# Process Explorer

https://technet.microsoft.com/en-us/sysinternals/bb896653

**By Mark Russinovich**

Published: February 17, 2017

[**[Download icon](https://download.sysinternals.com/files/ProcessExplorer.zip) Download Process Explorer**](https://download.sysinternals.com/files/ProcessExplorer.zip)**(1.8 MB)**

|  |  |
| --- | --- |
| **Rate:** |  |

Share this content

[[#](mailto:?subject=Process%20Explorer&Body=https://technet.microsoft.com/en-us/sysinternals/bb896653)](mailto:?subject=Process%20Explorer&Body=https://technet.microsoft.com/en-us/sysinternals/bb896653)

[[#](https://twitter.com/home?status=process%20explorer%20:%20https%3a%2f%2ftechnet.microsoft.com%2fen-us%2fsysinternals%2fbb896653)](https://twitter.com/home?status=process%20explorer%20:%20https%3a%2f%2ftechnet.microsoft.com%2fen-us%2fsysinternals%2fbb896653)

[[#](https://del.icio.us/post?url=https%3a%2f%2ftechnet.microsoft.com%2fen-us%2fsysinternals%2fbb896653&title=process%20explorer)](https://del.icio.us/post?url=https%3a%2f%2ftechnet.microsoft.com%2fen-us%2fsysinternals%2fbb896653&title=process%20explorer)

[[#](https://digg.com/submit?url=https%3a%2f%2ftechnet.microsoft.com%2fen-us%2fsysinternals%2fbb896653&title=process%20explorer)](https://digg.com/submit?url=https%3a%2f%2ftechnet.microsoft.com%2fen-us%2fsysinternals%2fbb896653&title=process%20explorer)

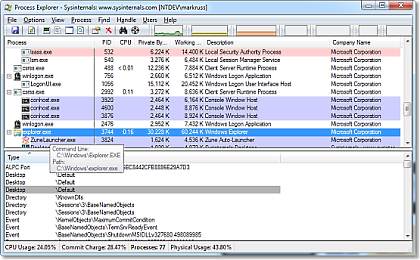
[[#](https://www.facebook.com/sharer.php?u=https%3a%2f%2ftechnet.microsoft.com%2fen-us%2fsysinternals%2fbb896653&t=process%20explorer)](https://www.facebook.com/sharer.php?u=https%3a%2f%2ftechnet.microsoft.com%2fen-us%2fsysinternals%2fbb896653&t=process%20explorer)

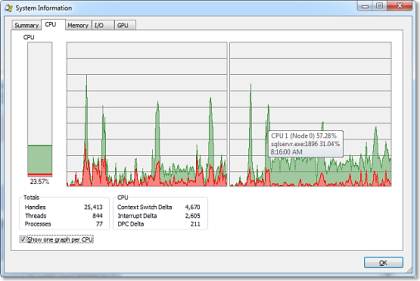
Introduction

Ever wondered which program has a particular file or directory open? Now you can find out. Process Explorer shows you information about which handles and DLLs processes have opened or loaded.

The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded. Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded.

The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.





**Related Links**

* [Windows Internals Book](https://technet.microsoft.com/en-us/sysinternals/bb963901)  
  The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
* [Windows Sysinternals Administrator's Reference](https://technet.microsoft.com/en-us/sysinternals/hh290819)  
  The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

**Download**

[[Download icon](https://download.sysinternals.com/files/ProcessExplorer.zip)](https://download.sysinternals.com/files/ProcessExplorer.zip)

[**Download Process Explorer**](https://download.sysinternals.com/files/ProcessExplorer.zip)**(1.8 MB)**

[**Run Process Explorer**](https://live.sysinternals.com/procexp.exe) now from Live.Sysinternals.com

# PsTools

https://technet.microsoft.com/en-us/sysinternals/bb896649

PsTools

**By Mark Russinovich**

Published: July 4, 2016

[**[Download icon](https://download.sysinternals.com/files/PSTools.zip) Download PsTools Suite**](https://download.sysinternals.com/files/PSTools.zip)**(2.7 MB)**

|  |  |
| --- | --- |
| **Rate:** |  |

**Introduction**

The Windows NT and Windows 2000 Resource Kits come with a number of command-line tools that help you administer your Windows NT/2K systems. Over time, I've grown a collection of similar tools, including some not included in the Resource Kits. What sets these tools apart is that they all allow you to manage remote systems as well as the local one. The first tool in the suite was PsList, a tool that lets you view detailed information about processes, and the suite is continually growing. The "Ps" prefix in PsList relates to the fact that the standard UNIX process listing command-line tool is named "ps", so I've adopted this prefix for all the tools in order to tie them together into a suite of tools named PsTools.

