



Mac Integration Basics 10.13

Participant Guide

November 2017



Contents

Introduction	4
Audience	4
What you'll learn	4
Before you start	4
Directory Services	5
Connect a Mac to an Active Directory server	5
Summary	12
Share Files	13
Connect to file servers	13
Turn on personal file sharing	17
Summary	18
Configure Collaborative Services	19
Manage Internet Accounts preferences	19
Connect to an Exchange Server	21
Connect Mail to non-Windows servers	23
Add accounts in Mail, Contacts, and Calendars	24

Introduction

Organizations are increasingly integrating Mac computers into Windows or other standards-based network environments. But users and the IT professionals who support them can relax, because Mac integration is easy. This guide provides step-by-step instructions for a successful integration. For additional help, please contact your Apple Authorized Reseller or account representative.

Audience

This guide is for these types of participants:

- Users who bring a Mac into organizations that predominantly use the Microsoft Windows operating system and Windows Server Essentials
- Users who replace a Windows computer with a Mac
- IT professionals who support Mac users in organizations that predominantly use Windows and Windows Server Essentials



What you'll learn

In this guide, you'll learn how to complete the following tasks:

- Integrate a Mac into a Windows network environment.
- Configure a Mac to work with Active Directory.
- Take advantage of network services, file sharing, printing, instant messaging, email, calendars, and contacts.
- Provide security at the user, local-networking, and remote-networking levels.
- Migrate data from a Windows computer to a Mac.
- Back up data.
- Run Windows programs on a Mac.

Before you start

To have the best learning experience with this guide, you should understand how to use a Mac, a Windows computer, and computer peripherals.



Note: Spotlight helps you quickly find things on your Mac. It shows suggestions from the Internet, iTunes, or App Store; movie showtimes and locations nearby; and more. If you're not sure what something is called on the Mac, see this list of Windows and Mac terms to help you find what you're looking for.

Directory Services



A directory service contains a database of user, group, and computer accounts and shares that information with other computers and devices. When you connect a Mac to your company's directory service, you can follow organizational policies for authentication and use password-protected network resources.

Microsoft's directory service for Windows network domains is called Active Directory. Windows Server Essentials Server and Windows Server use Active Directory to provide directory services to network users. macOS supports using directory services provided by Active Directory, Open Directory (macOS Server app), and OpenLDAP (an open-source directory service). This document focuses on joining (also called binding or connecting) a Mac to Active Directory.

A network user account is a user account that you define in a directory service and make available to clients of that directory service. After you connect a Mac to an Active Directory server, you can use an Active Directory network user account to log in to that Mac. Then Mac users with Active Directory accounts can access network resources without entering their credentials again. This is also called single sign-on (SSO).

When you change your Active Directory password using a Mac connected to Active Directory, the new password must adhere to any password policy required by Active Directory. Read [Directory Utility: Active Directory integration and Prepare for macOS Sierra 10.12 with Active Directory](#) for more information.

macOS 10.12 and later require the Active Directory domain to have a domain functional level of Windows Server 2008 or later, unless you enable "weak crypto." Even if the domain functional levels of all domains are Windows Server 2008 or later, the Active Directory administrator might need to specify each domain trust to use Kerberos AES encryption.

Connect a Mac to an Active Directory server

You must configure a Mac to connect to a directory server before you can use network accounts. You can make this connection in at least six ways:

- Configure the connection in [Users & Groups preferences](#).



- Install a configuration profile with directory settings through mobile device management (MDM).



- Use Directory Utility.



- In Terminal, use the dsconfigad command.



- Write a script.
- Use Enterprise Connect.

If you use Active Directory, consider buying Apple Enterprise Connect. Designed for one-to-one deployments, Enterprise Connect can help you access single sign-on services, such as file shares, printers, SharePoint, or any other Kerberos-enabled service. Enterprise Connect automatically reestablishes the SSO trust to Active Directory when your Mac connects to the network. It keeps your local Mac password in sync with your Active Directory password. Email consultingservices@apple.com for pricing and information.

Mac names

You use three similar names when you manage a Mac. macOS configures the names automatically when you complete Setup Assistant.

- The computer name is based on the full name of the computer account, followed by your Mac model. For example, if the computer account you create on a MacBook Pro has a full name of "Johnny Appleseed," the computer name is automatically set to "Johnny's MacBook Pro."
- The local hostname (also known as the Bonjour name) is based on the computer name, but modified to be compliant with the Domain Name Service (DNS). Special characters are removed, and spaces are converted to dashes. For example, if the computer name is "Johnny's MacBook Pro," the local hostname is automatically set to "Johnnys-MacBook-Pro.local."
- The Computer ID is based on the Local Hostname, without the .local suffix. For example, if the local hostname is "Johnnys-MacBook-Pro.local," the Computer ID is automatically set to "Johnnys-MacBook-Pro." A Computer ID is the name that Active Directory uses to create a computer account in Active Directory.

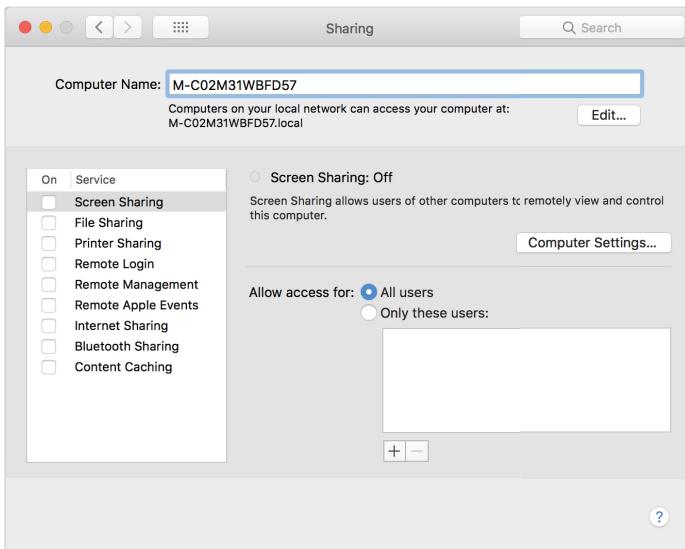
Note: When you turn on a new Mac, you use Setup Assistant to configure basic settings. Through MDM, your system administrator might change what you see in Setup Assistant and the names you use when you manage your Mac.



Prepare to make the connection

1. Optionally change the computer ID.

You can use Sharing preferences to change the computer name of your Mac. If you do, macOS automatically updates the local hostname and the Computer ID.



If you want to change the Computer ID but not the computer name and the local hostname, use User & Group preferences to change it when you join Active Directory.

Some organizations want you to follow a naming convention when you connect to Active Directory. If you don't know the name you should use, check with your Active Directory administrator.

Make sure that the Computer ID has the following characteristics:

- It is 15 characters or less.
- It uses only alphanumeric characters (A–Z, a–z), numbers (0–9), dashes (–), and underscores (_).
- It contains at least one alphanumeric character.

2. Get this information from your Active Directory administrator:

- Active Directory server domain name
- Active Directory credentials (user name and password) for an account that has permission to connect computers to Active Directory

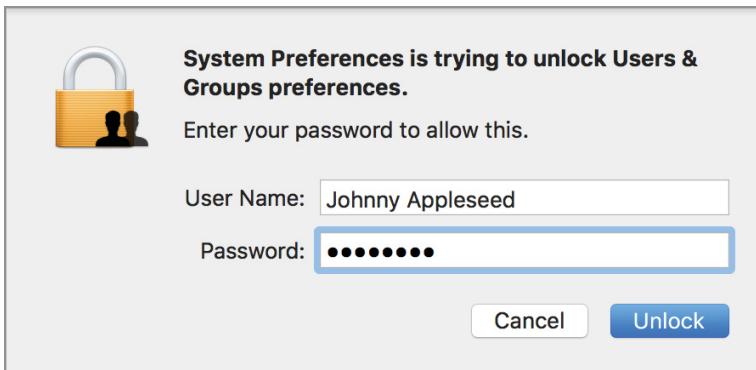
By default, standard Active Directory user accounts can no longer connect computers after they've attempted 10 connections.

When you join a Mac to Active Directory, Active Directory creates a computer account for the Mac. By default, Active Directory places that computer account in a built-in Active Directory container, or Organizational Unit, called "Computers." Some organizations require you to create Mac computer accounts in a different container. Other organizations use Active Directory tools to move a Mac computer account from the default container to a different container. To change the container that Active Directory creates when you join Active Directory, use a tool other than Users & Groups preferences. For example, use Directory Utility. Read Directory Utility Help for more information.



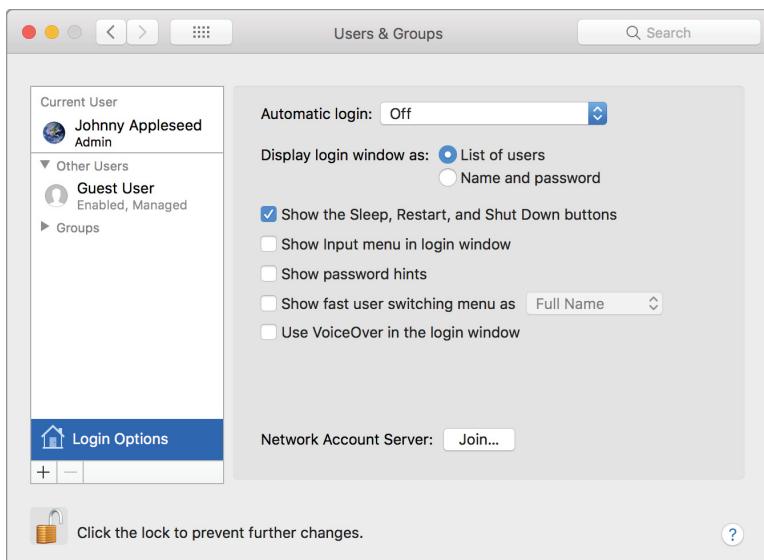
Connect a Mac to Active Directory

1. Open System Preferences.
2. Click Users & Groups.
3. If the lock button (🔒) is locked, click to unlock it.
4. Enter the user name and password for a user who is an administrator of the Mac.
5. Click Unlock.

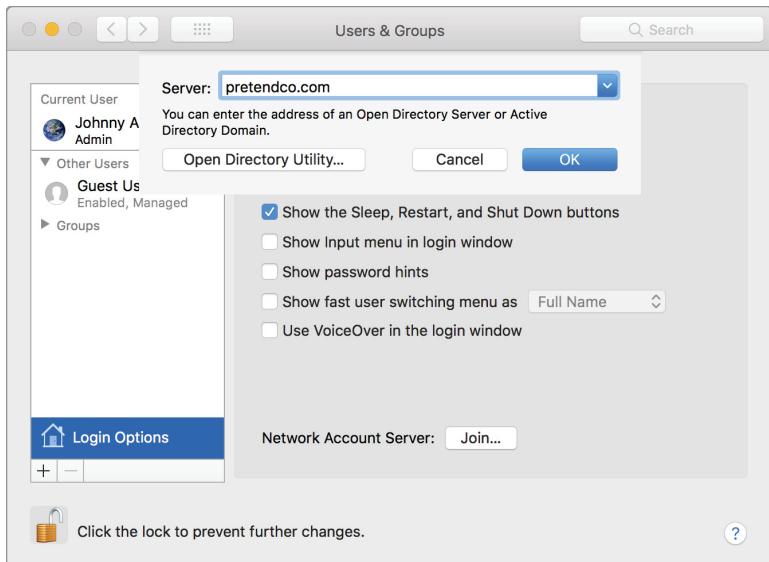


6. In the lower-left corner of Users & Groups preferences, click Login Options.
7. Click Join.

If you see an Edit button instead of a Join button, you're connected to another directory service. In this case, click Edit, then click Add (+) to connect to an additional directory service.



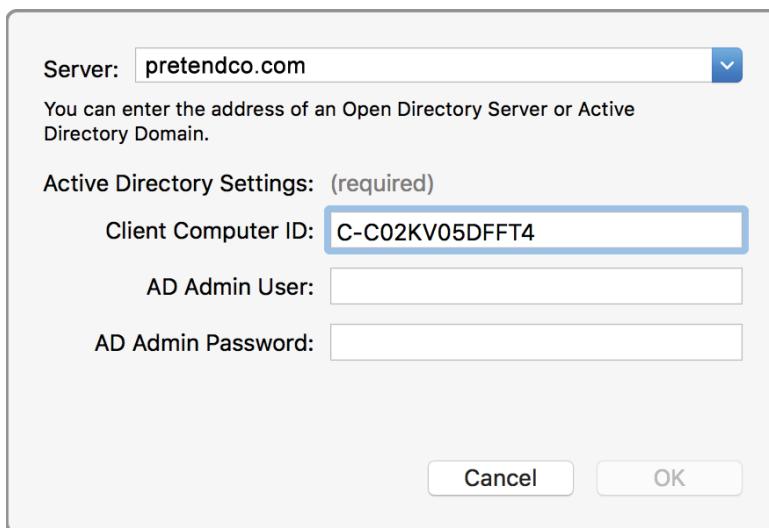
8. Enter the Active Directory Domain name.



9. Click OK.

When macOS identifies the Active Directory server address, the dialog expands to display the Active Directory Settings fields.

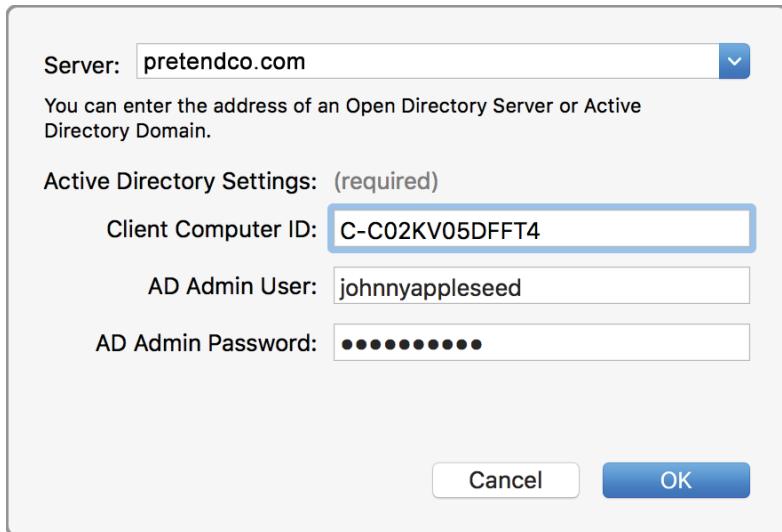
10. If you like, edit the client computer ID that you want Active Directory to use for the server.



11. Enter the user name and password for an Active Directory user who has privileges to add computers to Active Directory.

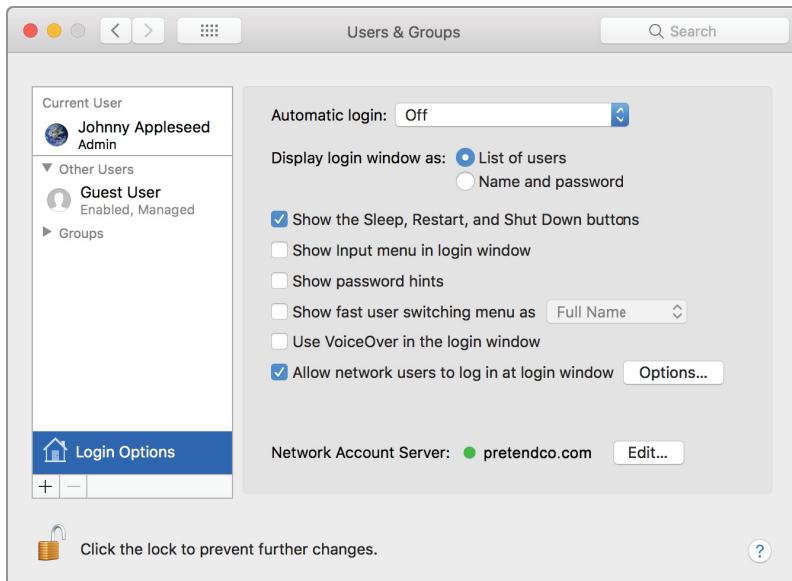
12. Click OK.

The Active Directory account doesn't need to be an Active Directory administrator.



13. Click OK.

The Active Directory domain appears with a green status indicator.



14. Confirm that a new checkbox appears for "Allow network users to log in at login window" and that it's selected.

In the previous steps, you used Users & Groups preferences to join to Active Directory. You provided credentials for two types of user accounts to authorize joining the Mac to Active Directory:

- Your local Mac administrator account
- Active Directory network user account

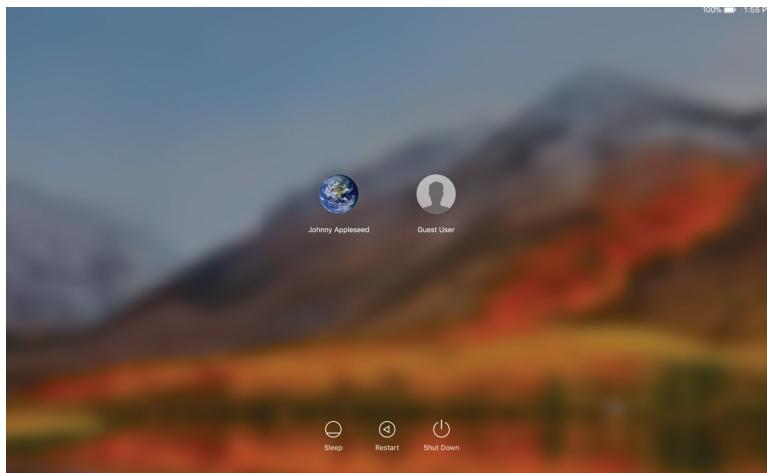
To access network resources, log in using a network account. To do this, you need a network account user name and password from the Active Directory administrator. For Active Directory user accounts, the user name can be in one of three formats:

- *shortname*
- *shortname@domain.com*
- *domain\shortname*

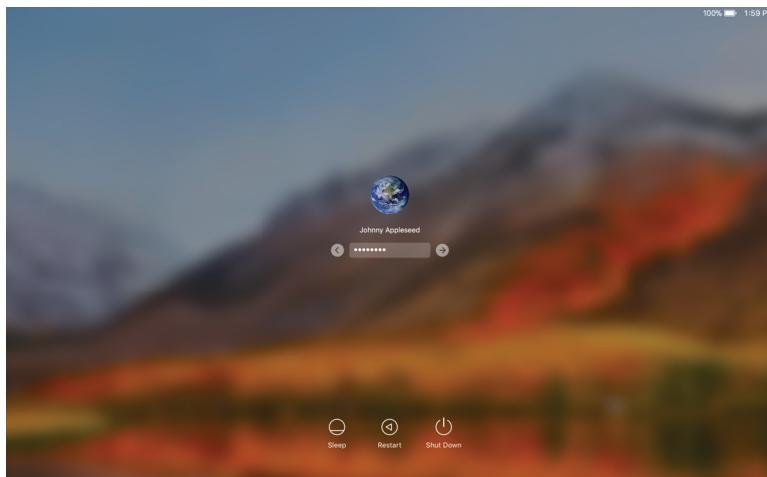
Log in with a network account

1. If you're logged in to the Mac, log out. Choose Log Out from the Apple menu.

macOS logs you out, and a login window lists the local user accounts, followed by Other.



2. Click Other.
3. Enter your Active Directory account user name and password.



4. Press Return or click the Log In (right arrow) button.
5. Respond to Setup Assistant prompts.

For example, in the Siri window, you can leave the checkbox selected for "Enable Talk to Siri on this Mac."

You're now logged in to the Mac with the account provided by the directory server. The Mac is integrated into the network. It can take advantage of user authentication and network resources provided by the Active Directory service.

Summary

In this section, you learned how to set up a Mac to connect to Active Directory. You should now be able to do the following tasks:

- Join a Mac to Active Directory.
- Log in to a Mac with an Active Directory network user account.

Share Files

You can share files and folders with others on your network. You can share your entire Mac with everyone, or allow specific users access to only certain folders.

In this section, you'll learn how to complete the following tasks:

- Connect a Mac to file servers.
- Configure personal file sharing to let other network users access files on a Mac.

Connect to file servers

You can connect a Mac to Windows computers that have file sharing turned on. You can also connect a Mac to file servers that use these protocols:

- Server Message Block (SMB), default
- Common Internet File System (CIFS)
- Network File System (NFS)
- Web Distributed Authoring and Versioning (WebDAV)
- File Transfer Protocol (FTP)

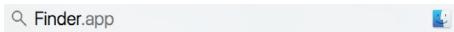
Use either of the following methods to access shared files on Windows computers and file servers on your network:

- Look for the computer or server in the Finder sidebar.
- Enter the computer or server IP address in the “Connect to Server” dialog.



