Application Opened

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

**Module**

**3**

**User Management**

* [Chapter Introduction](javascript://)
* **3-1**[User Accounts](javascript://)
  + **3-1a**[Sign-In Methods](javascript://)
  + **3-1b**[Naming Conventions](javascript://)
  + **3-1c**[Default User Accounts](javascript://)
  + **3-1d**[Default Groups](javascript://)
* **3-2**[Creating and Managing User Accounts](javascript://)
  + **3-2a**[Accounts](javascript://)
  + **3-2b**[User Accounts Applet](javascript://)
  + **3-2c**[Local Users and Groups MMC Snap-In](javascript://)
  + **3-2d**[Command-Line User Management](javascript://)
* **3-3**[Managing User Profiles](javascript://)
  + **3-3a**[The Default Profile](javascript://)
  + **3-3b**[Mandatory Profiles](javascript://)
  + **3-3c**[Roaming Profiles](javascript://)
  + **3-3d**[Folder Redirection](javascript://)
  + **3-3e**[The Public Profile](javascript://)
* **3-4**[Start Menu and Taskbar Customization](javascript://)
* **3-5**[Advanced Authentication Methods](javascript://)
  + **3-5a**[Picture Password](javascript://)
  + **3-5b**[Windows Hello PIN](javascript://)
  + **3-5c**[Windows Hello Biometric Authentication](javascript://)
  + **3-5d**[Windows Hello for Business](javascript://)
  + **3-5e**[Security Key](javascript://)
  + **3-5f**[Dynamic Lock](javascript://)
  + **3-5g**[Smart Cards](javascript://)
* **3-6**[Network Integration](javascript://)
  + **3-6a**[Peer-to-Peer Networks](javascript://)
  + **3-6b**[Domain-Based Networks](javascript://)
  + **3-6c**[Cached Credentials](javascript://)
  + **3-6d**[Azure AD Join](javascript://)
* **3-7**[Chapter Review](javascript://)
  + **3-7a**[Summary](javascript://)
  + **3-7b**[Key Terms](javascript://)
  + **3-7c**[Review Questions](javascript://)
  + **3-7d**[Case Projects](javascript://)

Go to pg.

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

Application Opened

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

Chapter Introduction

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

* **1**Describe local user accounts and groups
* **2**Create and manage user accounts
* **3**Manage user profiles
* **4**Configure advanced authentication methods
* **5**Describe Windows 10 integration with networks

User accounts are the most basic level of Windows 10 security. Authenticating to Windows 10 as an individual user account is the basis for all other Windows 10 security mechanisms. In this module, you learn about local user accounts and groups, including how to create and manage user accounts. Each user has customized settings, such as desktop and program configuration data, stored in a user profile.

Windows 10 includes advanced authentication methods, such as picture password, PIN, and biometrics. It is important to understand how these newer authentication methods can be used to increase security. In addition, the creation of user accounts for different network environments is important for efficiently controlling security.

Go to pg.

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

Application Opened

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

**3-1**User Accounts

User accounts are required for individuals to sign in to Windows 10 and use resources on the computer. Each [**user account**](javascript://) has attributes that describe the user and control access. Some user account attributes are:

* Name
* Password
* Group membership
* Profile location

When a Windows 10 computer is not part of an Active Directory domain, you can sign in by using a [**local user account**](javascript://) or a [**Microsoft account**](javascript://). Both types of accounts function similarly on a Windows 10 computer. The main difference between them is where the account credentials (user name and password) are stored. A local user account exists only on the one local Windows 10 computer and cannot be used to sign in to other computers. A Microsoft account is stored online by Microsoft and can be added to multiple Windows 10 computers and mobile devices.

Using a Microsoft account to sign in has several advantages:

* *Single set of credentials across devices*—If you configure multiple computers and mobile devices to use the same Microsoft account for authentication, you need to remember only one account name and one password for authentication. When you change the password for the Microsoft account, it automatically takes effect for all devices.
* *Password reset capability*—If you are authenticating with a Microsoft account, you can reset the password on the Microsoft account by using an alternate email account you’ve provided, a mobile phone number, or by answering security questions. A local user account has fewer options for password reset.
* *Synchronization of some profile information*—A Microsoft account includes cloud storage that can be used to synchronize some settings among devices running Windows 10. You can synchronize settings such as the theme, stored passwords, language preferences, and ease of access settings.
* *Integration with family settings*—For home computers, Microsoft accounts integrate with family settings to control web browsing and track computer usage.
* *Integration with other Microsoft apps*—A Microsoft account can be used for multiple Microsoft apps, such as OneDrive, Skype, or Xbox Live. When you use your Microsoft account to authenticate on Windows 10, those same credentials can automatically be used to access the Microsoft apps that use a Microsoft account. For example, when you authenticate using a Microsoft account in Windows 10, you automatically are authenticated to the OneDrive storage for that account.

Local user accounts are stored in the [**Security Accounts Manager (SAM) database**](javascript://) of Windows 10. When you sign in as a local user, the user name and password in the SAM database are used to verify your credentials.

If you use a Microsoft account to sign in to Windows 10, a local user account is created in the SAM database that is linked to the Microsoft account. Your credentials, however, are verified with Microsoft over the Internet. If your computer is disconnected from the Internet, you can still sign in by using a Microsoft account because the credentials are cached locally in Windows 10 when you authenticate. Changing the password for the Microsoft account does not affect the cached credentials. The new password is used only when the computer running Windows 10 is reconnected to the Internet.

If the computer is part of an Active Directory domain, and the user signs in using a domain user account, the SAM database is not used. Windows 10 sends domain user credentials to a server configured as a domain controller for verification.

To facilitate assigning permissions to resources, all user accounts have a [**security identifier (SID)**](javascript://). For example, when a user is assigned permissions to access a folder, the SID is written to the folder access control list, not the user account name. Using a SID for security ensures that accounts can be renamed without losing security information. The SID for each user account is a guaranteed unique identifier (GUID), such as S-1-5-21-1561371318-2357482352-4200497431-1002. When you work with user accounts and assigning permissions to resources, Windows 10 automatically translates the user name to a SID for you.

To fully comprehend user accounts, you should understand the following:

* Sign-in methods
* Naming conventions
* Default user accounts
* Default groups

Go to pg.

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

Application Opened

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

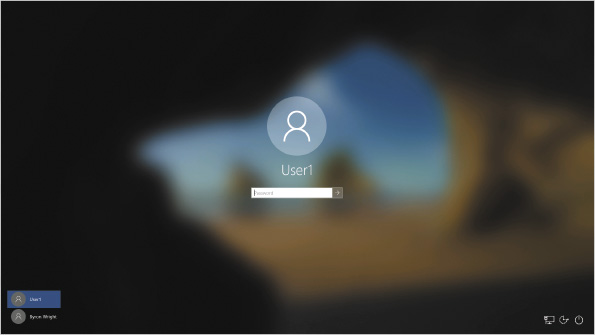
## 3-1aSign-In Methods

Users must sign in to Windows 10 before they can access resources and interact with the system. Windows 10 supports several sign-in methods; which method you choose depends on your requirements as network administrator, user needs, and whether the computer is a member of a domain.

### Windows Sign-In Screen

For computers that are not joined to a domain, the Windows sign-in screen shown in [Figure 3-1](javascript://) displays a list of local user accounts that you can select from for authentication. For domain-joined computers, only the most recently used account is listed. The SAM database typically has only a few user accounts, so a graphical sign-in screen that displays each local user account is reasonable. In a domain-based environment with hundreds or thousands of accounts, it would not be possible to display an icon for each user account.

**Figure 3-1Windows 10 Sign-In Screen**



Enlarge Image

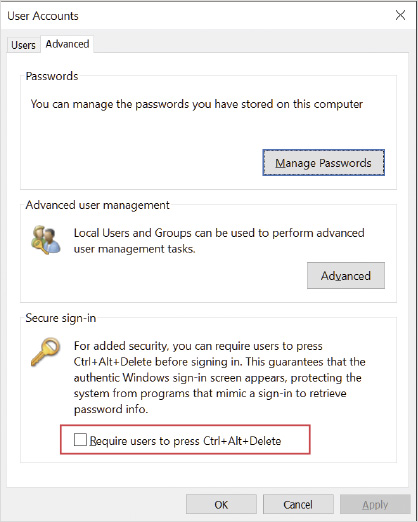
On the Windows sign-in screen, each user is represented by an icon and name. The name is the name of the user account. The icon is selected when the user account is created, but it can be changed at any time.

### Secure Sign-In

[**Secure sign-in**](javascript://) increases security on your computer by forcing you to press Ctrl+Alt+Delete before signing in. This protects your computer from malware that might attempt to steal your password by imitating the Windows sign-in screen.

The key sequence Ctrl+Alt+Delete is filtered by Windows operating systems, including Windows 10. The key sequence is captured by the operating system and not passed to applications. A virus or spyware never sees that you pressed Ctrl+Alt+Delete; therefore, if you press this key combination and a sign-in window appears, it is the legitimate Windows sign-in screen. Secure sign-in can be enabled on the Advanced tab of the advanced User Accounts applet, shown in [Figure 3-2](javascript://).

**Figure 3-2Enable Secure Sign-In**



**Activity 3-1**

### Implementing Secure Sign-In

**Time Required:**5 minutes

**Objective:**Implement secure sign-in for all users

**Description:**Secure sign-in makes Windows 10 more secure by ensuring that no malicious software running in Windows 10 is creating a false sign-in screen and capturing user names and passwords. In this activity, you implement secure sign-in, which forces users to press Ctrl+Alt+Delete before signing in.

1. 1

If necessary, start your computer and sign in.

1. 2

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

1. 3

Click the **Advanced** tab.

1. 4

Select the **Require users to press Ctrl+Alt+Delete** check box and then click **OK**.

1. 5

Sign out. Notice that the screen indicates that you must press Ctrl+Alt+Delete to sign in.

**Note 1**

Some virtualization software used remote desktop to connect to remote systems and won’t enforce using Ctrl+Alt+Del. For Hyper-V, ensure that you disable Enhanced Session on the View menu to experience the standard desktop sign-in.

### Fast User Switching

[**Fast user switching**](javascript://) allows multiple users to have applications running in the background on a Windows 10 computer at the same time; however, only one user can be actively using the computer at a time. For example, User1 signs in to Windows 10 and starts creating a document in Word. User1 then locks the computer before leaving for lunch with the Word document still open. User2 comes to the computer during lunch, signs in to check email, and then signs out. After lunch, User1 returns, signs in, and continues to compose the Word document. Fast user switching allows this to happen. Without fast user switching, User1 would have been signed out automatically when User2 signed in and any unsaved work in the Word document would have been lost.