Note: some anti-virus scanners report that one or more of the tools are infected with a "remote admin" virus. None of the PsTools contain viruses, but they have been used by viruses, which is why they trigger virus notifications.

The tools included in the PsTools suite, which are downloadable as a package, are:

* [PsExec](https://technet.microsoft.com/en-us/sysinternals/bb897553) - execute processes remotely
* [PsFile](https://technet.microsoft.com/en-us/sysinternals/psfile) - shows files opened remotely
* [PsGetSid](https://technet.microsoft.com/en-us/sysinternals/bb897417) - display the SID of a computer or a user
* [PsInfo](https://technet.microsoft.com/en-us/sysinternals/psinfo) - list information about a system
* [PsPing](https://technet.microsoft.com/en-us/sysinternals/jj729731) - measure network performance
* [PsKill](https://technet.microsoft.com/en-us/sysinternals/pskill) - kill processes by name or process ID
* [PsList](https://technet.microsoft.com/en-us/sysinternals/pslist) - list detailed information about processes
* [PsLoggedOn](https://technet.microsoft.com/en-us/sysinternals/psloggedon) - see who's logged on locally and via resource sharing (full source is included)
* [PsLogList](https://technet.microsoft.com/en-us/sysinternals/psloglist) - dump event log records
* [PsPasswd](https://technet.microsoft.com/en-us/sysinternals/bb897543) - changes account passwords
* [PsService](https://technet.microsoft.com/en-us/sysinternals/psservice) - view and control services
* [PsShutdown](https://technet.microsoft.com/en-us/sysinternals/psshutdown) - shuts down and optionally reboots a computer
* [PsSuspend](https://technet.microsoft.com/en-us/sysinternals/pssuspend) - suspends processes
* PsUptime - shows you how long a system has been running since its last reboot (PsUptime's functionality has been incorporated into [PsInfo](https://technet.microsoft.com/en-us/sysinternals/psinfo))

The PsTools download package includes an HTML help file with complete usage information for all the tools.

