Mission Guide: F-Response Collect for Apple OSX

Your Mission: Install and run the F-Response Collect Subject on Apple OSX

Using F-Response Collect to acquire data from an Apple OSX computer

Important Note

Disclaimer: F-Response works diligently to stay on top of operating system and user interface changes between releases. However, you may be dealing with an Apple computer where the display does not match what you see here exactly. Please use your best guess and if you have issues, you are welcome to reach out and we'll do our best to assist you.

Step 1: What is F-Response Collect for Apple OSX?

F-Response Collect for Apple OSX ("fr-collect-sub-osx") is a native software application developed on Apple OSX Ventura to provide filesystem and user directory collection options for the OSX platform (both arm/M1/M2 and heritage intel/x86_64). It is provided on our website on the downloads page (https://www.f-response.com/support/downloads) as package files for both the arm and intel chipset.

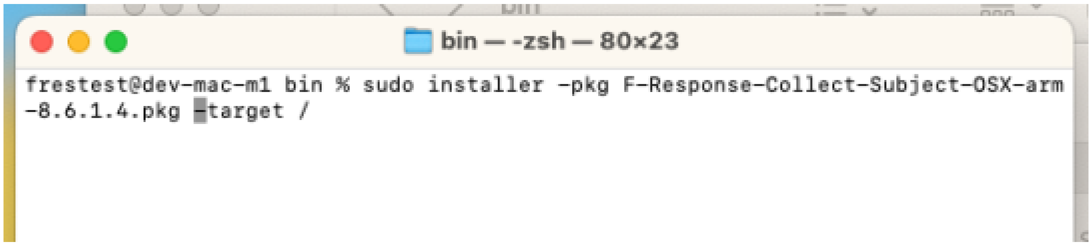
The F-Response Collect for Apple OSX executable is a subject executable, meaning it has no graphical component and is only designed to run in the background via launchd/launchctl. It follows the same process as other F-Response Collect subject executables in that it talks to your Collect Server, retrieves tasking, and executes those tasks.

Step 2: How do I install the pkg file and what is it doing?

In order to install F-Response Collect for OSX you will need administrative rights on the Apple machine and the ability to install pkg software. You will also need to use the F-Response Collect Management Console under windows to export a "non-windows" configuration file, specifically the "fr-collect-sub.cfg" file as referenced in the manual.

Once you have both the proper pkg for the apple machine in question and the configuration file from your Management Console on the apple machine, you are ready to begin.

Start by opening a terminal window via Applications->Utilities->Terminal. You will need to navigate to the location of the pkg file and install via the sudo command as shown below:



```
frestest@dev-mac-m1 bin % sudo installer -pkg F-Response-Collect-Subject-OSX-arm
-8.6.1.4.pkg -target /
```

This will make the following changes:

- Create the /etc/fr-collect-sub directory if it does not exist.
- Create an empty /etc/fr-collect-sub/fr-collect-sub.cfg file if it does not exist.
- Copy the fr-collect-sub-osx executable to /usr/local/bin.
- Create a com.f-response.collect.plist file in /Library/LaunchDaemons.
- Load and enable the com.f-response.collect system service.

The final step required is to replace the configuration file at /etc/fr-collect-sub/ with the exported one from the F-Response Collect Management Console. This is how the software will know where to go to connect to the Collect server and obtain tasking.

Once the file is replaced the service can be restarted using the following commands via terminal:

sudo launchctl unload /Library/LaunchDaemons/com.f-response.collect.plist

(*Note: The above command may return an error if the service is not already running or the fr-collect-sub.cfg file has not been replaced. It is safe to ignore this error provided the /etc/fr-collect-sub/fr-collect-sub.cfg file has been replaced with the one exported from the management console.)*

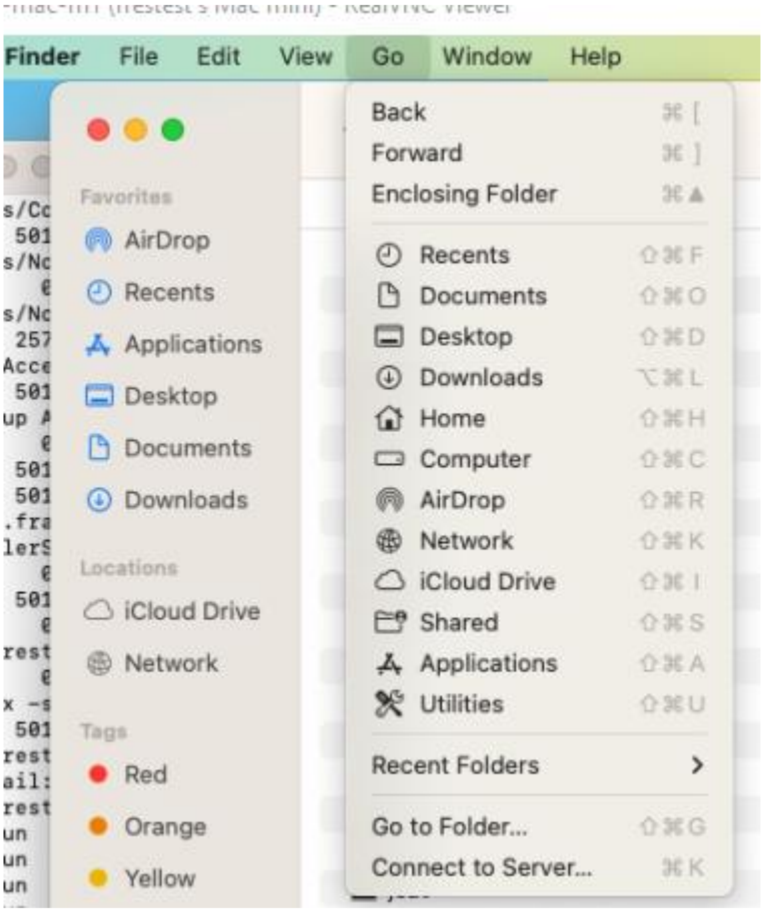
sudo launchctl load /Library/LaunchDaemons/com.f-response.collect.plist

