

Running Apps in Mojave

User Advice

Howard Oakley <https://eclecticlight.co>

macOS 10.14 Mojave includes strong features to protect most private information on your Mac. This advice explains those features, as detailed by Apple at WWDC 2018 (session 702), and how you may need to use them when running apps in Mojave. Please read this before trying to access any protected information in Mojave, as it should save you frustration and confusion.

Which information is protected?

Mojave protects information in three categories: prompting (such as Location Services), other data (such as Mail), and special (such as microphone audio). These in turn break down as follows.

Prompting:

- Location Services,
- Contacts (address books),
- Calendars,
- Reminders,
- Photos (Photos libraries).

Other data:

- Mail,
- Messages,
- Safari browsing history,
- HTTP cookies,
- Call history (iOS),
- Time Machine backups,
- iTunes backups.

Special:

- camera input,
- audio input through the built-in microphone,
- automation (AppleScript and others).

When you use apps to access all other data, the only protection which should be applied to it is that set by standard folder and file permissions, which still work in the normal way.

How can apps access protected information?

In many cases, the best way to access protected information is to export it from that protection. For example, a document attached to a message will be protected as long as it remains an attachment, and is stored in your Mail folder. When you save that attachment to your Documents folder, then that saved copy is no longer specially protected, and can be used normally.

Running Apps in Mojave

User Advice

Howard Oakley <https://eclecticlight.co>

There are situations in which you need to access protected information where it is, perhaps if you are experiencing a problem with those protected files and need to check them using a tool. Most apps and tools intended to be used for this purpose should have settings which will help enable this, but you might wish to use an app for an unusual purpose. For example, you might want to check whether an image in a Photos library has versions or extended attributes associated with it.

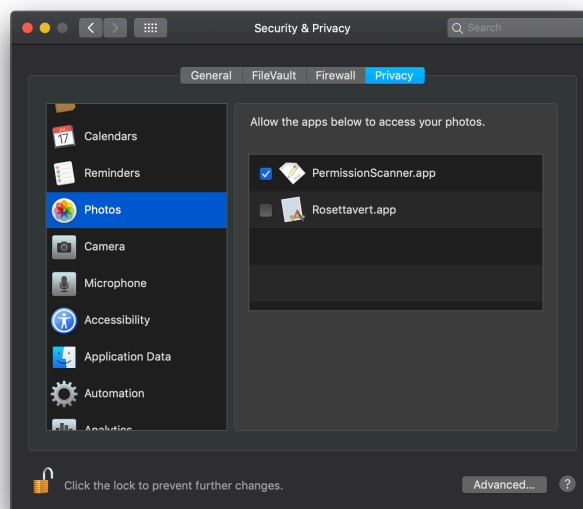
There are then two considerations: the app's **capabilities**, and your **consent**.

Regular apps compatible with Mojave may not declare any capabilities, but those which are specially 'hardened' for 10.14, including all apps which are 'notarized', have to declare any capability to access protected information. They can only do so for the information in the **Prompting** and **Special** categories, not those listed in the **Other data** category above. App behaviour can also be affected by whether the app is specifically built for Mojave, or whether it supports earlier versions of macOS too.

How to give your consent

There are two ways in which your consent will be sought, when required: in the **Security & Privacy** pane in advance, and at the time that the app wants to access protected information.

⚠ Whenever possible, anticipate that you will want to access protected information and change settings in the **Privacy** tab of the **Security & Privacy** pane beforehand. There are three types of setting there.



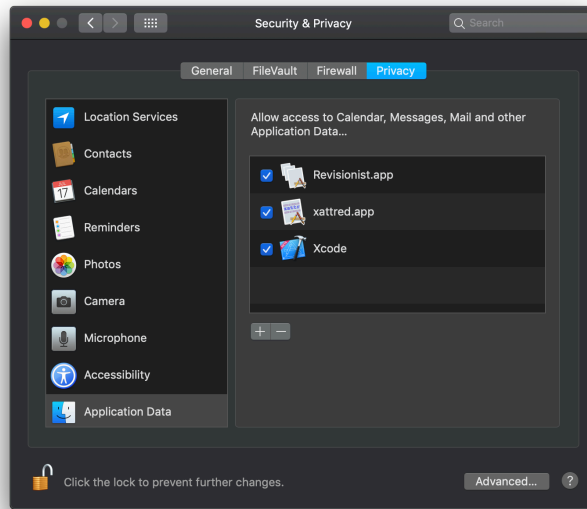
For each type of information in the **Prompting** category, there is a separate item listed at the left. If you want to let an app access the photos in your Photos libraries, for example, select the **Photos** item. You should then see a list of apps which are currently recognised as having the capability of accessing information in your Photos libraries. You cannot simply add an

