

Run this command in elevated powershell in the folder where the exe and xml files are:

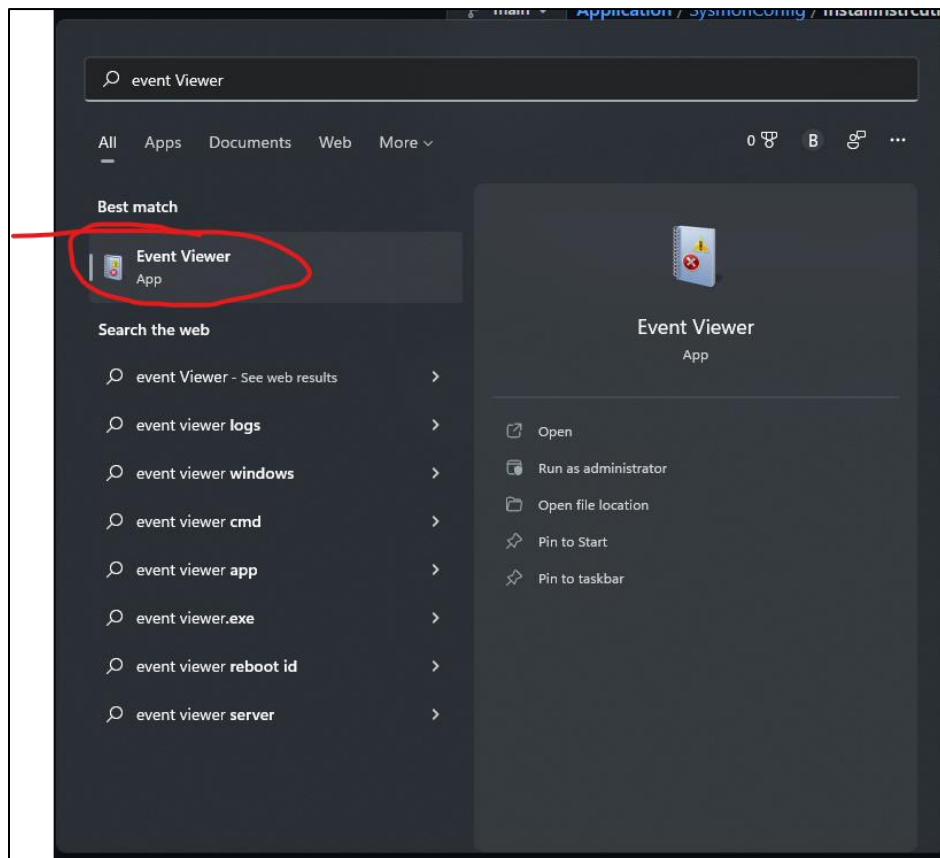
```
sysmon.exe -accepteula -i IncludeAllExcludeCommon.xml
```

```
PS C:\Users\Bryan\Desktop\sysmon> sysmon.exe -accepteula -i IncludeAllExcludeCommon.xml

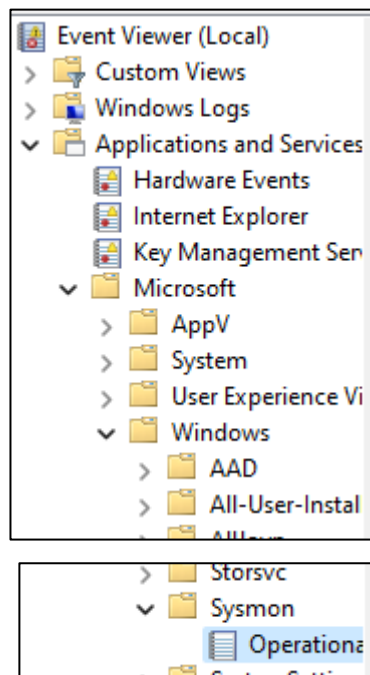
System Monitor v13.32 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2022 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.60
Sysmon schema version: 4.81
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
PS C:\Users\Bryan\Desktop\sysmon> |
```

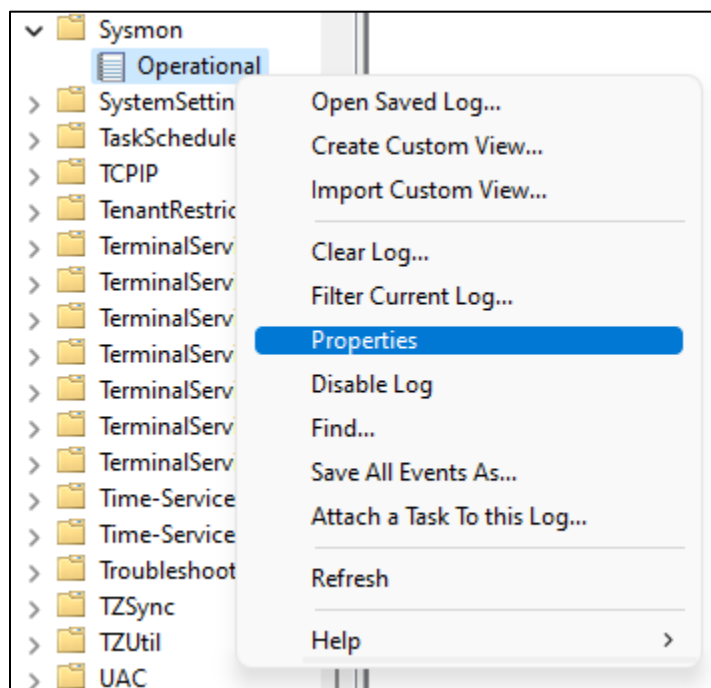
Once installed and started, open Windows Event Viewer



Navigate to Applications and Services > Microsoft > Windows > Sysmon



Right-click Operational and select properties



Change default logging to “Archive the log when full, do not overwrite events”

Log Properties - Operational (Type: Operational)

General Subscriptions

Full Name: Microsoft-Windows-Sysmon/Operational

Log path: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Sysmon%4Operational.e

Log size: 64.00 MB(67,112,960 bytes)

Created: Friday, April 8, 2022 1:40:53 PM

Modified: Monday, April 11, 2022 10:20:25 AM

Accessed: Monday, April 11, 2022 10:20:25 AM

☒ Enable logging

Maximum log size (KB): 65536

When maximum event log size is reached:

☐ Overwrite events as needed (oldest events first)

☒ Archive the log when full, do not overwrite events

☐ Do not overwrite events (Clear logs manually)

Clear Log

OK Cancel Apply

Select 'OK' and close the events viewer