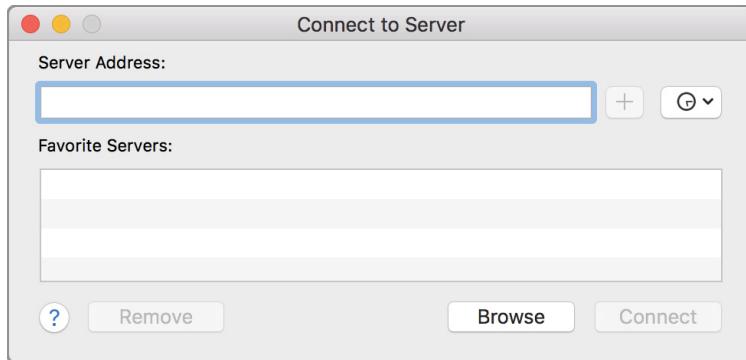
Connect to a computer or server with the Finder

1. Open the Finder from the Dock or use Spotlight to open it.

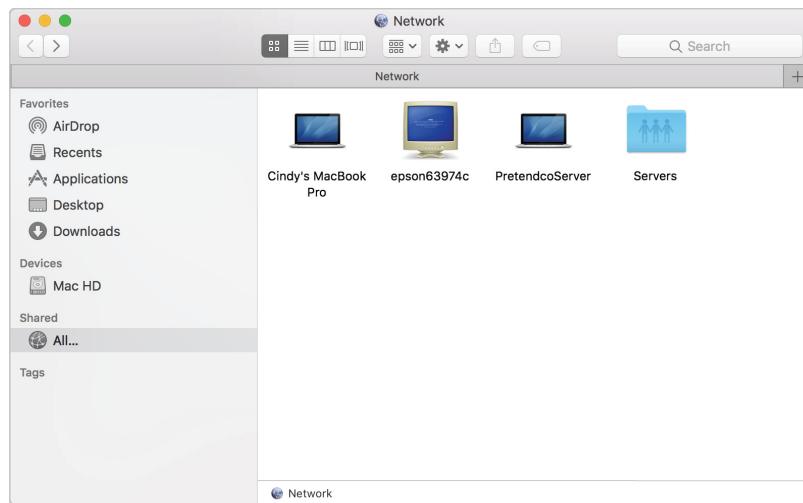


2. From the Go menu, choose “Connect to Server.”

3. Click Browse.



4. The Finder lists computers and servers on your network that have File Sharing or Screen Sharing turned on.

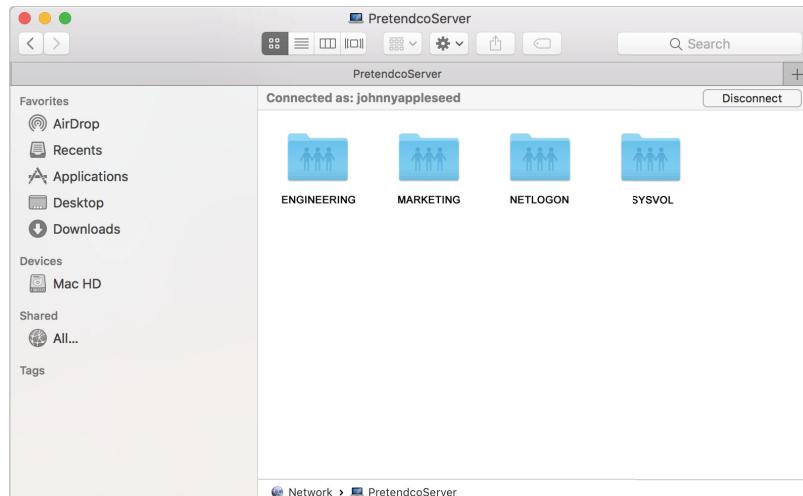


5. Locate the computer or server name that you want to connect to.

You might need to know the network area or workgroup where the computer is.

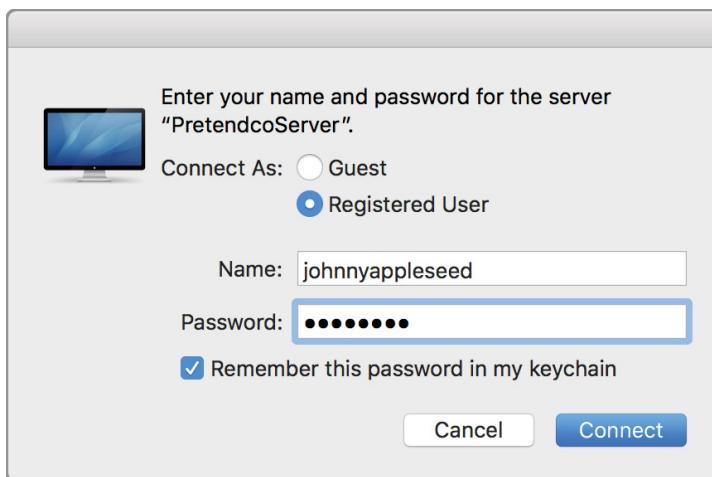
6. When you locate the shared computer or server that you want to connect to, select it, then choose File > Open.

If SSO enables you to connect without providing a password, you see the available shared folders.



7. If you see "Not Connected," click Connect.
8. Select "Connect As Registered User," if it's not selected. Then enter a user name and password for a user account that has permission to connect to the other computer.
9. Select "Remember this password in my keychain."

This step adds the user name and password for the other computer to your keychain. The next time you connect to that computer, you'll get access automatically.



10. Click Connect.

You now have access to the shared folder.

Connect directly to a Windows computer file sharing service

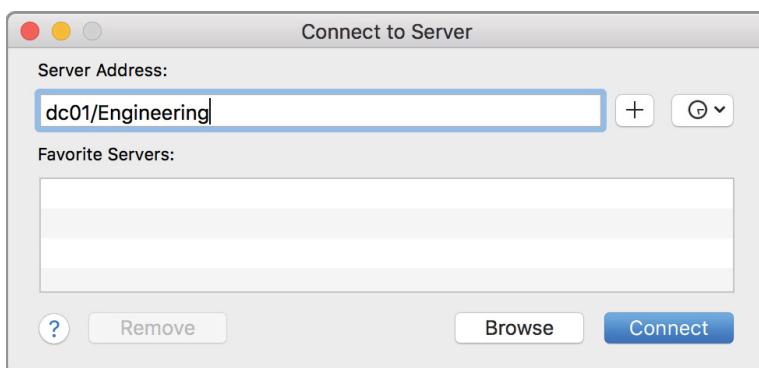
1. In the Finder, choose Go > Connect to Server.
2. Enter the Windows computer name, IP address, or DNS name, and optionally include the share name. Use one of these formats:

Computername/sharename

DNSname/sharename

IPaddress/sharename

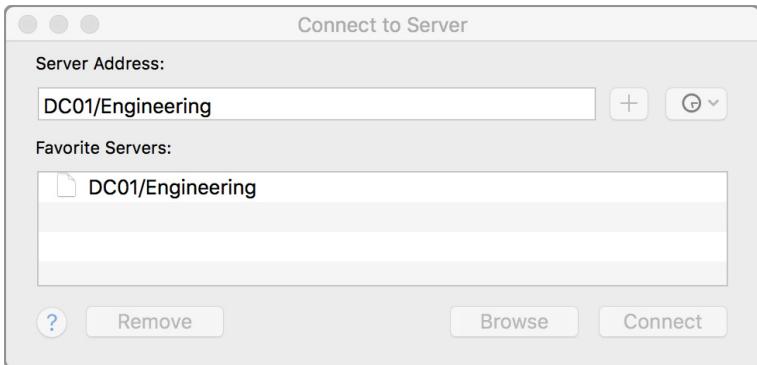
sharename is the name of the shared folder that you connect to.



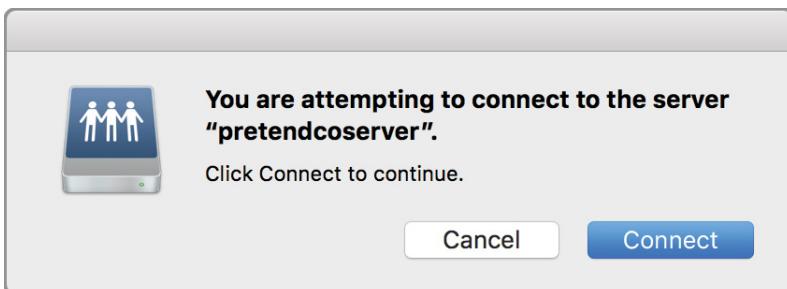
You don't have to specify the SMB protocol, because it's the default.

To add a computer or server to your Favorite Servers list

1. Enter the address.
2. Click Add (+).
3. Double-click the server address in the Favorite Servers section to connect your Mac to that server.
4. Click Connect.



3. If you see a dialog, click Connect to confirm that you are connecting to the other computer's file sharing service.



4. Select Connect As Registered User.
5. Enter the user name and password for a user account that has permission to connect to the other computer.
6. Click Connect.



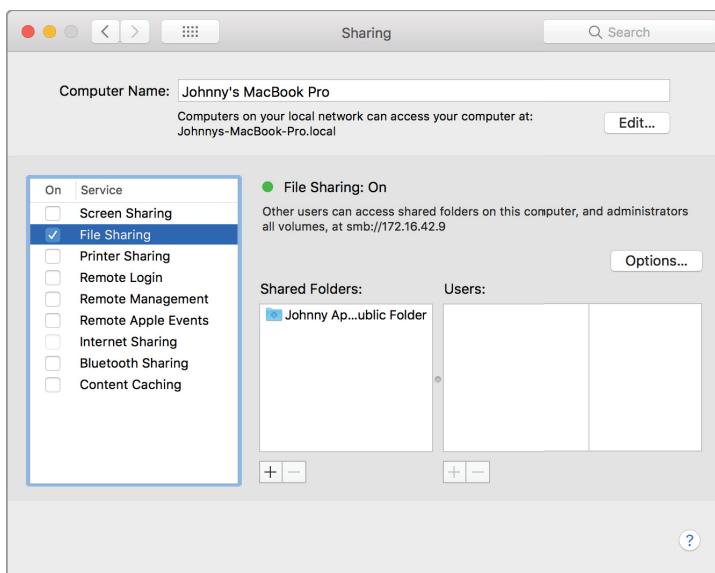
You've now used your Mac to access files stored on network file servers. You can also set up your Mac so that other network users can access your files with personal file sharing. In the next section, you'll learn how to enable personal file sharing. For advanced options and tips, see [Use File Sharing to share files](#).

Turn on personal file sharing



To enable other network users to share files with your Mac

1. Open System Preferences.
2. In the Sharing Preferences pane, select File Sharing.



3. To select a specific folder to share, click Add (+) at the bottom of the Shared Folders list, locate the folder, select it, and click Add.

The Public folder of each user with an account on your Mac is shared automatically. To prevent a folder from being shared, select it in the Shared Folders list and click Remove (-), and then click OK.

Specify user access to shared files

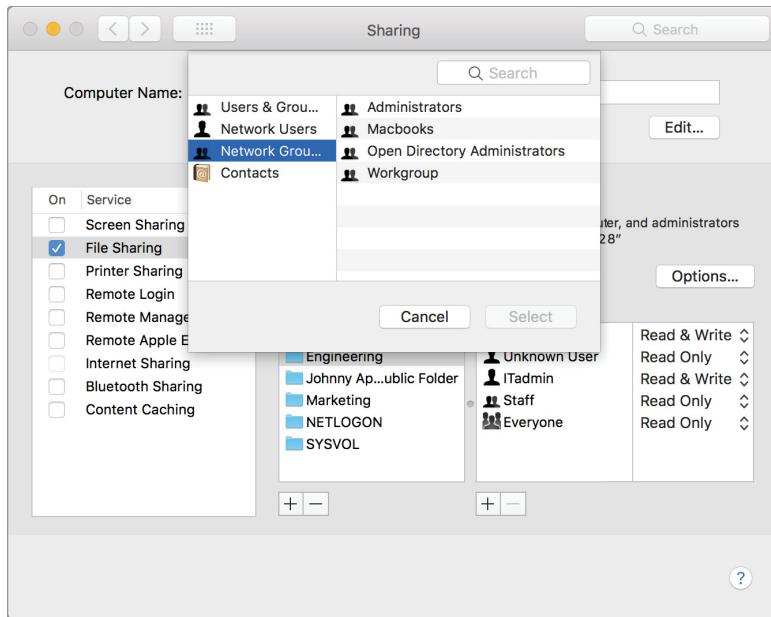
By default, any user set up on your Mac in Users & Groups preferences can connect to your Mac over the network. A user with an administrator account can access your entire Mac.

Give specific users access to a folder:

1. Select the folder in the Shared Folders list.
2. Click Add at the bottom of the Users list.

3. Do one of these things:

- Select a user from Users & Groups, which includes all the users of your Mac.
- Select a user from Network Users or Network Groups, which includes everyone on your network.
- Select a person from your contacts. Create a password for the person, and click Create Account.



4. To specify user access, select the user in the Users list.

5. Click the triangles next to the user name.

6. Choose one of the following permissions settings:

- Read & Write: The user can see and copy files to and from the folder.
- Read Only: The user can view the folder contents but can't copy files to it.
- Write Only (Drop Box): The user can copy files to a folder but can't view its contents.
- No Access: This option is available for the Everyone entry, which applies to users who aren't listed in the Users column. If you choose "No Access," users who aren't in the Users list can't see or copy files from the folder.



macOS enables guests to access shared folders on your Mac. To turn off guest access, deselect "Allow guest users to connect to shared folders" in the Guest Account pane of User & Groups preferences.

Summary

In this section, you learned how to share files. You should now be able to do these things:

- Connect a Mac to file servers.
- Configure personal file sharing to let other network users access files on a Mac.

Configure Collaborative Services

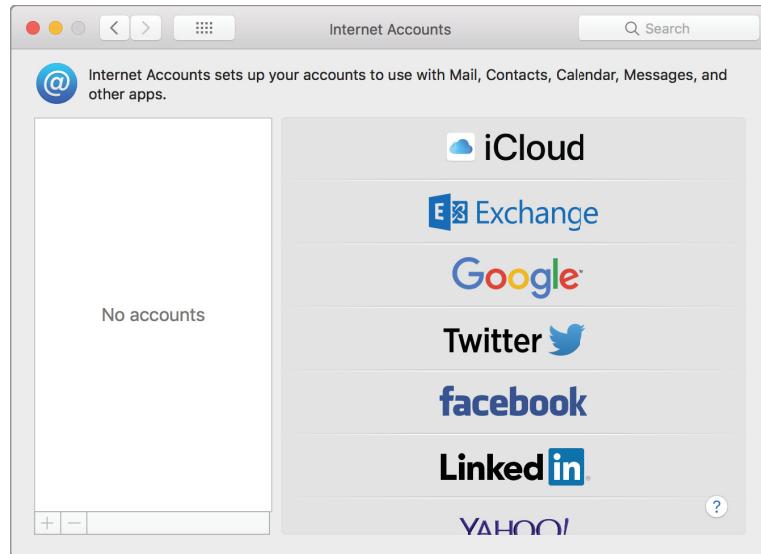
macOS supports email, contacts, and calendars using standards-based servers, including Microsoft Exchange Server, POP, IMAP, SMTP, and more. With macOS, you can connect to shared services such as email, calendars, and global address lists. In this section, you'll learn how to configure these apps:

- Mail: To send and receive email using common server types
- Contacts: To access shared contacts
- Calendar: To access shared calendar services

Manage Internet Accounts preferences

macOS includes built-in support for the latest version of Microsoft Exchange Server, so you can use your Mac with Microsoft features and apps. You'll also have your messages, meetings, and contacts in one place.

Using Internet Accounts, you can set up the accounts you want to use with Mail, Messages, Calendar, and other apps.



In the Internet Accounts pane, a list on the left shows web service accounts. You provided information for these accounts when you did the following:

- First configured macOS with Setup Assistant
- Created an account in an app
- Used Internet Accounts preferences

The list on the right shows major service providers that you can set up in Internet Accounts preferences. You can make changes to accounts:

- To view or change information about an account, select the account from the list on the left.
- To remove a selected account and turn off its features, click Remove (-).

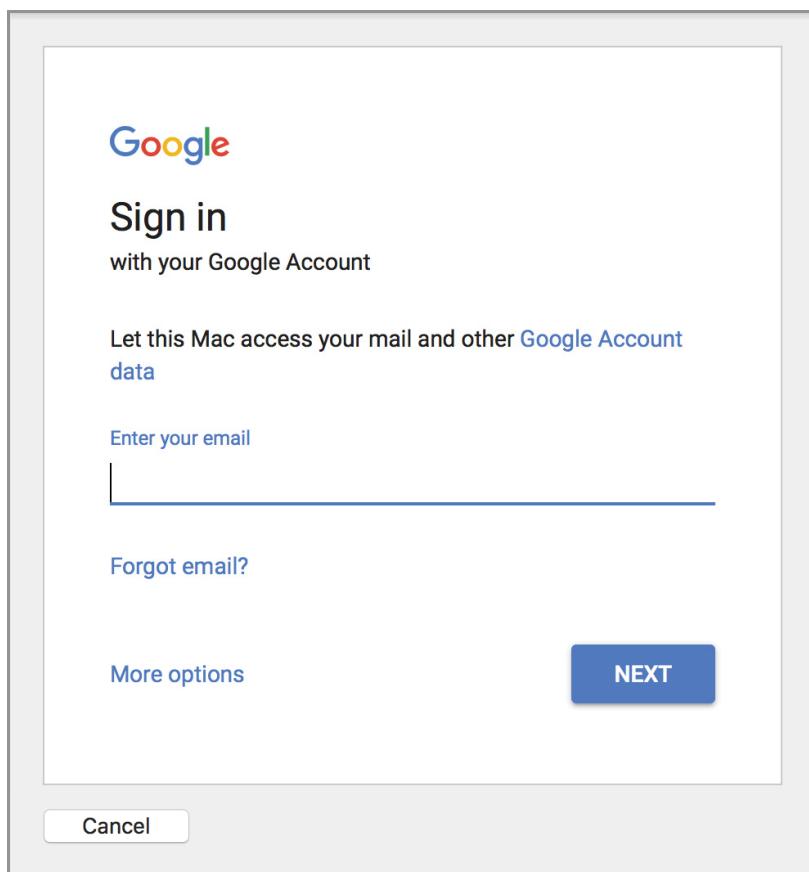
If multiple apps use a selected account, you can stop an app from using it by deselecting its checkbox.

Add an account in Internet Accounts preferences

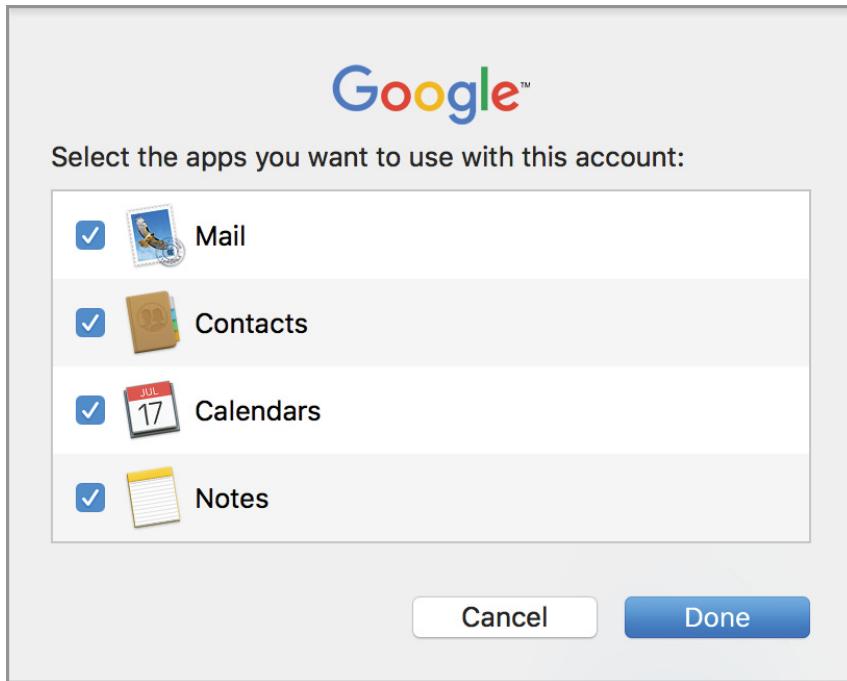
1. Open System Preferences.
2. Click Internet Accounts.
3. If you haven't added an account yet, click the account type that you want to add.
4. Enter your email address and password and click Sign in.
5. If you already added an account and it's selected, click Add (+).

You see the main Internet Accounts pane.

6. Click an account type, enter your account information, and follow the onscreen instructions.



7. Ensure that the apps you want to use with the account are selected.



Connect to an Exchange Server

Mail and Calendar support these Exchange Server versions:

- Office 365
- Exchange Server 2013
- Exchange Server 2010
- Exchange Server 2007

To connect a Mac to an Exchange server, obtain the server user name and password from your server administrator.

If the Exchange Autodiscover service isn't enabled on the Exchange server, obtain the fully qualified domain name for the organization's Client Access Server (CAS). The CAS fully qualified domain name usually looks like this:
exchange01.example.com.

After you have the required information, you can configure your Mac manually to use the Exchange Server, or configure it automatically by using the Exchange Autodiscover service.

The easiest way to set up Contacts and Calendar to access Exchange is with Exchange Autodiscover. If this feature is enabled on the Exchange server, perform the steps listed below.

[Connect to an Exchange server with Autodiscover enabled](#)

macOS uses the Autodiscover service in Exchange to get relevant account information. If it's enabled, you can start using Exchange services immediately.

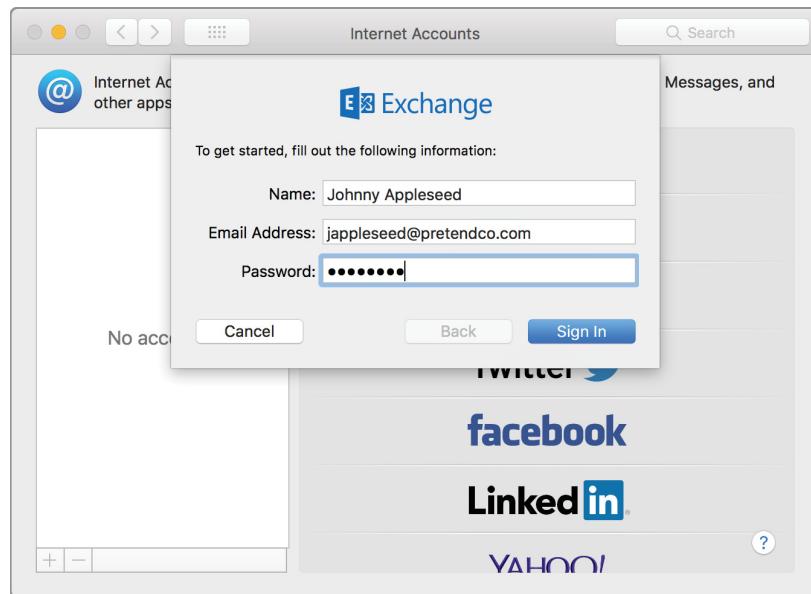
1. Open System Preferences.
2. Click Internet Accounts.

3. Click Exchange in the list of services.

Click Add (+) to add the Exchange server, if it isn't in your list of servers.

You won't see the plus sign until at least one account is created.