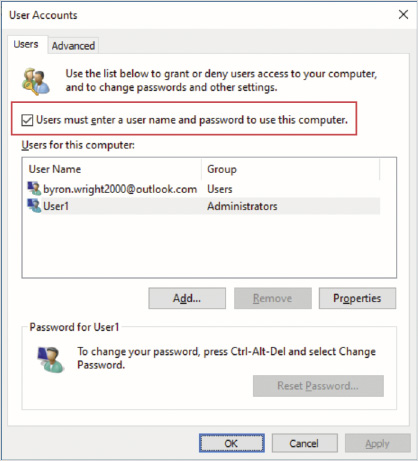
In environments where multiple users share the same computer, fast user switching is a very important feature. This is extremely useful in lab environments and for computers at a front reception desk in an office environment.

### Automatic Sign-In

In some environments, it is desirable for the computer to automatically sign in as a specific user each time it is started. This is appropriate for libraries and other public locations where users are not assigned their own sign-in credentials. The term kiosk is sometimes used to refer to an environment where automatic sign-in is desired. A [**kiosk**](javascript://) is a computer in a public space that is dedicated for a single purpose.

Automatic sign-in is configured on the Users tab of the User Accounts applet, shown in [Figure 3-3](javascript://). When you deselect the Users must enter a user name and password to use this computer check box and then click OK, you are prompted for the credentials to be used for the automatic sign-in. From this point forward, Windows 10 automatically signs in using the credentials you specified.

**Figure 3-3Enable Automatic Sign-In**



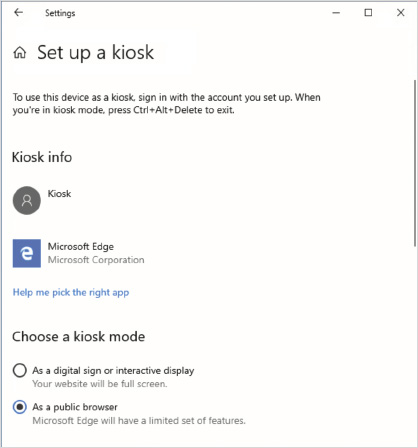
When you need to do system maintenance on a computer with automatic sign-in enabled, you must stop the automatic sign-in from occurring. Holding down the Shift key during the boot process stops the automatic sign-in from occurring. Then you can sign in with your own credentials to perform the maintenance tasks. Alternatively, you can sign out after the user is automatically signed in to access the Windows sign-in screen.

### Assigned Access

[**Assigned access**](javascript://) is an advanced sign-in option for configuring Windows 10 as a kiosk. This option can be used when a company has Windows 10 tablets being used for filling in surveys or when a public access computer is being used to search a catalog.

When you enable assigned access, you select (or create) a local user account and a Windows Store app, as shown in [Figure 3-4](javascript://). At that point, the selected user account is limited to using that one app when signed in. Many normal functions, such as exiting the application, are not possible.

**Figure 3-4Assigned Access**



If you select Microsoft Edge as the application, you are given specific configuration options for the kiosk. If you choose the As a digital sign or interactive display option, then Edge is forced to full screen and displays a URL that you specify. If you choose the As a public browser option, you can specify a home page and an idle timeout to restart the browser to clear private data.

**Note 2**

For more kiosk configuration options, see Configure kiosks and digital signs on Windows desktop editions at [https://docs.microsoft.com/en-us/windows/configuration/kiosk-methods](https://docs.microsoft.com/en-us/windows/configuration/kiosk-methods" \t "_blank).

Go to pg.

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

Application Opened

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

## 3-1bNaming Conventions

A naming convention is a standardized process for creating names on a network or stand-alone computer. Corporate environments establish naming conventions for user accounts, computers, folders, shared folders, printers, and servers. Names should be descriptive enough that anyone can figure out what the resource is. For example, computer names are often the same as their asset tracking number (inventory tracking number) or include the name of the person who uses the computer most often.

Using a naming convention for small networks might seem unnecessary, but even small networks benefit from resources with meaningful names. For example, in a small network with two servers named “Files” and “Email,” it is easy to guess what resources are on each server. In another network where the two servers are named “Sleepy” and “Dopey,” users have no logical way to know what resources are on each server. If your network grows, you will be happy you implemented a naming convention early in the process.

Some common naming conventions for user names are:

* First name—In small environments, there is little risk that two users will have the same first name. This approach is easy for users to remember.
* First name and last initial—This naming convention helps ensure that user sign-in names are not duplicated. In small and mid-sized environments, if two users have the same first name, they are unlikely to have the same last initial.
* First initial and last name—Many large environments use this naming convention or a variation of it. Last names are more likely to be unique than first names, so this convention reduces the risk of duplicate user sign-in names.
* First name.last name—This naming convention is becoming more popular because many organizations like to also use it for email addresses. This has an even lower chance of duplicates than other conventions.

No matter which naming convention you select, you must have a plan to address duplicate user sign-in names. For example, Byron Wright and Blair Wright might be in the same organization. If your naming convention is first initial and last name, both users will have the same user sign-in name of “bwright.” To fix this, you could add a numeral to the end of the second user account created, to make the user sign-in name “bwright2.” You could also use two letters of the first name, in which case the user sign-in names would be “bywright” and “blwright.”

When creating new local users, you must be aware of the restrictions imposed by Windows 10 on the user name, such as the following:

* User names must be unique—No two users can have the same sign-in name because the sign-in name is used by the computer to identify the user and verify the password associated with it during sign-in.
* User names must be 20 characters or fewer—This restriction is typically not a problem because no users want to type a sign-in name of more than 20 characters.
* User names are not case sensitive—You cannot change the case of letters to create unique user sign-in names; Windows 10 reads BWright and bwright as the same name. Helpfully, this means that users do not need to be concerned about case when they type in their user name. Passwords, however, are case sensitive.
* User names cannot contain invalid characters—Windows 10 uses some characters for special functions, so they cannot be used in user sign-in names. The following characters are invalid:

⁄ \ { } : ; | = , + \* ? < >

Go to pg.

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

Application Opened

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

## 3-1cDefault User Accounts

Each Windows 10 computer has an [**Administrator**](javascript://) account and a [**Guest**](javascript://) account that are created during installation. The Administrator and Guest accounts are called built-in accounts because they are created on every Windows 10 computer. They also have unique characteristics. In addition, a user-specified [**initial account**](javascript://) is created during installation. The initial account is not a built-in account.

### Administrator

The Administrator account is the most powerful local user account possible. This account has unlimited access and unrestricted privileges to every aspect of Windows. The Administrator account can manage all security settings, other users, groups, the operating system, printers, shares, and storage devices. Because of these far-reaching privileges, the Administrator account must be protected from misuse.

The Administrator account has the following characteristics:

* It is not visible on the sign-in screen.
* It has a blank password by default.
* It cannot be deleted.
* It cannot be locked out due to incorrect sign-in attempts.
* It cannot be removed from the local Administrators group.
* It can be disabled.
* It can be renamed.

To protect the Administrator account from misuse, it is disabled by default in Windows 10; however, the Administrator account is automatically enabled when you enter Safe Mode so that you can use it for troubleshooting. Safe Mode is a boot option you can use when troubleshooting Windows 10.

**Tip**

Because the Administrator account is available only in Safe Mode, it is typically used only for troubleshooting or as an account of last resort when signing in.

Because the password for the Administrator account is blank by default, this password should be changed immediately after installation. This prevents users from starting in Safe Mode and signing in as Administrator. If users sign in as Administrator, they can perform any system action, such as adding software, deleting files, creating a new account with administrative privileges, or increasing the privileges of an existing account.

**Tip**

Windows 10 restricts accounts with blank passwords to console access only. This means that no one can sign in over the network using an account with a blank password, including the Administrator account.

The Administrator account is unique because it is considered an account of last resort for signing in and troubleshooting; therefore, the Administrator account cannot be deleted or locked out after too many incorrect sign-in attempts. The Administrator account also cannot be removed from the local Administrators group because the local Administrators group is where the Administrator account derives most of its privileges.

### Guest

The Guest account is one of the least privileged user accounts in Windows. This account has extremely limited access to resources and computer activities and is intended for occasional use by low-security users. For example, a company might have a computer in the lobby with Internet access for customers. The customers would sign in as a guest. The Guest account has no capability to change the computer settings.

The Guest account has the following characteristics:

* It cannot be deleted.
* It can be locked out.
* It is disabled by default.
* It has a blank password by default.
* It can be renamed.
* It is a member of the Guests group by default.
* It is a member of the Everyone group.

Most organizations have no need for a Guest account. To ensure that the Guest account is not accidentally assigned privileges that are used by anonymous users, the Guest account is disabled by default. This way, even if privileges are assigned to the Guest account by accident, no one can sign in as the Guest account and use those privileges.

The Guest account derives all its privileges from being a member of the Guests group and the Everyone group. Both these groups have very limited privileges. The Guests group is explicitly created for assigning permissions to Guest users. The Everyone group encompasses all users who have signed in, including the Guest account. Windows security has evolved so that the Everyone group has very limited privileges. Most privileges formerly assigned to the Everyone group are now assigned to the Authenticated Users group. Authenticated Users includes all users who have signed in except for the Guest account.

**Caution**

If you enable the Guest account, the Everyone group includes anonymous users. This allows you to give users access to resources on a computer over the network without requiring a valid user name or password.

### Initial Account

During installation, you are prompted for the information required to create a user. The user created from that information is given administrative privileges. Having administrative privileges means that the initial account created during installation is capable of performing all the same tasks as the Administrator account. The initial account can be used to configure Windows 10, including creating other user accounts.

Differences between the Administrator account and the initial account include the following:

* The initial account is visible on the sign-in screen.
* The initial account does not have a blank password by default.
* The initial account can be deleted.
* The initial account can be locked out due to incorrect sign-in attempts.
* The initial account can be removed from the Administrators group.

### Other Accounts

Windows 10 creates multiple local accounts that it uses for background processes, such as Windows Defender Application Guard. These accounts are disabled by default to ensure that they don’t create a security risk. Little or no documentation about these accounts exist, and you should not modify them. These accounts are:

* DefaultAccount
* WDAGUtilityAccount

Go to pg.

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

Application Opened

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

## 3-1dDefault Groups

Groups are used to simplify the process of assigning security rights and permissions. When users are members of a group, they have access to all the resources that the group has been given permissions to access. It is easier to assign permissions to a group and make five users a member of that group than to assign permissions directly to five users, particularly if the permissions change.

Windows has a number of [**built-in local groups**](javascript://) that exist by default and cannot be deleted. These groups are assigned rights and permissions to Windows 10. Like local user accounts, local groups are stored in the SAM database and can be assigned permissions only to resources on the local computer.

