PsExec

Using PsExec

See the July 2004 issue of *Windows IT Pro Magazine* for [Mark's article](http://windowsitpro.com/systems-management/psexec) that covers advanced usage of PsExec.

**Usage: psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][-r servicename][-h][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]**

|  |  |
| --- | --- |
| **-a** | Separate processors on which the application can run with commas where 1 is the lowest numbered CPU. For example, to run the application on CPU 2 and CPU 4, enter: "-a 2,4" |
| **-c** | Copy the specified program to the remote system for execution. If you omit this option the application must be in the system path on the remote system. |
| **-d** | Don't wait for process to terminate (non-interactive). |
| **-e** | Does not load the specified account’s profile. |
| **-f** | Copy the specified program even if the file already exists on the remote system. |
| **-i** | Run the program so that it interacts with the desktop of the specified session on the remote system. If no session is specified the process runs in the console session. |
| **-h** | If the target system is Vista or higher, has the process run with the account's elevated token, if available. |
| **-l** | Run process as limited user (strips the Administrators group and allows only privileges assigned to the Users group). On Windows Vista the process runs with Low Integrity. |
| **-n** | Specifies timeout in seconds connecting to remote computers. |
| **-p** | Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password. |
| **-r** | Specifies the name of the remote service to create or interact with. |
| **-s** | Run the remote process in the System account. |
| **-u** | Specifies optional user name for login to remote computer. |
| **-v** | Copy the specified file only if it has a higher version number or is newer on than the one on the remote system. |
| **-w** | Set the working directory of the process (relative to remote computer). |
| **-x** | Display the UI on the Winlogon secure desktop (local system only). |
| **-priority** | Specifies -low, -belownormal, -abovenormal, -high or -realtime to run the process at a different priority. Use -background to run at low memory and I/O priority on Vista. |
| **computer** | Direct PsExec to run the application on the remote computer or computers specified. If you omit the computer name, PsExec runs the application on the local system, and if you specify a wildcard (\\\*), PsExec runs the command on all computers in the current domain. |
| **@file** | PsExec will execute the command on each of the computers listed in the file. |
| **cmd** | Name of application to execute. |
| **arguments** | Arguments to pass (note that file paths must be absolute paths on the target system). |
| **-accepteula** | This flag suppresses the display of the license dialog. |

You can enclose applications that have spaces in their name with quotation marks e.g.

**psexec \\marklap"c:\long name app.exe"**

Input is only passed to the remote system when you press the Enter key. Typing Ctrl-C terminates the remote process.

If you omit a user name, the process will run in the context of your account on the remote system, but will not have access to network resources (because it is impersonating). Specify a valid user name in the Domain\User syntax if the remote process requires access to network resources or to run in a different account. Note that the password and command are encrypted in transit to the remote system.

Error codes returned by PsExec are specific to the applications you execute, not PsExec.

Examples

This article I wrote [describes how PsExec works](http://windowsitpro.com/systems-management/psexec) and gives tips on how to use it:

The following command launches an interactive command prompt on \\marklap:

**psexec \\marklap cmd**

This command executes IpConfig on the remote system with the /all switch, and displays the resulting output locally:

**psexec \\marklap ipconfig /all**

This command copies the program test.exe to the remote system and executes it interactively:

**psexec \\marklap -c test.exe**

Specify the full path to a program that is already installed on a remote system if its not on the system's path:

**psexec \\marklap c:\bin\test.exe**

Run Regedit interactively in the System account to view the contents of the SAM and SECURITY keys::

**psexec -i -d -s c:\windows\regedit.exe**

To run Internet Explorer as with limited-user privileges use this command:

**psexec -l -d "c:\program files\internet explorer\iexplore.exe"**

Using PsFile

The default behavior of *PsFile* is to list the files on the local system that are open by remote systems. Typing a command followed by "- " displays information on the syntax for the command.