4. Enter your Exchange email address and password.



5. Click Sign In.

6. Select the services you want to connect to.

Manually configure a Mail account to connect to an Exchange server

If Autodiscover isn't enabled on the Exchange server, follow the steps below to manually configure your Mail account.

1. Open System Preferences.
2. Click Internet Accounts.
3. Click Exchange in the list of services on the right.
4. Enter your Exchange email address and password.
5. Click Sign In.
6. Enter a description for the account (for example, Work or Exchange).
7. Enter the internal and external URLs for your organization's Exchange client-access server.
8. Click Continue.
9. To set up Contacts and Calendar automatically, ensure their checkboxes are selected.
10. Click Done.
11. Send and receive emails from your Exchange account to confirm that you configured Mail successfully.

[Access an Exchange server from a Mac outside an organizational network](#)

Confirm the following with your Exchange administrator and your network administrator:

- Port 443 isn't blocked between your Mac and the Exchange server.
- Exchange Web Services (EWS) is enabled on the server.

For more information about using Exchange Web Services, read [Use Microsoft Exchange \(EWS\) accounts in Mail on your Mac](#).

Connect Mail to non-Windows servers

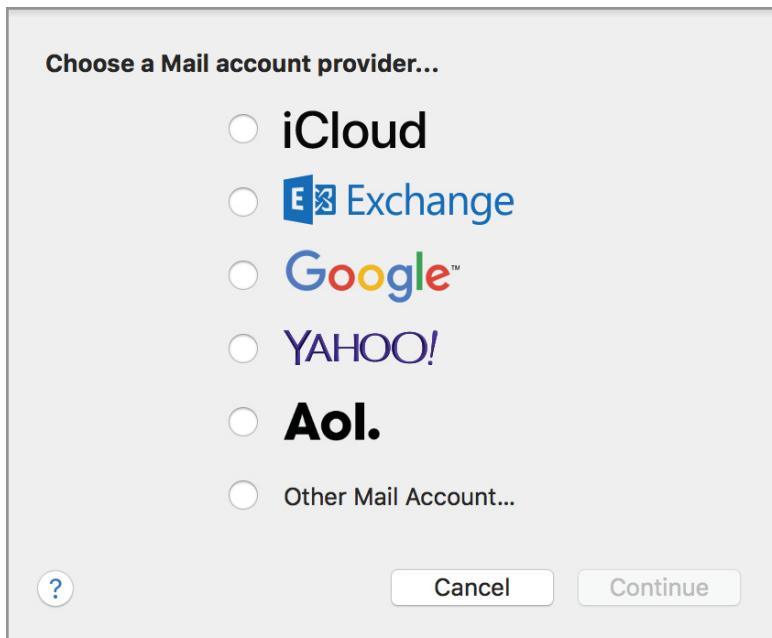
If your organization uses a non-Windows server for email services, you can configure Mail to access it. Common mail-server protocols for non-Windows servers include:

- Post Office Protocol (POP): This protocol allows client computers to access messages on a mail server.
- Internet Message Access Protocol (IMAP): This protocol allows client computers to access messages on a mail server.
- Simple Mail Transfer Protocol (SMTP): This protocol allows messages to be sent from a client computer to a mail server and between mail servers.

[Configure Mail to connect to non-Windows email services](#)

1. Open Mail.
2. From the "Choose a Mail account provider" dialog, select "Other Mail Account."

3. Click Continue.



4. Enter your Mail account full name, email address, and password.

5. Click Sign In.

If macOS identifies the mail server type and connects, it creates the mail account, and you can skip the rest of the steps in this procedure.

If macOS can't identify the mail server type, you must manually configure the account.

6. When you're prompted to manually create the account, click Next.

7. In the Incoming Mail Server Info pane, select the type of email account: IMAP or POP.

8. Enter the mail server address provided by your Internet service provider (ISP) or mail server administrator.

9. Verify that the user name and Password fields are correct, and click Next.

10. If the port address and authentication type are displayed, verify that they're correct, and click Next.

11. In the Outgoing Mail Server Info pane, enter the outgoing mail server address and authentication information.

12. Click Create.

You should now be able to use Mail.

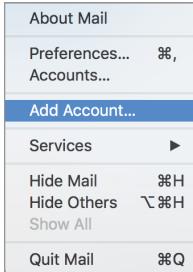
13. Send and receive email to verify that you've successfully configured Mail for use with common mail server protocols.

Add accounts in Mail, Contacts, and Calendars

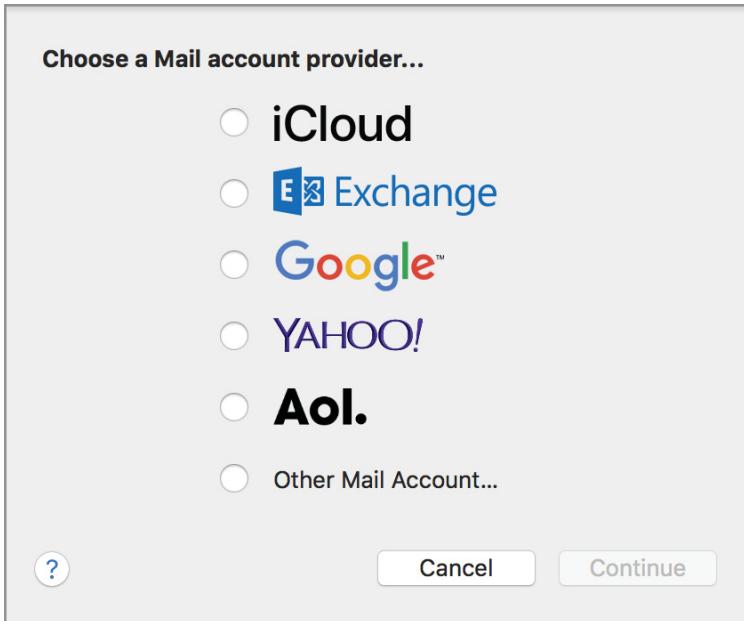
In addition to configuring accounts in Internet Accounts preferences, you can configure them in the Mail, Contacts, and Calendar apps.

[Add a new account from Mail](#)

1. Choose Add Account from the Mail menu.



2. Select a Mail account provider from the list, and click Continue.



An assistant appears and guides you through the steps to add a mail account.

If you can't connect to your mail server, see [Use Connection Doctor](#). Also, verify your login information with your mail service or support department.

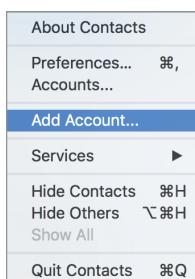
3. To view your login information, choose Mail > Preferences.

4. Click Accounts.

For Mail Help, click the question mark (?) in the lower-right corner of the pane.

Add a new account from Contacts

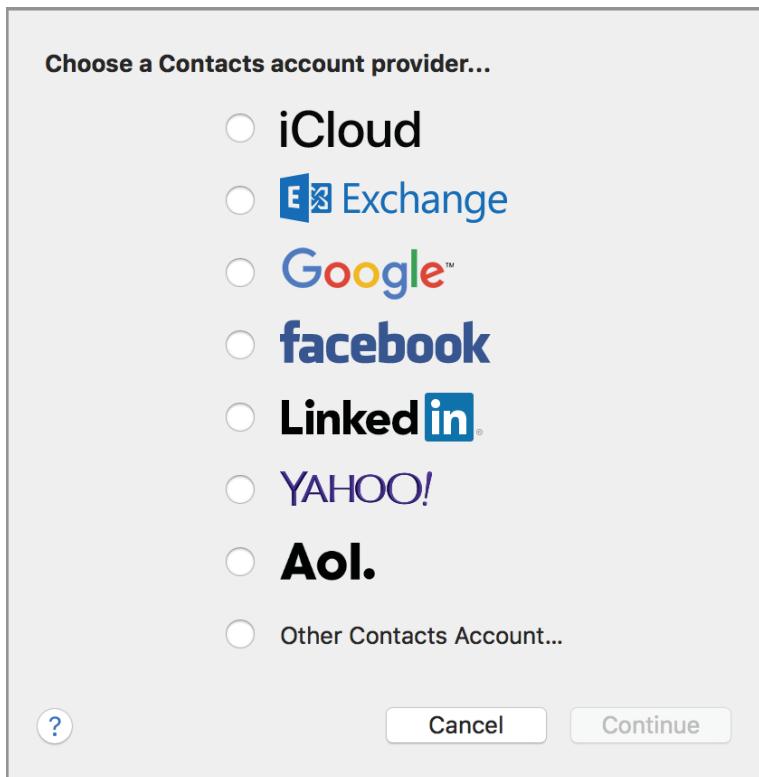
1. Open Contacts.
2. Choose Add Account from the Contacts menu.



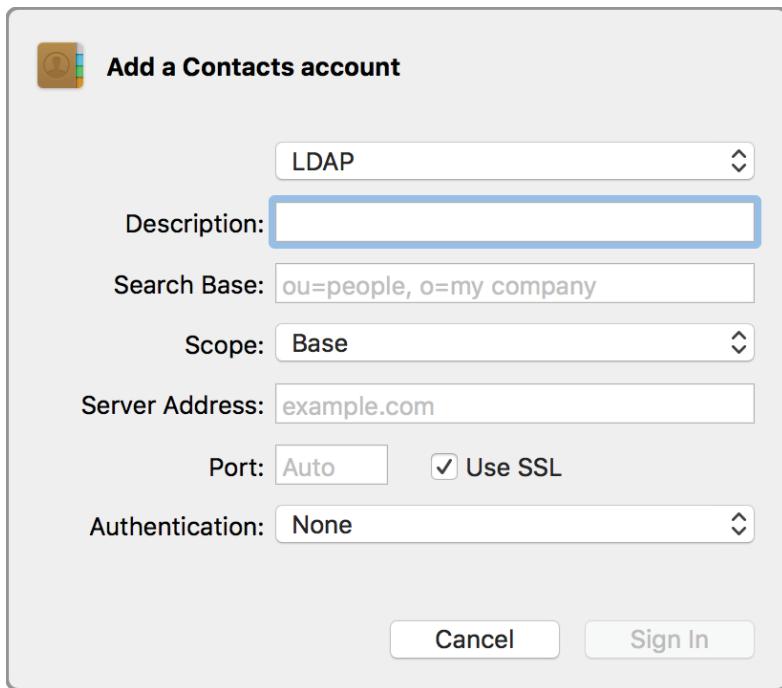
3. Select a Contacts account provider from the list, and click Continue.

If your organization uses CardDAV or LDAP for contact data, select Other Contacts Account. An assistant appears and guides you through the steps to add a Contacts account.

The Card Distributed Authoring and Versioning (CardDAV) protocol is based on an Internet standard for sharing contact information.

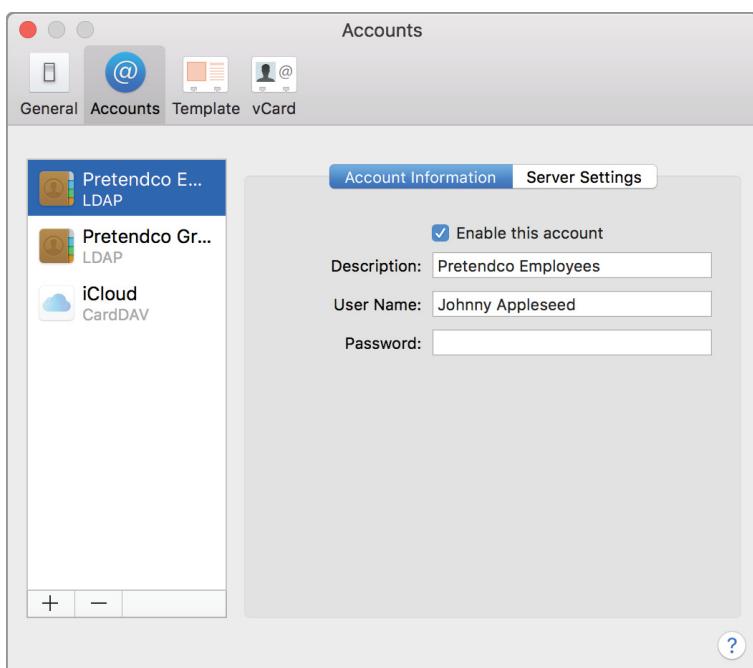


4. Ask your server administrator for the address of the CardDAV server that hosts your CardDAV account.
Ask your server administrator for the information you need to complete the fields in the LDAP pane.
An LDAP Internet account is based on an Internet standard for finding information on an LDAP directory server.
Depending on how your LDAP server is configured, the information you must provide might be complex.



Enable or disable accounts that are available to Contacts

1. Choose Contacts > Preferences.
2. Click Accounts and select the account.



3. To enable the account, select the checkbox "Enable this account." To disable the account, deselect the checkbox.

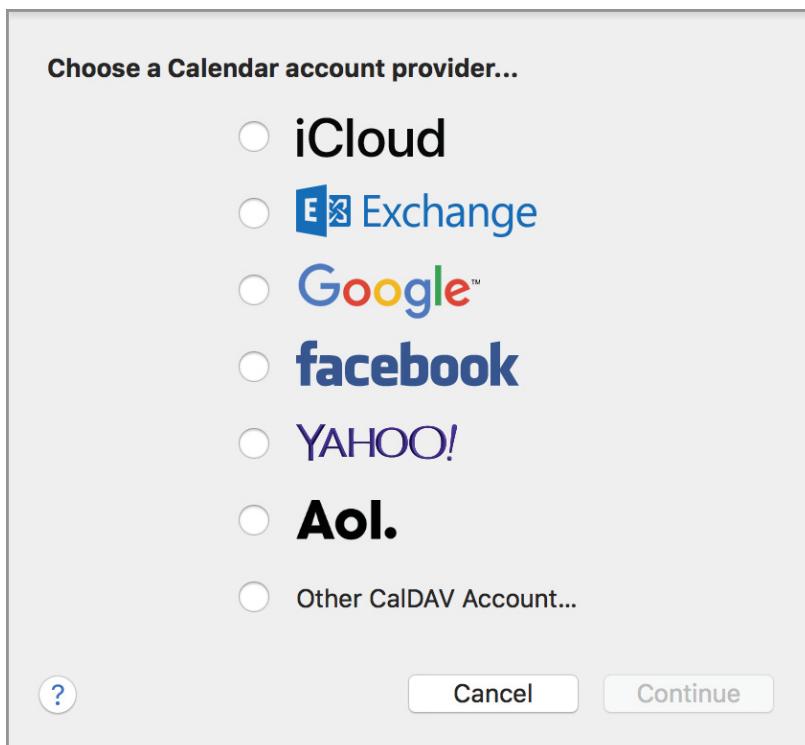
To add a new account from Calendar

1. Open Calendar.
2. If you see the What's New in Calendar window, read it.
3. Click Continue.
4. Choose Add Account from the Calendar menu.



5. Select a Calendar account provider from the list and click Continue.

An assistant guides you through the steps.



Enable or disable accounts that are available to Calendar

1. Choose Calendar > Preferences.



2. Click Accounts.
3. Select the account.
4. To enable the account, select the checkbox "Enable this account." To disable the account, deselect the checkbox.

Summary

In this section, you learned how to configure a Mac to access server-based mail, contacts, and calendar services. You should now be able to perform these actions:

- Use Internet Accounts preferences to add mail, contacts, and calendar accounts.
- Connect to an Exchange server.
- Connect Mail to POP and IMAP servers.
- Configure accounts directly from Mail, Contacts, and Calendar.

Secure a Mac

Apple cares deeply about security and protecting the systems, apps, and data of users and organizations. Mac provides a comprehensive approach to security that protects the entire platform, including the operating system, the services, the data on each device, and the apps.

macOS has a multi-layered approach to security. It's designed into the hardware, software, and app ecosystem and is an essential consideration in data storage, retrieval, and transmission. macOS offers technology and strong, easy-to-use tools for Mac and network security.

You can help maintain security by protecting user data, Mac computers, and networks. In this section, you'll learn about built-in security features and the following ways you can protect your Mac:

- Create strong passwords.
- Use two-factor authentication.
- Set a firmware password.
- Lock the Mac screen.
- Create user accounts.
- Disable automatic login.
- Protect start-up disk files.
- Use Gatekeeper to open safe apps.
- Provide network security.

Built-in security features

macOS offers multilayered security technologies that help protect against viruses, malicious apps, and malware. In this section, you'll learn about these automatic security features:

- System Integrity Protection
- User Approved Kernel Extension Loading
- Sandboxing
- Library Randomization
- Execute Disable

Sandboxing

Through sandboxing, macOS prevents hackers from harming your programs. Sandboxing restricts the following:

- Actions that programs can perform on your Mac
- Files that programs can access
- Programs that can be opened

System Integrity Protection

System Integrity Protection helps prevent potentially malicious software from modifying protected files and folders on a Mac. It uses sandboxing to restrict the root account and limits actions that the root account can perform on protected parts of macOS. It protects apps that are preinstalled with macOS and also these folders:

- /System
- /usr
- /bin
- /sbin

Folders that third-party apps and installers can write to include these:

- /Applications
- /Library
- /usr/local

Only apps and scripts that are signed by Apple and have entitlements to write to file systems can modify the protected parts of macOS. Examples of these processes include Apple software and Apple installers.

Apps downloaded from the App Store already work with System Integrity Protection. Consider removing third-party software that conflicts with System Integrity Protection.

System Integrity Protection also helps prevent software from changing your startup volume. To start up a Mac from a different volume, use the Startup Disk pane in System Preferences. Or press and hold the Option key while you restart, and select a volume from the list that appears.

Library Randomization

Library Randomization keeps malicious commands from finding their targets.

Execute Disable

Execute Disable protects the memory in your Mac from attacks.

Create strong passwords

macOS features Password Assistant, which checks your password strength or generates a strong password for you. You can tell Password Assistant what password type and length you'd like it to create. You can choose from these password types:

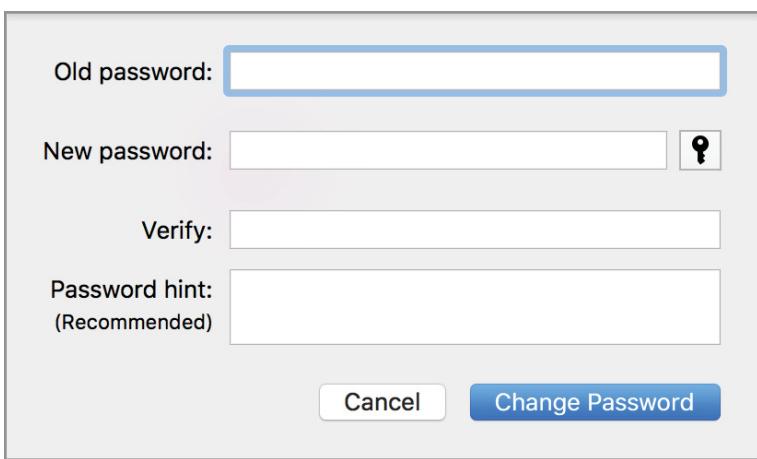
Password type	Description	Example
Manual	Enter a password. Password Assistant ranks the strength of the password on a sliding scale. If it's weak, Password Assistant offers tips for increasing its strength.	
Memorable	Adjust the password Length setting. Password Assistant generates a list of memorable passwords that contain words and some random characters.	wail49{clasp
Letters & Numbers	Adjust the password Length setting. Password Assistant generates a list of passwords with a combination of letters and numbers.	wShOZk8XspuZFx
Numbers Only	Adjust the password Length setting. Password Assistant generates a list of passwords that contain only numbers.	1261184494119718157669
Random	Adjust the password Length setting. Password Assistant generates a list of passwords that contain random characters.	t@Z)YPTLI:fU
Federal Information Processing Standard (FIPS)-181 compliant	Adjust the password Length setting. Password Assistant generates a password that is FIPS-181 compliant.	yphiochadiifydobnyibo

When you enter a password or change the length slider for a suggested password, Password Assistant displays a message that indicates how secure the password is.

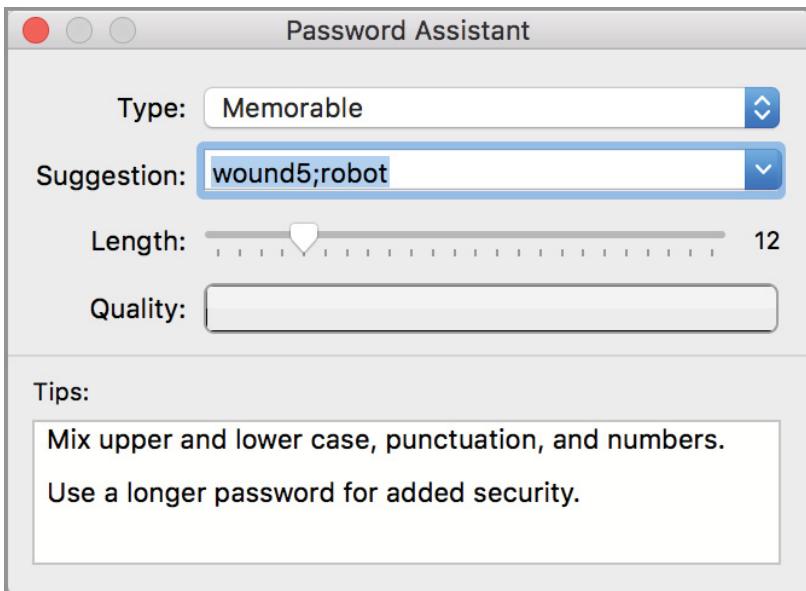
Use Password Assistant to create a password

You can get quick access to Password Assistant if you follow the steps as if you were going to change your own password. You don't have to change your password when you use Password Assistant.

1. Open System Preferences.
2. Click Users & Groups.
3. Select a user.
4. Click Change Password.
5. Click the Key (��) to the right of the "New password" field.



