

Windows Sysinternals

Search TechNet with Bing



United States (English) Sign in

[Home](#) [Learn](#) [Downloads](#) [Community](#)[Windows Sysinternals](#) > [Downloads](#) > [File and Disk Utilities](#) > **Process Monitor**

Utilities

[Sysinternals Suite](#)[Utilities Index](#)[File and Disk Utilities](#)[Networking Utilities](#)[Process Utilities](#)[Security Utilities](#)[System Information](#)[Utilities](#)[Miscellaneous Utilities](#)

Additional Resources

[Forum](#)[Site Blog](#)[Sysinternals Learning](#)[Mark's Webcasts](#)[Mark's Events](#)[Mark's Blog](#)[Software License](#)[Licensing FAQ](#)

Process Monitor v2.96

By Mark Russinovich and Bryce Cogswell

Published: August 16, 2011

[Download Process Monitor](#)
(1.26 MB)

Rate:

Share this content



Introduction

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Overview of Process Monitor Capabilities

Process Monitor includes powerful monitoring and filtering capabilities, including:

- More data captured for operation input and output parameters
- Non-destructive filters allow you to set filters without losing data
- Capture of thread stacks for each operation make it possible in many cases to identify the root cause of an operation
- Reliable capture of process details, including image path, command line, user and session ID
- Configurable and moveable columns for any event property
- Filters can be set for any data field, including fields not configured as columns
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data
- Process tree tool shows relationship of all processes referenced in a trace
- Native log format preserves all data for loading in a different Process Monitor instance
- Process tooltip for easy viewing of process image information
- Detail tooltip allows convenient access to formatted data that doesn't fit in the column
- Cancellable search
- Boot time logging of all operations

The best way to become familiar with Process Monitor's features is to read through the help file and then visit each of its menu items and options on a live system.

Screenshots

Advertisement



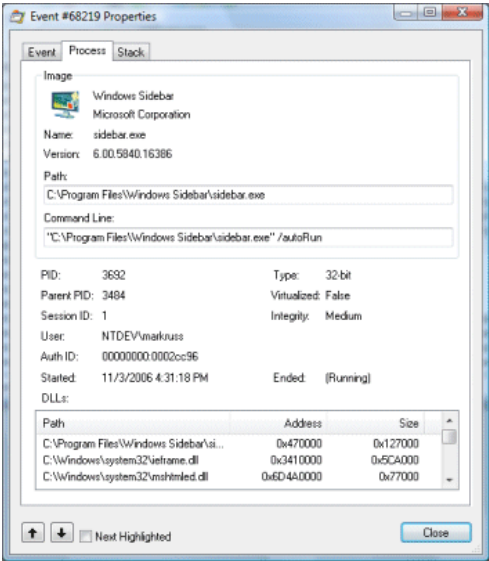
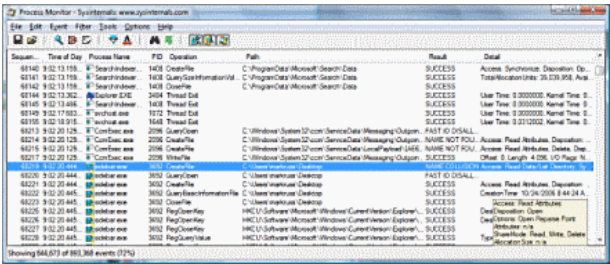
Download

[Download Process Monitor](#)
(1.26 MB)

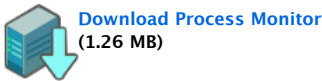
Runs on:

Client: Windows XP SP2 and higher.

Server: Windows Server 2003 SP1 and higher.



Download

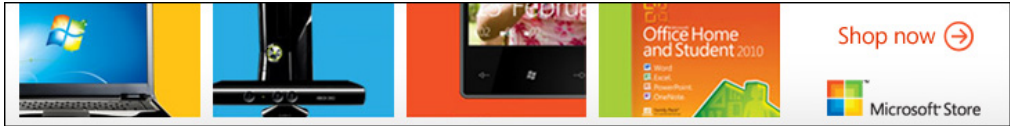


Run Process Monitor now from Live.Sysinternals.com

Runs on:

- Client: Windows XP SP2 and higher.
- Server: Windows Server 2003 SP1 and higher.

[Top of page](#)



Advertise Here