Recast

Sysmon

Last Modified on 04.16.26

When installing Sysmon, you can optionally use a configuration file.

You can find more information about installing and using a configuration file in the Microsoft documentation.

Example

Below is an example of common usage featuring simple command-line options to install and uninstall Sysmon, as well as to check and modify its configuration:

Install: sysmon64 -i [configfile]
Update configuration: sysmon64 -c [configfile]
Install event manifest: sysmon64 -m
Print schema: sysmon64 -s
Uninstall: sysmon64 -u [force]

Parameter	Description
-i	Install service and driver. It can optionally take a configuration file.
-c	Update the configuration of an installed Sysmon driver or dump the current configuration if no other argument is provided. It can optionally take a configuration file.
-m	Install the event manifest (implicitly done on service install).
-s	Print configuration schema definition.
-u	Uninstall service and driver. Using `-u force` causes uninstall to proceed even when some components are not installed.