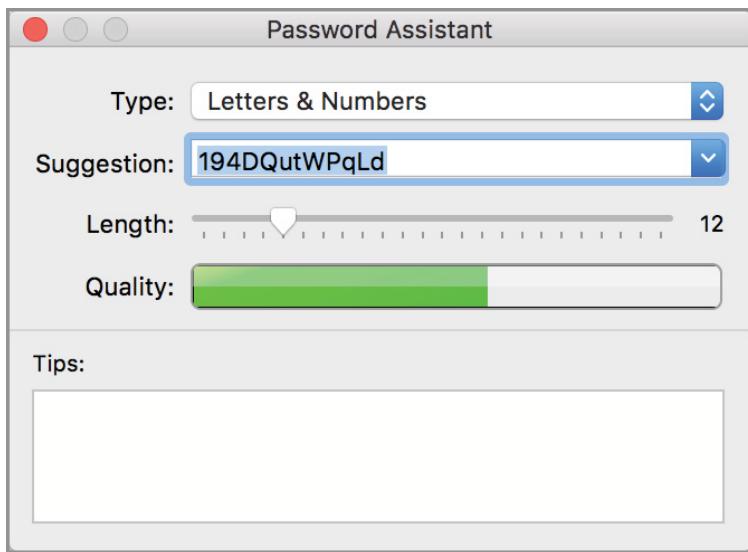
Password Assistant opens.



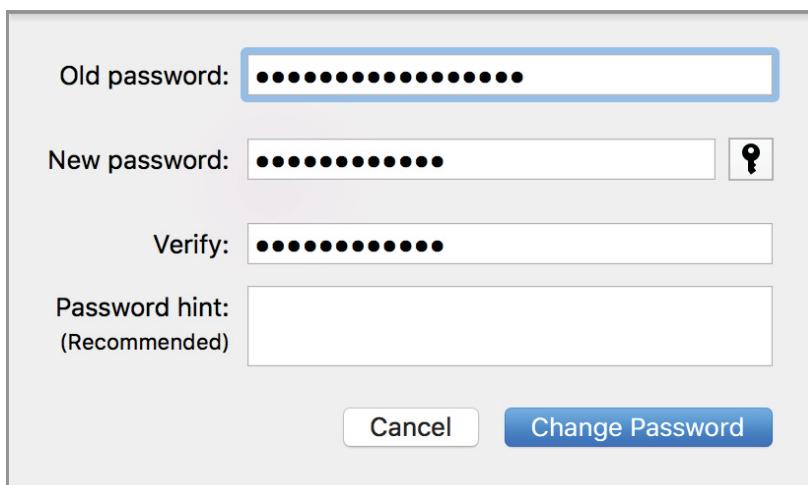
6. From the Type pop-up menu, choose the password type that meets your organizational security standards.



- To choose the number of characters for an automatically generated password, move the Length slider to the left or right.



- Close the Password Assistant pane.
- Click Change Password.



Use two-factor authentication

Two-factor authentication is an extra layer of security for your Apple ID. It's designed to ensure that you're the only person who can access your account—even if someone else knows your password.

How it works

With two-factor authentication, your account can be accessed only on devices you trust, such as your iPhone, iPad, or Mac. When you sign in to a new device for the first time, you provide two pieces of information—your password and the six-digit verification code that's automatically displayed on your trusted devices. By entering the code, you verify that you trust the new device. For example, suppose you have an iPhone and you sign in to your account for the first time on a new Mac. You'll be prompted to enter your password and the verification code that automatically displays on your iPhone.

Because your password alone isn't enough to access your account, two-factor authentication improves the security of your Apple ID. And all the personal information you store with Apple is more secure, too.

After you sign in, you won't be asked for a verification code on that device again. If you sign out completely, erase the device, or change your password, you'll be asked for the code. When you sign in on the web, you can choose to trust your browser. And you won't be asked for a verification code the next time you sign in from that computer.

Trusted devices

A trusted device is an Apple device that you've already signed in to using two-factor authentication. You can use it to verify your identity, because it displays a verification code from Apple when you sign in on a different device or browser. Trusted devices include:

- iOS devices using iOS 9 or later
- Mac computers using OS X El Capitan or later

Trusted phone numbers

You can use a trusted phone number to receive verification codes by text or phone call. You must verify at least one trusted phone number to enroll in two-factor authentication. Consider verifying other phone numbers that you can access, such as a home phone or a number used by a family member or close friend. You can use those numbers if you temporarily can't access your own device.

Verification codes

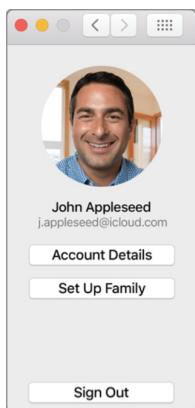
A verification code is a temporary code that is sent to your trusted device or phone number when you sign in to a new device or browser with your Apple ID. You can also get a verification code from Settings on your trusted device.

A verification code is different from the device passcode that you enter to unlock your iPhone, iPad, or iPod touch.

Confirm that two-factor authentication is on for your Apple ID

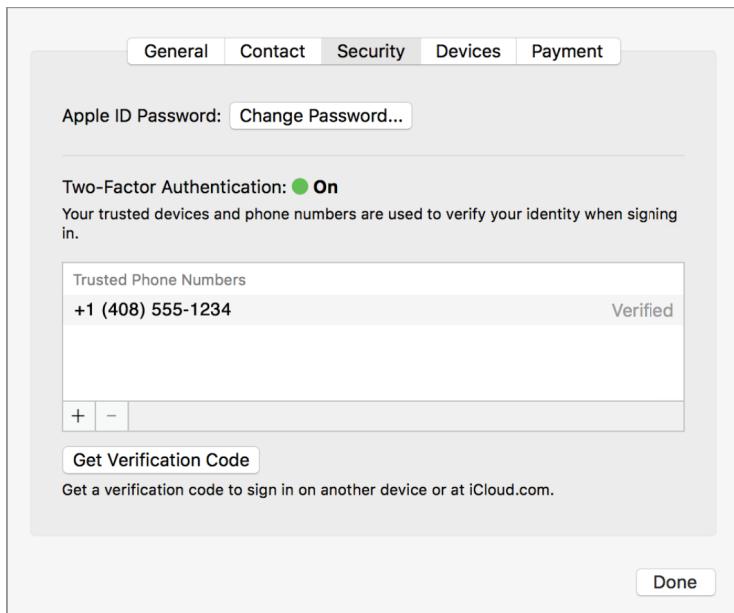
Some Apple IDs created in macOS 10.12.4 and later or iOS 10.3 or later are protected with two-factor authentication by default. In this case, you see that two-factor authentication is turned on.

1. Go to the Apple (⌘) menu and choose > System Preferences > iCloud.
2. Click Account Details.



3. Click Security.

4. Confirm that two-factor authentication is on.



If two-factor authentication isn't turned on for your Apple ID, click "Turn On Two-Factor Authentication."



Two-factor authentication significantly improves the security of your Apple ID. After you turn it on, signing in to your account requires two things:

- Your password
- Access to your trusted devices or trusted phone number

To keep your account secure and help ensure that you never lose access, follow these guidelines:

- Remember your Apple ID password.
- Use a device passcode on all your devices.
- Keep your trusted phone numbers up to date.
- Keep your trusted devices physically secure.

Set a firmware password

When you set a firmware password, you help prevent unauthorized startup devices from bypassing macOS security. Set a firmware password to enable low-level hardware protection for your Mac. It helps prevent unauthorized users from starting up your Mac from the following devices:

- External hard disk
- Universal Serial Bus (USB) flash drive

Set a firmware password

1. Restart your Mac.
2. Press and hold Command-R.
The Mac attempts to start up using the Recovery HD partition.
3. When the macOS Utilities window appears, choose Utilities > Firmware Password Utility.



4. Click "Turn On Firmware Password."



5. Enter a password in the Password and Verify fields.
6. Click Set Password.
7. Click Quit Firmware Password Utility.

Test your settings

1. Restart the Mac, and then press and hold the Option key.
The Mac attempts to start using Startup Manager.
2. Verify that you see a lock button with a password field.
If you see a lock button with a password field, changes made by Firmware Password Utility were successful.



3. Enter your firmware password to continue.

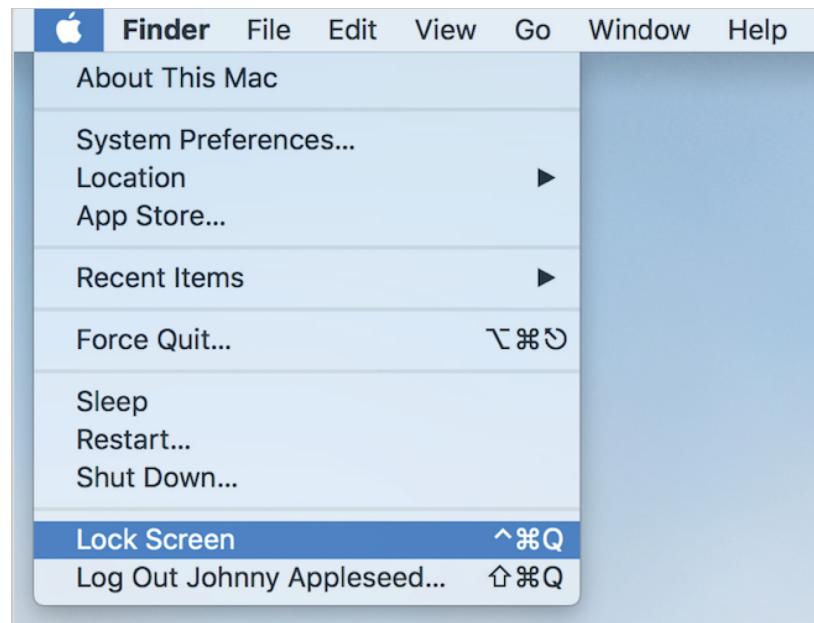
Reset a firmware password

To reset a lost firmware password, take your Mac to an Apple Retail Store or Apple Authorized Service Provider. For more information, read [If you lost or forgot your firmware password](#).

Lock a Mac screen

To stay logged in to your Mac while you're away and prevent others from using it, lock the screen.

1. Press Shift-Command-Q to immediately lock your screen. You can also click the Apple menu and choose Lock Screen.

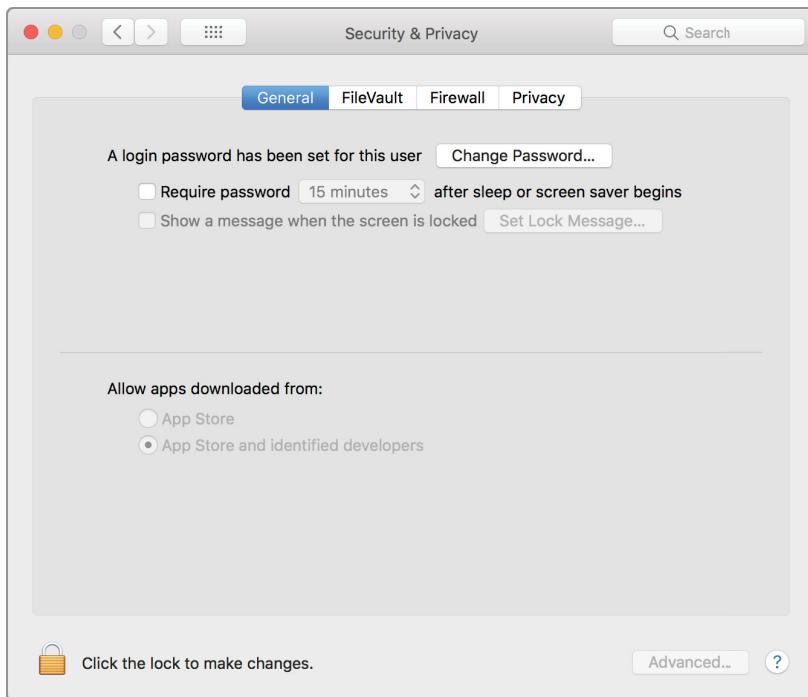


When you return to your Mac, enter your login name and password to continue.



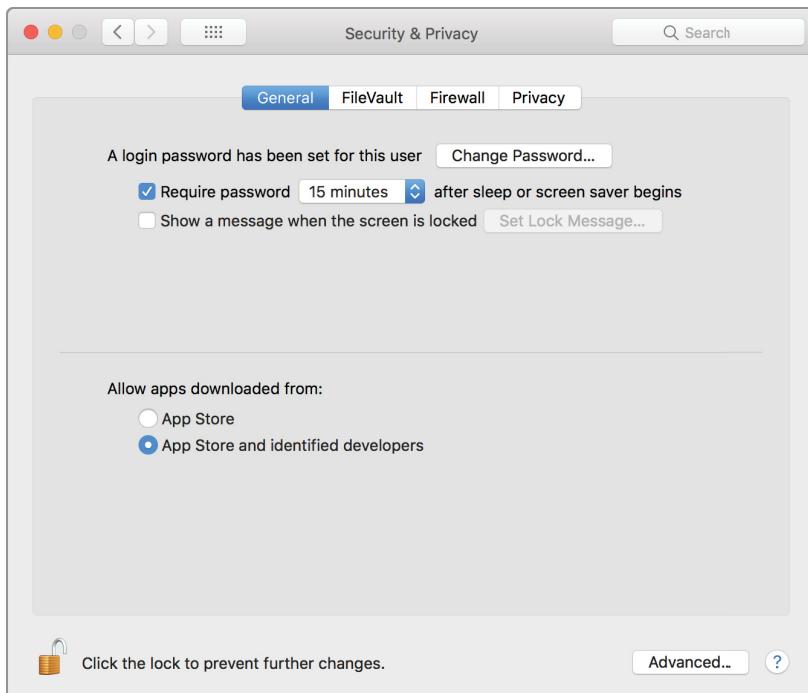
Require authentication after sleep or screen saver begins

1. Open System Preferences.
2. Click Security & Privacy.
3. Click General.
4. If the lock button (🔒) is locked, click to unlock it.

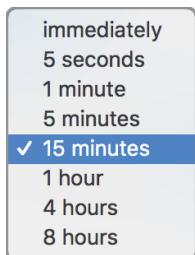


5. Enter your administrator user name and password.
6. Click Unlock.

7. Select the checkbox for "Require password after sleep or screen saver begins."



8. In the pop-up menu in the middle of the sentence, adjust the length of delay before a password is required.



When you lock a Mac screen, you don't prevent a user from turning off the Mac, restarting it, or logging in to an account on it. If you think someone might do those things, save your work before you lock the screen.

Create user accounts

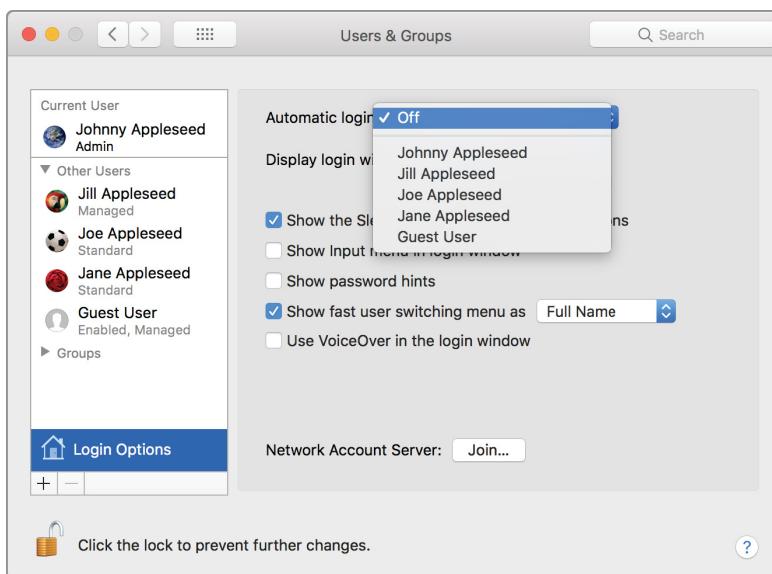
If you share a Mac, create an account for each user. Separate user accounts protect user information and make the Mac more secure.

Disable automatic login

Automatic login means that anyone can access your Mac just by restarting it. If your Mac has multiple accounts with automatic login configured for one account, it automatically logs in to that account during startup. Whether your Mac has multiple user accounts or just yours, you should disable automatic login if you want to keep the Mac more secure. If you decide to enable automatic login, make sure the Mac isn't set up to automatically log in to an administrator account.

Turn off automatic login

1. Open System Preferences.
2. Click Users & Groups.
3. If the lock icon (🔒) is locked, click to unlock it.
4. Enter your administrator user name and password.
5. Click Unlock.
6. Click Login Options.
7. Choose Off from the "Automatic login" pop-up menu.



The next time you start up your Mac, the login window appears.

8. Enter a user name and password to log in.

Protect start-up disk files

FileVault full-disk encryption uses XTS-AES 128 encryption to help prevent unauthorized access to your startup disk. The Advanced Encryption Standard with 128-bit keys (AES-128) is approved by the U.S. Secretary of Commerce for information technology encryption.

If you store sensitive content on your Mac, consider using FileVault. Say, for example, you lose your Mac, and it contains your business's financial data. Then an unauthorized person finds your Mac, accesses the data, and hurts your business. If you had enabled FileVault and logged out of your account, the data would have been protected.

When you turn on FileVault, you get a recovery key. You can use it to unlock the startup disk if you forget your administrator login password.

To ensure security, other security features are also turned on when you turn on FileVault. For example, you need a password to log in after your Mac does the following:

- Wakes from sleep
- Leaves the screen saver

After initial startup, only users who are enabled in FileVault can log in. Other users need an administrator to log in.

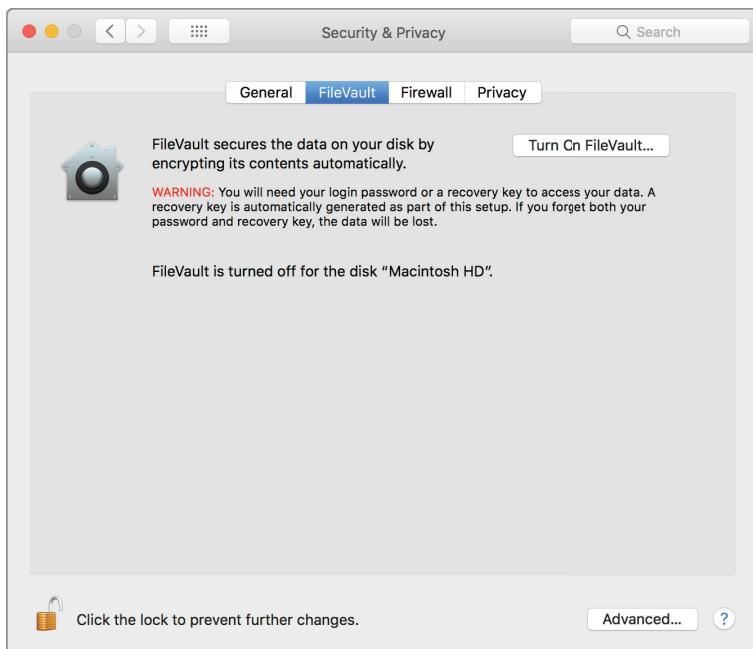


Note: If you turn on FileVault and forget your login password, Apple ID, and recovery key, you won't be able to log in to your account, and your files and settings will be lost.

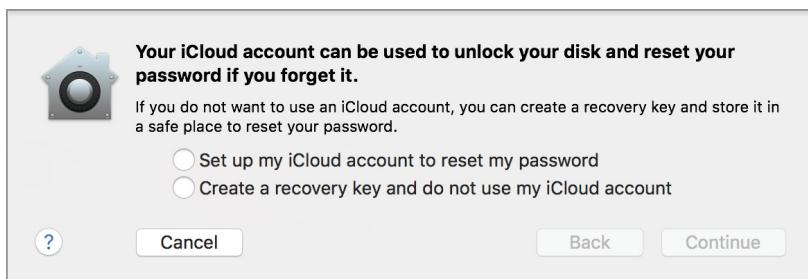


Set up FileVault

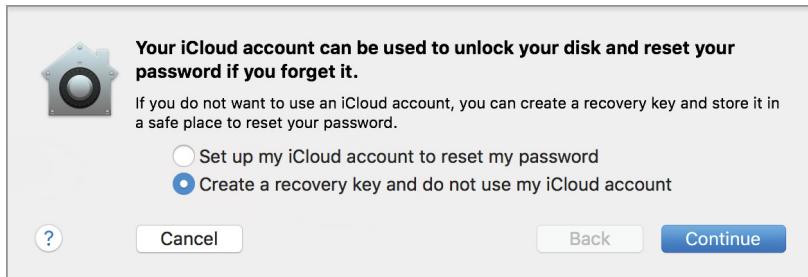
1. Open System Preferences.
2. Click Security & Privacy.
3. Click FileVault.
4. If the lock icon (🔒) is locked, click to unlock it.
5. Enter your administrator user name and password.
6. Click Unlock.
7. Click Turn On FileVault.



macOS presents the option to use your iCloud account to reset your password or create a recovery key.



- Choose "Create a recovery key and do not use my iCloud account."



- Click Continue.

A dialog appears with a recovery key you can use to unlock the disk if you forget your password.



- Copy the recovery key and store it in a safe place.

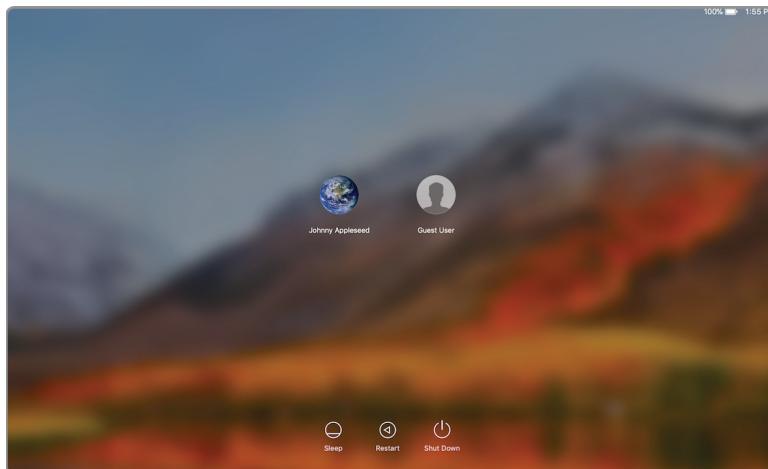


Note: If you forget your password and lose the recovery key, all data on your disk is unrecoverable.

