- 1. 1. 5. Managing user accounts, passwords, and credentials -

Before you can begin working with a device running Microsoft Windows 10, you must sign in with the credentials for a user account that is authorized to use that device.

User accounts are an essential cornerstone of Windows security and are key to providing a personalized user experience.

As an administrator, you determine which user accounts are allowed to sign in to a specific device.

In addition, you can configure user accounts on a Windows 10 device to accomplish the following goals:

- Control access to files and other resources.
- Audit system events, such as sign-ins and the use of files and other resources.
- Sync files and settings between different computers when signing in with the same account.
- Require each user to provide additional proof of their identity when signing in for the first time on a new device.

The credentials associated with a user account consist of a user name and password that serve as identification and, in theory, ensure that no one can use the computer or view files, email messages, and other personal data associated with a user account unless they're authorized to do so.

If your computer is in a seemingly secure location where only people you trust have physical access to it, you might be tempted to allow family members or co-workers to share your user account.

We strongly caution against using that configuration and instead recommend that you create a user account for each person who uses the computer.

Doing so allows each account to access its own user profile and store personal files and user preferences within that profile.

With fast user switching, a feature described in this chapter, you can switch between user accounts with only a few clicks.

Working with user accounts

When you install Windows 10 on a new computer, the setup program creates a profile for one user account, which is an administrator account.

An administrator account is one that has full control over the computer.

Depending on what type of account you select during setup, that initial account can be a Microsoft account, an Azure Active Directory (Azure AD) account, or a local user account.

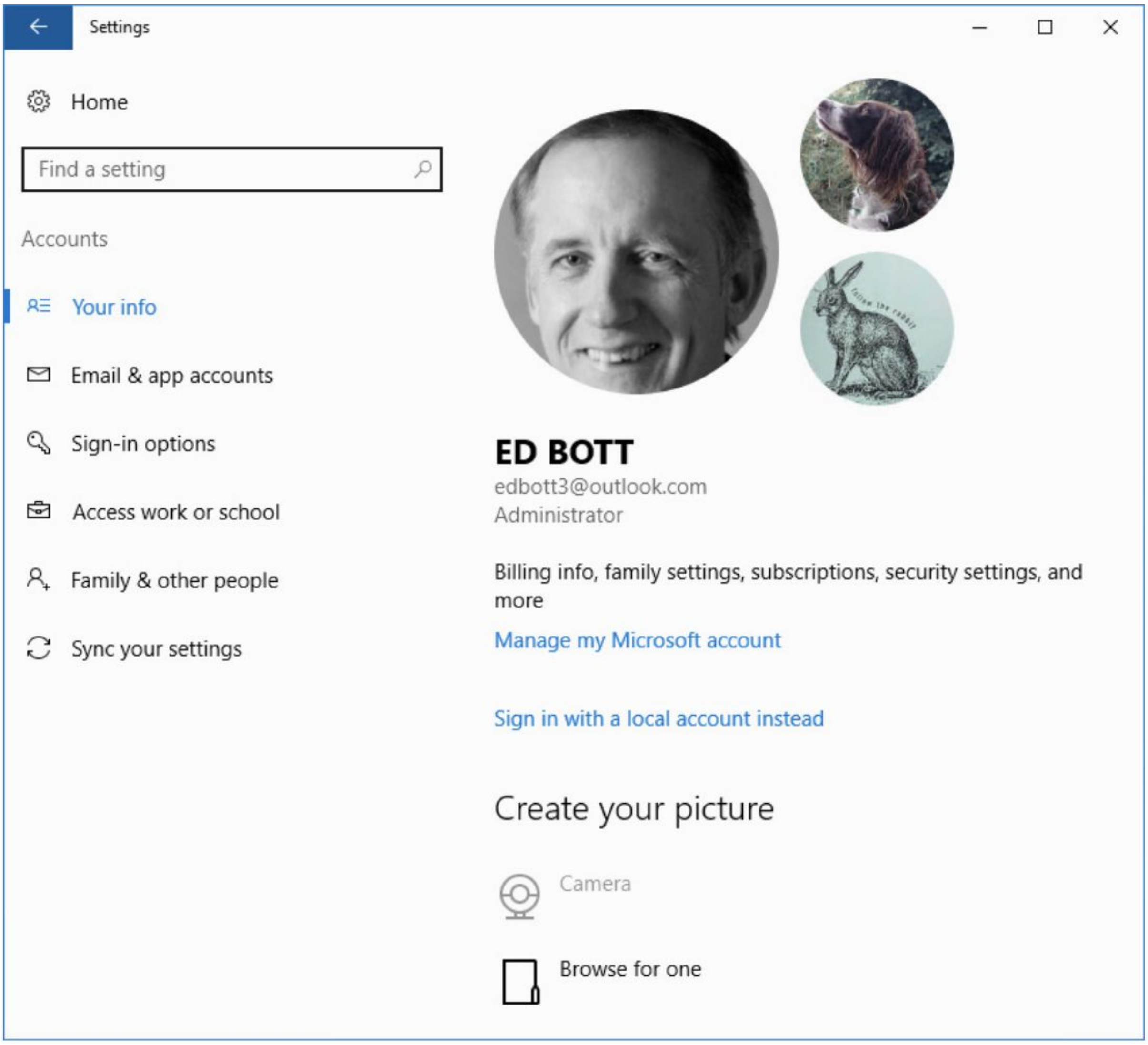
A fourth user account type—an account on a local Active Directory domain—is available only on a managed network after this initial account is created and you join the machine to the domain.

If you upgrade to Windows 10 from Windows 7 or Windows 8.1 and you had local accounts set up in your previous operating system, Windows migrates those accounts to your Windows 10 installation.

These migrated accounts maintain their group memberships and passwords.

After signing in for the first time, you can go to Settings > Accounts to create new user accounts and make routine changes to existing accounts.

The Your Info page provides an overview of your account, similar to the one shown in the next figure:



ED BOTT
edbott3@outlook.com
Administrator

Billing info, family settings, subscriptions, security settings, and more

Manage my Microsoft account
Sign in with a local account instead

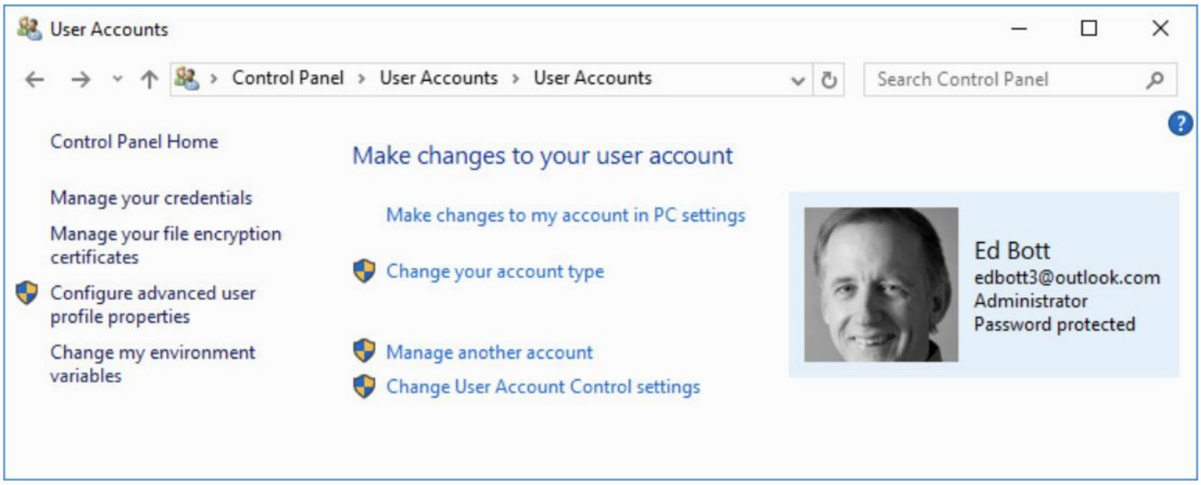
Create your picture

You'll find different options and settings in Accounts depending on the type of account you use (Microsoft account or local account), whether your account is a member of the Administrators group, and—if your computer is joined to a domain—group policies in effect.

On a computer joined to an Active Directory domain, all management of user accounts beyond basic tasks such as selecting a picture is normally handled at the domain level.

You'll find some account-related settings under the User Accounts heading in the old-school Control Panel, which is shown in the following figure.

Several of these settings duplicate functions that are available in Settings > Accounts.



User Accounts

Control Panel > User Accounts > User Accounts

Search Control Panel

Control Panel Home

Manage your credentials

Manage your file encryption certificates

Configure advanced user profile properties

Change my environment variables

Make changes to your user account

Make changes to my account in PC settings

Change your account type

Manage another account

Change User Account Control settings

Ed Bott
edbott3@outlook.com
Administrator
Password protected

You can add a new account only from the Accounts page in Settings.

You can remove an account or change its type from that location or its Control Panel counterpart.

All the esoteric options along the left side of the User Accounts page, as well as the Change User Account Control Settings option, are available only in Control Panel.

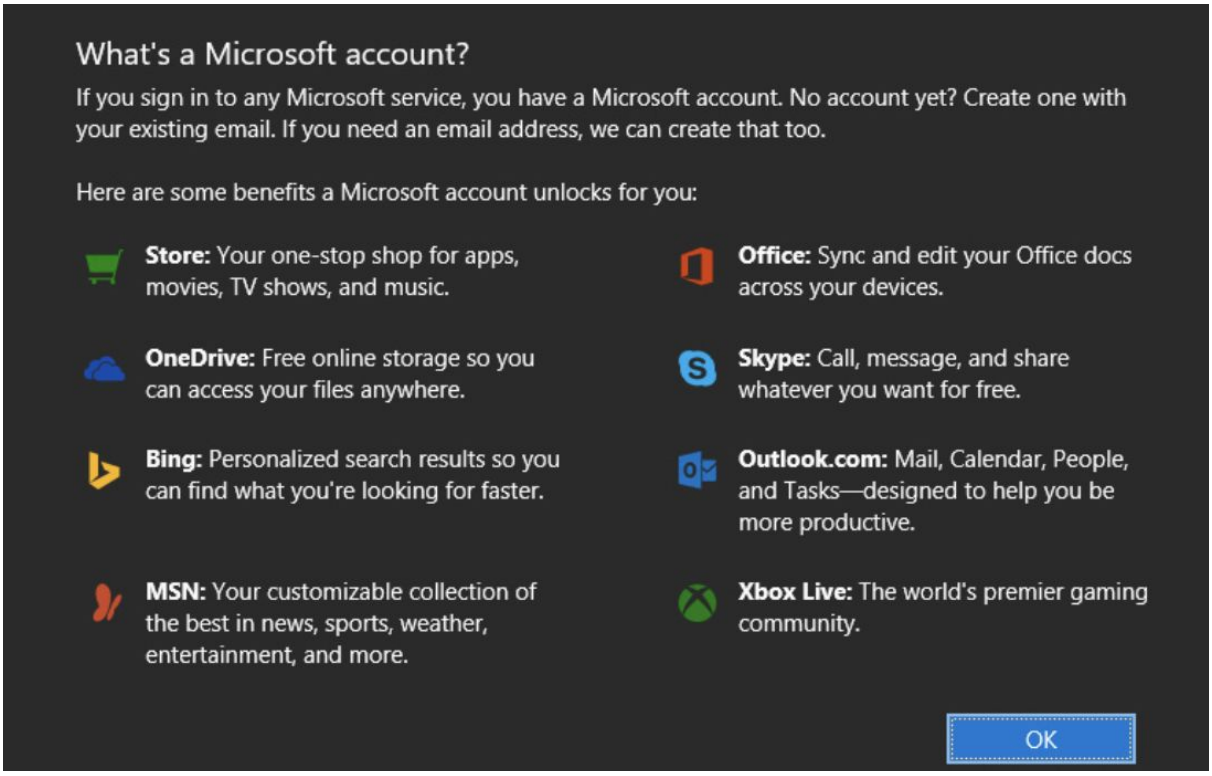
Choosing an account type

As we mentioned earlier, Windows 10 supports four different account types.