# Sysinternals Utilities

https://technet.microsoft.com/en-us/sysinternals/bb545027

|  |  |
| --- | --- |
| * [File and Disk Utilities](https://technet.microsoft.com/en-us/sysinternals/bb545046) * [Networking Utilities](https://technet.microsoft.com/en-us/sysinternals/bb795532) * [Process Utilities](https://technet.microsoft.com/en-us/sysinternals/bb795533) * [Security Utilities](https://technet.microsoft.com/en-us/sysinternals/bb795534) * [System Information Utilities](https://technet.microsoft.com/en-us/sysinternals/bb795535) * [Miscellaneous Utilities](https://technet.microsoft.com/en-us/sysinternals/bb842059)  Additional Resources  * [Forum](http://forum.sysinternals.com/) * [Site Blog](https://blogs.technet.microsoft.com/sysinternals/) * [Sysinternals Learning](https://technet.microsoft.com/en-us/sysinternals/bb469930) * [Mark's Webcasts](https://technet.microsoft.com/en-us/sysinternals/bb963887) * [Mark's Blog](https://blogs.technet.microsoft.com/markrussinovich/) * [Software License](https://technet.microsoft.com/en-us/sysinternals/bb469936) * [Licensing FAQ](https://technet.microsoft.com/en-us/sysinternals/bb847944) | Sysinternals Utilities Index [Sysinternals Suite](https://technet.microsoft.com/en-us/sysinternals/bb842062) The entire set of Sysinternals Utilities rolled up into a single download.  [Sysinternals Suite for Nano Server](https://download.sysinternals.com/files/SysinternalsSuite-Nano.zip) Sysinternals Utilities for Nano Server in a single download.  [AccessChk](https://technet.microsoft.com/en-us/sysinternals/accesschk) v6.1 (February 17, 2017) AccessChk is a command-line tool for viewing the effective permissions on files, registry keys, services, processes, kernel objects, and more.  [AccessEnum](https://technet.microsoft.com/en-us/sysinternals/accessenum) v1.32 (November 1, 2006) This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.  [AdExplorer](https://technet.microsoft.com/en-us/sysinternals/adexplorer) v1.44 (November 15, 2012) Active Directory Explorer is an advanced Active Directory (AD) viewer and editor.  [AdInsight](https://technet.microsoft.com/en-us/sysinternals/bb897539) v1.2 (October 26, 2015) An LDAP (Light-weight Directory Access Protocol) real-time monitoring tool aimed at troubleshooting Active Directory client applications.  [AdRestore](https://technet.microsoft.com/en-us/sysinternals/adrestore) v1.1 (November 1, 2006) Undelete Server 2003 Active Directory objects.  [Autologon](https://technet.microsoft.com/en-us/sysinternals/autologon) v3.10 (August 29, 2016) Bypass password screen during logon.  [Autoruns](https://technet.microsoft.com/en-us/sysinternals/bb963902) v13.7 (February 17, 2017) See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.  [BgInfo](https://technet.microsoft.com/en-us/sysinternals/bginfo) v4.21 (February 17, 2017) This fully-configurable program automatically generates desktop backgrounds that include important information about the system including IP addresses, computer name, network adapters, and more.  [BlueScreen](https://technet.microsoft.com/en-us/sysinternals/bluescreen) v3.2 (November 1, 2006) This screen saver not only accurately simulates Blue Screens, but simulated reboots as well (complete with CHKDSK), and works on Windows NT 4, Windows 2000, Windows XP, Server 2003 and Windows 95 and 98.  [CacheSet](https://technet.microsoft.com/en-us/sysinternals/bb897561) v1.0 (November 1, 2006) CacheSet is a program that allows you to control the Cache Manager's working set size using functions provided by NT. It's compatible with all versions of NT.  [ClockRes](https://technet.microsoft.com/en-us/sysinternals/bb897568) v2.1 (July 4, 2016) View the resolution of the system clock, which is also the maximum timer resolution.  [Contig](https://technet.microsoft.com/en-us/sysinternals/contig) v1.8 (July 4, 2016) Wish you could quickly defragment your frequently used files? Use Contig to optimize individual files, or to create new files that are contiguous.  [Coreinfo](https://technet.microsoft.com/en-us/sysinternals/cc835722) v3.31 (August 18, 2014) Coreinfo is a new command-line utility that shows you the mapping between logical processors and the physical processor, NUMA node, and socket on which they reside, as well as the cache’s assigned to each logical processor.  [Ctrl2cap](https://technet.microsoft.com/en-us/sysinternals/bb897578) v2.0 (November 1, 2006) This is a kernel-mode driver that demonstrates keyboard input filtering just above the keyboard class driver in order to turn caps-locks into control keys. Filtering at this level allows conversion and hiding of keys before NT even "sees" them. Ctrl2cap also shows how to use NtDisplayString() to print messages to the initialization blue-screen.  [DebugView](https://technet.microsoft.com/en-us/sysinternals/debugview) v4.81 (December 4, 2012) Another first from Sysinternals: This program intercepts calls made to DbgPrint by device drivers and OutputDebugString made by Win32 programs. It allows for viewing and recording of debug session output on your local machine or across the Internet without an active debugger.  [Desktops](https://technet.microsoft.com/en-us/sysinternals/cc817881) v2.0 (October 17, 2012) This new utility enables you to create up to four virtual desktops and to use a tray interface or hotkeys to preview what’s on each desktop and easily switch between them.  [Disk2vhd](https://technet.microsoft.com/en-us/sysinternals/ee656415) v2.01 (January 21, 2014) Disk2vhd simplifies the migration of physical systems into virtual machines (p2v).  [DiskExt](https://technet.microsoft.com/en-us/sysinternals/diskext) v1.2 (July 4, 2016) Display volume disk-mappings.  [Diskmon](https://technet.microsoft.com/en-us/sysinternals/diskmon) v2.01 (November 1, 2006) This utility captures all hard disk activity or acts like a software disk activity light in your system tray.  [DiskView](https://technet.microsoft.com/en-us/sysinternals/bb896650) v2.4 (March 25, 2010) Graphical disk sector utility.  [Disk Usage (DU)](https://technet.microsoft.com/en-us/sysinternals/du) v1.6 (July 4, 2016) View disk usage by directory.  [EFSDump](https://technet.microsoft.com/en-us/sysinternals/efsdump) v1.02 (November 1, 2006) View information for encrypted files.  [FindLinks](https://technet.microsoft.com/en-us/sysinternals/findlinks) v1.1 (July 4, 2016) FindLinks reports the file index and any hard links (alternate file paths on the same volume) that exist for the specified file.  A file's data remains allocated so long as at it has at least one file name referencing it.  [Handle](https://technet.microsoft.com/en-us/sysinternals/handle) v4.1 (July 4, 2016) This handy command-line utility will show you what files are open by which processes, and much more.  [Hex2dec](https://technet.microsoft.com/en-us/sysinternals/hex2dec) v1.1 (July 4, 2016) Convert hex numbers to decimal and vice versa.  [Junction](https://technet.microsoft.com/en-us/sysinternals/bb896768) v1.07 (July 4, 2016) Create Win2K NTFS symbolic links.  [LDMDump](https://technet.microsoft.com/en-us/sysinternals/ldmdump) v1.02 (November 1, 2006) Dump the contents of the Logical Disk Manager's on-disk database, which describes the partitioning of Windows 2000 Dynamic disks.  [ListDLLs](https://technet.microsoft.com/en-us/sysinternals/bb896656) v3.2 (July 4, 2016) List all the DLLs that are currently loaded, including where they are loaded and their version numbers.  [LiveKd](https://technet.microsoft.com/en-us/sysinternals/livekd) v5.61 (February 17, 2017) Use Microsoft kernel debuggers to examine a live system.  [LoadOrder](https://technet.microsoft.com/en-us/sysinternals/loadorder) v1.01 (July 4, 2016) See the order in which devices are loaded on your WinNT/2K system.  [LogonSessions](https://technet.microsoft.com/en-us/sysinternals/logonsessions) v1.4 (July 4, 2016) List the active logon sessions on a system.  [MoveFile](https://technet.microsoft.com/en-us/sysinternals/pendmoves) v1.01 (January 24, 2013) Allows you to schedule move and delete commands for the next reboot.  [NotMyFault](https://technet.microsoft.com/en-us/sysinternals/notmyfault) v4.01 (November 18, 2016) Notmyfault is a tool that you can use to crash, hang, and cause kernel memory leaks on your Windows system.  [NTFSInfo](https://technet.microsoft.com/en-us/sysinternals/bb897424) v1.2 (July 4, 2016) Use NTFSInfo to see detailed information about NTFS volumes, including the size and location of the Master File Table (MFT) and MFT-zone, as well as the sizes of the NTFS meta-data files.  [PendMoves](https://technet.microsoft.com/en-us/sysinternals/pendmoves) v1.2 (February 5, 2013) Enumerate the list of file rename and delete commands that will be executed the next boot.  [PipeList](https://technet.microsoft.com/en-us/sysinternals/dd581625) v1.02 (July 4, 2016) Displays the named pipes on your system, including the number of maximum instances and active instances for each pipe.  [PortMon](https://technet.microsoft.com/en-us/sysinternals/portmon) v3.03 (January 12, 2012) Monitor serial and parallel port activity with this advanced monitoring tool. It knows about all standard serial and parallel IOCTLs and even shows you a portion of the data being sent and received. Version 3.x has powerful new UI enhancements and advanced filtering capabilities.  [ProcDump](https://technet.microsoft.com/en-us/sysinternals/dd996900) v8.2 (November 18, 2016) This command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate process dumps when a process has a hung window or unhandled exception.  [Process Explorer](https://technet.microsoft.com/en-us/sysinternals/processexplorer) v16.2 (February 17, 2017) Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.  [Process Monitor](https://technet.microsoft.com/en-us/sysinternals/processmonitor) v3.32 (February 17, 2017) Monitor file system, Registry, process, thread and DLL activity in real-time.  [PsExec](https://technet.microsoft.com/en-us/sysinternals/bb897553) v2.11 (May 2, 2014) Execute processes on remote systems.  [PsFile](https://technet.microsoft.com/en-us/sysinternals/psfile) v1.02 (December 4, 2006) See what files are opened remotely.  [PsGetSid](https://technet.microsoft.com/en-us/sysinternals/bb897417) v1.44 (April 28, 2010) Displays the SID of a computer or a user.  [PsInfo](https://technet.microsoft.com/en-us/sysinternals/psinfo) v1.77 (April 28, 2010) Obtain information about a system.  [PsKill](https://technet.microsoft.com/en-us/sysinternals/pskill) v1.15 (June 28, 2012) Terminate local or remote processes.  [PsPing](https://technet.microsoft.com/en-us/sysinternals/psping) v2.01 (January 29, 2014) Measure network performance.  [PsList](https://technet.microsoft.com/en-us/sysinternals/pslist) v1.3 (March 23, 2012) Show information about processes and threads.  [PsLoggedOn](https://technet.microsoft.com/en-us/sysinternals/psloggedon) v1.34 (April 28, 2010) Show users logged on to a system.  [PsLogList](https://technet.microsoft.com/en-us/sysinternals/psloglist) v2.71 (April 28, 2010) Dump event log records.  [PsPasswd](https://technet.microsoft.com/en-us/sysinternals/bb897543) v1.23 (October 17, 2012) Changes account passwords.  [PsService](https://technet.microsoft.com/en-us/sysinternals/psservice) v2.24 (April 28, 2010) View and control services.  [PsShutdown](https://technet.microsoft.com/en-us/sysinternals/psshutdown) v2.52 (December 4, 2006) Shuts down and optionally reboots a computer.  [PsSuspend](https://technet.microsoft.com/en-us/sysinternals/pssuspend) v1.06 (December 4, 2006) Suspend and resume processes.  [PsTools](https://technet.microsoft.com/en-us/sysinternals/pstools) v2.45 (July 4, 2016) The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.  [RAMMap](https://technet.microsoft.com/en-us/sysinternals/rammap) v1.5 (February 2, 2016) An advanced physical memory usage analysis utility that presents usage information in different ways on its several different tabs.  [RegDelNull](https://technet.microsoft.com/en-us/sysinternals/regdelnull) v1.11 (July 4, 2016) Scan for and delete Registry keys that contain embedded null-characters that are otherwise undeleteable by standard Registry-editing tools.  [Registry Usage (RU)](https://technet.microsoft.com/en-us/sysinternals/ru) v1.2 (July 4, 2016) View the registry space usage for the specified registry key.  [RegJump](https://technet.microsoft.com/en-us/sysinternals/regjump) v1.1 (April 20, 2015) Jump to the registry path you specify in Regedit.  [SDelete](https://technet.microsoft.com/en-us/sysinternals/sdelete) v2.0 (July 4, 2016) Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.  [ShareEnum](https://technet.microsoft.com/en-us/sysinternals/shareenum) v1.6 (November 1, 2006) Scan file shares on your network and view their security settings to close security holes.  [ShellRunas](https://technet.microsoft.com/en-us/sysinternals/cc300361) v1.01 (February 28, 2008) Launch programs as a different user via a convenient shell context-menu entry.  [Sigcheck](https://technet.microsoft.com/en-us/sysinternals/bb897441) v2.54 (August 29, 2016) Dump file version information and verify that images on your system are digitally signed.  [Streams](https://technet.microsoft.com/en-us/sysinternals/streams) v1.6 (July 4, 2016) Reveal NTFS alternate streams.  [Strings](https://technet.microsoft.com/en-us/sysinternals/strings) v2.52 (June 20, 2013) Search for ANSI and UNICODE strings in binary images.  [Sync](https://technet.microsoft.com/en-us/sysinternals/bb897438) v2.2 (July 4, 2016) Flush cached data to disk.  [Sysmon](https://technet.microsoft.com/en-us/sysinternals/sysmon) v6.01 (March 13, 2017) Monitors and reports key system activity via the Windows event log.  [TCPView](https://technet.microsoft.com/en-us/sysinternals/tcpview) v3.05 (July 25, 2011) Active socket command-line viewer.  [VMMap](https://technet.microsoft.com/en-us/sysinternals/vmmap) v3.21 (July 20, 2015) VMMap is a process virtual and physical memory analysis utility.  [VolumeId](https://technet.microsoft.com/en-us/sysinternals/bb897436) v2.1 (July 4, 2016) Set Volume ID of FAT or NTFS drives.  [Whois](https://technet.microsoft.com/en-us/sysinternals/whois) v1.14 (July 4, 2016) See who owns an Internet address.  [WinObj](https://technet.microsoft.com/en-us/sysinternals/winobj) v2.22 (February 14, 2011) The ultimate Object Manager namespace viewer is here.  [ZoomIt](https://technet.microsoft.com/en-us/sysinternals/zoomit) v4.5 (June 20, 2013) Presentation utility for zooming and drawing on the screen. |