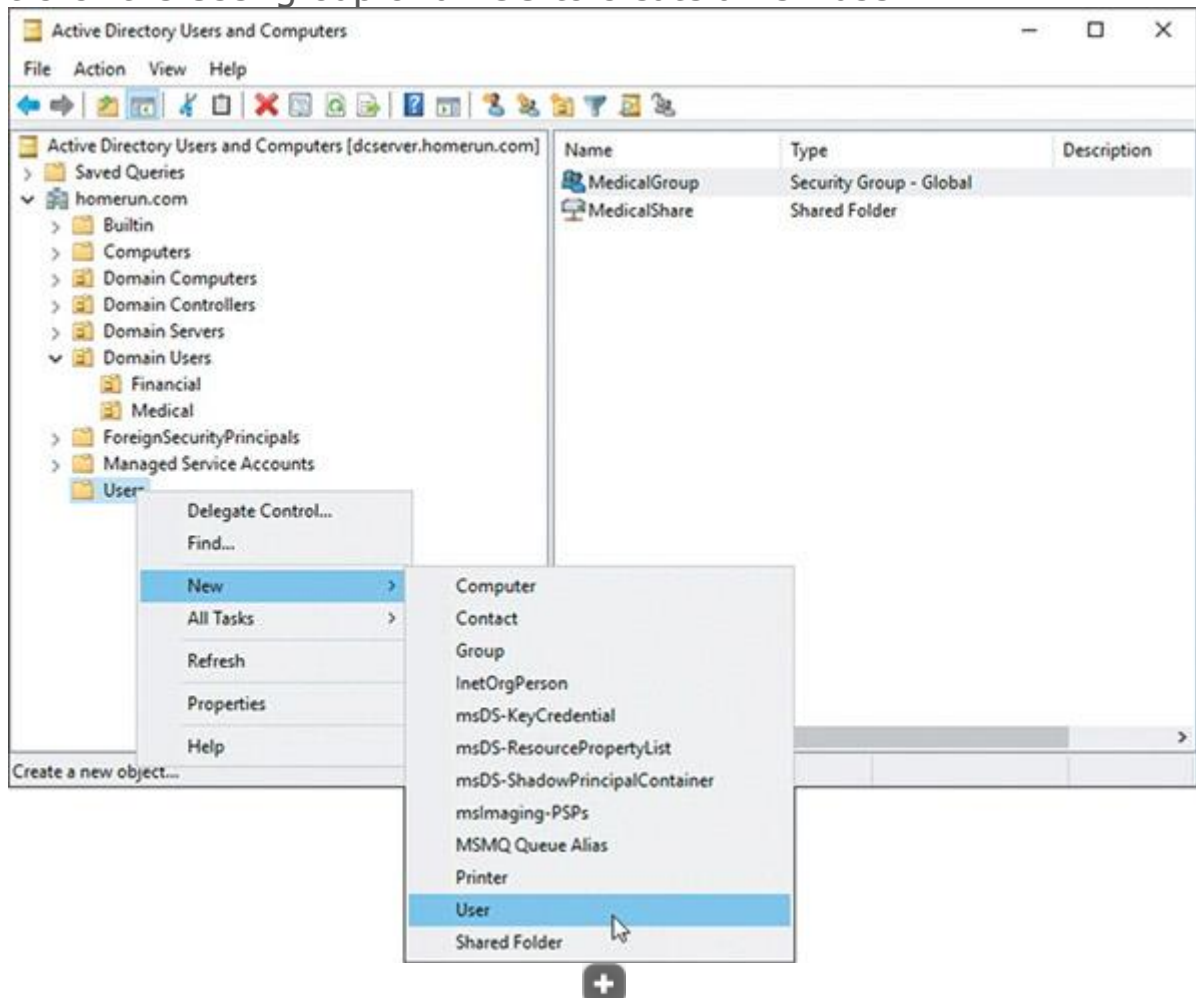
To share a folder in Active Directory, first set the folder's NTFS and share permissions for the security group, as you learned to do earlier in the module. Then, to publish the folder in AD, right-click the OU to which you want to include the folder, click **New**, click **Folder**, and point to the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

4. **4**

To add a new user, you can create the account inside an OU. (Right-click the OU, point to **New**, and click **User**.) Alternately, you can add the new user to the User folder. Right-click **User**, point to **New**, and click **User**, as shown in [Figure 17-43](#).

Figure 17-43

Right-click the User group or an OU to create a new user



Note 21

Organizations differ in the methods used to manage OUs, security groups, and users. Some prefer to create all users in the Users folder and then assign each user to an OU. Other organizations prefer to initially create the user in the OU. Also, the way OUs are organized differs greatly from one organization to another.


5. **5**

Enter the user's first name, last name, and user name (see [Figure 17-44A](#)). Click **Next**. On the next screen, decide how to handle the password (see [Figure 17-44B](#)).

Figure 17-44

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

New Object - User ✕

 Create in: homerun.com/Users

First name: Initials:

Last name:


Full name:

User login name:

User login name (pre-Windows 2000):

(A)

New Object - User ✕

 Create in: homerun.com/Users

Password:

Confirm password:

☒ User must change password at next login

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

(B)

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 login.
- 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.

6. **6**

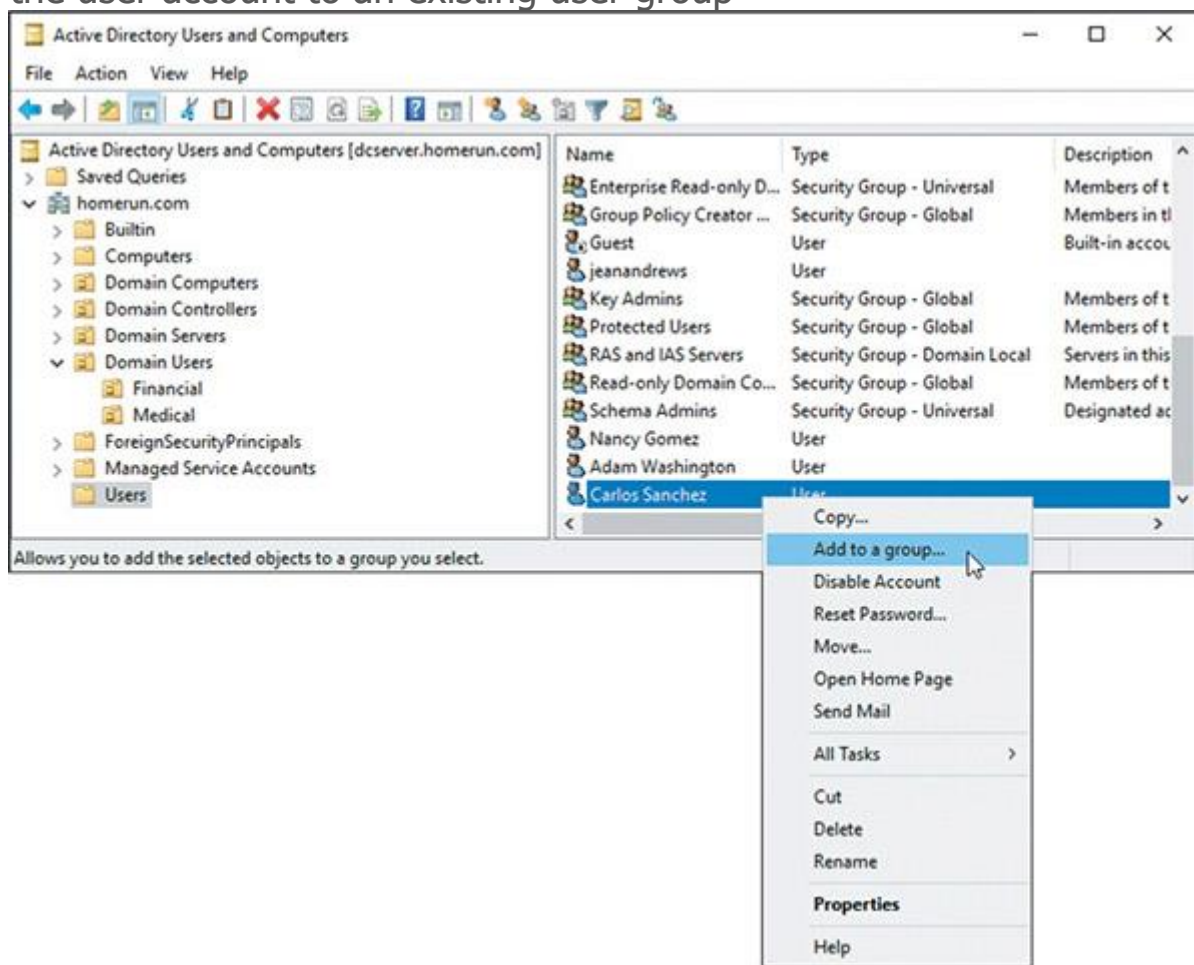
Click **Next** and click **Finish**. The account is created.