1. Microsoft account

When you go through the Out of Box Experience on a new PC (or a fresh installation of Windows 10), the default options strongly encourage you to sign in using a Microsoft account.

If you click Learn More during that initial setup process, you see this explanation:



What's a Microsoft account?

If you sign in to any Microsoft service, you have a Microsoft account. No account yet? Create one with your existing email. If you need an email address, we can create that too.

Here are some benefits a Microsoft account unlocks for you:

Store: Your one-stop shop for apps, movies, TV shows, and music.

Office: Sync and edit your Office docs across your devices.

OneDrive: Free online storage so you can access your files anywhere.

Skype: Call, message, and share whatever you want for free.

Bing: Personalized search results so you can find what you're looking for faster.

Outlook.com: Mail, Calendar, People, and Tasks—designed to help you be more productive.

MSN: Your customizable collection of the best in news, sports, weather, entertainment, and more.

Xbox Live: The world's premier gaming community.

You've probably used Microsoft accounts for years, perhaps without even knowing it.

If you've signed up for a Microsoft service, including Outlook.com (or its predecessor, Hotmail), Office 365 Home or Personal, or Xbox Live, you already have a Microsoft account.

Every email address that ends with msn.com, hotmail.com, live.com, or outlook.com is, by definition, a Microsoft account.

During setup, you can enter the email address associated with an existing Microsoft account, or you can create a new email address in the outlook.com domain.

However, you do not need a Microsoft address to create a Microsoft account; you can set up a Microsoft account using an existing email address from any domain and any email provider.

The biggest advantage of signing in with a Microsoft account is synchronizing PC settings between multiple computers.

If you use more than one PC—say, a desktop PC at work, a different desktop at home, a laptop for travel, and a tablet around the house—signing in with a Microsoft account lets you effortlessly use the same desktop colors and background, stored passwords, browser favorites and history, account picture, accessibility configuration, and so on.

The synchronization happens automatically and nearly instantly.

Some features in Windows 10 require the use of a Microsoft account.

The best example is Cortana, the personal assistant included as part of Windows 10; Cortana's services are available only when you sign in with a Microsoft account.

It’s possible to use OneDrive and other universal apps that depend on a Microsoft account even if you sign in to Windows with a local account.

However, you must sign in to each app individually, and some features might be unavailable or less convenient to use.

2. Local account

A local account is one that stores its sign-in credentials and other account data on your PC.

A local account works only on a single computer.

It doesn’t require an email address as the user name, nor does it communicate with an external server to verify credentials.

This type of account was the standard in Windows for decades.

Beginning with Windows 8 and continuing in Windows 10, Microsoft recommends the use of a Microsoft account rather than a local user account for PCs that aren’t part of a managed business network.

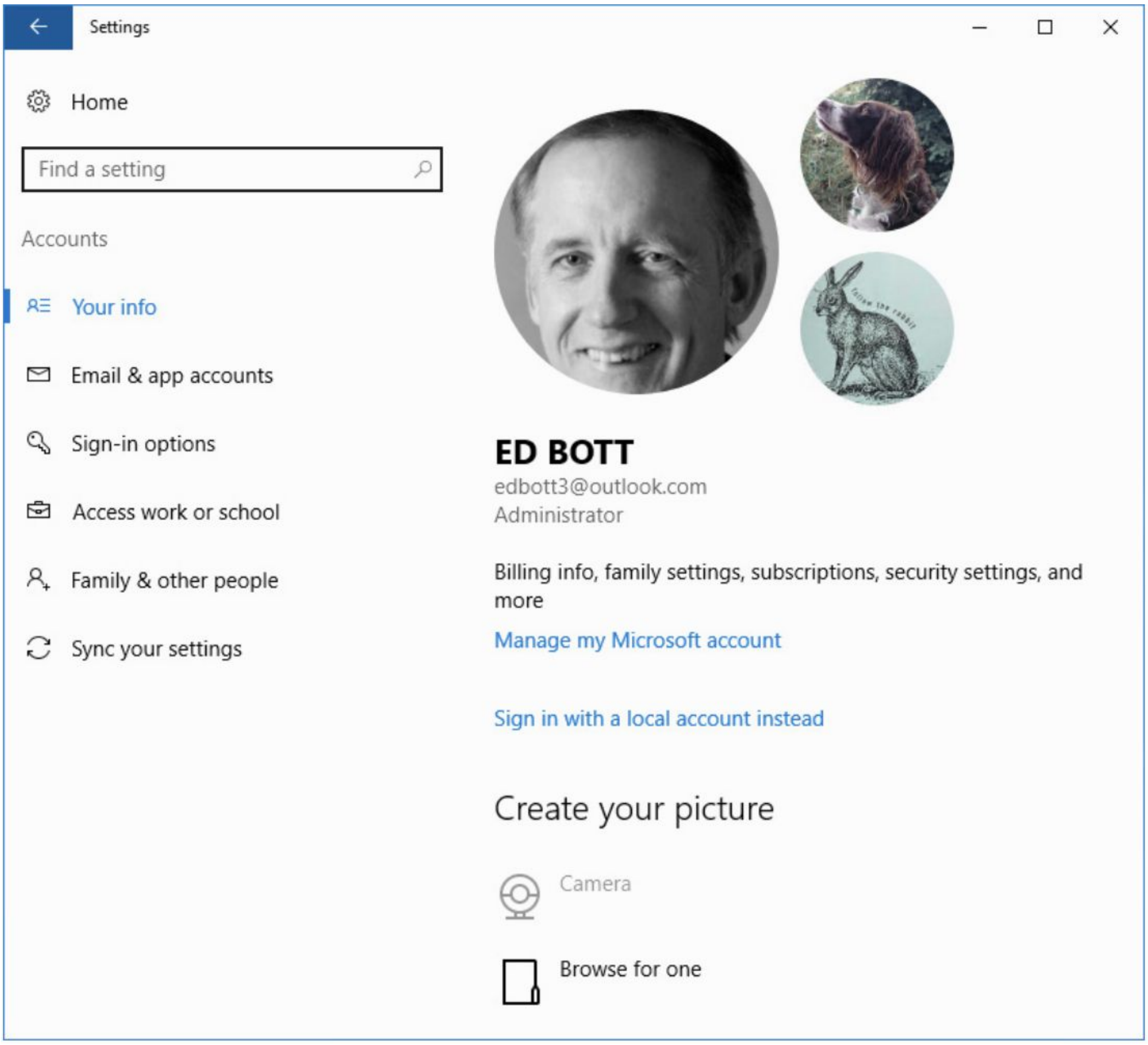
But using a Microsoft account is not a requirement; local accounts are still fully supported.

In addition, some folks have privacy and data security concerns about storing personal information on the servers of a large corporation, whether it is Microsoft, Google, Apple, Amazon, or others.

Signing in with a local account minimizes the amount of information your PC exchanges with Microsoft’s servers.

You can switch between using a Microsoft account and a local account by going to Settings, Accounts.

On the Your Info page, click "Sign In With A Local Account Instead":



ED BOTT
edbott3@outlook.com
Administrator

Billing info, family settings, subscriptions, security settings, and more

Manage my Microsoft account

Sign in with a local account instead

Create your picture

Windows leads you through a few simple steps to create a local account, which you'll then use for signing in.

If you're currently signed in using a local account, the link on that page reads "Sign In With A Microsoft Account Instead".

As part of making the switch, you need to enter your local password one more time.

A few screens later, you're connected to an existing Microsoft account or a new one you create.

From that time forward, you sign in using your Microsoft account.

Switching from a local account to a Microsoft account preserves your digital license details online, making activation easier if you need to reinstall Windows later.

3. Azure Active Directory account

The third type of account, available during initial setup of Windows 10 Pro, Enterprise, or Education, is a work or school account using Azure Active Directory.

Azure AD offers some of the advantages of a Microsoft account, including support for two-factor authentication and single sign-on to online services, balanced by the capability of network administrators to impose restrictions using management software.

These accounts are most common in medium-size and large businesses and schools.

Organizations that subscribe to Microsoft's business-focused online services—including Business or Enterprise editions of Office 365, Microsoft Intune, and Microsoft Dynamics CRM Online—automatically have Azure Active Directory services as part of their subscription.

Every user account in that service automatically has a corresponding Azure AD directory entry.