Step 3: How do we give it sufficient access? Handling Apple Full Disk Access (FDE).

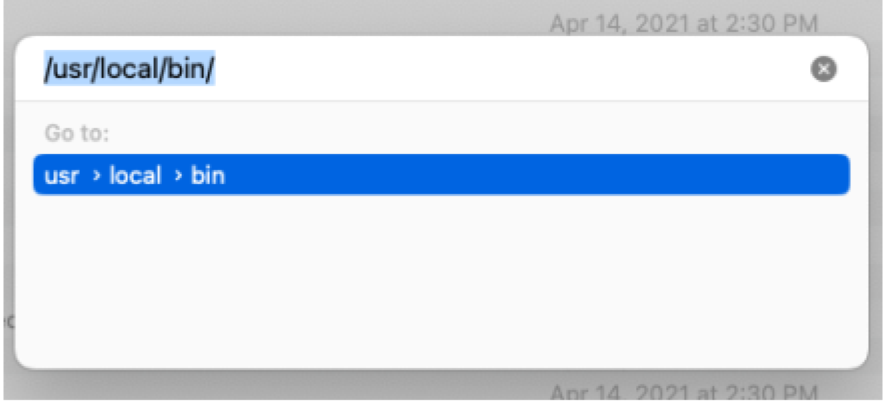
Starting in more recent versions of Apple OSX, access to multiple user directories is now unavailable to applications that do not possess “Full Disk Access” via the System Preferences panel. In the case of F-Response Collect, this means without enabling Full Disk Access the software will not be able to collect user content from Desktop, Documents, or Downloads.

While 3rd party tools (JAMF, etc) maybe be able to perform these steps in a more automated fashion, the exact specifics of those tools are outside the scope of this document. If you have sufficient Apple engineering in house and would like to discuss how to repackage and manage the F-Response Collect for OSX executable in a more automated fashion, we are happy to answer any specific questions about the application but we do not have large scale Apple management experience and can only speak to the product.

Start by opening a finder window and using the menu option to “Go to Folder…” to navigate to a specific folder.