7. **7**

After the account is created, you can add it to an existing security group. Right-click the user account and click **Add to a group** (see [Figure 17-45](#)).

Figure 17-45

Add the user account to an existing user group

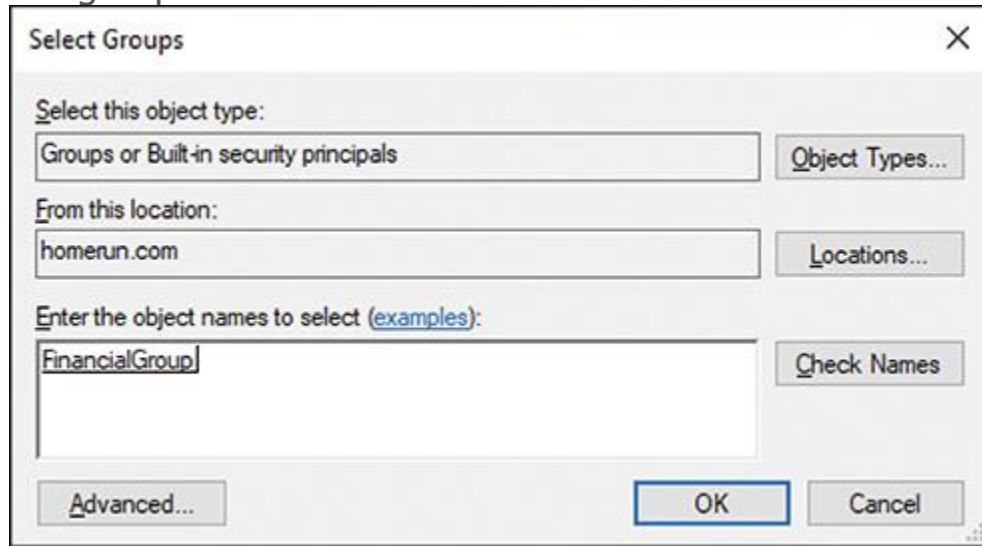


8. **8**

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 17-46](#)).

Figure 17-46

Type the user group name and click Check Names



Note 22

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

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

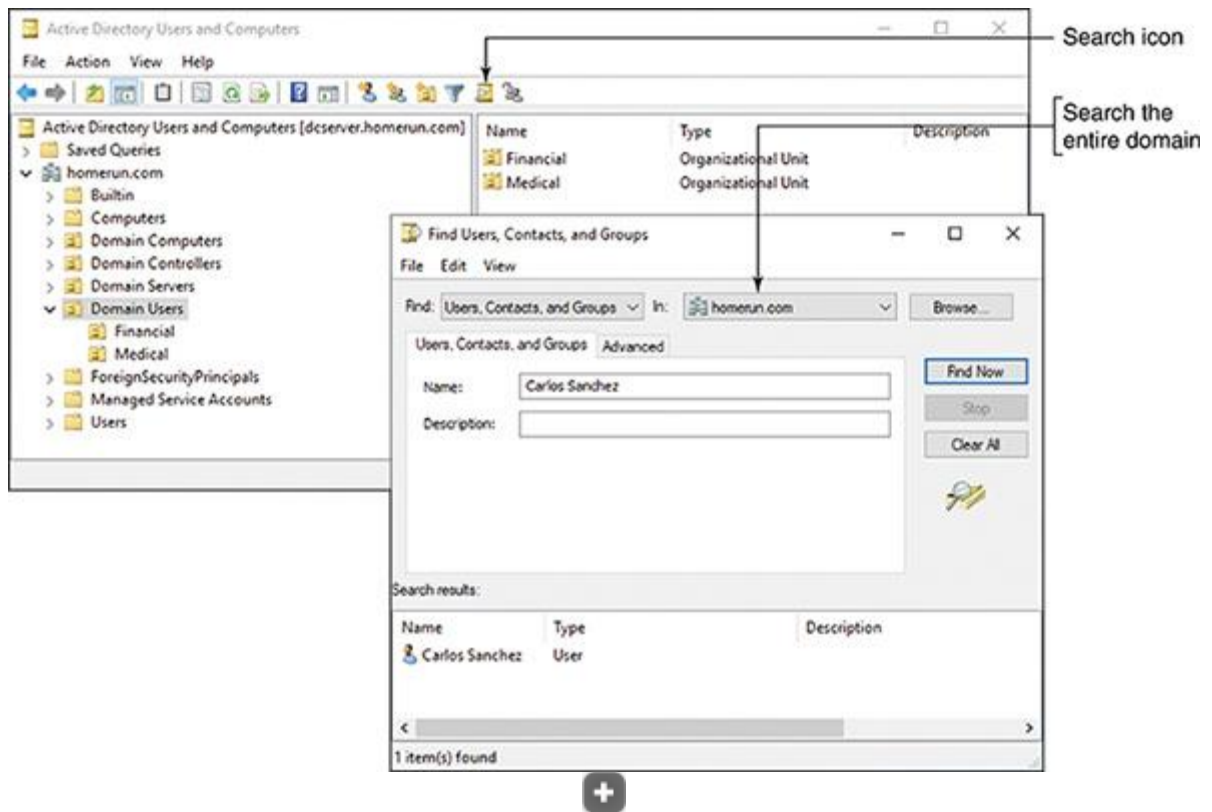
Manage Accounts and Passwords

An account might get locked after too many failed attempts to sign in. If the user says they know 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 17-47](#)).

Figure 17-47

Search for a user account



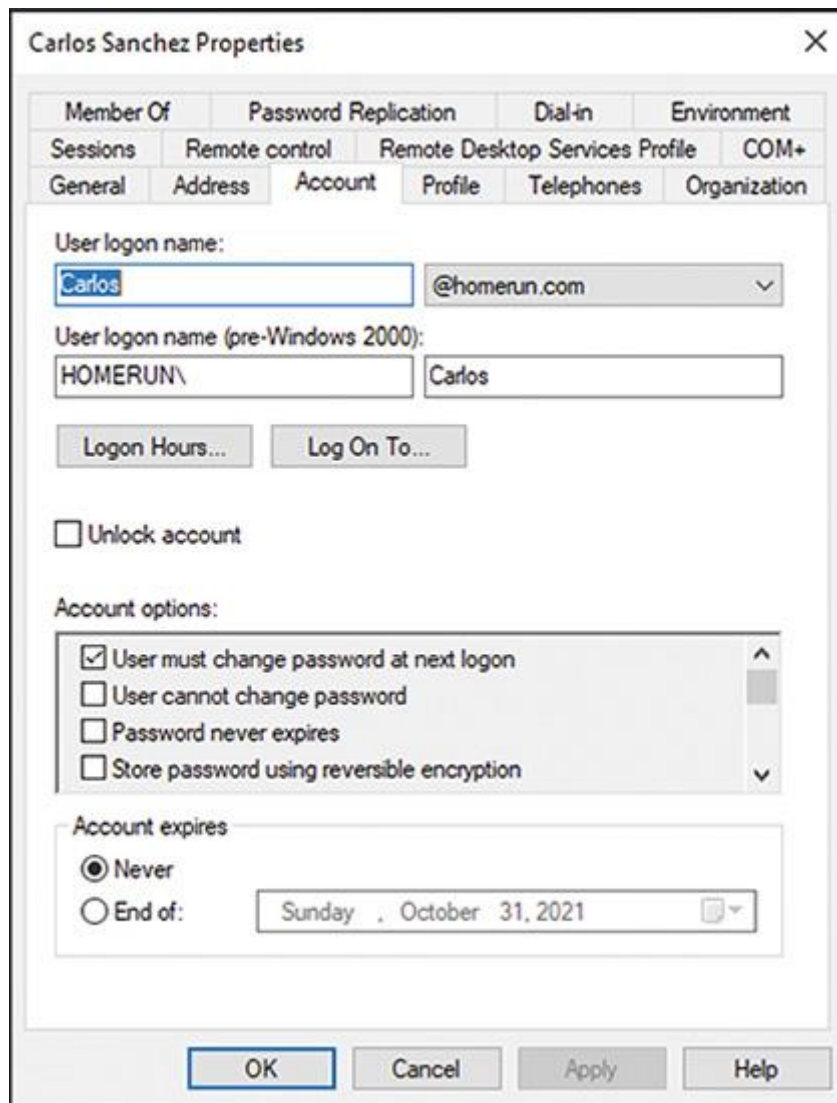
-
- Near the top of the Find Users, Contacts, and Groups dialog box, notice you can filter the search using the drop-down menus. Enter the name of the account and click **Find Now**. Double-click the account in the list of matches that appears. The account's Properties dialog box appears.
-
- If you know where to find the account, drill down to it, right-click it, and select **Properties**.