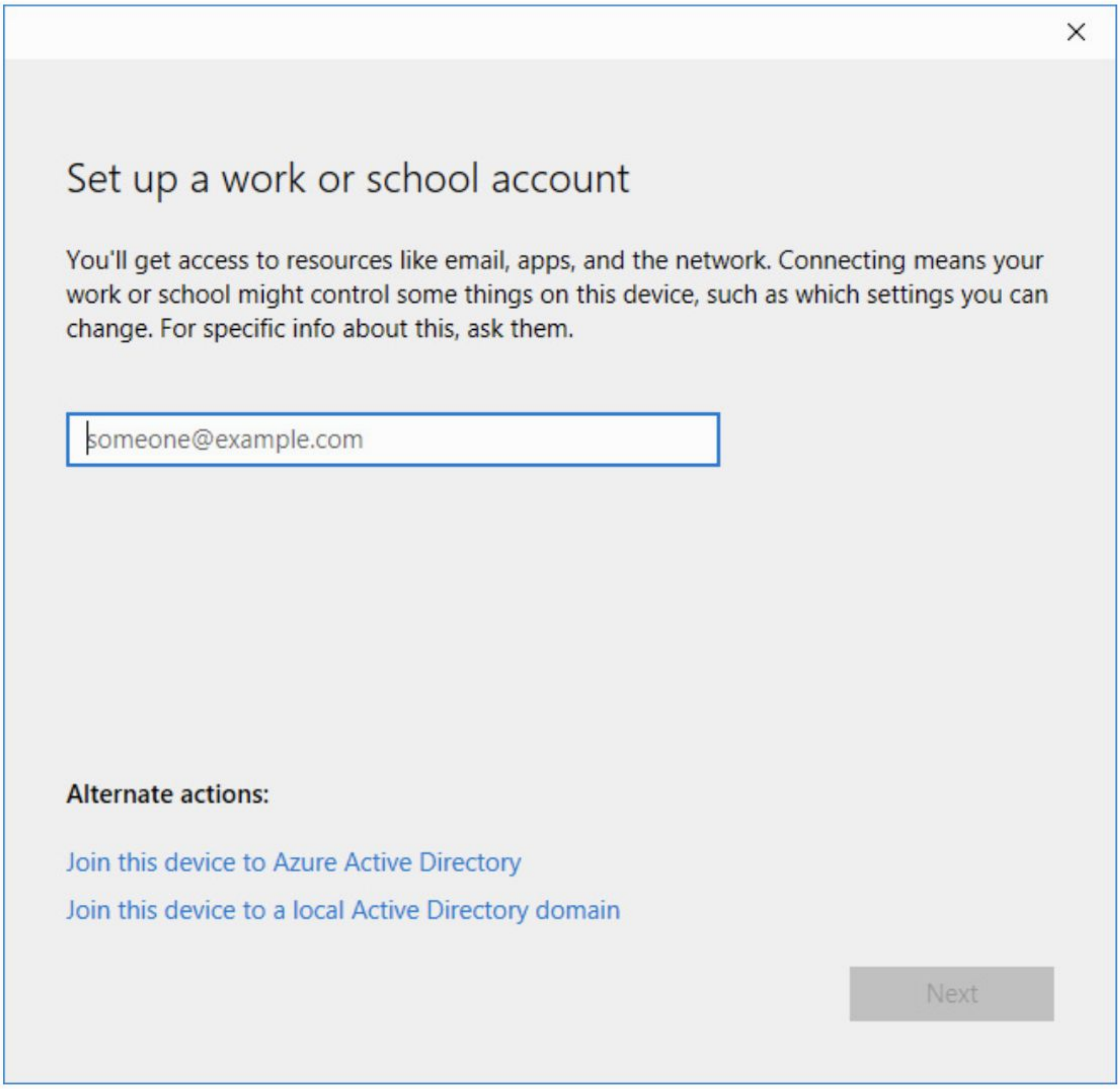
You can connect an Azure AD account to a new Windows 10 installation during the initial setup of Windows 10.

You can also connect a Windows 10 device to Azure AD after it has been set up using a local account or a Microsoft account.

To accomplish this task, go to Settings > Accounts > Access Work Or School, and then click Connect.

If you want to continue using your Microsoft account or your local account and only want to connect your Azure AD account for easier access to Office 365 and other business services, enter the email address associated with that account and follow the prompts.

If you want to be able to sign in to Windows using your Azure AD account, don't enter an email address in the Set Up A Work Or School Account dialog box; instead, click the small Join This Device To Azure Active Directory link at the bottom of that dialog box, as shown here:

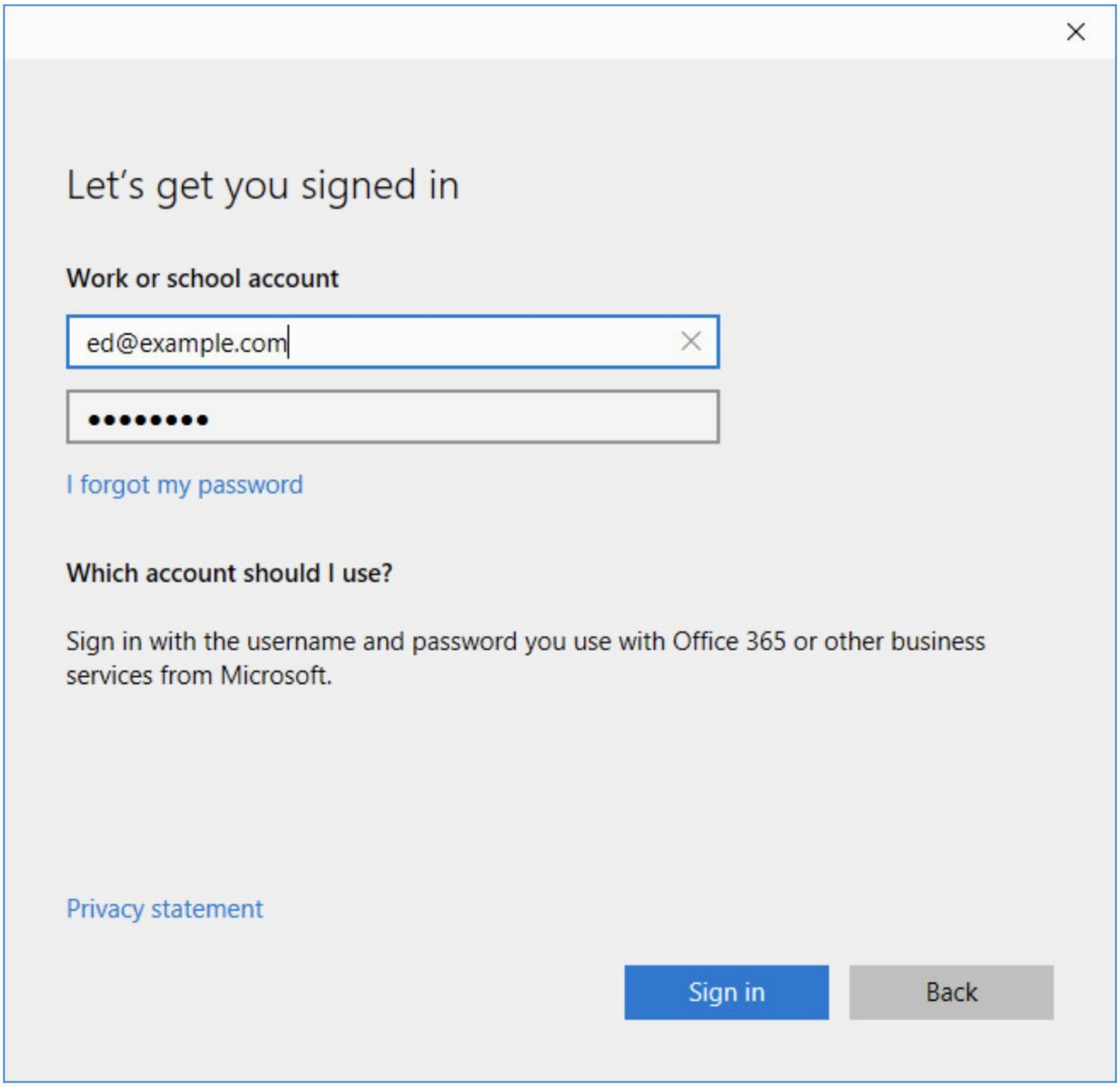


Set up a work or school account

You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

someone@example.com
Alternate actions:
Join this device to Azure Active Directory
Join this device to a local Active Directory domain
Next

That option opens the dialog box shown in the next figure:



Let's get you signed in

Work or school account

ed@example.com

••••••••

Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.

After you sign in using your Azure AD credentials, you have one final chance to confirm that you want to sign in with your organization's credentials and allow administrators to apply policies to your device.

After connecting a Windows 10 PC to Azure AD, you can view and edit your user profile by going to Settings > Accounts > Your Info and clicking Manage My Account.

You can use the options on the Profile page to request a password reset and manage multifactor authentication settings.

The Applications tab includes any apps that have been set up by your administrator for single sign-on.

4. Active Directory domain account

In organizations with Windows domains running Active Directory services, administrators can join a PC to the domain, creating a domain machine account.

This option is available only with Windows 10 Pro, Enterprise, or Education editions.

After this step is complete, any user with a domain user account can sign in to the PC and access local and domain-based resources.

Changing account settings

With options in Settings and Control Panel, you can make changes to your own account or another user's account.

To change your own account, go to Settings > Accounts > Your Info.

Here, you can change your account picture, either by browsing for a picture file or by using your computer's built-in camera to take a picture.

If you sign in with a Microsoft account, the Manage My Microsoft Account link opens your default web browser and loads your account page at https://account.microsoft.com .

On that page, you can change your password or edit the name associated with your Microsoft account.

Click other links along the top of the page to review your subscriptions and Store purchases, change your payment options, and get information about other devices associated with your Microsoft account.

You can also set security and privacy options.

If you have added one or more users to your computer, you (as a computer administrator) can make changes to the account of each of those users.

To change a user's account type, go to Settings > Accounts > Family & Other People.

Click the name of the account you want to change, and click Change Account Type.

Your choices are Standard User or Administrator.

If the person signs in with a Microsoft account, there are no other changes you can make.

You can't make changes to someone else's Microsoft account at https://account.microsoft.com .

For users who sign in with a local user account, you can make a few additional changes, but you must start from User Accounts in Control Panel.

Click Manage Another Account, and then click the name of the account you want to change.

You can make the following changes:

- Account Name. The name you're changing here is the full name, which is the one that appears on the sign-in screen, on the Start menu, and in User Accounts.
- Password. You can create a password and store a hint that provides a reminder for a forgotten password. If the account is already password protected, you can use User Accounts to change the password or remove the password.
- Account Type. Your choices here are the same as in Settings > Accounts: Administrator (which adds the account to the Administrators group) or Standard User (which adds the account to the Users group).