**Usage: psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]]**

|  |  |
| --- | --- |
| **-u** | Specifies optional user name for login to remote computer. |
| **-p** | Specifies password for user name. If this is omitted, you will be prompted to enter the password without it being echoed to the screen. |
| **Id** | Identifier (as assigned by PsFile) of the file for which to display information or to close. |
| **Path** | Full or partial path of files to match for information display or close. |
| **-c** | Closes the files identifed by ID or path. |

PsGetSid

Usage

**Usage: psgetsid [\\computer[,computer[,...] | @file] [-u username [-p password]]] [account|SID]**

|  |  |
| --- | --- |
| **-u** | Specifies optional user name for login to remote computer. |
| **-p** | Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password. |
| **Account** | PsGetSid will report the SID for the specified user account rather than the computer. |
| **SID** | PsGetSid will report the account for the specified SID. |
| **Computer** | Direct PsGetSid to perform the command on the remote computer or computers specified. If you omit the computer name PsGetSid runs the command on the local system, and if you specify a wildcard (\\\*), PsGetSid runs the command on all computers in the current domain. |
| **@file** | PsGetSid will execute the command on each of the computers listed in the file. |

If you want to see a computer's SID just pass the computer's name as a command-line argument. If you want to see a user's SID, name the account (e.g. "administrator") on the command-line and an optional computer name.

Specify a user name if the account you are running from doesn't have administrative privileges on the computer you want to query. If you don't specify a password as an option, *PsGetSid* will prompt you for one so that you can type it in without having it echoed to the display.

Using PsInfo

By default *PsInfo* shows information for the local system. Specify a remote computer name to obtain information from the remote system. Since *PsInfo* relies on remote Registry access to obtain its data, the remote system must be running the Remote Registry service and the account from which you run *PsInfo* must have access to the HKLM\System portion of the remote Registry.

In order to aid in automated Service Pack updates, *PsInfo* returns as a value the Service Pack number of system (e.g. 0 for no service pack, 1 for SP 1, etc).

**Usage: psinfo [[\\computer[,computer[,..] | @file [-u user  
[-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]**

|  |  |
| --- | --- |
| **\\computer** | Perform the command on the remote computer or computers specified. If you omit the computer name the command runs on the local system, and if you specify a wildcard (\\\*), the command runs on all computers in the current domain. |
| **@file** | Run the command on each computer listed in the text file specified. |
| **-u** | Specifies optional user name for login to remote computer. |
| **-p** | Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password. |
| **-h** | Show list of installed hotfixes. |
| **-s** | Show list of installed applications. |
| **-d** | Show disk volume information. |
| **-c** | Print in CSV format. |
| **-t** | The default delimiter for the -c option is a comma, but can be overriden with the specified character. |
| **filter** | Psinfo will only show data for the field matching the filter. e.g. "psinfo service" lists only the service pack field. |
|  |  |

Using PsPing

*PsPing* implements Ping functionality, TCP ping, latency and bandwidth measurement. Use the following command-line options to show the usage for each test type:

**Usage: psping -? [i|t|l|b]**

|  |  |
| --- | --- |
| **-? I** | Usage for ICMP ping. |
| **-? T** | Usage for TCP ping. |
| **-? L** | Usage for latency test. |
| **-? B** | Usage for bandwidth test. |

**ICMP ping usage: psping [[-6]|[-4]] [-h [buckets | <val1>,<val2>,...]] [-i <interval>] [-l <requestsize>[k|m] [-q] [-t|-n <count>] [-w <count>] <destination>**

|  |  |
| --- | --- |
| **-h** | Print histogram (default bucket count is 20). If you specify a single argument, it's interpreted as a bucket count and the histogram will contain that number of buckets covering the entire time range of values. Specify a comma-separated list of times to create a custom histogram (e.g. "0.01,0.05,1,5,10"). |
| **-i** | Interval in seconds. Specify 0 for fast ping. |
| **-l** | Request size. Append 'k' for kilobytes and 'm' for megabytes. |
| **-n** | Number of pings or append 's' to specify seconds e.g. '10s'. |
| **-q** | Don't output during pings. |
| **-t** | Ping until stopped with Ctrl+C and type Ctrl+Break for statistics. |
| **-w** | Warmup with the specified number of iterations (default is 1). |
| **-4** | Force using IPv4. |
| **-6** | Force using IPv6. |

For high-speed ping tests use -q and -i 0.