Running Apps in Mojave

User Advice

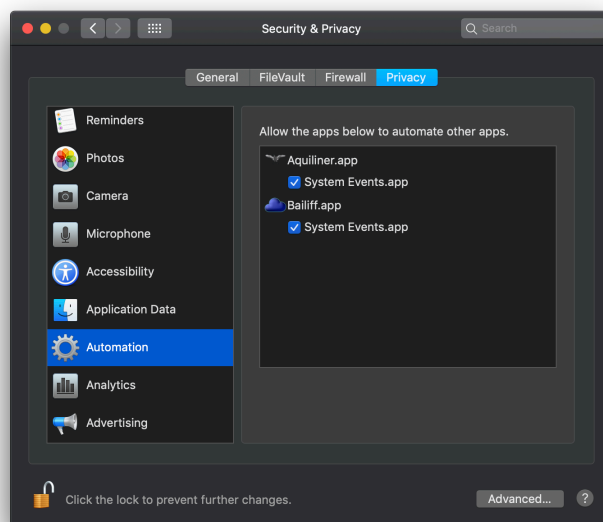
Howard Oakley <https://eclecticlight.co>

app to that list though: it depends on declared capabilities, and your personal history of which apps you have allowed to access those libraries in the past.



For general protected information, which includes items in the **Prompting** and **Other data** categories above, there is the **Application Data** item at the left. As these include types of information which are not included in an app's set capabilities, you can add apps of your choosing using the + button below the list of apps.

⚠ If you know that you will need to access protected information using an app, it is best to add it to this list when you install that app. You can then uncheck it when you don't want it to have access to protected information, and check it again when you do.



Information covered by the **Special** category is also covered by specific items in the list at the left. These include **Automation**, which covers scripting of all kinds, the **Camera** and

Running Apps in Mojave

User Advice

Howard Oakley <https://eclecticlight.co>

Microphone. You are not able to edit this list freely, as it too relies on set application capabilities.


You may also be prompted to give specific consent when an app wants to access protected information. Apps which are hardened/notarized are required to provide you with additional details of why they want such access, so the dialogs that you see should be more informative, and enable you to make an informed decision each time.

What happens when an app tries to access something that isn't permitted?

Even if an app has a capability set and you consent, there may still be occasions when macOS prevents access to protected information; without capability or consent, macOS will refuse every time.

In some circumstances, refused access passes in silence. The app may have asked for a list of files or folders which it shouldn't be able to see, and gets an empty response, as if they simply weren't there. If macOS could give access with your consent, you may be prompted to give it, in which case that app will pause while you respond to the consent dialog.

If there is no legitimate way for that app to obtain access, then macOS doesn't waste time with warning alerts, but the app unexpectedly quits, or crashes if you prefer that term. If you see a crash report, you can scroll down through it and spot a message such as **PRIVACY VIOLATION** in block capitals, which may confirm what has happened.

 But in Mojave, any app which crashes when trying to access protected information should be assumed to have done so because macOS won't give it access.

If you want an app to access something which is causing it to crash because of privacy protections, quit the app and see if you can improve its chances using the **Privacy** tab of the **Security & Privacy** pane, as detailed above. If you can't change its behaviour in that way, you will need to contact the developer of the app to see if there is anything that they can do to fix the problem.

Summary

1. Almost all the time, Mojave's new privacy protection shouldn't get in your way, but when it does you need to be prepared and know what to do.
2. If you need to access information or a document within a protected area, first try exporting or copying it to a folder in Documents, or similar, which isn't protected.
3. Give your prior consent for specific apps to access protected information whenever possible, using the Privacy tab of the Security & Privacy pane. When an app has been added, you can still quickly enable and disable its access using the checkbox.

Running Apps in Mojave

User Advice

Howard Oakley <https://eclecticlight.co>

4. When apps cannot access protected information, their behaviour may change, and they may become ‘blind’ to protected folders or files. At worst, attempting to access protected information may cause the app to crash.
5. Any app which crashes when trying to access protected information should be assumed to have done so because macOS won’t give it access.
6. If you need an app to access protected information but it cannot, contact the app’s developer. They may not be aware of the problem, and may be able to provide a solution.

Change list

1.0:

- initial release, for Mojave β5.

6 August 2018.