If you sign in with a local user account, you can make the following additional changes to your own account (that is, the one with which you're currently signed in) by clicking links in the left pane:

- Manage Your Credentials. This link opens Credential Manager, where you can manage stored credentials that you use to access network resources and websites.
- Create A Password Reset Disk. This link, available only when you are signed in with a local account, launches the Forgotten Password Wizard, from which you can create a password reset tool on removable media.
- Manage Your File Encryption Certificates. This link opens a wizard you can use to create and manage certificates that enable the use of Encrypting File System (EFS). EFS, which is available only in Pro and Enterprise editions of Windows 10, is a method of encrypting folders and files so that they can be used only by someone who has the appropriate credentials.
- Configure Advanced User Profile Properties. This link is used to switch your profile between a local profile (one that is stored on the local computer) and a roaming profile (one that is stored on a network server in a domain environment). With a local profile, you end up with a different profile on each computer you use, whereas a roaming profile is the same regardless of which computer you use to sign in to the network. Roaming profiles require a domain network running Windows Server Active Directory services.
- Change My Environment Variables. Of interest primarily to programmers, this link opens a dialog box in which you can create and edit environment variables that are available only to your user account; in addition, you can view system environment variables, which are available to all accounts.

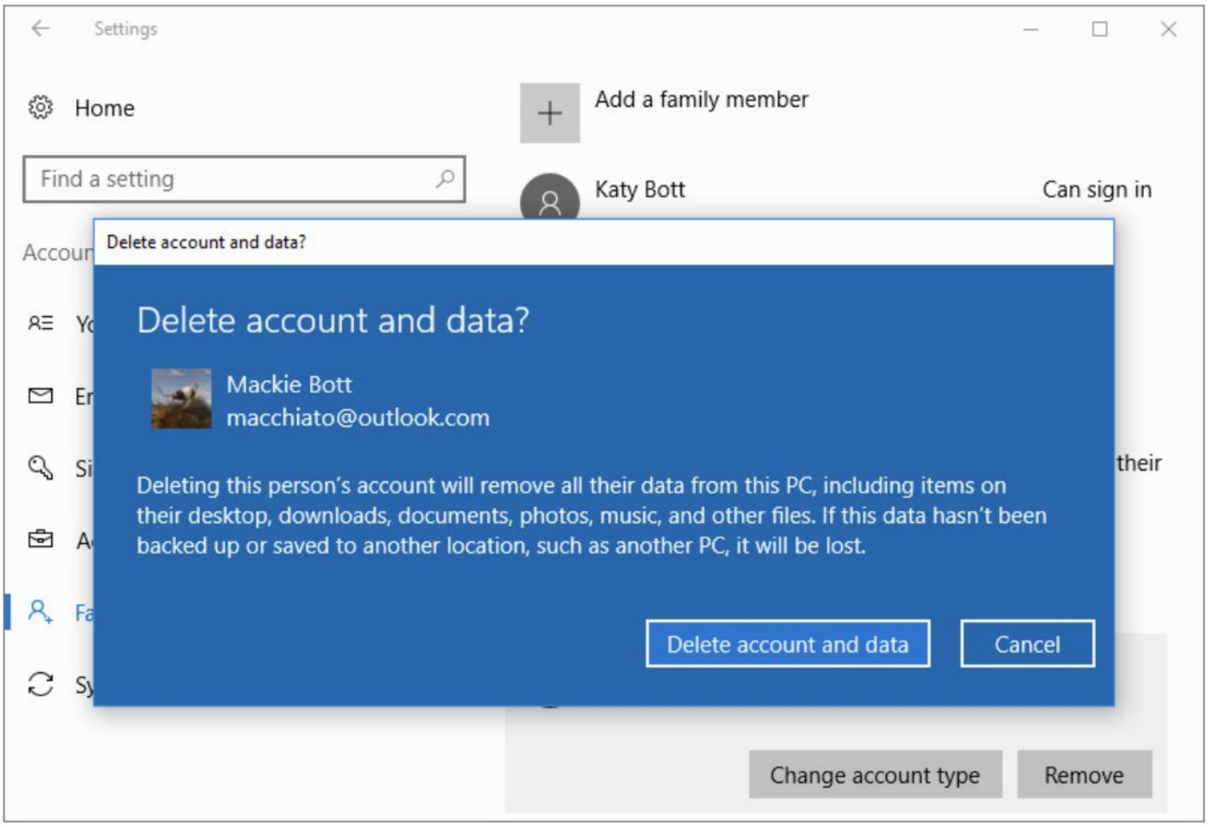
Deleting an account

As a local administrator, you can delete any local account or Microsoft account set up on a Windows 10 PC, unless that account is currently signed in.

To delete an account, go to Settings > Accounts > Family & Other People (the Family option is unavailable and this category is called simply Other People if you're signed in using an Azure AD account), and click the name of the account you want to delete.

Then click Remove.

Windows then warns about the consequences of deleting an account, as shown in the following figure:



Delete account and data?

Mackie Bott
macchiato@outlook.com

Deleting this person's account will remove all their data from this PC, including items on their desktop, downloads, documents, photos, music, and other files. If this data hasn't been backed up or saved to another location, such as another PC, it will be lost.

Before you click Delete Account And Data, be sure you have saved any local data you don't want to lose.

Windows won't let you delete the last local account on the computer, even if you signed in using the built-in account named Administrator.

This limitation helps to enforce the sound security practice of using an account other than Administrator for your everyday computing.

After you delete an account, of course, that user can no longer sign in.

Deleting an account also has another effect you should be aware of: you cannot restore access to resources that are currently shared with the user simply by re-creating the account. This includes files shared with the user and the user's encrypted files, personal certificates, and stored passwords for websites and network resources.

That's because those permissions are linked to the user's original security identifier (SID)—not the user name.

Even if you create a new account with the same name, password, and so on, it will have a new SID, which will not gain access to anything that was restricted to the original user account.

Managing the sign-in process

Users of Windows (as well as most other operating systems) are familiar with the time-honored sign-in method: at the sign-in screen, select your name (if it's not already selected) and then enter a password.

This continues to be a valid technique in Windows 10.

Windows 10 has other sign-in options that add security as well as convenience:

- You can enter a numeric PIN.
- You can trace a pattern of gestures on a picture.
- With appropriate hardware, you can use Windows Hello—a biometric sign-in method that scans your fingerprint, your face, or your iris.

These three methods each provide a form of two-factor authentication, a means of identifying yourself with multiple proofs.

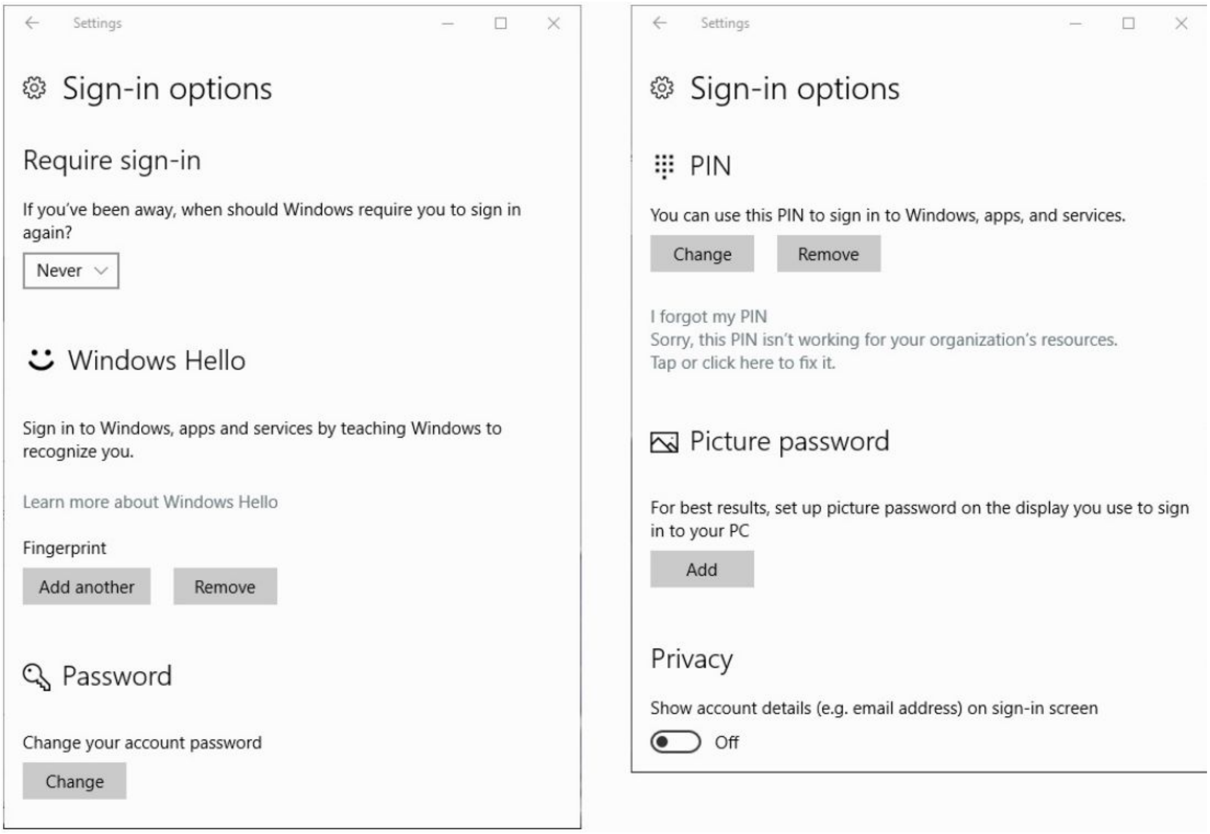
In the case of Windows sign-ins, the components include two of the following: something you know (such as a PIN or the gesture pattern), something you have (the device itself, which is registered with the Microsoft account servers), and something that's inseparable from you (your fingerprint, face, or iris).

The device you sign in on acts as an authentication component because your information (the PIN or your biometric data) is stored, in encrypted form, on the device—not on a remote server.

So, for example, if someone learns your PIN, that person can use it only on that device; he can't use it to sign in to your account on any other device.

If someone steals your computer, that person can't sign in unless she knows your PIN.

You configure each of these variations on the Sign-In Options page in Settings, Accounts, as shown in the next figure:



Settings

Sign-in options

Require sign-in

If you've been away, when should Windows require you to sign in again?

Never

Windows Hello

Sign in to Windows, apps and services by teaching Windows to recognize you.

Learn more about Windows Hello

Fingerprint

Add another | Remove

Password

Change your account password

Change

Settings

Sign-in options

PIN

You can use this PIN to sign in to Windows, apps, and services.

Change | Remove

I forgot my PIN
Sorry, this PIN isn't working for your organization's resources.
Tap or click here to fix it.

