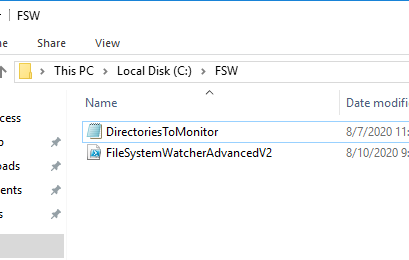
# Advanced FileSystemWatcher

# Setting Up

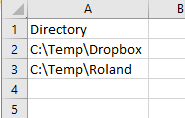
1. Copy the Powershell Script ***FileSystemWatcherAdvancedV2.ps1*** and the csv file ***DirectoriesToMonitor.csv*** to a location of your desire. In this demo, we are using **C:\FSW.**

* Note that after setting up, if these files are moved, the below steps will have to be repeated

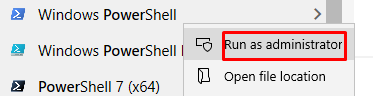


1. Make sure the csv file contains the full path to the directories to be monitored. There is no limit to the number of directories you can add.

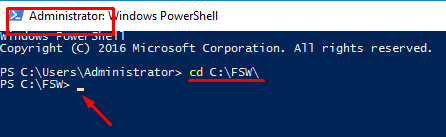
* Note that the script will **monitor all files and subfolders** inside the specified directory.



1. Open a PowerShell console as Administrator



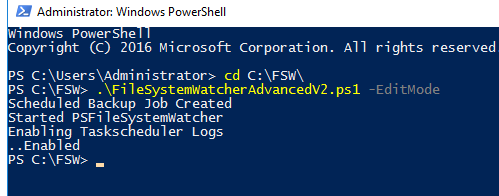
1. Change directory to the location you copied the files into.



1. Type the below command and hit Enter key.

.\FileSystemWatcherAdvancedV2.ps1 -EditMode

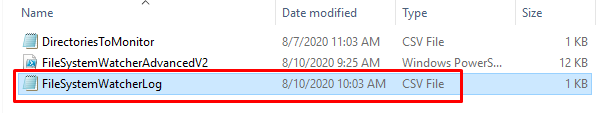
You should see results like below. If you have TaskScheduler jobs already enabled, you will not see the last 2 entries.



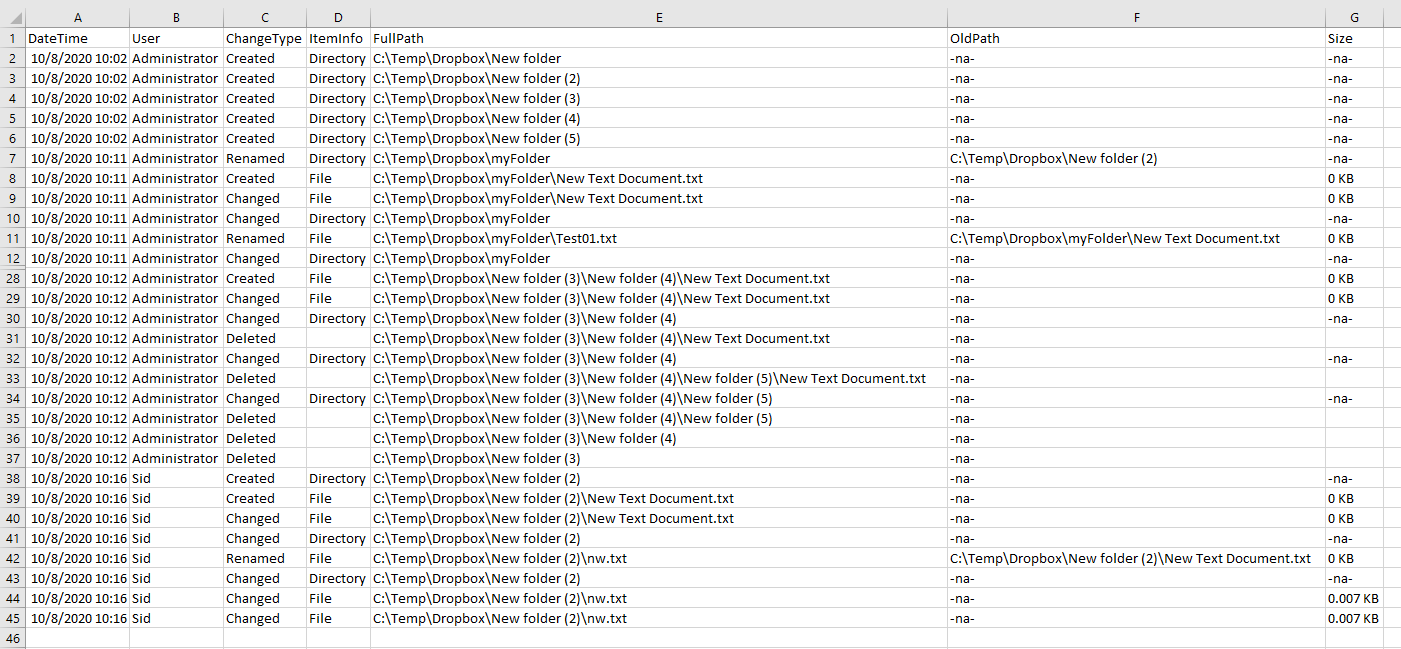
**And you are all set.**

## Testing

1. Go to any of the monitored folders mentioned in step 2 and make some file system changes
2. A log file like this will be generated on the source folder.

