

FIRMM INSTRUCTIONS

Last updated: 20220727

Running FIRMM

NOTE: The order in which you perform the following steps is very important.

1. Log onto the VPN on the FIRMM Mac so that you can access the FASSE network.
 - i. Open the Cisco AnyConnect window by clicking on the icon in the upper right menu bar and selecting "Show AnyConnect Window". This will open the normal VPN authorization window.
 - ii. Make sure that "vpn.rc.fas.harvard.edu" is written as the path in the first line and click "Connect". This will open a pop-up log-in window.
 - iii. Enter your RC username followed by "fasse" in the first line of this window (e.g., "jsegawa@fasse").
 - iv. Enter your RC password in the second line of this window (this will be your personal password associated with your account).
 - v. Enter your secondary authorization code by using your DuoMobile phone application.
 - vi. Click "Connect". This will cause the window to disappear. If the log in was successful, there will now be a green check mark icon on the main VPN authorization window, and it will read "Connected to vpn.rc.fas.harvard.edu".

***For troubleshooting the VPN connection, make sure the iMAC is connected via ethernet. The yellow cable should be plugged in, and you need to check that it is active. This computer is also used for eye tracking, so sometimes the ethernet is disabled (Open System preferences -> Internet, and make sure the location is set to 'Automatic').**

2. Register your subject and start FIRMM on the console computer.
 - i. Click "Cntrl-Esc" on the keyboard to bring up the Windows start menu.
 - ii. Select "Start FIRMM session" by right clicking and selecting "Run as administrator".
 - iii. Wait for a pop-up text window to scroll then disappear.
 - iv. Manually load your scans into the queue and start the session normally.
3. Wait for the first BOLD sequence to run, then start FIRMM on the FIRMM Mac.
 - i. Open a terminal window by clicking on the "Search" icon in the upper right corner of the menu bar on the FIRMM Mac.
 - ii. Type "Terminal" into the search bar and select the application when it appears. This will open a new terminal window.
 - iii. In the terminal window, type "ssh -X firmmproc@ncf-firmm1.rc.fas.harvard.edu" (you can also copy and paste this from a text file titled "FIRMM Pathway" on the desktop).

- iv. Enter the password “FIRMMpass2222” and then click "Enter" on the keyboard.
- v. Once you are sure that the first few BOLD sequences have been run on the console (it is usually a safe bet to wait until after the trigger has occurred), type “FIRMM” into Terminal and again click “Enter”.

4. Wait for the startup messages to start loading in the terminal window. The pop-up FIRMM window should appear with no data loaded yet.

5. Wait for the following string of messages to load in the terminal:

```
*** Queued processing series 10, frame 1
*** Queued processing series 10, frame 2
*** Queued processing series 10, frame 3
*** Queued processing series 10, frame 4 ***... and so on
```

This means that the scans are being properly loaded into and read by FIRMM.

6. Click on “Start” in the FIRMM window. A pop-up window will ask you to confirm the Patient ID and other information.

7. Click “OK” in this pop-up window. This should cause it to disappear and display the main FIRMM window.

*At this point, the message in blue at the top of the FIRMM window should read "Searching for BOLD scan" or "Waiting for next DICOM". If it displays "Initializing Startup Routine", the scanner and FIRMM have not properly synced and you will likely have to wait until the next BOLD scan for FIRMM to display data.

NOTE: If you have multiple BOLD runs, you can leave FIRMM running in between, and it will start again with the next sequence. You do NOT need to stop and start FIRMM for every run.

8. When you are done, log out and quit out of everything on the Mac.

- i. Close the FIRMM window.
- ii. Type "exit" or simply exit out of the terminal window.
- iii. Quit the VPN.

FIRMM Data Retrieval

1. Log in to VPN
2. Open a terminal window and SSH into the server

```
ssh -X firmmproc@ncf-firmm1.rc.fas.harvard.edupassword: FIRMMpass2222
```

3. CD to the logs directory

```
cd FIRMM/FIRMM_logs
```

4. Find the log for the session

iv. Use the date to find the session (still haven't found out how the other groups manage to get their scan name on the log file, but until then this isn't so bad). Example: `ls *20210113*`

v. It's possible that more than one log file will come up when you search for it – due to other groups using the software that day, or if you tried to boot up FIRMM multiple times (in which case it would make a new log file each time you open it up)

5. Copy the name of the session and log out of firm (literally highlight and CNTL-C the name, and type “logout”) 2. Back on your local computer, transfer the file into your data directory:

```
scp firmmproc@fasse  
firmm1.rc.fas.harvard.edu://home/firmmproc/FIRMM/FIRMM_logs/XXXXXX_20210113_01011  
3_FIRMM_log.csv /Users/jsegawa/Desktop/FIRMM
```