Picture password

For best results, set up picture password on the display you use to sign in to your PC

Add

Privacy

Show account details (e.g. email address) on sign-in screen

Off

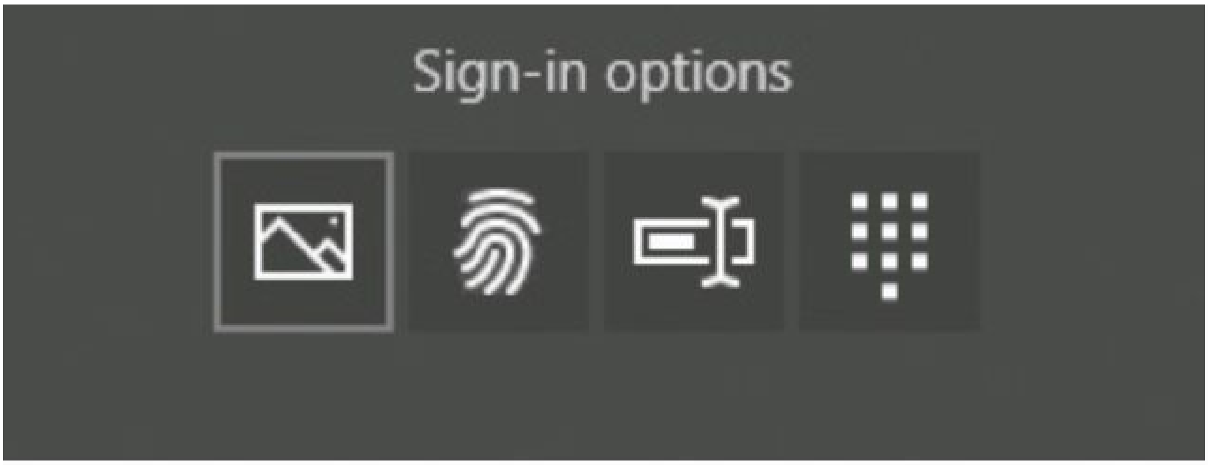
Choices on the Sign-In Options page in Settings depend on your computer's hardware.

For example, Windows Hello options are available only if you have a compatible fingerprint reader or camera.

If you set up more than one option for signing in, you can choose a method other than the default by clicking Sign-In Options on the sign-in screen.

This ability might come in handy, for example, if the fingerprint reader fails to recognize your grubby mitt.

Icons for each of the options you set up then appear as shown next; click or tap one to switch methods.



Note that these alternative sign-in options also work for some applications, including the Store.

Setting or changing a password

When you create a Microsoft account, you’re required to create a password.

Similarly, if you add a local user account to your computer, Windows 10 requires you to specify a password.

To set or change your own password, go to Settings > Accounts > Sign-in Options.

Click or tap Change under Password.

Next, you must enter your existing password to confirm your identity.

Windows then asks you to enter your new password twice.

For a local account, you must specify a password hint.

The password hint appears after you click your name on the sign-in screen and type your password incorrectly.

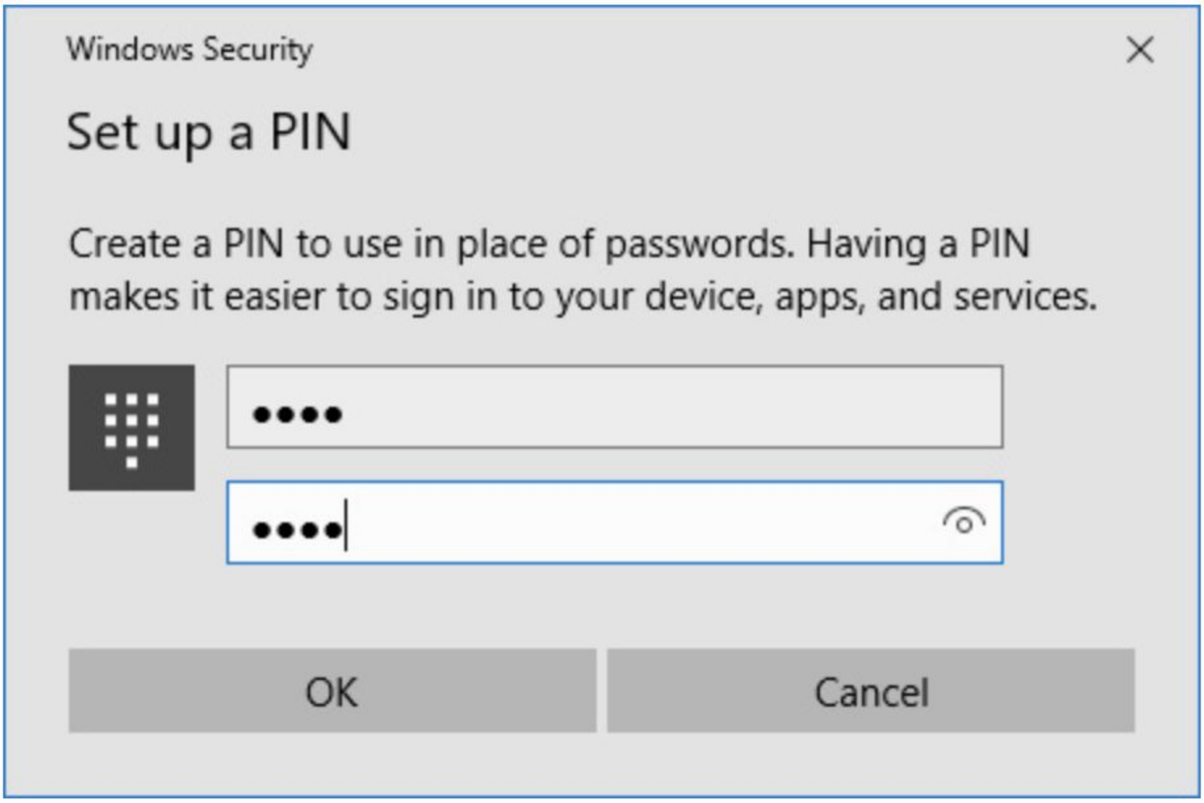
Be sure your hint is only a subtle reminder, because any user can click your name and then view the hint.

Using a PIN

To set up a PIN for signing in to your computer, go to the Sign-In Options page (shown in the next figure) and click Add under PIN.

After entering your password to confirm your identity, you enter numbers in a dialog box like the one shown here.

The minimum length is four digits (0–9 only; no letters or special characters allowed), but your PIN can be as long as you want.



Windows Security

Set up a PIN

Create a PIN to use in place of passwords. Having a PIN makes it easier to sign in to your device, apps, and services.

●●●●

●●●●

A PIN serves as a convenient alternative for signing in to Windows and verifying your identity in apps and services.

You can choose a PIN that's longer than the minimum of four characters.

To sign in using a PIN, you can type the numbers on your keyboard.

If your computer doesn't have a keyboard, a numeric pad appears on the screen so that you can tap your PIN.

If the numeric pad does not appear, tap in the PIN-entry box.

Using a picture password

With a picture password, you can sign in on a touchscreen using a combination of gestures (specifically, circles, straight lines, and taps) that you make on a picture displayed on the sign-in screen.

The easiest way to get comfortable with a picture password is to go ahead and create one.

To get started, go to Settings > Accounts > Sign-In Options.

Under Picture Password, click Add.

Verify your identity by entering your password to display an introductory screen where you can choose a picture.

You then get to select one of your own pictures to appear on the sign-in screen.

When you're satisfied with your selection, click Use This Picture.

On the next screen that appears, you specify the three gestures you'll use to sign in.

These gestures can consist of circles, straight lines, and taps.

After repeating the series of gestures to confirm your new "password," click Finish.

To sign in with a picture password, on the sign-in screen you must perform the same three gestures, in the same order, using the same locations, and in the same direction.

You don't need to be that precise; Windows allows minor variations in location.

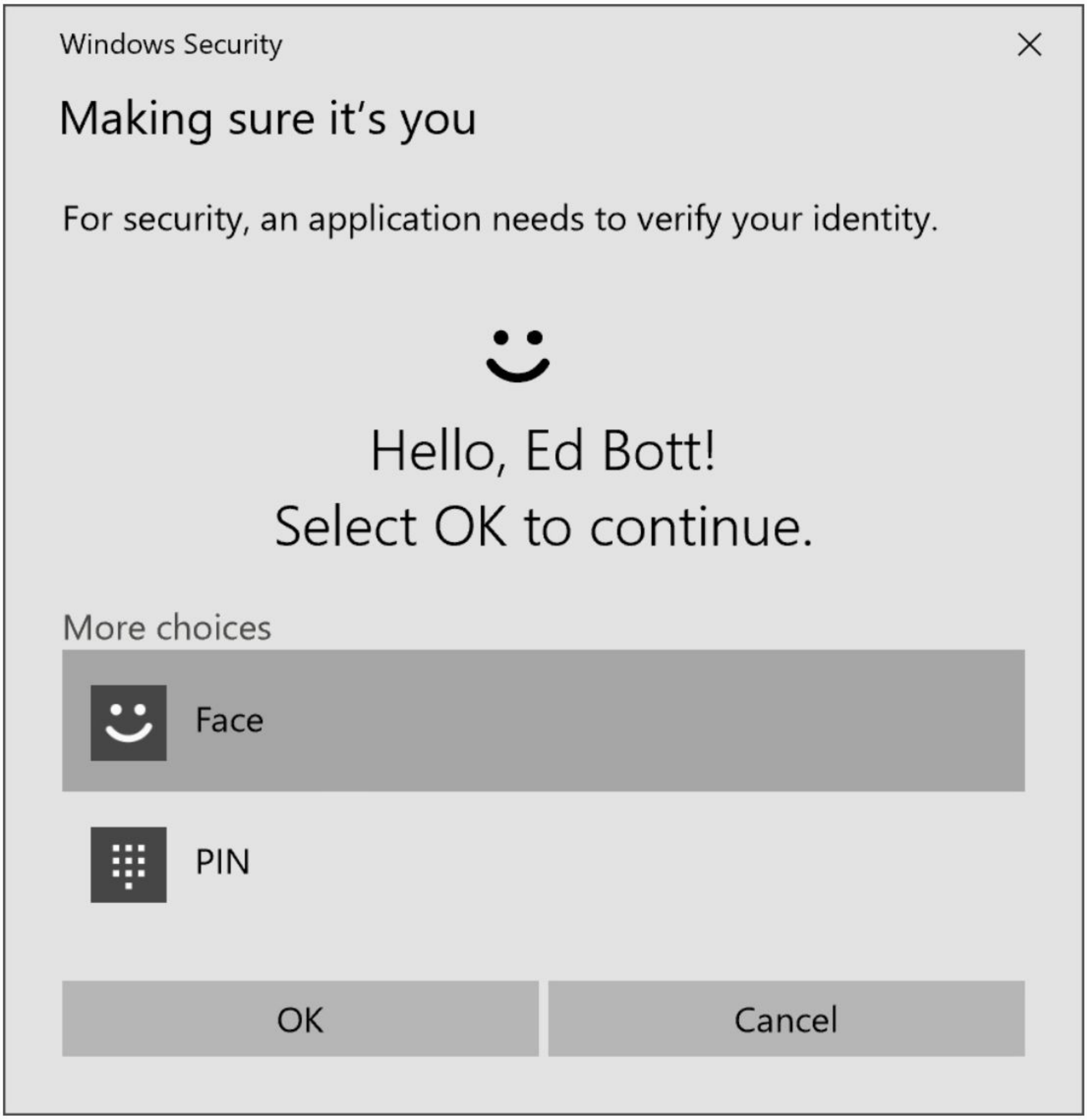
Using Windows Hello for biometric sign-ins

With the proper hardware, you can sign in simply by swiping your fingerprint or, even easier, showing your face in front of your computer's camera.