The Windows 10 built-in groups are:

* Access Control Assistance Operators—Members of this group can access authorization attributes and permissions for resources on this computer remotely. This group contains no default members.
* Administrators—Members of this group have full access to the computer. The local Administrator account is always a member of this group. The initial account created during installation is also a member of this group by default. If the computer has joined a domain, the Domain Admins group is a member of this group. Making Domain Admins a member of the local Administrators group provides centralized control of domain computers through a single sign in.
* Backup Operators—Members of this group can back up and restore all files and folders on the computer; however, the ability to read and modify files is still controlled by file system security. Backup operators cannot automatically read and modify files; they must be assigned the necessary file permissions. By default, this group has no members.
* Cryptographic Operators—Members of this group are able to perform cryptographic operations. Only members of this group are able to modify encryption settings for IPSec in Windows Firewall when configured in Common Criteria mode. Common Criteria is a standard for security.
* Device Owners—Members of this group can change system-wide settings.
* Distributed COM Users—Members of this group are able to run and activate Distributed COM objects on the computer. This group is relevant only when using DCOM applications, which is relatively rare.
* Event Log Readers—Members of this group have the ability to read event logs on the local computer. You can add members to this group if you want them to be able to review the event logs for errors but not have the ability to erase the logs.
* Guests—Members of this group have the same access to the system as members of the Users group. Members are able to sign in and save files but are not able to change system settings or install programs. The exception to this is the Guest account, which has additional restrictions.
* Hyper-V Administrators—Members of this group can manage all aspects of Hyper-V on this computer.
* IIS\_IUSRS—This group is used to configure security for Internet Information Services (IIS). Only the system account NT AUTHORITY\IUSR is a member by default. The rights and permissions assigned to this group are applied to all IIS users who are not authenticated.
* Network Configuration Operators—Members can configure network components and change IP address information. This group is useful if you need to delegate the ability to change IP address configuration to other users, but do not want to give those users full administrative rights. By default, this group has no members.
* Performance Log Users—Members of this group are able to monitor performance counters and access performance logs on the computer. This group has no members by default. In a domain environment, domain users and groups can be added to this group to perform remote monitoring.
* Performance Monitor Users—Members of this group are able to monitor performance counters on the computer but cannot access performance logs. This group has no members by default. In a domain environment, domain users and groups can be added to this group to perform remote monitoring.
* Power Users—Members of this group have almost all administrative permissions. It was common in previous versions of Windows to use this group for all users to ensure that they could make changes to their systems. In Windows 10, this group has been deprecated, and Microsoft recommends using it only when necessary to support legacy applications that do not run when a user has lower privileges.
* Remote Desktop Users—Members of this group can sign in remotely by using Remote Desktop. This group has no members by default.
* Remote Management Users—Members of this group can query and configure Windows Management Instrumentation (WMI) objects over the network.
* Replicator—This group is used by special user accounts to perform file replication between computers. This group has no members by default.
* System Managed Accounts Group—Members of this group are managed by Windows 10 and should not be manually modified.
* Users—Members can operate the computer and save files but cannot install programs, modify user accounts, share resources, or alter system settings. All user accounts created on the system are a member of this group by default. In addition, the system accounts NT AUTHORITY\Authenticated Users and NT AUTHORITY\INTERACTIVE are members of the group. In a domain environment, the Domain Users group is also a member.

Go to pg.

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

Application Opened

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

**3-2**Creating and Managing User Accounts

Creating a user account can be done from Settings, Control Panel, or the [**Local Users and Groups MMC snap-in**](javascript://). You also can create and manage users with command-line tools and Windows PowerShell cmdlets. The process varies depending on which tool is used, but the options are similar in each tool.

A [**standard user account**](javascript://) derives its privileges from being a member of the local Users group. As a member of the local Users group, a user account can use software but not install or remove software. A standard user also is not able to change computer settings that affect other users or delete operating system files. Effectively, a standard user cannot compromise the security or stability of Windows 10.

Some older software requires administrative rights to run properly. In this case, User Account Control prompts the user for the password of a user with administrative rights. To avoid being prompted for a password, you might want to make the user an administrative user.

An [**administrator account**](javascript://) derives its privileges from being a member of the local Administrators group. Administrator accounts have complete access to the system. An administrator can make changes that compromise the stability and security of Windows 10, such as installing software, changing file system security, and updating device drivers.

In Windows 10, most actions that are triggered by an administrator do not result in a prompt from User Account Control; however, changes triggered by software do result in a prompt from User Account Control. This ensures that changes are not made by malicious software.

Go to pg.

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

Application Opened

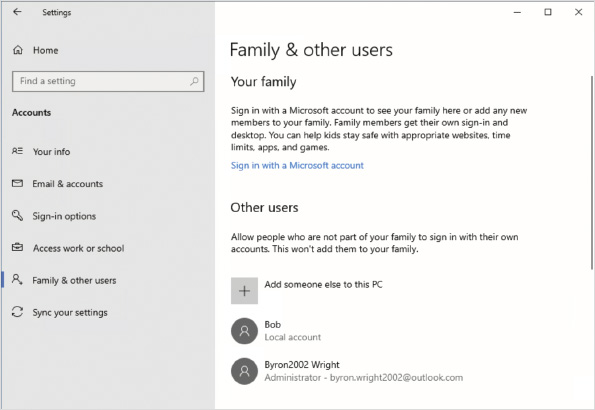
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 3-2aAccounts

From the Accounts settings, you manage your own user account and create additional user accounts. For your own account, you can switch authentication between a local account and a Microsoft account. When you switch between these options, your account settings remain the same and no data is lost. You merely are changing the process used to sign in.

You add other users from the Family & other users screen, shown in [Figure 3-5](javascript://). The wizard for adding new accounts starts by asking how the user will sign in. If you indicate that you don’t have sign-in information for the user (the user’s Microsoft account), you are prompted to create a Microsoft account for the user. If you don’t want to use a Microsoft account for authentication, you can choose the Add a user without a Microsoft account option to create a local user account instead.

**Figure 3-5Family & Other Users Screen**



Enlarge Image

**Tip**

Users should not create a new Microsoft account for authenticating to Windows 10 if they already have one. Using the same Microsoft account for multiple services makes authentication simpler for users.

**Activity 3-2**

### Creating a Local User Account in Settings

**Time Required:**10 minutes

**Objective:**Create a local user account

**Description:**Local user accounts are required to sign in to Windows 10. The Accounts window in Settings provides a simplified way to create accounts. In this activity, you create one user account that authenticates locally.

1. 1

If necessary, start your computer and sign in.

1. 2

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

1. 3

In the Settings window, click **Accounts** and then click **Family & other users**.

1. 4

In the Other users area, click **Add someone else to this PC**.

1. 5

On the How will this person sign in screen, click **I don’t have this person’s sign-in information**.

1. 6

On the Create account screen, click **Add a user without a Microsoft account**.

1. 7

On the Create an account for this PC screen, enter the following information and then click **Next**:

* + User name: **Bob**
  + Password: **password**
  + Security question 1: **What was your first pet’s name?**
  + Your answer: **Fido**
  + Security question 2: **What was your childhood nickname?**
  + Your answer: **Fido**
  + Security question 3: **What’s the first name of your oldest cousin?**
  + Your answer: **Fido**

1. 8

Sign out as Userx and sign in again as Bob. Notice that it takes a few minutes to build Bob’s profile during the first sign-in.

1. 9

On the Choose privacy settings for your device screen, click **Accept**.

1. 10

Click the **Start** button, click **Settings**, and then click **Accounts**. Notice that the Family & other users option is not available because Bob is a standard user instead of an administrator.

1. 11

Sign out as Bob.

**Activity 3-3**

### Creating a Microsoft Account in Settings

**Time Required:**10 minutes

**Objective:**Create a Microsoft account for signing in

**Description:**Microsoft accounts are an optional method for signing in to Windows 10. The Accounts window in Settings provides the option to create a new Microsoft account. In this activity, you create a user account that authenticates by using a Microsoft account.

1. 1

If necessary, start your computer and sign in.

1. 2

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

1. 3

In the Settings window, click **Accounts** and then click **Family & other users**.

1. 4

Click **Add someone else to this PC**.

1. 5

On the How will this person sign in screen, click **I don’t have this person’s sign-in information**.

1. 6

On the Create account screen, in the First name box, type your first name.

1. 7

In the Last name box, type your last name.

1. 8

Click **Get a new email address**.

1. 9

In the New email box, type **yourfirstname.yourlastname@outlook.com**, substituting your first name and last name in the email address and then click **Next**. If the email address is not available, try different combinations until an address is available.

1. 10

In the Create password box, type a password that you will remember and then click **Next**. Use a strong password because the Microsoft account you are creating is accessible on the Internet.

1. 11

On the What’s your name screen, enter your name and then click **Next**.

1. 12

On the What’s your birth date screen, select the correct country, enter your birth date, and then click **Next**.

1. 13

Read the list of users on the Family & other users screen. Notice that the new account has been added to the list of users.

1. 14

Click the new account and then click **Change account type**.

1. 15

In the Change account type window, in the Account type box, select **Administrator** and then click **OK**.

1. 16

Sign out as Userx and sign in with the new Microsoft account.

1. 17

When prompted to set up a PIN, close the window. (Signing in with a PIN is covered later in this module.)

1. 18

On the Back up your files with OneDrive screen, click **Next**.

1. 19

On the Choose privacy settings for your device screen, click **Accept**.

1. 20

Click the **Start** button, click **Settings**, and then click **Accounts**. Notice that the Family & other users option is available because the Microsoft account is recognized as an administrator instead of a standard user.

1. 21

Sign out of your Microsoft account.

Go to pg.

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

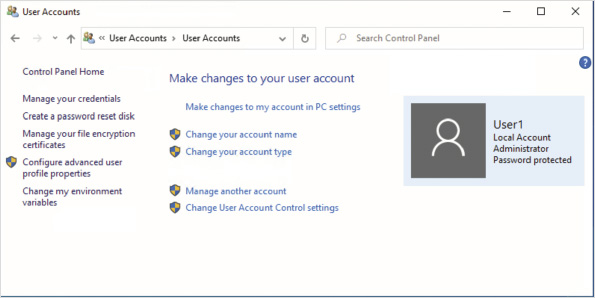
Application Opened

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

## 3-2bUser Accounts Applet

In older versions of Windows, the preferred interface for creating and managing user accounts was the [**User Accounts applet**](javascript://) in Control Panel. The User Accounts applet in Control Panel, shown in [Figure 3-6](javascript://), is still available in Windows 10 but has less functionality. For example, you cannot create a new user account in the User Accounts applet.

**Figure 3-6User Accounts Applet in Control Panel**



Enlarge Image

The administrative options with a shield beside them in the applet are restricted to administrative users. If a standard user tries to perform these tasks, the user is prompted to provide the credentials of an administrator account.

Administrative options for user accounts include the following:

* Change your account name—Allows administrators to change the account name of a user.
* Change your account type—Allows administrators to change the user account from one type of account to another. For example, you can change a standard user to an administrative user.
* Manage another account—Allows administrators to select a different account to manage.
* Change User Account Control settings—Allows administrators to modify when prompts from User Account Control (UAC) are presented.