- Click Continue.

FileVault begins the encryption process. You can use the Mac while FileVault encrypts the disk.

After you restart your Mac, the login window displays only the names of the users who can unlock the disk.



If you turn on Find My Mac in iCloud preferences, you also see the Guest User listed in the login window. If someone selects the Guest User at the login window of a stolen Mac, they have limited access to the system, but they can join a Wi-Fi network. When the stolen Mac is back online, the owner can use Find My Mac to locate it.

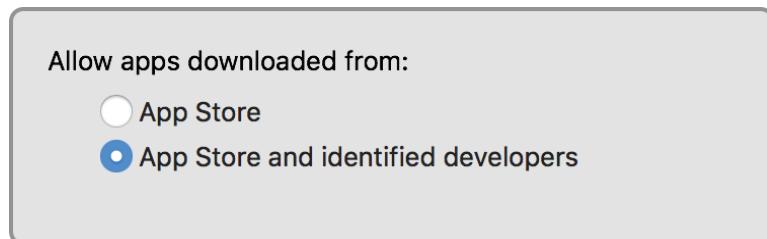
Even though it looks like macOS is running, the startup disk is locked, and macOS won't run until you follow these steps to unlock the startup disk:

1. Select a user who can unlock the disk.
2. Enter the user's password.
3. Click the right arrow or press Return.

Ensure that the apps you download are safe

Gatekeeper protects you from inadvertently opening potentially malicious apps. It gives you two options:

- You can download and install apps only from the App Store.
- You can download apps from the App Store and from identified developers.



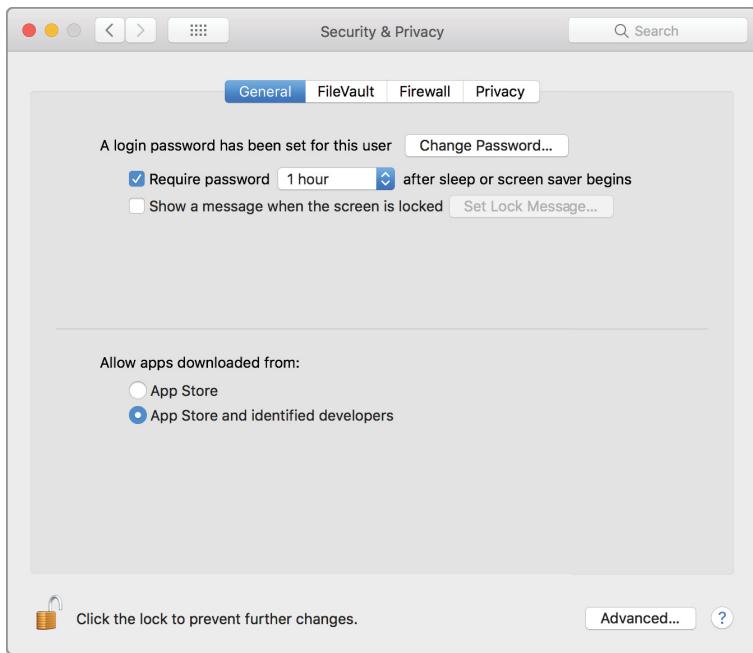
Apple reviews each app before it's added to the App Store. If an app develops a problem, Apple can quickly remove it.

Developers can get a unique Developer ID from Apple and use it to digitally sign their apps. If an app was developed by an unknown developer (one with no Developer ID), Gatekeeper blocks you from opening it.

Set allowed app sources

1. Open System Preferences.
2. Click Security & Privacy.
3. Click General.

4. Choose the software sources that you want to allow.

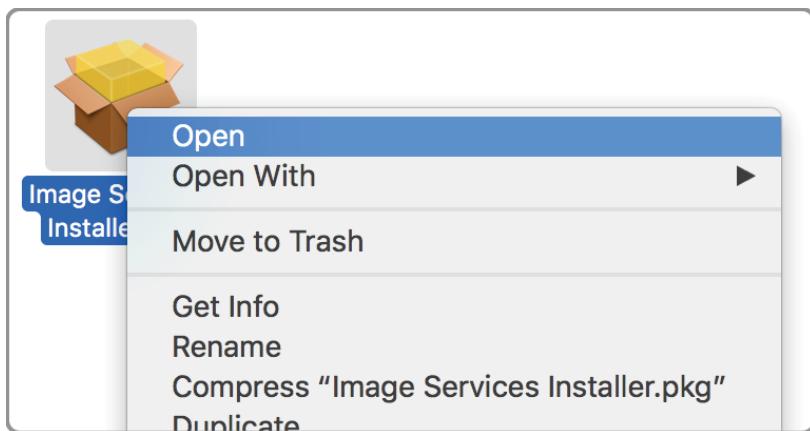


In addition to certain apps, other files might be unsafe. Scripts, web archives, kernel extensions, and Java archives can harm your Mac. An alert appears when you try to open these types of files. Be careful when you open any downloaded file.

If you are confident that an item you downloaded from the Internet is the latest version and is from a source that you trust, you can open it, even if the developer is unidentified.

Open an item that's blocked by Gatekeeper

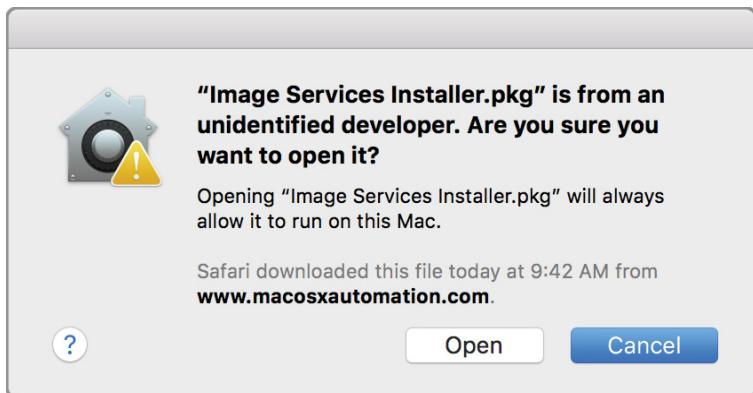
1. In the Finder, press and hold the Control key and click the item icon.



2. Choose Open from the shortcut menu.

You see a prompt that says that opening the item will always allow it to run on this Mac.

3. Click Open.



The item is saved as an exception to your security settings. You can open it in the future by double-clicking it, just as you can any authorized item.

Provide network security

Network security is just as important as user account and system security. The macOS firewall protects your Mac from unauthorized access by other systems on local networks and the Internet. The virtual private network (VPN) provides a secure way for your Mac to remotely access networks.

Turn on the macOS firewall

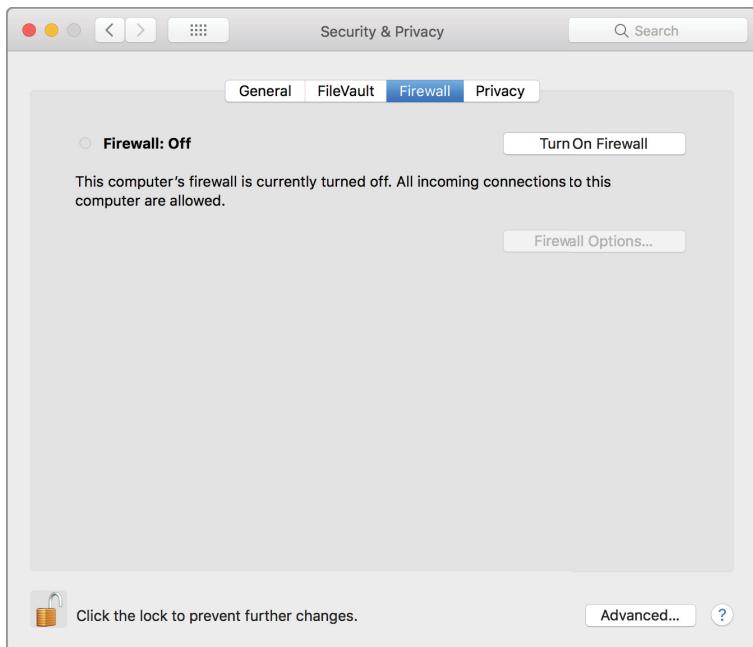
You can use the macOS personal firewall to block unwanted incoming connections to your Mac. A firewall protects the services on your Mac from other computers on the network or Internet. Services that are turned on in Sharing preferences appear in the list of services that other computers can connect to. To prevent incoming connections to these services, you must turn off the services in Sharing preferences.



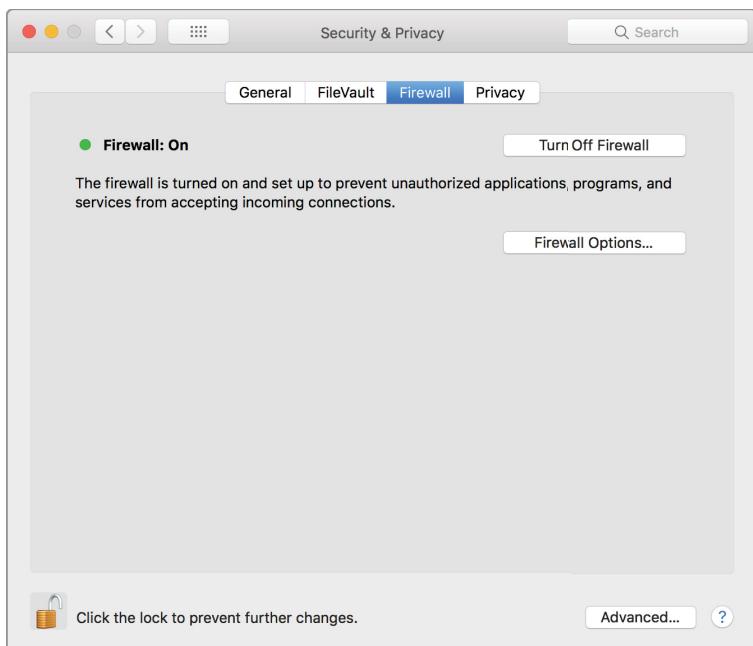
Turn on the macOS firewall

1. Open System Preferences.
2. Click Security & Privacy.
3. Click Firewall.
4. If the lock icon (🔒) is locked, click to unlock it.
5. Enter your administrator user name and password, and then click Unlock.

6. Click "Turn On Firewall" to enable the firewall.



7. Click the lock to prevent further changes.

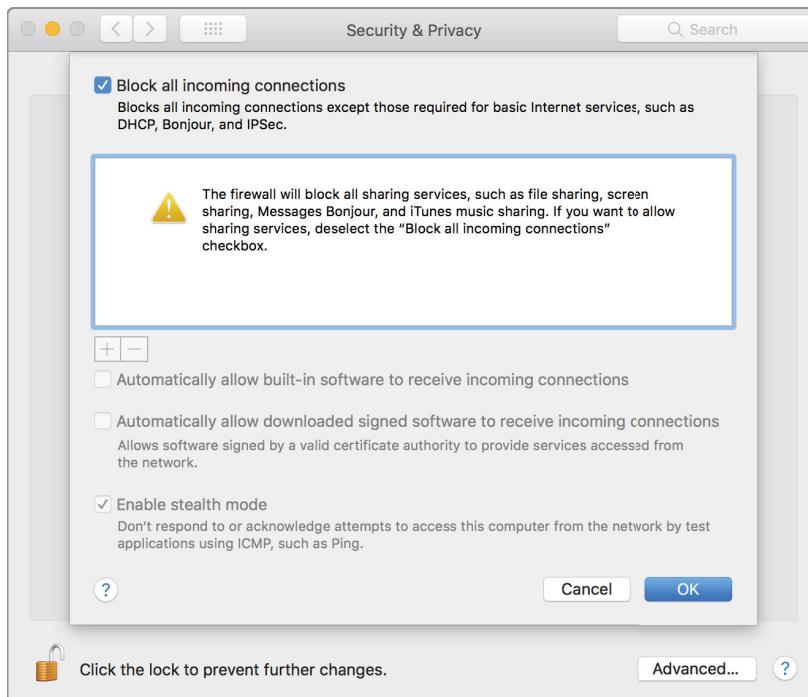


Configure advanced firewall options

1. If the lock icon (🔒) is locked, click to unlock it.
2. Enter your administrator user name and password, and then click Unlock.
3. In the Firewall pane of Security & Privacy preferences, click Firewall Options.

4. Select the firewall type or types you want:

- **Block all incoming connections:** Select this checkbox to allow incoming connections for basic Internet functions. You can check email and browse the web, but Sharing services won't be able to receive incoming connections. To use Sharing services, deselect this option.



- **Automatically allow built-in software to receive incoming connections:** Select this checkbox to allow built-in apps to be added automatically to the allowed-apps list. By making this choice, you won't be prompted to authorize the apps. For example, because Calendar is built by Apple, it's automatically allowed to receive incoming connections through the firewall.
- **Automatically allow signed software to receive incoming connections:** Select this checkbox to allow apps signed by a valid certificate authority to be automatically added to the allowed-apps list. By making this choice, you won't be prompted to authorize the apps. For example, because the app SubEthaEdit has a valid certificate, it's automatically allowed to receive incoming connections through the firewall. If you run an unsigned app that isn't listed in the firewall list, a dialog appears with options to allow or deny connections for the app. If you choose Allow, macOS signs the app and automatically adds it to the firewall list. If you choose Deny, macOS adds it to the list but denies incoming connections that are intended for this app.



- **Enable stealth mode:** Select this checkbox to prevent unauthorized or unexpected probes from receiving a response from your Mac. Your Mac will still answer requests for authorized apps. But other requests, such as network pings from other computers trying to discover your Mac, won't get a response. Stealth mode doesn't prevent your Mac from using Bonjour to advertise services like File Sharing and Screen Sharing that you turned on for your Mac.
5. Click OK when you're done making changes to the Firewall options.
 6. Click the lock to prevent further changes.

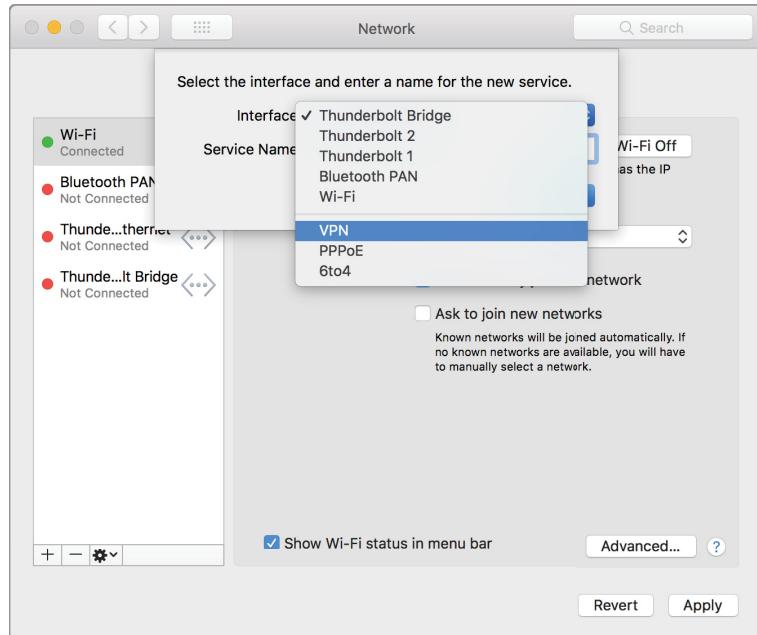
You've configured the built-in Firewall service and increased incoming network connections security.

Connect to a VPN service

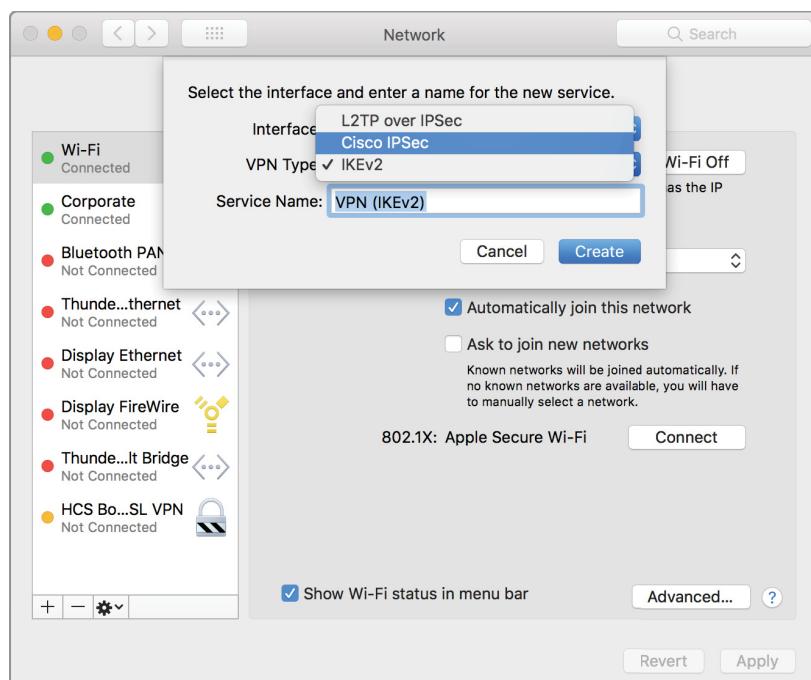
With VPN access, you can use network services while you're offsite and prevent access by unauthorized individuals. Through a built-in VPN client, macOS supports the following standards-based protocols to provide encrypted VPN connections:

- Layer 2 Tunneling Protocol over IPSec (L2TP/IPSec)
 - Internet Key Exchange (IKEv2) over Internet Protocol Security (IPSec) (IKEv2/IPSec)
 - Cisco IPSec
 - SSL VPN clients on the App Store, such as those from AirWatch, Aruba, Check Point, Cisco, F5 Networks, MobileIron, NetMotion, Open VPN, Palo Alto Networks, Pulse Secure, and SonicWall
1. Ask your network administrator for the following information:
 - VPN server address
 - VPN type
 - VPN account name
 - User authentication information

2. Open System Preferences.
3. Click Network.
4. Click Add (+) at the bottom of the network connection services list.
5. Choose VPN from the Interface pop-up menu.

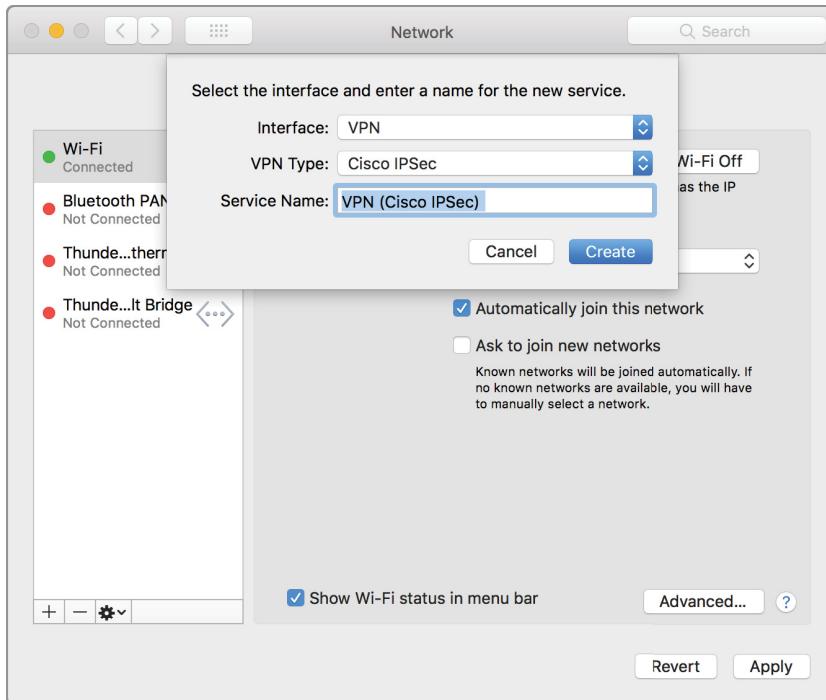


6. Choose the kind of VPN connection you want to set up from the VPN Type pop-up menu.

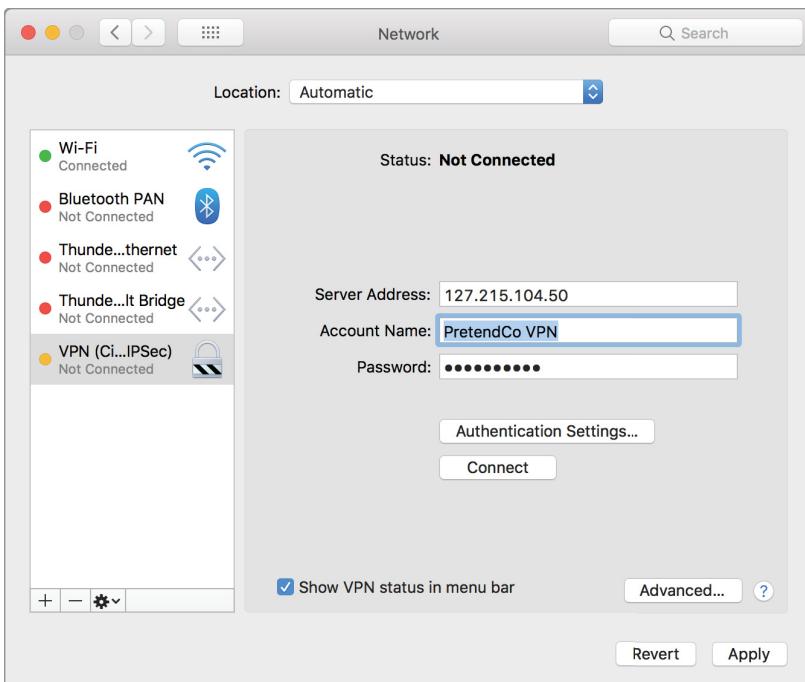


7. Give the VPN service a name.

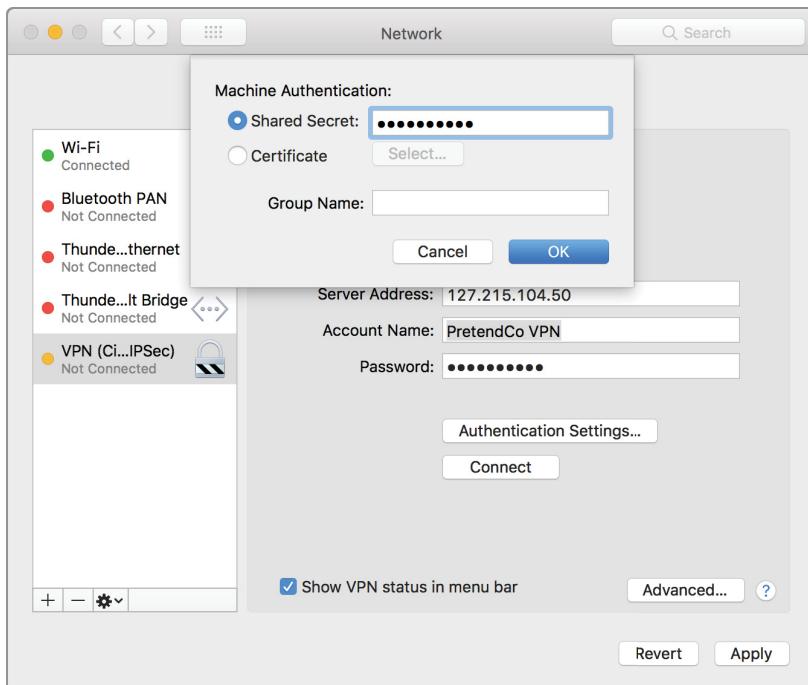
8. Click Create.