Some Windows 10 Mobile devices also support iris recognition.

You might also be asked to verify your identity when making a purchase or accessing a secure service.

When Windows Hello recognizes a fingerprint, face, or iris, it greets you by briefly displaying your name and a smiley face on the sign-in screen before going to your desktop, as shown in the following figure:



Windows Security

Making sure it's you

For security, an application needs to verify your identity.

Hello, Ed Bott!
Select OK to continue.

To use Windows Hello for biometric sign-ins on a PC, you need one of the following:

- A fingerprint reader that supports the Windows Biometric Framework; if this hardware isn't built in, you can add a USB-based fingerprint reader.
- An illuminated 3-D infrared camera such as those found on the Surface Pro, Surface Book, and other advanced devices; note that a standard webcam will not work.

You must add a PIN as described earlier in this chapter before you can use Windows Hello.

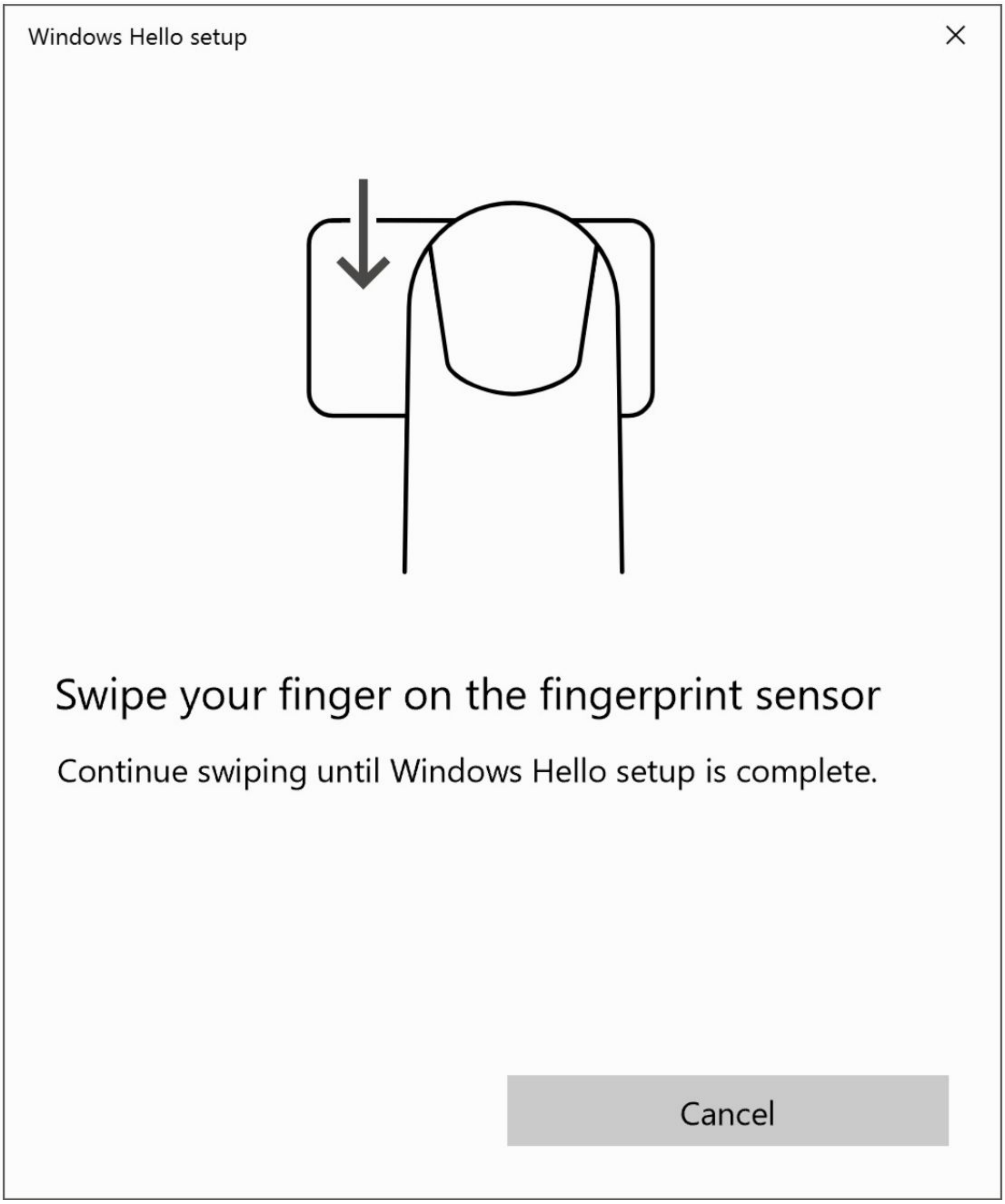
To set up Windows Hello, go to the Sign-In Options page in Settings, Accounts.

Under Windows Hello, click Set Up for the biometric device you want to use.

Windows asks you to enter your PIN to verify your identity.

After that, you need to enter your biometric data.

With face recognition, that involves staring into the camera; to set up a fingerprint reader, follow the prompts (as shown in the next figure) to swipe your fingerprint several times, until Windows Hello has recorded the data it needs.



Windows Hello setup

Swipe your finger on the fingerprint sensor

Continue swiping until Windows Hello setup is complete.

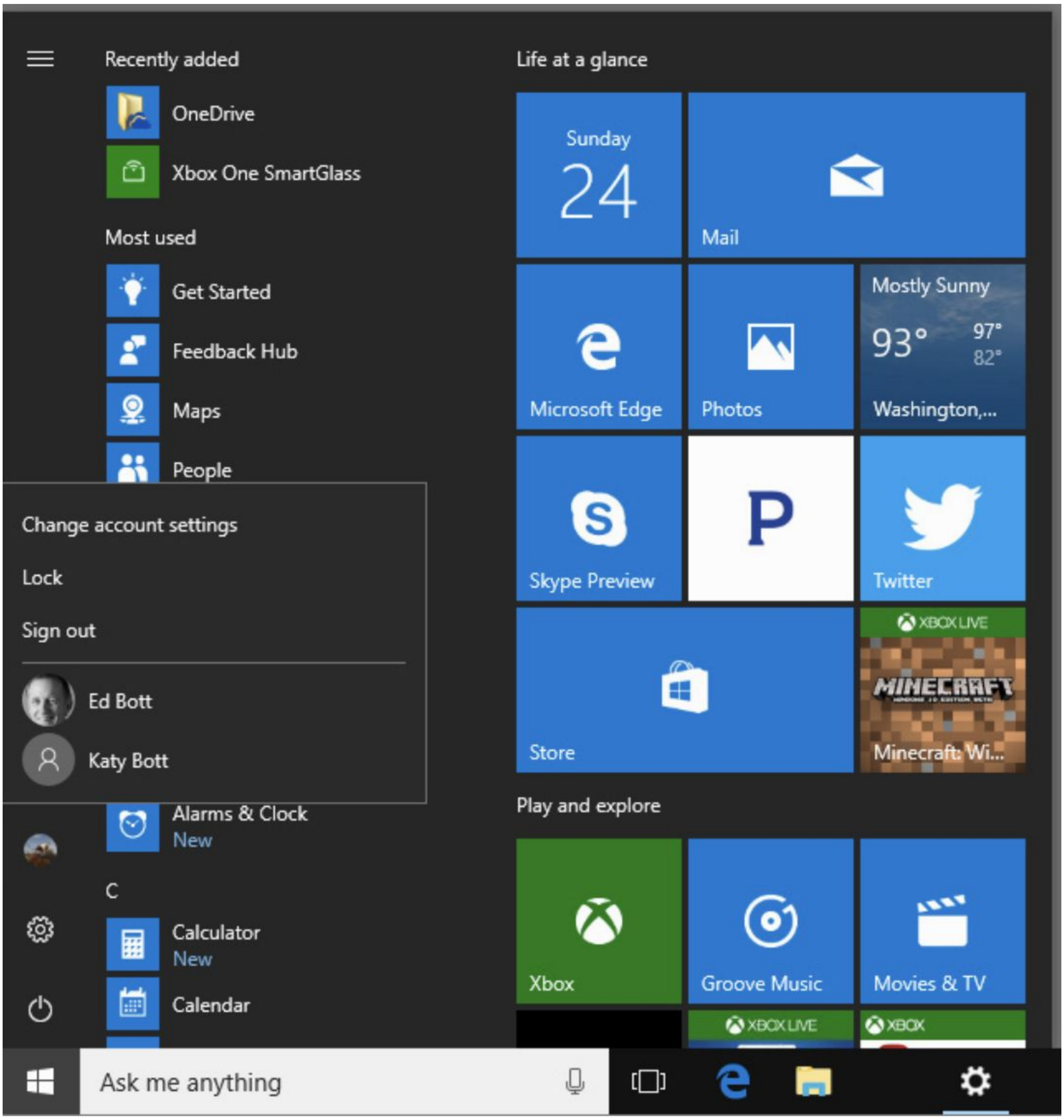
Signing out, switching accounts, or locking your computer

When you're finished using your computer, you want to be sure you don't leave it in a condition in which others can use your credentials to access your files.

To do that, you need to sign out, switch accounts, or lock your computer:

- Sign Out. With this option, all your programs close and the lock screen appears.
- Switch Account. With this option, also known as fast user switching, your programs continue to run. The sign-in screen appears, ready for the sign-in credentials of the person you select. Your account is still signed in, but only you can return to your own session, which you can do when the user you switch to chooses to sign out, switch accounts, or lock the computer.
- Lock. With this option, your programs continue to run, but the lock screen appears so that no one can see your desktop or use the computer. Only you can unlock the computer to return to your session; however, other users can sign in to their own sessions without disturbing yours.

To sign out, switch accounts, or lock your computer, open the Start menu and click or tap your name at the top of the menu to display a menu like the one shown in the following figure:



Sharing your PC with other users

Personal computers are usually just that—personal.