2. **2**

In the Properties dialog box for the account, select the **Account** tab (see [Figure 17-48](#)), check **Unlock account**, and click **Apply**. The user should then be able to sign in. (Also note that you can click the **Member Of** tab to find out which OUs and security groups the user belongs to.)

Figure 17-48

Unlock a locked account

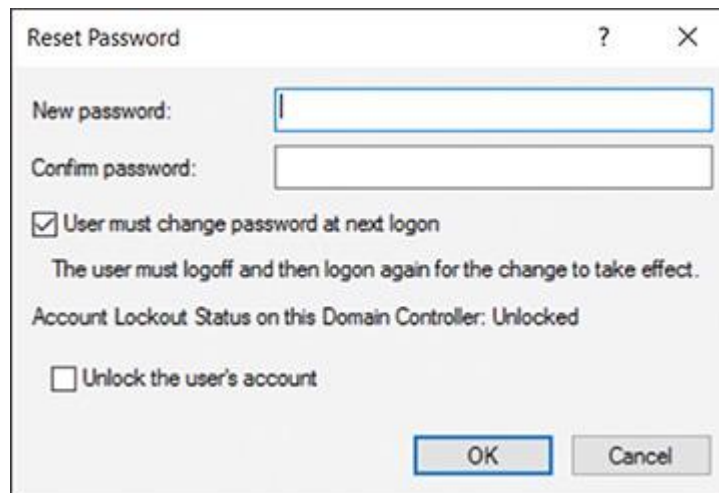


Follow these steps to reset a forgotten password and disable, enable, or delete an account:

1. **1** Locate the account and right-click it. In the shortcut menu, click **Reset Password** (refer back to [Figure 17-45](#)). In the Reset Password dialog box (see [Figure 17-49](#)), 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 17-49

Reset the user password



2. **2**

In the account's shortcut menu shown earlier in [Figure 17-45](#), 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 dialog box.

Note 23

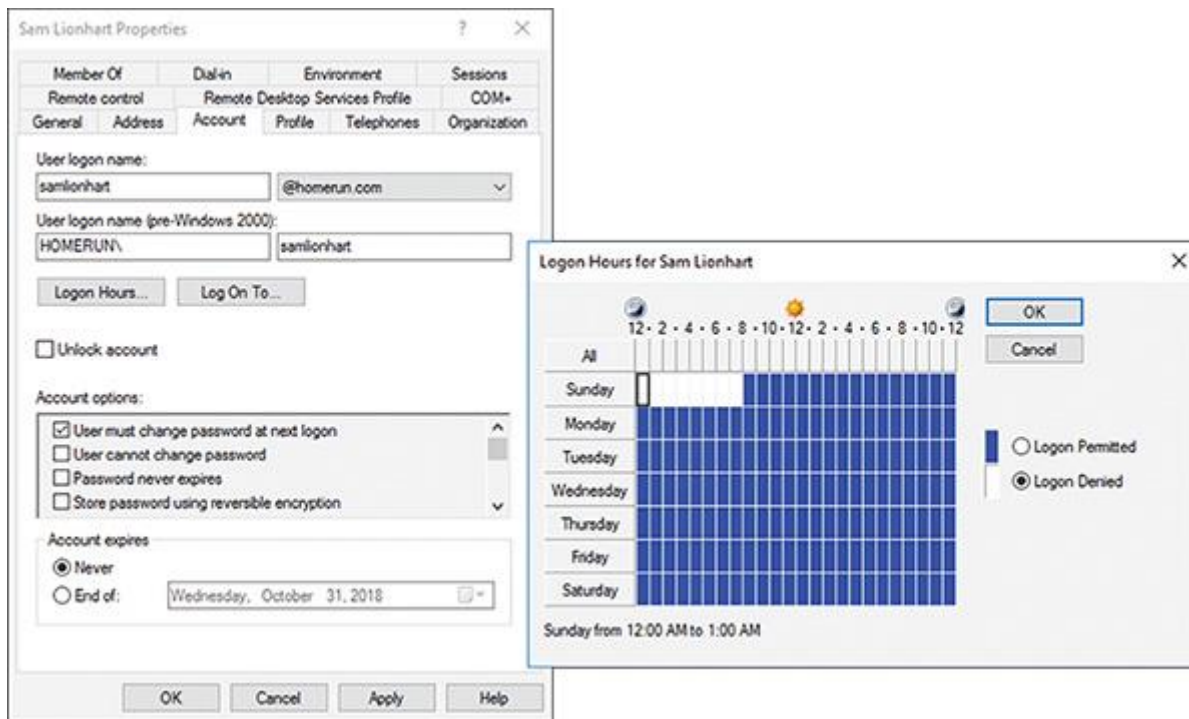
The user account is considered an object in Active Directory. When you delete an AD object, it goes to the Active Directory Recycle Bin, where it can be recovered until the Recycle Bin is emptied.

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 8:00 a.m. every Sunday is restricted for routine maintenance. To set logon time restrictions, open the user's **Properties** dialog box, select the **Account** tab, and click **Logon Hours** (see [Figure 17-50](#)). Click an hour, and then click **Logon Denied**. Notice that in [Figure 17-50](#), midnight to 8:00 a.m. on Sunday is denied.

Figure 17-50

Logon time restrictions

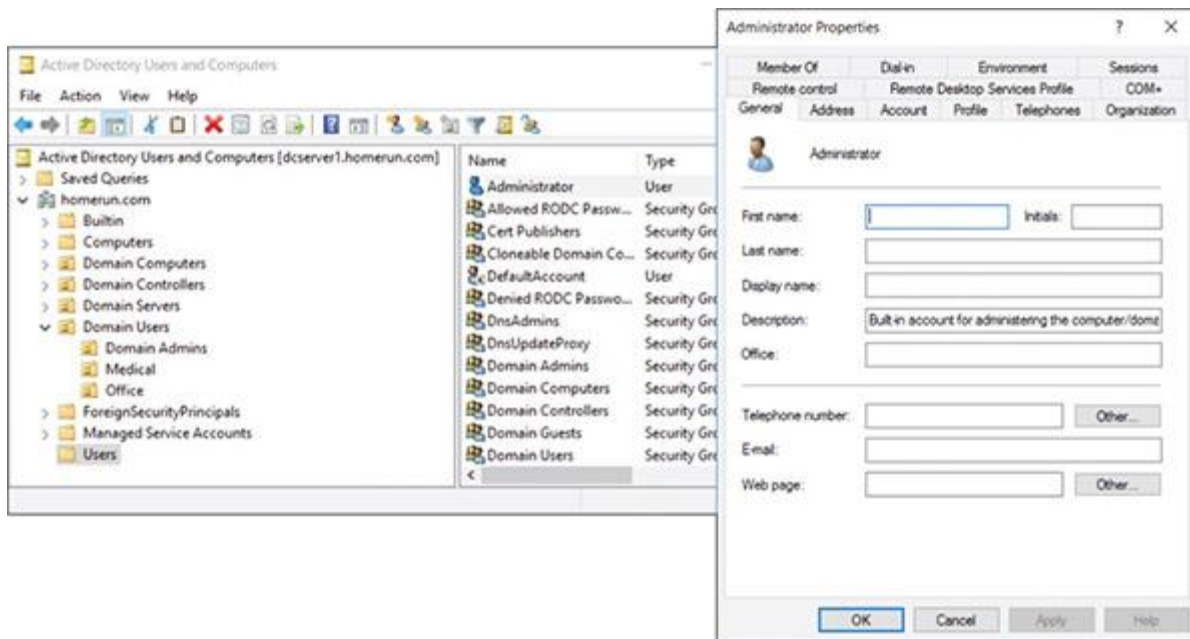


- **Timeout and screen lock.** On the Sessions tab of the user's Properties dialog box, you can limit how long a session remains disconnected before it ends (never or up to two days), how long an active session stays up (never or up to two days), and how long an idle session stays up. After you have 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 17-51](#). To change the password of the Administrator account, you can run the following command in an elevated command prompt window in Windows Server:

- `net user Administrator <password>`

Figure 17-51

Manage the properties of the Administrator account



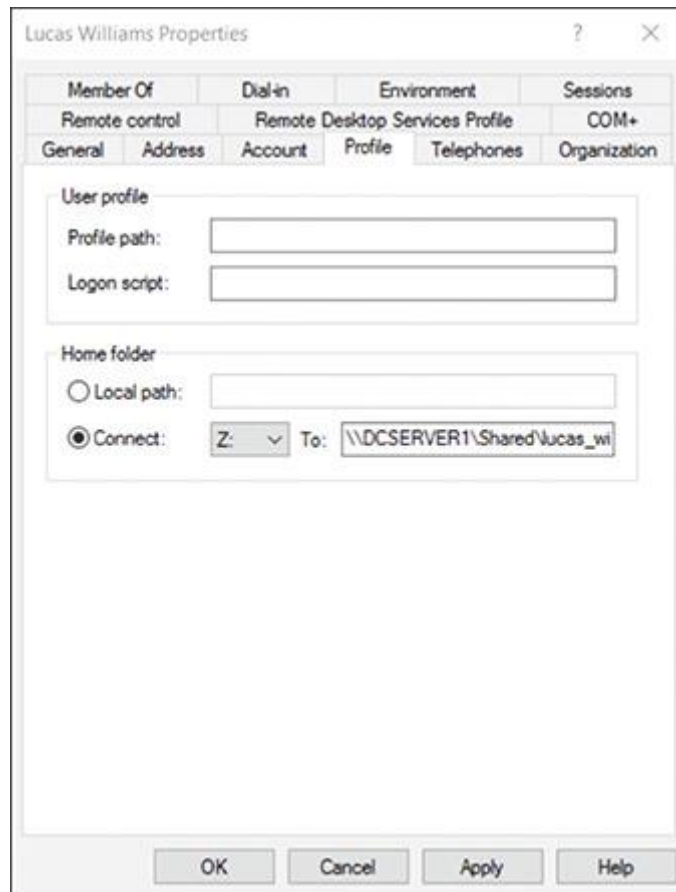
- **Home folder.** The **Home folder** is the default folder that is presented to the user whenever they are ready to save a file. On a peer-to-peer network, the Home folder in Windows is normally the Documents folder in the user profile at C:\Users\username\Documents. Active Directory is able to change this Home folder location to a share on the network, which is called **folder redirection**. Here are two reasons to apply folder redirection to the Home folder:

- On a domain, a user might sign in to different computers. When their Home folder is stored on the network, it's always available and does not need to be copied to each computer they use.
- 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 their local computer or on the network, select the **Profile** tab of the user's Properties dialog box (see [Figure 17-52](#)). For this user, the Home folder is in a network share.

Figure 17-52

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



Note 24

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**, also called a login 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, to assign the script to a single user, select the **Profile** tab in the user's Properties dialog box. See [Figure 17-52](#). Under Logon script, enter the name of the script file along with its file extension.
- **Multifactor authentication.** Some organizations require multifactor authentication (MFA) to sign in a domain to protect the credentials of certain privileged users. Azure Active Directory in the Microsoft cloud can implement the optional Microsoft Identity Manager (MIM) system that requires MFA along with other security measures to protect these privileged accounts. In addition, Windows Server Active Directory on

premises can provide Privileged Access Management (PAM) that works with MIM to enforce MFA as well as other security measures.

How these systems are implemented is beyond the scope of this text. Normally, when you want to change a setting for a single user, you use the user's Properties dialog 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.

17-3b Group Policy Objects

Core 2 Objective

- 2.1

Summarize various security measures and their purposes.

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.

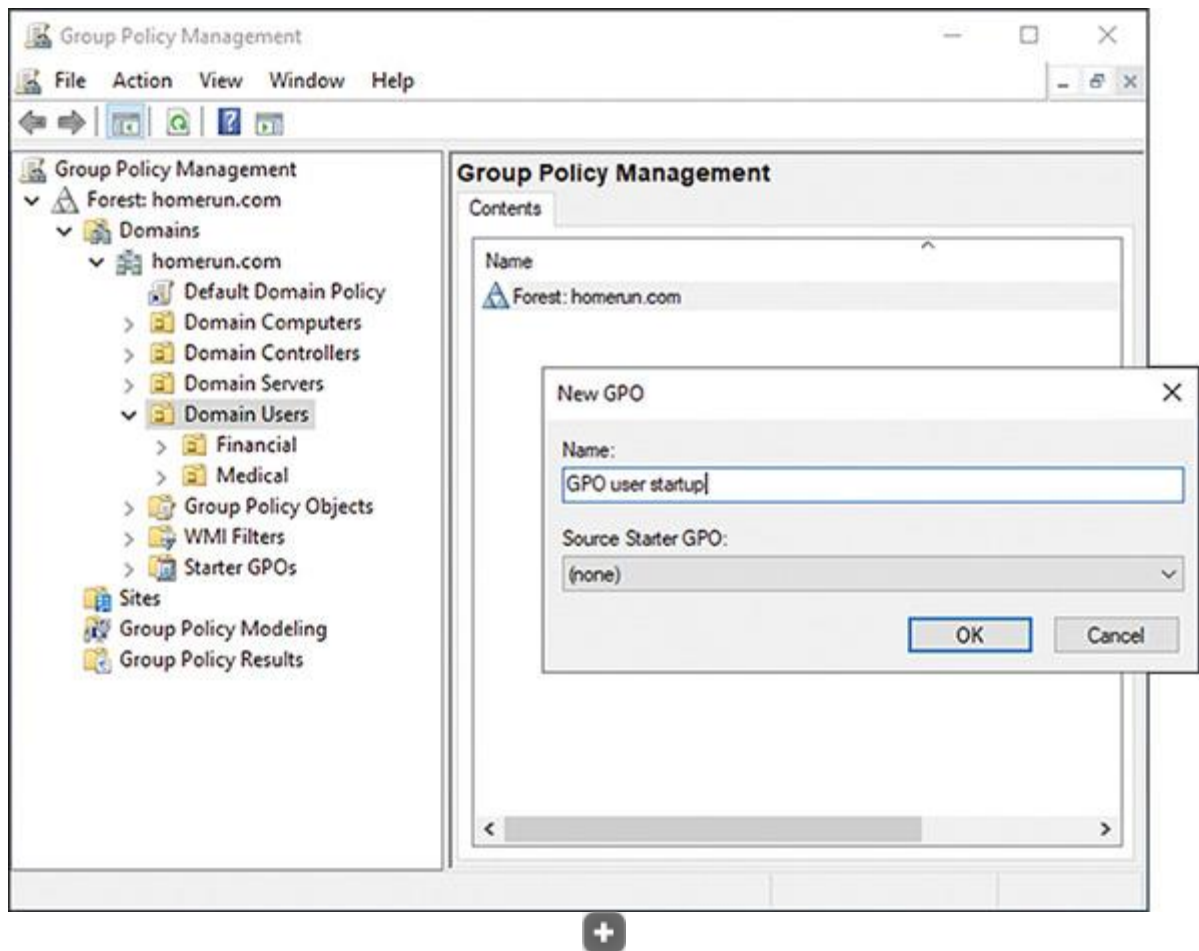
Create and Edit a GPO

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

1. **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. **2**
In the Group Policy Management window (see [Figure 17-53](#)), 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 17-53