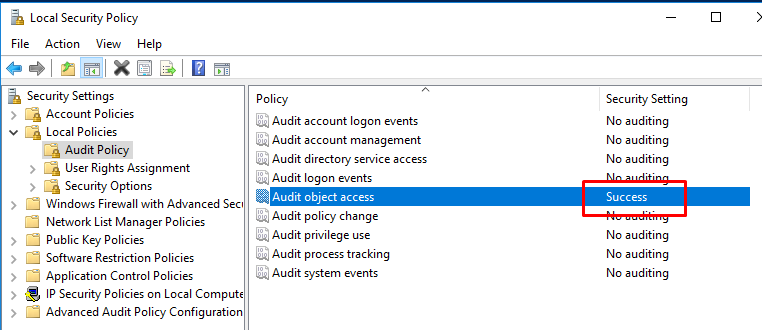


1. Please note that there will be a slight delay in the file getting updated as some data has to be read from eventlogs.
2. Below is a sample of how the log is going to look like.

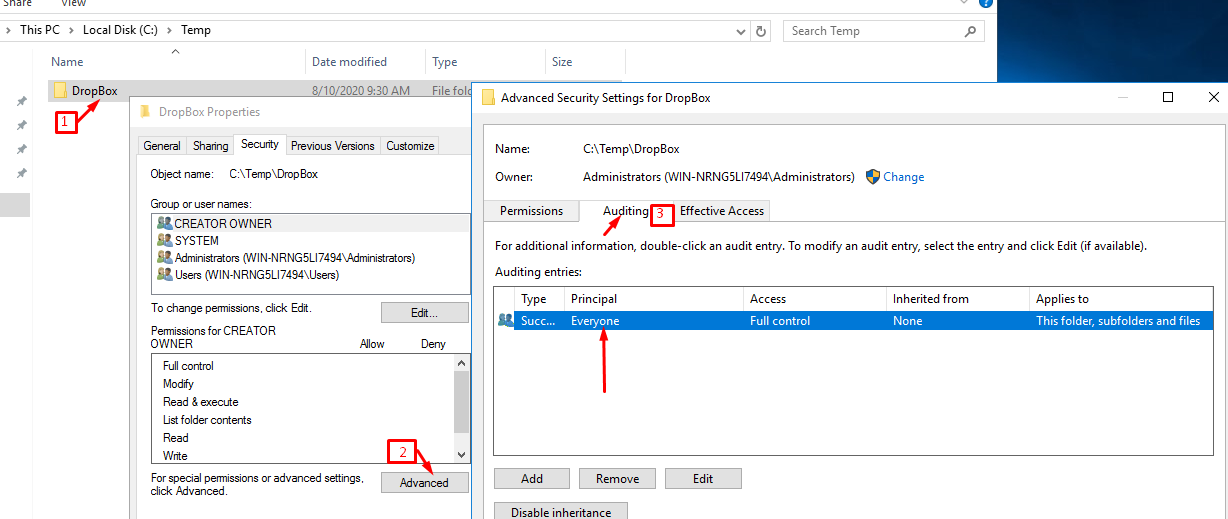


## AdvancedInfo: Important Read.

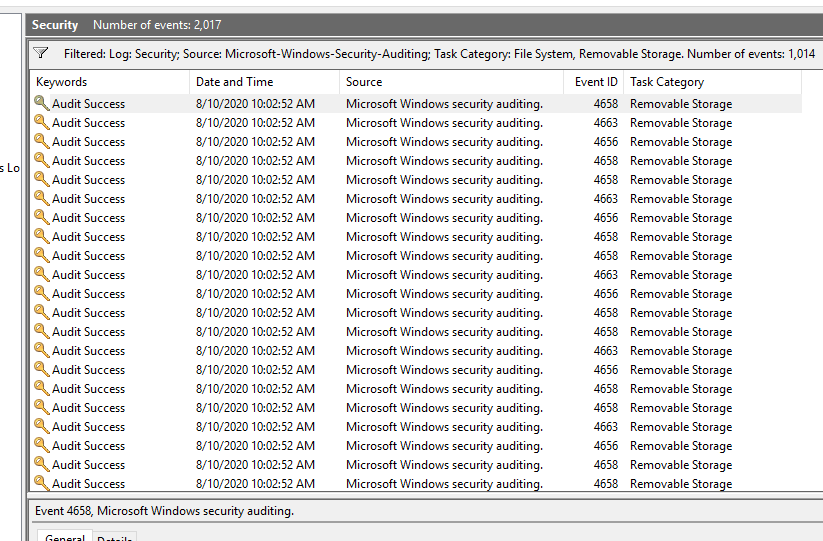
* Script will set the local audit policy for Object access on your machine to success.



* This will also enable file and folder auditing on the directories mentioned in step 2.



* As a result, all changes on these directories will generate a security event log in the eventviewer.



* This is necessary to obtain the user information of all file system events.
* The script will also create a Scheduled Task in Windows TaskScheduler and run it. Note that it will always be in a running state.