**TCP ping usage: psping [[-6]|[-4]] [-h [buckets | <val1>,<val2>,...]] [-i <interval>] [-l <requestsize>[k|m] [-q] [-t|-n <count>] [-w <count>] <destination:destport>**

|  |  |
| --- | --- |
| **-h** | Print histogram (default bucket count is 20). If you specify a single argument, it's interpreted as a bucket count and the histogram will contain that number of buckets covering the entire time range of values. Specify a comma-separated list of times to create a custom histogram (e.g. "0.01,0.05,1,5,10"). |
| **-i** | Interval in seconds. Specify 0 for fast ping. |
| **-l** | Request size. Append 'k' for kilobytes and 'm' for megabytes. |
| **-n** | Number of pings or append 's' to specify seconds e.g. '10s'. |
| **-q** | Don't output during pings. |
| **-t** | Ping until stopped with Ctrl+C and type Ctrl+Break for statistics. |
| **-w** | Warmup with the specified number of iterations (default is 1). |
| **-4** | Force using IPv4. |
| **-6** | Force using IPv6. |

For high-speed ping tests use -q and -i 0.

**TCP and UDP latency usage:**

**server: psping [[-6]|[-4]] [-f] <-s source:sourceport>**

**client: psping [[-6]|[-4]] [-f] [-u] [-h [buckets | <val1>,<val2>,...]] [-r] <-l requestsize>[k|m]] <-n count> [-w <count>] <destination:destport>**

|  |  |
| --- | --- |
| **-f** | Open source firewall port during the run. |
| **-u** | UDP (default is TCP). |
| **-h** | Print histogram (default bucket count is 20). If you specify a single argument, it's interpreted as a bucket count and the histogram will contain that number of buckets covering the entire time range of values. Specify a comma-separated list of times to create a custom histogram (e.g. "0.01,0.05,1,5,10"). |
| **-l** | Request size. Append 'k' for kilobytes and 'm' for megabytes. |
| **-n** | Number of sends/receives. Append 's' to specify seconds e.g. '10s' |
| **-r** | Receive from the server instead of sending. |
| **-w** | Warmup with the specified number of iterations (default is 5). |
| **-4** | Force using IPv4. |
| **-6** | Force using IPv6. |
| **-s** | Server listening address and port. |

The server can serve both latency and bandwidth tests and remains active until you terminate it with Control-C.

**TCP and UDP bandwidth usage:**

**server: psping [[-6]|[-4]] [-f] <-s source:sourceport>**

**client: psping [[-6]|[-4]] [-f] [-u] [-h [buckets | <val1>,<val2>,...]] [-r] <-l requestsize>[k|m]] <-n count> [-i <outstanding>] [-w <count>] <destination:destport>**

|  |  |
| --- | --- |
| **-f** | Open source firewall port during the run. |
| **-u** | UDP (default is TCP). |
| **-b** | Bandwidth test. |
| **-h** | Print histogram (default bucket count is 20). If you specify a single argument, it's interpreted as a bucket count and the histogram will contain that number of buckets covering the entire time range of values. Specify a comma-separated list of times to create a custom histogram (e.g. "0.01,0.05,1,5,10"). |
| **-i** | Number of outstanding I/Os (default is min of 16 and 2x CPU cores). |
| **-l** | Request size. Append 'k' for kilobytes and 'm' for megabytes. |
| **-n** | Number of sends/receives. Append 's' to specify seconds e.g. '10s' |
| **-r** | Receive from the server instead of sending. |
| **-w** | Warmup for the specified iterations (default is 2x CPU cores). |
| **-4** | Force using IPv4. |
| **-6** | Force using IPv6. |
| **-s** | Server listening address and port. |

The server can serve both latency and bandwidth tests and remains active until you terminate it with Control-C.

Using PsKill

See the September 2004 issue of Windows IT Pro Magazine for [Mark's article](http://windowsitpro.com/search/results/Mark's%20article?filters=ss_type:Article) that covers advanced usage of *PsKill*.