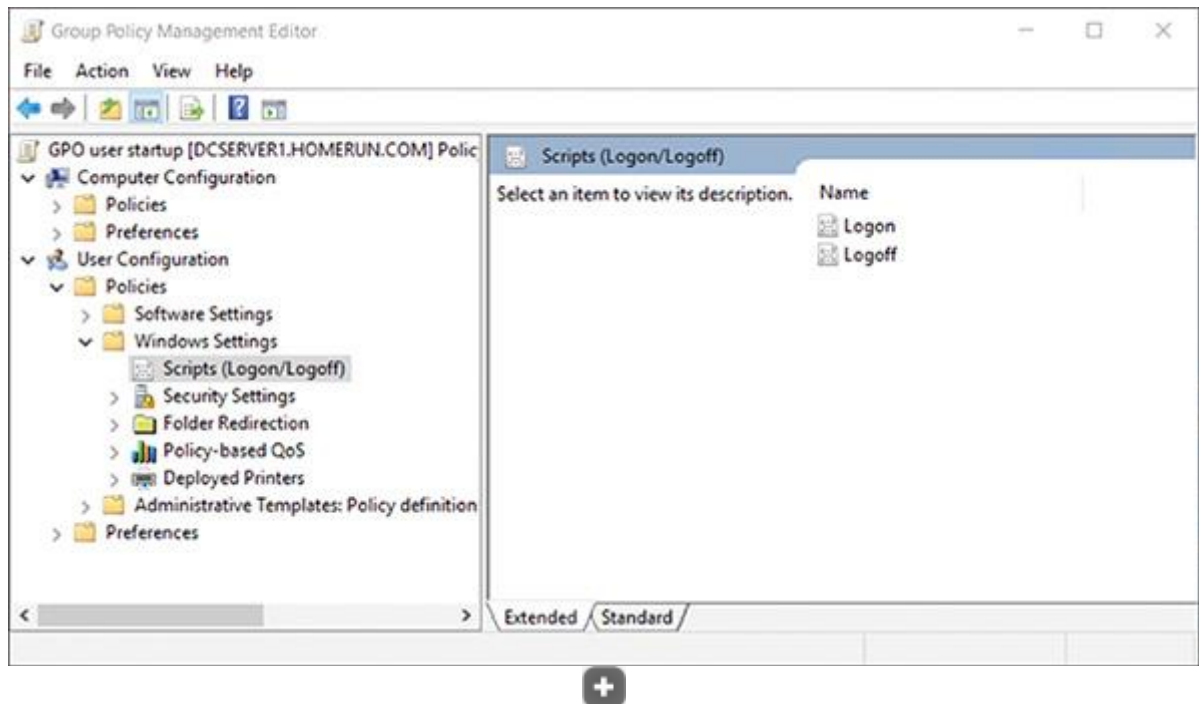
Create a new GPO for the Domain Users OU



3. **3** 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 Scope tab selected.
4. **4** 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 17-54](#)).

Figure 17-54

Drill down into the policies to find the ones you need



5. **5** 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 logon 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 17-54](#).
6. **6** When you're done setting policies, close the GPO editor to return to the Group Policy Management window.
7. **7** 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 run 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, followed by policies for sub-OUs.
5. **Enforced.** Policies that are tagged as Enforced policies are applied last and always win over other policies.

Note 25

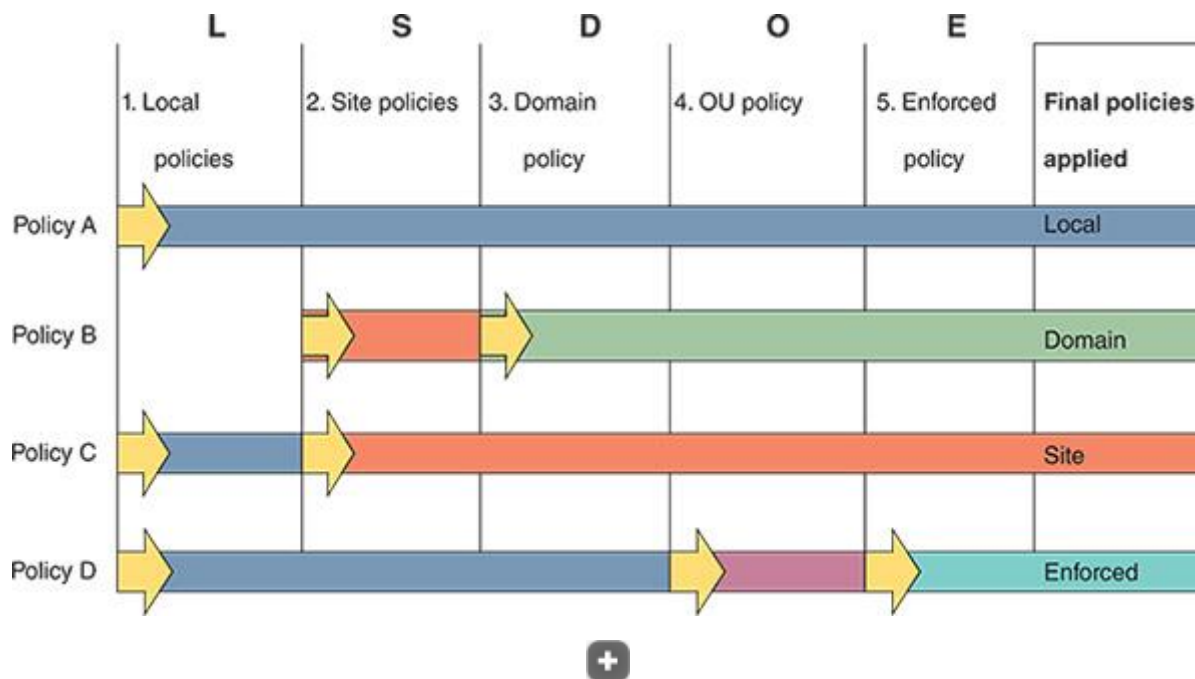
To tag a GPO as Enforced, right-click the GPO in the Group Policy Management window, and click **Enforced**.

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 17-55](#) 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 17-55

Resulting policies applied when conflicting policies exist



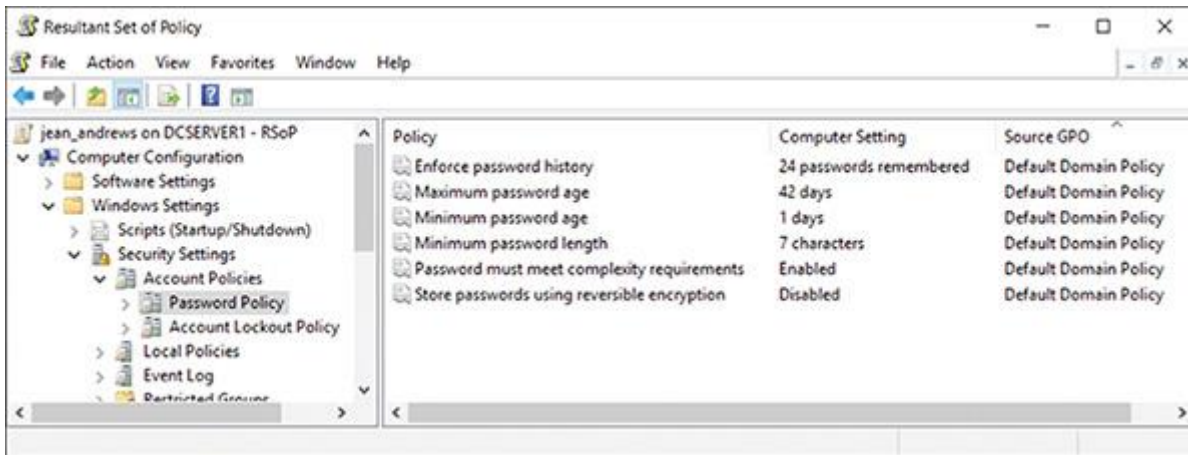
To find out the resulting policies for the computer or user, do one of the following:

- In a command prompt window, enter the `rsop.msc` command. The **Resultant Set of Policy (RSOP)** window opens, where you can

drill down to see the policies set for the computer or user. For example, [Figure 17-56](#) shows the RSoP for the Password Policy.