Additional available tasks include:

* Manage your credentials—This option opens the window for configuring Credential Manager. Credential Manager allows users to add, remove, and edit network locations with stored credentials. Network locations can include websites, FTP sites, and servers. Storing credentials avoids having to type in the credentials each time a resource is accessed. If your password for the resource changes, you need to edit the network location to change the password. In domain-based networks, this is not required to access domain resources.
* Create a password reset disk—This option creates a password reset disk. If users forget their password, the disk allows them to reset their password to a new password. Once created, a password reset disk does not need to be updated when the user password is changed. The password reset information is stored on a USB drive. This is less likely to be used now that Windows 10 has added security questions as an option for resetting passwords.
* Manage your file encryption certificates—This option allows users to manage the certificates used to support Encrypting File System (EFS). EFS encrypts specific files that are stored on the hard drive. Within this wizard, you can select or create a file encryption certificate, back up the certificate, configure EFS to use a smart card, and update a previously encrypted file to a new certificate.
* Configure advanced user profile properties—This option opens the dialog box that allows you to manage user profiles. For example, you can configure a roaming user profile. This option is seldom used.
* Change my environment variables—This option allows you to configure the environment variables for your computer that define characteristics such as the location of temporary files. This option seldom is used.

**Activity 3-4**

### Using the User Accounts Applet

**Time Required:**10 minutes

**Objective:**Manage a local user account by using the User Accounts applet in Control Panel

**Description:**You can use the User Accounts applet in Control Panel to manage existing user accounts. In this activity, you change a local user account to an administrator from a standard account.

1. 1

If necessary, start your computer and then sign in.

1. 2

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

1. 3

In the Control Panel window, click **User Accounts**.

1. 4

In the User Accounts window, click **User Accounts**.

1. 5

In the User Accounts window, click **Manage another account**.

1. 6

In the Choose the user you would like to change box, click **Bob**.

1. 7

Read the options you have for managing the account and then click **Change the account type**.

1. 8

In the Change Account Type window, click **Administrator** and then click **Change Account Type**.

1. 9

Close the Change an Account window.

Go to pg.

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

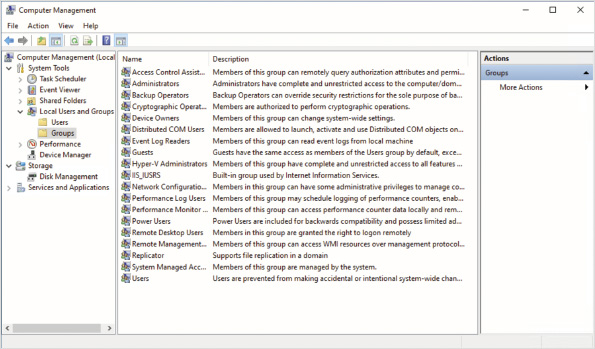
Application Opened

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

## 3-2cLocal Users and Groups MMC Snap-In

The Local Users and Groups MMC snap-in allows you to create and manage both user accounts and groups. The fastest way to access this snap-in is through the Computer Management Administrative Tool. The Users node contains all the users, and the Groups node contains all the groups, as shown in [Figure 3-7](javascript://).

**Figure 3-7Local Users and Groups in Computer Management**



Enlarge Image

The general user tasks you can perform are:

* Create a new user.
* Delete a user.
* Rename a user.
* Set a user password.

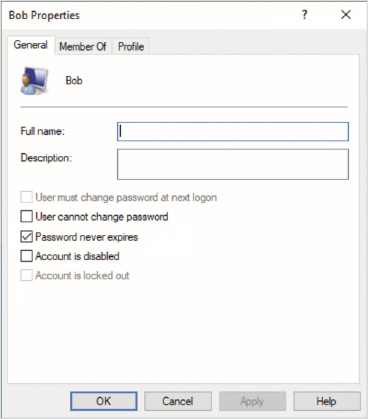
**Tip**

Setting a user password is relevant only for local user accounts. Accounts that are authenticated by using a Microsoft Account do not use a local password even though the option to reset the user’s password appears in the interface.

Other user options can be configured in the properties of the user account. The General tab, shown in [Figure 3-8](javascript://), lets you view and configure the following:

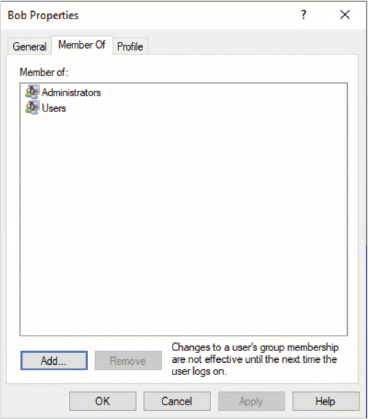
* Account name—This information is displayed at the top of the tab but cannot be changed on this tab. To change the account name, you must right-click the user account and then select Rename.
* Full name—This is the full name of the person using the account. This can be changed.
* Description—This is an optional text box that can be used to describe the purpose or use of the account.
* User must change password at next logon—This option forces users to change their password the next time they log on (sign in). Forcing a password change is common in corporate environments after a temporary password has been assigned.
* User cannot change password—This option prevents users from changing their passwords. Preventing a password change is often done for user accounts that are used as credentials for multiple services, such as scheduling system maintenance tasks. A password change would need to be updated on all services, and this ensures that it does not happen accidentally.
* Password never expires—This option exempts the user from the account policy that defines the maximum lifetime of a password. Preventing password expiration is useful for accounts that are used as credentials for services, such as scheduled tasks.
* Account is disabled—This option locks the account to prevent anyone from signing in and using the account; however, the account is retained and can be enabled again at any time. An account often is disabled when a user is away for an extended period of time. Disabling an account is also often done as an intermediary step before the account is deleted when a user leaves the organization.
* Account is locked out—This option is selected when Windows 10 locks out an account because of too many incorrect sign-in attempts. When an account is locked, no one can sign in by using the account. To unlock the account and allow the user to sign in again, deselect this option.

**Figure 3-8User Properties, General Tab**



The Member Of tab, shown in [Figure 3-9](javascript://), lists the groups of which the user account is a member. Any rights and permissions assigned to these groups are also given to the user account. You can add and remove the user account from groups on this tab. Be aware that changes in group membership do not take effect until the user has signed out and signed in again. This is because the security token that contains group memberships and is used to access resources is generated during sign-in.

**Figure 3-9User Properties, Member Of Tab**



The Profile tab typically is not used on stand-alone computers or workgroup members. Similar information is available for user accounts in a domain. It is much more common for these properties to be set in a domain.

This tab can be used to define the following:

* The location of a roaming user profile
* A logon script
* A home folder

The profile path specifies the location of the profile for this user. By default, profiles are stored in C:\Users\%USERNAME%, where %USERNAME% is a variable representing the name of the user account. If you specify a network location for the profile, the profile becomes a roaming user profile.

The logon script box defines a script that is run each time during sign-in. This script can be located on the local computer or another workgroup member. The logon script is typically a batch (.bat) file or VBScript (.vbs) file that is used to configure the computer with mapped drive letters for accessing network shares.

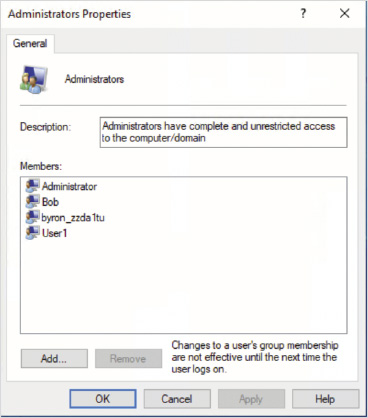
**Tip**

You can use Windows PowerShell scripts for log on scripts. To specify a Windows PowerShell script, you need to use Group Policy instead of the user properties.

The home folder defines a default location for saving files. If a network location is used as a home folder, a mapped drive letter is created that points to the network location. The default location for saving files is defined by the application being used. Some applications use the home folder, while others use the Documents folder. If you do not define a home folder, it resolves to the user’s profile folder, for example, C:\Users\User1.

When you view the properties of a group, there is only a single tab, as shown in [Figure 3-10](javascript://). The General tab provides a description of the group and a list of the group members. You can add and remove users from the group here.

**Figure 3-10Group Properties**



**Activity 3-5**

### Using the Local Users and Groups MMC Snap-In

**Time Required:**10 minutes

**Objective:**Manage users and groups by using the Local Users and Groups MMC snap-in

**Description:**The Local Users and Groups MMC snap-in is the only management tool for creating and managing groups. You can also use it for creating and managing users. The user management options in the Local Users and Groups MMC snap-in are more detailed than Accounts settings. In this activity, you create a new user, create a new group, and place the new user in the new group.

1. 1

If necessary, start your computer and sign in.

1. 2

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

1. 3

In the left pane, expand Local Users and Groups and then click **Users**. Notice the users who are listed here: Administrator, Bob, DefaultAccount, Guest, WDAGUtilityAccount, Userx, and your Microsoft account.

1. 4

Double-click **Bob**.

1. 5

In the Bob Properties dialog box, on the General tab, in the Full name box, type **Robert Smith** and read the other available options.

1. 6

Click the **Member Of** tab and read the list of groups that Bob is a member of, and then click **Cancel**.

1. 7

In Computer Management, right-click **Users** and then click **New User**.

1. 8

In the User name box, type **Jacob**.

1. 9

In the Full name box, type **Jacob Smith**.

1. 10

In the Password and Confirm password boxes, type **password**. Notice that, by default, the User must change password at next logon check box is selected.

1. 11

Click **Create** and then click **Close**.

1. 12

In the left pane, click **Groups**. Notice all the built-in groups that exist by default.

1. 13

Double-click **Administrators** and read the list of group members. Notice that any user account configured as an administrator account is a member of this group.

1. 14

In the Administrator Properties dialog box, click **Cancel**.

1. 15

Right-click **Groups** and then click **New Group**.

1. 16

In the New Group dialog box, in the Group name box, type **TestGroup**.

1. 17

Click the **Add** button.

1. 18

In the Select Users dialog box, in the Enter the object names to select box, type **Jacob**, click **Check Names**, and then click OK.

1. 19

Click **Create** and then click **Close**.

1. 20

In the left pane, click **Users**.

1. 21

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

1. 22

Click the **Member Of** tab. Notice that Jacob is a member of TestGroup and Users.

1. 23

Click **Cancel** and then close the Computer Management window.

1. 24

Switch the user to **Jacob Smith**. Notice that you are given a message indicating that the password must be changed.

1. 25

Click **OK**.

1. 26

In the New password and Confirm password boxes, type **password2** and then press **Enter**.

1. 27

Click **OK** and wait for the new profile to be created.