Running *PsKill* with a process ID directs it to kill the process of that ID on the local computer. If you specify a process name *PsKill* will kill all processes that have that name.

**Usage: pskill [- ] [-t] [\\computer [-u username] [-p password]] <process name | process id>**

|  |  |
| --- | --- |
| **-** | Displays the supported options. |
| **-t** | Kill the process and its descendants. |
| **\\computer** | Specifies the computer on which the process you want to terminate is executing. The remote computer must be accessible via the NT network neighborhood. |
| **-u username** | If you want to kill a process on a remote system and the account you are executing in does not have administrative privileges on the remote system then you must login as an administrator using this command-line option. If you do not include the password with the -p option then *PsKill* will prompt you for the password without echoing your input to the display. |
| **-p password** | This option lets you specify the login password on the command line so that you can use PsList from batch files. If you specify an account name and omit the -p option PsList prompts you interactively for a password. |
| **process id** | Specifies the process ID of the process you want to kill. |
| **process name** | Specifies the process name of the process or processes you want to kill. |

s

|  |  |
| --- | --- |
| **pslist exp** | would show statistics for all the processes that start with "exp", which would include Explorer. |
| **-d** | Show thread detail. |
| **-m** | Show memory detail. |
| **-x** | Show processes, memory information and threads. |
| **-t** | Show process tree. |
| **-s [n]** | Run in task-manager mode, for optional seconds specified. Press Escape to abort. |
| **-r n** | Task-manager mode refresh rate in seconds (default is 1). |
| **\\computer** | Instead of showing process information for the local system, *PsList* will show information for the NT/Win2K system specified. Include the -u switch with a username and password to login to the remote system if your security credentials do not permit you to obtain performance counter information from the remote system. |
| **-u** | username If you want to kill a process on a remote system and the account you are executing in does not have administrative privileges on the remote system then you must login as an administrator using this command-line option. If you do not include the password with the -p option then *PsList* will prompt you for the password without echoing your input to the display. |
| **-p** | password This option lets you specify the login password on the command line so that you can use *PsList* from batch files. If you specify an account name and omit the -p option *PsList* prompts you interactively for a password. |
| **name** | Show information about processes that begin with the name specified. |
| **-e** | Exact match the process name. |
| **pid** | Instead of listing all the running processes in the system, this parameter narrows *PsList's* scan to the process that has the specified PID. Thus: **pslist 53** would dump statistics for the process with the PID 53. |

Using PsLoggedOn

**Usage: psloggedon [- ] [-l] [-x] [\\computername | username]**

|  |  |
| --- | --- |
| **-** | Displays the supported options and the units of measurement used for output values. |
| **-l** | Shows only local logons instead of both local and network resource logons. |
| **-x** | Don't show logon times. |
| **\\computername** | Specifies the name of the computer for which to list logon information. |
| **username** | If you specify a user name *PsLoggedOn* searches the network for computers to which that user is logged on. This is useful if you want to ensure that a particular user is not logged on when you are about to change their user profile configuration. |

**usage: pspasswd [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] Username [NewPassword]**

|  |  |
| --- | --- |
| **computer** | Perform the command on the remote computer or computers specified. If you omit the computer name the command runs on the local system, and if you specify a wildcard (\\\*), the command runs on all computers in the current domain. |
| **@file** | Run the command on each computer listed in the text file specified. |
| **-u** | Specifies optional user name for login to remote computer. |
| **-p** | Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password. |
| **Username** | Specifies name of account for password change. |
| **NewPassword** | New password. If ommitted a NULL password is applied. |

Using PsService

The default behavior of *PsService* is to display the configured services (both running and stopped) on the local system. Entering a command on the command-line invokes a particular feature, and some commands accept options. Typing a command followed by "- " displays information on the syntax for the command.