Figure 17-56

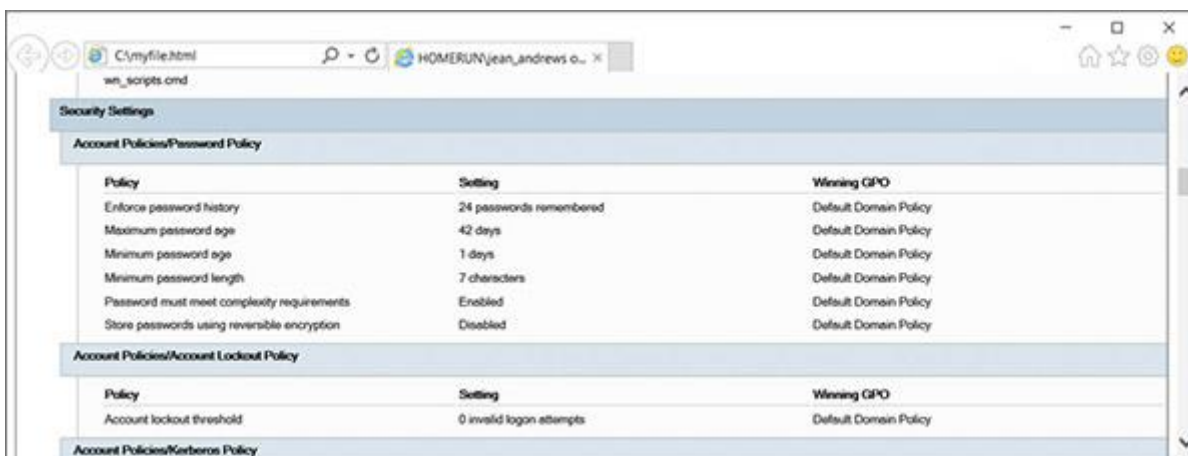
The Resultant Set of Policy for the Password Policy



- 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 Explorer. The HTML file opens in your default browser window. [Figure 17-57](#) shows a snip of the file that includes the Password Policy.

Figure 17-57

The gpresult output displayed as an HTML file in a browser



17-4a **Module Summary**

Securing a Windows Personal Computer

- Power-on passwords are managed by BIOS/UEFI firmware on the motherboard and work before Windows is launched.
- A long password is a strong password.
- Windows allows fingerprints, facial recognition, and PINs to be used to authenticate to Windows. This authentication data is kept on the local machine and applies only to the one device.
- Use Local Group Policies (gpedit.msc) and Local Security Policies (secpol.msc) to control what users and computers can do on the computer or network.
- 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 and make use of a TPM chip on the motherboard.

Controlling Access to Folders, Files, and Printers

- Access to folders and files on a network is controlled by assigning privileges to user accounts and assigning permissions 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 in a peer-to-peer network and Active Directory to control a domain. You can use share permissions and NTFS permissions.
- A mapped network drive makes it easier for users to access drives and folders on the network.
- 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.

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 organized into organizational units (OUs) and suborganizational units.
- Managing resources in AD revolves around the OU, security 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 is as follows: local, site, domain, OU, and enforced. Where there is a conflict in policies, the last policy applied wins.

17-4c **Thinking Critically**

These questions are designed to prepare you for the critical thinking required for the A+ exams and may use information from other modules 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
 - Resumes presented by several people applying for a job with the company
 - Payroll spreadsheets
 - Job openings at the company
2. 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 Explorer to verify that you can connect to the network.
 - Save the workbook file to your hard drive.
 - Using Explorer, remap the network drive.
 - Reboot your PC.
 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 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?
 1. Computer Configuration, Windows Settings, Security Settings, Local Policies, Biometrics
 2. Computer Configuration, Administrative Templates, System, Logon
 3. Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options
 4. User Configuration, Administrative Templates, System, Logon
6. You open a folder Properties dialog box to encrypt the folder, click Advanced, and discover that *Encrypt contents to secure data* is dimmed. What is the most likely problem?
 1. Encryption has not been enabled. Use the Computer Management console to enable it.
 2. You are not using an edition of Windows that supports encryption.
 3. Most likely a virus has attacked the system and is disabling encryption.
 4. 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 manager frequently copies the folder to their 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?
 1. It will be easier to inventory computers in the domain.
 2. It will help organize users into user groups.
 3. An OU must contain either users or computers but not both.
 4. 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?

1. Assign Megan read/write permissions to the Payroll folder, and explain to your manager that it is not a best practice to give only one employee access to an important folder.
2. Assign Megan read/write permissions to the Payroll folder.
3. Create a new user group named Payroll, put Megan in the group, and assign the group read/write permissions to the Payroll folder.
4. Ask your manager 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? (Choose all that apply.)

1. Share permissions do not work on an NTFS volume.
2. NTFS permissions work only on an NTFS volume.
3. If share permissions and NTFS permissions are in conflict, NTFS permissions win.
4. If you set NTFS permissions but do not set share permissions, NTFS permissions apply on the network.

14. Which security features are available on Windows 10 Home? (Choose all that apply.)

1. Local Group Policy
2. NTFS permissions
3. Active Directory
4. Share permissions

15. When NTFS and share permissions are used on the local file server, can a user signed in on a Windows 10 Home computer access these shares? Why or why not?

1. No, because Windows 10 Home does not have the Local Users and Groups console
2. No, because Windows 10 Home does not support NTFS permissions
3. Yes, because Windows 10 Home can join a Windows domain
4. Yes, because the user is authenticated on the file server to access its shares

16. Which Windows tool is used to reset the password for a user's Windows account?

1. Network Places Wizard (netplwiz.exe)
2. Local Group Policy Editor (gpedit.msc)
3. Accounts page in the Settings app
4. Disk Management

17. As the new network administrator managing Active Directory in your organization, you decide to set up a backup system for all folders in the domain authorized for users to store their data. Which tasks should you do first before you configure the backup routine? (Choose all that apply.)

1. Have a company-wide gathering to explain the idea to all users.
2. Evaluate backup software and storage requirements.
3. Apply all available updates to Windows Server.
4. Apply folder redirection to the Home folder for each user.

17-4d Hands-On Projects

Hands-On Project 17-1

Exploring Password Management Software

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 2.5

Password management software, also called password vault software—such as KeePass (keepass.info), LastPass (lastpass.com), and Dashlane (dashlane.com)—can hold your passwords safely so you don't forget them or have to write them down. Choose one of these programs and a second of your own selection that interests you, then answer the following questions about each one:

1. Which platforms are supported?
2. Which web browsers are supported?
3. From how many competitors can the program import passwords?
4. What types of authentication are supported (e.g., master password, fingerprint, etc.)?
5. Where are the passwords stored? Are they synced across devices? How is the information protected?
6. What are some of the differences between the free edition of each program and the paid versions?
7. What happens to the user's account if the user dies or is incapacitated?

Hands-On Project 17-2

Using Group Policy to Secure a Workstation

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 2.5

Using Windows 10/11 Professional or Enterprise, set local security policies to require a password for each account, to audit failed logon events, and to create a logon script that displays the message, "The Golden Pineapple Was Here!" when anyone signs in to the system. Test your policies by verifying that a password is required, your script executes when you sign in, and a failed sign-in event using an invalid password is logged and can be viewed in Event Viewer. Answer the following questions:

1. Which policies did you set, and what setting was applied to each policy?
2. What software did you use to create your script? What is the exact path and file name (including the file extension) to your script?
3. Which log in Event Viewer shows the logon failure event?
4. List three more policies you find in Group Policy that can make a workstation more secure but are not discussed in this module.

Hands-On Project 17-3

Researching a Laptop with a TPM Chip

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 2.5

Many laptops sold today have a TPM chip, and some have encryption-enabled hard drives that don't require encryption software such as BitLocker. Research the web for a laptop that offers a TPM chip and answer these questions:

1. What is the brand and model of laptop that has the TPM chip? Save or print the webpage that lists the laptop specifications for the chip.
2. Is the chip optional? If so, what is the cost of including the chip?
3. Does the laptop have an encryption-enabled hard drive?
4. Does the laptop come bundled with encryption software? If so, what is the name of the software?
5. Does the laptop offer a drive lock password?
6. What is the cost of the laptop, including the TPM chip?