1. 28

On the Choose privacy settings for your device screen, click **Accept.**

1. 29

Sign out as Jacob.

Go to pg.

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

Application Opened

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

## 3-2dCommand-Line User Management

Most management of local users is done with graphical utilities because they are easier to use; however, you do have the option to use command-line tools for local user administration. [Table 3-1](javascript://) lists Windows PowerShell cmdlets that you can use to manage local users.

**Table 3-1**

### Windows PowerShell Cmdlets for Local User Management

| **Cmdlet** | **Description** |
| --- | --- |
| New-LocalUser | Creates new local users. |
| Remove-LocalUser | Deletes local users. |
| Get-LocalUser | Retrieves information about local users. |
| Set-LocalUser | Modifies local users. |
| Rename-LocalUser | Renames local users. |
| Disable-LocalUser | Disable local users that are enabled. |
| Enable-LocalUser | Enables local users that are disabled. |

**Tip**

The net.exe command-line tool can create, configure, and delete local users. For more information run **net user /?** at a command prompt.

**Activity 3-6**

### Performing Command-Line User Management

**Time Required:**10 minutes

**Objective:**Manage users and groups by using command-line tools

**Description:**Most of the time you will perform user management tasks using graphical utilities. Sometimes, however, when you are querying information it is faster to use command-line tools. In this activity, you perform user management tasks by using command-line tools.

1. 1

If necessary, start your computer and sign in.

1. 2

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

1. 3

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

1. 4

At the Windows PowerShell prompt, type **net user** and then press **Enter**.

1. 5

At the Windows PowerShell prompt, type **net user /?** and then press **Enter**.

1. 6

At the Windows PowerShell prompt, type **net user Jacob** and then press **Enter**.

1. 7

At the Windows PowerShell prompt, type **Get-LocalUser** and then press **Enter**.

1. 8

At the Windows PowerShell prompt, type **Get-LocalUser | Where Enabled -eq $true** and then press **Enter**.

1. 9

At the Windows PowerShell prompt, type **Get-LocalUser Jacob** and then press **Enter**.

1. 10

At the Windows PowerShell prompt, type **Get-LocalUser Jacob | Format-List** and then press **Enter**.

1. 11

At the Windows PowerShell prompt, type **Set-LocalUser Jacob -Description "Test User Account"** and then press **Enter**.

1. 12

At the Windows PowerShell prompt, type **Disable-LocalUser Jacob** and then press **Enter**.

1. 13

At the Windows PowerShell prompt, type **Get-LocalUser Jacob | Format-List** and then press **Enter**. Notice that the describe text is present and the account is not enabled.

1. 14

Close the Windows PowerShell prompt window.

Go to pg.

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

Application Opened

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

**3-3**Managing User Profiles

A [**user profile**](javascript://) is a collection of desktop and environment configurations for a specific user or group of users. By default, each user has a separate profile stored in C:\Users. Many of the folders in the profile are not visible by default in File Explorer because they are marked as hidden or system files. You can change the view settings in File Explorer to make all of the folders visible.

A profile contains the following folders and information:

* *3D Objects*—The default save location for the Paint 3D application.
* *AppData*—A hidden folder containing user-specific information for applications, such as configuration settings.
* *Application Data*—A hidden shortcut to AppData for backward compatibility with Windows 2000 and Windows XP applications.
* *Contacts*—A folder to hold contacts and their properties. Contact properties include addresses, phone numbers, email addresses, and digital certificates. Contacts can be used by various applications, but the most common are email applications.
* *Cookies*—A hidden shortcut to the storage location for Internet Explorer cookies. This shortcut is for backward compatibility with previous versions of Internet Explorer. Microsoft Edge uses a location in the AppData folder for cookies.
* *Desktop*—A folder that contains all the shortcuts and files on the user desktop.
* *Documents*—A folder that is typically the default location for saving documents.
* *Downloads*—A folder that is used to store files and programs downloaded from the Internet.
* *Favorites*—A folder that holds Internet Explorer favorites. Microsoft Edge uses a location in the AppData folder for favorites.
* *Links*—A folder in Windows 8 that contained links that were displayed as Favorites in File Explorer. This folder is not used by File Explorer in Windows 10.
* *Local Settings*—A hidden shortcut that is included for backward compatibility with Windows 2000 and Windows XP applications.
* *Music*—A folder for storing music files.
* *My Documents*—A hidden shortcut that is included for backward compatibility with Windows 2000 and Windows XP applications.
* *NetHood*—A hidden shortcut to a location storing user-specific network information, such as drive mappings. This is included for backward compatibility.
* *OneDrive*—A folder that is synchronized with cloud storage in Microsoft OneDrive. All Microsoft accounts are allocated storage space online in OneDrive.
* *Pictures*—A folder for storing picture files. It appears as My Pictures in Windows Explorer.
* *PrintHood*—A hidden shortcut to a location storing user-specific printing information, such as network printers. This is included for backward compatibility.
* *Recent*—A hidden shortcut to a location storing shortcuts to recently used documents. This is included for backward compatibility.
* *Saved Games*—A folder for storing saved games that are in progress.
* *Searches*—A folder that stores saved search queries so that they can easily be accessed again.
* *SendTo*—A hidden shortcut to the location storing shortcuts that appear in the Send To menu when right-clicking a data file. This is included for backward compatibility.
* *Start Menu*—A hidden shortcut to the location storing the shortcuts and folders that appear in the Start menu. This is included for backward compatibility.
* *Templates*—A hidden shortcut to the location storing application templates, such as Word document templates. This is included for backward compatibility.
* *Videos*—A folder for storing videos.
* [***Ntuser.dat***](javascript://)—A file that stores user-specific registry information.
* *Ntuser.dat.log*x—A file that tracks changes in Ntuser.dat. This file is used to recover Ntuser.dat if the system shuts down unexpectedly.
* *Ntuser.dat{guid}.tm.blf*—A temporary file used for controlling registry changes.
* *Ntuser.ini*—A file that controls which portions of a profile are not to be copied up to a server when roaming profiles are enabled.

In most cases, you never need to customize profiles. You can allow users to modify their own profiles as desired; however, options are available that you can use to standardize and modify profiles, such as mandatory profiles, that might be useful in specific scenarios.

Go to pg.

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

Application Opened

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

## 3-3aThe Default Profile

The [**default profile**](javascript://) is used when new user profiles are created. When a new user signs in for the first time, Windows 10 copies the default user profile to create a profile for the new user. The folder structure in the default profile is the same as a user profile; however, the folders are empty by default.

In older versions of Windows, such as Windows XP, you created a consistent environment for users by configuring the default profile on each computer to be the same. In a more modern computer network, it is rare to manually configure the default profile. Instead, you should use centralized management tools such as Group Policy to enforce consistent settings on computers.

Although you can see user profiles in the file system, you cannot copy them using File Explorer. If you copy a profile using File Explorer, the security permissions are incorrect, and the user will experience several errors. If you want to configure the default profile, the only supported method is by using Sysprep.

**Caution**

Modifying the Start menu layout within the default profile is not supported.

To configure the default profile:

1. If desired, create a new local user with administrative privileges to allow for creation of a blank user profile. Domain users are not supported.
2. Sign in as the designated local user with administrative privileges.
3. Modify the user’s profile as desired and delete all other user profiles. You must delete the other profiles to ensure that the correct user profile is copied.
4. Create an answer file with the CopyProfile parameter set to true.
5. Run Sysprep with the /generalize option and specify the location of the answer file.
6. Image the computer and deploy the image. When the image is started after deployment, the default user profile is created from the profile of the local user account used in the preceding steps.

**Tip**

In many online blog postings, users complain about inconsistent functionality of CopyProfile with Windows 10. Instead of configuring a default profile, use Group Policy to provide consistent user settings. Default profile settings are copied only when the profile is first created, whereas Group Policy settings can be changed at any time after deployment.

Go to pg.

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

Application Opened

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

## 3-3bMandatory Profiles

A [**mandatory profile**](javascript://) is a profile that cannot be modified. Users can make changes to their desktop settings while they are signed in, but the changes are not saved. This means that if a configuration problem occurs, all the user needs to do is sign out and sign back in to get pristine settings again.

You can implement mandatory profiles for a single user that is causing problems or for a group of users. Most often, a single consistent desktop is implemented for a group of users. Most mandatory profiles are implemented as roaming user profiles.

To change a profile to a mandatory profile, you rename the file Ntuser.dat to Ntuser.man. After this change is made, user modifications to the profile are not saved.

**Caution**

If you implement mandatory profiles, you need to ensure that users are aware that any files that they save to their Desktop or Documents folders are lost when they sign out.

Go to pg.

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

Application Opened

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

## 3-3cRoaming Profiles

A [**roaming profile**](javascript://) is stored in a network location rather than on the local hard drive. The main benefit of roaming profiles is that settings move with a user from computer to computer on the network. Typically, roaming profiles are used in large corporations where users move among different computers each day, such as a call center.

When roaming user profiles are in place, users have a consistent work environment regardless of which computer they sign in at. This means that any customization application settings and configuration files move with the user between computers.

To configure a roaming profile, you must edit the user account to point the profile directory at a network location. You then copy the existing user profile up to the network location.

Each time a user signs in, the roaming profile is copied to the local computer. If a user signs in and cannot contact the server with the roaming profile, the local copy of the profile is used.

Many administrators prefer not to implement roaming user profiles for the following reasons:

* Slow sign-in and sign-out—If users store large files in their user profile, sign-in and sign-out are slow. The slowness is caused because the user profile is copied over the network each time the user signs in and signs out.
* Corrupted profiles—Although not as common as with older versions of Windows, roaming user profiles can become corrupted. When a profile is corrupted, users are signed in with a temporary profile and do not have access to their normal settings. Intervention by an administrator is required to remove the corrupted profile.

Go to pg.

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

Application Opened

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

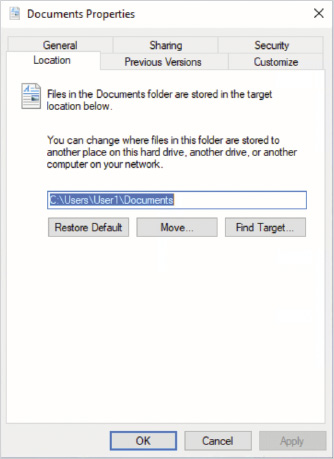
## 3-3dFolder Redirection

Most organizations that want the ability to roam among computers implement folder redirection. [**Folder redirection**](javascript://) lets you specify a network location for specific profile folders as an alternative to storing the data on the local client. Because the folders are redirected rather than copied, the speed of signing in or signing out is not impacted. To users, the redirected folders appear and function the same as if the folder were stored locally.

You can combine folder redirection with roaming profiles to mitigate the shortcomings of roaming profiles. Redirecting folders avoids the slow sign-in and sign-out process that can occur with large files. Profile corruption is also minimized because the sign-out process is faster and access to the registry is more likely to be terminated properly during sign-out.