But there are situations in which it makes sense for a single PC to be shared by multiple users.

In those circumstances, it's prudent to configure the shared device securely.

Doing so helps to protect each user's data from inadvertent deletions and changes as well as malicious damage and theft.

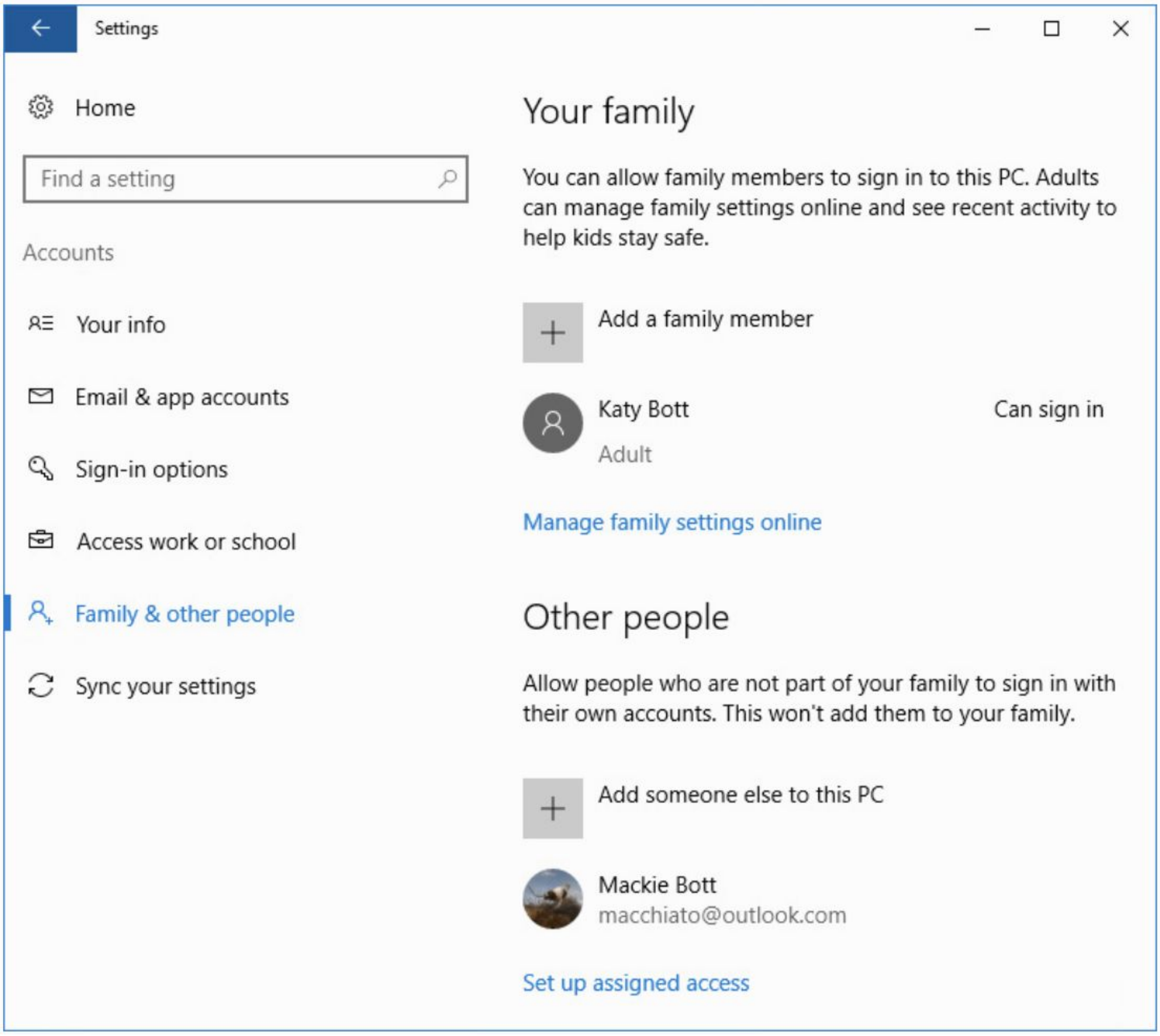
When you set up your computer, consider these suggestions:

- Control who can sign in. Create accounts only for users who need to use your computer's resources, either by signing in locally or over a network. If an account you created is no longer needed, delete or disable it.
- Use standard accounts for additional users. During setup, Windows sets up one local administrative account for installing programs, creating and managing accounts, and so on. All other accounts can and should run with standard privileges.
- Be sure that all accounts are protected by a strong password. This is especially important for administrator accounts and for other accounts whose profiles contain important or sensitive documents. Windows 10 requires a password on all local accounts.
- Restrict sign-in times. You might want to limit the computing hours for some users, especially children. The easiest way for home users to do this is by setting up family accounts.
- Restrict access to certain files. You'll want to be sure that some files are available to all users, whereas other files are available only to the person who created them. The Public folder and a user's personal folders provide a general framework for this protection. You can further refine your file-protection scheme by selectively applying permissions to varying combinations of files, folders, and users.

Adding a user to your computer

To allow another user to sign in on your computer, you as administrator must add that user's account.

Go to Settings > Accounts > Family & Other People, shown in the next figure:



Your family

You can allow family members to sign in to this PC. Adults can manage family settings online and see recent activity to help kids stay safe.

Katy Bott — Adult — Can sign in

Other people

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

Mackie Bott
macchiato@outlook.com

There, you'll find two separate sets of controls: one for adding members of your family and the second for adding "other people."

Accounts you add as family members are subject to restrictions that an adult member of the family can manage using a web-based interface.

Accounts you create under the Other People heading have all the rights and privileges associated with their account type, administrator or standard.

The Family & Other People page is available only when you sign in with an administrator account.

To add a user who's not a family member, under Other Users click Add Someone Else To This PC.

Windows then asks for the email address of the new user.

If the email address is already associated with a Microsoft account, all you need to do is click Next and the new user is ready to go.

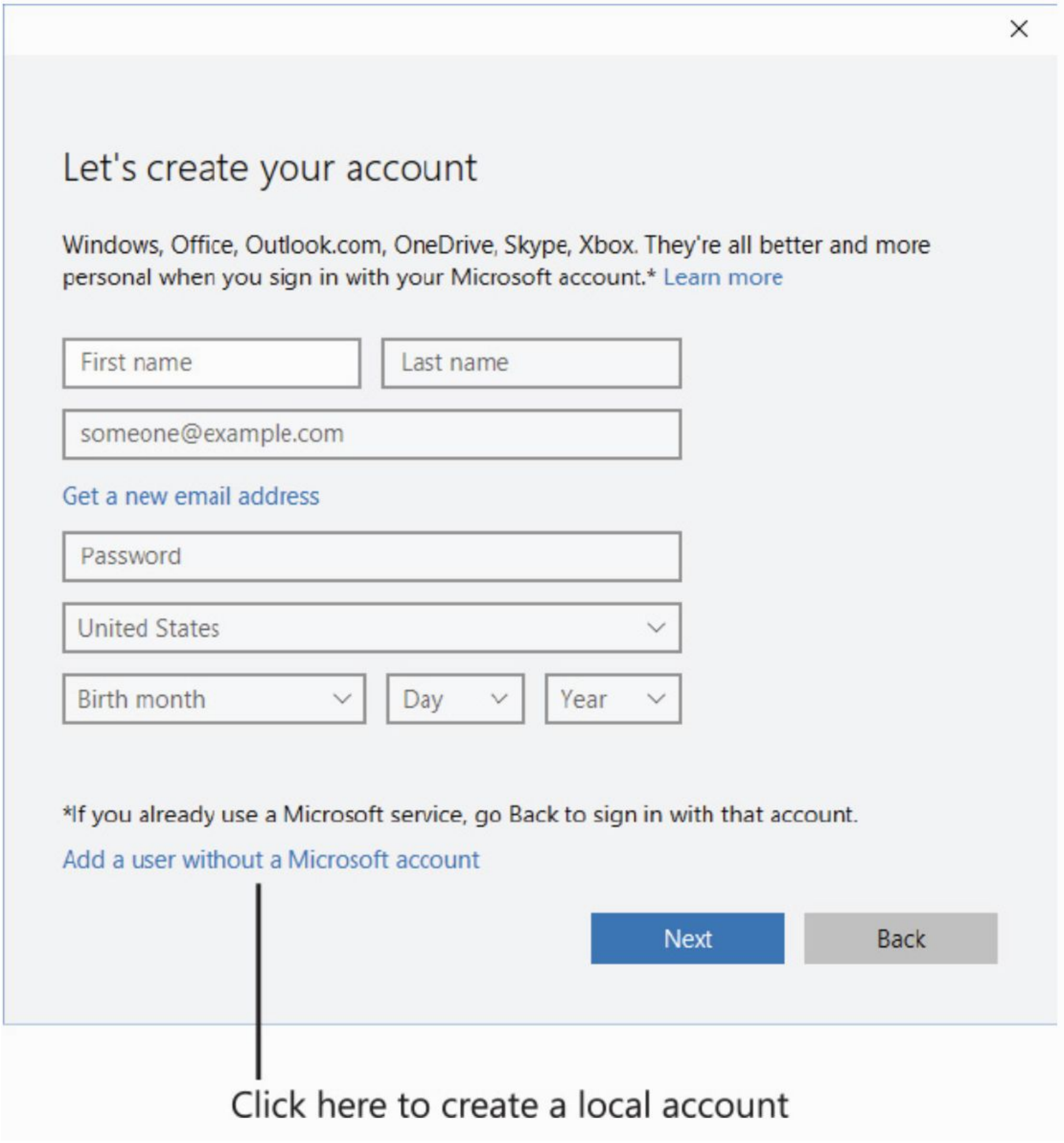
The first time the new user signs in, the computer must be connected to the internet.

If the email address you provide is not associated with a Microsoft account, Windows provides a link to sign up for a new Microsoft account.

What if you want to add a local account?

At the first screen—when Windows asks for an email address—instead click the link near the bottom: I Don’t Have This Person’s Sign-in Information.

In the next dialog box, shown in the next figure, ignore the offer to set up a new Microsoft account and instead click "Add A User Without A Microsoft Account”:



Let's create your account

Windows, Office, Outlook.com, OneDrive, Skype, Xbox. They're all better and more personal when you sign in with your Microsoft account.* Learn more

First name | Last name

someone@example.com

Get a new email address

Password

United States

Birth month | Day | Year

*If you already use a Microsoft service, go Back to sign in with that account.

Add a user without a Microsoft account

Click here to create a local account

That option opens a different dialog box where you can specify a user name and password for the new user.