9. Enter the server address and the account name for the VPN connection.



10. Click "Authentication Settings" and select an authentication type.



11. Click OK, and then click Apply.

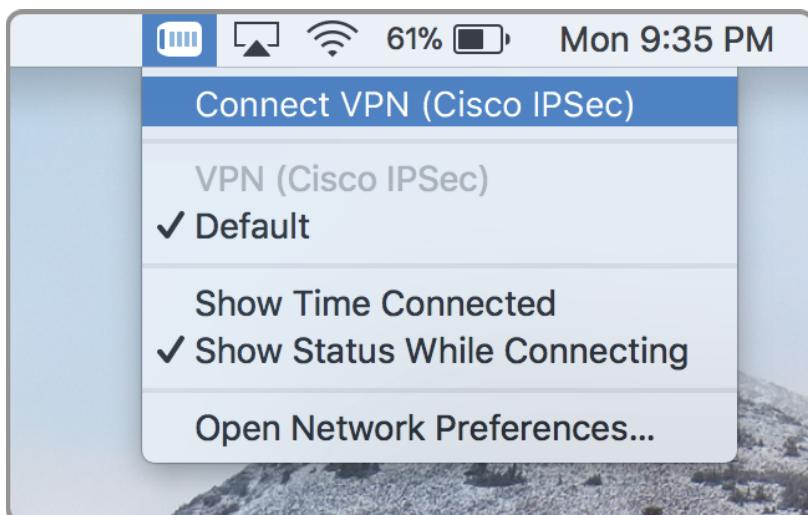
12. In the list of network services, select the VPN service you just created.

13. Select "Show VPN status in menu bar."

This option enables you to use the VPN status button to connect to the network and switch between VPN services.

14. Click the VPN icon in the menu bar.

15. Choose Connect for your VPN connection.



You can now connect remotely to your network and maintain security.

Summary

In this section, you learned how to secure a Mac at the user data, system, and network levels. You should now be able to perform these actions:

- Improve user account security for your Mac by using strong passwords.
- Use two-factor authentication.
- Set a firmware password for low-level system protection.
- Lock a Mac screen.
- Disable automatic login.
- Configure FileVault to protect your startup disk files.
- Use Gatekeeper to open safe apps.
- Configure the macOS firewall to restrict incoming network access to services and data by other computers.
- Configure your Mac to securely access a remote network using the VPN service.

Print



With macOS, you can quickly connect to and share a local printer. You can also use remote printers on a network. Mac computers can share printing resources with Windows computers, so both types of computers can access common printers.

In this section, you'll learn how to perform these tasks:

- Configure your Mac to print to a locally connected printer.
- Configure your Mac to print to networked printers:
 - With AirPrint
 - Over the Internet
- Optimize network printers.
- Share a printer with Windows users



Connect to a local printer

To make sure you have the latest software, don't install the software that came with the printer or from the manufacturer's website. macOS prompts you to download the latest software if it's needed. If a print queue is not automatically created when you connect a USB printer, follow these instructions.

[Add a USB printer](#)

1. In the App Store, click Updates.
2. Install the listed software updates.

Even if no updates appear, this step ensures that macOS has the latest information about printer software that it can download from Apple. If you don't take this step, you might see a message that software isn't available when you connect your printer.

3. Use the instructions that came with your printer to unpack it, install ink or toner, and add paper.
4. Turn on the printer and make sure it doesn't display errors.
5. Connect the USB cable to your Mac.
6. If you see a message that prompts you to download new software, download and install it.
7. Open System Preferences.
8. Click Printers & Scanners.
9. Click Add (+).
10. Select a printer from the list of printers.



Connect to, share, and print from network printers

You can connect to printers on your local network that use Bonjour, IP, and Open Directory, and you can connect to shared printers. If your printer has built-in Bluetooth or Wi-Fi, you can print to it wirelessly.

To help you set up your printer, Mac uses AirPrint to print to an AirPrint-enabled printer over a Wi-Fi, Ethernet, or Universal Serial Bus (USB). If a printer isn't AirPrint enabled, macOS can automatically download the latest printer software in most cases.

If you haven't connected your AirPrint enabled printer to your Wi-Fi network, see [Connect an AirPrint printer to a Wi-Fi network](#). You might be able to use a USB connection to set up Wi-Fi printing. After you add the printer through USB, disconnect the USB cable from the printer and Mac. The printer should remain connected to the Wi-Fi network.

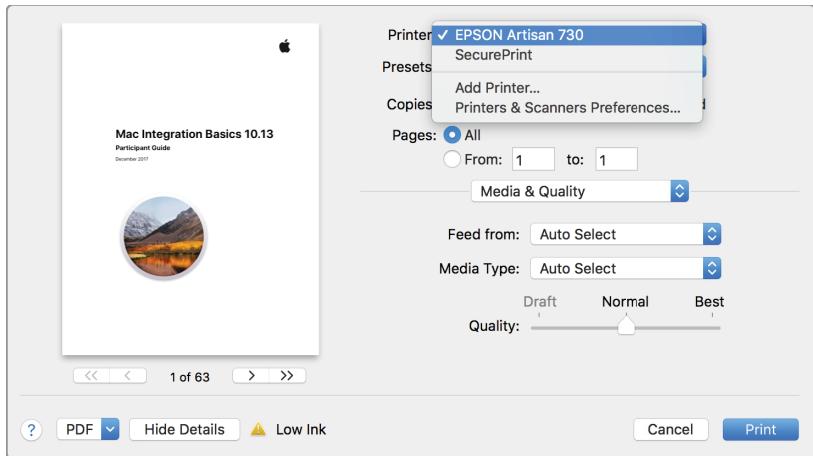
[Set up a printer with built-in Wi-Fi](#)

If you have an AirPrint printer, you don't need to check for software updates.

1. In the App Store, click Updates and install listed software updates.

Even if no updates appear, this step ensures that macOS has the latest information about printer software that it can download from Apple. If you don't take this step, you might see a message that software isn't available when you connect your printer.

2. Use the instructions that came with your printer to unpack the printer, install ink or toner, and add paper.
3. Turn on the printer and make sure it doesn't display any errors.
4. Open a document to print and choose File > Print.
5. Open the Printer pop-up menu and choose your printer in the Nearby Printers section of the menu.



Set up a Bluetooth printer

If you have an AirPrint printer, you don't need to check for software updates.

1. In the App Store, click Updates, then, and install listed software updates.

Even if no updates appear, this step ensures that macOS has the latest information about printer software it can download from Apple. If you don't take this step, you might see a message that software isn't available when you connect your printer.

2. Use the instructions that came with your printer to unpack the printer, install ink or toner, and add paper.
3. Turn on the printer and make sure it doesn't display errors.
4. Open a document to print and choose File > Print.
5. Open the Printer pop-up menu and choose Add Printer.
6. Select your Bluetooth printer and click Add.

If your printer isn't in the list, Bluetooth might not be enabled on your Mac.

7. Turn the printer on in Bluetooth preferences.

Set up an IP printer

If a network printer you want isn't in the Printers list, you can add it as an IP printer. An IP printer must support one of these printing protocols:

- Internet Printing Protocol (IPP)
- Line Printer Daemon (LPD)
- HP Jetdirect (Socket)

Add and print from an IP printer

1. Get the information listed below. If you need help, contact the person who manages the printer or server.

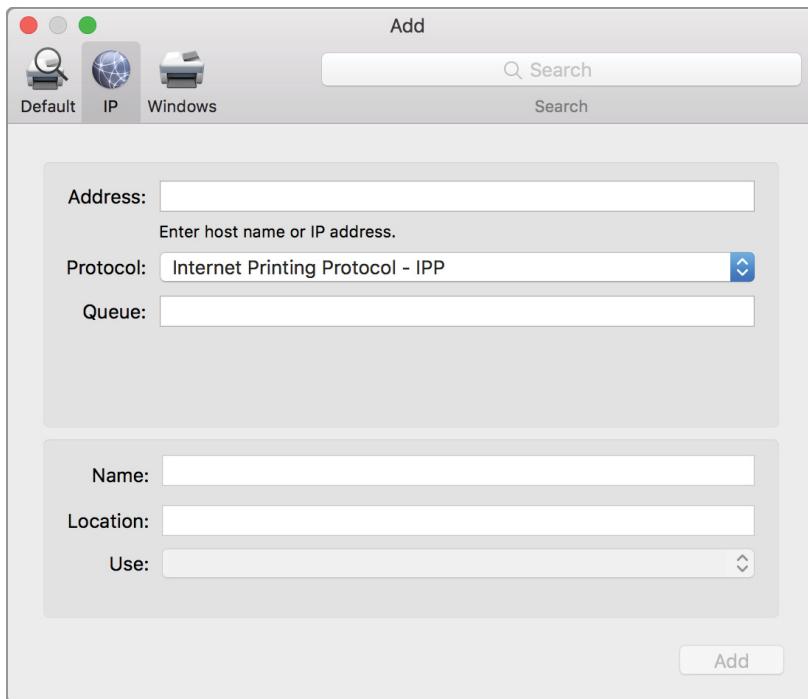
- The network printer IP address or hostname
- The printing protocol being used
- The network printer model number or printer software name
- The printer queue name, if the printer uses a special queue

2. On your Mac, choose Apple menu > Software Update (if you don't have an AirPrint printer).

This step ensures that macOS has the latest information about the printer software that it can download from Apple. macOS updates its list of available printer software and downloads the software as needed when you add printers.

If you have an AirPrint printer, you don't need to check for software updates.

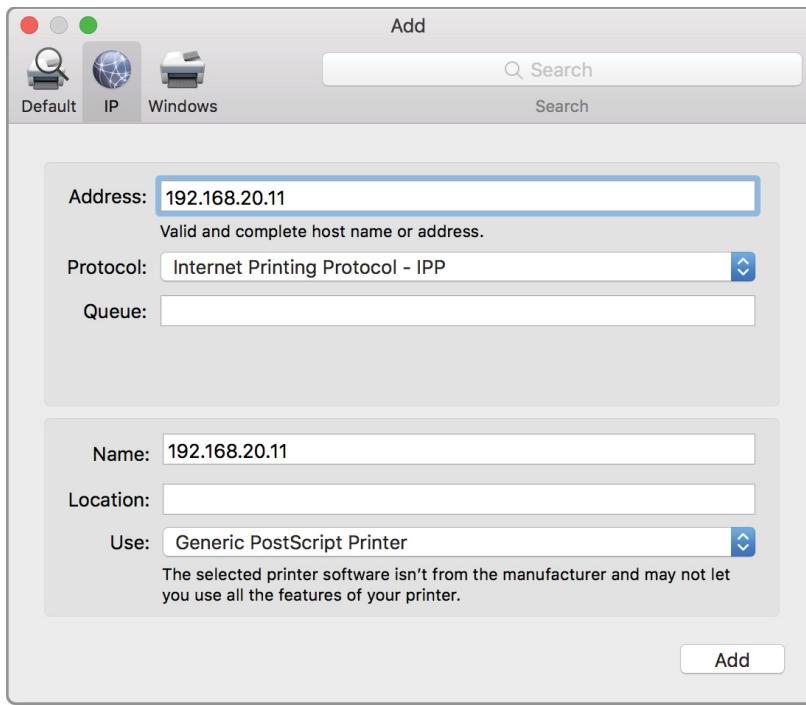
3. Ensure that the printer is connected to your network and ready to print.
4. Open a document to print and choose File > Print.
5. Choose Add Printer from the Printer pop-up menu.
6. Click IP.



7. Enter the printer information. Use the following table as a guide:

Option	Description
Address	Enter the printer IP address (for example, 192.168.20.11) or hostname (for example, printer.example.com).

Option	Description
Protocol	<p>From this pop-up menu, choose a printing protocol that your printer supports:</p> <ul style="list-style-type: none"> • AirPrint: The AirPrint protocol enables Wi-Fi, USB, and Ethernet network access to a printer's printing and scanning options (if the specific printer supports these features). You don't need to download or install printer software to use AirPrint-enabled printers. • Internet Printing Protocol (IPP): Modern printers and printer servers use this protocol. • Line Printer Daemon (LPD): Older printers and printer servers might use this protocol. • HP Jetdirect-Socket: HP and other printer manufacturers use this protocol.
Queue	<p>If your printer requires it, enter the queue name for your printer. If you don't know the queue name, leave it blank, or see your network administrator.</p>
Name	<p>Enter a descriptive name for the printer (for example, "Color Laser Printer") so you can identify it in the Printer pop-up menu.</p>
Location	<p>Enter the printer location (for example, "Outside my office") so you can identify it in the Printer pop-up menu.</p>
Use	<p>If the pop-up menu doesn't show the software for your printer, choose Select Printer Software. Then select your printer in the Printer Software list. If that list doesn't include your printer, install the printer software (printer driver) from the printer manufacturer. You can also choose generic printer software from the pop-up menu.</p>



You can share a printer that's connected to your Mac with another Mac or with a Linux or UNIX computer. The other computers must be on the same local network as your Mac. You don't need to share network printers, because they're already shared on the network.

8. Click Add.

You can print to a printer that's connected to a Windows computer if the printer supports SMB or CIFS.

Add a printer that is shared by a Windows computer

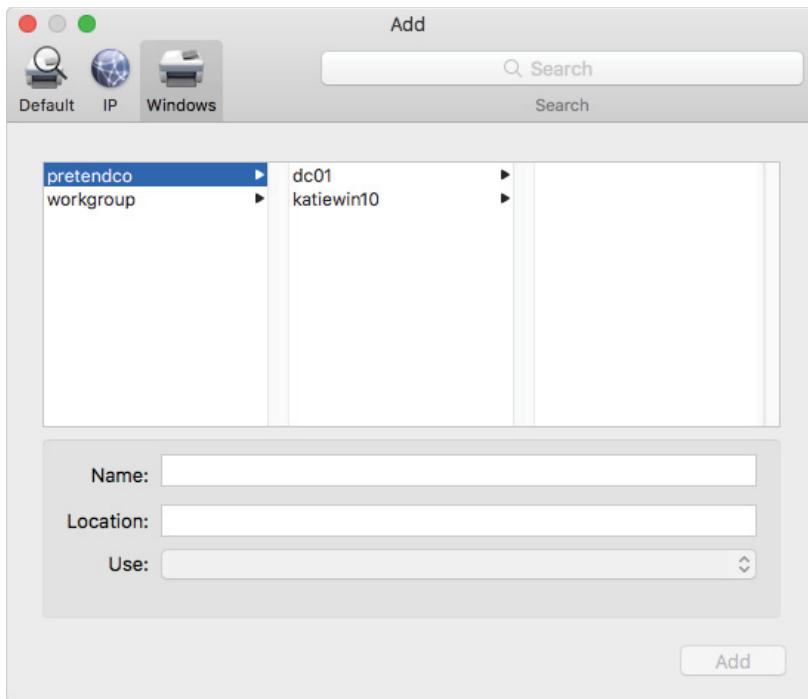
1. Collect this information:

- Windows computer name
- Windows computer workgroup name, if it is not joined to Active Directory
- Windows computer domain name, if it is joined to Active Directory
- Printer name
- Name and password for the Windows computer that has access to print to the printer

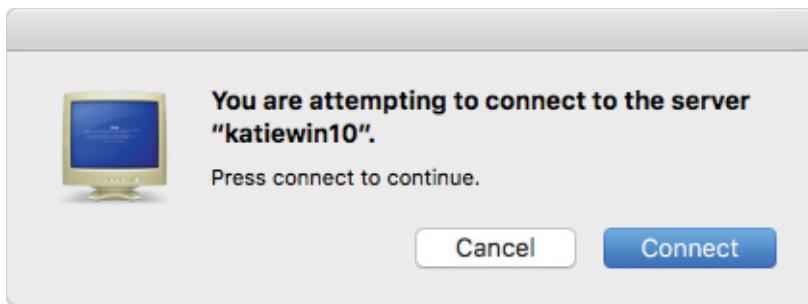
2. Open a document to print and choose File > Print.

3. Choose Add Printer from the Printer pop-up menu, then click Windows.

A network browser appears. It lists the Windows workgroups on your network.



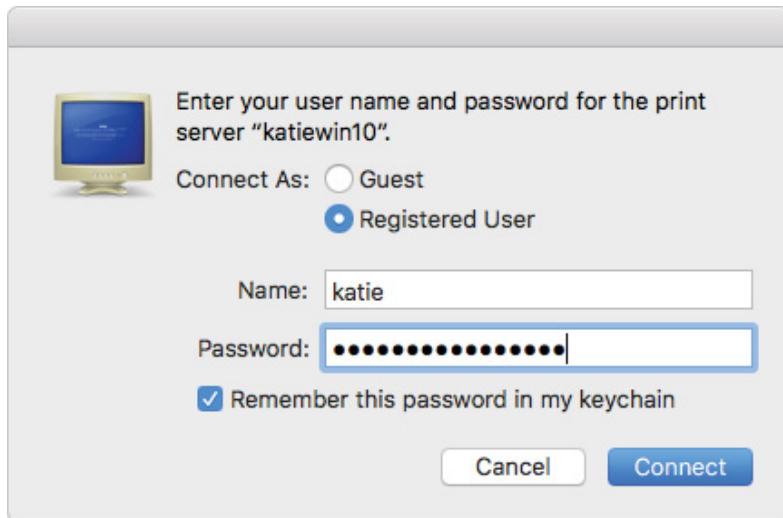
4. Select the workgroup of the computer that shares the printer.
5. Select the print server (the computer that shares the printer).
6. If you receive a notice that you are connecting to the Windows computer, click Connect.



7. Enter the user name and password for the printer.

8. Select the checkbox "Remember this password in my keychain."

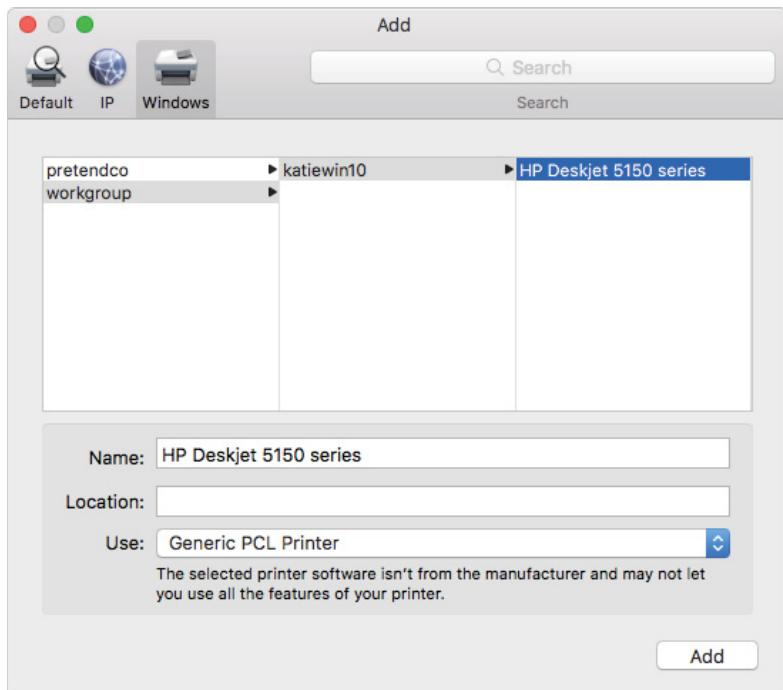
If you don't select this checkbox, macOS creates a Keychain item without a user name and password for this server, and you won't be able to print.



9. Click Connect.

10. Choose the printer software that's appropriate for the shared printer from the User pop-up menu.

Choose the correct printer model for the printer you're adding. For more information, read the documentation that came with the printer. If you have a printer that's compatible with HP Printer Command Language (PCL) but isn't listed, choose the most similar model.



11. Click Add.

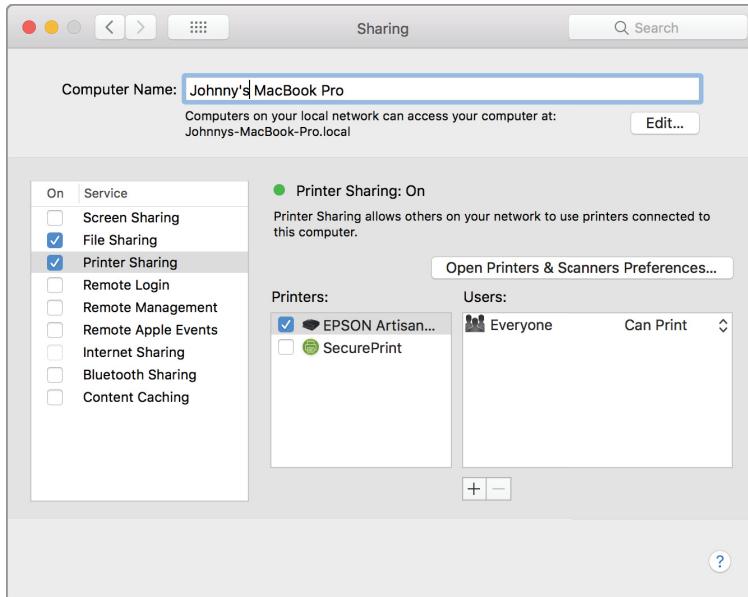
12. If prompted, select the appropriate checkbox for features that the printer supports, and then click OK.