You can manually redirect some folders, such as Documents, as shown in [Figure 3-11](javascript://). In most cases, however, folder redirection is implemented by using Group Policy.

**Figure 3-11Folder Redirection for Documents**



Go to pg.

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

Application Opened

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

## 3-3eThe Public Profile

The [**public profile**](javascript://) is different from other profiles because it is not a complete profile and it is not assigned exclusively to a user. The public profile does not include an Ntuser.dat file and consequently does not include any registry settings. The public profile is a series of folders. The content of these folders is merged into the profiles of other users when they sign in. For example, shortcuts or files placed in the Public Desktop Folder appear on the desktop of each user. Some applications place a shortcut in the Public Desktop folder as part of installation to make it available to all users. Only users with administrative permission can modify the contents of the Public profile.

The public profile includes the following folders:

* Libraries—Libraries stored here do not appear in user profiles but are available to all users in File Explorer.
* Public Account Pictures—Pictures selected by users for display with their user accounts are stored here.
* Public Desktop—Files and shortcuts stored here appear on the desktop of each user.
* Public Documents—Files stored here appear in the Documents library of each user.
* Public Downloads—Files stored here do not appear in profiles, but the files in it are available to all users.
* Public Music—Files stored here appear in the Music library of each user.
* Public Pictures—Files stored here appear in the Pictures library of each user.
* Public Videos—Files stored here appear in the Videos folder of each user.

**Activity 3-7**

### Modifying the Public Profile

**Time Required:**5 minutes

**Objective:**Modify the public profile and see how it affects users

**Description:**The public profile is merged into the profile of all users. Adding content to the public profile means that the content is available to all users. In this activity, you place a file in the Public Documents folder, which makes it available to all users.

1. 1

If necessary, start your computer and sign in.

1. 2

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

1. 3

In the left pane, expand **This PC**, expand **Local Disk (C:)**, expand **Users**, expand **Public**, and then click **Public Documents**.

1. 4

In the right pane, right-click an open area, point to **New**, and then click **Shortcut**.

1. 5

In the Type the location of the item box, type **C:\Windows\notepad.exe** and then click **Next**.

1. 6

In the Type a name for this shortcut box, type **Notepad** and then click **Finish**.

1. 7

Right-click the **Notepad** shortcut and then click **Cut**.

1. 8

In the File Explorer address bar, type **C:\Users\Public\Desktop** and then press **Enter**.

1. 9

Right-click an empty area and then click **Paste**. Notice that even an administrative user is prompted for permission to copy files here.

1. 10

Click **Continue**. Notice that a shortcut to Notepad now is on your desktop.

1. 11

Double-click the **Notepad** shortcut on your desktop to test it.

1. 12

Exit Notepad.

1. 13

Close the File Explorer window.

Go to pg.

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

Application Opened

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

# 3-4Start Menu and Taskbar Customization

In Windows 7, the Start menu was a collection of folders and shortcuts to applications. You could modify the Start menu by creating folders and shortcuts. In Windows 10, you cannot manually create folders and shortcuts in the Start menu. Instead, for your own profile, you can add and remove programs from the Start menu by right-clicking the program and pinning it to the Start menu. You can also create your own groups in the Start menu to organize items.

You can use Group Policy to customize the Start screen. The layout of the Start menu is defined by an XML file that you create. The XML file is stored in a central location, and the Group Policy directs computers to the XML file. You can apply a full Start layout, which users cannot modify, or a partial Start layout, in which the specified groups cannot be modified but other groups can.

By default, the exported XML file is configured to apply the full StartLayout. To apply a partial Start layout, you need to modify the <DefaultLayoutOverride> element as <DefaultLayoutOverride LayoutCustomizationRestrictionType="OnlySpecifiedGroups">. You also need to edit the XML file to include only the groups and tiles that you want to be locked because those are merged with the existing Start menu.

**Note 3**

For detailed information about customizing the Start layout, see Customize and export Start layout at [https://docs.microsoft.com/en-us/windows/configuration/customize-and-export-start-layout](https://docs.microsoft.com/en-us/windows/configuration/customize-and-export-start-layout" \t "_blank).

You can also customize the Start menu by using Windows Imaging and Configuration Designer (ICD). Windows ICD can create provisioning packages that configure a customized Start layout.

**Caution**

You cannot use Group Policy or provisioning packages to customize the Start menu layout or taskbar for Windows 10 Home.

**Activity 3-8**

### Customizing the Start Layout

**Time Required:**10 minutes

**Objective:**Modify the Start layout and see how it affects users

**Description:**You can customize the Start menu for Windows 10 Enterprise and Windows 10 Education editions. In this activity, you customize the Start menu and then export it so that it can be used on other computers. You also test applying the Start layout by using a local Group Policy.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **Paint**, right-click **Paint**, and then click **Pin to Start**.

1. 3

Click the **Start** button, move the pointer above the Paint tile until Name group appears, and then click **Name group.**

1. 4

Type **Tools** and then press **Enter**.

1. 5

Close the Start menu, click the **Start** button, type **Computer**, right-click **Computer Management**, and then click **Pin to Start**.

1. 6

Click the **Start** button and then drag **Computer Management** to the Tools group.

1. 7

Click the **Start** button, type **PowerShell**, right-click **Windows PowerShell**, and then click **Pin to Start**.

1. 8

Click the **Start** button and then drag **Windows PowerShell** to the Tools group.

1. 9

Click **Windows PowerShell**.

1. 10

At the Windows PowerShell prompt, type **md C:\Start** and then press **Enter**.

1. 11

Type **Export-StartLayout -Path C:\Start\Start.xml** and then press **Enter**.

1. 12

Type **notepad.exe C:\Start\Start.xml** and then press **Enter**.

1. 13

Review the contents of the file. Notice that two groups are named Productivity and Tools. Read the information for the programs in each group.

1. 14

Exit Notepad and close the Windows PowerShell window.

1. 15

Click the **Start** button, type **mmc**, and then click **mmc**.

1. 16

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

1. 17

In the Console1 window, click **File** on the menu bar and then click **Add/Remove Snap-in**.

1. 18

In the Add or Remove Snap-ins window, click **Group Policy Object Editor**, click **Add**, click **Finish,** and then click **OK**.

1. 19

In the Console1 window, in the left pane, navigate to **\Local Computer Policy\User Configuration\Administrative Templates\Start Menu and Taskbar**.

1. 20

In the right pane, right-click **Start Layout** and then click **Edit**.

1. 21

In the Start Layout window, click **Enabled**.

1. 22

In the Start Layout File box, type **C:\Start\Start.xml** and then click **OK**.

1. 23

Leave the Console1 window open.

1. 24

Switch users and then sign in as Bob.

1. 25

Click the **Start** button and verify that the Tools group appears.

1. 26

Sign out as Bob and then sign in as Userx.

1. 27

In the Console1 window, double-click **Start Layout**, click **Not Configured**, and then click **OK**.

1. 28

Close all open windows. Do not save settings if prompted.

**Tip**

After disabling the customized Start layout, user profiles with the customized layout will retain it, but users can now modify it.

You deploy a customized taskbar layout by using the same XML file that you use for customizing the Start layout. You need to add more XML elements for the taskbar apps you want to configure. No option to export the XML is available, but Microsoft does provide detailed examples on their website. You can configure the XML file to include only taskbar configuration information, which leaves the Start menu unmodified.

When you configure the taskbar, you can add apps to the existing default configuration or remove defaults and include only the apps you specify. This is controlled by the <CustomTaskBarLayoutCollection> tag. By default, the apps you specify merge with the existing default configuration. If you want to replace existing apps, you need to modify the tag as <CustomTaskBarLayoutCollectionPinListPlacement="Replace">.

**Note 4**

For detailed examples of customizing the taskbar, see Configure Windows 10 taskbar at [https://docs.microsoft.com/en-us/windows/configuration/configure-windows-10-taskbar](https://docs.microsoft.com/en-us/windows/configuration/configure-windows-10-taskbar" \t "_blank).

Go to pg.

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

Application Opened

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

**3-5**Advanced Authentication Methods

Windows 10 includes advanced authentication methods to make using your computer more convenient and more secure. PIN or picture password authentication allows you to sign in with unique information other than your user name and password. Biometric authentication allows you to sign in based on facial recognition, fingerprints, or iris scanning.

When you use a user name and password to authenticate to Windows 10, a risk exists that the user name and password could be stolen. They can be stolen by someone looking or recording over your shoulder when you sign in. They can also be stolen by keylogging malware installed on your computer. After your credentials are stolen, an unauthorized person can use your credentials to get access to all your resources. Advanced authentication methods avoid this problem because you no longer type in your user name and password.

Multifactor authentication increases security by requiring you to have something in addition to a user name and password. The advanced authentication methods add multifactor authentication because they are unique to the device on which you are authenticating. For example, if you enable PIN-based authentication, the PIN you select is different for each device. If someone steals your PIN, that person also needs your device for that information to be useful. In the case of biometric authentication, the something that must be provided is you.

Go to pg.

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

Application Opened

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

## 3-5aPicture Password

After [**picture password authentication**](javascript://) is configured, to sign in, you perform gestures on a picture that you have selected. To configure picture password authentication, you need to select a picture and then provide gestures on that picture. The gestures are typically going to be tracing out significant features on the picture, but they can be any gesture that you like.

When you configure picture password authentication, it is unique for each computer or device. Knowing your gestures and picture are useful only if someone also gets physical access to your device. Malware is unable to capture and use this information.

Go to pg.

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

Application Opened

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

## 3-5bWindows Hello PIN

Configuring [**PIN authentication**](javascript://) provides similar benefits to picture password authentication. When you configure PIN (personal identification number) authentication, you provide a unique PIN for authenticating instead of your user name and password. As with picture password authentication, this PIN is unique to a specific computer. Knowing the PIN is useful only if someone also gets physical access to your device.

**Activity 3-9**

### Configuring PIN Authentication

**Time Required:**10 minutes

**Objective:**Configure PIN authentication for a user

**Description:**PIN authentication enhances security in Windows 10 by avoiding reuse of a user name and password. In this activity, you enable and test PIN authentication for a user.

1. 1

If necessary, start your computer and sign in.

1. 2

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

1. 3

In the Settings window, click **Accounts** and then click **Sign-in options**.

1. 4

On the Sign-in options screen, click **Windows Hello PIN** and then click **Add**.

1. 5

In the First verify your account password dialog box, type **password** (or your password) and then click **OK**.

1. 6

In the Set up a PIN dialog box, in the New PIN and Confirm PIN boxes, type **982377** and then click **OK**.

1. 7

Sign out and then sign back in by using your PIN.

1. 8

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

1. 9

In the Settings window, click **Accounts** and then click **Sign-in options**.

1. 10

Click **Windows Hello PIN** and then click **Remove**.

