NOTE: Missing Images

This article lost the screenshot images that accompanied it in a KB system migration. We will endeavor to replace them soon.

Background

ProcMon (Process Monitor) is a Microsoft (SysInternals) tool which is available for download here:

https://learn.microsoft.com/en-us/sysinternals/downloads/procmon

What ProcMon does is to collect every bit of file system I/O that your computer does while capture mode is on. This is a very effective diagnostic tool with regard to understanding issues such as "where is this process looking for file xyz?" or "What is preventing file abc from being saved/opened?"

OCR-Specific Troubleshooting

NOTE we have a companion article - specific to troubleshooting issues with OCR Resources:

HOWTO: Use ProcMon to Debug OCR Resources Issues

Common Scenarios

PROBLEM:

You've got valid purchased license files in your `c:/users/YOUR_USERNAME/AppData/Local/Atalasoft/DotImage 10.x/` directory, but your application keeps erroring out saying "expired evaluation"

PROC-MON SOLUTION:

Using ProcMon while compiling your app, and filtering for Atalasoft.*.lic you find that the process is picking up an expired eval file hiding in `c:\yourApp\bin\debug\x86`

Deleting the old licenses and rebuild your solution... no more "expired evaluation" errors

PROBLEM:

Your web application keeps erroring out saying "file not found" when you are trying to open "/foo.tif"

PROC-MON SOLUTION:

Using ProcMon, you run your web app and try to open the file in your app... You filter your results for foo.tif and find that the app is interpolating the request is being interpreted as `c:\wwwroot\foo.tif` but your actual file is in `c:\wwwroot\myapp\foo.tif.`

Using that information, you change the URL to "/MyApp/foo.tif" and the file now opens properly

How to use ProcMon

First, download ProcMon from the above linked web page. ProcMon does not have an installer or require installation. You just download the zip, then unzip it and

double click either Procmon64.exe (64 bit) or Procmon.exe the (32 Bit). They also ship Procmon64a.exe for ARM64 but Atalasoft does not currently support ARM64 architecture.

As soon as ProcMon starts up, you will be presented with a filter list - by default, that filter will exclude procmon itself (important so that procmon doesn't log procmon logging a log of ProcMon logging a log and get into an infinite loop) as well as certain other system processes that are likely to cause severely overinflated logs.

As you grow more comfortable with ProcMon, you may add your own extra filters here to exclude your antivirus app (it tends to produce a lot of extra procMon log entries as it double-checks every file access...) or Vshost.exe (since the vshost is running while it debugs your app, you may find it contains a lot of unneeded entries)

If you're not sure what to log, just accept the default for now - the beauty of ProcMon is you can filter your results later (the info is captured, but simply eliminated form displaying)

- Once you click OK, ProcMon will immediately start capturing.

- You can stop/start capture by hitting CTRL + e (or click the tooltip icon that looks like a small microphone)
- You can toggle automatic scrolling while capture by hitting CTRL + a (or click the tooltip that looks like a page of text with a down arrow next to it)
- You can Clear the capture (useful for hitting just before recreating the error) by hitting CTRL + x (or clicking on the tooltip that looks like a document being erased)

So, you now run the program / start debugging / perform the action that you're attempting to get diagnostic data on. Once you've caused the condition/error you should hit CTRL + e to stop the capture.

At this point, you may want to save the log - using File -> Save

img

On the save options, you can choose "all events" or "Events displayed using current filter". We suggest that if you haven't done heavy filtering, you use the "Events displayed using current filter" option.

For format, it's best to just leave it in "native process monitor format" that way Atalasoft support personnel can use ProcMon locally to filter your report in ways that help us narrow things down.

If you ever need to send us the PML file, be sure to zip / tar.gz / rar the file as the log files can be HUGE if left uncompressed.

Filtering for Current Needs

You may have noticed that even with the default filtering on, the log file probably contains thousands of entries. The trick to getting the data you care about is to understand filtering.

The easiest way to get started is to look at your entries in ProcMon and right-click on one with a process name you know isn't relevant to your results. One of the options on the context menu is "Exclude 'processNameHere'". If you select that, it will remove that process ...

You can also scroll until you find the process name for the process you're watching and then

you can right-click and choose "Include 'processNameHere'" and the filtering will exclude everything BUT that process.

If you accidentally remove something you didn't mean to or if you want to just search for a specific thing such as "files ending in .lic" you can manually edit the filter. The filter options can be brought up by hitting CTRL + L (or clicking the icon that looks like a snow-cone with blue filling).

You will see your current filter entries - from this section you can remove existing filters (in case you accidentally included or excluded something you didn't mean to) or you can directly create new ones.

For instance, if I want to make a filter that shows only entries for files with filename ending in ".lic", I would use the filter dialog

img

- I would choose the first box as "PATH"
- The second box would be "ENDS WITH"

  and then I'd put in ".lic" without the quotes
- Leave the "then" box as "INCLUDE"
- The filter isn't applied until you hit "ADD"
- When you're done adding filters, hit "OK"

img

By looking / filtering for path or process name, you can narrow down to find the problems.

Making sense of it all

The thing is you'll see a LOT of entries for things you never thought were going on - like querying registry keys and when a file is accessed, you'll see separate entries for opening the file, writing, reading, and so on - FILE NOT FOUND or ACCESS DENIED aren't always indications of trouble... but as you gain more experience with ProcMon, they'll make more sense to you... but in cases where we've asked you to submit a ProcMon log, it's actually preferable to not filter too much - just zip it up and send it and we'll do the "heavy digging"

Original Article

Q10394 - HOWTO: Use ProcMon to Collect Diagnostic Information

Last Update

2026-11-11 - TD - (Fixed Formatting and marked missing images)

Atalasoft Knowledge Base
https://www.atalasoft.com/kb2/KB/50101/HOWTO-Use-ProcMon-to-Collect-Diagnos...