13. Click Print.

If you can't add the Windows printer, your printer software might not support printing though SMB or CIFS. If so, update the printer software on your Mac, or ask your network administrator for help.

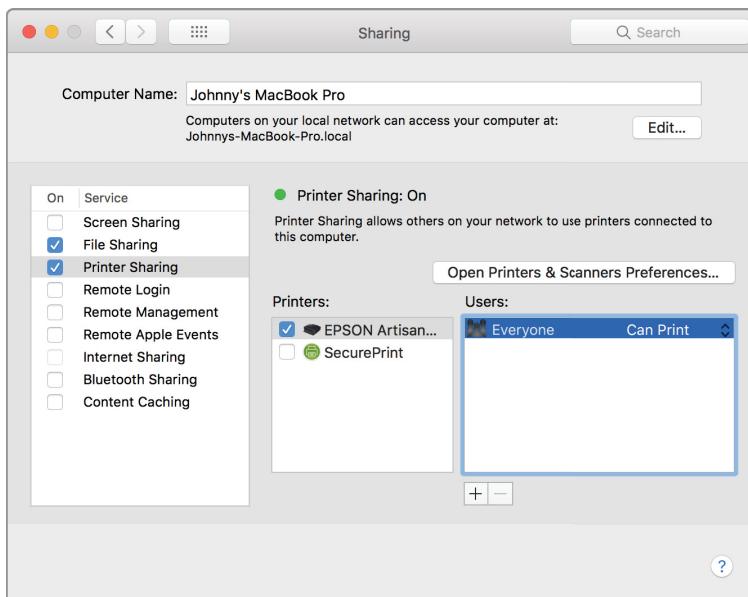
Share your printer

1. Open System Preferences.
2. Click Sharing.
3. Select the Printer Sharing checkbox, if it's not already selected.



4. Under Printers, select the printer you want to share.

When you share a printer, users on your network (Everyone) can use it by default. If you want to restrict access to specific people, continue with steps 5 and 6.



5. Click Add (+) at the bottom of the Users list.
6. Choose one of the following options:
 - Select a user or group from Users & Groups, which includes everyone who has a user account on your Mac.
 - Select a user or group from Network Users or Network Groups, which includes all users and groups from any directory services that you have joined your Mac to. Then click Select.
 - Select a person from your contacts, click Add (+), create a password for the person, click Create Account, and enter and verify a password for the new user. Then provide administrator credentials to create a sharing-only account for your contact.

When you add people to the Users list, access to the shared printer is reset to "No Access for Everyone." "Everyone" is users on your network. If you want Everyone to have access again, click the triangles and choose Can Print.

[Remove a user from the print list](#)

1. Select the user name.
2. Click Remove (-).

You can't remove "Everyone" from a print list.

[Print from a network printer](#)

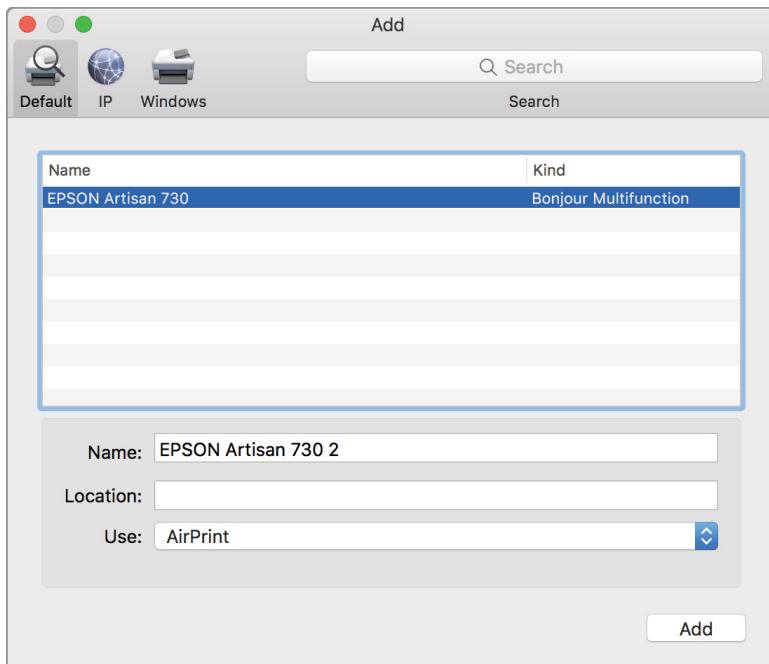
1. Set up the printer using the instructions that came with it.
2. Connect the printer to the network.
3. In the App Store, check for available updates.

This step ensures that macOS has the latest information about the printer software that it can download from Apple. macOS updates its list of available printer software and downloads the software as needed when you add printers.

4. Open a document to print and choose File > Print.
5. Open the Printer pop-up menu and choose your printer in the Nearby Printers section of the menu.
6. If you don't see your printer, choose Add Printer from the Printer pop-up menu.

A dialog appears listing any Bonjour, IP, Open Directory, and shared printers on your local network. Your printer might take a minute or two to appear.

- Select your printer when it appears in the list, and then click Add.



macOS automatically uses AirPrint if your printer supports it, or it selects printer software (also called a printer driver) and downloads it from Apple, if necessary. If you don't see your printer in the list, visit the following sections in this guide:

- Set up a printer with built-in Wi-Fi
- Set up an IP printer

A Mac can usually detect if a printer has special accessories such as the following installed:

- Additional paper trays
- Extra memory
- A duplex unit

If the Mac can't detect them, a dialog appears and you can specify the accessories. Ensure that the settings in the dialog reflect your printer's installed accessories so you can take advantage of them.

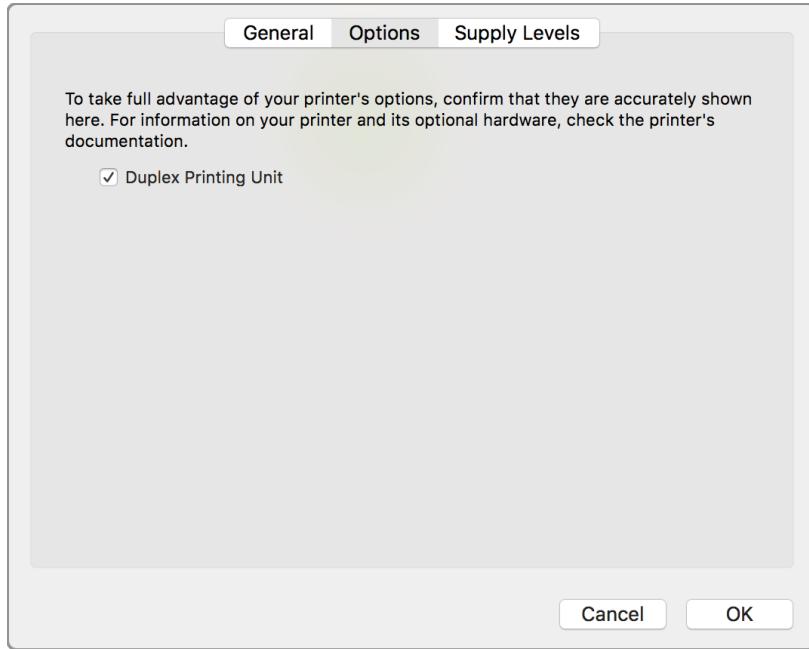
Note: If you connect a printer that has a scanner to a local network, other computers on the network can see what's on the scanner bed. If you scan documents with sensitive information, connect the scanner to your Mac USB port.

Specify printer features

If your printer options weren't detected when you added it to your Printers list, you can specify them. If you modified its features after you added a printer to your Printers list, you might need to update Options. For example, the Print dialog might not display options for two-sided printing because the printer duplex unit wasn't detected. Or you might have moved an extra paper tray from one printer to another and your printer didn't detect the change. If your printer uses AirPrint, printer features are determined automatically, and you can't turn them on or off.

- Open System Preferences.

2. Click Printers & Scanners.
3. Select your printer in the list at the left.
4. Click Options & Supplies.
5. Click Options.
6. Select the options you want to see when you print and click OK.



Summary

In this section, you learned different ways to use a Mac with local and network printers. You should now be able to perform these tasks:

- Configure a Mac to print to a USB printer.
- Configure a Mac to print to a network or Windows printer.
- Share a local printer with network users.
- Specify printer features.

Move and Back Up Content

When you switch from a Windows computer to a Mac, you can transfer and use many of the files you created with common Windows apps. These include text and PDF documents, images, audio, and video files.

Protecting your content is important. You should regularly back up your Mac and keep multiple backups of important content. Your organization might have a specific backup policy, but if it doesn't, a personal backup strategy is best.

In this section, you'll learn how to move Windows computer content to a Mac and back it up.

Move content

Use Migration Assistant to copy your documents, apps, user accounts, and settings to a new Mac from a Windows computer. Migration Assistant copies content to a Mac so that you don't have to do it manually.

If you have a small number of files, you can copy them from the Windows computer to an external storage device. You can use the external storage device to copy content to your Mac.

You can also send Windows files to your Mac using email.

Move content using Migration Assistant

Windows Migration Assistant transfers your content from a Windows computer and puts it in the appropriate places on your Mac.

Prepare to move content:

1. Make sure Windows is up to date.
Migration Assistant works with Windows XP and later.
2. Make sure you know the name and password of an administrator account on your Windows computer.
3. Connect your Mac and Windows computer to the same network, such as your home Wi-Fi network. You can also connect the computers with an Ethernet cable.
4. Use the check disk (chkdsk) utility on your Windows computer to ensure that your Windows drive has no issues.
 - a. Choose Start > Run.
 - b. Enter cmd in the Run window and press Return.
 - c. Enter chkdsk in the command window and press Return.
 - d. If the check disk utility reports that it found problems, enter chkdsk *drive: /F* and press Return.
drive (for example, d) is the letter that represents your Windows startup disk.
 - e. Press the Y key at the prompt.
 - f. Restart your Windows computer.
 - g. Repeat the process until the check disk utility reports no issues.

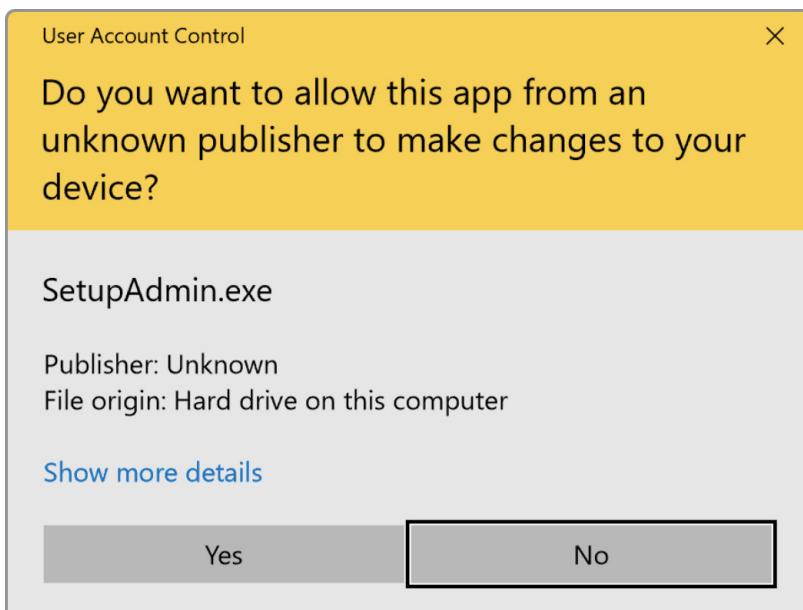
- h. If you can't clear a reported disk issue, get your Windows computer serviced before you migrate content to your Mac.

[Download Windows Migration Assistant to your Windows computer](#)

1. On your Windows computer, download the Windows Migration Assistant and install it.

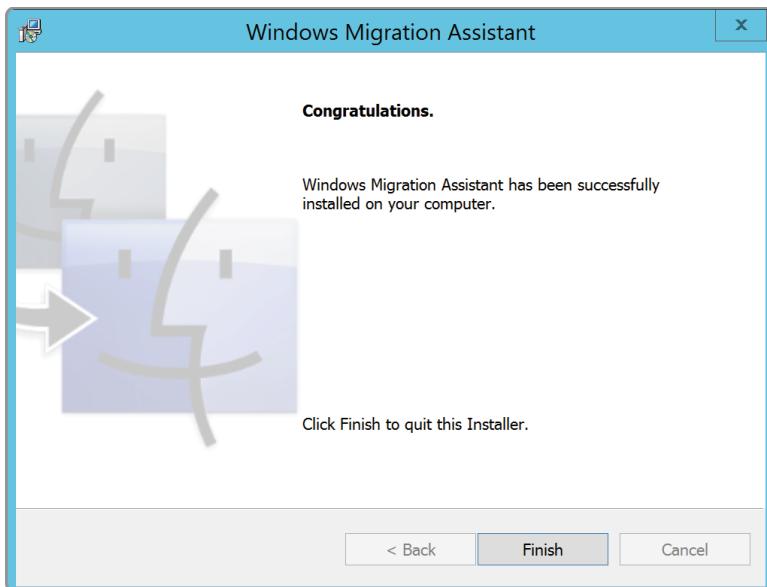


- a. During installation, if you are prompted to allow the app to make changes to your device, click Yes.



- b. During installation, if you are prompted to download and install additional Windows features, click Download and install the features.

The installation leaves a shortcut on the desktop of the current Windows user.



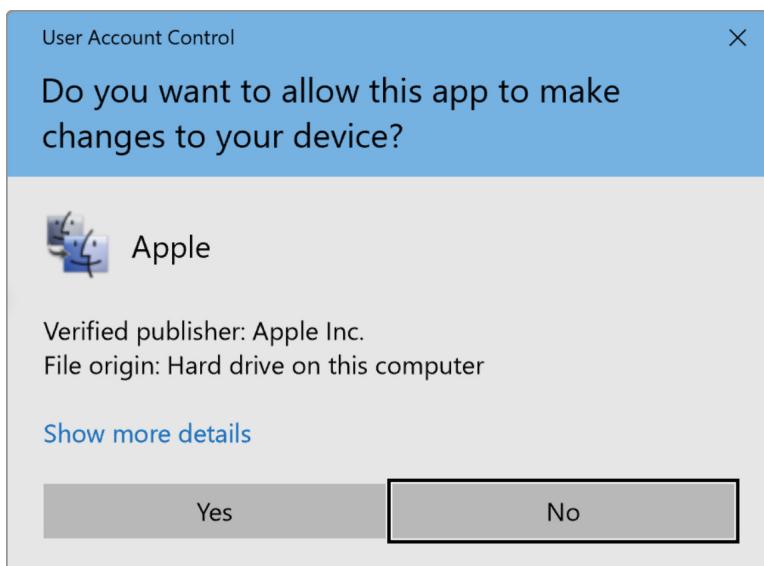
2. Quit other open apps in Windows.

Start Windows Migration Assistant on your Windows computer

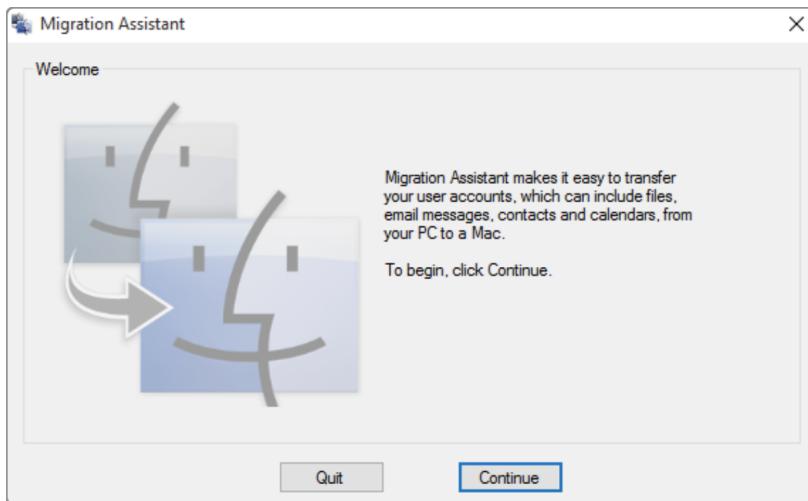
1. Open Windows Migration Assistant



2. If you're asked, "Do you want to allow this app to make changes to your device?" click Yes.



3. Click Continue to start the process.



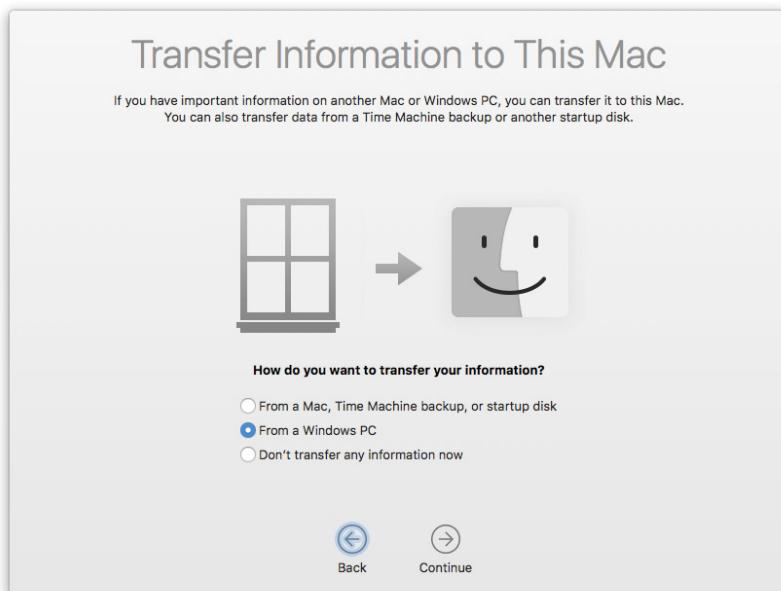
4. To prevent interruption to the migration process, click Continue again.

This disables the automatic installation of Windows updates.

If you haven't set up your Mac

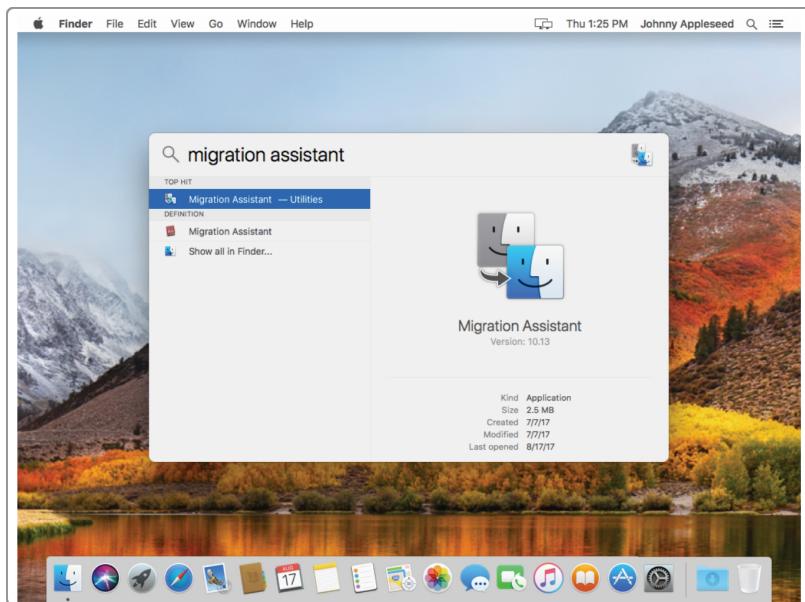
Setup Assistant automatically opens the first time you set up your Mac.

1. Start up your Mac.
2. Complete the Setup Assistant steps until the "Transfer Information to This Mac" window appears.

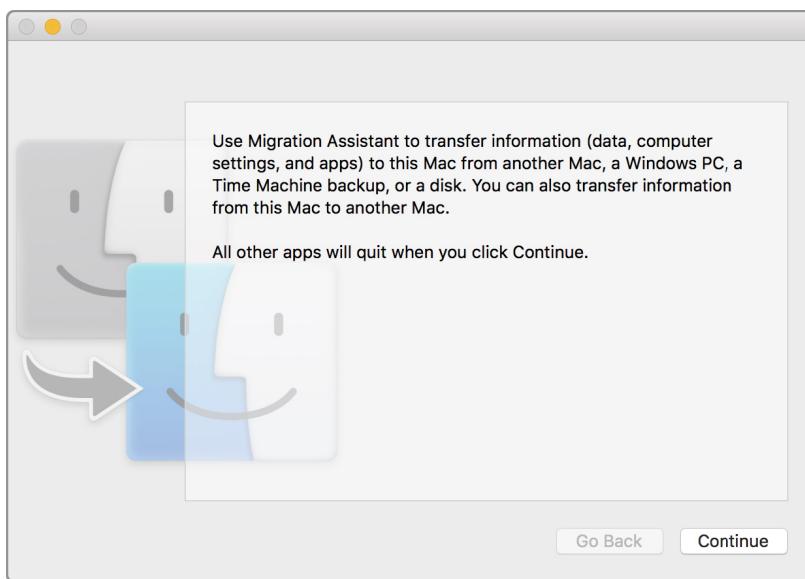


If your Mac is set up

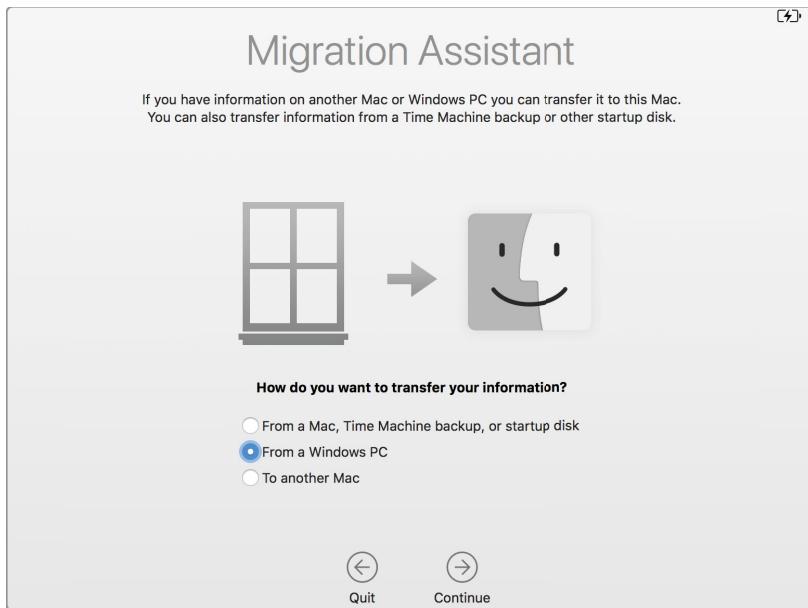
1. Start typing Migration Assistant in Spotlight, then double-click Migration Assistant.