1. 11

Read the message about removing the PIN and then click **Remove**.

1. 12

In the First, verify your account password dialog box, type **password** (or your password) and then click **OK**.

1. 13

Close all open windows.

Go to pg.

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

Application Opened

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

## 3-5cWindows Hello Biometric Authentication

[**Biometric authentication**](javascript://) has long been available for Microsoft operating systems. Many mobile computers include fingerprint readers that were compatible with earlier versions of Windows. As new versions of Windows were released, Microsoft enhanced the operating system support for biometric authentication. This made it easier for manufacturers of biometric readers to develop drivers because the operating system provided specific support for the process. In Windows 10, [**Windows Hello**](javascript://) is the infrastructure that supports passwordless authentication, including biometric authentication.

Windows Hello supports the following biometric authentication methods:

* Fingerprint—To authenticate with a fingerprint, you place your finger on a fingerprint reader (or swipe, depending on the type of reader).
* Facial recognition—To authenticate with facial recognition, you place your face in front of the camera. This can happen immediately when you sit down in front of your computer.

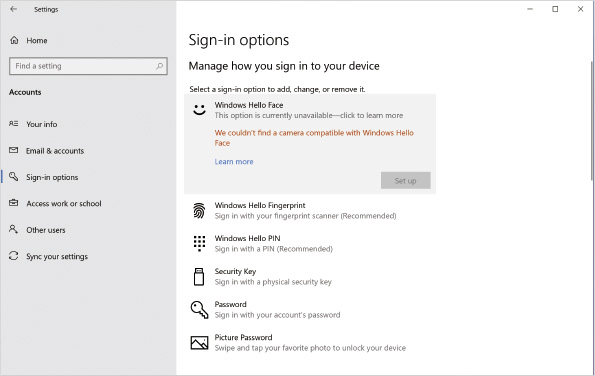
To make biometric authentication more secure, Windows Hello requires biometric readers to have advanced functionality to ensure accurate authentication. For example, cameras for facial recognition need to have infrared support (which prevents someone from using a picture of you to sign in). Consequently, most biometric readers available before the release of Windows 10 are not compatible with Windows Hello. If you want to use biometric authentication, verify that any new biometric readers are compatible with Windows Hello.

Before you enable biometric authentication, you need to configure PIN authentication. PIN authentication is used as a backup authentication method if biometric authentication fails.

When biometric authentication is enabled, you need to provide your biometric information during configuration. Windows Hello, however, does not store a picture of your fingerprint, face, or iris. Instead, Windows Hello stores information about the unique pattern that your biometric information provides. This ensures that data from Windows Hello cannot be used to re-create your biometric information.

You can tell whether your computer has the necessary hardware to support biometric authentication from the Sign-in options screen shown in [Figure 3-12](javascript://). If your computer lacks the necessary hardware, the sign-in option will indicate “This option is currently unavailable” like is shown for Windows Hello Face. A supported fingerprint reader is available on the computer.

**Figure 3-12Sign-In Options Screen**



Enlarge Image

Windows Hello is designed for stand-alone devices, and no synchronization of credentials between devices is supported. So, if you have two laptops and change your Microsoft account password on one of them, you will need to enter the new Microsoft account password manually on the second system before you can authenticate. Effectively, Windows Hello is encrypting a locally stored copy of the credentials. When you sign in by using Windows Hello, it unlocks the stored credentials.

Go to pg.

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

Application Opened

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

## 3-5dWindows Hello for Business

[**Windows Hello for Business**](javascript://) is a more advanced authentication system that builds on the infrastructure provided by Windows Hello. Its purpose is still to allow users to sign in by using a PIN or biometric authentication, but more advanced techniques are used for a high level of security and better user experience. In particular, changing your user password does not require manually entering the new password is multiple devices, because passwords are not used for authentication.

To use Windows Hello for Business, the computer running Windows 10 must be joined to a domain, Azure AD joined, or registered with Azure AD. Each identity provider that supports Windows Hello for Business identifies you by using a unique certificate with a public key and private key. The identity provider retains the public key while Windows 10 retains the private key. Access to the private key in Windows 10 is secured by Windows Hello. When you access an identity provider, Windows Hello authenticates you and then uses the private key to verify your identity with the identity provider holding the corresponding public key.

If your computer has a trusted platform module (TPM), the private key for the certificate is stored in the TPM. If no TPM is present, the private key is stored and secured by software. A TPM is a chip on the motherboard of a computer that is used to store encryption keys and certificates. Not all computers have a TPM.

**Note 5**

For an overview video of how Windows Hello for Business Works, see How Windows Hello for Business works at [https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works" \t "_blank).

Go to pg.

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

Application Opened

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

## 3-5eSecurity Key

A [**security key**](javascript://) is a hardware device (usually USB connected) that is used to uniquely identify you. Having possession of that security key allows you to sign in to websites, such as Office 365. You can take the security key with you to multiple devices, and your ability to authenticate to websites travels with the security key. You can also use a security key to sign into Windows 10.

Security key support for signing in to web-based applications is not a Microsoft-specific protocol. It is based on standards from the FIDO Alliance which are supported by the major browsers.

Simply plugging in the security key is not enough to allow authentication. You need to also provide a PIN or biometric information to unlock the security key. Many security keys include a fingerprint reader as part of the device.

**Tip**

You can use a security key to enable fingerprint-based authentication on computers that don’t have a fingerprint scanner.

Go to pg.

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

Application Opened

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

## 3-5fDynamic Lock

You can use [**dynamic lock**](javascript://) to increase security on computers that have Bluetooth functionality. When you leave a computer unattended, you should remember to lock the screen if you don’t sign out. If you don’t lock the screen, the computer could be used by an unauthorized person until the screen saver starts (assuming you’ve enabled the option to require unlock after the screen saver starts).

Dynamic lock triggers your computer to lock when a specified Bluetooth device that is paired with your computer is out of range. Most of the time a mobile phone will be used for dynamic lock, but you could use other devices like a Fitbit that is Bluetooth enabled. When you forget to lock the screen and leave to grab a coffee, your computer will lock when your Bluetooth device and computer can no longer communicate.

**Caution**

Because the signal strength of Bluetooth devices can vary, it’s not possible to predict the exact distance that will trigger dynamic lock.

Go to pg.

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

Application Opened

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

## 3-5gSmart Cards

You can use smart cards as another form of multifactor authentication in Windows 10. A [**smart card**](javascript://) contains a certificate that is used for authentication in much the same way as Microsoft Passport; however, smart card authentication is applicable only to signing in to Windows and not additional resources, such as websites.

To use smart cards for authentication, each computer must have a smart card reader. You also need to install and configure a certification authority to issue the certificates that are stored on the smart cards. The cost of hardware and relatively high complexity of smart cards has prevented most organizations from implementing smart cards even though they have been supported since Windows 2000.

When users sign in by using a smart card, they first need to put the smart card in the smart card reader. Then, the user is prompted to enter a PIN that is associated with the smart card. The PIN is required to access the certificate on the smart card.

Windows 8 and newer versions of Windows also have the ability to use virtual smart cards. A [**virtual smart card**](javascript://) stores the certificate in the TPM of the computer instead of on a physical smart card; however, like a physical smart card, the user needs to enter a PIN to use the virtual smart card.

When a virtual smart card is present in a computer, it functions like a smart card that is permanently attached to the computer. To authenticate by using the smart card at the sign-in screen, you need to select the correct sign-in option and then provide the PIN.

Virtual smart cards can be created by using the same certificate infrastructure that you would use for physical smart cards; however, you can also use the Tpmvscmgr.exe command-line tool. To use Tpmvscmgr.exe, you must have administrative rights on the computer.

**Caution**

Smart card sign-in can be used only on domain-based networks and local user accounts.

Go to pg.

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

Application Opened

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

**3-6**Network Integration

Additional considerations must be taken into account when you place Windows 10 on a network and want to interact with other network users. User sign-in and authorization is very different in a networked environment. A networked environment requires you to understand the configuration of the local computer and other networked computers. You need to understand both peer-to-peer and domain-based network types. You should also understand Azure AD and how cached credentials work in Windows 10.

Go to pg.

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

Application Opened

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

## 3-6aPeer-to-Peer Networks

A [**peer-to-peer network**](javascript://) (or workgroup) consists of multiple Windows computers that share information. No computer on the network serves as a central authoritative source of user information. Each computer maintains a separate list of users and groups in its own SAM database. [Figure 3-13](javascript://) shows a peer-to-peer network.

**Figure 3-13Peer-to-Peer Network**



This type of network is most commonly implemented in homes and small offices. Windows 10 has a limit of 20 concurrent connections, which makes it impractical for sharing files and printers in larger environments.

In a peer-to-peer network, when you access shared folders or printers on a remote computer, you must authenticate as a user that exists on the remote computer. In most cases, it is preferred that the remote computer has a user account with the exact same name and password as the local machine. This allows [**pass-through authentication**](javascript://) to occur. Pass-through authentication occurs when Windows attempts to authenticate to a remote resource by using the local Windows credentials to sign in to the remote computer. This requires a user account with the same user name and password to exist on the remote computer.

Pass-through authentication is the simplest authentication method for users. Managing the user accounts and passwords on each computer is difficult. No automated mechanism exists to synchronize user accounts and passwords among computers in a peer-to-peer network. As a consequence, security management for peer-to-peer networks is progressively more difficult as the number of computers expands.

Newer authentication methods, such as Windows Hello, PIN, picture password, and Microsoft accounts, do not work with pass-through authentication because you are no longer using a local password to authenticate and you cannot synchronize the alternate credentials.

**Tip**

You might see some older documentation that describes using Homegroups to simplify resource sharing in workgroups; however, this feature was removed from Windows 10 in the March 2018 feature update. Explore using cloud services, such as OneDrive, to simplify file sharing for workgroups.

Go to pg.

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

Application Opened

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

## 3-6bDomain-Based Networks

User accounts for a [**domain-based network**](javascript://) are much easier to manage than user accounts for a peer-to-peer network. A central server called a domain controller is responsible for maintaining user accounts and computer accounts. All computers in the domain share the user accounts on the domain controller. So, user accounts need to be created only once, and no concerns about synchronizing passwords among multiple accounts should arise. [Figure 3-14](javascript://) shows a domain-based network.

**Figure 3-14Domain-Based Network**



To participate in a domain, Windows 10 computers are joined to the domain. The joining process creates a computer account for the Windows 10 computer and integrates Windows 10 security with the domain. Any existing local user accounts continue to exist and can still be used for local authentication.

Security is integrated with the domain in the following ways:

* Windows 10 trusts domain controllers in the domain to perform authentication.
* The Domain Admins group in the domain becomes a member of the local Administrators group to allow centralized administration by the domain administrators.
* The Domain Users group becomes a member of the local Users group to allow all users in the domain to sign in to Windows 10.