Hands-On Project 17-4

Sharing and Securing a Folder

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 2.5

Using two computers networked together, do the following to practice sharing and securing folders using Windows:

1. **1**
Create a user account named **User1** on Computer 1. In the Documents folder for that account, create a folder named **Folder1**. Create a text file named **File1** in the folder. Edit the file and add the text **Golden Egg**.
2. **2**
On Computer 2, create a user account named **User2**. Try to read the Golden Egg text in File1 on Computer 1. What is the result?
3. **3**
Configure the computers so that User1 signed in to Computer 2 can open File1 and edit the text "Golden Egg," but User2 cannot view or access the contents of Folder1. List the steps you took to share and secure the folder and to test this scenario to make sure it works.
4. **4**
Now make the folder private so that it cannot be seen from Computer 2 in Explorer but can be accessed if User1 knows the folder name. Describe how you did that.

17-4e Real Problems, Real Solutions

Real Problem 17-1

Demonstrating Inherited and Explicit Permissions

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 2.5

In this activity, you set up situations to demonstrate how inherited and explicit permissions work. Do the following:

1. **1**
Sign in to Windows with an administrative account. Create two folders C:\Folder1 and C:\Folder2 on your hard drive.
2. **2**
Create the following text files. Be sure to put some text in each file:
 - C:\Folder1\File1.txt
 - C:\Folder2\File2inherited.txt
 - C:\Folder2\File3explicit.txt
3. **3**
Create a user account named User1.
4. **4**
Set the following permission:
 - User1 has full permission for access to Folder1.
 - User1 cannot access Folder2.
 - Change the permissions for C:\Folder2\File3explicit.txt from inherited permissions to explicit permissions.
5. **5**
Sign in to Windows with the User1 account, and verify that User1 can view and modify File1.txt in Folder1 but cannot access the contents of Folder2.
6. **6**
Sign in to Windows with your own administrative account.
7. **7**
With inherited permissions set, you would expect that File2inherited.txt will inherit the permissions of Folder1 when the file is copied or moved to Folder1. With explicit permissions set for File3explicit.txt, you would expect that File3explicit.txt retains its permissions when it is moved from Folder2 to Folder1. To verify this theory, move (don't copy) both files to Folder1. Open the **Security** tab for each file, and verify one file inherited the permissions of Folder1 and the other file retained its original permissions.
8. **8**
Sign in to Windows with the User1 account.
9. **9**

Verify that User1 can access the contents of C:\Folder1\File2inherited.txt but cannot access the contents of C:\Folder1\File3explicit.txt.

10. **10**
Sign in to Windows with your own administrative account. You have demonstrated that a file with explicit permissions retains its permissions when moved to a new parent folder. What happens when you copy the file? To find out, move File3explicit.txt back to Folder2, and then copy (don't move) it to Folder1. Check the file's Security tab, and note that File3explicit.txt inherited the permissions of Folder1 when copied to the folder. This occurred because, when you copy a file, a new file is actually created in the new location and therefore inherits the permissions of the new parent folder.
11. **11**
It's interesting to note that when you move or copy a file from one NTFS volume to another NTFS volume, the file always inherits the permissions of the parent object. This is because, when a file is moved or copied to a new volume, a new file is always created on the new volume, and, therefore, inherits permissions of its parent object. If you have access to two NTFS volumes on the same computer, you can set up this scenario and verify these actions.

Real Problem 17-2

Setting Up a Windows Domain in Google Cloud

- **Est. Time:** 45 minutes
- **Core 2 Objective:** 2.1

In the Core 1 module "[Network Infrastructure and Cloud Computing](#)" you used Google Cloud Platform to create a VM with Windows Server installed. To use that VM or a new VM to create a Windows domain, do the following:

1. **1**
Go to cloud.google.com. If you have not already set up a free trial, click **Get started for free**. You will need to sign in using a Google account. If you don't have an account, you can create one with any valid email address. When you first set up an account, you must enter payment information, which Google promises not to use during your free trial period. Create an individual account type, enter your information, and click **START MY FREE TRIAL**. Google automatically sets up your first project, aptly named My First Project.
2. **2**
In the left pane of the Google Cloud Platform page, click **Compute Engine**. (If you don't see the left pane, click the three-bar icon in the top-left corner.) If you don't already have a VM created with Windows Server, do the following:
 1. **a**
Click **CREATE INSTANCE** in the VM instances menu to create a VM.
 2. **b**

Use the default settings, except:

- Change the name of the VM to **dcserver**.
- Change the Boot disk to **Windows Server 2019 Datacenter**.

3. **c**

Click **Select**, click **Create**, and then wait for Google to create the instance.

3. **3**

In the VM instances list, click the **dcserver** instance, which takes you to the VM instance details page. Click **Set Windows password** and assign a user name to your VM instance. Note the user name and click **SET**. Google Cloud assigns a password, which displays on the screen. Copy the password, save it somewhere safe, then click **CLOSE**.

4. **4**

A domain controller needs a static IP address on the domain. To set the Primary internal IP address to a static address, follow these steps:

1. **a**

On the VM instance details page, in the *Network interfaces* group under *Network*, click **default**. The VPC network details page appears.

2. **b**

Click **STATIC INTERNAL IP ADDRESSES**. Then click **RESERVE STATIC ADDRESS**.

3. **c**

Under Name, enter **dcserver**. Click **RESERVE**.

5. **5**

To return to the list of VM instances, click the three-bar icon in the top-left corner, and then click **Computer Engine**. Click **VM instances**. Your list of VMs appears.

6. **6**

For the dcserver VM instance, write down the Internal IP and External IP addresses.

Note 26

Remote Desktop is a Windows utility that allows you to remotely control another computer. In this project, you use Remote Desktop from your workstation to remotely control your Windows Server in Google Cloud. You learn more about Remote Desktop in the module "[Network Security and Troubleshooting](#)."

7. **7**

You are now ready to use Remote Desktop with screen and file sharing to access your VM. Follow these steps:

1. **a**

Enter **mstsc** in the Windows 10/11 search box. In the Remote Desktop Connection dialog box, enter the External IP address of your VM, which is its public IP address available on the Internet. Click **Connect**.

2. **b**
In the *Enter your credentials* box, enter your Windows user name and password to dcserver. Click **OK** to connect.

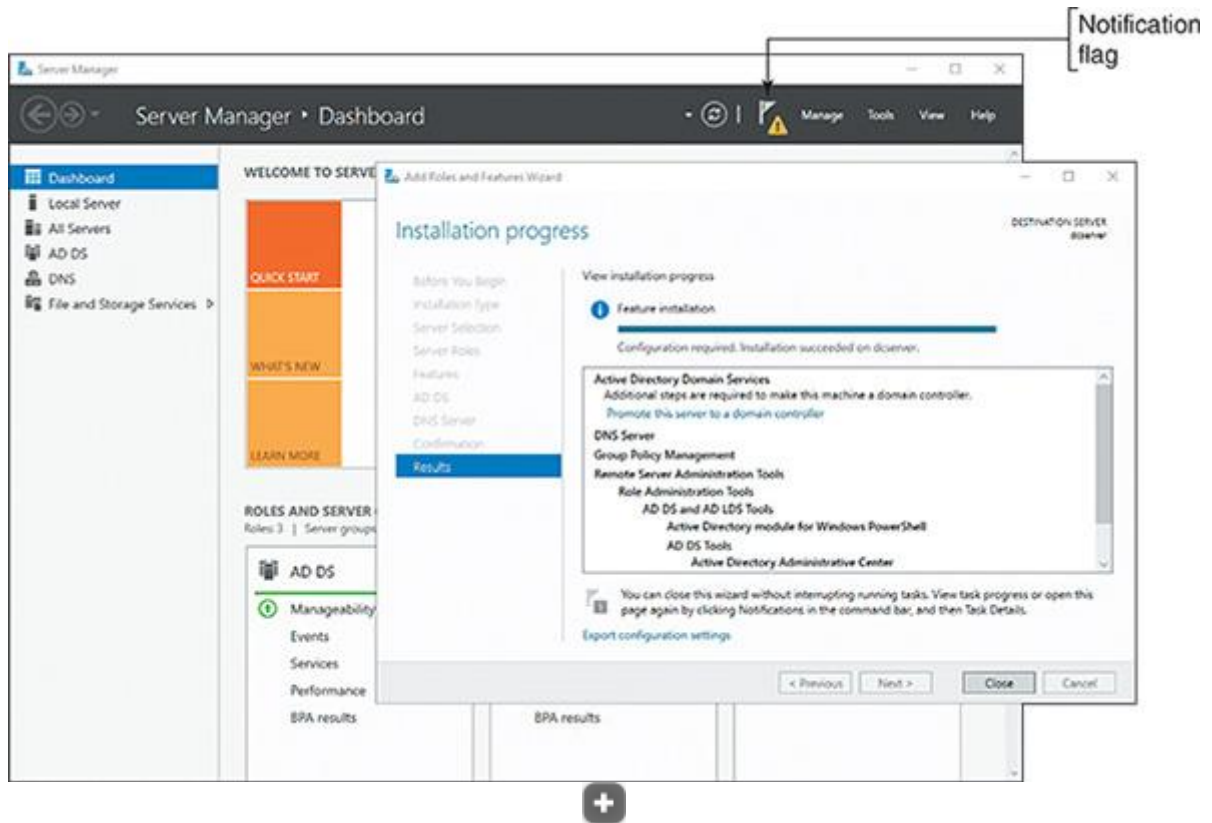
8. **8**
The Windows Server desktop appears in the Remote Desktop window with the Server Manager window open. In the Networks pane on the right, click **Yes** to turn on network discovery.