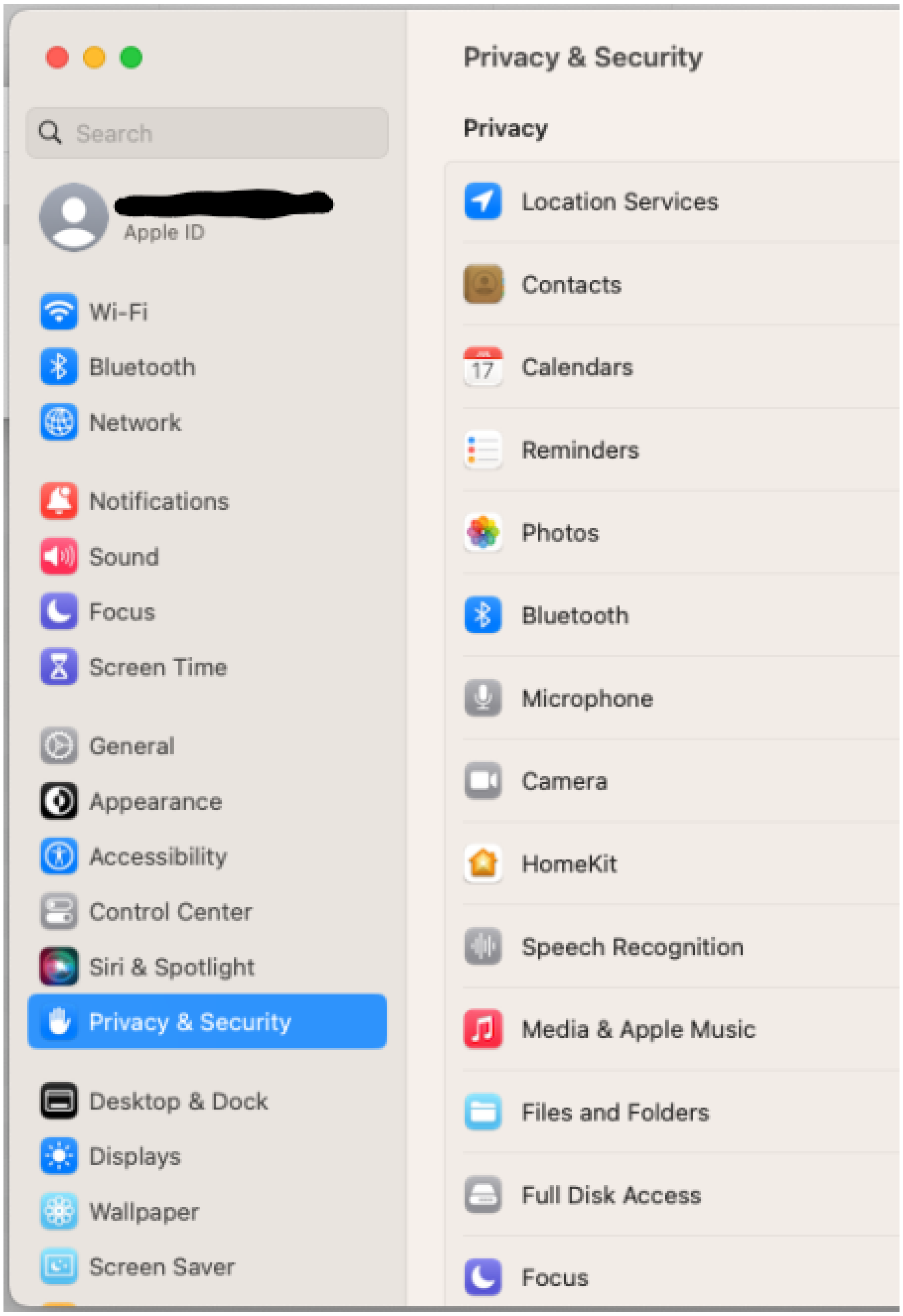


Input the location of F-Response Collect, /usr/local/bin.

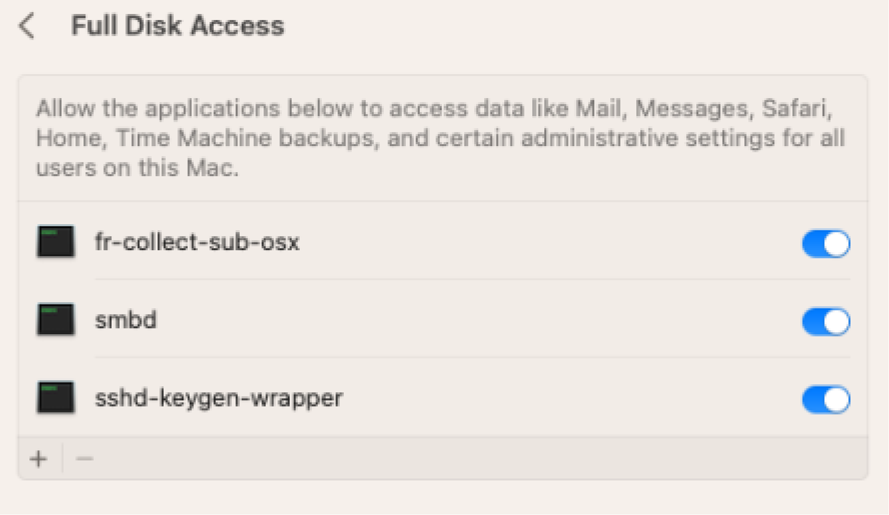


/usr/local/bin/

Now open the Preferences application and navigate to Privacy and Security, specifically Full Disk Access.



Once there, drag and drop the fr-collect-subject-osx executable from /usr/local/bin to the Full Disk Access window.



Full Disk Access

Allow the applications below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

fr-collect-sub-osx

smbd

sshd-keygen-wrapper

Make sure the toggle is switched to the "on" position.

Step 4: What are the Apple OSX targets for Collect and what do they mean?

F-Response Collect for OSX offers profile and custom collection targets. Profiles are simply the contents of the /Users/<USERNAME> directory. Custom collections are based off of the /Volumes/<DEVICE> directory and allow you to decide what gets collected just like existing F-Response Collect custom collections.

Important note: While F-Response Collect for OSX will automatically restart in the event of a loss in connectivity, it will NOT resume from where it left off. The application will see that a task needs to be performed and will restart performing it, but the restart will begin at position zero.

In addition, the percentage complete will rapidly reach 99% or 100% but will still be growing. That's because, unlike Windows, we are unable to pre-assess the total collection size sufficiently to create an accurate completion percentage. This is just a factor of how the technology works on this platform.

Troubleshooting

The Full Disk Access keeps switching back to grey for fr-collect-sub-osx? *You will need to remove any instance of fr-collect-sub-osx from the Full Disk Access dialog and re-add it using the instructions outlined above.*