# EvtMon

## Purpose:

Evtmon is a Windows event log monitoring tool developed by Matt Gravlin. With this tool you can monitor the 3 primary Windows event logs and perform various actions whenever matches occur. Actions include:

* Send alert to Spectrum
* Write to a log file
* Execute a script
* Send to Syslog

## To use:

1. Extract all the files to C:\evtmon
2. Execute evtmon-service-install.vbs which will install a Windows service called “Evtmon”.
3. Edit the evtmon.ini appropriately. This is where you setup:
   1. Scan interval – this is how often this program will scan all the log files you are monitoring. If it’s a single log file, it will be that interval. If you are monitoring 2 log files, it will be that interval for both log files, etc. Please do not use a setting that is too fast. The min value you should use is 5 seconds, but you should consider using a higher value.
   2. SNMP Trap destinations. This is how to send alerts to Spectrum. Refer to [this link](http://iitoei.intuit.com/iitoei/Tools/SNMP#SNMP_Trap_Configuration) to determine what setting s you should use.
   3. Syslog destinations – if you have an Rsyslog server and want to send to it, specify it here.
   4. Suppressions – this is used to prevent “event storms” how it works is that the program will remember every log that matched per action setting (for example every SNMP trap sent to Spectrum in the last xx intervals) if there is an exact match during that interval it will suppress sending it until the interval window expired. It is a good idea to use this setting and recommend using a value of 5 if you are unsure.
4. Determine which eventlogs you want to monitor, edit the related file application\_log.positive.patterns , system\_log.positive.patterns and/or security\_log.positive.patterns. Note that the syntax needs to be exact. Please refer to the examples in the files provided.
5. From a command prompt run “net start evtmon” or start the service from the services applet.

## Important Notes

* For additional documentation, please refer to the evtmon.ini file and provided positive.patterns files.
* If you edit the evtmon.ini file, you must restart the service.
* If you ever stop or restart the service, please verify that the evtmon.exe is actually stopped, it is common that the service may error saying it cannot stop the service or that the service says its stopped, but it is actually still running. Please verify in task manager and kill the process to ensure that it has stopped.
* If you edit any of the positive.patterns files, you do not need to restart the service.