9. **9**
You are now ready to set up your Windows domain. Follow these steps:

1. **a**
In the Server Manager window, under *Configure this local server*, click **Add roles and features**. The Add Roles and Features Wizard opens. Click **Next**.
2. **b**
On the *Select installation type* page, accept the default values, and click **Next**.
3. **c**
On the *Select destination server* page, accept the default values, and click **Next**.
4. **d**
Under *Select server roles*, check **Active Directory Domain Services**, and click **Add Features**.
5. **e**
Under *Select server roles*, check **DNS Server** and click **Add Features**. A warning message appears. Click **Continue**. (The message was caused by Google Cloud handling tasks that the domain controller would normally handle.)
6. **f**
Click **Next** four times to step through pages in the wizard, accepting default values. When the *Confirm installation selections* page appears, check **Restart the destination server automatically if required**, and click **Yes** to confirm. Then click **Install**. Wait while the installation happens. You can click the flag in the upper-right corner of the Server Manager window to view the progress. See [Figure 17-58](#). When the process finishes, click **Close** to close the Add Roles and Features Wizard.

Figure 17-58

The notification flag reports installation progress



10. **10** Although AD Domain Services is now installed, you cannot promote the server to a domain controller until you first set a password for the all-powerful Administrator account. (Recall that this account is different from your user name account, which has Administrative privileges.) To set the password, do the following:

1. **a** To open an elevated command prompt window, enter **cmd** in the Windows search box, right-click **Command Prompt**, and click **Run as administrator**. Respond to the UAC dialog box.
2. **b** Use a password that satisfies AD complexity requirements. For example, in the command prompt window, enter this command:

`net user Administrator Passw0rd /passwordreq:yes`
3. **c** Close the command prompt window.

11. **11** Click the notification flag in the Server Manager window, and then click **Promote this server to a domain controller**. The *Deployment Configuration* window appears. Select **Add a new forest**. Enter your root domain name. You can use homerun.com or another domain name. Click **Next**.

12. **12**

In the Domain Controller Options window, enter the DSRM password twice, and click **Next**. Ignore any warning messages and click **Next** several times to step through the wizard. Finally, click **Install**.

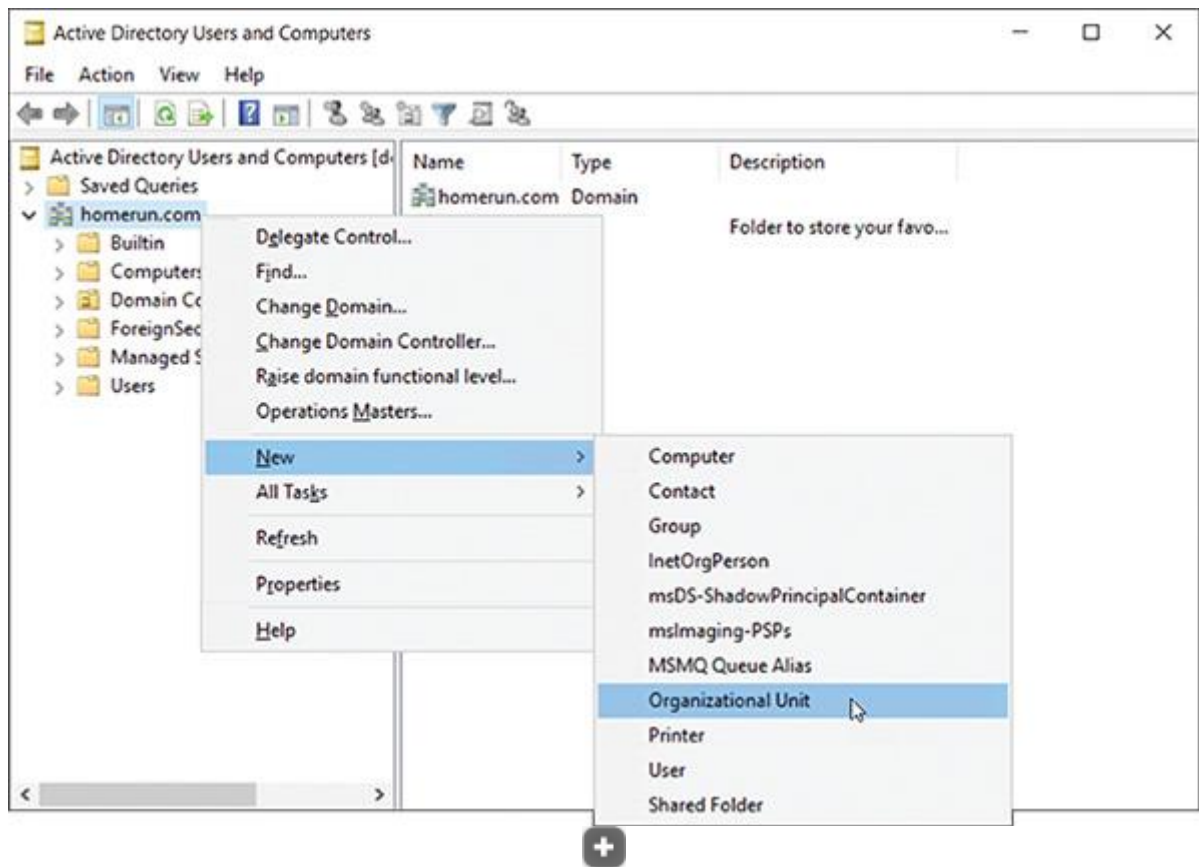
13. **13**

After the system reboots, you will need to connect again through Remote Desktop. At this point, you have a working domain controller and can practice the skills you learned in this module to manage Active Directory. Here is how to get started:

1. **a**
Each time you use Remote Desktop to connect to the server, check the VM instances page to verify the external IP address that you use with Remote Desktop has not changed. Use the current external IP address.
2. **b**
On the Windows Server desktop, if Server Manager is not already open, click **Start** and click **Server Manager**.
3. **c**
In the Server Manager window, to manage OUs, user groups, and users, click **Tools** and then click **Active Directory Users and Computers**. (Refer back to [Figure 17-42](#).)
4. **d**
By default, your domain has one OU: Domain Controllers. To create another OU directly under the domain, right-click the domain name, point to **New**, and click **Organizational Unit** (see [Figure 17-59](#)). You can then name the OU.

Figure 17-59

Create an OU directly under the domain



14. **14** Have fun poking around and learning to use Active Directory! Every great IT technician needs to have a working knowledge of AD, and you have started to develop that in this module. When you're finished working with AD, avoid accumulating any charges against your free quota by shutting down the server VM in the Remote Desktop Connection dialog box.

Note 27

You will use the Google Cloud Platform service for another project in the module "[Linux and Scripting](#)." Do not disable your Google Cloud Platform account until after you have completed that project.