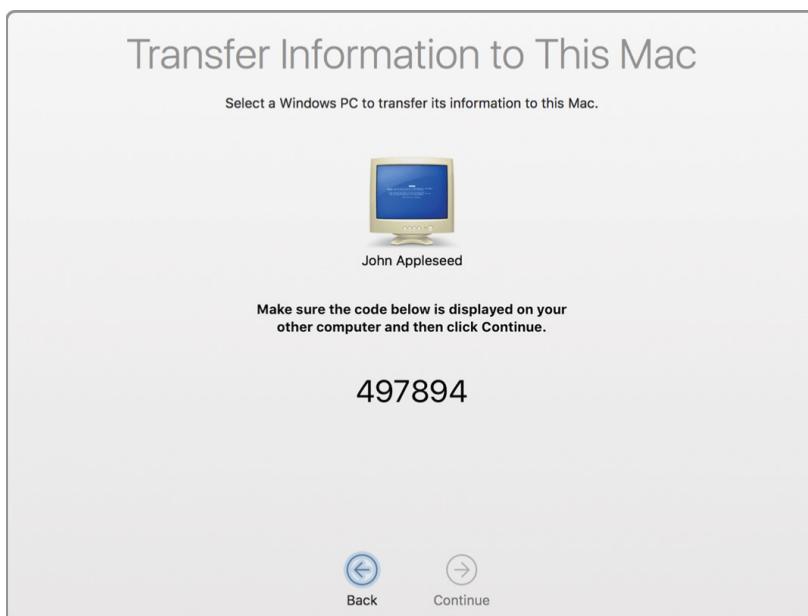
2. If prompted, enter an administrator name and password.
3. Click Continue to close open apps.



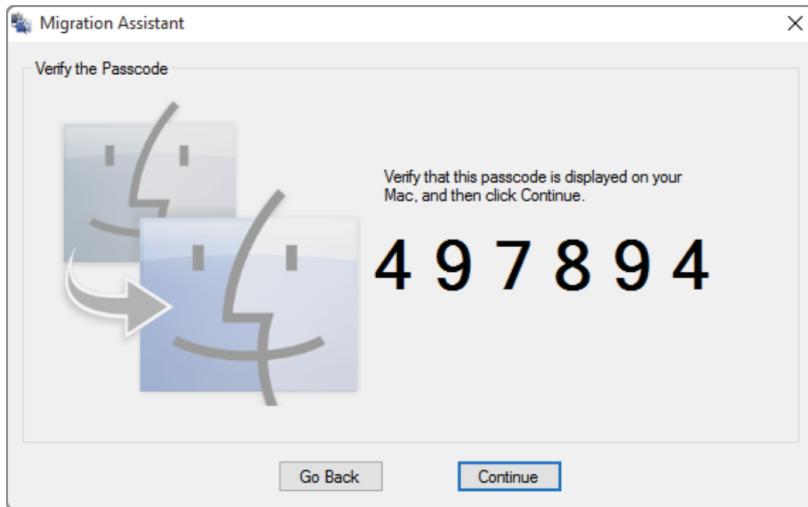
4. Select "From a Windows PC" to transfer information, and click Continue.



5. Select your Windows computer from the list of available computers in the migration window on your Mac, and click Continue.
6. Wait for the Windows computer to show the passcode displayed on the Mac.

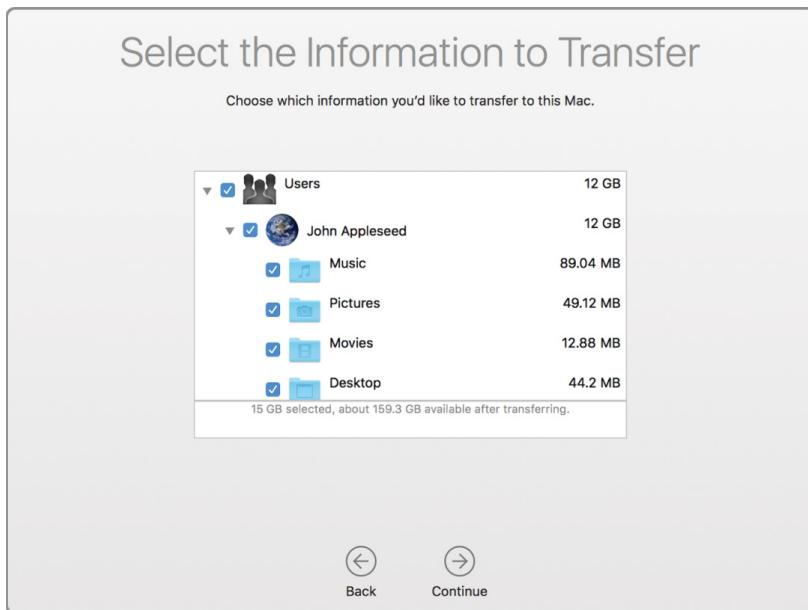


7. When you see the same passcode displayed on both computers, click "Continue on your Windows PC."



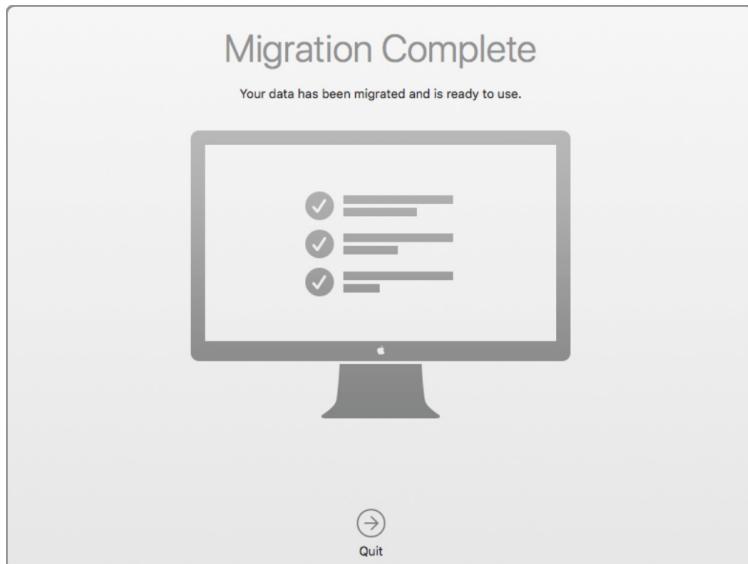
Your Mac scans the drives on your Windows computer to build a list of content to migrate.

8. When the scan is complete, select the content you want to migrate to your Mac, and click Continue.

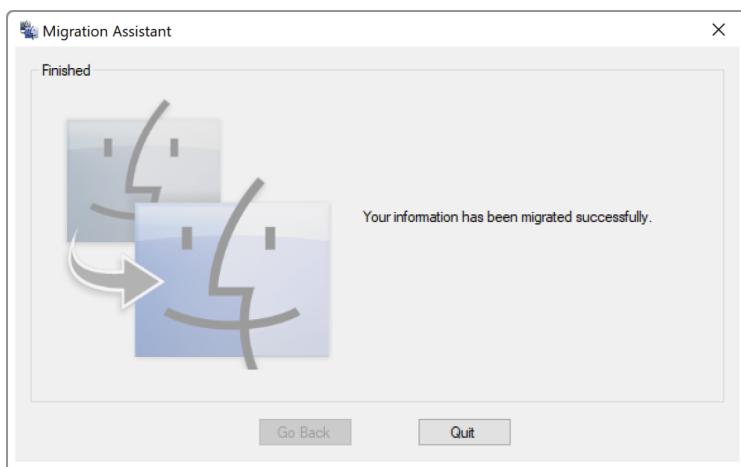


9. Watch the progress and estimated time remaining on both the Windows computer and your Mac.

Migration Assistant tells you when the migration is complete.



10. Close Migration Assistant on your Windows computer.



11. Log in to your new user account on your Mac.

12. The first time you log in to a user account that was migrated from a Windows computer, you're prompted to set a password. You can use the same password you used on your Windows computer or create a new password. Read Choosing good passwords for more information.



Back up content

Time Machine is the built-in backup feature of your Mac. You can back up your content and restore it later with Time Machine. To use it, you need an external storage disk. But your Mac might not always be near your external disk, so Time Machine saves some of its backups to your startup disk. These backups (called local snapshots) are automatically enabled when you turn on Time Machine and disabled when you turn Time Machine off. One daily snapshot is saved every 24 hours, beginning from the time you start or restart your Mac. One weekly snapshot is saved every week. Read About Time Machine local snapshots for more information.

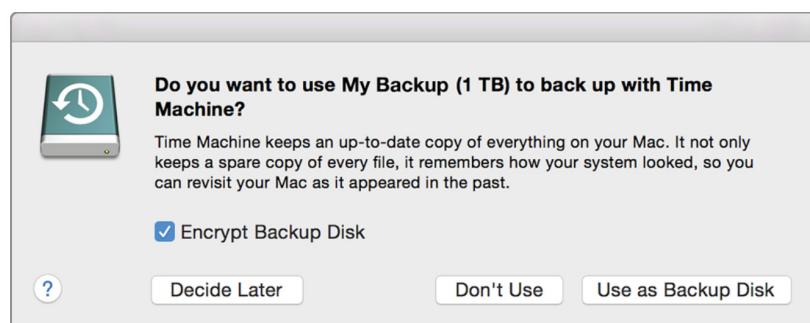
Set up Time Machine

Get one of these backup disks:

- An external disk that you can connect to your Mac through a USB or Thunderbolt port
- AirPort Time Capsule
- An external hard drive connected to the USB port of an AirPort Extreme base station on your network
- Network shared folder configured as a Time Machine backup destination

Read Use a shared folder with Time Machine for more information about sharing a folder that you'll use for Time Machine).

When you connect an external disk directly to your Mac, you might be asked if you want to use the drive to back up with Time Machine. Click "Use as Backup Disk." If you select the option to encrypt, your backups will be accessible only to users with the password.



If Time Machine doesn't ask you to choose a backup disk

1. Open Time Machine preferences from the Time Machine menu in the menu bar. Or choose Apple menu > System Preferences, and click Time Machine.
2. Click Select Backup Disk.
3. Select an external disk, Time Capsule, or other storage solution from the list. Optionally, select "Encrypt Disk" to encrypt, and click Use Disk.
4. If you selected a network disk, provide the user name and password for an account that has permission to use the network disk, and then click Connect.
5. After you choose a backup disk, you can click "Add or Remove Backup Disk" to add more backup disks for extra security and convenience.
6. When you are asked if you want to stop backing up to one disk and use a different disk instead, click Use Both.

Customize Time Machine

After you set up Time Machine, it automatically makes hourly backups for the past 24 hours, daily backups for the past month, and weekly backups for all previous months. The oldest backups are deleted when your backup drive is full.

- To back up now instead of waiting for the next automatic backup, choose Back Up Now from the Time Machine menu ⌘.

- To stop automatic backups, turn off Time Machine in Time Machine preferences. You can still back up manually by choosing Back Up Now from the Time Machine menu.
- To cancel a backup in progress, choose Skip This Backup (or Stop Backing Up) from the Time Machine menu.
- To check backup status, use the Time Machine menu. The icon shows when Time Machine is backing up , idle until the next automatic backup , or unable to complete the backup .
- To exclude items from your backup, open Time Machine preferences from the Time machine menu, click Options, and then click Add (+) and select the item to exclude.

Your first backup might take a long time, depending on how many files you have. You can continue to use your Mac during a backup. Some Mac computers make backups even when they're asleep. Time Machine backs up only the files that changed since the previous backup, so future backups will be faster. For more information, see support information about Time Machine backups and Power Nap.

Summary

In this section, you learned about migrating content from a Windows computer to a Mac. You also learned how to back up your content and protect against data loss. You should now be able to perform these tasks:

- Migrate content from a Windows computer to a Mac.
- Set up Time Machine.
- Back up content with Time Machine.

Run Windows on a Mac

In this section, you'll learn about the following topics:

- Different ways to install and run Windows
- How to install Office and how it works well with macOS
- Which apps have versions available for macOS and Windows
- Which Mac apps have built-in support for Windows files



Run Windows natively or virtually

A Mac uses the same processor as a Windows computer running Windows. Having the same processor enables a Mac to run Windows natively or virtually. Boot Camp, which is included with macOS, helps you install Windows on your Mac. You can then start up Windows natively. You can also run Windows directly in macOS with virtualization apps such as VMware Fusion, Parallels Desktop, and VirtualBox. These solutions create a virtual Windows computer on your Mac.



Install Windows natively

After you install Windows and restart your Mac, you can easily switch between macOS and Windows. Setup is simple and safe for your Mac content. And after you install Windows, it runs at native speeds. macOS High Sierra supports new installations of Windows 10, Windows 8.1, and Windows 7.

Windows running natively on a Mac

doesn't read from or write to Apple File System (APFS)-formatted volumes. If your Mac has all flash storage, the startup disk for the Mac partition is an APFS volume. If you must access files on your Mac when you run Windows, consider running Windows with virtualization apps instead of starting up Windows with Boot Camp. Boot Camp isn't supported if the startup disk uses a 3 TB Fusion Drive. Read [Prepare for APFS in macOS High Sierra](#) for more information.

You can use Boot Camp and a Windows installation disk (that you provide) to install Windows on a Mac. Windows is installed in its own partition. To find out which versions of Windows your Mac supports, read [System requirements to install Windows on your Mac using Boot Camp](#). While you use Boot Camp, Windows apps have full access to the following:

- Multiple processors
- Multiple cores
- Accelerated 3D graphics
- High-speed ports
- Networking technology (Thunderbolt, Wi-Fi (Airport), USB, and Gigabit Ethernet)

1. Gather these things:

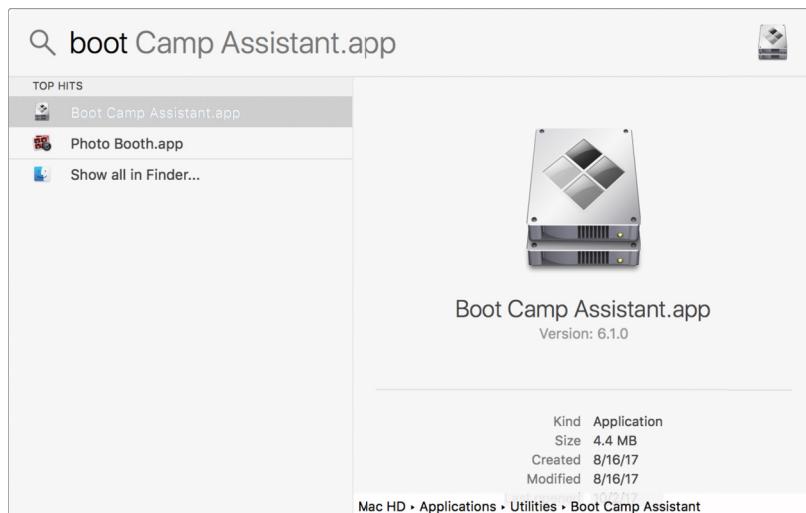
- The keyboard and mouse or trackpad that came with your Mac. If they aren't available, use a USB keyboard and mouse.
- A Microsoft Windows installation media or International Organization for Standardization (ISO) disk image containing a 64-bit version of Microsoft Windows 7 or later. When you buy Windows, it comes as an ISO disk image file that you download, an installation disc, or a USB flash drive. If your copy of Windows came on a DVD, you might need to create a disk image of it to work with Boot Camp. If your version of Windows came on a USB flash drive, you can download an ISO disk image from Microsoft.
- At least 55 GB of free disk space on your startup drive. Some versions of Windows require a certain processor and more hard drive space and memory (RAM) than others. Check the documentation that came with your copy of Windows to find out what you need. Then use System Information to see what your Mac currently has.

Note: If you have an older Mac, you might need an external USB drive to install Windows. If you need one, Boot Camp asks for it when you prepare your Mac. Read Install Windows on your Mac using a USB hard drive or flash drive for more information.

2. Use Time Machine or other methods to back up important content.
3. Start your Mac from macOS and check for software updates to make sure macOS and the firmware are current.
4. Use Boot Camp Assistant to prepare your Mac for Windows.
 - a. Press Command-Spacebar.

This opens Boot Camp Assistant.

- b. Start to type "boot camp Assistant," then double-click the words.



Boot Camp Assistant guides you through installing Windows.

- c. At the Introduction screen, click Continue.



- d. In the Install Windows step, click Choose, then select the ISO image you created or downloaded from Microsoft.
- e. Follow the onscreen instructions to automatically repartition your startup disk and download related software drivers for Windows.

Note: You can't resize the partition later.

- f. Click Install to format your Windows partition.

After you complete the installation with Boot Camp Assistant, your Mac restarts to the Windows installer.

5. When you're asked where you want to install Windows, select the BOOTCAMP partition, then click Format.
6. Follow the onscreen prompts to complete your Windows installation.
7. If you're asked where to install Windows, click Next.

The installation partition is preselected.

Note: Don't create or delete a partition or select another partition. If you do, you might delete the content of your macOS partition.

After you install the Windows software, your Mac automatically restarts using Windows.

8. Use the Windows setup screens to configure Windows.
9. Install Windows support software.

After you install Windows, Boot Camp drivers that support your Mac hardware start installing.

- a. Follow the onscreen instructions.

Note: Don't click the Cancel button in the installer dialogs.

- b. If a message appears that says the software you're installing hasn't passed Windows Logo testing, click "Continue Anyway."
- c. You don't need to respond to installer dialogs that appear only briefly during installation, but if a dialog asks you to install device software, click Install.
- d. If nothing appears to be happening, there may be a hidden window that you must respond to. Look behind open windows.
- e. When the support software finishes installing, click Finish.

10. After your Mac restarts, follow the instructions for other installers that appear.
11. Check for updated Windows support software. In macOS, choose Apple menu > App Store, click Updates, then install available updates.
12. After you install Windows, set the default operating system.
13. Read about the external startup disk in macOS or the Boot Camp control panel in Windows to select your startup disk, then restart your Mac.

Install Windows Virtually

To run macOS and Windows apps simultaneously, install Windows on macOS. You can choose from several solutions, including these:

- VMware Fusion
- Parallels Desktop for Mac
- VirtualBox

You need a full-install Windows installation disk or a Windows ISO disk image of the Windows version you use. After you complete this type of installation, you won't have to restart your Mac to switch between macOS and Windows.

Microsoft Office for macOS

A native version of Office is available for macOS, so you can create and share the following files just as you would on a Windows computer:

- Word documents
- PowerPoint presentations
- Excel spreadsheets

Even if you don't have Office installed on your Mac, you can use Quick Look to view Office documents without opening an app.

Cross-platform apps

Software developers offer versions of their apps for Windows and macOS to accommodate the mixed operating system environments that many organizations use. The following are examples of cross-platform productivity apps:

- Office 365: Includes Word, Excel, PowerPoint and Messaging
- Adobe Creative Cloud: Includes Acrobat, Photoshop, Illustrator, InDesign, After Effects, and Premiere Pro
- Intuit QuickBooks
- The FileMaker Platform

Cross-platform files

Most popular Mac apps use the same file format as their Windows counterparts. You can use a Mac to open and use files that were created in Windows. Using native Mac apps, you can import and export files created in Windows. With these apps, you can view most common file types, including Office documents, PDFs, images, text files, MP3s, videos, and ZIP files. Here's a list of popular Mac apps with support for Windows files:

- Pages: You can import and export Microsoft Word and most other Windows text formats.
- Numbers: You can import and export Excel and Open Financial Exchange (OFX) files from Quicken, comma-separated-values files, and tab-delimited files.
- Keynote: You can import and export PowerPoint presentations.
- Any QuickTime-compatible app: You can import .avi video and .wav audio files.

Summary

In this section, you learned about macOS cross-platform compatibility. This compatibility enables you to work seamlessly with Windows users. You should now be able to perform the following tasks:

- Configure a Mac to run Windows natively with Boot Camp.
- List third-party virtualization solutions for running Windows.
- Describe the benefits of using Office on a Mac.
- List apps that are available on both Windows and macOS.
- List native Mac apps that support Windows file formats.

Resources

Books

Visit Peachpit Press to find out more about the Apple Training Series books.

Courses

A page of basic information about your new Mac on the Apple Support site provides online training materials for new macOS users.

Visit training.apple.com for information about macOS courses.

Certifications

macOS certifications attest to the ability of IT professionals who support macOS users.

Apple Certified Associate - Mac Integration 10.13: This certification verifies that you understand the different ways to integrate a Mac into a Windows or other standards-based network. It also covers the seamless way that macOS users can work with Windows apps and files.

For more information about available Apple Certifications, visit Apple Training and Certification.

Documentation and Support

Apple provides online support where you can access technical articles, download manuals, and join discussion forums. You can start at the Business and Education Support website.