**Usage: psservice [\\computer [-u username] [-p password]] <command> <options>**

|  |  |
| --- | --- |
| **query** | Displays the status of a service. |
| **config** | Displays the configuration of a service. |
| **setconfig** | Sets the start type (disabled, auto, demand) of a service. |
| **start** | Starts a service. |
| **stop** | Stops a service. |
| **restart** | Stops and then restarts a service. |
| **pause** | Pauses a service |
| **cont** | Resumes a paused service. |
| **depend** | Lists the services dependent on the one specified. |
| **security** | Dumps the service's security descriptor. |
| **find** | Searches the network for the specified service. |
| **\\computer** | Targets the NT/Win2K system specified. Include the -u switch with a username and password to login to the remote system if your security credentials do not permit you to obtain performance counter information from the remote system. If you specify the -u option, but not a password with the -p option, *PsService* will prompt you to enter the password and will not echo it to the screen. |

Using PsShutdown

See the February 2005 issue of Windows IT Pro Magazine for [Mark's article](http://www.windowsitpro.com/Article/ArticleID/44973/44973.html) that covers advanced usage of *PsKill*.

You can use *PsShutdown* to initiate a shutdown of the local or a remote computer, logoff a user, lock a system, or to abort an imminent shutdown.

**Usage: psshutdown [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s] [-v nn] [-e [u|p]:xx:yy] [-m "message"]**

|  |  |
| --- | --- |
| **-** | Displays the supported options. |
| **computer** | Perform the command on the remote computer or computers specified. If you omit the computer name the command runs on the local system, and if you specify a wildcard (\\\*), the command runs on all computers in the current domain. |
| **@file** | Run the command on each computer listed in the text file specified. |
| **-u** | Specifies optional user name for login to remote computer. |
| **-p** | Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password. |
| **-a** | Aborts a shutdown (only possible while a countdown is in progress). |
| **-c** | Allows the shutdown to be aborted by the interactive user. |
| **-d** | Suspend the computer. |
| **-e** | Shutdown reason code. Specify 'u' for user reason codes and 'p' for planned shutdown reason codes. xx is the major reason code (must be less than 256). yy is the minor reason code (must be less than 65536). |
| **-f** | Forces all running applications to exit during the shutdown instead of giving them a chance to gracefully save their data. |
| **-h** | Hibernate the computer. |
| **-k** | Poweroff the computer (reboot if poweroff is not supported). |
| **-l** | Lock the computer. |
| **-m** | This option lets you specify a message to display to logged-on users when a shutdown countdown commences. |
| **-n** | Specifies timeout in seconds connecting to remote computers. |
| **-o** | Logoff the console user. |
| **-r** | Reboot after shutdown. |
| **-s** | Shutdown without power off. |
| **-t** | Specifies the countdown in seconds until the shutdown (default: 20 seconds) or the time of shutdown (in 24 hour notation). |
| **-v** | Display message for the specified number of seconds before the shutdown. If you omit this parameter the shutdown notification dialog displays and specifying a value of 0 results in no dialog. |

Using PsSuspend

Running *PsSuspend* with a process ID directs it to suspend or resume the process of that ID on the local computer. If you specify a process name *PsSuspend* will suspend or resume all processes that have that name. Specify the -r switch to resume suspended processes.

**Usage: pssuspend [- ] [-r] [\\computer [-u username] [-p password]] <process name | process id>**

|  |  |
| --- | --- |
| **-** | Displays the supported options. |
| **-r** | Resumes the specified processes specified if they are suspended. |
| **\\computer** | Specifies the computer on which the process you want to suspend or resume is executing. The remote computer must be accessible via the NT network neighborhood. |
| **-u username** | If you want to suspend a process on a remote system and the account you are executing in does not have administrative privileges on the remote system then you must login as an administrator using this command-line option. If you do not include the password with the -p option then *PsSuspend* will prompt you for the password without echoing your input to the display. |
| **-p password** | This option lets you specify the login password on the command line so that you can use *PsSuspend* from batch files. If you specify an account name and omit the -p option *PsSuspend* prompts you interactively for a password. |
| **process id** | Specifies the process ID of the process you want to suspend or resume. |
| **process name** | Specifies the process name of the process or processes you want to suspend or resume. |