Some organizations prefer not to allow all domain users to sign in to any domain-joined computer. After the computer is joined to the domain, you can remove Domain Users from the local Users group and add only the specific domain user accounts that you want to allow. You could allow only members of a specific department or a single user.

Go to pg.

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

Application Opened

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

## 3-6cCached Credentials

When you use Windows 10 and sign in to a domain, your authentication credentials are automatically cached in Windows 10. This [**cached credentials**](javascript://) capability is important for mobile computers that are not always connected to the domain. After credentials are cached locally, you can sign in to a computer using a domain user account, even when the domain cannot be contacted. For example, users with mobile devices can sign in with their domain account when on the road at a client site or at home.

By default, the credentials of the last 10 users to sign in are cached. If required, however, you can increase this up to 50 users, or disable cached credentials entirely. You might want to disable cached credentials because there are known methods for decrypting cached credentials if you are able to sign in as an administrator of the local computer.

**Tip**

Cached credentials can be disabled by using Group Policy to configure the Interactive logon: number of previous logons to cache (in case domain controller is not available) setting to a value of 0.

Cached credentials are also used when you select to sign in with a Microsoft account in non-domain networks. Cached credentials for Microsoft accounts ensure that you can sign in when your computer does not have access to the Internet. The Group Policy setting that disables cached domain credentials does not affect caching of a Microsoft account.

Go to pg.

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

Application Opened

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

## 3-6dAzure AD Join

Some smaller organizations are starting to use Microsoft cloud services as their core business applications. When user accounts are created for Microsoft cloud services like Office 365, the user account is created in Azure AD. Azure AD is the Microsoft cloud service for identity management.

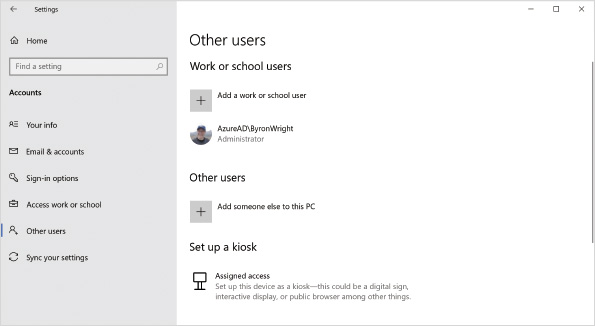
The role of Azure AD for cloud services is similar to Active Directory in on-premises environments. Recall that you can use Azure AD join to connect computers running Windows 10 to Azure AD and allow users to sign in by using Azure AD accounts. This means that users can authenticate to their desktop computer by using the same account that they use for Microsoft cloud services.

**Tip**

A computer running Windows 10 can be joined to Azure AD during initial setup or after initial configuration. For detailed information about how to perform an Azure AD join, see Join your work device to your organization’s network at [https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-join-device-on-network](https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-join-device-on-network" \t "_blank).

When you join Windows 10 to Azure AD, the user performing the join process is made a member of the local Administrators group. To support management by the organization, Azure AD global administrators and Azure AD device administrators are also made members of the local Administrators group. No other Azure AD user accounts are automatically given permission to use an Azure AD joined device; however, you can manually add more Azure AD users in the Accounts settings, as shown in [Figure 3-15](javascript://). In the figure, additional Azure AD users can be added in the Work or school users area. Local users and Microsoft accounts are managed in the Other users area.

**Figure 3-15Other Users Screen When Azure AD Joined**



Enlarge Image

**Tip**

It is possible to have a hybrid deployment where Windows 10 devices are joined to both Active Directory and Azure AD. Hybrid Azure AD join allows single sign-on to on-premises and cloud-based resources.

Go to pg.

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

Application Opened

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

# Chapter Review

## 3-7a**Summary**

* User accounts are required for users to sign in to Windows 10 and use resources on that computer. Local user accounts are stored in the SAM database of each computer. You can authenticate by using local credentials or a Microsoft account.
* Windows 10 sign-in security can be enhanced by enabling secure sign-in. When secure sign-in is enabled you need to press Ctrl+Alt+Delete to sign in.
* Fast user switching allows multiple users to be signed in to a computer at the same time.
* For kiosk computers, you can configure automatic sign-in and assigned access. Both features simplify using a kiosk computer.
* Three default accounts are created upon installation of Windows 10: Administrator, Guest, and the initial user account. The Administrator account does not have a password but is disabled to be used only in Safe Mode. The initial user account is configured as an administrator.
* Groups help to simplify management by organizing users. Many built-in groups are created by default. The Administrators group and the Users group are the more commonly used.
* User accounts can be created from Settings, Control Panel, or the User and Groups MMC snap-in. The Accounts settings provide access to the current functions, such as Microsoft accounts that older tools do not recognize. The User Accounts applet in Control Panel can still be used for managing users, but it is not preferred. The Local Users and Groups MMC snap-in allows you to manage users and groups. Command-line tools for user management also are available.
* User profiles store user-specific settings. Profiles contain a number of folders and an Ntuser.dat file. New profiles are based on the default profile and are created the first time a user signs in. The default location for user profiles is C:\Users.
* You can modify profiles to make them mandatory or roaming. Mandatory profiles cannot be modified by users. Roaming profiles move with users when they sign in to different computers. Folder redirection is generally preferred to roaming user profiles. Information in the public profile is applied to all users.
* You can modify the Start menu and taskbar layout by using an XML file defined in Group Policy. You can also use Windows ICD to create a provisioning package that modifies the Start menu and taskbar layout.
* Windows 10 includes advanced authentication methods to increase security by tying authentication to a specific device. Picture password and PIN authentication can be implemented without any special hardware. Biometric authentication requires hardware devices that meet the strict requirements of Windows Hello. A security key can be used to authenticate to Windows 10 and web-based applications. You can use smart cards and virtual smart cards in a domain environment.
* In a peer-to-peer network, each computer authenticates users by using the local SAM database. User accounts and passwords are not synchronized between computers automatically.
* In a domain-based network, user authentication is controlled centrally by a domain controller. Credentials are cached at first sign-in, which ensures users can sign in even if a domain controller cannot be contacted.
* Joining computers running Windows 10 to Azure AD lets you use Azure AD as a central identity store for authentication to Windows 10. This functions in a manner similar to joining Windows 10 to an on-premises Active Directory domain.

Go to pg.

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

Application Opened

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

# Chapter Review

## 3-7b**Key Terms**

* [**Administrator**](javascript://)
* [**administrator account**](javascript://)
* [**assigned access**](javascript://)
* [**biometric authentication**](javascript://)
* [**built-in local groups**](javascript://)
* [**cached credentials**](javascript://)
* [**default profile**](javascript://)
* [**domain-based network**](javascript://)
* [**dynamic lock**](javascript://)
* [**fast user switching**](javascript://)
* [**folder redirection**](javascript://)
* [**Guest**](javascript://)
* [**initial account**](javascript://)
* [**kiosk**](javascript://)
* [**local user account**](javascript://)
* [**Local Users and Groups MMC snap-in**](javascript://)
* [**mandatory profile**](javascript://)
* [**Microsoft account**](javascript://)
* [**Ntuser.dat**](javascript://)
* [**pass-through authentication**](javascript://)
* [**peer-to-peer network**](javascript://)
* [**picture password authentication**](javascript://)
* [**PIN authentication**](javascript://)
* [**public profile**](javascript://)
* [**roaming profile**](javascript://)
* [**secure sign-in**](javascript://)

* **[Security Accounts Manager (SAM) database](javascript://)**
* [**security identifier (SID)**](javascript://)
* [**security key**](javascript://)
* [**smart card**](javascript://)
* [**standard user account**](javascript://)
* [**user account**](javascript://)
* [**User Accounts applet**](javascript://)
* [**user profile**](javascript://)
* [**virtual smart card**](javascript://)
* [**Windows Hello**](javascript://)
* [**Windows Hello for Business**](javascript://)

Go to pg.

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

Application Opened

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

# Chapter Review

## 3-7c**Review Questions**

1. Local user accounts are stored in the SAM database. True or False?
2. Each user account is assigned a(n)  to ensure that security is kept intact if the account is renamed.
3. How do you reset the password for a Microsoft account?
   1. A local administrator can reset the password in the User Accounts applet in Control Panel.
   2. The user needs to reset the password on the Microsoft website for Microsoft accounts.
   3. Use a password reset disk.
   4. A local administrator can reset the password in Accounts settings.
   5. A local administrator can reset the password by using the Local Users and Groups MMC snap-in.
4. Which sign-in method requires users to press Ctrl+Alt+Delete before signing in?
   1. assigned access
   2. secure sign-in
   3. fast user switching
   4. automatic sign-in
5. Which sign-in method allows multiple users to have applications running on the computer at the same time?
   1. assigned access
   2. secure sign-in
   3. fast user switching
   4. automatic sign-in
6. Which characters are not allowed in user account names? (Choose all that apply.)
   1. \
   2. 1
   3. $
   4. \*
   5. !
7. Because user names are case sensitive, you can use capitalization to ensure that they are unique. True or False?
8. Which characteristics apply to the Administrator account? (Choose all that apply.)
   1. It has a blank password by default.
   2. It cannot be deleted.
   3. It cannot be renamed.
   4. It is visible on the sign-in screen.
   5. It can be locked out.
9. Which security feature can you enable to lock computers that are left unattended?
   1. security key
   2. dynamic lock
   3. secure sign-in
   4. fast user switching
   5. Windows Hello
10. Because the initial user account created during installation is a member of the Administrators group, it has all the characteristics of the Administrator account. True or False?
11. Standard users are members of which built-in local group?
    1. Administrators
    2. Guests
    3. Remote Desktop Users
    4. Users
12. Which user management tool is required to assign a logon script to a user?
    1. User Accounts in Control Panel
    2. Local Users and Groups MMC snap-in
    3. Advanced User Accounts applet
    4. Advanced Users and Groups MMC snap-in
13. Which file in a profile contains user-specific registry settings?
    1. AppData
    2. Ntuser.dat
    3. Ntuser.man
    4. System.dat
    5. Local Settings
14. Which profile is copied to create a profile for new user accounts?
    1. Default User
    2. Public
    3. Blank
    4. Default
    5. New
15. A roaming profile is located on a network server. True or False?
16. Which profile is merged into each user profile when the user is signed in?
    1. Default User
    2. Public
    3. Blank
    4. Default
    5. New
17. After you set a PIN for an Azure AD account on your laptop, that PIN can be used only on your laptop. True or False?
18. Which authentication method requires the computer to be joined to either a domain or Azure AD?
    1. Microsoft account
    2. domain account
    3. Windows Hello
    4. Windows Hello for Business
    5. security key
19. In a domain-based network, each server authenticates users by using the SAM database. True or False?
20. The  group becomes a member of the Administrators local group when a Windows 10 computer joins a domain.

Go to pg.

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