If your computer has only local accounts set up, you go directly to this final dialog box, skipping the two that guide you toward a Microsoft account.

Click Next, and your work is done.

Controlling your family's computer access

Previous versions of Windows had a feature called Parental Controls (Windows Vista and Windows 7) or Family Safety (Windows 8), which allowed parents to restrict and monitor their children's computer use.

Windows 10 offers similar capabilities, but the implementation is completely different.

Those earlier versions stored their settings on your PC, but in Windows 10 family settings are now stored and managed as part of your Microsoft account.

This architectural change has some obvious benefits:

- You don't need to make settings for each child on each computer. After you add a family member on one PC, you manage the settings for each child in the cloud, and those settings apply to all the family PCs where they sign in.
- You can manage your children's computer use from any computer that's connected to the internet.

Family settings have one requirement that some will perceive as a disadvantage: Each family member must have a Microsoft account and sign in with that account.

What can you do with family settings?

- Monitor each child's computer use. You can see what your children search for on the web and which sites they visit, which apps and games they use, and how much time they're signed in to each Windows 10 computer they use.
- Block inappropriate websites. When you enable this feature, Microsoft-curated lists of sites that are blocked or explicitly allowed are used by default, but you can supplement these lists with sites you want to always block or always allow.
- Control each child's use of apps and games. Based on age ratings, you can limit the apps and games a child can download and purchase. You can also block specific apps and games from running.
- Set spending limits for Store purchases. You can add money to a child's account and remove other purchase options.
- Restrict when your children can use the computer, and for how long.

You can add a family member using the online management interface or from within Windows 10; go to Settings > Accounts > Family & Other People, and click Add A Family Member.

Windows asks whether you want to add an account for an adult or a child; the difference is that an adult can manage family settings, whereas a child is controlled by family settings.

You then enter the family member's email address; if a Microsoft account is not associated with that address, Windows gathers the needed information to set one up.

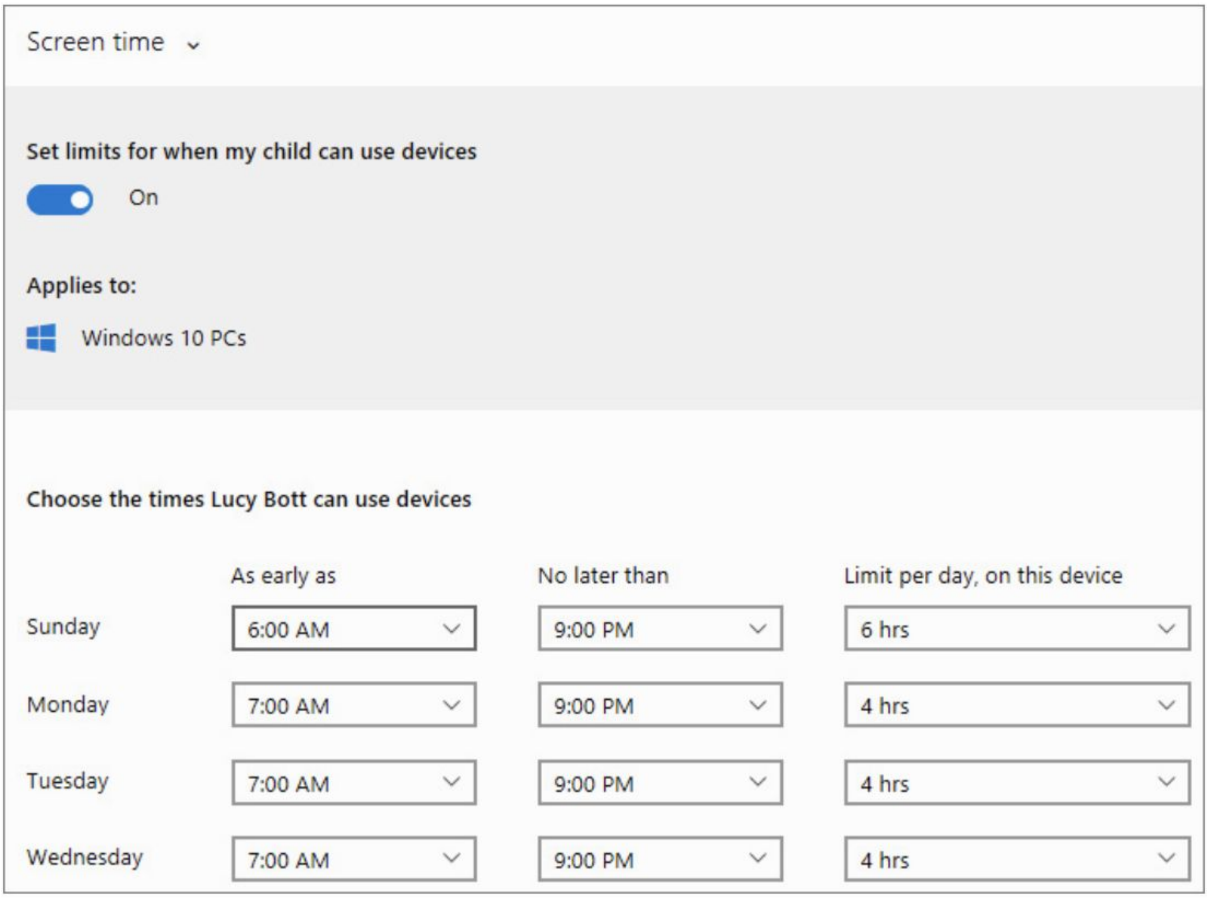
Because all family settings are managed online using Microsoft accounts, there is no option to use a local account.

If you don't see the Family & Other People page, confirm that you're signed in with a Microsoft account and that your account type is administrator.

All other management tasks occur online.

Click the Manage Family Settings Online link under the Your Family heading or visit https://account.microsoft.com/family to get started.

The following figure shows a portion of the interface for setting up both daily limits and the times during which a child can use a Windows 10 PC:



Screen time

Set limits for when my child can use devices

On

Applies to:

Windows 10 PCs

Choose the times Lucy Bott can use devices

	As early as	No later than	Limit per day, on this device
Sunday	6:00 AM	9:00 PM	6 hrs
Monday	7:00 AM	9:00 PM	4 hrs
Tuesday	7:00 AM	9:00 PM	4 hrs
Wednesday	7:00 AM	9:00 PM	4 hrs

"After you select a Microsoft account for the new family member, Microsoft Family sends an email invitation to that person.

If you use the web-based interface to add a child's account, you can sign in on the child's behalf using his credentials.

A new family member can sign in to your computer right away, but family settings take effect only after that family member opens the email message and clicks the Accept Invitation button.

What happened to the Administrator account?

Every computer running Windows has a special account named Administrator.

In versions of Windows before Windows 7, Administrator was the primary account for managing the computer.

Like other administrator accounts, the Administrator account has full rights over the entire computer.

But in Windows 10, the Administrator account is disabled by default.

In Windows 10, there's seldom a need to use the Administrator account instead of another administrator account.

The Administrator account runs with full administrative privileges at all times and never needs your consent for elevation.

For this reason, of course, it's rather risky.

Any application that runs as Administrator has full control of the computer—which means applications written by malicious or incompetent programmers can do significant damage to your system.

And the Guest account?

Historically, the built-in Guest account provided a way to offer limited access to occasional users.

Not so in Windows 10.

Although this account still exists, it's disabled by default, and the supported tools for enabling it (the Local Users And Groups console, for example) do not work as expected.

In our experience, trying to trick Windows 10 into enabling this capability is almost certain to end in frustration.

In the cloud-centric world of Windows 10, the Guest account no longer works as it used to and enabling it can cause a variety of problems.

A better solution (if your guests don't have their own device that can connect to your wireless network) is to set up a standard account for guest use.

Managing users and groups with the "lusrmgr.msc" console

Go to the Windows search box, write "lusrmgr.msc" and open the "Local Users and Groups" management console.

From here, you can manage local users and groups: creating, deleting, modifying, etc.

- Vocabulary -

- to sign in / to log in: loguearse / ingresar en un sistema.
- to sign up: registrarse (sólo la primera vez).
- to lock: bloquear.
- to sign out: cerrar sesión.
- theft: robo.
- thief / robber: ladrón.
- thieves: ladrones.
- to thieve: robar.
- to steal: robar.
- whose: cuyo/s.
- seldom: raramente / en pocas ocasiones.
- instead: en lugar de / en vez de.

- Exercises - 1. 1. 5. Managing user accounts, passwords, and credentials

Open the following Google Document that you have created in a previous sub-unit:

"1. 1. Getting started with Windows 10 - Apellidos, Nombre"

being "Apellidos, Nombre" your Last Name and Name.

Inside this Google Document you are going to copy and answer all the "Exercises" of this sub-unit:

1. With your local account, create a PIN, sign out from Windows, and login using the PIN.
2. With your local account, create a Picture Password, sign out from Windows, and login using the Picture Password.
3. Create a new Microsoft Office account "A" (in the "@iesdoctorbalmis.com" domain) using this link -> https://www.microsoft.com/es-es/education/products/office/default.aspx
4. Use that new Microsoft Office account “A” (in the "@iesdoctorbalmis.com" domain) in the computer "A" (your computer). To do so, go to Settings -> Accounts -> Your info -> Sign in with your Microsoft account instead -> Click on "No account? Create a new one" -> Enter the new Microsoft Office account "A" (in the "@iesdoctorbalmis.com" domain), the password and the date birth that you have already used when you registered this account on the web.
5. Enter your Windows password ("alumno").
6. Create a PIN.
7. This will be your default user in Windows 10 from now on. Now the local user "alumno" does not exist, and the current logged in user is a your @iesdoctorbalmis Microsoft account.
8. Create a local account (“Administrator” type) named “Fernando” on “Other people” -> I don't have this person's sign-in information -> Add a user without a Microsoft account.
9. Login into computer “A” with the new “Fernando” local account. Maybe you will have to add the Proxy in order to have Internet connection.
10. Go to Settings -> Accounts -> Family & other people -> “Sign in with a Microsoft account instead” and put the new Microsoft account “B” of one of your classmates.
11. Sign out from computer “A” (you are using Microsoft account “B”).
12. Login into computer “A” with your new Microsoft account “A”.
13. Add your classmate's Microsoft account “B” as a “child” family member.

14. Go to https://account.microsoft.com/family and change the limits of the connections of the “child” family member so that the “child” can only connect to Windows during the weekends.
15. After checking that the "child" has those limits, delete them.
16. Go to the Windows search box, and type "lusrmgr.msc". Open this "User Management" console, and check it out. Create a local user from here and check in which group has been added.